

Network Security Tools

ดร. ธนัญชัย ตริภาค

Class Outcome

- ▶ นักศึกษาสามารถเลือกใช้เครื่องมือ
 - ช่วยเหลือในการบริหารระบบสารสนเทศ
 - การรักษาความปลอดภัยระบบสารสนเทศได้
 - ช่วยตรวจสอบ และรับมือปัญหาความปลอดภัยเครือข่ายได้

Q : การทำงานพื้นฐานของผู้ดูแลระบบมีอะไรบ้าง แต่ละการทำงานมีขั้นตอนสำคัญอย่างไรบ้าง

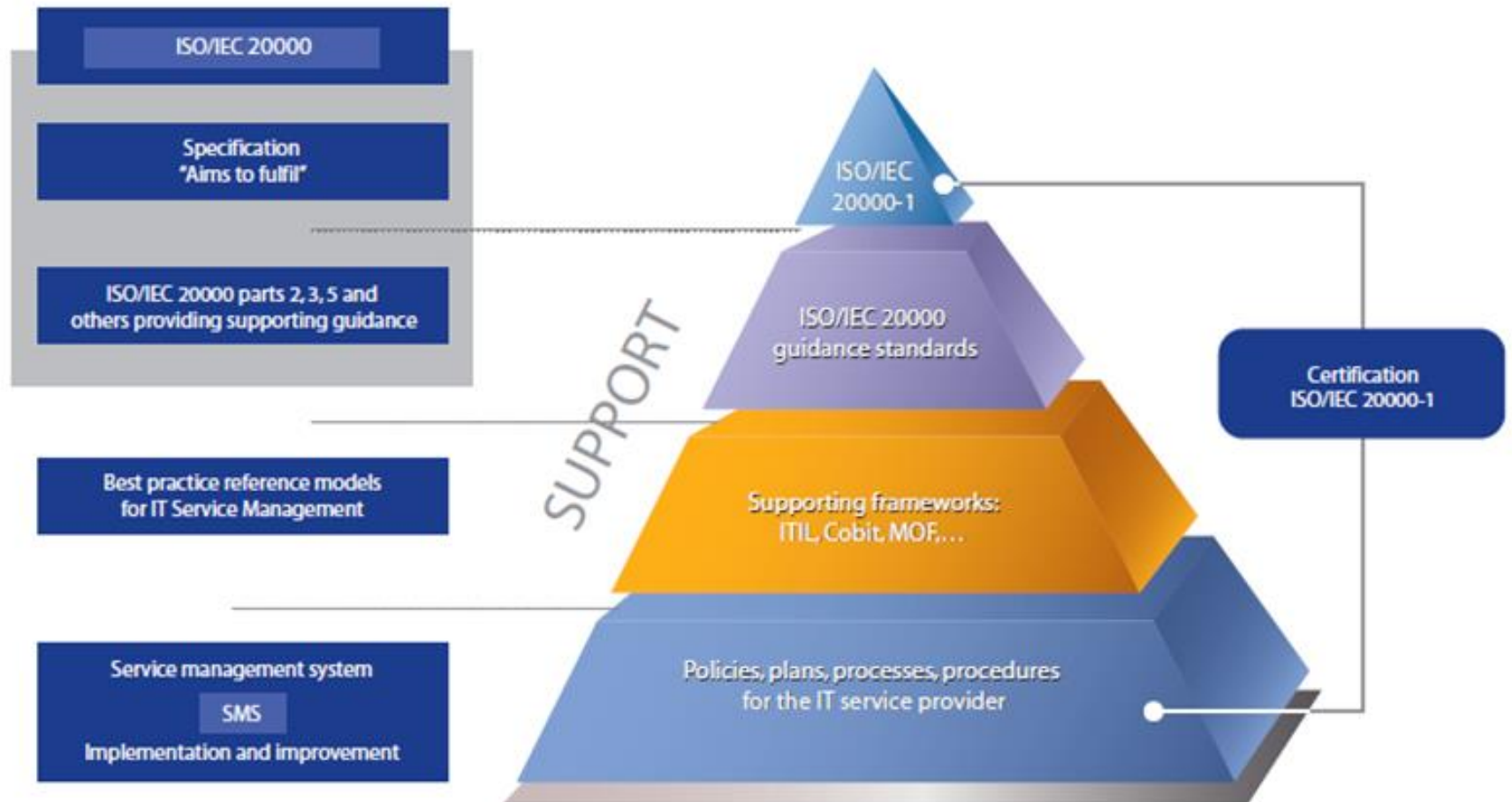


Mind Map

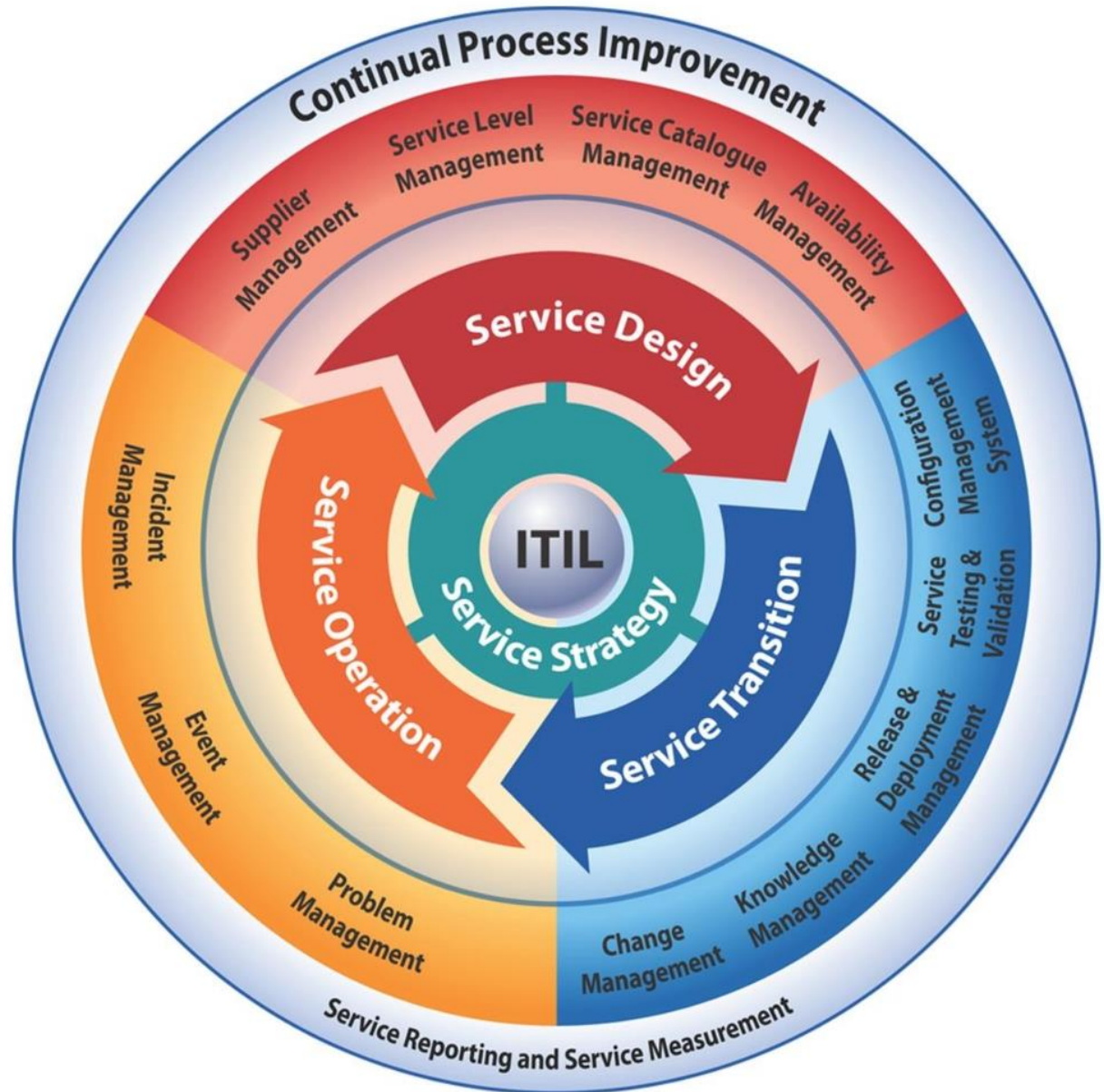
มาตรฐานการดูแลระบบ

- ▶ ISO/IEC 20000
 - International Standard for IT Service Management
- ▶ ITIL
 - Information Technology Infrastructure Library
- ▶ COBIT
 - Control Objectives for Information and Related Technology

ISO 20000 - Certification



ITIL – Process Improvement

