MasterScope SystemManager G Ver.8.0.0
Release Memo

July 2018
NEC Corporation

Thank you for purchasing our product. Taking this opportunity, we would like to provide the supplementary explanation of "MasterScope SystemManager G" so that you may make the best use of the product.

Revision History

Revision No.	Chapter/ Section	Description
1st issue	-	Ver7.1.0
2st edition	-	Ver.8.0.0

Table of Contents

Trademark

1) Adobe, the Adobe logo, and Reader are trademarks or registered trademarks of Adobe Systems Incorporated in the United States and other countries.
2) Microsoft, Windows, Windows Server and Internet Explorer are registered trademarks of Microsoft Corporation in the United States and other countries.
   In addition, Microsoft products included in this guide are registered trademarks of Microsoft Corporation in the United States and other countries.
3) Intel, Xeon and Itanium are trademarks or registered trademarks of Intel Corporation and its affiliated companies in the United States and other countries.
4) UNIX is a registered trademark of The Open Group in the United States and other countries.
5) HP-UX is a registered trademarks of Hewlett-Packard Company in the United States and other countries.
   In addition, Hewlett-Packard Company products included in this guide are registered trademarks of Hewlett-Packard Company in the United States and other countries.
6) Oracle, Exadata, Solaris, Java, and WebLogic are registered trademarks of Oracle Corporation and/or its affiliates.
7) Oracle Enterprise Manager is a trademark of Oracle Corporation.
8) Linux is a registered trademark of Mr. Linus Torvalds in the United States and other countries.
9) Red Hat is a registered trademark or trademark of Red Hat Software, Inc.
10) SUSE is a registered trademark of Novell, Inc. in Japan.
11) IBM, AIX, WebSphere are registered trademarks of the International Business Machines Corporation in the United States and other countries.
12) PostgreSQL is the name of open source object relational database management system proposed by the PostgreSQL Global Development Group.
13) Apache and Tomcat are trademarks of Apache Software Foundation.
14) SAP is a trademark or registered trademark of SAP AG in Germany and other countries in the world.
15) Super Visual Formade, Report Director, and Universal Connect / X are registered trademarks of WingArc1st Inc.
16) PATLITE is a registered trademark of PATLITE Corporation.
17) In addition, proper nouns such as company names and product names included in this guide are trademarks or registered trademarks of their respective companies.
18) "TM" and ® mark are omitted in text and figures in this guide.

Acknowledgement

1) Software developed by OpenSSL Project to use with OpenSSL Toolkit is built into this product. (http://www.openssl.org/)
2) This product includes encryption software developed by Eric Young (eay@cryptsoft.com).
3) This product includes software developed by Tim Hudson (tjh@cryptsoft.com).

Note

1) This manual assumes that the agent functions, manager functions, and monitoring terminal functions to be operated on Windows have all been installed in "C:\Program Files\NEC\UMF\Operations". Similarly, the agent functions and manager functions to be operated on UNIX have been installed in "/opt/UMF/Operations". If you installed them into a directory other than the default directory, you need to read the name of the former for that of the latter throughout this guide.

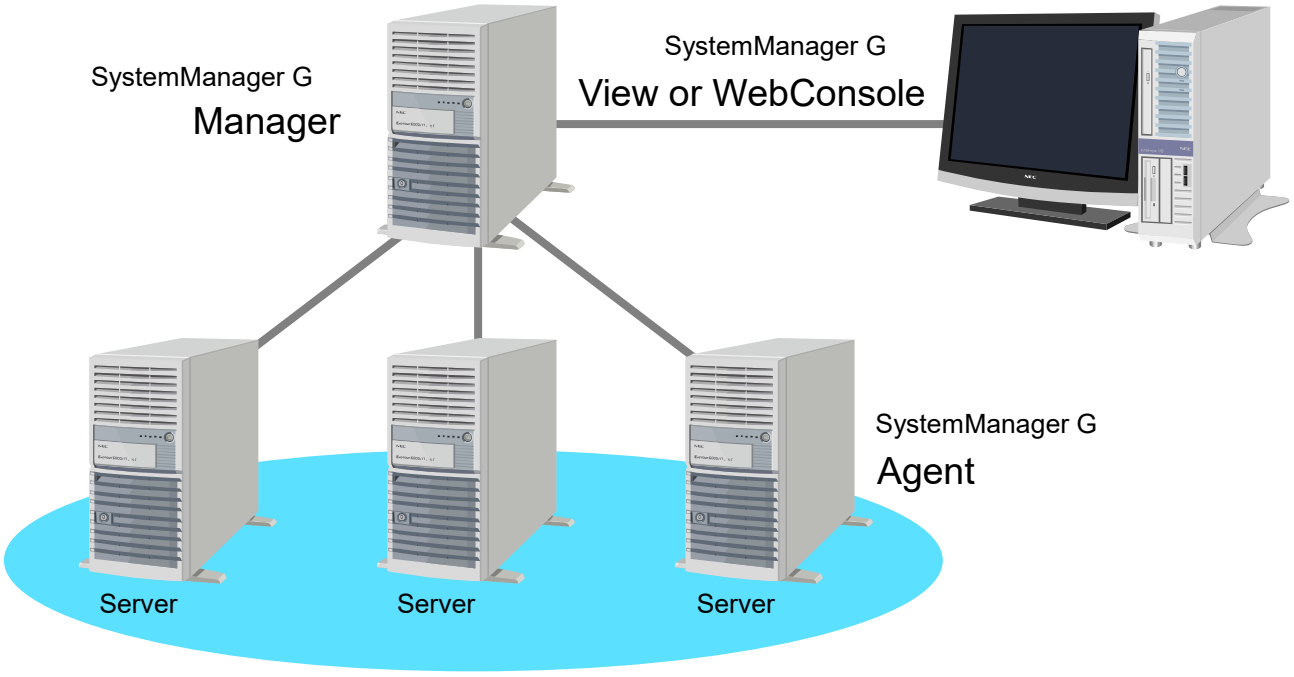
2) Specifications and designs of windows included in this guide are subject to change for improvement without notice.

1. Product Description

1.1. Product Details

MasterScope SystemManager G significantly reduces support costs and realizes stable business operation by monitoring failures from the business viewpoint and centrally managing a variety of application systems used in the business system.

The following shows an overview of a MasterScope SystemManager G configuration:



Terms	Description
Agent	Function to notify the manager of server monitoring information. Install the agent in the monitored server.
Manager	A function that integrates and manages the information collected by agents.
View	A console that displays on a view the information collected by the manager, and operates and issues a command to a server.
WebConsole	A Web based GUI that displays on a view the monitoring state.

The package that this release memo explains provides the following functions:

- **Service process monitoring**
  Enables users to monitor whether the process of an application or a service is dead or alive.

- **Message monitoring**
  Displays message information generated on each system on a window.

- **Log monitoring function**
  Monitors syslog or logs and event logs that application programs output, captures necessary information from them, and reports it as a message.

- **Performance monitoring**
  Displays the operating status of the system in graphic format.
  It monitors whether a threshold value is exceeded, and informs an operator when it occurs.
  It accumulates performance data as statistical information and facilitates the problem analysis and improvement of the system.

- **Configuration information monitoring function**
  Collects and displays the information on configured equipment, such as CPU and SCSI devices, making up a server.

- **Performance information displaying**
  Defines graphs with the performance data collected with the performance monitoring function regardless of hosts and instances, and display them in an integrated manner.

- **Report control**
  Reports a detected event via PATLITE, mail, and action.

- **Recovery function**
  Attempts to recover from a failure by starting a command that is automatically driven by the occurrence of a particular message.

- **Application start function**
  Enables a user to bundle business applications in a group and register the group so that he may instantly start his desired business application from a monitoring window.

- **Print function**
  The performance data collected by the performance monitoring function can be output as a report in the PDF format.

- **File monitoring function**
  Monitors files/directories on each server and reports such in a report when the upper limits for files/directories are exceeded or when an updated file is detected.

- **Agentless monitoring function**
  Monitors a host (remote host) to which any agent has not been installed.To use this function, a

remote monitoring agent is required.

◆ **IT Service Response Monitor function**

Emulates access to IT services provided by applications to measure their availability and response.
To use this function, the IT Service Response Monitor agent is required.

◆ **Service port monitoring function**

Provides functions to manage and display the service ports of the agent in the system.

◆ **External product linking function**

Enables users to obtain message information by working with an external product (such asESMPRO/ServerManager, MasterScope Network Node Manager).
Please refer to below for details.
SystemManager Event Trap Utility Release Memo (SysMEvTrap_readme.pdf)

◆ **User management**

Manages user information that is used in the system. A user is allowed to perform operations that are permitted with the authority that is assigned to a group to which the user belongs.

◆ **Trail management**

Enables users to manage a history of operations and results for operations and automatic processes executed in the monitoring window or on the manager.

◆ **Cluster supporting**

Supports operations of a manager and its agents on an active hot standby cluster system.
The following lists supported cluster systems:

- HP Serviceguard (HP-UX)
- EXPRESSCLUSTER X (Windows/Linux)
- Microsoft Failover Cluster (Windows Server 2008)
- Windows Server Failover Clustering (Windows Server 2012)

◆ **WebAPI**

The monitoring settings can be referenced or changed by using the WebAPI.
By using the WebAPI on the existing system or from a user-specific application, it becomes easy to link the monitoring settings with Application Navigator.
Please refer to below for details.
MasterScope SystemManager G WebAPI Reference (WebAPIReference.pdf)

Optional function

◆ **Message monitoring function (Business View)**

Enables a user to instantly identify the scope of the effect on his business when a failure occurs by grouping messages that were generated in systems, by business, and displaying them in tree format.
Since the function selects only the messages that are sufficient for monitoring systems from a vast number of messages before displaying them, a message that is being dealt with will not be scrolled away and will always stay visible.

◆ **Application integrated monitoring**

- Enables users to display the operating status of an application in graphic format and monitor the operating status over time and on a real-time basis.
- Enables users to detect the status of an error and warning by setting an appropriate threshold and report the results to an operator.
- Displays a summary of the operating statuses of applications and provides a summary view that enables users to understand the operating status of the entire system at a glance. It enables users to identify a section(s) that causes a problem by drilling down on possible faulty parts if the problem occurs.
- Provides monitoring templates with a set of typical monitored items. It enables users to introduce operation monitoring without complicated setting tasks.

◆ **Application operation monitoring**

Monitors the operating status of the following respective applications:

- Oracle Database
- Microsoft Internet Information Services
- Microsoft SQL Server
- Oracle WebLogic Server
- Apache HTTP Server
- Apache Tomcat
- SAP ERP
- Java application (hereinafter, sometimes written as "JavaAP")
- WebSphere Application Server

◆ **Service availability monitoring**

This function measures the availability and responses of an IT service provided by an application by simulating accessing the service. It can monitor IT services from the standpoint of end users, and quickly detect failures in the services. The monitorable IT services include the following:

- Web scenarios*
- Mail (POP3, SMTP)
- DNS
- TCP (any TCP port)
- FTP

* Web scenario monitoring monitors Web services by recording and replaying a serial flow of accessing them.

◆ **Knowledge control**

Provides product knowledge bundles for monitored applications (without charge). By importing product knowledge, a user can navigate through corrective actions for a failure that occurs in a middleware product. By registering a way of dealing with a newly generated problem, users can subsequently navigate through the registered measures and deal with the same types of the problems by referring to the appropriate measure. Product knowledge is provided for the following:

- Oracle Database
- Microsoft Internet Information Services
- Microsoft SQL Server
- Oracle WebLogic Server

- Apache HTTP Server

◆ **Scenario control function**
Events such as message and schedule can monitor whether operations for a day have been carried out according to the schedule. Since events are available to issue commands and messages, definition of the processing flow for each operation can implement the automation of the operation.

◆ **Operation control function**
This function prevents users from making operational mistakes by converting a set of operations for submitting a command to an agent or the manager to a routine procedure.

◆ **Manager linkage function**
Managers of multiple units can be linked with each other hierarchically to monitor the entire system in a centralized method by allowing a high-order manager to be notified of messages collected by low-order managers.

◆ **Application linkage function**
Collected messages can be output to the outer files to allow outer applications work together by reading those files into them.

◆ **ServiceManager linkage function**
When a specific message is generated, the product enables users to register the message into MasterScope ServiceManager as an incident.

◆ **Invariant Analyzer function**
Invariant Analyzer creates a model of the target system by finding invariant correlations between performance data collected while the system is running on a normally operating state. Invariant Analyzer then compares the recent performance data to the normal state model to detect any broken invariants, which is correlation different from normal operating state.
Please refer to below for details.
MasterScope SystemManager G Release Memo -Invariant Analyzer Edition- (IA_relememo.pdf)

◆ **Event collection function**
Analyzes the correlation between received messages and then displays a new message according to the results of the analysis.

◆ **CDO message API**
By implementing a program with the API, the program can send a message to MasterScope MISSION CRITICAL OPERATIONS.
API is compatible with OpenDIOSA/OPBASE.
Please refer to below for details.
MasterScope SystemManager G Release Memo - CDO Message API Edition –
(CDO_relememo.pdf)

◆ **Hypervisor monitoring function**

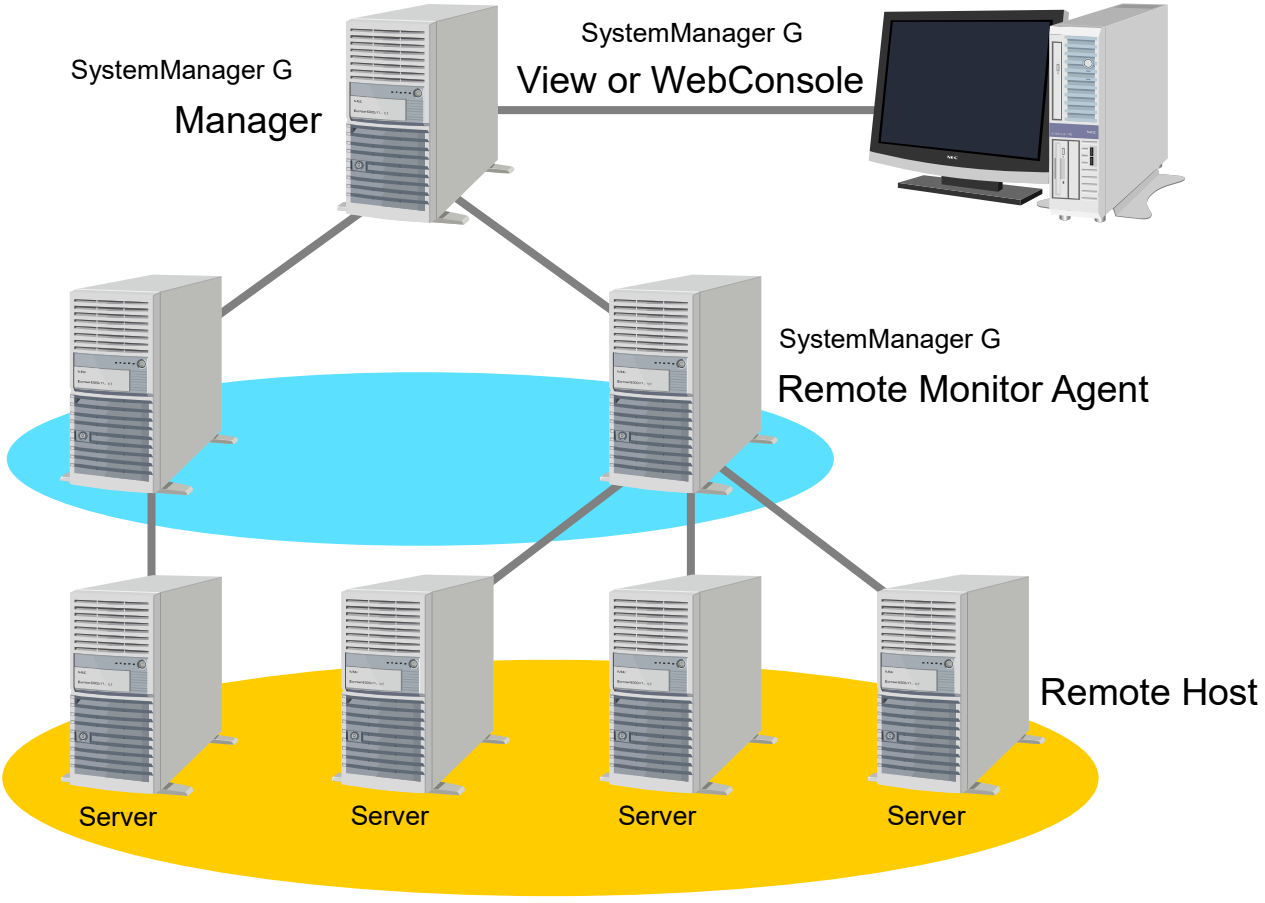
Monitors the usage of resources in the hypervisor (ESXi) and event logs without using agents. However, the agent must be introduced to monitor each guest OS.
For details, see the following document:
MasterScope SystemManager G VMWare Hypervisor Monitoring Function Usage Procedure Manual (HypervisorMonitoring_Guide.pdf)

◆ **Cloud service (AWS) monitoring function**
Event information such as performance information used in the AWS or the change of EC2 status can be acquired from the API provided by the public cloud service (Amazon Web Services).
For details, see the following document:
MasterScope SystemManager G Cloud Service (AWS) Monitoring Function Usage `Procedure (CloudService Monitoring_Guide.pdf)

1.2. About Agentless Monitoring

This product provides a function to monitor a server without installing the agent to the server.
To use this function, the remote monitor agent function is required.

The following shows an overview of an agentless monitoring configuration:



Terms	Description
Agentless monitoring	A function to monitor a server without installing the agent to the server.
Remote monitor agent	It refers to a host to which SystemManager GRemote Monitor Agent has been installed. It collects the information on serversfrom a remote host(s).
Remote host	It refers to a monitored server. SystemManager Gis not installed to it.
Agent (normal agent)	It refers to a host to which SystemManager G Agent has been installed. It is sometimes referred to as “a normal agent” to clearly distinguish it from a remote monitor agent.

The following lists applications supported by the agentless monitoring function:

- Oracle Database
- SQL Server
- Oracle WebLogic Server
- SAP ERP

For notes and constraints when monitoring each functionlisted above, refer to the following sections in the Product Help Manual.

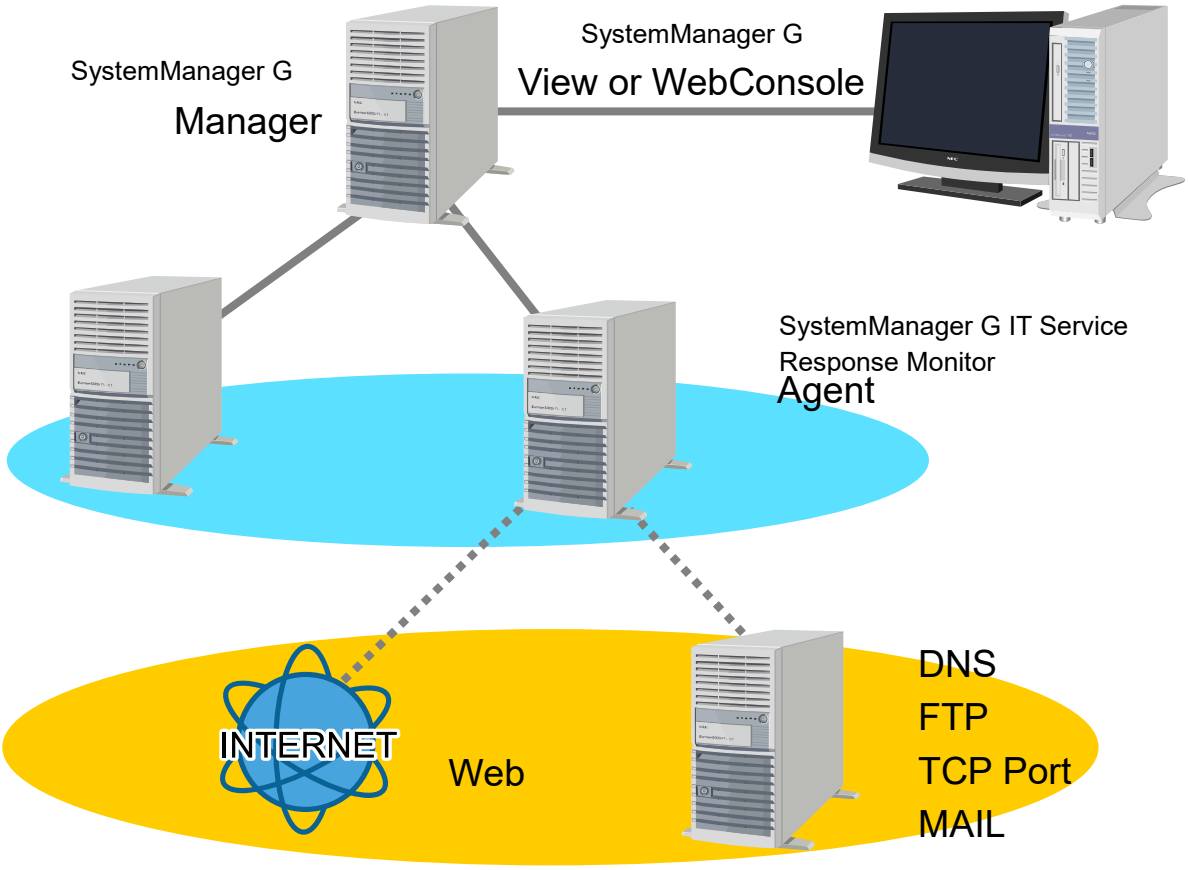
[Monitor a remote host]

1.3. About Probe

1.3.1. About Service Availability Monitoring

The Service availability monitoring function that uses the IT Service Response Monitor in this product emulates access to IT services provided by applications to measure their “availability” and “response”. This enables you to monitor services from the viewpoint of the end user and to quickly detect IT service errors.
To use this function, the probe agent is required.

The following shows the composition example of the “Service availability monitoring” configuration:



Terms	Description
Service availability monitoring	Function to monitor IT services that use IT Service Response Monitor.
Probe agent	Indicates the host to which SystemManager G IT Service Response MonitorAgent is installed. The probe agent actually emulates access to IT services for monitoring.

The following list IT services supported by the "Service availability monitoring" function:

- Web Scenario Monitoring
- DNS Monitoring
- FTP Monitoring
- TCP port Monitoring
- Mail Monitoring

For notes and constraints when monitoring operations service listed above, refer to the following sections in the Product Help Manual. XX is the monitored IT service name.

[Monitor service availability]
[Monitor XX]

1.3.2. About Hyper Visor Monitor

It's agentless and it's possible to watch the resource use situation of the hyper visor (ESXi) and event log. But, it's necessary to do agent implementation of a watch of each guest OS.

1.3.3. About Cloud Service (AWS) Monitor

Public cloud service (Amazon Web Service) can acquire the performance information which is being used in AWS more than offered API and the event information which investigated and said status change in EC2.About the Manual
The manual for this product is stored in the following path on the MasterScope Media by chm format.
\doc\SysMgrG\SystemManagerG.chm

It also can be referred to from a monitoring window after installing the product.

1.4. Installation Media

This product must be installed from the provided MasterScope Media (DVD media).

2. System Environment

This package runs on the following hardware and software.
The meanings of symbols are as follows; √: Supported -: Outside scope of product definition

For the platforms supporting the hypervisor monitoring function and the system requirements, see "MasterScope SystemManager G Hypervisor Monitoring Option for VMware User Guide"

For the platforms supporting the cloud service (AWS) monitoring function and the system requirements, see " MasterScope SystemManager G Cloud Service (AWS) Monitoring Function User's Guide”

For the platforms supporting WebConsole and the system requirements, see " SystemManager G 7.1 WebConsole Option Release Memo"

2.1. List of Supported Platforms

2.1.1. Supported platforms

OS name	Manager function	Agent function	Remote monitor agent function (*3)	Monitoring terminal function	IA external engine
Windows Server 2008 (SP1, SP2) (32bit)	√ (*1)	√ (*1)	Not Support	√	√
Windows Server 2008 (SP1, SP2) (x64)	√ (*1)	√ (*1)	Not Support	√	√
Windows Server 2008 (SP1, SP2) (Itanium)	-	-	-	-	-
Windows Server 2008 R2 (without SP, SP1)	√ (*1)	√ (*1)	√ (*1)	√	√
Windows Server 2012	√ (*1)	√ (*1)	√ (*1)	√	√
Windows Server 2012 R2	√ (*1)	√ (*1)	√ (*1)	√	√
Windows Server 2016 (*5)	√ (*1)	√ (*1)	√ (*1)	√	√
Windows 7 (without SP, SP1) (32bit) (*4)	Not Support	Not Support	Not Support	√	Not Support
Windows 7 (without SP, SP1) (x64) (*4)	Not Support	Not Support	Not Support	√	Not Support
Windows 8 (32bit) (*4)	Not Support	Not Support	Not Support	√	Not Support
Windows 8 (x64) (*4)	Not Support	Not Support	Not Support	√	Not Support
Windows 8.1 (32bit) (*4)	Not	Not	Not	√	Not

	Support	Support	Support		Support
Windows 8.1 (x64) (*4)	Not Support	Not Support	Not Support	√	Not Support
Windows 10 (32bit) (*4)	Not Support	Not Support	Not Support	√	Not Support
Windows 10 (x64) (*4)	Not Support	Not Support	Not Support	√	Not Support
HP-UX 11i v3 (Itanium)	Not Support	√ (*1)	Not Support	-	√
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (x86)	Not Support	√ (*1)	Not Support	-	√
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (x86_64)	Not Support	√ (*1)	Not Support	-	√
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (Itanium)	-	-	-	-	-
Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86)	√ (*1)	√ (*1)	Not Support	-	√
Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86_64)	√ (*1)	√ (*1)	Not Support	-	√
Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (x86)	√ (*1)	√ (*1) (*2)	Not Support	-	√
Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (x86_64)	√ (*1)	√ (*1) (*2)	Not Support	-	√
Red Hat Enterprise Linux 7.1, 7.2, 7.3 (x86_64)	√ (*1)	√ (*1) (*2)	Not Support	-	√
Red Hat Enterprise Linux 7.4, 7.5 (x86_64)	Not Support	√ (*1) (*2)	Not Support	-	-
SUSE Linux Enterprise Server 11 (SP3) (x86)	Not Support	√ (*1)	Not Support	Not Support	Not Support
SUSE Linux Enterprise Server 11 (SP3) (x86_64)	Not Support	√ (*1)	Not Support	Not Support	Not Support
Oracle Enterprise Linux 5.5 (x86_64)	Not Support	√ (*1)	Not Support	-	Not Support
Oracle Linux 6.2, 6.4 (UEK) (x86_64)	√	√ (*1)	Not Support	-	√
Solaris 10 (SPARC)	Not Support	√	Not Support	-	Not Support
Solaris 11, 11.1, 11.2, 11.3 (SPARC)	Not Support	√	Not Support	-	Not Support
AIX 6.1 (TL9)	Not Support	√	Not Support	-	Not Support
AIX 7.1 (TL0 – TL4)	Not Support	√	Not Support	-	Not Support
AIX 7.2 (TL0 – TL1)	Not Support	√	Not Support	-	Not Support

(*1) Enabled for cluster systems. Not supported for those not marked with *.

(*2) Refer to the Agent platforms supported on a-per-product basis because the products support different platforms.
(*3) This column indicates a platform on which the remote monitoring agent function itself is running. For the platforms that can be monitored as a remote host, refer to "2.1.3. Platforms supported by agentless monitoring".
(*4) The supported editions are as follows:
Windows 7 Professional, Enterprise, Ultimate
Windows 8 Pro, Enterprise
Windows 8.1 Pro, Enterprise
Windows 10 Pro, Education, Enterprise
(*5) Windows Server Core and Nano Server are not supported.

Supported platforms (using the IT Service Response Monitor function)

OS name	Manager function	Probe function	Monitoring terminal function
Windows Server 2008 (SP1, SP2) (32bit)	√ (*1)	√	√
Windows Server 2008 (SP1, SP2) (x64)	√ (*1)	√	√
Windows Server 2008 (SP1, SP2) (Itanium)	-	-	-
Windows Server 2008 R2 (SP1)	√ (*1)	√	√
Windows Server 2012	√ (*1)	√	√
Windows Server 2012 R2	√(*1)	√	√
Windows Server 2016	√(*1)	√	√
Windows 7 (SP1) (32bit) (*2)	Not Support	√	√
Windows 7 (SP1) (x64) (*2)	Not Support	√	√
Windows 8 (32bit) (*2)	Not Support	√	√
Windows 8 (x64) (*2)	Not Support	√	√
Windows 8.1 (32bit) (*2)	Not Support	√	√
Windows 8.1 (x64) (*2)	Not Support	√	√
Windows 10 (32bit) (*2)	Not Support	√	√
Windows 10 (x64) (*2)	Not Support	√	√
HP-UX 11i v3 (Itanium)	Not Support	-	-
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (x86)	-	-	-
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (x86_64)	-	-	-
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (Itanium)	-	-	-
Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86)	√ (*1)	-	-
Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86_64)	√ (*1)	-	-
Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (x86)	√ (*1)	-	-
Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (x86_64)	√ (*1)	-	-
Red Hat Enterprise Linux 7.1, 7.2, 7.3 (x86_64)	√ (*1)	-	-
Red Hat Enterprise Linux 7.4, 7.5 (x86_64)	Not Support	-	-
Oracle Enterprise Linux 5.5 (x86_64)	Not Support	-	-
Oracle Linux 6.2, 6.4 (UEK) (x86_64)	Not Support	-	-
Solaris 10 (SPARC)	Not Support	-	-
Solaris 11, 11.1, 11.2, 11.3 (SPARC)	Not Support	-	-
AIX 6.1 (TL9)	Not Support	-	-
AIX 7.1 (TL0 – TL4)	Not Support	-	-

(*1) Enabled for cluster systems. Not supported for those not marked with *.

(*2) The supported editions are as follows:

Windows 7 Professional, Enterprise, Ultimate

Windows 8 Pro, Enterprise
Windows 8.1 Pro, Enterprise
Windows 10 Pro, Education, Enterprise

2.1.2. Platforms supported on a per-application basis

Agent Platform	Monitored applications				
	Oracle Database (*1) (*2)	**WebLogic Server** (*1) (*2) (*3)	**IIS**	**SQL Server**	**SAP**
Windows Server 2008 (SP1, SP2) (32bit)	√	√	√	√	√
Windows Server 2008 (SP1, SP2) (x64)	√	√	√	√	√
Windows Server 2008 R2 (without SP, SP1)	√	√	√	√	√
Windows Server 2012	√	√	√	√	√
Windows Server 2012 R2	√	√	√	√	√
Windows Server 2016	√	√	√	√	√
HP-UX 11i v3 (Itanium)	√	√	-	-	Not Support
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (x86)	√	√	-	-	Not Support
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (x86_64)	√	√	-	-	Not Support
Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86)	√	√	-	-	Not Support
Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86_64)	√	√	-	-	Not Support
Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (x86)	√	-	-	-	Not Support
Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (x86_64)	√	√	-	-	Not Support
Red Hat Enterprise Linux 7.1, 7.2, 7.3, 7.4, 7.5 (x86_64)	√	√	-	-	Not Support
Oracle Enterprise Linux 5.5 (x86_64)	√	Not Support	-	-	Not Support
Oracle Linux 6.2, 6.4 (UEK) (x86_64)	√	√	-	-	Not Support
Solaris 10 (SPARC)	√	√	-	-	Not Support
Solaris 11, 11.1, 11.2, 11.3 (SPARC)	√	√	-	-	Not Support
AIX 6.1 (TL9)	√	√	-	-	Not Support
AIX 7.1 (TL0 – TL4)	√	√	-	-	Not Support

Agent Platform	Monitored applications			
	Apache	**Tomcat** (*3)	**JavaAP** (*3)	**WebSphere Application Server** (*2)(*3)
Windows Server 2008 (SP1, SP2) (32bit)	√	√	√	√
Windows Server 2008 (SP1, SP2) (x64)	√	√	√	√
Windows Server 2008 R2 (without SP, SP1)	√	√	√	√
Windows Server 2012	√	√	√	√
Windows Server 2012 R2	√	√	√	√
Windows Server 2016	√	√	√	-
HP-UX 11i v3 (Itanium)	Not Support	√	√	Not Support
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (x86)	√	√	√	√
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (x86_64)	√	√	√	√
Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86)	√	√	√	√
Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86_64)	√	√	√	√
Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (x86)	√	√	√	√
Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (x86_64)	√	√	√	√
Red Hat Enterprise Linux 7.1, 7.2, 7.3, 7.4, 7.5 (x86_64)	√	√	√	Not Support
Oracle Enterprise Linux 5.5 (x86_64)	-	-	-	-
Oracle Linux 6.2, 6.4 (UEK) (x86_64)	√	√	√	-
Solaris 10 (SPARC)	Not Support	√	Not Support	Not Support
Solaris 11, 11.1, 11.2, 11.3 (SPARC)	Not Support	√	Not Support	Not Support
AIX 6.1 (TL9)	Not Support	Not Support	√	√
AIX 7.1 (TL0 – TL4)	Not Support	Not Support	√	√

(*1) If you are using Oracle Database and WebLogic Server with a Named User Plus (NUP) license, you need to have a single-user license count for monitoring.

(*2) The separate table lists the status of support on a-per-version basis.

(*3) Being able to monitor with the product that uses Java is only one product in one host. However, monitoring is possible at the identical host by combination of Tomcat and JavaAP, and monitored by using the same Java.

Agent platforms supported on a-per-version Oracle Database

Agent Platform	Oracle Database version		
	11gR2	12cR1	12cR2
Windows Server 2008 (SP1, SP2) (32bit)	√	-	-
Windows Server 2008 (SP1, SP2) (x64)	√	√	-
Windows Server 2008 R2 (without SP, SP2)	√	√	-
Windows Server 2012	√	√	√
Windows Server 2012 R2	√	√	√
Windows Server 2016	-	-	√
HP-UX 11i v3 (Itanium)	√	√	√
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (x86)	√	-	-
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (x86_64)	√	√	-
Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86)	√	-	-
Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86_64)	√	√	-
Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (x86)	√	-	-
Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (x86_64)	√	√	√
Red Hat Enterprise Linux 7.1, 7.2, 7.3, 7.4, 7.5 (x86_64)	√	√	√
Oracle Enterprise Linux 5.5 (x86_64)	√ (*1)	-	-
Oracle Linux 6.2, 6.4 (UEK) (x86_64)	√	√	√
Solaris 10 (SPARC)	√	√	√
Solaris 11, 11.1, 11.2, 11.3 (SPARC)	√	√	√
AIX 6.1 (TL9)	√	√	√
AIX 7.1 (TL0 – TL4)	√ (*2)	√	√

(*1) Only monitoring in the Exadata environment is supported.

(*2) AIX 7.1 SP1 or higher is required.

Agent platforms supported on a-per-version WebLogic Server (AIX)

Agent Platform	WebLogic Server version		
	11gR1	12cR1	12cR2
AIX 6.1 (TL9)	√	√	-
AIX 7.1 (TL0 – TL4)	√	√	√ (*1)

(*1) AIX 7.1 TL1 or higher is required.

Agent platforms supported on a-per-version WebSphere

Agent Platform	WebSphere version 32-bit			WebSphere version 64-bit		
	7.0	8.0	8.5	7.0	8.0	8.5
Windows Server 2008 (SP1, SP2) (32bit)	√	√	√	-	-	-
Windows Server 2008 (SP1, SP2) (x64)	√	√	√	√	√	√
Windows Server 2008 R2 (without SP, SP1)	√	√	√	√	√	√
Windows Server 2012	√	√	√	√	√	√
Windows Server 2012 R2	-	√	-	-	√	-
Windows Server 2016	-	-	-	-	-	-
HP-UX 11i v3 (Itanium)	-	Not Support	Not Support	Not Support	Not Support	Not Support
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (x86)	√	√	√	-	-	-
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (x86_64)	√	√	√	√	√	√
Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86)	√	√	√	-	-	-
Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86_64)	√	√	√	√	√	√
Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (x86)	√	√	√	-	-	-
Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (x86_64)	√	√	√	√	√	√
Red Hat Enterprise Linux 7.1, 7.2, 7.3, 7.4, 7.5 (x86_64)	Not Support	-	-	Not Support	Not Support	-
Oracle Enterprise Linux 5.5 (x86_64)	-	-	-	-	-	-
Oracle Linux 6.2, 6.4 (UEK) (x86_64)	-	-	-	-	-	-
Solaris 10 (SPARC)	Not Support	Not Support	Not Support	Not Support	Not Support	Not Support
Solaris 11, 11.1, 11.2, 11.3 (SPARC)	Not Support	Not Support	Not Support	Not Support	Not Support	Not Support
AIX 6.1 (TL9)	√	√	√	√	√	√
AIX 7.1 (TL0 - TL3)	√ (*1)	√ (*1)	√ (*2)	√ (*1)	√ (*1)	√ (*2)

(*1) AIX 7.1 SP1 or higher is required.

(*2) AIX 7.1 TL1 SP2 or higher is required.

2.1.3. Platforms supported by agentless monitoring

The following platforms can be monitored as a remote host (a host monitored by the remote monitor agent function). It is necessary to set the respective servers that configure clusters as the targets to be monitored when monitoring the cluster environment. It is unable to monitor multiple remote hosts actually with the setting of a single agentless monitoring by specifying the IP address and host name that are shared among clusters.

