

Argus - Aggregated Alarm Console

Morten Brekkevold

NEMMO - 24.03.2021

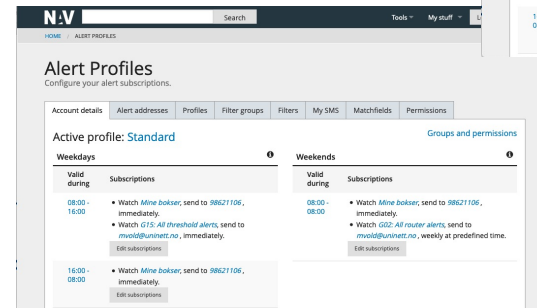
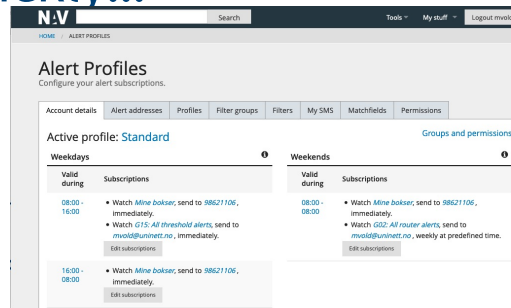
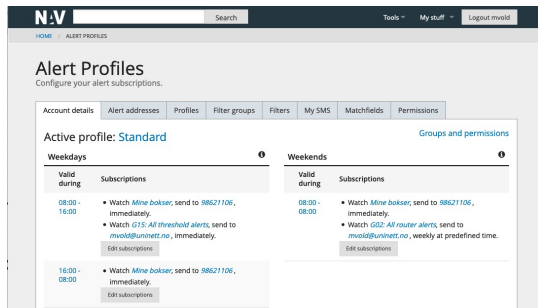
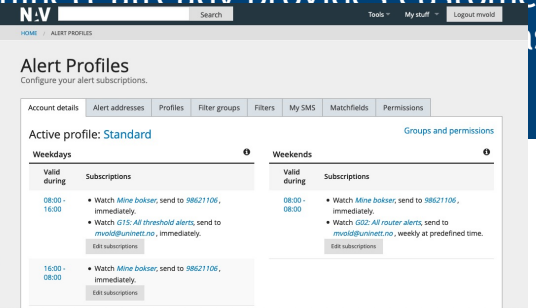
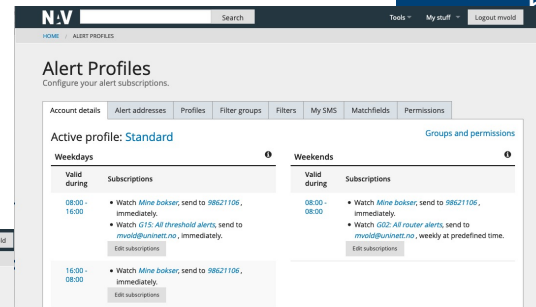
