Projet E5

ITWay

"ITWay : Sécuriser, Innover, Simplifier votre IT"

Installation du Server GrayLog

Commençons par une mise à jour du cache des paquets et l'installation d'outils nécessaires pour la suite des événements.

```
sudo apt-get update
sudo apt-get install curl lsb-release ca-certificates gnupg2 pwgen
```

A. Installation de MongoDB

Une fois que c'est fait, nous allons commencer l'installation de MongoDB. Téléchargez la clé GPG correspondante au dépôt MongoDB :

```
curl -fsSL https://www.mongodb.org/static/pgp/server-6.0.asc | sudo gpg -o
/usr/share/keyrings/mongodb-server-6.0.gpg --dearmor
```

Puis, ajoutez le dépôt de MongoDB 6 sur la machine Debian 12 :

```
echo "deb [ signed-by=/usr/share/keyrings/mongodb-server-6.0.gpg]
http://repo.mongodb.org/apt/debian bullseye/mongodb-org/6.0 main" | sudo tee
/etc/apt/sources.list.d/mongodb-org-6.0.list
```

Ensuite, nous allons mettre à jour le cache des paquets et tenter d'installer MongoDB :

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

L'installation de MongoDB ne peut pas être effectuée, car il manque une dépendance : libssl1.1. Nous allons devoir installer ce paquet manuellement avant de pouvoir poursuivre parce que Debian 12 ne l'a pas dans ses dépôts.

```
Les paquets suivants contiennent des dépendances non satisfaites :
 mongodb-org-mongos : Dépend: libssl1.1 (>= 1.1.1) mais il n'est pas
installable
 mongodb-org-server : Dépend: libssl1.1 (>= 1.1.1) mais il n'est pas
installable
E: Impossible de corriger les problèmes, des paquets défectueux sont en mode
« garder en l'état ».
```

Nous allons télécharger le paquet DEB nommé "libssl1.1_1.1.1f-1ubuntu2.23_amd64.deb" (version la plus récente) avec la commande wget, puis procéder à son installation via la commande dpkg. Ce qui donne les deux commandes suivantes :

```
wget
http://archive.ubuntu.com/ubuntu/pool/main/o/openssl/libssl1.1_1.1.1f
-1ubuntu2.23_amd64.deb
sudo dpkg -i libssl1.1_1.1.1f-1ubuntu2.23_amd64.deb
```

Relancez l'installation de MongoDB :

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

Ensuite, relancez le service MongoDB et activez son démarrage automatique au lancement du serveur Debian.

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

MongoDB est installé, nous pouvons passer à l'installation du prochain composant.

B. Installation d'OpenSearch

Nous allons passer à l'installation d'OpenSearch sur le serveur. La commande suivante permet d'ajouter la clé de signature pour les paquets OpenSearch :

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

Puis, ajoutez le dépôt OpenSearch pour que nous puissions télécharger le paquet avec apt par la suite :

```
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.x.list
```

Mettez à jour votre cache de paquets :

```
sudo apt-get update
```

Puis, installez OpenSearch en prenant soin de définir le mot de passe par défaut pour le compte Admin de votre instance. Ici, le mot de passe est "admin", mais remplacez cette valeur par un mot de passe robuste. Évitez les mots de passe faibles, sinon il y aura une erreur à la fin de l'installation. C'est un prérequis depuis OpenSearch 2.12.

```
sudo env OPENSEARCH_INITIAL_ADMIN_PASSWORD=IT-Connect2024! apt-get install
opensearch
```

Patientez pendant l'installation... Quand c'est terminé, prenez le temps d'effectuer la configuration minimale. Ouvrez le fichier de configuration au format YAML :

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

Lorsque le fichier est ouvert, configurez les options suivantes :

```
cluster.name: graylog
node.name: ${HOSTNAME}
path.data: /var/lib/opensearch
path.logs: /var/log/opensearch
discovery.type: single-node
network.host: 127.0.0.1
action.auto_create_index: false
plugins.security.disabled: true
```

Enregistrez et fermez ce fichier.

