



Systemwalker Service Quality Coordinator

User's Guide

Windows/Solaris/Linux

J2X1-6820-03ENZ0(00)
May 2011

Preface

Purpose of this manual

This manual describes the management functions provided by Systemwalker Service Quality Coordinator.

It explains practical issues, such as linking to middleware, setting thresholds, and how to create and install a Browser Agent package.

Target audience

This manual is intended for users who will set up and use the Systemwalker Service Quality Coordinator management functions.

Readers of this manual should also have a general understanding of basic operating system and GUI operations as well as a working knowledge of communications protocols such as TCP/IP and SMTP.

Organization of Systemwalker Service Quality Coordinator manuals

The Systemwalker Service Quality Coordinator manuals are organized as follows:

- Systemwalker Service Quality Coordinator Technical Guide
Provides an overview of the functions of Systemwalker Service Quality Coordinator.
- Systemwalker Service Quality Coordinator Installation Guide
Explains how to install and set up Systemwalker Service Quality Coordinator.
- Systemwalker Service Quality Coordinator User's Guide
Explains how to use the functions of Systemwalker Service Quality Coordinator.
- Systemwalker Service Quality Coordinator User's Guide (Console Edition)
Explains how to use those functions related to console windows.
- Systemwalker Service Quality Coordinator User's Guide (Dashboard Edition)
Explains how to use the dashboard functions.
- Systemwalker Service Quality Coordinator Reference Guide
Explains commands, data formats, messages and so on.
- Systemwalker Service Quality Coordinator Troubleshooting Guide
Explains how to handle any problems that may occur.
- Systemwalker Service Quality Coordinator User's Guide (Website Management Functions Edition)
Explains the Systemwalker Service Quality Coordinator functions that relate to analyzing Web usage and monitoring Web content tampering.
- Systemwalker Service Quality Coordinator Glossary
This manual explains Systemwalker Service Quality Coordinator terminology.

Organization of this manual

- [Chapter 1 Linking to Other Products](#)

This chapter explains the setup procedures for linking Systemwalker Service Quality Coordinator to other products.

- [Chapter 2 Managing the Volume of Web Transactions](#)

This chapter explains the procedure for managing the volume of Web transactions.

- [Chapter 3 Management with an Agent for Agentless Monitoring](#)

This chapter explains how to remotely manage a monitored server that does not have an Agent installed.

- [Chapter 4 Managing End User Response](#)

This chapter presents an overview of end user response measurement, and explains how to set up the environment and how to create and install the Browser Agent package.

- [Chapter 5 Service Operation Management](#)

This chapter presents an overview of service operational management and explains the environment settings.

- [Chapter 6 Response and Managed Object Configuration Information \(ServiceConf.xml\)](#)

This chapter explains how to edit the "ServiceConf.xml" file and how to create BODY files.

- [Chapter 7 Eco Information Management](#)

This chapter explains how to visually display the current power consumption and temperature status of the monitored IT system.

- [Chapter 8 Managing User Data](#)

This chapter explains customized data, such as business data and system operational data.

- [Chapter 9 Collection Template](#)

This chapter explains the definition settings that are made in the templates for getting performance information.

- [Chapter 10 Threshold Monitoring](#)

This chapter explains how to define thresholds for threshold monitoring and also describes the types of actions for notifying administrators.

- [Chapter 11 Policy Distribution](#)

This chapter explains how to operate the policy distribution function.

- [Chapter 12 Backup and Restore](#)

This chapter explains how to back up and restore the operation environment for Systemwalker Service Quality Coordinator.

- [Appendix A Setup Commands and Resident Processes](#)

This appendix explains the policy command used to set up Systemwalker Service Quality Coordinator, and describes the processes that are started.

Positioning of this document

This manual is common to the following Systemwalker Service Quality Coordinator products for Windows, Linux and Oracle Solaris:

- Systemwalker Service Quality Coordinator Enterprise Edition V13.5.0
- Systemwalker Service Quality Coordinator Standard Edition V13.5.0

Abbreviations

- Microsoft® Windows NT® Server network operating system Version 4.0 and Microsoft® Windows NT® Workstation operating system Version 4.0 are abbreviated as "Windows NT®".
- Microsoft® Windows® 2000 Professional operating system, Microsoft® Windows® 2000 Server operating system, and Microsoft® Windows® 2000 Advanced Server operating system are all abbreviated as "Windows® 2000".

- Microsoft® Windows® 98 operating system is abbreviated as "Windows® 98".
- Microsoft® Windows® XP Professional is abbreviated as "Windows® XP".
- Microsoft® Windows Server® 2003 Enterprise Edition, Microsoft® Windows Server® 2003 Standard Edition and Microsoft® Windows Server® 2003 Web Edition are all abbreviated as "Windows® 2003".
- Microsoft® Windows Server® 2008 Enterprise and Microsoft® Windows Server® 2008 Standard are abbreviated as "Windows® 2008".
- Windows Vista® Home Basic, Windows Vista® Home Premium, Windows Vista® Business, Windows Vista® Enterprise and Windows Vista® Ultimate are abbreviated as "Windows Vista®".
- Windows® 7 Home Premium, Windows® 7 Professional, Windows® 7 Enterprise and Windows® 7 Ultimate are abbreviated as "Windows® 7".
- Microsoft® SQL Server is abbreviated as "SQL Server".
- Microsoft® Cluster Server is abbreviated as "MSCS".
- Oracle Solaris might be described as Solaris, Solaris Operating System, or Solaris OS.
- Systemwalker Centric Manager is abbreviated as "Centric Manager".
- Symfoware Server is abbreviated as "Symfoware".
- Interstage Application Server is abbreviated as "Interstage".
- Oracle Database is abbreviated as "Oracle".
- Systemwalker Resource Coordinator is abbreviated as "Resource Coordinator".
- Versions of Systemwalker Service Quality Coordinator that operate under Windows are referred to as "Windows versions".
- Versions of Systemwalker Service Quality Coordinator that operate under Solaris are referred to as "Solaris versions".
- Versions of Systemwalker Service Quality Coordinator that operate under Linux are referred to as "Linux versions".
- Solaris and Linux versions of Systemwalker Service Quality Coordinator are referred to collectively as "UNIX versions".
- The term "Agent" is used to refer to articles common to both Agent for Server and Agent for Business.

Conventions used in this document

- Edition-specific information

This manual deals mainly with the Standard Edition and Enterprise Edition of Systemwalker Service Quality Coordinator. The following symbols appear in the title or text of an article to distinguish between the Standard Edition (standard specification) and the Enterprise Edition.

EE

This indicates that the article relates specifically to Systemwalker Service Quality Coordinator Enterprise Edition.

SE

This indicates that the article relates specifically to Systemwalker Service Quality Coordinator Standard Edition.

- Information specific to Windows or UNIX versions

This document contains information common to both Windows versions and UNIX versions of Systemwalker Service Quality Coordinator. Information specific to only the Windows versions and information specific to only the UNIX versions are distinguished from common information by attaching the following symbols:

[Windows]

This indicates that the article relates specifically to Windows versions.

[UNIX]

This indicates that the article relates specifically to UNIX versions.

The symbols **[Solaris]**, **[Linux]**, **[AIX]**, and **[HP-UX]** are used to distinguish Solaris, Linux, AIX, and HP-UX versions of Systemwalker Service Quality Coordinator.

If notice should be paid, the information is distinguished from common information by attaching the following symbols:

S

This indicates that the article relates specifically to Solaris versions.

Symbols

The symbols used with commands are explained below.

[Entry example]

```
[PARA={a | b | c |...}]
```

[Meaning of each symbol]

Symbol	Meaning
[]	Items enclosed in square brackets are optional.
{ }	Select one of the items enclosed in braces ({ }).
_	When all optional items enclosed in square brackets ([]) are omitted, the default value indicated by an underscore (_) is used.
	Select one of the items separated by vertical bars.
...	The item immediately before the ellipsis (...) can be repeatedly specified.

Trademarks

- MS-DOS, Microsoft, Windows, the Windows logo and Windows NT are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.
- Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Oracle is a registered trademark of ORACLE Corporation in the United States.
- Linux is a trademark or registered trademark of Mr. Linus Torvalds in the United States and other countries.
- Red Hat, RPM and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.
- Intel, Pentium and Itanium are registered trademarks of Intel Corporation.
- Systemwalker is a registered trademark of Fujitsu Limited.
- Interstage is a registered trademark of Fujitsu Limited.
- Symfoware is a registered trademark of Fujitsu Limited.
- Other company names and product names are trademarks or registered trademarks of their respective companies.

Acknowledgement

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

May 2011

Request

- No part of the content of this manual may be reproduced without the written permission of Fujitsu Limited.
- The contents of this manual may be changed without notice.

Copyright FUJITSU LIMITED 2003-2011

Contents

Chapter 1 Linking to Other Products.....	1
1.1 Linking to Interstage Application Server.....	1
1.1.1 Installation check.....	3
1.1.2 Transaction breakdown analysis.....	3
1.1.3 Definition method.....	4
1.1.4 Setup.....	5
1.1.5 Display.....	5
1.2 Linking to Symfoware Server.....	6
1.2.1 Installation check.....	6
1.2.2 Definition method.....	7
1.2.3 Setup.....	12
1.2.4 Display.....	12
1.2.5 Stopping Symfoware Server where a Service Quality Coordinator Agent has been installed.....	13
1.2.6 If performance information for Symfoware is not collected.....	13
1.3 Linking to Oracle Database Server.....	14
1.3.1 Installation check.....	14
1.3.2 Definition Method.....	15
1.3.3 Setup.....	19
1.3.4 Display.....	21
1.4 Linking to Systemwalker Centric Manager.....	21
1.4.1 Installation check.....	22
1.4.2 Threshold monitoring.....	23
1.4.3 Linking to Invoke the Summary View.....	24
1.4.4 Storing performance information (traffic information) in the PDB.....	24
1.4.4.1 Definition method.....	24
1.4.4.2 Setup.....	25
1.4.4.3 Storing traffic information in the PDB.....	25
1.4.4.4 Display.....	26
1.5 Linkage with Systemwalker Operation Manager.....	26
1.5.1 Installation check.....	26
1.5.2 Definition method.....	27
1.5.3 Setup.....	30
1.5.4 Displaying performance information.....	31
1.6 Linking to Systemwalker Network Manager.....	31
1.6.1 Installation check.....	31
1.6.2 Definition method.....	32
1.6.3 Setup.....	32
1.6.4 Display.....	32
1.7 Linking to Systemwalker Resource Coordinator (Server Provisioning).....	33
1.7.1 Installation check.....	33
1.7.2 Manual registration method.....	34
1.8 Linking to Systemwalker Resource Coordinator (Network Resource Manager).....	34
1.8.1 Installation check.....	35
1.8.2 Setup.....	35
1.8.3 Display.....	36
1.9 Linking to Systemwalker Resource Coordinator (Storage Resource Manager)/ETERNUS SF Storage Cruiser.....	36
1.9.1 Installation check.....	36
1.9.2 Setup.....	37
1.9.3 Display.....	37
1.10 Linking to Microsoft SQL Server.....	38
1.10.1 Installation check.....	38
1.10.2 Definition method.....	38
1.10.3 Setup.....	39
1.10.4 Display.....	39

1.11 Linking to Microsoft .NET.....	39
1.11.1 Installation check.....	39
1.11.2 Definition method.....	40
1.11.3 Setup.....	40
1.11.4 Display.....	40
1.12 Linking to SAP NetWeaver.....	41
1.12.1 Installation check.....	41
1.12.2 Definition method.....	41
1.12.2.1 Connection destination system definition file.....	42
1.12.2.2 Connection parameters definition file.....	43
1.12.3 Setup.....	45
1.12.4 Display.....	45
1.13 Linkage with Hyper-V.....	45
1.13.1 Check Installation.....	46
1.13.2 Definition Method.....	46
1.13.3 Setup.....	47
1.13.4 Display.....	47
1.14 Linkage with the Red Hat Virtualization Function (Xen).....	47
1.14.1 Check Installation.....	48
1.14.2 Definition Method.....	49
1.14.3 Setup.....	49
1.14.4 Display.....	49
Chapter 2 Managing the Volume of Web Transactions.....	50
2.1 Transaction Log Definitions.....	50
2.1.1 Definition format.....	51
2.1.2 Checking definition contents.....	60
2.2 Setup.....	60
2.3 Display.....	60
2.4 Transaction Log Definition File (Sample).....	60
2.4.1 Sample files.....	61
2.4.2 Transaction log definition file (Internet Information Services 5.0).....	62
2.4.3 Transaction log definition file (Internet Information Services 6.0).....	63
2.4.4 Transaction log definition file (Internet Information Services 7.0).....	63
2.4.5 Transaction log definition file (Apache HTTP Server [Common log format]).....	64
2.4.6 Transaction log definition file (Apache HTTP Server [Combined log format]).....	66
2.4.7 Transaction log definition file (Interstage HTTP Server [Common log format]).....	67
Chapter 3 Management with an Agent for Agentless Monitoring.....	69
3.1 Server Performance Management.....	69
3.1.1 Prerequisites.....	70
3.1.2 Settings for Monitored Servers.....	71
3.1.3 Settings for Monitoring Servers.....	74
3.1.3.1 Definition method.....	74
3.1.3.1.1 Connection account configuration file.....	75
3.1.3.1.2 Remote monitoring configuration file.....	76
3.1.3.2 Setup.....	78
3.1.4 Display.....	79
3.1.5 Differences between Agents for Agent-based Monitoring and Agents for Agentless Monitoring.....	81
3.2 Virtual Resource Management.....	83
3.2.1 Prerequisites.....	85
3.2.2 Settings for Monitored Servers.....	87
3.2.3 Settings for Monitoring Servers.....	92
3.2.3.1 Definition method.....	92
3.2.3.1.1 Creating a connection account configuration file.....	92
3.2.3.1.2 Creating remote monitoring configuration file.....	93
3.2.3.2 Setup.....	95
3.2.4 Display.....	96

Chapter 4 Managing End User Response.....	100
4.1 Overview of Measurements.....	100
4.2 Environment Settings.....	103
4.2.1 Setting up the temporary file environment of the collection server.....	103
4.2.2 Setting up the CGI environment of the collection server.....	103
4.2.3 Creating and applying collection policies.....	104
4.3 Installing a Browser Agent.....	104
4.3.1 Creating the package.....	106
4.3.2 Installation conditions.....	115
4.3.2.1 Hardware environment.....	115
4.3.2.2 Operating systems.....	116
4.3.2.3 Products that cannot be installed.....	116
4.3.3 Installing the package.....	116
4.3.4 Starting Browser Agents.....	121
4.3.5 Upgrading and reinstalling Browser Agent.....	122
4.3.6 Uninstalling Browser Agent.....	122
4.4 Supplementary Information Relating to Product Deployment.....	123
4.4.1 Basic product deployment pattern.....	123
4.4.2 Product deployment pattern to perform regular measurements.....	124
4.5 Supplementary Information Relating to Browser Agent Packages.....	126
4.5.1 When analyzing measurement results by given groups.....	127
4.5.2 When analyzing measurement results by end user attributes.....	127
4.5.3 When analyzing measurement results by end user attributes.....	127
4.6 Display.....	127
4.6.1 End user response resource data.....	127
Chapter 5 Service Operation Management.....	129
5.1 Measurement Overview.....	129
5.2 Environment Settings.....	129
5.3 Display.....	130
5.4 Service operation watch time-out value setting.....	130
5.4.1 Definition Method.....	132
Chapter 6 Response and Managed Object Configuration Information (ServiceConf.xml).....	133
6.1 Storage Location.....	134
6.2 Definition Method.....	134
6.2.1 Response information (WebSite tag).....	135
6.2.2 HTTP operation information (HTTP_Service tag).....	136
6.2.3 DNS operation information (DNS_Service tag).....	138
6.2.4 SMTP operation information (SMTP_Service tag).....	139
6.2.5 PORT operation information (PORT_Service tag).....	140
6.3 Definition Example.....	141
6.4 Setup.....	142
6.5 How to Create BODY Files.....	142
Chapter 7 Eco Information Management.....	146
7.1 Overview of Measurements Taken.....	146
7.2 Checks before Installation.....	148
7.3 Definition Method.....	148
7.3.1 Storing the MIB Definitions File.....	148
7.3.2 Setting the ECO Information Collection Definitions File.....	149
7.3.3 Setting the SNMP Agent Configuration Information File.....	150
7.4 Setup.....	152
7.5 Display.....	152
Chapter 8 Managing User Data.....	154
8.1 Defining User Data.....	154
8.1.1 Definition format.....	155

8.2 Setup.....	156
8.3 Storing User Data in the PDB.....	157
8.4 Display.....	160
Chapter 9 Collection Template.....	161
9.1 How to Set up Oracle Database Server.....	161
9.1.1 How to create a new user that can access the Oracle dynamic performance view.....	163
9.2 How to Set Up Microsoft .NET Server.....	164
9.3 How to Set Up Microsoft SQL Server.....	164
9.4 How to Set Up Hyper-V.....	165
9.5 How to Set Up the Red Hat Virtualization Function (Xen).....	165
9.6 Middleware Linkage Settings with Enterprise Manager.....	166
9.7 Stopping Middleware Management.....	167
Chapter 10 Threshold Monitoring.....	169
10.1 Threshold Monitoring Definitions.....	170
10.1.1 Definition Method.....	170
10.1.2 Sample definition.....	173
10.2 Threshold Monitoring Definition File (Sample).....	174
10.3 Alarm Action Definitions.....	176
10.3.1 Definition method.....	177
10.3.1.1 Defining the action type.....	177
10.3.1.2 When MAIL is selected.....	177
10.3.1.3 When TRAP is selected.....	179
10.3.1.4 When OTHER is selected.....	179
Chapter 11 Policy Distribution.....	181
11.1 Overview of the Policy Distribution Function.....	181
11.1.1 Policy distribution function.....	181
11.1.2 Usage conditions for the policy distribution function.....	183
11.1.2.1 Versions with which the policy distribution function can be used.....	183
11.1.2.2 Operating conditions for the policy distribution function.....	183
11.1.3 The Directory Structure of the Definition Folder.....	184
11.2 Policy Distribution Procedure.....	186
11.2.1 Creating policy distribution groups.....	187
11.2.2 Creating policy definition information files.....	188
11.2.3 Creating policy distribution definition files.....	190
11.2.4 Creating connection destination definition files.....	191
11.2.5 Policy Distribution.....	192
11.2.6 Creating and applying policies remotely.....	193
11.3 Supplementary Notes.....	194
11.3.1 How to check which servers policies can be distributed to.....	195
11.3.2 Changing the port number used by distribution destination server.....	195
Chapter 12 Backup and Restore.....	197
12.1 Operation Definitions.....	197
12.2 Backing Up and Restoring the Performance Database (PDB).....	198
12.2.1 PDB file.....	198
12.2.2 Archive files.....	199
Appendix A Setup Commands and Resident Processes.....	201
A.1 Server Resource Information Collection Policy Creation Command.....	201
A.2 Response/Operation Information Collection Policy Creation Command.....	203
A.3 sqcMdPolicy (Temporary Policy Change Command).....	205
A.4 How to Start and Stop Resident Processes.....	206
A.5 Starting the thttpd Service/Daemon Automatically.....	210
A.6 genpwd (password encryption command).....	211

Chapter 1 Linking to Other Products

This chapter explains the following procedures for managing the performance of middleware products:

- Checking the linked product (installation check)
- Definition method (customizing and setting up)
- Displaying performance information

Refer to Section 1.2.3, "Installation types corresponding to management types" in the *Technical Guide* for information about the relationship with supported installation types.

Before performing these procedures



Point

.....
To manage the performance of middleware on an Enterprise Manager, first make sure that the service/daemon has been stopped correctly. Then either modify "template.dat" or make sure that it has been modified already, by referring to "[9.6 Middleware Linkage Settings with Enterprise Manager](#)".
.....

The following sections explain the settings for middleware performance management.

- [1.1 Linking to Interstage Application Server](#)
- [1.2 Linking to Symfoware Server](#)
- [1.3 Linking to Oracle Database Server](#)
- [1.4 Linking to Systemwalker Centric Manager](#)
- [1.5 Linkage with Systemwalker Operation Manager](#)
- [1.6 Linking to Systemwalker Network Manager](#)
- [1.7 Linking to Systemwalker Resource Coordinator \(Server Provisioning\)](#)
- [1.8 Linking to Systemwalker Resource Coordinator \(Network Resource Manager\)](#)
- [1.9 Linking to Systemwalker Resource Coordinator \(Storage Resource Manager\)/ETERNUS SF Storage Cruiser](#)
- [1.10 Linking to Microsoft SQL Server](#)
- [1.11 Linking to Microsoft .NET](#)
- [1.12 Linking to SAP NetWeaver](#)
- [1.13 Linkage with Hyper-V](#)
- [1.14 Linkage with the Red Hat Virtualization Function \(Xen\)](#)

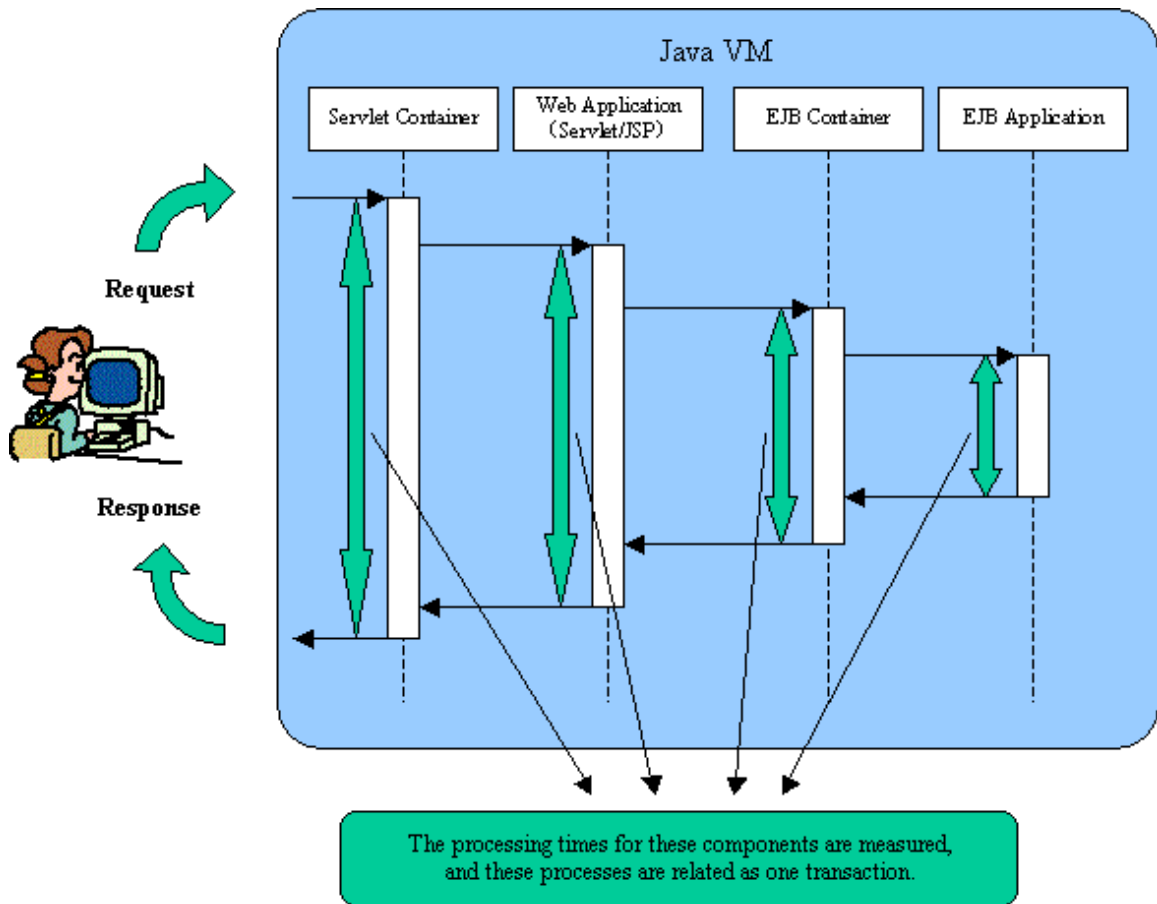
1.1 Linking to Interstage Application Server

Function overview

Systemwalker Service Quality Coordinator can be used to analyze the performance of business applications running on Interstage Application Server, analyzing things such as the size of the Java heap, the status of connections, and processing time. This makes it possible to create easy-to-understand reports according to various objectives, and also makes it possible to track the operational status of the system and various other trends.

If IJServer Work Units are monitored, the processing times for each component of J2EE applications can be measured.

This enables breakdown performance analysis for transactions in J2EE applications, which makes it easier to detect bottlenecks.



 See

Refer to the Interstage Application Server manuals for more information.

Collection interval

The collection interval is 5 minutes.

Procedure

The procedure for linking to Interstage Application Server is as follows:

- [1.1.1 Installation check](#)
- [1.1.2 Transaction breakdown analysis](#)
- [1.1.3 Definition method](#)
- [1.1.4 Setup](#)
- [1.1.5 Display](#)

1.1.1 Installation check

Execution environment

Service Quality Coordinator can be linked to Interstage Application Server by installing this product's Agent in an environment where the application server function for Interstage Application Server has been installed.

Refer to Section 1.2.3, "Installation types corresponding to management types" in the *Technical Guide* for information about the relationship with supported installation types.

Tasks to perform on the Interstage Application Server side

Before creating and applying collection policies, the following preparations and checks are required on the Interstage Application Server side.



Service Quality Coordinator does not support Interstage Application Server's multi-system function.

- To manage the performance of EJB, TD and CORBA Work Units, a monitoring environment for performance analysis must be created (error messages must not be displayed when the `ispstatus` command is executed). (It is not required when managing the performance of IJServer Work Units.)

Note 1: Refer to the Interstage Application Server manuals for information about how to create a monitoring environment for performance analysis.

Note 2: Set the collection interval to 5 minutes.

- Each Interstage service/daemon must be running.
- If "transaction breakdown analysis" is performed for IJServer Work Units, the settings described in "[1.1.2 Transaction breakdown analysis](#)" must be made.

1.1.2 Transaction breakdown analysis

If "transaction breakdown analysis" is performed for IJServer Work Units, make the following settings from the Interstage Management Console.

- Enable transaction breakdown analysis
- Specify the sampling frequency (measurement interval)

When transaction breakdown analysis measurements are made, only some data is sampled, because collecting information for all transactions that are running would increase the overheads for the system.

The default sampling frequency is 0.1%. In other words, data is collected for one transaction out of every 1,000 transactions. This sampling frequency can be changed using the "measurement interval" Interstage operating parameter.

Usually, Fujitsu recommends operating with the default value of 1000. Change the frequency only when there are very few transactions and very little transaction breakdown analysis data can be collected. The default value (1000) assumes a load of about 10 transactions per second. When changing the default value, change the value so that information is collected about once every 100 seconds.

If the measurement interval is too short, the overheads on the system will increase. Once the load increases beyond a certain point (that is, once an internal buffer fills up), data collection is temporarily suspended in order to prevent the load from increasing any further. As a result, there will be gaps in the transaction breakdown analysis data. If this happens, there will be gaps in the sequence of transaction IDs, which are normally numbered in ascending order. This can be checked by displaying collection data in the Drilled-Down view.

Refer to Section 3.2.4.3, "Interstage(TxnAnalysis) tree" in the *User's Guide (Console Edition)* for more information about transaction IDs.

If gaps are found in the sequence of transaction IDs, this means that the measurement interval is too short, so review the settings.



Refer to the Interstage Application Server manual for more information about how to make these settings.

1.1.3 Definition method

With the default settings, the records that can be collected for IJServer Work Units are as follows:

- IS_JMX_JVM
- IS_JMX_JTARESOURCE
- IS_JMX_JDBCRESOURCE

By implementing the definition procedure below, the following records can also be collected:

- IS_JMX_SERVLET
- IS_JMX_ENTITYBEAN_METHOD
- IS_JMX_ENTBEAN_POOL_AND_PASSIVATE
- IS_JMX_STFBEAN_METHOD
- IS_JMX_STFBEAN_INS_AND_IDLE
- IS_JMX_STLSBEAN_METHOD
- IS_JMX_MESSBEAN_METHOD
- IS_JMX_MESSBEAN_INFO



If the items that are collected by default meet the requirements for the operation, there is no need to implement the procedure in this section.



Some records cannot be collected, depending on the application running on the IJServer Work Unit.

The number of records that can be collected increases as a result of implementing this definition procedure, so collection processing may not be able to complete within the collection interval (because there are too many monitored objects, for example) and errors may occur.

Procedure for extending performance information collection for IJServer

Modify the "template.dat" file.

Definition location

[Windows]

```
<Variable file storage directory>\control\template.dat
```

[UNIX]

```
/etc/opt/FJSVssqc/template.dat
```

Content to be modified

Add the line "LEVEL=2" after the "ARMTXN=..." line in the INTSG section, as shown below.

```
#####  
## Interstage ispreport DCA_CMD  
[INTSG]  
DCAID="INTSGREPO"  
AUTOFLAG="ON"  
INTERVAL=5  
TDOBJ="ON"  
EJBAPL="ON"  
IMPLID="ON"  
IJSERVER="ON"  
ARMTXN="ON"  
LEVEL=2 *Add this line.  
#####
```

1.1.4 Setup

Execute the sqcRPolicy and sqcSetPolicy commands by referring to "[A.1 Server Resource Information Collection Policy Creation Command](#)".

If the configuration is subsequently changed by adding or deleting Work Units, the collection policy must be created and applied again.

Any collection policies that have been set up must be reflected to the Console. Use the Agent Setup window to get configuration information by referring to Section 1.2.2.3, "Agents" in the *User's Guide (Console Edition)*.

1.1.5 Display

Transaction breakdown analysis information can be displayed using the following method.

Summary

The Monitor can be displayed by selecting one of the following nodes from the Summary Tree: "Interstage(EJB)" node (Interstage(EJB)Monitor), the "Interstage(TD)" node (Interstage(TD)Monitor), the "Interstage(CORBA)" node (Interstage(CORBA)Monitor) or the "Interstage(IJServer)" node (Interstage(IJServer)Monitor).

Drilled-Down

A separate node for each Work Unit is generated under the "Interstage (TxnAnalysis)" node in the Detailed tree. Selecting a Work Unit displays all of the transactions that have been executed by that Work Unit. By setting up transaction ID nodes, information can be displayed for each individual transaction. Refer to Section 3.2.4.3, "Interstage (TxnAnalysis) tree" in the *User's Guide (Console Edition)* for more information.

Report

Full system inspection analysis/report

Categorized diagnostic analysis/report

Detailed analysis/report

1.2 Linking to Symfoware Server

Function overview

Bottlenecks can be made visible by monitoring the operational status of the database server using Systemwalker Service Quality Coordinator.

Collection interval

The collection interval is 5 minutes.

Procedure

The procedure for linking to Symfoware Server is explained in the following sections:

- [1.2.1 Installation check](#)
- [1.2.2 Definition method](#)
- [1.2.3 Setup](#)
- [1.2.4 Display](#)
- [1.2.5 Stopping Symfoware Server where a Service Quality Coordinator Agent has been installed](#)
- [1.2.6 If performance information for Symfoware is not collected](#)



.....

This linkage function collects performance information by periodically executing rdbsar or a similar Symfoware Server RDB command.

Thus, if other applications or RDB commands are executed while this function is operating, Symfoware/RDB exclusion control might cause a resource exclusive possession error for one or the other, and might cause a wait until the exclusive possession of the resource is released.

Refer to the Symfoware Server manuals for details.

Refer to Section 4.1.14, "SymfowareMonitor", and Section 4.2.12, "The Symfoware folder / Symfoware reports", in the Reference Guide for information about the RDB commands executed periodically by this linkage function.

.....

1.2.1 Installation check

Execution environment

Systemwalker Service Quality Coordinator can be linked to Symfoware Server by installing a Service Quality Coordinator Agent on a server where Symfoware Server exists.

Refer to Section 1.2.3, "Installation types corresponding to management types" in the *Technical Guide* for information about the relationship with supported installation types.

Tasks to perform on the Symfoware Server side

Before creating and applying collection policies, the following preparations and checks are required on the Symfoware Server side.

- Each of the following commands for displaying performance information (rdb sar, rdb ps, rdb spcinf and rdb inf) must be available. (That is, the RDB system must be running.)



See

.....
Refer to the *Symfoware Server RDB Administrator's Guide* for more information.
.....



Note

.....
An error message (such as qdg13315u) may be output if collection policies are created when a default RDB system for Symfoware Server does not exist.

These error messages are output in order to check the configuration of the RDB system. There is no problem if the creation and application of the collection policies has terminated normally.
.....

1.2.2 Definition method

If this linkage function is used, the following items are collected by default:

- RDBSAR_EB
- RDBSAR_ED
- RDBSAR_EM
- RDBSAR_AGE
- RDBSAR_EL
- RDBPS_S
- RDBPS_R

By implementing this definition procedure, the following items can be collected.

- RDBSAR_ER
- RDBSAR_EC
- RDBPS_IA
- RDBINF_AI
- RDBINF_AP
- RDBSPCINF_PD



Point

.....
If the items that are collected by default meet the requirements for the operation, there is no need to implement the procedure in this section.
.....

Procedure 1

Modify the "template.dat" file.

Definition location

[Windows]

```
< Variable file storage directory>\control\template.dat
```

[UNIX]

```
/etc/opt/FJSVssqc/template.dat
```

Modifications

Collecting RDBSAR_ER/RDBSAR_EC

In the SYMSAR section, perform the following tasks:

- Set the "DSIBUF" option to "ON" to enable collection for RDBSAR_ER.
- Set the "RDBCOM" option to "ON" to enable collection for RDBSAR_EC.

Extract from the SYMSAR section

```
#####  
## Symfoware RDBSAR DCA_CMD  
[SYMSAR]  
DCAID="SYMFOSAR"  
INTERVAL=5  
AUTOFLAG="ON"  
BUFPOOL="ON"  
DBSPIO="ON"  
TMPLOG="ON"  
ARCLOG="ON"  
MEMORY="ON"  
DSIBUF="OFF" *Set this option to "ON" to enable collection for RDBSAR_ER.  
RDBCOM="OFF" *Set this option to "ON" to enable collection for RDBSAR_EC.
```

Note

- RDBSAR_EC cannot be collected if the load share mechanism has not been enabled on the Symfoware side.
- Take care when enabling RDBSAR_ER collection, as this may place load on Symfoware depending on the environment or too much data may be collected. This may prevent data collection from completing within the collection interval, and data collection may not run correctly.

Collecting RDBPS_IA

In the SYMSAR section, perform the following task:

- Set the "DSISTATUS" option to "ON" to enable collection for RDBPS_IA.

Extract from the SYMPS section

```
#####
```

```
## Symfoware RDBPS DCA_CMD
[SYMPS]
DCAID="SYMFOPS"
INTERVAL=5
AUTOFLAG="ON"
SQLSTATUS="ON"
PRGSTATUS="ON"
DSISTATUS="OFF" *Set this option to "ON" to enable collection for RDBPS_IA.
```

 **Note**

- Take care when enabling RDBPS_IA collection, as this may place load on Symfoware depending on the environment or too much data may be collected. This may prevent data collection from completing within the collection interval, and data collection may not run correctly.

Collecting RDBINF_AI/RDBINF_AP

In the SYMINF section, perform the following tasks:

- Set the "SPCINFO" option to "ON" to enable collection for RDBINF_AP.
- Set the "DSIINFO" option "ON" to enable collection for RDBINF_AI.

Extract from the SYMINF section

```
#####
## Symfoware RDBINF DCA_CMD
[SYMINF]
DCAID="SYMFOINF"
AUTOFLAG="ON"
INTERVAL=5
SPCINFO="ON" *Set this option to "ON" to collect RDBINF_AP.
DSIINFO="ON" *Set this option to "ON" to collect RDBINF_AI.
```

Modify the ATTR::DB section.

Add the "SYMSPCINF" keyword to the GROUP parameter.

Extract from the ATTR::DB section.

```
[ATTR::DB]
GROUP="SYMSAR,SYMPS,ORA"
↓
GROUP="SYMSAR,SYMPS,ORA,SYMINF"
```

 **Note**

- To enable collection for RDBINF_AI/RDBINF_AP, the DSI names and database space names must also be specified in "Middlewareconf.xml" as monitored objects.
- If there are a large number of monitored objects, this may place load on Symfoware depending on the environment, or too much data may be collected. This may prevent data collection from completing within the collection interval, and data collection may not run correctly. As far as possible, try to limit the number of objects to be monitored.

Collecting RDBSPCINF_PD

In the SYMSPCINF section, perform the following tasks:

- Set the "SPCALL" option to "OFF" and the "SPCSEP" option to "ON" in order to enable collection for RDBSPCINF_PD.

Extract from the SYMSPCINF section

```
#####  
## Symfoware RDBSPCINF DCA_CMD  
[SYMSPCINF]  
DCAID="SYMFOCPCINF"  
INTERVAL=5  
AUTOFLAG="ON"  
SPCALL="ON" *Set this option to OFF.  
SPCSEP="OFF" *Set this option to ON.
```

Modify the ATTR::DB section.

Add the "SYMSPCINF" keyword to the GROUP parameter.

Extract from the ATTR::DB section

```
[ATTR::DB]  
GROUP="SYMSAR,SYMPS,ORA"  
  
↓  
GROUP="SYMSAR,SYMPS,ORA,SYMSPCINF"
```

 **Note**

To enable collection for RDBSPCINF_PD, the database space names must also be specified in "Middlewareconf.xml" as monitored objects.

Take care when enabling RDBSPCINF_PD collection, as this may place load on Symfoware depending on the environment or too much data may be collected. This may prevent data collection from completing within the collection interval, and data collection may not run correctly.

Procedure 2

Modify "MiddlewareConf.xml".

Definition location

[Windows]

```
< Variable file storage directory>\control\MiddlewareConf.xml
```

[UNIX]

```
/etc/opt/FJSVssqc/MiddlewareConf.xml
```



This file is created by executing the policy creation command.

Make sure that the Symfoware database to be monitored is detected when the policy creation command is executed, and then modify the "MiddlewareConf.xml" file.

Modifications

To collect RDBINF_AP/RDBINF_AI/RDBSPCINF_PD information, first make sure that there is a message indicating that Symfoware has been detected when the policy creation command is executed, and then specify the names of the databases, database spaces and DSIs to be monitored in this file.

Before modification

If Symfoware is detected when the policy creation command is executed, tags up to the <RDB_System> tag will be generated automatically in the file, as shown below.

```
<Symfoware DisplayName="Symfoware" InstanceName="" NodeType="F">
<SymfoEE DisplayName="" InstanceName="" NodeType=""/>
<RDB_System DisplayName="GYOMU" InstanceName="GYOMU" NodeType="I">
*Enter settings in here
</RDB_System>
</Symfoware>
```

* Make settings for the names of the databases, database spaces and DSIs to be monitored at the location indicated by the star (*).

Modification method

Enter information for the database for which information is to be collected inside the <RDB_System> tag (the line with the star symbol).

Syntax

```
<DB tag> #Required
<DB_Space tag> # Required
<DSI tag /> # Required if RDBINF_AI information is collected
</DB_Space tag>
</DB tag>
```

Modification example

```

<Symfoware DisplayName="Symfoware" InstanceName="" NodeType="F">
<SymfoEE DisplayName="" InstanceName="" NodeType=""/>
<RDB_System DisplayName="GYOMU" InstanceName="GYOMU" NodeType="I">
* <DB DisplayName="DB_A" InstanceName="DB_A" NodeType="I">
* <DB_Space DisplayName="DSPACE" InstanceName="DSPACE" NodeType="I">
* <DSI DisplayName="DSI1" InstanceName="DSI1" NodeType="I-D"/>
* <DSI DisplayName="DSI2" InstanceName="DSI2" NodeType="I-D"/>
* :
* :
* </DB_Space>
* </DB>
</RDB_System>
</Symfoware>

```

Note:

Enter the name of the database for the DisplayName and InstanceName attributes of the <DB> tag. Be sure to enter "I" for the "NodeType" attribute.

Enter the name of the database space for the DisplayName and InstanceName attributes of the <DB_Space> tag. Be sure to enter "I" for the "NodeType" attribute.

Enter the DSI names for the DisplayName and InstanceName attributes of the <DSI> tags. Be sure to enter "I-D" for the "NodeType" attribute.

1.2.3 Setup

Execute the `sqcRPolicy` and `sqcSetPolicy` commands by referring to "[A.1 Server Resource Information Collection Policy Creation Command](#)".

If the RDB system configuration for Symfoware Server is changed once collection policies have been set up, change the collection regime to match the system configuration for Symfoware Server by creating and applying collection policies again.

If collection policies are created and applied again, then the new policies must be reflected to the Console. Use the Agent Setup window to get configuration information by referring to Section 1.2.2.3, "Agents" in the *User's Guide (Console Edition)*.

Note

An error message (such as `qdg13315u`) may be output if collection policies are created when a default RDB system for Symfoware Server does not exist.

These error messages are output in order to check the configuration of the RDB system. There is no problem if the creation and application of the collection policies has terminated normally.

1.2.4 Display

Performance information for Symfoware Server can be displayed using the following method.

Summary

Performance information can be displayed by selecting the "Symfoware" node (SymfowareMonitor) in the Summary tree.

Drilled-Down

Performance information can be selected by selecting "Symfoware" in the Detailed tree.

Report

Full system inspection analysis/report

Categorized diagnostic analysis/report

Detailed analysis/report

Point

.....

If the Symfoware Server load sharing degrade function is enabled, the resource ID of the RDBSAR_EL record is displayed as "RDB system name: log group name".

.....

1.2.5 Stopping Symfoware Server where a Service Quality Coordinator Agent has been installed

For systems where Symfoware Server is being managed by Service Quality Coordinator, Symfoware Server cannot be stopped using the normal method. Stop Symfoware using either of the following methods:

- Stop Symfoware using the forced disconnection mode (redbsstop -mc). (This command can be used from Symfoware Server 9.0.)
- First stop the Service Quality Coordinator service, and then stop Symfoware Server.

Information

.....

Please follow the following steps when stopping the Service Quality Coordinator service first, and then stopping the Symfoware Server.

1. Stop the Service Quality Coordinator Agent
Stop the service/daemon by referring to "[A.4 How to Start and Stop Resident Processes](#)".
 2. Temporarily change policies
Change the policies by referring to "[A.3 sqcMdPolicy \(Temporary Policy Change Command\)](#)".
 3. Stop Symfoware Server
Execute the rdbstop command. (Refer to the Symfoware Server manuals for more information.)
-

1.2.6 If performance information for Symfoware is not collected

To make settings so that Service Quality Coordinator does not get performance information for Symfoware, implement the following procedure.

Note

.....

Implementing this procedure also disables performance information collection for Oracle and SQLServer.

.....

Definition location

[Windows]

```
<Variable file storage directory>\control\template.dat
```

Definition method

Edit the following key in the SERVERTYPE section. Do not change any other keys.

```
[SERVERTYPE]  
:  
DB="ON"  
:
```

Change this key as follows:

```
[SERVERTYPE]  
:  
DB="OFF"  
:
```

1.3 Linking to Oracle Database Server

Function overview

The operational status of various business activities can be tracked by monitoring thresholds for such information as the amount of free table space and the usage status of caches for database systems that have been created using Oracle Database Server.

Collection interval

The collection interval is 5 minutes.

Procedure

The following sections explain the procedure for linking to Oracle Database Server.

- [1.3.1 Installation check](#)
- [1.3.2 Definition Method](#)
- [1.3.3 Setup](#)
- [1.3.4 Display](#)

1.3.1 Installation check

Execution environment

Systemwalker Service Quality Coordinator can link to Oracle Database Server by installing a Service Quality Coordinator Agent on a server running Oracle Database Server.

Refer to Section 1.2.3, "Installation types corresponding to management types" in the *Technical Guide* for information about the relationship with supported installation types.

Tasks to perform on the Oracle Database Server side

Before creating and applying collection policies, the following preparations and checks are required on the Oracle Database Server side.

- Each Oracle service/daemon must be running.



Information

Refer to the Oracle manuals for more information.

1.3.2 Definition Method

Definition Procedure

1. Make settings on the Systemwalker Service Quality Coordinator side.
Definitions for getting Oracle performance information must be made in the collection template.
Refer to "[Chapter 9 Collection Template](#)" for more information about how to make these definitions.
2. Check and set up path information for Oracle.

[Windows]

Make sure that the path for Oracle has been set up in the PATH environment variable. The PATH environment variable should have been set up automatically when Oracle was installed, but the path for Oracle must be added to the PATH variable if it has not been set up already for some reason.

Refer to the Oracle manuals for more information.

[UNIX]

Make settings in the collection template.

Refer to "[9.1 How to Set up Oracle Database Server](#)" for more information.

If this linkage function is used, the following items are collected by default:

- ORA_IO
- ORA_QUEUE
- ORA_RETR
- ORA_TSS
- ORA_RC
- ORA_LC
- ORA_LT
- ORA_RBS

The definition procedure explained below allows the following items to also be collected:

- ORA_USR
- ORA_MEMORY
- ORA_TSF
- ORA_OSE
- ORA_DFS
- ORA_FS
- ORA_SEGS
- ORA_REDO
- ORA_WAIT
- ORA_FMEM

 **Point**

There is no need to perform the following procedure if the operating requirements can be met using the items that are collected by default.

Procedure for extending monitoring items

1. Stop Systemwalker Service Quality Coordinator if it is running on the target node.
2. Edit the "template.dat" file.

Definition location

[Windows]

<variable file storage directory>\control\template.dat

[UNIX]

/etc/opt/FJSVssqc/template.dat

Content to be modified

```

:
#####
# Oracle Information
[ORA]
DCAID="ORA"
INTERVAL=5
SID=""
USERNAME=""
PASS=""
VER="*.*.*"
ORAHOME=""
*Add here
#####

```

:

The following keys can be added:

Item name	Key
ORA_USR	USR="ON" or "OFF"
ORA_IO	IO="ON" or "OFF"
ORA_QUEUE	QUEUE="ON" or "OFF"
ORA_MEMORY	MEMORY="ON" or "OFF"
ORA_RETR	RETR="ON" or "OFF"
ORA_TSS	TSS="ON" or "OFF"
ORA_TSF	TSF="ON" or "OFF"
ORA_OSE	OSE="ON" or "OFF"
ORA_DFS	DFS="ON" or "OFF"
ORA_FS	FS="ON" or "OFF"
ORA_SEGS	SEGS="ON" or "OFF"
ORA_RC	RC="ON" or "OFF"
ORA_LC	LC="ON" or "OFF"
ORA_LT	LT="ON" or "OFF"
ORA_REDO	REDO="ON" or "OFF"
ORA_WAIT	WAIT="ON" or "OFF"
ORA_RBS	RBS="ON" or "OFF"
ORA_FMEM	FMEM="ON" or "OFF"

Add items, specifying "ON" for the keys for the items for which the item name is to be displayed in the Detailed tree of the Console, and specifying "OFF" for the keys for the items for which the item name does not need to be displayed.

3. Edit the Oracle Collection SQL Definition Source file.

Definition location

[Windows]

<variable file storage directory>\control\dsa_ora_all.sql
<variable file storage directory>\control\dsa_ora_<Oracle version>.sql

[UNIX]

/opt/FJSSvc/control/dsa_ora_all.sql
/opt/FJSSvc/control/dsa_ora_<Oracle version>.sql

Definition files

The "dsa_ora_all.sql" definition file contains definitions for the collection SQL statements that are common to all Oracle versions.

The "dsa_ora_<Oracle version>.sql" definition files contain definitions for the collection SQL statements that are specific to each version of Oracle.

This is because the SQL definition method for collecting ORA_IO varies depending on the version of Oracle.

The definition files that have been prepared already are listed below.

```
/etc/opt/FJSVssqc/control/dsa_ora_all.sql
```

[For V9]

```
/etc/opt/FJSVssqc/control/dsa_ora_v9.sql
```

[For V10 or later]

```
/etc/opt/FJSVssqc/control/dsa_ora_v10.sql
```

For each of these files, remove the comment identifier "--" for the processing corresponding to the items to be monitored.

The following example shows how to collect the "ORA_USR" item.

Definition example

[Before modification]

```
The monitoring item names are determined here. However, "ORA_QUEUE" is
replaced by "ORA QUE" and "ORA_MEMORY" is replaced by "ORA MEM".

↓

-- ORA_USR records %%%%%%%%%%
%%%%%%%%
-- TABLES NEED TO BE READ: V$SYSSTAT
-- The following data collection parameter set repo
-- the database.
--
-- [0300] COLUMN
-- (PKEY, INTERVAL, SAMPLE, INTERVAL, SAMPLE, IN
-- DELIM=",";
* -- PROMPT dsa_oracle_data_start 300 column 7 interva
* -- SELECT VALUE SYSSTAT
* -- FROM V$SYSSTAT
* -- WHERE NAME IN ('logons cumulative'
* -- ,'logons current'
* -- ,'opened cursors cumulative'
* -- ,'opened cursors current'
* -- ,'user calls'
* -- ,'user commits'
* -- ,'user rollbacks'
* -- )
```

```
* -- ORDER BY NAME;
```

Delete the "--" from within the scope of the SQL statement, starting from the "PROMPT" line (the lines indicated by *). Be careful not to delete the "--" in the header information.

