

Argus

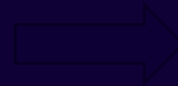
- an alarm aggregation and correlation tool

Vidar Faltinsen

Product manager, Sikt

27th STF – Zürich, October 20th

1993 – 2021






















2022 ->



Norwegian Agency for Shared Services
in Education and Research

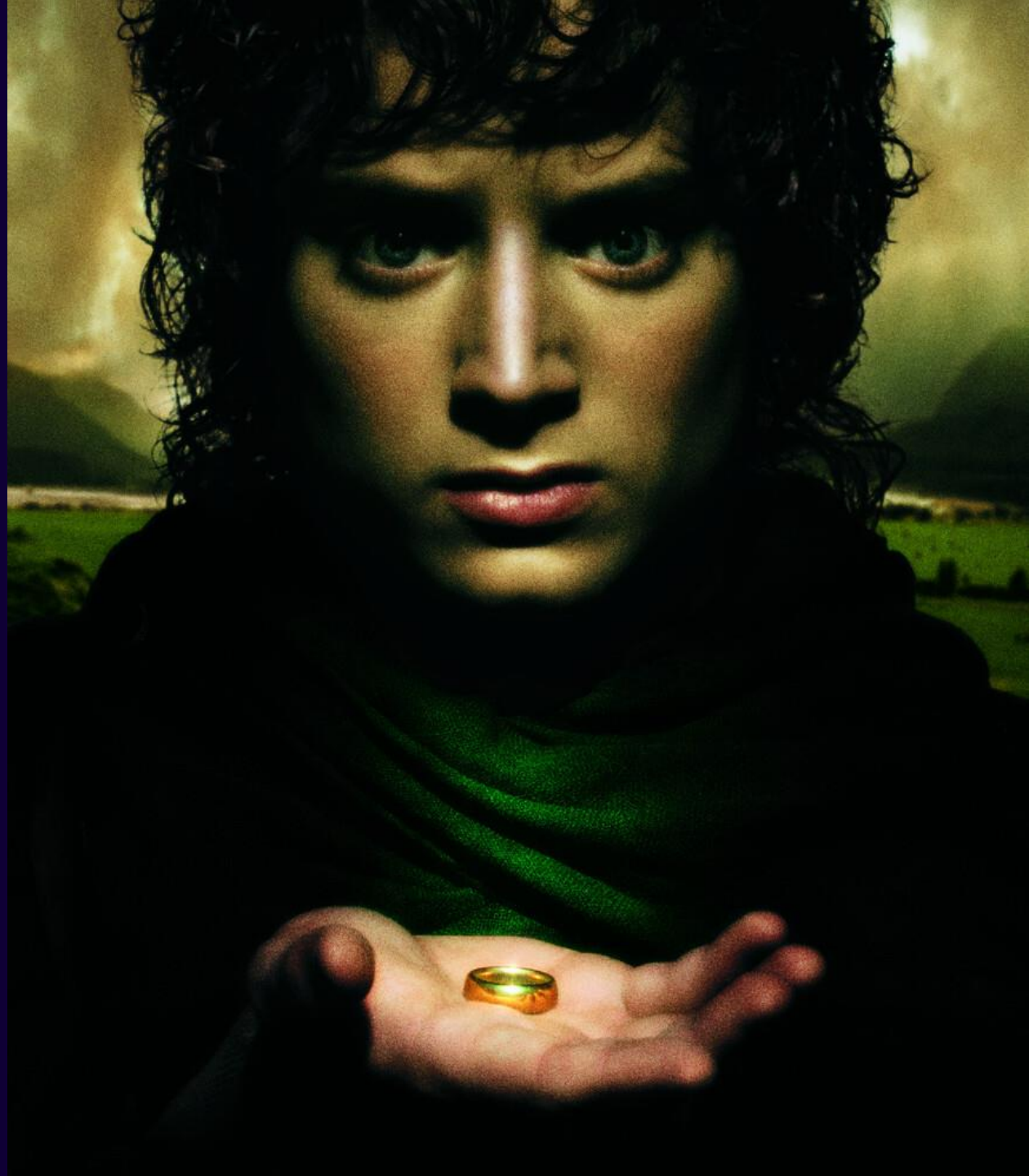
A story from our NOC in Trondheim...





