DEVOPS

Labo: ELK

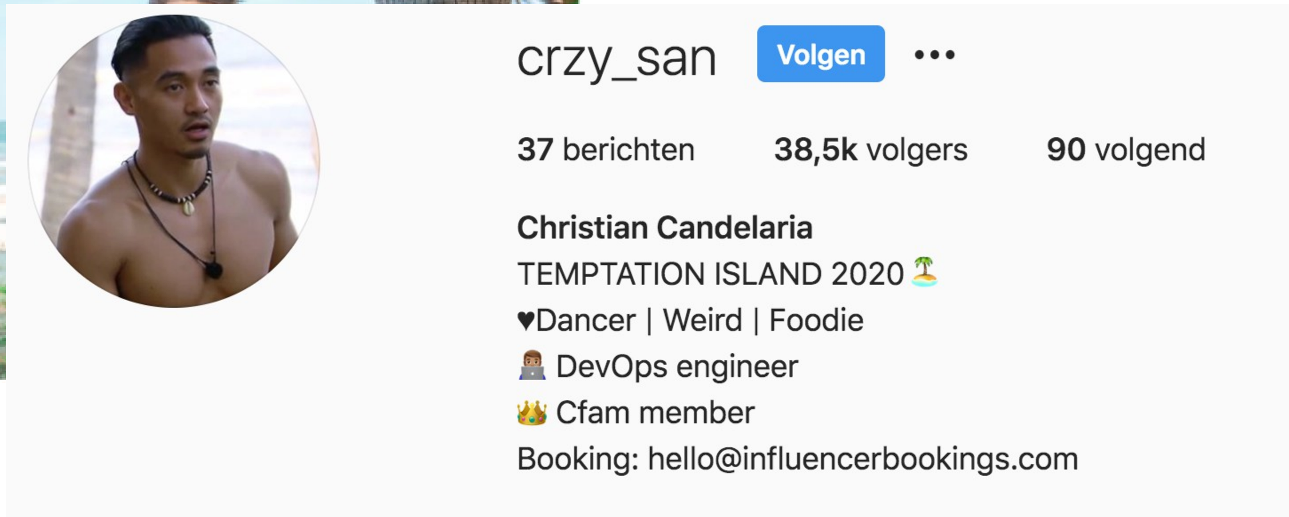
versie 0.1 – 20 april 2020

ARTESIS PLANTIJN
HOGESCHOOL ANTWERPEN

Housekeeping

- Dit is het laatste labo dat we een technologie in praktijk gaan brengen op zichzelf.
- Vanaf volgende week (en voor de volgende 4 labo's) gaan we aan jullie eindproject werken.
- In die 4 labo's gaan we jullie helpen om jullie eindproject waar je op geëvalueerd gaat worden af te werken.
- **DUS: denk voor welk, liefst eigen software-project jullie een CI/CD pipeline willen opzetten. Vanaf volgende week gaan we daar aan werken.**
- **Wie dit project tot een goed einde brengt kan mi overal beginnen als junior devops engineer.**

Weetje

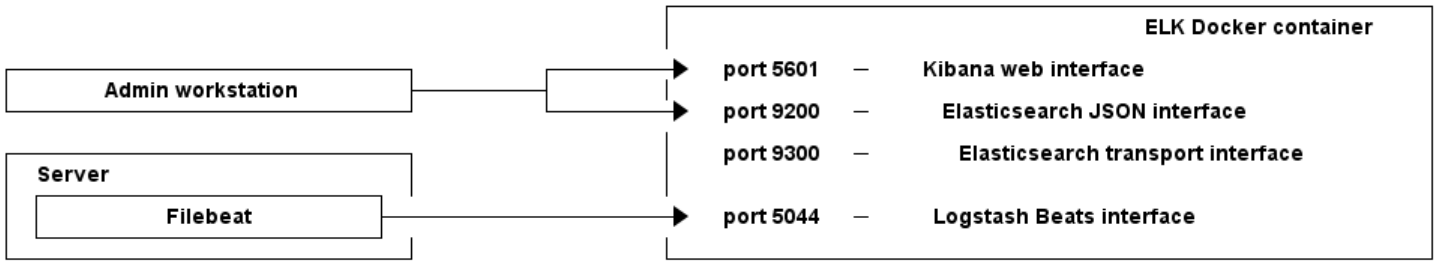

crzy_san
Volgen
37 berichten
38,5k volgers
90 volgend
Christian Candelaria
TEMPTATION ISLAND 2020 🏝
♥Dancer | Weird | Foodie
👨🏽‍💻 DevOps engineer
👑 Cfam member
Booking: hello@influencerbookings.com

