\Orchestrating a brighter world NEC

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

March, 2017

Cloud Platform Division,

NEC Corporation

\Orchestrating a brighter world

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

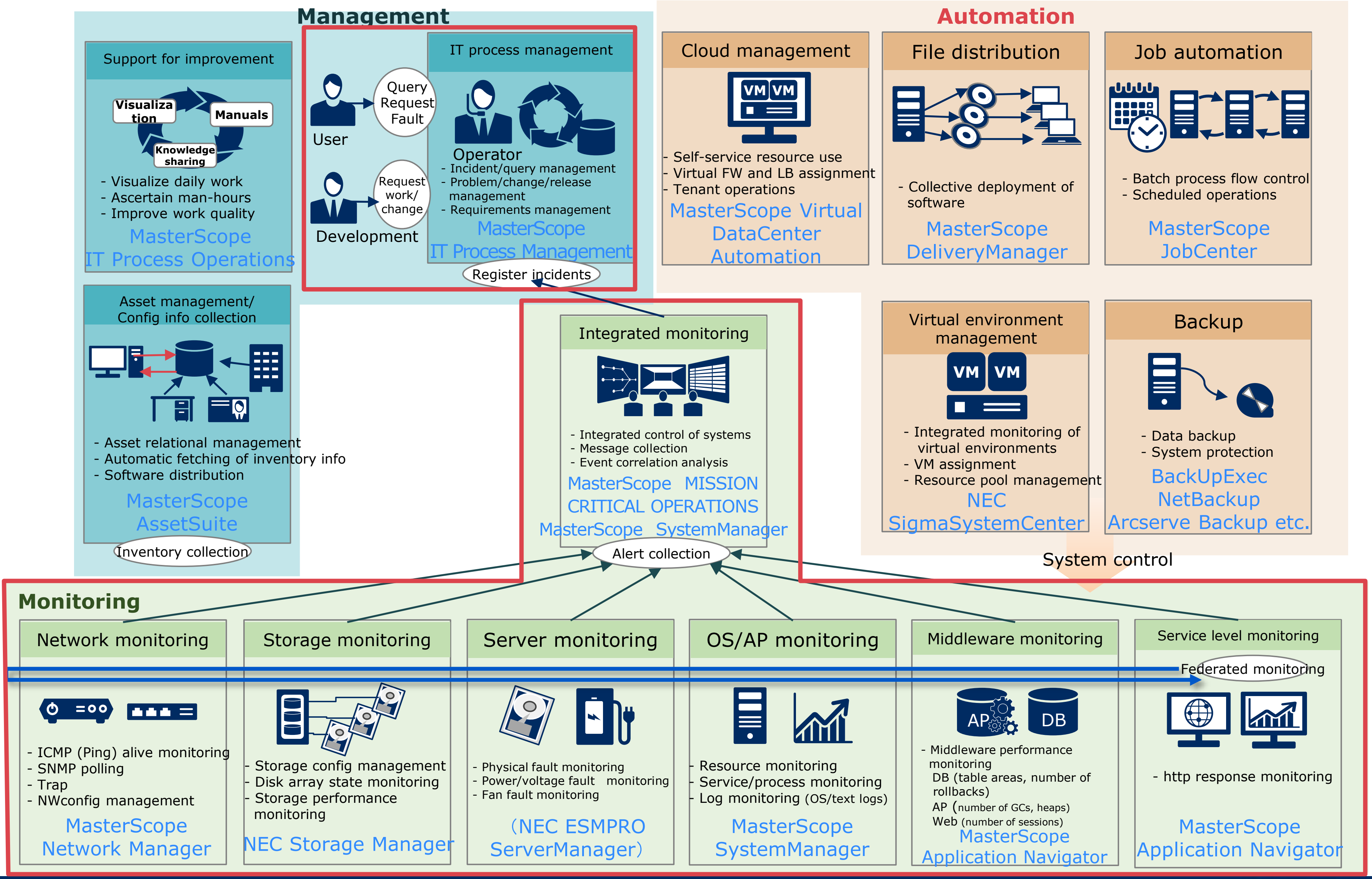
	Changes				Benefits for business departments	Challenges for operations departments
	Main frame	Physical servers	Virtualization	Cloud		
Platform/ technology complexity	Single vendor	Unix Windows Linux	VMware Hyper-V	AWS Azure NECCI etc.	More options 😄	Dependent on worker skills 😖
Time required to build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

Goals of operations departments

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

	Business departments	Challenges for operations departments		Goal
Platform/ technology complexity	More options 😄	**Inconsistent skills** 😖	⇨	**Simple operations** so that anyone can use even complex technology
Time required to build system (platform)	Faster 😄	**Insufficient time to accept/learn** 😖	⇨	**A framework** for quick acceptance
Number of operators/ system size	Cost reductions 😄	**Increased operational load** 😖	⇨	**Operational load does not increase** even with more devices/systems
Work content	Can respond to various requests 😄	**Higher requirements/ Lower quality** 😖	⇨	**Operational quality can be maintained** even with more diverse and advanced requirements

Operational management solution map made possible with MasterScope



Management

Support for improvement

- Visualize daily work
- Ascertain man-hours
- Improve work quality

MasterScope IT Process Operations

IT process management

- Incident/query management
- Problem/change/release management
- Requirements management

MasterScope IT Process Management

Register incidents

Asset management/ Config info collection

- Asset relational management
- Automatic fetching of inventory info
- Software distribution

MasterScope AssetSuite

Inventory collection

Integrated monitoring

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

MasterScope MISSION CRITICAL OPERATIONS

MasterScope SystemManager

Alert collection

Automation

Cloud management

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

MasterScope Virtual DataCenter Automation

File distribution

- Collective deployment of software

MasterScope DeliveryManager

Job automation

- Batch process flow control
- Scheduled operations

MasterScope JobCenter

Virtual environment management

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

NEC SigmaSystemCenter

Backup

- Data backup
- System protection

BackUpExec
NetBackup
Arcserve Backup etc.

System control

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

（NEC ESMPRO ServerManager）

OS/AP monitoring

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

MasterScope SystemManager

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

- http response monitoring

MasterScope Application Navigator

2. System fault monitoring basics

- Necessity of system fault monitoring

- Types of fault monitoring

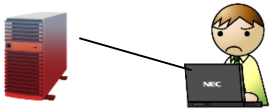
- Case study for troubleshooting

- Implementation of system fault monitoring

What is system fault monitoring?

What is a system fault?

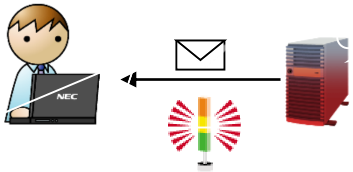
An issue that causes the services provided by IT systems to be suspended, thus making the services unavailable to users.



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.

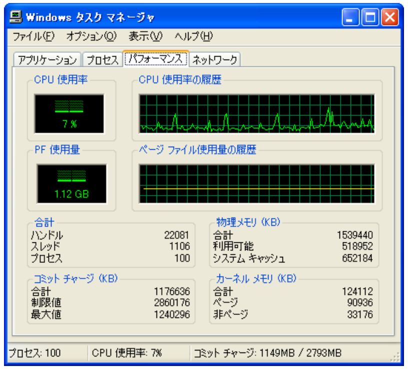
Monitoring tools provide a suite of functions to enable this process.



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


Windows タスク マネージャ
ファイル(F) オプション(O) 表示(V) ヘルプ(H)
アプリケーション プロセス パフォーマンス ネットワーク
CPU 使用率
7 %
CPU 使用率の履歴
PF 使用量
1.12 GB
ページ ファイル使用量の履歴

合計	
ハンドル	22081
スレッド	1106
プロセス	100

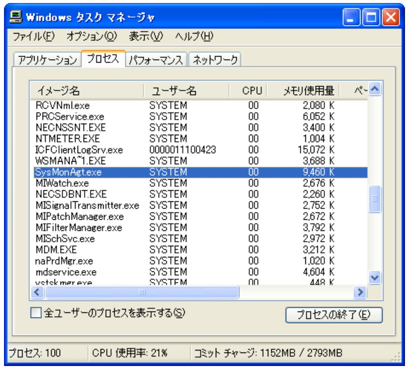
物理メモリ (KB)	
合計	1539440
利用可能	518952
システム キャッシュ	652184

コミット チャージ (KB)	
合計	1176636
制限値	2860176
最大値	1240296

カーネル メモリ (KB)	
合計	124112
ページ	90936
非ページ	33176

プロセス: 100 | CPU 使用率: 7% | コミット チャージ: 1149MB / 2793MB

Check running processes

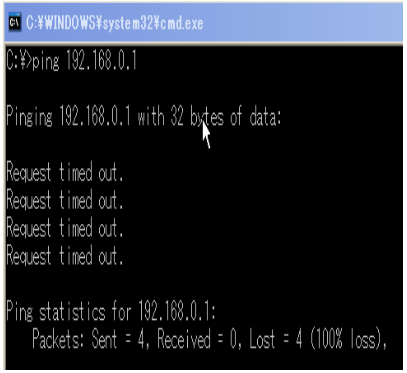

Windows タスク マネージャ
ファイル(F) オプション(O) 表示(V) ヘルプ(H)
アプリケーション プロセス パフォーマンス ネットワーク
プロセスの終了(E)

イメージ名	ユーザー名	CPU	メモリ使用量	ペ-
RCVNml.exe	SYSTEM	00	2,080 K	
PRCService.exe	SYSTEM	00	6,052 K	
NECNSSNT.EXE	SYSTEM	00	3,400 K	
NTMETER.EXE	SYSTEM	00	1,004 K	
ICFClientLogSrv.exe	0000011100423	00	15,072 K	
WSMANA~1.EXE	SYSTEM	00	3,688 K	
SysMonAgt.exe	SYSTEM	00	9,460 K	
MIWatch.exe	SYSTEM	00	2,676 K	
NECSDBNT.EXE	SYSTEM	00	2,260 K	
MISignalTransmitter.exe	SYSTEM	00	2,752 K	
MIPatchManager.exe	SYSTEM	00	2,672 K	
MIFilterManager.exe	SYSTEM	00	3,792 K	
MISchSvc.exe	SYSTEM	00	2,972 K	
MDM.EXE	SYSTEM	00	3,212 K	
naPrdMgr.exe	SYSTEM	00	1,020 K	
mdservice.exe	SYSTEM	00	4,604 K	
vstskmgr.exe	SYSTEM	00	448 K	

☐ 全ユーザーのプロセスを表示する(S)

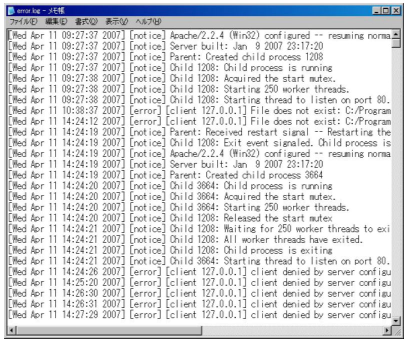
プロセス: 100 | CPU 使用率: 21% | コミット チャージ: 1152MB / 2793MB

