filebeat loglocatie toevoegen

context

dit document beschrijft hoe je een loglocatie toevoegt in filebeat.

algemeen

1. open /etc/filebeat/filebeat.yml
2. voeg toe:

```
  - type: log
  paths:
  - <pad/naar/logBestand>
```

3. herstart filebeat service:

```
sudo sytemctl restart filebeat
```

voorbeelden

- monitor alle *.log-bestanden in /var/log

```
- type: log
paths:
- /var/log/*.log
```

- monitor alle *.log-bestanden in /opt/trustbuilder/, inclusief subdirectories.

```
- type: log
paths:
- /opt/trustbuilder/**/*.log
```

- monitor alle bestanden in /opt/trustbuilder/tomcat-core/logs, uitgezonderd zip-bestanden.

```
- type: log
paths:
- /opt/trustbuilder/tomcat-core/logs/*
exclude_files: ['\.gz$']
```

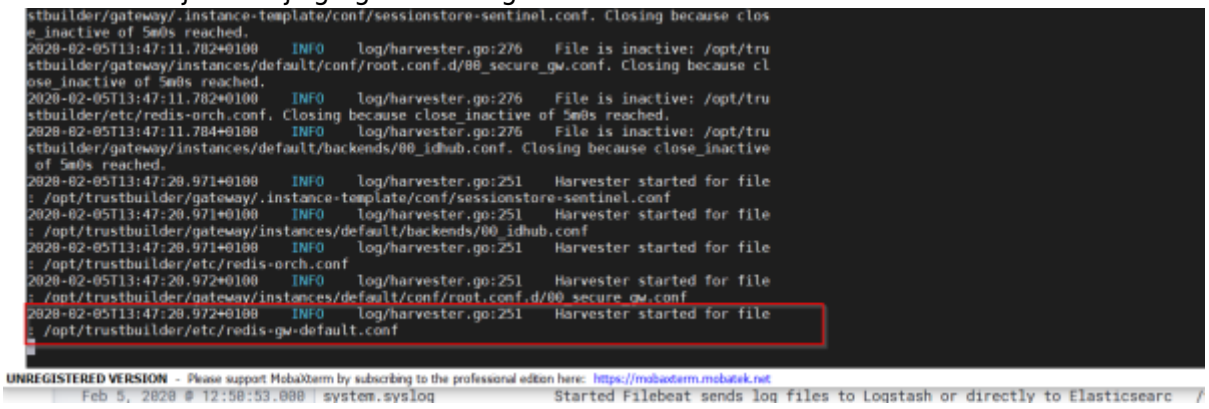
- monitor alle bestanden in /var/log/, uitgezonderd bestanden ouder dan 1 week__

```
- type: log
paths:
- /var/log/**/*
ignore_older: 1w
```

exclude_files: ['\.gz$']

testen

- open /var/log/filebeat/filebeat
- kijk of er een harvester wordt gestart
- kijk in Kibana of je de wijziging kunt terugvinden.



meer info

- Filebeat reference
- Filebeat example

elk stack, filebeat