[After modification]

The monitoring item names are determined here. However, "ORA_QUEUE" is replaced by "ORA QUE" and "ORA_MEMORY" is replaced by "ORA MEM".



```
-- ORA USR records %%%%%%%%%%  
%%%%%%%%  
-- TABLES NEED TO BE READ: V$SYSSTAT  
-- The following data collection parameter set repo  
-- the database.  
--  
-- [0300] COLUMN  
-- (PKEY, INTERVAL, SAMPLE, INTERVAL, SAMPLE, IN  
-- DELIM=",";  
* PROMPT dsa_oracle_data_start 300 column 7 interva  
* SELECT VALUE SYSSTAT  
* FROM V$SYSSTAT  
* WHERE NAME IN ('logons cumulative'  
* , 'logons current'  
* , 'opened cursors cumulative'  
* , 'opened cursors current'  
* , 'user calls'  
* , 'user commits'  
* , 'user rollbacks'  
* )  
* ORDER BY NAME;
```

Modify other monitoring items that need to be added in the same way.

1.3.3 Setup

1. Execute the sqcSetPolicy command.

Definition location

[Windows]

```
<Installation directory>\bin\sqcSetPolicy.exe [-h <host name>] [-p <IP address>]
```

[UNIX]

```
/opt/FJSVssqc/bin/sqcSetPolicy.sh [-h <host name>] [-p <IP address>]
```

Refer to Section 1.1.3, "sqcSetPolicy(Policy Application Command)" in the Reference Guide for details.

 **Note**

If the Policy Creation Command (sqcRPolicy) has never been executed before, execute the Policy Creation Command (sqcRPolicy) before performing this procedure.

Definition location

[Windows]

```
<Installation directory>\bin\sqcRPolicy.exe
```

[UNIX]

```
/opt/FJSVssqc/bin/sqcRPolicy.sh
```

Executing the sqcSetPolicy command creates a collection definition file based on the Oracle collection SQL definition source file.

Definition location

[Windows]

```
< Variable file storage directory>\control\<Section name>_all_sel.sql
```

```
< Variable file storage directory>\control\<Section name>_<Oracle version>_sel.sql
```

[UNIX]

```
/etc/FJSVssqc/<Section name>_all_sel.sql
```

```
/etc/opt/FJSVssqc/<Section name>_<Oracle version>_sel.sql
```

Definition files

<Section name> : This part of the file name will be set to the Oracle collection section name defined by "template.dat".

<Oracle version> : This part of the file name will be set to the Oracle version name defined by "template.dat".

The "*<Section name>*_all_sel.sql" definition file contains definitions for the collection SQL statements that are common to all Oracle versions.

Note: These names are based on "dsa_ora_all.sql".

The "*<section name>*_<Oracle version>_sel.sql" definition files contain definitions for the collection SQL statements that are specific to each version of Oracle.

Note: This file is based on "dsa_ora_<Oracle version>.sql".

[Definition example]

```
/etc/opt/FJSVssqc/control/ORA_all_sel.sql
```

```
/etc/opt/FJSVssqc/control/ORA_v9_sel.sql
```

Point

.....
If multiple instances are being monitored (that is, if multiple Oracle collection definition sections have been added to "template.dat"), a definition file will be generated for each monitored instance.
.....

2. Start Systemwalker Service Quality Coordinator.

After about five minutes have elapsed (or ten minutes, if "pull" operations are being used), get configuration information from the Admin Console.

Note

.....
Depending on the environment, collection may not complete before the collection interval elapses if there is a large amount of performance data. In this case, it is necessary to make adjustments, such as reducing the number of items so that collection can complete within the collection interval.
.....

If the Oracle instances being monitored are modified after the collection policy has been created and applied, repeat the procedure in this section again.

Note also that if the collection policy is set up more than once, the new policy will need to be reflected to the Console. Get configuration information using the Agent Settings window by referring to Section 1.2.2.3, "Agents" in the *User's Guide (Console Edition)*.

1.3.4 Display

Performance information for Oracle Database Server can be displayed using the following method.

Summary

Performance information can be displayed by selecting the "Oracle" node (OracleMonitor) in the Summary tree.

Drilled-Down

Performance information can be displayed by selecting "Oracle" in the Detailed tree.

Report

Full system inspection analysis/report

Categorized diagnostic analysis/report

Detailed analysis/report

1.4 Linking to Systemwalker Centric Manager

Function overview

The following functions are provided to allow linkage to Systemwalker Centric Manager.

- Threshold monitoring
- Invoking the **Summary** view

- Storing performance information (traffic information) in the PDB

Threshold monitoring

When a threshold violation is detected by threshold monitoring, a notification can be displayed in the Systemwalker Centric Manager Monitor view indicating that an error has occurred with the node in question (by making the node icon flash on and off, for example).

Invoking the Summary view

The **Summary** view for Service Quality Coordinator can be invoked from the Systemwalker Centric Manager Monitor view.

Storing performance information (traffic information) in the PDB

By getting the output results (traffic information) for the F3crTrfBcsv Performance Information CSV Output Command from the Systemwalker Centric Manager Section Management Server or Operation Management Server, and then storing this CSV output file in the PDB, reports of traffic information can be output from the Report view of Service Quality Coordinator.

Procedure

The following sections explain the procedure for linking to Systemwalker Centric Manager.

- [1.4.1 Installation check](#)
- [1.4.2 Threshold monitoring](#)
- [1.4.3 Linking to Invoke the Summary View](#)
- [1.4.4 Storing performance information \(traffic information\) in the PDB](#)

1.4.1 Installation check

Execution environment

Systemwalker Service Quality Coordinator can be linked to environments where Systemwalker Centric Manager has been installed.

Refer to Section 1.2.3, "Installation types corresponding to management types" in the *Technical Guide* for information about the relationship with supported installation types.

Tasks to perform on the Systemwalker Centric Manager side

Before creating and applying collection policies, the following preparations and checks are required on the Systemwalker Centric Manager side.

Using the threshold monitoring function

1. Register the "Performance monitoring" monitored event type.

The "Performance monitoring" monitored event type is registered by default. There is usually no need to register it explicitly. Use the procedure described in the following Systemwalker Centric Manager manual to register this type only if it has been deleted.

- Systemwalker Centric Manager User's Guide - Monitoring Functions

2. Register monitored events

Add the monitored event using Systemwalker Centric Manager's [Monitored Event Table] window and make a definition that allows performance monitoring to be performed on Systemwalker Service Quality Coordinator messages.

- The following conditions are used to identify Systemwalker Service Quality Coordinator messages:
"SSQC" is specified as the source name in the [Label Name] field of the [Event Definition] window, which is accessed via the [Monitored Event Table] window.
- The [Action Definition] setting used to perform performance monitoring is as follows:
[PerfMon] is selected as the monitored event type in the [Action Definition] window, which is accessed via the [Monitored Event Table] window.

Refer to the following manual for detailed information about Systemwalker Centric Manager's Monitored Event Table:

- Systemwalker Centric Manager User's Guide - Monitoring Functions

Invoking the summary view

No settings need to be made to enable the Monitor view to be invoked.

Storing performance information (traffic information) in the PDB

The performance monitoring function (monitoring network traffic information) must be enabled in advance. Set "60 minutes" as the "Performance information collection interval" for Systemwalker Centric Manager network performance.



.....
Refer to the Systemwalker Centric Manager manuals for more information.
.....

1.4.2 Threshold monitoring

If a threshold violation is detected by threshold monitoring, a notification can be displayed in the Systemwalker Centric Manager Monitor view indicating that an error has occurred with the node in question (by making the node icon flash on and off, for example).

For threshold monitoring of server resource information, the managed nodes recognized by the Systemwalker Centric Manager Monitor view match the managed objects for Service Quality Coordinator. However, for threshold monitoring of response and operational information, it is necessary to make decisions in advance about which node icons will flash on and off as a result of threshold violations.

Use the "AlertTarget" attribute of the various tags in the response and managed object configuration information file (ServiceConf.xml) to define which node icons should flash on and off. Refer to "[Chapter 6 Response and Managed Object Configuration Information \(ServiceConf.xml\)](#)" for more information about how to make these definitions.



.....
If "Event log/syslog" is selected at installation time as the notification method used when threshold violations occur, "CentricManager" must be defined as the type of alarm action to be executed. Refer to "[10.3 Alarm Action Definitions](#)" for more information about how to make these definitions.
.....

1.4.3 Linking to Invoke the Summary View

To invoke the Summary view of this product from the Monitor view of Systemwalker Centric Manager, the Summary view of this product must be registered as a menu item in the Monitor view of Systemwalker Centric Manager. Refer to Section 3.3.1, "Invoking the Summary View" in the *User's Guide (Console Edition)* for information about how to invoke the Summary view.

1.4.4 Storing performance information (traffic information) in the PDB

By getting the output results (traffic information) for the F3crTrfBcsv Performance Information CSV Output Command from the Systemwalker Centric Manager Section Management Server or Operation Management Server, and then storing this CSV output file in the PDB, reports of traffic information can be output from the Report view of Service Quality Coordinator.



.....

If traffic information is stored in the PDB, set "60 minutes" as the "Performance information collection interval" for Systemwalker Centric Manager network performance.

.....



.....

This type of linkage involves passing files, so a Service Quality Coordinator Agent does not necessarily have to be placed on the same host as Systemwalker Centric Manager.

.....

The procedure is explained in the following section.

1.4.4.1 Definition method

To store traffic information in the PDB, start by preparing the following file.

Definition location

The definition file is a text file. Use a text editor, such as Notepad, to create and edit this file. The path to the file is as follows:

[Windows]

```
< Variable file storage directory > \control\cntrconf.ini
```

[UNIX]

```
/etc/opt/FJSVssqc/cntrconf.ini
```

Format

```
[MIDDLEWARE_CONF]
XML=ON | OFF
```

Explanation

[MIDDLEWARE_CONF]

This item defines whether to manage traffic information.

XML=ON | OFF

The following table shows the options and their meanings. The default value is "OFF".

Option	Meaning
ON	Manage traffic information.
OFF	Do not manage traffic information.

1.4.4.2 Setup

Execute the `sqcRPolicy` and `sqcSetPolicy` commands by referring to "[A.1 Server Resource Information Collection Policy Creation Command](#)".

Any collection policies that have been set up must be reflected to the Console. Use the Agent Setup window to get configuration information by referring to Section 1.2.2.3, "Agents" in the *User's Guide (Console Edition)*.

1.4.4.3 Storing traffic information in the PDB

Use the `sqcPDBcloud` command to store traffic information in the PDB.

Path

[Windows]

```
<Installation directory>\bin
```

[UNIX]

```
/opt/FJSVssqc/bin
```

Syntax

```
sqcPDBcloud -c trafficdata-file
```

Option

-c trafficdata-file

Specify the traffic data file (a CSV file) to be stored in the PDB. The traffic data file contains the output results of the `F3crTrfBcsv Performance Information CSV Output Command`.

Usage example

[Windows/UNIX]

```
> sqcPDBcloud -c traffic.csv
```

1.4.4.4 Display

Traffic information can be displayed using the following method.

Report

Categorized diagnostic analysis/report

Detailed analysis/report



Only "One hour" can be used for the "Data interval". Traffic information will not be displayed if other units are specified.

1.5 Linkage with Systemwalker Operation Manager

Function overview

Linkage with Systemwalker Operation Manager makes it possible to visualize and analyze the correlation between the execution status of batch jobs and the load status of batch servers and database servers.

Collection interval

The collection interval is 5 minutes.

Procedure

The linkage procedure is explained in the following sections:

- [1.5.1 Installation check](#)
- [1.5.2 Definition method](#)
- [1.5.3 Setup](#)
- [1.5.4 Displaying performance information](#)

1.5.1 Installation check

Execution environment

Service Quality Coordinator can be linked to Systemwalker Operation Manager by installing a Systemwalker Service Quality Coordinator Agent on a Systemwalker Operation Manager server.

Refer to Section 1.2.3, "Installation types corresponding to management types" in the *Technical Guide* for information about the relationship with supported installation types.

Tasks to perform on the Systemwalker Operation Manager side

Before creating and applying collection policies, the following preparations and checks are required on the Systemwalker Operation Manager side.

1. Systemwalker Operation Manager must be installed.

2. The Systemwalker Operation Manager environment must be set up.
3. The settings must be made so that the operation results information file is saved when the environment is set up.
4. If the number of jobs that exceed the estimated execution time is to be analyzed, **Notify when job is not terminated even after the specified time is lapsed** must be specified in the **Event output** settings of the Jobscheduler startup parameters when the environment is set up.
5. All the Systemwalker Operation Manager services or daemons must be running.

Note, however, that if only the specific subsystems, queues and projects described are to be analyzed, there is no need for the Systemwalker Operation Manager services or daemons to be running.



If a queue is added, changed or deleted, or if the storage location of the operation results information file is changed, restart the Systemwalker Operation Manager services or daemons in initialized mode to enable the new settings.

Refer to the Systemwalker Operation Manager manuals for more information.

1.5.2 Definition method

If only specific Systemwalker Operation Manager subsystems, queues and projects are to be analyzed or under a cluster system, prepare the definition file referred to below.

Also prepare this definition file if Systemwalker Operation Manager is not running at the moment but will be running at some time in the future.



By using this definition file to restrict the subsystems, projects and queues that will be analyzed, the amount of data stored in the PDB can be kept down and the load on the management server can also be reduced.



- If this definition file is set up, data that is not related to the subsystems, queues and projects that have been specified will not be stored in the PDB.
- If this definition file is not set up, all the subsystems, queues and projects specified by Systemwalker Operation Manager will be subject to analysis.

For this reason there is no need to set up this definition file if the subsystems, queues and projects are not to be filtered in any way.

This definition file does not exist at installation time.

- If a server is subject to monitoring but is not running for some reason (Systemwalker Operation Manager is stopped or on standby, etc.), it will not be possible to obtain information about subsystem names, project names and queue names, and this definition file should be set up.

If it is not set up, it will not be possible to collect correct data when Systemwalker Operation Manager restarts.

Definition location

The definition file is a text file. Use a text editor, such as Notepad, to create and edit this file. The path to the file is as follows:

[Windows]

```
<Variable file storage directory>\control\jla.ini
```

[UNIX]

```
/opt/FJSVssqc/control/jla.ini
```

Format

```
[subsystem]
subsystem = LL
[project]
subsystemMM = project_name
[queue]
subsystemNN = queue_name
```

Explanation

[subsystem]

This section indicates the start of the definition block of a subsystem that will be subject to collection.

Use the following definition statement to specify the target subsystem:

```
subsystem = LL
```

LL: A two-digit integer between 00 and 09. It specifies the number of a target subsystem.

Note

- Systemwalker Service Quality Coordinator sets subsystems, queues and projects as resource IDs so that resource IDs can be filtered in the Report view according to the first matching part of the resource ID. To ensure that subsystem numbers are unique, they are represented using a two-digit integer. If Systemwalker Operation Manager subsystems use one-digit numbers, add a zero to the beginning of each number and read them as two-digit numbers.

Example: Change "2" to "02"

- To specify more than one subsystem, enter the relevant settings on multiple lines.
- Lines that do not have the "LL" component are ignored.
- If there are no definition statements in this block and this section is omitted, all subsystems will be analyzed.

[project]

Indicates the beginning of a definition block of the target project. It also indicates the end of the previous definition block.

Projects to be analyzed are specified using the following definition statement:

```
subsystemMM = project_name
```

MM: Here, 00 to 99 is a two-digit integer that specifies the subsystem number of the target project.

project_name: Specifies the name of a single target project.

Note

- Multiple projects and subsystems can be specified in the same way over multiple lines.
- Lines that do not have a project_name component are ignored.
- For subsystems that are not specified within the [project] section, all projects within those subsystems will be subject to analysis.
- No problems will arise if the same specification is entered more than once.
- This block can be omitted if there are no definition statements contained within it.
- If characters that are not permitted by Systemwalker Service Quality Coordinator (\ : < > " , \$ ' [] & =) are used as part of a project name, those characters will be converted to hexadecimal format before being displayed, as follows:

```
"|hexadecimal code of forbidden character|"
```

Example

```
"&" -> "|26|"
```

[queue]

Indicates the beginning of a definition block of the target queue. It also indicates the end of the previous definition block.

Queues to be analyzed are specified using the following definition statement:

```
subsystemNN = queue_name
```

NN: Here, 00 to 99 is a two-digit integer that specifies the subsystem number of the target queue.

queue_name: Specifies the name of a single target queue.

Note

- Multiple queues and subsystems can be specified in the same way over multiple lines
 - Lines that do not have a queue_name component are ignored.
 - For subsystems that are not specified within the [queue] section, all queues within those subsystems will be subject to analysis.
 - No problems will arise if the same specification is entered more than once.
 - This block can be omitted if there are no definition statements contained within it.
-
- [subsystem], [project] and [queue] blocks can be specified in any order.
 - Lines that begin with a hash character (#) are treated as comments and ignored.

Sample definition

The following is an example of a definition:

```
[subsystem]  
subsystem = 00
```

```
subsystem = 01
[project]
subsystem00 = eigyo
subsystem00 = keiri
subsystem01 = soumu
[queue]
subsystem00 = queue0
subsystem00 = queue1
subsystem01 = queue0
subsystem01 = queue1
```

Performing cluster system operation

- In the case of an active/standby server configuration:
 - Use the same settings in the definition file on both the active and standby servers.
- In the case of a mutual standby server configuration:
 - Set up definition files that contain the subsystems, projects and queues that are to be analyzed on both servers.
 - The same settings should be specified in both definition files.

1.5.3 Setup



Before setting up collection policies, check that the Systemwalker Operation Manager services or daemons are running. However, note that there is no need for the Systemwalker Operation Manager services or daemons to be running if a definition file (jla.ini) has been set up.

Note that if the objects to be analyzed are not specified in the definition file (jla.ini) before a collection policy is set up, analysis will take place as follows:

- If subsystems to be analyzed are not specified in the definition file (jla.ini), only the subsystems that are operating when the collection policy is created will be analyzed.
- If projects to be analyzed are not specified in the definition file (jla.ini), only the projects that are registered when the collection policy is created will be analyzed.
- If queues to be analyzed are not specified in the definition file (jla.ini), only queues that are specified in the Systemwalker Operation Manager initialization file (Job Execution Control) when the collection policy is created will be analyzed.

Execute the sqcRPolicy and sqcSetPolicy commands by referring to "[A.1 Server Resource Information Collection Policy Creation Command](#)".

If subsystems, queues or projects are added or deleted after collection policies have been set up, change the collection regime to match the system configuration for Systemwalker Operation Manager by creating and applying collection policies again.

After collection policies are created and applied, the changes must be reflected to the Console. Use the Agent Setup window to get configuration information by referring to Section 1.2.2.3, "Agents" in the *User's Guide (Console Edition)*.

1.5.4 Displaying performance information

The following methods can be used to display Systemwalker Operation Manager performance information:

Summary

Performance information can be displayed by selecting the "Operation Manager" node (OperationMgrMonitor) in the Summary tree.

Drilled-Down

Performance information can be displayed by selecting the "OperationMGR" node in the Detailed tree.

Report

Full system inspection analysis/report

Categorized diagnostic analysis/report

Detailed analysis/report

1.6 Linking to Systemwalker Network Manager

Function overview

A Systemwalker Network Manager operation management server can use the function to link reports with Service Quality Coordinator to output Systemwalker Network Manager log data from Service Quality Coordinator's Report view and to analyze TCP communications between servers and the status of network devices.

By using the function to link reports with Service Quality Coordinator from a Systemwalker Network Manager operation management server, it becomes possible to analyze TCP communications between servers and the status of network devices.

Procedure

The linkage procedure is explained in the following sections:

- [1.6.1 Installation check](#)
- [1.6.2 Definition method](#)
- [1.6.3 Setup](#)
- [1.6.4 Display](#)

1.6.1 Installation check

Execution environment

Systemwalker Service Quality Coordinator can be linked to Systemwalker Network Manager by installing a Service Quality Coordinator agent on a Systemwalker Network Manager operation management server.

Refer to Section 1.2.3, "Installation types corresponding to management types" in the *Technical Guide* for information about the relationship with supported installation types.



Information

Refer to the Systemwalker Network Manager manual for details.

Tasks to perform on the Systemwalker Network Manager side

Log data can be stored in the PDB automatically by using the function to link reports with Service Quality Coordinator to conduct a statistical monitoring schedule on a Systemwalker Network Manager operation management server.

1.6.2 Definition method

To display log data using Service Quality Coordinator, it is necessary to prepare the definition file shown below.

Definition location

The definition file is a text file. Use a text editor, such as Notepad, to create and edit this file. The path to the file is as follows:

[UNIX]

```
/etc/opt/FJSVssqc/snmconf.ini
```

Format

```
[MIDDLEWARE_CONF]
XML=ON | OFF
```

Explanation

[MIDDLEWARE_CONF]

This item specifies whether to manage log data.

XML=ON | OFF

The meaning of each option is shown in the following table. The setting is set to OFF by default.

Selection	Meaning
ON	Manage log data.
OFF	Do not manage log data.

1.6.3 Setup

Execute the sqcRPolicy and sqcSetPolicy commands by referring to "[A.1 Server Resource Information Collection Policy Creation Command](#)".

After collection policies are created and applied, the changes must be reflected to the Console. Use the Agent Setup window to get configuration information by referring to Section 1.2.2.3, "Agents" in the *User's Guide (Console Edition)*.

1.6.4 Display

The following methods can be used to display log data:

Report

Categorized diagnostic analysis/report

Detailed analysis/report



Only "One hour" and "One day" can be used for the "Data interval". Log data will not be displayed if other units are specified. (Only "One day" can be used for IP operation monitoring.)

1.7 Linking to Systemwalker Resource Coordinator (Server Provisioning)

Function overview

Systemwalker Service Quality Coordinator is one of the software products that can be set up automatically by linking to server resource allocation operation (the delivery of software images to managed servers) using Systemwalker Resource Coordinator's server provisioning function.

It supports provisioning by optimizing the allocation of server resources used by applications as needed and ensuring that system resources are used effectively.

Procedure

The linkage procedure is explained in the following sections:

[1.7.1 Installation check](#)

[1.7.2 Manual registration method](#)

1.7.1 Installation check

Execution environment

Systemwalker Service Quality Coordinator can be linked to Systemwalker Resource Coordinator by installing a Service Quality Coordinator agent on a Systemwalker Resource Coordinator Agent (managed server).

Refer to Section 1.2.3, "Installation types corresponding to management types" in the *Technical Guide* for information about the relationship with supported installation types.

Tasks to perform on the Systemwalker Resource Coordinator side

When a server resource allocation operation is performed, the allocated server appears as an unregistered Agent in the information relating to unregistered agents (UnregisteredAgents) in the environment setting window.

This series of operations takes place as follows:

- When Service Quality Coordinator is installed, the setup content of Service Quality Coordinator is registered with Systemwalker Resource Coordinator.
- When Systemwalker Resource Coordinator allocates server resources, it sets up Service Quality Coordinator according to the registered content.

This occurs when the products are installed in the following order:

- Systemwalker Resource Coordinator Agent is installed
- Systemwalker Service Quality Coordinator Agent is installed

Note

Note that the setup content will not be registered if a Service Quality Coordinator Agent is installed first. In this case, register the settings manually by referring to "[1.7.2 Manual registration method](#)".

1.7.2 Manual registration method

Storage path

[Windows]

```
<Installation directory>\bin
```

[UNIX]

```
/opt/FJSVssqc/bin
```

Format

[Windows]

```
sqRCset.exe -c|-d
```

[UNIX]

```
sqRCset.sh -c|-d
```

Options

-c

Registers the setup content.

-d

Deletes the setup content.

S

1.8 Linking to Systemwalker Resource Coordinator (Network Resource Manager)

Note

This function is only available with Solaris versions of Service Quality Coordinator.

Function overview

This function enables the status of a network to be reported from Systemwalker Service Quality Coordinator by linking to Systemwalker Resource Coordinator's network monitoring function.

Collection interval

The collection interval is 5 minutes.

Procedure

The linkage procedure is explained in the following sections:

[1.8.1 Installation check](#)

[1.8.2 Setup](#)

[1.8.3 Display](#)

1.8.1 Installation check

Execution environment

Systemwalker Service Quality Coordinator can be linked to Systemwalker Resource Coordinator Agent (Network Resource Manager) by installing a Service Quality Coordinator Agent on a Systemwalker Resource Coordinator Agent (network resource manager).

Refer to Section 1.2.3, "Installation types corresponding to management types" in the *Technical Guide* for information about the relationship with supported installation types.

Tasks to perform on the Systemwalker Resource Coordinator side

Before creating and applying collection policies, the following preparations and checks are required on the Systemwalker Resource Coordinator side.

1. The "FJSVnetsr" package must be installed.
2. Network monitoring must be in a usable state.
3. The Systemwalker Resource Coordinator services or daemons must be running.



See

.....
Refer to the Systemwalker Resource Coordinator manuals for more information.
.....

1.8.2 Setup

Execute the `sqcRPolicy` and `sqcSetPolicy` commands by referring to "[A.1 Server Resource Information Collection Policy Creation Command](#)".

If the Systemwalker Resource Coordinator system configuration is modified after a collection policy has been created and applied once, create and apply the collection policy again to ensure that collection takes place in accordance with the new system configuration.

If collection policies are created and applied again, the changes must be reflected to the Console. Use the Agent Setup window to get configuration information by referring to Section 1.2.2.3, "Agents" in the *User's Guide (Console Edition)*.

1.8.3 Display

The following methods can be used to display Systemwalker Resource Coordinator (Network Resource Manager) performance information:

Summary

Performance information can be displayed by selecting the "Network" node (TcpNetworkMonitor) in the Summary tree.

Drilled-Down

Performance information can be displayed by selecting the "TcpNetwork" node in the Detailed tree.

Report

Full system inspection analysis/report

Categorized diagnostic analysis/report

Detailed analysis/report

1.9 Linking to Systemwalker Resource Coordinator (Storage Resource Manager)/ETERNUS SF Storage Cruiser

Function overview

Linking to Systemwalker Resource Coordinator's storage management function or ETERNUS SF Storage Cruiser enables Systemwalker Service Quality Coordinator to report the operational status of storage devices.

Collection interval

The collection interval is 5 minutes.

Procedure

The linkage procedure is explained in the following sections:

- [1.9.1 Installation check](#)
- [1.9.2 Setup](#)
- [1.9.3 Display](#)

1.9.1 Installation check

Execution environment

Systemwalker Service Quality Coordinator can be linked to Systemwalker Resource Coordinator (Storage Resource Manager) or ETERNUS SF Storage Cruiser by installing a Service Quality Coordinator Agent on a Systemwalker Resource Coordinator Manager (Storage Resource Manager) or ETERNUS SF Storage Cruiser Manager.

Refer to Section 1.2.3, "Installation types corresponding to management types" in the *Technical Guide* for information about the relationship with supported installation types.

Tasks to perform on the Systemwalker Resource Coordinator/ETERNUS SF Storage Cruiser side

Before creating and applying collection policies, the following preparations and checks are required on the Systemwalker Resource Coordinator or ETERNUS SF Storage Cruiser side.

1. Storage Resource Manager or ETERNUS SF Storage Cruiser must be installed.
2. The services or daemons of Storage Resource Manager or ETERNUS SF Storage Cruiser must be running.
3. Settings for collecting performance information must be in place.

Note

Set a value of 5 minutes or less as the monitoring interval.

See

Refer to the Systemwalker Resource Coordinator or ETERNUS SF Storage Cruiser manuals for more information.

1.9.2 Setup

Execute the `sqcRPolicy` and `sqcSetPolicy` commands by referring to "[A.1 Server Resource Information Collection Policy Creation Command](#)".

If the system configuration of Systemwalker Resource Coordinator or ETERNUS SF Storage Cruiser is modified after a collection policy has been created and applied once, create and apply the collection policy again to ensure that collection takes place in accordance with the new system configuration.

If collection policies are created and applied again, the changes must be reflected to the Console. Use the Agent Setup window to get configuration information by referring to Section 1.2.2.3, "Agents" in the *User's Guide (Console Edition)*.

Note

- Information relating to a RAIDGroup will not be collected in the following situations:
 - The RAIDGroup does not have a LogicalVolume allocated to it.
 - An MLU has been allocated to the RAIDGroup using E6000.
- Performance information on ROE is not collected for ETERNUS on which ROE (RAID Offload Engine) is not mounted.

1.9.3 Display

The following methods can be used to display Systemwalker Resource Coordinator (Storage Resource Manager) or ETERNUS SF Storage Cruiser performance information:

Summary

Performance information can be displayed by selecting the "Storage" node (StorageMonitor) in the Summary tree.

Drilled-Down

Performance information can be displayed by selecting the "StorageResource" node in the Detailed tree.

Report

Full system inspection analysis/report

Categorized diagnostic analysis/report

1.10 Linking to Microsoft SQL Server

Function overview

Bottlenecks can be expressed visually by using Systemwalker Service Quality Coordinator to monitor the operational status of a database server.

Collection interval

The collection interval is 1 minute.

Procedure

The linkage procedure is explained in the following sections:

- [1.10.1 Installation check](#)
- [1.10.2 Definition method](#)
- [1.10.3 Setup](#)
- [1.10.4 Display](#)

1.10.1 Installation check

Execution environment

Service Quality Coordinator can be linked to Microsoft SQL-Server by installing this product's Agent in an environment where Microsoft SQL-Server has been installed.

Refer to Section 1.2.3, "Installation types corresponding to management types" in the *Technical Guide* for information about the relationship with supported installation types.

Tasks to perform on the Microsoft SQL Server side

The following preparations and checks must be performed on the Microsoft SQL Server side:

1. Microsoft SQL Server must be installed.
2. The Microsoft SQL Server services or daemons must be running.

1.10.2 Definition method

The collection template must have a definition for obtaining Microsoft SQL Server performance information.

Definition location

template.dat is stored in the following location:

[Windows]

< Variable file storage directory>\control\template.dat

[UNIX]


```
/etc/opt/FJSVssqc/template.dat
```

Refer to "[9.3 How to Set Up Microsoft SQL Server](#)" for the definition method.



See

Refer to the Microsoft SQL Server manual for details.

1.10.3 Setup

Execute the `sqcRPolicy` and `sqcSetPolicy` commands by referring to "[A.1 Server Resource Information Collection Policy Creation Command](#)".

1.10.4 Display

The following methods can be used to display Microsoft SQL Server performance information:

Summary

Performance information can be displayed by selecting the "MS-SQL" node (MS-SQL_Monitor) in the Summary tree.

Drilled-Down

Performance information can be displayed by selecting the "MS-SQL" node in the Detailed tree.

Report

Full system inspection analysis/report

Categorized diagnostic analysis/report

Detailed analysis/report

1.11 Linking to Microsoft .NET

Function overview

This function makes it possible to monitor and report on the various resources that make up a .NET configuration.

Collection interval

The collection interval is 1 minute.

Procedure

The linkage procedure is explained in the following sections:

- [1.11.1 Installation check](#)
- [1.11.2 Definition method](#)
- [1.11.3 Setup](#)
- [1.11.4 Display](#)

1.11.1 Installation check

Execution environment

Systemwalker Service Quality Coordinator can be linked to Microsoft .NET by installing this product's Agent in an environment in which Microsoft .NET (IIS's ASP.NET and .NET Framework) has been installed.

Refer to Section 1.2.3, "Installation types corresponding to management types" in the *Technical Guide* for information about the relationship with supported installation types.

Tasks to perform on the Microsoft .NET side

Before creating and applying collection policies, the following preparations and checks are required on the Microsoft .NET side.

- The Microsoft .NET application must be running.

1.11.2 Definition method

The collection template must have a definition for obtaining Microsoft .NET performance information.

Definition location

template.dat is stored in the following location:

[Windows]

```
<Variable file storage directory>\control\template.dat
```

[UNIX]

```
/etc/opt/FJSVssqc/template.dat
```

Refer to "[9.2 How to Set Up Microsoft .NET Server](#)" for the definition method.

1.11.3 Setup

Create and apply a collection policy by referring to "[A.1 Server Resource Information Collection Policy Creation Command](#)".

1.11.4 Display

The following methods can be used to display Microsoft .NET performance information:

Summary

Performance information can be displayed by selecting the "MS-.NET" node (MS-.NET_Monitor) in the Summary tree.

Drilled-Down

Performance information can be displayed by selecting the "MS-.NET" node in the Detailed tree.

Report

Full system inspection analysis/report

Categorized diagnostic analysis/report

Detailed analysis/report

1.12 Linking to SAP NetWeaver

Function overview

Service Quality Coordinator can use the CCMS linkage interface provided by SAP NetWeaver to collect performance information.

By using Systemwalker Service Quality Coordinator to analyze the performance of business applications operating on SAP NetWeaver, it becomes possible to manage aspects of Quality of Service such as application server performance and the response and throughput of business applications.

Collection interval

The collection interval is 5 minutes.

Incompatible information

For V13.4.0 or later, define encrypted password to `PASSWORD` in the connection parameters definition file (`sqcGetSAPalertmon.ini`) for linking to SAP NetWeaver.

When upgrade installation from V13.3.0 or earlier has been done, encrypt the password defined in `PASSWORD` in the connection parameters definition file of SAP NetWeaver cooperation.

Refer to "[1.12.2.2 Connection parameters definition file](#)" for information about encryption method.

Procedure

The linkage procedure is explained in the following sections:

- [1.12.1 Installation check](#)
- [1.12.2 Definition method](#)
- [1.12.3 Setup](#)
- [1.12.4 Display](#)

1.12.1 Installation check

Definition environment

Systemwalker Service Quality Coordinator can be linked to SAP NetWeaver by installing this product's Agent in an environment in which SAP NetWeaver has been installed.

Refer to Section 1.2.3, "Installation types corresponding to management types" in the *Technical Guide* for information about the relationship with supported installation types.

Tasks to perform on the SAP NetWeaver side

Before creating and applying collection policies, the following preparations and checks are required on the SAP NetWeaver side.

- SAP NetWeaver's Alert Monitor function must be in a usable state.

1.12.2 Definition method

The following two definition files are necessary to collect performance information from SAP NetWeaver:

- [1.12.2.1 Connection destination system definition file](#)
- [1.12.2.2 Connection parameters definition file](#)

1.12.2.1 Connection destination system definition file

To connect to a SAP NetWeaver system, the connection destination system definition file "saprfc.ini" must be set up correctly.



Refer to the SAP NetWeaver documentation for details on the format of saprfc.ini.

Definition method

The definition file is a text file. Use a text editor, such as Notepad, to create and edit this file. The path to the file is as follows:

[Windows]

```
< Variable file storage directory>\control\saprfc.ini
```

[UNIX]

```
/etc/opt/FJSVssqc/saprfc.ini
```

Format

```
DEST=destination  
TYPE=A  
ASHOST=hostname  
SYSNR=system-number
```

Explanation

DEST=destination

Defines the name of the connection destination system definition.

The name defined here is referred to as the "connection destination system definition name". This name must be used in conjunction with the DEST definition statement in the connection parameters definition file, which is explained in the next section.

TYPE=A

Specifies the connection type. The type should always be specified as "A".



The Type A parameter is used when designating a specific application server as a monitored object. If a different type is specified, the monitoring function will not operate correctly.

ASHOST=hostname

Defines the host name of the SAP NetWeaver application server that will be monitored. Specify a name defined in the hosts file as the host name.

SYSNR=system-number

Defines the system number of the SAP NetWeaver application server that will be monitored. The system number must be a two-digit integer between 00 and 99.

Definition example

The following is an example of a definition:

```
DEST=BIN_HS0011
TYPE=A
ASHOST=HS0011
SYSNR=01
```

1.12.2.2 Connection parameters definition file

This definition file contains information such as the parameters that are needed for establishing a session with a SAP NetWeaver system.

Definition example

The definition file is a text file. Use a text editor, such as Notepad, to create and edit this file. The path to the file is as follows:

[Windows]

```
< Variable file storage directory >\control\sqcGetSAPalertmon.ini
```

[UNIX]

```
/etc/opt/FJSVssqc/sqcGetSAPalertmon.ini
```

Format

```
DEST=destination-name
CLIENT=signon-data-client
USER= signon-data-user
PASSWORD= signon-data-password
LANGUAGE= signon-data-language
```

Explanation

DEST=destination-name

Defines the name of the connection destination system definition.

Specify the name of the connection destination system definition defined in the DEST definition statement in the connection destination system definition file (saprfc.ini) explained in the previous section.

Note

Specify only one set of definitions following "DEST=". It is not possible to set up a definition for multiple application servers.

CLIENT=signon-data-client

Defines the client number that will be used when connecting to a SAP NetWeaver system.

The client number is additional information that is defined when a user is registered.

USER=signon-data-user

Defines the user name that will be used when connecting to a SAP NetWeaver system.

The specified user must possess the privileges shown in the following table:

Privileged object name	Privileges	Details
RFC access privilege check	S_RFC	Generic module groups require SYST, SXMI and SALX.
External management tool privilege	S_XMI_PROD	Set the privilege information as follows: <ul style="list-style-type: none">- COMPANY (Product company information for which the connection is approved) Set * or fujitsu- EXTPRODUCT (Product information for which the connection is approved) Set * or SW/SQC- INTERFACE (Category of interface for which the connection is approved) Set * or XAL

PASSWORD=signon-data-password

Defines the user password that will be used when connecting to a SAP NetWeaver system. Specify the password encrypted by genpwd(*) corresponding to the USER definition statement.

(*) Refer to "[A.6 genpwd \(password encryption command\)](#)" for more information about how to use genpwd (password encryption command).

LANGUAGE= signon-data-language

Defines the language of the log that is output when connecting to a SAP NetWeaver system. Any language that can be used when outputting a SAP NetWeaver system log can be specified here.

Typically Japanese, English or German is specified here. Specify "J" or "JA" for Japanese, "E" or "EN" for English and "D" or "DE" for German.

Definition example

The following is an example of a definition:

```
DEST=BIN_HS0011
CLIENT=100
USER=ssqc
```

```
PASSWORD=password
LANGUAGE=E
```

1.12.3 Setup

Execute the `sqcRPolicy` and `sqcSetPolicy` commands by referring to "[A.1 Server Resource Information Collection Policy Creation Command](#)".

If new collection policies are created and applied, they must be reflected to the Console. Use the Agent Setup window to get configuration information by referring to Section 1.2.2.3, "Agents" in the *User's Guide (Console Edition)*.

1.12.4 Display

The following methods can be used to display SAP NetWeaver performance information:

Summary

Performance information can be displayed by selecting the "SAP" node (SAP Monitor) in the Summary tree.

Drilled-Down

Performance information can be displayed by selecting the "SAP" node in the Detailed tree.

Report

- Full system inspection analysis/report
- Categorized diagnostic analysis/report
- Detailed analysis/report

1.13 Linkage with Hyper-V

Functional Overview

Physical server and virtual server performance information from Hyper-V is collected and managed centrally.

The virtual server performance information collected by this function is put together with the physical server performance information and evaluated comprehensively. Accordingly, the resources in the server can be optimized, and improved user efficiency can be achieved.

- The physical server performance information (physical server CPU, memory, and disk usage status) is displayed as a report.
- The virtual server performance information (guest CPU, memory, and disk usage status) accumulates in guest units and is displayed as a report.

Information that can be collected

The methods used to collect the physical server and virtual server performance information and the main function information for Hyper-V are shown below.

Physical Server	Virtual Server
CPU performance information is collected from Hyper-V.	CPU performance information is collected from Hyper-V.

Physical Server	Virtual Server
Memory/disk performance information is collected from the host operating system (Windows).	

Note

If Hyper-V is a monitoring target, then Windows performance information will also be collected from the host operating system.

However, the value for the CPU performance information obtained from the Hyper-V host operating system (Windows) will not be correct. To check the physical server CPU performance information, check the value for CPU performance information that was obtained from Hyper-V.

Point

Hyper-V can also be managed using Agentless Monitoring (refer to "3.2 Virtual Resource Management" for details).

Collection Interval

The collection interval is one minute.

Procedure

The linkage procedure is explained as follows:

- [1.13.1 Check Installation](#)
- [1.13.2 Definition Method](#)
- [1.13.3 Setup](#)
- [1.13.4 Display](#)

1.13.1 Check Installation

Runtime environment

Linkage can be achieved by installing the Agent of this product in an environment in which Hyper-V has been installed.

Refer to Section 1.2.3, "Installation Types Corresponding to Management Types" in the Technical Guide for information about the relationship with supported installation types.

Tasks to be performed for Hyper-V

The following preparation/confirmation must be performed for Hyper-V first:

1. Hyper-V must have been installed.
2. Each Hyper-V service/daemon must have started.

1.13.2 Definition Method

A definition in the collection template will be required in order to obtain the Hyper-V performance information.

Location

The template.dat location is as follows:

Windows

```
<variable file storage directory>\control\template.dat
```

Refer to "[9.4 How to Set Up Hyper-V](#)" for details on the definition method.

1.13.3 Setup

Refer to "[A.1 Server Resource Information Collection Policy Creation Command](#)", then execute sqcRPolicy and sqcSetPolicy.

The message that will be output when sqcSetPolicy was executed is as follows:

```
This Computer Name is "<Hostname>"  
The policy has been set for the <Hyper-V>  
(Success) : sqcSetPolicy succeeded.
```

1.13.4 Display

The Hyper-V performance information can be displayed using the method shown below.

Summary

This can be displayed by selecting the "Hyper-V(host)" node (HyperV(Physical)Monitor) or "Hyper-V(guest piling)" node (HyperV(Virtual)StackMonitor) on the summary tree.

Details

This can be displayed by selecting the "Hyper-V" node on the details tree.

Reports

General review/analysis report

Category diagnosis/analysis report

Details analysis report

1.14 Linkage with the Red Hat Virtualization Function (Xen)

Functional Overview

Physical server and virtual server performance information from the Red Hat virtualization function (Xen) is collected and managed centrally.

The virtual server performance information collected by this function is put together with the physical server performance information and evaluated comprehensively. Accordingly, the resources in the server can be optimized, and improved user efficiency can be achieved.

- The physical server performance information (physical server CPU, memory, and disk usage status) is displayed as a report.

- The virtual server performance information (guest CPU, memory, and disk usage status) accumulates in guest units and is displayed as a report.

Information that can be collected

The methods used to collect the physical server and virtual server performance information and the main function information for the Red Hat virtualization function (Xen) are shown below.

Physical Server	Virtual Server
CPU/memory/disk performance information is collected from the host operating system (Linux).	CPU/memory/disk performance information is collected from the host operating system (Linux).

Note

If the Red Hat virtualization function (Xen) is a monitoring target, then Linux performance information will also be collected from the host operating system.

Point

The Red Hat virtualization function (Xen) can also be managed using Agentless Monitoring (refer to "[3.2 Virtual Resource Management](#)" for details).

Collection Interval

The collection interval is one minute.

Procedure

The linkage procedure is explained as follows:

- [1.14.1 Check Installation](#)
- [1.14.2 Definition Method](#)
- [1.14.3 Setup](#)
- [1.14.4 Display](#)

1.14.1 Check Installation

Runtime environment

Linkage can be achieved by installing the Agent of this product in an environment in which the Red Hat virtualization function (Xen) has been installed.

Refer to Section 1.2.3, "Installation Types Corresponding to Management Types" in the Technical Guide for information about the relationship with supported installation types..

Tasks to be performed for the Red Hat virtualization function (Xen)

The following preparation/confirmation must be performed for the Red Hat virtualization function (Xen) first:

1. The Red Hat virtualization function (Xen) must have been installed.

2. Each Red Hat virtualization function (Xen) service/daemon must have started.

1.14.2 Definition Method

A definition in the collection template will be required in order to obtain the Red Hat virtualization function (Xen) performance information.

Location

The template.dat location is as follows:

UNIX

```
/etc/opt/FJSVssqc/template.dat
```

Refer to "[9.5 How to Set Up the Red Hat Virtualization Function \(Xen\)](#)" for details on the definition method.

1.14.3 Setup

Refer to "[A.1 Server Resource Information Collection Policy Creation Command](#)", then execute sqcRPolicy and sqcSetPolicy.

The message that will be output when sqcSetPolicy was executed is as follows:

```
This Host Name is "<Hostname>"  
The policy has been set for the <Xen>  
(Success) : sqcSetPolicy succeeded.
```

1.14.4 Display

The Red Hat virtualization function (Xen) performance information can be displayed using the method shown below.

Summary

This can be displayed by selecting the "Xen(guest piling)" node (Xen(Virtual)StackMonitor) on the summary tree.

Details

This can be displayed by selecting the "Xen" node on the details tree.

Reports

General review/analysis report

Category diagnosis/analysis report

Details analysis report

Chapter 2 Managing the Volume of Web Transactions

The Web transaction volume management function is for analyzing transactions (processing requests) that come into the system via Web servers or proxy servers.

Information about user accesses is stored in log files on Web servers and proxy servers. The Web transaction volume management function collects information from these files, such as the number of requests, traffic volume, and request processing time.

This function is for performing a comprehensive analysis of the status of requests to Web servers or proxy servers. It collects the following data from Web access logs.

- Traffic volume
- Request processing time
- The number of requests
- The number of errors

Execution environment

These settings can be made on Managers, Proxy Managers and Agents for Business.

Privileges required for execution

[Windows]

The privileges of a user belonging to the "Administrators" group are required to make these settings.

[UNIX]

System administrator (superuser) privileges are required to make these settings.

Collection interval

Collection interval is 5 minutes.

Definition method

The following sections explain how to make definitions for managing the volume of Web transactions:

- [2.1 Transaction Log Definitions](#)
- [2.2 Setup](#)
- [2.3 Display](#)
- [2.4 Transaction Log Definition File \(Sample\)](#)

2.1 Transaction Log Definitions

A transaction log definition file is required in order to manage the volume of Web transactions. This definition file specifies how the transaction log analysis function will analyze log files.

Make definitions based on the sample file.

Storage location

[Windows]

```
Installation directory\sample\tlawatch.ini
```

[UNIX]

```
/opt/FJSVssqc/sample/tlawatch.ini
```

Back up the "tlawatch.ini" file before performing these tasks.

Definition location

The transaction log definition file is a text file. Use a text editor such as Notepad to create and edit the file. The path to the file is as follows:

[Windows]

```
Variable file directory\control\tlawatch.ini
```

[UNIX]

```
/etc/opt/FJSVssqc/tlawatch.ini
```

The character encodings for the text file are as follows:

```
ASCII
```

- [2.1.1 Definition format](#)
- [2.1.2 Checking definition contents](#)

2.1.1 Definition format

Create the transaction log definition file using the following format.

Syntax

```
[RequestLog]
Service=service-name
Type=web | proxy
Path=log-path
Format=format-symbol | "format"
TimeZone=timezone
Inclusion=inclusive-record
```

Point

- The vertical bars "|" mean "or". That is, either one option or the other can be specified.
- Blank lines are treated as comments.
- Lines that start with a hash "#" are treated as comments.

Description

[RequestLog]

Indicates the start of a new definition block and the end of the previous definition block.

Up to 20 definition blocks can be defined.

- **Service=service-name**

Define the identifier for the log to be analyzed. For "service-name", specify the identifier using up to 64 characters. The following characters cannot be used.

```
\ : < > " $ ' [ ] = & / * ? | ,
```

Note

Each definition block must have a different "service-name".

- **Type=web | proxy**

Indicates which type of server is being analyzed. The meanings of each option are as follows:

Option	Meaning
web	Web server
proxy	Proxy server

The default option is as below. For the default option, this line can be omitted.

```
Type=web
```

- **Path=log-path**

Defines the path to the log file to be analyzed.

For "log-path", specify the absolute path to the log file to be analyzed. If multiple log files are created in the same directory, use a wildcard ("*") in the file name to specify all of these files inclusively. If the path includes blank spaces, enclose the entire path in double quotes.

The wildcard feature is provided in order to allow file names to be specified in situations where log files are created for each date, or using file rotation. Wildcards cannot generally be specified with any random string.

Example

	Log file to be analyzed	log-path
Windows	Log files created in the C:\WINNT\system32\LogFiles\W3SVC3 directory using the following format: ex041002.log, ex041003.log,	C:\WINNT\system32\LogFiles\W3SVC3\ex*.log

	Log file to be analyzed	log-path
UNIX	Log files created in the /var/www/logs directory with logrotate using the following format: accesslog, accesslog.1, accesslog.2,	/var/www/logs/accesslog

Note

If the Path statement is not specified appropriately, it may not be possible to detect the latest log file, and analysis may not be possible.

- Format=format-symbol | "format"

Defines the entry format for the log file to be analyzed.

Here, "format-symbol" is a symbol corresponding to a fixed recording format.

For "format", specify the recording format using tokens and delimiters. Specify a "format" when the recording format for the log file to be analyzed does not correspond to any of the fixed recording formats.

The symbols and tokens that can be specified are listed below.