Conduct network polling



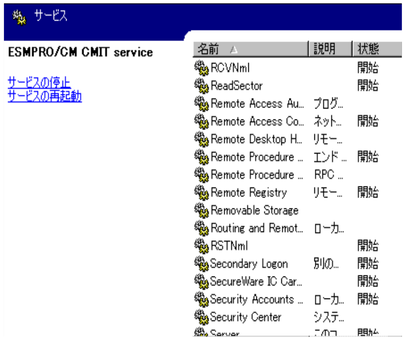
```
C:¥>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Check application logs



```
[Wed Apr 11 09:27:37 2007] [notice] Apache/2.2.4 (Win32) configured -- resuming norma
[Wed Apr 11 09:27:37 2007] [notice] Server built: Jan  9 2007 23:17:20
[Wed Apr 11 09:27:37 2007] [notice] Parent: Created child process 1208
[Wed Apr 11 09:27:37 2007] [notice] Child 1208: Child process is running
[Wed Apr 11 09:27:38 2007] [notice] Child 1208: Acquired the start mutex.
[Wed Apr 11 09:27:38 2007] [notice] Child 1208: Starting 250 worker threads.
[Wed Apr 11 09:27:38 2007] [notice] Child 1208: Starting thread to listen on port 80.
[Wed Apr 11 10:38:37 2007] [error] [client 127.0.0.1] File does not exist: C:/Program
[Wed Apr 11 14:24:12 2007] [error] [client 127.0.0.1] File does not exist: C:/Program
[Wed Apr 11 14:24:19 2007] [notice] Parent: Received restart signal -- Restarting the
[Wed Apr 11 14:24:19 2007] [notice] Child 1208: Exit event signaled. Child process is
[Wed Apr 11 14:24:19 2007] [notice] Apache/2.2.4 (Win32) configured -- resuming norma
[Wed Apr 11 14:24:19 2007] [notice] Server built: Jan  9 2007 23:17:20
[Wed Apr 11 14:24:19 2007] [notice] Parent: Created child process 3664
[Wed Apr 11 14:24:20 2007] [notice] Child 3664: Child process is running
[Wed Apr 11 14:24:20 2007] [notice] Child 3664: Acquired the start mutex.
[Wed Apr 11 14:24:20 2007] [notice] Child 3664: Starting 250 worker threads.
[Wed Apr 11 14:24:20 2007] [notice] Child 1208: Released the start mutex
[Wed Apr 11 14:24:21 2007] [notice] Child 1208: Waiting for 250 worker threads to exi
[Wed Apr 11 14:24:21 2007] [notice] Child 1208: All worker threads have exited.
[Wed Apr 11 14:24:21 2007] [notice] Child 1208: Child process is exiting
[Wed Apr 11 14:24:21 2007] [notice] Child 3664: Starting thread to listen on port 80.
[Wed Apr 11 14:24:26 2007] [error] [client 127.0.0.1] client denied by server configu
[Wed Apr 11 14:25:20 2007] [error] [client 127.0.0.1] client denied by server configu
[Wed Apr 11 14:26:30 2007] [error] [client 127.0.0.1] client denied by server configu
[Wed Apr 11 14:26:31 2007] [error] [client 127.0.0.1] client denied by server configu
[Wed Apr 11 14:27:29 2007] [error] [client 127.0.0.1] client denied by server configu
```

Check running services

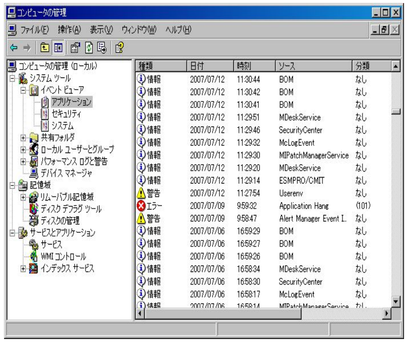


ESMPRO/CM CMIT service

サービスの停止
サービスの再起動

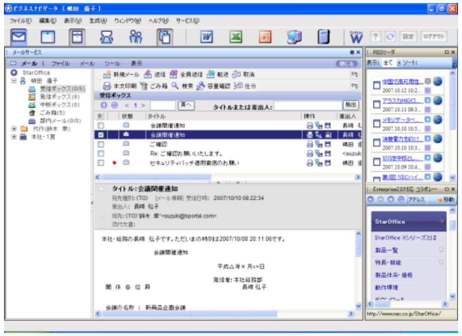
名前	説明	状態
RCVNml		開始
ReadSector		開始
Remote Access Au...	プログ...	
Remote Access Co...	ネット...	開始
Remote Desktop H...	リモー...	
Remote Procedure ...	エンド ...	開始
Remote Procedure ...	RPC ...	
Remote Registry	リモー...	開始
Removable Storage		
Routing and Remot...	ローカ...	
RSTNml		開始
Secondary Logon	別の...	開始
SecureWare IC Car...		開始
Security Accounts ...	ローカ...	開始
Security Center	システ...	
Server	このコ...	開始

Check event logs



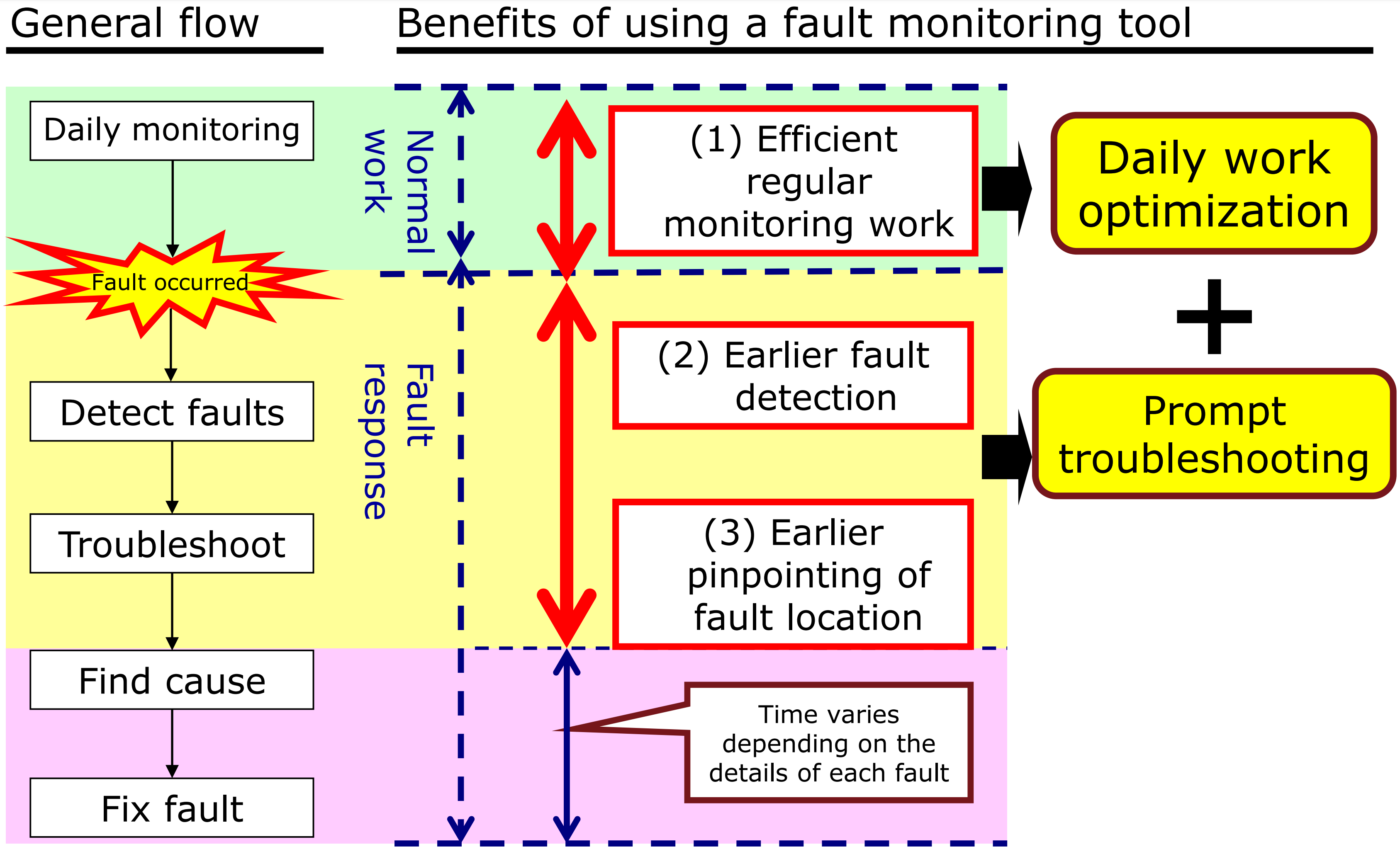
種類	日付	時刻	ソース	分類
情報	2007/07/12	11:30:44	BOM	なし
情報	2007/07/12	11:30:42	BOM	なし
情報	2007/07/12	11:30:41	BOM	なし
情報	2007/07/12	11:29:51	MDeskService	なし
情報	2007/07/12	11:29:46	SecurityCenter	なし
情報	2007/07/12	11:29:32	McLogEvent	なし
情報	2007/07/12	11:29:30	MIPatchManagerService	なし
情報	2007/07/12	11:29:20	MDeskService	なし
情報	2007/07/12	11:29:14	ESMPRO/CMIT	なし
警告	2007/07/12	11:27:54	Userenv	なし
エラー	2007/07/09	9:59:32	Application Hang	(101)
警告	2007/07/09	9:58:47	Alert Manager Event I...	なし
情報	2007/07/06	16:59:29	BOM	なし
情報	2007/07/06	16:59:27	BOM	なし
情報	2007/07/06	16:59:26	BOM	なし
情報	2007/07/06	16:58:34	MDeskService	なし
情報	2007/07/06	16:58:30	SecurityCenter	なし
情報	2007/07/06	16:58:17	McLogEvent	なし
情報	2007/07/06	16:58:14	MIPatchManagerService	なし

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
Benefits of using a fault monitoring tool
Daily monitoring
Fault occurred
Detect faults
Troubleshoot
Find cause
Fix fault
Normal work
Fault response
(1) Efficient regular monitoring work
(2) Earlier fault detection
(3) Earlier pinpointing of fault location
Time varies depending on the details of each fault
Daily work optimization
+
Prompt troubleshooting

2. System fault monitoring basics

- Necessity of system fault monitoring

- Types of fault monitoring

- Case study for troubleshooting

- Implementation of system fault monitoring

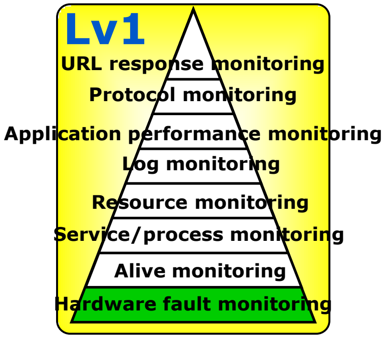
Fault monitoring types and system monitoring levels

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

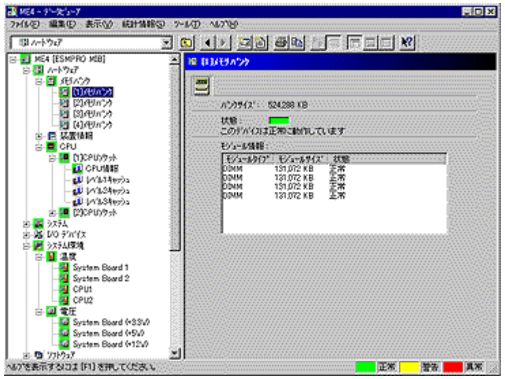
Monitoring layer	Monitoring level and details	Examples of monitoring	Applicable MasterScope product
Service	**Monitoring level 3** **- Service response monitoring** **- App-specific performance monitoring** **- Middleware performance monitoring**	- Monitoring of Web page response time - Monitoring of Oracle table area thresholds	**MasterScope Application Navigator**
App/middle			
OS	**Monitoring level 2** **- Application log monitoring** **- OS system log monitoring** **- Service/process monitoring** **- Resource monitoring**	- Monitoring of virtual platform (VMware vSphere) resources - Alive monitoring for Oracle/business application processes - Application log monitoring - OS resource (CPU, memory, etc.) monitoring	**MasterScope SystemManager**
Virtual platform			
Server	**Monitoring level 1** **- Device fault monitoring** **- Alive monitoring**	- HDD fault monitoring - Temperature monitoring - RAID monitoring - Monitoring of controllers, etc.	**Hardware monitoring by each vendor (linked with software)**
Storage			
Network		- Network device fault - Ping polling	**MasterScope Network Manager**

Overview of fault monitoring (1/5)

Monitoring layer	Image of monitoring	Description



Lv1
URL response monitoring
Protocol monitoring
Application performance monitoring
Log monitoring
Resource monitoring
Service/process monitoring
Alive monitoring
Hardware fault monitoring



ME4 [ESMPRO MIB]
ﾊｰﾄﾞｳｪｱ
ﾒﾓﾘﾊﾞﾝｸ
[1]ﾒﾓﾘﾊﾞﾝｸ
[2]ﾒﾓﾘﾊﾞﾝｸ
[3]ﾒﾓﾘﾊﾞﾝｸ
[4]ﾒﾓﾘﾊﾞﾝｸ
装置情報
CPU
[1]CPUﾕﾆｯﾄ
CPU情報
ﾚﾍﾞﾙ1ｷｬｯｼｭ
ﾚﾍﾞﾙ2ｷｬｯｼｭ
ﾚﾍﾞﾙ3ｷｬｯｼｭ
[2]CPUﾕﾆｯﾄ
ｼｽﾃﾑ
I/O ﾃﾞﾊﾞｲｽ
ｼｽﾃﾑ環境
温度
System Board 1
System Board 2
CPU1
CPU2
電圧
System Board (+3.3V)
System Board (+5V)
System Board (+12V)
ｿﾌﾄｳｪｱ

[1]ﾒﾓﾘﾊﾞﾝｸ

ﾊﾞﾝｸｻｲｽﾞ: 524288 KB

状態: 🟩
このﾃﾞﾊﾞｲｽは正常に動作しています

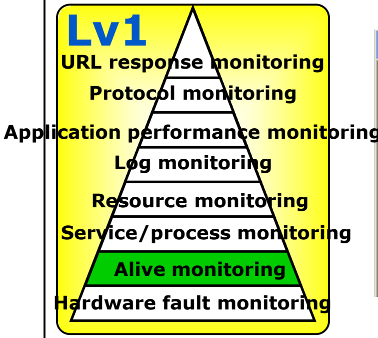
ﾓｼﾞｭｰﾙ情報:

ﾓｼﾞｭｰﾙﾀｲﾌﾟ	ﾓｼﾞｭｰﾙｻｲｽﾞ	状態
DIMM	131,072 KB	正常
DIMM	131,072 KB	正常
DIMM	131,072 KB	正常
DIMM	131,072 KB	正常

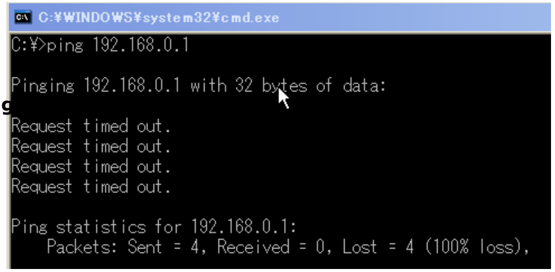
ﾍﾙﾌﾟを表示するには [F1] を押してください。

🟩 正常 🟨 警告 🟥 異常

Hardware faults (disk, fans, etc.) are monitored by tools provided by hardware vendors.
Express Servers are monitored by NEC ESMPRO/ServerManager and ServerAgentService.



Lv1
URL response monitoring
Protocol monitoring
Application performance monitoring
Log monitoring
Resource monitoring
Service/process monitoring
Alive monitoring
Hardware fault monitoring

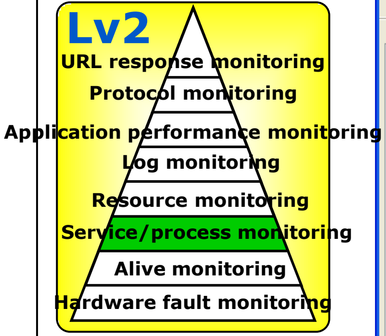


