MasterScope MISSION CRITICAL OPERATIONS Ver4.3 Release Memo

June 2016
NEC Corporation

Thank you for your continued patronage of our products. This time, we would like to explain how to operate "MasterScope MISSION CRITICAL OPERATIONS" in your company.

CONTENTS

1) Adobe, the Adobe logo, and Acrobat are trademarks or registered trademarks of Adobe Systems Incorporated in the United States and other countries.
2) Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and other countries.
   In addition, trademarks of Microsoft products included in this guide are registered trademarks of Microsoft Corporation in the United States and other countries.
3) Intel, Pentium, and Itanium are trademarks or registered trademarks of Intel Corporation and its affiliated companies in the United States and other countries.
4) Introscope is a registered trademark of CA Technologies.
5) UNIX is a registered trademark of The Open Group in the United States and other countries.
6) HP-UX are 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.
7) Oracle, Exadata, Solaris are registered trademarks of Oracle Corporation and its subsidiary and affiliated companies in the United States and other countries.
8) Linux is a registered trademark of Mr. Linus Torvalds in the United States and other countries.
9) Red Hat is a registered trademark of Red Hat Software, Inc. in the United States.
10) SUSE is a trademark of Novell, Inc. in Japan and other countries.
11) AIX is a registered trademark of International Business Machines Corp. in the United States.
12) PATLITE is a registered trademark of Patlite Corporation.
13) In addition, proper nouns such as company names and product names included in this guide are trademarks or registered trademarks of their respective companies.
14) "TM" and the ® mark are omitted in text and figures in this guide.
15) Specifications and designs of windows included in this guide are subject to change for improvement without notice.

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).

1. Product Description

1.1. Product Contents

MasterScope MISSION CRITICAL OPERATIONS is intended to implement the stable operation of open mission critical systems through failure monitoring from the viewpoint of business and recovery assistance with knowledge databases. This product provides the following functions.

Standard functions

- Service process monitoring function
  Monitors whether a process or service is dead or alive
- 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 function
  Displays the operating status (such as CPU/memory usage) of servers in graphical format
  Monitors whether a threshold value is exceeded and reports such in a message
  Accumulates data on the operating status of servers as statistical information
- Configuration information monitoring function
  Collects and displays the information on configured equipment, such as CPU and SCSI devices, making up a server.
- Message monitoring function
  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.
- Knowledge management function
  Navigates a user through appropriate countermeasures against subsequent failures that will occur in the future by accumulating past failure information and recovery methods
- Reporting function
  Reports a failure occurrence via a warning light and mail
- 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
- Event collection function
  Analyzes the correlation between received messages and then displays a new message according to the results of the analysis
- Clustering system monitoring function

Enbales a user to monitor a clustering system by working with NEC ExpressCluster.

- 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 the document contained under the following path in MasterScope Media for setup procedures.
  \doc\MCO\CDO_relememo.pdf
- 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.
- Service port monitoring function
  Provides functions to manage and display the service ports of the agent in the system.

Optional functions

- 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.

  We may refer to this feature as IA feature in the following documents.

  \doc\MCO\IA_relememo.pdf

MasterScope SystemManager specific functions

This product includes MasterScope SystemManager, which provides the functions described below.

- Message monitoring function

  Displays message information generated on each system on a window.
- External product linking function

  Enables users to obtain message information by working with an external product (such as ESMPRO/ServerManager, MasterScope Network Node Manager).

  For details such as creating the environment, etc. refer to the documents stored in the following paths on MasterScope Media:

  ¥doc¥SysMgr¥SysMEvTrap_readme_Win.pdf

1.2. About the Manual

The manual for this product is described in the chm format and recorded in the following path of MasterScope Media

\doc\MCO\MISSION CRITICAL OPERATIONS.chm

It can also be referenced via a monitoring window after installing the product.

1.3. Installation Media

This product is installed from MasterScope Media (DVD-ROM media).

2. System Environment

This package runs on the following hardware and software:

2.1. List of Supported Platforms

OS Name(*4)	Manager Function	Agents Function	Remote Monitoring Agent Function	Monitoring Terminal Function	IA external engine
Windows Server 2008 (SP1, SP2) (32bit)	○(*1)	○(*1)	×	○	○
Windows Server 2008 (SP1, SP2) (x64)	○(*1)	○(*1)	×	○	○
Windows Server 2008 R2 (No SP applied, SP1) (Intel64)	○(*1)	○(*1)	○(*1)	○	○
Windows Server 2012 (Intel64)	○(*1)	○(*1)	○(*1)	○	○
Windows Server 2012 R2 (Intel64)	○(*1)	○(*1)	○(*1)	○	○
Windows Vista Business, Enterprise, Ultimate (SP1, SP2)（IA32）	×	×	×	○	×
Windows Vista Business, Enterprise, Ultimate (SP1, SP2)（Intel64）	×	×	×	○	×
Windows 7 Professional, Enterprise, Ultimate (No SP applied, SP1) (IA32)	×	×	×	○	×
Windows 7 Professional, Enterprise, Ultimate (No SP applied, SP1) (Intel64)	×	×	×	○	×
Windows 8 Pro, Enterprise (IA32)	×	×	×	○	×
Windows 8 Pro, Enterprise (Intel64)	×	×	×	○	×
Windows 8.1 (IA32)	×	×	×	○	×
Windows 8.1 (Intel64)	×	×	×	○	×
Windows 10 Pro, Education, Enterprise (32bit)	×	×	×	○	×
Windows 10 Pro, Education, Enterprise (x64)	×	×	×	○	×
HP-UX 11i v3 (Itanium)	○(*1)	○(*1)	×	×	○
Red Hat Enterprise Linux AS4, 4.5, 4.6, 4.7, 4.8 (x86)	×	○(*1)	×	×	○
Red Hat Enterprise Linux AS4, 4.5, 4.6, 4.7, 4.8 (x86_64)	×	○(*1)	×	×	○
Red Hat Enterprise Linux ES4, 4.5, 4.6, 4.7, 4.8 (x86)	×	○(*1)	×	×	○
Red Hat Enterprise Linux ES4, 4.5, 4.6, 4.7, 4.8 (x86_64)	×	○(*1)	×	×	○
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (x86)	×	○(*1)	×	×	○
Red Hat Enterprise Linux 5, 5.1, 5.2, 5.3, 5.4, 5.5 (x86_64)	×	○(*1)	×	×	○

Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86)	○(*1)	○(*1)	×	×	○
Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 (x86_64)	○(*1)	○(*1)	×	×	○
Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7 (x86)	○(*1)	○(*1)	×	×	○
Red Hat Enterprise Linux 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 7.1 (x86_64)	○(*1)	○(*1)	×	×	○
SUSE Linux Enterprise Server 10 (SP3, SP4) (x86)	×	○(*1)	×	×	×
SUSE Linux Enterprise Server 10 (SP3, SP4) (x86_64)	×	○(*1)	×	×	×
SUSE Linux Enterprise Server 11 (No SP applied, SP1, SP2, SP3) (x86)	×	○(*1)	×	×	×
SUSE Linux Enterprise Server 11 (No SP applied, SP1, SP2, SP3) (x86_64)	×	○(*1)	×	×	×
Oracle Enterprise Linux 5.5 (x86_64)(*2)	×	○(*1)	×	×	×
Oracle Linux 6.2, 6.4 (UEK) (x86)	○(*1)	○(*1)	×	×	○
Oracle Linux 6.2, 6.4 (UEK) (x86_64)	○(*1)	○(*1)	×	×	○
Solaris 10 (SPARC)	×	○(*1)	×	×	×
Solaris 11 (SPARC)	×	○(*1)	×	×	×
AIX 6.1 (TL9)	×	○(*1)	×	×	×
AIX 7.1 (TL0 ~ TL3)	×	○(*1)	×	×	×

(*1) Support running on a clustering system

(*2) Only Exadata environments are supported.

(*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 "2.3 Platforms Supported by Remote Hosts".

(*4) Only English version is supported.

2.2. System Requirements

- Windows manager/agent/Remote Monitoring Agent Function/monitoring terminal/IA external engine

Item		Description
CPU	Manager function	Intel Pentium III 1GHz or higher is recommended Use Invariant Analyze function: Intel Dual Core Xeon or later, or any compatible equivalent processor (Note 5) 64bit CPU(x64) is recommended when using IA function.
	Agent function Terminal function Remote Monitoring Agent Function	Intel Pentium III 1GHz or higher is recommended

	IA external engine function	Intel Dual Core Xeon or later, or any compatible equivalent processor Recommend 64bit CPU(x64)
System Memory	Manager function	64 MB or more (128 MB or more is recommended) Use IA function: 1GB or more (2GB or more is recommended)
	Agent function	32 MB or more (64 MB or more is recommended)
	Remote Monitoring Agent Function	32 MB or more (64 MB or more is recommended)
	Monitoring terminal function	64 MB or more (128 MB or more is recommended) Use 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 1)	Manager function	200MB or more (300 MB or larger when using the included database)
	Agent function	100MB or more
	Remote Monitoring Agent Function (Note 10) (Note 11)	100MB or more
	Monitoring terminal function	100MB or more
	IA external engine function	100MB or more
Network		100Mbps LAN is recommended
OS (Note 6) (Note 17)	Manager function	Please refer to 2.1LIST OF SUPPORTED PLATFORMS x64 Edition is recommended when using IA function in manager function and external engine function.
	Agent function	
	Remote Monitoring Agent Function	
	Monitoring terminal function	
	IA external engine function	
Required software	Manager function	Duplicating manager: ExpressCluster(Ver X) or Microsoft Failover Cluster(MSFC/WFSC)
	Remote Monitoring Agent Function	.NET Framework is required to perform hypervisor monitoring by using the agentless monitoring function.(Note 16)
	Monitoring	Internet Explorer 9, 10, 11(Note 13)

	terminal function (When using Web Monitoring View)	

■ HP-UX manager/agent/ IA external engine

Item		Description
CPU	Manager function	Itanium
	Agent function	Itanium
	IA external engine function	Itanium
System Memory	Manager function	64 MB or more (128 MB or more is recommended) Use IA function: 1GB or more (2GB or more is recommended)
	Agent function	32 MB or more (64 MB or more is recommended)
	IA external engine function	1 GB or more (2 GB or more is recommended)
Disk (free size) (Note 1)	Manager function	500MB or more (600 MB or larger when using the included database)
	Agent function	100MB or more
	IA external engine function	100MB or more
Network		100Mbps LAN is recommended
OS (Note 2)	Manager function	Please refer to 2.1LIST OF SUPPORTED PLATFORMS
	Agent function	
	IA external engine function	
Required software	Manager function	Package：HPUXLocales(Only HP-UX11iv3) Duplicating manager: MC/ServiceGuard
	Manager function Agent function IA external engine function (Only HP-UX11iv3)	Package：HPUXLocales

Note) For the required software, packages required to be installed additionally based on the minimum OS configuration installation are described.

■ Linux manager/agent/ IA external engine

Item		Description
CPU	Manager function	Intel Pentium III 1GHz or higher is recommended Intel dual-core Xeon or subsequent ones or an equivalent compatible processor is recommended when using IA function. (Note 5) Recommend 64bit CPU(x64) when using IA function.

