HITACHI
Inspire the Next

Job Management Partner 1 Version 10

Job Management Partner 1/Consolidated Management 2/SNMP System Observer Description, Operator's Guide and Reference

3021-3-345-20(E)

Notices

■ Relevant program products

Job Management Partner 1/Consolidated Management 2/SNMP System Observer (For Windows):

P-2942-8RAL Job Management Partner 1/Consolidated Management 2/SNMP System Observer 10-50 (For Windows Server 2008 and Windows Server 2012)

Job Management Partner 1/Consolidated Management 2/SNMP System Observer (For UXIX):

P-9D42-8RAL Job Management Partner 1/Consolidated Management 2/SNMP System Observer 10-50 (For Solaris)

P-8242-8RAL Job Management Partner 1/Consolidated Management 2/SNMP System Observer 10-50 (For Linux)

■ 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

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

AIX is a trademark of International Business Machines Corporation in the United States, other countries, or both.

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

Firefox is a registered trademark of the Mozilla Foundation.

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

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

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

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

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

Mozilla is a trademark of the Mozilla Foundation in the U.S and other countries.

OpenView is a trademark of Hewlett-Packard Development Company, L.P. in the U.S. and other countries.

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

PRIMECLUSTER is a trademark or a registered trademark of Fujitsu Limited in the United States and other countries.

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

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

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

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

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

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

The following program products contain some parts whose copyrights are reserved by Oracle and/or its affiliates: P-9D42-8RAL.

The following program product contains some parts whose copyrights are reserved by UNIX System Laboratories, Inc.: P-9D42-8RAL.

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

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

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

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

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).

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 Ralf S.Engelschall <rse@engelschall.com> for use in the mod_ssl project (`http://www.modssl.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 Daisuke Okajima and Kohsuke Kawaguchi (`http://relaxngcc.sf.net/`).

This product includes software developed by Andy Clark.

This product includes software developed by Carnegie Mellon University. Copyright 1989, 1991, 1992 by Carnegie Mellon University.

This product includes software developed by Object Refinery Limited and Contributors (`http://www.jfree.org/`). (C)opyright 2000-2009, by Object Refinery Limited and Contributors.

This product includes RSA BSAFE Cryptographic software of EMC Corporation.

HITACHI
Inspire the Next

Hitachi, Ltd.

Other product and company names mentioned in this document may be the trademarks of their respective owners. Throughout this document Hitachi has attempted to distinguish trademarks from descriptive terms by writing the name

with the capitalization used by the manufacturer, or by writing the name with initial capital letters. Hitachi cannot attest to the accuracy of this information. Use of a trademark in this document should not be regarded as affecting the validity of the trademark.

■ Microsoft product screen shots

Microsoft product screen shot(s) 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
ActiveX		ActiveX(R)
IE		Microsoft(R) Internet Explorer(R)
		Windows(R) Internet Explorer(R)
SMS		Microsoft(R) Systems Management Server
Windows	Windows NT	Microsoft(R) Windows NT(R) Server Enterprise Edition Version 4.0
		Microsoft(R) Windows NT(R) Workstation Operating System Version 4.0
	Windows Server 2003	Microsoft(R) Windows Server(R) 2003, Enterprise Edition
		Microsoft(R) Windows Server(R) 2003, Enterprise Edition for Itanium-based Systems
		Microsoft(R) Windows Server(R) 2003, Standard Edition
		Microsoft(R) Windows Server(R) 2003, Standard Edition for Itanium-based Systems
	Windows Server 2003, or Windows Server 2003 x64 Editions	Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
		Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
	Windows Server 2008	Microsoft(R) Windows Server(R) 2008 Enterprise
		Microsoft(R) Windows Server(R) 2008 Standard
	Windows Server 2008, or Windows Server 2008 R2	Microsoft(R) Windows Server(R) 2008 R2 Enterprise
		Microsoft(R) Windows Server(R) 2008 R2 Standard
	Windows Server 2012	Microsoft(R) Windows Server(R) 2012 Standard
		Microsoft(R) Windows Server(R) 2012 Datacenter
	Windows Server 2012, or Windows Server 2012 R2	Microsoft(R) Windows Server(R) 2012 R2 Standard
		Microsoft(R) Windows Server(R) 2012 R2 Datacenter
	Windows XP	Microsoft(R) Windows(R) XP Professional Operating System

■ Restrictions

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

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

■ Issued

Dec. 2014: 3021-3-345-20(E)

■ Copyright

Summary of amendments

The following table lists changes in this manual (3021-3-345-20(E)) and product changes related to this manual.

Changes	Location
A description of the fraction of resource values that are displayed or output was added.	*2.2.4*, *2.3.4*, *2.4.4*, *2.4.5*, *2.4.6*, *2.4.7*, *2.4.8*, *4.2.2*, *4.2.3*, *4.2.4*, *4.2.6*, *4.5.2*, *4.5.4*, *5. ssoextractlog*
A note on NNMi cooperation functions was added.	*2.6*
The NNM action address definition file (`ssonnmactaddr.conf`) was added.	*2.6.4*, *3.1.1*, *6.1.1*, *6.3.32*
The Resource Data Reference window can now be used to search collected data by server name.	*4.1.1*, *4.5*, *4.5.8*
The settings of the monitoring applications can now be changed.	*4.1.1*, *4.6.1*, *4.6.7*
The settings of the monitoring processes and child processes can now be changed.	*4.1.1*, *4.6.1*, *4.6.2*, *4.6.8*
The settings of the monitoring services can now be changed.	*4.1.1*, *4.6.1*, *4.6.9*
The Process Configuration window, Process Configuration Browser window, and Process Monitor window can now be used to search for specific monitoring servers.	*4.1.1*, *4.6*, *4.6.11*, *4.8*, *4.8.4*
Items were added to the *Acquired data* column of *Collected data list* (list of data items to be collected for error investigation).	*5. jp1ssolog.bat*, *5. jp1ssolog.sh*
Conditions in which `ssocadel` fails were added.	*5. ssocadel*
The user name and password can now include single-byte spaces. With this improvement, a usage example was added.	*5. ssonnmsetup*
In the user resource definition file, MIB expressions can now be written in infix notation. With this improvement, the subresource definition and definition example were changed.	*6.3.14*
JP1/Cm2/Extensible SNMP Agent 10-50 was added as an SNMP agent.	*E.4*
The custom incident attribute `change-my-address` was added to the resource collection status change event.	*F.1*

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

Preface

This manual explains the functions and operation methods of the following product:

Job Management Partner 1/Consolidated Management 2/SNMP System Observer (abbreviated hereafter to SSO)

This manual is for all supported operating systems. Any differences between operating systems in regard to the operation of this program are mentioned at the appropriate place in the manual.

Note

In this manual, JP1 is an abbreviation for Job Management Partner 1.

■ Intended readers

This manual is intended for persons using JP1/Cm2/SSO products to manage server system resources on networks. It is assumed that the readers have working knowledge of the SNMP protocol and the management of TCP/IP networks that use SNMP.

■ Organization of the manual

This manual is organized into the following chapters:

1. Overview

Outlines the SSO series programs, and describes the system configuration and program configuration of the SSO series.

2.Functions

Describes the SSO functions.

3. Installation and Setup

Describes the installation and uninstallation of each SSO program. Information about setup required before operation is also included.

4. Windows

Describes how to open the various SSO windows, the window transitions, the items displayed in the windows, and the settings of those items.

5. Commands

Describes the syntax and method of commands provided by each SSO program.

6. Definition Files

Describes the contents of definition files provided by each SSO program and the method of defining each definition file.

■ Conventions: Fonts and symbols

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

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

The following table explains the symbols used in this manual:

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

■ Conventions: Version numbers

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

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

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

Contents

Appendixes 426

1 Overview

This chapter outlines the SSO series, and describes the system configuration and program configuration of the SSO series.

1.1 Overview of the SSO series

As corporate networks get bigger, the workload on their business servers is increasing. Since a shutdown of these servers would also cause business activity to close down, the administrator must consider system resources management for these servers to be just as important as network management.

The SSO series is a group of programs that monitor system resources, processes, and services on network servers. If a specified threshold is exceeded, a process stops, or a change in the operating status of a service is detected, an event can be issued to notify the administrator. The notified administrator can then take measures, such as reducing the business processing load and using resources more efficiently, thereby lowering the total cost of ownership (TCO) of the system.

The features of the JP1/Cm2/SSO programs are as follows.

- Collecting information about various kinds of resources

  The JP1/Cm2/SSO programs can monitor server operating information (such as CPU utilization, memory usage, and file system usage), network performance information (such as line usage), and other system resources. Users can also add resources to be monitored as user resources.
- Monitoring of the operating status of processes and services

  The operating status of applications can be monitored by monitoring the status of processes and services. The operating status can be monitored in real time by using the Process Monitor window.

  The monitor can use threshold values as triggers and can execute a specific action on the monitored server automatically. For example, an incident can be issued when the number of running processes exceeds the preset number.
- Management with NNMi

  SSO sends monitoring events as incidents to NNMi. This allows use of the incident view of NNMi to manage of the status of SSO monitoring.

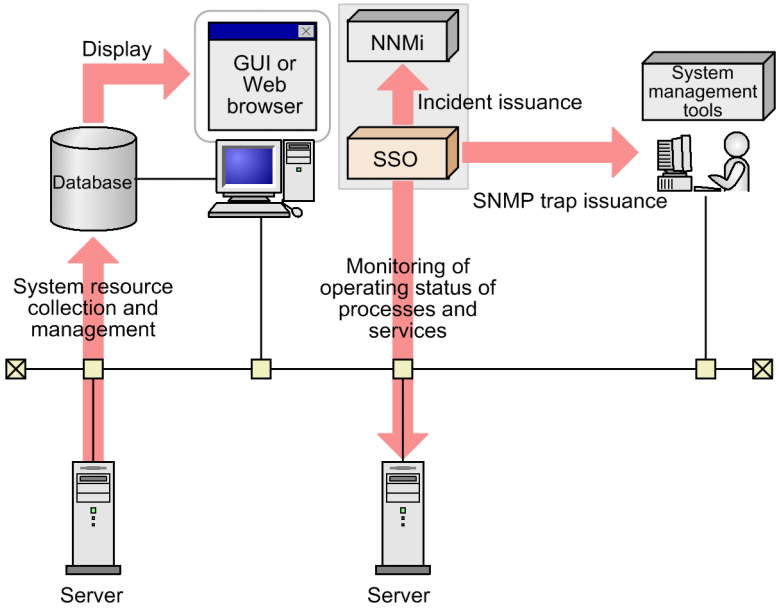
The main programs of the SSO series are SSO and APM. An overview of these programs is provided below.

1.1.1 Overview of the SSO

SSO collects and manages the system resources of network servers, and monitors the operating status of processes and services on network servers.

For the collection and management of system resources, the information managed by the SNMP agent on each server is acquired and stored in a database. The stored database information can be displayed graphically or as report files in a web browser. Incidents can also be issued to NNMi, and SNMP traps can be issued to system monitoring tools located on other hosts.

For monitoring the operating status of processes and services on network servers, monitoring conditions are set for the servers.


Display
GUI or Web browser
NNMi
Incident issuance
System management tools
Database
SSO
SNMP trap issuance
System resource collection and management
Monitoring of operating status of processes and services
Server
Server

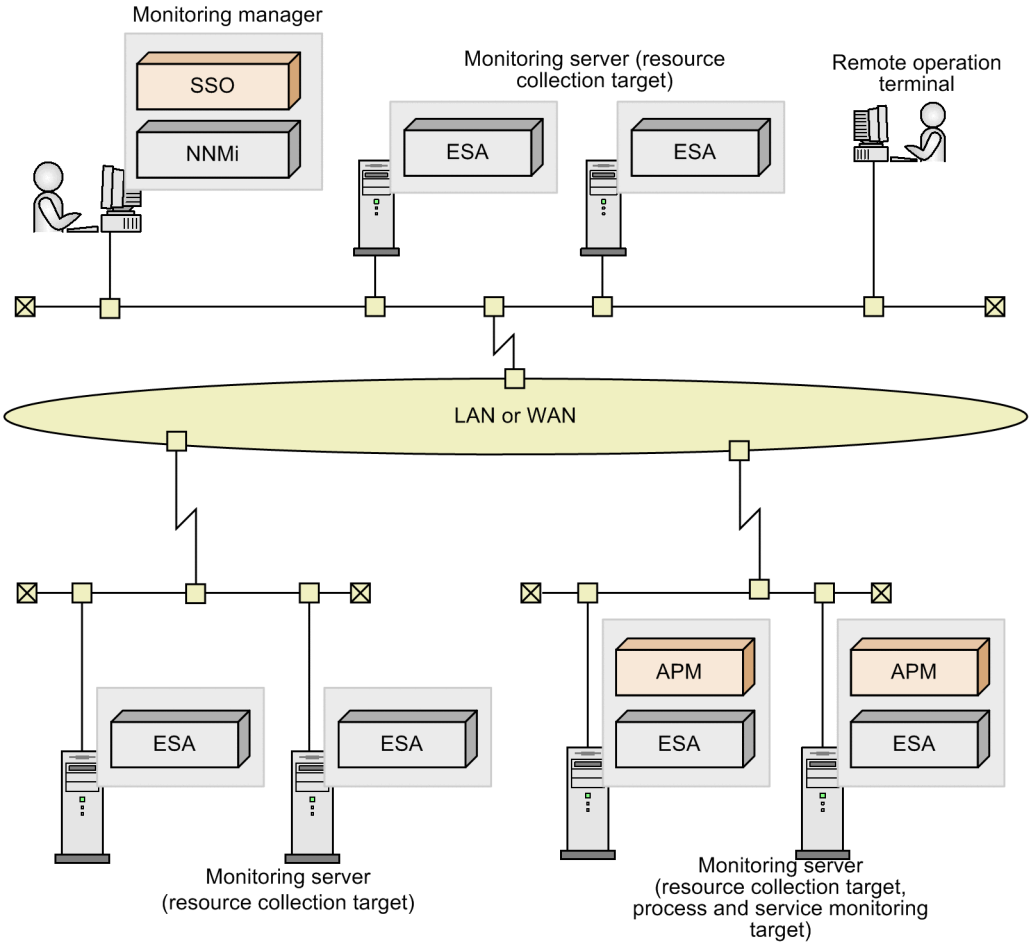
1.2 System configuration

This section describes SSO series systems in the basic configuration and in a distributed configuration, and describes the system components in these configurations.

1.2.1 Basic configuration

In the basic configuration, NNMi and SSO run on the same server. The following figure shows an example of the basic configuration.

Figure 1－1: System configuration (basic configuration)



In the basic configuration, the system is configured with the following components:

- Monitoring manager
- Monitoring server
- Remote operation terminal

Monitoring manager

The server on which SSO and NNMi run.

This server collects and monitors the system resource information of monitoring servers, and monitors processes and services on the monitoring servers.

Monitoring server

A server on which ESA and APM run.

ESA is an SNMP agent that is required for the collection of system resource information. APM is required for monitoring of the operating status of processes and services.

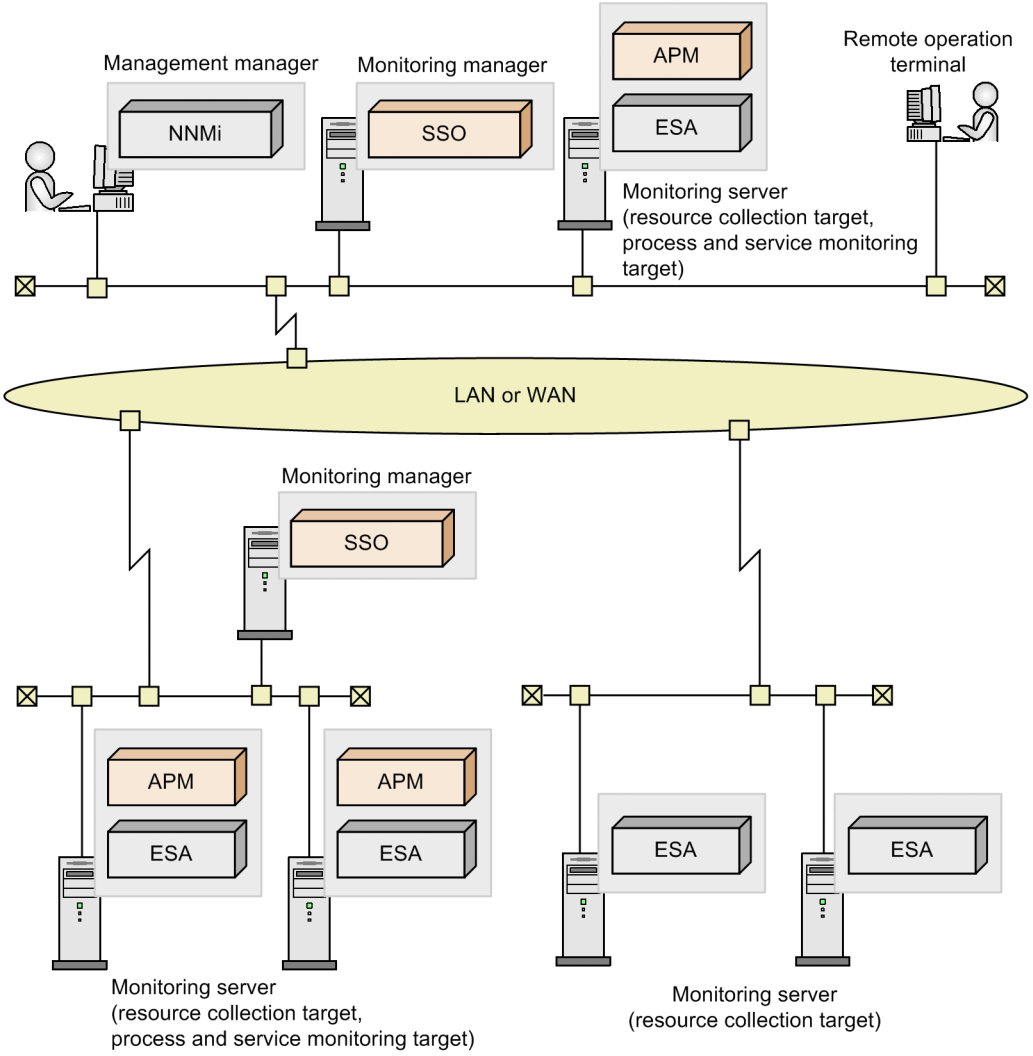
Remote operation terminal

A Windows or Linux machine that is required as a web browser execution environment for using the SSO console.

1.2.2 Distributed configuration

To monitor a large-scale system consisting of 1,000 or more monitoring servers, employ a distributed configuration in which NNMi and SSO run on separate servers. The following figure shows an example of a distributed configuration.

Figure 1-2: System configuration (distributed configuration)



In a distributed configuration, the system is configured with the following components:

- Management manager
- Monitoring manager
- Monitoring server

- Remote operation terminal

Management manager

The server on which NNMi runs. This server manages monitoring events that are reported as incidents from SSO.

Monitoring manager

The server on which SSO runs. This server collects and monitors the system resources information of monitoring servers, and monitors processes and services on the monitoring servers.

Monitoring server

A server on which ESA and APM run.

ESA is an SNMP agent that is required for the collection of system resource information. APM is required for monitoring of the operating status of processes and services.

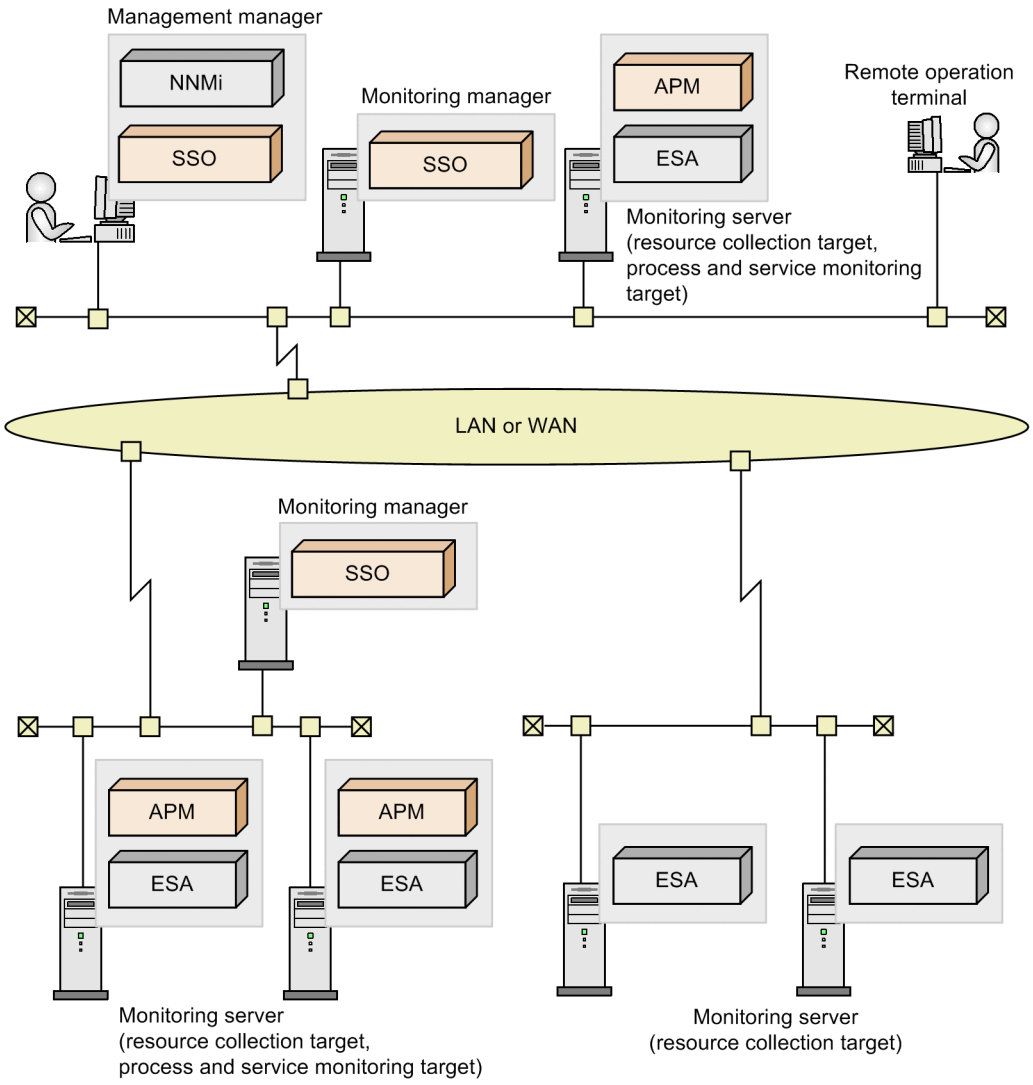
Remote operation terminal

A Windows or Linux machine that is required as a web browser execution environment for using the SSO console.

Supplementary note

The basic configuration and distributed configuration can be combined by installing SSO on the management manager. The following figure shows an example of the combination of the basic configuration and distributed configuration.

Figure 1‒3: System configuration (combination of basic configuration and distributed configuration)

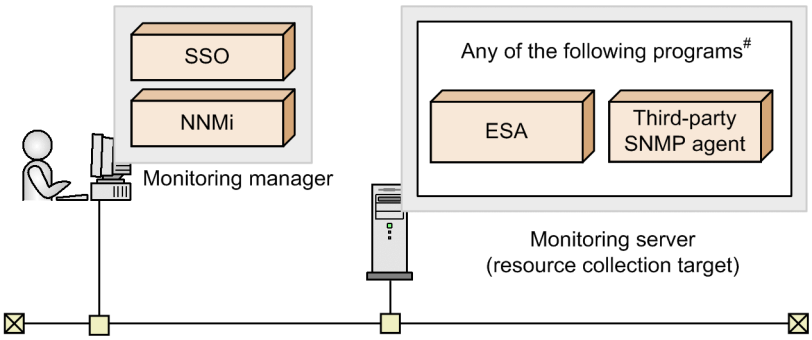


1.3 Programs

This section shows program configuration examples for systems that use the SSO series in the basic configuration and for systems that use the SSO series in a distributed configuration.

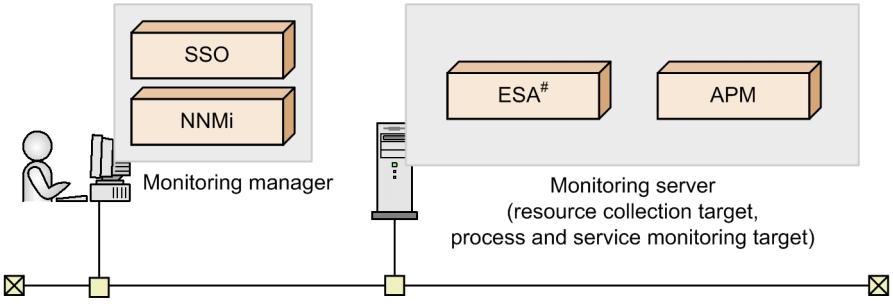
1.3.1 Basic configuration

(1) Program configuration for collecting resources



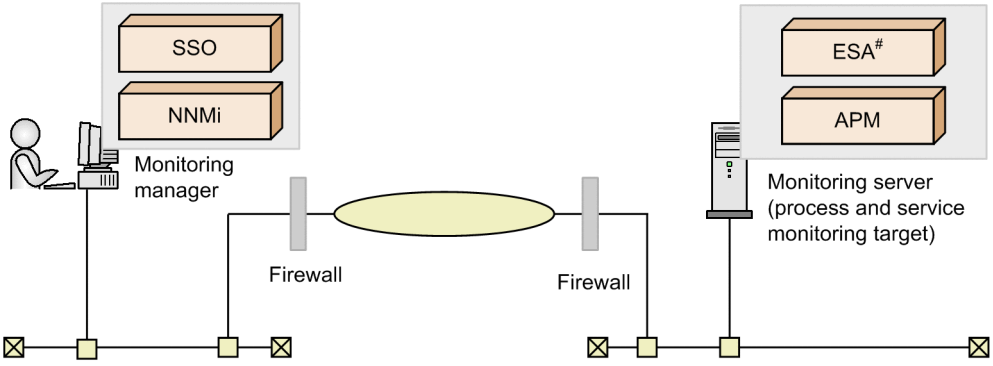
#: These programs are collectively referred to as *SNMP agents*.

(2) Program configuration for monitoring processes and services



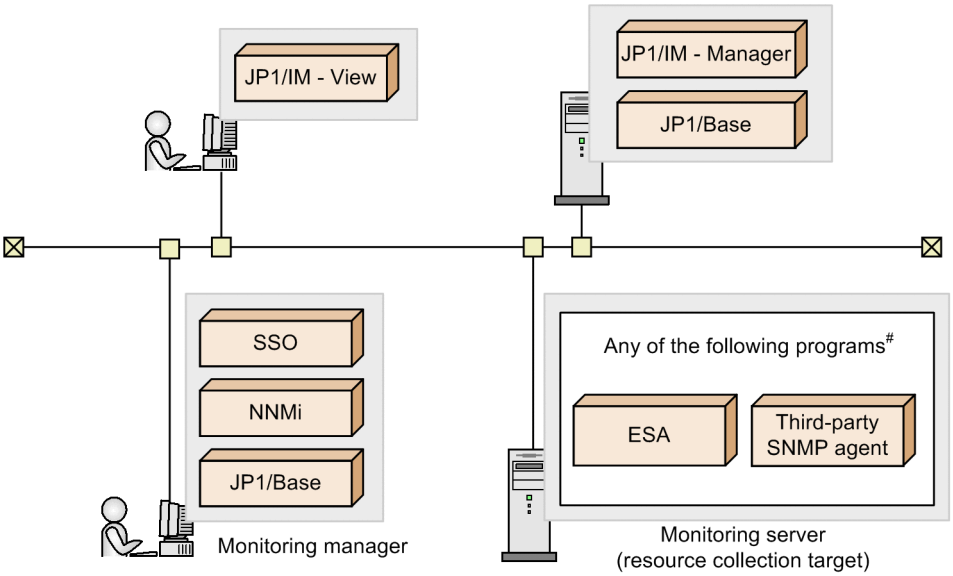
#: This program is referred to as *SNMP agent*.

(3) Program configuration for using firewalls



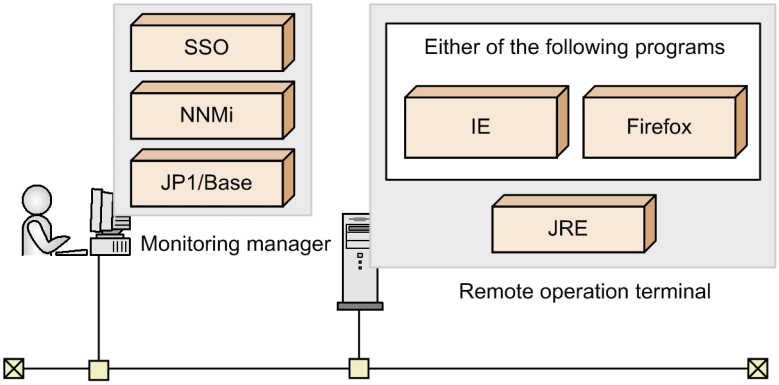
#: This program is referred to as *SNMP agent*.

(4) Program configuration for performing monitoring in conjunction with JP1/IM



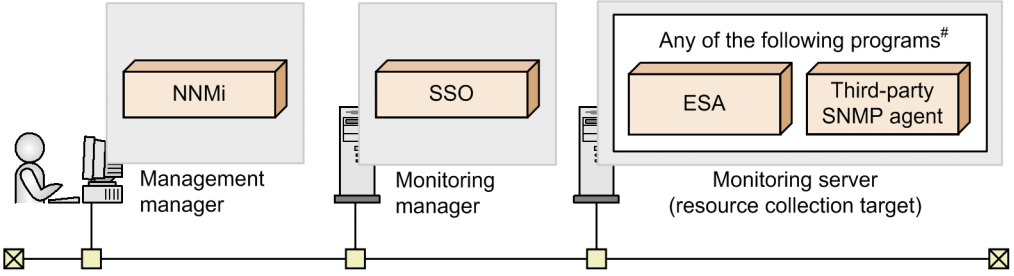
#: These programs are collectively referred to as *SNMP agents*.

(5) Program configuration for login from the SSO console by using the JP1 authentication method



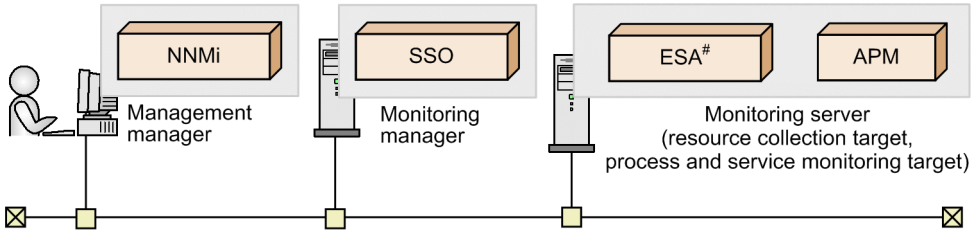
1.3.2 Distributed configuration

(1) Program configuration for collecting resources



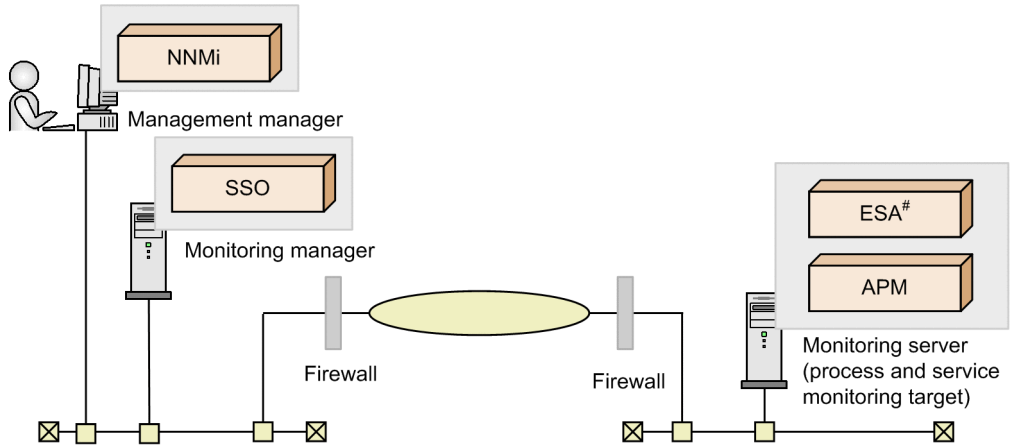
#: These programs are collectively referred to as *SNMP agents*.

(2) Program configuration for monitoring processes and services



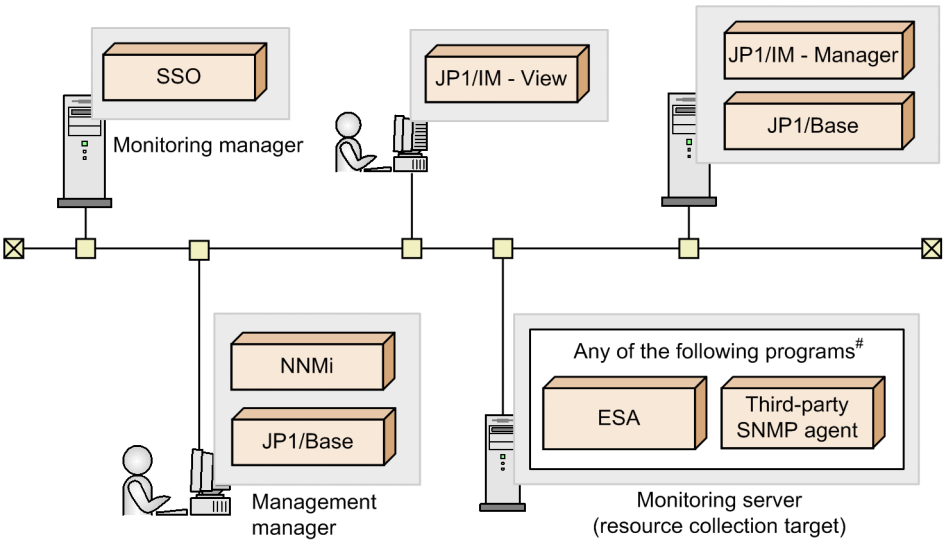
#: This program is referred to as *SNMP agent*.

(3) Program configuration for using firewalls



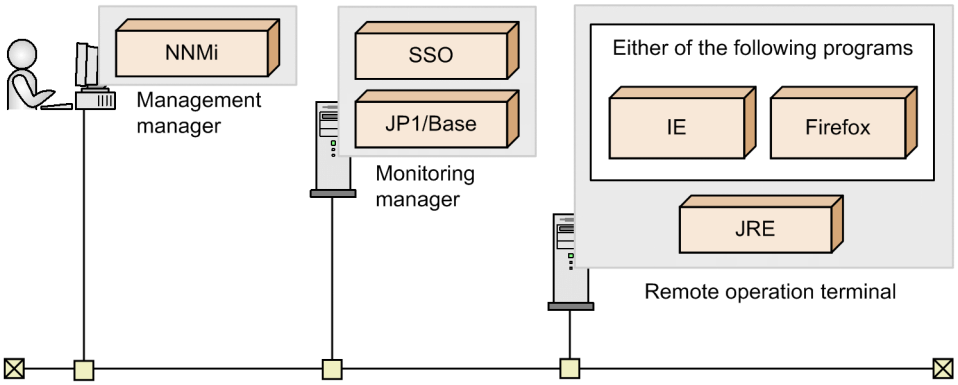
#: This program is referred to as *SNMP agent*.

(4) Program configuration for performing monitoring in conjunction with JP1/IM



#: These programs are collectively referred to as *SNMP agents*.

(5) Program configuration for login from the SSO console by using the JP1 authentication method



1.4 Monitoring in an IPv6 network environment

This section describes monitoring in an IPv6 network environment or in an environment in which IPv6 and IPv4 networks coexist.

1.4.1 System configuration for performing monitoring in an IPv6 network environment

This subsection describes the system configuration of the SSO series for performing monitoring in an IPv6 network environment, and the system components for the basic configuration and a distributed configuration.

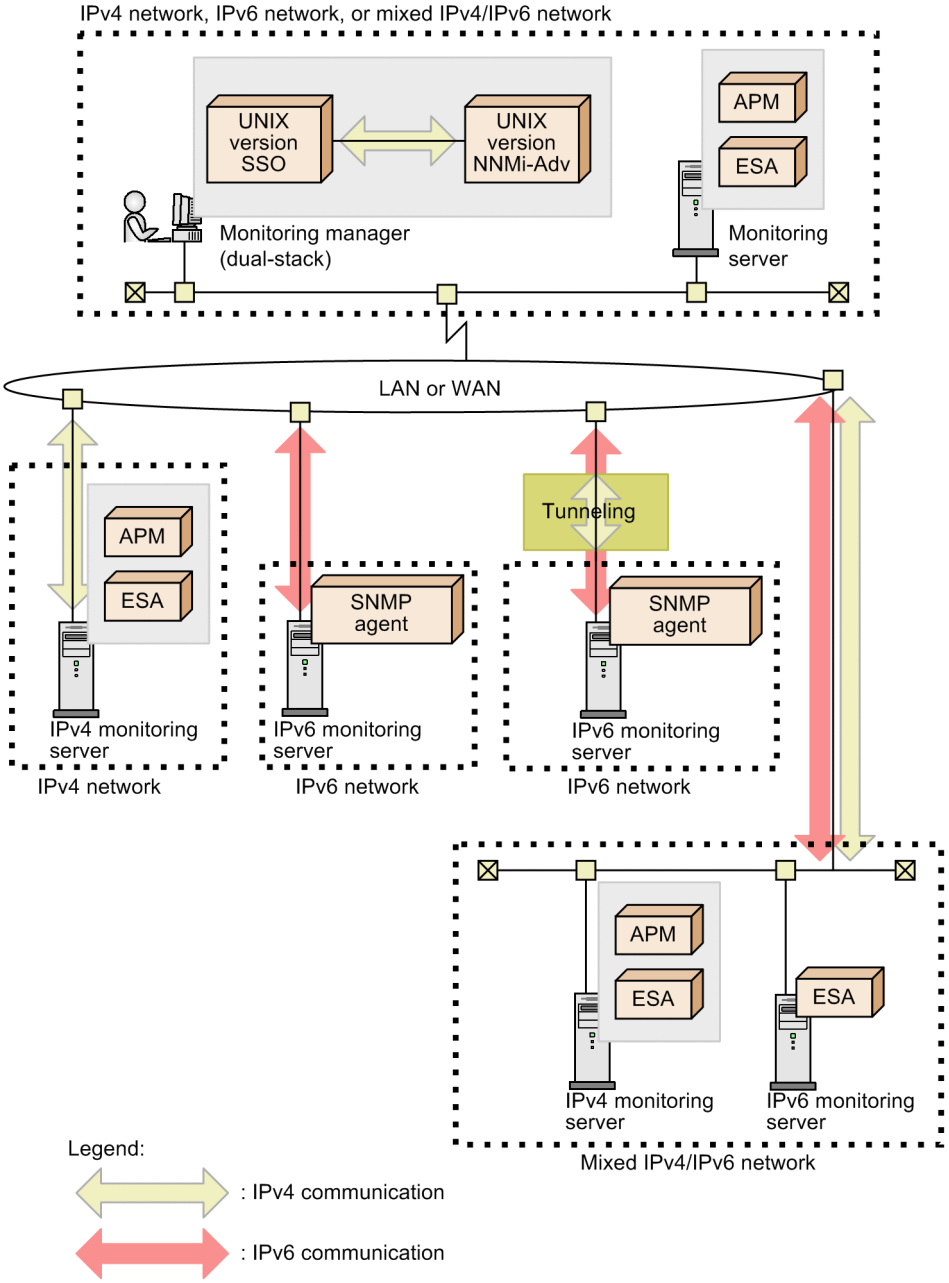
(1) Basic configuration

In the basic configuration, the monitoring manager host must be a dual-stack host.

In IPv4 networks, monitoring servers are monitored by using IPv4 communication. In IPv6 networks, monitoring servers are monitored by using IPv6 communication. In networks in which both IPv4 and IPv6 are used, monitoring servers are monitored by using IPv4 or IPv6 communication.

The following figure shows an example of the basic configuration.

Figure 1-4: Example of a system configuration including IPv6 networks (basic configuration)



(2) Distributed configuration

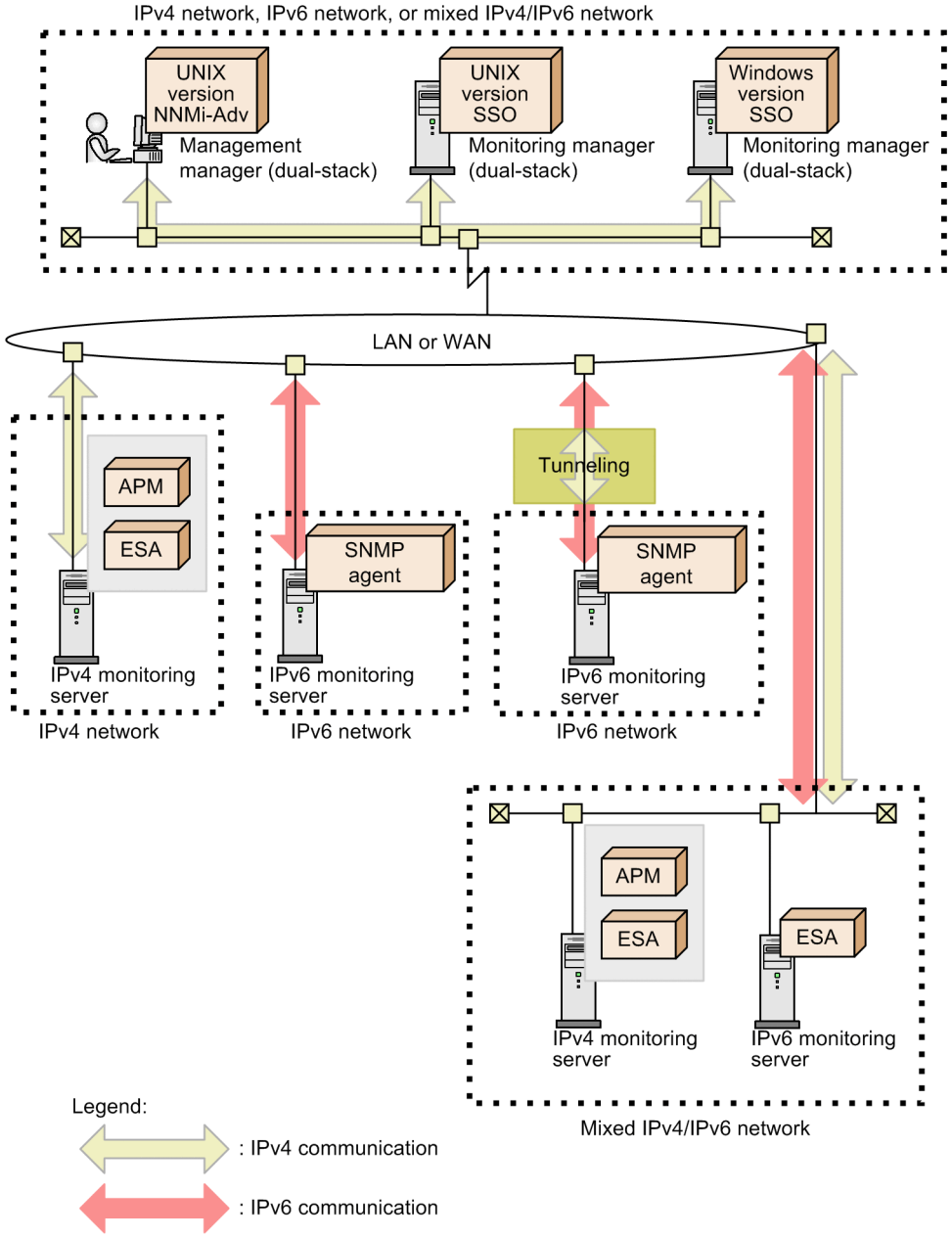
In a distributed configuration, the management manager host and the monitoring manager host must each be a dual-stack host.

In IPv4 networks, monitoring servers are monitored by using IPv4 communication. In IPv6 networks, monitoring servers are monitored by using IPv6 communication. In networks in which both IPv4 and IPv6 are used, monitoring servers are monitored by using IPv4 or IPv6 communication. Monitoring servers in IPv6 networks can also be monitored by using IPv6 communication via tunneling.

Note that the management manager host and the monitoring manager host must be able to communicate via IPv4.

The following figure shows an example of a distributed configuration.

Figure 1-5: Example of a system configuration including IPv6 networks (distributed configuration)



1.4.2 Notes on monitoring in an IPv6 network environment

This subsection presents notes on performing monitoring in an IPv6 network environment.

(1) Monitoring processes and services

APM does not support IPv6. Therefore, processes and services on monitoring servers in IPv6 networks cannot be monitored.

(2) Notes on IP addresses of monitoring servers

If you use an IPv6 address to specify a monitoring server via the GUI or a command, make sure that the address conforms to the IPv6 notation defined in RFC 2373. You cannot specify IPv4-compatible IPv6 addresses, link-local addresses, or multicast addresses.

(3) Notes on site-local addresses

Site-local addresses that have a scope ID are not supported. If a site local address that has a scope ID is specified, the scope ID (% + scope ID) is ignored.

(4) IPv6 addresses output to commands, windows, and definition files

The following explains the format of IPv6 addresses that are output to commands, windows, and definition files:

- Eight groups of 2-byte (16-bit) hexadecimal values delimited by colons (`:`).
- All hexadecimal alphabetic characters are output in lowercase.
- The leading 0s of a 2-byte hexadecimal number are omitted. However, a 2-byte hexadecimal that consists of all 0s is output as 0.
- Even in the case of consecutive 2-byte hexadecimal numbers that consist of all 0s, the abbreviation `::` is not used.
- If the last 32 bits of an IPv6 address indicate an IPv4 address, the IPv4 address is output with hexadecimal numbers rather than decimal numbers.

  For example, rather than `2001:db8::5efe:1.2.3.4`, `2001:db8:0:0:0:5efe:102:304` is output.
- IPv4-mapped IPv6 addresses are output as IPv4 addresses.

The following IPv6 addresses are all displayed as `2001:db8:0:0:1:0:0:1`.

- `2001:db8:0:0:1:0:0:1`
- `2001:0db8:0:0:1:0:0:1`
- `2001:db8::1:0:0:1`
- `2001:db8::0:1:0:0:1`
- `2001:0db8::1:0:0:1`
- `2001:db8:0:0:1::1`
- `2001:db8:0000:0:1::1`
- `2001:DB8:0:0:1::1`

1.5 Monitoring in an NNMi global network management environment

This section describes monitoring in an NNMi global network management environment.

1.5.1 System configuration in an NNMi global network management environment

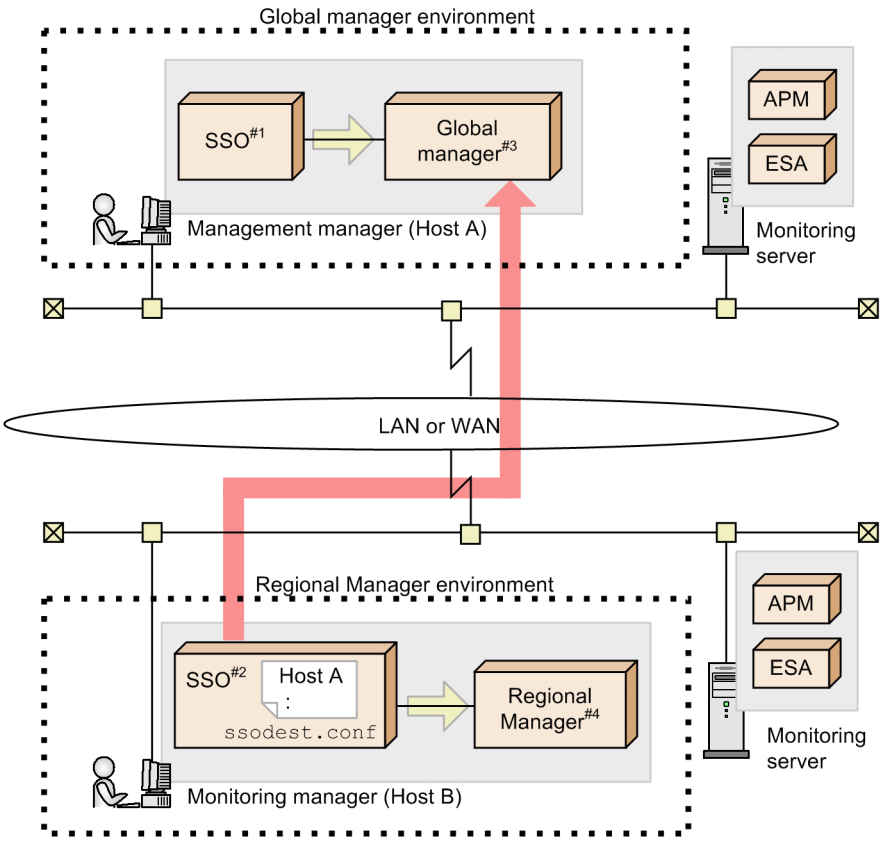
The system configuration of the SSO series in an NNMi global network management environment and the components that make up the system are described below.

In an NNMi global network management environment, SSO is placed in a Regional Manager environment. The system is configured so that events that occur during the collection of resources and the monitoring of processes and services are also transmitted to the global manager, so as to enable centralized monitoring from the global manager. Event transmission to the global manager can be enabled by using the event destination definition file (`ssodest.conf`). For details on this file, see *6.3.13 Event destination definition file (ssodest.conf)*.

If needed, SSO can also be placed in the global manager environment.

The following figure shows an example of the system configuration.

Figure 1-6: Example of the system configuration in an NNMi global network management environment



#1: Not required. Place as needed.
#2: Either the basic configuration or a distributed configuration can be used.
#3: Must be NNMi-Adv.
#4: Must be either NNMi or NNMi-Adv.

Legend:

: Event notification

: Event transmission (`ssodest.conf`)

1.5.2 Notes on an NNMi global network management environment

(1) Notes on dynamic NAT and PAT/NAPT environments

SSO does not support dynamic NAT environments or PAT/NAPT environments that use NNMi global network management functions.

(2) Notes on reconfiguration of an NNMi global network management environment

If an NNMi global network management environment is reconfigured while SSO is running (reconfiguration of the regional manager management node on the global manager), either restart SSO in the regional manager environment, or execute the `ssoapcom -n` command and the `ssocolmng -n` command.

2 Functions

This chapter describes the SSO functions.

2.1 SSO console function

The SSO console function allows remote operations, such as setting the conditions for the monitoring of processes and services, and creating reports, via a web browser. The users who are allowed to use the SSO console function can also be restricted by using user authentication. This section describes the SSO console function.

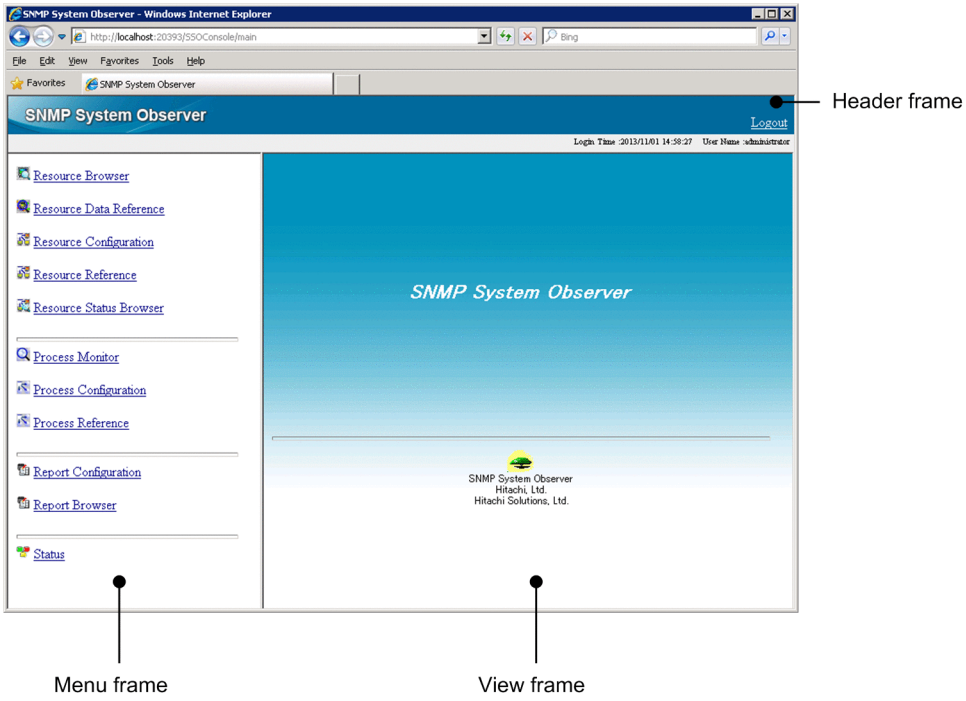
2.1.1 SSO console

The SSO console is a window used to reference reports and statuses. The Process Monitor window and other windows can be opened from the SSO console, which serves as the starting point for remote operation. The SSO console is displayed by accessing the following URI from a web browser and then logging in.

```
http://host-name:port-number/SSOConsole/
```

The following figure shows the SSO console window.

Figure 2-1: SSO console window



The items displayed in the above window are described below.

(1) Header frame

Logout

This item is displayed only if user authentication is enabled.

Click this item to log out from the SSO console. After you log out, the window changes to the SSO console login window.

If the user performs no operations on the SSO console until the timeout time expires, the user is forced to log out from the SSO console even if a window opened from the SSO console is being used. That window also is closed.

The timeout time can be changed by using the `ssoconsoled` action definition file. For details on this file, see *6.3.23 ssoconsoled action definition file (ssoconsoled.def)*.

(2) Menu frame

This is the area that contains the menu of functions provided by the SSO console. The menu consists of links. Clicking a menu item opens the corresponding window, or displays a report file list or status information in the view frame. The menu items of the menu frame are described below.

Resource Browser

Opens the Resource Browser window. For details, see *4.2 Resource Browser window*.

Resource Data Reference

Opens the Resource Data Reference window. For details, see *4.5 Resource Data Reference window*.

Resource Configuration

Opens the Resource Configuration window. For details, see *4.3 Resource Configuration window*.

Resource Reference

Opens the Resource Reference window. For details, see *4.4 Resource Reference window*.

Resource Status Browser

Displays the display condition setup view, which is used to set the resource status display conditions, in the view frame. The following shows the display condition setup view and describes the items displayed in that view.

Figure 2-2: Display condition setup view

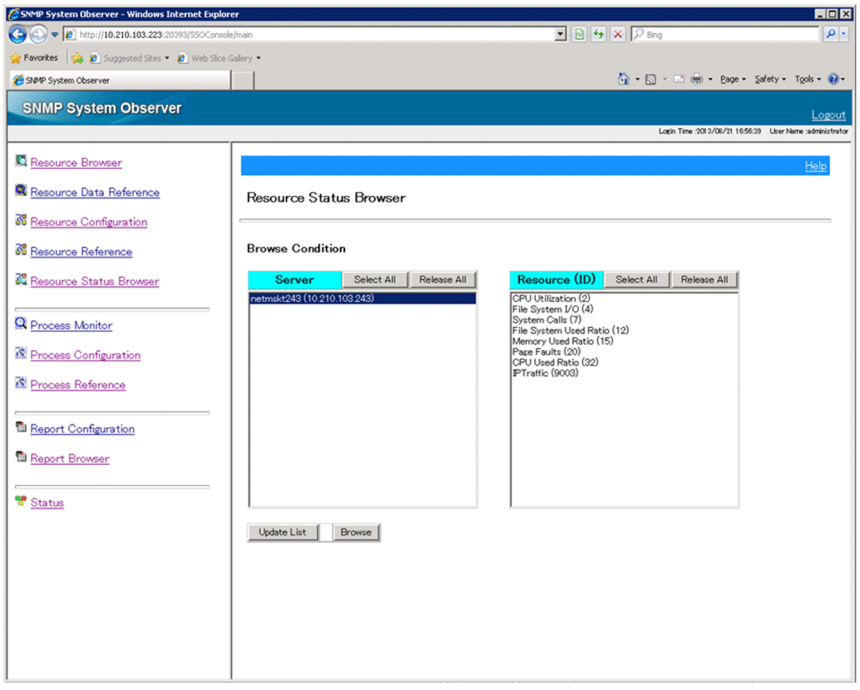


Table 2-1: Items displayed in the display condition setup view

Item	Description
Server	A list box that lists the servers whose resources are being monitored. In this list box, you can select the server whose resource status you want to display.
Resource (ID)	A list box that lists the resources that are being monitored. In this list box, you can select the resources whose status you want to display.
Select All	Click this item to select all the items displayed in the list box.

Item	Description
Release All	Click this item to deselect all the items selected in the list box.
Update List	Click this item to update the status of the monitored servers and resources.
Browse	Click this item to display the resource status display window, which displays the statuses of resources that match the specified display conditions.

After you have specified the conditions in the display condition setup window, if you click the **Browse** button, the resource status display window appears. The following shows the resource status display window and describes the resource status icons displayed in that window.

Figure 2-3: Resource status display window

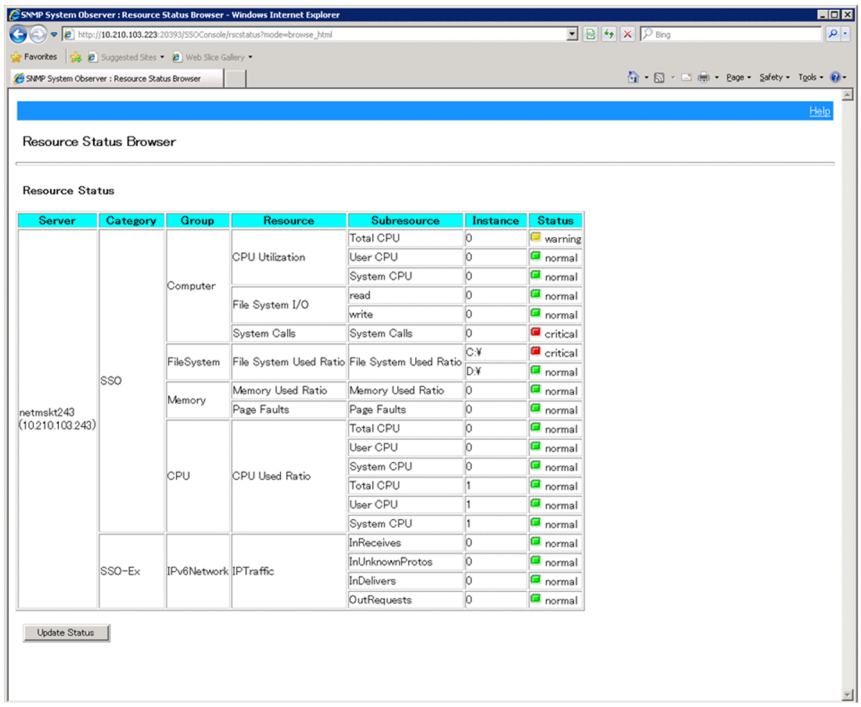


Table 2-2: Resource status icons displayed in the resource status display window

Icon	Resource status
(Green)	Normal
(Yellow)	Warning
(Red)	Critical
(Blue)	Unknown

Note

For resources whose values have not been calculated, a hyphen (-) is displayed. Resource values are not calculated in the following cases:

- Threshold monitoring is not performed.
- Resource values have not yet been collected (for example, immediately after the start of collection).

For the meaning of resource statuses, see *2.2.3(2) Thresholds and resource statuses*. For the resource hierarchy, such as categories and resource groups, see *2.2 Resource monitoring function*.

Process Monitor

Opens the Process Monitor window. For details, see *4.8 Process Monitor window*.

Process Configuration

Opens the Process Configuration window. For details, see *4.6 Process Configuration window*.

Process Reference

Opens the Process Reference window. For details, see *4.7 Process Reference window*.

Report Configuration

Opens the Report Configuration window. For details, see *4.9 Report Configuration window*.

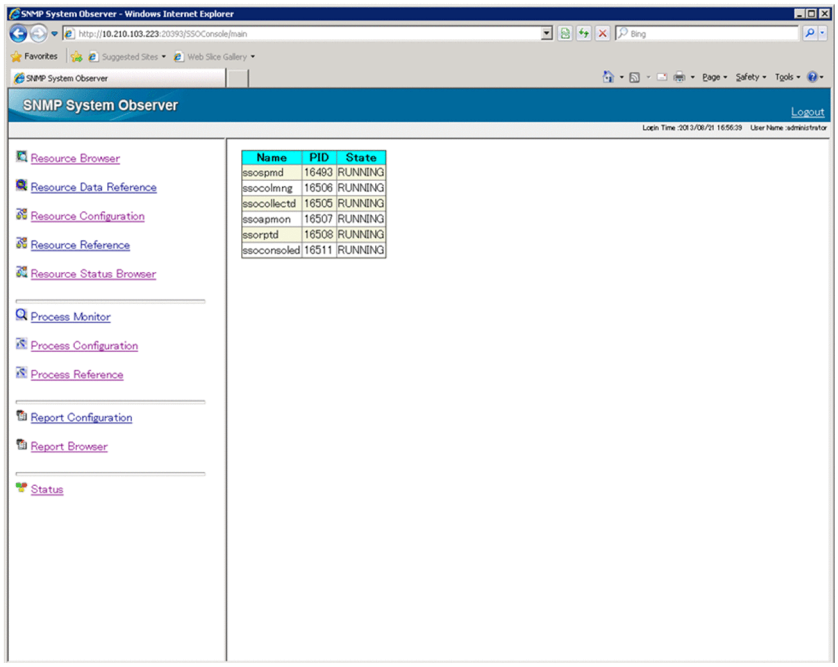
Report Browser

Displays a list of created report files in the view frame.

Status

Displays the status of each daemon process in the view frame. The following figure shows an example of the console window displayed when **Status** is clicked.

Figure 2–4: Example of the console window displayed (when Status is clicked)



(3) View frame

The area where the list of report files or status information is displayed.

(4) Note on use in a Chinese environment

If the OS of the monitoring manager is Windows or Linux and the language environment variable of SSO is Chinese, the text in the following areas is displayed in Chinese. For details on the supported Chinese language environment variables, see *H. Language Environment Variables*.

- Header frame
- Menu frame

- View frame (buttons and labels in the Resource Status Browser window and the Report Browser window)

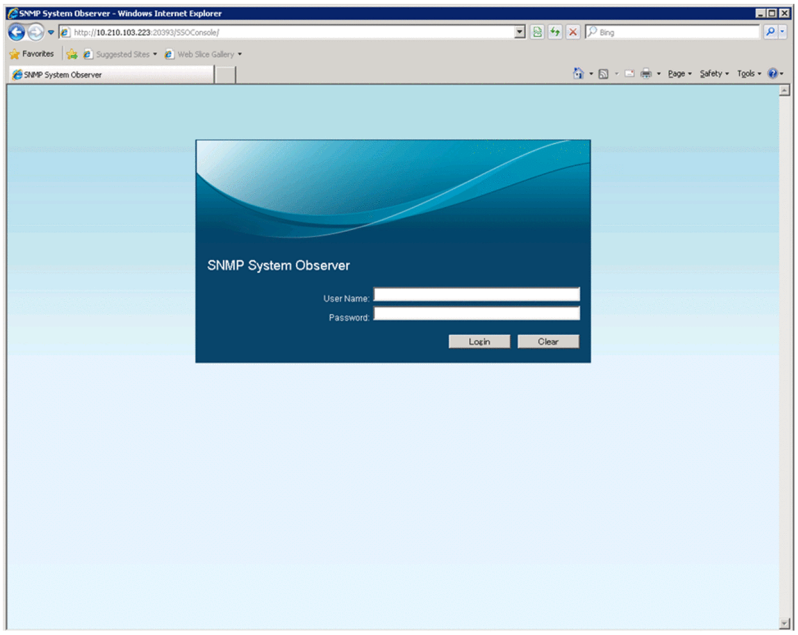
2.1.2 User authentication

User authentication can be used for users who wish to log in to the SSO console. If user authentication is enabled, the login window is displayed. If user authentication is not enabled, the SSO console is displayed directly without the login window being displayed.

(1) SSO console login window

The following figure shows the login window.

Figure 2-5: SSO console login window



The items displayed in the above window are described below.

User Name

The name of the user who is logging in is entered here.

- When using the SSO authentication method
  The name of a user account registered with the `ssoauth` command is entered.
- When using the JP1 authentication method
  The name of a user account registered as a JP1 user in JP1/Base is entered.

Password

The password for this user name is entered here. If no password was set by using the `ssoauth` command, no password need be entered.

Login

Authenticates the user. If authentication is successful, the SSO console is displayed.

Clear

Clears the entered user name and password.

(2) User authentication methods

The following two authentication methods are available:

- SSO authentication method
- JP1 authentication method

The default authentication method is the SSO authentication method. The following subsections describe the two authentication methods and how to change between the methods.

(a) SSO authentication method

The SSO authentication method is a user authentication method designed specifically for SSO, and in which the user information is managed by SSO. User information can be added, deleted, and edited by using the `ssoauth` command. User information is stored in the user authentication definition file (`ssoauth.conf`). For details on this file, see *6.3.26 User authentication definition file (ssoauth.conf)*.

For the SSO authentication method, `administrator` is registered as the default login user. Because no password is set for the `administrator` user, we recommend that you either set a password if needed, or delete the `administrator` user and then create a new user to meet the user's operation requirements.

(b) JP1 authentication method

The JP1 authentication method uses JP1/Base, and the user information is managed centrally by JP1/Base. Logged-in users are created as *JP1 users* by JP1/Base, which is the authentication server. User permission is set as follows:

- JP1 resource group name: `JP1_SSO`
- JP1 permission level: `JP1_SSO_Admin`

You can also use JP1 user `jp1admin`, which is the default JP1 user registered in JP1/Base.

For the JP1 authentication method, JP1/Base is required on the host where SSO is installed. For details on user authentication by using JP1/Base, see the *Job Management Partner 1/Base User's Guide*.

(c) Changing the authentication method

To change the authentication method or disable user authentication, change the `authentication` key in the `ssoconsoled` action definition file (`ssoconsoled.def`). For details on this file, see *6.3.23 ssoconsoled action definition file (ssoconsoled.def)*. The changes made to the `ssoconsoled` action definition file are applied by either restarting the `ssoconsoled` daemon, or by executing the `ssoconsoled -r` command.

2.2 Resource monitoring function

SSO provides the following two SSO resource monitoring methods:

- Browsing by using the Resource Browser
- Collection by using the collection conditions that are set
  In resource monitoring through collection, threshold monitoring is also possible.

The following table shows the hierarchy of resources that can be browsed and collected using SSO.

Table 2-3: Hierarchy of resources

Name	Description
Category	This is a group of multiple resource groups. This name categorizes the group as containing resources provided by SSO or user defined resources. The category name for resources provided by JP1/Cm2/SSO is *SSO* and *SSO-Ex*.
Resource group	This is a group of multiple resources.
Resource	This is a group of multiple subresources.
Subresource	This is the smallest unit of a resource that an SNMP agent can acquire.

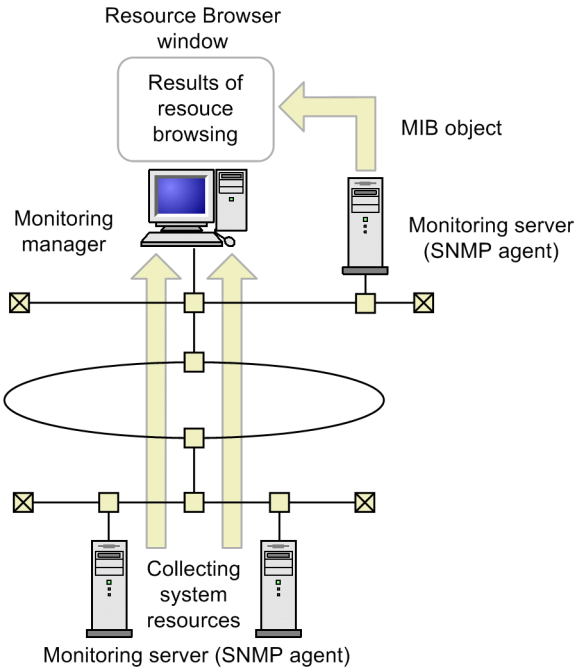
Resources are monitored based on this hierarchy of resources. This section describes the resource monitoring functions.

2.2.1 Resource browsing function

You can browse the resources of servers on a network. This function acquires MIB objects from SNMP agents and displays them in the Resource Browser window of the monitoring manager.

The following figure shows how SSO browses resources.

Figure 2-6: Flow of resource browsing



If the ESA is running on the SMS server, the SMS information can be browsed as well. SSO can browse two types of resources: summary data and performance data.

Summary data

Static information such as computer configuration information and setup information

Performance data

Dynamic information whose value varies by time such as operational information and statistics

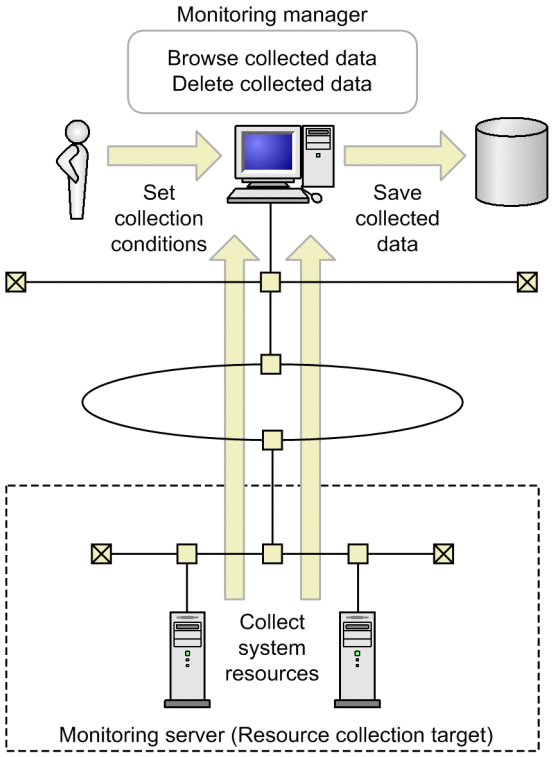
The SNMP-agent protocol versions that are supported for resource browsing are SNMP Version 1 (SNMPv1) and SNMP Version 2 (SNMPv2c).

The resources that JP1/Cm2/SSO can browse depend on the MIB object that can be acquired by the SNMP agent.

2.2.2 Resource collection function

Resources can be collected periodically according to predefined conditions. Data collected in this manner is stored in the database and can be browsed in the form of a table or graph. You can also set it so that if a preselected value is exceeded, the event is issued or a command is automatically executed. The following figure shows how SSO collects the resources.

Figure 2-7: Flow of resource collection



SSO saves the data collected from the monitoring server to a database. The collected data can be referenced and deleted on the monitoring manager. If threshold monitoring is used, an event can be issued to the monitoring manager when a threshold is exceeded.

Because resources are collected from the MIB object of the SNMP agent on the monitoring server, the get-community-names of SSO and the SNMP agent must match.

The SNMP-agent protocol versions that are supported for resource collection are SNMP Version 1 (SNMPv1) and SNMP Version 2 (SNMPv2c).

The collectable resources depend on the SNMP agent that can be acquired by the MIB object. The following explains the detail of resource collection function.

(1) Setting collection conditions

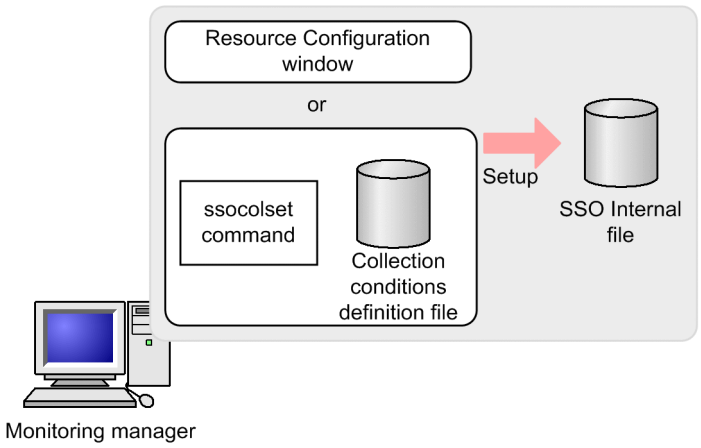
Set the following as the conditions for collecting resources:

- Server from which resources are to be collected
- Resources to be collected
- Instance
- Collection mode (save data, threshold)

Collection modes, such as thresholds, can be set individually for each subresource. Registering instances makes it possible to set a collection mode for each instance. You can also set an interval and time for collecting resources.

To set the collection conditions, use the Resource Configuration window or collection condition configuration command (`ssocolset`). The following figure shows how collection conditions are set up.

Figure 2-8: Collection condition setup schema



(2) Collecting resources

Resources are to be collected in accordance with the collecting conditions registered in the collecting condition configuration file. The MIB objects of the resources targeted for collection are acquired from the SNMP agent running on the servers targeted for collection. The MIB objects are then stored in the database.

In resource collection, the following functions can be used.

- Collection status management
- Monitoring threshold
- Automatic action

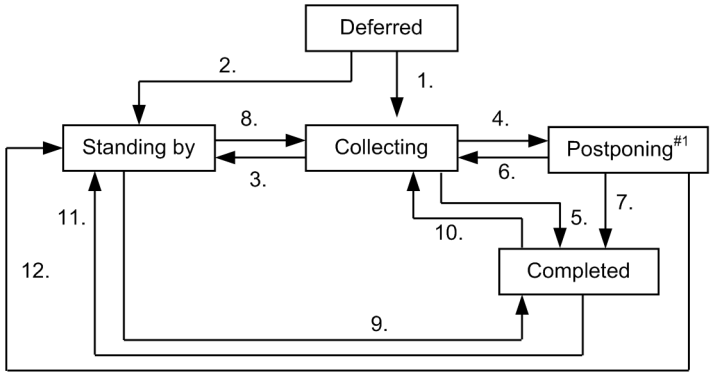
The timing at which the resource collection value is determined differs according to the resource. This is because there are resources that are calculated based on increments per collection interval for MIB objects, and resources that are calculated based on the current value of the MIB object.

Management of the collection status is described below. For details on threshold monitoring and automatic actions, see *2.2.3 Threshold monitoring*.

(a) Collection status management

Status is managed from the start to the end of resource collection. You can browse the collection status using the Resource Configuration window. Figure 2-9 shows the connection statuses managed by SSO and the collection status change triggers when the collection status *Impossibility* is disabled during a new installation. Figure 2-10 shows the connection statuses managed by SSO and the collection status change triggers when the collection status *Impossibility* is not disabled. For how to disable the collection status *Impossibility*, see *ssocollectd* and *ssocolmng* in *5. Commands*.

Figure 2-9: Transitions in collection status when collection status "Impossibility" is disabled



1. The following events occurred simultaneously when collection started:
   - The start time specified at the start of collection (or, if not specified, the current time) was reached.
   - No collection time period was specified, or the current time fell within the specified collection time period.
2. Either of the following events occurred at the start of collection:
   - The start time specified at the start of collection (or, if not specified, the current time) was not reached.
   - The current time was outside the specified collection time period.
3. The current time was outside the specified collection time period.
4. Any of the following events occurred:
   - An SNMP error response was received.
   - SNMP request issuance or SNMP response reception failed.
   - The resources to be collected were not supported.
   - Writing of the collected data to the database failed.
5. Any of the following events occurred:
   - SSO stopped or paused.#2
   - Collection was stopped either through the Resource Configuration window or by the `ssocolstop` command.
   - The end time specified at collection response reception or collection start was exceeded.
6. At reception of a collection response, a normal response was received.
7. Same as 5.
8. Any of the following events occurred:
   - The start time specified at collection start was reached.
   - The current time was within the specified collection time period.

- Collection restarted due to SSO startup.[#3]

9. Any of the following events occurred:
   - SSO stopped or paused.[#2]
   - Collection was stopped either through the Resource Configuration window or by the `ssocolstop` command.
   - The end time specified at collection start was reached.
10. Same as 1.
11. Same as 2.

    Alternatively, collection to be restarted at SSO startup[#3] did not restart because SSO start processing was in progress.
12. Same as 3.

#1

When the resource status is Postponing, the collection interval is changed to 30 minutes by default. When normal collection resumes, the collection interval reverts to the preselected setting. If the preselected collection interval is 30 minutes or greater, the above collection interval change does not take place. The collection interval for the Postponing status can be defined in the ssocollectd action definition file. For details about the ssocollectd action definition file, see *6.3.9 ssocollectd action definition file (ssocollectd.def)*.

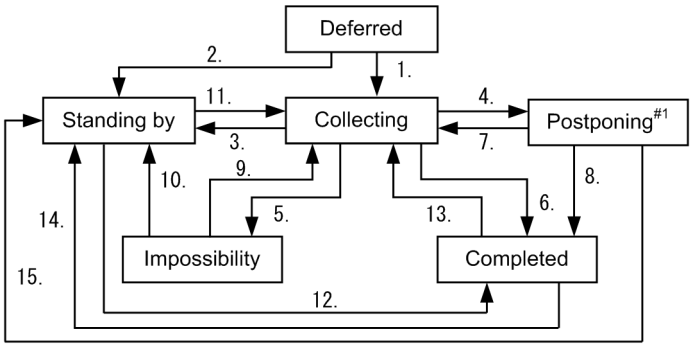
#2

If collection stops because SSO stopped or the `ssocolmng` daemon process paused, the *Completed* collection status change event is not issued. Also, if collection ends because the `ssocolmng` daemon process paused, no resource status change event is issued.

#3

Collection that stopped because SSO stopped or the `ssocolmng` daemon process paused can be restarted when SSO starts. In this case, the *Collecting* and *Standing by* collection status change events are not issued.

Figure 2－10: Transitions in collection status when collection status "Impossibility" is not disabled



1. The following events occurred simultaneously when collection started:
   - The start time specified at the start of collection (or, if not specified, the current time) was reached.
   - No collection time period was specified, or the current time fell within the specified collection time period.
2. Either of the following events occurred at the start of collection:
   - The start time specified at the start of collection (or, if not specified, the current time) was not reached.
   - The current time was outside the specified collection time period.
3. The current time was outside the specified collection time period.
4. A `noSuchName`, `genErr`, or `timeOut` SNMP error has been received.
5. Any of the following events occurred:

- An SNMP error other than `noSuchName`, `genErr`, or `timeOut` has been received.
- Issuance of an SNMP request or reception of an SNMP response failed.
- The resources to be collected were not supported.
- Writing of the collected data to the database failed.

6. Any of the following events occurred:
   - SSO stopped or paused. #2
   - Collection was stopped either through the Resource Configuration window or by the `ssocolstop` command.
   - The end time specified at collection response reception or collection start was exceeded.
7. At reception of a collection response, a normal response was received.
8. Same as 6.
9. Same as 1.
10. Same as 2.
11. Any of the following events occurred:
    - The start time specified at collection start was reached.
    - The current time was within the specified collection time period.
    - Collection restarted due to SSO startup.#3
12. Any of the following events occurred:
    - SSO stopped or paused.#2
    - Collection was stopped either through the Resource Configuration window or by the `ssocolstop` command.
    - The end time specified at collection start was reached.
13. Same as 1.
14. Same as 2.

    Alternatively, collection to be restarted at SSO startup#3 did not restart because SSO start processing was in progress.
15. Same as 3.

#1

When the resource status is Postponing, the collection interval is changed to 30 minutes by default. When normal collection resumes, the collection interval reverts to the preselected setting. If the preselected collection interval is 30 minutes or greater, the above collection interval change does not take place. The collection interval for the Postponing status can be defined in the ssocollectd action definition file. For details about the ssocollectd action definition file, see *6.3.9 ssocollectd action definition file (ssocollectd.def)*.

#2

If collection stops because SSO stopped or the `ssocolmng` daemon process paused, the *Completed* collection status change event is issued. Also, if collection ends because the `ssocolmng` daemon process paused, no resource status change event is issued.

#3

Collection that stopped because SSO stopped or the `ssocolmng` daemon process paused can be restarted when SSO starts. In this case, the *Collecting* and *Standing by* collection status change events are not issued.

When the collection status changes, SSO can issue a collection status change event. For details on events, see *F. Events*.

(3) Saving collected data

The collected data is saved in a database on a per-resource basis. This database is called the *collection database*. The collection database is classified into two types: master database and copy database. The master database stores collected data. Copying the master database of the local host or remote host generates the copy database. The following explains the collection database.

(a) Resource directory

The collection database is created for each server in the resource directory for collected resources. The resource directory is the directory that SSO creates for each resource. For the names of resource directories, see *E. Resource IDs*.

(b) Collection database name

Collection database consists of data files (`.log`) for collected data storage, information files (`.inf`) for database information storage, and instance files (`.ins`) for instance information storage. JP1/Cm2/SSO determines the collection database name according to the naming rules. The collection database naming rules are stated below:

`sso_`*database-identification monitoring-manager-name monitoring-server-name serial-number*

database-identification

Indicates the collection database type.

0: Master database (The IP address of the monitoring server is IPv4.)

1: Copy database (The IP address of the monitoring server is IPv4.)

2: Master database (The IP address of the monitoring server is IPv6.)

3: Copy database (The IP address of the monitoring server is IPv6.)

monitoring-manager-name

Indicates the IP address of the monitoring manager that has collected the resources and created the master database.

monitoring-server-name

Indicates the IP address of the monitoring server that is targeted for resource collection.

serial-number

If the monitoring manager name and monitoring server name are duplicated in a copy database, a five-digit serial number (starting from 00001) is automatically appended.

If, for instance, moitoring manager (IP address: `123.45.67.10`) collects the resources of moinitoring server (IP address: `123.45.67.20`), the files having the following names are created:

- Data file: `sso_01230450670101230450670 20.log`
- Information file: `sso_01230450670101230450670 20.inf`
- Instance file: `sso_01230450670101230450670 20.ins`

When the above master database is copied, a copy database that has the following file names is created:

- Data file: `sso_11230450670101230450670 2000001.log`
- Information file: `sso_11230450670101230450670 2000001.inf`
- Instance file: `sso_11230450670101230450670 2000001.ins`

If, for instance, moitoring manager (IP address: `123.45.67.10`) collects the resources of moinitoring server (IP address: `1234:567:89:a::20`), the files having the following names are created:

- Data file: `sso_212304506701012340567008900a0000000000000020.log`
- Information file: `sso_212304506701012340567008900a0000000000000020.inf`
- Instance file: `sso_212304506701012340567008900a0000000000000020.ins`

When the above master database is copied, a copy database that has the following file names is created:

- Data file: `sso_312304506701012340567008900a00000000000000002000001.log`
- Information file: `sso_312304506701012340567008900a00000000000000002000001.inf`
- Instance file: `sso_312304506701012340567008900a00000000000000002000001.ins`

However, if a copy database with serial number 00001 already exists, the copy database is created with serial number 00002.

For details on how to copy a database, see *ssoextractlog* in *5. Commands*.

(c) Collection database size

The size of one entry in the collection database can be calculated by the following formula:

(*subresource count* **x** 31 + 3) **x** *instance count* + *total length of character strings of all instance names* + 12 (bytes)

The data file size of the collection database can be calculated by the following formula:

One-entry size **x** *collection count*

The maximum sizes of the collection databases that SSO can handle are as follows.

Unit	Maximum size
Per data file	Less than 2 gigabytes
Per resource directory	Less than 4 terabytes
Total database capacity	Less than 4 terabytes

The data files in the collection database monotonically increase in size according to the above-described formula. For details on this monotonic increase, see *(e) Collection database maintenance*.

(d) Collection database monitoring

The collection database size monitoring command (`ssodbcheck`) allows you to monitor the collection database size. In situations where the collection database size is monitored, it can be output into a text file, or an event can be issued when the preselected threshold is exceeded. For details on events, see *F. Events*.

(e) Collection database maintenance

Resource collection databases increase in size monotonically. (For the formula for estimating the file size of a collection database, see *(c) Collection database size*.) Partial deletion by using the `ssoextractlog` or `ssodbdel` commands, or partial deletion of data through a dialog box takes time in proportion to the size of the collection database. Therefore, if the collection data is saved periodically, make sure that you periodically delete the collected data (either by deleting all the data or partially deleting the data for a specific period) in order to secure a sufficient amount of free space on the disk.

For how to delete collection data, see *4.5 Resource Data Reference window* and *ssodbdel* in *5. Commands*.

The following is an example of periodically deletion of collection data.

Example:

This example shows how to delete the collection data collected up until the last weekend by executing the following command every weekend:

```
ssodbdel -all -stop BDATE 7
```

Note, however, that if the free space in the file system of the collection database is already insufficient (less than the size of the largest data file in the collection database), you must delete all the data in the collection database. Partial deletion of the data for a specific period is not possible. To check the data file size of the collection database, execute the `ssoextractlog -list` command, and then check *Size* in the information output to the standard output. Alternatively, check *Size (KBytes)* in the collection data list in the Resource Data Reference window.

For details on the `ssoextractlog` command, see *ssoextractlog* in *5. Commands*. For details on the Resource Data Reference window, see *4.5 Resource Data Reference window*.

(4) Browsing collected data

The data stored in the collection database can be browsed. To browse collected data, use the Resource Data Reference window or the command for browsing collected data (`ssoextractlog`).

The collected data can be filtered allowing you to choose whether to view the data collected at a specific time or the data within a specific range. It can also be stored in a file in binary format or CSV format. When the collected data is stored in binary format, the resulting database serves as a copy database.

(5) Deleting collected data

Data stored in the collection database can be deleted. You can delete the entire database by specifying the resource, monitoring manager, or monitoring server, or delete specific data within the database by specifying the data collection time. This deletion process can be executed from the Resource Data Reference window or collection database deletion command (`ssodbdel`).

2.2.3 Threshold monitoring

If you are monitoring resources based on the collection conditions that have been set, you can monitor whether the collected data exceeds given thresholds. If a given threshold is exceeded, an event can be issued or a command can be automatically executed.

(1) Threshold monitoring methods

The following two threshold monitoring methods are available:

- Fixed threshold method

  This method sets and uses a fixed threshold. Use this method for normal system monitoring operation.

  Note that determining a fixed threshold at times such as the start of operation might be difficult. Therefore, for the resources that can be collected by SSO, default values are provided in the threshold definition file. However, these default values are simply reference values and must be optimized if needed.
- Statistical threshold method

This method theoretically calculates threshold values from the standard deviation based on statistics. How much collected data indicating warning or critical is included is specified as the *ratio of data*, treating the actually collected data as the statistical target parameter. The collection data that is the statistics target is specified as *statistical total time*. Since the statistical target parameter changes as the collection progresses, specify the *calculation timing* so that the threshold also changes at a given timing. The current threshold can be checked by using the `ssocolshow` command. You can also calculate the threshold by time zone by dividing the statistical period into time zones. The ID given to each time zone is referred to as *time zone ID*.

For the fixed threshold method, you must consider and set appropriate threshold values. For the statistical threshold method, you must consider and set the ratio of appropriate data. Generally, users can more intuitively understand fixed thresholds than statistical thresholds. Therefore, the fixed threshold method is preferable for the design of a monitoring system.

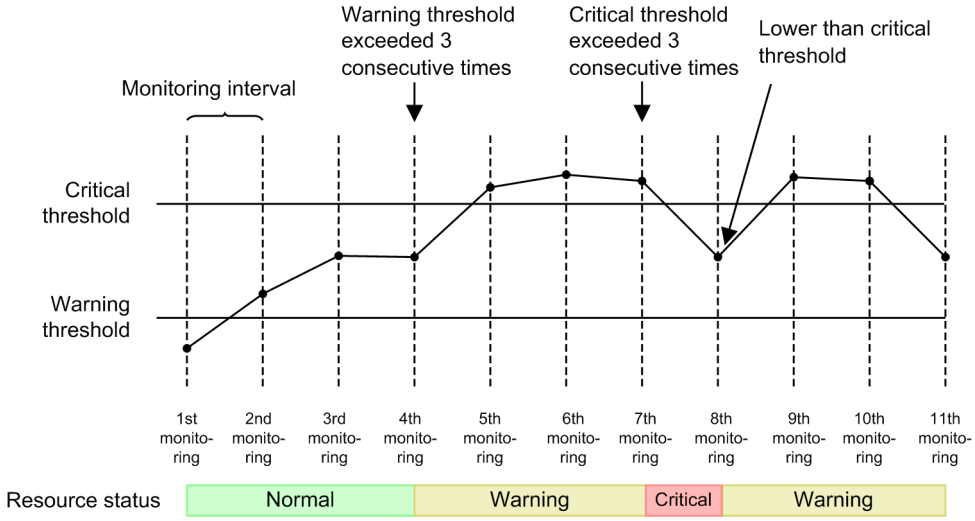
Regardless of the method, to change the threshold according to the time zone, you must link a task scheduler (Windows), cron (UNIX), or a product that has a scheduler function (JP1/AJS3) with the SSO operation commands.

(2) Thresholds and resource statuses

Threshold monitoring of the resource monitoring function can monitor whether the resource collection value exceeds the threshold. You can set a warning threshold and a critical threshold. With these thresholds, you can check the resource status (*Normal*, *Warning*, or *Critical*). Note that there are some resources whose threshold is often exceeded momentarily. In such a case (in the event of a singularity), you can also set a continuous over counter so as not to change the resource status.

The following figure shows the relationship between the thresholds (warning and critical) and the resource statuses. This figure is an example for when the continuous over counters of the warning threshold and the critical threshold are both set to 3.

Figure 2-11: Relationship between threshold and resource status



The following table describes how the resource statuses are judged.

Table 2-4: How resource statuses are judged

Status	How the status is judged
Normal	The resource value is below[#1] the warning threshold value. Alternatively, the number of times the resource value has consecutively gone above[#2] the warning threshold does not exceed the value of the warning-threshold continuous over counter.

Status	How the status is judged
Warning	The number of times the resource value has consecutively gone above[#2] the warning threshold exceeds the value of the warning-threshold continuous over counter, but the conditions for judging the status as *Critical* have not been met.
Critical	The number of times the resource value has consecutively gone above[#2] the critical threshold exceeds the value of the critical-threshold continuous over counter.
Unknown	The collection status has become *Postponing*.
Non-monitoring	• The collection status has become *Completed*, *Impossibility*, or *Standing by*. • The number of monitored instances being collected has decreased.

#1

Below a threshold includes the threshold.

#2

Above a threshold does not include the threshold.

A resource status change event can be issued when the resource status changes. For details on the events, see *F. Events*.

(3) Threshold verification

During initial deployment and the initial stage of operation, it is difficult to determine the optimal fixed thresholds and the ratio of data. Therefore, you might have to revise the thresholds (fixed thresholds or ratio of data). At this time, you can use the actual collection data to check how many times the resource status has changed to *Warning* or *Critical* based on certain values specified as thresholds and continuous over counters. You can specify the current values or any values for the thresholds and continuous over counters. After verification, the specified values can also be used for collection conditions.

(4) Automated action

Actions can also be automatically executed when the resource status changes. An automated action is a function that automatically starts commands that execute operations such as notification to the system administrator and data collection. You can also define variables in these commands. For details on the variables you can define, see *G. Variables That Can Be Defined via Automated Action*. Commands can be executed by *superuser* in UNIX or by *Administrator* in Windows.

(5) Notes

(a) Automated actions in Windows

To execute a batch file on Windows, add `cmd /q /c` at the beginning of the command line. For example, to execute `C:\temp\aaa.bat`, specify `cmd /q /c C:\temp\aaa.bat`.

(b) Execution of an automated action at ssocolmng daemon process startup

An automated action is executed as indicated in the following table according to the resource status at `ssocolmng` daemon process startup.

Resource status at ssocolmng daemon process startup	Resource status for which an automated action is set
normal	normal
warning	warning
critical	critical

(c) Notes on statistical thresholds

In statistical threshold monitoring, the threshold becomes 0 in the following cases:

- When initial value calculation is not performed
- When collection data required for obtaining the statistical threshold does not exist during initial value calculation or regular calculation

2.2.4 Cautionary notes on the resource monitoring function

Resource values that are displayed or output:

For the following functions, depending on the resource, the decimal places `.00` might be added to resource values that are displayed or output even when the resource values are integers:

Command:

- `ssoextractlog -text`

Resource Browser window:

- Summary Data window
- Performance Data window
- Files storing regular queries

Resource Data Reference window:

- Listing Display window
- Files storing collected data

Report:

- All report files#

Incident cooperation:

- Custom incident attribute (resource-value)
- Resource status change event
- Incident View Range Specification window
- Incident graph window

#:

In report files, the decimal places `.00` are unconditionally added to any integer resource values.

2.3 User resource monitoring function

The user resource monitoring function allows you to add resources. You can execute collection and browsing of these resources in the same way as for already provided resources (that have the category name of SSO). This section describes the user resource monitoring function of SSO.

2.3.1 User resources that can be defined

You can define the following as company resources: company-specific MIB objects, that are implemented by another vendor's SNMP agent, and user-specific MIB objects, that are created by using the user extension MIB definition function of the ESA The following table lists the types of MIB objects that can be collected as user resources.

Table 2-5: Types of collectable MIB objects

MIB object type	Range of MIB values settable for user resources	Object type defined in user resources	Resource values of user resources
INTEGER	Integer from -2,147,483,648 to 2,147,483,647	Integer	Collected MIB value
Integer32			
Gauge	Integer from 0 to 4,294,967,295	Gauge (or Counter#1)	If the object type is defined as Counter: Difference between the previously collected MIB value and the currently collected MIB value If the object type is defined as Gauge: Collected MIB value
Gauge32			
Unsigned32			
CounterBasedGauge64	Integer from 0 to 18,446,744,073,709,551,615		
TimeTicks	Integer from 0 to 4,294,967,29	Counter (or Gauge#2)	
Counter			
Counter32			
Counter64	Integer from 0 to 18,446,744,073,709,551,615		
OCTET STRING	Printable ASCII character string whose length is from 0 to 255 bytes	String	Collected MIB value
DisplayString			

#1

In contrast with the MIB object type definition, the MIB value might substantially have the nature of the Counter type (a cumulative value that increases under certain conditions, and whose increase per unit of time is meaningful). In this case, make sure that you define Counter as the object type in user resources.

#2

If the MIB value substantially has the nature of the Gauge type (for which an absolute value is meaningful) in contrast with the MIB object type definition, make sure that you define Gauge as the object type in user resources.

You can incorporate multiple MIB objects to be obtained and then use the resulting calculation value as the user resource value. In this case, the possible resource value is a real number from -18,446,744,073,709,552,000 to 18,446,744,073,709,552,000.

2.3.2 User resource definition

Define the names of user resources, MIB objects to be collected, and calculation formulas in the user resource definition file. For details on the user resource definition file, see *6.3.14 User resource definition file*. Up to 10,000 user resources can be defined. Up to 32 subresources can be defined per resource. However, if there are multiple user resource configuration files, a maximum of 10,000 user resources in total can be defined in all the user resource configuration files.

After you create the user resource definition file, execute the user resource definition command (`ssocolconf`). When the `ssocolconf` command is executed, the user resource definition file is loaded into JP1/Cm2/SSO to create a user resource setup file. To set user resources on JP1/Cm2/SSO running on remote hosts or to browse collected data, distribute the user resource setup file to each host. Store the user resource definition file in the following directory:

```
In UNIX: $SSO_CONF/rsc/user*#
In Windows: $SSO_CONF\sso\rsc\user*#
```

#

The string `user*` indicates a user resource configuration file name that begins with `user` and has 32 or fewer bytes. Alphanumeric characters and hyphens (-) can be used. A user resource configuration file name is a character string where the category name set in the resource definition file has been converted to lowercase.

The procedures for creating, deleting, and changing user resource definitions are described below.

(1) Adding a definition

To create a new user resource configuration file, or to re-create a user resource configuration file by adding definitions on a per-resource basis, use the following procedure:

1. Create a new or edit an existing user resource definition file.

   We do not recommend that you create the user resource definition file under the SSO installation directory. In particular, do not create the file under the `$SSO_CONF/rsc` (in UNIX) or `$SSO_CONF\sso\rsc` (in Windows) directory, which contains the user resource configuration file. If that directory contains a file other than the user resource configuration file (for example, a user resource definition file or a work file), the `ssocolmng` daemon process might unduly monopolize the CPU or consume memory.
2. If the Resource Configuration window or the Resource Data Reference window is open, close it.
3. Create or re-create a new user resource configuration file by using the `ssocolconf` command.
4. Restart the `ssocollectd`, `ssocolmng`, and `ssorptd` daemon processes.

(2) Deleting a definition

If a definition is deleted, the existing collection data of the relevant user resources can no longer be referenced by using the `ssoextractlog` command or the Resource Data Reference window. If necessary, use the `ssoextractlog` command to extract that definition in text format, and then save the extracted data in a file.

To delete a user resource definition:

1. Stop the collection of all target user resources by using the `ssocolstop` command or the Resource Configuration window.
2. If necessary, use the `ssoextractlog` command (with the `-text` and `-savefile` options specified) to extract the existing collection data of the target user resources in text format.

3. Delete all the collection data of the target resource by using the `ssodbdel` command or the Resource Data Reference window.
4. Delete all the collection condition definitions of the target user resource by using the `ssocolset` command or the Resource Configuration window.
5. If the Resource Configuration window or the Resource Data Reference window is open, close it.
6. If you want to delete only some resources, re-create the user resource configuration file by using the `ssocolconf` command. If you delete a user resource configuration file, you must also delete the corresponding user resource configuration file.
7. Restart the `ssocollectd`, `ssocolmng`, and `ssorptd` daemon processes.

(3) Changing a definition

The procedure to change a user resource definition differs depending on the condition. The following shows the procedure for each condition.

Condition 1: When performing either of the following operations within the resource definitions of the same English resource name (`rsc_label_e` key value):

- Changing a resource ID (`rsc_id` key value).
- Deleting some definitions related to existing subresources (`subrsc_label_j`, `subrsc_label_e`, and `subrsc_mib_data` keys).

Before changing user resource definitions, you must delete all the existing collection data of those user resources as well as the resource configuration. If necessary, use the `ssoextractlog` command to extract the existing collection data in text format and save it as a file.

Execute the same procedure as that described in *(2) Deleting a definition*.

Condition 2: When changing the English resource name (`rsc_label_e` key value) within resource definitions that have the same resource ID (`rsc_id` key value):

Note that after changing user resource definitions, you cannot view the existing collection data of those user resources in the Resource Data Reference window.

If necessary, use the `ssoextractlog` command to extract the existing collection data in binary format or text format and save it as a file.

The procedure for changing user resource definitions is as follows:

1. Stop the collection of all target user resources by using the `ssocolstop` command or the Resource Configuration window.
2. If necessary, use the `ssoextractlog` command to extract the existing collection data of the target user resources and save it as a file.
   - To save the collection data in binary format

     Execute the `ssoextractlog` command with the `-bin` and `-savefile` options specified.

     You cannot view the data from the Resource Data Reference window, but you can view the data by using the `ssoextractlog` command with the `-text` and `-logfile` options specified.
   - To save the collection data in text format

     Execute the `ssoextractlog` command with the `-text` and `-savefile` options specified.
3. Delete all the collection data of the target user resources by using the `ssodbdel` command or the Resource Data Reference window.

4. Delete all the collection conditions definitions of the target resources by using the `ssocolset` command or the Resource Configuration window.
5. If the Resource Configuration window or the Resource Data Reference window is open, close it.
6. Use the `ssocolconf` command to re-create the user resource configuration file.
7. Restart the `ssocollectd`, `ssocolmng`, and `ssorptd` daemon processes.

Condition 3: When neither of the above conditions applies:

Execute the same procedure as that described in *(1) Adding a definition*.

2.3.3 User resource icon

You can allocate any icon to a user resource to be displayed in the windows of JP1/Cm2/SSO. To allocate an icon, create a resource-icon definition file. If no resource-icon definition file is created, the default icon is displayed instead. For details, see *6.3.15 Resource-icon definition file*.

2.3.4 Precautions

The following explains the precautions to be noted when user resources were defined.

(1) Collecting resources

- If user resources cannot be collected from a target server during resource collection, the resulting resource collection status is `Postponing`.
- If the calculation formula for the resource value of user resources includes division by 0, the resulting resource value is 0.

(2) Storing collected data

SSO creates a collection database in accordance with the resource group name and resource name written in the user resource definition file.

(3) Location of user resource definition files

Do not save user resource definition files in the `$SSO_RSC` directory, which is used to save only user resource configuration files.

(4) Resource value

User resource values displayed or output by the functions listed below are rounded to the second decimal place. If the user resource value is an integer, the decimal places `.00` are added.

Command:

- `ssoextractlog -text`

Resource Browser window:

- Summary Data window
- Performance Data window

- Files storing regular queries

Resource Data Reference window:

- Listing Display window
- Files storing collected data

Report:

- All report files

Incident cooperation (action cooperation):

- Custom incident attribute (resource-value)
- Resource status change event
- Incident View Range Specification window
- Incident graph window

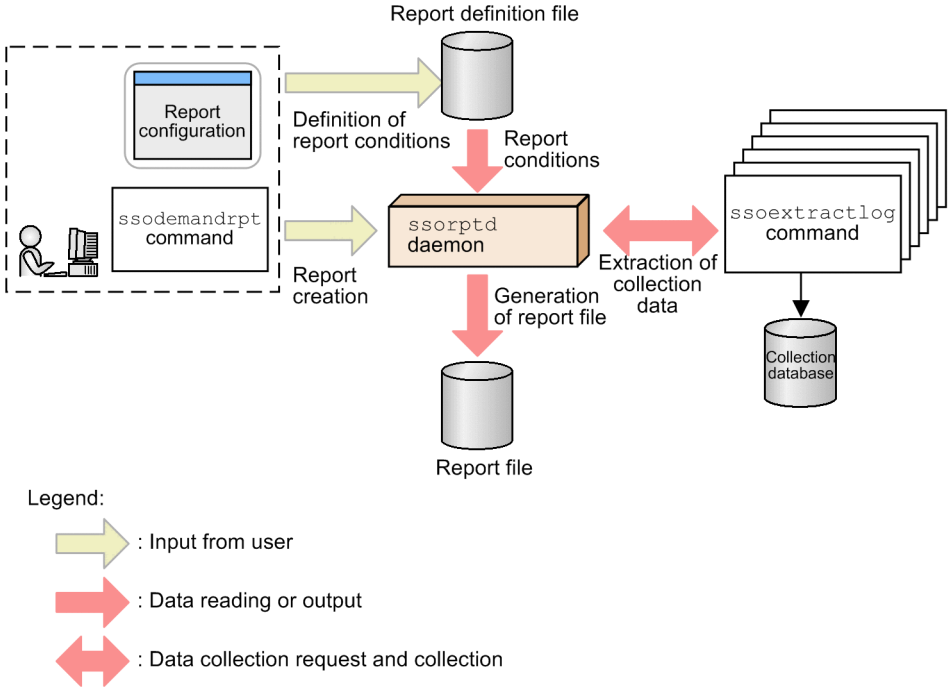
2.4 Report function

The report function is used to create reports, according to specific report conditions, on collection data saved in the database, and to display created reports. This section describes the report function.

2.4.1 Creating reports

Before you can create reports, you must either define the report conditions in the Report Configuration window, or create a report definition file. You can then create a report by using either the Report Configuration window or the `ssodemandrpt` command. When report creation starts, collection data is extracted by executing the `ssoextractlog` command for each report condition in the report definition file, and a report file in CSV format or HTML format is created. The following figure shows an overview of report creation.

Figure 2-12: Overview of report creation



(1) Report file formats

There are two report file formats: the CSV format and the HTML format. In CSV-format reports, the maximum value, minimum value, and average can be output.

HTML-format reports can be output in table format or graph format. In table-format reports, the maximum value, minimum value, and average of the resource collection data within the specified period are output.

In graph-format reports, a graph and its introductory notes are output. You can select one of the following graph types:

- Line graph
- Histogram
- Bar graph
- Stacked bar graph
- Pie chart

When you output a report in HTML format, you can select either the VML or SVG standard. Note, however, that for the graph format, these standards are not always compatible with all web browsers. The following table lists the compatibility between standards and web browsers.

Table 2-6: Compatibility between standards and web browsers

Standard	Web browser	
	IE	Firefox
VML	*	N
SVG	*	Y

Legend:

Y: Compatible

*: Whether the standard is compatible depends on the version of IE. For details on which standards are compatible, check the IE specifications.

N: Not compatible

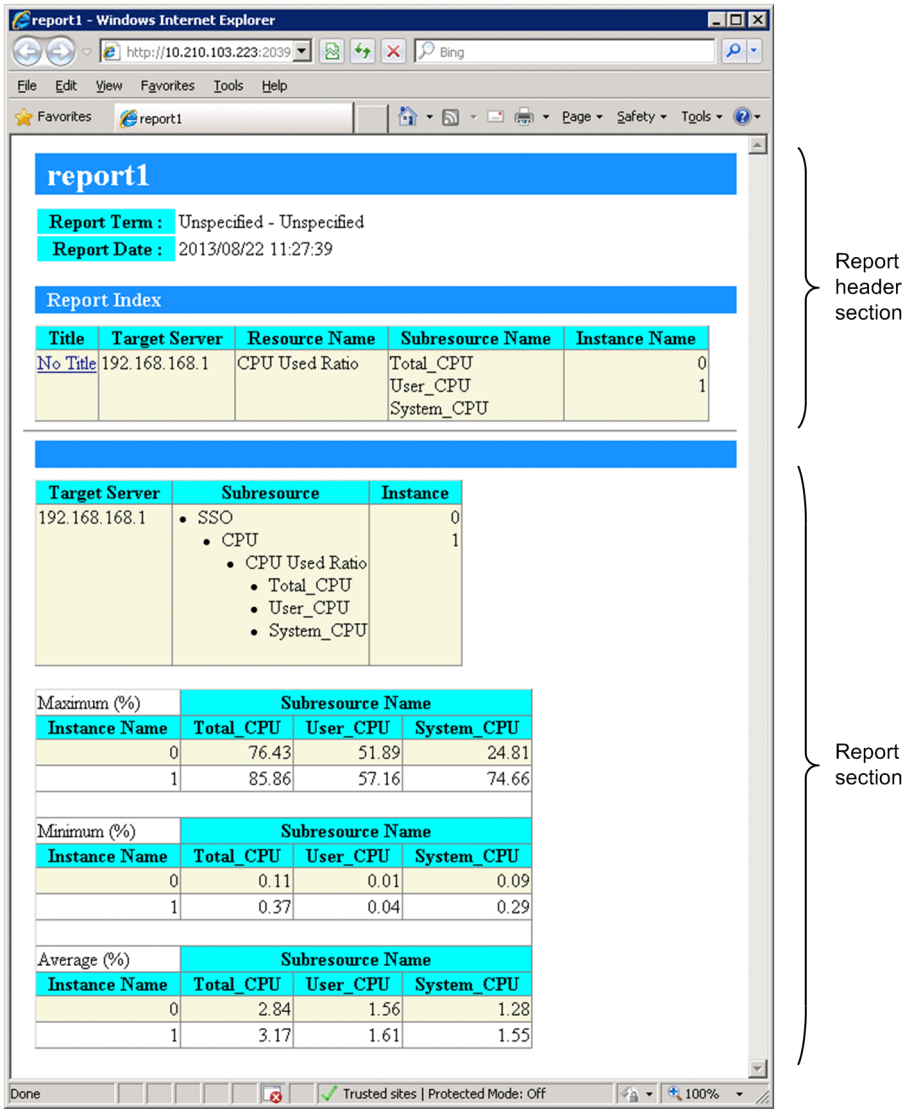
Reference note

Report files created with SSO 10-00 or earlier are in the VML standard. The displayed report looks the same whether the VLM or the SVG standard is used.

(2) Configuration of report files

JP1/Cm2/SSO creates a collection database in accordance with the resource group name and resource name written in the user resource definition file. The following figure shows an example of the report file configuration.

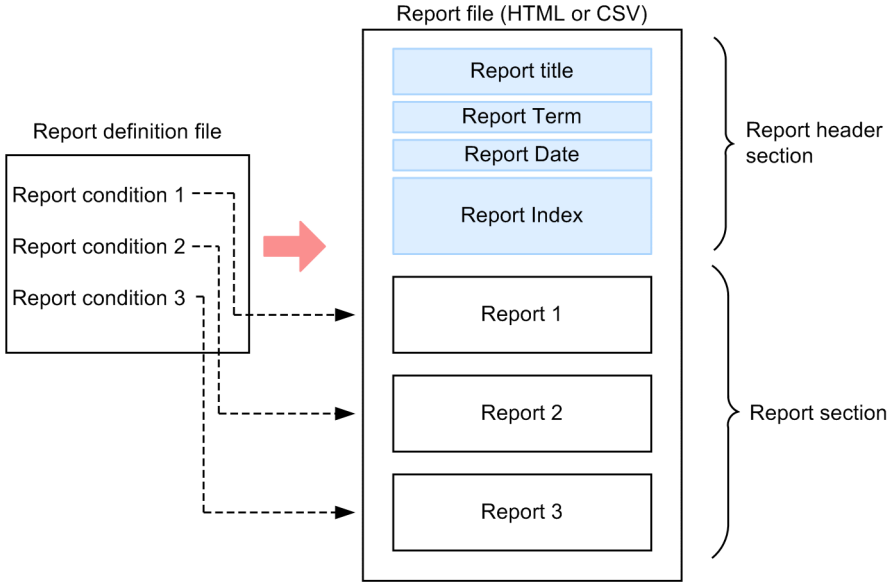
Figure 2-13: Example of the report file configuration



If the report file is in HTML format, you can view the desired report by clicking the index.

If you want to create a report file, define the report conditions in the report definition file. Report conditions define the collected data to be output to the report and the format for displaying the report. The following figure illustrates the relationship between the report definition file and the report file.

Figure 2-14: Relationship between the report definition file and the report file



SSO creates one report file from one report definition file. Since you can define multiple report conditions in the report definition file, you can display reports of multiple servers and resources in a single report file.

You can set the report target, report term, report format and other parameters from the web browser.

In CSV-format reports, the maximum value, minimum value, and average of the resource collection data within the specified period are output.

HTML-format reports can be output in either graph format or table format.

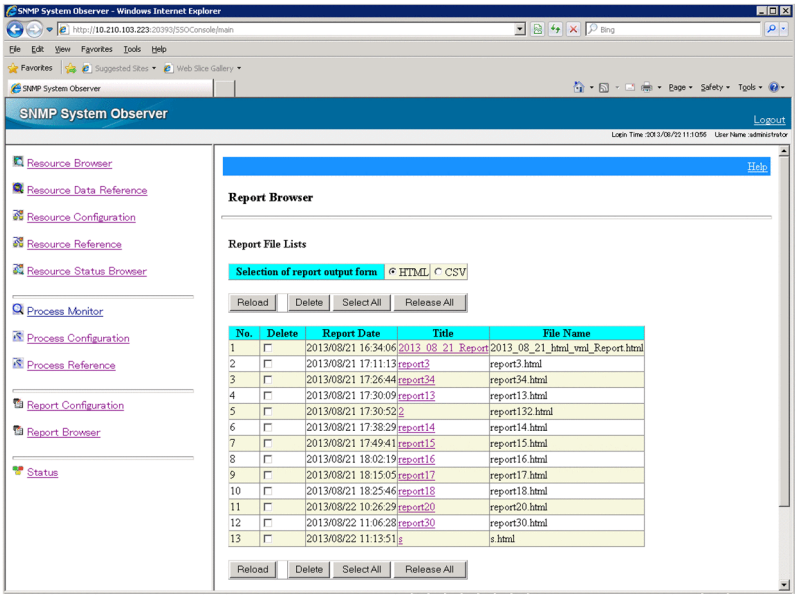
- Table-format report: Maximum value, minimum value, and average of the resource collection data within the specified period
- Graph-format report: Graph introductory notes and graph

2.4.2 Displaying reports

To display a report, in the report file list displayed by format (CSV or HTML), select the report file to be displayed. The report file list is displayed in the view frame that appears when you log in to the SSO console and select **Report Browser** in the menu frame of the SSO console.

The following figure shows an example of the report file list.

Figure 2－15: Example of the report file list



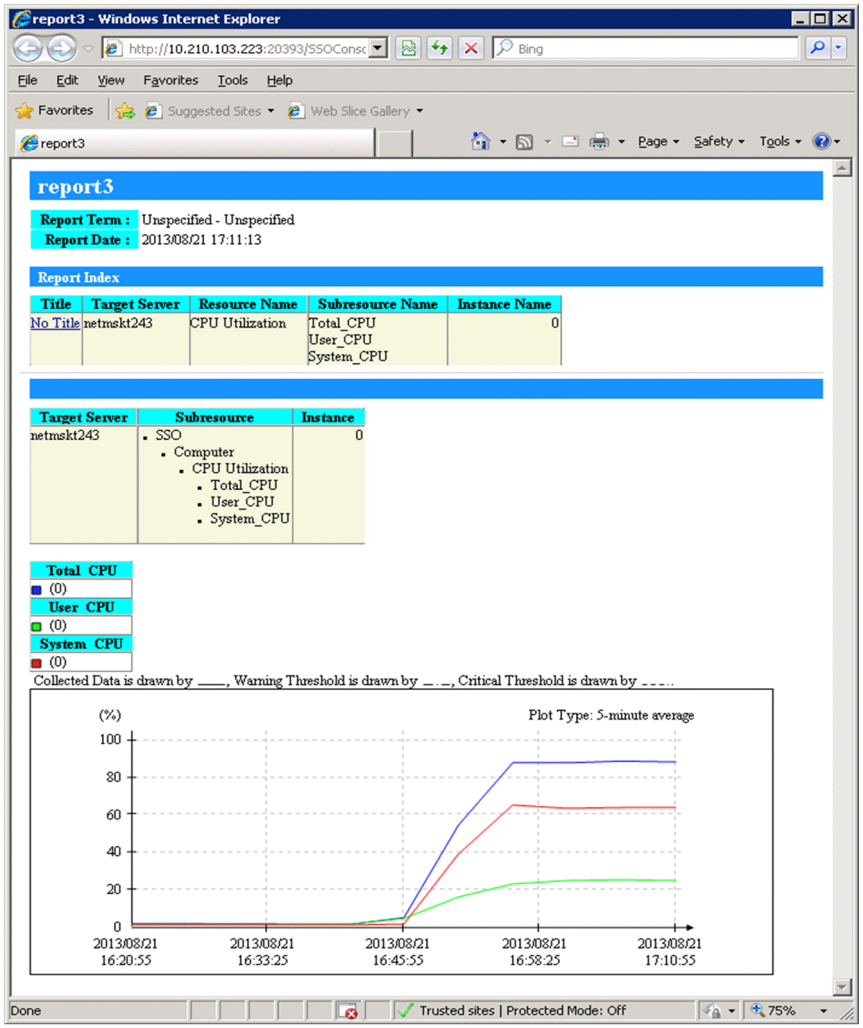
(1) CSV-format report files

CSV-format report files can be displayed with a text editor or spreadsheet software.

(2) HTML-format report files

HTML-format report files can be displayed with a web browser. The following figure shows an example of an HTML-format report file displayed with a web browser.

Figure 2-16: Example of an HTML-format report file displayed with a web browser



Note

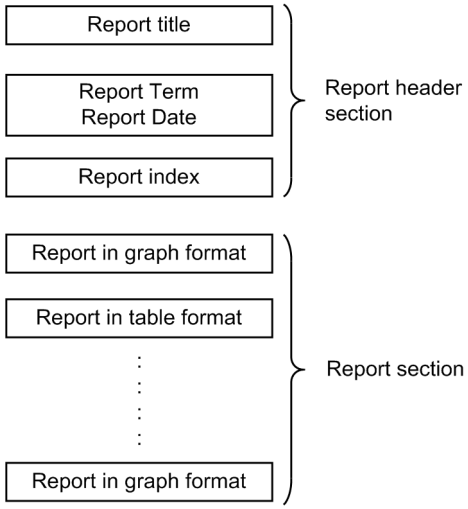
The display of text in graphs depends on the font settings of the web browser. Depending on the font settings, text might extend beyond the graph, overlap, or be partly missing. In such a case, change the font settings of the web browser.

2.4.3 Details of HTML-format report files

This subsection describes the HTML-format report files created with the report creation function. You can save HTML-format report files to a directory of your choosing. However, if you want to display HTML-format report files with Report Browser, you must save these files in an HTML database.

