Orchestrating a brighter world

NEC

MasterScope SystemManager G Function Introduction

NEC Corporation
2018

MasterScope

Function Lists

Major functions of MasterScope SystemManager G
(standard functions)

Category	Function	Functional outline
Monitoring functions	Service and process monitoring	• Windows service alive monitoring/process alive monitoring • Threshold monitoring of process ID changes and the number of startup processes.
	Performance monitoring	• Resource information (CPU/memory usage, disk usage, etc.) is collected from each server and threshold monitoring of upper and lower limitation is performed. Performance monitoring per process is available as well. • Threshold monitoring and notification to the operator by three judgment methods: sequential, N times continuous, N times average. • Resource information can be accumulated and displayed as a graph or printed out. Support for analyzing operating status and problems.
	Log monitoring • Event logs • Syslogs • Application logs	• Message monitoring by extracting necessary logs from syslogs, event log, and any text log files output by applications. • Suppress identical messages on the Agent side to avoid message overload.
	File and directory capacity monitoring	• Monitor existence, capacity, and updates of files and directories. • Prevent disk space exhaustion and enable early detection of essential system file deletion or update.
	Service port monitoring	• Monitor open/close status of user-specified TCP/UDP ports
Management functions	Topology management	Monitoring target servers can be grouped by location or customer-specified role.
	Message management	Messages can be accumulated and managemed per server or system. Messages can be marked according to the presence of comments or response status, allowing information to be shard between operators.
	Notification control	• Notification by email or alarm lamp triggered by message issuance, change in monitoring process or service status, or excess of resource threshold values. • Commands can be executed on the Manager triggered by message issuance.
	Configuration management	Centralized view of monitoring target server configuration information (such as devices, systems, software, networks, and disks)
	User management	Limitation of investigation range authorities for each user prevents operational errors and improves security by assigning appropriate authorities.
	Audit logs management	Support for internal control by managing the operational details and result history of operations performed on the console and automatically executed.
	Schedule control	Schedule monitoring to start/stop for each server.
	Command execution	Predefined recovery commands can be executed triggered by events.
Build functions	Agent auto-build	Ansible scenarios (roles) is provided to perform operations from Agent installation to monitoring configuration. Remote execution and error-free auto-building of Agents.

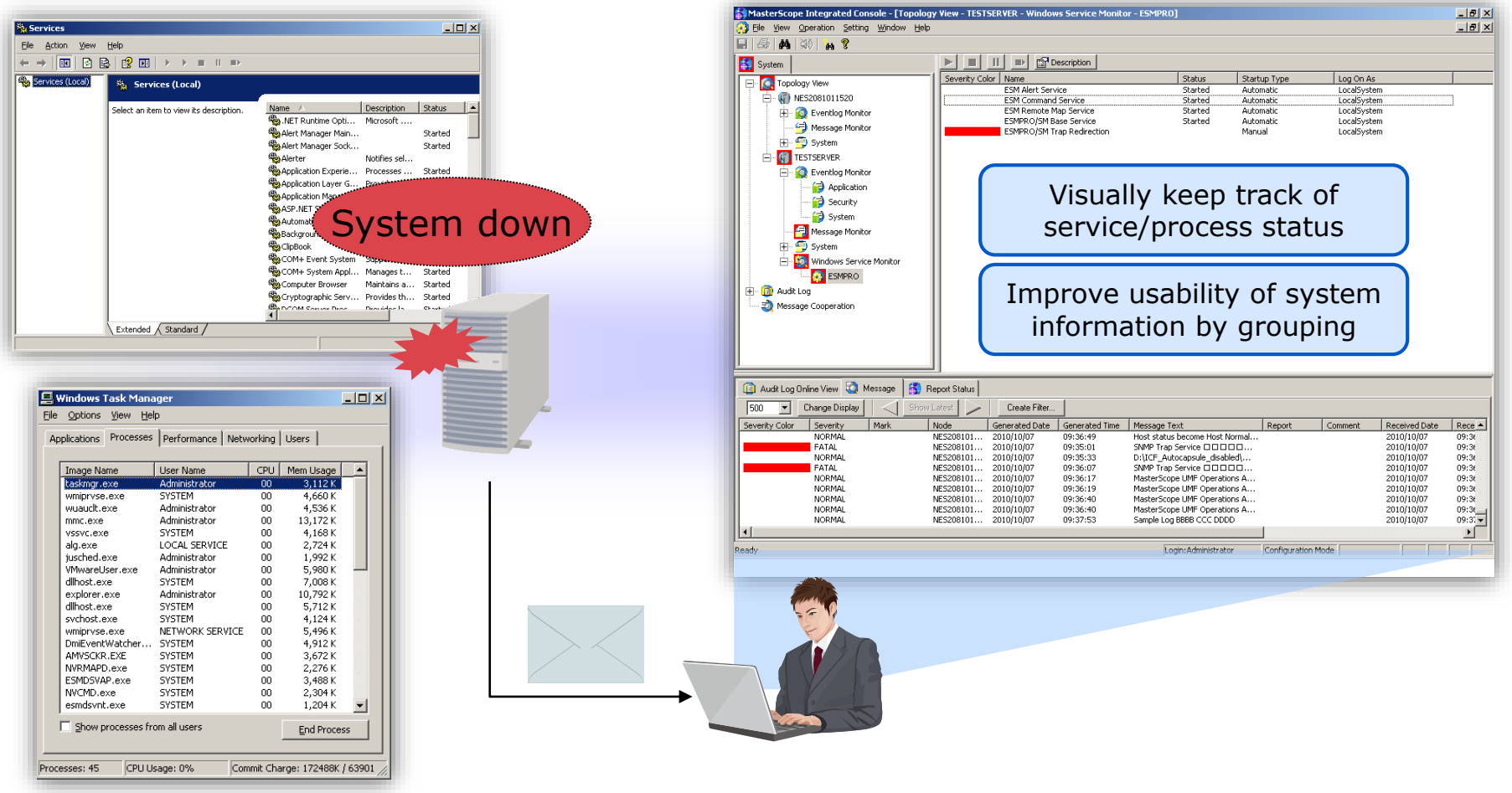
Major functions of MasterScope SystemManager G
(optional functions)

Category	Function	Functional outline
Monitoring functions	Application monitoring	Monitoring of performance with graphical view of application operating status. Accumulation of operating status data as statistics for system problem analysis and improvement.
	IT service response monitoring	Monitoring of end-to-end operating status and response for HTTP, Mail, DNS, TCP, and FCP based on settings that accord with the user's purpose.
	Hypervisor monitoring	Monitoring of virtual server resources and events for the hypervisor (VMware ESXi).
	Cloud monitoring	Instances on the cloud can be monitored via an API provided by public cloud (CloudWatch) without installing an Agent.
	Customizable performance monitoring	User-specified commands and program output results can be extracted by column and used as monitor counters. It can be displayed as a graph or output as a unified form.
Management functions	Message management (Monitoring from a business perspective)	Events reported from monitoring targets can be classified on the Business View from the perspective of the customer's business.
	Knowledge management	Users are informed of actions to take for failure recovery.
	Message correlation analysis	Correlation analysis function of multiple event information, automated action, and notification. Conditions can be specified such as the satisfaction of condition 1 & condition 2, and the occurrence of an event for the specified number of times within the specified time frame.
	Hierarchical Manager	Messages across the entire system are monitored centrally by linking multiple Managers hierarchically and having lower-level Managers report collected messages to higher level Managers.
	System performance analysis	Regression analysis on collected performance data shows the tendency and predicts the future values. Correlation analysis on collected performance data detects abnormal behavior and suggests the cause.
	Web Console	Web-based monitoring dashboard to view overall system status at a glance.
Control functions	Operation control	Commands can be executed for monitoring target servers at user-specified timing.
	Workflow control	Flows such as failure recovery and daily operations can be predefined as scenarios and automatically executed.
Linkage functions	Application linkage	Logs collected by MasterScope SystemManager G can be output as text files.
	Service desk linkage	Incidents can be registered to incident management software automatically or manually.

Function Detail

Service and Process Monitoring

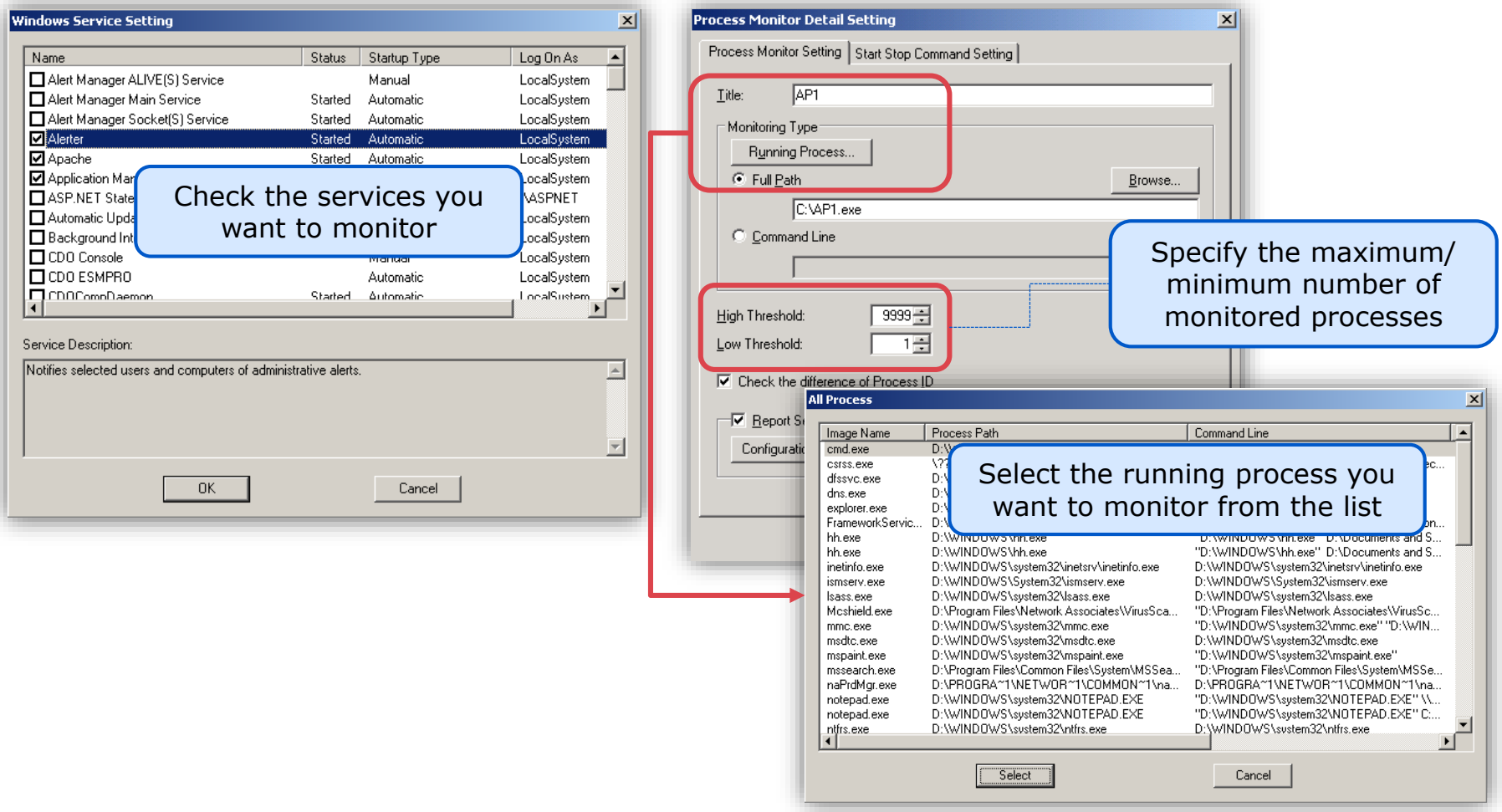
Monitoring processes and services allows admin to receive alerts when an anomaly is detected.



Service and Process Monitoring Setup

■Service monitoring setup

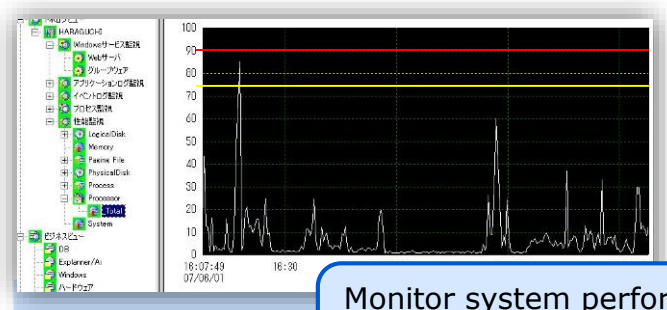
■Process monitoring setup



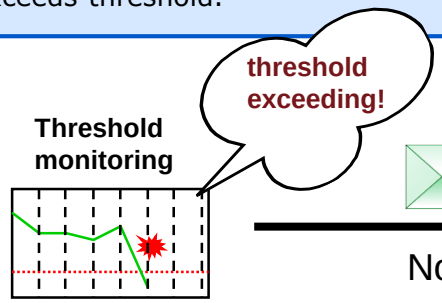
Performance Monitoring

Monitor OS information (like CPU utilization, memory, and disk space) by simply setting thresholds to warning and anomaly notifications.

Available threshold setting can be selected from the following patterns:
Sequential: an event occurs when a collected value exceeds threshold
Continuous: an event occurs when a collected value exceeds threshold consecutively for the specified number of times
Average: an event occurs when the average collected values of the specified number of times exceeds threshold.

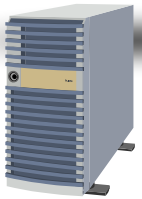


Monitor system performance with two level threshold settings



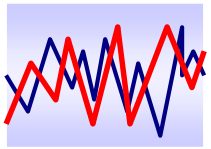
Example:
If available MEM become less than 50Mbytes, notify admins of an anomaly.

Notify



Performance data

Performance data accumulation enables
Tendency/Resource analysis

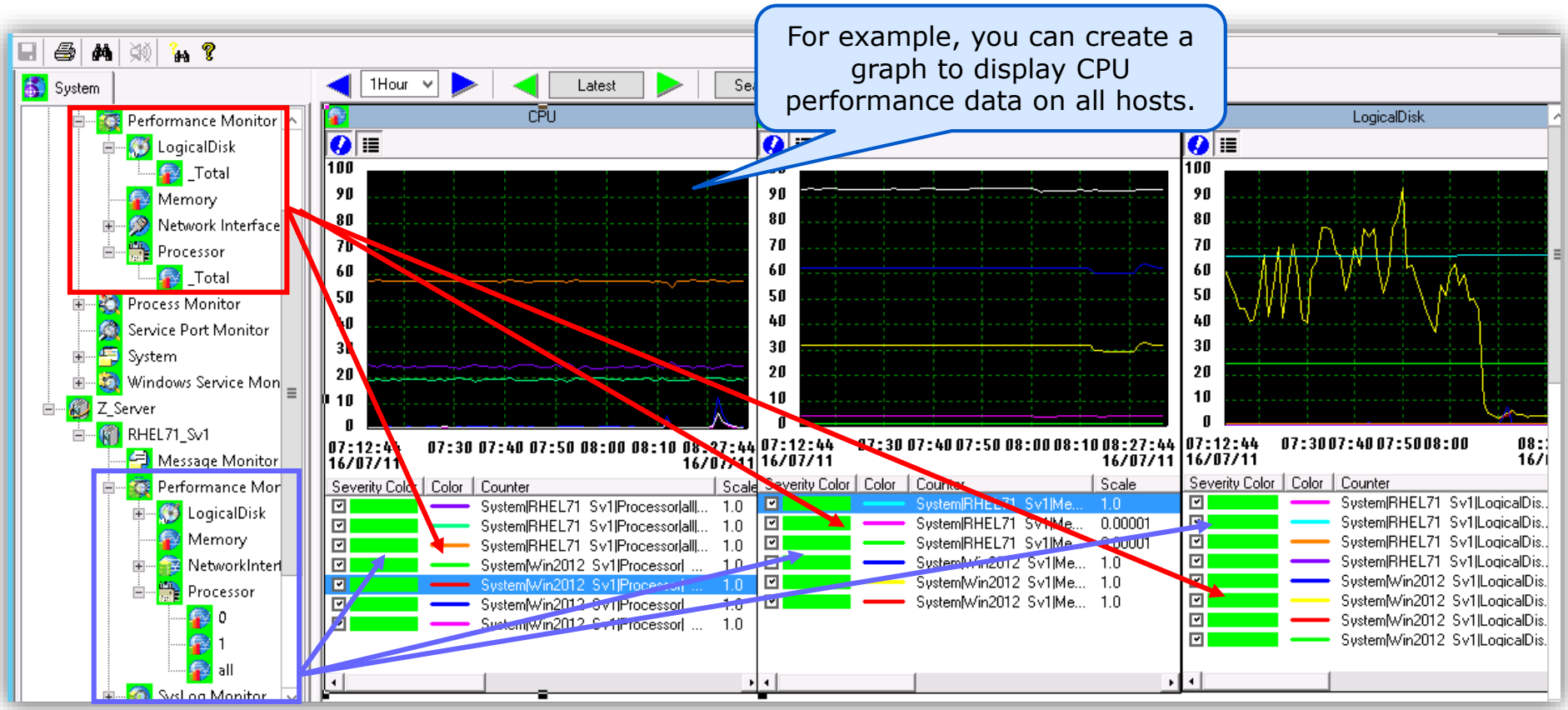


Performance data accumulation could be utilized for operations status/failure analysis

Performance data accumulation can be enabled simply by checking settings boxes

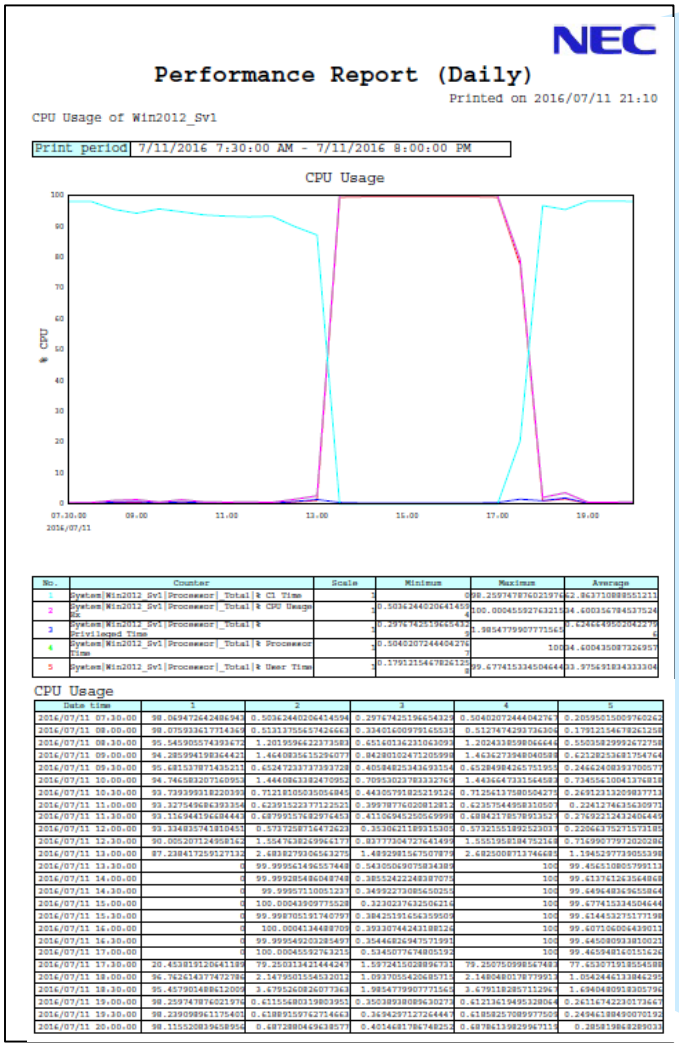
Reporting (Multi-Graph View)

SystemManager G provides a multi-graph view to visualize the data gathered from the hosts and quickly creates a graph to compare the past data and the current data.



