Single Node Elasticsearch op Centos 7

Begin met een Clone van de CentOS7 minimal

repository

Elasticsearch is te vinden in een eigen repository. koppel deze aan de server door:

`vi /etc/yum.repos.d/elasticsearch.repo`

en zet hier in:

```
[elasticsearch-2.x]
name=Elasticsearch repository for 2.x packages
baseurl=http://packages.elastic.co/elasticsearch/2.x/centos
gpgcheck=1
gpgkey=http://packages.elastic.co/GPG-KEY-elasticsearch
enabled=1
```

haal de GPG key op en importeer deze in in rpm:

`rpm --import http://packages.elastic.co/GPG-KEY-elasticsearch`

java

Elasticsearch heeft java nodig. Het wordt aanbevolen om java van oracle te gebruiken, maar openJDK zou ook moeten werken.

Omdat ik liever zoveel mogelijk opensource en standaard repositories wil gebruiken (ook in verband met updates) heb ik besloten om openJDK te gebruiken.

Installeer openJDK door:

`yum install java`

(uit een andere handleiding `yum install java-1.8.0-openjdk-headless`)

Java Heap size

De default na een installatie van elasticsearch staat op een heap van 1 GB. In bijna alle gevallen is dat te weinig. Je zult dit moeten aanpassen.

de regels zijn als volgt:

1. Geef ongeveer de helft van het beschikbare geheugen aan elastic search, de rest is nodig voor

de lucene engine.
2. Geef minder dan 32 GB aan elasticsearch, Java gebruikt een truckje om het geheugen efficiënter met pointers te besturen. Als het geheugen voorbij een bepaalde grote komt werkt deze niet meer en zal de performance drastisch dalen.

bepaal de helft van het beschikbare geheugen: `free`

```
              total        used        free      shared  buff/cache
available
Mem:        8011180      443292     7363480        9328      204408
7362484
Swap:        839676           0      839676
```

dat is dus: 8011180/2=4005590, 4005590/1024 is ongeveer 3900 MB (naar beneden afronden)

Om deze environment variabele permanent op het systeem te setten doe je: `vi /etc/environment`

en voegt hier toe:

```
ES_HEAP_SIZE=3900m
```

Na een reboot is deze variabele op het systeem geset, je kan dit controleren door in te loggen en `echo $ES_HEAP_SIZE`

Om zonder reboot de variabele te setten zodat je door kan doe je `export ES_HEAP_SIZE=3900m`

swap

Swapping is de dood voor de performance van elastic search en lucene. Zet daarom swapping extreem laag.

`vi 90-override.conf`

en voeg toe:

```
#ABEL - zet swap bijna uit ivm performance van elasticsearch
vm.swappiness = 1
```

pas de nieuwe instelling toe:

`sysctl -p`

storage ruimte

Per default slaat Elasticsearch zijn data op in `/var/lib/elasticsearch`. daar moet een eigen filesysteem voor komen.

maak in de iscsi pool een volume aan.En mount dat op deze server

maak hieronder de dat en log directories aan:

```
mkdir -p /DATA/elasticsearch/data
mkdir -p /DATA/elasticsearch/logs
```

Elasticsearch installeren

installeer elasticsearch door:

```
yum install elasticsearch
```

en in de toekomst automatisch laten starten:

```
systemctl enable elasticsearch.service
```

Elasticsearch configureren

De Elasticsearch configuratie files bevinden zich in `/etc/elasticsearch`. Er zijn 2 files:

elasticsearch.yml — gaat over de Elasticsearch server settings.

logging.yml — Gaat over de settings van de logging.

De waarde `cluster.name` wordt door het auto-discovery mechanisme van Elasticsearch gebruikt om automatisch ontdekte elasticsearch nodes toe te voegen aan een het cluster. Als je deze op default laat staan bestaat de kans dat net default geïnstalleerde nodes onverwacht worden toegevoegd.

```
vi /etc/elasticsearch/elasticsearch.yml
```

en pas deze aan naar:

```
cluster.name: cluster-auriel
node.name: node-1

path.data: /DATA/elasticsearch/data
path.logs: /DATA/elasticsearch/logs

network.host: localhost
http.port: 9200
```

pas vervolens de owner aan van de data directories: `chown -R elasticsearch:elasticsearch /DATA/*`

Aangezien de http stack niet echt beveiligd is laten we elasticsearch alleen op localhost luisteren. Later komt er een Module voor die Elasticsearch voedt, denk aan logstash of fluentd, en een graphische module die de data queries weergeeft, denk aan kibana of grafana.

Elastic search starten en testen

start elasticsearch door: `systemctl start elasticsearch.service`

en kijk of de http interface werkt: `curl -X GET 'http://localhost:9200'`

de output lijkt op:

```
{
  "name" : "node-1",
  "cluster_name" : "cluster-auriel",
  "version" : {
    "number" : "2.3.5",
    "build_hash" : "90f439ff60a3c0f497f91663701e64ccd01edbb4",
    "build_timestamp" : "2016-07-27T10:36:52Z",
    "build_snapshot" : false,
    "lucene_version" : "5.5.0"
  },
  "tagline" : "You Know, for Search"
}
```

management interface optional Elasticsearch Management Plug-in

Er bestaat een aantal plugins voor elasticsearch die een graphische management interface voor Elasticsearch bieden.

installer er twee om flexibiliteit te hebben:

`/usr/share/elasticsearch/bin/plugin install lmenezes/elasticsearch-kopf/2.1.1`

vervolgens kan je de interface benaderen nadat je een reverse proxy hebt geinstalleerd door http://ipnummer:9200/_plugin/kopf

`/usr/share/elasticsearch/bin/plugin install mobz/elasticsearch-head`

vervolgens kan je de interface benaderen nadat je een reverse proxy hebt geinstalleerd door http://ipnummer:9200/_plugin/head/

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
```

Bronnen

https://www.digitalocean.com/community/tutorials/how-to-set-up-a-production-elasticsearch-cluster-on-centos-7

https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-elasticsearch-on-centos-7

https://www.elastic.co/guide/en/elasticsearch/guide/2.x/heap-sizing.html