

werking Filebeat

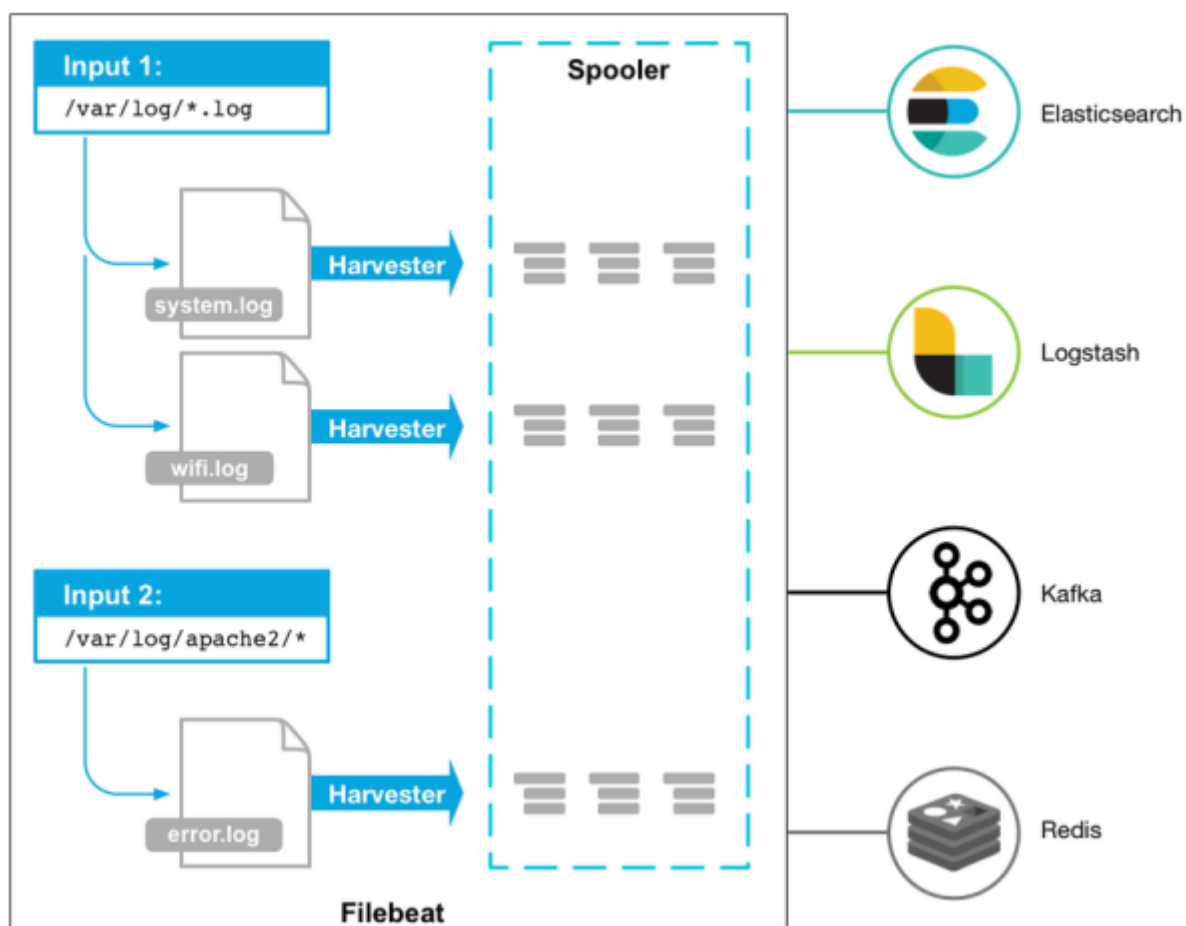


context

dit document beschrijft de werking van filebeat

algemeen

1. agent die logbestanden in de gaten houdt en naar ELK stack waar ze kunnen geïndexeerd worden. Ook wel: lightweight data shipper, genoemd.
 1. bij opstarten, worden 1 of meerdere inputs gestart die in de logdirs kijken
 2. voor elk logbestand (dat in config staat) wordt een **harvester** gestart zodra er nieuwe inhoud wordt aan toegevoegd.
 3. die data stuurt de filebeat door naar libbeat die ze aggregeert en doorstuurt naar output die voor Filebeat werd ingesteld.



2. de functionaliteit van filebeat wordt uitgebreid door **modules** die je kan activeren (zie: [Filebeat](#))

[installatie](#). Standaard activeer je de system module

3. de interval tussen controles staat standaard op 30 seconden.

werking testen

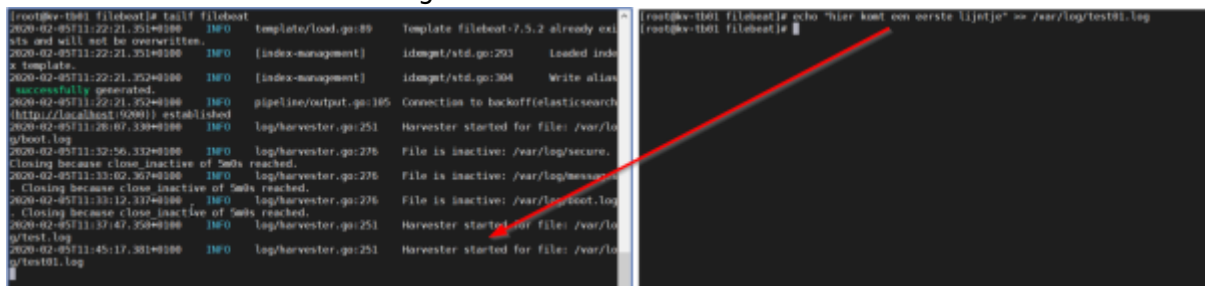
1. meld aan op de linux
2. open het logboek van filebeat:

```
tail -f /var/log/filebeat/filebeat.log
```