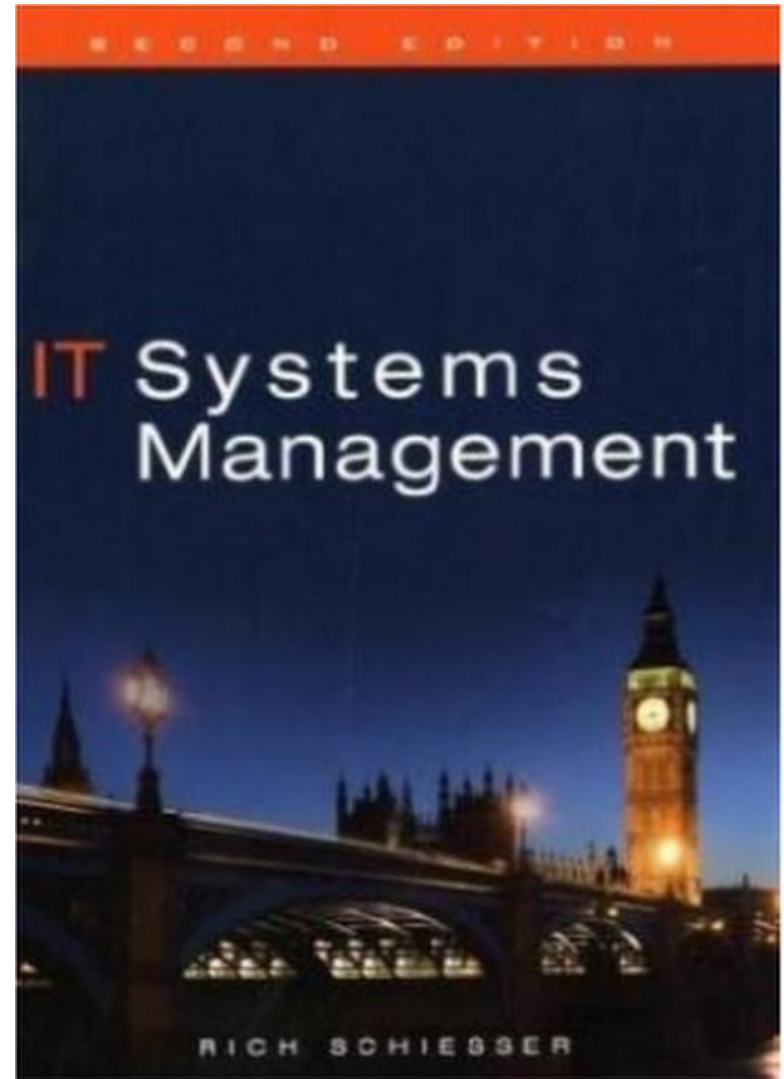


COBIT - IT Governance Framework



IT Systems Management

- ▶ Organization & Staff
- ▶ Availability
- ▶ System Monitoring
 - Application
 - Network
 - System
- ▶ Change Management
- ▶ Problem Management
- ▶ Network Management
- ▶ Storage Management
- ▶ Capacity Planning
- ▶ Performance Tuning
- ▶ Security



Q : แต่ละการทำงาน มีเครื่องมืออะไรเกี่ยวข้องบ้าง



- ▶ Availability
- ▶ System Monitoring
- ▶ Problem Management
- ▶ Network Management
- ▶ Storage Management
- ▶ Capacity Planning
- ▶ Performance Tuning
- ▶ Security


Q : ให้นักศึกษายกตัวอย่างเครื่องมือในกลุ่มต่างๆ

Monitoring Tools	Detection Tools	Protection Tools
“?”	“?”	“?”

