

ความสำคัญของ IT Monitoring

กับ

ยุคปัจจุบัน

by Thirawat Suwonnachote

Netway Connect ครั้งที่ 17

21 สิงหาคม 2562

Netway Communication Co., Ltd.

Agenda



- Mean of Monitoring
- Why to Monitoring?
- What are common features of Monitoring?
- TYPES OF SERVER MONITORING
- Monitoring Software
- Benefit Of Monitoring

Mean of Monitoring

Meaning of Monitoring



Monitoring ความหมายโดยทั่วไปก็คือการเฝ้าสังเกตและบันทึกพฤติกรรมที่เกิดขึ้นเป็นประจำ อาจจะเป็นใน Project , Program , Service หรืออื่น ๆ อีกมากมาย เป็นกระบวนการรวบรวมข้อมูลเป็นประจำในทุกๆ ด้าน เพื่อนำมาใช้ในการวิเคราะห์ ตรวจสอบ แก้ไข และหาวิธีป้องกัน

ในมุมมองของเหล่า IT ก็คงอยู่ในประเด็นที่ไม่ต่างกัน หลัก ๆ คือการเฝ้าสังเกตการทำงานของ Service ต่าง ๆ ที่มีอยู่ใน Infrastructure ของตัวเองว่ามีการทำงานที่เป็นปกติหรือไม่ , มี Performance เป็นเช่นไร , มีสิ่งผิดปกติเกิดขึ้นใหม่ไม่ว่าจะเป็นเรื่องของการ Attack ต่าง ๆ , Malware ต่าง ๆ

Meaning of Monitoring



ทั้งนี้ในปัจจุบันโลกของเทคโนโลยีมันไปไกลมาก ทั้งในเรื่องของ Programming ,Hardware , AI , ML และอื่นๆ อีกมาก และในอนาคตเองในประเทศไทยเองก็คงจะมีเรื่องของ IoT เข้ามาอีก นั่นทำให้เรื่องของการทำ Monitoring ที่ดีมีความสำคัญมากขึ้นอย่างหลีกเลี่ยงไม่ได้

Why to Monitoring?

Why to Monitoring?



เป็นคำถามที่น่าสนใจสำหรับบุคคลที่ไม่ได้ทำงานหรือเกี่ยวข้องในสายงาน IT ว่า "ทำไมล่ะ ทำไมเราต้องลงทุนทำระบบ Monitoring" แต่สำหรับคนที่โลดแล่นในงานสาย IT แล้วคงรับรู้ รับทราบเป็นอย่างดีว่าหากคุณมีระบบใด ๆ ที่ทำงานอยู่ใน Infrastructure ที่คุณดูแลแล้วล่ะก็ คุณจำเป็นต้องมีระบบการ Monitoring ที่ดี ตรวจสอบประเด็นปัญหาต่างๆ ที่เกิดขึ้นได้อย่าง รวดเร็ว ทันที

ยังเป็นเรื่องของช่องโหว่ต่าง ๆ , Critical Incident ต่าง ๆ เพราะหากระบบเกิดปัญหา ขึ้นมาจนไม่สามารถใช้งานได้ล่ะก็ เราคนปฏิบัติงานคงพบความยากลำบากกันไม่น้อย

Why to Monitoring?



- Protect the image of your business
- Keep your customers and your company be happy
- Prevent losing data
- Prevent System down
- Prevent Low performance
- Prevent System run slowly
- Prevent business damage

What are common features of Monitoring?

What are common features of Monitoring?