Supported platforms

OS name
Windows Server 2008 (SP1, SP2) (32bit)
Windows Server 2008 (SP1, SP2) (x64)
Windows Server 2008 R2 (without SP, SP1)
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86)
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86_64)
Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (x86)
Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (x86_64)
Red Hat Enterprise Linux 7.1, 7.2, 7.3, 7.4, 7.5 (x86_64)
Oracle Enterprise Linux 5.5
Oracle Linux 6.2, 6.4 (UEK) (x86_64)

Platforms supported on a per-application basis

Supported platforms for remote monitor agent(*3)	Supported platforms for remote host(*3)	Monitored applications			
		Oracle Database (*1)(*2)	WebLogic Server (*1)	SQL Server	SAP
Windows Server 2008 R2 (without SP, SP1) Windows Server 2012 Windows Server 2012 R2	Windows Server 2008 (SP1, SP2) (32bit)	√	√	√	√
	Windows Server 2008 (SP1, SP2) (x64)	√	√	√	√
	Windows Server 2008 R2 (without SP, SP1)	√	√	√	√
	Windows Server 2012	√	√	√	√
	Windows Server 2012 R2	√	√	√	√
	Windows Server 2016	√	√	√	√
	HP-UX 11i v3 (Itanium)	Not Support	Not Support	-	Not Support
	Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (x86)	√	√	-	Not Support

	Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (x86_64)	√	√	-	Not Support
	Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86)	√	√	-	Not Support
	Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86_64)	√	√	-	Not Support
	Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (x86)	√	-	-	Not Support
	Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (x86_64)	√	√	-	Not Support
	Red Hat Enterprise Linux 7.1, 7.2, 7.3, 7.4, 7.5 (x86_64)	√	√	-	Not Support
	Oracle Enterprise Linux 5.5	Not Support	Not Support	-	Not Support
	Oracle Linux 6.2, 6.4 (UEK) (x86_64)	√	√	-	Not Support
	Solaris 10 (SPARC)	Not Support	Not Support	-	Not Support
	Solaris 11, 11.1, 11.2, 11.3 (SPARC)	Not Support	Not Support	-	Not Support
	AIX 6.1 (TL9)	Not Support	Not Support	-	Not Support
	AIX 7.1 (TL0 – TL4)	Not Support	Not Support	-	Not Support

(*1) If you are using Oracle Database and WebLogic Server with a Named User Plus (NUP) license, you need to have a single-user license count for monitoring.

(*2) A separate table lists how Oracle is supported according to its versions.

(*3) Windows Server Core and Nano Server are not supported.

Remote host platforms supported on a-per-version Oracle Database

Remote host	Oracle Database version		
	11gR2	12cR1	12cR2
Windows Server 2008 (SP1, SP2) (32bit)	√	-	-
Windows Server 2008 (SP1, SP2) (x64)	√	√	-
Windows Server 2008 R2 (without SP, SP1)	√	√	-
Windows Server 2012	√	√	√
Windows Server 2012 R2	√	√	√
Windows Server 2016	-	-	√
HP-UX 11i v3 (Itanium)	Not Support	Not Support	Not Support
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (x86)	√	-	-
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (x86_64)	√	√	-
Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86)	√	-	-
Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9,	√	√	-

5.10, 5.11 (x86_64)			
Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (x86)	√	-	-
Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 (x86_64)	√	√	√
Red Hat Enterprise Linux 7.1, 7.2, 7.3, 7.4, 7.5 (x86_64)	√	√	√
Oracle Enterprise Linux 5.5 (x86_64)	Not Support	-	-
Oracle Linux 6.2, 6.4 (UEK) (x86_64)	√	√	√
Solaris 10 (SPARC)	Not Support	Not Support	Not Support
Solaris 11, 11.1, 11.2, 11.3 (SPARC)	Not Support	Not Support	Not Support
AIX 6.1 (TL9)	Not Support	Not Support	Not Support
AIX 7.1 (TL0 – TL4)	Not Support	Not Support	Not Support

2.2. System Requirements

2.2.1. Windows manager/agent/remote host/monitoring terminal/IA external engine

Item		Description
CPU		Intel dual core Xeon or later, or any compatible equivalent processor 64bit CPU(x64) is recommended when using IA function.
System memory	Manager function	400MB or more Estimate the required memory capacity for when importing probe function settings by: 1.5MB x Number derived from totaling (the number of monitoring settings x the maximum number of the following counters) for all possible types of monitoring (For example, assuming 2 mail monitoring settings and 3 DNS monitoring settings, we obtain 85.5MB from the following calculation: 1.5 × { (2×24) + (3×3) } = 85.5MB) The maximum number of counters in one monitoring setting of each Service availability monitoring is as follows: Web scenario (8 counters x number of steps + 8) Mail 24 counters DNS 3 counters TCP 7 counters FTP 11 counters Estimate the maximum memory capacity used by calculating: Total number of counters = Total number of monitoring x Number listed above (i.e. when you monitor Mail service, apply 24) * If there are no counter settings in the imported settings, the memory capacity calculated by the above method will not be required.
	Manager function (when using IA function)	1GB or more (2GB or more is recommended)
	Agent function	300MB or more (1.5GB or more of virtual memory for Java product monitoring)

Item		Description
	Probe function	100MB or more The following amount of memory is required in addition to the basic requirement when executing the monitoring commands: Web scenario: 300MB x Number of monitored configurations to be executed concurrently Mail: 10MB x Number of monitored configurations to be executed concurrently DNS: 5MB x Number of monitored configurations to be executed concurrently TCP: 5MB x Number of monitored configurations to be executed concurrently FTP: 10MB x Number of monitored configurations to be executed concurrently * For Web scenario monitoring, the amount for the scenario number that the amount of the memory (about 300MB) used with IE executes at the same time is needed. Estimate the required memory capacity for when importing probe function settings by: 1.5MB x Number derived from totaling (the number of monitoring settings x the maximum number of the following counters) for all possible types of monitoring (For example, assuming 2 mail monitoring settings and 3 DNS monitoring settings, we obtain 85.5MB from the following calculation: 1.5 × { (2×24) + (3×3) } = 85.5MB) The maximum number of counters in one monitoring setting of each Service availability monitoring is as follows: Web scenario (8 counters x number of steps + 8) Mail 24 counters DNS 3 counters TCP 7 counters FTP 11 counters Estimate the maximum memory capacity used by calculating: Total number of counters = Total number of monitoring x Number listed above (i.e. when you monitor Mail service, apply 24) * If there are no counter settings in the imported settings, the memory capacity calculated by the above method will not be required.
	Monitoring terminal function	200MB or more

Item		Description
	Monitoring terminal function(when using the probe function)	200MB or more added 300MB (for recording scenario) * For recording scenario, the amount of the memory (about 300MB) used with IE is needed.
	Monitoring terminal function(when using IA function)	1GB or more (2GB or more is recommended)
	IA external engine function	1GB or more (2GB or more is recommended)
Disk (free size) (Note 11)	Manager function	300MB or more (Note 1) (400 MB or larger when using the included database)
	Agent function	100MB or more
	Probe function	100MB or more (Note 9)
	Monitoring terminal function	200MB or more
Network		At least, 100Mbps LAN is recommended
OS (Note 7, 8)	Manager function/ Agent function/ Remote host function/ Monitoring terminal function/ IA external engine function	Refer to "2.1. List of Supported Platforms." x64 Edition is recommended when using IA function in manager function and external engine function.
Required software	Manager function/ Agent function	Either one below for cluster system EXPRESSCLUSTER X 1.x/2.x/3.x for Windows Microsoft Failover Cluster (Windows Server 2008) Windows Server Failover Clustering (Windows Server 2012)
	Agent function	- Oracle Database Client (32-bit) When monitoring x64 environment Oracle by 32-bit mode
		- Microsoft Visual C++ 2010 redistributable package (Note 10) When monitoring by 64-bit mode
		- Java 6/7/8 (32-bit/64-bit execution environment) (Note 11) Only when monitoring WebLogic Server/Tomcat/ JavaAP/WebSphere - Java 9 (64-bit execution environment) Only when monitoring JavaAP by 64-bit mode
		- SAP NW RFC SDK (32-bit) 7.11 Patch level 4 or higher - DLL indicated in the SAP Note 684106 Only when monitoring SAP

Item		Description
	Monitoring terminal function(when using Web Monitoring View) (Note 2)	- Internet Explorer 9, 10, 11
	Probe function	Either one below for cluster system EXPRESSCLUSTER X 3.x for Windows Windows Server Failover Clustering (Windows Server 2012)
		- Internet Explorer 9, 10, 11
	Monitoring terminal function(when using the probe function)	- Internet Explorer 9, 10, 11
Monitored software	Agent function	- Oracle Database Oracle 11gR2, 12cR1, 12cR2 * RAC service monitoring is only intended for the administrator management database * RAC service monitoring for 12c is only intended for the configuration of a standard cluster and for the standard ASM
		- IIS (Note 3, 4, 5) IIS 7.0, 7.5, 8.0, 8.5, 10.0
		- SQL Server SQL Server 2008 SP4, 2008 R2 SP3, 2012 SP3, 2014 SP1/SP2, 2016 (SP1), 2017
		- WebLogic Server WebLogic Server 11gR1, 12cR1, 12cR2
		- Apache HTTP Server Apache 2.2, 2.4
		- Apache Tomcat Tomcat 6.0, 7.0, 8.0, 8.5
		- SAP SAP ERP 6.0 SAP NetWeaver 7.0, 7.3 * It is necessary to apply SAP note 1050662.
		- WebSphere Application Server WebSphere Application Server 7.0, 8.0, 8.5

(Note 1) When using the performance information displaying function (multi graph view), and form function, estimate the usage of disk by referring to "9.5.3. About Accumulating Collected Performance Data."

(Note 2) For notes and restrictions when using the Web monitoring window, refer to "MasterScope Media Release Notes."

(Note 3) IIS versions depend on Windows versions. The versions of FTP included in IIS also depend on Window versions.

Windows version	IIS version	FTP version

Windows Server 2008	IIS 7.0	FTP 6.0
Windows Server 2008 R2	IIS 7.5	FTP 7.5
Windows Server 2012	IIS 8.0	FTP 8.0
Windows Server 2012 R2	IIS 8.5	FTP 8.5
Windows Server 2016	IIS 10.0	FTP 10.0

For IIS 7.0, you can change its FTP version to 7.5 by installing “Microsoft FTP Service 7.5 for IIS 7.0,” which is released on the Microsoft site.

(Note 4) If you want to monitor counters on an FTP site in an environment where Microsoft FTP Service 7.5 for IIS 7.0 has been installed, you must apply the Hotfix of KB970838.
For details, refer to http://support.microsoft.com/kb/970838/en-us.

(Note 5) If you want to monitor the [State] counter on a Web site in an IIS 7.5 environment, you must apply the Hotfix of KB2428216.
For details, refer to http://support.microsoft.com/kb/2428216/en-us.

(Note 6) Windows Server Core and Nano Server are not supported.

(Note 7) Only English version is supported.

(Note 8) When using FTP monitoring, capacity for the acquired files is also required.

(Note 9) Microsoft Visual C++ 2010 redistributable package is installed by executing the following file of MasterScope Media.
\tools\Microsoft\2010\vcredist_x64\vcredist_x64.exe
For details about 64-bit counters, see the file of "List of monitored items" on the following NEC support portal (Japanese).
https://www.support.nec.co.jp/View.aspx?NoClear=on&id=3140102695

(Note 10) The Java Runtime Environment corresponding to the operating mode of the application monitoring function is required. For details, refer to "8.5. Operating mode of the application monitoring functions."

(Note 11) This does not include areas such as those for data files to be created following installation of the package.

2.2.2. Windows remote monitor agent

Item		Description
CPU		Intel dual core Xeon or later, or any compatible equivalent processor
System memory	Remote monitor agent function	300 MB or more (1.5 GB or more of virtual memory for Java product monitoring)
Disk (free size)	Remote monitor agent function	1 GB or more (Note 1, 2)
Network		At least, 100 Mbps LAN is recommended

OS (Note 7, 8)	Remote monitor agent function	Refer to "2.1. List of Supported Platforms."
Required software	Remote monitor agent function	- Oracle Database Client (32-bit/64-bit) (Note 3) Only when monitoring Oracle
		- Java 6/7/8 (32-bit/64-bit execution environment) (Note 4, 9) Only when monitoring WebLogic Server
		- SAP NW RFC SDK (32bit) 7.11 Patch level 4 or higher (Note 5) - DLLs that are described in SAP Note 684106 Only when monitoring SAP
		.NET Framework is required to perform hypervisor monitoring by using the agentless monitoring function. (Note 9)
Monitored software	Remote monitor agent function	- Oracle Database Oracle 11gR2, 12cR1, 12cR2
		- SQL Server SQL Server 2008 SP4, 2008 R2 SP3, 2012 SP3, 2014 SP1/SP2, 2016 (SP1), 2017
		- WebLogic Server WebLogic Server 11gR1, 12cR1, 12cR2
		- SAP SAP ERP 6.0 SAP NetWeaver 7.3 * SAP Note 1050662 must be applied
Maximum number of monitored remote host instances	Remote monitor agent function	- Oracle Database 64 instances (Note 6)
		- SQL Server 64 instances (Note 6)
		- WebLogic Server 32 instances (Note 6)
		- SAP 32 instances (Note 6)

(Note 1) Note that if you have a large number of monitored remote hosts and need to store performance data on disk over a long period of time, it may cause impact on disk on the relevant remote monitor agent.
The arithmetic expression to calculate the disk usage is described in the following item for the respective product help manuals:

[Maintenance]
[Backup information]
[Collected data] - refer to "History data for performance monitoring"

(Note 2) When a remote monitor agent cannot communicate with the manager, the agent retains the information on itself on a temporary basis. Note that when a remote host agent has many remote hosts, the retained information may cause impact on the disk usage of the remote monitor agent. For information on changing the number of pieces of retained information, refer

to "11.2.7. About Retaining Information on Remote Monitor Agent."

(Note 3) For details about the supported combinations of Oracle Database on a remote host and Oracle Client, refer to the following:
KROWN#56903: About support for compatibility among different versions of Oracle Servers

(Note 4) Agentless monitoring requires a client Jar file for WebLogic Server created on the WebLogic server. For how to create the file, refer to the following item in the relevant online help:
[Monitor a remote host]
[Monitor applications on a remote host]
[Monitor WebLogic]
[Perform preparations before monitoring WebLogic Server on a remote host]

(Note 5) For the combinations of SAP system versions and OS versions with SAP NetWeaver RFC library versions and for the upper/lower compatibility of the SAP NetWeaver RFC library, refer to SAP NOTE 413708.

(Note 6) Ensure that the total number of monitored instances on one remote monitor agent does not exceed the maximum number of monitored remote host instances. Note that if you want to monitor 17 instances or more of the WebLogic server in WebLogic monitoring, refer to the following item in the relevant online help:
[Monitor a remote host]
[Monitor applications on a remote host]
[Monitor WebLogic]
[Perform preparations before monitoring WebLogic Server on a remote host]

(Note 7) Windows Server Core and Nano Server are not supported.

(Note 8) Only English version is supported.

(Note 9) The Java Runtime Environment corresponding to the operating mode of the application monitoring function is required. For details, refer to "8.5. Operating mode of the application monitoring functions."

(Note 10) .NET Framework is required to perform hypervisor monitoring by using the agentless monitoring function.
For details, refer to the documentation in the following location.
MasterScope SystemManager G Hypervisor Monitor Option for VMware
(HypervisorMonitor_Guide.pdf)

(Note 11) .NET Framework 3.5 is required to perform cloud service (AWS) monitoring by using the agentless monitoring function.
For details, refer to the documentation in the following location.
MasterScope SystemManager G Cloud Service (AWS) Monitoring Function
(CloudServiceMonitor_Guide.pdf)

2.2.3. HP-UX manager/agent/ IA external engine

Item		Description
CPU		Itanium
System memory	Manager function	400MB or more Estimate the required memory capacity for when importing probe function settings by: 1.5MB x Number derived from totaling (the number of monitoring settings x the maximum number of the following counters) for all possible types of monitoring (For example, assuming 2 mail monitoring settings and 3 DNS monitoring settings, we obtain 85.5MB from the following calculation: 1.5 × { (2×24) + (3×3) } = 85.5MB) The maximum number of counters in one monitoring setting of each Service availability monitoring is as follows: Web scenario (8 counters x number of steps + 8) Mail 24 counters DNS 3 counters TCP 7 counters FTP 11 counters Estimate the maximum memory capacity used by calculating: Total number of counters = Total number of monitoring x Number listed above (i.e. when you monitor Mail service, apply 24) * If there are no counter settings in the imported settings, the memory capacity calculated by the above method will not be required.
	Manager function (when using IA function)	1GB or more (2GB or more is recommended)
	Agent function	100MB or more (300MB or more of virtual memory for Java product monitoring)
	IA external engine function	1GB or more (2GB or more is recommended)
Disk (free size) (Note 3)	Manager function	500MB or more (600 MB or larger when using the included database) (Note 1)
	Agent function	200MBor more
Network		At least, 100Mbps LAN is recommended

OS (Note 2)	Manager function/ Agent function/ IA external engine function	Refer to "2.1. List of Supported Platforms."
Required software	Manager function/ Agent function	- OS package HP-UX common: DCE-Core HP-UX 11i v3: HPUXLocales
	Agent function	- Oracle Database Client (32-bit) When monitoring Oracle by 32-bit mode
		- Java 6/7/8 execution environment Only when monitoring WebLogic Server/Tomcat/ JavaAP
Monitored software	Agent function	- Oracle Database Oracle 11gR2 (Itanium only), 12cR1 (Itanium only), 12cR2 (Itanium only) * In the case of 12c, RAC service monitoring is not supported. * RAC service monitoring is supported for administrator managed database only.
		- WebLogic Server WebLogic Server 11gR1, 12cR1, 12cR2
		- Apache Tomcat Tomcat 6.0, 7.0, 8.0, 8.5

(Note 1) When using the performance information displaying function (multi graph view), and form function, estimate the usage of disk by referring to "9.5.3. About Accumulating Collected Performance Data."

(Note 2) The following OS patches are required:

HP-UX 11i v3
Manager function / IA external engine function
PHCO_41407 or its subsequent patches
PHKL_41967 or its subsequent patches
PHCO_44582 or its subsequent patches
Agent function
PHCO_41407 or its subsequent patches
PHKL_41967 or its subsequent patches

(Note 3) This does not include areas such as those for data files to be created following installation of the package.

2.2.4. Linux manager/agent/remote host

Item		Description
CPU		Intel dual core Xeon or later, or any compatible equivalent processor 64bit CPU(x64) is recommended when using IA function.
System memory	Manager function	1GB or more Estimate the required memory capacity for when importing probe function settings by: 1.5MB x Number derived from totaling (the number of monitoring settings x the maximum number of the following counters) for all possible types of monitoring (For example, assuming 2 mail monitoring settings and 3 DNS monitoring settings, we obtain 85.5MB from the following calculation: 1.5 × { (2×24) + (3×3) } = 85.5MB) The maximum number of counters in one monitoring setting of each Service availability monitoring is as follows: Web scenario (8 counters x number of steps + 8) Mail 24 counters DNS 3 counters TCP 7 counters FTP 11 counters Estimate the maximum memory capacity used by calculating: Total number of counters = Total number of monitoring x Number listed above (i.e. when you monitor Mail service, apply 24) * If there are no counter settings in the imported settings, the memory capacity calculated by the above method will not be required.
	Manager function (when using IA function)	1GB or more (2GB or more is recommended)
	Agent function	500MB or more (1.5GB or more of virtual memory for Java product monitoring, 2GB or more of virtual memory for 64-bit mode)
	IA external engine function	1GB or more (2GB or more is recommended)
Disk (free size)	Manager function	300MB or more (Note 1) (400 MB or larger when using the included database)
	Agent function	100MB or more

Item		Description
	IA external engine function	100MB or more
Network		At least, 100Mbps LAN is recommended
OS (Note 2)	Manager function/ Agent function/ Remote host function/ IA external engine function	Refer to "2.1. List of Supported Platforms."
Required software	Manager function/ Agent function	- In the cluster environment EXPRESSCLUSTER X 3.x for Linux

Item		Description
		- OS package Linux common : bc (Required in agent function) compat-libstdc++-33 (32bit) (Note 5) libgcc (32bit) ncompress (or gzip) net-tools (iproute in RHEL 7) procps (procps-ng in RHEL 7) redhat-lsb (Note 5) rpm-build (Note 4) rsh (Required in manager function) RHEL 7: (Note 7) glibc (32bit) libuuid (32bit) ncurses-libs (32bit) sysstat (10.1.5) (This is unnecessary for an external engine.) RHEL 6, Oracle Linux 6 : glibc (32bit) libuuid (32bit) ncurses-libs (32bit) sysstat (9.0.4) (This is unnecessary for an external engine.) RHEL 5, Oracle Enterprise Linux 5 : e2fsprogs-libs (32bit) glibc (32bit) ncurses (32bit) sysstat (any one of 5.0.5, 6.0.2, 7.0.0, 7.0.2) (This is unnecessary for an external engine.) Linux common (64bit environment) : For a 64bit environment, you need the following packages in addition to 32bit versions of the packages: libgcc (64bit) glibc (64bit) libstdc++ (64bit) To use 64-bit mode, the agent function needs a 64-bit package in addition to a 32-bit package.
	Agent function	- Oracle Database Client (32bit) When monitoring x86_64 environment Oracle by 32-bit mode
		- Java 6/7/8 (32-bit/64-bit execution environment) (Note 5, 6) Only when monitoring WebLogic Server/Tomcat/ JavaAP/WebSphere - Java 9 (64-bit execution environment) Only when monitoring JavaAP by 64-bit mode

Item		Description
	Remote host function	- OS package Linux common : bc glibc (32bit) libgcc (32bit) procps (procps-ng in RHEL 7) openssh openssh-server openssh-clients (Note 3) openssl * The ssh daemon must be operating in addition to the packages above. RHEL 7: ncurses-libs (32bit) sysstat (10.1.5) RHEL 6, Oracle Linux 6 : ncurses-libs (32bit) sysstat (9.0.4) RHEL 5, Oracle Enterprise Linux 5 : ncurses (32bit) sysstat (7.0.2)
Monitored software	Agent function	- Oracle Database Oracle 11gR2, 12cR1, 12cR2 * RAC service monitoring is only intended for the administrator management database * RAC service monitoring for 12c is only intended for the configuration of a standard cluster and for the standard ASM
		- WebLogic Server WebLogic Server 11gR1, 12cR1, 12cR2
		- Apache HTTP Server Apache 2.2, 2.4
		- Apache Tomcat Tomcat 6.0, 7.0, 8.0, 8.5
		- WebSphere Application Server WebSphere Application Server 7.0, 8.0, 8.5

(Note 1) When using the the performance information displaying function (multi graph view), and form function, estimate the usage of disk by referring to "9.5.3. About Accumulating Collected Performance Data."

(Note 2) When using Linux, set SELinux to "disabled" beforehand. Note that SELinux is enabled by default in Red Hat Enterprise Linux 6 or later.

(Note 3) When the packages isn't introduced, a remote monitor agent will abnormal end.

(Note 4) This is necessary when specifying a Service Identifier for the service to install. Identifier specification can be omitted for a normal configuration (the concerned package is not required when omitted), however, it cannot be omitted for a multi-instance configuration.

(Note 5) This package is not included in an installation media of RHEL 7 (ISO image). Download it at the customer portal of Red Hat, Inc. (https://access.redhat.com)

(Note 6) The Java Runtime Environment corresponding to the operating mode of the application monitoring function is required. For details, refer to "8.5. Operating mode of the application monitoring functions."

(Note 7) systemd-219-19.el7 to systemd-219-19.el7_2.3 of systemd package in RHEL7 contains a bug that inter-process communication (IPC) resources are cleared when the user session ends. The included DB might be crashed due to its effects. This problem was corrected in systemd-219-19.el7_2.4 or later.
Update the version to systemd-219-19.el7_2.4 or later when installing the package using the " Use Bundled DB " setting. In addition, restart systemd with the following command after updating the version.

```
# systemctl restart systemd-logind.service
```

Update is not required in systemd-219-19.el7 or earlier version, which does not contain this bug.

2.2.5. Solaris agent

Item		Description
CPU		UltraSPARC-IIi 650MHz or higher is recommended
System memory	Agent function	200MB or more
Disk (free size)	Agent function	1GB or more
Network		At least, 100Mbps LAN is recommended
OS	Agent function	Refer to "2.1. List of Supported Platforms."
Required software	Agent function	The latest libC patch - OS package Solaris common: SUNWbash SUNWcsl SUNWlibC SUNWlibms SUNWuiu8 Solaris 11: SUNWiconv-unicode Solaris 10: SUNWjiu8 SUNWaccu SUNWaccr * You must apply the following patch unless you have Solaris 10 after June 2007. - 125100-04 Kernel Update Patch - 120473-05 libc nss ldap PAM zfs Patch - 125800-01 Fault Manager Patch
		- Oracle Database Client (32-bit) When monitoring Oracle by 32-bit mode
		- Java 6/7/8 (32-bit/64-bit execution environment) (Note 1) Only when monitoring WebLogic Server/Tomcat
Monitored software	Agent function	- Oracle Database Oracle 11gR2, 12cR1, 12cR2 * RAC service monitoring function is not supported
		- WebLogic Server WebLogic Server 11gR1, 12cR1, 12cR2
		- Apache Tomcat Tomcat 6.0, 7.0, 8.0, 8.5

(Note 1) The Java Runtime Environment corresponding to the operating mode of the application monitoring function is required. For details, refer to "8.5. Operating mode of the application monitoring functions."

2.2.6. AIX agent

Item		Description
CPU		POWER5 1.6GHz or higher is recommended
System memory	Agent function	100MB or more
Disk (free size)	Agent function	1GB or more
Network		At least, 100Mbps LAN is recommended
OS (Note 1)	Agent function	Refer to "2.1. List of Supported Platforms."
Required software	Agent function	- OS package AIX common: xlC.rte bos.rte.iconv bos.rte.libpthreads bos.rte.libc bos.rte.bind_cmds bos.rte.security bos.rte.libcur bos.adt.insttools (Note 3) bos.iconv bos.acct bos.perf.tools bos.net.tcp.client UTF-8 language environment (Note 2) AIX 7.2: - AIX 7.1: bos.net.ncs AIX 6.1: bos.net.ncs
		- Oracle Database Client (32-bit) When monitoring Oracle by 32-bit mode
		- Java 6/7 (32-bit/64-bit execution environment) (Note 4) Only when monitoring WebLogic Server/JavaAP/WebSphere
Monitored software	Agent function	- Oracle Database Oracle 11gR2, 12cR1, 12cR2 * RAC service monitoring function is not supported
		- WebLogic Server WebLogic Server 11gR1, 12cR1, 12cR2
		- WebSphere Application Server WebSphere Application Server 7.0, 8.0, 8.5

(Note 1) If you want to use AIX, please apply the patches provided by IBM Corporation. The following lists the APAR numbers that have been confirmed now.

AIX version	Required patch
6.1	IV56395, or TL9SP3 or later Fixpack
7.1	IV56004, or TL3SP3 or later Fixpack

Please get the patch information at Web site etc. of IBM Corporation.

If making the application using Java work, it is necessary to apply the following OS patches.

AIX version	Required patch
6.1 TL2	IZ84087
6.1 TL3	IZ83815
6.1 TL4	IZ65501, IZ84055
6.1 TL5	IZ73931, IZ83856
6.1 TL6	IZ81170, IZ81962
7.1	IZ86109
7.1 TL1	IV09585

[Reference]
AIX APARs required when running the IBM SDK or JRE for Java
http://www-01.ibm.com/support/docview.wss?uid=swg21605167

(Note 2) To install the UTF-8 language environment, set the OS media, run the following command:
smitty lang
select [Add Additional LanguageEnvironments]
select [UTF-8 English (United States) [EN_US]] in [CULTURAL convention to install]
select [UTF-8 English (United States) [EN_US]] in [LANGUAGE translation to install]

(Note 3) This is necessary when specifying a Service Identifier for the service to install. Identifier specification can be omitted for a normal configuration (the concerned package is not required when omitted), however, it cannot be omitted for a multi-instance configuration.

(Note 4) The Java Runtime Environment corresponding to the operating mode of the application monitoring function is required. For details, refer to "8.5. Operating mode of the application monitoring functions."

2.2.7. PATLITE

The PATLITE reporting function supports the following products from PATLITE Corporation:

Item	Description
Serial Interface type	PHE-3FB-RYG PHE-3FBE1-RYG PHC-100A PHC-D08 (Note 1) (Note 2) PHE-3FB2-RYG (Note 1) (Note 2)
LAN Interface lighting type	NHE-3FB-RYG NHC-3FB-RYG NHM-3FB-RYG NHS-3FB1-RYG NHP-3FB1-RYG NHL-3FB1-RYG

(Note 1) This function can be used even with USB connection.

(Note 2) Use the normal operation mode of PATLITE. PATLITE does not operate in the PHU compatible mode.

3. What's New in this Release

This section outlines new features and enhances functions.

3.1. WebConsole function enhancements

A new WebGUI function has been added.
Performance and other information can now be checked by using a web browser.

For details, see the following:
MasterScope SystemManager G WebConsole Option Release Memo
(webconsole_rel.pdf)

4. Improvements

This version contains the improvements for SystemManager G as described in Table 1. Note that √ indicates the improved functions.

Table 1 Improvements

Item No	Details	Function applied									
		Console function	Manager function			Agent function					Remote monitoring agent
			Windows	HP-UX	Linux	Windows	HP-UX	Solaris	AIX	Linux	Windows
1	A correction has been made to overcome the problem whereby the monitoring definition is deleted if the system fails to create a monitoring target list for the event log or the system log during the startup of the manager or an agent for some reason. In addition,	√	√	√	√		√	√	√	√	√

	messages to be output by the event log monitoring and system log monitoring functions (message IDs: 00480003, 00480004, 00440003, and 00440004) have been added.										
2	A correction has been made to overcome the problem whereby, after a change to the event time zone for the cloud service monitoring, the time zone is not changed but instead returned to its default setting when the event is updated in accordance with the latest information.	√									√ (Hypervisor monitoring/ AWS monitoring)

5. Preparations

Prior to installing this product, perform the following preparations:

5.1. About Preparations for Agentless Monitoring

- Before using the agentless monitoring function, carefully read the functional overview and notes of the agentless monitoring in the following item in the help:

  [Monitor a remote host]
  [About remote host monitoring]

- If you need to monitor the applications, using the agentless monitoring function, perform preparations by referring to the following sections in the Product Help Manual. XX is the monitored application name.

  [Monitor a remote host]
  [Monitoring applications on a remote host]
  [Monitor XX]
  [Perform preparations before monitoring XX on a remote host]

5.2. Application Monitoring

To monitor applications by using the agent, perform the preparation described in the following sections of the Product Help Manual. XX is the monitored application name.

[Monitor applications]
[Monitor XX]
[Preparations for XX performance monitoring] -> [Preparation]

or

[Monitor applications]
[Monitor XX]
[Preparations for XX performance monitoring]
[About preparations for XX performance monitoring] -> [Preparation]

5.3. Service Availability Monitoring

To monitor service availability, perform the preparation described in the following sections of the Product Help Manual.

[Monitor service availability]
  [Monitor through a Web scenarios]
    [Perform preparations for Web scenario monitoring]

  [Monitor mail services]
    [Perform preparations for mail monitoring]

  [Monitor DNS services]
    [Perform preparations for DNS monitoring]

  [Monitor TCP port]
    [Perform preparations for TCP monitoring]

  [Monitor FTP services]
    [Perform preparations for FTP monitoring]

6. How to Install or Uninstall the Product

For information on how to install and uninstall this product, refer to the following document:

"MasterScope Media Release Notes"
PDF file, relmemo.pdf, in the root folder on "MasterScope Media"

■ **Ansible**

The Ansible roles assisting construction automation are released.
For details, see the following:

http://support.pf.nec.co.jp/gh/View.aspx?id=4140100069

■ **Agent function**

Several kinds of agents are existed in SystemManager G as follows. Select it for many purposes.

Product name	Description
MasterScope SystemManager G Agent	Normal agent (Application monitoring)
MasterScope SystemManager G Logical Agent	Logical system agent
MasterScope SystemManager G Remote Monitor Agent	Agentless monitoring (Remote monitor agent)
MasterScope SystemManager G Probe Agent	Service availability monitoring (Probe)

■ **WebConsole function**

To use WebConsole, install the SystemManager G WebConsole Option function.
For details, see " WebSAM SystemManager G 7.1 WebConsole Option Installation Guide"

■ **Note on host name**

As the default host name displayed by Windows installer is a NETBIOS name, it is described in upper case. To monitor Oracle RAC, it must completely match the Public node name retained by Oracle for configuring RAC, including the upper case/lower case description. If they do not match, rewrite the Public node name of Oracle.

When installing several products in separate installation directories inside one node, installing one product several times (multi-instance), or using normal agents with logical system agents, set a different name for the hostname of each agents so that the manager can identify each agents uniquely by its hostname.

* When installingSystemManager G IT Service Response Monitor options, SystemManager G agent, and other agents of MasterScope products on the same machine, the above rule for hostname applies (equivalent to the case which several products are installed with one node by dividing the installation directory). Set probe's hostname different from the agent i.e. by adding "_Probe" to the end of the hostname of the probe. The hostname of the probe set here does not need to be resolved by hosts file and other methods.

■ **Separation of data**

Installing data in the active/standby hot standby type cluster system saves the program on the local disk and data on the common disk. In contrast, for single nodes, both the program and data are saved in the installation directory. To separate the data in single nodes, specify the common directory.

■ **Cluster system support**

For information on support for the active/standby hot standby type cluster system, refer to "2.1. List of Supported Platforms".

■ **DB setting when monitoring Oracle**

If you want to set up Oracle as a target to be monitored, you must set up DB with a setup script/cleanup script when installing/uninstalling the product. For details, refer to the following sections in the Product Help manual.

[Monitor applications]
  [Monitor Oracle]
    [Preparations for Oracle performance monitoring]
      [DB setting when monitoring Oracle]

■ **About Target Licenses when using Service availability monitoring**

The license system for probes consists of target licenses described in the following:

- The number of licenses depends not on the number of probe terminals, but on that of monitored targets (instances).
- More than one monitoring setting can be configured on one probe terminal. Each monitoring setting has a setting value of [enable/disable] to indicate whether the monitoring is actually to be performed.
- Without a proper license, it is still possible to connect the probe terminal to the manager and to add a monitoring setting to the probe terminal.
- One license is consumed for each enabled monitoring setting.
- Instances whose monitoring settings are disabled are not monitored.

7. Duplex Setting

7.1. Settings for Duplexing Manager

For information on duplexing and using your manager, refer to the cluster setup guides.

The cluster setup guides are stored at the following path in the MasterScope Media.
\doc\SysMgrG\Cluster

- When you use EXPRESSCLUSTER X in Windows:
  Cluster_Win_EXPRESSCLUSTER_X.pdf

- When you use Microsoft Failover Cluster in Windows Server 2008:
  Cluster_Win_MSFC.pdf

- When you use Windows Server Failover Clustering in Windows Server 2012:
  Cluster_Win_WSFC.pdf

- When you use EXPRESSCLUSTER X in Linux:
  Cluster_Linux_EXPRESSCLUSTER_X.pdf

- When you use Remote Monitor:
  RemoteMonitor_ClusterSetupGuide.pdf

7.2. Settings for Duplexing Agent

For information on setting agents to be used in a duplex configuration, refer to the "Logical Agent Installation Guide," in addition to the "Duplexing Setup Guide" described earlier.
Refer to \doc\SysMgrG\Logical_Agent.pdf in “MasterScope Media”.

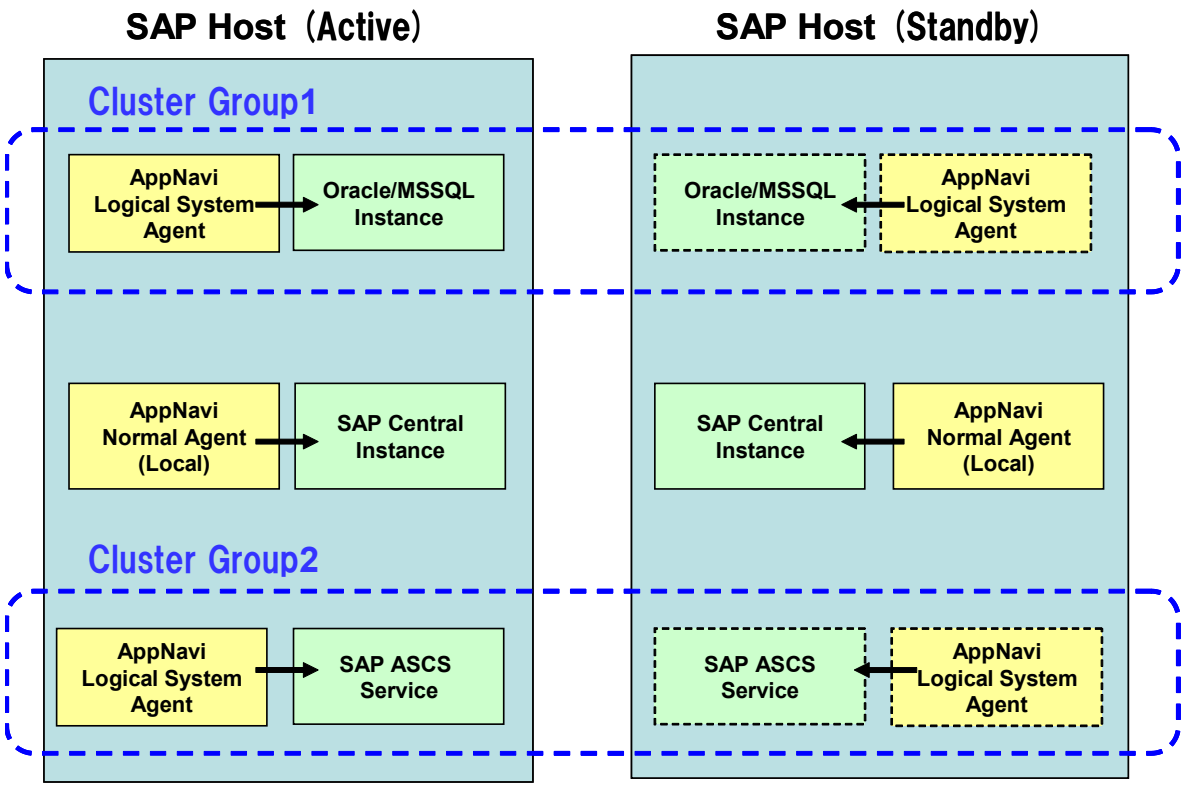
For information on setting Service availability monitoring to be use in duplex system, refer to be the "MasterScope SystemManager G IT Service Response Monitor Duplex Setup Guide", in addition to the Chapter 5.1 described earlier.
Refer to \doc\SysMgrG\ ITServiceResponseMonitorAgent_ClusterSetupGuide.pdf in “MasterScope Media”.