	Agent function	Intel Pentium III 1GHz or higher is recommended
	IA external engine function	Intel dual-core Xeon or subsequent ones or an equivalent compatible processor is recommended. Recommend 64bit CPU(x64)
System Memory	Manager function	64 MB or more (128 MB or more is recommended) 1 GB or more (2 GB or more is recommended) when using IA function
	Agent function	32 MB or more (64 MB or more is recommended)
	IA external engine function	1 GB or more (2 GB or more is recommended)
Disk (free size) (Note 1)	Manager function	200MB or more (300 MB or larger when using the included database)
	Agent function	100MB or more
	IA external engine function	100MB or more
Network		100Mbps LAN is recommended
OS(Note 12)	Manager function	Please refer to 2.1LIST OF SUPPORTED PLATFORMS x64 Edition is recommended when using IA function in manager function and external engine function.
	Agent function	
	IA external engine function	
Required software (Note 3)(Note 4)	Manager function /Agent function/ IA external engine function (Red Hat Enterprise Linux 4)	Package：bc(Required in agent function.) Package：compat-libstdc++-33(32bit) Package：e2fsprogs (32bit) Package：glibc-2.3.4-2.25 or later(32bit) Package：libgcc (32bit) Package：ncompress or gzip Package：ncurses (32bit) Package：net-tools Package：procps Package：redhat-lsb Package：rpm-build (Note 14) Package：sg3_utils(Required in agent function.) Package：sysstat(One of 5.0.5, 6.0.2, 7.0.0, 7.0.2 Not required in IA external engine function.) For a 64-bit environment, you need the following packages in addition to 32-bit versions of the packages: Package：libgcc (64bit) Package：glibc (64bit) Package：libstdc++ (64bit)

	Manager function /Agent function/IA external engine function (Red Hat Linux5 or before) (Oracle Enterprise Linux 5.5(x86_64))	Package：bc(Required in agent function.) Package：compat-libstdc++-33(32bit) Package：e2fsprogs-libs (32bit) Package：glibc (32bit) Package：libgcc (32bit) Package：ncompress or gzip Package：ncurses (32bit) Package：net-tools Package：procps Package：redhat-lsb Package：rpm-build (Note 14) Package：rsh(Required in manager function.) Package：sysstat(One of 5.0.5, 6.0.2, 7.0.0, 7.0.2 Not required in IA external engine function.) For a 64-bit environment, you need the following packages in addition to 32-bit versions of the packages: Package：libgcc (64bit) Package：glibc (64bit) Package：libstdc++ (64bit)
	Manager function /Agent function/IA external engine function (Red Hat Enterprise Linux6) (Red Hat Enterprise Linux7) (Oracle Linux 6)	Package：bc(Required in agent function.) Package：compat-libstdc++-33 (32bit) Package：glibc (32bit) Package：libgcc (32bit) Package：libuuid (32bit) Package：ncompress or gzip Package：ncurses-libs (32bit) Package：redhat-lsb Package：rpm-build (Note 14) Package：net-tools (Note 15) Package：rsh(Required in manager function.) Package：sysstat (9.0.4 required in Red Hat Linux6. 10.1.5 required in Red Hat Linux7.Not required in IA external engine function.) For a 64-bit environment, you need the following packages in addition to 32-bit versions of the packages: Package：libgcc (64bit) Package：glibc (64bit) Package：libstdc++ (64bit)

	Agent function (SUSE Linux Enterprise server 10)	Package：bc Packaget：glibc(32bit) 32bit OS：glibc-2.4-31.77.76.1 or later 64bit OS：glibc-32bit-2.4-31.77.76.1 or later Packaget：glibc-locale(32bit) 32bit OS：glibc-locale-XXXXX.rpm 64bit OS：glibc-locale-32bit-XXXXX.rpm Package：gzip Package：libstdc++33 (32bit) 32bit OS：libstdc++33-XXXXX.rpm 64bit OS：libstdc++33-32bit-XXXXX.rpm Package：lsb Package：procps Package：net-tools Package：scsi Package：e2fsprogs (32bit) 32bit OS：e2fsprogs -XXXXX.rpm 64bit OS：e2fsprogs-32bit-XXXXX.rpm Package：libgcc (32bit) Package：ncurses (32bit) 32bit OS：ncurses-XXXXX.rpm 64bit OS：ncurses-32bit-XXXXX.rpm Package：sysstat(8.0.4)

	Agent function (SUSE Linux Enterprise Server 11)	Package : bc Packaget : glibc(32bit) 32bit OS : glibc-XXXXX.rpm 64bit OS : glibc-32bit-XXXXX.rpm Packaget : glibc-locale(32bit) 32bit OS : glibc-locale-XXXXX.rpm 64bit OS : glibc-locale-32bit-XXXXX.rpm Package : gzip Package : libstdc++33 (32bit) 32bit OS : libstdc++33-XXXXX.rpm 64bit OS : libstdc++33-32bit-XXXXX.rpm Package : lsb Package : procps Package : net-tools Package : libgcc43 (32bit) 32bit OS : libgcc43-XXXXX.rpm 64bit OS : libgcc43-32bit-XXXXX.rpm Package : libncurses5 (32bit) 32bit OS : libncurses5-XXXXX.rpm 64bit OS : libncurses5-32bit-XXXXX.rpm Package : libuuid1 (32bit) 32bit OS : libuuid1-XXXXX.rpm 64bit OS : libuuid1-32bit-XXXXX.rpm Package : sysstat(8.1.5)

Note) For the required software, packages required to be installed additionally based on the minimum OS configuration installation are described.

■ Solaris Agent

Item		Description
CPU		UltraSPARC-II i 650MHz or higher is recommended
System Memory		32MB or more (64MB or more is recommended)
Disk (free size) (Note 1)		100MB or more
Network		100Mbps LAN is recommended
OS (Note 2)		Please refer to 2.1LIST OF SUPPORTED PLATFORMS
Required software	Solaris 10	Package : SUNWjiu8 Package : SUNWuiu8 Package : SUNWaccu Package : SUNWaccr Package : SUNWbash Patch of latest libC

	Solaris 11	Package：SUNWiconv-unicode Package：SUNWuiu8 Package：SUNWbash Package：compatibility/ucb Patch of latest libC

Note) For the required software, packages required to be installed additionally based on the minimum OS configuration installation are described.

■ AIX Agent

Item	Description
CPU	POWER5 1.6GHz or higher is recommended
System Memory	32MB or more (64MB or more is recommended)
Disk (free size)(Note 1)	100MB or more
Network	100Mbps LAN is recommended
OS(Note 8)	Please refer to 2.1LIST OF SUPPORTED PLATFORMS
Required software	bos.adt.insttools (Note 15) bos.iconv and bos.rte.iconv xlC.rte bos.rte libpthreads bos.rte libc bos.rte bind_cmds bos.rte security bos.rte libcur bos.net.ncs bos.acct bos.perf.tools bos.net.tcp.client UTF-8 language environment (Note 7)

Note) For the required software, packages required to be installed additionally based on the minimum OS configuration installation are described.

(Note 1) This does not include areas such as those for data files to be created following installation of the package.

(Note 2) The following OS patches may be required, depending on the OS being used.

OS	patch
HP-UX 11i v3	PHCO_41407 or later PHKL_41967 or later

It is recommended to apply the following patches. Note that these patches are automatically included in Solaris 10 Release which was released in June 2007 or later releases.

OS	patch
Solaris10	125100-04 Kernel Update Patch 120473-05 libc nss ldap PAM zfs Patch 125800-01 Fault Manager Patch

(Note 3) If you use Red Hat Enterprise Linux AS/ES 4.0, there might be a malfunction depending on the version of procps. Please refer to "10.3 Using Red Hat Linux AS/ES 4.0" in detail and actions.

(Note 4) If you use Red Hat Enterprise Linux AS/ES 4.6, there might be a malfunction depending on the version of procps. Please refer to "10.4 Using Red Hat Linux AS/ES 4.6" in detail and actions.

(Note 5) This requirement does not apply if using external IA engine features.

(Note 6) Server Core for Windows Server 2008 and Windows Server 2012 are not supported.

(Note 7) To install the UTF-8 language environment, set the OS media, run the following command, select [Add Additional LanguageEnvironments], and select [UTF-8 English (United States) [EN_US]] in [CULTURAL convention to install] and [UTF-8 English (United States) [EN_US]] in [LANGUAGE translation to install].

```
# smitty lang
```

(Note 8) To use AIX, apply the patches provided by IBM Japan Ltd.
The APAR numbers and Fixpack currently verified are shown below.

OS	Patch
AIX 6.1	IV56395 or Fixpack of TL9SP3 of later
AIX 7.1	IV56004 or Fixpack of TL3SP3 of later

(Note 9) Required to mount the media.

(Note 10) If you have many remote hosts to be monitored and store the performance data in disk over time, be careful that it could have impact on the capacity of disk for the remote monitoring agent(s).
The following item in the manual (help) describes the formula for computation for disk usage.
[Maintenance]
-[Make a backup]
[Collected data] – Refer to the history data for performance monitoring.

(Note 11) If the system cannot communicate with the manager, it holds the information on the remote monitoring agent on a temporary basis. Be careful that the saved information could have impact on the disk capacity if the number of remote hosts is large. For changing the number of held pieces of the information, refer to "12.6 About Holding Information on Remote Monitoring Agent".

(Note 12) When using Linux, disable SELinux in advance. Note that SELinux is enabled by default in Red Hat Enterprise Linux 6.

(Note 13) Restrictions apply when using Web Monitoring View. For details, see the “MasterScope Media Release Memo”.

(Note 14) System requirements are necessary when setting an identifier to the service (Service Identifier) to be installed. The identifier setting can be omitted for the normal configuration (the applicable package is not necessary if it is omitted); however, it cannot be omitted in the multi instance configuration.

(Note 15) In Red Hat Enterprise Linux 7, it is required to select "Use bundled DB".

(Note 16) .NET Framework is required to perform hypervisor monitoring by using the agentless monitoring function.
For details, refer to the documentation in the following location in the MasterScope Media.
/doc/SysMgr/HypervisorMonitor_Guide.pdf

(Note 17) It's incompatible with a tablet mode of Windows 10.

2.3. Platforms Supported by Remote Hosts

It is possible to monitor the following platforms as remote hosts (hosts to be monitored by the remote monitoring 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 remote host monitoring by specifying the IP address and host name that are shared among clusters.

OS Name
Windows Server 2008 (SP1, SP2) (32bit)
Windows Server 2008 (SP1, SP2) (x64)
Windows Server 2008 R2 (No SP applied, SP1) (x64)
Windows Server 2012 (x64)
Windows Server 2012 R2 (x64)
Red Hat Enterprise Linux 5.8, 5.9, 5.10, 5.11 (x86)
Red Hat Enterprise Linux 5.8, 5.9, 5.10, 5.11 (x86_64)
Red Hat Enterprise Linux 6.2, 6.3, 6.4, 6.5, 6.6, 6.7 (x86)
Red Hat Enterprise Linux 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 7.1 (x86_64)
Oracle Linux 6.2, 6.4 (UEK) (x86)
Oracle Linux 6.2, 6.4 (UEK) (x86_64)

The system requirements for performing monitoring as a remote host are described below.

Item		Description
Required software	Red Hat Linux 5	Package : glibc(32bit) Package : procps Package : ncurses(32bit) Package : sysstat(7.0.2) Package : bc Package : openssh Package : openssh-server Package : openssh-clients (*1) Package : openssl(1.0.1h or later) Package:libgcc(32bit) *The ssh daemon must be operating in addition to the packages above.

	Red Hat Linux 6 Red Hat Linux 7 Oracle Linux 6	Package:glibc(32bit) Package:ncurses-libs(32bit) Package:sysstat(9.0.4 required in Red Hat Linux6. 10.1.5 required in Red Hat Linux7.) Package:bc Package:openssh Package:openssh-server Package:openssh-clients(*1) Package:openssl(1.0.1h or later) Package:libgcc(32bit) *A ssh daemon has to be working in addition to the above package.

(*1) A remote monitoring agent might crash if the package is not install.

2.4. Patrol light

The patrol light reporting function supports the following products from Patlite Corporation:

Item	Description
Serial connection type	PHE-3FB-RYG PHE-3FBE1-RYG PHC-100A
LAN connection type	NHE-3FB-RYG NHC-3FB-RYG NHM-3FB-RYG NHS-3FB1-RYG NHP-3FB1-RYG NHL-3FB1-RYG

3. What's New in this Release

This section outlines new features and enhances functions.

3.1. Support of AIX by the CDO Message API

The CDO message API can now be used in an AIX environment.

3.2. Support of Web API

A Web API can now be used to add, change, or delete monitoring settings.
You can easily link with MISSION CRITICAL OPERATIONS by using a Web API from an existing system or user-specific application.

For details, see the "WebAPI Reference".
The file of "WebAPI Reference" is stored under the following path in the MasterScope Media.
\doc\MCO\WebAPIReference.pdf

3.3. Enhanced Scenario Control Functions

The group/scenario definition can be edited and imported by using a manager command.

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

For details, see the "MasterScope MISSION CRITICAL OPERATIONS ScenarioCmd Import Definition Specifications".
The file is stored under the following path in the MasterScope Media.
\doc\MCO\ScenarioCmdImport.pdf

3.4. Enhanced Operation Control Functions

The group/action definition can be edited and imported by using a manager command.

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

[Command reference]
-[OperationCmd]
  -[OperationCmd SU]
  -[OperationCmd IMPORT]

For details, see the “MasterScope MISSION CRITICAL OPERATIONS OperationCmd Batch Registration of Action Definitions Operation Manual”.
The file is stored under the following path in the MasterScope Media.
\doc\MCO\OperationCmdSgImport.pdf

3.5. Increase in supported platforms

Windows 10 is now supported.

3.6. Enhanced message monitoring functions (SystemManager-specific functions)

Reference privileges (Other host message reference) can now be set for a message output from the host under the topology view or from a node that has not been registered as a host under message linkage.

For details, see the following chapters in the manual or in Help.
[Using SystemManager-specific functions]
-[Configuring authority]
  -[Message Cooperation]

4. Improvements

The improvements shown in Table1, and modifications shown in Table 2 have been applied in this version of SystemManager. “○” in the tables indicates an improved item.

