Zabbix Monitoring

- ZABBIX is an enterprise-class open source database driven distributed monitoring solution.
  - Distributed monitoring
  - Scalability
  - Real-time monitoring
  - Visualisation
  - WEB monitoring
  - Flexibility
  - Agentless monitoring
  - Auto discovery
Zabbix Monitoring

• Support
  – OpenSource Options
    • User Forums (www.zabbix.com/forum)
    • Mailing list
    • IRC support channel
    • The code (written in C, PHP)
  – Commercial Support
    • Zabbix SIA, Riga, Latvia (www.zabbix.com)
      • Annual Support Agreements
      • Turn-key Solutions
      • Technical Account Manager
      • Professional Services
      • 4 levels of annual maintenance.
Zabbix Monitoring

- Operating system support
  - Linux, FreeBSD, NetBSD, OpenBSD
  - AIX HP-UX, MacOS, Solaris, Tru64/OSF, SCO Open Server
  - Win32, Novell Netware.
Zabbix Monitoring

• Database Support
  – MySQL
  – PostgreSQL
  – SQLite
  – Oracle.
Zabbix Monitoring

- Software Requirements (Zabbix ver. 1.4)
  - Apache 1.3.12
  - PHP 4.3
  - MySQL 3.22
  - Oracle 9.0.2.4
  - PostgreSQL 7.0.2
  - SQLite 3.3.5
Zabbix Monitoring

- ZABBIX Components
  - Server
  - Client
  - Web Interface
Zabbix Monitoring

Server

- Main configuration file /etc/zabbix/zabbix_server.conf
- Server processes, zabbix_server runs as user zabbix
- Can host database, web front-end and be a client as well.
- Monitoring Configuration
Zabbix Monitoring

Client

- Main configuration file /etc/zabbix/zabbix_agentd.conf
- Processes, zabbix_agentd run as user zabbix
- Some won't run the Zabbix client.
  - routers
  - webservers
  - POP, IMAP
  - ping
Zabbix Monitoring

- **Item**
  - I just gather data and log it.

- **Trigger**
  - Is that data within my parameters?
  - If not, give it a severity level.

- **Actions**
  - Giving a scenario, I run remote commands or email.

- **Media**
  - Define email, SMS, jabber, or email scripts.
Zabbix Monitoring

Checks (Items), in detail.

- Simple checks
  - agent-less (FTP, mail, http)
- Internal Checks
  - Monitoring internal Zabbix parameters (i.e. how many triggers?)
- External checks
  - shell scripts or binaries
- Aggregated checks
- SNMP
- Zabbix agent checks
  - built-in
  - Custom
Zabbix Monitoring

Zabbix agent checks

- Sample checks that the client can monitor:
  - CPU load
  - Memory
  - Disk (inodes, free, read/write)
  - Files (md5sum, exists, size, regex, time)
  - Network traffic (eth#, lo)
  - number of processes running
  - Agent ping and version.

- User defined
  - Everything else...
Zabbix Monitoring

User defined agent checks

"In order to define a new parameter for monitoring, one line has to be added to configuration file of ZABBIX agent and the agent must be restarted."

UserParameter=ping,echo 1
UserParameter=myscript,/usr/local/bin/critical.sh
UserParameter=mysql.ping,mysqldadmin -uroot ping|grep alive|wc –l
Zabbix Monitoring

Triggers

A Trigger is defined as a logical expression that represents a monitored system state. The expression is recalculated every time Zabbix server receives new value (Item).

- Depending on the configured range or value, assigns it a severity level.
- Dependencies
- Expressions include:
  - Exit codes
  - Echo'd integers
  - Strings
  - Absolute values
  - Averages
  - Sum of values
  - Min/Max for a specified time
  ...and more.
Zabbix Monitoring

**Trigger** severity levels

- Disaster
- High
- Average
- Warning
- Informational
- Not Classified
Zabbix Monitoring

Actions
What a trigger utilizes.

- **Email**
  - Individual
  - Group

- **Scripts**
  - Local or remote script disabled by default
Media Types

Media is a delivery channel for ZABBIX alerts. Several media types can be assigned to a user.

- Email
- SMS (serial modem)
- jabber
- Email scripts (Zabbix passes: Recipient, Subject and Message)
Zabbix Monitoring

- Item
- Trigger
- Action
- Media
- db
- Scripts
- Email
Zabbix Monitoring

Demo time!

- A walk through zabbix_server.conf and zabbix_agentd.conf
- Add a Group
- Add a template
- Add a host
- Show host items and triggers
- Configure a custom item / trigger
- Configure alerts
- Graphs and screens
Zabbix Monitoring

A recent deployment...

- 1,100 monitored hosts
- 86,000 monitoring items
- 35,000 triggers
- 2,400 queries/sec.

• Hardware stats
  - 2 Quad core Xeons (2.00GHz)
  - 8 Gb RAM
  - 1GB NIC
  - MySQL db currently at 120GB, expected to reach 300GB within the year.
Zabbix Monitoring

CPU Loads (31d history)

- Processor load5 [avg] mean:0.83 max:6.39 last:4.002
- Processor load1 [avg] mean:0.24 max:0.74 last:0.803
- Processor load15 [avg] mean:1.72 max:5.63 last:4.22

Generated in 9.75 sec
Zabbix Monitoring

Network utilization (7d history)

Outgoing traffic on interface eth0 (avg) [min:23.02 Kbps max:13.05 Mbps last:96.75 Kbps]
Incoming traffic on interface eth0 (avg) [min:17.22 Kbps max:444.19 Mbps last:126.95 Kbps]
Zabbix Monitoring

Questions?