For duplexing remote monitor agent, refer to the "Remote Monitor Duplication Setup Guide."
Refer to \doc\SysMgrG\RemoteMonitor_ClusterSetupGuide.pdf in “MasterScope Media”.

In addition to the above, refer to the "Notes."

7.2.1. Example of Settings for SAP Monitoring

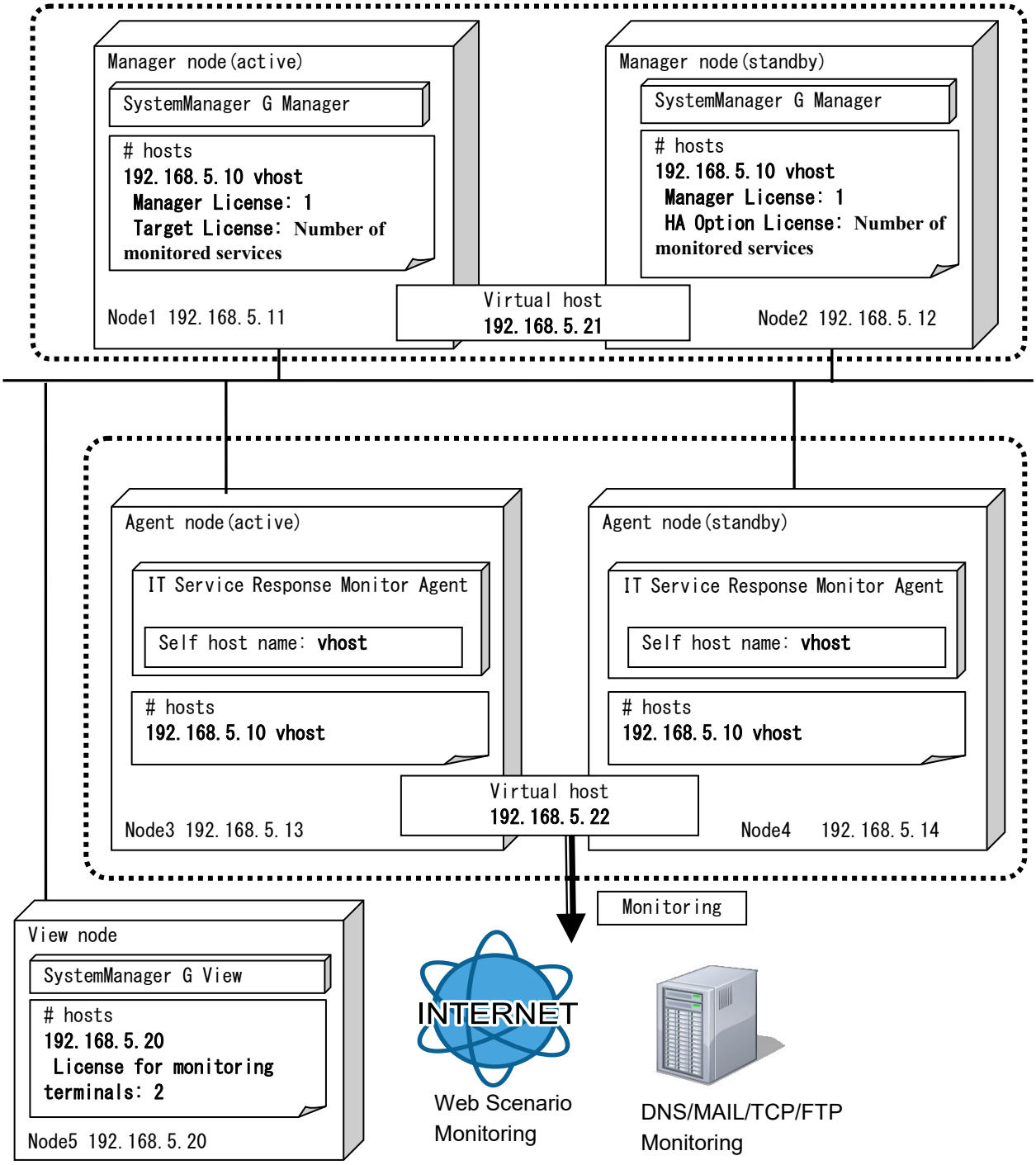
To operate the SAP system as a cluster system, the package can be switched as HA cluster for ASCS (ABAP Central Services instance) and database, etc., and CI (central instance) can be constructed on the individual hosts.
The following describes an example of settings for SAP monitoring in this case.



As shown in the figure, the agent monitoring the SAP central instance is installed in both the active and standby hosts as the normal agent, and monitoring is carried out.
In addition, the agent monitoring the ASCS process and agent monitoring the database are installed in both the active and standby systems as logical system agents so that when failures occur, the logical system agent also failovers linked to the failover of the cluster group, allowing monitoring to be continued.

The figure is based on the following configuration.

- The normal agent is installed in the local disk to monitor the performance of the SAP instance, SAP system log, and CCMS alert on the same host.
- The shared disk is specified in the data area and the logical system agent is installed to monitor performance of the Oracle or MSSQL instance in the same cluster group.
- The shared disk is specified in the data area and the logical system agent is installed to monitor the SAP ASCS process (service) on the same cluster group.


Manager node(active)
SystemManager G Manager
hosts
192.168.5.10 vhost
Manager License: 1
Target License: Number of monitored services
Node1 192.168.5.11
Manager node(standby)
SystemManager G Manager
hosts
192.168.5.10 vhost
Manager License: 1
HA Option License: Number of monitored services
Node2 192.168.5.12
Virtual host
192.168.5.21
Agent node(active)
IT Service Response Monitor Agent
Self host name: vhost
hosts
192.168.5.10 vhost
Node3 192.168.5.13
Agent node(standby)
IT Service Response Monitor Agent
Self host name: vhost
hosts
192.168.5.10 vhost
Node4 192.168.5.14
Virtual host
192.168.5.22
Monitoring
View node
SystemManager G View
hosts
192.168.5.20
License for monitoring terminals: 2
Node5 192.168.5.20
INTERNET
Web Scenario Monitoring
DNS/MAIL/TCP/FTP Monitoring

8. Set up an Environment after Installation

8.1. About Agentless Monitoring Environment Configuration

If you need to monitor the applications, using the agentless monitoring function, configure the environment by referring to the following sections in the Product Help Manual. XX is the monitored application name.

[Monitor a remote host]
[Monitor applications on a remote host]
[Monitor XX]
[Perform preparations before monitoring XX on a remote host]

8.2. Application Monitoring

To monitor applications by using the agent, perform the environment setting after the installation as described in the following sections of the Product Help Manual. XX is the monitored application name.

[Monitor applications]
[Monitor XX]
[Preparations for XX performance monitoring] -> [Environment setting after installing SystemManager G]

or

[Monitor applications]
[Monitor XX]
[Preparations for XX performance monitoring]
[About preparations for XX performance monitoring] -> [Environment setting after installing SystemManager G]

8.3. Service Availability Monitoring

To use Service availability monitoring function, refer to the following section in the Product Help Manual, and set a filter definition at the business view.

[Monitor service availability]
[Monitor through a Web scenario]
[Web scenario monitoring]
[Set a filter definition]

8.4. When Using IPv6

SystemManager G can use IPv6 as communication protocol for the communications between the manager and agent, and the manager and monitoring window (Web monitoring window). However, confirm the following descriptions when monitoring using IPv6 communications.

- When communicating using IPv6, it is necessary to configure the ini file after the installation. For details, see "8.4.1Configuring Protocols".

- IPv6 addresses can be entered for other than Apache monitoring of application monitoring functions.
- Only IPv4 IP addresses can be entered when entering IP addresses in the monitoring window unless otherwise described in the individual function manuals except the application monitoring function. IPv6 addresses cannot be described. In addition, only IPv4 addresses can be used instead of host names. Use host names that can be resolved in advance by DNS or host when communicating using IPv6.

- IPv6 communications cannot be used for the following functions. Use IPv4 communications (default value) when using the following functions.

Standard functions

- Agentless monitoring function
- MCO Linker function
- Manager linkage function
- WebConsole Option

Optional functions

- Invariant Analyzer function
- Service Availability Monitoring functions (DNS monitoring, MAIL monitoring, TCP port monitoring, FTP monitoring)
- Operation control function
- Scenario control function
- ServiceManager linkage function
- External product linkage function

8.4.1. Configuring Protocols

■ Notes on the configuration

- The [UpperNode] and [SelfNode] sections are already described in each configuration file. Add the protocol settings at the end of each section.
- If the protocol settings are not described, IPv4 communications are used.
- To use IPv6 communications, the settings must be specified for both functions to communicate. For example, to communicate between the manager and agent using IPv6 communications, the protocol used for the connection with the manager must be specified on the agent side, and the protocol used to wait the connection with the agent must be specified on the manager side.

- When using dual stack for communications, if the IPv4 only mode or IPv6 only mode is selected for the protocol settings, it does not switch to the other protocol communication upon failure of the specified protocol communication. To communicate using both protocols, specify the IPv4 and IPv6 communications combination mode.
- To reflect the settings, restart the processes of each function.

■ Agent (Remote monitor agent not included)

[File path]

Windows	<Installation path>\Agent\sg\SysMonAgt.ini
Linux	<Installation path>/Agent/sg/SysMonAgt.ini

[Descriptions to be added]

```
[UpperNode]
Protocol=6                  ...1

[SelfNode]
SvcServerProtocol=6         ...2
```

[Parameter details]

	Key name	Description
1	Protocol	Specify the communication protocol for the manager to be connected. Operates as shown below depending on the specified value. 4: IPv4 communication only (default value) 6: IPv6 communication only 46: IPv4 and IPv6 communications combination (IPv4 overrides IPv6)
2	SvcServerProtocol	Specify the communication protocol for the command to connect to the agent. Operates as shown below depending on the specified value. 4: IPv4 communication only (default value) 6: IPv6 communication only 46: IPv4 and IPv6 communications combination (IPv4 overrides IPv6)

■ Manager

[File path]

Windows	<Installation path>\Manager\sg\SysMonMgr.ini
Linux	<Installation path>/Manager/sg/SysMonMgr.ini

[Descriptions to be added]

```
[SelfNode]
ServerProtocol=6            ...1
SvcServerProtocol=6         ...2
```

[Parameter details]

	Key name	Description

1	ServerProtocol	Specify the communication protocol to wait for the connection from the agent. Operates as shown below depending on the specified value. 4: IPv4 communication only (default value) 6: IPv6 communication only 46: IPv4 and IPv6 communications combination (IPv4 overrides IPv6)
2	SvcServerProtocol	Specify the communication protocol to wait the connection of a command to connect with the monitoring window, Web monitoring window and manager. Operates as shown below depending on the specified value. 4: IPv4 communication only (default value) 6: IPv6 communication only 46: IPv4 and IPv6 communications combination (IPv4 overrides IPv6)

■ Monitoring window

[File path]

Windows	<Installation path>\Svc\sg\SysMonSvc.ini

[Descriptions to be added]

```
[UpperNode]
Protocol=6                    ...1
```

[Parameter details]

	Key name	Description
1	Protocol	Specify the communication protocol to wait the connection from the agent. Operates as shown below depending on the specified value. 4: IPv4 communication only (default value) 6: IPv6 communication only 46: IPv4 and IPv6 communications combination (IPv4 overrides IPv6)

■ Web monitoring window

[File path]

Windows	<Installation path>\Manager\sg\HttpServerMgr.ini <Installation path>\Manager\Svc\Common\sg\SysMonSvc.ini
Linux	<Installation path>/Manager/sg/HttpServerMgr.ini <Installation path>/Manager/Svc/Common/sg/SysMonSvc.ini

[Descriptions to be added]

HttpServerMgr.ini

```
[SelfNode]
ServerProtocol=6              ...1
```

SysMonSvc.ini

```
[UpperNode]
Protocol=6                    ...2
```

[Parameter details]

	Key name	Description
1	ServerProtocol	Specify the communication protocol to wait for the connection from the Web monitoring window. Operates as shown below depending on the specified value. 4: IPv4 communication only (default value) 6: IPv6 communication only 46: IPv4 and IPv6 communications combination (IPv4 overrides IPv6)
2	Protocol	Specify the communication protocol to wait a command to connect with the monitoring window, Web monitoring window and manager. Operates as shown below depending on the specified value. 4: IPv4 communication only (default value) 6: IPv6 communication only 46: IPv4 and IPv6 communications combination (IPv4 overrides IPv6)

8.4.2. Example of Protocol Settings

Setting example 1

When using IPv4 and IPv6 communications combination for all inter-function communications

■ Agent

<Installation path>\Agent\sg\SysMonAgt.ini

```
[UpperNode]
Protocol=46

[SelfNode]
SvcServerProtocol=46
```

■ Manager

<Installation path>\Manager\sg\SysMonMgr.ini

```
[SelfNode]
ServerProtocol=46
SvcServerProtocol=46
```

■ Monitoring window

<Installation path>\Svc\sg\SysMonSvc.ini

```
[UpperNode]
Protocol=46
```

■ Web monitoring window

<Installation path>\Manager\sg\HttpServerMgr.ini

```
[SelfNode]
ServerProtocol=46
```

<Installation path>\Manager\Svc\Common\sg\SysMonSvc.ini

```
[UpperNode]
Protocol=46
```

Setting example 2

When using IPv6 for communications between the monitoring window and manager, and IPv4 for other inter-function communications

■ Manager

<Installation path>\Manager\sg\SysMonMgr.ini

```
[SelfNode]
ServerProtocol=6
SvcServerProtocol=6
```

■ Monitoring window

<Installation path>\Svc\sg\SysMonSvc.ini

```
[UpperNode]
Protocol=6
```

8.5. Operating mode of the application monitoring functions

The application monitoring function allows you to select either 32-bit or 64-bit mode as the operating mode for each monitoring application. When monitoring a 32-bit application, select 32-bit mode; when monitoring a 64-bit application, select 64-bit mode.

- 32-bit mode
  On both 32-bit and 64-bit OSs, a 32-bit agent process monitors 32-bit and 64-bit applications by using a 32-bit middleware library and 32-bit JDK/JRE.

  Monitoring image

  To monitor a 64-bit application, use 64-bit mode.
  When upgrading this product from Application Navigator version 4.1.1 or earlier (in 32-bit mode), monitoring in 32-bit mode can continue by using the installed 32-bit middleware and 32-bit

JDK/JRE.

64-bit mode
On a 64-bit OS, a 32-bit agent process and 64-bit child process monitor 64-bit applications by using a 64-bit middleware library and 64-bit JDK/JRE.

Monitoring image

For how to switch the operating mode, refer to the following sections of Product Help Manual.

[Monitor applications]
[Changing the operating mode]

8.6. Configuring managers in a hierarchy

8.6.1. Outline

Multiple managers can be linked in layers, and the upper manager can monitor the messages and performance information collected by lower managers. In addition, lower manager commands can be executed from the upper manager.

When using Message linking and Command linking in a hierarchical configuration of managers, purchase the license for implementing managers in a hierarchy and register the license to the upper manager.

◆ Message linking
Message linking enables messages generated on a lower manager to be reported the upper manager and monitored on the business view of the upper manager.

For details about how to set up command linking, see the following chapters in the manual or in Help.
[Linking with other managers]
-[Linking between managers]

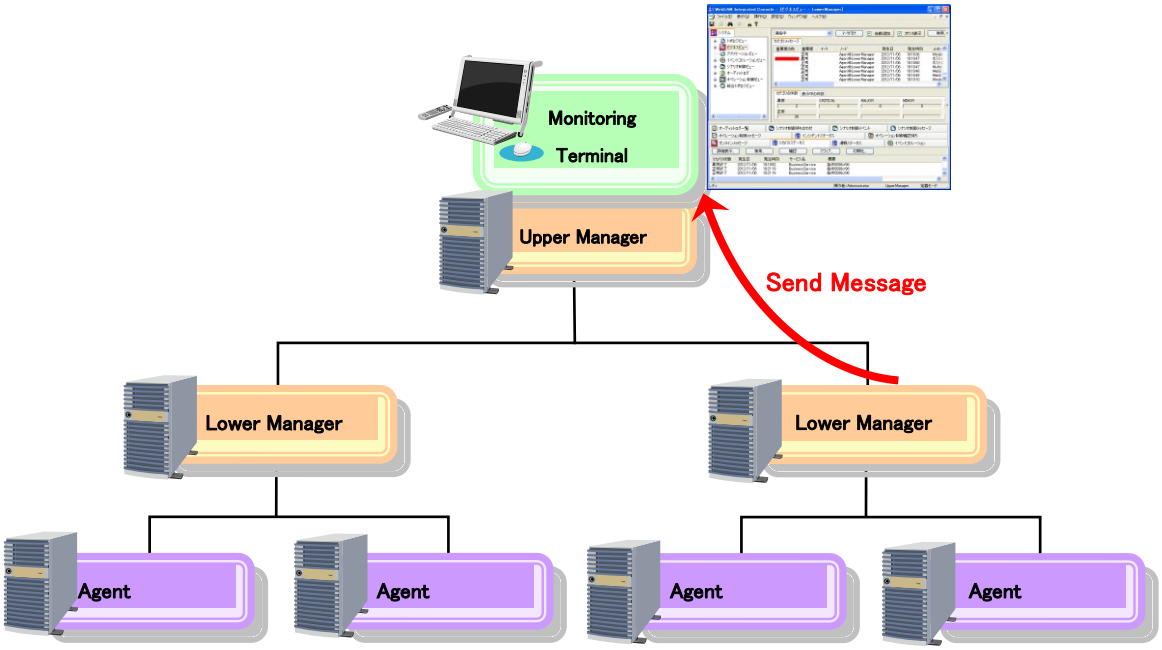


Figure 8-1　Message reporting by managers in a hierarchical configuration

◆　Command linking

The commands of lower managers or the agents under the lower managers can be executed from the upper manager.

For details about how to set up command linking, see the following chapters in the manual or in Help.

[Linking with other managers]

-[Setting up recovery linking with lower managers]

-[Setting up command linking]

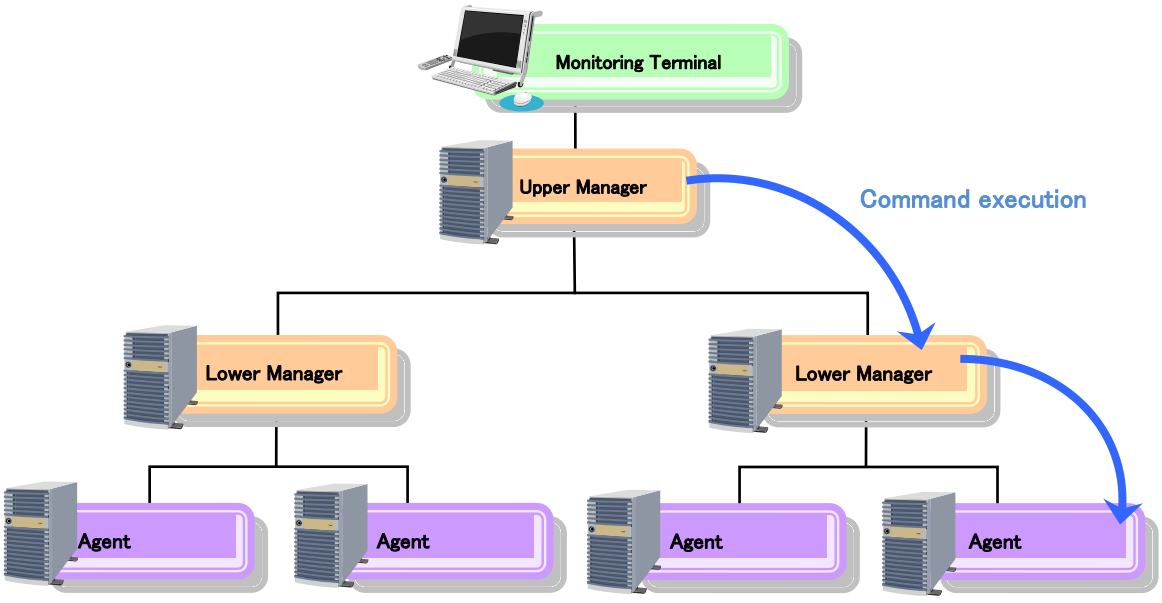


Figure 8-2　Command execution by managers in a hierarchical configuration

◆ Multi graph view and print view

The counters retained by lower managers can be specified in the multi graph view and print view of the upper manager. The performance information of the specified counter can be accumulated on the lower manager and a graph indicating that information can be displayed on the multi graph view of the upper manager or printed out from the print view of the upper manager.

For details about how to set up multi graph view and print view, see the following chapters in the manual or in Help.

[Use Multi-graph View]

- [Define a performance statistics graph]
  - [Define a performance statistical counter]

[Output a report]

-[Creating a print definition]

-[Report item settings]

-[Output data settings]

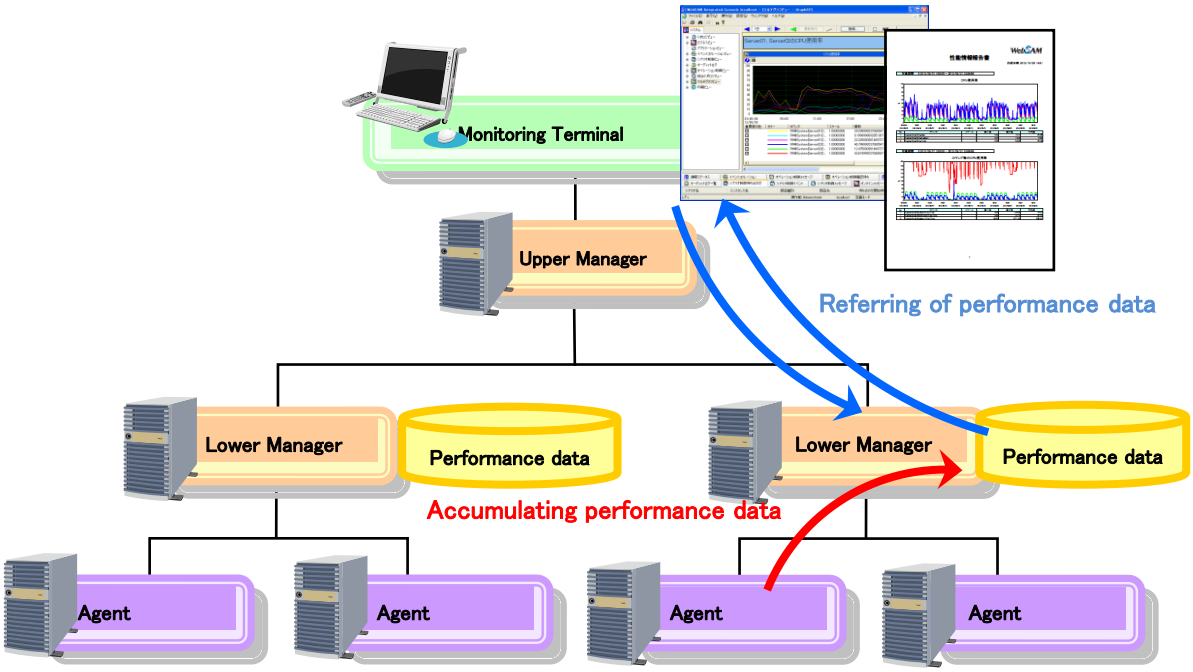


Figure 8-3　Multi graph and print views of managers in a hierarchical configuration

◆ Scenario control

A scenario of a lower manager can be executed by the upper manager by specifying the scenario of the lower manager as an scenario execution component on the upper manager.

This function is provided as an option. To use this function, purchase a scenario control function license. The license must be applied to both the upper and lower managers.

For details about how to set up scenario control, see the following chapters in the manual or in Help.

[Using the scenario control]
 -[Define a scenario]
  -[Create and save a scenario]
   -[Define actions by allocating parts]
    -[Allocate a part to execute a scenario]

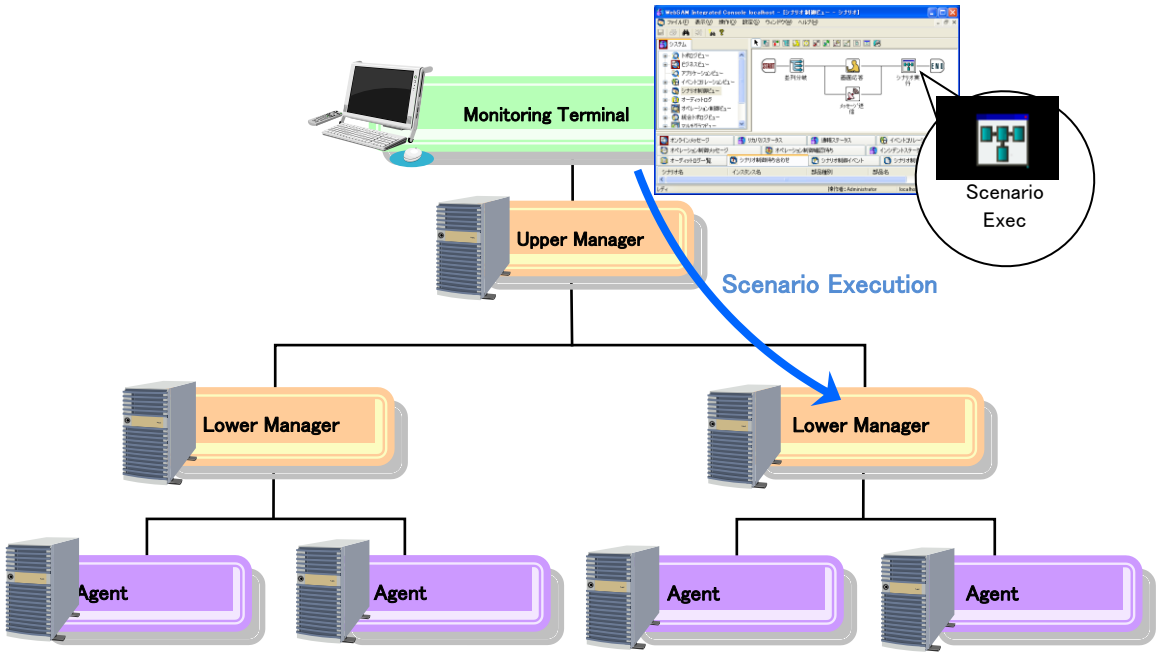


Figure 8-4　Scenario control performed by managers in a hierarchical configuration

8.6.2. Setting procedure

This section describes how to set up managers in a hierarchical configuration.
It is assumed that the upper and lower managers are already installed.

● Setting up the lower managers

Specify the following settings for the lower manager to enable linking with the upper manager.
Note that this setting procedure is not required when using only message linking and command linking.

Notes

To use lower managers in a cluster environment, perform specify the settings for both the active and standby nodes.

Procedure

1. Open the following file using a text editor.
   Windows:　<Installation directory>\Manager\sg\SysMonMgr.ini
   UNIX:　　<Installation directory>/Manager/sg/SysMonMgr.ini

2. Add the following description.

```
[UpperNode]
HostName=Upper manager host name
ServerPort=Port number

[ServiceModule000]
ModuleNo=Number of functions to link
ModuleXXX=Function to link
```

- Upper manager host name:
  Specify the name of the host in which the upper manager is installed.
  * Specify a resolvable name (or IP address).
  * Specify a virtual host name if the upper manager is in a cluster environment.

- Port number:
  Specify the [Agent port] that was specified when the upper manager was installed.
  * This is 12520 if the default value was used during installation. If you do not know the value of [Agent port], check the value of ServerPort in the [SelfNode] section of following file in the upper manager.
  Windows: <Installation directory>\Manager\sg\SysMonMgr.ini
  UNIX: <Installation directory>/Manager/sg/SysMonMgr.ini
  Example
  [SelfNode]
  HostName=xxxxxxxx
  ServerPort=12520 → Port for communicating with the agent (Agent port)

- Number of functions to link:
  Specify the number of functions to be linked.
  Add as many ModuleXXX lines as the specified number of functions.

- ModuleXXX:
  Add as many lines as the specified number of functions to link.
  Specify ascending sequential numbers for XXX, starting from 001 (e.g., “Module001”).
  Example
  [ServiceModule000]
  ModuleNo=2
  Module001=PerfStatisticsMgr.dll
  Module002=WorkflowMgr.dll

- Function to link:
  Specify the function to be linked with the upper manager. The values shown below can be specified.

Function to be linked	Value to specify
Multi graph view and print view	PerfStatisticsMgr.dll
Scenario control	WorkflowMgr.dll

3. Restart the lower manager.

This concludes the setup.
Perform the relevant definitions for each function, referring to the MCOperations manual or Help.

Whether or not the connection with the lower manager is established correctly can be checked from the MCOperations console of the upper manager.Check the connection as described below.

- For multi graph view and print view

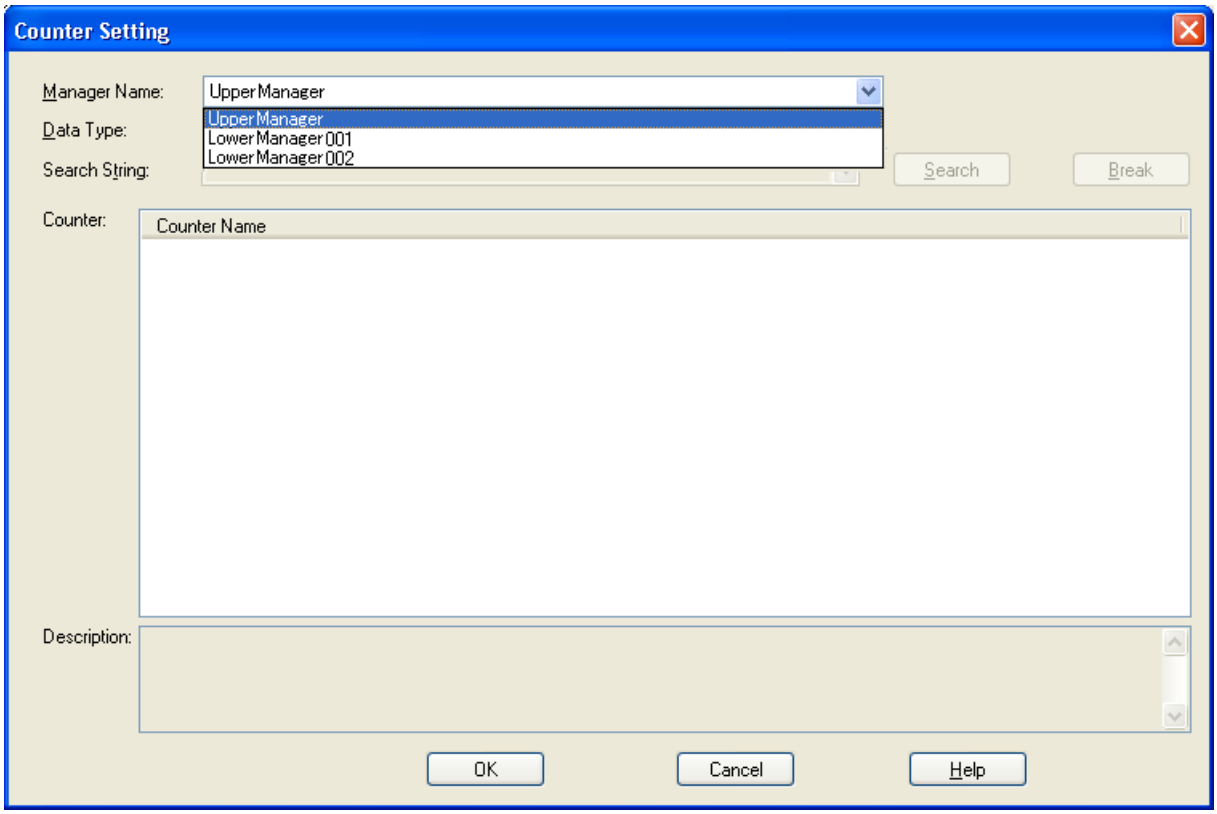


Figure 8-5 Multi graph view [Counter Setting] dialog box

If the self host name (Self hostname) of the lower manager is displayed as a manager name in the [Counter Setting] dialog box, the connection is established correctly.
For details about the [Counter Setting] dialog box, see the following pages in the MCOperations manual or in Help.

[Use Multi-graph View]
- [Define a performance statistics graph]
  - [Define a performance statistical counter]

[Output a report]
-[Creating a print definition]
  -[Report item settings]
    -[Output data settings]
      -[Multi graph view]

◆ For scenario control

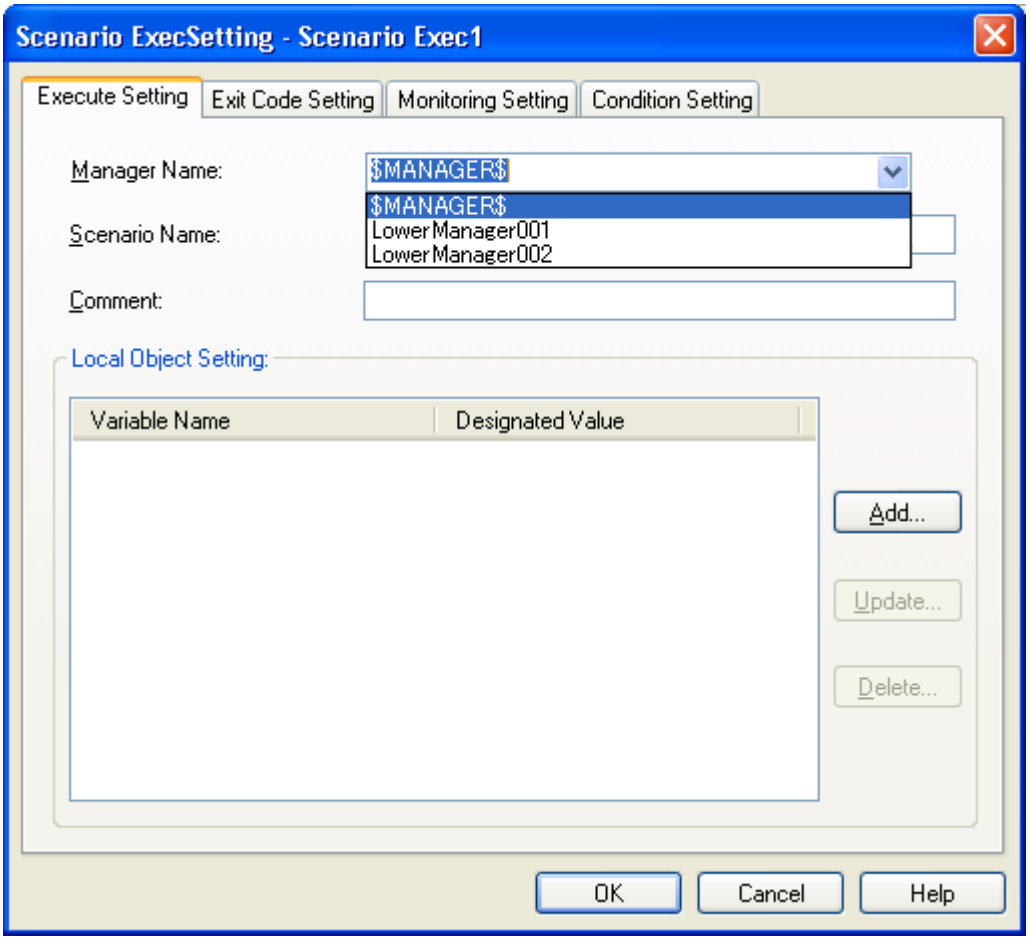


Figure 8-6 Scenario control [Execute Setting] dialog box

Add a scenario execution component to the [Edit Definition] dialog box, right click the component and select [Properties] from the pop-up menu to display the [Scenario ExecuteSetting] dialog box.If the self host name (Self hostname) of the lower manager is displayed as a target manager name on the [Execute Setting] tab in the [Scenario ExecuteSetting] dialog box, the connection is established correctly.

For details about the [Scenario ExecuteSetting] dialog box, see the following pages in the MCOperations manual or in Help.

[Using the scenario control]
-[Define a scenario]
-[Create and save a scenario]
-[Define actions by allocating parts]
-[Allocate a part to execute a scenario]

8.6.3. Notes on manager hierarchies

● Self host names of upper and lower managers

The self host names (Self hostname) specified when installing an upper manager or lower manager must be unique within the system.

