

JP1 Version 11

**Performance Management: Getting Started  
(Service Level Management)**

3021-3-A31-10(E)

## Notices

### ■ Relevant program products

*JP1/Service Level Management - Manager (for Windows)*

P-292C-FABL JP1/Service Level Management - Manager version 11-01 (for Windows Server 2008 R2, Windows Server 2012, Windows Server 2016)

*JP1/Service Level Management - User Response (for Windows)*

P-292C-FBBL JP1/Service Level Management - User Response version 11-00 (for Windows Server 2008 R2, Windows Server 2012, Windows Server 2016)

### ■ Export restrictions

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

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

### ■ Trademarks

HITACHI, HiRDB, JP1 are either trademarks or registered trademarks of Hitachi, Ltd. in Japan and other countries. Internet Explorer is either a registered trademark or 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.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

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

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

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

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

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](mailto: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).



JP1/Service Level Management - Manager and JP1/Service Level Management - User Response includes RSA<sup>(R)</sup> BSAFE<sup>TM</sup> Cryptographic software of EMC Corporation.



### ■ 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 Windows Server 2008 R2 Datacenter
		Microsoft Windows Server 2008 R2 Enterprise
		Microsoft Windows Server 2008 R2 Standard
	Windows Server 2012	Microsoft Windows Server 2012 Datacenter
		Microsoft Windows Server 2012 Standard
		Microsoft Windows Server 2012 R2 Datacenter
		Microsoft Windows Server 2012 R2 Standard
	Windows Server 2016	Microsoft Windows Server 2016 Datacenter
		Microsoft Windows Server 2016 Standard



■ **Issued**

Apr. 2020: 3021-3-A31-10(E)

■ **Copyright**

All Rights Reserved. Copyright (C) 2016, 2020, Hitachi, Ltd.

## Summary of amendments

The following table lists changes in this manual (3021-3-A31-10(E)) and product changes related to this manual.

Changes	Location
Internet Explorer versions earlier than 11 are no longer supported.	-
Following the removal of Flash Player as a prerequisite product, all screenshots in this manual were updated. In addition, the descriptions of some windows were changed.	Throughout the manual
The use of Windows Server 2016 is now supported.	<a href="#">1.2.1</a>

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

# Preface

## ■ What you can do with JP1/Service Level Management

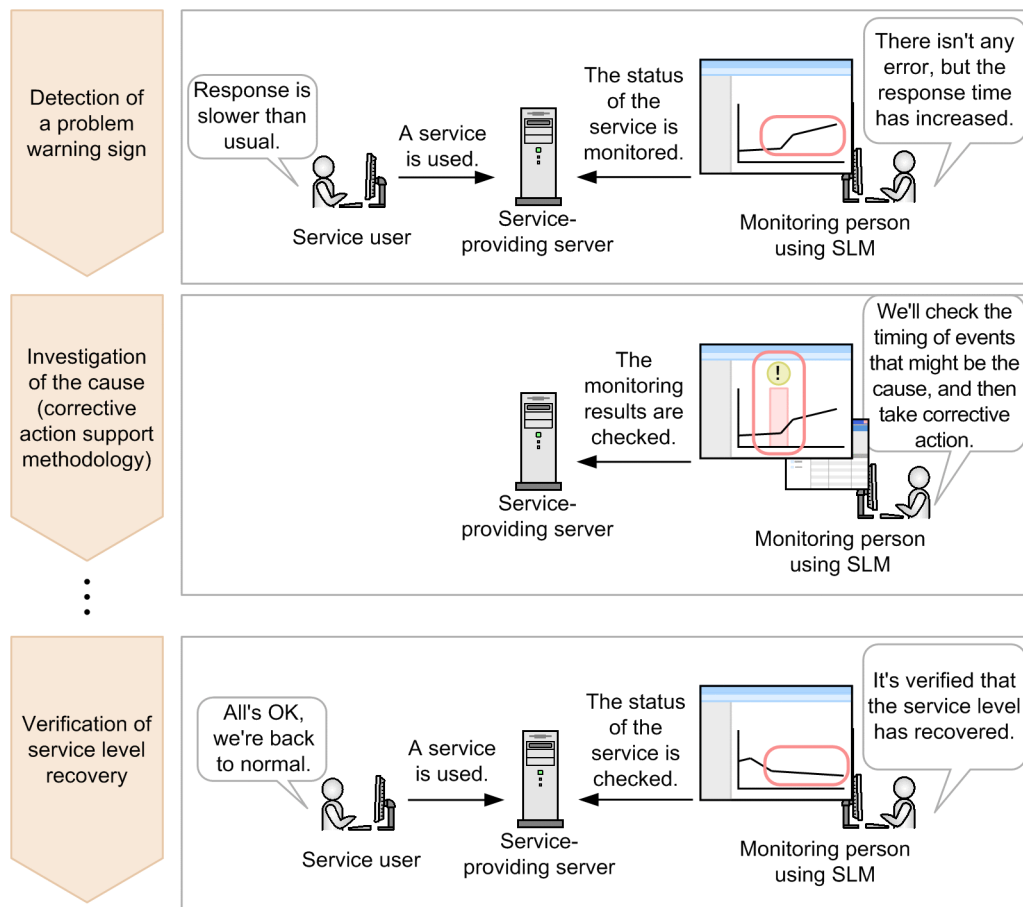
In recent years, many business systems have been created to provide services to users.

The business system (the service) must be 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.

JP1/Service Level Management (SLM) meets these demands by providing the capability to monitor the service status and maintain a required service level.

SLM can achieve monitoring based on threshold values that are used as evaluation metrics (SLOs). SLM can also predict an abnormality in service performance by monitoring for unusual service status.

The following provides an example in which SLM detects an unusual service status as a sign of an abnormality in the performance of a monitored service, and allows for handling of problems at an early stage.



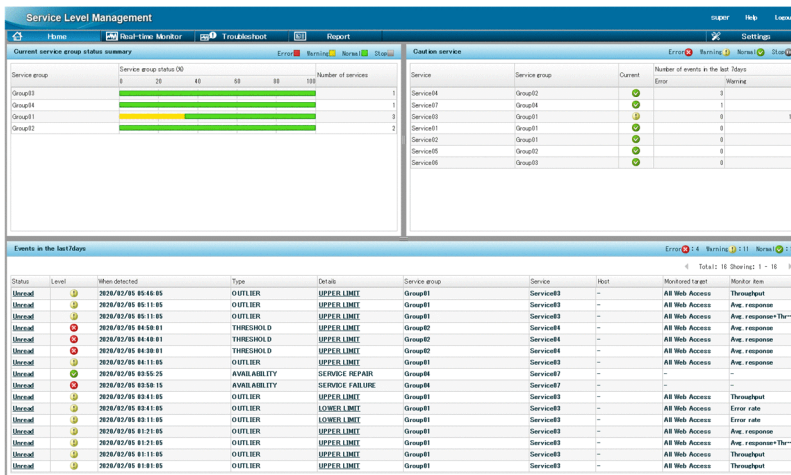
1. Slower response time (a sign of an abnormality in service performance) is detected during service status monitoring by SLM.
2. The user checks the past monitoring results in SLM to determine when the event that is regarded as the cause (of the sign of the abnormality in service performance) occurred.  
The result of this confirmation can be used to take appropriate action for the detected event.
3. The user identifies the cause and takes appropriate action to solve any potential problems. If the user can confirm that the level of service has recovered on SLM, handling of the abnormalities in service performance is complete.

Thus, by detecting any signs of abnormality in a monitored service's performance, SLM can facilitate handling of any problems before they occur, thereby increasing the satisfaction of the service's users.

SLM also supports maintenance of the level of service by providing various windows.

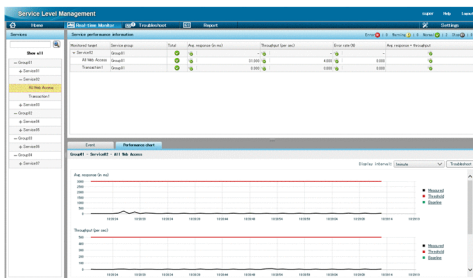
### One-glance display of all service statuses

You can check the statuses of all monitored services in an integrated manner.



### Real-time monitoring of level of services

You can check the detailed status of monitored services in real time.



### Problem investigation support

You can check when the event that caused a problem occurred.



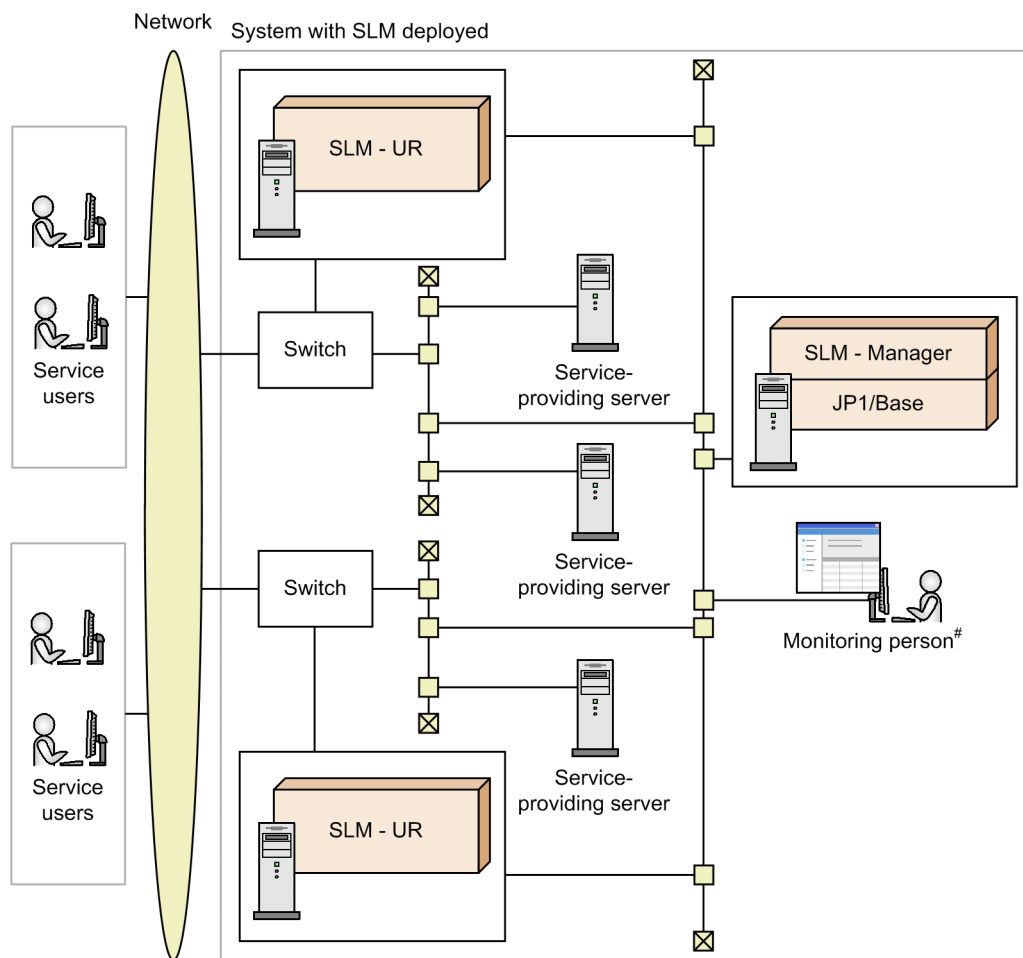
In this manual, JP1/Service Level Management - Manager and JP1/Service Level Management - User Response are generally called *SLM*.

## ■ What is explained in this manual

This manual describes the basic functions of SLM, and how to operate SLM. This manual intends that the readers of this manual will have a general understanding of how to maintain the level of service by using SLM. This manual is intended for the following readers:

- Monitoring staff  
Person who monitors the service status by using SLM
- System operator  
Person who introduces SLM (System administrator)

Among the system configuration (service monitoring configuration) that mainly monitors the service status (service performance), this manual assumes a system configuration in which only service performance is monitored. For details about operation in other configurations, see the manual *JP1/Service Level Management*.



#

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

### SLM - Manager (JP1/Service Level Management - Manager)

Aggregates and analyzes the HTTP packets collected by SLM - 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 SLM - URs can be connected to a single SLM - Manager.

#### SLM - UR (JP1/Service Level Management - User Response)

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

A single SLM - UR can monitor multiple services.

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

#### JP1/Base

Manages the users (JP1 users) who access SLM - 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.

## ■ How to read this manual

SLM has two manuals (including this manual). Read either of the manuals, depending on your purpose.

- Getting Started (Service Level Management)  
Read this manual when you want to perform basic operations for maintaining the level of service.
- JP1/Service Level Management  
Read this manual for a detailed understanding of the operational methods for maintaining level of service, linkage with other products, and troubleshooting.

A reference to another manual is written as follows: For details about something, see *topic-title* in the manual-name. Using *topic-title* as a keyword, search for the relevant section in the target manual.

The following environment is assumed for operations in individual windows:

Operations on a computer by the person who monitors services

Environment in which Windows Server 2012 R2 and Internet Explorer 11 are used

Some windows in this manual might differ from the windows of your product because of improvements made without prior notice.

# Contents

Notices 2

Summary of amendments 5

Preface 6

## **1 Setting Up SLM 13**

- 1.1 General procedure for setting up SLM 14
- 1.2 Preparation before installation 15
  - 1.2.1 Prerequisite OSs 15
  - 1.2.2 Memory and disk space required for installation 15
- 1.3 Installing the prerequisite product 16
  - 1.3.1 Installing and setting up JP1/Base 16
- 1.4 Installing SLM 17
  - 1.4.1 Installing SLM 17
- 1.5 Setting up SLM 19
  - 1.5.1 Setting up SLM - Manager 19
  - 1.5.2 Setting up SLM - UR 20
- 1.6 Setting users in SLM 23
  - 1.6.1 Procedure for specifying user settings in SLM 23
  - 1.6.2 Authentication server 23
  - 1.6.3 Setting up JP1 users in JP1/Base 25
  - 1.6.4 Specifying operation permissions for each JP1 user 26

## **2 Editing the System Definition Files of SLM 28**

- 2.1 Editing the system definition files to change settings 29
  - 2.1.1 Editing the system definition files 29
  - 2.1.2 Editable definitions 30

## **3 Starting and Logging In to SLM 33**

- 3.1 Starting SLM 34
  - 3.1.1 Starting SLM - Manager 34
  - 3.1.2 Starting SLM - UR 35
- 3.2 Logging in to SLM - Manager 37
  - 3.2.1 Logging in to SLM - Manager 37
  - 3.2.2 Notes about operations after login to SLM - Manager 39

## **4 Monitoring the Services to Be Monitored and Setup Required for Monitoring 41**

- 4.1 Monitoring supported by SLM 42
- 4.2 Monitoring methods and monitor items of SLM 43
  - 4.2.1 Monitoring all Web accesses (All Web Access monitoring) 43
  - 4.2.2 Monitoring items for All Web Access 43
- 4.3 Detection of an excess beyond the threshold by threshold value monitoring 45
- 4.4 Advance detection of an excess beyond the threshold by trend monitoring 47
- 4.5 Detection of an unusual status of a monitored service by out-of-range value detection 50
- 4.6 How to register monitored services and set up monitoring items 55
  - 4.6.1 Registering monitored services 55
  - 4.6.2 Setting up the monitoring items for service performance 57

## **5 Monitoring Services by Using SLM 61**

- 5.1 Overview of monitoring tasks using SLM 62
- 5.2 General monitoring procedure 63
- 5.3 Starting monitoring 64
  - 5.3.1 Starting monitoring 64
- 5.4 Monitoring the status of monitored services 66
  - 5.4.1 Checking the status of the monitored services of all service groups 66
  - 5.4.2 Checking the status of the monitored services in a specific service group 67

## **6 Supporting Root Cause Investigation When an Error or Warning Is Displayed for a Monitored Service 70**

- 6.1 Support of root cause investigation when an error or warning is displayed for a monitored service 71
  - 6.1.1 Predictive error detection in the performance of a monitored service 71
  - 6.1.2 Corrective action to be taken after a warning sign was detected in the performance of a monitored service 72
    - 6.1.3 Verifying the service performance after taking corrective action 73
- 6.2 Checking when an event causing an error or warning occurred 74
  - 6.2.1 Checking the timing of an event causing an error or warning 74
- 6.3 Checking the past performance of monitored services 77
  - 6.3.1 Checking the past performance of monitored services 77
- 6.4 Verifying the recovery of a monitored service after taking corrective action 80
  - 6.4.1 Verifying the recovery of monitored services after taking corrective action 80

## **Appendixes 82**

- A Commands 83
  - A.1 Format of command explanations 83
  - A.2 List of commands 83
  - A.3 Notes about command execution 84
  - A.4 jslmmgrsetup (sets up SLM - Manager) 85

A.5	jslmurnals(displays the network adapter address and IP address)	89
A.6	jslmursetup (sets up SLM - UR)	90
B	List of Port Numbers Used by SLM	93
C	SLM Communication	95
D	Advanced Use	97
E	Reference Material for This Manual	98
E.1	Related publications	98
E.2	Conventions: Fonts and symbols	98
E.3	Conventions: SLM installation folder	99
E.4	Conventions: Abbreviations for product names	99
E.5	Conventions: Acronyms	100
E.6	Conventions: Units (such as KB, MB, GB, and TB)	100
F	Glossary	101

## **Index 104**

# 1

## Setting Up SLM

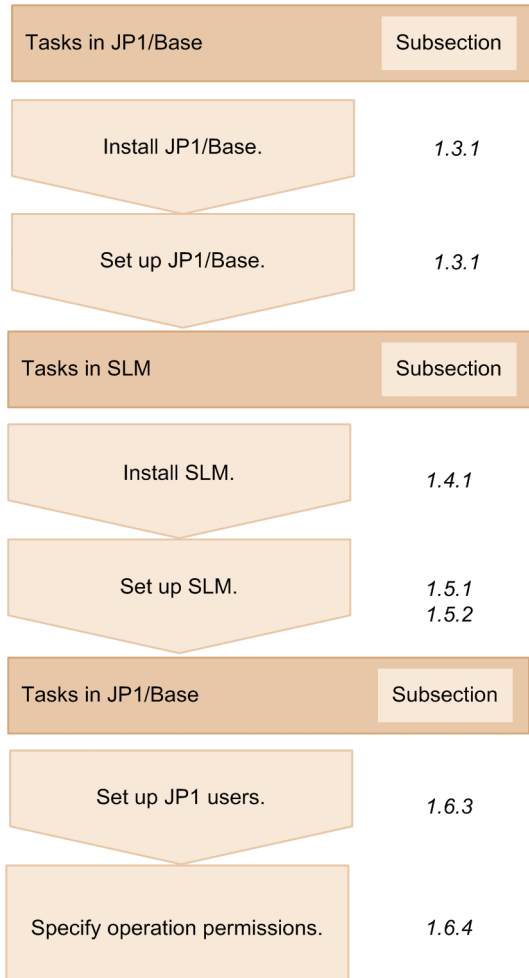
This chapter describes the preparation required for starting SLM, such as the installation, setup, and user settings.