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	·Service port monitoring function Changed the default connection timeout time from one second to three seconds. (This is because timeouts occur frequently if the connection timeout time is one second.)	○	○	○	○						
2	·Message monitoring function Added an option to specify multiple categories as the target of the BusinessCmd ACTV/HOLD command (-F option). For details, see the manual (Help).		○	○	○						
3	·Configuration information monitoring function The function to display HP-UX11.31(IPF) configuration information now collects "Intel(R) Itanium 2 processor" instead of "ia64" as system information.						○				
4	·Configuration information monitoring function Enhanced the function to display Solaris configuration information so that the number of processor cores and other data as system information can be displayed.							○			
5	·Schedule Improved the processing performance when updating the schedule definition.	○	○	○	○	○	○	○	○	○	
6	·Manager linkage function Improved the performance when sending messages to the upper-level manager in a UNIX environment.			○	○						
7	Reduced the CPU usage by the manager when connecting SVC.		○	○	○						
8	·CDO message API Enhanced the API to enable		○			○					

	the parameters for the CDO message edit daemon to be edited by editing the registry in the Windows environment.										
9	·Message monitoring function Improved the category message list screen so that it automatically scrolls even if a message is selected.	○									

Table 2 Modification details

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	·Invariant Analyzer function Corrected the problem that additional analysis of the model used for on-demand analysis fails after validation when a target counter is added.	○	○	○	○						
2	·Service port monitoring function Corrected the problem that the manager process may go down while referencing a specific definition of the service port monitoring function (9000101460).		○	○	○						
3	·Service port monitoring function Corrected the problem that the messages about the service port monitoring function are not sent even when resuming monitoring by using the TopologyCmd ACTV command after stopping agent monitoring by using the TopologyCmd HOLD command (9000101460).		○	○	○						
4	·Service port monitoring function Corrected the problem that the	○									

	setting changes to [Normal port status:Open] if you open the monitoring definition specification dialog box when [Normal port status:Close] is specified for service port monitoring and close the dialog box by using the [OK] button without clicking the [Normal port status] item (9000101460).										
5	Corrected the problem that the console may go down when you move the mouse while shutting down the console (9000101215).	○									
6	·Process monitoring function Corrected the problem that the replacement character string $SEVERITY$ in the report is not replaced when a change of process ID is detected.		○	○	○						
7	·Remote host monitoring Corrected the problem that continuation of the monitoring process may become impossible or the load of the log collection process may become high if a replacement character string is used in the log file name in the applications log monitoring function or syslog monitoring function (9000101258).										○
8	·Reporting Corrected the problem that email reporting may fail if the body of the email report contains line feeds whose line feed code is just CR or just LF (9000101425).		○	○	○						
9	Corrected the problem that monitoring settings may become invalid if the definition is updated at the same time as a new agent establishes connection.		○	○	○						
10	Corrected the problem that the manager process may go down		○	○	○	○	○	○	○	○	

	if you specify an invalid regular expression on a specific filter definition dialog box (9000101492).										
11	Corrected the problem that the manager may terminate abnormally during startup when Oracle is used in a UNIX environment.			○	○						
12	·CDO message API Corrected the problem that the product cannot be installed in a Linux (32-bit) environment.				○					○	
13	·CDO message API Corrected the problem that the service may not end normally in a Windows environment when the OS is shut down.		○			○					
14	Corrected the problem that operations, setup, or monitoring on the console may no longer be able to be performed if the map view is updated while you are dragging an icon in the map view.	○									
15	·service port monitoring function Corrected the problem that a memory leak of about 200 bytes occurs in the agent process if you add, update, or delete monitoring settings by using the service port monitoring function.					○					
16	Corrected the problem that a memory leak of about 24 bytes occurs pre one rule process if you add or delete schedule.		○	○	○						
17	·message monitoring functions (SystemManager-specific functions) Corrected the problem that a message might be displayed for a user who did not have reference privileges for the appropriate host when a filter is deleted.	○	○	○	○						

18	·message monitoring functions (SystemManager-specific functions) Corrected the problem that the message in question might be displayed for a user who did not have reference privileges when [Confirm], [Make Unconfirmed], or [Mark] is selected for a message from the right-click menu.	○	○	○	○						
19	·message monitoring functions (SystemManager-specific functions) Corrected the problem that messages displayed at the bottom of the window could not be hidden even if the host node was moved to a group that did not have reference privileges.	○	○	○	○						
20	·event log monitoring function. Corrected the problem that some logs might be missing or displayed in the wrong order (not displayed in the log occurrence order) in the log list (log list window displayed by double-clicking an event log node) of the event log monitoring function. (Contents ID:9000101544)					○					
21	·message monitoring functions Corrected the problem that the search period was shortened by one day and messages could not be extracted, or the manager process was heavily loaded if certain conditions were met when searching the business view. (Contents ID:9000101594)					○	○			○	
22	·application log monitoring/syslog monitoring function. Corrected the problem that all log contents might be reported if a log whose last line length was 4096 bytes or more was					○	○	○	○	○	

	set to be monitored by the application log monitoring/syslog monitoring function. (Contents ID:9000101567)										

5. How to Install or Uninstall the Product

For information on how to install and uninstall this product, refer to the MasterScope Media release memo (relmemo.pdf).

IA analysis engine can be installed on a different machine as a external engine to separate the heavy loads caused by analysis from the Manager. In order to use the external engine, you must install the "MasterScope MISSION CRITICAL OPERATIONS RelayManager" features.
Please refer to the document contained under the following path in MasterScope Media in detail.
\doc\MCO\IA_relememo.pdf

Install the “MasterScope MISSION CRITICAL OPERATIONS Remote Monitor Agent” function (remote monitoring agent) to use the agentless monitoring function.
Install the “MasterScope MISSION CRITICAL OPERATIONS Logical Agent” function to use the logical system agent.

■ Notes of hostname
The default self hostname set by the Windows installer is a NETBIOS name.
If you install several products to separate installation directories in one node, you must specify each of the self hostnames of agents so that the manager can recognize each agent uniquely.

*This applies to a case where a normal agent(s) and a logical agent(s) are installed to the same node.

5.1. When IPv6 is Used

IPv6 can be used as a communication protocol among the manager, agent and the monitoring screen (the Web monitoring screen) from MISSION CRITICAL OPERATIONS Ver4.2. It is required to set a protocol to the setting file after installing the product when monitoring is conducted by using IPv6.

■ Notes
- 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.

- To reflect the settings, restart the processes of each function.
- The IPv4 address is the only IP address that can be entered when the IP address is entered on the monitoring screen unless otherwise described in the individual function manuals. The IPv6 address cannot be entered.
  The IPv4 address is also the only IP address that can be used instead of the host name. A host name that can be resolved by DNS or hosts in advance shall be used when utilizing the IPv6 communication.
- The IPv6 communication cannot be used for some of the functions. Instead, use the IPv4 communication (set by default) for the functions for which the IPv6 communication cannot be established. For details about the function with the IPv6 disabled, see "11.11 IPv6".
- 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. Specify the combined mode of the IPv4 and IPv6 communications when the communication is conducted by using both protocols.
- When a manager is a local machine, web console connects to a manager using the loop back address.IPv4 communication only (default) is used, and when IPv6 is used for the loop back address, fails in a connection to a manager.When connecting in IPv6, please change the web console and manager to IPv6 Mode.
  When connecting in IPv4 without changing the communication mode, please give priority to IPv4 address over IPv6 as the address for a self-host.

  The order of priority confirmation command
  #netsh interface ipv6 show prefixpolicies

  command output example

Precedence	Label	Prefix
50	0	::1/128
40	1	::/0
30	2	2002::/16
20	3	::/96
10	4	::ffff:0:0/96
5	5	2001::/32

  The order of priority change command
  #netsh interface ipv6 set prefixpolicy <Prefix> <Precedence> <Label>
  ex) netsh interface ipv6 set prefixpolicy ::ffff:0:0/96 60 0

5.1.1. Protocol Setting

■Agent (The remote monitoring agent is excluded.)
[File path]

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

[Added descriptions]

[UpperNode] Protocol=6 (*1) [SelfNode] SvcServerProtocol=6 (*2)

[Parameter details]

	Key Name	Description
*1	Protocol	Specifies the communication protocol when the agent is connected to the manager. The communication operates as described below depending on the specified value: 4: IPv4 communication only (set by default) 6: IPv6 communication only 46: Communication in the combination of IPv4 and IPv6 (IPv4 is prioritized)
*2	SvcServerProtocol	Specify the communication protocol for the command to connect to the agent. The communication operates as described below depending on the specified value: 4: IPv4 communication only (set by default) 6: IPv6 communication only 46: Communication in the combination of IPv4 and IPv6 (IPv4 is prioritized)

■Manager

[File path]

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

[Added descriptions]

[SelfNode] ServerProtocol=6 (*1) SvcServerProtocol=6 (*2)

[Parameter details]

	Key Name	Description
*1	ServerProtocol	Specifies the communication protocol that waits for and receives the connection from the agent. The communication operates as described below depending on the specified value: 4: IPv4 communication only (set by default) 6: IPv6 communication only 46: Communication in the combination of IPv4 and IPv6 (IPv4 is prioritized)
*2	SvcServerProtocol	Specifies the communication protocol that waits for and receives the command connected to the monitoring screen, Web monitoring screen, and the manager. The communication operates as described below depending on the specified value: 4: IPv4 communication only (set by default)

		6: IPv6 communication only 46: Communication in the combination of IPv4 and IPv6 (IPv4 is prioritized)

■Monitoring screen

[File path]

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

[Added descriptions]

[UpperNode] Protocol=6 (*1)

[Parameter details]

	Key Name	Description
*1	Protocol	Specifies the communication protocol when connecting a monitoring screen to the manager. The communication operates as described below depending on the specified value: 4: IPv4 communication only (set by default) 6: IPv6 communication only 46: Communication in the combination of IPv4 and IPv6 (IPv4 is prioritized)

■Web monitoring screen

[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

[Added descriptions]

HttpServerMgr.ini

[SelfNode] ServerProtocol=6 (*1)

SysMonSvc.ini

[UpperNode] Protocol=6 (*2)

[Parameter details]

	Key Name	Description
*1	ServerProtocol	Specifies the communication protocol that waits for and receives the connection from the Web monitoring screen. The communication operates as described below depending on the specified value: 4: IPv4 communication only (set by default) 6: IPv6 communication only 46: Communication in the combination of IPv4 and IPv6 (IPv4 is

		prioritized)
*2	Protocol	Specifies the communication protocol when connecting a Web monitoring screen to the manager. The communication operates as described below depending on the specified value: 4: IPv4 communication only (set by default) 6: IPv6 communication only 46: Communication in the combination of IPv4 and IPv6 (IPv4 is prioritized)

5.1.2. Protocol Setting

■Example 1
When the communication in the combination of IPv4 and IPv6 is conducted between all of the functions

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

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

- Web monitoring screen
  <Installation path>\Manager\sg\HttpServerMgr.ini

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

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

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

■Example 2

When the communication between the monitoring screen and the manager is conducted via IPv6 while the communication between functions other than the monitoring screen and the manager is conducted via IPv4

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

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

- Monitoring screen
  <Installation path>\Svc\sg\SysMonSvc.ini

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

6. How to Upgrade the Product

The version of this product is upgraded by an overwrite installation of its new version.
For information on how to perform an overwrite installation of the product, refer to the "MasterScope Media release memo" (relmemo.pdf).

* Ensure that you will first upgrade the version of the manager. When the version of an agent is later than that of the manager, it is not guaranteed that the agent can be connected to the manager.
* When upgrading the version of your manager or agent to Ver3.6 or later in an environment where a Windows version of CDO message API is being used, ensure that you also upgrade the version of the CDO message API function to Ver3.6 or later.
* When upgrading the UNIX agent from Ver. 3.6.1 or older, the values obtained by the agent may be changed because the default values of data acquisition mode for the performance data are changed. For details, see “10.18 Default values of performance data acquisition method for UNIX agent”.
* See the notes described in "10.44 History of the Event Correlation Function" when the event correlation function is used.

7. Setting for Duplicating Manager

For information on duplicating and using your manager, refer to the appropriate duplicating setup guide.