When using managers in a cluster environment, the self host names of the active and standby nodes must be the same.

If the self host name of the lower manager is changed, the definition information held by the upper manager will not be changed automatically. This information needs to be specified again manually.

● Notes on scenario control function

For details and notes about the scenario execution components, see the following chapters in the manual or in Help.
[Using the scenario control]
-[Define a scenario]
  -[Scenario control parts]
    -[Scenario Exec]

8.6.4. Restrictions on manager hierarchies

● Restrictions on multi graph view

◆ Disconnecting a lower manager while saving a definition
If communication with the lower manager specified in the multi graph view definition is disconnected while saving a multi graph view definition on the upper manager, the definition may be incomplete. Delete the counter retained by the lower manager disconnected from the graph, and register the definition again.

For the method of storing the definitions, see the following chapters in the manual or in Help.
[Use Multi-graph View]
  -[Use the multi-graph view window]
    -[Description of the operation mode of multi-graph view window]

For the method of counter setting, see the following in the manual.
[Use Multi-graph View]
  -[Defining the performance statistical graph]
    -[Defining the performance statistical counter]

● Restrictions on print view

The following restrictions apply when multi graph view is specified for “Data type” in the upper manager print view.

◆ Disconnecting a lower manager while saving a definition

If communication with the lower manager specified in the print view definition is disconnected while saving the print view definition on the upper manager, updating the definition fails. Delete the counter in question in the [Graph Setting for Print] dialog box, and register the definition again.

For details about the setting dialog box, see the following chapters in the manual or in Help.
[Output a report]
-[Creating a print definition]
-[Report item settings]
-[Output data settings]
-[Multi graph view]

◆ Specifying counters by using regular expressions

If counters of lower managers are specified by using a regular expression, only the counters that matched the search string when counters were added to the print definition will be printed. To collect counters that matched the search string by using the performance monitoring function, etc., delete the counters using the [Delete] button in the [Graph Setting for Print] dialog box and specify them again.

For details about the setting dialog box, see the following chapters in the manual or in Help.
[Output a report]
-[Creating a print definition]
-[Report item settings]
-[Output data settings]
-[Multi graph view]

8.6.5. Restrictions on the print view

There are the following restrictions when [MultiGraphView] is set to [Data Kind] on the print view of the upper-level manager.

◆ Disconnecting the lower-level manager while the definition is being saved

While the definition of the print view is being saved on the upper-level manager, if communication with the lower-level manager that is specified in the definition is disconnected, updating the definition fails. In this case, delete the corresponding counter from the [Graph setting for Print] screen and then register the definition again.

For details of the setting screen, see the following chapters in the manual or in Help.
[Output a report]
-[Creating a print definition]
-[Report item settings]
-[Output data settings]

-[Multi graph view]

◆ Specifying a counter in regular expression

When a counter of the lower-level manager is specified in regular expression and it is added to the print definition, only the counter that matches the search string is to be output. When counters that match the search string are set to be collected newly by the function such as performance monitoring, delete the counters by clicking the [Delete] button on the [Graph setting for Print] screen and make the setting again.

For details of the setting screen, see the following chapters in the manual or in Help.
[Output a report]
-[Creating a print definition]
-[Report item settings]
-[Output data settings]
-[Multi graph view]

8.7. WebConsole

To use WebConsole, perform the environment setting after the installation as described below:
WebSAM SystemManager G 7.1 WebConsole Option Environment Configuration Guide

9. Notes

9.1. License

9.1.1. License Registration Task

The license agreement for each function used by this product is verified by using the license management function. After installing the product, basic functions can be used for 3 months based on the trial version license. Thereafter, an official license needs to be registered to use the product. Use the following procedure to register an official license:

1. Register the Product Code and License Key. Obtain a Request Code in the monitoring view.
   *The license key is described in the "Code Word Application Form" included with the product.

2. Refer to the "Code Word Application Form" included in the media, and apply for your Code Word.

3. Register the obtained Code Word.

4. Restart the manager. *If it is needed.

*Only when registering a manager or a manager option license, manager's restart is needed.

If the manager is configured in a duplex environment, you need to register the license to each of a pair of the managers as you fail over to the active manager and to the standby one.

For details, refer to the following sections in the Product Help Manual.
[Manage the licenses]

9.1.2. Trial Version License

After installation, the trial version licenses of all the SystemManager G products will be set up. In the valid state of the license, the corresponding menu will also be valid. Once you have registered the official license(s) of your product(s), delete the trial license(s) (product model number: SysMgrG-Trial). Note that before deleting the trial license, you must delete the corresponding monitoring settings of the trial-licensed product. After deleting the license, the settings cannot be undone.

A list of trial licenses is shown below.

License name	Number of Licenses
WebSAM SystemManager G : IT Resource Monitor[DNS]	1
WebSAM SystemManager G : IT Resource Monitor[FTP]	1

WebSAM SystemManager G : IT Resource Monitor[TCP]	1
WebSAM SystemManager G : IT Resource Monitor[Web Scenario]	5
WebSAM SystemManager G : IT Resource Monitor[mail]	1
WebSAM SystemManager G : Agent[UNIX]	5
WebSAM SystemManager G : Agent[Windows/Linux]	5
WebSAM SystemManager G : Agent[Apache][Windows/Linux]	5
WebSAM SystemManager G : Agent[IIS][Windows]	5
WebSAM SystemManager G : Agent[JavaAP][UNIX]	5
WebSAM SystemManager G : Agent[JavaAP][Windows/Linux]	5
WebSAM SystemManager G : Agent[Oracle][UNIX]	5
WebSAM SystemManager G : Agent[Oracle][Windows/Linux]	5
WebSAM SystemManager G : Agent[SAP][Windows]	5
WebSAM SystemManager G : Agent[SQLServer][Windows]	5
WebSAM SystemManager G : Agent[Tomcat][UNIX]	5
WebSAM SystemManager G : Agent[Tomcat][Windows/Linux]	5
WebSAM SystemManager G : Agent[WebLogicServer][UNIX]	5
WebSAM SystemManager G : Agent[WebLogicServer][Windows/Linux]	5
WebSAM SystemManager G : Agent[WebSphere][UNIX]	5
WebSAM SystemManager G : Agent[WebSphere][Windows/Linux]	5
WebSAM SystemManager G : Console	1
WebSAM SystemManager G : Manager	1

9.1.3. Application Management Host Settings

When an agent has been added to the monitored hosts from the [Unregistered Host] group, you must select the agent host that will be monitored for each application in [Application Host Setting].

9.2. Installation

9.2.1. Service Setup in Additional Overwrite Installation

If other products (NetvisorPro) are additionally installed in the same installation directory, or if SystemManager G has been installed by overwriting, service settings will be reinitialized. Specifically, in Windows, the service start-up type will be returned to “Automatic”, and in UNIX, the rc script will be re-registered. If service settings had been changed from the defaults in a cluster environment, etc., perform the settings again.

9.2.2. Files not Updated in Overwrite Installation

Setting files are generated and populated with initial values in new installations. On the other hand, to maintain existing settings if upgrading or performing overwrite installation on the version of the existing installation environment, user customizable files will not be overwritten. The following shows the settings that are not updated:

Function	Windows	UNIX
Manager	Business View filter settings	
	<Installation directory>\Manager\sg: AppNaviMgr.ini EventLogHelperMgr.ini SysLogHelperMgr.ini	<Installation directory>/Manager/sg: AppNaviMgr.ini EventLogHelperMgr.ini SysLogHelperMgr.ini
Agent	<Installation directory>\Agent\sg: CollectorApache.ini CollectorExchsrvr.ini CollectorJavaAP.ini CollectorOracle.ini CollectorSAP.ini CollectorTomcat.ini CollectorWebLogic.ini CollectorWebSphere.ini CollectorProxy64.ini ApLogHelperAgt.ini EventLogBaseAgt.ini EventLogHelperAgt.ini MessageAgt.ini	<Installation directory>/Agent/sg: CollectorApache.ini CollectorJavaAP.ini CollecotrOracle.ini CollectorSAP.ini CollectorTomcat.ini CollectorWebLogic.ini CollectorWebSphere.ini CollectorProxy64.ini ApLogHelperAgt.ini MessageAgt.ini PlatformTool.ini SysLogBaseAgt.ini SysLogHelperAgt.ini <Installation directory>/Agent/bin: config

The following files are updated to the latest versions at installation. Any customized files should therefore be saved under different names.

- Knowledge files
- SG templates
- Collector.ini
- CollectorObject.ini

9.2.3. Installation Directory for Windows 64-bit Environment

The Windows default installation directory is <System drive>\Program Files\NEC\UMF\Operations. The 64-bit OS will be installed in <System drive>\Program Files (x86)\NEC\UMF\Operations.

9.2.4. Notes on reinstallation

When the manager function of this product is reinstalled, it is necessary to apply for a code word again. Reapplying for a code word is not required for cases other than reinstallation.
When data is restored from a backup after reinstallation, it is also necessary to apply for a code word again.

9.3. UnInstallation

9.3.1. When patches are applied

If a patch has been applied, delete the following directory before uninstalling the product.

UNIX
<Installation path>/<Function>/patch/
Example:
For a manager:
<Manager installation path>/Manager/patch/

Windows
<Installation path>\Patch\<Name of Patch>\<Function>
(Multiple deletions are required when multiple patches are applied.)
Example
For a agent.
<Agent Installation path>\Patch\NECfw234\Agent

Apply the patch again once the product has been reinstalled.

9.3.2. Before Uninstall

9.3.2.1. Delete Monitoring Definition

Before uninstalling the agent, be sure to delete all monitoring definitions of the agent on the topology view.
Note that monitoring definitions can be deleted only when the relevant agent is connected to the manager.

9.4. Version Upgrade

9.4.1. Version Upgrade for a Part of Function

When upgrading a version, be sure to upgrade the versions of the manager and all monitoring terminals. It is not possible to only upgrade versions of the agents. It is possible to manage old version agents with new version managers, but this is limited to only those functions within the scope of the old version. It is recommended that the agent version be upgraded at the same time.

*When using the Service availability monitoring, upgrade and/or downgrade the console, manager, and probe to the same version before starting the monitoring. Previous versions of probes cannot be managed with a new version of manager.

*In the hierarchical structure, managers are supported only when the version of the upper-level manager is higher.

9.4.2. Upgrading Version from MasterScope Application Navigator

9.4.2.1. Oracle Monitoring Agent Version Upgrade

To upgrade an Application Navigator Ver4.0.0 or older agent that is performing Oracle monitoring, the users, tables, and stored procedures dedicated to SystemManager G must be registered to the monitored DB by executing the setup script as described in the table below.

Procedure for running setup script

Version of your Application Navigator	Monitored Oracle version		
	10g	11g	12c
Before v3.2.0	Not supported	Procedure A	Not supported
v3.2.1	Not supported	Procedure A	Not supported
v3.2.2 - v3.3.3	Not supported	Procedure A	Not supported
v4.0.0	Not supported	Procedure B (*1)	Not supported
v4.1.0 or later	Not supported	No operation needed	No operation needed

(*1) If you have not run the setup script in v4.0.0 (perform monitoring with the sys user), perform not procedure C but procedure A.

For information on how to execute the setup script and cleanup script, see the following sections in the Product Help Manual.

[Monitor applications]
[Monitor Oracle]
[Preparations for Oracle performance monitoring]
[DB setting when monitoring Oracle]

Procedure A

In this version, you must register users, tables, and stored procedures dedicated to Application Navigator to the monitored DB for monitoring Oracle. Run the setup script.

Procedure B

In this version, you must register users, tables, and stored procedures dedicated to Application Navigator to the monitored DB for monitoring Oracle. If you created users dedicated to Application Navigator by running the setup script in a previous version, you must remove the users temporarily and then run the setup script for this version again. Run the cleanup script and setup script by following the steps below.

(1) Stop the agent service(s)

(2) Run the cleanup script (OracleCleanup.sql)
(3) Install the upgraded version of Application Navigator
(4) Run the setup script (OracleSetup.sql)
(5) Start the agent service(s)

Note that as to parameters such as user names and passwords that you enter in step (4), you must specify the same as those specified prior to version upgrading.

In addition, change the user to connect to the DB after performing procedures A, B and C as described below.

[Steps]
1. In the monitor window, right-click the agent node that is monitoring Oracle, and select [Oracle] from the [Edit Application Management Instance] menu. The [Oracle Monitor - Instance Setting] dialog is displayed.

2. Select a desired instance and click the [Edit] button to display the [Edit Instance] dialog. Change the user name and password to those for the user dedicated to Application Navigator you have created by the setup script, and click the [OK] button.

* If you are using OS authentication, you can omit these steps.
* If you were using a SYS user in a previous version, you can continue to monitor Oracle without changing the user.

9.4.2.2. Upgrading Version from Ver1.x

The resources used by the products have been changed from Ver1.2 to Ver2.0. Please take note. If Ver2.0 or later is installed by overwriting Ver1.x, the Ver1.x resources will be retained (*with some exceptions). If re-installed, the resources will be those of Ver2.0 or later. Note that Ver2.0 or later documents are based on Ver2.0 or later resources. If Ver1.x resources are retained by an overwriting installation, reread such documents where appropriate.

- Installation path

Function	Ver1.x	Ver2.0 or later
Monitoring terminal	\Program Files\NEC\ ApplicationNavigator\Svc	\Program Files\NEC\ UMF\Operations\Svc
Manager (Windows)	\Program Files\NEC\ ApplicationNavigator\Manager	\Program Files\NEC\ UMF\Operations\Manager
Agent (Windows)	\Program Files\NEC\ ApplicationNavigator\Agent	\Program Files\NEC\ UMF\Operations\Agent
Manager (UNIX)	/opt/ApplicationNavigator/Manager	/opt/UMF/Operations/Manager
Agent (UNIX)	/opt/ApplicationNavigator/Agent	/opt/UMF/Operations/Agent

- Port number

Communication path	Ver1.x	Ver2.0 - 3.0	Ver3.0.1 or later

Between manager and agent	12505	12520	12520
Between manager and monitoring terminal	12506	12521	12521
In own agent station	-	12591-12593	12570-12589

*The port number used by service availability monitoring is the same as the agent.

- Service name/rc script

Function	Ver1.x	Ver2.0 or later
Manager (Windows)	Application Navigator Manager	(MasterScope) UMF Operations Manager__*identifier*_n (Note 1)
Agent (Windows)	Application Navigator Agent	(MasterScope) UMF Operations Agent__*identifier*_n (Note 1)
Manager (UNIX)	AppNaviMgr	UMFOperationsManager__*identifier*_n (Note 1)
Agent (UNIX)	AppNaviAgt	UMFOperationsAgent__*identifier*_n (Note 1)

(Note 1) __*identifier* (—*identifier* on Solaris) is used when identifier was specified during installation. However, when the identifier is added to the existing service, the service name and rc file name will not be reflected.
Where n stands for a service number. For details, refer to "MasterScope Media Release Notes."

- Monitoring terminal window title*

Function	Ver1.x	Ver2.0 or later
Monitoring terminal	Application Navigator	(MasterScope) Integrated Console

*The window title will show Ver2.0 or later after upgrading any earlier version.

- Messages

Function	Ver1.x	Ver2.0 or later
Default Filter Definition*1	- [Application Navigator] category Generated product messages and messages hit to Windows knowledge are saved collectively in this category.	- [OS] category group Messages hit to Windows knowledge are saved in the [Windows] category. - Product messages are classified into categories by function under the [Unified Management Framework] category group.
[Message attribute] category *2	Application Navigator	Unified Management Framework
[Message attribute] Application *2	Application Navigator	Unified Management Framework

*1 The default filter definition is retained in version upgrade, but remains as that in Ver1.x.
To display added messages in Ver2.0 or later in Business View, add additional filter settings by referring to the message list in the "Messages output by Manager/Agents" in the help.

*2 The category and application attributes of output messages are Ver2.0 or later values after version upgrade. The Ver1.x default filter definition has Ver1.x categories and applications. When combining with the Ver1.x default filter definition, product messages will not be displayed in Business View. Perform "9.4.2.3. Filter Definition Migration from Ver1.x."

9.4.2.3. Filter Definition Migration from Ver1.x

As described in "9.4.2.2. Upgrading Version from Ver1.x", some attribute data (categories, applications) of messages output by Application Navigator are changed. There is a need to return output message attributes to those in Ver1.x or change filter definitions.

(1) Changing message attributes to those in Ver1.x
If you intend to operate Application Navigator only, independently of MISSION CRITICAL OPERATIONS, SystemManager, and NetvisorPro, in the same installation directory, or without any plan to use these programs in the future, assign Application Navigator specific names to the message attributes so that the filter definitions in Ver1.x can be used as they are.
If using any other product, proceed to “(2) Changing the message filter”.

To change message attributes to those in Ver1.x, perform the following settings and restart the service.

- Setting files to be edited

[Windows]
C:\Program Files\NEC\ApplicationNavigator\Manager\sg\SysMonMgr.ini (manager)
C:\Program Files\NEC\ApplicationNavigator\Agent\sg\SysMonAgt.ini (agent)
[UNIX]
/opt/ApplicationNavigator/Manager/sg/SysMonMgr.ini (manager)
/opt/ApplicationNavigator/Agent/sg/SysMonAgt.ini (agent)

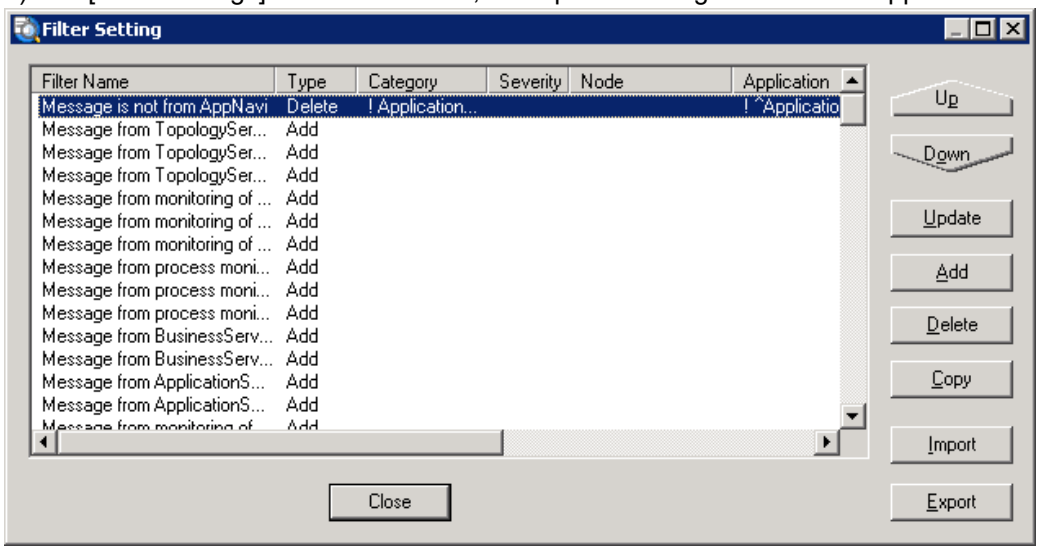
- Editing example (Add the following description to the end)

```
[Event]
ApplicationName=Application Navigator
EventCategory=Application Navigator
```

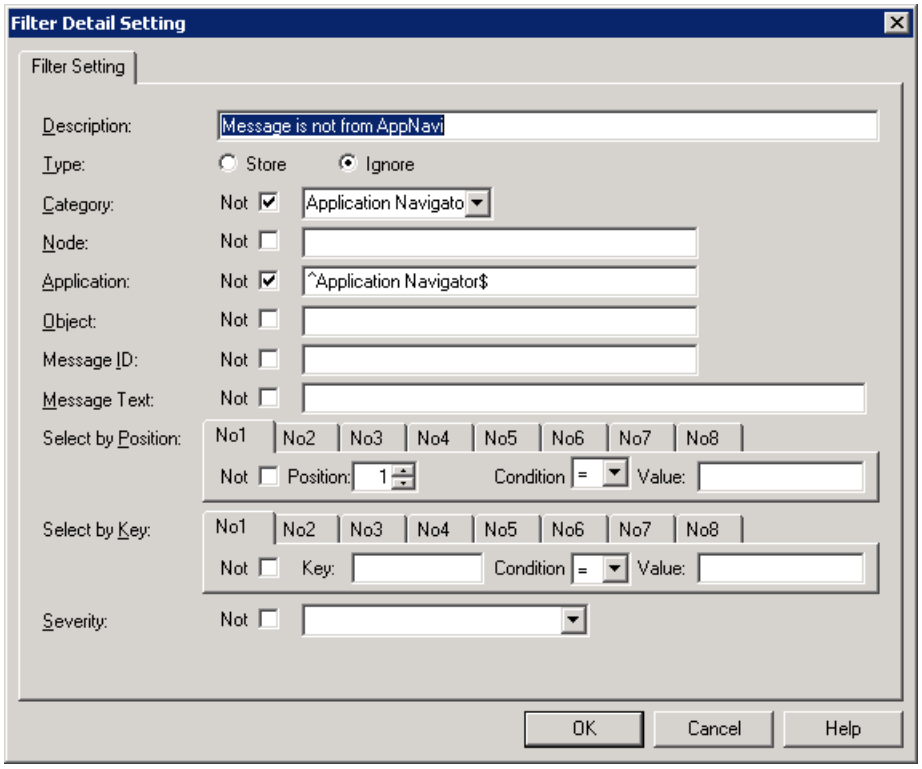
(2) Changing the message filter
Even if using the Ver1.x default filter definition (Application Navigator category) as it is, you must still modify the filter definition.

The following shows how to change the message filter, using Application Navigator Ver1.2 default filter settings as an example:

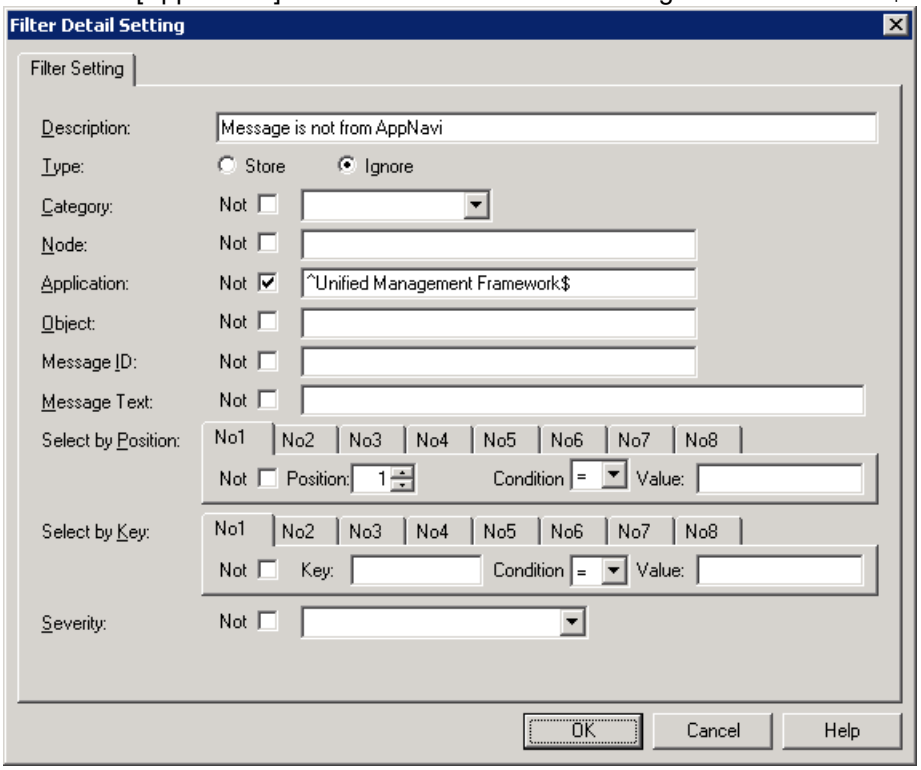
1) Call [Filter Settings] in Business View, and open “Messages other than Application Navigator”.



2) The [Filter Item Setting] window for "Messages other than Application Navigator" opens



3) Delete the [Not] definition for [Category].
Revise the [Application] definition to read “Unified Management Framework$”.



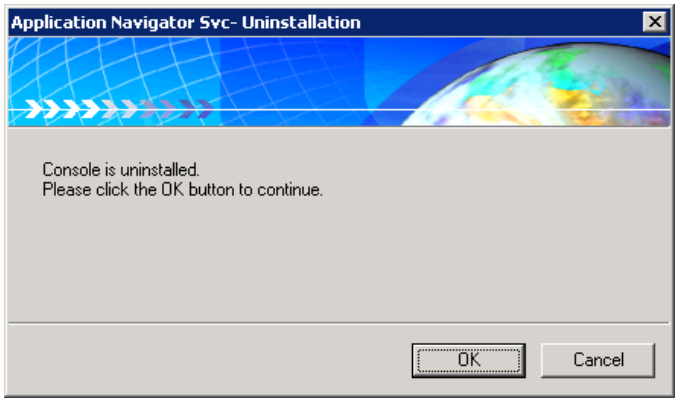
Be careful when the versions of some agents are not upgraded and, as a result, Ver1.x and Ver2.0 or later agents mix under the manager. Messages are generated in the message attribute of each version and gather in the manager. In this case, change the [Not] definition in [Application] to “^Unified

Management Framework$|^Application Navigator$" or a regular expression that supports both versions.

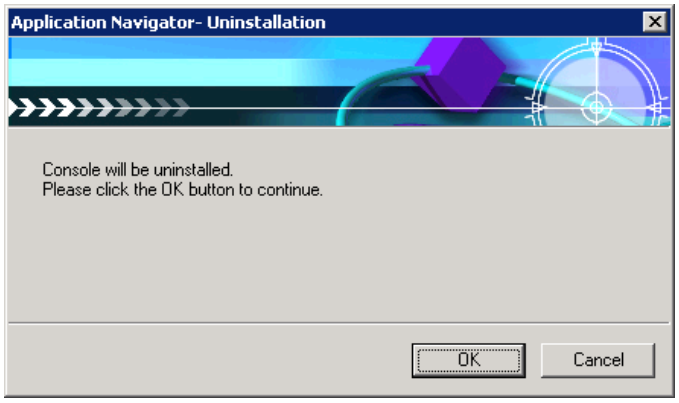
9.4.2.4. Uninstalling a Version Upgrade Environment from Ver1.x

If multiple entries of "Application Navigator" are displayed in the [Add/Delete Applications] window when uninstalling an environment that was upgraded from Ver1.x to Ver2.0 or later, uninstall them as follows:

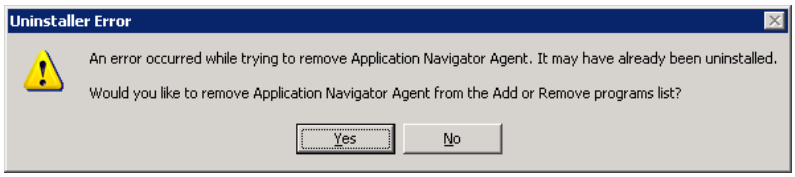
1) First, run the Ver2.0 or later uninstaller. As the uninstaller cannot be recognized in the list window, run "Modify and Delete" and wait for the confirmation dialog to be displayed. The following window shows the Ver2.0 or later uninstaller. If not the desired one, select [Cancel] and run another entry.



2) Next, run the ver1.x uninstaller for the remaining items. The following window shows the Ver1.x uninstaller.



If "Deletion Error" occurs, select [YES] to delete it from the program list.



If Ver2.x cannot be reinstalled in the opposite order of these steps, delete the following registry keys:
Monitoring terminal:
HKEY_LOCAL_MACHINE\SOFTWARE\NEC\UMFSetup\Common\Svc
Manager:

HKEY_LOCAL_MACHINE\SOFTWARE\NEC\UMFSetup\Common\Manager
Agent:
HKEY_LOCAL_MACHINE\SOFTWARE\NEC\UMFSetup\Common\Agent

9.4.2.5. Upgrading Version from Ver3.0.1

The libraries used by the SAP monitoring function have been changed from Ver3.0.1 to Ver3.0.2. If you are using the SAP monitoring function in Ver3.0.1, you must acquire the libraries separately when upgrading the version to Ver3.0.2. For more information, refer to “Perform preparations for SAP monitoring”.

9.4.2.6. Upgrading Version from Ver3.0.2

Since Ver3.1, the logical view is displayed directly under the Application Monitor on the tree view of the console. As the user management function has been added since Ver3.1, remove the reference privilege to the logical view by referring to the following if you want to hide the view:

[Perform User Management]
[Manage group information]
[Configuring authority]
[Application Monitor]

9.4.2.7. Version Upgrading Cluster Monitoring Agent before Ver3.0.2

Ver3.1 or later has supported logical system agents, and switched monitoring agents on a cluster system to logical system agents. The versions before Ver3.0.2 customize the regular agents to use them. If you disabled event log and system log monitoring by editing Agent\sg\SysMonAgt.ini, the customized items will be restored by installing and upgrading the regular agent.

1) Stop the agent
2) Version upgrade installation
3) Disable event log and system log monitoring
4) Start the agent

For information on the disabling step, refer to the Cluster Setup Guide for the previous version.

9.4.2.8. Upgrading Version from Ver3.2.1 or Earlier Versions

For information on version upgrading from Ver3.2.1 or earlier versions, refer to the following note.

- 9.5.6. About the Default Value of Data Acquisition Method for UNIX Agent Performance Data

9.4.2.9. Version Upgrade to Ver4.0.1 or Later for Agent

In Ver4.0.1 or later, the default values for some parameters of monitoring timeout and the number of threads have been changed to make the operation of each monitoring agent more recognizable.

The following lists the versions to be upgraded:

Monitoring Function	Version	Agent type
Oracle	v3.2.0 - v4.0.0	Normal / Remote monitor
SQL Server	v3.2.0 - v4.0.0	Normal / Remote monitor
WebLogic Server	v3.3.1 - v4.0.0	Remote monitor
SAP	v3.2.0 - v4.0.0	Normal
JavaAP	v3.3.2 - v4.0.0	Normal
WebSphere	v4.0.0	Normal

The following lists the parameters to be changed for application monitoring:

Section	Key	Monitoring function	v4.0.0 or earlier default	v4.0.1 or later default
[Config]	MonitoringTimeout	Oracle SQL Server	60	0
		WebLogic Server JavaAP WebSphere	180	
	MonitoringTimeoutMessage	Oracle SQL Server WebLogic Server JavaAP WebSphere	0	1
	MaxThreadsExcessMessage			
	CollectingTimeoutMessage	Oracle SQL Server	0	1
	SkipMessage	Oracle SQL Server WebLogic Server JavaAP WebSphere	0	1
[Performance] [SAPsyslog] [SAPalert]	SkipMessage	SAP	0	1
	TimeOutMessage			

The following describes impacts from changing the default values:

- When the parameters have been set
  After upgrading to V4.0.1 or later, the parameter settings will be kept intact.
  The application monitoring operates according to the specified parameters, without any impacts from version upgrading.

- When the parameters have not been set
  After upgrading to V4.0.1 or later, each of the default values for the parameters brings a different operation.

"MonitoringTimeout" does not cause a timeout event because its operation has been changed from timeout to waiting for a response from a monitored object.
The message output parameter outputs a message when an occurrence condition becomes true. The occurrence of an event can be confirmed in the business view. A skip message, timeout message, and threads excess massage do not mean any Application Navigator failure. They inform users that a response from an application that is being monitored is delayed.

9.4.2.10. Upgrading the agent from version 4.1.0.2

To upgrade a Ver4.1.0.2 agent in which the LogicalDisk object in performance monitoring is specified to be monitored to Ver4.1.1 or later in a Red Hat Enterprise Linux 7 environment, perform the following procedure:

1. Save LogicalDisk.dat under <Agent installation directory(*1)>/Agent/sg/PerformanceDefault/10.1.5 to another directory.
2. Stop the agent service.
3. Upgrade the agent.
4. Overwrite the original directory with the saved LogicalDisk.dat.
5. Start the agent service.

(*1) For the logical agent, use the path specified for [Data area folder], which can be defined at installation.

9.4.3. Upgrading Version from MasterScope MISSION CRITICAL OPERATIONS

9.4.3.1. Incompatibility with MISSION CRITICAL OPERATIONS Ver. 2.x

This release is not compatible with MISSION CRITICAL OPERATIONS Ver. 2.x or earlier.
Interconnections between a console, manager and/or agent are not possible, and upgrading from MISSION CRITICAL OPERATIONS Ver. 2.x or earlier is not possible.

9.4.4. Upgrading Version from MasterScope SystemManager

9.4.4.1. Incompatibility with SystemManager Ver. 3 and earlier

This release is not compatible with SystemManager Ver. 3.x or earlier. Interconnections between a console, manager and/or agent are not possible, and upgrading from SystemManager Ver. 3.x or earlier is not possible.

9.5. General Monitoring Functions

9.5.1. Edit of SysMonMgr.ini

When you edited SysMonMgr.ini, refer to "7.3.4. Notes when the SysMonMgr.ini was changed" in "MasterScope Media Release Notes."

9.5.2. Business View Default Category Settings

When SystemManager G is installed, the default category will be set in Business View. If MISSION CRITICAL OPERATIONS or Application Navigator is installed first in the same installation directory, however, the first product's default category will be set instead of that for SystemManagerG. As the SystemManager G default category data is installed in the monitoring terminal, the SystemManager G knowledge can be set up by importing the knowledge manually. For more information, refer to "11.2.1 Knowledge".

9.5.3. About Accumulating Collected Performance Data

Performance data collected by the performance monitoring function and by SystemManager Gare accumulated on the manager.
To delete the accumulated data automatically, use the performance data accumulation management function.
The performance data accumulation management function manages the performance data accumulated on the manager for the accumulation period specified for each data type.
Performance data exceeding the accumulation period will be deleted automatically.
For details about how to use the [Performance Storage Setting] tab, see the online manual

The size of accumulated performance data is 16byte per piece.
The performance data is stored in one file on a daily basis.
E.g.: The amount of accumulated performance data when 7-days data is retained as a result of monitoring 100 counters at a time interval of 30 seconds with 1 agent

Amount of data saved in 1 file:
16 (byte) * 3600 (seconds) * 24 (hours) / 30 (seconds) = 46080 byte
Size of disk to be used for 1 file:
49152byte (assuming the block size is 4KB)
7-days data for 100 counters (equals 700 files):
49152byte * 700 = 34406400 (approximately 32.9MB)
*The above calculation method only produces a rough approximation, and the exact figure depends on how you operate your system.

For the UNIX manager, the following describes the approximation of the number of inodes to be used to accumulate the performance data.

Number of monitored counters * (Number of retention days + 4)

E.g.: When retaining data for 30,000 counters for a time period of 30 days, 1.02 million inodes will be used.

If you want to store performance data form a few ten thousand counters for a long period of time, you must secure a sufficient inode area when constructing the file system.

The performance data is saved under the following directory:

Windows: <Manager installation directory>\Manager\sg\PerfManager
UNIX: <Manager installation directory>/Manager/sg/PerfManager

It is possible to stop accumulate the performance data unless you use performance information displaying function (multi graph view), and form function.
To stop accumulating the data, refer to "11.2.4 Procedure to Stop Accumulating Performance Information."

*In case of cluster environment, <Manager installation directory> indicates data of a shared directory

9.5.4. Accumulating Statistical Data

The statistical data of a counter to be output to the multi-graph view or a form is generated using the performance data collected by the performance monitoring function or Network Node Manager, and accumulated on the manager.
The accumulated data is automatically deleted based on the statistical data retention period specified in the Options setting of the multi-graph view.

The statistical data is derived from averaging the performance data for a certain period of time for each counter and is generated over more than one time period. The data is stored in separate files by the data period.
The following list shows the file size for each data period for one counter:
Daily file (created at 00:00 every day)

Statistical Data Period	Daily File Size (Byte)
1 minute	69,152
2 minutes	34,592
10 minutes	6,944
30 minutes	2,336
1 hour	1,184
6 hours	224
12 hours	128

Yearly file (created at 00:00 on 1/1 every year)

Statistical Data Period	Daily File Size (Byte)
1 day	17,552

* The statistical data with the data period shorter than the data collection interval of a monitored counter is not generated. For example, for a counter that collects data for every 5 minutes, the

statistical data with a data period of 1 minute or 2 minutes will not be generated, and only the one with a data period of more than 10 minutes will be generated.
However, for performance data collected with Network Node Manager, statistical data for all the periods can be generated regardless of data collected intervals for the counter.

E.g.: Amount of data derived from monitoring 100 counters at intervals of 5 minutes and saving data for 7 days on one agent
Amount of data in the file generated every day:
6,944 + 2,336 + 1,184 + 224 + 128 = 10,816 bytes
Amount of data in the file generated every year:
17,552 bytes
Amount of data for 7 days for 100 counters:
(10,816 bytes * 7 days + 17,552 bytes) * 100 counters = 9,326,400(8.89MB)

In the case of UNIX managers, a rough approximation of the number of inodes to be used to store the statistical data is as follows:
Number of monitored counters * (Number of retention days * Number of daily files + Number of retention years * Number of yearly files)

E.g.: Number of inodes derived from monitoring 100 counters at intervals of 5 minutes and saving data for 7 days on one agent
Number of inodes in the file generated every day: 5
Number of inodes in the file generated every year: 1
Inodes for 7 days for 100 counters: (5 × 7 days + 1) * 100 counters = 3600

If you need to store statistical data for a long period of time, ensure that you will secure an ample inode area and a sufficient disk area when creating the file system.

The statistical data will be saved under the following directories:

Windows:<Manager installation directory>\Manager\sg\PerfStatistics
UNIX :<Manager installation directory>/Manager/sg/PerfStatistics

* In a duplexed environment, <Manager installation directory> indicates a data area on the shared disk.

