

PETIT Antoine

Date de début : 29/11/24

Date de fin : 02/11/24

GrayLog Debian 12



Sommaire

1	CONTEXTE	3
2	OBJECTIFS	3
3	PORTÉE	3
4	PRÉREQUIS	3
5	RÉALISATION	4
5.1	INSTALLATION MONGODB	4
5.2	INSTALLATION DATA NODE	4
5.3	INSTALLATION GRAYLOG	5
5.4	INITIALISATION GRAYLOG INTERFACE WEB	6

1 CONTEXTE

Dans un environnement informatique moderne, la gestion des logs est cruciale pour la sécurité, la conformité et la performance des systèmes. **Graylog** est une solution de gestion centralisée des logs permettant de collecter, stocker, analyser et visualiser les données des logs générées par les serveurs, applications, équipements réseaux et systèmes de sécurité.

2 OBJECTIFS

Mettre en place une plateforme **Graylog** pour la centralisation, l'analyse et la visualisation des logs en temps réel, afin de détecter rapidement les anomalies, assurer la conformité et améliorer la performance des systèmes.

3 PORTÉE

Le projet porte sur l'installation et la configuration de **Graylog** pour collecter les logs des serveurs Linux, Windows, des applications, des équipements réseaux (firewall, switches, routeurs), ainsi que des bases de données. L'objectif est d'offrir une vue d'ensemble sur les événements de l'infrastructure IT.

4 PRÉREQUIS

Effectuez une installation propre de Debian 12 avec un nom de machine approprié.

5 RÉALISATION

5.1 INSTALLATION MONGODB

```
sudo apt-get update
sudo apt-get install -y gnupg curl
curl -fsSL https://www.mongodb.org/static/pgp/server-7.0.asc | sudo gpg -o
/usr/share/keyrings/mongodb-server-7.0.gpg --dearmor
echo "deb [signed-by=/usr/share/keyrings/mongodb-server-7.0.gpg]
https://repo.mongodb.org/apt/debian bookworm/mongodb-org/7.0 main" | sudo tee
/etc/apt/sources.list.d/mongodb-org-7.0.list
sudo apt-get update
sudo apt-get install -y mongodb-org
sudo systemctl daemon-reload
sudo systemctl enable mongod.service
sudo systemctl restart mongod.service
sudo systemctl --type=service --state=active | grep mongod
```

5.2 INSTALLATION DATA NODE

```
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 -y graylog-datanode
cat /proc/sys/vm/max_map_count
sudo nano /etc/sysctl.conf
dans nano :
vm.max_map_count=262144
/exit nano
sudo sysctl -p
```

Cette commande va créer une clef d'identification.

```
< /dev/urandom tr -dc A-Z-a-z-0-9 | head -c${1:-96};echo;
```

Clef d'identification générée :

GCEOSAlssuH0lhN7GJq6l4Kmi6wnoolzaIUfFPVaa0sm79q8PrZF36aLqJ8AmhytMs8VJKE5vFv
HGkbOeyM595AxQJ37m4lE

```
sudo nano /etc/graylog/datanode/datanode.conf
dans nano :
password_secret = <clef d'identification>
/exit nano
sudo systemctl enable graylog-datanode.service
sudo systemctl start graylog-datanode
```

5.3 *INSTALLATION GRAYLOG*

```
sudo apt-get install -y graylog-server
sudo nano /etc/graylog/server/server.conf
dans nano :
password_secret = <clef d'identification>
/exit nano
echo -n "Enter Password: " && head -1 </dev/stdin | tr -d '\n' | sha256sum | cut -d" " -f1
Enter Password: Blaise36!
```

Mot de passe chiffré : Blaise36 !

