ZINO 2.0

THE RESEARCH NETWORK STATE MONITOR

Morten Brekkevold

Sikt

20th SIG-NOC, Helsinki 2024-05-08

WHAT IS ZINO?

WHAT IS ZINO?

- Zino Is Not Openview

WHAT IS ZINO?

- Zino Is Not Openview
  - HP OpenView is/was a behemoth. Zino is not.

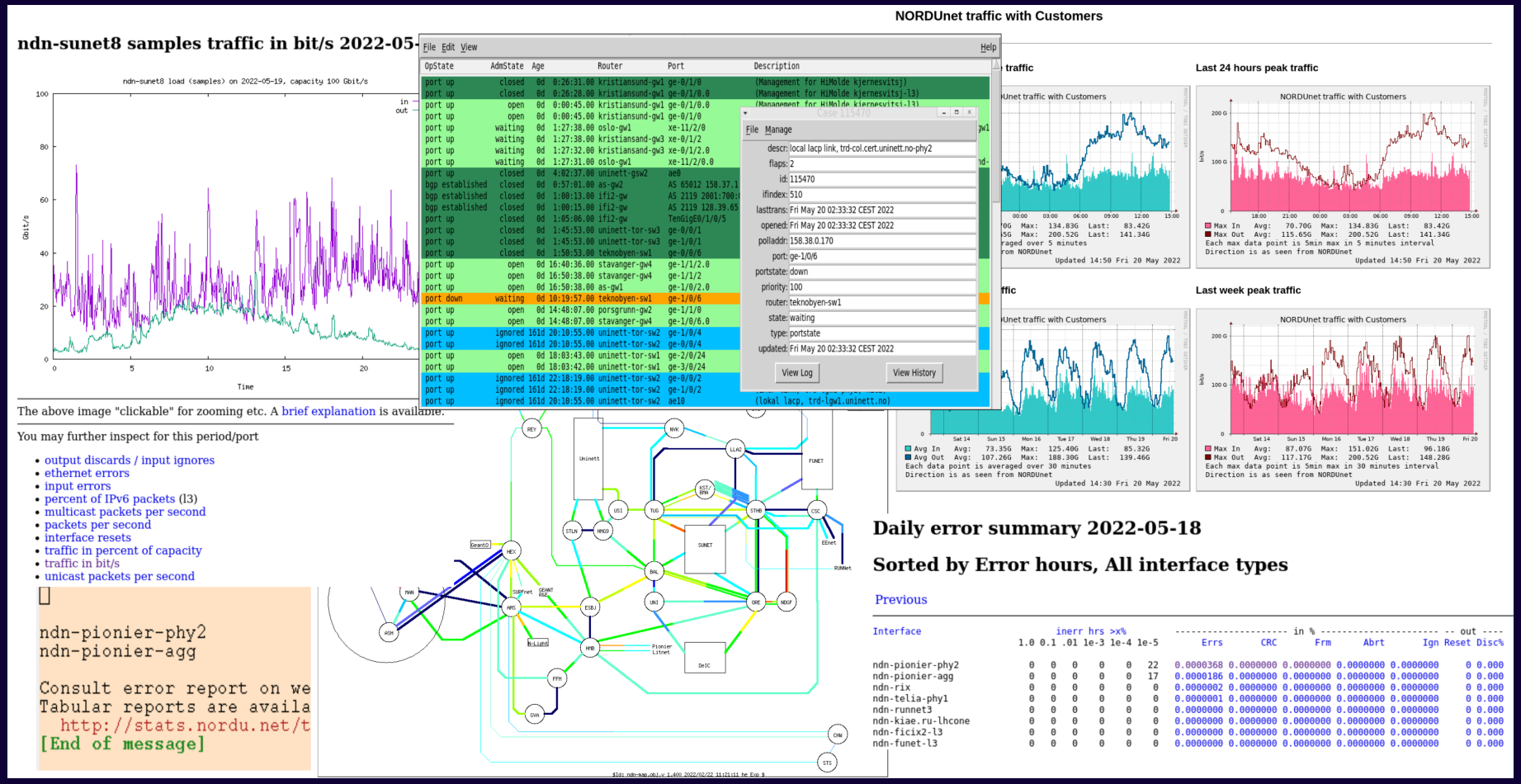
WHAT IS ZINO?

- Zino Is Not Openview
  - HP OpenView is/was a behemoth. Zino is not.
  - (Recursive acronyms are fun!)

WHAT IS ZINO?

