Monitoring system data analysis

Lukas Macura

CESNET

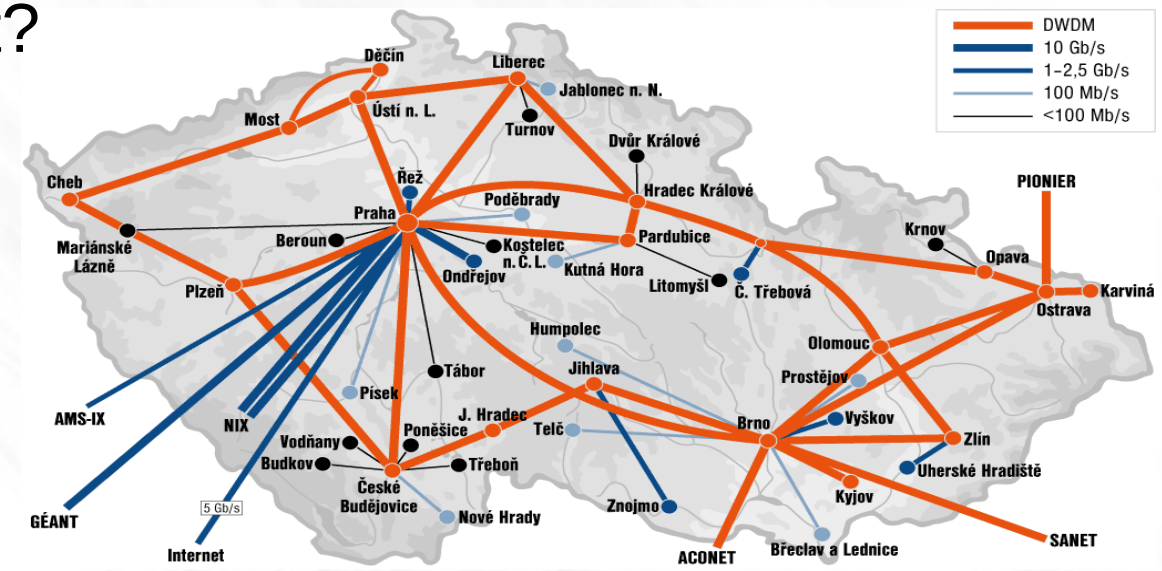
Silesian University in Opava

Lukas.macura@cesnet.cz

Zabbix Conference 2014, Riga

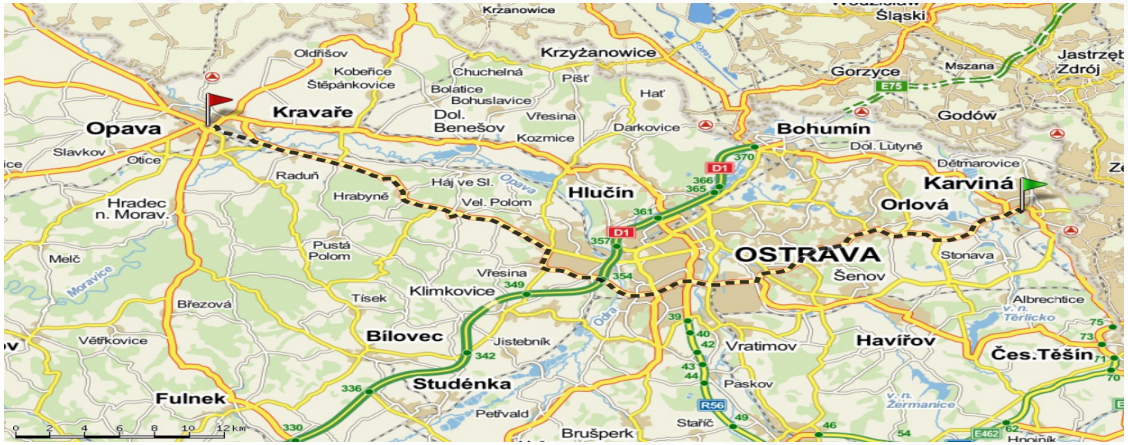
Contents

- Introduction
- What is Monda?
- How it works?
- How to download/configure/install?
- What will be next?
- Conclusions



CESNET & Silesian University

- Czech academical network for research
- Includes all public Czech Universities
- Silesian University is located at Opava&Karvina



Zabbix on SLU today

- Karvina:
- Version 2.2.5
- Works very well
- **Migrated to postgresql!! :)**
- Huge amount of config and inventory
- History and trends are partitioned, all data from 11/2013 included
- **1034 active hosts, 33226 active items, 146 new values per second**
- VmWare monitoring with LLD
- Cisco monitoring with LLD
- Aproximately 240G of data (shared with pdns and nav).

What is Monda?

- System to analyze monitoring data
- It uses SQL/Zabbix API
- It computes overal stats and correlations
- It is GPL :)
- Written in Nette framework
- Can generate CSV and HTML reports
- Will generate maps directly in Zabbix based on reports

How it works?

- Divide history into time windows
- Time window can have more lengths
- In each timewindow, there is analysis of history data (history, history_uint)
- Data are correlated
- Reports are created

TimeWindow

- Similar to trends windows
- Flexible window length
- Include statistics about item history in window
- Found/ignored statistics per window
- Level Of Interrest (**LOI**)

ItemStat

- Similar to trends table
- Item statistics are computed per timewindow
- Min,Max,Avg,Stddev,Cv,Cnt,**LOI**
- More statistics method in future (like derivation of Stddev, probably using pl/r)
- Preprocess phase (find interesting items per timewindow)
- In future, this phase can be part of housekeeper?

ItemCorr

- Item corellations
- Huge number of combinations
- Only items with biggest **LOI** are correlated to reduce CPU and IO
- Correlations:
  - per timewindow
  - Per dayofweek
  - Per hourofday

Results

- Csv reports for item statistics per window
- Csv reports for item correlations
- HTML report for timeline (interresting windows)
- HTML reports for items per window (interresting items)
- HTML item dependency reports (interresting correlations)

Conclusions

- Please test it! :)
- Somebody want to help? For example, to create zabbix map based on reports, ...
- **Zabbix is great software, stay on!**

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

Download/configure/install

- # su -l monda
  $ git clone https://code.google.com/p/monda/
- **Please carrefully read readme.md!!**
  $ cd monda
  $ export PATH=$PATH:$PWD
  $ su postgres
  $ ./misc/db.sh init
- Do not forget to create zabbix user for monda and host group to analyze (monda)

Setting mondarc

- **$ vi ~/.mondarc**

```
--zabbix_api_url 'http://zabbix/api_jsonrpc.php'
--zabbix_api_user monda
--zabbix_api_pw someApiPassword
--za
--zabbix_dsn
'pgsql:host=127.0.0.1;port=5432;dbname=zabbix'
--zabbix_db_user zabbix
--zabbix_db_pw some_password
--zabbix_id 1
--monda_dsn
'pgsql:host=127.0.0.1;port=5432;dbname=monda'
--monda_db_user monda
--monda_db_pw M0nda
```

Usage

```
$ monda tw:create -s yesterday
$ monda tw:show -s yesterday
$ monda tw -xh
$ monda is:compute -s yesterday
$ monda is:show -s yesterday -Ov id -Ov csv
$ monda ic:compute -s yesterday
$ monda ic:show -s yesterday
```

Easy way?

- If you have enough power and you are not afraid of your server ;)

- ```
  $ monda cron:1hour
  $ monda cron:1day
  $ monda cron:1week
  $ monda cron:1month
  $ monda cron:1month -Sc
  ```
  ```