

1/2

context

dit document beschrijft hoe je met queries werkt in ELK stack. Deze zijn de basis voor verdere verwerking van je logdate:

- queries \rightarrow visualisaties: geven je queries weer in visueel aantrekkelijk formaat
- visualisties \rightarrow dashboards: geven je visualisaties weer in dashboard waarbij je in 1 oogopslag je data ziet

query maken

- 1. Discover: Search
- 2. (change): selecteer de index die je wilt gebruiken (filebeat, metricbeat, ...) nu worden alle pages weergegeven binnen die index. Nu kan je best wat **filteren**
- 3. (Search)(1):typ het veld in waarop je wilt zoeken:
 - 1. log.file.path: logbestand
 - 2. event.dataset.key: soort dataset
- 4. om je zoekactie te verfijnen, combineer je velden ahv AND en OR
- 5. druk op het **kalender**(2) icoontje om je zoekactie in tijd te beperken (dag, week, maand, afgelopen ... uren, ...)
- 6. het **zoekresultaat** wordt weegegeven in een staafdiagram (3) met het aantal gevonden pages/tijdstip:



nu kan je de gevonden documenten verder filteren:

- 1. klik in available fields op het veldje dat je wilt zien
 - 1. staafdiagram geeft resultaten aflopend weer, met vermelding van:

- 1. aantal documenten (muis-over)
- 2. percent van totaal aantal resulaten
- 3. mogelijkheid resulten in filter op te nemen/uit te sluiten (+ en teken)

J ,				
				NOST.10: 0840009010/248T1845104800T0048TA NOST.0S.NAME: CONTUS LINUX NOST.OS.TAMILY: FOONAT NOST.OS.VEFSION: / (COFE)
process.executable			host.os.codename: Core host.os.kernel: 3.10.0-1062.9.1.el7.x86_64 host.os.platform: centos host.architecture: x86_64	
process.name				host.hostname: kv-tb01 tags: beats_input_raw_event, _grokparsefailure user.name: tomcat-gui process.pid: 1838 process.args: //
Top 5 values in 223 / 223 records			> Mar 4, 2020 @ 14:32:01.127	agent.id: e228ed13-4955-4298-b369-85e3d53e5bc1 agent.version: 7.6.0 agent.type: metricbeat agent.ephemeral_id: cfaa1468-1944-4
ava	ର୍ ର୍	Q 3% Q 5%		ae84-e6c638764235 agent.hostname: kv-tb01 @version: 1 host.containerized: false host.name: kv-tb01
	53.8%			host.id: e84d0a9b107248f18451d4806f0e48fa host.os.family: redhat host.os.name: CentOS Linux host.os.version: 7 (Core)
node	Q Q 12.5%			host.os.codename: Core host.os.kernel: 3.10.0-1062.9.1.el7.x86_64 host.os.platform: centos host.architecture: x86_64
metricbeat	0.0%			host.hostname: kv-tb01 tags: beats_input_raw_event, _grokparsefailure user.name: root process.pid: 11593 process.args: /usr/sl
	13.5%		> Mar 4, 2020 @ 14:32:01.127	anant id: a228ad12_4055_4208_h260_85a2d52a5hc1 anant tuna: matrichast anant vareion: 7 5 8 anant anhamaral id: cfaa1468_1044_4
systemd-journal	ଷ୍	Q 5% Q 4%		agent at construction and based on the second state of the second
	13.5%			aeo4-eoco38/04235 agent.hostname: kv-tbel vversion: i host.containerized: haise host.name: kv-tbel
rsyslogd	ଉ ଉ			host.id: e84d0a9b107248f18451d4806f0e48fa host.os.family: redhat host.os.name: CentOS Linux host.os.version: 7 (Core)
	4%			host.os.codename: Core host.os.kernel: 3.10.0-1062.9.1.el7.x86_64 host.os.platform: centos host.architecture: x86_64
process.pgid				host.hostname: kv-tb01 tags: beats_input_raw_event, _grokparsefailure user.name: root process.pid: 676 process.args: /usr
process.pid			> Mar 4, 2020 @ 14:32:01.127	agent.id: e228ed13-4955-4298-b369-85e3d53e5bc1 agent.type: metricbeat agent.version: 7.6.0 agent.ephemeral_id: cfaa1468-1944-4

- 2. bovenstaand voorbeeld:
 - 1. toont top5 van processen die werden gevonden in 223 zoekresultaten.
 - 2. wil ik enkel de java processen zien, dan klik ik op +-teken naast java

query bewaren

vaak wil je de gevonden resultaten verder verwerken ivv visualizations of elk_stack:dashboards. Doe dit als volgt:

- 1. klik in het menu op Save
- geef een betekenisvolle <u>naam</u> op. Gezien je die queries later verwerkt in je dashboard/visualizaties, kies je best een naam die duidelijk zegt wat de query doet.
- 3. vink aan: include filters
- 4. Save

Nu is deze query een **source** die je als dusdanig bij visualizations verder kunt gebruiken.

meer info

voeg hier linken toe naar verdere uitleg

elk stack

From: https://louslab.be/ - **Lou's lab**

Permanent link: https://louslab.be/doku.php?id=elk_stack:query

Last update: 2024/11/16 18:14

