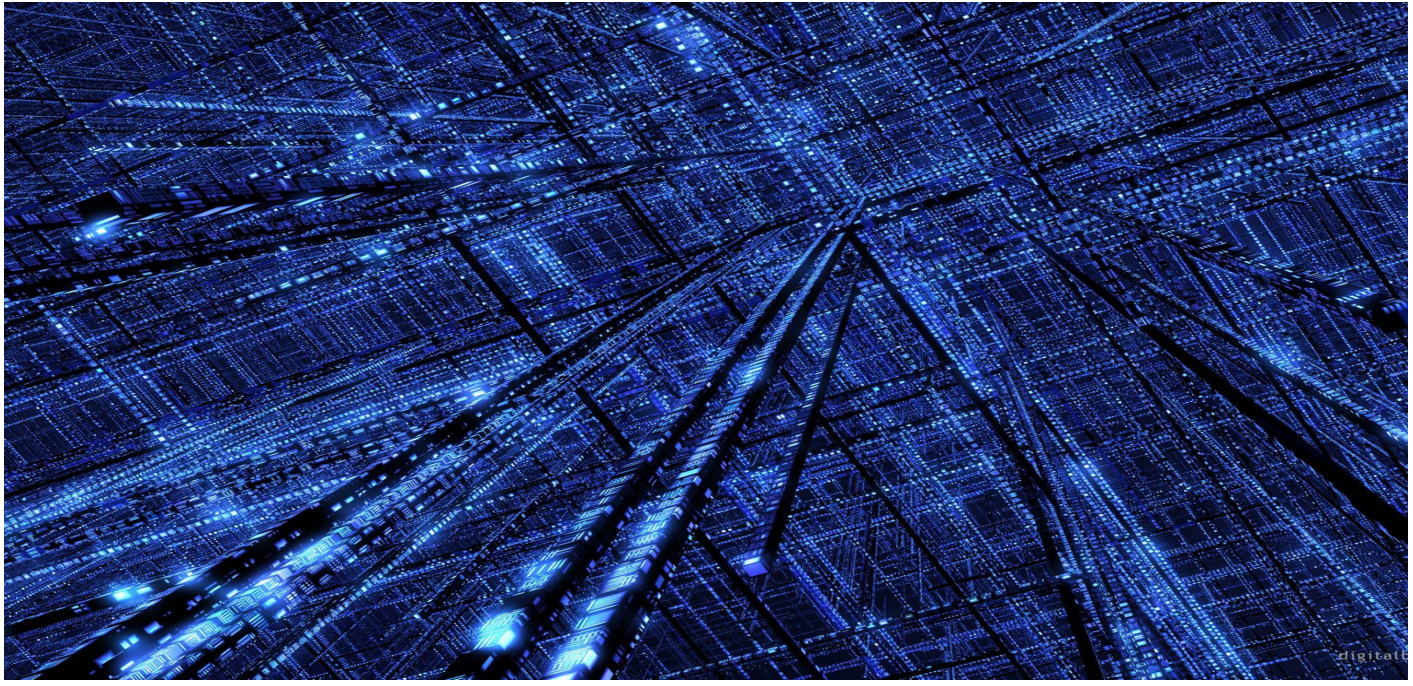
Grunnlagsdata, overvåking og trending

Rafael Martinez Guerrero / Trond H.Amundsen
IT-konferanse 2015
Universitetet i Oslo

IT infrastruktur ved UiO



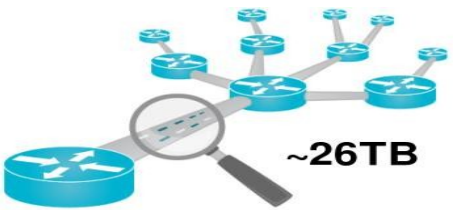
IT infrastruktur ved UiO

~2.100

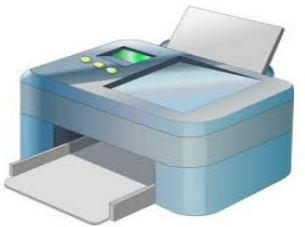
~16.000

~12.000TB

~2.200



~26TB



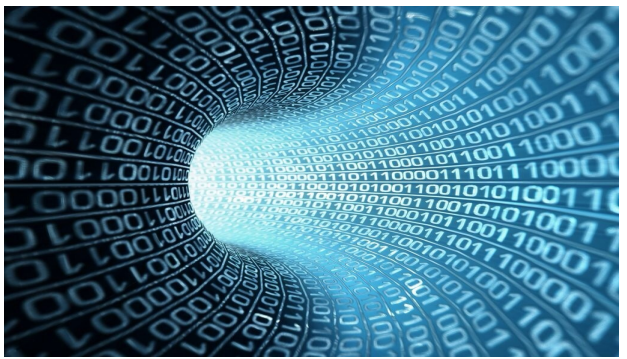
~1.000 / 38.000.000

~133 / 2.000

??? mill.

~1.600

Områder



Grunnlagsdata

1987
(Første Sun desktop ved MatNat)

1989
(Første Unix server ved USIT)

ca 1993
(Filelog første versjon)

2011

(Forbedret Filelog som bruker SSL)

2014
(Nivlheim)

2015
(Nivlheim for Windows)