Each HTML-format report file consists of a report header section and a report section. The following figure shows the structure of an HTML-format report file.

Figure 2-17: Structure of an HTML-format report file



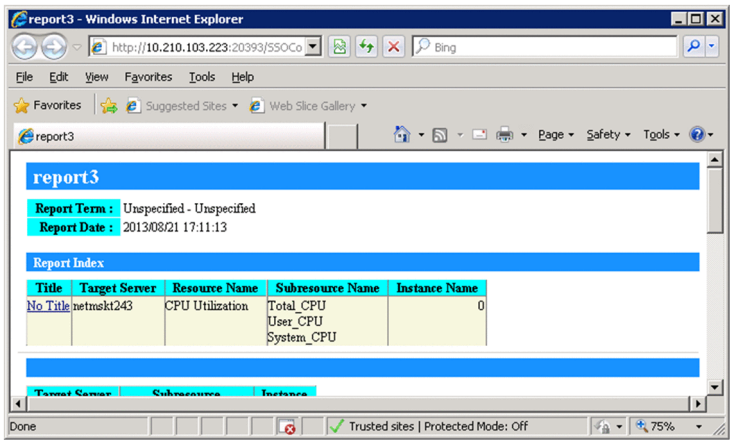
The following table lists the display forms of instance names in HTML-format report files.

Instance name by resource	Instance name order	Alignment
All numeric values	Sorted in ascending order as numeric values	Right-aligned
Other than the above	Sorted in ascending order as strings	Left-aligned

(1) Report header section

The report header section displays the report title, report term, report date, and report index. The following figure shows an example of the report header section.

Figure 2-18: Report header section of an HTML-format report file



Report title

The report title specified during report creation is displayed.

Report Term

The report term specified during report creation is displayed.

Report Date

The date on which report creation was executed by using the Report Configuration window or report command is displayed.

Report Index

The indexes of graphs and tables displayed in the report section are listed. The list displays all the subresources and instances on which the report was created. To move to the actual graph or table, click the name of the server targeted for collection.

(2) Report section

Report sections can have the following formats (graph formats and a table format):

1. Line graph format
2. Histogram format
3. Bar graph format
4. Stacked bar graph format
5. Pie chart format
6. Table format

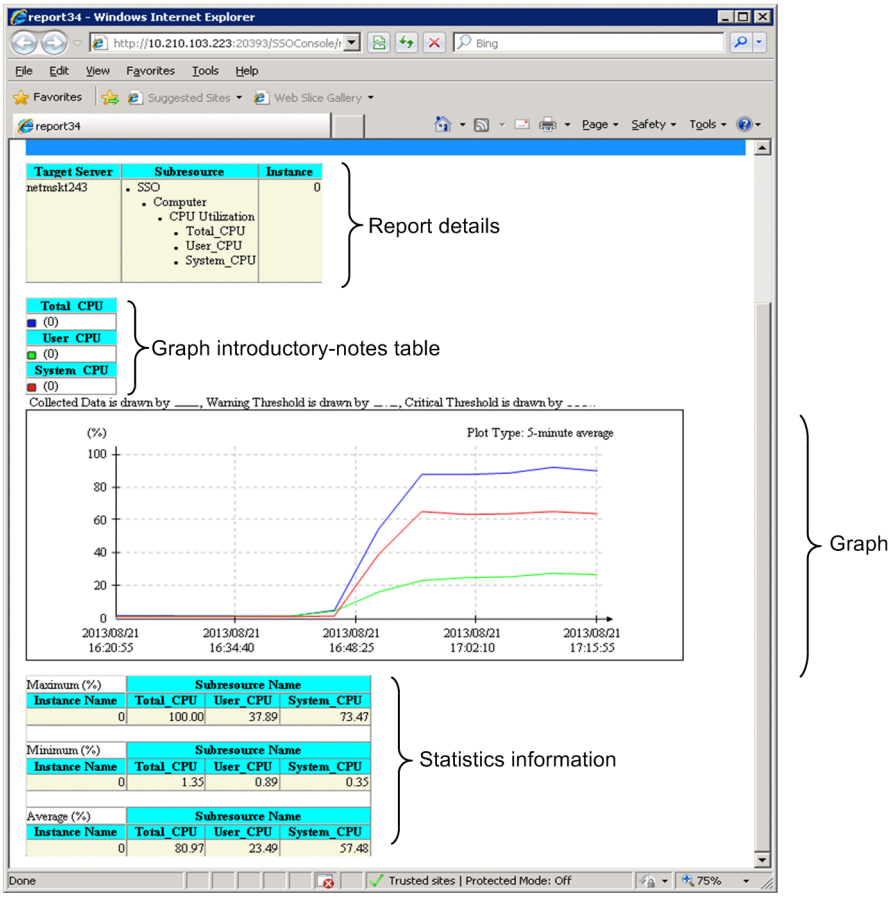
   The table format can further be categorized into the following four formats:

   - Subresource columns - Instance rows
   - Instance columns - Subresource rows
   - According to instance
   - According to subresource

2.4.4 Report files in line graph format

The report section of a report in line graph format displays the report details, the graph, and the graph introductory notes table. You can also specify settings to display multiple lines in a graph. The following figure shows an example of a report file in line graph format.

Figure 2－19: HTML-format report file (line graph format)



The following subsections describe the contents displayed in report files.

(1) Report details

This area displays the collection target server name, subresource names, and instance names.

(2) Graph introductory-notes table

As the introductory notes to the lines in a graph, the graph line colors, subresource names, and instance names are displayed. A graph introductory-notes table can be displayed in two formats: the instance count-based format and the subresource-based format.

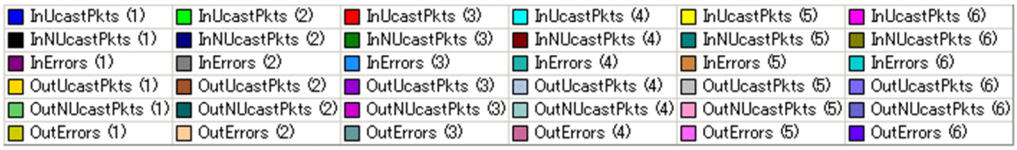
(a) Instance count-based format

In a table in this format, each introductory note is output in the *subresource-name* (*instance-name*) format for each graph line color.

Introductory-notes tables in this format are output if **It turns up and displays** is cleared in the Graph Detail Setup window, or if the `graph_legend_row` key (or its value) is omitted from the report definition file.

The columns of a table in instance count-based format are sorted by the number of instances. You cannot specify the number of columns. The following figure shows an example of a graph introductory-notes table in instance count-based format.

Figure 2-20: Graph introductory-notes table in instance count-based format



(b) Subresource-based format

In a table in this format, the introductory notes on the graph lines are grouped by subresource. A note is output in (*number-of-instances*) format for each graph line color. Introductory-notes tables in this format are output if **It turns up and displays** is selected in the Graph Detail Setup window, or if a value is set for the `graph_legend_row` key in the report definition file.

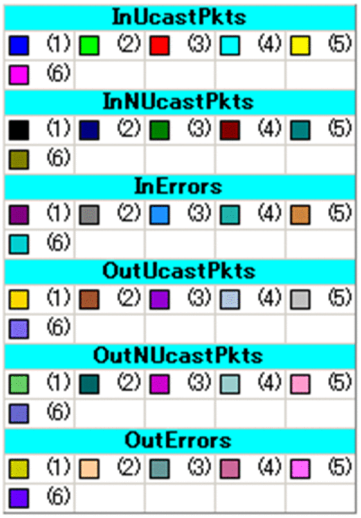
For the subresource-based format, columns are created according to the number of instances. You can also specify the number of columns.

If the specified number of columns is greater than needed, only the necessary columns are created. By default, when a report is created, the subresource-based format is used and the maximum number of columns is set to 10.

For details about the **It turns up and displays** checkbox on the Graph Detail Setup window, see *4.9.5(1) Graph Detail Setup window*. For details about the `raph_legend_row key` of the Report definition file, see *6.3.21(3) Details of the report conditions definition*.

The following figure shows an example of a graph introductory-notes table in subresource-based format. In this example, the maximum number of columns is set to 5 when there are 6 instances for each subresource.

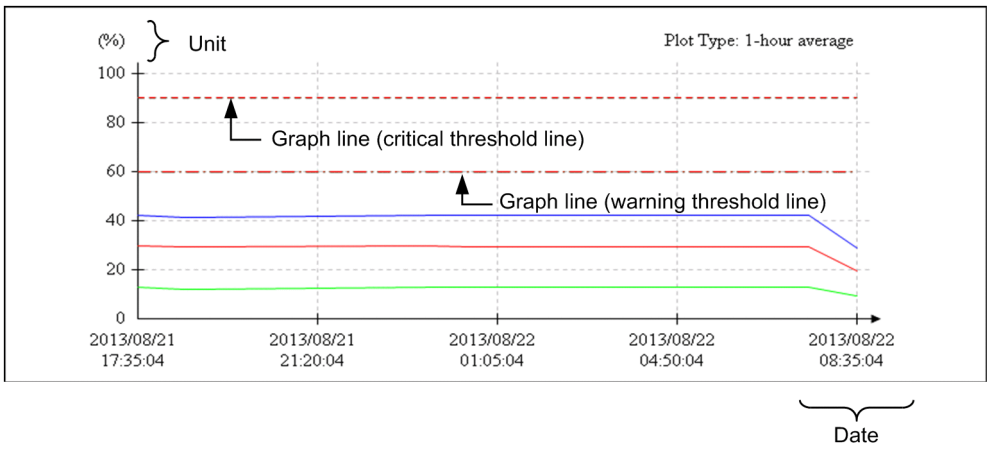
Figure 2-21: Graph introductory-notes table in subresource-based format



(3) Graph

Each graph consists of a graph frame, graph lines, units, plot type, line-type introductory notes, and dates. The following figure shows a graph output example.

Figure 2-22: Graph output example (line-graph format)



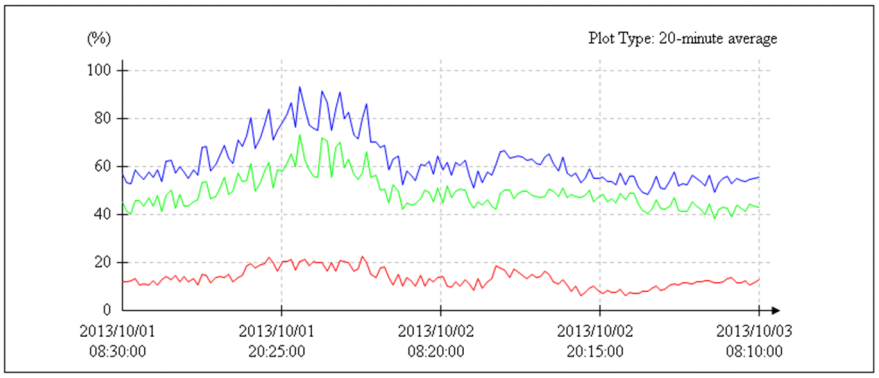
(a) Graph frame

- The vertical axis indicates the value, and the horizontal axis indicates the time.
- Values of up to 6 digits can be displayed as the scale values for the vertical axis.
- For a graph in which the scale values on the vertical axis exceed 1,000,000, you can select whether the values are displayed with exponents or displayed with integers or decimal numbers. You can specify the display format in the `exponential-notation` key of the `ssorptd` action definition file. For details on the `exponential-notation` key, see *6.3.22 ssorptd action definition file (ssorptd.def)*.
- You can select which period will be used to determine the start and end times of the graph time axis, the period within the report term for which collection data exists, or the data extraction period. The details are shown below.

  If the period within the report term for which collection data exists is selected:

  The times of the first and last plot points within the data extraction period specified by using the Creating of Report File window or the `ssodemandrpt` command become the start time and the end time. This period is used by default. The following figure shows an example of a graph displayed when the period within the report term for which collection data exists is selected.

  Figure 2-23: Example of a graph displayed when the period within the report term for which collection data exists is selected



  Collection data and plot point conditions used in the above example:

  Data extraction period: From 00:00:00 on October 1, 2013 to 00:00:00 on October 4, 2013

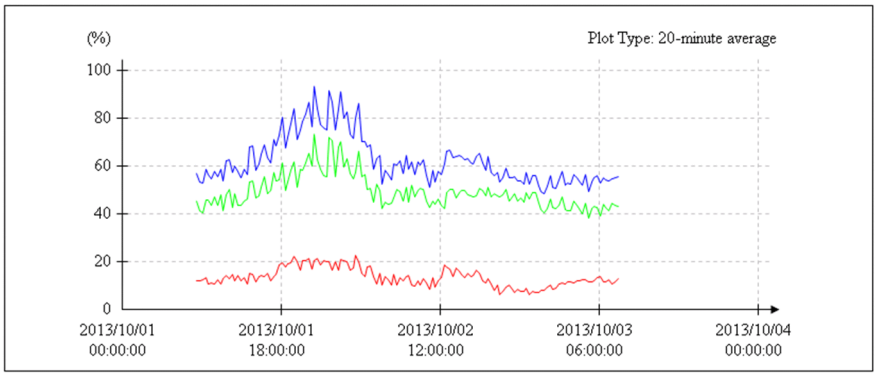
  Plot points: From 08:30:00 on October 1, 2013 to 08:10:00 on October 3, 2013

  If the data extraction period is selected:

  The data extraction period specified by using the Creating of Report File window or the `ssodemandrpt` command is used to determine the start and end times.

If the start time is omitted, the time at the first plot point is used as the start time. If the end time is omitted, the time at the last plot point is used as the end time. The following figure shows an example of a graph displayed when the data extraction period is selected.

Figure 2-24: Example of a graph displayed when the data extraction period is selected



Collection data and plot point conditions used in the above example:

Data extraction period: From 00:00:00 on October 1, 2013 to 00:00:00 on October 4, 2013

Plot points: From 08:30:00 on October 1, 2013 to 08:10:00 on October 3, 2013

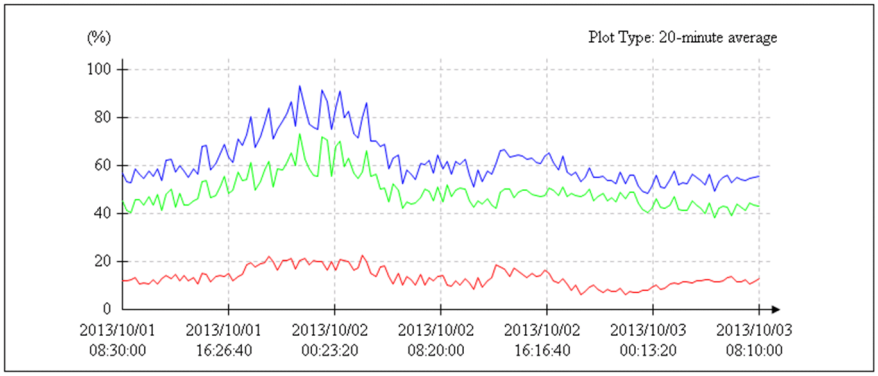
The data extraction period can be specified in either the **Time-axis** in the Graph Detail Setup window or the `graph_time_adjust` key in the report definition file. For details on the **Time-axis**, see *4.9.5(1) Graph Detail Setup window*. For details on the `graph_time_adjust` key, see *6.3.21(3) Details of the report conditions definition*.

- You can select either of the following methods to scale the graph time axis:

Specifying the number of divisions:

You can specify 1 to 60 as the number of divisions. However, if you specify a value larger than 50, the displayed time strings overlap. The following figure shows an example of a time axis that is scaled by the number of divisions of the time axis. In this example, 6 is specified as the number of divisions.

Figure 2-25: Example of the time axis scaled by the number of divisions



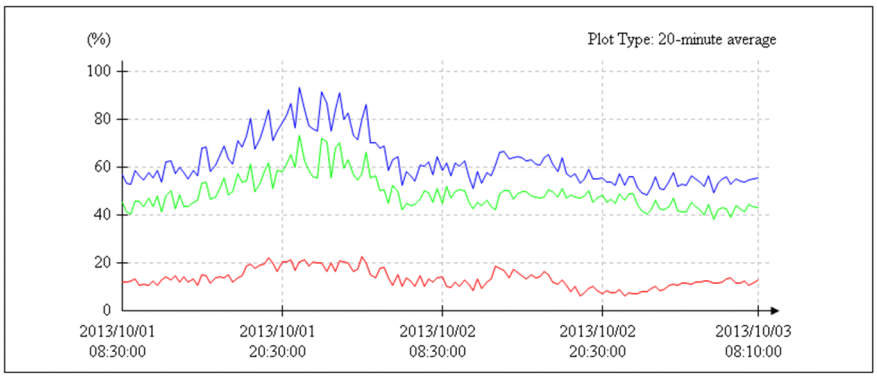
Specifying the time interval:

You can specify from 1 minute to 365 days as the time interval. The time axis of a graph is scaled at the specified interval from the start time on the axis.

If you specify a short interval that divides the time axis into more than 50, the displayed time strings overlap.

The time interval can be specified in either **Scale Line** in the Graph Detail Setup window or the `graph_xdivide` key in the report definition file. For details on **Scale Line**, see *4.9.5(1) Graph Detail Setup window*, and for details on the graph_xdivide key, see *6.3.21(3) Details of the report conditions definition*. The following figure shows an example of a time axis that is scaled by time interval.

Figure 2-26: Example of a time axis scaled by time interval



Display interval and plot point conditions used in the above example:

Display interval: 12-hour intervals

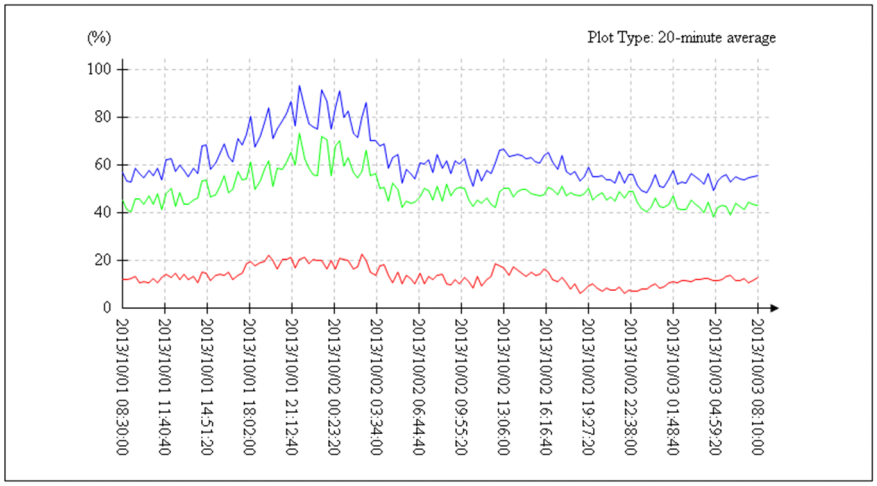
Plot points: From 08:30:00 on October 1, 2013 to 08:10:00 on October 3, 2013

- The dates are rotated by 90 degrees in the following cases:

If 7 or a larger value is specified as the number of divisions:

The following figure shows an example of the time axis displayed when 7 or a larger value is specified as the number of divisions. In this example, the dates are rotated by 90 degrees because 15 is specified as the number of divisions.

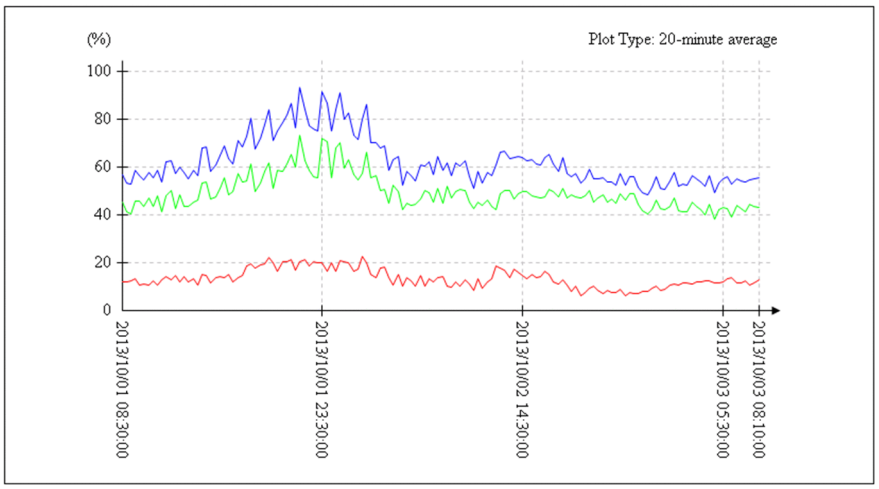
Figure 2-27: Example of the time axis displayed when 7 or a larger value is specified as the number of divisions



If the time axis is scaled by the time interval and the last scale point is too close to the end time:

The following figure shows an example of a graph whose time axis is scaled by time interval. The time axis is scaled at 15-hour intervals when plot points are created from 08:30:00 on October 1, 2013 to 08:10:00 on October 3, 2013. Because the third scale point and the end time of the graph time axis are close to each other, 90-degree rotation is employed.

Figure 2-28: Example of the time axis scaled by time interval



(b) Graph lines

There are three types of graph lines, collection data lines, warning threshold lines, and critical threshold lines. For details on each type of graph line, see *(e) Introductory notes on line types*.

Collection data lines

A maximum of 100 collection data lines can be drawn in one graph. The number of lines can be calculated as *number-of-subresources* **x** *number-of-instances*. Lines are drawn in ascending order of instance number for each subresource. However, if *number-of-subresources* **x** *number-of-instances* exceeds 100, then only the first 100 lines are drawn.

Table 2-7 shows instances for which the lines will not be drawn if *number-of-subresources* **x** *number-of-instances* exceeds 100 under a certain condition. In this table, there are 9 subresources, and each subresource has 13 instances. In this case, the lines for all instances of subresources 1 to 7 are drawn. For subresource 8, lines are drawn for instances 1 to 9, but not for instances 10 to 13. Lines are not drawn for instance numbers 10 and higher of subresource ID8, or for any instances of subresource 9.

Table 2-7: Instances for which lines will not be drawn if number-of-subresources **x** number-of-instances exceeds 100 (in the case of a resource consisting of 9 subresources, each of which has 13 instances)

Subresource ID	Instance number	Accumulated number of collection data lines
1	1	1
	2	2
	:	:
	13	13
2	1	14
	2	15
	:	:
	13	26
:	:	:
8	1	92
	2	93

Subresource ID	Instance number	Accumulated number of collection data lines
8	:	:
	9	100
	10	*Not drawn*
	:	:
	13	*Not drawn*
9	*1*	*Not drawn*
	:	:
	13	*Not drawn*

Within the specified extraction period, the average is obtained for the data in each interval that is specified as a plot type, and collection data lines are drawn for those intervals. If no data is extracted in an interval, you can select whether to draw lines for that interval. Figure 2-29 shows an example of a graph when lines are drawn for an interval in which no data was extracted. Figure 2-30 shows an example of a graph when no lines are drawn for an interval in which no data was extracted.

Figure 2-29: Example of a graph when part of the data was not extracted during extraction at the time intervals specified as a plot type (lines are drawn for missing data)

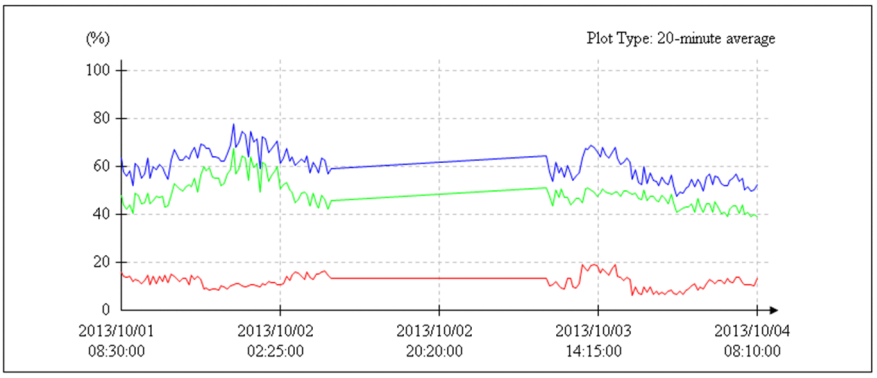
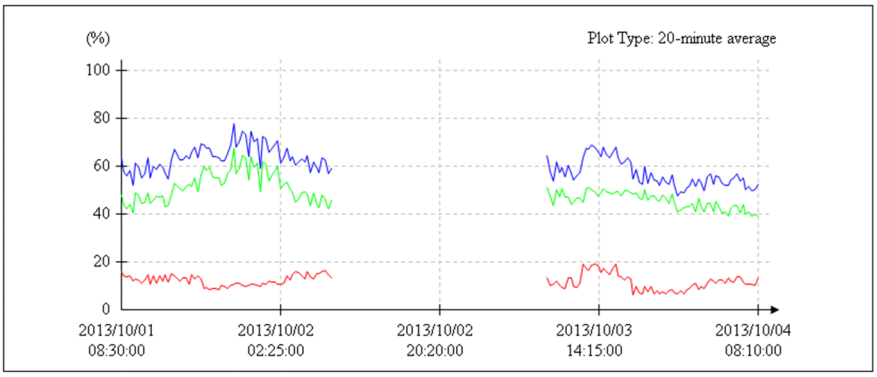


Figure 2-30: Example of a graph when part of the data was not extracted during extraction at the time intervals specified as a plot type (lines are not drawn for missing data)



Whether to draw lines for missing data can be specified in **Graph Line** in the Graph Detail Setup window or the `graph_blank` key in the report definition file. For details on **Graph Line**, see *4.9.5(1) Graph Detail Setup window*, and for details on the `graph_blank` key, see *6.3.21(3) Details of the report conditions definition*.

Graph lines can be associated with subresources and instances by using the graph line color and graph introductory notes. When you position the mouse pointer over a collection data line, the names of the subresource and instance

associated with that line are displayed in a tooltip. In the tooltip, these names are displayed in the *subresource-name* (*instance-name*) format. The tooltips for collection data lines can be displayed only for lines that are displayed.

If multiple collection data lines overlap, the line drawn last takes precedence over other lines.

Warning threshold lines

- Warning threshold lines are drawn if **Warning Threshold** is selected in **The display of Threshold** in the Threshold Line Detail Setup window. Warning threshold lines are also drawn if **It displays by setup of every Subresource** is selected under **Threshold Line**, or **Warning threshold** or **Warning and critical thresholds** is selected under **Threshold Line** in the Graph Detail Setup window. You can also set the drawing of warning threshold lines in the `graph_threshold` key in the report definition file. For details on the Threshold Line Detail Setup window, see *4.9.4(2) Threshold Line Detail Setup window*. For details on the Graph Detail Setup window, see *4.9.5(1) Graph Detail Setup window*. For details on the `graph_threshold` key, see *6.3.21(3) Details of the report conditions definition*.

  Note that even if drawing of warning threshold lines is set, warning thresholds are not output unless the corresponding collection data lines are output.
- By default, warning threshold lines are not drawn.
- Warning threshold lines are drawn as dashed lines.
- Warning threshold lines are drawn in the same colors as those of the target collection data lines.
- You can specify whether to draw a warning threshold line for each subresource.
- While a warning threshold line is being drawn, if the threshold changes, the variation is applied to the drawing.
- If multiple lines overlap, the threshold that is drawn last is displayed.
- The subresource and instance names are displayed in a tooltip in the *subresource-name* (*instance-name*) format. Tooltips can be displayed only for lines that are displayed.

Critical threshold lines

- Critical threshold lines are drawn if **Critical Threshold** is selected in **The display of Threshold** in the Threshold Line Detail Setup window, or if **Threshold Line** is selected in the Graph Detail Setup window. Drawing of critical threshold lines can also be set in the `graph_threshold` key in the report definition file. For details on the Threshold Line Detail Setup window, see *4.9.4(2) Threshold Line Detail Setup window*. For details on the Graph Detail Setup window, see *4.9.5(1) Graph Detail Setup window*. For details on the `graph_threshold` key, see *6.3.21(3) Details of the report conditions definition*.

  Note that even if critical threshold lines are set, critical thresholds are not output unless the corresponding collection data is output.
- By default, critical threshold lines are not drawn.
- Critical threshold lines are drawn as dotted lines.
- Critical threshold lines are drawn in the same colors as those of the target collection data lines.
- You can specify whether to draw a critical threshold line for each subresource.
- If the threshold changes while a critical threshold line is being drawn, the variation is applied to the drawing.
- If multiple lines overlap, the threshold that is drawn last is displayed.
- The subresource and instance names are displayed in a tooltip in the *subresource-name* (*instance-name*) format. Tooltips can be displayed only for lines that are displayed.

(c) Unit

Displays the unit for collection data values.

(d) Prot type

Displays the plot type specified in the Report Type Setup window or in the `plot_type` key in the report definition file.

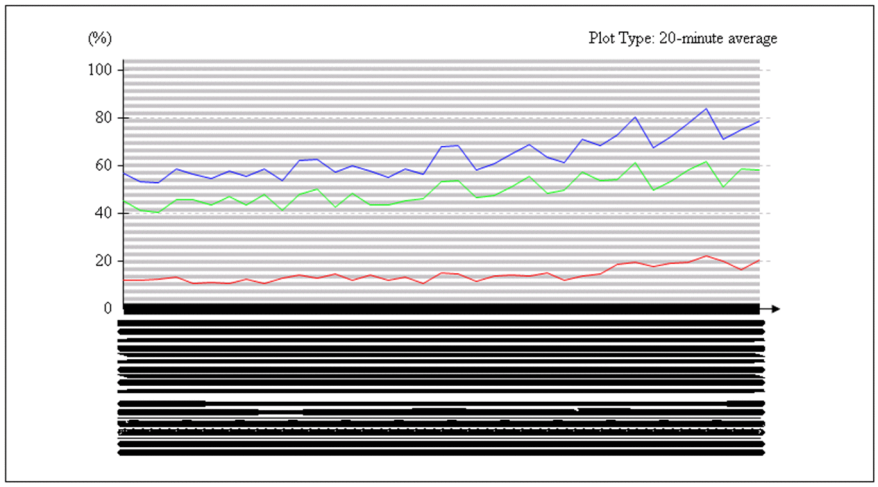
(e) Introductory notes on line types

- The graph line types are described below the graph introductory-notes table.
- Lines are drawn in black.
- Collection data lines are drawn as solid lines, warning threshold lines as dashed lines, and critical threshold lines as dotted lines.
- All three types are displayed regardless of warning threshold line and critical threshold line output.

(f) Date

- On the time axis, times are displayed in *YYYY*/*MM*/*DD* *hh*:*mm*:*ss* format. Normally, a line break is inserted between *DD* and *hh*.
- For the conditions in which 90-degree rotation is employed, see *(a) Graph frame*.
- Even if 90-degree rotation is employed, depending on the settings, character strings might overlap and be difficult to read. If character strings overlap excessively, they might be displayed as if they are horizontal lines. The following figure shows an example.

Figure 2-31: Example of a graph that has excessively-overlapping character strings



Time axis and scale line conditions:

Time axis: The start time is 08:30:00 on October 1, 2013, and the end time is 20:30:00 on October 1, 2013.

Scale line setting: 1-minute interval

Depending on the settings, multiple scale lines might be output at the same X coordinate. In this case, the date is output only for the first drawn scale line.

(4) Statistics information

You can output the maximum value, minimum value, and average of each subresource and instance that are the targets of the report. If the maximum value or minimum value is a fraction, it is rounded to the second decimal place. If that value is an integer, the decimal places `.00` are added.

This setting can be specified in **Statistics** in the Graph Detail Setup window or the report definition file. For details on **Statistics**, see *4.9.5(1) Graph Detail Setup window*. For details on the `graph_statistics_info` key, see *6.3.21(3) Details of the report conditions definition*. By default, statistics information is not output.

You can select the statistics information format from among the four table formats for report output. The statistics information is displayed below each graph.

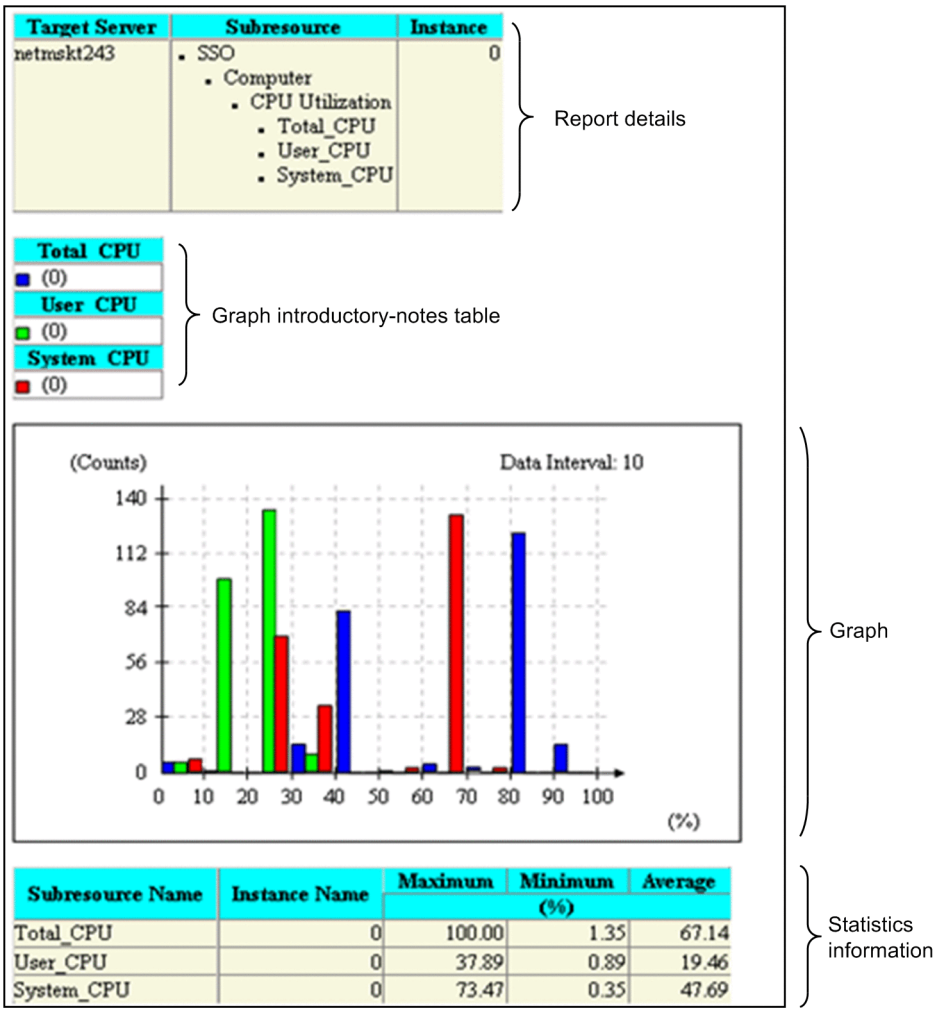
(5) Notes

For line graphs, data is averaged according to the specified plot type, by using the start time on the graph time axis as the base. Drawing of a line in a graph is based on the time at which averaging of the data for the line starts. For example, assume that the report term is from 10:00 to 20:00 and the plot type is 1 hour. In addition, assume that the `graph_time_adjust` key is set to off or that **The start and end of a time-axis are united during the data extraction** is cleared in the Graph Detail Setup window. In this case, if data actually exists only in the period from 10:30 to 19:00, the graph is drawn with values plotted at 1-hour intervals on the time axis that starts at 10:30 and ends at 18:30.

2.4.5 Report files in histogram format

The report section of a report in histogram format displays the report details, histogram, and graph introductory-notes table. The following figure shows an example of a report file in histogram format.

Figure 2-32: HTML-format report file (histogram format)



The following subsections describe the contents displayed in report files.

(1) Report details

The collection target server name, subresource names, and instance names are displayed as report details.

(2) Graph introductory-notes table

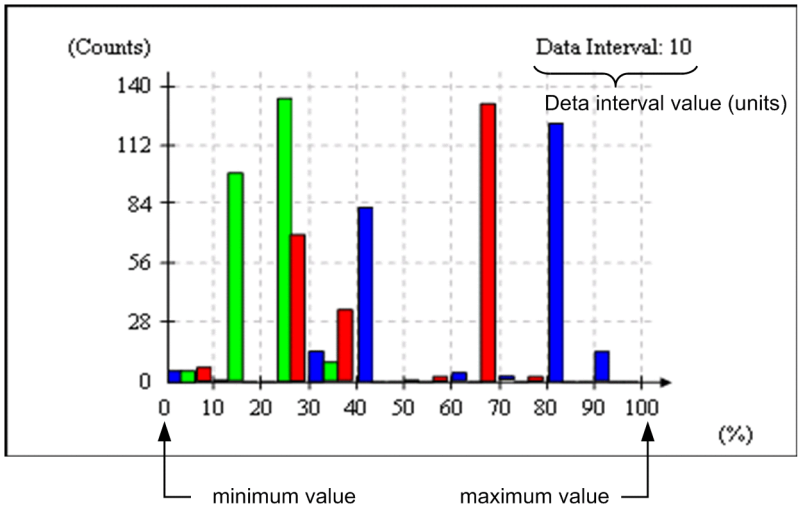
A graph introductory-notes table displays the legend for the display colors of the graph and the subresource or instance names. The value specified in **Introductory-notes Table** in the Graph Detail Setup window or the value set with the `graph_legend_row` key in the report definition file is used as the number of columns to be displayed. The maximum number of columns that can be displayed is 100. The default is 10.

(3) Graph

The number of data occurrences is displayed for equally divided intervals in a graph. This information can be displayed for a maximum of 8 types of data. Placing the mouse pointer over a bar in the graph displays the subresource name and instance name of that bar in a tooltip. In the tooltip, these names are displayed in the *subresource-name* (*instance-name*) format.

The following figure shows an example of a graph in histogram format.

Figure 2-33: Example of a graph in histogram format



(a) Graph frame

- The vertical axis displays the number of data occurrences within each data interval. The bottom of the axis indicates the minimum value, and the top of the axis indicates the maximum value. The scale lines are positioned at 5 equidistant points between the top and the bottom of the vertical axis.
- The horizontal axis displays the data values. The left end of the axis indicates the minimum value, and the right end the maximum value.

(b) Data interval

The value of the data interval is the difference between the maximum value and minimum value divided by the number of data occurrences in the data interval. The number of data items in the data interval is specified in **Report Setting** in the Report Type Setup window. For details on **Report Setting**, see *4.9.5 Report Type Setup window*.

(4) Statistics

The minimum value, maximum value, and average values can be output (as numeric values) for all subresources or data instances that are used to create a report. If the minimum value or maximum value is a fraction, it is rounded to the second decimal place. If that value is an integer, the decimal places `.00` are added.

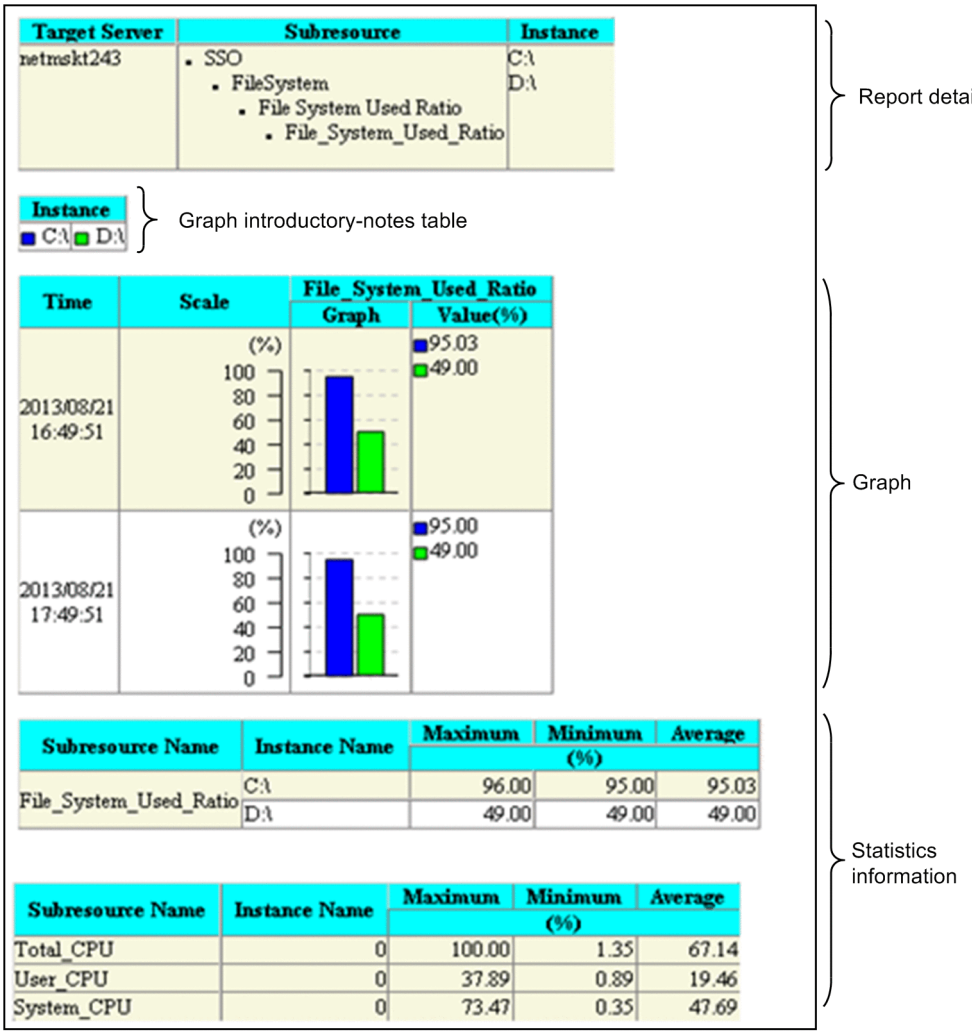
The settings for output of the above values are specified in the **Statistics** area of the Graph Detail Setup window or by using the report definition file. For details on **Statistics**, see *4.9.5(1) Graph Detail Setup window*. For details on `graph_statistics_info` key, see *6.3.21(3) Details of the report conditions definition*. Note that the above values are not output with the default settings.

The format of statistical information output to reports can be selected from four table formats. The statistical information is displayed in the selected format under the graph.

2.4.6 Report files in bar graph format

The report section of a report in bar graph format displays the report details, the graph, and graph introductory-notes table. Depending on the settings, related statistical information can also be displayed. The following figure shows an example of a report file in bar graph format.

Figure 2-34: HTML-format report file (bar graph format)



The following subsections describe the contents displayed in report files.

(1) Report details

The collection target server name, subresource names, and instance names are displayed as report details.

(2) Graph introductory-notes table

A graph introductory-notes table displays the legend for the display colors of the graph and the subresource or instance names. If the subresource-based format is used, the columns display instances. If the instance count-based format is used, the columns display subresources.

The number of columns in the graph introductory-notes table can be specified in **Introductory-notes Table** in the Graph Detail Setup window or the `graph_legend_row` key in the report definition file. The maximum number of columns that can be displayed is 100. The default is 10.

(3) Graph

The values of subresources and instances are displayed in bar graph format. A graph in this format consists of a graph frame, times, scale, and values. A graph is displayed from the perspective of instances or from the perspective of subresources, as specified in **Report Setting** in the Report Type Setup window. For details on **Report Setting**, see *4.9.5 Report Type Setup window*.

Placing the mouse pointer over a bar in the graph displays the subresource name and instance name of that bar in a tooltip. In the tooltip, these names are displayed in the *subresource-name* (*instance-name*) format.

Figure 2-35 shows an example of a graph output from the perspective of subresources. Figure 2-36 shows an example of a graph output from the perspective of instances.

Figure 2－35: Example of a graph output in bar graph format (from the perspective of subresources)

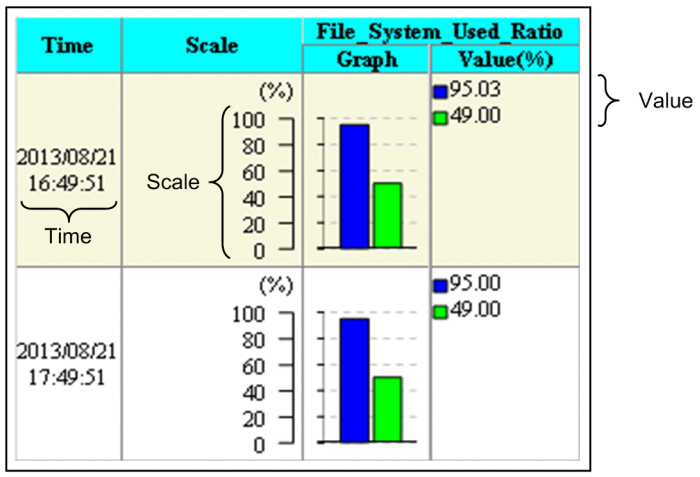
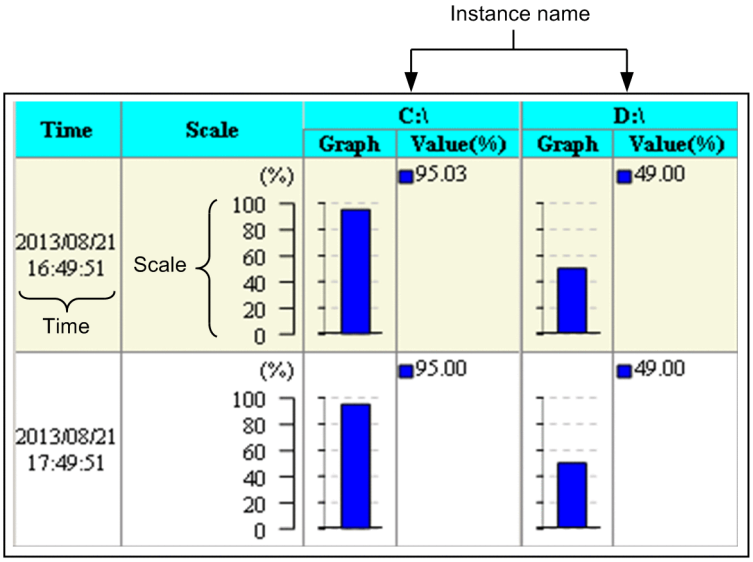


Figure 2-36: Example of a graph output in bar graph format (from the perspective of instances)



(a) Graph frame

- A graph is created for each graph interval, and the created graphs are aligned vertically.
- A maximum of 100 bars can be displayed in one graph.
- The value set for **Graph** in the Graph Detail Setup window or the value specified in the `graph_maxline` key in the report definition file is used as the maximum number of lines that can be displayed. For details on **Graph**, see *4.9.5(1)(c) For bar graph, stacked bar graph and pie chart*. For details on the `graph_maxline` key, see *6.3.21(3) Details of the report conditions definition*.

(b) Time

The time of each graph interval is displayed in the *YYYY*/*MM*/*DD hh*:*mm*:*ss* format.

(c) Scale

- The graph is scaled by dividing the difference between the maximum and minimum values into 5 equal parts.
- The lower limit is calculated from the minimum of the average values for the graph intervals within the extraction period. The upper limit is calculated from the maximum of the average values for the graph intervals within the extraction period.
- A unit is displayed for the scale, and its value remains unchanged for the entire time.

(d) Subresource name or instance name

If the perspective of subresources is specified as the graph type under **Report Setting** in the Report Type Setup window or specified in the `format` key in the report definition file, the subresource name is displayed. If the perspective of instances is specified, the instance name is displayed.

For details on **Report Setting**, see *4.9.5 Report Type Setup window*. For details on the `format` key, see *6.3.21(3) Details of the report conditions definition*.

(e) Value

Values are displayed together with a legend. Fractional values are rounded to the second decimal place. For integer values, the decimal places `.00` are added.

(4) Statistics information

For the data for which a report is to be created, the minimum value, maximum value, and average can be output for each subresource and instance as numeric values. If the minimum value or maximum value is a fraction, it is rounded to the second decimal place. If that value is an integer, the decimal places `.00` are added.

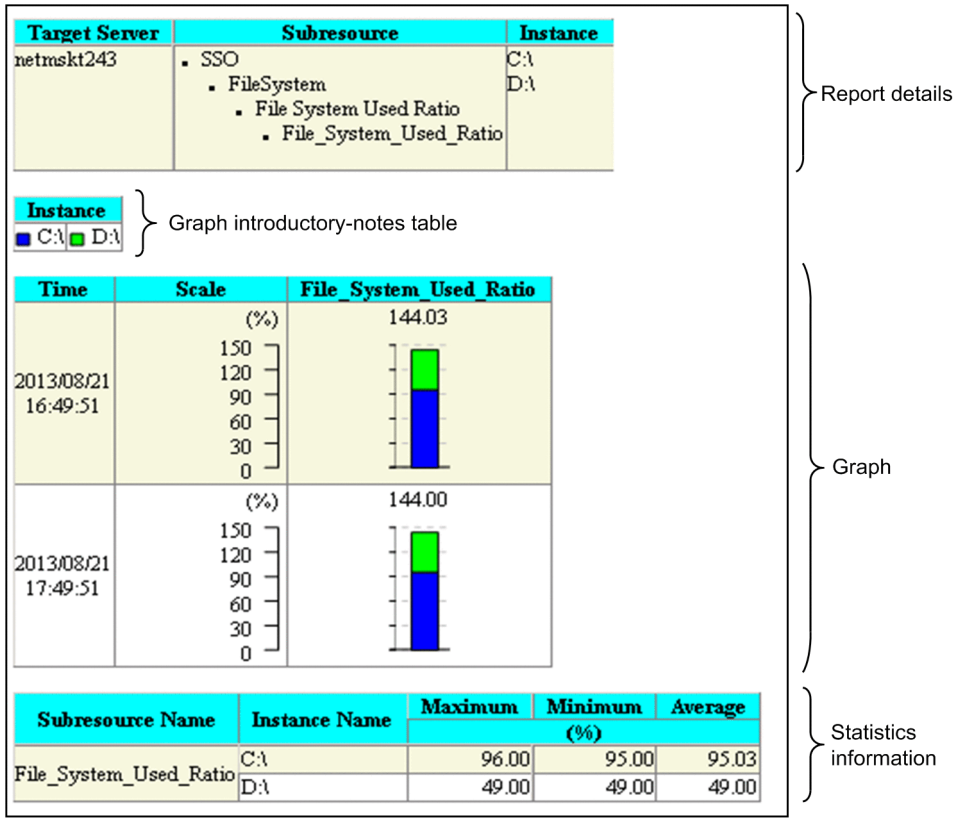
The settings for outputting the statistics information can be specified in **Statistics** in the Graph Detail Setup window or the report definition file. For details on **Statistics**, see *4.9.5(1) Graph Detail Setup window*. For details on the `graph_statistics_info` key, see *6.3.21(3) Details of the report conditions definition*. By default, statistics information is not output.

You can select the statistics information format from among the four display formats for report output. The statistics information is displayed below each graph.

2.4.7 Report files in stacked bar graph format

The report section of a report in stacked bar graph format displays the report details, graph, and graph introductory-notes table. Depending on the settings, related statistical information can also be displayed. The following figure shows an example of a report file in stacked bar graph format.

Figure 2-37: Example of a graph output in stacked bar graph format



The following subsections describe the contents displayed in report files.

(1) Report details

The collection target server name, subresource names, and instance names are displayed as report details.

(2) Graph introductory-notes table

A graph introductory-notes table displays the legend for the display colors of the graph and the subresource or instance names. If the perspective of subresources is used, the columns display instances. If the perspective of instances is used, the columns display subresources.

The number of columns in the graph introductory-notes table can be specified in **Introductory-notes Table** in the Graph Detail Setup window or the `graph_legend_row` key in the report definition file. The maximum number of columns that can be displayed is 100. The default is 10.

(3) Graph

The values of subresources and instances are added up and displayed in bar graph format. A graph in this format consists of a graph frame, times, scale, and values. A graph is displayed from the perspective of instances or from the perspective of subresources, as specified in **Report Setting** in the Report Type Setup window. For details on **Report Setting**, see *4.9.5 Report Type Setup window*.

Placing the mouse pointer over a bar in the graph displays the subresource name and instance name of that bar in a tooltip. In the tooltip, these names are displayed in the *subresource-name* (*instance-name*) format.

Figure 2-38 shows an example of a graph output from the perspective of subresources. Figure 2-39 shows an example of a graph output from the perspective of instances.

Figure 2-38: Example of a graph output in stacked bar graph format (from the perspective of subresources)

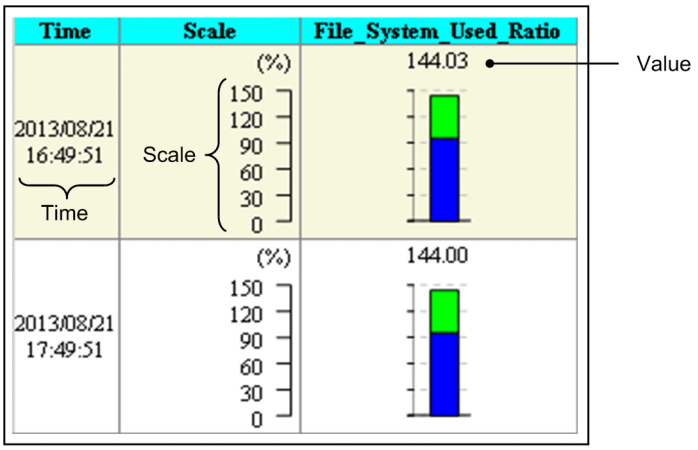
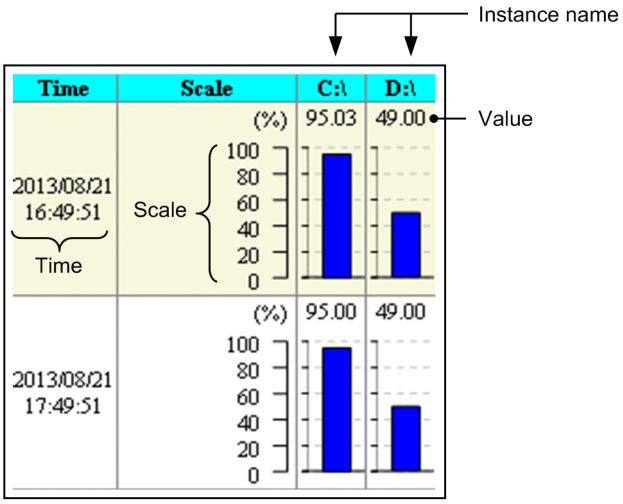


Figure 2-39: Example of a graph output in stacked bar graph format (from the perspective of instances)



(a) Graph frame

- A graph is created for each graph interval, and the created graphs are aligned vertically.
- A maximum of 100 bars can be displayed in one graph.
- The value set for **Graph** in the Graph Detail Setup window or the value specified in the `graph_maxline` key in the report definition file is used as the maximum number of lines that can be displayed. For details on **Graph**, see *4.9.5(1)(c) For bar graph, stacked bar graph and pie chart*. For details on the `graph_maxline` key, see *6.3.21(3) Details of the report conditions definition*.

(b) Time

The time of each graph interval is displayed in the *YYYY*/*MM*/*DD hh*:*mm*:*ss* format.

(c) Scale

- The graph is scaled by dividing the difference between the maximum and minimum values into 5 equal parts.
- The lower limit is calculated from the minimum of the average values for the graph intervals within the extraction period. The upper limit is calculated from the maximum of the average values for the graph intervals within the extraction period.
- A unit is displayed for the scale, and its value remains unchanged for the entire time.

(d) Subresource name or instance name

If the perspective of subresources is specified as the graph type under **Report Setting** in the Report Type Setup window or specified in the `format` key in the report definition file, the subresource name is displayed. If the perspective of instances is specified, the instance name is displayed.

For details on **Report Setting**, see *4.9.5 Report Type Setup window*. For details on the `format` key, see *6.3.21(3) Details of the report conditions definition*.

(e) Value

Fractional values are rounded to the second decimal place. For integers, the decimal places `.00` are added.

(4) Statistics information

For the data for which a report is to be created, the minimum value, maximum value, and average can be output for each subresource and instance as numeric values. If the minimum value or maximum value is a fraction, it is rounded to the second decimal place. If that value is an integer, the decimal places `.00` are added.

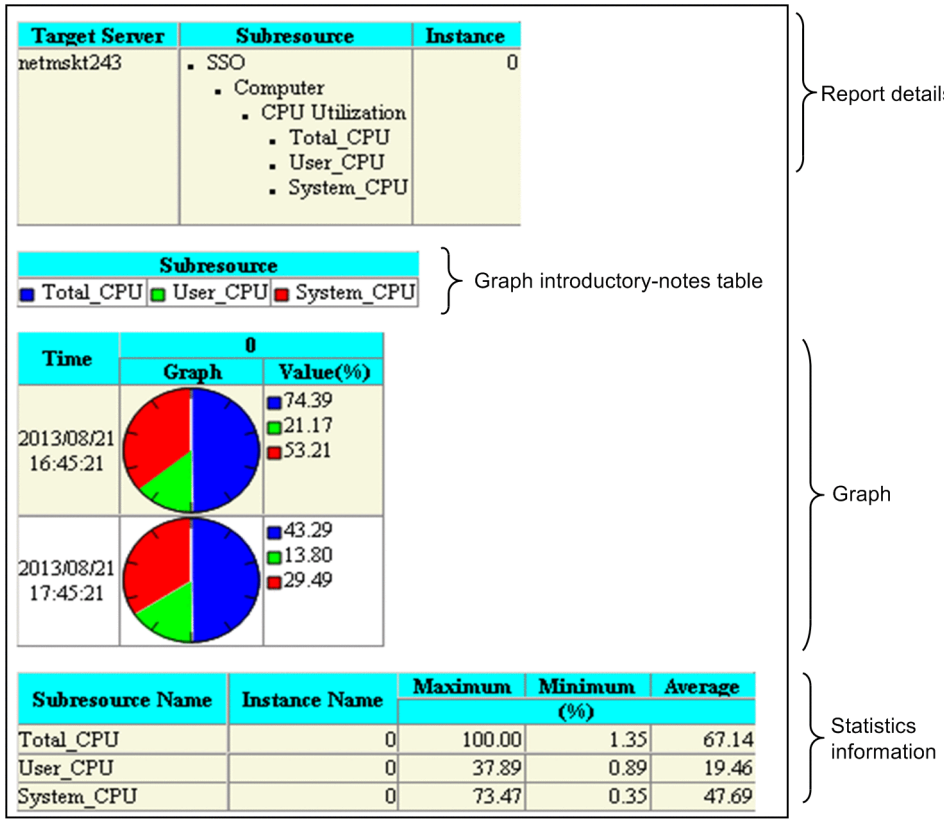
The settings for outputting the statistics information can be specified in **Statistics** in the Graph Detail Setup window or the report definition file. For details on **Statistics**, see *4.9.5(1) Graph Detail Setup window*. For details on the `graph_statistics_info` key, see *6.3.21(3) Details of the report conditions definition*. By default, statistics information is not output.

You can select the statistics information format from among the four display formats for report output. The statistics information is displayed below each graph.

2.4.8 Report files in pie chart format

The report section of a report in pie chart format displays the report details, the graph, and graph introductory-notes table. Depending on the settings, related statistical information can also be displayed. The following figure shows an example of a graph in pie chart format.

Figure 2-40: Example of a graph output in pie chart format



The following subsections describe the contents displayed in report files.

(1) Report details

The collection target server name, subresource names, and instance names are displayed as report details.

(2) Graph introductory-notes table

A graph introductory-notes table displays the legend for the display colors of the graph and the subresource or instance names. If the perspective of subresources is used, the columns display instances. If the perspective of instances is used, the columns display subresources.

The number of columns in the graph introductory-notes table can be specified in **Introductory-notes Table** in the Graph Detail Setup window or the `graph_legend_row` key in the report definition file. The maximum number of columns that can be displayed is 100. The default is 10.

(3) Graph

The values of subresources and instances are displayed in pie chart format. A graph in this format consists of a graph frame, times, and values.

A graph can be displayed in one of two forms, the perspective of instances or the perspective of subresources, as specified under **Report Setting** in the Report Type Setup window. For details on **Report Setting**, see *4.9.5 Report Type Setup window*. For either perspective, you can select whether to display values as percentages or as ratios to the base value.

Placing the mouse pointer over a pie chart displays the subresource name and instance name of that pie chart in a tooltip. In the tooltip, these names are displayed in the *subresource-name* (*instance-name*) format.

Figure 2-41 shows an example of outputting graphs, from the perspective of subresources, that have values indicated as percentages. Figure 2-42 shows an example of outputting graphs, from the perspective of instances, that have values indicated as percentages. Figure 2-43 shows an example of outputting graphs, from the perspective of subresources, that have values indicated as ratios to the base value. Figure 2-44 shows an example of outputting graphs, from the perspective of instances, that have values indicated as ratios to the base value.

Figure 2-41: Example of outputting graphs in pie chart format (from the perspective of subresources, with values indicated as percentages)

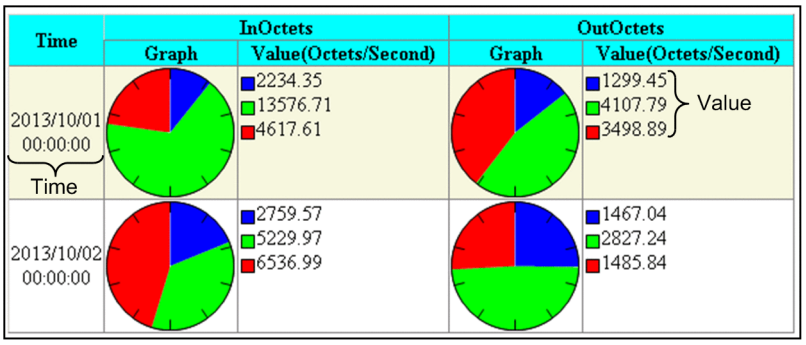


Figure 2-42: Example of outputting graphs in pie chart format (from the perspective of instances, with values indicated as percentages)

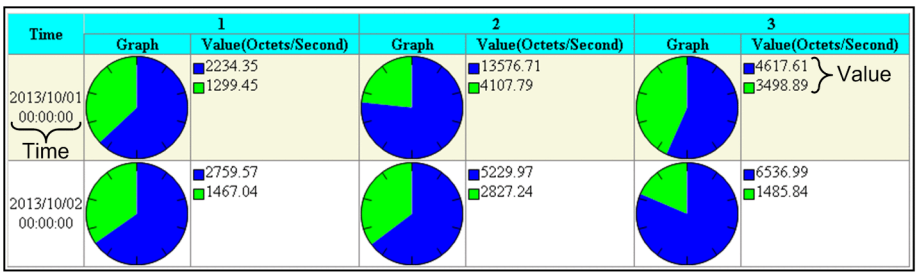


Figure 2-43: Example of outputting graphs in pie chart format (from the perspective of subresources, with values indicated as ratios to the base value)

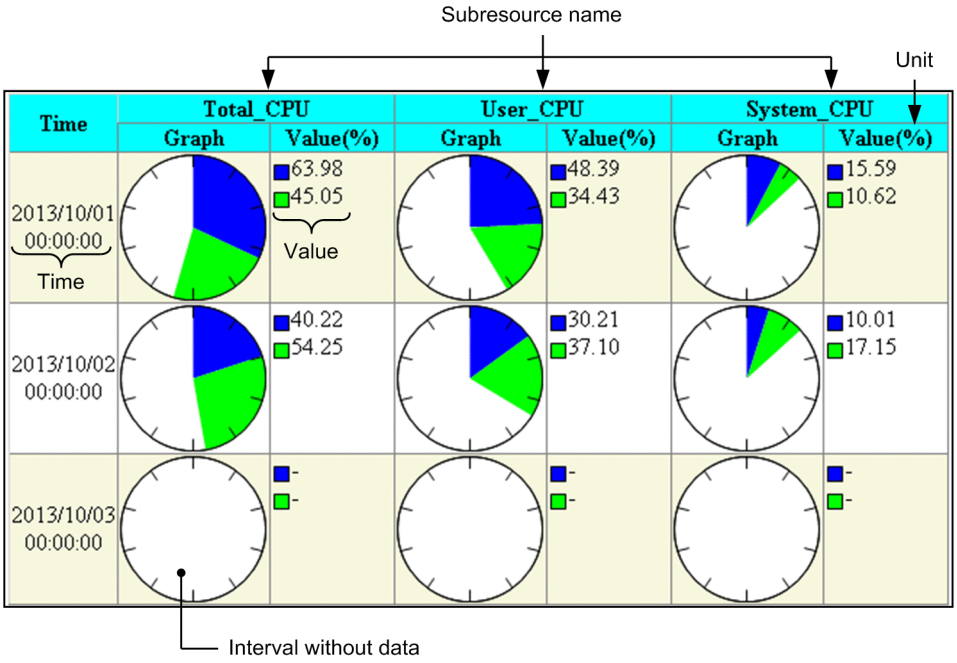
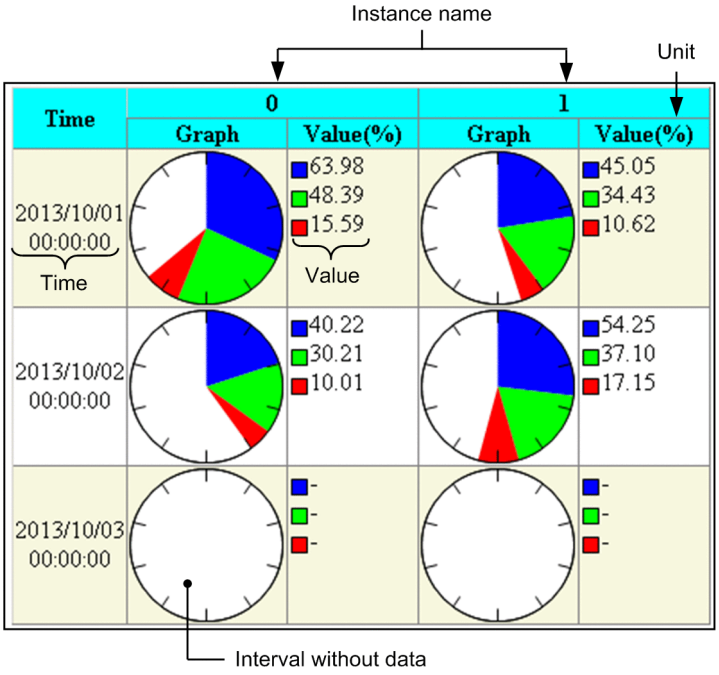


Figure 2-44: Example of outputting graphs in pie chart format (from the perspective of instances, with values indicated as ratios to the base value)



(a) Graph frame

- If percentage mode is selected, the absolute value of each subresource or instance is used to draw the pie chart. If ratio mode is selected, the ratio of the absolute value of each subresource or instance to the user-specified base value is used to display the pie chart.

  Ratio mode is available if **Specify 100% value** is selected under **Report Setting** in the Report Type Setup window. Alternatively, ratio mode is available if the `graph_piechart_standard` key in the report definition file is set

to a value that will be displayed as 100%. For details on **Report Setting**, see *4.9.5 Report Type Setup window*. For details on the `graph_piechart_standard` key, see *6.3.21(3) Details of the report conditions definition*.

- A graph is created for each graph interval, and the created graphs are aligned vertically.
- A maximum of 100 items can be displayed in one graph.
- Sections and locations without data are displayed as blanks.
- The maximum number of rows on which graphs can be displayed is the value set in **Graph** in the Graph Detail Setup window or the value specified in the `graph_maxline` key in the report definition file. For details on **Graph**, see *4.9.5(1)(c) For bar graph, stacked bar graph and pie chart*, and for details on the `graph_maxline key`, see *6.3.21(3) Details of the report conditions definition*.

(b) Time

The time of each graph interval is displayed in the *YYYY/MM/DD hh:mm:ss* format.

(c) Value

Values are displayed together with a legend. Fractional values are rounded to the second decimal place. For integer values, the decimal places `.00` are added.

(d) Subresource name or instance name

If the perspective of subresources is specified as the graph type under **Report Setting** in the Report Type Setup window or specified in the `format` key in the report definition file, the subresource name is displayed. If the perspective of instances is specified, the instance name is displayed.

For details on **Report Setting**, see *4.9.5 Report Type Setup window*. For details on the `format` key, see *6.3.21(3) Details of the report conditions definition*.

(4) Statistics information

For the data for which a report is to be created, the minimum value, maximum value, and average can be output for each subresource and instance as numeric values. If the minimum value or maximum value is a fraction, it is rounded to the second decimal place. If that value is an integer, the decimal places `.00` are added.

The settings for outputting the statistics information can be specified in **Statistics** in the Graph Detail Setup window or the report definition file. For details on **Statistics**, see *4.9.5(1) Graph Detail Setup window*. For details on the `graph_statistics_info` key, see *6.3.21(3) Details of the report conditions definition*. By default, statistics information is not output.

You can select the statistics information format from among the four display formats for report output. The statistics information is displayed below each graph.

2.4.9 Report files in table format

The report section of a report in table format displays the report details and the table.

(1) Subresource columns - Instance Rows

The following subsections describe the displayed contents. Figure 2-45 shows the display format.

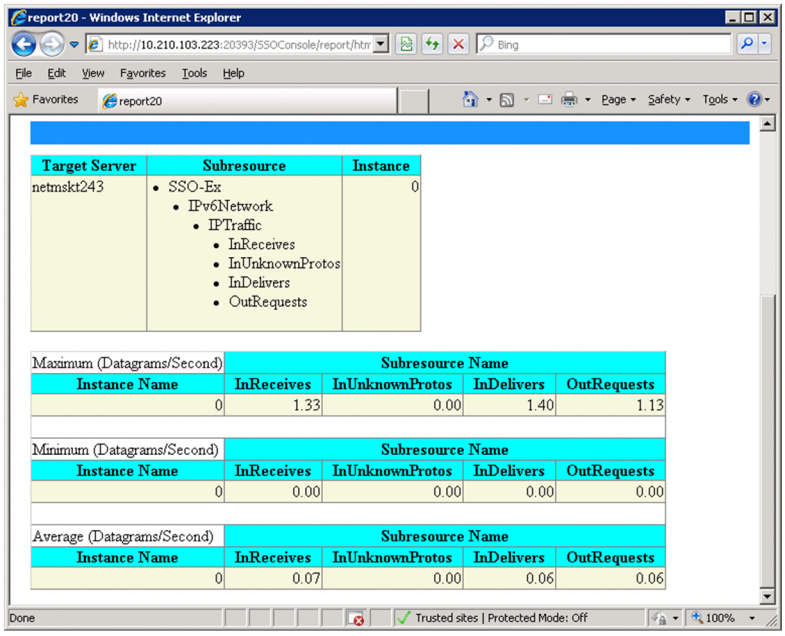
(a) Report details

The collection target server name, unit, subresource names, and instance names are displayed as report details.

(b) Table

A row is created for each instance name and a column is created for each subresource name. The minimum value, maximum value, and average for the report term are displayed as the report result.

Figure 2-45: Table with subresource-based columns and instance-based rows



(2) Instance columns - Subresource rows

The following subsections describe the displayed contents. Figure 2-46 shows the display format.

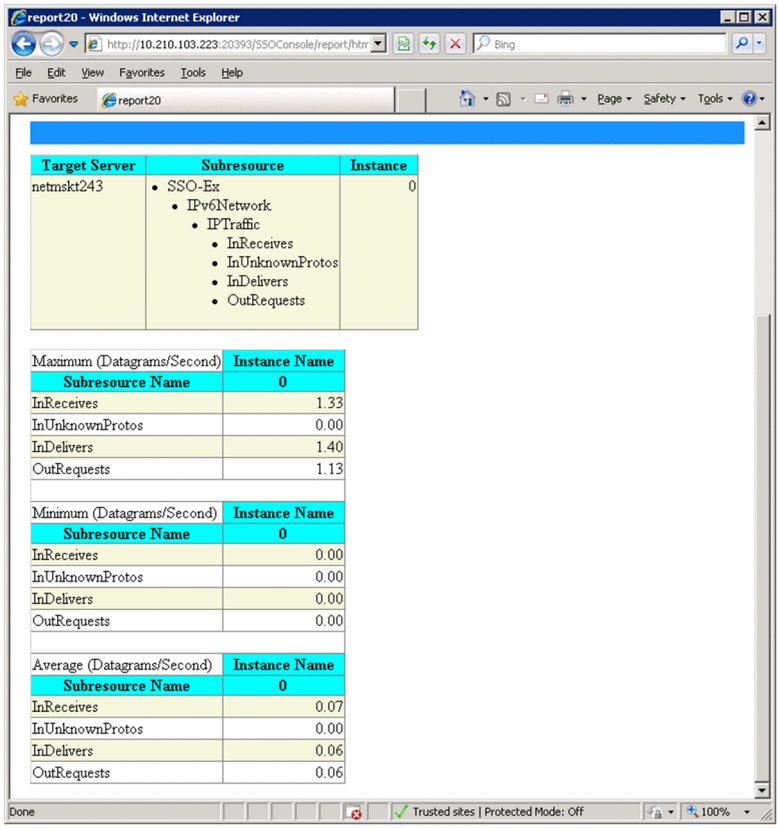
(a) Report details

The collection target server name, unit, subresource names, and instance names are displayed as report details.

(b) Table

A row is created for each subresource name and a column is created for each instance name. The minimum value, maximum value, and average for the report term are displayed as the report result.

Figure 2-46: Table with instance-based columns and subresource-based rows



(3) According to instance

The following subsections describe the displayed contents. Figure 2-47 shows the display format.

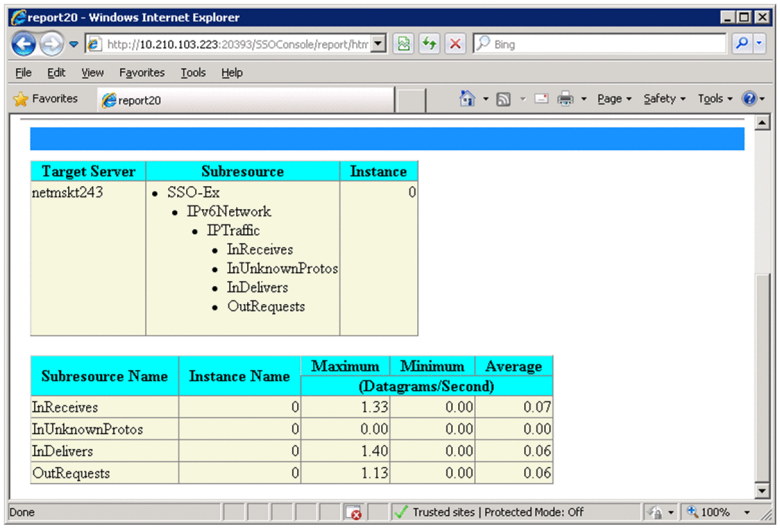
(a) Report details

The collection target server name, unit, subresource names, and instance names are displayed as report details.

(b) Table

A subresource name is displayed as the parent category of a row, and instance names are displayed as child categories of that row. The minimum value, maximum value, and average for the report term are displayed as the report result.

Figure 2-47: Table created from the perspective of instances (according to instance)



(4) According to subresource

The following subsections describe the displayed contents. Figure 2-48 shows the display format.

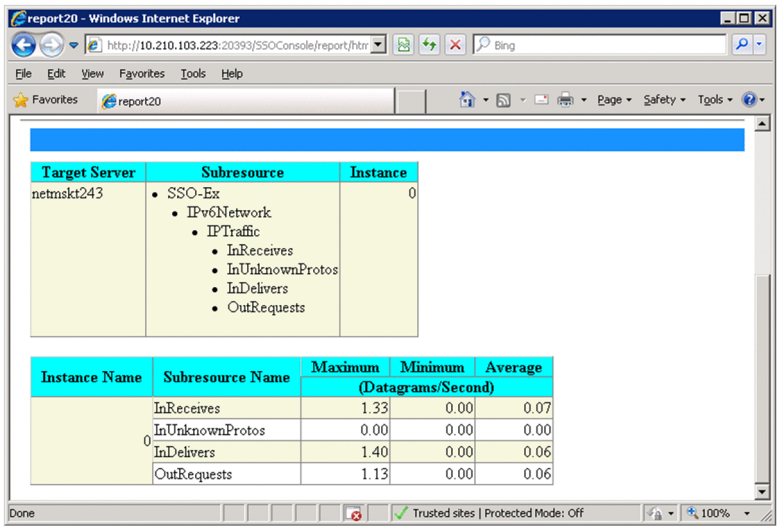
(a) Report details

The collection target server name, unit, subresource names, and instance names are displayed as report details.

(b) Table

An instance name is displayed as the parent category of a row, and the subresource name is displayed as the child category of that row. The minimum value, maximum value, and average for the report term are displayed as the report result.

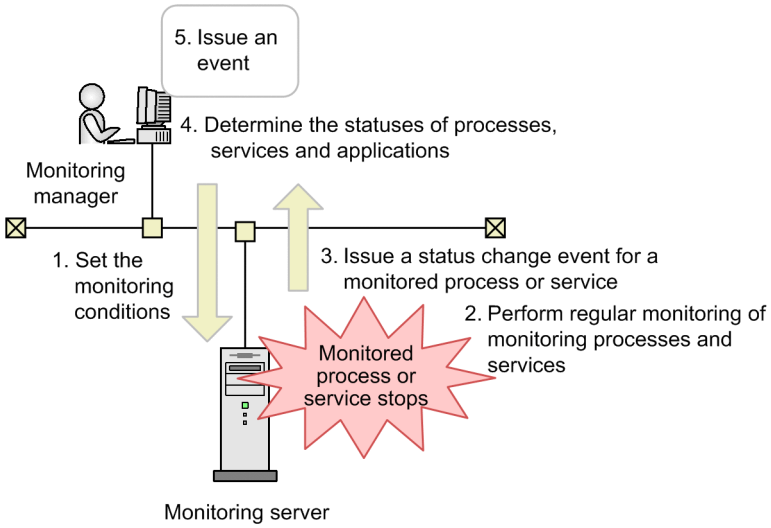
Figure 2-48: Table created from the perspective of subresources (according to subresource)



2.5 Process and service monitoring function

The operating status of all processes and Windows services running on a server can be monitored. The operating status of monitored processes and services is checked to determine whether the application is running normally. A set of parent and child processes can be monitored while considering their parent-child relationship. For process and service monitoring, the APM must exist on the server running the processes and services targeted for monitoring. The following figure shows how SSO monitors processes and services.

Figure 2-49: Flow of process and service monitoring by SSO



1. Set the monitoring conditions

   From SSO, set the monitoring conditions to APM.

2. Perform regular monitoring of monitored processes and services

   APM performs regular monitoring of processes and services according to the conditions set in step 1.

3. Issue a status change event for a monitored process or service

   APM issues a status change event upon detecting a status change, such as a monitoring process or service stop, during the regular monitoring of step 2.

4. Determine the statuses of processes, services, and applications

   Based on the events sent from the APM in step 3, SSO determines the statuses of the processes, services, and applications.

5. Issue an event

   Following determination of the status, SSO issues an event (incident). The issued event is displayed in the incident view of NNMi. For details on the types of events that are issued by SSO, see *F.1(2) Process and service monitoring event*.

Note that since the monitoring conditions are set to APM using the SNMP protocol, the community name set for the monitoring manager and agent must match.

If the monitored server runs UNIX, when you set the process type for a process to be monitored, select either an executable file name or command line name. If the monitored server runs Windows, select an executable file name.

The following sections describe in detail the process and service monitoring function.

2.5.1 Setting the monitoring conditions

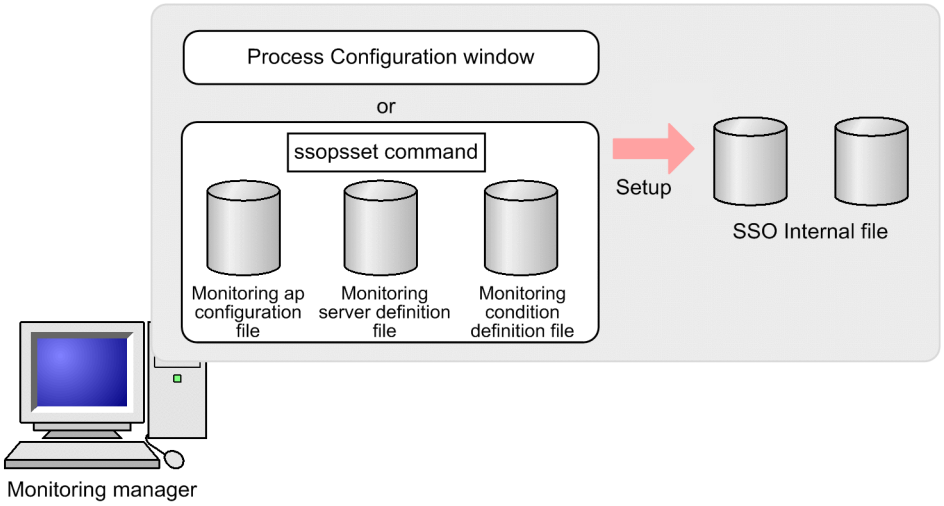
Set the following as the conditions for monitoring processes and services:

- Monitoring server, monitoring interval, and health check interval
- Applications, processes, child processes, and services to be monitored
- Thresholds
- Mapping of service operating states

The monitoring conditions are set with the Process Configuration window or the monitoring condition setting command (`ssopsset`). When the monitoring conditions are set, they are registered in the monitoring condition definition file (an internal SSO file) and monitoring app setting file (an internal SSO file). Thresholds can be set for each application, process, and child process. Mapping of service operating states can be set on an individual-service basis.

The following figure shows how the monitoring conditions are set.

Figure 2-50: Schema of setting up monitoring conditions



(1) Notes on setting monitoring conditions (process monitoring)

(a) Notes regarding long monitoring-process names

A monitoring process name can have 60 or fewer bytes. To monitor a process whose name is longer than 60 bytes, use wildcard characters to shorten the process name to 60 bytes or less. You can use asterisks (`*`) or question marks (`?`) as wildcard characters. An asterisk can indicate 0 or more characters, and a question mark can indicate 1 character. However, if the version of APM is earlier than 07-10, you can use an asterisk only at the beginning and end of the process name.

Example:

Actual command line:

```
/opt/CM2/SSO/bin/ssocolmng -f
```

Alternative representation:

```
/opt/*/ssocolmng*
```

(b) Notes on specifying a monitoring process name that includes a period (.)

When you set process monitoring conditions for monitoring servers where all of the conditions listed below exist, be careful when specifying a process name that includes a period (`.`). In such a case, make sure that you specify the character string up to but not including the period (`.`). However, if the process name begins with a period (`.`), specify the process name from the beginning, up to but not including the next period (`.`).

- The monitoring server runs Windows
- The APM version is earlier than 07-50-01
- The `tlist` command is used to obtain process information

When you specify process monitoring condition settings for monitoring servers that run UNIX and do not satisfy all of the above conditions, you can specify process names that include a period (`.`) as-is.

(c) Notes on specifying monitoring process names and types for monitoring servers that run Windows

When you specify monitoring process names, make sure that you do not include an extension (such as `.exe`). As monitoring cannot be executed from the command line, select an executable file name as the monitoring process type.

(d) Notes on specifying monitoring process types for monitoring servers that run UNIX

The following describes how to select the monitoring process type.

Executable file name:

If the APM version is earlier than 07-50, when you specify a monitoring process name that is displayed by the `ps` command with the `-e` option, specify an executable file name as the monitoring process type. If the APM version is 07-50 or later, when you specify a monitoring process name that is displayed by the `apmproclist` command with the `-e` option, specify an executable file name.

Command line name:

If the APM version is earlier than 07-50, when you set a process name that is displayed by the `ps` command with the `-ef` option, you must specify a command line name as the monitoring process type. If the APM version is 07-50 or later, when you set a process name that is displayed by the `apmproclist` option with the `-c` option, you must specify a command line name as the monitoring process type. If the process name that you specify is displayed by the `ps` or `apmproclist` command with the `-e` option, specify an executable file name, instead of a command line name. Note that if the monitoring server runs AIX or Linux, you cannot monitor swapped-out processes (processes enclosed in square brackets in the execution results of the `ps` or `apmproclist` command) from the command line.

(2) Notes on setting monitoring conditions (service monitoring)

You can monitor services if the OS of the target monitoring servers is Windows and the APM version is 07-10 or later. The following describes how to specify the names of the Windows services to be monitored.

Service name:

If the version of APM is 07-50 or later:

Set one of the service names displayed by using the `apmservlist` command.

If the version of APM is 07-10:

From the **Start** menu, select **Control Panel**, **Administrative Tools**, **Services**, and select the service to be monitored. When the properties are displayed, set the name to be displayed as the service name.

2.5.2 Process and service monitoring

Process monitoring is conducted by APM on a server on which the processes to be monitored are running. SSO then determines the process status, service status, and application status based on the received process status change event from APM.

In process and service monitoring, the following functions can be used:

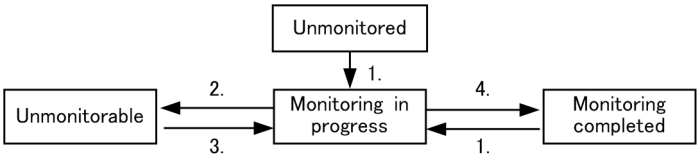
1. Monitored status management
2. Threshold monitoring (only process monitoring)
3. Monitoring of service operating states
4. Automated action and remote command

Each of the above is explained below.

(1) Monitored status management

The monitored status of a process and service is managed. The following figure shows the monitored status managed by SSO and the timing of monitored status changes.

Figure 2−51: Monitored statuses of a process



1. Monitoring has started.
2. Monitoring has stopped due to the following reasons:
   - The monitoring conditions were not successfully set for monitoring server.
   - The APM of the monitoring server stopped.
   - The health check for the APM of the monitoring server failed.
   - The status change trap from APM disappeared.
3. The APM of the monitoring server started.
4. Either of the following events occurred:
   - Either SSO stopped or the `ssoapmon` daemon process paused.#
   - Monitoring was stopped by the user.

If monitoring stops because the `ssoapmon` daemon process paused, a status change event is not issued.

When the monitored status changes, JP1/Cm2/SSO can issue a monitored status change event. For details on events, see *F. Events*.

(2) Monitoring threshold

When a threshold is set, it is possible to check whether the monitored process exceeds the threshold. The results of threshold monitoring can be treated as the process or application status. To indicate the status of a process or child process, three categories are used: Normal, Critical, and Unknown. To indicate the status of an application, four categories are used: Normal, Warning, Critical, and Unknown.

If the process monitoring status changes, a process status change event is issued. For details on these events, see *F. Events*.

A number of running processes must be specified for use as the threshold. If multiple instances of a process having the same name run or a wildcard character is used for the process name, the minimum (lower threshold) and maximum (upper threshold) values must be specified in order to define the number of running processes. If the number of running processes moves outside the preselected threshold range, the process status changes. The following table lists how the process status and child process status are determined.

Table 2-8: Method for determining the status of a process or child process

Status	Determination method
Normal	The number of running processes# of the monitored processes is within the threshold limit.
Critical	The number of running processes# of the monitored processes is outside the threshold limit.
Unknown	No process status change event exists.

#

Zombie processes that can be detected only if the OS of the agent is HP-UX or HP-UX (IPF) are not included in the number of running processes.

SSO determines application status in accordance with process status. The following table lists how application status is determined.

Table 2-9: Method for determining the status of an application

Status	Determination method
Normal	All the processes are normal.
Warning	There is at least one normal and one critical process. In addition, unknown processes do not exist.
Critical	All the processes are critical.
Unknown	At least one process is unknown.

(a) Notes on threshold monitoring

Generally, in UNIX, when a given process generates a child process, that child process temporarily inherits the process name, command line name, and other execution environment settings of the parent process. For this reason, when SSO monitors processes on UNIX, the number of running monitored processes might include the number of their child processes.

Therefore, for processes monitored on UNIX, if the upper threshold is set without taking into consideration the number of child processes, the threshold might be exceeded, reporting *Critical* status even if the status is *Normal*. Therefore, if the OS of the monitoring server is UNIX, you must tune the value of the upper threshold. Set the upper threshold value shown below for any monitoring-target processes and their child processes.

If the maximum number of processes that concurrently exist as child processes of a monitoring-target process (or child process) is known:

Assume that the maximum number of instances of a process (or child process) to be monitored is *m*, and the maximum number of child processes that concurrently exist per process is *n*. Then, set the value obtained from the following calculation formula for the upper threshold of that process (or child process):

m **x** (1 + *n*)

However, if the result of the above calculation exceeds 9999, set 9999.

If the maximum number of processes that exist simultaneously as the child processes of a monitoring-target process (or child process) is unknown:

Set 9999.

(3) Monitoring of service operating states

If you have mapped service states and service operating states, you can manage the operating status of monitored services by using the service monitoring status and application status. There are three service monitoring statuses (*Normal*, *Critical*, and *Unknown*) and four application statuses (*Normal*, *Warning*, *Critical*, and *Unknown*).

If the status of a service changes, a service status change event is issued. If the status of an application changes, an application status change event is issued. For details on these events, see *F. Events*.

The following table lists how the service monitoring status is determined.

Table 2-10: Method for determining the service monitoring status

Status	Determination method
Normal	The monitored service is operating in the status that was set as *Normal* in the service operating status mapping.
Critical	The monitored service is operating in the status that was set as *Critical* in the service operating status mapping.
Unknown	No service status change event has been issued. Alternatively, the specified service does not exist on the monitoring server.

SSO determines application status in accordance with service status. The following table lists how application status is determined.

Table 2-11: Method for determining the status of an application

Status	Determination method
Normal	All the services are normal.
Warning	There is at least one normal and one critical service. In addition, unknown services do not exist.
Critical	All the services are critical.
Unknown	At least one service is unknown.

(4) Automated actions and remote commands

A command can be automatically executed when an application status changes. Commands can be set individually for the normal, warning, and critical regions. These commands can be executed on the monitoring manager and on the monitoring server. Executing a command automatically on the monitoring manager or monitoring server is called an *automated action*. Commands that are executed either automatically or on demand on the monitoring server are called *remote commands*. You can also specify variables in a command. For details on the variables you can define, see *G. Variables That Can Be Defined via Automated Action*.

From the Process Monitor window, you can execute on an on-demand basis commands that were registered by the monitoring application on the monitoring server. You cannot specify variables for commands that are executed on demand.

To execute commands as automatic actions, you must be a superuser (in UNIX) or a member of the Administrators (in Windows). To execute remote commands in UNIX, you must be a superuser. To execute remote commands in Windows, you must have permission to log on to SNMP System Observer - Agent for Process, which is an APM service.

If you run batch files on Windows, add `cmd /q /c` at the beginning of the command line. For example, to execute `C:\temp\aaa.bat`, specify `C:\temp\aaa.bat`.

The following lists the triggers for the execution of automatic actions and remote commands.

- Normal -> Warning
- Normal <- Warning
- Warning -> Critical
- Warning <- Critical
- Normal -> Critical
- Normal <- Critical
- Unknown -> Normal
- Unknown <- Normal
- Unknown -> Warning
- Unknown <- Warning
- Unknown -> Critical
- Unknown <- Critical

Note that automatic actions are executed according to the application status determined when the `ssoapmon` daemon process is started, as shown in the following table.

Table 2-12: Application statuses and automatic action execution triggers

Application status when ssoapmon is started	Automatic action execution trigger
Normal	Unknown -> Normal
Warning	Unknown -> Warning
Critical	Unknown -> Critical

2.5.3 Real-time monitor of monitoring status of processes and services

From the Process Monitor window, you can check the statuses of processes, services, and applications for each monitoring server. You can also update the monitoring status to the latest status and execute remote commands on demand for the desired monitoring server.

2.5.4 Process and services status adjustment

When the process status does not match between SSO and APM the process status can be forcibly adjusted. The process status can be adjusted from the Process Monitor window or by the `ssoapcom` command.

2.5.5 Health check

The health check function checks the operating status of APM on the monitoring server, and checks for discrepancies of monitoring conditions between SSO and APM.

Upon detecting discrepancies in monitoring conditions between SSO and APM, the health check function synchronizes the monitoring conditions between SSO and APM.

The function can conduct three types of checks: a system health check, a regular health check, and an on-demand health check. The following describes these types of checks.

(1) System health check

A system health check is a health check that SSO always performs automatically.

The following are the execution triggers for system health checks:

- JP1/Cm2/SSO is started.
- A monitoring server is added.
- The startup event is received from APM.
- For a monitoring server that is in the status in which monitoring is impossible, the monitoring conditions are changed, or discrepancies in monitoring conditions are corrected.
- An error occurs during TCP communication with APM.

The following describes settings related to the system health check.

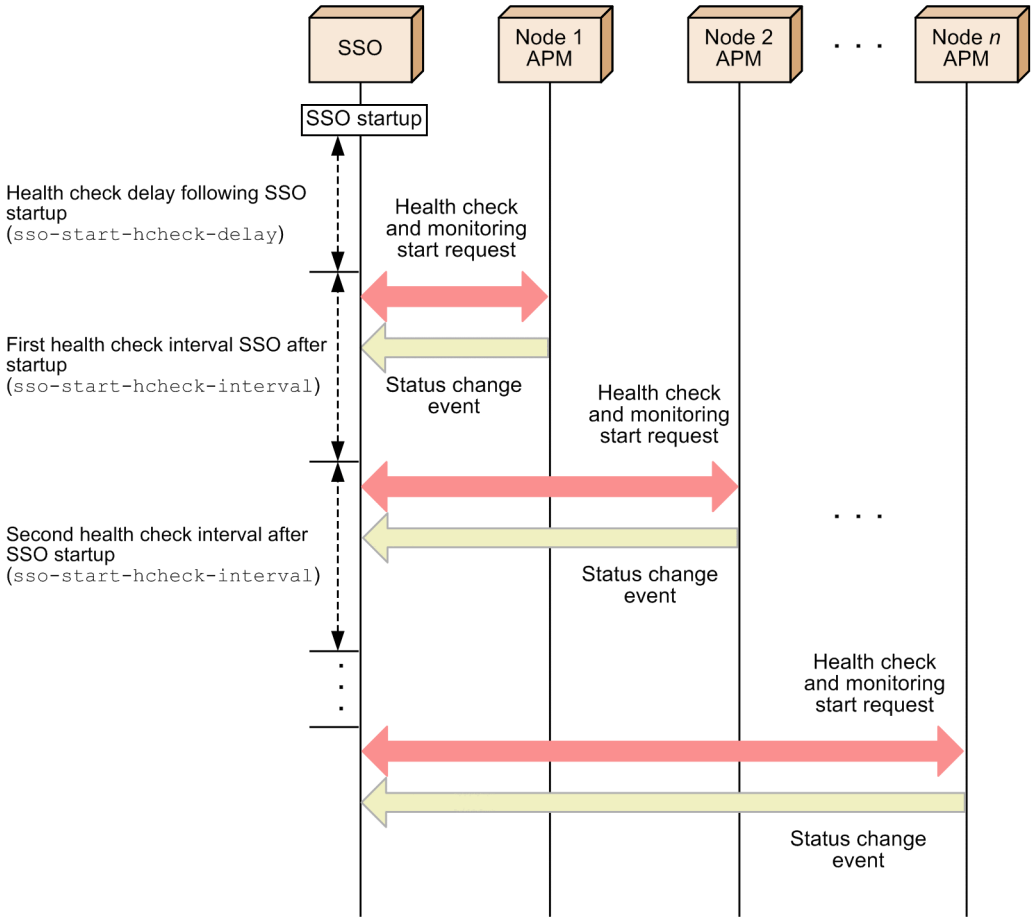
(a) System health check at SSO startup

The monitoring manager might be in a high load state when SSO starts. In such a high load state, if a health check is conducted on all the monitoring servers, a communication overload might occur when, for example, the monitoring manager receives monitoring start requests, causing the health check to fail. To prevent such health check failures, you can specify settings that delay the start of health checks or that conduct health checks sequentially for a certain group of monitoring servers. The relevant settings are the following keys in the `ssoapmon` action definition file (`ssoapmon.def`):

- `sso-start-hcheck-delay`
- `sso-start-hcheck-interval`
- `sso-start-hcheck-unit`

The figure below shows an overview of conducting system health checks at SSO startup. The operations instructed by the above-listed keys are described in this figure. Note that this figure is an example of when `sso-start-hcheck-unit` is set to 1 and a health check is performed for each APM.

Figure 2-52: Overview of system health checks conducted at SSO startup



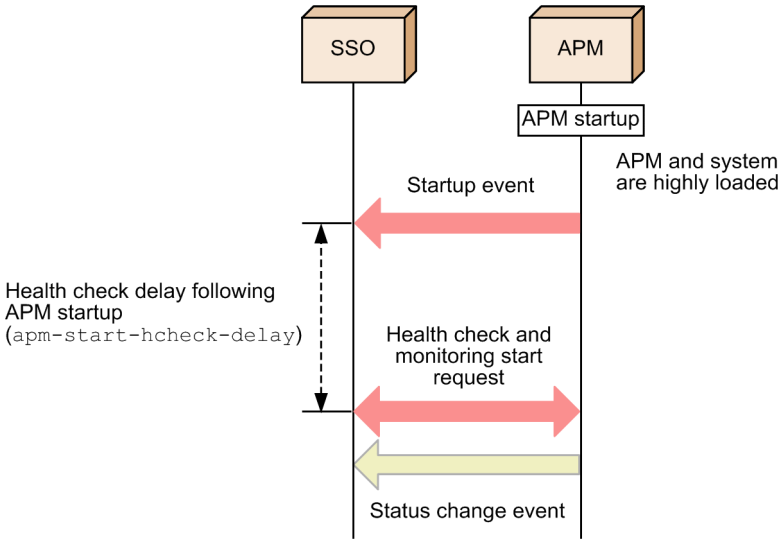
The system health checks conducted at SSO startup notify SSO of the states of all the processes and services monitored on the monitoring servers as events.

By setting an interval time for system health checks at SSO startup, you can distribute monitoring start requests to the monitoring servers, making it possible to distribute the load of receiving status change events from the monitoring servers. You can also distribute the NNMi processing load caused by issuance of incidents.

(b) System health check at APM startup event reception

When APM starts, it issues a startup event to SSO. After receiving the event, SSO runs a health check on APM following the lapse of the health check delay time at APM startup. The delay time is specified in the `ssoapmon` action definition file. The following figure shows the overview of a system health check when an APM startup event is received.

Figure 2-53: Overview of a system health check conducted at APM startup



After receiving an APM startup event, SSO conducts a health check on the target monitoring server. When the health check finishes, the statuses of all monitored processes and services are reported to SSO as events.

APM or the whole machine might be in a high load state when the monitoring server starts. In this case, response to the health check might be delayed, causing the health check to fail. You can avoid health check failure by setting a delay time for starting of the health check at APM startup.

(2) Regular health check

A regular health check means a health check that SSO periodically executes.

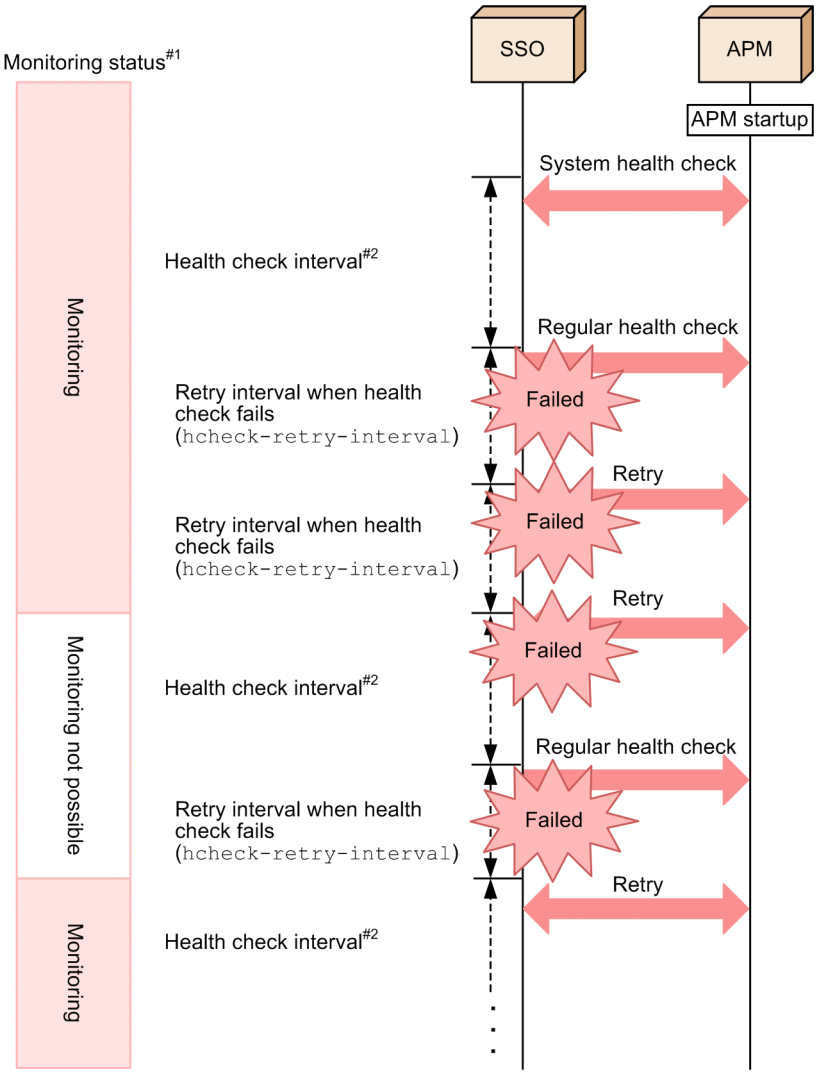
To enable regular health checks, set a health check interval either from the Set Health Check Interval window or in the `hcheck` key in the monitoring server definition file.

(a) Health check retry function

SSO periodically executes a regular health check. At such times, if the monitoring server is in a high load state, response from APM might be delayed. If this delay leads to a timeout, the health check will fail. To prevent the health check from failing in such a situation, use the health check retry function. You can set this function to retry execution of the health check when the health check temporarily fails.

If a regular health check fails, the health check is retried the number of times set for `hcheck-retry-count` in the `ssoapmon` action definition file. If the health check fails even after the set number of retries, the status of APM processes and services becomes *Unknown*. When a health check fails, its execution is retried at the time interval set to `hcheck-retry-interval` in the `ssoapmon` action definition file. The following figure shows an overview of retrying a health check.

Figure 2-54: Overview of retrying a health check



#1

For details on the monitoring status, see *2.5.2(1) Monitored status management*.

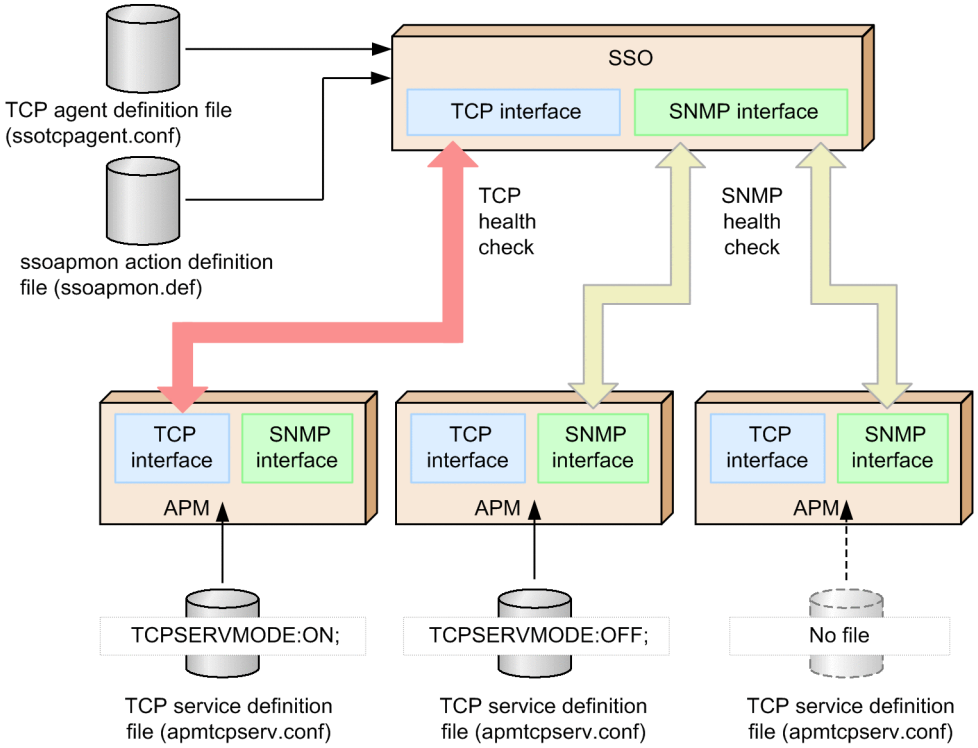
#2

This is the health check interval that can be set in the Set Health Check Interval window.

(b) Communication protocols of a regular health check

By default, regular health checks use communication via the SNMP (UDP) protocol. However, by enabling the TCP health check function, you can perform health checks with the highly reliable TCP protocol. The communication method for regular health checks can be selected according to the monitoring server. The following figure shows an example of a system that uses both of these protocols for health checks.

Figure 2-55: Example of a system that uses two communication protocols for health checks



As shown in the above figure, some definition files are required for enabling the TCP health check function. Make sure that the necessary definition files are created and set up on both the monitoring manager (SSO side) and the monitoring server (APM side) as shown below.

- On the monitoring manager (SSO side)
  Set up the TCP agent definition file (`ssotcpagent.conf`). In addition, if necessary, adjust the value of the `connect-retry-interval:` key in the `ssoapmon` action definition file (`ssoapmon.def`).
- On the monitoring server (APM side)
  Set up the TCP service definition file (`apmtcpserv.conf`). Setting up this file is unnecessary on monitoring servers that are not subject to TCP health checks.

(3) On-demand health check

On-demand health checks refer to health checks that are performed at the timing chosen by the user. You can conduct health checks on monitoring servers by executing the `ssoapcom` command with the `-H` option set.

2.5.6 Methods for receiving events from APM in the basic configuration

SSO in the basic configuration can receive events from APM by using one of two event reception methods:

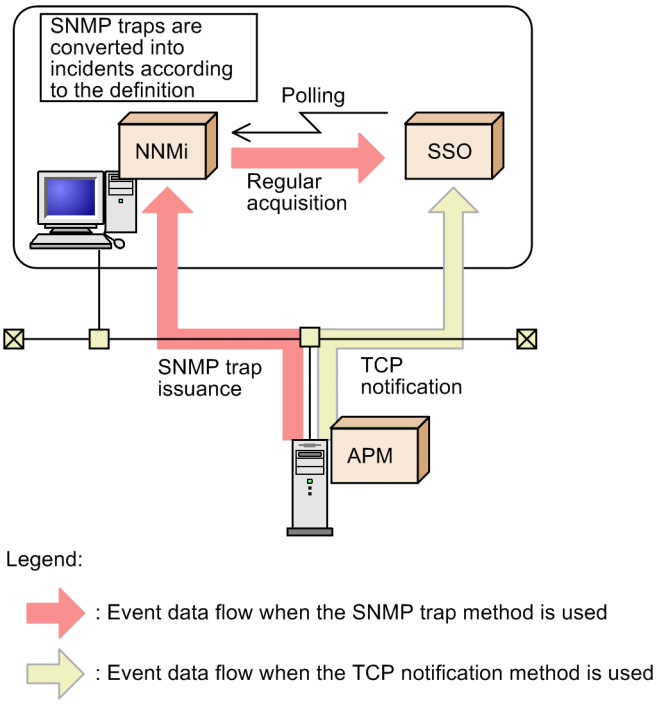
- TCP notification method
  This is the default reception method, under which SSO receives events directly from APM.
- SNMP trap method
  APM sends SNMP traps to NNMi, and NNMi converts them into incidents. After that, SSO periodically polls NNMi to receive the incidents.#

#:

By default, SSO polls NNMi once every five seconds. You can change the polling interval with the `apm-incident-check-interval:` key in the `ssoapmon` action definition file (`ssoapmon.def`). For details, see *6.3.7 ssoapmon action definition file (ssoapmon.def)*.

The following figure shows the data flow during event reception from APM in the basic configuration.

Figure 2-56: Data flow during event reception from APM (basic configuration)



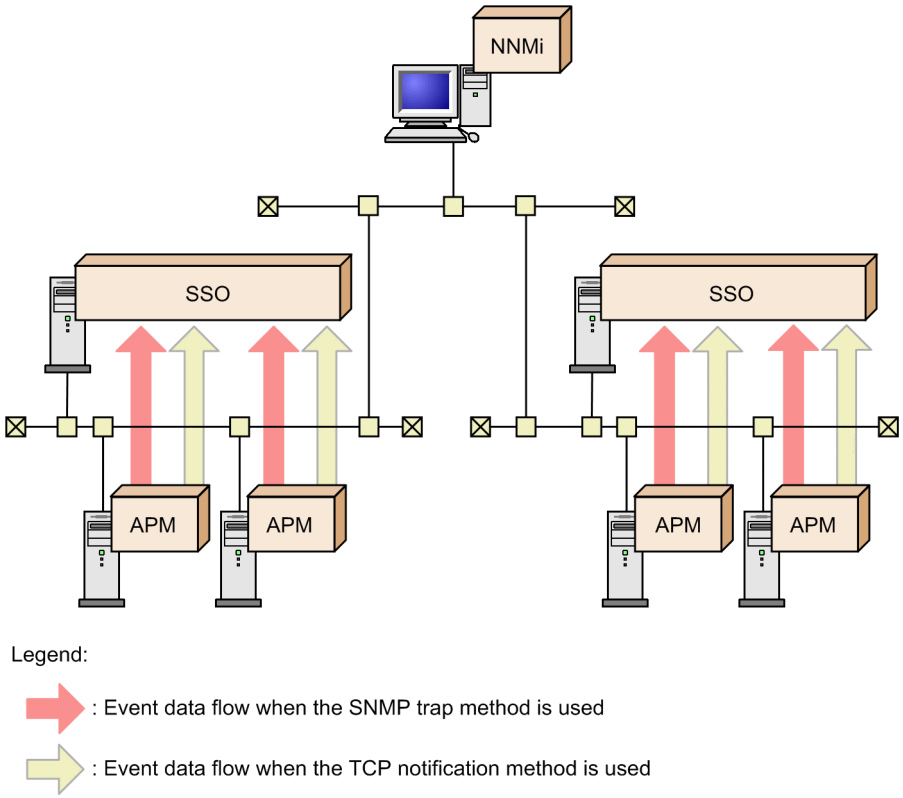
2.5.7 Methods for receiving events from APMs in a distributed configuration

SSOs in a distributed configuration can receive events from APMs by using one of two event reception methods:

- TCP notification method
  This is the default reception method, under which each SSO receives events directly from APMs.
- SNMP trap method
  Each SSO receives SNMP trap notifications directly from APMs.

The following figure shows the data flow during event reception from APMs in a distributed configuration.

Figure 2-57: Data flow during event reception from APMs (distributed configuration)



Legend:

: Event data flow when the SNMP trap method is used

: Event data flow when the TCP notification method is used

2.6 NNMi cooperation functions

SSO provides the following four NNMi link functions:

- Incident cooperation (event cooperation)

  This function allows SSO to issue incidents to NNMi and to detect events sent from APM.
- Incident cooperation (action cooperation)

  This function allows the user to display an incident graph in the incident view of the NNMi console. After selecting the **Action** menu or right-clicking in the incident view, when the user selects an SSO action, the incident graph is displayed according to the selected action.
- Map cooperation (symbol cooperation)

  This function registers the statuses of resources, processes, and services monitored by SSO in NNMi as NNMi-specific statuses. This function allows the user to check the monitoring statuses of SSO in the NNMi map view.
- Map cooperation (action cooperation)

  This function allows the user to display a monitoring status or open a window by selecting an SSO action from the **Action** menu in the NNMi console window. By using this function, the user can check monitoring statuses or manipulate windows without logging in to the SSO console.

The following three conditions must be met before the NNMi cooperation functions can be used:

- The monitoring manager# and monitoring server have been detected by NNMi (regardless of the mode in which they are managed by NNMi).

  #:

  The monitoring manager needs to be detected only when the user uses map cooperation (action cooperation) by selecting the node symbol for the monitoring manager.
- The IP address of the monitoring server is managed by the IP address inventory of NNMi or the SNMP agent inventory.
- The monitoring server is managed by NNMi when all of the following conditions are met:
  - The basic configuration (SSO and NNMi run on the same server) is used.
  - The process and service monitoring function is used.
  - The event notification method of APM is the SNMP trap method (rather than the TCP notification method).

If the IP addresses of the monitoring manager and another host are the same, and both IP addresses are registered in the NNMi IP address inventory, the following functions might not be able to operate correctly:

- Map cooperation functions (action cooperation functions) used by selecting the node symbol for the monitoring manager
- An issuance of an incident by using the `ssodbcheck` command

SSO periodically checks whether the monitoring server is detected by NNMi (whether cooperation is possible). For details, see *2.6.5 Checking whether NNMi cooperation is possible*.

2.6.1 Incident cooperation (event cooperation)

This function notifies NNMi of events that occur during collection of resources and monitoring of processes and services. You can also notify NNMi on another node by setting the destination in the event destination definition file (`ssodest.conf`).

For the monitoring of processes and services in the basic configuration, the environment settings must be specified so that SNMP trap events[#1] issued by APM are received by NNMi[#2].

When NNMi receives SNMP traps, it converts them into incidents that SSO can handle. When SSO detects these incidents by regular polling[#3], SSO can detect events that occurred in APM.

For details on incidents reported by SSO, see *F.1 Events (incidents) that are issued by SSO*.

#1:

In cases where `TCPSMODE` is set to `OFF` in the event TCP notification definition file (`apmtcpsend.conf`).

#2:

Setting #2 in *Table 3-1* must be specified.

In addition, the monitoring service for monitoring processes and services must be managed by NNMi.

#3:

The polling interval is defined for `apm-incident-check-interval` in the `ssoapmon` action definition file (`ssoapmon.def`).

Note

The status change events that occur when the status of the `ssoapmon` and `ssocolmng` daemon processes is `DEGENERATING` are not sent to NNMi even when the status later changes to `RUNNING`.

2.6.2 Incident cooperation (action cooperation)

The incident cooperation (action cooperation) function allows the user to display an incident graph in the incident view of the NNMi console. After selecting the **Action** menu or right-clicking in the incident view, when the user selects an SSO action, the incident graph is displayed according to the selected action.

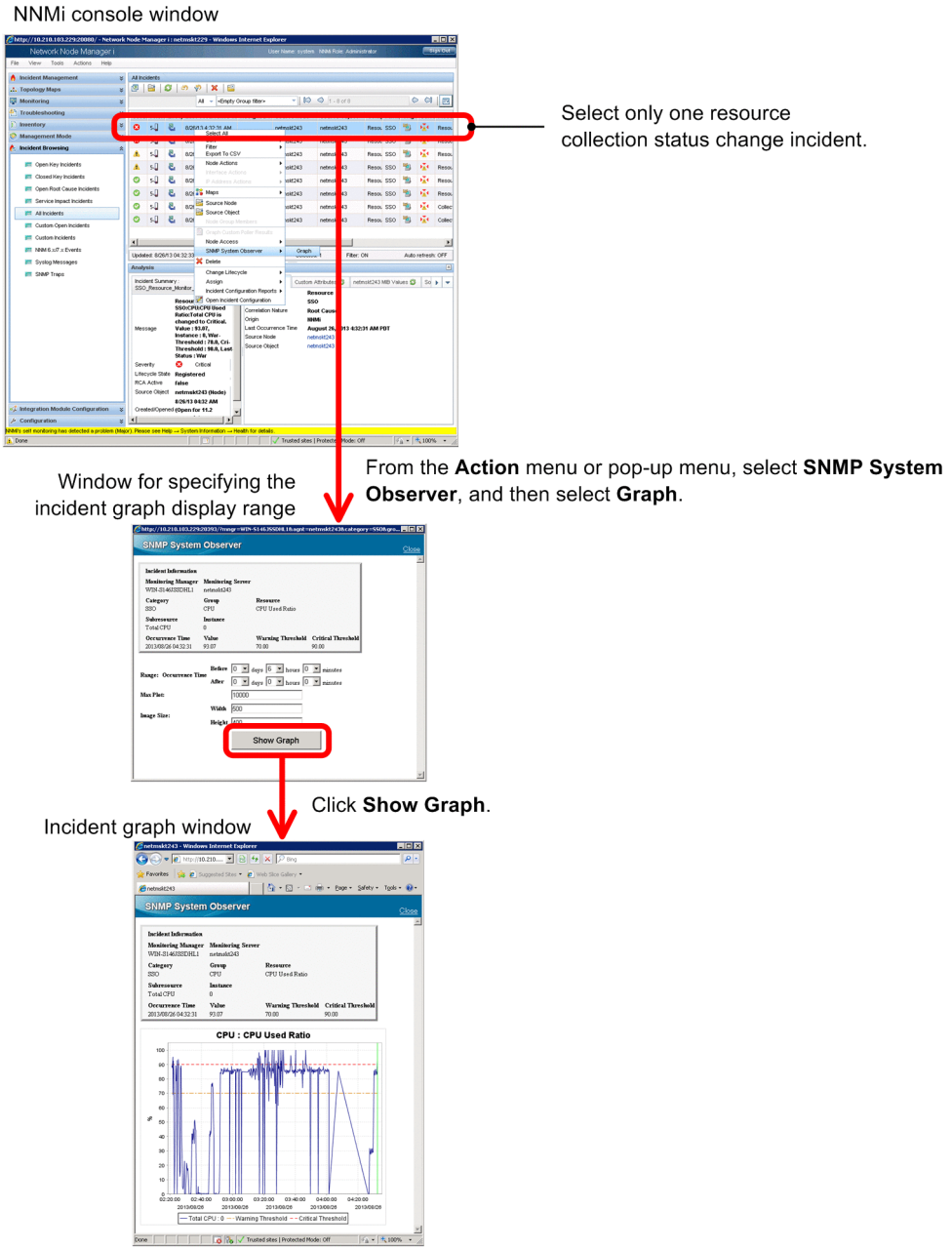
(1) Incident graph display

A graph of data collected before and after issuance of a resource collection status change incident is called an *incident graph*. This graph allows the user to check the transition of data collected before and after issuance of that incident.