C. Configurer Java (JVM)

Vous devez configurer Java Virtual Machine utilisé par OpenSearch afin d'ajuster la quantité de mémoire que peut utiliser ce service. Éditez le fichier de configuration suivant :

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

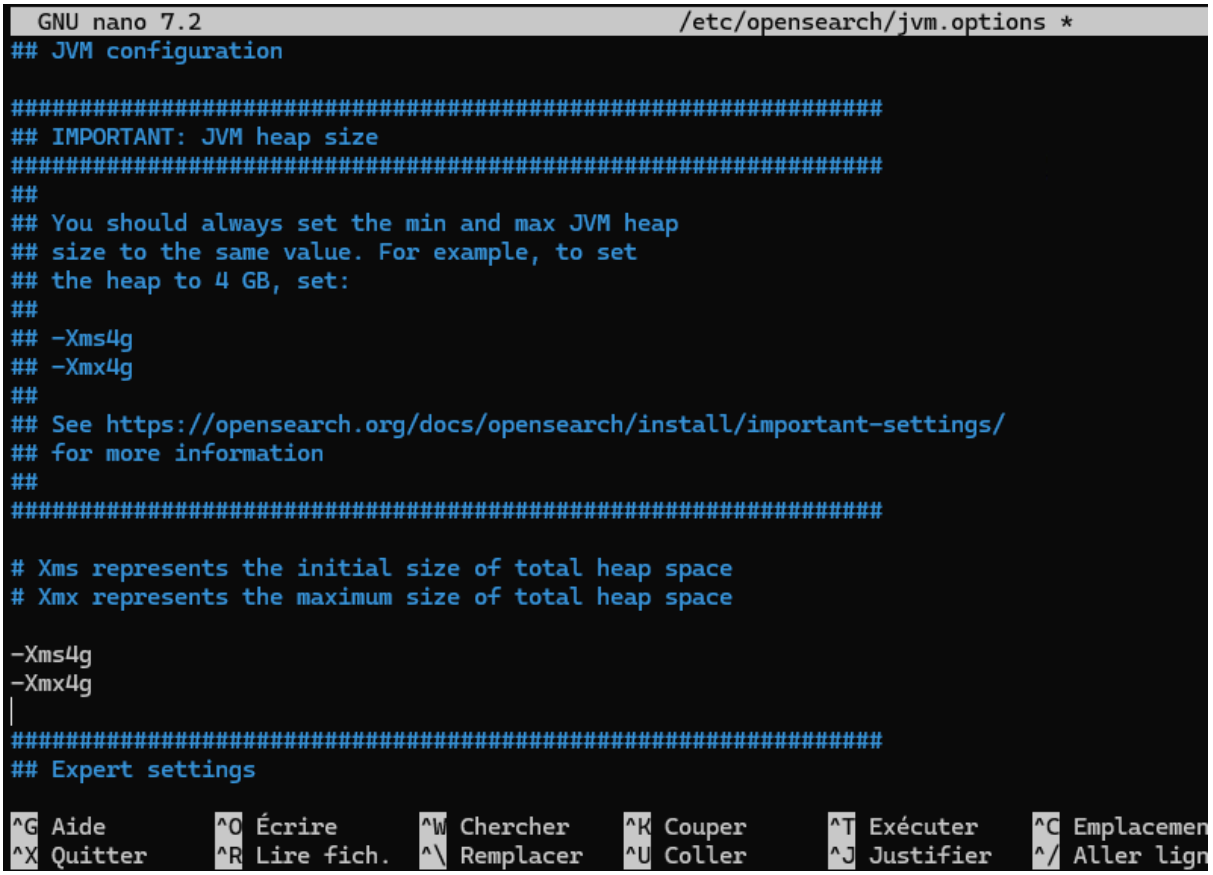
Avec la configuration déployée ici, OpenSearch démarrera avec une mémoire allouée de 4 Go et pourra atteindre jusqu'à 4 Go, il n'y aura donc pas de variation de mémoire pendant le fonctionnement. Ici, la configuration tient compte du fait que la machine virtuelle dispose d'un total de 8 Go de RAM. Les deux paramètres doivent avoir la même valeur. Ceci implique de remplacer ces lignes :

```
-Xms1g
-Xmx1g
```

Par ces lignes :

```
-Xms4g
-Xmx4g
```

Voici la modification à apporter en image :



Fermez ce fichier après l'avoir enregistré.

En complément, nous devons vérifier la configuration du paramètre "max_map_count" au niveau du noyau Linux. Il définit la limite des zones de mémoire mappées par processus, afin de répondre aux besoins de notre application. OpenSearch, au même titre que Elasticsearch, recommande de fixer cette valeur à "262144" pour éviter des erreurs liées à la gestion de la mémoire.

