Kibana op CentOS 7

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

repository

Kibana is te vinden in een eigen repository.

Koppel deze aan de server door:
`vi /etc/yum.repos.d/kibana.repo`

en zet hier in:

```
[kibana-4.5]
name=Kibana repository for 4.5.x packages
baseurl=http://packages.elastic.co/kibana/4.5/centos
gpgcheck=1
gpgkey=http://packages.elastic.co/GPG-KEY-elasticsearch
enabled=1
```

De GPG key is dezelfde als de Elasticsearch key, dus die hoeft niet opnieuw te worden geïmporteerd.

Installeer Kibana

Installeer kibana uit de repository door:

`yum -y install kibana`

Configureer Kibana server

Open de configuratie file:

`vi /opt/kibana/config/kibana.yml`

en verander de `server.host` entry in:

```
server.host: "localhost"

logging.dest: /var/log/kibana.log
```

Ook willen we over SSL communiceren zodat we in de toekomst wellicht over het internet kunnen monitoren.
maak een signed certificaat/key pair aan voor kibana.

Plaats de verkregen server certificaat en CA certificaat in `/etc/pki/tls/certs/kibana/` en plaats de verkregen server key in `/etc/pki/tls/certs/kibana/private`

zet de permissies goed:

```
chmod 770 /etc/pki/tls/certs/kibana/private
chmod 600 /etc/pki/tls/certs/kibana/private/kibana.example.com.key
```

stel vervolgens kibana in om SSL te gebruiken: `vi /opt/kibana/config/kibana.yml`

en pas de volgende regels aan:

```
# SSL for outgoing requests from the Kibana Server to the browser (PEM
formatted)
server.ssl.cert: /etc/pki/tls/certs/kibana/kibana.example.com.crt
server.ssl.key: /etc/pki/tls/certs/kibana/private/kibana.example.com.key
```

Apache reverse proxy

Een httpd server is nodig om de kibana interface beveiligd te presenteren. Installeer apache volgens deze handleiding

zorg er voor dat het SSL gedeelte van apache met virtual hosts om kan gaan: `vi /etc/httpd/conf.d/ssl.conf`

en zorg dat daar in staat:

```
Listen 443 https
NameVirtualHost *:443
```

Maak een password aan voor de website:

```
htpasswd -c /etc/httpd/conf.d/kibana.htpasswd kibanaadmin
```

```
New password: Pa55w0Rd
Re-type new password: Pa55w0Rd
Adding password for user kibanaadmin
```

maak vervolgens de virtualhost configuratie voor kibana aan.

```
vi /etc/httpd/sites-available/kibana.conf
```

en stel hier de reverse proxy configuratie in:

```
<VirtualHost *:443>

        ServerName kibana.auriel.nl

        SSLEngine On
        BrowserMatch "MSIE [2-5]" \
```

```
            nokeepalive ssl-unclean-shutdown \
            downgrade-1.0 force-response-1.0

        SSLProxyEngine On
        SSLProxyVerify none
        SSLProxyCheckPeerCN off
        SSLProxyCheckPeerName off
        SSLProxyCheckPeerExpire off

        # proxy
        ProxyRequests Off
        ProxyPreserveHost On

        SSLCertificateFile /etc/pki/tls/certs/kibana/kibana.auriel.nl.crt
        SSLCertificateKeyFile
/etc/pki/tls/certs/kibana/private/kibana.auriel.nl.key
        SSLCACertificateFile /etc/pki/tls/certs/kibana/cacert.crt

        ProxyPass / https://localhost:5601/
        ProxyPassReverse / https://localhost:5601/
        <Proxy *>
                ## Auth
                AuthType Basic
                AuthName "Kibana"
                AuthUserFile /etc/httpd/conf.d/kibana.htpasswd
                Require valid-user
        </Proxy>
</VirtualHost>
```

En zorg dat de firewall open staat:

```
firewall-cmd --permanent --add-port=5601/tcp
firewall-cmd --reload
```

start kibana

en start de applicatie nu en in de toekomst:

```
systemctl enable kibana
systemctl start kibana
```

en test of de interface bereikbaar is langs: https://kibana.example.com

Configureer Kibana dashboard

Nadat er een systeem is geconfigureerd en geactiveerd is om data in Elasticsearch in te voeren (B.V. Fluentd of Logstash) kan de data in kibana worden gevisualiseerd. Verschillende visualisaties kunnen in dashboards worden geconfigureerd en opgeslagen. Dit is een verhaal appart.

Bronnen

https://www.elastic.co/guide/en/kibana/current/setup.html

http://totech.hateblo.jp/entry/2016/01/06/214218

http://www.techstricks.com/elasticsearch-fluentd-kibana-efk-setup-guide/

https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elk-stack-on-centos-7

http://blog.stevenmeyer.co.uk/2014/02/securing-kibana-and-elasticsearch-with-https-ssl.html

https://neverendingsecurity.wordpress.com/2015/04/13/open-source-log-visualization-with-elasticsearch-fluentd-and-kibana/

https://wiki.centos.org/SpecialInterestGroup/OpsTools

http://simonhanmer.co.uk/using-apache-to-authenticate-access-to-kibana-4/