Optimize Your IT System Operation with NEC MasterScope Product Suite
- Introduction to Fault Monitoring -

March, 2017
Cloud Platform Division,
NEC Corporation
NEC brings together and integrates technology and expertise to create the ICT-enabled society of tomorrow.

We collaborate closely with partners and customers around the world, orchestrating each project to ensure all its parts are fine-tuned to local needs.

Every day, our innovative solutions for society contribute to greater safety, security, efficiency and equality, and enable people to live brighter lives.
Contents

1. Operational challenges brought about by changing systems
2. System fault monitoring basics
3. Benefits of moving to MasterScope central monitoring for users of NEC ESMPRO
1. Operational challenges brought about by changing systems
System changes and the operational challenges they bring

<table>
<thead>
<tr>
<th>Platform/technology complexity</th>
<th>Changes</th>
<th>Benefits for business departments</th>
<th>Challenges for operations departments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main frame</td>
<td>Unix, Windows, Linux</td>
<td>More options</td>
<td>Dependent on worker skills</td>
</tr>
<tr>
<td>Physical servers</td>
<td>VMware, Hyper-V, AWS, Azure, NECCI, etc.</td>
<td>Faster</td>
<td>Insufficient time to accept/learn</td>
</tr>
<tr>
<td>Virtualization</td>
<td>Cloud</td>
<td>Cost reductions</td>
<td>Increased operational load</td>
</tr>
<tr>
<td>Time required to build system (platform)</td>
<td>Years</td>
<td>Can respond to various requests</td>
<td>Higher requirements/Lower quality</td>
</tr>
<tr>
<td>Number of operators/system size</td>
<td>Large, Small</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Work content</td>
<td>Limited and simple</td>
<td>Varied and complex</td>
<td></td>
</tr>
</tbody>
</table>
Goals of operations departments

A framework enabling continuous improvement is crucial for high-speed, high-quality, and efficient business operations.

<table>
<thead>
<tr>
<th>Platform/technology complexity</th>
<th>Business departments</th>
<th>Challenges for operations departments</th>
<th>Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>More options</td>
<td>Inconsistent skills</td>
<td>Simple operations so that anyone can use even complex technology</td>
</tr>
<tr>
<td>Time required to build system (platform)</td>
<td>Faster</td>
<td>Insufficient time to accept/learn</td>
<td>A framework for quick acceptance</td>
</tr>
<tr>
<td>Number of operators/system size</td>
<td>Cost reductions</td>
<td>Increased operational load</td>
<td>Operational load does not increase even with more devices/systems</td>
</tr>
<tr>
<td>Work content</td>
<td>Can respond to various requests</td>
<td>Higher requirements/Lower quality</td>
<td>Operational quality can be maintained even with more diverse and advanced requirements</td>
</tr>
</tbody>
</table>
Operational management solution map made possible with MasterScope

Management

Support for improvement
- Visualize daily work
- Ascertain man-hours
- Improve work quality

MasterScope IT Process Management

Asset management/Config info collection
- Asset relational management
- Automatic fetching of inventory info
- Software distribution

MasterScope AssetSuite

Integrated monitoring
- Integrated control of systems
- Message collection
- Event correlation analysis

MasterScope MISSION CRITICAL OPERATIONS
MasterScope SystemManager

Alert collection

Monitoring

Network monitoring
- ICMP (Ping) alive monitoring
- SNMP polling
- Trap
- NWConfig management

MasterScope Network Manager

Storage monitoring
- Storage config management
- Disk array state monitoring
- Storage performance monitoring

NEC Storage Manager

Server monitoring
- Physical fault monitoring
- Power/voltage fault monitoring
- Fan fault monitoring

MasterScope SystemManager

OS/AP monitoring
- Resource monitoring
- Service/process monitoring
- Log monitoring (OS/text logs)

MasterScope Application Navigator

Middleware monitoring
- Middleware performance monitoring
- DB (table areas, number of rollbacks)
- AP (number of GCs, heaps)
- Web (number of sessions)

MasterScope Application Navigator

Service level monitoring
- Federated monitoring

Network monitoring
- Service level monitoring

File distribution
- Collective deployment of software

MasterScope DeliveryManager

Backup
- Data backup
- System protection

BackUpExec NetBackup Arcserve Backup etc.

Virtual environment management
- Integrated monitoring of virtual environments
- VM assignment
- Resource pool management

NEC SigmaSystemCenter

Job automation
- Batch process flow control
- Scheduled operations

MasterScope JobCenter

Cloud management
- Self-service resource use
- Virtual FW and LB assignment
- Tenant operations

MasterScope Virtual DataCenter Automation

Automation

Integrated control of systems
Message collection
Event correlation analysis

Alert collection

Manuals

Virtual environment management
- Integrated monitoring of virtual environments
- VM assignment
- Resource pool management

NEC SigmaSystemCenter

Job automation
- Batch process flow control
- Scheduled operations

MasterScope JobCenter

Backup
- Data backup
- System protection

BackUpExec NetBackup Arcserve Backup etc.