En principe, sur une machine Debian 12 fraîchement installée, la valeur est déjà correcte. Mais, nous allons le vérifier. Exécutez cette commande :

```
cat /proc/sys/vm/max_map_count
```

Si vous obtenez une valeur différente de "262144", exécutez la commande suivante, sinon ce n'est pas nécessaire.

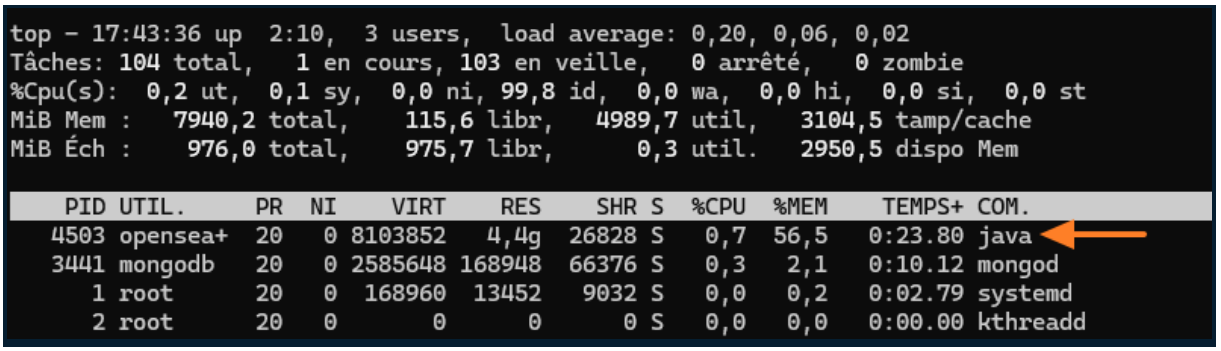
```
sudo sysctl -w vm.max_map_count=262144
```

Enfin, activez le démarrage automatique d'OpenSearch et lancez le service associé.

```
sudo systemctl daemon-reload
sudo systemctl enable opensearch
sudo systemctl restart opensearch
```

Si vous affichez l'état de votre système, vous devriez voir un processus Java avec 4 Go de RAM.

```
top
```



D. Installation de Graylog

Pour effectuer l'installation de Graylog 6.1 dans sa dernière version, exécutez les 4 commandes suivantes afin de télécharger et d'installer Graylog Server :

```
wget
https://packages.graylog2.org/repo/packages/graylog-6.1-repository_latest.deb
sudo dpkg -i graylog-6.1-repository_latest.deb
sudo apt-get update
sudo apt-get install graylog-server
```

Quand c'est fait, nous devons apporter des modifications à la configuration de Graylog avant de chercher à le lancer.

Commençons par configurer ces deux options :

- password_secret : ce paramètre sert à définir une clé utilisée par Graylog pour sécuriser le stockage des mots de passe utilisateurs (dans l'esprit d'une clé de salage). Cette clé doit être unique et aléatoire.

root_password_sha2 : ce paramètre correspond au mot de passe de l'administrateur par défaut dans Graylog. Il est stocké sous forme d'un hash SHA-256.

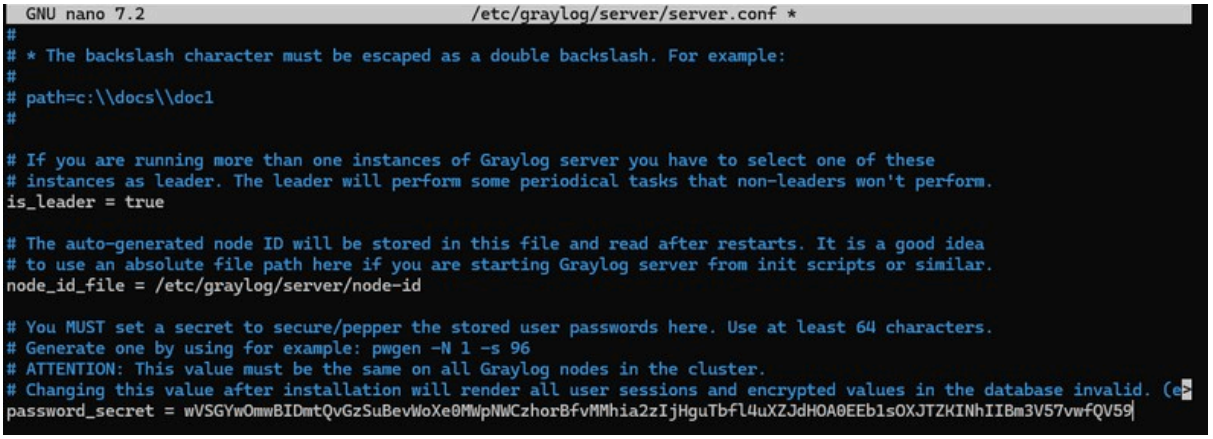
Nous allons commencer par générer une clé de 96 caractères pour le paramètre password_secret :

```
pwgen -N 1 -s 96
wVSGYwOmwBIDmtQvGzSuBevWoXe0MWpNWCzhorBfvMMhia2zIjHguTbfl4uXZJdHOA0EEb1sOXJT
ZKINhIIBm3V57vwfQV59
```