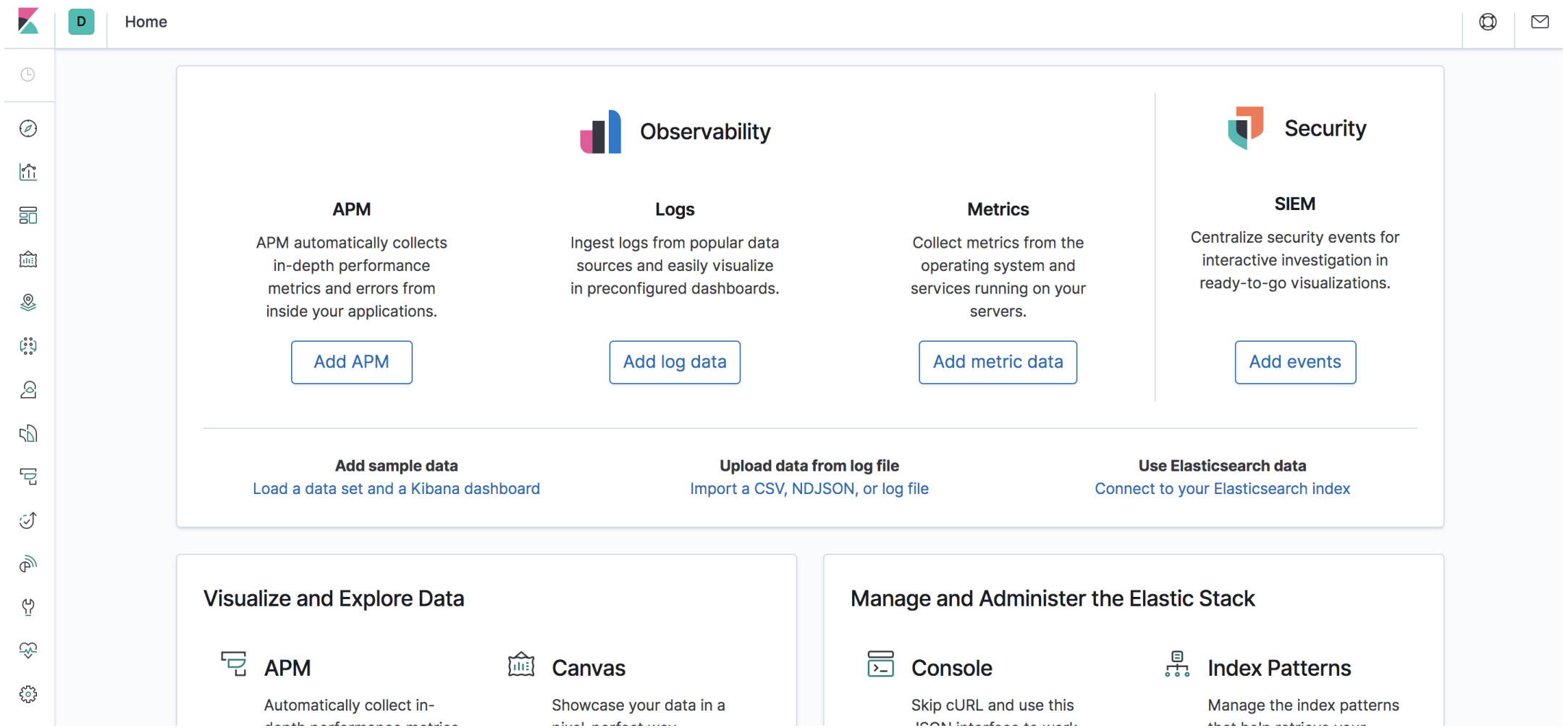
Stap 1: installeer een standalone ELK stack

- Op je Linux docker host, standalone.
- Gebruik `sebp/elk`
- Zie :
  - https://hub.docker.com/r/sebp/elk/
  - https://elk-docker.readthedocs.io/
  - https://www.elastic.co/guide/en/kibana/current/getting-started.html
- Denk aan :
  - We draaien een single node !
  - Persistant storage voorzien !
  - Geef het een goeie, makkelijke naam
- Debugging :
  - `docker exec -it bash` om te debuggen
  - `docker logs`
- If it works -> **http://<yourip>:5601**

KIBANA

- http://<yourip>:5601
- Wat draait er
- Wandel eens door de aangeboden dashboards en demo-data




D
Home
Observability
APM
APM automatically collects in-depth performance metrics and errors from inside your applications.
Add APM
Logs
Ingest logs from popular data sources and easily visualize in preconfigured dashboards.
Add log data
Metrics
Collect metrics from the operating system and services running on your servers.
Add metric data
Security
SIEM
Centralize security events for interactive investigation in ready-to-go visualizations.
Add events
Add sample data
Load a data set and a Kibana dashboard
Upload data from log file
Import a CSV, NDJSON, or log file
Use Elasticsearch data
Connect to your Elasticsearch index
Visualize and Explore Data
APM
Automatically collect in-
Canvas
Showcase your data in a
Manage and Administer the Elastic Stack
Console
Skip cURL and use this
Index Patterns
Manage the index patterns

Filebeat import

- Filebeat → software die de gegevens gaat filteren en doorpompen naar Elasticsearch.
- Installeer filebeat op je **linux** host en duw de standaard syslog bestanden door naar je elasticsearch
- Maak je eerste dashboard
- Doe nu hetzelfde voor je Mac of Windows hostmachine.
- https://www.elastic.co/guide/en/beats/filebeat/7.6/filebeat-getting-started.html

Opdracht vandaag

- Upload je beide screenshots van je dashboards naar Digitap.
- Zorg dat tegen volgende week je, liefst een eigen software-project of een project van GITHUB, hebt waar je een CI/CD tunnel gaat voor maken.