The documents are stored in the following path in MasterScope Media.
\doc\MCO\

・Windows
When using CLUSTERPRO X, refer to "Cluster_Win_EXPRESSCLUSTER_X.pdf"
When using WSFC, refer to "Cluster_Win_WSFC.pdf"

・Linux
When using CLUSTERPRO X, refer to "Cluster_Linux_EXPRESSCLUSTER_X.pdf "

See the Duplication Setup Guide of the remote monitoring agent when the remote monitoring agent is used under the dual environment.
RemoteMonitor_ClusterSetupGuide.pdf

See the installation guide of the logical system agent when several types of resources are monitored that switch in conjunction with the cluster packages.
Logical_Agent.pdf

8. Configuring managers in a hierarchy

8.1. 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]

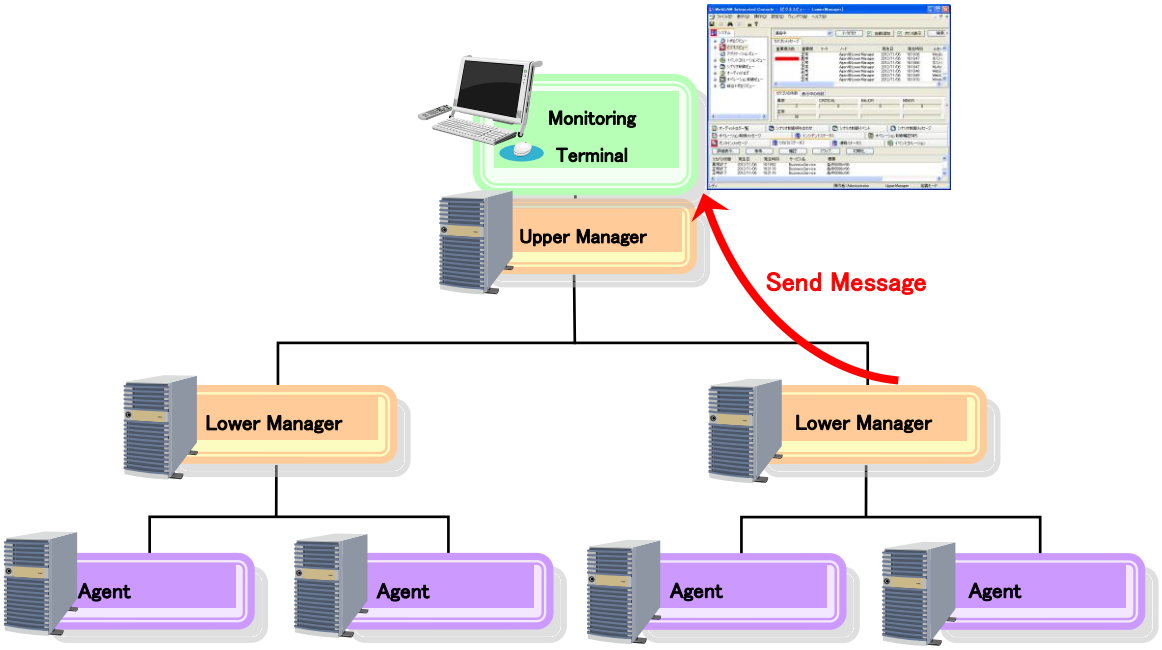


Figure 8-1　Message reporting by managers in a hierarchical configuration

◆　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]

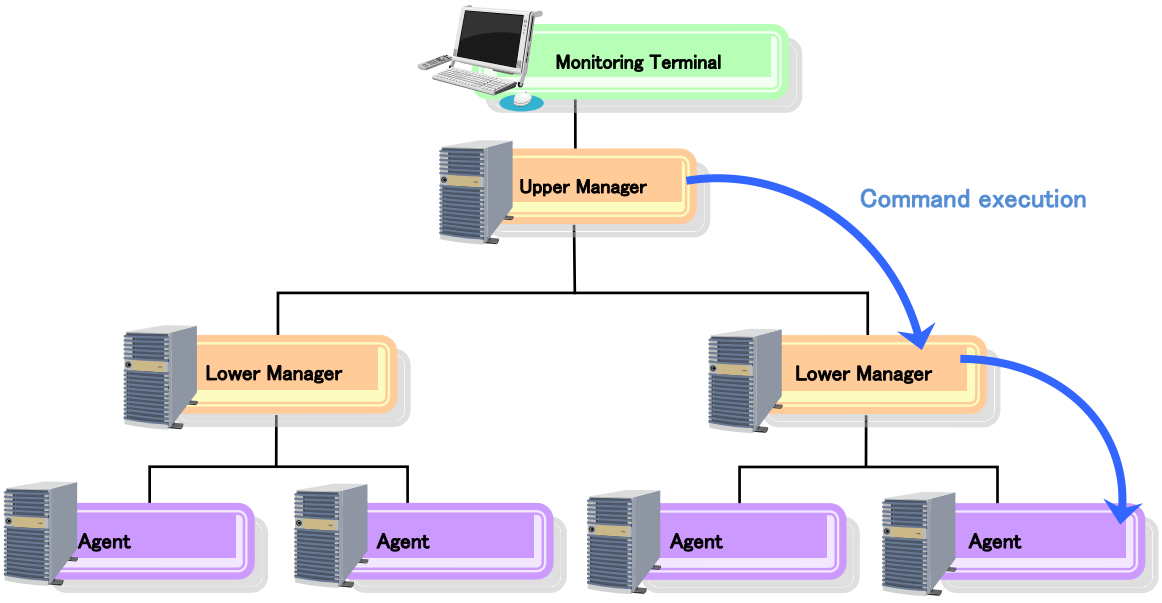


Figure 8-2　Command execution by managers in a hierarchical configuration

◆　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]

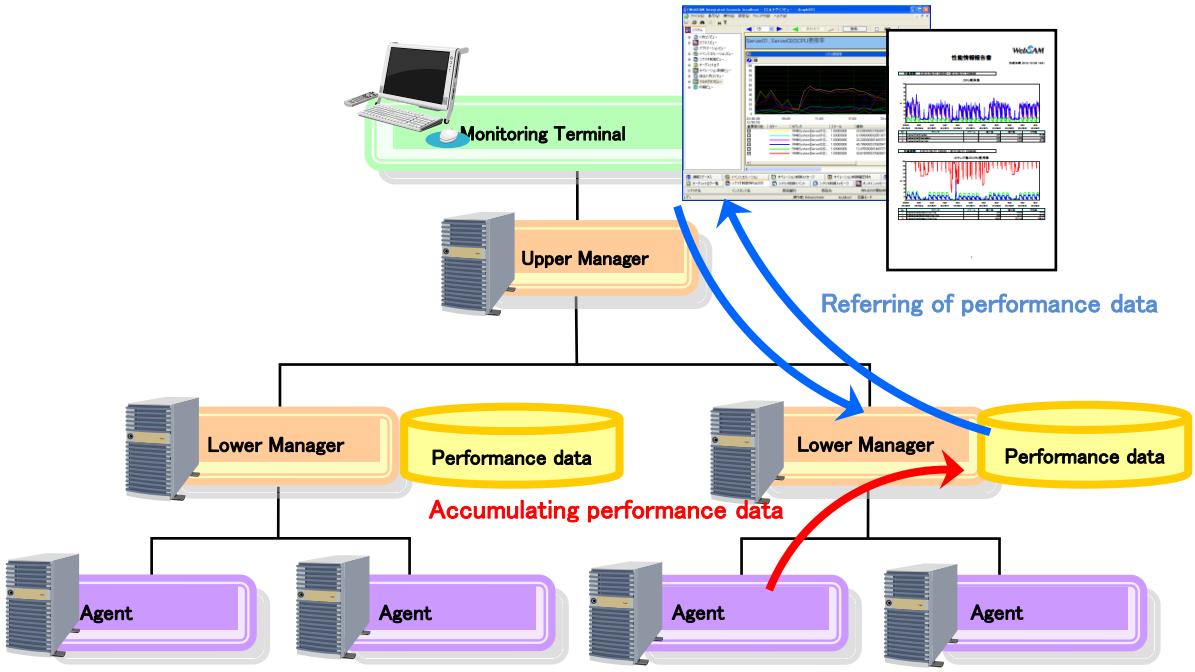


Figure 8-3　Multi graph and print views of managers in a hierarchical configuration

◆　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]

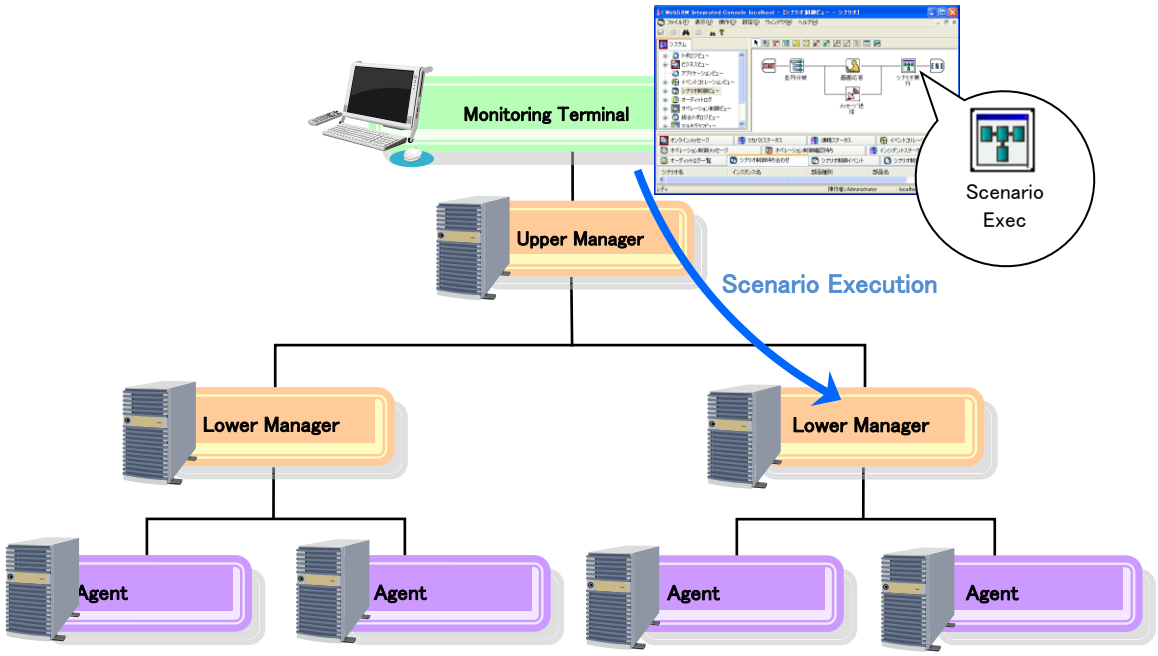


Figure 8-4　Scenario control performed by managers in a hierarchical configuration