# 1.1 General procedure for setting up SLM

---

The following figure shows the general procedure for setting up SLM.

Figure 1-1: General procedure for setting up SLM



## 1.2 Preparation before installation

---

The following describes the preparation necessary before installing SLM.

### 1.2.1 Prerequisite OSs

The following shows the prerequisite OSs for SLM.

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

### 1.2.2 Memory and disk space required for installation

For details about the memory and disk space required for installing SLM, see the Release Notes.

## 1.3 Installing the prerequisite product

---

Install and set up JP1/Base, which is a prerequisite product for SLM.

### 1.3.1 Installing and setting up JP1/Base

Install JP1/Base on the host on which you install SLM - Manager. For details about how to install and set up JP1/Base, see the JP1/Base User's Guide.



## 1.4 Installing SLM

---

To install SLM, install SLM - Manager and SLM - UR. The method of installing SLM is the same as for SLM - Manager and SLM - UR.

### 1.4.1 Installing SLM

Use an installer to install SLM - Manager or SLM - UR. The system operator performs this operation.

#### (1) Before you start

- Verify that your user account belongs to the OS's Administrators group.

#### (2) Procedure

To install SLM:

1. Insert the distribution medium into the correct drive.
2. Install SLM 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 SLM - UR is being installed on the same host where SLM - Manager has already been installed, the installation folder for SLM - UR will already be set to the folder specified when SLM - Manager was installed; no other folder can be specified. Similarly, if SLM - Manager is being installed on the same host where SLM - UR has already been installed, the installation folder for SLM - Manager will already be set to the folder specified when SLM - 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 SLM - Manager has been installed.

For details about how to install JP1/Base, see the *JP1/Base User's Guide*.

- The reference time of the host on which SLM - Manager and SLM - UR have been installed is GMT. On the other hand, the reference time of the computer from which a monitoring person logs in to SLM - Manager is based on that computer's time zone.
- When SLM - Manager or SLM - 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 SLM - Manager or SLM - UR on a host on which the same version of SLM - Manager or SLM - 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 SLM - Manager or SLM - 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 SLM - Manager or SLM - UR on a host on which the same version of SLM - Manager or SLM - UR has already been installed.
- If SLM 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

- [1.5.1 Setting up SLM - Manager](#) or [1.5.2 Setting up SLM - UR](#)

## 1.5 Setting up SLM

Set up SLM - Manager and SLM - UR.

### 1.5.1 Setting up SLM - Manager

Set up SLM - Manager to create an execution environment. Use the `jslmmgrsetup` command for setup. The system operator performs this operation.

#### (1) Before you start

- Verify that your user account belongs to the OS's Administrators group.
- Before you start the setup, install the SLM - Manager that is to be set up.  
For details about the installation, see [1.4.1 Installing SLM](#).
- Verify that JP1/Base has been installed on the host on which SLM - Manager is being installed.  
For details about how to install JP1/Base, see the *JP1/Base User's Guide*.

#### (2) Procedure

To set up SLM - Manager:

1. Create the options file required for setup.

For details about the options file, see [A.4 jslmmgrsetup \(sets up SLM - Manager\)](#) in [A. 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:

```
SLM-Manager-installation-folder\mgr\bin\jslmmgrsetup absolute-path-of-options-file
```

For details about the setup command, see [A.4 jslmmgrsetup \(sets up SLM - Manager\)](#) in [A. Commands](#).

When the command terminates normally, SLM - Manager setup is complete.

When setup finishes, the default startup method of each service is initially set as follows:

Table 1-1: Default startup method of each service when setup finishes

Service	Service name	Default startup method
SLM - Manager DB Service	HiRDBEmbeddedEdition_JL0	Automatic
SLM - Manager DB Cluster Service	HiRDBClusterService_JL0	Manual
SLM - Manager Service	JP1_ITSLM_MGR_Service	Manual
SLM - Manager Web Service	JP1_ITSLM_MGR_Web_Service	Manual

Be careful if you have already set up SLM - Manager and have changed the default startup methods of services. In this case, if you perform `unsetup` of SLM - Manager and then set it up again, the default startup methods of the services are reset to the initial settings.

### (3) Supplementary information

- If a firewall has been set up on the host on which SLM - 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 SLM - Manager and SLM - UR and between SLM - 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:
    - *SLM - Manager-installation-folder*\mgr\bin\system\jslmmUR.exe
    - *SLM - Manager-installation-folder*\mgr\bin\system\jslmmRMI.exe
    - *SLM - 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 SLM - Manager is set up.
- To adjust the time on the host on which SLM - Manager has been set up, you must first terminate all SLM - Managers and SLM - URs. To do this, first stop all services running on the SLM - Managers and SLM - URs.  
It is preferable to adjust SLM - Manager's time forward. If SLM - 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 SLM - Manager and SLM - UR. For example, if you moved the computer's time backward by five minutes, wait for at least five minutes before you start SLM - Manager.  
Note that you can adjust the time of a computer that displays windows used for monitoring at any time, regardless of whether SLM - 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:  
*SLM-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.

### (4) Next task

- [1.5.2 Setting up SLM - UR](#) or [1.6.3 Setting up JP1 users in JP1/Base](#)

## 1.5.2 Setting up SLM - UR

Set up SLM - UR to create an execution environment. The system administrator performs this operation. The system operator performs this operation.

### (1) Before you start

- Verify that your user account belongs to the OS's Administrators group.
- Before you start the setup, install the SLM - UR that is to be set up.  
For details about the installation, see [1.4.1 Installing SLM](#).

## (2) Procedure

1. Execute the command that checks the network adapter address and IP address of the host on which SLM - UR has been installed.

Execute the following command:

```
SLM-UR-installation-folder\ur\bin\jسلمurnals
```

For details about the command that checks the network adapter address and IP address, see [A.5 jسلمurnals\(displays the network adapter address and IP address\)](#) in [A. Commands](#).

2. Create the options file required for setup based on the information provided by executing the `jسلمurnals` command.

For details about the options file, see [A.6 jسلمursetup \(sets up SLM - UR\)](#) in [A. 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:

```
SLM-UR-installation-folder\ur\bin\jسلمursetup absolute-path-of-options-file
```

For details about the setup command, see [A.6 jسلمursetup \(sets up SLM - UR\)](#) in [A. Commands](#).

When the command terminates normally, SLM - UR setup is complete.

When setup finishes, the default startup method of each service is initially set as follows:

- **SLM - User Response Service:**

(Service name: `JP1_ITSLM_UR_Service`, default startup method: Manual)

Be careful if you have already set up SLM - UR and have changed the default startup methods of services. In this case, if you perform setup of SLM - UR again, the default startup methods of the services are reset to the initial settings.

## (3) Supplementary information

- If a firewall has been set up on the host on which SLM - 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 SLM - UR and SLM - 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:

- *SLM-UR-installation-folder*\ur\bin\system\jسلمuUR.exe
- *SLM-UR-installation-folder*\ur\bin\system\jسلمuRMI.exe
- *SLM-UR-installation-folder*\ur\system\sdp\bin\sدppcap.exe

- To adjust the time of the host on which SLM - UR has been set up, you must first terminate all SLM - Managers and SLM - URs.

Adjust SLM - UR's time to SLM - Manager's time. If SLM - UR's time moved backward (earlier) as a result of adjustment, there is no need to wait to start SLM - UR until the amount of time that moved backwards has elapsed. However, if monitoring of monitored services starts while SLM - UR's time is in the past, the service performance data acquired by SLM - UR is discarded until the last monitoring period has elapsed.

## **(4) Next task**

- 1.5.1 Setting up SLM - Manager or 1.6.3 Setting up JP1 users in JP1/Base

## 1.6 Setting users in SLM

---

To use SLM, prepare an **authentication server** (JP1/Base), set up JP1 users in the JP1/Base to be used as the authentication server, and then specify operation permissions in SLM.

### 1.6.1 Procedure for specifying user settings in SLM

The following describes the procedure for specifying user settings in SLM.

Figure 1-2: Procedure for specifying user settings in SLM

Tasks	Subsection
Set up JP1 users in JP1/Base.	1.6.3
Specify operation permissions for each user.	1.6.4

For details about the authentication server that must be prepared before JP1 user settings can be specified in JP1/Base, see [1.6.2 Authentication server](#).

### 1.6.2 Authentication server

To use SLM, you must have an authentication server for managing the users. SLM 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 SLM - 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.

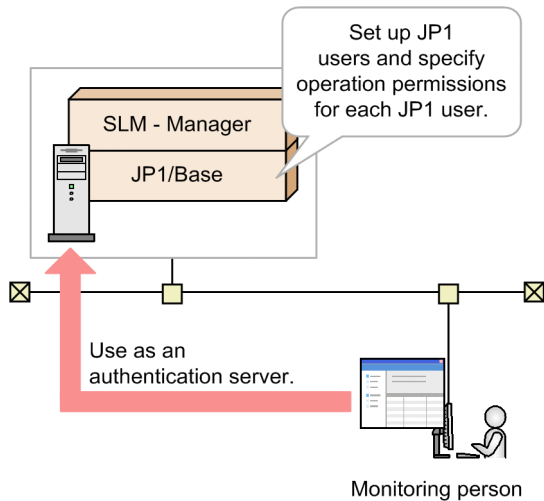
The host specified as the authentication server (primary authentication server) is used to manage JP1 users and operation permissions for JP1 resource groups (service groups).

Therefore, before you set up SLM 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 SLM - Manager is installed as the authentication server.

Figure 1-3: Using JP1/Base on the host on which SLM - Manager is installed as the authentication server

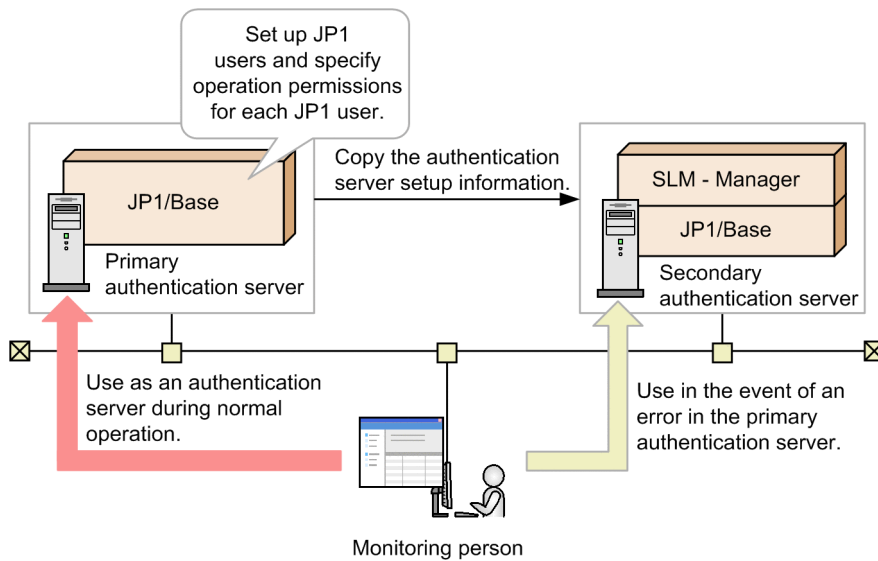


If you use JP1/Base on the host on which SLM - Manager is installed as the authentication server, you can use SLM with the minimum system configuration. However, in the event of a problem in JP1/Base, applications using SLM will stop.

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 1-4: Using two hosts on which JP1/Base is installed and using them as primary and secondary authentication servers



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 *JP1/Base User's Guide*.



## 1.6.3 Setting up JP1 users in JP1/Base

The users of SLM 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). The system operator performs this operation.

For details about the authentication server, see [1.6.2 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 SLM - 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 SLM - Manager has been set up.

For details about how to install JP1/Base, see the *JP1/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 *JP1/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 **JP1 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) Notes

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 SLM, do not perform any of the change or deletion operations in JP1/Base shown below; if any of these operations are performed, SLM 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

## (4) Supplementary information

- For details about restrictions of the specification of JP1 users, see the description about the settings of JP1 users (standard users) in the *JP1/Base User's Guide*.

## (5) Next task

- [1.6.4 Specifying operation permissions for each JP1 user](#)

### 1.6.4 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). After setting JP1 users in JP1/Base, specify operation permissions for each JP1 user. Use the JP1/Base Environment Settings dialog box of JP1/Base or JP1/Base command. In the procedure below, the JP1/Base Environment Settings dialog box is used. The system operator performs this operation.

#### (1) Before you start

- Set up the users as JP1 users.  
For details about how to set up users as JP1 users, see [1.6.3 Setting up JP1 users in JP1/Base](#).
- Evaluate how you want to set up JP1 resource groups (*service groups*<sup>#</sup>) and the JP1 permission level that is to be applied to each service group for the JP1 users.  
SLM'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 SLM, operation permissions are defined for each JP1 permission level as described in the following table.

Table 1-2: 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	<ul style="list-style-type: none"><li>• Add and delete monitored services.</li><li>• Set up monitoring items.</li><li>• Start and stop monitoring.</li><li>• Monitor the status of monitored services.</li><li>• Investigate problems.</li></ul>
2	JP1_ITSLM_User	Service user	<ul style="list-style-type: none"><li>• Monitor the status of monitored services.</li><li>• Investigate problems.</li></ul>

Because SLM 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.

For an example of specifying operation permissions for each JP1 user, see the description about the example setting of operation permissions in the manual *JP1/Service Level Management*.

## (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 *JP1/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.

# 2

## Editing the System Definition Files of SLM

To change the behavior of SLM, edit the system definition files. Perform this operation, as necessary, before starting SLM.

## 2.1 Editing the system definition files to change settings

---

To change the behavior of SLM, edit the system definition files. The following describes the system definitions that can be edited, and how to edit them.

SLM enables you to change settings, including host names and port numbers, by editing SLM - Manager's system definition file (`jplitslm.properties`) and SLM - UR's system definition file (`jplitslmur.properties`).

This section explains how to edit the system definition files and the definitions that can be edited.

### 2.1.1 Editing the system definition files

The following describes how to edit the system definition files (`jplitslm.properties` and `jplitslmur.properties`) of SLM. You can change information, such as host names and port numbers, by editing the system definition files of SLM. The system operator performs this operation.

This subsection explains how to edit SLM's system definition files (`jplitslm.properties` and `jplitslmur.properties`).

#### (1) Before you start

- Terminate the SLM - Manager or SLM - UR whose system definition file you will be editing.  
For details about the termination method, see (5) [Procedure for terminating SLM - Manager](#) in 3.1.1 [Starting SLM - Manager](#), or (5) [Procedure for terminating SLM - UR](#) in 3.1.2 [Starting SLM - 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 SLM - Manager:

*SLM-Manager-installation-folder*\mgr\conf\jplitslm.properties

For SLM - UR:

*SLM-UR-installation-folder*\ur\conf\jplitslmur.properties

For a list of the definitions that can be edited, see 2.1.2 [Editable definitions](#).

If you are editing properties that are common to both SLM - Manager and SLM - UR, make sure that you edit both system definition files.

2. Start the SLM - Manager or SLM - UR whose system definition file has been edited.

For details about how to start SLM - Manager or SLM - UR, see 3.1.1 [Starting SLM - Manager](#) or 3.1.2 [Starting SLM - UR](#).