- Zino Is Not Openview
  - HP OpenView is/was a behemoth. Zino is not.
  - (Recursive acronyms are fun!)
- A toolset that has monitored Nordic research networks for **nearly 30 years**

ZINO SUITE COMPONENTS



BACK-END COMPONENTS (SNMP)

- Zino state monitor
  - With accessible API to inspect and modify events
- Traffic poller (tpoll)
- Shared Tcl libraries in original implementation

THE STATE MONITOR

Trap-directed SNMP polling:

THE STATE MONITOR

Trap-directed SNMP polling:

- Router reachability

THE STATE MONITOR

Trap-directed SNMP polling:

- Router reachability
- Interface link state

THE STATE MONITOR

Trap-directed SNMP polling:

- Router reachability
- Interface link state
- BGP peering state

THE STATE MONITOR

Trap-directed SNMP polling:

- Router reachability
- Interface link state
- BGP peering state
- BFD session state

THE STATE MONITOR

Trap-directed SNMP polling:

- Router reachability
- Interface link state
- BGP peering state
- BFD session state
- Juniper chassis alarms

THE STATE MONITOR API

- Text-based, stateful API (similar to SMTP)
- Provides:

THE STATE MONITOR API

- Text-based, stateful API (similar to SMTP)
- Provides:
  - Insight into ongoing network events

THE STATE MONITOR API

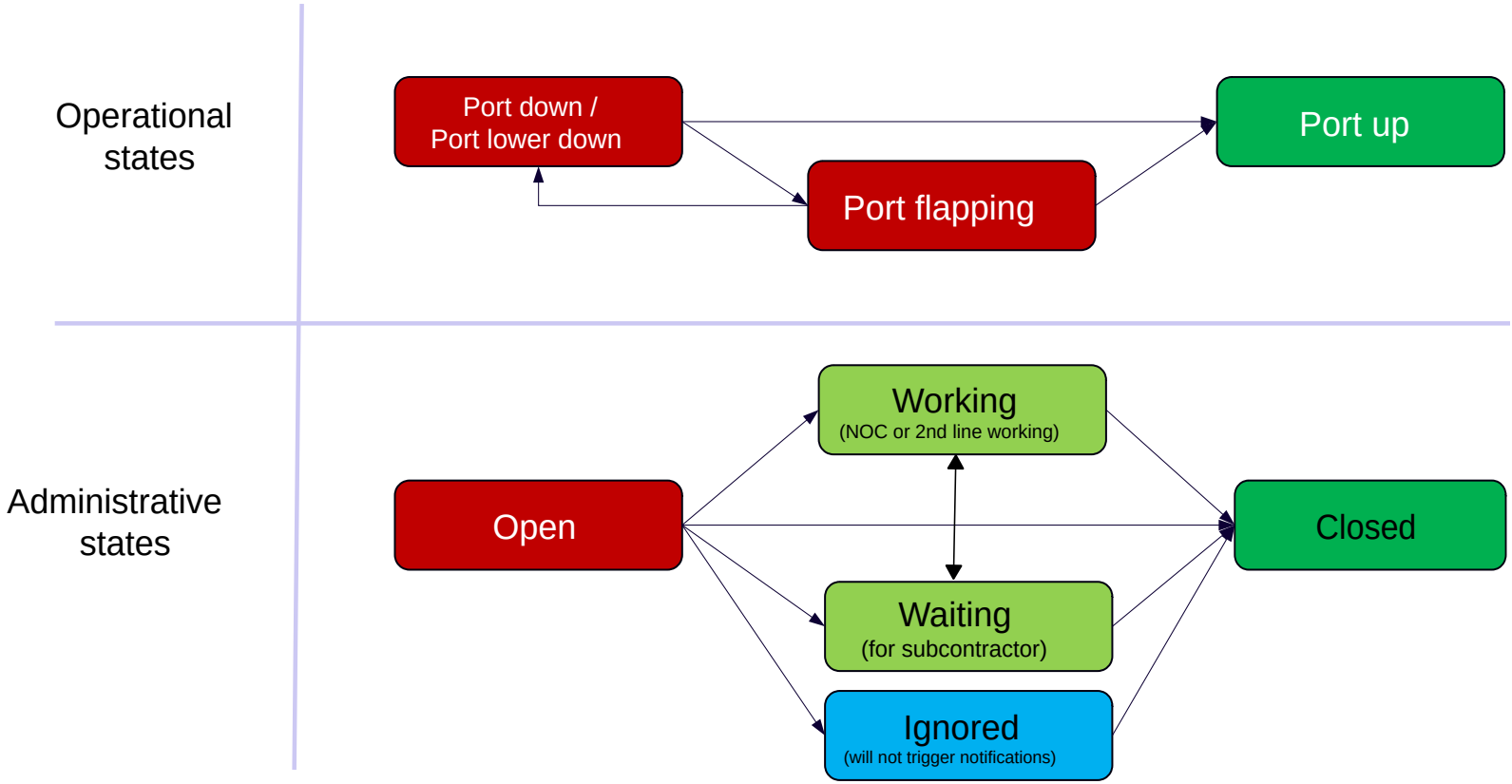
- Text-based, stateful API (similar to SMTP)
- Provides:
  - Insight into ongoing network events
  - Administrative management of events

THE STATE MONITOR API

- Text-based, stateful API (similar to SMTP)
- Provides:
  - Insight into ongoing network events
  - Administrative management of events
  - Realtime notifications of event changes

ZINO EVENT STATES

Deliberate separation of operational and administrative states



TRAFFIC STATS

- Also part of legacy Zino suite:
  - Traffic stats
  - Error reports from stats data