```
C:¥>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

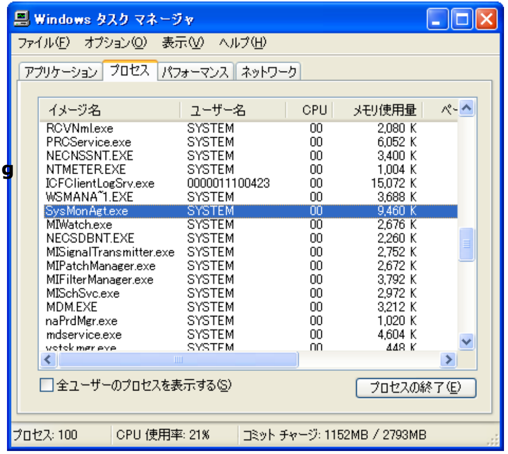
Ping (ICMP) is used to confirm network communication between monitored servers and network devices.

Overview of fault monitoring (2/5)

Monitoring layer | **Image of monitoring** | **Description**



Process monitoring


Windows タスク マネージャ
ファイル(F) オプション(O) 表示(V) ヘルプ(H)
アプリケーション
プロセス
パフォーマンス
ネットワーク
□ 全ユーザーのプロセスを表示する(S)
プロセスの終了(E)

イメージ名	ユーザー名	CPU	メモリ使用量	ペ-
RCVNml.exe	SYSTEM	00	2,080 K	
PRCService.exe	SYSTEM	00	6,052 K	
NECNSSNT.EXE	SYSTEM	00	3,400 K	
NTMETER.EXE	SYSTEM	00	1,004 K	
ICFClientLogSrv.exe	0000011100423	00	15,072 K	
WSMANA~1.EXE	SYSTEM	00	3,688 K	
SysMonAgt.exe	SYSTEM	00	9,460 K	
MIWatch.exe	SYSTEM	00	2,676 K	
NECSDBNT.EXE	SYSTEM	00	2,260 K	
MISignalTransmitter.exe	SYSTEM	00	2,752 K	
MIPatchManager.exe	SYSTEM	00	2,672 K	
MIFilterManager.exe	SYSTEM	00	3,792 K	
MISchSvc.exe	SYSTEM	00	2,972 K	
MDM.EXE	SYSTEM	00	3,212 K	
naPrdMgr.exe	SYSTEM	00	1,020 K	
mdservice.exe	SYSTEM	00	4,604 K	
vstskmgr.exe	SYSTEM	00	448 K	

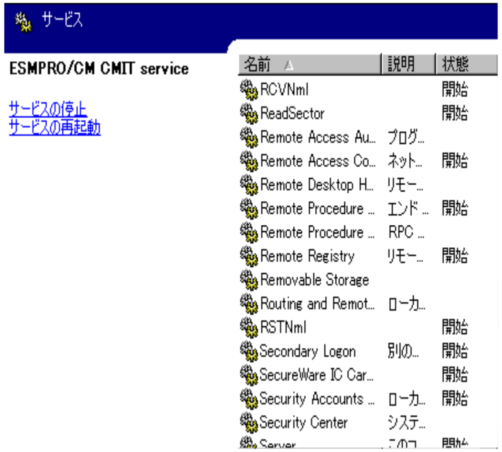
プロセス: 100　CPU 使用率: 21%　コミット チャージ: 1152MB / 2793MB

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



ESMPRO/CM CMIT service

名前	説明	状態
RCVNml		開始
ReadSector		開始
Remote Access Au...	プログ...	
Remote Access Co...	ネット...	開始
Remote Desktop H...	リモー...	
Remote Procedure ...	エンド ...	開始
Remote Procedure ...	RPC ...	
Remote Registry	リモー...	開始
Removable Storage		
Routing and Remot...	ローカ...	
RSTNml		開始
Secondary Logon	別の...	開始
SecureWare IC Car...		開始
Security Accounts ...	ローカ...	開始
Security Center	システ...	
Server	このコ...	開始

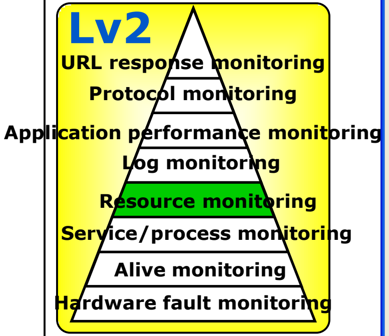
Statuses of services to be provided are monitored. This monitoring is very important because the stoppage of services could directly cause operations to stop.

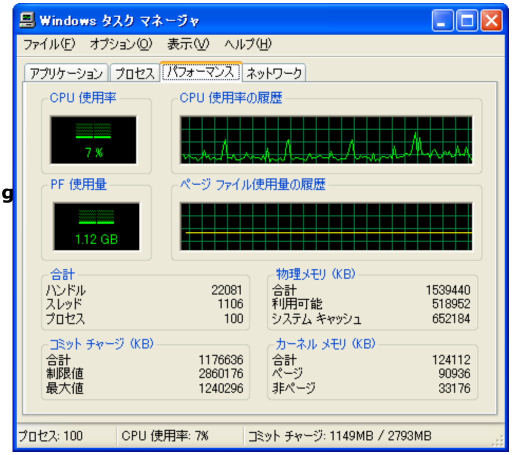
Key point

Services that need to be always running are monitored.

Overview of fault monitoring (3/5)

Monitoring layer | **Image of monitoring** | **Description**


Lv2
URL response monitoring
Protocol monitoring
Application performance monitoring
Log monitoring
Resource monitoring
Service/process monitoring
Alive monitoring
Hardware fault monitoring


Windows タスク マネージャ
ファイル(F) オプション(O) 表示(V) ヘルプ(H)
アプリケーション プロセス パフォーマンス ネットワーク
CPU 使用率
7 %
CPU 使用率の履歴
PF 使用量
1.12 GB
ページ ファイル使用量の履歴

合計
ハンドル 22081
スレッド 1106
プロセス 100

物理メモリ (KB)
合計 1539440
利用可能 518952
システム キャッシュ 652184

コミット チャージ (KB)
合計 1176636
制限値 2860176
最大値 1240296

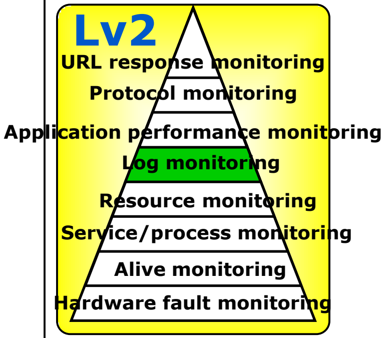
カーネル メモリ (KB)
合計 124112
ページ 90936
非ページ 33176

プロセス: 100 CPU 使用率: 7% コミット チャージ: 1149MB / 2793MB

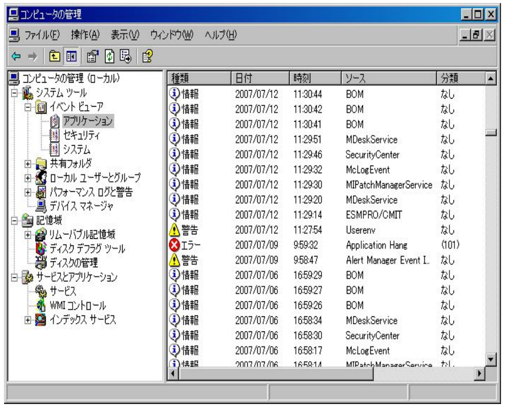
Threshold values for CPU load and memory/disk free space are used for monitoring. Resource faults need to be monitored regularly because they may degrade performance and cause operations to stop.

