Drive From ICMP Pings to Enterprise Security

Lukas Macura
CESNET
Silesian University in Opava
Lukas.macura@cesnet.cz

Zabbix Conference 2013, Riga
Contents

- Introduction
- Embedding Zabbix
- Meteo4u – using Zabbix and API
- Managing couple of embedded devices
- Multi-criterial network analysis using Zabbix
- Conclusions
CESNET

- Czech academical network for research
- Includes all public Czech Universities
Silesian University in Opava

- Divided into Karvina and Opava
  - Faculty of Philosophy and Science in Opava
  - School of Business Administration in Karvina
  - Faculty of Public Policies in Opava
  - Institute of Mathematics in Opava
Zabbix on SLU today

• Karvina:
  • Version 2.0.7
  • Works very well
  • Still on mysql. We still want to migrate to postgresql...
  • Huge amount of config and inventory
  • History and trends are copied to backup tables (+40G on disk)
  • **752 active hosts, 37983 active items, 116 new values per second**
  • Big inventory, connected with other systems like obnovang through API.
  • Aproximately 12G of data.
Zabbix on SLU today

- Opava:
  - Version 2.0.6
  - Works very well
  - Mysql
  - 213 active hosts, 3435 active items, 140 new values per second
  - Approximately 14G of data.
Embedding Zabbix agent

- We absolutely need this
- We use Zabbix agent in http://besip.cesnet.cz/
- We are in touch with OpenWrt community
- We sent patches for OpenWrt to upgrade Zabbix to latest version
- `zabbix_agentd` and `zabbix_sender` are working perfectly
Embedding server?

- Do we need to embed zabbix server? (discussion...)
  - We say yes...

- Problem1: With frontend, package is too big
  - We can split localizations (lang specific packages)
  - We can have server without frontend (preconfigured from XML?)

- Problem2: Where to store data and config?
  - Flash is not good for many changes (history,trends)
  - Ram is not good to store config :)
  - We need to store configuration data on flash (maybe import script on each boot?) and history in RAM (cache only?)
  - We need cli import/export
  - In some scenarios, long history is not important. Only actions.
http://Meteo4u.cz

- Community to monitor weather conditions using specialized HW
- Running on relatively slow HW
- Zabbix is used for monitoring and visualization
- **We do not want users to see Zabbix internals**
- **We want high speed and many requests per second**
  - We cache every output of Zabbix
  - Granularity 10min is OK
  - Predefined graphs for 1hour, 1day, 1week and 1month are OK. Cached on disk for simultaneous access
  - Redirected predefined urls to zabbix
Apache config:
AliasMatch /x/last/t$ /var/www/api/lastvalue.php
<LocationMatch ^/x/graphs>
  RewriteEngine on
  RewriteRule /x/graphs/p/1d$ /chart2.php?graphid=93&width=595&period=86400 [P]
  RewriteRule /x/graphs/p/1w$ /chart2.php?graphid=93&width=595&period=604800 [P]
</LocationMatch>
Apache config:
CacheEnable disk /x
<Location /x>
  Header unset Expires
  Header unset Set-Cookie
  RequestHeader unset Cookie
  Header set Cache-Control "max-age=600, must-revalidate"
</Location>
Monitoring couple of devices

- We have lot of devices to manage, configure and monitor
- We hacked preinit and init script of OpenWrt (no need in future, we are working on OpenWrt provisioning system now)

**Firstboot script:**

- Download its configuration from server (tftp, http or https).
- Upgrade is proceeded (sysupgrade, upgrade of specific packages, reboot)
- Zabbix agent registers to zabbix server (autocreate) and sends all informations about itself.
- Every step is logged into zabbix server. So we can setup triggers and actions
- Device can ask zabbix server any time for specific parameters (using API and inventory)
Multi criteria network analysis

- Do you know what happens in your network?
- If you say „yes“, it means you don't know :) 
- How do you want to find incidents, if you do not know what you are searching for? :) 
- You can setup triggers and actions, but YOU are teacher of the system  
- What will happen if teacher does not know any consequencies? 
- In my work, I am trying to solve this 
- Using GNU octave scripts for theoretical part
Statistical analysis

- We need to do statistical analysis over history and trends data
- Maybe we need to „better know“ what happened in trend hours? (only avg, min, max today, linear approximation could help)
- We want to find unique correlations of data
- If something goes wrong, correlations will change
Neural network analysis

- We need to use correlations, triggers and acknowledgements to teach NN
- We need to find abnormalities
- Analysis is „cheap“, we are only analysing data which we have
- We can split analysis into parts
- We can use free CPU time to compute it
Problems to solve..

- Should it be done externally (API, SQL)?
- Or internally (zabbix_server plugin)?
- Huge amount of data – we need to divide it to parts
- Too big threshold will find no abnormalities
- Other side, we have many false positives
- Do we need to store all data?
Conclusions

- Tool for analyzing data externally in Octave will be OSS and will be announced in forum. Anybody can analyze its data.
- Great software, stay on!

- Lukas Macura
- CESNET
- Silesian University in Opava
- Lukas.macura@cesnet.cz