Virtual environment management
- Integrated monitoring of virtual environments
- VM assignment
- Resource pool management

NEC SigmaSystemCenter

Job automation
- Batch process flow control
- Scheduled operations

MasterScope JobCenter

Monitoring

Network monitoring
- ICMP (Ping) alive monitoring
- SNMP polling
- Trap
- NWConfig management

MasterScope Network Manager

Storage monitoring
- Storage config management
- Disk array state monitoring
- Storage performance monitoring

NEC Storage Manager

Server monitoring
- Physical fault monitoring
- Power/voltage fault monitoring
- Fan fault monitoring

MasterScope SystemManager

OS/AP monitoring
- Resource monitoring
- Service/process monitoring
- Log monitoring (OS/text logs)

MasterScope Application Navigator

Middleware monitoring
- Middleware performance monitoring
- DB (table areas, number of rollbacks)
- AP (number of GCs, heaps)
- Web (number of sessions)

MasterScope Application Navigator

Service level monitoring
- Federated monitoring

Network monitoring
- Service level monitoring

File distribution
- Collective deployment of software

MasterScope DeliveryManager

Backup
- Data backup
- System protection

BackUpExec NetBackup Arcserve Backup etc.

Virtual environment management
- Integrated monitoring of virtual environments
- VM assignment
- Resource pool management

NEC SigmaSystemCenter

Job automation
- Batch process flow control
- Scheduled operations

MasterScope JobCenter

Integration
- Integrated control of systems
- Message collection
- Event correlation analysis

Alert collection

Manuals

Knowledge sharing
2. System fault monitoring basics

- **Necessity of system fault monitoring**
- Types of fault monitoring
- Case study for troubleshooting
- Implementation of system fault monitoring
What is system fault monitoring?

An issue that causes the services provided by IT systems to be suspended, thus making the services unavailable to users.

What is a system fault?

An issue that causes the services provided by IT systems to be suspended, thus making the services unavailable to users.

What is system fault monitoring?

A monitoring process whereby a monitoring tool detects the suspension of services and notifies the administrator of the issue using a pre-determined method.

Monitoring tools provide a suite of functions to enable this process.

Got it! I’ll troubleshoot it straight away!
What is involved in manual fault monitoring?

There are many steps involved in motoring faults manually and a lot of information has to be checked, which takes a long time and slows down fault detection.

Check resources
Check running processes
Conduct network polling

Check application logs
Check running services
Check event logs
Run and check each application
Benefits of using fault monitoring tools

Fault monitoring tools streamline daily monitoring work and enable immediate fault detection and troubleshooting.

General flow:
- Daily monitoring
  - Fault occurred
  - Detect faults
  - Troubleshoot
  - Find cause
  - Fix fault

Benefits of using a fault monitoring tool:
- (1) Efficient regular monitoring work
- (2) Earlier fault detection
- (3) Earlier pinpointing of fault location

Benefits:
- Daily work optimization
- Prompt troubleshooting

Time varies depending on the details of each fault.
2. System fault monitoring basics

- Necessity of system fault monitoring
- **Types of fault monitoring**
- Case study for troubleshooting
- Implementation of system fault monitoring
Fault monitoring types and system monitoring levels

Fault monitoring suited to the features of each system is required to raise the system monitoring level.

<table>
<thead>
<tr>
<th>Monitoring layer</th>
<th>Monitoring level and details</th>
<th>Examples of monitoring</th>
<th>Applicable MasterScope product</th>
</tr>
</thead>
</table>
| Service          | Monitoring level 3          | - Monitoring of Web page response time
                   | - App-specific performance monitoring
                   | - Monitoring of Oracle table area thresholds  |
| OS               | Monitoring level 2          | - Monitoring of virtual platform (VMware vSphere) resources
                   | - Application log monitoring
                   | - Alive monitoring for Oracle/business application processes
                   | - OS system log monitoring
                   | - Application log monitoring
                   | - Service/process monitoring
                   | - OS resource (CPU, memory, etc.) monitoring
                   | - Resource monitoring |
| Virtual platform | Monitoring level 1          | - HDD fault monitoring
                   | - Device fault monitoring
                   | - Temperature monitoring
                   | - Alive monitoring
                   | - RAID monitoring
                   | - Monitoring of controllers, etc. |
| Server           |                             | - Network device fault
                   |                             | - Ping polling |
| Storage          |                             |                        |
| Network          |                             |                        |
Hardware faults (disk, fans, etc.) are monitored by tools provided by hardware vendors. Express Servers are monitored by NEC ESMPRO/ServerManager and ServerAgentService.