1. Specifying log files using "format-symbol"



- Analyzing log files for Web servers
- Analyzing log files for proxy servers

2. Specifying tokens for "format"

1. Specifying log files using "format-symbol"

- Analyzing log files for Web servers

Symbol	Corresponding log
	Corresponding "format"
Common	<p>W3C Common Logfile Format. Corresponds to the following logs:</p> <p>The W3C httpd (CERN httpd) Common log format</p> <p>The Apache httpd Common log format and Custom log format</p> <p>Microsoft Internet Information Services' Common log format (NCSA common log file format), the W3C Extended log format (W3C extended log file format)</p> <p>Netscape Enterprise Server's Common log format, Flexible log format and Custom log format</p> <p>Fujitsu InfoProvider Pro's Common log format, Extended log format, etc.</p> <pre>"* * * [s-time{ dd/mon/yyyy:HH:MM:SS } *] \"c-request\" s-status s-bytes"</pre>
Microsoft-MS50	<p>Microsoft Internet Information Services custom format. Corresponds to the following log:</p>

Symbol	Corresponding log
	Corresponding "format"
	<p>Microsoft Log Format for Microsoft Internet Information Services 5.0.</p> <p> Note</p> <p>.....</p> <p>This symbol is valid only if the default settings have been left unchanged since Microsoft Internet Information Services 5.0 was installed.</p> <p>.....</p> <p>"s-time{yyyy-mm-dd HH:MM:SS} * * * * s-method s-path * s-status *"</p>
Microsoft-MS60	<p>Microsoft Internet Information Services custom format. Corresponds to the following log:</p> <p>Microsoft Log Format for Microsoft Internet Information Services 6.0.</p> <p> Note</p> <p>.....</p> <p>This symbol is valid only if the default settings have been left unchanged since Microsoft Internet Information Services 6.0 was installed.</p> <p>.....</p> <p>"s-time{yyyy-mm-dd HH:MM:SS} * * * s-method s-path * s-status * *"</p>

- Analyzing log files for proxy servers

Symbol	Corresponding log
	Corresponding "format"
Common	<p>W3C Common Logfile Format. Corresponds to the following logs:</p> <p>Netscape Proxy Server's Common log format, Extended log format, Extended2 log format, Flexible log format, and Custom log format</p> <p>Squid's Common log format</p> <p>DeleGate's Common log format and Custom log format</p> <p>The Apache httpd Common log format and Custom log format</p> <p>The W3C httpd (CERN httpd) Common log format</p> <p>Fujitsu InfoProxy's Common log format, etc</p> <p>"* * * [s-time{dd/mon/yyyy:HH:MM:SS} *] \"c-request\" s-status s-bytes"</p>
Common+Ts	<p>Adds the processing time (in seconds) to Common. Can be applied to the following logs or customized formats.</p> <p>Netscape Proxy Server's Flexible log format and Custom log format</p>

Symbol	Corresponding log
	Corresponding "format"
	DeleGate's Custom log format The Apache httpd Custom log format <pre>*** [s-time{dd/mon/yyyy:HH:MM:SS} *]\c-request\ s- status s-bytes s-elapse{s}"</pre>
Common +Tms	Adds the processing time (in milliseconds) to Common. Can be applied to the following logs or customized formats: Netscape Proxy Server's Flexible log format and Custom log format DeleGate's Custom log format Fujitsu InfoProxy's Extend log format <pre>*** [s-time{dd/mon/yyyy:HH:MM:SS} *]\c-request\ s- status s-bytes s-elapse{ms}"</pre>
Netscape- Extend	Netscape Proxy Server custom format. Corresponds to the following log: Netscape Proxy Server's Extended log format and Extended2 log format <pre>*** [s-time{dd/mon/yyyy:HH:MM:SS} *]\c-request\ s- status s-bytes r-status * * * * * s-elapse{s}"</pre>
Squid- Native11	Squid custom format. Corresponds to the following log. Squid's Native log format (Version 1.1 format) <pre>"s-time{seconds} s-elapse{ms} * */s-status s-bytes s- method s-url * */* *"</pre>
Microsoft- Native	Microsoft Proxy Server custom format. Corresponds to the following logs: Microsoft Proxy Server's WebProxy log format <pre>"*, *, *, *, time{yy/mm/dd, HH:MM:SS}, *, *, *, *, *, *, s- elapse{ms}, s-bytes, *, *, *, s-method, s-url, *, *, s-status, *"</pre>
DeleGate- Default	DeleGate custom format. Corresponds to the following log: DeleGate's HTTP default log format <pre>*** [s-time{dd/mon/yyyy:HH:MM:SS} *]\c-request\ s- status s-bytes s-elapse{ms};*"</pre>
InfoProxy- Extend	Fujitsu InfoProxy custom format. Corresponds to the following log: Fujitsu InfoProxy's Extend log format <pre>*** [s-time{dd/mon/yyyy:HH:MM:SS} *]\c-request\ s- status s-bytes s-elapse{ms} r-status * * * * * * * * * * * *"</pre>

 **Note**

- When specifying the entry format for the log file using a symbol, compare the records in the log file to be analyzed with the format that corresponds to the symbol and specify the symbol that matches the actual entry format. Take particular care with the date section, as this can vary from system to system.

- The "Microsoft-MS50" and "Microsoft-MS60" symbols are valid only if the settings have been left unchanged since Microsoft Internet Information Services 5.0 or 6.0 was installed. If the log format has been changed since installation, specify a symbol so that the entry format matches the records in the log to be analyzed. If there is no such symbol, specify the entry format using a "format" string.
- The following performance information cannot be collected if the log entry format is specified using a symbol.

Symbol	Performance information that cannot be collected
Common	Request processing time
Microsoft-MS50	Request processing time
Microsoft-MS60	Traffic volume
Common+Ts	-
Common+Tms	-
Netscape-Extend	-
Squid-Native11	-
Microsoft-Native	-
DeleGate-Default	Request processing time
InfoProxy-Extend	-

2. Specifying tokens for "format"

Token	Meaning
s-time{time-format}	The time when the server finished processing the request
c-request	The first request that the client sent to the server
s-method	The method that the client used to send the request to the server (part of c-request)
s-url	The URL that the client used to send the request to the server (part of c-request)
s-host	The host name or IP address in the client request to the server (part of s-url)
s-path	The file path in the client request to the server (part of s-url)
s-status	The status code that the server sent to the client
r-status	The status code that the remote server sent to the server
s-bytes	The number of bytes that the server sent to the client
s-elapse{elapse-format}	The time that it took for the server to process the request
*	Variable elements other than the above
\	Escape character (add the escape character to specify " or \ as \" or \\)

The relationship between c-request, s-method, s-url, s-host and s-path is as follows:

Mandatory tokens
s-time
s-status

- If the entry format for the log file is specified using a "format" string, make sure that the token required for analysis in operation windows is specified.

Analysis (operation window)	Mandatory token
Various URL-based analyses (Detailed and Report)	s-url (or c-request, s-path)

- TimeZone=timezone

Defines the time zone for the time data recorded in the log file to be analyzed. For "timezone", specify the time difference with respect to Coordinated Universal Time (UTC). The format is shown below.

Format	Description
[+ -]HHMM M	+: Indicates that the time is ahead of UTC. -: Indicates that the time is behind UTC. HH: Hours (00 to 23) MM: Minutes (00 to 59)

The default setting is as below. For the default setting, this line can be omitted.

TimeZone=+0000

or

TimeZone=0000



Note

Use the manuals for each server to check the local time used by the log file to be analyzed.

- Inclusion=inclusive-record

Defines URLs to be analyzed.

Specify this item in order to isolate particular URLs for monitoring and analysis in the **Detailed** and **Report** views. For "inclusive-record", specify the path (enclosed in double quotation marks) for the URL to be analyzed, without any parameters or the server name part of the Web content. Up to 1,023 characters can be used. The following characters cannot be used.

```
^|[]{}<>()&$#'*,?=:\"
```

Up to 20 Inclusion statements can be defined.

If a forward slash is specified at the end of the URL, all of the content under the specified URL (including subdirectories) will be aggregated and monitored as a single URL. However, for the following definition, the forward slash will be treated as a file name, and the content below it will not be aggregated or monitored.

```
Inclusion="/"
```

- All URLs not defined by Inclusion statements will be analyzed as "URL [CONTENTS]".
- By default, all URLs are analyzed as "URL [CONTENTS]".
For the default setting, this line can be omitted.

Example

The following example shows how Inclusion statements are defined.

```
Inclusion="/SSQC/eg.htm"
Inclusion="/cgi-bin/query.cgi"
Inclusion="/tool/program"
Inclusion="/segment01/"
```

Note

All of the following URLs are monitored as "/SSQC/eg.htm".

- http://www.fujitsu.com/SSQC/eg.htm
- https://www.fujitsu.com/SSQC/eg.htm
- http://www.fujitsu.co.jp/SSQC/eg.htm

Examples

Definition examples are as follows:

[Windows]

```
[RequestLog]
Service=www1
Path="C:\WINNT\system32\LogFiles\W3SVC1\ex*.log"
Format="s-time{yyyy-mm-dd HH:MM:SS} * s-method s-url s-status s-
bytes"
```

[UNIX]

```
[RequestLog]
Service=www2
Type=web
Path=/usr/local/apache/logs/access_log
Format=Common
TimeZone=+0900
Inclusion="/cgi-bin/query.cgi"
```

2.1.2 Checking definition contents

The transaction log monitoring engine includes an option for checking the definition format of the content that has been set up in the transaction log definition file. The method for checking the definition format is as follows:

Procedure

Run the transaction log monitoring engine with the "-c" option specified.

[Windows]

```
Installation directory\bin\tlwatch -c
```

[UNIX]

```
/opt/FJSVssqc/bin/tlwatch -c
```

A message will be output to the standard error output if there is a problem with the definition format.

No message will be output if no problems with the definition content are discovered.

2.2 Setup

To enable the changes that have been made to this file, collection policies must be created and applied.

Execute the sqcRPolicy and sqcSetPolicy commands by referring to "[A.1 Server Resource Information Collection Policy Creation Command](#)".

2.3 Display

Information about the volume of Web transactions can be displayed using the following method.

Summary view of the Console window

Use the "Web transaction" node (WebTrnMonitor) in the Summary tree.

Drilled-Down view of the Console window

Use the "WebTrn" node in the Detailed tree.

Report view

- Full system inspection analysis/reports
- Categorized diagnostic analysis/reports
- Detailed analysis/reports

2.4 Transaction Log Definition File (Sample)

The sample transaction log definition file can be used to monitor the following Web servers when managing the volume of Web transactions.

No.	Monitored Web server	Log format	Target operating system
1	Internet Information Services 5.0	Microsoft Log Format	Windows

No.	Monitored Web server	Log format	Target operating system
		This is the default log file format after IIS 5.0 is installed	
2	Internet Information Services 6.0	Microsoft Log Format This is the default log file format after IIS 6.0 is installed	Windows
3	Internet Information Services 7.0	Microsoft Log Format Note: Default log file format after installing IIS 7.0	Windows
4	Apache HTTP Server	Common log format	Windows Solaris Linux
5	Apache HTTP Server	Combined log format	Windows Solaris Linux
6	Interstage HTTP Server	Common log format	Windows Solaris Linux

Storage directory

The sample file is stored in the following directory:

[Windows]

<Installation directory>\sample

[UNIX]

/opt/FJSVssqc/sample



- To use a sample definition file on a server where the volume of Web transactions is to be managed, back up the existing transaction log definition file (tlawatch.ini) and then overwrite it with the sample definition file.
- Check the content of the sample files in "2.4.1 Sample files", and change any settings that need to be changed.

2.4.1 Sample files

The transaction log definition files stored in sample files are as shown below.

Note that the values of some parameters may need to be changed depending on the Web server environment. Change the values of the parameters listed in "Value to change according to the environment" to match the Web server environment.

- [2.4.2 Transaction log definition file \(Internet Information Services 5.0\)](#)
- [2.4.3 Transaction log definition file \(Internet Information Services 6.0\)](#)
- [2.4.4 Transaction log definition file \(Internet Information Services 7.0\)](#)
- [2.4.5 Transaction log definition file \(Apache HTTP Server \[Common log format\]\)](#)

- [2.4.6 Transaction log definition file \(Apache HTTP Server \[Combined log format\]\)](#)
- [2.4.7 Transaction log definition file \(Interstage HTTP Server \[Common log format\]\)](#)

2.4.2 Transaction log definition file (Internet Information Services 5.0)

Usage

Use this transaction log definition file to manage the volume of Web transactions if the default settings have not been changed since Internet Information Services 5.0 was installed on the Web server (that is, if the log file format has not been changed).

Storage directory

```
<Installation directory>\sample\tlwatch.ini.<OS name>_iis5
```

Settings in the sample file

[Windows]

```
# Microsoft Internet Information Server 5.0 (Microsoft Log Format) sample
[RequestLog]
Service=www1
Type=web
Path="C:\WINNT\system32\LogFiles\W3SVC1\ex*.log"
Format=Microsoft-MS50
TimeZone=0000
```

Content of the settings in the sample file

Definition item	Parameter	Sample value	Value to change according to the environment
Identifier for the log to be analyzed	Service	www1	
Type of server to be analyzed	Type	web	
Path to the analysis log file	Path	[Windows] "C:\WINNT\system32\LogFiles\W3SVC1\ex*.log"	Change this value if the path to the log file to be analyzed is not the same as the path listed on the left.
Recording format used in the analysis log file	Format	Microsoft-MS50	
Time zone for the time data recorded in the log file to be analyzed	TimeZone	0000	

2.4.3 Transaction log definition file (Internet Information Services 6.0)

Usage

Use this transaction log definition file to manage the volume of Web transactions if the default settings have not been changed since Internet Information Services 6.0 was installed on the Web server (that is, if the log file format has not been changed).

Storage directory

```
<Installation directory>\sample\tlwatch.ini.<OS name>_iis6
```

Settings in the sample file

[Windows]

```
# Microsoft Internet Information Server 6.0 (Microsoft Log Format) sample

[RequestLog]
Service=www1
Type=web
Path="C:\WINDOWS\system32\LogFiles\W3SVC1\ex*.log"
Format=Microsoft-MS60
TimeZone=0000
```

Content of the settings in the sample file

Definition item	Parameter	Sample value	Value to change according to the environment
Identifier for the log to be analyzed	Service	www1	
Type of server to be analyzed	Type	web	
Path to the analysis log file	Path	[Windows] "C:\WINDOWS\system32\LogFiles\W3SVC1\ex*.log"	Change this value if the path to the log file to be analyzed is not the same as the path listed on the left.
Recording format used in the analysis log file	Format	Microsoft-MS60	
Time zone for the time data recorded in the log file to be analyzed	TimeZone	0000	

2.4.4 Transaction log definition file (Internet Information Services 7.0)

Usage

Use this transaction log definition file to manage the volume of Web transactions if the default settings have not been changed since Internet Information Services 7.0 was installed on the Web server (that is, if the log file format has not been changed).

Storage directory

```
<Installation directory>\sample\tlwatch.ini.<OS name>_iis7
```

Settings in the sample file

[Windows]

```
# Microsoft Internet Information Server 7.0 (Microsoft Log Format) sample
[RequestLog]
Service=www1
Type=web
Path="C:\inetpub\logs\LogFiles\W3SVC1\u_ex*.log"
Format="s-time{yyyy-mm-dd HH:MM:SS} * s-method s-path * * * * * s-status * * s-elapse{ms}"
TimeZone=0000
```

Content of the settings in the sample file

Definition item	Parameter	Sample value	Value to change according to the environment
Identifier for the log to be analyzed	Service	www1	
Type of server to be analyzed	Type	web	
Path to the analysis log file	Path	[Windows] C:\inetpub\logs\LogFiles\W3SVC1\u_ex*.log	Change this value if the path to the log file to be analyzed is not the same as the path listed on the left.
Recording format used in the analysis log file	Format	s-time{yyyy-mm-dd HH:MM:SS} * s-method s-path * * * * * s-status * * s-elapse{ms}	
Time zone for the time data recorded in the log file to be analyzed	TimeZone	0000	

2.4.5 Transaction log definition file (Apache HTTP Server [Common log format])

Usage

Use this transaction log definition file to manage the volume of Web transactions if the log file format for Apache HTTP Server on the Web server is the "Common" format.

Storage directory

```
<Installation directory>\sample\tlwatch.ini.<OS name>_apache_common
```

Settings in the sample file

[Windows]

```
# Apache HTTP Server (Common Log Format) sample
[RequestLog]
Service=www1
Type=web
Path="C:\Program Files\Apache Software Foundation\Apache2.2\logs\access.log"
Format=Common
TimeZone=+0900
```

[UNIX]

```
# Apache HTTP Server (Common Log Format) sample
[RequestLog]
Service=www1
Type=web
Path="/var/log/httpd/access_log"
Format=Common
TimeZone=+0900
```

Content of the settings in the sample file

Definition item	Parameter	Sample value	Value to change according to the environment
Identifier for the log to be analyzed	Service	www1	
Type of server to be analyzed	Type	web	
Path to the analysis log file	Path	[Windows] "C:\Program Files\Apache Software Foundation\Apache2.2\logs\access.log" [UNIX] "/var/log/httpd/access_log"	Change this value if the path to the log file to be analyzed is not the same as the path listed on the left.
Recording format used in the analysis log file	Format	Common	
Time zone for the time data recorded	TimeZone	+0900	

Definition item	Parameter	Sample value	Value to change according to the environment
in the log file to be analyzed			

2.4.6 Transaction log definition file (Apache HTTP Server [Combined log format])

Usage

Use this transaction log definition file to manage the volume of Web transactions if the log file format for Apache HTTP Server on the Web server is the "Combined" format.

Storage directory

```
<Installation directory>\sample\tlwatch.ini.<OS name>_apache_combined
```

Settings in the sample file

[Windows]

```
# Apache HTTP Server (Combined Log Format) sample
[RequestLog]
Service=www1
Type=web
Path="C:\Program Files\Apache Software Foundation\Apache2.2\logs\access.log"
Format="* * * [s-time{dd/mon/yyyy:HH:MM:SS} *] \"c-request\" s-status s-bytes \"%\" \"%\" \"%\"
TimeZone=+0900
```

[UNIX]

```
# Apache HTTP Server (Combined Log Format) sample
[RequestLog]
Service=www1
Type=web
Path="/var/log/httpd/access_log"
Format="* * * [s-time{dd/mon/yyyy:HH:MM:SS} *] \"c-request\" s-status s-bytes \"%\" \"%\" \"%\"
TimeZone=+0900
```

Content of the settings in the sample file

Definition item	Parameter	Sample value	Value to change according to the environment
Identifier for the log to be analyzed	Service	www1	
Type of server to be analyzed	Type	web	
Path to the analysis log file	Path	[Windows] "C:\Program Files\Apache Software Foundation\Apache2.2\logs\access.log" [UNIX] "/var/log/httpd/access_log"	Change this value if the path to the log file to be analyzed is not the same as the path listed on the left.
Recording format used in the analysis log file	Format	"* * * [s-time{dd/mon/yyyy:HH:MM:SS} *] \"c-request\" s-status s-bytes \"%\" \"%\""	
Time zone for the time data recorded in the log file to be analyzed	TimeZone	+0900	

2.4.7 Transaction log definition file (Interstage HTTP Server [Common log format])

Usage

Use this transaction log definition file to manage the volume of Web transactions if the log file format for Interstage HTTP Server on the Web server is the "Common" format.

Storage directory

```
<Installation directory>\sample\tlwatch.ini.<OS name>_apache_common
```

Settings in the sample file

[Windows]

```
# Interstage HTTP Server (Common Log Format) sample
[RequestLog]
Service=www1
Type=web
Path="C:\Interstage\F3FMihs\logs\accesslog"
Format=Common
TimeZone=+0900
```

[UNIX]

```
# Interstage HTTP Server (Common Log Format) sample
```

```

[RequestLog]
Service=www1
Type=web
Path="/var/opt/FJSVihs/logs/accesslog"
Format=Common
TimeZone=+0900

```

Content of the settings in the sample file

Definition item	Parameter	Sample value	Value to change according to the environment
Identifier for the log to be analyzed	Service	www1	
Type of server to be analyzed	Type	web	
Path to the analysis log file	Path	[Windows] "C:\Interstage\F3FMihs\logs\accesslog" [UNIX] "/var/opt/FJSVihs/logs/accesslog"	Change this value if the path to the log file to be analyzed is not the same as the path listed on the left.
Recording format used in the analysis log file	Format	Common	
Time zone for the time data recorded in the log file to be analyzed	TimeZone	+0900	

Chapter 3 Management with an Agent for Agentless Monitoring

This chapter explains how to remotely manage a monitored server that doesn't have an Agent installed.

Refer to Section 2.4, "Operation Model for Agents for Agentless Monitoring" and Section 3.2.1.2, "Agent for Agentless Monitoring" in the Technical Guide for more about the functions of agents for Agentless Monitoring.

Refer to Section 3.2.1, "Agent" in the Technical Guide for differences between agents for Agent-based Monitoring and agents for Agentless Monitoring.

Execution environment

Can be executed under Manager/Proxy Manager.

Privileges required for execution

Windows

The Administrators group user privileges are required.

UNIX

System administrator (superuser) privileges are required.

Communication method

Communication is performed between the monitoring server and monitored server (agent for Agentless Monitoring) by one of telnet, ssh or https when remotely collecting performance information. Refer to "[3.1.1 Prerequisites](#)" or "[3.2.1 Prerequisites](#)" for details.

Note

- Set up the environment so that the monitoring server can connect to the monitored server through telnet (port number 23) when using telnet.
- Set up the environment so that the monitoring server can connect to the monitored server through ssh (port number 22) when using ssh.

System time

Set the system time on the monitoring server and monitored server to the same time.

Management type

Settings on the agent for Agentless Monitoring to manage performance are described below.

- [3.1 Server Performance Management](#)
- [3.2 Virtual Resource Management](#)

3.1 Server Performance Management

Function overview

Server performance management can centrally manage the performance information (CPU, memory, and disk, for example) of Windows, Solaris, Linux, AIX, and HP-UX operating systems.

There are differences between agents for Agent-based Monitoring and agents for Agentless Monitoring in the items collected and the collection intervals. Refer to "[3.1.5 Differences between Agents for Agent-based Monitoring and Agents for Agentless Monitoring](#)" for details.

Collection interval

Collection interval is 5 minutes.

Procedure

Steps for setting an agent for Agentless Monitoring to manage server performance are described below.

- [3.1.1 Prerequisites](#)
- [3.1.2 Settings for Monitored Servers](#)
- [3.1.3 Settings for Monitoring Servers](#)
- [3.1.4 Display](#)

3.1.1 Prerequisites

For the hardware and operating systems to use for the monitoring server (Manager/Proxy Manger) and monitored server (agent for Agentless Monitoring), refer to Chapter 2, "Installation Conditions and Resource Estimation" in the Installation Guide.

Required software

The software required for communication between the monitoring server and the monitored server is described below.

Communication method	Software required for monitoring server	Software required for monitored server (agent for Agentless Monitoring)
telnet (selectable for Windows and UNIX)		telnet server
ssh (selectable for UNIX)		ssh server (*1)

*1: The following software is required to communicate by SSH. We recommend using ssh from a security perspective:

- SSH V2.0 or later

SSH is installed as a standard function with Solaris9, Solaris10, Red Hat Enterprise Linux 5 and Red Hat Enterprise Linux 6.

Resource estimation

Number of connection sessions

The following explains the number of telnet/ssh connection sessions required on the monitored server so that performance information can be collected from the monitored server.

Platform of the monitored server (agent for Agentless Monitoring)	Number of telnet or ssh connection sessions
Windows	2
Solaris	7
Linux	5
AIX	8
HP-UX	7

Note

- If the total number of connection sessions is very large, it may take some time for the DCM services/daemons of the monitoring server to start or stop.
- Communications by telnet or ssh may not be performed properly if the network status of the environment is not optimal (there are intermittent interruptions, etc.) or if the monitored server is busy. Perform monitoring in an environment with consistently reliable communications.
- The default maximum number of sessions that can be connected simultaneously with Windows telnet is "2". Therefore it will be necessary to change the maximum number of sessions that can be connected simultaneously. Follow the steps in "[3.1.2 Settings for Monitored Servers](#)".
There is no limit to the maximum number of sessions that can be connected simultaneously by default with UNIX telnet and ssh.

Free space on disk

The following explains the disk space required on the monitored server so that performance information can be collected from the monitored server.

- Disk space required on the monitored server: 1MB

3.1.2 Settings for Monitored Servers

The following explains the settings required so that performance information can be collected from the monitored server.

If the server to be monitored is a Windows server

1. Create a user so that connections can be made remotely.
Do not specify "User must change password at next logon" for the user.
2. Add a user to the groups necessary for connecting remotely and collecting information ("TelnetClients" group and "Performance Monitor Users" group).

Follow these steps to make the settings.

- a. Create a "TelnetClients" local group.
 1. Open Computer Management.
 2. In the console tree, expand Local Users and Groups and click Groups.
 3. If the "TelnetClients" group already exists in the list, skip the next step and go on to "b. Add user to the "TelnetClients" group".
 4. Right-click on Groups, and click New Group.
 5. In the New Group dialog, enter "TelnetClients". Add descriptions as required.
 6. If the user has already been created, click Add and enter the user name in the Select Users, Computers, or Groups dialog.

7. Click Create.
- b. Add user to the "TelnetClients" group.
 1. Open Computer Management.
 2. In the console tree, expand Local Users and Groups and click Groups.
 3. Double-click the "TelnetClients" local group.
 4. Click Add.
 5. Follow the instructions in the Select Users, Computers, or Groups dialog to add the user to the "TelnetClients" group and click OK.
 - c. Add user to the "Performance Monitor Users" group.
 1. Open Computer Management.
 2. In the console tree, expand Local Users and Groups and click Groups.
 3. Double-click the "Performance Monitor Users" group.
 4. Click Add.
 5. Follow the instructions in the Select Users, Computers, or Groups dialog to add the user to the "Performance Monitor Users" group and click OK.

 **Note**

- From a security point of view, it is not recommended to use a user belonging to the Administrators group.
- To open Computer Management, from the Windows **Start** menu, click **Control Panel** and double-click **Administrative Tools >> Computer Management**.
- When entering the group name, be sure to spell "TelnetClients" as shown.
- Users cannot login after creating a "TelnetClients" group until the "Telnet Server" service is stopped and then started again.

3. Make settings to have the "Telnet" service start automatically.

Windows Server® 2003

Make settings to have the "Telnet" service start automatically.

 **Note**

The "Telnet" service is set to not start automatically by default.

- a. Open Computer Management.
- b. In the console tree, click Services.
- c. Double-click the "Telnet" service.
- d. Make the startup type Automatic, change the service status to Start, and click OK.

Windows Server® 2008

Enable the "Telnet Server" function and set the "Telnet" service to start automatically.

 **Note**

The "Telnet Server" function is disabled by default.

The "Telnet" service is also set to not start automatically by default.

The following describes how to enable the "Telnet Server" function and set the "Telnet" service to start automatically.

- a. Start the Windows **Server Manager**.
- b. Select **Features** in the tree on the left and click **Add Features** in the window on the right.
- c. Select **Telnet Server** and click **Next**.
- d. Click the **Install** button.

When installation is finished, start Windows **Services**, and follow the steps below to have the Telnet service start automatically.

- a. Open Computer Management.
 - b. In the console tree, click Services.
 - c. Double-click the "Telnet" service.
 - d. Make the startup type Automatic, change the service status to Start, and click OK.
4. Change the maximum number of sessions that can be connected simultaneously with the "Telnet" service.

The default maximum number of sessions that can be connected simultaneously with the "Telnet" service is "2". Set the maximum number of sessions with consideration for the number of sessions required shown in "[Number of connection sessions](#)".

Use the Windows "tntadmn" command to change the maximum number of sessions that can be connected simultaneously.

```
tntadmn config maxconn=<maximum number of connection sessions>
```

Note

When running the command under Windows Server® 2008, run as the administrator. To do so, from the **Start** menu, select **All Programs, Accessories**, then right-click **Command Prompt** and select **Run as administrator**. Now run the commands described below in the command prompt that appears.

```
tntadmn config maxconn=<maximum number of connection sessions>
```

5. Logon to the computer with the new user.

Note

The user profile of the connecting user is necessary for connecting remotely and collecting information. For this reason, logon to the Windows computer as the connecting user.

6. Connect to the set server with telnet and confirm that you can log in with the created user.

If the server to be monitored is a UNIX server

When communicating by telnet

1. Create a user so that connections can be made remotely. Set a user home directory at this time.

For instance, when using the `useradd` or `usermod` command, set the home directory of the user with the `-d` option, for example. If a home directory does not exist, create one. Set a directory with user write access privileges for the home directory.



.....
A user registered in the `adm` group is required to run the `sar` command if the monitored server is an AIX server. If the user for connecting remotely is not a root user, register the user in the `adm` group.
.....

2. Make settings to have the telnet daemon start automatically.

Refer to the telnet manual for information about how to start and set the daemon.

3. Connect to the set server with telnet and confirm that you can log in with the created user. Also confirm that the current directory when you login is the home directory created for the user.

When communicating by ssh

1. Create a user so that connections can be made remotely. Set a user home directory at this time.

For instance, when using the `useradd` or `usermod` command, set the home directory of the user with the `-d` option, for example. If a home directory does not exist, create one. Set a directory with user write access privileges for the home directory.



.....
A user registered in the `adm` group is required to run the `sar` command if the monitored server is an AIX server. If the user for connecting remotely is not a root user, register the user in the `adm` group.
.....

2. Make settings to have the ssh daemon start automatically.

Install SSH (or OpenSSH) if it has not been installed yet.

Refer to the ssh manual for information about how to install and start the daemon.

3. Connect to the set server with ssh and confirm that you can log in with the created user. Also confirm that the current directory when you login is the home directory created for the user.

3.1.3 Settings for Monitoring Servers

Steps for setting the monitoring server are described below.

1. [Definition method](#)
2. [Setup](#)

3.1.3.1 Definition method

The following two definition files are necessary to collect performance information from the monitored server.

- [Connection account configuration file](#)
- [Remote monitoring configuration file](#)

3.1.3.1.1 Connection account configuration file

Define the settings for telnet/ssh communication between the monitoring server and the monitored server.

Edit the Connection account configuration file (remoteAccount.txt).

Storage location

The file is stored in the following location:

Windows

```
<variable file storage directory>\control\remoteAccount.txt
```

UNIX

```
/etc/opt/FJSVssqc/remoteAccount.txt
```

Edit the above file using the definition method described below.

Definition method

This is an ini format file.

Set the sections by connection account groups for communication between the monitoring server and the monitored server.

The method of definition depends on the communication method. Edit to match the communication method.

1. When communicating by telnet

No	Item	Mandatory/ optional	Format	Description
-	[ACCOUNT]	Mandatory	63 characters or fewer, using alphanumerics, hyphens (-), periods (.), and hash symbols (#) only	Use an account group name for the section name. Make it so that the section name is a unique character string.
1	CONNECTTY PE	Mandatory	TELNET	Set the connection method when connecting with the agentless function. Set to "TELNET" as this is for telnet connection.
2	USER	Mandatory	63 characters or fewer The following characters cannot be used: V[!]; <>+=,?*@.	Set the login account for telnet connection.
3	PASSWORD	Mandatory	Character string generated with genpwd (*1)	Set the password for telnet connection.

*1: Refer to "[A.6 genpwd \(password encryption command\)](#)" for details about how to use the genpwd command to generate encrypted passwords.

2. When communicating by ssh

No	Item	Mandatory/ optional	Format	Description
-	[ACCOUNT]	Mandatory	63 characters or fewer, using alphanumerics, hyphens (-), periods (.), and hash symbols (#) only	Use an account group name for the section name. Make it so that the section name is a unique character string.
1	CONNECTTYPE	Mandatory	SSH	Set the connection method when connecting with the agentless function. Set to "SSH" as this is for ssh connection.
2	USER	Mandatory	63 characters or fewer The following characters cannot be used: √[]; <>+=,*#@.	Set the account for ssh connection.
3	PASSWORD	Mandatory	Character string generated with genpwn (*1)	Set the password for ssh connection.

*1: Refer to "[A.6 genpwn \(password encryption command\)](#)" for details about how to use the genpwn command to generate encrypted passwords.

Example of definition

The following is an example of definitions when the communication method is telnet or ssh.

```
# When communicating by telnet
[TELNET-ACCOUNT1]
CONNECTTYPE=TELNET
USER=telnetuser
PASSWORD=C5sJGBE3ONs=

# When communicating by ssh
[SSH-ACCOUNT2]
CONNECTTYPE=SSH
USER=sshuser
PASSWORD=6zAp+gTGDzHyzswPuANqsw==
```

3.1.3.1.2 Remote monitoring configuration file

Define the settings for the monitored server.

Edit the remote monitoring configuration file (remoteAgent.txt).

Storage location

The file is stored in the following location:

Windows

<variable file storage directory>\control\remoteAgent.txt

UNIX

/etc/opt/FJSVssqc/remoteAgent.txt

Edit the above file using the definition method described below.

Definition method

This is an ini format file.

Set sections for each server to be monitored.

No	Item	Mandatory/ optional	Format	Description
-	[HOSTNAME]	Mandatory	63 characters or fewer, using alphanumerics, hyphens (-), periods (.), and hash symbols (#) only	Set an optional section name as the section name. Make it so that the section name is a unique character string. It is recommended to use the host name.
1	HOSTNAME	Mandatory	63 characters or fewer, using alphanumerics, hyphens (-), periods (.), and hash symbols (#) only	Specify the IP address or host name used for connection to the monitored server.
2	DISPLAYNAME	Any	63 characters or fewer, using alphanumerics, hyphens (-), periods (.), and hash symbols (#) only	Specify the system name displayed in the SQC console. Note: HOSTNAME becomes the system name if this is not specified.
3	OSTYPE	Any	WINDOWS LINUX SOLARIS AIX HP-UX	OS of the monitored host. WINDOWS: For Windows LINUX: For Linux SOLARIS: For Solaris AIX: For AIX HP-UX: For HP-UX Note: OS is set to the OS of the monitoring server if this is not specified.
4	ACCOUNT	Mandatory	63 characters or fewer, using alphanumerics, hyphens (-), periods (.), and hash symbols (#) only	Specify a connection account for communicating with the monitored server. Specify the section name of the account group set in remortAccount.txt (Connection account configuration file).
5	CONNECTION	Any	ON or OFF	Set ON/OFF for monitoring. Specify "OFF" to stop monitoring.

No	Item	Mandatory/ optional	Format	Description
				Note: Set to "ON" if this is not specified.

Example of definition

The following is an example of definitions when the communication method is telnet or ssh.

```
# If the monitoring server is a Solaris server
[host1]
HOSTNAME=host1
OSTYPE=SOLARIS
ACCOUNT=TELNET-ACCOUNT1

# If the monitoring server is a Linux server
# When this monitoring server is not to be monitored
[linux-host2]
HOSTNAME=192.168.1.2
DISPLAYNAME=host2
OSTYPE=LINUX
ACCOUNT=SSH-ACCOUNT2
CONNECTION=OFF
```

3.1.3.2 Setup

Refer to "[A.1 Server Resource Information Collection Policy Creation Command](#)" and execute sqcRPolicy and sqcSetPolicy.

Point

Perform a check of the text entered into the definitions files during setup. Start the service to check that connection can be made to the monitored server. Warning messages are output to the event log when performance information collection is executed on monitored servers that cannot be connected. Refer to Section 5.1, "Common Messages" in the *Reference Guide* and take the steps described.

If definitions files (Connection account configuration file and remote monitoring configuration file) have errors, monitored servers that have the errors will not be managed.

When sqcSetPolicy is executed, the following message is output for monitored servers that have been excluded from management due to errors in the definition.

```
(Warning) : <Install-less Agent> ignored section name[section name]
```

The section name defined in "remote monitoring configuration file" is output to "section name".

The following message is also output if any errors are found in a definitions file.

```
(Warning) : <Install-less Agent> There is an error in definition.
Please confirm the file (file name).
```


The following is output to "file name".

Windows

```
<variable file storage directory>\log\setpolicy_error.log
```

UNIX

```
/var/opt/FJSVssqc/setpolicy_error.log
```

If this message appears, check the file content, correct the definitions files (Connection account configuration file and remote monitoring configuration file) according to the message in the file, and then setup again. Refer to Section 1.1.3, "sqcSetPolicy (Policy Application Command)" in the *Reference Manual* for details about messages output to the file.

Note that collection policy setup must be passed to the console. Refer to Section 1.2.2.3, "Agents" in the *User's Guide (Console Edition)* and use the Agent Settings window to collect configuration information.

Note

- It takes about 15 to 20 minutes for this information to appear in the console's "UnregisteredAgents folder" after starting the Manager/Proxy Manager service.
If it does not appear, look in the Manager/Proxy Manager's event log/syslog to see if a message has been output.
- It is necessary to create directories and files (needed to carry out monitoring) on the server to be monitored when managing with an agent for Agentless Monitoring.
Directories and files are created in the following location:
 - If the server to be monitored is a Windows server
%USERPROFILE%\sqc_temp directory
%USERPROFILE% : Path name of the user profile folder
 - If the server to be monitored is a UNIX server
Home directory of the user

The created directory name is as follows:

dsa_temp_***

Do not delete the above directory during monitoring. Performance information will not be collected if this directory is deleted. If this directory is deleted by accident, restart the Manager/Proxy Manager service.

Delete the above directory to exclude the server from monitoring.

3.1.4 Display

OS performance information collected by an agent for Agentless Monitoring can be displayed as follows.

Summary view

Performance information can be displayed by selecting the "Server resource" node (ServerMonitor) in the Summary tree.

Drilled-Down view

Performance information can be displayed by selecting the Windows, Solaris, Linux, AIX, and HP-UX nodes in the Detailed tree.

Report view

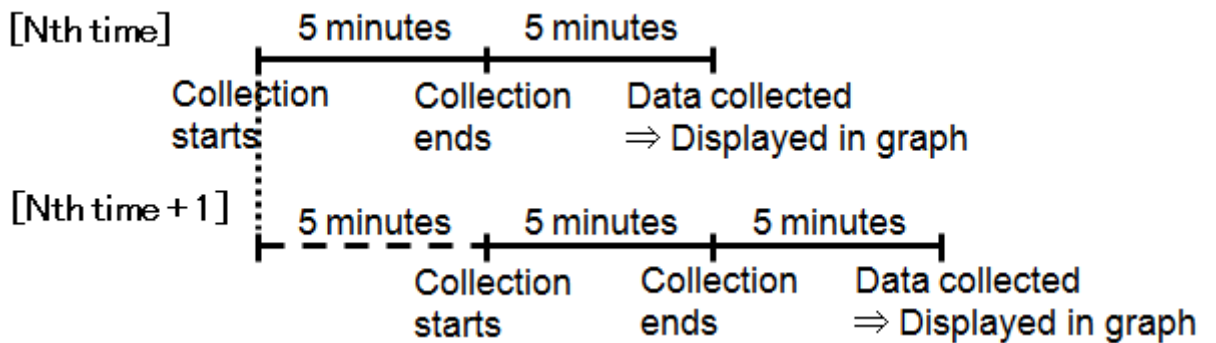
Full system inspection analysis/report

Categorized diagnostic analysis/report

Detailed analysis/report

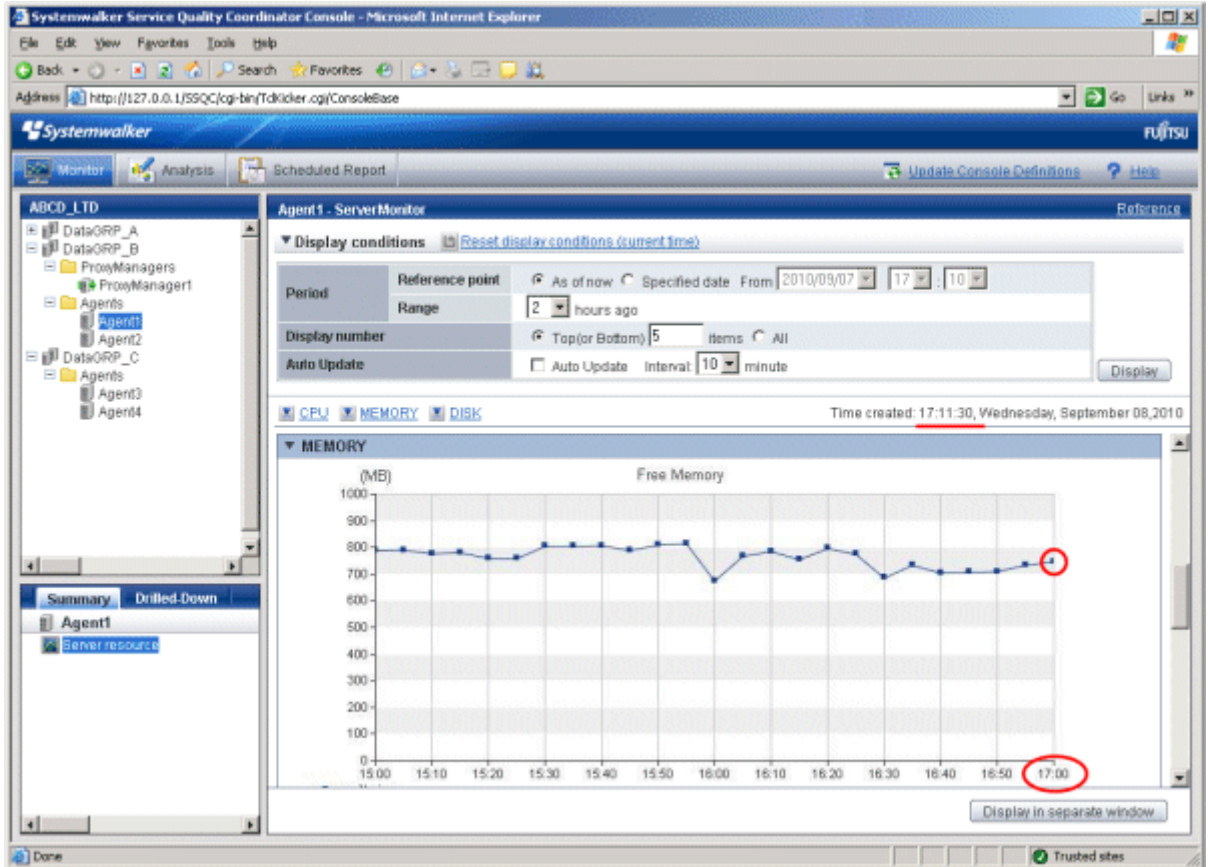
Note

- The full system inspection analysis/report and categorized diagnostic analysis/report can show reports that have "Windows" or "UNIX" in the report title. They cannot display the "Windows process" and "UNIX process" reports, however.
- When this data is to be displayed in the summary view, it will take 10 to 15 minutes for the data to appear. This is due to the way that the data is collected by the agent for Agentless Monitoring, as described below.



Data for 17:00, for example

17:00	Begin collection
17:05	End collection
17:10	Manager/Proxy Manager collects the data This data is displayed in the console as the data for 17:00. (Data display is based on the time that data collection starts. The data value for 17:00 is the average of data collected between 17:00 and 17:05.) This state continues for the next five minutes (until about 17:15) until performance data is next collected.



- The first data will appear 15 to 20 minutes after starting the Manager/Proxy Manager service because the script is sent to the monitored server at the timing of the first collection.

3.1.5 Differences between Agents for Agent-based Monitoring and Agents for Agentless Monitoring

This section explains the differences between agents for Agent-based Monitoring and agents for Agentless Monitoring.

Collection interval

Differences in collection intervals are as follows.

Agent type	Collection interval
Agent for Agent-based Monitoring	1 minute
Agent for Agentless Monitoring	5 minutes

Collection items

The values collected for OS performance information differ between agents for Agent-based Monitoring and agents for Agentless Monitoring.

The main differences in the items collected are as follows.

Agent type	Main collection items
Agent for Agent-based Monitoring	CPU, memory, disk, network, processes, and IPC resources
Agent for Agentless Monitoring	CPU, memory, and disk

The differences in the detailed items collected by record ID are as follows.

Refer to Chapter 4, "Data Formats" in the *Reference Guide* for information about record IDs.

Agent for Agent-based Monitoring: Ag. Agent for Agentless Monitoring: Agl

Yes: Collected No: Not collected -: Relevant collection item does not exist

Data types	Record ID	Windows		Solaris		Linux		AIX		HP-UX	
		Ag	Agl	Ag	Agl	Ag	Agl	Ag	Agl	Ag	Agl
Summary data	SUM_PROC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	SUM_MEM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	SUM_DISK	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Resource data	WIN_DISKSPACE	Yes	Yes	-	-	-	-	-	-	-	-
	WIN_PROCESS	Yes	No	-	-	-	-	-	-	-	-
	WIN_LOGDISKBUSY	Yes	Yes	-	-	-	-	-	-	-	-
	WIN_PHYDISKBUSY	Yes	Yes	-	-	-	-	-	-	-	-
	WIN_MEMORY	Yes	Yes	-	-	-	-	-	-	-	-
	WIN_PAGEFILE	Yes	Yes	-	-	-	-	-	-	-	-
	WIN_CPUBUSY	Yes	Yes	-	-	-	-	-	-	-	-
	WIN_NET_INTERFACE	Yes	No	-	-	-	-	-	-	-	-
	WIN_NET_SYSTEM	Yes	No	-	-	-	-	-	-	-	-
	WIN_SYSTEM	Yes	Yes	-	-	-	-	-	-	-	-
	WIN_SYSTEMINFO	Yes	No	-	-	-	-	-	-	-	-
	UX_DISKSPACE	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	UX_SYSCALLS	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	UX_FILEIO	-	-	Yes	Yes	-	-	Yes	Yes	Yes	Yes
	UX_MQSEMA	-	-	Yes	Yes	-	-	Yes	Yes	Yes	Yes
	UX_PAGING	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	UX_CPUQUEUE	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	UX_MEMFREE	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	UX_SYSTBLS	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	UX_SWAPIO	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	UX_PROCESS	-	-	Yes	No	Yes	No	Yes	No	Yes	No
	UX_NET_INTERFACE	-	-	Yes	No	Yes	No	Yes	No	Yes	No
	UX_NET_SYSTEM	-	-	Yes	No	Yes	No	Yes	No	Yes	No
UX_DISKBUSY	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	

Data types	Record ID	Windows		Solaris		Linux		AIX		HP-UX	
		Ag	Agl	Ag	Agl	Ag	Agl	Ag	Agl	Ag	Agl
	UX_C PUBUSY	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	UX_SWAPSTATUS	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	UX_SWAPUSAGE	-	-	Yes	Yes	-	-	Yes	Yes	Yes	Yes
	UX_SYS_PAGINGDETA IL	-	-	Yes	Yes	-	-	-	-	-	-
	UX_KMA	-	-	Yes	Yes	-	-	-	-	-	-
	UX_IPCSMQ	-	-	Yes	No	Yes	No	Yes	No	Yes	No
	UX_IPCSMQSUM	-	-	Yes	No	Yes	No	Yes	No	Yes	No
	UX_IPCSSM	-	-	Yes	No	Yes	No	Yes	No	Yes	No
	UX_IPCSSMSUM	-	-	Yes	No	Yes	No	Yes	No	Yes	No
	UX_IPCSSEM	-	-	Yes	No	Yes	No	Yes	No	Yes	No
	UX_IPCSSEM SUM	-	-	Yes	No	Yes	No	Yes	No	Yes	No
	UX_ZONE	-	-	Yes	No	-	-	-	-	-	-
	UX_CPUSTAT_CORE	-	-	Yes	No	-	-	-	-	-	-
	UX_SYSTEMINFO	-	-	Yes	No	Yes	No	-	-	-	-
	LX_DISKBUSY	-	-	-	-	Yes	Yes	-	-	-	-
	LX_MEMFREE	-	-	-	-	Yes	Yes	-	-	-	-
	LX_SYSTBLS	-	-	-	-	Yes	Yes	-	-	-	-
	LX_PAGING	-	-	-	-	Yes	Yes	-	-	-	-
	LX_CPUQUEUE	-	-	-	-	Yes	Yes	-	-	-	-
	LX_MEMORY	-	-	-	-	Yes	Yes	-	-	-	-
	AX_DISKBUSY	-	-	-	-	-	-	Yes	Yes	-	-
	AX_KERNELPROC	-	-	-	-	-	-	Yes	Yes	-	-
	AX_PAGING	-	-	-	-	-	-	Yes	Yes	-	-
	HP_PAGING	-	-	-	-	-	-	-	-	Yes	Yes

3.2 Virtual Resource Management

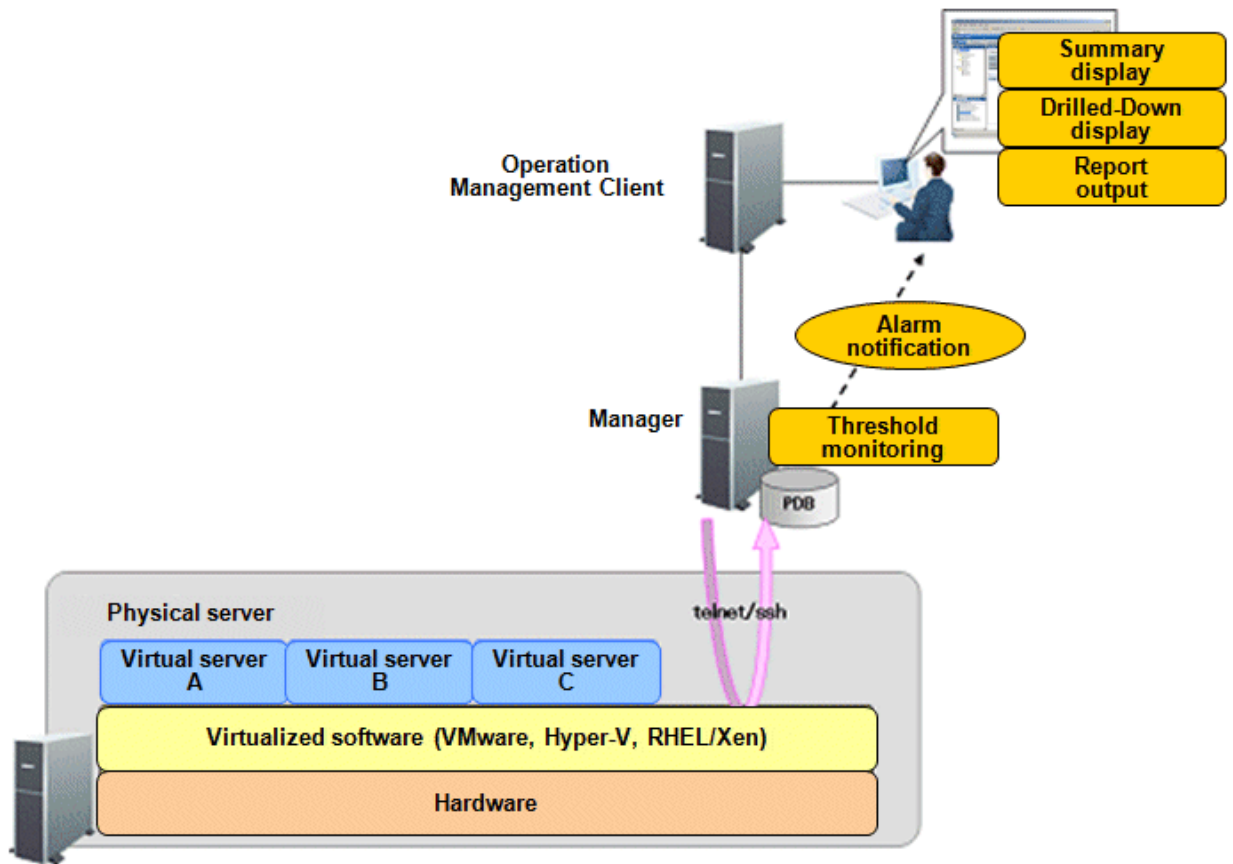
Function Overview

Virtual resource management collects performance information from physical and virtual servers of operating systems and virtualized software and centrally manages it.