To display the window for specifying the incident graph display range, in the NNMi console window, select a resource collection status change incident, and then select the **Action** menu or right-click that incident to display a pop-up menu. Next, select **SNMP System Observer**, and then select **Graph**. In the window that appears, specify the range of data to be displayed in a graph, and then click **Graph**. The incident graph window opens, displaying a graph of data in the specified range.

The following figure shows examples of the NNMi console window, the window for specifying the incident graph display range, and the incident graph window.

Figure 2−58: Examples of the NNMi console window, the window for specifying the incident graph display range, and the incident graph window



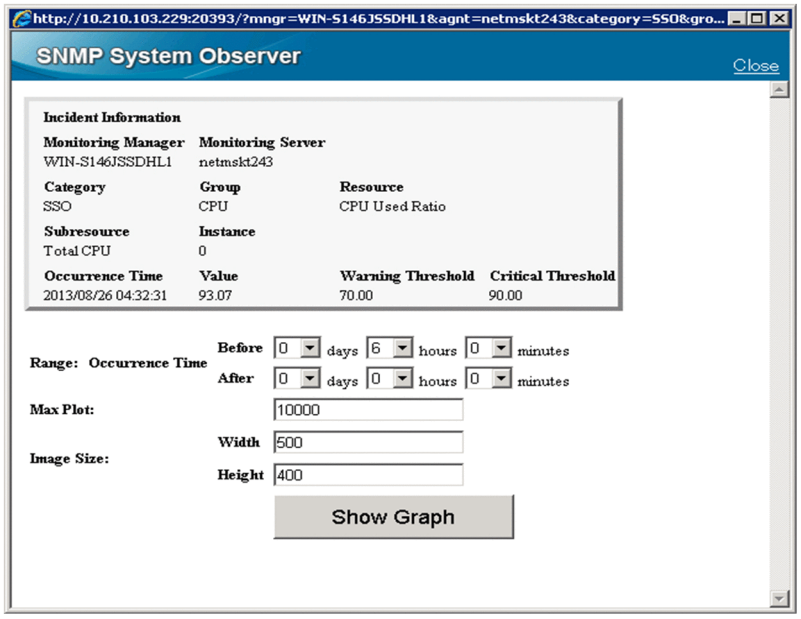
The incident graph window is used only for actions that are executed from the NNMi console, and cannot be displayed from the menu of the SSO console.

(a) Window for specifying the incident graph display range

In the window for specifying the incident graph display range, specify the range of data to be displayed in a graph.

The following figure shows the window for specifying the incident graph display range.

Figure 2-59: Window for specifying the incident graph display range



The items displayed in the above window are described below.

Incident Information area

The following items are displayed in this area as the information about the selected incident:

- **Monitoring Manager**
- **Monitoring Server**
- **Category**
- **Group**
- **Resource**
- **Subresource**
- **Instance**
- **Occurrence Time**
- **Value**
- **Warning Threshold**
- **Critical Threshold**

Range: Occurrence Time

Specify the range of the data to be displayed on the graph.

Before

Specify the extent to which data before the incident occurrence time is to be displayed on the graph, by using the drop-down lists for selecting the number of days, the number of hours, and the number of minutes.#1, #2, #3

After

Specify the extent to which data after the incident occurrence time is to be displayed on the graph, by using the drop-down lists for selecting the number of days, the number of hours, and the number of minutes.#1, #2, #3

Max Plot

Specify the maximum number of plots. The number of plots refers to the number of collection data items in the specified range.#1, #2, #3

Image size

Width

Specify the width of the graph image to be displayed.#2, #3

Height

Specify the height of the graph image to be displayed.#2, #3

Show Graph

Opens the incident graph window.

#1:

The displayed graph covers the period in which collection data exists in the following range:

From: Incident occurrence time minus the value specified for **Before**

To: Incident occurrence time minus the value specified for **After**

Note, however, that the number of data items to be plotted cannot exceed the value specified for **Maximum number of plots**.

For details, see *(3) Notes*.

#2:

The value ranges that can be specified in the drop-down lists and text boxes are as follows:

- **days**: 0 to 30
- **hours**: 0 to 23
- **minutes**: 0 to 59
- **Max Plot**: 1 to 20,000
- **Width**: 320 to 1,024
- **Height**: 240 to 768

#3:

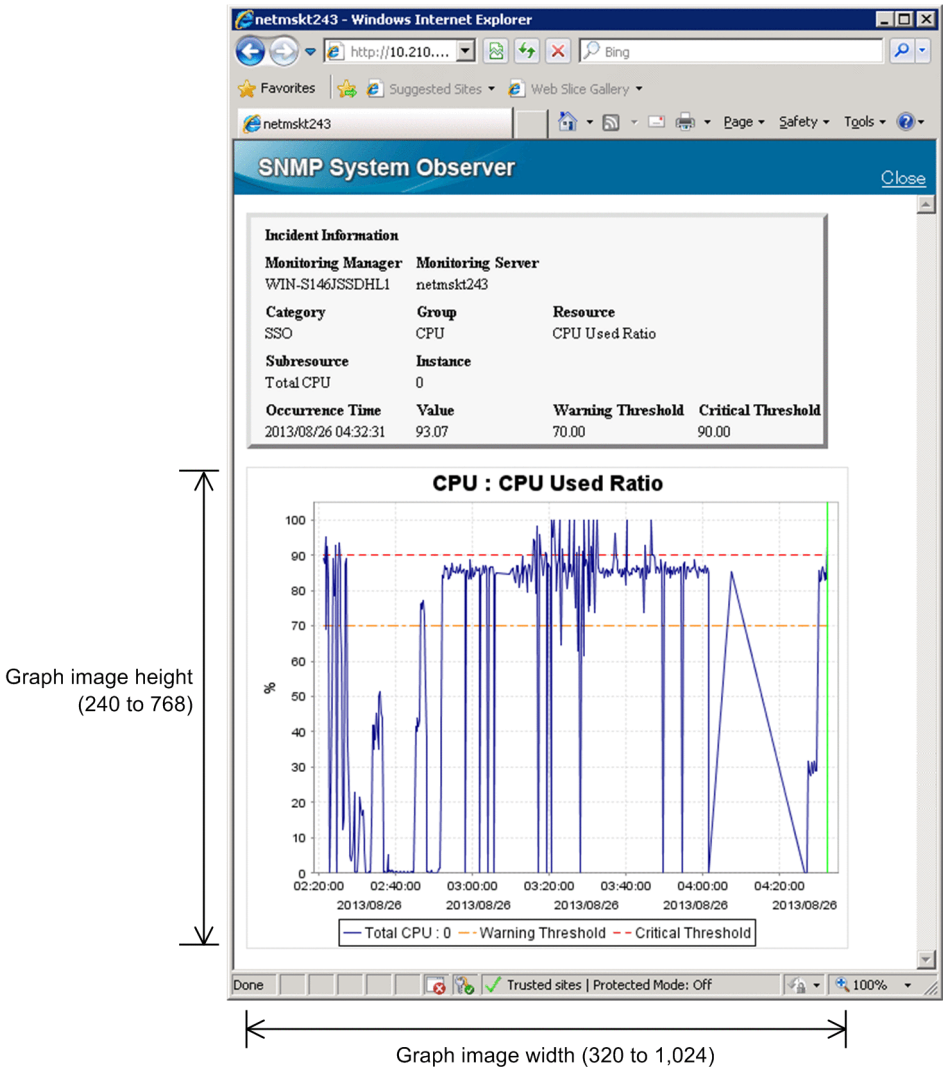
The initial values can be set in the NNM action definition file. For details on this file, see *6.3.30 NNM action definition file (ssonnmaction.conf)*.

(b) Incident graph window

The incident graph window displays a graph of the data in the range specified in the window for specifying the incident graph display range.

The following figure shows the incident graph window.

Figure 2-60: Incident graph window



The items displayed in the above window are described below.

Incident Information area

The following items are displayed in this area as the information about the selected incident:

- **Monitoring Manager**
- **Monitoring Server**
- **Category**
- **Group**
- **Resource**
- **Subresource**
- **Instance**
- **Occurrence Time**
- **Value**
- **Warning Threshold**
- **Critical Threshold**

Graph area

This area displays a graph image in PNG format.

The title of the graph, the vertical axis (data values and unit), the horizontal axis (time and date[#1]), and the introductory notes on the lines[#2] are also displayed.

The graph displayed in this area is a line graph on which the following three lines are drawn:

- Collection data
- Warning threshold (value at incident occurrence)
- Critical threshold (value at incident occurrence)

The graph display range is determined by the range specified in the window for specifying the incident graph display range and the maximum number of plots. For details, see *(3) Notes*.

In addition to the above lines, a vertical line that indicates the incident occurrence time is displayed.

The vertical and horizontal axes are scaled automatically according to the display range of the graph.

The image displayed in this area is assigned a name in the following format (where the incident occurrence time is indicated in *YYYYMMDDhhmmss* format):

```
incgraph_resource-ID_subresource-ID_incident-occurrence-time
```

For example, if the resource ID is 32, the subresource ID is 1, and the incident occurrence time is 13:27:24 on 2012-01-25, the name of the image is as follows:

```
incgraph_32_1_20120125132724
```

#1:

The time and date at the right end of the horizontal axis of the graph might be incompletely displayed.

#2:

If the introductory notes on lines are long and extend beyond the width of the graph image, only the part that fits within the graph image width is displayed.

(2) Action menu access rights

The action menu access rights are controlled by the NNMi roles. The role required for executing an action differs according to the menu item. The following table lists the role set by default.

Table 2-13: Default role

Menu item	Role
Graph	Operator level 1

The NNMi role required for execution can be changed according to the operation. To change the role, change the role of the menu item in question from the NNMi console. For details, see the NNMi console's Help.

One of the following roles can be selected:

- Administrator
- Operator level 1
- Operator level 2

Note

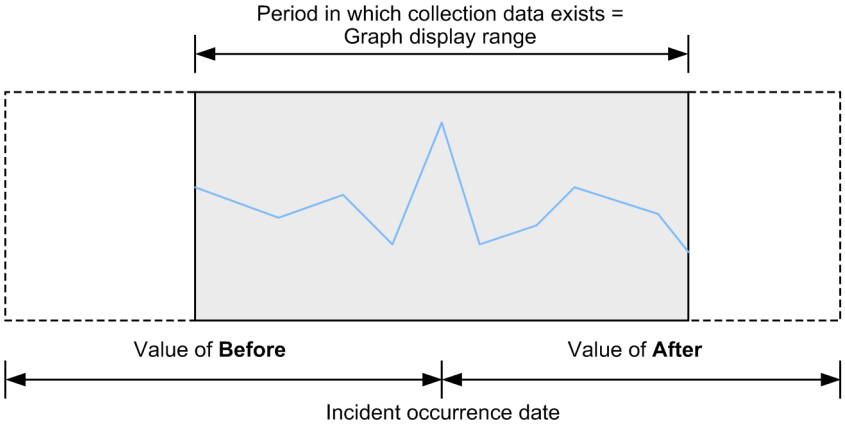
The role is reset to the default role when the URL action definition file is re-imported to NNMi.

(3) Notes

- Graph display range

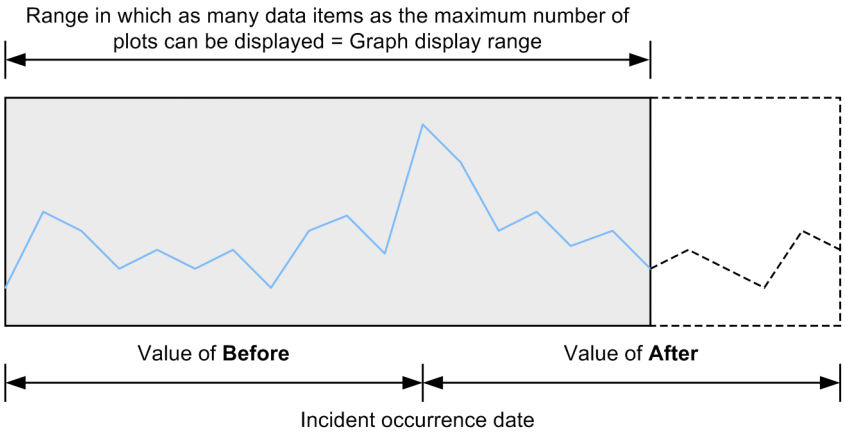
  The graph display range is the period within the specified range in which collection data exists. The following figure shows an example of this.

  Figure 2-61: Example of the graph display range (from the viewpoint of the period in which collection data exists)



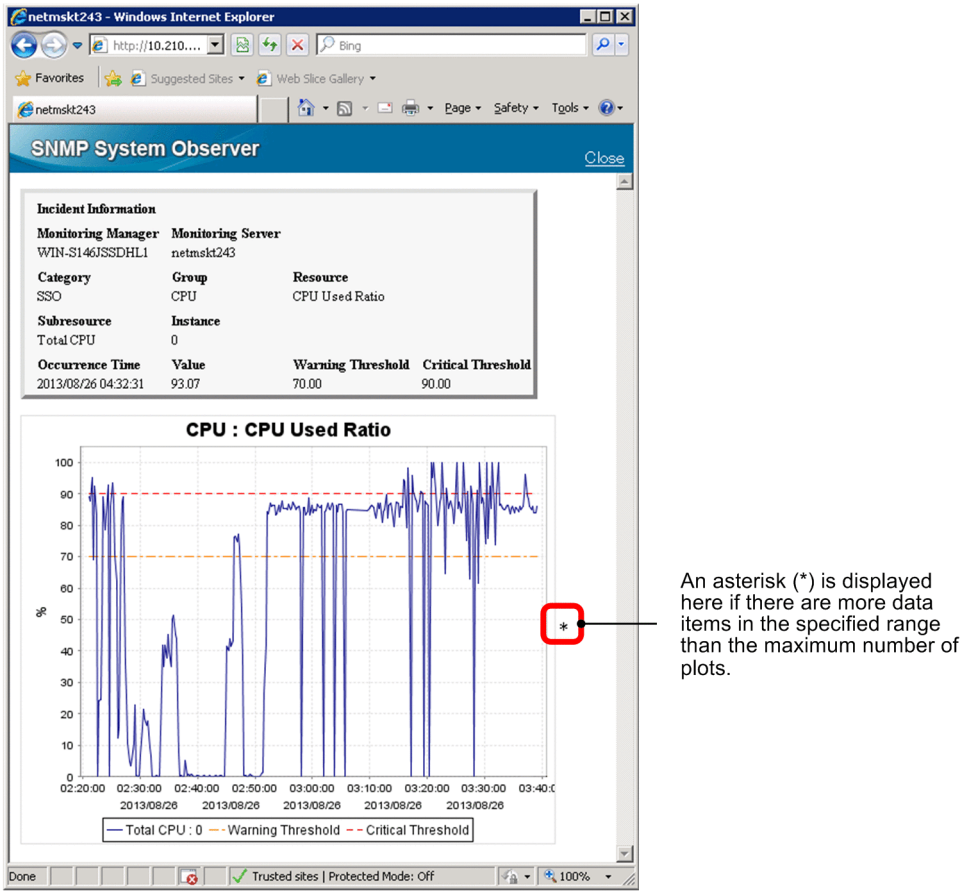
  If the number of collection data items in the specified range exceeds the maximum number of plots, only as many collection data items as the maximum number of plots are displayed on the graph. The following figure shows an example of this.

  Figure 2-62: Example of the graph display range (from the viewpoint of the maximum number of plots)



  If the number of collection data items in the specified range exceeds the maximum number of plots, an asterisk (*) is displayed at the right edge of the graph. The following figure shows a display example of this.

Figure 2-63: Example of displaying a graph when the maximum number of plots is exceeded



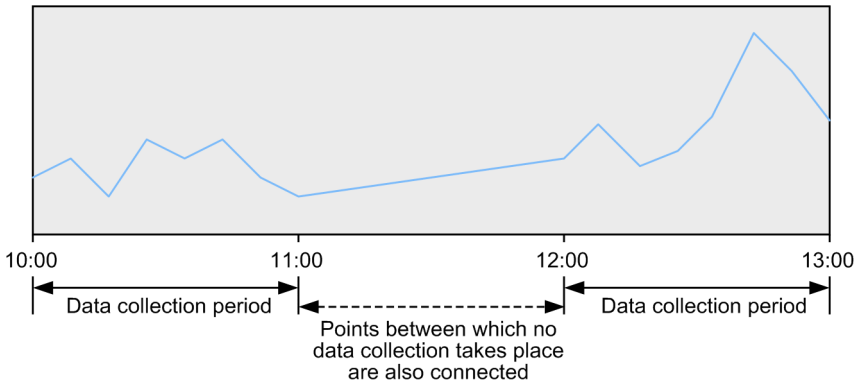
- Drawing of graph lines

  A single continuous line is always drawn along plots without consideration for continuity of plots.

  The figure below shows an example of a graph for data collected from 10:00 to 13:00 under the following conditions:

  - Resource collection starts at 10:00, and stops at 11:00.
  - Resource collection starts at 12:00, and stops at 13:00.

  Figure 2-64: Example of drawing a line



  In this example, a line is drawn throughout the graph display range even though no data was collected during the period from 11:00 to 12:00.

- If the incident graph is displayed after the value of `ssoconsoleweb` in the port number definition file (`ssoport.conf`) is changed

  If the value of `ssoconsoleweb` in the port number definition file (`ssoport.conf`) is changed after resource collection status change incidents occur, you can no longer display incident graphs for any incidents that occurred

before the change. You can display only incident graphs for resource collection status change incidents that occurred after the change.

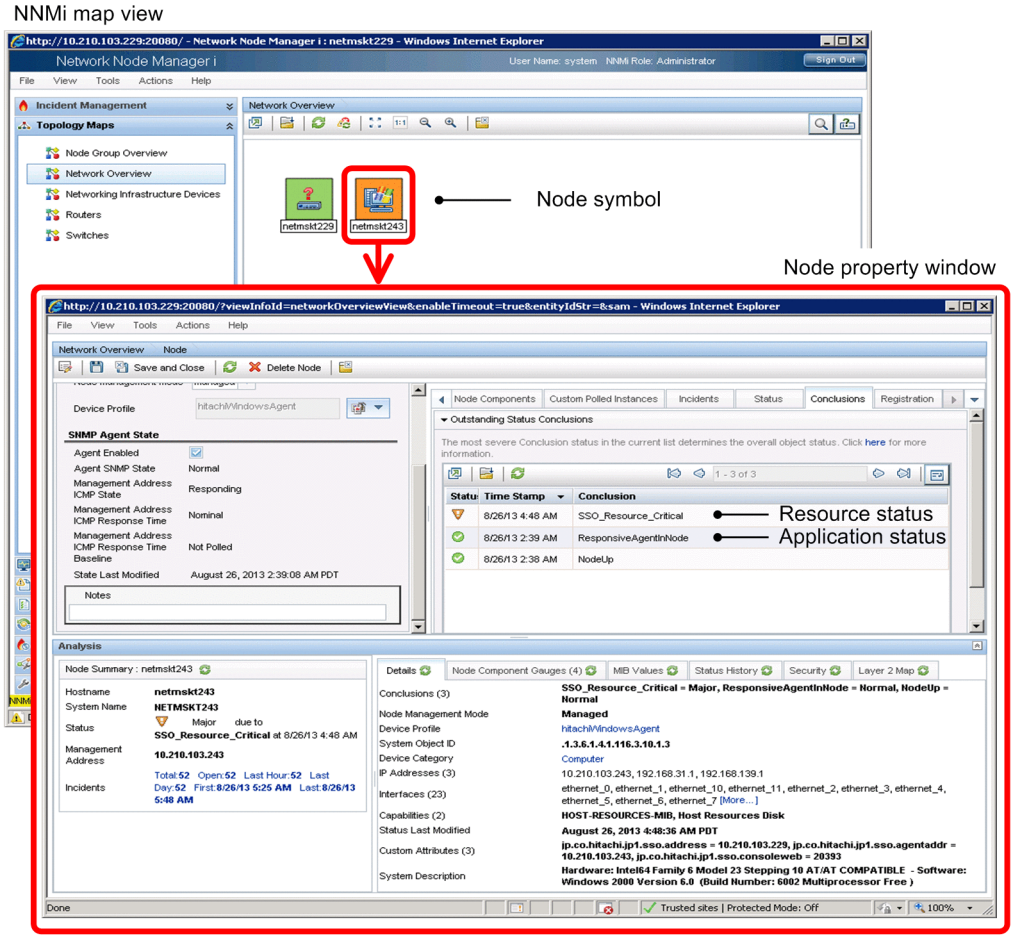
2.6.3 Map cooperation (symbol cooperation)

The map cooperation (symbol cooperation) function registers the resource status during resource collection (threshold monitoring) and the application status (process and service monitoring) in NNMi for each node symbol in the NNMi map view. The statuses registered in NNMi are associated with *Normal*, *Warning*, *Critical*, or *Unknown* status in SSO. The registered statuses allow users to visually understand the monitoring statuses in SSO by the color of the node symbol in the NNMi map view. This function is especially useful for checking for monitoring servers in *Warning* or *Critical* status.

This function can also be used for NMMi on another host by using the event destination definition file (`ssodest.conf`).

The following figure shows examples of the NNMi map view and the node property window.

Figure 2-65: NNMi map view and the node property window



If the resource status and application status that reflect the statuses managed in SSO are registered in NNMi, the node symbols in the NNMi map view are displayed in green, yellow, blue-green, orange, or red according to the status. Note that if different statuses are displayed in the node property window, the color for the most severe status is applied to the node.

For details on the correspondence between the statuses managed in SSO and the statuses registered in NNMi, see *(2) Correspondence between the statuses managed in SSO and the severity statuses registered in NNMi*.

For details on how the node symbol colors and the statuses of NNMi are determined, see *(3) How the statuses registered in NNMi are determined*.

(1) Map cooperation (symbol cooperation) operating conditions

(a) Status registration conditions

When all of the following conditions are met, the resource and application statuses managed in SSO are added as severity statuses to the properties of nodes displayed in the NNMi map view:

- NNMi cooperation is possible.
- In the `ssoapmon` action definition file (`ssoapmon.def`) or `ssocolmng` action definition file (`ssocolmng.def`), the value of the `nnm-map-coop:` key is `on`.
- Threshold monitoring is enabled (for resource collection only).
- The initial resource status or application status after start of collection (monitoring)# has been determined.

#:

This includes the case where the `ssocolmng` or `ssoapmon` daemon process is stopped without collection (monitoring) being stopped, and that collection automatically resumes when the daemon process is restarted.

(b) Status update conditions

While the status registration conditions in *(a)* above are met, the status is updated when either of the following events occurs:

- The resource status or application status changes.
- The `ssomapstatus -sync` command is executed.

For details on the `ssomapstatus` command, see *ssomapstatus* in *5. Commands*.

(c) Status deletion conditions

The statuses registered as properties of nodes in the NNMi map view are deleted when any of the following events occurs:

- Collection (monitoring) stops.#
- The collection status changes to *Standing by* or *Impossibility*.
- Threshold monitoring is disabled (for resource collection only).
- The `ssomapstatus -del` command is executed.

#:

This includes the case where collection (monitoring) conditions are deleted and the case where the daemon process is stopped.

For details on the `ssomapstatus` command, see *ssomapstatus* in *5. Commands*.

(d) Behavior when NNMi cooperation becomes impossible

When NNMi cooperation becomes impossible, the statuses registered as properties of nodes in the NNMi map view remain as they are, and when NNMi cooperation becomes possible again, these statuses are updated. However, if you delete collection conditions while NNMi cooperation is impossible, the statuses corresponding to the deleted collection conditions are left undeleted. If such statuses remain, delete them by using the `ssomapstatus -del` command. For details on the `ssomapstatus` command, see *ssomapstatus* in *5. Commands*.

(e) Status registration, update, and deletion

Status registration, update, and deletion are executed regardless of the mode in which the node is managed by NNMi (*Managed*, *Not managed*, or *Service stopped*).

(2) Correspondence between the statuses managed in SSO and the severity statuses registered in NNMi

The following table describes the correspondence between the statuses managed in SSO and the severity statuses registered in NNMi.

Table 2-14: Correspondence between the statuses managed in SSO and the severity statuses registered in NNMi

Status managed in SSO		Status registered in NNMi	
Monitoring object	Monitoring status	Severity status#1	Result
Resource status	Normal	Normal	`SSO_Resource_Normal`
	Warning	Minor, warning#2, major, or critical	`SSO_Resource_Warning`
	Critical	Major or critical#2	`SSO_Resource_Critical`
	Unknown	Warning	`SSO_Resource_Unknown`
Application status	Normal	Normal	`SSO_Application_Normal`
	Warning	Minor, warning#2, major, or critical	`SSO_Application_Warning`
	Critical	Major or critical#2	`SSO_Application_Critical`
	Unknown	Warning	`SSO_Application_Unknown`

#1:

The following lists the node symbol colors corresponding to the respective statuses:

Normal: Green

Minor: Yellow

Warning: Blue-green

Major: Orange

Critical: Red

#2:

The *Warning* monitoring status in SSO can be associated with one of four severity statuses in NNMi. The *Critical* monitoring status in SSO can be associated with one of two severity statuses in NNMi. For details on how to specify the NNMi severity status to be associated, see the descriptions of the `map-status-warning:` key and the `map-status-critical:` key in *6.3.7 ssoapmon action definition file (ssoapmon.def)* and *6.3.8 ssocolmng action definition file (ssocolmng.def)*.

(3) How the statuses registered in NNMi are determined

Monitoring multiple resources or applications on a monitoring server means that you must manage multiple resource or application statuses for that server. However, if different resource statuses or application statuses exist on a monitoring server, only the most severe status is registered in NNMi as the resource status or the application status. The resource status or application status is determined as follows:

- The color for the most severe of the resource statuses or application statuses is applied to the node in the NNMi map view.#
- If multiple resources to be monitored exist on a monitoring server, the status of the resource in the most severe status is registered.
- If multiple applications exist to be monitored on a monitoring server, the status of the application in the most severe status is registered.
- The severity order of resource or application statuses is as follows: *Unknown* > *Critical* > *Warning* > *Normal*

#:

The statuses that are used to determine the node color include those that are registered by NNMi itself.

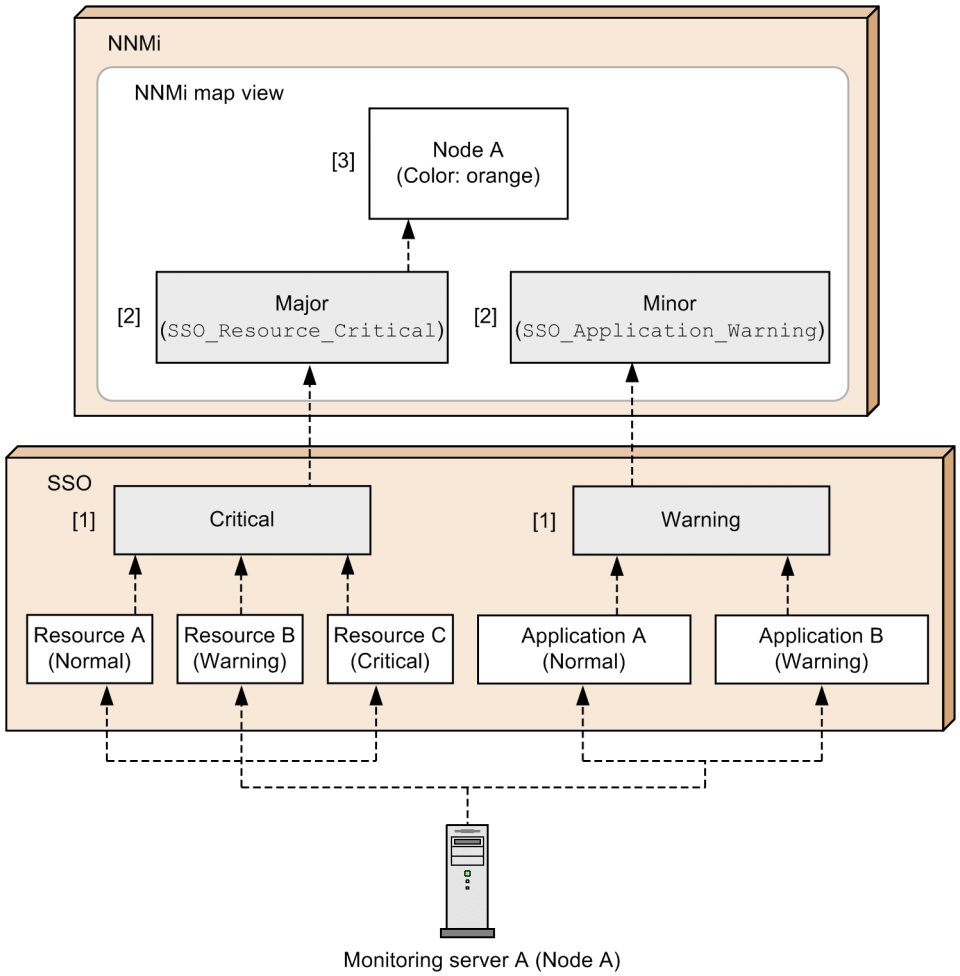
The following figure shows how the status registered in NNMi is determined.

Figure 2-66: How the status registered in NNMi is determined

[1]: The status is determined.

[2]: The corresponding status is registered in NNMi.

[3]: The color for the most severe status is applied to the node.



2.6.4 Map cooperation (action cooperation)

The map cooperation (action cooperation) function allows users to manipulate SSO without logging in to the SSO console, simply by selecting an SSO-provided action from the **Action** menu in the NNMi console window. For example, the monitoring status can be viewed from that menu.

The following two actions can be performed:

- Viewing the monitoring status
  This action displays the monitoring status display window. This window can be opened from only the NNMi console, and cannot be opened from the SSO console menu.
- Opening a window
  This action starts a window provided by the SSO console.

Note that the above windows can be opened when only one monitoring manager node symbol or monitoring server node symbol is selected. Multiple monitoring status display windows or other windows cannot be opened in a single action by selecting multiple node symbols.

For details on how to add the above listed actions to the **Action** menu of the NNMi console window, see *3.1 Installation and setup flowcharts*.

(1) Viewing the monitoring status

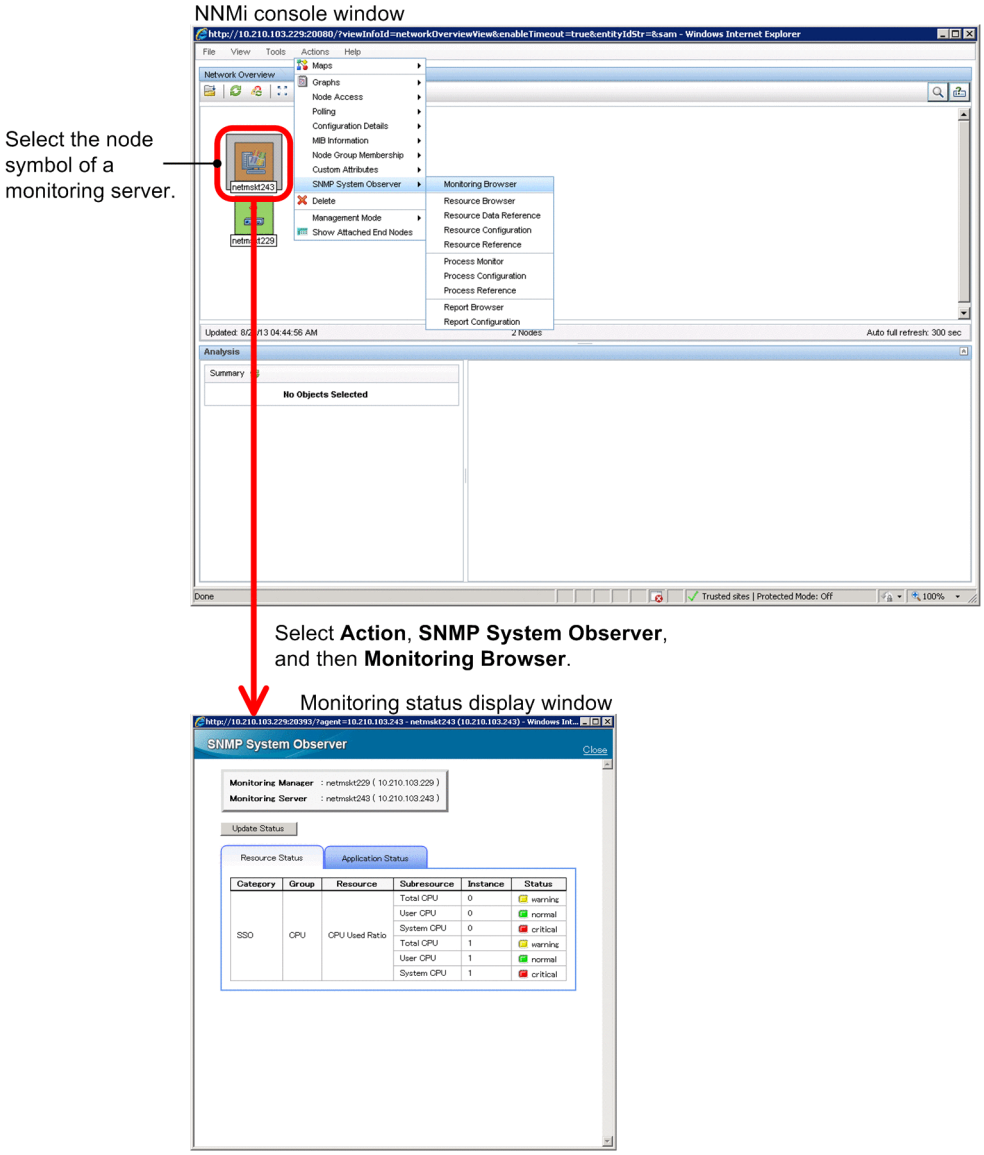
This subsection assumes that **View Monitoring Status** has been added under **SNMP System Observer** in the **Action** menu of the NNMi console window. By selecting **View Monitoring Status**, you can open the monitoring status display window that displays both the resource statuses during resource collection (threshold monitoring) and the application statuses (process and service monitoring).

If the map cooperation (symbol cooperation) function is being used, the node symbol color is updated every time the status associated with a status managed in SSO is registered. If you select a node and then select **View Monitoring Status**, you can check the status of that node without logging in to the SSO console. In this way, if the color of a node changes, you can easily find out the cause.

For details on the settings for opening the monitoring status display window, see *(4) Executing actions*.

The following figure shows examples of the NNMi console window and the monitoring status display window.

Figure 2-67: NNMi console window and the monitoring status display window



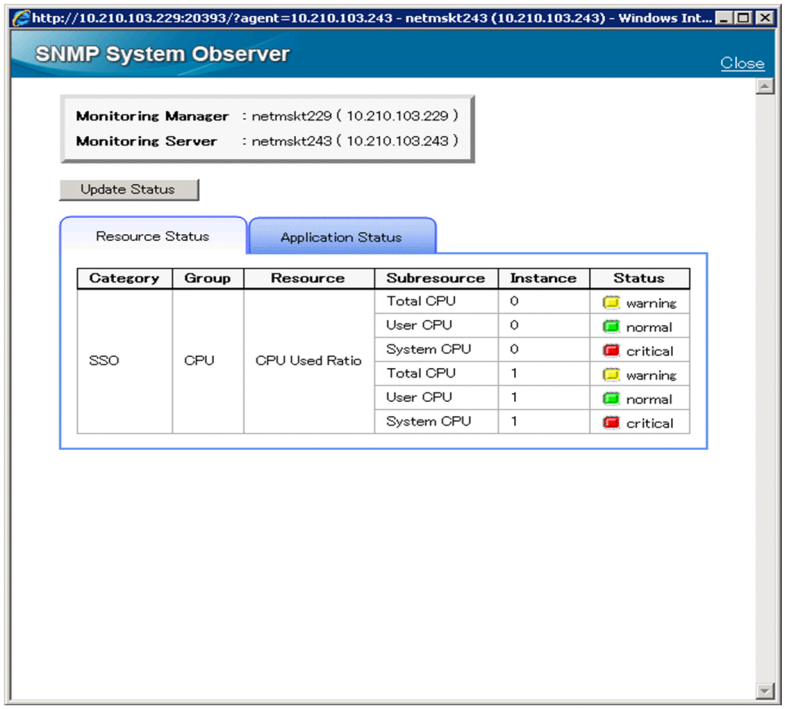
The following describes the monitoring status display window.

(a) Monitoring status display window

The monitoring status display window displays the resource statuses and application statuses, as well as the process statuses or service statuses.

The following figure shows the monitoring status display window.

Figure 2-68: Monitoring status display window



The items displayed in the above window are described below.

Monitoring Manager

Displays the host name and IP address of the monitoring manager.

Monitoring Server

Displays the host name and IP address of the monitoring server.

Update Status

Displays the latest monitoring status of SSO.

Resource Status tab

Select this tab to display the resource status. For details on the items displayed when the **Resource Status** tab is selected, see *(b) Viewing the resource status*.

Application Status tab

Select this tab to display the application status. For details on the items displayed when the **Application Status** tab is selected, see *(c) Viewing the application status*.

Important note

The monitoring status display window appears with the **Resource Status** tab selected when you select **View Monitoring Status** from the **Action** menu of the NNMi console window or click the **Update Status** button in the monitoring status display window.

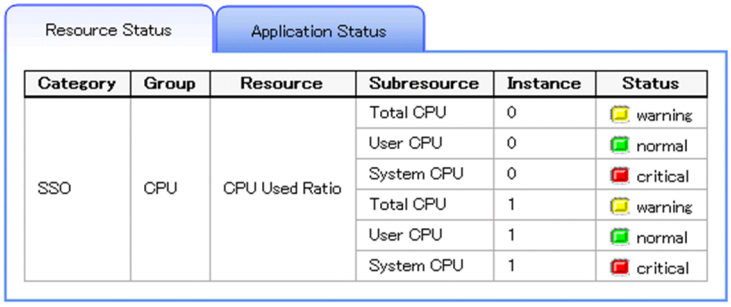
However, when only process monitoring or service monitoring is being performed, the monitoring status display window appears with the **Application Status** tab selected.

(b) Viewing the resource status

The **Resource Status** tab displays the resource status items (**Category**, **Resource Group**, **Resource**, **Subresource**, **Instance**, and **Status**).

The following figure shows an example of the selected **Resource Status** tab.

Figure 2-69: Example of the Resource Status tab



The items displayed in the above tab are described below.

Category

Displays categories.

Group

Displays resource groups.

Resource

Displays resources.

Subresource#

Displays subresources.

Instance#

Displays instances.

Status#

Displays resource statuses.

The following table lists the correspondence between icons and statuses.

Table 2-15: Icons and statuses

Icon	Resource status
(Green)	Normal
(Yellow)	Warning
(Red)	Critical
(blue)	Unknown

#:

For the resources whose values are not calculated, a hyphen (-) is displayed. Resource values are not calculated in the following cases:

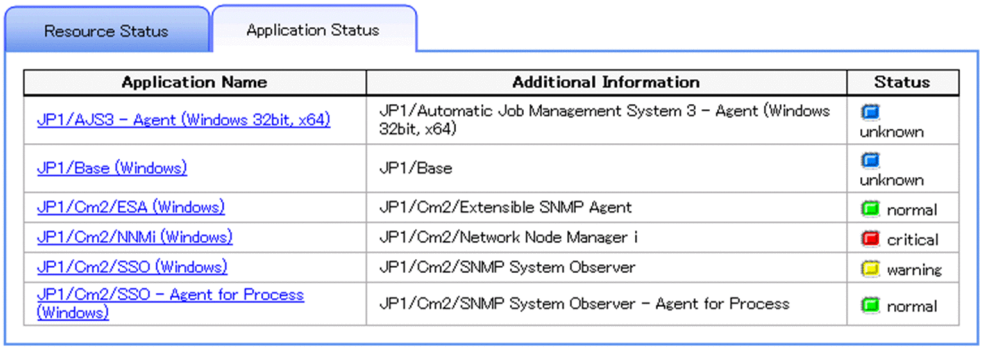
- Threshold monitoring is not being performed.
- Resource values have not yet been collected (for example, immediately after the start of collection).

(c) Viewing the application status

Selecting the **Application Status** tab displays the application status items (**Application Name**, **Additional Information**, and **Status**).

The following figure shows an example of the **Application Status** tab.

Figure 2-70: Example of the Application Status tab



The items displayed in the above tab are described below.

Application Name

Displays applications.

When one of the displayed applications is selected, depending on whether the process or service of the application is being monitored, the process status or service status is displayed.

For details on the process status and service status, see *(d) Viewing the process status and service status*.

Additional Information

Displays additional information about the application. If additional information has not been set, a hyphen (-) is displayed.

Status

Displays the application statuses.

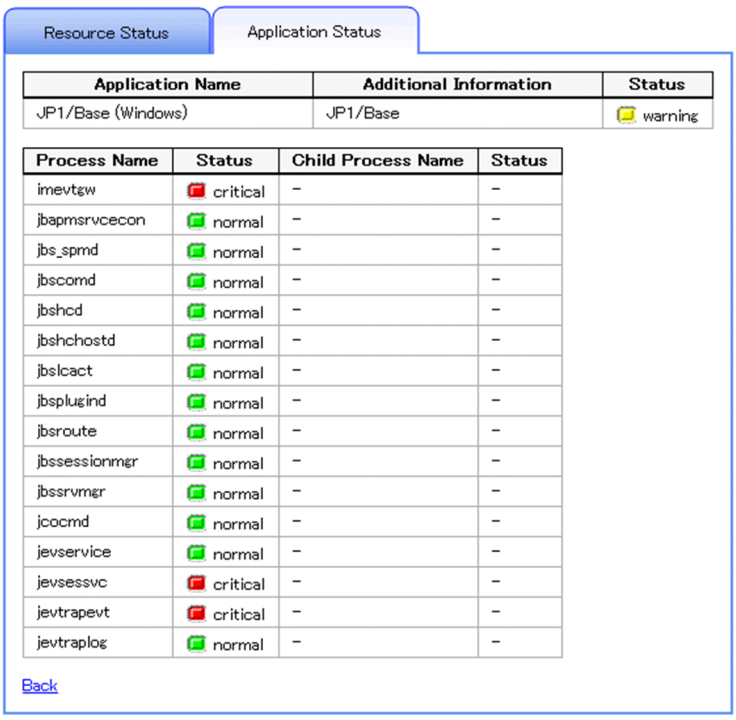
For the correspondence between icons and statuses, see *Table 2-15*.

(d) Viewing the process status and service status

For applications whose processes are being monitored, the process statuses are displayed. For applications whose services are being monitored, the service statuses are displayed.

The following figure shows an example of the **Application Status** tab when process statuses are displayed.

Figure 2-71: Example of the Application Status tab when process statuses are displayed



The items displayed in the above tab are described below.

Process Name

Displays monitoring processes.

Child Process Name

Displays monitoring child processes.

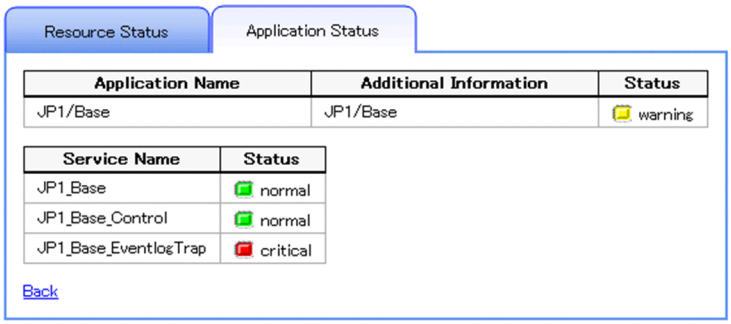
Status

Displays the monitoring process and monitoring child process statuses.

For the correspondence between icons and statuses, see *Table 2-15*.

The following figure shows an example of the **Application Status** tab when service statuses are displayed.

Figure 2-72: Example of the Application Status tab when service statuses are displayed



The items displayed in the above tab are described below.

Service Name

Displays monitoring services.

Status

Displays the monitoring service status.

For the correspondence between icons and statuses, see *Table 2-15*.

(e) Notes

The **Resource Status** tab and **Application Status** tab cannot display statuses when the `ssocolmng` daemon process and the `ssoapmon` daemon process are stopped.

(2) Opening a window

This subsection assumes that window names (such as **Resource Configuration**) have been added under **SNMP System Observer** in the **Action** menu of the NNMi console window. By selecting such a window name, you can remotely open and manipulate an SSO window. The following lists the windows that can be opened:

- Resource Browser window
- Resource Data Reference window
- Resource Configuration window
- Resource Reference window
- Process Monitor window
- Process Configuration window
- Process Reference window
- Report Configuration window
- Report Browser window#

#:

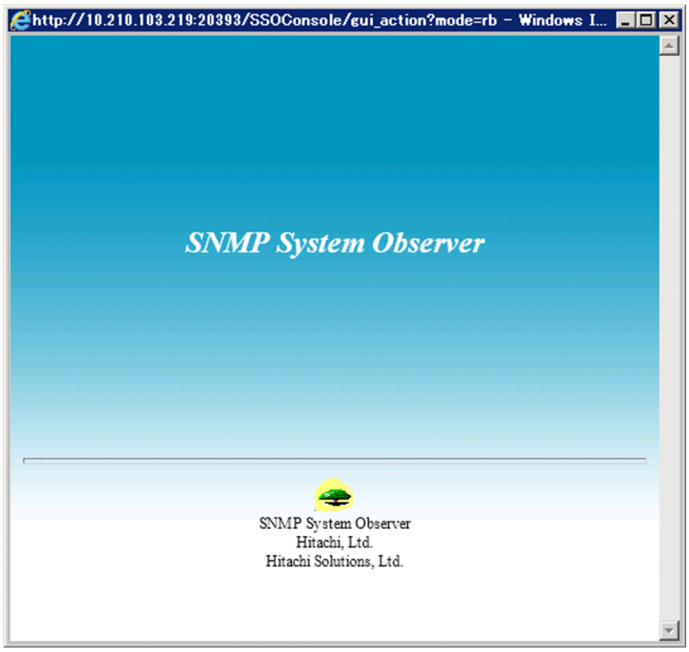
A list of the created report files is displayed.

The SSO that is remotely operated by opening a window differs depending on the node that is selected when the action is executed. If the selected node is a monitoring manager, the remotely-operated SSO is the SSO on the monitoring manager. If the selected node is a monitoring server, the remotely-operated SSO is the SSO that monitors the monitoring server.

Note

When you open a window (other than Report Browser), the following window also opens. If you close the following window, the parent window, which you want to manipulate, also closes. Therefore, while you are manipulating the window that you opened, do not close the following window.

After you finish manipulating the window and close it, make sure that you manually close the following window, which does not close automatically.



(3) Action menu access rights

The action menu access rights are controlled by the NNMi roles. The role required for action execution differs depending on the menu item. The following table lists the roles set by default for the menu items.

Table 2-16: Default roles of menu items

No	Menu item	Role#	
		Definition 1	Definition 2
1	**View Monitoring Status**	Operator level 1	Operator level 1
2	**Resource Browser**	Operator level 1	Operator level 1
3	**Resource Data Reference**	Operator level 1	Administrator
4	**Resource Configuration**	Administrator	Administrator
5	**Resource Reference**	Operator level 1	Administrator
6	**Process Monitor**	Operator level 1	Administrator
7	**Process Configuration**	Administrator	Administrator
8	**Process Reference**	Operator level 1	Administrator
9	**Report Configuration**	Administrator	Administrator
10	**Report Browser**	Operator level 1	Administrator

#:

The default role is set to either definition 1 or definition 2 according to the definition in the imported URL action definition file. For details on the URL action definition file, see *3.1.1 Flow of SSO installation and setup tasks*.

The NNMi role required for execution can be changed according to the operational requirements. To change the role, change the role of the menu item in question from the NNMi console. For details, see the NNMi console's Help.

You can select one of the following roles:

- Administrator

- Operator level 1
- Operator level 2

Note

When the URL action definition file is re-imported to NNMi, the role is reset to the default role.

(4) Executing actions

Before you can open the monitoring status display window and other windows as actions, you must specify the URLs of those windows in URL action definitions of NNMi.

From version 09-10, SSO supports distributed system configurations. To execute an SSO action from the **Action** menu, you must take into consideration the fact that the monitoring manager of each node might be different. Also, you must keep in mind that the URL of each window includes the IP address and port number of the monitoring manager. If the monitoring manager is different, the IP address and port number also are different. Therefore, the NNMi custom attribute function is used to hold the IP address and port number information of the monitoring manager for each node. By registering monitoring manager information as custom attributes, support for SSO in a distributed configuration is provided.

The following subsections describe NNMi custom attributes.

(a) Overview of custom attributes

When an action is executed on a node, the monitoring manager that manages the resource status and application status of that node must be identified. For the monitoring manager to be identified, you must register the information about the monitoring manager on the **Custom Attributes** tab in NNMi's node window for the target node. On that tab, specify the names and values of custom attributes.

The following table describes the names and values of the custom attributes to be registered.

Table 2-17: Information registered on the Custom Attributes tab

No	Name	Description
1	jp.co.hitachi.jp1.sso.address	IP address of the monitoring manager that monitors the target node (The IP address of the physical host or the IP address specified for the `change-my-address:` key. If the `ssonnmactaddr.conf` file exists, this item indicates the monitoring manager's IP address specified in the file.)
2	jp.co.hitachi.jp1.sso.agentaddr	IP address of the monitoring server
3	jp.co.hitachi.jp1.sso.consoleweb	Port number specified for `ssoconsoleweb` in the `ssoport.conf` file

The custom attributes that must be registered differ according to the node. The following table lists the custom attributes that must be registered for each node.

Table 2-18: Custom attributes that must be registered for each node

No	Custom attribute	Monitoring manager	Monitoring server
1	jp.co.hitachi.jp1.sso.address	Y	Y
2	jp.co.hitachi.jp1.sso.agentaddr	N#	Y
3	jp.co.hitachi.jp1.sso.consoleweb	Y	Y

Legend:

Y: Register this attribute.

N: Do not register this attribute.

#:

This attribute must be registered if the monitoring manager is monitoring the monitoring manager itself.

The custom attributes required for executing actions from the **Action** menu differ according to the action. The following table lists the required custom attributes for each action.

Table 2-19: Custom attributes required for executing actions from the Action menu

No	Custom attribute	Monitoring status	Window startup
1	jp.co.hitachi.jp1.sso.address	Y	Y
2	jp.co.hitachi.jp1.sso.agentaddr	Y	--
3	jp.co.hitachi.jp1.sso.consoleweb	Y	Y

Legend:

Y: Required

--: Not required

(b) Triggers for registering custom attributes

The following describes the triggers for registering custom attributes.

- Registration on the monitoring server node

  When all the following conditions are met, the custom attributes are registered on the monitoring server node:

  - NNMi cooperation is enabled.
  - In the `ssoapmon` action definition file (`ssoapmon.def`) or `ssocolmng` action definition file (`ssocolmng.def`), the value of the `nnm-urlaction-coop:` key is `on`.
  - Resource collection conditions or process monitoring conditions are added.

    If NNMi cooperation was disabled when the conditions were added, the custom attributes are registered when NNMi cooperation becomes enabled. However, custom attributes are not registered on the monitoring server on which custom attributes had already been registered when the conditions were added.
  - Resource collection conditions and process monitoring conditions were already registered when the `ssoapmon` and `ssocolmng` daemon processes were started.

    Custom attributes are registered only once after these daemon processes start.

- Registration on the monitoring manager node

  When all the following conditions are met, the custom attributes are registered on the monitoring manager node:

  - NNMi cooperation is enabled.
  - In the `ssoapmon` action definition file (`ssoapmon.def`) or `ssocolmng` action definition file (`ssocolmng.def`), the value of the `nnm-urlaction-coop:` key is `on`.
  - Either of the following conditions is met:

    - The `ssoapmon` or `ssocolmng` daemon process started (if NNMi cooperation is disabled at startup, the custom attributes are registered when NNMi cooperation becomes enabled).

    - The `ssoapcom -n` command or the `ssocolmng -n` command is executed.

For details on the `ssoapmon` action definition file (`ssoapmon.def`), see *6.3.7 ssoapmon action definition file (ssoapmon.def)*. For details on the `ssocolmng` action definition file (`ssocolmng.def`), see *6.3.8 ssocolmng action definition file (ssocolmng.def)*.

(c) Triggers for deleting custom attributes

Custom attributes are deleted when:

- The `ssocadel` command is executed.
- SSO is uninstalled.

The custom attributes that will be deleted are those that were registered by the monitoring manager that executed the `ssocadel` command. For details on this command, see *ssocadel* in *5. Commands*.

(d) Notes

- After SSO stops, the monitoring manager's IP address and port number registered on the **Custom Attributes** tab for a node displayed in the NNMi map view remain.
- The `ssoconsoleweb` value in the `ssoport.conf` file is used as the port number. After you change this value, if you restart only the `ssoconsoled` daemon process, the action cooperation function does not work correctly. In such a case, restart both the `ssocolmng` and `ssoapmon` daemon processes.
- Once custom attributes are registered, they are not deleted unless the `ssocadel` command is executed. Therefore, even after the `nnm-urlaction-coop:` key is set to `off`, SSO actions can be executed from the **Action** menu for any monitoring servers on which custom attributes have been registered. To prevent SSO action execution from the **Action** menu, execute the `ssocadel` command to delete the custom attributes.

(5) Notes on map cooperation (action cooperation)

- To use the action link function, you must start the `ssoconsoled` daemon process of the SSO console by using the monitoring manager.
- If the URL action of SSO is not defined in NNMi, the SSO menu is not displayed on the NNMi console screen.

2.6.5 Checking whether NNMi cooperation is possible

The NNMi cooperation function is available when NNMi has detected the servers monitored by SSO. *Servers detected by NNMi* here means servers recognized by NNMi as nodes, regardless of whether the servers are managed by NNMi.

SSO periodically checks whether cooperation with NNMi is possible, based on the NNMi cooperation related settings in the `ssospmd` action definition file. This check can also be initiated by any daemon process linked with NNMi. Any detected change in the linkability with NNMi can be used as a trigger to, for example, start or stop the relevant daemon process, or change the operation mode of the daemon process to normal or reduced mode. However, a change in the linkability with the NNMi set in the event destination definition file (`ssodest.conf`) is not used as a trigger.

(1) Timing for checking linkability with NNMi

`ssospmd` checks the linkability with NNMi at the following timings:

- At the interval set for `nnm-coop-check-interval` in the `ssospmd` action definition file
- When a process that uses cooperation with NNMi (`ssoapmon` or `ssocolmng`) detects before `ssospmd` that cooperation with NNMi is unavailable

(2) Operation when change in linkability is detected

Upon detection of a change in the linkability with NNMi, `ssospmd` operates as described below according to the `nnm-coop-policy` setting in the `ssospmd` action definition file.

(a) When a change from linkable to unlinkable is detected

If `nnm-coop-policy` is `0`:

`ssospmd` stops all daemon processes except `ssospmd`, and sets the state of the stopped daemon processes to `SUSPENDING`.

If `nnm-coop-policy` is `1`:

`ssospmd` changes the operation mode of the `ssoapmon` and `ssocolmng` daemon processes to reduced mode, and sets the state of these daemon processes to `DEGENERATING`.

(b) When a change from unlinkable to linkable is detected

If `nnm-coop-policy` is `0`:

`ssospmd` starts the daemon processes that are in the `SUSPENDING` state.

If `nnm-coop-policy` is `1`:

`ssospmd` changes the operation mode of the daemon processes that are in the `DEGENERATING` state to normal mode.

2.7 Backup and restore functions

The backup function is implemented by the `ssobackup` command and is used to back up SSO files and databases. The restore function is implemented by the `ssorestore` command and is used to restore files or databases that were backed up by the `ssobackup` command. For details on these commands, see `ssobackup` and `ssorestore` in *5. Commands*. This section describes the backup function and the restore function.

2.7.1 Backup function

The backup function backs up SSO files and databases. For details on what this function can back up, see *2.7.3 Backup targets and restore targets*.

If a backup is executed while a daemon process is running, the processing of that daemon process is interrupted. The daemon process automatically resumes processing when the backup finishes. For details on the daemon processes that are interrupted, see *2.7.4 Daemon process behavior during backup or restore*. Daemon processes cannot start or stop while a backup is in progress.

The backup function backs up files first, and then databases. The function can also be used to back up either files or databases. The time required to back up a database depends on the size of that database.

(1) File backup

If a file backup is attempted while daemon processes are running, the backup function interrupts all daemon processes other than `ssospmd`, `ssoconsoled`, and `ssotrapd`, and then starts backup processing. This means that all the functions provided by the interrupted daemon processes are unavailable during the backup. These functions become available when the backup is completed.

(2) Database backup

If a database backup is attempted while daemon processes are running, the backup function interrupts all daemon processes other than `ssospmd`, `ssoapmon`, and `ssotrapd`, and then starts backup processing. This means that all the functions provided by the interrupted daemon processes are unavailable during the backup. These functions become available when the backup is completed.

2.7.2 Restore function

The restore function restores SSO files and databases from their backups. For details on what this function can restore, see *2.7.3 Backup targets and restore targets*.

Before restore processing can start, all the daemon processes must be stopped. Daemon processes cannot be started during restore processing.

The restore function first restores files, and then restores databases. The function can also be used to restore either files or databases. The time required to restore a database depends on the size of that database.

(1) File restore

The restore function can restore only files that have been backed up by the file backup function.

(2) Database restore

The restore function can restore databases that have become corrupted or otherwise damaged only if they have been backed up by the backup function.

2.7.3 Backup targets and restore targets

The table below lists the files that can be backed up and restored. In this table, `$SSO_BACKUP` indicates the default backup destination directory.

Table 2-20: List of files that can be backed up and restored

Type	Backup/Restore target	Backup destination	
		UNIX	Windows
File	All files in `$SSO_CONF`	In `$SSO_BACKUP/$SSO_CONF`	In `$SSO_BACKUP\$SSO_CONF`
	All files in `$SSO_IMAGE/`*category-name*#	In `$SSO_BACKUP/$SSO_IMAGE/`*category-name*#	In `$SSO_BACKUP\SSO_IMAGE\`*category-name*#
Database	All files in `$SSO_DB`	In `$SSO_BACKUP/$SSO_DB`	In `$SSO_BACKUP\$SSO_DB`
	All files in `$SSO_REPORT`	In `$SSO_BACKUP/$SSO_REPORT`	In `$SSO_BACKUP\$SSO_REPORT`

#:

The value of *category-name* is the category name that is specified in the user resource definition file. For details on user resource definitions, see *2.3 User resource monitoring function*.

The following table lists the backup or restore targets, and shows which type of data, files or databases are backed up or restored.

Table 2-21: Backup or restore targets and the type of data that is backed up or restored

Backup/Restore target	File	Database
All files in `$SSO_CONF`#	Y	N
In `$SSO_IMAGE/`*category-name*	Y	N
All files in `$SSO_DB`	N	Y
All files in `$SSO_REPORT`	N	Y

Legend:

Y: Backed up and restored

N: Not backed up or restored

#

The `ssover.def` file in `$SSO_CONF` can be backed up but cannot be restored.

2.7.4 Daemon process behavior during backup or restore

A backup can be executed regardless of the state of daemon processes. However, all the running daemon processes (except `ssospmd`, `ssoconsoled`, and `ssotrapd`) are interrupted when the backup is executed. The daemon processes that will be interrupted differ depending on the backup target. The following table lists the daemon processes for each backup target.

Table 2-22: List of daemon processes interrupted during backup

Daemon process name	Backup	
	File	Database
ssospmd	N	N
ssocolmng	Y	Y
ssocollectd	Y	Y
ssoapmon	Y	N
ssorptd	Y	Y
ssoconsoled	N	N
ssotrapd	N	N

Legend:

Y: Interrupted

N: Not interrupted

A restore can be executed only when all the daemon processes have been stopped.

3 Installation and Setup

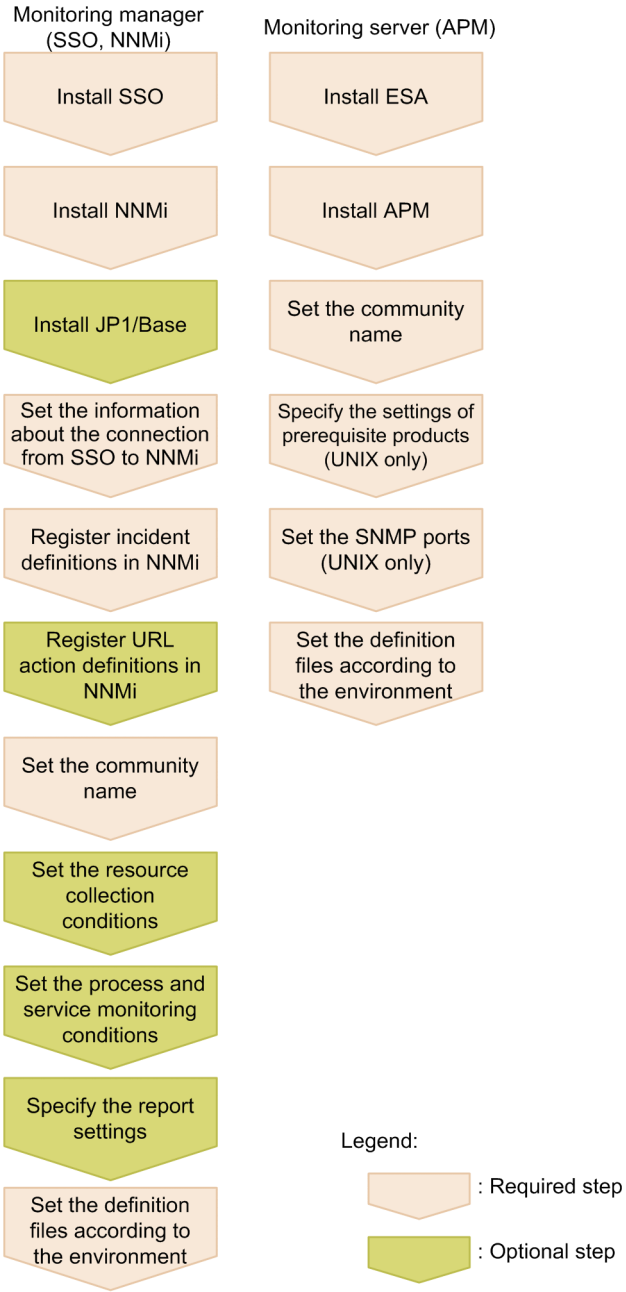
This chapter describes the procedures for installing and uninstalling SSO series programs and explains the setup procedures to be completed before the programs can be used.

3.1 Installation and setup flowcharts

This section describes the flow of tasks from SSO installation to setup for the basic configuration and for a distributed configuration.

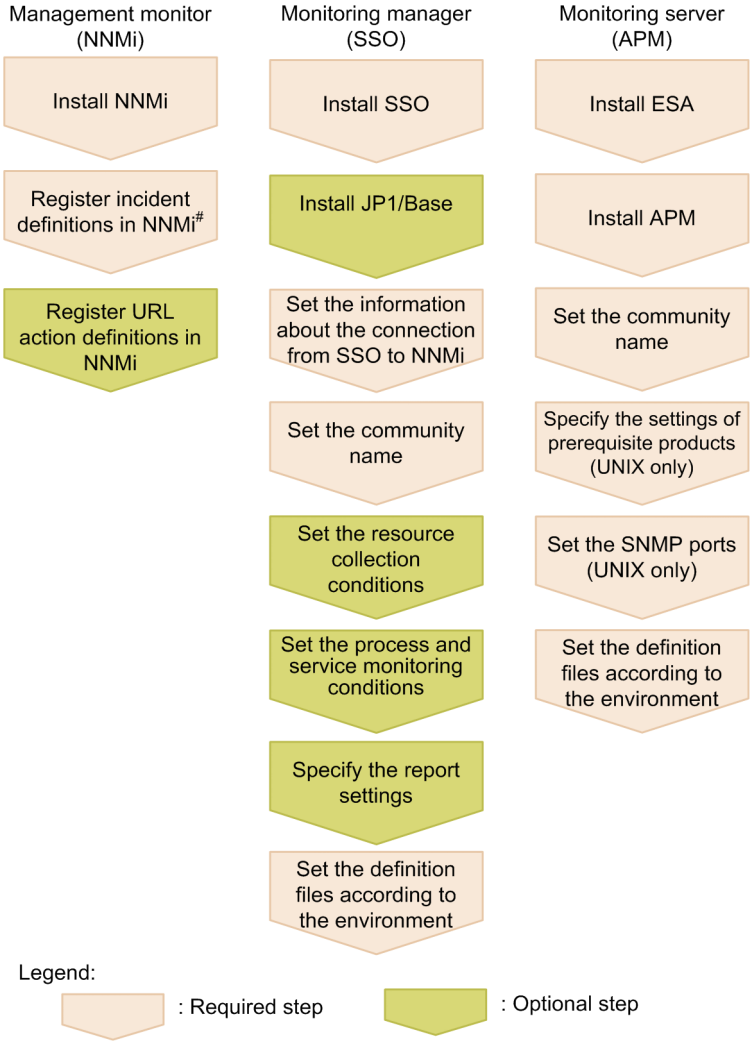
The following figure shows the flow of tasks from SSO installation to setup for the basic configuration.

Figure 3-1: Installation and setup flowcharts (basic configuration)



The following figure shows the flow of tasks from SSO installation to setup for a distributed configuration.

Figure 3-2: Installation and setup flowcharts (distributed configuration)



#: Incident definitions need to be registered only once.

3.1.1 Flow of SSO installation and setup tasks

This subsection describes the flow of SSO installation and setup tasks.

1. Install SSO.

   You can perform product installation steps 1 to 3 in any order.

   In a distributed configuration, install NNMi and each SSO program on different hosts. Note that every SSO program must be set up.

   For how to install SSO, see *3.2.1 Installing*.

2. Install NNMi.

   For how to install NNMi, see the *Job Management Partner 1/Consolidated Manager 2/Network Node Manager i Installation Guide*.

3. Install JP1/Base.

   JP1/Base is required only when the user authentication function of JP1/Base is to be used. You can install JP1/Base at any point before step 6.

For details about how to install JP1/Base, see the *Job Management Partner 1/Base User's Guide*.

4. Set the information about connection to NNMi.

   Execute the `ssonnmsetup -add` command.

   For details about the `ssonnmsetup` command specification, including options, see *ssonnmsetup* in *5. Commands*.

5. Set the incident definitions of SSO in NNMi.

   The following table lists the incident definition file names and definition conditions.

   Table 3-1: Names and registration conditions for incident definition files

#	Incident definition file name	Registration condition
1	`$SSO_INCIDENT/ssoincident.def`	This file must be registered.
2	`$SSO_INCIDENT/apmtrap.def`	Set this file if an APM that does not use TCP communication for event notification is set for process and service monitoring.

   The incident definition file `ssoincident.def` is set by using the `nnmconfigimport.ovpl` command.

   If NNMi is stopped, start it before executing the `nnmconfigimport.ovpl` command. After moving the current directory to `bin` in the NNMi installation directory, execute the following command:

```
nnmconfigimport.ovpl -u user-name -p password -f $SSO_INCIDENT/
ssoincident.def
```

   The following describes the values that can be specified for the command arguments.

   user-name: Specify the user name of the NNMi administrator.

   password: Specify the password for the NNMi administrator account.

   You do not need to re-register the incident definition file when you perform an upgrade installation of SSO.

   In a distributed configuration, the incident definition file `ssoincident.def` must be copied and registered to the management manager. Since the incident definition file needs to be registered only once, you do not need to perform registration for each host on which SSO is installed. Registration of `apmtrap.def` is unnecessary.

   Note that the incident definition file must be copied and registered to NNMi on all other hosts specified as transmission destinations in the event destination definition file (`ssodest.conf`), as in a distributed configuration.

6. Set the URL action definitions of SSO in NNMi.

   The following table lists the URL action definition file names and recommended registration requirements.

   Table 3-2: Names of URL action definition files and recommended registration requirements

#	URL action definition file name	Registration requirement
1	`$SSO_URLACTION/ssourlaction.def`	Set this file if NNMi is other than a multitenant environment.
2	`$SSO_URLACTION/ssourlaction-mt.def`	Set this file if NNMi is a multitenant environment.

   The same menu items are registered for either of the above files, but the local settings differ. Select either one of these file names. If both are registered, only the definitions of the file that was registered last are valid.

   The roles of the menu items registered in that definition file can be changed according to the operation. For details about the roles, see *2.6.2(2) Action menu access rights* and *2.6.4(3) Action menu access rights*.

   TheURL action definition file is set by using the `nnmconfigimport.ovpl` command.

   If NNMi is stopped, start it before executing the `nnmconfigimport.ovpl` command. After moving the current directory to `bin` in the NNMi installation directory, execute the following command:

```
nnmconfigimport.ovpl -u user-name -p password -f $SSO_URLACTION/
ssourlaction.def
```

The following describes the values that can be specified for the command arguments.

user-name: Specify the user name of the NNMi administrator.

password: Specify the password for the NNMi administrator account.

Do not re-register the URL action definition file when you perform an upgrade installation of SSO. If you do so, resource status change events that were generated before the upgrade installation can no longer be used to display incident graphs.

However, you must re-register the URL action definition file if you set the NNM action address definition file when you upgrade SSO from a version earlier than 10-10.

In a distributed configuration, the URL action definition file must be copied and registered to the management manager. Since the URL action definition file needs to be registered only once, you do not need to perform registration for each host on which SSO is installed.

Note that the URL action definition file must be copied and registered to NNMi on all other hosts specified as transmission destinations in the event destination definition file (`ssodest.conf`), as in a distributed configuration.

7. Register the users for user authentication on the SSO console.

   Set the user authentication method on the SSO console. Two user authentication methods are available. Set the desired method in the `ssoconsoled` action definition file. For details about the settings of the `ssoconsoled` action definition file, see *6.3.23 ssoconsoled action definition file (ssoconsoled.def)*.

   If the user authentication method is the SSO authentication method:

   Execute the `ssoauth -add` command.

   For details about the SSO console, see *2.1.1 SSO console*.

   For details about the `ssoauth` command, see *ssoauth* in *5. Commands*.

   If the user authentication method is the JP1 authentication method:

   For details about how to register the JP1/Base authentication user, see the *Job Management Partner 1/Base User's Guide*.

8. Set the community name.

9. Set the resource collection conditions.

10. Set the process monitoring conditions.

3.2 Installing and uninstalling SSO

This section describes the procedures for installing and uninstalling SSO.

3.2.1 Installing

This subsection describes the procedure for installing SSO.

(1) UNIX

(a) Installation prerequisites

Before performing the installation, make sure that the following prerequisites are met:

- If performing an overwrite installation, make sure that the product to be installed is not an earlier version or revision.
- The user performing the installation must have superuser permission.

(b) Installation method

Perform the installation by following the Hitachi Program Product Installer instructions.

For the remote installation method that uses JP1/Software Distribution, see the applicable Job Management Partner 1/Software Distribution Manager manual and the Job Management Partner 1/Software Distribution SubManager (UNIX) manual.

(c) Notes on installation

- Before starting an SSO installation or SSO patch application, stop SSO.
- Following the SSO installation, the daemon processes of SSO do not start. Start them according to the operating environment.
- When upgrading to this version from a version 10-10 (including corrective versions), perform the following procedure:
  1. Backs up `$SSO_BIN/jp1ssolog.sh`.
     The following example shows how to back up a `$SSO_BIN/jp1ssolog.sh`:
     `mv $SSO_BIN/jp1ssolog.sh $SSO_BIN/org_jp1ssolog.sh`
  2. Copy the `$SSO_NEWCONF/jp1ssolog.sh` to `$SSO_BIN`.
     The following example shows how to copy the `$SSO_NEWCONF/jp1ssolog.sh` to `$SSO_BIN`:
     `cp -p $SSO_NEWCONF/jp1ssolog.sh $SSO_BIN/jp1ssolog.sh`
  3. If you have modified any settings, those settings will also be applied to `$SSO_BIN/jp1ssolog.sh`.
  4. Delete the `$SSO_BIN/org_jp1ssolog.sh`.
     The following example shows how to delete a `$SSO_BIN/jp1ssolog.sh`:
     `rm $SSO_BIN/org_jp1ssolog.sh`

(2) Windows

(a) Installation prerequisites

Before performing the installation, make sure that the following prerequisites are met:

- In an overwrite installation, make sure that the product to be installed is not an earlier version or revision.
- The user performing the installation must have administrator permission.
  If UAC is enabled, installation by a user who has administrator permission but is not an administrator requires elevation of that user to administrator.

(b) Installation method

Perform the installation by following the installer instructions.

In a new installation, the following items must be set. In an overwrite installation, the information set during the new installation is carried over, and thus these items need not be set again.

- User information (user name and affiliation)
- Installation directory
  The default installation directory is as follows:

  ```
  %SystemDrive%\Program Files (x86)\HITACHI\JP1Cm2SSO\
  ```

  To change the installation directory from the default directory, specify a directory that meets the following rules:
  - The directory path must begin with a drive letter (such as `C:` or `D:`).
  - The directory path string must not include multi-byte code or any of the following 1-byte characters: `/`, `:`, `*`, `?`, `"`, `<`, `>`, `|`, `,`, `;`, `$`, `%`, `^`, `'`, `!`, `(`, `)`, `=`, `+`, `{`, `}`, `@`, `[`, `]`
    The `\` symbol can be used only as a directory separator.
  - The directory path cannot consist of only a drive letter or root directory (such as `C:` or `D:`).
  - The length of the directory path string must be 45 bytes or fewer in length, including the `\` symbol at the end of the directory.
  - SSO cannot be installed under `%SystemDrive%\Program Files\`. If a location under `%SystemDrive%\Program Files\` is specified as the installation directory, SSO will be installed to a directory where `%SystemDrive%\Program Files\` is replaced with `%SystemDrive%\Program Files (x86)\`.

For details about how to install SSO remotely by using JP1/Software Distribution, see the *Job Management Partner 1/Software Distribution Description and Planning Guide*, for Windows systems and the *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems.

(c) Notes on installation

- Before starting an SSO installation or SSO patch application, stop SSO.
- Set the following permission for SYSTEM and administrators for the files under the SSO installation directory as well as sub-directories:
  Read, write, execute, delete
- Following the SSO installation, the daemon processes of SSO do not start. Start them according to the operating environment.

- When upgrading to this version from a version 10-10 (including corrective versions), perform the following procedure:

  1. Backs up `$SSO_BIN\jp1ssolog.bat`.
     The following example shows how to back up a `$SSO_BIN\jp1ssolog.bat`:
     `ren $SSO_BIN\jp1ssolog.bat $SSO_BIN\org_jp1ssolog.bat`
  2. Copy the `$SSO_NEWCONF\jp1ssolog.bat` to `$SSO_BIN`.
     The following example shows how to copy the `$SSO_NEWCONF\jp1ssolog.bat` to `$SSO_BIN`:
     `copy /a $SSO_NEWCONF\jp1ssolog.bat $SSO_BIN\jp1ssolog.bat`
  3. If you have modified any settings, those settings will also be applied to `$SSO_BIN\jp1ssolog.bat`.
  4. Delete the `$SSO_BIN\org_jp1ssolog.bat`.
     The following example shows how to delete a `$SSO_BIN\org_jp1ssolog.bat`:
     `del $SSO_BIN\org_jp1ssolog.bat`

3.2.2 Uninstalling

This subsection describes the procedure for uninstalling SSO.

(1) UNIX

Uninstalling SSO requires superuser permission.

1. If windows or dialog boxes are open, close them.
2. Exit SSO.
3. Execute the `ssocadel` command and delete the URL action definitions.
   Perform this step if URL action link functions are being used.
4. Install SSO with the Hitachi Program Product Installer.

Note that cases where user-specified log files and trace files are not deleted exist. If these files are not needed, delete them manually after uninstallation.

(2) Windows

Uninstalling SSO requires Administrators permission.

1. If windows or dialog boxes are open, close them.
2. Exit the programs.
3. Execute the `ssocadel` command and delete the URL action definitions.
   Perform this step if URL action link functions are being used.
   From the Windows **Control Panel**, select **Add/Remove Programs**.# Then, select **SNMP System Observer**, and click **Add/Remove**.
   The window for selecting the program operation is displayed.
4. Select **Remove**, and click **Next**.

Note that cases where user-specified log files and trace files are not deleted exist. If these files are not needed, delete them manually after uninstallation.

#:

In Windows Server 2008 or Windows Server 2012, **Programs and Features** is displayed.

(3) Notes on uninstallation

- When the SSO uninstallation is performed, all the files under the installation directory are deleted. However, the files and directories that access the installation directory are not deleted. Moreover, in the case of Windows, in some cases, the installation directory `\uCPSB` might not be deleted. In such a case, collect data with the `jp1ssolog.bat` data collection command for Windows. For details about the `jp1ssolog.bat` data collection command for Windows, see *jp1ssolog.bat (Windows only)* in *5. Commands*.
- After SSO has been uninstalled, delete the incident definitions from NNMi by using the incident form of the NNMi console.
- If URL action cooperation functions are being used, execute the `ssocadel` command before uninstalling SSO. Also, delete the URL action definitions registered by SSO from the NNMi console.

3.3 SSO setup

3.3.1 Setting the community name

The resource collection function of SSO collects resources from the MIB objects of the SNMP agents by using the SNMP protocol. Therefore, to use the resource collection function of SSO, the SNMP agents and Get community name of the monitoring manager must be matched.

Moreover, in the case of the monitoring function for the processes and services of SSO, the monitoring conditions are set to APM by using the SNMP protocol. Therefore, to use the process and service monitoring function, the SNMP agents and the Set community name of the monitoring manager must be matched.

The Get community name and Set community name are set in the SNMP definition file (`ssosnmp.conf`). For details about the SNMP definition file (`ssosnmp.conf`), see *6.3.6 SNMP definition file (ssosnmp.conf)*.

For details about how to set the community name of SNMP agents, see the manual *Job Management Partner 1/ Consolidated Manager 2/Extensible SNMP Agent* and the manual of the SNMP agent product that is used.

3.3.2 Using SSO on a host that has multiple IP addresses

As the IP address of the monitoring manager, set an IP address that can communicate with the monitoring server.

The IP address of the monitoring manager is defined in the `change-my-address` key of the `ssoapmon` action definition file and the `ssocolmng` action definition file.

When creating a report definition file, specify the IP address specified in the `change-my-address` key of the `ssocolmng` action definition file of SSO as the report conditions collection server name.

For details, see *6.3.7 ssoapmon action definition file (ssoapmon.def)* or *6.3.8 ssocolmng action definition file (ssocolmng.def)*.

In an environment in which the monitoring manager interfaces with multiple networks that are not routed to each other, set the NNM action address definition file when you perform the following operation: Using NNMi cooperation (action cooperation) from a terminal that cannot communicate with the monitoring manager by using the IP address set by the `change-my-address:` key in the `ssocolmng` action definition file and `ssoapmon` action definition file. For details, see *6.3.32 NNM action address definition file (ssonnmactaddr.conf)*. If you also want to monitor the monitoring manager itself, use the IP address set by the `change-my-address:` key.

3.3.3 Notes on Windows

(1) Execution of automated actions

If a window program is to be run with automated actions, access to the desktop is required. In such a case, you must change the service account to allow desktop access with the following procedure.

1. From the **Control Panel**, open **Administrative Tools** and select **Services**.
2. From the **Services** list, select **SNMP System Observer** and open **Properties**.

3. Set the service account to **System account**.

4. Select the **Allow Service to Interact with Desktop** check box.

(2) Security setting for installation directory of SSO

If removing `Everyone` or denying full control in the security settings for the SSO installation directory, specify the following setting:

In the case of an account set for **SNMP System Observer** Windows service logon (in the case of a local system account, SYSTEM account), set **Read & Execute** to **Allow**.

3.3.4 Notes on Linux

(1) /etc/hosts file definition

When Red Hat Linux is installed, loopback address 127.0.0.1 might be defined for the IP address of a local node (in the following definition example, `linux01`) in the `/etc/hosts` file.

```
127.0.0.1   linux01 localhost.localdomain localhost
```

If the local SSO node is defined with a loopback address, various problems might occur, such as the collection database becoming unreferenceable, or the monitoring status for processes and services becoming unrecognizable. Therefore, in an environment that uses SSO, do not define 127.0.0.1 for the local node, but the local IP address (in this example, 172.16.49.18) instead. A definition example is shown below.

```
127.0.0.1          localhost.localdomain localhost
172.16.49.18       linux01
```

If the action IP address of SSO is set for the `change-my-address:` key in the `ssoapmon` action definition file (`ssoapmon.def`) and `ssocolmng` action definition file (`ssocolmng.def`), the above-described handling is not required.

For details about the respective definition files above, see *6.3.7 ssoapmon action definition file (ssoapmon.def)* and *6.3.8 ssocolmng action definition file (ssocolmng.def)*.

3.3.5 Settings for distributed configuration

In a distributed configuration, make the following settings for the management manager and monitoring manager.

- Management manager

  Set the incident definitions of SSO to NNMi. For details about how to set the incident definitions of SSO, see *3.1.1 Flow of SSO installation and setup tasks*.
- Monitoring manager
  - Configure the definition so that the NNMi host is set to the Host key in the NNM information definition file (`ssonnminfo.conf`). For details about the NNM information definition file, see *6.3.29 NNM information definition file (ssonnminfo.conf)*.

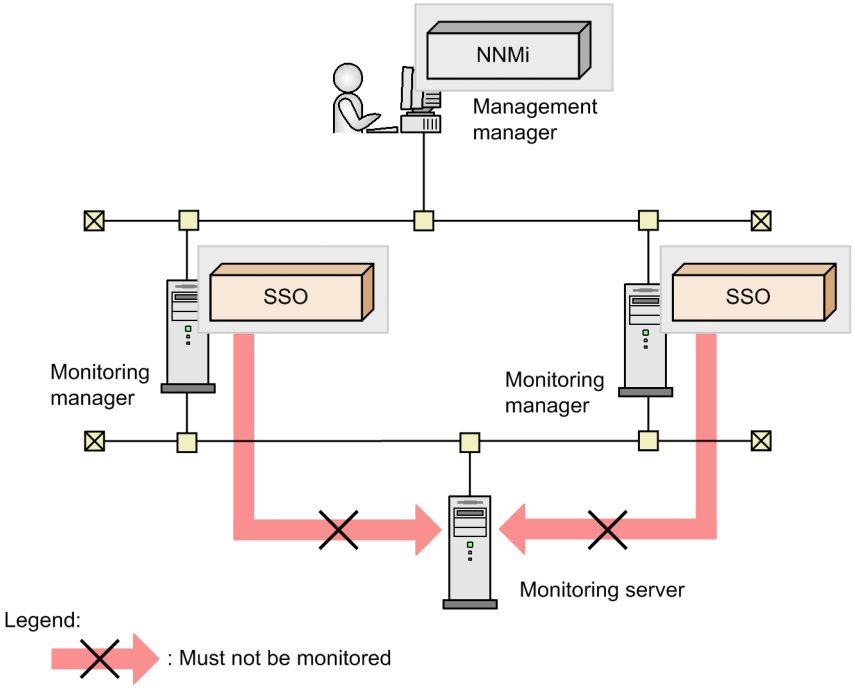
- If SNMP notification is included in the event notification methods of APM, define the `ssotrapd` daemon process in the SSO startup definition file (`ssostartup.conf`). For details about the SSO startup definition file, see *6.3.24 SSO startup definition file (ssostartup.conf)*.

Notes on distributed configuration are as follows:

- A NAT device cannot be placed between NNMi and SSO.
- Monitoring of the same monitoring server from multiple monitoring managers managed by one management manager must not be allowed.

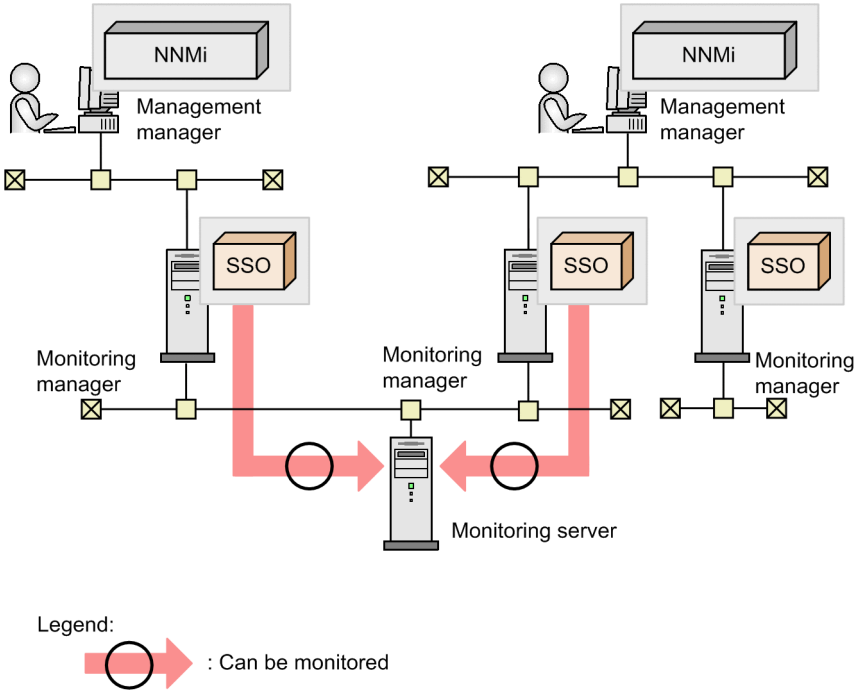
  Do not create a configuration such as the one in the following figure.

  Figure 3-3: Example of prohibited monitoring (distributed configuration)



  Note that the same monitoring server can be monitored from multiple monitoring managers managed by different management managers, as shown in the following figure.

Figure 3-4: Example of possible monitoring (distributed configuration)



4 Windows

This chapter describes the windows of SSO.

4.1 About windows

Start a window of SSO from the **Start** menu of Windows, by executing the `ssoguistart` command, or from the SSO console.

Windows that can be started from the **Start** menu, or by executing the `ssoguistart` command are listed below.

When UAC is active, if a user with permissions other than those of an Administrator starts a window, the dialog box for controlling the user account appears, and the user is requested to have the relevant permission levels elevated to those of an Administrator.

- Resource Browser window
- Resource Configuration window
- Resource Reference window
- Resource Data Reference window
- Process Configuration window
- Process Reference window
- Process Monitor window

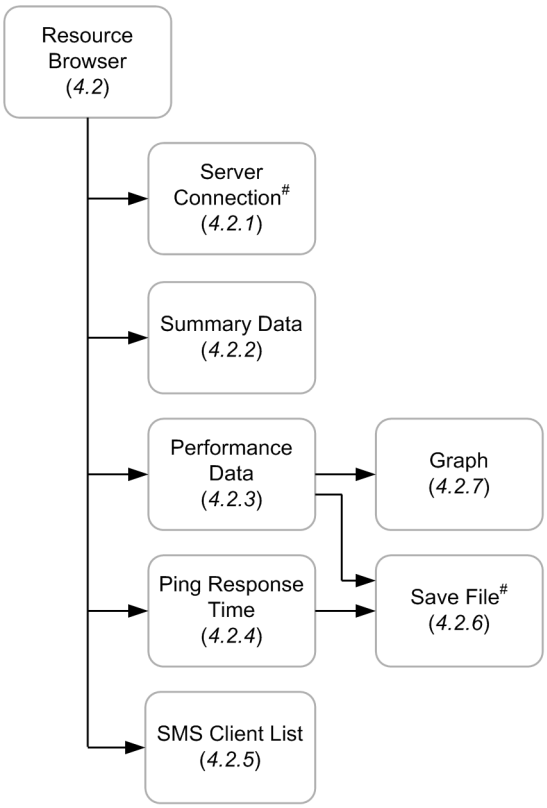
The following are the windows that can be opened from the SSO console:

- Resource Browser window
- Resource Configuration window
- Resource Reference window
- Resource Data Reference window
- Process Configuration window
- Process Reference window
- Process Monitor window
- Report Configuration window

4.1.1 Window transition

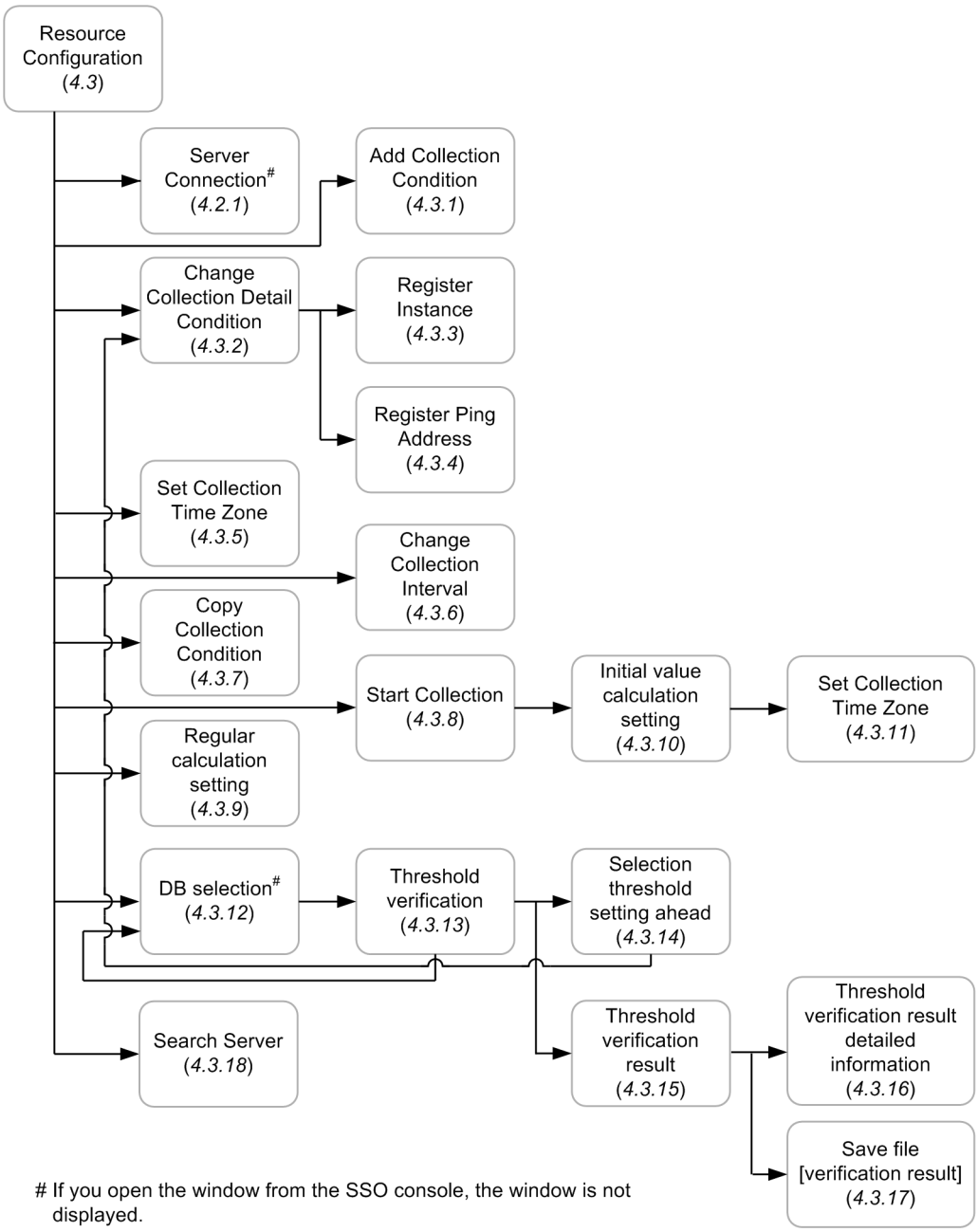
The following explains the window transition of each window. The numbers given in parentheses indicate the section that explains the window.

Figure 4－1: Window transition of the Resource Browser window



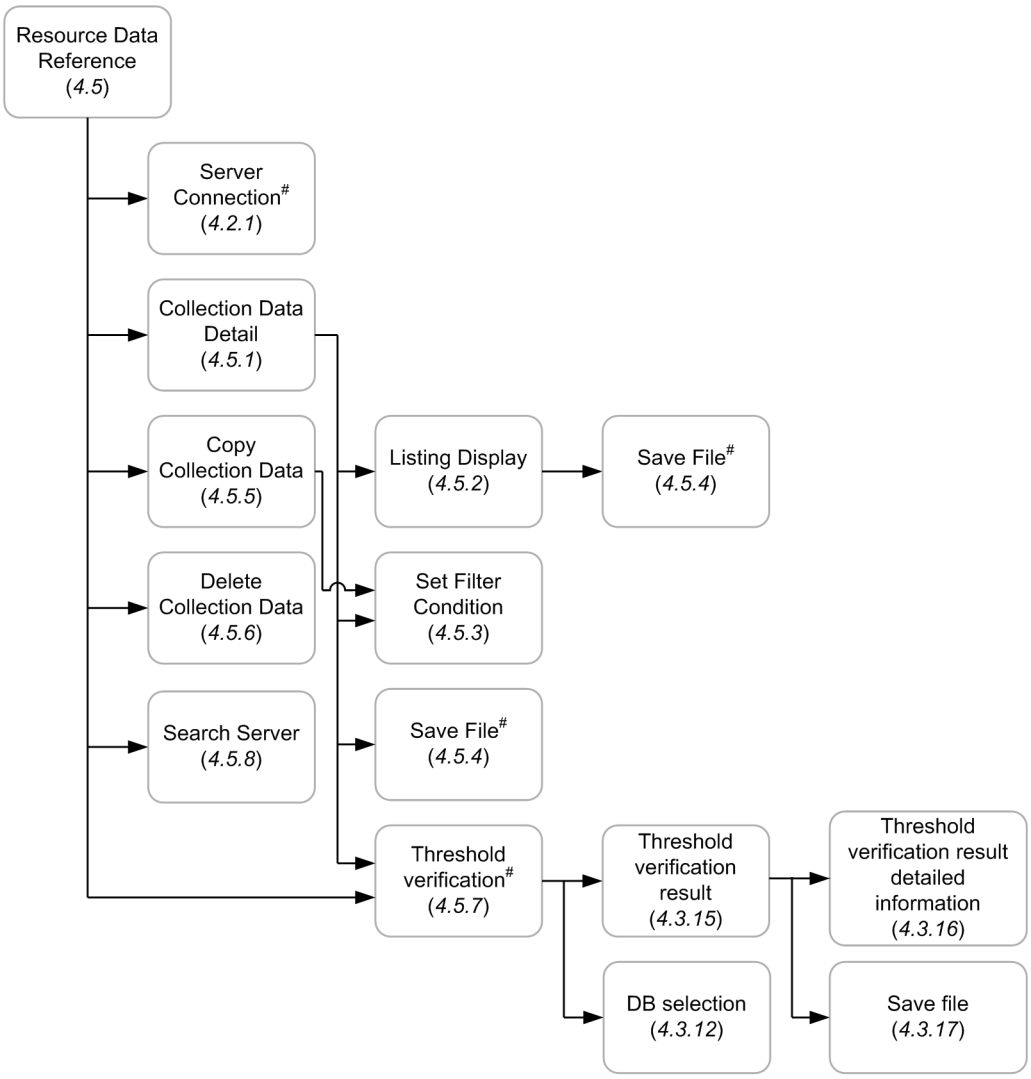
If you open the window from the SSO console, the window is not displayed.

Figure 4－2: Window transition of the Resource Configuration window



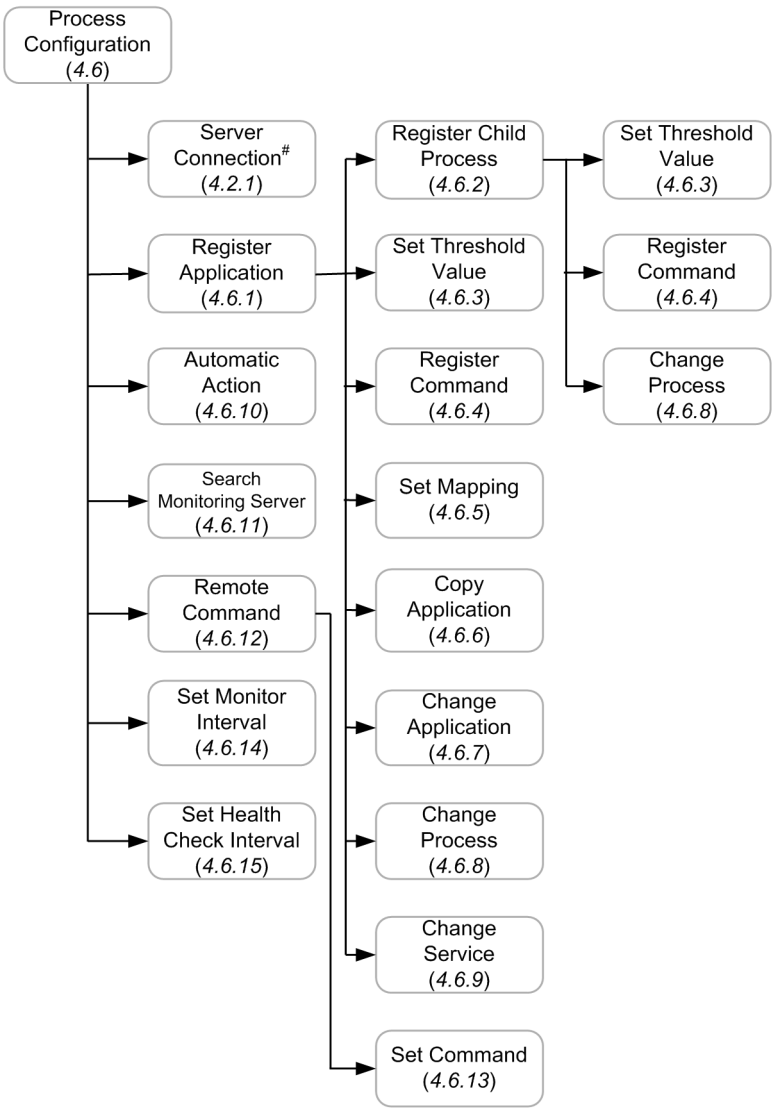
If you open the window from the SSO console, the window is not displayed.

Figure 4－3: Window transition of the Resource Data Reference window



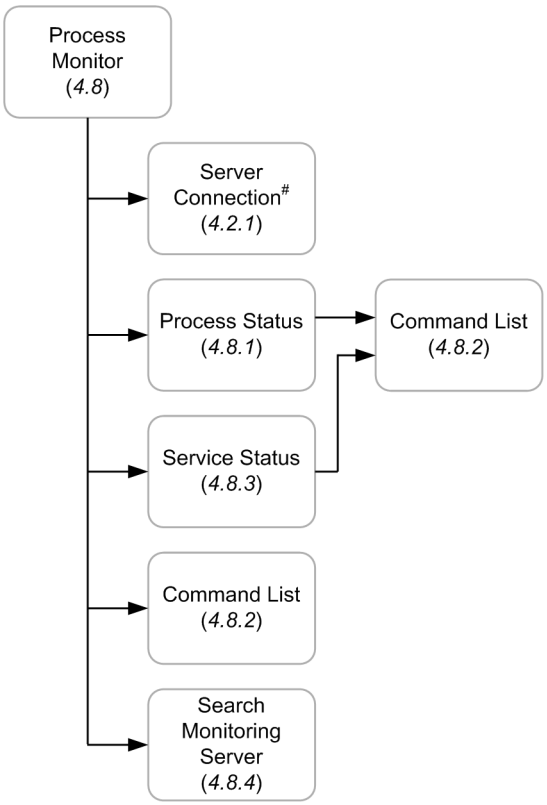
If you open the window from the SSO console, the window is not displayed.

Figure 4-4: Window transition of the Process Configuration window



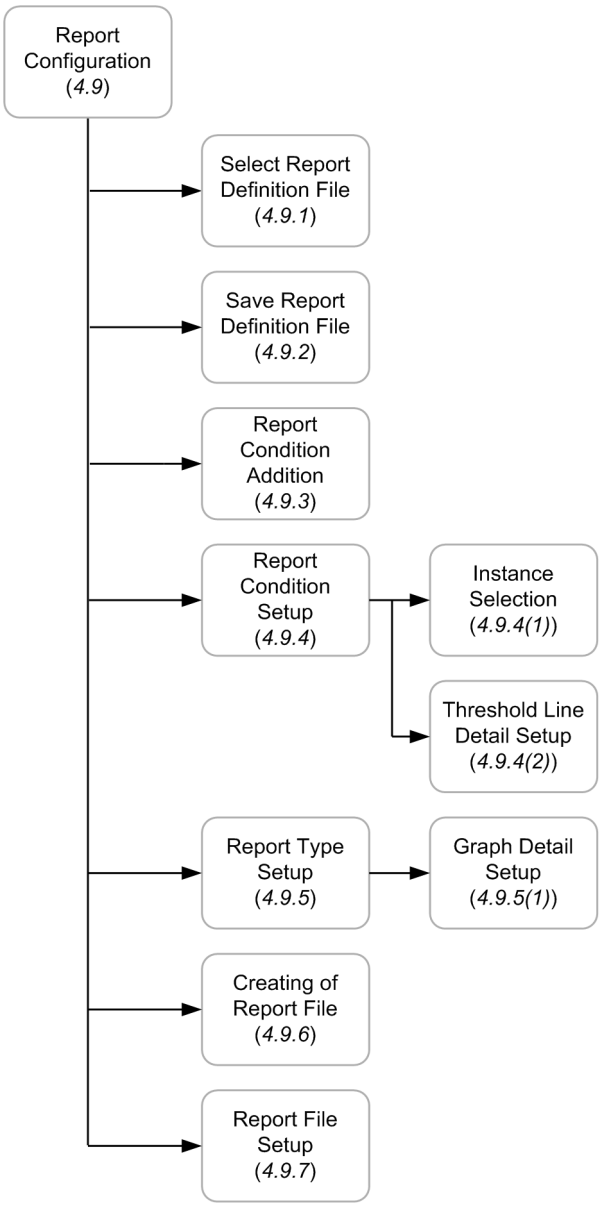
If you open the window from the SSO console, the window is not displayed.

Figure 4-5: Window transition of the Process Monitor window



If you open the window from the SSO console, the window is not displayed.

Figure 4-6: Window transition of the Report Configuration window



4.1.2 Common buttons used in the SSO windows

This subsection describes the buttons used in the windows of SSO.

OK

Reflects the new settings and closes the window.

Cancel

Closes the window without reflecting the new settings.

Close

Closes the window.

Help

Displays Help.

Version

Displays version information.

4.1.3 Notes on using SSO windows

This subsection provides notes on using SSO windows.

(1) Monitors

When using SSO windows, use a monitor with the following resolution or higher:

For Windows: 1,024 **x** 768

For UNIX: 1,280 **x** 1,024

(2) Notes on using SSO windows from an X server emulator in Windows (UNIX)

When using SSO windows from an X server emulator in Windows, do not use a local window manager. The display position or size of a window might become invalid. Use a window manager in UNIX.

(3) Environmental variables (UNIX)

Set and use the `XFILESEARCHPATH` environmental variable correctly. Otherwise, a window might not start (Settings vary depending on the user's computing environment).

Example

```
XFILESEARCHPATH=/usr/openwin/lib/locale/%L/%T/%N%S:/usr/openwin/lib/%T/%N
%S
```

(4) Languages for Help provided by this product

This product provides Help in Japanese and English. If Japanese does not display correctly, change the encoding for the page displayed in the Web browser to "Unicode (UTF-8)".

(5) Using Java applet windows

Windows you start from the SSO console are Java applet windows. Therefore, when you close the SSO console, the applet windows also close.

(6) Viewing Help in UNIX

To view Help in UNIX, you need a Web browser. Install a Web browser, and define the path in the GUI definition file. For details, see *6.3.11 GUI definition file (ssogui.conf)*.

(7) Note on use in a Chinese environment (in Windows or Linux)

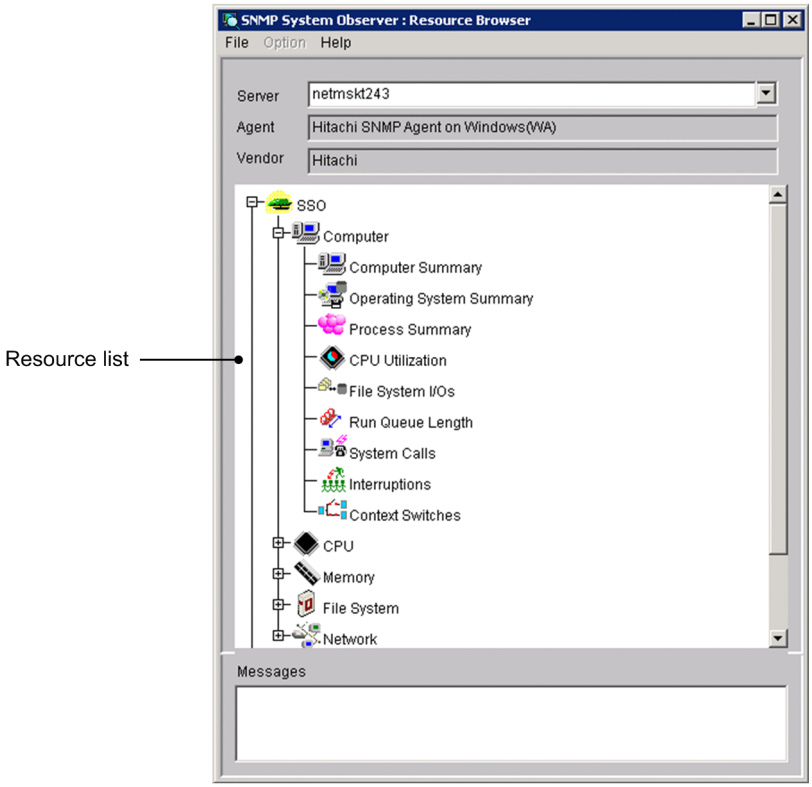
If the language environment variable of SSO is Chinese, the text in the following areas is displayed in Chinese. For details on the supported Chinese language environment variables, see *H. Language Environment Variables*.

- Title
- Menu
- Button
- Label

4.2 Resource Browser window

The Resource Browser window enables you to collect and browse a server's resources at any time. The following figure shows the Resource Browser window.

Figure 4-7: Resource Browser window



The items to be set are:

Server

Enter the host name or IP address of the server containing the resource you want to browse.

Agent

This box displays the name of the SNMP agent that runs on the server indicated in the **Server** box.

Vendor

This box displays the name of the vendor of the SNMP agent indicated in the **Agent** box.

Resource list

This list box displays a list of the resources that you can obtain from the SNMP agent indicated in the **Agent** box.

The next table explains the menu items.

Menu bar	Menu command	Description
File	Open	Displays the results of browsing the specified resources in the Resource list.
	Change Connection#	Displays the Connect Server window.
Option	SMS Client List	Displays the SMS Client List: window.
	Re-acquire SMS Information	Acquires SMS client information again.

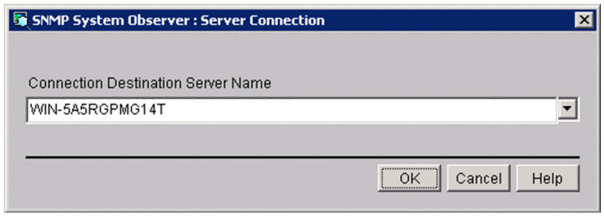
#

If you open the window from the SSO console, the menu command is not displayed.

4.2.1 Server connection window

The Server connection window changes the connection destination server. The following figure shows the Server connection window.

Figure 4-8: Server connection window



The items to be set are:

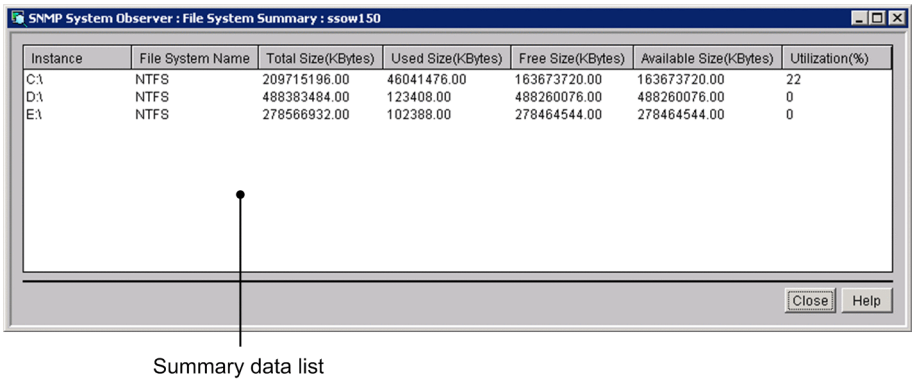
Connection destination server name

Enter a host name or IP address in 255 bytes or less.

4.2.2 Summary Data window

The Summary Data window displays summary data about the resource selected in the Resource Browser window. The following figure shows the Summary Data window.

Figure 4-9: Summary Data window



The items to be set are:

Summary data list

This list box displays a list of the collected summary data. The details differ depending on the resource to be browsed.

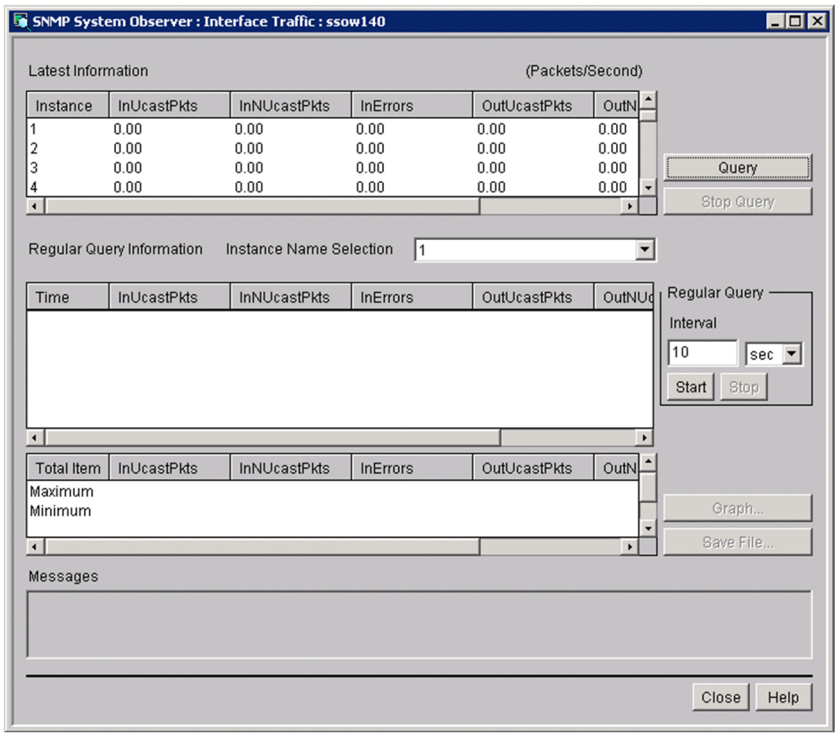
Resource values to be displayed:

Fractional resource values are rounded to two decimal places.

4.2.3 Performance Data window

The Performance Data window displays performance data about the resource selected in the Resource Browser window. The following figure shows the Performance Data window.

Figure 4－10: Performance Data window



The items to be set are:

Latest Information

This list box displays a list of the collected data. The details differ depending on the resource to be browsed.

Query

This button obtains a resource and updates **Latest Information**.

Stop Query

This button cancels update of the resource information.

Instance Name Selection

This box selects an instance about which a regular query is to be performed.

Regular Query Information

This box displays the result of regular query for each instance. It also totals and displays the maximum value, minimum value, and average of regular query information.

Regular Query

Interval

Specify an interval for regular query between 10 seconds and 60 minutes. Specify **Second** or **Minute** as the unit of time.

Start, **Stop**

These buttons start and stop regular query.

Graph

This button displays regular query data in a graph.

Save File

This button displays the Save File window. If you open the Performance Data window from the SSO console, this button is not displayed.

Messages

This box displays messages about SSO operation.

(1) Notes

Performing regular queries in the Resource Browser window for a long time

If you use performance data or a regular query of a ping response time in the Resource Browser window for a long time, the Resource Browser window might not work properly.# This is mainly caused by insufficient memory for storing the data of regular queries. You can avoid this situation by limiting the maximum number of queries for a regular query.

When the behavior of a regular query in the Resource Browser window is not stable, reduce the number of queries for a regular query until the behavior becomes stable in the current environment.

If the maximum number of queries has already been determined, such as when an operation policy calling for performing a query every 10 seconds for 1 hour exists, we recommend you set a minimum value which is large enough for the maximum number of queries.

#

For example, the Resource Browser window might freeze (operation of the GUI stops, or it does not accept any operation requests), or crash (the GUI ends abnormally).

For how to change the maximum number of queries for a regular query, see *6.3.11 GUI definition file (ssogui.conf)*.

Resource values to be displayed:

Fractional resource values are rounded to two decimal places.

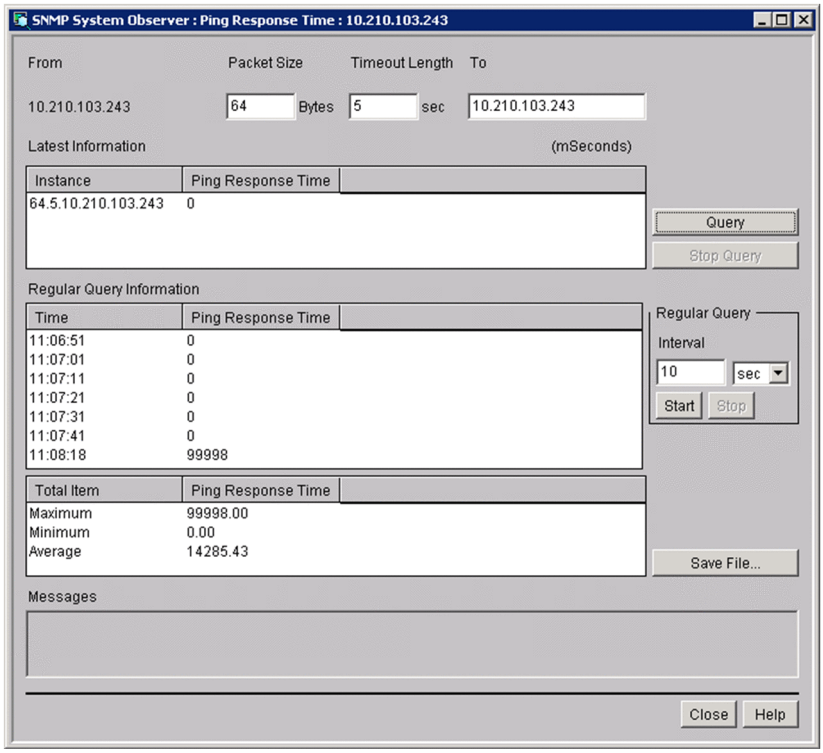
The maximum value and minimum value to be displayed:

If the maximum value or minimum value is an integer, the decimal places `.00` are added.