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.


Lv2
URL response monitoring
Protocol monitoring
Application performance monitoring
Log monitoring
Resource monitoring
Service/process monitoring
Alive monitoring
Hardware fault monitoring

Event logs



種類	日付	時刻	ソース	分類
情報	2007/07/12	11:30:44	BOM	なし
情報	2007/07/12	11:30:42	BOM	なし
情報	2007/07/12	11:30:41	BOM	なし
情報	2007/07/12	11:29:51	MDeskService	なし
情報	2007/07/12	11:29:46	SecurityCenter	なし
情報	2007/07/12	11:29:32	McLogEvent	なし
情報	2007/07/12	11:29:30	MIPatchManagerService	なし
情報	2007/07/12	11:29:20	MDeskService	なし
情報	2007/07/12	11:29:14	ESMPRO/CMIT	なし
警告	2007/07/12	11:27:54	Userenv	なし
エラー	2007/07/09	9:59:32	Application Hang	(101)
警告	2007/07/09	9:58:47	Alert Manager Event I..	なし
情報	2007/07/06	16:59:29	BOM	なし
情報	2007/07/06	16:59:27	BOM	なし
情報	2007/07/06	16:59:26	BOM	なし
情報	2007/07/06	16:58:34	MDeskService	なし
情報	2007/07/06	16:58:30	SecurityCenter	なし
情報	2007/07/06	16:58:17	McLogEvent	なし
情報	2007/07/06	16:58:14	MIPatchManagerService	なし

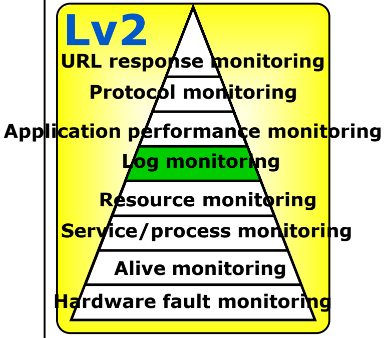
Windows OS logs are used as event logs.
Logs to be monitored can be filtered based on attributes such as the event type (error, warning, etc.), source name, and event ID.

Key point

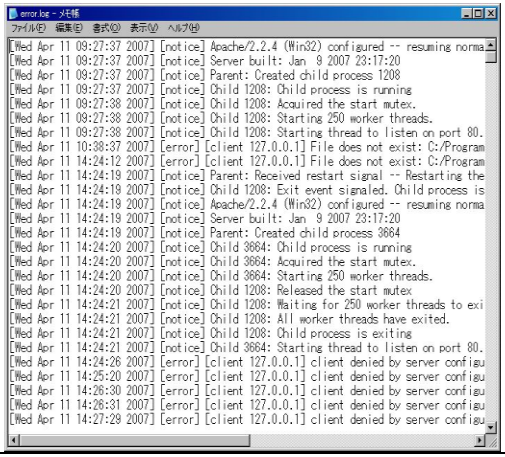
- It is important to clarify which logs need to be monitored since various application logs are output as event logs.
- Note that if all the logs are monitored, operator workloads will increase due to the large number of messages.

Overview of fault monitoring (4/5)

Monitoring layer	Image of monitoring	Description



Text log / syslog

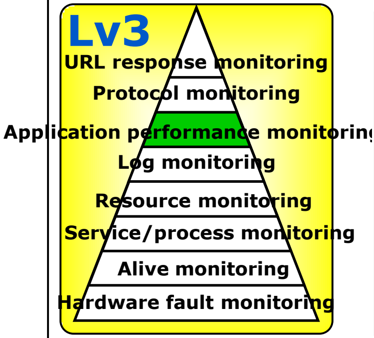


```
[Wed Apr 11 09:27:37 2007] [notice] Apache/2.2.4 (Win32) configured -- resuming norma
[Wed Apr 11 09:27:37 2007] [notice] Server built: Jan  9 2007 23:17:20
[Wed Apr 11 09:27:37 2007] [notice] Parent: Created child process 1208
[Wed Apr 11 09:27:37 2007] [notice] Child 1208: Child process is running
[Wed Apr 11 09:27:38 2007] [notice] Child 1208: Acquired the start mutex.
[Wed Apr 11 09:27:38 2007] [notice] Child 1208: Starting 250 worker threads.
[Wed Apr 11 09:27:38 2007] [notice] Child 1208: Starting thread to listen on port 80.
[Wed Apr 11 10:38:37 2007] [error] [client 127.0.0.1] File does not exist: C:/Program
[Wed Apr 11 14:24:12 2007] [error] [client 127.0.0.1] File does not exist: C:/Program
[Wed Apr 11 14:24:19 2007] [notice] Parent: Received restart signal -- Restarting the
[Wed Apr 11 14:24:19 2007] [notice] Child 1208: Exit event signaled. Child process is
[Wed Apr 11 14:24:19 2007] [notice] Apache/2.2.4 (Win32) configured -- resuming norma
[Wed Apr 11 14:24:19 2007] [notice] Server built: Jan  9 2007 23:17:20
[Wed Apr 11 14:24:19 2007] [notice] Parent: Created child process 3664
[Wed Apr 11 14:24:20 2007] [notice] Child 3664: Child process is running
[Wed Apr 11 14:24:20 2007] [notice] Child 3664: Acquired the start mutex.
[Wed Apr 11 14:24:20 2007] [notice] Child 3664: Starting 250 worker threads.
[Wed Apr 11 14:24:20 2007] [notice] Child 1208: Released the start mutex
[Wed Apr 11 14:24:21 2007] [notice] Child 1208: Waiting for 250 worker threads to exi
[Wed Apr 11 14:24:21 2007] [notice] Child 1208: All worker threads have exited.
[Wed Apr 11 14:24:21 2007] [notice] Child 1208: Child process is exiting
[Wed Apr 11 14:24:21 2007] [notice] Child 3664: Starting thread to listen on port 80.
[Wed Apr 11 14:24:26 2007] [error] [client 127.0.0.1] client denied by server configu
[Wed Apr 11 14:25:20 2007] [error] [client 127.0.0.1] client denied by server configu
[Wed Apr 11 14:26:30 2007] [error] [client 127.0.0.1] client denied by server configu
[Wed Apr 11 14:26:31 2007] [error] [client 127.0.0.1] client denied by server configu
[Wed Apr 11 14:27:29 2007] [error] [client 127.0.0.1] client denied by server configu
```

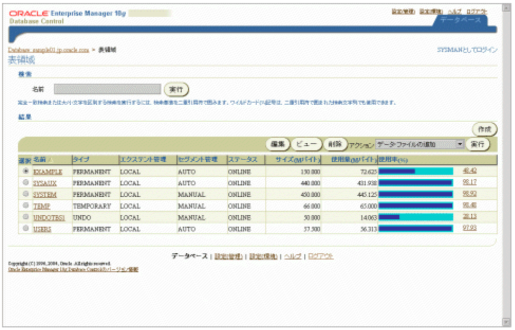
Logs can be viewed in text format.
Log contents matching keywords are monitored.

Key point

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



Example of Oracle performance screen



Database: sample01.jp.oracle.com > 表領域

表領域

検索

名前 実行

完全一致検索または大/小文字を区別する検索を実行するには、検索語を二重引用符で囲みます。ワイルドカード(%)記号は、二重引用符で囲まれた検索文字列でも使用できます。

結果

選択	名前△	タイプ	エクステント管理	セグメント管理	ステータス	サイズ(Mバイト)	使用量(Mバイト)	使用率(%)
●	EXAMPLE	PERMANENT	LOCAL	AUTO	ONLINE	150.000	72.625	48.42
○	SYSAUX	PERMANENT	LOCAL	AUTO	ONLINE	440.000	431.938	98.17
○	SYSTEM	PERMANENT	LOCAL	MANUAL	ONLINE	450.000	445.125	98.92
○	TEMP	TEMPORARY	LOCAL	MANUAL	ONLINE	66.000	65.000	98.48
○	UNDOTBS1	UNDO	LOCAL	MANUAL	ONLINE	50.000	14.063	28.13
○	USERS	PERMANENT	LOCAL	AUTO	ONLINE	57.500	56.313	97.93

データベース | 設定(管理) | 設定(環境) | ヘルプ | ログアウト

Copyright (C) 1996, 2004, Oracle. All rights reserved.
Oracle Enterprise Manager 10g Database Controlのバージョン情報

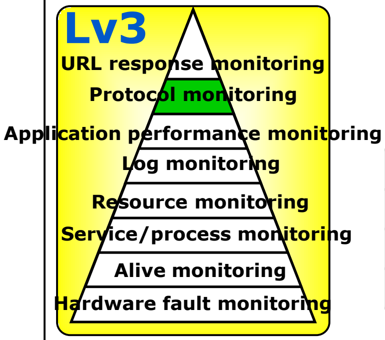
For database servers, the instance startup status, table area free space, number of sessions, and other DB-specific performance items are monitored based on threshold values.
For application servers, the heap memory capacity, number of garbage collections, and other performance items are monitored based 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 | **Image of monitoring** | **Description**



Lv3
URL response monitoring
Protocol monitoring
Application performance monitoring
Log monitoring
Resource monitoring
Service/process monitoring
Alive monitoring
Hardware fault monitoring

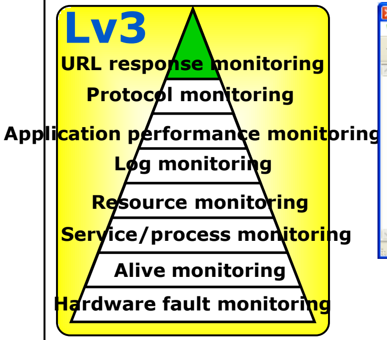
Example of monitoring

Http/Https	Check connectivity via http
Email	Check SMTP/POP requests
FTP	Get files from FTP servers
Port	Check port connectivity

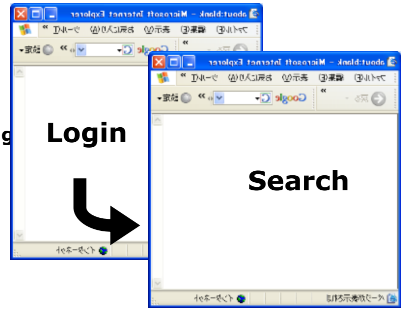
Check whether services are available using specific protocols.

