



## Installation de Graylog sur Debian 12 pour la centralisation et l'analyse des logs

Équipe de rédaction et d'approbation		
<b>NGANSOP NJANOU ULRICH SOSTAIRE</b>	Junior Network Administrator <b>EVOLV IZSOFTWARES GROUP Ltd</b>	Date: 20 janvier 2025
<b>GILDAS FOTSO TABAFO</b>	Junior Network Administrator <b>EVOLV IZSOFTWARES GROUP Ltd</b>	Date: 20 janvier 2025
<b>Beryl Ngonga</b>	Professional Framer <b>EVOLV IZSOFTWARES GROUP Ltd</b>	Date de fin : _
Sommaire des révisions		
Historique de Révision	Description générale	Date approuvée
0.0.2	Document, version 2	

Centralisez et analysez facilement vos logs grâce à Graylog, déployé sur Debian 12.

### I. Introduction

Graylog est une solution open source de gestion centralisée des logs, permettant de collecter, stocker et analyser en temps réel les journaux de vos serveurs et équipements réseaux. Ce tutoriel explique comment installer la version gratuite de Graylog sur une machine Debian 12.

Dans un système d'information, chaque serveur (Linux ou Windows) et chaque équipement réseau (switch, routeur, firewall, etc.) génère des journaux stockés localement. L'analyse et la corrélation de ces journaux dispersés est complexe. Graylog, agissant comme un "puits de logs", centralise ces données. Vos machines envoient leurs logs à Graylog (via syslog, par exemple), qui les stocke, les indexe, et permet des recherches globales et la création d'alertes.

Graylog est un outil d'analyse et de surveillance facilitant l'identification des comportements suspects et la résolution de problèmes liés à la stabilité et aux performances.

## II. Prérequis

La stack **Graylog** repose sur plusieurs composants qui doivent être installés et configurés. Nous allons installer **Graylog 6.2**, la version la plus récente à ce jour.

Voici les composants recommandés pour une configuration optimale :

- **MongoDB** : Graylog recommande d'utiliser **MongoDB 6** (version minimale **5.0.7**, maximale **7.x**). MongoDB est utilisé pour le stockage des configurations et des métadonnées.
- **OpenSearch** : Un fork open-source d'Elasticsearch, développé à l'origine par Amazon. Les versions recommandées vont de **1.1.x à 2.15.x**. OpenSearch offre une plateforme de recherche et d'analyse puissante et flexible.
- **OpenJDK 17** : La dernière version de Java, nécessaire au bon fonctionnement du serveur Graylog. Elle permet de garantir la stabilité et la performance du système.

Le serveur **Graylog** est installé sur **Debian 12** avec une machine virtuelle équipée de **8 Go de RAM et 256 Go d'espace disque**. Cette configuration offre suffisamment de ressources pour tous les composants nécessaires au bon fonctionnement du serveur. Cependant, cela est uniquement à titre indicatif, car le dimensionnement de l'architecture Graylog dépend en grande partie de la quantité de données à traiter. Graylog est une solution **scalable**, capable de gérer de petites quantités de données, comme **30 Mo ou 300 Mo par jour**, jusqu'à des volumes beaucoup plus importants, pouvant atteindre **300 Go** voire **des téraoctets** de logs par jour, sans compromettre la performance.

**i** Avant de configurer votre système, assurez-vous d'attribuer une adresse IP statique à la machine Graylog et d'installer les dernières mises à jour du système.

**i** Veillez aussi à configurer le fuseau horaire de la machine locale et définissez un serveur NTP pour la synchronisation de la date et l'heure. Voici la commande à exécuter :

```
sudo timedatectl set-timezone Europe/Paris
```

**i Remarque** : l'installation d'**OpenSearch est facultative** si vous utilisez **Graylog Data Node** à la place

## III. Installation de Graylog

Commençons par mettre à jour le cache des paquets et installer les outils nécessaires.`sudo apt-get update`

