

filebeat Logstash configuratie



context

dit document beschrijft hoe je [filebeat](#) configureert om logs naar [Logstash](#) te sturen.

Logstash

1. bevat al ondersteuning om beats als input te gebruiken
2. /etc/logstash/logstash-sample.conf bevat een voorbeeldje:

```
# Sample Logstash configuration for creating a simple
# Beats -> Logstash -> Elasticsearch pipeline.

input {
  beats {
    port => 5044
  }
}

output {
  elasticsearch {
    hosts => ["http://localhost:9200"]
    index => "%{[@metadata][beat]}-%{[@metadata][version]}-
%{+YYYY.MM.dd}"
    #user => "elastic"
    #password => "changeme"
  }
}
```

Filebeat

1. open /etc/filebeat/filebeat.yml en voeg volgende key toe aan een filebeat.input:

```
output.logstash:
  hosts: ["localhost:5044"]
```

voorbeeld:

```
filebeat.inputs:
- type: log
  paths:
    - /var/log/voorbeeld.log
output.logstash:
  hosts: ["localhost:5044"]
```

/var/log/voorbeeld.log wordt linea recta naar logstash gestuurd.

testen

1. zet filebeat in debug modus:
 1. open /etc/filebeat/filebeat.yml
 2. ga naar de sectie **Logging**
 3. voeg toe: logging.level: debug
 4. herstart filebeat:

```
sudo systemctl restart filebeat
```

2. open het logboek van filebeat:

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

3. voeg een lijn tekst toe aan je logboek:

```
echo "Ha! Het zal wel werken >> /var/log/voorbeeld.log"
```

4. kijk na of:
 1. filebeat
 1. de wijziging oppikt in het bestand
 2. een event doorstuurt naar logstash
 2. het event beschikbaar is in kibana

meer info

voeg hier linken toe naar verdere uitleg

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

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

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

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

