Installation de Graylog

sous Debian 12

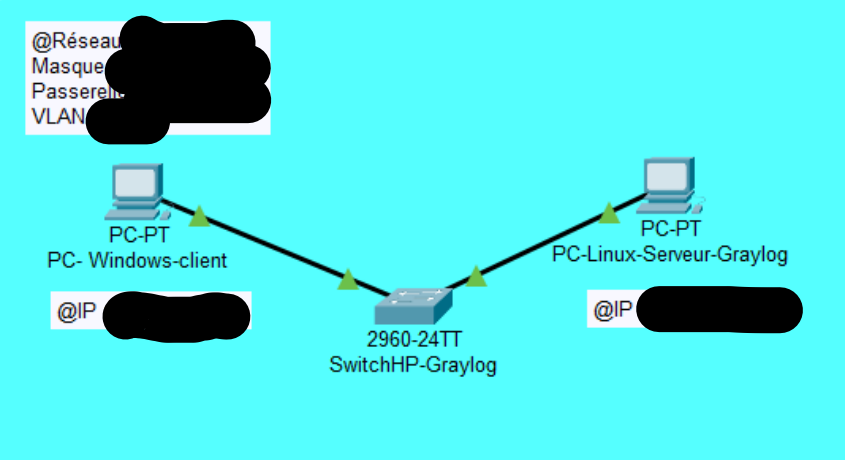
SOMMAIRE

I. Introduction..... 2
1.1. Schéma réseau de la mise en place du lab..... 2
II. Installation Graylog 6.0 sous Debian 12..... 2
2.1. Prérequis.....2
2.1.1. Configuration IP.....2
2.1.2. Mise à Jour/ Niveau des paquets.....2
3.1. MongoDB installation..... 3
3.1.1. Paquets nécessaires à installer.....3
3.1.2. Importation de la clé GPG publique MongoDB..... 3
3.1.3. Création d'un fichier pour MongoDB..... 3
3.1.4. Recharge de la base de données des packages locaux.....3
3.1.5. Installation des packages MongoDB (dernière version).....3
3.1.6. Activation de MongoDB lors du démarrage du système d'exploitation..... 3
3.1.7. Vérification du status du service MongoDB.....4
4.1. OpenSearch installation..... 4
4.1.1. Installation des packages nécessaire.....4
4.1.2. Importation de la clé GPG publique (Vérifier que le dépôt APT est signé)..... 4
4.1.3. Création d'un dépôt APT pour OpenSearch.....4
4.1.4. Vérification que le référentiel a été créé avec succès..... 4
4.1.5 . Sélection version d'OpenSearch..... 5
4.2. Configuration d'OpenSearch..... 5
4.2.1. Ouvrir le fichier yml.....5
4.2.2. MAJ les champs suivants pour un état d'exécution non sécurisé minimum..... 5
4.2.3. Activez les options de la JVM.....5
4.2.4. MAJ les paramètres Xms et Xmx avec la moitié de la mémoire système installée..... 6
4.2.5. Configuration des paramètres du noyau au moment de l'exécution..... 6
4.2.6. Activation du service..... 6
4.2.7. Vérification du status du service OpenSearch..... 6
5.1. Installation de Graylog.....6
5.1.1. Installation configuration du référentiel Graylog et Graylog Open.....6

I. Introduction

L'objectif est de mettre en place un outil de supervision en Open Source en récupérant les logs afin de pouvoir les analyser et les visualiser sur une interface web. Pour ce faire nous allons mettre en place un serveur Graylog sous Linux.

1.1. Schéma réseau de la mise en place du lab



II. Installation Graylog 6.0 sous Debian 12

2.1. Prérequis

2.1.1. Configuration IP

PC-Windows-client	PC-Linux-Serveur-Garylog

Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP :
Masque de sous-réseau :
Passerelle par défaut :
	`# Static IP address`
	
	`allow-hotplug enp1s0`
	`iface enp1s0 inet static`
	`address`
	`network`
	`gateway`

2.1.2. Mise à Jour/ Niveau des paquets

```
sudo apt -y update && -y apt upgrade -y
```

3.1. MongoDB installation

MongoDB est une base de données NoSQL orientée documents. Contrairement aux bases de données relationnelles traditionnelles qui utilisent des tables et des lignes, MongoDB stocke les données dans des documents similaires à des objets JSON.