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

```
flo@srv-graylog:~$ sudo apt-get install curl lsb-release ca-certificates gnupg2
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
lsb-release est déjà la version la plus récente (12.0-1).
lsb-release passé en « installé manuellement ».
ca-certificates est déjà la version la plus récente (20230311).
Les paquets supplémentaires suivants seront installés :
  dirmngr gnupg gnupg-l10n gnupg-utils gpg gpg-agent gpg-wks-client gpg-wks-server gpgconf
    libksba8 libnpth0 pinentry-curses
Paquets suggérés :
  pinentry-gnome3 tor parcimonie xloadimage scdaemon pinentry-doc
Les NOUVEAUX paquets suivants seront installés :
  curl dirmngr gnupg gnupg-l10n gnupg-utils gnupg2 gpg gpg-agent gpg-wks-client gpg-wks-server gpgconf
    libassuan0 libcurl4 libksba8 libnpth0 pinentry-curses
0 mis à jour, 17 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 9 031 ko dans les archives.
Après cette opération, 17,8 Mo d'espace disque supplémentaires seront utilisés.

Souhaitez-vous continuer ? [O/n] o
```

## A. Installation de MongoDB

Après cela, nous installerons MongoDB. Commencez par télécharger la clé GPG du 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
```

Ensuite, ajoutez le dépôt MongoDB 6 à votre 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, puis tenter l'installation de 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 : **libssl1.1.1**. 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 ».

Pour installer la dernière version du paquet DEB "**libssl1.1\_1.1.1f-1ubuntu2.23\_amd64.deb**", nous utiliserons d'abord la commande **wget** pour le télécharger, puis **dpkg** pour son installation. Voici les deux commandes :

```
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
```

```
flo@srv-graylog:/tmp$ wget http://archive.ubuntu.com/ubuntu/pool/main/o/openssl/libssl1.1_1.1.1f-1ubuntu2.23_amd64.deb
--2024-10-29 16:19:21-- http://archive.ubuntu.com/ubuntu/pool/main/o/openssl/libssl1.1_1.1.1f-1ubuntu2.23_amd64.deb
Résolution de archive.ubuntu.com (archive.ubuntu.com)... 185.125.190.81, 91.189.91.83, 91.189.91.81, ...
Connexion à archive.ubuntu.com (archive.ubuntu.com)|185.125.190.81|:80... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 1323104 (1,3M) [application/vnd.debian.binary-package]
Sauvegarde en : « libssl1.1_1.1.1f-1ubuntu2.23_amd64.deb »

libssl1.1_1.1.1f-1ubuntu2.23_ 100%[=====] 1,26M 52,1KB/s   ds 20s
2024-10-29 16:19:42 (64,5 KB/s) - « libssl1.1_1.1.1f-1ubuntu2.23_amd64.deb » sauvegardé [1323104/1323104]

flo@srv-graylog:/tmp$ sudo dpkg -i libssl1.1_1.1.1f-1ubuntu2.23_amd64.deb
 Sélection du paquet libssl1.1:amd64 précédemment désélectionné.
(Lecture de la base de données... 34237 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de libssl1.1_1.1.1f-1ubuntu2.23_amd64.deb ...
Dépaquetage de libssl1.1:amd64 (1.1.1f-1ubuntu2.23) ...
Paramétrage de libssl1.1:amd64 (1.1.1f-1ubuntu2.23) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.36-9+deb12u8) ...
flo@srv-graylog:/tmp$
```

Relancez l'installation de MongoDB.

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

Ensuite, redémarrez le service MongoDB et configurez son démarrage automatique au démarrage 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 étant installé, nous pouvons passer à l'installation du composant suivant.

## B. Installation d'OpenSearch

Installons OpenSearch sur le serveur. Commencez par ajouter la clé de signature des paquets OpenSearch à l'aide de la commande suivante :

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

Ensuite, ajoutez le dépôt OpenSearch pour pouvoir télécharger le paquet avec `apt` :

```
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
```

Actualisez votre cache de paquets :

```
sudo apt-get update
```

Ensuite, installez OpenSearch en veillant à définir un mot de passe administrateur robuste pour votre instance. Utilisez un mot de passe complexe, d'au moins 8 caractères, comprenant des minuscules, des majuscules, des chiffres et des caractères spéciaux (ex: "MonMotDePasse1!"). Évitez les mots de passe faibles comme "P@ssword123". Depuis OpenSearch 2.12, ceci est obligatoire. Une erreur surviendra autrement à la fin de l'installation.

Pour ce faire, exécutez la commande suivante (remplacez "IZSoftware" par votre mot de passe):