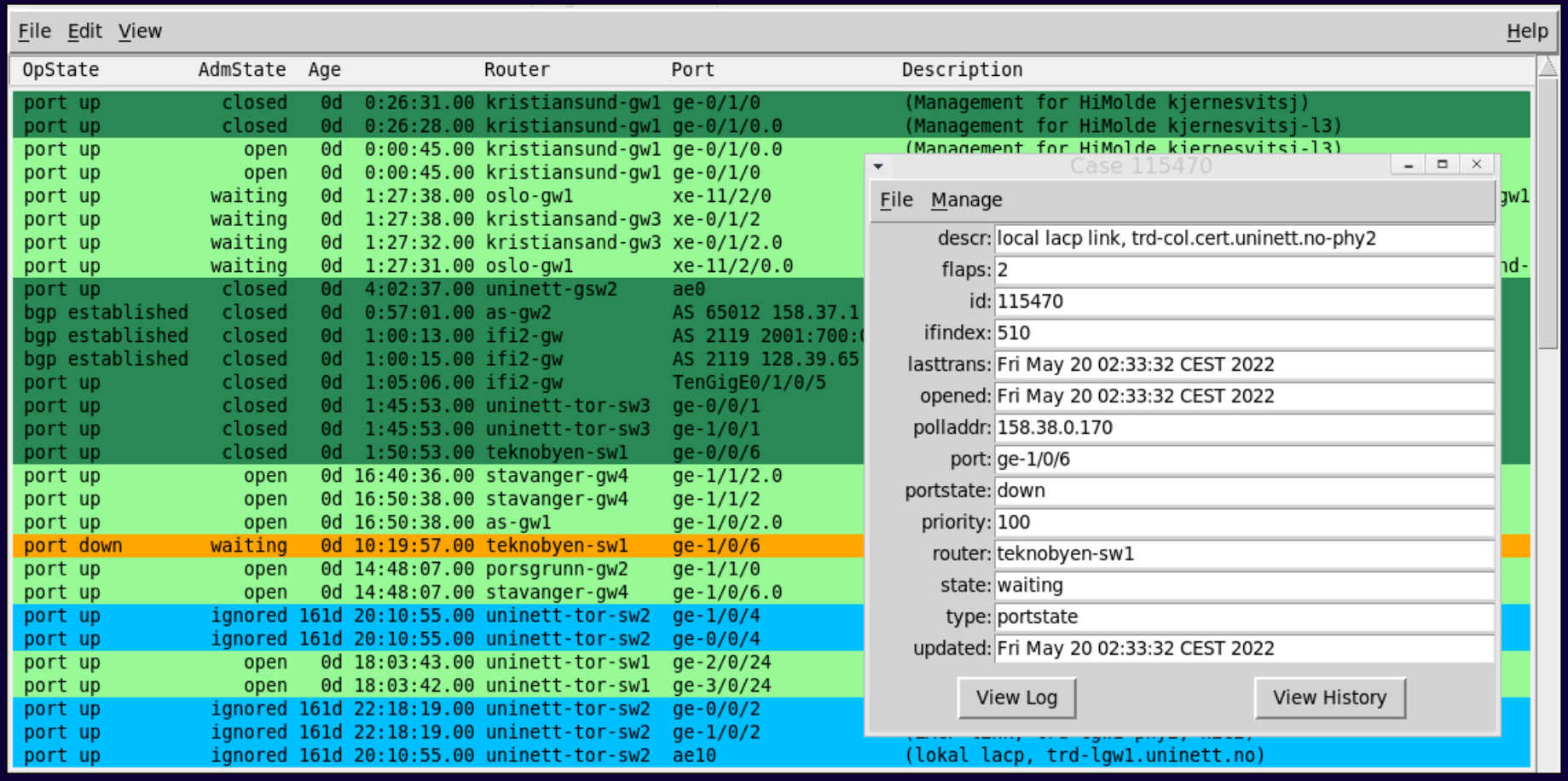
TRAFFIC STATS

- Also part of legacy Zino suite:
  - Traffic stats
  - Error reports from stats data
- But we dont have time to delve into that here....