8.2. 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

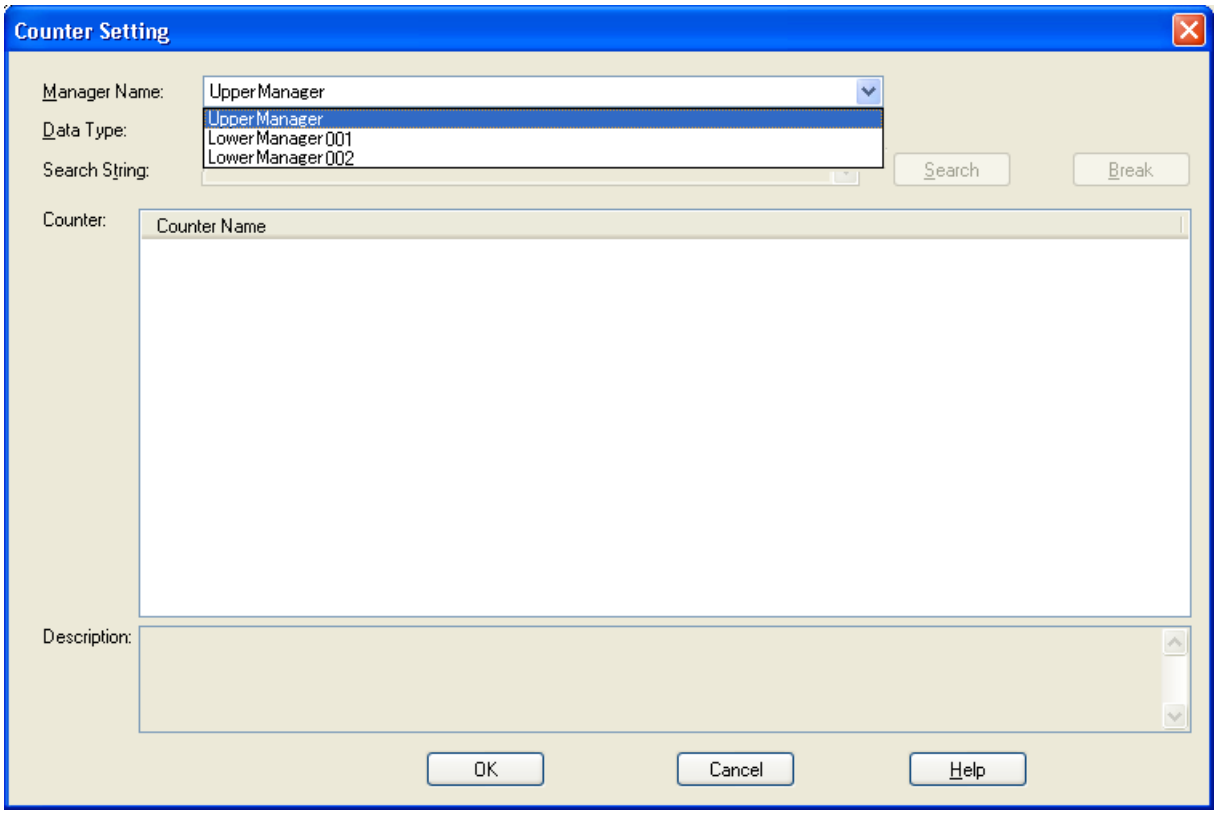


Figure 8-5 Multi graph view [Counter Setting] dialog box

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

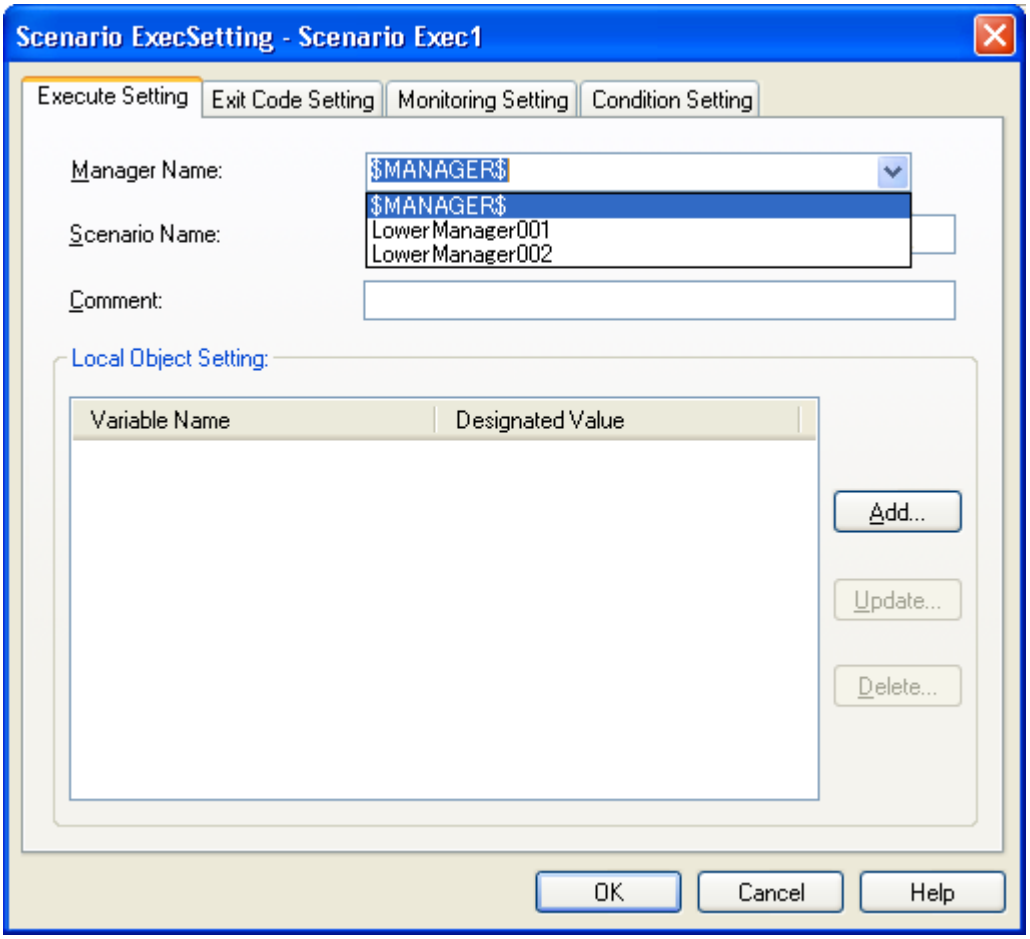


Figure 8-6 Scenario control [Execute Setting] dialog box

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]

8.3. 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]

8.4. 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]

9. Knowledge Information Included in this Product

Knowledge information to be used for the message monitoring function (business view) is provided. Knowledge files are stored in the following path on the monitoring terminal.

<monitoring terminal installation directory>\Svc\knowledge

For information on how to import a knowledge file, refer to the following chapters in the manual (Help).

-[Monitor messages]
-[How to define message monitoring]
- [Define conditions of messages stored in categories and display method]
-[Import a knowledge file]

■ Knowledge files related to functions of MISSION CRITICAL OPERATIONS

Applicable Function	File Name	Remarks
Application log monitor	UMF_ApplicationLogMonitor.txt	
Application view	UMF_ApplicationView.txt	
Business view	UMF_BusinessView.txt	Updated in Ver4.2.0
EXPRESSCLUSTER monitoring	UMF_ExpressClusterMonitor.txt	
Event correlation	UMF_EventCorrelation.txt	Updated in Ver4.2.0
EventLog Monitor	UMF_EventLogMonitor.txt	
Syslog Monitor	UMF_SyslogMonitor.txt	
Windows service monitoring	UMF_NTServiceMonitor.txt	
Performance monitoring	UMF_PerformanceMonitor.txt	
Process monitoring	UMF_ProcessMonitor.txt	
Scenario control	UMF_ScenarioView.txt	
Remote Connection management(API/WMI)	UMF_RemoteConnectCtlWMI.txt	
Remote Connection management(SSH)	UMF_RemoteConnectCtlSSH.txt	
Topology view	UMF_TopologyView.txt	
Manager linkage	UMF_MessageLinker.txt	
File monitoring	UMF_FileMonitor.txt	
Operation control	UMF_OperationView.txt	
Application linker	UMF_ApLinker.txt	
ServiceManagerLinker	UMF_ServiceManagerLinker.txt	
Manage the message	UMF_Message.txt	
Invariant analyze	UMF_InvariantAnalyzer.txt	
MultiGraphView	UMF_MultiGraphView.txt	Added from Ver3.6.1. Function of MasterScope

		SystemManager.
Service port monitoring	UMF_PortMonitor.txt	Added in Ver 4.1.1

* When a knowledge file has been imported into a category, the category is automatically created under the "Unified Management Framework" group with the manager installed.
* An updated knowledge file is not automatically applied on version up. Please import the knowledge file after deleting filters in the relevant category.

■Kowledge files related to other products

Applicable Function	File Name	Remarks
EXPRESSCLUSTER (V7.0)	ExpressCluster7.0.txt	
EXPRESSCLUSTER (V8.0)	ExpressCluster8.0.txt	
EXPRESSCLUSTER X	ExpressClusterX.txt	
Exchange	Exchange.txt	
iStorageManager(Ver.3.3 ~)	iStorage.txt	Updated in Ver4.2.0
MasterScope NetworkManager	NetworkManager.txt	
ServerAgent	ServerAgent.txt	
Oracle Clusterware	ApLog_OracleClusterware_en.txt	
Oracle	ApLog_OracleRDBMS_en.txt	
Oracle9i Database R2	K4ORACLE9iR2_en.txt	(Note 1)
Oracle Database10g R1	K4ORACLE10gR1_en.txt	(Note 1)
Oracle Database10g R2	K4ORACLE10gR2_en.txt	(Note 1)
Oracle Database11g R1	K4ORACLE11gR1_en.txt	(Note 1)
Oracle Database11g R2	K4ORACLE11gR2_en.txt	(Note 1)
RootCauseView	UMF_RootCauseView.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 MISSION CRITICAL OPERATIONS.
※ These knowledge files are based on causes and actions of the past inquiries. Please note that they don’t provide all the causes and actions for the target products.
※ These knowledge files cannot be used from the Web Monitoring Terminal. Please use them from regular Monitoring Terminal.

(Note 1) Refer to the release note contained under the following path in your monitoring console.
<Console installation directory>\Svc\bin\Oracle\
NEC Knowledge for Oracle Release Memo rev1.2 en.pdf

10. Notes

10.1. Registering a license

This product verifies the license agreement using the license management function.The product can be used with a trial version license for three months after installation and can be used with an application period license for a month after a license key was registered; however, an official license needs to be registered to use the product after this period.Use the following procedure to register an official license:

1) Register a license key to obtain a code word application code.
2) Refer to the attached documentation and obtain a code word.
3) Register the code word.
4) Restart the manager.

Restart the manager as soon as the code word is registered.
The number of licenses for the trial version is described below.

License name	Number of licenses
MasterScope MISSION CRITICAL OPERATIONS View	1
MasterScope MISSION CRITICAL OPERATIONS Base Manager for Win/Linux	1
MasterScope MISSION CRITICAL OPERATIONS Base Manager for HP-UX	1
MasterScope MISSION CRITICAL OPERATIONS Base Agent for Win/Linux	5
MasterScope MISSION CRITICAL OPERATIONS Base Agent for HP-UX/Solaris/AIX	5

10.2. Notes on Duplicated Environment

About not removed files

When uninstalling a standby system, files on the shared disk will not be removed. After the system is uninstalled, remove them manually.

About license registrations

Register licenses on both the active and standby nodes in a redundant environment.
Register licenses for the active node from the console.Licenses can be registered to the stopped manager for the standby node by using LicenseCmd.

For details, see the following chapters in the manual or in Help.
- Registering licenses
- Command reference
- LicenseCmd

10.3. Using Red Hat Linux AS/ES 4.0

If you use Red Hat Linux AS/ES 4.0, there might be a memory leak depending on version of OS libraries.

[Libraries with problems]
glibc-2.3.4-2.19
glibc-common-2.3.4-2.19
glibc-utils-2.3.4-2.19

To avoid this issue, please get updated packages of relevant libraries from the following URL, then install it and reboot OS.

[Red Hat Support]
https://rhn.redhat.com/errata/RHBA-2006-0510.html

10.4. Using Red Hat Linux AS/ES 4.6

As procps-3.2.3-8.9 provided by Red Hat Linux AS/ES 4.6 has a bug, if monitoring a process by performance monitoring function, it may display invalid value. This bug has been fixed in procps-3.2.3-8.12, so please update the library if you are using procps-3.2.3-8.9.

10.5. 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.

10.6. Installing a product on Linux

Disable SELinux when installing the product on Linux.

10.7. About Console Launching User

Start the console as a user with administrative authority for the operating system.
Users without administrative authority cannot start the console.

10.8. About Character Set of CDO Message API

CDO message API doesn't support UNICODE.
For information on the supported character set, please refer to the release note of CDO Message API, which is stored in the following path in the MasterScope Media.
/doc/MCO/CDO_relememo.pdf

10.9. 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.

- In RedHat Enterprise Linux4 and SuSE Linux Enterprise Server 10, SCSI drivers might not be recognized. Check the following items when a SCSI device is connected but the information cannot be referenced.

1. Check if the required software *sg3_utils* (or *scsi* in case of SLES10) is installed.
   Install it if it is not installed.
2. Execute the command “/sbin/lsmod” and check if “sg” is loaded.
   (“sg” is displayed in the Module column in the command execution result.)

```
% lsmod
```

```
Module                  Size  Used by
sg                     40313
```

If it is not loaded, execute the command “/sbin/modprobe sg” and check if “sg” is loaded. Then, obtain the latest device information and confirm that the SCSI device information can be obtained.

3. Add the following description at the end of the “/etc/rc.d/rc.modules” file.

(Create the “/etc/rc.d/rc.modules” file and grant the execution authority if the file does not exist. Add a symbolic link to “rc.d/rc.modules” with the name of “rc.module” directly under “/etc”.

```
#!/bin/sh
～
/sbin/modprobe sg                                   * Add this description
```

4. Restart the system and confirm that the SCSI device information is obtained at the system startup time.

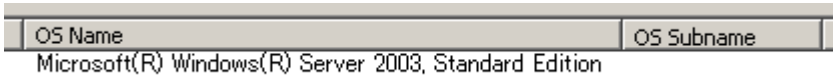
9) Displaying a set of configuration information

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.

10) 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.

11) 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.

12) 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.

13) 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.

10.10. Combining different versions

Combining different versions of Monitoring Terminal, Manager, and Agents are supported only under the following conditions.

・ Manager and Monitoring Terminal must be exact same versions.

ex) Manager Ver.3.4.1 - Monitoring Terminal Ver.3.4.1 : Supported
Manager Ver.3.4.1 - Monitoring Terminal Ver.3.4.0 : Not Supported

・ Manager versions must be greater then Agents, and they both must have the same major version.

ex) Manager Ver.3.4.0 - Agent Ver.3.0.0 : Supported
Manager Ver.3.4.0 - Agent Ver.3.5.0 : Not Supported

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

ex) Upper-level manager with Ver3.6.0 vs. Lower-level manager with Ver3.5.0: Supported
Upper-level manager with Ver3.5.0 vs. Lower-level manager with Ver3.6.0: Not supported

10.11. Accumulating collected performance data

The performance data collected by the performance monitoring function, Application Navigator, or NetvisorPro V is 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 manual (help).