The system definition file has been edited and the SLM 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 SLM - Manager or SLM - UR is started (or restarted).
- If an invalid keyword that is not defined in SLM is specified in a system definition file, SLM 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 SLM - Manager or SLM - 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 SLM - Manager or SLM - 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

## 2.1.2 Editable definitions

Editing definitions is optional in SLM.

This subsection explains the definitions that can be edited in SLM.

### (1) List of definitions that can be edited in SLM

The following table explains the definitions that can be edited when it is necessary to do so.

Table 2-1: List of definitions that can be edited in SLM

No.	Property	Trgt	Spec	Description	Specification range	Default	Error handling
1	managerHost	M, U	R	Specifies the host name of SLM - Manager.	<p>ASCII codes 0x20 to 0x7e (excluding control characters) and a length of 1 to 256 bytes (permitted number of bytes depends on Windows).</p> <p>Characters that are not permitted in host names in Windows cannot be specified.</p> <p>None of the following addresses can be specified:</p> <ul style="list-style-type: none"> <li>• 0.0.0.0</li> <li>• 127.0.0.1</li> <li>• 255.255.255.255</li> </ul>	None	T
2	urHost	U	R	Specifies the host name of SLM - UR.	<p>ASCII codes 0x20 to 0x7e (excluding control characters) and a length of 1 to 256 bytes (permitted number of bytes depends on Windows).</p> <p>Characters that are not permitted in host names in Windows cannot be specified.</p> <p>None of the following addresses can be specified:</p> <ul style="list-style-type: none"> <li>• 0.0.0.0</li> <li>• 127.0.0.1</li> <li>• 255.255.255.255</li> </ul>	None	T
3	urNetworkAdapterAddress	U	R	<p>Specifies the address of the network adapter to which SLM - UR connects.</p> <p>If you have changed the network interface configuration on the host on which SLM - UR is installed, make sure that you use the <code>jslmurnals</code> command to check and, if necessary, revise the specified value.</p> <p>For details about the <code>jslmurnals</code> command, see <a href="#">A.5 jslmurnals</a>(displays the network adapter address and IP address) in <a href="#">A. Commands</a>.</p>	<p>Hexadecimal integer (up to 12 digits) that uses half-width alphanumeric characters.</p> <p>Note that, if you specify a network adapter address that does not exist in the execution result of the <code>jslmurnals</code> command, an error occurs.</p>	None	T

Legend:

Trgt: Target

Spec: Specification

M: SLM - Manager

U: SLM - UR

R: Specification is required

O: Specification is optional

D: If there is an error in the setting, SLM - Manager or SLM - UR assumes the default value upon startup.

T: If there is an error in the setting, SLM - Manager or SLM - UR terminates.

#1

If you want to run SLM - 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 (`jplitslm.properties` or `jplitslmur.properties`) are stored at the following locations:

For SLM - Manager:

*SLM-Manager-installation-folder*\mgr\conf\jplitslm.properties

For SLM - UR:

*SLM-UR-installation-folder*\ur\conf\jplitslmur.properties

- The following shows example definitions in the system definition files:

For SLM - Manager:

```
managerHost=192.168.2.109
```

For SLM - UR:

```
managerHost=192.168.2.109
urHost=192.168.2.109
urNetworkAdapterAddress=005056A38090
```

- For details about the port numbers used by SLM, see [B. List of Port Numbers Used by SLM](#).



# 3

## Starting and Logging In to SLM

This chapter describes how to start and log in to SLM, and provides notes about the operations subsequent to login.

## 3.1 Starting SLM

---

In SLM, you must follow the order of starting SLM - Manager and SLM - UR. Start SLM - Manager, and then SLM - UR.

### 3.1.1 Starting SLM - Manager

To start SLM - Manager, start the services that comprise SLM - Manager and set their service status to **Start**. The system operator performs this operation.

You can have the SLM - 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 SLM or issuing JP1 events might fail. If SLM - Manager and SLM - 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 SLM - Manager services to start first when the OS starts. For details about using JP1/Base for startup control, see the *JP1/Base User's Guide*.

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

This subsection explains how to start SLM - Manager manually.

#### (1) Before you start

- Verify that JP1/Base is running.  
For details about how to start JP1/Base, see the *JP1/Base User's Guide*.
- Verify that your user account belongs to the OS's Administrators group.
- Verify that SLM - Manager has been set up.  
For details about how to set up SLM - Manager, see [1.5.1 Setting up SLM - Manager](#).
- Verify that SLM - UR is not running.

#### (2) Procedure

To start SLM - Manager:

1. From the Windows **Start** menu, select **Administrative Tools**, and then **Services**.
2. Start the SLM - Manager service **SLM - Manager DB Service** (service name: `HiRDBEmbeddedEdition_JL0`).
3. Start the SLM - Manager service **SLM - Manager Service** (service name: `JP1_ITSLM_MGR_Service`).
4. Start the SLM - Manager service **SLM - 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, SLM - Manager has started.

#### (3) Supplementary information

- To restart SLM - Manager, perform (2) [Procedure](#) after SLM - Manager has terminated.
- When you start SLM - Manager and SLM - UR, if you perform the following steps in this order, you might not be able to log in to SLM - Manager for about two minutes because it takes time for SLM - Manager to initialize:

1. Terminate SLM - Manager.
  2. Terminate SLM - UR.
  3. Start SLM - Manager.
- If you restart SLM - Manager while you are logged in to SLM - Manager, you must log in to SLM - Manager again because the logged-in session becomes invalid.  
For details about how to log in, see [3.2.1 Logging in to SLM - Manager](#).
  - The services that comprise SLM - Manager are dependent on each other. If you start **SLM - Manager Service** before starting **SLM - Manager DB Service**, **SLM - Manager DB Service** starts automatically. Similarly, if you start **SLM - Manager Web Service** before starting **SLM - Manager Service**, **SLM - Manager Service** starts automatically.
  - If you have changed the system configuration (including when you restore the system configuration after a change) while SLM - Manager is running, you must restart SLM - Manager.
  - If a firewall has been set up on the machine from which you access SLM - Manager via a browser, you need to release the ephemeral ports used for communication between the browser and SLM - Manager.

## (4) Next task

- [3.1.2 Starting SLM - UR](#)

## (5) Procedure for terminating SLM - Manager

Terminate SLM - Manager, for example, when you change the system definitions.

To terminate SLM - Manager:

1. From the Windows **Start** menu, select **Administrative Tools**, and then **Services**.
2. Stop the SLM - Manager service **SLM - Manager Web Service** (service name: JP1\_ITSLM\_MGR\_Web\_Service).
3. Stop the SLM - Manager service **SLM - Manager Service** (service name: JP1\_ITSLM\_MGR\_Service).
4. Stop the SLM - Manager service **SLM - Manager DB Service** (service name: HiRDBEmbeddedEdition\_JL0).

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

## 3.1.2 Starting SLM - UR

To start SLM - UR, start the SLM - UR service and set its service status to **Start**. The system operator performs this operation.

You can have the SLM - UR service start automatically when the OS starts if you set it up in the OS to start automatically. If SLM - Manager and SLM - 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 SLM - Manager services to start first when the OS starts. For details about using JP1/Base for startup control, see the *JP1/Base User's Guide*.

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

## (1) Before you start

- Verify that your user account belongs to the OS's Administrators group.
- Verify that SLM - UR has been set up.  
For details about how to set up SLM - UR, see [1.5.2 Setting up SLM - UR](#).
- Verify that SLM - Manager is running.  
For details about how to start SLM - Manager, see [3.1.1 Starting SLM - Manager](#).

## (2) Procedure

To start SLM - UR:

1. From the Windows **Start** menu, select **Administrative Tools**, and then **Services**.
2. Start the SLM - UR service **SLM - User Response Service** (service name: JP1\_ITSLM\_UR\_Service).

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

## (3) Supplementary information

- To restart SLM - UR, perform [\(2\) Procedure](#) after SLM - UR has terminated.
- If you restart SLM - UR while monitored services are being monitored, the restarted SLM - UR starts monitoring automatically.  
For details about starting monitoring, see [5.3.1 Starting monitoring](#).
- If you have changed the system configuration (including when you restore the system configuration after a change) while SLM - UR is running, you must restart SLM - UR.

## (4) Next task

- [3.2.1 Logging in to SLM - Manager](#)

## (5) Procedure for terminating SLM - UR

Terminate SLM - UR, for example, when you change the system definitions.

To terminate SLM - UR:

1. From the Windows **Start** menu, select **Administrative Tools**, and then **Services**.
2. Stop the SLM - UR service **SLM - User Response Service** (service name: JP1\_ITSLM\_UR\_Service).

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

## 3.2 Logging in to SLM - Manager

---

The following describes how to log in to SLM, and provides notes about the operations after login.

### 3.2.1 Logging in to SLM - Manager

To set up and perform monitoring in SLM, start Internet Explorer (browser), and then log in to SLM - Manager. The monitoring staff performs this operation.

This subsection explains how to log in to SLM - 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 SLM - Manager.  
For details about setting JP1 user operation permissions, see [1.6.4 Specifying operation permissions for each JP1 user](#).
- Verify that the target SLM - Manager is running.  
For details about starting SLM - Manager, see [3.1.1 Starting SLM - Manager](#).

If you are performing monitoring, the SLM - UR connected to the login target SLM - Manager must also be running in addition to the above conditions. For details about starting SLM - UR, see [3.1.2 Starting SLM - UR](#).

#### (2) Procedure

To log in to SLM - Manager:

1. Display the following access destination in the browser:

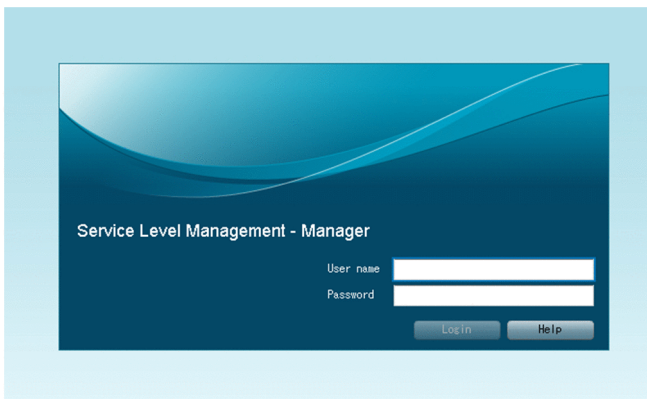
```
http://IP-address-of-SLM-Manager's-Web-server:listen-port-number-of-SLM-Manager's-Web-server/jplitslm/jplitslm.jsp
```



#### Important

Do not specify a loopback address for *IP-address-of-SLM-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 SLM - Manager window is displayed, you have successfully logged in to SLM - Manager.

### (3) Supplementary information

- *listen-port-number-of-SLM-Manager's-Web-server* is the value of the `psb_Listen` definition item in the options file that you specified when you set up SLM - 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.
- 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 log files, see the description about the log files in the manual *JP1/Service Level Management*.

- If a firewall has been set up on a host from which you access SLM - Manager via a browser, you need to configure the firewall to release ephemeral ports used for communication between the browser and SLM - Manager.

### (4) Logging out of SLM - Manager

Log out from SLM - Manager, for example, when you want to display on a browser the monitored services that other users registered or deleted.

The following window is used in this task:

1. Click **Logout** in the upper right corner of the window.

In SLM, 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.

### 3.2.2 Notes about operations after login to SLM - Manager

The following provides notes about the operations after logging in to SLM - 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 SLM - 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 SLM - 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 SLM - Manager is interrupted for one minute. You must re-log in.

For details about how to log in, see 3.2.1 [Logging in to SLM - 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.
- 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.



# 4

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

This chapter describes the different types of monitoring supported by SLM. This chapter also explains how to register the services to be monitored and how to set up the monitoring items for the monitored services.

## 4.1 Monitoring supported by SLM

---

SLM monitors three monitor items (average response time, throughput, and error rate), based on the users' actual accesses to monitored services. SLM can perform out-of-range value detection and SLO monitoring, based on the monitor items.

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.

SLM 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 4-1: 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.

## 4.2 Monitoring methods and monitor items of SLM

The following describes the monitoring methods and monitor items of SLM. A *Web access* covers the period from when a request was initiated by a user being monitored by SLM until the response to that request is completed. SLM monitors Web accesses for all monitored services.

SLM monitors Web accesses by using the following methods:

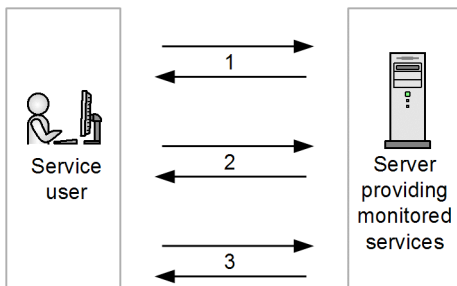
- Monitoring all Web accesses (All Web Access monitoring)  
This method monitors Web accesses for all monitored services. In this method, the monitored target is called *All Web Access*.

### 4.2.1 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 4-1: Range of monitored target when all Web accesses are monitored



Legend:

 : Web access

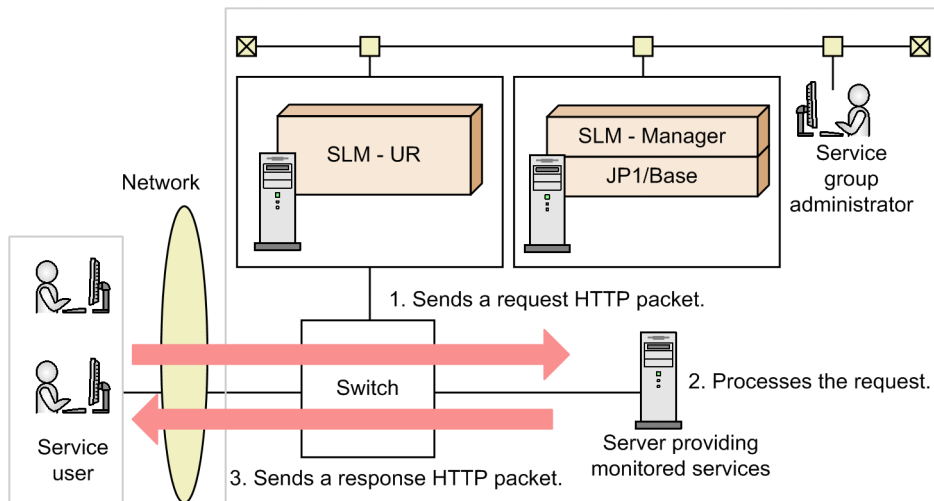
In this example, Web accesses 1 through 3 have occurred from the service user to monitored services. With this monitoring method, the averages or the totals of Web accesses 1 through 3 constitute the service performance of the monitoring items.

### 4.2.2 Monitoring items for All Web Access

All Web Access has three monitor items.

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

Figure 4-2: Relationship among monitoring items (for All Web Access)



Legend:



- 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 SLM - 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 SLM - UR.

#

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

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

## (1) Supplementary information

- The maximum length of an HTTP packet that SLM 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, SLM can monitor it successfully. Any data following byte 1,500 is discarded.

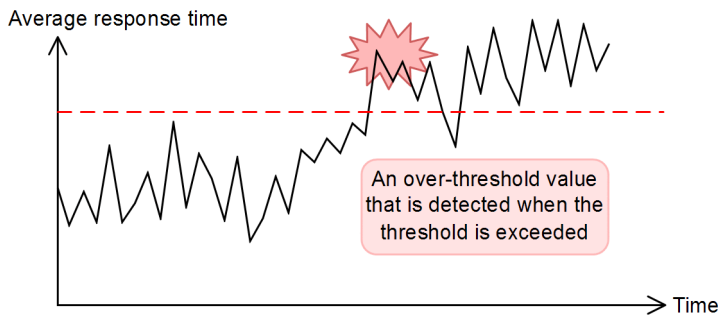
## 4.3 Detection of an excess beyond the threshold by threshold value monitoring

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

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 4-3: Example in which an overage of a threshold is detected



Legend:

--- : Threshold

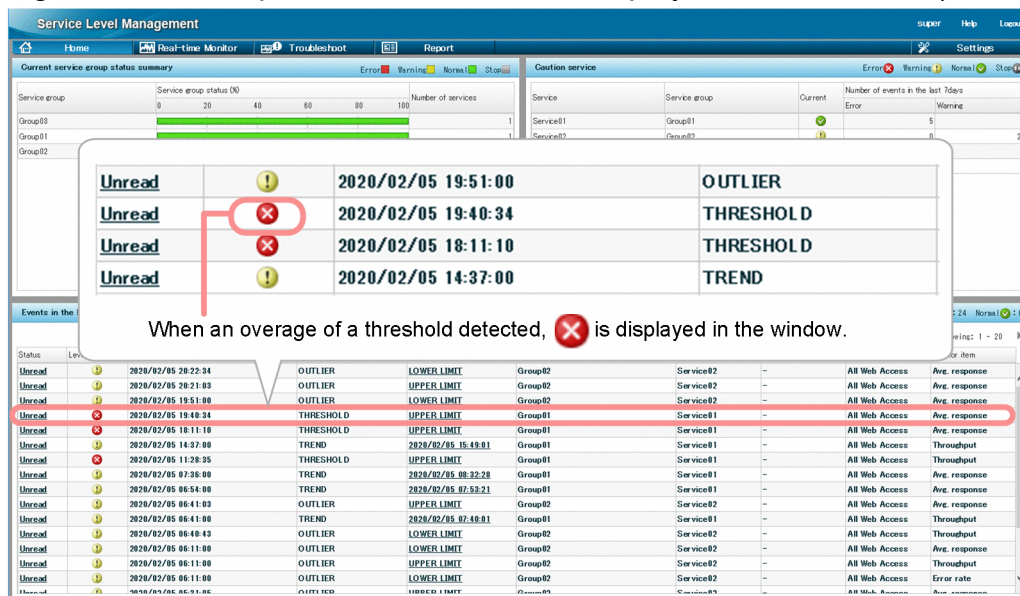
— : Service performance

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.