4.2.4 Ping Response Time window

The Ping Response Time window displays the browsing results if you specified a ping response time in the Resource Browser window. The following figure shows the Ping Response Time window.

Figure 4-11: Ping Response Time window



The items to be set are:

From

This area displays the IP address of the server containing the resources being browsed.

Packet Size

Specify a ping packet size between 32 and 2048 bytes.

Timeout Length

Specify a ping timeout length between 1 and 60 seconds.

To

Specify the IP address of the ping destination. Use the *n*.*n*.*n*.*n* format, where *n* is an integer from 0 to 255. You cannot specify `0.0.0.0` and `255.255.255.255`.

The other items are the same as those in the Performance Data window shown in *Figure 4-10*.

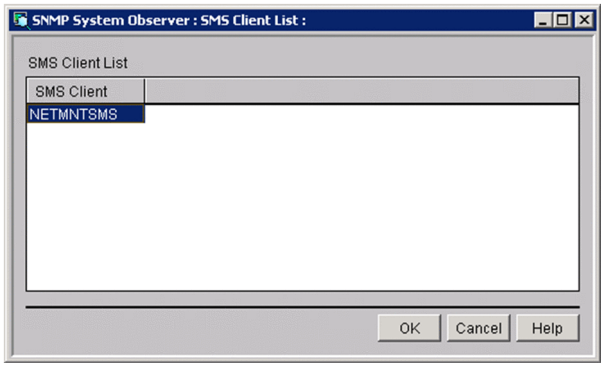
The maximum value and minimum value to be displayed:

For the maximum value and minimum value, the decimal places `.00` are added.

4.2.5 SMS Client List window

The SMS Client List window displays SMS clients. The following figure shows the SMS Client List window.

Figure 4-12: SMS Client List window



The items to be set are:

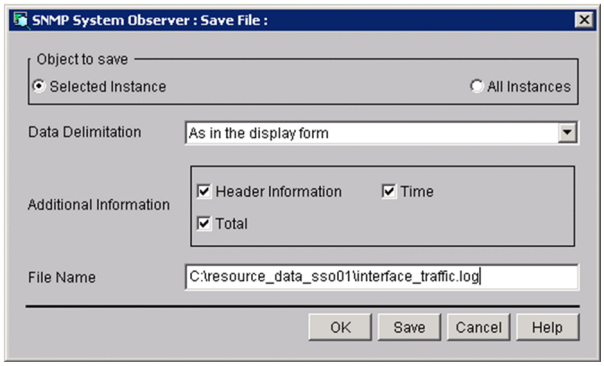
SMS Client List

This box displays a list of the SMS clients that you can obtain from the SMS server. Define the SMS server beforehand in the GUI definition file. For details, see *6.3.11 GUI definition file (ssogui.conf)*.

4.2.6 Save File window

The Save File window saves the results of a regular query to a file. The following figure shows the Save File window.

Figure 4-13: Save File window



The items to be set are:

Object to save

Select the instance to be saved to a file.

Selected Instance

SSO saves performance information only for the instance selected in the Performance Data window.

All Instances

SSO saves performance information for all instances.

Data Delimitation

Specify a character for delimiting data.

As in the display form

SSO uses spaces to set out the lines and outputs the data to a file as displayed in **Regular Query Information** in the Performance Data window.

Delimit by comma, **Delimit by tab**, **Delimit by space**

SSO delimits the data in accordance with the specified format.

Additional Information

Specify the information to be output to the save file.

Header Information

SSO outputs (to the file) the resource name or other title of the data.

Time

SSO outputs (to the file) the date and time at which the information was obtained.

Total

SSO outputs (to the file) the total of the minimum value, maximum value, and average.

File Name

Specify a file name by its absolute path. If you omit the path on Windows, SSO creates the file in the SSO installation directory. If you omit the path on UNIX, SSO creates the file in the root directory.

Save

SSO saves the data to the specified file.

Resource values to be output:

Fractional resource values are rounded to two decimal places.

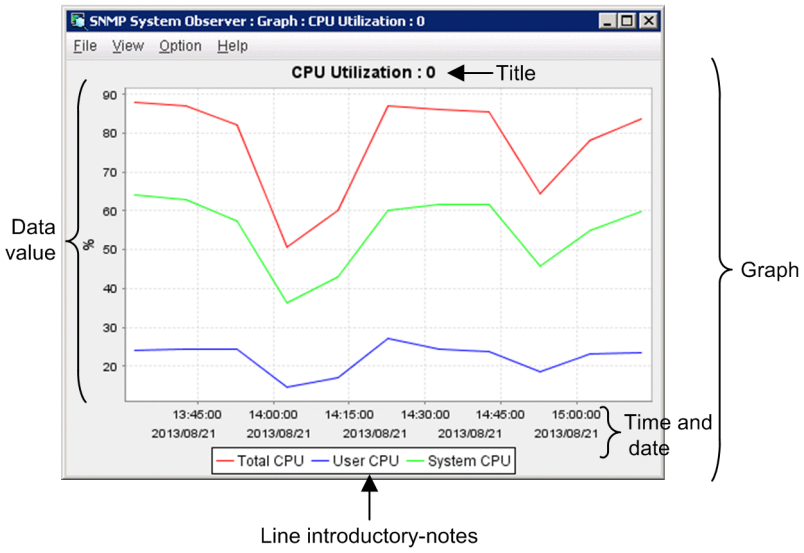
The maximum value and minimum value to be output:

If the maximum value or minimum value is an integer, the decimal places `.00` are added.

4.2.7 Graph window

The Graph window displays regular query data in a graph. The following figure shows the Graph window.

Figure 4-14: Graph window



The items to be set are:

Graph

Displays regular query data in a line graph.

A graph consists of the title, vertical and horizontal axes, and line introductory notes (a label key identifying the lines). The vertical axis shows the values of the data, and the horizontal axis shows times and dates.#

You can display or hide the lines in a graph in the Line Configuration window. You cannot change the color of the lines.

#

Part of the rightmost time and date might be hidden.

The following table lists the menu commands.

Menu bar	Menu command	Description
File	Close	Closes the Graph window.
View	Zoom In	Zooms in a graph.
	Zoom Out	Zooms out a graph.
	Show All	Releases the zoom in or out mode.
Option	Line Configuration	Displays the Line Configuration window.

Zooming in or out with the mouse

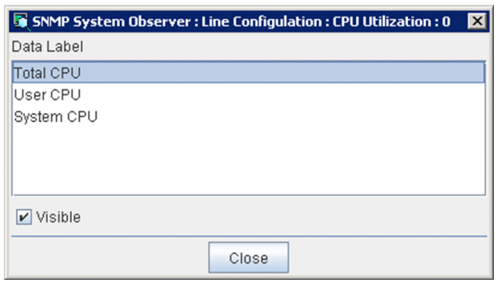
Dragging toward the lower right: Enlarges the dragged area.

Dragging toward other directions: Cancels the enlarge mode.

Line Configuration window

Displays or hides lines in the Graph window. The following figure shows the Line Configuration window.

Figure 4-15: Line Configuration window



The items to be displayed are:

Data Label

Displays the names of the lines displayed in a graph.

Visible

Displays or hides the line selected in the **Data Label** area.

(1) Notes

- Maximum number of data items that can be displayed in a graph#
  - Number of lines: 32
  - Number of data items for each line: 20,000

#

The maximum number of data items that can be displayed in a graph might be restricted by operating environments. For details, see *4.2.3(1) Notes*.

- Lines in a graph

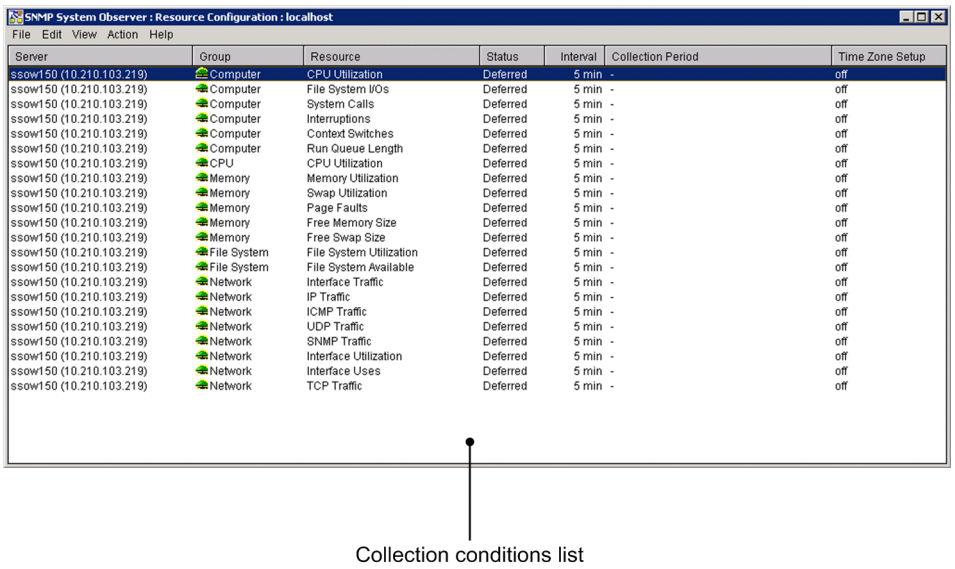
  Data items in a graph are connected without considering the continuity. For example, if you display the following regular query data in a graph in the Performance Data window, 11:00 and 12:00 are also connected by a line.

  - Started at 10:00, and stopped at 11:00
  - Started at 12:00, and stopped at 13:00

4.3 Resource Configuration window

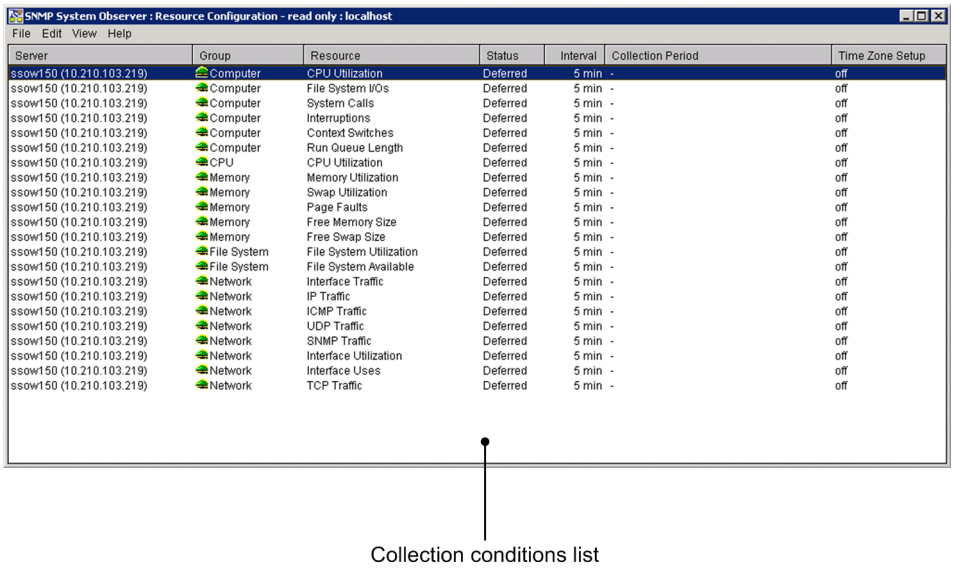
The Resource Configuration window displays the collection conditions and collection status. The following figure shows the Resource Configuration window.

Figure 4-16: Resource Configuration window



If the Resource Configuration window is already running, or a command used to set collection conditions (`ssocolset`) is being executed, the Resource Configuration window can be opened in reference mode. The following figure shows the Resource Configuration window (reference mode).

Figure 4-17: Resource Configuration window (reference mode)



The collection conditions list displays the set collection conditions and the collection status. The next table explains the menu items.

Menu bar	Menu command	Description
File	Change Connection[#1]	Displays the Server connection window.

Menu bar	Menu command	Description
Edit	Add Collection Condition	Displays the Add Collection Condition wizard. This command is deactivated and cannot be used if you start the window in reference mode.
	Copy Collection Condition	Displays the Copy Collection Condition window. This command is deactivated and cannot be used if you start the window in reference mode.
	Delete Collection Condition	Deletes the collection condition selected in the collection conditions list. This command is deactivated and cannot be used if you start the window in reference mode.
	Change Collection Condition	Displays the Change Collection Detail Condition window for the collection condition selected in the collection conditions list.
	Set Collection Time Band	Displays the Set Collection Time Zone window for the collection conditions selected in the collection conditions list.
	Change Collection Interval	Displays the Change Collection Interval window for the collection condition selected in the collection conditions list.
	Regular Calculation Setting	Displays the Regular calculation setting window.
	Threshold verification[#1]	Displays the DB selection window.
View	Updating Collection Condition[#2]	Obtains a collection condition again. You can use this function if you start the window in reference mode.
	Search Server	Displays the Search Server window.
Action[#3]	Start Collection	Displays the Start Collection window for the collection condition selected in the collection conditions list.
	Stop Collection	Terminates the collection selected in the collection conditions list.

#1

This command is not displayed if you start this window from the SSO console.

#2

This command is displayed if you start this window in reference mode.

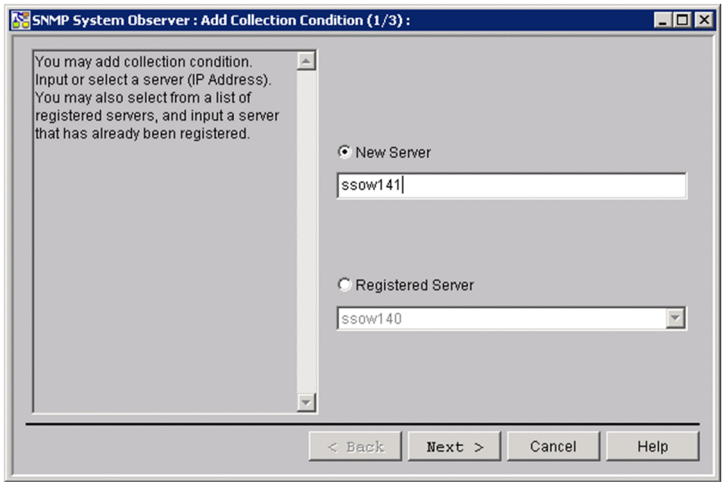
#3

This menu is not displayed if you start this window in reference mode.

4.3.1 Add Collection Condition wizard

The Add Collection Condition wizard adds a collection condition. Figures 4-18 to 4-20 show the Add Collection Condition wizard.

Figure 4－18: Add Collection Condition (1/3) wizard



The items to be set are:

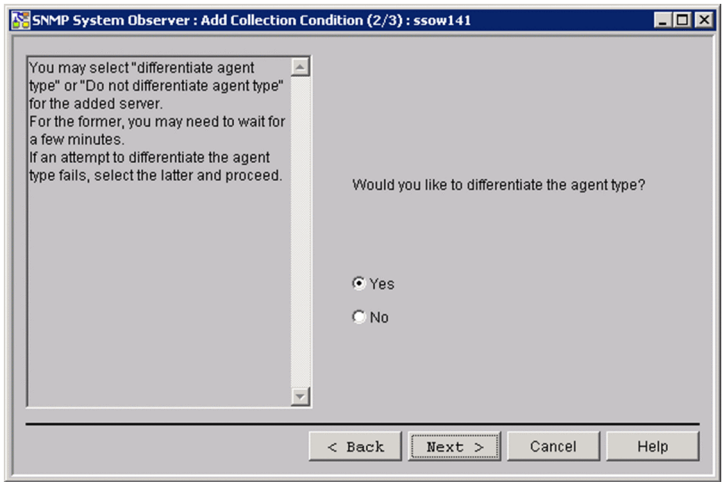
New server

Specify the host name or IP address of a server containing a resource to be collected. Specify the host name or IP address in 255 bytes or less.

Registered server

When you want to add a collection condition to a registered server, select a server in this box.

Figure 4－19: Add Collection Condition (2/3) wizard

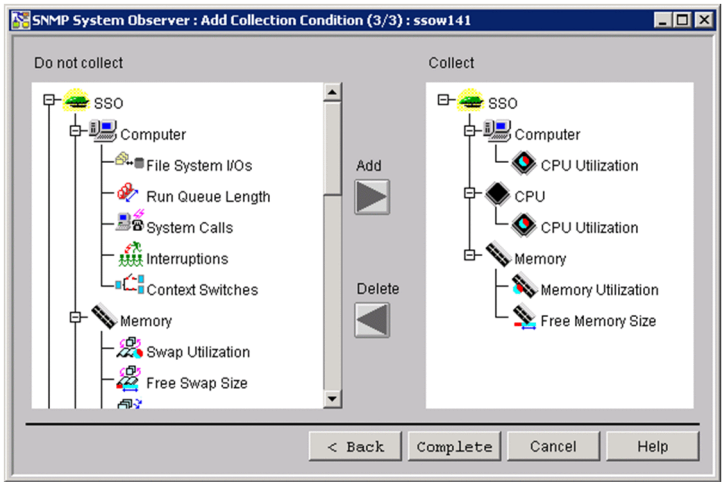


The items to be set are:

Yes / No

Select whether to judge the agent type. If you select **Yes**, the Add Collection Condition (3/3) wizard displays only the resources that can be obtained from the agent.

Figure 4-20: Add Collection Condition (3/3) wizard



The items to be set are:

Do not Collect

This area displays the resources that are not to be collected. Selecting a resource and clicking the **Add** button adds the resource to the **Collect area**.

Collect

This area displays the resources that are to be collected. Selecting a resource and clicking the **Delete** button deletes the resource from the **Collect area**.

Add

This button adds a resource to the **Collect area**. You can add resources by category, resource group, or in units of resources.

Delete

This button deletes a resource from the **Collect area**. You can delete resources by category, resource group, or in units of resources.

4.3.2 Change Collection Detail Condition window

The Change Collection Detail Condition window sets collection conditions such as thresholds. The appearance of this window differs slightly depending on the resource. Figures 4-21 to 4-23 show the Change Collection Detail Condition window.

Figure 4-21: Change Collection Detail Condition window (for Fixed threshold)

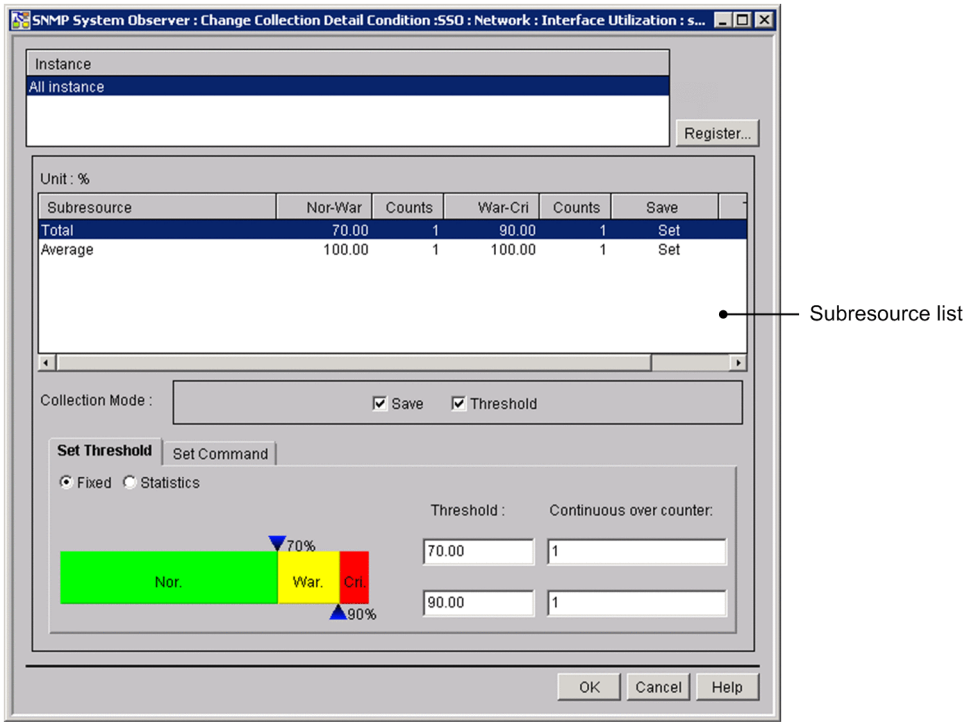


Figure 4-22: Change Collection Detail Condition window (for Statistical threshold)

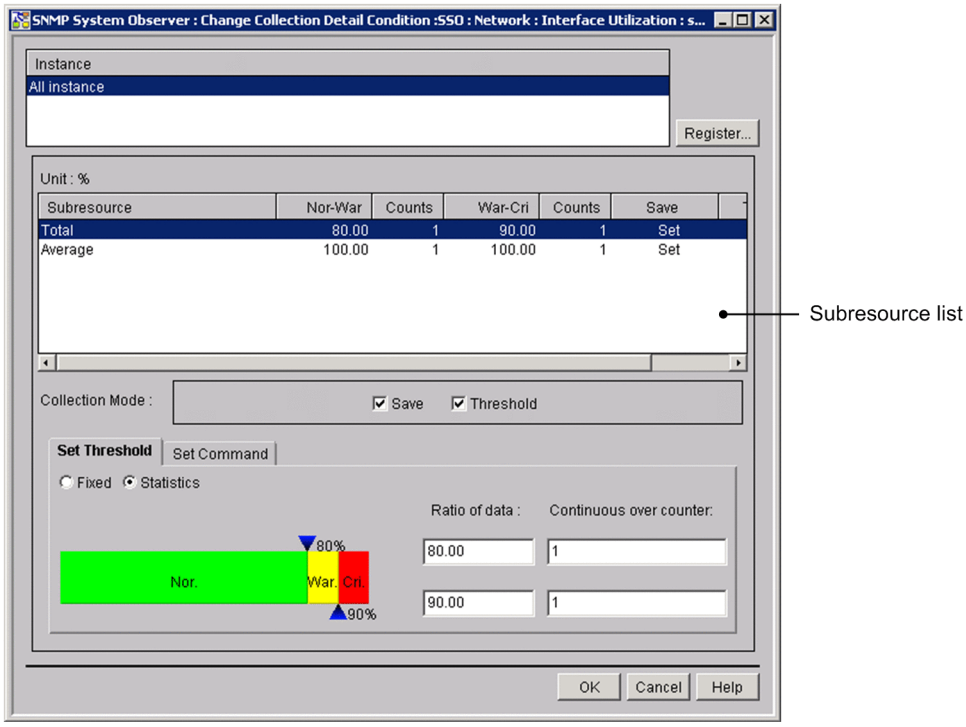
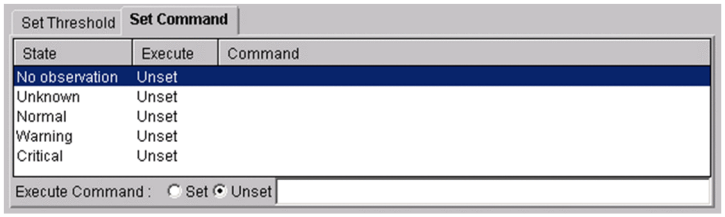


Figure 4-23: Change Collection Detail Condition window (Set Command)



The items to be set are:

Instance

This area displays a list of instances. If no instances have been registered, this area displays **All instance**. If you want to set collection conditions for a particular instance, you must register the instance in the Register Instance window.

Register

This button displays the Register Instance window or the Register Ping Address window.

Subresource list

This box displays the subresources and collection conditions for the instance selected in the instance list. You can set collection conditions for the subresource selected in this box in the **Collection Mode** area, **Set Threshold** tab, and **Set Command** tab.

Collection Mode

Save

Set whether SSO is to save collected data to the collection database.

Threshold

When you select this checkbox, SSO monitors collected data to see if it exceeds the set threshold and issues an event when it does exceed the threshold. Set a threshold in the **Set Threshold** tab.

Set Threshold tab

Specify whether to monitor a fixed threshold value or a statistical threshold value.

Fixed

Threshold

Specify a warning threshold and critical threshold. Specify the following resource thresholds as percentages:

- CPU Utilization (Computer group)
- CPU Utilization (CPU group)
- Memory Utilization
- Swap Utilization
- File System Utilization
- Interface Utilization (Network group)
- Interface Utilization (HighCapacityNetwork group)

You can specify 0 or any floating decimal point (double-precision real number) between $\pm 1.00 \times 10^{-2}$ and $\pm 1.7976931348623157 \times 10^{308}$ as a threshold. If the fixed-point part exceeds 1.7976931348623157, SSO rounds it off. If you set the same value for the warning threshold and critical threshold, the warning region is eliminated. You can therefore specify only one continuous over counter in this case.

Continuous over counter

Set the number of times that collected data must consecutively exceed the threshold before SSO changes the status of the resource. The specifiable range is 1 to 99. The default is 1.

Statistics

Ratio of data

When you gather statistics from collected data, specify in a percentage the ratios of the number of normal value collections, and the number of collections including a warning threshold against the total number of data collections. For example, assuming that normal values are collected 97 times, warning threshold values are collected twice, and a critical threshold value is collected once, the data ratios would be as follows:

```
Nor. - War.: (97/100)x100=97.00
War. - Cri.: ((97+2)/100)x100=99.00
```

Specify the data ratio by using either of the following methods:

- Move an icon above or below the slide bar to the left or right.
  The specifiable range is 0.01 to 99.99.
- Enter the ratio of standard normal distribution data in the applicable text box.
  The specifiable range is 0.01 to 99.99.

Continuous over counter

Set the number of times that collected data must consecutively exceed the threshold, which is calculated from the data ratio set from the collected data values, before the resource status changes. The specifiable range is 1 to 99. The default is 1.

Set Command tab

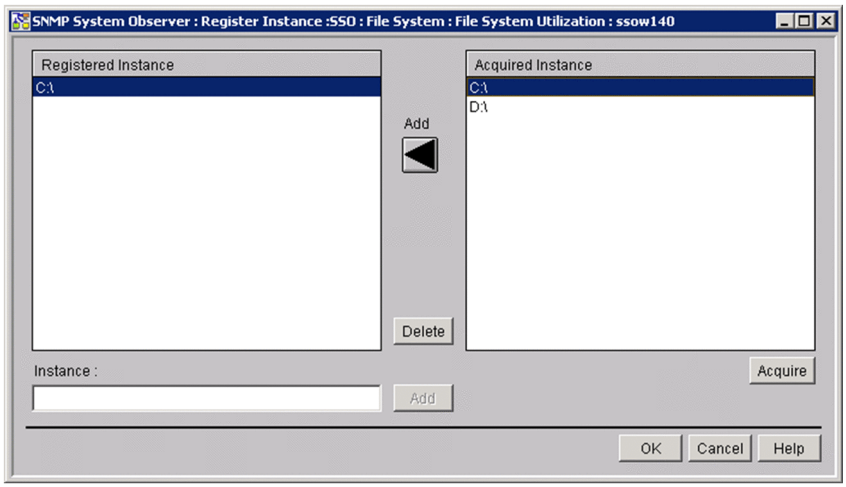
Specify the command that is to be executed when the status of the resource changes. If you selected **Set** in the **Execute command:** area, specify a command name with a character string of 1 to 259 bytes.

For details on automated actions, see *2.2.3(4) Automated action*.

4.3.3 Register Instance window

The Register Instance window registers an instance when you want to collect resources for a particular instance. The following figure shows the Register Instance window.

Figure 4-24: Register Instance window



The items to be set are:

Registered Instance

This box displays the registered instances.

Acquired Instance

This box displays instances acquired from the agent targeted for collection. If you selected a resource for which you cannot obtain an instance or if the agent targeted for collection is not running, the list of instances cannot be displayed.

Add

This button adds an instance to the **Registered Instance** box.

Delete

This button deletes an instance from the **Registered Instance** box.

Instance

Specify the instance to be registered with a character string of 1 to 255 bytes.

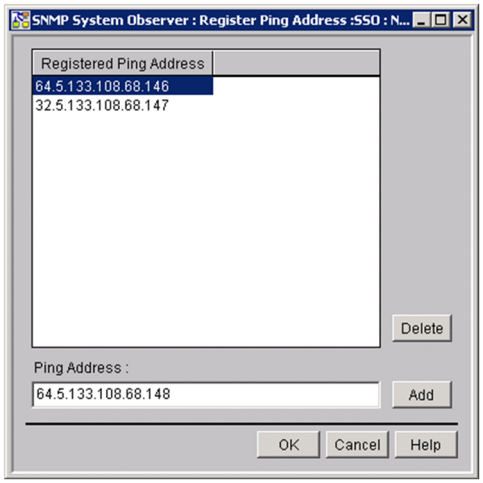
Acquire

This button obtains a list of instances from the agent targeted for collection and displays it in the **Acquired Instance** box.

4.3.4 Register Ping Address window

The Register Ping Address window registers a ping address as an instance. The following figure shows the Register Ping Address window.

Figure 4-25: Register Ping Address window



The items to be set are:

Registered Ping Address

This box displays a list of registered addresses.

Delete

This button deletes an address from the **Registered Ping Address** box.

Ping Address

Specify a ping packet size, timeout length, and IP address, delimiting the values with a period (.). You can omit the packet size and timeout length, but you cannot omit the period (.). The next table explains the items to be specified.

Item	Description
Packet size	Specify a packet size in 32 to 2048 bytes. The default is 64 bytes.
Timeout length	Specify a timeout length between 1 and 60 seconds. The default is 5 seconds.
IP address (for IPv4)	Specify an IP address in the format *n.n.n.n* (where *n* is an integer between 0 and 255). However, you cannot specify 0.0.0.0 or 255.255.255.255.
IP address (for IPv6)	Specify an IP address in the format *n:n:n:n:n:n:n:n* (where *n* is a hexadecimal number between 0000 and ffff). Note that the address 0000 can be replaced with :: (two consecutive colons).

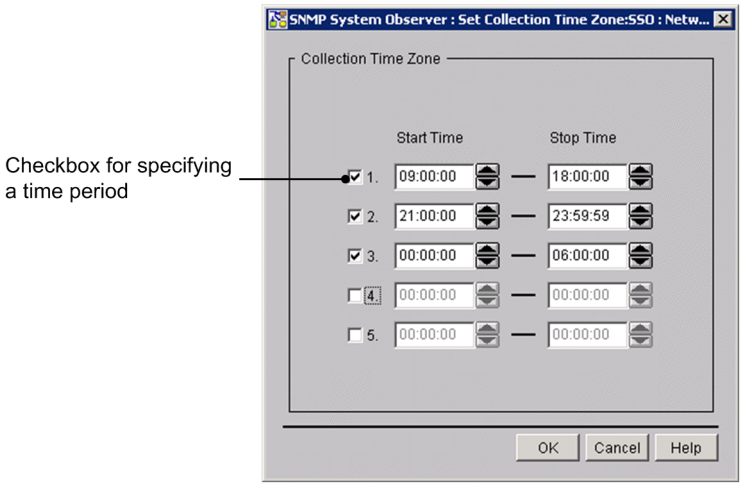
Add

This button adds the information entered to the **Ping Address** box to the **Registered Ping Address** box.

4.3.5 Set Collection Time Zone window

The Set Collection Time Zone window sets a time period during which resources are to be collected. The following figure shows the Set Collection Time Zone window.

Figure 4-26: Set Collection Time Zone window (for collecting resources)



The items to be set are:

Checkbox for specifying a time period

Set whether to enable the specified collection time period. Only a time period in a selected line is enabled. By default, no time period is specified.

Start Time

Specify a time for starting collection between 00:00:00 and 23:59:59.

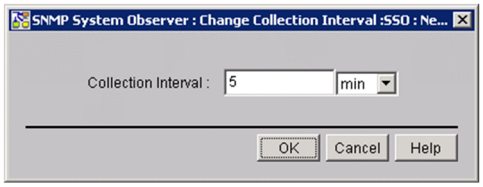
Stop Time

Specify a time for stopping collection between 00:00:00 and 24:00:00. Specify a later time than the start time.

4.3.6 Change Collection Interval window

The Change Collection Interval window sets an interval at which to collect resources. The following figure shows the Change Collection Interval window.

Figure 4-27: Change Collection Interval window



The items to be set are:

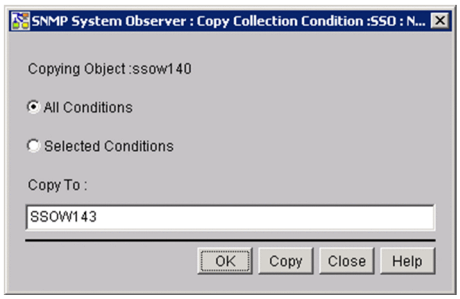
Collection Interval

Specify a collection interval between 10 seconds and 24 hours. You can select **sec**, **min**, or **hour** as the unit of time. The default is 5 minutes.

4.3.7 Copy Collection Condition window

The Copy Collection Condition window copies collection conditions to a remote host. The following figure shows the Copy Collection Condition window.

Figure 4-28: Copy Collection Condition window



The items to be set are:

Copying Object

This area displays the hosts (copy sources) for which collection conditions are set.

All Conditions

This button copies all the collection conditions set for the copy source host to the copy destination.

Selected Conditions

This button copies only the collection conditions of the resource selected in the Resource Configuration window to the copy destination.

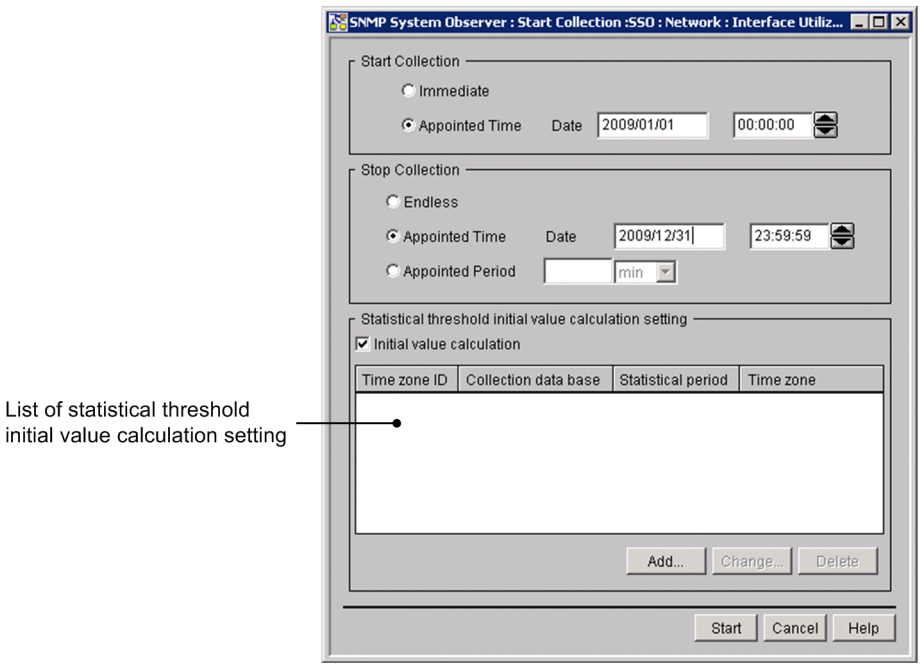
Copy To

Specify the host name or IP address of the copy destination in 255 bytes or less. If you want to specify multiple host names or IP addresses, separate them by a space. You can specify them within 1,024 bytes.

4.3.8 Start Collection window

The Start Collection window sets a collection period and starts collection. The following figure shows the Start Collection window.

Figure 4-29: Start Collection window



The items to be set are:

Start collection

Immediate

Clicking the Start button starts collection immediately.

Appointed Time

SSO starts collection when the specified date and time are reached. In the Date fields, specify a date between January 1, 1980 and December 31, 2029 in the format *yyyy/mm/dd*. Specify a time between 00:00:00 and 23:59:59 in the format `00:00:00`.

Endless

SSO continues collecting resources until the user instructs it to stop.

Appointed Time

SSO stops collecting resources when the specified date and time are reached.

In the Date fields, specify a date between January 1, 1980 and December 31, 2029 in the format *yyyy/mm/dd*. Specify a time between 00:00:00 and 23:59:59 in the format `00:00:00`. When you have specified a collection start date and time, specify a later date and time for stopping collection.

Appointed Period

SSO stops collecting resources when the specified period has elapsed since collection started.

The specifiable range is 1 minute to 31 days (44,640 minutes). You can specify any value between 1 and 44,640. You can select **min**, **hour**, or **days** as the unit of time.

Statistical threshold initial value calculation setting

Specify settings for calculating the initial value. If multiple collection conditions are selected in the Resource Configuration window, you cannot specify this setting.

Initial value calculation

Select this check box when you want to activate the deactivated list of statistical threshold initial value calculation settings, and the **Add**, **Change**, and **Delete** buttons.

When no information is displayed in the list of statistical threshold initial value calculation settings, the initial value is not calculated.

List of statistical threshold initial value calculation setting

Displays the list of statistical threshold initial value calculation settings you specified in the Initial value calculation setting window. By default, the list is blank.

Add

Displays the Initial value calculation setting window. For details on the Initial value calculation setting window, see *4.3.10 Initial value calculation setting window*.

Change

Changes settings selected in the list of statistical threshold initial value calculation settings.

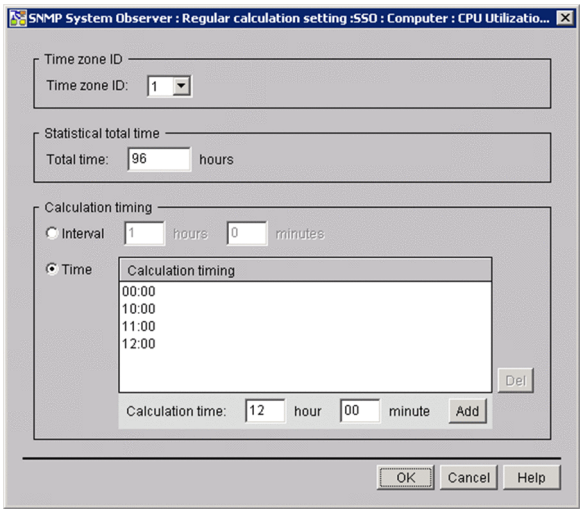
Delete

Deletes settings selected in the list of statistical threshold initial value calculation settings.

4.3.9 Regular calculation setting window

The Regular calculation setting window sets the information necessary to calculate a statistical threshold regularly. The following figure shows the Regular calculation setting window.

Figure 4-30: Regular calculation setting window



Note

Some GUI characters might be hidden. If this happens, enlarge the window.

The items to be set are:

Time zone ID

Specify the time zone ID. The specifiable range is 1 to 10. The default is 1.

Statistical total time

Specify 24 to 720 (hours) as the period for extracting data that is needed for calculating a statistical threshold. The default is 96 hours.

Calculation timing

Interval

Select this radio button to specify the interval for calculating a threshold. The specifiable range is 15 minutes to 60 hours. By default, an interval of 1 hour is set.

Time

Select this radio button to specify the time at which a threshold is to be calculated. By default, the time is not set.

Del

Deletes the time selected from the calculation timing list.

Calculation time

You can specify the calculation period between 00:00 and 23:59.

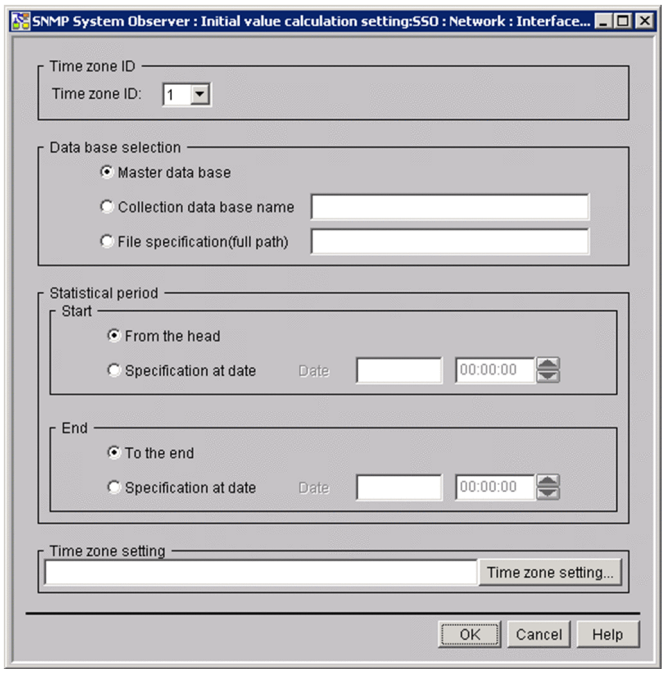
Add

Adds the time you specified to the **Calculation timing** list.

4.3.10 Initial value calculation setting window

The Initial value calculation setting window sets the conditions for extracting data for the initial value calculation of a statistical threshold value. The following figure shows the Initial value calculation setting window.

Figure 4-31: Initial value calculation setting window



The items to be set are:

Time zone ID

Assign the time zone ID to the period for extracting data for the initial value calculation. The specifiable range is 1 to 10. The default is 1.

Data base selection

Master data base

Select this radio button to select the master database.

Collection data base name

Select this radio button to select the master database or a copy database.

If you want to specify a collection database, enter the file name only.

File specification(full path)

Select this radio button to specify a collection database in a location other than the collection database storage directory.

Enter the full path name when you specify a file.

Statistical period

Specify the time to start and end data extraction.

Start

- **From the head**

  Extracts data from the top of the specified collection database.

- **Specification at date**

  Extracts data on or after the specified date and time in the specified collection database.

  For the **Date** text box, specify the date and time when you want to start extracting data in the collection database.

  Specify a date from January 1st, 1980 to December 31, 2029 in *yyyy*/*mm*/*dd* format. Specify the time from 00:00:00 to 23:59:59 in *00*:*00*:*00* format.

  The **Date** text box is activated only when you select to specify the date and time.

End

- **To the end**

  Extracts data to the end of the specified collection database.

- **Specification at date**

  Extracts data on or before the specified date in the specified collection database.

  For the **Date** text box, specify the date and time when you want to stop extracting data in the collection database.

  Specify a date from January 1st, 1980 to December 31, 2029 in *yyyy*/*mm*/*dd* format. Specify the time from 00:00:00 to 23:59:59 in *00*:*00*:*00* format.

  If you specified the date and time to start data extraction, specify a date and time on or after the start date and time.

Time zone setting

Displays the extraction time zone you specified in the Set Collection Time Zone window.

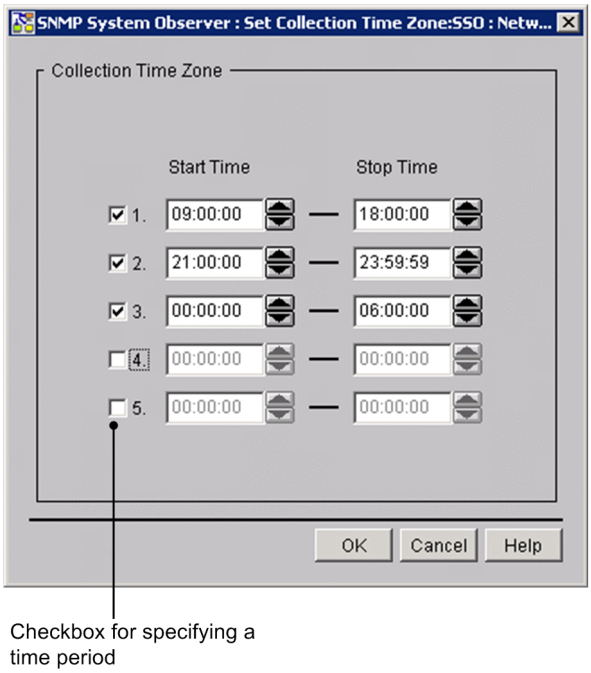
Time zone setting

Opens the Set Collection Time Zone window. For details on the Set Collection Time Zone window, see *4.3.11 Set Collection Time Zone window*.

4.3.11 Set Collection Time Zone window

The Set Collection Time Zone window sets the period for collecting data for calculating the initial value of the statistical threshold. The following figure shows the Set Collection Time Zone window.

Figure 4-32: Set Collection Time Zone window (for collecting statistical threshold data)



The items to be set are:

Checkbox for specifying a time period

Specify whether to activate the specified collection period. Only the selected periods are activated. By default, no time period is selected.

Start Time

Specify the time to start collection from 00:00:00 to 23:59:59.

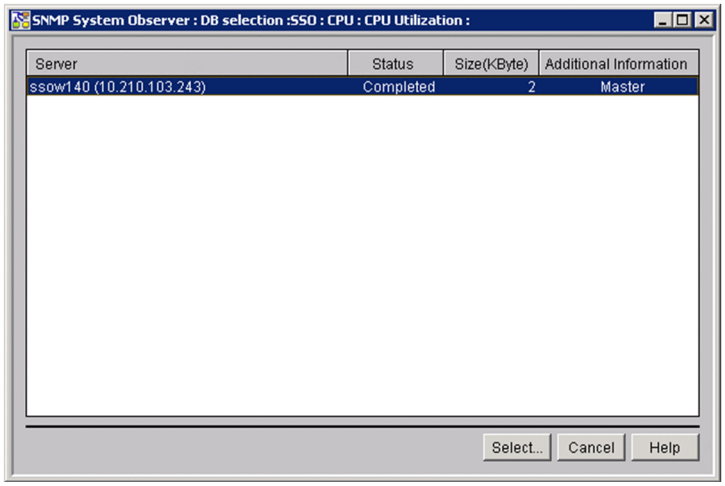
Stop Time

Specify the time to stop collection from 00:00:01 to 24:00:00. Specify a time after the start time.

4.3.12 DB selection window

The DB selection window selects the database that is used to verify the threshold from the list of collection databases. The following figure shows the DB selection window.

Figure 4－33: DB selection window



The items to be set are:

Server

Displays the names of the monitored servers for which resources are monitored.

Status

Displays the collection status of the database.

For the master database, the collection status is displayed. For a copy database, or a database for which collection conditions have been deleted, a hyphen (－) is displayed.

Size(KByte)

Displays the size of the collection database in kilobytes.

Decimal numbers are rounded up.

Additional Information

Displays additional information.

If the displayed database is the master file, `Master` is displayed. For a copied file, `Copy` is displayed.

Select

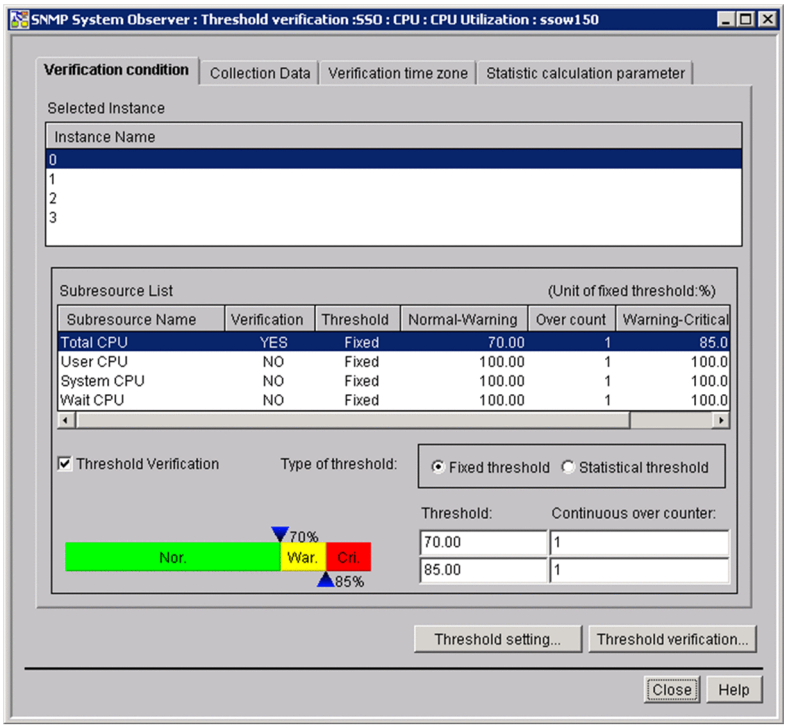
Select the database to be verified.

You can select only one database.

4.3.13 Threshold verification window

The Threshold verification window sets the information necessary to verify thresholds from the collected data. The following figure shows the Threshold verification window.

Figure 4-34: Threshold verification window



Note

Some GUI characters might be hidden. If this happens, enlarge the window.

The items to be set are:

Verification condition tab

Select this tab to set the conditions for verifying the method of verifying thresholds. For descriptions about display items in the **Verification condition** tab, see *4.3.13(1) Verification condition tab*.

Collection Data tab

Select this tab to set the conditions for the data of which threshold you want to verify. For descriptions about display items in the **Collection Data** tab, see *4.3.13(2) Collection Data tab*.

Verification time zone tab

Select this tab to set the time zone for verifying thresholds. For descriptions about display items in the **Verification time zone** tab, see *4.3.13(3) Verification time zone tab*.

Statistic calculation parameter tab

Select this tab to set the time when a statistical threshold is to be calculated. For descriptions about display items in the **Statistic calculation parameter** tab, see *4.3.13(4) Statistic calculation parameter tab*.

Threshold setting

Displays the Selection threshold setting ahead window.

For details on the Selection threshold setting ahead window, see *4.3.14 Selection threshold setting ahead window*. You can click this button when you specify the applicable items in the **Subresource List**.

Threshold verification

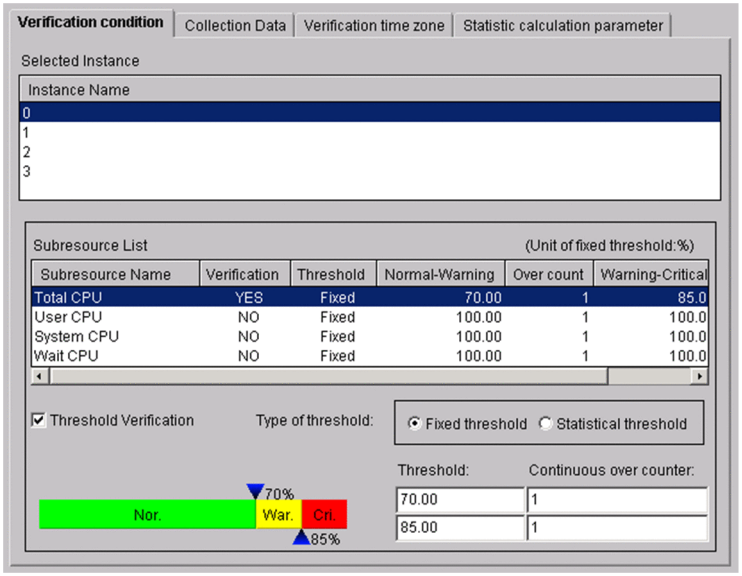
Verifies thresholds, and opens the Threshold verification result window.

For details on the Threshold verification result window, see *4.3.15 Threshold verification result window*.

While thresholds are being verified, the command prompt is displayed. Do not close it during verification.

(1) Verification condition tab

Figure 4-35: Threshold verification window (Verification condition tab)



The items to be set are:

Selected Instance

The instance name of the collected data is displayed.

Select the name of the instance of the threshold you want to verify.

Subresource List

This list is displayed only when you have selected an instance name in the Instance Selection window.

Select the name of the subresource of the threshold you want to verify.

Threshold verification

Select this check box when you want to specify the type of the threshold and verification conditions.

Select both a subresource name in **Subresource List** and this check box. By doing so, you can specify the type of the threshold, the threshold or data ratio, and the value for **Continuous over counter**. In addition, when you select this check box, display in the **Verification** column of **Subresource List** changes from `NO` to `YES`.

By default, this check box is not selected.

Type of threshold

Specify the method for verifying the threshold. By default, **Fixed threshold** is selected.

Fixed threshold

Verifies the threshold by using the fixed threshold method.

When you select this method, the **Threshold** and **Continuous over counter** columns are displayed.

For the **Threshold** column, specify the warning threshold and the critical threshold.

You can specify 0 or any floating decimal point between $\pm 1.00 \times 10^{-2}$ and $\pm 1.7976931348623157 \times 10^{308}$. If the value in the mantissa exceeds 1.7976931348623157, it is rounded.

For **Continuous over counter**, set the number of times that collected data must consecutively exceed the threshold before SSO changes the resource status. You can specify a value from 1 to 99.

If you set the same value for the warning threshold and the critical threshold, the warning region is eliminated. Therefore, in such a case, you can specify only one value.

Statistical threshold

Verifies the threshold by using the statistical threshold method.

When you select this method, the **Ratio of data** and **Continuous over counter** columns are displayed.

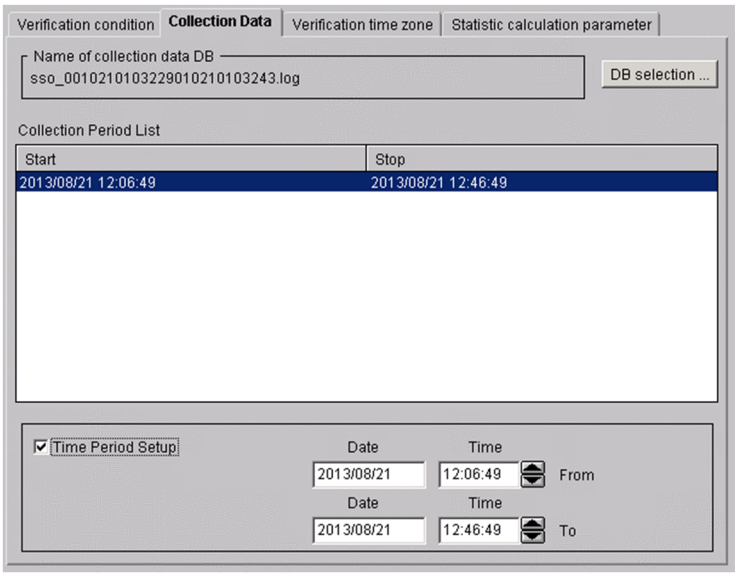
For **Ratio of data**, specify the data ratio in the warning region and the critical region of the threshold. You can specify a value from 0.01 to 99.99.

For **Continuous over counter**, set the number of times that collected data must consecutively exceed the threshold before SSO changes the resource status. You can specify a value from 1 to 99.

If you set the same value for the warning threshold and the critical threshold, the warning region is eliminated. Therefore, in such a case, you can specify only one value.

(2) Collection Data tab

Figure 4-36: Threshold verification window (Collection Data tab)



The items to be set are:

Name of collection data DB

Displays the name of the database in which data that has the thresholds to be verified is collected.

DB selection

This button displays the DB selection window. For details on the DB selection window, see *4.3.12 DB selection window*.

Collection Period List

This box displays the collection period of the data in the selected database. If only the collection start date is displayed, it means that the data is currently being collected. You can select multiple lines as long as they are adjacent.

Time Period Setup

Select this check box to narrow down the collection period of the data to be verified.

When you select this check box, you can specify a specific period based on the range within the collection period.

Date

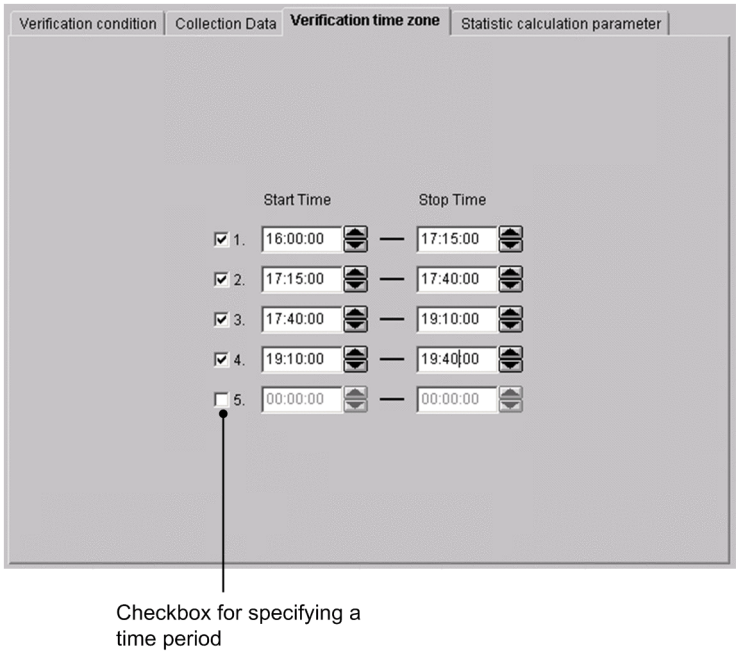
Specify a range between January 1, 1980 and December 31, 2029 in the *yyyy/mm/dd* format. You can specify a range if you selected **Time Period Setup**.

Time

Specify a range between 00:00:00 and 23:59:59 in the 00:00:00 format. You can specify a range if you selected **Time Period Setup**.

(3) Verification time zone tab

Figure 4-37: Threshold verification window (Verification time zone tab)



The items to be set are:

Check box for specifying a time period

Specify whether to activate the specified verification period. Only the time zone for the selected line is activated. By default, no time zone is specified.

Start Time

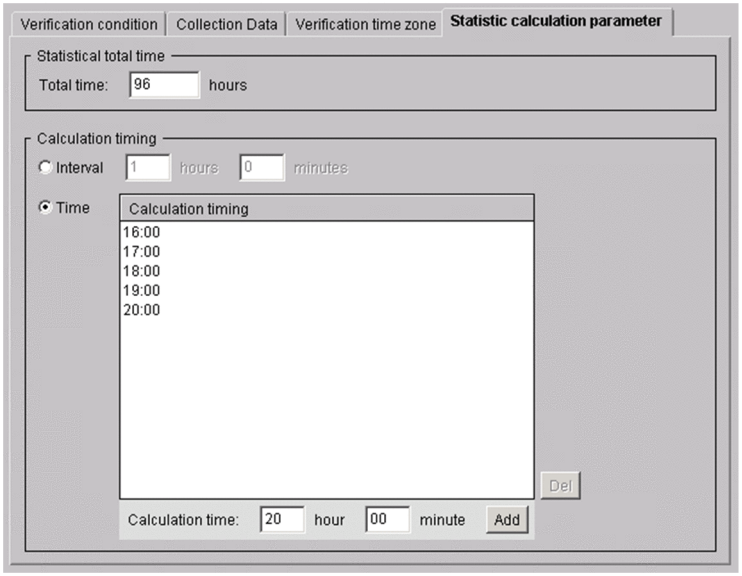
Specify the time to start verification in the range from 00:00:00 to 23:59:59.

Stop Time

Specify the time to stop verification in the range from 00:00:01 to 24:00:00. Specify a time after the start time.

(4) Statistic calculation parameter tab

Figure 4-38: Threshold verification window (Statistic calculation parameter tab)



The items to be set are:

Statistical total time

Specify 24 to 720 (hours) as the period for extracting data that is needed for calculating a statistical threshold. The default is 60 hours.

Calculation timing

Interval

Select this radio button to specify the interval for calculating a threshold. The specifiable range is 15 minutes to 24 hours. By default, an interval of 1 hour is set.

Time

Select this radio button to specify the time at which a threshold is to be calculated. By default, the time is not set.

Del

Deletes the time selected from the calculation timing list.

Calculation time

You can specify the calculation period between 00:00 and 23:59.

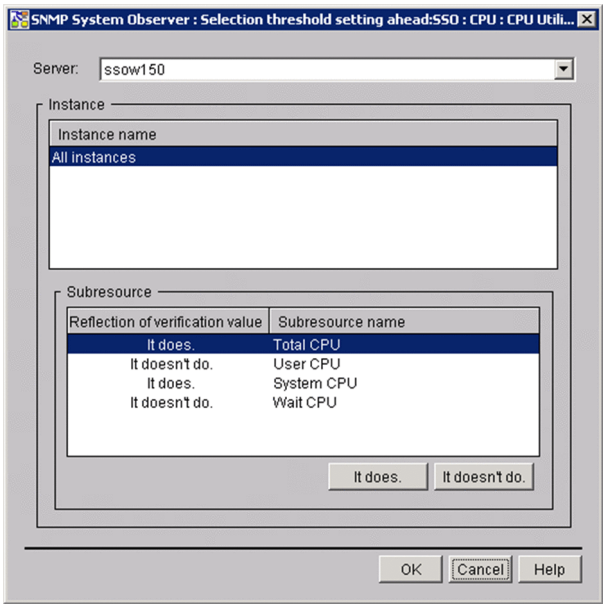
Add

Adds the time you specified to the **Calculation timing** list.

4.3.14 Selection threshold setting ahead window

The Selection threshold setting ahead window applies the threshold verification result to the collection condition. The following figure shows the Selection threshold setting ahead window.

Figure 4-39: Selection threshold setting ahead window



The items to be set are:

Server

A list of monitored servers to which you can apply the verification result is displayed. Select the server to which you want to apply the verification result.

Instance

A list of instances that are set as a collection condition of the selected monitored server is displayed.

Subresource

A list of subresources corresponding to the selected instance is displayed. Subresources that show `It does` in the **Reflection of verification value** column will be the target for applying verification values. Note that only subresources for which threshold verification is performed show `It does` in the **Reflection of verification value** column.

It does

Changes the **Reflection of verification value** column of the item selected in the **Subresource** list to `It does`.

It doesn't do

Changes the **Reflection of verification value** column of the item selected in the **Subresource** list to `It doesn't do`.

OK

Displays the Change Collection Detail Condition window to which the verification result is applied.

For details on the Change Collection Detail Condition window, see *4.3.2 Change Collection Detail Condition window*.

The verification result is not applied to the collection condition until you click the **OK** button in the Change Collection Detail Condition window.

4.3.15 Threshold verification result window

The Threshold verification result window displays the result of a threshold verification. The following figure shows the Threshold verification result window.

Figure 4-40: Threshold verification result window (for Selected subresource)

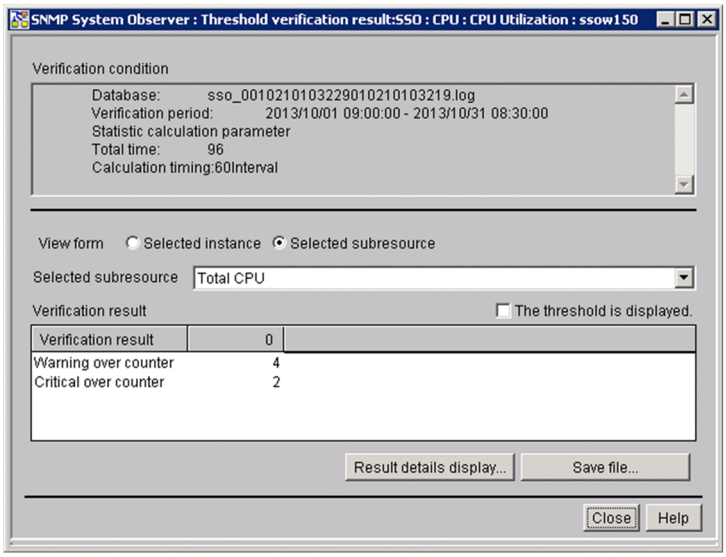
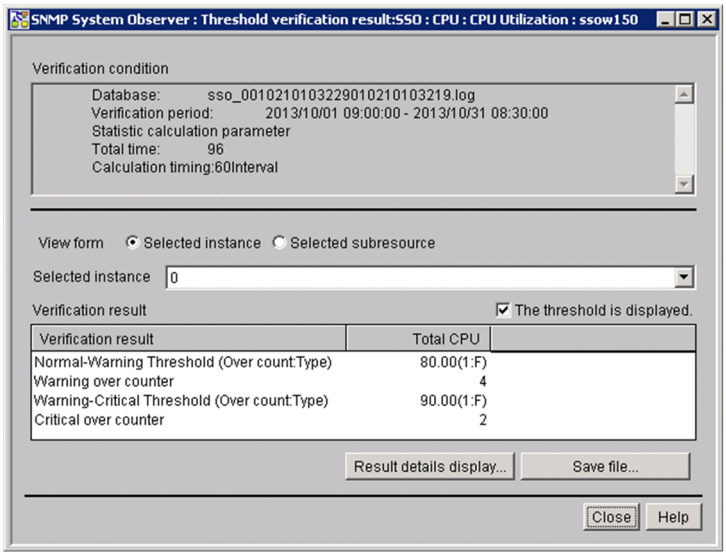


Figure 4-41: Threshold verification result window (for Selected instance)



The items to be set are:

Verification condition

Displays the list of verification settings you specified when you verify a threshold. The items to be displayed include any verification conditions.

The following items are displayed:

- **Database**

  Displays the name of the database in which you want to verify a threshold.

- **Verification period**

  Displays the verification period of a threshold. If the period is changed for each threshold, the period after the change is displayed.

- **Verification time zone**

  This item is displayed if the verification time zone is specified as a verification condition.

- **Statistic calculation parameter Total time**

Displays the total time set in the **Statistic calculation parameter** tab of the Threshold verification window.

- **Calculation timing**

  Displays the calculation timing set in the **Statistic calculation parameter** tab of the Threshold verification window.

View form

Displays the display format of the verification result. By default, **Selected instance** is selected.

- **Selected instance**

  Select this radio button to display the verification result for each instance. When this button is selected, the **Selected instance** text box is displayed.

  Select the instance you want to display in **Selected instance**.

- **Selected subresource**

  Select this radio button to display the verification result for each subresource. When this button is selected, the **Selected subresource** text box is displayed.

  Select the subresource you want to display in **Selected subresource**.

The threshold displayed

Select this check box to display the setting value for verifying a threshold. When you select this check box, the value you set for **Threshold verification** in the **Verification condition** tab of the Threshold verification window is displayed as detailed information. By default, this check box is not selected.

Verification result

Displays the result of a threshold verification for each instance or subresource. The displayed information is the number of times that a threshold exceeds the warning region and the critical region.

Result details display

Displays the Threshold verification result detailed information window. For details on the Threshold verification result detailed information window, see *4.3.16 Threshold verification result detailed information window*.

Save file

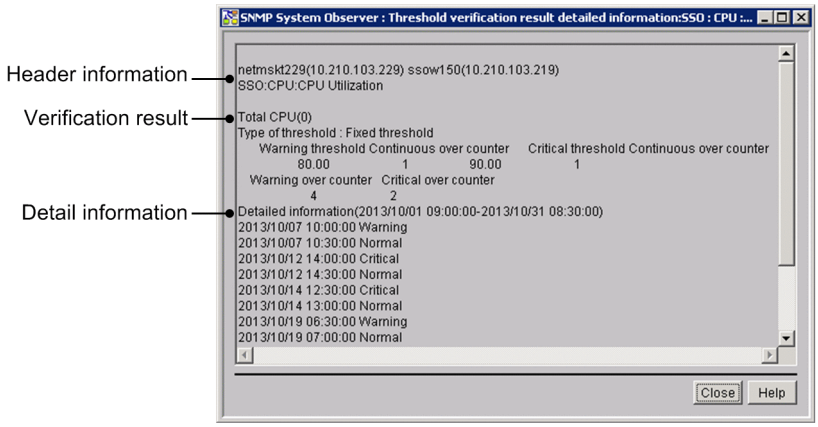
Displays the Save file window.

For details on the Save file window, see *4.3.17 Save file window*.

4.3.16 Threshold verification result detailed information window

The Threshold verification result detailed information window displays detailed information of the threshold verification result. The following figure shows the Threshold verification result detailed information window.

Figure 4-42: Threshold verification result detailed information window



The items to be set are:

Note that the lines after 500th line are not displayed because the maximum number of lines that can be displayed in this window is 500.

Header information

The following information, which is specified as verification conditions for verifying thresholds, is displayed:

- Collecting server
- Server targeted for collection
- Name of the resource to be verified

Verification result

The following information is displayed as the threshold verification result:

- Subresource name
- Instance name
- Type of threshold
- Statistical total time
- Calculation timing
- Warning threshold, critical threshold and continuous over counter
- Warning and critical over counter

Detail information

Displays status changes of the period and the result of the threshold verification.

Note that some detailed log data might not be displayed because the maximum number of lines that can be displayed in this window is 500.

4.3.17 Save file window

The Save file window saves the threshold verification result in a file. The following figure shows the Save file window.

Figure 4-43: Save file window (for selected instance)

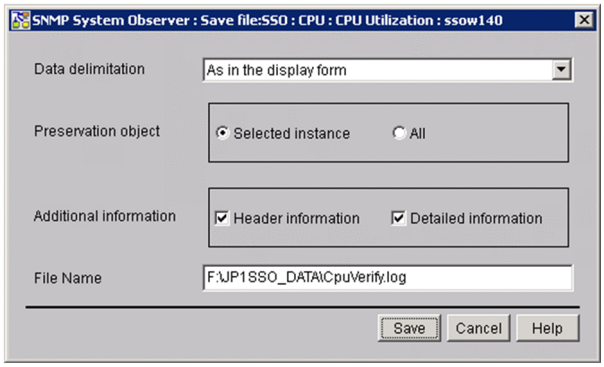
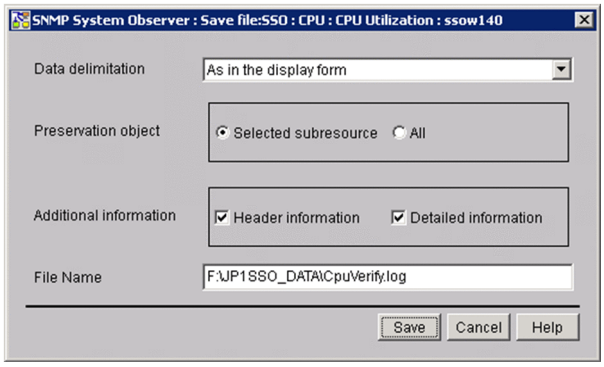


Figure 4-44: Save file window (for selected subresource)



The items to be set are:

Data delimitation

Specify the delimiter you want to use.

As in the display form

Adjusts the layout by using multiple spaces, and outputs the data as displayed in the Threshold verification result window to a file.

Delimit by comma, **Delimit by tab**, and **Delimit by space**

Separates data items by using the specified delimiter.

Preservation object

Specifies information to be output to a file.

Selected instance or **Selected subresource**

Select this radio button to display only the verification result in the form you selected by using **Verification form** in the Threshold verification result window.

All

Select this radio button to display all threshold verification results.

Additional Information

Specifies information to be output to a file.

Header information

Select this check box to output the title of data to a file.

Detailed information

Select this check box to output the threshold verification result and detailed log to a file.

File Name

Specify the full-path name and the absolute path name of the file. You cannot omit the file name.

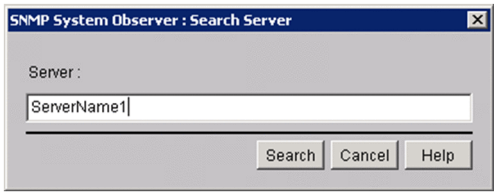
Save

Saves data in the specified file.

4.3.18 Search Server window

The Search Server window searches collection conditions for each server name. The following figure shows the Search Server window.

Figure 4-45: Search Server window



The items to be set are:

Server

Specify the host name or the IP address for the name of the server you want to search based on the collection conditions. You can specify a maximum of 255 bytes.

Search

Start a search with the condition specified for **Server**.

Searches conditions from the top of the collection condition list, and moves the items that are perfect matches to the collection condition of the applicable server. If no server name matches perfectly, the selected item is moved to the collection condition of the server that has the name which was found first through a forward match.

If no applicable server name exists, a warning dialog box appears.

When you specify an IP address in the **Server** text box, a matching string is searched through the IP address section in the list of collection conditions.

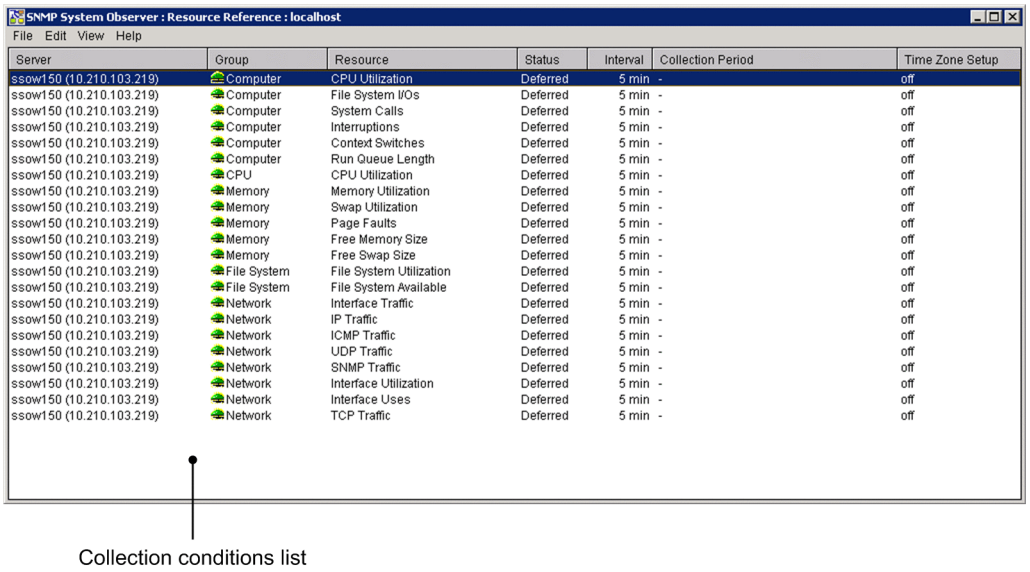
Important note

If the OS that opened the window is UNIX, the host names are case sensitive. Be careful when you enter the server name as a collection condition.

4.4 Resource Reference window

The Resource Reference window displays collection conditions or collection statuses. The following figure shows the Resource Reference window.

Figure 4-46: Resource Reference window



The collection conditions list shows the collection conditions or collection statuses set. The next table explains the menu items.

Menu bar	Menu command	Description
File	Change Connection#1	Displays the Server connection window.
Edit	Copying Collection Data	Displays the Change Collection Detail Condition window for the collection conditions selected from the collection conditions list.
	Set Collection Time Zone	Displays the Set Collection Time Zone window for the collection conditions selected from the collection conditions list.
	Change Collection Interval	Displays the Change Collection Interval window for the collection conditions selected from the collection conditions list.
	Regular Calculation Setting	Displays the Regular calculation setting window.
	Threshold verification#	Displays the DB selection window.
View	Updating Collection Condition	Obtains a collection condition again.

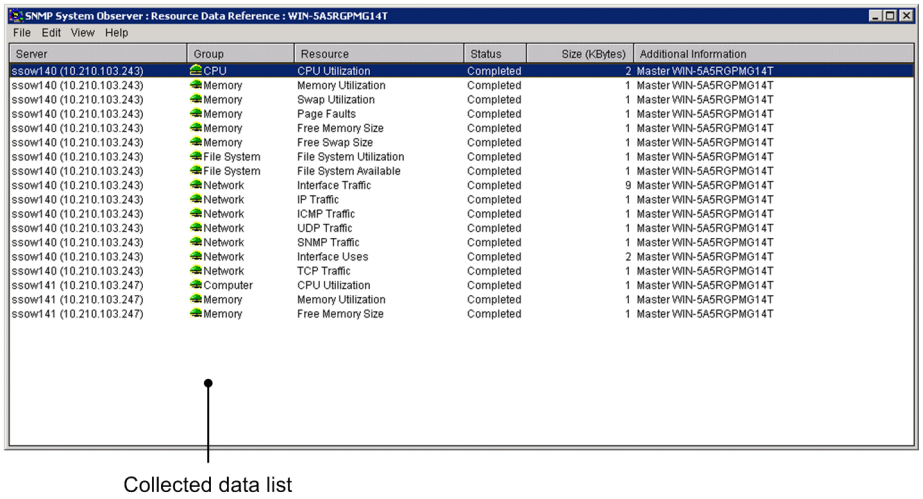
#

The menu command is not displayed if you opened the window from the SSO console.

4.5 Resource Data Reference window

The Resource Data Reference window references collected data. The following figure shows the Resource Data Reference window.

Figure 4-47: Resource Data Reference window



The collected data list displays not only the collected resources but also the size of the collection database and information indicating whether the database is a master database or copy database. The next table explains the menu items.

Menu bar	Menu command	Description
File	Change Connection#1	Displays the Server connection window.
Edit	Copying Collection Data	Displays the Copy Collection Data window.#2
	Deleting Collection Data	Deletes the collection database containing the selected collected data.
	Partially Deleting Collection Data	Delete Collection Data window.#2
	Threshold verification#1	Displays the Threshold verification window.
View	Collection Data Details	Displays the Collection Data Detail window.
	Updating Collection Data List	Updates the collected data list to the latest information.
	Search Server	Displays the Search Server window. This menu command can be selected only when the collected data list contains at least one data item.

#1

The menu command is not displayed if you opened the window from the SSO console.

#2

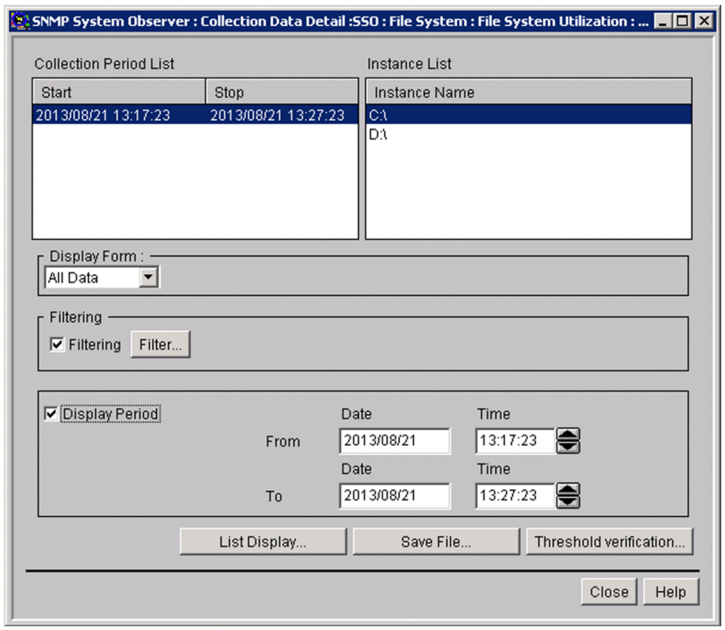
If the available space in a file system of a collection database is already insufficient (the available space is smaller than the maximum size of a data file in a collection database), delete the entire collection database from the **Deleting Collection Data** menu command to secure the available space in the file system. You cannot execute the **Copying Collection Data** and **Partially Deleting Collection Data** menu commands.

4.5.1 Collection Data Detail window

The Collection Data Detail window references the values of collected data. It displays the period during which the data was collected and the instance name. In this window, you select a date and time and an instance and reference the values

of the collected data. You can also filter the data to display only data within a specified range. The following figure shows the Collection Data Detail window.

Figure 4-48: Collection Data Detail window



The items to be set are:

Collection Period List

This box displays the collection period of the collected data. If only the collection start date and time are displayed, it means that the data is currently being collected. You can select multiple lines as long as they are adjacent.

Instance List

This box displays the instances for which resources were collected.

Display Form:

All Data

SSO displays the collected data as is.

Daily Data

SSO displays the data collected over one day.

Monthly Data

SSO displays the data collected over one month.

Filtering

Select this checkbox when you want to filter collected data. You can specify a range of values for each subresource and filter just those values.

Filter

This button displays the Set Filter Condition window.

Display Period

Select this checkbox when you want to specify the collection period of the data to be displayed. When this checkbox is selected, you can specify a period for displaying the collected data.

Date

Specify a range between January 1, 1980 and December 31, 2029 in the format *yyyy/mm/dd*. You can specify a range if you selected the **Display Period** checkbox.

Time

Specify a range between 00:00:00 and 23:59:59 in the format `00:00:00`. You can specify a range if you selected the **Display Period** checkbox.

List Display

This button displays the collected data selected in Collecting Period List and Instance List, in the Listing Display window.

Save file

This button displays the Save file window.

For details on the Save file window, see *4.5.4 Save File window*. If you opened this window from the SSO console, this button is not displayed.

Threshold verification

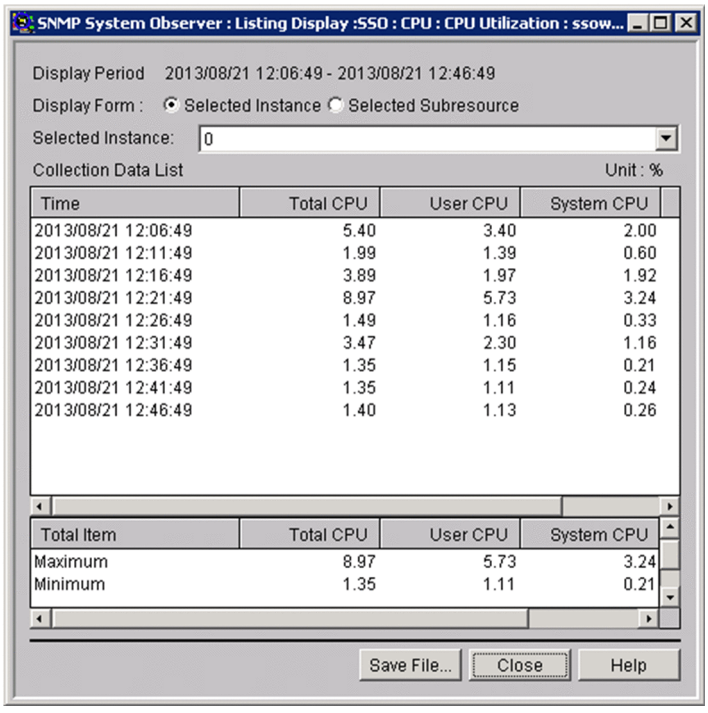
This button displays the Threshold verification window.

For details on the Threshold verification window, see *4.5.7 Threshold verification window*. If you opened this window from the SSO console, this button is not displayed.

4.5.2 Listing Display window

The Listing Display window displays a list of the data collected at each time. You can display the data by subresource or by instance. The following figure shows the Listing Display window.

Figure 4-49: Listing Display window



The items to be set are:

Display Period

This field displays the period specified in the Collection Data Detail window.

Display Form

Select whether to display the collected data by instance or by subresource.

Selected Instance

This field is displayed if you selected the **Selected Instance** button in **Display Form:**.

Selected Subresource

This field is displayed if you selected the **Selected Subresource** button in **Display Form**.

Collection Data List

This box displays the collected data for each collection period. It also totals the data within the display period and displays the maximum value, minimum value, and average.

Save File

This button displays the Save File window. If you opened this window from the SSO console, this button is not displayed.

Resource values to be displayed:

Fractional resource values are rounded to two decimal places.

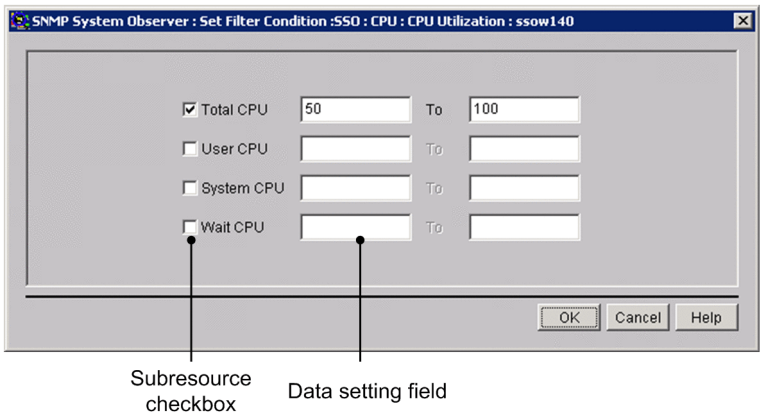
The maximum value and minimum value to be displayed:

If the maximum value or minimum value is an integer, the decimal places `.00` are added.

4.5.3 Set Filter Condition window

The Set Filter Condition window filters the collected data to be displayed in the Listing Display window or the data to be copied in the Copy Collection Data window. The following figure shows the Set Filter Condition window.

Figure 4-50: Set Filter Condition window



The items to be set are:

Subresource checkbox

Select the checkbox of the subresource to be filtered. SSO does not output data for the subresources that are not selected.

Data setting field

Specify the range of values to be filtered. You can specify 0 or any floating decimal point between $\pm 1.00 \times 10^{-2}$ and $\pm 1.7976931348623157 \times 10^{308}$. In the right field, specify a value that is equal to or greater than the value specified in the left field.

4.5.4 Save File window

The Save File window saves the collected data to a file. The following figure shows the Save File window.

Figure 4-51: Save File window (opened from the Listing Display window)

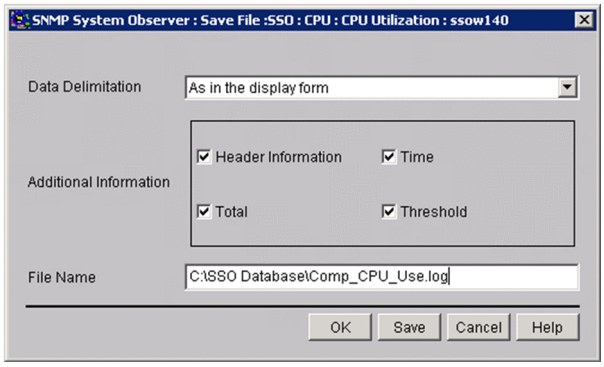
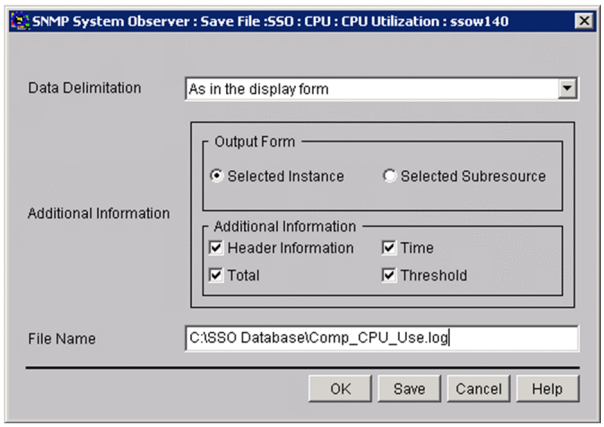


Figure 4-52: Save File window (opened from the Collection Data Detail window)



The items to be set are:

Data Delimitation

Specify a character for delimiting data.

As in the display form

SSO uses spaces to set out the lines and outputs the data to a file as displayed in the Listing Display window.

Delimit by comma, **Delimit by tab**, **Delimit by space**

SSO delimits the data in accordance with the specified format.

Additional Information

Specify the information to be output to the save file.

Output Form

Specifies the output format of collection data.

- **Selected Instance**
  Outputs collection data for each instance.
- **Selected Subresource**
  Outputs collection data for each subresource.

Header Information

SSO outputs (to the file) the resource name or other title of the data.

Time

SSO outputs (to the file) the date and time at which the information was obtained.

Total

SSO outputs (to the file) the total of the minimum value, maximum value, and average.

Threshold

SSO outputs the threshold to the file. However, it cannot output the threshold if you specified Daily Data or Monthly Data for **Display Form:** in the Collection Data Detail window.

File Name

Specify a file name by its absolute path. If you omit the path on Windows, SSO creates the file in the SSO installation directory. If you omit the path on UNIX, SSO creates the file in the root directory.

Save

Clicking this button saves the data to the specified file.

Resource values to be output:

Fractional resource values are rounded to two decimal places.

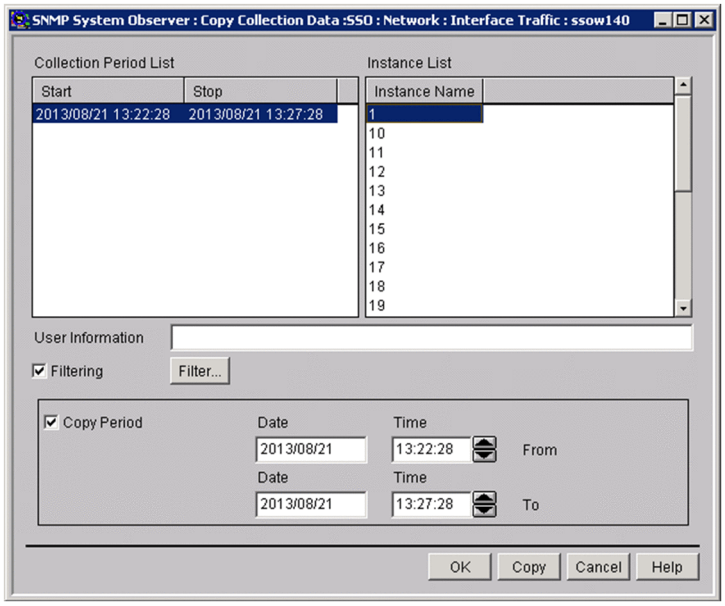
The maximum value and minimum value to be output:

If the maximum value or minimum value is an integer, the decimal places `.00` are added.

4.5.5 Copy Collection Data window

The Copy Collection Data window copies the collection database. The following figure shows the Copy Collection Data window.

Figure 4-53: Copy Collection Data window



The items to be set are:

Collection Period List

This box displays the collection period of the collected data. If only the collection start date and time are displayed, it means that the data is currently being collected. You can select multiple lines as long as they are adjacent.

Instance List

This box displays the instances for which resources were collected.

User Information

Specify information to be displayed in the **Additional Information** field of the Resource Data Reference window. Specify the information with a character string of 255 bytes or less. You can enter Japanese characters (multi-byte code), but the character code will be the language code in effect based on the language environment variable of SSO. As a result, if you execute the `ssoextractlog` command under a different Japanese environment, characters are garbled.

Filtering

Select this checkbox when you want to filter collected data. You can specify a range of values for each subresource and filter just those values.

Filter

This button displays the Set Filter Condition window.

Copy Period

Select this checkbox when you want to specify the collection period of the data to be copied. When this checkbox is selected, you can specify a period for copying the collected data.

Date

Specify a range between January 1, 1980 and December 31, 2029 in the format *yyyy/mm/dd*. You can specify a range if you selected the **Copy Period** checkbox.

Time

Specify a range between 00:00:00 and 23:59:59 in the format `00:00:00`. You can specify a range if you selected the **Copy Period** checkbox.

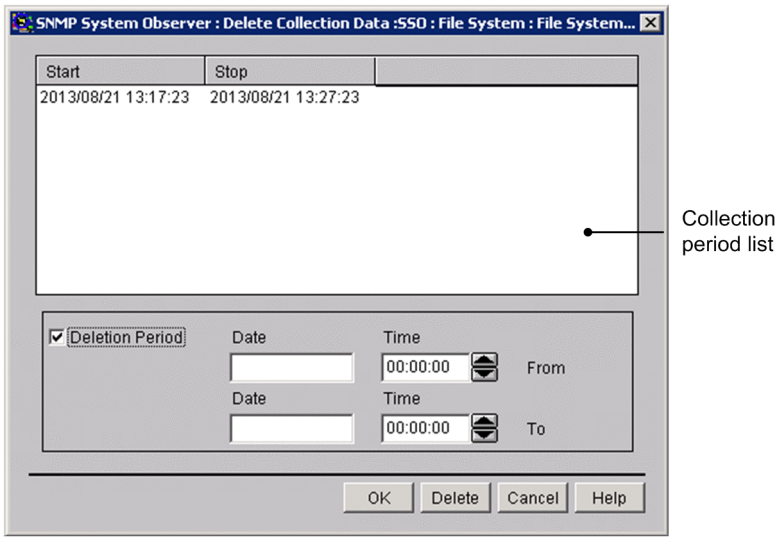
Copy

This button copies the specified collected data.

4.5.6 Delete Collection Data window

The Delete Collection Data window specifies data in the collection database and deletes it. The following figure shows the Delete Collection Data window.

Figure 4-54: Delete Collection Data window



The items to be set are:

Collection period list

This box displays the collection period of the collected data. If only the collection start date and time are displayed, it means that the data is currently being collected. You can select multiple lines as long as they are adjacent.

Deletion Period

Select this checkbox when you want to specify the collection period of the data to be deleted. When this checkbox is selected, you can specify a period for deleting the collected data.

Date

Specify a range between January 1, 1980 and December 31, 2029 in the format *yyyy/mm/dd*. You can specify a range if you selected the **Deletion Period** checkbox.

Time

Specify a range between 00:00:00 and 23:59:59 in the format `00:00:00`. You can specify a range if you selected the **Deletion Period** checkbox.

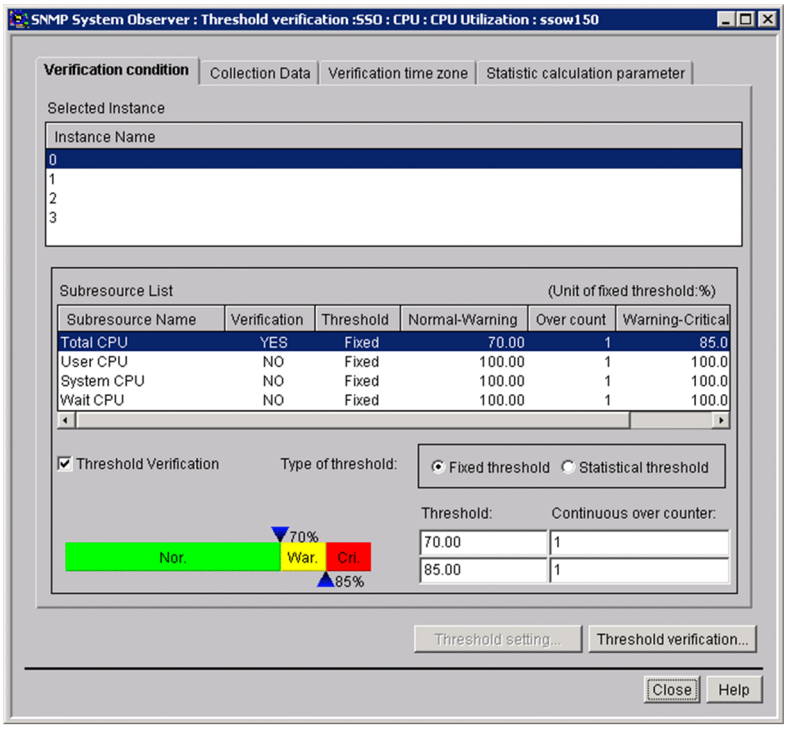
Delete

This button deletes the specified collected data.

4.5.7 Threshold verification window

The Threshold verification window sets information necessary to verify threshold values from the collected data. The following figure shows the Threshold verification window.

Figure 4-55: Threshold verification window



The items to be set are:

Verification condition tab

Select this tab to set conditions for verifying threshold verification methods. For descriptions about display items when the **Verification condition** tab is selected, see *4.5.7(1) Verification condition tab*.

Collection Data tab

Select this tab to set conditions of data for threshold verification. For descriptions about display items when the **Collection Data** tab is selected, see *4.5.7(2) Collection Data tab*.

Verification time zone tab

Select this tab to set the time zone for threshold verification. For descriptions about display items when the **Verification time zone** tab is selected, see *4.5.7(3) Verification time zone tab*.

Statistic calculation parameter tab

Select this tab to set the time at which a statistical threshold is to be calculated. For descriptions about items displayed when the **Statistic calculation parameter** tab is selected, see *4.5.7(4) Statistic calculation parameter tab*.

Threshold verification

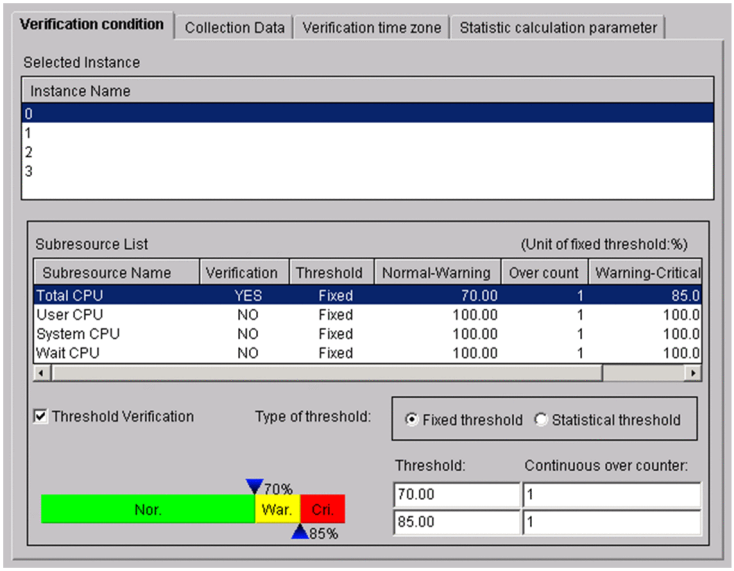
This button displays the Threshold verification result window.

You can click this button when you specify the instance name and the subresource to be verified.

For details on the Threshold verification result window, see *4.3.15 Threshold verification result window*.

(1) Verification condition tab

Figure 4-56: Threshold verification window (Verification condition tab)



The items to be set are:

Selected Instance

Displays the name of the instance for the collected data.

Select the name of the instance of which the threshold you want to verify.

Subresource List

This list is displayed when you select an instance name in **Selected instance**.

Select the subresource name of which the threshold you want to verify.

Threshold verification

Select this check box to specify the threshold type and verification conditions.

By selecting the subresource name in **Subresource List**, and then this check box, you can specify the threshold type, threshold value, data ratio, and the consecutive number of times that a threshold is exceeded. In addition, when you select this check box, the **Verification** column in **Subresource List** changes from `NO` to `YES`.

By default, this check box is not selected.

Type of threshold

Select the type of threshold verification. The default is **Fixed threshold**.

Fixed threshold

Verifies thresholds by using the fixed threshold method.

When you select this method, the **Threshold** and **Continuous over counter** columns are displayed.

For the **Threshold** columns, specify the warning threshold and the critical threshold.

You can specify 0 or any floating decimal point between $\pm 1.00 \times 10^{-2}$ and $\pm 1.7976931348623157 \times 10^{308}$. If the value in the mantissa exceeds 1.7976931348623157, it is rounded.

For the **Continuous over counter** columns, set the number of times that collected data must consecutively exceed the threshold before SSO changes the resource status. You can specify a value from 1 to 99.

If you set the same value for the warning threshold and the critical threshold, the warning region is eliminated. Therefore, in such a case, you can specify only one value.

Statistical threshold

Verifies the threshold by using the statistical threshold.

When you select this method, the **Ratio of data** and **Continuous over counter** columns are displayed.

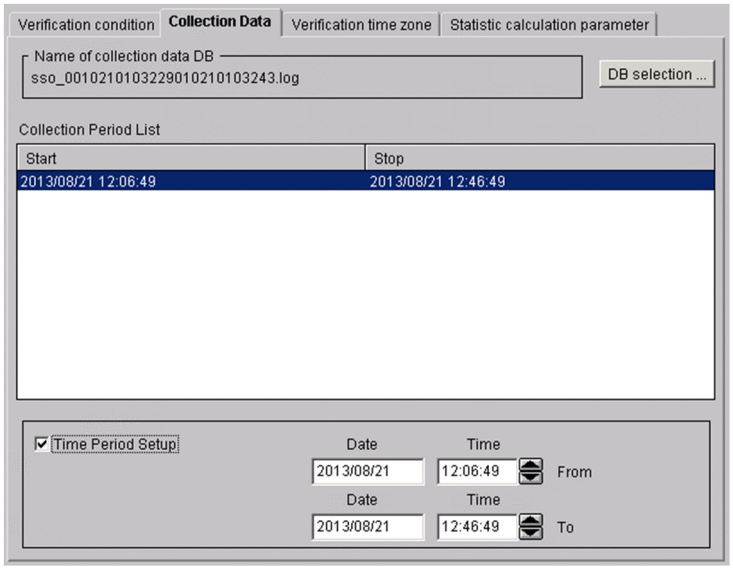
For **Ratio of data**, specify the data ratio in the warning region and the critical region of the threshold. You can specify a value from 0.01 to 99.99.

For **Continuous over counter**, set the number of times that collected data must consecutively exceed the threshold before SSO changes the resource status. You can specify a value from 1 to 99.

If you set the same value for the warning threshold and the critical threshold, the warning region is eliminated. Therefore, in such a case, you can specify only one value.

(2) Collection Data tab

Figure 4-57: Threshold verification window (Collection Data tab)



The items to be set are:

Name of collection data DB

Displays the name of the database in which data that has the thresholds to be verified is collected.

DB selection

This button displays the DB selection window. For details on the DB selection window, see *4.3.12 DB selection window*.

Collection Period List

This box displays the collection period of the data in the selected database. If only the collection start date is displayed, it means that the data is currently being collected. You can select multiple lines as long as they are adjacent.

Time Period Setup

Select this check box to narrow down the collection period of the data to be verified.

When you select this check box, you can specify a specific period based on the range within the collection period.

Date

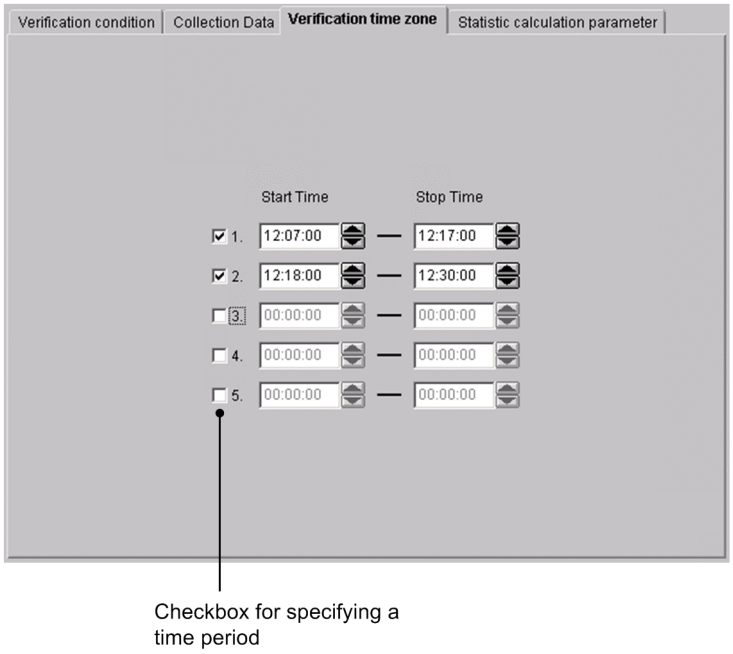
Specify a range between January 1, 1980 and December 31, 2029 in the *yyyy/mm/dd* format. You can specify a range if you selected **Time Period Setup**.

Time

Specify a range between 00:00:00 and 23:59:59 in the `00:00:00` format. You can specify the range if you selected **Time Period Setup**.

(3) Verification time zone tab

Figure 4-58: Threshold verification window (Verification time zone tab)



The items to be set are:

Check box for specifying a time period

Specify whether to activate the specified verification period. Only the time zone for the selected line is activated. By default, no time zone is specified.

Start Time

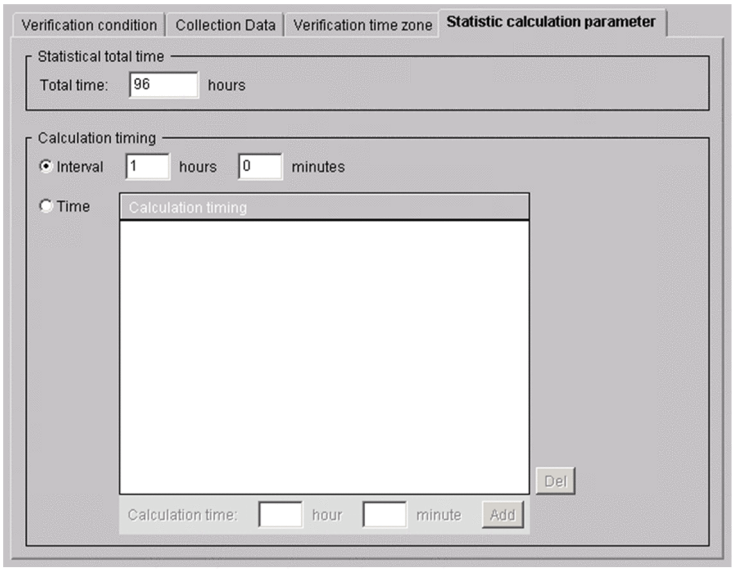
Specify the time to start verification in the range from 00:00:00 to 23:59:59.

Stop Time

Specify the time to stop verification in the range from 00:00:00 to 23:59:59. Specify a time after the start time.

(4) Statistic calculation parameter tab

Figure 4-59: Threshold verification window (Statistic calculation parameter tab)



The items to be set are:

Statistical total time

Specify 24 to 720 hours as the period for extracting data that is needed for calculating a statistical threshold. The default is 96 hours.

Calculation timing

Interval

Select this radio button to specify the interval for calculating a threshold. The specifiable range is 15 minutes to 24 hours. By default, an interval of 1 hour is set.

Time

Select this radio button to specify the time at which a threshold is to be calculated. By default, the time is not set.

Del

Deletes the time selected from the calculation timing list.

Calculation time

You can specify the calculation period between 00:00 and 23:59.

Add

Adds the time you specified to the calculation timing list.

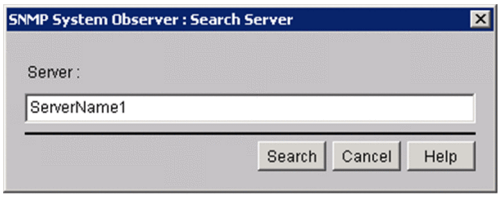
(5) Note

When verifying a threshold value by using the GUI, a work space which is as large as the collection database you specified as the verification target is required under `$SSO_VAR`.

4.5.8 Search Server window

The Search Server window searches collection data for each server name. The following figure shows the Search Server window.

Figure 4-60: Search Server window



The items to be set are:

Server

Specify the host name or the IP address for the name of the server you want to search based on the collection data. You can specify a maximum of 255 bytes.

Search

Start a search with the condition specified for **Server**.

Searches collection data from the top of the collection data list, and moves the items that are perfect matches to the collection data of the applicable server. If no server name matches perfectly, the selected item is moved to the collection data of the server that has the name which was found first through a forward match.

If no applicable server name exists, a warning dialog box appears.

When you specify an IP address in the **Server** text box, a matching string is searched through the IP address section in the list of collection data.

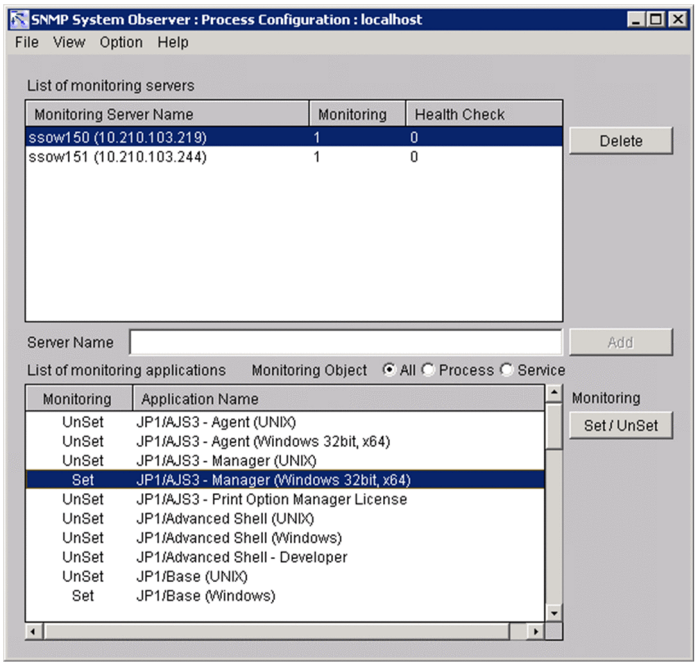
Important note

If the OS that opened the window is UNIX, the host names are case sensitive. Be careful when you enter the server name as a collection data.

4.6 Process Configuration window

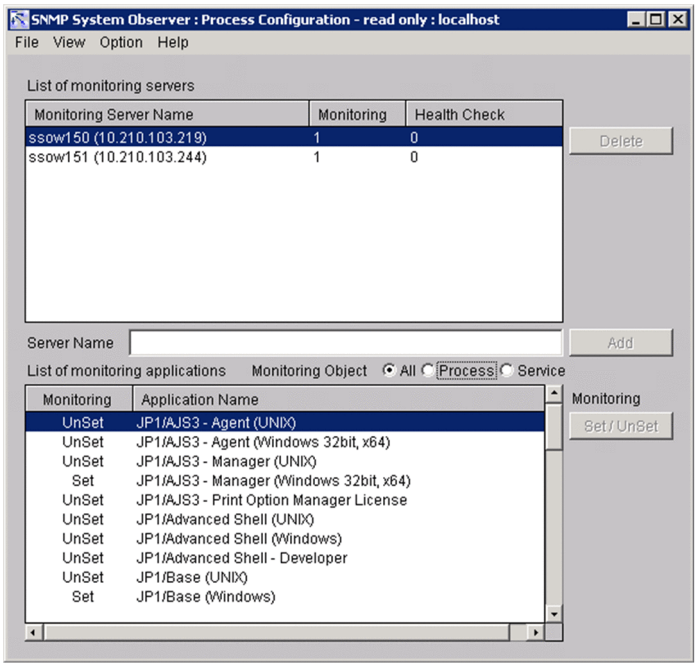
The Process Configuration window sets the process monitoring conditions. The following figure shows the Process Configuration window.

Figure 4-61: Process Configuration window



If the Process Configuration window is already running, or the `ssopsset` command that sets monitoring conditions is being executed, you can start the Process Configuration window in reference mode. The following figure shows the Process Configuration window(reference mode).

Figure 4-62: Process Configuration window(reference mode)



The items to be set are:

List of monitoring servers

This box displays the servers registered as monitoring servers and the monitoring conditions set for each server.

Item	Description
Monitoring Server Name	Displays the host name and IP address of the monitoring server for process monitoring. In addition, if the host name cannot be resolved, only the IP address is displayed.
Monitoring	Displays the monitoring interval (in minutes) for process monitoring, which is set in the Set Monitor Interval window. If the process monitoring interval setting cannot be applied to a monitoring server, a hyphen (−) is displayed.#
Health Check	Displays the health check interval (in minutes) which is performed regularly from the monitoring server, which is set in the Set Health Check Interval window.

#

When a hyphen (−) is displayed, communication names between a monitoring server and a monitoring manager might not match, communication between them might not be established, or data might be lost due to a communication overload.

Delete

This button deletes the selected server from **List of monitoring servers**.

Server Name

Specify a host name or IP address to be added to **List of monitoring servers** by specifying a character string of 256 bytes or less.

Add

This button adds the server specified in **Server Name** to **List of monitoring servers**.

List of monitoring applications

This box displays the applications registered in the server selected in **List of monitoring servers** and the monitoring conditions set for each application.

Item	Description
Monitoring	Displays the setting status of monitoring mode for the application. When the application is being monitored, `Set` is displayed. When the application is not being monitored, `UnSet` is displayed.
Application Name	Displays the registered applications.

Monitoring Object

Limits the applications to be displayed in **List of monitoring applications**.

- **All**
  Displays applications that monitor both processes and services.
- **Process**
  Displays applications that monitor processes only.
- **Service**
  Displays applications that monitor services only.

Monitoring - Set / Unset

Set whether to monitor the selected application.

The next table explains the menu items.

Menu bar	Menu command	Description
File	Change Connection#	Changes the connection destination.
	Save	Saves the settings and starts monitoring.

Menu bar	Menu command		Description
View	Update Condition		Obtains a monitoring condition again. You can use this command when you opened the window in reference mode.
	Search Monitoring Server		Displays the Search Monitoring Server window. This menu command can be selected only when **List of monitoring servers** contains at least one server.
Option	Monitoring Server	Setting the monitoring interval	Displays the Set Monitor Interval window.
		Setting the health check interval	Displays the Set Health Check Interval window.
	Monitoring Application	Automatic Action	Displays the Automatic Action window.
		Remote Command	Displays the Remote Command window.
	Application Registration		Displays the Register Application window.

#

The menu command is not displayed if you opened the window from the SSO console.

4.6.1 Register Application window

The Register Application window registers applications to be monitored dynamically. The following figures show the Register Application window when the monitoring object is **Process**, and the Register Application window when the monitoring object is **Service**.

Figure 4-63: Register Application window (when Process is selected as Monitoring Object)

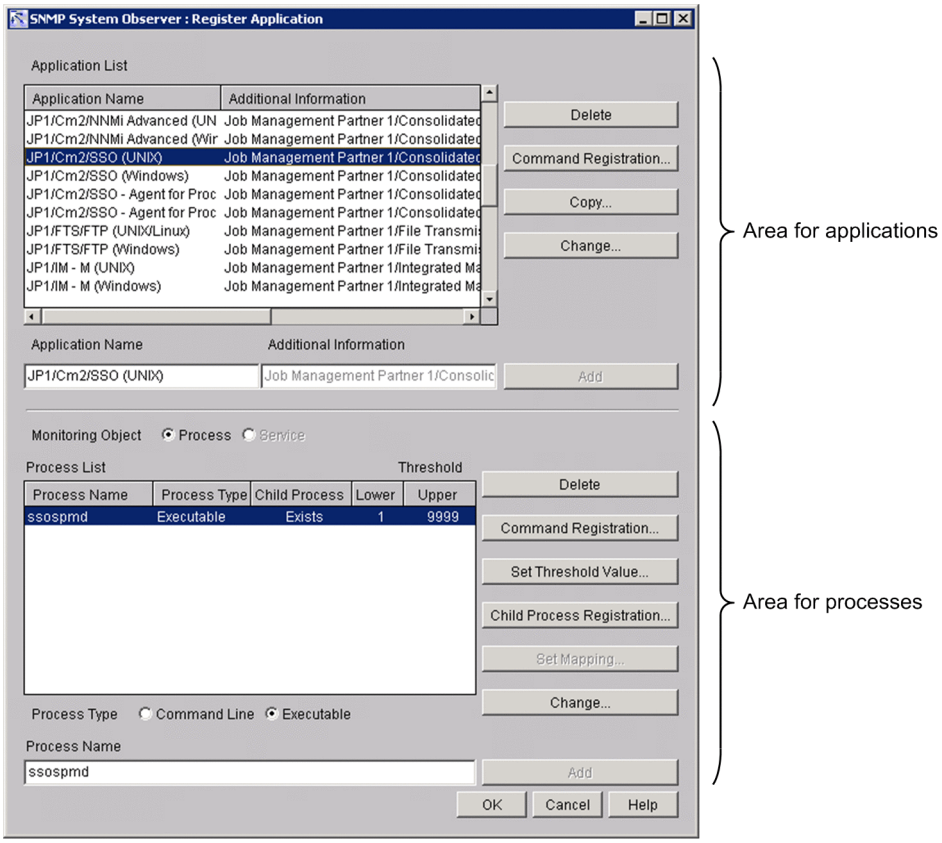
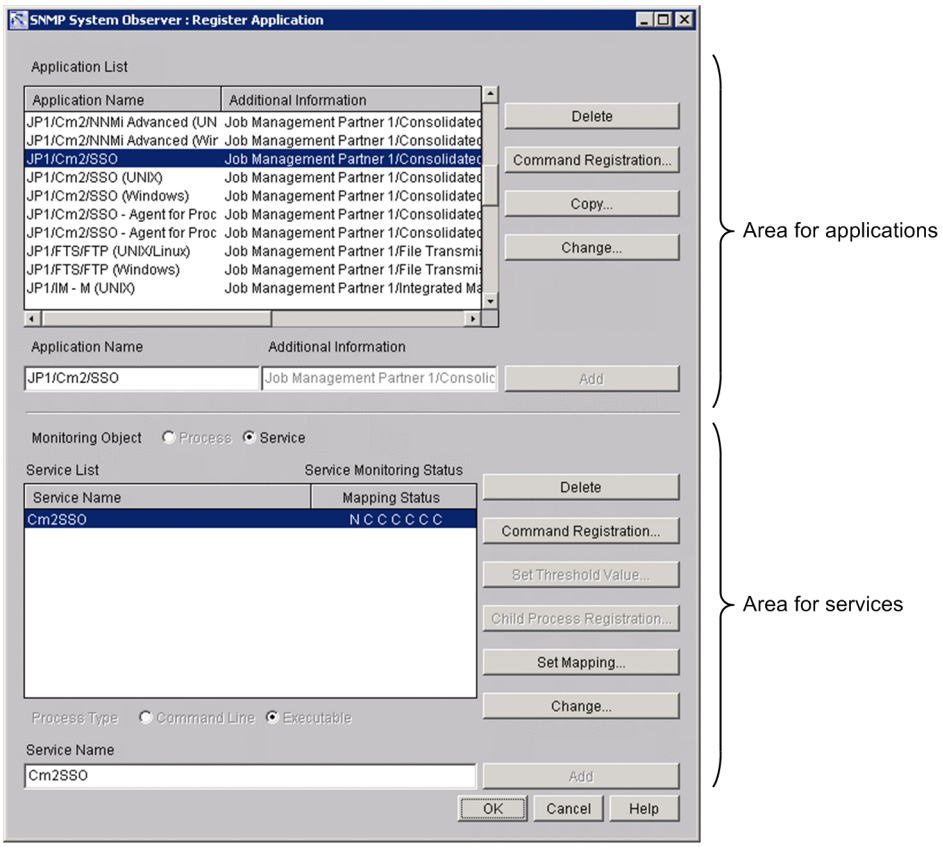


Figure 4-64: Register Application window (when Service is selected as Monitoring Object)



The items to be set are:

Area for applications

Application List

This box displays the applications to be monitored by the monitoring server selected in the Process Configuration window.

