query

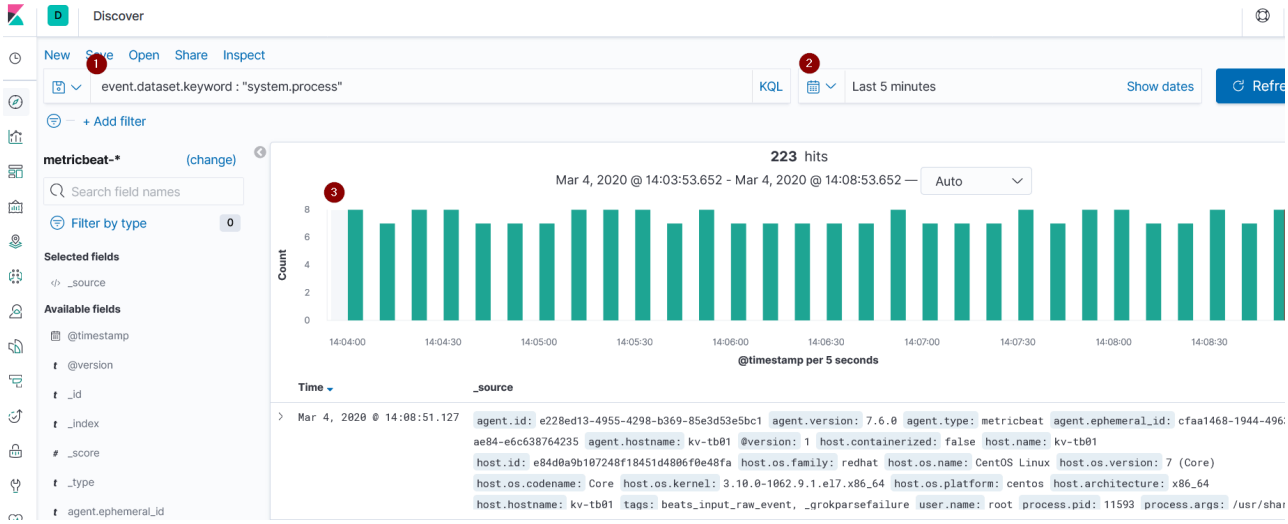
context

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

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

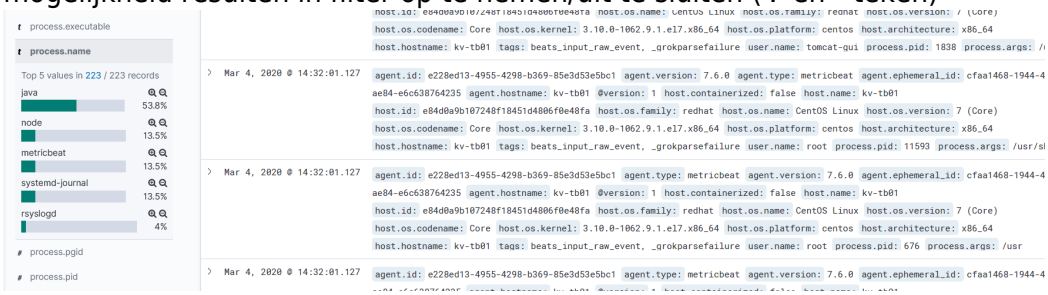
query maken

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)



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**
2. geef een betekenisvolle naam 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**