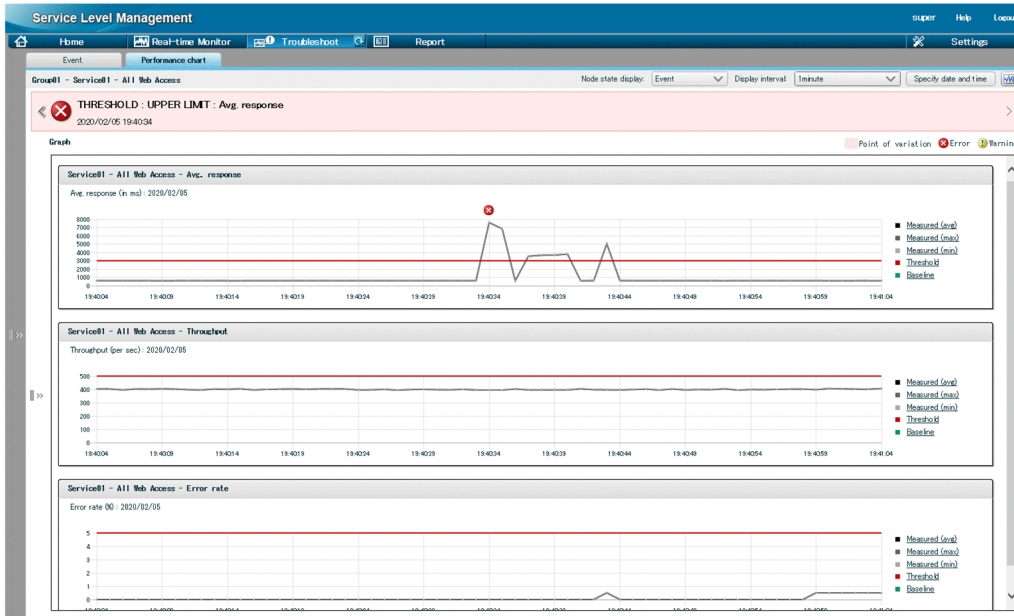
Figure 4-4: Example in which an error is displayed in the window (threshold value monitoring)



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 4-5: Example of a graph that is displayed (threshold value monitoring)



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.

For details about monitor items, see [4.2 Monitoring methods and monitor items of SLM](#).

For details about threshold value monitoring, see the description about threshold value monitoring in the manual *JPI/Service Level Management*.

## 4.4 Advance detection of an excess beyond the threshold by trend monitoring

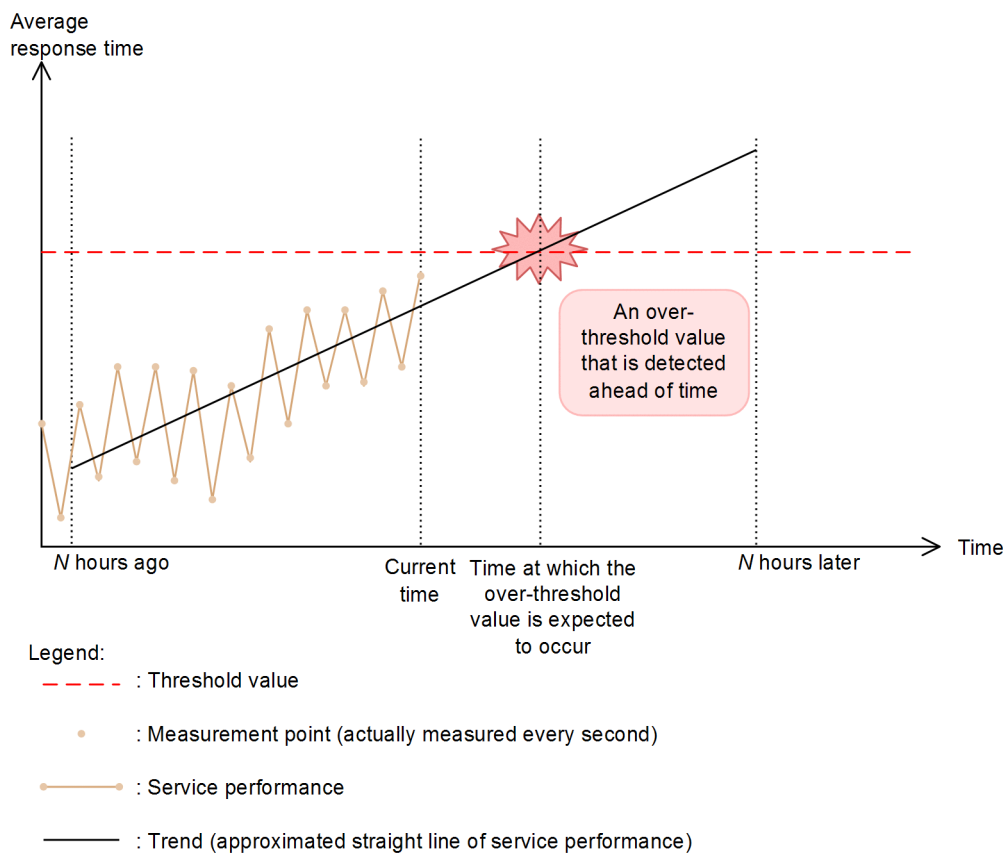
Trend monitoring calculates trends in the performance trends of monitored services and detects in advance possible overages of a service performance threshold. Trend monitoring monitors each monitoring item.

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 [4.6.2 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 4-6: Example in which an overage of a threshold is detected ahead of time



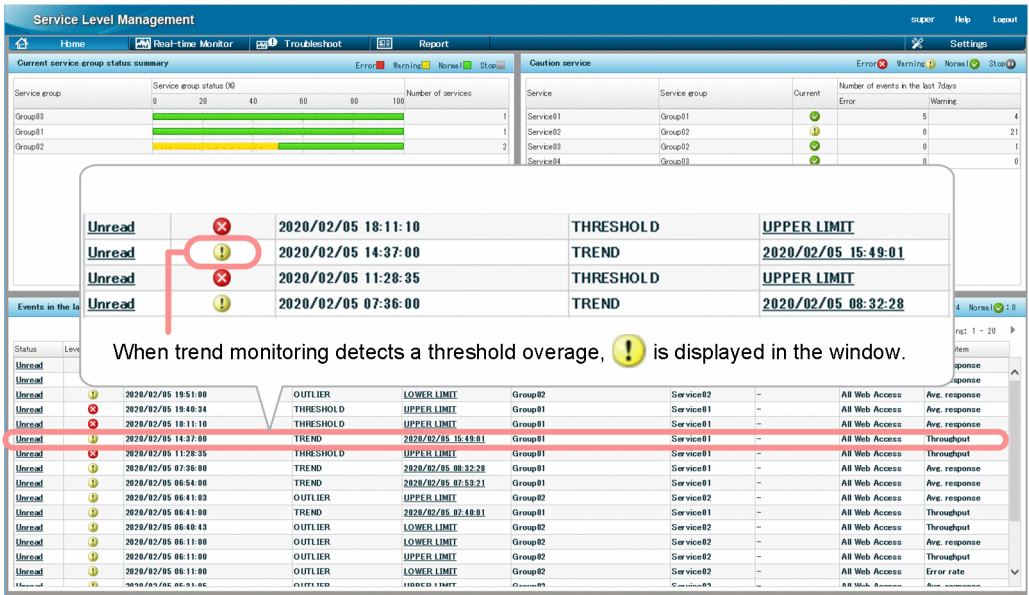
This example monitors average response time. The trend is calculated from the past  $N$  hours of service performance. A warning sign is detected if the service performance is predicted to exceed the threshold within the next  $N$  hours.

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.

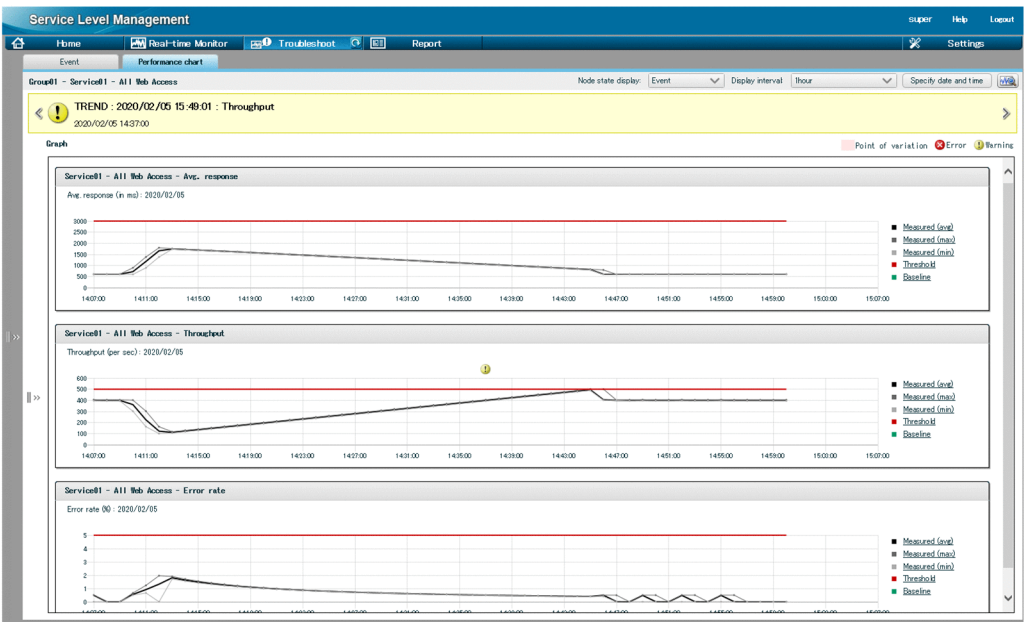
Figure 4-7: Example of a warning displayed in the window (trend monitoring)



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 4-8: Example of a graph that is displayed (trend monitoring)



In the graph, a warning icon is displayed indicating the time when a value that exceeded the trend threshold was detected. Also, a yellow band is displayed indicating the time when service performance is predicted to exceed the threshold and the time when a value that exceeded the trend threshold was detected.

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.

For details about monitor items, see [4.2 Monitoring methods and monitor items of SLM](#). Note, however, that trend monitoring cannot be used for monitoring the error rate.

For details about trend monitoring, see the description about trend monitoring in the manual *JPI/Service Level Management*.

## 4.5 Detection of an unusual status of a monitored service by out-of-range value detection

When the performance of a monitored service is particularly different from usual, out-of-range value detection perceives this as a sign of an abnormality in service performance. Out-of-range value detection is performed for each monitoring item. You can also combine multiple monitoring items and monitor them as a set.

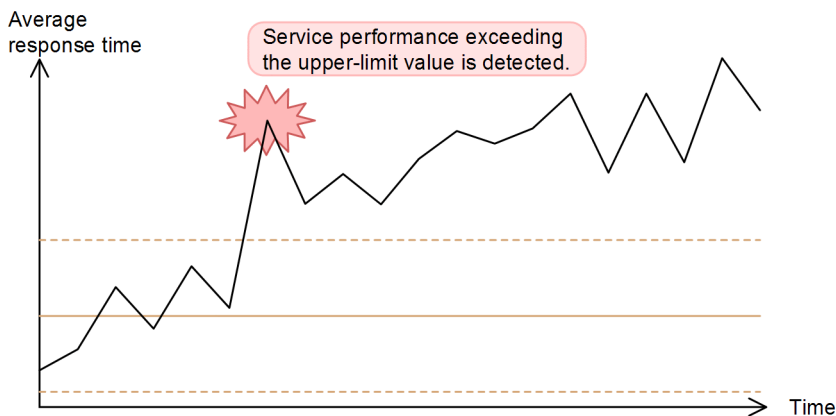
The method obtains an average value from accumulated past service performance data and detects any value that differs significantly from this average as constituting an *out-of-range value*. The average value obtained from accumulated past service performance data is called the *baseline*.

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 4-9: Example in which unusual service performance is detected by out-of-range value detection



Legend:

- : Service performance
- : Baseline
- - - : Upper-limit or lower-limit value

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.

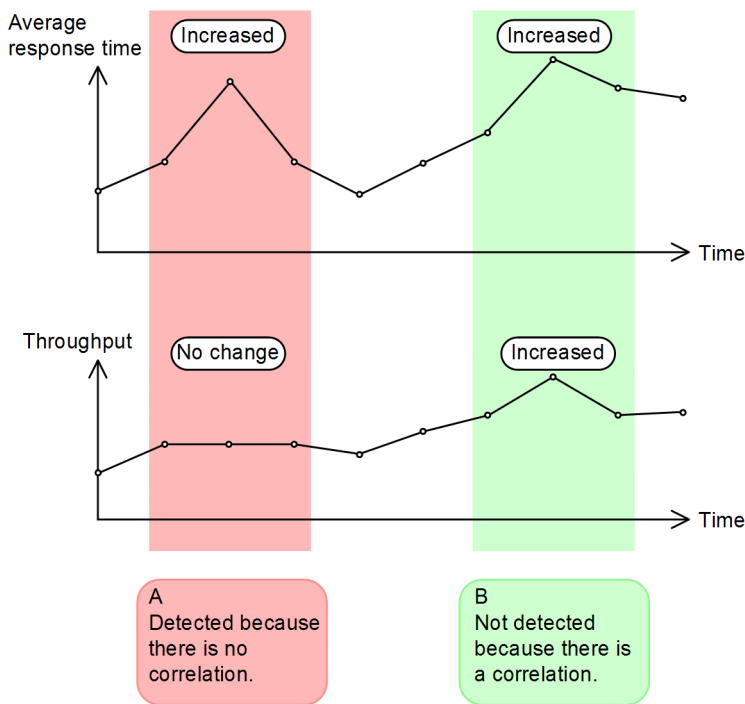
In out-of-range value detection, you can combine multiple monitoring items together as a set.

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 4-10: Example in which unusual service performance is detected by out-of-range value detection with a combination of multiple monitoring items



Legend:

- : Measurement point
- : Service performance

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.

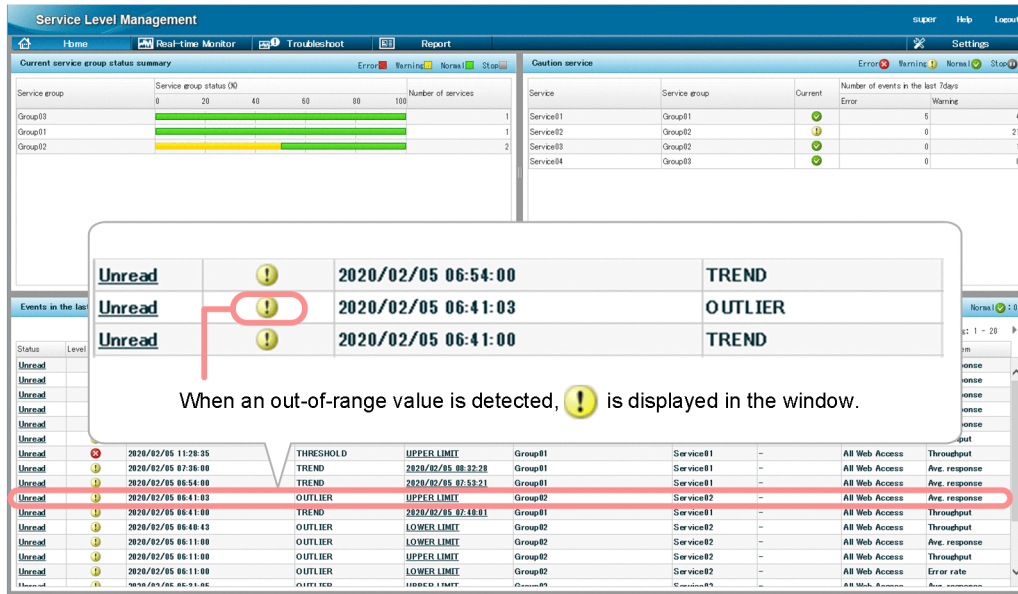
In out-of-range value detection with a combination of multiple monitoring items, the correlation of the two service performance items is taken into account in determining the baseline. When service performance falls beyond the upper-limit or lower-limit value that has been determined based on this baseline, 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.