Delete

This button deletes the selected application from **Application List**.

Command Registration

This button displays the Register Command window. In the Register Command window, register the command to be executed when the status of an application changes.

Copy

This button displays the Copy Application window. Copies the application you selected in **Application List**. For details on the Copy Application window, see *4.6.6 Copy Application window*.

Change

This button displays the Change Application window. For details on the Change Application window, see *4.6.7 Change Application window*.

This button is enabled when an application is selected in **Application List**. This button is always disabled in reference mode.

Application Name

Specify an application to be added to **Application List**. Specify the application with a character string of 128 bytes or less. Do not specify a semicolon (;), tab, or multibyte code. In addition, do not specify the hash character (#) at the beginning of the application name.

Additional Information

Specify additional information about the application specified in Application Name. Specify the information with a character string of 128 bytes or less. Do not specify a semicolon (;), tab, or multibyte code.

Add

This button adds the application specified in **Application Name** to **Application List**.

Area for processes or Services

Monitoring Object

Specifies the monitoring target.

- **Process**

  Select this radio button to monitor processes. If you add process information to this application, you cannot register additional services.

- **Service**

  Select this radio button to monitor services. If you add service information to this application, you cannot register additional processes.

Process List

When processes are monitored, a list of processes to be monitored by the application selected in **Application List** is displayed. In the list, process names, process types, registered child process names, and the highest and lowest threshold values are displayed. You can select multiple process names.

Service List

When services are monitored, a list of services to be monitored by the application selected in **Application List** is displayed. In the list, service names and the mapping statuses are displayed. You can select multiple service names.

Delete

This button deletes the selected process from **Process List** or **Service List**. You can delete multiple application programs.

Command Registration

This button displays the Register Command window. In the Register Command window, register the command to be executed when the status of a process changes. For details on the Register Command window, see *4.6.4 Register Command window*. You can click this button when you selected processes from **Process List**, or selected services from **Service List**.

Set Threshold Value

This button displays the Set Threshold Value window. For details on the Set Threshold Value window, see *4.6.3 Set Threshold Value window*. You can click this button when you selected processes from **Process List**.

Child Process Registration

This button displays the Register Child Process window. For details on the Register Child Process window, see *4.6.2 Register Child Process window*. You can click this button when you selected processes from **Process List**.

Set Mapping

This button displays the Set Mapping window. For details on the Set Mapping window, see *4.6.5 Set Mapping window*. You can click this button when you selected services from **Service List**.

Change

If this button is clicked when a process is selected in **Process List**, the Change Process window opens. If this button is clicked when a service is selected in **Service List**, the Change Service window opens.

For details on the Change Process window, see *4.6.8 Change Process window*. For details on the Change Service window, see *4.6.9 Change Service window*.

This button is enabled only when a process or service is selected in **Process List** or **Service List**. This button is always disabled in reference mode.

Process Name

Specify a process name to be added to **Process List**. You can use an asterisk (*) or a question mark (?) as wild card characters. Do not specify a semicolon (;) or a tab. In addition, do not specify a linefeed code (0x0A and 0x0D0A). When you copy and paste data created by using a spreadsheet program, if a linefeed code is specified, the monitoring condition is deleted.

When the monitoring server is Windows, specify a process without including the extension (.exe).

Service Name

Specify a service name to be added to **Service List** by a string within 100 bytes. If an asterisk (*) or a question mark (?) is used in the service name, it is treated as a regular character, and service monitoring as a wildcard character is not performed. Do not specify a semicolon (;), a tab, a forward slash (/), or a back slash (\). In addition, do not specify linefeed characters (0x0A and 0x0D0A). When you copy and paste data created by using a spreadsheet program, if a linefeed character is specified, the monitoring condition is deleted.

Command line, **Executable**

Specify the type of the process specified in **Process Name**.

If the OS is Windows, select **Executable**. If the OS is UNIX, select **Executable** or **Command line**. For details on how to check whether a process is the Command line or Executable type, see *2.5 Process and service monitoring function*.

Add

Adds the process specified in the **Process Name** text box to **Process List**, or the service specified in the **Service Name** text box to **Service List**.

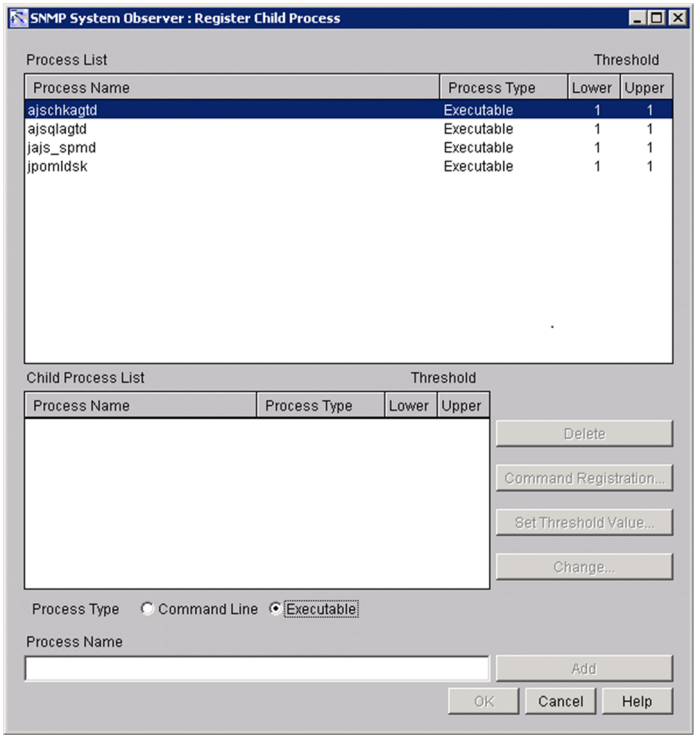
Important note

If a monitored application is deleted or renamed, monitoring of that application stops.

4.6.2 Register Child Process window

The Register Child Process window registers a child process. The following figure shows the Register Child Process window.

Figure 4-65: Register Child Process window



The items to be set are:

Process List

This box displays the process selected in the Register Application window.

Child Process List

This box displays the child processes to be monitored by the process displayed in **Process List**. It also displays the process type and thresholds of each child process.

Delete

This button deletes the selected child process from **Child Process List**.

Command Registration (for child processes)

This button displays the Register Command window. In the Register Command window, register the command to be executed when the status of a child process changes.

Set Threshold Value

This button displays the Set Threshold Value window.

Change

This button displays the Change Process window. For details on the Change Process window, see *4.6.8 Change Process window*.

This button is enabled only when a child process is selected in **Child Process List**. This button is always disabled in reference mode.

Process Name

Specify a child process name to be added to **Child Process List**. Specify the child process name with a character string of 60 bytes or less. You can use an asterisk (*) or question mark (?) as a wild card at the child process name. Do not specify a semicolon (;) or a tab. In addition, do not specify `.exe`.

Command Line, **Executable**

Specify the type of the process specified in **Process Name**.

If the OS is Windows, select **Executable**. If the OS is UNIX, select **Executable** or **Command line**. For details on how to check whether a process is the Command line or Executable type, see *2.5 Process and service monitoring function*.

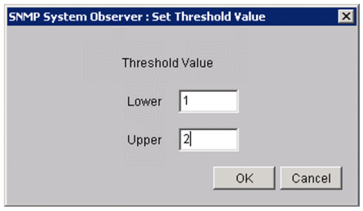
Add

This button adds the child process specified in **Process Name** to **Child Process List**.

4.6.3 Set Threshold Value window

The Set Threshold Value window sets thresholds for a process or child process. A threshold indicates the number of processes or child processes that can be executed at one time. The following figure shows the Set Threshold Value window.

Figure 4-66: Set Threshold Value window



The items to be set are:

Threshold Value

Lower

Specify the lower limit for the number of processes that can be executed at one time. Specify a value that is equal to or smaller than the upper limit. The default is 1.

Upper

Specify the upper limit for the number of processes that can be executed at one time. Specify a value that is equal to or greater than the lower limit. If you do not wish to set an upper limit, specify 9999. The default is 1.

The following are examples for setting threshold values:

Example 1: When 3 is specified as the upper limit of the threshold, and 1 as the lower limit:

Normal if the number of running processes is from 1 to 3

Critical if the number of running processes is 0 or 4 or greater

Example 2: When 0 is specified as the upper limit of the threshold, and 0 as the lower limit:

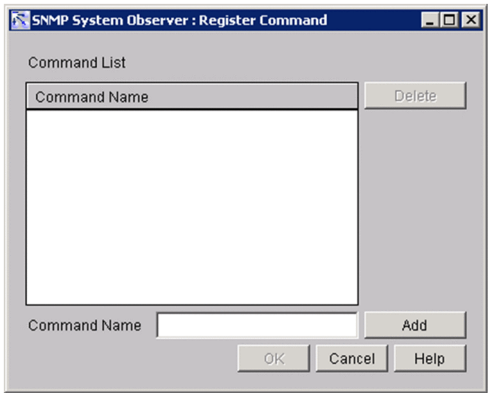
Normal if the number of running processes is 0

Critical if the number of running processes is 1 or greater

4.6.4 Register Command window

The Register Command window registers remote commands to be executed at any timing for an application, process, child process, or service. The remote commands registered in this window are displayed in the Remote Command window or the Command Setup window. The following figure shows the Register Command window.

Figure 4-67: Register Command window



The items to be set are:

Command List

This box displays the registered commands.

Delete

This button deletes the selected command from **Command List**.

Command Name

Specify a command name to be added to **Command List** with a character string of 160 bytes or less. Do not specify a tab.

Add

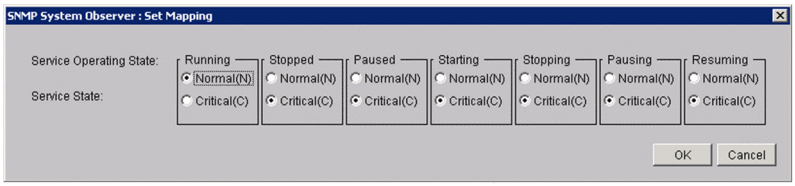
This button adds the process specified in **Command Name** to **Command List**.

4.6.5 Set Mapping window

The Set Mapping window maps the service status and the service's operating status. Based on this setting, SSO determines the status of the monitoring service.

The following figure shows the Set Mapping window.

Figure 4-68: Set Mapping window



The items to be set are:

Service Operating State

Displays the service status that can be obtained through service monitoring.

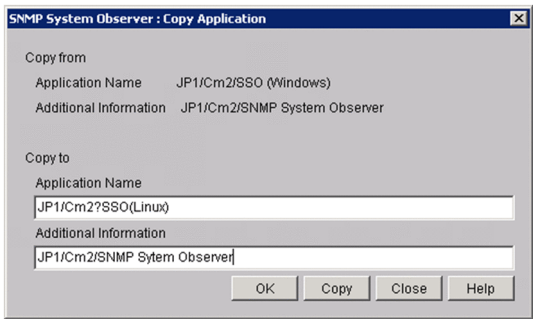
Service State

For each service operating status, set the status (either **Normal** or **Critical**) to be used to monitor services. By default, only the **Running** status is set to **Normal**, and other statuses are set to **Critical**.

4.6.6 Copy Application window

The Copy Application window copies the application you selected in **Application List** of the Register Application window. The following figure shows the Copy Application window.

Figure 4-69: Copy Application window



The items to be set are:

Copy from

Application Name

Displays the application name selected from **Application List**.

Additional Information

Displays the additional information selected from **Application List**.

Copy to

Application Name

Specifies the copy destination application name.

Specify a character string of up to 128 bytes. Do not specify a semicolon (`;`), a comma (`,`), a tab, or multi-byte codes. In addition, you cannot specify a hash mark (`#`) at the beginning of the application name. You cannot specify a registered application name.

Additional Information

Specifies additional information on the copy destination application.

Specify a character string of up to 128 bytes. Do not specify a semicolon (`;`), a tab, or multi-byte codes.

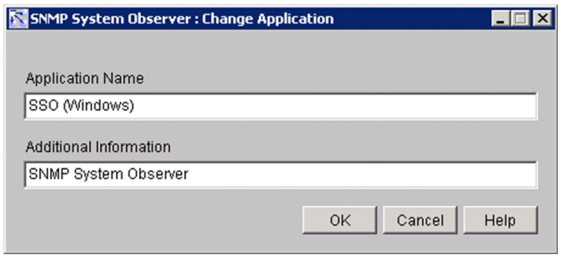
Copy

Copies the specified application.

4.6.7 Change Application window

The Change Application window can be used to change the name and additional information of the application selected in **Application List** in the Register Application window. The following figure shows the Change Application window.

Figure 4-70: Change Application window



The items to be set are:

Application Name

You can specify the application name with a character string of 128 bytes or less. Do not specify a semicolon (`;`), a comma (`,`), a tab, or multi-byte codes. In addition, you cannot specify a hash mark (`#`) at the beginning of the application name.

Additional Information

You can specify the additional information of application with a character string of 128 bytes or less. Do not specify a semicolon (`;`), a tab, or multi-byte codes.

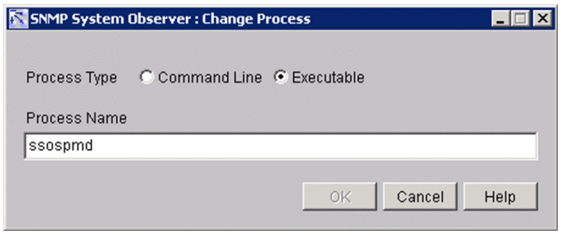
Important note

If a monitored application is renamed, monitoring of that application stops.

4.6.8 Change Process window

The Change Process window is used to change the process type of a process and child processes. The window is also used to rename processes and child processes. The following figure shows the Change Process window.

Figure 4-71: Change Process window



The items to be set are:

Command Line, **Executable**

Specify the type of the process specified in **Process Name**.

Process Name

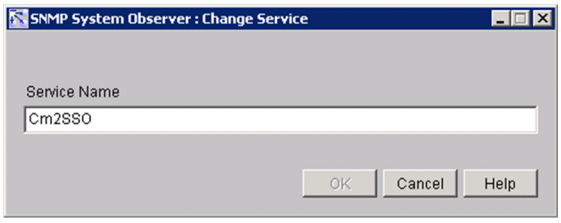
You can specify the process name with a character string of 60 bytes or less. The process name you specify can include asterisks (`*`) and question marks (`?`) as wildcard characters. Do not include semicolons (`;`) or tabs.

If the OS of the monitoring server is Windows, specify a process name without the file name extension `.exe`.

4.6.9 Change Service window

The Change Service window is used to change the name of a service. The following figure shows the Change Service window.

Figure 4-72: Change Service window



The items to be set are:

Service Name

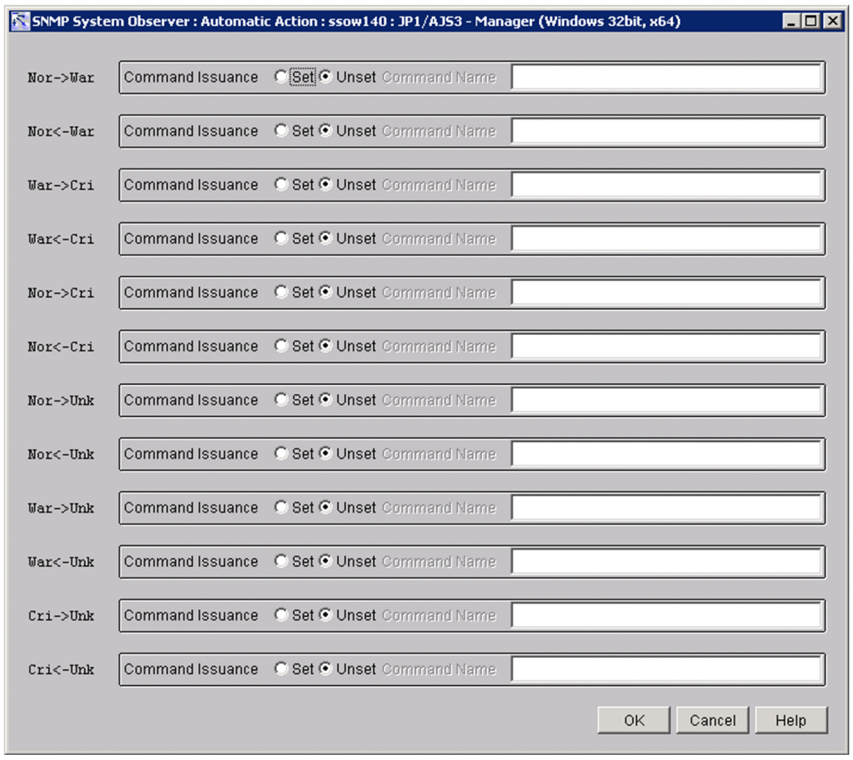
Specify the new service name with a string of no more than 100 bytes. Asterisks (*) and question marks (?) included in the service name are treated as ordinary characters. That is, you cannot use wildcard characters to specify monitoring-target services.

Do not specify a semicolon (;), a tab, a slant (/), or a backslash (\).

4.6.10 Automatic Action window

The Automatic Action window specifies the command to be executed by automated action on the SSO when the status of monitoring application changes. The following figure shows the Automatic Action window.

Figure 4-73: Automatic Action window



The items to be set are:

Command Issuance

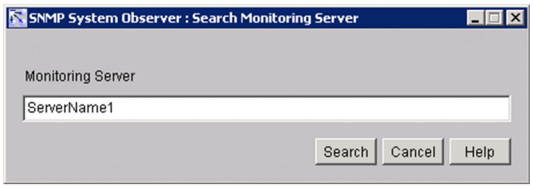
Select whether to execute a command for each change in the application status. If you select **Set**, specify the command to be executed in the **Command Name** box. Specify the command in 160 bytes or less.

For details on automated actions and remote commands, see *2.5.2(4) Automated actions and remote commands*.

4.6.11 Search Monitoring Server window

The Search Monitoring Server window is used to search for a monitoring server. The following figure shows the Search Monitoring Server window.

Figure 4-74: Search Monitoring Server window



The items to be set are:

Monitoring Server

Specify the host name or IP address of the monitoring server that you want to search for. You can specify a maximum of 255 bytes.

Search

Start a search with the condition specified for **Monitoring Server**.

Searches server names from the top of the **List of monitoring servers**, and moves the items that are perfect matches to the monitoring server. If no monitoring server name matches perfectly, the selected item is moved to the server that has the name which was found first through a forward match.

If no applicable monitoring server name exists, a warning dialog box appears.

When you specify an IP address in the **Monitoring Server** text box, a matching string is searched through the IP address section in the **List of monitoring servers**.

Important note

If the OS that opened the window is UNIX, the host names are case sensitive. Be careful when you enter the monitoring server name.

4.6.12 Remote Command window

The Remote Command window specifies the remote command that SSO will instruct APM to execute by automated action when the status of a monitored application changes. Commands whose execution is prohibited in the executable command definition file cannot be carried out. Figure 4-75 shows the Remote Command window which is used to select an application for process monitoring, and Figure 4-76 shows the Remote Command window which is used to select an application for service monitoring.

Figure 4-75: Remote Command window (monitoring process)

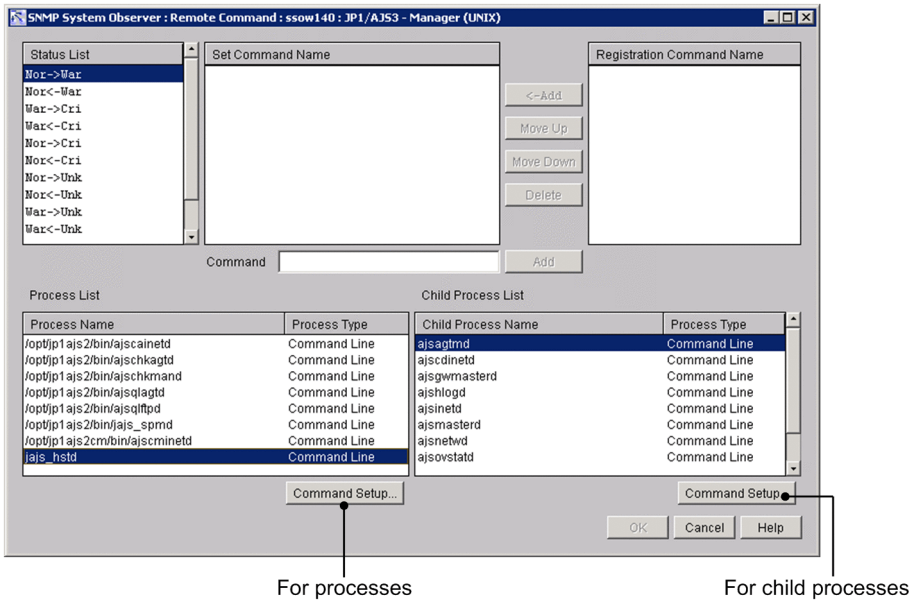
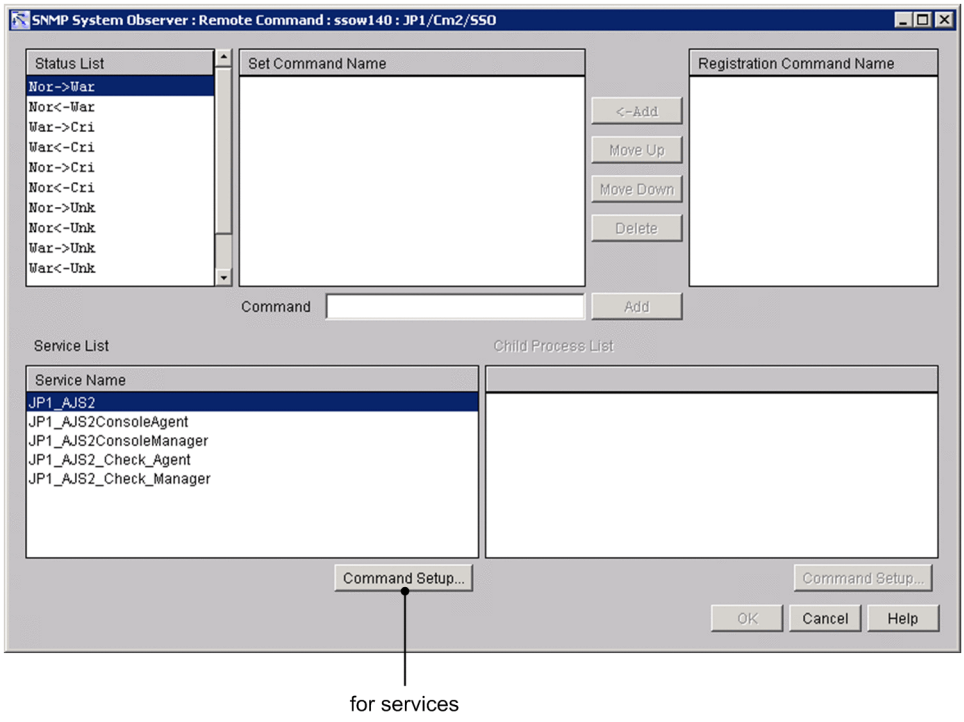


Figure 4-76: Remote Command window (monitoring service)



The items to be set are:

Status List

This box displays changes in the status of the application. You can set a command for each status change.

Set Command Name

This box displays the command to be executed when the status selected in **Status List** changes. If multiple commands have been set, SSO executes them in order from the top.

<-Add

This button adds the command selected in **Registration Command Name** to **Set Command Name**.

Move Up

This button reverses the order of the command selected in **Set Command Name** and the command immediately above it.

Move Down

This button reverses the order of the command selected in **Set Command Name** and the command immediately below it.

Delete

This button deletes the command selected in **Set Command Name**.

Command

Specify a command by specifying the command name with a character string of 160 bytes or less. Do not specify a tab.

Add

Adds a command specified in **Registration Command Name** to **Set Command Name**.

Registration Command Name

Commands registered in the Command window are displayed in the order they were registered.

Process List

This box displays the processes registered for the application selected in **List of monitoring applications** of the Process Configuration window.

Service List

This box displays the Services registered for the application selected in List of monitoring applications of the Process Configuration window.

Command Setup (for processes / services)

This button displays the Set Command window. In the Set Command window, set the command to be executed when the status of a process, and service changes. For details on the Set Command window, see *4.6.13 Set Command window*.

For details on the automated actions and remote commands, see *2.5.2(4) Automated actions and remote commands*.

Child Process List

This box displays the child processes registered for the process selected in **Process List**.

Command Setup (for child processes)

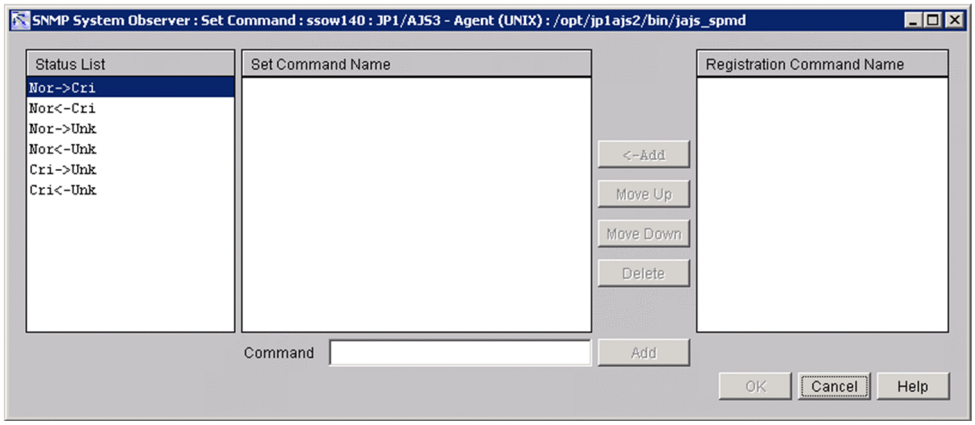
This button displays the Set Command window. In the Set Command window, set the command to be executed when the status of a child process changes. For details on the Set Command window, see *4.6.13 Set Command window*.

For details on the automated actions and remote commands, see *2.5.2(4) Automated actions and remote commands*.

4.6.13 Set Command window

The Set Command window specifies the remote command that SSO will instruct APM to execute by automated action when the statuses of a monitored process, monitored child process, or monitored service change. Commands whose execution is prohibited in the executable command definition file cannot be carried out. The following figure shows the Set Command window.

Figure 4-77: Set Command window



The items to be set are:

Status List

This box displays changes in the status of the monitored processes, child processes, and services. You can set a command for each status change.

Set Command Name

This box displays the command to be executed when the status selected in **Status List** changes. If multiple commands have been set, SSO executes them in order from the top.

<-Add

This button adds the command selected in **Registration Command Name** to **Set Command Name**.

Move Up

This button reverses the order of the command selected in **Set Command Name** and the command immediately above it.

Move Down

This button reverses the order of the command selected in **Set Command Name** and the command immediately below it.

Delete

This button deletes the command selected in **Set Command Name**.

Command

Directly enter the name of a command to be executed when the status of a process or a service changes. You can specify the command name with a character string of 160 bytes or less. Do not specify a tab. For details on the automated actions and remote commands, see *2.5.2(4) Automated actions and remote commands*.

Add

Adds a command specified in **Registration Command Name** to **Set Command Name**.

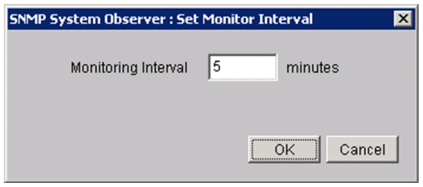
Registration Command Name

Commands registered in the Command window are displayed in the order they were registered.

4.6.14 Set Monitor Interval window

The Set Monitor Interval window sets the interval at which the monitoring server is to monitor processes. The following figure shows the Set Monitor Interval window.

Figure 4-78: Set Monitor Interval window



The items to be set are:

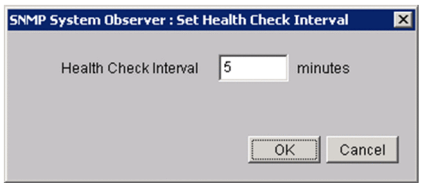
Monitoring Interval

Specify a monitoring interval between 1 and 60 minutes. The default is 1 minute.

4.6.15 Set Health Check Interval window

The Set Health Check Interval window sets an interval for the monitoring server when SSO is to regularly perform a health check. The following figure shows the Set Health Check Interval window.

Figure 4-79: Set Health Check Interval window



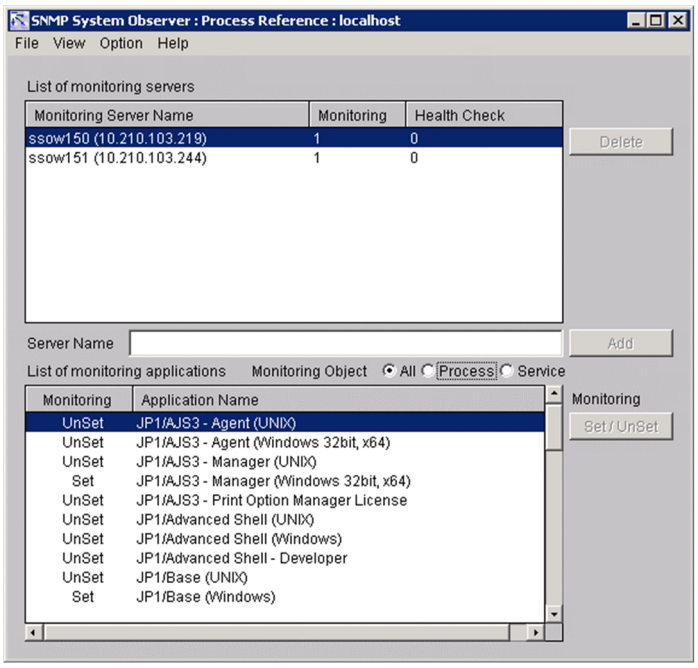
Health Check Interval

Specify a health check interval between 0 and 525,600 minutes. If you specify 0, SSO does not regularly perform a health check.

4.7 Process Reference window

The Process Reference window references the monitoring conditions of a process. The following figure shows the Process Reference window.

Figure 4-80: Process Reference window



The items to be set are:

List of monitoring servers

Displays the servers registered as monitoring server and the monitoring conditions set for each server.

Server Name

Cannot be entered.

Add

This button is deactivated and cannot be used.

List of monitoring applications

Displays the applications registered in the server selected in **List of monitoring servers**, and the monitoring conditions for each application.

Monitoring Object

Limits the applications to be displayed in **List of monitoring applications**.

- All

  Displays applications that monitor both processes and services.

- Process

  Displays applications that monitor processes only.

- Service

  Displays applications that monitor services only.

The next table explains the menu items.

Menu bar	Menu command		Description
File	Change Connection#		Change the connection destination.
	Save		Saves the settings and starts monitoring.
View	Update Condition		Obtains a monitoring condition again.
Option	Monitoring Server	Setting the monitoring interval	Displays the Set Monitor Interval window.
		Setting the health check interval	Displays the Set Health Check Interval window.
	Monitoring Application	Automatic Action	Displays the Automatic Action window.
		Remote Command	Displays the Remote Command window.
	Application Registration		Displays the Register Application window.

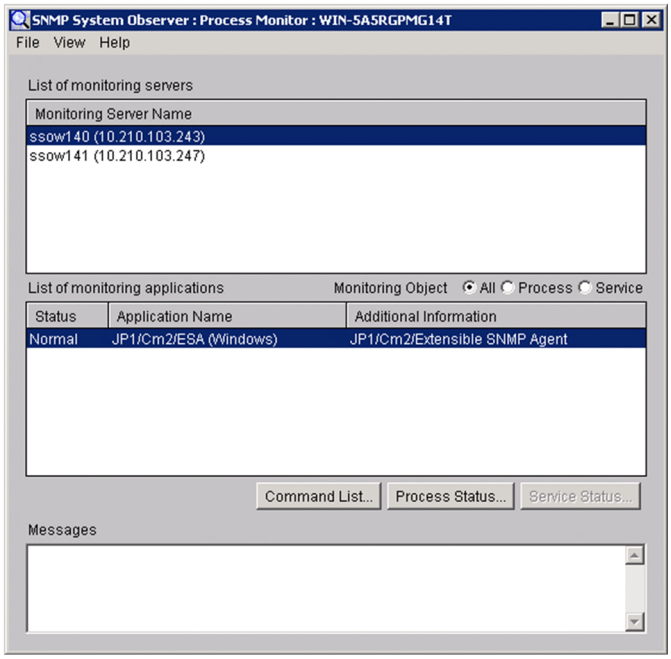
#

The menu command is not displayed if you opened the window from the SSO console.

4.8 Process Monitor window

The Process Monitor window references the statuses of monitoring applications. The following figure shows the Process Monitor window.

Figure 4-81: Process Monitor window



The items to be set are:

List of monitoring servers

This box displays the servers registered as monitoring servers.

List of monitoring applications

This box displays the statuses of the applications registered on the server selected in **List of monitoring servers**.

Monitoring Object

Limits the applications to be displayed in **List of monitoring applications**.

- **All**

  Displays applications that monitor both processes and services.

- **Process**

  Displays applications that monitor processes only.

- **Service**

  Displays applications that monitor services only.

Command List

This button displays the Command List window. In the Command List window, you can execute a registered command on APM at the desired time. For details on the Command List window, see *4.8.2 Command List window*.

Process Status

This button displays the Process Status window that shows the statuses of processes and child processes according to the monitoring conditions. For details on the Process Status window, see *4.8.1 Process Status window*.

Service Status

This button displays the Service Status window that shows service statuses according to the monitoring conditions. For details on the Service Status window, see *4.8.3 Service Status window*.

Messages

This box displays messages.

The next table explains the menu items.

Menu bar	Menu command	Description
File	Change Connection#	Changes the connection destination.
View	Update status	Matches the status on SSO and APM of an application of the server selected in **List of monitoring servers**.
	Search Monitoring Server	Displays the Search Monitoring Server window. This menu command can be selected only when **List of monitoring servers** contains at least one server.

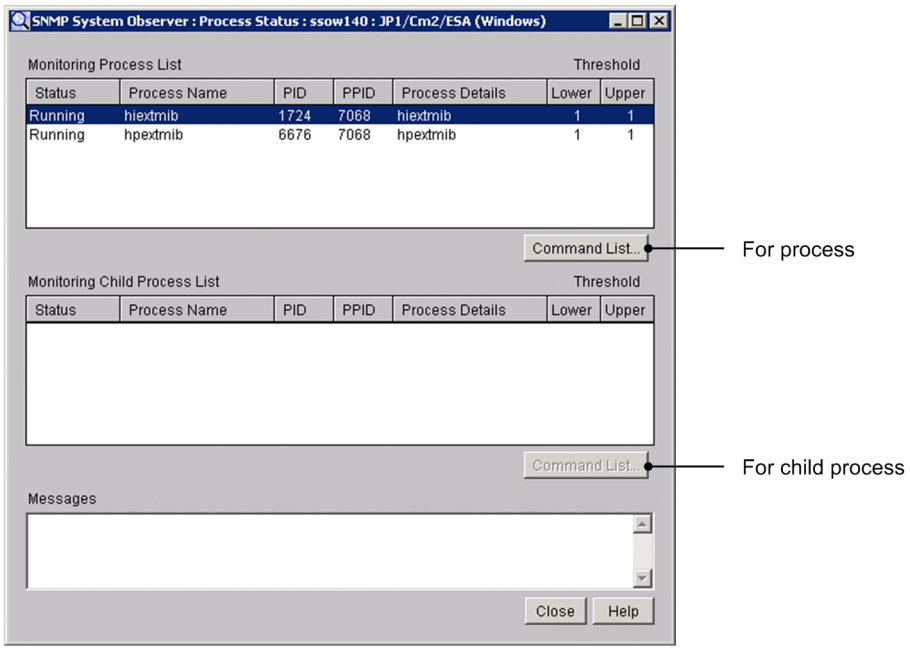
#

The menu command is not displayed if you opened the window from the SSO console.

4.8.1 Process Status window

The Process Status window references the statuses of monitored processes and monitored child processes. The following figure shows the Process Status window.

Figure 4-82: Process Status window



The items to be set are:

Monitoring Process List

This box displays the statuses of monitored processes. The following table describes the items displayed in the list.

Status	Description
Running	Indicates that the applicable process is a running monitored process.
Not Running	Indicates that the applicable process is a monitored process which is not found, not running, or terminated.
Unknown	Indicates the applicable process is a monitored process for which process information cannot be obtained because a communication error occurred between a manager and an agent or an APM stopped.
Zombie	Indicates that the parent process cannot recognize termination of the applicable monitored child process. This status can be detected only when the OS of the agent is HP-UX or HP-UX (IPF).

Command List (Monitored process)

This button displays the Command List window. In the Command List window, you can execute a registered command on APM at the desired time. For details on the Command List window, see *4.8.2 Command List window*

Monitoring Child Process List

This box displays the statuses of monitored child processes. The following table describes the items displayed in the list.

Status	Description
Running	Indicates that the applicable process is a running monitored process.
Not Running	Indicates that the applicable process is a monitored process which is not found, not running, or terminated.
Unknown	Indicates the applicable process is a monitored process for which process information cannot be obtained because a communication error occurred between a manager and an agent or an APM stopped.
Zombie	Indicates that the parent process cannot recognize termination of the applicable monitored child process. This status can be detected only when the OS of the agent is HP-UX or HP-UX (IPF).
Outside the target range	Indicates that the applicable process is not monitored, but is a running child process.

Command List (monitoring child process)

This button displays the Command List window. In the Command List window, you can execute a registered command on APM at the desired time. For details on the Command List window, see *4.8.2 Command List window*

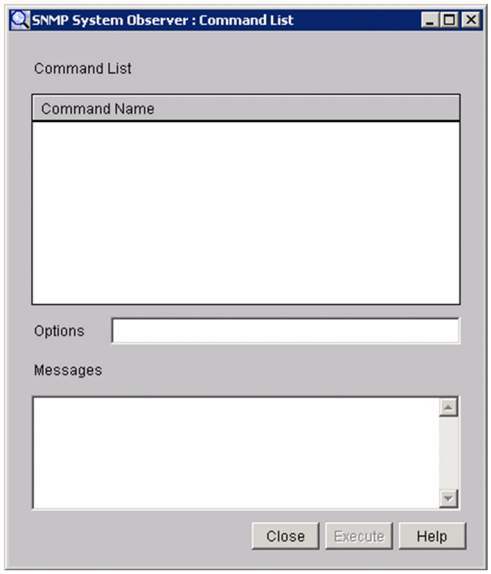
Messages

This box displays messages.

4.8.2 Command List window

The Command List window executes a command on APM at the desired time. The following figure shows the Command List window.

Figure 4－83: Command List window



The items to be set are:

Command List

This box displays the registered commands. Select a command to be executed.

Options

Specify options for the command selected in **Command List**. Specify the command name and option in 160 bytes or less. Do not specify a tab.

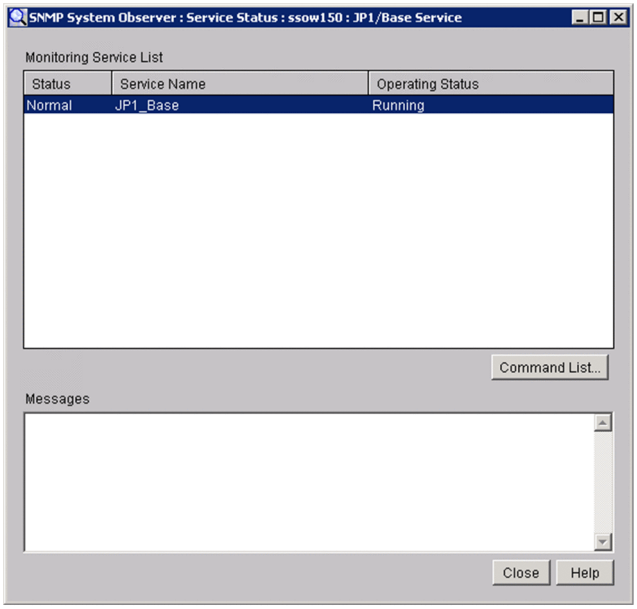
Messages

This box displays the result of executing the command.

4.8.3 Service Status window

The Service Status window displays monitoring condition of a service according to the monitoring conditions. The following figure shows the Service Status window.

Figure 4-84: Service Status window



The items to be set are:

Monitoring Service List

Displays the status of monitored services. Statuses, names, and operating statuses of services are displayed.

Command List

This button displays the Command List window. For details on the Command List window, see *4.8.2 Command List window*

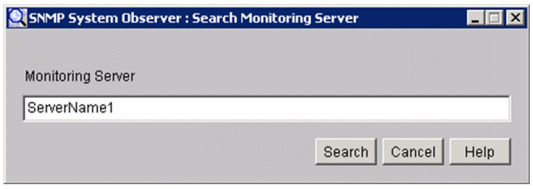
Messages

Displays messages.

4.8.4 Search Monitoring Server window

The Search Monitoring Server window is used to search for a monitoring server. The following figure shows the Search Monitoring Server window.

Figure 4-85: Search Monitoring Server window



The items to be set are:

Monitoring Server

Specify the host name or IP address of the monitoring server that you want to search for. You can specify a maximum of 255 bytes.

Search

Start a search with the condition specified for **Monitoring Server**.

Searches server names from the top of the **List of monitoring servers**, and moves the items that are perfect matches to the monitoring server. If no monitoring server name matches perfectly, the selected item is moved to the server that has the name which was found first through a forward match.

If no applicable monitoring server name exists, a warning dialog box appears.

When you specify an IP address in the **Monitoring Server** text box, a matching string is searched through the IP address section in the **List of monitoring servers**.

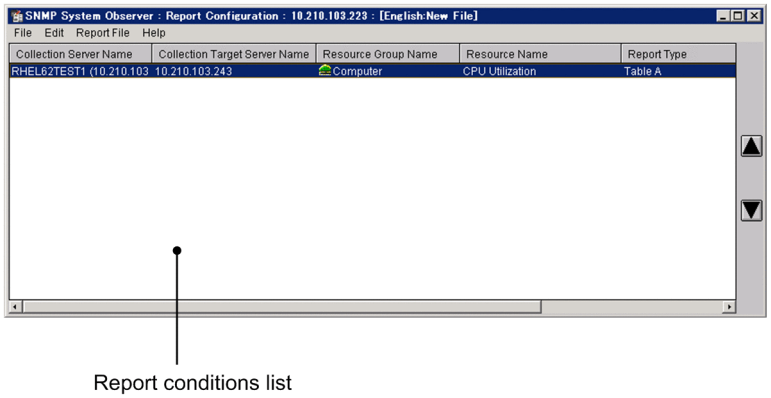
Important note

If the OS that opened the window is UNIX, the host names are case sensitive. Be careful when you enter the monitoring server name.

4.9 Report Configuration window

The Report Configuration window displays the report conditions. The following figure shows the Report Configuration window.

Figure 4-86: Report Configuration window



The report conditions list displays the report conditions saved in the report definition file. The Additional Information field displays information about the collected data file targeted for the report. The next table explains the format of additional information.

Format	Description
Database type	Displays the type of the collected data file.  : Indicates that the file is a master file.  : Indicates that the file is a copy file. If the file is a copy file, the copy ID is displayed after the icon.
File ID	Displays the ID of the file.

The next table explains the menu items.

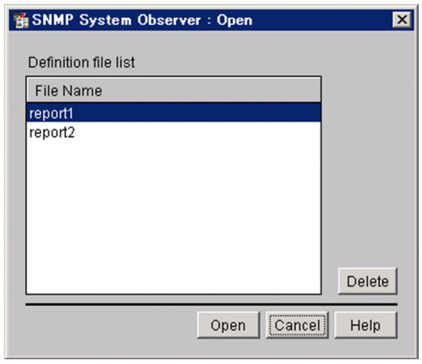
Menu bar	Menu command	Description
File	New	Creates a report definition file.
	Open	Displays the Select Report Definition File window.
	Save	Saves the report definition file.
	Save as	Displays the Save Report Definition File window.
Edit	Add Condition	Displays the Report Condition Addition wizard.
	Delete Condition	Deletes the report condition selected in the report conditions list.
	Set Condition	Displays the Report Condition Setup window.
	Set Report Type	Displays the Report Type Setup window.
	Move Up	Reverses the order of the report condition selected in the report conditions list and the report condition immediately above it.
	Move Down	Reverses the order of the report condition selected in the report conditions list and the report condition immediately below it.
Report File	Create	Displays the Creating of Report File window.

Menu bar	Menu command	Description
Report File	Set	Displays the Set Report File window.

4.9.1 Select Report Definition File window

The Select Report Definition File window opens a report definition file that has been saved. The following figure shows the Select Report Definition File window.

Figure 4-87: Select Report Definition File window



The items to be set are:

Definition File List

This list box displays the definition files saved in the directory containing the report definition file. The directory containing the report definition file is:

```
UNIX: $SSO_CONF/rpt
Windows: $SSO_CONF\rpt
```

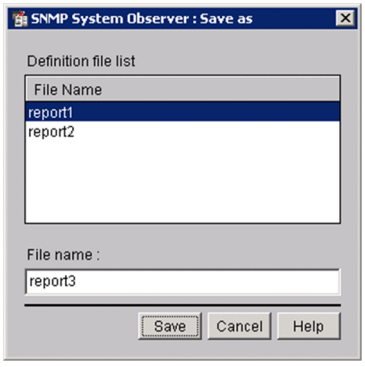
Delete

This button deletes the definition file selected in **Definition File List**.

4.9.2 Save Report Definition File window

The Save Report Definition File window saves a report definition file that has been saved. The following figure shows the Save Report Definition File window.

Figure 4-88: Save Report Definition File window



The items to be set are:

Definition file list

This list box displays the definition files that have been saved.

File Name

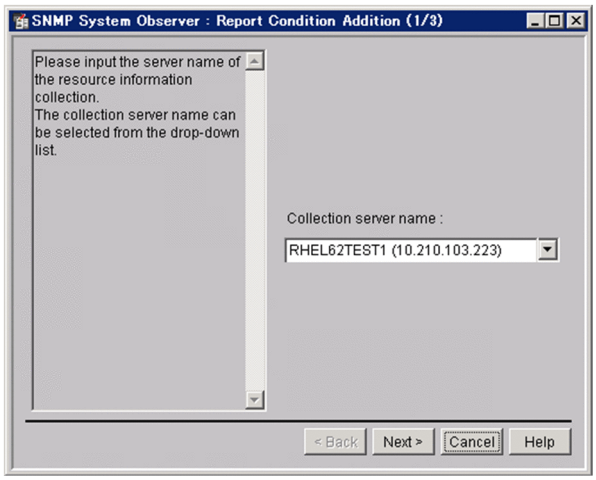
Specify the name of the file to be saved. Specify the file name with a character string of 1 to 255 bytes including the path to the report definition file storage directory. You cannot use a slant (/) and a backslash (\) in the file name. The directory containing the report definition file is:

```
UNIX: $SSO_CONF/rpt
Windows: $SSO_CONF\rpt
```

4.9.3 Report Condition Addition wizard

The Report Condition Addition wizard adds a report condition. Figures 4-89 to 4-91 show the Report Condition Addition wizard.

Figure 4－89: Report Condition Addition wizard (1/3)

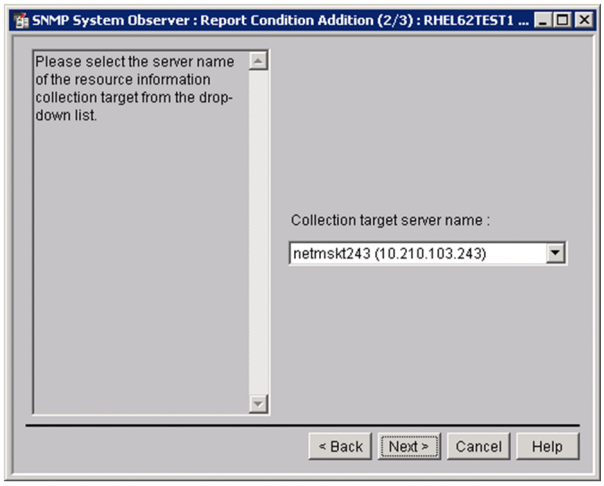


The items to be set are:

Collection server name

Specify the host name or IP address of the server that is collecting resources. Specify the host name or IP address in 255 bytes or less.

Figure 4-90: Report Condition Addition wizard (2/3)

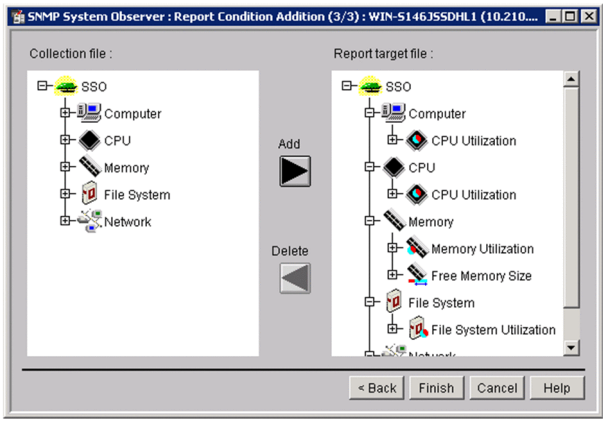


The items to be set are:

Collection target server name

Specify the server targeted for collection.

Figure 4-91: Report Condition Addition wizard (3/3)



The items to be set are:

Collection file

This box displays the files of the collection database specified in **Collection Server Name** and **Collection target server name**. These files can be output to a report.

Report target file

This box displays the collection database files to be output to a report.

Add

This button adds items of data to **Files Targeted For Report**. You can add items of data not only in units of files but also in units of categories, resource groups, or resources.

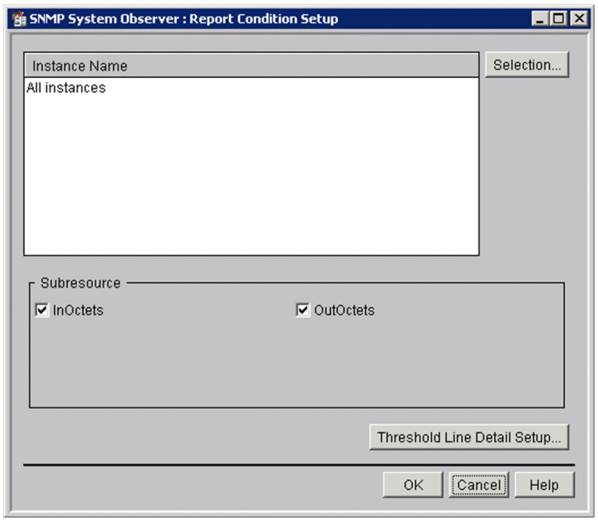
Delete

This button deletes items of data from **Files Targeted For Report**. You can delete items of data not only in units of files but also in units of categories, resource groups, or resources.

4.9.4 Report Condition Setup window

The Report Condition Setup window sets subresources and instances to be reported. The following figure shows the Report Condition Setup window.

Figure 4-92: Report Condition Setup window



The items to be set are:

Instance Name

This list box displays a list of instances. If no instances have been registered, the list box displays **All Instances**. If you want to set report conditions for a particular instance, you must register the instance in the Select Instance window.

Selection

This button displays the Select Instance window.

Subresource

Select the checkbox indicating each subresource to be output to the report. The options that are displayed depend on the resource. By default, all subresources are eligible to be output to the report.

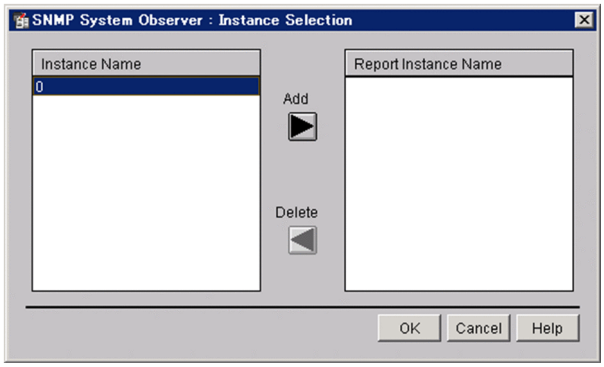
Threshold Line Detail Setup

Sets how to display threshold information in a graph. This button opens the Threshold Line Detail Setup window. When the report type is table format, the display setting of the threshold is ignored.

(1) Instance Selection window

The Instance Selection window selects an instance when you create a report for a particular instance. The following figure shows the Instance Selection window.

Figure 4-93: Instance Selection window



The items to be set are:

Instance Name

This box lists the instances that have been saved to the collection file.

Report Instance Name

This box displays the instances for which a report is to be created.

Add

This button adds an instance to **Report Instance Name**.

You cannot specify an instance name that has a space character at the beginning or the end.

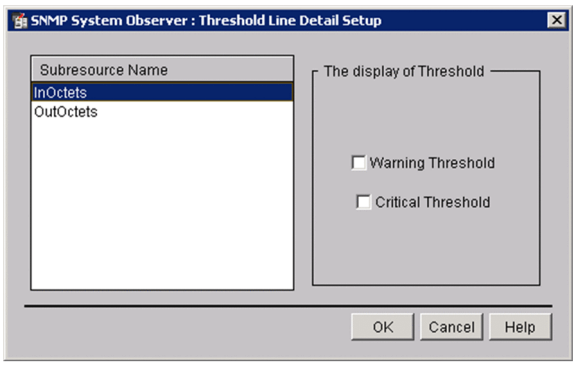
Delete

This button deletes an instance from **Report Instance Name**.

(2) Threshold Line Detail Setup window

The Threshold Line Detail Setup window specifies settings for displaying threshold lines for each subresource. Lines for the warning threshold and the critical threshold can be set to be displayed for each subresource. The following figure shows the Threshold Line Detail Setup window.

Figure 4-94: Threshold Line Detail Setup window



Subresource Name

Displays a list of subresource names. Subresources vary depending on the resource. Select the subresource of which threshold line you want to display.

Warning Threshold

When you select this check box, the warning threshold of the applicable subresource is displayed in a graph. If you clear this check box, the warning threshold is not displayed. By default, this check box is not selected. This setting

is applied to a graph if you select **The display of Threshold Line** and **It displays by setup of every Subresource** in the Graph Detail Setup window.

Caution Threshold

When you select this check box, the critical threshold of the applicable subresource is displayed in a graph. If you clear this check box, the critical threshold is not displayed. By default, this check box is not selected. This setting is applied to a graph if you select **The display of Threshold Line** and **It displays by setup of every Subresource** in the Graph Detail Setup window.

4.9.5 Report Type Setup window

The Report Type Setup window sets the title of a report and the report format. The following figure shows the Report Type Setup window.

Figure 4-95: Report Type Setup window (for table)

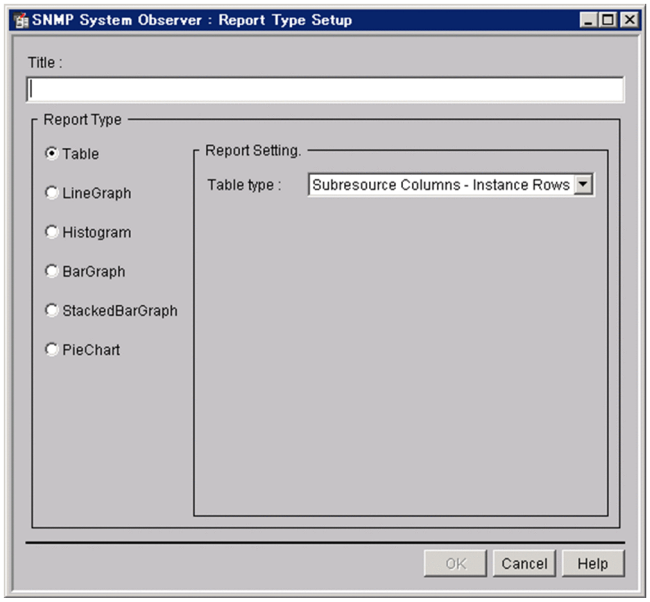


Figure 4-96: Report Type Setup window (for line graph)

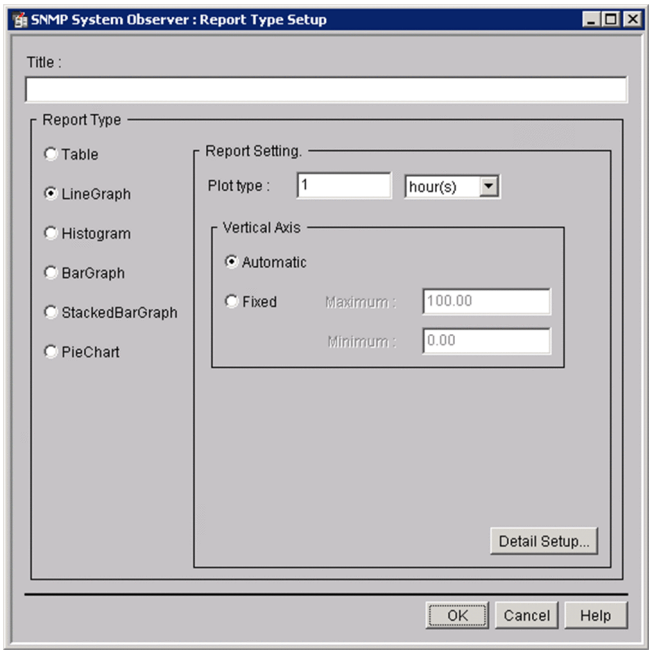


Figure 4-97: Report Type Setup window (for histogram)

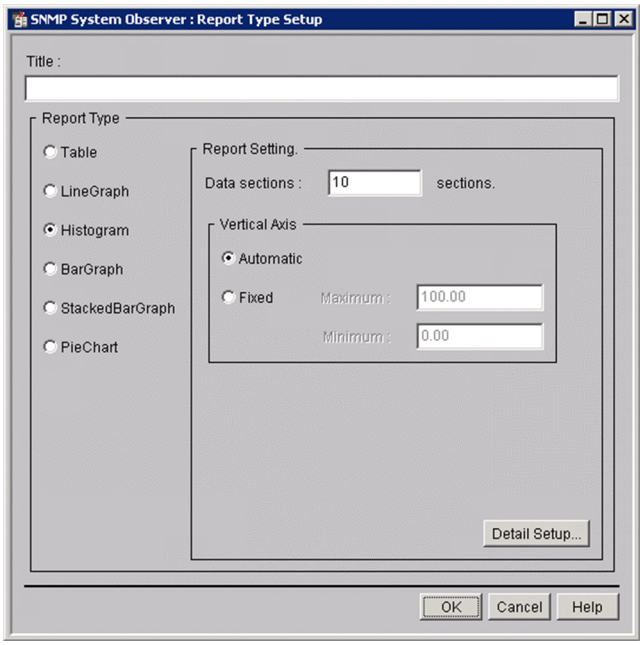


Figure 4-98: Report Type Setup window (for bar graph)

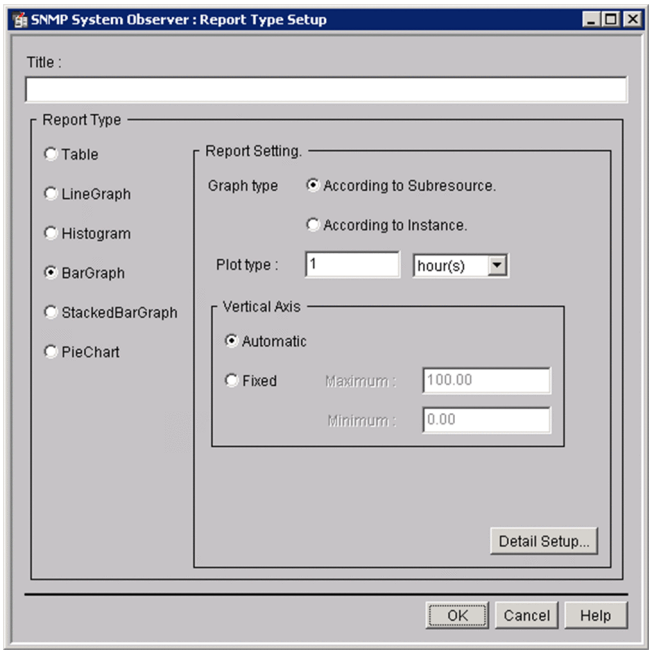


Figure 4-99: Report Type Setup window (for stacked bar graph)

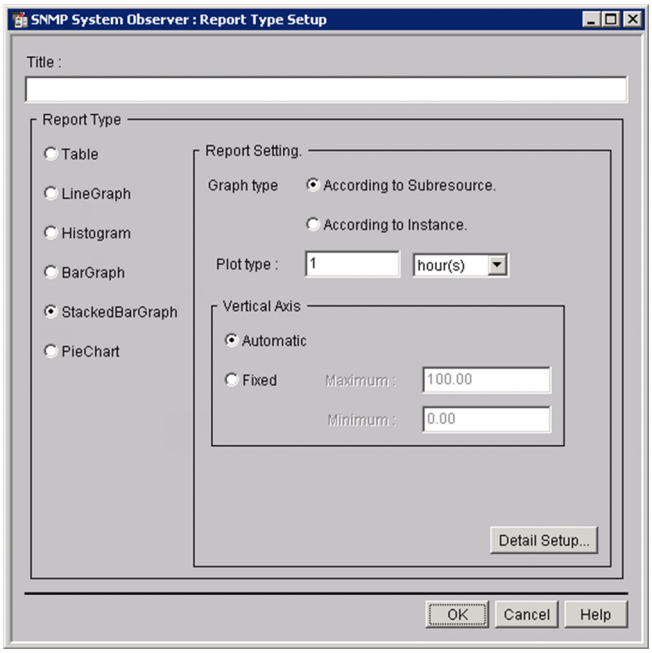
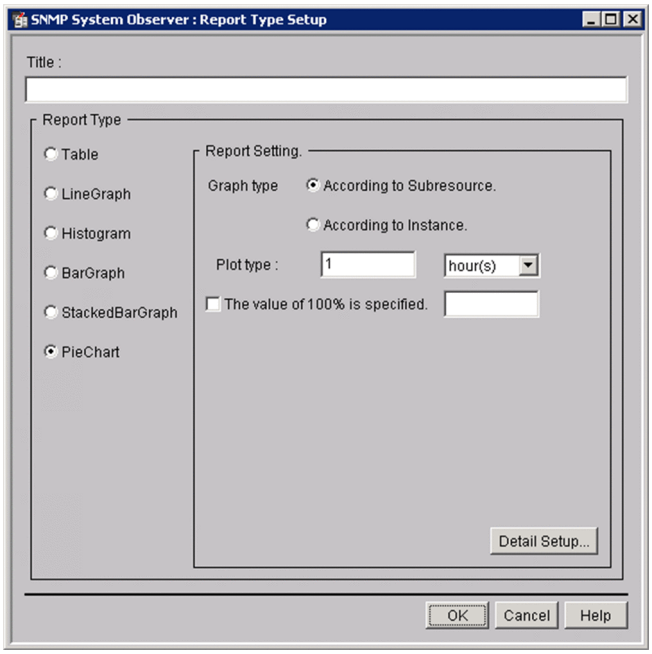


Figure 4－100: Report Type Setup window (for pie chart)



The items to be set are:

Title

Specify the title of the report with a character string of 1 to 255 bytes.

Report Type

Select the format of the report you want to create.

- **Table**
  Creates the report in table format.
- **LineGraph**
  Creates a report in line graph format.
- **Histogram**
  Creates a report in histogram format.
- **BarGraph**
  Creates a report in bar graph format.
- **StackedBarGraph**
  Creates a report in stacked bar graph format.
- **PieChart**
  Creates a report in pie chart format.

By default, **Table** is selected.

For a graph, the number of columns that can be drawn in a graph is as follows:

- Line graph: 100
- Histogram: 8
- Other than the above: 100 elements per graph

Report Setting

Table type

Select one of the following output formats to be used for a table:

- **Subresource Columns - Instance Rows**
- **Instance Columns - Subresource Rows**
- **According to Instance**
- **According to Subresource**

By default, **Subresource Columns - Instance Rows** is selected.

For details on output formats, see *2.4.3 Details of HTML-format report files*.

Plot type

When creating the report in graph format, specify the interval to be plotted in the graph. Specify an interval between 5 minutes and 1 day. The default is 1 hour.

For a line graph, calculates the average value from collected data at the interval specified for **Plot type**, and set the value as a plot point. A line that connects adjacent plot points is a collection data line. If no collection data exists in a plot interval, a plot point is not created. In such a case, the period for which a plot point is not created is ignored, and a line that connects adjacent plot points is drawn.

For a bar graph, stacked bar graph, or pie chart, each plot point constitutes a graph.

Data sections

Specify the number of data sections, from 4 to 20, when you create a report in histogram format.

By default, 10 is set.

Vertical Axis

When you create a report in HTML format, specify the maximum and minimum values for the vertical axis of a graph.

- **Automatic Action**

  Sets the maximum and minimum values automatically.

- **Fixed**

  Sets the maximum and minimum values manually. The range of specifiable values is from 0.00 to 4,294,967,295.00. You can specify a value that has 1 decimal place.

The default is **Automatic Action**.

Graph type

Specifies the output format when you create a report in bar graph format, stacked bar graph format, or pie chart format.

- **According to Subresource**
- **According to Instance**

The default is **According to Subresource**.

100% of valure is specified.

Select this check box to specify the reference value of a pie chart.

When you select this check box, the value of each item is displayed in a pie chart assuming that the value entered in the text box is 100 percent. You can specify a value from 0.01 to 1.7976931348623157 **x** 10^{308}. If the value in the mantissa exceeds 1.7976931348623157, it is rounded.

In the text box, you can enter an exponent, `e` in addition to numbers. For example, when you enter `1.4e3`, it means 1.4 **x** 10^{3}.

Detail Setup

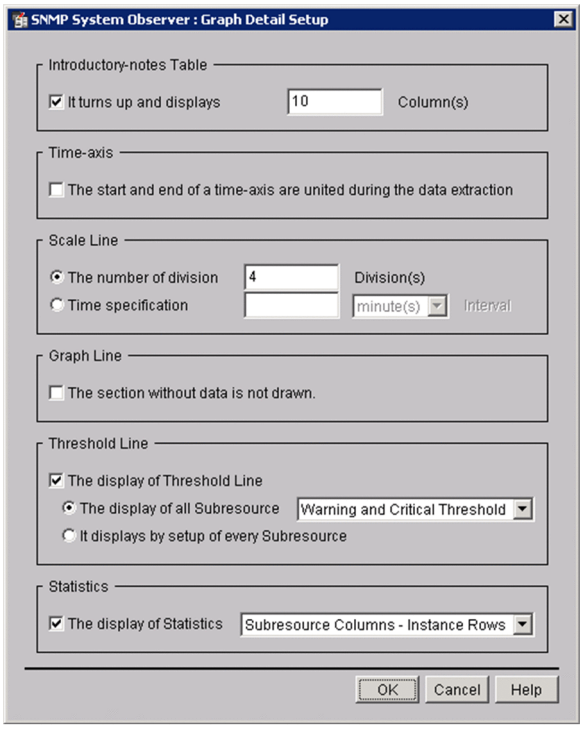
This button displays the Graph Detail Setup window. For details on the Graph Detail Setup window, see *(1) Graph Detail Setup window*.

(1) Graph Detail Setup window

The Graph Detail Setup window sets the detailed items of a graph. The Graph Detail Setup window shows different display items, depending on the format. The following subsections describe the items for each format.

(a) For Line graph

Figure 4-101: Graph Detail Setup window (for line graph)



Introductory-notes Table

It turns up and displays

Specifies the number of columns for a graph introductory-notes table. When this check box is selected, the graph introductory-notes table is output in the appropriate format for each subresource. In such a case, the number in the text box is applied as the number of columns in a graph introductory-notes table.

When this check box is cleared, the graph introductory-notes table is displayed in instance count-based format. In such a case, the number of columns in a graph introductory-notes table is the number of instances.

By default, this check box is selected. For details on the graph introductory-notes table format, see *2.4.4(2) Graph introductory-notes table*.

Column(s)

Specify the number of columns for a graph introductory-notes table. The setting is valid only when **It turns up and displays** is selected.

For the differences of report output results that depend on the setting, see *2.4.4 Report files in line graph format*.

The entered value is the number of columns. If you enter a value which is greater than the number of instances of a resource to be reported, the number of columns in the graph introductory-notes table is the number of instances.

Specifiable values are an integer from 0 to 100. No invalid values can be entered. By default, 10 is set.

Time-axis

The start and end of a time-axis are united during the data extraction

Selecting this check box sets the extraction start date and time of the data extraction period as the start time for the time axis of the graph, and the extraction end date and time as the end time of the graph.

Clearing this check box sets the first plotted point as the start time for the time axis of the graph, and the last plotted time as the end time of the graph. By default, this check box is not selected.

If you select this check box, but omit the start and/or end time of the data extraction period, the omitted time axis follows the rule in effect when this check box is cleared.

For details on the data extraction period, see *4.9.6 Creating of Report File window*.

Scale Line

Specifies the scale for the time axis of a graph. You can specify either the number of divisions of the time axis, or the interval of scales.

The number of division

Specify the number of scale lines of the time axis. Enter the number in the text box to the right. By default, this radio button is selected.

Division

Specify the number of scale lines for the time axis. You cannot enter a value if **Time specification** is selected. The default is 4.

Specifiable values are an integer from 1 to 60. You cannot enter an invalid value. If you click the **OK** button without entering any value, an error dialog box appears.

Time specification

Specify the interval of the time axis. Enter the number in the text box to the right. You cannot enter a value if **The number of division** is selected. By default, this button is not selected.

Although the value you can enter depends on the selection in the **Interval** drop-down list box, you can enter an integer from 1 (minute) to 365 (days).

When **Time specification** is selected, if you enter a space, a non-integer value, or a number other than 1 through 525,600, and click the **OK** button, an error dialog box appears.

Interval

Enter the unit for the value you entered in the left text box. You can select `minute(s)`, `hour(s)`, or `day(s)`. When **The number of division** is selected, you cannot select the unit.

Although `minute(s)` is selected by default, the selection is invalid if **The number of division** is selected.

Graph Line

The section without data is not drawn.

A graph line is drawn at the interval specified for **Plot type**.

When you select this check box, if no data to be used for calculating the average value in the interval specified for **Plot type** in the Report Type Setup window exists, a graph line with the interval is not drawn.

When you clear this check box, if no applicable data in the interval specified for **Plot type** exists, a line is drawn connecting the points with applicable data. This setting is valid for lines of collection data only.

When you select this check box, if you specify a value smaller than the actual resource collection interval in **Plot type**, a dashed graph line might be displayed. By default, this check box is not selected.

Threshold Line

The display of Threshold Line

Specifies the display settings of a threshold line. After selecting this check box, you can select **The display of all Subresources** or **It displays by setup of every Subresource**. The threshold line is displayed according to the radio button you selected.

By default, this check box is not selected.

When threshold settings are specified in the Threshold Line Detail Setup window, if this check box is cleared, the threshold line is not displayed.

If you specify settings for displaying a threshold line, the value set as the threshold is displayed regardless of the threshold monitoring settings.

The display of all Subresource

Displays the threshold line for all subresources. You can select the threshold line you want to display from the drop-down list box.

When threshold settings are specified in the Threshold Line Detail Setup window, if you select **The display of all Subresources**, this setting takes precedence over the settings in the Threshold Line Detail Setup window. Therefore, the threshold lines of all subresources are displayed. However, the settings in the Threshold Line Detail Setup window are still valid.

You can select one of the following options for the threshold line to be displayed:

- **Warning and Caution Threshold**
- **Warning Threshold**
- **Caution Threshold**

It displays by setup of every Subresource

Specifies threshold settings for each subresource and displays the threshold.

Perform this setting in the Threshold Line Detail Setup window. If you do not specify threshold settings for each subresource in the Threshold Line Detail Setup window, no threshold line is displayed.

Statistics

The display of Statistics

Specifies whether to display statistics information under a graph. Select the statistics information output format for tables. You can select one of the following formats for tables from the applicable drop-down list box:

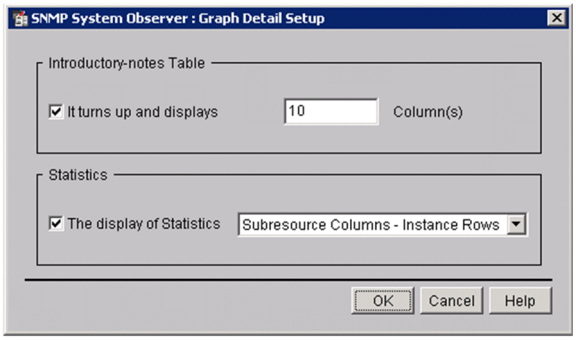
- **Subresource Columns - Instance Rows**
- **Instance Columns - Subresource Rows**
- **According to Instance**
- **According to Subresource**

The default is **Subresource Columns - Instance Rows**.

You can select the above formats when **The display of Statistics** is selected. By default, the check box is not selected.

(b) For histogram

Figure 4-102: Graph Detail Setup window (For histogram)



Introductory-notes Table

It turns up and displays

Specifies the number of columns for a graph introductory-notes table. When this check box is selected, the graph introductory-notes table is output in the appropriate format for each subresource. In such a case, the number in the text box is applied as the number of columns in a graph introductory-notes table.

When this check box is cleared, the graph introductory-notes table is displayed in instance count-based format. In such a case, the number of columns in a graph introductory-notes table is the number of instances.

By default, this check box is selected. For details on graph introductory-notes table formats, see *2.4.4(2) Graph introductory-notes table*.

Column(s)

Specify the number of columns for a graph introductory-notes table. The setting is valid only when **It turns up and displays** is selected.

For the differences in report output results that depend on the setting, see *2.4.4 Report files in line graph format*.

The entered value is the number of columns. If you enter a value which is greater than the number of instances of a resource to be reported, the number of columns in a graph introductory-notes table is the number of instances.

Specifiable values are an integer from 0 to 100. No invalid values can be entered. By default, 10 is set.

Statistics

The display of Statistics

Specifies whether to display statistics information under a graph. Select the statistics information from the output formats for tables. You can select one of the following output formats for tables in the applicable drop-down list box:

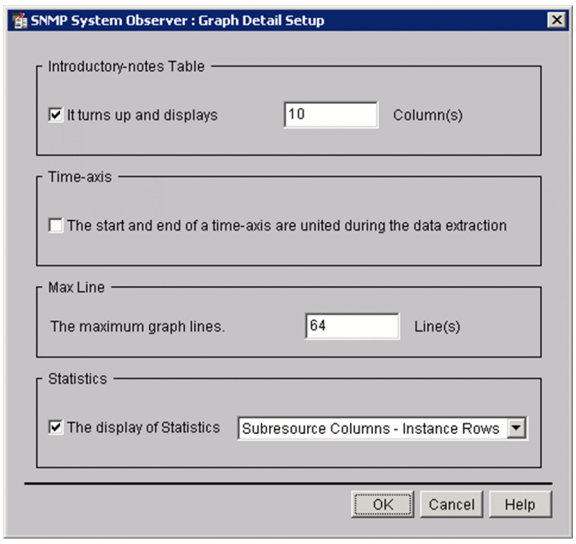
- **Subresource Columns - Instance Rows**
- **Instance Columns - Subresource Rows**
- **According to Instance**
- **According to Subresource**

The default is **Subresource Columns - Instance Rows**.

You can select the above formats when **The display of Statistics** is selected. By default, the check box is not selected.

(c) For bar graph, stacked bar graph and pie chart

Figure 4-103: Graph Detail Setup window (For bar graph and stacked bar graph)



Introductory-notes Table

It turns up and displays

Specifies the number of columns for a graph introductory-notes table. When this check box is selected, the graph introductory-notes table is output in the format appropriate for each subresource. In such a case, the number in the text box is applied as the number of columns in a graph introductory-notes table.

When this check box is cleared, the graph introductory-notes table is displayed in instance count-based format. In such a case, the number of columns in a graph introductory-notes table is the number of instances.

By default, this check box is selected. For details on graph introductory-notes table formats, see *2.4.4(2) Graph introductory-notes table*.

Column(s)

Specify the number of columns for a graph introductory-notes table. The setting is valid only when **It turns up and displays** is selected.

For differences in the report output results that depend on the setting, see *2.4.4 Report files in line graph format*.

The entered value is the number of columns. If you enter a value which is greater than the number of instances of a resource to be reported, the number of columns in a graph introductory-notes table is the number of instances.

Specifiable values are an integer from 0 to 100. No invalid values can be entered. By default, 10 is set.

Time-axis

The start and end of a time-axis are united during the data extraction

Selecting this check box sets the extraction start date and time of the data extraction period as the start time for the time axis of the graph, and the extraction end date and time as the end time of the graph.

Clearing this check box sets the start time and end time of the actual data period as the start time and end time of the graph. By default, this check box is not selected.

If you select this check box, but omit the start and/or end time of the data extraction period, the omitted time axis follows the rule in effect when this check box is cleared.

For details on the data extraction period, see *4.9.6 Creating of Report File window*.

Max Line

The maximum graph lines.

Specify the maximum number of columns to be displayed. When you select this check box, you can enter an integer from 1 to 1024. By default, `64` is set.

Statistics

The display of Statistics

Specifies whether to display statistics information under a graph. Select the statistics information output format for tables. You can select one of the following formats for tables from the applicable drop-down list box:

- **Subresource Columns - Instance Rows**
- **Instance Columns - Subresource Rows**
- **According to Instance**
- **According to Subresource**

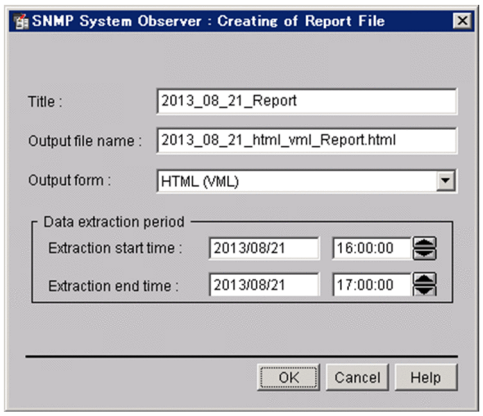
The default is **Subresource Columns - Instance Rows**.

You can select the above formats when **The display of Statistics** is selected. By default, the check box is not selected.

4.9.6 Creating of Report File window

The Creating of Report File window sets the title, output destination, format of a report file, and the period for the report. The following figure shows the Creating of Report File window.

Figure 4－104: Creating of Report File window



The items to be set are:

Title

Specify the title of the report file with a character string of 1 to 255 bytes. If you omit this value, no report file title is displayed.

Output file name

Specify a save destination for the report by its absolute path. Specify the destination in 255 bytes or less including the file name. Specifiable characters are single-byte alphanumeric characters, periods (.), underscores (_), and hyphens (-).

If the specified file already exists, SSO overwrites it. If you omit the file extension, SSO assigns the extension of the file format specified in **Output form**. If you specify only the file name, SSO saves the report to the following directory:

UNIX:

```
$SSO_REPORT/Report/CSV
$SSO_REPORT/Report/HTML
```

Windows:

```
$SSO_REPORT\Report\CSV
$SSO_REPORT\Report\HTML
```

Output form

Select CSV, HTML (VML), or HTML (SVG) as the output format for the report. If you selected Graph in Report Type and you create the report in csv format, SSO ignores the graph report. The default is CSV.

For details about the VML and SVG, see *2.4.1(1) Report file formats*.

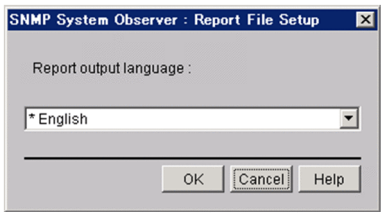
Data extraction period

Specify the start date and time and the stop date and time for extracting data to be output to the report. In the date fields, specify a date between January 1, 1980 and December 31, 2029 in the format *yyyy/mm/dd*. Specify a time between 00:00:00 and 23:59:59 in the format `00:00:00`.

4.9.7 Report File Setup window

The Report File Setup window specifies the character code of the report to be created by SSO. The following figure shows the Report File Setup window.

Figure 4－105: Report File Setup window



The items to be set are:

Report output language

Select **English**, **Japanese (Shift-JIS)**, **Japanese (EUC)**, or **Japanese (UTF-8)** as the character code for the report you are creating. When SSO is running in a language environment such as Shift-JIS, EUC, or UTF-8, the default value is the same character code as that for SSO. In other language environments, the default is **English**.

5 Commands

This chapter describes the syntax and usage of the commands provided by SSO series. The commands are described in detail in alphabetical order.

To execute a command in UNIX, the user must have superuser permission. To execute a command in Windows, the user must have Administrators permission.

Commands

This chapter describes the commands provided by the programs for SSO series.

Commands provided by SSO

The following tables list the commands provided by SSO. The commands are divided up according to function.

Table 5-1: Commands provided by SSO

Category	Function	Command name
Commands used at resource collection	Changes the collection conditions for a resource	ssocolset
	Starts collection of a resource	ssocolstart
	Stops collection of a resource	ssocolstop
	Checks the format of a collection conditions definition file	ssocolchk
	Converts a collection conditions definition file to the tab-delimited format	ssocolcvt
	Displays the resource collection status and resource threshold monitoring status	ssocolshow
	Verifies the validity of a threshold	ssocolverify
	Extracts collected data from a collection database	ssoextractlog
	Deletes data from a collection database	ssodbdel
	Monitors the size of a collection database	ssodbcheck
	Executes a MIB collection process	ssocollectd
	Executes a resource collection process	ssocolmng
Commands used at process or service monitoring	Changes a process or a service monitoring condition	ssopsset
	Starts process or service monitoring	ssopsstart
	Stops process or service monitoring	ssopsstop
	Checks the format of the definition file to be used at process or service monitoring	ssopschk
	Converts a definition file used at process monitoring to tab-delimited format	ssopscvt
	Displays the process or service monitoring status	ssopsshow
	Matches a process's status or a service's status, executes of a health check, or re-reads definition files	ssoapcom
Commands used at NNMi cooperation	• Sets up a cooperation with NNMi • Edits (adds, changes, or deletes) the NNM information definition file	ssonnmsetup
Commands used when defining user resources	Creates a user resource configuration file	ssocolconf
Commands that collect data upon occurrence of error	Collects data upon occurrence of error in SSO running in a UNIX system	jp1ssolog.sh (UNIX only)
	Collects data upon occurrence of error in SSO running in a Windows system	jp1ssolog.bat (Windows only)

Category	Function	Command name
Commands used at user authentication	Adds, changes, or deletes an SSO authentication user from the SSO console	ssoauth
Commands used at backup and restore	Backs up files and databases provided by SSO	ssobackup
	Restores files and databases provided by SSO	ssorestore
Commands used when a report is created	Issues an instruction to create a report file	ssodemandrpt
	Creates a report file	ssorptd
Commands used for opening a window	Opens a window other than windows related to the report function	ssoguistart
Commands that manage daemon processes	Starts each daemon process	ssostart
	Re-reads a definition file	ssospmd
	Stops each daemon process	ssostop
	Displays the status of each daemon process	ssostatus
Commands used for the NNMi map cooperation (symbol cooperation) function	Operates (deletes, matches, or displays) the status of the map cooperation (symbol cooperation) function	ssomapstatus
Commands used for the NNMi map cooperation (action cooperation) function	Deletes the custom attribute of the map cooperation (action cooperation) function	ssocadel
Commands used for receiving APM traps	Receives SNMP trap events	ssotrapd
Commands used for the SSO console function	Re-reads a definition file	ssoconsoled
Commands used for setting up an SSO cluster system environment	Sets up an SSO cluster system environment in a UNIX system	ssoclustersetup (UNIX only)
	Sets up an SSO cluster system environment in a Windows system	ssoclustersetup.vbs (Windows only)

Execution privileges and storage directory

Execution privileges

In Windows: Administrators

In UNIX: Superuser

Storage directory

The commands provided by each SSO program are stored in the following directories:

For Windows

```
installation-directory\bin
```

For UNIX

```
/opt/CM2/SSO/bin
```

Notes

(1) Notes on successively executing commands

- Prevent the following two combinations of commands from being executed in succession.

  When you want to execute these combinations of commands in succession, make sure that you have an interval of 1 or more minutes between the commands. If you execute these combinations of commands at an interval of less than 1 minute, the SSO window might freeze up.

  - Combination of the `ssopsstop` command and the `ssopsstart` command
  - Combination of the `ssocolstop` command and the `ssocolstart` command

- Prevent the `ssopsstop` command or the `ssopsstart` command from being executed in succession for a specific monitoring server.

  When you execute those commands in succession, you must have an interval of 1 or more minutes or specify multiple applications. For details about how to specify multiple applications, see the explanation of the `-af` option in *ssopsstart* and *ssopsstop* in *5. Commands*. If you execute those commands at an interval of less than 1 minute, the status of the process monitoring application might become unstable.

(2) Notes on simultaneously activating commands and windows

You cannot simultaneously activate multiple commands and windows related to setup of process monitoring conditions shown in the following (a) and multiple commands and windows related to setup of resource collection conditions shown in the following (b).

You can perform operations in the window by switching the mode in reference mode. However, you cannot perform setting operations.

(a) `ssopsset` command and the Process Configuration window

(b) `ssocolset` command and the Resource Configuration window

(3) Notes on backup immediately after execution of the ssopsset, ssopsstart, or ssopsstop command

Do not perform a backup (`ssobackup`) immediately after or during execution of the `ssopsset`, `ssopsstart`, or `ssopsstop` command.

When you perform a backup immediately after execution of the `ssopsset`, `ssopsstart`, or `ssopsstop` command, do so 1 or more minutes afterwards to ensure the integrity of the backup data.

jp1ssolog.bat (Windows only)

Format

```
jp1ssolog.bat [-col] [-d output-destination-directory-name] [<agent> ...]
```

Function

The `jp1ssolog.bat` command collects data for an error investigation upon occurrence of an error in SSO. This command is only for Windows.

This command creates a `JP1SSO` directory in the default directory or the directory specified for the `-d` option and outputs data to be collected in the created directory. If a `JP1SSO` directory already exists, it is deleted and a new `JP1SSO` directory is created.

The default output destination for the data to be collected is `%TEMP%\jp1log`. You can change the default output destination by editing this command (a batch file).

Option

-col

Collects data in `$SSO_DB\Coll` as data for an error investigation.

-d *output-destination-directory-name*

Specifies the output destination for the data to be collected by using either a relative or absolute path.

<agent> ...

Collects the results of executing the `ping` command on the specified monitoring server as data for an error investigation. Specify an IP address or host name for <*agent*>. If the specified IP address or host name is incorrect, or the monitoring server is not running, the return value of the command is `1`.

Customize

This command is a batch file. You can customize the following items, if necessary:

If you want to change the default output destination

Edit the output file name in the following line:

```
set OUTPUTDIR=%TEMP%\jp1log
```

If the installation path for SSO is different from the standard installation path

Edit the installation path in the following line:

```
set INST_DIR_SSO=%SystemDrive%\Program Files (x86)\HITACHI\JP1Cm2SSO
```

Usage example

- To collect data when an error has occurred on monitoring servers `agt1` and `agt2`, execute the following command:

  ```
  jp1ssolog.bat agt1 agt2
  ```

Collected data list

The following table lists and describes the data for an error investigation to be collected:

Classification	Collection method	Acquired data		
Main Information	Manual	An environment configuration chart (OS, IP address, No. of interfaces, and the product configuration and version of each terminal)		
		A memo about how an error occurred (details about the occurrence date/time, OS, host name, IP address, performed operations, and symptoms)		
		Event log file[#1]		
		Problem report and user dump[#2]		
OS information	`jp1ssolog.bat`	Collected files	In `%SystemRoot%\system32\drivers\etc`	
		Command execution results	`hostname`	
			`set`	
			`netstat -a`	
			`netstat -aon`	
			`netstat -r`	
			`net start`	
			`ipconfig /all`	
			Registry information	In `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\`
				In `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\HITACHI\`
			`tasklist`	
			`msinfo32`	
			`netsh -c advfirewall show allprofiles`	
			`netsh -c advfirewall firewall show rule name=all verbose`	
SSO information	`jp1ssolog.bat`	Collected files	In *SSO-installation-folder*`\conf` folder	
			In *SSO-installation-folder*`\log` folder	
			In *SSO-installation-folder*`\report` folder	
			SSO-installation-folder`\uCPSB\CC\web\containers\SSOConsole\logs`	
			SSO-installation-folder`\uCPSB\CC\web\containers\SSOConsole\usrconf`	
			SSO-installation-folder`\uCPSB\CC\web\containers\SSOConsole\work`	
			SSO-installation-folder`\uCPSB\httpsd\conf`	
			SSO-installation-folder`\uCPSB\httpsd\logs`	
			SSO-installation-folder`\uCPSB\CC\client\logs\system\ejbcl\CJW`	

Classification	Collection method	Acquired data		
SSO information	`jp1ssolog.bat`	Collected files	*SSO-installation-folder*`\uCPSB\CC\web\redirector\logs`	
			In *SSO-installation-folder*`\auditlog`	
			SSO-installation-folder`\tmp\ssoclustersetup.log` (when applicable)	
			`%windir%\Temp\HCDINST\`*PP-ID*`.LOG` (when applicable)	
			`%windir%\Temp\jp1cm2sso_installer.log` (when applicable)	
			SSO-installation-folder`\uCPSB\install.log` (when applicable)	
			SSO-installation-folder`\uCPSB\insresult.dat` (when applicable)	
		Command execution results	`ssostatus`	
			`ssoapcom -X 4095`[#3]	
			`ssocollectd -X 4095`[#3]	
			`ssocolmng -X 4095`[#3]	
			`ssorptd -X 4095`[#3]	
			`ssotrapd -X 4095`[#3]	
			`ssomapstatus -show -all`	
			A list of folders and files in the installation directory	`dir /s` *SSO-installation-folder*
	`jp1ssolog.bat` with the `-col` option specified	In *SSO-installation-folder*`\databases\Coll`		
	`jp1ssolog.bat` with the IP address or host name of the monitoring server specified	Results of executing `ping -n 5` on the specified monitoring server		
NNMi information	Manual	Command execution results		`ovstatus`

#1

The procedure for collecting event logs is described below. Note that the procedures in Windows Server 2008, Windows Server 2008 R2, and either Windows Server 2012 or Windows Server 2012 R2 are different.

To collect event logs (for Windows Server 2008):

1. Select **Control Panel**, **Administrative Tools**, and then **Event Viewer**.
2. Select **Windows Logs**, and then each of **Application**, **Security**, and **System**, and click **Action** and then **Save Events As**, and set **Save as type** to **Text (Tab delimited) (*.txt)** and save the file as the desired name.

To collect event logs (for Windows Server 2008 R2):

1. Select **Control Panel**, **Administrative Tools**, and then **Event Viewer**.

2. Select **Windows Logs**, and then each of **Application**, **Security**, and **System**, and click **Action** and then **Save All Events As**, and set **Save as type** to **Text (Tab delimited) (*.txt)** and save the file as the desired name.

To collect event logs (for Windows Server 2012, and Windows Server 2012 R2):

1. Select **Control Panel**, **Administrative Tools**, and then **Event Viewer**.
2. Select **Windows Logs**, and then each of **Application**, **Security**, and **System**, and click **Action** and then **Save All Events As**, and set **Save as type** to **Text (Tab delimited) (*.txt)** and save the file as the desired name.

#2

Manually collect a problem report when a daemon process stops due to an application error, and a user dump when a command process stops due to an application error.

The following is the procedure for collecting problem reports and user dumps. Note that the method of collecting problem reports is different for Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.

To collect problem reports (for Windows Server 2008):

1. Open the Windows Run dialog box, enter `wercon`, and then click the **OK** button.
   The Problem Reports and Solutions window appears.
2. Click **View problem history** in the left area.
   The problem history list is displayed.
3. Double-click the corresponding problem.
   The details of the problem report are displayed.
4. Click **View a temporary copy of these files**.
   A new window appears. Collect the files displayed in the window.

To collect problem reports (for Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2):

1. Select **Control Panel**, **Action Center**, **Maintenance**, and then **View reliability history**.
   The **Review your computer's reliability and problem history** window appears.
2. Select **View all problem reports** at the bottom.
   The list of problem reports is displayed.
3. Double-click the corresponding problem.
   The details of the problem report are displayed.
4. Click **View a temporary copy of these files**.
   A new window appears. Collect the files displayed in the window.

To collect user dumps:

Perform the following operations while the error dialog box is being displayed.

1. Start the task manager.
2. Click the **Processes** tab in the Windows Task Manager dialog box.
3. Right-click the name of the process that stopped due to an application error and select **Create Dump File**.
   A dialog box indicating the output-destination path of the user dump appears. Collect the files in the output-destination path displayed in the dialog box.

#3

Data cannot be collected when the corresponding daemon process is not running.

Return values

0	Data collection is completed.
1	Part of the data could not be collected, but no problem exists.
4	Data collection failed (incorrect output-destination directory).

Notes

- Execute this command immediately after the failure occurs, if possible. Even if a daemon process terminates abnormally, you must execute the command before restarting the daemon process or SSO.
- If the disk space becomes insufficient while collected data is being saved, the data cannot be saved correctly. When you execute this command, make sure beforehand that the output-destination disk has enough free space. When the `-col` option is not specified, *log-capacity* + *100-megabytes* is required for free space as a rule-of-thumb. When the `-col` option is specified, *log-capacity* + *100-megabytes* + *$SSO_DB-capacity* is required for free space as a rule-of-thumb.
- Do not specify a directory on a shared disk on a network that is not connected to the output-destination directory. If you do so, data collection might fail.

jp1ssolog.sh (UNIX only)

Format

```
jp1ssolog.sh [-col] [-d output-destination-directory-name] [<agent> ...]
```

Function

The jp1ssolog.bat command collects data for an error investigation upon occurrence of an error in SSO. This command is only for UNIX.

This command creates a work directory in the default directory or the directory specified for the -d option. Then, the command creates a JP1SSO directory temporarily in the work directory and outputs data to be collected in the JP1SSO directory created. If a JP1SSO directory already exists, it is deleted and a new JP1SSO directory is created. The default directory is /tmp/jp1sso/work/JP1SSO.

Data that is output in a temporary directory is collectively archived to a file in tar format and the file is compressed by the compress command. However, if the compress command is not included in the standard commands, the file is not compressed. If the file already exists, it is deleted and a new file is created.

The default output destination of the data to be collected is as follows.

When data is compressed:

/tmp/jp1sso/jp1ssolog.tar.Z file

When data is not compressed:

/tmp/jp1sso/jp1ssolog.tar file

If the file is output successfully, all the compression-source data pieces to be temporarily output are deleted. You can change the default output destination by editing this command (a shell script file).

Option

-col

Collects the data in $SSO_DB/Coll as data for an error investigation.

-d *output-destination-directory-name*

Specifies the output destination of the data to be collected by using either a relative or absolute path.

<agent> ...

Collects the results of executing the ping command on the specified monitoring server as data for an error investigation. Specify an IP address or host name for <*agent*>. If the specified IP address or host name is incorrect, or the monitoring server is not running, the return value of the command is a value other than 0.

Customize

This command is a shell script. You can customize the following item:

If you want to change the default output directory

Edit the output destination directory in the following line:

```
OUTPUTDIR="/tmp/jp1sso"
```

Usage example

- To collect data when an error has occurred on monitoring servers `agt1` and `agt2`, execute the following command:

```
jp1ssolog.sh agt1 agt2
```

Collected data list

The following table lists and describes the data for an error investigation to be collected:

Classification	Collection method	Acquired data		
Common information	Manual	An environment configuration chart (OS, IP address, No. of interfaces, and the product configuration and version of each terminal)		
		A memo about how an error occurred (details about the occurrence date/time, OS, host name, IP address, performed operations, and symptoms)		
OS information	`jp1ssolog.sh`	Collected files	`/etc/hosts`	
			`/etc/nsswitch.conf` (when applicable)	
			`/etc/services`	
			`/etc/rc.log` (when applicable)	
			syslog file[#1] (when applicable)	HP-UX: `/var/adm/syslog/syslog.log*`
				Solaris: `/var/adm/messages*`
				Linux: `/var/log/messages*`
			`/core` (when applicable)	
			`/etc/.hitachi/pplistd/pplistd`	
			`/etc/.hitachi/.hitachi.log*`	
		Command execution results	`date`	
			OS version information	HP-UX: `uname -a`
				Solaris: `showrev`
				Linux: `uname -a`
			`ps -elf` (collects data twice at a specific time interval)	
			`hostname`	
			`netstat -a`	
			`netstat -an`	
			`netstat -rn`	
			`netstat -i`	
			`set`	
			`env`	
			Free disk space information	HP-UX: `bdf`

Classification	Collection method	Acquired data		
OS information	jp1ssolog.sh	Command execution results	Free disk space information	Solaris: df -k
				Linux: df -k
			Application patch list	HP-UX: swlist -l patch
				Solaris: patchadd -p
				Linux: rpm -qa -last
			Linux only: /sbin/iptables -L -n	
			Linux only: /sbin/ip6tables -L -n	
SSO information	jp1ssolog.sh	Collected files	In /var/opt/CM2/SSO/log	
			In /etc/opt/CM2/SSO/conf	
			In /etc/opt/CM2/SSO/report	
			/opt/CM2/SSO/uCPSB/CC/web/containers/SSOConsole/logs	
			/opt/CM2/SSO/uCPSB/CC/web/containers/SSOConsole/usrconf	
			/opt/CM2/SSO/uCPSB/CC/web/containers/SSOConsole/work	
			/opt/CM2/SSO/uCPSB/httpsd/conf	
			/opt/CM2/SSO/uCPSB/httpsd/logs	
			Linux and Solaris only: /opt/CM2/SSO/uCPSB/CC/client/logs/system/ejbcl/CJW	
			/opt/CM2/SSO/uCPSB/CC/web/redirector/logs	
			In /var/opt/CM2/SSO/auditlog	
			In /var/opt/CM2/SSO/tmp/ssoclustersetup.log (when applicable)	
		Command execution results	ssostatus	
			ssoapcom -X 4095[#2]	
			ssocollectd -X 4095[#2]	
			ssocolmng -X 4095[#2]	
			ssorprtd -X 4095[#2]	
			ssotrapd -X 4095[#2]	
			ssomapstatus -show -all	
			A list of folders and files in the installation directory	ls -lRaL /opt/CM2/SSO
				ls -lRaL /etc/opt/CM2/SSO
				ls -lRaL /var/opt/CM2/SSO
	jp1ssolog.sh	In /var/opt/CM2/SSO/databases/Coll		

Classification	Collection method	Acquired data	
SSO information	with the `-col` option specified	In `/var/opt/CM2/SSO/databases/Coll`	
	`jp1ssolog.sh` with the IP address or host name of the monitoring server specified	Results of executing `ping -n 5` on the specified monitoring server#3	
NNMi information	Manual	Command execution results	`ovstatus`

#1

If the output destination of the syslog file is not the default, manually collect the syslog file.

#2

Data cannot be collected when the corresponding daemon process is not running.

#3

When the OS is Linux, if the return value of the `ping` command is not `0`, execute the `ping6` command.

Return values

0	Data collection is completed.
1	Part of the data could not be collected, but no problem exists.
2	The executing user has no superuser privileges.
3	System error
4	Data collection failed (incorrect output-destination directory).

Notes

- Execute this command immediately after the failure occurs, if possible. Even if a daemon process terminates abnormally, you must execute the command before restarting the daemon process or SSO.
- If the disk space becomes insufficient while the collected data is being saved, the data cannot be saved correctly. When you execute this command, make sure beforehand that the output-destination disk has enough free space. When the `-col` option is not specified, {*log-capacity* + *100-megabytes*} **x** 2 is required for free space as a rule-of-thumb. When the `-col` option is specified, {*log-capacity* + *100-megabytes* + *$SSO_DB-capacity*} **x** 2 is required for free space as a rule-of-thumb.

ssoapcom

Format

To match the monitoring status between the monitoring manager and the monitoring server:

```
ssoapcom [-S connection-target-server-name] -g monitoring-server-name
```

To execute a demand health check for the monitoring server:

```
ssoapcom [-S connection-target-server-name] -H monitoring-server-name
```

To give the ssoapmon daemon process an order to re-read a definition file:

```
ssoapcom [-S connection-target-server-name] -r
```

To delete process and service monitoring conditions held on the monitoring server:

```
ssoapcom -a monitoring-server-name -s monitoring-manager-name
```

To give the ssoapmon daemon process an order to update the NNMi cooperation information (node information):

```
ssoapcom -n
```

Function

The ssoapcom command matches the monitoring status of a process and service, executes a demand health check, and gives the ssoapmon daemon process orders to re-read a definition file and to update the NNMi cooperation information (node information). Also, the command deletes monitoring conditions remaining on the monitoring server.

Options

-S *connection-target-server-name*

Specifies the connection-target monitoring manager. Specify the connection-target server name by using a host name or an IP address. If this option is not specified, the connection target is SSO on the local host.

-g *monitoring-server-name*

Matches the monitoring status of processes and services with the specified monitoring server. Specify the monitoring server name by using a host name or an IP address.

-H *monitoring-server-name*

Executes a demand health check for the specified monitoring server. Specify the monitoring server name by using a host name or an IP address.

-r

Instructs the ssoapmon daemon process to re-read the following definition files:

- ssoapmon action definition file (ssoapmon.def)
- Event destination definition file (ssodest.conf)
- SNMP definition file (ssosnmp.conf)
- Event filter definition file (ssoevtfilter.conf)

- Action log definition file (`ssoauditlog.conf`)
- TCP agent definition file (`ssotcpagent.conf`)

-a *monitoring-server-name*

Issues a request to the specified monitoring server to stop monitoring processes and services from the SSO specified for the `-s` option. Specify the monitoring server name by using a host name or an IP address.

-s *monitoring-manager-name*

Use this option with the `-a` option. When you change the IP address of the monitoring manager without stopping monitoring processes and services, this option deletes the monitoring conditions set by the monitoring manager (the IP address before the change) that remain on the monitoring server. Specify the IP address before the change for the monitoring manager name. Although the monitoring process on the monitoring server temporarily stops when this command is executed, the process will automatically resume at the next regular health check.

-n

Instructs the `ssoapmon` daemon process to update NNMi cooperation information (node information). Use the `-n` option in either of the following cases:

- When you re-create a node symbol for the monitoring server after the `ssoapmon` daemon process has started
- When you create or re-create a node symbol for the monitoring manager after the `ssoapmon` daemon process has started (However, when you select the node symbol of the monitoring manager and do not use the map cooperation (action cooperation) function, the option is not necessary.)

Return values

0	Normal termination
-1	Execution error such as incorrect arguments
-2	Not executable (because, if you specified the `-H` option, a regular health check is being executed for the specified monitoring server, or if you specified the `-n` option, NNMi cooperation cannot be performed)

Note

When you execute the `ssoapcom -r` command after deleting the line containing a key in the ssoapmon action definition file, the deleted key value is not changed to the default value. To allow the default value of the deleted key to take effect, restart the `ssoapmon` daemon process.

ssoauth

Format

To add or change user information that is used for the SSO authentication method:

```
ssoauth -add -user user-name [-password password]
```

To delete user information that is used for the SSO authentication method:

```
ssoauth -delete -user user-name
```

To output the command usage:

```
ssoauth -h
```

Function

The `ssoauth` command adds, changes, or deletes user information (the user name and its password) when you use SSO authentication for user authentication in the SSO console. User information is stored in the user authentication definition file (`ssoauth.conf`). For details about the user authentication definition file, see *6.3.26 User authentication definition file (ssoauth.conf)*.

If you execute the `ssoauth` command during execution of the following commands, the command terminates abnormally:

`ssobackup`, `ssorestore`, `ssoauth`

Options

-add

Adds or changes user information to be used for SSO authentication.

If you specify a user name that does not exist for the `-user` option, it is added. If you specify a user name that already exists, the existing user information is changed. That is, the password is overwritten.

If you omit the `-password` option, the user is a user without a password.

-delete

Deletes the user information to be used for SSO authentication. If you specify a user name that does not exist for the `-user` option, an error occurs.

-user *user-name*

Specifies a user name to be used for SSO authentication. The user name can have only ASCII characters and must be 1 byte to 32 bytes long.

Note that you cannot use a space, tab, quotation mark (`"`), asterisk (`*`), vertical bar (`|`), less-than sign (<), more-than sign (>), question mark (`?`), comma (`,`), equal sign (=), or hash mark (`#`).

-password *password*

Specifies the user password to be used for SSO authentication. The password can have only ASCII characters and must be 6 bytes to 32 bytes long.

Note that you cannot use a space, tab, quotation mark (`"`), asterisk (`*`), vertical bar (`|`), less-than sign (<), more-than sign (>), question mark (`?`), comma (`,`), equal sign (=), or hash mark (`#`).

-h

Outputs the command usage. This option cannot be specified together with other options.

Return values

0	Normal termination.
-1	Execution error such as incorrect arguments
-2	Execution error that occurred during editing of an SSO authentication user or backup and restore processing

ssobackup

Format

To back up files or databases provided by SSO:

```
ssobackup {-all | -conf | -db} [-d backup-destination-directory]
```

To output the command usage:

```
ssobackup -h
```

Function

The `ssobackup` command backs up SSO files and databases. For details about the backup function, see *2.7.1 Backup function*.

While the `ssobackup` command is being executed, if a daemon process related to the backup target is running, the command interrupts the daemon process. This operation prevents the daemon process from writing to the backup target during backup and secures the integrity of the backup data. The interrupted daemon process automatically resumes after the backup is completed.

The `ssobackup` command backs up files first and databases second. The command can also back up either files or databases. For details about backup targets, see *2.7.3 Backup targets and restore targets*.

If backup data already exists in the backup destination, the command deletes the backup data and then performs the backup.

If you attempt to execute the `ssobackup` command while any of the commands or operations listed below are being executed, or while the status of the daemon process is being changed, the command or operation terminates abnormally. Likewise, if you execute the following commands or operations during execution of the `ssobackup` command, the commands or operations terminate abnormally:

`ssostart`, `ssostop`, `ssobackup`, `ssorestore`, `ssodbdel`, `ssoauth`, `ssonnmsetup`, startup of SSO services, stopping of SSO services, and deletion of databases from the GUI

Options

-all

Specify this option when you back up both files and databases.

-conf

Specify this option when you back up only files.

-db

Specify this option when you back up only databases.

-d *backup-destination-directory*

Specifies the backup destination directory. You can specify a directory name by using either an absolute path or a relative path. If the directory specified for this option does not exist, the command terminates abnormally.

If you do not specify this option, the directory to store backup data is set to `$SSO_BACKUP`.

If you specify this option, a `ssobackup` directory is created in the specified directory, and backup data is stored in the created directory.

You can specify a directory on the local disk or a shared disk connected to the network as the backup-destination directory. Note that if you specify a directory in a shared disk on the network, the backup time depends on the network performance.

-h

Outputs the command usage. This option cannot be specified together with other options.

Return values

0	Normal termination.
-1	Execution error such as incorrect arguments
-2	Execution error occurred during processing of startup or stop, editing of an SSO authentication user, deletion of databases, editing of the NNM information definition file, backup and restore processing, or daemon process status transition.

Notes

The following provides notes on backup operations.

About disk capacity:

The `ssobackup` command checks the amount of data in the backup target and the free space of the backup-destination disk before performing a backup. If the free space of the backup-destination disk is less than the amount of data in the backup target, the backup terminates abnormally. Also, if the free space of the disk becomes insufficient during backup after it is checked, the backup terminates abnormally.

Therefore, when you perform a backup, make sure that the capacity of the backup-destination disk is more than the total of the amount (size on a disk) of each backup-target directory.

To avoid an error termination due to insufficient disk space, provide space for the backup-destination disk, or change the backup-destination to a disk with enough free space and perform the backup again.

About daemon processes and operations:

When you perform a backup, pay attention to the following notes on SSO daemon processes and operations. However, if you forcibly terminate a backup in progress, the following notes do not apply.

Before backup:

You must close windows before backup. If you execute a daemon process from a window during backup without closing the window, no response is returned until the backup is completed.

During backup:

- During backup, all functions provided from daemon processes to be interrupted are interrupted. Interrupted functions automatically resume when the backup is completed. However, during backup of databases, the monitoring function for processes and services is not interrupted.
- You cannot start and stop SSO during backup.
- You cannot execute a restore during backup.
- You cannot delete a collection database during backup.
- You cannot concurrently perform multiple backups.
- If you execute the following commands or connect to SSO from the SSO console during a backup, no response is returned until the backup is completed.

ssoapcom, ssocollectd, ssocolmng, ssocolset, ssocolshow, ssocolstart, ssocolstop, ssodbcheck, ssodemandrpt, ssoextractlog, ssopsset, ssopsshow, ssopsstart, ssopsstop, ssorptd

Forced termination:

If you forcibly terminate a backup in progress, the state of the daemon process might be different before and after the backup. In such a case, use the following procedure to restore the previous state:

1. Execute the command for obtaining the state of daemon processes (ssostatus) to check the state of all daemon processes.
2. If daemon processes in PAUSING status are included in the checked daemon processes, execute the command for stopping daemon processes (ssostop) to stop all the daemon processes that are in PAUSING status. If daemon processes in PAUSING* status are included, wait until the status changes to PAUSING, and if daemon processes in RUNNING* status are included, wait until the status changes to RUNNING.
3. Execute the command for starting daemon processes (ssostart) to start the stopped daemon processes.

User authentication function:

You cannot add and delete a user for SSO authentication during backup.

ssocadel

Format

To delete custom attributes:

```
ssocadel
```

To output the command usage:

```
ssocadel -h
```

Function

The `ssocadel` command deletes all custom attributes registered by SSO on the host on which the command is executed from nodes on the NNMi map view.

If you execute the `ssocadel` command in the following conditions, the command terminates abnormally.

- The SSO service is being started.
- The `ssostart` command is being executed.
- SSO is being started.
- NNMi cooperation failed.
- The `nnm-urlaction-coop:` key was set to `off`.

Option

-h

Outputs the command usage.

Return values

0	Normal termination.
-1	Execution error such as incorrect arguments

Notes

- This command operates when the `nnm-urlaction-coop:` key value in the `ssoapmon` action definition file or the `ssocolmng` action definition file is `on`.
- This command is intended to be executed as post-processing to be performed before uninstallation. Therefore, the command can be executed only when SSO is stopped. If you execute the command while SSO is running, a message is output and the command execution terminates.
- This command retrieves custom attributes registered by the monitoring manager that executes the command from all the nodes which NNMi detects and deletes them. Therefore, the command needs processing time depending on the number of nodes which NNMi detects.

ssoclustersetup.vbs (Windows only)

Format

To configure an SSO cluster system:

(a) When configuring an executing system

```
ssoclustersetup.vbs -construction -primary shared-folder-name logical-IP-address
```

(b) When configuring a standby system

```
ssoclustersetup.vbs -construction -secondary shared-folder-name
```

To maintain an SSO cluster system:

(a) When specifying the pre-maintenance settings

```
ssoclustersetup.vbs -beforemaint {-primary|-secondary} shared-folder-name
```

(b) When specifying the post-maintenance settings

```
ssoclustersetup.vbs -aftermaint {-primary|-secondary} shared-folder-name
```

To release an SSO cluster system:

```
ssoclustersetup.vbs -release {-primary|-secondary} shared-folder-name
```

To configure a JP1 logical host:

(a) When setting up a JP1 logical host

```
ssoclustersetup.vbs -logicalset JP1-logical-host-name
```

(b) When clearing the settings of a JP1 logical host

```
ssoclustersetup.vbs -logicalunset
```

To set up an action definition file:

```
ssoclustersetup.vbs -defset logical-IP-address
```

To output the command usage:

```
ssoclustersetup.vbs -h
```

Function

The `ssoclustersetup.vbs` command configures and releases SSO, specifies the pre-maintenance settings and post-maintenance settings, sets up and clears a logical host in the JP1 authentication method, and sets up action definition files in an SSO cluster environment. This command is only for Windows.

Configuring an SSO cluster environment:

- Configuring an executing SSO cluster environment
- Configuring a standby SSO cluster environment

Specifying the maintenance settings for an SSO cluster environment:

- Specifying the pre-maintenance settings

- Specifying the post-maintenance settings

Releasing an SSO cluster environment:

Release the cluster environment when SSO is uninstalled or SSO operation is switched from the logical host to the physical host.

Setting up or clearing a logical host in the JP1 authentication method:

- Setting up a logical host in the JP1 authentication method
- Clearing the settings of a logical host in the JP1 authentication method

Setting up action definition files:

Set a logical IP address and NNM cooperation policy.

Options

-construction

Specify this option when you configure an SSO cluster environment. Note that a logical IP address to be specified for this option must be an IPv4 address.

-beforemaint

Specify this option when you specify the settings required for maintenance of SSO before maintaining SSO (an overwrite installation, upgrade installation, or application of a patch).

-aftermaint

Specify this option when you specify the settings required for the maintained SSO after maintaining an SSO (an overwrite installation, upgrade installation, or application of a patch).

-release

Specify this option when you release an SSO cluster environment.

-logicalset

Specify this option when you use the JP1 authentication method as the authentication method and perform authentication in JP1/Base on a logical host.

-logicalunset

Specify this option when you clear the authentication method on a logical host in the JP1 authentication method.

-defset

Specify this option when you set or change an IPv4 or IPv6 logical IP address that is set in an action definition file. For details, see the `snmp-address:`, `snmp-address-v6:`, `change-my-address:`, and `default-disp-address:` keys in the action definition file.

-primary

Specify this option when you execute the command in the executing system.

-secondary

Specify this option when you execute the command in the standby system.

shared-folder-name

Specifies an SSO shared folder name on the shared disk.

logical-IP-address

Specifies a logical IP address that SSO uses.

JP1-logical-host-name

Specifies the JP1 logical host name when you use the JP1 authentication method as the authentication method and perform authentication in JP1/Base on a logical host.

-h

Outputs the command usage. This option cannot be specified together with other options.

Return values

0	Normal termination.
1	Execution error such as incorrect arguments

Notes

- You must specify `cscript` at the beginning of the command line to be executed.
- If the current folder of the command prompt in which the command is executed is not `$SSO_BIN`, specify the command by using its full pathname following `cscript`.
- When you execute this command, you must be able to access the shared disk, except in the following cases:
  - When setting up configuration in the standby system
  - When specifying the pre-maintenance settings in the standby system
  - When specifying the post-maintenance settings in the standby system
- If you execute this command with the `-beforemaint` option specified, the SSO service stops. If you execute this command with the `-aftermaint` option specified, the SSO service starts.

ssoclustersetup (UNIX only)

Format

To configure an SSO cluster system:

(a) When configuring an executing system

```
ssoclustersetup -construction -primary shared-directory-name logical-IP-address
```

(b) When configuring a standby system

```
ssoclustersetup -construction -secondary shared-directory-name
```

To maintain an SSO cluster system:

(a) When specifying the pre-maintenance settings

```
ssoclustersetup -beforemaint {-primary|-secondary} shared-directory-name
```

(b) When specifying the post-maintenance settings

```
ssoclustersetup -aftermaint {-primary|-secondary} shared-directory-name
```

To release an SSO cluster system:

```
ssoclustersetup -release {-primary|-secondary} shared-directory-name
```

To configure a JP1 logical host:

(a) When setting up a JP1 logical host

```
ssoclustersetup -logicalset JP1-logical-host-name
```

(b) When clearing the settings of a JP1 logical host

```
ssoclustersetup -logicalunset
```

To set up an action definition file:

```
ssoclustersetup -defset logical-IP-address
```

To output the command usage:

```
ssoclustersetup -h
```

Function

The `ssoclustersetup` command configures and releases SSO, specifies the pre-maintenance settings and post-maintenance settings, sets up and clears a logical host in the JP1 authentication method, and sets up action definition files in an SSO cluster environment. This command is only for UNIX.

Configuring an SSO cluster environment:

- Configuring an executing SSO cluster environment
- Configuring a standby SSO cluster environment

Specifying the maintenance settings for an SSO cluster environment:

- Specifying the pre-maintenance settings

- Specifying the post-maintenance settings

Releasing an SSO cluster environment:

Release the cluster environment when SSO is uninstalled or SSO operation is switched from the logical host to the physical host.

Setting up or clearing a logical host in the JP1 authentication method:

- Setting up a logical host in the JP1 authentication method
- Clearing the settings of a logical host in the JP1 authentication method

Setting up action definition files:

Set a logical IP address and NNM cooperation policy.

