Logganalyse – hvorfor og hvordan

Jon Strømme, tjenesteansvarlig

UNINETT

Hvorfor: rask og effektiv oversikt over drift av systemer

- Med et blikk, se last, bruk, profil over tid, akkurat de parameterne man ønsker
- Gå inn på detaljer, se om nødvendig rå-loggene
- Du må ha Logganalyse for å se oversiktene fra Sikkerhetsanalyse

  som er en del av UNINETTs grunntjeneste, så Logganalyse for Sikkerhetsanalyse blir ikke fakturert. Logganalyse for alle andre tjenester koster – meget lite i forhold til alternativene

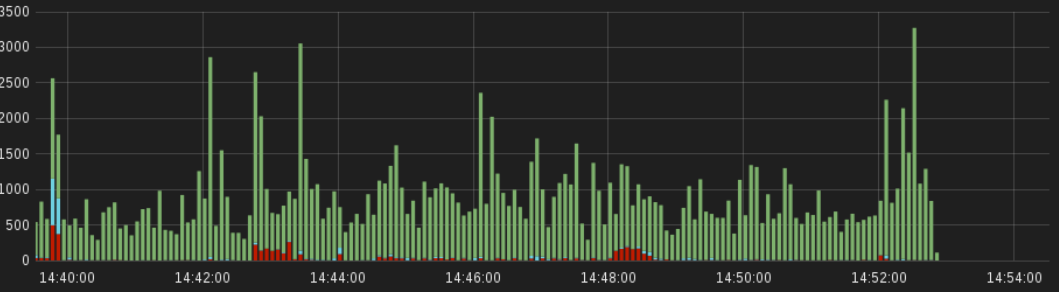
- Eksempel 1: Windows event log
- Eksempel 2: Apache weblog
- Eksempel 3: Sikkerhetsanalyse

TERING

time must
field : @timestamp
from : now-15m
to : now

WINDOWS-EVENT-LOG

View | Zoom Out |



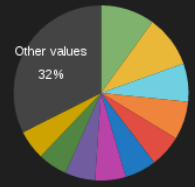
WINDOWS-FIREWALL

View | Zoom Out |

SEVERITY

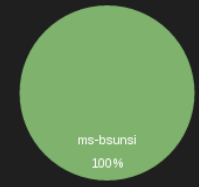
Term	Count	Action
INFO	139349	
ERROR	4488	
WARNING	2821	
DEBUG	38	
CRITICAL	18	

HOST



TYPE

SERVICE



WIN-EVENT-SOURCE(NOT-INFO)

Term	Count	Action
Microsoft-Windows-FailoverClustering	3373	
Microsoft-Windows-WMI-Activity	2031	
Microsoft-Windows-ServerManager-ManagementProvider	363	
Microsoft-Windows-PowerShell	349	
Health Service Modules	331	
Microsoft-Windows-WinRM	257	
Microsoft-Windows-KnownFolders	244	
Microsoft-Windows-SMBClient	114	
HealthService	111	

WIN-EVENT-CHANNEL(NOT-INFO)

Term	Count	Action
Microsoft-Windows-FailoverClustering/Diagnostic	3371	
Microsoft-Windows-WMI-Activity/Operational	2031	
Operations Manager	443	
Microsoft-Windows-ServerManager-MgmtProvider/Operational	356	
Microsoft-Windows-PowerShell/Operational	349	
Microsoft-Windows-WinRM/Operational	257	
Microsoft-Windows-Known Folders API Service	244	
Microsoft-Windows-SmbClient/Connectivity	114	
Microsoft-Windows-Hyper-V-Integration-Admin	43	


VENTS OVER TIME
Zoom Out | (217530) count per 5m | (217530 hits)
16:00 11-01
18:00 11-01
20:00 11-01
22:00 11-01
00:00 11-02
02:00 11-02
04:00 11-02
06:00 11-02
08:00 11-02
10:00 11-02
12:00 11-02
14:00 11-02
REPONSE CODE
Term Count Action
200 109333
204 52002
304 10655
303 8175
301 3768
302 3694
401 1447
404 555
403 534
499 498
Other values 399
TYPES
haproxy 12%
apache-access 88%
LOGSOURCE
vltrd035 50%
vltrd036 50%
YTES READ
Zoom Out | (217477) bytes_read total per 10m | (217477 hits)
BYTES SENT
View | Zoom Out | (217481) bytes total per 5m | (217481 hits)
48 MB
40 MB
32 MB
24 MB
16 MB
8 MB
0 B
USER AGENTS
Chrome 44%
Other 32%
USER AGENT OS
Other 33%
Windows 11%
Linux 33%
LL EVENTS
ields
0 to 100 of 500 available for paging