Nivlheim

https://nivlheim.uio.no/

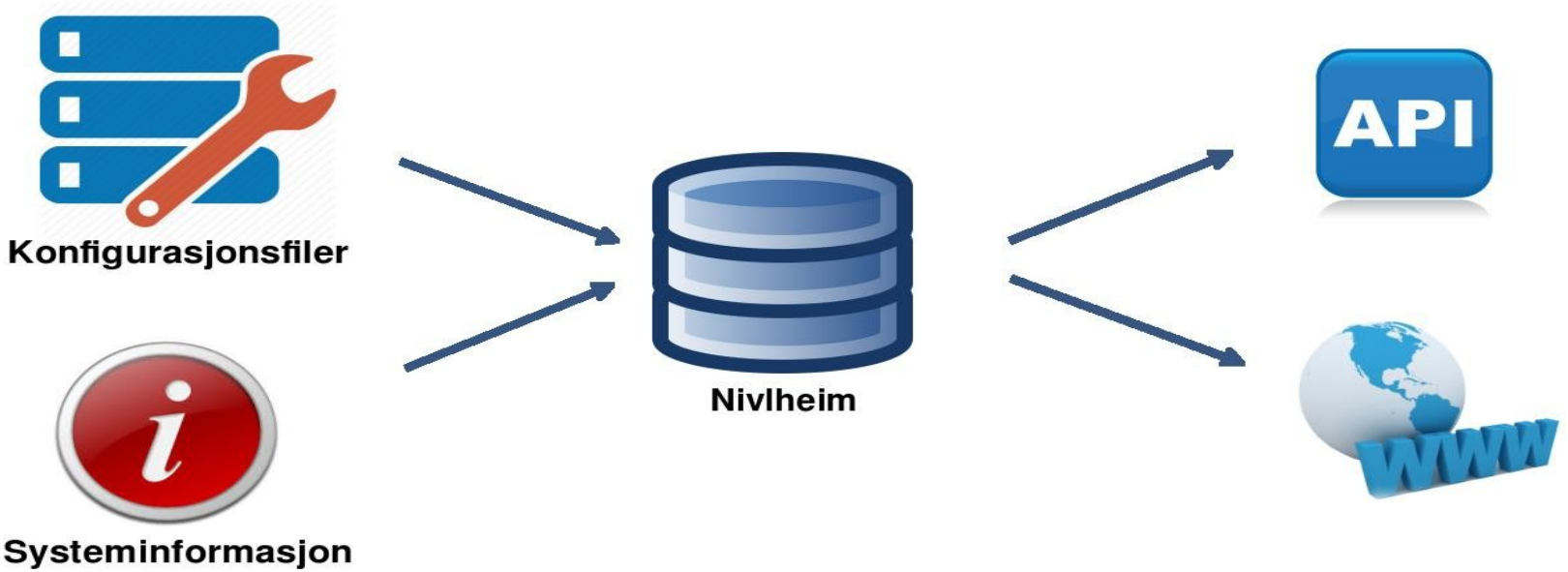
Bruksområder

Rapporter

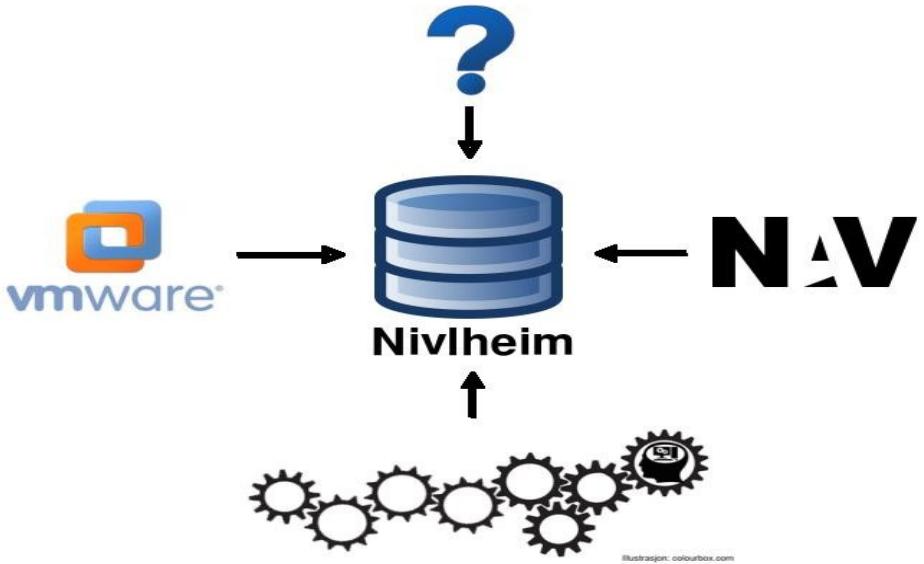
Kontroll

Automatisering

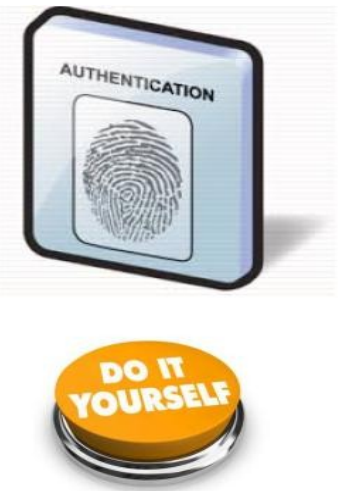
Arkitektur


Konfigurasjonsfiler
Systeminformasjon
Nivlheim
API
WWW

TODO



Datakilder++



Selvbetjening

https://nivlheim.uio.no/api/hostinfo2

.../hostinfo2?hostname=tux.uio.no

```
{
   "result" : [
      {
         "certfp" : "5E3934238D03606DDB72761E9CB1DCF1E4872FD7",
         "serial" : "CZC1035208",
         "daysLeftOfWarranty" : 107,
         "siteadmin" : "trondham@usit.uio.no",
         "hostname" : "tux.uio.no",
         "os" : "RHEL7",
         "kernel" : "3.10.0-229.el7.x86_64",
         "manufacturer" : "Hewlett-Packard",
         "osclass" : "Linux",
         "lastseen" : "2015-04-17T10:52:30Z",
         "type" : "Client",
         "product" : "HP Compaq 8100 Elite CMT PC",
         "ipaddr" : "129.240.6.13",
         "warranty" : [
            {
               "active" : false,
               "description" : "HP Care Pack - Next Business Day Onsite, HW Support, 4",
               "daysleft" : -2457129,
               "start" : "",
               "expires" : ""
            },
            [.................]
         ]
      }
   ]
}
```

```
{
   "result" : [
      {
         "certfp" : "5E3934238D03606DDB72761E9CB1DCF1E4872FD7",
         "serial" : "CZC1035208",
         "daysLeftOfWarranty" : 107,
         "siteadmin" : "trondham@usit.uio.no",
         "hostname" : "tux.uio.no",
         "os" : "RHEL7",
         "kernel" : "3.10.0-229.el7.x86_64",
         "manufacturer" : "Hewlett-Packard",
         "osclass" : "Linux",
         "lastseen" : "2015-04-17T10:52:30Z",
         "type" : "Client",
         "product" : "HP Compaq 8100 Elite CMT PC",
         "ipaddr" : "129.240.6.13",
         "warranty" : [
            {
               "active" : false,
               "description" : "HP Care Pack - Next Business Day Onsite, HW Support, 4",
               "daysleft" : -2457129,
               "start" : "",
               "expires" : ""
            },
            [.................]
         ]
      }
   ]
}
```

.../hostinfo2?hostname=tux.uio.no
&fl=hostname,lastseen

```
{
    "result" : [
        {
            "hostname" : "tux.uio.no",
            "lastseen" : "2015-04-17T10:52:30Z"
        }
    ]
}
```

.../hostinfo2?osclass=windows
&fl=hostname,product,os

```
{
   "result" : [
      {
         "hostname" : "win-ts05.uio.no",
         "product" : "VMware Virtual Platform",
         "os" : "Win2012R2"
      },
      {
         "hostname" : "scurque.uio.no",
         "product" : "HP Compaq Elite 8300 MT",
         "os" : "Win7"
      },
      {
         "hostname" : "d2mac.uio.no",
         "product" : "OptiPlex 7010",
         "os" : "Win7"
      },
      {
         "hostname" : "wjump-kat.uio.no",
         "product" : "VMware Virtual Platform",
         "os" : "Win2012R2"
      },
      [.................]
   ]
}
```

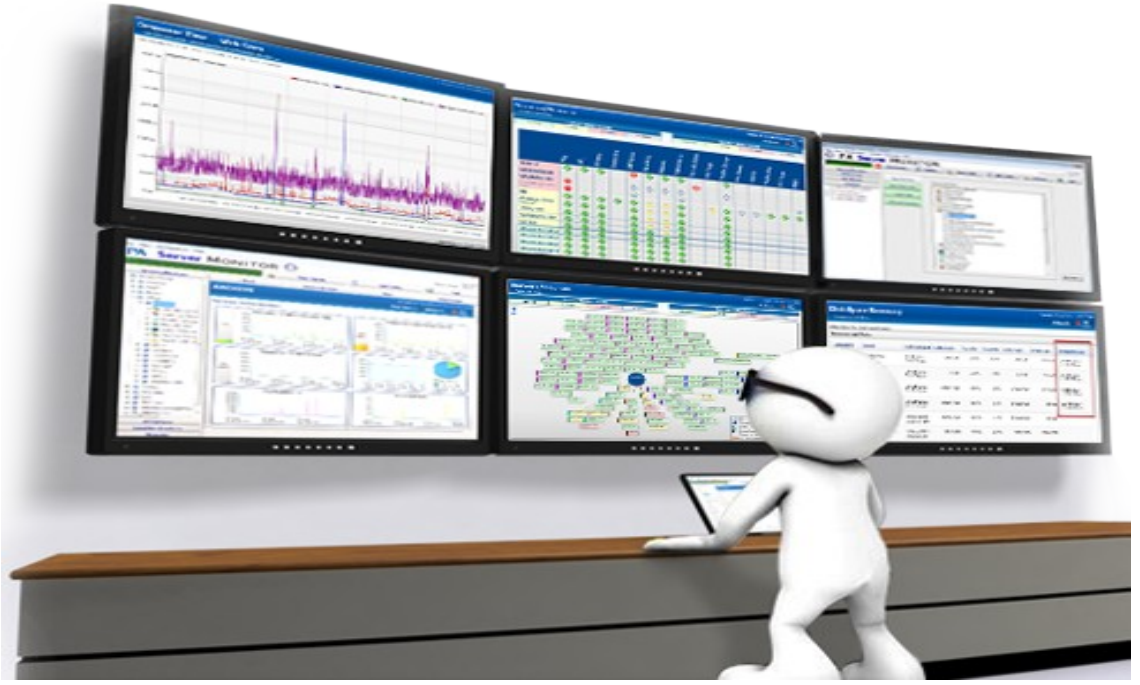
.../hostinfo2?osclass=windows
&fl=product&count=1

```
{
   "result" : [
      {
         "count" : 1,
         "product" : "HP Compaq Elite 8300 MT"
      },
      {
         "count" : 1,
         "product" : "OptiPlex 7010"
      },
      {
         "count" : 3,
         "product" : "RHEV Hypervisor"
      },
      {
         "count" : 16,
         "product" : "VMware Virtual Platform"
      }
   ]
}
```