Key point

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



Lv3
URL response monitoring
Protocol monitoring
Application performance monitoring
Log monitoring
Resource monitoring
Service/process monitoring
Alive monitoring
Hardware fault monitoring



How many seconds?

Response times of Web systems are monitored based on threshold values.
Response can be measured from an end user perspective.

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

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

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?**

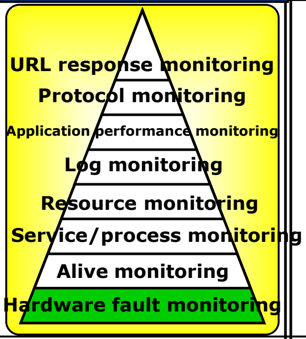
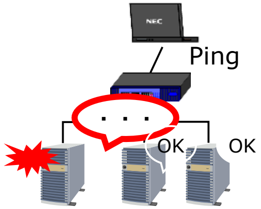
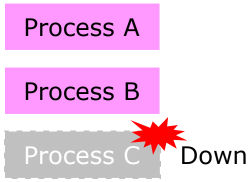
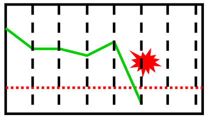
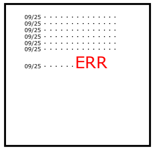
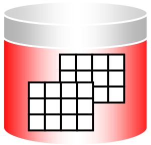
etc.

➡ **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.

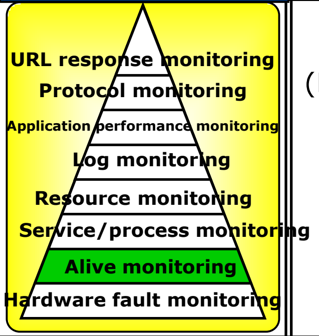
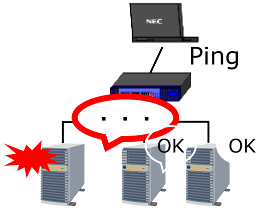
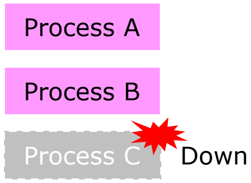
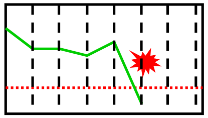
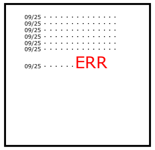
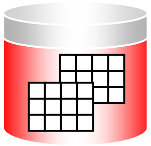
Case 1. Hardware fault monitoring

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

Monitoring level	Fault details					
 URL response monitoring Protocol monitoring Application performance monitoring Log monitoring Resource monitoring Service/process monitoring Alive monitoring Hardware fault monitoring	Disk fault (Hardware fault) 	Network disconnection  	Process down (Service down)  	Resource fault 	Error log  Log file	Application performance (e.g. database) 
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. √/- Different 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.**					

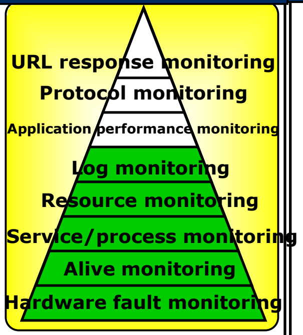
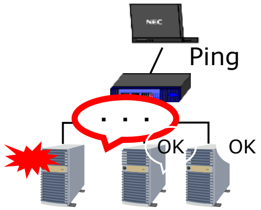
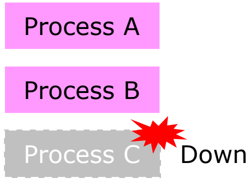
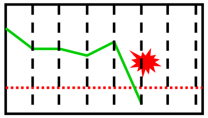
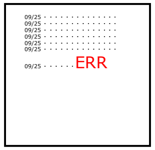
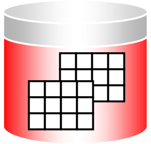
Case 2. Alive monitoring by ping

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

Monitoring level	Fault details					
 URL response monitoring Protocol monitoring Application performance monitoring Log monitoring Resource monitoring Service/process monitoring Alive monitoring Hardware fault monitoring	Disk fault (Hardware fault) 	Network disconnection 	Process down (Service down) 	Resource fault 	Error log  Log file	Application performance (e.g. database) 
Detection/ Troubleshooting	-	✓	-	-	-	-
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.					

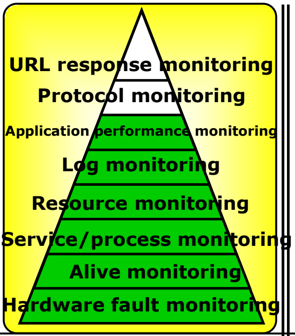
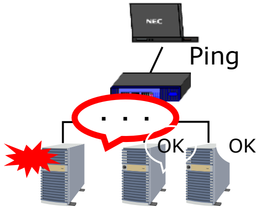
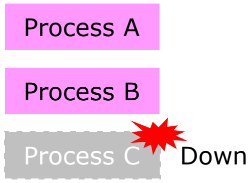
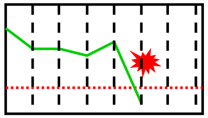
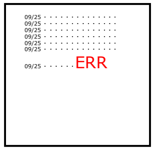
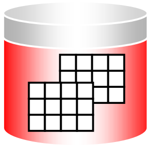
Case 3. Including server monitoring

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

Monitoring level	Fault details					
 URL response monitoring Protocol monitoring Application performance monitoring Log monitoring Resource monitoring Service/process monitoring Alive monitoring Hardware fault monitoring	Disk fault (Hardware fault) 	Network disconnection 	Process down (Service down) 	Resource fault 	Error log  Log file	Application performance (e.g. database) 
Detection/ Troubleshooting	✓	✓	✓	✓	✓	-
Key points	✓ 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

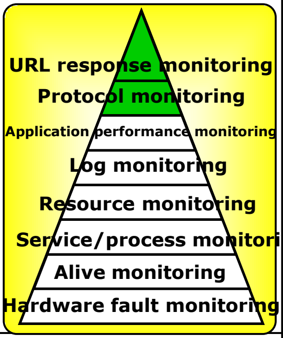
This configuration is normally used for advanced monitoring including monitoring of middleware performance (databases, application servers, and Web servers).

Monitoring level	Fault details					
 URL response monitoring Protocol monitoring Application performance monitoring Log monitoring Resource monitoring Service/process monitoring Alive monitoring Hardware fault monitoring	Disk fault (Hardware fault) 	Network disconnection 	Process down (Service down)  Process A Process B Process C Down	Resource fault 	Error log  09/25 ・・・・・・・・・・・・・・ 09/25 ・・・・・・・・・・・・・・ 09/25 ・・・・・・・・・・・・・・ 09/25 ・・・・・・・・・・・・・・ 09/25 ・・・・・・・・・・・・・・ 09/25 ・・・・・・・・・・・・・・ 09/25 ・・・・・・ERR Log file	Application performance (e.g. database) 
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.

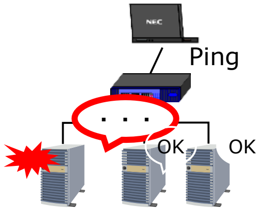
Monitoring level


URL response monitoring
Protocol monitoring
Application performance monitoring
Log monitoring
Resource monitoring
Service/process monitoring
Alive monitoring
Hardware fault monitoring

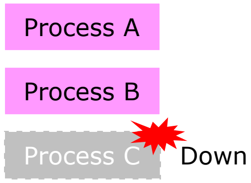
Fault details

Disk fault (Hardware fault)

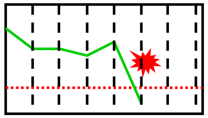
Network disconnection



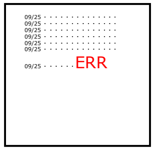
Process down (Service down)



Resource fault

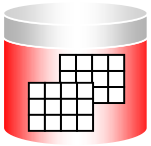


Error log



Log file

Application performance (e.g. database)



Detection/ Troubleshooting

Service level fault detection is possible

Notes

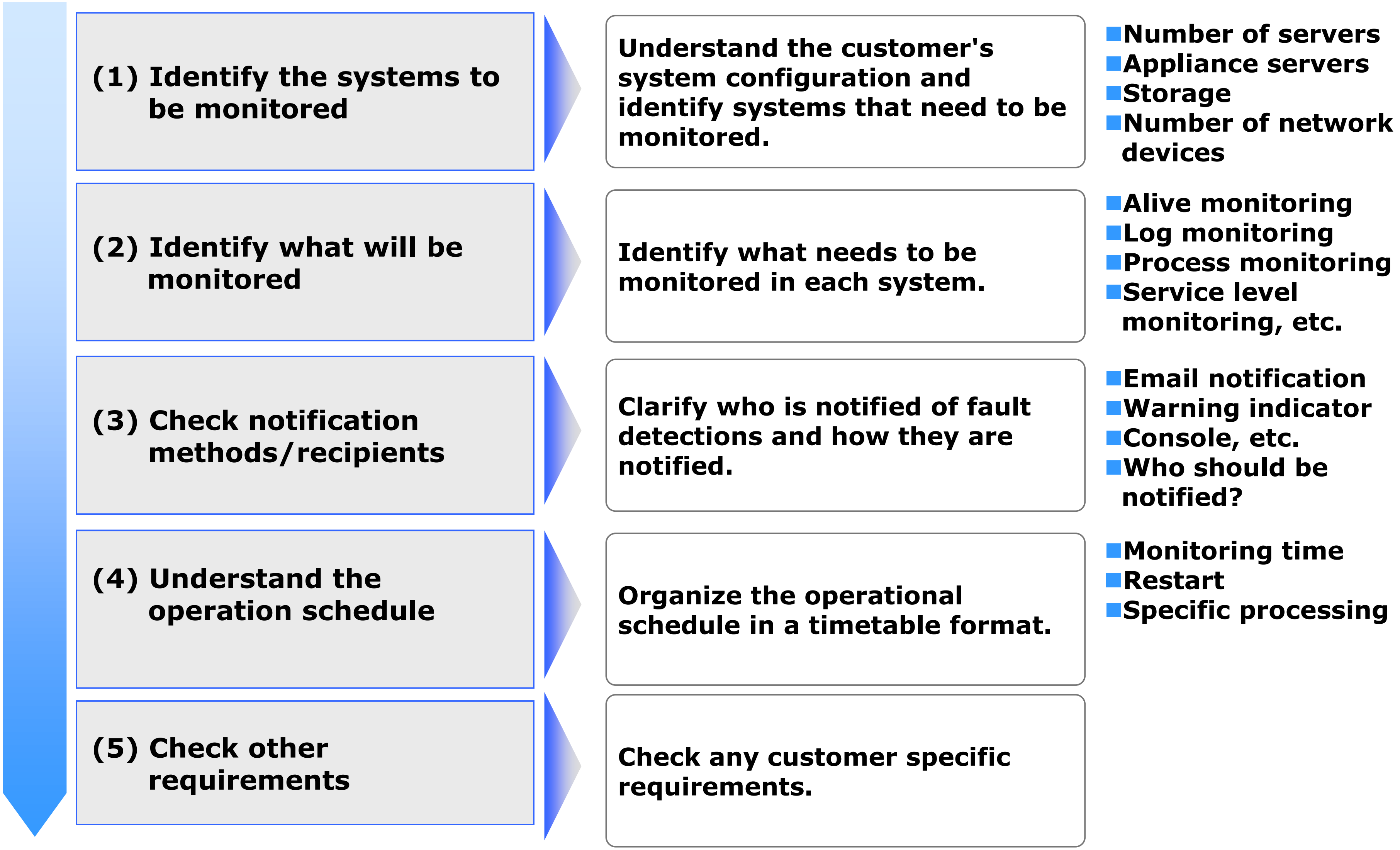
- ✓ Monitoring is possible without installing an agent on the server.
- √/- System faults and slow responses can be detected but troubleshooting is difficult.
- √/- Not all systems can be monitored (systems that do not support relevant protocols cannot be monitored).

