Gabriel LIÉBAUT

Guide d'installation de Elasticsearch, MongoDB et Graylog

INFORMATION SUR L'INSTALLATION :
Elasticsearch 7.10.2 est la **SEULE** version compatible avec Graylog 5.2.
Ne jamais installer Elasticsearch 7.11, cela casserait définitivement votre instance Graylog.

Composant	Version a utiliser
Elasticsearch	`7.10.2`
MongoDB	`6.0.x`
Graylog	`5.2.x`

Information hardware de la VM

Composant	Valeur recommandée
OS	Debian 12
CPU	4 CPU minimum
RAM	16 Go recommandé
Disque	50 Go SSD minimum

Préparation du système

Mettez à jour le système et installez les dépendances nécessaires :

```
sudo apt update && sudo apt upgrade -y
sudo apt install -y curl wget gnupg apt-transport-https
sudo apt install -y uuid-runtime pwgen dirmngr
```

Configuration du paramètre « vm.max_map_count » (essentiel pour l'installation de Elasticsearch) :

```
sudo sysctl -w vm.max_map_count=262144
echo 'vm.max_map_count=262144' | sudo tee -a /etc/sysctl.conf
sudo sysctl -p
```

Installation d'Elasticsearch 7.10.2

Pour installer Elasticsearch, nous allons importer la clé GPG, ajouter le dépôt officiel, puis lancer l'installation de la version 7.10.2.

Un dépôt est un serveur qui contient un ou plusieurs paquets nécessaires à l'installation du logiciel.

Ajouter la clé GPG de Elasticsearch :

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o/usr/share/keyrings/elasticsearch-keyring.gpg
```

Ajouter le dépôt Elasticsearch 7.x :

```
echo 'deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/
packages/7.x/apt stable main' | sudo tee /etc/apt/sources.list.d/elastic-7.x.list
```

Mettre à jour :

```
sudo apt update
```

Installation de la version 7.10.2 de Elasticsearch :

```
sudo apt install -y elasticsearch=7.10.2
```

Bloquer les mises à jour automatiques afin de ne pas basculer sur une version supérieure :

```
sudo apt-mark hold elasticsearch
```

La commande apt-mark hold empêche la mise à jour accidentelle vers une version incompatible.

Configuration d'Elasticsearch

Aller dans le fichier /etc/elasticsearch/elasticsearch.yml :

```
sudo nano /etc/elasticsearch/elasticsearch.yml
```

Mettre à jour ou ajouter les informations suivantes :

```
cluster.name: graylog
node.name: node-1
path.data: /var/lib/elasticsearch
path.logs: /var/log/elasticsearch
network.host: 127.0.0.1
http.port: 9200
discovery.type: single-node
action.auto_create_index: false
xpack.security.enabled: false
xpack.security.transport.ssl.enabled: false
```

Configurer la taille du segment de mémoire (heap) pour Elasticsearch :

```
sudo nano /etc/elasticsearch/jvm.options.d/heap.options
```

Mettre à jour le contenu :

```
-Xms2g
-Xmx2g
```

Activez et démarrez le service Elasticsearch :

```
sudo systemctl daemon-reload
sudo systemctl enable elasticsearch
sudo systemctl start elasticsearch
sudo systemctl status elasticsearch
```

Installation de MongoDB 6.x

Importation de la clé publique MongoDB :

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

Ajouter le dépôt de MongoDB 6.0 :

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

Mettre à jour :

```
sudo apt update
```

Installation de MongoDB :

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

Aller dans le fichier /etc/mongod.conf pour limiter la mémoire de MongoDB :

```
sudo nano /etc/mongod.conf
```

Mettre à jour le contenu :

```
storage:
  wiredTiger:
    engineConfig:
      cacheSizeGB: 2
```

Activez et démarrez le service MongoDB :

```
sudo systemctl daemon-reload
sudo systemctl enable mongod
sudo systemctl start mongod
sudo systemctl status mongod
```

Installation de Graylog 5.2

Téléchargement du dépôt, mise à jour et installation de Graylog :

```
wget https://packages.graylog2.org/repo/packages/graylog-5.2-repository_latest.deb
sudo dpkg -i graylog-5.2-repository_latest.deb
sudo apt update
sudo apt install -y graylog-server
```

Générer le secret de mot de passe (password_secret), qui nécessite un minimum de 96 caractères :

```
pwgen -N 1 -s 96
```

Générer le hash SHA256 du mot de passe administrateur :

```
echo -n 'VotreMotDePasse' | sha256sum
```

Attention : Notez immédiatement ces deux valeurs car elles ne peuvent pas être récupérées ensuite.

Configuration de Graylog

Ouvrez le fichier de configuration de Graylog :

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

Renseignez les paramètres essentiels suivants :

```
password_secret = <valeur_générée_pwgen>
root_password_sha2 = <hash_sha256_mot_de_passe>
http_bind_address = 0.0.0.0:9000
elasticsearch_hosts = http://127.0.0.1:9200
mongodb_uri = mongodb://localhost:27017/graylog
```

Activez et démarrez le service Graylog :

```
sudo systemctl daemon-reload
sudo systemctl enable graylog-server
sudo systemctl start graylog-server
```

Vérification des status

Vérifier l'état des services dans cette ordre précis :

```
sudo systemctl status elasticsearch
sudo systemctl status mongod
sudo systemctl status graylog-server
```

Vérifier les ports ouverts :

```
sudo ss -tlnp | grep -E '9200|9300|9000|27017'
```

Vérifier la mémoire RAM disponible sur le système :

```
free -h
```

Se connecter à l'interface

Ouvrer un navigateur et connectez-vous à l'URL suivante :

http://<IP de la VM>:9000
Identifiant : admin
Mot de passe : MDP utilisé pour générer le hash SHA256

Remontée des logs Proxmox vers Graylog

Créer un Input Syslog UDP dans Graylog

- Aller dans System → Inputs
- Sélectionner Syslog UDP dans la liste déroulante
- Cliquer Launch new input
- Title: Proxmox | Bind address: 0.0.0.0 | Port: 5140
- Cliquer Save → l'input doit afficher RUNNING

Configurer rsyslog sur l'hôte Proxmox

Connectez-vous au Shell de votre hôte Proxmox et installez rsyslog :

```
apt update && apt install -y rsyslog
```

Créer le fichier de configuration :

```
sudo nano /etc/rsyslog.d/graylog.conf
```

Ajoutez la ligne suivante à l'intérieur du fichier :

```
*.* @<IP_VM_GRAYLOG>:5140
```

Activez et redémarrez le service rsyslog sur Proxmox :

```
sudo systemctl daemon-reload
sudo systemctl enable rsyslog
sudo systemctl start rsyslog
sudo systemctl status rsyslog
```

Pour terminer, rendez-vous dans l'interface de Graylog, allez dans l'onglet **Search** et tapez * dans la barre de recherche pour voir vos logs Proxmox apparaître en temps réel !