Reporting (Print view)

Report the performance data collected on SystemManager G to a PDF file.



NEC

Performance Report (Daily)

Printed on 2016/07/11 21:10

CPU Usage of Win2012_Sv1

Print period 7/11/2016 7:30:00 AM - 7/11/2016 8:00:00 PM

CPU Usage

% CPU

2016/07/11

CPU Usage

Graph of performance data

Maximum, minimum and average of each counter

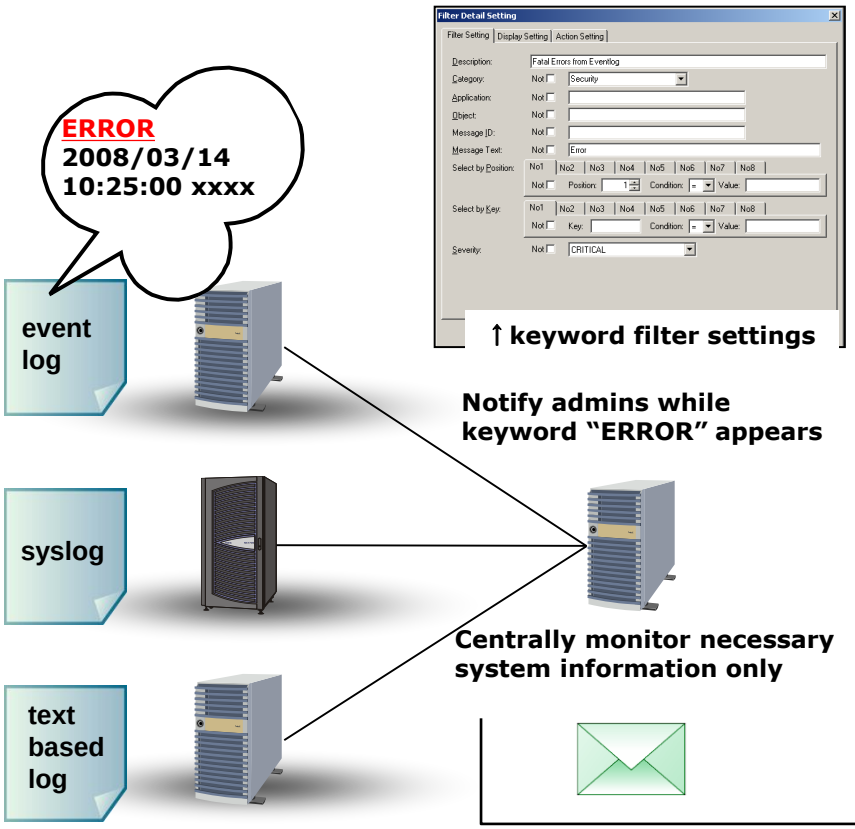
History of each counter

Reporting the performance data in predefined intervals (weekly/monthly/yearly)

Administrator

Log Monitoring (event log/syslog/application log)

Monitor all text-based log/syslog/event log, and notifies admin on specified information with the keyword filtering.



↑keyword filter settings

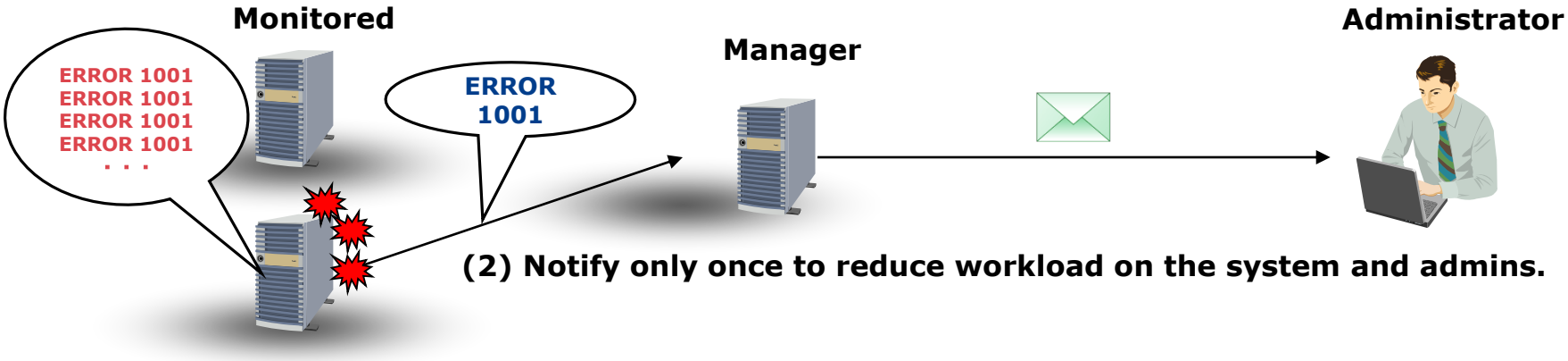
Notify admins while keyword "ERROR" appears

Centrally monitor necessary system information only

*Some text-based log files are rotated in some unintentional situations (its size exceeds some values, date change, etc.). MasterScope SystemManager G is capable of monitoring this type of text-based log.

(Ref) Keyword Filtering

Message filtering extracts important messages and suppresses duplicate messages for efficient analysis.



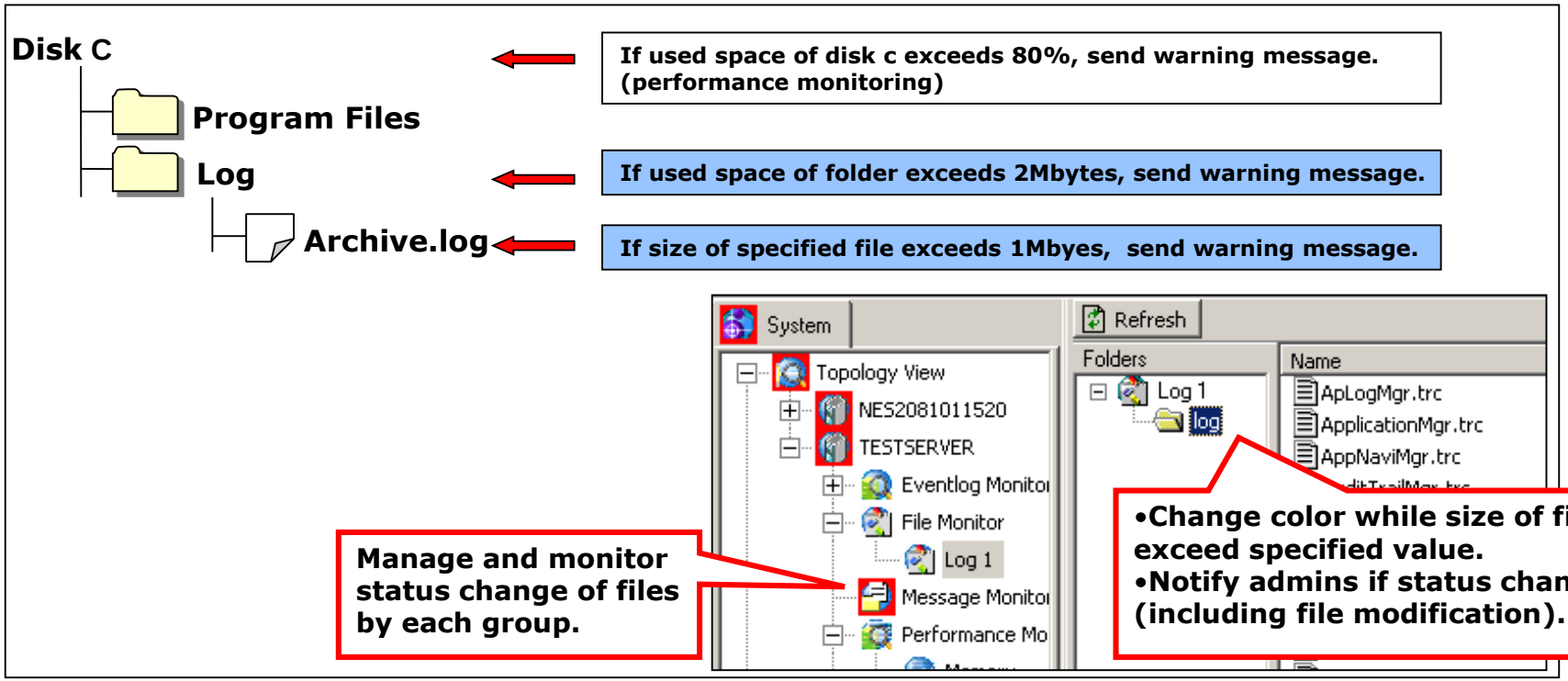
Functions	Description
Filter for extraction	Notify if a message includes the specified keywords.
Filter for deletion	Do not notify if a message include the specified keywords.
Suppression of duplicate messages	Do not notify if identical messages are generated during the specified time frame.

File and Directory Monitoring

File/directory monitoring prevents disk depletion by monitoring file size and enables early detection of deletion/modification of important files.

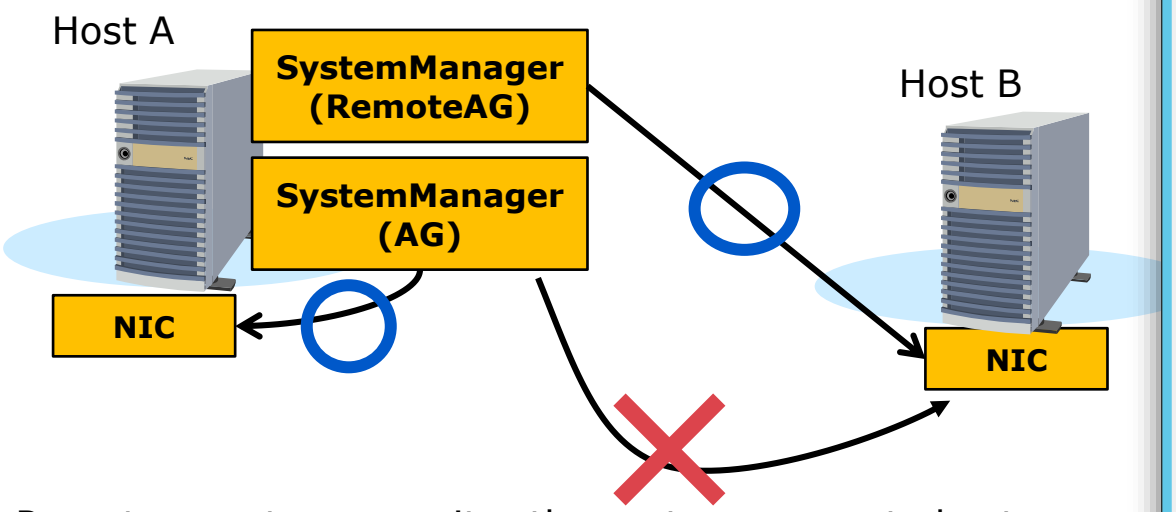
- ✓ Monitors target agents' files and directories for their existence, used space and modification
- ✓ Changes the color of icon if utilization of file exceeds specified value, or file is deleted
- ✓ Message or alert is notified if its status changes (including file modification)

<Example: monitoring log files/folders>

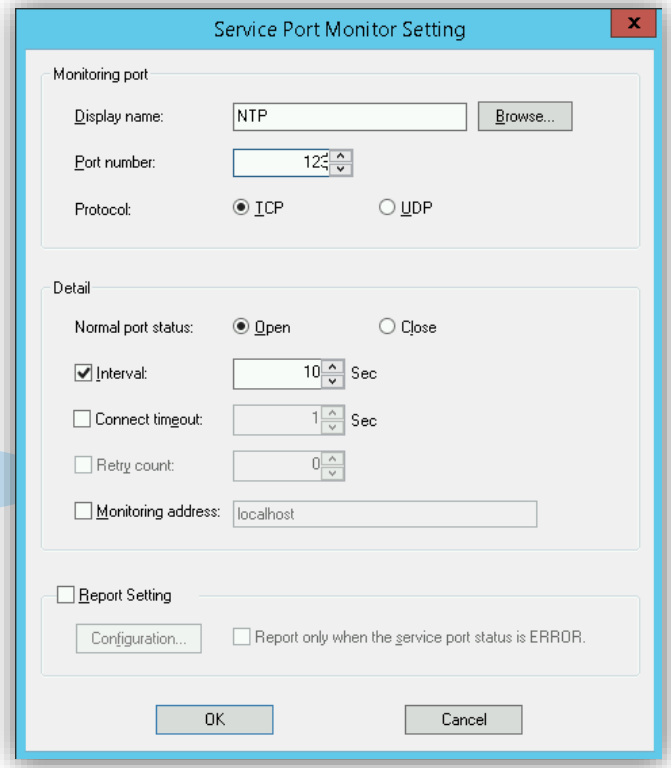


Service Port Monitoring

Monitor TCP/UDP port (ftp, telnet, http, etc.) on the agent. Show message on message view if the status of monitored port is changed.



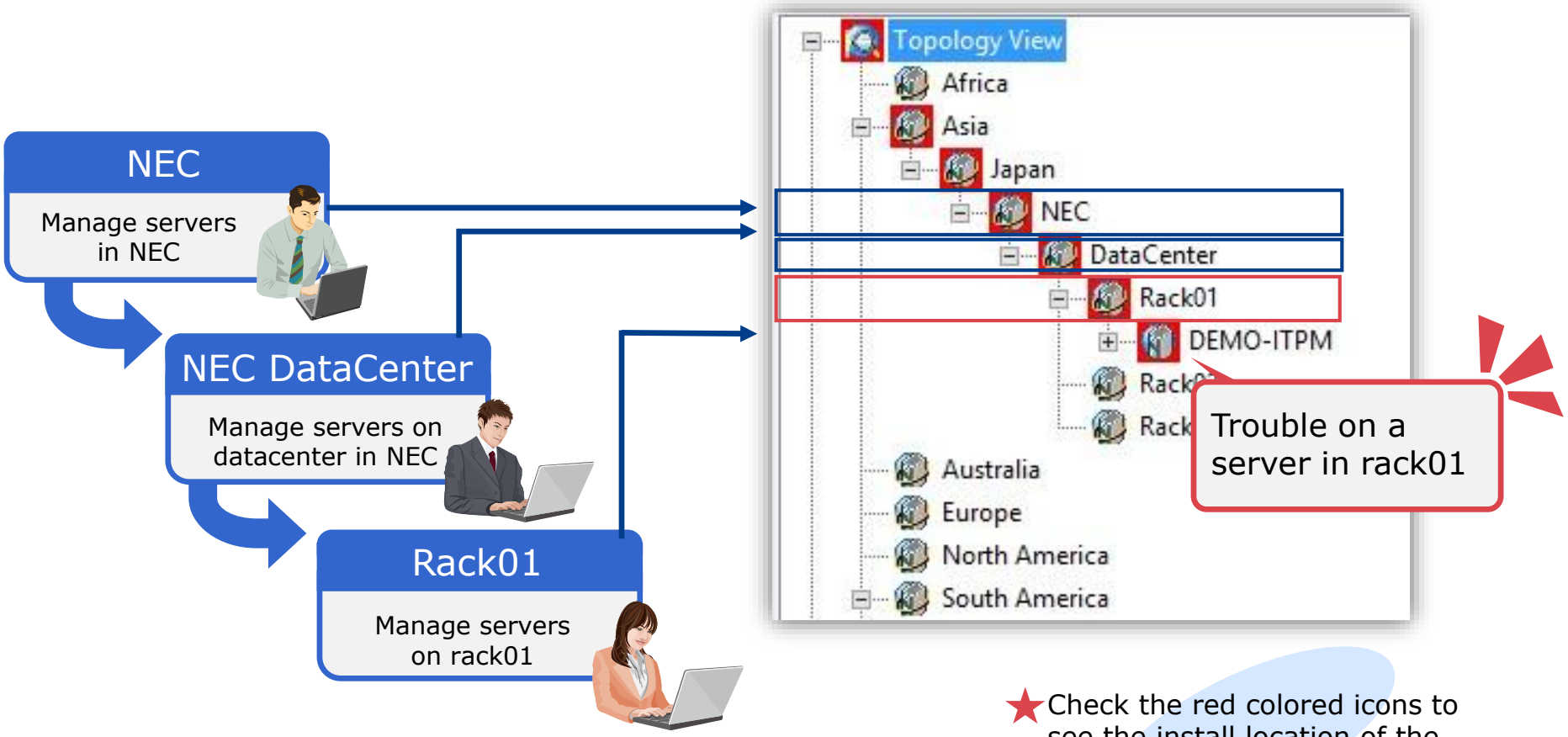
Remote agent can monitor the port on a remote host



Service Port Monitor Setting

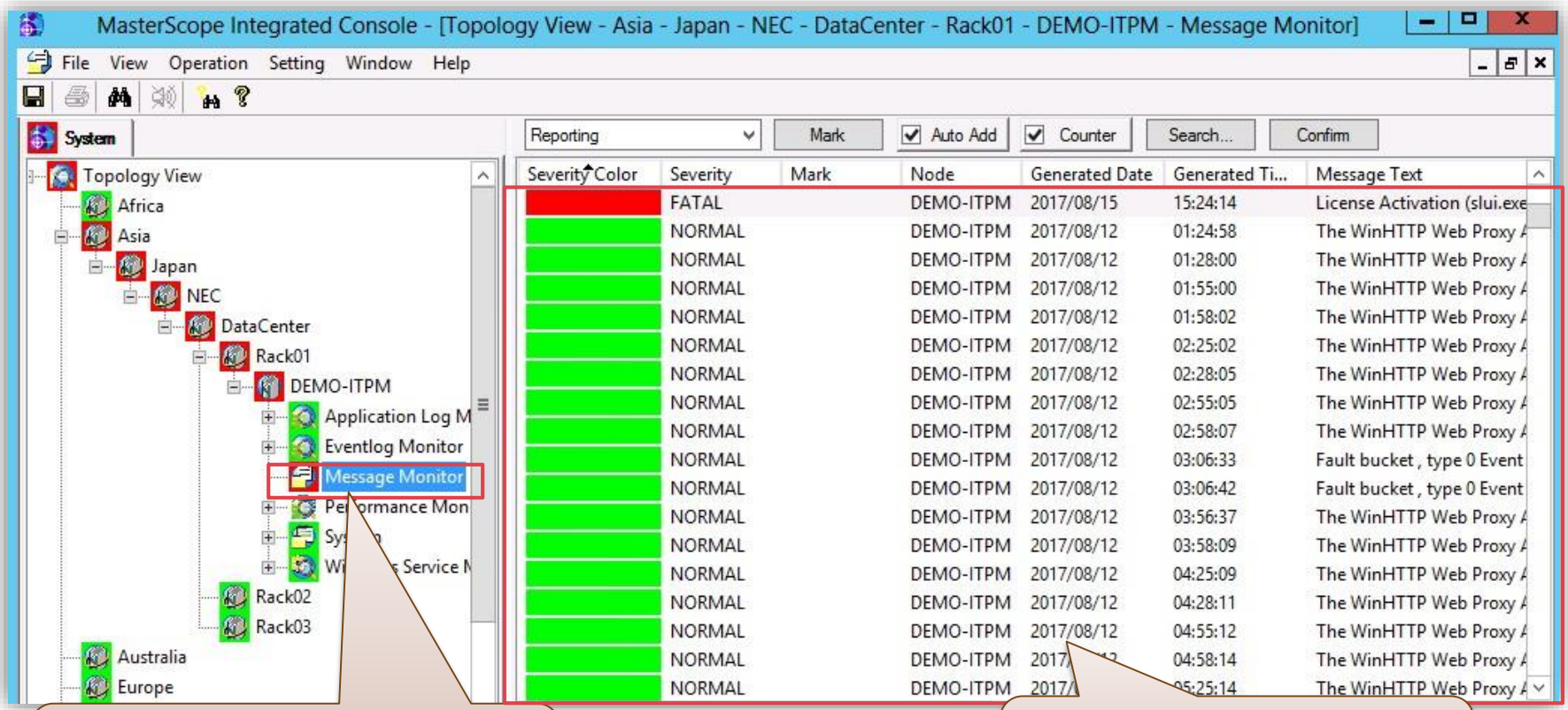
Topology Management（from the view point of managing server）

Topology view allows you not only to monitor server physically, but also to manage servers with information about location and role.