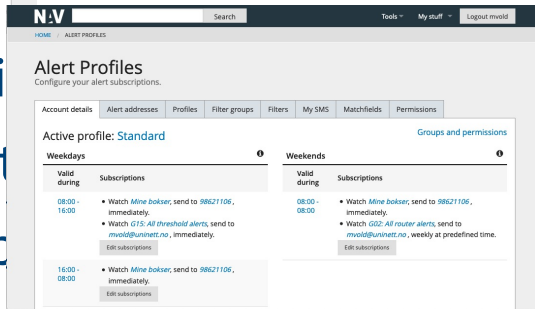
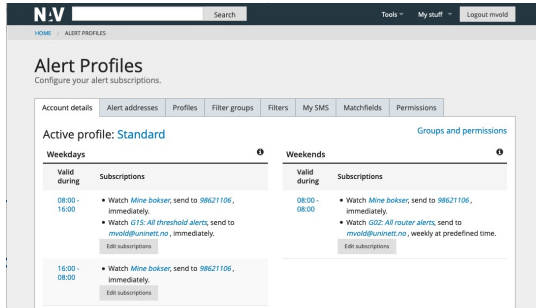
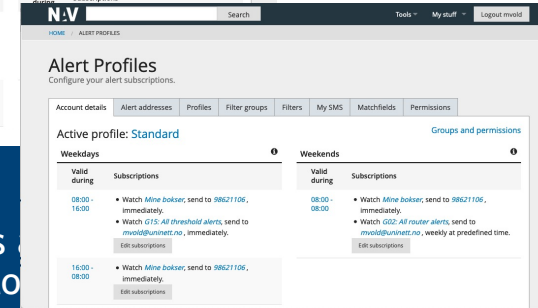
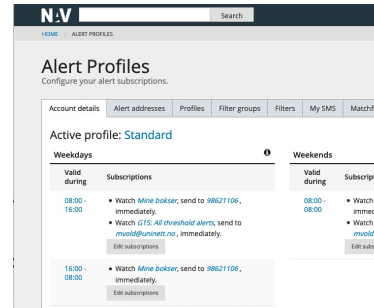
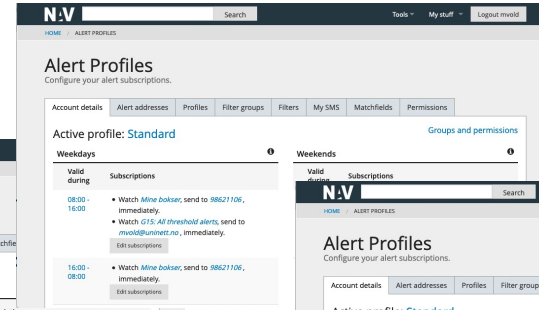
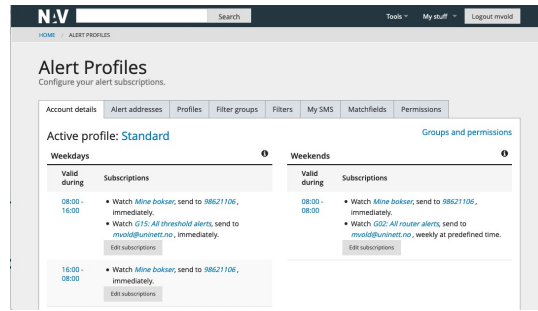
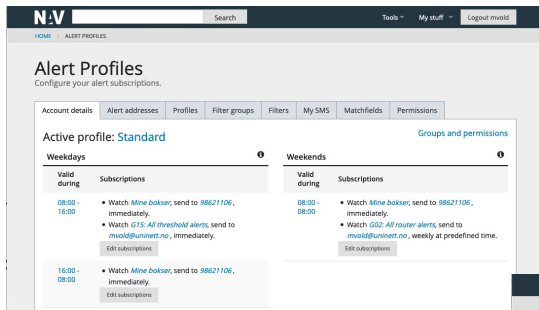
UNINETT