Size of accumulated performance data is 16 byte per record.
The performance data will create a file on a daily basis.
E.g.: Amount of data derived from monitoring 100 counters at intervals of 30 seconds and saving data for 7 days on one agent

Amount of data to be saved in one file:
16 (bytes) * 3,600 (seconds) * 24 (hours) / 30 (seconds) = 46,080 (bytes)
Size of disk to be used for one file:
49,152 bytes (assuming the block size is 4 KB)
Seven-day data for 100 counters (700 files):
49,152 (bytes) * 700 = 34,406,400 (approx. 32.9 MB）

*This calculation method only produces a rough approximation, and the exact figure will slightly change, depending on how you operate your system.

In the case of UNIX managers, a rough approximation of the number of inodes to be used to store the performance data is as follows:

(Number of monitored counters) * (number of days during which data is retained + 4)

E.g.: If the number of monitored counters is 30,000 and the number of days for holding data is 30, 1,020,000 inodes should be used.

If you need to store performance data for tens of thousands of monitored counters for a long period of time, ensure that you will secure an ample inode area when creating the file system.

The performance data will be saved under the following directories:

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

The performance data accumulation can be stopped when not the Invariant Analyzer functions or the performance information display and form functions of SystemManager are not being used.
For details about how to stop accumulation, see "12.9 Stopping the accumulation of performance information"

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

10.12. 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	Yearly 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.

10.13. Maximum number of counters that 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; linkage with Introscope)
- 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, see the following chapters in the manual or in Help.
  [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.

  For details, see the following chapters in the manual or in Help.
  [Performing invariant analysis]
  -[Maintaining counter information]
  -[Maintaining counter information]

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.

10.14. 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.

10.15. Storing messages

Since SystemManager specific functions include a message monitoring function, messages are accumulated in duplicate by SystemManager and the business view.
If it does not cause any operational problems, it is recommended to disable the message monitoring function of SystemManager.

10.16. Default category settings for business view

The default category settings are specified for the business view when MasterScope is installed. However, the default category settings for Application Navigator, rather than those of MasterScope, are specified when Application Navigator is installed first in the same location.Since the default category data of MasterScope is installed on the console, the knowledge for MasterScope can be set up by importing the knowledge manually.For details, see “9Knowledge Information Included in this Product”

10.17. User account control for Windows Vista or later versions

Note the following when using the product in a Windows Vista or later version environment in which user account control is enabled
A user account control warning dialog “[A program needs your permission to continue]” is displayed when starting the console.Select [Continue] to start the console.This warning dialog cannot be suppressed in an environment in which user account control is enabled.
%ProgramFiles% folder is located in the virtual memory.diting the SysMonSvc.ini file must be performed with an editor with administrator authority when a folder under Program Files is selected as the installation location

10.18. Default values of performance data acquisition method for UNIX agent

To reduce the impact on the performance data values due to the momentary load rise caused by the agent monitoring operations, the default values of the performance data acquisition method for the UNIX agent monitoring objects, Device, Network Interface, Processor, and System, have been changed from momentary value mode to average value mode from MISSION CRITICAL OPERATIONS Ver. 3.6.2.
The values obtained by the agent may differ after upgrading due to the changes in default values.

To change the performance data acquisition method to the previous momentary value mode for some reason, see the following chapters in the manual or in Help, and change the settings.

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

10.19. 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.

10.20. Displaying device information for SPARC T3/T4 servers

For SPARC T3/T4 servers, SCSI device information is not displayed in [System] - [Device Information] in the topology view even if SCSI devices are configured.
This is because WWN is included in logical device names.

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

MCOperations Ver 3.7.1 or later 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.

10.22. Searching for command logs by using the operation control function

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

10.23. 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.

10.24. 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.

10.25. Agentless Monitoring

- As the status of a remote host is monitored through a remote monitoring agent, the monitoring will be halted when the remote monitoring agent is not started.
- Any remote monitoring agent cannot monitor its own host as a remote host. Use a regular agent to monitor a host for the remote monitoring agent.
- The remote monitoring 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 installing a regular agent to monitor a host to which the remote monitoring agent has been installed, set the different names for the remote monitoring agent and the regular agent.
- The remote monitoring agent sends an ICMP echo request to the monitored remote host regularly. If there is no response, the agent recognizes the remote host as “not-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.

- When the authentication information is not used when performing the automatic detection, the detailed information might not be obtained in Windows operating systems. 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.
- Agentless monitoring in Windows uses WMI interfaces, SMB services, and NETBIOS services. Specifically, agentless monitoring cannot be properly performed without being allowed to access the port numbers of 135, 139, and 445 for TCP and 137 and 138 for UDP. In addition to the above port numbers, access to port numbers dynamically assigned after 1024 for TCP/UDP that will be used by WMI must be allowed. For required settings for remote hosts and remote monitoring agents, refer to "12.11 Security Settings for Agentless Monitoring Function"
- A network connection by SSH is used for the Linux remote host monitoring. For this reason, the SSH daemon must be running on the remote host and allowed to access the port number used by the SSH daemon. 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.
- It is recommended to use the Administrator authority to specify the authentication information for the Windows remote host monitoring. Using a standard user account might cause incorrect monitoring for access authority reasons.

- It is recommended to use the root authority to specify the authentication information for the Linux remote host monitoring. Using a standard user account causes the following restrictions.
  - Process monitoring
    When performing process monitoring using a process path, no distinction is made for processes started by users other than the specified user.
  - File monitoring
    Only files for which the specified user is granted read permission and directories for which the user is granted read and execution permissions can be monitored. The status of the files and directories for which no permissions are granted is unknown. Only files with read permission are used to add up file size for capacity monitoring.
  - Application log monitoring
    Only log files for which the connection user is granted read permission can be monitored. Logs are not reported for log files without permission.
  - Syslog monitoring
    No syslogs are reported if the connection user is not granted read permission for the following files. When the connection user is granted read permission for the following files, only syslogs for which the user is granted read permission can be monitored. Logs are not reported for the log files without permission.
    /etc/syslog.conf
    /etc/rsyslog.conf
    /etc/syslog-ng/syslog-ng.conf
  - Recovery execution
    Only commands for which the connection user is granted read and execution permissions can be executed.

➢ File/directory specification dialog box

Only files and directories in the directory for which the connection user is granted read and execution permissions are displayed.

- The "Remote Registry" service must be in the start-up state automatically or manually when monitoring the performance of the Windows remote host. If the service is disabled or not running, the data of performance monitoring cannot be acquired (including object acquisition).
- During Linux remote host monitoring, directories and files for the monitoring program are created in the home directory of the connection user. For this reason, the connection user must be granted read and write permissions for the home directory. Monitoring cannot be operated correctly if the permissions are not granted.
- A temporary file is created in /tmp to perform performance monitoring during Linux remote host monitoring. For this reason, the connection user must be granted read and write permissions for /tmp. Monitoring cannot be operated correctly if the permissions are not granted.
- In the Linux remote host, the maximum supported number of monitoring targets including the number of monitored logs in the syslog monitoring function and the number of monitored files and directories in the file/directory monitoring functions is 90.
- Files in /proc/meminfo are referred to perform performance monitoring during Linux remote host monitoring. For this reason, the connection user must be granted read permission for /proc/meminfo. Monitoring cannot be operated correctly if the permission is not granted.
- The definition information on a remote host is stored in the following location:
  <Installation directory>\Agent\sg\RemoteAgent\<Display name for remote host>\sg
- If a remote host exists in Topology View and a new regular agent with the same name as the remote monitoring host is connected to it, irregular operations may occur.
- The monitoring functions may remain in the unknown statuses (such as SERVICEUNKNOWN and PROCESSUNKNOWN) for about 5 minutes in a case where the remote host is restarted.
- When entering a command in a remote host, a temporary file will be created in a folder pointed by the system environmental variable %TEMP%. In any remote host where the variable %TEMP% is not set, the entered command fails in execution. And, through the account information specified in the authentication information, write/read/execution rights on the %TEMP% folder must be granted.
  Neither automatic detection nor monitoring of remote hosts is supported for IPv6.
- Automatic detection and monitoring of remote hosts are performed based on IP addresses. For this reason, hosts whose IP address is dynamically changed by DHCP, etc. cannot be monitored properly.
- It may take some time to stop an agent service in a case where API used within the system may wait for a response in vain from a remote host.
- For the monitoring definitions for remote hosts, some environmental variables can be similarly to defining agents. However, the available environmental variable are only the System environmental variable and %SystemRoot%.
- In operations from the console, file names and directory names on remote hosts are in lowercase.
- To execute a recovery to the Linux remote host, the recovery execution result (standard output) must be less than 5 MB. A recovery with standard output of 5 MB or more might remain under execution.
- A remote host in the NAT environment cannot be monitored.
- The remote monitoring agent must be run on a host that does not belong to any domain such as WORKGROUP.
  When you run a remote monitoring agent on a host belonging to a domain, the agent may not perform performance monitoring on the remote host.

If that is the case, you can enable the agent to perform performance monitoring by following the [Steps to change an account for running services] described below.

[Steps to change an account for running services]

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

* Enter a domain account or local account which can log into the remote host.

10.26. 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
   <Agent installation directory>\Agent\sg\SysMgrMRCAS

   * 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
   <Manager installation directory>\Manager\sg\SysMgrMRCAS\[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.

5. Start the target agent service.

10.27. Notes on uninstalling the product

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.

10.28. Character code of Event Trap Utility and the operation message reporting API

Event Trap Utility and the operation message reporting API do not support Unicode.
Only SJIS and EUC character codes are supported.

10.29. On-access virus scan

If the folders used by MCOperations are subject to an on-access virus scan, MCOperations might not function normally. For this reason, exclude the folders (installation folder/data area folder) used by MCOperations as the target of the on-access scan.
Do not allow external programs such as virus scan software to access the folders used by MISSION CRITICAL OPERATIONS.

10.30. Editing SysMonMgr.ini

See the “7.3.4. Notes on changing the SysMonMgr.ini file” of “MasterScope Media Release Memo” if the SysMonMgr.ini file was edited.

10.31. 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.

10.32. Notes on upgrading

The backup file specification pattern for syslog monitoring in the Linux agent (the Linux remote host for the agentless monitoring) has been changed depending on the version of logrotate from version 4.0.3 of this product.

- logrotate version 3.7.5 or older
  [Log file name].<N>
  * <N> is a number from 1 to 4.

- logrotate version 3.7.6 or later
  [Log file name]-<YYYYMMDD>
  * <YYYYMMDD> is a date.

When upgrading the agent (upgrading the remote monitoring agent for agentless monitoring) from a version older than 4.0.3 of this product, the specification pattern of [Log file name].<N> is inherited regardless of the version of logrotate.
In addition, the backup file specification pattern is changed to the pattern mentioned above depending on the version of logrotate when the agent is reinstalled (for agentless monitoring, when the remote monitoring agent version is reinstalled).
Change the backup file specification in the [Filter Option Setting] dialog box for each syslog monitoring when the pattern is different from the backup method of the monitored syslog.

10.33. External Engines

To install and use MasterScope MISSION CRITICAL OPERATIONS and MasterScope Application Navigator individually, use an external engine compatible with each product respectively.
To install and use MasterScope MISSION CRITICAL OPERATIONS and MasterScope Application Navigator in the same core, use an external engine compatible with either product. It is not necessary to install external engines for both products.
When additionally installing MasterScope Application Navigator after MasterScope MISSION CRITICAL OPERATIONS has been installed, or additionally installing MasterScope MISSION CRITICAL OPERATIONS after MasterScope Application Navigator has been installed, the external engine used until then can be used as is for the newly installed product. Thus, is not necessary to install an external engine compatible with the additionally installed product.

10.34. Outputting crash dump when a failure occurs in Windows environment

It is recommended to specify the settings for crash dump output in advance in order to speed up investigation when a failure occurs.
Registry setting is required to specify the settings mentioned above for Windows Server 2008 or later.
For the detailed setting method, see the Microsoft technical support information related to Windows Error Reporting (WER).
When specifying the crash dump output settings, specify output of the complete dump information.

Note the following items.

※ When the crash dump is output, the file size might become large and clutter the disk depending on the situation.

※ If the crash dump settings are specified, the crash dump is also output when software other than MISSION CRITICAL OPERATIONS software crashes.

10.35. Resource monitoring switched in conjunction with cluster package

For resource monitoring switched in conjunction with the cluster package such as performance monitoring for shared disks and log files on shared disks, use the logical agent.

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.

10.36. 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.

10.37. 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.

10.38. Upgrading the agent from Ver4.2

To upgrade a Ver4.2 agent in which the LogicalDisk object in performance monitoring is specified to be monitored to Ver4.2.1 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 version.
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 Directory], which can be defined at installation.

10.39. 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. (It is identical to the one that is output when executing the TopologyCmd IMPORT command.)

10.39.1. 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.

10.39.2. 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.

10.39.3. 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.

10.39.4. 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.

10.40. 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.

10.40.1. 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.

10.40.2. 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.