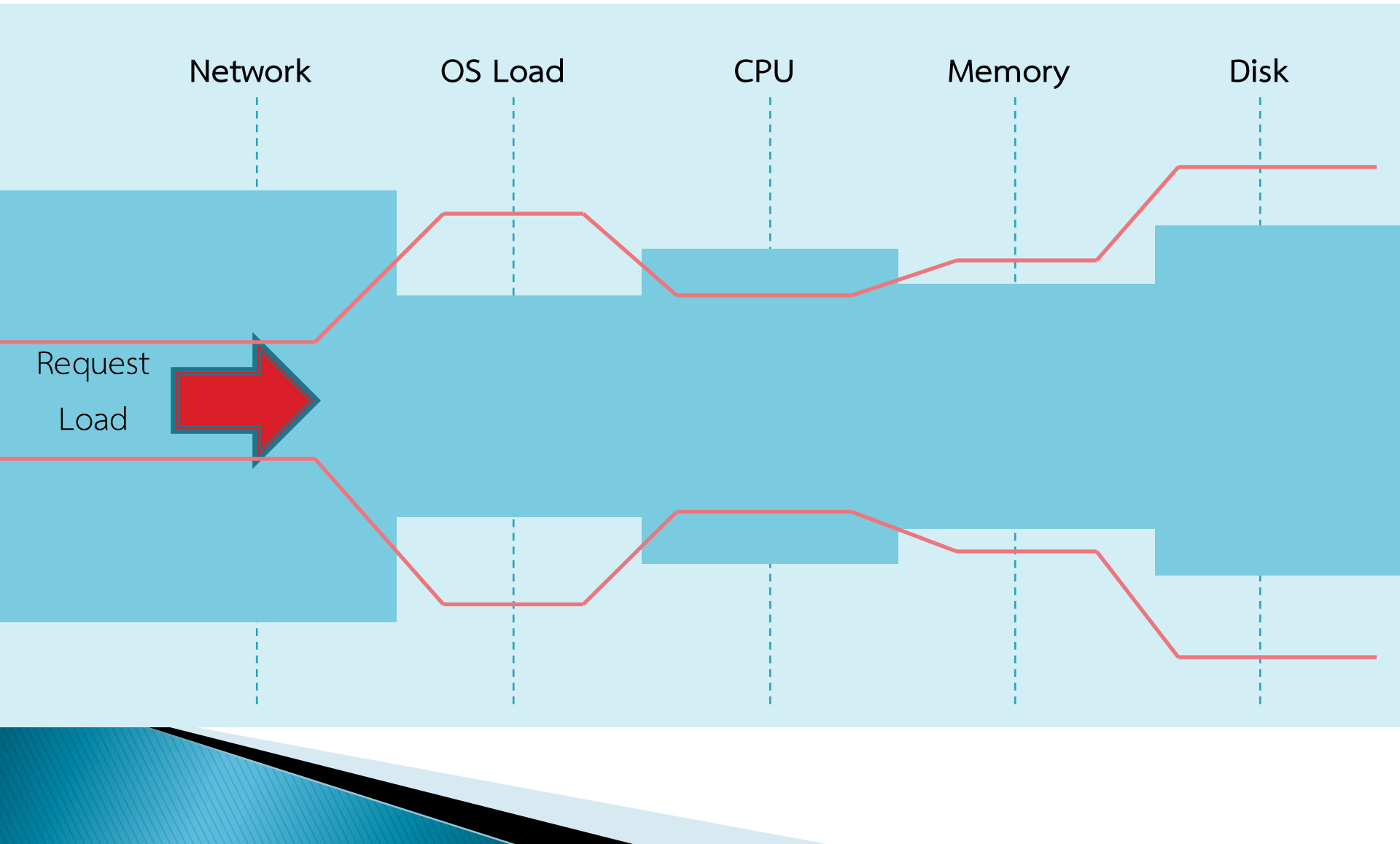
Q : เครื่องมือแต่ละชนิด มีการทำงานอย่างไร และให้ผลลัพธ์อะไรบ้าง