Message Management（1/2）

Message management function allows you to monitor messages generated by log monitoring, process monitoring, and so on.

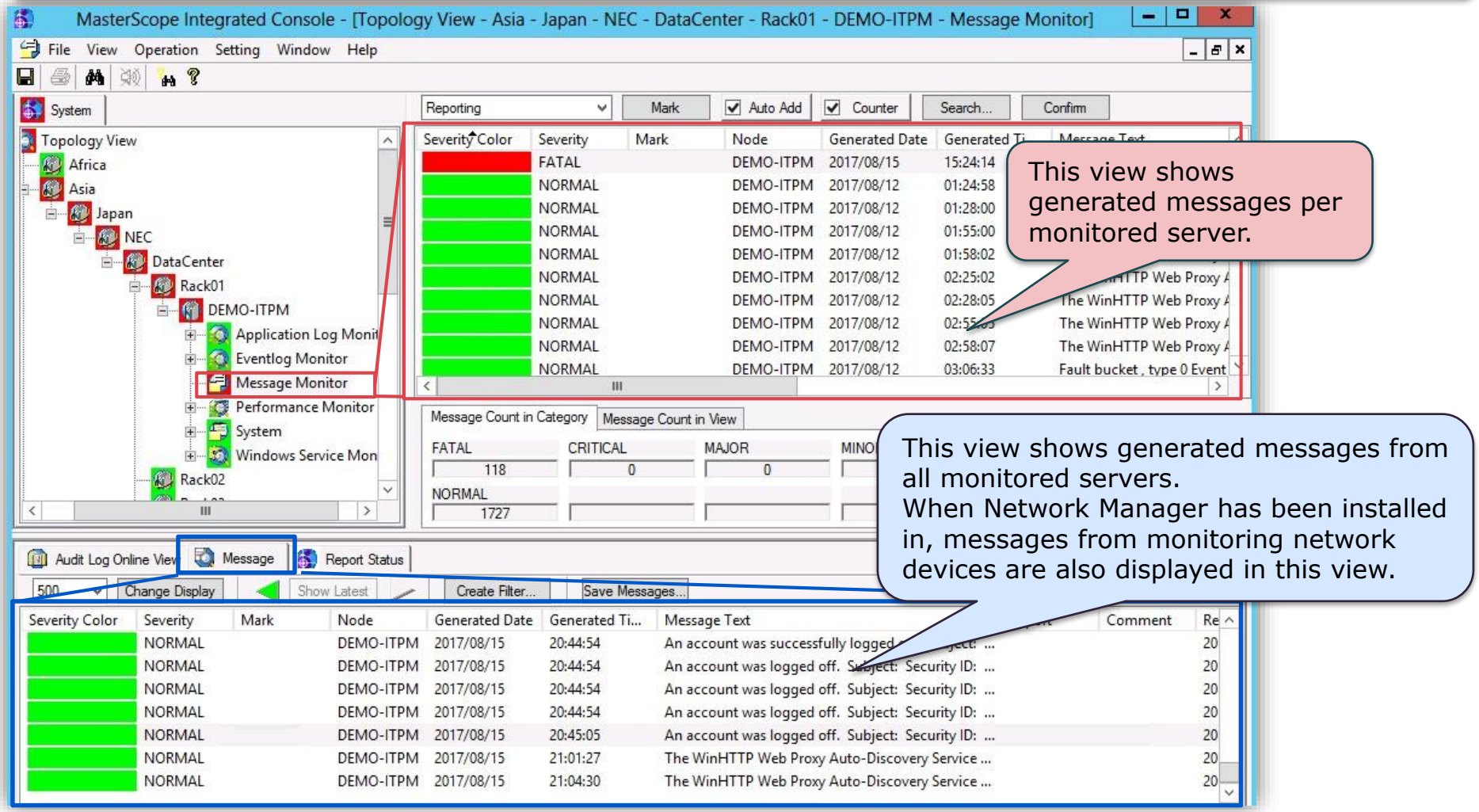


Box color changes according to the priority of the generated messages

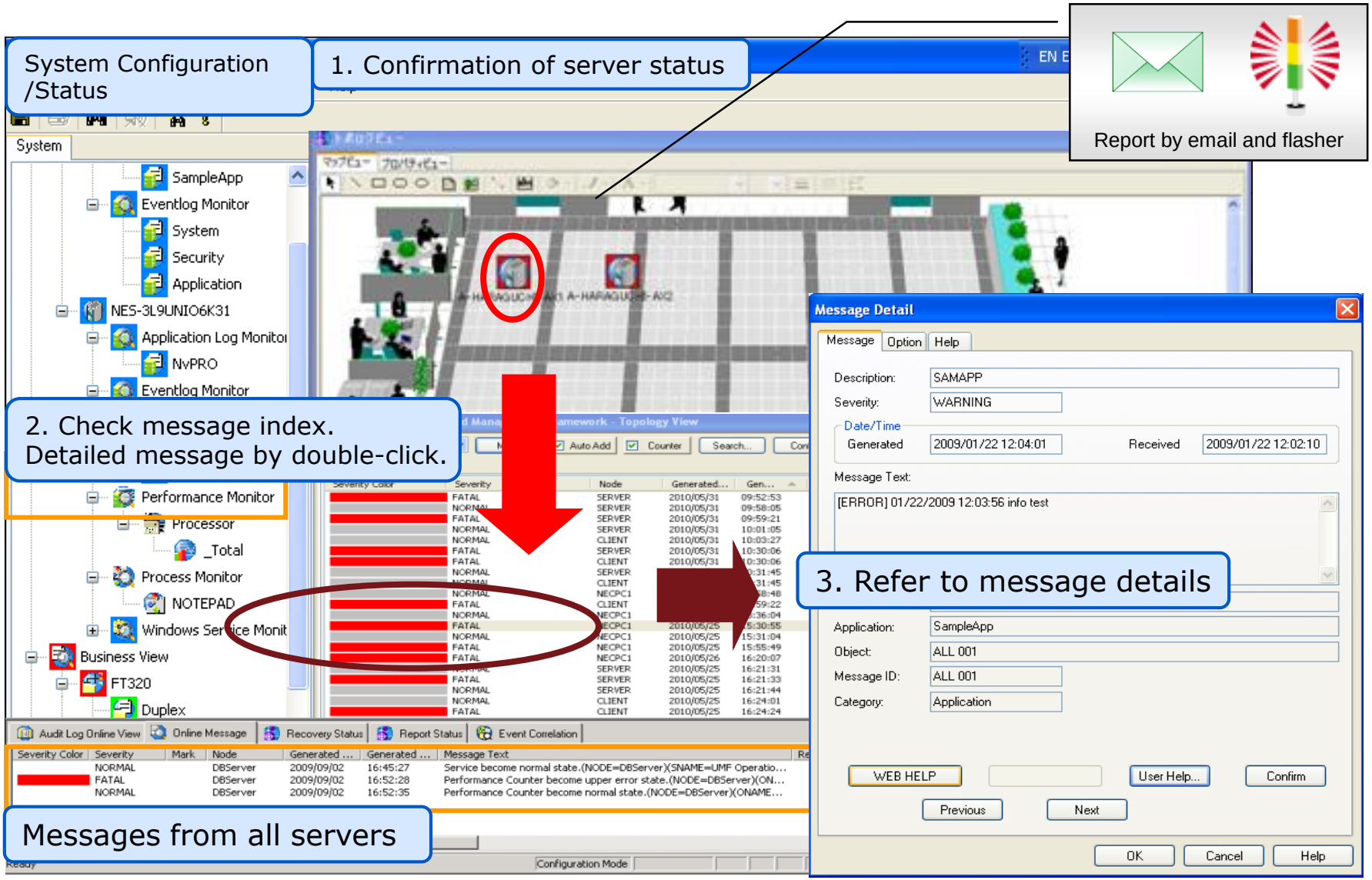
This view shows messages generated by monitoring function

Message Management（2/2）

Messages can be displayed per server or for all monitored servers in one console.

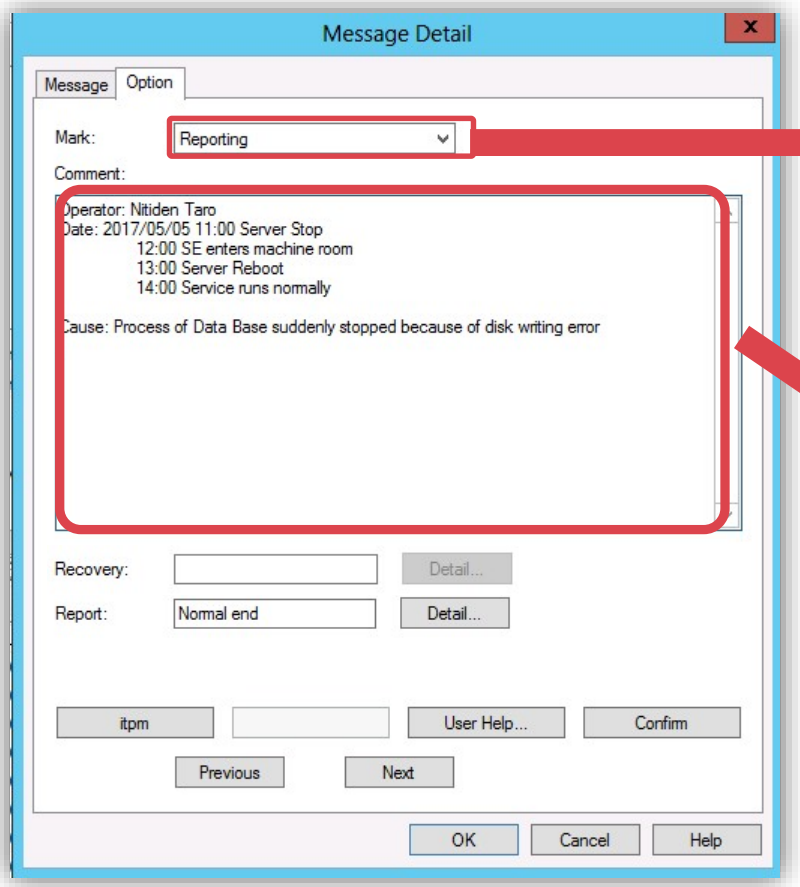


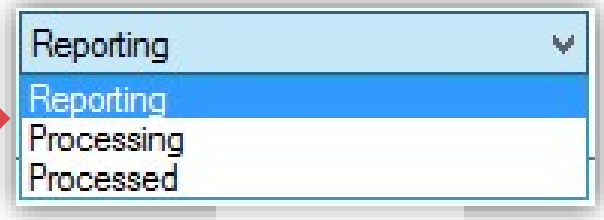
Easy Process of Identifying Failure



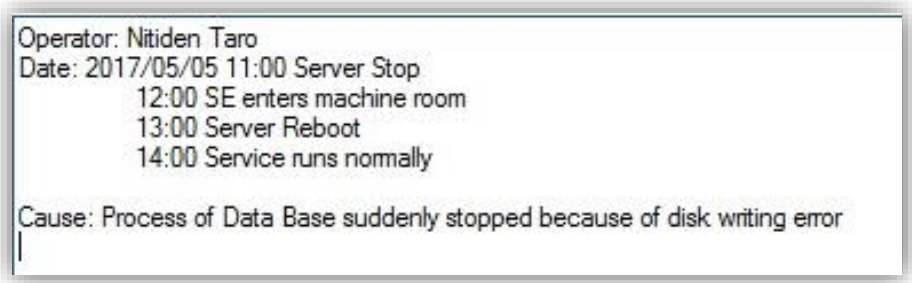
Share Recovery Status

Registering troubleshooting steps to messages enables team members to share the current working status, ensuring a smooth handover.





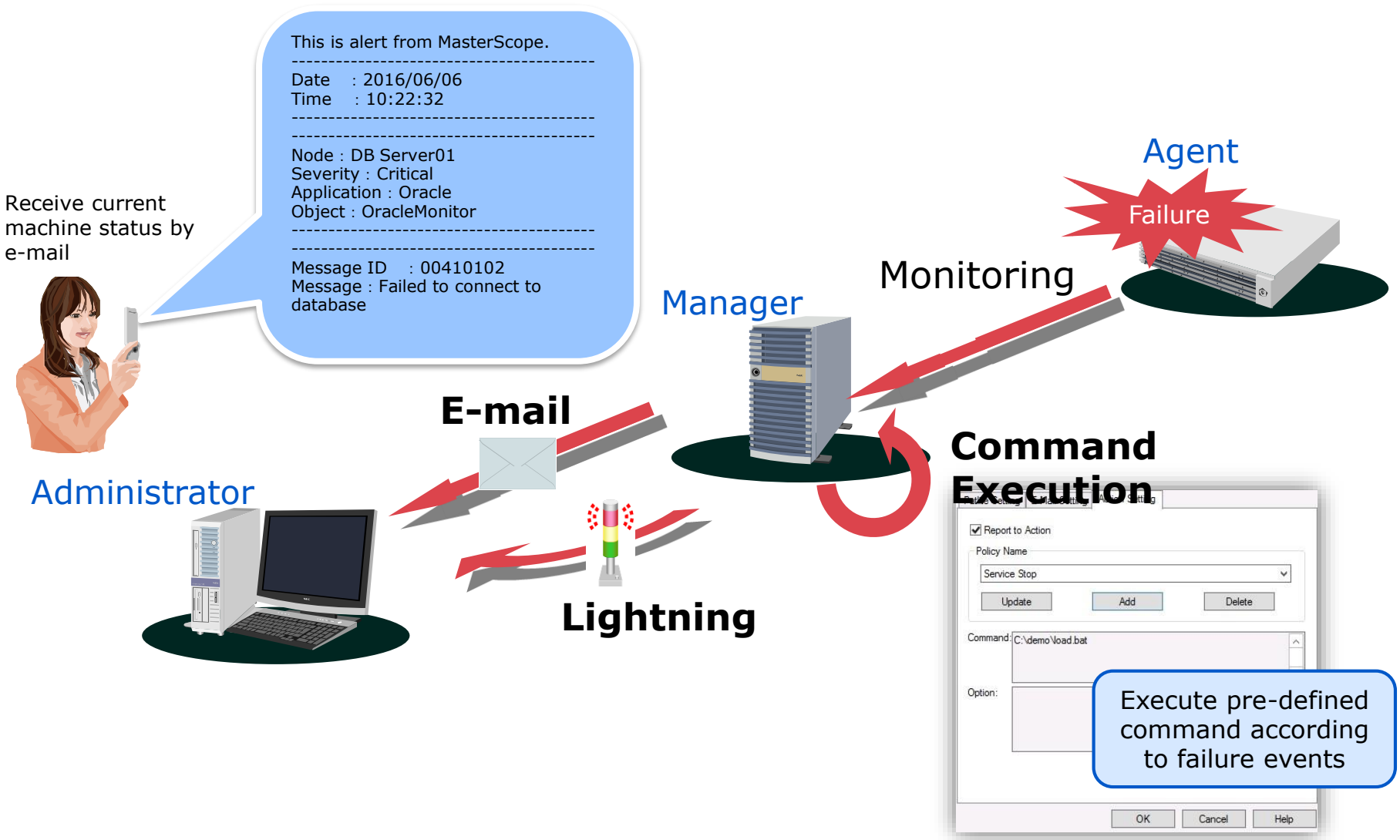
Status



Details on troubleshooting steps (Information sharing)

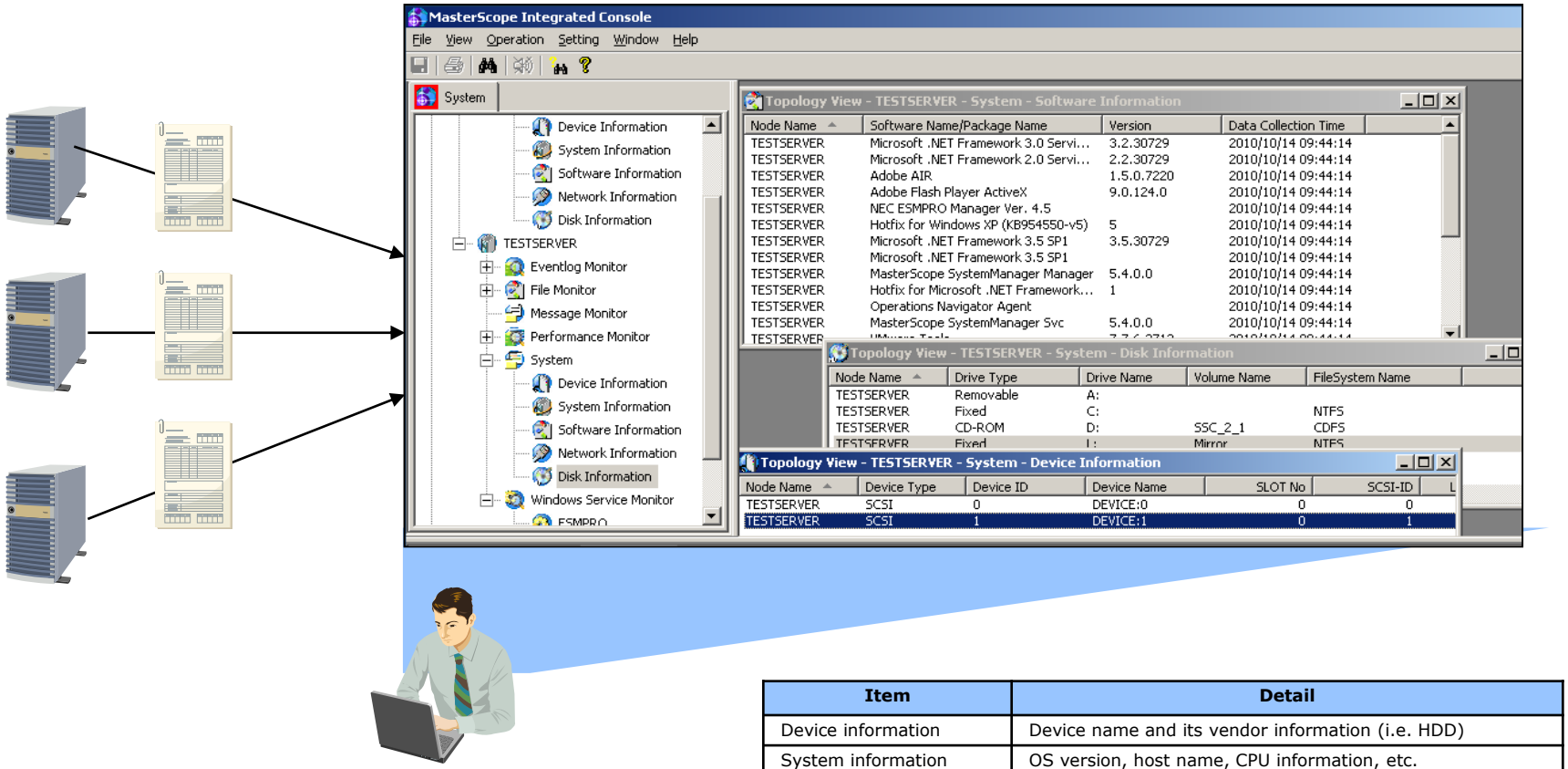
Notification Control

Automatically send e-mail and execute recovery command in case of failure.