.../hostinfo2?product=HP*dc5800*
&fl=product&count=1

```
{
   "result" : [
      {
         "count" : 11,
         "product" : "HP Compaq dc5800 Microtower"
      },
      {
         "count" : 18,
         "product" : "HP Compaq dc5800 Small Form Factor"
      }
   ]
}
```

Status overvåking



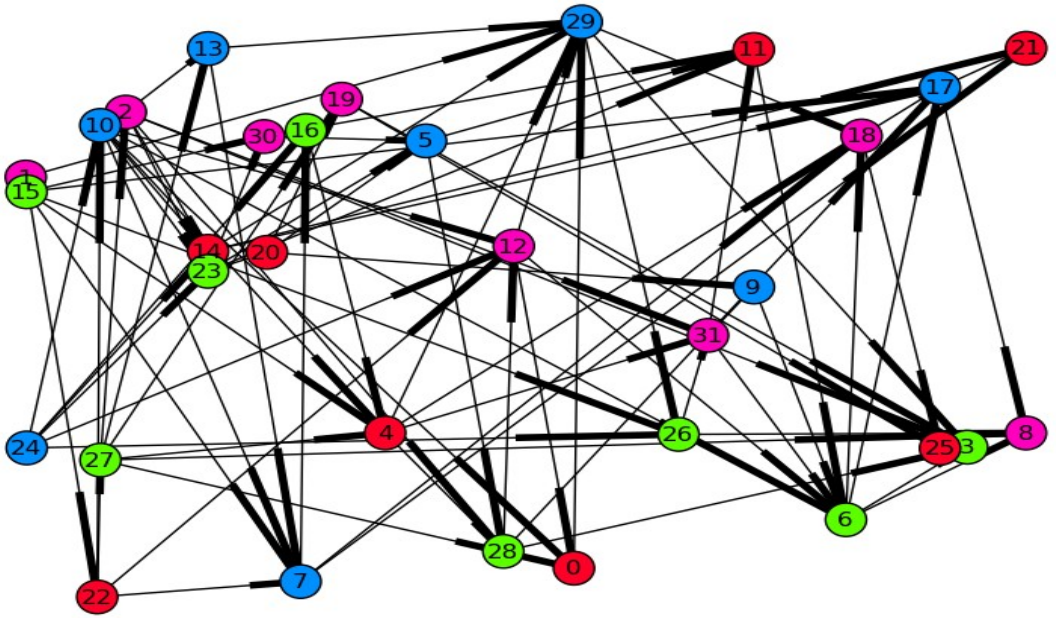

at&t
GLOBAL NETWORK at&t OPERATIONS CENTER
at&t


Ganglia
mrtg
SIPadm
SCCM
JON
Munin
OracleCC
SCOM
vCenter
NAV
Nagios
Graphite
vCops
Cron
Pgcladmin
Webhomer
tailnmail
Command-Suite