- Analysis in real time
- System alerts
- Notifications
- Graphic visualization
- Production of reports
- Record Available
- Possibility of installing plug-ins
- Distinction by type of user

TYPES OF SERVER MONITORING

TYPES OF SERVER MONITORING



- Uptime/Availability Monitoring
- Site Performance Monitoring
- Resource Monitoring
- Error Monitoring
- Log Monitoring
- Database Monitoring
- Security or Malware Monitoring
- Customizing for Your Own Needs

Monitoring Software

Monitoring Software



ตัว Software ที่นิยมใช้ในการ Monitor ระบบมีหลายตัวมาก ขึ้นอยู่กับความถนัด ความชอบ และต้นทุนของแต่ละคน แต่ละองค์กร ในที่นี้จะขอยกตัวอย่างดังนี้

Monitoring Software



Solarwinds Network Performance Monitor(NPM)

NPM Summary

All Nodes managed by NPM

GROUPED BY REGION

- ▶ APAC
- ▶ EMEA
- ▶ North America
 - 3Com
 - Switch sales
 - American Power Conversion Co.,p.
 - APC NetBotz
 - Aruba Networks Inc
 - Avaya Communication
 - ▶ Cisco
 - ▶ Compatible Systems Corp.
 - ▶ Dell Computer Corporation
 - ▶ Extreme Networks
 - ▶ F5 Networks, Inc.
 - ▶ FlowPoint Corporation
 - ▶ Foundry Networks, Inc.
 - ▶ HP
 - ▶ IBM
 - ▶ Juniper Networks, Inc.
 - ▶ Juniper Networks/NetScreen
 - ▶ Linksys
 - ▶ Linux
 - ▶ Meraki Networks, Inc.
 - ▶ Multi-Tech Systems, Inc.

Hardware Health Overview

Nodes Count: 37

23 Up 3 Warning 7 Critical 4 Undefined

High Errors & Discards Today

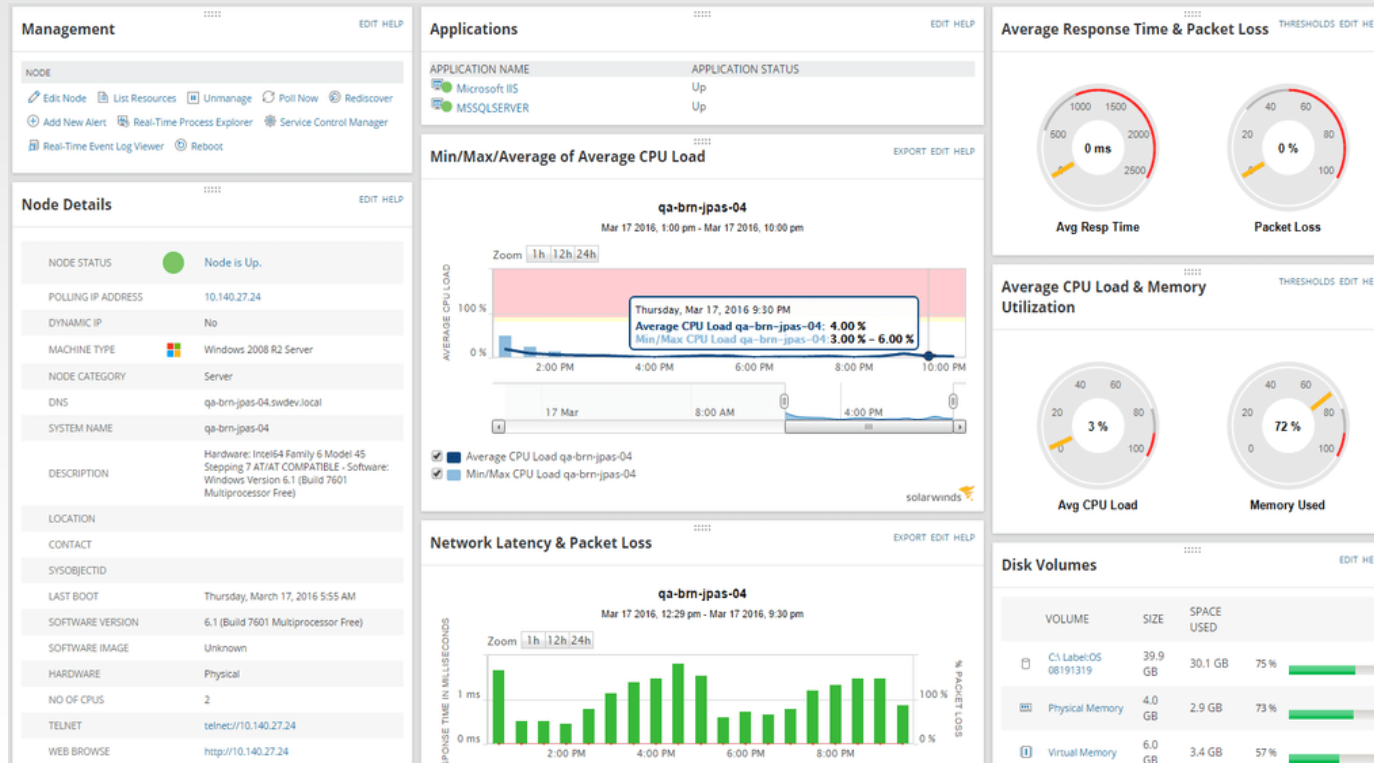
INTERFACES WITH ERRORS+DISCARDS GREATER THAN 10000 TODAY