By comparing the virtual server performance information collected with this function with performance information about the physical server, overarching decisions can be made to optimize the resources in the server and improve use efficiency.

- Performance information for the physical server is displayed as a report. This allows usage of the physical server's CPU, memory, and disk to be seen.

- The virtual server's performance information is stacked for display in reports for each guest. This allows usage of the CPU, memory, and disk to be seen for each guest.



Information that can be collected

- Performance information for physical servers and virtual servers is collected by using the agent for Agentless Monitoring functions from virtualized software and connecting remotely through telnet, ssh or https.

Performance information that can be collected depends on the virtualization software to be monitored.

The methods for collecting the performance information of physical servers and virtual servers and the main types of performance information collected by the monitoring virtualized software are described below.

Virtualized software	Physical server	Virtual server
VMware ESX	CPU, memory, and disk performance information is collected from VMware.	CPU, memory, and disk performance information is collected from VMware.
VMware ESXi		
Hyper-V	CPU performance information is collected from Hyper-V. Memory and disk performance information is collected from the host OS (Windows).	CPU performance information is collected from Hyper-V.
Red Hat virtualization function (Xen)	CPU, memory, and disk performance information is collected from the host OS (Linux).	CPU, memory, and disk performance information is collected from Red Hat virtualization function (Xen).

Note

- The performance information of the host OS (Windows) is also collected if you make Hyper-V the subject of monitoring.
The CPU performance information values collected from Hyper-V's host OS (Windows) are not correct, however. If it is necessary to check the CPU performance information of the physical server, look at the CPU performance information values collected from Hyper-V.
 - The performance information of the host OS (Linux) is also collected if you make the Red Hat virtualized function (Xen) the subject of monitoring.
-
- The virtual server's resources are stacked for display in a report.
 - Threshold monitoring can be performed on the different pieces of information and notifications can be sent as alarms when a monitored item exceeds a defined value.

Information Collection Differences between VMware ESX and VMware ESXi

The values collected from VMware ESX by logging in the remote console by ssh and command execution on the virtual server. It causes the delay of displaying as shown at "Notes" in "3.2.4 Display".

Meanwhile, the values collected from VMware ESXi by SOAP API through https communication. So data is displayed in real time.

Collection interval

Collection interval is 5 minutes.

Procedure

Steps for setting an agent for Agentless Monitoring to manage virtual resources are described below.

- [3.2.1 Prerequisites](#)
- [3.2.2 Settings for Monitored Servers](#)
- [3.2.3 Settings for Monitoring Servers](#)
- [3.2.4 Display](#)

3.2.1 Prerequisites

Required Software

The software required for communication between the monitoring server and the monitored server is described below.

Virtual Software	Communication Method	Software required for monitoring server	Software required for mMonitored server (agent for Agentless Monitoring)
Hyper-V	telnet	-	telnet server
VMware ESX Red Hat Virtualization function (Xen)	ssh	-	ssh server (*1)

Virtual Software	Communication Method	Software required for monitoring server	Software required for monitored server (agent for Agentless Monitoring)
VMware ESXi	https	-	-

*1: The following software is required to communicate by SSH:

- SSH V2.0 or later
 - For VMware ESX and Red Hat Virtualization function (Xen).
Please use ssh installed as a standard function.

Conditions under which collection can be performed

- VMware ESX:
The command for collecting performance information (esxtop) must be able to be used.
- VMware ESXi
HTTPS communication must be able to be used.
- Hyper-V:
The command for collecting performance information (typeperf) must be able to be used.
- Red Hat virtualization function (Xen):
The command for collecting performance information (xentop) must be able to be used.

Resource estimation

Number of connection sessions

The following explains the number of telnet/ssh connection sessions required on the monitored server so that performance information can be collected from the monitored server.

Platform of the monitored server (agent for Agentless Monitoring)	Number of telnet or ssh connection sessions
VMware ESX	1
VMware ESXi	-
Hyper-V	3
Red Hat virtualization function (Xen)	6

Note

- If the total number of connection sessions is very large, it may take some time for the DCM services/daemons of the monitoring server to start or stop.
- Communications by telnet or ssh may not be performed properly if the network status of the environment is not optimal (there are intermittent interruptions, etc.) or if the monitored server is busy. Perform monitoring in an environment with consistently reliable communications.
- The default maximum number of sessions that can be connected simultaneously with Hyper-V (Windows) telnet is "2". Therefore it will be necessary to change the maximum number of sessions that can be connected simultaneously.

Follow the steps in "3.2.2 Settings for Monitored Servers".

There is no limit to the maximum number of sessions that can be connected simultaneously by default with VMware ESX/Red Hat Virtualization function (Xen) (UNIX) ssh.

Free space on disk

The following explains the disk space required on the monitored server so that performance information can be collected from the monitored server.

- Disk space required on the monitored server: 1MB

3.2.2 Settings for Monitored Servers

- If the server to be monitored is a VMware ESX server
- If the server to be monitored is a VMware ESXi server
- If the monitored server is a Hyper-V
- If the server to be monitored is a Red Hat Virtualization function (Xen) server

If the server to be monitored is a VMware ESX server

When communicating by ssh

1. Create a user so that connections can be made remotely.
 - a. Log into the VMware ESX host directly with the VMware Client.
 - For ESX 3.5
Log into the VMware ESX host directly with the VMware Infrastructure Client.
 - For ESX 4.0
Log into the VMware ESX host directly with the VMware vSphere Client.



- For ESX 3.5
Users cannot be created if VirtualCenter is logged into. Log into the VMware ESX host directly.
 - For ESX 4.0
Users cannot be created if vCenter Server is logged into. Log into the VMware ESX host directly.
-

- b. Select the server from the pane at the left.
 - c. Click the **Users & Groups** tab and click **Users**.
 - d. Right-click on the user table and click **Add**.
 - e. The **Add New User** dialog opens.
 - f. Set the login, user name, numeric user ID (UID) and password.
 - g. Select **Grant shell access to this user**.
 - h. Input the group name for each existing group that the user is to be added to and click **Add**.
 - i. Click the **OK** button.
2. Make settings to have the SSH server start automatically.

Point

The VMware ESX SSH server is set to start automatically by default.

Refer to the VMware manual for information about how to start and set the SSH server.

3. Connect to the set server with ssh and confirm that you can log in with the created user.
4. Add the right to execute the command used to collect performance information to the created user.

Execute the following settings:

- a. Log into VMware as a superuser.
- b. Execute the visudo command and edit the sudoers file.

```
# /usr/sbin/visudo
```

- c. Add the following lines to the end of the sudoers file and save it.
The following example shows the connection account with "user1". Change to match the actual connection account.

Settings example

```
user1 ALL=(ALL) NOPASSWD: /usr/bin/esxtop
user1 ALL=(ALL) NOPASSWD: /usr/sbin/esxcfg-vmhbadevs
user1 ALL=(ALL) NOPASSWD: /usr/sbin/vdf
user1 ALL=(ALL) NOPASSWD: /usr/sbin/esxcfg-nics
user1 ALL=(ALL) NOPASSWD: /usr/sbin/esxcfg-vswitch
user1 ALL=(ALL) NOPASSWD: /bin/egrep
user1 ALL=(ALL) NOPASSWD: /usr/sbin/esxcfg-scsidevs
```

- d. Log into the connection account and execute the "sudo -l" command.

```
$ sudo -l
```

Execution result example

```
$ sudo -l
User user1 may run the following commands on this host:
(ALL) NOPASSWD: /usr/bin/esxtop
(ALL) NOPASSWD: /usr/sbin/esxcfg-vmhbadevs
(ALL) NOPASSWD: /usr/sbin/vdf
(ALL) NOPASSWD: /usr/sbin/esxcfg-nics
(ALL) NOPASSWD: /usr/sbin/esxcfg-vswitch
(ALL) NOPASSWD: /bin/egrep
(ALL) NOPASSWD: /usr/sbin/esxcfg-scsidevs
```

If the server to be monitored is a VMware ESXi server

1. Create a user so that connections can be made remotely.
 - a. Use VMware vSphere Client to log in directly to the VMware ESXi server using the system administrator account.

Note

Users cannot be created if vCenter Server is logged into. Log into the VMware ESXi server directly.

- b. Select the server from the pane at the left.
 - c. Click the **Users & Groups** tab and click **Users**.
 - d. Right-click on the user table and click **Add**.
 - e. The **Add New User** dialog opens.
 - f. Set the login, user name, numeric user ID (UID) and password.
 - g. Select the **Group membership** group, then select the **users** group from the list and click **Add**.
 - h. Click **OK**.
2. Assign read permission to the created user.
 - a. Select the server from the left pane.
 - b. Right-click the server and then click **Add Permission** - the **Assign Permissions** dialog box opens.
 - c. Click **Add** - the **Select Users** dialog box opens.
 - d. From the list, select the user created in step 1, then click **Add** and **OK**.
 - e. Select **Read-Only** as the role of the added user, then select the [Propagate to Child Objects] check box and click **OK**.
 3. Check the user settings.
 - a. Select the server from the left pane.
 - b. Click the **Permissions** tab, and make sure that the created user is displayed in the list.

If the monitored server is a Hyper-V

1. Create a user so that connections can be made remotely.
Do not specify "User must change password at next logon" for the user.
2. Add a user to the groups necessary for connecting remotely and collecting information ("TelnetClients" group and "Performance Monitor Users" group).

Follow these steps to make the settings.

- a. Create a "TelnetClients" local group.
 1. Open Computer Management.
 2. In the console tree, expand Local Users and Groups and click Groups.
 3. If the "TelnetClients" group already exists in the list, skip the next step and go on to "b. Add user to the "TelnetClients" group".
 4. Right-click on Groups, and click New Group.
 5. In the New Group dialog, enter "TelnetClients". Add descriptions as required.
 6. If the user has already been created, click Add and enter the user name in the Select Users, Computers, or Groups dialog.
 7. Click Create.
- b. Add user to the "TelnetClients" group.
 1. Open Computer Management.
 2. In the console tree, expand Local Users and Groups and click Groups.
 3. Double-click the "TelnetClients" local group.
 4. Click Add.

5. Follow the instructions in the Select Users, Computers, or Groups dialog to add the user to the "TelnetClients" group and click OK.
- c. Add user to the "Performance Monitor Users" group.
 1. Open Computer Management.
 2. In the console tree, expand Local Users and Groups and click Groups.
 3. Double-click the "Performance Monitor Users" group.
 4. Click Add.
 5. Follow the instructions in the Select Users, Computers, or Groups dialog to add the user to the "Performance Monitor Users" group and click OK.

Note

- From a security point of view, it is not recommended to use a user belonging to the Administrators group.
- To open Computer Management, from the Windows **Start** menu, click **Control Panel** and double-click **Administrative Tools >> Computer Management**.
- When entering the group name, be sure to spell "TelnetClients" as shown.
- Users cannot logon after creating a "TelnetClients" group until the "Telnet Server" service is stopped and then started again.

3. Make settings to have the "Telnet" service start automatically.

Enable the "Telnet Server" function and set the "Telnet" service to start automatically.

Note

The "Telnet Server" function is disabled by default.

The "Telnet" service is also set to not start automatically by default.

The following describes how to enable the "Telnet Server" function and set the "Telnet" service to start automatically.

- a. Start the Windows **Server Manager**.
- b. Select **Features** in the tree on the left and click **Add Features** in the window on the right.
- c. Select **Telnet Server** and click **Next**.
- d. Click the **Install** button.

When installation is finished, start Windows **Services**, and follow the steps below to have the Telnet service start automatically.

- a. Open Computer Management.
- b. In the console tree, click Services.
- c. Double-click the "Telnet" service.
- d. Make the startup type Automatic, change the service status to Start, and click OK.

4. Change the maximum number of sessions that can be connected simultaneously with the "Telnet" service.

The default maximum number of sessions that can be connected simultaneously with the "Telnet" service is "2". Set the maximum number of sessions with consideration for the number of sessions required shown in "[Number of connection sessions](#)".

Use the Windows "tntadmn" command to change the maximum number of sessions that can be connected simultaneously.

```
tntadmn config maxconn=<maximum number of connection sessions>
```

Note

This needs to be run with administrator privileges. To do so, from the **Start** menu, select **All Programs, Accessories**, then right-click **Command Prompt** and select **Run as administrator**. Now run the commands described below in the command prompt that appears.

```
tntadmn config maxconn=<maximum number of connection sessions>
```

5. Logon to the computer with the new user.

Note

The user profile of the connecting user is necessary for connecting remotely and collecting information. For this reason, logon to the Windows computer as the connecting user.

6. Connect to the set server with telnet and confirm that you can log in with the created user.

If the server to be monitored is a Red Hat Virtualization function (Xen) server

1. Create a user so that connections can be made remotely.
2. Make settings to have the ssh daemon start automatically.

Install SSH if it is not already installed.

Refer to the ssh manual for information about how to install and start the daemon.

3. Connect to the set server with ssh and confirm that you can log in with the created user.
4. Add the right to execute the command used to collect performance information to the created user.

Execute the following steps:

- a. Login as a superuser to the Linux server where the Red Hat Virtualization function is operating.
- b. Execute the visudo command and edit the sudoers file.

```
# /usr/sbin/visudo
```

- c. Add the following lines to the end of the sudoers file and save it.

The following example shows the connection account with "user1". Change to match the actual connection account.

Settings example

```
user1 ALL=(ALL) NOPASSWD: /usr/sbin/xentop
```

- d. Log into the connection account and execute the "sudo -l" command.

```
$ sudo -l
```

Execution result example

```
$ sudo -l
User user1 may run the following commands on this host:
(ALL) NOPASSWD: /usr/sbin/xentop
```

3.2.3 Settings for Monitoring Servers

Steps for setting the monitoring server are described below.

1. [Definition method](#)
2. [Setup](#)

3.2.3.1 Definition method

Define in the following order:

- [Connection account configuration file](#)
- [Remote monitoring configuration file](#)

3.2.3.1.1 Creating a connection account configuration file

When using VMware ESX/Hyper-V/Red Hat Virtualization function (Xen)

Define the settings for telnet/ssh communication between the monitoring server and the monitored server.
Edit the connection account configuration file (remoteAccount.txt).

Refer to "[3.1.3.1.1 Connection account configuration file](#)" for setting details.

When using VMware ESXi

Define the settings for https communication between the monitoring server and the monitored server.

Edit the connection account configuration file (remoteAccount.txt).

Storage location

The file is stored in the following location:

Windows

```
<variable file storage directory>\control\remoteAccount.txt
```

UNIX

```
/etc/opt/FJSVssqc/remoteAccount.txt
```

Edit the above file using the definition method described below.

Definition method

This is an ini format file.

Set the sections by connection account groups for communication between the monitoring server and the monitored server.

The method of definition depends on the communication method. Edit to match the communication method.

- 1.

No	Item	Mandatory/ optional	Format	Description
-	[ACCOUNT]	Mandatory	63 characters or fewer, using alphanumerics, hyphens (-), periods (.), and hash symbols (#) only	Use an account group name for the section name. Make it so that the section name is a unique character string.
1	CONNECTTYPE	Mandatory	HTTPS	Set the connection method when connecting to the VMware ESXi. Set to "HTTPS" as this is for https connection.
2	USER	Mandatory	63 characters or fewer The following characters cannot be used: V[]: <>+=,?*@.	Set the login account for connection.
3	PASSWORD	Mandatory	Character string generated with genpwd (*1)	Set the password for connection.

*1: Refer to "[A.6 genpwd \(password encryption command\)](#)" for details about how to use the genpwd command to generate encrypted passwords.

Example of definition

The following is an example of definitions when using VMware ESXi.

```
[ESXi-Account1]
CONNECTTYPE=HTTPS
USER=httpsuser
PASSWORD=C5sJGBE3ONs=
```

3.2.3.1.2 Creating remote monitoring configuration file

Define the settings for the virtual server.

Edit the remote monitoring configuration file (remoteAgent.txt).

File storage location

Windows

```
<variable file storage directory>\control\remoteAgent.txt
```

UNIX

```
/etc/opt/FJSVssqc/remoteAgent.txt
```

File format

ini file format

Setup items

Set sections for each server to be monitored.

No	Item	Mandatory/ optional	Format	Description
-	[HOSTNAME]	Mandatory	63 characters or fewer, using alphanumerics, hyphens (-), periods (.), and hash symbols (#) only	Set an optional section name as the section name. Make it so that the section name is a unique character string. It is recommended to use the host name.
1	HOSTNAME	Mandatory	63 characters or fewer, using alphanumerics, hyphens (-), periods (.), and hash symbols (#) only	Specify the IP address or host name used for connection to the monitored server.
2	DISPLAYNAME	Any	63 characters or fewer, using alphanumerics, hyphens (-), periods (.), and hash symbols (#) only	Specify the host name displayed in the SQC console. * HOSTNAME becomes the host name if this is not specified.
3	VMTYPE	Any	VMWARE ESXI HYPERV XEN	Type of virtual server of the monitored host. VMWARE: VMware ESX ESXI: VMware ESXi HYPERV: Hyper-V XEN: With the Red Hat virtualization function (Xen)
4	ACCOUNT	Mandatory	63 characters or fewer, using alphanumerics, hyphens (-), periods (.), and hash symbols (#) only	Specify a connection account for communicating with the monitored server. Specify the section name of the user group set in remortAccount.txt (Connection account configuration file).
5	CONNECTION	Any	ON or OFF	Set ON/OFF for monitoring. Specify "OFF" to stop monitoring. * Set to "ON" if this is not specified.

Example of definition

The following is an example of definitions if the virtual server is a VMware ESX, VMware ESXi, Hyper-V, or Red Hat Virtualization function (Xen) server

```
# If the monitoring server is a VMware ESX server:
[192.168.1.1]
HOSTNAME=192.168.1.1
DISPLAYNAME=vmware-host1
VMTYPE=VMWARE
ACCOUNT=SSH-ACCOUNT1
```



```
# If the monitoring server is a VMware ESXi server:
[192.168.1.2]
HOSTNAME=192.168.1.2
DISPLAYNAME=esxi-01
VMATYPE=ESXI
ACCOUNT=ESXi-Account1

# If the monitoring server is a Hyper-V server:
[host2]
HOSTNAME=host2
VMATYPE=HYPERV
ACCOUNT=TELNET-ACCOUNT2

# When the monitoring server is a Red Hat Virtualization function (Xen) server and is not to
be monitored:
[xen-host3]
HOSTNAME=192.168.1.3
DISPLAYNAME=host3
VMATYPE=XEN
ACCOUNT=SSH-ACCOUNT3
CONNECTION=OFF
```

3.2.3.2 Setup

Refer to "[A.1 Server Resource Information Collection Policy Creation Command](#)" and execute sqcRPolicy and sqcSetPolicy.

Point

Perform a check of the text entered into the definitions files during setup. Start the service to check that connection can be made to the monitored server. Warning messages are output to the event log when performance information collection is executed on monitored servers that cannot be connected. Refer to Section 5.1, "Common Messages" in the Reference Guide and take the steps described.

If definitions files (Connection account configuration file and remote monitoring configuration file) have errors, monitored servers that have the errors will not be managed.

When sqcSetPolicy is executed, the following message is output for monitored servers that have been excluded from management due to errors in the definition.

```
(Warning) : <Install-less Agent> ignored section name[section name]
```

The section name defined in "remote monitoring configuration file" is output to "section name".

The following message is also output if any errors are found in a definitions file.

```
(Warning) : <Install-less Agent> There is an error in definition.
Please confirm the file (file name).
```

The following is output to "file name".

Windows

```
<variable file storage directory>\log\setpolicy_error.log
```

UNIX

```
/var/opt/FJSVssqc/setpolicy_error.log
```

If this message appears, check the file content, correct the definitions files (Connection account configuration file and remote monitoring configuration file) according to the message in the file, and then setup again. Refer to Section 1.1.3, "sqcSetPolicy (Policy Application Command)" in the *Reference Manual* for details about messages output to the file.

Note that collection policy setup must be passed to the console. Refer to Section 1.2.2.3, "Agents" in the *User's Guide (Console Edition)* and use the Agent Settings window to collect configuration information.

Note

- It takes about 15 to 20 minutes for this information to appear in the console's "UnregisteredAgents folder" after starting the Manager/Proxy Manager service.
If it does not appear, look in the Manager/Proxy Manager's event log/syslog to see if a message has been output.

- It is necessary to create directories and files (needed to carry out monitoring) on the server to be monitored when managing with an agent for Agentless Monitoring.

Directories and files are created in the following location:

- If the monitored server is a Hyper-V:
 - When communicating by telnet
%USERPROFILE%\SQC_TEMP directory
%USERPROFILE% : Path name of the user profile folder
- If the server to be monitored is a VMware or Red Hat Virtualization function (Xen) server:
Home directory of the user

The created directory name is as follows:

```
dsa_temp_***
```

Do not delete the above directory during monitoring. Performance information will not be collected if this directory is deleted. If this directory is deleted by accident, restart the Manager/Proxy Manager service.

Delete the above directory to exclude the server from monitoring.

3.2.4 Display

Virtual server performance information collected by an agent for Agentless Monitoring can be displayed as follows.

VMware ESX/VMware ESXi

- Summary

Performance information can be displayed by selecting the "VMware(host)" node (VMware(Physical)Monitor) and "VMware(guest piling)" node (VMware(Virtual)StackMonitor) in the Summary tree.

- Details

Performance information can be displayed by selecting the VMware node in the Detailed tree.

- Reports

Full system inspection analysis/report
Categorized diagnostic analysis/report
Detailed analysis/report

Hyper-V

- Summary

Performance information can be displayed by selecting the "Server resource" node (ServerMonitor), "Hyper-V(host)" node (HyperV(Physical)Monitor), and "Hyper-V(guest piling)" node (HyperV(Virtual)StackMonitor) in the Summary tree.

- Details

Performance information can be displayed by selecting the Windows node and Hyper-V node in the Detailed tree.

- Reports

Full system inspection analysis/report
Categorized diagnostic analysis/report
Detailed analysis/report



Note

The performance information of Windows is also displayed if you make Hyper-V the subject of monitoring.

The following CPU performance information values collected from Hyper-V's host OS (Windows) are not correct, however.

- CPU Usage for the ServerMonitor in Summary
- CPUBUSY (WIN_CPUBUSY) information for Windows in Drilled-Down
- CPU and WIN_CPUBUSY related information for Windows in Report
- If it is necessary to check the CPU performance information of the physical server, look at the CPU performance information values collected from Hyper-V.
- CPU Usage for HyperV(Physical)Monitor in Summary
- HV_CPU information for Hyper-V in Drilled-Down
- CPU and HV_CPU related information for Hyper-V in Report

With the Red Hat virtualization function (Xen)

- Summary

Performance information can be displayed by selecting the "Server resource" node (ServerMonitor) and "Xen(guest piling)" node (Xen(Virtual)StackMonitor) in the Summary tree.

- Details

Performance information can be displayed by selecting the Linux node and Xen node in the Detailed tree.

- Reports

Categorized diagnostic analysis/report
Detailed analysis/report

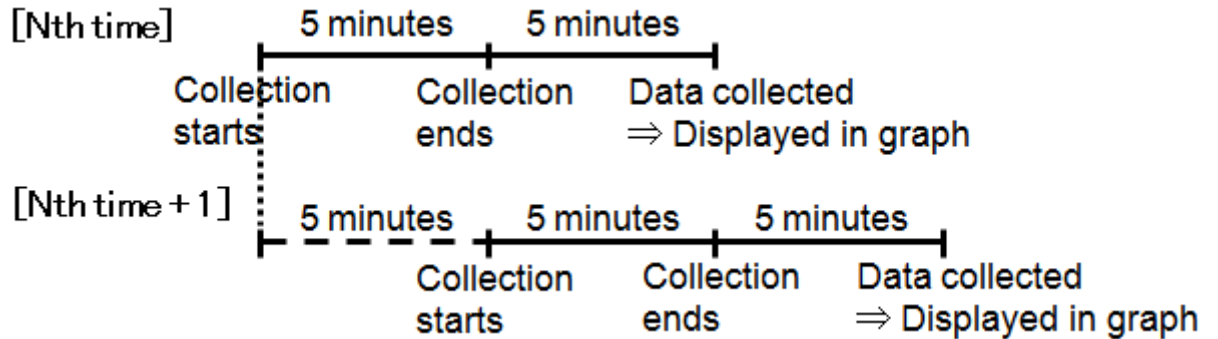


Note

The performance information of Linux is also displayed if you make the Red Hat virtualized function (Xen) the subject of monitoring.

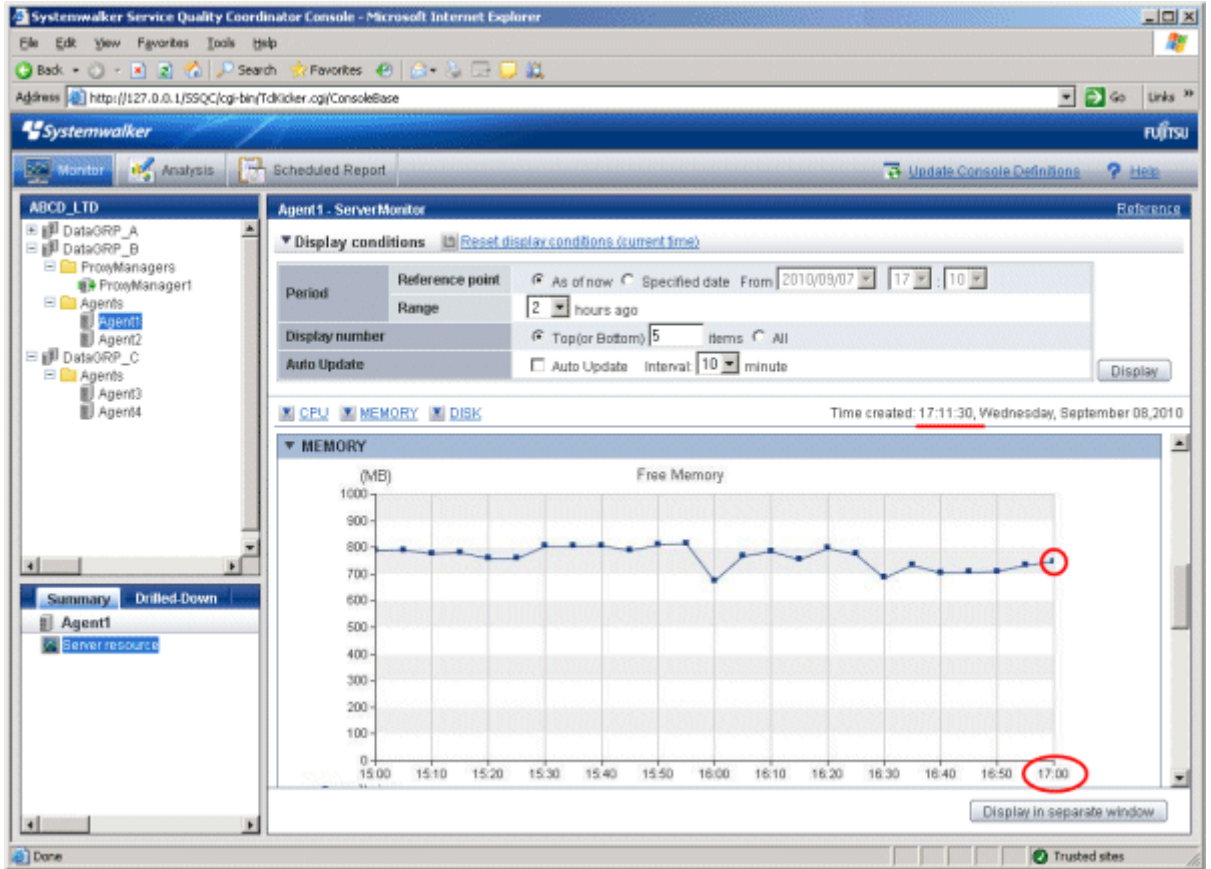
 Note

- When this data is to be displayed in the summary window, it will take 10 to 15 minutes for the data to appear. This is due to the way that the data is collected by the agent for Agentless Monitoring, as described below.



Data for 17:00, for example

17:00	Begin collection
17:05	End collection
17:10	<p>Manager/Proxy Manager collects the data</p> <p>This data is displayed in the console as the data for 17:00. (Data display is based on the time that data collection starts. The data value for 17:00 is the average of data collected between 17:00 and 17:05.</p> <p>This state continues for the next five minutes (until about 17:15) until performance data is next collected.</p>



- The first data will appear 15 to 20 minutes after starting the Manager/Proxy Manager service because the script is sent to the monitored server at the timing of the first collection.
- The values collected from VMware ESXi by SOAP API through https communication. So data is displayed in real time.



Chapter 4 Managing End User Response

This chapter explains how to manage end user response with Browser Agent.

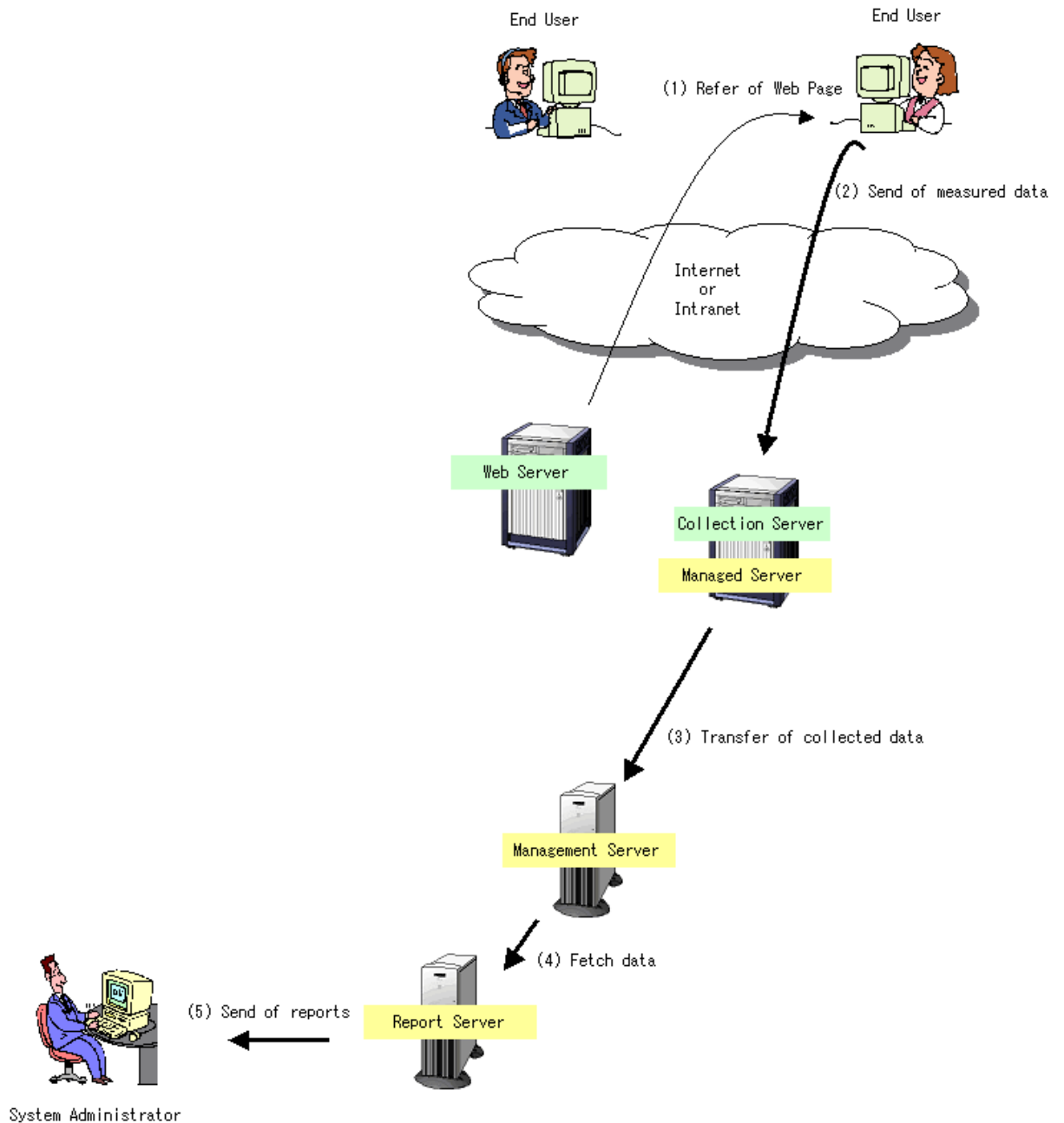
- [4.1 Overview of Measurements](#)
- [4.2 Environment Settings](#)
- [4.3 Installing a Browser Agent](#)
- [4.4 Supplementary Information Relating to Product Deployment](#)
- [4.5 Supplementary Information Relating to Browser Agent Packages](#)
- [4.6 Display](#)

4.1 Overview of Measurements

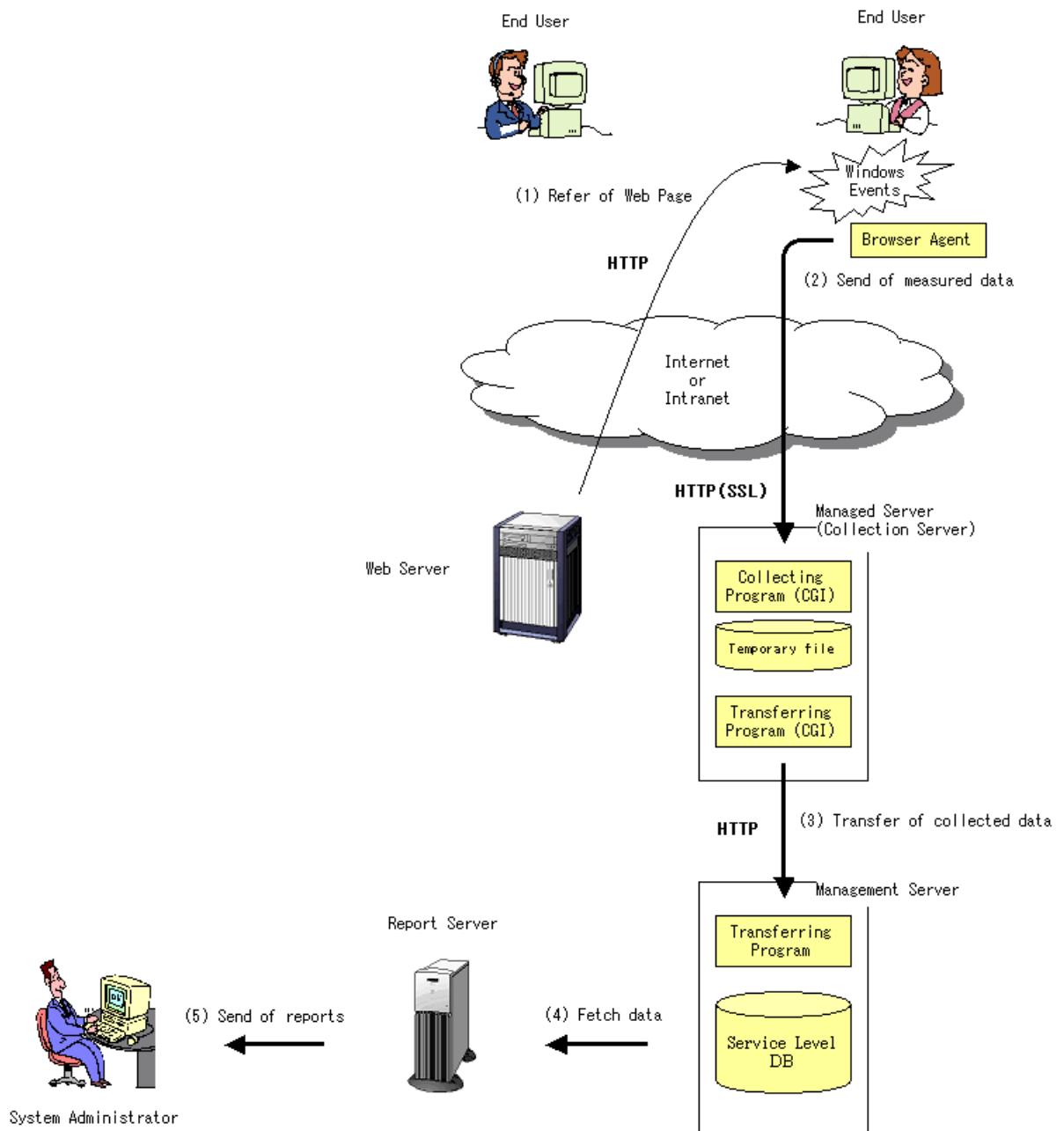
The diagram shown on the following page provides an outline of how end user response is measured. When an end user uses a browser to view a Web page (step 1), the end user response measurement function collects data and sends it to the Proxy Manager (the collection server) (step 2). The data is then sent to the Manager and converted into database form (step 3).

When the system administrator requests data from the Manager, the operation management client extracts data from the Manager (step 4), processes it for viewing and displays it to the system administrator (step 5).

End user response information can also be sent directly to the Manager without traveling via the Proxy Manager.



During this process, the internal operation of the Manager, the Proxy Manager and the end user machine is as shown in the following diagram. The yellow areas of the diagram are the components of the end user response measurement function. Operation 1 in the diagram occurs when the Browser Agent, which is monitoring Windows events, detects that the user has finished viewing a Web page and sends the collected data to the Proxy Manager (collection server). Operation 3 involves transferring the collected data from the Proxy Manager to the Manager and converting it into database form.



Point

- In the case of a Web system within a company, a Browser Agent is installed on the machine of the end user of a business service, and then the work efficiency of the business service (i.e., the response) can be managed based on data relating to the actual system response felt by the end user.
- In the case of a Web system used to conduct electronic commerce between businesses (BtoB), a Browser Agent is installed on the business terminal of the partner company, and customer satisfaction levels (the response) given by the services of one's own company can be managed based on data relating to the actual system response felt by the users at the partner company.
- In the case of a Web system used to conduct electronic commerce aimed at consumers (BtoC), a Browser Agent is installed on the machine of the member customer, and customer satisfaction levels (the response) given by the services of one's own company can be managed based on data relating to the actual system response felt by each customer.

4.2 Environment Settings

Environment settings are specified in the following order:

- [4.2.1 Setting up the temporary file environment of the collection server](#)
- [4.2.2 Setting up the CGI environment of the collection server](#)
- [4.2.3 Creating and applying collection policies](#)

4.2.1 Setting up the temporary file environment of the collection server

Privileges required for execution

[Windows]

The privileges of a user belonging to the "Administrators" group are required to make these settings.

[UNIX]

System administrator (superuser) privileges are required to make these settings.

The collection program (CGI) and the transfer program (CGI) are executed using the user permissions for CGI. For this reason, access permissions associated with the location of temporary files (the collection directory included in the installation materials for Manager or Proxy Manager) must be appropriate for the user permissions for CGI.

If the access permissions for the installation materials have been collectively changed to improve security, log in to the system with Administrator authority and use the following procedure to return the access permissions of the collection directory to the state existing immediately after installation. (The security risk will increase.)

[Windows]

```
C:\> installation directory\bin\sqlSetFileSec.exe -u variable file directory\wslm
```

[UNIX]

```
# chmod 777 /var/opt/FJSVssqc/wslm
```

4.2.2 Setting up the CGI environment of the collection server

From a Web server on a collection server, define "SQL" as a virtual directory corresponding to the following directory:

[Windows]

```
Installation directory\www\
```

[UNIX]

```
/opt/FJSVssqc/www/
```

In addition, add the right to execute CGI programs to the following subdirectory:

[Windows]

```
Installation directory\www\cgi-bin\
```

[UNIX]

```
/opt/FJSVssqc/www/cgi-bin/
```

 See

Refer to Chapter 5, "Setting up Communication Environment" in the Installation Guide for concrete examples. Note that the above settings are not required if a virtual directory has already been defined.

 Note

If the collection server is a Manager and the Manager operates in a cluster system, perform the above settings on both the active and standby servers. (Cluster system operation is only available with the Enterprise Edition.)

 Point

SSL can be used in HTTP communications between the Browser Agent and the collection server. If information is to be collected via the Internet, the use of SSL is recommended to prevent information from being leaked to a third person as it travels.

To use SSL, define a separate virtual directory for SSL with respect to the above directory.

Also, client authentication can be performed if SSL is used for HTTP communications between Browser Agents and the collection server. Define the virtual directory used for SSL so that client authentication can be performed.

4.2.3 Creating and applying collection policies

Define the name of the site to be managed by the Browser Agent in the response information section (the <WebSite> tag) of the response and managed object configuration information file (ServiceConf.xml).

Refer to "[Chapter 6 Response and Managed Object Configuration Information \(ServiceConf.xml\)](#)" for information about how to make this definition.

4.3 Installing a Browser Agent

Use the Browser Agent Installation Package (hereafter referred to as "the package") with built-in measurement conditions to install the Browser Agent in the following order. All operations apply to Windows systems.

 Note

On operating systems where the Browser Agent operates, apply the security update KB973544 provided by Microsoft (refer to the Microsoft website for information).

- The Browser Agent will not start if the update is not applied.

- The update is provided as three types, but you need to apply "vcredist_x86.exe", regardless of the operating system that runs the Browser Agent.
-

Privileges required for execution

[Windows]

For Windows 2000: The privileges of a user belonging to the "Administrators" group are required to make these settings.

For Windows XP: The privileges of a user belonging to the "Administrators" group are required to make these settings.

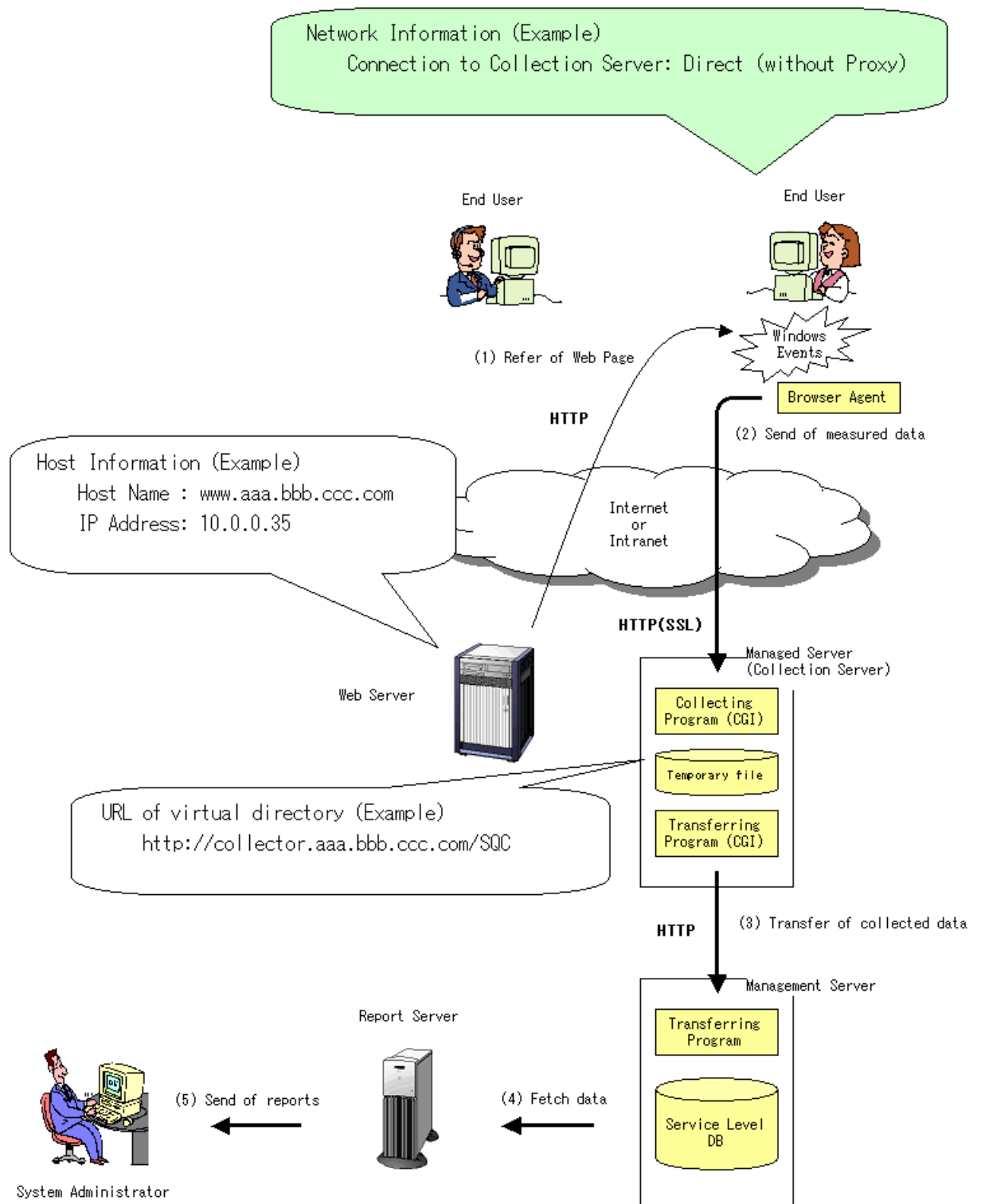
For Windows Vista: The privileges of a user belonging to the "Performance Monitor Users" group are required to make these settings.

For Windows 7: The privileges of a user belonging to the "Performance Monitor Users" group are required to make these settings.

Procedure

- [4.3.1 Creating the package](#)
- [4.3.2 Installation conditions](#)
- [4.3.3 Installing the package](#)
- [4.3.4 Starting Browser Agents](#)
- [4.3.5 Upgrading and reinstalling Browser Agent](#)
- [4.3.6 Uninstalling Browser Agent](#)

For illustration purposes, the method used to specify the settings shown in the diagram shown below will be explained in the following sections.



4.3.1 Creating the package

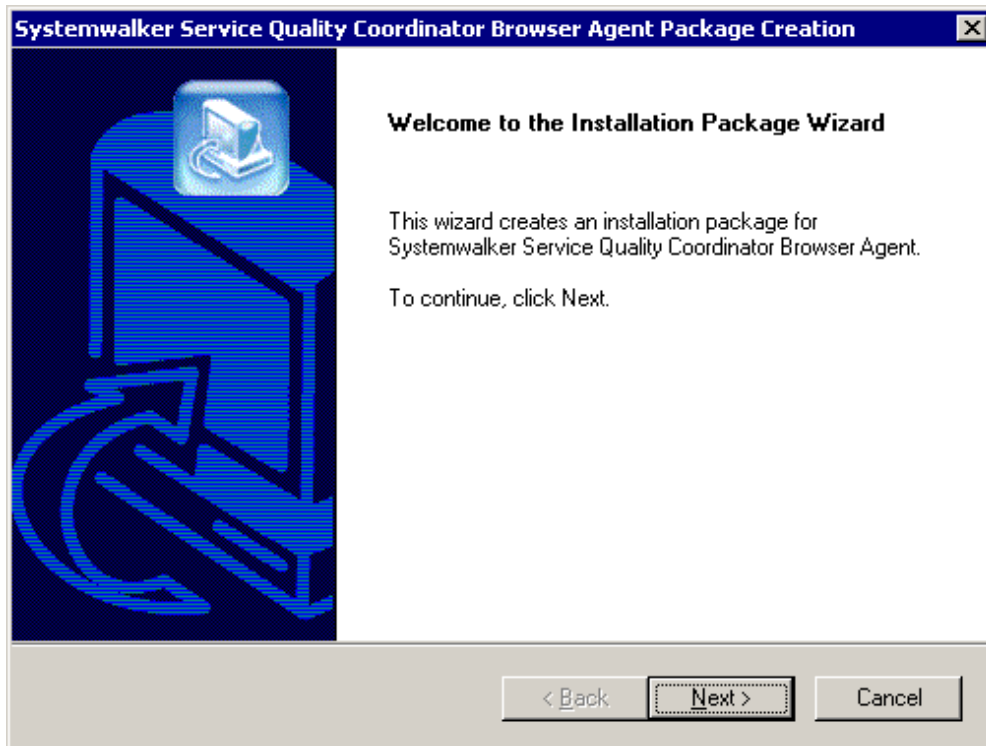
First, use the following procedure to start the packager.