Distribuert overvåking

Roller / grupper

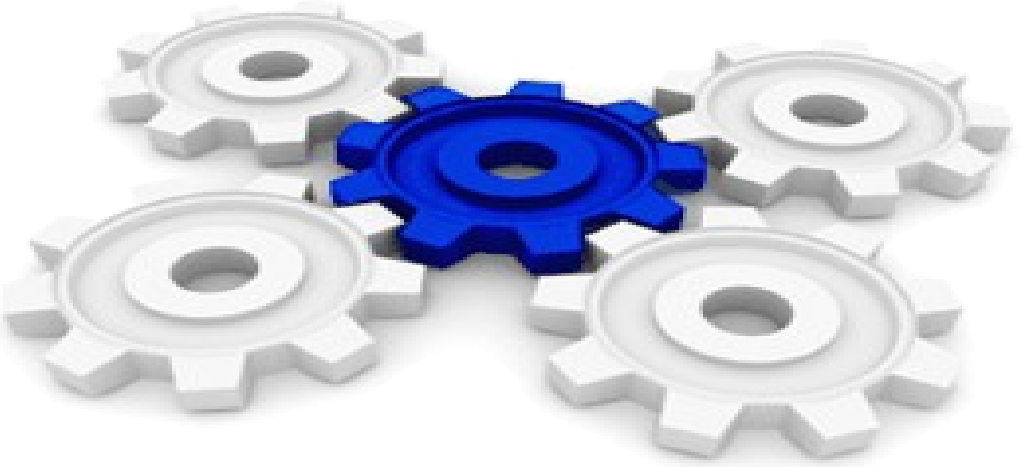
Avhengigheter / rotårsak



Filtrering

Tjenester

Integrasjon



Sentral konsoll

ZABBIX

The Ultimate Open Source Monitoring Solution

~1.300

~200

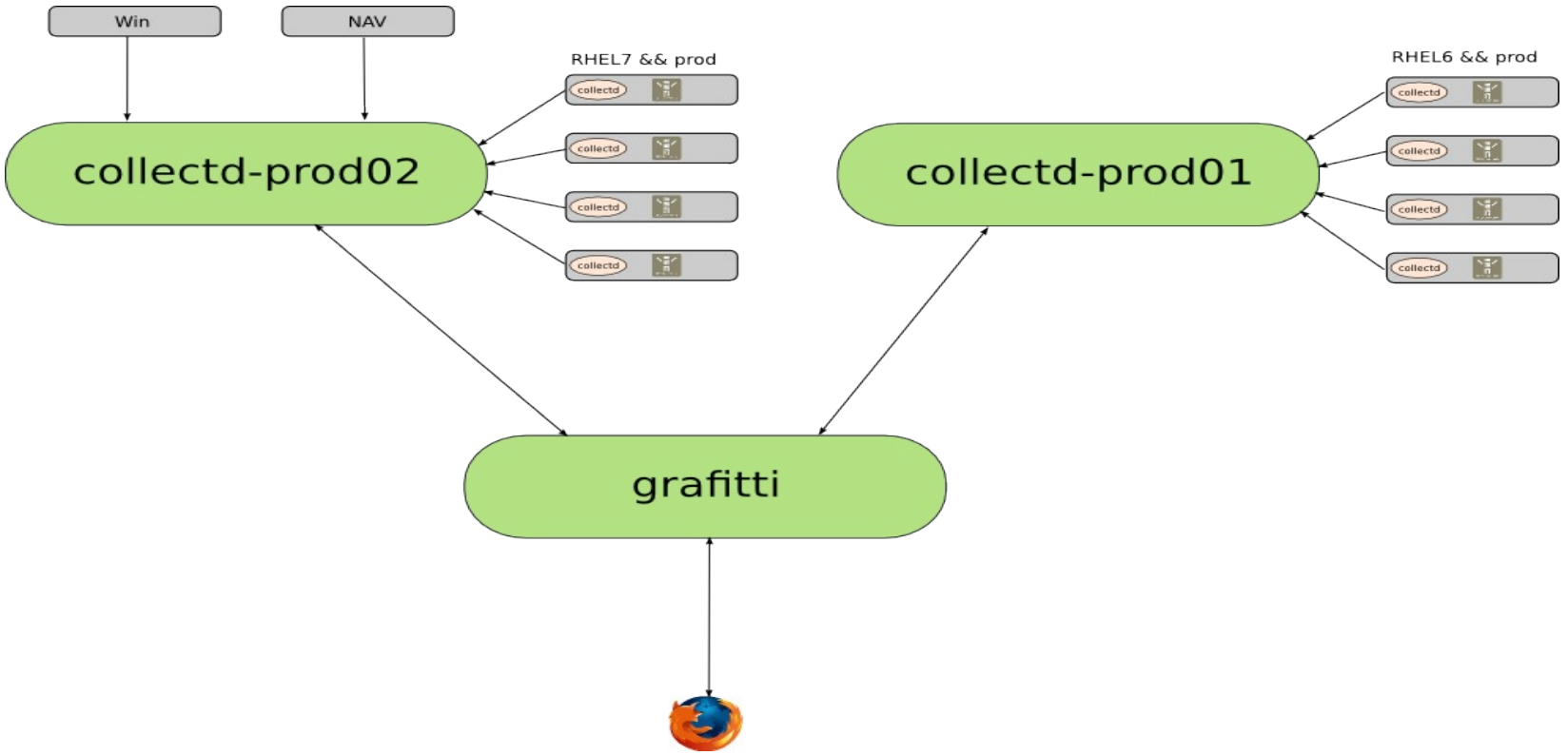
~190.000
~61.000.000 / 24h

~120.000

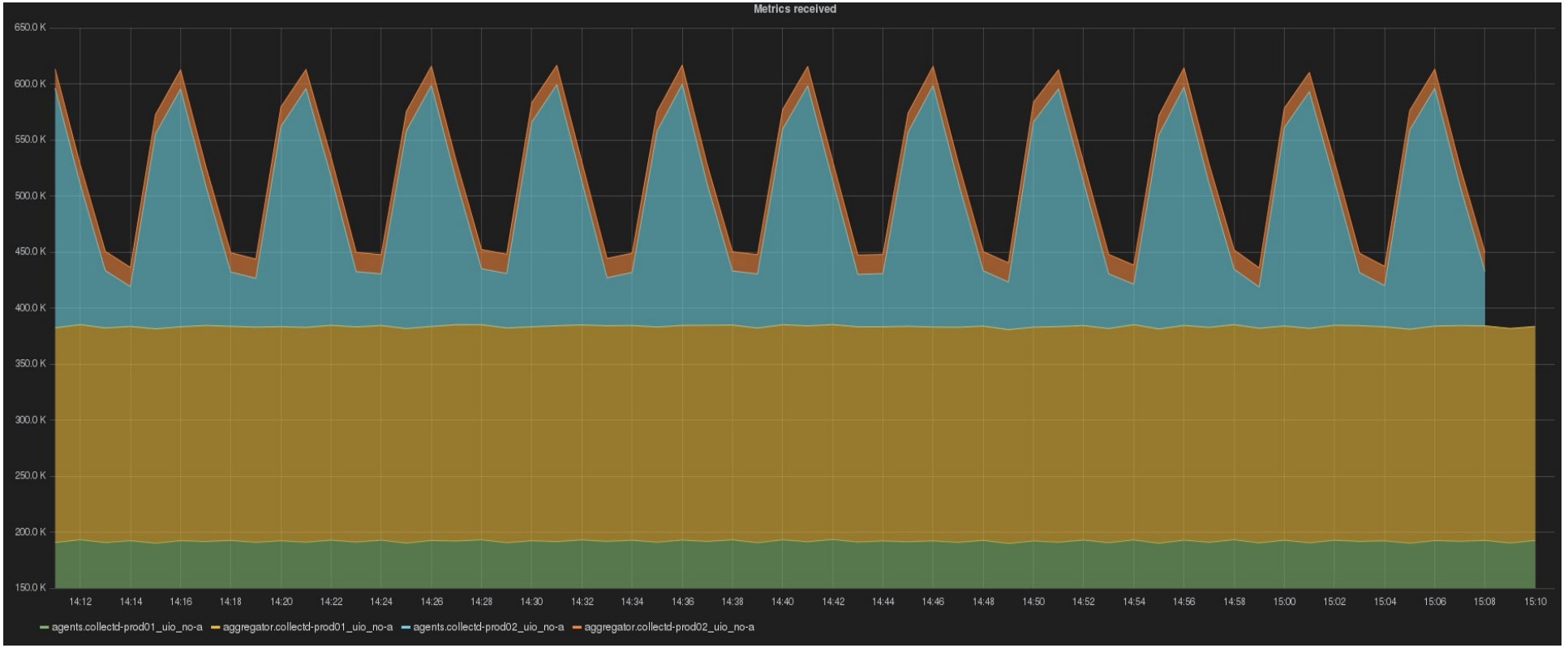
750.000.000

Trending

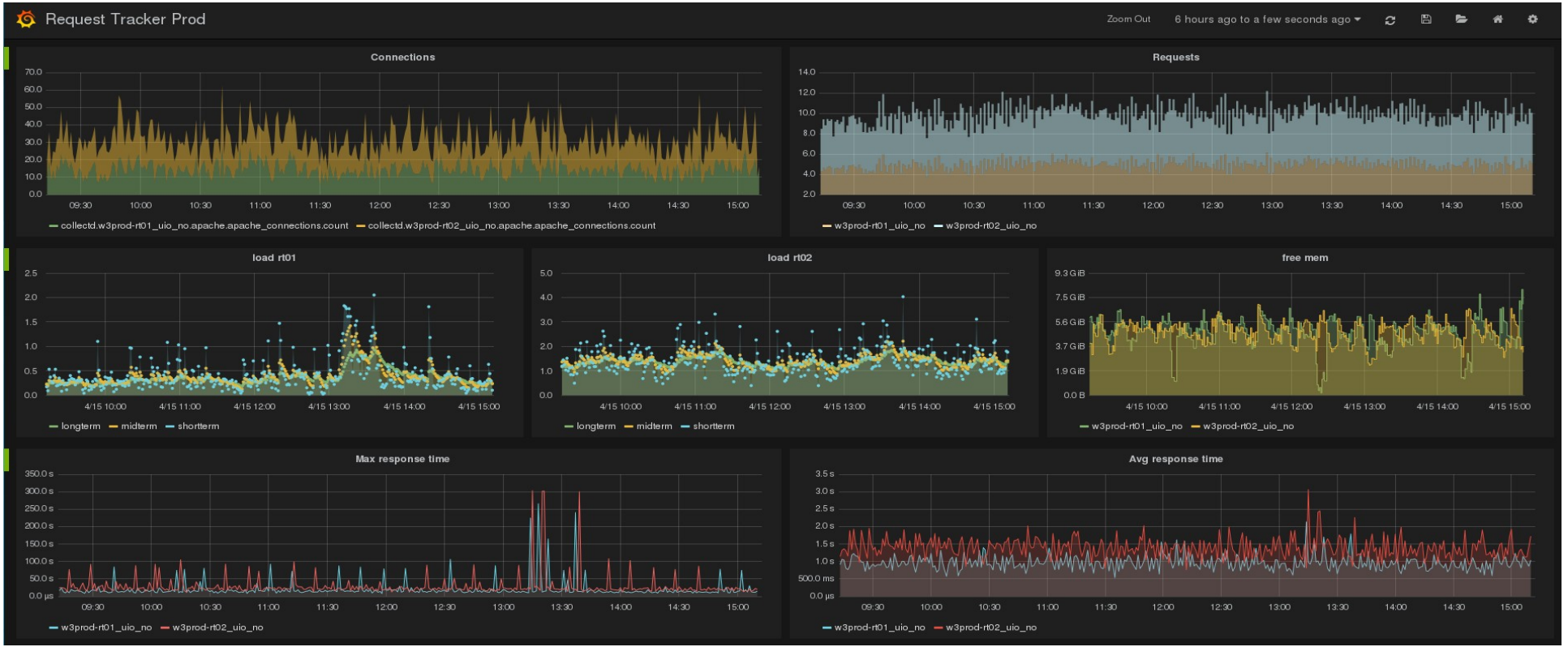
Arkitektur


Win
NAV
RHEL7 && prod
collectd
collectd
collectd
collectd
collectd-prod02
collectd-prod01
RHEL6 && prod
collectd
collectd
collectd
collectd
grafitti