Ping (ICMP) is used to confirm network communication between monitored servers and network devices.
Overview of fault monitoring (2/5)

All the program processes required for service provision are monitored. This monitoring is very important because a process going down could directly cause operations to stop.

**Key point**
Processes of applications that need to be always running are monitored.

---

**Windows service monitoring**

Statues of services to be provided are monitored. This monitoring is very important because the stoppage of services could directly cause operations to stop.

**Key point**
Services that need to be always running are monitored.
### Overview of fault monitoring (3/5)

<table>
<thead>
<tr>
<th>Monitoring layer</th>
<th>Image of monitoring</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lv2 URL response monitoring</td>
<td><img src="image1.png" alt="Image of monitoring" /></td>
<td>Threshold values for CPU load and memory/disk free space are used for monitoring. Resource faults need to be monitored regularly because they may degrade performance and cause operations to stop.</td>
</tr>
<tr>
<td>Lv2 Protocol monitoring</td>
<td></td>
<td>Key point The threshold may be exceeded for an instant, which should not be regarded as fault. Therefore monitoring should be configured so that a fault is determined only if the threshold is exceeded several times in a row.</td>
</tr>
<tr>
<td>Lv2 Application performance monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lv2 Log monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lv2 Resource monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lv2 Service/process monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lv2 Alive monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lv2 Hardware fault monitoring</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Event logs**

Windows OS logs are used as event logs. Logs to be monitored can be filtered based on attributes such as the event type (error, warning, etc.), source name, and event ID.

**Key point**

- It is important to clarify which logs need to be monitored since various application logs are output as event logs.
- Note that if all the logs are monitored, operator workloads will increase due to the large number of messages.
### Overview of fault monitoring (4/5)

#### Monitoring layer

<table>
<thead>
<tr>
<th>Monitoring layer</th>
<th>Image of monitoring</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lv2</td>
<td><img src="image1.png" alt="Resource monitoring" /></td>
<td><strong>Resource monitoring</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image2.png" alt="Protocol monitoring" /></td>
<td><strong>Protocol monitoring</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image3.png" alt="Alive monitoring" /></td>
<td><strong>Alive monitoring</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image4.png" alt="Hardware fault monitoring" /></td>
<td><strong>Hardware fault monitoring</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image5.png" alt="Service/process monitoring" /></td>
<td><strong>Service/process monitoring</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image6.png" alt="Application performance monitoring" /></td>
<td><strong>Application performance monitoring</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image7.png" alt="Log monitoring" /></td>
<td><strong>Log monitoring</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image8.png" alt="URL response monitoring" /></td>
<td><strong>URL response monitoring</strong></td>
</tr>
<tr>
<td>Lv3</td>
<td><img src="image9.png" alt="Example of Oracle performance screen" /></td>
<td><strong>Example of Oracle performance screen</strong></td>
</tr>
</tbody>
</table>

**Text log / syslog**

Logs can be viewed in text format. Log contents matching keywords are monitored.

**Key point**

For monitoring using keyword matching, it is important to clarify the keywords to be monitored.

**Example of Oracle performance screen**

For database servers, the instance startup status, table area free space, number of sessions, and other DB-specific performance items are monitored based on threshold values.

For application servers, the heap memory capacity, number of garbage collections, and other performance items are monitored based on threshold values.

**Key point**

Monitoring must be configured per each application because performance items to be monitored vary.
### Overview of fault monitoring (5/5)

#### Monitoring layer
- Resource monitoring
- Log monitoring
- Application performance monitoring
- URL response monitoring
- Protocol monitoring
- Alive monitoring
- Service/process monitoring
- Hardware fault monitoring

#### Image of monitoring

<table>
<thead>
<tr>
<th>Example of monitoring</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Http/Https</strong></td>
<td>Check connectivity via http</td>
</tr>
<tr>
<td><strong>Email</strong></td>
<td>Check SMTP/POP requests</td>
</tr>
<tr>
<td><strong>FTP</strong></td>
<td>Get files from FTP servers</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Check port connectivity</td>
</tr>
</tbody>
</table>

**Key point**
Service level availability can be confirmed but additional monitoring methods are needed to find root causes.

#### How many seconds?

<table>
<thead>
<tr>
<th>Login</th>
<th>Search</th>
</tr>
</thead>
</table>

**Key point**
Response varies depending on the location of the monitoring server. Equivalent conditions should be applied to monitoring servers to measure response from an end user perspective.
## Fault detection methods generally used for systems