```
sudo env OPENSEARCH_INITIAL_ADMIN_PASSWORD=IT-IZSoftware apt-get install opensearch
```

Patiencez pendant l'installation...

Une fois l'installation terminée, configurez OpenSearch. Ouvrez le fichier de configuration YAML avec la commande suivante :

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

Puis, ajoutez ou modifiez les lignes suivantes :

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

Enregistrez et fermez le fichier.

Cette configuration OpenSearch est conçue pour un nœud unique. Voici une explication détaillée des paramètres utilisés :

- **cluster.name: graylog** : Le cluster OpenSearch est nommé "**graylog**".
- **node.name: \${HOSTNAME}** : Le nom du nœud est défini dynamiquement en utilisant le nom d'hôte de la machine Linux. Même pour un nœud unique, un nom explicite est crucial.
- **path.data: /var/lib/opensearch** : OpenSearch stocke ses données dans le répertoire "**/var/lib/opensearch**".
- **path.logs: /var/log/opensearch** : Les fichiers journaux d'OpenSearch sont stockés dans "**/var/log/opensearch**".
- **discovery.type: single-node** : Ce paramètre spécifie le mode nœud unique pour OpenSearch.
- **network.host: 127.0.0.1** : OpenSearch écoute uniquement sur l'interface loopback (localhost), car il est hébergé sur le même serveur que Graylog.

- **action.auto\_create\_index: false** : La création automatique d'index est désactivée. OpenSearch ne créera pas d'index automatiquement pour les documents envoyés sans index pré-existant.
- **plugins.security.disabled: true** : Le plugin de sécurité OpenSearch est désactivé. Ceci implique l'absence d'authentification, de contrôle d'accès et de chiffrement. Cette configuration accélère le déploiement de Graylog, mais est fortement déconseillée en production.

Certaines options sont déjà définies ; il suffit de supprimer le symbole « # » pour les activer et spécifier leur valeur. Si une option est manquante, vous pouvez l'ajouter directement à la fin du fichier.

```

GNU nano 7.2                               /etc/opensearch/opensearch.yml *
#
# Before you set out to tweak and tune the configuration, make sure you
# understand what are you trying to accomplish and the consequences.
#
# The primary way of configuring a node is via this file. This template lists
# the most important settings you may want to configure for a production cluster.
#
# Please consult the documentation for further information on configuration options:
# https://www.opensearch.org
#
# ----- Cluster -----
#
# Use a descriptive name for your cluster:
#
cluster.name: graylog
#
# ----- Node -----
#
# Use a descriptive name for the node:
#
node.name: ${HOSTNAME}
#
# Add custom attributes to the node:
#
#node.attr.rack: r1
#
# ----- Paths -----
^G Aide          ^O Écrire        ^W Chercher      ^K Couper       ^T Exécuter      ^C Emplacement
^X Quitter       ^R Lire fich.   ^\ Remplacer     ^U Coller       ^J Justifier    ^/ Aller lign

```



Enregistrez et fermez ce fichier.

## C. Configurer Java (JVM)

Configurez Java (JVM) d'OpenSearch pour contrôler la quantité de mémoire qu'il utilise. Modifiez le fichier de configuration suivant :

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

Avec la configuration ci-dessous, OpenSearch démarrera avec 4 Go de mémoire allouée et pourra utiliser jusqu'à 4 Go au maximum. La consommation mémoire restera donc constante. Cette configuration suppose que la machine dispose de 8 Go de RAM au total. Les deux paramètres doivent avoir la même valeur. Remplacez donc :