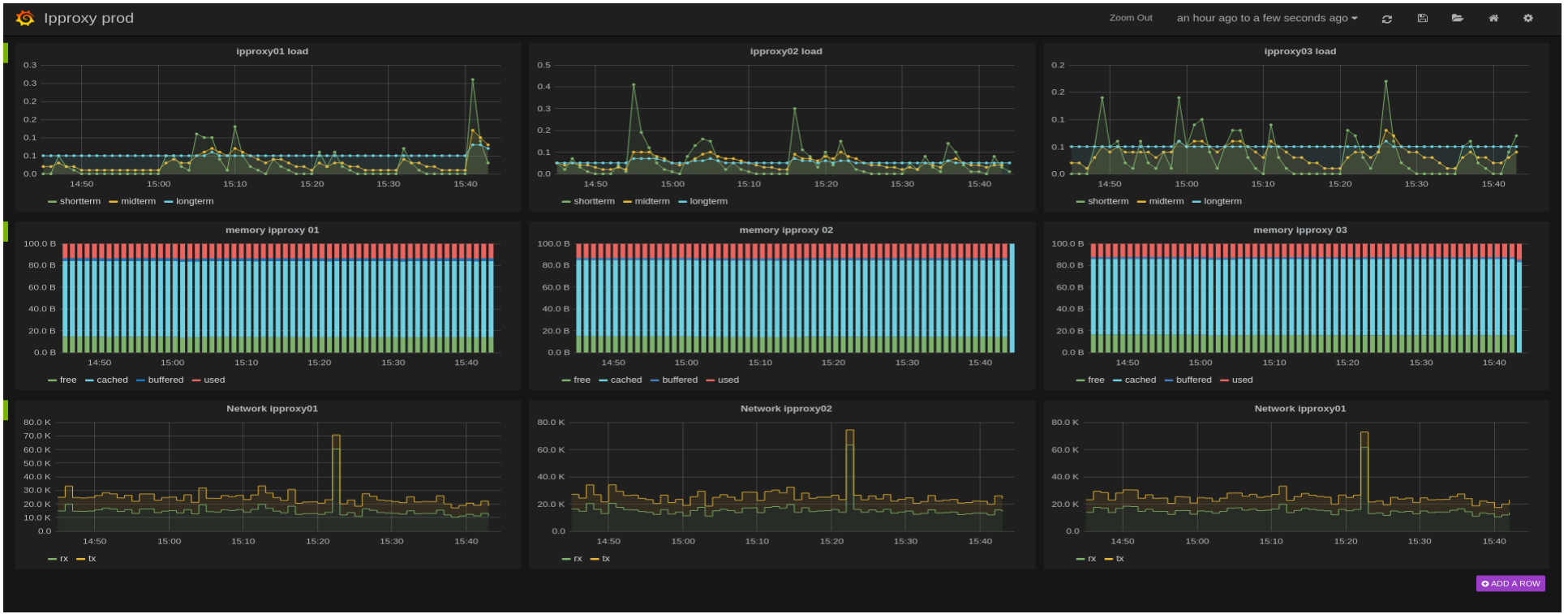
400k – 600k metrics / min



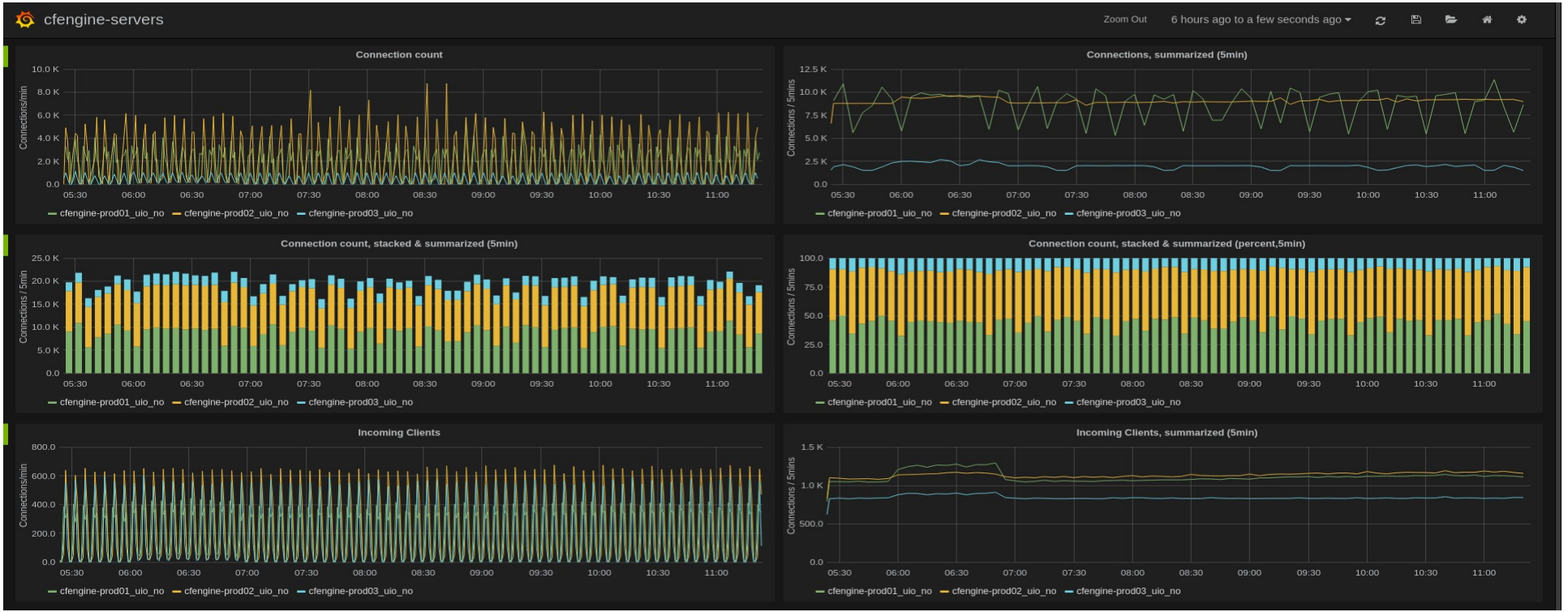
Grafana


Request Tracker Prod
Zoom Out
6 hours ago to a few seconds ago
Connections
collectd.w3prod-rt01_uio_no.apache.apache_connections.count
collectd.w3prod-rt02_uio_no.apache.apache_connections.count
Requests
w3prod-rt01_uio_no
w3prod-rt02_uio_no
load rt01
longterm
midterm
shortterm
load rt02
longterm
midterm
shortterm
free mem
w3prod-rt01_uio_no
w3prod-rt02_uio_no
Max response time
w3prod-rt01_uio_no
w3prod-rt02_uio_no
Avg response time
w3prod-rt01_uio_no
w3prod-rt02_uio_no

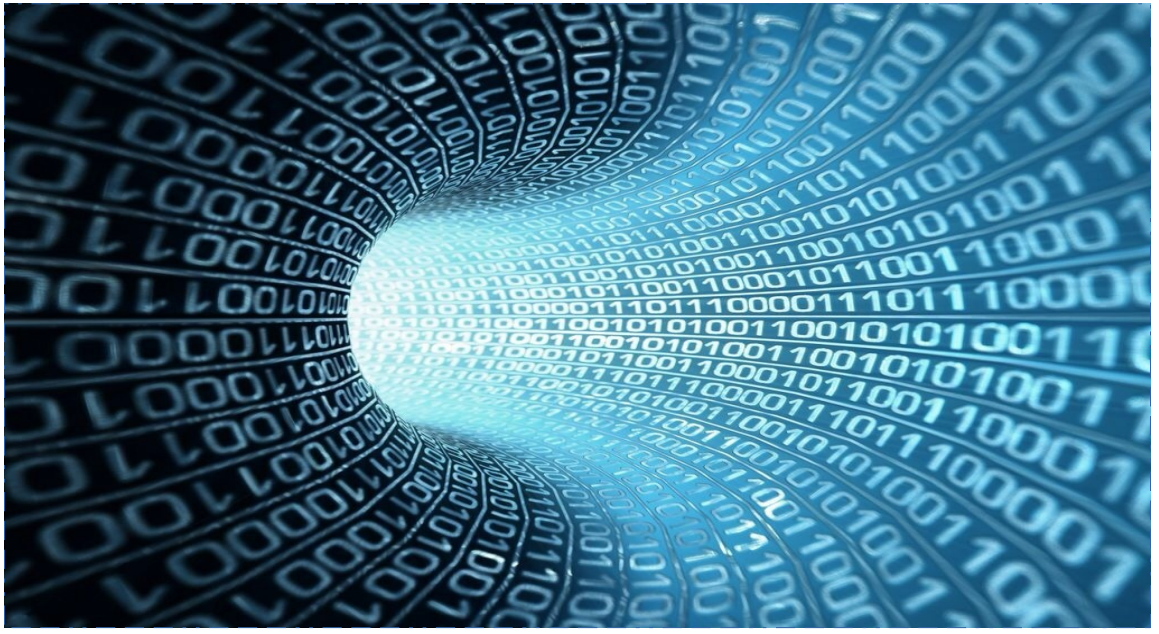
Grafana


Ipproxy prod
Zoom Out
an hour ago to a few seconds ago
ipproxy01 load
ipproxy02 load
ipproxy03 load
shortterm midterm longterm
memory ipproxy 01
memory ipproxy 02
memory ipproxy 03
free cached buffered used
Network ipproxy01
Network ipproxy02
Network ipproxy01
rx tx
ADD A ROW