Options

-construction

Specify this option when you configure an SSO cluster environment. Note that a logical IP address to be specified for this option must be an IPv4 address.

-beforemaint

Specify this option when you specify the settings required for maintenance of SSO before maintaining SSO (an overwrite installation, upgrade installation, or application of a patch).

-aftermaint

Specify this option when you specify the settings required for a maintained SSO after maintaining an SSO (an overwrite installation, upgrade installation, or application of a patch).

-release

Specify this option when you release an SSO cluster environment.

-logicalset

Specify this option when you use the JP1 authentication method as the authentication method and perform authentication in JP1/Base on a logical host.

-logicalunset

Specify this option when you clear the authentication method on a logical host in the JP1 authentication method.

-defset

Specify this option when you set or change an IPv4 or IPv6 logical IP address that is set in an action definition file. For details, see the `snmp-address:`, `snmp-address-v6:`, `change-my-address:`, and `default-disp-address:` keys in the action definition file.

-primary

Specify this option when you execute the command in the executing system.

-secondary

Specify this option when you execute the command in the standby system.

shared-directory-name

Specifies an SSO shared folder name on the shared disk.

logical-IP-address

Specifies a logical IP address that SSO uses.

JP1-logical-host-name

Specifies the JP1 logical host name when you use the JP1 authentication method as the authentication method and perform authentication in JP1/Base on a logical host.

-h

Outputs the command usage. This option cannot be specified together with other options.

Return values

0	Normal termination
1	Execution error such as incorrect arguments

Notes

- When you execute this command, you must be able to access the shared disk, except in the following cases:
  - When specifying the pre-maintenance settings in the standby system
  - When specifying the post-maintenance settings in the standby system
- If you execute this command with the `-beforemaint` option specified, the SSO service stops. If you execute this command with the `-aftermaint` option specified, the SSO service starts.

ssocolchk

Format

To check the format of the collection conditions definition file:

```
ssocolchk -c collection-conditions-definition-file-name
```

To output the command usage:

```
ssocolchk -h
```

Function

The `ssocolchk` command checks the format of a collection conditions definition file. However, it does not check the correlation (such as duplicate definitions) between fields.

Options

-c *collection-conditions-definition-file*

Specifies the collection conditions definition file whose format you want to check. Specify the collection conditions definition file in 512 bytes or less, including the path name.

For details about collection conditions definition files, see *6.3.1 Collection conditions definition file*.

-h

Outputs the command usage. This option cannot be specified together with other options.

Return values

0	Normal termination
-1	Execution error such as incorrect arguments

ssocolconf

Format

To create a user resource configuration file:

```
ssocolconf {-C | -SJIS | -EUC | -UTF8}
            -s user-resource-definition-file-name
            -o output-destination-directory-name [-r]
```

To output the contents of a user resource configuration file:

```
ssocolconf -p file-name [-g user-resource-configuration-file-name]
```

Function

The `ssocolconf` command analyzes the contents of a user resource definition file and creates a user resource configuration file.

Options

{-C | -SJIS | -EUC | -UTF8}

Specifies the language code in which the user resource definition file was created. Specify an appropriate language code. If a multi-byte code is contained in a definition such as `rsc_label_j` in the user resource definition file, specify the `-SJIS`, `-EUC`, or `-UTF8` option.

-s *user-resource-definition-file-name*

Analyzes the contents of the specified definition file and creates a user resource configuration file. Specify the definition file by its absolute path.

-o *output-destination-directory-name*

Specifies the name of the directory to which you want to output a user resource configuration file. The name of the user resource configuration file to be output is a character string obtained by converting the category name to lower-case characters.

-r

Creates a user resource configuration file in the user resource configuration file storage directory of SSO in addition to the output destination specified for the `-o` option. For details about the user resource configuration file storage directory, see *2.3.2 User resource definition*. The name of the user resource configuration file to be created is a character string obtained by converting the category name to lower-case characters.

-p *file-name*

Creates a user resource definition file from the user resource configuration file contained in the directory that stores the resource settings file for SSO, and outputs it to the specified file.

-g *user-resource-configuration-file-name*

Specifies the file name of the file that you want to read from the user resource configuration file storage directory when you create a user resource definition file. Specify this option together with the `-p` option. If you omit this option, `user` is assumed as the file name.

Return values

0	Normal termination
-1	Execution error such as incorrect arguments

Notes

- If the disk becomes full while the user resource definition file is being output as specified by the `-p` option, only part of the data is saved in the file (no error message is output). Before outputting the user resource definition file to a file, verify that the disk has sufficient free space.
- Specify options in the order of the above descriptions.
- Do not store files other than user resource configuration files in the user resource configuration file storage directory (in UNIX: `$SSO_CONF/rsc`, in Windows: `$SSO_CONF\sso\rsc`). If you store files (such as a user resource definition file or other work files) other than user resource configuration files in the user resource configuration file storage directory, the `ssocolmng` daemon process might incorrectly occupy the CPU or consume memory unnecessarily.
- For details about how to add, change, or delete a user resource definition, see *2.3.2 User resource definition*.

ssocolcvt

Format

To convert to the tab-delimited format:

```
ssocolcvt -s collection-conditions-definition-file -p output-file-name
```

To convert to collection conditions definition file format:

```
ssocolcvt -c text-file-having-tab-delimited-format -p output-file-name
```

To output the command usage:

```
ssocolcvt -h
```

Function

The `ssocolcvt` command converts a collection conditions definition file to a text file having the tab-delimited format. It also converts a text file having the tab-delimited format to data having the collection conditions definition file format. Converting a file to the tab-delimited format makes it possible to manage the collection conditions definition file using spreadsheet software.

Options

-s *collection-conditions-definition-file*

Converts the specified collection conditions definition file to data having the tab-delimited format.

-p *output-file-name*

Specifies the file to which you want to output the conversion result.

-c *text-file-having-tab-delimited-format*

Converts the specified file having the tab-delimited format to a collection conditions definition file.

-h

Outputs the command usage. This option cannot be specified together with other options.

Return values

0	Normal termination
-1	Execution error such as incorrect arguments

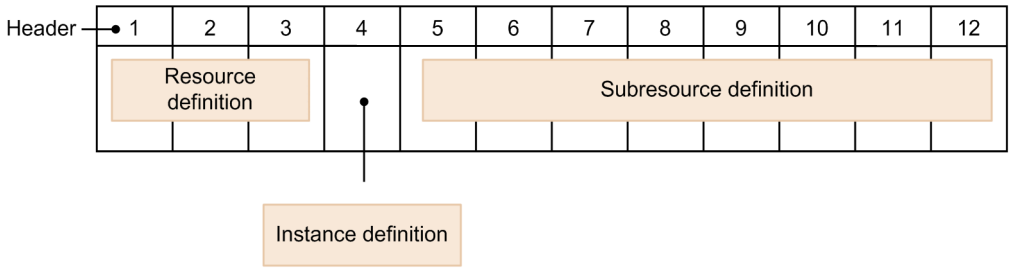
Notes

- When you use the `-c` option to convert a file to the collection conditions definition file format, if the text file having the tab-delimited format contains a control character intended for spreadsheet software, conversion may fail.
- The first line of the tab-delimited format file is ignored because it is treated as a title line.
- If the disk becomes full while the conversion result is being output to a file as specified by the `-p` option, only part of the data is saved in the file (no error message is output). Before outputting the conversion result to a file, verify that the disk has sufficient free space.

- If you have specified a tab in the collection conditions definition, it may not be converted properly to tab-delimited format data.
- You cannot convert definitions related to statistical thresholds by using this command. If you describes a definition related to statistical thresholds in the collection conditions definition file and execute this command, an error occurs.

Example of outputting the tab-delimited format file

The format of the tab-delimited format file is shown below.



The following key names corresponding to numbers are inserted into the header, starting from the left:

```
1:target,2:interval,3:d_range,4:instance,5:subcondition,6:commandUM,
7:commandUK,8:commandNM,9:commandWR,10:commandCR,11:threshold,
12:threshold_OVER
```

The following shows an example of converting the collection conditions definition file, shown in *6.3.1 (5) Examples*, to tab-delimited format data. For more information about key names and their values, see *6.3.1 Collection conditions definition file*.

1	2	3	4	5	6	7	8	9	10	11	12
30; 2o4gsv01	20	06:00:00; 23:00:00	1	Y;Y;Y						90.00; 95.00	1;2
				N;N;N						100.00; 100.00	1;1
			2	Y;Y;Y						95.00; 98.00	2;3
				N;N;N						100.00; 100.00	1;1
32; netmps01	15	07:00:00; 22:00:00		Y;Y;Y				D: \JP1Cm2\SSO \mnr32.bat	D: \JP1Cm2\SSO \crt32.bat	90.00; 98.00	3;5
				N;N;N						100.00; 100.00	1;1
				N;N;N						100.00; 100.00	1;1
				N;N;N						100.00; 100.00	1;1

ssocollectd

Format

To issue an instruction to re-read the definition file:

```
ssocollectd -r
```

Option to be specified in the SSO startup definition file:

```
[-f]
```

Function

The `ssocollectd` command is a daemon process to collect resources. If you execute the daemon process as a command, the definition file is re-read.

Options

-f

Prevents the collection status from being `Impossibility`. If you specify the `-f` option, the collection status does not transition to `Impossibility`. If you do not specify the `-f` option, the collection status will transition to `Impossibility`. For details about the transition of the collection status, see *2.2.2 Resource collection function*. You can specify this option only in the SSO startup definition file. Also, you must match whether to specify this option with the setting of the `ssocolmng` daemon process.

-r

Re-reads the `ssocollectd` action definition file (`ssocollectd.def`) and SNMP configuration file (`ssosnmp.conf`). If you specify this option, execute the command from the command line. Do not specify this option in the SSO startup definition file (`ssostartup.conf`).

Return values

The return values for the `-r` option is as follows.

0	Normal termination
-1	Execution error

ssocolmng

Format

To issue an instruction to re-read the definition file:

```
ssocolmng -r
```

Option to be specified in the SSO startup definition file:

```
[-f]
```

To issue an instruction to update the NNMi cooperation information (node information):

```
ssocolmng -n
```

Function

The ssocolmng command is a daemon process to manage the collected resource data. If you execute the daemon process as a command, the definition file is re-read and the NNMi cooperation information (node information) is updated.

Options

-f

Prevents the collection status from being Impossibility. If you specify the -f option, the collection status does not transition to Impossibility. If you do not specify the -f option, the collection status will transition to Impossibility. For details about the transition of the collection status, see *2.2.2 Resource collection function*. You can specify this option only in the SSO startup definition file. Also, you must match whether to specify this option with the setting of the ssocollectd daemon process. For details about the SSO startup definition file, see *6.3.24 SSO startup definition file (ssostartup.conf)*.

-r

Re-reads the ssocolmng action definition file (ssocolmng.def), action log definition file (ssoauditlog.conf), event filter definition file (ssoevtfilter.conf), and event destination definition file (ssodest.conf). If you specify this option, execute the command from the command line. Do not specify this option in the SSO startup definition file (ssostartup.conf).

-n

Updates the NNMi cooperation information (node information). User this option in either of the following cases:

- When you re-create a node symbol for the monitoring server after the ssocolmng daemon process has started
- When you create or re-create a node symbol for the monitoring manager after the ssocolmng daemon process has started (However, if you select the node symbol of the monitoring manager and do not use the map cooperation (action cooperation) function, the option is not necessary.)

If you specify this option, execute the command from the command line for a resource collection process that is running. Do not specify this option in the SSO startup definition file (ssostartup.conf).

Return values

The return values for the -r option or the -n option is as follows.

0	Normal termination
-1	Execution error.
-2	NNMi cooperation cannot be performed (if you specified the `-n` option).

ssocolset

Format

To add or change a collection condition:

```
ssocolset [-S connection-destination-server-name]
          {-s collection-conditions-definition-file-name
          | -sn collection-conditions-definition-file-name}
```

To delete all collection conditions:

```
ssocolset [-S connection-destination-server-name] -d
```

To partially delete collection conditions:

(a) When you specify a server (either -ds or -dsf is needed)

```
ssocolset [-S connection-destination-server-name]
          {-ds server-name,... | -dsf group-definition-file, group-name}
          [-dr resource-ID,...
          | -drf group-definition-file, group-name]
```

(b) When you specify a resource (either -dr or -drf is needed)

```
ssocolset [-S connection-destination-server-name]
          [-ds server-name,... | -dsf group-definition-file, group-name]
          {-dr resource-ID,...
          | -drf group-definition-file, group-name}
```

To output collection conditions to a file:

```
ssocolset [-S connection-destination-server-name] -p output-file-name
```

To output the command usage:

```
ssocolset -h
```

Function

The ssocolset command adds, changes, or deletes the collection conditions for a resource. When it adds or changes collection conditions, it updates the collection conditions configuration file with the contents of the created collection conditions definition file.

Options

-S *connection-destination-server-name*

Specifies the server name of the monitoring manager whose collection conditions are to be changed. Specify the host name or IP address in 255 bytes or less. If you omit this option, the command changes the collection conditions for the server on which you execute the command.

-s *collection-conditions-definition-file-name*

Completely changes the collection conditions configuration file to the contents of the specified collection conditions definition file.

If an item defined in the collection conditions definition file exists in the collection conditions configuration file, the command replaces the set value. It also deletes from the collection conditions configuration file any item that is not defined in the collection conditions definition file.

Specify the collection conditions definition file name in 512 bytes or less, including the path name.

-sn *collection-conditions-definition-file-name*

Changes the collection conditions to the contents defined in the file specified in the collection conditions definition file name.

If an item defined in the collection conditions definition file exists in the collection conditions configuration file, the command replaces the set value. It retains the contents of the collection conditions configuration file for any items not defined in the collection conditions definition file.

Specify the collection conditions definition file name in 512 bytes or less, including the path name.

-d

Deletes all collection conditions contained in the collection conditions configuration file.

-ds *server-name*,...

Deletes only the collection conditions for the specified server. To specify multiple server names, delimit the names with a comma (`,`).

You can specify this option together with the `-dr` or `-drf` option. If you do not specify the `-dr` or `-drf` option, the command deletes the collection conditions for all resources of the specified server.

-dsf *group-definition-file*, *group-name*

Deletes only the collection conditions for the servers defined in the specified group.

You can specify this option together with the `-dr` or `-drf` option. If you do not specify the `-dr` or `-drf` option, the command deletes the collection conditions for all resources of the servers.

Specify the group definition file in 512 bytes or less, including the path name. For details about group definition files, see *6.3.5 Group definition file*.

-dr *resource-ID*,...

Deletes only the collection conditions for the specified resource. To specify multiple resource IDs, delimit the IDs with a comma (`,`).

You can specify this option together with the `-ds` or `-dsf` option. If you do not specify the `-ds` or `-dsf` option, the command deletes the collection conditions for the specified resource from the collection conditions for all servers set in the collection conditions configuration file.

For details about resource IDs, see *E. Resource IDs*.

-drf *group-definition-file, group-name*

Deletes only the collection conditions for the resources defined in the specified group.

You can specify this option together with the `-ds` or `-dsf` option. If you do not specify the `-ds` or `-dsf` option, the command deletes the collection conditions for the resource IDs defined in the group from the collection conditions for all servers set in the collection conditions configuration file.

Specify the group definition file in 512 bytes or less, including the path name. For details about group definition files, see *6.3.5 Group definition file*. For details about resource IDs, see *E. Resource IDs*.

-p *output-file-name*

Outputs the collection conditions contained in the collection conditions configuration file to the specified file. Specify the output file name in 512 bytes or less, including the path name.

-h

Outputs the command usage. This option cannot be specified together with other options.

Examples

- The following example changes the collection conditions for a server (`vr260`) to the contents of `/tmp/ssocol.conf`:

```
ssocolset -S vr260 -s /tmp/ssocol.conf
```

- The following example deletes all collection conditions for a server (`vr260`):

```
ssocolset -S vr260 -d
```

- The following example deletes collection conditions for resource IDs `1`, `2`, and `4` set for the server's `netmda11` and `netmda22` from the collection conditions for a server (`vr260`):

```
ssocolset -S vr260 -ds netmda11,netmda22 -dr 1,2,4
```

Return values

0	Normal termination. If the `-s` option was specified and the definition file contains an invalid definition, the command outputs a message to the standard output.
-1	Execution error such as incorrect arguments

Notes

- You cannot execute this command while the Resource Configuration window is active. Furthermore, you cannot activate the Resource Configuration window while this command is executing.
- If you execute this command, do not cancel it before processing finishes.
- You cannot change a collection period definition contained in a collection conditions definition file for a resource whose collection status is `Collecting`, `Postponing`, or `Standing By`.
- If the disk becomes full while the collection conditions are being output as specified by the `-p` option, only part of the data is saved in the file (no error message is output). Before outputting the collection conditions to a file, verify that the disk has sufficient free space.
- Suppose that when collecting a resource, you specify the *Ping response time* resource in the Network resource group as a collection target. In such a case, you cannot add or change the collection conditions in a collection conditions definition file that contains an instance name of the collection target that is not specified by using the `ssocolset` command.

ssocolshow

Format

To browse the resource collection or monitoring status:

```
ssocolshow [-S connection-destination-server-name]
           [-s server-name,... | -sf group-definition-file, group-name]
           [-r resource-ID,... | -rf group-definition-file, group-name]
           [-stime collection-start-date, time]
```

To generate a monitoring status definition file:

```
ssocolshow [-S connection-destination-server-name]
           [-s server-name,... | -sf group-definition file, group-name]
           [-r resource-ID,... | -rf group-definition file, group-name]
           [-stime collection-start-date, time]
           -p collection-status-definition-file-name
```

To output the command usage:

```
ssocolshow -h
```

Function

The `ssocolshow` command displays the resource threshold monitoring status and the resource collection status. This command also generates the collection status definition file.

Options

-S *connection-destination-server-name*

Specify the monitoring manager for which you want to display the collection status and generate the collection status definition file. Specify the connection destination server name as a host name or IP address in 255 bytes or less. If you do not specify this option, the local host will be the connection destination.

-s *server-name*

Displays the collection status for the monitoring server specified by the server name from the collection status managed by the connection destination SSO. The command does nothing if the specified server is not contained in the management information. Specify the server name as a host name or IP address in 255 bytes or less. To specify multiple server names, delimit them with a comma (,).

You can specify this option together with the `-r` or `-rf` option.

-sf *group-definition-file-name, group-name*

Displays the collection status for the server defined in the group specified in the group definition file, from the collection statuses managed by the connection destination SSO. The command does nothing if the expanded server is not contained in the management information. Specify the group definition file name, including the path name, in 512 bytes or less. Specify the group name in 20 bytes or less.

You can specify this option together with the `-r` or `-rf` option.

For details on how to define the group definition file, see *6.3.5 Group definition file*.

-r *resource-ID,...*

Displays the collection conditions for the resource having the specified resource ID from the monitoring status (management information) managed by the connection destination SSO. The command does nothing if the resource having the specified resource ID is not contained in the management information. To specify multiple resource IDs, delimit them with a comma (,).

You can specify this option together with the `-s` or `-sf` option.

For details on the resource ID and resource correspondence, see *E. Resource IDs*.

-rf *group-definition-file-name, group-name*

Displays the collection conditions for the resource having the resource ID defined in the group specified in the group definition file from the collection conditions (management information) managed by the connection destination SSO. The command does nothing if the resource having the expanded resource ID is not contained in the management information. Specify the group definition file name, including the path name, in 512 bytes or less. Specify the group name in 20 bytes or less.

You can specify this option together with the `-s` or `-sf` option.

For details on how to define the group definition files, see *6.3.5 Group definition file*.

-stime *collection-start-time*

Of information items being collected at the connection destination SSO, this option displays only those items whose collection has begun at the time specified in this option. Specify the collection start time in the *yyyy.mm.dd.hh.mm.ss* format. The specifiable range is January 1, 1980 00:00:00 to December 31, 2029 23:59:59.

-p *resource-collection-condition-definition-file-name*

Specify the name of the resource collection condition definition file, you want to generate. Specify the file name, including the path, in 512 bytes or less.

-h

Outputs command usage. You cannot specify this option together with other options.

Return values

0	Normal termination.
-1	Execution error such as incorrect arguments

Note

When you use this command to browse the resource collection or monitoring status, in the following cases, the display of an instance name is `unknown`.

- When you collect resources for all instances and cannot acquire resource values even once after the collection starts
- When threshold monitoring is disabled for all instances and subresources

ssocolstart

Format

To start collection based on all collection conditions:

```
ssocolstart [-S connection-destination-server-name] -all
            [-stime collection-start-time]
            [-ptime collection-end-time | -period collection-period]
```

To specify a server or resource and start collection:

(a) When you specify a server (either `-s` or `-sf` is needed)

```
ssocolstart [-S conection-destination-server-name]
            {-s server-name,...
            |-sf group-definition-file-name,group-name}
            [-r resource-ID,...
            | -rf group-definition-file-name,group-name]
            [-stime collection-start-time]
            [-ptime collection-end-time | -period collection-period]
```

(b) When you specify a resource (either `-r` or `-rf` is needed)

```
ssocolstart [-S conection-destination-server-name]
            [-s server-name,...
            | -sf group-definition-file-name,group-name]
            {-r resource-ID,...
            | -rf group-definition-file-name,group-name}
            [-stime collection-start-time]
            [-ptime collection-end-time | -period collection-period]
```

To specify the name of a collection status definition file and start collection:

```
ssocolstart [-S connection-destination-server-name]
               -i collection-status-definition-file
```

To output the command usage:

```
ssocolstart -h
```

Function

The `ssocolstart` command starts collection of resources.

This command is effective for collection conditions whose collection status is `Deferred`, `Completed`, `Impossibile`, or `SNMP error`. It is ineffective for collection conditions having any other collection status.

Options

-S *connection-destination-server-name*

Specifies the monitoring manager on which you want to start collection. Specify the host name or IP address in 255 bytes or less. If you omit this option, the command starts collection on the server on which you executed the command.

-all

Starts collection of all the collection conditions set in the collection condition configuration file.

-stime *collection-start-time*

Specifies the date and time at which to start collection in the format *yyyy.mm.dd.hh.mm.ss*. The specifiable range is January 1, 1980 00:00:00 to December 31, 2029 23:59:59. If you omit this option or if the specified collection start time has passed, collection starts at the time the command is executed.

-ptime *collection-end-time*

Specifies the date and time at which to end collection in the format *yyyy.mm.dd.hh.mm.ss*. The specifiable range is January 1, 1980 00:00:00 to December 31, 2029 23:59:59. If you specify this option together with the `-stime` option to set collection dates and times, specify a later date and time than the start date and time. If you omit the `-ptime` and `-period` options, the command collects resources indefinitely. You cannot specify this option together with the `-period` option.

-period *collection-period*

Specifies the resource collection end time by using time elapsed from the collection start time. Specify the collection period in one of days, hours, and minutes. The unit is *d* (days), *h* (hours), and *m* (minutes). You can specify a period not longer than 31 days. The default unit of time is *m* (minutes). If you omit the `-period` and `-ptime` options, the command collects resources indefinitely. You cannot specify this option together with the `-ptime` option.

-s *server-name*,...

Starts collection on the specified server. Specify the host name or IP address in 255 bytes or less. If the collection conditions configuration file contains no collection conditions for the specified server, the command takes no action. To specify multiple server names, delimit the names with a comma (`,`).

You can specify this option together with the `-r` or `-rf` option. If you do not specify the `-r` or `-rf` option, the command starts collection of all resources of the specified server.

-sf *group-definition-file-name*, *group-name*

Starts collection on the servers defined in the specified group. If the collection conditions configuration file contains no collection conditions for the defined servers, the command takes no action.

You can specify this option together with the `-r` or `-rf` option. If you do not specify the `-r` or `-rf` option, the command starts collection of all resources of the servers defined in the group.

Specify the group definition file in 512 bytes or less, including the path name. For details about group definition files, see *6.3.5 Group definition file*.

-r *resource-ID*,...

Starts collection of the resource having the specified resource ID. If the collection conditions configuration file contains no collection conditions for the specified resource ID, the command takes no action. To specify multiple resource IDs, delimit the IDs with a comma (`,`).

You can specify this option together with the `-s` or `-sf` option. If you do not specify the `-s` or `-sf` option, the command starts collection of the specified resource on all servers set in the collection conditions configuration file.

For details about the correspondence between resource IDs and resources, see *E. Resource IDs*.

-rf *group-definition-file-name*, *group-name*

Starts collection of the resources defined in the specified group. If the collection conditions configuration file contains no collection conditions for the defined resource IDs, the command takes no action.

You can specify this option together with the -s or -sf option. If you do not specify the -s or -sf option, the command starts collection of the resources defined in the group on all servers set in the collection conditions configuration file.

Specify the group definition file in 512 bytes or less, including the path name. For details about group definition files, see *6.3.5 Group definition file*.

-i *collection-status-definition-file-name*

Reads the collection status definition file specified in this option, and then starts collection as specified in the file.

For details on how to define the collection status definition file, see *6.3.17 Collecting condition definition file*.

-h

Outputs the command usage. This option cannot be specified together with other options.

Examples

- The following example starts collection based on all set collection conditions on a server (vr260):

```
ssocolstart -S vr260 -all
```

- The following example starts collection of resource IDs 1 and 2 from the set collection conditions on a server (vr260):

```
ssocolstart -S vr260 -r 1,2
```

- The following example starts collection of the group RSC contained in a group definition file (/tmp/file.grp) from the set collection conditions on a server (vr260):

```
ssocolstart -S vr260 -rf /tmp/file.grp,RSC
```

- The following example starts collection according to the collection status definition file name (/tmp/file.col) from the set collection conditions on a server (vr260):

```
ssocolstart -S vr260 -i /tmp/file.col
```

Return values

0	Normal termination
-1	Execution error such as incorrect arguments

Note

If you execute this command, do not cancel it before processing finishes.

ssocolstop

Format

To stop collection based on all collection condition:

```
ssocolstop [-S connection-destination-server-name] -all
```

To specify a server or resource and stop collection:

(a) When you specify a server (either `-s` or `-sf` is needed)

```
ssocolstop [-S connection-destination-server-name]
           {-s server-name,...
           | -sf group-definition-file-name,group-name}
           [-r resource-ID,... | -rf group-definition-file-name,group-
name]
```

(b) When you specify a resource (either `-r` or `-rf` is needed)

```
ssocolstop [-S connection-destination-server-name]
           [-s server-name,... | -sf group-definition-file-name,group-
name]
           {-r resource-ID,... | -rf group-definition-file-name,group-
name}
```

To specify the name of a collection status definition file and stop collection:

```
ssocolstop [-S connection-destination-server-name]
           -i collection-status-definition-file-name
```

To output the command usage:

```
ssocolstop -h
```

Function

The `ssocolstop` command stops collection of resources.

This command is effective for collection conditions whose collection status is `Collecting`, `Standing By`, or `Postponing`. It is ineffective for collection conditions having any other collection status.

Options

-S *connection-destination-server-name*

Specifies the monitoring manager on which you want to stop collection. Specify the host name or IP address in 255 bytes or less. If you omit this option, the command stops collection on the server on which you executed the command.

-all

Stops collection based on all collection conditions in the collection conditions configuration file.

-s *server-name*,...

Stops collection on the specified server. Specify the host name or IP address in 255 bytes or less. If the collection conditions configuration file contains no collection conditions for the specified server, the command takes no action. To specify multiple server names, delimit the names with a comma (`,`).

You can specify this option together with the -r or -rf option. If you do not specify the -r or -rf option, the command stops collection of all resources of the specified server.

-sf *group-definition-file-name, group-name*

Stops collection on the servers defined in the specified group. If the collection conditions configuration file contains no collection conditions for the defined servers, the command takes no action.

You can specify this option together with the -r or -rf option. If you do not specify the -r or -rf option, the command stops collection of all resources of the servers defined in the group.

Specify the group definition file in 512 bytes or less, including the path name. For details about group definition files, see *6.3.5 Group definition file*.

-r *resource-ID,...*

Stops collection of the resource having the specified resource ID. If the collection conditions configuration file contains no collection conditions for the specified resource ID, the command takes no action. To specify multiple resource IDs, delimit the IDs with a comma (,).

You can specify this option together with the -s or -sf option. If you do not specify the -s or -sf option, the command stops collection of the specified resource on all servers set in the collection conditions configuration file.

For details about resource IDs, see *E. Resource IDs*.

-rf *group-definition-file-name,group-name*

Stops collection of the resources defined in the specified group. If the collection conditions configuration file contains no collection conditions for the defined resource IDs, the command takes no action.

You can specify this option together with the -s or -sf option. If you do not specify the -s or -sf option, the command stops collection of the resources defined in the group on all servers set in the collection conditions configuration file.

Specify the group definition file in 512 bytes or less, including the path name. For details about group definition files, see *6.3.5 Group definition file*.

-i *collection-status-definition-file-name*

Reads the collection status definition file specified in this option, and then stops collection as specified in the file.

For details on how to define the collection definition file, see *6.3.17 Collecting condition definition file*.

Collection start time, collection end time, and collection period settings for the collection status definition file are ignored.

-h

Outputs the command usage. This option cannot be specified together with other options.

Examples

- The following command stops collection based on all set collection conditions on a server (vr260):

```
ssocolstop -S vr260 -all
```

- The following command stops collection of resource IDs 1 and 2 from the set collection conditions on a server (vr260):

```
ssocolstop -S vr260 -r 1,2
```

- The following command stops collection of the group RSC contained in a group definition file (/tmp/file.grp) from the set collection conditions on a server (vr260):

```
ssocolstop -S vr260 -rf /tmp/file.grp,RSC
```

- The following example stops collection according to the collection status definition file (/tmp/file.col) from the set collection conditions on a server (vr260):

```
ssocolstop -S vr260 -i /tmp/file.col
```

Return values

0	Normal termination
-1	Execution error such as incorrect arguments

Note

If you execute this command, do not cancel it before processing finishes.

ssocolverify

Format

To verify a threshold:

```
ssocolverify -i threshold-verification-definition-file
              -r collection-data-extraction-file
             [-o output-file-name] [-l]
```

To output the command usage:

```
ssocolverify -h
```

Function

The `ssocolverify` command verifies the validity of thresholds defined by the resource monitoring function. Write the verification method and parameters for verification in the threshold verification definition file and specify the file as an entry for the command.

Options

-i *threshold-verification-definition-file*

Write information required for verification in the threshold verification definition file beforehand, and specify the file name as the argument of this option. You must specify the threshold verification definition file.

-o *output-file-name*

Specify this option when you execute the command to specify the file output destination and the output file name. The output results are transformed into an easy-to-understand format and output. Specify a file name that is not longer than 512 bytes including the path. Note that if you omit this option, the output result is displayed as in the standard output.

-l

Specify this option when you want to add the detailed verification information to the verification results to be output. The detailed information consists of the time when the status (*Normal*, *Warning*, or *Critical*) of an individual subresource changes. Note that you can specify this option only for execution from the command.

-r *collection-data-extraction-file*

Specifies the name of a file that contains data extracted from the collection database. The file must be a file generated by the `ssoextractlog` command with the `F` option. If you do not specify such a file, you cannot verify thresholds. The maximum length of a specifiable file name is 255 bytes including the path.

-h

Outputs the command usage. This option cannot be specified together with other options.

Return values

0	Normal termination
-1	Execution error such as incorrect arguments

ssoconsoled

Format

To issue an instruction to re-read the definition file:

```
ssoconsoled -r
```

Function

The `ssoconsoled` command is a daemon process to execute the SSO console. If you execute the daemon process as a command, the definition file is re-read.

Option

-r

Re-reads the `ssoconsoled` action definition file (`ssoconsoled.def`). Do not specify this option in the SSO startup definition file (`ssostartup.conf`).

Return values

0	Normal termination
-1	Execution error such as incorrect arguments

ssodbcheck

Format

To output the size of a collection database:

```
ssodbcheck [-S connection-destination-server-name] -col [-list]
```

To check the size of a collection database by a threshold:

```
ssodbcheck [-S connection-destination-server-name] -col
           [-th threshold [-event ["text"]]]
```

Functions

The `ssodbcheck` command outputs the size of a collection database and checks the size by a threshold. It checks the threshold set for the size of the collection database, and can issue an incident if the size exceeds the specified size.

Options

-S *connection-destination-server-name*

Specifies the monitoring manager for which you want to check the size of the collection database. Specify the host name or IP address in 255 bytes or less. If you do not specify this option, the connection target is assumed as the local host.

-col

Checks the size of the collection database.

If you specify only this option, the command outputs the size of the collection database to the standard output.

The unit is kilobytes.

-list

Outputs for each subresource the size of the collection database to the standard output.

-th *threshold*

Specifies a threshold for the size of the collection database. Specify an `unsigned long` value within the range 0 to 4,294,967,295 (kilobytes). If the threshold is exceeded, the command returns a value of 1.

-event ["*text*"]

Issues an event if the size of the collection database has exceeded the threshold. To specify this option, you must have specified the `-th` option.

This argument allows you to specify text to be displayed as a message. Specify the text in 255 bytes or less.

Examples

0	Normal termination
1	Normal termination (If the `-th` option was specified, the threshold was exceeded.)
-1	Execution error such as incorrect arguments

ssodbdel

Format

To delete all databases:

```
ssodbdel [-S connection-destination-server-name] [-st]
         -all
         [-start {DATE date-and-time | BDATE date
          | BMONTH month[,date]}]
         [-stop {DATE date-and-time | BDATE date
          | BMONTH month[,date]}]
```

To specify and delete a database:

```
ssodbdel [-S connection-destination-server-name]
         -dbname resource-ID,database-name
         [-start {DATE date-and-time | BDATE date
          | BMONTH month[,date]}]
         [-stop {DATE date-and-time | BDATE date
          | BMONTH month[,date]}]
```

To specify and delete a resource:

```
ssodbdel [-S connection-destination-server-name] [-st]
         {-r resource-ID,... | -rf group-definition-file,group-name}
         [-s server-name,... | -sf group-definition-file,group-name]
         [-start {DATE date-and-time | BDATE date
          | BMONTH month[,date]}]
         [-stop {DATE date-and-time | BDATE date
          | BMONTH month[,date]}]
```

To specify and delete a server:

```
ssodbdel [-S connection-destination-server-name] [-st]
         [-r resource-ID,... | -rf group-definition-file,group-name]
         {-s server-name,... | -sf group-definition-file,group-name}
         [-start {DATE date-and-time | BDATE date
          | BMONTH month[,date]}]
         [-stop {DATE date-and-time | BDATE date
          | BMONTH month[,date]}]
```

Function

The `ssodbdel` command deletes a collection database or statistics information database.

Options

-S *connection-destination-server-name*

Specifies the monitoring manager whose collection database or statistics information database you want to delete. Specify the host name or IP address in 255 bytes or less. If you omit this option, the command deletes the collection database or statistics information database of the server on which you executed the command.

-st

Deletes the statistics information database. The collection database is not deleted. If you omit this option, only the collection database is deleted.

-all

Deletes all the master databases and copy databases on the connection-destination server, or deletes the statistics information database.

-start {DATE *date-and-time* | BDATE *date* | BMONTH *month*[,*date*]}

Specifies the range of data to be deleted.

DATE *date-and-time*

Starts deletion at the collected data or statistics data for the specified date and time.

Specify the date and time in the format *yyyy.mm.dd.hh.mm.ss*. The specifiable range is January 1, 1980 00:00:00 to December 31, 2029 23:59:59.

BDATE *date*

Starts deletion at data for 00:00:00 on the date preceeding the current date by the specified number of days. Specify the number of days preceeding the date on which the command is executed.

The specifiable range is 0 to 30 (days). If you specify `0`, the command deletes data starting with data for 00:00:00 on the date the command is executed.

BMONTH *month*[,*date*]

Starts deletion at data for 00:00:00 on the specified date of the month preceeding the current month by the specified number of months.

The specifiable range for the month is 0 to 13 (months). The specifiable range for the date is 1 to 31 (date).

If you specify `0` for the month, the command deletes data for the month in which you executed the command.

If you do not specify *date*, the command deletes data from the first day of the month.

-stop {DATE *date-and-time* | BDATE *date* | BMONTH *month*[,*date*]}

Specifies the range of data to be deleted.

DATE *date-and-time*

Deletes collected data or statistics data up to the specified date and time.

Specify the date and time in the format *yyyy.mm.dd.hh.mm.ss*. The specifiable range is January 1, 1980 00:00:00 to December 31, 2029 23:59:59.

BDATE *date*

Deletes data up to 23:59:59 on the date preceeding the current date by the specified number of days.

The specifiable range is 0 to 30 (days). If you specify `0`, the command deletes data up to 23:59:59 on the date the command is executed.

BMONTH *month*[,*date*]

Deletes data up to 23:59:59 on the specified date of the month preceeding the current month by the specified number of months.

The specifiable range for the month is 0 to 13 (months). The specifiable range for the date is 1 to 31 (date). If you specify `0` for the month, the command deletes data up to the month in which you executed the command.

If you do not specify *date*, the command deletes data up to 23:59:59 on the last day of the month.

-dbname *resource-ID,collection-database-name*

Deletes the specified database. Verify the resource ID and database name by using the `-list` option in the `ssoextractlog` command.

-r *resource-ID,...*

Deletes the master database and copy database of the specified resource, or deletes the statistics information database. To specify multiple resource IDs, delimit the IDs with a comma (`,`).

You can specify this option together with the `-s` or `-sf` option. If you do not specify these options, all the collection databases or statistics information databases stored in the resource directory of the specified resource are deleted.

For details about resource IDs, see *E. Resource IDs*.

-rf *group-definition-file-name,group-name*

Deletes the master database and copy database of the resource defined in the specified group, or deletes the statistics information database.

You can specify this option together with the `-s` or `-sf` option. If you do not specify these options, all the collection databases or statistics information databases stored in the resource directory of the resource defined in the specified group are deleted.

Specify the group definition file in 512 bytes or less, including the path name.

For details about group definition files, see *6.3.5 Group definition file*.

-s *server-name,...*

Deletes the master database and copy database for the specified monitoring server, or deletes the statistics information database. Specify the host name or IP address in 255 bytes or less. To specify multiple server names, delimit the names with a comma (`,`).

You can specify this option together with the `-r, -rf` option or `-c, -cf` option. If you are not specify these options all collection databases or statistics information database at the specified server will be deleted.

-sf *group-definition-file-name,group-name*

Deletes the master database and copy database for the server defined in the specified group, or deletes the statistics information database.

You can specify this option together with the `-r, -rf` option or `-c, -cf` option. If you do not specify these options, all the collection databases or statistics information databases of the server defined in the specified group are deleted.

Specify the group definition file in 512 bytes or less, including the path name.

For details about group definition files, see *6.3.5 Group definition file*.

Examples

- The following example deletes all the collection databases of the monitoring manager (local host):

```
ssodbdel -all
```

- The following example deletes all the collection data of monitoring servers `netmda01` and `netmda02` from the collection database of the monitoring manager (local host name: `netmds02`) on another host:

```
ssodbdel -S netmds02 -s netmda01,netmda02
```

- The following example deletes collection data whose resource ID is 1, 2, or 12 from the collection databases of the monitoring manager (local host):

```
ssodbdel -r 1,2,12
```

- The following example deletes collection data that was collected until 23:59:59 on March 31, 2009 from the collection databases of the monitoring manager (local host):

```
ssodbdel -all -stop DATE 2009.03.31.23.59.59
```

- The following example deletes all the data of the previous day from the specified server (vr260):

```
ssodbdel -S vr260 -all -start BDATE 1 -stop BDATE 1
```

- The following example deletes all the data of the previous week (Monday to Friday) from the specified server (vr260) on the current day (Monday):

```
ssodbdel -S vr260 -all -start BDATE 7 -stop BDATE 3
```

- The following example deletes all the data of the previous month from the specified server (vr260):

```
ssodbdel -S vr260 -all -start BMONTH 1 -stop BMONTH 1
```

- The following example deletes all the data over 1 year ago from the specified server (vr260):

```
ssodbdel -S vr260 -all -stop BMONTH 13
```

Return values

0	Normal termination
-1	Execution error such as incorrect arguments

Notes

- This command also deletes databases of resources currently being collected and databases of resources currently being displayed on a GUI.
- If the file system of the collection database has insufficient free space (the free space is less than the maximum size of the data file of the collection database), delete all data without using the -stop option or the -start option to specify a period.

  Check the value displayed in Size which the ssoextractlog -list command outputs as standard or Size (KBytes) in the collection data list in the Resource Data Reference window to obtain the size of the data file of a collection database. For details about the ssoextractlog command, see *ssoextractlog*. For details about the Resource Data Reference window, see *4.5 Resource Data Reference window*.
- Notes on concurrently executing the ssodbdel command and the ssoextractlog command

  Do not concurrently execute the ssodbdel command and the ssoextractlog command (during execution of one of the commands, you try to execute the other command). If these commands are concurrently executed, the ssoextractlog command outputs the following error message, and the processing might be interrupted if data extraction and copy are incomplete.

  In such a case, after the ssodbdel command is completed, re-execute the ssoextractlog command.

  ```
  The applicable database does not exist. Extraction of the collection database failed.
  ```

- Partial deletion of data by this command takes time in proportion to the size of the collection database. Therefore, make sure that you regularly delete collection data (either by deleting all data or by deleting part of the data by specifying a time period).
- Do not execute the following commands and GUI operations during execution of the `ssodbdel` command.

  Command

  - `ssoextractlog` command
  - `ssodbdel` command
  - `ssobackup` command

  GUI operations

  - Reference to resource data from the Resource Data Reference window
  - Extraction from the Save file window to a file
  - Copy of collection data from the Copy Collection Data window
  - Deletion of collection data from the Delete Collection Data window

ssodemandrpt

Format

To create a report:

```
ssodemandrpt -def report-definition-file-name
             -savefile report-file-name
             [-title report-title]
             [-type {CSV | HTML | HTMLSVG}]
             [-start {DATE date-and-time
              | BDATE date | BMONTH month[,date]}]
             [-stop  {DATE date-and-time | BDATE date
              | BMONTH month[,date]}]
```

To output the command usage:

```
ssodemandrpt -h
```

Function

The `ssodemandrpt` command extracts data from a collection database and creates a report in either HTML or CSV format.

Options

-def *report-definition-file-name*

Specifies a report definition file. Specify the report definition file name in 255 bytes or less, including the path name.

-savefile *report-file-name*

Specifies the name of the file to which the created report is to be output by using only a file name or an absolute path.

If you specify only a file name, the file is stored in either an HTML or CSV database. Specify the report file name in 255 bytes or less, including the path name. If you do not specify an extension with the file name, `.html` or `.csv` is automatically added according to the report type. Therefore, specify a file name in 250 bytes or fewer or 251 bytes or fewer, including the path name, because an extension is automatically added.

If the specified file exists, the created report overwrites the file.

When you specify an absolute path, if the directory specified for the path name does not exist, a report file is not created. Specifiable characters are single-byte alphanumeric characters, periods (.), underscores (_), and hyphens (-).

-title *report-title*

Specifies the title of the report file. If you omit this option, no title is displayed in the report file. Specify the title in 255 bytes or less. Also, do not specify Japanese and multi-byte codes that are different from the character encoding specified for the `lang` key in the report definition file.

-type {CSV | HTML | HTMLSVG}

Specifies a report output format. Specify `CSV`, `HTML`, or `HTMLSVG` for the report output format. If you omit this option, the report is output in the CSV format. No graph-format report is displayed in CSV-format report files.

If you specify `HTML`, a report is output in the VML standard. If you specify `HTMLSVG`, a report is output in the SVG standard. For details about the VML standard and the SVG standard, see *2.4.1(1) Report file formats*.

-start {DATE *date-and-time* | BDATE *date* | BMONTH *month*[,*date*]}

Specifies the start date and time of the data extraction range.

DATE *date-and-time*

Starts extracting the data collected after the specified date and time. Specify the date and time in the *yy.mm.dd.hh.mm.ss* format. The specifiable range is January 1, 1980 00:00:00 to December 31, 2029 23:59:59.

BDATE *date*

Extracts data from 00:00:00 on the date the specified number of days before the command execution date. The values that can be specified are 0 to 30 (days). If you specify 0, the command extracts data, starting at 0:00:00 on the date the command was executed.

BMONTH *month*[,*date*]

Extracts data at 00:00:00 on the specified date in the month the specified number of months before the command execution month. The values that can be specified in *month* are 0 to 12 (months). The values that can be specified in *date* are 1 to 31 (date). If you specify 0, the command extracts data for the month in which the command was executed. If you do not specify *date*, the command extracts data from the first day of the month.

-stop {DATE *date-and-time* | BDATE *date* | BMONTH *month*[,*date*]}

Specifies the end date and time of the data extraction range.

DATE *date-and-time*

Extracts collected data to the specified date and time. Specify the date and time in the *yy.mm.dd.hh.mm.ss* format. The specifiable range is January 1, 1980 00:00:00 to December 31, 23:59:59.

BDATE *date*

Extracts data until 23:59:59 on the date the specified number of days before the command execution date. The values that can be specified are 0 to 30 (days). If you specify 0, the command extracts data to 23:59:59 on the date the command was executed.

BMONTH *month*[,*date*]

Extracts data until 23:59:59 on the specified date in the month the specified number of months before the command execution month. The values that can be specified in *month* are 0 to 12 (months). The values that can be specified in *date* are 1 to 31 (date). If you specify 0 as *month*, the command extracts data to the month in which the command was executed. If you do not specify *date*, the command extracts data to 23:59:59 on the last day of the month.

-h

Outputs the command usage. This option cannot be specified together with other options.

Return values

0	Normal termination
-1	Execution error such as incorrect arguments

ssoextractlog

Format

To output collected data in text format:

```
ssoextractlog [-S connection-destination-server-name]
              -text [A | B | C | D | E | F | G | H] [1 | 2 | 3]
              {-logfile file-name
               | -masterlog resource-ID,collection-target-server-name
               | -dbname resource-ID,collection-database-name}
              [-instance instance-name,...]
              [-subrsc subresource-ID,...]
              [-start {DATE date-and-time | BDATE date
               | BMONTH month [,date]}]
              [-stop {DATE date-and-time | BDATE date
               | BMONTH month [,date]}]
              [-savefile file-name] [-notitle]
```

To copy collection databases:

```
ssoextractlog [-S connection-destination-server-name]
              -bin
              {-logfile file-name
               | -masterlog resource-ID,collection-target-server-name
              | -dbname resource-ID,collection-database-name}
              [-instance instance-name,...]
              [-start {DATE date-and-time | BDATE date
               | BMONTH month [,date]}]
              [-stop {DATE date-and-time | BDATE date
               | BMONTH month [,date]}]
              [-savefile file-name] [-user user-information]
```

To output a list of collection databases:

```
ssoextractlog [-S connection-destination-server-name]
                 -list [-savefile file-name]
```

Other:

```
ssoextractlog {? | ?id | ?text}
```

Function

The ssoextractlog command extracts collection data from an SSO collection database. You can output the extracted data as a text file. You can also copy specified data.

Options

-S *connection-destination-server-name*

Specifies a monitoring manager on which a collection database exists. Specify the host name or IP address in 255 bytes or less. If you omit this option, the command extracts the collected data of the server on which you executed the command.

-text [A | B | C | D | E | F | G | H] [1 | 2 | 3]

Extracts collected data in text format. You can specify the display type and delimitation type.

display-type

Specifies an output unit and output item. Select `A`, `B`, `C`, `D`, `E`, `F`, `G`, or `H` as the display type. The default is `A`. The table below lists the output units and output items that can be specified.

Type	Output unit	Output item
A	Instance	Value per collection date, collection time, and sub-resource; maximum value, minimum value, and mean value per sub-resource
B	Instance	Value per collection date, collection time, and sub-resource; threshold (from Normal to Warning and from Warning to Critical); maximum value, minimum value, and mean value per sub-resource
C	Instance	Value, maximum value, and minimum value per collection date and sub-resource; maximum value, minimum value, and mean value per sub-resource
D	Instance	Value, maximum value, and minimum value per collection month and sub-resource; maximum value, minimum value, and mean value per instance
E	Subresource	Value per collection date, collection time, and instance; maximum value, minimum value, and mean value per instance
F	Subresource	Value per collection date, collection time, and instance; threshold (from Normal to Warning and from Warning to Critical); maximum value, minimum value, and mean value per instance
G	Subresource	Value, maximum value, and minimum value per collection date and instance; maximum value, minimum value, and mean value per maximum value, minimum value, and instance
H	Subresource	Value, maximum value, and minimum value per collection month and instance; maximum value, mean value, minimum value, and mean value per instance

delimitation-type

Specifies a character for delimiting data.

1: Delimits by the comma

2: Delimits by the tab

3: Delimits by the space

The default is 1. The following shows an example of data output when A is specified as the display type and 1 as the delimition type.

```
Group name:Resource name,IP address,Instance,Unit
Collection date,Collection time,Subresource name,Subresource name,
Subresource name
2000/12/17,14:30:10,0.85,1.13,1.36
2000/12/17,14:30:37,0.94,1.12,1.35
2000/12/17,14:31:08,1.05,1.13,1.35
2000/12/17,14:31:38,0.84,1.08,1.32
2000/12/17,14:32:07,0.79,1.04,1.30
2000/12/17,14:32:38,0.67,0.99,1.27
2000/12/17,14:33:08,0.59,0.94,1.25
2000/12/17,14:33:37,0.70,0.93,1.24
Maximum,1.05,1.13,1.36
Minimum,0.59,0.93,1.24
Average,0.80,1.04,1.3
```

-logfile *file-name*

Extracts data of the specified file name. If you specify the file name specified in the `-savefile` option as the file name in this option, specify `.log` at the end of the file name.

Specify the file name by its absolute path. You cannot specify this option together with the `-S` option.

-masterlog *resource-ID,collection-target-server-name*

Specifies the master database whose data you want to extract, by its resource ID and server name. Specify the server name by the server's host name or IP address in 255 bytes or less. Verify the resource ID and server name by using the `-list` option. You cannot specify this option together with the `-S` option.

-dbname *resource-ID,database-name*

Specifies the master database or copy database whose data you want to extract, by its resource ID and database name. Verify the resource ID and database name by using the `-list` option.

-instance *instance-name,...*

Extracts collected data of the specified instance. To specify multiple instances, delimit the instances with a comma (`,`). If you omit this option, the command extracts collected data of all instances. If the instance name includes a comma (,) enclose it in double quotation marks (" "). If the instance name includes double quotation marks, enclose the entire instance name in double quotation marks.

-subrsc *subresource-ID,...*

Extracts collection data by using the specified subresource ID. If you want to specify multiple subresource IDs, delimit them with commas (`,`). If you omit this option, all the subresource IDs are to be extracted.

For details about subresource IDs added to subresources of user resources, see *6.3.14(6)(d) Subresource ID*.

For details about subresource IDs of resources provided by SSO, see *E. Resource IDs*.

-start {DATE *date-and-time* | BDATE *date* | BMONTH *month*[,*date*]}

Specifies the range of data to be extracted.

DATE *date-and-time*

Starts extraction at the collected data for the specified date and time.

Specify the date and time in the format *yyyy.mm.dd.hh.mm.ss*. The specifiable range is January 1, 1980 00:00:00 to December 31, 2029 23:59:59.

BDATE *date*

Starts extraction at data for 00:00:00 on the date preceeding the current date by the specified number of days. The specifiable range is 0 to 30 (days). If you specify `0`, the command extracts data starting with data for 00:00:00 on the date the command is executed.

BMONTH *month*[,*date*]

Starts extraction at data for 00:00:00 on the specified date of the month preceeding the current month by the specified number of months.

The specifiable range for the month is 0 to 12 (months). The specifiable range for the date is 1 to 31 (date). If you specify `0` for the month, the command extracts data for the month in which you executed the command.

If you do not specify *date*, the command extracts data from the first day of the month.

-stop {DATE *date-and-time* | BDATE *date* | BMONTH *month*[,*date*]}

Specifies the range of data to be extracted.

DATE *date-and-time*

Extracts collected data up to the specified date and time.

Specify the date and time in the format *yyyy.mm.dd.hh.mm.ss*. The specifiable range is January 1, 1980 00:00:00 to December 31, 2029 23:59:59.

BDATE *date*

Extracts data up to 23:59:59 on the date preceeding the current date by the specified number of days.

The specifiable range is 0 to 30 (days). If you specify `0`, the command extracts data up to 23:59:59 on the date the command is executed.

BMONTH *month*[,*date*]

Extracts data up to 23:59:59 on the specified date of the month preceeding the current month by the specified number of months.

The specifiable range for the month is 0 to 12 (months). The specifiable range for the date is 1 to 31 (date). If you specify `0` for the month, the command extracts data up to the month in which you executed the command.

If you do not specify *date*, the command extracts data up to 23:59:59 on the last day of the month.

-savefile *file-name*

- Output to a text file (specify `-text`)

  Specifies the file name to which you want to output the extracted data, by its absolute path. The command creates a file having the specified file name on the host on which you executed the command. If the specified file already exists, the command overwrites it.

  If you omit this option, the command outputs the result to the standard output.

- Copy (specify `-bin`)

  Specifies the copy destination file by its absolute path. The command creates three files on the connection destination host. The files have the specified file name followed by `.log`, `.inf`, and `.ins` respectively. If the specified file already exists, the command overwrites it.

  If you omit this option, the command creates a copy database. The copy database is created in the directory storing the collection database of the connection destination host. A file name is given to the database automatically when it is created. To create multiple copy databases, we recommend specifying the `-user` option to identify the databases.

  You cannot omit this option if you specified `-logfile` or `-masterlog`.

- To output the list of collection databases (with `-list` specified):

  Specify a file name to which you want to output the list of collection databases by using its full pathname. The specified file is created on the host on which the command is executed. If the specified file name already exists, it is overwritten. If you omit this option, the result is output to the standard output.

When you create a file with the `-text`, `-bin`, or `-list` option specified, if the disk space is filled, an incomplete set of data is stored in the file (an error message is not output). Confirm that the disk has enough free space, and then execute the command.

-notitle

Deletes the title and summary value from the output result.

-bin

Copies collection databases.

-list

Outputs a list of collection databases. The following shows the output format for the list of collection databases.

```
resource-ID  database collection-server collection-target-server category-group resource-size user-information
```

-user *user-information*

Specify information which you want to add to a copy database in 255 bytes or less. Multi-byte codes cannot be specified for user information.

?

Outputs the command usage. This option cannot be specified together with other options.

?id

Outputs a list of resource IDs.

?text

Outputs the usage of the `-text` option.

Examples

The following shows examples of specifying the `start` and `stop` options.

- The following example extracts data from December 15, 2000 00:00:00 to April 2, 2001 15:00:00:

```
-start DATE 2000.12.15.00.00.00 -stop DATE 2001.04.02.15.00.00
```

- The following example extracts data of the previous week (Monday to Friday) on the date on which the command is executed (Friday):

```
-start BDATE 4 -stop BDATE 0
```

- The following example extracts data from the first day of the current month to the last day of the month, on the last day of the current month:

```
-start BMONTH 0 -stop BMONTH 0
```

- The following example extracts data from the 21st day of the month three months previously to the 20th day of the current month, on the 21st day of the current month:

```
-start BMONTH 3,21 -stop BMONTH 0,20
```

Return values

0	Normal termination
-1	Execution error such as incorrect arguments

Notes

- If the disk becomes full while the file is being saved, only part of the data is saved in the file (no error message is output). Before saving data, verify that the disk has sufficient free space.
- Notes on concurrently executing the `ssodbdel` command and the `ssoextractlog` command

  Do not concurrently execute the `ssodbdel` command and the `ssoextractlog` command (during execution of one of the commands, you try to execute the other command). If these commands are concurrently executed, the `ssoextractlog` command outputs the following error message, and the processing might be interrupted if data extraction and copy are incomplete.

  In such a case, after the `ssodbdel` command is completed, re-execute the `ssoextractlog` command.

```
The applicable database does not exist. Extraction of the collection
database failed.
```

- Using the ssoextractlog command on a host with multiple IP addresses

  If you try to reference collection data on a host with multiple IP addresses such as a cluster system with the -masterlog option of the ssoextractlog option specified, you can reference nothing. Specify the -dbname option or the -logfile option.

- About the extraction time for the ssoextractlog command

  The extraction time for the ssoextractlog command is different depending on the display type setting. In display types A to D, data is extracted for each instance. Accordingly, extraction time becomes longer in proportion to the number of instances. In display types E to H, data is extracted for each subresource. Accordingly, extraction time becomes longer in proportion to the number of subresources. Therefore, setting a larger one of the number of instances and the number of subresources will shorten extraction time.

- Executing this command takes time in proportion to the size of the collection database. Therefore, make sure that you regularly delete collection data (either by deleting all data or by deleting part of the data by specifying a time period).
- Fractional resource values are rounded to two decimal places.
- If the date specified for the -start option and the -stop option is invalid (such as February 30), the operation becomes undefined.

ssoguistart

Format

To start a window:

```
ssoguistart -{rb|rc|rr|rd|pc|pr|pm}
```

To output the command usage:

```
ssoguistart -h
```

Function

The `ssoguistart` command starts windows provided by SSO.

Options

-rb

Starts the Resource Browser window. For details on the window, see *4.2 Resource Browser window*.

-rc

Starts the Resource Configuration window. For details on the window, see *4.3 Resource Configuration window*.

-rr

Starts the Resource Reference window. For details on the window, see *4.4 Resource Reference window*.

-rd

Starts the Resource Data Reference window. For details on the window, see *4.5 Resource Data Reference window*.

-pc

Starts the Process Configuration window. For details on the window, see *4.6 Process Configuration window*.

-pr

Starts the Process Reference window. For details on the window, see *4.7 Process Reference window*.

-pm

Starts the Process Monitor window. For details on the window, see *4.8 Process Monitor window*.

-h

Outputs the command usage. This option cannot be specified together with other options.

Return values

0	Normal termination
-1	Execution error such as incorrect arguments

ssonnmsetup

Format

To add or change information for connecting to NNMi on the local host:

```
ssonnmsetup -add -user user-name -password password
            -port port-number [-ssl]
```

To add or change information for connecting to NNMi on the event-destination host:

```
ssonnmsetup -add -dest IP-address -user user-name -password password
            -port port-number [-ssl]
```

To delete information for connecting to NNMi on the event-destination host:

```
ssonnmsetup -delete -dest IP-address
```

To add or change information for connecting to NNMi on other hosts in a distributed configuration:

```
ssonnmsetup -add -host management-manager-name
            -user user-name
            -password password -port port-number [-ssl]
```

To output the command usage:

```
ssonnmsetup -h
```

Function

The `ssonnmsetup` command adds, changes, and deletes information for connecting to NNMi when linking to NNMi. Define information for connecting to NNMi in the NNM information definition file (`ssonnminfo.conf`). For details about the NNM information definition file, see *6.3.29 NNM information definition file (ssonnminfo.conf)*.

If you execute the `ssonnmsetup` command during execution of the following commands, the command terminates abnormally:

`ssobackup`, `ssorestore`, `ssonnmsetup`

Options

-add

Adds or changes a definition for connecting to NNMi.

If you do not specify the `-dest` option, information for connecting to NNMi on the local host is to be defined. In such a case, the definition target is the `default` definition in the NNM information definition file. If you specify the `-dest` option, information for connecting to NNMi on the event-destination host is to be defined. In such a case, the IP address specified for the `-dest` option is set as the node key name in the NNM information definition file. If the `default` definition has been set or the IP address specified for the `-dest` option has been defined as a node key name in the NNM information definition file, the corresponding definition information is updated with the specified information.

-host *management-manager-name*

Specifies the host name or IP address of the management manager in 255 bytes or less in a distributed configuration. The `default` definition in the NNM information definition file is to be executed. This option cannot be specified together with the `-dest` option. Also, the local host name and the local host IP address cannot be specified.

-user *user-name*

Specifies an NNMi user name for connecting to NNMi.

Specify a user name that consists of only ASCII characters and is 1 byte to 40 bytes long. Specifiable characters are spaces, single-byte alphanumeric characters, and underscores (_).

Note that you cannot use a tab, quotation mark (`"`), asterisk (`*`), vertical bar (`|`), less-than sign (<), more-than sign (>), question mark (`?`), comma (`,`), equal sign (=), and hash mark (`#`).

Although we recommend that you specify *Web service client* of NNMi as the role for the user, *Administrator* and *System* can also be specified as roles.

-password *password*

Specifies the password for the user name specified for the `-user` option.

Specify a password that consists of only ASCII characters and is 1 byte to 40 bytes long. Specifiable characters are spaces, single-byte alphanumeric characters, and underscores (_).

Note that you cannot use a tab, quotation mark (`"`), asterisk (`*`), vertical bar (`|`), less-than sign (<), more-than sign (>), question mark (`?`), comma (`,`), equal sign (=), and hash mark (`#`).

-port *port-number*

Specifies the port number of *NNM Web server port* of NNMi. Specify the port number by using an integer from 1 to 65,535.

If you specify `-ssl`, the option specifies the port number of *NNM Web server port* for HTTPS communication.

-delete

Deletes the definition that the IP address specified for the `-dest` option set as a node key name.

-dest *IP-address*

Specifies the destination IP address in the event destination definition file.

-ssl

Specify this option when you communicate with NNMi by using HTTPS. If you do not specify this option, communication is performed by using HTTP.

-h

Outputs the command usage. This option cannot be specified together with other options.

Usage example

1. To set a user name (`jp1user`), password (`jp1sso`), and port number (`80`) for a NNMi connection on the local host:

```
ssonnmsetup -add -user jp1user -password jp1sso -port 80
```

2. To change the password in the `default` definition set in step 1 to `jp1cm2sso`:

```
ssonnmsetup -add -user jp1user -password jp1cm2sso -port 80
```

3. To set a user name (`jp1user`), password (`jp1sso`), and port number (`20080`) for a NNMi connection on the event destination host (IP address = `133.108.120.14`):

```
ssonnmsetup -add -dest 133.108.120.14 -user jp1user -password jp1sso -
port 20080
```

4. To delete the definition set in step 3:

```
ssonnmsetup -delete -dest 133.108.120.14
```

5. To set a user name (`jp1user`), password (`jp1sso`), and port number (`80`) for a NNMi connection on another host (host name = `nnmhost`) in a distributed configuration:

```
ssonnmsetup -add -host nnmhost -user jp1user -password jp1sso -port 80
```

6. To set a user name (`jp1user`), password (`jp1sso`), and port number (`443`) for a NNMi connection on the local host and establish HTTPS communication:

```
ssonnmsetup -add -user jp1user -password jp1sso -port 443 -ssl
```

7. To set a user name and password that include a single-byte space:

```
ssonnmsetup -add -user "jp1 user" -password "jp1 sso" -port 80
```

Return values

0	Normal termination
-1	Execution error such as incorrect arguments
-2	Execution error during editing of the NNM information definition file or backup and restore processing

ssomapstatus

Format

To delete the statuses of all the nodes:

```
ssomapstatus -del -all
             [-dest IP-address]
```

To delete the status of the specified server name:

```
ssomapstatus -del -s server-name,...
             [-dest IP-address]
```

To match the statuses of all the nodes:

```
ssomapstatus -sync -all
             [-dest IP-address]
```

To match the statuses applicable to the specified monitoring server:

```
ssomapstatus -sync -s server-name,...
             [-dest IP-address]
```

To display the statuses of all the nodes:

```
ssomapstatus -show -all
             [-dest IP-address]
```

To display the status of the specified server name:

```
ssomapstatus -show -s server-name,...
             [-dest IP-address]
```

To output the command usage:

```
ssomapstatus -h
```

Function

The ssomapstatus command is used to manage the status of the map cooperation (symbol cooperation) function. The command can delete, match, and display the status.

Options

-del -all

Deletes the status of resource statuses and application statuses on all the nodes in the NNMi map view.

-del -s *server-name*

Deletes the status of resource statuses and application statuses on nodes applicable to the monitoring server specified for *server-name*. Specify a host name or IP address in 255 bytes or less for the server name. If you want to specify multiple server names, delimit them with commas (,).

-sync -all

Match the resource statuses and application statuses of all the monitoring servers with the statuses in the NNMi map view.

-sync -s *server-name*

Match the resource statuses and application statuses of the monitoring server specified for *server-name* with the statuses in the NNMi map view. Specify a host name or IP address in 255 bytes or less for the server name. If you want to specify multiple server names, delimit them with commas (`,`).

-show -all

Outputs the resource statuses and application statuses in SSO and the statuses in the NNMi map. If no status is defined, a hyphen (`-`) is output. If the monitoring status in SSO matches the status in NNMi, `Matched` is output to the end of the output line. If the monitoring status in SSO does not match the status in NNMi, `Unmatched` is output to the end of the output line. If you execute the command while the SSO daemon processes (`ssocolmng` and `ssoapmon`) are running, the command is executed for the monitoring server that is monitored by SSO. If you execute the command while the SSO daemon processes (`ssocolmng` and `ssoapmon`) are stopped, the command is executed for all the nodes in the NNMi map view.

-show -s *server-name*

Outputs the resource statuses and application statuses in SSO and the statuses in the NNMi map for the monitoring server specified for *server-name*. If no status is defined, a hyphen (`-`) is output. If the monitoring status in SSO matches the status in NNMi, `Matched` is output to the end of the output line. If the monitoring status in SSO does not match the status in NNMi, `Unmatched` is output to the end of the output line. Specify a host name or IP address in 255 bytes or less for the server name. If you want to specify multiple server names, delimit them with commas (`,`).

-dest *IP-address*

Performs a map cooperation with NNMi on the event-destination host specified for *IP-address*. Specify the destination IP address in the event destination definition file for the IP address. If you do not specify this option, a map cooperation is performed with NNMi on the monitoring manager in a basic configuration or NNMi on the management manager in a distributed configuration.

-h

Outputs the command usage. This option cannot be specified together with other options.

Return values

0	Normal termination
-1	Execution error such as incorrect arguments
-2	One or both of the `ssoapmon` daemon process and the `ssocolmng` daemon process is not running.
-3	The `ssospmd` daemon process is not running.
-4	The `nnm-map-coop:` key in the `ssoapmon` action definition file and the `ssocolmng` action definition file is set to `off`.
-5	NNMi cooperation cannot be performed.

Depending on the options, unused return values may exist. Return values are listed by options in the following table.

Return values	Option		
	-del	-sync	-show
0	Y	Y	Y
-1	Y	Y	Y
-2	--	Y	Y
-3	--	Y	--
-4	Y	Y	Y
-5	Y	--	Y

Legend:
Y: Used
--: Unused

Notes

- If you specify `-del -all` in SSO in a distributed configuration, node statuses registered by other SSO are also deleted.
- If you execute the command with `-all` specified, all the nodes are to be processed, and it might take a long time.
- You cannot specify `-sync` while the SSO daemon processes (`ssocolmng` and `ssoapmon`) are stopped.
- If you specify `-sync` or `-show` while the SSO daemon processes (`ssocolmng` and `ssoapmon`) are running, the processing target is the object which SSO monitors with a threshold at the initial execution of the command.
- If you specify `-show` while the SSO daemon processes (`ssocolmng` and `ssoapmon`) stop, all the statuses set in the NNMi map view are displayed.
- This command can operate when the `nnm-map-coop:` key in the `ssoapmon` action definition file and the `ssocolmng` action definition file is set to `on`.
- If you specify `-show -all`, host name resolution is performed so that the output format is created. If host name resolution cannot be performed normally on the host running the monitoring manager, execution of the command takes long time.
- Do not execute this command together with another command.

Output format

The following is the output format of the `-show` option:

```
[      (1)      ] [  (2)  ] [  (3)  ] [  (4)  ] [  (5)  ] [  (6)  ]
```

(1) Monitoring server name (IP address)
(2) Resource status (SSO side)
(3) Application status (SSO side)
(4) Resource status (NNMi side)
(5) Application status (NNMi side)
(6) "Matched" or "Unmatched"

[ ] is not output.

The following is an example of output of status information by the `-show` option:

```
SSOW141 (133.108.68.141)   Critical  Normal   Critical  Normal   Matched
SSOW146 (133.108.68.146)   Normal    Warning  Normal    Critical Unmatched
SSOW157 (133.108.68.157)   Unknown   Normal   --------  -------- Unmatched
                                       :
```

ssopschk

Format

To check the format of definition files for monitoring processes:

```
ssopschk {-a monitoring-app-definition-file-name
          | -s monitoring-server-definition-file-name
          | -m monitoring-condition-definition-file-name}
```

To output the command usage:

```
ssopschk -h
```

Function

The `ssopschk` command checks the format of a monitoring app definition file, monitoring server definition file, or monitoring condition definition file. However, it does not check the correlation (such as duplicate definitions) between fields.

Options

-a *monitoring-app-definition-file-name*

Checks the format of the monitoring app definition file.

Specify the monitoring app definition file name in 512 bytes or less, including the path name. For details about monitoring app definition files, see *6.3.2 Monitoring app definition file*.

-s *monitoring-server-definition-file-name*

Checks the format of the monitoring server definition file.

Specify the monitoring server definition file name in 512 bytes or less, including the path name. For details about monitoring server definition files, see *6.3.3 Monitoring server definition file*.

-m *monitoring-condition-definition-file-name*

Checks the format of the monitoring condition definition file.

Specify the monitoring condition definition file name in 512 bytes or less, including the path name. For details about monitoring condition definition files, see *6.3.4 Monitoring condition definition file*.

-h

Outputs the command usage. This option cannot be specified together with other options.

Return values

0	Normal termination
-1	Execution error such as incorrect arguments

ssopscvt

Format

To convert a definition file to the tab-delimited format:

```
ssopscvt {-a monitoring-app-definition-file-name
          | -s monitoring-server-definition-file-name
          | -m monitoring-condition-definition-file-name}
         -p output-file-name
```

To convert a file having the tab-delimited format to the definition file format:

```
ssopscvt {-ca tab-delimited-format-file-name
          | -cs tab-delimited-format-file-name
          | -cm tab-delimited-format-file-name}
         -p output-file-name
```

To output the command usage:

```
ssopscvt -h
```

Function

The `ssopscvt` command converts a monitoring app definition file, monitoring server definition file, or monitoring condition definition file to data having the tab-delimited format. It also converts a file having the tab-delimited format to data having the monitoring app definition file format, monitoring server definition file format, or monitoring condition definition file format. Converting these definition files to the tab-delimited format makes it possible to manage the files using spreadsheet software.

Options

-a *monitoring-app-definition-file-name*

Converts the specified monitoring app definition file to data having the tab-delimited format.

-s *monitoring-server-definition-file-name*

Converts the specified monitoring server definition file to data having the tab-delimited format.

-m *monitoring-condition-definition-file-name*

Converts the specified monitoring condition definition file to data having the tab-delimited format.

-p *output-file-name*

Specifies the file to which you want to output the conversion result.

-ca *tab-delimited-format-file-name*

Converts the specified tab-delimited format file to a monitoring app definition file.

-cs *tab-delimited-format-file-name*

Converts the specified tab-delimited format file to a monitoring server definition file.

-cm *tab-delimited-format-file-name*

Converts the specified tab-delimited format file to a monitoring condition definition file.

-h

Outputs the command usage. This option cannot be specified together with other options.

Example

To convert a monitoring app definition file (`/tmp/sso_aps.conf`) to a file with the tab-delimited format (`/tmp/sso_aps.tab`):

```
ssopscvt -a /tmp/sso_aps.conf -p /tmp/sso_aps.tab
```

Return values

0	Normal termination
-1	Execution error such as incorrect arguments

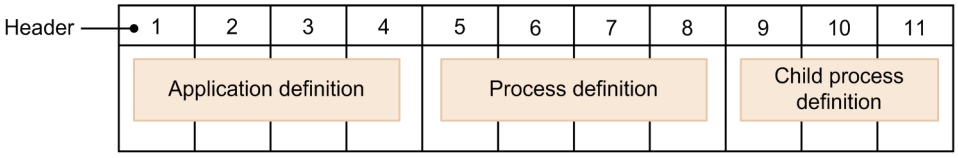
Notes

- If the disk becomes full while data is being output to a file as specified by the `-p` option, only part of the data is saved in the file (no error message is output). Before outputting data to a file, verify that the disk has sufficient free space.
- If you have specified a tab in an application definition or monitoring condition definition, it may not be converted properly to tab-delimited format data.
- Definitions for monitoring services cannot be converted by this command. If you specify a file containing definitions for monitoring services such as a monitoring app definition file or monitoring condition definition file, an error occurs.

Format of tab-delimited format file

Tab-delimited format of a monitoring app definition file

The tab-delimited format of a monitoring app definition file is described as follows:

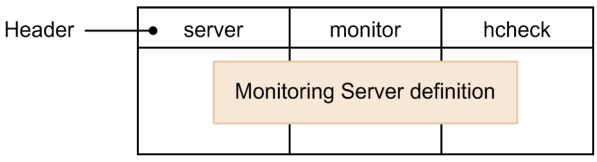


The following key names corresponding to numbers are displayed in the header part, starting from the left. Tabs delimit these key names.

1:apname,2:apinfo,3:apcommand,4:psnumber,5:psname,6:pscommand,7:psthreshold,8:cpsnumber,9:cpsname, 10:cpscommand,11:cpsthreshold

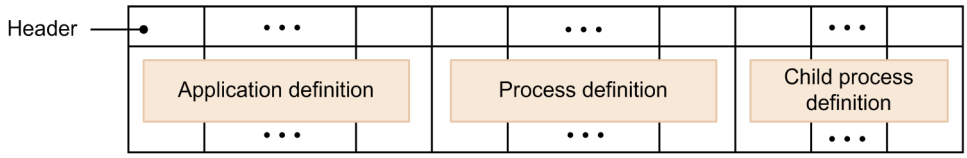
Tab-delimited format of a monitoring server definition file

The tab-delimited format of a monitoring server definition file is described as follows:



Tab-delimited format of a monitoring condition definition file

The tab-delimited format of a monitoring condition definition file is described as follows:



Monitoring condition definition key names are displayed in turn in the header part.

Examples of outputting the tab-delimited format file

Examples of outputting the tab-delimited format file are explained taking the monitoring app definition file as an example. The following shows an example of converting the monitoring app definition file shown in *6.3.2 (6) Example* to tab-delimited format data. For more information about key names and their values, see *6.3.2 Monitoring app definition file*.

1	2	3	4	5	6	7	8	9	10	11
JP1/SIA V6i	JP1/Security Investigator - Agent	N/A	5	E;gettlog	N/A	1;9999	0	N/A	N/A	N/A
N/A	N/A	N/A	N/A	E;logmgr	N/A	1;1	1	E;gettlog	N/A	1;9999
N/A	N/A	N/A	N/A	E;po	N/A	1;1	0	N/A	N/A	N/A
N/A	N/A	N/A	N/A	E;procmgr	N/A	1;1	3	E;logmgr	N/A	1;1
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	E;po	N/A	1;1
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	E;rulmgr	N/A	1;1
N/A	N/A	N/A	N/A	E;rulmgr	N/A	1;1	0	N/A	N/A	N/A

ssopsset

Format

To add or change a monitoring condition:

(a) To replace a monitoring process and a monitoring server completely with the contents of the definition file:

(a1) When you specify a monitoring process (`-as` is needed):

```
ssopsset [-S connection-destination-server-name]
         -as monitoring-app-definition-file-name
         [-ss monitoring-server-definition-file-name]
```

(a2) When you specify a monitoring server (`-ss` is needed):

```
ssopsset [-S connection-destination-server-name]
          [-as monitoring-app-definition-file-name]
           -ss monitoring-server-definition-file-name
```

(b) To replace a monitoring process and a monitoring server partially with the contents of the definition file:

(b1) When you specify a monitoring process (`-asn` is needed):

```
ssopsset [-S connection-destination-server-name]
         -asn monitoring-app-definition-file-name
         [-ssn monitoring-server-definition-file-name]
```

(b2) When you specify a monitoring server (`-ssn` is needed):

```
ssopsset [-S connection-destination-server-name]
         [-asn monitoring-app-definition-file-name]
          -ssn monitoring-server-definition-file-name
```

(c) To change a condition for monitoring an application by a process or service:

```
ssopsset [-S connection-destination-server-name]
         -ms monitoring-condition-definition-file-name
```

To delete a monitoring condition:

(a) When you specify an application:

```
ssopsset [-S connection-destination-server-name]
          {-ad [application-name,...]
           | -adf group-definition-file,group-name}
ssopsset [-S connection-destination-server-name]
          {-sd [server-name,...] | -sdf group-definition-file,group-name}
```

(b) When you specify a server:

```
ssopsset [-S connection-destination-server-name]
          {-sd [server-name,...]
           | -sdf group-definition-file,group-name}
```

To output a monitoring condition to a file:

```
ssopsset [-S connection-destination-server-name]
          {-ap | -sp | -mp}
          output-file-name
```

To output the command usage:

```
ssopsset -h
```

Function

The `ssopsset` command defines (adds, changes, and deletes) a process and service monitoring condition based on the specified definition file and outputs the defined monitoring condition to a definition file. Here, the definition file means a monitoring app definition file, monitoring server definition file, or a monitoring condition definition file.

Options

-S *connection-destination-server-name*

Specifies a monitoring manager which you use to redefine and output a process and service monitoring condition. Specify a host name or IP address in 255 bytes or less as the connection destination server name. When this option is not specified, the local host will be the connection destination.

-as *monitoring-app-definition-file-name*

Defines the monitoring application information by using the specified monitoring app definition file. If the monitoring application information has been defined, it is replaced with the specified monitoring app definition file. At this time, any monitoring application information that is not defined in the monitoring app definition file, and monitoring conditions related to the deleted monitoring application are also deleted.

Specify the monitoring app definition file name in 512 bytes or less, including the path name. You can specify this option together with the `-ss` option.

-ss *monitoring-server-definition-file-name*

Defines the monitoring server information by using the specified monitoring server definition file. If the monitoring server information has been defined, it is replaced with the specified monitoring server definition file. At this time, any monitoring server information that is not defined in the monitoring server definition file, and monitoring conditions related to the deleted monitoring server are also deleted.

Specify the monitoring server definition file name in 512 bytes or less, including the path name. You can specify this option together with the `-as` option.

-asn *monitoring-app-definition-file-name*

Changes the configured monitoring application information by using the specified monitoring app definition file. Any configured monitoring application information that is not defined in the monitoring app definition file remains as is.

Specify the monitoring app definition file name in 512 bytes or less, including the path name. You can specify this option together with the `-ssn` option.

-ssn *monitoring-server-definition-file-name*

Changes the configured monitoring server information by using the specified monitoring server definition file. Any configured monitoring server information that is not defined in the monitoring server definition file remains as is.

Specify the monitoring server definition file name in 512 bytes or less, including the path name. You can specify this option together with the `-asn` option.

-ms *monitoring-condition-definition-file-name*

Defines a monitoring condition by using the specified monitoring condition definition file. Any configured monitoring condition that is not defined in the monitoring condition definition file remains as is. If the monitoring application

information and monitoring server information that are defined in the monitoring condition definition file do not exist, an execution error occurs.

Specify the monitoring condition definition file name in 512 bytes or less, including the path name.

-ad *application-name*

Deletes the specified application information from the configured monitoring application information. At this time, monitoring conditions related to the deleted monitoring application are also deleted.

Note the following when specifying an application name:

- Specify the name in 128 bytes or less.
- If you include a blank, enclose it with double quotes (`" "`).
- To specify multiple application names, delimit them with a comma (`,`).
- If you omit specifying an application, the command deletes the settings for all applications.

-adf *group-definition-file,group-name*

Deletes the application information defined in the specified group from the configured monitoring application information. At this time, monitoring conditions related to the deleted monitoring application are also deleted.

Specify the group definition file in 512 bytes or less, including the path name. Specify the group name in 20 bytes or less.

-sd *server-name*

Deletes the monitoring server specified for *server-name* from the configured monitoring server information. Specify the host name or IP address in 255 bytes or less. To specify multiple servers, delimit the names with a comma (`,`). If you omit specifying a server, the command deletes the settings for all monitoring server information.

-sdf *group-definition-file,group-name*

Deletes the monitoring server information defined in the specified group from the configured monitoring server information.

Specify the group definition file in 512 bytes or less, including the path name. Specify the group name in 20 bytes or less.

-ap *output-file-name*

Outputs the monitoring application settings from the monitoring condition configuration file to the specified file. Specify the output file name in 512 bytes or less, including the path name.

-sp *output-file-name*

Outputs the monitoring server settings from the monitoring condition configuration file to the specified file. Specify the output file name in 512 bytes or less, including the path name.

-mp *output-file-name*

Outputs the monitoring condition settings from the monitoring condition configuration file to the specified file. Specify the output file name in 512 bytes or less, including the path name.

-h

Outputs the command usage. This option cannot be specified together with other options.

Examples

- The following example changes the monitoring application settings to the contents of the monitoring app definition file (`/tmp/ssoas.conf`) (Any monitoring application configuration that is not defined in the monitoring app definition file is deleted):

```
ssopsset -as /tmp/sso_aps.conf
```

- The following example outputs the configuration information related to the monitoring application of the configured monitoring conditions to `/tmp/sso_aps.conf` in a monitoring app definition file format:

```
ssopsset -ap /tmp/sso_aps.conf
```

Return values

0	Normal termination
-1	Execution error such as incorrect arguments

Notes

- If you add, change, or delete a monitoring condition while the Process Configuration window is open, an execution error occurs. Also, while this command is adding, changing, or deleting a monitoring condition, you cannot start the Process Configuration window (the window starts in reference mode).
- If you execute this command, do not cancel it before processing finishes.
- If the disk becomes full while data is being output to a file, only part of the data is saved in the file (no error message is output). Before outputting data to a file, verify that the disk has sufficient free space.

ssopsshow

Format

To view the process or service monitoring status:

```
ssopsshow [-S connection-destination-server-name]
          [-a application-name,...
           | -af group-definition-file,group-name]
          [-s monitoring-server-name,...
           | -sf group-definition-file,group-name]
```

To generate the monitoring status definition file:

```
ssopsshow [-S connection-destination-server-name]
          [-a application-name,...
           | -af group-definition-file,group-name]
          [-s monitoring-server-name,...
           | -sf group-definition-file,group-name]
          -p monitoring-status-definition-file-name
```

To output the command usage.

```
ssopsshow -h
```

Function

The `ssopsshow` command displays a process and service monitoring status in the standard output and creates a monitoring status definition file.

Options

-S *connection-destination-server-name*

Specify the monitoring manager for which you want to display the monitoring status and generate the monitoring status configuration file. Specify the connection destination server name as a hostname or IP address in 255 bytes or less. When you do not specify this option, the local host will be the connection destination.

-a *application-name*

Displays a monitoring status or creates a monitoring status definition file for the specified application. To specify multiple application names, delimit them with a comma (`,`).

This option cannot be specified together with the `-af` option.

-af *group-definition-file,group-name*

Displays a monitoring status or creates a monitoring status definition file for the applications defined in the specified group definition file.

Specify the group definition file in 512 bytes or less, including the path name.

This option cannot be specified together with the `-a` option.

-s *monitoring-server-name*

Displays a monitoring status or creates a monitoring status definition file for the specified monitoring server. Specify the monitoring server name as a host name or IP address in 255 bytes or less. When specifying multiple server names, delimit them with a comma (,).

This option cannot be specified together with the `-sf` option.

-sf *group-definition-file-name, group-name*

Displays a monitoring status or creates a monitoring status definition file for the monitoring servers defined in the specified group definition file.

Specify the group definition file name, including the path name, in 512 bytes or less.

This option cannot be specified together with the `-s` option.

-p *monitoring-status-definition-file-name*

When generating a monitoring status definition file, specify the name of the file to be generated. Specify the file name, including the path, in 512 bytes or less.

If the specified file has already exited, it is overwritten.

-h

Outputs the command usage. This option cannot be specified together with other options.

Examples

- The following example displays the monitoring status of applications `uap01` and `uap02` in monitoring server `apm01`:

```
ssopsshow -s apm01 -a uap01,uap02
```

- The following example outputs all the monitoring statuses to a monitoring status definition file `/tmp/file.ps`:

```
ssopsshow -p /tmp/file.ps
```

Return values

0	Normal termination
-1	Execution error such as incorrect arguments

ssopsstart

Format

To start monitoring all targets:

```
ssopsstart [-S connection-destination-server-name] -all
```

To specify an application or server and start monitoring:

(a) When you specify an application (either -a or -af is needed)

```
ssopsstart [-S connection-destination-server-name]
           {-a application-name,...
            | -af group-definition-file,group-name}
           [-s monitoring-server-name,...
            | -sf group-definition-file,group-name]
```

(b) When you specify a server (either -s or -sf is needed)

```
ssopsstart [-S connection-destination-server-name]
           [-a application-name,...
            | -af group-definition-file,group-name]
           {-s monitoring-server-name,...
            | -sf group-definition-file,group-name}
```

To specify the name of a monitoring status definition file and start monitoring:

```
ssopsstart [-S connection-destination-server-name]
           -i monitoring-status-definition-file-name
```

To output the command usage:

```
ssopsstart -h
```

Function

The ssopsstart command starts process or service monitoring.

Options

-S *connection-destination-server-name*

Specify the monitoring manager processes for which you want to start monitoring. Specify the connection destination server name as a host name or IP address in 255 bytes or less. When this option is not specified, process monitoring at the local host will start.

-all

Starts monitoring all the monitoring applications defined in the monitoring app configuration file in the monitoring servers defined in the monitoring condition configuration file.

-a *application-name*,...

Starts monitoring the specified application. If no monitoring server is defined in the monitoring condition configuration file, nothing is performed. To specify multiple application names, delimit them with a comma (,).

This option cannot be specified together with the -af option.

-af *group-definition-file-name,group-name*

Starts monitoring the applications defined in the specified group definition file. If no monitoring server is defined in the monitoring condition configuration file, nothing is performed.

Specify the group definition file in 512 bytes or less, including the path name.

This option cannot be specified together with the `-a` option.

-s *monitoring-server-name,...*

Starts monitoring the specified monitoring server. If the monitoring server defined in the monitoring condition configuration file does not exist, nothing is performed.

Specify the host name or IP address in 255 bytes or less. To specify multiple server names, delimit the names with a comma (`,`).

This option cannot be specified together with the `-sf` option.

-sf *group-definition-file-name,group-name*

Starts monitoring the monitoring servers defined in the specified group definition file. If the monitoring server defined in the monitoring condition configuration file does not exist, nothing is performed.

Specify the group definition file in 512 bytes or less, including the path name.

This option cannot be specified together with the `-s` option.

-i *monitoring-status-definition-file-name*

Starts the monitoring operation defined in the specified monitoring status definition file.

-h

Outputs the command usage. This option cannot be specified together with other options.

Examples

- The following example starts monitoring applications `uap01` and `uap02` in monitoring server `apm01`:

```
ssopsstart -a uap01,uap02 -s apm01
```

- The following example starts monitoring the applications in a group `apps` that are defined in a group definition file `/tmp/file.grp`:

```
ssopsstart -af /tmp/file.grp,apps
```

- The following example starts the monitoring operation defined in a monitoring status definition file `/tmp/file.ps`:

```
ssopsstart -i /tmp/file.ps
```

Return values

0	Normal termination
-1	Execution error such as incorrect arguments

Note

If you execute this command, do not cancel it before processing finishes.

ssopsstop

Format

To stop monitoring all the targets:

```
ssopsstop [-S connection-destination-server-name] -all
```

To specify an application or server and stop monitoring:

(a) When you specify an application (either -a or -af is needed)

```
ssopsstop [-S connection-destination-server-name]
          {-a application-name,...
           | -af group-definition-file,group-name}
          [-s monitoring-server-name,...
           | -sf group-definition-file,group-name]
```

(b) When you specify a server (either -s or -sf is needed)

```
ssopsstop [-S connection-destination-server-name]
          [-a application-name,...
           | -af group-definition-file,group-name]
          {-s monitoring-server-name,...
           | -sf group-definition-file,group-name}
```

To specify the name of a monitoring status definition file and stop monitoring:

```
ssopsstop [-S connection-destination-server-name]
          -i monitoring-status-definition-file-name
```

To output the command usage:

```
ssopsstop -h
```

Function

The ssopsstop command stops process or service monitoring.

Options

-S *connection-destination-server-name*

Specify the monitoring manager processes or services for which you want to stop monitoring. Specify the connection destination server name as a host name or IP address in 255 bytes or less. When this option is not specified, process monitoring at the local host will stop.

-all

Stops monitoring all the targets.

-a *application-name*

Stops monitoring the specified application. If the monitoring condition configuration file does not contain the specified application, the command takes no action. To specify multiple application names, delimit them with a comma (,).

This option cannot be specified together with the -af option.

-af *group-definition-file-name,group-name*

Stops monitoring the applications defined in the specified group definition file. If the application defined in the group definition file does not exist in the monitoring condition configuration file, nothing is performed.

Specify the group definition file in 512 bytes or less, including the path name. Specify the group name in 20 bytes or less.

This option cannot be specified together with the `-a` option.

-s *monitoring-server-name*

Stops monitoring the specified monitoring server. If the monitoring server defined in the monitoring condition configuration file does not exist, nothing is performed. Specify the host name or IP address in 255 bytes or less. To specify multiple server names, delimit the names with a comma (`,`).

This option cannot be specified together with the `-sf` option.

-sf *group-definition-file-name,group-name*

Stops monitoring the monitoring servers defined in the specified group definition file. If the monitoring server defined in the group definition file does not exist in the monitoring condition configuration file, nothing is performed.

Specify the group definition file in 512 bytes or less, including the path name. Specify the group name in 20 bytes or less.

This option cannot be specified together with the `-s` option.

-i *monitoring-status-definition-file-name*

Stops the monitoring operation defined in the specified monitoring status definition file.

-h

Outputs the command usage. This option cannot be specified together with other options.

Examples

- The following example stops monitoring applications `uap01` and `uap02` in monitoring server `apm01`:

```
ssopsstop -a uap01,uap02 -s apm01
```

- The following example stops monitoring the applications in a group `apps` that are defined in a group definition file `/tmp/file.grp`:

```
ssopsstop -af /tmp/file.grp,apps
```

- The following example stops the monitoring operation defined in a monitoring status definition file `/tmp/file.ps`:

```
ssopsstop -i /tmp/file.ps
```

Return values

0	Normal termination
-1	Execution error such as incorrect arguments

Note

If you execute this command, do not cancel it before processing finishes.

ssorestore

Format

To restore files or databases provided by SSO:

```
ssorestore {-all | -conf | -db}
           [-clear] [-d restore-source-directory]
```

To output the command usage:

```
ssorestore -h
```

Function

The `ssorestore` command restores SSO files and databases that were backed up by the `ssobackup` command. For details about the restore function, see *2.7.2 Restore function*.

If you execute the `ssorestore` command while a daemon process is running, the command terminates abnormally. Therefore, make sure that you stop all the daemon processes before executing the command.

The `ssorestore` command restores files first and databases second. The command can also restore either files or databases. For details about restore targets, see *2.7.3 Backup targets and restore targets*.

The `ssorestore` command overwrites a file to be restored unless the `-clear` option is specified. Therefore, if a file other than SSO files or databases exists in the directory to be restored in the SSO installation directory, the file remains as is.

If you execute the `ssorestore` command during execution of the following commands and operations, the command terminates abnormally.

`ssostart`, `ssostop`, `ssobackup`, `ssorestore`, `ssoauth`, `ssonnmsetup`, starts the SSO services

Likewise, if you execute the following commands or operations during execution of the `ssorestore` command, the commands or operations terminate abnormally:

`ssostart`, `ssobackup`, `ssorestore`, `ssoauth`, `ssonnmsetup`, starts the SSO services

Options

-all

Specify this option when you restore both files and databases. To specify this option, the backup data of the files and databases is needed. If the backup data does not exist, the command terminates abnormally.

-conf

Specify this option when you restore only files. To specify this option, the backup data of the files is needed. If the backup data does not exist, the command terminates abnormally.

-db

Specify this option when you restore only databases. To specify this option, the backup data of the databases is needed. If the backup data does not exist, the command terminates abnormally.

-clear

Specify this option when you delete the directory to be restored in the SSO installation destination.

If you specify this option, the restore destination is totally replaced by the backup data. If you do not specify this option, the command overwrites files to be restored.

If the directory to be restored contains a file other than SSO files, or you do not want to delete the latest database, do not specify this option.

-d *restore-source-directory*

Specifies a directory in which the restore-source backup data is stored. You can specify a directory name by using either an absolute or relative path. If the specified directory does not exist, or the backup directory to be restored does not exist in the specified directory, the command terminates abnormally.

If you do not specify this option, the restore-source backup data is `$SSO_BACKUP`.

-h

Outputs the command usage. This option cannot be specified together with other options.

Usage example

The following example completely replaces the restore-destination database by the backup data of both phases that was stored in `/tmp/ssov9/backup`:

```
ssorestore -db -clear -d /tmp/ssov9/backup
```

Return values

0	Normal termination
-1	Execution error such as incorrect arguments
-2	Execution error during processing of startup or stop, editing of an SSO authentication user, editing of the NNM information definition file, or backup and restore processing

Notes

The following provides notes on restore operations.

About disk capacity:

The `ssorestore` command checks the amount of data in the restore target and the free space of the SSO installation destination disk before performing a restore. If the free space of the disk is less than the amount of data in the restore target, the restore terminates abnormally. Also, if the free space of the disk becomes insufficient during the restore after it is checked, the restore terminates abnormally.

Therefore, when you perform a restore, make sure that the capacity of the SSO installation destination disk is more than the total of the amount (size on a disk) of each restore-target directory.

To avoid an error termination due to insufficient disk space, provide sufficient space on the SSO installation destination disk.

About daemon processes and operations:

When you perform a restore, pay attention to the following notes on SSO daemon processes and operations.

Before a restore:

You must close the GUI and stop SSO before a restore. If you perform a restore without stopping SSO, the restore terminates abnormally.

During a restore:

You cannot start SSO during a restore.

About restoring corrupted backup data:

If the backup data is corrupted, the restore terminates abnormally. At this time, you cannot recover the state before the restore.

User authentication function:

You cannot add and delete a user for SSO authentication during a restore.

ssorptd

Format

To issue an instruction to re-read the definition file:

```
ssorptd -r
```

Option to be specified in the SSO startup definition file:

None

Function

The `ssorptd` command is a daemon process to create reports. If you execute this daemon process as a command, the definition file is re-read.

Option

-r

Re-reads the `ssorptd` action definition file (`ssorptd.def`). Do not specify this option in the SSO startup definition file (`ssostartup.conf`).

Return values

The return values for the `-r` option are as follows.

0	Normal termination
-1	Execution error such as incorrect arguments

Note

When you create a report, the processes of the `ssoextractlog` command for the number of report conditions start concurrently.

ssospmd

Format

To issue an instruction to re-read the definition file:

```
ssospmd -r
```

Function

The ssospmd command re-reads the definition file.

Option

-r

Re-reads the ssospmd action definition file (ssospmd.def) and the action log definition file (ssoauditlog.conf).

Return values

0	Normal termination
-1	Execution error such as incorrect arguments
-3	The ssospmd daemon process is not running.

ssostart

Format

```
ssostart [-c] [daemon-process-name...]
```

Function

The ssostart command starts a SSO daemon process. The command starts the specified daemon process (when a daemon process name is not specified, all daemon processes) based on the SSO startup definition file.

The command continues running until the startup process of all the daemon processes to be started is completed (startup finishes successfully or fails).

If you execute the ssostart command during the processing of starting or stopping SSO services, the processing of the transition of a daemon process, or execution of the following commands, the command terminates abnormally.

ssostart, ssostop, ssobackup, ssorestore, ssocadel

Options

-c

Outputs information about the success or failure of the startup of each process.

daemon-process-name...

The following are the specifiable daemon process names:

- ssocolmng (resource collection management daemon process)
- ssocollectd (resource collection daemon process)
- ssoapmon (process and service monitoring daemon process)
- ssorptd (report creation daemon process)
- ssoconsoled (SSO console daemon process)
- ssotrapd (SNMP trap receiving daemon process)

Examples

- The following example starts the resource collection function:

  ```
  ssostart -c ssocolmng
  ```

  The ssocollectd daemon process also starts because of the dependence relationship.
- The following example starts the process and service monitoring function:

  ```
  ssostart -c ssoapmon
  ```

Return values

0	Normal termination
-1	Execution error such as incorrect arguments, startup timeout, or when you try to start multiple daemon processes concurrently and some of the daemon processes fail to start.

-2	Execution error during the processing of starting or stopping, backup and restore processing, or the processing of the transition of a daemon process

ssostatus

Format

```
ssostatus [daemon-process-name...]
```

Function

The `ssostatus` command displays the status of a SSO daemon process. If you specify one or more daemon process names as an argument and execute the `ssostatus` command, the statuses of the specified daemon processes are output. If you do not specify a daemon process name, the statuses of all the daemon processes defined in the SSO startup definition file are output.

Table 5-2 describes the output contents of the `ssostatus` command. Additionally, Table 5-3 lists the statuses of a daemon process.

For details about the status transition of a daemon process, see *D. Daemon Process Status Transitions*.

Table 5-2: Output contents of the ssostatus command

Item	Description
Name	Daemon process name
PID	Process ID of daemon process
State	Daemon process status

Table 5-3: List of statuses of a daemon process

Status	Description
RUNNING	The daemon process is running.
NOT_RUNNING	The daemon process is stopped.
PAUSING	The daemon process is interrupted.
SUSPENDING	The daemon process has stopped temporarily.
DEGENERATING	The daemon process is performing a degeneration operation.
RUNNING*	Shown during the processing of starting, resuming, restarting, or normal operation of the daemon process.
NOT_RUNNING*	Shown during the processing of stopping of the daemon process.
PAUSING*	Shown during the processing of interruption of the daemon process.
SUSPENDING*	Shown during the processing of temporarily stopping the daemon process.
DEGENERATING*	Shown during the processing of a degeneration operation of the daemon process

Option

daemon-process-name...

The following are the specifiable daemon process names:

- `ssocolmng` (resource collection management daemon process)

- ssocollectd (resource collection daemon process)
- ssoapmon (process and service monitoring daemon process)
- ssorptd (report creation daemon process)
- ssoconsoled (SSO console daemon process)
- ssotrapd (SNMP trap receiving daemon process)

Return values

0	Normal termination
-1	Execution error such as incorrect arguments
-3	The ssospmd daemon process is not running.

Note

The statuses of the cjstartweb and httpsd processes are not output. You can check the statuses of those processes in the list of processes of the task manager in Windows, or by the ps command in UNIX.

ssostop

Format

```
ssostop [-c] [daemon-process-name...]
```

Function

The ssostop command stops the daemon processes.If you specify one or more daemon process names as an argument and execute the ssostop command, the command stops the specified daemon processes after stopping daemon processes that depend on the specified daemon processes. If you do not specify a daemon process name, all the daemon processes that are running, including ssospmd, are stopped.

If you execute the ssostop command during the processing of starting or stopping SSO services, the processing of the transition of a daemon process, or execution of the following commands, the command terminates abnormally.

ssostart, ssostop, ssobackup, ssodbdel

Options

-c

Outputs information about the success or failure of stopping each process.

daemon-process-name...

The following are the specifiable daemon process names:

- ssocolmng (resource collection management daemon process)
- ssocollectd (resource collection daemon process)
- ssoapmon (process and service monitoring daemon process)
- ssorptd (report creation daemon process)
- ssoconsoled (SSO console daemon process)
- ssotrapd (SNMP trap receiving daemon process)

Examples

- The following example stops the resource collection function:

  ```
  ssostop -c ssocollectd
  ```

  The ssocolmng daemon process also stops because of a dependence relationship.
- The following example stops the process and service monitoring function:

  ```
  ssostop -c ssoapmon
  ```

Return values

0	Normal termination
-1	Execution error such as incorrect arguments, stop timeout, or when you try to stop multiple daemon processes concurrently and some of the daemon processes fail to stop.

-2	Execution error during the processing of starting or stopping SSO daemon processes, backup processing, the processing of deletion of databases, or the processing of the transition of a daemon process

Note

If the following error message is output during execution of the `ssostop` command, the termination processing of the daemon process that the error message indicates did not finish within the timeout time. In such a case, extend the timeout time of the daemon process in the SSO startup definition file.

`ssospmd: A timeout occurred in a daemon process (`*daemon-process-name*`).`

The following is an example of an error message when the `ssoapmon` daemon process did not finish within the timeout time:

```
ssospmd: A timeout occurred in a daemon process (ssoapmon).
```

ssotrapd

Format

To issue an instruction to re-read the definition file:

```
ssotrapd -r
```

Function

The `ssotrapd` command is a daemon process to receive SNMP trap events issued by APM. The command uses the SNMP trap receiving port number `162/udp`.

If you execute the daemon process as a command, the `ssotrapd` action definition file is re-read.

Option

-r

Re-reads the `ssotrapd` action definition file (`ssotrapd.def`). Do not specify this option in the SSO startup definition file (`ssostartup.conf`).

Return values

0	Normal termination
-1	Execution error

6 Definition Files

This chapter describes the contents of definition files provided by SSO series and how to define the necessary information.

6.1 Overview of definition files

This section lists definition files that can be created or edited by users.

6.1.1 Definition files for SSO

The following table lists definition files that can be used for SSO. Definition files (that have fixed definition file names) provided by SSO are stored in the `$SSO_CONF` directory.

Table 6-1: Definition files (SSO)

Classification	Definition file	File name
Definition files common to functions	SNMP definition file	ssosnmp.conf
	Port number definition file	ssoport.conf
	Group definition file	Any
	Event destination definition file	ssodest.conf
	Event filter definition file	ssoevtfilter.conf
Definition files for resource collection function	`ssocolmng` action definition file	ssocolmng.def
	`ssocollectd` action definition file	ssocollectd.def
	Collection conditions definition file	Any
	Collecting condition definition file	Any
	Threshold definition file	ssothreshold.conf
	Threshold verification definition file	Any
	User resource definition file	Any
	Resource-icon definition file	The file name varies by the type of icon. For details, see *6.3.15 Resource-icon definition file*.
Definition files for process and service monitoring function	`ssoapmon` action definition file	ssoapmon.def
	Monitoring app definition file	Any
	Monitoring server definition file	Any
	Monitoring condition definition file	Any
	Monitor status definition file	Any
	TCP agent definition file	ssotcpagent.conf
	`ssotrapd` action definition file	ssotrapd.def
Definition files for report function	`ssorptd` action definition file	ssorptd.def
	Report definition file	Any
Definition files for GUI functions	GUI definition file	ssogui.conf
	GUI log definition file	ssoguilog.conf
Definition files for NNM cooperation function	NNM information definition file	ssonnminfo.conf

Classification	Definition file	File name
Definition files for NNM cooperation function	NNM action definition file	ssonnmaction.conf
	NNM action address definition file	ssonnmactaddr.conf
Definition files for SSO console function	`ssoconsoled` action definition file	ssoconsoled.def
	User authentication definition file	ssoauth.conf
Definition file for action log output function	Action log definition file	ssoauditlog.conf
Definition files for daemon process management function	`ssospmd` action definition file	ssospmd.def
	SSO startup definition file	ssostartup.conf

6.2 Creation rules common to definition files

Creation rules common to definition files are shown below.

6.2.1 Rules on comments and empty lines

The following rules on comments and empty lines are common to definition files:

- Lines beginning with a number sign (#), a tab, or a space are treated as comments.
- The empty lines (a line that contains only tabs or spaces) are ignored.

These rules, however, do not apply to the definition files listed in the following table.

Table 6-2: Definition files not subject to the common rules on comments and empty lines

Definition file	Description
GUI definition file	*6.3.11 GUI definition file (ssogui.conf)*
Resource-icon definition file	Not subject to the rules because this file is a GIF file
Report definition file	*6.3.21 Report definition file*
User authentication definition file	Not subject to the rules because this file cannot be edited
NNM information definition file	Not subject to the rules because this file cannot be edited
NNM action definition file	*6.3.30 NNM action definition file (ssonnmaction.conf)*
GUI log definition file	*6.3.31 GUI log definition file (ssoguilog.conf)*

6.2.2 Rules on the use of multi-byte characters

You can use multi-byte characters for the items listed below. Do not use multi-byte characters for any other items.

- Comment lines
- Values of the `rsc_label_j` and `subrsc_label_j` keys in the user resource definition file
- Instance name

  Note, however, that multi-byte characters can be used on condition that the language environment of the collecting server is the same as that of the collection target server.
- Report title

  Note, however, that multi-byte characters can be used on condition that the language environment for creating reports is the same as that for referencing reports.
- Directory name and file name

  Note, however, that for remote commands, multi-byte characters can be used on condition that the language environment of the monitoring manager is the same as that of the monitoring server.

6.3 Details of definition files for SSO

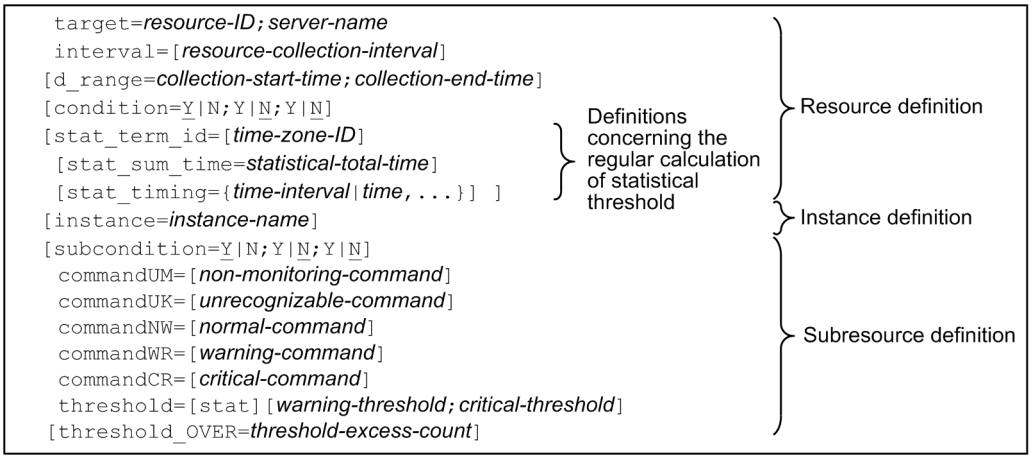
This section describes the contents of each definition file for SSO.

6.3.1 Collection conditions definition file

If you want to collect resource information, use the collection conditions definition file to define the conditions for resource information collection, including the resources whose information should be collected and the period in which resource information is to be collected.

(1) Format

You can define multiple sets of collection conditions in a collection conditions definition file. Specify collection conditions in the following format:



(2) Details of resource definition

The next table lists the items that constitute a resource definition. You must write a resource definition for each resource. You must write fields in the definition file in the order in which they are listed in the table below. For more information about resource IDs, see *E. Resource IDs*.

Key name	Value
`target` ((character string of up to 255 bytes))	Specify a semicolon-separated pair consisting of the resource ID and server name to be collected. Specify a host name or IP address as the server name.
`interval` <<5m; the default unit is s>> ((10s to 24h))	Specify a resource collection interval. Select s (second), m (minute), or h (hour) as the resource collection interval unit.
`d_range` ((00:00:00 to 24:00:00))	Specify a semicolon-separated pair consisting of a collection start time and a collection end time, in the *hh:mm:ss* format. You cannot specify a time period that extends over midnight. For example, to set a collection time period from 21:00 to 9:00 of the following day, specify as follows: d_range=00:00:00;09:00:00 d_range=21:00:00;24:00:00
`condition` <<Y;N;N[#1]>>	To set the following items, specify `Y`. If you do not wish to set them, specify `N`. Separate these items with a semicolon (;).

Key name	Value
condition <<Y;N;N[#1]>>	• Saving of collected data in file • Threshold check • Symbol display[#2]
stat_term_id <<1>> ((1 to 10))	Specify a time zone ID.
stat_sum_time <<96>> ((24 to 720))	Specify a total time preceding the calculation time as the range of the collection period of collected data that is to be extracted to calculate the statistical threshold.
stat_timing <<1h>>	Specify an interval or point of time as the timing for calculating the statistical threshold. The default is an interval of 1 hour. When specifying a time interval, use the format **h**m. The ** part indicates a numerical value. The specifiable range is 15m to 24h. When specifying a point of time, use the format hh:mm. The specifiable range is 00:00 to 23:59. To specify multiple points of time, delimit the values with a comma (,), and ensure a difference of 15 minutes or more between the values.

#1

For some resources, a different default value may be used.

#2

Because this item is intended to maintain compatibility with earlier versions, this item is ignored regardless of whether Y or N is specified.

When coding a resource definition, note the following:

- As a rule, when you omit an optional definition item, you can only omit the value; you must write the key name and an equal sign (=). When you omit the collection period (key name: d_range) or the collection mode (key name: condition), however, you must omit the entire field -- including the key name.
- If one definition file contains two or more collection conditions definitions that have the same value assigned to the key name target, only the first collection conditions definition will be regarded as valid and the other collection conditions definitions will be ignored.
- When using the ssocolset command to change the collection conditions, remember that you cannot modify the d_range of the resources where the collection state is collecting, postponing, or standing by.

(3) Details of instance definition

If you want to define different collection conditions for different instances, you must define instances. If you want to use the same collection conditions for all the instances, you need not define instances.

When defining collection conditions for each instance, you must define all the instances. Undefined instances will be regarded as ineligible for resource information collection.

The next table lists the items that constitute an instance definition.

Key name	Value
instance ((character string of up to 255 bytes))	Specify an instance name in up to 255 bytes. Instance names cannot include any spaces.

When coding an instance definition, note the following:

- When omitting an optional definition item, omit the entire field including the key name.

- If one resource definition contains two or more instance definitions that have the same value assigned to the key name `instance`, only the first instance definition will be regarded as valid and the other instance definitions will be ignored.

(4) Details of subresource definition

You must write a subresource definition for each subresource that belongs to the resource. You must enter subresource definition items into the definition file in the order in which they are listed in the following table.

Key name	Value
`subcondition` <<Y;N;N[#1]>>	To set the following items, specify `Y`. If you do not wish to set them, specify `N`. Separate these items with a semicolon (;). The specification in this key overrides the specification in the `condition` key. • Saving of collected data in file • Threshold check • Symbol display[#2]
`commandUM`	Specify the commands to be executed when the threshold is exceeded. Specify each of the commands to be executed with a character string of up to 259 bytes. When you use a command common to all the three items above, specify the command for each item.
`commandUK`	
`commandNM`	
`commandWR`	
`commandCR`	
`Threshold` • For Fixed threshold ((0 or a floating-point number from ± 1.00 **x** 10^{-2} to ± 1.7976931348623157 **x** 10^{308})) • For Statistical threshold <<`99.95;99.99`>> ((0.01 to 99.99))	• For Fixed threshold (when `stat` is not specified) Specify a semicolon-separated pair consisting of a warning threshold and a critical threshold. • For Statistical threshold (when `stat` is specified) Specify the ratio of the count of collection operations by which normal data is collected to the total collection count and the ratio of the count of collection operations by which warning data is collected to the total collection count. Delimit the ratios with a semicolon (`;`). Assume, for example, that collection was done 100 times, normal data was collected 97 times, warning data was collected twice, and critical data was collected once. In such a case, statistically, the percentage of normal data is 97%, and the percentage of normal and warning data is 99%. Then, the specification must be `threshold=stat97.00;99.00`. Values can be omitted. The default values are `99.95` (warning data) and `99.99` (critical data). `stat_term_id` must always be specified.
`threshold_OVER` <<`1;1`>> ((1 to 99))	Specify a warning threshold excess count and a critical threshold excess count. Separate the threshold values with a semicolon (;).

#1

Some resource may use different defaults.

#2

Because this item is intended to maintain compatibility with earlier versions, this item is ignored regardless of whether `Y` or `N` is specified.

When coding a subresource definition, note the following:

- If you want to set a different collection condition for each instance, define as many collection conditions as the number of subresources after the instance definition.
- If you want to set a common collection condition for all instances, define as many collection conditions as the number of subresources after the resource definition.
- As a rule, when you omit an optional definition item, you can only omit the value; you must write the key name and an equal sign (=). When you omit the collection mode (key name: `subcondition`) or the threshold excess count (key name: `threshold_OVER`), however, you must omit the entire field -- including the key name.

- If the number of subresource definitions contained in an instance definition exceeds the number (*n*) of subresources belonging to the instance, only the first to *n*-th definitions will be treated as valid. The subsequent collection conditions will be ignored.
- If you define both `condition` and `subcondition` in a resource definition, the definition of `subcondition` takes effect in the subresource for which `subcondition` is defined.
- For details about the automated action, see *2.2.3(4) Automated action*.

(5) Examples

An example of a collection conditions definition file is given below.

Example of collection conditions definition file (Interface Utilization):

```
# Interface Utilization
target=30;2o4gsv01                          } Resource definition
interval=20
d_range=06:00:00;23:00:00
instance=1                                  } Instance definition
subcondition=Y;Y;Y                          }
commandUM=                                  }
commandUK=                                  }
commandNM=                                  } Subresource defition (Max)
commandWR=                                  }
commandCR=                                  }
threshold=90.00;95.00                       }
threshold_OVER=1;2                          }
subcondition=N;N;N                          }
commandUM=                                  }
commandUK=                                  }
commandNM=                                  } Subresource definition (Average)
commandWR=                                  }
commandCR=                                  }
threshold=100.00;100.00                     }
threshold_OVER=1;1                          }
instance=2                                  } Instance definition
subcondition=Y;Y;Y                          }
commandUM=                                  }
commandUK=                                  }
commandNM=                                  } Subresource defition (Max)
commandWR=                                  }
commandCR=                                  }
threshold=95.00;98.00                       }
threshold_OVER=2;3                          }
subcondition=N;N;N                          }
commandUM=                                  }
commandUK=                                  }
commandNM=                                  } Subresource definition (Average)
commandWR=                                  }
commandCR=                                  }
threshold=100.00;100.00                     }
threshold_OVER=1;1                          }
```

Example of collection conditions definition file (CPU Utilization):

```
# CPU Using Rate
target=32;netmps01
interval=15
d_range=07:00:00;22:00:00
subcondition=Y;Y;Y
commandUM=
commandUK=
commandNM=
commandWR=cmd /q /c D:\JP1Cm2\SSO\minor.bat
commandCR=cmd /q /c D:\JP1Cm2\SSO\critical.bat
threshold=90.00;98.00
threshold_OVER=3;5
subcondition=N;N;N
commandUM=
commandUK=
commandNM=
commandWR=
commandCR=
threshold=100.00;100.00
threshold_OVER=1;1
subcondition=N;N;N
commandUM=
commandUK=
commandNM=
commandWR=
commandCR=
threshold=100.00;100.00
threshold_OVER=1;1
subcondition=N;N;N
commandUM=
commandUK=
commandNM=
commandWR=
commandCR=
threshold=100.00;100.00
threshold_OVER=1;1
```

Resource definition

Subresource difinition (Total CPU)

Subresource difinition (User CPU)

Subresource difinition (System CPU)

Subresource difinition (Wait CPU)

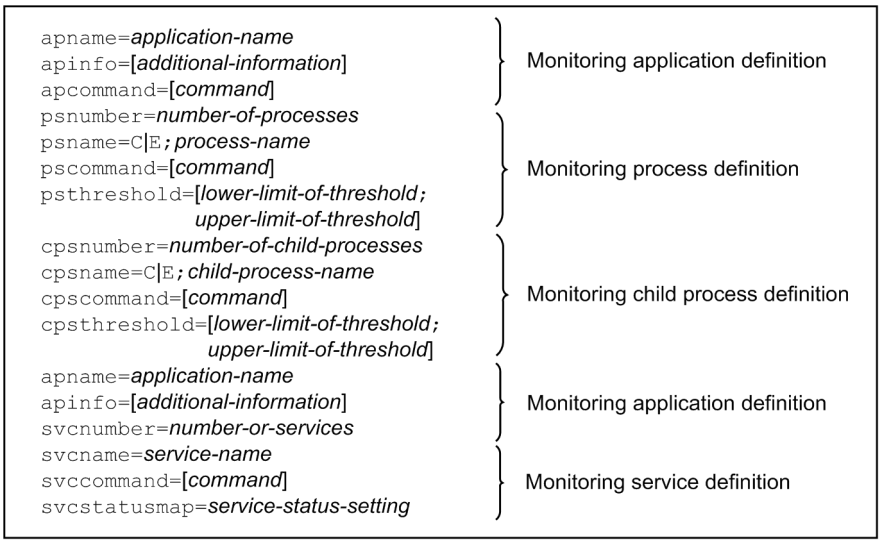
Example of collection conditions definition file (regular statistical threshold calculation)

6.3.2 Monitoring app definition file

If you want to monitor one or more processes, use the monitoring app definition file to define the applications, processes, child processes, and services to be monitored.