Configuration Management

Centrally manage and view the monitored servers via console



Even if communication with agent is not available, configuration view is available.

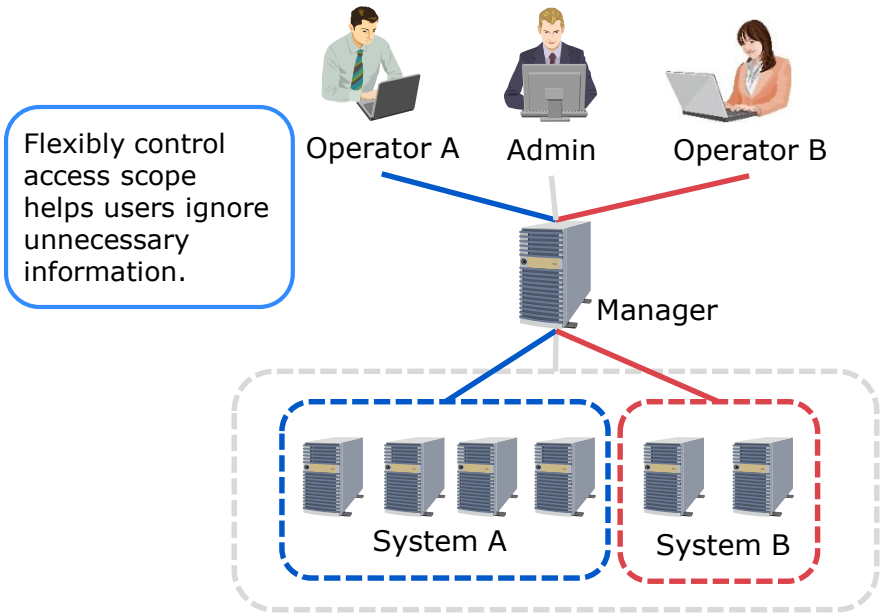
Item	Detail
Device information	Device name and its vendor information (i.e. HDD)
System information	OS version, host name, CPU information, etc.
Software information	Installed software with its version.
Network information	IP, MAC address, network identifier, etc.
Disk information	Drive name, available space, etc.

Note: acquirable information is dependent on platforms

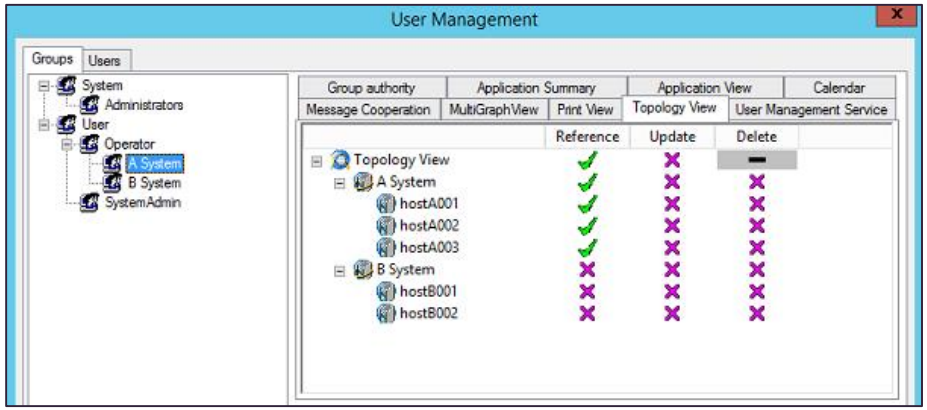
User Management

Assigns operating permission to each user to prevent operation mistakes and enhance security

■Operator can see only his own servers
■Admin can see overall system information



Set permission and add users to group.



Permission	Details
Reference	Refer to the information of the system.
Operation	Perform operations such as confirming messages and starting/stopping processes/Windows services.
Configuration	Define configuration with the configuration mode.
License	Register and manage licenses.
User Management	Create users/groups and assign permissions to them.

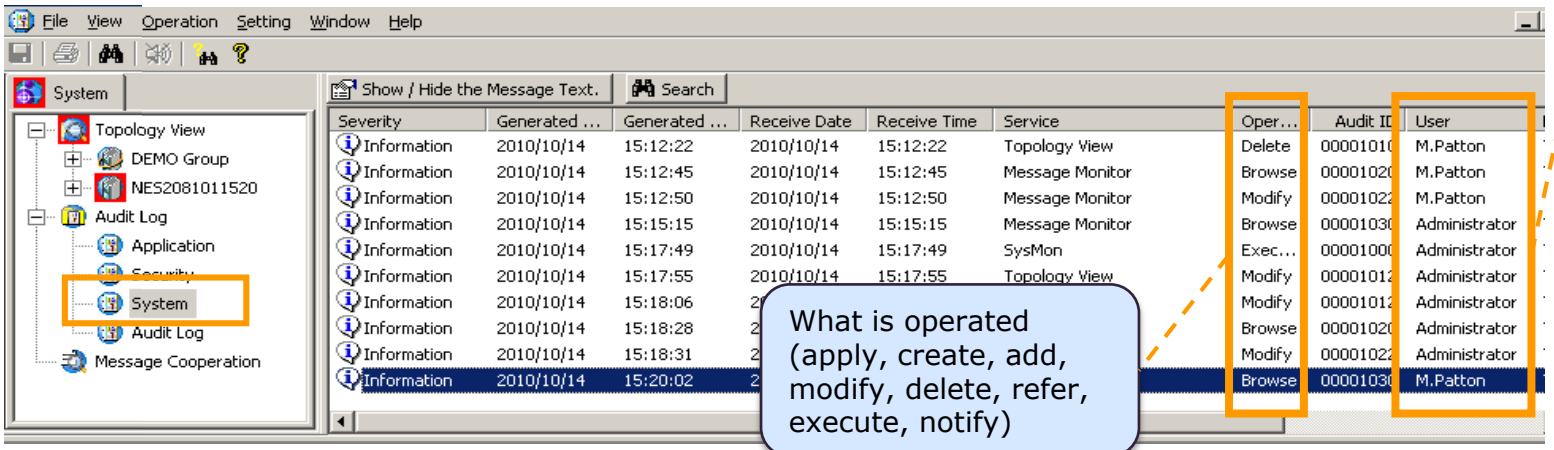
Audit Logs Management

For operations on SystemManager G, when, who, and what are recorded and admin is notified as configured.

- ✓ Operations on MasterScope SystemManager G (including monitored nodes, manager's GUI, automatic operations) are recordable as audit logs for future tracing.
- ✓ These logs can be displayed by categories and notification settings can be specified for categories.

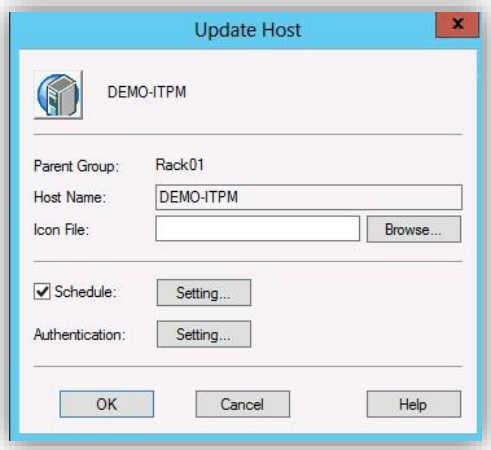
Tree view for audit logs mgmt

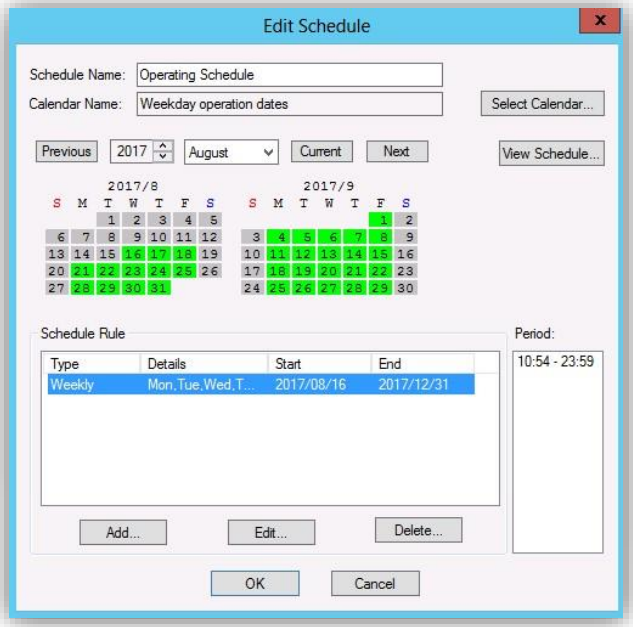
Category	Log details
Application	Record logs generated by applications
Security	Record audit logs from user management
System	Record audit logs from SystemManager G
Audit logs	Record audit logs from this function itself

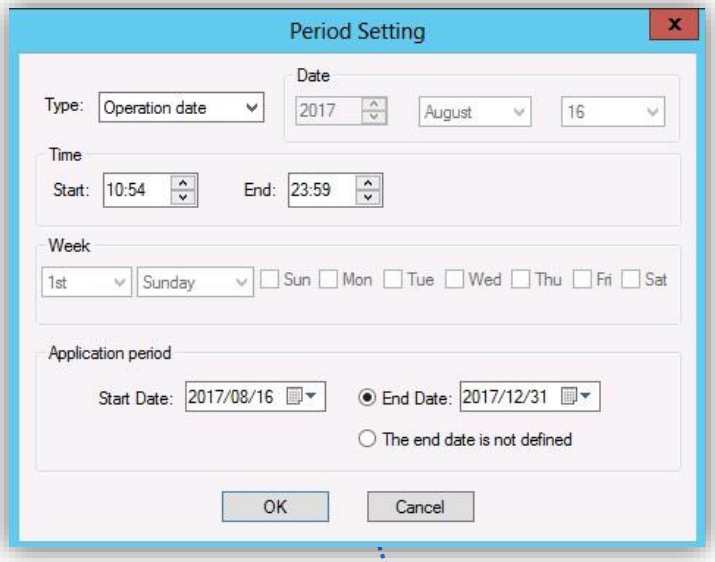


Schedule Control

SystemManager G can start and stop monitoring according to pre-defined schedule.



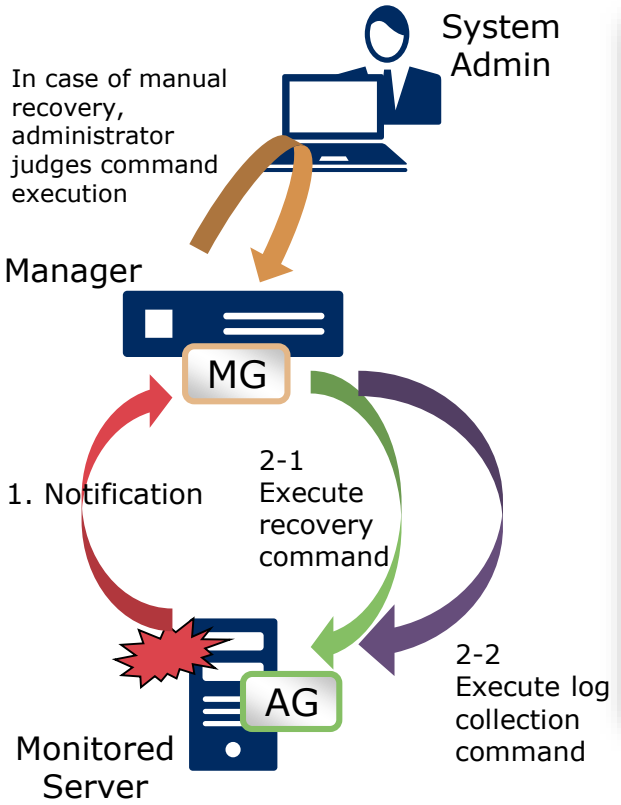


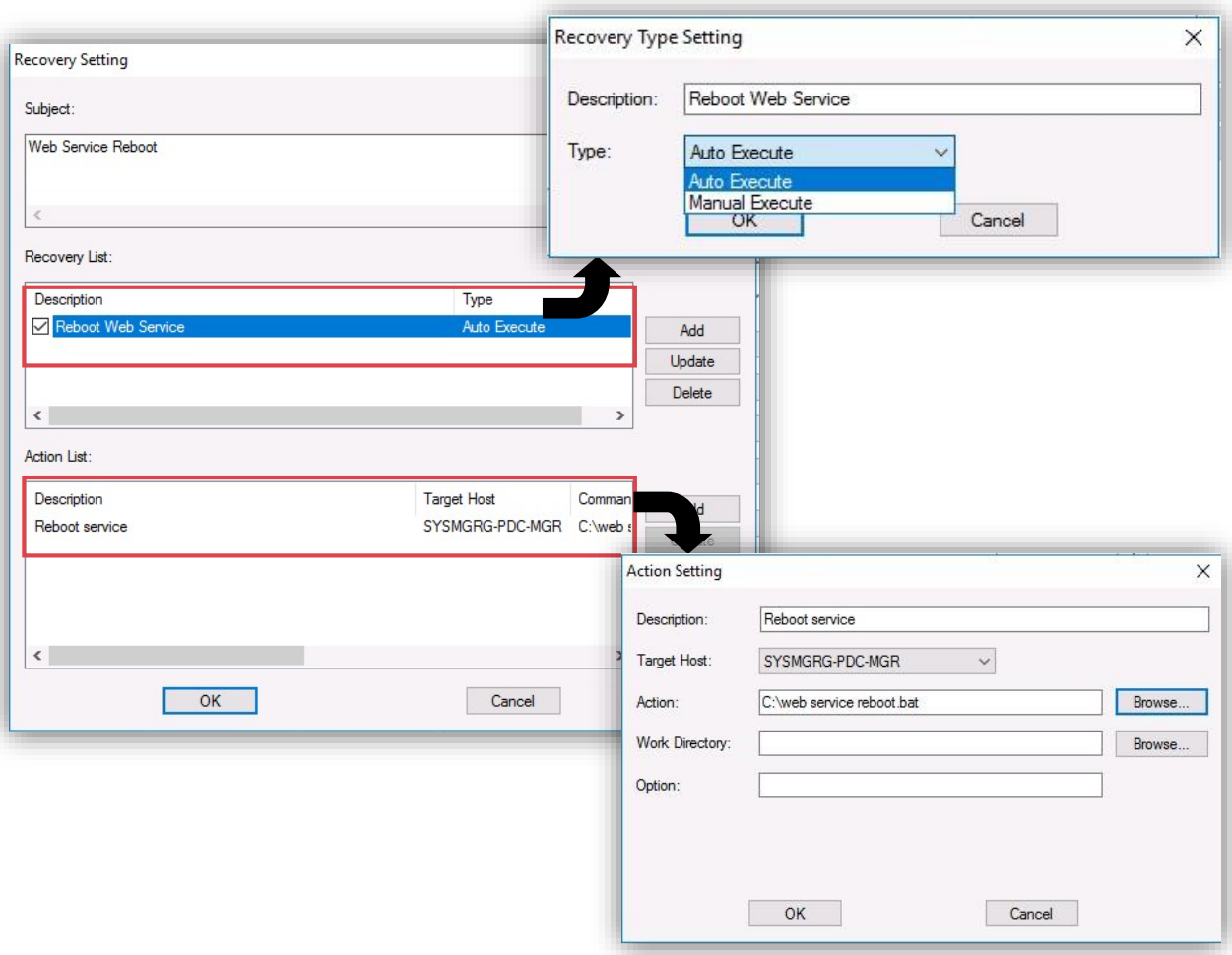


It allows you to set monitoring schedule per server

Command Execution on Monitoring Server

SystemManager G can execute commands i.e. recovery job and log collect job on monitoring server by manual or automatic.





Automatic Setup of SystemManager G Agent

NEC Provides "Role" of Ansible which automates the procedure to install and setup an agent, reducing setup time, human error, and SI costs.