One Screen To Display Them All



Argus - an alarm aggregation and correlation tool

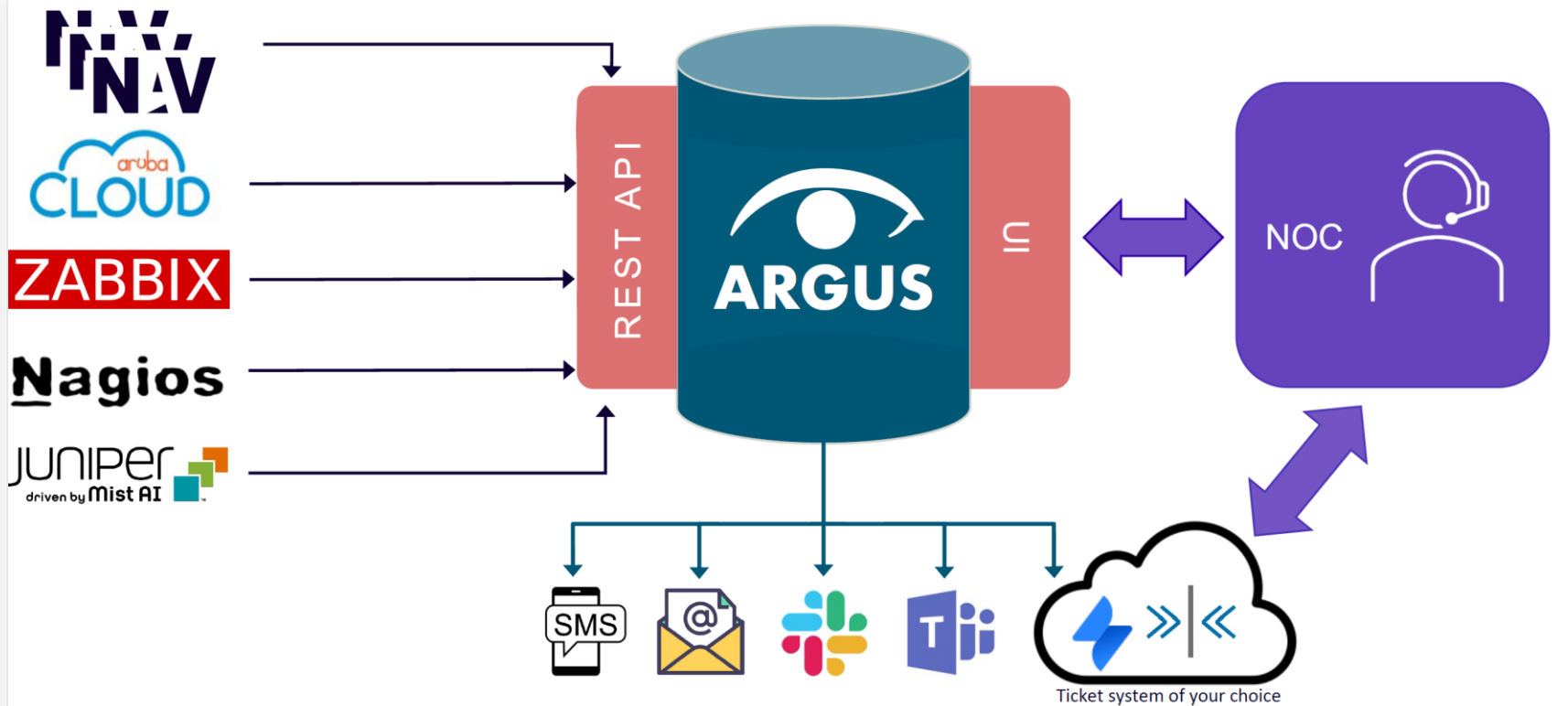
The screenshot shows the Argus Main dashboard. At the top, there is a dark blue header with the ARGUS logo on the left and 'N NOC' on the right. Below the header, there are three main navigation buttons: 'INCIDENTS' (active), 'TIMESLOTS', and 'PROFILES'. The dashboard is divided into several sections: 'Open State' with buttons for 'OPEN', 'CLOSED', and 'BOTH'; 'Acked' with buttons for 'ACKED', 'UNACKED', and 'BOTH'; 'Sources' with a search box and a note 'Press enter to add new source'; 'Tags' with a search box containing 'service=Campus_CNaaS' and a note 'Press enter to add new tag'; and 'Max level' with a dropdown menu set to '5 - Information'. Below these is a 'Filter' section with a search box and icons for adding, deleting, and settings. The main part of the dashboard is a table titled 'Incidents' with columns for 'Timestamp', 'Status', 'Severity level', 'Source', 'Description', and 'Actions'. The table contains five rows of incident data.

