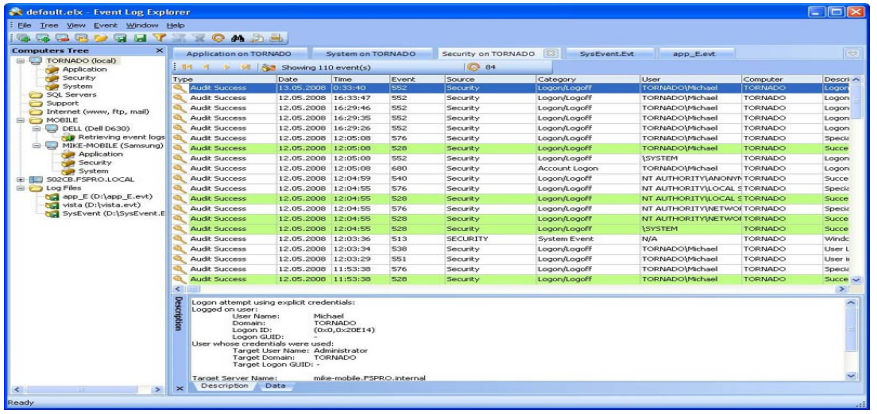
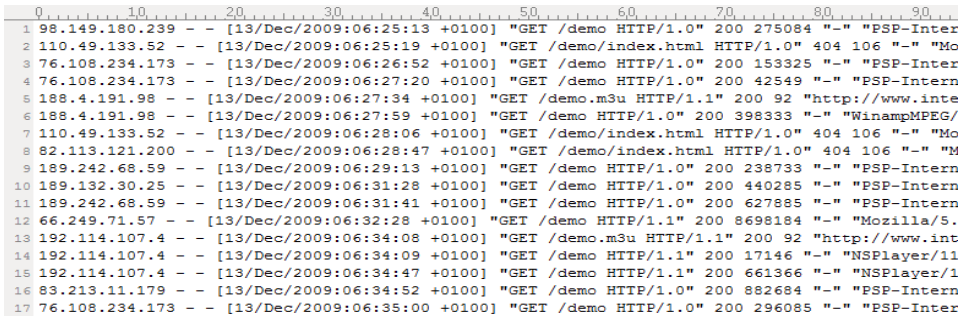
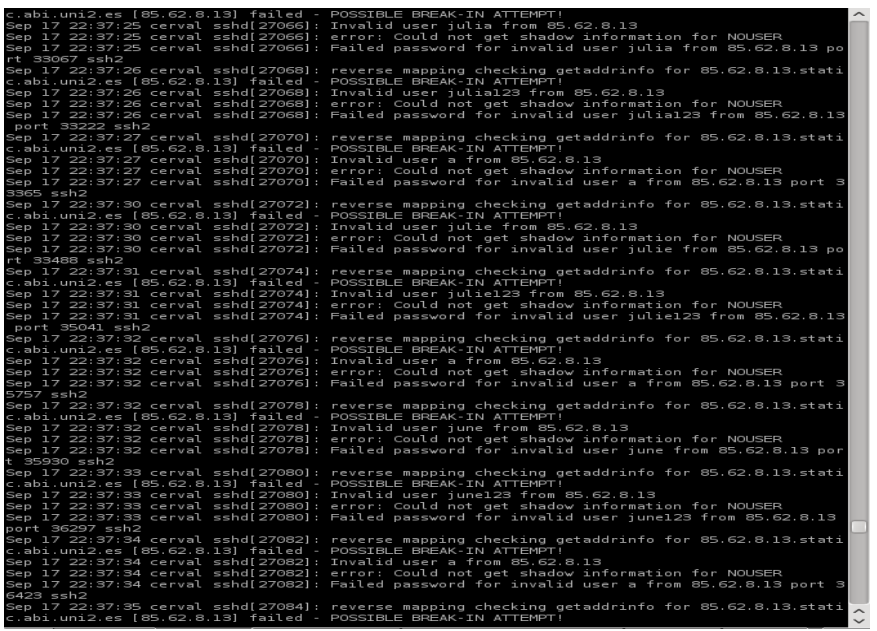
Sentralisert logging på UiO