Before

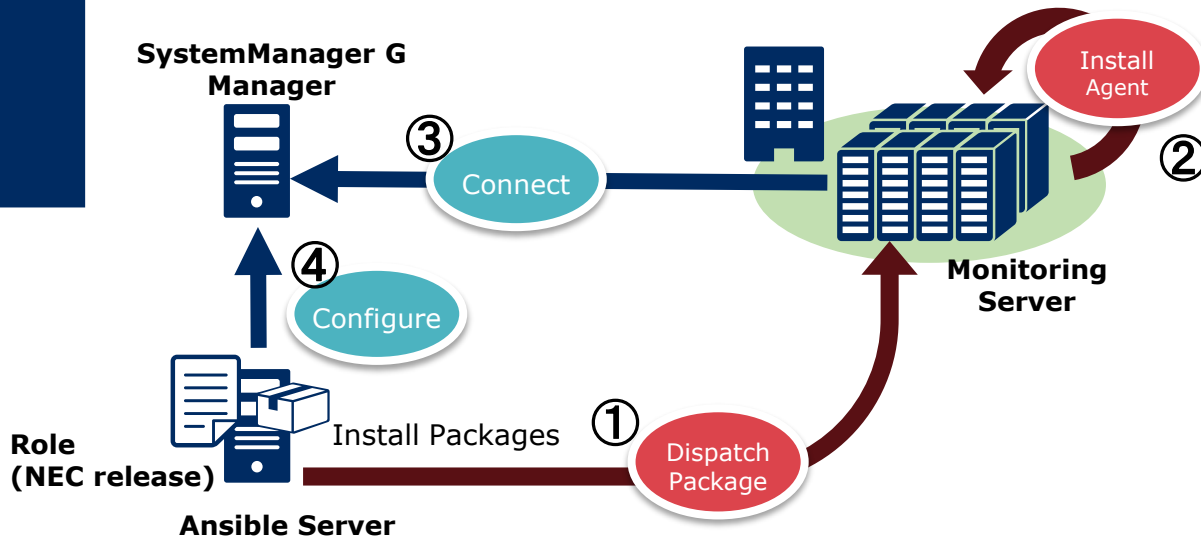
- Need to install an agent on each server. Currently engineers are manually setting parameters via install wizard (GUI).

Manual installation of agents on many servers may
- require so much time and workload
- cause human errors such as mistyping parameters

After

Agent installation is completed just by running playbook from Ansible server.

Automated installation -> Low cost
Automated setting -> No human errors

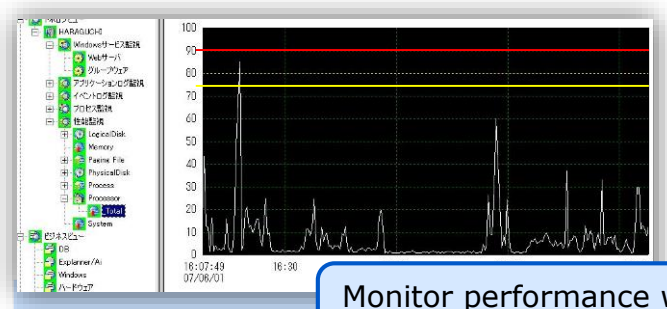


Application Monitoring

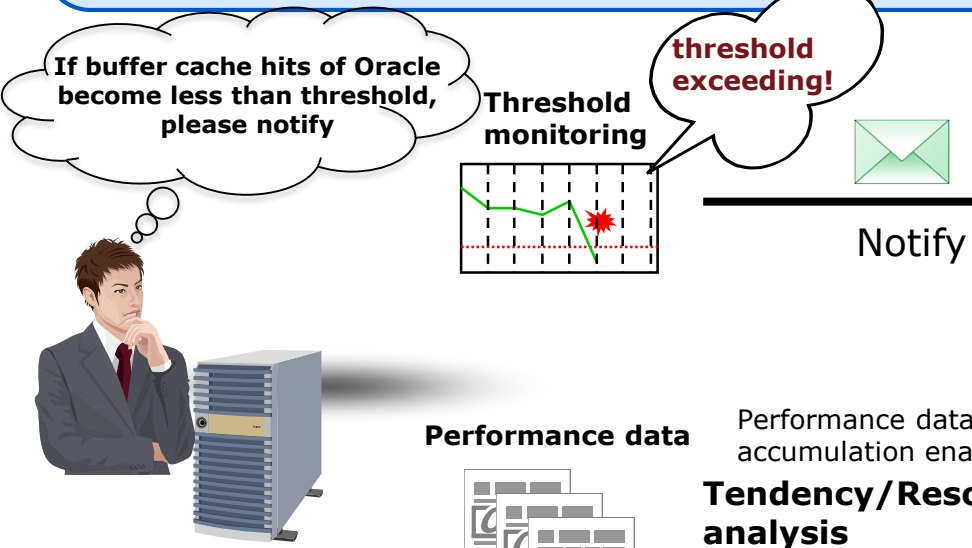
Option
Oracle Monitoring etc.

Monitor application performance by simply setting thresholds for warning and anomaly.

Available threshold setting can be selected from the following patterns:
Sequential: an event occurs when a collected value exceeds threshold
Continuous: an event occurs when a collected value exceeds threshold consecutively for the specified number of times
Average: an event occurs when the average collected values of the specified number of times exceeds threshold.

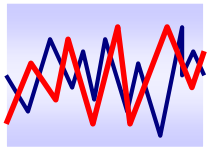


Monitor performance with two level threshold settings



Performance data

Performance data accumulation enables
Tendency/Resource analysis



Performance data accumulation could be utilized in operations status/failure analysis

Performance data accumulation can be enabled simply by checking settings boxes

Support Application Lists

The following table provides support platform information.

Middleware		Support version
Data Base	Oracle Database	・Oracle 11gR2, 12cR1, 12cR2
	SQL Server	・SQL Server 2008 SP4, 2008R2 SP3, 2012 SP3, 2014 SP1/SP2, 2016(SP1), 2017
Web/AP Server	IIS	・IIS 7.0, 7.5, 8.0, 8.5, 10.0
	WebLogic Server	・WebLogic Server 11gR1, 12cR1, 12cR2
	WebSphere Application Server	・WebSphere Application Server 7.0, 8.0, 8.5
	Apache HTTP Server	・Apache 2.2, 2.4
	Apache Tomcat	・Tomcat 6.0, 7.0, 8.0, 8.5
Others	SAP	・SAP ERP 6.0 ・SAP NetWeaver 7.0, 7.3
	Java application	・Running applications on Java 6, 7, 8, 9

Application Monitoring Template

Option
Oracle Monitoring etc.

Addition/change of monitoring items can be implemented easily.

・It looks too difficult to set monitoring items to all target servers.
・Only experts know what monitoring items are necessary to our system

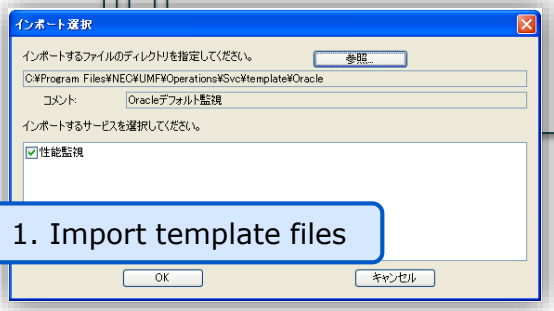
Extensive monitoring items
Monitoring items are available as template

Easy settings of monitoring items
Detailed settings are in dialogue form and can be set easily

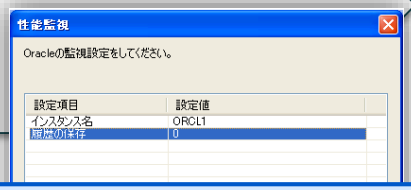
Customization
Monitoring items can be added/modified easily

High Operability
Operation is possible right after implementation

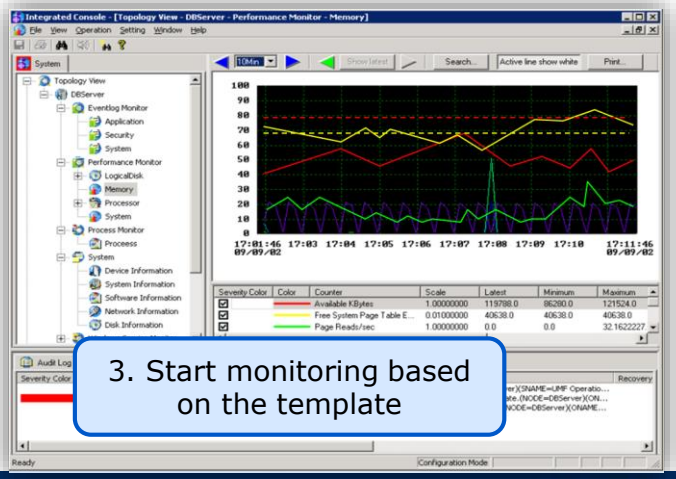
3 Steps to start monitoring after installation.
Easy customize of monitoring items by GUI.



1. Import template files



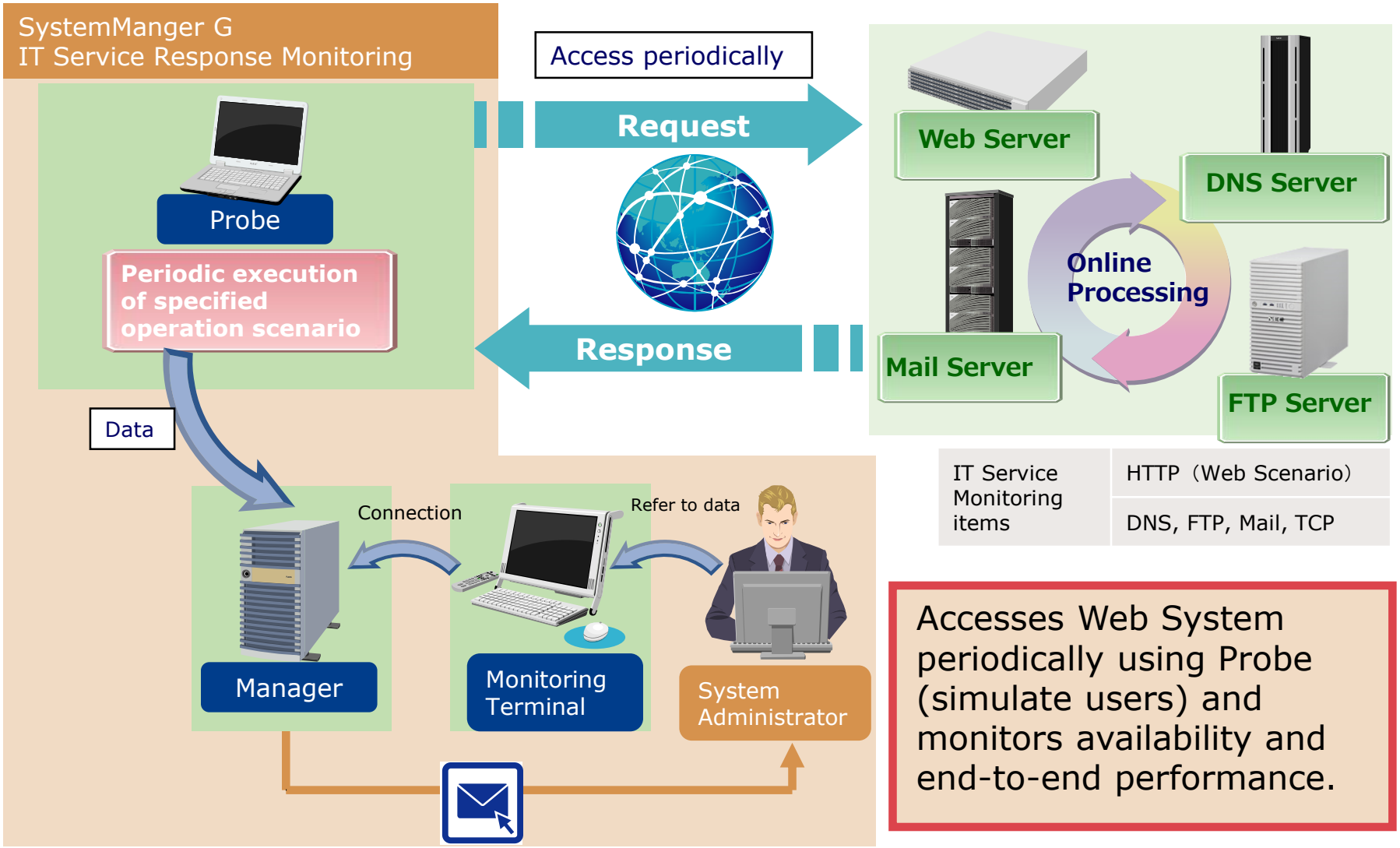
2. Select an application instance name and check whether to store history log or not.



3. Start monitoring based on the template

IT Service Response Monitoring

Option
IT Service Response Monitor



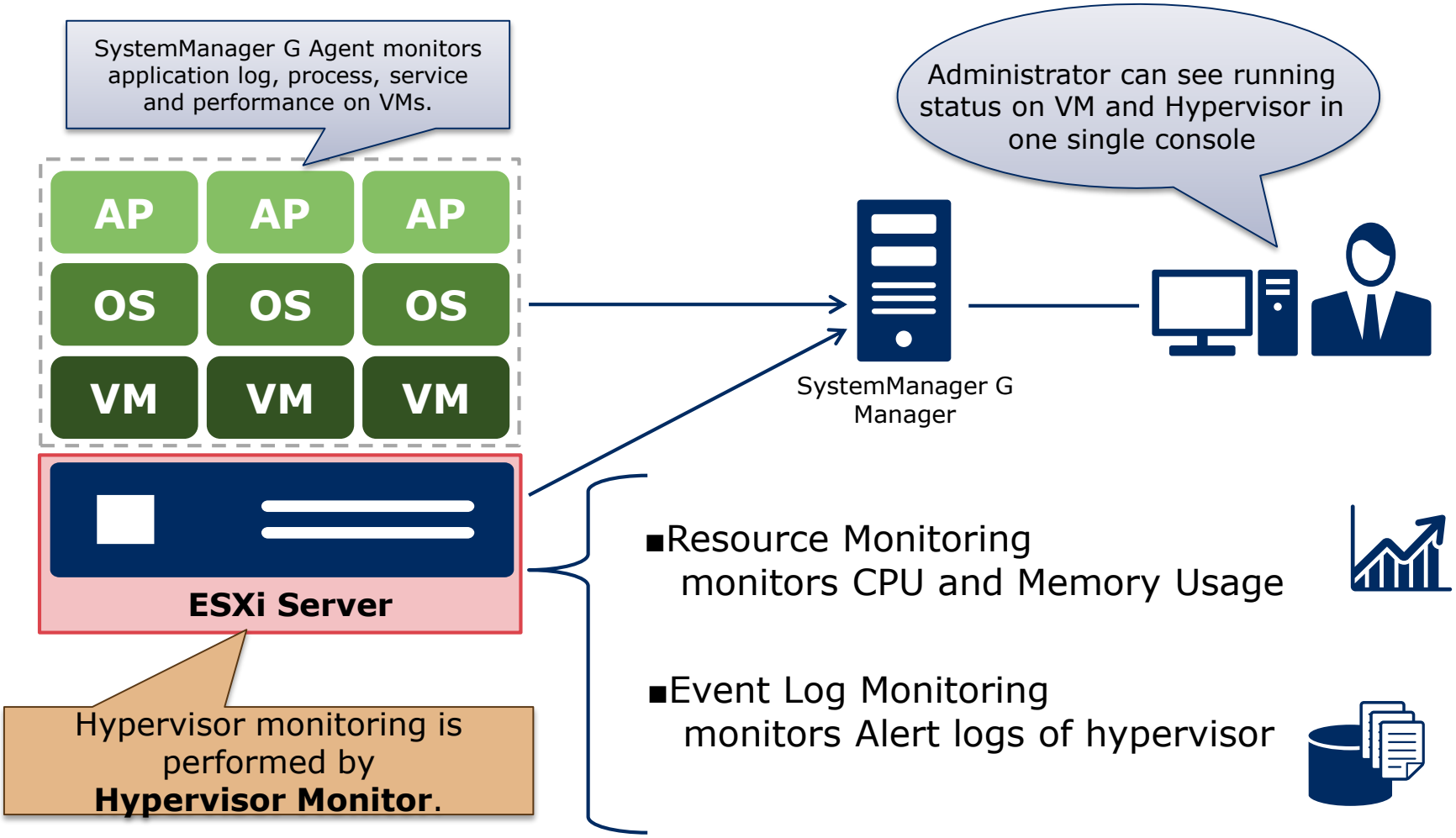
IT Service Monitoring items	HTTP（Web Scenario）
	DNS, FTP, Mail, TCP

Accesses Web System periodically using Probe (simulate users) and monitors availability and end-to-end performance.

Note: Scenario is a record of executed operation in the browser. It is used to access IT server for monitoring.

Hypervisor Monitor

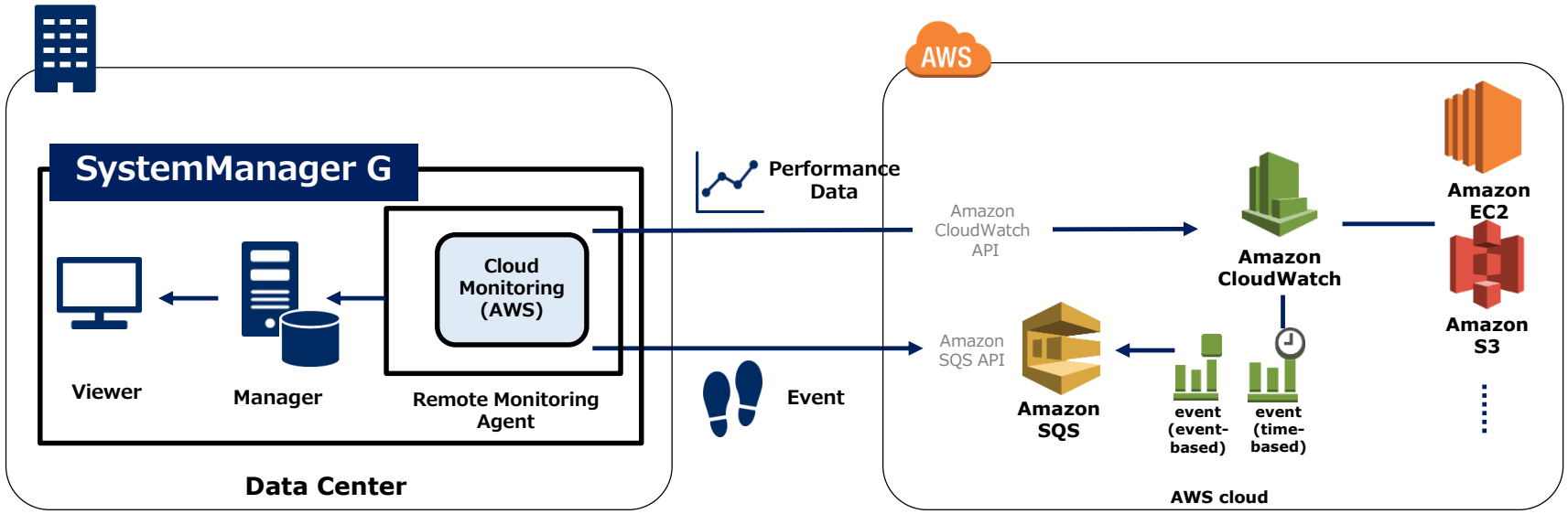
Hypervisor Monitor option enables integrated monitoring of Hypervisor and VMs.



Cloud Monitor

Cloud Monitoring option enables integrated monitoring of on-premise and Amazon Web Services.

