Monitoring and alert aggregation

Uninett CNaaS

22nd October 2019
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
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

Customer A

- Customer and Asset Database
- NAV (monitor)
- NAV 1st line config
- CNaaS-NMS (2nd and 3rd line config)
- Campus network
- oxidized (tracking changes)
- Nornir/NAPALM

SNMP read

Netconf

Customer B

Customer C

Aggregated alarm view (at NOC)

-KIND in Norway
-NI in Sweden

Uninett

SUNET

SNMP

Nornir/NAPALM

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 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 3<sup>rd</sup> party monitoring software
  - Link back to source systems for details
- Integration options for 3<sup>rd</sup> party ticketing systems
- NAV’s alarm profiles UI serves as example of how NOT to do it
<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Alert ID</th>
<th>Source</th>
<th>Description</th>
<th>Details URL</th>
<th>Object</th>
<th>Parent object</th>
<th>Problem type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000-01-05T17:...</td>
<td>570605</td>
<td>2</td>
<td>Cq!i vy!dw.</td>
<td><a href="http://x8.nav.no/5">http://x8.nav.no/5</a>...</td>
<td>11</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>2000-04-04T13:...</td>
<td>94245</td>
<td>1</td>
<td>E!cc!d ave hoqqz ...</td>
<td><a href="http://v7.nav.no/9">http://v7.nav.no/9</a>...</td>
<td>46</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>2000-04-09T16:...</td>
<td>621276</td>
<td>2</td>
<td>Xyyusza rtac yf f...</td>
<td><a href="http://x8.nav.no/6">http://x8.nav.no/6</a>...</td>
<td>15</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>2000-06-25T22:...</td>
<td>239034</td>
<td>6</td>
<td>Yuqkv qeqeuyd i...</td>
<td><a href="http://a8.zabbix.n">http://a8.zabbix.n</a>...</td>
<td>10</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>2000-08-06T08:...</td>
<td>833255</td>
<td>3</td>
<td>Mbmc yq otsuhy ...</td>
<td><a href="http://e4.nav.no/">http://e4.nav.no/</a>...</td>
<td>21</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>2000-11-21T19:...</td>
<td>682550</td>
<td>1</td>
<td>Ydqjudwevx row...</td>
<td><a href="http://v7.nav.no/6">http://v7.nav.no/6</a>...</td>
<td>34</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>2000-11-29T01:...</td>
<td>154725</td>
<td>4</td>
<td>Uu!jxx efboqoway t...</td>
<td><a href="http://r8.zabbix.n">http://r8.zabbix.n</a>...</td>
<td>17</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>2001-02-02T13:...</td>
<td>926035</td>
<td>5</td>
<td>Qyf zxixfc.</td>
<td><a href="http://a8.zabbix.n">http://a8.zabbix.n</a>...</td>
<td>33</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>2001-03-08T03:...</td>
<td>714740</td>
<td>3</td>
<td>Vkwv!laa lmdnp l...</td>
<td><a href="http://e4.nav.no/7">http://e4.nav.no/7</a>...</td>
<td>46</td>
<td>9</td>
<td>2</td>
</tr>
<tr>
<td>2001-03-17T11:...</td>
<td>761154</td>
<td>5</td>
<td>Lbe yi zntqoxp ...</td>
<td><a href="http://a8.zabbix.n">http://a8.zabbix.n</a>...</td>
<td>38</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>2001-10-23T14:...</td>
<td>621079</td>
<td>3</td>
<td>Oz nduepfz mqkf...</td>
<td><a href="http://e4.nav.no/">http://e4.nav.no/</a>...</td>
<td>28</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>2001-10-28T05:...</td>
<td>600656</td>
<td>5</td>
<td>Vw cnhzhvl lo tzs...</td>
<td><a href="http://a8.zabbix.n">http://a8.zabbix.n</a>...</td>
<td>18</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>2001-11-21T08:...</td>
<td>34501</td>
<td>5</td>
<td>Zaxwhvpgt wfw ...</td>
<td><a href="http://a8.zabbix.n">http://a8.zabbix.n</a>...</td>
<td>17</td>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td>2002-05-17T08:...</td>
<td>285266</td>
<td>3</td>
<td>Jnoaworuk hy ct...</td>
<td><a href="http://e4.nav.no/2">http://e4.nav.no/2</a>...</td>
<td>32</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>2002-08-12T04:...</td>
<td>214600</td>
<td>6</td>
<td>Grhtyq tqrndfykl ...</td>
<td><a href="http://a4.zabbix.n">http://a4.zabbix.n</a>...</td>
<td>26</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>2002-08-30T14:...</td>
<td>193212</td>
<td>2</td>
<td>Mu acockmg uxc</td>
<td><a href="http://x8.nav.no/1">http://x8.nav.no/1</a>...</td>
<td>4</td>
<td>9</td>
<td>8</td>
</tr>
</tbody>
</table>
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/