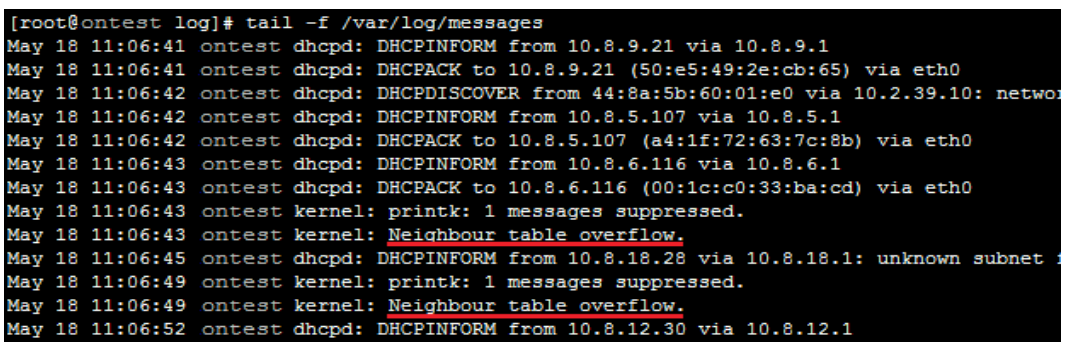
Rafael Martinez Guerrero
It-drift-gd-gid
IT-konferanse 2016
Universitetet i Oslo


CONFIDENTIAL


default.elx - Event Log Explorer
File Tree View Event Window Help
Computers Tree
TORNADO (local)
Application
Security
System
SQL Servers
Support
Internet (www, ftp, mail)
MOBILE
DELL (Dell D630)
Retrieving event logs
MIKE-MOBILE (Samsung)
Application
Security
System
S02CB.FSPRO.LOCAL
Log Files
app_E (D:\app_E.evt)
vista (D:\vista.evt)
SysEvent (D:\SysEvent.E
Application on TORNADO
System on TORNADO
Security on TORNADO
SysEvent.Evt
app_E.evt
Showing 110 event(s)
Type Date Time Event Source Category User Computer
Audit Success 12.05.2008 16:29:46 552 Security Logon/Logoff TORNADO\Michael TORNADO
Audit Success 12.05.2008 16:29:35 552 Security Logon/Logoff TORNADO\Michael TORNADO
Audit Success 12.05.2008 16:29:26 552 Security Logon/Logoff TORNADO\Michael TORNADO
Audit Success 12.05.2008 12:05:08 576 Security Logon/Logoff TORNADO\Michael TORNADO
Audit Success 12.05.2008 12:05:08 528 Security Logon/Logoff TORNADO\Michael TORNADO
Audit Success 12.05.2008 12:05:08 552 Security Logon/Logoff \SYSTEM TORNADO
Audit Success 12.05.2008 12:05:08 680 Security Account Logon TORNADO\Michael TORNADO
Audit Success 12.05.2008 12:04:59 540 Security Logon/Logoff NT AUTHORITY\ANONYM TORNADO
Audit Success 12.05.2008 12:04:55 576 Security Logon/Logoff NT AUTHORITY\LOCAL S TORNADO
Audit Success 12.05.2008 12:04:55 528 Security Logon/Logoff NT AUTHORITY\LOCAL S TORNADO
Audit Success 12.05.2008 12:04:55 576 Security Logon/Logoff NT AUTHORITY\NETWOI TORNADO
Audit Success 12.05.2008 12:04:55 528 Security Logon/Logoff NT AUTHORITY\NETWOI TORNADO
Audit Success 12.05.2008 12:04:55 528 Security Logon/Logoff \SYSTEM TORNADO
Audit Success 12.05.2008 12:03:36 513 SECURITY System Event N/A TORNADO
Audit Success 12.05.2008 12:03:34 538 Security Logon/Logoff TORNADO\Michael TORNADO
Audit Success 12.05.2008 12:03:29 551 Security Logon/Logoff TORNADO\Michael TORNADO
Audit Success 12.05.2008 11:53:38 576 Security Logon/Logoff TORNADO\Michael TORNADO
Audit Success 12.05.2008 11:53:38 528 Security Logon/Logoff TORNADO\Michael TORNADO
Description
Logon attempt using explicit credentials:
Logged on user:
User Name: Michael
Domain: TORNADO
Logon ID: (0x0,0x20E14)
Logon GUID: -
User whose credentials were used:
Target User Name: Administrator
Target Domain: TORNADO
Target Logon GUID: -
Target Server Name: mike-mobile.FSPRO.internal
Description Data
Ready