QUERY ▸

*

FILTERING ▸

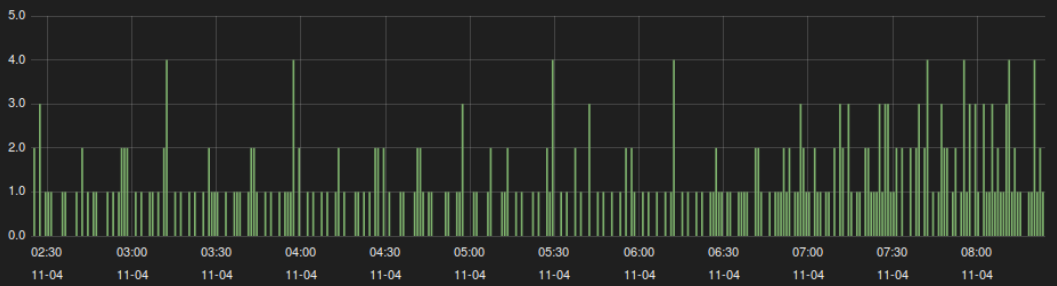
time must
field : @timestamp
from : now-6h
to : now

field must
field : event_type
query : "alert"

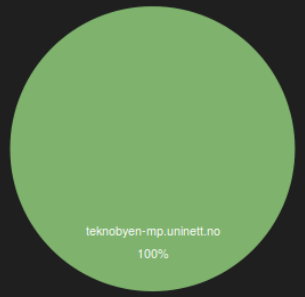
terms must
field : logsource.raw
value : teknobyen-mp.uninett.no

EVENTS OVER TIME

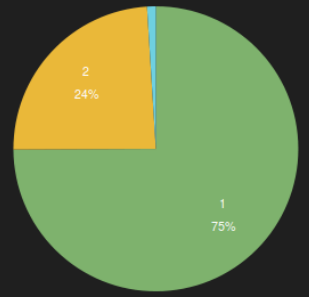
View ▸ | Zoom Out | * (304) count per **1m** | (**304** hits)



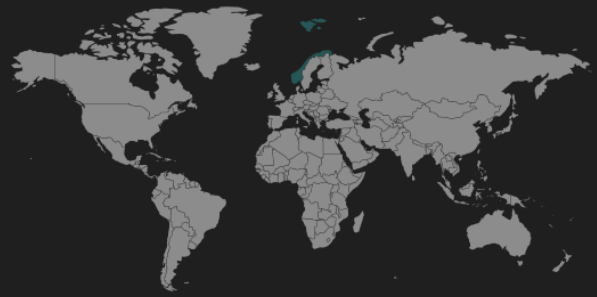
LOG SOURCE



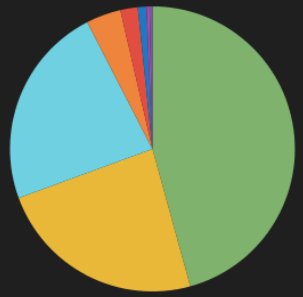
SEVERITY



SRC COUNTRY

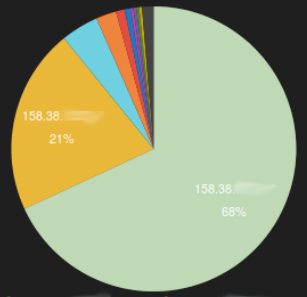


ALERTS



- ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted (139)
- ET POLICY Vulnerable Java Version 1.7.x Detected (72)
- ETPRO POLICY Python Requests Suspicious User Agent (70)
- ET CNC Shadowserver Reported CnC Server IP group 3 (12)
- ET POLICY SSLv3 inbound connection to server vulnerable to POODLE attack (6)
- ET INFO Session Traversal Utilities for NAT (STUN Binding Request obsolete rfc 3489 CHANGE-REQUEST attribute change IP flag false change port flag false) (3)
- ET POLICY Vulnerable Java Version 1.8.x Detected (1)
- ET CNC Shadowserver Reported CnC Server IP group 39 (1)