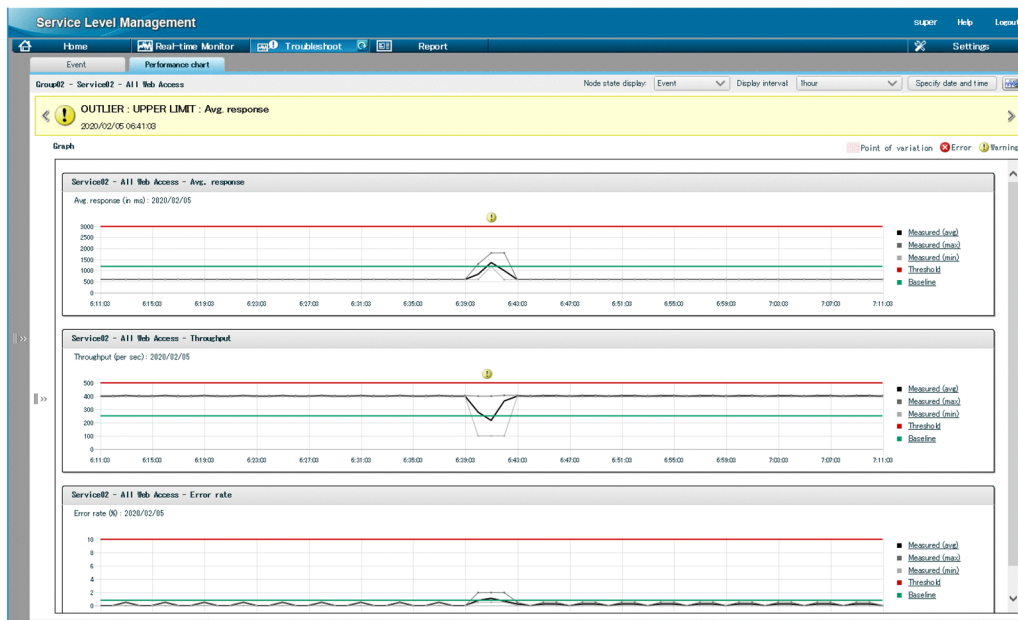
Figure 4-11: Example of window with a warning displayed (out-of-range value detection)



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 4-12: Example of a graph (out-of-range value detection)



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

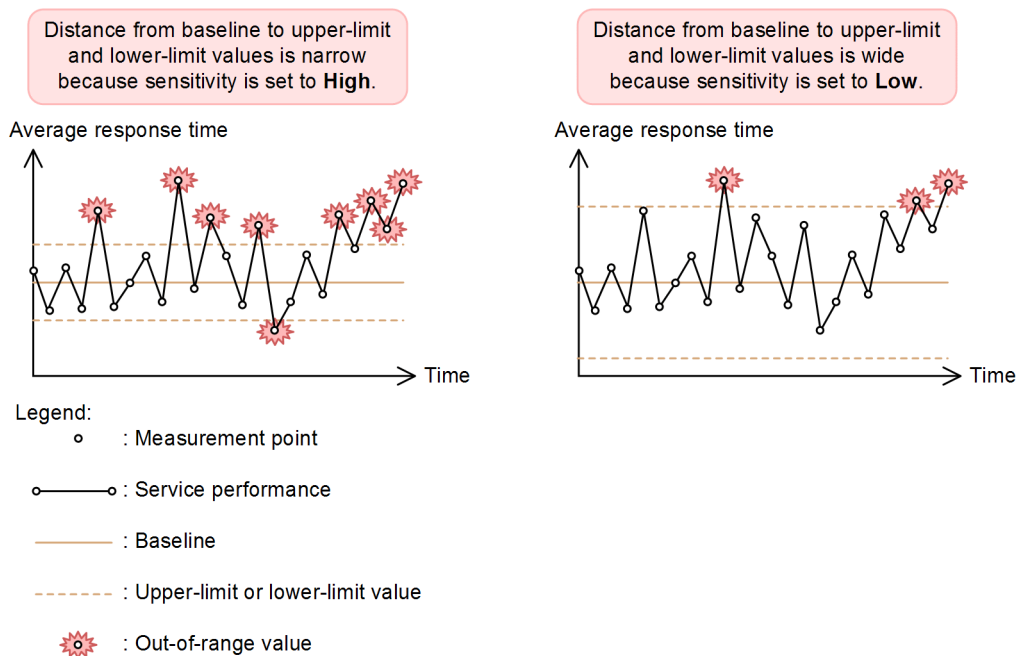
Specifies the number of days' worth of accumulated past service performance data that are to be used for calculation of the baseline.

### 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 4-13: 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.

For details about monitor items, see [4.2 Monitoring methods and monitor items of SLM](#).

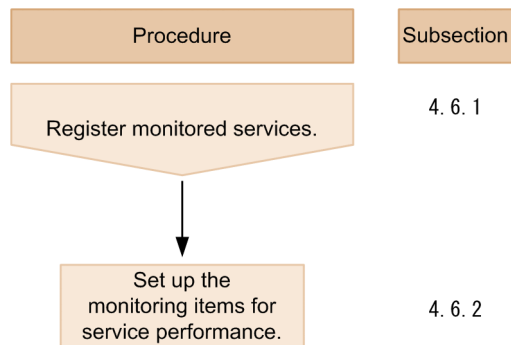
For details about out-of-range value detection, see the description about out-of-range value detection in the manual *JPI/Service Level Management*.

## 4.6 How to register monitored services and set up monitoring items

To perform monitoring, monitored services must be registered, and monitoring items must be set up.

The following figure provides an overview of the procedure.

Figure 4-14: Procedure for registering monitored services and setting up monitoring items



### 4.6.1 Registering monitored services

To add a monitoring-target service, register the URI of the service Web page in SLM - Manager. The monitoring staff performs this operation.

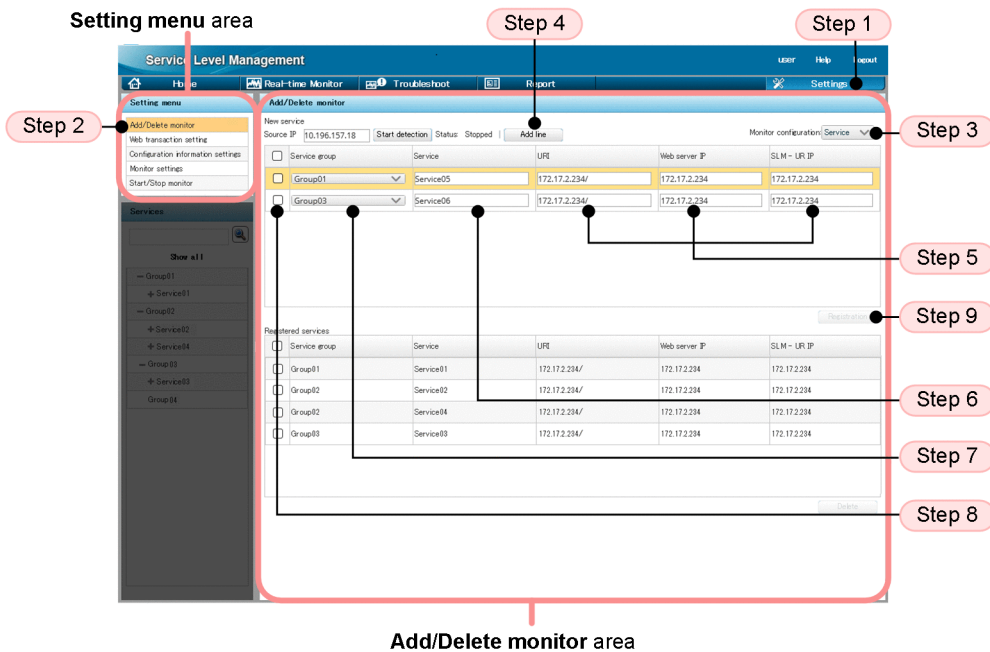
For details about the maximum number of monitored services that can be registered in SLM - Manager, see the description about the registration of monitored services in the manual *JPI/Service Level Management*.

#### (1) Before you start

- Verify that you have the service group administrator permissions.
- Log in to SLM - Manager.  
For details about how to log in, see [3.2.1 Logging in to SLM - Manager](#).
- Verify that you can access the Web page of the monitored service that you want to register from a host that is accessing SLM - Manager.

#### (2) Procedure

The following shows the Settings window used in this procedure.



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 SLM 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 SLM - UR.

3. Select **Monitor configuration**.

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

**Service:** Monitors service performance.

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 SLM - UR in **SLM - 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**.

### (3) Next task

- 4.6.2 Setting up the monitoring items for service performance

## 4.6.2 Setting up the monitoring items for service performance

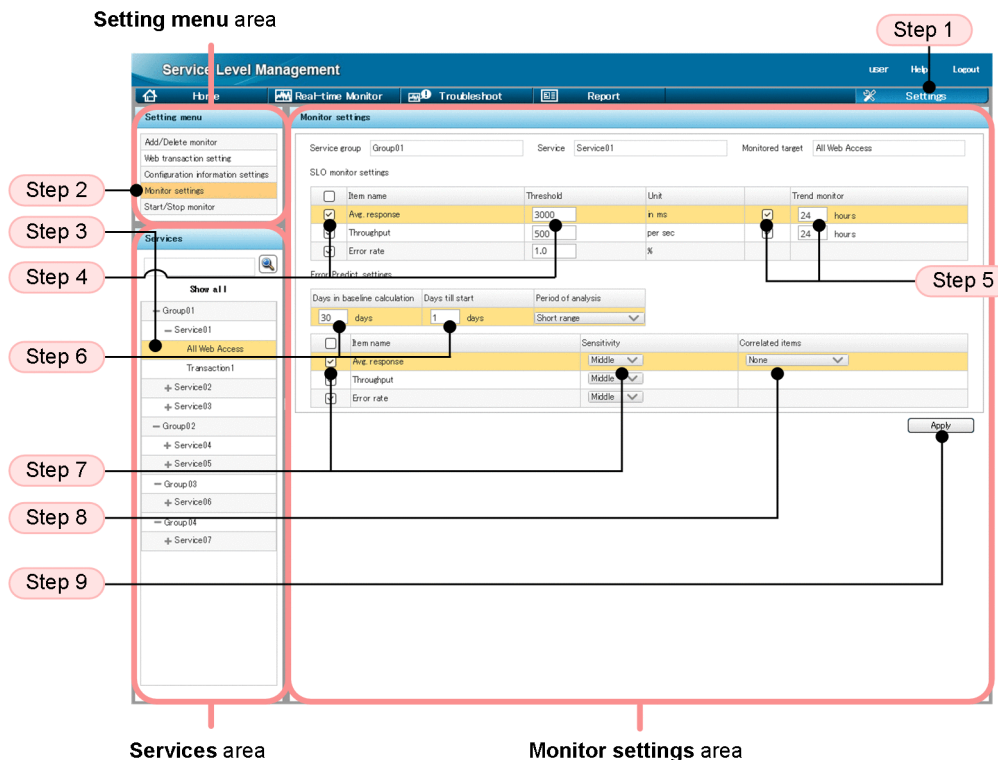
Set the monitor items for each monitored service. The monitoring staff performs this operation.

### (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 4.6.1 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, see (3) Procedure for stopping monitoring in 5.3.1 Starting monitoring.

### (2) Procedure

The following shows the Settings window used in this task:



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 or an invalid value is entered in the text box.
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 **Trend monitor** 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

- [5.3.1 Starting monitoring](#)

### (4) Setting example

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.

## (a) Defining SLOs from the SLA

### Tasks required for setting up monitoring items in SLM

The monitoring staff 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 monitoring staff defines the SLOs as follows:

- Average response time: 3,000 milliseconds
- Throughput: 800 count/second
- Error rate: 1.0%

The monitoring staff 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 monitoring staff decides to set up monitoring items for each monitored service.

## (b) Setting up monitoring items

### Tasks in SLM

The monitoring staff decides to log in to SLM - 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 4-15: Setup example of monitoring items for the monitored services based on the SLOs

The screenshot shows the 'Service Level Management' interface. The top navigation bar includes 'Home', 'Real-time Monitor', 'Troubleshoot', 'Report', and 'Settings'. The left sidebar contains a 'Setting menu' with options like 'Add/Delete monitor', 'Web transaction setting', 'Configuration information settings', 'Monitor settings', and 'Start/Stop monitor'. Below this is a 'Services' section with a tree view showing 'Group01' expanded to show 'Service01' (All Web Access), 'Transaction1', 'Service02', 'Service03', 'Group02', 'Service04', 'Service05', 'Group03', 'Service06', 'Group04', and 'Service07'. The main content area is titled 'Monitor settings' and shows configuration for 'Service group: Group01' and 'Service: Service01' with a 'Monitored target' of 'All Web Access'. It features two tables: 'SLO monitor settings' and 'Error Predict. settings'. The 'SLO monitor settings' table has columns for 'Item name', 'Threshold', 'Unit', and 'Trend monitor'. The 'Error Predict. settings' table has columns for 'Item name', 'Sensitivity', and 'Correlated items'. An 'Apply' button is located at the bottom right of the settings area.

Item name	Threshold	Unit	Trend monitor
<input checked="" type="checkbox"/> Avg. response	3000	in ms	<input checked="" type="checkbox"/> 5 hours
<input checked="" type="checkbox"/> Throughput	800	per sec	<input checked="" type="checkbox"/> 5 hours
<input checked="" type="checkbox"/> Error rate	1.0	%	

Item name	Sensitivity	Correlated items
<input checked="" type="checkbox"/> Avg. response	High	Throughput
<input checked="" type="checkbox"/> Throughput	High	
<input checked="" type="checkbox"/> 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 4-2: 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 4-3: 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 monitoring staff proceeds to set up monitoring items for the remaining monitored services in the same manner.

# 5

## Monitoring Services by Using SLM

This chapter gives an overview of monitoring tasks by using SLM, and describes how to start and stop monitoring, monitoring of the status of monitored services, and execution examples of monitoring.

## 5.1 Overview of monitoring tasks using SLM

---

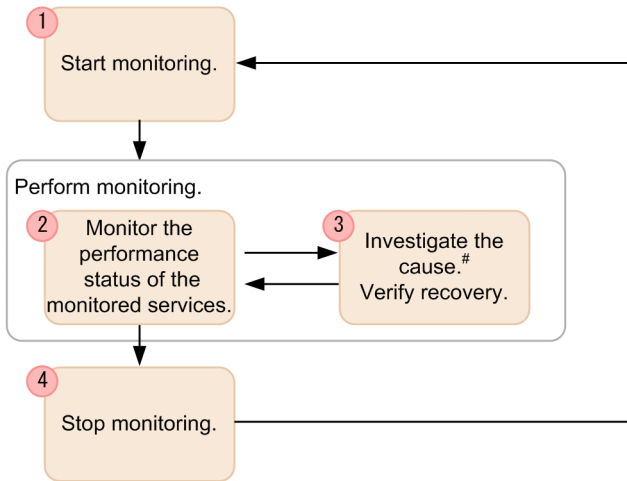
SLM supports stable operation of monitored services by enabling the monitoring persons to monitor the status of the services. In a system with predefined SLOs, which are the evaluation metrics for the statuses of the monitored services, monitoring is performed so as to comply with the SLOs and to maintain the service level. SLM 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.

This section explains the procedure from start to stop of monitoring when SLM is used and the windows in SLM that are used for monitoring.

## 5.2 General monitoring procedure

The following describes the procedure for monitoring the status of monitored services by using SLM. This procedure assumes that monitored services have already been registered in SLM, and that the necessary settings for monitoring have been completed.

Figure 5-1: General procedure for monitoring the status of monitored services



#: 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 [5.3.1 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.

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 [5.4 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 [6.1 Support of root cause investigation when an error or warning is displayed for a monitored service](#).

### 4. Stop monitoring.

If you need to change monitoring item settings or SLM log output operations, you must first stop monitoring.

For details about how to stop monitoring, see [\(3\) Procedure for stopping monitoring in 5.3.1 Starting monitoring](#).

To resume monitoring the monitored services, go back to step 1.

## 5.3 Starting monitoring

To start monitoring, start the registered monitored services.

### 5.3.1 Starting monitoring

To start monitoring of monitored services, the service group administrator logs in to SLM - Manager and specifies the settings necessary to start monitoring. The monitoring staff performs this operation.

#### (1) Before you start

- Verify that you have the service group administrator permissions.
- Log in to SLM - Manager.  
For details about how to log in, see [3.2.1 Logging in to SLM - Manager](#).
- Verify that monitoring items have been set up.  
For details about how to set up monitoring items, see [4.6.2 Setting up the monitoring items for service performance](#).

#### (2) Procedure

The following shows the Settings window that is used in this task:



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.