1. Log in to the Windows machine, and insert the product CD-ROM (Client/Documentation).
2. Execute the following file:

CD-ROM drive:\tools\wslm\wslmpack.exe

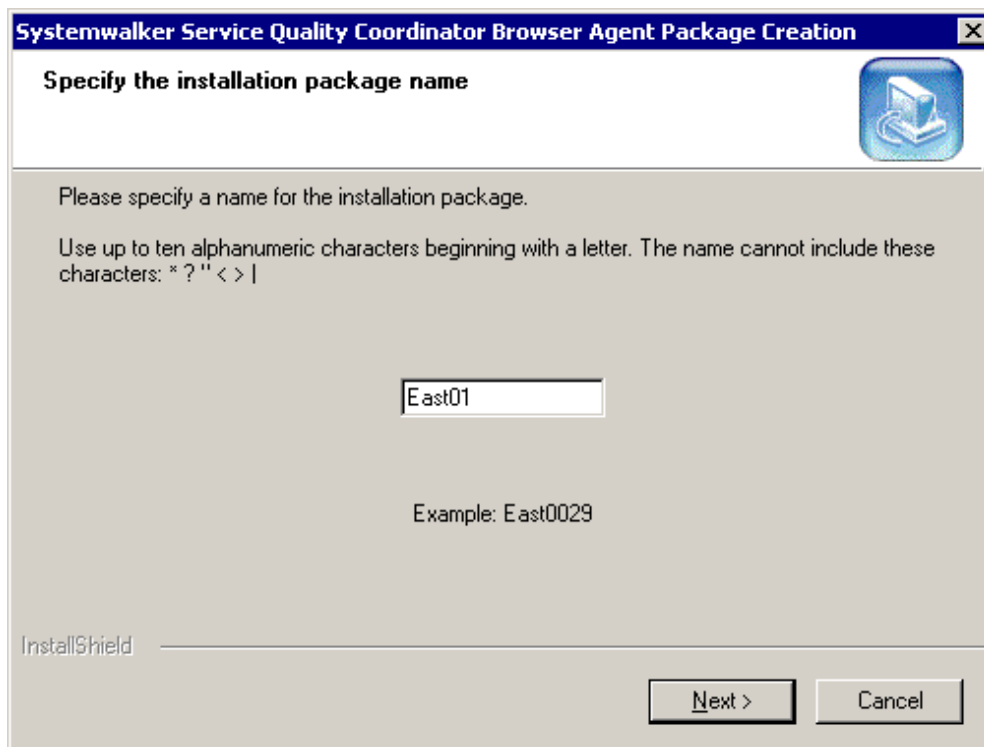
To perform the example settings shown in the previous diagram, operations will proceed as shown in the following screen shots.

The Package Creation window



Click the **Next** button.

Specify the installation package name



Systemwalker Service Quality Coordinator Browser Agent Package Creation [X]

Specify the installation package name

Please specify a name for the installation package.

Use up to ten alphanumeric characters beginning with a letter. The name cannot include these characters: * ? " < > |

East01

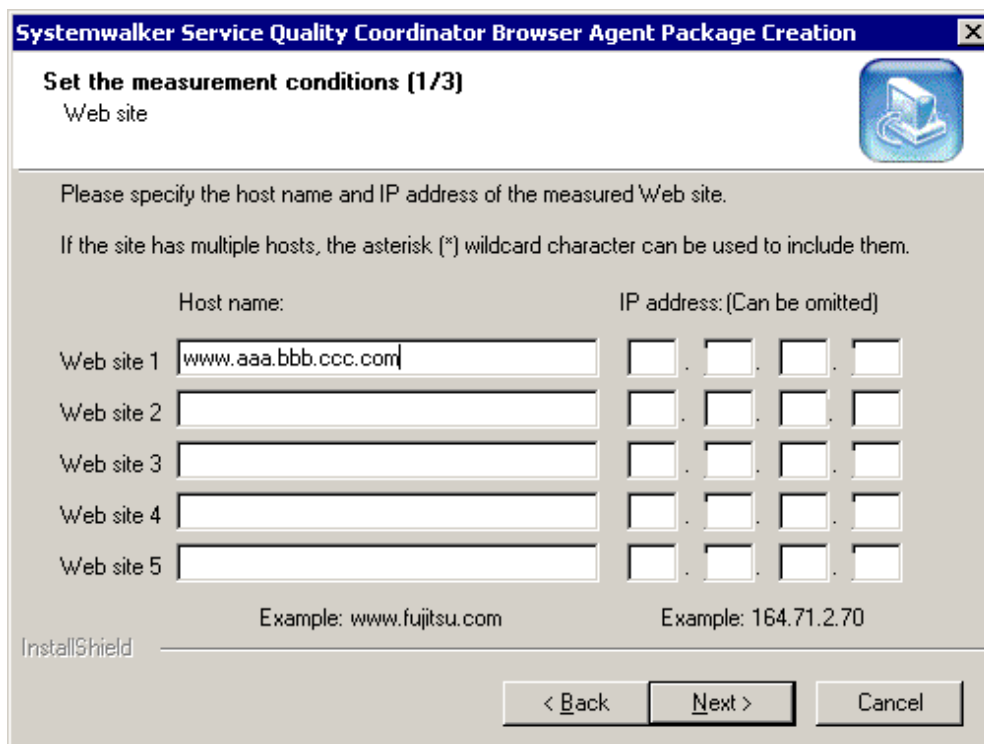
Example: East0029

InstallShield

Next > Cancel

Here, specify "East01" as the package name.

Set the measurement conditions(1/3)



Systemwalker Service Quality Coordinator Browser Agent Package Creation [X]

Set the measurement conditions (1/3)

Web site

Please specify the host name and IP address of the measured Web site.

If the site has multiple hosts, the asterisk (*) wildcard character can be used to include them.

Host name:	IP address: (Can be omitted)
Web site 1 <input type="text" value="www.aaa.bbb.ccc.com"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Web site 2 <input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Web site 3 <input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Web site 4 <input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Web site 5 <input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

Example: www.fujitsu.com Example: 164.71.2.70

InstallShield

< Back Next > Cancel

Web sites of the measuring object can be specified up to five.

The following sites are observed when setting it as stated above.

Site	Host name	IP address
Site 1	www.aaa.bbb.ccc.com	*.*.*.*

Set the measurement conditions(2/3)

Systemwalker Service Quality Coordinator Browser Agent Package Creation [X]

Set the measurement conditions (2/3)
End user information

End user information can be added to the measured data. Please specify any end user information to be added.

Package name
 End user input (E-mail address)
 End user input (User name and company name (Form: User@Company))
 End user machine attribute (IP address)
 End user machine attribute (IP address as viewed from the collection server)

InstallShield

< Back Next > Cancel

Refer to "[the Customize Input Content](#)" when you select the following.

- End user input (E-mail address)
- End user input (User name and company name (Form: User@Company))

When the report is made, end user information enables the each end user's total. Refer to "[4.5 Supplementary Information Relating to Browser Agent Packages](#)" for details.

Set the measurement conditions(3/3)

Systemwalker Service Quality Coordinator Browser Agent Package Creation

Set the measurement conditions (3/3)
Collection server

Please specify the URL of the virtual directory allocated to Systemwalker Service Quality Coordinator at the collection server of measured data.

Example: https://collector.www.fujitsu.com/SQC/

InstallShield

< Back Next > Cancel

Specify the URL for the virtual directory that has been allocated to Systemwalker Service Quality Coordinator.

Set up client authentication

Systemwalker Service Quality Coordinator Browser Agent Package Creation

Set the license agreement file

Please specify the necessary information for client authentication.

Client authentication will be performed.

Please specify the path to the client certificate file (X.509).

Refer...

Please specify the path to the client certificate's private key file.

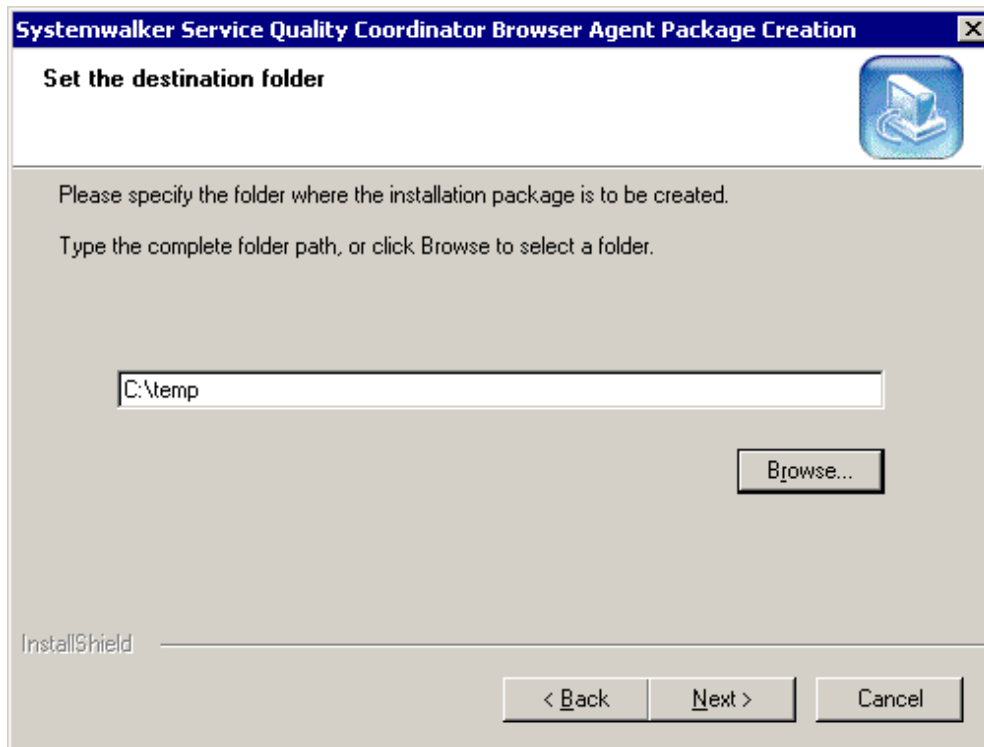
Refer...

InstallShield

< Back Next > Cancel

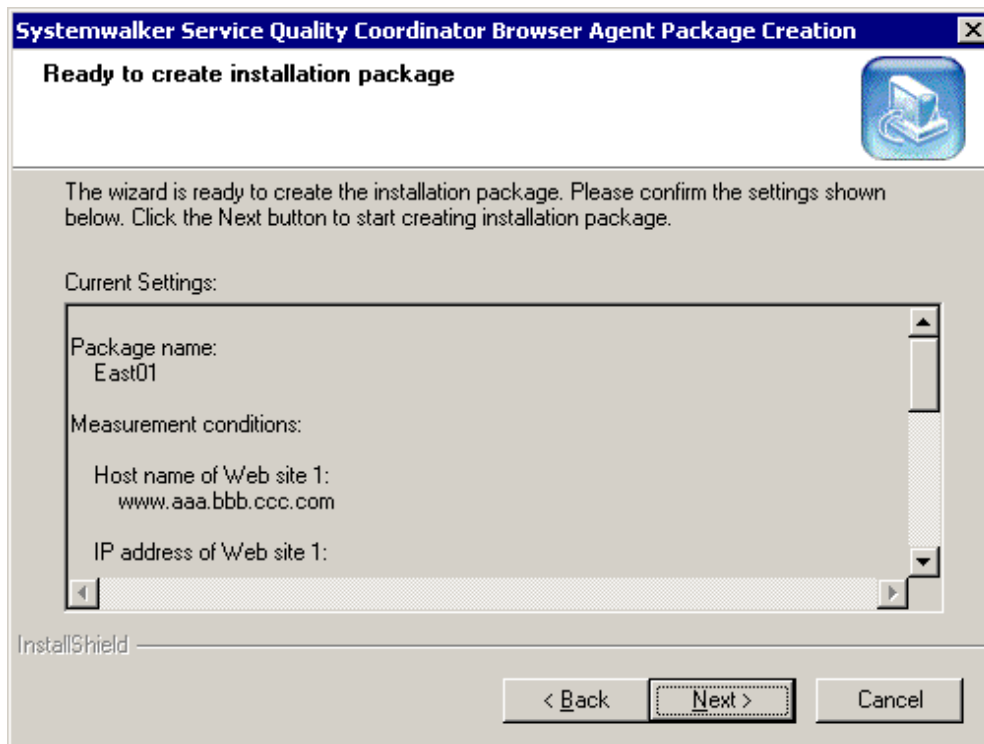
To use client authentication, specify the client certificate file using an absolute path specification, and then specify the private key file for the client corresponding to the client certificate file.

Set the destination folder



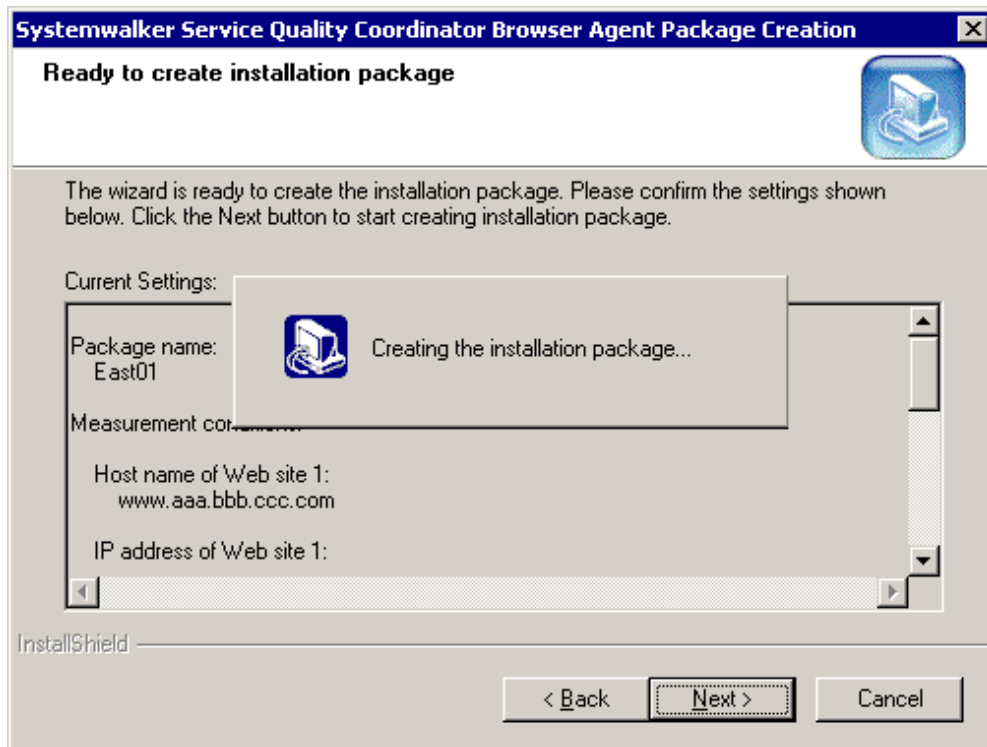
Here, specify "C:\temp" as the destination folder where the installation package is to be created.

Start creating the installation package (confirm the settings)

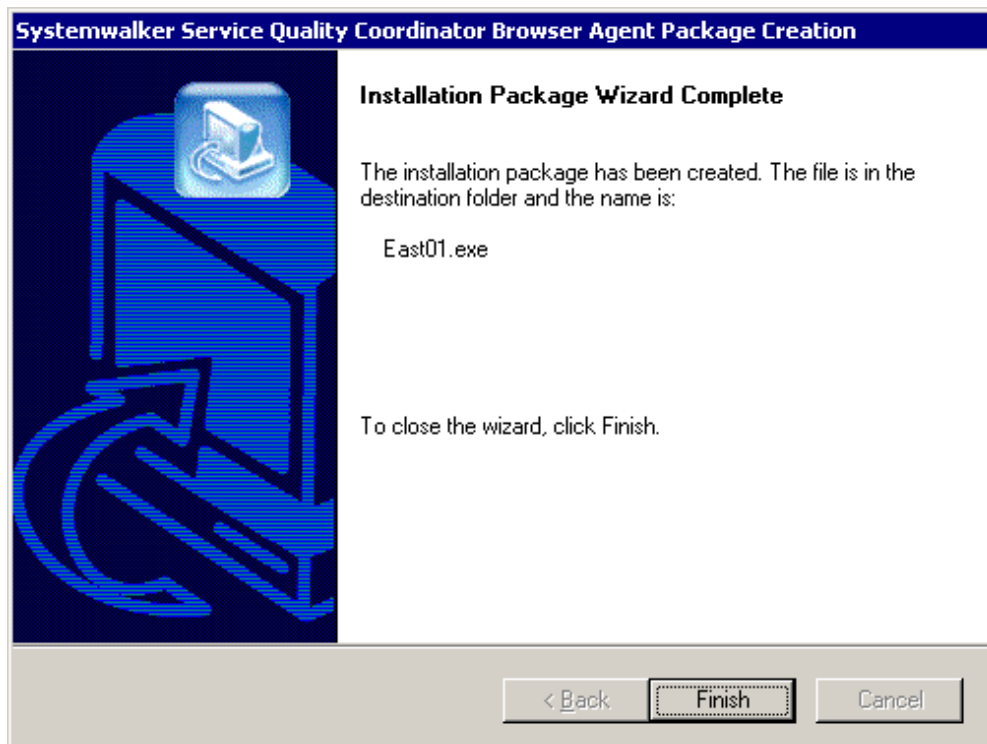


Check the settings for the package, and then click the **Next** button.

Starting to create the installation package



Installation package has been created



Note

Even if a package is created successfully, it will not measure correctly if any of the specified measurement conditions is incorrect. After creating a package, refer to "4.3.3 Installing the package" and install the package to check if it can measure correctly according to the specified measurement conditions.

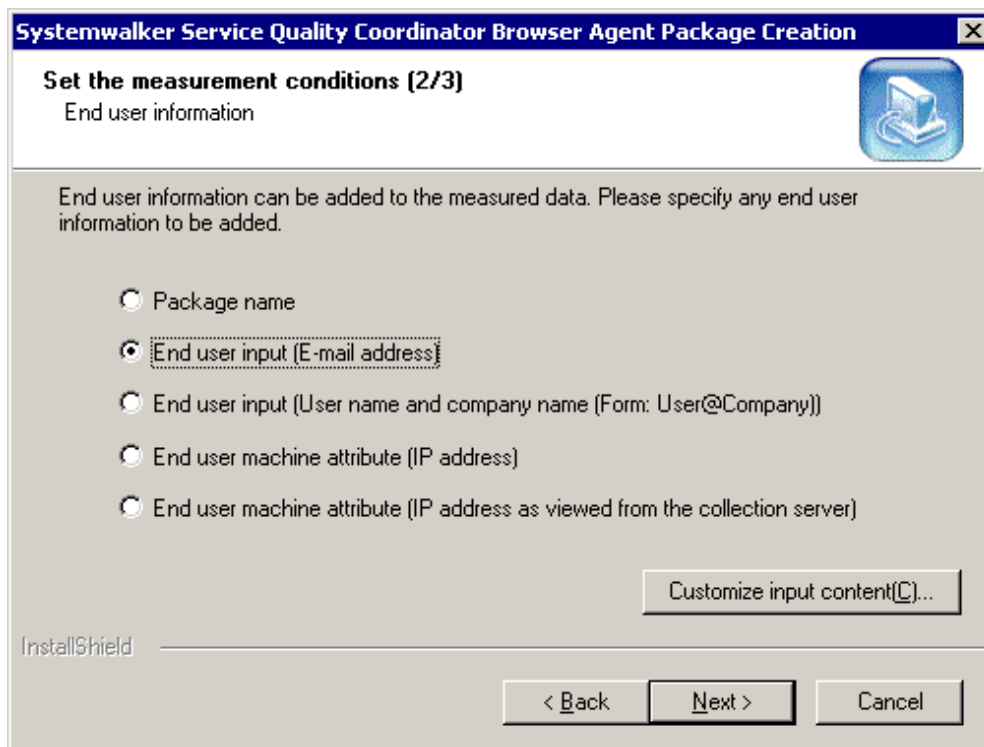
the Customize Input Content

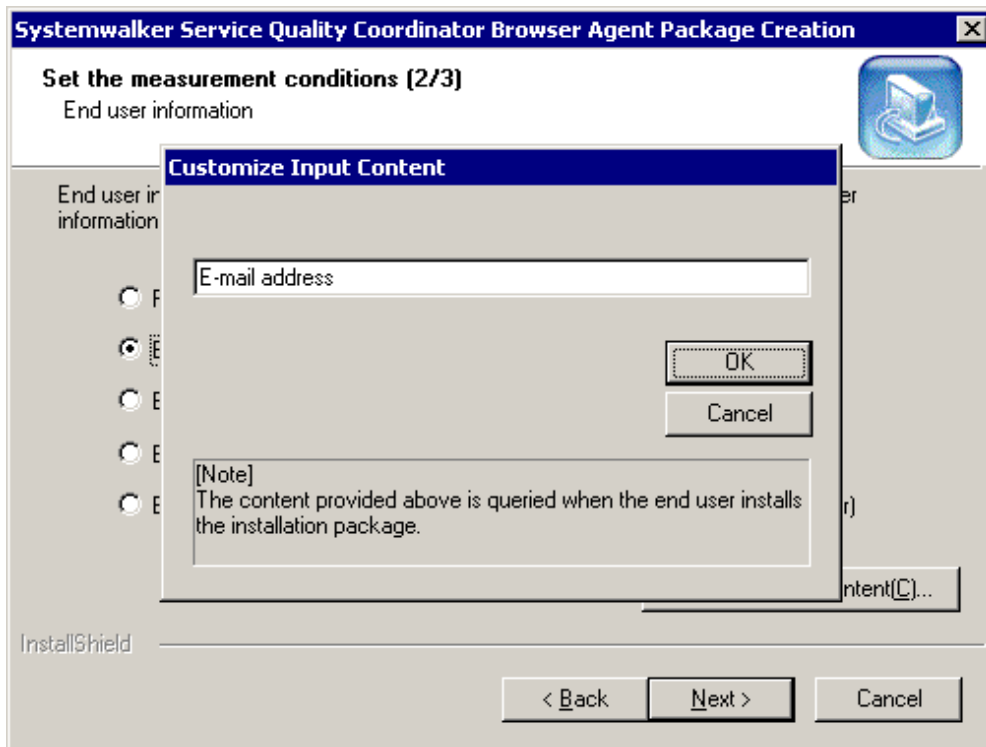
Point

If the following options are selected in the **Set the measurement conditions (2/3)** window, the end user will be prompted to enter the items enclosed in parentheses when installing the package.

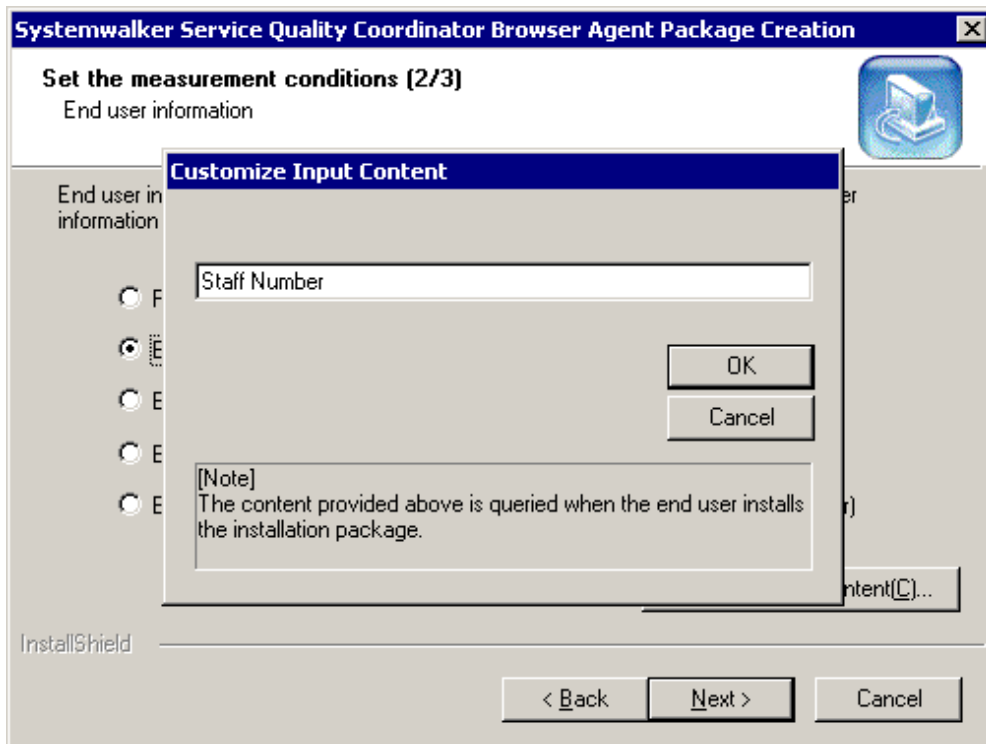
- End user input (E-mail address)
- End user input (User name and company name (Form: User@Company))

Note that when the above options are selected, the **Customize input content(C)** button will be enabled so that the items shown in parentheses can be customized. The following screen shot shows an example of the **Customize input content(C)** button and the **Customize Input Content** window that is displayed when the button is clicked.

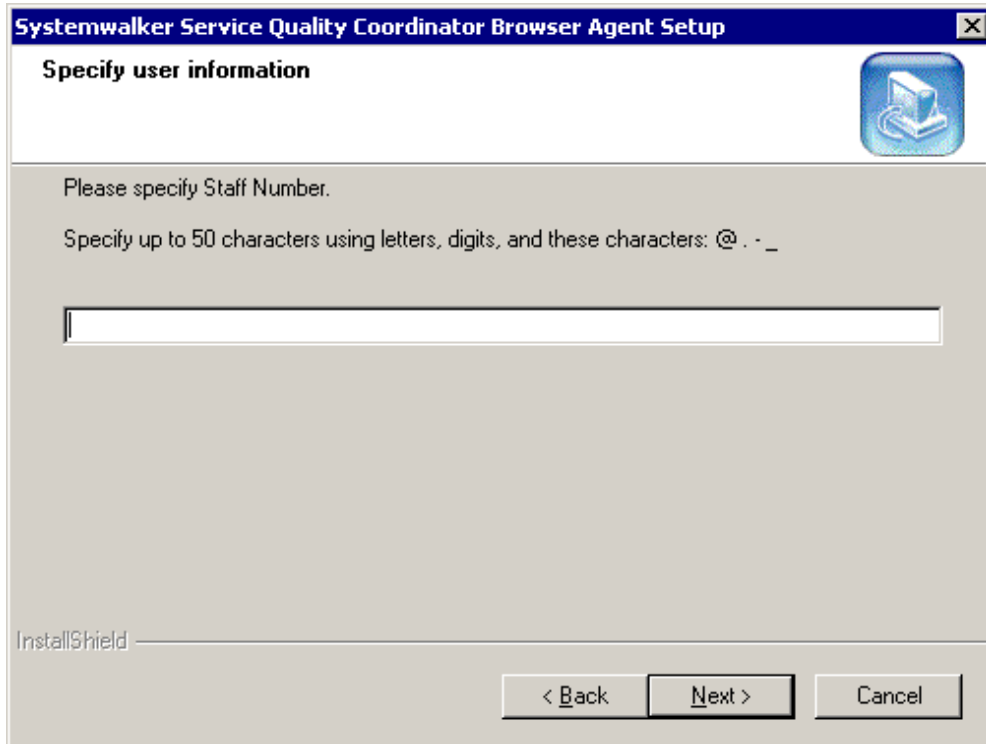




For example, it is possible to customize the item as below.



In this case, the following prompt window will appear when the end user installs the installation package.



If client authentication is also performed by using SSL for HTTP communications between Browser Agents and the collection server, the client certificate files and private key files used by client authentication must also be included in the package.

Prepare the client certificate files and private key files used by client authentication in advance, and specify them in the **Set up client Authentication** window.

The client certificate files and private key files used by Browser Agents use the following formats:

File type	Format
Client certificate	X.509 format
Private key	No password

Distributing the package

The system administrator distributes the created package to the end user.

Packages can be distributed on floppy disks or downloaded from the Website, etc.

4.3.2 Installation conditions

This section explains the installation conditions for Browser Agents.

4.3.2.1 Hardware environment

[Windows]

Item	Requirement	Remarks
CPU	Intel® Pentium 3 equivalent or higher	

Item		Requirement	Remarks
Available disk space	Installation directory	4 MB min.	
Available memory space		10 MB min.	

4.3.2.2 Operating systems

[Windows]

Item	Requirement	Remarks
Operating system	Microsoft® Windows® 2000 Professional(x86)	
	Microsoft® Windows® XP Professional(x64)	
	Microsoft® Windows® XP Professional(x86)	
	Windows Vista® Home Basic(x64)	Service Pack 1/2
	Windows Vista® Home Premium(x64)	Service Pack 1/2
	Windows Vista® Business(x64)	Service Pack 1/2
	Windows Vista® Enterprise(x64)	Service Pack 1/2
	Windows Vista® Ultimate(x64)	Service Pack 1/2
	Windows Vista® Home Basic(x86)	Service Pack 1/2
	Windows Vista® Home Premium(x86)	Service Pack 1/2
	Windows Vista® Business(x86)	Service Pack 1/2
	Windows Vista® Enterprise(x86)	Service Pack 1/2
	Windows Vista® Ultimate(x86)	Service Pack 1/2
	Windows® 7 Home Premium(x86)	Service Pack: None/1
	Windows® 7 Professional(x86)	Service Pack: None/1
Windows® 7 Enterprise(x86)	Service Pack: None/1	
Windows® 7 Ultimate(x86)	Service Pack: None/1	
Web browser	Microsoft® Internet Explorer 6.0 or later (32-bit)	

4.3.2.3 Products that cannot be installed

If resource data about end user responses is to be collected, the following products cannot be installed:

Product name	Remarks
Systemwalker Centric Manager (Operation Management Server, Section Management Server, Job Server and Operation Management Client) Interstage Application Server	

4.3.3 Installing the package

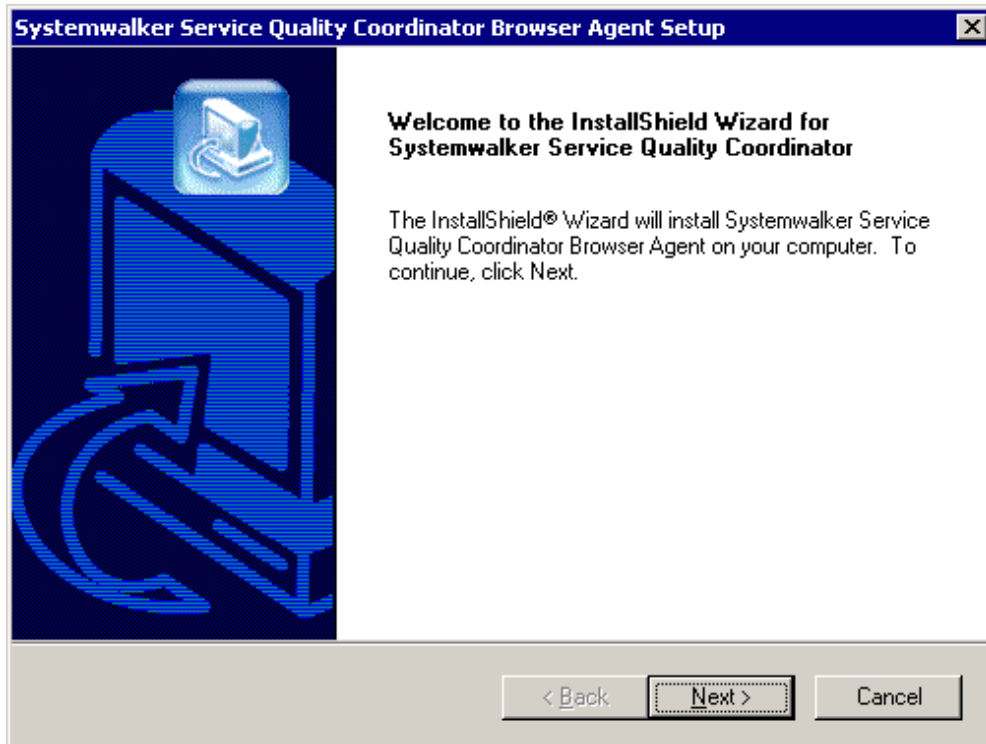
Use the following procedure to install the package that has been created.

1. Log in to the Windows system.

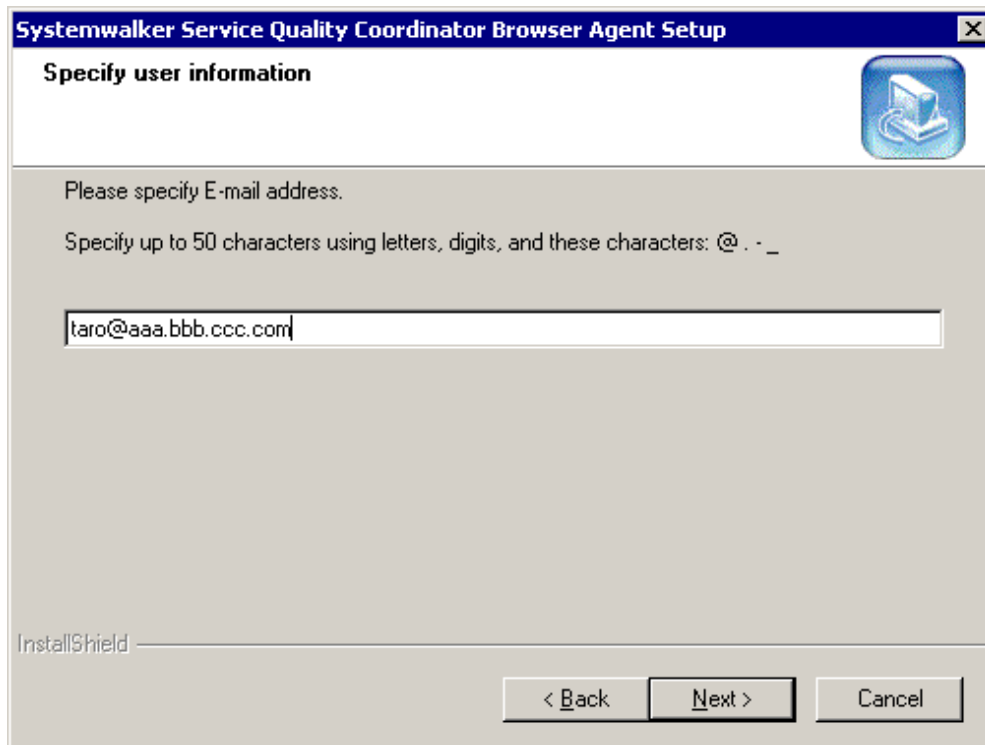
2. Execute the package provided by the system administrator as a command.

To perform the example settings shown in the previous diagram, operations will proceed as shown in the following screen shots. Note that the default installation directory is used in this example.

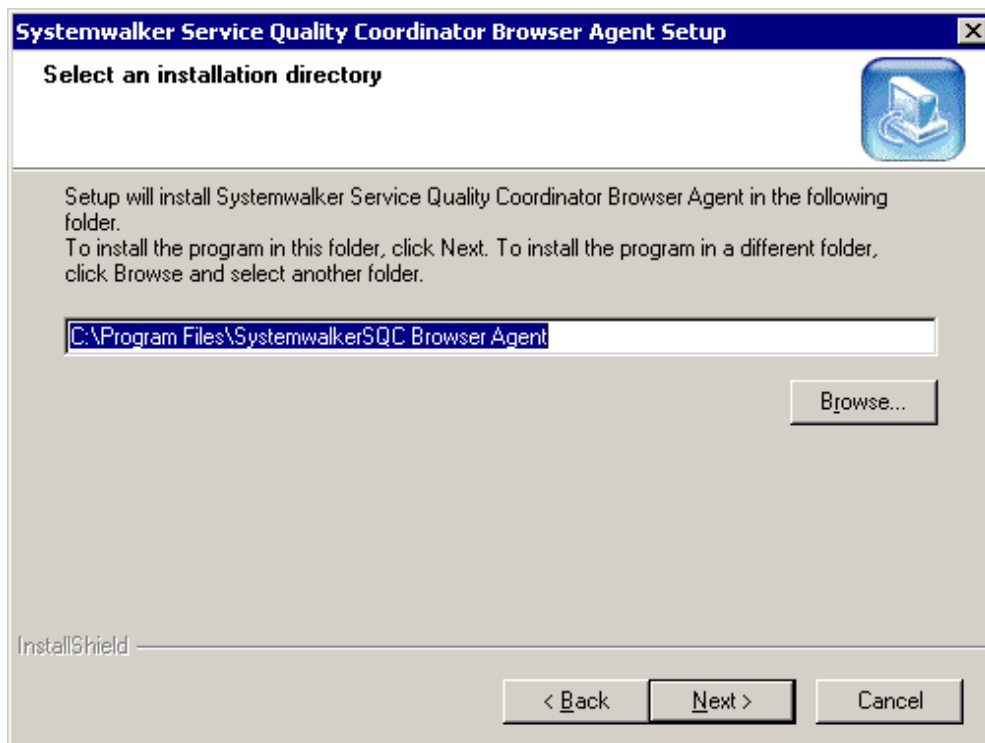
Installation window



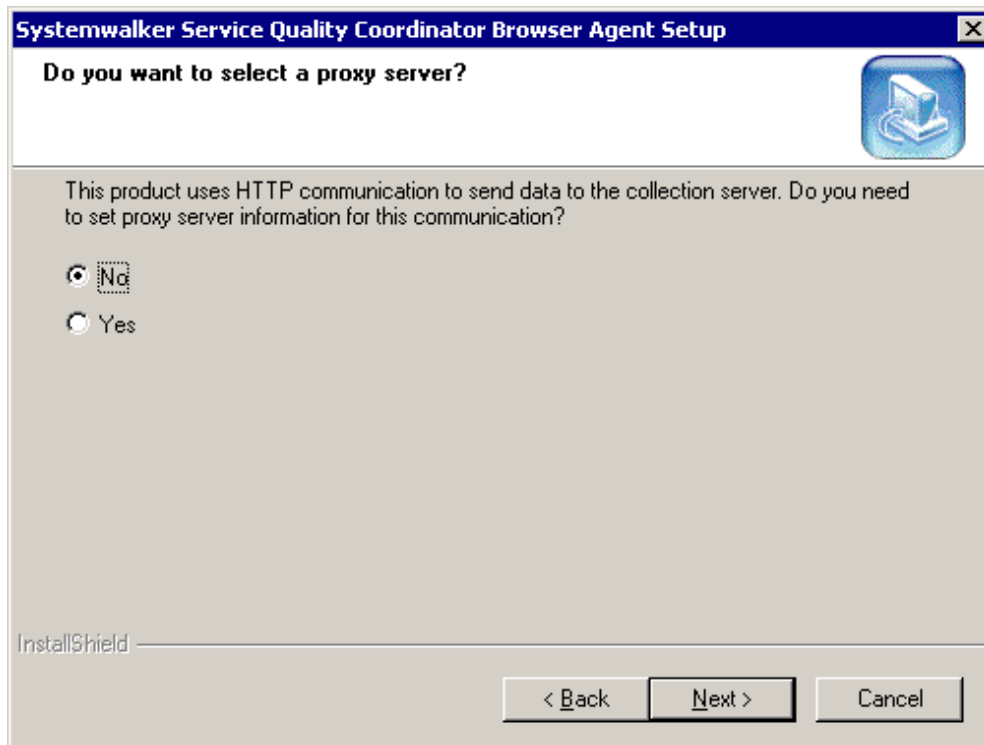
Specify user information (only when end user information needs to be entered by the end user)



Select an installation directory

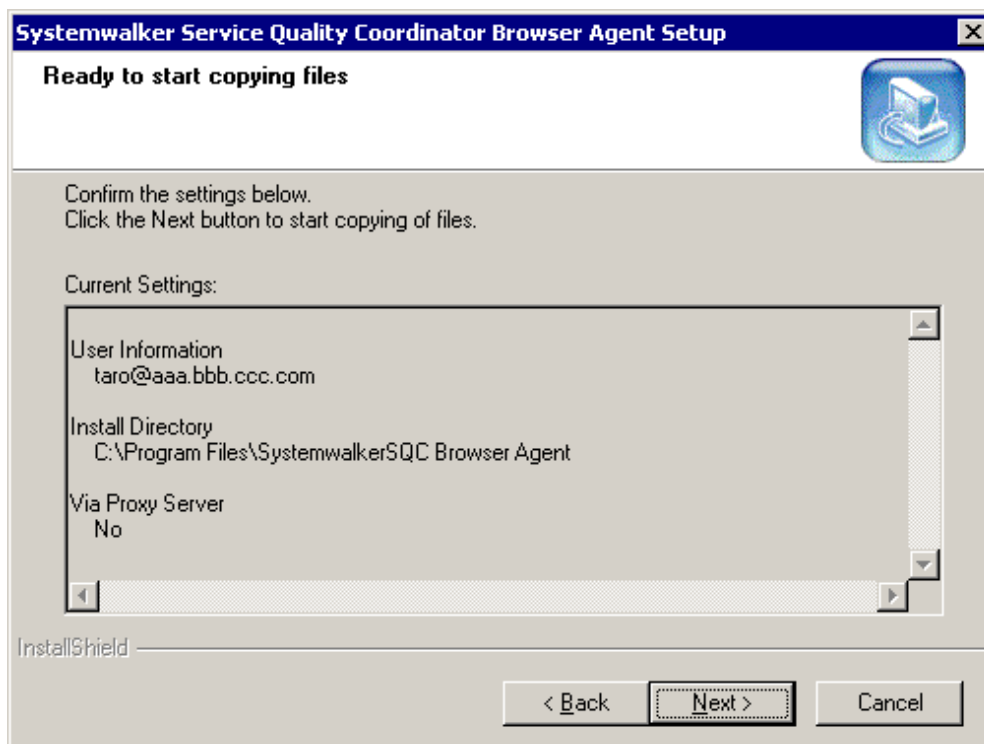


Specify whether to use a proxy server

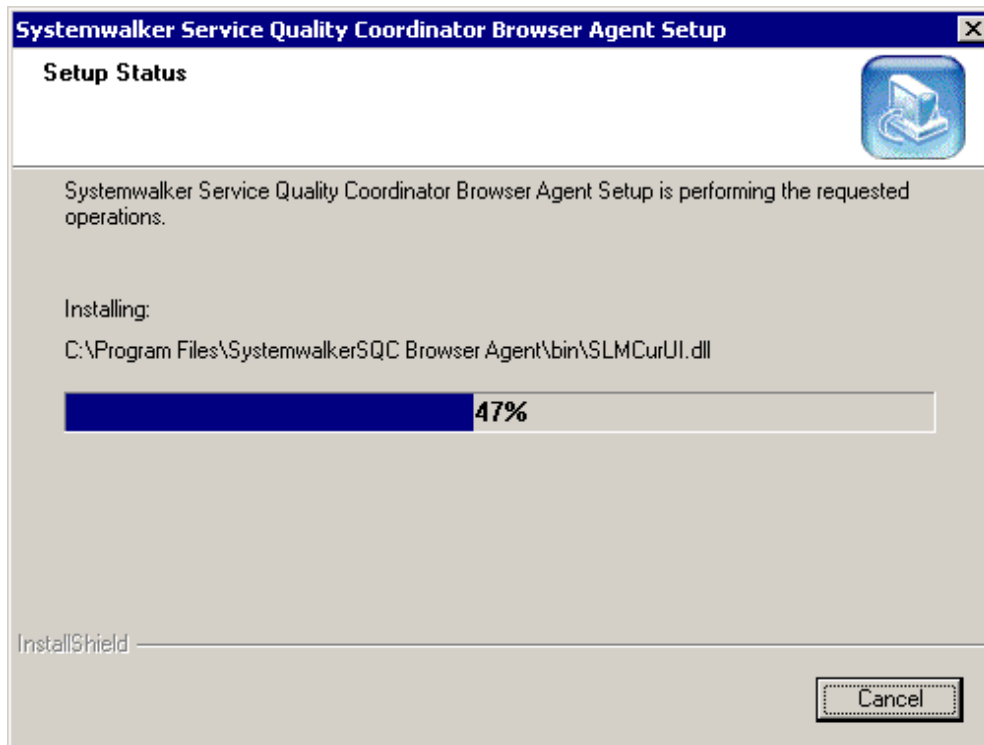


If "Yes" is selected, refer to "[Specify proxy server information](#)".

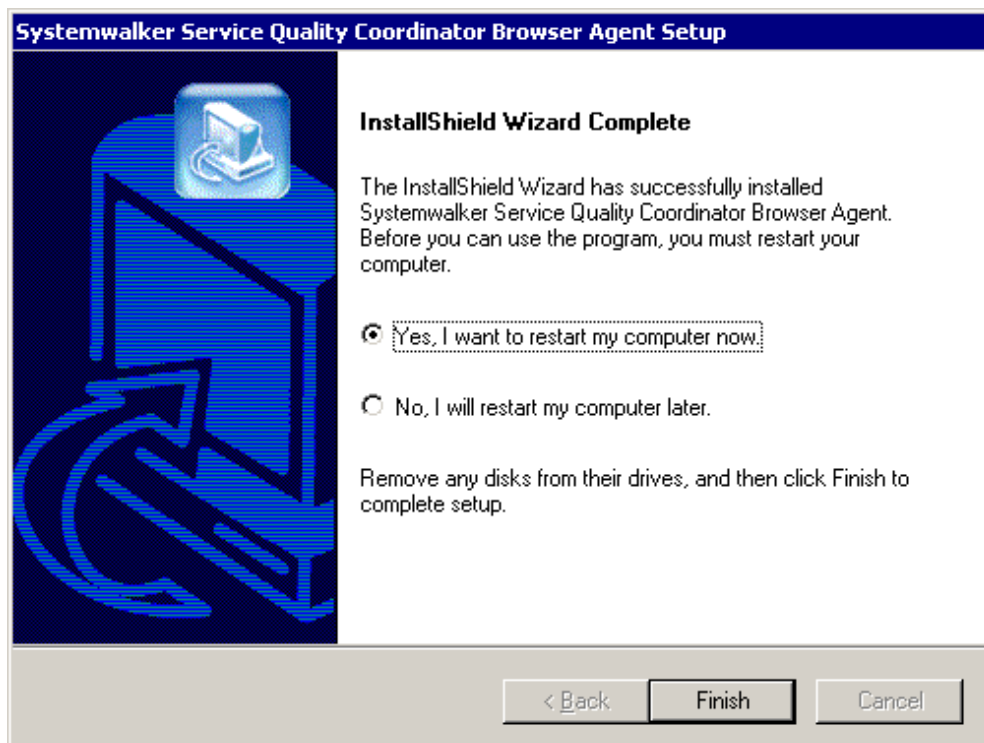
Check whether copying files can be started



Setup status



The installation process is completed



Restart the computer after installation completes.

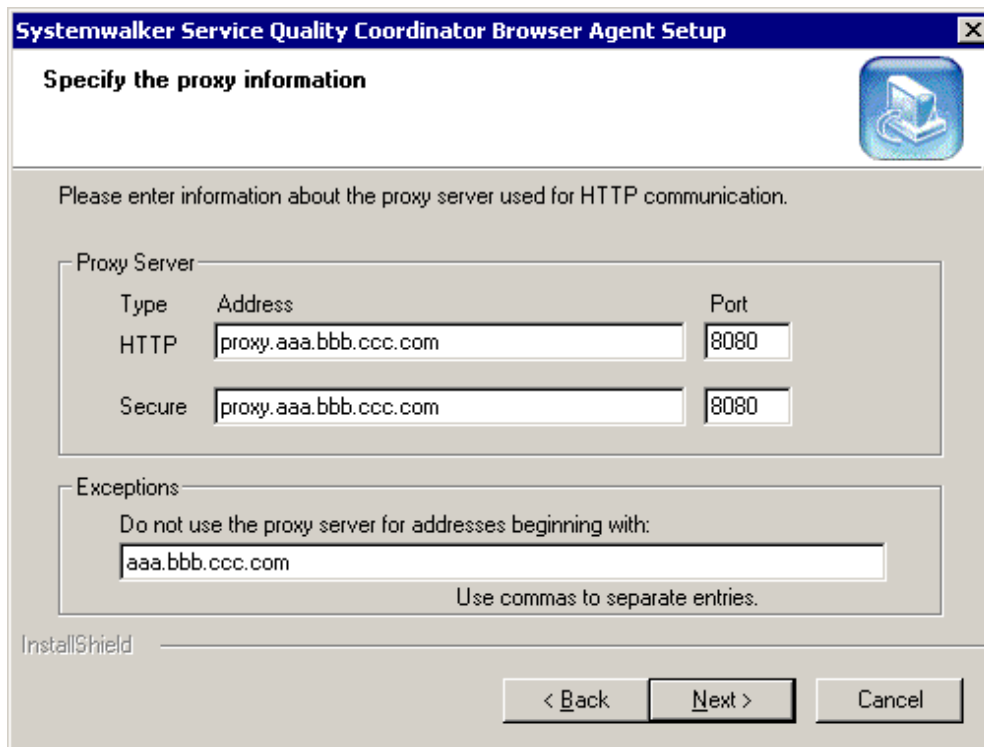
Specify proxy server information



If Yes was selected at the Do you want to select a proxy server?

Window, specify the necessary information in the Specify the proxy information window.

An example of the Specify the proxy information window is shown on the next page.



The screenshot shows a Windows-style dialog box titled "Systemwalker Service Quality Coordinator Browser Agent Setup". The main heading is "Specify the proxy information". Below the heading is a sub-heading "Please enter information about the proxy server used for HTTP communication." The dialog contains two main sections: "Proxy Server" and "Exceptions".