<table>
<thead>
<tr>
<th>Monitoring</th>
<th>Outline</th>
<th>Manual procedure</th>
<th>MasterScope product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alive monitoring</td>
<td>PING (ICMP) polling</td>
<td>Check by running a Ping command</td>
<td>MasterScope Network Manager</td>
</tr>
<tr>
<td>Monitoring via SNMP</td>
<td>Trap reception and MIB polling via SNMP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol monitoring</td>
<td>Monitor the response of specific protocols (http, SMTP, FTP, etc.)</td>
<td>Use an actual service to check response (e.g. send an email)</td>
<td>MasterScope Application Navigator</td>
</tr>
<tr>
<td>Service level monitoring (URL response monitoring)</td>
<td>Monitor the response speed in a process flow of a specific Web application</td>
<td>Use an actual service to check response (e.g. log in to a Web application and run a test process)</td>
<td></td>
</tr>
<tr>
<td>Application performance</td>
<td>Monitor API performance thresholds of specific middleware (App server heap area, DB table space, etc.)</td>
<td>Run the management tool or special commands of the middleware</td>
<td></td>
</tr>
<tr>
<td>Service alive</td>
<td>Monitor start/stop of Windows services</td>
<td>Use OS management tools</td>
<td></td>
</tr>
<tr>
<td>Process alive</td>
<td>Monitor the number of processes using a threshold</td>
<td>Use Task Manager and PS commands</td>
<td>MasterScope SystemManager</td>
</tr>
<tr>
<td>Resources</td>
<td>Monitor the CPU, disk, and memory based on thresholds</td>
<td>For UNIX systems, use the Top command, etc. For Windows systems, use Task Manager, etc.</td>
<td></td>
</tr>
<tr>
<td>Logs</td>
<td>Monitor event logs, syslogs, and text logs based on specific keywords</td>
<td>Use Event Viewer or open a log file</td>
<td>Various hardware vendor tools (for Express Server : NEC ESMPRO/ServerManager and ServerAgentService)</td>
</tr>
<tr>
<td>Hardware monitoring</td>
<td>Monitor hardware-specific faults on servers and storage devices</td>
<td>Check indicators of servers onsite</td>
<td></td>
</tr>
</tbody>
</table>
2. System fault monitoring basics

- Necessity of system fault monitoring
- Types of fault monitoring
- Troubleshooting case studies
- Implementation of system fault monitoring
What should we do if a system fault occurs?

When a system fault occurs, first we need to detect it, and then troubleshoot to find the location.

- Example of initial troubleshooting

  - Which system (IT service) is not available?
  - Is the network available? How far is it available?
  - Is there a problem with the hardware?
  - Is the resource status normal?
  - Is any service or process stopped (application abend)?
  - Is any fault indicated in the logs?
  - Is there a problem with the DB or middleware performance?
    etc.

Based on this information, find out which layer (hardware, OS, network, middleware, or application) has a problem, find the root cause, and analyze the problem in detail.

Five fault detection and troubleshooting case studies are described on the following pages.
Case 1. Hardware fault monitoring

If only the server monitoring tool bundled with the hardware is used, generally only hardware faults can be detected.

<table>
<thead>
<tr>
<th>Monitoring level</th>
<th>Fault details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk fault (Hardware fault)</td>
<td>Network disconnection</td>
</tr>
<tr>
<td>![Disk fault icon]</td>
<td>![Network disconnection icon]</td>
</tr>
<tr>
<td>✓</td>
<td>-</td>
</tr>
</tbody>
</table>

Detection/ Troubleshooting

Key points

- ✓ Easy to get started. (Generally, the monitoring software bundled with the hardware can be used.)
- ✓ Generally, only hardware faults can be detected.
- ✓ Difference monitoring tools need to be used if servers are provided by multiple vendors, which could delay initial response and increase operator workloads.

⇒ An integrated monitoring tool is needed for central monitoring.
Case 2. Alive monitoring by ping

Alive monitoring by means of ping can only monitor network connectivity.

<table>
<thead>
<tr>
<th>Monitoring level</th>
<th>Fault details</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL response monitoring</td>
<td>Disk fault (Hardware fault)</td>
</tr>
<tr>
<td>Protocol monitoring</td>
<td>Network disconnection</td>
</tr>
<tr>
<td>Log monitoring</td>
<td>Process down (Service down)</td>
</tr>
<tr>
<td>Resource monitoring</td>
<td>Resource fault</td>
</tr>
<tr>
<td>Service/process monitoring</td>
<td>Error log</td>
</tr>
<tr>
<td>Alive monitoring</td>
<td>Application performance (e.g. database)</td>
</tr>
<tr>
<td>Hardware fault monitoring</td>
<td></td>
</tr>
</tbody>
</table>

Detection/ Troubleshooting

- Ping

Key points

- Easy to get started. (Monitoring is possible if ping is successful. No agent is required.)
- No dependency on hardware and OS.
- Only network connectivity can be monitored.
Case 3. Including server monitoring

Faults of applications running on servers can also be monitored. This configuration is normally used for system fault monitoring.