```
-Xms1g
```

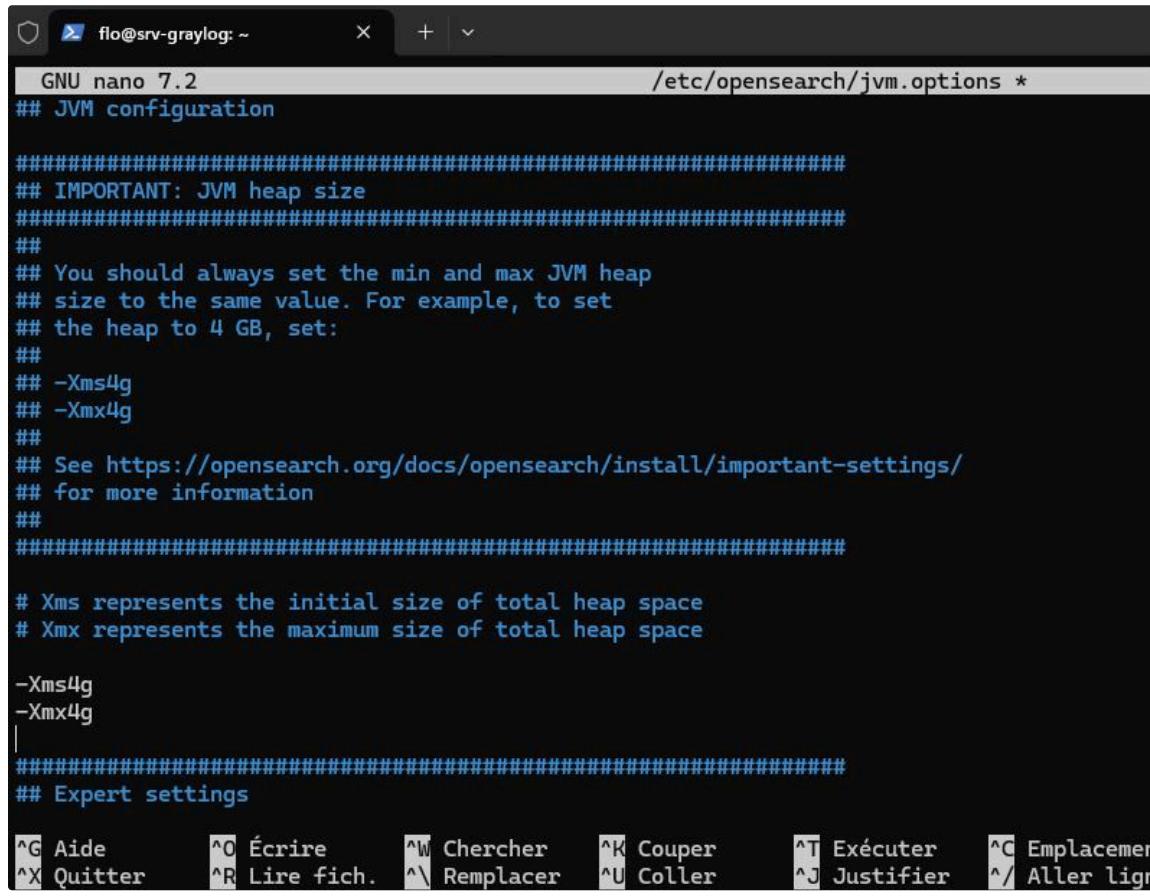
```
-Xmx1g
```

Par :

```
-Xms4g
```

```
-Xmx4g
```

Une illustration de la modification est fournie ci-dessous :



```
GNU nano 7.2 /etc/opensearch/jvm.options *
## 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

-Xms4g
-Xmx4g
|
#####
## Expert settings

^G Aide      ^O Écrire      ^W Chercher      ^K Couper      ^T Exécuter      ^C Emplacement
^X Quitter    ^R Lire fich.  ^\ Remplacer    ^U Coller       ^J Justifier    ^/ Aller ligne
```

i Fermez ce fichier après l'avoir enregistré.

Pour garantir le bon fonctionnement d'OpenSearch, vérifiez la configuration du paramètre noyau Linux "**max\_map\_count**". Ce paramètre limite le nombre de zones de mémoire mappées par processus. **OpenSearch**, tout comme **Elasticsearch**, recommande de le **fixer à 262144 pour prévenir les erreurs de gestion mémoire**.

Sur une installation Debian 12 standard, cette valeur devrait déjà être correcte. Pour vous en assurer, exécutez la commande suivante :

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

Si la valeur affichée diffère de **262144**, exécutez la commande ci-dessous. Sinon, ignorez cette étape.

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

Enfin, activez le démarrage automatique et redémarrez le service OpenSearch :

```
1 sudo systemctl daemon-reload
2 sudo systemctl enable opensearch
3 sudo systemctl restart opensearch
```

Vous devriez ensuite observer un processus Java utilisant environ 4 Go de RAM en affichant l'état du système avec la commande :

```
1 top
```

```

top - 17:43:36 up 2:10, 3 users, load average: 0,20, 0,06, 0,02
Tâches: 104 total, 1 en cours, 103 en veille, 0 arrêté, 0 zombie
%Cpu(s): 0,2 ut, 0,1 sy, 0,0 ni, 99,8 id, 0,0 wa, 0,0 hi, 0,0 si, 0,0 st
MiB Mem : 7940,2 total, 115,6 libr, 4989,7 util, 3104,5 tmap/cache
MiB Éch : 976,0 total, 975,7 libr, 0,3 util. 2950,5 dispo Mem