Alerts, alerts, alerts!

- ▶ Uninett CNaaS will use NAV for monitoring
- ▶ NAV is **not** multi-tenant
- ▶ One installation per customer is needed

- ▶ Gets unwieldy pretty quickly...

1. NAV is an open source campus network monitoring tool with a 21 year long history in the Norwegian HE sector.
2. NAV is developed by Uninett.
3. Uninett already provides customers with network management services based on NAV.



➤ Uninett CaaS with

Multi-tenancy
on platform

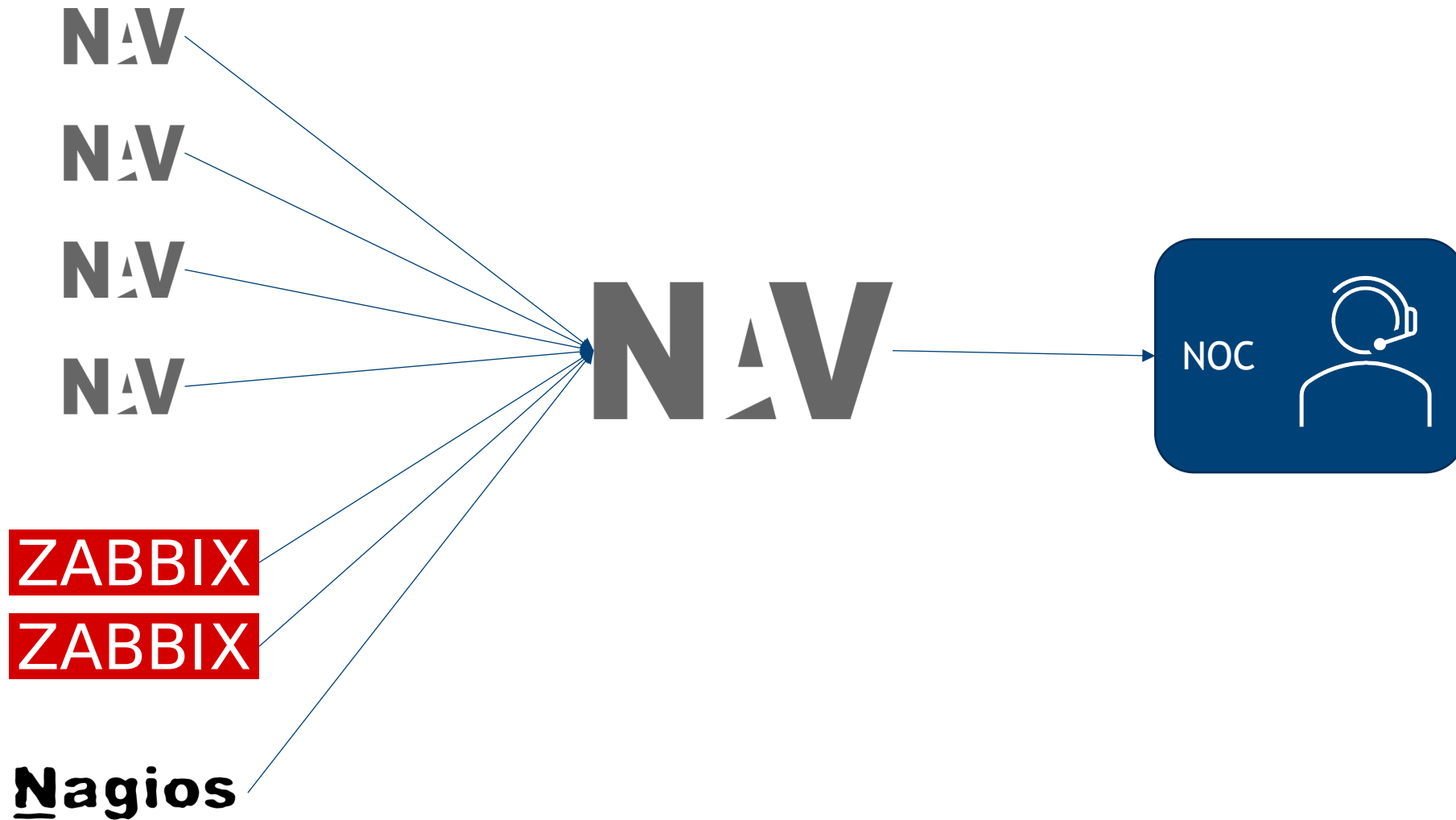
very pretty quickly...

