Monitoring and alert aggregation

Uninett CNaaS

22nd October 2019

UNINETT

Using NAV for CNaaS monitoring

- NAV = Network Administration Visualized
- Open source network monitoring software
- 20 years of active development in Norway
  - Uninett leads the way

UNINETT

Current service model: NMT

- Network Monitoring Toolkit in production since 2006
- Providing the tooling for campus NOCs to monitor their own network
- CPE based

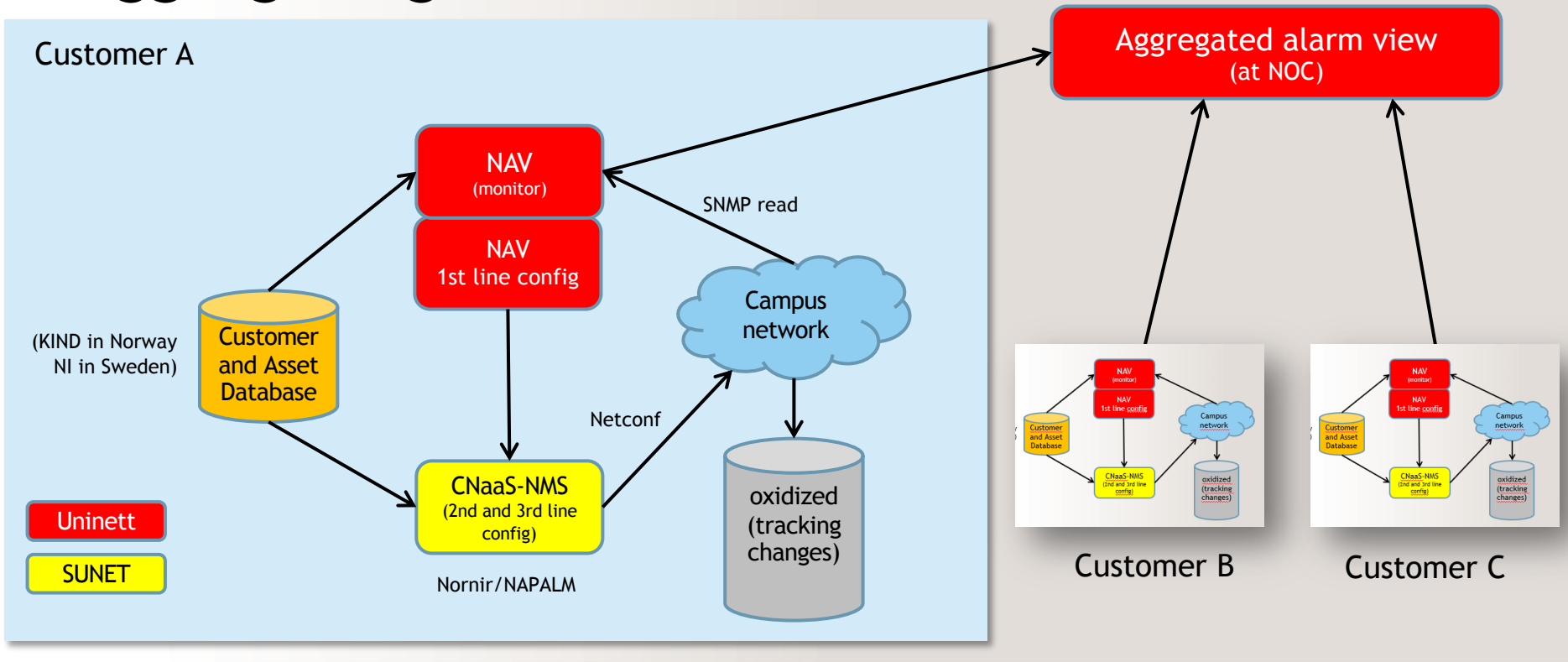
CNaaS monitoring model

- Using NAV is still the obvious choice
- However: No multi-tenancy support in NAV
  - Therefore: 1 instance per customer.

Multi-instance issues

- Method of deployment
  - Hardware, VM, Docker, Kubernetes, NMaaS?
- Access management
  - Local users, LDAP, SSO?
- Alert/notification management

Aggregating alarms



Develop!

- SSO support
- Feature to export all alerts to an aggregator
- Build an aggregator…

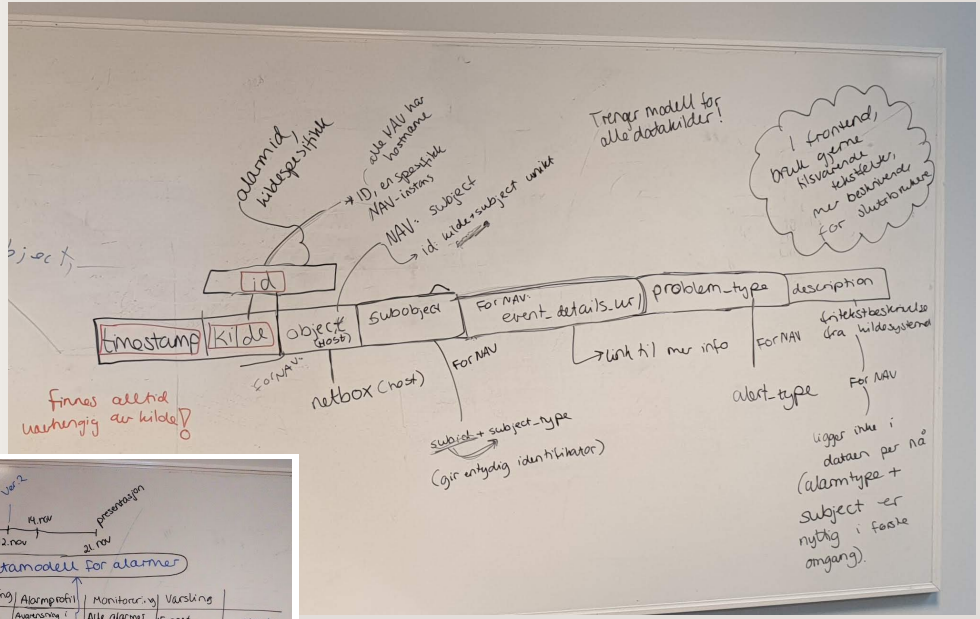
- … in addition to supporting new vendors selected in CNaaS tenders