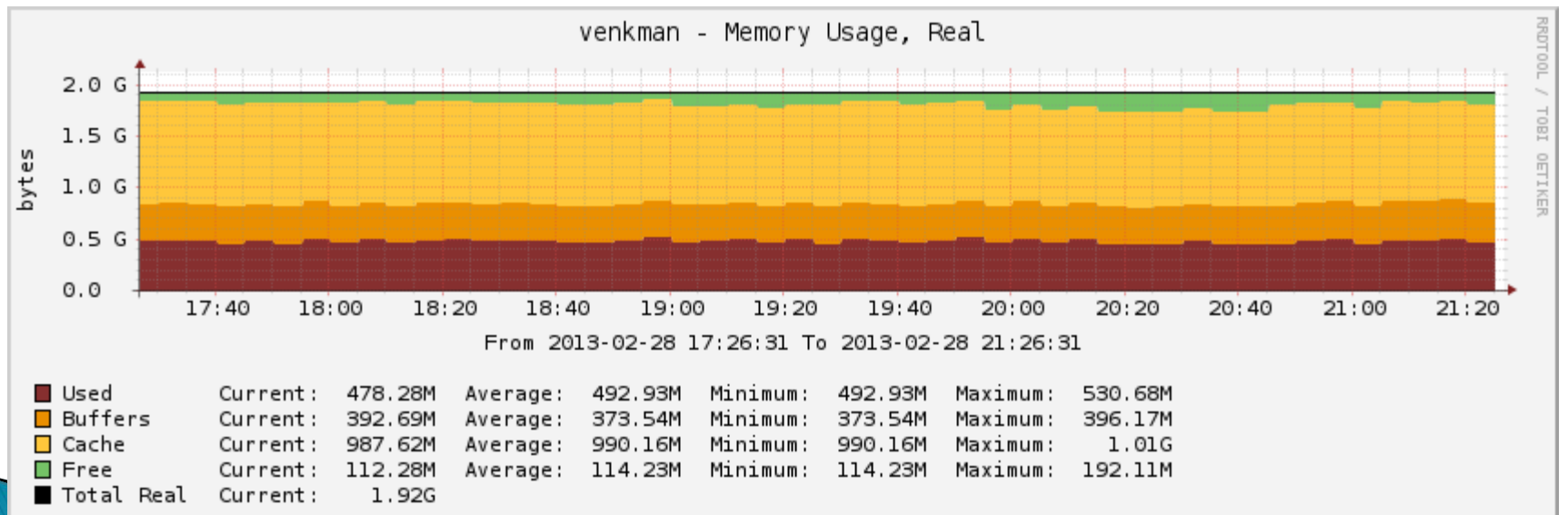
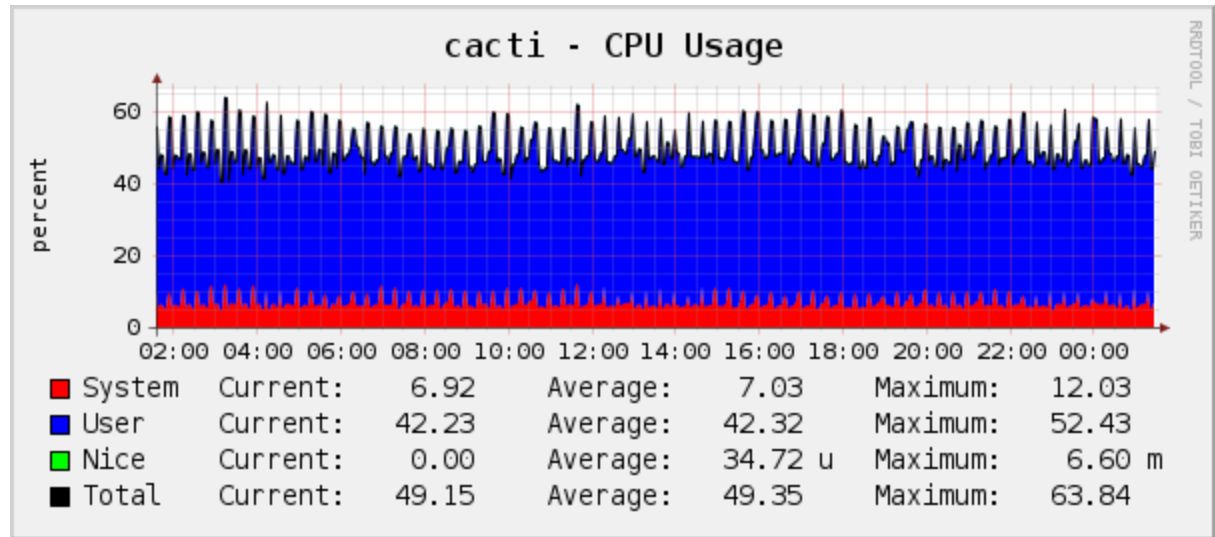
System Monitoring

- ▶ System
 - CPU Utilization
 - Memory Usage
 - Disk Utilization
 - ▶ Application
 - No Response
 - Shutdown
 - ▶ Network
 - Utilization
 - Connectivity
- 

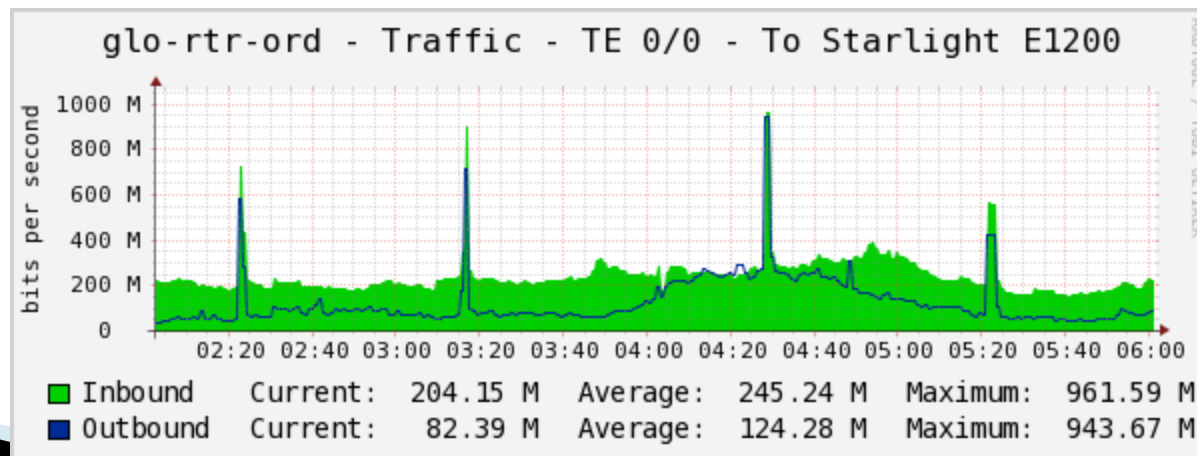
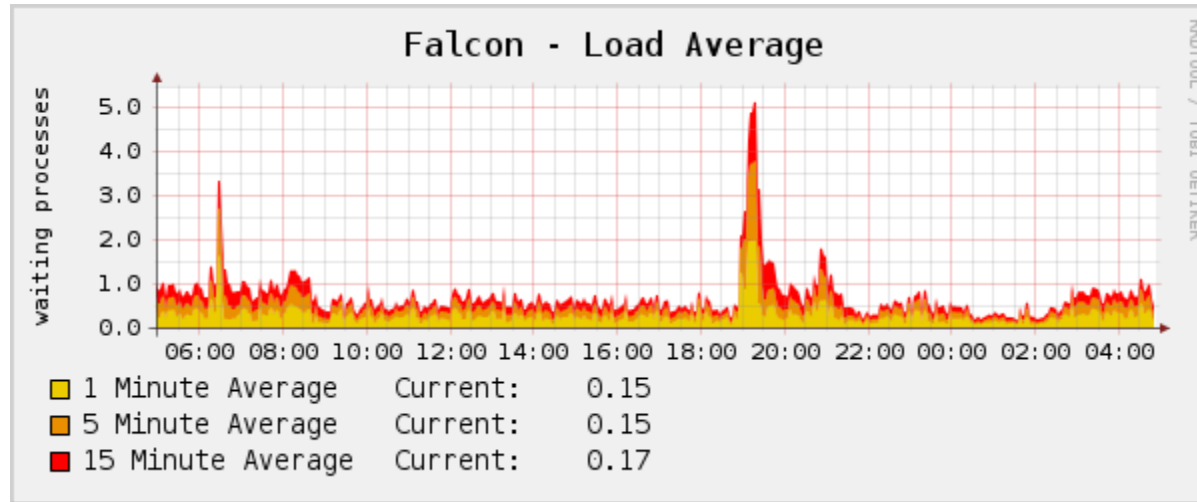
Performance Tuning