STATE MONITOR CLIENTS

- ritz *(Tcl/Tk)*
- curitz *(Python)*
- emt *(Tcl)*

RITZ


File Edit View
Help
OpState AdmState Age Router Port Description
port up closed 0d 0:26:31.00 kristiansund-gw1 ge-0/1/0 (Management for HiMolde kjernesvitsj)
port up closed 0d 0:26:28.00 kristiansund-gw1 ge-0/1/0.0 (Management for HiMolde kjernesvitsj-l3)
port up open 0d 0:00:45.00 kristiansund-gw1 ge-0/1/0.0
port up open 0d 0:00:45.00 kristiansund-gw1 ge-0/1/0
port up waiting 0d 1:27:38.00 oslo-gw1 xe-11/2/0
port up waiting 0d 1:27:38.00 kristiansand-gw3 xe-0/1/2
port up waiting 0d 1:27:32.00 kristiansand-gw3 xe-0/1/2.0
port up waiting 0d 1:27:31.00 oslo-gw1 xe-11/2/0.0
port up closed 0d 4:02:37.00 uninett-gsw2 ae0
bgp established closed 0d 0:57:01.00 as-gw2 AS 65012 158.37.1
bgp established closed 0d 1:00:13.00 ifi2-gw AS 2119 2001:700:
bgp established closed 0d 1:00:15.00 ifi2-gw AS 2119 128.39.65
port up closed 0d 1:05:06.00 ifi2-gw TenGigE0/1/0/5
port up closed 0d 1:45:53.00 uninett-tor-sw3 ge-0/0/1
port up closed 0d 1:45:53.00 uninett-tor-sw3 ge-1/0/1
port up closed 0d 1:50:53.00 teknobyen-sw1 ge-0/0/6
port up open 0d 16:40:36.00 stavanger-gw4 ge-1/1/2.0
port up open 0d 16:50:38.00 stavanger-gw4 ge-1/1/2
port up open 0d 16:50:38.00 as-gw1 ge-1/0/2.0
port down waiting 0d 10:19:57.00 teknobyen-sw1 ge-1/0/6
port up open 0d 14:48:07.00 porsgrunn-gw2 ge-1/1/0
port up open 0d 14:48:07.00 stavanger-gw4 ge-1/0/6.0
port up ignored 161d 20:10:55.00 uninett-tor-sw2 ge-1/0/4
port up ignored 161d 20:10:55.00 uninett-tor-sw2 ge-0/0/4
port up open 0d 18:03:43.00 uninett-tor-sw1 ge-2/0/24
port up open 0d 18:03:42.00 uninett-tor-sw1 ge-3/0/24
port up ignored 161d 22:18:19.00 uninett-tor-sw2 ge-0/0/2
port up ignored 161d 22:18:19.00 uninett-tor-sw2 ge-1/0/2
port up ignored 161d 20:10:55.00 uninett-tor-sw2 ae10
(lokal lacp, trd-lgw1.uninett.no)
Case 115470
File Manage
descr: local lacp link, trd-col.cert.uninett.no-phy2
flaps: 2
id: 115470
ifindex: 510
lasttrans: Fri May 20 02:33:32 CEST 2022
opened: Fri May 20 02:33:32 CEST 2022
polladdr: 158.38.0.170
port: ge-1/0/6
portstate: down
priority: 100
router: teknobyen-sw1
state: waiting
type: portstate
updated: Fri May 20 02:33:32 CEST 2022
View Log
View History

CURITZ


cuRitz version 0.9.17.dev3+g5b7bdb3 - zino.uninett.no
S OpState AdmState Age Dt Router Port Description
PORT up open 0d 01:40 0s kristiansund-gw1 ge-0/1/0 Management for HiMolde kjernesvits j
PORT up waiting 0d 05:27 0s oslo-gw1 xe-11/2/0.0 UNO00136 GC11520020, oslo-kristiansand-l3, kristiansand-g
PORT up waiting 0d 05:27 0s kristiansand-gw3 xe-0/1/2.0 UNO00136 GC11520020, kristiansand-oslo-l3
PORT up waiting 0d 05:27 6s kristiansand-gw3 xe-0/1/2 UNO00136 GC11520020, kristiansand-oslo
PORT up waiting 0d 05:27 4m oslo-gw1 xe-11/2/0 UNO00136 GC11520020, oslo-kristiansand, kristiansand-gw1
PORT down waiting 0d 14:19 14h teknobyen-sw1 ge-1/0/6 local lacp link, trd-col.cert.uninett.no-phy2
PORT up open 0d 18:48 6m stavanger-gw4 ge-1/0/6.0 UPW000127, uis-svg-porsgrunn-l2vpn
PORT up open 0d 18:48 6m porsgrunn-gw2 ge-1/1/0 UNO01054, uis-porsgrunn-stavanger, L2vpn AC
PORT up open 0d 22:03 4s uninett-tor-sw1 ge-3/0/24 LACP-link, trd-agw1_ny.uninett.no-phy2
PORT up open 0d 22:03 6s uninett-tor-sw1 ge-2/0/24 LACP-link, trd-agw1_ny.uninett.no-phy1
PORT up open 0d 22:03 4m uninett-tor-sw1 ae21 LACP-link, trd-agw1_ny.uninett.no
BGP down waiting 2d 08:51 tullin-gw1 AS29695 2001:7f8:12:2::2:9695 peer is down
BGP down waiting 2d 08:51 tullin-gw1 AS29695 185.1.65.16 peer is down
BGP down waiting 7d 19:02 tullin-gw1 AS64625 riksantikvaren-gw2.ra.no. peer is down
BGP down waiting 7d 19:02 ifi2-gw AS64625 riksantikvaren-gw1.ra.no. peer is down
PORT down working 14d 02:25 14d ma2-gw xe-2/1/0 UNO01325, ma2-mettromso
BGP down waiting 15d 02:52 tromso-fh-gw AS64526 mettromso-fw.met.no. peer is admin turned off
PORT down working 23d 05:56 23d narvik-gw2 gr-11/0/10.0 lokal tunnel, narvik-janitor.cert, janitor.cert
PORT down waiting 23d 07:49 23d uninett-tor-sw1 ae11 LACP-link, pltrd037.moosefs.fs.uninett.no
BGP down waiting 25d 05:19 stavanger-gw2 AS64535 uis-d202-gsw03.uis.no. peer is admin turned off
BGP down waiting 25d 05:19 stavanger-gw2 AS64535 uis-d202-gsw03.uis.no. peer is admin turned off
BGP down waiting 25d 05:44 stavanger-gw2 AS64535 uis-kkh-gsw01.uis.no. peer is admin turned off
BGP down waiting 25d 05:44 stavanger-gw2 AS64535 uis-kkh-gsw01.uis.no. peer is admin turned off
PORT down working 25d 05:59 25d tullin-gw1 xe-100/0/4.20 UNO00777 GC10306676, tullin-udir-l3
PORT lower waiting 28d 05:17 0s stavanger-gw3 xe-0/1/5.0 UNO00528 -- stavanger-uis -- uis-kkh-gsw01.uis.no-l3
BGP down waiting 28d 05:18 stavanger-gw3 AS64535 uis-kkh-gsw01.uis.no. peer is admin turned off
BGP down waiting 28d 05:18 stavanger-gw3 AS64535 uis-kkh-gsw01.uis.no. peer is admin turned off
PORT lower waiting 28d 19:45 0s hamar-gw5 xe-0/1/4.0 UNO01347, hamar-udir-l3
BGP down waiting 28d 19:45 hamar-gw5 AS64668 2001:700:0:800a::1 peer is admin turned off
BGP down waiting 28d 19:45 hamar-gw5 AS64668 udir-hmr-fw1-0.c.uninett.no. peer is admin turned off
BGP down working 39d 05:08 bergen-gw3 AS64640 bergen-fw1.met.no. peer is down
BGP down working 39d 05:08 bergen-gw3 AS64532 2001:700:0:4303::2 peer is down
<=>=Display attributes m=Clear Flapping i=Show/Hide ID X=Restore last selection
s=Set State u=Update History U=Update History and Set State f=Filter y=Remove Closed
<ENTER>=Show history <UP/DOWN>=Navigate q=Quit l=Show Logs x=(de)select c=Clear selection