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.**	■**Number of servers** ■**Appliance servers** ■**Storage** ■**Number of network devices**
(2) Identify what will be monitored	**Identify what needs to be monitored in each system.**	■**Alive monitoring** ■**Log monitoring** ■**Process monitoring** ■**Service level monitoring, etc.**
(3) Check notification methods/recipients	**Clarify who is notified of fault detections and how they are notified.**	■**Email notification** ■**Warning indicator** ■**Console, etc.** ■**Who should be notified?**
(4) Understand the operation schedule	**Organize the operational schedule in a timetable format.**	■**Monitoring time** ■**Restart** ■**Specific processing**
(5) Check other requirements	**Check any customer specific requirements.**	

(1) Identify the systems to be monitored

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

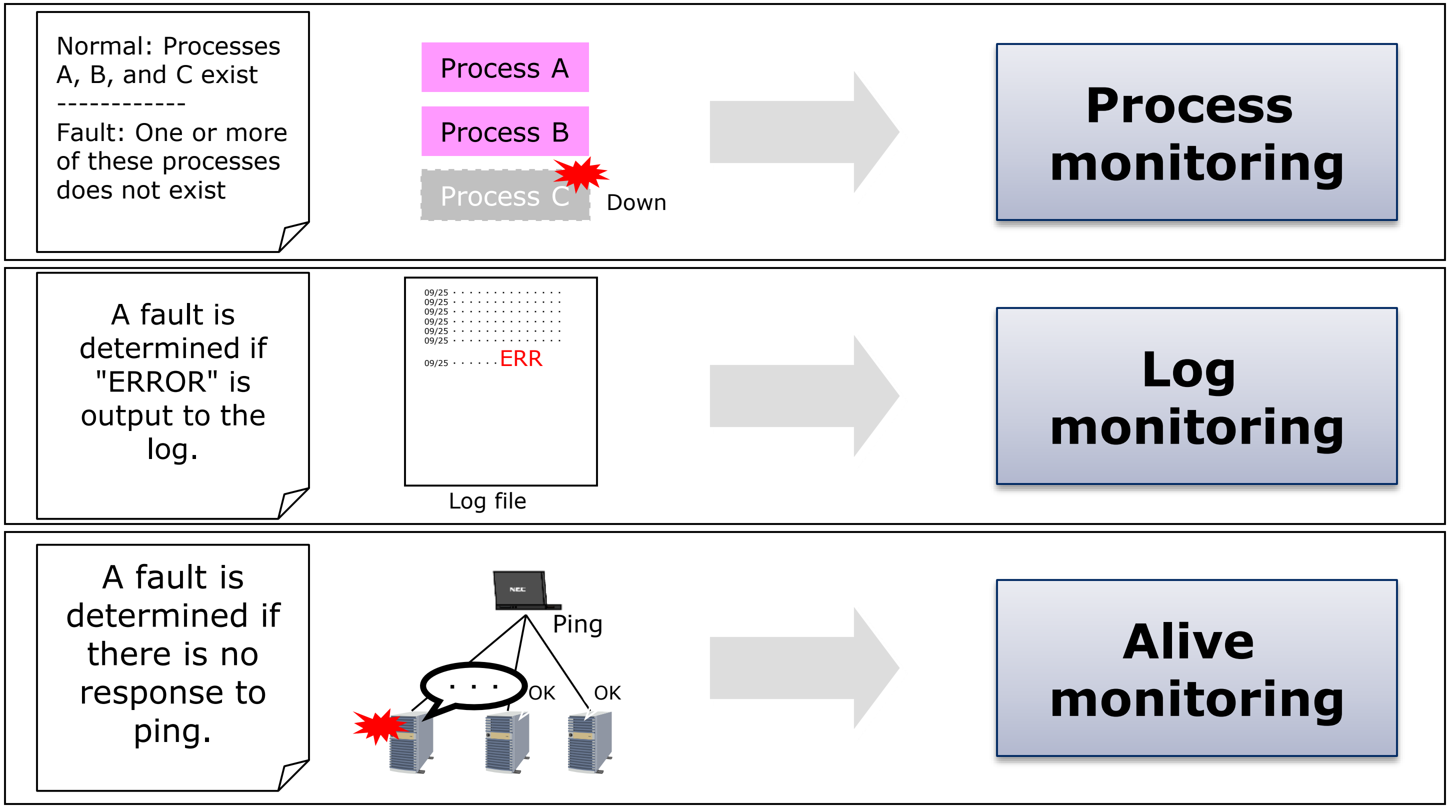
System name	Host name	Model	OS	…
DB	SV1	Express5800/120Rj-2	Windows 2012 R2	
Email	SV2	Express5800/120Rj-2	Windows 2012 R2	
Report	SV3	Express5800/110Ri-2	Windows 2012 R2	
Batch	SV4	Express5800/120Rj-2	Windows 2012 R2	
EDI	SV5	Express5800/120Rj-2	Windows 2012 R2	
ERP	SV6	Express5800/120Rj-2	Windows 2012 R2	
Operational management	SV7	Express5800/120Rj-2	Windows 2012 R2	
Other	SV8	Express5800/1**	Windows 2008 R2	
Other	SV9	Express5800/1**	Windows 2008 R2	
Other	SV10	Express5800/1**	Windows 2008 R2	

(2) 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

Monitored items



Normal: Processes A, B, and C exist

Fault: One or more of these processes does not exist

Process monitoring

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

```
09/25 · · · · · · · · · · · · · ·
09/25 · · · · · · · · · · · · · ·
09/25 · · · · · · · · · · · · · ·
09/25 · · · · · · · · · · · · · ·
09/25 · · · · · · · · · · · · · ·
09/25 · · · · · · · · · · · · · ·

09/25 · · · · · ·ERR
```

Log monitoring

A fault is determined if there is no response to ping.

Alive monitoring

(2) Identify what should be monitored (2/2)

Organize current and future monitoring targets for each system.

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

◎: Should be monitored in the future, ●: Currently monitored,
- : No need to be monitored, △: Should be improved or discontinued

(3) Check notification methods/recipients(1/2)

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

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

(3) Check notification methods/recipients (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

System name	Model	OS	Recipient
DB	Express5800/120Rj-2	Windows 2012 R2	Administrator A
Email	Express5800/120Rj-2	Windows 2012 R2	Administrator B
Report	Express5800/110Ri-2	Windows 2012 R2	Administrator A
EIP	Express5800/120Rj-2	Windows 2012 R2	Administrator A
EDI	Express5800/120Rj-2	Windows 2008 R2	Administrator A
ERP	Express5800/120Rj-2	Windows 2008 R2	Administrator A
Operational management	Express5800/120Rj-2	Windows 2008 R2	Administrator B

(4) Understand the operation schedule

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

Daily schedule		6:00						12:00						18:00						24:00					
	Time restart	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5
DB	✓		🟨	🟨					🟨							🟨				Job	🟩	Re			
Email	—		🟨	🟨					🟨							🟨									
Report	—		🟨	🟨					🟨							🟨									
Job	—		🟨	🟨					🟨							🟨									
EDI	✓		🟨	🟨					🟨							🟨					Job	🟩	Re		
ERP	✓		🟨	🟨					🟨							🟨						Job	🟩	Re	
Operation / management	—		🟨	🟨					🟨							🟨									
Other	—		🟨	🟨					🟨							🟨									
Other	—		🟨	🟨					🟨							🟨									
Other	—		🟨	🟨					🟨							🟨									

- Check job execution results
- Check backup results
- Check application status
- Check performance status

🟨 Time when system is monitored manually

🟩 Specific processing is executed

🟥 System stop (restart) time

(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

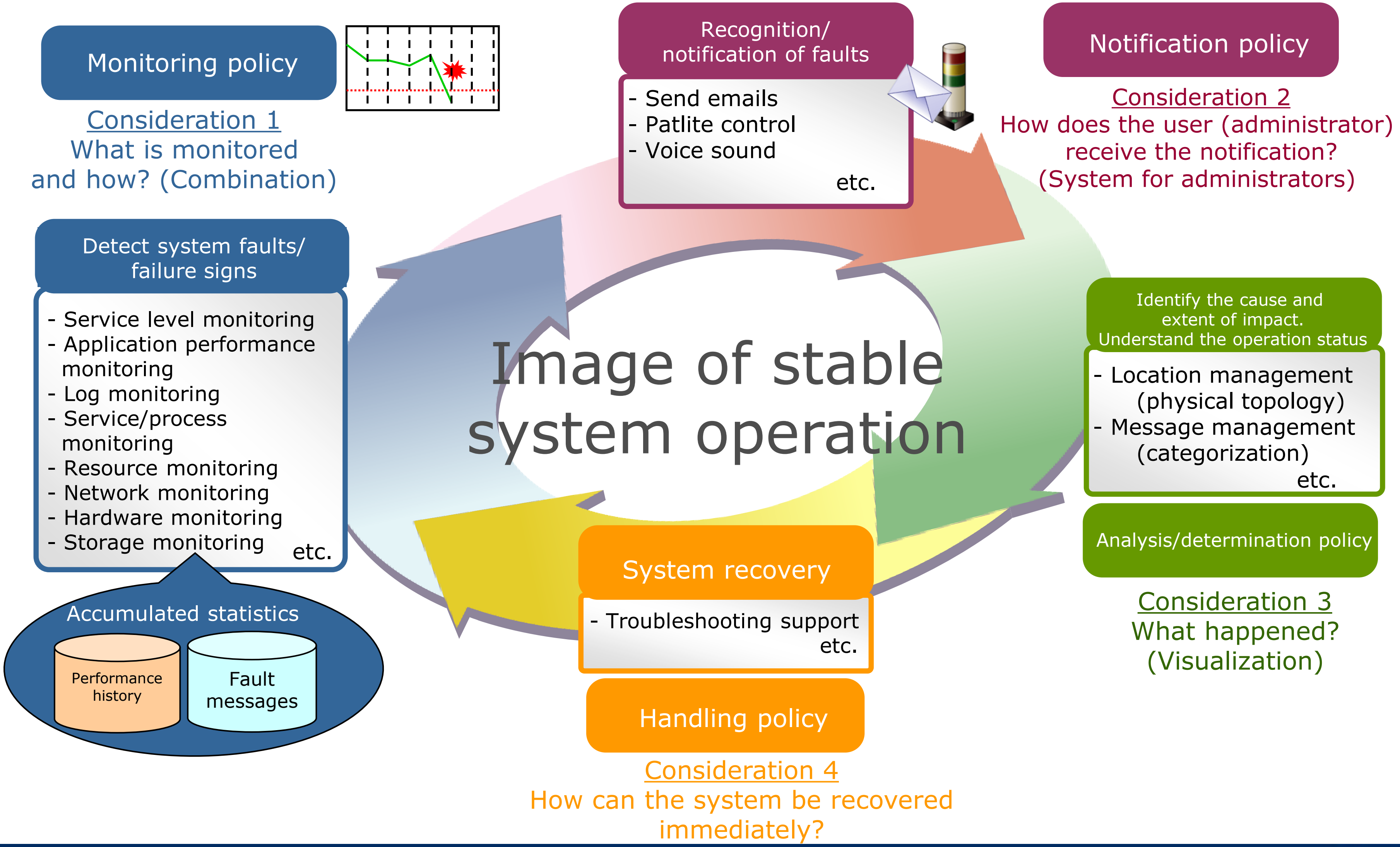


Image of stable system operation

Monitoring policy

Consideration 1
What is monitored and how? (Combination)

Detect system faults/ failure signs

- Service level monitoring
- Application performance monitoring
- Log monitoring
- Service/process monitoring
- Resource monitoring
- Network monitoring
- Hardware monitoring
- Storage monitoring

etc.