Grafana

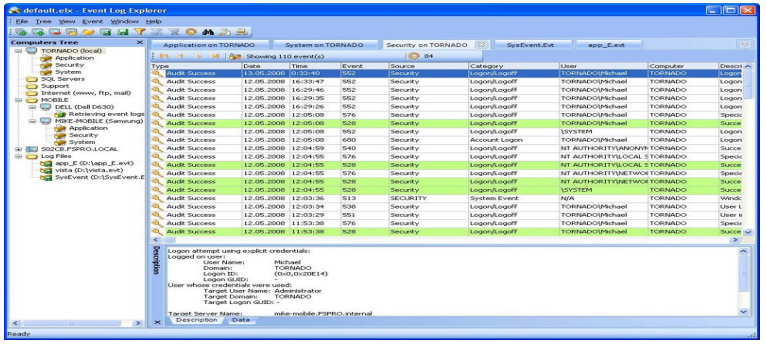

cfengine-servers
Zoom Out
6 hours ago to a few seconds ago
Connection count
Connections/min
cfengine-prod01_uio_no
cfengine-prod02_uio_no
cfengine-prod03_uio_no
Connections, summarized (5min)
Connections / 5mins
Connection count, stacked & summarized (5min)
Connections / 5min
Connection count, stacked & summarized (percent,5min)
Incoming Clients
Incoming Clients, summarized (5min)

Logghåndtering



Mengde

Logtyper




```
    0        10        20        30        40        50        60        70        80        90
 1 98.149.180.239 - - [13/Dec/2009:06:25:13 +0100] "GET /demo HTTP/1.0" 200 275084 "-" "PSP-Inter
 2 110.49.133.52 - - [13/Dec/2009:06:25:19 +0100] "GET /demo/index.html HTTP/1.0" 404 106 "-" "Mo
 3 76.108.234.173 - - [13/Dec/2009:06:26:52 +0100] "GET /demo HTTP/1.0" 200 153325 "-" "PSP-Inter
 4 76.108.234.173 - - [13/Dec/2009:06:27:20 +0100] "GET /demo HTTP/1.0" 200 42549 "-" "PSP-Intern
 5 188.4.191.98 - - [13/Dec/2009:06:27:34 +0100] "GET /demo.m3u HTTP/1.1" 200 92 "http://www.inte
 6 188.4.191.98 - - [13/Dec/2009:06:27:59 +0100] "GET /demo HTTP/1.0" 200 398333 "-" "WinampMPEG/
 7 110.49.133.52 - - [13/Dec/2009:06:28:06 +0100] "GET /demo/index.html HTTP/1.0" 404 106 "-" "Mo
 8 82.113.121.200 - - [13/Dec/2009:06:28:47 +0100] "GET /demo/index.html HTTP/1.0" 404 106 "-" "M
 9 189.242.68.59 - - [13/Dec/2009:06:29:13 +0100] "GET /demo HTTP/1.0" 200 238733 "-" "PSP-Intern
10 189.132.30.25 - - [13/Dec/2009:06:31:28 +0100] "GET /demo HTTP/1.0" 200 440285 "-" "PSP-Intern
11 189.242.68.59 - - [13/Dec/2009:06:31:41 +0100] "GET /demo HTTP/1.0" 200 627885 "-" "PSP-Intern
12 66.249.71.57 - - [13/Dec/2009:06:32:28 +0100] "GET /demo HTTP/1.1" 200 8698184 "-" "Mozilla/5.
13 192.114.107.4 - - [13/Dec/2009:06:34:08 +0100] "GET /demo.m3u HTTP/1.1" 200 92 "http://www.int
14 192.114.107.4 - - [13/Dec/2009:06:34:09 +0100] "GET /demo HTTP/1.1" 200 17146 "-" "NSPlayer/11
15 192.114.107.4 - - [13/Dec/2009:06:34:47 +0100] "GET /demo HTTP/1.1" 200 661366 "-" "NSPlayer/1
16 83.213.11.179 - - [13/Dec/2009:06:34:52 +0100] "GET /demo HTTP/1.0" 200 882684 "-" "PSP-Intern
17 76.108.234.173 - - [13/Dec/2009:06:35:00 +0100] "GET /demo HTTP/1.0" 200 296085 "-" "PSP-Inter
```

```
c.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:25 cerval sshd[27066]: Invalid user julia from 85.62.8.13
Sep 17 22:37:25 cerval sshd[27066]: error: Could not get shadow information for NOUSER
Sep 17 22:37:25 cerval sshd[27066]: Failed password for invalid user julia from 85.62.8.13 po
rt 33067 ssh2
Sep 17 22:37:26 cerval sshd[27068]: reverse mapping checking getaddrinfo for 85.62.8.13.stati
c.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:26 cerval sshd[27068]: Invalid user julia123 from 85.62.8.13
Sep 17 22:37:26 cerval sshd[27068]: error: Could not get shadow information for NOUSER
Sep 17 22:37:26 cerval sshd[27068]: Failed password for invalid user julia123 from 85.62.8.13
 port 33222 ssh2
Sep 17 22:37:27 cerval sshd[27070]: reverse mapping checking getaddrinfo for 85.62.8.13.stati
c.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:27 cerval sshd[27070]: Invalid user a from 85.62.8.13
Sep 17 22:37:27 cerval sshd[27070]: error: Could not get shadow information for NOUSER
Sep 17 22:37:27 cerval sshd[27070]: Failed password for invalid user a from 85.62.8.13 port 3
3365 ssh2
Sep 17 22:37:30 cerval sshd[27072]: reverse mapping checking getaddrinfo for 85.62.8.13.stati
c.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:30 cerval sshd[27072]: Invalid user julie from 85.62.8.13
Sep 17 22:37:30 cerval sshd[27072]: error: Could not get shadow information for NOUSER
Sep 17 22:37:30 cerval sshd[27072]: Failed password for invalid user julie from 85.62.8.13 po
rt 33488 ssh2
Sep 17 22:37:31 cerval sshd[27074]: reverse mapping checking getaddrinfo for 85.62.8.13.stati
c.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:31 cerval sshd[27074]: Invalid user julie123 from 85.62.8.13
Sep 17 22:37:31 cerval sshd[27074]: error: Could not get shadow information for NOUSER
Sep 17 22:37:31 cerval sshd[27074]: Failed password for invalid user julie123 from 85.62.8.13
 port 35041 ssh2
Sep 17 22:37:32 cerval sshd[27076]: reverse mapping checking getaddrinfo for 85.62.8.13.stati
c.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:32 cerval sshd[27076]: Invalid user a from 85.62.8.13
Sep 17 22:37:32 cerval sshd[27076]: error: Could not get shadow information for NOUSER
Sep 17 22:37:32 cerval sshd[27076]: Failed password for invalid user a from 85.62.8.13 port 3
5757 ssh2
Sep 17 22:37:32 cerval sshd[27078]: reverse mapping checking getaddrinfo for 85.62.8.13.stati
c.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:32 cerval sshd[27078]: Invalid user june from 85.62.8.13
Sep 17 22:37:32 cerval sshd[27078]: error: Could not get shadow information for NOUSER
Sep 17 22:37:32 cerval sshd[27078]: Failed password for invalid user june from 85.62.8.13 por
t 35930 ssh2
Sep 17 22:37:33 cerval sshd[27080]: reverse mapping checking getaddrinfo for 85.62.8.13.stati
c.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:33 cerval sshd[27080]: Invalid user june123 from 85.62.8.13
Sep 17 22:37:33 cerval sshd[27080]: error: Could not get shadow information for NOUSER
Sep 17 22:37:33 cerval sshd[27080]: Failed password for invalid user june123 from 85.62.8.13
port 36297 ssh2
Sep 17 22:37:34 cerval sshd[27082]: reverse mapping checking getaddrinfo for 85.62.8.13.stati
c.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:34 cerval sshd[27082]: Invalid user a from 85.62.8.13
Sep 17 22:37:34 cerval sshd[27082]: error: Could not get shadow information for NOUSER
Sep 17 22:37:34 cerval sshd[27082]: Failed password for invalid user a from 85.62.8.13 port 3
6423 ssh2
Sep 17 22:37:35 cerval sshd[27084]: reverse mapping checking getaddrinfo for 85.62.8.13.stati
c.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
```

```
[root@ontest log]# tail -f /var/log/messages
May 18 11:06:41 ontest dhcpd: DHCPINFORM from 10.8.9.21 via 10.8.9.1
May 18 11:06:41 ontest dhcpd: DHCPACK to 10.8.9.21 (50:e5:49:2e:cb:65) via eth0
May 18 11:06:42 ontest dhcpd: DHCPDISCOVER from 44:8a:5b:60:01:e0 via 10.2.39.10: netwo
May 18 11:06:42 ontest dhcpd: DHCPINFORM from 10.8.5.107 via 10.8.5.1
May 18 11:06:42 ontest dhcpd: DHCPACK to 10.8.5.107 (a4:1f:72:63:7c:8b) via eth0
May 18 11:06:43 ontest dhcpd: DHCPINFORM from 10.8.6.116 via 10.8.6.1
May 18 11:06:43 ontest dhcpd: DHCPACK to 10.8.6.116 (00:1c:c0:33:ba:cd) via eth0
May 18 11:06:43 ontest kernel: printk: 1 messages suppressed.
May 18 11:06:43 ontest kernel: Neighbour table overflow.
May 18 11:06:45 ontest dhcpd: DHCPINFORM from 10.8.18.28 via 10.8.18.1: unknown subnet
May 18 11:06:49 ontest kernel: printk: 1 messages suppressed.
May 18 11:06:49 ontest kernel: Neighbour table overflow.
May 18 11:06:52 ontest dhcpd: DHCPINFORM from 10.8.12.30 via 10.8.12.1
```

Produkter

splunk>™

logstash

fluentd

Uninett

logstash

elasticsearch.