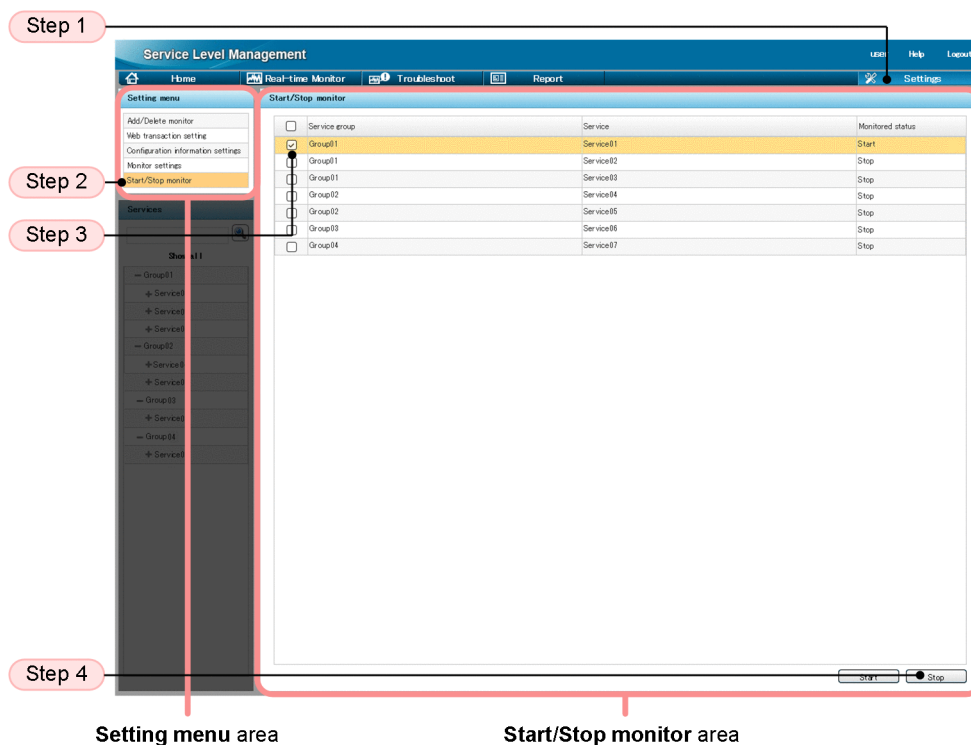
Monitoring of the selected monitored service begins.

If the start processing is successful, **Monitored Status** changes to **Start**.

### (3) Procedure for stopping monitoring

For example, if you want to change the settings of the monitor items for the services for which monitoring has already started, stop monitoring of the monitored services whose settings you want to change.

The following shows the Settings window that is used in this task:



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**.

## 5.4 Monitoring the status of monitored services

---

SLM 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.

### 5.4.1 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. The monitoring staff performs this operation.

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.

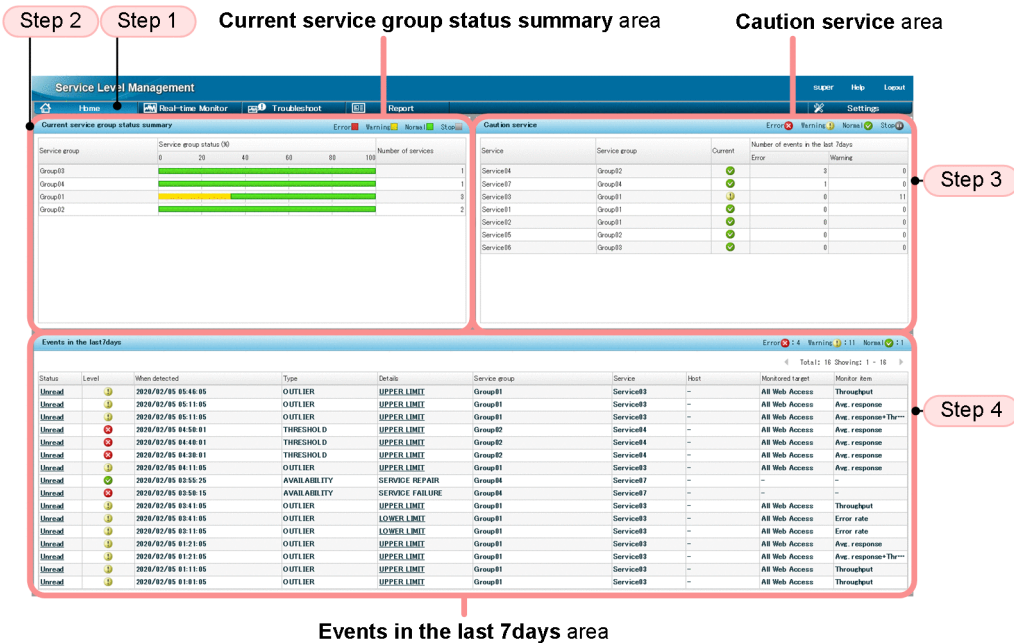
The information displayed in the Home window is refreshed every three seconds.

#### (1) Before you start

- Log in to SLM - Manager.  
For details about how to log in, see [3.2.1 Logging in to SLM - Manager](#).
- Verify that monitoring has started.  
For details about how to start monitoring, see [5.3.1 Starting monitoring](#).

#### (2) Procedure

The following shows the Home window that is used in this task:



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 6.2.1 [Checking the timing of an event causing an error or warning](#).

## 5.4.2 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. The monitoring staff performs this operation.

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 SLM - Manager.  
For details about how to log in, see [3.2.1 Logging in to SLM - Manager](#).
- Verify that monitoring has started.  
For details about how to start monitoring, see [5.3.1 Starting monitoring](#).

## (2) Procedure

The following shows the Real-time Monitor window that is used in this task:

The screenshot shows the Service Level Management Real-time Monitor interface. It features a sidebar for navigating through service groups, a top navigation bar, and a main area with tabs for 'Event' and 'Performance chart'. The 'Performance chart' tab displays two graphs: 'Ave. response (in ms)' and 'Throughput (per sec)'. The 'Event' tab shows a table of monitored targets. Annotations indicate the following steps:

- Step 2:** Services area (left sidebar)
- Step 3:** Service performance information area (top navigation bar)
- Step 4:** Event and Performance chart tabs area (main content area)
- Step 1:** Performance chart area (bottom graph area)

To check the status of monitored services in a specific service group:

1. Click the **Real-time Monitor** button.  
The **Services** and **Service 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** area 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** area, the check is complete.

If errors, warnings, or alarm statuses are displayed in the **Service 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 [6.2.1 Checking the timing of an event causing an error or warning](#).

# 6

## Supporting Root Cause Investigation When an Error or Warning Is Displayed for a Monitored Service

SLM can be used for root cause investigation, for example, when an occurrence (or trend) of excess beyond the threshold is detected for a monitored service. This chapter describes how SLM can be used for root cause investigation, and the procedure of root cause investigation by using SLM.

## 6.1 Support of root cause investigation when an error or warning is displayed for a monitored service

To investigate the cause of an error or warning, you can use SLM to check when the event that caused the error or warning occurred, and the past service performance. You can also check whether the monitored service has recovered to the normal status after taking proper action for the error or warning.

The following describes how to support SLM's prediction and handling of an abnormality in the service performance for monitored services, and provides examples showing the specific execution methods based on certain conditions.

### 6.1.1 Predictive error detection in the performance of a monitored service

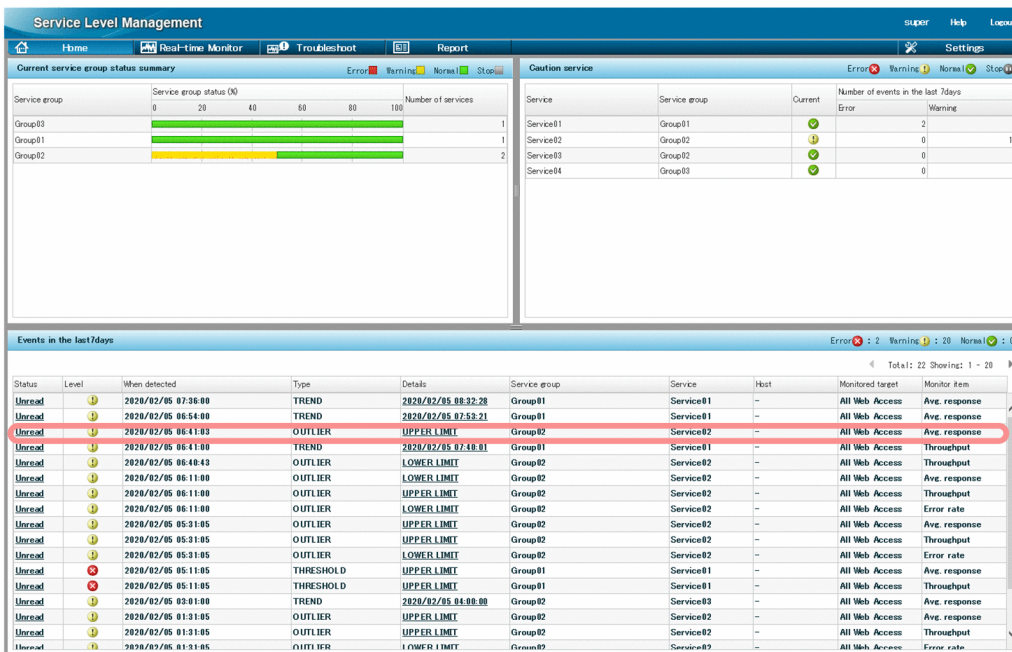
The following provides a specific example of when a warning is displayed for a monitored service.

#### Tasks in SLM

While the monitoring staff 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 6-1: Display example of the Home window that contains a warning for a monitored service



Details of the warning displayed in this figure are as follows:

- When detected: 2020-02-05 06:41:03
- 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 `Service02` belonging to `Group02` that was obtained at 06:41:03 on February 5, 2020, 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

Because the warning might lead to an error if left unattended, the monitoring staff decided to take corrective action immediately.

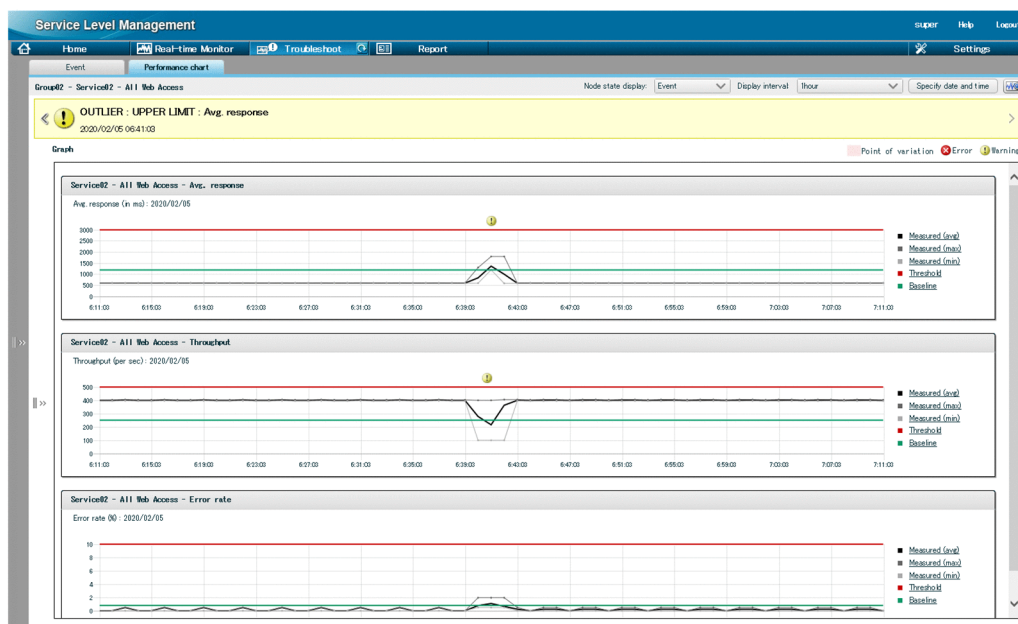
## 6.1.2 Corrective action to be taken after a warning sign was detected in the performance of a monitored service

The following provides detail examples of actions that are to be taken after a warning is displayed for a monitored service.

### Tasks in

After being notified of the warning displayed in the Home window, the monitoring staff 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 6-2: Display example of the Troubleshoot window in which a warning is displayed for a monitored service



This performance chart of average response time indicates that the event causing the warning occurred between 06:39:03 and 06:43:03.

### 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 monitoring staff notified the maintenance service provider for the monitored service and requested a root cause investigation and corrective action.



## 6.1.3 Verifying the service performance after taking corrective action

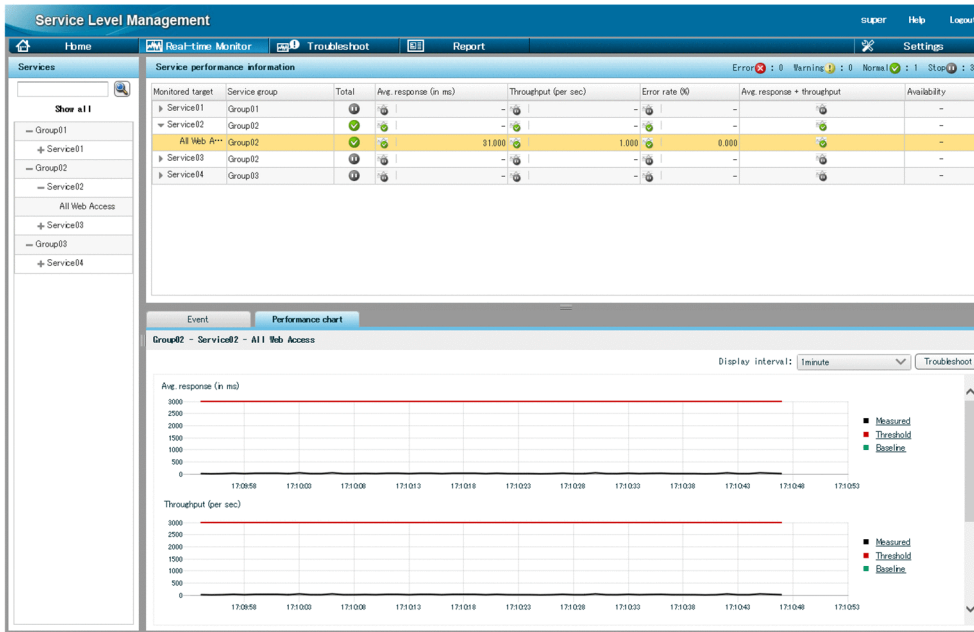
The following provides a specific example of verifying service performance after taking corrective action for a warning displayed for a monitored service.


### Tasks in SLM

After corrective action was taken by the maintenance service provider for the monitored service based on the results of a root cause investigation, the monitoring staff 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 6-3: Display example of the Real-time Monitor window showing that service performance has returned to normal



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 monitoring staff 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.

## 6.2 Checking when an event causing an error or warning occurred

If an error or warning is displayed for a monitored service, check the performance graph of the monitor items of the service, to determine when the event that caused the error or warning occurred.

### 6.2.1 Checking the timing of an event causing an error or warning

Use the Home window, Real-time Monitor window, and Troubleshoot window to check when the event that caused an error or warning occurred. The monitoring staff performs this operation.

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 SLM - Manager.  
For details about how to log in, see [3.2.1 Logging in to SLM - Manager](#).
- Verify that monitoring has started.  
For details about how to start monitoring, see [5.3.1 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**

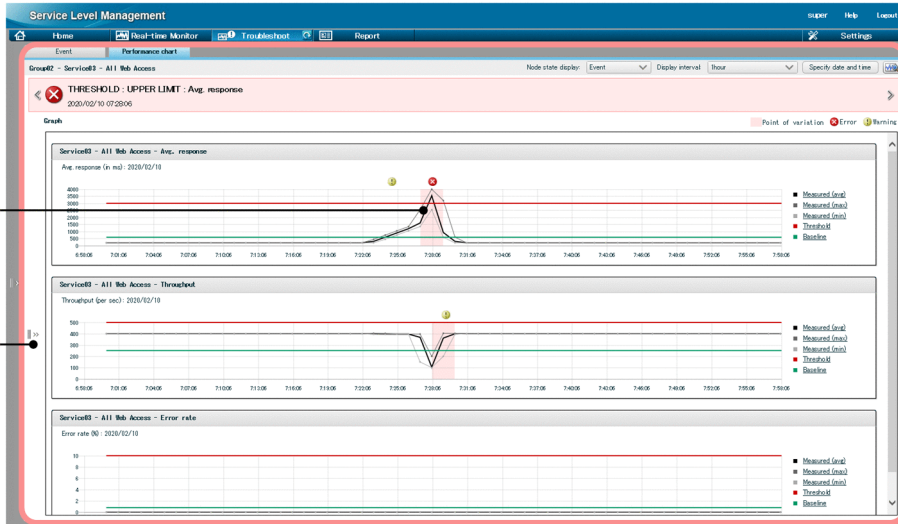
**Step 2** Events in the last 7 days area