PID UTIL. PR NI VIRT RES SHR S %CPU %MEM TEMPS+ COM.
4503 opensea+ 20 0 8103852 4,4g 26828 S 0,7 56,5 0:23.80 java
3441 mongodb 20 0 2585648 168948 66376 S 0,3 2,1 0:10.12 mongod
 1 root 20 0 168960 13452 9032 S 0,0 0,2 0:02.79 systemd
 2 root 20 0 0 0 0 S 0,0 0,0 0:00.00 kthreadd

```

## D. Installation de Graylog ↗

Pour installer la dernière version de Graylog 6.1, suivez ces quatre étapes simples pour télécharger et installer Graylog Server :

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

Une fois l'installation terminée, quelques modifications de configuration sont nécessaires avant le lancement de Graylog. Configurez notamment ces deux paramètres :

- `password_secret` : Cette clé unique et aléatoire assure la sécurité du stockage des mots de passe utilisateurs (principe de salage).
- `root_password_sha2` : Correspond au mot de passe administrateur par défaut, stocké sous forme de hachage SHA-256.

Pour commencer, générerons une clé de 96 caractères pour le paramètre `password_secret` :

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

Ceci vous fournira une clé similaire à celle-ci :

`wVSGYw0mwBIDmtQvGzSuBevWoXe0MwpNWcZhorBfvMMhia2zIjHguTbf14uXZJdHOA0EEb1s0XJTZKINhIIBm3V57vwfQV59` (Copiez la clé générée, pas celle-ci).

Ensuite, ouvrez le fichier de configuration de Graylog :

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

Enfin, collez la clé générée dans le paramètre `password_secret` du fichier de configuration.

```

GNU nano 7.2                               /etc/graylog/server/server.conf *
# * The backslash character must be escaped as a double backslash. For example:
#
# path=c:\\docs\\doc1
#
# If you are running more than one instances of Graylog server you have to select one of these
# instances as leader. The leader will perform some periodical tasks that non-leaders won't perform.
is_leader = true
#
# The auto-generated node ID will be stored in this file and read after restarts. It is a good idea
# to use an absolute file path here if you are starting Graylog server from init scripts or similar.
node_id_file = /etc/graylog/server/node-id
#
# You MUST set a secret to secure/pepper the stored user passwords here. Use at least 64 characters.
# Generate one by using for example: pwgen -N 1 -s 96
# ATTENTION: This value must be the same on all Graylog nodes in the cluster.
# Changing this value after installation will render all user sessions and encrypted values in the database invalid. (e.g.
password_secret = wVSGYw0mwBIDmtQvGzSuBevWoXe0MwpNWcZhorBfvMMhia2zIjHguTbf14uXZJdHOA0EEb1s0XJTZKINhIIBm3V57vwfQV59

```



Enregistrez et fermez le fichier.

Vous devez ensuite définir le mot de passe du compte administrateur par défaut. Le fichier de configuration doit stocker le hachage de ce mot de passe, que vous devez calculer. L'exemple suivant montre comment hacher le mot de passe "PuitsDeLogs@" ; remplacez cette valeur par votre propre mot de passe :

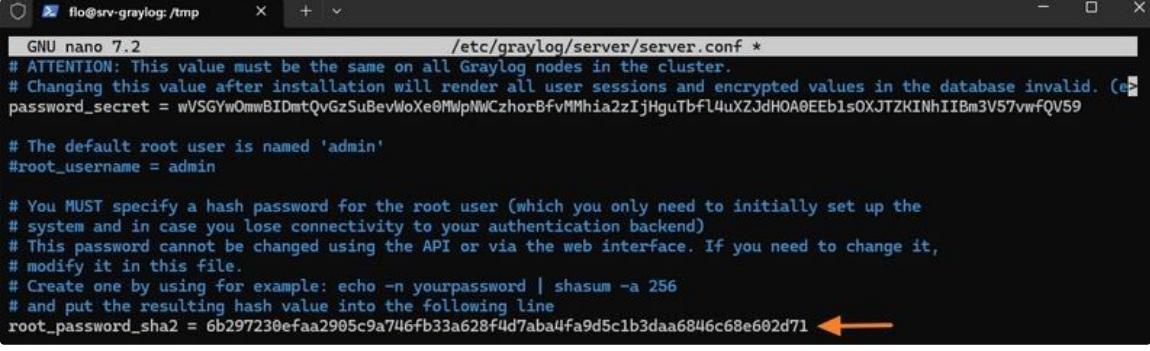
```
1 echo -n "PuitsDeLogs@" | shasum -a 256
```

Copiez la valeur de sortie (sans le tiret final).

Ouvrez ensuite le fichier de configuration de Graylog :

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

Collez cette valeur dans l'option `root_password_sha2`.