EMT

- Sends email alarms
- Sends SMS alarms (via external mail-to-SMS gateway)
- Implements failover mechanism

BACK TO THE 90S

The Zino suite has been continuously developed, deployed and maintained since the mid-90s

DEPLOYMENT

- Zino is mainly developed by Sikt
- Deployed at Sikt (Uninett), NORDUnet and Sunet

THE GOOD

- Separation of concerns
- Very stable
- Few dependencies
- Battle-proven (for more than 25 years)

THE NOT SO GOOD

- Good luck finding Tcl programmers in 2023
- Project "bus factor" is approaching zero...

```
proc pollSingleIf { sh ix } {
    set bpl [basePollList $sh]
    foreach v [split $bpl] {
    lappend pl [format "%s.%d" $v [expr $ix - 1]]
    lappend sl [mib oid $v]
    }
    if [catch {set res [$sh getnext $pl]} msg] {
    log [format "%s: error polling single intf %s: %s" \
        [name $sh] $ix $msg]
    return
    }
    set fres [filterLowestMatching $sl $ix $res]
    if { "$fres" == "" } {
    log [format "%s: error polling single intf %s: no match" \
        [name $sh] $ix]
```

FAST FORWARD TO 2023

NORDUnet is sponsoring a reimplementation of Zino in *two* separate work packages

NORDUnet
Nordic Gateway for Research & Education

WP1: STATE MONITOR RE-IMPLEMENTATION

- State monitoring is the most crucial component for NOCs
- The Zino designs are already robust
- Decision: Port codebase to *Python*, using a team of developers

WP1: STATE MONITOR RE-IMPLEMENTATION

- Also: Build a web-based client for the Zino API

WP2: TRAFFIC STATS COLLECTION AND WEATHERMAP

(As presented by Jonas Hagström just a few minutes ago...)

- NORDUnet members already collect traffic stats in different ways
  - SNMP, Telemetry, multiple toolsets
- Concentrate on aggregation of existing data from members into a shared network map.