3.1.1. Paquets nécessaires à installer

```
sudo apt-get install gnupg curl
```

3.1.2. Importation de la clé GPG publique MongoDB

```
curl -fsSL https://www.mongodb.org/static/pgp/server-7.0.asc | \
   sudo gpg -o /usr/share/keyrings/mongodb-server-7.0.gpg \
   --dearmor
```

3.1.3. Création d'un fichier pour MongoDB

```
echo "deb [ signed-by=/usr/share/keyrings/mongodb-server-7.0.gpg ]
http://repo.mongodb.org/apt/debian bookworm/mongodb-org/7.0 main"
| sudo tee /etc/apt/sources.list.d/mongodb-org-7.0.list
```

3.1.4. Recharge de la base de données des packages locaux

```
sudo apt-get update
```

3.1.5. Installation des packages MongoDB (dernière version)

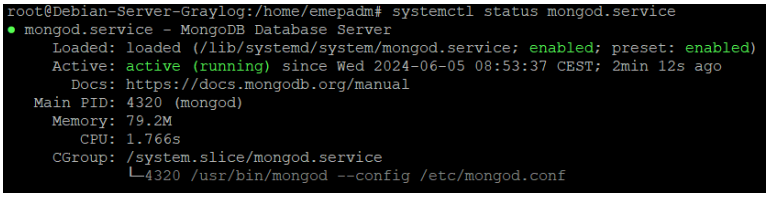
```
sudo apt-get install -y mongodb-org
```

3.1.6. Activation de MongoDB lors du démarrage du système d'exploitation

```
sudo systemctl daemon-reload

sudo systemctl enable mongod.service

sudo systemctl restart mongod.service

sudo systemctl status mongod.service
```

3.1.7. Vérification du status du service MongoDB

Il est essentiel de contrôler l'état du service pour garantir son bon fonctionnement.



4.1. OpenSearch installation

OpenSearch est un moteur de recherche qui indexe les logs pour permettre des recherches rapides via des requêtes complexes. Les données de logs sont stockées de manière efficace en utilisant des index et des shards pour une performance optimale.

4.1.1. Installation des packages nécessaire

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

4.1.2. Importation de la clé GPG publique (Vérifier que le dépôt APT est signé)

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

4.1.3. Création d'un dépôt APT pour OpenSearch

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

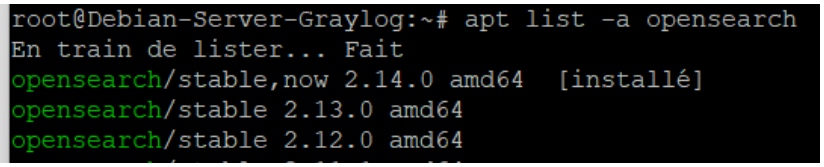
4.1.4. Vérification que le référentiel a été créé avec succès

```
sudo apt-get update
```

4.1.5 . Sélection version d'OpenSearch

```
sudo apt list -a opensearch
```

On installe la version souhaitée d'OpenSearch et on définit un mot de passe.



Ce mot de passe est utilisé pour sécuriser l'accès à OpenSearch.

```
sudo OPENSEARCH_INITIAL_ADMIN_PASSWORD="Gir@fe2pin$Exist3!"
apt-get -y install opensearch=2.14.0
```

Pour éviter que la version du package OpenSearch ne soit automatiquement mise à niveau vers une version plus récente lors de l'installation des mises à jour, on peut figer la version en utilisant la commande suivante :

```
sudo apt-mark hold opensearch
```

4.2. Configuration d'OpenSearch

4.2.1. Ouvrir le fichier yml

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

4.2.2. MAJ les champs suivants pour un état d'exécution non sécurisé minimum

```
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
```

4.2.3. Activez les options de la JVM

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

4.2.4. MAJ les paramètres Xms et Xmx avec la moitié de la mémoire système installée

```
# Xms represents the initial size of total heap space
# Xmx represents the maximum size of total heap space

-Xms1g
-Xmx1g
```

4.2.5. Configuration des paramètres du noyau au moment de l'exécution

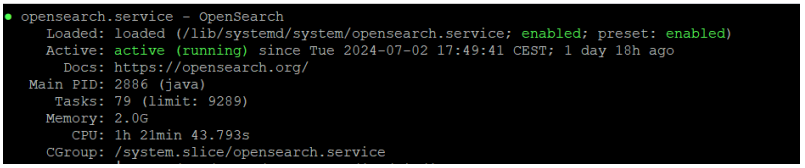
```
sudo sysctl -w vm.max_map_count=262144
sudo echo 'vm.max_map_count=262144' >> /etc/sysctl.conf
```

4.2.6. Activation du service

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

4.2.7. Vérification du status du service OpenSearch

Il est essentiel de contrôler l'état du service pour garantir son bon fonctionnement.



5.1. Installation de Graylog

5.1.1. Installation configuration du référentiel Graylog et Graylog Open

```
wget
https://packages.graylog2.org/repo/packages/graylog-6.0-repository
_latest.deb
sudo dpkg -i graylog-6.0-repository_latest.deb
sudo apt-get update && sudo apt-get install graylog-server
```

Enfin même principe que pour Opensearch si l'on souhaite figer la version :

```
sudo apt-mark hold graylog-server
```