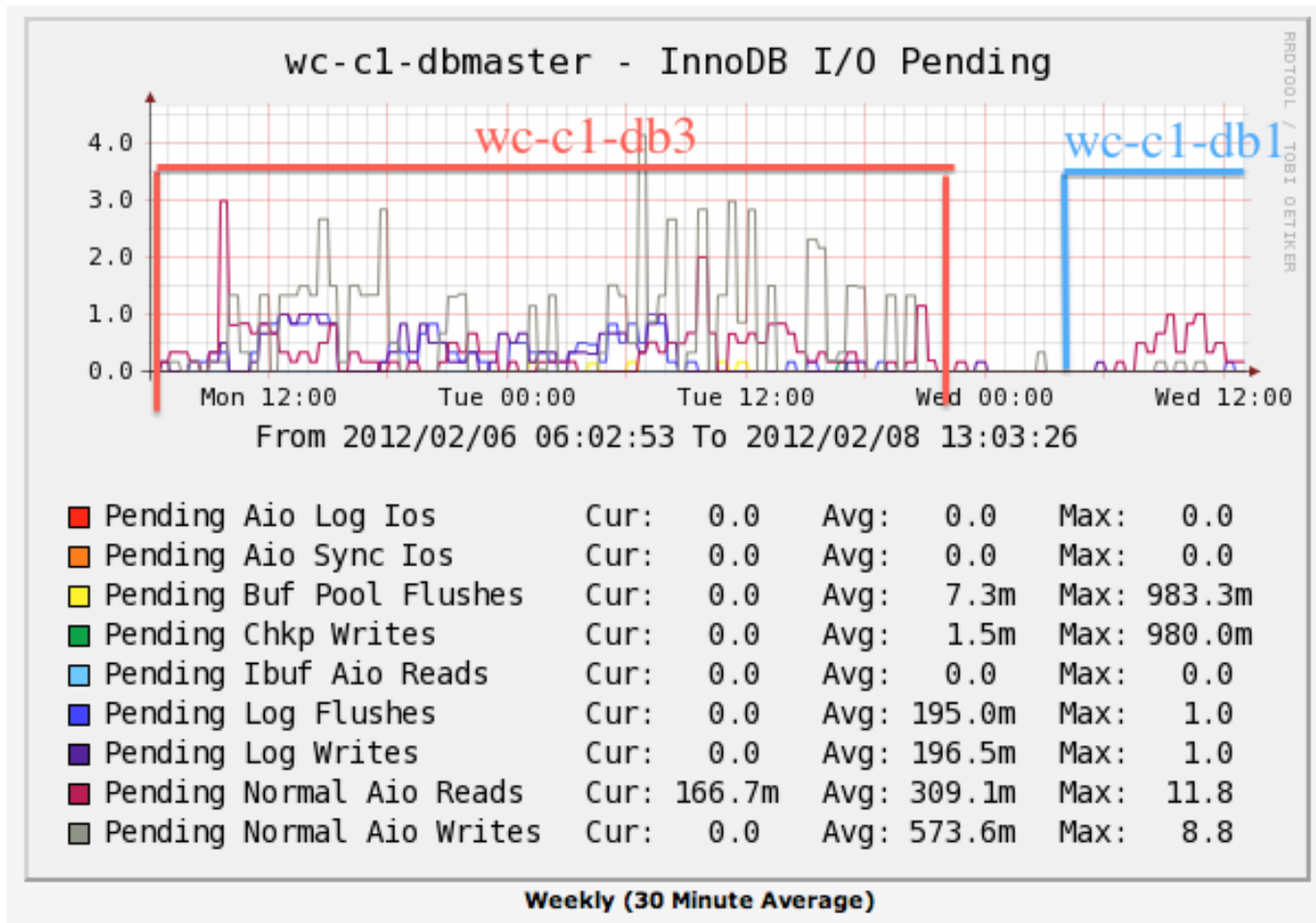
CACTI



CACTI



CACTI



Solar
wind

solarwinds

HOMEAPPLICATIONSTRANSACTIONS

SummaryGroupsTop 10EventsSyslogTrapsMessage CenterReportsVMwareThwackTraining

Application Summary Home

All Applications

GROUPED BY APPLICATION TEMPLATE, NODE NAME

[MANAGE APPLICATIONS](#) [HELP](#)

Active Directory 2003-2008 Services and Counters	All applications up
Bind (Linux)	All applications up
Citrix XenApp 5.0 ICA Session WMI counters	All applications up
DNS User Experience	All applications up
Exchange 2007 OWA Form Login	All applications up
Exchange 2007-2010 Client Access Role Services and Counters (Basic)	All applications up
Exchange 2007-2010 Hub Transport Role Service and Counters (Basic)	1 application down
Exchange Server 2000 and 2003	All applications up
HTTP Form Login	All applications up 1 application down
IBM DB2	All applications up
IS Logfile Watcher	All applications up
Internet Information Service (IIS) Services and Counters	All applications up
Java Application Server (SNMP)	All applications up
Legacy Active Directory	2 applications down
Legacy Exchange 2007	1 application down
Legacy Exchange 2007 WMI Counters	All applications up
Legacy Exchange 2010 Hub Transport Role Performance Counters	All applications up
Legacy Exchange 2010 Mailbox Role Services	All applications up
Legacy Internet Information Services	All applications up
Legacy Linux/Unix Operating System	All applications up
Legacy SQL Server 2005 Database	All applications up
Legacy SQL Server 2008 Database	1 application down
Legacy Windows Server 2003-2008	All applications up
Linux CPU Monitoring Perl	All applications up
Microsoft Forefront Threat Management Gateway 2010	All applications up
Microsoft Network Policy Server RADIUS Server	All applications up
MySQL Server	All applications up
Nagios Linux File & Directory Count Script	All applications up
Oracle Database	All applications up

