Kiuru MSSP 5.0 Monitoring

27.5.2015

Introduction

This presentation shows:

1. How Kiuru MSSP 5.0 can be monitored using Zabbix.

   - Zabbix templates are shipped with Kiuru MSSP.

2. Screenshots of monitoring Kiuru MSSP 5.0 with Zabbix.

   - Each figure is extracted from Zabbix views.

   - Example data is from test traffic.

   - Figure data is explained in the slide notes.

Monitoring Software

ZABBIX

Zabbix is an open source monitoring application, and it can be used to monitor Kiuru MSSP servers.

Zabbix is used as an example of monitoring software because:

1. It supports both JMX and SNMP.
2. It supports XML configuration templates.
3. It has an easy web-based user interface.

Runtime Environment Monitoring

Kiuru MSSP 5.0 runs on a Java Virtual Machine environment.

Useful monitorable data items are:

- CPU usage
- Memory usage
- Thread usage

Runtime Environment Monitoring
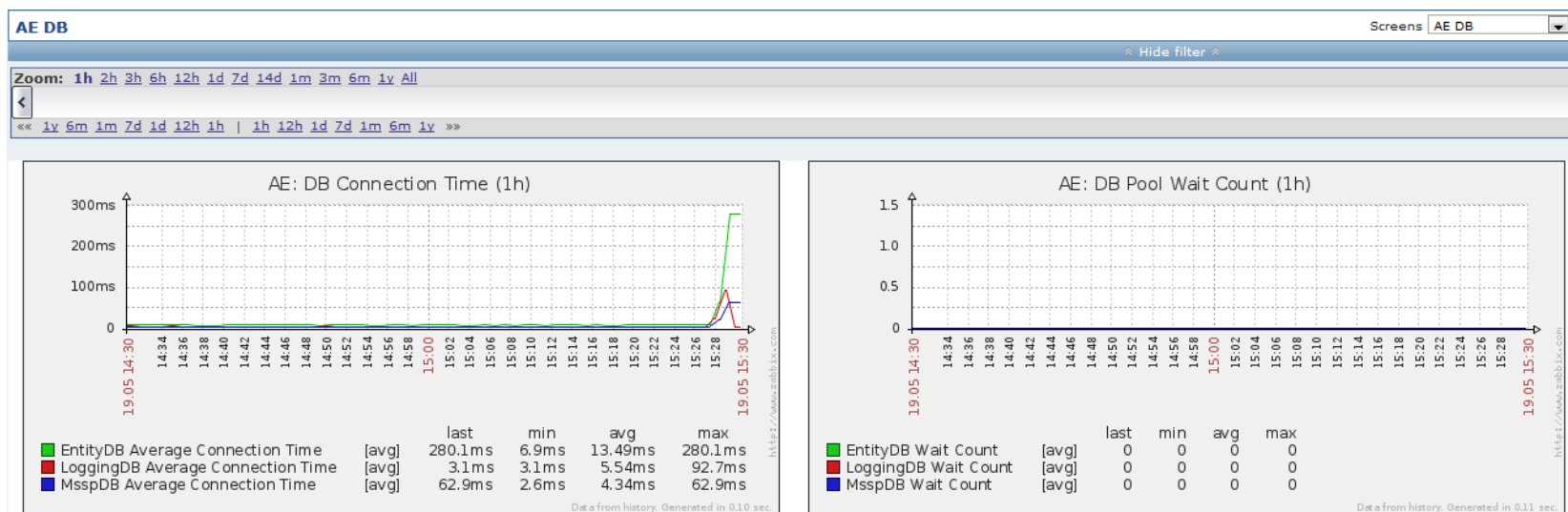
Database Environment Monitoring

Kiuru MSSP 5.0 uses up to 6 different databases.

- Each database can be monitored separately.
- There are more than 10 different monitoring items in each database connection.

Useful monitoring data items are:

- Pool usage
- Query time

Database Environment Monitoring

Service Monitoring

Kiuru MSSP 5.0 implements a Mobile ID service. User experience is the most important aspect of the service.