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

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

Status	Level	When detected	Type	Details	Service group	Service	Host	Monitored target	Monitor item
Unread	🟡	2020/02/10 07:28:15	OUTLIER	UPPER LIMIT	Group02	Service03	-	All Web Access	Throughput
Unread	🔴	2020/02/10 07:28:06	THRESHOLD	UPPER LIMIT	Group02	Service03	-	All Web Access	Avg. response
Unread	🟡	2020/02/10 07:24:36	OUTLIER	UPPER LIMIT	Group02	Service03	-	All Web Access	Avg. response
Unread	🟡	2020/02/10 08:14:00	OUTLIER	UPPER LIMIT	Group02	Service03	Host01	Client01	CPU/Device name...
Unread	🟡	2020/02/10 08:08:55	OUTLIER	UPPER LIMIT	Group02	Service03	-	All Web Access	Throughput
Unread	🟡	2020/02/10 08:08:40	OUTLIER	UPPER LIMIT	Group02	Service03	-	All Web Access	Avg. response
Unread	🟡	2020/02/09 19:35:09	OUTLIER	UPPER LIMIT	Group03	Service04	-	All Web Access	Avg. response
Unread	🟡	2020/02/09 19:35:05	OUTLIER	UPPER LIMIT	Group02	Service03	-	All Web Access	Avg. response
Unread	🟡	2020/02/09 19:35:05	OUTLIER	UPPER LIMIT	Group02	Service03	-	All Web Access	Throughput
Unread	🟡	2020/02/09 19:35:05	OUTLIER	UPPER LIMIT	Group02	Service03	-	All Web Access	Error rate
Unread	🟡	2020/02/09 19:35:05	OUTLIER	UPPER LIMIT	Group03	Service04	-	All Web Access	Throughput
Unread	🟡	2020/02/09 19:35:05	OUTLIER	UPPER LIMIT	Group03	Service04	-	All Web Access	Error rate
Unread	🟡	2020/02/09 02:00:05	OUTLIER	UPPER LIMIT	Group02	Service03	-	All Web Access	Avg. response
Unread	🟡	2020/02/09 02:00:05	OUTLIER	UPPER LIMIT	Group02	Service03	-	All Web Access	Throughput

- Troubleshoot window

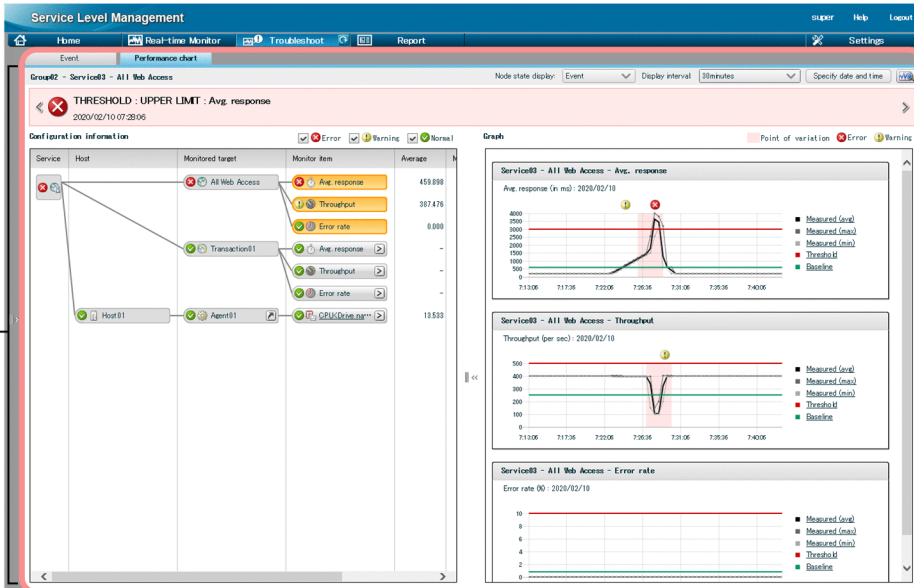


Step 3

Step 4

Event and Performance chart tabs area

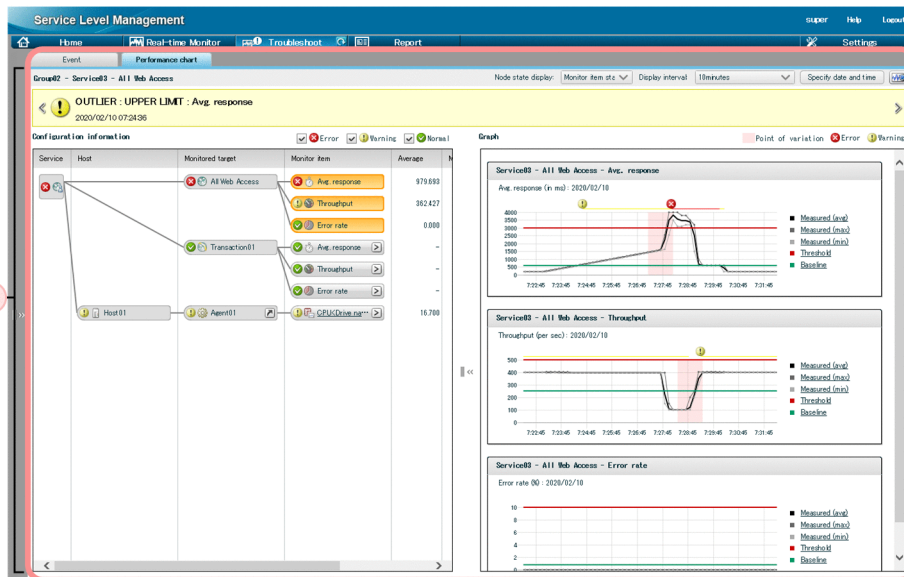
- Troubleshoot window (displaying configuration information)



Step 4

Event and Performance chart tabs area

- Troubleshoot window (displaying **Monitor item state** on the **Performance chart** tab)



Step 4

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.

4. Click **>>** to display configuration information.

Configuration information helps you identify the monitoring item of the monitored service that resulted in the error.

You can also check in the performance chart past service performance. For details about how to check past service performance, see 6.3.1 [Checking the past performance of monitored services](#).

## 6.3 Checking the past performance of monitored services

You can check the past performance of monitored services in the performance graph to investigate the cause. When you find a possible sign while checking the performance graph, or when you receive inquiry from a monitored service's user, you can check the past performance of the monitored service, as necessary.

### 6.3.1 Checking the past performance of monitored services

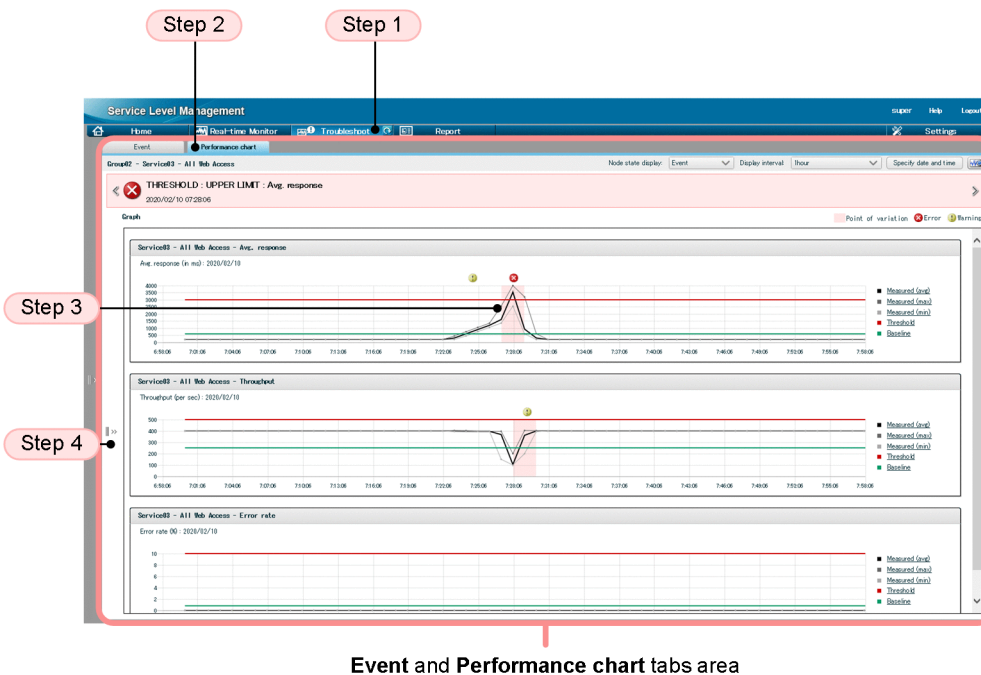
Use the Troubleshoot window to check the past service performance. The monitoring staff performs this operation.

#### (1) Before you start

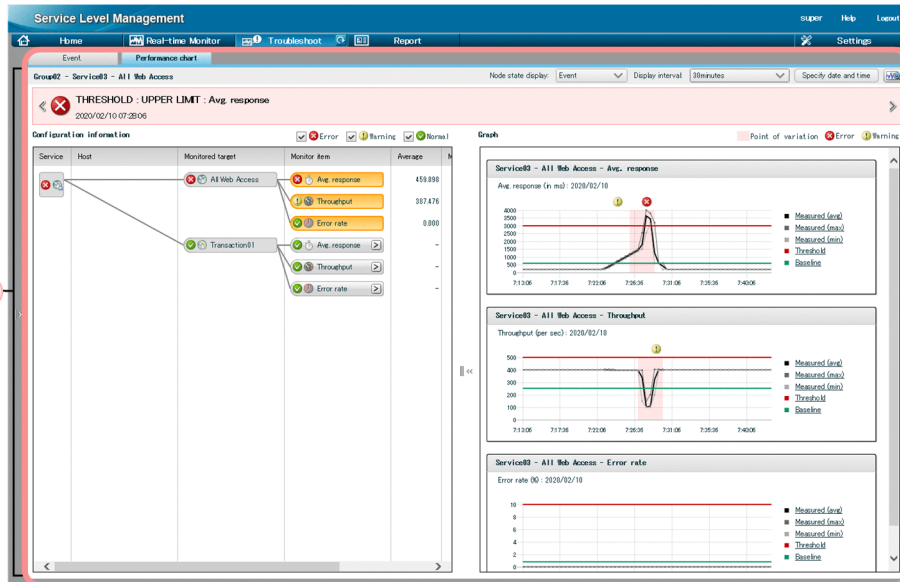
- Log in to SLM - Manager.  
For details about how to log in, see [3.2.1 Logging in to SLM - Manager](#).
- Verify that monitoring has started.  
For details about how to start monitoring, see [5.3.1 Starting monitoring](#).

#### (2) Procedure

- Troubleshoot window



- Troubleshoot window (with the configuration information displayed)



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.

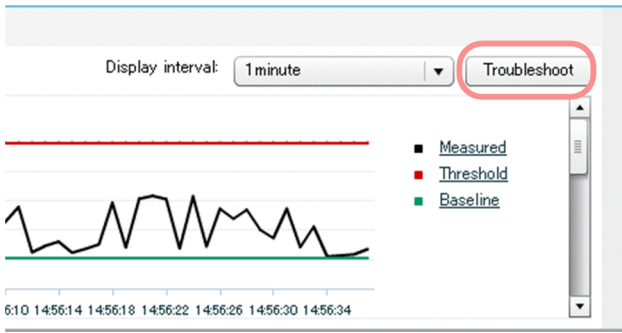
4. Click **>>** to display configuration information and add to the performance charts any monitoring item that you want to check.

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.

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.



## 6.4 Verifying the recovery of a monitored service after taking corrective action

After taking corrective action for the cause of an error or warning, you can check whether a monitored service has been recovered to the normal status.

### 6.4.1 Verifying the recovery of monitored services after taking corrective action

Use the Real-time Monitor window to verify whether monitored services have been recovered to the normal status. The monitoring staff performs this operation.

#### (1) Before you start

- Log in to SLM - Manager.  
For details about how to log in, see 3.2.1 Logging in to SLM - Manager.

#### (2) Procedure

The following shows the Real-time Monitor window that is used in this task:

The screenshot displays the Service Level Management Real-time Monitor interface. It is divided into several sections:

- Services area:** A tree view on the left showing a hierarchy of services. 'All Web Access' is selected under 'Service02'.
- Service performance information area:** A table showing performance metrics for selected services. The table has columns for Monitored target, Service group, Total, Avg. response (in ms), Throughput (per sec), Error rate (%), and Avg. response + throughput. All metrics are shown with green status indicators.
- Event and Performance chart tabs area:** Two tabs are visible: 'Event' and 'Performance chart'. The 'Performance chart' tab is active, showing two line graphs. The top graph plots 'Avg. response (in ms)' and the bottom graph plots 'Throughput (per sec)'. Both graphs show a measured line (black) that is well below a red threshold line. A blue baseline is also visible.

Four numbered steps are overlaid on the screenshot:

- Step 1: Points to the 'Real-time Monitor' button in the top navigation bar.
- Step 2: Points to the 'All Web Access' service in the Services area.
- Step 3: Points to the 'Performance chart' tab.
- Step 4: Points to the performance data in the Performance chart area.

To verify recovery of a monitored service after taking corrective action:

- Click the **Real-time Monitor** button.  
The **Services** and **Service 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.
- From the **Services** area, select a monitored target of a monitored service.
- In the **Service performance information** area, 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.

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.

# Appendixes

## A. Commands

---

This chapter explains the syntax of the SLM commands.

### A.1 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 [A.3 Notes about command execution](#).

#### Return value

Explains the command's return values.

#### Example

Shows an example of specifying the command.

#### Example output

Shows an example of the command's output.

### A.2 List of commands

The following table lists and provides an overview of the commands supported by SLM.

Table A-1: List of commands supported by SLM

No.	Command name	Target	Overview of function
1	A.4 <a href="#">jslmmgrsetup</a> (sets up SLM - Manager)	M	Creates an execution environment for SLM - Manager.
2	A.5 <a href="#">jslmurnals</a> (displays the network adapter address and IP address)	U	Displays, on the command prompt screen, the IP address and network adapter address of the host on which SLM - UR is installed. The information displayed by this command is needed for setting up SLM - UR.
3	A.6 <a href="#">jslmursetup</a> (sets up SLM - UR)	U	Creates an execution environment for SLM - UR.

Legend:

Mgr: SLM - Manager

UR: SLM - UR

### A.3 Notes about command execution

This section provides notes that apply to all commands.

#### Important

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 A-2: Characters and symbols permitted for paths in command arguments

No.	Characters and symbols	Remarks
1	Alphanumeric characters	--
2	Space	<ul style="list-style-type: none"> <li>• If a path contains a space, enclose the entire path in double quotation marks ("").</li> <li>• Folder names cannot begin or end with a space.</li> </ul>
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).

- Do not specify the same file when simultaneously executing multiple commands that perform file input or output.

## A.4 jslmmgrsetup (sets up SLM - Manager)

### Function

This command creates an execution environment for SLM - Manager. It can also be used to reconfigure the execution environment for an existing SLM - Manager.

You execute this command after you have installed SLM - Manager.

The command execution results are output to the standard output and displayed in the console window.

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 SLM - Manager has been newly installed or after the execution environment for SLM - 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 SLM - Manager already exists, the command reconfigures the existing execution environment for SLM - 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 SLM - Manager are to be changed
- The embedded Web server environment in the execution environment for a configured SLM - Manager is to be reconfigured
- The execution environment for a configured SLM - 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 SLM - Manager execution environment is reconfigured.

### Format

```
jslmmgrsetup absolute-path-of-options-file
```

### Execution permission

User account that belongs to the OS's Administrators group

### Storage folder

```
SLM-Manager-installation-folder\mgr\bin\
```

## Arguments

### *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:

```
SLM-Manager-installation-folder\mgr\template\mgr\conf\jplitslm_setup.opt
```

The following shows the definitions in the options file:

```
manager_host=host-name-or-IP-address-of-SLM-Manager
manager_port=port-number-of-SLM-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_area_size=capacity-of-embedded-database-area
```

The following table provides the details of the definition items.

Table A-3: Details of definition items in options file for SLM - Manager

No.	Definition item	Specification	Description	Default value
1	manager_host	R	Specifies the host name or IP address of the host on which SLM - Manager is installed, as the information for identifying SLM - Manager's execution environment.	--
2	manager_port	O	Specifies the port number used by SLM - 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
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.	20903

No.	Definition item	Specification	Description	Default value
7	<code>hdb_port</code>	O	<p>An error results if any of the following numbers is specified:</p> <ul style="list-style-type: none"> <li>• Number outside the permitted range</li> <li>• Port number that is already specified in the <code>services</code> file</li> <li>• Port number that is already in use</li> </ul> <p>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.</p>	20903
8	<code>hdb_area_path</code> <sup>#3</sup>	R	<p>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.</p> <p>None of the following is permitted:</p> <ul style="list-style-type: none"> <li>• Specification in UNC representation</li> <li>• Specification containing a network drive</li> <li>• Specification of a drive name only</li> <li>• Specification containing the SLM - Manager installation folder</li> <li>• Specification containing an SLM - UR installation folder</li> </ul>	--
9	<code>hdb_area_size</code> <sup>#3</sup>	O	<p>Specifies the size of the embedded database area for storing the data handled by SLM - Manager. Specify an integer in the range from 5000 through 1048575 (MB).</p> <p>If the specified value is not within this range, an error results.</p> <p>This definition is ignored when the execution environment is being reconfigured.</p>	39000

**Legend:**

R: Specification is required.

O: Specification is optional.

--: Not applicable

#1

If the specified value is not within the permitted range, setup is completed, but an error occurs when the SLM - Manager service **SLM - 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 SLM - Manager service **SLM - Manager Web Service** (service name: `JP1_ITSLM_MGR_Web_Service`) starts.

#3

If you are reconfiguring the execution environment for a configured SLM - 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 `jplitslm_setup.opt` after command execution and stored at the following location:

```
SLM-Manager-installation-folder\mgr\conf\jplitslm_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:

```
SLM-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` command).
- If a definition item is omitted, its default value is used.
- If you are reconfiguring the execution environment of a configured SLM - 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:

```
SLM-Manager-installation-folder\mgr\conf\jplitslm_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\SLMSYS04
```

## Return value

Return value	Description
0	Setup processing terminated normally.
1	Setup processing failed.

