

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.

```
stbuilder/gateway/.instance-template/conf/sessionstore-sentinel.conf. Closing because close
inactive of 5m0s reached.
2028-02-05T13:47:11.782+0100 INFO log/harvester.go:276 File is inactive: /opt/tru
stbuilder/gateway/instances/default/conf/root.conf.d/00_secure_gw.conf. Closing because cl
ose inactive of 5m0s reached.
2028-02-05T13:47:11.782+0100 INFO log/harvester.go:276 File is inactive: /opt/tru
stbuilder/etc/redis-orch.conf. Closing because close_inactive of 5m0s reached.
2028-02-05T13:47:11.784+0100 INFO log/harvester.go:276 File is inactive: /opt/tru
stbuilder/gateway/instances/default/backends/00_idhub.conf. Closing because close_inactive
of 5m0s reached.
2028-02-05T13:47:20.971+0100 INFO log/harvester.go:251 Harvester started for file
: /opt/trustbuilder/gateway/.instance-template/conf/sessionstore-sentinel.conf
2028-02-05T13:47:20.971+0100 INFO log/harvester.go:251 Harvester started for file
: /opt/trustbuilder/gateway/instances/default/backends/00_idhub.conf
2028-02-05T13:47:20.971+0100 INFO log/harvester.go:251 Harvester started for file
: /opt/trustbuilder/etc/redis-orch.conf
2028-02-05T13:47:20.972+0100 INFO log/harvester.go:251 Harvester started for file
: /opt/trustbuilder/gateway/instances/default/conf/root.conf.d/00_secure_gw.conf
2028-02-05T13:47:20.972+0100 INFO log/harvester.go:251 Harvester started for file
: /opt/trustbuilder/etc/redis-gw-default.conf
```

UNREGISTERED VERSION - Please support Mobaxterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>
Feb 5, 2028 @ 12:58:53.888 system.syslog Started Filebeat sends log files to Logstash or directly to Elasticsearch

meer info

- [Filebeat reference](#)
- [Filebeat example](#)

[elk stack](#), [filebeat](#)

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

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

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

