Graylog

Requis

- Opensearch ou Elasticsearch
- MongoDB

Requis Container

Le container doit avoir 6Go de RAM pour être stable et assez d'espace disk pour contenir les logs.

Installation MongoDB

Pour installer MongoDB il faut installer les répertoires de dépots de MongoDB :
On installe GNUPG pour recevoir et installer la clé du dépôt de MongoDB :

```
  apt install gnupg
  wget -qO - https://www.mongodb.org/static/pgp/server-6.0.asc | sudo apt-
key add -
```

On indique le chemin du dépôt de MongoDB dans le répertoire source et on installe MongoDB.

```
  echo "deb http://repo.mongodb.org/apt/debian bullseye/mongodb-org/6.0
main" | sudo tee /etc/apt/sources.list.d/mongodb-org-6.0.list
  sudo apt-get update
  sudo apt-get install -y mongodb-org
```

Pour finir on fait à ce que MongoDB se lance au démarrage de la machine.

```
sudo systemctl daemon-reload
sudo systemctl enable mongod.service
sudo systemctl restart mongod.service
sudo systemctl --type=service --state=active | grep mongod
```

Installation Opensearch

Pour installer Opensearch il nous faut des paquets tiers.

```
  sudo apt-get update && sudo apt-get -y install lsb-release ca-certificates
```

```
curl gnupg2
```

Ils nous permettent de télécharger la clé GPG de Opensearch et pour vérifier la signature du répértoire APT.

```
  curl -o- https://artifacts.opensearch.org/publickeys/opensearch.pgp | sudo
gpg --dearmor --batch --yes -o /usr/share/keyrings/opensearch-keyring
```

On ajoute le chemin du dépôt de Opensearch dans le répertoire source de la machine.

```
  echo "deb [signed-by=/usr/share/keyrings/opensearch-keyring]
https://artifacts.opensearch.org/releases/bundle/opensearch/2.x/apt stable
main" | sudo tee /etc/apt/sources.list.d/opensearch-2.13.list
```

On installe Opensearch :

```
  wget --no-check-certificate
https://artifacts.opensearch.org/releases/bundle/opensearch/2.13.0/opensearc
h-2.13.0-linux-x64.deb
  apt install ./opensearch-2.13.0-linux-x64.deb #On le change dans un
répertoire non restreint par des droits particuliers
```

Configurer Opensearch

On vas configurer Opensearch pour Graylog :

```
  nano /etc/opensearch/opensearch.yml
```

Il faut changer les valeurs pour les remplacés par ci-dessous.

```

cluster.name: graylog
node.name: ${HOSTNAME}
path.data: /var/lib/opensearch
path.logs: /var/log/opensearch
discovery.type: single-node
network.host: 0.0.0.0
action.auto_create_index: false
plugins.security.disabled: true
indices.query.bool.max_clause_count: 32768
```

Maintenant on vas modifier la JVM (Java Virtual Machine).

```
sudo nano /etc/opensearch/jvm.options
```

Les options Xms et Xmx doivent être mis à la moitié de la RAM de la machine.

```
## JVM configuration
################################################################
## IMPORTANT: JVM heap size
################################################################
##
## You should always set the min and max JVM heap
## size to the same value. For example, to set
## the heap to 4 GB, set:
##
## -Xms4g
## -Xmx4g
##
## See https://opensearch.org/docs/opensearch/install/important-settings/
## for more information
##
################################################################
# Xms represents the initial size of total heap space
# Xmx represents the maximum size of total heap space
-Xms3g
-Xmx3g
```

Maintenant on modifie les paramètres de kernel :

```
sudo sysctl -w vm.max_map_count=262144
sudo echo 'vm.max_map_count=262144' >> /etc/sysctl.conf
```

Puis on active le service :

```
sudo systemctl daemon-reload
sudo systemctl enable opensearch.service
sudo systemctl start opensearch.service
```

Installation de Graylog

Pour installer Graylog open nous allons télécharger le package :

```
wget
```

```
https://packages.graylog2.org/repo/packages/graylog-5.0-repository_latest.de
b
  sudo dpkg -i graylog-5.0-repository_latest.deb
  sudo apt-get update && sudo apt-get install graylog-server
```

Maintenant nous allons mettre les mots de passe dans le fichier de conf de Graylog. Il faut modifier les valeurs de “password_secret” et “root_password_sha2”. Il y a des règles à suivre pour “password_secret”, plus de 16 caractères contenant majuscule, minuscule et chiffre.
Pour “root_password_sha2” il faut le générer via une commande :

```
  echo -n "MOT DE PASSE ICI" && head -1 </dev/stdin | tr -d '\n' | sha256sum
| cut -d" " -f1
```

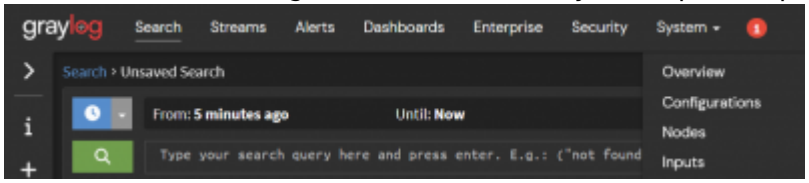
Pour finir avec la configuration modifier le “http_bind_address”. A l'adresse IP de la machine (10.31.192.115:9000 Dans notre cas).