Type	Address	Port
HTTP	proxy.aaa.bbb.ccc.com	8080
Secure	proxy.aaa.bbb.ccc.com	8080

The "Exceptions" section contains a text box with the text "Do not use the proxy server for addresses beginning with:" followed by a text box containing "aaa.bbb.ccc.com". Below this text box is the instruction "Use commas to separate entries." At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel". The "InstallShield" logo is visible in the bottom left corner.

4.3.4 Starting Browser Agents

This section explains how to start Browser Agents.

- How to start Browser Agents from the Start menu

Log in as a user that uses Browser Agent, and then start Browser Agent from Start menu as follows:

Start >> Programs >> Start measurement of web page load time

- How to start Browser Agent by registering it in the startup program

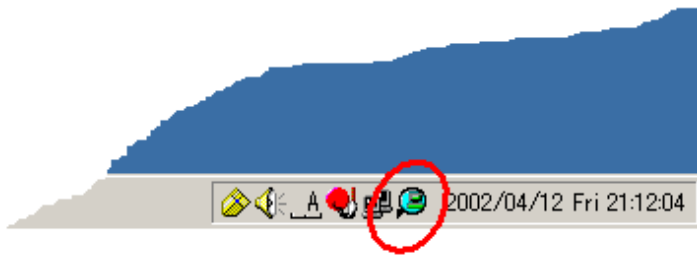
To start Browser Agent automatically when a user that uses Browser Agent logs in, add the following file path to the startup program:

<Installation directory>\bin\SLMCurat.exe

If Browser Agent is running normally after it starts up, the following icon will be displayed in the task tray.



The following is an example. The icon is circled in red.



Note

- If the end user is using Microsoft® Internet Explorer, select **Tools** followed by **Internet Options** to open the **Internet Options** dialog box, then click the **Advanced** tab and verify that **Enable third-party browser extensions (requires restart)** under the **Browsing** heading is selected.
Browser Agent data will not be sent to the collection server if this option is not selected.
- Browser Agent does not support data transmissions to Managers or Proxy Managers running lower versions. Any data that is collected and sent to lower versions may be lost.
- If the end user is using Microsoft® Internet Explorer 9, a message stating that 'SlmBhoExtension Class' add-on from Fujitsu Australia Limited has been enabled may be output when it starts.
In this case, click [Enable(E)] to enable add-on.

4.3.5 Upgrading and reinstalling Browser Agent

This section explains how to upgrade and reinstall Browser Agent.

To install Browser Agent in an environment where Browser Agent has already been installed, first uninstall the Browser Agent that has already been installed, and then install Browser Agent again.

Refer to "[4.3.6 Uninstalling Browser Agent](#)" for information about uninstalling Browser Agent.

Refer to "[4.3.3 Installing the package](#)" for information about how to install Browser Agent.

4.3.6 Uninstalling Browser Agent

It explains the procedure for uninstalling Agent.

Procedure

Implement the following procedure.

[Windows]

1. Check the task tray to verify that the Browser Agent is operating.
If it is operating, one of the following icons will appear in the task tray.



2. If the Browser Agent is running, close it by right-clicking the icon and selecting Exit from the pop-up menu that appears.





3. Double-click **Add/Remove Programs** or **Add or Remove Programs** in Control Panel.
4. Select "Systemwalker Browser Agent" from the application list, and then click the **Add/Remove** or **Change/Remove** button.
5. The uninstallation process will begin.

Note

After uninstalling the software, the **InstallShield Wizard Complete** screen will ask if you want to restart your computer immediately. When you select "Yes, I want to restart my computer now." to restart, a message may appear telling you that it is possible that the Browser Agent has already been uninstalled. This has no effect on the uninstallation procedure.

4.4 Supplementary Information Relating to Product Deployment

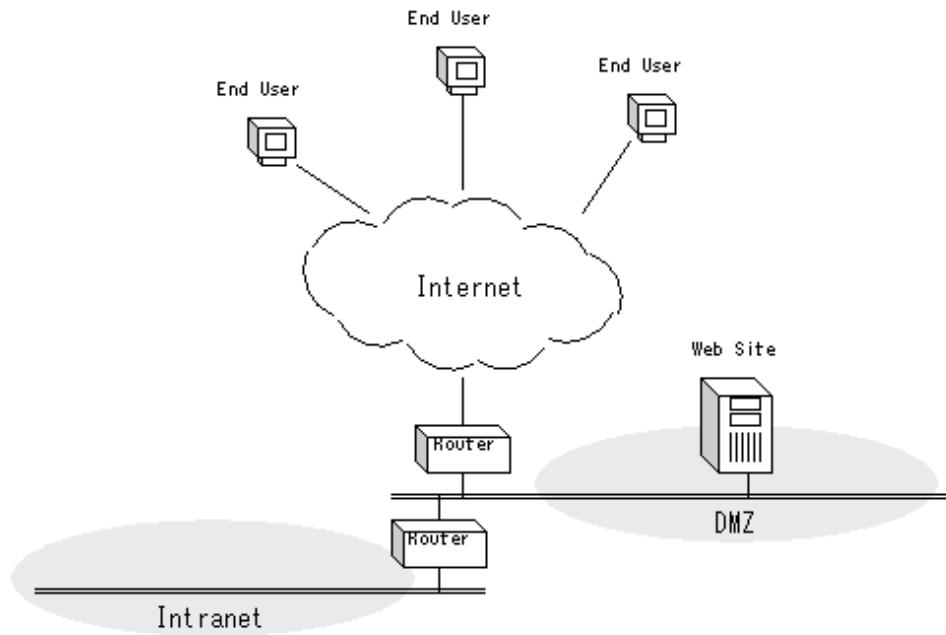
In the explanation that follows, the following icons will be used to represent each product:

	Browser Agent
	Proxy Manager
	Manager
	Operation Management Client

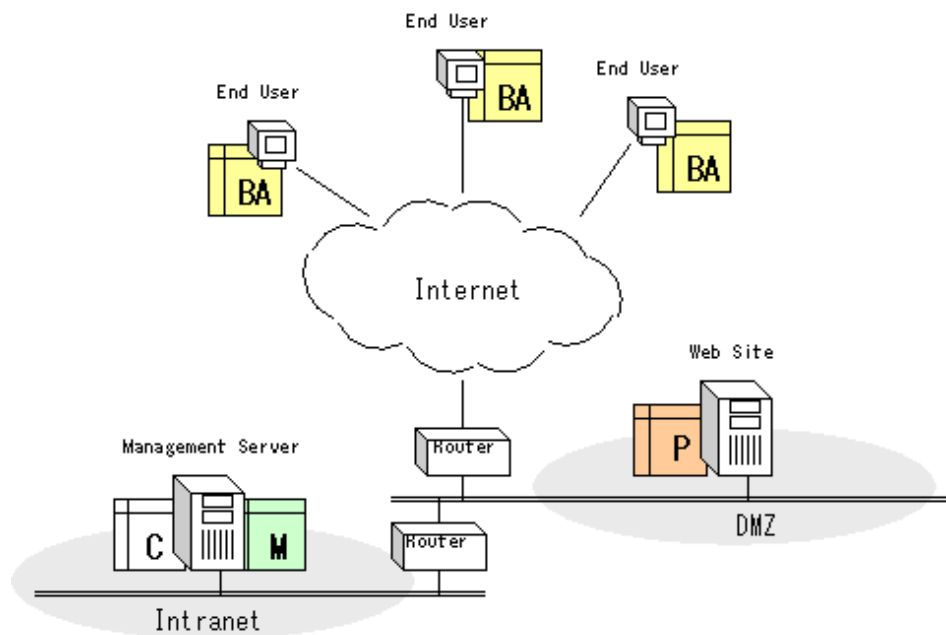
- [4.4.1 Basic product deployment pattern](#)
- [4.4.2 Product deployment pattern to perform regular measurements](#)

4.4.1 Basic product deployment pattern

The following hypothetical model is used as a sample Website arrangement:



In this example, the basic product deployment pattern is shown below.



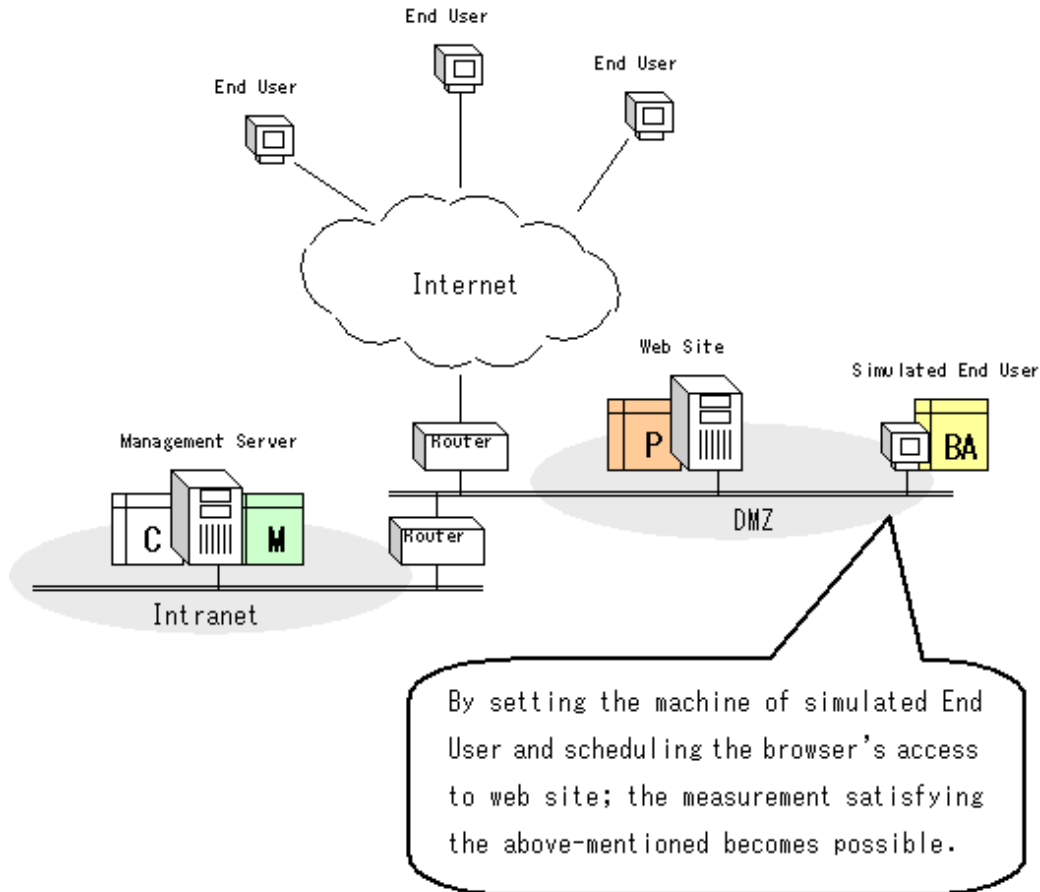
4.4.2 Product deployment pattern to perform regular measurements

The following conditions are required to ascertain the capacity of a Website by conducting hourly checks.

- The end user's measurement environment (machine environment and network environment) on the end user side must be the same.
- Measurements on the end user side must be conducted regularly.

In the previous section ("[4.4.1 Basic product deployment pattern](#)"), the Browser Agent was deployed to the actual end user. In that case, the measurement environment on the end user side is not fixed, and measurements are not taken regularly because measurements are taken only when the end user actually uses the Website's services.

Therefore, to meet the above conditions, it is recommended that the following product deployment pattern, which provides a dummy environment that repeats the operations of an end user (hereafter referred to as the "simulated end user"), be used.



Additional information about a support tool that can be used to conduct regular schedules is provided overleaf.

Supplement: Regular startup tool (command) for browser

Location:
 This tool is located in the following directory of the CD-ROM for Service Quality Coordinator (Client/Documentation):
CD-ROM drive:\tools\wslm\repeatbrowser.exe

Note: If you are going to use a copy in a different folder, put the following three files into the same folder and run repeatbrowser.exe:

- repeatbrowser.exe
- run_ie_default.vbs
- run_ie7_vis.vbs

Operating conditions:
 OS: Microsoft(R) Windows 2000 Professional or later
 Browser: Microsoft(R) Internet Explorer 6.0 or later

Specification:

[Format]

repeatbrowser interval period

[Description]

Repeats starting and stopping a browser at regular intervals.

[Parameters]

interval:Specifies the browser startup interval in seconds.

period:Specifies the browser operation time in seconds.

Note that "interval" and "period" must be specified as follows: interval > period > 1

[Initial preparations]

First, set the Web page to be accessed regularly as the browser's home page. (In Internet Explorer, Select **Internet Options** from the **Tools** menu and then set the address in the **Home page** field of the **General** tab.

To prevent the browser cache from being used during access, specify that the cache be deleted when the browser stops. (In Internet Explorer, Select **Internet Options** from the **Tools** menu, then click the **Advanced** tab and select the **Empty Temporary Internet Files folder when browser is closed** check box under **Security**.)

[Startup method]

Execute the command from a DOS prompt.

[Stop method]

Press CTRL+C to stop the command.

[Standard output]

Outputs a message whenever the browser starts or stops.

[Standard error output]

Outputs a message when an error occurs.

[Example]

To start the browser every three minutes (180 seconds) and operate it for one minute (60 seconds):

```
C:\> repeatbrowser 180 60
2002/06/08 20:06:47 Start IE
2002/06/08 20:07:47 Stop IE
2002/06/08 20:09:47 Start IE
```

4.5 Supplementary Information Relating to Browser Agent Packages

When distributing a Browser Agent package, the user needs to consider how the response data should be analyzed, and distribute the package that is appropriate for that purpose. This section explains the Browser Agent package distribution patterns in the following order:

- [4.5.1 When analyzing measurement results by given groups](#)
- [4.5.2 When analyzing measurement results by end user attributes](#)
- [4.5.3 When analyzing measurement results by end user attributes](#)

4.5.1 When analyzing measurement results by given groups

For example, to analyze measurement results by given groups, such as the Eastern District and Western District, create a Browser Agent package for each group, specify a name to denote the group as the package name, and select the **Package name** option as **End user information**. When distributing the packages, distribute the package corresponding to each group.



Refer to "4.3.1 Creating the package" for details on package creation.

4.5.2 When analyzing measurement results by end user attributes

To analyze measurement results by end user attributes (E-mail address, user name and company name, or any single item of user information), create a single Browser Agent package and select either **End user input (E-mail address)** or **End user input (User name and company name (Form: User@Company))** as **End user information**. (Both can be customized.)



Refer to "4.3.1 Creating the package" for details on package creation.

4.5.3 When analyzing measurement results by end user attributes

To analyze measurement results by end user machine attributes (IP address or IP address as viewed from the collection server), create a single Browser Agent package and select either the **End user machine attribute (IP address)** or the **End user machine attribute (IP address as viewed from the collection server)** as **End user information**.

4.6 Display

End user response information can be displayed using the following methods.

- Displaying information in the Console Summary
 - Display information using the "End user response" node (UserResponseMonitor) in the Summary tree.
- Displaying information using Drilled-Down in the Console
 - Display information using the "Proxy Managers" node in the Detailed tree.
- Reports
 - Full system inspection analysis/report
 - Categorized diagnostic analysis/report
 - Detailed analysis/report

4.6.1 End user response resource data

If WEBSLM_URL, WEBSLM_TCP, and WEBSLM_DNS data need to be collected, execute the following command in the environment where Browser Agent is installed.

Note

WEBSLM_URL, WEBSLM_TCP, and WEBSLM_DNS data cannot be collected if the Web server being measured is HTTPS.

1. Log in with administrator privileges.
2. Open a Command Prompt window and switch to the following directory.

Point

In Windows Vista® and Windows®7, select [Programs] and then [Accessories] from the [Start] menu. Then, right-click on [Command Prompt] and select [Run as Administrator] to open the Command Prompt window.

```
<Browser Agent installation directory>\tool
```

3. Execute the following command.

```
instlsp -install
```

4. Restart the machine.

However, some products cannot be installed if resource data is to be collected. Refer to "[4.3.2.3 Products that cannot be installed](#)" for information about such products.

Note

Refer to Section 4.2.1, "End user response reports for the ResponseCondition folder" in the Reference Guide for more information about WEBSLM_URL WEBSLM_TCP and WEBSLM_DNS.

To stop collecting data for WEBSLM_URL, WEBSLM_TCP and WEBSLM_DNS, execute the following command in the environment where the Browser Agent is installed.

1. Log in with administrator privileges.
2. Open a Command Prompt window and switch to the following directory.

Point

In Windows Vista® and Windows®7, select [Programs] and then [Accessories] from the [Start] menu. Then, right-click on [Command Prompt] and select [Run as Administrator] to open the Command Prompt window.

```
<Browser Agent installation directory>\tool
```

3. Execute the following command.

```
instlsp -remove
```

4. Restart the machine.

Chapter 5 Service Operation Management

This chapter explains how to manage the operational status of services.

Execution environment

These settings can be made in Manager and Proxy Manager environments.

Privileges required for execution

[Windows]

The privileges of a user belonging to the "Administrators" group are required to make these settings.

[UNIX]

System administrator (superuser) privileges are required to make these settings.

- [5.1 Measurement Overview](#)
- [5.2 Environment Settings](#)
- [5.3 Display](#)
- [5.4 Service operation watch time-out value setting](#)

5.1 Measurement Overview

This product can manage services such as HTTP and DNS. It monitors the operational status of these services by periodically polling them and checking the response.

The following types of service can be monitored:

- HTTP (GET/POST) - including communications such as JSPs, Servlets and SOAP
- DNS
- SMTP
- Arbitrary TCP ports



.....
For HTTPS, only SSL 2.0 can be monitored.
.....

5.2 Environment Settings

Define information relating to the services to be monitored in the response and managed object configuration information file (ServiceConf.xml).

- To monitor the HTTP Service, make definitions in the HTTP operational information section (the <HTTP_Service> tag)
- To monitor the DNS Service, make definitions in the DNS operational information section (the <DNS_Service> tag)
- To monitor the SMTP Service, make definitions in the SMTP operational information section (the <SMTP_Service> tag)

To monitor arbitrary ports, make definitions for each port in the PORT operational information section (the <PORT_Service> tag).

Refer to "[Chapter 6 Response and Managed Object Configuration Information \(ServiceConf.xml\)](#)" for information about how to make these definitions.

5.3 Display

Operational information about services can be displayed using the following methods:

Summary view of the Console window

Use the "Service operation" node (ServiceAvailMonitor) in the Summary tree.

Drilled-Down view of the Console window

Use the "ServiceCondition" node in the Detailed tree.

Report view

- Full system inspection analysis/report
- Categorized diagnostic analysis/report
- Detailed analysis/report

5.4 Service operation watch time-out value setting

This section explains the procedure for setting a separate timeout value for each monitored object for service operation monitoring.



Use this procedure if the timeout values for service operation monitoring need to be changed while service operation management is being performed.

Privileges required for execution

[Windows]

The privileges of a user belonging to the "Administrators" group are required to make these settings.

[UNIX]

System administrator (superuser) privileges are required to make these settings.

Storage location

The storage location of this file is as follows:

[Windows]

<Variable file directory>\control\template.dat

[UNIX]

/etc/opt/FJSVssqc/template.dat

The service operation monitoring function has two types of timeouts.

- **Collection timeout**

The value of the collection timeout is the maximum amount of time allowed for the collection process (the process that operates during each collection interval). The collection timeout is set at 70 seconds by default.

When a collection timeout occurs, all the data collected during that collection interval becomes invalid and no performance information record is created.

- **Monitoring timeout**

The value of the monitoring timeout is the maximum amount of time allowed for receiving a response to a request that was sent to a monitored object. The monitoring timeout is set at 10 seconds by default.

If a monitoring timeout occurs, "-1" is stored as the performance value of the monitored object that caused the timeout.



"-1" is also stored in the performance information record when communications errors occur.

Approach for defining monitored objects

Performance information records are not created if collection timeouts occur. This means that definitions must be made so that collection timeouts do not occur, in order to perform successful monitoring.

If there are multiple monitored objects, the number of monitored objects and the values for monitoring timeouts and collection timeouts must satisfy the condition shown in the formula below, in order to take into account the possibility that timeouts will occur for all monitored objects.

$$\text{Number of monitored objects} * \text{Monitoring timeout}(10 \text{ seconds}) < \text{Collection timeout}(70 \text{ seconds})$$

Note: The maximum number of monitored objects is set at six by default.

The following items for the service operation monitoring function can be changed using the template file.

- Collection interval: Either 1, 2, 5 or 10 (minutes) can be specified
- Monitoring timeout value: Any value equal to or less than the collection interval
- Collection timeout value: 5 seconds (or collection interval whichever is greater) + 30 seconds



The larger the value specified for the monitoring timeout value, the less objects can be monitored, so take into account the number of monitored objects when specifying the monitoring timeout.

A warning message will be output if, as a result of the settings in "[A.2 Response/Operation Information Collection Policy Creation Command](#)", the number of monitored objects and the timeout values do not satisfy the condition shown in the formula above. However, the policy will be created even though the warning message is output.

If there are a lot of monitored objects, or if there is a problem with the settings for the monitored objects, the command may take a long time to return.

Information used

Collection timeout

template.dat PING section CMDTIMEOUT parameter Default value: 70 seconds

Monitoring timeout

template.dat PING section TIMEOUT parameter Default value: 10 seconds

Number of monitored objects

ServiceConf.xml The number of monitored objects for each monitoring type

5.4.1 Definition Method

Add the following parameters to the PING section.

Specify parameters so that the condition in the formula below is satisfied, taking into account the number of monitored objects and the maximum response times.

Calculation formula:

$$\text{Number of monitored objects} * \text{Monitoring timeout} < \text{Collection timeout}$$

Parameter name	Meaning	Default value
INTERVAL	Collection interval	1 (units: minutes)
TIMEOUT	Monitoring timeout	10 (units: seconds)
CMDCMDTIMEOUT	Collection timeout	70 (units: seconds)

Definition example

Example where the collection interval is 1 minute, the collection timeout is 70 seconds and the monitoring timeout is 20 seconds.

```
#####  
# ProtoPing Information  
[PING]  
DCAID="PING"  
TIMEOUT=20
```

Note

The following alert messages might be output by combining the number of watch objects and the watch time-out value, when "[A.2 Response/Operation Information Collection Policy Creation Command](#)" is executed.

```
sqcAPolicy template.dat warning.  
(The time taken for monitoring processing may exceed the collection interval  
depending on the timeout value and the number of monitoring targets  
specified with the <PORT> tag.)
```

In this case, either reduce the monitoring timeout value, or increase the collection timeout value so that the condition in the formula above is satisfied.

However, the collection timeout value must be within the range [5 seconds (or collection interval whichever is greater) + 30 seconds].

Chapter 6 Response and Managed Object Configuration Information (ServiceConf.xml)

Follow the procedures in this chapter when performing service operation management or end user response management as described in the following sections.

Installation Guide

- 3.2 Basic Manager-Agent Model
- 3.3 Relay Model Using Proxy Manager
- 3.4 Two-tier Manager Operation Model
- 3.5 Redundant Manager Operation Model
- 3.6 Cluster System Operation Model for MSCS/Failover Clustering
- 3.7 PRIMECLUSTER Cluster System Operation Model

Execution environment

These settings can be made in Manager and Proxy Manager environments.

Privileges required for execution

[Windows]

The privileges of a user belonging to the "Administrators" group are required to make these settings.

[UNIX]

System administrator (superuser) privileges are required to make these settings.

This configuration information file is an XML document. Definitions for each managed object can be created by adding structured tags to the document tree.



The following operating environment is required:

- Microsoft(R) Windows 2000 Professional or later
- Microsoft Internet Explorer 5.5 or later

Always use ASCII mode when transferring the response and managed object configuration information file (ServiceConf.xml) edited with the XML editor provided to the server.



- For response information, define the name of the site that will be managed by the Browser Agent.
- For operation management information, define the HTTP, DNS, SMTP or PORT service that will be monitored.
- For cluster system operations, make sure that the variable file storage directory for Systemwalker Service Quality Coordinator can be checked when these procedures are performed.

- In order to enable the changes to this file, a collection policy must be created and applied.

.....

The XML file can be easily edited with the XML editor that can be found in the following directory of the Systemwalker Service Quality Coordinator CDROM (Client/Documentation):

Storage location



The following sections explain how to make definitions in the "ServiceConf.xml" file.

- [6.1 Storage Location](#)
- [6.2 Definition Method](#)
- [6.3 Definition Example](#)
- [6.4 Setup](#)
- [6.5 How to Create BODY Files](#)

6.1 Storage Location

The storage location of the configuration information file is as follows:

[Windows]

Variable file directory\control\ServiceConf.xml

[UNIX]

/etc/opt/FJSVssqc/ServiceConf.xml

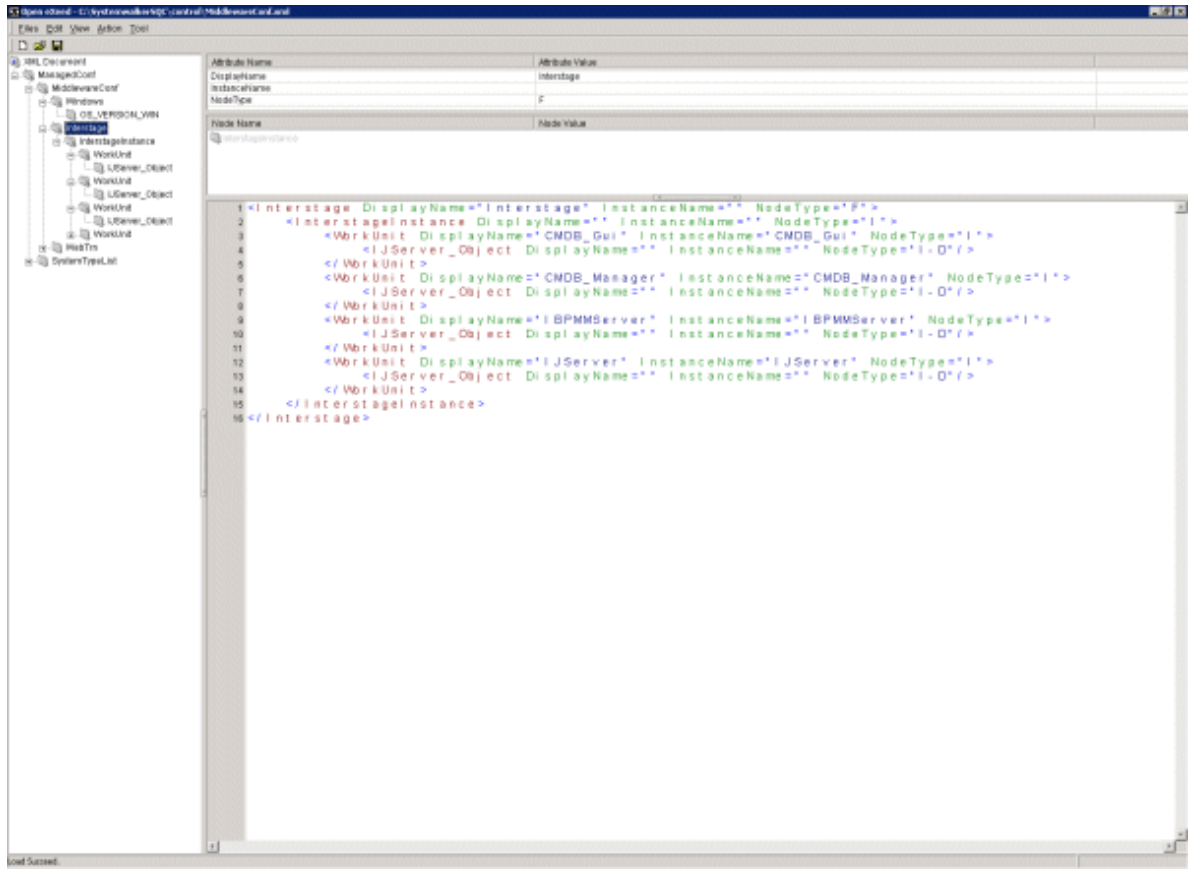
There is a sample configuration information file named "ServiceConf.sample" in the same directory. Back up this sample file, and then rename it as "ServiceConf.xml" before editing it.

6.2 Definition Method

The following sections explain how to define each tag. Take note of the following points when using the XML editor included in this product:

- Check each tag in the tree of the XML editor (View:XML Structure).
- To define an attribute, select the tag to be edited on the tree and then double-click the attribute name to be defined in its displayed location (View:XML Data). Alternatively, an attribute can also be defined by using the **Edit Attributes** window displayed by clicking the right mouse button and selecting **Edit** from the context menu that appears.

- Individual tags can be added easily by using **Copy** and **Paste** from the **Edit** menu or by using **Duplicate** or **Copy/Paste** from the right-click context menu.



Note

Create definitions by editing the sample file. Each tag in the sample file includes an attribute called "NodeType". Do not change the value of this attribute when editing the sample file.

Definitions cannot include the following symbols or characters other than ASCII.


<code>\ : , < > " \$ ' [] = & _ %</code>

The following sections explain how to make definitions for each tag.

- [6.2.1 Response information \(WebSite tag\)](#)
- [6.2.2 HTTP operation information \(HTTP_Service tag\)](#)
- [6.2.3 DNS operation information \(DNS_Service tag\)](#)
- [6.2.4 SMTP operation information \(SMTP_Service tag\)](#)
- [6.2.5 PORT operation information \(PORT_Service tag\)](#)

6.2.1 Response information (WebSite tag)

Define the name of the site managed by the Browser Agent in the "WebSite" tag.

Attribute name	Description	Definition example
DisplayName	Define the name to be displayed in the Console window. The following characters can be used. - Alphanumeric characters - Symbols (except for \, <, > "\$'[]= and &) The maximum length is 64 characters.	www.fujitsu.com
InstanceName	Define the host name of the site managed by the Browser Agent.	www.fujitsu.com
AlertTarget	Define the node name (corresponding to the managed site) that is recognized by Centric Manager. When Centric Manager message linkage is performed, the defined node will become the node where an alarm will be generated. If this attribute is omitted, either the Manager or the Proxy Manager where this definition resides will become the node where an alarm will be generated.	webservers
NodeType	 Note This attribute is used for control purposes. Do not change the value of this attribute in the sample file.	I-D

Note

None of the attributes for the child tags of the WebSite tag (tags between <WebSite> and </WebSite>) need to be changed. Leave the contents of the sample file unchanged.

Point

To define multiple site names, create multiple "WebSite" tags (blocks between <WebSite> and </WebSite>).



To delete a Web site for which response information is to be collected, delete the blocks between <WebSite> and </WebSite>

6.2.2 HTTP operation information (HTTP_Service tag)

Define information relating to the HTTP service whose operational status is to be monitored in the "HTTP_Service" tag.

Attribute name	Description	Definition example
DisplayName	Define the name to be displayed in the Console window. The following characters can be used for the name: - Alphanumeric characters - Symbols (except for \, <, > "\$'[]=&)	HTTPPage1

Attribute name	Description	Definition example
	The name to be displayed can be no longer than 64 characters.	
InstanceName	<p>Define the name that will identify the HTTP service being monitored.</p> <p>The following characters can be used for the name:</p> <ul style="list-style-type: none"> - Alphanumeric characters - Symbols (except for \, <, > "\$'[]=&) <p>The name can be no longer than 64 characters.</p>	HTTPPage1
AlertTarget	<p>Define the node name (corresponding to the managed site) that is recognized by Centric Manager. When Centric Manager message linkage is performed, the defined node will become the node where an alarm will be generated.</p> <p>If this attribute is omitted, either the Manager or the Proxy Manager where this definition resides will become the node where an alarm will be generated.</p>	webserver
IP_Address	If an IP-based virtual host is being used, set the logical IP address for accessing the service being monitored. Otherwise, this attribute can be omitted.	100.100.100.100
URL	Set the URL for accessing the service being monitored.	<p>http://host[:port]/path</p> <p>https://host[:port]/path</p>
ProxyServer	To access the service via a proxy server, set this attribute to "ON". To access the service directly, set this attribute to "OFF".	ON
ProxyServer_Addr	<p>To access the service via a proxy server, define the IP address of the proxy server.</p> <p>To access the service directly, specify an empty string ("").</p>	100.100.100.100
ProxyServer_Port	To access the service via a proxy server, define the port number of the proxy server. To access the service directly, specify an empty string ("").	8080
BodyFile	<p>To access the service using the HTTP POST method, specify the absolute path of the BODY file that contains the BODY data that will be sent.</p> <p>If the service is accessed without using the HTTP POST method (if an empty string ("") has been defined), then the GET method is used. If a BODY file has been specified, then the POST method is used.</p>	<p>C:\temp\body.txt</p> <p>/var/temp/body.txt</p>

Attribute name	Description	Definition example
	 Note If BODY file is specified, the BODY file must be prepared as specified by the path.	
BasicAuthentication	If the monitored URL is performing basic authentication, set this attribute to "ON". Otherwise, set this attribute to "OFF".	ON
BasicAuthentication_User	If basic authentication is being performed, set the user ID required to access the service.	User1
BasicAuthentication_Password	If basic authentication is being performed, set the user password required to access the service.	User1
NodeType	 Note This attribute is used for control purposes. Do not change the value of this attribute in the sample file.	I-D

Point

.....

To monitor multiple HTTP services, create multiple "HTTP_Service" tags (blocks between < HTTP_Service > and </ HTTP_Service >). If multiple BODY files are created, store them all in the same directory. Refer to "6.5 How to Create BODY Files" for details on how to create BODY files.


To remove HTTP service collection targets, delete the block enclosed by the <HTTP_Service> and </HTTP_Service> tags.

.....

6.2.3 DNS operation information (DNS_Service tag)

Define information relating to the DNS service whose operational status is being monitored in the "DNS_Service" tag.

Attribute name	Description	Definition example
DisplayName	Define the name to be displayed in the Console window. The following characters can be used for the name: - Alphanumeric characters - Symbols (except for \, <, > "\$[]=&) The name can be no longer than 64 characters.	DNS
InstanceName	Define the name that will identify the DNS service being monitored. The following characters can be used for the name: - Alphanumeric characters - Symbols (except for \, <, > "\$[]=&) The name can be no longer than 64 characters.	DNS

Attribute name	Description	Definition example
AlertTarget	Define the node name (corresponding to the managed site) that is recognized by Centric Manager. When Centric Manager message linkage is performed, the defined node will become the node where an alarm will be generated. If this attribute is omitted, either the Manager or the Proxy Manager where this definition resides will become the node where an alarm will be generated.	dnsserver
IP_Address	Define the IP address of the service being monitored.	100.100.100.100
Port	Define the port number of the service being monitored.	53
TargetHost	Define the host name used for name resolution.	abcserver
NodeType	 Note This attribute is used for control purposes. Do not change the value of this attribute in the sample file.	I-D

Point

.....

To monitor multiple DNS services, create multiple "DNS_Service" tags (blocks between <DNS_Service> and </DNS_Service>).


To remove DNS service collection targets, delete the block enclosed by the <DNS_Service> and </DNS_Service> tags.

.....

6.2.4 SMTP operation information (SMTP_Service tag)

Define information relating to the SMTP service whose operational status is being monitored in the "SMTP_Service" tag.

Attribute name	Description	Definition example
DisplayName	Define the name to be displayed in the Console window. The following characters can be used for the name: <ul style="list-style-type: none"> - Alphanumeric characters - Symbols (except for \, <, > "\$[]=&) The name can be no longer than 64 characters.	SMTP
InstanceName	Define the name that will identify the SMTP service being monitored. The following characters can be used for the name: <ul style="list-style-type: none"> - Alphanumeric characters - Symbols (except for \, <, > "\$[]=&) The name can be no longer than 64 characters.	SMTP
AlertTarget	Define the node name (corresponding to the managed site) that is recognized by Centric Manager. When Centric Manager message linkage is performed, the	smtpserver

Attribute name	Description	Definition example
	<p>defined node will become the node where an alarm will be generated.</p> <p>If this attribute is omitted, either the Manager or the Proxy Manager where this definition resides will become the node where an alarm will be generated.</p>	
IP_Address	Define the IP address of the service being monitored.	100.100.100.100
Port	Define the port number of the service being monitored.	25
NodeType	 Note <p>.....</p> <p>This attribute is used for control purposes. Do not change the value of this attribute in the sample file.</p> <p>.....</p>	I-D

Point

.....

To monitor multiple SMTP services, create multiple "SMTP_service" tags (blocks between <SMTP_service> and </SMTP_service>).


To remove SMTP service collection targets, delete the block enclosed by the <SMTP_Service> and </SMTP_Service> tags.

.....

6.2.5 PORT operation information (PORT_Service tag)

Define information relating to the arbitrary port whose operational status is being monitored in the "PORT_Service" tag.

Attribute name	Description	Definition example
DisplayName	<p>Define the name to be displayed in the Console window.</p> <p>The following characters can be used for the name:</p> <ul style="list-style-type: none"> - Alphanumeric characters - Symbols (except for \;,<>"\$'[]=&) <p>The name can be no longer than 64 characters.</p>	PORT123
InstanceName	<p>Define the name that will identify the arbitrary port being monitored.</p> <p>The following characters can be used for the name:</p> <ul style="list-style-type: none"> - Alphanumeric characters - Symbols (except for \;,<>"\$'[]=&) <p>The name can be no longer than 64 characters.</p>	PORT123
AlertTarget	<p>Define the node name (corresponding to the managed site) that is recognized by Centric Manager.</p> <p>When Centric Manager message linkage is performed, the defined node will become the node where an alarm will be generated.</p> <p>If this attribute is omitted, either the Manager or the Proxy Manager where this definition resides will become the node where an alarm will be generated.</p>	server123

Attribute name	Description	Definition example
IP_Address	Define the IP address of the service being monitored.	100.100.100.100
Port	Define the port number of the service being monitored.	123
NodeType	 Note <hr style="border-top: 1px dotted orange;"/> This attribute is used for control purposes. Do not change the value of this attribute in the sample file. <hr style="border-top: 1px dotted orange;"/>	I-D

 **Point**

To monitor multiple arbitrary ports, create multiple "PORT_Service" tags (blocks between <PORT_Service> and </PORT_Service>).

To remove PORT service collection targets, delete the block enclosed by the <PORT_Service> and </PORT_Service> tags.

6.3 Definition Example

In the sample definition file below, the site name "www.fujitsu.com" monitored by the Browser Agent is defined using "WebSite" tags, two monitored HTTP services ("AAAPage" and "BBBPage") are defined using "HTTP_Service" tags, and the DNS_Service, SMTP_Service and PORT_Service tags are defined.

Copy the sample definition, and paste it into the XML Source for OpeneXeed, overwriting any existing content.

The definitions will be updated, and it will become possible to check the configuration of XML Structure, and so on.

```

<?xml version="1.0" encoding="Shift_JIS"?>
<ServiceConf DisplayName="ManagedObject" NodeType="F">
<ResponseCondition DisplayName="ResponseCondition" NodeType="F">
<WebSiteList DisplayName="WebSites" NodeType="F">
<WebSite DisplayName="www.fujitsu.com" InstanceName="www.fujitsu.com" AlertTarget=""
NodeType="I-D">
<ResourceList DisplayName="Resources(URL)" InstanceName="" NodeType="F"/>
<URL DisplayName="URL" InstanceName="" AlertTarget="" NodeType="I-D">
<ResourceList DisplayName="Resources(URL)" InstanceName="" NodeType="F"/>
</URL>
<DNS DisplayName="DNS" InstanceName="" AlertTarget="" NodeType="I-D">
<ResourceList DisplayName="Resources(URL)" InstanceName="" NodeType="F"/>
</DNS>
<TCP DisplayName="TCP" InstanceName="" AlertTarget="" NodeType="I-D">
<ResourceList DisplayName="Resources(URL)" InstanceName="" NodeType="F"/>
</TCP>
</WebSite>
</WebSiteList>
</ResponseCondition>

```

```

<ServiceCondition DisplayName="ServiceCondition" NodeType="F">
<Default_ProxyServer Addr="" Port=""/>
<HTTP_ServiceList DisplayName="HTTP" NodeType="F">
<HTTP_Service DisplayName="AAA Home Page" InstanceName="AAAPage"
AlertTarget="manet" NodeType="I-D" IP_Address="" URL="http://manet.fujitsu.co.jp/"
ProxyServer="OFF" ProxyServer_Addr="" ProxyServer_Port="" BodyFile=""
BasicAuthentication="OFF" BasicAuthentication_User="" BasicAuthentication_PassWord=""/>
<HTTP_Service DisplayName="BBB Home Page" InstanceName="BBBPage"
AlertTarget="ent" NodeType="I-D" IP_Address="" URL="http://ent.fujitsu.co.jp/"
ProxyServer="OFF" ProxyServer_Addr="" ProxyServer_Port="" BodyFile=""
BasicAuthentication="OFF" BasicAuthentication_User="" BasicAuthentication_PassWord=""/>
</HTTP_ServiceList>
<DNS_ServiceList DisplayName="DNS" NodeType="F">
<DNS_Service DisplayName="DNS" InstanceName="DNS" AlertTarget="dnsserver"
IP_Address="100.100.100.100" Port="53" TargetHost="abcserver" NodeType="I-D"/>
</DNS_ServiceList>
<SMTP_ServiceList DisplayName="SMTP" NodeType="F">
<SMTP_Service DisplayName="SMTP" InstanceName="SMTP" AlertTarget="smtpserver"
IP_Address="100.100.100.100" Port="25" NodeType="I-D"/>
</SMTP_ServiceList>
<PORT_ServiceList DisplayName="PORT" NodeType="F">
<PORT_Service DisplayName="PORT123" InstanceName="PORT123"
AlertTarget="server123" IP_Address="100.100.100.100" Port="123" NodeType="I-D"/>
</PORT_ServiceList>
</ServiceCondition>
</ServiceConf>

```

6.4 Setup

In order to enable the changes to this file, a collection policy must be created and applied.

Execute the `sqcAPolicy` and `sqcSetPolicy` commands by referring to "[A.2 Response/Operation Information Collection Policy Creation Command](#)".

6.5 How to Create BODY Files

A BODY file must be created if HTTP POST communications are used to monitor the operation of HTTP services. When creating the BODY file, be sure to observe the points explained in this chapter.

Items that do and do not need to be specified in the BODY file

Monitoring Web services that use the POST method requires a BODY file. Of the messages sent to the Web service by a client using the POST method, those HTTP headers, parameters and parameter values that are requested by the service to be monitored must be defined in the BODY file.

For this reason, the content of the BODY file will vary according to the service to be monitored. This section explains those items that need to be specified in the BODY file, and those that do not.

Note that before attempting to create a BODY file, it is necessary to identify the parameters that will be requested by the service to be monitored.

This is explained below using the following sample transmission data.

Example of transmission data when using POST

```
1 POST /examples/servlet/HttpTestServlet HTTP/1.1
2 Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint,
application/vnd.ms-excel, application/msword, */*
3 Accept-Language: ja
4 Content-Type: application/x-www-form-urlencoded
5 Accept-Encoding: gzip, deflate
6 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; Q312461; .NET CLR
1.0.3705)
7 Host: localhost:8001
8 Content-Length: 33
9 Connection: Keep-Alive
10 Cache-Control: no-cache
11 Blank line
12 msg=Hello+World&submit=%91%97%90M
```

To perform monitoring using a BODY file, as in the above example, the user must prepare a BODY file that contains messages indicated by the blue text and has a linefeed appended to the end of the file.

The following shows the BODY file defined for the above example:

```
1 Content-Type: application/x-www-form-urlencoded
2 Blank line
3 msg=Hello+World&submit=%91%97%90M
```

1. Add the HTTP header "Content-Type". (Mandatory)
2. Use a linefeed to show the end of the header. (Mandatory)
3. Parameters and values. (Mandatory)


Note

The content of the BODY file depends on the Web service to be monitored.

Ask the Web service developer to explain the meaning of the HTTP header.

Note the points shown in the following table.

Item	Important point
Size of BODY file	The file size can be up to 64 KB. If this limit is exceeded, the excess portion of the file will be truncated, and the file may not function correctly.

Item	Important point
Location of file	When monitoring more than one HTTP service, always store all BODY files in the same directory.
File name	File names must be unique and consist of alphanumeric characters. Files should also be in plain text format (with extension ".txt").
Supported HTTP protocol versions	HTTP/1.0
Length of HTTP message bodies (Content-Length HTTP header)	<p>There is no need to specify the message length in the HTTP message header.</p> <p>The service processing performance monitoring function automatically calculates the length of the body of an HTTP message, adds the Content-Length HTTP header, and sends it to the Web server.</p> <p>If the length is specified (i.e., if the Content-Length header definition is duplicated), the behavior depends on the specifications of the destination Web server.</p>
Character encoding	<p>Ensure that the character encoding used in the BODY file is one that can be received by the Web server and application server. The service processing performance monitoring function does not convert character encodings.</p> <p> Note</p> <p>.....</p> <p>Note also that the service processing performance monitoring function does not support Base64 encoding or decoding.</p> <p>SOAP (XML) messages normally use UTF-8 or UTF-16, so the character encoding of the BODY file should be UTF-8 or ANSI.</p> <p>.....</p> <p>Refer to RFC-2279 (RFC 2279 UTF-8, a transformation format of ISO 10646) for a description of UTF-8.</p> <p>The version of Notepad provided with Microsoft® Windows 2000 can handle UTF-8.</p>

Ignoring empty lines in a BODY file

The service operation monitoring function ignores any empty lines that exist between the beginning and the end of the BODY file.

Ignoring the Byte Order Mark (BOM) at the beginning of a BODY file

When the version of Notepad provided with Microsoft(R) Windows 2000 saves a file in UTF-8 format, it unconditionally inserts a Byte Order Mark (BOM) at the beginning of the file.

The service operation monitoring function ignores the BOM when it reads a UTF-8 file created in Microsoft(R) Windows 2000, and sends the file to the Web server without the BOM attached.

If the BOM is not present, the file is sent to the Web server in its entirety.

The BODY file cannot be modified dynamically

The service operation monitoring function cannot dynamically modify a BODY file. For this reason, it is not possible to reply to a Web server by combining the response message from the Web server with the BODY file.

The service operation monitoring function does not support a mechanism by which a dynamically changing key such as a cookie must be sent by the POST method using the URL specified in [URL] when a service is registered.

Chapter 7 Eco Information Management

Power consumption and temperature of servers vary, depending on the applications being used, for example, so getting information about them is difficult. The ECO information management function makes power consumption and temperature of the monitored IT system available visually to help understand its current status. As well as making it easy to make plans to reduce power consumption, it also enables evaluation of the effects of such plans.

Execution environment

Can be executed under Manager/Proxy Manager.

Privileges required for execution

[Windows]

The Administrators group user privileges are required.

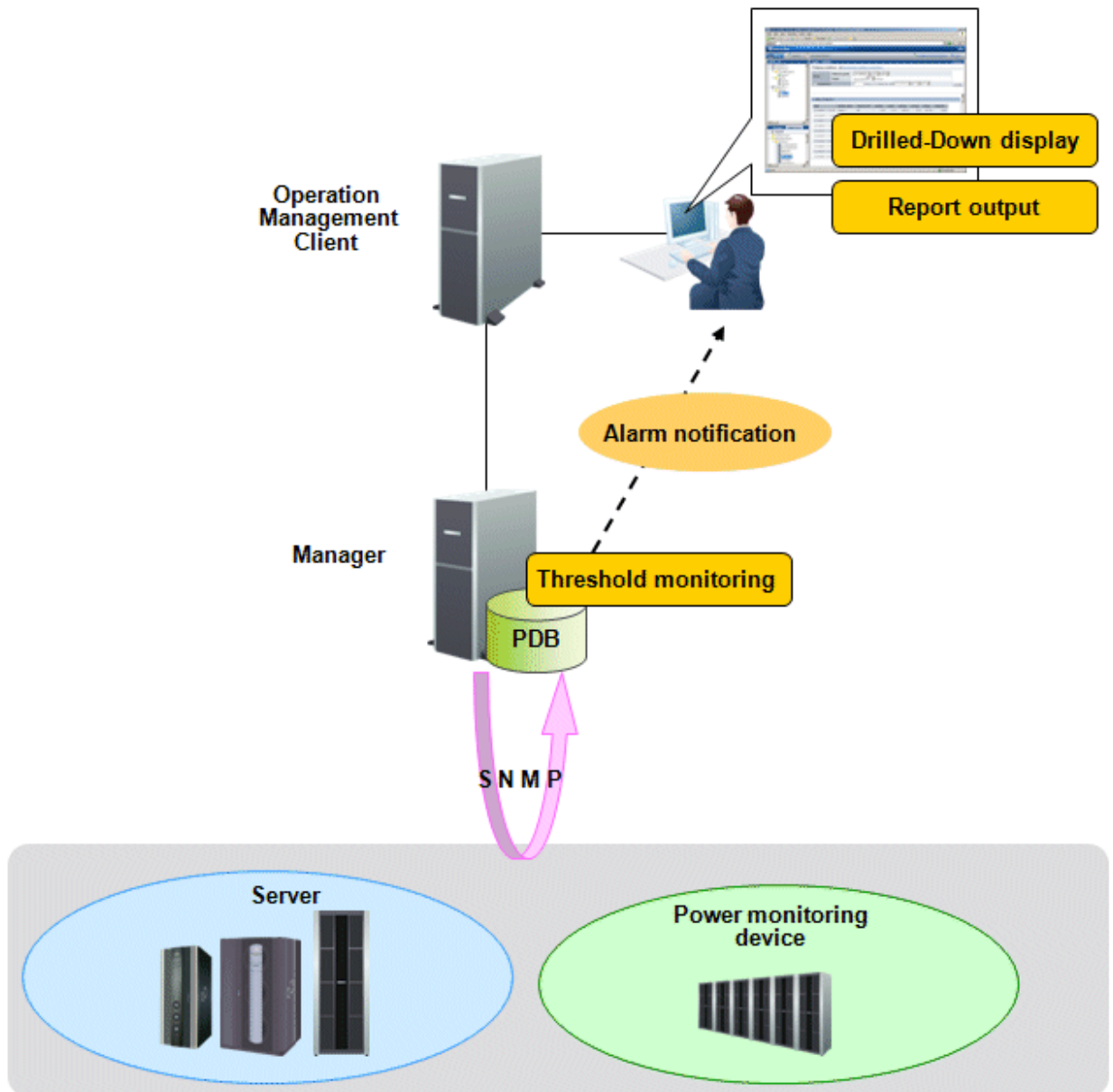
[UNIX]

System administrator (superuser) privileges are required.