(1) Format

In a monitoring app definition file, you can define multiple applications to be monitored. The definition for an application to be monitored consists of multiple definitions. These definitions include the definition of the application and the definitions of one or more processes or services (included in the application). Definitions of child processes might also exist (included in the processes). The format of a monitoring app definition file is as follows:



(2) Details of monitored application definition

Define the applications to be monitored by APM. You must write a monitored application definition for each application to be monitored.

The next table lists the items that constitute a monitored application definition.

Key name	Value
apname ((character string of up to 128 bytes))	Specify the name of the application to be monitored. You cannot specify a semicolon (;), comma (,), tab, and multibyte code.
apinfo ((character string of up to 128 bytes))	Specify additional information for the application to be monitored. You cannot specify a semicolon (;), tab, and multibyte code.
apcommand ((character string of up to 160 bytes))	Specify the application start or stop remote command. You can specify the application start or stop remote command more than once. To specify multiple commands, write the key name apcommand for each command to be executed on multiple lines as follows: Example: apcommand=cmd /q /c C:\abc.bat apcommand=cmd /q /c C:\def.bat apcommand=cmd /q /c C:\ghi.bat
psnumber ((integer of 1 or above))	Specify the number of processes to be registered in the application.
svcnumber ((integer of 1 or above))	Specify the number of services to be registered in the application.

When coding a monitored application definition, note the following:

- When you omit an optional definition item, you can only omit the value; you must write the key name and an equal sign (=).
- If a single definition file contains more than one definition with the same value of apname, only the first application definition will be regarded as valid and the other application definitions will be ignored.
- If two or more identical values are assigned to an item that accepts multiple specifications, only the first specification will be regarded as valid and the other specifications will be ignored.

- You cannot specify `psnumber` and `svcnumber` together under a single `apname` key.
- For remote commands, see *2.5.2(4) Automated actions and remote commands*.

(3) Details of definitions of processes to be monitored

Define the processes to be monitored by APM. You must write the same number of process definitions as the value assigned to `psnumber` in the monitored application definition.

The next table lists the items that constitute a monitored process definition. For information on process types, see *2.5 Process and service monitoring function*.

Key name	Value
`psname` ((C or E;character string of up to 60 bytes))	Specify semicolon-separated pair consisting of the type and name of the process to be monitored. If the process type is a command line name, specify `C`. If it is an executable file name, specify `E`. If the monitoring server runs on Windows, exclude the extension `.exe` from the process name. You can use an asterisk (`*`) or question mark (`?`) as a wild card.

`pscommand`
((character string of up to 160 bytes))
	Specify the process start or stop remote command. You can specify the process start or stop remote command more than once. To specify multiple commands, write the key name `pscommand` for each command to be executed on multiple lines as follows:
	Example:
	`pscommand=cmd /q /c C:\abc.bat`
	`pscommand=cmd /q /c C:\def.bat`
	`pscommand=cmd /q /c C:\ghi.bat`

`psthreshold` <<1;1>> ((0 to 9999))	Specify a semicolon-separated pair consisting of the upper and lower limits of the threshold (the number of processes to be started at the same time). The upper limit must be equal to or greater than the lower limit.
`cpsnumber` ((integer of 0 or above))	Specify the number of child processes to be registered in the process. If you specify `0`, you need not define the child processes to be monitored.

When coding a monitored process definition, note the following:

- When you omit an optional definition item, you can only omit the value; you must write the key name and an equal sign (=).
- If two or more identical values are assigned to an item that accepts multiple specifications, only the first specification will be regarded as valid and the other specifications will be ignored.
- If a single definition file contains more than one definition with the same value of `psname`, only the first process definition will be regarded as valid and the other process definitions will be ignored.
- For remote commands, see *2.5.2(4) Automated actions and remote commands*.

(4) Details of definitions of child processes to be monitored

Define the child processes to be monitored by APM. You must define the same number of child process definitions as the value assigned to `cpsnumber` in the monitored process definition.

The next table lists the items that constitute a monitored child process definition. For information on child process types, see *2.5 Process and service monitoring function*.

Key name	Value
`cpsname`	Specify a semicolon-separated pair consisting of the type and name of the child process to be monitored. If the child process type is a command line name, specify `C`. If it is an executable file name, specify `E`.

Key name	Value
((character string of up to 60 bytes))	If the monitoring server runs on Windows, exclude the extension `.exe` from the process name. You can use an asterisk (`*`) or question mark (`?`) as a wild card.

`cpscommand`
((character string of up to 160 bytes))
	Specify the child process start or stop remote command. You can specify the child process start or stop remote command more than once. To specify multiple commands, write the key name `cpscommand` for each command to be executed on multiple lines as follows:
	Example:
	`cpscommand=cmd /q /c C:\abc.bat`
	`cpscommand=cmd /q /c C:\def.bat`
	`cpscommand=cmd /q /c C:\ghi.bat`

`cpsthreshold` <<1;1>> ((0 to 9999))	Specify a semicolon-separated pair consisting of the upper and lower limits of the threshold (the number of child processes which are to be started at the same time). The upper limit must equal to or greater than the lower limit.

When coding a monitored child process definition, note the following:

- When you omit an optional definition item, you can only omit the value; you must write the key name and an equal sign (=).
- If a single definition file contains more than one definition with the same value of `cpsname`, specification will be regarded as valid and the other specifications will be ignored.
- If one monitored process definition contains two or more child process definitions that have the same value assigned to the key name `cpsname`, only the first child process definition will be regarded as valid and the other child process definitions will be ignored.
- For remote commands, see *2.5.2(4) Automated actions and remote commands*.

(5) Details of definitions of services to be monitored

Define the services to be monitored by APM. You must write the same number of service definitions as the value assigned to `svcnumber` in the monitoring application definition. The next table lists the items that constitute a monitored service definition.

Key name	Value
`svcname` ((character string of up to 100 bytes))	Specify a service name. You cannot use a semicolon (`;`) in the service name. An asterisk (`*`) or question mark (`?`) specified in a service name is not treated as a wild card but treated as a normal character. You cannot monitor services by using their service display names.

`svccommand`
((character string of up to 160 bytes))
	Specify the service start or stop remote command. You can specify the child service start or stop remote command more than once. To specify multiple commands, write the key name `svccommand` for each command to be executed on multiple lines as follows:
	Example:
	`svccommand=net start xxxxx`
	`svccommand=net stop yyyyy`
	`svccommand=cmd /q /c C:\abc.bat`

`svcstatusmap`	Specify each state of the service to be monitored as normal or critical state. Write the key name, and specify normal or critical for service states, such as *Running*, *Stopped*, *Paused*, *Starting*, *Stopping*, *Pausing*, and *Resuming*, in this order. Delimit the states with a semicolon (`;`). Specify `N` for a state to be treated as a normal state or `C` for a state to be treated as a critical state.

When coding a monitored service definition, note the following:

- When you omit an optional definition item, you can only omit the value; you must write the key name and an equal sign (=).
- If two or more identical values are assigned to an item that accepts multiple specifications, only the first specification will be regarded as valid and the other specifications will be ignored.
- If the definition for an application to be monitored includes multiple `svcname` key values defined for the same service to be monitored, the `svcname` value defined first is assumed to be valid. The other `svcname` values are assumed to be invalid.
- For remote commands, see *2.5.2(4) Automated actions and remote commands*.

(6) Example

An example of a monitoring app definition file is given below.

```
#
# definition file
#
##
apname=JP1/Cm2/SSO (Windows)                                  } Application definition
apinfo=JP1/Cm2/SNMP System Observer (Windows)                 }
apcommand=                                                    }
psnumber=2                                                    }
##
psname=E;ssospmd                                              } Process definition
pscommand=                                                    }
psthreshold=1;1                                               }
cpsnumber=2                                                   }
#
cpsname=E;ssocollectd                                         } Child process definition
cpscommand=                                                   }
cpsthreshold=1;9999                                           }
cpsname=E;ssocolmng                                           } Child process definition
cpscommand=                                                   }
cpsthreshold=1;9999                                           }
##
psname=E;ssorptd                                              } Process definition
pscommand=                                                    }
psthreshold=1;1                                               }
cpsnumber=0                                                   }

##
apname=JP1/Cm2/SSO - Agent for Process                        } Application definition
apinfo=JP1/Cm2/SNMP System Observer - Agent for Process       }
apcommand=                                                    }
svcnumber=1                                                   }
svcname=Cm2APM                                                } Service definition
svccommand=                                                   }
svcstatusmap=N;C;C;C;C;C;C                                    }
```

6.3.3 Monitoring server definition file

If you want to monitor processes or services, use the monitoring server definition file to define the details of monitoring, including monitoring servers and monitoring intervals.

(1) Format

In a monitoring server definition file, you can define multiple monitoring servers. The following is a format for the monitoring server definition file.

```
server=monitoring-server-name
monitor=[monitoring-interval]
hcheck=[health-check-time]
```

(2) Items to be specified in the monitoring server definition file

The next table lists the items that must be or can be defined in a monitoring server definition file. You must write a set of these definition items for each monitoring server.

Key name	Value
`server` ((character string of up to 255 bytes))	Specify the name or IP address of the host on which the process to be monitored operates.
`monitor` <<1>> ((1 to 60 minutes))	Specify the interval at which the process is to be monitored.
`hcheck` <<0>> ((0 to 525,600 minutes))	Specify the interval at which health check is to be regularly executed. If you specify `0`, health check is not executed regularly.

When coding a monitoring server definition, note the following:

- When you omit an optional definition item, you can only omit the value; you must write the key name and an equal sign (=).
- If a single definition file contains more than one definition with the same value of `server`, only the first process definition will be regarded as valid and the other process definitions will be ignored.

(3) Example

The following gives an example of a monitoring server definition file.

```
#
# definition file
#
server=100.100.100.100
monitor=5
hcheck=0
server=100.100.100.101
monitor=
hcheck=
```

(4) Note

If monitoring server setting information is output by the `ssopsset` command with the `-sp` option specified when the monitoring server is stopped, a hyphen (`-`) is set for the `monitor` key in the output information.

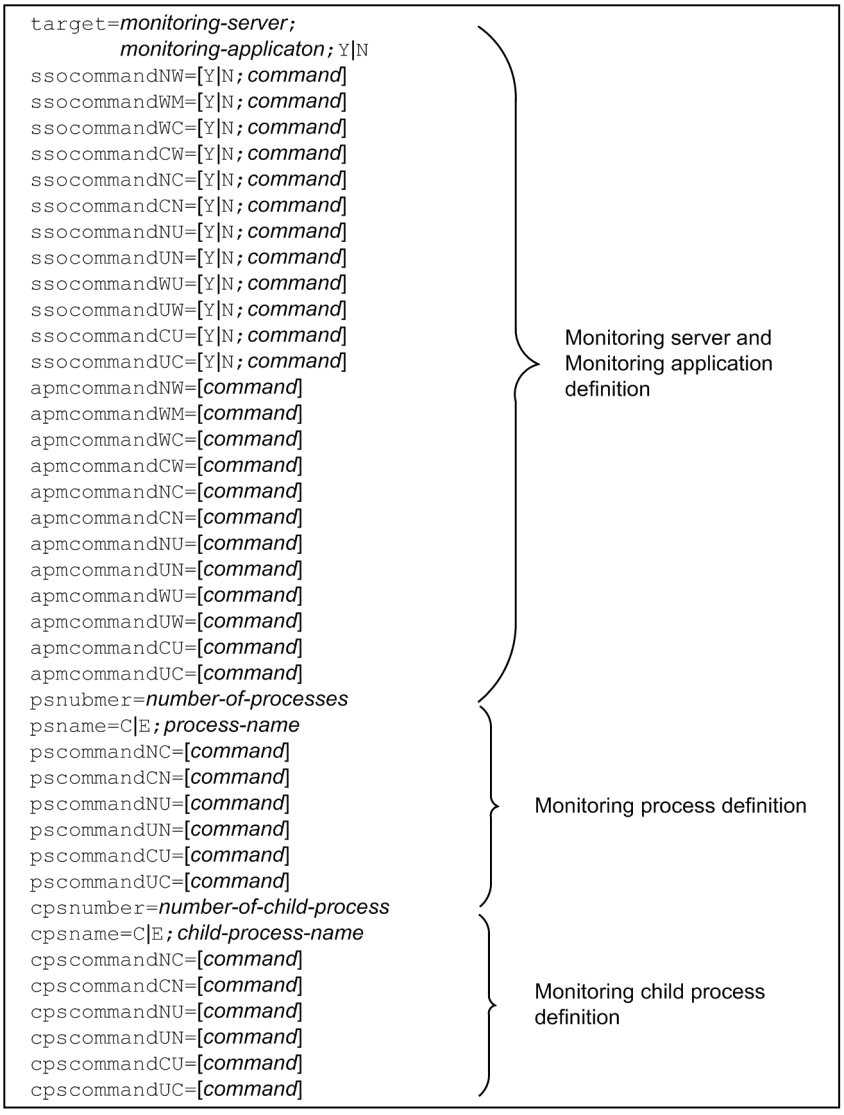
If a monitoring server definition file specifying a hyphen (`-`) in the monitor key is read by the `ssopsset` command with the `-ss` or `-ssn` option specified, monitoring starts with existing settings when the monitoring server is running. If, in such a case, the monitoring server is not running, the monitoring interval is not set by the command.

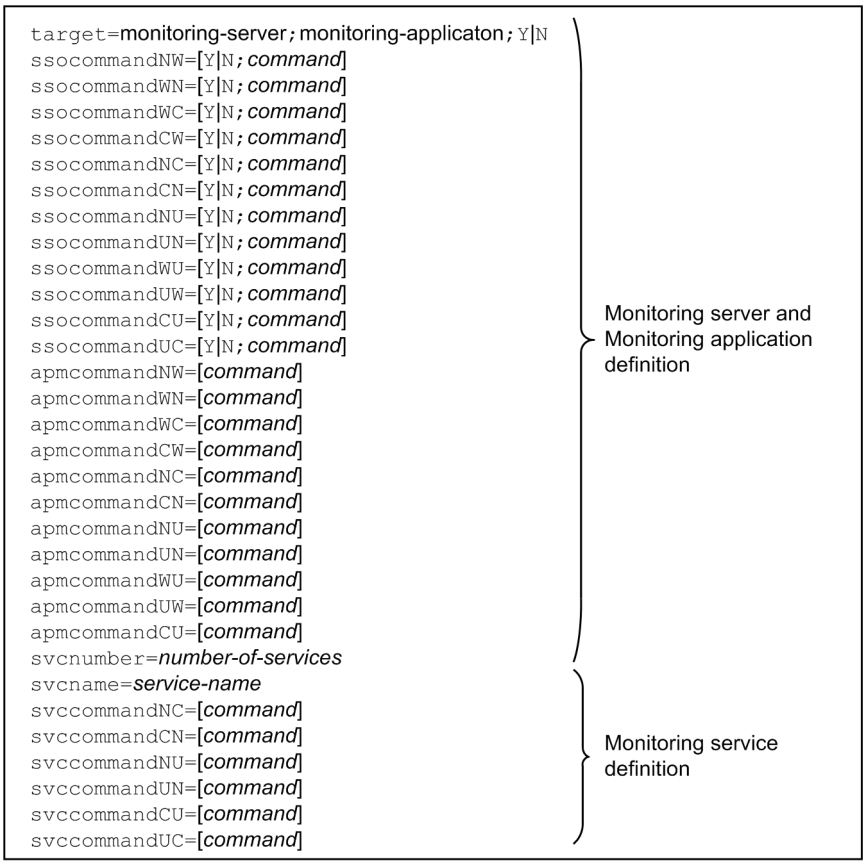
6.3.4 Monitoring condition definition file

In the monitoring condition definition file, define the conditions for monitoring the processes or services of applications.

(1) Format

In a monitoring condition definition file, you can define multiple sets of monitoring conditions. The format of a monitoring condition definition file is as follows:





(2) Details of definitions of servers and applications to be monitored

Define the conditions for monitoring servers and applications. You must write a monitoring server/application definition for each pair consisting of a server to be monitored and an application to be monitored. The next table lists the items that constitute a monitoring server/application definition.

Key name	Value
target	Specify a monitoring server name, application name, and symbol display setting, separate these items with semicolons (;). • Specify a host name or IP address of up to 255 bytes as the monitoring server name. • Specify the application name in up to 128 bytes. • To display symbols, specify Y. If you do not wish to display symbols, specify N.#
ssocommandNW	• If the application state changes, specify whether to execute commands on the SSO side and the names of the commands to be executed. Specify the command names, separated with semicolons (;). • To execute a command, specify Y. If you do not wish to execute a command, specify N. • Specify a command name in up to 160 bytes.
ssocommandWN	
ssocommandWC	
ssocommandCW	
ssocommandNC	
ssocommandCN	
ssocommandNU	
ssocommandUN	
ssocommandWU	
ssocommandUW	

Key name	Value
ssocommandCU ssocommandUC	• If the application state changes, specify whether to execute commands on the SSO side and the names of the commands to be executed. Specify the command names, separated with semicolons (;). • To execute a command, specify Y. If you do not wish to execute a command, specify N. • Specify a command name in up to 160 bytes.
apmcommandNW apmcommandWN apmcommandWC apmcommandCW apmcommandNC apmcommandCN apmcommandNU apmcommandUN apmcommandWU apmcommandUW apmcommandCU apmcommandUC	• If the application state changes, specify the names of the remote command to be executed on the APM side. • You can specify multiple commands. To specify multiple commands, write the corresponding key name for each command to be executed on multiple lines as follows: Example: apmcommandNW=cmd /q /c C:\abc.bat apmcommandNW=cmd /q /c C:\def.bat apmcommandNW=cmd /q /c C:\ghi.bat • Specify a command name in up to 160 bytes.
psnumber ((integer of 1 or above))	Specify the number of the processes to be registered in the application.
svcnumber ((integer of 1 or above))	Specify the number of the services to be registered in the application.

#

Because this item is intended to maintain compatibility with earlier versions, this item is ignored regardless of whether Y or N is specified.

When defining server and process monitoring conditions, note the following:

- When you omit an optional definition item, you can only omit the value; you must write the key name and an equal sign (=).
- If a single definition file contains more than one definition with the same value of target, only the first process definition will be regarded as valid and the other process definitions will be ignored.
- If two or more identical values are assigned to an item that accepts multiple specifications, only the first specification will be regarded as valid and the other specifications will be ignored.
- You cannot specify psnumber and svcnumber together under a single target key.
- For automated actions and remote commands, see *2.5.2(4) Automated actions and remote commands*.

(3) Details of definitions of processes to be monitored

Define process monitoring conditions. The next table lists the items to be specified as process monitoring conditions. For information on process types, see *2.5 Process and service monitoring function*.

Key name	Value
psname	Specify a semicolon-separated pair consisting of the type and name of the process to be monitored. • If the process type is a command line name, specify C. If it is an executable file name, specify E.

Key name	Value
psname	• Specify the process name in up to 60 bytes.
pscommandNC pscommandCN pscommandNU pscommandUN pscommandCU pscommandUC	• Specify the command to be executed via automated action when the process status changes. • Specify a command name in up to 160 bytes. • You can specify multiple commands. To specify multiple commands, write the corresponding key name for each command to be executed on multiple lines as follows: Example: pscommandNC=cmd /q /c C:\abc.bat pscommandNC=cmd /q /c C:\def.bat pscommandNC=cmd /q /c C:\ghi.bat
cpsnumber ((integer of 0 or above))	Specify the number of child processes to be registered in the process. If you specify 0, you need not define the child process to be monitored.

When defining monitoring conditions for a monitored process, note the following:

- When you omit an optional definition item, you can only omit the value; you must write the key name and an equal sign (=).
- If a single definition file contains more than one definition with the same value of psname, only the first process definition will be regarded as valid and the other process definitions will be ignored.
- If two or more identical values are assigned to an item that accepts multiple specifications, only the first specification will be regarded as valid and the other specifications will be ignored.
- For automated actions and remote commands, see *2.5.2(4) Automated actions and remote commands*.

(4) Details of definitions of child processes to be monitored

Define monitoring conditions for the child processes to be monitored. The next table lists the items to be specified as child process monitoring conditions. For child process types, see *2.5 Process and service monitoring function*.

Key name	Value
cpsname	Specify a semicolon-separated pair consisting of the type and name of the child process to be monitored. • If the child process type is a command line name, specify C. If it is an executable file name, specify E. • Specify the name of the child process to be monitored in up to 60 bytes.
cpscommandNC cpscommandCN cpscommandNU cpscommandUN cpscommandCU cpscommandUC	• Specify the command to be executed via automated action when the child process status changes. • Specify a command name in up to 160 bytes. • You can specify multiple commands. To specify multiple commands, write the corresponding key name for each command to be executed on multiple lines as follows: Example: cpscommandNC=cmd /q /c C:\abc.bat cpscommandNC=cmd /q /c C:\def.bat cpscommandNC=cmd /q /c C:\ghi.bat

When coding a monitored child process definition, note the following:

- When you omit an optional definition item, you can only omit the value; you must write the key name and an equal sign (=).
- If a single definition file contains more than one definition with the same value of cpsname, only the first child process definition will be regarded as valid and the other child process definitions will be ignored.

- If two or more identical values are assigned to an item that accepts multiple specifications, only the first specification will be regarded as valid and the other specifications will be ignored.
- For automated actions and remote commands, see *2.5.2(4) Automated actions and remote commands*.

(5) Details of definitions of services to be monitored

The next table lists the items to be specified as service monitoring conditions.

Key name	Value
`svcname`	Specify a service name. • Specify a service name in up to 160 bytes. • You cannot use a semicolon (`;`) in the service name.

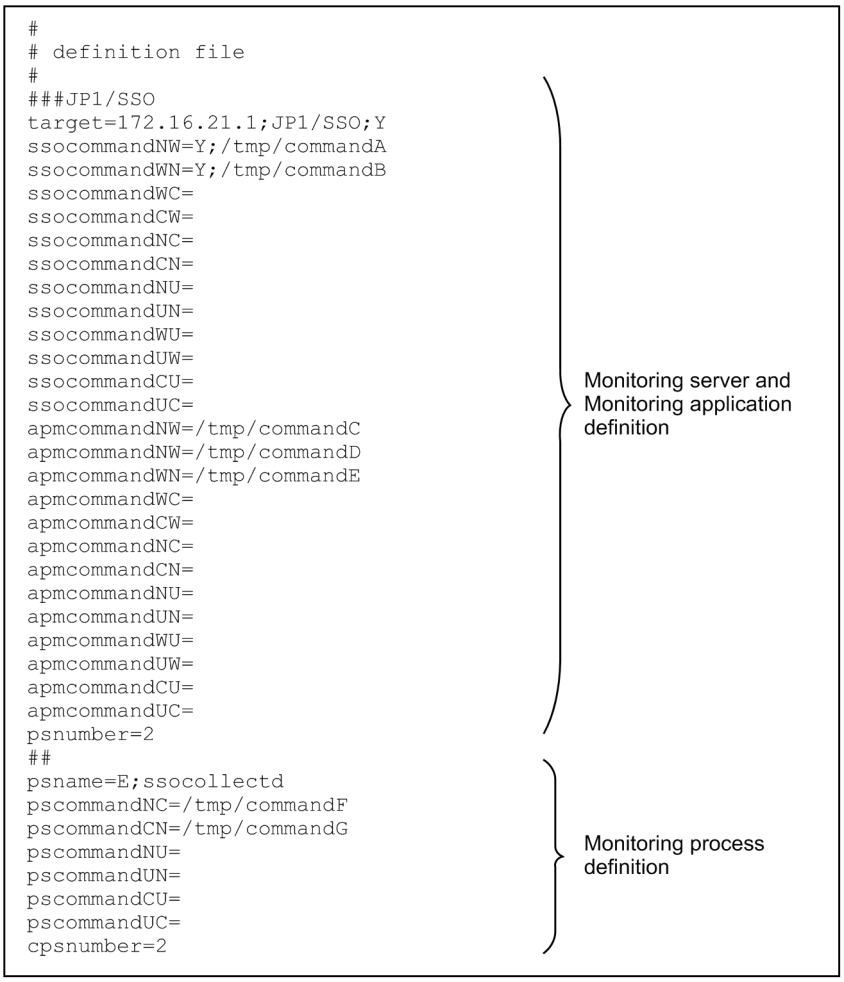
`svccommandNC`
`svccommandCN`
`svccommandNU`
`svccommandUN`
`svccommandCU`
`svccommandUC`
	• Specify the command to be executed via automated action when the service status changes.
	• Specify a command name in up to 160 bytes.
	• You can specify multiple commands. To specify multiple commands, write the corresponding key name for each command to be executed on multiple lines as follows:
	Example:
	`svccommandNC=cmd /q /c C:\abc.bat`
	`svccommandNC=cmd /q /c C:\def.bat`
	`svccommandNC=cmd /q /c C:\ghi.bat`

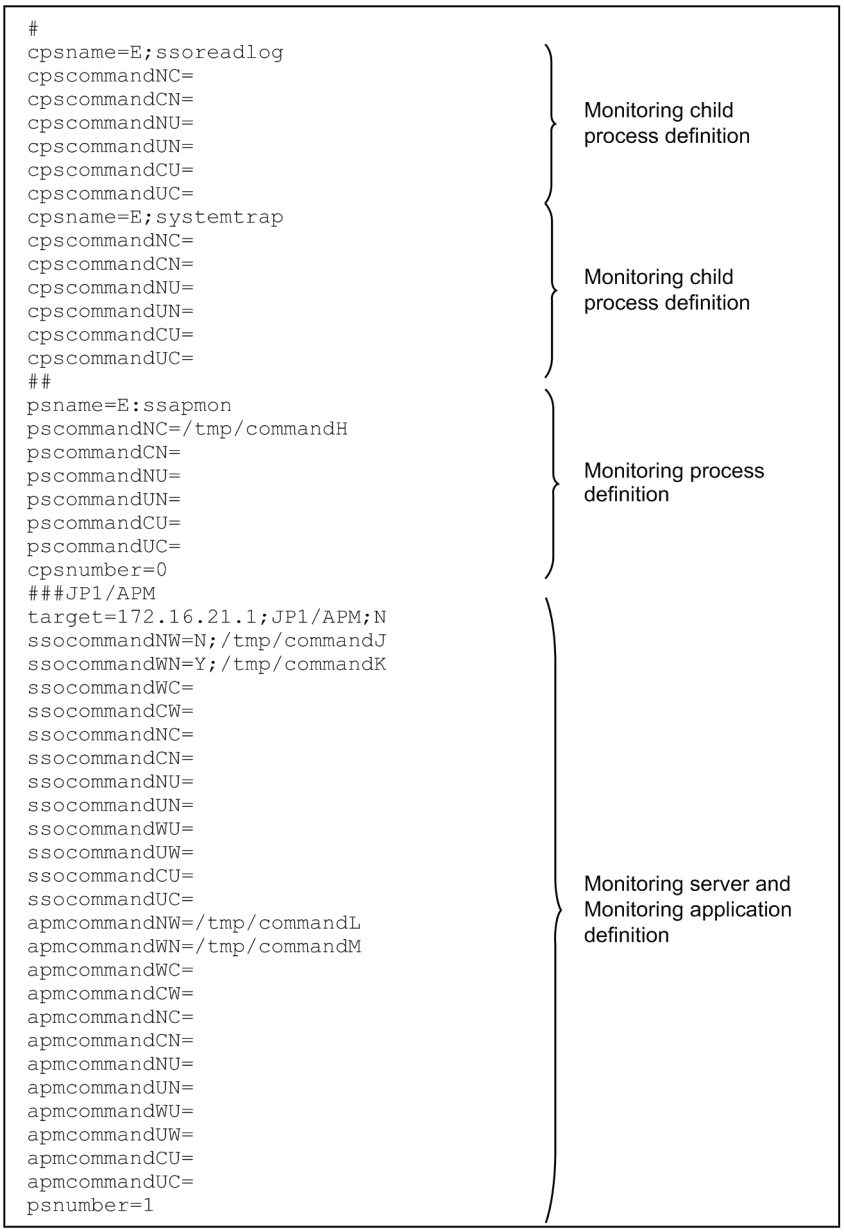
The next table lists the items to be specified as service monitoring conditions.

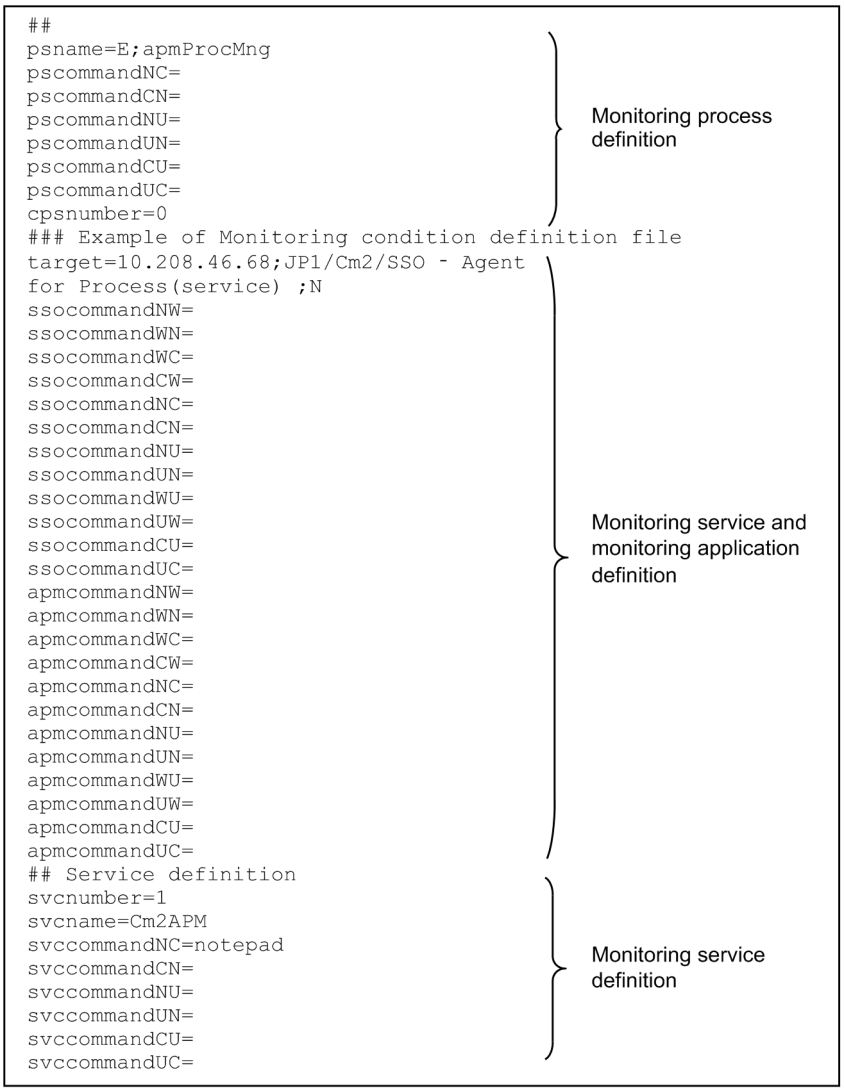
- When you omit an optional definition item, you can only omit the value; you must write the key name and an equal sign (=).
- If the same value is written in more than one instance of a field multiple entries of which are allowed, the field defined first is assumed to be valid, and the fields defined subsequently are assumed to be invalid.
- If multiple `svcname` key values (service names) are specified for the same monitoring service in one monitoring server and monitoring application definition, only the first specified value is valid, and the other values are invalid.
- Write the same number of service definitions as the value assigned to `svcnumber` in the definitions for the monitoring server and monitoring application.
- For automated actions and remote commands, see *2.5.2(4) Automated actions and remote commands*.

(6) Example

The following gives an example of a monitoring condition definition file.


#
definition file
#
###JP1/SSO
target=172.16.21.1;JP1/SSO;Y
ssocommandNW=Y;/tmp/commandA
ssocommandWN=Y;/tmp/commandB
ssocommandWC=
ssocommandCW=
ssocommandNC=
ssocommandCN=
ssocommandNU=
ssocommandUN=
ssocommandWU=
ssocommandUW=
ssocommandCU=
ssocommandUC=
apmcommandNW=/tmp/commandC
apmcommandNW=/tmp/commandD
apmcommandWN=/tmp/commandE
apmcommandWC=
apmcommandCW=
apmcommandNC=
apmcommandCN=
apmcommandNU=
apmcommandUN=
apmcommandWU=
apmcommandUW=
apmcommandCU=
apmcommandUC=
psnumber=2
##
psname=E;ssocollectd
pscommandNC=/tmp/commandF
pscommandCN=/tmp/commandG
pscommandNU=
pscommandUN=
pscommandCU=
pscommandUC=
cpsnumber=2
Monitoring server and Monitoring application definition
Monitoring process definition


#
cpsname=E;ssoreadlog
cpscommandNC=
cpscommandCN=
cpscommandNU=
cpscommandUN=
cpscommandCU=
cpscommandUC=
Monitoring child process definition
cpsname=E;systemtrap
cpscommandNC=
cpscommandCN=
cpscommandNU=
cpscommandUN=
cpscommandCU=
cpscommandUC=
Monitoring child process definition
##
psname=E:ssapmon
pscommandNC=/tmp/commandH
pscommandCN=
pscommandNU=
pscommandUN=
pscommandCU=
pscommandUC=
cpsnumber=0
Monitoring process definition
###JP1/APM
target=172.16.21.1;JP1/APM;N
ssocommandNW=N;/tmp/commandJ
ssocommandWN=Y;/tmp/commandK
ssocommandWC=
ssocommandCW=
ssocommandNC=
ssocommandCN=
ssocommandNU=
ssocommandUN=
ssocommandWU=
ssocommandUW=
ssocommandCU=
ssocommandUC=
apmcommandNW=/tmp/commandL
apmcommandWN=/tmp/commandM
apmcommandWC=
apmcommandCW=
apmcommandNC=
apmcommandCN=
apmcommandNU=
apmcommandUN=
apmcommandWU=
apmcommandUW=
apmcommandCU=
apmcommandUC=
psnumber=1
Monitoring server and Monitoring application definition



6.3.5 Group definition file

In the group definition file, define the information for grouping monitoring target server names, resource IDs, or monitoring application names. Grouping enables you to monitor multiple servers under the same collection and monitoring conditions. For process monitoring, the monitoring start time can be offset for each server group.

(1) Format

In a group definition file, write a group name, and list, on subsequent lines, monitoring target server names, resource IDs, or monitoring application names as member names. Write a semicolon (;) after each group name. In a group definition file, you can define multiple groups.

When coding definitions in a group definition file, note the following:

- Each statement must start at the beginning of a line.
- The specified group name must be within 20 bytes.
- No group name or member name may contain a space, tab, or new line characters.
- No group name may contain a semicolon (`;`).

- Member names must follow the format rules for command options. Member names, however, cannot be delimited with a comma (`,`).
- If two or more group definitions have the same group name, only the first specified group definition will be treated as valid and the other group definitions will be ignored. If one group definition has two or more identical member names, only the first specified member name will be treated as valid and the other member names will be ignored.

(2) Example

The following give an example of a group definition file.

```
#Monitoring target server group
server-GrpA;                          Group name (server group)
133.108.120.14                        }
133.108.120.15                        } Member names (monitoring target server names)
133.108.120.16                        }
2001:0db8::1234:5678:90ab:cdef        }

#Resource ID group
resource-GrpA;                        Group name (resource group)
1                                     }
2                                     } Member names (resource IDs)
3                                     }

#Monitoring application group
application-GrpA;                     Group name (monitoring application group)
JP1/SSO                               }
JP1/NNM                               } Member names (monitoring application names)
```

6.3.6 SNMP definition file (ssosnmp.conf)

In the SNMP definition file, specify definitions of SNMP requests to be issued by SSO. If you have changed this file, perform one of the following operations:

- Execute the `ssoapcom` and `ssocollectd` commands with the `-r` option specified to re-read the file.
- Restart the `ssoapmon` and `ssocollectd` daemon processes.

(1) Format

In the SNMP definition file, specify each SNMP agent definition on one line. Write the definition items in the order in which they are listed in the table in *(2) Description*, and delimit the items with a colon (`:`).

(2) Description

The next table lists the items that must be or can be defined in an SNMP definition file.

Entry name	Value
category-name	• For resource collection Specify a category name. To collect the resources provided by SSO, specify `sso` or `sso-ex`. To collect user resources, specify the category name. If you do not specify a category name, the `sso` definition becomes valid. • For process or service monitoring `process` definition becomes valid. If the `process` definition is not found, the definition specifying `sso` becomes valid. If neither `process` nor `sso` is defined, the default is set.

Entry name	Value
category-name	The specified category name is not case sensitive.
IP-address	Specify the IP address of the target agent. The specification format varies between IPv4 and IPv6. For IPv4, specify the IP address in the *n*.*n*.*n*.*n* format. For *n*, specify a value from 0 to 255 or an asterisk (*) as a wild card. For IPv6, specify the IP address in the [*x*:*x*:*x*:*x*:*x*:*x*:*x*:*x*] format. For *x*, specify a value from 0 to FFFF or an asterisk (*) as a wild card. The default value of each item is set in undefined agents.
get-community-name <<public>> ((character string of up to 255 bytes))	Set the community name to be used when an SNMP Get/Get-Next request is issued to the target agent. You cannot specify a colon (:).
set-community-name <<*get-community-name*>> ((character string of up to 255 bytes))	Set the community name to be used when an SNMP Set request is issued to the target agent. You cannot specify a colon (:).
response-monitoring-time <<20>> ((1 to 990))	Specify, in units of 1/10 seconds, the response monitoring time to be used when an SNMP request is issued to the target agent.
retry-count <<3>> ((0 to 99))	Specify the number of retries to be attempted when an SNMP request is issued to the target agent.
port-number <<161>> ((1 to 65535))	Specify the port number to be used when an SNMP request is issued to the target agent.
SNMP-proxy-IP-address#1	The proxy IP address for issuing an SNMP request to the target agent is specified in the format of *n.n.n.n*. For *n*, specify a value from 0 to 255.
SNMP-version <<1>>#2, #3	Specify the version of SNMP to be used to collect user resources if the name of a user resource category is specified as the category name. The specifiable values are 1 or 2. 1: Use SNMP Version 1 (SNMPv1) to issue requests. 2: Use SNMP Version 2 (SNMPv2c) to issue requests. This item is ignored when it is specified on a line where sso, sso-ex, or process is specified as the category name.

#1

When omitting specification of the SNMP proxy IP address and SNMP version that follows, you can also omit the delimiter (:).

#2

When omitting specification of the SNMP version, you can also omit the delimiter (:) that is to be specified at the end of the value.

#3

The SNMP version is fixed to 1 for the sso and process categories. If you intend to acquire Counter64-type MIB values during user resource collection, always specify 2 for the IP address and port number of the collection target agent.

If the collection target agent does not support SNMP Version 1, you can collect user resources by specifying 2 for the SNMP version. In such a case, however, you can neither reference resources nor collect the resources in category sso.

When coding definitions in an SNMP definition file, note the following:

- If the file includes multiple definitions that use the same combination of category name and IP address, the definition written first is assumed to be valid, and the definitions written subsequently are ignored.
- If the definition file includes multiple definitions that define the same category name and the IP address (that might include wild cards) corresponding to a common IP address, the definition written first is valid for the common IP address. Therefore, if a definition specifying *.*.*.* or *:*:*:*:*:*:*:* for the IP address of the target agent is written as the top, the SNMP request following the definition will be issued to all agents.

- If the definition file includes multiple category definitions for the same IP address, those definitions can be written in any order. For example, if an sso definition and an sso-ex definition are to be written for the same IP address, both definitions are always valid regardless of the order of writing.
- If the category and target of the resource that issues the SNMP request are not defined, the definition of category name `sso` becomes valid.
- If the process monitoring category `process` and monitoring target are not defined for issuing the SNMP request, the definition of category name `sso` becomes valid.

(3) Example

The following is an example of an SNMP definition file.

```
#
# ssosnmp.conf
#
# FORMAT
# Category:IPaddress:GetCommunity:SetCommunity:TimeOut:Retry:Port:
  Proxy:SNMPVersion:
#
# 1. IP Address
sso:172.16.43.61:public:secret:8:2::
sso-ex:172.16.43.61:public:secret:8:2:8161:
sso:172.16.43.137:public:public:10:2::
sso:172.16.45.41:172.16.45.41:172.16.45.41::::172.16.45.200:
sso:[2001:0db8::1234:5678:90ab:cdef]::secret:10:3:::
user:172.16.110.10:usr::20:2:161::
# 2. IP Address Wildcards
sso:172.16.43.*:public:jp1sso:20:2:::
sso:172.16.45.*:public:jp1sso:8:2:::
sso:172.19.*.*:public::10:3:::
user:172.20.*.*:public:secret:::50161::2:
user:[2001:0db8::1234:*:*:*]::secret:20:3:161::
# 3. Default
sso-ex:*.*.*.*:public:public:20:3::::
sso:*.*.*.*:public:public:8:2:161::
process:*.*.*.*:public:public:20:3:161::
sso-ex:[*:*:*:*:*:*:*:*]:public:public:20:3::::
sso:[*:*:*:*:*:*:*:*]:public:public:8:2:161:::
```

In this example, when you collect SSO-Ex resources for target 100.100.100.2, the definition of `sso-ex:*.*.*.*:public:public:20:3::::` becomes valid. When you collect user resources for the same target, the definition of `sso:*.*.*.*:public:public:8:2:161::` becomes valid.

6.3.7 ssoapmon action definition file (ssoapmon.def)

The `ssoapmon` action definition file contains definitions of `ssoapmon` daemon process actions. If you have made any changes in this definition file, perform one of the following operations to apply these changes:

- Execute the `ssoapcom -r` command.

  Note that the changes might not become valid depending on the key that has been changed.
- Restart the `ssoapmon` daemon process.

(1) Format

The following is a format for the `ssoapmon` action definition file.

```
[threshold-event:          on|off]
[status-event:             on|off]
[nnm-urlaction-coop:       on|off]
[nnm-map-coop:             on|off]
[map-status-warning:       warning | minor | major | critical]
[map-status-critical:      major | critical]
[max-client:               maximum-number-of-concurrent-connections-with-GUI-and-
command]
[change-my-address:        IP-address]
[snmp-address:             logical-IP-address]
[max-snmp-session:         number-of-concurrent-SNMP-sessions-with-monitoring-server]
[max-logfile-size:         maximum-size-of-logging-file]
[logfile-num:              number-of-log-files]
[trace:                    on|off]
[max-tracefile-size:       maximum-size-of-trace-file]
[tracefile-num:            number-of-trace-files]
[event-lost-limit:         waiting-time-for-event-loss-detection]
[event-lost-retry:         number-of-retries-after-event-loss]
[omit-unknown-event:       on|off]
[snmp-dump:                on|off]
[max-dumpfile-size:        maximum-size-of-SNMP-packet-dump-trace-files]
[sso-start-hcheck-interval:  health-check-interval-at-SSO-start]
[sso-start-hcheck-delay:   health-check-delay-time-at-SSO-start]
[sso-start-hcheck-unit:    number-of-servers-whose-health-check-delays-at-SSO-startup]
[apm-start-hcheck-delay:   delay-in-starting-system-health-check-at-APM-start-event-reception]
[hcheck-retry-count:       health-check-number-of-retry]
[hcheck-retry-interval:    health-check-retry-interval]
[max-apmevtfile-size:      maximum-size-of-TCP-event-log-file]
[apmevtfile-num:           number-of-TCP-event-log-files]
[max-apm-session:          number-of-concurrently-receivable-TCP-events]
[connect-retry-interval:   TCP-connection-retry-interval]
[apm-incident-check-interval:  APM-incident-check-interval]
[apm-incident-delete:      on|off]
[max-incident-logfile-size:  size-of-incident-log-files]
[incident-logfile-num:     number-of-incident-log-files]
[fs-redirect:              on|off]
```

(2) Description

The next table lists the items that must be or can be defined in an `ssoapmon` action definition file.

Key name	Value
`threshold-event:` <<on>>	Specify whether to issue the process status change event, service status change event, and application status change event to NNMi. To issue these events, specify `on`. To not issue these events, specify `off`. Even when `on` is specified, the incidents that are filtered with the event filter definition file (`ssoevtfilter.conf`) will not be issued. Note that if `off` is specified, no event is issued even when destinations are specified in the event destination definition file (`ssodest.conf`).
`status-event:` <<on>>	Specify whether to issue the monitoring status change event to NNMi. To issue the event, specify `on`. To not issue the event, specify `off`. Even when `on` is specified, the incidents that are filtered with the event filter definition file (`ssoevtfilter.conf`) will not be issued. Note that if `off` is specified, no event is issued even when destinations are specified in the event destination definition file (`ssodest.conf`).
`nnm-urlaction-coop:`[#1] <<on>>	Specify whether to use the NNMi map cooperation function (action cooperation). To use the function, specify `on`. To not use the function, specify `off`.
`nnm-map-coop:`[#1] <<on>>	Specify whether to use the NNMi map cooperation function (symbol cooperation). To use the function, specify `on`. To not use the function, specify `off`.

Key name	Value
`map-status-warning:`[#1] <<minor>>	Specify the NNMi node status that corresponds to the warning-level application status for the NNMi map cooperation function (symbol cooperation). The warning-level application status can correspond to the `warning`, `minor`, `major`, or `critical` NNMi node status. For the correspondence between the application status on SSO and the status registered with NNMi, see *2.6.3(2) Correspondence between the statuses managed in SSO and the severity statuses registered in NNMi*.
`map-status-critical:`[#1] <<major>>	Specify the NNMi node status that corresponds to the critical-level application status for the NNMi map cooperation function (symbol cooperation). The caution-level application status can correspond to the `major` or `critical` NNMi node status. For the correspondence between the application status on SSO and the status registered with NNMi, see *2.6.3(2) Correspondence between the statuses managed in SSO and the severity statuses registered in NNMi*.
`max-client:`[#1] <<16>> ((1 to 99))	Specify the maximum number of concurrent sessions with the windows and commands[#2] that connect to the `ssoapmon` daemon process.
`change-my-address:`[#1] <<none>>	When the monitoring manager has multiple IP addresses or when it is operating in a cluster system, specify the operating IP address of SSO in the *n*.*n*.*n*.*n* format. (*n* is an integer from 0 to 255.) In other cases, specify `none`. • When the monitoring manager has multiple IP addresses: Specify an IP address at which SSO can communicate with the monitoring server. You can freely select one of the monitoring manager's IP addresses at which SSO can communicate with the monitoring server. • When operating SSO in a cluster system: Specify a logical IP address. The operating IP address of SSO defined in the `ssoapmon` action definition file is the destination IP address for the event that is issued by the APM on the monitoring server to the monitoring manager.
`snmp-address:` <<default>>	When operating SSO in a cluster system, specify a logical IP address in the *n*.*n*.*n*.*n* format. (*n* is an integer from 0 to 255.) By using this specification, you can use a fixed logical IP address as the monitoring manager IP address that is allowed to pass through the firewall located between the monitoring manager and monitored servers. If multiple logical IP addresses are available, specify the logical IP address at which the monitoring server can communicate with all monitored servers. In other cases, specify `default`. When `default` is specified, the local host IP address that enables communication with the monitoring server is used as the monitoring manager IP address that is allowed to pass through the firewall. If multiple local host IP addresses are available for this purpose, the monitoring manager IP address is undefined. Specification of this key is invalid for TCP health check.
`max-snmp-session:`[#1] <<32>> ((1 to 99))	Specify the maximum number of monitored servers that are concurrently connected to the monitoring server.
`max-logfile-size:` <<4>> ((1 to 32 megabytes))	Specify the maximum size of a log file.
`logfile-num:` <<3>> ((1 to 10))	Specify the number of the log files.
`trace:` <<off>>	Specify whether to output a trace file for troubleshooting at failure occurrence. To output the trace file, specify `on`. To not output the trace file, specify `off`.
`max-tracefile-size:` <<4>> ((1 to 32 megabytes))	Specify the maximum size of a trace file.
`tracefile-num:` <<3>> ((1 to 10))	Specify the number of the trace files.

Key name	Value
event-lost-limit: <<10>> ((3 to 60 seconds))	Specify the number of seconds during which the system will wait before determining that the APM-issued SNMP trap event has been lost. Specify the maximum interval for event delay.[#3]
event-lost-retry: <<1>> ((0 to 5 times))	Specify the number of retries to be attempted when the event is lost. If monitoring cannot be restarted even after retry was attempted the specified number of times, the system then determines that the event was lost.
omit-unknown-event: <<off>>	Specify whether to suppress the unknown event[#4] that is issued at the detection of APM communication failure (communication error occurrence, stop event reception, or event loss detection) and issue a process and service monitoring failure event. To issue an unknown event (a status change event that has changed to the Unknown status) at the detection of communication failure, specify off. To issue a process and service monitoring failure event instead of issuing the unknown event at the detection of communication failure, specify on. As many unknown events as the number of processes are issued. If you want to collectively manage unknown events, specify the issuance of the process and service monitoring failure event.
snmp-dump: <<off>>	Specify whether to output an SNMP packet dump for troubleshooting at failure occurrence. To output the SNMP packet dump, specify on. To not output the SNMP packet dump, specify off.
max-dumpfile-size: <<8>> ((0 to 99 megabytes))	Specify the maximum size of the SNMP packet dump trace file. When 0 is specified, the trace is acquired without limiting the file size.
sso-start-hcheck-interval:[#1] <<0>> ((0 to 60 seconds))	Specify the interval at which to execute the system health check at SSO startup in units of the number of monitored servers specified by sso-start-hcheck-unit.
sso-start-hcheck-delay:[#1] <<0>> ((0 to 600 seconds))	Specify the delay in starting the system health check at SSO startup.
sso-start-hcheck-unit:[#1] <<1>> ((1 to 32))	Specify the number of monitored servers for which to sequentially execute the system health check at SSO startup at the intervals specified by sso-start-hcheck-interval.
apm-start-hcheck-delay: <<0>> ((0 to 600 seconds))	Specify the delay in starting the system health check at the reception of APM start event.
hcheck-retry-count:[#5] <<2>> ((0 to 10 times))	Specify the number of retries to be attempted when SSO fails in the health check in communication with APM. When 0 is specified, the health check is not retried.
hcheck-retry-interval:[#5] <<30>> ((0 to 3,600 seconds))	Specify the interval of retries (in seconds) to be attempted when SSO fails in the health check in communication with APM. When 0 is specified, the interval of the health checks on agents is used.
max-apmevtfile-size: <<4>> ((1 to 32 megabytes))	Specify the maximum size of a TCP event logging file.
apmevtfile-num: <<3>> ((1 to 10))	Specify the number of the TCP event logging files.
max-apm-session:[#1] <<40>> ((1 to 99))	Specify the maximum number of sessions to receive TCP events from APM.
connect-retry-interval: <<10>> ((3 to 60 seconds))	Specify the interval of retries to be attempted when SSO fails in the TCP connection to APM.
apm-incident-check-interval:[#6] <<5>> ((0 to 60 seconds))	Specify the interval at which whether an APM incident has occurred is checked. When 0 is specified, APM incidents are not checked.

Key name	Value
apm-incident-delete:[#6] [#7] <<on>>	Specify whether to delete APM incidents. Specify on to delete the incidents that occur during the interval of APM incident checks. Specify off to not delete them. When on is specified, all the APM incidents on NNMi are deleted when the ssoapmon daemon process starts.
max-incident-logfile-size: <<4>> ((1 to 32 megabytes))	Specify the maximum size of an incident logging file.
incident-logfile-num: <<3>> ((1 to 10))	Specify the number of the incident logging files.
fs-redirect: <<on>>	Specify on to enable the File System Redirector when executing automated action in a WOW64 environment. Specify off to disable the File System Redirector. This key is valid only for the Windows version.

#1: If you change the value of this item, you must restart the ssoapmon daemon process.

#2: The following lists the windows and commands that connect to the ssoapmon daemon process:

- Process Monitor window
- Process Reference window
- Process Configuration window
- ssoapcom command
- ssopschk command
- ssopsset command
- ssopsshow command
- ssopsstart command
- ssopsstop command

#3: The value of the event-lost-limit: key must be at least twice as high as the value of each of the following keys in the respective definition files:

- DINTERVAL: key of the event-delay configuration file (apmdelay.conf)
- apm-incident-check-interval: key of the ssoapmon action definition file (ssoapmon.def)

#4: The following table describes the timings of suppressing unknown events.

Timing	Description
When an APM stop event is received	When an Agent for Process stop event is received from APM
When health check fails	When the health check on APM fails
When a communication error occurs	When a request (to change a monitoring condition, change the monitoring interval, or update the status) to APM fails
When an event loss is detected	When an event sent from APM is lost

#5: The health check is retried at the following timings:

- When a start event is received from APM
- When the health check interval has passed since the last health check succeeded
- When an event other than the stop event is received from the APM recognized by SSO as stopped APM
- When the ssoapcom -H command is received
- When an error is detected in TCP connection or event transmission or reception during the event notification from APM on TCP

#6: An APM incident is an incident converted by NNMi from an event that was reported to NNMi as an SNMP trap by APM.

#7: The number of SNMP traps NNMi can receive is limited. If the number of traps received by NNMi comes close to the maximum limit, the SNMP trap events from APM are not converted any more, and process monitoring is thereby disabled. For this reason, be careful to prevent the number of traps received by NNMi from coming close to the maximum limit. For the SNMP trap reception by NNMi and the specifications of the conversion of received SNMP traps into incidents, see the NNMi Help.

When coding definitions in an ssoapmon action definition file, note the following:

- If the definition file includes multiple definitions for the same item, the definition written last is assumed to be valid, and those definitions preceding the last definition are ignored.
- When omitting the specification of a key on a line, omit the whole line.
- The maximum number of files that ssoapmon daemon process can open at the same time is obtained by the following formula:
  (*max-client value*) + (*max-snmp-session value*) + (*max-apm-session value*) + 20
- The value of the max-client: key can be calculated by the following formula:
  max-client ≧ (*number-of-concurrently-opened-windows*#1 + *number-of-concurrently-executed-commands*#2) **x** *number-of-monitoring-managers*
  #1: The concurrently opened windows are as follows:
  Process Monitor window, Process Configuration window, and Process Reference window
  #2: The concurrently executed commands are as follows:
  ssopsset, ssopsstart, ssopsstop, ssopschk, ssoapcom, ssopscvt, ssopsshow
- The value of the max-snmp-session: key can be calculated by the following formula:
  max-snmp-session > number of monitored servers that cannot communicate with the monitoring manager
  Note
  If the number of monitored servers that cannot communicate with the monitoring manager exceeds the value of the max-snmp-session: key, the health check might be delayed and not be executed according to the settings. If this occurs, adjust the settings so that the number of monitored servers matches the above formula, or extend the health check interval.
- The value of the max-apm-session: key can be calculated by the following formula:
  max-apm-session ≧ ((*number-of-monitored-servers*) / (1 + (*number-of-retries-by-APM*))) **x** 1.2 (*safety-factor*)
  Note
  If the value of the max-apm-session key exceeds 99 (maximum specifiable value) when the value is calculated with a maximum number of retries by APM, reduce the value of the key to 99, and then enable regular health checks.

6.3.8 ssocolmng action definition file (ssocolmng.def)

The ssocolmng action definition file contains definitions of ssocolmng daemon process actions. If you have made any changes in this definition file, perform one of the following operations to validate these changes:

- Execute the ssocolmng -r command.
  Note that the changes might not become valid depending on the key that has been changed.
- Restart the ssocolmng daemon process.

(1) Format

The following is an example of an ssocolmng action definition file.

```
[threshold-event:          on|off]
[status-event:             on|off]
[nnm-urlaction-coop:       on|off]
[nnm-map-coop:             on|off]
[map-status-warning:       warning | minor | major | critical]
[map-status-critical:      major | critical]
[max-client:               maximum-number-of-concurrent-connections
                           -with-GUI-and-command]
[change-my-address:        IP-address]
[max-logfile-size:         maximum-size-of-logging-file]
[logfile-num:              number-of-the-log-files]
[trace:                    on|off]
[max-tracefile-size:       maximum-size-of-trace-file]
[tracefile-num:            number-of-the-trace-files]
[snmp-dump:                on|off]
[max-dumpfile-size:        maximum-number-of-SNMP-packet-dump-trace-files]
[max-incident-logfile-size:  maximum-size-of-an-incident-logging-file]
[incident-logfile-num:     number-of-the-incident-logging-files]
[fs-redirect:              on|off]
[omit-first-monitor-event: on|off]
[sso-start-collect-interval:  collection-restart-interval-at-SSO-startup]
[sso-start-collect-unit: number-of-servers-for-which-collection-delays-at-SSO-startup]
[get-specific-instance:  {resource-ID|resource-ID-range-specification}, ... |all|none]
```

When coding definitions in an `ssocolmng` action definition file, note the following:

- If the definition file includes multiple definitions for the same item, the definition written last is assumed to be valid, and those definitions preceding the last definition are ignored.
- When omitting the specification of a key on a line, omit the whole line.

(2) Description

The next table lists the items that must be or can be defined in an `ssocolmng` action definition file.

Key name	Value
`threshold-event:` `<<on>>`	Specify whether to issue the resource status change event to NNMi. To issue the event, specify `on`. To not issue the event, specify `off`. Even when `on` is specified, the incidents that are filtered with the event filter definition file (`ssoevtfilter.conf`) will not be issued. Note that if `off` is specified, no event is issued even when destinations are specified in the event destination definition file (`ssodest.conf`).
`status-event:` `<<on>>`	Specify whether to issue the collection status change event to NNMi. To issue the event, specify `on`. To not issue the event, specify `off`. Even when `on` is specified, the incidents that are filtered with the event filter definition file (`ssoevtfilter.conf`) will not be issued. Note that if `off` is specified, no event is issued even when destinations are specified in the event destination definition file (`ssodest.conf`).
`nnm-urlaction-coop:`[#1] `<<on>>`	Specify whether to use the NNMi map cooperation function (action cooperation). To use the function, specify `on`. To not use the function, specify `off`.
`nnm-map-coop:`[#1] `<<on>>`	Specify whether to use the NNMi map cooperation function (symbol cooperation). To use the function, specify `on`. To not use the function, specify `off`.
`map-status-warning:`[#1] `<<minor>>`	Specify the NNMi node status that corresponds to the warning-level application status for the NNMi map cooperation function (symbol cooperation). The warning-level application status can correspond to the `warning`, `minor`, `major`, or `critical` NNMi node status. For the correspondence between the application status on SSO and the status registered with NNMi, see *2.6.3(2) Correspondence between the statuses managed in SSO and the severity statuses registered in NNMi*.

Key name	Value
`map-status-critical:`[#1] <<major>>	Specify the NNMi node status that corresponds to the critical-level application status for the NNMi map cooperation function (symbol cooperation). The caution-level application status can correspond to the `major` or `critical` NNMi node status. For the correspondence between the application status on SSO and the status registered with NNMi, see *2.6.3(2) Correspondence between the statuses managed in SSO and the severity statuses registered in NNMi*.
`max-client:` <<32>> ((1 to 99))	Specify the maximum number of concurrent sessions with the GUI and commands[#2] to connect to the `ssocolmng` daemon process. Note that, when creating a report, as many `ssoextractlog` commands as the number of report conditions start concurrently.
`change-my-address:`[#1] <<none>>	When the monitoring manager has multiple IP addresses or when it is operating in a cluster system, specify the operating IP address of SSO in the *n.n.n.n* format. (*n* is an integer from 0 to 255.) In other cases, specify `none`. • When the monitoring manager has multiple IP addresses: Specify an IP address at which SSO can communicate with the monitoring server. You can freely select one of the monitoring manager's IP addresses at which SSO can communicate with the monitoring server. • When operating SSO in a cluster system: Specify a logical IP address. The operating IP address of SSO defined in the `ssoapmon` action definition file is the IP address of collection database monitoring manager. The IP address is used for the following purposes: • Collection database name • Display of collection data list in the Resource Data Reference window • Display of `ssoextractlog -list` command results
`max-logfile-size:` <<4>> ((1 to 32 megabytes))	Specify the maximum size of a log file.
`logfile-num:` <<3>> ((1 to 10))	Specify the number of the log files.
`trace:` <<off>>	Specify whether to output a trace file for troubleshooting at failure occurrence. To output the trace file, specify `on`. To not output the trace file, specify `off`.
`max-tracefile-size:` <<4>> ((1 to 32 megabytes))	Specify the maximum size of a trace file.
`tracefile-num:` <<3>> ((1 to 10))	Specify the number of the trace files.
`snmp-dump:` <<off>>	Specify whether to output an SNMP packet dump for troubleshooting at failure occurrence. To output the SNMP packet dump, specify `on`. To not output the SNMP packet dump, specify `off`.
`max-dumpfile-size:` <<8>> ((0 to 99 megabytes))	Specify the maximum size of the SNMP packet dump trace file. When `0` is specified, the trace is acquired without limiting the file size.
`max-incident-logfile-size:` <<4>> ((1 to 32 megabytes))	Specify the maximum size of an incident logging file.
`incident-logfile-num:` <<3>> ((1 to 10))	Specify the number of the incident logging files.
`fs-redirect:` <<on>>	Specify `on` to enable the File System Redirector when executing automated action in a WOW64 environment. Specify `off` to disable the File System Redirector. This key is valid only for the Windows version.
`omit-first-monitor-event:` <<off>>	Specify whether to suppress the resource status change event (`SSO_Resource_Monitor_Normal` incident) that is to be issued when the initial resource

Key name	Value
`omit-first-monitor-event:` <<off>>	status is determined to be in the normal region after resource collection (threshold monitoring) starts. Specify `on` to suppress the event. Specify `off` to not suppress the event.
`sso-start-collect-interval:` <<0>> ((0 to 60 seconds))	Specify the interval at which to restart resource collection at SSO startup in units of the number of monitored servers specified by `sso-start-collect-unit`. If you specify 1 or larger value for this key, you can distribute the CPU load and communication load on the monitoring manager host at SSO startup. When you intend to distribute the loads, specify a value for this key as a rough standard that meets the following condition: *Value-of-this-key-(in seconds)* ≦ *minimum-collection-interval-(in seconds)* / *number-of-monitored-servers* **x** *value-of-the-sso-start-collect-unit-key*
`sso-start-collect-unit:` <<1>> ((1 to 32))	Specify the number of monitored servers for which to sequentially restart resource collection at SSO startup at the interval specified by `sso-start-collect-interval`.
`get-specific-instance:`#1, #3, #4 <<none>> ((1 to 2147483647))	When you collect resources from a specific instance, specify the resource ID to acquire only the MIB object of the specific instance. When specifying multiple resource IDs, delimit them with a comma (`,`). You can specify a range of resource IDs by using a hyphen (`-`). You cannot enter a tab or space in the specified string. Example: `10000,11000-12000` When `none` is specified, the MIB objects of all instances are acquired. When `all` is specified, this definition is valid for all resources. Specify a value within 2,047 bytes from the top of the line.

#1: If you change the value of this item, you must restart the `ssocolmng` daemon process.

#2: The following lists the GUI windows and commands to connect to the `ssocolmng` daemon process:

- Resource Browser window
- Resource Data Reference window
- Resource Reference window
- Resource Configuration window
- Threshold verification window
- `ssocolchk` command
- `ssocolmng` command
- `ssocolset` command
- `ssocolshow` command
- `ssocolstart` command
- `ssocolstop` command
- `ssodbcheck` command
- `ssodbdel` command
- `ssoextractlog` command

#3: When this setting is enabled and a resource that meets all the conditions below is collected, the resource value is undefined if the resource is collected right after the number of instances of the collection target MIB object has changed.

- The resource is a user resource.
- The MIB object ID of instance is not unique to the entity (instance) because of the specification of the collection target agent (for example, serial numbers of existing instances are always used as MIB object IDs).
- The definition of the resource in the user resource definition file includes the definition of a subresource Counter-type MIB object.

When this setting is disabled, collection of the resource that meets the above conditions is skipped right after the number of instances has changed.

#4: You cannot collect only specific instances as resources from the SNMP agent in which SysUpTime (mib-2.1.3) is not installed.

6.3.9 ssocollectd action definition file (ssocollectd.def)

The `ssocollectd` action definition file contains definitions of `ssocollectd` daemon process actions. If you have made any changes in this definition file, perform one of the following operations to validate these changes:

- Execute the `ssocollectd -r` command.
  Note that the changes might not become valid depending on the key that has been changed.
- Restart the `ssocollectd` daemon process.

(1) Format

The following is a format of the `ssocollectd` action definition file.

```
[snmp-address:           IPv4-logical-IP-address]
[snmp-address-v6:        IPv6-logical-IP-address]
[max-snmp-session:       maximum-number-of-concurrent-SNMP-sessions]
[postponing-interval:    interval-until-next-collection-after-change-to-postponing-status]
[postponing-retry:       retry-count-before-change-to-postponing-status]
[max-logfile-size:       maximum-size-of-logging-file]
[logfile-num:            number-of-the-log-files]
[trace:                  on|off]
[max-tracefile-size:     maximum-size-of-trace-file]
[tracefile-num:          number-of-the-trace-files]
[snmp-dump:              on|off]
[max-dumpfile-size:      maximum-number-of-SNMP-packet-dump-trace-files]
```

When coding definitions in an `ssocollectd` action definition file, note the following:

- If the definition file includes multiple definitions for the same item, the definition written last is assumed to be valid, and those definitions preceding the last definition are ignored.
- When omitting the specification of a key on a line, omit the whole line.

(2) Description

The next table lists the items that must be or can be defined in an `ssocollectd` action definition file.

Key name	Value
`snmp-address:` `<<default>>`	When operating SSO in a cluster system, specify a logical IP address for IPv4 in the IPv4 address format. By using this specification, you can use a fixed logical IP address for IPv4 as the monitoring manager IP address that is allowed to pass through the firewall located between the monitoring manager and monitored servers. If multiple logical IP addresses are available, specify the logical IP address at which the monitoring server can communicate with all monitored servers. In other cases, specify `default`. When `default` is specified, the local host IP address for IPv4 that enables communication with the monitoring server is used as the monitoring manager IP address that is allowed to pass through the firewall. If multiple local host IP addresses for IPv4 are available for this purpose, selection of the IP address that is allowed to pass through the firewall depends on the OS.
`snmp-address-v6:` `<<default>>`	When operating SSO in a cluster system, specify a logical IP address for IPv6 in the IPv6 address format. By using this specification, you can use a fixed logical IP address for IPv6 as the monitoring manager IP address that is allowed to pass through the firewall located between the monitoring manager and monitored servers. If multiple logical IP addresses are available, specify the logical IP address at which the monitoring server can communicate with all monitored servers.

Key name	Value
snmp-address-v6: <<default>>	In other cases, specify default. When default is specified, the local host IP address for IPv6 that enables communication with the monitoring server is used as the monitoring manager IP address that is allowed to pass through the firewall. If multiple local host IP addresses for IPv6 are available for this purpose, selection of the IP address that is allowed to pass through the firewall depends on the OS.
max-snmp-session:#1 <<32>> ((1 to 99))	Specify the number of monitored servers that concurrently communicate with the monitoring manager.
postponing-interval: <<1800>> ((10 to 86,400 seconds))	Specify the time to wait for executing the next collection after the collection status has changed to *Postponing*#2. If a value less than the resource collection interval is specified, the next collection is executed according to the setting of the resource collection interval.
postponing-retry: <<2>> ((0 to 99 times))	Specify the number of retries that will be attempted before the collection status enters postponing.
max-logfile-size: <<4>> ((1 to 32 megabytes))	Specify the maximum size of a log file.
logfile-num: <<3>> ((1 to 10))	Specify the number of the log files.
trace: <<off>>	Specify whether to output a trace file for troubleshooting at failure occurrence. To output the trace file, specify on. To not output the trace file, specify off.
max-tracefile-size: <<4>> ((1 to 32 megabytes))	Specify the maximum size of a trace file.
tracefile-num: <<3>> ((1 to 10))	Specify the number of the trace files.
snmp-dump: <<off>>	Specify whether to output an SNMP packet dump for troubleshooting at failure occurrence. To output the SNMP packet dump, specify on. To not output the SNMP packet dump, specify off.
max-dumpfile-size: <<8>> ((0 to 99 megabytes))	Specify the maximum size of the SNMP packet dump trace file. When 0 is specified, the trace is acquired without limiting the file size.

#1 If you change the value of this item, you must restart the ssocollectd daemon process.

#2: For the *Postponing* status, see *Figure 2-9* and *Figure 2-10*.

6.3.10 ssotrapd action definition file (ssotrapd.def)

In the ssotrapd action definition file, define the actions of the ssotrapd daemon process. If you have made any changes in this definition file, perform one of the following operations to apply these changes:

- Execute the ssotrapd -r command.
- Restart the ssotrapd daemon process.

(1) Format

The following is a format of the ssotrapd action definition file.

```
[max-logfile-size:    maximum-size-of-logging-file]
[logfile-num:         number-of-the-log-files]
[trace:               on|off]
[max-tracefile-size:  maximum-size-of-trace-file]
[tracefile-num:       number-of-the-trace-files]
[snmp-dump:           on|off]
[max-dumpfile-size:   maximum-size-of-SNMP-packet-dump-trace-files]
```

When coding definitions in an `ssotrapd` action definition file, note the following:

- If the definition file includes same definitions, the definition written last is assumed to be valid, and those definitions preceding the last definition are ignored.
- When omitting the specification of a key on a line, omit the whole line.

(2) Description

The next table lists the items that must be or can be defined in an `ssotrapd` action definition file.

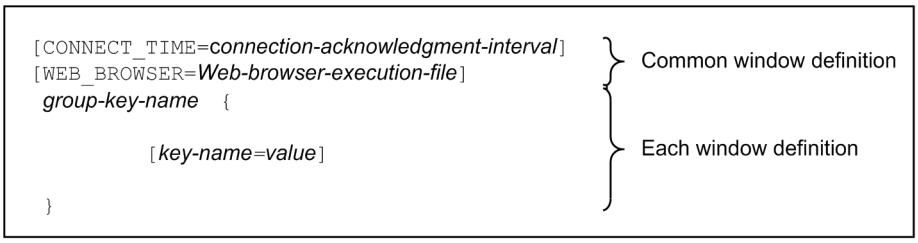
Key name	Value
`max-logfile-size:` <<4>> ((1 to 32 megabytes))	Specify the maximum size of a log file.
`logfile-num:` <<3>> ((1 to 10))	Specify the number of the log files.
`trace:` <<off>>	Specify whether to output a trace file for troubleshooting at failure occurrence. To output the trace file, specify `on`. To not output the trace file, specify `off`.
`max-tracefile-size:` <<4>> ((1 to 32 megabytes))	Specify the maximum size of a trace file.
`tracefile-num:` <<3>>((1 to 10))	Specify the number of the trace files.
`snmp-dump:` <<off>>	Specify whether to output an SNMP packet dump for troubleshooting at failure occurrence. To output the SNMP packet dump, specify `on`. To not output the SNMP packet dump, specify `off`.
`max-dumpfile-size:` <<8>> ((0 to 99 megabytes))	Specify the maximum size of the SNMP packet dump trace file. When `0` is specified, the trace is acquired without limiting the file size.

6.3.11 GUI definition file (ssogui.conf)

In the GUI definition file, define the behavior of GUI components such as windows. The GUI definition file is read when a GUI component is activated, and the GUI component operates according to the definition in the definition file.

(1) Format

If you specify definition items for each window, write the group key name that indicates a window, and specify definition items on subsequent lines. The following is a sample format of a GUI definition file.



If the same items are defined by both default settings and the settings for a specific window, the settings for the specific window (that is, the settings within the scope of the corresponding group key) take effect. The next table lists the relationship between window names and group key names.

Window name	Group key name	Required/ Optional
Resource Browser window	`browser`	Optional
Resource Configuration window	`collect-c`	Optional
Resource Data Reference window	`collect-m`	Optional
Process Configuration window	`process-c`	Optional
Process Monitor window	`process-m`	Optional
Resource Browser (Web) window	`web-browser`	Optional
Resource Configuration (Web) window	`web-collect-c`	Optional
Resource Data Reference (Web) window	`web-collect-m`	Optional
Process Configuration (Web) window	`web-process-c`	Optional
Process Monitor (Web) window	`web-process-m`	Optional
Report Configuration (Web) window	`web-report-c`	Optional

(2) Description

The next table lists the items that must be or can be defined in a GUI definition file. If the value of a definition item is written in a position where it cannot be written, the written value is ignored.

Key name	Value	Definition position
`CONNECT_TIME` `<<60>>` ((1 to 300))	Specify the interval, in seconds, for checking connection between the daemon process and windows.	• Definition common to windows (outside the scope of group key) • Definition for each window (inside the scope of group key)
`SMS_SERVER`	Specify the SMS server name used by the Resource Browser window. You can specify a host name or IP address that can be resolved by the host that started the window. You can specify this item more than once.	Definition for each window (inside the scope of group key (specifiable only for the browser group))
`WEB_BROWSER`#	Specify, in a full-path name, the WWW browser execution file to be used when you reference the help pages from each Window. If your OS is Windows NT or Windows 2000, you need not specify this item. Specification of this item is also invalid for the WWW interface.	Definition common to windows (outside the scope of group key)

`REGULAR_QUERY`
`<<20,000>>`
((1 to 20,000))
	Specify the maximum number of times of regular query that can be executed in the Performance Data window and Ping Response Time window under the Resource Browser window.	Definition for each window (inside the scope of group key (specifiable only for the browser group))

Key name	Value	Definition position
MAX_HEAP_SIZE <<128>> ((32 to 1,024 megabytes))	Specify the size of the heap area that is used by Java virtual machine when a GUI component is activated.	• Definition common to windows (outside the scope of group key) • Definition for each window (inside the scope of group key)

#: These definitions are invalid for the windows provided by Windows and those opened from the SSO console.

(3) Example

The following is an example of an SNMP definition file.

```
#
# ssogui.conf
#

CONNECT_TIME = 60
WEB_BROWSER = /usr/bin/firefox

browser {
         CONNECT_TIME = 30
         SMS_SERVER = 172.16.45.40
         SMS_SERVER = netmps01
                  REGULAR_QUERY= 20000
                  MAX_HEAP_SIZE=64
}

web-process-c {
         CONNECT_TIME = 90
}

web-process-m {
         CONNECT_TIME = 90
}
```

(4) Note

For the keys that can be defined as both the definitions common to windows and the definitions for each window, the values specified for each window, and not the values specified for the definitions common to windows, take effect.

6.3.12 Port number definition file (ssoport.conf)

In the port number definition file, you define port numbers to be used by SSO.

(1) Format

In the port number definition file, write each process and command as a key name, followed by a port number. Note that if the definition file includes multiple definitions for the same item, the definition written last is assumed to be valid, and those definitions preceding the last definition are ignored.

(2) Description

The next table lists the items that must be or can be defined in a port number definition file. Definition items must be written in the order indicated in this table. A port number must be in a range from 1 to 65,535 and must not be the same as any other port number.

For the remote connection from the GUI or by a command, you must specify the same port number for daemon processes in the port number definition file at both the connection source and destination.

Key name	Value
ssocolmng: <<20086>>	Specify the port number to be used for a connection with the ssocolmng daemon process and Resource Browser window, Resource Configuration window, Resource Reference window, Resource data Reference window, ssocolmng, ssocolset, ssocolstart, ssocolstop, ssocolshow, ssodbcheck, ssodbdel, and the ssoextractlog command. This number is bound by the ssocolmng daemon process.
ssocollectd: <<20223>>	Specify the port number to be used for a connection between ssocollected daemon process and ssocollectd command or ssocolmng daemon process. This port number is bound by ssocollected daemon process.
ssoapmon: <<20147>>	Specify the port number to be used for a connection with the ssoapmon daemon process and the Process Configuration window, Process Reference window, process monitor window, ssopsset, ssopsstart, ssopsstop, and the ssopsshow command. This port number is bound by ssoapmon daemon process.
ssoapcom: <<20228>>	Specify the port number to be used for a connection between ssoapmon daemon process and the ssoapcom command. This port number is bound by ssoapmon daemon process.
ssoapmevt: <<20264>>	Specify the port number to be used for a connection between ssoapmon daemon process and the APM. This port number is bound by ssoapmon daemon process. Specify the port number specified here for the setting key TCPSPORT in the event TCP notification definition file (apmtcpsend.conf) of APM.
ssospmdcmd: <<20391>>	Specify the port number to be used for a connection between ssospmd daemon process and ssospmd, ssostart, ssostop, ssostatus, or the ssobackup command. This port number is bound by ssospmd daemon process.
ssospmdcpro: <<20392>>	Specify the port number to be used for a connection between ssospmd daemon process and ssocollectd, ssocolmng, ssoapmon, ssorptd, or ssoconsoled daemon process. This port number is bound by ssospmd daemon process.
ssorptd: <<22297>>	Specify the port number to be used for a connection between ssorptd daemon process and Report Configuration window or ssodemandrpt command. This port number is bound by ssorptd daemon process.
ssoconsoleweb: <<20393>>	Specify the port number that is used for the HTTP connection between the SSO console and Web browser and the connection between the SSO console and ssoconsoled command. This port number is bound by the Web server process (httpsd) on the SSO console.
ssoconsolec: <<20394>>	Specify the port number that is used for the connection between the Web server and Web container on the SSO console. This port number is intended for the internal processing on the SSO console, and bound by the Web container process (cjstartweb) on the SSO console.
ssoconsoles: <<20395>>	Specify the port number for Web container management on the SSO console. This port number is intended for the internal processing on the SSO console, and bound by the Web container process (cjstartweb) on the SSO console.
ssotrapd: <<20396>>	Specify the port number to be used for a connection between ssotrapd daemon process and ssotrapd command or ssoapmon daemon process. This port number is bound by ssotrapd daemon process.

(3) Note

Stop SSO before changing settings in the port number definition file. Changing the value of ssospmdcmd while SSO is running disables execution of the start command (ssostart), stop command (ssostop), status display command (ssostatus), backup command (ssobackup), and the ssospmd -r command.

6.3.13 Event destination definition file (ssodest.conf)

In the event destination definition file, you can define the destination of the event issued by SSO to a remote host.

If you have defined or changed an event transmission destination related to resource collection in this definition file, perform one of the following operations:

- Execute the `ssocolmng` command with the `-r` option specified to re-read the definition file.
- Restart the `ssocolmng` daemon process.

Also, if you have defined or changed an event transmission destination related to process monitoring in this definition file, perform one of the following operations:

- Execute the `ssoapcom` command with the `-r` option specified to re-read the definition file.
- Restart the `ssoapmon` daemon process.

(1) Format

The following is a format for an event destination definition file.

```
ssocolmng|ssoapmon;event;destination-IP-address;[language];
[host-name-display];[target-agent-IP-address];[event-type];[port-number];
                                    ⋮
```

Separate each item with a semicolon (;). Be sure to write a semicolon (;) even if you omit an item.

(2) Description

The following table shows the content of the definition.

Item	Explanation
`ssocolmng` or `ssoapmon`	Specify an event issuing function. If you specify `ssocolmng`, define the event transmission destination for resource collection. If you specify `ssoapmon`, define the event transmission destination for process monitoring.
event	Specify the type of the event to be issued. Collection or monitoring status change event[#1]: `1` Threshold event[#2]: `2` Status change event: `16` If you want to issue multiple events, add the values of the events. For example, if you want to issue the collection status change or monitoring status change event and the threshold event, specify `3`. The specification of status change event is valid only when `1` is specified as the event type (the event transmission destination is NNMi).
destination-IP-address	Specify the IP address of the host to which you want to transmit an event.
language[#3] <<language of transmission destination>>	Specify the language used by the event transmission destination. Specify this item when the language is different between the event transmission source and event transmission destination. This setting is valid only when `2` is specified as the event type (the event transmission destination is other than NNMi).
host-name-display <<`off`>>	Specify the display of a host name indicating the agent host (source) as a custom incident attribute in the incident form. If you want to display the agent host in a host name, specify `on`. If you specify `off`, the IP address is displayed.

Item	Explanation
target-agent-IP-address <<all agents for resource collection and process monitoring>>	You can only transmit events for the specified agent to the defined transmission destination host. When you specify multiple agents, separate them with a colon (:) per IP address. When `ssocolmng` is specified, both IPv4 addresses and IPv6 addresses can be specified. When `ssoapmon` is specified, only IPv4 addresses can be specified. To specify IPv6 addresses, enclose them in brackets (`[ ]`).
event-type <<1>> ((1 or 2))	Specify the type of the event to be transmitted. Specify one of the following settings according to the SNMP manager at the event transmission destination: When the event transmission destination is NNMi: `1` When the event transmission destination is other than NNMi: `2` When `1` is specified as the event type, the collection status change, monitoring status change, and threshold events are transmitted as incidents, and the status change event is transmitted as a status. In this case, use the `ssonnmsetup` command to add the information about connections to NNMi to which events are transmitted. When `2` is specified as the event type, the collection status change, monitoring status change, and threshold events are transmitted as SNMP traps. When you specify `2` as the event type, do not specify the status change event for the Event item.
port-number <<162>> ((1 to 65535))	Specify the port number of the event transmission destination. This setting is valid only when `2` is specified as the event type (the event transmission destination is other than NNMi).

#1: This type of event indicates the collection status change event, monitoring status change event, and process or service monitoring failure event.

#2: This type of event indicates the resource status change event, process status change event, service status change event, and application status change event.

#3 The value to be specified for the destination language varies depending on the OS and the language environment variable used on the destination, as shown in the next table.

OS	Language environment variable	Value to be specified
HP-UX	ASCII code	`C`
	Shift JIS code	`SJIS`
	EUC code	`EUC`
Solaris	ASCII code	`C`
	EUC code	`EUC`
	Shift JIS code	`SJIS`
Linux	ASCII code	`C`
	UTF-8 code	`UTF-8`
Windows	ASCII code	`C`
	Shift JIS code	`SJIS`

(3) Example

The following is an example of an event destination definition file.

```
#
# ssodest.conf
#
# FORMAT
# process name;event
mask;DestIPaddress;[language];[on|off];[AgentIPaddress
[:AgentIPaddress...]];[event type];[port no];
ssocolmng;1;100.1.20.6;EUC;on;100.20.30.1;1;;
ssocolmng;3;100.2.12.8;EUC;off;100.20.30.1:100.20.30.2:100.20.30.3:100.20.
30.4;2;10000;
ssoapmon;2;100.1.20.6;;on;;;;
ssoapmon;3;100.2.12.8;SJIS;;100.20.30.1:100.20.30.2;;;
ssocolmng;1;100.1.20.6;SJIS;on;100.20.30.1;1;;
ssocolmng;1;100.1.20.9:SJIS;off;10.210.103.243:[2001:0db8::1234:5678:90ab:
cdef];2;;
ssocolmng;16;100.1.20.10:SJIS;off;10.210.103.243;1;;
ssoapmon;19;100.1.20.10:SJIS;off;10.210.103.243;1;;
```

6.3.14 User resource definition file

The user resource definition file contains definitions of user-specific resources. You can define resources in a resource category in the user resource definition file.

(1) Format

The following shows the format of the user resource definition file.

```
[rsc_category=resource-category-name]                          } Resource category definition
 rsc_id=resource-ID                                            } Resource definition
 rsc_label_j=[Japanese-resource-name]                          }
 rsc_label_e=English-resource-name                             }
 rsc_units=[unit]                                              }
 rsc_threshold_MODE=[1|2]                                      }
[instance_mib_oid=instance-MIB-object-ID;number-1;number-2:number-3  } Subresource definition
 instance_mib_type=MIB-object-type]                            }
 subrsc_mib_oid=MIB-object-ID                                  }
 subrsc_mib_type=Counter|Gauge|Integer|String                  }
 subrsc_label_j=[Japanese-resource-name]                       }
 subrsc_label_e=English-resource-name                          }
 subrsc_mib_data=keyword-and-operator                          }
```

(2) Details of resource category definition

The next table lists the items that constitute a resource category definition.

Key name	Value
rsc_category <<USER>> ((alphanumeric characters and hyphen (-) of 32 or fewer bytes))	Specify a resource category name. • The resource category name must begin with USER. Also, the resource category name must not exceed 32 bytes, including USER. • The resource category name is not case sensitive#. USER at the top of the name, however, must be written in uppercase.

#: When a category name is displayed by a command or in a window, the category name is case sensitive.

When coding a resource category definition, note the following:

- Write this field at the top of the user resource definition file.

- In a user resource definition file, you can write this field only once.
- When omitting this field, omit the whole field, including the key name.

(3) Details of resource definition

The next table lists the items that constitute a resource definition. You must write fields in the definition file in the order in which they are listed the following table.

Key name	Value
`rsc_id` ((10000 to 19999))	Specify a resource ID.
`rsc_label_j` <<English resource name>> ((The resource group label name and resource label name can have 32 or fewer bytes each.))	Specify this item when you specify a Japanese resource name. Specify a semicolon-separated pair consisting of a resource group label name and a resource label name. Omit this item when you use an English resource name. You can use not only multi-byte characters but also 1-byte alphanumeric characters and symbols. You cannot use one-byte katakana characters. The label names cannot include tabs, commas (,), colons (:), and/or semicolons (;).
`rsc_label_e` ((The resource group label name and resource label name can have 32 or fewer bytes each.))	Specify a semicolon-separated pair consisting of a resource group label name and a resource label name. For an English label name, you can use the ASCII characters other than tab character, space character, comma (`,`), colon (`:`), semicolon (`;`), forward slash (`/`), and escape character (`\`).
`rsc_units` <<unit not displayed>>	Specify a resource unit. Usable characters are alphanumeric characters of up to 32 bytes, percent sign (%), underbar (_), and hyphen (-).
`rsc_threshold_MODE` <<1>> ((1 or 2))	Specify a threshold display mode. • Normal < Warning < Critical: `1` • Critical < Warning < Normal: `2`

When coding a resource definition, note the following:

- After the resource category definition, write as many resource definitions as the number of resources.
- When you omit an optional definition item, you can only omit the value; you must write the key name and an equal sign (=).
- If one definition file contains two or more definitions with the same resource IDs, only the first resource definition will be regarded as valid and the other resource definitions will be ignored.
- The values specified for key names `rsc_label_j` and `rsc_label_e` must be unique within the file.
- For a summary resource (a resource that includes a subresource whose data consists of string-type MIB values), the definitions of `rsc_units` and `rsc_threshold_MODE` are ignored.

(4) Details of subresource definition

The definition for subresources consists of one instance MIB object definition (optional), one or more subresource MIB object definitions, and one or more subresource definitions:

```
[instance-MIB-object-definition]
 subresource-MIB-object-definition
  :
 subresource-definition
  :
```

When coding a subresource definition, note the following:

- After the resource definition, write as many subresource definitions as the number of subresources.

(a) Definitions for the instance MIB object

The following table shows the content of definitions for the instance MIB object. You must write fields in the definition file in the order in which they are listed in the following table.

Key name	Value
`instance_mib_oid`	• Enter the MIB object ID when replacing the key name with another MIB object name having a suffix that matches the suffix of an MIB object specified in `subrsc_mib_oid`. • Enter the numbers that will be compared with the objects comprising the suffix of the MIB object ID and MIB object (*number-1*;*number-2*) and the number that will replace (*number-3*), separated by semicolons (;). • For the MIB object ID, enter the MIB object ID for acquiring the MIB value, which will be replaced with the MIB object suffix entered in `subrsc_mib_oid`. • For *number-1*, enter the ordinal number of the object which form the suffix of the MIB object specified in MIB object ID, that will be compared with the suffix of the MIB object entered in `subrsc_mib_oid`. A number from 1 to 32 can be specified for *number-1*. You can specify multiple numbers. When specifying multiple numbers, write the numbers in ascending order, and delimit each number with a comma (`,`) or delimit the first and last numbers with a comma (`,`). • For *number-2*, enter the ordinal number of the object which forms the suffix of the MIB object described in `subrsc_mib_oid`, that will be compared with the suffix of the MIB object described in MIB object ID. A number from 1 to 32 can be specified for *number-2*. You can specify multiple numbers. When specifying multiple numbers, write the numbers in ascending order, and delimit each number with a comma (`,`) or delimit the first and last numbers with a comma (`,`). • For *number-3*, enter the ordinal number of the object which forms the suffix of the MIB object specified in `subrsc_mib_oid`, that will be replaced with the MIB value of the MIB object specified in MIB object ID. A number from 1 to 32 can be specified for *number-3*. You can specify multiple numbers. When specifying numbers, write the numbers in ascending order, and delimit each number with a comma (`,`) or delimit the first and last numbers with a comma (`,`). • Always start an MIB object ID with a period (.).
`instance_mib_type`	• Enter the type of MIB object entered in instance_mib_oid. Specify `Counter`, `Gauge`, `Integer`, or `String`. Note that data is handled in the same way either when `Counter` is specified or when `Gauge` is specified. For the data handling according to the object type, see *Table 2-5 Types of collectable MIB objects* in *2.3.1 User resources that can be defined*. • If the MIB object data type specified in `instance_mib_oid` is Counter64 of SNMP version 2, specify `2` as the SNMP version for the corresponding resource category in the SNMP configuration file. For the SNMP configuration file, see *6.3.6 SNMP definition file (ssosnmp.conf)*.

When coding definitions related to instance MIB objects, note the following:

- When omitting the instance MIB object definition, omit the whole definition, including the key name.

(b) Definitions for the subresource MIB object

The next table lists the items that constitute a subresource MIB object definition. You must write fields in the definition file in the order in which they are listed in the following table.

Key name	Value
`subrsc_mib_oid`	Specify a MIB object ID. • The MIB object ID must start with a period (.). • Specify the MIB object ID of a node object (MIB object ID that does not include instances). • Obtain the MIB values of all instances as the MIB object using table format.

Key name	Value
subrsc_mib_type	• Specify Counter, Gauge, Integer, or String for the type of the MIB object specified in subrsc_mib_oid. For the data handling according to the object type, see *Table 2-5 Types of collectable MIB objects* in *2.3.1 User resources that can be defined*. • If the MIB object data type specified in subrsc_mib_oid is Counter64 of SNMP version 2, specify 2 as the SNMP version for the corresponding resource category in the SNMP configuration file. For the SNMP configuration file, see *6.3.6 SNMP definition file (ssosnmp.conf)*. • If Counter is specified in subrsc_mib_type, the resource value is calculated from the increase of the value of the subresource MIB object from the previous value. Therefore, the resource value is not calculated right after collection starts (at the first collection). For this reason, for such a resource, collected data saving and resource status change event issuance start when the collection interval time elapses (at the second collection) after collection starts.

When coding definitions related to subresource MIB objects, note the following:

- After the instance MIB object definition, write as many subresource MIB object definitions as the number of MIB objects to be acquired.
- When you omit an optional definition item, you can only omit the value; you must write the key name and an equal sign (=).
- If one definition file contains two or more resource definitions that have the same value assigned to the key name subrsc_mib_oid, only the first resource definition will be regarded as valid and the other resource definitions will be ignored.
- When specifying two or more subresource definitions in one resource definition, you must specify MIB object IDs with the same suffix for the key name subrsc_mib_oid contained in the subresource MIB object definitions.
- You can define up to 26 subresource MIB objects. If you define 27 or more subresource MIB objects, the first eight definitions will be regarded as valid and the 27th and subsequent definitions will be ignored.

(c) Definitions for the subresource definition

The next table lists the items that constitute a subresource definition. You must write fields in the definition file in the order in which they are listed in the following table.

Key name	Value
subrsc_label_j <<English subresource name>> ((up to 32 bytes))	Specify a Japanese subresource name. You can use not only multi-byte characters but also 1-byte alphanumeric characters and symbols. You cannot use one-byte katakana characters. The Japanese subresource name cannot include tabs, spaces, commas (,), colons (:), and/or semicolons (;).
subrsc_label_e ((up to 32 bytes))	Specify an English subresource name. For an English subresource name, you can use ASCII characters other than the tab character, space character, comma (,), colon (:), semicolon (;), forward slash (/), and escape character (\).
subrsc_mib_data (({ a - z}, *operator-symbol* { + , - , * , / }[#1] ,*integer*, *parentheses* {( )}[#2], SamplingTime))	Specify which of the MIB values specified in subrsc_mib_oid is to be used as data with reserved keywords (a to z) and operator symbols. The reserved keywords are assigned in the order specified in subrsc_mib_oid. If, however, the subresource includes an MIB whose object type is String, you must write reserved keywords alone. Therefore, you cannot write operator symbols. • When you specify a MIB expression[#3, #4], use infix notation or postfix notation. If you use postfix notation, insert one or more spaces between a value and a value, between an operator and an operator, or between a value and an operator. • It is possible to include the collection interval in the MIB expression. In this case, specify *SamplingTime* variable. The actual collection interval (seconds) will be entered automatically in *SamplingTime*. [#5] • Specify a value within 8,191 bytes from the top of the line.

#1 The usable operation method is only addition, subtraction, multiplication and division operation in a user resource.

#2 Parentheses can be used only when infix notation is used.

#3 The MIB expression referred to here is a combination of values and operators represented in the infix notation or postfix notation. The following MIB expression that is represented in the infix notation,

((*a*-*b*)/(*a*-*b* + *c*))*100

is represented in the postfix notation as follows:

a b - *a b* - *c* + / 100*

#4 The number of variables and constants that can be used in 1 MIB expression is 128 or less.

#5 The MIB expression by infix notation *(a-b)/SamplingTime* which uses *SamplingTime*, will become *a b* - *SamplingTim /* in the postfix notation.

When coding a subresource MIB object definition, note the following:

- After the subresource MIB object definition, write as many subresource definitions as the number of subresources.
- When you omit an optional definition item, you can only omit the value; you must write the key name and an equal sign (=).
- If one definition file contains two or more resource definitions that have the same value assigned to the key name `subrsc_label_j` or `subrsc_label_e`, only the first resource definition will be regarded as valid and the other resource definitions will be ignored.
- You can define up to 32 subresources.
- If a resource includes at least a subresource whose data consists of string-type MIB values, the resource is treated as a summary resource (a resource that does not allow collection (regular query) but allows only a single query).

(5) Example

The following is an example of a user resource definition file.

```
#
# resource configuration file
#

# Resource Category
rsc_category=     USER-RSC

# Network ifInOutOctets
rsc_id=           10000
rsc_label_j=      Network;InOutOctets
rsc_label_e=      Network;InOutOctets
rsc_units=        Octets/Second
rsc_threshold_MODE=1
instance_mib_oid= .1.3.6.1.2.1.2.2.1.1;1;1;1
instance_mib_type=Gauge
subrsc_mib_oid=   .1.3.6.1.2.1.2.2.1.10
subrsc_mib_type=  Counter
subrsc_mib_oid=   .1.3.6.1.2.1.2.2.1.16
subrsc_mib_type=  Counter
subrsc_label_j=   InOctets
subrsc_label_e=   InOctets
subrsc_mib_data=  a / SamplingTime
subrsc_label_j=   OutOctets
subrsc_label_e=   OutOctets
subrsc_mib_data=  b / SamplingTime
subrsc_label_j=   InOutOctets
subrsc_label_e=   InOutOctets
subrsc_mib_data=  (a + b) / SamplingTime

# FileSystem FileSystemUsedRatio
rsc_id=           10001
rsc_label_j=      file-system;file-system-utilization
rsc_label_e=      FileSystem;FileSystemUsedRatio
rsc_units=        %
rsc_threshold_MODE=1
instance_mib_oid=
         .1.3.6.1.4.1.116.5.1.2.1.21.2.1.11;1,3;1,3;1,3
instance_mib_type=String
subrsc_mib_oid=   .1.3.6.1.4.1.116.5.1.2.1.21.2.1.5
subrsc_mib_type=  Gauge
subrsc_mib_oid=   .1.3.6.1.4.1.116.5.1.2.1.21.2.1.6
subrsc_mib_type=  Gauge
subrsc_mib_oid=   .1.3.6.1.4.1.116.5.1.2.1.21.2.1.7
subrsc_mib_type=  Gauge
subrsc_label_j=   file-system-utilization
subrsc_label_e=   FileSystemUsedRatio
subrsc_mib_data=  (a - b) / (a - b + c) * 100
```

(6) Notes

(a) Storage directory for user resource definition files

Do not store any other files than the user resource configuration file under the storage directory (`$SSO_CONF/rsc` on UNIX or `$SSO_CONF\sso\rsc` on Windows) for the user resource configuration file. If a file (user resource definition file or other work file) other than the user resource configuration file is stored under the user resource configuration file storage directory, the `ssocolmng` daemon process might unduly tax the CPU or consume memory.

(b) Procedure to change user resource definitions

For how to add, change, and delete a user resource definition, see *2.3.2 User resource definition*.

(c) Handling of division by zero during resource value calculation

When the value of a resource is calculated during resource reference or collection, the result of division by 0 is always treated as 0.

(d) Subresource ID

Subresource IDs are automatically assigned to the subresources of a user resource.

Sequential numbers beginning with 1 are assigned as subresource IDs to the subresources of a resource in the order of the subresource definitions in the resource definition.

Example

When a subresource is defined by the fifth definition among the definitions for a resource, subresource ID `5` is assigned to the subresource.

6.3.15 Resource-icon definition file

In the resource-icon definition file, define the resource icons to be displayed on the SSO's GUI.

When you create a resource-icon definition file for a user resource definition, store the file under the following directory:

- Directory for resource-icon definition file storage

  For UNIX

  ```
  $SSO_IMAGE/category-name#
  ```

  For Windows

  ```
  $SSO_IMAGE\category-name#
  ```

  #

  As *category-name*, specify the category name set in the user resource definition file.

The next table lists the formats of the icons to be defined. The file format is GIF89a.

Icon	Size (in pixels)	Window
Category icon (small)	13 **x** 13	• Collecting Condition Configuration window • Collected Data Reference window
Category icon (large)	24 **x** 24	• Resource Browser window • Collection Condition Addition wizard
Resource group icon	24 **x** 24	• Resource Browser window • Collection Condition Addition wizard • Report Configuration window • Report Condition Addition wizard
Resource icon	24 **x** 24	• Resource Browser window • Collection Condition Addition wizard • Report Configuration window • Report Condition Addition wizard

JP1/Cm2/SSO determines whether original icon files for categories and resources have been created. If no original icon files have been created, SSO searches for its own icon files. The following table shows the order in which SSO searches for icon files.

Table 6-3: Icon file search order (for UNIX)

Icon	Search order 1	Search order 2
Category icon (small)	`$SSO_IMAGE/`*category-name*`/CATEGORY_S.gif`	`$SSO_IMAGE/CATEGORY_S.gif`
Category icon (large)	`$SSO_IMAGE/`*category-name*`/CATEGORY_L.gif`	`$SSO_IMAGE/CATEGORY_L.gif`
Resource group icon	`$SSO_IMAGE/`*category-name*`/GROUP_<`*resource-ID*`>`[#]`.gif`	`$SSO_IMAGE/GROUP.gif`
Resource icon	`$SSO_IMAGE/`*category-name*`/`*resource-ID*`.gif`	`$SSO_IMAGE/RESOURCE.gif`

#

As *resource-ID*, specify the resource ID of one of the resources in the relevant group. Note, however, that if you specify the resource ID of a summary resource (which includes a subresource containing string-type MIB values as data), the group icon is not normally displayed in the Resource Configuration window and Resource Data Reference window. When group icons need to be displayed in the windows, specify the resource ID of a non-summary resource. You can specify the resource ID of a summary resource as *resource-ID* if the group does not include any non-summary resources or if group icons do not need to be displayed in the windows.

Table 6-4: Icon file search order (for windows)

Icon	Search order 1	Search order 2
Category icon (small)	`$SSO_IMAGE\`*category-name*`\CATEGORY_S.gif`	`$SSO_IMAGE\CATEGORY_S.gif`
Category icon (large)	`$SSO_IMAGE\`*category-name*`\CATEGORY_L.gif`	`$SSO_IMAGE\CATEGORY_L.gif`
Resource group icon	`$SSO_IMAGE\\`*category-name*`\GROUP_<`*resource-ID*`>`[#]`.gif`	`$SSO_IMAGE\GROUP.gif`
Resource icon	`$SSO_IMAGE\`*category-name*`\`*resource-ID*`.gif`	`$SSO_IMAGE\RESOURCE.gif`

#

As *resource-ID*, specify the resource ID of one of the resources in the relevant group. Note, however, that if you specify the resource ID of a summary resource (which includes a subresource containing string-type MIB values as data), the group icon is not normally displayed in the Resource Configuration window and Resource Data Reference window. When group icons need to be displayed in the windows, specify the resource ID of a non-summary resource. You can specify the resource ID of a summary resource as *resource-ID* if the group does not include any non-summary resources or if group icons do not need to be displayed in the windows.

6.3.16 Monitor status definition file

The monitoring status definition file contains definitions of the monitoring status of a process or service.

(1) Format

The following shows the format of the monitoring status definition file.

```
server=monitoring-target-server-name          } Monitoring target server definition
apname=monitoring-target-application-name     } Monitoring target application definition
```

(2) Details of the monitoring target server definition

Write as many definitions as the number of monitoring target servers. This definition requires one or more definitions for the monitored application.

The following table shows the content of the definition.

Key name	Explanation
server	Enter the monitoring target server name. For the server name, specify the host name or IP address within 255 bytes.

(3) Details of the monitored application definition

After the monitoring target server definition, write as many monitored application definitions as the number of applications to be monitored on the target servers.

The following table shows the content of the definition.

Key name	Explanation
apname	Enter the name of the monitoring target application. Enter an application name of 128 bytes or less.

(4) Example

The following shows an example of a monitoring status definition file.

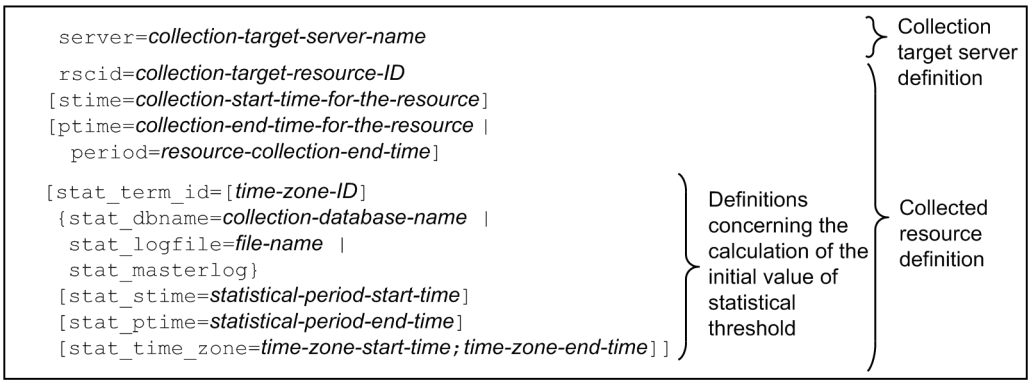
```
#
# Monitoring status definition file
#
server=netmw61
apname=JP1/Cm2/NNM V6i NT
apname=ap1
server=netmw81
apname=JP1/Cm2/NNM V6i NT
apname=ap1
        :
        :
```

6.3.17 Collecting condition definition file

The collecting condition definition file contains definitions of the resource collection status.

(1) Format

The following shows the format of the collecting condition definition file.



(2) Details of the collection target server definition

Write as many definitions as the number of collection target servers. This definition requires one or more definitions for the collected resource.

The following table shows the contents of the definition for the collection target server.

Key name	Explanation
`server`	Enter the collection target server name. Specify a server name, host name or IP address within 255 bytes. If you specify an IP address, use the IPv4 address or IPv6 address format.

(3) Details of the collected resource definition

After the collection target server definition, write as many collected resource definitions as the number of resources to be collected by target server. You must write fields in the definition file in the order in which they are listed in the table below.

The following table shows the contents of the definition regarding collected resources.

Key name	Explanation
`rscid`	Specify the collection target resource ID. For details of the resource ID, see *E. Resource IDs*.
`stime`	Specify the collection start time for the resource. Specify this in the same format as the `-stime` option of the `ssocolstart` command. When the specification is omitted, or the specified collection start time has already passed, the collection will be started when the command is executed.
`ptime`	Specify the collection end time for the resource. Specify this in the same format as the `-ptime` option of the `ssocolstart` command. When both this key and the `period` key are omitted, this indicates that the resource collection condition will be collected indefinitely. Also, this key cannot be specified at the same time as the `period` key.
`period`	Specifies the resource collection end time, by the amount of time passed since the collection start time. Specify this in the same format as the `-period` option of the `ssocolset` command. When both this key and the `ptime` key are omitted, this indicates that the resource collection conditions will be collected indefinitely. Also, this key cannot be specified at the same time as the `period` key.
`stat_term_id` <<1>> ((1 to 10))	Specify the time zone ID of the time zone for which to calculate the initial value of the statistical threshold. When collection starts, an initial value is calculated for the same time zone ID as that of regular calculation. For other time zone IDs, an initial value is calculated for a specific time zone ID when the time zone ID of regular calculation is switched to the same one as that of the specific time zone ID. Specify this definition item for each resource ID.
`stat_dbname`	Specify the name of a master database or collection database.
`stat_logfile`	Specify an absolute path as the file name.#
`stat_masterlog`	Specify the key name when you specify the master database on the local host.
`stat_stime` ((1980.01.01.00.00.00 to 2029.12.31.23.59.59))	Specify the start time of the statistical period. When this key is omitted, the start time is the same as the start time specified for the collection database. You cannot specify the same time as that specified in `stat_ptime`.
`stat_ptime`	Specify the end time of the statistical period. You cannot specify the same time as or an earlier time than the time specified in `stat_ptime`.

Key name	Explanation
((1980.01.01.00.00.00 to 2029.12.31.23.59.59))	Specify the end time of the statistical period. You cannot specify the same time as or an earlier time than the time specified in `stat_ptime`.
`stat_time_zone` start time ((00:00:00 to 23:59:59)) end time ((00:00:01 to 24:00:00))	Specify the start time and end time of the time zone. Delimit each value with a semicolon (`;`). You can specify the start and end times for up to five time zones. When this key is omitted, no time zone is set and data will be extracted regardless of the time. An error occurs in the following cases: • Overlapping time zones are specified. • The time zone start time is the same as the time zone end time.

#: An error occurs if no collection database exists when the defined time zone ID is the same as the time zone ID defined in the collection conditions definition file.

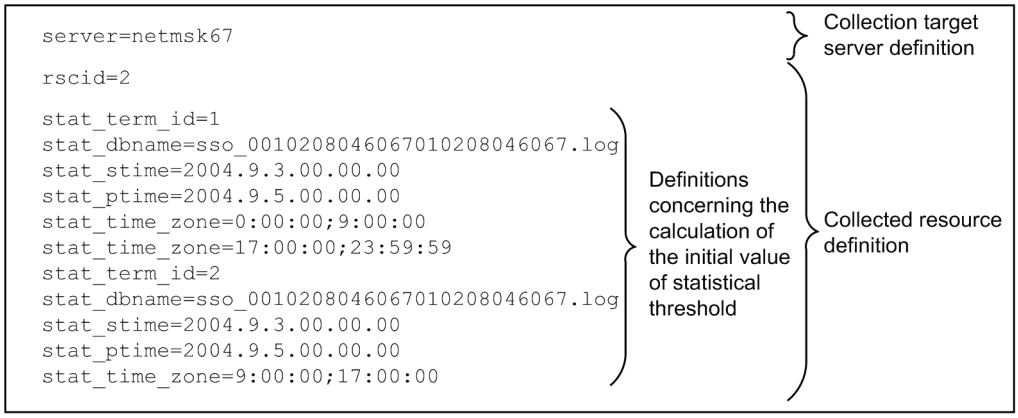
Note the following for the definition concerning the initial value of the statistical threshold:

- When omitting a definition item, omit the whole definition item, including the key name.

(4) Example

The following shows an example of a collecting condition definition file.

Example of collection conditions definition file (defining the initial value calculation for a statistical threshold)

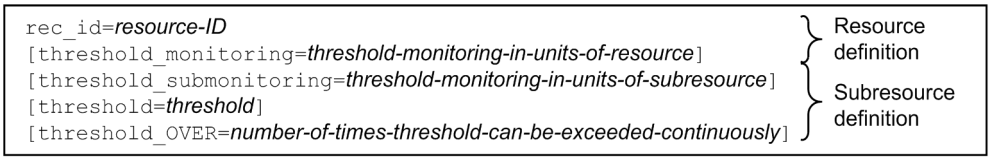


6.3.18 Threshold definition file (ssothreshold.conf)

In the threshold definition file, define the initial value of a fixed threshold for threshold monitoring.

(1) Format

The following shows the format of the threshold definition file.



(2) Details of resource definition

Key name	Value
rsc_id	Specify a resource ID[#1].
threshold_monitoring <<N[#2]>>	Specify whether to perform the threshold check on collected data for all subresources. Write Y to perform the check or N to not perform the check.

#1: For the correspondence between resource IDs and resources, see *E. Resource IDs*.

#2: Some resources might require you to specify Y.

When coding a resource definition, note the following:

- Write as many resource definitions as the number of resources to be defined.
- When omitting the threshold_monitoring definition, omit the whole definition, including the key name.
- If the definition of a resource includes multiple definitions of threshold_monitoring, the definition written first is assumed to be valid, and the definitions written subsequently are assumed to be invalid.
- If the definition file includes multiple resource definitions whose rsc_id value is the same, the definition written first is assumed to be valid, and the definitions written subsequently are assumed to be invalid.

(3) Details of subresource definition

Key name	Value
threshold_submonitoring <<N[#]>>	Specify whether to perform the threshold check on collected data for each subresource. Write Y to perform the check or N to not perform the check. Definition of this key overrides the definition of threshold_monitoring.
threshold ((0, or integer or floating decimal point (double precision number) between ± 1.00 **x** 10^{-2} to ± 1.7976931348623157 **x** 10^{127}))	Specify the warning threshold and critical threshold. Delimit each threshold with a semicolon (;).
threshold_OVER <<1;1>> ((1 to 99))	Specify the number of times the warning threshold can be exceeded continuously and number of times the critical threshold can be exceeded continuously. Delimit each continuous over count with a semicolon (;).

#: Some subresources might require you to specify Y.

When coding a subresource definition, note the following:

- After the resource definition, write as many subresource definitions as the number of subresources to be defined.
- When omitting the threshold definition, omit only the value of the definition. The key name and equal sign, however, must be written. When omitting the threshold_submonitoring or threshold_OVER definition, omit the whole definition, including the key name.
- If a subresource definition includes multiple definitions of threshold_submonitoring and threshold_OVER, the definitions written first are assumed to be valid, and the definitions written subsequently are assumed to be invalid.
- If a resource definition includes more subresource definitions than the specified number of subresources, only the subresource definitions as many as the specified number of resources become valid, when counted from the top, and subsequent definitions become invalid.
- If a resource definition includes less subresource definitions than the specified number of subresources, the subresource definitions that are not written are assumed to be omitted.

(4) Example

The following shows an example of a threshold definition file.

```
#
# SSO Threshold Definition File
#

## CPU Utilization
rsc_id=2
threshold_monitoring=N
# Total CPU
threshold_submonitoring=Y
threshold=60;70
threshold_OVER=1;1
# User CPU
threshold_submonitoring=N
threshold=50;80
threshold_OVER=2;1
# System CPU
threshold_submonitoring=Y
threshold=80;90
threshold_OVER=2;3
# Weight CPU
threshold_submonitoring=N
threshold=85;95
threshold_OVER=1;1

## Interface Utilization
rsc_id=30
threshold_monitoring=Y
# Total
threshold_submonitoring=Y
threshold=30;50
threshold_OVER=1;1
# Average
threshold_submonitoring=N
threshold=50;50
threshold_OVER=1;1
```

6.3.19 Threshold verification definition file

In the threshold verification definition file, define the conditions for verifying thresholds.

(1) Format

In a threshold verification definition file, you can write verification conditions for fixed and statistical thresholds together. The following shows the format of the threshold verification definition file.

```
 rscid=resource-ID
[stime=start-time]
[ptime=end-time]
[col_range=time-range-of-verification-object]
[stat_sum_time=statistical-total-time]
[stat_timing={time-interval|time,...}]
 subrscid=subresource-ID
 instance=instance-Name
 threshold=[stat]warning-threshold;critical-threshold
 threshold_OVER=number-of-times-threshold-can-be-exceeded-continuously
```

Resource definition

Subresource and instance definition

(2) Details of resource definition

The table below describes the contents of the definitions concerning resources in the threshold verification definition file. You must write fields in the definition file in the order in which they are listed in the following table.

Key name	Value
`rscid`	Specify the resource ID of the verification object. If you specify multiple resource IDs, define all the necessary keys as separate key definitions.
`stime`	Specify the start time of verification object based on the information extracted from the database. Specifiable parameters are year, month, day, hour, minute, and second. If this key is omitted, the start time is the earliest time recorded among the extracted data.
`ptime`	Specify the end time of verification object based on the information extracted from the database. Specifiable parameters are year, month, day, hour, minute, and second. If this key is omitted, the end time is the latest time recorded among the extracted data.
`col_range` start time ((00:00:00 to 23:59:59)) end time ((00:00:01 to 24:00:00))	Specify the time range of verification objects by specifying the start time and end time. Delimit hour, minute, and second values with a colon (`:`). Delimit start time and end time with a semicolon (`;`). If you specify multiple points of time, write them continuously as separate key definitions. You can define this key up to five times.
`stat_sum_time` ((24 to 720))	Specify the total length of the time zones to calculate the statistical threshold.
`stat_timing`	Specify the time or interval to calculate the statistical threshold. If this key is omitted, the statistical threshold is calculated at intervals of 1 hour. • Time specification Specify the time to calculate in the *hour*`:`*minute* format. When you specify multiple points of time, delimit the time value with a comma (`,`). Specifiable values are from `0:00` to `23:59`. • Interval specification Specify the interval of calculation in minutes (`m`) or hours (`h`) in a range from `15m` to `24h`. Specification of multiple intervals causes an error.

When coding a resource definition, note the following:

- Write as many resource definitions as the number of resources to be defined.

(3) Details of subresource and instance definition

The table below describes the contents of the definitions concerning subresources and instances in the threshold verification definition file. You must write fields in the definition file in the order in which they are listed in the following table.

Key name	Value
`subrscid`#	Specify the subresource ID of the verification object. Specification of a nonexistent subresource ID causes an error.
`instance` ((character string of up to 255 bytes))	Specify the instance name of the verification object instance by a character string of up to 255 bytes. You can specify multiple instance names successively to verify multiple instances.
`threshold` • For fixed threshold ((0, or floating decimal point between $\pm$ 1.00 **x** 10^{-2} to $\pm$ 1.7976931348623157 **x** 10^{308}))	• For fixed threshold (when `stat` is not specified) Specify the thresholds for verification in the order of warning threshold first and then critical threshold, while delimiting each threshold with a semicolon (`;`). A threshold must be 0 or a floating point number from $\pm$ 1.00 **x** 10^{-2} to $\pm$ 1.7976931348623157 **x** 10^{308}. If the mantissa of the number exceeds 1.7976931348623157, round it off. You can specify the same value for

Key name	Value
• For statistical threshold <<99.95;99.99>> ((0.01 to 99.99))	the warning and critical thresholds. When the same value is specified, the warning region is eliminated. • For statistical threshold (when stat is specified) After specifying stat, specify the ratios of data to be verified (as thresholds) in the order of warning threshold first and then critical threshold, delimiting each threshold with a semicolon (;). A threshold must be in the range from 0.01 to 99.99, and can be specified with up to 2 digits after the decimal point.
threshold_OVER ((1 to 99))	Specify the number of times the threshold can be exceeded continuously.

#

For the subresource IDs that are assigned to the subresources of user resources, see *6.3.14(6)(d) Subresource ID*.

For the subresource IDs if the resources provided by SSO, see *E. Resource IDs*.

When coding a subresource and instance definition, note the following:

- After the resource definition, write as many subresource and instance definitions as the number of combinations of subresource and instance to be defined.

(4) Examples

The following shows examples of a threshold verification definition file.