```
GNU nano 7.2 /etc/graylog/server/server.conf *
# ATTENTION: This value must be the same on all Graylog nodes in the cluster.
# Changing this value after installation will render all user sessions and encrypted values in the database invalid. (e.g.
password_secret = wVSGYwOmwBIDmtQvGzSuBewWoXeOMWpNWChorBfvMMhia2zIjHguTbfI4uXZJdHOA0EEb1sOXJTZKINhIIBm3V57vwfQV59

# The default root user is named 'admin'
#root_username = admin

# You MUST specify a hash password for the root user (which you only need to initially set up the
# system and in case you lose connectivity to your authentication backend)
# This password cannot be changed using the API or via the web interface. If you need to change it,
# modify it in this file.
# Create one by using for example: echo -n yourpassword | shasum -a 256
# and put the resulting hash value into the following line
root_password_sha2 = 6b297230efaa2905c9a746fb33a628f4d7aba4fa9d5c1b3daa6846c68e602d71 ←
```

Configurez l'option « `http_bind_address` » dans le fichier de configuration en définissant la valeur « `0.0.0.0:9000` ». Cela rendra l'interface web de Graylog accessible sur le port 9000 depuis n'importe quelle adresse IP du serveur.

```
#####
# HTTP settings
#####

#### HTTP bind address
#
# The network interface used by the Graylog HTTP interface.
#
# This network interface must be accessible by all Graylog nodes in the cluster and by all clients
# using the Graylog web interface.
#
# If the port is omitted, Graylog will use port 9000 by default.
#
# Default: 127.0.0.1:9000
http_bind_address = 0.0.0.0:9000
#http_bind_address = [2001:db8::1]:9000
```

Configurez ensuite l'option "elasticsearch\_hosts" avec la valeur "`http://127.0.0.1:9200`" pour spécifier notre instance OpenSearch locale. Cette étape est indispensable car nous n'utilisons pas de nœud de données Graylog. Sans cette configuration, la suite du processus est impossible.

```
# List of Elasticsearch hosts Graylog should connect to.
# Need to be specified as a comma-separated list of valid URIs for the http ports of your elasticsearch nodes.
# If one or more of your elasticsearch hosts require authentication, include the credentials in each node URI that
# requires authentication.
#
# Default: http://127.0.0.1:9200
elasticsearch_hosts = http://127.0.0.1:9200
```

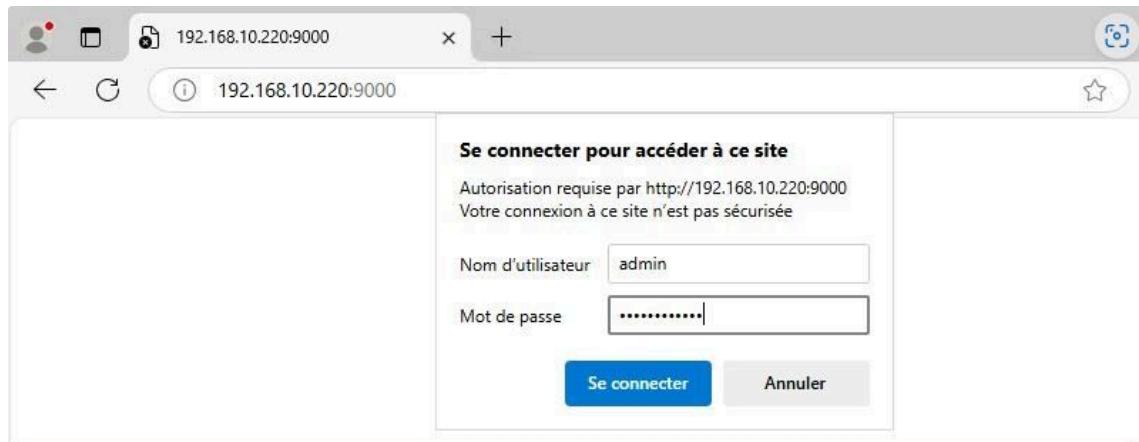
 Enregistrez et fermez le fichier.

Configurez Graylog pour un démarrage automatique au prochain démarrage du système et activez immédiatement le serveur.

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

Une fois cette opération terminée, connectez-vous à Graylog depuis un navigateur web. Saisissez l'adresse IP (ou le nom de domaine) du serveur et le port 9000.

- i** Pour information : lors de la première connexion à Graylog, une fenêtre d'authentification (similaire à celle ci-dessous) s'affichait, demandant l'identifiant « admin » et le mot de passe. Il était alors possible de constater que la connexion ne fonctionnait pas.



Il était nécessaire de retourner en ligne de commande sur le serveur Graylog et de consulter les journaux. On pouvait alors que pour la première connexion, il est nécessaire d'utiliser un mot de passe temporaire, spécifié dans les logs.