7.1 Overview of Measurements Taken

Function overview

The ECO information management function uses the MIB interfaces of the commonly used SNMP to collect and display information from devices such as server or UPS that provide information about power and temperature.



Note: The devices to be monitored must meet the following conditions.

Prerequisites

Devices that can be monitored are as follows:

- The device to be monitored provides management information base (MIB) files (provided by the product and over the Web)
- The device to be monitored provides any of the following MIB object IDs (OID) for ECO information (power and temperature)
 - Power Information
 - Current power consumption and electrical energy
 - Temperature Information
 - Current temperature



Note

Before monitoring a device, ensure it meets the above two conditions.

Information that can be displayed

The ECO information management function displays the following information obtained from the information provided by the device to be monitored.

- Power Information
Power, average power, minimum power, maximum power, and electrical energy
- Temperature Information
Temperature, average temperature, minimum temperature, and maximum temperature

Collection interval

Collection interval is 10 minutes.

7.2 Checks before Installation

- The SNMP agent of the device to be monitored is running
- The device to be monitored can be connected to a network (through port number 161)



Note

Before monitoring a device, confirm its SNMP information.

7.3 Definition Method

Set in the following order:

1. Storing the MIB definitions file
2. Setting the ECO information collection definitions file
3. Setting the SNMP agent configuration file
4. Define collection template

7.3.1 Storing the MIB Definitions File

1. Prepare the MIB definition file, which defines the following information that the device to be monitored provides.
 - Power Information
Current power consumption and electrical energy
 - Temperature Information
Current temperature

- As the file name, use the module name that comes before "DEFINITIONS" in the first line of the file. Make the extension "txt".

Example: The first line in the MIB definitions file is as follows:

```
<First line of the MIB definitions>
OPL-SP-MIB DEFINITIONS ::= BEGIN
```

The module name is "OPL-SP-MIB", so the file name, after adding the extension "txt", is as follows:

```
<File name>
OPL-SP-MIB.txt
```

- Store the file created in the following folder:

[Windows]

```
<variable file storage directory>\control\mibs
```

[UNIX]

```
/etc/opt/FJSVssqc/mibs
```

7.3.2 Setting the ECO Information Collection Definitions File

Edit collectOID.txt (the ECO information collection definitions file) to define the object IDs (OID) of the ECO information to be monitored for each device.

File storage location

[Windows]

```
<variable file storage directory>\control\collectOID.txt
```

[UNIX]

```
/etc/opt/FJSVssqc/collectOID.txt
```

File format

ini file format

Setup items

Item	Description
[machinename] (Required)	This is a section name. Define the name of the device to be monitored.
mibfilename (Required)	Define the MIB file of the device to be monitored.
powerresource	To monitor more detailed units than the device, define the OID for those units. This appears in the resource ID as follows: "hostname:<sequence number>:powerresource" Note: "hostname" is the IP address (host name) defined in ecoAgentInfo.txt (the configuration information file of the device to be monitored).
power	Defines the power OID.

Item	Description
poweravg	Average power Defines the power OID (the same as "power"). (Calculated from power)
powermin	Minimum power Defines the power OID (the same as "power"). (Calculated from power)
powermax	Maximum power Defines the power OID (the same as "power"). (Calculated from power)
energy	Defines the electrical energy OID.
temperatureresource	To monitor more detailed units than the device, define the OID for those units. This appears in the resource ID as follows: "hostname:<sequence number>:temperatureresource" Note: "hostname" is the IP address (host name) defined in ecoAgentInfo.txt (the configuration information file of the machine to be monitored).
temperature	Defines the temperature OID.
temperatureavg	Average temperature Defines the temperature OID (the same as "temperature"). (Calculated from temperature)
temperaturemin	Minimum temperature Defines the temperature OID (the same as "temperature"). (Calculated from temperature)
temperaturemax	Maximum temperature Defines the temperature OID (the same as "temperature"). (Calculated from temperature)

Use alphanumeric characters only for all items.

Add sections when there are two or more devices to be monitored.

Example of definition

Definition example when SPARC Enterprise M3000 is to be monitored

```
[OPL-SP-MIB]
mibfilename=OPL-SP-MIB.txt
power=multiple:scfSystemActualPowerConsumptionValue
poweravg=multiple:scfSystemActualPowerConsumptionValue
powermin=multiple:scfSystemActualPowerConsumptionValue
powermax=multiple:scfSystemActualPowerConsumptionValue
temperature=multiple:scfSystemAmbientTemperatureValue
temperatureavg=multiple:scfSystemAmbientTemperatureValue
temperaturemin=multiple:scfSystemAmbientTemperatureValue
temperaturemax=multiple:scfSystemAmbientTemperatureValue
```

7.3.3 Setting the SNMP Agent Configuration Information File

Edit ecoAgentInfo.txt (the configuration information file of the device to be monitored) to define the device to be monitored from which ECO information is to be collected.

File storage location

[Windows]

```
<variable file storage directory>\control\ecoAgentInfo.txt
```


[UNIX]

/etc/opt/FJSVssqc/ecoAgentInfo.txt

When the SNMP version is v2 or v2c

Format:

IP address (host name), version, Community name, and device name

IP address (host name):

Specify the IP address or host name of the SNMP agent.

version:

Specify the SNMP version. You can specify either v2 or v2c.

If v2c is specified as the SNMP version, then the method of collecting performance information can be changed by specifying a value.

v2: Collects performance information with GETNEXT.

v2c: Collects performance information with GETBULK.

Community name

Specify the Community name of the SNMP agent.

device name

Specify the device name defined in collectOID.txt (the ECO information collection definitions file of the device to be monitored).

When the SNMP version is v3

Format:

IP address (host name), version, user name, password, authentication type, and device name

IP address (host name):

Specify the IP address or host name of the SNMP agent.

version:

Specify v3.

user name

Specify the user name used for authentication.

password

Specify the password for the user name used for authentication.

Specify the encrypted password generated with the genpwd command.

Refer to "[A.6 genpwd \(password encryption command\)](#)" for details about how to use the genpwd command to generate encrypted passwords.

authentication type

Specify MD5 (the default) or SHA.

device name

Specify the device name defined in collectOID.txt (the ECO information collection definitions file of the device to be monitored).

Example of definition

```
# List of parameter information for SNMP agents
server1,v2c,public,OPL-SP-MIB
server2,v3,demo ID,demo PW,MD5,OPL-SP-MIB
192.168.1.100,v3,admin,"",SHA,OPL-SP-MIB
```

7.4 Setup

Refer to "[A.1 Server Resource Information Collection Policy Creation Command](#)" and execute sqcRPolicy and sqcSetPolicy.

If a monitored server's definitions file has errors, that server will not be managed.

When sqcSetPolicy is executed, the following message is output for monitored servers that have been excluded from management due to errors in the definition.

```
(Warning) : <ECO> ecoAgentInfo.txt:ignored line(hostname[host name or IP address of monitored device])
```

The output host name or IP address of the monitored device is that defined in the "SNMP agent configuration information file".

The following message is also output if any errors are found in a definitions file.

```
(Warning) : <ECO> There is an error in definition.
Please confirm the file (file name).
```

The following is output to "file name".

[Windows]

```
<variable file storage directory>\log\setpolicy_error.log
```

[UNIX]

```
/var/opt/FJSVssqc/setpolicy_error.log
```

If this message appears, check the file content, correct the definitions file according to the message in the file, and then setup again. Refer to Section 1.1.3, "sqcSetPolicy (Policy Application Command)" in the *Reference Manual* for details about messages output to the file.

Note that collection policy setup must be passed to the console. Refer to Section 1.2.2.3, "Agents" in the *User's Guide (Console Edition)* and use the Agent Settings window to collect configuration information.

7.5 Display

ECO information is displayed as follows:

- Details

Display by selecting the ECO node in the Detailed tree.

- Reports

Detailed analysis/report

Note

- As the units used for data in different devices may be different, no units are displayed.
Confirm the units used for the data unit when setting the OID.

Chapter 8 Managing User Data

This chapter explains how to manage user-specific data such as business data and system operational data.

Any data whose format matches certain conditions can be stored in this product's PDB. Data stored in the PDB can be displayed using this product's Summary, Drilled-Down, and Report functions.

The "certain conditions" above refers to the following conditions:

- The fields in each record are delimited by commas (CSV format).
- There is a new line for each record.
- Each record has the same format.
- Each record contains a resource ID that identifies the record.

Execution environment

These settings can be made on Enterprise Managers, Managers, Proxy Managers and Agents.

Privileges required for execution

[Windows]

The privileges of a user belonging to the "Administrators" group are required to make these settings.

[UNIX]

System administrator (superuser) privileges are required to make these settings.

The following sections explain how to manage user data, in the following order.

- [8.1 Defining User Data](#)
- [8.2 Setup](#)
- [8.3 Storing User Data in the PDB](#)
- [8.4 Display](#)

8.1 Defining User Data

In order to manage user data, a user data definition file must be created.

Definition location

The user data definition file is a text file. Use a text editor such as Notepad to create and edit the file. The path to the file is as follows:

[Windows]

```
Variable file directory\control\udataconf.ini
```

[UNIX]

```
/etc/opt/FJSVssqc/udataconf.ini
```

8.1.1 Definition format

Create the user data definition file using the following format.

Syntax

```
[MIDDLEWARE_CONF]
XML=ON | OFF

[SELECT_RECORDID]
UDATA_1=ON | OFF
UDATA_2=ON | OFF
UDATA_3=ON | OFF
UDATA_4=ON | OFF
UDATA_5=ON | OFF

UDATA_20=ON | OFF
```

Point

- The vertical bars "|" mean "or". That is, either one option or the other can be specified.
- Blank lines are treated as comments.
- Lines that start with a hash "#" are treated as comments.

Description

[MIDDLEWARE_CONF]

Specifies whether to manage user data.

XML=ON | OFF

The meanings of each option are as follows:

Option	Meaning
ON	Manages user data.
OFF	Does not manage user data.

The default value is OFF.

[SELECT_RECORDID]

Selects the record IDs in the PDB that will be used to manage the user data.

Twenty types of record ID have been prepared - UDATA_1 to UDATA_20 (including SUM_UDATA_1 to SUM_UDATA_20 for each of these). Select which of these record IDs to use.

UDATA_1=ON | OFF

UDATA_2=ON | OFF

UDATA_3=ON | OFF

UDATA_4=ON | OFF

UDATA_5=ON | OFF

UDATA_20=ON | OFF

The meanings of each option are as follows:

Option	Meaning
ON	Selects the record ID. If a record ID is selected, the corresponding SUM_UDATA_1 to SUM_UDATA_20 are also selected.
OFF	Do not select the record ID.

The default value is ON.

Set record IDs that will not be used to OFF.

Example

[Windows/UNIX]

The following example shows a definition for managing two types of user data.

```
[MIDDLEWARE_CONF]
XML=ON
[SELECT_RECORDID]
UDATA_1=ON
UDATA_2=ONUDATA_3=OFF
UDATA_4=OFF
UDATA_5=OFF
UDATA_6=OFF
UDATA_7=OFF
UDATA_8=OFF
UDATA_9=OFF
UDATA_10=OFF
UDATA_11=OFF
UDATA_12=OFF
UDATA_13=OFF
UDATA_14=OFF
UDATA_15=OFF
UDATA_16=OFF
UDATA_17=OFF
UDATA_18=OFF
UDATA_19=OFF
UDATA_20=OFF
```

8.2 Setup

To enable the changes that have been made to the user data definition file, collection policies must be created and applied.

Execute the `sqcRPolicy` and `sqcSetPolicy` commands by referring to "[A.1 Server Resource Information Collection Policy Creation Command](#)".

After collection policies have been set up, they must be reflected to the Console on the operation management client. Use the Agent setup window to get configuration information by referring to Section 1.2.2.3, "Agents" in the *User's Guide (Console Edition)*.

8.3 Storing User Data in the PDB

Use the `sqcPDBcload` command to store user data in the PDB.

Refer to Section 1.7.2, "sqcPDBcload (User Data Input Command)" in the *Reference Guide* for more information about the `sqcPDBcload` command.

Note

When monitoring the threshold of user data, an alarm occurs when the defined value is exceeded by the value of the monitored item at the time that the user data is loaded into the PDB by the `sqcPDBcload` command.

Syntax

[Windows]

Installation directory\bin\sqcPDBcload.exe	-u udata-file -i conv-file
--	----------------------------

[UNIX]

/opt/FJSVssqc/bin/sqcPDBcload.sh	-u udata-file -i conv-file
----------------------------------	----------------------------

Options

-u udata-file

Specifies the user data file (CSV file) to be stored in a PDB.

-i conv-file

Specifies the data conversion definition file (as an ini file). A data conversion definition file specifies rules for converting user data to the record format used in a PDB. The following is an example:

```
[USERDATA]
consol_flag=2
record_id=1
col_resource_id=2,5
col_start_date_time=6
col_data_num1=10
col_data_num2=9
col_data_text1=4
```

[Data conversion definition file (conv-file)]

Refer to Chapter 4, "Data Formats" in the *Reference Guide* for information about the formats of the records that are generated.

consol_flag

Specify the data type. There are four data types, as shown below. Each of these data types has different display functions and storage periods. Decide which data type to use by referring to Section 3.2.2, "Manager" in the *Technical Guide*.

- 0: Summary data
- 1: Resource data (10 minutes)
- 2: Resource data (1 hour)
- 3: Resource data (24 hours)

If 0 is specified, record "SUM_UDATA_#n" is created.

If 1, 2 or 3 is specified, record "UDATA_#n" is created.

record_id

Specifies which record between "SUM_DATA_1" and "SUM_DATA_20" or between "U_DATA_1" and "U_DATA_20" is to be created.

col_resource_id

Specifies the field number of the user data file that will be set as a resource ID. A resource ID is a unique identifier for identifying a record.

In the case of process information, for example, the process name is used as the resource ID.

It is also possible to connect multiple fields and use these together as a resource ID. If "col_resource_id=2,5" is specified, fields 2 and 5 are used in combination as the resource ID.

col_start_date_time

Specifies the field number that will be set as the collection start time.

Note that data is stored in the following format:

'YYYY-MM-DD [hh[:mm[:ss]]]'

'MM-DD-YYYY [hh[:mm[:ss]]]'

(YYYY: year; MM: month; DD: day; hh: hour; mm: minute; ss: second)

"col_data_num1" to "col_data_num7"

Specifies the field number of the user data file data (numerical) to be stored in field "smud#data1" to "smud#data7" or "ud#data1" to "ud#data7" (up to ud#data5 when Record ID is UDATA_1, 2, 3, 6, 7, 8, 11, 12, 13, 16, 17, and 18).

"col_data_text1" to "col_data_text7"

Specifies the field number of the user data file data (text) to be stored in field "smud#txt1" or "ud#txt1" to "ud#txt7" (up to ud#txt5 when Record ID is UDATA_1, 2, 3, 6, 7, 8, 11, 12, 13, 16, 17, and 18.).

[Examples of data conversion definition files and the records that are created]

Data conversion definition file specification	Created record		Remarks
	Record ID	Field Name	
consol_flag=0 record_id=1 col_data_num3=9	SUM_UDATA_1	smud1data3	If "0" is specified for consol_flag, record "SUM_DATA_#n" is created. If "1" is specified for record_id, record "SUM_DATA_1" is created. If "9" is specified for col_data_num3, the 9th field of the CSV file is stored in field "sumud1data3".
consol_flag=1 record_id=1 col_data_num3=9	UDATA_1	ud1data3	If 1, 2 or 3 is specified for console_flag, record "UDATA_#n" is created. If "1" is specified for record_id, record "UDATA_1" is created.

Data conversion definition file specification	Created record		Remarks
	Record ID	Field Name	
			If "9" is specified for col_data_num3, the 9th field of the CSV file is stored in field "ud1data3".
consol_flag=3 record_id=2 col_data_num3=9	UDATA_2	ud2data3	If 1, 2 or 3 is specified for console_flag, record "UDATA_n" is created. If "2" is specified for record_id, record "UDATA_2" is created. If "9" is specified for col_data_num3, the 9th field of the CSV file is stored in field "ud2data3".

Example

[Windows]

```
C:\>cd C:\Program Files\SystemwalkerSQC\bin
C:\Program Files\SystemwalkerSQC\bin>sqcPDBcload -u C:\temp\udata.csv -i C:\temp\conv.ini
sqcPDBcload succeeded
```

[UNIX]

```
# cd /opt/FJSVssqc/bin/
# ./sqcPDBcload.sh -u /tmp/udata.csv -i /tmp/conv.ini
sqcPDBcload succeeded.
```

In this case, the content of udata.csv is as follows:

```
2004-09-09 10:00:00,kaminaka,2,octets,data,767872,28856,22400
```

The content of conv.ini is as follows:

```
[USERDATA]
consol_flag=2
record_id=1
col_resource_id=2,3
col_start_date_time=1
col_data_num1=6
col_data_num2=7
col_data_text1=4
```

8.4 Display

Information about user data can be displayed using the following method.

Summary view of the Console window

Use the "User data" node (UserDataMonitor) in the Summary tree.

Drilled-Down view of the Console window

Use the "UserData" node in the Detailed - "Agent" tree.

Report view

Displays detailed analysis/reports.



.....
The Summary view is displayed only if "consol_flag=0" is specified in the data conversion definition file that is specified as an option with the sqcPDBload command.
.....

Chapter 9 Collection Template

In order to collect performance information, definitions must be added to the collection template for some management targets.

This chapter explains how to make these definitions.

Storage location

The storage location of the definition file is as follows:

[Windows]

Variable file directory\control\template.dat

[UNIX]

/etc/opt/FJSVssqc/template.dat

Definition method

This file contains definitions for items that are always collected. Collection policies are created automatically according to these definitions when policies are created and applied.


However, when managing the following middleware, collection policies are created by adding extra settings to these definitions.

Management target	Name of the section in this definition file	Reference
Oracle Database Server	[ORA]	9.1 How to Set up Oracle Database Server
Microsoft .NET Server	[ATTR::AP]	9.2 How to Set Up Microsoft .NET Server
Microsoft SQL Server	[ATTR::DB]	9.3 How to Set Up Microsoft SQL Server
Hyper-V	[ATTR::AP]	9.4 How to Set Up Hyper-V
Red Hat Virtualization Function (Xen)	[ATTR::AP]	9.5 How to Set Up the Red Hat Virtualization Function (Xen)

9.1 How to Set up Oracle Database Server

To make Oracle a management target, define the following keys for the [ORA] section:

Item	Description	Definition example
[ORA]	The section name. Do not change this item.	ORA
DCAID	A specific ID for monitoring Oracle. Do not change this item.	"ORA"
INTERVAL	The collection interval in minutes.	5
SID	Set the Oracle instance name.	ORCL

Item	Description	Definition example
	 Point The name that is specified here is attached to the beginning of the resource ID.	
USERNAME	Enter the ID for the user that will access Oracle and obtain information from the dynamic performance view (an administrator user that has been granted a DBA role). The Oracle default is usually "system". If the default is to be changed, refer to " 9.1.1 How to create a new user that can access the Oracle dynamic performance view ".	System
PASS	Enter the password for the user that will access Oracle and obtain information from the dynamic performance view (an administrator user that has been granted a DBA role). The Oracle default is usually "manager". If the default is to be changed, refer to " 9.1.1 How to create a new user that can access the Oracle dynamic performance view ".	manager
VER	Specify the version of the Oracle instance to be monitored. Use the format "X.X.X".	9.2.0
ORAHOME	Set the value of ORACLE_HOME for the Oracle database to be monitored.	/opt/app/9iee/product/9.2.0

Definition example

```

:
#####
# Oracle Information
[ORA]
DCAID="ORA"
INTERVAL = 5
SID = ORCL
USERNAME = system
PASS = manager
VER = 9.2.0
ORAHOME="/opt/app/9iee/product/9.2.0"
:

```

Point

To monitor more than one instance of Oracle, perform the following steps:

1. Add the relevant section and set its parameters.
 - The section can be freely defined within a template, but the user should ensure that the section name is not duplicated. In the following example, the section name "ORA2" will be added.
 - Even when monitoring multiple Oracle instances, the value of the DCAID key must remain as "ORA".

Definition example

```

:
#####
# Oracle Information
[ORA]
DCAID="ORA"
INTERVAL = 5
SID = ORCL
USERNAME = system
PASS = manager
VER = 9.2.0
ORAHOME="/opt/app/9iee/product/9.2.0"
[ORA2]
DCAID="ORA"
INTERVAL = 5
SID = ORCL2
USERNAME = system
PASS = manager
VER = 9.2.0
ORAHOME="/opt/app/9iee/product/9.2.0"
:

```

2. Add the section added in step 1 above to the GROUP key of the ATTR::DB section. If the definition is as shown in the above example, amend as follows:

Before change

```

:
[ATTR::DB]
GROUP="SYMSAR,SYMPS,ORA"
:

```

After change

```

:
[ATTR::DB]
GROUP="SYMSAR,SYMPS,ORA,ORA2"
:

```

9.1.1 How to create a new user that can access the Oracle dynamic performance view



This operation is not required if the default ID and PASSWORD for Oracle are used.

To create a new user that can access the Oracle dynamic performance view, enter the following SQL command from svrmgr1 using an Oracle administrator ID (usually "system").

In the following example, the necessary privileges are given to a user with ID "id1" and password "pass1".

```
create user id1 identified by pass1;  
grant dba to id1;  
grant connect to id1;
```

9.2 How to Set Up Microsoft .NET Server

To make Microsoft .NET Server a management target, add "DOTNET" to the "GROUP" key in the [ATTR::AP] section.

Before change

```
:  
[ATTR::AP]  
GROUP="INTSG,SSC,DSA_JLA,UDATA,CNT"  
:
```

After change

```
:  
[ATTR::AP]  
GROUP="INTSG,SSC,DSA_JLA,UDATA,CNT,DOTNET"  
:
```

9.3 How to Set Up Microsoft SQL Server

To make Microsoft SQL Server a management target, add "MSSQL" to the "GROUP" key in the [ATTR::DB] section.

Before change

```
:  
[ATTR::DB]  
GROUP="SYMSAR,SYMPS,ORA"  
:
```

After change

```
:  
[ATTR::DB]  
GROUP="SYMSAR,SYMPS,ORA,MSSQL"
```

```
:
```

9.4 How to Set Up Hyper-V

To make Hyper-V a management target, add "HYPERV" to the "GROUP" key in the [ATTR::AP] section.

Before change

```
:  
[ATTR::AP]  
GROUP="INTSG,SSC,DSA_JLA,UDATA,CNT"  
:
```

After change

```
:  
[ATTR::AP]  
GROUP="INTSG,SSC,DSA_JLA,UDATA,CNT,HYPERV"  
:
```

9.5 How to Set Up the Red Hat Virtualization Function (Xen)

To make the Red Hat virtualization function (Xen) a management target, add "XEN" to the "GROUP" key in the [ATTR::AP] section.

Before change

```
:  
[ATTR::AP]  
GROUP="INTSG,SSC,DSA_JLA,UDATA,CNT,SNM "  
:
```

After change

```
:  
[ATTR::AP]  
GROUP="INTSG,SSC,DSA_JLA,UDATA,CNT,SNM,XEN "  
:
```

9.6 Middleware Linkage Settings with Enterprise Manager

Make these settings when managing middleware performance with an Enterprise Manager.

Change the parameters in the SERVeRTYPE section from OFF to ON.

Storage location

The storage location of this file is as follows:

[Windows]

```
<Variable file directory>\control\template.dat
```

[UNIX]

```
/etc/option/FJSVssqc/template.dat
```

Before change

```
:  
[SERVERTYPE]  
OS="ON"  
DB="OFF"  
AP="OFF"  
PM="OFF"  
WB="OFF"  
TA="ON"  
MG="ON"  
:
```

Definition example

- To monitor database servers:
DB="OFF" DB="ON"
- To monitor application servers:
AP="OFF" AP="ON"
- To monitor Web transactions:
WB="OFF" WB="ON"

```
:  
[SERVERTYPE]  
OS="ON"  
DB="ON"  
AP="ON"  
PM="OFF"
```



```
WB="ON"
TA="ON"
MG="ON"
:
```

Setup

Refer to "[A.1 Server Resource Information Collection Policy Creation Command](#)" and execute sqcRPolicy and sqcSetPolicy.

9.7 Stopping Middleware Management

When policy creation and application is executed, middleware is automatically detected and is managed according to the collection policy.

Do the following if you do not want the middleware to be managed.

Storage location

The storage location of the configuration file is as follows:

Windows

```
<variable file storage directory>\control\template.dat
```

UNIX

```
/etc/opt/FJSVssqc/template.dat
```

Setting method

1. Changing template.dat settings

This file defines items that are usually collected. Collection policy is automatically created at the time of policy creation and application execution according to these definitions.

In order to stop the middleware from being managed (automatically started by the collection policy), delete the parameters in this file (template.dat file) that correspond to the middleware.

Management target	Section name in this file	Parameter to delete from the GROUP key
Interstage Application Server	[ATTR::AP]	INTSG
Interstage Service Integrator	[ATTR::AP]	ISI
Systemwalker Operation Manager	[ATTR::AP]	DSA_JLA
Systemwalker Resource Coordinator(Storage) ETERNUS SF Storage Cruiser	[ATTR::AP]	SSC
Symfoware Server	[ATTR::DB]	SYMSAR SYMPS

Note

Make sure you make a backup copy of template.dat before making any adjustments to it.

Middleware that can be managed depends on the platform and type of installation. Parameters for middleware that is not subject to management may not be present in the template.dat file.

Do not change parameters that are not described in "Setting method".

2. Setup

Refer to "[A.1 Server Resource Information Collection Policy Creation Command](#)" and execute sqcRPolicy and sqcSetPolicy.

Setting example

To stop "Interstage Application Server" from being managed, delete the INTSG parameter from the GROUP key of the [ATTR::AP] section, as shown below.

Before setting

```
:  
[ATTR::AP]  
GROUP="INTSG,SSC,DSA_JLA,DSA_TDA,UDATA,CNT,SNM,SAP,ISI"  
:
```

After setting

```
:  
[ATTR::AP]  
GROUP="SSC,DSA_JLA,DSA_TDA,UDATA,CNT,SNM,SAP,ISI"  
:
```

Chapter 10 Threshold Monitoring

"Threshing monitoring" is a monitor function for monitoring whether the whole system is healthy or whether errors have occurred.

This product can define thresholds for threshold monitoring. These thresholds are defined on Managers, Agents or Proxy Managers. If monitored item values exceed the defined thresholds, an alarm will be generated.

Refer to "[10.3 Alarm Action Definitions](#)" for details on how to define alarm action executed when thresholds are exceeded.

Execution environment

These settings can be made on Enterprise Managers, Managers, Proxy Managers and Agents.



Make threshold monitoring definitions on the server collecting the information. Alarms will be activated on the server with the definitions.

Under a cluster system, make threshold monitoring definitions on both the active server and the standby server.

Locations for threshold monitoring definitions are as follows:

- Agent for Agent-based Monitoring

Make threshold monitoring definitions on the Agent (including Enterprise Manager/Manager/Proxy Manager using Agent functions) collecting the information.

Threshold monitoring cannot be performed by defining the Threshold Value of an agent for Agent-based monitoring on a Proxy Manager/Manager.

- Agent for Agentless Monitoring

Make threshold monitoring definitions on the Manager/Proxy Manager collecting the information remotely.

- End user response management

Make threshold monitoring definitions on the collecting server (Manager/Proxy Manager) collecting the end user response data.

- Service operation management

Make Threshold Monitoring definitions on the Manager/Proxy Manager collecting the information.

- Web transaction management

Make threshold monitoring definitions on the Manager/Proxy Manager/Agent for Business collecting the information.

- Eco Information Management

Make threshold monitoring definitions on the Manager/Proxy Manager collecting the information.

- User Data Management

Make threshold monitoring definitions on the Agent (including Manager/Proxy Manager using Agent functions) collecting the information.

Privileges required for execution

[Windows]

The privileges of a user belonging to the "Administrators" group are required to make these settings.

[UNIX]

System administrator (superuser) privileges are required to make these settings.

The following sections explain how to define thresholds:

- [10.1 Threshold Monitoring Definitions](#)
- [10.2 Threshold Monitoring Definition File \(Sample\)](#)
- [10.3 Alarm Action Definitions](#)

10.1 Threshold Monitoring Definitions

This section explains how to make definitions for threshold monitoring.

Storage location

The storage location of the definition file is as follows:

[Windows]

```
Variable file directory\control>alertconfig.txt
```

[UNIX]

```
/etc/opt/FJSVssqc/alertconfig.txt
```

Edit the above file according to the following definition method.




After this file has been placed in this location, its presence will be periodically checked (every 5 minutes) and recognized by this product, and then the definitions will be incorporated automatically. For this reason, edit this file from a different location, and place it in the storage location above when all of the definitions have been completed.

- [10.1.1 Definition Method](#)
- [10.1.2 Sample definition](#)

10.1.1 Definition Method

This file is in CSV format. Each item that will be subject to threshold monitoring is defined on a separate line.

Column	Description
1	<p>The threshold monitoring ID. Use a unique ID for each line.</p>  Note <p>.....</p> <p>When using the agent for Agentless Monitoring function</p> <p>Add "<host name>" after "threshold monitoring ID", with "<host name>" being the name of the host to be monitored when monitoring more than one server using the agent for Agentless Monitoring function on a Manager/Proxy Manager.</p>

Column	Description
	<p><threshold monitoring ID> <host name></p> <ul style="list-style-type: none"> - For the server monitored by Agent for Agent-based Monitoring function <p>Use the host name specified in "DISPLAYNAME" in the remote monitoring configuration file (remoteAgent.txt).</p> <ul style="list-style-type: none"> - When doing threshold monitoring of Manager/Proxy Manager itself. <p>Use the host name displayed in the sqcSetPolicy.</p> <p>Example: If the threshold monitoring ID is "AlertID1" and the name of the host to be monitored is "hostnameA": AlertID1 hostnameA</p> <p>Wildcards can be used for host names. Example: If the host name is "aaabbbccc", then any of the following examples will match it; "aaabbbccc", "aaa*", "aa?bb?cc?", "???bbb???", "[abc]aa[abc]bb[abc]cc".</p> <p>If " <host name>" is not added, then all servers being monitored will also have their threshold monitored.</p> <p>.....</p>
2	<p>The record number for the item being monitored. See "The correspondence between record numbers and field names for monitored items" for record number values.</p>
3	<p>Field name + record number of the item being monitored.</p> <p>Example: To monitor field name "usrproc" and record number "1052", specify "usrproc1052".</p> <p>See "The correspondence between record numbers and field names for monitored items" for field name and record number values.</p>
4	<p>Define the resource ID of the resource being monitored.</p> <p>The resource ID can be seen in the Resource ID column by displaying the content of the target node in the Console's Drilled-Down view.</p> <p>Wildcards can also be used in the resource ID.</p> <p>For example, if the resource ID is "aaabbbccc", then any of the following specifications will match this resource ID: "aaabbbccc", "aaa*", "aa?bb?cc?", "???bbb???", or "[abc]aa[abc]bb[abc]cc", and so on.</p>
5	<p>Define the name that will be used to send notifications regarding the monitored item.</p>
6	<p>Define the starting time for the time period for which threshold monitoring will be performed. Specify the time using HH:MM:SS format. This item cannot be omitted. For continuous monitoring (24 hours a day), specify "00:00:00" as the starting time.</p>
7	<p>Define the finishing time for the time period for which threshold monitoring will be performed. Specify the time using HH:MM:SS format. This item cannot be omitted. For continuous monitoring (24 hours a day), specify "00:00:00" as the finishing time.</p>
8	<p>Define the threshold violation count (N), which is the number of times (within the standard sampling count) that the threshold has to be exceeded before an alert will be notified.</p>
9	<p>Define the standard sampling count (M) for determining alert notifications. The maximum standard sampling count is 9 and the minimum value is 1. Specify an integer between 1 and 9 inclusive. If the sampling count is 1, define the threshold violation count as 1 as well.</p>

Column	Description
	Define the threshold violation count (N) and the standard sampling count (M) so that the following relationship exists: $N \geq M/2$
10	Warning threshold
11	Error threshold
12	Define either "<" or ">". >: Sends an alert notification if the value exceeds the threshold (useful for monitoring CPU usage, etc.). <: Sends an alert notification if the value drops below the threshold (useful for monitoring available memory, etc.).

Point

- The values that can be specified as the warning and error thresholds in the threshold monitoring definitions are as follows:
 - Integers
 - Real numbers (up to 15 decimal places can be specified)
 - Negative values can also be specified.
- It is not possible to specify only warning thresholds or only error thresholds in the threshold monitoring definitions.
- If a value that cannot occur (ex. To monitor thresholds for CPU usage, specify "120%" for the error threshold) is specified for the warning threshold, alarms will not be notified even if the error threshold is violated.

The correspondence between record numbers and field names for monitored items

Category	Record number	Field name	Item description
Processor	1052	usrproc	CPU usage in user mode
		sysproc	CPU usage in system mode
		intproc	UNIX: The time spent waiting for I/O to complete Windows: The time spent waiting for I/O to be interrupted
		totproc	Total CPU usage
Memory	1053	freemem	Available memory
		pagins	Page-in count
		pagflts	Page fault count
		swapused	The ratio of swap or page files being used
		pagouts	Page-out count
Disk	1054	dskreads	Number of disk reads
		dskwrits	Number of disk writes
		kbread	The number of disk reads per kilobyte
		kbwritn	The number of disk writes per kilobyte
		dsksrvtim	Read/write service time
		dskwaittim	Time spent waiting for read/write operations

The information in the table above is resource information relating to the operating system, which is displayed in the Summary window of the Console. Additional items can be monitored with threshold monitoring. In this case, specify the appropriate record numbers and field names by referring to Chapter 4, "Data Formats" in the *Reference Guide*.

10.1.2 Sample definition

A sample alertconfig.txt definition is shown below.

Refer to the detailed screen when you set the size of the threshold.

```
#####
# The following examples check the free space on all disks reported in 1018 records.
# The thresholds are a warning for less than 200MB and an error for less than 150MB.
#AlertId1,1018,free1018,*,FreeSpace,00:00:00,00:00:00,1,1,200000000.0,150000000.0,<

1,1052,usrproc1052,Total,UserCPU,00:00:00,00:00:00,1,1,80,95,>
2,1052,sysproc1052,*,SysCPU,00:00:00,00:00:00,1,1,80,95,>
3,1053,freemem1053,*,MEMORY,00:00:00,00:00:00,3,6,300000000,0,<
4,1053,freemem1053,*,MEMORY,00:00:00,00:00:00,1,1,50000000, 50000000,<
```

Explanation

- Issuing a warning if the CPU usage in user mode exceeds 80% even once, and an error message if the CPU usage exceeds 95% even once

```
1,1052,usrproc1052,Total,UserCPU,00:00:00,00:00:00,1,1,80,95,>
```

- Issuing an error message if the CPU usage in system mode exceeds 95% even once

```
2,1052,sysproc1052,*,SysCPU,00:00:00,00:00:00,1,1,95,95,>
```

- Issuing a warning message if the amount of free memory drops below 30% three times within 6 minutes
(Assuming that the total amount of memory is 1 GB = 1,000,000,000 bytes)

```
3,1053,freemem1053,*,MEMORY,00:00:00,00:00:00,3,6,300000000,0,<
```

- Issuing an error message if the amount of free memory drops below 5% even once.
(Assuming that the total amount of memory is 1 GB = 1,000,000,000 bytes)

```
4,1053,freemem1053,*,MEMORY,00:00:00,00:00:00,1,1,50000000, 50000000,<
```



Set as follows when system names "HostnameA" and "HostnameB" are to have their threshold monitored when monitoring more than one server using the agent for Agentless Monitoring function on a Manager/Proxy Manager:

```
HostnameA1|HostnameA,1052,usrproc1052,Total,UserCPU,00:00:00,00:00:00,1,1,80,95,>
HostnameA2|HostnameA,1052,sysproc1052,*,SysCPU,00:00:00,00:00:00,1,1,80,95,>
HostnameA3|HostnameA,1053,freemem1053,*,MEMORY,00:00:00,00:00:00,3,6,300000000,0,<
HostnameA4|HostnameA,1053,freemem1053,*,MEMORY,00:00:00,00:00:00,1,1,50000000, 50000000,<
HostnameB1|HostnameB,1052,usrproc1052,Total,UserCPU,00:00:00,00:00:00,1,1,80,95,>
```

```

HostnameB2|HostnameB,1052,sysproc1052,*,SysCPU,00:00:00,00:00:00,1,1,80,95,>
HostnameB3|HostnameB,1053,freemem1053,*,MEMORY,00:00:00,00:00:00,3,6,300000000,0,<
HostnameB4|HostnameB,1053,freemem1053,*,MEMORY,00:00:00,00:00:00,1,1,50000000, 50000000,<

```

Always set a unique ID for the "threshold monitoring ID" in the first column.

10.2 Threshold Monitoring Definition File (Sample)

The sample threshold monitoring definition file can be used to enable threshold monitoring to be performed with respect to the server performance information items shown in the following table.

Windows server performance information

If the monitored object is running Windows, the sample definition file can be used to monitor the following server performance information.

No.	Monitoring item	Evaluation method
1	CPU usage [%]	If the usage rate stays above 80% (48 seconds' usage in one minute), then there is a bottleneck at the CPU and performance problems may occur (or may have occurred already).
2	Physical disk idle time [sec]	If the disk busy rate for a physical disk stays above 60% (that is, if the physical disk is idle for less than 24 seconds in one minute), then the disk load is causing a bottleneck and performance problems may occur (or may have occurred already).
3	Free disk space[%]	Business activities may stop if the amount of free disk space becomes too low.
4	Free memory [bytes]	If the amount of free memory intermittently trends around 4 MB, then there is a memory bottleneck and performance problems may occur (or may have occurred already).

Solaris server performance information

If the monitored object is running Solaris, the sample definition file can be used to monitor the following server performance information.

No.	Monitoring item	Evaluation method
1	CPU usage [%]	If the usage rate stays above 90% (54 seconds' usage in one minute), then there is a bottleneck at the CPU and performance problems may occur (or may have occurred already).
2	Physical disk busy time [sec]	If the disk busy rate for a physical disk stays above 60% (that is, if the physical disk is busy for more than 32 seconds in one minute, then the disk load is causing a bottleneck and a performance problem may occur (or may have occurred already).
3	Free disk space [%]	Business activities may stop if the amount of free disk space becomes too low.

No.	Monitoring item	Evaluation method
4	Free memory [bytes]	If the amount of free memory intermittently trends around the value of the "lotsfree" kernel parameter (*1), then there is a memory bottleneck and performance problems may occur (or may have occurred already).

*1: The value that has been set for the "lotsfree" kernel parameter can be checked using the kstat command. By default, the value of this parameter is either 1/64 of physical memory or 512 KB, whichever is larger. Refer to the Solaris manuals for more information.

Linux server performance information

If the monitored object is running Linux, the sample definition file can be used to monitor the following server performance information.

No.	Monitoring item	Evaluation method
1	CPU usage [%]	If the usage rate stays above 90% (54 seconds' usage in one minute), then there is a bottleneck at the CPU and performance problems may occur (or may have occurred already).
2	Physical disk busy time [sec]	If the disk busy rate for a physical disk stays above 80% (that is, if the physical disk is busy for more than 48 seconds in one minute), then the disk load is causing a bottleneck and a performance problem may occur (or may have occurred already).
3	Free disk space [%]	Business activities may stop if the amount of free disk space becomes too low.
4	Available memory space [bytes]	If the amount of free memory tends to intermittently show a low value, then memory shortages may be a bottleneck and a performance problem may occur (or may have occurred already). The threshold value for the amount of free memory varies according to factors such as the version of Linux, the edition and the amount of memory on board. It should be adjusted to suit the operating conditions. The free memory threshold is set at 5,120 KB in the sample file.

Storage directory

The sample file is stored in the following directory:

[Windows]

<Installation directory >\sample>alertconfig.txt

[UNIX]

/opt/FJSVssqc/sample/alertconfig.txt



To use the sample definition file on a server where threshold monitoring is being performed, back up the existing threshold definition file (alertconfig.txt) and then overwrite it with the sample definition file.

10.3 Alarm Action Definitions

Execution environment

These settings can be made on Enterprise Managers, Managers, Proxy Managers and Agents.

Privileges required for execution

[Windows]

The privileges of a user belonging to the "Administrators" group are required to make these settings.

[UNIX]

System administrator (superuser) privileges are required to make these settings.

Once threshold monitoring is defined, any threshold violation will result in an action to report the violation to the administrator. The following action types are available:

- Event log/syslog
- Systemwalker Centric Manager message linkage
- Mail
- Trap
- Execution of user-specified command

When installation is complete, the event log/syslog or Systemwalker Centric Manager message linkage is set up according to the answer that the user provides in response to the queries given by the installer.



- Threshold alarms are generated only when thresholds are exceeded. If the value being monitored remains over (or under) the threshold continuously, an alarm will be generated only the first time the threshold is exceeded, and no further alarms will be generated until the monitored value returns to the normal range.
- Under a cluster system, make the settings on both the active server and the standby server.

Storage location

The storage location of this definition file is as follows:

[Windows]

Installation directory\bin\threshold.bat
--

[UNIX]

```
/opt/FJSVssqc/bin/threshold.sh
```

10.3.1 Definition method

10.3.1.1 Defining the action type

The execution of actions is controlled by an ON/OFF specification. When an action is set to ON, it will be executed. More than one action can be set to ON.

Definition content	Meaning
EVENTLOG="ON" or SYSLOG="ON"	Event log or syslog
OPAPOST2="OFF"	Systemwalker Centric Manager message linkage
MAIL="OFF"	Mail
TRAP="OFF"	Trap
OTHER="OFF"	Execution of user-specified command



Note

- If MAIL, TRAP, or OTHER is selected, the following detailed parameters must be defined.
- Do not delete the definitions for parameters that are not used.

- [10.3.1.2 When MAIL is selected](#)
- [10.3.1.3 When TRAP is selected](#)
- [10.3.1.4 When OTHER is selected](#)

10.3.1.2 When MAIL is selected

[Windows]

Define the parameters associated with Windows mail notifications.

Definition content	Meaning
MAILSMTPSRV="00.00.00.00"	Address of the SMTP server
MAILSMTPPRT="25"	Port of the SMTP server
MAILFROM="aa@xx.co.jp"	Address of sender ("From")
MAILTO="bb@xx.co.jp"	Address of recipient ("To")
MAILPOP3PRT="110"	POP3 server port (if POP authentication is required)
MAILPOP3SRV="00.00.00.00"	POP3 server address (if POP authentication is required)
MAILAUTHTYPE="Pop"	Specify "Pop" if POP authentication is required.
MAILUSERID=""	User ID (if POP authentication is required)
MAILPASSWD=""	Password (if POP authentication is required)

Definition content	Meaning
MAILCC="cc@xx.co.jp, dd@xx.co.jp"	"Cc" address of mail
MAILBCC="ee@xx.co.jp, ff@xx.co.jp"	"Bcc" address of mail
MAILSUB="SSQC threshold %MSGINFO%: %2(%PARA3%)"	"Subject" of mail The following variable parameters (% followed by characters) can be specified: %2: System name %PARA3%: Monitoring item name %PARA4%: Resource ID %5: Measurement value %6: Threshold %7: Number of times detected %8: Criterion for the number of times detected

Note

If POP authentication is not required, modify the parameters as follows:

- MAILPOP3PRT=""
- MAILPOP3SRV=""
- MAILAUTHTYPE=""
- MAILUSERID=""
- MAILPASSWD=""

[UNIX]

Define the parameters associated with Solaris/Linux mail notifications.

Definition content	Meaning
MAILSMTPSRV="00.00.00.00"	Address of the SMTP server
MAILSMTPPRT="25"	Port of the SMTP server
MAILFROM="aa@xx.co.jp"	Address of sender ("From")
MAILTO="bb@xx.co.jp"	Address of recipient ("To")
MAILPOP3PRT="110"	POP3 server port (if POP authentication is required)
MAILPOP3SRV="00.00.00.00"	POP3 server address (if POP authentication is required)
MAILAUTHTYPE="Pop"	Specify "Pop" if POP authentication is required.
MAILUSERID=""	User ID (if POP authentication is required)
MAILPASSWD=""	Password (if POP authentication is required)
MAILCC="cc@xx.co.jp, dd@xx.co.jp"	"Cc" address of mail
MAILBCC="ee@xx.co.jp, ff@xx.co.jp"	"Bcc" address of mail

Definition content	Meaning
MAILSUB="SSQC threshold \$MSGINFO: \$2(\$3)"	"Subject" of mail The following variable parameters (% followed by characters) can be specified: \$2: System name \$3: Monitoring item name \$4: Resource ID \$5: Measurement value \$6: Threshold \$7: Number of times detected \$8: Criterion for the number of times detected

 **Note**

If POP authentication is not required, modify the parameters as follows:

- MAILPOP3PRT=""
- MAILPOP3SRV=""
- MAILAUTHTYPE=""
- MAILUSERID=""
- MAILPASSWD=""

10.3.1.3 When TRAP is selected

Define the parameters associated with trap notifications.

Definition content	Meaning
TRAPAGT="\$2"	Address of Trap agent
TRAPDEST="hostname"	Address of Trap destination
TRAPCOMMUNITY="public"	Trap community name
TRAPENTERPRISE="1.3.6.1.4.1.211"	Enterprise value of Trap
TRAPGENERIC="6"	Generic value of Trap
TRAPSPECIFIC="1"	Specific value of Trap
TRAPOBJNAME="1.3.6.1.4.1.211"	Object name
TRAPOBJTYPE="2"	Object type

10.3.1.4 When OTHER is selected

It is possible to execute a command specified by the user.

Specify the command name on the following line:

SQCOTHEREXE=""

Edit the processing that begins on the following line according to the specifications of the command:

```
if "%OTHER%"=="ON" (
```

Chapter 11 Policy Distribution

This chapter presents an overview of the policy distribution function and explains how to use it.

- [11.1 Overview of the Policy Distribution Function](#)
- [11.2 Policy Distribution Procedure](#)
- [11.3 Supplementary Notes](#)

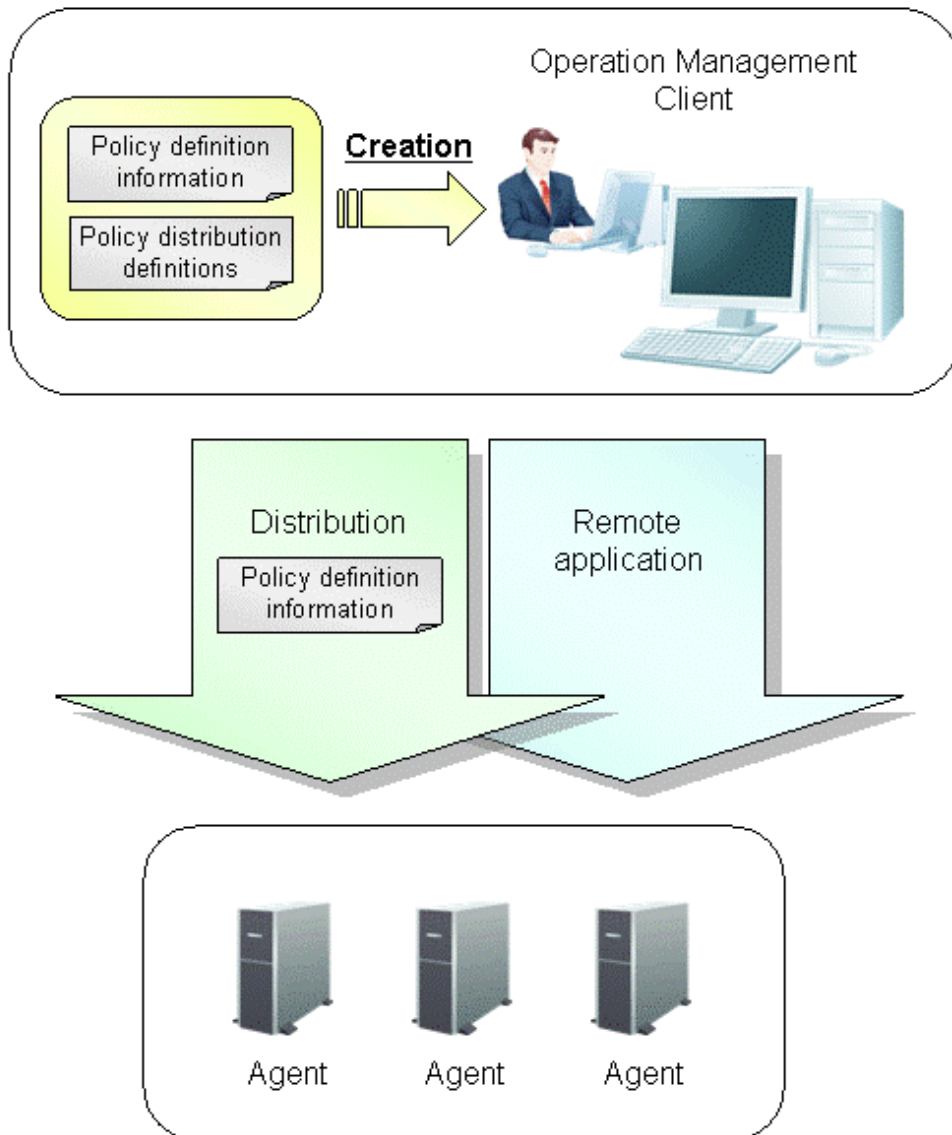
11.1 Overview of the Policy Distribution Function

This section presents an overview of the policy distribution function.