3. maak een nieuw logbestand aan:

```
echo "hier komt een eerste lijntje" > /var/log/test01.log
```

4. kijk na of nieuwe harvester wordt gestart:



5. kijk in kibana of het logbestand doorzoekbaar is:

1. **menu: Logs**
2. **zoekvenster:** log.file.path : "var/log/test01.log"

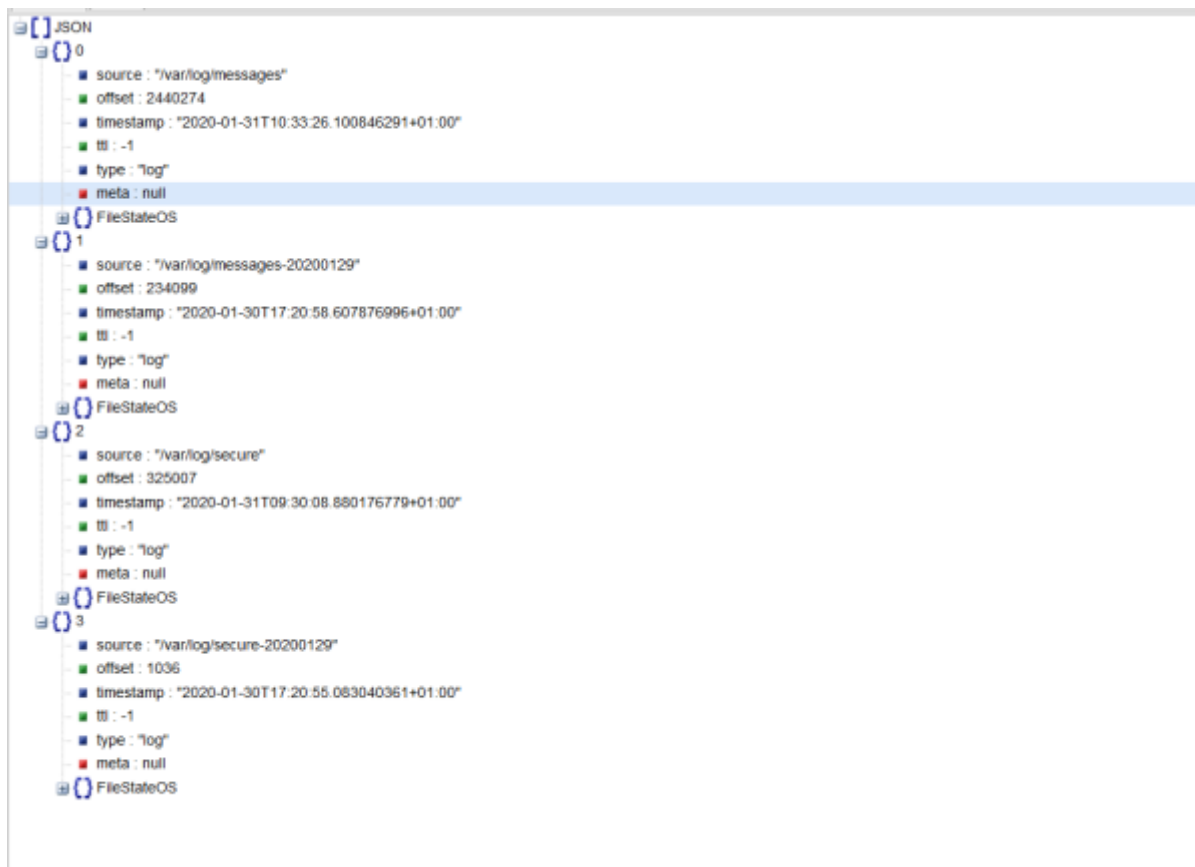


configuratie

- locatie: /etc/filebeat
- filebeat.yml: main config file
- als je [Filebeat modules](#) gebruikt, staat de config in /etc/filebeat/module.d
- [filebeat loglocatie toevoegen](#)
- [elk_stack:filebeat_logstash_configuratie](#)
- schakel [logging_naar_syslog_uit](#)
- activeer de **voorbeeld dashboards** op dezelfde manier als in [metricbeat](#) vervang metricbeat door filebeat

datadir

- /var/lib/filebeat
- bevat json bestand met logs die worden verwerkt:



logging

- dir: /var/log/filebeat/filebeat.log
- staat zo ingesteld dat bij elke herstart van de service, logbestand wordt geroteerd.

meer info

[Filebeat overview](#)

[elk stack, filebeat](#)

From:

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

Permanent link:

https://louslab.be/doku.php?id=elk_stack:werking_filebeat

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

