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.Installeer een Linux Distribution

We zullen gebruik maken Hyper-V en netinst 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.

> **Hulp nodig bij het installeren van Debian Linux gelieven naar de document MakeVirtualMachine.pdf"**

Linux Updaten en extra packetten installeren

> root@graylogDebian:sudo apt update && sudo apt upgrade
>
> root@graylogDebian:sudo apt install apt-transport-https openjdk-8-jre-headless uuid-runtime pwgen dirmngr -y
>
> root@graylogDebian:sudo apt update -y && sudo apt upgrade -y

Error bij het installeren van de openjdk-8-jre-headless wordt opgelost in document Resolving Java installation error

```
root@graylogDebian:/home/debiangraylog# apt install apt-transport-https openjdk-8-jre-headless uuid-runtime pwgen dirmngr -
Pakketlijsten worden ingelezen... Klaar
Boom van vereisten wordt opgebouwd
De statusinformatie wordt gelezen... Klaar
Pakket openjdk-8-jre-headless is niet beschikbaar, hoewel er naar verwezen wordt door
een ander pakket. Mogelijk betekent dit dat het pakket ontbreekt,
verouderd is, of enkel beschikbaar is van een andere bron

E: Pakket 'openjdk-8-jre-headless' heeft geen kandidaat voor installatie
root@graylogDebian:/home/debiangraylog#
```

2. Install 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*

`root@graylogDebian: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

`root@graylogDebian:sudo apt-get update`

En nu gaan we MongoDG installeren

`root@graylogDebian:sudo apt-get install -y mongodb-org`

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

> root@graylogDebian:sudo systemctl daemon-reload
>
> root@graylogDebian:sudo systemctl enable mongod.service
>
> root@graylogDebian:sudo systemctl restart mongod.service

3. Install Elasticsearch op de Virtual pc

> root@graylogDebian:wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
>
> root@graylogDebian: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

> root@graylogDebian:sudo apt update && sudo apt install elasticsearch-oss

Pas de Elasticsearch configuratie file aan

1. Install vim Editor

> root@graylogDebian:apt install vim -y

2. Pas de configuratie file aan

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

> root@graylogDebian: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

```
#
cluster.name: graylog
action.auto_create_index:false
# ---------------------------------- Node ------------------------------------
#
# Use a descriptive name for the node:
#
#node.name: node-1
#
# Add custom attributes to the node:
#
#node.attr.rack: r1
```

Herstart Elasticsearch

> root@graylogDebian:sudo systemctl daemon-reload
>
> root@graylogDebian:sudo systemctl enable elasticsearch.service
>
> root@graylogDebian:sudo systemctl restart elasticsearch.service

3. Install Graylog configuraties repositories en graylog zelf

> root@graylogDebian:wget https://packages.graylog2.org/repo/packages/graylog-3.1-repository_latest.deb
>
> root@graylogDebian:sudo dpkg -i graylog-3.1-repository_latest.deb
>
> root@graylogDebian: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

> root@graylogDebian: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

> root@graylogDebian:vim /etc/graylog/server/server.conf

3. Voeg password_secret toe

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

> root@graylogDebian: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.

```
# You MUST set a secret to secure/pepper the stored user passwords here. Use at least 64 characters.
# Generate one by using for example: pwgen -N 1 -s 96
password_secret =AcmrEknZdeMTKm9UmjQP7EBf64agOeqKg938nlA4PxqEjIsQAvRZK66rOjpcEKKLLT92EBzZ7WMZEZhsQBhNncAayRfflXdz

# The default root user is named 'admin'
#root_username = admin

# You MUST specify a hash password for the root user (which you only need to initially set up the
# system and in case you lose connectivity to your authentication backend)
# This password cannot be changed using the API or via the web interface. If you need to change it,
# modify it in this file.
# Create one by using for example: echo -n yourpassword | shasum -a 256
# and put the resulting hash value into the following line
root_password_sha2 =796f8353d128b6341eae6680dd5d21bf68cbcf8277fa4a6043c13afd3ecf4099
```

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.

```
#
# This network interface must be accessible by all Graylog nodes in the cluster and by all clients
# using the Graylog web interface.
#
# If the port is omitted, Graylog will use port 9000 by default.
#
# Default: 127.0.0.1:9000
http_bind_address =10.20.120.9:9000
#http_bind_address = [2001:db8::1]:9000

#### HTTP publish URI
#
```

Herstart Graylog

> root@graylogDebian:sudo systemctl daemon-reload
>
> root@graylogDebian:sudo systemctl enable graylog-server.service
>
> root@graylogDebian:sudo systemctl start graylog-server.service

check graylog status

> root@graylogDebian:systemctl status graylog-server

```
root@graylogDebian:/etc# systemctl daemon-reload
root@graylogDebian:/etc#  systemctl enable graylog-server.service
Synchronizing state of graylog-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable graylog-server
root@graylogDebian:/etc# systemctl start graylog-server.service
root@graylogDebian:/etc# systemctl status graylog-server
● graylog-server.service - Graylog server
   Loaded: loaded (/lib/systemd/system/graylog-server.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2019-12-17 14:23:12 CET; 4s ago
     Docs: http://docs.graylog.org/
 Main PID: 2152 (graylog-server)
    Tasks: 15 (limit: 5705)
   Memory: 139.9M
   CGroup: /system.slice/graylog-server.service
           ├─2152 /bin/sh /usr/share/graylog-server/bin/graylog-server
           └─2166 /usr/bin/java -Xms1g -Xmx1g -XX:NewRatio=1 -server -XX:+ResizeTLAB -XX:+UseConcMarkSweepGC -XX:+CMSConc
```