8da40490c21d49384bc01a1f2533fe6b5317862aae87f2fdd8db1c810d3a2e71

```
sudo nano /etc/graylog/server/server.conf
dans nano :
root_password_sha2 = <mdp-chiffre>
/exit nano
sudo sed -i 's/#http_bind_address = 127.0.0.1.*/http_bind_address = 0.0.0.0:9000/g'
/etc/graylog/server/server.conf
sudo systemctl daemon-reload
sudo systemctl enable graylog-server.service
sudo systemctl start graylog-server.service
sudo systemctl --type=service --state=active | grep graylog
tail /var/log/graylog-server/server.log
```


5.4 INITIALISATION GRAYLOG INTERFACE WEB





Allez sur l'interface web de GrayLog : <IP-GrayLog>:9000.
Entrez le login et le mot de passe fournis par la commande *tail*.
Vous arriverez donc sur cette page :

Graylog Data Nodes

Graylog data nodes offer a better integration with Graylog and simplify future updates. Once a Graylog data node is running and you configured the certificate authority, you can resume startup.

These are the data nodes which are currently registered. The list is constantly updated.

 C02BE21E – Srv-deb12-x64-Graylog-PETIT

-  Configure a certificate authority
-  Configure a renewal policy
-  Provision certificates for your data nodes
-  Configuration finished

You can always restart the configuration

Configure Certificate Authority

In this first step you can either upload or create a new certificate authority.
Using it we can provision your data nodes with certificates easily.

[Create new CA](#) [Upload CA](#)

Here you can quickly create a new certificate authority. All you need to do is to click on the "Create CA" button. The CA should only be used to secure your Graylog data nodes.

Organization Name *

Graylog CA

Create CA

Cliquez sur "Create CA"

Une fois la page actualisée, elle doit apparaître comme suit :

Graylog Data Nodes

Graylog data nodes offer a better integration with Graylog and simplify future updates. Once a Graylog data node is running and you configured the certificate authority, you can resume startup. These are the data nodes which are currently registered. The list is constantly updated.

C02BE21E

 – Srv-deb12-x64-Graylog-PETIT

- ☒ Configure a certificate authority
- ☒ Configure a renewal policy
- ☐ Provision certificates for your data nodes
- ☐ Configuration finished

You can always [restart](#) the configuration

Configure Renewal Policy

In this step you can configure if certificates which are close to expiration should be renewed automatically. If you choose manual renewal, a system notification will show up when the expiration date is near, requiring you to confirm renewal.

Renewal Policy *

Automatic

Certificate lifetime *

30

^
v

Day(s)

^
v


Create policy





Laissez les paramètres par défaut et cliquez sur "Create policy".

La page va s'actualiser à nouveau.

Graylog Data Nodes

Graylog data nodes offer a better integration with Graylog and simplify future updates. Once a Graylog data node is running and you configured the certificate authority, you can resume startup. These are the data nodes which are currently registered. The list is constantly updated.

 C02BE21E – Srv-deb12-x64-Graylog-PETIT

-  Configure a certificate authority
-  Configure a renewal policy
-  Provision certificates for your data nodes
-  Configuration finished

You can always **restart** the configuration

Provision certificates


Certificate authority has been configured successfully.
You can now provision certificate for your data nodes.





[Provision certificate and continue](#) [Skip provisioning](#)

Cliquez ensuite sur "Provision certificate and continue".

Graylog Data Nodes

Graylog data nodes offer a better integration with Graylog and simplify future updates. Once a Graylog data node is running and you configured the certificate authority, you can resume startup. These are the data nodes which are currently registered. The list is constantly updated.

 C02BE21E https://Srv-deb12-x64-Graylog-PETIT:9200 – Srv-deb12-x64-Graylog-PETIT

-  Configure a certificate authority
-  Configure a renewal policy
-  Provision certificates for your data nodes
-  Configuration finished

You can always **restart** the configuration

Configuration finished

The provisioning has been successful and all data nodes are secured and reachable.

[Resume startup](#)

Cliquez sur "Resume startup".

Une fois la page actualisée, vous arriverez sur la page de connexion de GrayLog.

Username : admin / Password : [≤Mdp-chiffrer>](#)