9.5.5. Restoring Backup Data for the Manager Accumulating Performance Data

If the settings for adding or deleting a monitoring counter has been changed after the online backup was performed by the manager, the performance data accumulated on the manager must be deleted when restoring the backup.

After stopping the manager, delete all directories and files in the following directory before executing the restore command.

• Performance data
Windows: <Manager installation directory>\Manager\sg\PerfManager
UNIX: <Manager installation directory>/Manager/sg/PerfManager

• Statistical data
Windows: <Manager installation directory>\Manager\sg\PerfStatistics
UNIX: <Manager installation directory>/Manager/sg/PerfStatistics

*In a duplexed environment, <Manager installation directory> indicates a data area on the shared disk.

Performing the online backup after a monitoring counter is added or deleted is recommended when accumulating and using the performance data for a long period of time.

9.5.6. About the Default Value of Data Acquisition Method for UNIX Agent Performance Data

To reduce influence on performance data values from a momentary increase of load due to the monitoring operation of the agent itself, MISSION CRITICAL OPERATIONS Ver3.6.2/SystemManager Ver5.5.2/Application Navigator Ver3.2.2 or later has changed the default value for the method to get performance data for UNIX agent monitored objects or Device, NetwowrkInterface, Processor, and System from the momentary value mode to the average value mode.
This change of the default value is likely to bring slight changes between performance data values agents got before version-upgrading and those they gets after version-upgrading.

If you need to change back the method to get the performance data to the previous momentary value mode due to any reason, you must change appropriate settings by referring to the following item in the help manual.

[Monitor the agents]
[Monitor the performance]
[Define the performance monitoring]
[Change the mode used to acquire performance data]

9.5.7. Change of Specifications for Syslog Monitoring

■ Backup Files
the Linux agent (Linux remote host in the case of agentless monitoring), the specified pattern for backup files in syslog monitoring has been changed, depending on the logrotate versions, from MISSION CRITICAL OPERATIONS Ver4.0.3/SystemManager Ver6.0.3/Application Navigator Ver3.3.2 of this product.

• Before change of specifications
[Log file name].<N>
*<N> takes one from numbers 1 to 4.

• After change of specifications
[Log file name]-<YYYYMMDD>
*<YYYYMMDD> takes a number for year, month, and day, respectively.

When upgrading any agent (any remote monitor agent in the agentless monitoring) from its version before change of specifications, the specified pattern of [Log file name].<N> is inherited regardless of the logrotate versions.
And, when reinstalling an agent (a remote monitor agent in the case of agentless monitoring), the specified pattern for the backup files will be changed to the one described above, depending on the logrotate versions.
When the pattern is different from that of the backup method for the monitored syslog, you must change the specification of the backup files in the filter setting option window for each syslog monitoring operation.

■ Default Filter
When newly installing SystemManager G Ver7.0 or later, SystemManager G does not set up [Default Filter], which defines to filter and report all logs logged in syslog on the Linux agent (Linux remote host in the case of agentless monitoring). Therefore, configure the filtering setting so as to log syslog and report necessary messages only.

- Before changing the specifications
  [Default Filter] is defined to all logs in syslog by installing the agent function.

- After changing the specifications
  Filtering is not defined to any logs even when installing the agent function.

9.5.8. Agentless Monitoring

■ Common subject matter

- As the status of a remote host is monitored through the remote monitor agent, the remote host monitoring stops when the agent has not been started.
- Any remote monitor agent cannot monitor its own host as a remote host. If you need to monitor a host on which a remote monitor agent resides, use a normal agent.
- A remote monitor agent cannot be used to conduct monitoring by specifying the IP address and the host name that switch in conjunction with the cluster package. Use a logical agent to monitor the respective statuses of resources that switch in conjunction with the cluster package without being conscious of in which host the package operates.
- When you need to install a normal agent to monitor a host in which a remote monitor agent has been installed, set the agent name for the normal agent to be different from that of the remote monitor agent.
- A remote monitor agent sends an ICMP echo request periodically to its monitored remote host(s). If any response is not returned, the agent regards the monitored remote host(s) as not being started, and does not monitor it. In addition, an ICMP echo request is also sent when registering a remote host to be monitored. For this reason, the ICMP echo request must be allowed at the host where the remote monitoring agent is installed and between the remote hosts.

- The definition information for a remote host is saved in the following location:
  <Installation directory>\Agent\sg\RemoteAgent\<Display name for remote host>\sg
- When a normal agent with the same name as a remote host is newly connected while the remote host is in the topology view, a malfunction may occur.
- The monitoring functions may take on the unknown statuses (such as SERVICEUNKNOWN and PROCESSUNKNOWN) for about 5 minutes in such a case where a remote host is restarted.
- The automatic detection and monitoring of IPv6 are not supported.
- The automatic detection and monitoring of remote hosts are performed based on their IP addresses. For this reason, the hosts whose IP addresses dynamically change through DHCP, etc. cannot be properly monitored.
- It may take some time to stop an agent service in such a case where an API used within the system waits for a response in vain to return from a remote host.
- In operations from the console, all the file names and directory names on remote hosts are treated in lower case.
- Can't monitor remote host in NAT environment.
- Run a remote monitor agent on a host, such as WORKGROUP, which does not belong to any domain. If you run a remote monitor agent on a host that belongs to a domain, the agent may not monitor the performance of its remote host(s).
  If that is the case, you may monitor the performance of the remote host by following "Steps to change a service execution account.

  [Steps to change a service execution account]
  - Stop the "MasterScope UMF Operations Remote Agent" service.
  - Open the service window, and display the property window for "MasterScope UMF Operations Remote Agent."
  - Select the [Logon] tab, and change the account from [Local system account] to [Account] and enter the Administrator account information. *
  - Start the "MasterScope UMF Operations Remote Agent" service.

  *Enter an appropriate domain account or local account that enables you to log in to remote hosts.

- Oracle monitoring with the agentless monitoring function does not support Oracle RAC service monitoring. If you need to monitor the Oracle RAC system on a remote host, you can monitor it by connecting to the system as a normal instance.

■ Windows agentless monitoring

- Unless the authentication information is used when automatically detecting a remote host, the agent may not obtain the detailed information on OSs belonging to Windows. In addition, the ICMP echo request and SNMP access must be allowed at the host where the remote monitoring agent is installed and between the remote hosts.
- In agentless monitoring on Windows, the remote monitor agent uses the WMI interface and SMB service and NETBIOS service. Specifically, it is possible for the agent not to properly monitor remote hosts when it is not allowed to access the following port numbers: 135, 139, 445 for TCP and 137, 138 for UDP. In addition to the above, it must address TCP/UPD for the dynamically allocated ports after 1024 used by WMI. For settings for remote hosts and remote monitor agents, refer to "11.2.5. Security Settings for Agentless Monitoring."

- For Windows agentless monitoring, it is recommended that the authentication information is set with the Administrator right. If you logged in to the system with a general user account, remote hosts may not be properly monitored due to the access right.
- To use performance monitoring for a Windows remote host, the [Remote Registry] service must be running by having been made to start either automatically or manually. If the service is disabled or not running, the data of performance monitoring cannot be acquired (including object acquisition).
- When entering a command to a Windows remote host, specify a command that will terminate in less than 60 seconds. After 60 seconds, a timeout occurs and command execution fails.
- When you enter a command to a Windows remote host, a temporary file will be created in a folder indicated by the system environment variable %TEMP% on the host. On the remote host on which %TEMP% is not set, the command execution fails. You also must have the write/read/execute right for the %TEMP% folder through the account information specified in the authentication information.
- To define Windows remote host monitoring, you can use environmental variables similarly to defining an agent. However, the environmental variables that can be used for that purpose are only a System environmental variable and %SystemRoot%.
- In agentless monitoring on Windows, some objedts (*1) in performance monitoring might not be monitored. All objects can be monitored with the implementation of the following steps.

  [Steps to change a service execution account]
  - Stop the "MasterScope UMF Operations Remote Agent" service.
  - Open the service window, and display the property window for "MasterScope UMF Operations Remote Agent."
  - Select the [Logon] tab, and change the account from [Local system account] to [Account] and enter the Administrator account information. *
  - Start the "MasterScope UMF Operations Remote Agent" service.

  *Enter an appropriate domain account or local account that enables you to log in to remote hosts. Also, when using local account, an account of remote host side needs any one of the following authorities.
  Authority: Administrators, Performance Log Users, Performance Monitor Users

  (*1)...The appropriate object information is under the following registry added.
  HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion¥Perflib¥_V2Providers

■ Linux agentless monitoring

- SSH network connection is used for Linux agentless monitoring. For this reason, the SSH daemon must be started in the remote host and access to the port number used by the SSH daemon must be enabled. Similarly, the host where the remote monitoring agent is installed must be allowed to access the remote host via the port in question. The SSH daemon must support password authentication.
- For Linux agentless monitoring, it is recommended to specify authentication information by using root privileges. The following restrictions apply to a general user account:
  - Process monitoring
    When process monitoring is performed by using a process path, the process path is not identified for processes started by a user other than the specified user.

  - File monitoring
    Only files for which the specified user has the authority to read and directories for which the specified user has the authority to read and execute can be monitored. The status of files and directories for which the user does not have the correct authority becomes "unknown". For capacity monitoring, only the size of files for which read authority has been granted is added.
  - Application log monitoring
    Only log files for which the connected user has the authority to read can be monitored. Log files for which read authority has not been granted will not be reported.
  - Syslog monitoring
    If the connected user does not have the authority to read the files listed below, no syslogs will be reported. If the user has the authority to read the following files, only syslog files for which the connected user has read authority can be monitored. Log files for which read authority has not been granted will not be reported.
    /etc/syslog.conf
    /etc/rsyslog.conf
    /etc/syslog-ng/syslog-ng.conf
  - Recovery execution
    Only commands for which the connected user has read and execution authority can be executed.
  - File/directory specification dialog box
    Only files and directories in the directory for which the connected user has read and execution authority are displayed.
- In Linux agentless monitoring, a directory and files for the monitoring program are created in the home directory of the connected user. For this reason, the connected user must have read and write authority for the home directory. Monitoring is not performed correctly if the user does not have this authority.
- When performing performance monitoring by using Linux agentless monitoring, a temporary file is created in the /tmp directory. For this reason, the connected user must have read and write authority for the /tmp directory. Monitoring is not performed correctly if the user does not have this authority.
- Linux agentless monitoring supports up to 90 logs, files, and directories in total, including the logs monitored by the syslog monitoring function and the files and directories monitored by the file/directory monitoring function.
- When performing performance monitoring by using Linux agentless monitoring, files in the /proc/meminfo directory are referenced. For this reason, the connected user must have read authority for the /proc/meminfo directory. Monitoring is not performed correctly if the user does not have this authority.
- To recover a Linux remote host, the recovery execution result (standard output) must be less than 5 MB. Recovery in which more than 5 MB is output to the standard output might stay permanently in the "executing" status without finishing.

9.5.9. Changing the Date of Agent Machines

If the date of a machine on which an agent is installed is changed to a future date and then changed back to the original date, messages after the date change might not be reported because the date is not synchronized with the manager.

When changing the date to a future date and then back to the original date, stop the agent first.

If the messages are not reported due to the date change, perform the following procedure to restore the messages.

* "\" is used as a directory separator in the following procedure.
  Replace it with "/" for UNIX.
* Once this procedure is performed, the messages added after at the next monitoring timing after the manager is connected will be reported.
* If the manager is in a redundant environment, replace the following manager installation directory with the shared disk directory of the manager.
* If the agent is a logical agent, replace the following agent installation directory with the shared disk directory of the logical agent.

1. Stop the target agent service.

2. Delete the following directories on the target agent machine.
   <Agent installation directory>\Agent\sg\EventLogHelper
   <Agent installation directory>\Agent\sg\SysLogHelper
   <Agent installation directory>\Agent\sg\ApLogHelper
   <Agent installation directory>\Agent\sg\Message

   * The directories above might not exist, depending on the environment.
     Delete only the directories that exist.

3. Delete the following files on the target agent machine.
   <Agent installation directory>\Agent\sg\PerformanceHelper\log\<Manager name>_007
   Files with a future date among YYYYMMDD_<Counter ID> files in the directory above.

   * The files above might not exist, depending on the environment.
     Delete only the files that exist.

4. Delete the following files on the manager.
   <Manager installation directory>\Manager\sg\ApLogHelper\[Agent]_***.pos
   <Manager installation directory>\Manager\sg\EventLogHelper\[Agent]_***.pos
   <Manager installation directory>\Manager\sg\Message\[Agent]_***.pos
   <Manager installation directory>\Manager\sg\SysLogHelper\[Agent]_***.pos

   * Delete only the files with [Agent] as the target agent name.
   * Replace *** with any number.
   * The files mentioned above might not exist, depending on the environment.
     Delete only the files that exist.
   * It is not necessary to stop the manager function when performing step 4.

9.5.10. Output of Crash Dump in case of Trouble in the Windows Environment

It is recommended that you configure in advance the crash dump setting to speed up the investigation of a failure when it occurs.
For Windows Server 2008 or later, you must set some registries for the above configuration.
For more information on setting these registries, refer to the support technical information related to Microsoft Windows Error Reporting (WER).
Once you decide to set the crash dump, set it so that a full dump may be output.

However, note the following points:

* When the crash dump is output, the file size may increase in some cases to such a degree that it may impact the disk capacity.
* If you configure the crash dump output setting, the crash dump will be output when other software than SystemManager G crashes.

9.5.11. About Outputting Core Files when a Failure Occurs in UNIX environment

This product is configured to output core files as follows to make examinations faster when a failure occurs:

■ Destination for core file output

- Manager
  <Installation path>/Manager
- Agent
  <Installation path>/Agent

■ Maximum size of core files
No limit.

If there is any problem with the above setting, edit the following file accordingly:

- Files to be edited
  Manager (HP-UX)
  /sbin/init.d/UMFOperationsManager_1

  Agent (HP-UX)
  /sbin/init.d/UMFOperationsAgent_1

  Manager (Linux)
  /etc/init.d/UMFOperationsManager_1

Agent (Linux)
/etc/init.d/UMFOperationsAgent_1

Agent (Solaris)
/etc/init.d/UMFOperationsAgent_1

Agent (AIX)
/etc/rc.d/init.d/UMFOperationsAgent_1

*If you install them in an environment where other MasterScope products are using rc script files with the same names as them, their last numeric characters will be changed to 2 or higher (e.g.: UMF Operations Manager_2 and UMFOperationsAgent_3). You need to reread the explanation above according to your actual environment.

- What to be edited
  The above files include the following statement:
  ulimit -c unlimited
  Change this portion of “unlimited” to your desired maximum file size.

Note that you should pay attention to the following points:
*When upgrading the version of a product, the edited files may be overwritten; if that is the case, those files must be edited again.
*If you specify any other value than unlimited for the size of the core files, the core files may become imperfect. If that is the case, we may ask you to sample the core files again after specifying “unlimited” as the maximum file size.
*As any output core file is assigned to a process ID and the file is not overwritten in Linux, there may be impact on the disk capacity when failures continue to occur on the product in a row.

9.5.12. Changing the Directory Mount Point Used within the Product

The mount points cannot be assigned separately for each directory in the directory pointed by the installation path of the product.

9.5.13. Event Log Monitoring

■ **About node name**
The computer name of event log is used as a node name of the message sent by the event log monitoring.
It might be different from the node name registered to the topology view depending on the environment.
Note that the message might not be received if the node name registered to the topology view is specified for the message filter of the message receiving function.
Moreover, note that messages that are not matched with the node name registered to the topology are not stored for the message monitoring function.

■ **About body text**

If MISSION CRITICAL OPERATIONS Ver3.6.0/SystemManager Ver5.5.0/Application Navigator Ver3.2.0 or earlier of this product is used with Windows Server 2008, the text of an event log might not be acquired, depending on the OS to which the event log is output or the application behavior.
In this case, the event log text is replaced with the following message, and normal monitoring cannot be performed.
"EventLog Monitor Message : Not found message text."

9.5.14. Change of Specifications for Event Log Monitoring

When newly installing SystemManager G Ver7.0 or later, SystemManager G does not set up [Default Filter], which defines to filter and report all logs logged in the event log on the Windows agent (Windows remote host in the case of agentless monitoring). Therefore, configure the filtering setting so as to log the event log and report necessary messages only.

- Before changing the specifications
  [Default Filter] is defined to all event logs by installing the agent function.

- After changing the specifications
  Filtering is not defined to any event logs even when installing the agent function.

9.5.15. Changes in the Specifications of Performance Monitoring

From MISSION CRITICAL OPERATIONS Ver3.6.0/SystemManager Ver5.5.0/Application Navigator Ver4.0.1, the configuration under the Processor object is changed for UNIX agents with single processor core, as shown below.

Before change: [Object] - [Counter] configuration
After change: [Object] - [Instance] - [Counter] configuration
* For Solaris agents, [Object] - [Counter] configuration in any kind of environment.

If the version is upgraded when the definition of [Object] - [Counter] configuration still exists, the configuration will not be changed. However, it cannot be monitored with this configuration if the number of processor cores increases after it is upgraded. For this reason, change to the [Object] - [Instance] - [Counter] configuration by re-specifying the monitoring definition. Reconfiguration can also be performed by executing the following command.
<Manager installation directory>/Manager/bin/PerformanceCmd.exe RE-SETUP -P <HostName>

9.5.16. The upper limit of the number of counters which can be managed by the performance management function

The performance management function can manage up to 1,000,000 counters. Counters exceeding 1,000,000 cannot be registered.

The following functions register counters to the performance management function.

- Performance monitoring function
- Invariant Analyzer function (Importing performance data by using a monitoring terminal and command)
- Performance management function (Importing performance data by using a command)

A counter can be deleted by using the following methods.

- Performance monitoring function
  Remove the counter to be deleted from the monitoring targets.

  For details, refer to the following sections of Product Help Manual.
  [Monitor the agents]
  [Monitor the performance]
  [Define the performance monitoring]
  [Define the monitored resource]

- Invariant Analyzer function
  Delete the counter from the Counter Information window.

A counter can also be deleted by deleting a logical item from the Integrated Topology view. In this case, delete all logical items with the same host name.

9.5.17. Number of processors that can be monitored with the performance monitoring function

On the Windows server with 33 or more processors, the [Processor] object in the performance monitoring function can monitor up to 32 processors.
The [Server Work Queues] object cannot perform monitoring.

9.5.18. Description on the performance monitoring counter

Some counters may not display description in the performance monitoring function in the Windows agent. This event is caused by a bug in Windows. For details about the versions of Windows and counters with which this event occurs, see Document no. 4010202 in Microsoft Knowledge Base (support technical information).

9.5.19. Storing messages

Messages are accumulated in duplicate by message monitoring function and the business view.
If it does not cause any operational problems, it is recommended to disable the message monitoring function.

9.5.20. Changing the audit log when the agent monitoring definition is imported from the monitoring terminal

The contents of the audit log that is output when the agent monitoring definition is imported from the monitoring terminal are changed from MISSION CRITICAL OPERATIONS Ver.4.1.2/SystemManager Ver6.2.0 (It is identical to the one that is output when executing the TopologyCmd IMPORT command.)

9.5.20.1. Monitoring the AP Log

The following trail is output when the import succeeds.

Message ID	00001026
Severity	Information
Service name	Application log monitoring
Message definition statement (in English)	Succeeded in importing a monitoring definition.

The following trail is output when the import fails.

Message ID	00001027
Severity	Error
Service name	Application log monitoring
Message definition statement (in English)	Failed to import a monitoring definition.

9.5.20.2. Event log monitoring

The following trail is output when the import succeeds.

Message ID	00001008
Severity	Information
Service name	Event log monitoring
Message definition statement (in English)	Succeeded in importing a monitoring definition.

The following trail is output when the import fails.

Message ID	00001009
Severity	Error

Service name	Event log monitoring
Message definition statement (in English)	Failed to import a monitoring definition.

9.5.20.3. Windows service monitoring

The following trail is output when the import succeeds.

Message ID	00001026
Severity	Information
Service name	Windows service monitoring
Message definition statement (in English)	Succeeded in importing a monitoring definition.

The following trail is output when the import fails.

Message ID	00001027
Severity	Error
Service name	Windows service monitoring
Message definition statement (in English)	Failed to import a monitoring definition.

9.5.20.4. Process monitoring

The following trail is output when the import succeeds.

Message ID	00001026
Severity	Information
Service name	Process monitoring
Message definition statement (in English)	Succeeded in importing a monitoring definition.

The following trail is output when the import fails.

Message ID	00001027
Severity	Error
Service name	Process monitoring
Message definition statement (in English)	Failed to import a monitoring definition.

9.5.21. Change of the audit log when the schedule definition and calendar definitions are imported from the monitoring terminal

The contents of the audit log that is output when the schedule definition and calendar definitions are imported from the monitoring terminal are changed as of MISSION CRITICAL OPERATIONS Ver.4.2.1/SystemManager Ver6.2.1.

9.5.21.1. Schedule

The following trail is output when the import succeeds.

Message ID	00001006
Severity	Information
Service name	Schedule
Message definition statement (in English)	Succeeded to import a schedule definition.

The following trail is output when the import fails.

Message ID	00001007
Severity	Error
Service name	Schedule
Message definition statement (in English)	Failed to import a schedule definition.

9.5.21.2. Calendar

The following trail is output when the import succeeds.

Message ID	00001106
Severity	Information
Service name	Calendar
Message definition statement (in English)	Succeeded to import a calendar definition.

The following trail is output when the import fails.

Message ID	00001107
Severity	Error
Service name	Calendar
Message definition statement (in English)	Failed to import a calendar definition.

9.5.22. Limit of the Number of the PerformanceCmd MSCV counters

The specification has been changed so that the command execution is stopped when the number of counters exceeds 2000 when all of the counter data items are subjected to being obtained by PerformanceCmd MSCV from MISSION CRITICAL OPERATIONS Ver.4.1.2, in order to prevent overload on the manager from occurring due to the simultaneous transmission of the vast amount of counter data items to the manager.

For details, see the following chapters in the manual or in Help.
[Command reference]
- [PerformanceCmd]
  - [PerformanceCmd MSCV]

9.5.23. History of the Event Correlation Function

If a manager is upgraded from the version prior to MISSION CRITICAL OPERATIONS Ver4.2.0 of this product,
the history before the upgrading cannot be referred to.
It is necessary to execute the conversion command in advance when referring to the history before the upgrade.

For details, see the following chapters in the manual or in Help.
[Command reference]
- [EventCorrelationCmd]
  - [EventCorrelationCmd CNV]

9.5.24. Change of Default Connection Timeout for Service Port Monitoring

As of MISSION CRITICAL OPERATIONS Ver.4.2.1, the default connection timeout value for service port monitoring has been changed from one second to three seconds.
Although the default connection timeout value was one second in MISSION CRITICAL OPERATIONS Ver.4.2.0 or earlier, timeouts might occur frequently even if a normal connection is able to be established. Therefore, this value has been changed to three seconds.

If you were using the default connection timeout value in MISSION CRITICAL OPERATIONS Ver.4.2.0 or earlier, the connection timeout time will change to three seconds when you upgrade to Ver4.2.1 or later. If you changed the connection timeout value before upgrading, the changed value is applied after the upgrade. That is, the connection timeout time remains the same.

9.5.25. Performance data when communication is disconnected

While communication between the agent and manager is disconnected due to a manager shutdown, etc., performance data will not be output to the multi-graph view and form function because the data is not accumulated on the manager.
The performance data can be output to the multi-graph view and form function by importing the data to the manager following the steps below when the performance data is accumulated on the agent.

1. Output the performance data to a file by using the PerformanceCmd MCSV command.
2. Import the performance data from the output file by using the PerfImportCmd command.

For details, see the following chapters in the manual or in Help.

[Command reference]
-[PerformanceCmd]
-[PerformanceCmd MCSV]

-[PerfImportCmd]
-[PerfImportCmd]

9.5.26. About hostname for Message Linker

When adding a host under "Message Linker" node, it must be distinct from sub nodes under the Topology View node or the Message Linker node.

9.5.27. Authentication information setting for agentless monitoring function (Linux)

When the “line feed code" and “character encoding” specified in the authentication information of agentless monitoring function are not the same as the “line feed code" and “character encoding” of the monitored Linux remote host, the “System information” is not displayed.

Perform the following procedure to confirm.

i. Confirming the line feed code

1) Log in to the monitored Linux remote host with the user account specified in the authentication information.
2) Execute the following command:

```
%stty -a
speed 9600 baud; rows 24; columns 80; line = 0;
intr = ^C; quit = ^\; erase = ^?; kill = ^U; eof = ^D; eol = <undef>;
eol2 = <undef>; start = ^Q; stop = ^S; susp = ^Z; rprnt = ^R; werase = ^W;
lnext = ^V; flush = ^O; min = 1; time = 0;
-parenb -parodd cs8 -hupcl -cstopb cread -clocal -crtscts
-ignbrk -brkint -ignpar -parmrk -inpck -istrip -inlcr -igncr icrnl ixon -ixoff
-iuclc -ixany -imaxbel
opost -olcuc -ocrnl onlcr -onocr -onlret -ofill -ofdel nl0 cr0 tab0 bs0 vt0 ff0
isig icanon iexten echo echoe echok -echonl -noflsh -xcase -tostop -echoprt
echoctl echoke
```

Select “CRLF” if “onlcr” is displayed.
Select “LF” if “-onlcr” is displayed.

ii. Confirming the character encoding

1) Log in to the monitored Linux remote host with the user account specified in the authentication information.
2) Execute the following command:

```
env|grep LANG
LANG=***
```

Confirm the language environment, and then select UTF8 or EUC.

9.6. General function

9.6.1. Coverage of command execution

This product provides functions to execute commands of external products on the system such as the scenario control function and operation control function. This product can warrant the command execution using these functions, however, cannot warrant the operations of the executed commands. Confirm with the support of the command provider when the command fails or a failure occurs.

9.6.2. Character encoding when outputting a file

It is recommended to specify UNICODE for the character string when outputting a file by using the file output function of the console, manager, or agent function.
When a file is output by using other than UNICODE character encoding, characters that cannot be expressed by using the specified character encoding might be output as different characters.

9.6.3. Backup and recovery when managers are configured in a hierarchy

If the settings for the upper manager are inconsistent with the settings for a lower manager, the messages and performance information collected by the lower manager cannot be viewed correctly. For this reason, do not change the definitions specified from the upper manager to a lower manager, and be sure to back up the data of both the upper and lower managers. Backed up data should be restored on both the upper and lower managers in the same way as described above.

9.6.4. About support of UNICODE

The following functions aren't supporting UNICODE.

- CDO Message API
  Please refer to below for details.
  MasterScope SystemManager G Release Memo - CDO Message API Edition –
  (CDO_relememo.pdf)
- SystemManager Event Trap Utility
  Only SJIS and EUC character codes are supported.

9.7. Application Monitoring

9.7.1. Change of Specifications for Export Data

The connection information portion of export data in application monitoring has adopted a replacement type of data similar to the monitoring template since Application Navigator Ver3.0. The connection information portion of the replacement type of export data has values in the exporting environment as the predefined values. In any version earlier than Application Navigator Ver3.0, the connection information portion has the same data as that in an execution environment, importing such data will cause inconvenience when the importing environment has different connection information than that in the exporting environment. As it has adopted a replacement type of data, users can specify the connection information when importing the data.

	Up to Ver2.x	From Ver3.0
Export data type	Connection information reflects real values in an exporting environment	Connection information is a replacement type
Default value	-	Real values in an exporting environment
Is a replacement dialog displayed when importing the data?	No	Yes

9.7.2. Oracle Monitoring

- In Oracle monitoring, one agent can monitor only one version of Oracle.

- In the HP-UX agent, it may take some time to display a dialog when you bring up the [RAC Setting] window for the first time after starting the SystemManager G agent. Click and hold the mouse button and wait for the dialog to appear.

- UNIX agents do not support OS authentication processes. Enable password authentication access by sys user.

- In monitoring Oracle, a stored procedure is called to get a performance value. The procedure is registered to a monitored DB by running the setup script. For information on the setup script, refer to the following sections of Product Help Manual.

  [Monitor applications]
  [Monitor Oracle]
  [Preparations for Oracle performance monitoring]
  [DB setting when monitoring Oracle]

  The procedure is called at monitoring intervals (default 30 seconds) set in SystemManager G and internally copies a dynamic performance views to work tables. Some monitored counters in Application Navigator are affected by registering a stored procedure to DB and a periodic procedure call at monitoring intervals.

Instance	Affected counter
Datafile (*1)	As Disk I/O occurs due to stored procedure processing, the performance values for [Physical Blocks Read] and [Physical Blocks Written] increase.
Disk	As Disk I/O occurs due to stored procedure processing, the performance values for [I/O/sec], [Physical Reads], [Physical Reads/sec], [Physical Writes], [Physical Writes(%)], and [Physical Writes/sec] increase.
SQL	As a stored procedure issues SQL, the performance value for [SQL Executions] increases.
Tablespace (*1)	The execution of a setup script registers a table and stored procedure required for Oracle monitoring in the specified table area. For this reason, the performance values for [FreeRate(%)], [FreeSpace], [MaxFreeRate(%)], [MaxFreeSpace], [MaxUseRate(%)], [UseMount], [UseRate(%)], and [DataFile (*2)] increase or decrease.
Transaction	As COMMIT is periodically performed at monitoring intervals within a stored procedure, the performance values for [Transaction] and [Transaction/sec] increase.

(*1) This is only applied to the table area and data file specified with a setup script.
(*2) The real counter name for the Datafile counter is the title part of the data file.

- The magnitude of impact (how much the difference is between those in Ver3.2.1 and those in the previous versions) depends on operating environments.
- For other counters (such as resource usage and cache hit rate) than those listed above, it is also likely that performance values may increase or decrease, depending on other factors such as machine environments, monitoring settings, and Oracle environment settings, compared to the previous versions.
- If load on Oracle is heavy, the load can be reduced by extending the monitoring interval.

- The Oracle monitoring agent operates as Oracle client. When the access error occurs while the database server is stopping, the error is recorded in the log file of Oracle. The disk space might be pressed when continuously operating it. Delete log file after it confirms it if there is no problem in the output error.

  The diagnostic information is logged in Oracle Database by Automatic Diagnostic Repository feature. The trace and the core are located in root user's ADR directory. Configure the ADR policy, and perform the automatic or manual delete. Please refer to the Oracle Database manager guide for details.

- The listener monitoring in RAC environments are only targeted for local listeners. It cannot monitor SCAN listeners. For example, do not set "ENABLE_GLOBAL_DYNAMIC_ENDPOINT_..." or "LISTENER_SCAN…" in the listener monitoring setting window as a monitored target.

- If you operate Oracle in the archive log mode, the archive log will increase due to monitoring by SystemManager G. The increase in logs is proportionate to the number of records there are of the following dynamic performance views:

  V$FILESTAT
  V$TEMPSTAT
  V$TEMPFILE
  V$PARAMETER
  V$SGASTAT
  V$PGASTAT
  V$STATNAME
  V$SESSTAT
  V$ROLLNAME
  V$ROLLSTAT
  V$SORT_SEGMENT
  V$TEMP_EXTENT_POOL

  The logs increase by 12 to 23 MB per hour when Oracle Database 12.1.0.2.0 is used, the monitoring interval is 30 seconds, and there are a total of about 40,000 records of the above dynamic performance views.

- When failures occur in Oracle monitoring function, and it is necessary to investigate by the viewpoint of Oracle libraries, Oracle Programmer license is needed to investigate.
  Please be aware that if you don't have Oracle Programmer license, there is a possibility that it becomes difficult to continue the investigation.

9.7.3. WebLogic Monitoring

- If you want to import and use a definition file for the performance monitoring function shipped with the product, pay attention to the following considerations.

  If the cost of operating a Servlet instance among monitored counters included in a performance monitoring definition file is high and the CPU usage is high for a SysMonAgt process on the agent, remove the monitoring process for Servlet instances if it is not necessary, or change the default monitoring interval (30 seconds) to 60 seconds or more, before operating the system.

- From Application Navigator Ver3.2, the formulas of the ExecuteThreadIdleRate(%) and ExecuteThreads counters of the Thread instance have been changed as follows:
  - ExecuteThreadIdleRate(%)
    ExecuteThreadIdleCount / (ExecuteThreadTotalCount - StandbyThreadCount) * 100
  - ExecuteThreads
    ExecuteThreadTotalCount – (StandbyThreadCount + ExecuteThreadIdleCount)

9.7.4. Apache Monitoring

- Users cannot establish a connection to an Apache server through a proxy server.
- The monitoring functionality does not support HTTP authentication processes. Configure settings so that a connection to the Apache server can be established without such authentication.
- The monitoring functionality does not support HTTPS (SSL communication).

9.7.5. SAP Monitoring

- Since Application Navigator Ver.3.1, the monitoring interval for system log has been changed from 30 to 60 seconds.
- Since Application Navigator Ver.3.3.1, the default for the interface to monitor system logs has been changed from XAL to XMB.
- With SAP system log monitoring by the XAL interface, increasing the entry size of the system log (local log) may disable collection of logs due to failure process within the monitoring interval. For instance, when the entry size is 100MB, monitoring may take more than 100 seconds in some environments, disabling system monitoring to be performed normally. This may cause temporary delay of other monitoring functions as well.
  As SAP becomes high load during processing, long collection time may also cause reduced system performance.
  In such cases, decrease the maximum size of the system log (rslg/max_diskspace/local) to a value with which no warning message is displayed at the SAP side. As an approximate, set values under 5,000,000 (5MB).
- If SAP system log monitoring is performed with the XAL interface in a NetWeaver7.3 environment, an event where an accurate system log cannot be obtained has been reported. In any NetWeaver7.3 environment, SAP system log monitoring must be set using an XMB interface.

9.8. Service Availability Monitoring

9.8.1. Common notice

- A monitoring counter of the service availability monitoring is using "performance monitoring function".
  See "9.5. General Monitoring Functions."

- Some of the counters which are usually displayed in the [Counter Setting] window may not appear sometimes. One possibility is that an added or configured instance(s) may not be reflected in the probe terminal. Wait for a while, and open the [Counter Setting] window again.

- You cannot change any Monitor Name once you have set it. If you want to change a Monitor Name, you need to delete the Monitor Name and then set it again.

- When using the Web scenario monitoring function, prepare an account with Administrator right for Probe terminal.
  Choose one of them of the following way.

  - Change the logon account of probe service (MasterScope SystemManager G Probe Agent) to an account of a Administrator right.
  - Change the logon account of probe service to an account of a Local System.
    Set an account of a Administrator right as [Run As User Setting] of the [Monitor Configuration] dialog of the service availability monitoring.

- Set the following privilege to the account to be set to [Run As User Setting]:
  Log on as a service
  Deny log on as a service

- The account to be set to an [Run As User] requires that the user profile directory has been created in C:\Users. Confirm that the directory exists on the probe terminal.

- If [User Name] under [Run As User Setting] includes a domain name or server name, you need to specify it in the following format:
  [Only user name]
  username
  [To specify username and domain name]
  username@domainname
  [To specify username and server name]
  username@servername

- When using [Run As User], the event which shows that I logged on to event log (security) is output at the timing of a monitoring.

- If you want to run multiple monitoring processes on one probe terminal, you must set each monitoring process to a priority or set to “1” the number of concurrently executed processes ([Number of concurrent requests]) in the [Probe Terminal Setting] dialog. Otherwise, it is likely that as multiple monitoring processes are executed concurrently, the terminal may not measure

accurate responses.
If you set [Number of concurrent requests] to “1,” you must specify ample time in [Monitor Interval Timeout] so that all the monitoring processes may have been completed within the time. Any monitoring processes that have not been completed within the time will be carried over to the next monitoring interval.
If you want to change the above settings, set a desired Monitor Interval Timeout and Monitor Timeout by referring to the following relationships between the number of concurrent requests, Monitor Interval Timeout, and Monitor Timeout.

- Relationships between the number of concurrent requests, Monitor Interval Timeout, and Monitor Timeout

Assume that the probe settings are set as follows:

Number of monitoring processes: 4 (each named Monitor 1, Monitor 2, Monitor 3, and Monitor 4)
Monitor Timeout for Monitors 1 and 2: 90 seconds
Monitor Timeout for Monitors 3 and 4: 180 seconds
Monitor Interval Timeout: 300 seconds
Monitor interval: 5 minutes

1. The solid arrowline " → " indicates the Monitor Timeout for scenarios (Monitors) 1 and 2.
2. The dotted arrowline " ⇢ " indicates the Monitor Timeout for scenarios (Monitors) 3 and 4.
3. The broken arrowline " ⇢ " indicates the Monitor Interval Timeout.

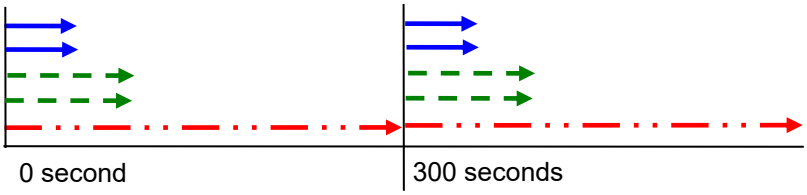


Figure – Priority: None; Concurrent Requests: 10

In this example, all the configured monitoring processes are executed concurrently to such a degree that the number of the processes does not exceed 10.