<table>
<thead>
<tr>
<th>Monitoring level</th>
<th>Fault details</th>
<th>Key points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk fault (Hardware fault)</td>
<td>Network disconnection</td>
<td>Process down (Service down)</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

- Faults of applications running on servers can also be monitored.
- Can monitor hardware faults and other faults in a central manner by linking with various hardware monitoring tools.
- Middleware details such as Oracle table area capacity cannot be monitored.
### Case 4. Including application (middleware) performance monitoring

This configuration is normally used for advanced monitoring including monitoring of middleware performance (databases, application servers, and Web servers).

<table>
<thead>
<tr>
<th>Monitoring level</th>
<th>Fault details</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL response monitoring</td>
<td>Disk fault (Hardware fault)</td>
</tr>
<tr>
<td>Protocol monitoring</td>
<td>Network disconnection</td>
</tr>
<tr>
<td>Application performance monitoring</td>
<td>Process down (Service down)</td>
</tr>
<tr>
<td>Log monitoring</td>
<td>Resource fault</td>
</tr>
<tr>
<td>Resource monitoring</td>
<td>Error log</td>
</tr>
<tr>
<td>Service/process monitoring</td>
<td>Application performance (e.g. database)</td>
</tr>
<tr>
<td>Alive monitoring</td>
<td>Hardware fault monitoring</td>
</tr>
<tr>
<td>Hardware fault monitoring</td>
<td></td>
</tr>
</tbody>
</table>

**Detection/Troubleshooting**

- ✓
- ✓
- ✓
- ✓
- ✓
- ✓

**Key points**

- ✓ Application (middleware) performance can also be monitored.
- ✓ More detailed troubleshooting is possible compared with server monitoring.
Case 5. Service level monitoring

The entire system is monitored in a cross functional manner to monitor operational status and response from a user perspective.

Service level fault detection is possible

- Monitoring is possible without installing an agent on the server.
- System faults and slow responses can be detected but troubleshooting is difficult.
- Not all systems can be monitored (systems that do not support relevant protocols cannot be monitored).

Notes
2. System fault monitoring basics

- Necessity of system fault monitoring
- Types of fault monitoring
- Case study for troubleshooting
- Implementing system fault monitoring
Considerations before implementing system fault monitoring

The following points need to be considered before implementing system fault monitoring:

1. Identify the systems to be monitored
   - Understand the customer's system configuration and identify systems that need to be monitored.

2. Identify what will be monitored
   - Identify what needs to be monitored in each system.

3. Check notification methods/recipient
   - Clarify who is notified of fault detections and how they are notified.

4. Understand the operation schedule
   - Organize the operational schedule in a timetable format.

5. Check other requirements
   - Check any customer specific requirements.

- Number of servers
- Appliance servers
- Storage
- Number of network devices
- Alive monitoring
- Log monitoring
- Process monitoring
- Service level monitoring, etc.
- Email notification
- Warning indicator
- Console, etc.
- Who should be notified?
- Monitoring time
- Restart
- Specific processing
(1) Identify the systems to be monitored

Check the quantities and types of servers, network devices, and storage devices to be monitored.

<table>
<thead>
<tr>
<th>System name</th>
<th>Host name</th>
<th>Model</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB</td>
<td>SV1</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>Email</td>
<td>SV2</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>Report</td>
<td>SV3</td>
<td>Express5800/110Ri-2</td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>Batch</td>
<td>SV4</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>EDI</td>
<td>SV5</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>ERP</td>
<td>SV6</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>Operational management</td>
<td>SV7</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>Other</td>
<td>SV8</td>
<td>Express5800/1**</td>
<td>Windows 2008 R2</td>
</tr>
<tr>
<td>Other</td>
<td>SV9</td>
<td>Express5800/1**</td>
<td>Windows 2008 R2</td>
</tr>
<tr>
<td>Other</td>
<td>SV10</td>
<td>Express5800/1**</td>
<td>Windows 2008 R2</td>
</tr>
</tbody>
</table>
Identify what should be monitored (1/2)

It is important to define what is the “normal” state and what phenomena are regarded as faults for each system (server).

**Example of judging normal/fault states**

<table>
<thead>
<tr>
<th>Normal: Processes A, B, and C exist</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault: One or more of these processes does not exist</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process A</th>
<th>Process B</th>
<th>Process C</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Down</strong></td>
</tr>
</tbody>
</table>

**Monitored items**

- **Process monitoring**
- **Log monitoring**
- **Alive monitoring**

A fault is determined if "ERROR" is output to the log.

A fault is determined if there is no response to ping.
## (2) Identify what should be monitored (2/2)

Organize current and future monitoring targets for each system.