ing

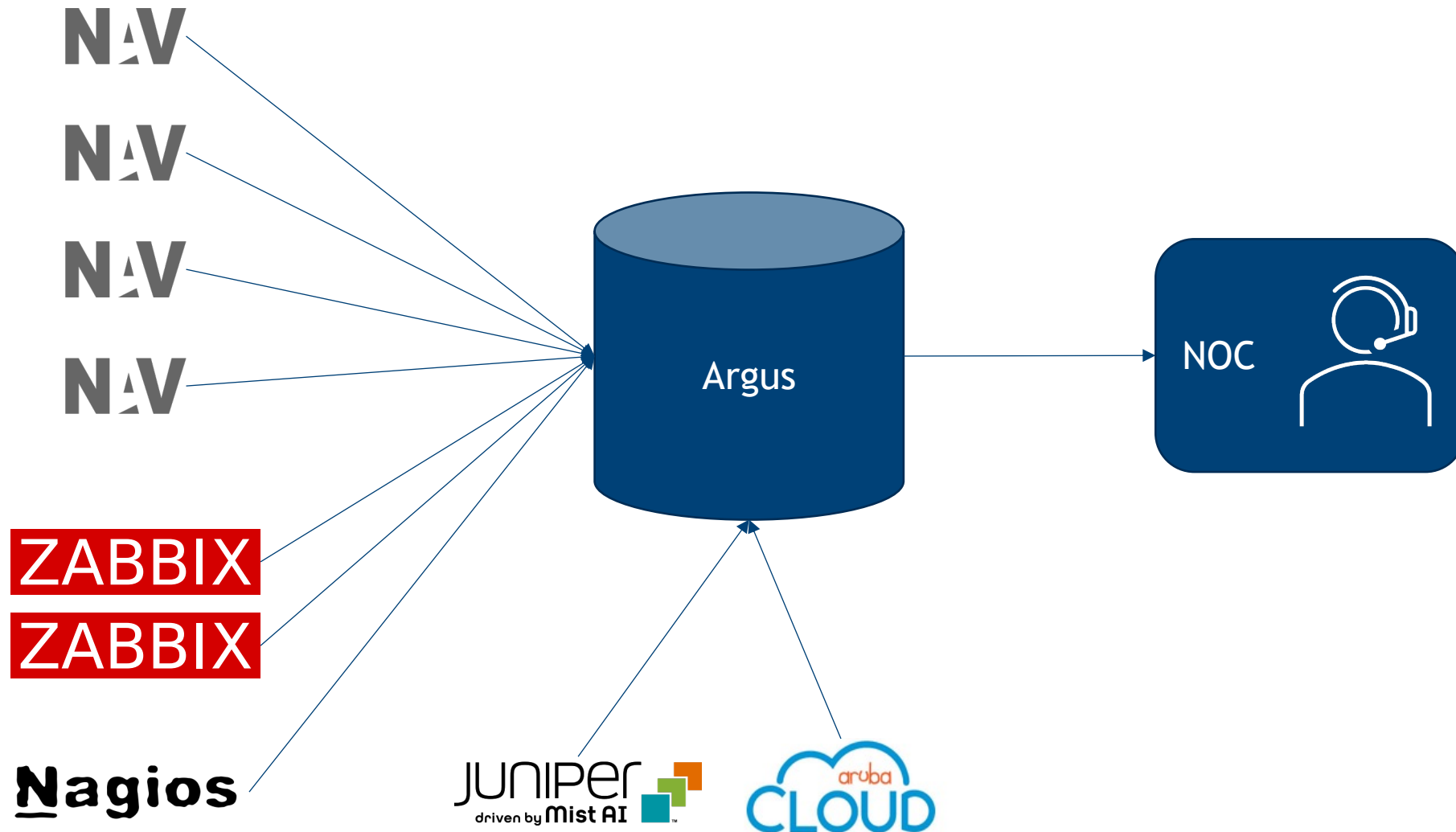
NAV is monitoring
history in the Norwegian HE sector.
NAV is developed by Uninett.