Enrôler des machines

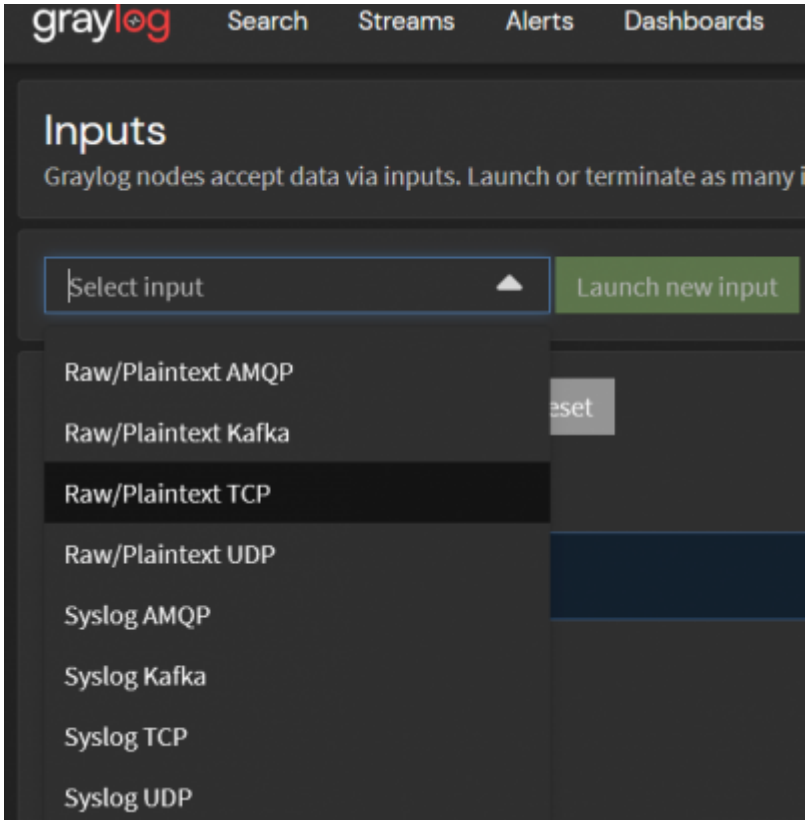
Linux

Coté serveur

Dans Graylog on vas crée un “input” qui vas nous permettre de recevoir les logs.
Dans la barre de navigation on vas dans “system” puis “input”.



Après on choisit “syslog UDP” dans “Select Input” et “Launch new input”.



Coté Machine

Pour Debian nous allons utiliser l'outil rsyslog, qui va nous permettre à l'aide du module "imfile" de transformer le texte des logs en message syslog que rsyslog pourra envoyer au serveur Graylog.
On active un syslog UDP :
Comme rsyslog n'est plus installer de base sur les versions les plus récentes de Debian on vérifie :

```
sudo apt install rsyslog
```

On modifie le fichier de conf syslog :

```
/etc/syslog.conf
```

```
$ModLoad imudp
$UDPServerRun 514
*.* @IP de graylog:514;RSYSLOG_SyslogProtocol23Format
```

Puis on crée un fichier de conf pour récupérer les lignes des fichiers de logs, exemple pour récupérer les fichiers de logs d'apache :

```
/etc/rsyslog.d/apache2.conf
```

```
module(load="imfile" PollingInterval="10"
```

```
statefile.directory="/var/spool/rsyslog")
    input(type="imfile"
         File="/var/log/apache2/access.log"
         Tag="apache2_http_access"
      Severity="info"
      Facility="local6")
input(type="imfile"
      File="/var/log/apache2/error.log"
      Tag="apache2_http_error"
      Severity="info"
      Facility="local6")
local6.access        @192.168.122.40:1514
```

Explication :

module(load=“imfile” PollingInterval=“10” statefile.directory=“/var/spool/rsyslog”)
input(type=“imfile”

```
  File="/var/log/apache2/access.log" #Position du fichier de log
  Tag="apache2_http_access" #“application_name” dans Graylog permet de
différencier
    Severity="info"
    Facility="local6")
```

Pour finir :

```
  systemctl restart rsyslog
```