Example of definitions in the threshold verification definition file (when fixed thresholds and multiple instances are specified)

```
# CPU Utilization
rscid=2
stime=2004.10.14.00.00.00
ptime=2004.10.14.15.10.59
col_range=01:00:00;03:00:00
col_range=05:00:00;07:59:59
subrscid=1
instance=0
threshold=1;2
threshold_OVER=1;1
subrscid=1
instance=1
threshold=1;2
threshold_OVER=1;1
```

Specify the multiple instance

Example of definitions in the threshold verification definition file (when fixed thresholds and multiple subresources are specified)

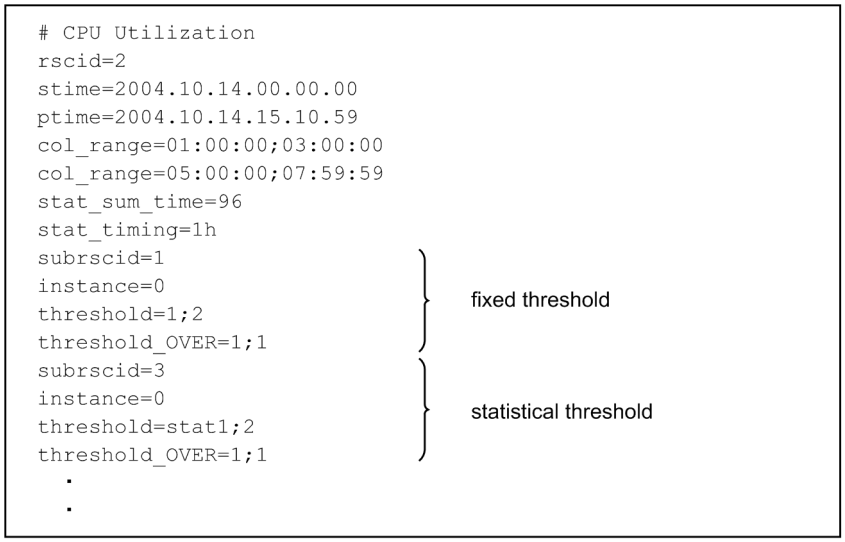
```
# CPU Utilization
rscid=2
stime=2004.10.14.00.00.00
ptime=2004.10.14.15.10.59
col_range=01:00:00;03:00:00
col_range=05:00:00;07:59:59
subrscid=1
instance=0
threshold=1;2
threshold_OVER=1;1
subrscid=2
instance=0
threshold=1;2
threshold_OVER=1;1
```

Specify the multiple subresource

Example of definitions in the threshold verification definition file (when statistical thresholds are specified)

```
# CPU Utilization
rscid=2
stime=2004.10.14.00.00.00
ptime=2004.10.14.15.10.59
col_range=01:00:00;03:00:00
col_range=05:00:00;07:59:59
stat_sum_time=96
stat_timing=02:00
subrscid=1
instance=0
threshold=stat1;2
threshold_OVER=1;1
subrscid=3
instance=0
threshold= stat1;2
threshold_OVER=1;1
    .
    .
```

Example of definitions in the threshold verification definition file (when fixed and statistical thresholds are specified)



6.3.20 TCP agent definition file (ssotcpagent.conf)

In the TCP agent definition file, define the APM to be a target of TCP health check.

(1) Format

In a TCP agent definition file, specify the definition for each agent on a line. Delimit each definition item with a colon (**:**). Note the following when creating the TCP agent definition file:

- The TCP health check is performed for a specified agent only when the version of the APM on the specified agent is 08-00 or later. For other agents, the health check by using SNMP (UDP) is performed as normal.
- If no TCP agent definition file is found in the `$SSO_CONF` directory, the health check by using SNMP (UDP) is performed for all agents as normal.
- If the definition file includes multiple definitions for the same agent, the definition written first is assumed to be valid, and the other definitions are ignored. Therefore, if a definition specifying `*.*.*.*` as the IP address of the monitoring target agent is written at the top of the definition file, that definition applies to all agents.

- To apply updates in this definition file, restart the `ssoapmon` daemon process or execute the `ssoapcom -r` command.

(2) Details of definition

Item	Value
IP-address	Specify the IP address of the monitoring target agent in the *n*.*n*.*n*.*n* format. For *n*, you can specify a value from 0 to 255 or an asterisk (`*`) or question mark (`?`) as a wild card.
port-number <<20307>> ((1 to 65535))	Specify the port number to be used to perform the health check for the monitoring target agent. The port number must match the value of the `LISTENPORT` key in the TCP service definition file on the monitoring target agent.
response-monitoring-time <<50>> ((10 to 36000))	Specify the response monitoring time during the health check for the monitoring target agent. Specify the time in units of 1/10 second.
retry-count <<1>> ((0 to 99))	Specify the number of retries to be attempted when the health check on the monitoring target agent fails.

(3) Example

The following shows an example of a TCP agent definition file.

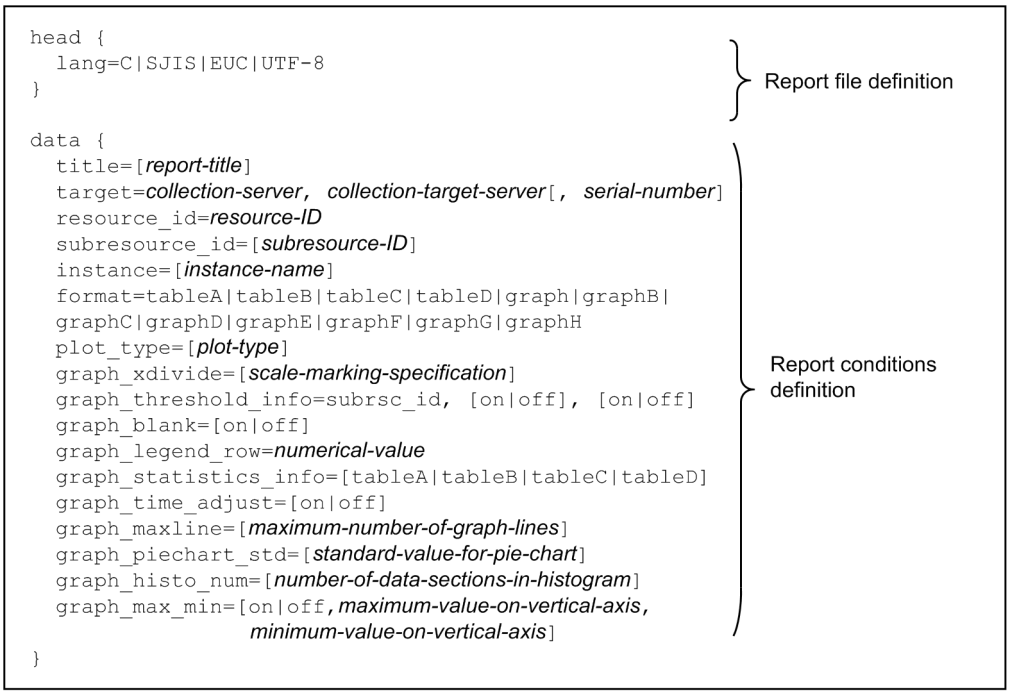
```
#
# ssotcpagent.conf
#
# FORMAT
#   IPaddress:Port:TimeOut:Retry:
#

# 1. Specific Hosts
10.208.46.62:20308:100:1:

# 2. IP Address Wildcards
10.208.4?.*::80:1:

# 3. Default
*.*.*.*::::
```

6.3.21 Report definition file

Define report conditions in the report definition file. You can also use the Report Condition Configuration window to create this file.

(1) Format

The following shows the format of the report definition file.



(2) Details of the report file definition

Define the language used to define the report definition file. Write one definition in each report definition file. Enclose the contents of the definition in braces as follows:

```
head{ contents-of-definition }
```

The next table lists the items that must be, or can be, defined in the report definition file.

Key name	Value
`lang`	Specify one of the following values as the language to be used when a report file is output: • English: `C` • Japanese (Shift-JIS): `SJIS` • Japanese (EUC): `EUC` • Japanese (UTF-8): `UTF-8` All the titles specified in the definition file are converted into the language specified in this key when a report file is output. The character encoding of the report definition file must match the character encoding specified here.

(3) Details of the report conditions definition

Define report conditions. Define report conditions repeatedly for the number of the reports to be displayed in one report file. You can define as many report conditions as the value specified in the `max-data` key in the `ssorptd` action definition file. Enclose each report condition in braces as follows:

```
data{ contents-of-definition }
```

The next table lists the report conditions to be defined in the report definition file.

Key name	Value
`title` ((character string of up to 255 bytes))	Specify the title of each report. You can write spaces in the title.
`target`	Specify the collection server, collection target server, and the serial number to be output to the report, separated by commas (,). • Collection server: specify the monitoring manager. • Collection target server: specify the monitoring server. • Serial number[#1]: specify the serial number of the copy database to be reported. Specify none when you report the master database.
`resource_id`	Specify the resource ID to be output to the report.
`subresource_id`[#2]	Specify the subresource ID to be output to the report. If you omit this item, all subresources are to be output to the report.
`instance` ((character string of up to 255 bytes))	Specify the instance name of the instance to be reported. To specify multiple instance names, specify this key multiple times. If you omit this item, all instances are to be output to the report. You cannot specify an instance name that has a space character at the beginning or the end.
`format`	Specify a report type. `tableA`: Outputs the report in the table format that lists subresources in columns and instances in rows. `tableB`: Outputs the report in the table format that lists instances in columns and subresources in rows. `tableC`: Outputs the report in the table format that lists data according to instance. `tableD`: Outputs the report in the table format that lists data according to subresource. `graph`: Outputs the report in the line graph format. `graphB`: Outputs the report in the histogram format. `graphC`: Outputs the report in the bar graph format that displays data according to subresource. `graphD`: Outputs the report in the bar graph format that displays data according to instance. `graphE`: Outputs the report in the stacked bar graph format that displays data according to subresource. `graphF`: Outputs the report in the stacked bar graph format that displays data according to instance. `graphG`: Outputs the report in the pie chart format that displays data according to subresource. `graphH`: Outputs the report in the pie chart format that displays data according to instance. If you omit this key, `tableA` is assumed to be specified.
`plot_type` ((5 minutes to 1 day))	Specify the plot type for the output in a graph format. The average data at the specified time is plotted in the graph. You can specify *m* (minute), *h* (hour), or *d* (day) as the unit. • When the report output format is the line graph: An average of collected data is calculated at intervals of the time specified in `plot_type`, and the average values are used to determine plot points. The line formed by connecting adjacent plot points is a collected-data line. If no data is collected during a plot interval, no plot point is created. In such a case, the period in which no plot point is created is ignored, and the next plot point is used to plot the line. • When the report output format is the bar graph or stacked bar graph: An average of collected data is calculated at intervals of the time specified in `plot_type`, and the average values are displayed in a bar graph. If no data is collected during a plot interval, no bar is displayed for the period in the graph. • When the report output format is the pie chart: An average of collected data is calculated at intervals of the time specified in `plot_type`, and the ratios between elements are displayed in a pie chart. If a standard value for pie chart is specified in `graph_piechart_std`, the percentage of each element in relation to the specified value is displayed in the pie chart. • When the report output format is the table or histogram: This key is ignored even if a value is specified.
`graph_xdivide`	Specify the scale on the time axis for a report to be output in a graph format. For a report in a table format, this key is ignored.

Key name	Value
<<4n>> When number of division: ((1 to 60)) When time specification: ((1 minutes to 365 day))	Write a unit after the numerical value to be specified. Write n (number of divisions), m (minute), h (hour), or d (day) as the unit. When a number of divisions is to be specified (when the unit is n), the specifiable range of values is 1 to 60. When a time interval is to be specified (when the unit is m, h, or d), the specifiable range of values is 1 minutes to 365 days. Specification of an invalid value or unit causes an error in report creation and disables report creation.
graph_threshold_info <<*,off,off>>	Specify whether to display threshold information in the report to be output in a graph format. For a report in a table format, this key is ignored. subrsc_id Specify the target subresource ID. The ID to be specified must match the subresource_id definition. If you specify *, the specification of this key applies to all the subresources to be output in the report. If you specify an ID instead of *, specify a unique ID. [on|off] (first) Specify whether to display the warning threshold. When on is specified, the threshold is displayed. When off is specified, the threshold is not displayed. [on|off] (second) Specify whether to display the critical threshold. When on is specified, the threshold is displayed. When off is specified, the threshold is not displayed. If both * and a subresource ID are specified, * overrides. Specification of an invalid value or character string causes an error in report creation and disables report creation. When the display of threshold line is specified, the threshold line is output as the line whose value is 0 if threshold monitoring is not performed for the subresource or instance that is the object of threshold display.
graph_blank <<off>>	Specify whether to display a graph line when no resource data was collected during the time interval specified for each plot type in the specified data extraction period. For a report in a table format, this key is ignored. [on|off] When on is specified, the graph line is not displayed (the blank is not reflected). When off is specified, the graph line is displayed (the blank is reflected). Specification of an invalid value or character string causes an error in report creation and disables report creation.
graph_legend_row <<10>> ((integer from 0 to 100))	Specify the number of rows of instance display in the legend for a graph. For a report in a table format, this key is ignored. Numerical value When a value is specified, the legend is output in the format to display instances separately for each subresource. When no value is specified or this key is omitted, the legend is output in the format to display instances by line wrapping for the number of instances. When a value is specified, the legend is displayed with the specified number of columns even if the number of instances is larger than the specified number of columns. If the number of instances is smaller than the specified number of columns, the legend is displayed with the same number of columns as the number of instances. Specification of an invalid value or character string causes an error in report creation and disables report creation.
graph_statistics_info	Specify whether to display statistical information in a graph. For a report in a table format, this key is ignored. [tableA|tableB|tableC|tableD] Specify a table format among the values that can be specified in the format key. When a value is specified, statistical information is displayed in the specified table format under the graph. When no value is specified or this key is omitted, statistical information is not displayed. Specification of an invalid value or character string causes an error in report creation and disables report creation.
graph_time_adjust <<off>>	Specify whether to apply the start time and end time specified for the data extraction period to the start time and end time on the time axis of the graph. For a report in a table format, this key is ignored.

Key name	Value
`graph_time_adjust <<off>>`	When `on` is specified: The start time and end time specified for the data extraction period are used as the start time and end time on the time axis of the graph. When `off` is specified: The earliest time and latest time of resource data collected during the data extraction period are used as the start time and end time on the time axis of the graph. If `on` is specified when either the start time or end time, or both, are not specified for the data extraction period, the time to be applied when `off` is specified is applied to the time that is not specified. Specification of an invalid value or character string causes an error in report creation and disables report creation.
`graph_maxline <<64>>` ((1 to 1024))	Specify the maximum number of graph lines that can be displayed in the bar graph, stacked bar graph, or pie chart.
`graph_piechart_std <<100>>` ((1 **x** 10^{-2} to 1.7976931348623157 **x** 10^{308}))	When the report format is the pie chart, specify a value that is used as the 100-percent value to calculate the percentages of graph elements and display them in a pie chart.
`graph_histo_num <<10>>` ((4 to 20))	When the report format is histogram, specify the number of data sections.
graph_max_min `<<off,100.00,0.00>>` ((-1.7976931348623157 **x** 10^{308} to 1.7976931348623157 **x** 10^{308}))	When you specify `on`, a maximum value on the vertical axis, and a minimum value on the vertical axis, the maximum value and minimum value are set for the vertical axis of the graph. If a value in the graph is more than the set maximum value on the vertical axis or less than the set minimum value on the vertical axis, the vertical axis is adjusted automatically. Similarly, the vertical axis is adjusted automatically when a threshold is more than the set maximum value on the vertical axis or less than the set minimum value on the vertical axis. • The specified maximum value must be larger than the specified minimum value. • For the histogram, specify 4,294,967,295 or less as the maximum value and 0 or more as the minimum value. For a graph other than the histogram, specify maximum and minimum values between which the difference is 1.7976931348623157 **x** 10^{308} or less. • As the maximum value and minimum value, specify values that have at most 2 digits after the decimal point. (If a value that has 3 or more digits after the decimal point is specified, the value is rounded off to 2 decimal places.) When `off`, a maximum value and a minimum value are specified on the vertical axis, and the action to be taken when `on` is specified is disabled. Then, the maximum and minimum values on the vertical axis are set automatically. Note, however, that the maximum and minimum values specified in this key are checked for validity (the valid range of the values on the vertical axis in a created graph is the same as that of SSO version 08-00).

#1

You can reference serial numbers by executing the `ssoextractlog` command with the `-list` option specified.

#2

For the subresource IDs that are assigned to the subresources of user resources, see *6.3.14(6)(d) Subresource ID*.

For the subresource IDs of the resources provided by SSO, see *E. Resource IDs*.

The following table describes how individual key definitions are applied to individual types of HTML-format reports.

Table 6-5: How key definitions are applied to HTML-format reports

Key value	Multiple definitions	Omission	Report type					
			Table	Line graph	Histogram	Bar graph	Stacked bar graph	Pie chart
`title`	N	Y	Y	Y	Y	Y	Y	Y

Key value	Multiple definitions	Omission	Report type					
			Table	Line graph	Histogram	Bar graph	Stacked bar graph	Pie chart
target	N	N	Y	Y	Y	Y	Y	Y
resource_id	N	N	Y	Y	Y	Y	Y	Y
subresource_id	Y	Y	Y	Y	Y	Y	Y	Y
instance	Y	Y	Y	Y	Y	Y	Y	Y
format	N	Y	Y	Y	Y	Y	Y	Y
plot_type	N	Y	N	Y	N	Y	Y	Y
graph_xdivide	N	Y	N	Y	N	N	N	N
graph_threshold_info	Y	Y	N	Y	N	N	N	N
graph_blank	N	Y	N	Y	N	N	N	N
graph_legend_row	N	Y	N	Y	Y	Y	Y	Y
graph_statistics_info	N	Y	N	Y	N	Y	Y	Y
graph_time_adjust	N	Y	N	Y	N	Y	Y	Y
graph_maxline	N	Y	N	N	N	Y	Y	Y
graph_piechart_standard	N	Y	N	N	N	N	N	Y
graph_histo_num	N	Y	N	N	Y	N	N	N
graph_max_min	N	Y	N	Y	Y	Y	Y	N

Legend:

Y: The key definition is applied.

N: The key definition is not applied.

(4) Example

The following is an example of defining the report definition file.

```
#
# Report Definition File for SNMP System Observer
#

head {
  lang=SJIS
}

data {
  title=General affairs server 1
  target=soumu01,soumu01
  resource_id=34
  subresource_id=1
  instance=C:\
  instance=D:\
  instance=E:\
  format=graph
  plot_type=2h
  graph_xdivide=4n
  graph_blank=on
  graph_threshold_info=1,on,off
  graph_time_adjust=on
}
data {
  title=General affairs server 2
  target=soumu01,soumu02
  resource_id=32
  subresource_id=1
  subresource_id=2
  subresource_id=3
  instance=0
  instance=1
  format=tableA
  graph_xdivide=1d
  graph_blank=off
  graph_threshold_info=1,off,off
  graph_threshold_info=2,on,off
  graph_threshold_info=3,on,on
  graph_legend_row=5
  graph_statistics_info=tableD
}
```

(5) Note

If you write an invalid definition in the report definition file, an error is output as follows:

- When creating a report by using the `ssodemandrpt` command:
  The error is output to the standard output and a log file.
- When creating a report from the GUI:
  The error is output as an error message and output to a log file.

6.3.22 ssorptd action definition file (ssorptd.def)

Define `ssorptd` daemon process actions in the `ssorptd` action definition file. If you have made any changes in this definition file, perform one of the following operations to apply these changes:

- Execute the `ssorptd -r` command.
  Note that the changes might not become valid depending on the key that has been changed.
- Restart the `ssorptd` daemon process.

(1) Format

The following shows the format of the `ssorptd` action definition file.

```
[max-logfile-size:      maximum-size-of-logging-file]
[logfile-num:           number-of-the-log-files]
[trace:                 on|off]
[max-tracefile-size:    maximum-size-of-trace-file]
[tracefile-num          number-of-the-trace-files]
[max-client:            maximum-number-of-concurrent-connections-with-GUI-and-command]
[max-data:              maximum-number-of-report-conditions-per-report-definition-file]
[default-disp-address: collecting-server-IP-address-to-be-displayed-in-Report-Condition-Addition-wizard]
[exponential-notation: on|off]
```

When coding definitions in the `ssorptd` action definition file, note the following:

- If the definition file includes multiple definitions for the same item, the definition written last is assumed to be valid, and those definitions preceding the last definition are ignored.
- When omitting the specification of a key on a line, omit the whole line.

(2) Description

The next table lists the items that must be, or can be, defined in the `ssorptd` action definition file.

Key name	Value
`max-logfile-size:` <<4>>((1 to 32 megabytes))	Specify the maximum size of a log file.
`logfile-num:` <<3>> ((1 to 10))	Specify the number of the log files.
`trace:` <<off>>	Specify whether to output a trace file for troubleshooting at failure occurrence. To output the trace file, specify `on`. To not output the trace file, specify `off`.
`max-tracefile-size:` <<4>> ((1 to 32 megabytes))	Specify the maximum size of a trace file.
`tracefile-num:` <<3>> ((1 to 10))	Specify the number of the trace files.
`max-client:` <<2>> ((1 to 99))	Specify the maximum number of concurrent sessions the `ssorptd` daemon process allows for the connections via the Report Configuration window and the report command (`ssodemandrpt`). In other words, specify the maximum number of concurrent sessions with the Report Configuration window and the report command (`ssodemandrpt`). Note that one of the specified number of sessions is always secured for the Report Configuration window. Also, regardless of the setting of this key, multiple Report Configuration windows cannot be opened concurrently.
`max-data:`[#2] <<20>> ((1 to 64))	Specify the maximum number of report conditions that can be defined in a report definition file. Note To create a report, as many `ssoextractlog` commands as the number of report conditions are executed concurrently. Therefore, if you increase the value of this key, you must add that increase to the value of the `max-client:` key in the `ssocolmng` action definition file (`ssocolmng.def`).
`default-disp-address:` <<none>>	Specify the collecting server IP address to be displayed in the *host-name* format (*IP-address*) in the Report Condition Addition wizard.

Key name	Value
`default-disp-address:` `<<none>>`	Specify the same value as that specified in the `change-my-address:` key in the `ssocolmng` action definition file.
`exponential-notation:` `<<on>>`	Select the format in which values are displayed for the scale markings on the vertical and horizontal axes of the graphs in HTML-format report files if values to be displayed are 1,000,000 or larger. You can select one of two formats. One is the integer or decimal fraction display format, and the other is the exponent display format. The selected format is applied to line graphs, histograms, bar graphs, and stacked bar graphs. When `on` is specified, exponent display is used. When `off` is specified, integer or decimal fraction display is used. Note that if the value of a scale marking is less than 1,000,000, integer or decimal fraction display is used regardless of the specification in this key. Note If a scale marking exceeds 17 digits (including the minus sign), the displayed value might protrude from the vertical axis or outside the graph frame or be partly hidden. In such a case, specify `on` (exponent display) in this key. For the text display in a graph, see also *Note* in *2.4.2(2) HTML-format report files*.

#1 If you change the value of this item, you must restart the `ssorptd` daemon process.

#2 If you change the value of this item, you must restart the Report Configuration window.

6.3.23 ssoconsoled action definition file (ssoconsoled.def)

In the `ssoconsoled` action definition file, define the actions of the `ssoconsoled` daemon process. If you have made any changes in this definition file, perform one of the following operations to apply these changes:

- Execute the `ssoconsoled -r` command.
  Note that the changes might not become valid depending on the key that has been changed.
- Restart the `ssoconsoled` daemon process.

(1) Format

The following shows the format of the `ssoconsoled` action definition file.

```
[authentication:          SSO-console-login-authentication-method]
[logical-hostname:        logical-host-name]
[logout-time:             SSO-console-session-timeout-value]
[max-logfile-size:        maximum-size-of-logging-file]
[logfile-num:             number-of-the-log-files]
[trace:                   on|off]
[max-tracefile-size:      maximum-size-of-trace-file]
[tracefile-num:           number-of-the-trace-files]
```

When coding definitions in the `ssoconsoled` action definition file, note the following:

- If the definition file includes the same definitions, the definition written last is assumed to be valid, and those definitions preceding the last definition are ignored.
- When omitting the specification of a key on a line, omit the whole line.

(2) Description

The next table lists the items that must be, or can be, defined in the `ssoconsoled` action definition file.

Key name	Value
`authentication:` `<<sso>>`	Specify the user authentication method to be used for the login to the SSO console. You can also specify omission of the user authentication. `sso`: SSO authentication method `jp1`: JP1 authentication method `none`: Omission of user authentication
`logical-hostname:`# `<<none>>`	When JP1/Base is installed on the same logical host where SSO is installed, specify the logical host name set in JP1/Base for user authentication (JP1 authentication method) in a cluster environment. By using this setting, the JP1/Base on the logical host is used for the user authentication. When `none` is specified, the JP1/Base on the physical host is used for the user authentication. For how to set a logical name on JP1/Base, see the *Job Management Partner 1/Base User's Guide*.
`logout-time:`# `<<1080>>` ((0, 30 to 1440 minutes))	Specify a session timeout for the SSO console. This setting is valid for SSO or JP1 authentication. When 0 is specified, session timeout is not implemented.
`max-logfile-size:` `<<4>>` ((1 to 32 megabytes))	Specify the maximum size of a log file.
`logfile-num:` `<<3>>` ((1 to 10))	Specify the number of the log files.
`trace:` `<<off>>`	Specify whether to output a trace file for troubleshooting at failure occurrence. To output the trace file, specify `on`. To not output the trace file, specify `off`.
`max-tracefile-size:` `<<4>>` ((1 to 32 megabytes))	Specify the maximum size of a trace file.
`tracefile-num:` `<<3>>` ((1 to 10))	Specify the number of the trace files.

If you change the value of this item, you must restart the ssoconsoled `daemon` process.

6.3.24 SSO startup definition file (ssostartup.conf)

In the SSO startup definition file, define the settings concerning the startup of the daemon processes of SSO.

(1) Format

The following shows the format of the SSO startup definition file.

daemon-process-name`:`*prerequisite-daemon-process*`:`*option*`:`*start-or-stop-monitoring-timeout-value*`:`

When coding definitions in the SSO startup definition file, note the following:

- Delimit each field with a colon (`:`).
- For the value in a field, you cannot use a space character, colon (`:`), comma (`,`), backslash or escape character (`\`), and hash mark (`#`).
- If you omit a field, always write a colon (`:`).
- If you have made any changes in the SSO startup definition file, you must restart SSO.

(2) Description

The next table lists the items that must be, or can be, defined in the SSO startup definition file.

Field name	Value
daemon-process-name	You must always specify one of the following daemon process names: • `ssocolmng` (resource collection management daemon process) • `ssocollectd` (resource collection daemon process) • `ssoapmon` (process and service monitoring daemon process) • `ssorptd` (report creation daemon process) • `ssoconsoled` (SSO console daemon process) • `ssotrapd` (SNMP trap reception daemon process) By default, the `ssotrapd` daemon process is disabled. Enable the daemon if SSO is used in a distributed configuration and SNMP traps can be received from APM. When the `ssotrapd` daemon process is enabled, you must always specify `ssotrapd` in the definition of the process dependent on the `ssoapmon` process.
prerequisite-daemon-process	Specify the name of the daemon process prerequisite for SSO operation. If you specify multiple daemon process names, delimit each daemon name with a comma (`,`). You must always specify `ssocollectd` for the definition of the `ssocolmng` daemon process.
option	Specify startup options for each daemon process. For the startup options, see the explanations of the commands corresponding to the daemon processes in *5. Commands*.
start-or-stop-monitoring-timeout-value <<300>> ((10 to 600))	Specify the starting or stopping timeout period in seconds for each daemon process. If a starting timeout occurs while a daemon process is being started, the startup of the daemon process is skipped. If a stopping timeout occurs while a daemon process is being stopped, the daemon process is terminated forcibly by a termination signal.

(3) SSO startup definition file at installation

The following shows the SSO startup definition file at the time of installation.

```
#
# ssostartup.conf
#
# FORMAT
#  process-name:dependence-process-name:option:time-out:

# resource collection management process
ssocolmng:ssocollectd:-f:300:

# resource collection process
ssocollectd::-f:300:

# process/service monitoring process
ssoapmon:::300:

# report creating process
ssorptd:::300:

# SSO console process
ssoconsoled:::300:

# APM trap reception process
#ssotrapd:::300:
```

(4) Examples

The following is an example of defining the SSO startup definition file.

When setting the timeout period of process and service monitoring daemon process (`ssoapmon`) to 600 seconds:

```
#
# ssostartup.conf
#
# FORMAT
#  process-name:dependence-process-name:option:time-out:

# resource collection management process
ssocolmng:ssocollectd:-f:300:

# resource collection process
ssocollectd::-f:300:

# process/service monitoring process
ssoapmon:::600:

# report creating process
ssorptd:::300:

# SSO console process
ssoconsoled:::300:

# APM trap reception process
#ssotrapd:::300:
```

When SSO is used in a distributed configuration and SNMP traps can be received from APM:

```
#
# ssostartup.conf
#
# FORMAT
#  process-name:dependence-process-name:option:time-out:

# resource collection management process
ssocolmng:ssocollectd:-f: 300:

# resource collection process
ssocollectd::-f: 300:

# process/service monitoring process
ssoapmon:ssotrapd::300:

# report creating process
ssorptd::: 300:

# SSO console process
ssoconsoled:::300:

# APM trap reception process
ssotrapd:::300:
```

(5) Note

If the error message below is output while the `ssostop` command is being executed, this indicates that stopping of the daemon process indicated in the message has not ended within the timeout period. In such a case, increase the timeout period specified for the indicated daemon process in the SSO startup definition file.

`ssospmd: (`*daemon process name*`) is timeout.`

For example, if the ssoapmon daemon process has not been stopped within the timeout period, the following error message is output:

```
ssospmd: (ssoapmon) is timeout.
```

6.3.25 ssospmd action definition file (ssospmd.def)

In the ssospmd action definition file, define the actions of the ssospmd daemon process. If you have made any changes in this definition file, perform one of the following operations to apply these changes:

- Execute the ssospmd -r command.

  Note that the changes might not become valid depending on the key that has been changed.
- Restart the ssospmd daemon process.

(1) Format

The following shows the format of the ssospmd action definition file.

```
[max-logfile-size:       maximum-size-of-logging-file]
[logfile-num:            number-of-the-log-files]
[trace:                  on|off]
[max-tracefile-size:     maximum-size-of-trace-file]
[tracefile-num:          number-of-the-trace-files]
[nnm-coop-check-interval:NNM-linkage-check-interval]
[nnm-coop-policy:        NNM-linkage-policy]
```

When coding definitions in the ssospmd action definition file, note the following:

- If the definition file includes the same definitions, the definition written last is assumed to be valid, and those definitions preceding the last definition are ignored.
- When omitting the specification of a key on a line, omit the whole line.

(2) Description

The next table lists the items that must be, or can be, defined in the ssospmd action definition file.

Key name	Value
max-logfile-size: <<4>> ((1 to 32 megabytes))	Specify the maximum size of a log file.
logfile-num: <<3>> ((1 to 10))	Specify the number of the log files.
trace: <<off>>	Specify whether to output a trace file for troubleshooting at failure occurrence. To output the trace file, specify on. To not output the trace file, specify off.
max-tracefile-size: <<4>> ((1 to 32 megabytes))	Specify the maximum size of a log file.
tracefile-num: <<3>> ((1 to 10))	Specify the number of the trace files.
nnm-coop-check-interval: <<10>> ((1 to 60 seconds))	Specify the interval for checking whether NNMi can be linked.

Key name	Value
`nnm-coop-policy`:# <<0>> ((0 or 1))	Specify `0` or `1` to specify how the daemon process managed by ssospmd acts when NNMi cannot be linked. 0: The daemon process enters the suspending status. 1: The daemon process enters the degenerating status. For the statuses of SSO daemon processes and status changes, see *D. Daemon Process Status Transitions*.

If you change the value of this item, you must restart the `ssospmd` daemon process.

6.3.26 User authentication definition file (ssoauth.conf)

In the user authentication definition file, define the user information to be used on the SSO console. The definitions in the user authentication definition file are valid when SSO authentication is used (when `sso` is specified in the authentication key in the `ssoconsoled` action definition file) on the SSO console.

Use the `ssoauth` command to define the user information. You cannot directly edit this definition file because the password is encrypted before it is stored.

(1) Format

The following shows the format of the user authentication definition file.

```
user-name△password
```

Legend △ : space

(2) Description

The following table describes the contents of definitions in the user authentication definition file.

Item	Description
user-name	Contains the value specified in the `-user` option of the `ssoauth` command
password	Contains the encrypted text that is computed based on the values specified in the `-user` and `-password` options of the `ssoauth` command. The text is encrypted in the `ssoauth` command process.

(3) Example

The following is an example of defining the user authentication definition file.

```
ssouser1 8704bed8d4405713
ssouser2 8704bed8d4405713
```

6.3.27 Event filter definition file (ssoevtfilter.conf)

In the event filter definition file, define whether to filter the incidents to be issued to NNMi. This definition file is used to prevent the issuance of unnecessary incidents.

When `off` is specified in the `threshold-event` or `status-event` key in the `ssocolmng` action definition file (`ssocolmng.def`) and `ssoapmon` action definition file (`ssoapmon.def`), incidents are not issued even if `off` is specified in the event filter definition file.

(1) Format

The following shows the format of the event filter definition file.

```
[incident-name : [on|off]]
```

(2) Description

The following table describes the content of the definition in the event filter definition file.

Key name	Value
incident-name# <<off>>	Specify whether to filter the specified incident. on: Filters the incident. off: Does not filter the incident.

#: As *incident-name*, specify the incident name of an event SSO issues to NNMi. For incident names, see *F.1 Events (incidents) that are issued by SSO*.

(3) Example

The following is an example of defining the event filter definition file.

```
#
# ssoevtfilter.conf
#
# FORMAT
# keyname:[on|off]
#

# Collection status change event(SSO_Resource_Collect)
SSO_Resource_Collect_Normal:        off
SSO_Resource_Collect_Waiting:       on
SSO_Resource_Collect_Pending:       on
SSO_Resource_Collect_Complete:      off
SSO_Resource_Collect_Failure:       on

# Resource collection status change events(SSO_Resource_Monitor)
SSO_Resource_Monitor_Cancel:        off
SSO_Resource_Monitor_Unknown:       on
SSO_Resource_Monitor_Normal:        off
SSO_Resource_Monitor_Warning:       on
SSO_Resource_Monitor_Critical:      on

# Monitoring status change event(SSO_Process_Monitor)
SSO_Process_Monitor_Normal:         off
SSO_Process_Monitor_Complete:       on
SSO_Process_Monitor_Failure:        on
```

(4) Writing a definition in a field

The following describes how to write a definition in a field:

- In each field, write an incident name delimited with a colon (**:**) and a value on one line.

- Write the incident name at the top of the line.
- You can write a tab or 1 or more spaces after the colon (`:`).

(5) Application of definitions

If you have changed the definition of an incident in the event filter definition file, you must execute the daemon process that notifies NNMi of the incident to re-read the definition file. The following table describes incidents, the daemon processes that require re-reading of the definition file, and the re-reading methods.

Table 6-6: Daemon processes that require re-reading of the definition file in which definitions are changed

Event name	Incident name#	Daemon process requiring re-reading	Re-reading method
• Collection status change event • Resource status change event	Incident name beginning with `SSO_Resource`	`ssocolmng`	• `ssocolmng -r` command • Restart the `ssocolmng` daemon process.
• Monitoring status change event • Process status change event • Process and service monitoring failure event	Incident name beginning with `SSO_Process`	`ssoapmon`	• `ssoapcom -r` command • Restart the `ssoapmon` daemon process.
Service status change event	Incident name beginning with `SSO_Service`		
Application status change event	Incident name beginning with `SSO_Application`		

#: For the official names of incident, see *F.1 Events (incidents) that are issued by SSO*.

(6) Incident not subject to event filtering

The table below describes the incident that is not subject to the filtering based on the event filter definition file. Even if the incident is defined in the event filter definition file, the definition is invalid, and the incident will be issued.

Table 6-7: Incident not subject to event filtering

Category	Incident name	Description
Resource collection	`SSO_Resource_DB_Size_Warning`	A threshold for a collection database was exceeded.

(7) Notes

Note the following when writing definitions in the event filter definition file:

- If the definition file includes multiple definitions specifying the same incident name, the definition written last is assumed to be valid, and the other definitions are ignored.
- The incidents that are not defined in the definition file are treated according to the default settings.
- If an error is detected in a definition, only the line that contains the error is skipped, and reading continues from the next line.
- The settings specified in this definition file are also applied to SNMP trap events issued by SSO.

6.3.28 Action log definition file (ssoauditlog.conf)

In the action log definition file, define the output of SSO action log files. The action log definition file is read when a daemon process is started or a command is executed. Therefore, if you have changed a definition in the action log definition file, you must restart the daemon process.

(1) Format

The following shows the format of the action log definition file.

```
auditlog-mode:          on|off
auditlog-num:           number-of-action-log
auditlog-size:          maximum-size-of-action-log
auditlog-level:         event-log-or-syslog-output-level
```

When coding definitions in the action log definition file, note the following:

- Specify a key name and a definition value by separating them by a colon (**:**).
- The space or tab at the top of the line, after the colon (**:**), or after the definition value is ignored.
- If the definition file includes the same definitions, the definition written last is assumed to be valid, and those definitions preceding the last definition are ignored.

(2) Description

The next table lists the items that must be, or can be, defined in the action log definition file.

Key name	Value
`auditlog-mode` <<on>> ((on|off))	Set whether to output the action log file. `on`: Outputs the action log file. `off`: Does not output the action log file.
`auditlog-num` <<3>> ((2 to 10))	Specify the number of the action log files. For example, when `3` is specified, up to 2 generations of backups are stored for the action log file.
`auditlog-size` <<4>> ((1 to 32 megabytes))	Specify the maximum size of an action log file.
`auditlog-level` <<0>>	Specify whether to output an action log to the event log (in Windows) or syslog (in UNIX) and the level of output. If you specify `I`, `W`, or `E`, you must specify `on` in the `auditlog-mode` key. `0`: Does not output the action log to the event log or syslog. `I`: Outputs the information of all message ID types. `W`: Outputs the information of such message ID types as W and E. `E`: Outputs the information of message ID type E.

(3) Example

The following is an example of defining the action log definition file.

```
#
# ssoauditlog.conf
#
# FORMAT
#  keyname:value

auditlog-mode:on
auditlog-num:3
auditlog-size:4
auditlog-level:E
```

6.3.29 NNM information definition file (ssonnminfo.conf)

In the NNM information definition file, define the information required to connect to NNMi. Use the `ssonnmsetup` command to edit (add, change, or delete) definitions in the NNM information definition file. Do not directly edit the definition file by using a text editor or by any other method. This definition file is read when SSO starts.

(1) Format

The following shows the format of the NNM information definition file.

```
#
# ssonnminfo.conf
#
default {
     key-name:value
     key-name:value
     key-name:value
}
Node key name {
     key-name:value
     key-name:value
     key-name:value
}
```

When coding definitions in the NNM information definition file, note the following:

- Specify key name and value pairs, and enclose the pairs for each node key name in curly brackets (`{ }`).
- Delimit the key name and the value with a colon (`:`)
- The space or tab at the top of the line, after a curly bracket (`{` or `}`), after the colon (`:`), or after the value is ignored.

(2) Description

(a) Node key name

As the node key name, `default` or an IP address is set. Under `default`, the information on the connection to NNMi is defined. Under an IP address, the information on the connection to another NNMi is defined according to definitions in the event destination definition file.

(b) Key name

The following table describes the contents of key definitions.

Key name	Value
User	User name that is used to connect to NNMi. This key contains the information specified in the -user option of the ssonnmsetup command.
Password	User password that is used to connect to NNMi. This key contains the encrypted code of the information specified in the -password option of the ssonnmsetup command.
Port	Port number of the NNM Web server port of NNMi. This key contains the information specified in the -port option of the ssonnmsetup command.
Host	Host name or IP address of the host where the connection destination NNMi is located in a distributed configuration. This key contains the information specified in the -host option of the ssonnmsetup command. This key is valid only when the node key name is default. In the basic configuration, SSO connects to the NNMi running on the same host where SSO is running. If you define the Host key, you can connect and link SSO to the NNMi running on a different host.
SSL	Specify on when performing HTTPS communication with NNMi. Specify off when performing HTTP communication with NNMi.

6.3.30 NNM action definition file (ssonnmaction.conf)

In the NNM action definition file, define the settings concerning action cooperation. This definition file is read when the Incident Graph window is opened for the first time after the ssoconsoled daemon process starts. If you have changed a definition in this definition file, you must restart the ssoconsoled daemon process.

(1) Format

The following shows the format of the NNM action definition file.

```
nnm-incidentgraph-before = date;hour;minute
nnm-incidentgraph-after = date;hour;minute
nnm-incidentgraph-maxplot = maximum-number-of-plot
nnm-incidentgraph-imgsize = width-of-image;height-of-image
```

When coding definitions in the NNM action definition file, note the following:

- Delimit the key name and the value with an equal sign (=).
- If the definition file includes multiple definitions for the same item, the definition written last is assumed to be valid, and those definitions preceding the last definition are ignored.
- Lines beginning with a hash mark (#) or exclamation mark (!) are treated as comment lines.

(2) Description

The next table lists the items that must be, or can be, defined in the NNM action definition file.

Key name	Value
nnm-incidentgraph-before <<0;6;0>> ((0 to 30;0 to 23;0 to 59))	This setting is used by the function to display the incident graph. Specify a length of time preceding the occurrence of an incident as the time range of the data to be displayed in the incident graph. The specified value is displayed as the initial value in the **Before** field under **Range: Occurrence Time** in the Incident View Range Specification window.
nnm-incidentgraph-after	This setting is used by the function to display the incident graph.

Key name	Value
<<0;0;0>> ((0 to 30;0 to 23;0 to 59))	Specify a length of time following the occurrence of an incident as the time range of the data to be displayed in the incident graph. The specified value is displayed as the initial value in the **After** field under **Range: Occurrence Time** in the Incident View Range Specification window.
nnm-incidentgraph-maxplot <<10000>> ((1 to 20000))	This setting is used by the function to display the incident graph. Specify the maximum number of plots. The *number of plots* here means the number of pieces of collected data that is displayed in the incident graph. The specified value is displayed as the initial value in the **Max Plot** field in the Incident View Range Specification window.
nnm-incidentgraph-imgsize <<500;400>> ((320 to 1024;240 to 768))	This setting is used by the function to display the incident graph. Specify the size of the graph image that is displayed in the Incident Graph window. The specified values are displayed as the initial values in the **Width** and **Height** fields under **Image Size** in the Incident View Range Specification window.

(3) Example

The following is an example of defining the NNM action definition file.

```
nnm-incidentgraph-before = 0;6;0
nnm-incidentgraph-after = 0;0;0
nnm-incidentgraph-maxplot = 10000
nnm-incidentgraph-imgsize = 500;400
```

(4) Note

If you have changed a definition in the NNM action definition file, you must restart the `ssoconsoled` daemon process.

6.3.31 GUI log definition file (ssoguilog.conf)

In the GUI log definition file, define the settings for logging operations performed from the GUI. The GUI log definition file is read when a GUI component is activated. Therefore, if you change a definition in this definition file while you are using a GUI component, you must re-activate the GUI component.

(1) Format

The following shows the format of the GUI log definition file.

```
LOG_LEVEL = OFF|ERROR|WARN|INFO
FILE_SIZE = maximum-size-of-GUI-log
```

When coding definitions in the GUI log definition file, note the following:

- Delimit the key name and the value with an equal sign (=).
- If the definition file includes multiple definitions for the same item, the definition written last is assumed to be valid, and the other definitions are ignored.

(2) Description

The next table lists the items that must be, or can be, defined in the GUI log definition file.

Key name	Value
LOG_LEVEL <<ERROR>> ((OFF|ERROR|WARN|INFO))	Specify a log output level. Specifiable levels are as follows: OFF: Does not output log. ERROR: Outputs only error log. WARN: Outputs error log and warning log. INFO: Outputs warning log and information log.
FILE_SIZE <<4>> ((1 to 100 megabytes))	Specify the maximum size of the log file.

(3) Example

The following is an example of defining the GUI log definition file.

```
#
# ssoguilog.conf
#
# FORMAT
#  keyname=value
#
LOG_LEVEL = ERROR
FILE_SIZE = 4
```

(4) Note

If you want to change a definition in the GUI log definition file, deactivate all GUI components such as windows, change the definition in the GUI log definition file, delete the existing GUI log file (ssogui_*.log), and then re-activate the GUI components.

6.3.32 NNM action address definition file (ssonnmactaddr.conf)

In an environment in which the monitoring manager interfaces with multiple networks that are not routed to each other, set the NNM action address definition file according to the operational requirements when you perform the following operation: Using NNMi cooperation (action cooperation) from a terminal that cannot communicate with the monitoring manager by using the IP address set by the change-my-address: key in the ssocolmng action definition file or ssoapmon action definition file.

This definition file is loaded when the ssocolmng and ssoapmon daemon processes start. Therefore, if the settings of this file are changed, you must restart those daemon processes.

(1) Format

The following is a format of the NNM action address definition file.

```
action-node-IP-address:monitoring-manager-IP-address
```

(2) Description

The next table lists the items that must be, or can be defined in the NNM action address definition file.

Item	Explanation
action-node-IP-address	Specify IP addresses for the monitoring manager nodes or monitoring server nodes that use NNMi cooperation (action cooperation) functions. • For the monitoring manager nodes, specify the IP address set by the `change-my-address:` key in the `ssocolmng` action definition file and `ssoapmon` action definition file. • For the monitoring server nodes, specify the IP address that SSO uses for monitoring. The specification format differs depending on whether you specify an IPv4 or IPv6 address. To specify an IPv4 address, use the *n*`.`*n*`.`*n*`.`*n* format. For *n*, you can specify a decimal value in the range from 0 to 255, or an asterisk (`*`) as a wildcard character. To specify an IPv6 address, use the `[`*x*`:`*x*`:`*x*`:`*x*`:`*x*`:`*x*`:`*x*`:`*x*`]` format. For *x*, you can specify a hexadecimal value in the range from 0 to FFFF, or an asterisk (`*`) as a wildcard character.
monitoring-manager-IP-address	Specify the IP address of the monitoring manager with which SSO can communicate from a terminal that uses NNMi cooperation (action cooperation). Make sure that you specify the IP address in the *n*`.`*n*`.`*n*`.`*n* format.

(3) Notes

Note the following when writing definitions in the NNM action address definition file:

- If the file contains multiple *action-node-IP-address* entries that are the same, only the first specified entry takes effect, and the other entries are ignored.
- If the file contains multiple *action-node-IP-address* entries that use wildcard characters corresponding to either the monitoring manager or monitoring server, only the first specified entry takes effect. For example, if the first *action-node-IP-address* entry in the file is `*.*.*.*` or `[*:*:*:*:*:*:*:*]`, that entry takes effect on all action nodes.

Appendixes

A. Processes and Services

This appendix explains the processes and services provided by each SSO program.

A.1 Processes provided by SSO

The processes provided by SSO are listed below.

Table A-1: Processes (SSO)

Process		Function
UNIX	Windows	
ssoapmon	ssoapmon.exe	Daemon process that monitors processes and services.
ssocollectd	ssocollectd.exe	Daemon process that collects MIBs.
ssocolmng	ssocolmng.exe	Daemon process that manages resource collection.
ssoconsoled	ssoconsoled.exe	Daemon process that runs the SSO console.
ssorptd	ssorptd.exe	Daemon process that creates report files.
ssospmd	ssospmd.exe	Daemon process that manages all other daemon processes.
ssotrapd	ssotrapd.exe	Daemon process that receives SNMP traps issued by APM and notifies the ssoapmon daemon process of events.
cjstartweb	cjstartweb.exe	Background process that is started by a daemon process of the SSO console to provide Web pages.
httpsd	httpsd.exe	Background process that is started by a daemon process of the SSO console to provide Web server functionality.

A.2 Services provided by SSO (Windows only)

The services provided by SSO are listed below (Windows only).

Table A-2: Services (SSO)

Display name	Service name	Description
SNMP System Observer	Cm2SSO	This service manages starting, stopping, and status of all daemon processes of SSO. When this service starts, it starts the ssospmd daemon process, which then starts other daemon processes according to the definitions in the SSO startup definition file. When this service stops, the ssospmd daemon process stops after stopping other daemon processes. Executing the ssostart command starts this service. If this service has already started when execution of the ssostart command is requested, the request is received by the ssospmd daemon process without affecting the status of this service. When the ssostop command is executed, the ssospmd daemon process stops other daemon processes and then this service. Executing the ssostatus command (or selecting **Status** in the SSO console window) displays the status of the SSO daemon processes managed by the ssospmd daemon process.

Display name	Service name	Description
SNMP System Observer - Console	SNMPSystemObserver-Console	This service provides Web server functionality and Web pages for the SSO console. This service is controlled by the `ssoconsoled` daemon process. When the `ssoconsoled` daemon process starts, it starts this service. When the `ssoconsoled` daemon process stops, it stops this service.

B. Directions of Traffic Through a Firewall

The table below describes the port numbers of the ports that are used by SSO programs and NNMi and the directions of traffic through the firewall.

Note that, as the port number of the communication source, a port number not being used by the source host is assigned.

Table B-1: Port numbers to be used and the directions of traffic through the firewall

Function	Port number[#1]	Protocol	Direction of the firewall traffic
Resource collection	20086	TCP	SSO <- window[#2] SSO <- command[#2]
	161[#3]	UDP	SSO -> SNMP agent
Process and service monitoring	20147	TCP	SSO <- window[#2] SSO <- command[#2]
	161[#3]	UDP	SSO -> SNMP agent
	162	UDP	NNMi <- APM[#4] or SSO <- APM[#5]
Report creation and browsing	22297 20393	TCP	SSO <- Report Configuration window[#2] SSO <- Report Browser window[#6]
SSO console	20393	TCP	SSO <- Web browser[#6]
TCP notification of APM event	20264	TCP	SSO <- APM
TCP health check	20307	TCP	SSO -> APM
Event transmission	80[#7]	TCP	SSO -> NNMi
	162	UDP	SSO -> SNMP manager[#8]

Legend:

->: The program on the left starts communication (connection) with the program on the right.

<-: The program on the right starts communication (connection) with the program on the left.

#1

Default value.

#2

This direction of traffic through the firewall applies to the case in which a connection is established from the local host to SSO on a remote host through window operations or by executing a command. This direction of traffic also applies to the case in which a connection is established from the SSO console to SSO.

#3

If the SNMP agent is the ESA for Red Hat Enterprise Linux, the default port number is 22161.

#4

This direction of traffic through the firewall applies to the case in which an APM event is reported as an SNMP trap in a basic system configuration.

#5

This direction of traffic through the firewall applies to the case in which an APM event is reported as an SNMP trap in a distributed system configuration.

#6

This direction of traffic through the firewall applies to the case in which a Web browser is used to access SSO.

#7

This port number is that of the NNM Web server port of NNMi defined in the NNM information definition file.

#8

This direction of traffic through the firewall applies to the case in which an event is reported to the SNMP manager (for example, NNM) on a remote host according to definitions in the event destination definition file.

C. Kernel Parameters

When using SSO programs in a UNIX environment, you must tune OS kernel parameters as needed to allocate system resources required to run an SNMP agent. This appendix describes the system resources required to run an SNMP agent for each OS.

C.1 Kernel parameters of SSO

(1) In HP-UX

The following table lists the kernel parameters that must be tuned when the OS is HP-UX.

Table C-1: Kernel parameters of SSO that must be tuned (in HP-UX)

System resource	Parameter	Estimate
File system	`maxfiles`	In this parameter, set the largest value among the following: • Resource collection (`ssocolmng` and `ssocollectd`) *Value-of-max-client-in-the-ssocolmng-action-definition-file* + *value-of-max-snmp-session-in-the-ssocollectd-action-definition-file* + *number-of-concurrent-executions-of-command* **x** 3 + 20 • Process monitoring (`ssoapmon`) *Value-of-max-client-in-the-ssoapmon-action-definition-file* + *value-of-max-snmp-session-in-the-ssoapmon-action-definition-file* + *value-of-max-apm-session-in-the-ssoapmon-action-definition-file* + *number-of-concurrent-executions-of-command* **x** 3 + 10 • Daemon process management (`ssospmd`) *Number-of-concurrent-executions-of-command* **x** 4 + 16 • SSO console (`ssoconsoled`) 235 • Report function (`ssorptd`) *Value-of-max-client-in-the-ssorptd-action-definition-file* + *value-of-max-data-in-the-ssorptd-action-definition-file* + 7 • SNMP trap reception (`ssotrapd`) *Number-of-concurrent-executions-of-command* **x** 2 + 10
Processes	`nproc`	*Number-of-concurrent-executions-of-command-or-GUI-function* + *number-of-concurrent-executions-of-automated-action* + *number-of-conditions-for-the-report-to-be-created* + 16

(2) In Solaris

The following table lists the kernel parameters that must be tuned when the OS is Solaris.

Table C-2: Kernel parameters of SSO that must be tuned (in Solaris)

System resource	Parameter	Estimate
File system	`rlim_fd_cur`	In this parameter, set the largest value among the following: • Resource collection (`ssocolmng` and `ssocollectd`) *Value-of-max-client-in-the-ssocolmng-action-definition-file* + *value-of-max-snmp-session-in-the-ssocollectd-action-definition-file* + *number-of-concurrent-executions-of-command* **x** 3 + 20

System resource	Parameter	Estimate
File system	rlim_fd_cur	• Process monitoring (ssoapmon) *Value-of-max-client-in-the-ssoapmon-action-definition-file* + *value-of-max-snmp-session-in-the-ssoapmon-action-definition-file* + *value-of-max-apm-session-in-the-ssoapmon-action-definition-file* + *number-of-concurrent-executions-of-command* **x** 3 + 10 • Daemon process management (ssospmd) *Number-of-concurrent-executions-of-command* **x** 4 + 16 • SSO console (ssoconsoled) 235 • Report function (ssorptd) *Value-of-max-client-in-the-ssorptd-action-definition-file* + *value-of-max-data-in-the-ssorptd-action-definition-file* + 7 • SNMP trap reception (ssotrapd) *Number-of-concurrent-executions-of-command* **x** 2 + 100
Processes	max_nprocs	*Number-of-concurrent-executions-of-command-or-GUI-function* + *number-of-concurrent-executions-of-automated-action* + *number-of-conditions-for-the-report-to-be-created* + 16

(3) In Linux

The following table lists the kernel parameters that must be tuned when the OS is Linux.

Table C-3: Kernel parameters of SSO that must be tuned (in Linux)

System resource	Parameter	Estimate
File system	file-max (/proc/sys/fs/file-max)	In this parameter, set the sum total of the following values for the functions to be used: • Resource collection (ssocolmng and ssocollectd) *Value-of-max-client-in-the-ssocolmng-action-definition-file* + *value-of-max-snmp-session-in-the-ssocollectd-action-definition-file* + *number-of-concurrent-executions-of-command* **x** 3 + 20 • Process monitoring (ssoapmon) *Value-of-max-client-in-the-ssoapmon-action-definition-file* + *value-of-max-snmp-session-in-the-ssoapmon-action-definition-file* + *value-of-max-apm-session-in-the-ssoapmon-action-definition-file* + *number-of-concurrent-executions-of-command* **x** 3 + 10 • Daemon process management (ssospmd) *Number-of-concurrent-executions-of-command* **x** 4 + 16 • SSO console (ssoconsoled) 235 • Report function (ssorptd) *Value-of-max-client-in-the-ssorptd-action-definition-file* + *value-of-max-data-in-the-ssorptd-action-definition-file* + 7 • SNMP trap reception (ssotrapd) *Number-of-concurrent-executions-of-command* **x** 2 + 100 + 10

D. Daemon Process Status Transitions

A daemon process changes its status according to changes in SSO operation (starting, stopping, and backup) and the linkage of SSO with NNMi. You can check the statuses of SSO daemon processes by selecting **Status** in the menu frame of the SSP console window. This appendix describes the statuses of SSO daemon processes and their changes (status transitions).

D.1 Daemon process status

The following table lists the available statuses of a daemon process and their meanings.

Table D－1: Statuses of a daemon process

Status	Description
RUNNING	The daemon process is running normally.
NOT_RUNNING	The daemon process is stopped.
PAUSING	The daemon process is interrupted.
SUSPENDING	The daemon process is stopped temporarily.
DEGENERATING#1	The daemon process is running in reduced mode#2.
RUNNING*	The daemon process is starting, restarting, or being restarted.
NOT_RUNNING*	The daemon process is being stopped.
PAUSING*	The daemon process is being interrupted.
SUSPENDING*	The daemon process is being stopped temporarily.
DEGENERATING*#1	The daemon process is being degenerated#2.

#1: Only the `ssocolmng` daemon and `ssoapmon` daemon processes can enter this status.

#2: In reduced mode, NNMi cooperation is not available. In that case, in a basic system configuration, process and service monitoring cannot be performed normally from a monitoring server that is set to report events as SNMP traps. To perform monitoring normally in the basic system configuration, you must change the server setting to send events via TCP. In a distributed configuration, however, monitoring can be performed with either SNMP trap notification or TCP communication.

E. Resource IDs

This appendix describes the resources that can be collected with category name SSO or SSO-Ex. It includes the following information on resources:

Resource and subresource names:

These names identify the resource and subresource that can be collected. The resources that can be collected depends on the agent type.

Resource and subresource IDs

Resources and subresources are assigned IDs. You can use these IDs when using commands to specify collection conditions or to extract collected data.

Resource directories

Resource directories are used to store collected data. A resource directory is created for each resource under the following directory:

UNIX

```
$SSO_DB/Coll
```

Windows

```
$SSO_DB\Coll
```

E.1 Resources (Computer group)

The following table lists those resources in the Computer group which can be collected by SSO.

Table E-1: Resources (Computer group)

Resource: Resource ID	Subresource: Subresource ID	Unit	Resource directory	Description
Computer Summary: 40#	Host Name: 1	--	--	System host name
	System Up-Time: 2	--	--	Time elapsed since the system started
	System Location: 3	--	--	System location
	System Contact: 4	--	--	System administrator contact info
Operating System Summary: 41#	OS Name: 1	--	--	Operating system name (Windows 2000 is displayed when the OS of the agent is Windows 2000 or later.)
	OS Version: 2	--	--	Operating system version
	System Description: 3	--	--	System explanation
Process Summary: 42#	PID: 1	--	--	Process ID
	PPID: 2	--	--	Parent process ID
	UID: 3	--	--	Process user ID
	Priority: 4	--	--	Process priority
	User Name: 5	--	--	Name of the user who started the system

Resource: Resource ID	Subresource: Subresource ID	Unit	Resource directory	Description
Process Summary: 42#	User CPU: 6	--	--	Process time spent in user mode
	System CPU: 7	--	--	Process time spent in system (kernel) mode
	Start Command: 8	--	--	Command line character string that started the process
	Status: 9	--	--	Process status: sleep (1), run (2), stop (3), zombie (4), other (5), or idle (6)
	Data Size: 10	Pages	--	Data area size
	Text Size: 11	Pages	--	Text area size
	Stack Size: 12	Pages	--	Stack area size
	Nice: 13	--	--	Nice value
	TTY Major: 14	--	--	Control terminal major number
	TTY Minor: 15	--	--	Control terminal minor number
	Group ID: 16	--	--	Process group ID
	Process Address: 17	--	--	User area address (physical memory address if the process is loaded into memory or disk address if the process is swapped out)
	CPU Utilization: 18	%	--	Processor utilization for scheduling
	Up-Time: 19	--	--	Time elapsed since the process has started
	Process Flag: 20	--	--	Process flag: incore (1), sys (2), locked (4), trace (8), or trace2 (16)
	Sleep Address: 21	--	--	Address where the processor sleeps
	Last Processor: 22	--	--	Processor that last executed the process
	In-Core Time: 23	Seconds	--	In-core time used by the process
	Time Slice CPU: 24	--	--	Number of CPU ticks used by the process during the current time slice
	Total CPU: 25	--	--	Number of CPU ticks used by the process since the process was generated
	FSS Group ID: 26	--	--	Uniform allocation scheduler ID to which the process belongs
	In-Core CPU Utilization: 27	%	--	Percentage of the CPU time to the in-core time elapsed
	In-Core Pages: 28	Pages	--	Number of in-core loaded pages
	SUID: 29	--	--	Actual process user ID
CPU Load Average: 1	CPU Load Average 1 Min: 1	--	COM_CPULd	Average 1-minute load for the entire computer
	CPU Load Average 5 Min: 2			Average 5-minute load for the entire computer
	CPU Load Average 15 Min: 3			Average 15-minute load for the entire computer
CPU Utilization: 2	Total CPU: 1	%	COM_CPUUsg	Total CPU utilization for the entire computer

Resource: Resource ID	Subresource: Subresource ID	Unit	Resource directory	Description
CPU Utilization: 2	User CPU: 2	%	COM_CPUUsg	CPU utilization for users on the entire computer
	System CPU: 3			CPU utilization for the system on the entire computer
	Wait CPU: 4			CPU's wait on the entire computer
System Table Entries: 3	Process: 1	Entries	COM_SysTbl	Number of process table entries currently in use
	i Node: 2			Number of i-node table entries currently in use
	File: 3			Number of file table entries currently in use
File System I/Os: 4	read: 1	Bytes/Second	COM_FileIO	Number of bytes that were transferred during an all-read operation
	write: 2			Number of bytes that were transferred during an all-write operation
Run Queue Length: 38	Run Queue Length: 1	Queues	COM_Que	Processor queue/Instantaneous length, represented by the number of threads
System Calls: 7	System Calls: 1	Times/Second	COM_SysCall	Number of system calls issued
Interruptions: 10	Interruptions: 1	Times/Second	COM_Ipt	Number of device (hardware) interruptions
Context Switches: 11	Context Switches: 1	Times/Second	COM_Ctx	Number of context switches
Active Processes: 22	Wait for Execution: 1	Processes	COM_PrcA	Number of non-system processes that have been loaded into system storage and are waiting for execution
	Wait for Transfer: 2			Number of processes that are waiting for data transfer from disks
	Wait for Page In: 3			Number of processes that are waiting for page-in from disks
	Sleep: 4			Number of sleeping processes in physical memory (This quantity does not include processes that are sleeping while waiting for I/O or processes that have slept continuously for at least 20 seconds)
	Swap Out: 5			Number of swapped-out processes (processes that will begin waiting for execution as soon as they are swapped in)
Process Size: 23	Total Physical Memory: 1	Bytes	COM_PrcS	Size of the physical memory that has been allocated for text, data, and stacks used by all processes within the system
	Wait Physical Memory: 2			Size of the physical memory allocated for all processes waiting for execution
	Total Virtual Memory: 3			Size of the virtual memory that has been allocated for text, data, and stacks used by all non-system processes within the system
	Wait Virtual Memory: 4			Size of the virtual memory allocated for all processes waiting for execution
Login Users: 70	Login Users: 1	--	COM_Users	Number of users logged into the system

This table lists summary information that can only be viewed in the Resource Browser window.

E.2 Resources (CPU group)

The following table lists those resources in the CPU group which can be collected by SSO.

Table E-2: Resources (CPU group)

Resource: Resource ID	Subresource: Subresource ID	Unit	Resource directory	Description
CPU Summary: 43#	CPU Quantity: 1	--	--	Number of CPUs included in the system
CPU Load Average: 31	CPU Load Average 1 Min: 1	--	CPU_CPULd	Average 1-minute processor load
	CPU Load Average 5 Min: 2	--		Average 5-minute processor load
	CPU Load Average 15 Min: 3	--		Average 15-minute processor load
CPU Utilization: 32	Total CPU: 1	%	CPU_CPUUsg	Total CPU utilization on each processor
	User CPU: 2			CPU utilization for users on each processor
	System CPU: 3			CPU utilization for the system on each processor
	Wait CPU: 4			CPU's wait on each processor
File System I/Os: 33	read: 1	Bytes/Second	CPU_FileIO	Number of bytes that have been read from the processor-specific file system
	write: 2			Number of bytes that have been written from the processor-specific file system
NFS I/Os: 5	read: 1	Bytes/Second	CPU_NFSIO	Number of bytes that have been read from the NFS
	read: 1			Number of bytes that have been written from the NFS
Run Queue Length: 6	Run Queue Length: 1	Queues/Second	CPU_Que	Number of processes on the processor
System Calls: 8	exec: 1	Times/Second	CPU_SysCall	Number of exec system calls issued on the processor
	read: 2			Number of read system calls issued on the processor
	write: 3			Number of write system calls issued on the processor
I/O Characters: 9	read: 1	Characters/ Second	CPU_IOChar	Number of characters that have been encountered during raw device read operations performed by the processor
	canon: 2			Number of characters that have been encountered during canon operations performed by the processor
	output: 3			Number of characters that have been output by the processor

This table lists summary information that can only be viewed in the Resource Browser window.

E.3 Resources (Memory group)

The following table lists those resources in the Memory group which can be collected by SSO.

Table E-3: Resources (Memory group)

Resource: Resource ID	Subresource: Subresource ID	Unit	Resource directory	Description
Memory Summary: 44[#1]	Physical Memory: 1	KBytes	--	Physical memory size
	Free Memory: 2		--	Free physical memory size
	Memory Utilization: 3	%	--	Physical memory utilization
	Configured Swap: 4	KBytes	--	Total swap area size[#2]
	Enabled Swap: 5		--	Enabled swap area size[#2]
	Free Swap: 6		--	Free swap area size[#3]
	Swap Utilization: 7	%	--	Swap area utilization[#4]
Swap Summary: 45[#1]	Swap Type: 1	--	--	Location of swap area allocation swblock(1): On block-based device swfs(2): On file system
	Swap Using Flag: 2	--	--	Whether the swap area is enabled or disabled enable(1): Enabled disable(2): Disabled
	Swap Priority: 3	--	--	Swap area priority
	Swap Space: 4	KBytes	--	Swap area size
	Free Swap: 5	KBytes	--	Size of the enabled swap area
	Mount Point: 6	--	--	Location where the file system is mounted
Memory Utilization: 15	Memory Utilization: 1	%	MEM_MemUsg	Physical memory utilization
Free Memory Size: 16	Free Memory Size: 1	KBytes	MEM_FreeMem	Free physical memory size
Swap Utilization: 16	Swap Utilization: 1	%	MEM_SwpS	Swap area utilization[#4]
Free Swap Size: 36	Free Swap Size: 1	KBytes	MEM_FreeSwp	Free swap area size[#3]
Paging Pages: 17	Free: 1	Pages/Second	MEM_PgU	Number of pages that have been freed by the page-out daemon
	Load: 2			Number of pages that have been demand-loaded by executable files
	Page In: 3			Number of pages that have been paged in
	Page Out: 4			Number of pages that have been paged out
	Swap In: 5			Number of pages that have been swapped in
	Swap Out: 6			Number of pages that have been swapped out
	Scan: 7			Number of pages that have been scanned by the page-out daemon
	Reclaimed: 8			Number of reclaimed pages
Paging Times: 18	Page In: 1	Times/Second	MEM_Pg	Number of page-ins

Resource: Resource ID	Subresource: Subresource ID	Unit	Resource directory	Description
Paging Times: 18	Page Out: 2	Times/Second	MEM_Pg	Number of page-outs
Swapping Times: 19	Swap In: 1	Times/Second	MEM_Swp	Number of swap-ins
	Swap Out: 2			Number of swap-outs
Page Faults: 20	Page Faults: 1	Times/Second	MEM_PgF	Number of page faults
TLB Flashes: 21	TLB Flashes: 1	Times/Second	MEM_TLB	Number of TLB flashes (1-second average, updated at 5-second intervals)

#1 Indicates summary information that can only be viewed at the Resource Browser window.

#2 Indicates the total commit charge (limit value) if the collection target is running in Windows.

#3 Indicates the size of the empty space for the commit charge if the collection target is running in Windows.

#4 Indicates ((*total-commit-charge* - *empty-space-size-for-commit-charge*) / *total-commit-charge* **x** 100) if the collection target is running in Windows.

E.4 Resources (Disk group)

The following table lists those resources in the Disk group which can be collected by SSO.

Table E-4: Resources (Disk group)

Resource: Resource ID	Subresource: Subresource ID	Unit	Resource directory	Description
Disk Busy Utilization: 67	Disk Busy Utilization: 1	%	DISK_DskS	Percentage of the time spent by the device for the service to fulfill a transfer request When the agent type is SB: Average of 5 seconds When the agent type is SD, SC, AC or AB: Average of 5 minutes When the agent type is LD or LC: Average of the collection interval
Disk Busy: 13	Disk Busy: 1	Timeticks/ Second	DISK_DskB	Disk busy utilization during collection interval (percentage of the time spent by the device for the service to fulfill a transfer request) The unit *Timeticks/Second* means a percentage.
Disk I/Os: 68	read: 1	KBytes/Second	DISK_DskIO	Number of kilobytes that have been read from disk
	write: 2			Number of kilobytes that have been written to disk
Data Transfers: 14	Data Transfers: 1	Times/Second	DISK_Trns	Number of data transfers, one 2-byte word at each transfer

E.5 Resources (File System group)

The following table lists those resources in the File System group which can be collected by SSO.

Table E-5: Resources (File System group)

Resource: Resource ID	Subresource: Subresource ID	Unit	Resource directory	Description
File System Summary: 46#	File System Name: 1	--	--	Name of the mounted file system
	Total Size: 2	KBytes	--	Total file system size
	Used Size: 3		--	Size of used area in the file system
	Free Size: 4		--	Size of free area in the file system
	Available Size: 5		--	Size of area that can be used by users other than superusers
	Utilization: 6	%	--	Area utilization in the file system
File System Utilization: 12	File System Utilization: 1	%	FILE_FileS	File system utilization
File System Available: 34	File System Available: 1	KBytes	FILE_FileAva	Size of free area that can be used by users other than superusers

This table lists summary information that can only be viewed in the Resource Browser window.

E.6 Resources (Network group)

The following table lists those resources in the Network group which can be collected by SSO.

Table E-6: Resources (Network group)

Resource: Resource ID	Subresource: Subresource ID	Unit	Resource directory	Description
Network Summary: 47#1	Interface Name: 1	--	--	Interface name
	Interface Type: 2	--	--	Interface type
	Maximum IP Datagram: 3	Bytes	--	Maximum value of IP datagrams that can be sent or received via the interface
	Interface Speed: 4	Bits/Second	--	Transfer rate
	IP Address: 5	--	--	Addressing information IP address
	Subnet Mask: 6	--	--	IP address related subnet mask
	Interface Address: 7	--	--	Interface address of the protocol layer that is immediately below the IP
	Interface Status: 8	--	--	Interface operation status
Interface Utilization: 30#2	Total: 1	%	NET_IfUsRt	Percentage of I/O volume to the line capacity
	Average: 2			I/O volume average as compared with the line capacity
Interface Uses: 37#2	InOctets: 1	Octets/Second	NET_IfUsAt	Number of octets received via the interface
	OutOctets: 2			Number of octets sent via the interface
Interface Traffic: 24#2	InUcastPkts: 1	Packets/ Second	NET_Tff	Number of subnet unicast packets that have been delivered to the high-order protocol

Resource: Resource ID	Subresource: Subresource ID	Unit	Resource directory	Description
Interface Traffic: 24[#2]	InNUcastPkts: 2	Packets/ Second	NET_Tff	Number of subnet broadcast or multicast packets that have been delivered to the high-order protocol
	InErrors: 3			Number of receive packets that have not been delivered to the high-order protocol because of one or more errors
	OutUcastPkts: 4			Number of packets that have been sent to subnet unicast addresses requested by the high-order protocol
	OutNUcastPkts: 5			Number of packets that have been sent to subnet broadcast or multicast destinations requested by the high-order protocol
	OutErrors: 6			Number of sent packets that were not sent because of one or more errors
IP Traffic: 26	InReceives: 1	Datagrams/ Second	NET_IPIO	Number of datagrams that have been received via the interface
	InUnknownProtos : 2			Number of datagrams that have been destroyed because of an unknown or undefined protocol
	InDelivers: 3			Number of input datagrams that have been successfully delivered to the IP user protocol
	OutRequests: 4			Number of IP datagrams that have been supplied from the IP user protocol
	OutNoRoutes: 5			Number of IP datagrams that have been destroyed because no transfer route to the destination was found
ICMP Traffic: 27	InMsgs: 1	Messages/ Second	NET_ICMPIO	Number of received ICMP messages
	InErrors: 2			Number of received ICMP error messages
	InEchos: 3			Number of received ICMP echo request messages
	InEchoReps: 4			Number of received ICMP echo response messages
	OutMsgs: 5			Number of sent ICMP messages
	OutErrors: 6			Number of sent ICMP error messages
	OutEchos: 7			Number of sent ICMP echo request messages
	OutEchoReps: 8			Number of sent ICMP echo response messages
TCP Traffic: 69	InSegs: 1	Segments/ Second	NET_TCPIO	Number of received segments
	OutSegs: 2			Number of sent segments
	RetransSegs: 3			Number of resent segments
	InErrs: 4			Number of received error segments
	OutRsts: 5			Number of connection reset segments
UDP Traffic: 28	InDatagrams: 1	Datagrams/ Second	NET_UDPIO	Number of UDP datagrams that have been delivered to UDP users
	InNoPorts: 2			Number of UDP datagrams for which no application is available at the destination port
	InErrors: 3			Number of UDP datagrams that have not been for a reason other than InNoPorts

Resource: Resource ID	Subresource: Subresource ID	Unit	Resource directory	Description
UDP Traffic: 28	OutDatagrams: 4	Datagrams/ Second	NET_UDPIO	Number of delivered UDP datagrams
SNMP Traffic: 29	InPkts: 1	Messages/ Second	NET_SNMPIO	Number of SNMP messages that have been received from the transport service
	OutPkts: 2			Number of SNMP messages that have been sent from the transport service
	OutTooBigs: 3			Number of sent messages whose error status is *tooBig*
	OutNoSuchNames : 4			Number of sent messages whose error status is *noSuchName*
	OutBadValues: 5			Number of sent messages whose error status is *BadValueno*
	OutGenErrors: 6			Number of sent messages whose error status is *GenErr*
Ping Response Time: 39	Ping Response Time: 1	mSeconds	NET_PING	Time from the transmission of an IPv4 ICMP echo request to the reception of a response, as well as error information The value will be one of the following if the ICMP echo request encounters an error. • 99997 (invalid echo reply) • 99998 (ICMP echo request time-out) • 99999 (internal error)

#1: This table lists summary information that can only be viewed in the Resource Browser window.

#2: When the OS of the collection target agent is Solaris 2.5.1, SSO cannot collect this resource regardless of the agent type.

E.7 Resources (SMS group)

The following table lists those resources in the SMS group which can be collected by SSO.

Table E-7: Resources (SMS group)

Resource: Resource ID	Subresource: Subresource ID	Unit	Description
Computer Summary: 48#	Host Name: 1	--	Host name
	Domain Name: 2	--	Name of the SMS domain that includes the managed PC
Operating System Summary: 49#	OS Name: 1	--	Operating system name
	OS Version: 2	--	Operating system version number
	Installation Date: 3	--	Day the operating system was installed
	Registered Owner: 4	--	Operating system owner
	Registered Organization: 5	--	Organization to which the operating system owner belongs
	Build Number: 6	--	Operating system build number
	Build Type: 7	--	Operating system build type
	Root Directory: 8	--	Directory in which the operating system resides

Resource: Resource ID	Subresource: Subresource ID	Unit	Description
Operating System Summary: 49#	Start Operation: 9	--	Operating system start option
	Country Code: 10	--	Operating system country code
	Language ID: 11	--	Operating system language code
CPU Summary: 50#	CPU Name: 1	--	Processor name
	CPU Type: 2	--	Processor type
Memory Summary: 51#	Physical Memory: 1	KBytes	Total physical memory size
	Total Page File Space: 2	KBytes	Total paging file space size included in physical memory
	Page File Name: 3	--	Name of the page file included in physical memory
	File Size: 4	MBytes	Physical memory file size
	Base Memory: 5	Bytes	Physical memory base size
	Extended Memory: 6	KBytes	Physical memory extension size
Disk Summary: 52#	Disk Drive: 1	--	Disk index name
	Storage Type: 2	--	Disk type
	File System Type: 3	--	Disk file system
	Volume Name: 4	--	Disk volume name
	Serial Number: 5	--	Disk serial number
	Total Size: 6	MBytes	Total disk size
	Used Size: 7		Used disk size
	Free Size: 8		Free disk size
	Utilization: 9	%	Disk utilization
	Sectors: 10	--	Number of disk sectors
	Cylinders: 11	--	Number of disk cylinders
	Heads: 12	--	Number of disk heads
Network Summary: 53#	Network Status: 1	--	Network operating status
	Software Major Version: 2	--	Major version of the network software
	Software Minor Version: 3	--	Minor version of the network software
	Software Name: 4	--	Network type
	IPX Address: 5	--	IPX address
	IP Address: 6	--	IP address
	Subnet Mask: 7	--	Network subnet mask
	Default Gateway: 8	--	Gateway address of the managed PC
	Logon User: 9	--	Logon user name
	Work Group: 10	--	Networking group

Resource: Resource ID	Subresource: Subresource ID	Unit	Description
Network Summary: 53#	Shell Major Version: 11	--	Major shell version
	Shell Minor Version: 12	--	Minor shell version
Serial Port Summary: 54#	Port Address: 1	--	Serial port address
	Baud Rate: 2	--	Current baud rate on the serial port
	Parity Enabled: 3	--	Serial port parity check enabled/disabled
	Parity: 4	--	Serial port parity
	Byte Size: 5	Bytes	Serial port packet size
	Stop Bits: 6	--	Number of stop bits at the serial port
	Carrier Detect: 7	--	Carrier Detect at the serial port
	Dataset Ready: 8	--	Dataset Ready at the serial port
	CTS: 9	--	CTS at the serial port
Parallel Port Summary: 55#	Port Address: 1	--	Parallel port address
Video Summary: 56#	Video Mode: 1	--	Current video mode of the display
	Maximum Rows: 2	--	Current line on the display
	Adapter Type: 3	--	Display adapter type
	Manufacturer: 4	--	Display manufacturer
	Display Type: 5	--	Display type
	Second Adapter Type: 6	--	Second display type
	BIOS Date: 7	--	Day the display BIOS was released
Mouse Summary: 57#	Hardware Installed: 1	--	Mouse installation type
	Hardware Type: 2	--	Mouse hardware type
	Manufacturer: 3	--	Mouse manufacturer
	Buttons: 4	--	Number of mouse buttons
	Language ID: 5	--	Mouse language code
	IRQ: 6	--	Mouse IRQ
BIOS Summary: 58#	Manufacturer: 1	--	BIOS manufacturer
	Category: 2	--	BIOS category
	Release Date: 3	--	BIOS release date
IRQ Summary: 59#	IRQ Number: 1	--	IRQ number
	IRQ Address: 2	--	IRQ address
	Description: 3	--	IRQ description
	Detected: 4	--	IRQ description
	Handled By: 5	--	IRQ handler
Environment Summary: 60#	Environment Variable: 1	--	Environment variable name
	Environment Value: 2	--	Environment variable value

Resource: Resource ID	Subresource: Subresource ID	Unit	Description
Service Summary: 61#	Service Name: 1	--	Service name
	Status: 2	--	Service status
	Start Type: 3	--	Service starting method
	Start Name: 4	--	Service execution file
	EXE Path: 5	--	Service execution directory
Network Card Summary: 62#	Manufacturer: 1	--	Network card manufacturer
	IRQ: 2	--	Network card IRQ
	Port Address: 3	--	Network card port address
Audited Software Summary: 63#	Package Number: 1	--	Authentication software package number
	Software Name: 2	--	Authentication software package name
	File Path: 3	--	Directory that includes the authentication software
	File Size: 4	--	Authentication software file size
	File Date: 5	--	Authentication software creation date

#: This table lists summary information that can only be viewed in the Resource Browser window.

E.8 Resources (HighCapacityNetwork group)

The following table lists those resources in the HighCapacityNetwork group which can be collected by SSO-Ex.

Table E-8: Resources (HighCapacityNetwork group)

Resource: Resource ID	Subresource: Subresource ID	Unit	Resource directory	Description
Interface Utilization: 9000#	HalfDuplex: 1	%	HCNET_IfUsRt	Percentage of I/O volume to the line capacity by interface
	FullDuplex: 2			Percentage of the average of input and output volumes to the line capacity by interface
Interface Uses: 9001	InOctets: 1	Octets/Second	HCNET_IfUsAt	Number of octets received via the interface
	OutOctets: 2			Number of octets sent via the interface
Interface Traffic: 9002#	InUcastPkts: 1	Packets/ Second	HCNET_Tff	Number of subnet unicast packets that have been delivered to the high-order protocol
	InMulticastPkts: 2			Number of multicast packets that have been delivered to the high-order protocol
	InBroadcastPkts: 3			Number of subnet broadcast packets that have been delivered to the high-order protocol
	OutUcastPkts: 4			Number of packets that have been sent to subnet unicast addresses requested by the high-order protocol
	OutMulticastPkts: 5			Number of packets that have been sent to multicast destinations requested by the high-order protocol

Resource: Resource ID	Subresource: Subresource ID	Unit	Resource directory	Description
Interface Traffic: 9002#	OutBroadcastPkts: 6	Packets/ Second	HCNET_Tff	Number of packets that have been sent to subnet broadcast destinations requested by the high-order protocol

#: This table lists summary information that can only be viewed in the Resource Browser window.

E.9 Resources (IPv6 Network group)

The following table lists those resources in the IPv6 Network group which can be collected by SSO-Ex.

Table E-9: Resources (IPv6 Network group)

Resource: Resource ID	Subresource: Subresource ID	Unit	Resource directory	Description
IP Traffic: 9003	InReceives: 1	Datagrams/ Second	V6NET_IPIO	Number of datagrams that have been received via the interface
	InUnknownProtos: 2			Number of datagrams that have been destroyed because of an unknown or undefined protocol
	InDelivers: 3			Number of input datagrams that have been successfully delivered to the IP user protocol
	OutRequests: 4			Number of IP datagrams that have been supplied from the IP user protocol
ICMP Traffic: 9004	InMsgs: 1	Messages/ Second	V6NET_ICMPIO	Number of received ICMP messages
	InErrors: 2			Number of received ICMP error messages
	InEchos: 3			Number of received ICMP echo request messages
	InEchoReps: 4			Number of received ICMP echo response messages
	OutMsgs: 5			Number of sent ICMP messages
	OutErrors: 6			Number of sent ICMP error messages
	OutEchos: 7			Number of sent ICMP echo request messages
	OutEchoReps: 8			Number of sent ICMP echo response messages

F. Events

This appendix describes the events that are reported by SSO programs to SNMP managers, for example NNMi.

- Event notification by SSO
  SSO notifies an SNMP manager of an event in the following way:
  - Issuing an incident
    SSO notifies the NNMi on the local or a remote host of an event by issuing an incident. The event reported by SSO is displayed in the incident view of NNMi. For the contents of event display on NNMi, see *F.1 Events (incidents) that are issued by SSO*.

  By default, SSO notifies the NNMi on the local host of events. If you want to change the event destination to another host, define the IP address of the destination host and an event type in the event destination definition file. For the event destination definition file, see *6.3.13 Event destination definition file (ssodest.conf)*.

F.1 Events (incidents) that are issued by SSO

This section describes events that are issued as incidents.

Note that the following items are displayed as the same information for any event on NNMi.

Type: Management event

Family: SSO

(1) Resource collection events

(a) Collection status change events

An event is issued when resource collection status changes. In the `ssocolmng` action definition file, you can specify whether to issue this event. For further information, see *6.3.8 ssocolmng action definition file (ssocolmng.def)*.

The following table lists the contents of the collection status change events that are displayed in the incident view of NNMi.

Table F-1: Contents of the collection status change events displayed in the incident view of NNMi

Incident name	Category	Severity	Message
SSO_Resource_Collect_Normal	Resource	Normal	`The collection status of` *$4* `(resource-ID:` *$1*`) of` *$3* `of` *$2* `is now Collecting. reason:` *$5*
SSO_Resource_Collect_Waiting	Resource	Normal	`The collection status of` *$4* `(resource-ID:` *$1*`) of` *$3* `of` *$2* `is now Standing By. reason:` *$5*
SSO_Resource_Collect_Pending	Resource	Warning	`The collection status of` *$4* `(resource-ID:` *$1*`) of` *$3* `of` *$2* `is now Postponing. reason:` *$5*
SSO_Resource_Collect_Complete	Resource	Normal	`The collection status of` *$4* `(resource-ID:` *$1*`) of` *$3* `of` *$2* `is now Completed. reason:` *$5*
SSO_Resource_Collect_Failure	Resource	Critical	`The collection status of` *$4* `(resource-ID:` *$1*`) of` *$3* `of` *$2* `is now Impossibility. reason:` *$5*

The following table lists the contents of the custom incident attributes that are displayed in the incident form of NNMi.

Table F-2: Contents of the custom incident attributes displayed in the incident form of NNMi (collection status change events)

Attribute	Name	Value
$1	*resource-ID*	Resource ID
$2	*category-name*	Category name
$3	*group-name*	Group name
$4	*resource-name*	Resource name
$5	*reason*	Reason
$6	*event-issuer-host-name*	Event issuer host name
$7	*source-name*	Monitoring server host name#

#: If the definition of host name display is set to `off` (default) in the event destination definition file (`ssodest.conf`) of the event source SSO, the monitoring server IP address is displayed in place of the monitoring server host name.

(b) Resource status change event

SSO issues an event when the status of a resource is changed. Whether to issue the event is defined in the `ssocolmng` action definition file. For the definition in the `ssocolmng` action definition file, see *6.3.8 ssocolmng action definition file (ssocolmng.def)*.

The following table lists the contents of the resource status change events that are displayed in the incident view of NNMi.

Table F-3: Contents of the resource status change events displayed in the incident view of NNMi

Incident name	Category	Severity	Message
SSO_Resource_Monitor_Cancel	Resource	Normal	`The status of` *$4*`:` *$5* `belonging to the` *$3* `group of` *$2* `has changed to Non-monitoring. current-value =`*$7*`, instance =` *$6*`, warning-threshold =` *$8*`, critical-threshold =` *$9*`, previous-status =` *$10*
SSO_Resource_Monitor_Unknown	Resource	Warning	`The status of` *$4*`:` *$5* `belonging to the` *$3* `group of` *$2* `has changed to Unknown. current-value =` *$7*`, instance =` *$6*`, warning-threshold =` *$8*`, critical-threshold =` *$9*`, previous-status =` *$10*
SSO_Resource_Monitor_Normal	Resource	Normal	`The status of` *$4*`:` *$5* `belonging to the` *$3* `group of` *$2* `has changed to Normal region. current-value =`*$7*`, instance =` *$6*`, warning-threshold =` *$8*`, critical-threshold =` *$9*`, previous-status =` *$10*
SSO_Resource_Monitor_Warning	Resource	Warning	`The status of` *$4*`:` *$5* `belonging to the` *$3* `group of` *$2* `has changed to Warning region. current-value =`*$7*`, instance =` *$6*`, warning-threshold =` *$8*`, critical-threshold =` *$9*`, previous-status =` *$10*
SSO_Resource_Monitor_Critical	Resource	Critical	`The status of` *$4*`:` *$5* `belonging to the` *$3* `group of` *$2* `has changed to Critical region. current-value =`*$7*`, instance =` *$6*`, warning-threshold =` *$8*`, critical-threshold =` *$9*`, previous-status =` *$10*

The following table lists the contents of the custom incident attributes that are displayed in the incident form of NNMi.

Table F-4: Contents of the custom incident attributes displayed in the incident form of NNMi (resource status change events)

Attribute	Name	Value
$1	*resource-ID*	Resource ID
$2	*category-name*	Category name
$3	*group-name*	Group name
$4	*resource-name*	Resource name
$5	*subresource-name*	Subresource name
$6	*instance-name*	Instance name
$7	*resource-value*	Resource value
$8	*warning-threshold*	Warning threshold
$9	*critical-threshold*	Critical threshold
$10	*state-before-change*	Status before change (non-monitoring: `Unm`, unknown: `Unk`, normal: `Nor`, warning: `War`, critical: `Cri`)
$11	*event-issuer-host-name*	Event issuer host name[#1]
$12	*source-name*	Monitoring server host name[#2]
$13	*subresource-ID*	Subresource ID
$14	*occurrence-time*	Incident occurrence time
$15	*event-issuer-ip-address*	Event issuer IP address[#3]
$16	*ssoconsole-port*	Port number of the SSO console
$17	*source-ip-address*	Monitoring server IP address
$18	*change-my-address*	SSO action IP address[#4]

#1 This attribute indicates the name of the host at the address in $15.

#2 If the definition of host name display is set to `off` (default) in the event destination definition file (`ssodest.conf`) of the event source SSO, the monitoring server IP address is displayed in place of the monitoring server host name.

#3 This attribute indicates the IP address of the physical host or the IP address set by the `change-my-address:` key. If the NNM action address definition file (`ssonnmactaddr.conf`) is set, this attribute indicates the monitoring manager's IP address that is set.

#4 This attribute indicates the IP address of the physical host or the IP address set by the `change-my-address:` key.

(c) Database threshold excess events

When database monitoring is enabled, SSO issues an event if the size of the collection database exceeds a set threshold.

The following table lists the content of the database threshold excess event that is displayed in the incident view of NNMi.

Table F-5: Content of the database threshold excess event displayed in the incident view of NNMi

Incident name	Category	Severity	Message
SSO_Resource_DB_Size_Warning	Resource	Critical	`The threshold` *$1* `(Kbytes) was exceeded by the collection database (`*$4*`) size. current-value =` *$2* `(Kbytes). user-text:` *$3*

The following table lists the contents of the custom incident attributes that are displayed in the incident form of NNMi.

Table F-6: Contents of the custom incident attributes displayed in the incident form of NNMi (database threshold excess event)

Attribute	Name	Value
$1	*user-specified-threshold*	User specified threshold
$2	*collection-database-size*	Size of collection database
$3	*user-text*	User text
$4	*target-server-name*	Target server name

(2) Process and service monitoring event

(a) Monitoring status change events

SSO issues an event when process monitoring status is changed. Whether to issue the event is defined in the `ssoapmon` action definition file. For the definition in the `ssoapmon` action definition file, see *6.3.7 ssoapmon action definition file (ssoapmon.def)*.

The following table lists the contents of the monitoring status change events that are displayed in the incident view of NNMi.

Table F-7: Contents of the monitoring status change events displayed in the incident view of NNMi

Incident name	Category	Severity	Message
SSO_Process_Monitor_Normal	Process	Normal	`The` *$1* `'s monitored status is changed to Monitoring in progress. reason:` *$2*#
SSO_Process_Monitor_Complete	Process	Normal	`The` *$1* `'s monitored status is changed to Monitoring completed. reason:` *$2*#
SSO_Process_Monitor_Failure	Process	Warning	`The` *$1* `'s monitored status is changed to Unmonitorable. reason:` *$2*#

#: The following table lists the reasons.

Reason	Description
SNMP error.	An SNMP communication error occurred when monitoring conditions had been set.
received event.	An event was received from APM.
lost event.	An event sent from APM was lost.
health check.	A health check request was issued.

The following table lists the contents of the custom incident attributes that are displayed in the incident form of NNMi.

Table F-8: Contents of the custom incident attributes displayed in the incident form of NNMi (monitoring status change events)

Attribute	Name	Value
$1	*application-name*	Application name
$2	*reason*	Reason#1

Attribute	Name	Value
$3	*event-issuer-host-name*	Event issuer host name
$4	*source-name*	Monitoring server host name#2

#1: The following table lists the reasons.

Reason	Description
SNMP error.	An SNMP communication error occurred when monitoring conditions had been set.
received event.	An event was received from APM.
lost event.	An event sent from APM was lost.
health check.	A health check request was issued.

#2: If the definition of host name display is set to `off` (default) in the event destination definition file (`ssodest.conf`) of the event source SSO, the monitoring server IP address is displayed in place of the monitoring server host name.

(b) Process status change events

SSO issues an event when the status of a process is changed. Whether to issue the event is defined in the `ssoapmon` action definition file. For details on the ssoapmon action definition file, see *6.3.7 ssoapmon action definition file (ssoapmon.def)*.

The following table lists the contents of the process status change events that are displayed in the incident view of NNMi.

Table F-9: Contents of the process status change events displayed in the incident view of NNMi

Incident name	Category	Severity	Message
SSO_Process_Status_Unknown_to_Normal	Process	Normal	*$2* of *$1* status changed Unknown to Normal region. The number of running processes=*$3*, upper threshold=*$4*, lower threshold=*$5*
SSO_Process_Status_Unknown_to_Critical	Process	Critical	*$2* of *$1* status changed Unknown to Critical region. The number of running processes=*$3*, upper threshold=*$4*, lower threshold=*$5*
SSO_Process_Status_Normal_to_Unknown	Process	Warning	*$2* of *$1* status changed Normal region to Unknown. The number of running processes=*$3*, upper threshold=*$4*, lower threshold=*$5*
SSO_Process_Status_Normal_to_Critical	Process	Critical	*$2* of *$1* status changed Normal region to Critical region. The number of running processes=*$3*, upper threshold=*$4*, lower threshold=*$5*
SSO_Process_Status_Critical_to_Unknown	Process	Warning	*$2* of *$1* status changed Critical region to Unknown. The number of running processes=*$3*, upper threshold=*$4*, lower threshold=*$5*
SSO_Process_Status_Critical_to_Normal	Process	Normal	*$2* of *$1* status changed Critical region to Normal region. The number of running processes=*$3*, upper threshold=*$4*, lower threshold=*$5*

The following table lists the contents of the custom incident attributes that are displayed in the incident form of NNMi.

Table F-10: Contents of the custom incident attributes displayed in the incident form of NNMi (process status change events)

Attribute	Name	Value
$1	*application-name*	Application name
$2	*process-name*	Process name
$3	*the-number-of-running-processes*	The number of running processes
$4	*upper-threshold*	Upper threshold
$5	*lower-threshold*	Lower threshold
$6	*event-issuer-host-name*	Event issuer host name
$7	*source-name*	Monitoring server host name#

#: If the definition of host name display is set to `off` (default) in the event destination definition file (`ssodest.conf`) of the event source SSO, the monitoring server IP address is displayed in place of the monitoring server host name.

(c) Service status change events

SSO issues an event when the status of a monitoring service is changed. Whether to issue the event is defined in the `ssoapmon` action definition file. For details on the ssoapmon action definition file, see *6.3.7 ssoapmon action definition file (ssoapmon.def)*.

The following table lists the contents of the service status change events that are displayed in the incident view of NNMi.

Table F-11: Contents of the service status change events displayed in the incident view of NNMi

Incident name	Category	Severity	Message
SSO_Service_Status_Unknown_to_Normal	Service	Normal	*$2* of *$1* status changed Unknown to Normal region. A state of operation=*$3*
SSO_Service_Status_Unknown_to_Critical	Service	Critical	*$2* of *$1* status changed Unknown to Critical region. A state of operation=*$3*
SSO_Service_Status_Normal_to_Unknown	Service	Warning	*$2* of *$1* status changed Normal region to Unknown. A state of operation=*$3*
SSO_Service_Status_Normal_to_Critical	Service	Critical	*$2* of *$1* status changed Normal region to Critical region. A state of operation=*$3*
SSO_Service_Status_Critical_to_Unknown	Service	Warning	*$2* of *$1* status changed Critical region to Unknown. A state of operation=*$3*
SSO_Service_Status_Critical_to_Normal	Service	Normal	*$2* of *$1* status changed Critical region to Normal region. A state of operation=*$3*

The following table lists the contents of the custom incident attributes that are displayed in the incident form of NNMi.

Table F-12: Contents of the custom incident attributes displayed in the incident form of NNMi (service status change events)

Attribute	Name	Value
$1	*application-name*	Application name
$2	*service-name*	Service name
$3	*service-status-ja*	Service operating status

Attribute	Name	Value
$4	*service-status-en*	Service operating status
$5	*event-issuer-host-name*	Event issuer host name
$6	*source-name*	Monitoring server host name#

#: If the definition of host name display is set to `off` (default) in the event destination definition file (`ssodest.conf`) of the event source SSO, the monitoring server IP address is displayed in place of the monitoring server host name.

(d) Application status change events

SSO issues an event when the status of an application is changed. Whether to issue the event is defined in the `ssoapmon` action definition file. For details on the ssoapmon action definition file, see *6.3.7 ssoapmon action definition file (ssoapmon.def)*.

The following table lists the contents of the application status change events that are displayed in the incident view of NNMi.

Table F－13: Contents of the application status change events displayed in the incident view of NNMi

Incident name	Category	Severity	Message
SSO_Application_Status_Unknown_to_Normal	Application	Normal	*$1* `status changed Unknown to Normal region.`
SSO_Application_Status_Unknown_to_Warning	Application	Warning	*$1* `status changed Unknown to Precaution region.`
SSO_Application_Status_Unknown_to_Critical	Application	Critical	*$1* `status changed Unknown to Critical region.`
SSO_Application_Status_Normal_to_Unknown	Application	Warning	*$1* `status changed Normal to Unknown region.`
SSO_Application_Status_Normal_to_Warning	Application	Warning	*$1* `status changed Normal to Precaution region.`
SSO_Application_Status_Normal_to_Critical	Application	Critical	*$1* `status changed Normal to Critical region.`
SSO_Application_Status_Warning_to_Unknown	Application	Warning	*$1* `status changed Precaution to Unknown region.`
SSO_Application_Status_Warning_to_Normal	Application	Normal	*$1* `status changed Precaution to Normal region.`
SSO_Application_Status_Warning_to_Critical	Application	Critical	*$1* `status changed Precaution to Critical region.`
SSO_Application_Status_Critical_to_Unknown	Application	Warning	*$1* `status changed Critical to Unknown region.`
SSO_Application_Status_Critical_to_Normal	Application	Normal	*$1* `status changed Critical to Normal region.`
SSO_Application_Status_Critical_to_Warning	Application	Warning	*$1* `status changed Critical to Precaution region.`

The following table lists the contents of the custom incident attributes that are displayed in the incident form of NNMi.

Table F－14: Contents of the custom incident attributes displayed in the incident form of NNMi (application status change events)

Attribute	Name	Value
$1	*application-name*	Application name
$2	*event-issuer-host-name*	Event issuer host name
$3	*source-name*	Monitoring server host name[#]

#: If the definition of host name display is set to `off` (default) in the event destination definition file (`ssodest.conf`) of the event source SSO, the monitoring server IP address is displayed in place of the monitoring server host name.

(e) Process and service monitoring failure events

If the unknown event to be issued when a failure of communication with APM is detected is suppressed by setting, SSO issues a process and service monitoring failure event in place of the unknown event. Whether to issue the process and service monitoring failure event is defined in the `ssoapmon` action definition file. For details on the ssoapmon action definition file, see *6.3.7 ssoapmon action definition file (ssoapmon.def)*.

The following table lists the contents of the process and service monitoring failure events that are displayed in the incident view of NNMi.

Table F－15: Contents of the process and service monitoring failure events displayed in the incident view of NNMi

Incident name	Category	Severity	Message
SSO_Process_Agent_Stop	Process	Warning	`Agent for Process has stopped.`
SSO_Process_Agent_NotCommunicate	Process	Critical	`It cannot communicate with Agent for Process. reason:` *$3*[#]

#: The following table lists the reasons.

Reason	Description
SNMP error.	An SNMP communication error occurred when monitoring conditions had been set.
received event.	An event was received from APM.
lost event.	An event sent from APM was lost.
health check.	A health check request was issued.

The following table lists the contents of the custom incident attributes that are displayed in the incident form of NNMi.

Table F－16: Contents of the custom incident attributes displayed in the incident form of NNMi (process/service monitoring failure notification events)

Attribute	Name	Value
$1	monitoring-server-host-name	Host name of monitoring target server
$2	monitoring-server-ip-address	IP address of monitoring target server
$3	reason	Reason[#1]
$4	event-issuer-host-name	Event issuer host name
$5	source-name	Monitoring server host name[#2]

#1: The following table lists the reasons.

Reason	Description
SNMP error.	An SNMP communication error occurred when monitoring conditions had been set.
received event.	An event was received from APM.
lost event.	An event sent from APM was lost.
health check.	A health check request was issued.

#2: If the definition of host name display is set to `off` (default) in the event destination definition file (`ssodest.conf`) of the event source SSO, the monitoring server IP address is displayed in place of the monitoring server host name.

G. Variables That Can Be Defined via Automated Action

G.1 Variables that can be used

This section describes the variables that are available for the commands to be used for automated actions. For automated actions, see *2.5.2(4) Automated actions and remote commands*.

The following table lists the variables.

Table G-1: Variables that can be defined via automated action

Variable name	Value	Availability for resource collection	Availability for process monitoring	Availability for service monitoring
$DATE$	Event date (format: *yyyy/mm/dd*)	Y	Y	Y
$TIME$	Event time (format:*hh:mm:ss*)	Y	Y	Y
$SERVERNAME$	Name of the server to be monitored	Y	Y	Y
$IPADDRESS$	IP address of the server to be monitored	Y	Y	Y
$RSCID$	Target resource ID	Y	N	N
$CATEGORY$	Target resource category name	Y	N	N
$RSCNAME$	Target resource name	Y	N	N
$SUBRSCNAME$	Target resource subresource name	Y	N	N
$INSTANCE$	Target instance name	Y	N	N
$DATAVALUE$	Target data value	Y	N	N
$THRESHOLD_WAR$	Warning threshold for target resource	Y	N	N
$THRESHOLD_CRI$	Critical threshold for target resource	Y	N	N
$APPLICATION$	Target application name	N	Y	Y
$PROCESSNAME$	Target process name • For parent process: *parent-process-name(process-type)* • For child process: *parent-process-name(process-type):child-process-name(process-type)* *process-type*: Execution file name: `F` Command line name: `C`	N	Y#	N
$PROCESSCOUNT$	Number of active target processes	N	Y#	N
$THRESHOLD_UP$	Upper threshold for target process	N	Y#	N
$THRESHOLD_LOW$	Lower threshold for target process	N	Y#	N
$STATUS$	Status the resource, application, or process after the change • For resource monitoring Not monitored: `Unm`	Y	Y	Y

Variable name	Value	Availability for resource collection	Availability for process monitoring	Availability for service monitoring
$STATUS$	Unrecognizable: `Unk` Normal: `Nor` Warning: `War` Critical: `Cri` • For process monitoring Unrecognizable: `Unk` Normal: `Nor` Warning: `War` Critical: `Cri`	Y	Y	Y
$SERVICENAME$	• Service name *service-name* (*type*) • Type Service name: `S`	N	N	Y
$SERVICESTATUS$	• Service operating status after the change Running: `Running` Stopped: `Stopped` Paused: `Paused` Starting: `Start Pending` Stopping: `Stop Pending` Pausing: `Pause Pending` Resuming: `Continue Pending` Invalid name: `Invalid Name` Unknown: `Unknown`	N	N	Y

Legend:

Y: The variable is available.

N: The variable is not available.

You can only specify this variable in a situation that involves process status change.

H. Language Environment Variables

The following table lists the language environment variables that are supported by SSO.

Table H-1: Language environment variables supported by SSO

OS	Character code	LANG environment variable
Solaris	ASCII	C
	Shift-JIS	ja_JP.PCK
	EUC	ja ja_JP.eucJP
Linux	ASCII	C
	Shift-JIS	Cannot used
	EUC	Cannot used
	UTF-8	ja_JP.UTF-8 ja_JP.UTF8 ja_JP.utf-8 ja_JP.utf8 zh_CN.utf8
Windows	ASCII	C
	Shift-JIS	Japanese_Japan.932
	GBK	Chinese (Simplified)_People's Republic of China.936 or Chinese (Simplified)_China.936

I. General Purpose Path Names

The file storage directories for SSO programs vary according to the OS. Therefore, this manual uses general purpose path names.

I.1 General purpose path names for SSO

The next table lists the relationship between the general path names of the files used by SSO and the path names actually assigned under each operating system.

Table I-1: General-purpose path names of SSO files

General purpose path name	Actual path name	
	UNIX	Windows
$SSO_AUDITLOG	/var/opt/CM2/SSO/auditlog	*installation-directory*\auditlog
$SSO_BACKUP	/var/opt/CM2/SSO/tmp/ssobackup	*installation-directory*\tmp\ssobackup
$SSO_BIN	/opt/CM2/SSO/bin	*installation-directory*\bin
$SSO_CONF	/etc/opt/CM2/SSO/conf	*installation-directory*\conf
$SSO_DB	/var/opt/CM2/SSO/databases	*installation-directory*\databases
$SSO_ETC	/etc/opt/CM2/SSO	*installation-directory*
$SSO_HELP	/opt/CM2/SSO/help	*installation-directory*\help
$SSO_HELP_EN	/opt/CM2/SSO/help_en	*installation-directory*\help_en
$SSO_IMAGE	/opt/CM2/SSO/www/htdocs/images/sso	*installation-directory*\www\htdocs\C\images\sso
$SSO_INCIDENT	/etc/opt/CM2/SSO/incident	*installation-directory*\incident
$SSO_JAR	/opt/CM2/SSO/classes	*installation-directory*\classes
$SSO_JRE	/opt/CM2/SSO/uCPSB	*installation-directory*\uCPSB
$SSO_LIB	/opt/CM2/SSO/lib	*installation-directory*\lib
$SSO_NEWCONF	/etc/opt/CM2/SSO/newconfig	*installation-directory*\newconfig
$SSO_NLS	/opt/CM2/SSO/nls	*installation-directory*\nls
$SSO_OPT	/opt/CM2/SSO	*installation-directory*
$SSO_REPORT	/var/opt/CM2/SSO/report	*installation-directory*\report
$SSO_RSC	/etc/opt/CM2/SSO/conf/rsc	*installation-directory*\conf\sso\rsc\
$SSO_SAMPLE	/opt/CM2/SSO/sample	*installation-directory*\sample
$SSO_TEMPLATE	/etc/opt/CM2/SSO/template	*installation-directory*\template
$SSO_TMP	/var/opt/CM2/SSO/tmp	*installation-directory*\tmp
$SSO_URLACTION	/etc/opt/CM2/SSO/urlaction	*installation-directory*\urlaction
$SSO_USERRSC	/etc/opt/CM2/SSO/sample/userrsc	*installation-directory*\sample\userrsc
$SSO_VAR	/var/opt/CM2/SSO	*installation-directory*

J. Version Revisions

J.1 Revisions in 10-50

- A description of the fraction of resource values that are displayed or output was added.
- A note on NNMi cooperation functions was added.
- The NNM action address definition file (`ssonnmactaddr.conf`) was added.
- The Resource Data Reference window can now be used to search collected data by server name.
- The settings of the monitoring applications can now be changed.
- The settings of the monitoring processes and child processes can now be changed.
- The settings of the monitoring services can now be changed.
- The Process Configuration window, Process Configuration Browser window, and Process Monitor window can now be used to search for specific monitoring servers.
- Items were added to the *Acquired data* column of *Collected data list* (list of data items to be collected for error investigation).
- Conditions in which `ssocadel` fails were added.
- The user name and password can now include single-byte spaces. With this improvement, a usage example was added.
- In the user resource definition file, MIB expressions can now be written in infix notation. With this improvement, the subresource definition and definition example were changed.
- JP1/Cm2/Extensible SNMP Agent 10-50 was added as an SNMP agent.
- The custom incident attribute `change-my-address` was added to the resource collection status change event.

K. Reference Material for This Manual

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

K.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):

About JP1:

- *Job Management Partner 1/Base User's Guide* (3021-3-301(E))
- *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide* (3021-3-305(E))
- *Job Management Partner 1/Consolidated Management 2/Extensible SNMP Agent Description, Operator's Guide and Reference* (3021-3-346(E))
- *Job Management Partner 1/Consolidated Management 2/Network Node Manager i Installation Guide* (3021-3-342(E))
- *Job Management Partner 1/Consolidated Management 2/Network Node Manager i Setup Guide* (3021-3-343(E))
- *Job Management Partner 1/Software Distribution Description and Planning Guide* (3020-3-S79(E)), for Windows systems
- *Job Management Partner 1/Software Distribution System Administrator's Guide Volume 1* (3020-3-S81(E)), for Windows systems
- *Job Management Partner 1/Software Distribution SubManager Description and Administrator's Guide* (3020-3-L42(E)), for UNIX systems
- *Job Management Partner 1/Software Distribution Manager Description and Administrator's Guide* (3000-3-841(E))

K.2 Conventions: Abbreviations for product names

This manual uses the following abbreviations for product names:

Full name or meaning	Abbreviation	
Job Management Partner 1/Consolidated Management 2/ SNMP System Observer	JP1/Cm2/SSO	SSO
Job Management Partner 1/Consolidated Management 2/ SNMP System Observer - Agent for Process	APM	
Job Management Partner 1/Consolidated Management 2/ Extensible SNMP Agent	ESA	
HP Network Node Manager i Advanced Software	HP NNMi	NNMi
HP Network Node Manager i Software		
Job Management Partner 1/Consolidated Management 2/ Network Node Manager i	JP1/Cm2/NNMi	
Job Management Partner 1/Consolidated Management 2/ Network Node Manager i Advanced		

Full name or meaning	Abbreviation	
Job Management Partner 1/Consolidated Management 2/ Network Node Manager i Advanced	NNMi-Adv	
HP Network Node Manager i Advanced Software		
Job Management Partner 1/Integrated Management - Manager	JP1/IM - Manager	JP1/IM
Job Management Partner 1/Integrated Manager - View	JP1/IM - View	
Job Management Partner 1/Automatic Job Management system 3	JP1/AJS3	
Itanium(R) Processor Family	IPF	
Mozilla Firefox(R)	Firefox	
Red Hat Enterprise Linux(R)	Linux	
AIX	UNIX	
HP-UX		
Linux		
Solaris		

K.3 Conventions: Acronyms

This manual also uses the following acronyms:

Acronym	Full name or meaning
AP	Application Program
APIPA	Automatic Private IP Addressing
BIOS	Basic Input/Output System
CPU	Central Processing Unit
CSV	Comma Separated Values
DB	Database
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
EUC	Extended UNIX Code
GUI	Graphical User Interface
HTML	Hyper Text Markup Language
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ID	Identification
IP	Internet Protocol
IPF	Itanium(R) Processor Family
IPv4	Internet Protocol Version 4

Acronym	Full name or meaning
IPv6	Internet Protocol Version 6
JIS	Japanese Industrial Standard code
JRE	JavaTM 2 Runtime Environment
LAN	Local Area Network
MIB	Management Information Base
NAPT	Network Address Port Translation
NAT	Network Address Translation
NIC	Network Interface Card
OS	Operating System
PAT	Port Address Translation
PC	Personal Computer
RFC	Request For Comment
SJIS	Shift JIS
SNMP	Simple Network Management Protocol
SVG	Scalable Vector Graphics
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UAC	User Account Control
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VM	Virtual Machine
VML	Vector Markup Language
WAN	Wide Area Network
WOW64	Windows On Windows 64
WSFC	Windows Server Failover Clustering
WWW	World Wide Web

K.4 Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

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

- 1 TB (terabyte) is $1{,}024^4$ bytes.

K.5 General Purpose Path Names

The file storage directories for SSO programs vary according to the OS. Therefore, this manual uses general purpose path names.

For the correspondence between the general purpose path names used in this manual for individual software products and the actual paths that vary according to the OS, see *I. General Purpose Path Names*.

K.6 Online manual

SSO comes with an HTML manual that you can read in the Web browsers.

To read the HTML manual, perform the following operation:

In Windows

Select **Help** on the menu bar of the SSO console window or another window. Alternatively, from the **Start** menu of Windows, select **Programs**, **SNMP System Observer**, **SSO**, **Online Documentation**, and then **Manual**.

In UNIX

Select **Help** on the menu bar of the SSO console window or another window.

When the OS is UNIX, you must in advance specify the Web browser installation path in the GUI definition file.

K.7 IP addresses

In this manual, *IP address* means an IPv4 or IPv6 address when referring to the IP address of a monitoring server that collects resources. In other cases, *IP address* always means an IPv4 address.

When specifying an IPv6 address, use the IPv6 address notation defined in RFC 2373. For the notes on specifying an IPv6 address, see *1.4.2(2) Notes on IP addresses of monitoring servers*.

Also, for the format of the IPv6 address that is output to commands, windows, and definition files, see *1.4.2(4) IPv6 addresses output to commands, windows, and definition files*.

L. Glossary

automated action

A function that issues a command automatically on the monitoring manager or the agent when a status change is detected during the threshold monitoring by SSO for an application or resource.

category

A group of multiple resources. Resources provided by SSO belong to the `SSO` or `SSO-Ex` category. Resources provided by JP1/Cm2/SSO for Database Server belong to the `ORACLE` category. Resources that are defined by users belong to the `USER` category.

cluster system

A system that includes multiple server systems linked to each other appropriately. The purpose of clustering is to continue system operation when an error occurs. When an error occurs in the operating server (main system), the standby server (secondary system) will take over the system operation tasks. Since the secondary system switches to the main system, the cluster system is also referred to as a *system-switching system*.

The term *cluster system* also means a system provided with a load distribution feature based on parallel processing. In this manual, however, the term is used to indicate the system switching function that is useful for preventing system operation from being interrupted.

collecting server

A server that collects resources. A collecting server requires that SSO be installed.

collection condition

Condition for resource collection. It includes information on the resource to be collected, collection interval, collection duration, and collection mode (data storage and threshold).

collection database

A database that holds data representing collected resources.

dual stack

A capability of a host that has both of IPv4 and IPv6 addresses and can communicate with others by using either Internet protocol.

health check

A function used to verify that APM is normally active on a server and that the monitoring condition on SSO matches that on APM. The health check function is also used for other types of verification.

instance

The entity of a resource value in terms of the resource collection by SSO.

For example, regarding the file system utilization in the file system group, each file system is an instance, and, regarding the CPU utilization in the CPU group, each CPU is an instance.

IPv4

An acronym of Internet Protocol Version 4. IPv4 manages addresses as 32-bit data.

IPv6

An acronym of Internet Protocol Version 6. IPv6 manages addresses as 128-bit data.

JP1/Cm2/SSO

A program that collects and manages server resources in a network and monitors processes.

JP1/Cm2/SSO - Agent for Process

A program that monitors processes that run on a server.

logical host

A host that functions as a logical server in a JP1 environment for a cluster system. When an error occurs on the main system, the logical host that has served for the secondary system will be switched to the logical host for the main system.

A logical host is assigned its own IP address (logical IP address). When system switching takes place, the new main system will take over the IP address from the logical system that has served for the main system. When clients access the server, they can use the same IP address before and after the error occurs, as if only one server served for the clients.

logical IP address

The address that is specified as the IP address of a logical host included in a cluster system.

management manager

A machine that manages the monitoring events that are reported from SSO in a distributed system configuration. The management manager must have NNMi installed.

monitoring manager

A machine that monitors results of resource collection and process monitoring in a consistent manner. Any monitoring manager requires that SSO be installed.

In the basic system configuration, the monitoring manager is the machine on which SSO and NNMi are running. In a distributed system configuration, the monitoring manager is a machine on which SSO alone is running.

monitoring server

A machine that monitors processes. Any monitoring server requires that APM be installed.

NNMi

A program used to manage the configuration, performance, and problems of a network. You can reference the incidents and events issued by SSO programs in the incident view and incident form of NNMi. NNMi is a prerequisite program for SSO.

performance data

Dynamic information, such as system operation information and statistical information. Performance data can be displayed in the Resource Browser window.

periodic inquiry

A function to periodically collect resources at specified intervals.

plot interval

A length of time that is specified in the `plot_type` key in the report definition file and in the **Plot type** field in the Report Type Setup window.

plot point

Plot points are used to draw a graph line in a graph to be output. The collected data is averaged at plot intervals, and calculated as coordinate values.

Regional Manager

A manager that sends event and other information to the global manager in an NNMi global network management environment.

remote command

A command that is issued automatically or at any timing from the monitoring manager to a monitoring server.

resource

A group of multiple subresources. A collection condition can be specified for each resource.

resource directory

A directory that holds a collection database.

resource group

A group of multiple resources.

server targeted for collection

A server from which resources are to be collected. A server targeted for collection requires SNMP Agent installed.

SNMP agent

A program that manages system resources on a server. SSO manages resources based on information managed by SNMP Agent.

statistics information database

A database that is used internally to calculate thresholds when statistical thresholds are monitored.

subresource

A minimum unit of resource that can be acquired from SNMP Agent. Thresholds can be specified for each subresource.

summary data

Static information, including computer configuration and setting information. Summary data can be displayed in the Resource Browser window.

system-switching system

See *Cluster system*.

threshold

A value used to judge the status of a resource or process. For a resource, a threshold can be set for each subresource. For processes, a threshold indicates the number of processes that can be activated concurrently.

tunneling

A technology that enables communication between different protocols by packet encapsulation and decapsulation.

variable binding(s) or VarBind

A list of pairs of an object identifier (that specifies the information attached to an SNMP trap) and a value.

zombie

A process the termination of which is not known to its parent process.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z