| NODE | INTERFACE | RECEIVE ERRORS | RECEIVE DISCARDS | TRANSMIT ERRORS | TRANSMIT DISCARDS |
|------------------------|---------------|--------------------|---------------------|----------------------|---------------------|
| PERM_TEX-MDS9120-76-76 | fc1/5 | 0 errors | 0 discards | 5,582,170,112 errors | 5,808,010 discards |
| PERM_AP6511-E6C8C0 | fe4 | 64,088,776 errors | 78,073,384 discards | 0 errors | 0 discards |
| PERM_AP6511-E6C8C0 | fe2 | 100,061,432 errors | 2,349 discards | 0 errors | 0 discards |
| PERM_TEX-MDS9120-76-76 | fc1/6 | 0 errors | 0 discards | 5,808,179 errors | 10,024,648 discards |
| PHX-NEXUS 1000V | port-channel1 | 0 errors | 1,244,402 discards | 0 errors | 0 discards |

Monitoring Software



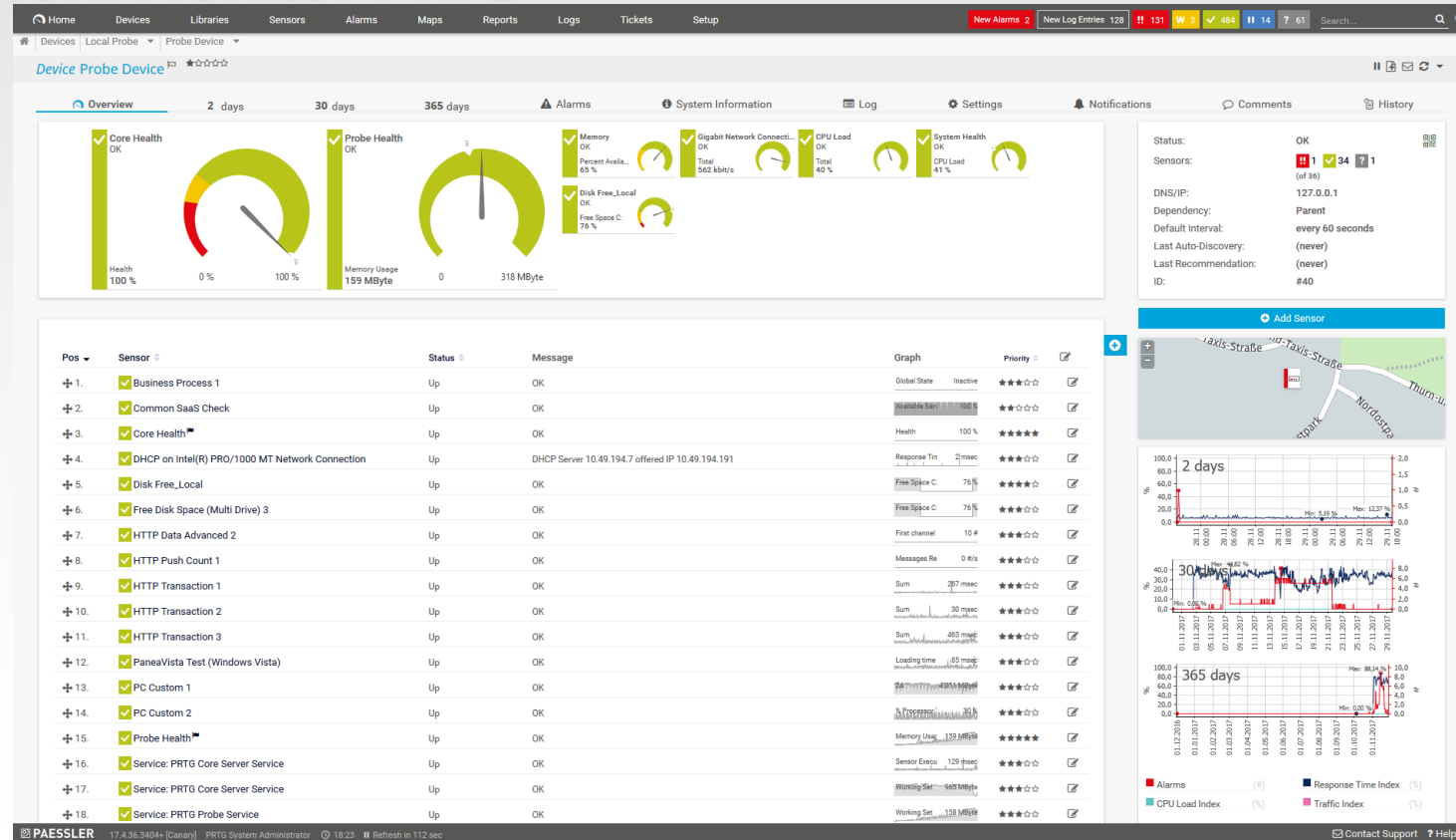
Solarwinds Server and Application Monitor (SAM)



Monitoring Software



PRTG Network Monitor PRTG



Monitoring Software



Nagios XI

Nagios XI

Home Views Dashboards Reports Configure Tools Help Admin

Quick View: Home Dashboard, Tactical Overview, Birdseye, Operations Center, Operations Screen, Open Service Problems, Open Host Problems, All Service Problems, All Host Problems, Network Outages