## Example

```
C:\Program Files\HITACHI\JP1ITSLM\mgr\bin\jslmmgrsetup C:\Users\Administrator\Desktop\jplitslm_setup.opt
```



## A.5 jslmurnals(displays the network adapter address and IP address)

### Function

This command displays, on the command prompt screen, the network adapter address and IP address of the host on which SLM - UR is installed.

The information displayed by executing this command is necessary for setting up SLM - UR, or for changing the network adapter address by editing the system definition files of SLM - UR.

Execute this command at the following timing:

- When viewing the network adapter address to be specified during the setup of SLM - UR
- When adding or deleting network interface cards
- When changing the settings of the network interface
- When migrating from the setup of SLM - UR for which the network interface number (ur\_ni\_number) is specified for the setup option file, to the setup for which the network adapter address (ur\_na\_address) is specified

### Format

```
jslmurnals
```

### Execution permission

User account that belongs to the OS's Administrators group

### Storage folder

```
SLM-Manager-installation-folder\ur\bin\
```

### Notes

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 display processing terminated normally.
1	The display processing failed.
130	The import processing was canceled because <b>Ctrl+C</b> was pressed.

### Example

```
C:\Program Files\HITACHI\JP1ITSLM\ur\bin\jslmurnals
```

### Example output

```
KNAS99000-I network-adapter-address----IP-address
```

## A.6 jslmursetup (sets up SLM - UR)

### Function

This command creates an execution environment for SLM - UR. It can also be used to reconfigure the execution environment for an existing SLM - UR.

Before you execute this command, install SLM - UR, and then execute the `jslmurnals` command to check the network adapter and IP address for which HTTP packets are to be collected.

The command execution results are output to the standard output and displayed in the console window.

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 SLM - UR has been newly installed or after the execution environment for SLM - 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 SLM - UR already exists, the command reconfigures the existing execution environment for SLM - 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 SLM - UR are to be changed.
- The execution environment for a configured SLM - UR is to be reconfigured after an upgrade installation was performed.

### Format

```
jslmursetup absolute-path-of-options-file
```

### Execution permission

User account that belongs to the OS's Administrators group

### Storage folder

```
SLM-UR-installation-folder\ur\bin\
```

### Arguments

*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:

```
SLM-UR-installation-folder\ur\template\ur\conf\jplitslm_setup.opt
```

The following shows the definitions in the options file:

```
manager_host=host-name-or-IP-address-of-SLM-Manager
manager_port=port-number-of-SLM-Manager
ur_host=host-name-or-IP-address-of-SLM-UR
ur_port=port-number-of-SLM-UR
ur_na_address=network-adapter-address
```

The following table provides the details of definition items.

Table A-4: Details of definition items in options file for SLM - UR

No.	Definition item	Specification	Description	Default value
1	manager_host	R	Specifies the host name or IP address of the host on which SLM - Manager is installed, as the information for identifying SLM - Manager's execution environment. If SLM 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 SLM - 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 SLM - UR is installed, as the information for identifying SLM - UR's execution environment. If SLM 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 SLM - Manager, as a number in the range from 1 through 65535.#	20910
5	ur_na_address	R	Specifies the network adapter address that SLM - UR connects to, by using half-width alphanumeric characters (hexadecimal) up to 12 digits. You can use the <code>jslmurnals</code> command to check the connected network device. For details about the <code>jslmurnals</code> command, see <a href="#">A.5 jslmurnals(displays the network adapter address and IP address)</a> in <a href="#">A. Commands</a> .	--

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 SLM - UR service **SLM - User Response Service** (service name: `JPl1_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 `jpl1itslm_setup.opt` after command execution and stored at the following location:

```
SLM-UR-installation-folder\ur\conf\jpl1itslm_setup.opt
```

- Do not execute commands other than the `j slmurnals` command while this command is being executed. Do not execute another command while this command is executing, except for the `j slmurnals` 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:

```
SLM-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 `j slmursetup` command).

## Return value

Return value	Description
0	Setup processing terminated normally.
1	Setup processing failed.

## Example

```
C:\Program Files\HITACHI\JP1ITSLM\ur\bin\j slmursetup C:\Users\Administrator\Desktop\j plitslm_setup.opt
```

## B. List of Port Numbers Used by SLM

The following table lists the port numbers used by SLM.

Table B-1: Port numbers used by SLM

Default port number	Purpose	Target	Definition file where port number is defined	Property
20900	Embedded Web server's listen port	Mgr	<i>SLM-Manager-installation-folder</i> \mgr\system\psb\httpsd\conf\httpsd.conf	Listen
20901	Embedded Web server's internal communication port	Mgr	<i>SLM-Manager-installation-folder</i> \mgr\system\psb\CC\web\containers\JP1_ITSLM_MGR_WC_Server\usrconf\usrconf.properties	webserver.connector.ajp13.port
			<i>SLM-Manager-installation-folder</i> \mgr\system\psb\CC\web\redirector\workers.properties	worker.itslm.port
20902	Embedded Web server's completion-message receiving port	Mgr	<i>SLM-Manager-installation-folder</i> \mgr\system\psb\CC\web\containers\JP1_ITSLM_MGR_WC_Server\usrconf\usrconf.properties	webserver.shutdown.port
20903	Embedded database's listen port	Mgr	<i>SLM-Manager-installation-folder</i> \mgr\system\hdb\CONF\pdsys	pd_name_port
			<i>SLM-Manager-installation-folder</i> \mgr\system\hdb\CONF\emb\HiRDB.ini	PDNAMEPORT
			<i>SLM-Manager-installation-folder</i> \mgr\conf\jplitslm.properties	rdbPort
20904	RMI communication port	Mgr	<i>SLM-Manager-installation-folder</i> \mgr\conf\jplitslm.properties	rmiManagerPort
			<i>SLM-Manager-installation-folder</i> \mgr\sdengine\analysisN <sup>#1</sup> \conf\system_config.properties	rmi.serverPort
		UR	<i>SLM-UR-installation-folder</i> \ur\conf\jplitslmur.properties <sup>#2</sup>	rmiManagerPort
20910		UR	<i>SLM-UR-installation-folder</i> \ur\conf\jplitslmur.properties	rmiUrPort
			<i>SLM-UR-installation-folder</i> \ur\sdengine\collector\conf\system_config.properties	rmi.serverPort
			<i>SLM-UR-installation-folder</i> \ur\sdengine\collector2\conf\system_config.properties	
			<i>SLM-UR-installation-folder</i> \ur\sdengine\recorder\conf\system_config.properties	

Legend:

Mgr: SLM - Manager

UR: SLM - UR

#1

*N* is a number from 1 to 10.

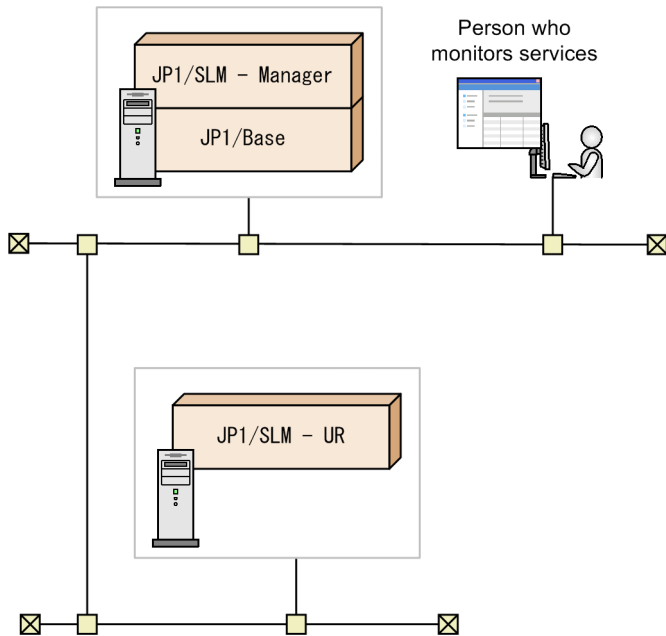
#2

Port numbers are defined in all the corresponding SLM - UR system definition files linked to SLM - Manager.

## C. SLM Communication

This section uses the example system configuration shown below to explain the port numbers used in SLM communication and the direction in which data passes through a firewall (the direction in which a connection is established).

Figure C-1: Example system configuration



1. The person who monitors services uses a browser to connect to SLM - Manager.
2. SLM - UR is deployed to monitor the Web system services.

- Communication between SLM - Manager and the browser

Communication between SLM - Manager and the browser is as follows:

Port number of the browser	Pass-through direction	Communication protocol	Port number of SLM - Manager (HTTP server)
(ANY)/tcp	→	HTTP	20900/tcp (httpd)

- Communication between SLM - Manager and SLM - UR

Communication between SLM - Manager and SLM - UR is as follows:

Port number of SLM - Manager	Pass-through direction	Communication protocol	Port number of SLM - UR
(ANY)/tcp	→	RMI	20910/tcp (jslmuRMI)
(ANY)/tcp	→	RMI	(ANY)/tcp
20904/tcp (jslmmRMI)	←	RMI	(ANY)/tcp
(ANY)/tcp	←	RMI	(ANY)/tcp

In addition to these communications, the following communications are also available:

- Communications using ports in the range from 20901/tcp to 20904/tcp on the local host on which SLM - Manager is running

- Communications using port 20910/tcp on the local host on which SLM - UR is running
- Collection of HTTP packets by SLM - UR

Set up the firewall so that SLM - UR can obtain HTTP packets that were copied by the port mirroring function. To specify a program to allow communication, specify settings on the host where SLM - UR was set up so that communication of the following program is allowed:

- *SLM-UR-installation-folder*\ur\system\sdp\bin\sdppcap.exe



## D. Advanced Use

---

For advanced use of SLM, see the manual *JPI/Service Level Management*.

## E. Reference Material for This Manual

---

This appendix provides reference information, including various conventions, for this manual.

### E.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):

#### SLM

- *JP1 Version 11 JP1/Service Level Management Description, User's Guide, Reference and Operator's Guide(3021-3-A32(E))*

#### JP1/Base

- *JP1 Version 11 JP1/Base User's Guide(3021-3-A01(E))*

Note that, in this manual, JP1 Version 11 is omitted from the titles of the related publications.

### E.2 Conventions: Fonts and symbols

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

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

The following table explains the symbols used in this manual:

Symbol	Convention
	In syntax explanations, a vertical bar separates multiple items, and has the meaning of OR. For example: <code>A   B   C</code> means A, or B, or C.

Symbol	Convention
{ }	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: <i>monitoring-item-name</i> < Δ <i>monitoring-item-name</i> . . . > This means that following <i>monitoring-item-name</i> , a single-byte space ( Δ ) and <i>monitoring-item-name</i> might be displayed repeatedly.

### E.3 Conventions: SLM installation folder

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

Product name	Convention used to indicate the installation folder	Default installation folder <sup>#</sup>
IT Service Level Management - Manager	<i>SLM-Manager-installation-folder</i>	<i>system-drive</i> : \Program Files\HITACHI\JP1ITSLM
IT Service Level Management - User Response	<i>SLM-UR-installation-folder</i>	

#

The default installation folder is the folder into which the SLM 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.

### E.4 Conventions: Abbreviations for product names

This manual uses the following abbreviations for product names:

Abbreviation	Full name or meaning	
HNTRLib2	Hitachi Network Objectplaza Trace Library 2	
SLM	SLM - Manager	JP1/Service Level Management - Manager
	SLM - UR	JP1/Service Level Management - User Response
JP1/NETM/DM	JP1/NETM/DM Client	
	JP1/NETM/DM Client - Base	
	JP1/NETM/DM Manager	

## E.5 Conventions: Acronyms

This manual uses the following acronyms:

Acronym	Full name or meaning
ASCII	American Standard Code for Information Interchange
BNF	Backus Normal Form
DB	Database
GMT	Greenwich Mean Time
GUI	Graphical User Interface
IP	Internet Protocol
NTFS	NT File System
RMI	Remote Method Invocation
SLA	Service Level Agreement
SLO	Service Level Objective
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

## E.6 Conventions: Units (such as KB, MB, GB, and TB)

This manual uses the following conventions:

- 1 KB (kilobyte) is 1,024 bytes.
- 1 MB (megabyte) is 1,024<sup>2</sup> bytes
- 1 GB (gigabyte) is 1,024<sup>3</sup> bytes.
- 1 TB (terabyte) is 1,024<sup>4</sup> bytes.

## F. Glossary

---

### All Web Access

A monitored target in SLM. 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 SLM 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.

### 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.

### 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.

### SLM - Manager

A program that aggregates and analyzes HTTP packets collected by SLM - UR in order to monitor the status of services.

SLM - Manager is accessed in order to check the status of services being monitored.

### SLM - 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 SLM - Manager.

### JP1/Base

A program that is a prerequisite for SLM - 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 SLM.

### 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 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.

SLM 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 SLM. 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.

## monitoring item

An item that is monitored in SLM 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.

## 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.

## performance data

The data that used in SLM monitoring, consisting of the following:

- Service performance data collected by SLM - UR

## RD area

A data storage area for a database. When the SLM setup process is run at the time of installation, RD areas are created in folders specified by an absolute path. In SLM, RD areas are used to provide data management while SLM is operating.

## 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.

#### system definition file

A definition file (properties file) that specifies the details of how SLM functions. Host names, port numbers, and similar information are specified in the system definition file.

#### 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 SLM that represents a combination of requests and responses.

# Index

## A

- abbreviations for products 99
- acronyms 100
- All Web Access 43, 101
- authentication server 23, 101
- availability information 101
- average response time
  - All Web Access 43

## B

- baseline 50, 101
- BNF notation 101
- browser 37

## C

- checking past performance of monitored service 77
- command 83
  - displaying network adapter address and IP address 89
  - format of explanation 83
  - setting up SLM - Manager 85
  - setting up SLM - UR 90
- commands, list of 83
- conventions
  - abbreviations for products 99
  - acronyms 100
  - fonts and symbols 98
  - KB, MB, GB, and TB 100
  - version numbers 99

## D

- drilldown 101

## E

- editable definition 30
- error rate
  - All Web Access 43
- event 101
- example definition (system definition file) 32

## F

- firewall
  - setting up SLM - Manager 20

- setting up SLM - UR 21
- font conventions 98

## G

- GB meaning 100
- general procedure for setting up SLM 14

## H

- Home window 74
  - checking monitored service statuses of all service groups 66

## I

- installation folder 17
- installing
  - SLM 17
- installing and setting up JP1/Base 16

## J

- JP1 event 101
- JP1 permission level 101
- JP1 user 101
  - setting up in JP1/Base 25
  - specifying operation permission for each 26
- JP1\_ITSLM\_Admin 26
- JP1\_ITSLM\_User 26
- JP1/Base 101
- jp1itslm.properties 29
- jp1itslmur.properties 29
- jslmmgrsetup 85
- jslmurnals 89
- jslmursetup 90

## K

- KB meaning 100

## L

- logging in to, SLM - Manager 37
- logging out of, SLM - Manager 38

## M

- managerHost 30
- MB meaning 100



- memory and disk space required for installation 15
- monitored service
  - after taking corrective action, verifying recovery of 80
  - in specific service group, checking status of 67
  - of all service groups, checking status of 66
  - registering 55
- monitoring
  - general procedure for 63
  - starting 64
- monitoring item 42, 101
  - setting up, for service performance 57

## O

- operation permission
  - specifying 26
- out-of-range value 50
- out-of-range value detection 101
  - about 50

## P

- performance data 101
- prerequisite OS 15
- primary authentication server 23

## R

- RD area 101
- Real-time Monitor window 74
  - checking status of monitored service of specific service group 68
  - verifying recovery of monitored service after taking corrective action 80
- restarting
  - SLM - Manager 34
  - SLM - UR 36

## S

- secondary authentication server 23
- sensitivity 50, 101
- service 101
- service group 26, 101
- service group administrator 26, 101
- service performance 42, 101
- service performance monitoring 101
- service user 26, 101
- setting up
  - JP1 user 25

- SLM - Manager 19
- SLM - UR 20
- Settings window
  - setting up monitoring item for service performance 57
  - starting monitoring 64
  - stopping monitoring 65
- SLA 101
- SLM
  - installing 17
  - starting 34
- SLM - Manager 101
  - logging in to 37
  - logging out of 38
  - notes about operations after login to 39
  - restarting 34
  - setting up 19
  - starting 34
- SLM - UR 101
  - restarting 36
  - setting up 20
  - starting 35
- SLM communication 95
- SLM installation folder conventions 99
- SLO 101
- starting
  - SLM 34
  - SLM - Manager 34
  - SLM - UR 35
- symbol conventions 98
- system definition file 101
  - editing 29
  - example definition in 32

## T

- TB meaning 100
- threshold value monitoring 101
  - about 45
- throughput
  - All Web Access 43
- timing of event causing error or warning, checking 74
- trend 47
- trend monitoring 101
  - about 47
- Troubleshoot window 74
  - checking timing of event causing error or warning 74

## U

upper-limit and lower-limit values 50

urHost 30

URI 101

urNetworkAdapterAddress 30

user setting 23

user setup, notes about 25

## W

Web access 43, 101

---

 **Hitachi, Ltd.**

6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100-8280 Japan

---