Accumulated statistics

Recognition/ notification of faults

- Send emails
- Patlite control
- Voice sound

etc.

Notification policy

Consideration 2
How does the user (administrator) receive the notification? (System for administrators)

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

- Location management (physical topology)
- Message management (categorization)

etc.

Analysis/determination policy

Consideration 3
What happened? (Visualization)

System recovery

- Troubleshooting support

etc.

Handling policy

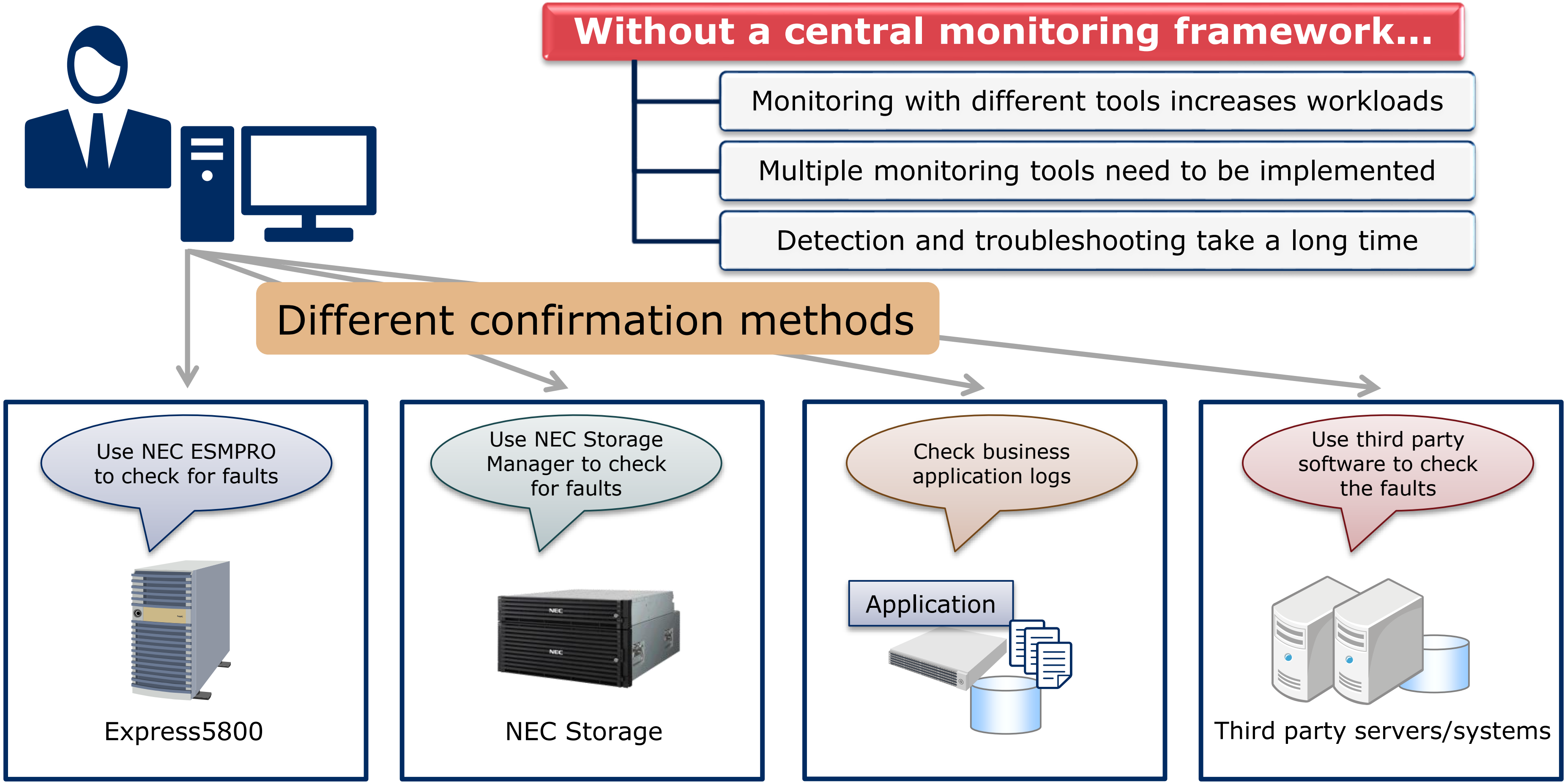
Consideration 4
How can the system be recovered immediately?

3. Benefits of utilizing MasterScope central monitoring for users of NEC ESMPRO

Issues when system faults cannot be centrally monitored

Before

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 ESMPRO to check for faults

Express5800

Use NEC Storage Manager to check for faults

NEC Storage

Check business application logs

Application

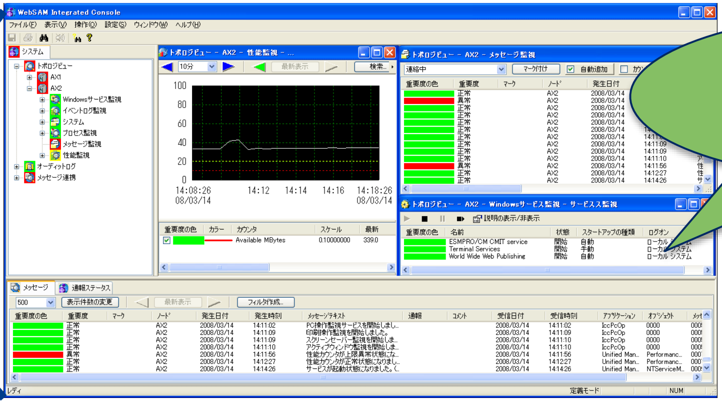
Use third party software to check the faults

Third party servers/systems

Advantages of central monitoring for system faults

After

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



WebSAM Integrated Console

重要度の色	カラー	カウンタ	スケール	最新
☑ 🟩	—	Available MBytes	0.10000000	339.0

トポロジビュー － AX2 － メッセージ監視

重要度の色	重要度	マーク	ノード	発生日付
🟩	正常		AX2	2008/03/14
🟥	異常		AX2	2008/03/14
🟩	正常		AX2	2008/03/14
🟩	正常		AX2	2008/03/14
🟩	正常		AX2	2008/03/14
🟩	正常		AX2	2008/03/14
🟩	正常		AX2	2008/03/14
🟩	正常		AX2	2008/03/14
🟩	正常		AX2	2008/03/14
🟩	正常		AX2	2008/03/14
🟥	異常		AX2	2008/03/14
🟩	正常		AX2	2008/03/14
🟩	正常		AX2	2008/03/14

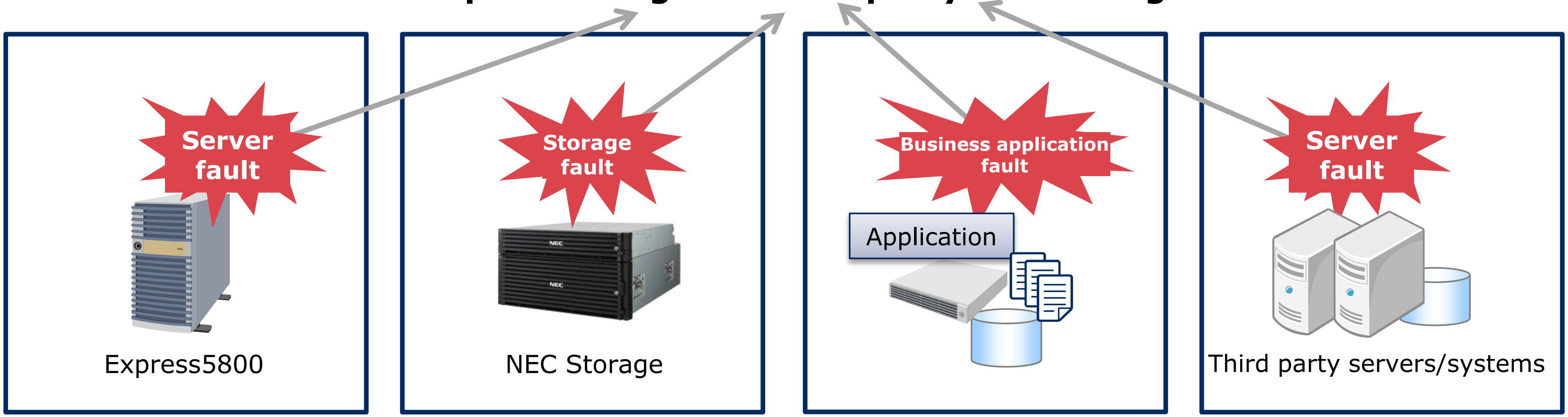
トポロジビュー － AX2 － Windowsサービス監視 － サービス監視

重要度の色	名前	状態	スタートアップの種類	ログオン
🟩	ESMPRO/CM CMIT service	開始	自動	ローカル システム
🟩	Terminal Services	開始	手動	ローカル システム
🟩	World Wide Web Publishing	開始	自動	ローカル システム

重要度の色	重要度	マーク	ノード	発生日付	発生時刻	メッセージテキスト	通報	コメント	受信日付	受信時刻	アプリケーション	オブジェクト	メッセ
🟩	正常		AX2	2008/03/14	14:11:02	PC操作監視サービスを開始しまし…			2008/03/14	14:11:02	IccPcOp	0000	000!
🟩	正常		AX2	2008/03/14	14:11:09	印刷操作監視を開始しました。			2008/03/14	14:11:09	IccPcOp	0000	000!
🟩	正常		AX2	2008/03/14	14:11:09	スクリーンセーバー監視を開始しま…			2008/03/14	14:11:10	IccPcOp	0000	000!
🟩	正常		AX2	2008/03/14	14:11:10	アクティブウィンドウ監視を開始しま…			2008/03/14	14:11:10	IccPcOp	0000	000!
🟥	異常		AX2	2008/03/14	14:11:56	性能カウンタが上限異常状態にな…			2008/03/14	14:11:56	Unified Man…	Performanc…	000
🟩	正常		AX2	2008/03/14	14:12:27	性能カウンタが正常状態になりまし…			2008/03/14	14:12:27	Unified Man…	Performanc…	000
🟩	正常		AX2	2008/03/14	14:14:26	サービスが起動状態になりました。(…			2008/03/14	14:14:26	Unified Man…	NTServiceM…	000!