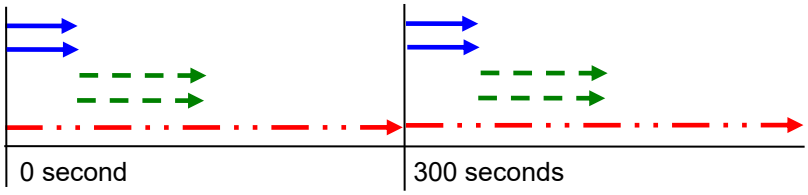


Figure – Priority: 1 for Scenarios 1 and 2, 2 for Scenarios 3 and 4; Concurrent Requests: 2

First, Monitors 1 and 2 are executed, and then Monitors 3 and 4. A maximum of 2 monitor processes with the same priority are executed concurrently.

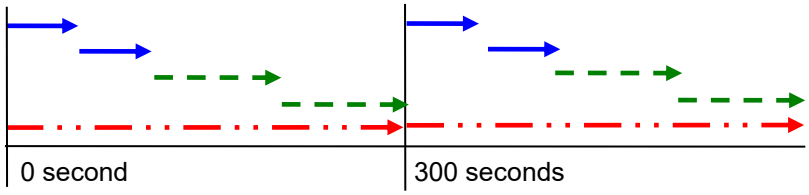


Figure – Priority: 1 for Scenarios 1 and 2, 2 for Scenarios 3 and 4; Concurrent Requests: 1

First, Monitors 1 and 2 are executed, and then Monitors 3 and 4. All the monitoring processes are executed one-by-one sequentially.

- The icon of the probe group displayed on the topology cannot be changed. Even if you specify an icon for [Icon File] in the [Update Group] dialog opened from the probe group node, the icon will not be changed.

- Do not move any probe node from a probe group on Topology View. Once you have moved a probe node, the Service availability monitoring function cannot be used any longer. Once you have moved it inadvertently, restore it by following these steps:
  (1) Remove the probe node from Topology View.
  (2) On the removed probe terminal, restart the service (MasterScope SystemManager G Probe Agent).

- In the case of the schedule period outside, the performance counter value makes 0 and the severity unknown.

- When using schedule setting by service availability monitoring, the type of the period setting is supporting only "working day".

- Service availability monitoring uses the monitoring interval of the service availability monitoring and the monitoring interval of the performance monitoring. The "Monitor Interval" parameter for the service availability monitoring is a monitoring interval during which a monitoring operation is executed. On the other hand, the monitored interval ([Option]-[Performance Monitoring]) for the performance monitoring is an interval during which measurement results (performance counter values) for the service availability monitoring are collected or the results are displayed as a graph.

- To prevent security tools, etc. from blocking access to monitored targets, configure exclusion settings etc. as necessary.

- Group Managed Service Accounts (gMSA) can't be used.

- Set the start time in the schedule setting to a time with a margin of about two minutes earlier than the start time of monitoring.(For example when you'd like to begin monitoring from 9:00, set the start time of the schedule setting as 8:58.)Similarly to the start time, set the end time with an ample margin.

- When a monitoring operation is still running at the end time set in the schedule setting, it will not be terminated immediately but continue to run until the operation has been completed. However, the result will not be included in the monitored counter.

- When the monitoring resulted in an error, the error information capture file is output on the probe terminal. Delete this file regularly because the probe does not delete it automatically.

<Output folder> C:\Program Files\NEC\UMF\OperationsProbe\Agent\sg\AppNaviPrb\error_info * When it is installed in C:\Program Files\NEC\UMF

9.8.2. Web scenario monitoring

- It's necessary to be able to refer to a monitoring target site by IE on the probe terminal. Therefore do the following confirmation on the probe terminal.
  (1) Log on to Windows OS by the account to use by [Run As User] or probe service(*).
  * probe service = MasterScope SystemManager G Probe Agent
  (2) After logging on to the OS, start IE.
  (3) Complete IE first run wizard.
  (4) Confirm that you can refer to a monitoring target site.

If you can't refer to it, set [security setting] or [Advanced] of the internet option.
If the dialog of IE is indicated, set it so as not to be indicated.

- It is recommended that you change the following settings with IE on the probe terminal:

  (1) Register the monitored site to [Tools] - [Internet Options] - [Security] - [Intranet] or [Trusted Sites] - [Site].

  (2) In [Tools] - [Internet Options] - [Security] - [Intranet] or [Trusted Sites] - [Custom Level...] items, change several selected [Prompt] to [Enable]. The following lists the typical items under which you must change [Prompt] to [Enable]:

    - [Submit non-encrypted form data]
    - [Web sites in less privileged Web content zones can navigate into this zone]
    - [Navigate windows and frames across different domains]
    - [Display mixed content]

  (3) Disable several items under [Tools]-[Internet Options]-[Advanced]. The following lists the typical items you must disable:

    - [Warn if POST submittal is redirected to a zone that does not permit posts]
    - [Warn if changing between secure and not secure mode]
    - [Turn on the display of a notification about every script error]

  (4) Enable several items under [Tools] - [Internet Options] - [Advanced]. The following lists the typical items you must enable:

    - [Disable script debugging (Internet Explorer)]
    - [Disable script debugging (Other)]

  *The above setting items depend on IE versions.

  The dialogs configured with the above settings are also displayed in Web scenario monitoring. This dialog isn't shown to the time of recoding and is sometimes shown to the time of monitoring. (In other words, monitoring is failure.)
  When the probe terminal and console reside on different machines, such an event occurs due to different settings of IE if the logon account on OS that runs the console and the account that is used for monitoring are different.
  Using the [dialog] parameters in the [Step Edit] dialog enables you to operate dialogs displayed at the time of monitoring, but it is recommended that you suppress as many dialogs as possible using IE settings in advance.

- When you have modified a monitor scenario, resulting in reducing the number steps in it, you cannot delete counter settings for the reduced steps. Before modifying the scenario, delete on a temporary basis either the counter settings or the whole instance setting (scenario setting), and add them again after the scenario has been modified.

- Note that when creating a scenario for a Web page that requires basic authentication, the authentication setting dialog will appear only the first time after the scenario writer is started. Within the same session, the authentication window appears only once because the previous

authentication information is carried over. If you want to change the authentication settings again after setting them once, end the scenario writer and restart it again.

- When client authentication monitoring a necessary Web site, it's necessary to import a necessary client certificate into IE browser of probe terminal to access the Web page.
  You have to set the logon account which imported client authentication as Run As User. Set the account to [Run As User Setting] of the [Monitor Configuration] dialog.

- Within any Web pages, the close operation cannot be recorded. When a “window.close()" process is run in JavaScript, the Window will be initialized to the white state within it without being closed.

- Within the browser view, only the operation that can be recorded is the left click operation of the mouse. If you press any button with the Enter key, the operation will not be recorded. Use the mouse operation to click any button.

- Only the operations that can be recorded in the browser view are the left-click of the mouse. Pressing any buttons such as the Enter key will not be recorded. Click the buttons with the mouse.

- When monitoring Web scenarios without using the browser cache, the cache information on the probe terminal will be deleted on a temporary basis in time to the monitoring.

- When creating a scenario setting with Scenario Writer, you may mistakenly record a unintended step (for example, you may mistakenly click an entry form). If this is the case, remove that extra step by following these steps.
  If you click the [Stop] button to remove the extra step while recording operations, the “AGAINCLICK” parameter may be set when recording the operations again.
  (1) Record all the operation steps.
  (2) Click the [Stop] button to finish recording the scenario setting.
  (3) Remove the extra, recorded step from the right-click menu.

- Web Scenario Monitoring acquires information about operation on the web through API in IE. Therefore, there is a possibility that the following object can't do recording and monitoring:

  Flash
  JavaScript (*)
  Silverlight
  Office documents
  PDF files
  Explorer
  etc

  *The dialog and web page using the following JavaScript function can't be recorded:
  - using prompt, showModalDialog, showModelessDialog
  - window.open, document.write, window.close

(1) Screen operations when recording
- Right-click operations
- Wheel operations

- Screen transition operations with the shortcut, tab, space or Enter keys
  (Character entry in a text box is not included.)

(2) Contents, Plug-ins, etc.
- Websites in the HTML5 configuration (Smartphone sites included)
- Plug-in part of movie websites
- Social service plug-in part
- Website specific plug-ins (Search forecast display, etc.)
- The web site built using a HTML IFRAME tag

(3) Script
- JavaScript
  Operations of JavaScript processing part without communicating with a server (List box, etc.)
  Processing whose screen is started by window.open(), generated by document.write() without communicating with a server, and closed by window.close()
  Submit processing of form data is called within JavaScript. (*)
  Objects (elements or attributes) are dynamically generated within JavaScript. (*)
  Dialogs using functions of prompt(), showModalDialog() and showModelessDialog()
- Ajax

(4) ActiveX control
- Flash
- Silverlight
- JavaApplet
- Shockwave
- QuickTime/Windows Media Player
- Explorer (folder) operations of Windows OS
- File downloading/uploading
- Application startup
- Plug-in display for PDF, Office, etc.

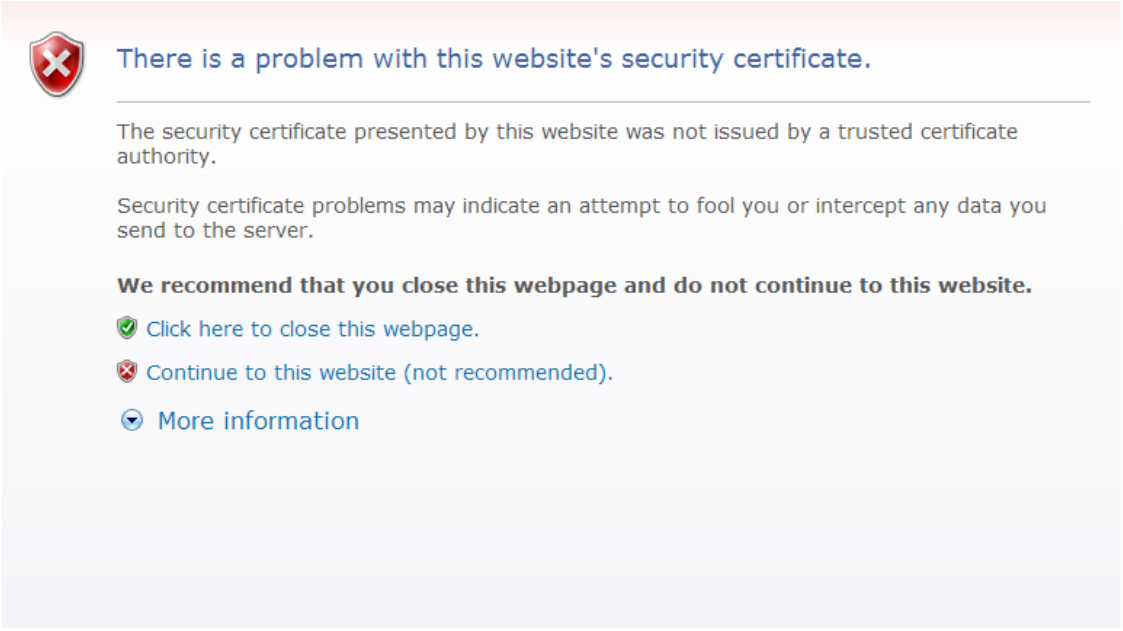
(5) Other
- Connection via FTP protocol communications
- Mobile phone sites

(*) Processing related to the monitored click operations

- The maximum settable number of counters per scenario is 100. If you want to set more than 100 counters, decrease the number of counters for each step, or divide the monitoring configuration (scenario) into two scenarios and configure them so that the number of counters for each scenario may not exceed 100.

- Before using the Web scenario monitoring, set the number of concurrent requests to 1, or set the priority so that multiple instances of Web scenario monitoring may not be executed concurrently. When multiple instances of Web scenario monitoring are concurrently executed, load on the machine due to concurrent operations may cause a response time not to be measured accurately.

- If the following certificate error page appears when monitoring an SSL site in the Web scenario monitoring, the site cannot be monitored with the probe.



Set it so that a certificate error page isn't indicated by the following methods.
(Set it on console and Probe terminal.)

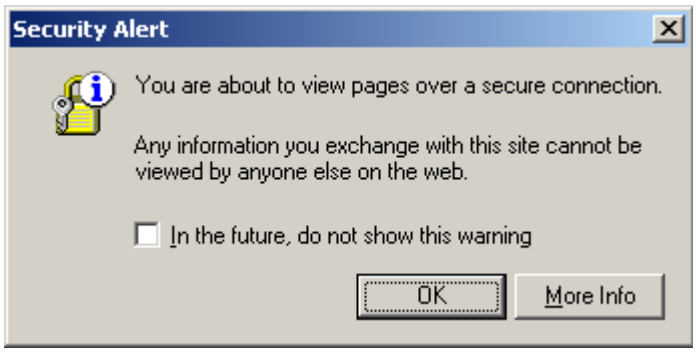
- Clear a [An error message (ScriptError) is ignored] checkbox(*).
  * [ScenarioWriter]-[File]-[Setting]-[Web Scenario Monitor Setting] dialog
- From Internet Options in Internet Explorer, import the server certificate to [Trusted Publishers] and root certificate to [Trusted Root Certification Authorities]. This error page also appears when there is any problem with the relevant certificates such as expiration and inconsistent host names. Configure settings so that any security warning may not appear.

If you cannot suppress the display of [security warning] dialogs, set a dialog operation, which clicks the [Yes] or [OK] button, in the [DIALOG_1] parameter as a step setting in the [Step Edit] dialog.

Dialog example 1

DIALOG_1=Security Alert,TAB,TAB,CLICK

Dialog example 2



DIALOG_1=Security Alert,CLICK

- In the Web scenario monitoring, recording and playback has been successful, but if the monitoring fails, check the following on the probe terminal:
  (1) You must do the account of the probe service other than a local system account.
  (2) Be possible to refer to a monitoring target site from IE on the probe terminal.
  (3) A monitoring target website(*) has to be added to [trusted site] or [local intranet].
  * hostname(FQDN), domain, IP address.
  (4) When monitoring a HTTPS site, it's necessary to import a server certificate/a route certificate/a client certificate into IE on the probe terminal.

- The schedule setting for probe groups and probe host nodes are not supported.
  However, the service availability monitoring can use the monitoring schedule settings for monitored instances.

- If you want to set dialog operations in the Web scenario monitoring, the following items must be considered:
  (1) Set the waiting time to an appropriate value (3000 mill seconds or more) higher than the

default when including dialog operations in a scenario. As a dialog operation cannot be completed because of a low waiting time, a monitoring operation may fail. Set the waiting time to be large enough so that, after recording a dialog operation with the scenario writer, the loading icon will stop after the dialog operation is completed when reproducing it.

(2) While reproducing the dialog operation, do not perform a mouse operation on any dialog and/or any HTML window part of the scenario writer. Before performing any mouse operation, press the stop button to stop reproducing the dialog operation.

(3) When using probe service (An account was set), set the Web Scenario Monitoring which does dialog operation as follows.
[Probe terminal setting] [Number of concurrent requests] of the dialog is set as "1".
[Monitoring Configuration] designate the [priority] of the dialog, and make sure that the plural won't be monitored at the same time.
When not setting these, dialog operation is affected, and monitoring time-out is sometimes done.
(It's recommended to set Number of concurrent requests as 1.)

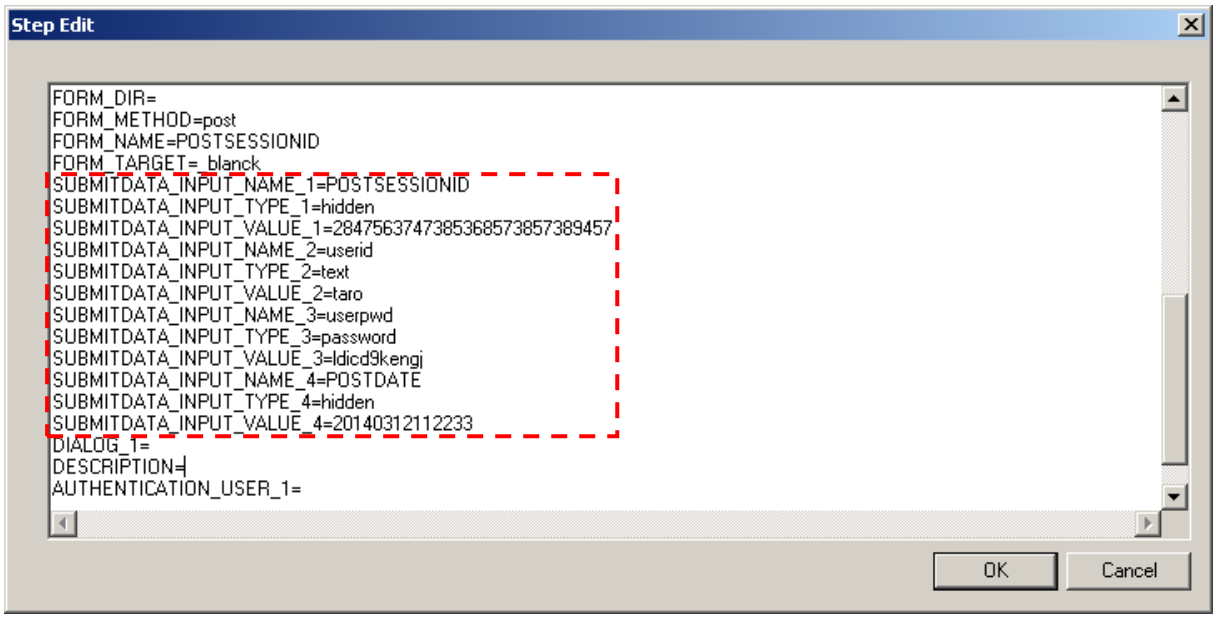
The following describes a configuration example.

I have specified five Web monitoring scenario.
If the monitoring of (*) contains a step of the dialog operation, specify the priority of monitoring (*) so that it is not running at the same time:

Monitoring configuration		
Web scenario monitoring A (*)	Priority	1
Web scenario monitoring B	Priority	3
Web scenario monitoring C (*)	Priority	2
Web scenario monitoring D	Priority	3
Web scenario monitoring E	Priority	3

(4) For the monitoring in which a dialog operation is set, an application error in ScenarioWriter.exe may be output to the event log when the monitoring operation has been completed. This error is output because the parent process is terminated while a dialog is displayed, but it does not have any impact on the next monitoring operation or other monitoring operations.

- The case when the form data by which the value turns dynamic (the hidden attribute) is sent is relevant.
  * Session ID, date, time etc.
  To record all form data by Web Scenario Monitoring, the hidden attribute which makes the session ID the value is also recorded.
  The recorded value is used for playback and monitoring.
  The value recorded at that time is judged as wrong form data on the monitoring target Web site side, and I fail in monitoring.
  Delete setting of the hidden attribute from step edit of a scenario manually in such case.



The [SUBMITDATA_] parameter must be edited.

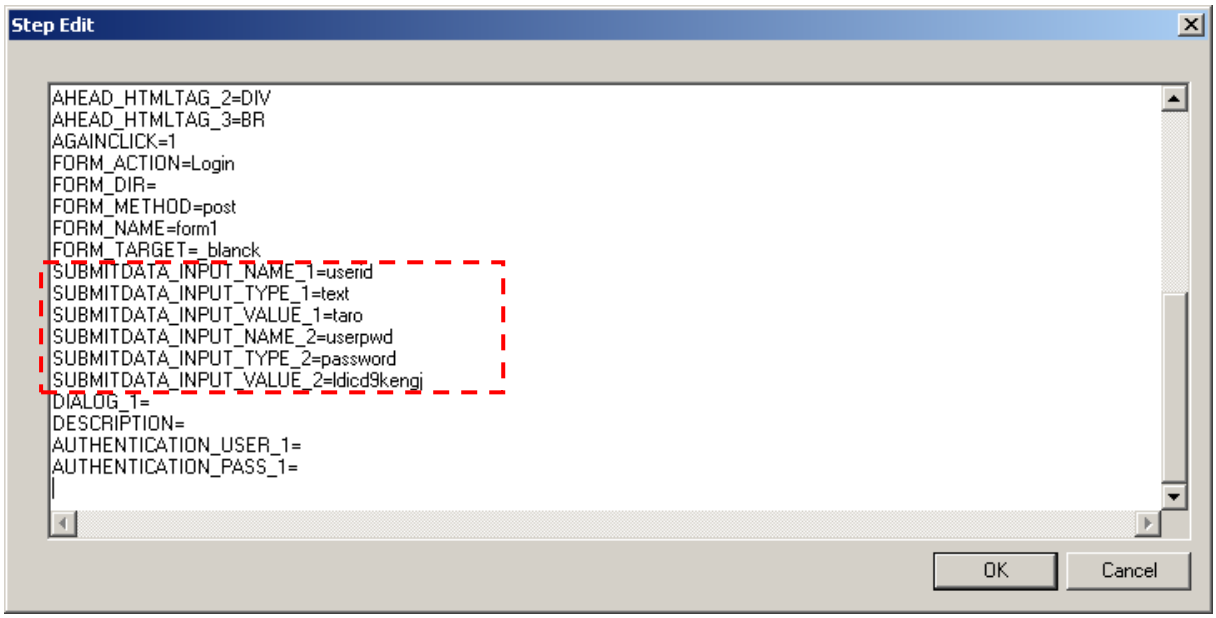
```
SUBMITDATA_INPUT_NAME_1=POSTSESSIONID
SUBMITDATA_INPUT_TYPE_1=hidden
SUBMITDATA_INPUT_VALUE_1=284756374738536857385738945 7
SUBMITDATA_INPUT_NAME_2=userid
SUBMITDATA_INPUT_TYPE_2=text
SUBMITDATA_INPUT_VALUE_2=taro
SUBMITDATA_INPUT_NAME_3=userpwd
SUBMITDATA_INPUT_TYPE_3=password
SUBMITDATA_INPUT_VALUE_3=ldicd9kengj
SUBMITDATA_INPUT_NAME_4=POSTDATE
SUBMITDATA_INPUT_TYPE_4=hidden
SUBMITDATA_INPUT_VALUE_4=20140312112233
```

Form data consists of _NAME, _TYPE, VALUE.
If "_TYPE" is the hidden attribute, delete a group of SUBMITDATA_.

```
SUBMITDATA_INPUT_NAME_2=userid
SUBMITDATA_INPUT_TYPE_2=text
SUBMITDATA_INPUT_VALUE_2=taro
SUBMITDATA_INPUT_NAME_3=userpwd
SUBMITDATA_INPUT_TYPE_3=password
SUBMITDATA_INPUT_VALUE_3=ldicd9kengj
```

An index of a group of remaining SUBMITDATA_, assign the serial number which starts from 1 again.

```
SUBMITDATA_INPUT_NAME_1=userid
SUBMITDATA_INPUT_TYPE_1=text
SUBMITDATA_INPUT_VALUE_1=taro
SUBMITDATA_INPUT_NAME_2=userpwd
SUBMITDATA_INPUT_TYPE_2=password
SUBMITDATA_INPUT_VALUE_2=ldicd9kengj
```



If edit is completed, press a "OK" button. If there is a step to which edit is necessary, change it. If all edit is completed, confirm whether you playback and succeed. After that, save the scenario.

- When using the Web scenario monitoring in the IE10 or higher environment, the cache settings for Web scenario monitoring are not available. This is because temporary files such as pre-created cookies and cache cannot be referenced due to enhanced IE security restrictions.
  When specifying a monitoring scenario using automatic login by loading cookies,

  Access the monitored URL --> Login (Enter user/password, etc.)
  --> Logout once (Cookie is created)
  --> Access the monitored URL again
  (Automatic login using the cookie created in the same monitoring session)

  Monitoring can be performed by creating a scenario like this.

- Note the following when using the page contents comparison function (by setting the COMPARE_HTML parameter to 1):

  (1) A HTML before and after redirection is compared. (The Web page redirected in the step)
  (2) If the following was operated, the information saved to compare the page contents is deleted.

  Restarting the Probe Agent service (MasterScope SystemManager G Probe Agent__identifier_n)

Updating the web scenario monitoring settings
Enabling/disabling the status
Stopping monitoring according to the schedule setting

(3) The following monitoring doesn't compare a HTML because there is no information to compare.
* After addition of web scenario monitoring setting
* After operation of (2)

(4) If the schedule is set and monitoring is stopped, the information saved to compare page contents is deleted. However, information may not be deleted under the following conditions:

The period during which monitoring is stopped is shorter than the value set to [Monitor Interval].
The period during which monitoring is stopped is shorter than the value set to [Monitor Timeout].
The period during which monitoring is stopped is shorter than the value set to [Monitor Interval Timeout].

For example, if the schedule is set as follows, monitoring is stopped for 30 minutes.

Start Time	End Time
0:00	2:00
2:30	23:59

To use the page contents comparison function in this schedule, set a set value as [Monitor Interval], [Monitor Timeout], and [Monitor Interval Timeout] shorter than 30 minutes (1800 seconds).

- Application Navigator Ver4.1.2 or later, the HTTP error status is displayed when the server returns an error message if the "PATTERN_STRING" parameter is unmatched. For example, a message includes an error status such as 404.

9.8.3. Mail monitoring

- The protocol which can be used for receive is only POP3.

- The mail monitoring does not support SMTPs, POPs, IMAPs, and POP/SMTP over SSL.

- Mail monitoring sends a test mail.
  When a sent test mail could be received, availability will be "1".
  It is set to "0" when one of send and receive is successful.
  When success or failure of send checks it, specify the Send Availability in a counter.
  When success or failure of receive checks it, specify the Receive Availability in a counter.

- If the mail monitoring succeeds in transmission, but fails in reception, test mails for the monitoring will accumulate in the mail box. When a number of mails accumulate in the mail box, the mail monitoring may time out because monitoring takes too much time as all the mails in the box must

be checked when the monitoring on the reception side has been restored. If that is the case, clear the test mails that have accumulated in the mail box by using an appropriate software program such as mail client software to receive them once from within the box.

- Do not monitor the same mail account from two probe terminals at the same time. In the same mail account, more than one, when logging in, access continues.
  Monitoring sometimes fails because a session doesn't end when he doesn't log out completely.

9.8.4. TCP monitoring

- If the connected port requests a linefeed when sending a command to the port, specify the following character string as the linefeed and send it to the port.
  <PROBE_CR>

- If a response is returned from the port promptly after a connection to it has been established, you must check [Receive an Opening Message from a server first] in the [Probe for TCP – Monitor Setting] window.

- In some type of applications or protocol, session information may remain on the server side after each TCP port monitoring access. Keep in mind that such situation may occur when using the TCP port monitoring.

9.8.5. FTP monitoring

- Monitoring large files or setting a large value to [Number for the concurrent] might affect all types of monitoring, including FTP monitoring.
  For example, the message "failed in making of a communication socket." due to the decrease of resources or throughput of the probe terminal, monitored servers or communications devices between servers might be output. In this case, change the concurrent execution count to a smaller number, or change the transferred file size to a file size whose transfer can be finished in about 15 seconds.

- Monitoring might not be performed in an environment where accesses are restricted by security tools or a firewall.

- In FTP monitoring, acquired files are output as is to the following <Monitor ID> directory on the probe terminal.

<Output folder> C:\Program Files\NEC\UMF\OperationsProbe\Agent\sg\AppNaviPrb\Ftp\<Monitor ID> * When it is installed in C:\Program Files\NEC\UMF

- The target <Monitor ID> directory is deleted when the FTP monitor settings are deleted.
  For this reason, do not delete the target <Monitor ID> directory manually.
  Note that the directory might not be deleted due to an access problem etc when the FTP monitoring indicated by the monitor ID is running. In this case, <Monitor ID> directory deletion will not be performed again. Therefore, delete it manually.

- When using the file comparison function (by selecting the [files are compared] check box), note

the following:

(1) If the size of the file to be acquired is large, the monitoring execution time is longer than when the file comparison function is not used.
* For reference, the execution time of the test FTP monitoring to a file of 500MB performed by NEC is described below.

When the file comparison function is disabled: 55 seconds
When the file comparison function is enabled: 65 seconds

(2) If the following was operated, the information saved to compare files is deleted.

Restarting the Probe Agent service (MasterScope SystemManager G Probe Agent__identifier_n)
Updating FTP monitoring settings
Enabling/disabling the status
Stopping monitoring according to the schedule setting

(3) The following monitoring doesn't compare files because there is no information to compare.
* After addition of FTP monitoring setting
* After operation of (2)

(4) If the schedule is set and monitoring is stopped, the information saved to compare files is deleted. However, information may not be deleted under the following conditions:

The period during which monitoring is stopped is shorter than the value set to [Monitor Interval].
The period during which monitoring is stopped is shorter than the value set to [Monitor Timeout].
The period during which monitoring is stopped is shorter than the value set to [Monitor Interval Timeout].

For example, if the schedule is set as follows, monitoring is stopped for 30 minutes.

Start Time	End Time
0:00	2:00
2:30	23:59

To use the file comparison function in this schedule, set a value as [Monitor Interval], [Monitor Timeout], and [Monitor Interval Timeout] shorter than 30 minutes (1800 seconds).

9.8.6. Import/Export

- When importing the Application Navigator Ver3.1.0 export file by Application Navigator Ver3.1.2 later, schedule settings will not be imported. Perform schedule settings for each monitoring setting after importing.

- If schedule settings with the same name as the schedule to be imported already exist, those duplicating schedule settings will not be imported. In this case, you must change the existing schedule settings as new settings. To use the schedule in import file, change the name of the existing schedule settings before importing.

- If multiple counter values are set to the monitoring settings, it will take some time for the imported settings to be applied to the probe terminal. For this reason, monitoring results may not be displayed at the monitoring timing immediately after import.

- The status of monitoring settings newly added by import will all be enabled regardless of the settings of the imported file.
  To set the status of newly added settings to disabled, change the status to disabled manually after import, or update the status by importing again.

- When adding new monitoring settings by import, make sure that the number of licenses is sufficient. If there are not enough licenses, monitoring settings that lack the licenses including existing monitoring settings will be set to disabled state.

- Do not import monitoring settings exported from other MasterScope products into the probe host.

- To import large volumes of monitoring settings at once, the manager and probe terminal will require considerable memory. Adjust the maximum number of settings imported according to the machine specifications of the customer environment, referring to the following measured values.

*Specifications of machines used for measurement

Manager

CPU	Intel(R) Xeon(R) CPU E5405 @ 2.00GHz
System Memory	4GB
OS	Microsoft Windows Server 2008 R2

Probe terminal

CPU	Intel(R) Xeon(R) CPU E5405 @ 2.00GHz
System Memory	4GB
OS	Microsoft Windows Server 2008 R2

Following values shows the memory used while importing monitoring settings using the above machine environment.

*Measurement case 1

Monitoring settings in measurement

Monitoring Setting	Target 5 Web scenario instances (Set 10 steps per target)
Monitor counter settings	[8 counters× (10 steps + Total)] × 5 targets = 440 counters *8 counters per step

Memory used

Manager	200MB
Probe terminal	200MB

*Measurement case 2

Monitoring settings in measurement

Monitoring Setting	Target 40 Web scenario instances (Set 4 steps per target)
Monitor counter settings	[8 counters× (4 steps + Total)] × 40 targets = 1600 counters *8 counters per step

Memory used

Manager	2GB
Probe terminal	2GB

9.9. Service port monitoring

9.9.1. Notes on service port monitoring

- Monitoring time

The monitoring time per port can be roughly calculated using the formula below. Consider the monitoring time per port and the number of monitored ports when specifying the monitoring interval. The monitoring might not be completed within the monitoring interval if the monitoring time exceeds the monitoring interval. In addition, all monitoring processes might not be completed within the monitoring interval if many monitoring service ports are specified. When the monitoring is not completed within the monitoring interval and still continues when the next monitoring starts, the monitoring is skipped and will be performed next time.

The maximum monitoring time per port can be roughly calculated using the formula below. Consider the monitoring time per port and the number of monitored ports when specifying the monitoring interval.

•For TCP

Monitoring time (seconds) = Connection timeout

•For UDP

Monitoring time (seconds) = Connection timeout * (Retry count +1) * 2

•Local address monitoring for remote hosts

Local addresses cannot be monitored on remote hosts.

•TCP port monitoring

The TCP port monitoring tries to connect to the service port of the monitoring target, and determines to open and close based on the response from the monitoring target service.

•UDP port monitoring

The UDP port monitoring sends UDP packets to the service port of the monitoring target. When an ICMP undelivered response packet is received, it is recognized as “close”.

When it is timed out without receiving an ICMP undelivered response, a ping request packet (ECHO Request) is sent to the target agent. When a ping response packet (ECHO Reply) is received, it is recognized as “open”.

When *ping* is also timed out, it is recognized as “unknown”.

•To monitor UDP ports, change the firewall settings of the agent, remote monitoring agent and remote host to allow the ICMP packet transmission.

•When the service port monitoring is performed sequentially, it might be recognized as a port scanning in the monitored computer and the packet rating might be performed.

9.10. About Configuration Information

9.10.1. About Collection/Display of Configuration Information

1) Displaying IP address
   If you set several IP addresses to one network interface card in the Windows agent, all the IP addresses may not be displayed due to the limitations of GUI. A maximum of 259 characters can be displayed.
   If you set the same IP address to more than one NIC in AIX, it will be displayed correctly on the windows, but the network information is not stored in CMDB.
   The IP address of IPv6 cannot be displayed in HP-UX, AIX, and Solaris.

2) Displaying CPU operation status
   When several CPUs are installed to one machine in the agent (on all the platforms), all the CPU operation statuses may not be displayed due to the limitations of GUI. A maximum of 259 characters can be displayed.

3) Displaying memory size
   The size of memories HP-UX displays in the nPartitions/Virtual Partitions environment is a total value of the size of ILM (interleave memory) and the one of CLM (cell local memory).

4) Displaying virtual IP
   If you assign one physical network interface to a logical interface in Linux whose Kernel version is 2.2 or later, the IP addresses assigned to the logical interface may not be displayed.
   In AIX, the network information on logical interfaces and on NIB (Network Interface Backup) is not displayed.

5) Displaying whether DHCP is used
   The information on “whether DHCP is used” is displayed based on the content of the setting file. The content of the setting files is reflected by restarting the dhcp daemon.

6) Displaying the disk information
   If you mount several directories to one mount point, they are displayed correctly on window, but the disk information is not stored in CMDB.
   The value displayed for the usage (KB) is derived from subtracting the free space (KB) from the total space (KB).

7) Displaying the network information
   As it takes some time for name resolution due to DNS settings, it may also take some time to update windows.

8) Displaying the device information
- Obtain and display the following disk device information.

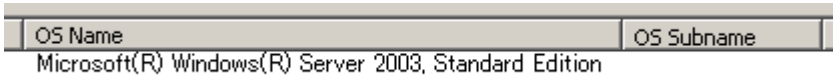
OS	Recognizable devices
Windows	IDE and SCSI disks recognized by WMI (Windows Management Instrumentation) Win32_DiskDevice
Linux	Devices to which one of the following device files applies. - When the Kernel version is under 2.6.18. IDE: /dev/hd[a-z] SCSI: /dev/sd[a-z], /dev/scd (Devices other than disk devices might be obtained when sg drivers can be recognized.) - When the Kernel version is under 2.6.18 or higher. IDE: /dev/hd[a-z] SCSI: /dev/sd[a-z], /dev/scd (Devices other than disk devices might be obtained when sg drivers can be recognized.) Xen Virtual Block Device: /dev/xvd[a-g] AWS environment: /dev/sda1, /dev/xvda1, /dev/xvde1, /dev/sda2, /dev/sda3, /dev/xvda3, /dev/xvde3
HP-UX	SCSI: Class disk, devices with scsi bus type of host bus adapter
Solaris	IDE: Class disk, module dad devices SCSI: Class disk, module sd devices
AIX	SCSI: Device class disk, subclass scsi devices in the AIX device configuration database

- Multi-path disk devices are not supported.

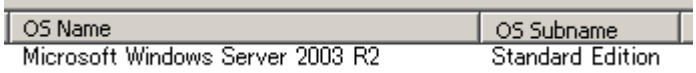
9) Displaying a set of configuration information
If you display the device information, system information, software information, network information, and disk information by selecting [Topology] - [System], the configuration information for a maximum of 256 agents is displayed.

・ Displaying the Windows edition
The Windows edition is displayed in the OS sub-name up to Ver3.7.0, but it is displayed as a part of the OS name after Ver3.7.1.

・ Displaying the Windows edition after Ver3.7.1



・ Displaying the Windows edition before Ver3.7.0



If you are connected to an agent before Ver3.7.0, the information on Windows on that agent is displayed separately in OS name and in OS sub-name as usual. Note that the OS sub-name is not displayed in Windows Server 2008 R2.

If you need to make the display items consistent with those of agents before Ver3.7.0, you configure the following settings on appropriate agents.
(i) Add the following to <Agent installation directory>\Agent\sg\wfsgAgt\wfsgAgt.ini.

```
[Win]
OSNameFlag=1
```

* For Windows, describe using UTF-16 LE code for the character encoding and CR+LF for the line feed code.
* For UNIX, describe using UTF-8 code for the character encoding and LF for the line feed code.

(ii) Restart the agent.

10) Displaying information on the Windows OS version

- Changes in Ver. 4.0

The OS major version and the OS minor version are displayed when the agent before Ver4.0 is connected.

The OS major version, the OS minor version, and the OS version are displayed when the agent before Ver4.0 is connected.

11) Displaying the Linux OS name

- Changes in Ver. 4.0

With versions older than Ver. 4.0, “Linux” is displayed as the OS name and the distribution is displayed as the OS sub name. From Ver. 4.0, the distribution is displayed as the OS name.

The display method above applies when an agent older than Ver. 4.0 is connected.