<table>
<thead>
<tr>
<th>System name</th>
<th>Model</th>
<th>OS</th>
<th>Ping alive</th>
<th>Service monitoring</th>
<th>Process monitoring</th>
<th>Resource monitoring</th>
<th>Event log Syslog monitoring</th>
<th>Other (currently performed)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current method</td>
<td>Tool</td>
<td>Not performed</td>
<td>Not performed</td>
<td>Checked on monitor</td>
<td>Checked on monitor</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DB</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2012 R2</td>
<td>◎</td>
<td>-</td>
<td>◎</td>
<td>◎</td>
<td>◎</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2012 R2</td>
<td>◎</td>
<td>-</td>
<td>◎</td>
<td>◎</td>
<td>◎</td>
<td>Check by sending email</td>
</tr>
<tr>
<td>Report</td>
<td>Express5800/110Ri-2</td>
<td>Windows 2012 R2</td>
<td>◎</td>
<td>◎</td>
<td>◎</td>
<td>◎</td>
<td>◎</td>
<td></td>
</tr>
<tr>
<td>EIP</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2012 R2</td>
<td>◎</td>
<td>-</td>
<td>◎</td>
<td>◎</td>
<td>◎</td>
<td>Connect and check each device</td>
</tr>
<tr>
<td>EDI</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2012 R2</td>
<td>◎</td>
<td>-</td>
<td>◎</td>
<td>◎</td>
<td>◎</td>
<td></td>
</tr>
<tr>
<td>ERP</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2012 R2</td>
<td>◎</td>
<td>-</td>
<td>◎</td>
<td>◎</td>
<td>◎</td>
<td>Check the response speed</td>
</tr>
<tr>
<td>Operational</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2012 R2</td>
<td>◎</td>
<td>◎</td>
<td>◎</td>
<td>◎</td>
<td>◎</td>
<td></td>
</tr>
<tr>
<td>management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2008 R2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2008 R2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2008 R2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

◎: Should be monitored in the future, ●: Currently monitored, -: No need to be monitored, △: Should be improved or discontinued
(3) Check notification methods/recipient (1/2)

Consider who is notified and how to notify when a fault is detected.

<table>
<thead>
<tr>
<th>Notification method</th>
<th>Notification scope</th>
<th>Awareness of notification</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Several users (including remote users)</td>
<td></td>
<td>Emails may be checked later.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A mail server (SMTP) is required on the network.</td>
</tr>
<tr>
<td>Warning indicator</td>
<td>Users near warning indicators</td>
<td></td>
<td>Light and sound catches users’ attention.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Check supported models. Command creation may be required.</td>
</tr>
<tr>
<td>Monitoring screen</td>
<td>Only users viewing the monitoring screen</td>
<td></td>
<td>Must check the screen all the time to detect a fault as it happens.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The screen must always be open.</td>
</tr>
<tr>
<td>Popup</td>
<td>Users viewing the PC screen</td>
<td></td>
<td>Must check the screen all the time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>May need to create a popup script.</td>
</tr>
<tr>
<td>Beep</td>
<td>Users near the device that beeps</td>
<td></td>
<td>Beeps are easy for users to hear.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Need to find where is the beep is coming from (Admin terminal, server, etc.).</td>
</tr>
</tbody>
</table>
(3) Check notification methods/recipient (2/2)

■ Changing the notification method according to the severity

**When a fault event is issued**
- Send an email to Administrators A and B (PC and mobile).
- Sound the alarm.

**When a warning event is issued**
- Send an email only to Administrator B (PC only).

■ Changing the recipient according to who handles the system

<table>
<thead>
<tr>
<th>System name</th>
<th>Model</th>
<th>OS</th>
<th>Recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2012 R2</td>
<td>Administrator A</td>
</tr>
<tr>
<td>Email</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2012 R2</td>
<td>Administrator B</td>
</tr>
<tr>
<td>Report</td>
<td>Express5800/110Ri-2</td>
<td>Windows 2012 R2</td>
<td>Administrator A</td>
</tr>
<tr>
<td>EIP</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2012 R2</td>
<td>Administrator A</td>
</tr>
<tr>
<td>EDI</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2008 R2</td>
<td>Administrator A</td>
</tr>
<tr>
<td>ERP</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2008 R2</td>
<td>Administrator A</td>
</tr>
<tr>
<td>Operational management</td>
<td>Express5800/120Rj-2</td>
<td>Windows 2008 R2</td>
<td>Administrator B</td>
</tr>
</tbody>
</table>
(4) Understand the operation schedule

Check the operation schedule to know when monitoring will stop due to system stoppage/restart.

| Daily schedule | 6:00 | 7:00 | 8:00 | 9:00 | 10:00 | 11:00 | 12:00 | 13:00 | 14:00 | 15:00 | 16:00 | 17:00 | 18:00 | 19:00 | 20:00 | 21:00 | 22:00 | 23:00 | 0:00 | 1:00 | 2:00 | 3:00 | 4:00 | 5:00 |
|----------------|------|------|------|------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|------|------|------|------|------|------|
| **Time restart** | 6:00 | 7:00 | 8:00 | 9:00 | 10:00 | 11:00 | 12:00 | 13:00 | 14:00 | 15:00 | 16:00 | 17:00 | 18:00 | 19:00 | 20:00 | 21:00 | 22:00 | 23:00 | 0:00 | 1:00 | 2:00 | 3:00 | 4:00 | 5:00 |
| DB | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | |
| Email | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Report | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Job | | | | | | | | | | | | | | | | | | | | | | | | | | |
| EDI | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | |
| ERP | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | |
| Operation / management | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Other | | | | | | | | | | | | | | | | | | | | | | | | | | |

- Time when system is monitored manually
- Specific processing is executed
- System stop (restart) time

Orchestrating a brighter world
(5) Check other requirements

Identify current operational tasks and relevant issues, and consider whether they can be improved by using tools.