- Cloud Monitoring monitors performance data and events in AWS through Amazon CloudWatch API.
  - Operation and performance monitoring
  - Resource status event monitoring

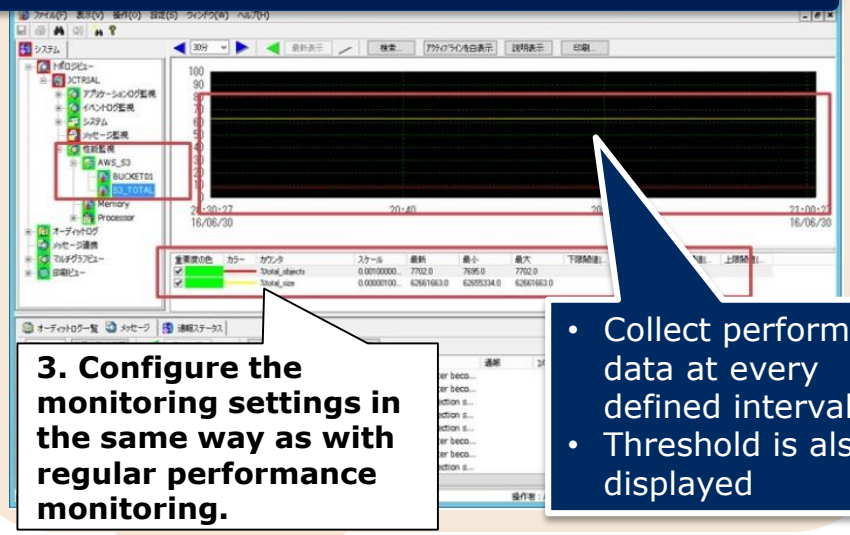


Customizable Performance Monitoring

Option
Customizable Performance Monitoring

The numerical data results of arbitrary command and program are stored in database as performance data. The data is used for threshold monitoring, performance chart, and report.

Display custom monitoring items



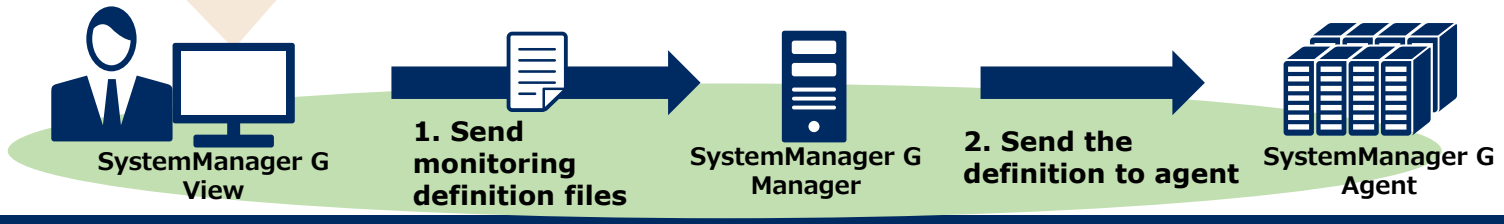
3. Configure the monitoring settings in the same way as with regular performance monitoring.

- Collect performance data at every defined interval
- Threshold is also displayed

Use Case

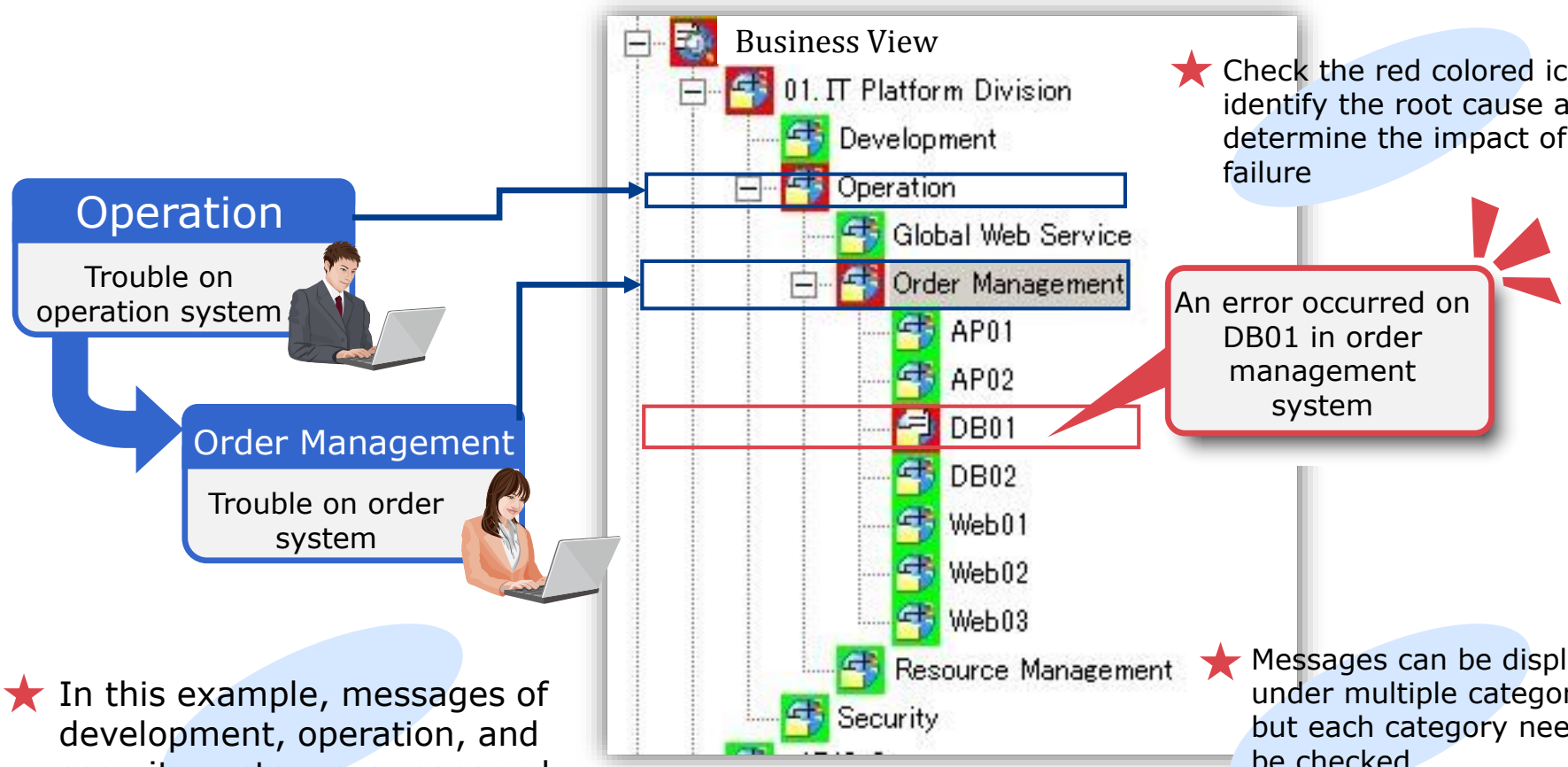
Users want to integrate new system and existing system, but existing system collects performance data using user defined program.
⇒ Utilize the existing program and realize integrated monitoring

There are programs to output data of user access and users want to show the data on chart and report.
⇒Customizable performance monitoring realizes this request by monitoring data of user access



Message Management（from the view point of business）

Not only are online messages displayed, Business View also allows you to categorize messages and change message levels for easy management.



★ Check the red colored icons to identify the root cause and determine the impact of the failure

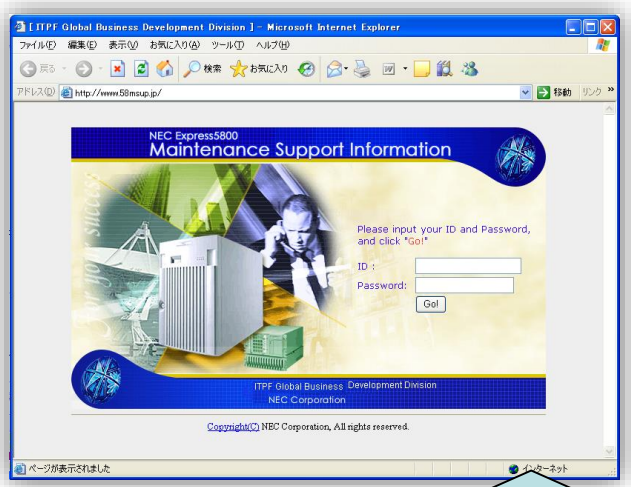
★ In this example, messages of development, operation, and security system are managed.

★ Messages can be displayed under multiple categories, but each category needs to be checked.

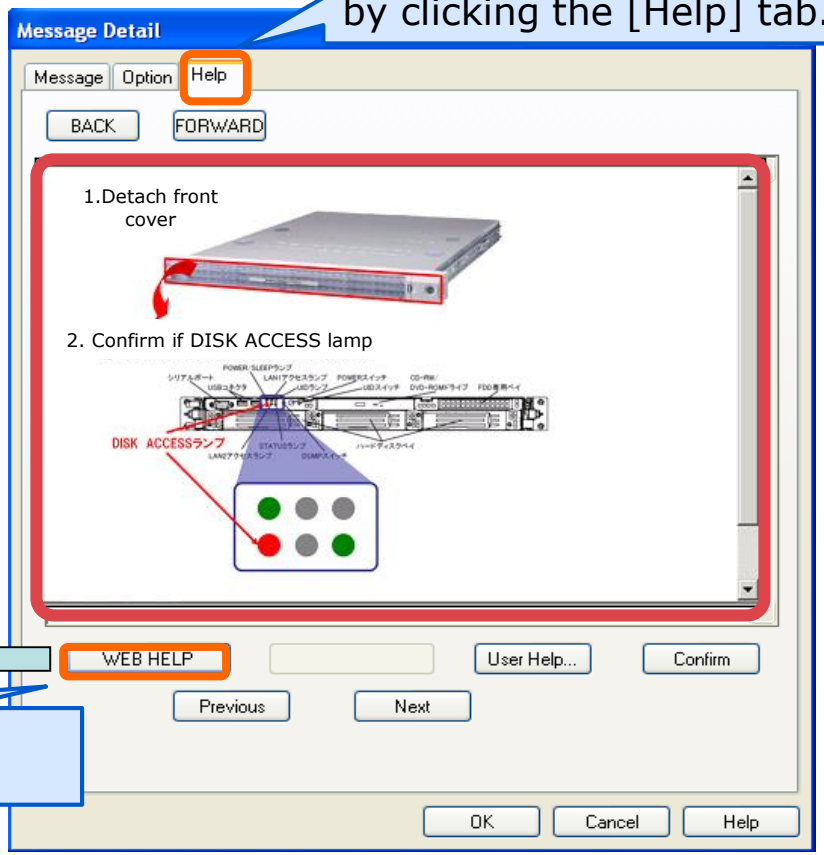
Knowledge Management (Share Operation Know-How)

Option
BusinessView

Knowledge function enables to share daily operation as know-how, standardize the skill and speedy action, and reduce operational cost.



Knowledge can be displayed only by clicking the [Help] tab.



Linked application or file can be activated from the button on message detail.

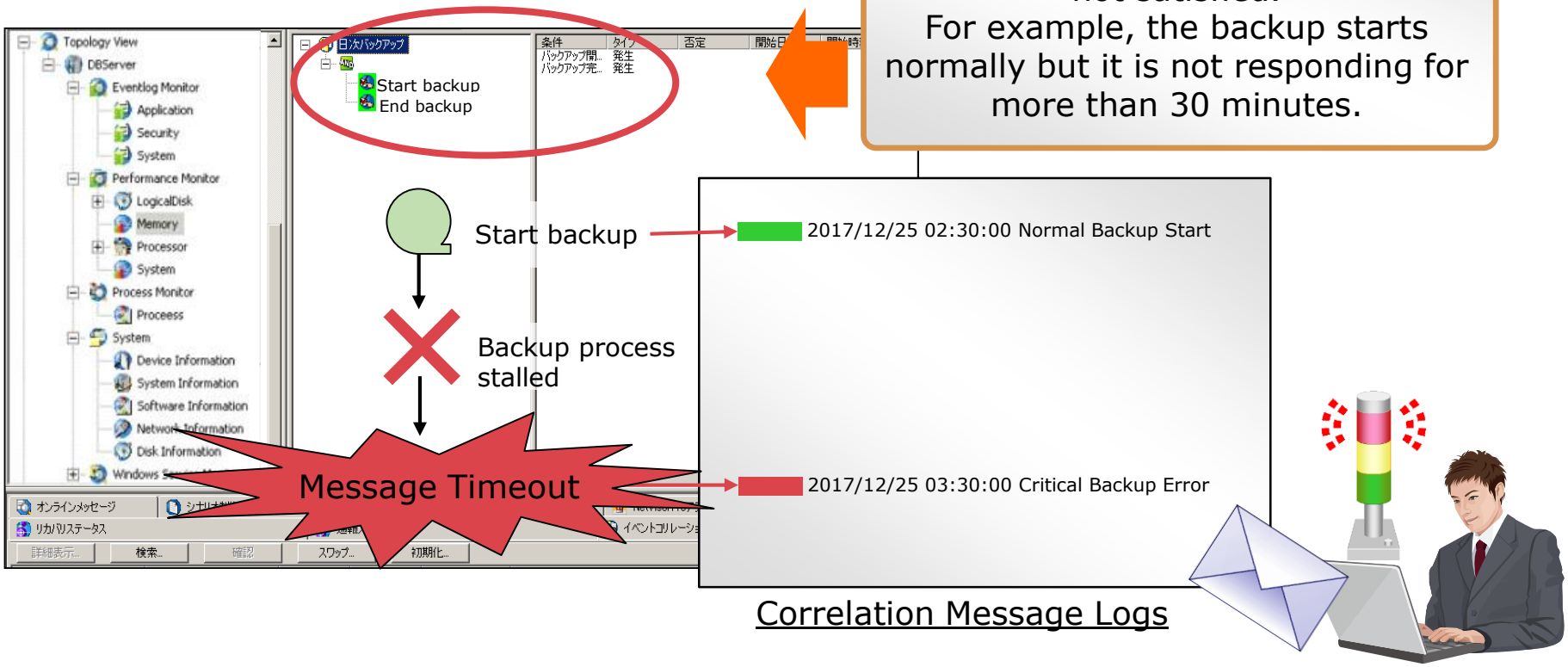
Analyze Event Correlation Messages

Option
EventCorrelation

Correlation monitoring of multiple events enables to detect failures which cannot be discovered by monitoring single event.

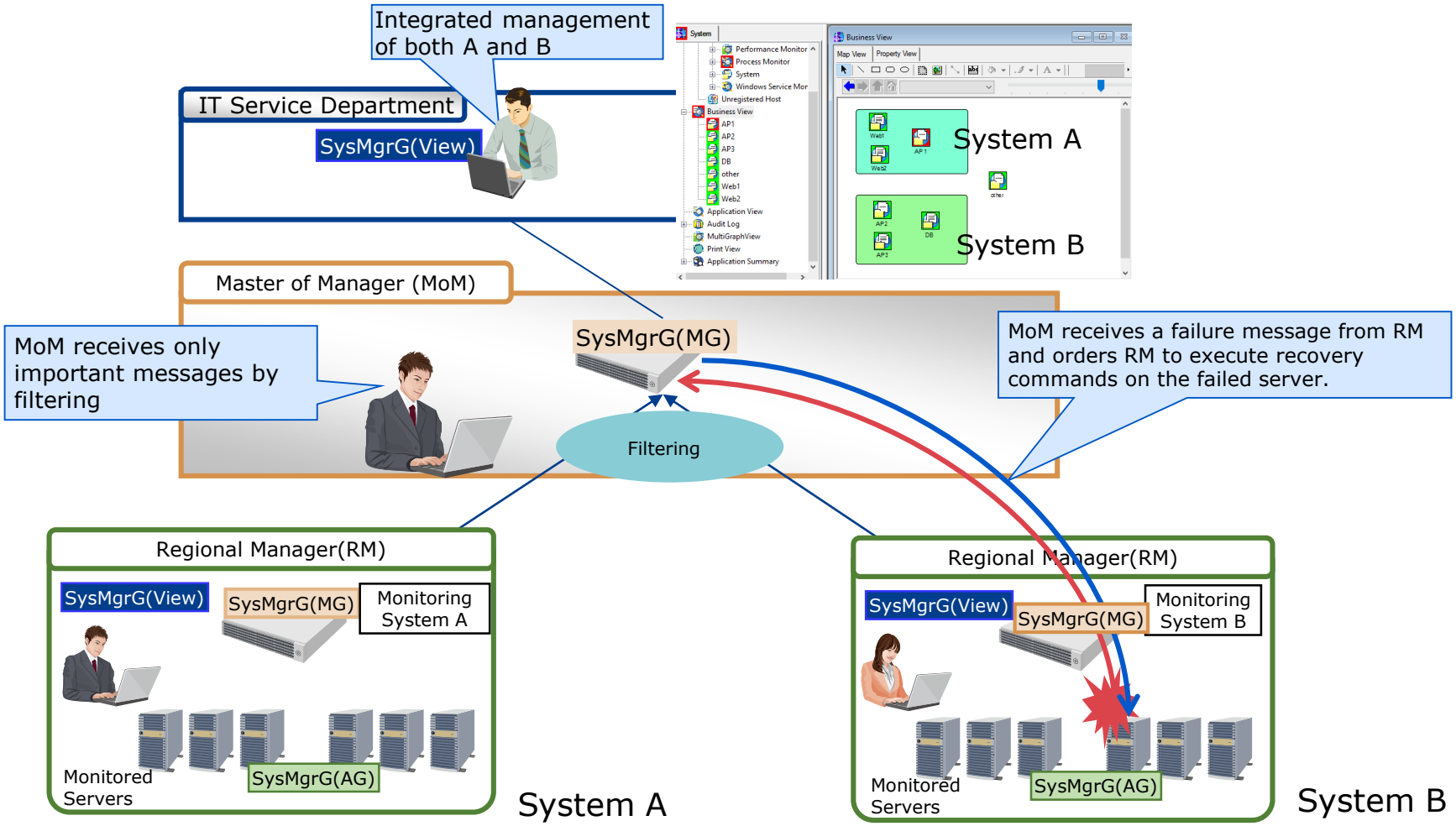
Monitoring only normal messages cannot detect abnormal status.

SystemManager G sends alert messages if correlated filter rule is not satisfied.
For example, the backup starts normally but it is not responding for more than 30 minutes.



Hierarchical Manager

Hierarchical architecture redistributes workload to available resources and enables system administrator to monitor all systems in one console.