* Displaying the Linux OS name for Ver. 4.0

* Displaying the Linux OS name for a version older than Ver. 4.0

- Changes in Ver. 4.0.3

The method of obtaining the distribution to be displayed in the OS name was changed for Ver. 4.0.3 or later.

Perform the following setting procedure to change the obtaining method to the previous method for Ver. 4.0.2 or older, obtaining the distribution from the file contents described in $INSTALL/Agent/sg/wfsgAgt/wfsgAgt.ini in sequence.

(i) Add the following line to $INSTALL/Agent/sg/wfsgAgt.ini.

```
[Linux]
OSNameFlag=1                                    * Add this line
SubnameReleaseFile1=/etc/SuSE-release
SubnameReleaseFile2=/etc/asianux-release
SubnameReleaseFile3=/etc/redhat-release
```

(ii) Restart the agent.

12) About reducing load when many agents are working

If many agents are working, it is likely that heavy load will be imposed on the manager because it is subjected to receiving the collected information many times.

By configuring the following setting, you can specify the initial collection interval between collections of the configuration information on a newly connected agent.

Edit the following files on the manager with your text editor:

Windows：<Manager installation directory>\Manager\sg\wfsgMgr\wfsgMgr.ini
UNIX： <Manager installation directory>/Manager/sg/wfsgMgr/wfsgMgr.ini

Add the following statements:

```
[Interval]
DiskInterval=60
NetworkInterval=60
SoftInterval=60
SystemInterval=0
DeviceInterval=0
```

* For Windows, describe using UTF-16 LE code for the character encoding and CR+LF for the line feed code.
* For UNIX, describe using UTF-8 code for the character encoding and LF for the line feed code.

Each of the above statements indicates the default interval (in minutes) to collect each piece of the configuration information.
To reduce the load, set a large value to make the collection interval longer.
(You can specify any value in the range of 0 to 3600. A value of 0 means that the information will not be collected.)

If you connect 200 agents or more to the manager, it is recommended that you set the value of collection interval to the number of connected agents or more, or 0.

13) Information is displayed differently on remote agents and normal agents as described below.
* Windows
- Network information
  - The MAC address is displayed in lowercase letters on normal agents and in uppercase letters on remote hosts.
  - Normally, only network interfaces with an IP address specified are displayed for the agent. For the remote host individual node display, interfaces without an IP address specified are displayed.
- Software information
  - The collected content for normal agents may differ from the content for remote hosts.
- System information
  - The number of logical CPUs is displayed on normal agents, but the number of physical CPUs is displayed on remote hosts.

* Linux
- Disk information
  - The device mount point is displayed in the [Partition] column on normal agents; however, it is not displayed on remote hosts.
  - The device path is displayed in the [Drive Name/Device] column on remote hosts.
  - Information in which the device path does not start with “.dev” will not be collected on remote hosts.
- Network information
  - The virtual NIC is displayed as an individual NIC on normal agents; however, it is displayed as a physical NIC to which multiple IP addresses are assigned on remote hosts.
  - IPv6 addresses can be displayed on normal agents, but not on remote hosts.
- System information

- If the host name is in the FQDN format, it is displayed without the domain on remote hosts.

9.11. Operation control function

9.11.1. Searching for command logs

When upgrading from MISSION CRITICAL OPERATIONS Ver. 3.6.2 or earlier, the command logs executed by MISSION CRITICAL OPERATIONS Ver. 3.6.2 or earlier cannot be searched.

9.12. ServiceManager linkage function

- An incident is displayed in the "incident status" of the monitoring console when the incident is created with a message stored in the business view category which is not visible to the user currently using console.
- Type (Auto Register/Manual Register) to be displayed on "Incident Details" window of history is not a type of registration for when you have registered the incident, is the type that is set to the current policy.

9.13. Invariant Analyzer function

- The Linux manager cannot analyze performance data collected by MasterScope Network Manager.
- When using the Linux manager, specify 50,000 or less for the total number of counters to be analyzed.The maximum number of counters that can be used varies depending on the configuration and performance of the computer on which the manager is installed.Use this number as a guideline

9.14. Duplexed Environment

9.14.1. Setup in the Duplexed Environment

For details, refer to an appropriate clustering setup guide.

- When uninstalling an active/standby system, files on the shared disk will not be removed. After the system has been uninstalled, remove them manually.

- When you use a duplex system Probe Agent in Service availability monitoring, prepare the same account and password for the [Run As User] setting on each node.

9.14.2. Resource Monitoring that is Switched Over in Conjunction with Cluster Package

Use a logical agent for monitoring the performance of the shared disk or monitoring any resource, such as log files on the shared disk, which will be switched as the cluster package is switched.
It is because the phenomenon, for example, the normal agent which uses resources (shared disk and others) is forcibly stopped by the cluster control software, and others may occur when monitoring the resources that switch in conjunction with the cluster package by using the normal agent.

9.15. Security

9.15.1. Communication Environment and Security Settings

- Windows firewall
  If Windows firewall is enabled, the following program needs to be registered as an exception.
  Program to be registered as an exception:
  <Manager function install directory>\bin\SysMonMgr.exe

- Ports used
  Refer to "11.2.12. List of Communication Ports" about the port used by MasterScope SystemManager G.

- About NAT
  In MasterScope SystemManager G communications take place between the manager and its console, and between the manager and its agents. If NAT is used for networks between them, it can be operated as long as address conversion can be resolved on a one-to-one correspondence basis.

9.15.2. User Account Control

If you use the system in an environment where user account control is enabled, you must pay attention to the following considerations:
At the time of starting the monitoring terminal, user account control will cause the [Program needs your permission to continue] warning dialog to appear. Once you have selected [Continue], the monitoring terminal will be started. As long as user account control is enabled, this warning dialog cannot be suppressed.
The %Program Files% folder has been virtualized. If you select any location under Program Files as the installation folder, you must use an editor with the administrative right to edit the SysMonSvc.ini file.
In an environment where you have installed any version earlier than Application Navigator Ver3.0, the files in the virtualized folder cannot be removed with an uninstallation process and may impact the operation of Application Navigator Ver3.0 or later.
Check if the virtualized folder holds any data, and delete the data if any.
C:\Users\<Username>\AppData\Local\VirtualStore\Program Files\NEC\UMF\Operations

9.15.3. On-access Virus Scan

If the folders used by this product are subject to an on-access virus scan, this product might not function normally. For this reason, exclude the folders (installation folder/data area folder) used by this product as the target of the on-access scan.

9.15.4. Setting of SELinux in Linux

When using Linux, set SELinux to "disabled" beforehand.

9.16. Platform

9.16.1. When using Red Hat Linux 5.6 to 5.8 or 6.1 to 6.3

If a manager is used on Red Hat Linux 5.6 to 5.8 or 6.1 to 6.3, a defect in the glibc library included in these versions might cause the following problems.

- Only one message might be output when the message CSV file output command MessageViewCmd CSV is executed.
  The message CSV file can be output from the console without problem.
- The import command controlled by scenario fails.
  The import from the monitoring terminal can be executed without problems.

This problem does not occur under Red Hat Enterprise Linux 5.9 or later and 6.4 or later.

9.16.2. Use in the LPAR environment

When the AIX agent is installed, the settings are specified for a non-LPAR environment. For this reason, the following procedure must be performed after the agent is installed in the LPAR environment.

1. Stop the agent service.
2. Replace the dat file.
   Use the commands below to replace Processor_forSingle.dat and Processor_forMulti.dat stored in the installation directory sg/PerformanceDefault/ with Processor_forSingle-LPAR.dat and Processor_forMulti-LPAR.dat respectively.

   ```
   # cd <Installation Directory>/sg/PerformanceDefault/
   # cp –p Processor_forSingle-LPAR.dat Processor_forSingle.dat
   # cp -p Processor_forMulti-LPAR.dat Processor_forMulti.dat
   ```

3. Start the agent service.

9.17. WebConsole

For the notes on WebConsole, see the following:

10. Restrictions

10.1. General Monitoring Functions

10.1.1. Web Monitoring Terminal Function

- About files to be set up
  For Web monitoring terminals, only the minimum number of files required to run programs are set up.
  Among the files to be set up in installing a monitoring terminal, the following are not set up for Web monitoring terminals:
  - Knowledge files
  - Monitoring template files
  - Image files
  - Icon files
  - Option modules

  You need to locate the files required for Web monitoring terminals by referring to the monitoring terminal folder or copying the files in the folder.

- Product knowledge
  The usage of knowledge* for other products at Web monitoring terminals is not supported at this time.

  * Refer to "Message knowledge file for other products" in "11.2.1 Knowledge".

- Communication protocol
  If the priority of IPv6 connection is higher than that of IPv4 connection, connection to the manager may fail.
  If connection to the manager fails, check the priority order with the following command and prioritize IPv4 connection over IPv6 connection.

  Priority order check command
  #netsh interface ipv6 show prefixpolicies

  Example of command output result

Priority order	Label	Prefix
50	0	::1/128
40	0	::/0
30	0	2002::/16
20	0	::/96
10	0	::ffff:0:0/96
5	0	2001::/32

Priority order change command
#netsh interface ipv6 set prefixpolicy <Prefix> <Priority order> <Label>
Example) netsh interface ipv6 set prefixpolicy ::ffff:0:0/96 60 0

To use IPv6 as the communication protocol between the manager and the Web monitoring screen, see "8.4When Using IPv6"
Windows Service Monitoring

In Windows service monitoring, explanations may not be displayed for some services.

10.1.2. Windows Process Monitoring

In Windows process monitoring, if processes existing in paths containing JIS2004 characters are monitored, process path names may not be displayed normally.

10.1.3. Performance Monitoring

- There may be errors in the decimal portion of the graph data displayed on the monitoring terminals and in the CSV data output by PerformanceCmd.
- The value of [Memory]-[% Memory Used Ex] might become invalid on HP-UX when the memory usage for the entire system exceeds 20 GB.

10.1.4. About Monitoring Log Files on the Shared Disk

If you monitor log files on the shared disk with an agent, you may lose messages when the disk switches.

10.1.5. Schedule Monitoring

As Application Navigator does not support schedule monitoring, period messages that fall outside the monitored targets cannot completely be suppressed. As the state transition messages from performance counters for applications monitored by Application Navigator are controlled by schedule monitoring, they are suppressed during periods that are not under monitoring.
But, service availability monitoring can set a monitoring schedule from the [Monitor Configuration] dialog. A message of service availability monitoring of monitoring outside the specified period is restrained.

10.1.6. Time Synchronization Effects

If time is synchronized by network time protocol or manually during performance data collection interval, the performance data will be computed using the time difference between the pre-synchronized time when the last collection occurred, and the post-synchronized time when the current collection occurred. If the current time was synchronized to the time before the last collection time, computed time difference becomes negative and shows an incorrect performance data for that interval.

Set a performance monitoring interval that is adequately larger than the time correction. Set a performance monitoring interval that is adequately larger than the time correction.

10.1.7. Form Output Function for Performance Information

In this version, the form output function for performance information operates only in Window manager environments It can neither be used in any HP-UX manager environment nor in any Linux manager environment.

10.1.8. Context Menu in the List Display

If one of the following operations is executed, the item at which the mouse cursor is pointing might become the target of the operation of the context menu.

Conditions

- If the context menu is opened on an unselected item while the SHIFT or CTRL key is being held down in a list in which multiple items can be selected.
- If the context menu is opened on an unselected item in a list that is updated automatically.

Target window

The target windows are as follows:

- business view
  - Category message window
  - Search result window

- Operation control function
  - Command log dialog box
  - Action log dialog box
  - Command execution result dialog box

- Invariant Analyzer function
  - Analysis result list dialog box
  - Model list dialog box
  - Analysis result related information dialog box

- ServiceManager linkage function
  - Incident status dialog box

- Message monitoring function
  - Message monitoring dialog box (right pane)
  - Message monitoring dialog box (lower pane)

10.2. Application Monitoring

10.2.1. Instance Registration

For Windows agents, AUX, COM1 to COM9, CON, LPT1 to LPT9, NUL, PRN cannot be used for the following names and IDs in the instance and server registrations of the monitoring application.

- Oracle monitoring, SQL Server monitoring instance name
- Apache monitoring, Tomcat monitoring, WebSphere monitoring server ID
- SAP monitoring, Java application monitoring instance ID

10.2.2. Oracle Monitoring

■ Automatic Instance Detection Function
The following environments, the automatic instance detection function does not work properly. Enter the instance name manually.

- Linux (x86_64), HP-UX, Solaris, AIX

■ Oracle RAC Service Monitoring
Oracle RAC service monitoring uses the srvctl command of Oracle. If the output result from the following command exceeds 115 KB, the statuses of some RAC services may not be obtained.

```
srvctl status service -d DatabaseName -S 1
```

■ Scale-in and Scale-out for RAC Configuration
The system does not support scale-in and scale-out operations that decrease and increase the number of Oracle RAC nodes while SystemManager G is running. Actions activated by clicking on the [Latest Config Update] button in the [Oracle Monitor - RAC Setting] window are not guaranteed.

[Measure to avoid this event]
When scale-in and scale-out of a RAC configuration have occurred, cancel the RAC service settings once and then register them again.

10.2.3. WebLogic Server Monitoring

Only remote monitoring agents can use [Set a timeout for WebLogic Server monitoring] and [Change the number of threads monitoring WebLogic Server].
Normal agents cannot use them.

10.2.4. Tomcat Monitoring

When the following conditions are all met and [Instance Setting] or [Counter Setting] is selected, acquiring the list fails.

- Cannot connect to the configured Tomcat server when starting the agent.
- Counter settings for the configured Tomcat server do not exist.

If this incident occurs, the list can be acquired by right-clicking the performance monitoring node in the topology view when Tomcat server can be connected, and selecting [Performance Monitor Setting] from the displayed pop-up menu to display the [Performance Monitor Setting] dialog box.

10.3. Service Availability Monitoring

- The user management function is not supported for nodes under the probe host.
- In [Alert Message Setting] in the [Probe Terminal Setting] window, you cannot set suppression so that any alerts that exceed the [Monitor Interval Timeout] are allowed only the first time (or [Only the first time] is disabled). Every time a Monitor Interval Timeout occurs, the occurrence will be displayed in Business View.
- In [Alert Message Setting] in the [Probe Terminal Setting] window, you cannot set alerts for [Monitored data delayed].
- The Web scenario monitoring does not support monitoring on Web sites consisting of HTML5 (+CSS3).
- The account using a roaming user profile cannot be specified as an [Run As User].
- User accounts for Web scenario monitoring do not support double-byte characters and UNICODE specific characters.
- Severity in a monitoring counter of the monitoring overtime becomes unknown at the time of use of schedule setting. This severity can't be changed.
- The page contents comparison function (setting the COMPARE_HTML parameter to 1) of the web scenario monitoring function does not support websites that use following composition:

  The web site built using a multiple frames
  The contents which a HTML elements are created dynamically
  (For example, websites on which page contents are created dynamically by using JavaScript and so on the client side, or websites on which page contents are changed at each access.)

- If the "ASCII" type is set for FTP monitoring, the file comparison function cannot be used. (The [files are compared] check box cannot be selected.)

10.4. TopologyCmd IMPORT

In the definition for a single host, if the monitoring definition file in which reporting is set to two or more of the message monitoring, service port monitoring, and performance monitoring functions is imported at a time by using the TopologyCmd command, a wrong action reporting definition might be applied. Importing the monitoring definition file might fail depending on the definition.
You can check whether the monitoring definition file includes two or more reporting settings by using the following tool.

[Tool]

\tool\SysMgrG\TopologyCmd\CheckImportFile
CheckImportFileTool.bat
bom.txt

[How to use]
1. Save the tool (consisting of two files) in the folder that stores the import file.
   (For operating systems other than Windows, move the import file to a Windows OS.)
2. Double-click CheckImportFileTool.bat to execute.
3. Check the result from the prompt.
4. Exit the tool by pressing any key.
5. Divide the import file of the topology view by referring to "TopologyCmd Batch Registration and Setting Detail Confirmation of Monitoring Definitions File Specifications (TopologyCmdSgImpExp_File.pdf)."
   Divide the monitoring function described in the [RELATED_SERVICE] section.
   For details, see "3.2.2 Definition part" of “File Specifications.”

[Notes]
・ This tool is only available for a Windows OS.
・ This tool cannot be used on a remote disk such as a network drive.
Use this tool by copying the import file and this tool in a local disk.
・ If the import file name is changed, this tool cannot be used.
If the file name is changed, edit the file name described in CheckImportFileTool.bat.
The target file names are as follows:
・ Performance.txt
・ MessageView.txt
・ PortMonitor.txt
・ Even if there is a line including the import file commented out by using a symbol such as #, a message indicating that the import file is required to divide is displayed.
Before executing this tool, be sure to delete the commented out definition.

10.5. Note on Overwriteing or Upgrading

When this product is installed by overwriting or upgrading the installed product in the environment where this product of the official license is running, the trial version license might be registered.
If the trial version is registered by overwrite installation, delete the installed trial version by referring to “9.1.2 Trial Version License”

10.6. WebConsole

For the restrictions on WebConsole, see the following:
SystemManager G 7.1 WebConsole Option Release Memo

11. Remarks

11.1. Starting/Stopping SystemManager G

11.1.1. Starting SystemManager G Monitoring Terminal Function

You must start the SystemManager G monitoring terminal function with an OS user account that has the Administrator right.

11.1.2. Restarting SystemManager G

This section describes steps to manually restart SystemManager G.

Restarting the manager (Windows)
To restart your manager manually, restart the Windows service.
Service name: MasterScope UMF Operations Manager__*identifier_**n***

Restarting an agent (Windows)
To restart your agent manually, restart the Windows service.
Service name: MasterScope UMF Operations Agent__*identifier_**n***

Restarting a logical agent (Windows)
To restart your logical agent manually, restart the Windows service.
Service name: MasterScope UMF Operations Logical Agent__*identifier_**n***

Restarting a linker agent (Windows)
To restart your linker agent manually, restart the Windows service.
Service name: MasterScope UMF Operations Agent__*identifier_**n***

Restarting a remote monitor agent (Windows)
To restart your remote monitor agent manually, restart the Windows service.
Service name: MasterScope UMF Operations Remote Agent__*identifier_**n***).

Restarting a probe (Windows)
To restart your probe manually, restart the Windows service.
Service name: MasterScope SystemManager G Probe Agent__*identifier_**n***).

Restarting external IA engine (Windows)

To manually restart external IA engine, please restart the following windows service.
ServiceName: MasterScope UMF Operations RelayManager_***n***

Restarting Manager(HP-UX)

To restart your manager manually, execute the following.

*# sh /sbin/init.d/UMFOperationsManager__identifier_**n*** stop [-i retry interval(sec)] [-c number of retries]↵
*# sh /sbin/init.d/UMFOperationsManager__identifier_**n*** start↵

Restarting an agent (HP-UX)

To restart your agent manually, run the following commands:

sh /sbin/init.d/UMFOperationsAgent__*identifier_**n*** stop [-i retry interval(sec)] [-c number of retries]↵
sh /sbin/init.d/UMFOperationsAgent__*identifier_**n*** start↵

Restarting a logical agent (HP-UX)

To restart your logical agent manually, run the following commands:

sh /sbin/init.d/UMFOperationsLogicalAgent__*identifier_**n*** stop [-i retry interval(sec)] [-c number of retries]↵
sh /sbin/init.d/UMFOperationsLogicalAgent__*identifier_**n*** start↵

Restarting a linker agent (HP-UX)

To restart your linker agent manually, run the following commands:

sh /sbin/init.d/UMFOperationsLinkerAgent__*identifier_**n*** stop [-i retry interval(sec)] [-c number of retries]↵
sh /sbin/init.d/UMFOperationsLinkerAgent__*identifier_**n*** start↵

Restarting IA external engine (HP-UX)

To restart your IA external engine manually, execute the following.

sh /sbin/init.d/UMFOperationsRelayManager_***n*** stop [-i retry interval(sec)] [-c number of retries]↵
sh /sbin/init.d/UMFOperationsRelayManager_***n*** start↵

Restarting the manager (Linux)

To restart your manager manually, run the following commands:

- OS of which system is controlled by init

sh /etc/rc.d/init.d/UMFOperationsManager__*identifier_**n*** stop [-i retry interval(sec)] [-c number of retries]↵
sh /etc/rc.d/init.d/UMFOperationsManager__*identifier_**n*** start↵

- OS of which system is controlled by systemd (e.g. Red Hat Enterprise Linux 7.1)

systemctl stop UMFOperationsManager__identifier_n↵
systemctl start UMFOperationsManager__identifier_n↵

* When init is used in Linux, the process name (the second field) in /proc/1/stat is init. When systemd is used, the process name (the second field) in /proc/1/stat is systemd.

Restarting an agent (Linux)

To restart your agent manually, run the following commands:

- OS of which system is controlled by init

  # sh /etc/rc.d/init.d/UMFOperationsAgent__*identifier_**n*** stop [-i retry interval(sec)] [-c number of retries]↵
  # sh /etc/rc.d/init.d/UMFOperationsAgent__*identifier_**n*** start↵

- OS of which system is controlled by systemd (e.g. Red Hat Enterprise Linux 7.1)

  # systemctl stop UMFOperationsAgent__identifier_n↵
  # systemctl start UMFOperationsAgent__identifier_n↵

  * When init is used in Linux, the process name (the second field) in /proc/1/stat is init. When systemd is used, the process name (the second field) in /proc/1/stat is systemd.

Restarting a logical agent (Linux)

To restart your logical agent manually, run the following commands:

- OS of which system is controlled by init

  # sh /etc/rc.d/init.d/UMFOperationsLogicalAgent__*identifier_**n*** stop [-i retry interval(sec)] [-c number of retries]↵
  # sh /etc/rc.d/init.d/UMFOperationsLogicalAgent__*identifier_**n*** start↵

- OS of which system is controlled by systemd (e.g. Red Hat Enterprise Linux 7.1)

  # systemctl stop UMFOperationsLogicalAgent__identifier_n↵
  # systemctl start UMFOperationsLogicalAgent__identifier_n↵

  * When init is used in Linux, the process name (the second field) in /proc/1/stat is init. When systemd is used, the process name (the second field) in /proc/1/stat is systemd.

Restarting IA external engine (Linux)

To restart your IA external engine manually, execute the following.

- OS of which system is controlled by init

  # sh /etc/rc.d/init.d/UMFOperationsRelayManager_***n*** stop [-i retry interval(sec)] [-c number of retries]↵
  # sh /etc/rc.d/init.d/UMFOperationsRelayManager_***n*** start↵

- OS of which system is controlled by systemd (e.g. Red Hat Enterprise Linux 7.1)

  # systemctl stop UMFOperationsRelayManager__identifier_n↵
  # systemctl start UMFOperationsRelayManager__identifier_n↵

  * When init is used in Linux, the process name (the second field) in /proc/1/stat is init. When systemd is used, the process name (the second field) in /proc/1/stat is systemd.

Restarting an agent (Solaris)

To restart your agent manually, run the following commands:

sh /etc/init.d/UMFOperationsAgent—*identifier_**n*** stop [-i retry interval(sec)] [-c number of retries]↵
sh /etc/init.d/UMFOperationsAgent—*identifier_**n*** start↵

Restarting a logical agent (Solaris)

To restart your logical agent manually, run the following commands:

sh /etc/init.d/UMFOperationsLogicalAgent—*identifier_**n*** stop [-i retry interval(sec)] [-c number of retries]↵

sh /etc/init.d/UMFOperationsLogicalAgent—*identifier_**n*** start↵

Restarting an agent (AIX)

To restart your agent manually, run the following commands:

sh /etc/rc.d/UMFOperationsAgent__*identifier_**n*** stop [-i retry interval(sec)] [-c number of retries]↵
sh /etc/rc.d/UMFOperationsAgent__*identifier_**n*** start↵

Restarting a logical agent (AIX)

To restart your logical agent manually, run the following commands:

sh /etc/rc.d/UMFOperationsLogicalAgent__*identifier_**n*** stop [-i retry interval(sec)] [-c number of retries]↵
sh /etc/rc.d/UMFOperationsLogicalAgent__*identifier_**n*** start↵

The retry option for the stop command is an option to delay a check on whether a service process is terminated. Normally, this option does not need to be specified. When the stop command has been abnormally completed with the return value of not 0, the retry option may be useful.
For example, when you specify "-i 1 –c 5", it means that, immediately after the stop command for a service process has been completed due to timeout, the ps command will make a maximum of 5 checks at intervals of 1 second on whether the service process has been completed. When the service process has vanished during the process termination check, then the check has been completed, and the command also has been completed normally.
Note that if you specify the retry option, ensure that you specify a desired number larger than 0 for the number of retries.
The valid retry interval range to be specified is 1 to 60.

* In UNIX (HP-UX, Linux, Solaris or AIX), restart SystemManager G with an account that has the super-user privilege.
* If you install your SystemManager G specifying the installation folder of the existing MasterScope product, the services and rc script files of the product will be used. You need to reread the explanation above according to your actual environment.
* Where n stands for a service number. For details, refer to "MasterScope Media Release Notes."
* If you install your SystemManager G in an environment where other MasterScope products are using their services and rc script files with the same names as those for the SystemManager G, the rc script files will be renamed so that their last numeric characters are 2 or higher (e.g.: MasterScope UMF Operations Manager_2 and UMFOperationsAgent_3). You need to reread the explanation above according to your actual environment.
* In the case of logical system agents, “Logical” is attached to the names of services and the rc script file (e.g.: MasterScope UMF Operations Logical Agent_2, UMFOperationsLogicalAgent_3).

11.1.3. Predefined Account (Login Name)

The predefined system administration user, Administrator, is automatically created immediately after installing the product. When you log in to your system for the first time, use the following information:

Login name: Administrator
Password: websam

* Change the default Administrator password before operating the system.

11.2. General Monitoring Functions

11.2.1. Knowledge

Knowledge files are saved in the \Svc\knowledge folder on the monitoring terminal. If adding functionality from the default state to the system, reinitializing functionality of the system, or customizing a configuration in the system, use the following files:

File name	Type	Content	Default setting
UMF_*.txt	Business	Product message knowledge	√
Files under the ApplicationNavigator folder	Business	• Application Monitoring performance counter message knowledge • Application Monitoring SAP monitoring message knowledge	√
Files other than above* *ApLog*	AP Log	AP log monitoring knowledge for monitored products	Not Support
Files other than above and except *ApLog*	Business	Message knowledge for monitored products	Not Support
JobCenter_R12.9_Unix folder JobCenter_R12.9_Win folder	Product knowledge	Knowledge files for JOBCenter (HTML)	-

For information on how to import message knowledge files, refer to the following chapter in the manual (help):

[Monitor the message]
[Define message monitoring]
[Define the condition and displaying way of messages storing to category]
[Import the knowledge file]

For information on how to import AP log monitoring knowledge files, refer to the following chapter in the manual (help):

[Monitor the agents]
[Monitor the Agent's log]
[Monitor the application log]
[Define the application log monitoring]
[Define the filter of the application log]

■ **Message knowledge file for each SystemManager G function**

Target function	File name	Remarks
Application Linker	UMF_ApLinker.txt	
Application Log Monitoring	UMF_ApplicationLogMonitor.txt	
Application Management	UMF_ApplicationMonitor.txt	
Application view	UMF_ApplicationView.txt	
Business View	UMF_BusinessView.txt	
Event correlation	UMF_EventCorrelation.txt	

Event Log Monitoring	UMF_EventLogMonitor.txt	
File Monitoring	UMF_FileMonitor.txt	
Invariant analyze	UMF_InvariantAnalyzer.txt	
Manager linkage	UMF_MessageLinker.txt	
Manage the message	UMF_Message.txt	
MCO Linker	UMF_MCOLinker.txt	
Multi Graph View	UMF_MultiGraphView.txt	
Operation control	UMF_OperationView.txt	
Performance Monitoring	UMF_PerformanceMonitor.txt	
Process Monitoring	UMF_ProcessMonitor.txt	
Proxy Service (SSH)	UMF_RemoteConnectCtlSSH.txt	
Proxy Service (API/WMI)	UMF_RemoteConnectCtlWMI.txt	
Scenario control	UMF_ScenarioView.txt	
Service Availability Monitoring	UMF_ProbeOption.txt	
ServiceManagerLinker	UMF_ServiceManagerLinker.txt	
Service port monitoring	UMF_PortMonitor.txt	
Syslog Monitoring	UMF_SyslogMonitor.txt	
Topology View	UMF_TopologyView.txt	
Windows Service Monitoring	UMF_NTServiceMonitor.txt	

* Any category to which one or more of the knowledge files listed above are imported will be automatically created under the [Unified Management Framework] group at the time of installing the manager.
* If you upgrade SystemManager G from a lower version to a higher version, knowledge files that have been updated or newly added will not be imported automatically. You must create a category manually, and import them to it.
* If you install the manager of this product by overwriting the one to which MISSION CRITICAL OPERATIONS/ Application Navigator has been already installed, none of the knowledge files listed above will be imported automatically. Create a category that does not exist in the existing environment, and import any necessary knowledge files to the category.
* These knowledge files cannot be used from the Web Monitoring Terminal. Please use them from regular Monitoring Terminal.

■ **Message knowledge file for other products**

Target product	File name	Remarks
Exchange	Exchange.txt	
EXPRESSCLUSTER (V7.0)	ExpressCluster7.0.txt	
EXPRESSCLUSTER (V8.0)	ExpressCluster8.0.txt	
EXPRESSCLUSTER X	ExpressClusterX.txt	
iStorageManager(Ver.3.3 ~)	iStorage.txt	
MasterScope NetworkManager	NetworkManager.txt	
Oracle10g Database R1	K4ORACLE10gR1_en.txt	
Oracle10g Database R2	K4ORACLE10gR2_en.txt	
Oracle11g Database R1	K4ORACLE11gR1_en.txt	
Oracle11g Database R2	K4ORACLE11gR2_en.txt	
Oracle12c Database R1	K4ORACLE12cR1_en.txt	
Oracle9i Database R2	K4ORACLE9iR2_en.txt	
SQL Server 2000	SQL.txt	
Windows 2000 Server	Windows2000.txt	
Windows Server 2003	Windows2003.txt	

* To apply these knowledge files, you must subscribe to maintenance support service of relevant products and SystemManager G.
* These knowledge files have been created by referring to the causes and solutions corresponding to past inquiries. They are not intended to comprehensively provide all causes and solutions for the target products.
* If you upgrade your product from a lower version to a higher version, the upgraded knowledge file will not reflect the one for the higher version automatically. You need to manually import it again.
* These knowledge files cannot be used from the Web Monitoring Terminal. Please use them from regular Monitoring Terminal.

(Note 1) The release memo for this knowledge file is stored in the following path on the monitoring terminal so that you may refer to it:
<Monitoring terminal install directory>\Svc\bin\Oracle\
NEC Knowledge for Oracle Release Memo rev*.pdf

(Note 2) See the knowledge application procedure that is stored on the following path of MasterScope Media.

■ **AP log monitoring knowledge files for other products**

Target product/function	File name	Remarks
Oracle Clusterware	ApLog_OracleClusterware.txt	(Note 1)
Oracle RDBMS	ApLog_OracleRDBMS.txt	(Note 1)

* To apply these knowledge files, you must subscribe to maintenance support service of relevant products and SystemManager G.
* These knowledge files have been created by referring to the causes and solutions corresponding to past inquiries. They are not intended to comprehensively provide all causes and solutions for the target products.
* If you upgrade your product/function from a lower version to a higher version, the upgraded knowledge file will not reflect the one for the higher version automatically. You need to manually import it again.
* These knowledge files cannot be used from the Web Monitoring Terminal. Please use them from regular Monitoring Terminal.

(Note 1) The release memo for this knowledge file is stored in the following path on the monitoring

terminal so that you may refer to it:
<Monitoring terminal install directory>\Svc\bin\Oracle\
NEC Knowledge for Oracle Release Memo rev*.pdf

■ **Message knowledge files for Application Navigator performance counters**

Target product/function	File name	Remarks
Apache	ApachePerformanceCounter.txt	
IIS	IISPerformanceCounter.txt	
MS SQL Server	MSSQLPerformanceCounter.txt	
Oracle	OraclePerformanceCounter.txt	
Exclusively performance monitoring	PerformanceGeneral1.txt	
Performance monitoring in general	PerformanceGeneral2.txt	
WebLogic Server	WeblogicPerformanceCounter.txt	

* If you upgrade your product/function from a lower version to a higher version, the upgraded knowledge file will not reflect the one for the higher version automatically. You need to manually import it again.

■ **Message knowledge files for Application Navigator SAP monitoring**

Target product/function	File name	Remarks
SAP System Log	SAPsyslog.txt	Added from Ver3.0.1

11.2.2. Resident process names

The resident process names of Application Navigator are as follows.

functions	Windows	UNIX/Linux
Monitoring terminal	SysMonSvc.exe	-
Manager	SysMonMgr.exe	SysMonMgr ProcessExec
Agent	SysMonAgt.exe CollectorProxy64.exe (64-bit mode)	SysMonAgt ProcessExec CollectorProxy64.exe (64-bit mode)
Probe	SysMonAgt.exe	-

11.2.3. Changing Message Management Queue Size on Manager

With an aim to prevent memory resources from being used up because the manager cannot keep up with message processing when narrowing down of messages via filtering does not serve its purpose, the size of the internal queue for message processing on the manager has been set to an upper limit (initial value: 5000 messages) since MISSION CRITICAL OPERATIONS Ver3.4.0/SystemManager Ver5.3.0/Application Navigator Ver3.0.1.

When the upper limit is exceeded, the older messages held in the internal queue will be deleted. The system also will issue a message stating that messages have been deleted from the internal queue. The messages take the following format:

Item	Description
Severity	Warning
Message text	The message was deleted because the maximum number of messages that can be stored in the queue was exceeded.(NUM=%d)(RECVFROM=YYYY/MM/DD hh:mm:ss) (RECVTO=YYYY/MM/DD hh:mm:ss)
Application	Unified Management Framework
Object	Message
Message ID	00270001
Category	Unified Management Framework

* %d indicates the number of deleted messages followed by the range of the date and time the oldest deleted message was received to those when the newest deleted message was received.

To change the size of the internal queue from 5000, follow these steps:

1.Edit the following files on the manager with your text editor:
Windows: <Manager install directory>\Manager\sg\MessageMgr.ini
UNIX : <Manager install directory>/Manager/sg/MessageMgr.ini

```
[Passage]
InputQueueSize=5000
```

Change the "5000" shown above to any desired value.

* If there are no MessageMgr.ini files, create new ones.
* If you specify "0", the upper limit for the queue size will be deselected.

2.Restart the manager.

* If messages are deleted because the upper limit for the internal queue is exceeded, review relevant settings, as the following may have been a possible cause:
  ✓ Too many messages are collected in the manager
    – As logs with identical content may be generated when a failure occurs, enable the "Identical Message Suppression Function" in the log monitoring function on the agents.
    – The filter definitions for monitoring logs on agents are set so that all the logs will be identified as messages. If this is the case, and particularly if you have many managed agents, review the filter definitions so that the agents will not report unnecessary logs as messages.

* Note that a queue is provided for each of the following functions, and the number of items specified for each function is the upper limit.
  ・ Business View

- Message View
- Event correlation
- Operation control
- Scenario control

* The disk size estimation for the internal queue can be calculated using the following formulas.
File size for 1 message: Approx. 3 KB
Message count in 1 queue: 1 to 128
(Since the estimation depends on the number of messages that are processed at the same time, use the maximum number 128 for the estimation.)

11.2.4. Procedure to Stop Accumulating Performance Information

The accumulation of performance information on the manager can be stopped by using the performance data accumulation management function.
For details about how to stop accumulation, see the online manual.
Do not perform this procedure if the performance information display (multi graph view) or form function is being used because the performance information needs to be accumulated on the manager.

11.2.5. Security Settings for Agentless Monitoring

Remote host security settings required to use the agentless monitoring function are described.

For the agentless monitoring function, the WMI security settings and network resource security settings as shown below are required for collecting information via WMI and collecting information via accessing network resources.

■ Security settings for WMI
For the agentless monitoring function, it is necessary to allow communication of the port used by WMI on the remote host because WMI collects information.

[Procedure]
1. Open [Windows Firewall with Advanced Security].
2. In [Inbound Rules]/[Outbound Rules], select and right-click the following item to display [Properties].
   ・Windows Management Instrumentation (DCOM-In)
   ・Windows Management Instrumentation (WMI-In)
3. Select [Allow the connection] in [Operations], and click the [OK] button.

■ Security settings for network resources
For remote monitor agents and remote hosts, access to network resources must be allowed.

[Procedure]
1. Open [Control Panel] - [Windows Firewall].

2. Open the [Exception] tab and check [File and Printer Sharing].

[Steps to set antivirus software]
As antivirus software blocks access to files, agentless monitoring may not operate normally. As an example procedure to set up antivirus software, the following describes steps to set up "VirusScan Enterprise 8.7.0i," an antivirus software product from McAfee, Inc.

1. Start [VirusScan Console].
2. Double-click [Access Protection].
3. Select [Virus prevention outbreak control] and deselect the access blocking [Do not allow read and write from all shares].

11.2.6. About Retaining Information on Agent

If an agent cannot make a connection to its manager due to some failures such as the manager stopped or a network failure, the agent retains the information on itself and will send it to the manager when a connection to the manager is restored.
The pieces of information to be retained by agents are as follows:

- Logs obtained with the event log monitoring function
- Logs obtained with the system log monitoring function
- Logs obtained with the application log monitoring function
- Messages issued by CDO message API

If nothing has been changed after the installation of an agent, the agent will retain 200 packets of each such information.
Each of the event log monitoring function, system log monitoring function, and application log monitoring function stores up to128 logs obtained during one monitoring interval in one packet.
When the upper limit for the number of pieces of retained information is exceeded, the oldest information will be deleted first.