THE GOAL

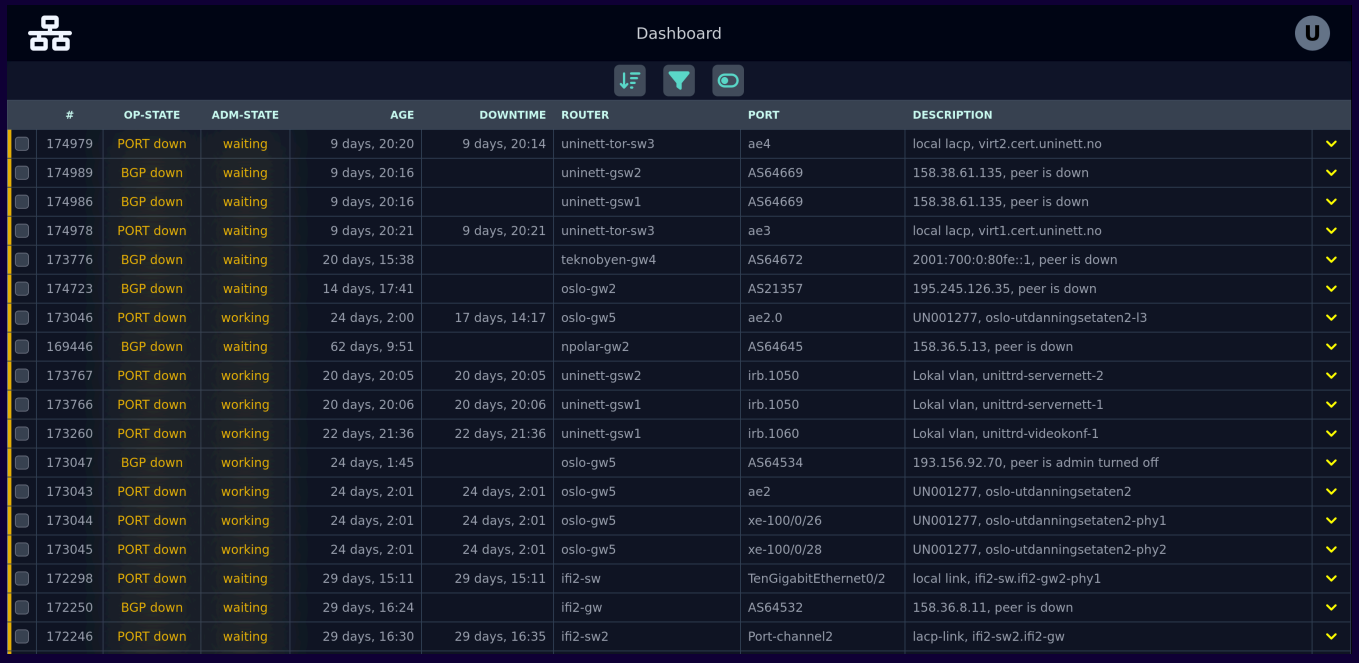
- All 5 NORDUnet members are using Zino in their NOCs

THE GOAL

- All 5 NORDUnet members are using Zino in their NOCs
- **... and maybe even more?**

2024 STATUS

- Rewritten state monitor nearly complete
- Howitz is a new web-based client to the Zino API



#	OP-STATE	ADM-STATE	AGE	DOWNTIME	ROUTER	PORT	DESCRIPTION
174979	PORT down	waiting	9 days, 20:20	9 days, 20:14	uninett-tor-sw3	ae4	local lacp, virt2.cert.uninett.no
174989	BGP down	waiting	9 days, 20:16		uninett-gsw2	AS64669	158.38.61.135, peer is down
174986	BGP down	waiting	9 days, 20:16		uninett-gsw1	AS64669	158.38.61.135, peer is down
174978	PORT down	waiting	9 days, 20:21	9 days, 20:21	uninett-tor-sw3	ae3	local lacp, virt1.cert.uninett.no
173776	BGP down	waiting	20 days, 15:38		teknobyen-gw4	AS64672	2001:700:0:80fe::1, peer is down
174723	BGP down	waiting	14 days, 17:41		oslo-gw2	AS21357	195.245.126.35, peer is down
173046	PORT down	working	24 days, 2:00	17 days, 14:17	oslo-gw5	ae2.0	UN001277, oslo-utdanningsetaten2-l3
169446	BGP down	waiting	62 days, 9:51		npolar-gw2	AS64645	158.36.5.13, peer is down
173767	PORT down	working	20 days, 20:05	20 days, 20:05	uninett-gsw2	irb.1050	Lokal vlan, unittrd-servernett-2
173766	PORT down	working	20 days, 20:06	20 days, 20:06	uninett-gsw1	irb.1050	Lokal vlan, unittrd-servernett-1
173260	PORT down	working	22 days, 21:36	22 days, 21:36	uninett-gsw1	irb.1060	Lokal vlan, unittrd-videokonf-1
173047	BGP down	working	24 days, 1:45		oslo-gw5	AS64534	193.156.92.70, peer is admin turned off
173043	PORT down	working	24 days, 2:01	24 days, 2:01	oslo-gw5	ae2	UN001277, oslo-utdanningsetaten2
173044	PORT down	working	24 days, 2:01	24 days, 2:01	oslo-gw5	xe-100/0/26	UN001277, oslo-utdanningsetaten2-phy1
173045	PORT down	working	24 days, 2:01	24 days, 2:01	oslo-gw5	xe-100/0/28	UN001277, oslo-utdanningsetaten2-phy2
172298	PORT down	waiting	29 days, 15:11	29 days, 15:11	ifi2-sw	TenGigabitEthernet0/2	local link, ifi2-sw.ifi2-gw2-phy1
172250	BGP down	waiting	29 days, 16:24		ifi2-gw	AS64532	158.36.8.11, peer is down
172246	PORT down	waiting	29 days, 16:30	29 days, 16:35	ifi2-sw2	Port-channel2	lacp-link, ifi2-sw2.ifi2-gw

2024 STATUS

- "Bus factor" is now closer to 5!
- Zino is in active alpha release
- Fully open source and available on GitHub and PyPI

WHAT'S NEXT?