Example of operations

- If a specific log file had been updated, an error may have occurred, so check whether any files have been updated.
- If a new file was created, it means that a specific application was stopped, so check for any new files.
- Run specific commands to resolve faults that have occurred.
- Because the monitoring tools differ depending on the system, several monitoring screens need to be checked.
Key points for monitoring

Policies for stable system operations

Consideration 1
What is monitored and how? (Combination)
- Service level monitoring
- Application performance monitoring
- Log monitoring
- Service/process monitoring
- Resource monitoring
- Network monitoring
- Hardware monitoring
- Storage monitoring
- etc.

Detect system faults/failure signs

Consideration 2
How does the user (administrator) receive the notification? (System for administrators)
- Send emails
- Patlite control
- Voice sound
- etc.

Recognition/notification of faults

Consideration 3
What happened? (Visualization)
- Location management (physical topology)
- Message management (categorization)
- etc.

Identification of faults
- Send emails
- Patlite control
- Voice sound
- etc.

Consideration 4
How can the system be recovered immediately?
- Troubleshooting support
- etc.

System recovery

Handling policy

Analysis/determination policy

Identify the cause and extent of impact. Understand the operation status

Monitoring policy

Notification policy

Image of stable system operation

Accumulated statistics

Performance history

Fault messages
3. Benefits of utilizing MasterScope central monitoring for users of NEC ESMPRO
Issues when system faults cannot be centrally monitored

System consists of various devices such as servers, networks, and storage, as well as elements such as middleware, applications, and performance. If these elements cannot be centrally monitored, various different tools and procedures will be needed, resulting in complex operations.

Without a central monitoring framework...

- Monitoring with different tools increases workloads
- Multiple monitoring tools need to be implemented
- Detection and troubleshooting take a long time

Different confirmation methods

- Use NEC ESM PRO to check for faults
- Use NEC Storage Manager to check for faults
- Check business application logs
- Use third party software to check the faults

Express5800

NEC Storage

Application

Third party servers/systems
Advantages of central monitoring for system faults

If a central monitoring framework is implemented, systems can be monitored from one location, which simplifies system monitoring operations and standardizes monitoring methods.

Central monitoring enables quick detection of system faults

Example of using MasterScope SystemManager

- Server fault
  - Express5800
- Storage fault
  - NEC Storage
- Business application fault
  - Application
- Server fault
  - Third party servers/systems
Example of faults that cannot be detected by NEC ESMPRO hardware monitoring alone

Monitoring by MasterScope is needed to detect not only hardware faults but also faults of the OS and applications running on servers.

If only hardware is monitored...

I cannot connect to the business system.

It’s not a hardware problem... What is the cause?

Points to confirm

- Process down
- Application errors
- Resources
- Application performance

MasterScope solutions

1. Process monitoring
   Alive monitoring for processes on servers is needed.

2. Text log monitoring
   Logs output by server applications need to be monitored.

3. Resource monitoring
   OS performance details need to be monitored.

4. Application performance monitoring
   Application performance needs to be monitored.

Requires skilled operators who can use their own knowledge to identify the cause...
Comparison between SystemManager and NEC ESMPRO (physical server monitoring)

A major difference is that MasterScope SystemManager offers advanced monitoring of operating systems and business applications (logs, processes/services, OS resources, etc.). Consider promoting MasterScope SystemManager for customers who require business application monitoring.

<table>
<thead>
<tr>
<th>Monitoring</th>
<th>MasterScope SystemManager</th>
<th>NEC ESMPRO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware faults</strong></td>
<td>—</td>
<td>○ Available</td>
</tr>
<tr>
<td></td>
<td>• Instead of directly monitoring the hardware, faults are detected by monitoring the fault information in the logs output by other tools (such as NEC ESMPRO).</td>
<td></td>
</tr>
<tr>
<td><strong>System logs</strong></td>
<td>○</td>
<td></td>
</tr>
<tr>
<td>(Event logs, syslogs)</td>
<td>• Monitored servers can be configured in the View.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Advanced monitoring settings are available such as keyword-based text filtering.</td>
<td></td>
</tr>
<tr>
<td><strong>Text logs</strong></td>
<td>○</td>
<td>X Not available</td>
</tr>
<tr>
<td></td>
<td>• Application logs in text format are filtered by keywords for monitoring.</td>
<td></td>
</tr>
<tr>
<td><strong>Processes/services</strong></td>
<td>○</td>
<td>X Not available</td>
</tr>
<tr>
<td></td>
<td>• Alive monitoring for application processes (for Windows services, startup is also monitored)</td>
<td></td>
</tr>
<tr>
<td><strong>Resources</strong></td>
<td>○</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Not only CPU and memory but also thresholds for various resources on the OS are monitored.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Resource status can be viewed on a performance graph.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Accumulated resource status information can be output as statistics in CSV format.</td>
<td></td>
</tr>
<tr>
<td><strong>(Note) Monitoring settings</strong></td>
<td>— Collectively configured from the control device.</td>
<td>— Log in to the server to configure event log monitoring</td>
</tr>
</tbody>
</table>

