ELK

Crash course

ELK

- **E**lasticsearch
- **L**ogstash
- **K**ibana

Elasticsearch

- Dokumentdatabase
  - Erstatter ikke tradisjonelle databaser
- Søkeserver
- Bygger på Lucene
  - Lucene spørrespråk
- REST-grensesnitt
- SDK for alle platformer

Logstash

- Prosessering av data
  - CSV, XML, JSON
- Normalisering av data på ulike format
- Kan konfigureres til å lese “alle” logger

Kibana

- Søke
- Analysere og visualisere data
- Dashboard

Hvordan ser en index ut

- En index er samling med dokumenter
- For en index kan det defineres en eller flere typer
  - En type er definert for dokumenter som har felles egenskaper
  - Angir typene til egenskapene i et dokument (tekst, numerisk, dato, geo-lokasjon …)
- Et dokument er enheten som kan indexeres

Heldigvis fikser Elasticsearch dette veldig bra selv.

Installere

- Open source
- ZIP-installering
- Krever Java
- Docker images på Docker Hub

Vi tester Elasticsearch sitt REST-grensesnitt

1. Opprette index
2. POST data til index
3. GET data fra index
4. PUT data på index
5. Liste ut alle indexer i Elasticsearch
6. Søke
7. DELETE data i index

Vi bruker Logstash og indexerer log-fil

- Logstash konfigurasjon
  - Input
  - Filters
  - Output
- Kjøre Logstash
- Se på index

Vi indexerer tusenvis av adresser