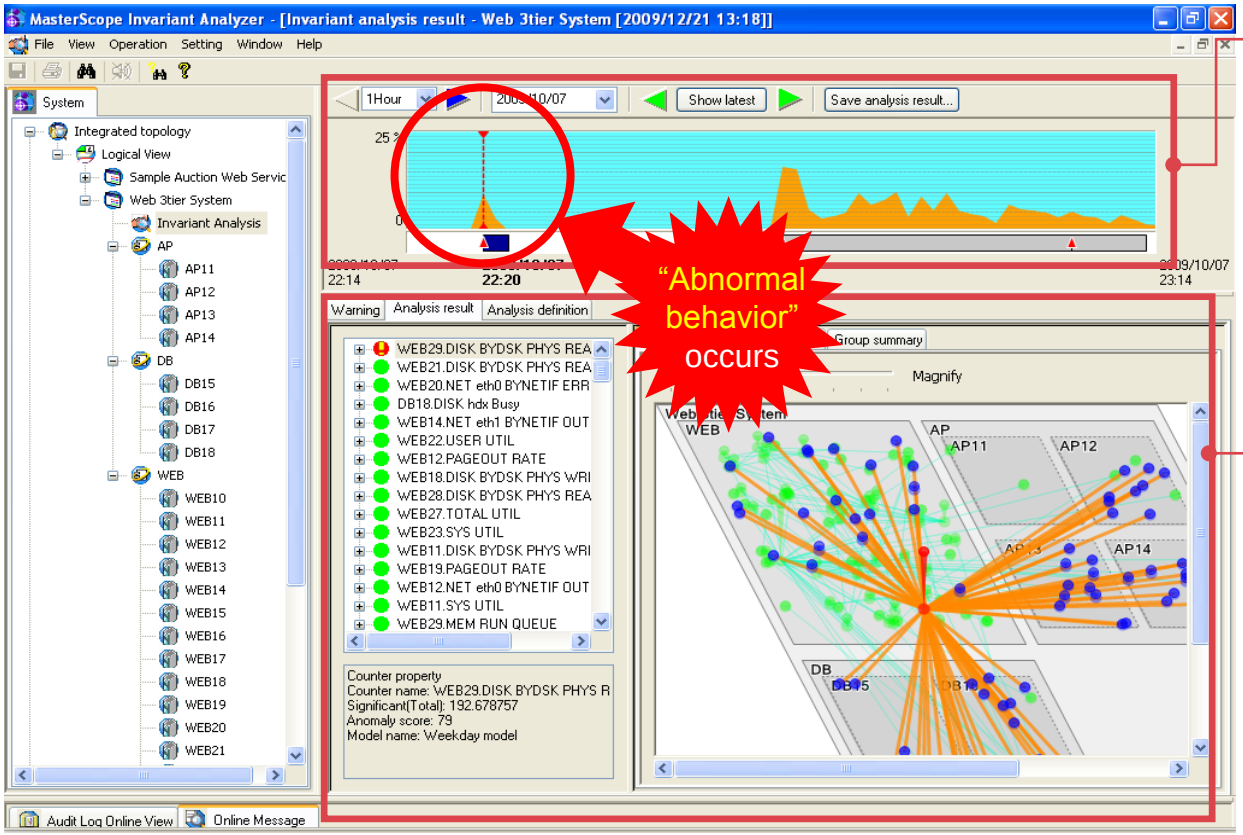


System Performance Analysis

Option
Invariant Analyzer

Graphs indicate the time of occurrence and severity of failures. Map view shows specific component primarily causing "abnormal behavior" and its impact.

- ✓ Extract and visualize specific component primarily causing the "**abnormal behavior**" by automatic analysis.
- ✓ The impact of abnormal behavior can also be observed at a glance.



Visualize "abnormal behaviors"

Shows the time of occurrence and the severity of the abnormal behavior using an intuitive graph.

Visualize by map views

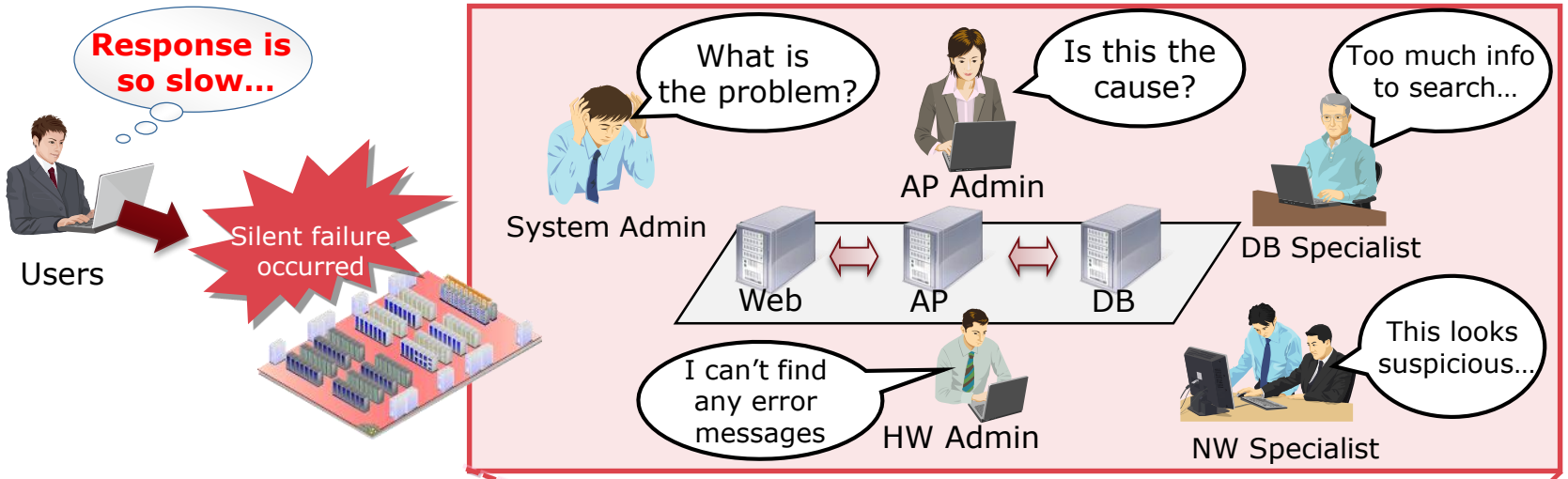
The red point indicates the component primarily causing the "abnormal behavior" and its severity.
The blue points indicate all the components affected by the root cause.

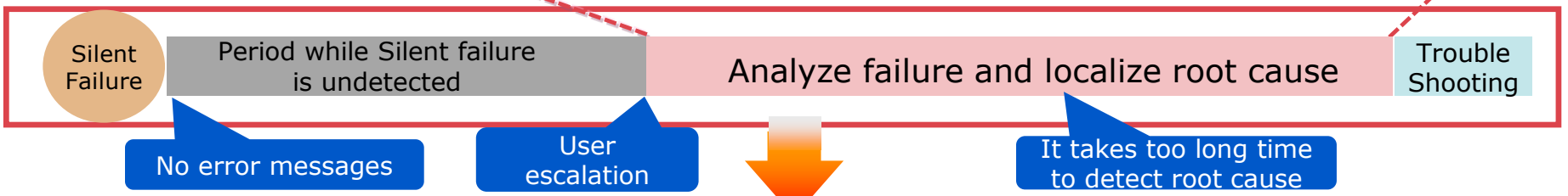
Silent Failure Detection

Option
Invariant Analyzer

For failures without error messages, various system components need to be checked by specialists with specific skills and experience.

- ✓ Silent failure occurs often in complex large-scale IT systems and it is difficult to resolve the failure.
- ✓ Silent failure may generate performance degradation caused by undetectable bottlenecks.





MasterScope SystemManager G Invariant Analyzer Option can resolve it

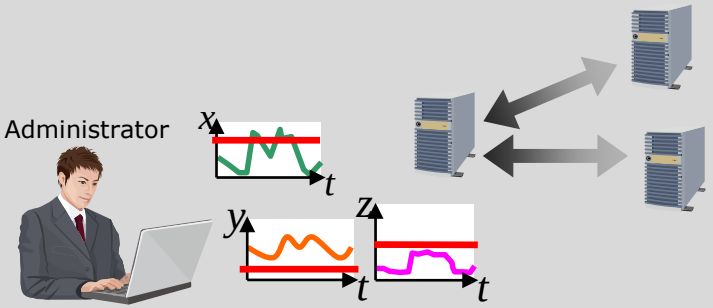
Difference between SystemManager G and other performance monitoring tools

Option
Invariant Analyzer

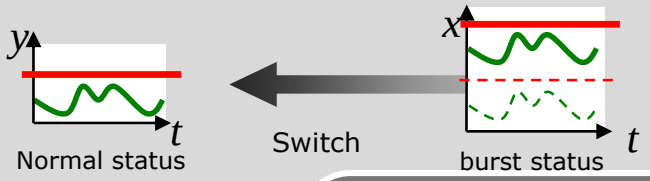
Complex configurations are not required. You Just need to input performance data. It is unnecessary to set up thresholds since it focuses only on invariant relationships among performance data.

Traditional Monitoring tool

Analyzing numerous data points is not simple and easy.



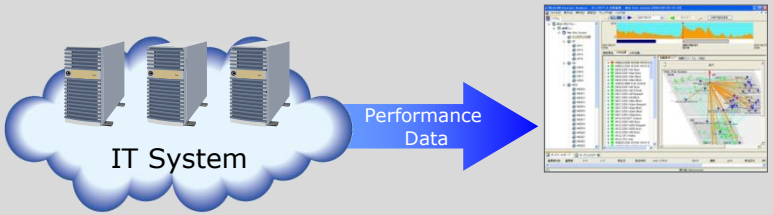
Frequent review of the thresholds is required due to business condition changes.



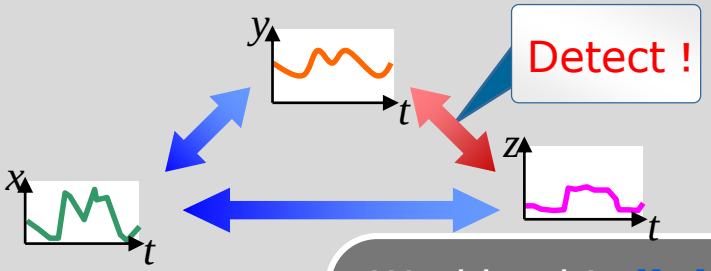
Workload is **heavy**

SystemManager G

Just input performance data.
Easy analysis without specialized expertise



No need to adjust the configuration from time to time due to business conditions.

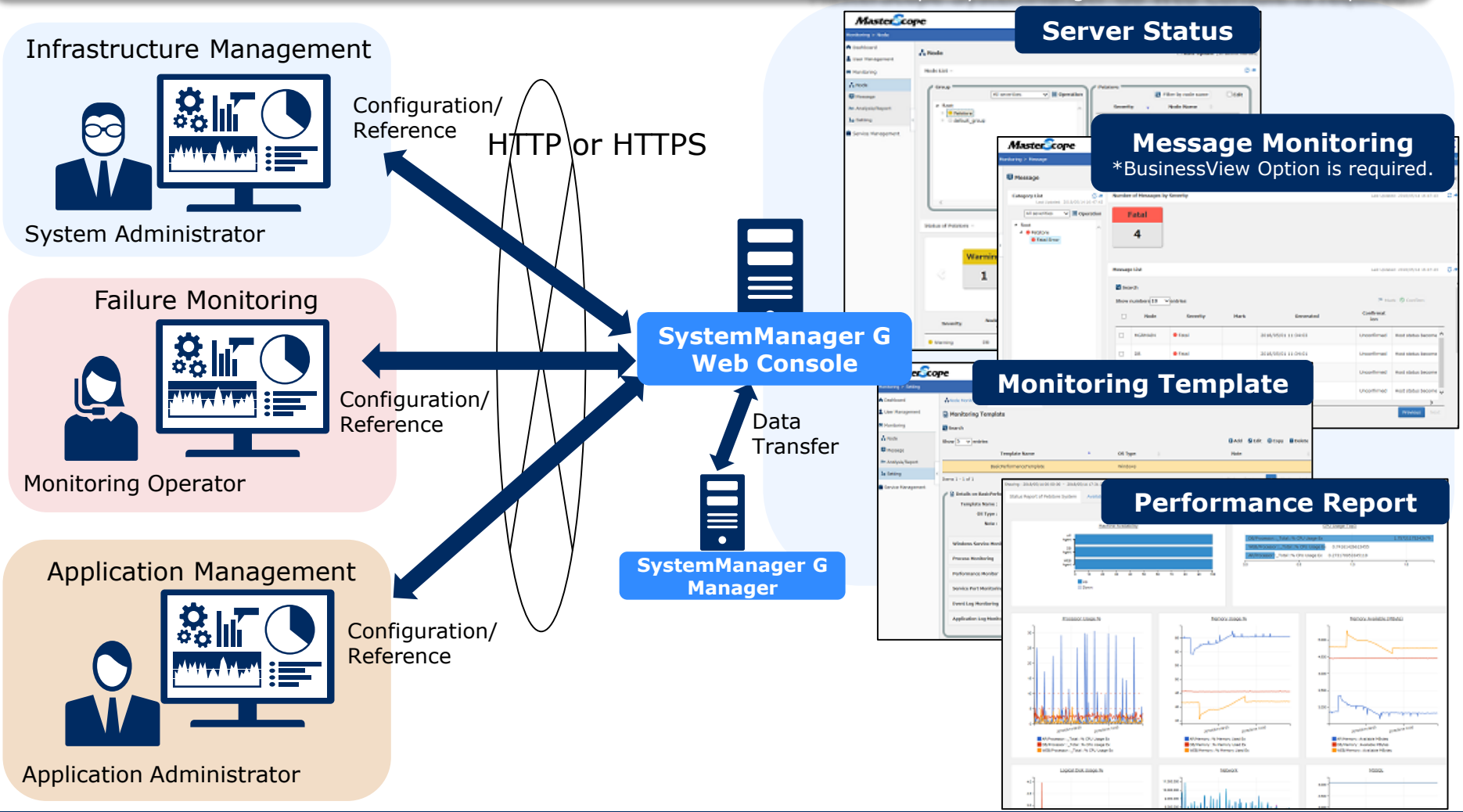


Workload is **light**

Web Console

Web browser console allows you to monitor systems from terminals without View installed.

*MasterScope SystemManger G8 Web Console is required.

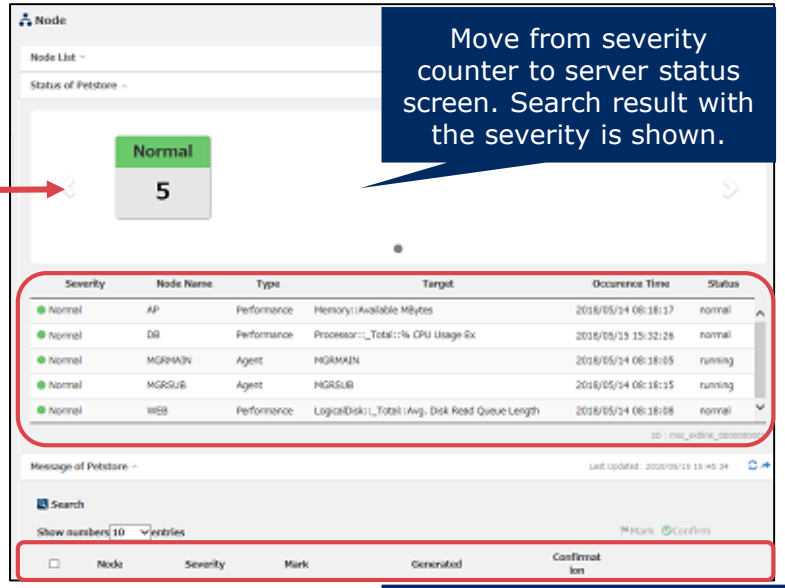


Monitoring Dashboard (Web Console)

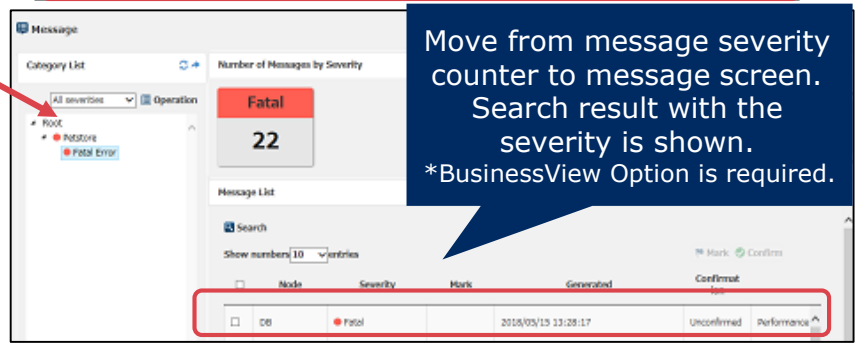
Option
Web Console

You can create and customize your dashboard with widgets to get a quick view of the system status as soon as you login.

Widgets can be freely added and adjustable on a personal dashboard for each user.



Move from severity counter to server status screen. Search result with the severity is shown.

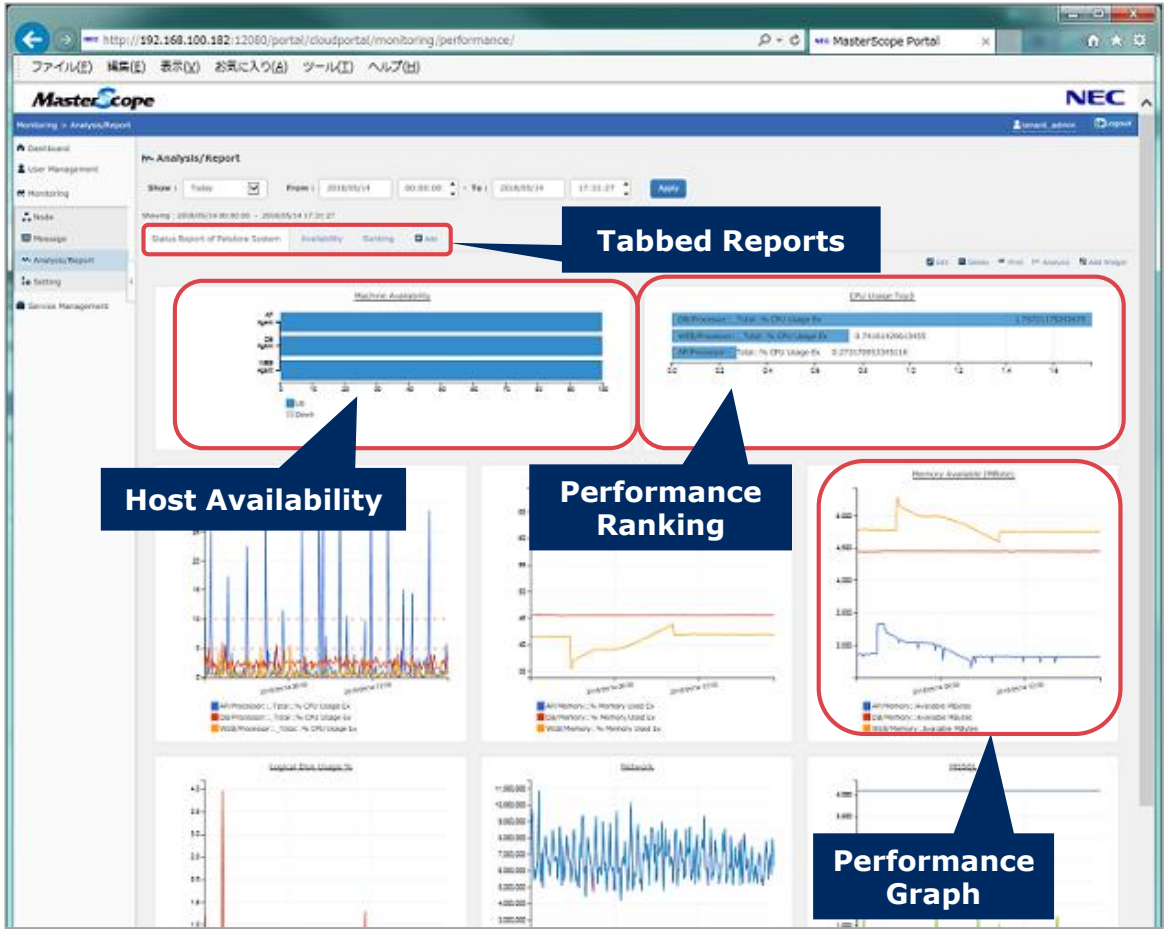


Move from message severity counter to message screen. Search result with the severity is shown.
*BusinessView Option is required.