10.41. 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]

10.42. Specification Change for the Performance Monitoring

The configuration under the Processor object has been changed as below for the UNIX agent for which there is only one processor core since version 4.1 of this product.

Before change: [Object]-[Counter] configuration
After change: [Object]-[Instance]-[Counter] configuration
* For the Solaris agent, the configuration is always the [Object] - [Counter] configuration under any environment.

The configuration is not changed when the software is upgraded if the definition of the [Object] - [Counter] configuration remains. However, monitoring cannot be conducted when the number of processor cores increases after the upgrade. Therefore, reset the monitoring definition in order to change to the [Object] - [Instance] - [Counter] configuration. Executing the command below also can reset the definition.
<Manager Installation Directory>/Manager/bin/PerformanceCmd.exe RE-SETUP -P <HostName>

10.43. Node name for the Event Log Monitoring

The computer name of event log is used as a node name of the message sent by the event log monitoring.
The node name may possibly differ from the one that is registered in 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.

In addition, the message that does not match the node name registered in the topology view cannot be stored, in the message monitoring function (MasterScope SystemManager function).

10.44. History of the Event Correlation Function

If a manager is upgraded from the version prior to the version 4.2.0 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]

10.45. 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.

10.46. When Using a Web API

If the Web API updates setting items while the console is displaying the settings screen, a dialog box is displayed prompting you to close the settings screen on the console.
If this dialog box is displayed, close and then reopen the settings screen.

When the performance monitoring function is monitoring 5000 counters, all the counters are registered in the performance management function. Avoid exceeding the specified accumulated log volume in the performance management function when specifying the number of counters.

10.47. 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.

If model generation or analysis is performed on a lot of counters, the memory usage of the process exceeds the limitation, causing the process to fail.

11. Restrictions

11.1. Restrictions on Monitoring Windows Services

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

11.2. Performance monitoring function

A data accuracy error after the decimal may occur in the graph data displayed on the console and the CSV data output by PerformanceCmd.
Performance monitoring of [NetworkInterface] might not be possible to perform on Solaris11.
The value of [Memory]-[% Memory Used Ex] might become invalid on HP-UX when the memory usage for the entire system exceeds 20 GB.
The value of the counter under [Process] might become invalid on HP-UX when the memory usage for the process exceeds 2 GB.

11.3. Impact of time synchronization

When time adjustment is executed manually or through the Network Time Protocol, the performance data is for the period from the last time to the adjusted time, not for the interval period.If the adjusted time is earlier than the last time, the data may be a negative value.
Specify a performance monitoring interval larger than the time adjustment.

11.4. Web console function

- Files to be set up
Only the minimum files required to execute programs are set up for the web console.
The following files are set up for the console installation but are not set up for the web console.

- Knowledge files
- Monitoring template files
- Image files
- Icon files
- Optional modules

Obtain the files required for the web console by referring to the console folder or copy-and-pasting files in the console folder.

- Product knowledge
Using knowledge of other products* on a Web console is not supported yet.

* “Knowledge files related to other products” in “9 Knowledge Information Included in this Product”

11.5. ServiceManager link 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.

11.6. 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

11.7. Monitoring Linux remote hosts

Specify LANG C for the LANG setting of the login user used when monitoring remote hosts that use a Linux OS.

11.8. 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]

11.9. 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 dialog boxes

The target dialog boxes are as follows:

- Message monitoring function
  - Category message dialog box
  -Search result dialog box

- 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

WebSAM SystemManager specific functions

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

11.10. Restrictions when using a console on Windows 7 or later

The operation of this product is not guaranteed in an environment where touch keyboard operation is enabled.

For Windows 7, disable the Tablet PC Input Panel function and “Tablet PC Input Service” of Windows Service.

For Windows 8, disable the touch keyboard function and “Touch Keyboard and Handwriting Panel Service” of Windows Service.

11.11. IPv6

The following functions do not support the IPv6. Establish communications via the IPv4 when the following commands are used.

Standard functions
・Agentless monitoring function
・Manager hierarchization

Optional functions
・SSC linkage function
・Operation control function
・Scenario control function
・Invariant Analyzer function
・ServiceManager linkage function
・ACOS monitoring function

Unique functions of the MasterScope SystemManager
・External product linkage function

11.12. Scenario control function

If the instance which priority of severity is lower than "NOTEXEC" (for example, "NORMAL") remained in history after you remove the history (SWAP), severity color in the tree of Scenario View in the left section of monitoring screen is no longer displayed correctly.

[Recovery method]
Reconfigure the severity from [Options Setting] in the following procedure.

1. Select "Configuration mode" in the [Setting] menu, and go to configuration mode.
2. In [Options Setting] in the [Setting] menu, open the [Options Setting] dialog, and select the [Priority Setting] tab.
3. Select any of severity, click the [Up] arrow key and then click the [down] arrow key to return to the original from replacing the sequence once.
4. Click the [OK] button.

11.13. Message monitoring function

In the [Message] tab of the bottom of the monitoring screen, if you perform the following operation, screen with no message will be displayed.

[Operating procedure]

1. Messages exist more than the maximum display number, and  button is enabled.
2. Click the  button, and move to the previous page. ( Button will be enabled)
3. Click the  button, and return to the latest screen. ( Button will be disabled)
4. In the latest screen, give a mark in any of the message.
5. Click the  button.
6. Screen with no message is displayed.

[Recovery method]

Click the  button to go back to the previous screen.

12. Remarks

12.1. Restarting Mission Critical Operations

The following describes the steps to manually restart MISSION CRITICAL OPERATIONS:

Restarting Manager(Windows)
To restart your manager manually, restart the Windows service (service name: MasterScope UMF Operations Manager_1).

Restarting Agent(Windows)
To restart your agent manually, restart the Windows service (service name: MasterScope UMF Operations Agent_1).

Restarting a remote monitoring agent (Windows)
To restart your remote monitoring agent manually, restart a Windows service (service name: MasterScope UMF Operations Remote Agent_1).

Restarting external IA engine (Windows).
To manually restart external IA engine, please restart the following windows service.
ServiceName: MasterScope UMF Operations RelayManager_1

Restarting Manager(HP-UX)
To restart your manager manually, execute the following.

```
# sh /sbin/init.d/UMFOperationsManager_1 stop [-i retry interval(second)] [-c retry count]↵
# sh /sbin/init.d/UMFOperationsManager_1 start ↵
```

Restarting Agent(HP-UX)
To restart your agent manually, execute the following.

```
# sh /sbin/init.d/UMFOperationsAgent_1 stop [-i retry interval(second)] [-c retry count]↵
# sh /sbin/init.d/UMFOperationsAgent_1 start ↵
```

Restarting IA external engine (HP-UX)
To restart your IA external engine manually, execute the following.

```
# sh /sbin/init.d/ UMFOperationsRelayManager_1 stop [-i retry interval(second)] [-c retry count]↵
# sh /sbin/init.d/ UMFOperationsRelayManager_1 start ↵
```

Restarting Manager(Linux)
To restart your manager manually, execute the following.

```
# sh /etc/init.d/UMFOperationsManager_1 stop [-i retry interval(second)] [-c retry count]↵
```

```
# sh /etc/init.d/UMFOperationsManager_1 start ↵
```

Restarting Agent(Linux)

To restart your agent manually, execute the following.

```
# sh /etc/init.d/UMFOperationsAgent_1 stop [-i retry interval(second)] [-c retry count]↵
# sh /etc/init.d/UMFOperationsAgent_1 start ↵
```

Restarting IA external engine (Linux)

To restart your IA external engine manually, execute the following.

```
# sh /etc/init.d/ UMFOperationsRelayManager_1 stop [-i retry interval(second)] [-c retry count]↵
# sh /etc/init.d/ UMFOperationsRelayManager_1 start ↵
```

Restarting Agent(Solaris)

To restart your agent manually, execute the following.

```
# sh /etc/init.d/UMFOperationsAgent_1 stop [-i retry interval(second)] [-c retry count]↵
# sh /etc/init.d/UMFOperationsAgent_1 start ↵
```

Restarting Agent(AIX)

To restart your agent manually, execute the following.

```
# sh /etc/rc.d/init.d/UMFOperationsAgent_1 stop [-i retry interval(second)] [-c retry count]↵
# sh /etc/rc.d/init.d/UMFOperationsAgent_1 start ↵
```

The retry option of the stop command is an option to extend the completion check for service processes. Usually it is not necessary to specify this option. The retry option might be useful when an abnormal end with a return value other than 0 occurs.

For example, if “-i 1 –c 5” is specified, the service process completion check is performed up to 5 times at intervals of 1 second by using the ps command immediately after the stop command for the service process times out. If the service process is eliminated during the process completion check, the process completion check ends at this point and the stop command ends normally.

1 or a larger number must be specified for the retry count when the retry option is specified. The valid specification range for the retry interval is from 1 to 60.

※ In UNIX (HP-UX, Linux, Solaris, AIX), run the command with an account that has root authority.

※ If you install the product to the directory where other MasterScope products have been installed, the existing service and rc script file will be used. Read the contents above accordingly.

※ If you install this product in a server that service and rc script file of the same name are used by another MasterScope product, the suffix number is changed to 2 or more (e.g. MasterScope UMF Operations Manager_2, UMFOperationsAgent_3). Read the service names above accordingly.

12.2. 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

* When performing the operation, be sure to change the Administrator password.

12.3. About Monitoring Microsoft Products

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, then 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 kbfind.zip and referring to read_kbfind.txt, which will be created in the location to which kbfind.zip is unzipped.

12.4. About WebLogic monitoring

To import and use the knowledge files for WebLogic, monitor the following log file by the application log monitoring function.

Windows: <DOMAIN_HOME>\servers\<SERVER_NAME>\logs\<SERVER_NAME>.log
e.g.) c:\bea\user_projects\domains\base_domain\servers\AdminServer\logs\AdminServer.log

UNIX : <DOMAIN_HOME>/servers/<SERVER_NAME>/logs/<SERVER_NAME>.log
e.g.)
${HOME}/bea/user_projects/domains/base_domain/servers/AdminServer/logs/AdminServer.log
* ${HOME} is the home directory of user which have installed WebLogic.

12.5. Holding Data on Agents

If agents cannot reach managers due to their outage or a network failure, agents hold data and send it when they become available again.
Agents hold the following data.

- Log data collected by the event log monitoring function
- Log data collected by the syslog monitoring function

- Log data collected by the application log monitoring function
- Messages issued by CDO message API
- Messages issued by Operational Message Notification API function

At the status of installation, 200 packets of each data are storead respectively.
For the event log monitoring function, the syslog monitoring function and the application log monitoring function, agents can store up to 128 logs collected in one monitoring process into one packet.
If stored data exceeds the limit, log data begins to be deleted in the chronological order, beginning with the oldest.

If you want to change the limit of available packets from 200, follow the next steps of instructions.

1. Edit the following files of agents by a text editor.

   Event log monitoring function
   Windows: <Agent install directory>\Agent\sg\EventLogHelperAgt.ini

   syslog monitoring function
   UNIX : <Aent install directory>/Agent/sg/SysLogHelperAgt.ini

   Application log monitoring function
   Windows: <Agent install directory>\Agent\sg\ApLogHelperAgt.ini
   UNIX : <Agent install directory>/Agent/sg/ApLogHelperAgt.ini

   CDO message API
   Windows: <Agent install directory>\Agent\sg\MessageAgt.ini
   UNIX : <Agent install directory>/Agent/sg/MessageAgt.ini

   Operational Message Notification API function(Operational Message Notification Command)
   Windows: <Agent install directory>\Agent\sg\SysMgrMRCASAgt.ini
   UNIX : <Agent install directory>/Agent/sg/SysMgrMRCASAgt.ini

   ```
   [Passage]
   OutputQueueSize=200
   ```

   * 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.

   Change 200 specified above to any number.

2. Reboot agents.

Note: Each held piece of the information uses about 3 KB in disk. As the event log monitoring function, syslog monitoring function, and application log monitoring function store a maximum of 128 logs in a file when more than one log was collected in one monitoring timing, they use up to 3 KB x 128 x value of OutputQueueSize in disk.

Note: If you have set a large number as a limit, managers might be overloaded when a large amounts of data is sent to them all at once after the connection is recovered. Therefore, you should set a reasonable value as a limit if you have many agents.

12.6. About Holding Information on Remote Monitoring Agent

If a remote monitoring agent cannot be connected to its manager due to some reasons such as the manager being stopped or a network failure, the system holds information on the agent and sends the information to the manager when the agent is connected to the manager.
The following lists the information to be held.

- Logs acquired with the event log monitoring function
- Logs acquired with the syslog monitoring function
- Logs acquired with the application log monitoring function
- Error messages that occurred within the remote monitoring agent

For each remote host, 200 packets of the event log information and 200 packets of the application log information are held if the settings have not been changed after installation.
The event log monitoring function and the application log monitoring function store 128 logs obtained in one monitoring timing in one packet.