Useful monitoring data items are:

- Failure counters
- Performance metrics
- Service state

Service Monitoring

ZABBIX

Service State

System status

Host group	Disaster	High	Average	Warning	Information	Not classified
AE	0	0	0	0	0	0
HMSSP	0	0	0	0	0	0
ME	0	0	0	0	0	0

Updated: 15:54:18

Host status

Host group	Without problems	With problems	Total
AE	1	0	1
HMSSP	1	0	1
ME	1	0	1

Updated: 15:54:18

Last 20 issues

Host	Issue	Last change	Age	Info	Ack	Actions
		No events found.				

0 of 0 issues are shown

Updated: 15:54:18

Web monitoring

Host group	Ok	Failed	Unknown
AE	1	0	0
HMSSP	1	0	0
ME	1	0	0

Updated: 15:54:18

What are Triggers and Alerts
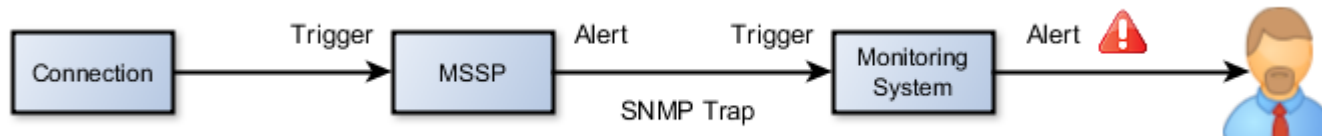
Triggers and alerts are defined in both MSSP and Monitoring system (Zabbix).

- When an MSSP trigger event happens, the MSSP sends an SNMP trap. The SNMP trap is an alert that the MSSP creates.

- When a Monitoring system trigger event happens, the Monitoring system shows a visual effect, sends an e-mail or otherwise tries to alert management personnel.

- Monitoring system's trigger may be an SNMP trap received from an MSSP.

Monitoring System Triggers and Alerts

Monitoring system triggers can be configured to be fired, for example, based on:

- SNMP traps received from MSSP

- Monitoring values exceeding a threshold

- Web service availability probe's response

Each trigger has to be configured separately in the Zabbix configuration.

MSSP SNMP Traps

MSSP can send SNMP traps based on:

1. Connections, which

    - are probed periodically.

    - have monitorable success and failure counters.

2. Adapters, which

    - implement MSSP features.

    - have monitorable success and failure counters.

3. Databases, which

    - are probed periodically.

    - have monitorable success and failure counters.

4. Logs, which

    - have documented error codes.

Monitoring Data Overview

Monitoring data items can be listed using SNMP and JMX commands.

You can browse this data with Zabbix and produce monitoring views you prefer.

The following picture shows a sample of the monitoring data items from AE, HMSSP and ME.

Altogether there are around 100 monitoring data items.

Monitoring Data Overview

ZABBIX

Overview

Hosts location [Top ▼]   Group [MSSP ▼]   Type [Data ▼]

≫ Show filter ≫

Items	AE	HMSSP	ME
Bytes received per second	815.11 Bps	2.63 KBps	0 Bps
Bytes sent per second	4.89 KBps	6.43 KBps	0.1993 Bps
Cluster ID	1	3	3
Cluster Seniority Status	true	true	true
CPU Count	2	2	2
CPU Load	34.46 %	25.64 %	30.83 %
CPU Load Average	0.8	0.8	0.74
Current Threads	77	92	48
Daemon Threads	65	78	36
Device contact details	eemeli	eemeli	eemeli
Device description	Kiuru Platform	Kiuru Platform	Kiuru Platform
Device location	test	test	test
Device name	eemeli-ae	eemeli-hmssp	eemeli-me
Device uptime	03:15:25	02:04:12	02:03:18
Download speed for scenario "Service State".	330 Bps	215 Bps	260 Bps
Download speed for step "Service State" of scenario "Service State".	330 Bps	215 Bps	260 Bps
EntityDB Average Connection Time	7.2ms	7.5ms	0
EntityDB Pool Active	0	0	0
EntityDB Pool Size	10	10	10
EntityDB Total Connections	53	52	0
EntityDB Total Connection Time	380ms	388ms	0
EntityDB Wait Count	0	0	0

Monitoring Data Overview

You can create a map of your MSSP network and systems.

Zabbix shows system states and communication problems.

You can see the system status in a single view.