What comes after Zino 2.0 is complete?

WHAT'S NEXT?

- API modernization (REST + TLS encryption)?

WHAT'S NEXT?

- API modernization (REST + TLS encryption)?
- Optical state monitoring?

WHAT'S NEXT?

- API modernization (REST + TLS encryption)?
- Optical state monitoring?
  - ... probably not ...

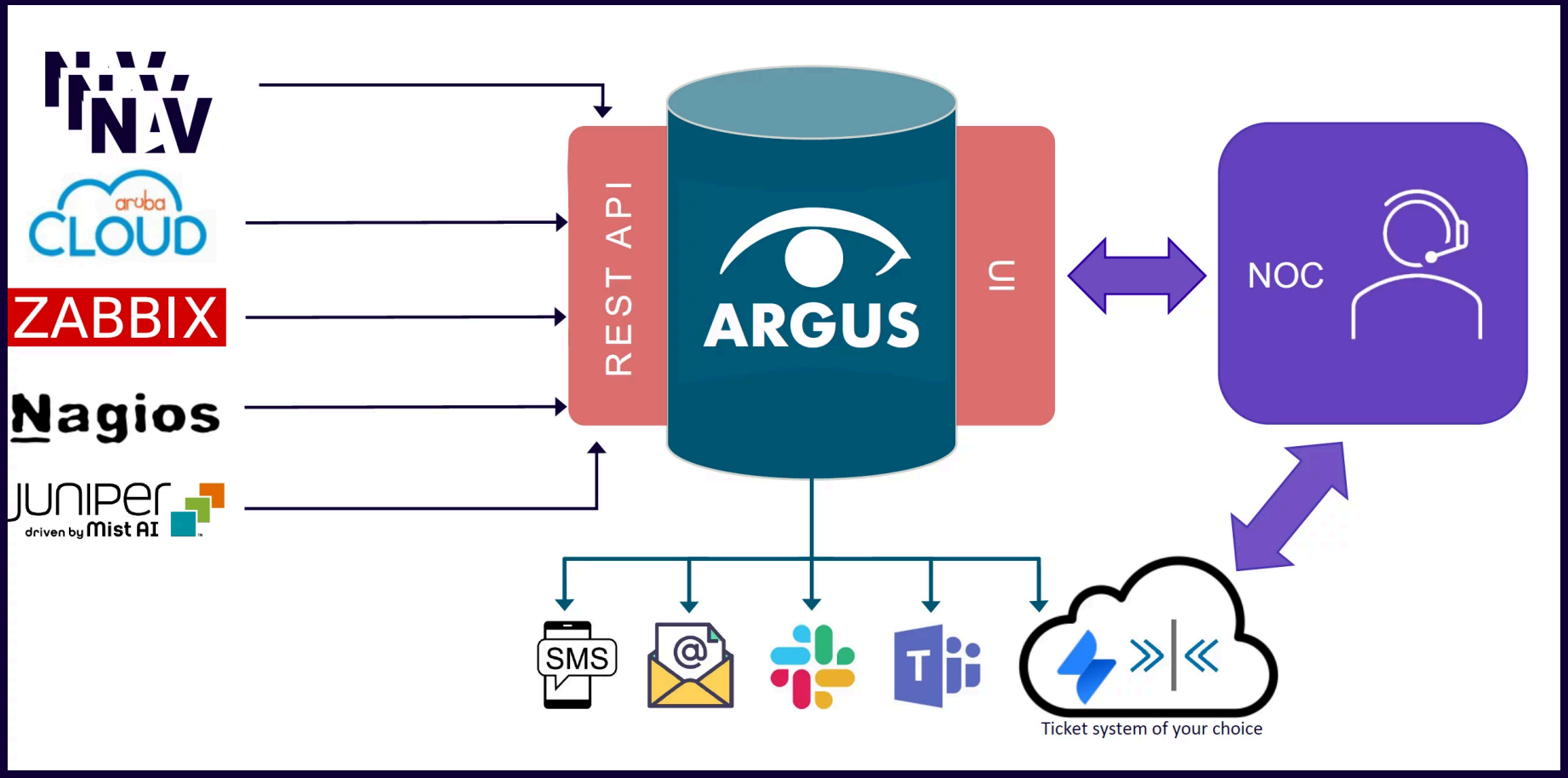
WHAT'S NEXT?

- API modernization (REST + TLS encryption)?
- Optical state monitoring?
  - ... probably not ...
- **Argus** integration is more likely!