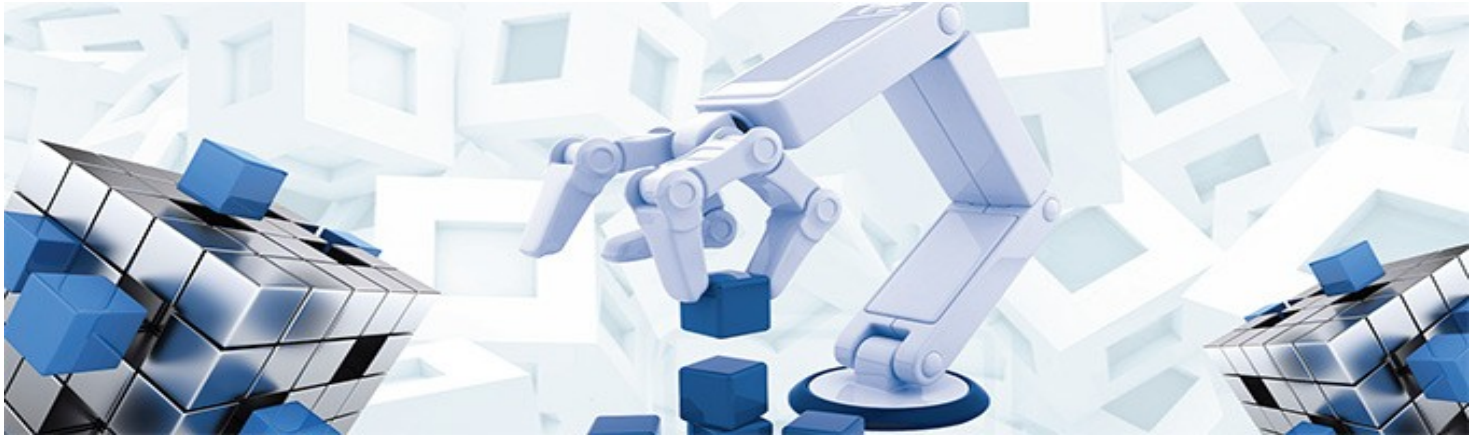

1 98.149.180.239 - - [13/Dec/2009:06:25:13 +0100] "GET /demo HTTP/1.0" 200 275084 "-" "PSP-Inter
2 110.49.133.52 - - [13/Dec/2009:06:25:19 +0100] "GET /demo/index.html HTTP/1.0" 404 106 "-" "Mo
3 76.108.234.173 - - [13/Dec/2009:06:26:52 +0100] "GET /demo HTTP/1.0" 200 153325 "-" "PSP-Inter
4 76.108.234.173 - - [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

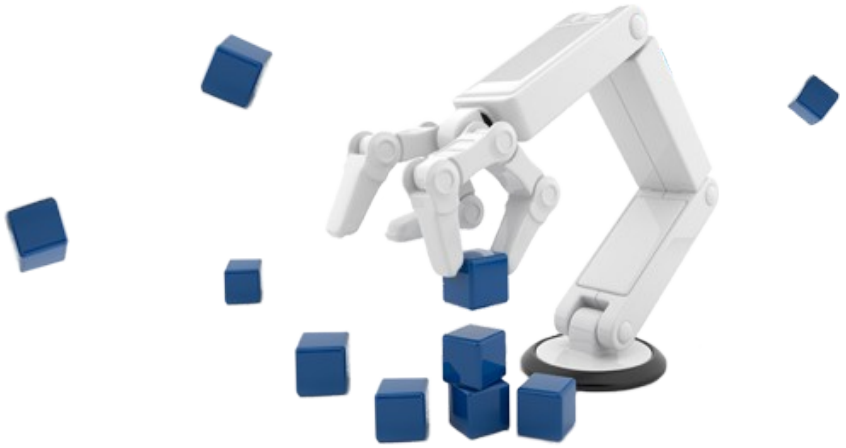

c.abi.uni2.es [85.62.8.13] failed - POSSIBLE BREAK-IN ATTEMPT!
Sep 17 22:37:25 cerval sshd[27066]: Invalid user julia from 85.62.8.13
Sep 17 22:37:25 cerval sshd[27066]: error: Could not get shadow information for NOUSER
Sep 17 22:37:25 cerval sshd[27066]: Failed password for invalid user julia from 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


Search


Projected sales of main products in 2013
Share of market activity
Distribution of the securities market key players
Revenue growth divisions
TYU division
FRT division
Distribution marketing participation in the securities market.






