ELK Stack



context

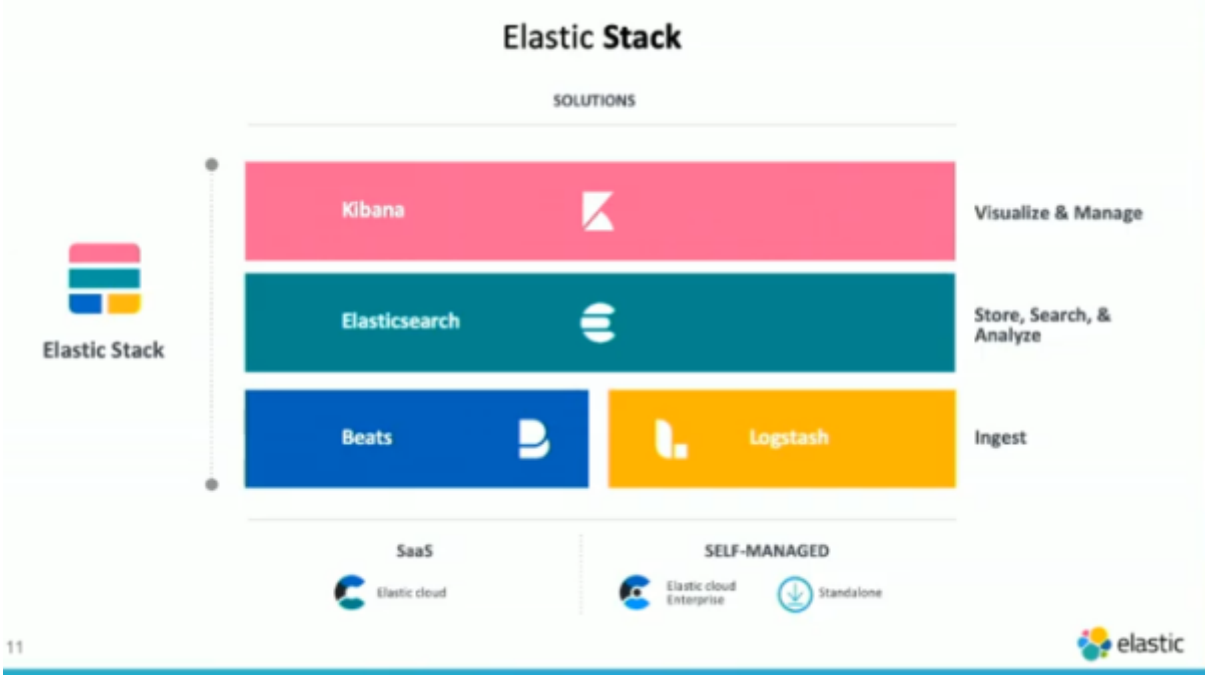
dit document beschrijft algemene werking van ELK Stack

Log analysis

1. keep logs in central place and analyse from there.
2. collection of raw (unstructured) data
3. convert into structured form
4. usefull for:
    1. issue debugging: detect problems
    2. predictive analysis: use log to foresee problems
    3. security analysis: analyse access logs
    4. performance analysis: how well is your app performing
5. problems with Log analysis:
    1. non-consistent log format: most apps have their own log format
    2. non-consistent time format: CET, US time format
    3. decentralised logs: logs are not on 1 server and are spread over your environment
    4. expert knowledge required: not everyone has access/knowledge to analyse the logs

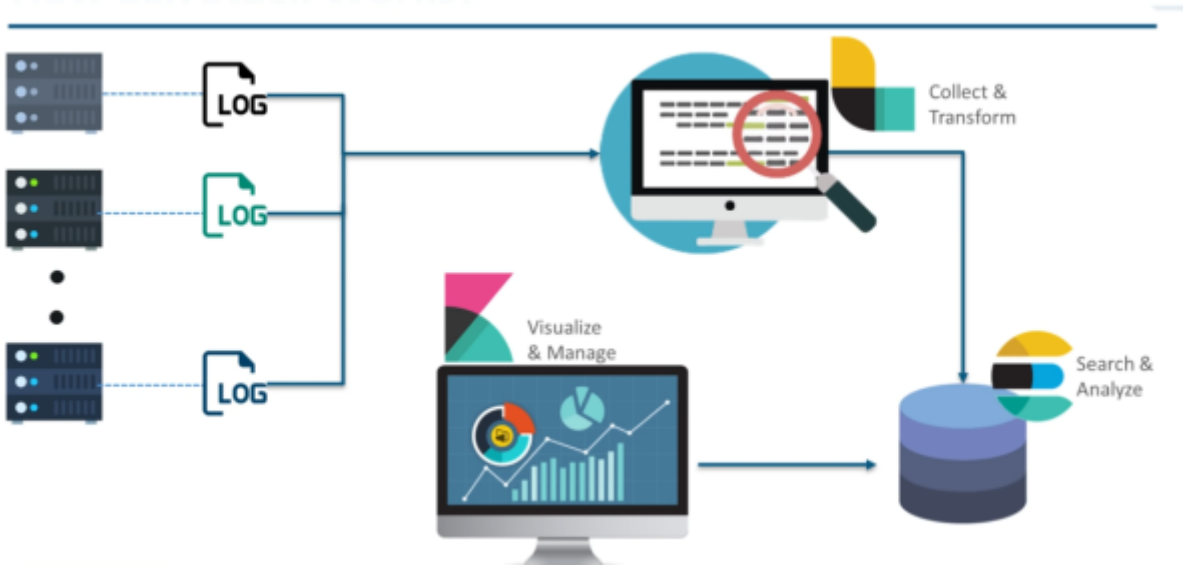
ELK Stack

- combination of 3 opensource tools:
    - elasticsearch: store logs and make them searcheable, NoSQL database, Apache Lucene, FAST (based on indexing)!
    - logstash: collect, parse and filter logs (unstructured data), plugins connect to various sources
    - kibana: web interface to display data in graphs and dashboards



How does it work?

1. logstash collects individual logs from servers
2. elasticserach works on collected data (indexing)
3. kebana presents data visually



meer info

uitleg gebaseerd op YouTube video

Linux

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

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

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