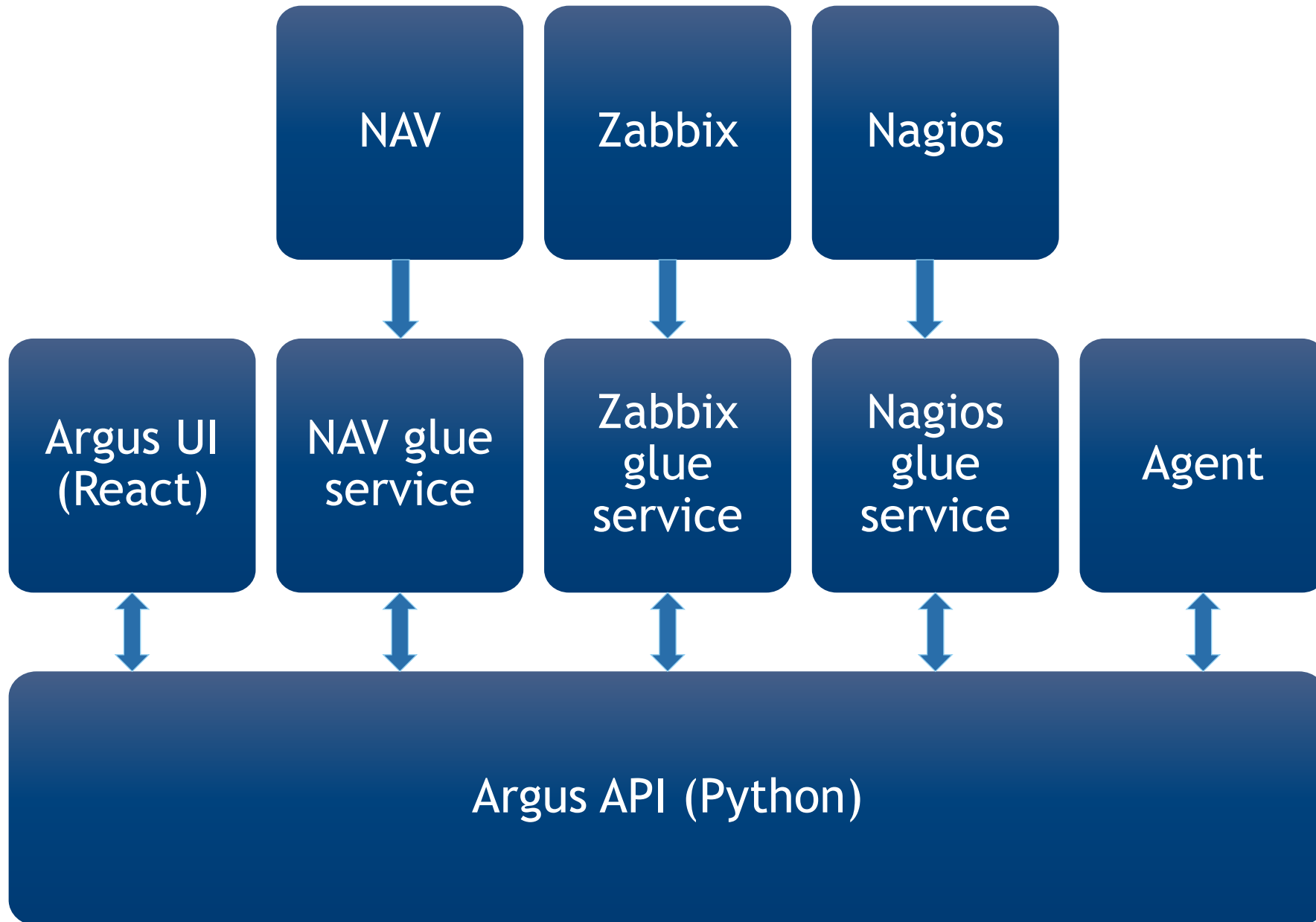
Uninett already provides customers with
based on

Idea 1: Re-use NAV



Idea 2: Something new!







INCIDENTS

FILTERS

TIMESLOTS

PROFILES



Admin

Open State

Acked

Sources

Tags

Filter

OPEN

CLOSED

BOTH

UNACKED

BOTH

CNaaS



Select from your filters

| Timestamp | Status | Source | Description | Actions |
|---------------------|--|----------------------------|---|---------|
| 3/24/2021, 07:55:05 | Open Non-acked | mobility-master.uninett.no | AP down: ap345-f5:1e at Teknobyen | |
| 3/22/2021, 15:00:48 | Open Acked | lokalnav.uninett.no | box down teknobyen-5etg-sw2.uninett.no 158.38.129.52 | |
| 3/9/2021, 17:35:14 | Open Non-acked | lokalnav.uninett.no | PSU not OK on cessda-gsw1.c.uninett.no (PEM 1) | |
| 8/3/2020, 15:12:56 | Open Acked | unit-vk.c.uninett.no | 2001:700:5701::2 BGP session with 158.36.4.14 is DOWN | |
| 4/1/2020, 09:14:33 | Open Acked | lokalnav.uninett.no | Service ssh on buick.lab.uninett.no is down since 2020-04-01 09:14:33 | |

Rows per page: 10

1-5 of 5



Last refreshed 10:41:11, updating every 30

Status

Open

Acknowledged

Ticket <https://rt.uninett.no/Ticket/Display.html?id=226759>

Tags

event_type=bgpState

alert_type=bgpDown

kunde=unit.no

host=2001:700:5701::2

room=Teknobyen-5etg-sør

location=unittrd

kundetjeneste=Campus_CNaaS

Primary details (#1296)

