How to install and configure Graylog

> Deze document is een instructie handleiding voor het installeren en configureren van een Graylog server. De Graylog server zal gebruikt worden voor het opslaan van de informatie die de Netflow metingen in het netwerk gedaan heeft. Deze documenten is op gesteld door Sedric Yaovi Lodonou op 8 december 2019.

requirements

- Linux distribution (Debian Linux, Ubuntu Linux, or CentOS recommended)
- Elasticsearch 5 or 6
- MongoDB 3.6 or 4.0
- Oracle Java SE 8(OpenJDK 8 is ook goed; Kies de laatste stabiele versie)

1.Intalleer een Linux Distribution

We zullen gebruik maken Oracle VM Virtualbox voor het installeren van onze vertuele PC's. Bij het aan maken van de vertuele pc is het belangerijk dat we meer dan 4GB RAM kiezen anders Zullen Elasticsearch en JAVA niet goed werken. De Debian ISO file kan op de officiele pagina van Debian gedownload worden.

Linux Updaten en extra packetten installeren

> $ sudo apt update && sudo apt upgrade
>
> $ sudo apt install apt-transport-https openjdk-8-jre-headless uuid-runtime pwgen dirmngr -y
>
> $ sudo apt update -y && sudo apt upgrade -y

2. Intall MongoDB op de Virtual pc

`$ sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv 9DA31620334BD75D9DCB49F368818C72E52529D4``

Als we een error krijgen over de "dirmngr" moet je eerste de dirmngr installeren met*apt-get install dirmngr -y*

```
$ echo "deb http://repo.mongodb.org/apt/debian stretch/mongodb-org/4.0 main" | sudo tee /etc/apt/sources.list.d/mongodb-org-4.0.list
```

Als je een error krijgt over sudo, haal je sudo weg bij de eerste PIPE

```
$ sudo apt-get update
```

En nu gaan we MongoDG installeren

```
$ sudo apt-get install -y mongodb-org
```

configureer MongoDB zodat hij bij de boot van de systeem automatish aan gaat.

> $ sudo systemctl daemon-reload

```
$ sudo systemctl enable mongod.service

$ sudo systemctl restart mongod.service
```

3. Intall Elasticsearch op de Virtual pc

```
$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

$ echo "deb https://artifacts.elastic.co/packages/oss-6.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-6.x.list

$ sudo apt update && sudo apt install elasticsearch-oss
```

Pas de Elasticsearch configuratie file aan

1. Install vim Editor

```
apt install vim -y
```

2. Pas de configuratie file aan

Open met vim de file in `/etc/elasticsearch/elasticsearch.yml`

```
$ vim /etc/elasticsearch/elasticsearch.yml
```

Verander de **cluster name** naar `graylog`, haal de regel uit commentaar door de "#" vor de regel te verwijderen. Nu voeg een regel toe met `action.auto_create_index: false`. De file zal er nu zo uit moeten zien.

```
cluster.name: graylog

action.auto_create_index: false
```

Herstart Elasticsearch

```
$ sudo systemctl daemon-reload

$ sudo systemctl enable elasticsearch.service

$ sudo systemctl restart elasticsearch.service
```

3. Intall Graylog configuraties repositories en graylog zelf

```
$ wget https://packages.graylog2.org/repo/packages/graylog-3.1-repository_latest.deb

$ sudo dpkg -i graylog-3.1-repository_latest.deb

$ sudo apt update && sudo apt install graylog-server
```

Pas de Graylog configuratie file aan

We moete een paar dingen aan passen in de `server.conf`. De `password_secret` en `root_password_sha2`

moeten geconfigureerd worden , dit is verplicht anders zal Graylog **niet** starten. Volg de volgende stampen om dit in orde te krijgen.

1. Maak een root_password_sha2

> echo -n "Enter Password: " && head -1 </dev/stdin | tr -d '\n' | sha256sum | cut -d" " -f1
>
> Enter Password:"jou root wachtwoord"

Jou wachtwoord word geincrypteerd met sha256. de Geincrypteerde code copieer je naar een notpad.

2. Ga naar de server.conf

> vim /etc/graylog/server/server.conf

3. Voeg password_secret toe

Maak een tweede comandline open. Genereer de password_secret met de volgende commando:

> pwgen -N 1 -s 96

kopieer de code die net gegenreerd is en voet het in de conf file als "password_secret"

4. Voeg root_password_sha2 toe

Plak de sha256 code die in stap `1. Maak een root_password_sha2` gemaakt is in de file op de juiste plaats.

5. verander de http_bind_address

om te kunnen connecteren met Graylog moet de `http_bind_address` gezet worden naar de**public host name** of public ip address van een machine waar je toegang op heb.

Herstart Graylog

> $ sudo systemctl daemon-reload
>
> $ sudo systemctl enable graylog-server.service
>
> $ sudo systemctl start graylog-server.service

check graylog status

> systemctl status graylog-server