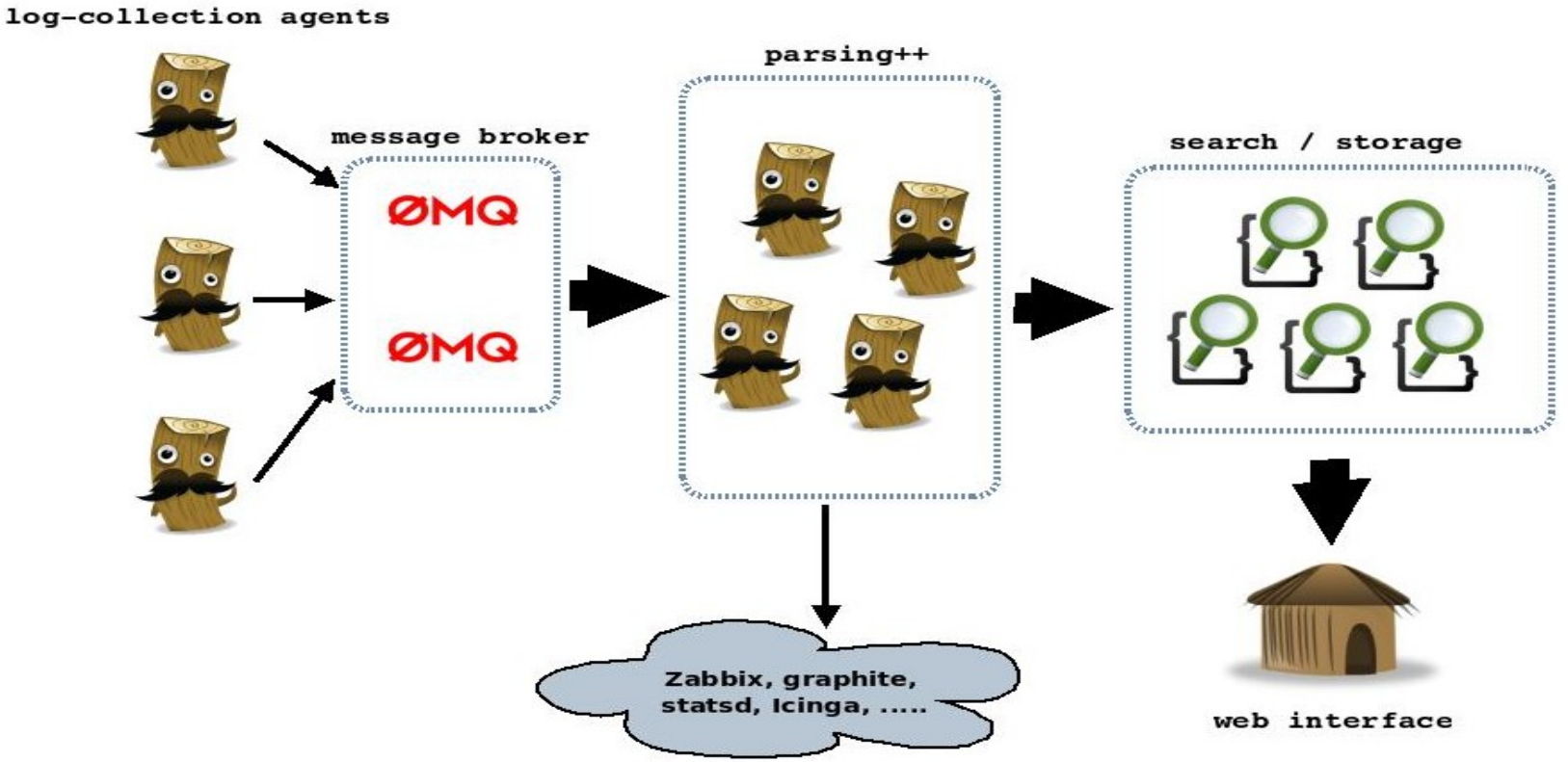
Kibana

Logstash

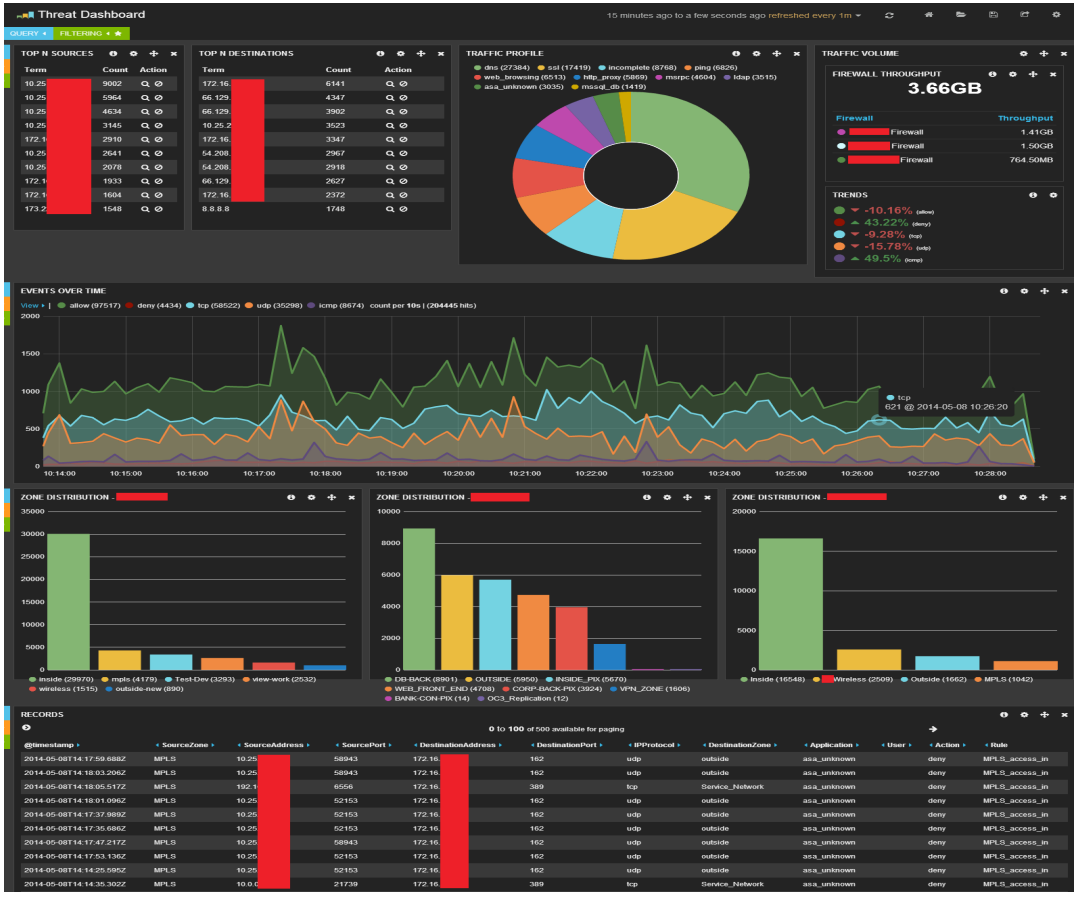

MySQL
Syslog
Apache
App
logstash
PARSE
TAG
FILTER
ENHANCE
Riemann
ElasticSearch
Graphite
Zabbix