Description

2001:700:5701::2 BGP session with 158.36.4.14 is DOWN

Start time

8/3/2020, 15:12:56

Duration

8 months

Source

unit-vk.c.uninett.no

Details URL

<https://unit-vk.c.uninett.no/search/event/334>

Ticket

<https://rt.uninett.no/Ticl>

EDIT 

CLOSE INCIDENT

Acknowledgements

RT 226759

gjewig@uninett.no 11/25/2020, 08:22:02

CREATE ACKNOWLEDGMENT

Related events

Incident start

2001:700:5701::2 BGP session with 158.36.4.14 is DOWN

unit-vk.c.uninett.no 8/3/2020, 15:12:56

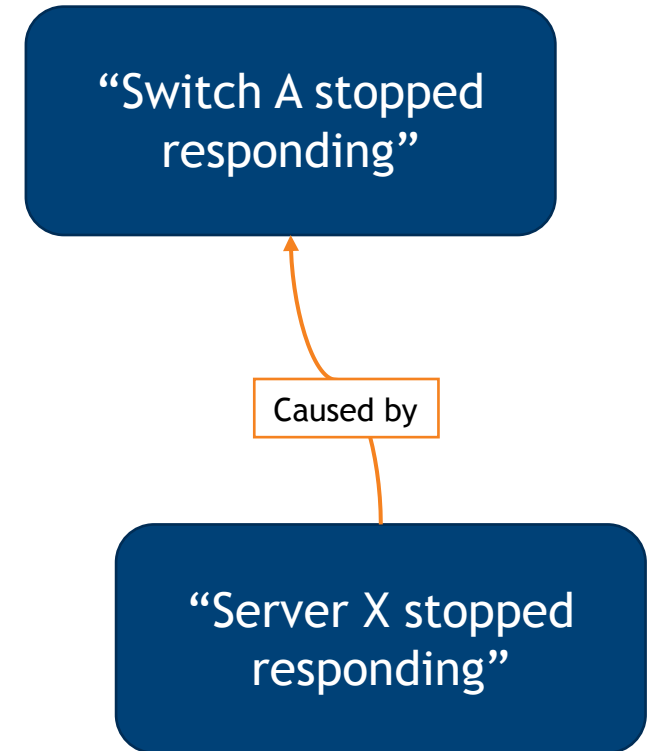
Notifications

Active: Timeslots: On Duty | v Filtername: CNaaS boxDown x | v Media: SMS x | v Phone number: +4799999999 | v

- Each user can configure a personal notification profile
 - Filters define which alerts are interesting
 - Timeslots decide when notifications are desirable
- E-Mail and SMS notifications are supported
- More mediums will come:
 - Slack
 - Teams

Incident relationships

- ◆ Incidents may be related, somehow...
 - "Same root cause"
 - "Same issue reported by two separate source systems"
 - "One issue is caused by the other"
- ◆ These relations can be added
 - Manually (although, not quite yet)
 - By an external agent



Argus status, March 2021

- ◆ Argus is already being used in production at Uninett, with 4 CNaas customers
- ◆ We are currently in the process of writing glue services for
 - Zabbix
 - Zino
- ◆ We are currently testing glue services for:
 - Mist AI (Juniper's cloud-based control plane for WiFi APs)
 - Aruba Mobility Master (Aruba's cloud-based control plane for WiFi Aps)
- ◆ These glue services all use the existing Python API access library

Argus going forward...

- ◆ Implementing severity level as a core attribute
- ◆ Improving the filter implementation
- ◆ Improving the notification implementation
- ◆ Actual integration with our ticketing system (Request Tracker)

- ◆ And, a lot of work deciding what should be mapped to incidents, and how...

Argus is free software

- ▶ It's paid for by Géant!
- ▶ You can try it out!
- ▶ You can contribute!
- ▶ Got questions? Get in touch!

opensource@uninett.no

References

- ▶ <https://argus-server.readthedocs.io/en/latest/>
- ▶ <https://github.com/Uninett/Argus>
- ▶ <https://github.com/Uninett/Argus-frontend>
- ▶ <https://github.com/Uninett/pyargus>

- ▶ <https://github.com/Uninett/nav-argus-glue>
- ▶ <https://nav.uninett.no/>



@Uninett



@Uninett



Uninett



uninett.no