STANDARDS


OPEN
SOURCE
SOFTWARE
ACCESS
FREE
WORK
COPYRIGHT
SYSTEM
INNOVATION
CONCEPT
CREATED
DEVELOPMENT
AVAILABLE
MEDIA
EDIT
COMMONS
CULTURE
CODE
USED
PDF
BEER
RESEARCH
TECHNOLOGY
OPEN-SOURCE
COMPUTER
COMMUNITY
CULTURAL
INTERNET
PUBLIC
INFORMATION
SHARING
DIGITAL
ALSO
EXAMPLE
PRODUCTION
CONTENT
INITIATIVE
ETHICS
FORMAT
ECONOMIC
COST

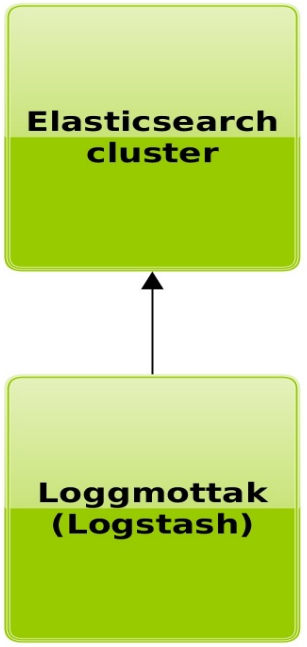
ELK stack

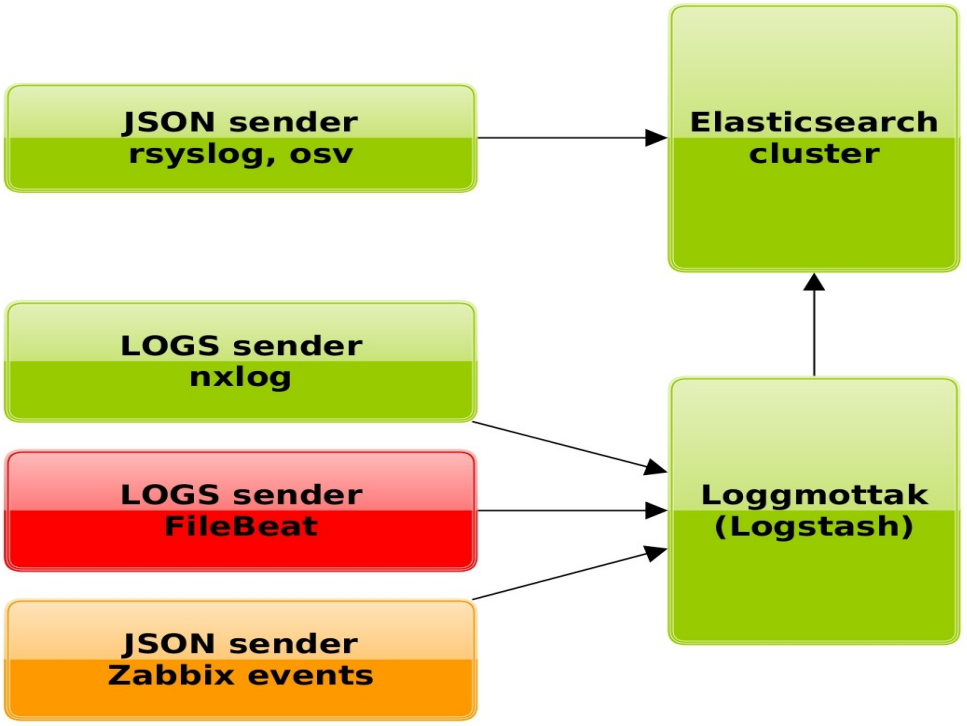
logstash

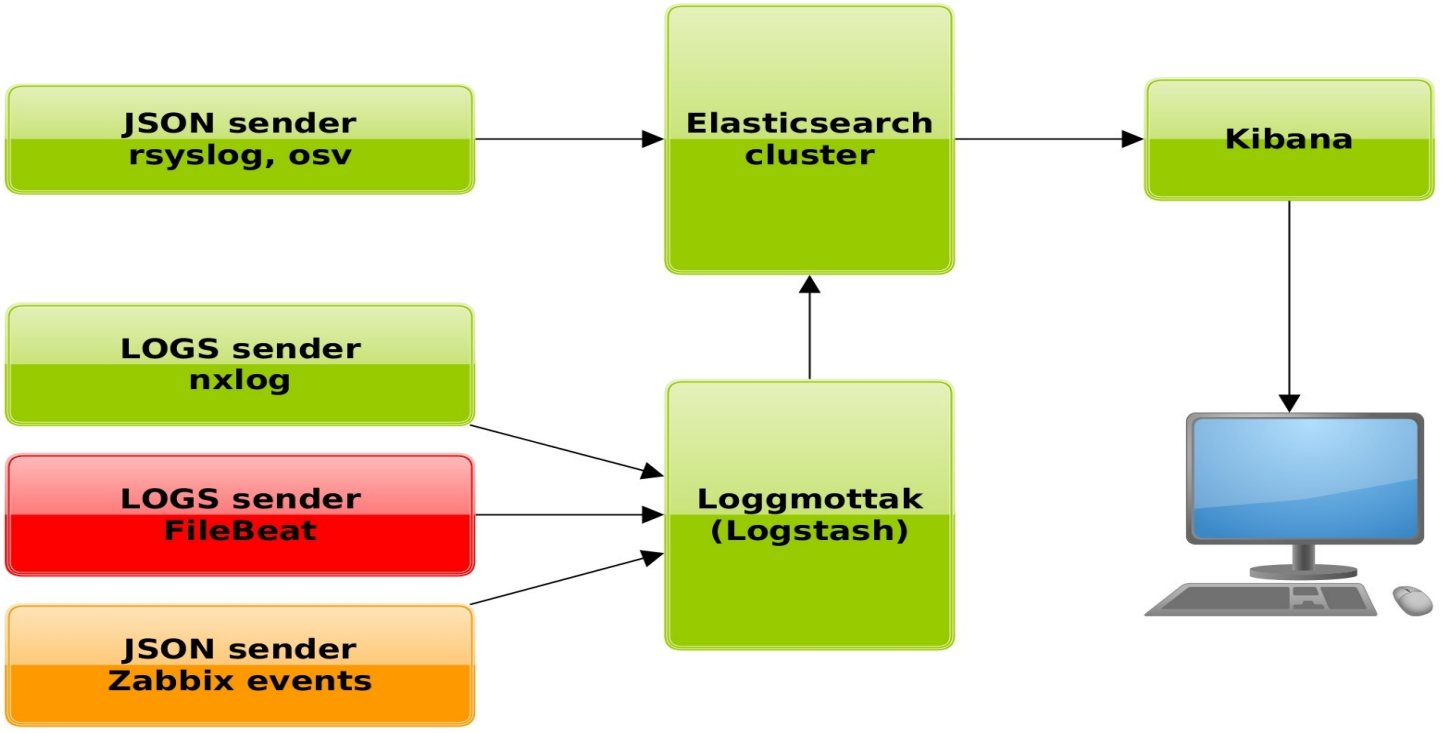
elasticsearch.