Timestamp	Status	Severity level	Source	Description	Actions
2022-04-28 09:56	Open Non-acked	3 - Moderate	nav.customer1.example.org	box down example-sw.customer1 192.168.42.42	[Icon]
2022-04-27 11:42	Open Non-acked	4 - Low	mobility-master.example.org	AP down: AP 1553 at somecollege	[Icon]
2022-04-02 13:12	Open Acked	1 - Critical	nav.customer1.example.org	box down main-gsw.customer1 192.168.0.1	[Icon]
2022-04-02 09:32	Open Acked	3 - Moderate	nav.someschool.example.org	nav.devices.holophonor-sw1_someschool.sensors.xe-1_2_2_jnxDomCurrentRxLaserPower exceeded at -37.32 <-14	[Icon]
2022-04-02 08:32	Open Acked	2 - High	zabbix.example.org	slurm.example.org: Software RAID: Device md0 is active,degraded	[Icon]

Main dashboard

The screenshot shows the Argus Incident details for incident #23629. It features a 'Tags' section with several key-value pairs: room=100, location=Teknobyen Innovasjonsenter, alert_type=boxDown, event_type=boxState, host_url=/ipdevinfo/temp-serverrom.example.org/, host=temp-serverrom.example.org, kunde=example.org, organization=sikt.srv, and kundetjeneste=Campus_CNaaS. Below the tags is the 'Primary details (#23629)' section, which includes: 'Description' (box down temp-serverrom.example.org 10.0.42.250), 'Start time' (2022-04-13 12:00:10), 'Duration' (6 days), 'Source' (NAV), and 'Details URL' (<https://nav.example.org/search/event/205047>). At the bottom, there is a 'Ticket' section with the URL <https://rt.example.org/1>.

Incident details



Flexible setup of your alarm profile

- ✓ For a given filter match...
- ✓ ... in a defined time slot
- ✓ ... send alarm on preferred channel

Two way integration with ticket system of your choice

- ✓ Create new ticket from Argus
- ✓ Argus incident links to ticket
- ✓ Ticket links to argus

Implemented support for:

- ✓ RT, Jira, GitHub, GitLab

- ✓ Agnostic to details in the underpinning monitoring applications
- ✓ Easy to integrate with new monitoring systems
- ✓ Concept of glue services

- ✓ Classifies incidents in severity levels (1-5)
- ✓ Can be tagged with arbitrary metadata
- ✓ Can include URLs to source application to explore more details

Argus – a GÉANT production service
Open source – developed by Sikt
<http://network.geant.org/argus/>



Argus - an alarm aggregation and correlation tool

The screenshot shows the Argus Main dashboard. At the top, there is a dark blue header with the ARGUS logo on the left and 'N NOC' on the right. Below the header, there are three main navigation buttons: 'INCIDENTS' (active), 'TIMESLOTS', and 'PROFILES'. The dashboard is divided into several sections: 'Open State' with buttons for 'OPEN', 'CLOSED', and 'BOTH'; 'Acked' with buttons for 'ACKED', 'UNACKED', and 'BOTH'; 'Sources' with a search box and a note 'Press enter to add new source'; 'Tags' with a search box containing 'service=Campus_CNaaS' and a note 'Press enter to add new tag'; and 'Max level' with a dropdown menu set to '5 - Information'. Below these is a 'Filter' section with a search box and icons for adding, deleting, and settings. The main content area is titled 'Incidents' and contains a table with the following data:

Timestamp	Status	Severity level	Source	Description	Actions
2022-04-28 09:56	Open Non-acked	3 - Moderate	nav.customer1.example.org	box down example-sw.customer1 192.168.42.42	[Action icon]
2022-04-27 11:42	Open Non-acked	4 - Low	mobility-master.example.org	AP down: AP 1553 at somecollege	[Action icon]
2022-04-02 13:12	Open Acked	1 - Critical	nav.customer1.example.org	box down main-gsw.customer1 192.168.0.1	[Action icon]
2022-04-02 09:32	Open Acked	3 - Moderate	nav.someschool.example.org	nav.devices.holophonor-sw1_someschool.sensors.xe-1_2_2_jnxDomCurrentRxLaserPower exceeded at -37.32 <-14	[Action icon]
2022-04-02 08:32	Open Acked	2 - High	zabbix.example.org	slurm.example.org: Software RAID: Device md0 is active,degraded	[Action icon]

Main dashboard

The screenshot shows the Argus Incident details for incident #23629. It features a 'Tags' section with several key-value pairs: room=100, location=Teknobyen Innovasjonsenter, alert_type=boxDown, event_type=boxState, host_url=/ipdevinfo/temp-serverrom.example.org/, host=temp-serverrom.example.org, kunde=example.org, organization=sikt.srv, and kundetjeneste=Campus_CNaaS. Below the tags is the 'Primary details (#23629)' section, which includes: 'Description: box down temp-serverrom.example.org 10.0.42.250', 'Start time: 2022-04-13 12:00:10', 'Duration: 6 days', 'Source: NAV', and 'Details URL: https://nav.example.org/search/event/205047'. At the bottom, there is a 'Ticket' section with the URL: https://rt.example.org/1.

Incident details

Interesting?

Join an Argus infoshare on Mon Nov 28 14-15

- ✓ Live demo
- ✓ How to get started
- ✓ How to implement a glue service I need
- ✓ Q & A

Vidar.Faltinsen@sikt.no

Morten.Brekkevold@sikt.no

argus@lists.geant.org