Flow

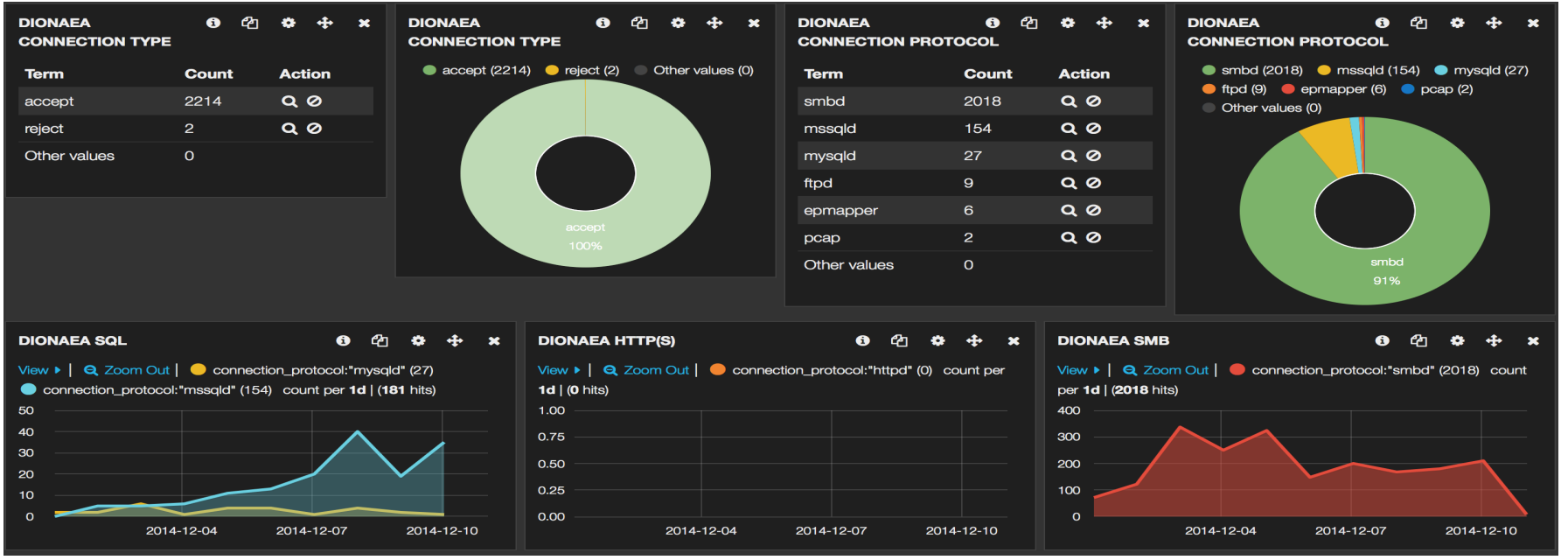
Arkitektur


log-collection agents
message broker
ØMQ
ØMQ
parsing++
search / storage
Zabbix, graphite,
statsd, Icinga, ...
web interface

Kibana


Threat Dashboard
15 minutes ago to a few seconds ago refreshed every 1m
QUERY
FILTERING
TOP N SOURCES
Term
Count
Action
TOP N DESTINATIONS
Term
Count
Action
TRAFFIC PROFILE
dns (27384)
ssl (17419)
incomplete (8768)
ping (6826)
web_browsing (6513)
http_proxy (5869)
msrpc (4604)
ldap (3515)
asa_unknown (3035)
mssql_db (1419)
TRAFFIC VOLUME
FIREWALL THROUGHPUT
3.66GB
Firewall
Throughput
Firewall 1.41GB
Firewall 1.50GB
Firewall 764.50MB
TRENDS
-10.16% (allow)
43.22% (deny)
-9.28% (tcp)
-15.78% (udp)
49.5% (icmp)
EVENTS OVER TIME
allow (97517)
deny (4434)
tcp (58522)
udp (35298)
icmp (8674)
count per 10s | (204445 hits)
tcp
621 @ 2014-05-08 10:26:20
ZONE DISTRIBUTION -
inside (29970)
mpls (4179)
Test-Dev (3293)
view-work (2532)
wireless (1515)
outside-new (890)
ZONE DISTRIBUTION -
DB-BACK (8901)
OUTSIDE (5950)
INSIDE_PIX (5670)
WEB_FRONT_END (4708)
CORP-BACK-PIX (3924)
VPN_ZONE (1606)
BANK-CON-PIX (14)
OC3_Replication (12)
ZONE DISTRIBUTION -
Inside (16548)
Wireless (2509)
Outside (1662)
MPLS (1042)
RECORDS
0 to 100 of 500 available for paging
@timestamp
SourceZone
SourceAddress
SourcePort
DestinationAddress
DestinationPort
IPProtocol
DestinationZone
Application
User
Action
Rule
2014-05-08T14:17:59.688Z MPLS 58943 162 udp outside asa_unknown deny MPLS_access_in
2014-05-08T14:18:03.206Z MPLS 58943 162 udp outside asa_unknown deny MPLS_access_in
2014-05-08T14:18:05.517Z MPLS 6556 389 tcp Service_Network asa_unknown deny MPLS_access_in
2014-05-08T14:18:01.096Z MPLS 52153 162 udp outside asa_unknown deny MPLS_access_in
2014-05-08T14:17:37.989Z MPLS 52153 162 udp outside asa_unknown deny MPLS_access_in
2014-05-08T14:17:35.686Z MPLS 52153 162 udp outside asa_unknown deny MPLS_access_in
2014-05-08T14:17:47.217Z MPLS 58943 162 udp outside asa_unknown deny MPLS_access_in
2014-05-08T14:17:53.136Z MPLS 52153 162 udp outside asa_unknown deny MPLS_access_in
2014-05-08T14:14:25.595Z MPLS 52153 162 udp outside asa_unknown deny MPLS_access_in
2014-05-08T14:14:35.302Z MPLS 21739 389 tcp Service_Network asa_unknown deny MPLS_access_in

Kibana


DIONAEA CONNECTION TYPE
Term Count Action
accept 2214
reject 2
Other values 0
DIONAEA CONNECTION TYPE
accept (2214) reject (2) Other values (0)
accept
100%
DIONAEA CONNECTION PROTOCOL
Term Count Action
smbd 2018
mssqld 154
mysqld 27
ftpd 9
epmapper 6
pcap 2
Other values 0
DIONAEA CONNECTION PROTOCOL
smbd (2018) mssqld (154) mysqld (27)
ftpd (9) epmapper (6) pcap (2)
Other values (0)
smbd
91%
DIONAEA SQL
View | Zoom Out | connection_protocol:"mysqld" (27)
connection_protocol:"mssqld" (154) count per 1d | (181 hits)
50 40 30 20 10 0
2014-12-04 2014-12-07 2014-12-10
DIONAEA HTTP(S)
View | Zoom Out | connection_protocol:"httpd" (0) count per 1d | (0 hits)
1.00 0.75 0.50 0.25 0.00
2014-12-04 2014-12-07 2014-12-10
DIONAEA SMB
View | Zoom Out | connection_protocol:"smbd" (2018) count per 1d | (2018 hits)
400 300 200 100 0
2014-12-04 2014-12-07 2014-12-10

Kibana


Logstash Search
2 days ago to 3 minutes ago
QUERY
bytes:[0 TO 4000000] AND @tags:success
FILTERING
EVENTS OVER TIME
View | Zoom Out | html (ext) (888) php (ext) (659) png (ext) (317) gif (ext) (229) css (ext) (121) count per 30m | (2214 hits)
MAP
REVENUE
22%
VOLUME
9%
TOP DESTINATIONS
Other values 42%
CN 19%
IN 16%
TOP SOURCES
Other values 52%
IN 19%
US 10%
GEO PAIRS
ALL EVENTS
0 to 100 of 500 available for paging
Fields
Type to filter...
@message
@tags
@tags
geo.srcdst
extension
clientip
bytes
id
phpmemory
response
success,security MY:VN html 167.12.22.189 8540 1066 200
success,info IT:MM png 164.87.170.73 2045 1903 200
success,info AR:ES html 222.23.102.238 1801 1133 200
success,info IN:DZ html 138.226.66.81 7029 1801 200

usit-gid@rt.uio.no