○: Advanced, ○: Normal, x: Not available, - : Out of scope
## Comparison between SystemManager and NEC ESMPRO (virtual server monitoring)

Consider using MasterScope SystemManager to monitor not only hardware but also ESXi and guest OS’s (business applications) for faults.

<table>
<thead>
<tr>
<th>Monitoring</th>
<th>MasterScope SystemManager</th>
<th>NEC ESMPRO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware faults</td>
<td>• Instead of directly monitoring the hardware, faults are detected by monitoring the fault information in the logs output by other tools (such as NEC ESMPRO).</td>
<td>○ Optional</td>
</tr>
<tr>
<td><strong>ESXi</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resources</td>
<td>○ • Use HypervisorMonitorOption.</td>
<td>× Not available</td>
</tr>
<tr>
<td>Logs</td>
<td>○ • Use HypervisorMonitorOption.</td>
<td>△ • Linked with NEC ESMPRO/ServerAgent for vMA.</td>
</tr>
<tr>
<td><strong>Guest OS’s</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System logs (Event logs, syslogs)</td>
<td>• Monitored servers can be configured in the View. • Advanced monitoring settings are available such as keyword-based text filtering.</td>
<td>△ • Use NEC ESMPRO/ServerAgent for Guest OS (fee-based). • For Windows servers, monitoring is configured based on the source and event ID (keywords are available for Linux).</td>
</tr>
<tr>
<td>Text logs</td>
<td>○ • Application logs in text format are filtered by keywords for monitoring.</td>
<td>× Not available</td>
</tr>
<tr>
<td>Processes/services</td>
<td>○ • Alive monitoring for application processes (for Windows services, startup is also monitored)</td>
<td>× Not available</td>
</tr>
<tr>
<td>Resources</td>
<td>◎ • Not only CPU and memory but also thresholds for various resources on the OS are monitored. • Resource status can be viewed on a performance graph. • Accumulated resource status information can be output as statistics in CSV format.</td>
<td>△ • Use NEC ESMPRO/ServerAgent for Guest OS (fee-based). • Thresholds for CPU/memory usage and disk space can be used for monitoring.</td>
</tr>
</tbody>
</table>

◎: Advanced, ○: Normal, △: Partly available, ×: No feature, —: Out of scope
Comparison between MasterScope SystemManager and NEC ESMPRO (event log monitoring)

MasterScope SystemManager monitoring allows you to specify detailed conditions such as severity and content of event logs. It is especially helpful that the severity of each log message output by applications can be changed based on its content.

**MasterScope SystemManager**

Event log monitoring for all monitored servers can be configured from the View.

In addition to the event source and ID, the message text and severity can be specified as fault detection conditions.

**NEC ESMPRO/SM, SAS**

Event log monitoring needs to be configured on the SAS on each monitored server.

Can only specify only the source and event IDs as fault detection conditions.

*Message texts cannot be specified.*
Comparison between MasterScope SystemManager and NEC ESMPRO (resource monitoring)

MasterScope SystemManager can monitor various resources on the OS, and can output accumulated data as a graph or in CSV files, which can then be used for performance analysis and reporting.

**Resource information that can be monitored**
- CPU usage
- Memory usage (amount and ratio)
- Disk space
- CPU usage per process
- Processor queue
- Disk I/O
- NIC traffic etc.

*Various resources on the OS can be monitored*
(For Windows, performance monitoring or equivalent is possible. For Linux, monitoring via sar and df is possible)

In addition to threshold monitoring, resource info is displayed on a graph. **Accumulated statistics can be output as CSV files.**

Threshold monitoring is possible. The icons of items with their threshold exceeded will change. *Statistical data cannot be accumulated.*

**Resource information that can be monitored**
- CPU usage
- Memory usage
- Disk space
(As of November 2015)

NEC ESMPRO/SM, SAS

**Resource information that can be monitored**
- CPU usage
- Memory usage
- Disk space
(For Windows, performance monitoring or equivalent is possible. For Linux, monitoring via sar and df is possible)
Orchestrating a brighter world

NEC