Application Health Overview

[HELP](#)


Application Count: 42



31 Application Up	1 Application Warning
4 Application Critical	6 Application Down
0 Unknown	0 Other

Pesky Applications

[HELP](#)




All Groups


NO GROUPING APPLIED


[MANAGE GROUPS](#) [HELP](#)




- Cairo Nodes
- Datacenter Summary Hardware
- Down Applications
- Enterprise IOS licences
- ERP Application Stack
- Low Free Space
- Orlando AD Hots
- Production vCenter Servers
- Tokyo Exchange Email
- Unreachable ESX Hosts

Solarwind




 Server & Application Monitor



Appinsight for SQL -  MSSQLSERVER


Last 24 Hours 



Application Details











Management:  Edit Application Monitor  Unmanage  Poll Now

 Real-Time Process Explorer  Service Control Manager

 Real-Time Event Log Viewer

Instance Name	MSSQLSERVER
Status	Critical
SQL Server Version	10.0.5500.0
SQL Server Product Level	SP3
SQL Server Edition	Standard Edition (64-bit)

All Databases

NAME	STATUS	DATABASE SIZE	TRANSACTION LOG SIZE
 APM4.2	Online	593.25 MB	259.13 MB
 EOC_131	Online	10.25 MB	28.81 MB
 master	Online	4.00 MB	1.00 MB
 model	Online	2.25 MB	512.00 KB
 msdb	Online	25.06 MB	6.75 MB
 NCM_131	Online	4.25 MB	1.00 MB
 NetPerfMon_131	Online	653.94 MB	101.00 MB
 ReportServer	Online	3.25 MB	6.13 MB
 ReportServerTempDB	Online	2.25 MB	768.00 KB
 tempdb	Online	8.00 MB	512.00 KB

Active Alerts

ALL UNACKNOWLEDGED



TIME OF ALERT	NAME
---------------	------

SQL Error Log

DATE/TIME	ERROR MESSAGE
Monday, August 05, 2013 4:18:40 PM	Setting database option COM ReportServerTempDB.
Monday, August 05, 2013 4:18:40 PM	Setting database option COM
Monday, August 05, 2013 4:18:39 AM	Setting database option COM ReportServerTempDB.
Monday, August 05, 2013 4:18:39 AM	Setting database option COM
Monday, August 05, 2013 12:00:32 AM	This instance of SQL Server I 4:18:39 PM (local) 7/24/2013 only; no user action is require

Page 1 of 6 | Items on page 5

Processes and Services

COMPONENT NAME	PROCESS NAME (ID)	CPU
 SQL Server	sqlservr.exe (1440)	0
 SQL Server VSS Writer	sqlwriter.exe (1972)	0

See SQL server error logs & other server performance metrics

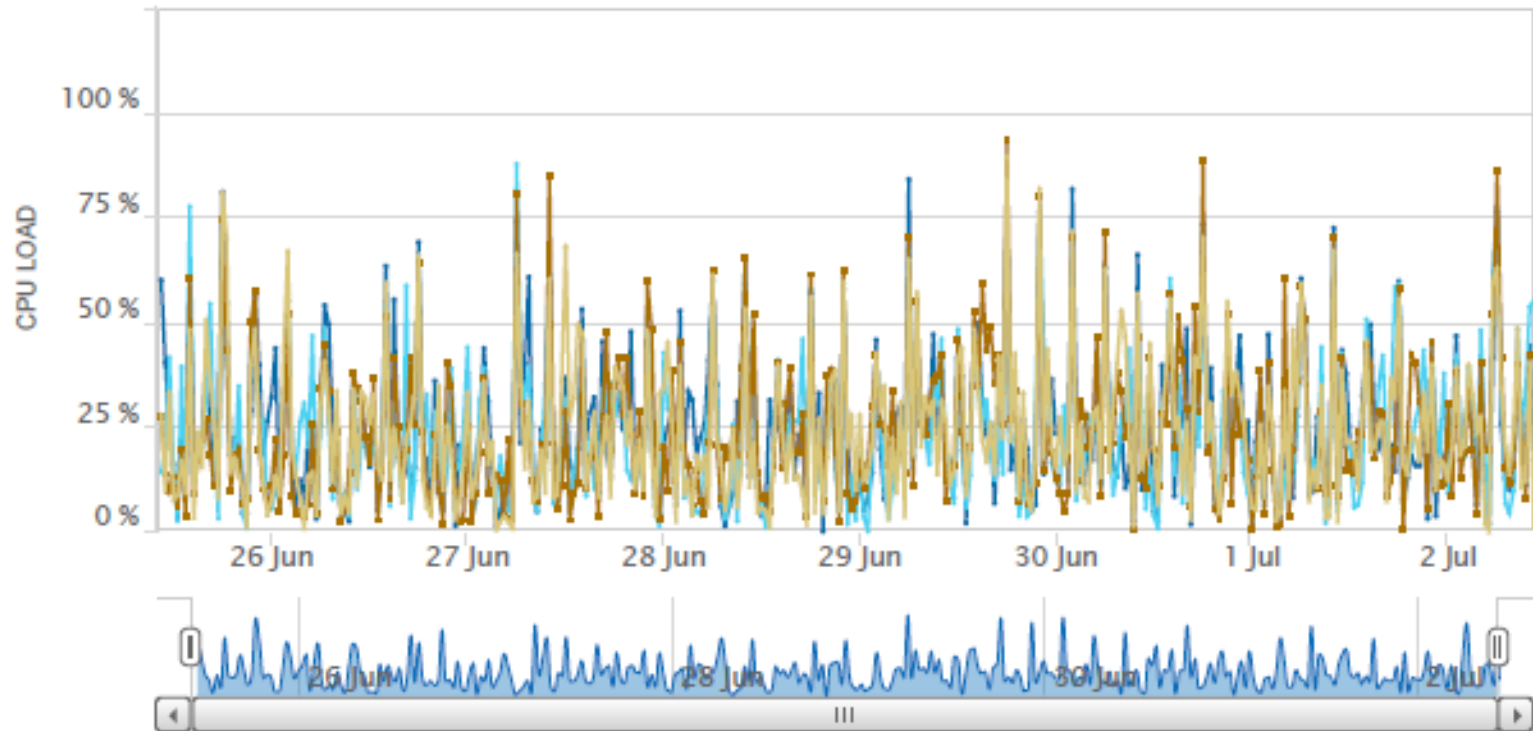
Drill into individual database performance