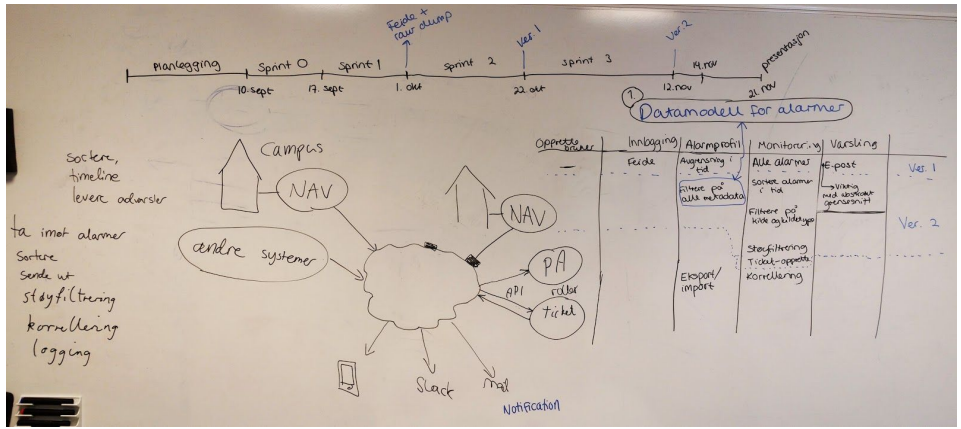
Alert aggregation: A complex task

- Let’s have students do it for free! 😉
- Proposal to the ”Customer Driven Project” course at NTNU’s Computer Science Department
- Accepted and assigned to a group of 6 CS students
  - Self-organized group, with a PhD student as their supervisor and Uninett as their customer

Planning

- Requirements
- Data model
- APIs





Functional requirements

- Functional requirements are inspired by NAV's alert model, such as:
  - Web dashboard with filters
  - Acknowledgements
  - Personal profiles for notifications via e-mail, SMS, Slack etc.

But also:

- Must support multiple source systems and system types
  - Must be able to easily write plugin support for more 3rd party monitoring software
  - Link back to source systems for details
- Integration options for 3rd party ticketing systems
- NAV's alarm profiles UI serves as example of how NOT to do it

Timestamp	Alert ID	Source	Description	Details URL	Object	Parent object	Problem type
2000-01-05T17:...	570605	2	Cqli vydw.	http://x8.nav.no/5...	11	8	10
2000-04-04T13:...	94245	1	Eiccd ave hoqqz ...	http://v7.nav.no/9...	46	8	2
2000-04-09T16:...	621276	2	Xyyusza rtac yf f...	http://x8.nav.no/6...	15	2	4
2000-06-25T22:...	239034	6	Yuoqiv qeqeuyd i...	http://a4.zabbix.n...	10	2	8
2000-08-06T08:...	833255	3	Mbmc yq otsuhy ...	http://e4.nav.no/...	21	5	4
2000-11-21T19:1...	682550	1	Ydxqudwevx row...	http://v7.nav.no/6...	34	6	8
2000-11-29T01:5...	154725	4	Uujkx efbqoway t...	http://r8.zabbix.n...	17	5	4
2001-02-02T13:...	926035	5	Qyf zxlxfc.	http://a8.zabbix.n...	33	7	6
2001-03-08T03:...	714740	3	Vkxwvlaa lmdnp l...	http://e4.nav.no/7...	46	9	2
2001-03-17T11:2...	761154	5	Lbe yi zntqooxp ...	http://a8.zabbix.n...	38	1	8
2001-10-23T14:...	621079	3	Oz nduepfz mqkf...	http://e4.nav.no/...	28	8	8
2001-10-28T05:...	600656	5	Vw cnhzhvl lo tzs...	http://a8.zabbix.n...	18	8	1
2001-11-21T08:1...	34501	5	Zaxwhvpgt wfw ...	http://a8.zabbix.n...	17	10	9
2002-05-17T08:...	285266	3	Jnoaworuvk hy ct...	http://e4.nav.no/2...	32	2	8
2002-05-18T13:...	255089	6	Gsrsvnaov wux.	http://a4.zabbix.n...	43	1	9
2002-08-12T04:...	214600	6	Grhtyq tqnfdfykl ...	http://a4.zabbix.n...	26	2	2
2002-08-30T14:...	193212	2	Mu acockmq uxc...	http://x8.nav.no/1...	4	9	8

Non-functional requirements

- Must be open-source
- Must use toolchain familiar to us
  - PostgreSQL
  - Python
  - Django
  - Django REST Framework
  - GitHub

So long, and thanks for all the fish!

- Morten Brekkevold
  Senior Systems Developer

- E-Mail: morten.brekkevold@uninett.no

- https://nav.uninett.no/