```
tail -f /var/log/graylog-server/server.log
```

```
flo@srv-graylog:/tmp$ tail -f /var/log/graylog-server/server.log
=====
It seems you are starting Graylog for the first time. To set up a fresh install, a setup interface has
been started. You must log in to it to perform the initial configuration and continue.

Initial configuration is accessible at 0.0.0.0:9000, with username 'admin' and password 'gWMJDXsbAu'.
Try clicking on http://admin:gWMJDXsbAu@0.0.0.0:9000
=====
```

Il fallait ensuite retenter une connexion avec l'utilisateur "admin" et le mot de passe temporaire, et cela permettait de se connecter !

- i** Désormais, ce n'est plus le cas. Il suffit de se connecter avec son compte admin et le mot de passe configuré en ligne de commande.

**Bienvenue sur l'interface de Graylog !**

## Welcome to Graylog!

This is your personal page, allowing easy access to the content most relevant for you.

### Last Opened

Overview of recently visited saved searches and dashboards.

- i** You have not opened any searches/dashboards yet.  
From now on, whenever you open a saved search/dashboard, it will show up here. In the meantime, you can start a new [Search or Dashboard](#).

### Recent Activity

This list includes all actions Graylog users performed, like creating or sharing an entity.

- i** There is no recent activity yet.  
Whenever any other user will update content you have access to, or share new content with you, it will show up here.

## E. Graylog : création d'un nouveau compte administrateur ↗

Pour une meilleure sécurité, créez un compte administrateur personnel plutôt que d'utiliser le compte administrateur par défaut de Graylog. Accédez au menu "Système", puis sélectionnez "Utilisateurs et équipes". Cliquez sur le bouton "Créer un utilisateur", remplissez le formulaire et attribuez le rôle d'administrateur à votre nouveau compte.

The screenshot shows the Graylog web interface with the 'System / Users and Teams' tab selected. In the 'Users Overview' section, there is a table with one row:

Full name	Username	E-Mail Address	Client Address	Enabled	Role	Actions
Administrator	admin		192.168.10.199	✓	Admin	<a href="#">System user</a> <a href="#">Edit tokens</a>

A green arrow points to the 'Create user' button in the top right corner of the 'Users Overview' panel.

Les comptes personnalisés, contrairement aux comptes administrateur natifs, peuvent inclure des informations supplémentaires telles que le nom, le prénom et l'adresse électronique. Cette approche améliore la traçabilité des actions réalisées, chaque personne étant identifiée par son compte personnel.

## V - Conclusion ↗

Votre serveur Graylog est désormais pleinement opérationnel sous Debian 12 ! Cela signifie que vous pouvez profiter de toutes les fonctionnalités puissantes qu'il offre pour centraliser, indexer et analyser vos journaux à partir d'une interface unique et conviviale. Cette capacité à gérer vos journaux de manière centralisée est essentielle pour une surveillance efficace et une gestion des incidents, vous permettant ainsi de garder un œil sur les performances de votre système et d'identifier rapidement les problèmes potentiels.

Dans les sections suivantes, nous allons explorer en détail comment configurer et envoyer les journaux de vos machines Linux ainsi que de vos serveurs Windows vers votre serveur Graylog. Cette étape est cruciale pour garantir que toutes

vos données de journalisation sont acheminées correctement et que vous pouvez bénéficier d'une vue d'ensemble de l'ensemble de votre infrastructure.

Pour toute difficulté, veuillez contacter les auteurs de ce document ou consulter les articles d'aide et les forums Graylog.

**Équipe de rédaction :**

**Ulrich Sostaire Ngansop Njanou** (Junior Network Administrator)

**Gildas Fotso Tabafo** (Junior Network Administrator)