Top CPUs by Percent Load

[EXPORT](#)[HELP](#)

Jun 25 2015, 10:00 am - Jul 2 2015, 10:30 am

Zoom **1h** 12h 24h



- ☒ CPU Load . CPU # 1
- ☒ CPU Load . CPU # 2
- ☒ CPU Load . CPU # 3
- ☒ CPU Load . CPU # 4

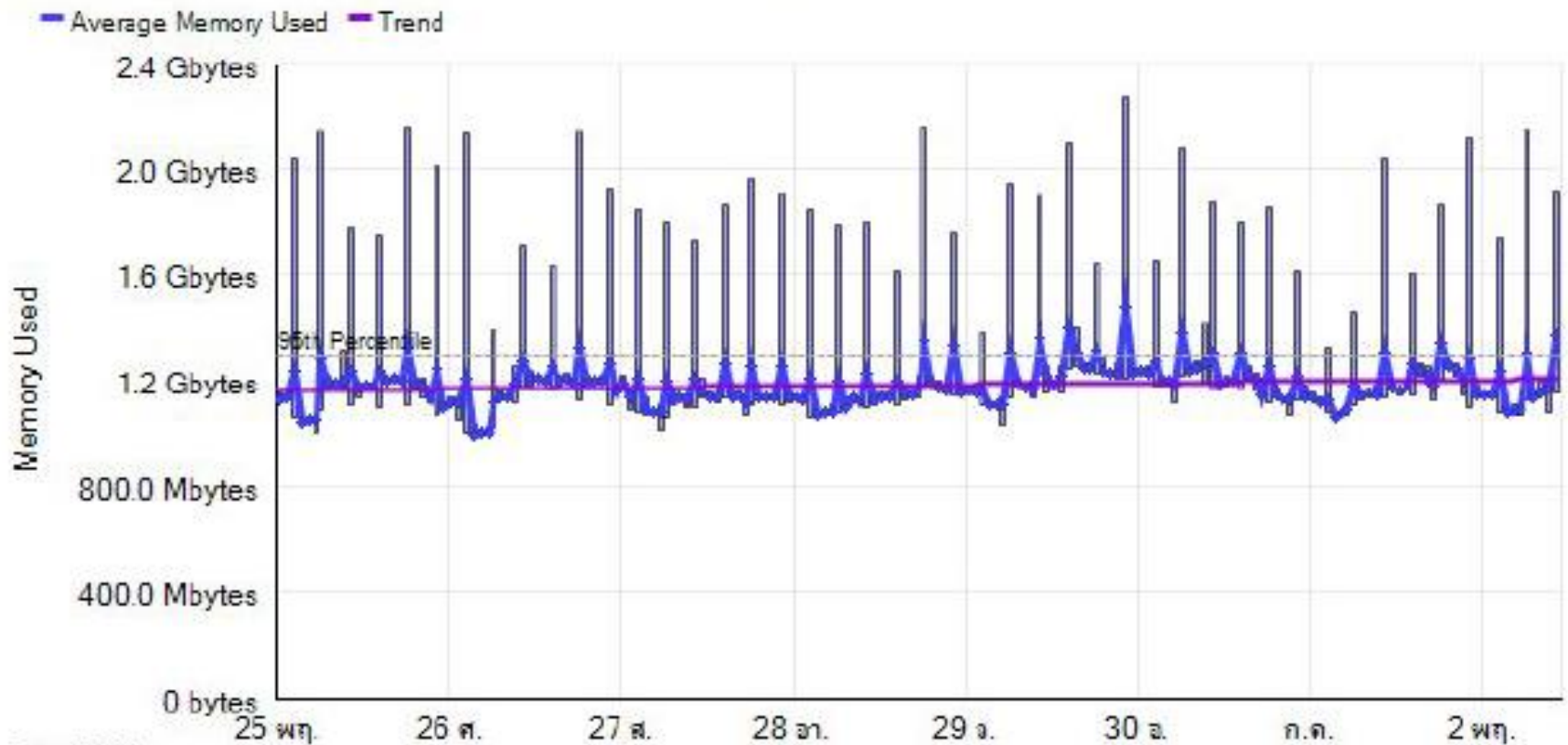
Min/Max/Average Memory Usage - Now

LAST 7 DAYS

View Options

HELP

Min/Max/Average Memory Usage - Total Memory is 3.2 GB
Last 7 Days



ณ.บ. 2558

95th Percentile: Average Memory Used is 1.2908 Gbytes

SolarWinds Orion Core Services 2014.1

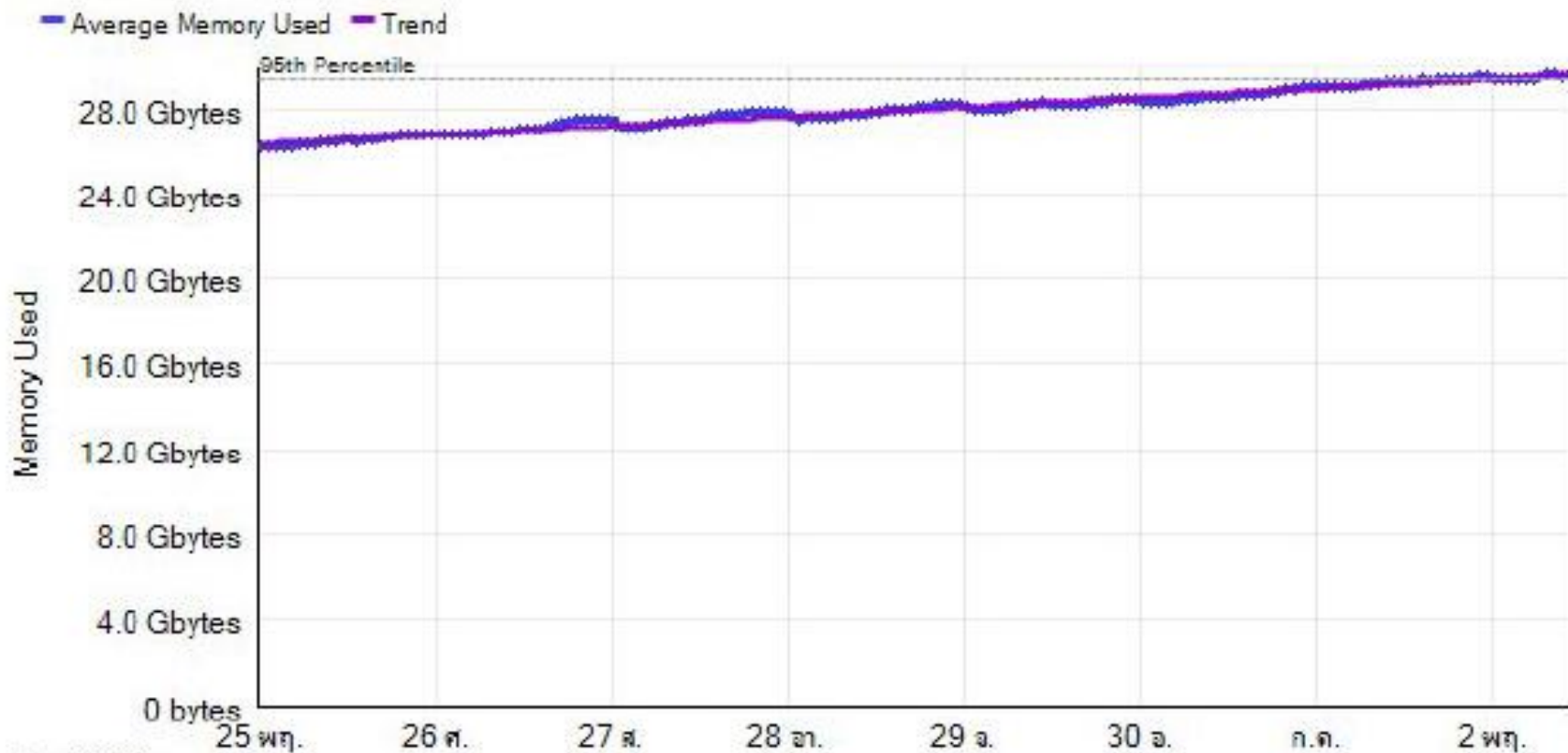
Min/Max/Average Memory Usage - Now

LAST 7 DAYS

View Options

HELP

Min/Max/Average Memory Usage - Total Memory is 32.0 GB
Last 7 Days

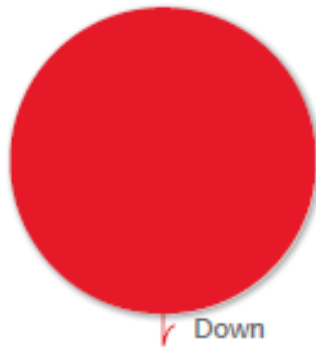


ณ.บ. 2558







95th Percentile: Average Memory Used is 29.4099 Gbytes

SolarWinds Orion Core Services 2014.1

Application Health Overview


