UNINETT's monitoring suite -> Nordunet Moose?

CTO-forum meeting Sept 4 2014 in Espoo

Vidar Faltinsen

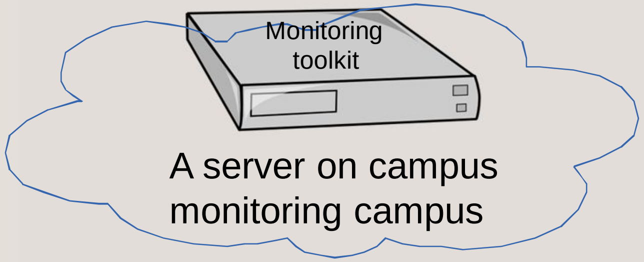
UNINETT

NORDUnet Moose

Monitoring as a Service

UNINETT’s monitoring services

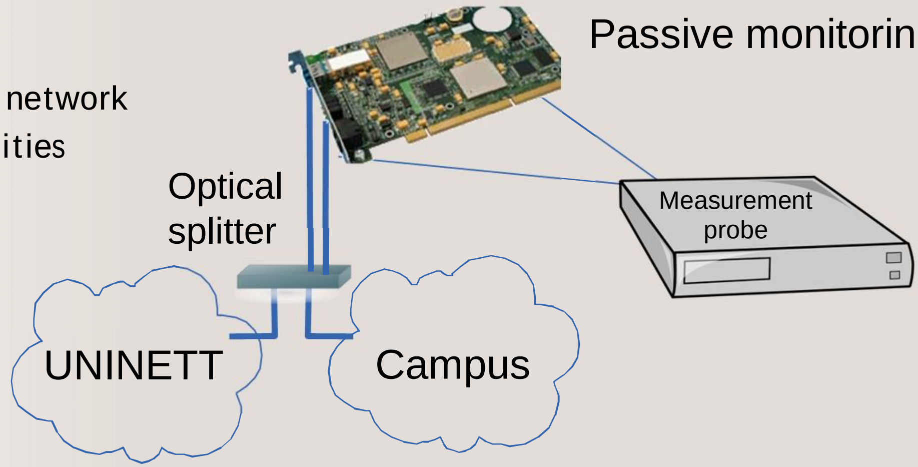
- Offered to our customers since 2005 – almost 10 years (development startet years before that)
- 30 customers – two main services
- **The monitoring toolkit server**
  - Monitor the campus network.



Monitoring toolkit

A server on campus monitoring campus

- **The measurement probe**
  - Passive: Analyze traffic in/out of the campus network
  - Active: Monitor the research network capabilities



