Logstash werking

context

dit document beschrijft de werking van Logstash, OpenSource data collection engine die raw logdate verwerkt en verder doorstuurd naar Elasticsearch

installatie

1. zie: Logstash: installatie

werking

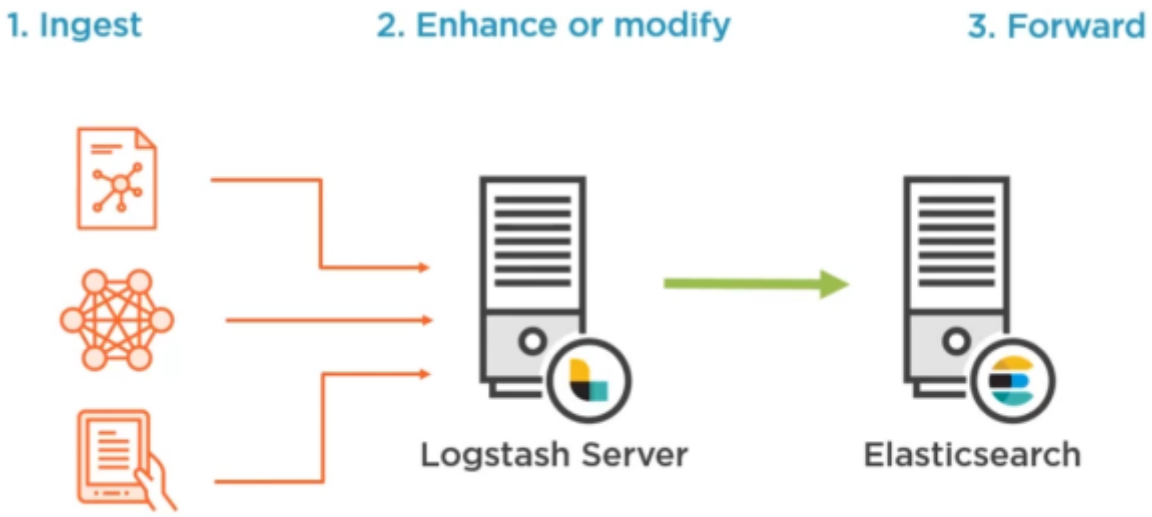
- dataverwerking gebeurt ahv een zgn **pipeline**:
  - input: tekstbestand, application log, Beats
  - filter: parse, change, ignore
  - output: waar wordt de data naartoe gestuurd.
- vaak wordt input voorzien door Filebeat
- daarnaast pelthora aan plugins
- meestgebruiker filters:
  - grok filter: parse unstructured into structured data
  - geopip filter: lookup van ip adressen, bv
- standaard wordt er ook naar /var/log/messages gestuurd. Om dit uit te schakelen:

beheer services

- ahv klassieke sudo systemctl commands
- process wordt gestart als gebruiker **logstash**

werking

:



meer info

voeg hier linken toe naar verdere uitleg

elk stack