[HELP](#)

Application Count: 1

0		Up	0		Warning
0		Critical	1		Down
0		Unknown	0		Other

Applications

[EDIT](#)[HELP](#)

APPLICATION NAME	APPLICATION STATUS
 Oracle Database	Down

Intrusion Prevention System

- ▶ Network-based IPS
- ▶ Host-based IPS

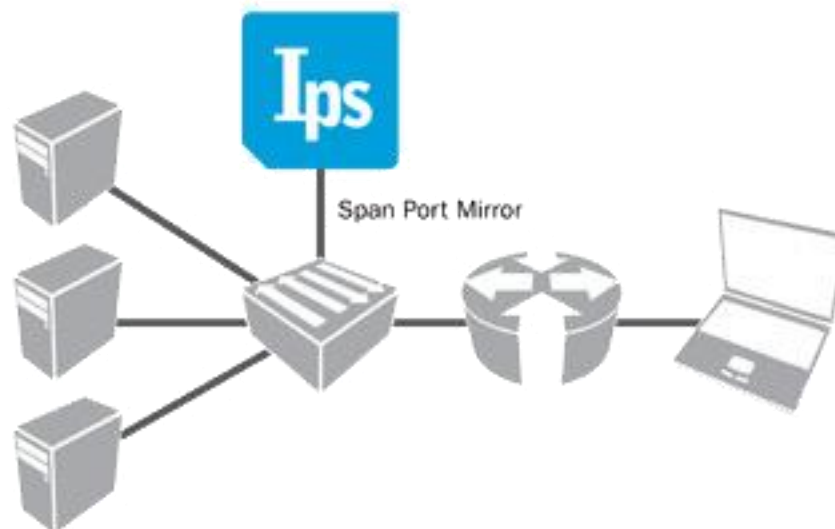
IPS Detection Method

- ▶ Signature-Based Detection
- ▶ Statistical Anomaly-Based Detection
- ▶ Stateful Protocol Analysis Detection

การติดตั้ง IPS

StoneGate Deployment

IDS (Intrusion Detection System) mode



StoneGate Deployment

IPS (Intrusion Prevention System) mode



Q : กับปัญหาหรือกระบวนการ ... จะเลือกใช้เครื่องมือใดช่วย
ตรวจสอบและจัดการ



5 ปัญหา /
กระบวนการ

Q : เครื่องมือที่นักศึกษาที่มีอยู่ ช่วยในการจัดการกับปัญหา หรือ
ช่วยเพิ่มความปลอดภัยอะไรได้บ้าง อย่างไร



แล้วยังรับมือกับ
อะไรไม่ได้บ้าง

สรุป / สิ่งที่ได้เรียนรู้