Logstash op CentOS 7

Deze handleiding gaat er van uit dat Logstash op een server wordt waarop ook Elasticsearch is geïnstalleerd volgens deze handleiding.

Installatie

Maak de repo file voor yum aan:
`vi /etc/yum.repos.d/logstash.repo`

en zet hier in:

```
[logstash-2.3]
name=logstash repository for 2.3 packages
baseurl=http://packages.elasticsearch.org/logstash/2.3/centos
gpgcheck=1
gpgkey=http://packages.elasticsearch.org/GPG-KEY-elasticsearch
enabled=1
```

de key is al geïmporteerd bij het configureren van de elasticsearch repository.

en installeer door : `yum install logstash`

configuratie

De configuratie van logstash gebeurt per input output set met eventuele filters. Je kan meerdere `.conf` files aanmaken in `/etc/logstash/conf.d/`. De indeling is grofweg als volgt:

```
# This is a comment. You should use comments to describe
# parts of your configuration.
input {
  ...
}

filter {
  ...
}

output {
  ...
}
```

start Logstash

Nadat er minstens één configuratie file is gemaakt start je de applicatie nu en in de toekomst:

```
systemctl enable logstash
systemctl start logstash
```

Bronnen

https://www.digitalocean.com/community/tutorial_series/centralized-logging-with-logstash-and-kibana-on-centos-7

https://www.elastic.co/guide/en/logstash/current/configuration-file-structure.html

https://www.elastic.co/guide/en/logstash/current/config-examples.html