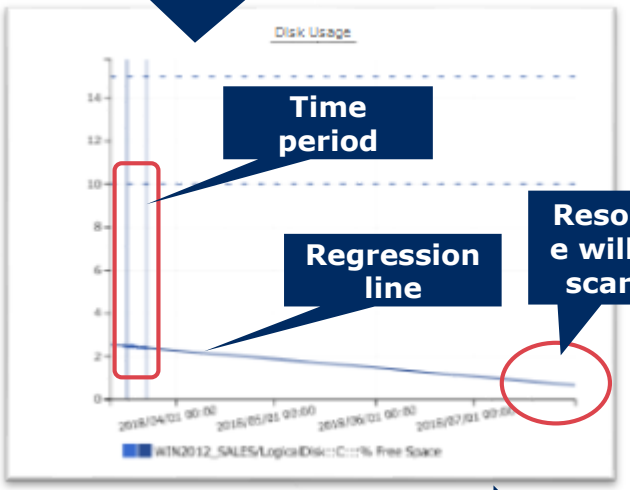
Performance Report (Web Console)

Option
Web Console

Performance reports are displayed using tabs. Host availability, ranking, and capacity management by regression lines are newly added features.



Drawing a regression line based on performance data during the specified time period enables you to estimate resource scarcity in the future.

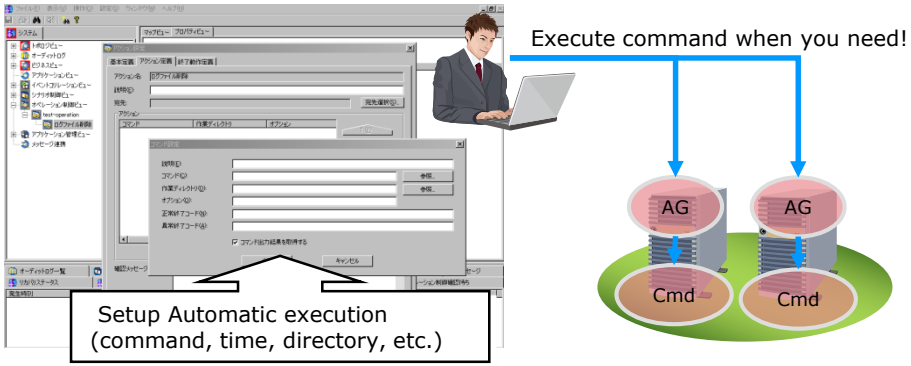


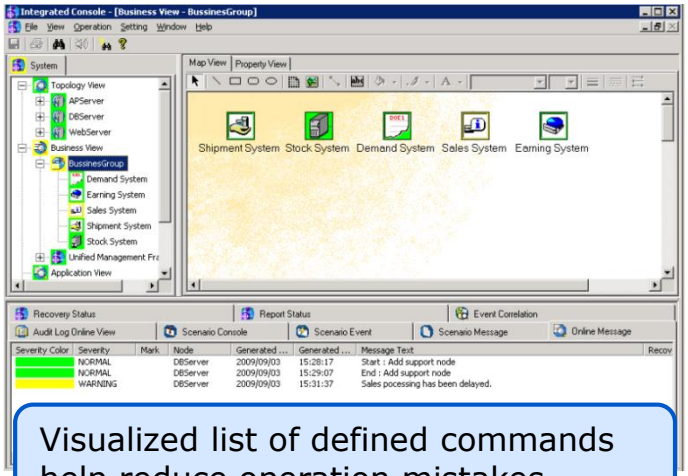
Operation Control

You can execute frequently used commands from integrated console. Visual command control helps reduce human error and simplify the operation.

Useful for executing routine commands such as deleting log files, starting and restarting services, etc.

No need to develop remote execution setup.





Visualized list of defined commands help reduce operation mistakes.

Integrated console shows execution status

Generated Time	Action Name	ActionID	Target Host	Command	Message
2010/06/18 16:45:51	Delete Log File	20100618000000001			To start action.
2010/06/18 16:45:51	Delete Log File	20100618000000001	$MANAGER$	C:\WINDOWS\notepad.exe	Start the command.
2010/06/18 16:50:30	Delete Log File	20100618000000002			To start action.
2010/06/18 16:50:30	Delete Log File	20100618000000002	$MANAGER$	C:\WINDOWS\notepad.exe	Start the command.
2010/06/18 16:53:01	dir	20100618000000001			To start action.
2010/06/18 16:53:01	dir	20100618000000001	$MANAGER$	dir	Start the command.
2010/06/18 16:53:01	dir	20100618000000001	$MANAGER$	dir	End command execute.
2010/06/18 16:53:01	dir	20100618000000001			The action ended.

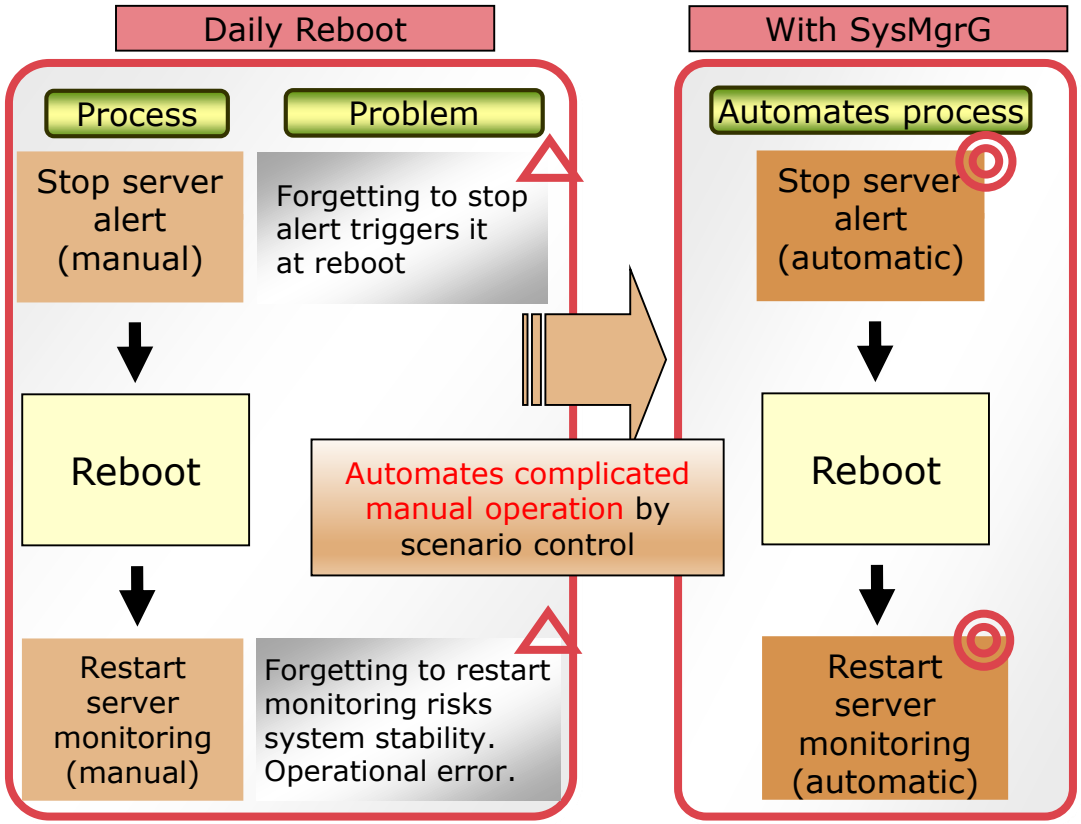
Time for Action | Action Name | Action ID (Automatic Assignment) | Node for Command Execution | Execution Command | Action Status Message

You can keep track with all the operations.

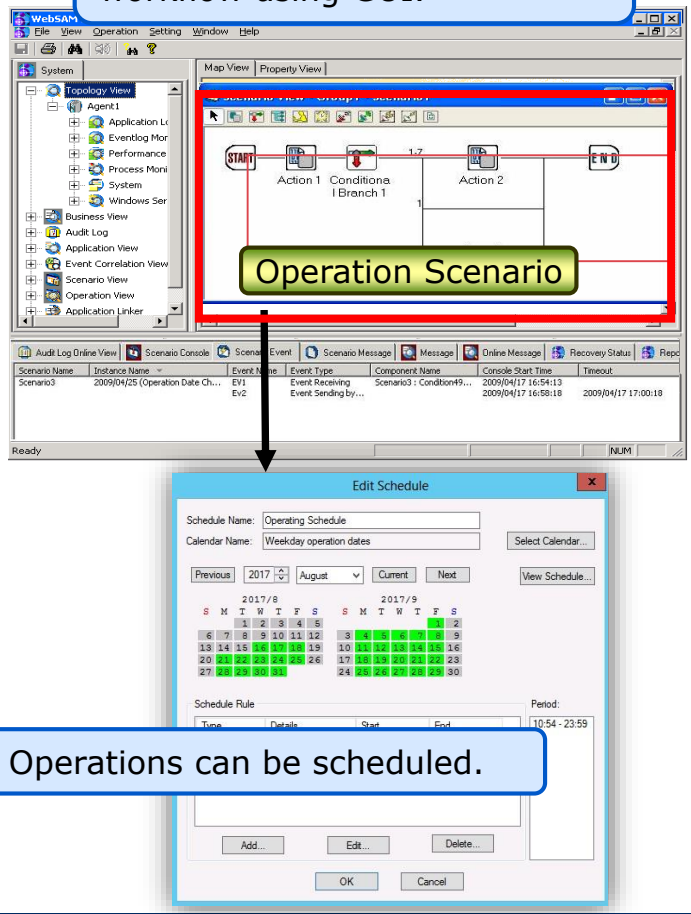
Workflow Control

Execute various commands by operation workflow registered in advance.
Automatic operation realizes safe and efficient management.

Reduce human error and workload by automating alert settings for daily reboot, planned system down for maintenance, etc.



Easy setup for operation workflow using GUI.

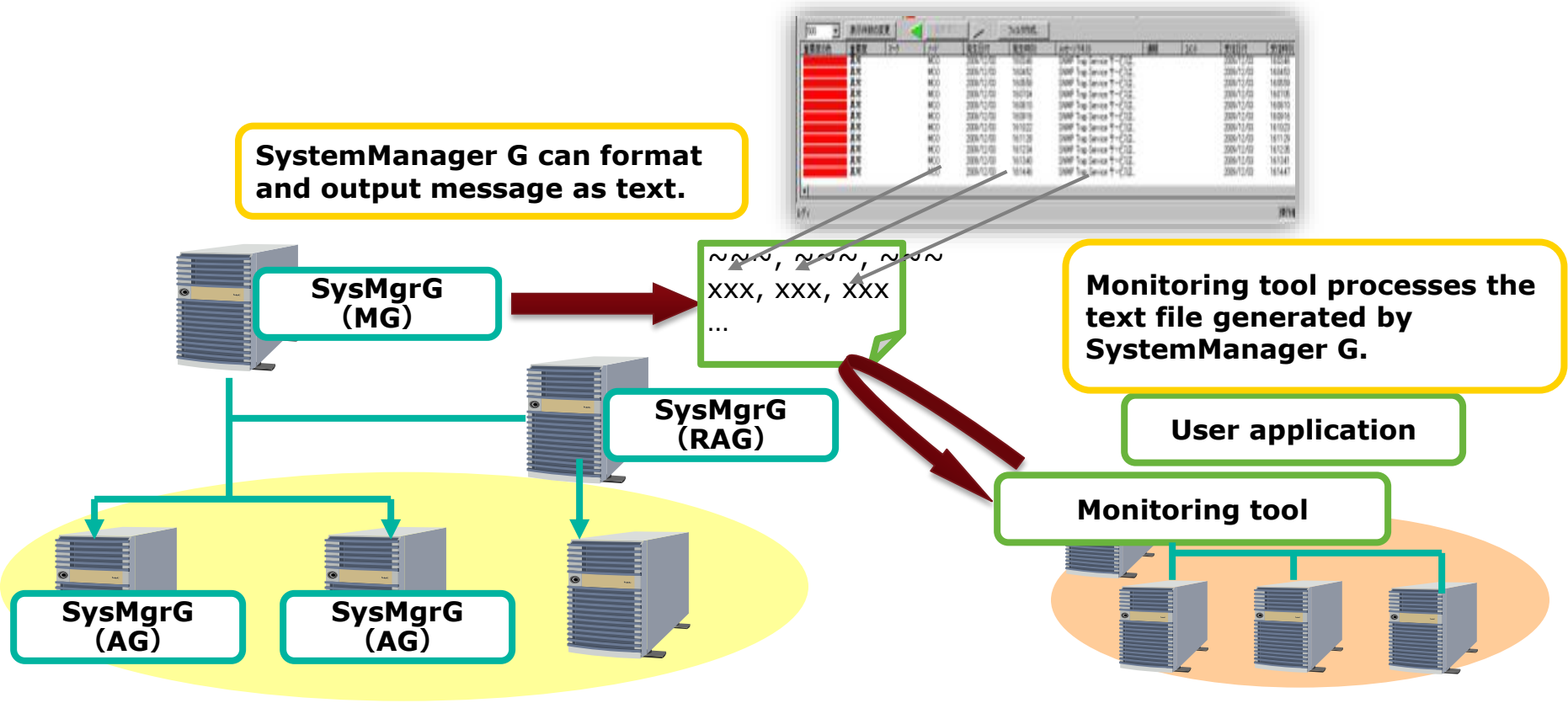


Operations can be scheduled.

Application Linkage

Option
ApLinker

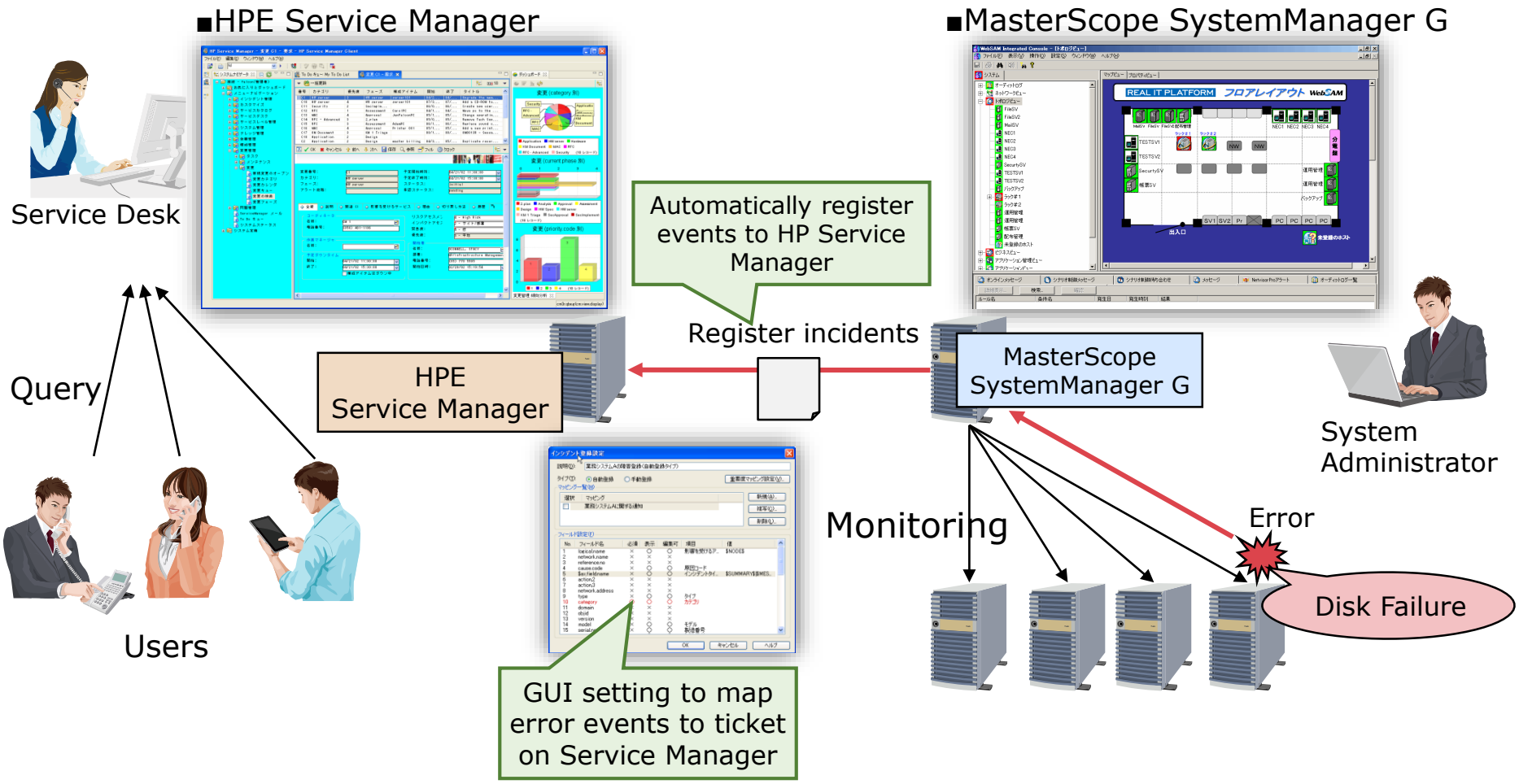
SystemManager G can link another monitoring tool by outputting collected messages to an external file.



Service Desk Linkage (Integration with HPE Service Manager)

Option
ServiceManagerLinker

Collaborating HP Service Manager and SystemManager G makes the acquisition of the server status and tracking work progress very easy.



Thank You

Realize simple and integrated system operation

For more product information,
visit >> http://www.nec.com/masterscope/

For more information, please contact your local NEC representative or contact us at global@soft.jp.nec.com


Orchestrating a brighter world
NEC