Copiez la valeur retournée, puis ouvrez le fichier de configuration de Graylog :

```
sudo nano /etc/graylog/server/server.conf
```

Collez la clé au niveau du paramètre password_secret, comme ceci :



Enregistrez et fermez le fichier.

Ensuite, vous devez définir le mot de passe du compte "admin" créé par défaut. Dans le fichier de configuration, c'est le hash du mot de passe qui doit être stocké, ce qui implique de le calculer. L'exemple ci-dessous permet d'obtenir le hash du mot de passe "admin" : adaptez la valeur avec votre mot de passe.

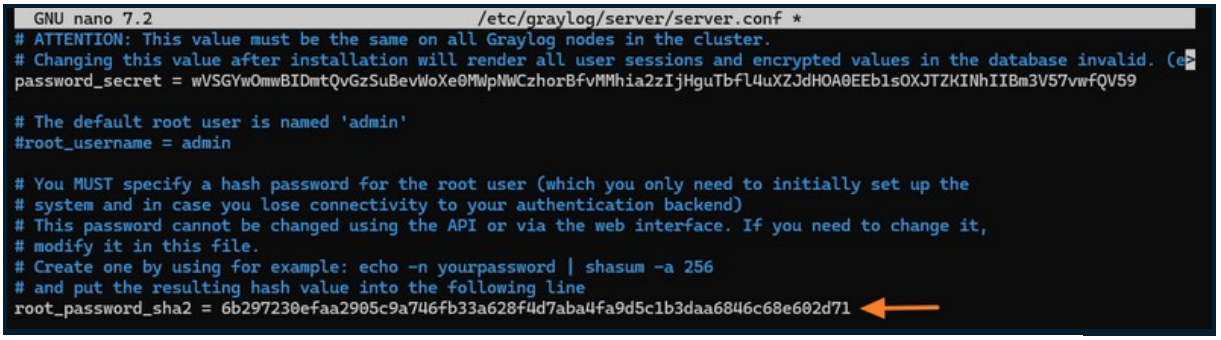
```
echo -n "admin" | shasum -a 256
6b297230efaa2905c9a746fb33a628f4d7aba4fa9d5c1b3daa6846c68e602d71
```

Copiez la valeur obtenue en sortie (sans le tiret en bout de ligne).

Ouvrez de nouveau le fichier de configuration de Graylog :

```
sudo nano /etc/graylog/server/server.conf
```

Collez la valeur au niveau de l'option root_password_sha2 comme ceci :



Profitez d'être dans le fichier de configuration pour configurer l'option nommée "http_bind_address". Indiquez "0.0.0.0:9000" pour que l'interface web de Graylog soit accessible sur le port 9000, via n'importe quelle adresse IP du serveur.

Puis, configurez l'option "elasticsearch_hosts" avec la valeur "http://127.0.0.1:9200" pour déclarer notre instance locale OpenSearch. Ceci est nécessaire, car nous n'utilisons pas de Graylog Data Node. Et sans cette option, il ne sera pas possible d'aller plus loin

Enregistrez et fermez le fichier.

Cette commande active Graylog pour qu'il démarre automatiquement au prochain démarrage et elle lance immédiatement le serveur Graylog.

```
sudo systemctl enable --now graylog-server
```

Une fois que c'est fait, tentez une connexion à Graylog à partir d'un navigateur. Indiquez l'adresse IP du serveur (ou son nom) et le port 9000.