Details: Service Detail, Host Detail, Hostgroup Summary, Hostgroup Overview, Hostgroup Grid, Servicegroup Summary, Servicegroup Overview, Servicegroup Grid, BPI, Metrics

Graphs: Performance Graphs, Graph Explorer

Maps: 8Bmap, Google Map, Hypermap, Minemap, Nagvis, Network Status Map

Incident Management: Latest Alerts, Acknowledgements, Scheduled Downtime, JIRA Integration, Mass Acknowledge, Recurring Downtime, Notifications

Monitoring Process: Process Info, Performance, Event Log

Status Summary For All Host Groups

| Host Group | Hosts | Services |
|-----------------------------------|-------|------------------------------|
| All EMC SAN Hosts (all_emc_hosts) | 1 Up | 4 OK |
| Firewalls (firewalls) | 1 Up | 1 OK |
| Linux Servers (linux-servers) | 6 Up | 43 OK, 4 Warning, 2 Critical |
| new group (new group) | 11 Up | 5 Warning, 2 Critical |
| Printers (printers) | 3 Up | 5 OK, 1 Warning |
| Switches (switches) | 2 Up | 72 OK, 2 Warning, 2 Critical |
| Websites (websites) | 3 Up | 25 OK, 2 Critical |
| Windows Servers (windows-servers) | 1 Up | 10 OK, 2 Critical |