Passive monitoring card

Measurement probe

Optical splitter

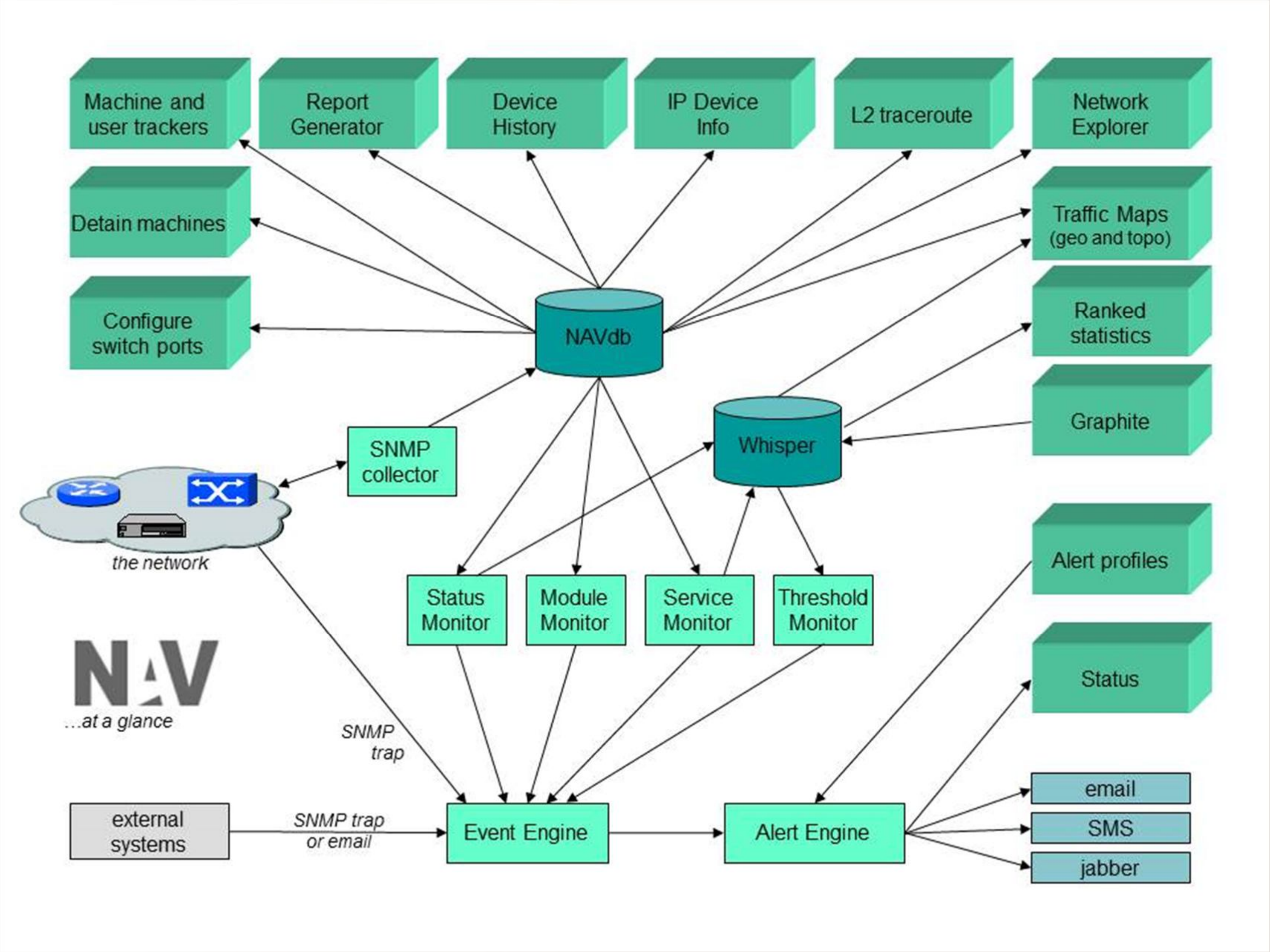
UNINETT

Campus

In-house Open Source Development
(in the monitoring area)

- NAV – developed since 1999
- Appflow / passive monitoring (EU funded)
- Working on an Internet draft for LMAP (Large-Scale Measurement of Broadband Performance)
- Log analysis – Splunk killer (uses Logstash, Elasticsearch, Kibana)
- New project: Mini measurement probe (monitoring on a raspberry pi)

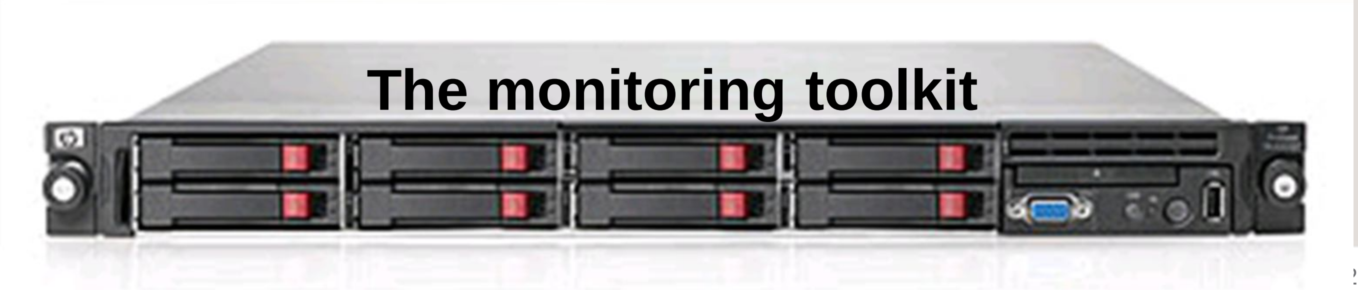
NAV


Machine and user trackers
Report Generator
Device History
IP Device Info
L2 traceroute
Network Explorer
Detain machines
Traffic Maps (geo and topo)
Configure switch ports
NAVdb
Ranked statistics
Graphite
Whisper
SNMP collector
the network
Alert profiles
Status Monitor
Module Monitor
Service Monitor
Threshold Monitor
Status
NAV ...at a glance
SNMP trap
external systems
SNMP trap or email
Event Engine
Alert Engine
email
SMS
jabber

UNINETT

The monitoring toolkit server

- The network management system NAV (the most comprehensive tool in the toolkit)
- The Netflow analysis tool NfSen (including NfDump)
- Application Recognition with Appflow (requires UNINETT's measurement probe in addition)
- The service monitor Xymon (previously Hobbit / Big Brother)
- TFTP setup with RCS revision control for switch and router configuration archive
- Firewall Builder for managing access lists
- Syslog server (for logging from network gear)
- A Radius-based authentication service for routers and switches



Current spec – monitoring toolkit

- HP ProLiant DL360 Gen8 with single Intel Xeon E5-2620 v2 six-core CPU @ 2.1 GHz
- 16 GB memory
- 4x 600 GB SAS disk 10K RPM in a RAID 10 configuration
- Redundant power
- iLO for out of band management console

- For larger institutions (1000 nodes, 40000 ports):

  A cluster of two or even three servers are used.

Operational concept

- Management with CFEngine, soon Puppit
- Maintain debian packages
- Monitoring by UNINETT NOC 24x7
- Spare servers on the shelf

- Resources to operate:
- A new server can be setup in two hours – fully operational
- 1-2 MM per year

Alternatives to physical servers

- Run the monitoring toolkit on an IaaS platform

  Security... SNMP v2c... firewall rules...

  Not on campus...

- Or run it on a VM on campus using the intitutions VM environment

Added value: community building

- Annual monitoring workshops with our community
- Discussions on how to improve management /operations of the campus networks

(Potential) Case: Adopt the service in Sweden

- SUNET promotes the service to your customers

  Included in the SUNET portfolio

- Operations and first line of support by SUNET

  Operational model copied from Norway

- UNINETT develops software, maintain packages

  Collaboration on software development?

- Second line of support by UNINETT

- Promoted as a Nordunet service

Monit**o**ring as a **Se**rvice

UNINETT