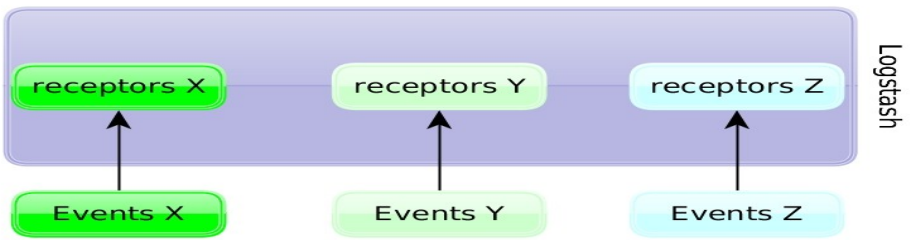
Kibana

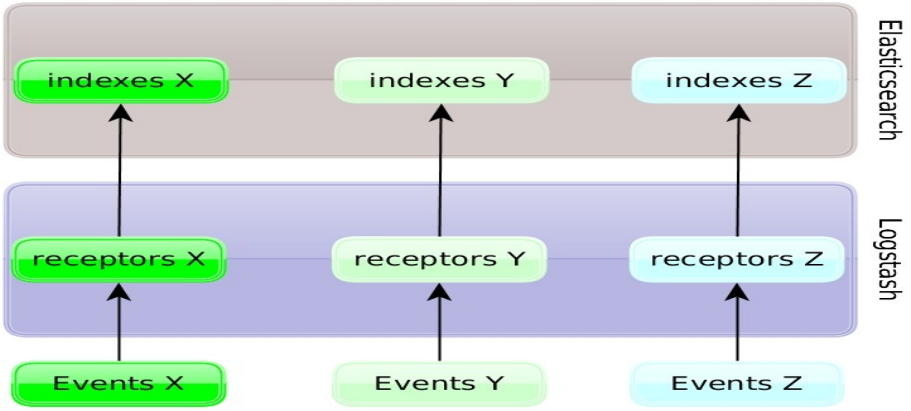

Elasticsearch
cluster

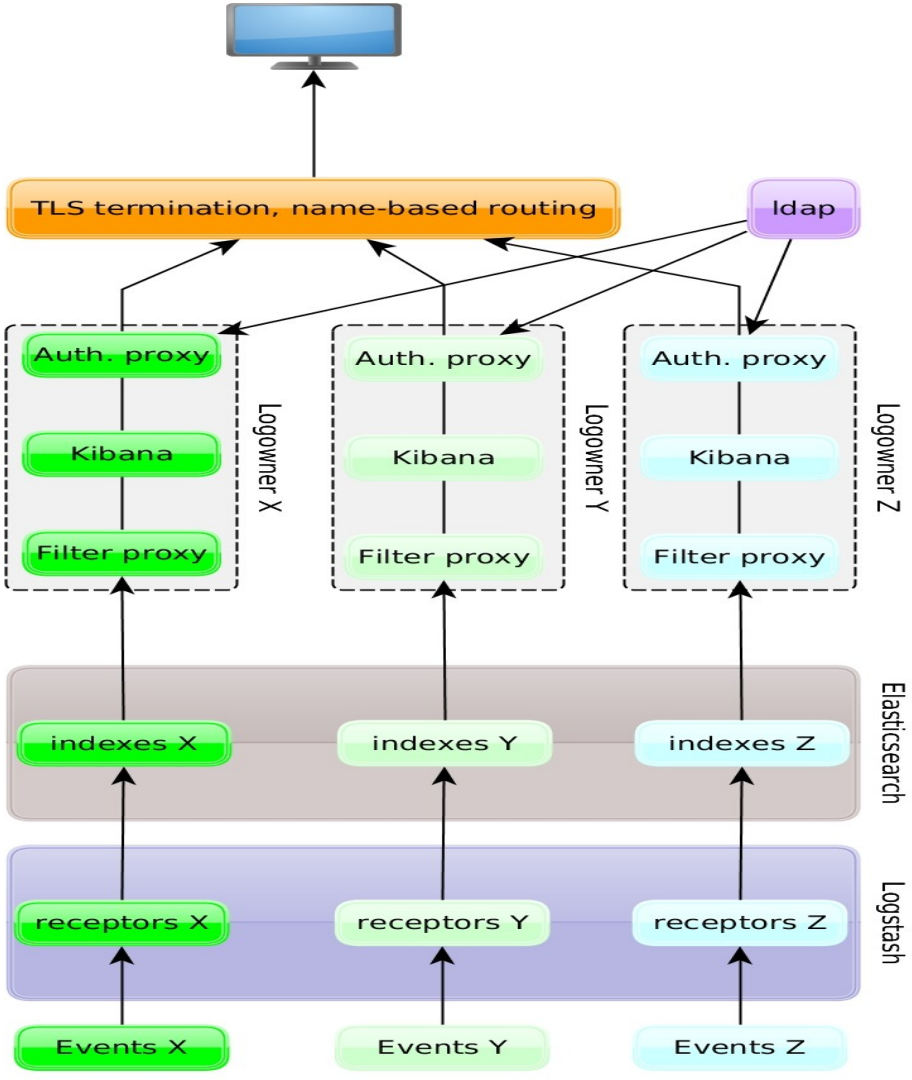

Elasticsearch
cluster
Loggmottak
(Logstash)