Last Updated: 2016-03-03 16:29:03

Key Services

7.5ms 0.06s 30%

5ms 0.04s 20%

2.5ms 0.02s 10%

18:00 21:00 3: Mar 09:00 06:00 09:00 12:00 15:00

CPU Usage (ScottServer) [5 min avg Load] HTTPS (gateway.nagios.local) [time] HOST (gateway.nagios.local) [rta] HOST (gateway.nagios.local) [pl]

My Graph

vs1.nagios.com : Ping

ms X ms ms

18:00 3: Mar 06:00 12:00

rta pl Warning Critical

Host Status Summary

| Up | Down | Unreachable | Pending |
|----|------|-------------|---------|
| 47 | 0 | 0 | 1 |

| Unhandled | Problems | All |
|-----------|----------|-----|
| 2 | 3 | 51 |

Last Updated: 2016-03-03 16:29:03

Monitoring Engine Event Queue

Monitoring Engine Event Queue

Scheduled Events Over Time

20

10

0

New +5 Min

Last Updated: 2016-03-03 16:29:22

Hostgroup Status Overview

Linux Servers (linux-servers)

| Host | Status | Services |
|------------------------|--------|-------------------|
| xxx2.nagios.local | Up | 6 OK |
| exchange.nagios.org | Up | 17 OK, 2 Critical |
| imiltchev.nagios.local | Up | No services found |
| | | 17 OK |

Host Status TAC Summary

| 3 Down | 0 Unreachable | 47 Up | 1 Pending |
|--------------------|---------------|-----------|-----------|
| Unhandled Problems | | 46 Active | 1 Passive |
| 1 Acknowledged | | 1 Passive | |
| 3 Active | | | |