- [11.1.1 Policy distribution function](#)
- [11.1.2 Usage conditions for the policy distribution function](#)
- [11.1.3 The Directory Structure of the Definition Folder](#)

11.1.1 Policy distribution function

"Policy distribution" refers to a function that distributes definition information (relating to performance information collection and threshold monitoring) from the operation management client to each server.



Note 1: "Policy definition information" refers to collection policies and threshold monitoring definitions.

Note 2: When distributing policies to Managers, distribute the policies to the Agent function on the Manager.

Features

The policy distribution function has the following features:

- There is no need to log in to managed servers, or set up definitions for each individual managed server.
- Definitions for managed servers can be set up in a single operation, whereas previously each managed server had to be set up individually.

Note

Policy distribution function cannot be used if basic authentication settings are used when setting up connection environment for operation management client.

Procedure

Perform the following operations on the operation management client in order to use the policy distribution function.

1. Create the definition information files

Create the definition information files to be distributed to the servers where performance information (such as server resource information and response/operating information) is collected or where threshold monitoring is performed.

2. Define distribution destination servers

Define information about distribution destination servers in policy distribution definition files.

3. Distribute the definition information created in step 1 to the servers defined in step 2.

Execute the command for distributing policy definition information to the distribution destination servers.

4. Create and apply collection policies for the distribution destination servers

Create and apply collection policies on the distribution destination servers remotely by executing the operation command.



The policy distribution function is particularly effective when distributing the same definitions to multiple servers. Use this function according to the number and status of the managed servers.

Note that certain conditions, such as the version of Systemwalker Service Quality Coordinator, must be met when the policy distribution function is used.

The following sections explain the operating conditions for the policy distribution function.

11.1.2 Usage conditions for the policy distribution function

11.1.2.1 Versions with which the policy distribution function can be used

The versions of Systemwalker Service Quality Coordinator with which the policy distribution function can be used are as follows:

Operation Management Client V/L and Manager V/L	Destination server V/L		
	V11.0L10 to V13.2.0	V13.3.0/V13.4.0	V13.5.0
V11.0L10 to V13.2.0	-	-	-
V13.3.0/V13.4.0	No	(*1)	No
V13.5.0	No	Yes (*2)	Yes (*2)

*1: Refer to V13.3.0 or V13.4.0 manuals.

*2: The policy distribution function to Manager and Enterprise Manager composed of the cluster is excluded.

-: No policy distribution function

Yes: Policies can be distributed

No: Policies cannot be distributed

11.1.2.2 Operating conditions for the policy distribution function

The following conditions must be met when the policy distribution function is used.

1. The DCM service/daemon and the thttpd service/daemon must be running on the connection destination server (Manger) for the operation management client.
2. The connection destination server for the distribution destination servers (servers with Agent functions) must be the Manger in 1.
3. The DCM service/daemon and the thttpd service/daemon must be running on the distribution destination server.

Refer to "[A.4 How to Start and Stop Resident Processes](#)" for information about how to start the DCM service/daemon and the thttpd service/daemon. Refer to Chapter 2, "Starting and Stopping Resident Processes" in the *Reference Guide* for information about these processes.

11.1.3 The Directory Structure of the Definition Folder

Definitions for the policy distribution function are made on the operation management client.

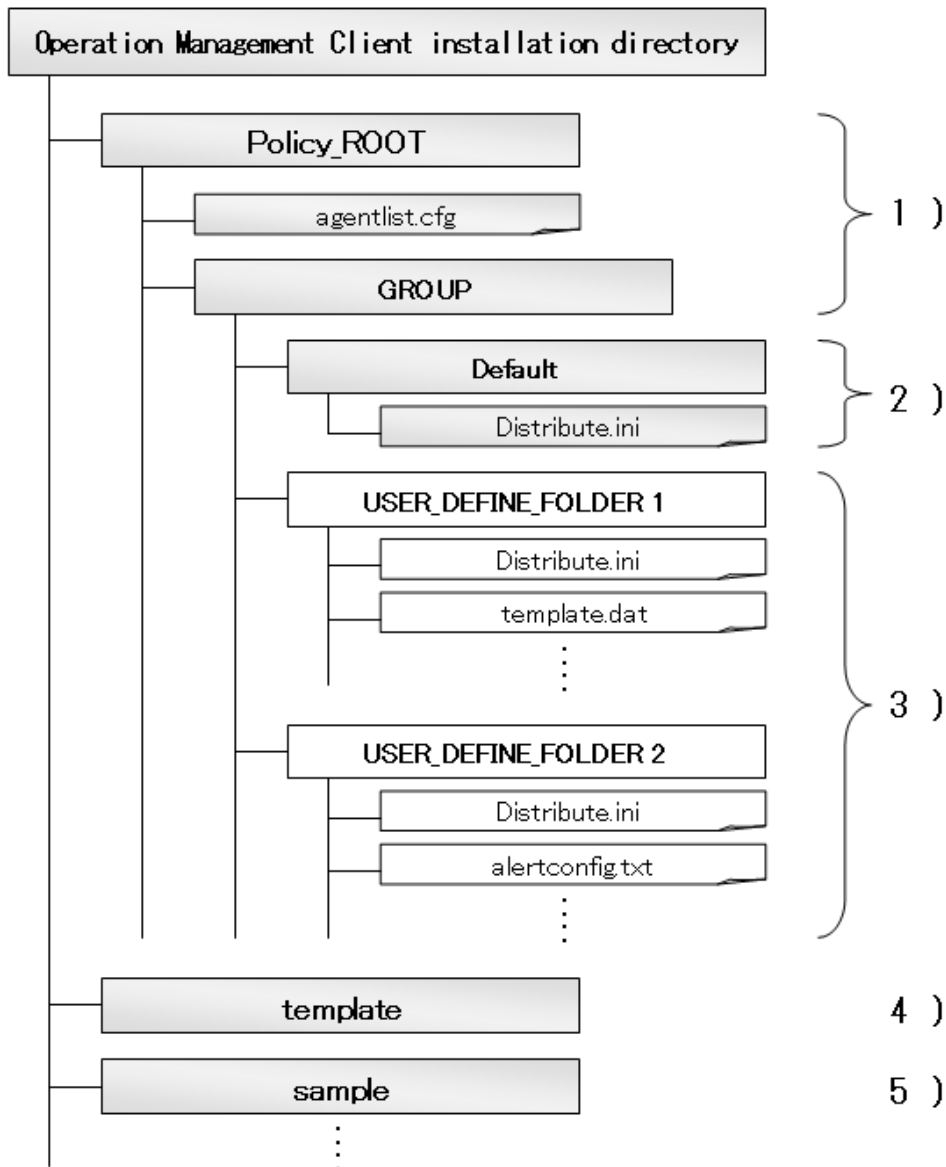
This section explains the directory structure of the policy management folder that stores these definitions.

- Create policy definition information files for collecting performance information (server resource information and response/operating information) and for performing threshold monitoring.
- Create a policy distribution definition file (Distribute.ini) to define which servers the policy definition information files should be distributed to.

Storage location

The policy management folder is on the Operation Management Client.

<Operation Management Client installation directory>\Policy_ROOT
--



The gray part indicates the files that exist by default.

1. Policy management folder (Policy_ROOT, GROUP)

The policy management folder is where policy distribution groups are stored.

The policy management folder (Policy_ROOT) contains connection destination definition files (agentlist.cfg), which define connection information for policy distribution destination servers.

2. Policy distribution group folder (Default)

The "Default" folder is the base for folders for each policy group. It is created at installation time,

Either use the "Default" folder as the policy distribution group folder or create multiple policy distribution group folders by copying the "Default" folder. The default policy distribution group folder contains a policy distribution definition file (Distribute.ini) for specifying distribution destinations.

3. Policy distribution group folder

When Systemwalker Service Quality Coordinator is first installed, only the "Default" folder exists.

To add more policy distribution groups, create policy distribution groups by copying and then renaming the "Default" folder under the "GROUP" folder. The names of these new folders are used to specify the policy distribution group when policies are distributed.

The policy definition information files that are distributed to servers are also stored in the policy distribution group folders.

4. **Template folder(template)**

The template folder contains templates of policy definition information files to be distributed for each version level and each operating system as a package. Use these templates by copying them into policy distribution groups according to the version level and operating system of the distribution destination.

5. **Sample folder (sample)**

The sample folder contains sample definition files that are used for threshold monitoring and Web transaction volume management. These files are preset definition files and can be used by copying to a folder. Sample definitions are the same as for those stored on the Agent.

Refer to "[10.2 Threshold Monitoring Definition File \(Sample\)](#)" and "[2.4 Transaction Log Definition File \(Sample\)](#)" for the definition content.



When the policy distribution function is used to perform threshold monitoring or Web transaction volume management, use the sample definition files stored in the "sample" folder.



Definition information being distributed is not encrypted. For this reason, when using the function for linking with Oracle Database Server or SAP NetWeaver that requires password definition, do not perform policy distribution.

Refer to "[11.2.2 Creating policy definition information files](#)" for more information about definition information files.

11.2 Policy Distribution Procedure

This section explains the procedure for implementing the policy distribution function.

Privileges required for execution

[Windows]

The privileges of a user belonging to the "Administrators" group are required to make these settings.

Execution environment

This procedure can be performed on the operation management client.

- [11.2.1 Creating policy distribution groups](#)
- [11.2.2 Creating policy definition information files](#)
- [11.2.3 Creating policy distribution definition files](#)
- [11.2.4 Creating connection destination definition files](#)
- [11.2.5 Policy Distribution](#)
- [11.2.6 Creating and applying policies remotely](#)

11.2.1 Creating policy distribution groups

Procedure

Create folders in the Operation Management Client installation directory using Windows Explorer or some other tool in order to create policy distribution groups.

The names of the folders that are created are used to specify the policy distribution group when policies are distributed.

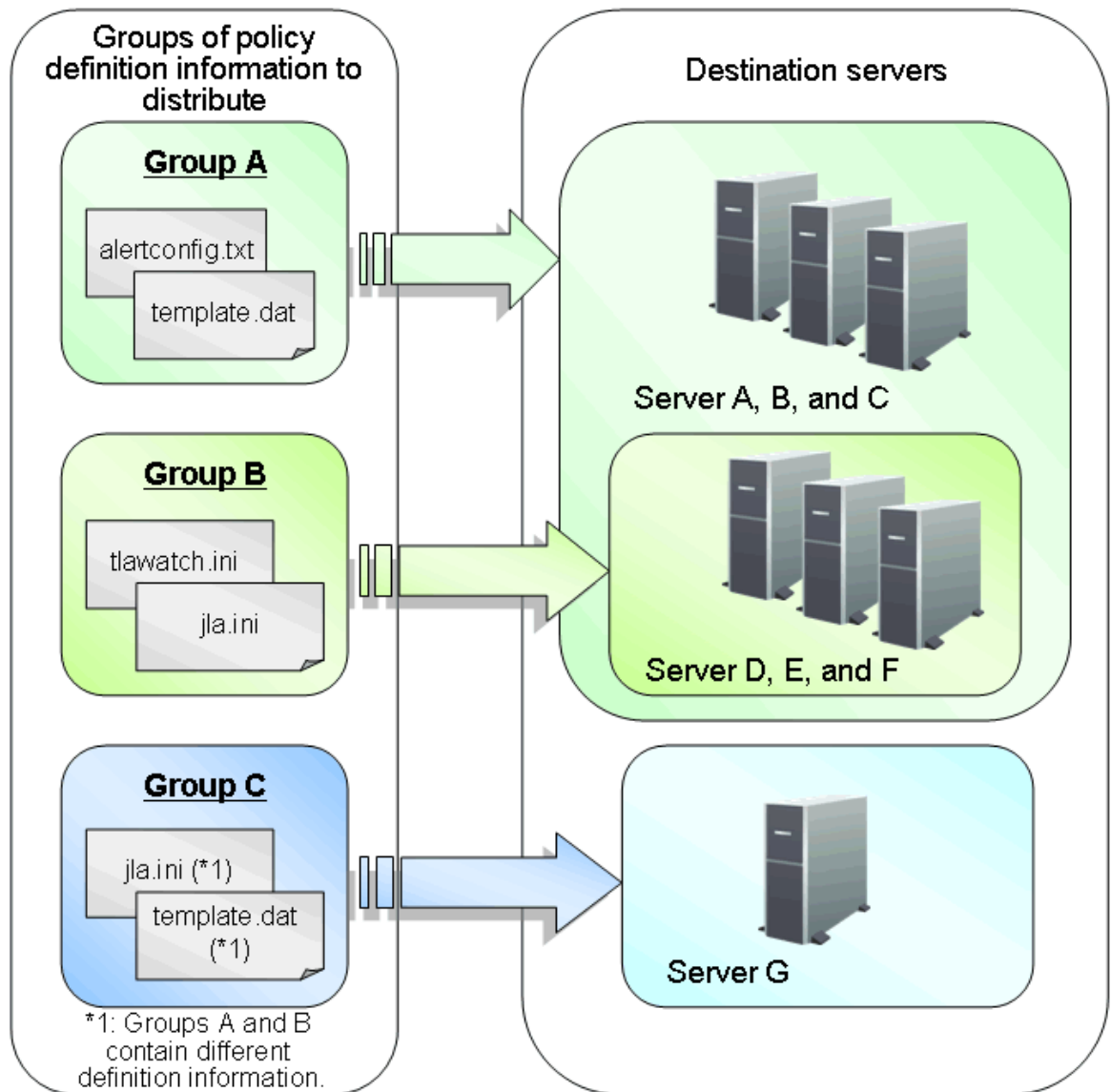
Create folders using any desired name, and store the policy definition information files to be distributed in these folders.

Storage location

```
<Operation Management Client installation directory>\Policy_ROOT\GROUP
```

Create the necessary policy distribution groups by referring to the following example.

Example



Groups A, B and C in the figure are policy distribution groups.

Group A

Group A is a group for policy definition information files to be distributed to all servers except Server G.

Group B

Group B is a group for policy definition information files to be distributed to servers D, E and F.

Group C

Group C is a group for policy definition information files to be distributed to server G only.

By creating multiple groups for distributing policies, different policy definition information can be distributed to only the necessary servers.

If groups A, B and C in the example above are labeled "PolicyGP01", "PolicyGP02" and "PolicyGP03" respectively, create the following folders and store the appropriate policy definition information files in each folder.

```
<Installation directory>\Policy_ROOT\GROUP\PolicyGP01
```

```
<Installation directory>\Policy_ROOT\GROUP\PolicyGP02
```

```
<Installation directory>\Policy_ROOT\GROUP\PolicyGP03
```

11.2.2 Creating policy definition information files

Create the definition information files that will be distributed to the servers where performance information (server resource information and response/operating information) is collected or threshold monitoring is performed.

Policy definition information files

The policy distribution function can be used to distribute collection policies and threshold monitoring definitions. These definitions are collectively referred to as "policy definition information".

Collection policies

- Server resource information (server information/middleware information)
 - Managed object configuration information (resource configuration information)
 - Templates (information to be collected continuously)
- Response/operating information
 - Managed object configuration information (response/operating managed object configuration information)
 - Templates (information to be collected continuously)

Threshold monitoring definition

- Threshold monitoring definition



Note

Collection policies are made up of multiple definition files. However, some settings files, for agent for Agentless Monitoring, virtual resource management, ECO information, and linking to non-Fujitsu products (such as Oracle and SAP), must be made on each individual server and cannot be distributed as policies. This is because there will be a risk in security

management if definition information is set up and stored on the operation management server and then transmitted over the network when authentication information is required.

Procedure

1. Copy the policy definition information file to be distributed

Templates for policy definition information files are stored in the following locations.

Storage location of sample files

<Operation Management Client installation directory>\template

Copy the sample policy definition information templates as required, and store them in the policy distribution group folders that were created in "11.2.1 Creating policy distribution groups".

The following files can be distributed. No other files can be distributed.

File name	Usage	Reference
ServiceConf.xml	Managing end user responses	Chapter 4 Managing End User Response
	Managing the operational status of services	Chapter 6 Response and Managed Object Configuration Information (ServiceConf.xml)
alertconfig.txt	Making definitions for threshold monitoring	Chapter 10 Threshold Monitoring
threshold.bat (Windows)	Making definitions for alarm actions	10.3 Alarm Action Definitions
threshold.sh (UNIX)	Making definitions for alarm actions	10.3 Alarm Action Definitions
tlawatch.ini	Managing the volume of Web transactions	Chapter 2 Managing the Volume of Web Transactions
cntrconf.ini	Linking to Systemwalker Centric Manager	1.4 Linking to Systemwalker Centric Manager
jla.ini	Linking to Systemwalker Operation Manager	1.5 Linkage with Systemwalker Operation Manager
snmconf.ini	Linking to Systemwalker Network Manager	1.6 Linking to Systemwalker Network Manager
template.dat	Microsoft SQL Server	1.10 Linking to Microsoft SQL Server
	Microsoft .NET Server	1.11 Linking to Microsoft .NET
	Setting the log data (Troubleshoot) retention period	Section 6.7.2, " Changing the retention period of log data (Troubleshoot)" in the <i>Installation Guide</i>

2. Make definitions in the policy definition information files that are copied.

Refer to the relevant sections shown above for information about how to make definitions in each of these files.



Linefeed code is automatically converted to suit the destination server during policy distribution.

11.2.3 Creating policy distribution definition files

Define the distribution destination servers for each policy distribution group in policy distribution definition files (Distribute.ini).

Create a policy distribution definition file (Distribute.ini) for each policy distribution group folder and use it to define the distribution destinations for each policy distribution group.

By creating policy distribution definitions in advance, policies can be automatically distributed to these destinations.

Creating policy distribution definition files (Distribute.ini) is not absolutely necessary, but creating definition files when Systemwalker Service Quality Coordinator is first installed does reduce the administrative workload when collection policies are changed during operations. This is because definition information can be distributed as a batch to only those servers that are affected.

Storage location

Policy distribution definition files (Distribute.ini) are text files. Use a text editor such as Notepad to create and edit these files. The paths to these files are as follows:

[Windows]

```
<Operation Management Client installation directory>\Policy_ROOT\GROUP\<Policy distribution group folder>\Distribute.ini
```

File format

```
[POLICY_DEF]
DISTHOST =
```

Explanation

[POLICY_DEF]

Define the distribution destination servers for the policy definition information using the DISTHOST key in this section.

DISTHOST

Use host names to define the distribution destination servers for the policy distribution group. Multiple distribution destination servers can be specified by separating each server with a comma (",").



Policies can also be distributed by specifying distribution destination servers directly using a parameter of the Policy Definition Information Distribution Command. However, creating this definition file in advance reduces the administrative workload if collection policies are changed during operation.

Usage example

If the distribution destinations for a certain policy distribution group are HOSTA, HOSTB, HOSTC and HOSTD, then specifying HOSTA, HOSTB, HOSTC and HOSTD in a definition file beforehand eliminates the need to specify the distribution destination servers again when collection policies are changed later, and also reduces the likelihood of omissions.

Use the DISTHOST key in the [POLICY_DEF] section to define the distribution destination servers in the policy definition information. Specify the host names in DISTHOST.

Multiple host names can be specified by separating each name with a comma.

```
#[POLICY_DEF]
#DISTHOST = AAAA,BBBBBB,CCCC,DDDDD
[POLICY_DEF]
DISTHOST =
HOSTA,HOSTB,HOSTC,HOSTD,HOSTE,HOSTF,HOSTG,HOSTH,HOSTI,HOSTJ,HOSTL
```

11.2.4 Creating connection destination definition files

Connection destination definition files (agentlist.cfg) are used to define connection information for policy distribution destination servers.

If multiple IP addresses exist in a policy distribution destination server, the operation management client may be unable to connect to the server by using connection information that is obtained automatically. To prevent this kind of problem, use a connection destination definition file (agentlist.cfg) to define information that enables the operation management client to connect to the policy distribution destination server. Connection information defined in agentlist.cfg takes precedence over connection information that is obtained automatically.

Storage location

Connection destination definition files (agentlist.cfg) are text files. Use a text editor such as Notepad to create and edit these files. The paths to these files are as follows:

[Windows]

```
<Operation Management Client installation directory>\Policy_ROOT\agentlist.cfg
```

File format

Add the following entry for each host name.

```
[AgentList]
host name,http://connection destination:port number/SQC/
```

Definition method

connection destination: Define an IP address or host name that can be connected from the operation management client.

port number: Define a port number that is used for policy distribution.

Definition example

The following is a definition example of agentlist.cfg:

```
[AgentList]
system_name1, http://192.168.111.333:23440/SQC/
system_name2, http://192.168.111.444:23440/SQC/
```

11.2.5 Policy Distribution

To distribute the policy definition information files to the distribution destination servers, execute the sqcSendPolicy command (Policy Definition Information Distribution Command) on the operation management client.

Refer to Section 1.1.6, "sqcSendPolicy (Policy Definition Information Distribution Command)" in the *Reference Guide* for more information about the sqcSendPolicy command (Policy Definition Information Distribution Command)

Privileges required for execution

[Windows]

The privileges of a user belonging to the "Administrators" group are required to make these settings.

Before performing this procedure

Check that the operating conditions for the policy distribution function are met, by referring to "[11.1.2.2 Operating conditions for the policy distribution function](#)".

Format

<i><Installation directory>\bin\sqcSendPolicy.exe</i>	<i>-g <policy distribution group name>,</i>
	<i>-g <policy distribution group name> [-s <server name>.]</i>

Options

-g <policy distribution group name>

Specify one or more policy distribution group names.

Specifying groups distributes the policy definition information files that have been created in the policy distribution group folders to the servers defined in the policy distribution definition file (Distribute.ini).

-s <Server name>

Specify the name of the server to which the policy definition information should be distributed.

If the "-s" option is specified, the policy distribution definition file (Distribute.ini) for the policy distribution group with the "-g" option will be ignored. Instead, all of the policy definition information files stored in the group folder will be distributed to the specified server or servers.

Note that if the "-s" option is specified, only one policy distribution group can be specified with the "-g" option.

To check which servers policy definition information will be distributed to, execute the sqcViewPolicy command by referring to "[11.3.1 How to check which servers policies can be distributed to](#)".

Usage example 1

Distributing policies using the following definitions:

[Policy distribution group]

USER_DEFINE_FOLDER1

[Distribution servers defined in the policy distribution definition file (Distribute.ini)]

wasabi1,wasabi2

[Policy distribution definition file]

Threshold monitoring definition

```
C:\Program Files\SystemwalkerSQL-C\bin\sqcSendPolicy.exe -g USER_DEFINE_FOLDER1
```

Explanation 1

By specifying USER_DEFINE_FOLDER1 with the "-g" option, the policy definition information file (threshold monitoring definitions) will be distributed to the distribution destination servers (wasabi1 and wasabi2) that have been defined in the policy distribution definition file (Distribute.ini).

Usage example 2

Distributing policies using the following definitions:

[Policy distribution group]

USER_DEFINE_FOLDER

[Distribution servers defined in the policy distribution definition file (Distribute.ini)]

wasabi1,wasabi2

[Policy distribution definition file]

Threshold monitoring definition

```
C:\Program Files\SystemwalkerSQL-C\bin\sqcSendPolicy -g USER_DEFINE_FOLDER -s  
wasabi3,wasabi4
```

Explanation 2

By specifying wasabi3 and wasabi4 with the "-s" option, the policy definition information file (threshold monitoring definitions) will be distributed to wasabi3 and wasabi4, ignoring the definitions (wasabi1 and wasabi2) in the policy distribution definition file (Distribute.ini).

11.2.6 Creating and applying policies remotely

Policies can be created and applied to distribution destination servers remotely from the operation management client. Use the sqcCtrlPolicy command (Policy Remote Operation Command) to create and apply policies.

Refer to section 1.1.7, "sqcCtrlPolicy (Policy Remote Operation Command)" in the *Reference Guide* for more information about the sqcCtrlPolicy command (Policy Remote Operation Command).

Format

<i><Operation Management Client installation directory>\bin\sqcCtrlPolicy.exe</i>	<i>-e <Command type> {-g <Policy distribution group>, -s <Server name>, }</i>
---	---

Options

-e *<Command type>*

Specify the command type for the remote operation.

- AP: Collection policy creation command (sqcAPolicy: collection policies for response/operating information)
- RP: Collection policy creation command (sqcRPolicy: collection policies for server resource information)
- SP: Collection policy application command (sqcSetPolicy)

-g *<Policy distribution group>*

Specify one or more policy distribution group names.

-s *<Server name>*

Specify the server where the remote operation will be performed.

To check which servers policy definition information will be distributed to, execute the sqcViewPolicy command by referring to "[11.3.1 How to check which servers policies can be distributed to](#)".

Point

From Systemwalker Service Quality Coordinator V13.3.0 or later, the services/daemons do not have to be stopped before the policy application command is executed.

However, if the services/daemons are running and performance data for various middleware is being collected when the policy application command is executed, then the collection of this performance data will be temporarily suspended while policies are applied. Collection of this performance data will start again after the policies have been finished being applied.

Usage example

Performing remote policy operations using the following definitions

[Operation server]

wasabi

[Operation command]

Collection policy creation (sqcRPolicy)

C:\Program Files\SystemwalkerSQC-C\bin\sqcCtrlPolicy.exe -e RP -s wasabi
--

11.3 Supplementary Notes

This section presents the following supplementary notes.

- [11.3.1 How to check which servers policies can be distributed to](#)
- [11.3.2 Changing the port number used by distribution destination server](#)

11.3.1 How to check which servers policies can be distributed to

If Systemwalker Service Quality Coordinator has already been installed, a list of servers to which policies can be distributed can be displayed by executing the sqViewPolicy command (Policy Definition Information Verification Command) on the operation management client.

Refer to Section 1.1.5, "sqViewPolicy (Policy Definition Information Verification Command)" in the *Reference Guide* for more information about sqViewPolicy (Policy Definition Information Verification Command).

Before performing this procedure

Check that the operating conditions for the policy distribution function are met, by referring to "[11.1.2.2 Operating conditions for the policy distribution function](#)".

Format

<code><Operation management client installation directory>\bin\sqViewPolicy.exe [-l [as ab mg pm em]]</code>
--

<code><Operation management client installation directory>\bin\sqViewPolicy.exe -c</code>

Options

-l *Parameter*

Lists the host names of the installation type specified by *parameter* that are targeted for policy distribution.

Note: If *parameter* is omitted, policies will be distributed to all the systems.

-c

Checks if the distribution destination servers are ready to receive policies.

Parameters

The following parameters specify the abbreviation of each installation type.

The following shows the correspondence between the abbreviations and installation types.

As : Agent for Server

Ab : Agent for Business

Mg : Manager

Pm : Proxy Manager

Em : Enterprise Manager

11.3.2 Changing the port number used by distribution destination server

To change the port number used by the policy distribution destination server, perform the following procedure on the policy distribution destination server.

If the policy distribution function is used as part of the HTTP communications environment on the Agent side, the port number is set to 23440 by default. To change this port number, edit the following definition file. (Change the port=23440 part).

Procedure

1. Change the thttpd.conf file on the policy distribution destination server.

Storage directory

[Windows]

```
<variable file storage directory>\control\thttpd.conf
```

[UNIX]

```
/etc/opt/FJSVssqc/thttpd.conf
```

Definition method

```
cgipat=/cgi-bin/*  
chroot  
dir=C:\Program Files\SystemwalkerSQC\www  
port=23440 *Change here.
```

2. Apply collection policies, by referring to "[A.1 Server Resource Information Collection Policy Creation Command](#)".
3. Restart the thttpd service or daemon of the Manager and Agent by referring to "[A.4 How to Start and Stop Resident Processes](#)".

Chapter 12 Backup and Restore

Systemwalker Service Quality Coordinator provides steps for backing up and restoring user registration information and operation management information, in case the operating environment is accidentally deleted or damaged or needs to be migrated in future.

Privileges required for execution

[Windows]

The privileges of a user belonging to the "Administrators" group are required to make these settings.

[UNIX]

System administrator (superuser) privileges are required to make these settings.

Before performing this procedure

Fujitsu recommends that backup be performed in the following situations:

- When changing definitions or settings
- When saving operation data

The following sections explain the backup and restoration procedures.

- [12.1 Operation Definitions](#)
- [12.2 Backing Up and Restoring the Performance Database \(PDB\)](#)

12.1 Operation Definitions

Enterprise Manager/Manager/Proxy Manager/Agent

The storage location of the operation definitions are shown below. Backup at the directory level. When restoring, put the backed up files in the same location.

[Windows]

Variable file directory\control

[UNIX]

/etc/opt/FJSVssqc

Point

.....
If redundant Manager operation is being conducted, perform a backup/restoration at each Manager. (Redundant operation of Managers is only available with the Enterprise Edition.) If cluster system operation is being performed, perform the backup/restoration at the current system (the node that is conducting management tasks). (Cluster system operation is only available with the Enterprise Edition.)
.....

Operation management client

The operation definitions for operation management clients are stored in the following location. Backup at the directory level. When restoring, put the backed up files in the same location.

[Windows]

```
Installation directory\www\
```

12.2 Backing Up and Restoring the Performance Database (PDB)

Enterprise Managers and Managers include a performance database (PDB) file. There are two ways of backing up and restoring the PDB, as shown below. Combine these methods as appropriate to the operation.

- PDB file
- Archive files



If redundant Manager operation is being conducted, perform a backup/restoration at each Manager. (Redundant operation of Managers is only available with the Enterprise Edition.) If cluster system operation is being performed, perform the backup/restoration at the current system (the node that is conducting management tasks). (Cluster system operation is only available with the Enterprise Edition.)

The following sections explain how to back up and restore the performance database (PDB).

- [12.2.1 PDB file](#)
- [12.2.2 Archive files](#)

12.2.1 PDB file

This method is for backing up and restoring the performance database files only.

Before performing this procedure

Stop the service or daemon for the Enterprise Manager or Manager to be backed up or restored (if it is running) by referring to "[A.4 How to Start and Stop Resident Processes](#)". Check that the resident process has stopped correctly.

Storage Location

By default, the PDB files are stored in the directory below (refer to Section 6.6.1.1, "Changing the PDB Storage Location" in the *Installation Guide* for information on how to change it):

[Windows]

```
Variable file directory\data\
```

[UNIX]

```
/var/opt/FJSVssqc/PDB/
```


The following files are generated in this directory:

File name	Description
pdb.dat	This is a single file for storing management data.
pdb_SUMMARY_yyyymmdd.dat	These files store summary data. A new file is created each day, and the "yyymmdd" part of the file name indicates the date when the file was created.
pdb_10MIN_yyyymmdd.dat	These files store resource data (which is collected at 10 minute intervals). A new file is created each day, and the "yyymmdd" part of the file name indicates the date when the file was created.
pdb_1HR_yyyymmdd.dat	These files store resource data (which is collected at hourly intervals). A new file is created each week, and the "yyymmdd" part of the file name indicates the date of the Sunday in the week when the file was created.
pdb_1DAY_yyyymmdd.dat	These files store resource data (which is collected at daily intervals). A new file is created each month, and the "yyymmdd" part of the file name indicates the date of the first day of the month when the file was created.
pdb_other.dat	This is a single file for storing control data.

Backup/Restore

- For PDB files, move all of the "*.dat" files in the directory above together.
- Do not change the file names of the "*.dat" files that have been backed up.
- To restore these files, place the files that have been backed up in the same location as the original files.

12.2.2 Archive files

This method backs up the archive files that are output for the purpose of conducting daily backups.

Storage Location

By default, the archive files are stored in the directory below (refer to Section 6.6.1.2, "Changing the Archive File Location" in the *Installation Guide* for information on how to change it):

[Windows]

Variable file directory\spool\BackupPDBinsert

[UNIX]

/var/opt/FJSVssqc/BackupPDBinsert

The following file is output to the above directory.

pdbinsert_%SYSTEM%_%N%.txt

%SYSTEM%: System name

%N%: File number

A new archive file is created every 24 hours, or whenever the DCM service/daemon is executed. Note that file numbers (represented by %N%) increment cyclically between 1 and 3. This makes it possible to archive information for up to three days.

Backup

Backup the files above.

Restore

To restore an archive file, change the file extension from "txt" to "tmp" and then copy the file to the following directory:

[Windows]

```
Variable file directory\transfer\DsaPDBWriter
```

[UNIX]

```
/var/opt/FJSVssqc/temp/DsaPDBWriter
```

Note

When archive files are restored, they are written to the PDB as a single transaction. At this time, the performance database is locked and no performance information other than the archive files can be written to or read from the performance database. For this reason, when restoring archive files, they should be divided up and stored as multiple individual files.

Appendix A Setup Commands and Resident Processes

This appendix explains the various setup commands and how to start and stop resident processes.

Refer to Section 1.1, "Policy Commands" and Chapter 2, "Starting and Stopping Resident Processes" in the *Reference Guide* for details.

- [A.1 Server Resource Information Collection Policy Creation Command](#)
- [A.2 Response/Operation Information Collection Policy Creation Command](#)
- [A.3 sqcMdPolicy \(Temporary Policy Change Command\)](#)
- [A.4 How to Start and Stop Resident Processes](#)
- [A.5 Starting the thttpd Service/Daemon Automatically](#)
- [A.6 genpwd \(password encryption command\)](#)

A.1 Server Resource Information Collection Policy Creation Command

This section explains the Server Resource Information Collection Policy Creation Command.

Refer to Section 1.1.1, "sqcRPolicy (Server Resource Information Collection Policy Creation Command)" and Section 1.1.3, "sqcSetPolicy (Policy Application Command)" in the *Reference Guide* for more information.

Required privileges

[Windows]

The user must have the privileges of a member of the Administrators group.

[UNIX]

The user must have the privileges of the system administrator (superuser).

[Windows]

For Windows systems, to collect disk-related performance information, the *diskperf* Windows command must be executed beforehand to enable information to be collected. This command is used as follows:

```
diskperf -y
```

Refer to the Windows help for details on the *diskperf* command. Before using this command, be sure to enable both physical drives and logical drives.

Point

- The system must be restarted after settings are made using the *diskperf* command.
- The *diskperf* command must be executed before the Systemwalker Service Quality Coordinator DCM service starts (before performance information starts being collected).

Format

1. Create a server resource information collection policy

[Windows]

```
Installation directory\bin\sqrPolicy.exe
```

[UNIX]

```
/opt/FJSVssqc/bin/sqrPolicy.sh
```

2. Apply the policy

[Windows]

```
Installation directory\bin\sqrSetPolicy.exe [-h host name] [-p <IP address>]
```

[UNIX]

```
/opt/FJSVssqc/bin/sqrSetPolicy.sh [-h <host name>] [-p <IP address>]
```



From Systemwalker Service Quality Coordinator V13.3.0 or later, the services/daemons do not have to be stopped before the policy application command is executed.

However, when using the "-h" or "-p" option, stop the service or daemon first by referring to "[A.4 How to Start and Stop Resident Processes](#)".

If the services/daemons are running and performance data for various middleware is being collected when the policy application command is executed, then the collection of this performance data will be temporarily suspended while policies are applied. Collection of this performance data will start again after the policies have been finished being applied.

Options of sqrSetPolicy (Policy Application Command)

-h <host name>

Use this option to specify a system name to change the managed system name.

Also, use this option to specify a system name for the managed system in the following kinds of cluster operations:

- Where the server is a Manager and information about resources within the server is to be collected.
=> Specify the inheritance node.
- Where the server is an Agent in a cluster system that uses node name inheritance.
=> Specify node name of each Agent.

If this option is omitted, host name which is set at the installation or the system name which was set at the last -h option will be used as system name.

Host name will not be updated automatically, so use this option to change the host name.



If this command is re-executed or an Agent is reinstalled where an operating environment for this product already exists and an Agent has already been registered, then use the same system name as was used before if the -h option is specified.

If the system name has to be changed for some reason, first delete the previous system name information from the PDB using the data deletion command explained in Section 1.7.3 "sqcPDBerase (Data Deletion Command)" in the *Reference Guide* for details. However, in this case, performance information that has already been collected cannot be displayed.

-p <IP address>

In the dashboard, management target is managed by using IP address.

When using the dashboard, be sure to specify IP address of the management target by using this option after installation. Specify the IP address of the connection Manager or Enterprise Manager which is available for connection.

Specify the inheritance node if the cluster system is being used.

If this option is omitted, IP address which was set at the last -p option will be used.

IP address will not be updated automatically, so use this option to change the IP address.



Note

If this command is executed at the first time after the installation, and if this option is omitted, IP address will be set by the address which is automatically collected. However, if multiple IP addresses are existed, IP address which can communicate with the connection Manager or Enterprise Manager might not be acquired. Be sure to specify IP address of the management target by using -p option.



Point

When the Server Resource Information Collection Policy Creation Command (sqcRPolicy) or sqcCtrlPolicy.exe -e RP (Remote Policy Operation Command) is executed, a file named "MiddlewareConf.xml" is created. To delete a managed object, edit the content of MiddlewareConf.xml by referring to Chapter 3, "Resource Configuration Information (MiddlewareConf.xml)" in the *Reference Guide*.

A.2 Response/Operation Information Collection Policy Creation Command

This section explains the Response/Operation Information Collection Policy Creation Command.

Refer to Section 1.1.2, "sqcAPolicy (Response/Operation Information Collection Policy Setup Command)" and Section 1.1.3, "sqcSetPolicy (Policy Application Command)" in the *Reference Guide* for more information.

Required privileges

[Windows]

The user must have the privileges of a member of the Administrators group.

[UNIX]

The user must have the privileges of the system administrator (superuser).

1. Create response/operation information collection policy

[Windows]

```
Installation directory\bin\sqcAPolicy.bat
```

[UNIX]

```
/opt/FJSVssqc/bin/sqcAPolicy.sh
```

2. Apply the policy

[Windows]

```
Installation drectory\bin\sqcSetPolicy.exe [-h host name] [-p <IP address>]
```

[UNIX]

```
/opt/FJSVssqc/bin/sqcSetPolicy.sh [-h <host name>] [-p <IP address>]
```

Point

From Systemwalker Service Quality Coordinator V13.3.0 or later, the services/daemons do not have to be stopped before the policy application command is executed.

When using the "-h" or "-p" option, stop the service or daemon first by referring to "[A.4 How to Start and Stop Resident Processes](#)".

However, if the services/daemons are running and performance data for various middleware is being collected when the policy application command is executed, then the collection of this performance data will be temporarily suspended while policies are applied. Collection of this performance data will start again after the policies have been finished being applied.

Options of sqcSetPolicy (Policy Application Command)

-h <host name>

Use this option to specify a system name to change the managed system name.

Also, use this option to specify a system name for the managed system in the following kinds of cluster operations:

- Where the server is a Manager and information about resources within the server is to be collected.
=> Specify the inheritance node.
- Where the server is an Agent in a cluster system that uses node name inheritance.
=> Specify node name of each Agent.

If this option is omitted, host name which is set at the installation or the system name which was set at the last -h option will be used as system name.

Host name will not be updated automatically, so use this option to change the host name.

Note

If this command is re-executed or an Agent is reinstalled where an operating environment for this product already exists and an Agent has already been registered, then use the same system name as was used before if the -h option is specified.

If the system name has to be changed for some reason, first delete the previous system name information from the PDB using the data deletion command explained in Section 1.7.3 "sqcPDBerase (Data Deletion Command)" in the *Reference Guide* for details. However, in this case, performance information that has already been collected cannot be displayed.

-p <IP address>

In the dashboard, management target is managed by using IP address.

When using the dashboard, be sure to specify IP address of the management target by using this option after installation. Specify the IP address of the connection Manager or Enterprise Manager which is available for connection.

Specify the inheritance node if the cluster system is being used.

If this option is omitted, IP address which was set at the last -p option will be used.

IP address will not be updated automatically, so use this option to change the IP address.

Note

If this command is executed at the first time after the installation, and if this option is omitted, IP address will be set by the address which is automatically collected. However, if multiple IP addresses are existed, IP address which can communicate with the connection Manager or Enterprise Manager might not be acquired. Be sure to specify IP address of the management target by using -p option.

A.3 sqcMdPolicy (Temporary Policy Change Command)

Policies can be changed after they have been applied and started operating (while collection is running). Specifically, once information collection policies for the following middleware products have been created and applied, collection can be stopped (by specifying "off") and started (by specifying "on").

- Symfoware Server
- Oracle Database Server

Refer to Section 1.1.4, "sqcMdPolicy (Temporary Policy Change Command)" in the *Reference Guide* for more information.

Privileges required for execution

[Windows]

The privileges of a user belonging to the "Administrators" group are required to make these settings.

[UNIX]

System administrator (superuser) privileges are required to make these settings.

Point

Use temporary policy changes to control information collection behavior according to the operation mode of jobs or cluster systems.

Syntax

[Windows]

```
Installation directory\bin\sqcMdPolicy.exe on|off|stat -c Type [ -i instance-name ]
```

[UNIX]

```
/opt/FJSVssqc/bin/sqcMdPolicy.sh on|off|stat -c Type [ -i instance-name ]
```

Options

on|off|stat

Specify either of the following types of changes:

- on: Enables the target policy
- off: Disables the target policy
- stat: Display the status of the policy (enabled or disabled)

-c Type

Specify one of the following managed objects:

- sym : Symfoware Server
- ora : Oracle Database Server
- reg : Registry (Windows only)
- sar : Server performance (UNIX only)
- jla : OperationManger

-i instance-name (only a database server can be specified)

Specify the instance name for the managed object that is specified with the "-c" option. If this option is omitted, all instances of the managed object will be targeted.

- If the managed object is "sym", specify the RDB system name.
- If the managed object is "ora", specify the instance name.



Point

If the RDB system does not have a name, specify "-i @default".

- ora: Oracle instance name (SID)

A.4 How to Start and Stop Resident Processes

This section explains how to start and stop resident processes.

Refer to Chapter 2, "Starting and Stopping Resident Processes" in the *Reference Guide* for more information about processes, etc.

Manager

[Windows]

Start/stop the following service:

- Systemwalker SQC DCM



Point

This process is started when using "Pull" method communications provided by this product.

- Systemwalker SQC sqcschdle

Start/stop the following service when using Pull-mode communications and the policy distribution function:

- Systemwalker SQC thttpd

Refer to "A.5 Starting the thttpd Service/Daemon Automatically" for information about how to start the thttpd service automatically.

Note

When restarting the [Systemwalker SQC DCM] service, do not execute "Restart the service" from the Windows **Services** window.

First execute "Stop the service", then after waiting a while execute "Start the service".

[UNIX]

Use the following scripts to start and stop the processes.

To start the processes:

```
/etc/rc2.d/S99ssqcdcm start
```

To stop the processes:

```
/etc/rc0.d/K00ssqcdcm stop
```

To stop the processes completely:

```
/etc/rc0.d/K00ssqcdcm stop_wait
```

Point

If the stop option (stop) is selected, this command completes without waiting for ending of the process.

If the complete stop (stop_wait) is selected, this command sends a finish signal, and completes after ending of running process.

When restarting the process, stop the process by using the complete stop option (stop_wait), and after command completion, start option (start) to start the process.

Point

This process is started when using "Pull" method communications provided by this product.

To start the processes:

```
/etc/rc2.d/S99ssqsch start
```

To stop the processes:

```
/etc/rc0.d/K00ssqsch stop
```

If the policy distribution function is being used, start and stop the resident process by using the following script:

Starting:

```
/opt/FJSVssqc/bin/ssqchttp start
```

Stopping:

```
/opt/FJSVssqc/bin/ssqchttp stop
```

Refer to "[A.5 Starting the tthttpd Service/Daemon Automatically](#)" for information about how to start the tthttpd daemon automatically.

Agent/Proxy Manager

[Windows]

Start/stop the following service:

- Systemwalker SQC DCM

Point

If the Pull mode is to be used for communication and the policy distribution function is to be used, use the following script to start and stop the processes:

- Systemwalker SQC tthttpd

Refer to "[A.5 Starting the tthttpd Service/Daemon Automatically](#)" for details on how to start the tthttpd service automatically.

Note

When restarting the [Systemwalker SQC DCM] service, do not execute "Restart the service" from the Windows **Services** window.

First execute "Stop the service", then after waiting a while execute "Start the service".

[UNIX]

Use the following scripts to start and stop the processes.

To start the processes:

```
/etc/rc2.d/S99ssqcdcm start
```

To stop the processes:

```
/etc/rc0.d/K00ssqcdcm stop
```

To stop the processes completely:

```
/etc/rc0.d/K00ssqcdcm stop_wait
```

Point

If the stop option (stop) is selected, this command completes without waiting for ending of the process.

If the complete stop (stop_wait) is selected, this command sends a finish signal, and completes after ending of running process.

When restarting the process, stop the process by using the complete stop option (stop_wait), and after command completion, start option (start) to start the process.

Point

If the Pull mode is to be used for communication and the policy distribution function is to be used, use the following scripts to start and stop the processes.

To start the processes:

```
/opt/FJSVssqc/bin/ssqchttp start
```

To stop the processes:

```
/opt/FJSVssqc/bin/ssqchttp stop
```

Refer to "[A.5 Starting the thttpd Service/Daemon Automatically](#)" for details on how to start the thttpd daemon automatically.

Enterprise Manager

[Windows]

Start/stop the following service:

- Systemwalker SQC DCM

Point

If the policy distribution function is to be used, use the following script to start and stop the processes:

- Systemwalker SQC thttpd

Refer to "[A.5 Starting the thttpd Service/Daemon Automatically](#)" for details on how to start the thttpd service automatically.

Note

When restarting the [Systemwalker SQC DCM] service, do not execute "Restart the service" from the Windows Services window.

First execute "Stop the service", then after waiting a while execute "Start the service".

[UNIX]

Use the following scripts to start and stop the processes.

To start the processes:

```
/etc/rc2.d/S99ssqcdcm start
```

To stop the processes:

```
/etc/rc0.d/K00ssqcdcm stop
```

To stop the processes completely:

```
/etc/rc0.d/K00ssqcdcm stop_wait
```

Point

If the stop option (stop) is selected, this command completes without waiting for ending of the process.

If the complete stop (stop_wait) is selected, this command sends a finish signal, and completes after ending of running process.

When restarting the process, stop the process by using the complete stop option (stop_wait), and after command completion, start option (start) to start the process.

Point

If the policy distribution function is to be used, use the following script to start and stop the processes:

To start the processes:

```
/opt/FJSVssqc/bin/ssqchttp start
```

To stop the processes:

```
/opt/FJSVssqc/bin/ssqchttp stop
```

Refer to "[A.5 Starting the thttpd Service/Daemon Automatically](#)" for details on how to start the thttpd daemon automatically.

A.5 Starting the thttpd Service/Daemon Automatically

This section explains the procedure for starting the thttpd service/daemon when both the policy distribution function and communications using the "Pull" method are to be used.

Required privileges

[Windows]

The user must have the privileges of a member of the Administrators group

[UNIX]

The user must have system administrator (superuser) privileges.

Procedure

[Windows]

1. Select [Administrative Tools] and then [Services] from the Control Panel.
2. Select [Systemwalker SQC thttpd], and then open the [Properties] window.
3. In the [General] tab, change the [Startup type] to [Automatic].

[UNIX]

Set up a startup script by executing the following commands:

```
# cd /etc/rc2.d
# ln -s /opt/FJSVssqc/bin/ssqchttp S99ssqchttp
```

Set up a stop script by executing the following commands:

```
# cd /etc/rc0.d
# ln -s /opt/FJSVssqc/bin/ssqchttp K00ssqchttp
```

A.6 genpwd (password encryption command)

It is necessary to execute this command to generate an encrypted password to add to the password parameter definition for connection in the following two cases; Connection Account configuration file (remoteAccount.txt) for agent for Agentless Monitoring and Configuration information file (ecoAgentInfo.txt) of the SNMP agent (if the SNMP agent is version 3) for ECO information.

The following explains the command that generates encrypted passwords.

Required privileges

[Windows]

The Administrators group user privileges are required.

[UNIX]

System administrator (superuser) privileges are required.

Syntax

[Windows]

```
<Installation directory>\bin\genpwd.exe
```

[UNIX]

```
/opt/FJSVssqc/bin/genpwd.sh
```

Function

Generates encrypted passwords.

Options

None.

Termination status

Normal termination: 1

Abnormal termination: Other than 1

Usage example

Execute as follows to generate encrypted passwords.

After executing the command, a dialog appears asking for the password and confirmation of the password. Enter the password to be encrypted.

Copy the generated text and paste it into the password parameter in the definition file.

[Windows]

```
C:\ cd C:\Program Files\SystemwalkerSQL\bin
C:\Program Files\SystemwalkerSQL\bin>genpwd.exe
Password:
Confirm password:
bpnM2i65/s+k5YhGb15JKw==
C:\Program Files\SystemwalkerSQL\bin>
```

[UNIX]

```
# cd /opt/FJSVssqc/bin
# ./genpwd.sh
Password:
Confirm password:
bpnM2i65/s+k5YhGb15JKw==
#
```