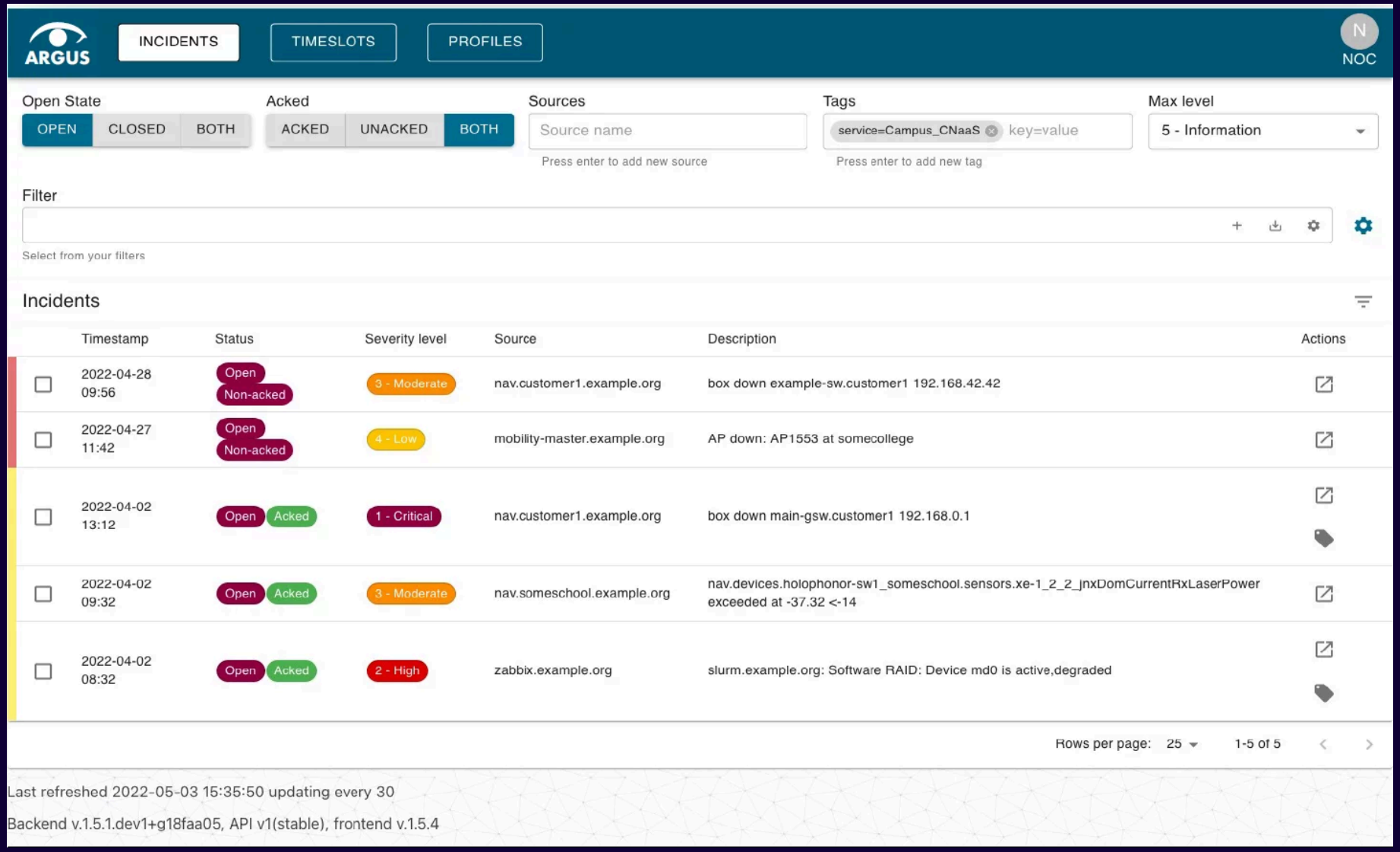
ARGUS

- Alarm Aggregation and correlation tool
- Manages your incidents across all your monitoring tools
- A GÉANT production service

ARGUS


NAV
aruba CLOUD
ZABBIX
Nagios
JUNIPER driven by Mist AI
REST API
ARGUS
UI
NOC
SMS
Ticket system of your choice

ARGUS


ARGUS
INCIDENTS
TIMESLOTS
PROFILES
N
NOC
Open State
OPEN
CLOSED
BOTH
Acked
ACKED
UNACKED
BOTH
Sources
Source name
Press enter to add new source
Tags
service=Campus_CNaaS
key=value
Press enter to add new tag
Max level
5 - Information
Filter
Select from your filters
Incidents
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
2022-04-27 11:42
Open
Non-acked
4 - Low
mobility-master.example.org
AP down: AP1553 at somecollege
2022-04-02 13:12
Open
Acked
1 - Critical
nav.customer1.example.org
box down main-gsw.customer1 192.168.0.1
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
2022-04-02 08:32
Open
Acked
2 - High
zabbix.example.org
slurm.example.org: Software RAID: Device md0 is active,degraded
Rows per page: 25
1-5 of 5
Last refreshed 2022-05-03 15:35:50 updating every 30
Backend v.1.5.1.dev1+g18faa05, API v1(stable), frontend v.1.5.4

REFERENCES

- New state monitor back-end: https://github.com/Uninett/zino
- Howitz interface to Zino: https://github.com/Uninett/howitz
- cuRitz interface to Zino: https://github.com/Uninett/curitz
- Argus: https://network.geant.org/argus/