Central monitoring enables quick detection of system faults

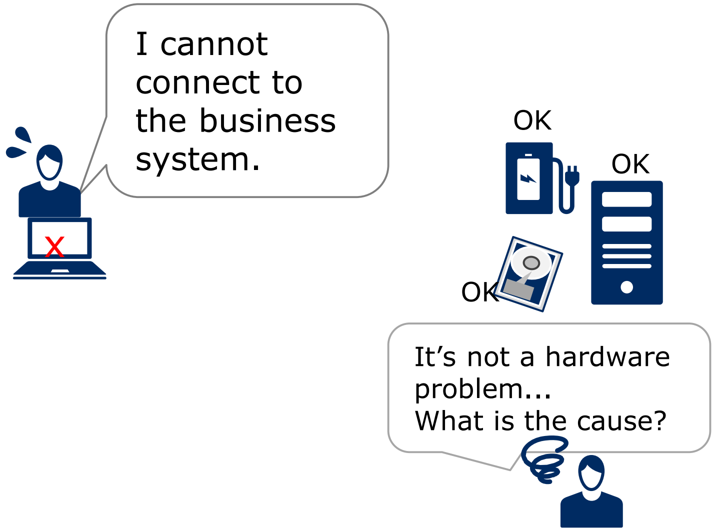
Example of using MasterScope SystemManager



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

Points to confirm

- Process down
- Application errors
- Resources
- Application performance

Requires skilled operators who can use their own knowledge to identify the cause...

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.

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.

Monitoring	MasterScope SystemManager		NEC ESMPRO	
Hardware faults	—	• 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).	○	Available
System logs (Event logs, syslogs)	◎	• Monitored servers can be configured in the View. • Advanced monitoring settings are available such as keyword-based text filtering.	○	• Monitoring settings are configured in NEC ESMPRO/SAS and SA on monitored servers. • For Windows servers, monitoring is configured based on the source and event ID (keywords are available for Linux).
Text logs	○	• Application logs in text format are filtered by keywords for monitoring.	x	Not available
Processes/services	○	• Alive monitoring for application processes (for Windows services, startup is also monitored)	x	Not available
Resources	◎	• 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.**	○	• Thresholds for CPU/memory usage* and disk space can be used for monitoring. Note: For SAS, memory usage monitoring is supported in version 1.2 or later.
(Note) Monitoring settings	—	Collectively configured from the control device.	—	Log in to the server to configure event log monitoring

◎: Advanced, ○: Normal, ×: 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.

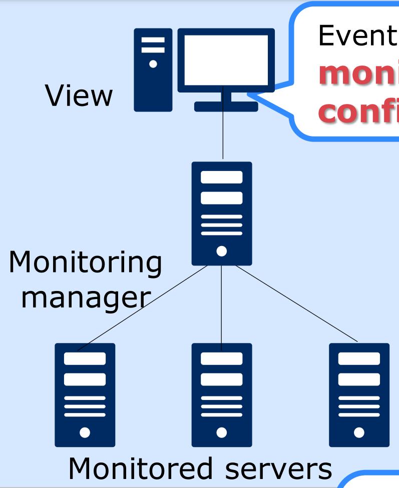
Monitoring		MasterScope SystemManager		NEC ESMPRO	
Hardware	**Hardware faults**	—	• Instead of directly monitoring the hardware, faults are detected by monitoring the fault information in the logs output by other tools (such as NEC ESMPRO).	○	Optional
ESXi	**Resources**	○	• Use HypervisorMonitorOption.	x	Not available
	Logs	○	• Use HypervisorMonitorOption.	△	• Linked with NEC ESMPRO/ServerAgent for vMA.
Guest OS’s	**System logs (Event logs, syslogs)**	◎	• Monitored servers can be configured in the View. • Advanced monitoring settings are available such as keyword-based text filtering.	△	• 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).
	Text logs	○	• Application logs in text format are filtered by keywords for monitoring.	x	Not available
	Processes/ services	○	• Alive monitoring for application processes (for Windows services, startup is also monitored)	x	Not available
	Resources	◎	• 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.	△	• Use **NEC ESMPRO/ServerAgent for Guest OS (fee-based).** • Thresholds for CPU/memory usage and disk space can be used for monitoring.

◎: Advanced, ○: Normal, △: Partly available, ×: No feature, —: Out of scope

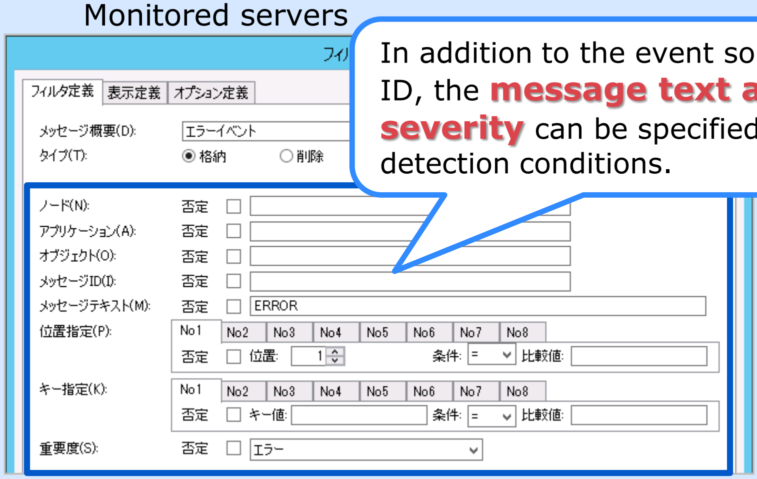
Comparison between MasterScope SystemManager and NEC ESMPRO (event log monitoring)

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.**

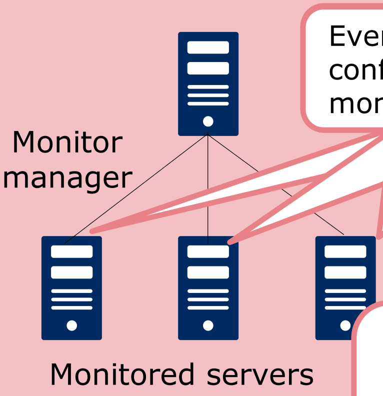


メッセージ概要(D): エラーイベント
タイプ(T): ● 格納 ○ 削除

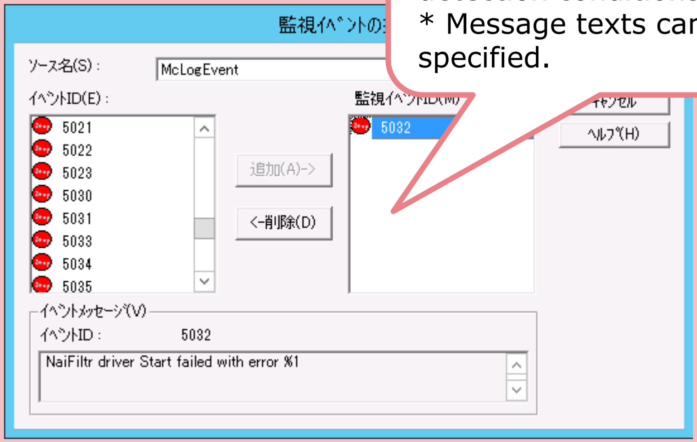
ノード(N): 否定 □
アプリケーション(A): 否定 □
オブジェクト(O): 否定 □
メッセージID(I): 否定 □
メッセージテキスト(M): 否定 □ ERROR
位置指定(P): No1 No2 No3 No4 No5 No6 No7 No8
否定 □ 位置: 1 条件: = 比較値:
キー指定(K): No1 No2 No3 No4 No5 No6 No7 No8
否定 □ キー値: 条件: = 比較値:
重要度(S): 否定 □ エラー

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.



ソース名(S) : McLogEvent
イベントID(E) : 5021 5022 5023 5030 5031 5033 5034 5035
監視イベントID(M) : 5032
イベントメッセージ(V)
イベントID : 5032
NaiFiltr driver Start failed with error %1

Can only specify only the source and event IDs as fault detection conditions.
* Message texts cannot be specified.

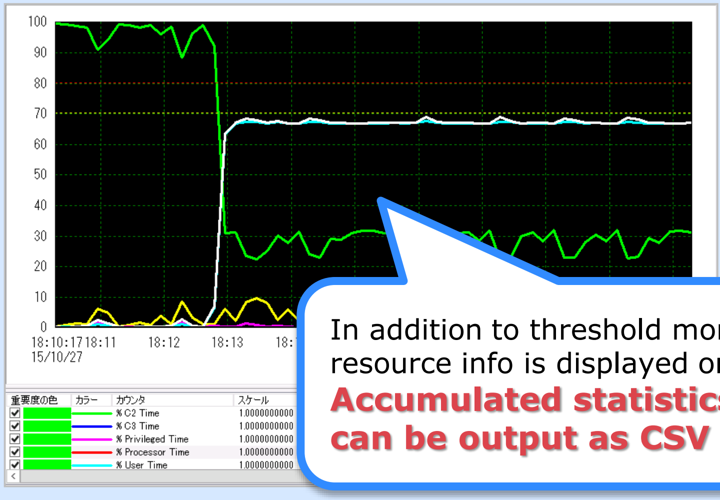
Comparison between MasterScope SystemManager and NEC ESMPRO (resource monitoring)

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.

MasterScope SystemManager

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)



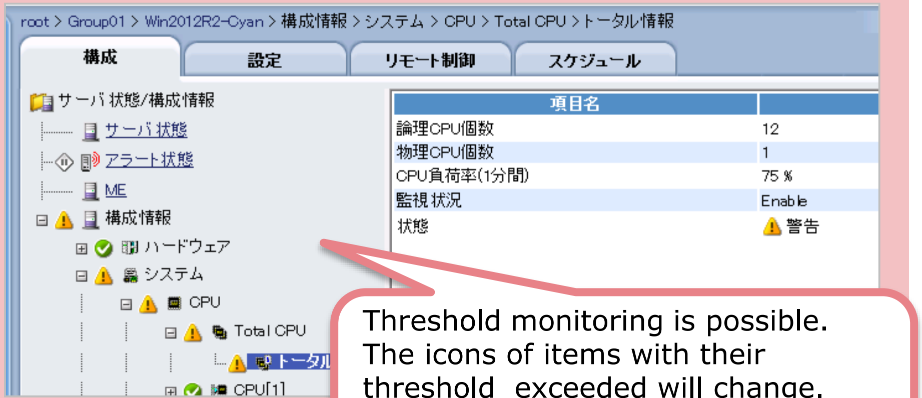
重要度の色	カラー	カウンタ	スケール
☑ 🟩		% C2 Time	1.0000000000
☑ 🟩		% C3 Time	1.0000000000
☑ 🟩		% Privileged Time	1.0000000000
☑ 🟩		% Processor Time	1.0000000000
☑ 🟩		% User Time	1.0000000000

Performance.CSV

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

NEC ESMPRO/SM, SAS

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


root > Group01 > Win2012R2-Cyan > 構成情報 > システム > CPU > Total CPU > トータル情報

サーバ状態/構成情報
- サーバ状態
- アラート状態
- ME
- 構成情報
  - ハードウェア
  - システム
    - CPU
      - Total CPU
        - トータル
      - CPU[1]

項目名	
論理CPU個数	12
物理CPU個数	1
CPU負荷率(1分間)	75 %
監視状況	Enable
状態	⚠ 警告

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

\Orchestrating a brighter world

NEC