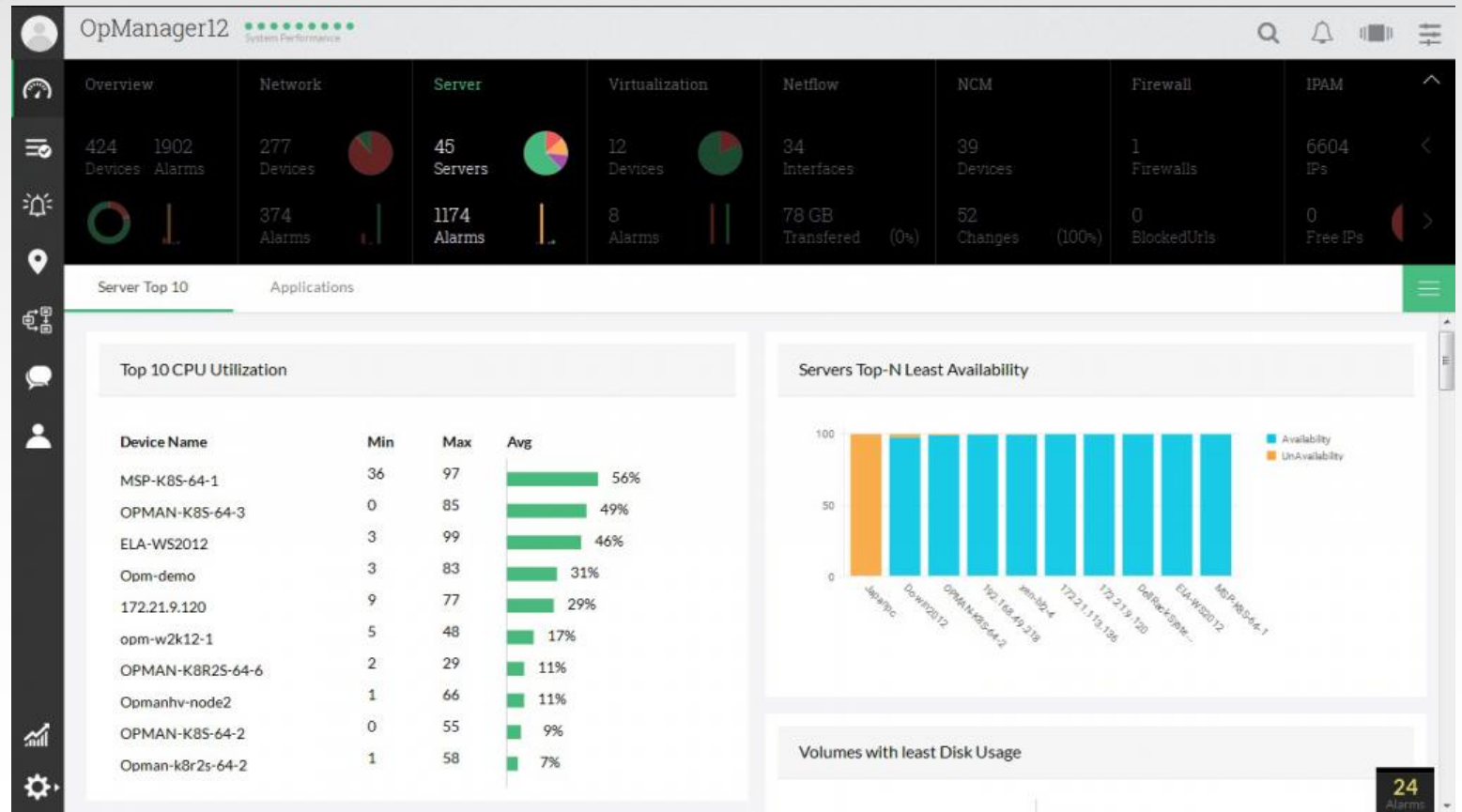
Last Updated: 2016-03-03 16:29:02

ScottsServer : CPU Usage

Monitoring Software



ManageEngine OpManager



Monitoring Software



Zabbix

The screenshot displays the Zabbix web interface dashboard. At the top, there is a navigation bar with tabs for Monitoring, Inventory, Reports, Configuration, and Administration. Below this is a secondary navigation bar with options like Dashboard, Overview, Web, Latest data, Triggers, Events, Graphs, Screens, Maps, Discovery, and IT services. The main dashboard area is divided into several panels:

- Favourite maps:** Shows 'Local network' as the selected map.
- Favourite graphs:** Shows 'New host CPU load' as the selected graph.
- Favourite screens:** Shows 'Zabbix server' as the selected screen.
- Last 20 issues:** A table listing recent issues. Two issues are highlighted: 'Version of zabbix-agent(d) was changed on Zabbix server 1' (2016-01-11, 1m 39s, No) and 'Lack of free swap space on Zabbix server 1' (2015-08-11, 5m 3d, Yes 4).
- Status of Zabbix:** A table showing system parameters such as 'Zabbix server is running' (Yes), 'Number of hosts (enabled/disabled/templates)' (54 / 10 / 43), 'Number of items (enabled/disabled/not supported)' (356 / 350 / 0 / 6), 'Number of triggers (enabled/disabled [problemok])' (95 / 94 / 1 [2 / 92]), 'Number of users (online)' (3 / 2), and 'Required server performance, new values per second' (4.79).
- System status:** A table showing the status of various host groups. 'Discovered hosts' and 'Zabbix servers' show 1 warning each.
- Host status:** A table showing the status of host groups. 'Discovered hosts' has 7 without problems and 1 with problems. 'Zabbix servers' has 0 without problems and 1 with problems.
- Discovery status:** A table showing the status of discovery rules. 'Local network2' has 6 UP and 1 DOWN.

At the bottom right of the dashboard, there is a 'Debug' button.

Benefit Of Monitoring

Benefit Of Monitoring



- Enable data driven insights and decisions
- Detect problems early to prevent disasters
- Improve productivity and performance
- Plan and budget for IT upgrades
- Prevent and reduce downtime and business losses

Business Strong when you
have the best
infrastructure monitoring

Keytakaways



**Netway Communication
Co., Ltd.**

T: 02 912 2558

E: support@netway.co.th

W: <https://netway.co.th/>

F: @netway.official