If the setting has not been changed after installation, 20,000 error messages that occur within the remote monitoring agent are held.

When these upper limits for the held pieces of information are exceeded, the older information will be deleted in order.

If you need to change the numbers of held pieces of information, carry out the following steps.

1. Edit the following files on the remote monitoring agent with your text editor:
   Event log monitoring function
   <Remote monitoring agent installation directory>\Agent\sg\EventLogHelperAgt.ini

   Syslog monitoring function
   <Remote monitoring agent installation directory>\Agent\sg\SysLogHelperAgt.ini

   Application log monitoring function
   <Remote monitoring agent installation directory>\Agent\sg\ApLogHelperAgt.ini

   Error messages within the remote monitoring agent
   <Remote monitoring agent installation directory>\Agent\sg\MessageAgt.ini

[Passage] OutputQueueSize=**200**

*Describe using UTF-16 LE code for the character encoding and CR+LF for the line feed code.

Change the "200" shown above to any desired value.

※ In the case of MessageAgt.ini, the initial value is 20000.

2. Restart the agent.

※ Each held piece of the information uses about 3 KB in disk. As the event log monitoring function and application log monitoring function store a maximum of 128 logs in a file when more than one log was collected in one monitoring timing, they use up to 3 KB x 128 x value of OutputQueueSize of disk for one host to be monitored.

※ If the numbers of held pieces of the information are set to a large value, vast amount of information will be reported to the manager at once as soon as the connection to the manager is restored; as this may cause too much load to be imposed on the manager, the memory resources may be used up. As the information for the number of remote hosts is held on the remote monitoring agent, many disks could be used. If you have the large number of remote hosts, please design the upper limits carefully.

※ If you adopt a duplexed configuration for the remote monitoring agent, configure the settings both in the active system and in the standby system.

12.7. Change Message Management Queue Size on Manager

The internal queue size for message processing on a manager is limited to 5000 in default from Ver 3.4 in order to prevent from exhausting memory resource when messages are not well fitered and the manager can not process messages.
If the limit is exceeded, old messages in the internal queue are deleted, issuing a message that informs of the deletion. Message format is as below.

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

Note: %d specifies the number of deleted messages, and then duration of received dates of deleted messages is displayed.

To change the internal queue size from 5000, please perform the following steps.

1. Edit the following file of a manager with a text editor.
   Windows: <Manager install directory>\Manager\sg\MessageMgr.ini
   UNIX : <Manager install directory>/Manager/sg/MessageMgr.ini

```
[Passage]
InputQueueSize=5000
```

   * 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.

   Change 5000 above to other number.

   Note: Create the file if it doesn't exist. The queue size is unlimited if specifying 0.

2. Reboot the manager

※ If a message is deleted due to exceed the limit of internal queue size, please refine setting as the following causes are suspected
- ✓ Messages collected to a manager are too much
  - As the same logs might be duplicated on a failure, please enable "Same Message Ignore Function".
  - Filter definition of log monitoring on agent might be set to notify all the logs as messages. In that case, especially many agents are managed by a manager, please consider the filter definition on agents not to notify 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.)

12.8. List of communication ports

MasterScope uses the network ports shown below.To operate MasterScope normally, change the firewall settings to enable communication through the network ports shown below.

	Sender	Port	Direction	Receiver	Port	
Manager-agent, manager-IA external engine, manager-Event Trap Utility communication	Agent IA external engine Event Trap Utility	ANY/TCP (*1)	→	Manager	12520/TCP	Alterable (12507 when installed in a directory that differs from that of other MasterScope products)
Manager-console communication	Console	ANY/TCP (*1)	→	Manager	12521/TCP	Alterable (12508 when installed in a directory that differs from that of other MasterScope products)
Manager-Web console communication	Web console	ANY/TCP (*1)	→	Manager	8080/TCP	A value between 1000 and 32767 that is not used by MasterScope framework supporting products Alterable (See the Release Note in the MasterScope media.)

	Web console	ANY/TCP (*1)	→	Manager	12521/TCP	A value between 1000 and 32767 that is not used by MasterScope framework supporting products Alterable (See the Release Note in the MasterScope media.)
Used within an manager	Manager	ANY/TCP (*1)	→	Manager	12521/TCP	Command of this product uses.
Hierachical Manager	Lower Manager	ANY/TCP (*1)	→	Upper Manager	12520/TCP	Specify a port used for communication with an agent of a upper manager.
Used within an agent	Agent	ANY/TCP (*1)	→	Agent	12570 to 12589/TCP	A value between 12570 and 12589 that is not used by MasterScope framework supporting products Alterable (See the Release Note in the MasterScope media.)
Email report	Manager	ANY/TCP (*1)	→	Mail server	1 to 32767/TCP	Specify a value between 1 and 32767 according to the mail server (SMTP server) port.
Patrol lamp report (RS232C connection)	Manager	ANY/TCP (*2)	→	Patrol lamp	1 to 32767/TCP	Specify a value between 1 and 32767 according to the mail server (SMTP server) port.

Patrol lamp report (LAN connection)	Patrol lamp	ANY/TCP (*2)	→	Manager	1022/TCP (*2)	When “PHC-100A, PHE-3FB, PHE-3FBE1” is specified for the type.
	Manager	ANY/TCP (*3)	→	Patrol lamp	514/TCP	When “NHE-3FB, NHM-3FB” is specified for the type.
Service Manager Linker	Manager	ANY/TCP (*1)	→	Service Manager	1～65535/TCP	Specify a value between 1 and 65535 according to the ServiceManager Server port.
Used for ServerAgent link	ServerAgent	ANY/TCP (*1)	→	Manager	31134/TCP	When using the ServerAgent link function Alterable (see the Release Note of the ServerAgent link function)

※ ANY indicates a port number between 1024 and 65535.

※ Use a port number between 512 and 1022 when rsh has been started and port number 1022 is used.

※ Use a port number between 513 and 1023 when rsh has been started and port number 1023 is used.

For the port number used by the agentless monitoring function, see “12.11Security Settings for Agentless Monitoring Function”.

12.9. Stopping the accumulation of 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 manual (help).
Do not perform this procedure if Invariant Analyzer or the performance information display or form function of SystemManager is being used because the performance information needs to be accumulated on the manager.

12.10. Set the Method to Display Command Name for the 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 MCOperations 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)]

12.11. Security Settings for Agentless Monitoring Function

This section describes security settings for remote monitoring agents and remote hosts that are required to use the agentless monitoring function.

12.11.1. Windows

In the Windows agentless monitoring function, you must configure security settings for WMI and those for network resources described below about remote hosts in order to collection information through WMI and by 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.

[Windows Server 2008 / 2008R2 / 2012/ 2012R2 setting procedure]

1. Open [Security-enhanced Windows Firewall].
2. Select and right-click the following items in [Rx rule]/[Tx rule] to display properties.
   - Windows Management Instrumentation(DCOM Rx)
   - Windows Management Instrumentation(WMI Rx)
3. Select [Allow connection] in [Operation] and click the [OK] button.

■Security settings for network resources
In the remote monitoring agent and remote host, you must allow access to network resources.

[Windows Server 2008 / 2008R2 / 2012/ 2012R2 setting procedure]

1. Open [Control Panel] -[Windows Firewall].
2. Open the [Exception] tab and check [Share File and Printer].

[Setting procedure for vaccine software]
Vaccine software may cause the agentless monitoring function to malfunction by blocking the function from accessing files. The following describes steps to set “VirusScan Enterprise 8.7.0i” from McAfee to prevent this from happening.

1. Start [VirusScan console].
2. Double-click [Access Protection].
3. Select [Virus measures outbreak control] and deselect the [Prohibit read and write from all shares] block.

12.12. 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.
Note that there are precautions for this function. When using this function, confirm the precautions below before use.

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:
   <Installation path>\Manager\sg\TopologyMgr.ini

   HP-UX/Linux manager:
   <Installation path>/Manager/sg/TopologyMgr.ini

   Setting content:

```
[Restart]
StatusKeep=1
```

   * <Installation path> indicates the installation path of the MCOperations manager.

* 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.

■ Precautions
When this function is enabled, the importance color for each agent in the topology view changes according to the connection status between the manager and agent as in the conventional way. The importance color of “STOP” when disconnected and the actual importance color of the agent when connected are reflected.

12.13. Guidelines when specifying MCOperations monitoring settings

Use the following information as a guideline when specifying MCOperations settings such as specifying monitoring items and setting up performance monitoring. The described values are just a rough indication, so that the monitoring would never be immediately stopped when the actual value exceeds the described value. We appreciate your adequate assessment for the monitoring specification in advance. The total number of the values set in the respective products shall be set as a rough indication when the multiple WebSAM Framework products are installed in an identical service.

12.13.1. 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.

12.13.2. 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 "12.7 Change Message Management Queue Size on Manager" * 1 *2

Item	Specification value
Business view (*3)	80/sec
Message view (*4)	80/sec

*1: If the queue size is increased, approximately 80 bytes of memory and 3,000 bytes of free disk space are consumed per additional item of data.

*2: This is a guide to the total number of messages to be filtered. It is not the number of messages that matched the filter condition and were 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.

12.13.3. 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
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

12.13.4. 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)	5,000 data/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.

12.13.5. 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

12.13.6. 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 sys-log 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 (in single byte)
Command line: 50 characters (in single byte)
Default setting for the items other than described above (any value can be set for the numeric value entry.)

*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 (in single byte)
Monitoring target: 50 characters (in single byte)
Default settings for other items (any values for numeric entries)

*3. With respect to the target log to be monitored, the flow rate of the logs that are added is large, it will take much time for reading and filtering processing, resulting in the message output possibly being 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 (in double bytes)
Message text: 40 characters (in double bytes)
Node name: 6 characters (in single byte)
Application name: 10 characters (in single byte)
Object name: 10 characters (in single byte)
Message ID: 10 characters (in double bytes)
Severity setting: Enabled
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 (in double bytes)
Application name: 10 characters (in single byte)
Message ID: 10 characters (in double bytes)
Message text: 40 characters (in double bytes)
Severity setting: Enabled
Default settings for other items

*6. When the performance monitoring function is monitoring 5000 counters, all the counters are registered in the performance management function. Avoid exceeding the specified accumulated log volume in the performance management function when specifying the number of counters.

12.13.7. Manager definition volume

The specifications of the definitions for each manager function are as follows:

Item	Specification value
Number of categories for the business view	200
Number of scheduled categories	50
Number of categories linked to manager	50
Number of business view filters (*1 *2)	10000
Number of filters with recovery setting	1000

Number of filters with reporting setting	1000
Number of filters linked to service manager	1000
Number of recovery definitions	100
Number of reporting definitions	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 launcher function definitions	100
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 following cases, "80 messages per second for a single manager" that is specified as indicated in A), cannot possibly 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 (in double bytes) Node name: 255 characters (in single byte) Message ID: 10 characters (in double bytes) Message text: 40 characters (in double bytes) Related information: One of them must be set.

Displayed name: 40 characters (in double bytes)
Application: 3 characters (in single byte)
Working directory: 20 characters (in single byte)
Severity setting: Enabled
Reporting setting: Enabled
Default settings for other items

- The product is evaluated in the following environment. The specification values cannot be satisfied depending on the environment.

[Environment for the manager evaluation]
Windows

OS	Windows Server 2008 R2 Enterprise
CPU	Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz 8Core
Memory	16 GB
Network	1 Gbps
Disk	NEC Storage M500

Linux

OS	Red Hat Enterprise Linux 6.2 (x86_64)
CPU	Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz 8Core
Memory	16GB
Network	1 Gbps
Disk	NEC Storage M500

HP-UX

OS	HP-UX 11i v3 (Itanium)
CPU	Intel(R) Itanium 2 9100 series processors (1.42 GHz, 12 MB) 8Core
Memory	31.97 GB
Network	1 Gbps
Disk	NEC Storage M500

- The specification values described above are just a rough indication. The processing load of MISSION CRITICAL OPERATIONS fluctuates depending on the contents to be defined for monitoring (for example, the order for filter application, contents of the regular expression, with/without the linkage setting, for example, reporting, and the monitoring interval, and others).

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. The entire filtering process is wasted when there is no match for the condition in all of the filtering processes. Since the processing load is larger depending on the status of the target for the filtering process, it is recommended to locate filters with higher match rates on the upper side of the filter definition list, or to set the definition that deletes unnecessary messages by using the delete filter.

- When some of the functions are not used, it may be possible to increase the specification value of the other monitoring items. 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.

12.14. Upper Limit for Business View Message Accumulation

In the business view, the maximum number of messages that can be accumulated for one category in one day is approximately 700,000, and subsequent messages are not accumulated when this maximum has been reached. Message accumulation resumes as the date changes at midnight (0:00).

12.15. Authentication information setting for agentless monitoring function

12.15.1. 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.

1. 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.

2. 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.