Kibana

context

dit document verzamelt info rond Kibana, het venster op de ELK stack. \\3 functies:

- visualiseer je data: zoek de naald in de hooiberg
- monitoring & beheer: hou je ELK stack in de gaten en beheerde verschillende componenten
- eigen oplossingen: gebruik modules om je applicatie-specifieke data te doorzoeken.

zoeken

- start vanuit **Dashboards**
- gebruik de **datepicker** zoveel mogelijk. Hiermee kan je datum ingeven en de slider rechts gebruiken voor een specifiek tijdstip
- query bar gaat uit van Kibana Query Language
- resultaten worden weergegeven als **documenten** in tab of JSON-formaat.
- binnen deze resulaten kan je op bepaalde velden klikken die automatisch in de filter verschijnen
- **dashboard** geven je vrijheid data op je eigen manier weer te geven.
- **visualizations**: de manier waarop je zoekactie wordt weergegeven (pie, cloud, tabel, ...) deze kan je dan later gebruiken in je dashboards. Zo maak je visualizations aan.

problemen, problemen

1. melding: `failed to find message`
2. oorzaak: als een document geen messageveld heeft (cfr Elastic Common Scheme), wordt die fout getoond. Dat betekent dus dat het logbestand een inhoud heeft die niet overeenkomt met het formaat dat ECS voor message hanteert.
3. oplossing: ???

meer info

- Getting started with Kibana

elk stack

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

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

Last update: **2024/11/16 18:14**