JSON sender
rsyslog, osv
Elasticsearch
cluster
LOGS sender
nxlog
LOGS sender
FileBeat
Loggmottak
(Logstash)
JSON sender
Zabbix events


JSON sender
rsyslog, osv
Elasticsearch
cluster
Kibana
LOGS sender
nxlog
LOGS sender
FileBeat
JSON sender
Zabbix events
Loggmottak
(Logstash)

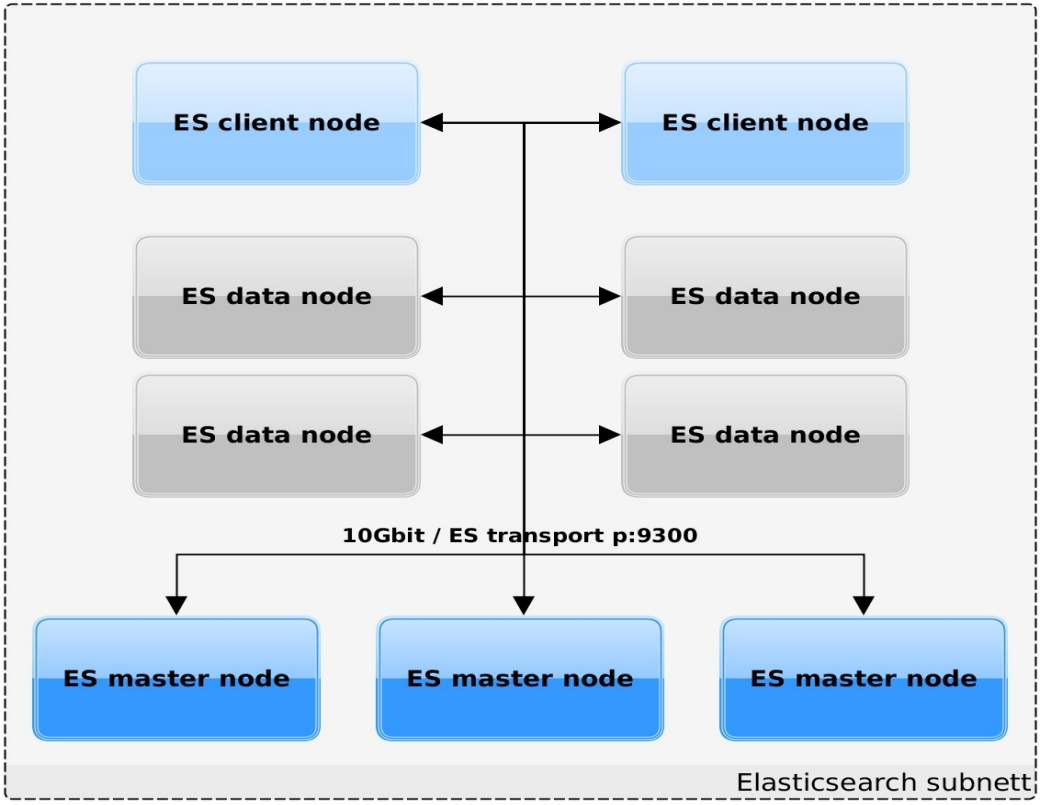

receptors X
receptors Y
receptors Z
Logstash
Events X
Events Y
Events Z

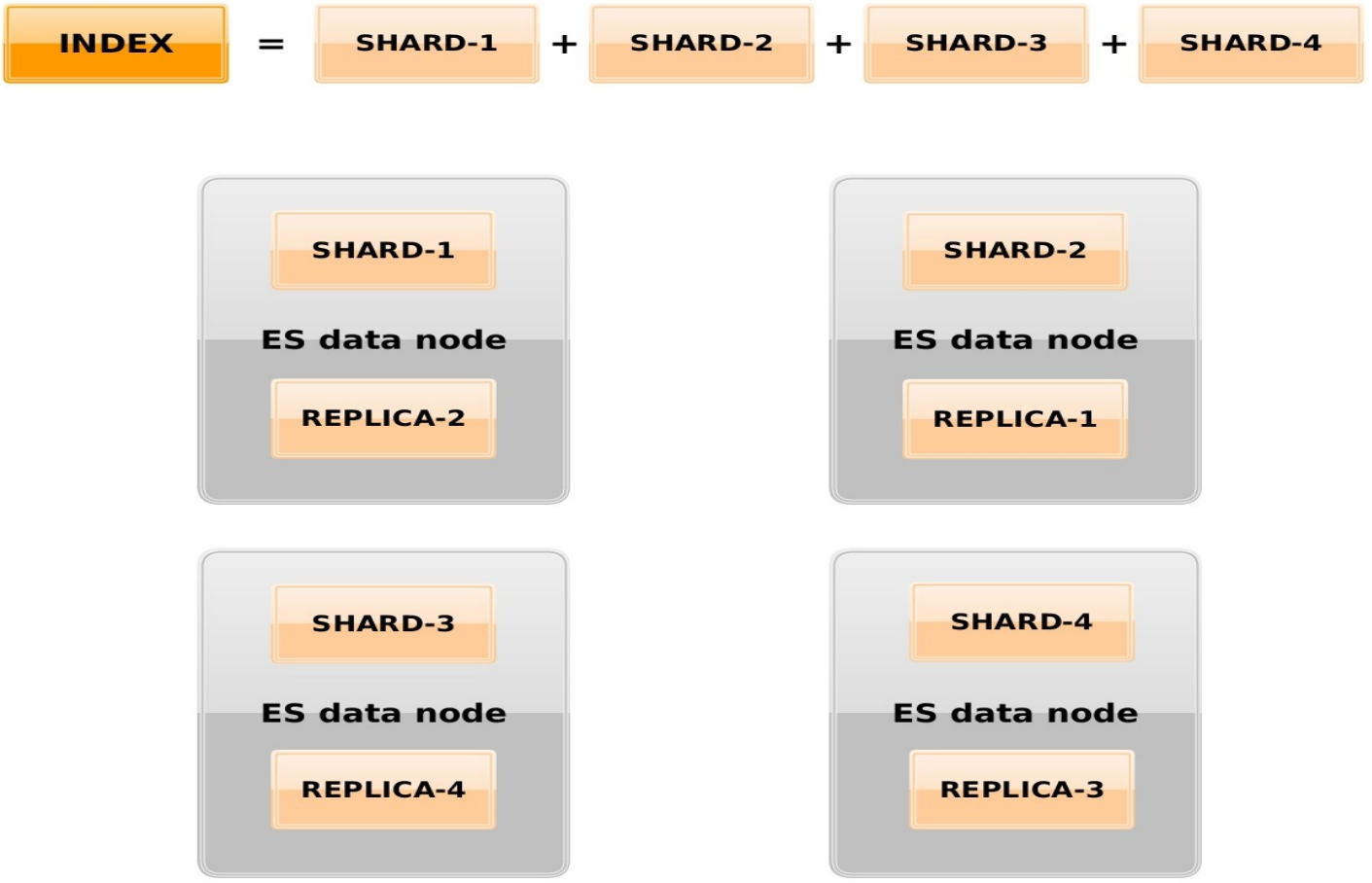

indexes X
indexes Y
indexes Z
Elasticsearch
receptors X
receptors Y
receptors Z
Logstash
Events X
Events Y
Events Z


TLS termination, name-based routing
ldap
Auth. proxy
Kibana
Filter proxy
Logowner X
Auth. proxy
Kibana
Filter proxy
Logowner Y
Auth. proxy
Kibana
Filter proxy
Logowner Z
indexes X
indexes Y
indexes Z
Elasticsearch
receptors X
receptors Y
receptors Z
Logstash
Events X
Events Y
Events Z

Elasticsearch

- SSD 1.4TB x 4 = 5.6TB
- 256GB ram – håndtering av indekser
- 128GB ram – håndtering av spørringer
- 3 master noder
- Bonding - 2 x 10Gbit




INDEX
=
SHARD-1
+
SHARD-2
+
SHARD-3
+
SHARD-4
SHARD-1
ES data node
REPLICA-2
SHARD-2
ES data node
REPLICA-1
SHARD-3
ES data node
REPLICA-4
SHARD-4
ES data node
REPLICA-3

usit-gid@usit.uio.no