SRCIP



- 158.38. (207)
- 158.38. (64)
- 158.38. (13)
- 158.38. (7)
- 128.39. (3)
- 158.38. (2)
- 158.38. (1)
- 158.38. (1)
- 158.38. (1)
- 158.38. (1)
- Missing field (0)
- Other values (4)

Hvordan: Påmelding og oppkobling

Påmelding:

- Du går inn på agora.uninett.no/web/institusjonsansvarlige
  Der finner du riktig sjef ved din institusjon. Hvis det ikke er utpekt noen ennå, ta kontakt.
- Sjefen går inn på agora.uninett.no/group/institusjonsansvarlige og trykker på «Meld på» for Logganalyse. Angir teknisk kontakt, kanskje deg. Trykker på «Lagre» – ferdig!
  UNINETT tar det videre med teknisk kontakt.

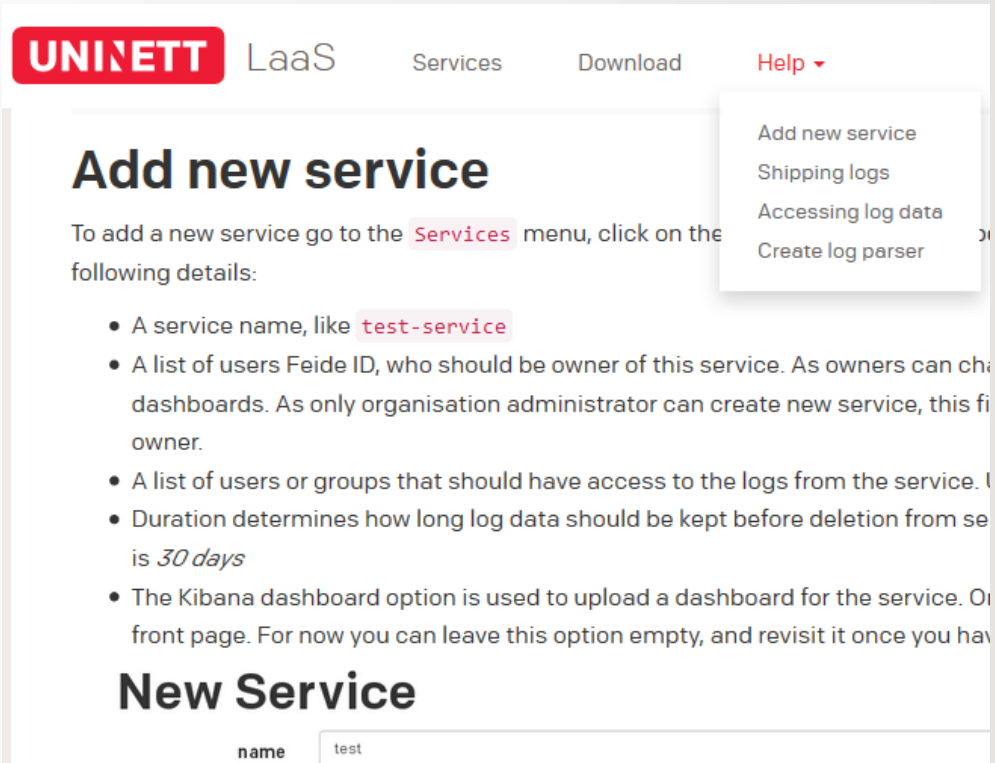
Oppkobling:

- UNINETT jobber sammen med teknisk kontakt < 1 dag for å etablere brukere, tilgang og en trygg veg for loggene.
- Teknisk kontakt legger inn og tester ønskede tjenester. Raskt!

UNINETT

Selvbetjening for logger, med støtte

- Det er instruksjoner i tjenesten, men vi tar det gjerne sammen første gang.



Og så er du i gang!

- Mer informasjon finner du på

  www.uninett.no/tjenester/logganalyse