

# visualizations



## context

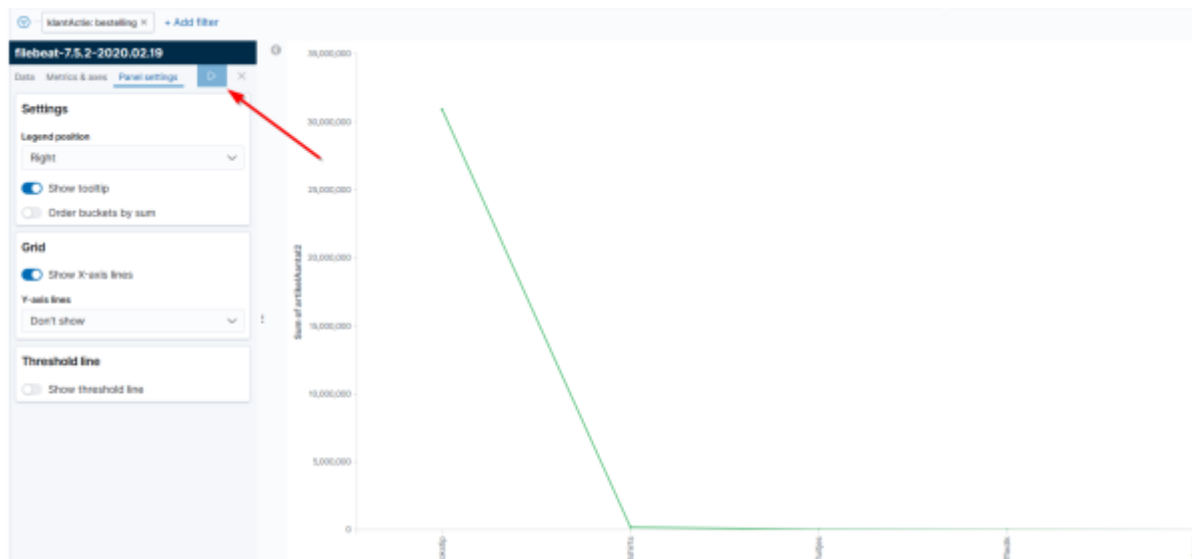
dit document beschrijft hoe je visualizations aanmaakt. Dit is een manier om je verzamelde data weer te geven.

## stappenplan

1. **menu > Visualize: Create Visualization**
2. kies een **type** (tabel, grafiek, ...)
3. kies een **Bron**: filebeat-\*
4. configureer nu je gekozen type visualisatie
5. bewaar de visualisatie

## algemene werking

1. je gaat uit van een meetbaar **aantal**. Standaard is dat het aantal events in ES, maar je kan ook elke telbare waarde uitkiezen (aantal verkochte producten, aantal alarmen, ...).  
Minimumvereisten is dat het gekozen veld als type **number** heeft. Logisch, rite?
2. kies **Buckets** om je weergave verder op te delen. Kies tussen opdeling in
  1. gelijke delen (**split slices**), meestal overzichtelijker
  2. nieuwe grafieken (**split chart**)
3. **Aggregation** geeft aan hoe je de data wilt groeperen:
  1. **Date Histogram/Date Range**: grafiek die evolutie over bepaalde tijd weergeeft
  2. **IPv4 Range**: op basis van IP range
  3. **Terms**: op basis van velden uit de ES event
4. het resultaat kan je meteen zien door op het blauw driehoekje te klikken



5. **Filters** laten je toe om de weergave van je resultaten verder te verfijnen (vb enkel bepaalde artikelen, ...)

## TIPS

- neem je tijd om met visualisaties te leren werken.  
Time well spent, gezien dit de bouwstenen zijn om je data op een visueel aantrekkelijke manier weer te geven!!!

## problemen, problemen

### Kibana geeft melding: Unknown field

- die fout krijg je als je een nieuw veld hebt toegevoegd in een Grok filter
- doe een refresh van de field list: **Management > Kibana > Index Patterns > filebeat-\***: **<refresh-icoontje>**

★ filebeat-\*

Time Filter field name: @timestamp

Default

This page lists every field in the **filebeat-\*** index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Elasticsearch [Mapping API](#)

Fields (1803)

Scripted fields (0)

Source filters (0)



## 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:visualizations](https://louslab.be/doku.php?id=elk_stack:visualizations)

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

