Logstash: installatie

context

dit document beschrijft de installatie van Logstash

vereisten

1. Java: Java Runtime
2. voeg ELK stack repository toe
3. jq

installatie

1. installeer logstash:
    1. YUM:

        ```
        sudo yum install logstash
        ```

    2. APT:

        ```
        sudo apt-get install logstash
        ```

2. indien /tmp directory mount optie `noexec` heeft, voer onderstaande stappen uit:
    1. open /etc/logstash/jvm.options
    2. vervang
        1. `#-Djava.io.tmpdir=$HOME` door:
        2. `-Djava.io.tmpdir=/var/lib/logstash/tmp`
    3. maak de vermelde directory aan en stel toegangsrechten in:

        ```
        mkdir /var/lib/logstash/tmp && chown logstash:logstash
        /var/lib/logstash/tmp && chmod -R 2777 /var/lib/logstash/tmp
        ```

3. open /etc/logstash/log4j2.properties
    1. zet onderstaande lijnen in commentaar (#):

        ```
        rootLogger.appenderRef.console.ref = ${sys:ls.log.format}_console
        logger.slowlog.appenderRef.console_slowlog.ref =
        ${sys:ls.log.format}_console_slowlog
        ```

4. activeer logstash @bootup:

```
sudo systemctl enable logstash
```

5. start logstash:

```
sudo systemctl start logstash
```

6. open /var/log/logstash/logstash-plain.log:

```
[2020-02-10T10:06:04,612][INFO ][logstash.runner          ] Starting Logstash {"logstash.version"=>"7.5.2"}
[2020-02-10T10:06:05,862][INFO ][logstash.config.source.local.configpathloader] No config files found in path {:path=>"/etc/logstash/conf.d/*.conf"}
[2020-02-10T10:06:05,910][ERROR][logstash.config.sourceloader] No configuration found in the configured sources.
[2020-02-10T10:06:06,289][INFO ][logstash.agent           ] Successfully started Logstash API endpoint {:port=>9600}
[2020-02-10T10:06:11,214][INFO ][logstash.runner          ] Logstash shut down.
[2020-02-10T10:06:46,106][INFO ][logstash.runner          ] Starting Logstash {"logstash.version"=>"7.5.2"}
[2020-02-10T10:06:47,326][INFO ][logstash.config.source.local.configpathloader] No config files found in path {:path=>"/etc/logstash/conf.d/*.conf"}
[2020-02-10T10:06:47,397][ERROR][logstash.config.sourceloader] No configuration found in the configured sources.
[2020-02-10T10:06:47,823][INFO ][logstash.agent           ] Successfully started Logstash API endpoint {:port=>9600}
[2020-02-10T10:06:52,730][INFO ][logstash.runner          ] Logstash shut down.
```

Gezien er nog geen config bestand bestaat, wordt logstash endpoint gestart en daarna terug afgesloten. Dit is NIET de service zelf

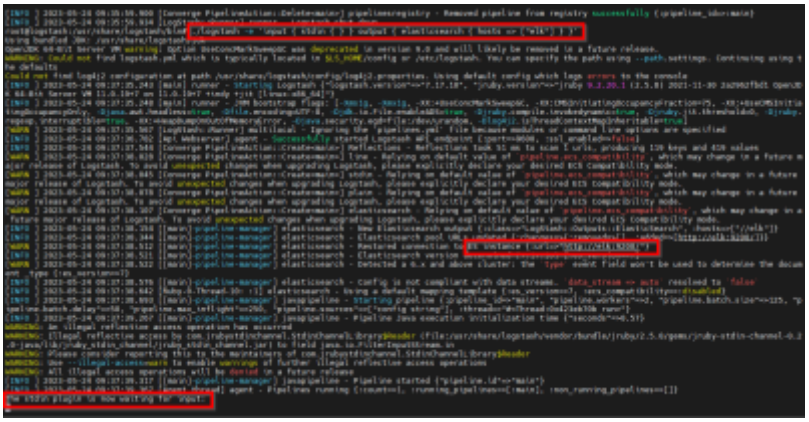
testen

- voer een eerste pipeline uit waarmee je een tekstboodschap naar output stuurt:

```
cd /usr/share/logstash/bin
sudo ./logstash -e 'input { stdin { } } output { stdout {} }'
<type een willekeurige tekst en sluit af met ctrl,D>
```

- je kan ook de data naar je elasticsearch sturen:

```
./logstash -e 'input { stdin { } } output { elasticsearch { hosts =>
["<IP/Hostname>"] } }'
```



- controleer het resultaat in elasticsearch: `curl http://elk:9200/logstash-*/_search`
- met jq kan je het JSON-bestand proper weergeven:`curl http://elk:9200/logstash-*/_search|jq .`

configuratie

Ga nu verder met de logstash_configuratie

meer info

voeg hier linken toe naar verdere uitleg

elk stack, logstash, installatie