If you want to change the upper limit from 200, follow these steps:

1. Edit the following files on the agent with your text editor:
   Event log monitoring function
   Windows: <Agent installation directory>\Agent\sg\EventLogHelperAgt.ini

   System log monitoring function
   UNIX: <Agent installation directory>/Agent/sg/SysLogHelperAgt.ini

   Application log monitoring function
   Windows: <Agent installation directory>\Agent\sg\ApLogHelperAgt.ini
   UNIX: <Agent installation directory>/Agent/sg/ApLogHelperAgt.ini

   CDO message API
   Windows: <Agent install directory>\Agent\sg\MessageAgt.ini
   UNIX : <Agent install directory>/Agent/sg/MessageAgt.ini

```
[Passage]
OutputQueueSize=200
```

Change the "200" shown above to any desired value.

2. Restart the agent.

* One piece of the retained information uses approximately 3 KB of disk space. As each of the event log monitoring function, system log monitoring function, and application log monitoring stores up to 128 logs in one file when it obtains more than one log during one monitoring interval, it uses a disk space of up to 3 KB x 128 x value of OutputQueueSize for one monitored host.
* If the number of pieces of the retained information were set to a large value, it would be likely that the manager would use up its own memory resources because a vast amount of information would be sent to the manager at once when the connections to it were restored and therefore too much load would be imposed on it. When you have many agents, you must design the value with a care.

11.2.7. About Retaining Information on Remote Monitor Agent

If a remote monitor agent cannot make a connection to its manager due to some failures such as the manager stopped and a network failure, the agent retains the information on itself and will send it to the manager when a connection to the manager is restored.
The pieces of information to be retained by remote monitor agents are as follows:

- Logs obtained with the event log monitoring function
- Logs obtained with the application log monitoring function
- Error messages generated within the remote monitor agent

If nothing has been changed since the installation of a remote monitor agent, the agent retains 200 packets of each of the even log information and application log information for each remote host.
Each of the event log monitoring function and system log monitoring function stores up to128 logs obtained during one monitoring interval in one packet.
A remote monitor agent retains 20,000 messages for the error message information generated within the agent if nothing has been changed since the installation of the agent.
When the upper limit for the number of pieces of retained information is exceeded, the oldest information will be deleted first.

If you want to change the upper limit, follow these steps:

1. Edit the following files on the remote monitor agent with your text editor:
   Event log monitoring function
   <Remote monitor agent installation directly>\Agent\sg\EventLogHelperAgt.ini

   Application log monitoring function
   <Remote monitor agent installation directly>\Agent\sg\ApLogHelperAgt.ini

   Error messages generated within the remote monitor agent

<Remote monitor agent installation directly>\Agent\sg\MessageAgt.ini

```
[Passage]
OutputQueueSize=200
```

Change the "200" shown above to any desired value.
* For MessageAgt.ini, the initial value is 20000.

2. Restart the agent.

* One piece of the retained information uses approximately 3 KB of disk space. As each of the event log monitoring function and application log monitoring stores up to 128 logs in one file when it obtains more than one log in one monitoring interval, it uses a disk space of up to 3 KB x 128 x value of OutputQueueSize for one monitored host.
* If the number of pieces of the retained information were set to a large value, it would be likely that the manager would use up its own memory resources because a vast amount of information would be sent to the manager at once when the connections to it were restored and therefore too much load would be imposed on it. As a remote monitor agent retains the information for the number of its remote hosts, it could use a vast amount of disk space. When you have many remote hosts, you must design this value with a care.
* If you have adopted a duplex configuration of a remote monitor agent, you must configure the above settings both in the active system and in the standby system.

11.2.8. Function to Suppress the Generation of Agent stop/start Messages When the Manager Restarts

The following messages (two types) that are generated when communication with the agent is disconnected because the manager is restarted can be stopped by enabling this function.

Item	Description
Severity	Normal / Abnormal
Message text	Host is running. / Host is stopped.
Application	Unified Management Framework
Object	TopologyService
Message ID	00010001 / 00010002
Category	Unified Management Framework

Perform the following procedure to enable this function.

1. Stop the manager.

2. Create and edit the following ini file.
   [Windows manager]
   <Manager installation directory>\Manager\sg\TopologyMgr.ini
   [UNIX manager]
   <Manager installation directory>/Manager/sg/TopologyMgr.ini

Setting content:

```
[Restart]
StatusKeep=1
```

*Create a file if the file does not exist.
* If the manager is in a cluster environment, the file needs to be created and edited on both the active and standby nodes.
* For Windows, describe using UTF-16 LE code for the character encoding and CR+LF for the line feed code.
For UNIX, describe using UTF-8 code for the character encoding and LF for the line feed code.

3. Start the manager.

■ Note
When this function is enabled, the severity color of each agent on the topology view changes as before to reflect the status of how the manager and agent are connected. If they are disconnected, it reflects the color of "STOP" severity, and if they are connected, it reflects the color of the actual severity for the agent.

11.2.9. Guidelines When Specifying SystemManager G Monitoring Settings

When specifying the monitoring settings for SystemManager G, use the following as a guide for setting the monitoring items and performance monitoring. Use the values are provided only as a guide and the monitoring will not stop immediately when the actual values exceed the described values. Thoroughly verify in advance. In addition, when multiple MasterScope Framework products are installed in the same service, use the total value of the values specified for each product as a guide for settings.

■ Number of connections
The specification for the number of connections to the manager is described below.

Item	Specification value
Number of agents (*1)	250

*1: The total of the number of normal agents, number of logical agents, and the number of hosts that are monitored from the agentless monitoring function.

■ Received message volume
Specifications of message volume received by the manager are as follows: If messages exceeding this value are received, the messages might be deleted because they cannot be processed. For details, see "11.2.3. Changing Message Management Queue Size on Manager". *1 *2

item	Specification value
Business view (*3)	80 messages/sec
Message view (*4)	80 messages/sec

*1. By increasing the queue size by one unit, approx. 80 bytes of memory and approx. 3,000 bytes of free disk space are consumed.

*2. This value is the specification for the number of all messages to be filtered. It is not the number of messages that are matched with the filter and displayed.

*3. The value when the message view is disabled, messages are received with one category, and linkage services (e.g. reporting) are not running.

*4. The value when the business view is disabled, messages are received with one node, and linkage services (e.g. reporting) are not running.

■ Processing when the status of message or agent is changed

Specifications of processing when the status of message or agent is changed are as follows:

item	Specification value
Reporting	1/sec
Recovery	1/sec
Reporting to MCO manager	1/sec
Event correlation	1/sec
Service manager notice	1/sec
Operation of the component waiting for the scenario control message	1/sec
Notice to the upper-level manager	1/sec

■ Accumulated log volume

Specifications of accumulated log volume are as follows:

item	Specification value
Business view	10,000/day
Message view	10,000/day
Audit log	1,000/day
Reporting	100/day
Recovery	100/day
Performance management (*1)	5,000data/min
Event correlation	1,000/day
Service manager notice	100/day
Scenario control	1,000/day
Operation control	1,000/day

*1. For example, specify 1 minute or longer for the monitoring interval when 5,000 counters per manager are specified for performance monitoring.

■ Schedule function

The specifications of the schedule function are as follows:

item	Specification value
Number of schedule definitions	30
Total number of schedule rules	100
Number of calendar definitions	30
Total number of calendar rules	100

■ Agent definition volume

Specifications of agent definitions are as follows:

item	Specification value of the entire managers	Specification value of each agent
Number of monitoring processes (*1)	2500	10
Number of monitoring services	2500	10
Number of monitoring files and directories (*2)	2500	10
Number of monitoring application logs (*3)	2500	10
Number of application log monitoring filters (*4)	5000	20
Number of syslog monitoring filters (*4)	5000	20
Number of event log monitoring filters (*5)	5000	20
Service port monitoring	2500	10
Number of performance monitoring counters	5000 (*6)	20

*1. The following is assumed to be the content of process monitoring.
If there is a lot of definition content larger than this, the specification values that can be specified will be smaller.

Display name: 50 characters
Command line: 50 characters
Default settings for other items (any values for numeric entries)

*2. The following is assumed to be the content of file capacity monitoring.
If there is a lot of definition content larger than this, the specification values that can be specified will be smaller.

Display name: 50 characters
Command line: 50 characters
Default settings for other items (any values for numeric entries)

*3. For monitoring target logs, when the flow volume of recorded logs is large, the loading and filtering processes take a while and the message output might be delayed.

*4. The following is assumed to be the filter content of the application log and syslog monitoring.
If there is a lot of definition content larger than this, the specification values that can be specified

will be smaller.

Message overview: 10 characters Message text: 40 characters Node name: 6 characters Application name: 10 characters Object name: 10 characters Message ID: 10 characters Severity: Specified 　Default settings for other items

*5. The following is assumed to be the filter content of the event log monitoring.
If there is a lot of definition content larger than this, the specification values that can be specified will be smaller.

Message overview: 10 characters Application name: 10 characters Message ID: 10 characters Message text: 40 characters Severity: Specified 　Default settings for other items

*6. When monitoring 5000 counters using performance monitoring function, all counters are registered to the performance management function. Set it so as not to exceed the amount of history accumulation in the performance management function.

■ Manager definition volume
The specifications of the definitions for each manager function are as follows:

item	Specification value
Number of business view categories	200
Number of scheduled categories	50
Number of MCO-linked categories	50
Number of categories linked to manager	50
Number of business view filters (*1, *2)	10000
Number of filters with recovery settings	1000
Number of filters with reporting settings	1000
Number of filters linked to service manager	1000
Number of recovery definitions	100
Number of reporting definition	100
Number of policies linked to the service manager	100
Number of mappings linked to the service manager	150
Number of users	100
Number of user groups	25
Number of print definitions	100
Number of print targets of each print definition	100
Number of setting counters in the entire print definitions	1000
Total number of items in multi graph view	100
Total number of graphs in multi graph view	500
Total number of counters in multi graph view	1000
Number of definitions for the event correlation	1000
Number of filters for the event correlation	1500
Maximum number of monitoring (Number of instances)	10000
Number of definitions for the scenario control	750
Number of scheduled scenarios	250
Number of components for the respective scenarios	100
Number of scenarios for the parallel operation	100
Number of message filters included in the instance in progress of execution	500
Number of simultaneous command issues of the instance in progress of execution	100
Number of operation control definitions	500
Number of scheduled operations	250
Number of commands for the respective operation definitions	10
Number of filters for the respective operation definitions	10

*1. In the cases shown below, "80 messages per 1 second by one manager" mentioned in item A" might not be processed.

- When reporting, recovery or help desk is specified
- When there are many filters to be applied to one message
- When one message matches with filters of multiple categories (not depending on the ACTIVE/HOLD status of category)

*2. The following is assumed to be the filter content of the business view.
If there is a lot of definition content larger than this, the specification value of the number of items that can be specified will be smaller.

Filter name: 10 characters Node name: 255 characters Message ID: 10 characters Message text: 40 characters Related information: One of the following items specified Display name: 16 characters Application: 3 characters Work directory: 20 characters Severity: Specified Reporting: Specified Default settings for other items

- The product is evaluated in the following environment. Specification values mentioned above might not be satisfied depending on the environment.

[Manager evaluation environment]
Windows

OS	Windows Server 2008 R2 Enterprise
CPU	Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz 8 cores
Memory	16GB
Network	1Gbps
Disk	iStorageM500

Linux

OS	Red Hat Enterprise Linux 6.2 (x86_64)
CPU	Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz 8 cores
Memory	16GB
Network	1Gbps
Disk	iStorageM500

HP-UX

OS	HP-UX 11i v3 (Itanium)
CPU	Intel(R) Itanium 2 9100 series processors (1.42GHz, 12MB) 8 cores
Memory	31.97GB
Network	1Gbps
Disk	iStorageM500

- Use the specification values above as a guide. Processing loads of the Application Navigation vary depending on the content defined for the monitoring (e.g. filter application order, regular expression content, with/without linkage settings such as reporting and monitoring interval)

- Filtering is processed from the top to the bottom of the filter definition list sequentially, and the operation of the filter definition whose condition is matched first is performed. The subsequent filtering processes after the first matched filter definition are not performed. In addition, when the conditions are not matched with any filter, prior filtering processing will be wasted. It is recommended to place filters with high matching rate in the top part of the filter definition list and define a deletion definition to delete unnecessary messages because processing loads might become large depending on the situation of the filtering targets.

- When there is unused function, the specification of other monitoring item can be increased in some cases. If the specifications mentioned above are insufficient, contact the support center.

- If you want to confirm the specifications for functions that are not mentioned above, contact the support center.

11.2.10. Upper Limit of the Message Accumulation Amount of the Business View

When more than about 700,000 messages are accumulated per day for one category in the business view, messages after that will not be stored. Just when the date turns to 0:00, the accumulation of messages will be resumed.

11.2.11. Using message filter storage function

This section describes the function of the message monitoring functions to save the message filter information on the console when the console shuts down and load the saved information automatically when the console starts the next time.
This function does not operate immediately after the installation.
Perform the following operations to enable this function.

1. Stop the manager.
2. Create and edit the following *ini* file.

Windows manager:
<Installation path>\Manager\sg\MessageViewMgr.ini

UNIX manager:
<Installation path>/Manager/sg/MessageViewMgr.ini

Settings:

```
[FunctionSwitch]
FilterViewSave=1
```

* <Installation path> indicates the installation path of the manager of SystemManager.
* If the file does not exist, create the file.

* When the manager is in the cluster environment, the file must be created and edited for both active and standby nodes.
* For Windows, use the character encoding “UTF-16 LE code with BOM” and the line feed code “CR+LF”. For UNIX, use the character encoding “UTF-8 code” and the line feed code “LF”.

3. Start the manager.

■ Precautions

- Notes on timing to save the message filter
  The message filter information is saved when the console shuts down. It is not saved when the console does not shut down normally.
  Shut down the console to save the message filter information when the message filter information is updated.
- Storage location of message filter settings
  The message filter settings are saved for each machine where the console is installed. For this reason, the filter setting must be performed for each machine.
- Notes when multiple consoles are running simultaneously (1)
  - When using multiple consoles on the same machine, the message filter information saved by the console that shut down first is overwritten with the message filter information saved by the console that shut down next.
    When creating a new message filter or updating an existing message filter, be sure to stop other monitoring windows on the same machine.
  - If another console is starting or stopping on the same machine when starting a new console, a conflict of access to the file where the message filter is saved occurs and filter information loading might fail.
    If the message filter information is not restored on startup during use in such environment, shut down all consoles on the machine where the problem occurred and restart the console.
- Notes when modifying the option settings
  When the message monitoring option settings are specified to not use the message monitoring itself, the filter information of all consoles is deleted.
  In particular, the information is deleted when one of the following operations is performed.
  - Remove the check mark from [Use Message Monitor], and then click the [OK] button.
  - Remove the check mark from [Show Message View], and then click the [OK] button.

11.2.12. List of Communication Ports

MasterScope SystemManager G uses the network ports shown below. To operate MasterScope SystemManager G normally, change the firewall settings to enable communication through the network ports shown below. If another process is using the port that is to be used by MasterScope SystemManager G, the services of MasterScope SystemManager G cannot be started.

Communication name	Sender	Port	Direction	Receiver	Port	Remarks
Manager-agent communication	Agent	ANY/TCP (*1)	->	Manager	12520/TCP	● The port number of the destination is the default value specified at
	Probe	ANY/TCP (*1)	->	Manager	12520/TCP	

Manager-IA external engine communication	IA external engine	ANY/TCP (*1)	->	Manager	12520/TCP	installation. For the installation, any unused value from 1024 to 65535 can be assigned. ● The destination port can be changed after installation. For details on how to change the port, see the following in the online help. [Change port / connection destination] – [Change the port number]
Manager-SystemManager EventTrap Utility communication	EventTrap Utility	ANY/TCP (*1)	->	Manager	12520/TCP	
Manager-console communication	Console	ANY/TCP (*1)	->	Manager	12521/TCP	
Manager-Web console communication	Web Console	ANY/TCP (*1)	->	Manager	8080/TCP	● The port number of the destination is the default value. It can be changed to any unused value from 1000 to 32767. For details on how to change the port, see the following in the online help. [Before Operation] – [Startup and Shutdown of Web Monitoring Console]
	Web Console	ANY/TCP (*1)	->	Manager	12521/TCP	● The port number of the destination is the default value specified at installation. For the installation, any unused value from 1024 to 65535 can be assigned. ● The destination port can be changed after installation. For details on how to change the port, see the following in the online help. [Change

						port / connection destination] – [Change the port number]
Used within an manager	Manager	ANY/TCP (*1)	->	Manager	12521/TCP	● Used by the command in this product. ● The port number of the destination is the default value specified at installation. For the installation, any unused value from 1024 to 65535 can be assigned. ● The destination port can be changed after installation. For details on how to change the port, see the following in the online help. [Change port / connection destination] – [Change the port number]
Hierarchical configuration of manager	Lower Manager	ANY/TCP (*1)	->	Upper Manager	12520/TCP	The port number of the destination is the default value specified at installation of upper manager of "Port for Agent Internal Communication". Any unused value from 1024 to 65535 can be assigned..
Used within an agent	Agent	ANY/TCP (*1)	->	Agent	12570-12589/TCP	● For the installation, any unused value from 12570 to 12589 can be assigned. ● The destination port can be changed after installation. For details on how to change the port, see

						the following in the online help. [Change port / connection destination] – [Change the port number]
Email report	Manager	ANY/TCP (*1)	->	Mail server	1-32767/TCP	Specify a value between 1 and 32767 according to the mail server (SMTP server) port.
Patlite report (RS232C connection)	Manager	ANY/TCP (*1)	->	Patlite	1-32767/TCP	When "Serial-controlled Type" is specified for the type.
Patlite report (LAN connection	Patlite	ANY/TCP (*2)	->	Manager	1022/TCP (*2)	When "Network Type" is specified for the type.
	Manager	1023/TCP (*3)	->	Patlite	514/TCP	When "Network Type" is specified for the type.
ServiceManager linkage	Manager	ANY/TCP (*1)	->	Service Manager	1-65535/TCP	● Specify a value between 1 and 65535 according to the ServiceManager Server port. ● For details on how to change the port, see the following in the online help. [Register an Incident into ServiceManager]-[Set the Incident Registration Function]-[Set the ServiceManager into which messages will be registered as incidents]

	Sender	Port	Direction	Receiver	Port	Remarks
Oracle monitoring	Agent	ANY/TCP (*1)	->	Oracle	1521/TCP	Alterable on the Oracle side
SQL Server monitoring	Agent	ANY/TCP (*1)	->	SQL Server	1433/TCP	The port when monitoring a default instance
	Agent	ANY/TCP	->	SQL	Fixed	The port when

		(*1)		Server	port/TCP 1434/UDP	monitoring a named instance (fixed port)
	Agent	ANY/TCP (*1)	->	SQL Server	1434/UDP	The port when monitoring a named instance (dynamic port) A TCP port is permitted by program designation (SQL Server installation directory\Binn\sqlserver.exe)
WebLogic monitoring	Agent	ANY/TCP (*1)	->	WebLogic	6202/TCP 6702/TCP	The port when monitoring Admin server Alterable on the WebLogic side
	Agent	ANY/TCP (*1)	->	WebLogic	6212/TCP 6712/TCP	The port when monitoring managed server Alterable on the WebLogic side
Apache monitoring	Agent	ANY/TCP (*1)	->	Apache	80	Alterable on the Apache side
	Agent	ANY/TCP (*1)	->	Apache	ANY/TCP	The port which is specified by a monitor page when using the user definition URL response monitoring
Tomcat monitoring	Agent	ANY/TCP (*1)	->	Tomcat	8999/TCP	Alterable on the Tomcat side
SAP monitoring	Agent	ANY/TCP (*1)	->	SAP	3300/TCP	3300-3399 33<NN> NN=Instance number
JavaAP monitoring	Agent	ANY/TCP (*1)	->	JavaAP	8999/TCP	Alterable on the JavaAP side
WebSphere monitoring	Agent	ANY/TCP (*1)	->	WebSphere	8880/TCP	Alterable on the WebSphere side

(*1) ANY indicates a port number between 1024 and 65535.

(*2) Use a port number between 512 and 1022 when rsh has been started and port number 1022 is used.

(*3) Use a port number between 513 and 1023 when rsh has been started and port number 1023 is used.

For the port numbers used by the agentless monitoring function, "11.2.5Security Settings for Agentless Monitoring"

11.3. Application Monitoring

11.3.1. JIS2004

The following describes the support for JIS2004 characters.

[Common items]
- When JIS2004 characters are used in an area for entering descriptions in connection settings on various monitoring applications, a Supplementary Character consumes two characters. A combined character consumes the number of characters configuring the character.

[Oracle Monitoring]
- Database and character sets must be AL32UTF8.
- National character sets must be AL16UTF16.
- JIS2004 characters that can be handled in user defined SQL execution text are dependent on Oracle specifications.

[IIS Monitoring]
- The instance names (Web site names) of Web Service and Web Service Ext objects support JIS2004 characters.
- If JIS2004 characters are used for the instance names (FTP site names) of FTP Service and FTP Service Ext objects, the instance names will not display correctly. In addition, the State counter cannot be monitored.

[SQL Server Monitoring]
- JIS2004 characters that can be handled in user defined SQL execution text are dependent on SQL Server specifications.

[WebLogic Monitoring]
- There are no particular precautions to note, except for the common items.

[Apache Monitoring]
- In response monitoring, describe URL-encoded character strings in UTF-8 in the monitoring page to monitor pages including JIS2004 characters.

[Tomcat Monitoring]
- There are no particular precautions to note, except for the common items.

[SAP Monitoring]
- There are no particular precautions to note, except for the common items.

[JavaAP Monitoring]
- There are no particular precautions to note, except for the common items.

[WebSphere Monitoring]
- There are no particular precautions to note, except for the common items.

11.3.2. About Path to JAVA_HOME

When specifying the JAVA_HOME parameter in SystemManager G, specify the path to the following file location under JAVA_HOME:

OS	Operational mode of SystemManager G	Path
Windows	32-bit mode	<JAVA_HOME>\bin\server\jvm.dll <JAVA_HOME>\bin\client\jvm.dll
	64-bit mode	<JAVA_HOME>\bin\server\jvm.dll
HP-UX	32-bit mode	<JAVA_HOME>/lib/IA64N/server/libjvm.so <JAVA_HOME>/lib/IA64N/hotspot/libjvm.so
	64-bit mode	<JAVA_HOME>/lib/IA64W/server/libjvm.so <JAVA_HOME>/lib/IA64W/hotspot/libjvm.so
Linux	32-bit mode	<JAVA_HOME>/lib/i386/server/libjvm.so <JAVA_HOME>/lib/i386/client/libjvm.so
	64-bit mode	<JAVA_HOME>/lib/amd64/server/libjvm.so
Solaris	32-bit mode	<JAVA_HOME>/lib/sparc/server/libjvm.so <JAVA_HOME>/lib/sparc/client/libjvm.so
	64-bit mode	<JAVA_HOME>/lib/sparcv9/server/libjvm.so
AIX	32-bit mode	<JAVA_HOME>/lib/ppc/classic/libjvm.so <JAVA_HOME>/lib/ppc/j9vm/libjvm.so
	64-bit mode	<JAVA_HOME>/lib/ppc64/server/libjvm.so

11.3.3. Monitoring Microsoft Products

Monitor metrics

When you monitor Microsoft applications (SQL Server, Internet Information Services), you can use the monitor metrics defined by SystemManager G as well as performance monitor objects (metrics displayed with the performance monitor or an OS tool) provided by Microsoft. Using a combination of these two sets of metrics enables you to perform effective monitoring of the Microsoft applications.
For more information on the performance monitor objects provided by Microsoft, refer to Books Online or "Performance Counter Guide" from Microsoft.
Some monitoring templates may include both the monitor metrics defined by SystemManager G and the performance monitor objects provided by Microsoft.

Adding performance counters

To monitor a performance counter that was added during the operation of an agent, the agent may need to be restarted.

How to apply knowledge

To use a knowledge file that corresponds to a Microsoft application, enable kbfind by following these steps:
Unzip C:\Program Files\NEC\UMF\Operations\Svc\OptionModule\kbfind\kbfind.zip on the monitoring terminal, locate the kbfind.exe that is created in the location to which kbfind.zip was unzipped and place it in C:\Program Files\NEC\UMF\Operations\Svc\bin.

If your environment is using a proxy, proceed with configuration by unzipping the kbfind.zip and referring to the read_kbfind.txt that was created in the location to which the kbfind.zip was unzipped.

11.3.4. WebLogic Server Monitoring

To import and use a knowledge file that corresponds to WebLogic Server, monitor the following log files by using the application log monitoring function:
- Windows: <DOMAIN_HOME>\servers\<SERVER_NAME>\logs\<SERVER_NAME>.log
  e.g.)
  C:\Oracle\Middleware\user_projects\domains\base_domain\servers\AdminServer\logs\AdminServer.log
- UNIX : <DOMAIN_HOME>/servers/<SERVER_NAME>/logs/<SERVER_NAME>.log
  e.g.)
  /u01/app/oracle/Middleware/user_projects/domains/base_domain/servers/AdminServer/logs/AdminServer.log

Note that you must set the log files for WebLogic so that they will not rotate.

11.4. Operation Control Function

The operation control function displays just the portion of the command name by removing the directory path from the entire character string specified in the command field in some windows.
If the character of "\" or "/" not intended to be a part of the directory path is included in a command name, the command name may not displayed correctly.
Creating an OperationMgr.ini file or editing the existing one enables any character string entered in the command field to be displayed as it is.

Path to OperationMgr.ini file

Windows manager:
<Installation path>\Manager\sg\OperationMgr.ini

HP-UX/Linux manager:
<Installation path>/Manager/sg/OperationMgr.ini

- ※ <Installation path> indicates the installation path of the SystemManager G manager.
- ※ If these files are not present, create them.
- ※ If the manager is in a cluster environment, the files must be created or edited in the active system and in the standby system.
- ※ Once you edited the OperationMgr.ini, restart the manager to reflect it.

The OperationMgr.ini file is created or edited with your text editor.
The following list the definition item in the OperationMgr.ini file.

[CmdDisplaySettings] section

Key	Valid Range	Default Value	Meaning

CmdDispMode	0 or 1	0	Specify whether any character string entered in the command field on the command setting window is displayed as it is. 0: Display only the command name 1: Display the entire entered character string as it is

※ In windows, describe “UTF-16 LE code” for the character code and “CR+LF” for the new line code.
In Unix, describe “UTF-8 code” for the character code and “LF” for the new line code.

Setting example:

```
[CmdDisplaySettings]
CmdDispMode=1
```

The following lists the windows for which the above display method is set:

- Action definition window ([Action Definition] tab)
- Action execution window ([Action Definition] tab)
- Command detailed history widow (tree section)

For details of each window, refer to the following chapters of the manual (help):
[Using the Operation control]
-[How to Define an Action]
-[Define an action]
-[Set an action definition (command execution)]
-[Operate an action]
-[Run an action manually]
-[Refer to the history of action executions]
-[Refer to the details of the action history (command results)]

11.5. Message Interactions

The message interaction function is able to link Network Node Manager 7.01/7.50/7.51/7.53 (HP-UX Version), ESMPRO/ServerManager and MasterScope SystemManager Version 2.x and monitor alert messages gathered from these products in an integrated manner.

To use this feature, install and configure the linker module, "SystemManager Event Trap Utility". Refer to the manual and “System Manager Event Trap Utility readme.pdf”(SysMEvTrap_readme_Win.pdf, SysMEvTrap_readme_HP.pdf) in detail.

12. Troubleshooting

12.1. Diagnosis Information Collection Tool

The collected information common to the platforms can be collected with an information collection tool, common to all the products, provided with MasterScope Media. The information to be collected on each monitored target should be collected separately, without using the information collection tool.
To use the information collection tool, copy the following file to your machine from the MasterScope Media and ensure that you read the release memo in the same folder carefully. Note that DVD drive and mount point must be reread where appropriate.

- Windows (assuming the DVD drive to be drive E)
  E:\tools\dawebsaminfo\Windows\dawebsaminfo.bat
- UNIX (assuming the DVD mount point to be /SD_CDROM)
  /SD_CDROM/tools/dawebsaminfo/UNIX/dawebsaminfo.sh

12.2. Diagnosis Information to be Collected

■ **Considerations when collecting information**
If you want to collect information, you are advised to do so after you stop services in SystemManager G.

For more information, refer to the following in the product help menu:
[Before You Start Operation] - [Start and Stop of manager/agent functions]
- [Open and Close the monitoring window]

12.2.1. Diagnosis Information of Manager

■ **Windows manager**
*The following information can be collected with the information collection tool.

- SystemManager G log and sg directories
  <InstallDir>\Manager\log
  <InstallDir>\Manager\sg
  * If you are in a cluster environment, collect information from the following:
  <Shared disk directory>\Manager\sg

- File list in the bin directory on SystemManager G (dir command)
  <InstallDir>\Manager\bin

- OS version (ver command)

- hosts file
  %SystemRoot%\system32\drivers\etc\hosts

- Results from executing netstat -an

- Event logs
  Collect files that have been saved in the form of .evt regarding "system" and "application" event logs.

*The following information cannot be collected with the information collection tool. Please collect them manually.

- Crash dump
  Sample a crash dump by referring to "9.5.10. Output of Crash Dump in case of Trouble in the Windows Environment."

■ **HP-UX/Linux manager (common)**

*The following information can be collected with the information collection tool.

- SystemManager G log and sg directories
  <InstallDir>/Manager/log
  <InstallDir>/Manager/sg
  * If you are in a cluster environment, collect information from the following:
  <Shared disk directory>/Manager/sg

- File list in the bin directory on SystemManager G (ls -l)
  <InstallDir>/Manager/bin

- OS version (uname -a)

- hosts file
  /etc/hosts

- Results from executing netstat -an

- Results from executing kctune and kctune -s

- Results from executing swapinfo

- syslog
  Under /var/adm/syslog directory

- swlist
  Results from executing swlist -l product

12.2.2. Diagnosis Information of Agent

■ **Windows agent (common)**

*The following information can be collected with the information collection tool.

- SystemManager G log and sg directories
  <InstallDir>\Agent\log
  <InstallDir>\Agent\sg
  * If you are in a cluster environment, collect information from the following:
  <Shared disk directory>\Agent\sg

- File list in the bin directory on SystemManager G (dir command)
  <AppNaviInstallDir>\Agent\bin

- OS version (ver command)

- hosts file
  %SystemRoot%\system32\drivers\etc\hosts

- Results from executing netstat -an

- Event logs
  Collect files that have been saved in the form of .evt regarding "system" and "application" event logs.

*The following information cannot be collected with the information collection tool. They must be collected manually.

- Crash dump
  Sample a crash dump by referring to "9.5.10. Output of Crash Dump in case of Trouble in the Windows Environment."

■ **Windows agent (Oracle)**

*The following information cannot be collected with the information collection tool. They must be collected manually.

- Oracle instance name
- Oracle database name, service name (for RAC monitoring)

- Oracle setting files
  <ORACLE_HOME>\NETWORK\ADMIN\listener.ora
  <ORACLE_HOME>\NETWORK\ADMIN\sqlnet.ora
  <ORACLE_HOME>\NETWORK\ADMIN\tnsnames.ora

- Results from executing srvctl (for RAC monitoring)
  srvctl config database
  srvctl status database -d <database name> -S 1
  srvctl config service -d <database name> -S 1

srvctl status service -d <database name> -S 1
* Specify the result output from "srvctl config database" in "<database name>".

- System environment variable PATH
  Obtain PATH from the environment variable.

- List of files under <ORACLE_HOME>
  Execute from the command prompt.
  > cd <ORACLE_HOME>
  > dir /s > ./dir.txt
  * When 64-bit Oracle Database is monitored in 32-bit mode, acquire the dir results of both the 64-bit Oracle Database and 32-bit Oracle Client.

■ **Windows agent (IIS)**

*The following information cannot be collected with the information collection tool. They must be collected manually.

- Service status
  FTP Publishing Service (IIS 7.0)
  Microsoft FTP Service (IIS 7.5 or later)
  World Wide Web Publishing Service

- Log files for IIS (in case of default)
  %SystemDrive%\inetpub\logs\LogFiles
  Collect only files that have the same date as the date the failure occurred

■ **Windows Agent (SAP)**

*The following information cannot be collected with the information collection tool. They must be collected manually.

SAP system information
Collect a screenshot of the SAP GUI [System Menu]-[Status] window.
Also, take notes of the server name, if the Host Data - Server Name does not fit inside the screenshot.

*System log information
After displaying the date log checked at SM21,
List of files saved in the HTML format at [System Menu]-[List]-[Save]-[Local File]

■ **HP-UX/Solaris/Linux/AIX agent (common)**

*The following information can be collected with the information collection tool.

- SystemManager G log and sg directories
  <InstallDir>/Agent/log
  <InstallDir>/Agent/sg
  * If you are in a cluster environment, collect information from the following:
  <Shared disk directory>/Agent/sg

- config file for SystemManager G

<InstallDir>/Agent/bin/config

- File list in the bin directory on SystemManager G (ls -l)
  <InstallDir>/Agent/bin

- OS version (uname -a)

- hosts file
  /etc/hosts

- Results from executing netstat -an

- Results from executing kctune and kctune -s

- Results from executing swapinfo

- syslog
  Under /var/adm/syslog directory

- swlist
  Results from executing swlist -l product

■ **HP-UX/Solaris/Linux/AIX agent (Oracle)**

*The following information cannot be collected with the information collection tool.

- Oracle instance name
- Oracle database name, service name (for RAC monitoring)

- Oracle setting files
  <ORACLE_HOME>/network/admin/listener.ora
  <ORACLE_HOME>/network/admin/sqlnet.ora
  <ORACLE_HOME>/network/admin/tnsnames.ora

- Results from executing srvctl (for RAC monitoring)
  srvctl config database
  srvctl status database -d database name -S 1
  srvctl status service -d database name -S 1
  * Specify the result output from "srvctl config database" in "database name".

- List of files under <ORACLE_HOME>
  Execute from the command prompt.
  >> cd <ORACLE_HOME>
  >> ls -lR > ./ls.txt
  * When 64-bit Oracle Database is monitored in 32-bit mode, acquire the dir results of both the 64-bit Oracle Database and 32-bit Oracle Client.

12.2.3. Diagnosis Information of Monitoring Terminal

- SystemManager G　log and sg directories
  <InstallDir>\Svc\log
  <InstallDir>\Svc\sg

- File list in the bin directory on SystemManager G (dir command)
  <InstallDir>\Svc\bin

- OS version (ver command)

12.2.4. Windows Probe Error Information Sampling

When a monitored event in the Windows probe is reported to Business View, you can check what was returned from an IT service (a displayed window(s) for the service availability monitoring and details of exchanged messages for other monitoring activities) when the monitoring fails.

E.g. 1: When a scenario cannot be replayed in Web scenario monitoring
When a Web scenario cannot be replayed, the following events will be generated:
[AGT" <*Probe hostname*> "]Failed to monitor Web Scenario <*Scenario name*> (ID: <*Scenario ID*>) Pattern match failed at <StepNo> (<*Step description*>). Pattern string (<*Pattern matching character string*>) doesn't exist

* The above messages will be displayed when the window is displayed, but the pattern character string is searched for and not found in the window.

[AGT" <*Probe hostname*> "]Failed to monitor Web Scenario <*Scenario name*> (ID: <*Scenario ID*>) An object of a click target wasn't found at Step<StepNo> (<*Step description*>).

* The above messages will be displayed when the window is displayed, but objects, such as buttons or links on which the operations in the next Step will be performed, are searched for and not found in the window.

When the above messages are displayed in Business View, the window images and HTML sources that make up the windows will be output to the following directory on the Windows probe terminal.
* For comparison, the normal window images and HTML sources will also be output to the same directory.

<Output directory>
<InstallDir>OperationsProbe\Agent\sg\AppNaviPrb\error_info\WebScenario

<Output file name>
•Abnormal information
Cap_Html_E_<*Monitor ID*>_<Identifier>.html
Cap_Window_E_<*Monitor ID*>_<Identifier>.gif

*Specify a desired MIME type for captured images from the setting window for Scenario Writer.

•Normal information

Cap_Html_N_<*Monitor ID*>_<Identifier>.html

Cap_Window_N_<*Monitor ID*>_<Identifier>.gif

E.g. 2: When mail monitoring fails because there is a problem with a monitored target

The following event indicating a failure in a monitored target will be generated:

SMTP protocol error occurred when sending mail.

* This message will be output when an unexpected response is returned from the transmission server.

When the above message is displayed in Business View, a text file that has recorded the protocol information exchanged with the server will be output to the following directory on the Windows probe terminal.

* For comparison, the normal protocol information will also be output to the same directory as a text file.

<Output directory>

<InstallDir>OperationsProbe\Agent\sg\AppNaviPrb\error_info\SMTP

<Output file name>

Cap_SMTP_E_<*Monitor ID*>_<Identifier>.txt .....When completed unsuccessfully

Cap_SMTP_N_<*Monitor ID*>_<Identifier>.txt .....When completed successfully

Note that if an error occurs when receiving a mail, read "POP" for “SMTP” in the names of the directories and the text files.

The similar information will be output in the cases of DNS, TCP and FTP monitoring.

* In the names of the output directories and text files, “SMTP” will be replaced with “DNS”, “TCP” and “FTP” respectively.