Documentation Technique : Installation et Configuration du Serveur de Centralisation de Logs Graylog

1. Introduction et Objectifs SIEM

La centralisation, l'analyse et la conservation des journaux d'événements (logs) sont des composants fondamentaux de la gouvernance et de la sécurité d'un système d'information. Cette documentation retrace le déploiement d'une solution **SIEM / Log Management** articulée autour de **Graylog** sur un serveur Linux Debian 12 (Bookworm). Cette plateforme permet de collecter en temps réel les flux d'événements générés par les pare-feux, serveurs et équipements du réseau.

2. Installation et Configuration de la Base de Données MongoDB

Étape 2.1 : Installation des prérequis et clés du dépôt

Graylog utilise MongoDB pour stocker l'intégralité de ses configurations système, fiches d'utilisateurs, métadonnées, flux et alertes. Nous commençons par valider la présence des utilitaires de transport sécurisés, puis nous importons la clé GPG officielle et ajoutons le dépôt amont MongoDB 7.0 dans les sources APT du système.

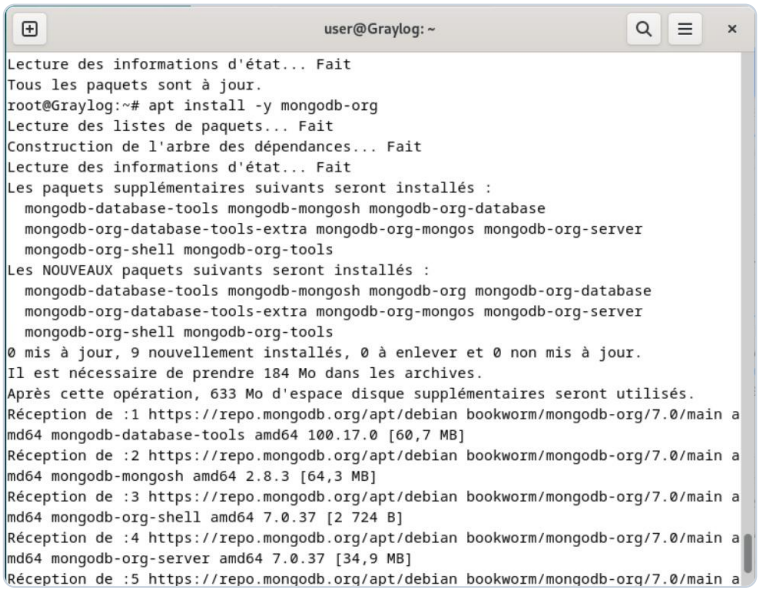
```
sudo apt install -y gnupg wget curl uuid-runtime dirmngr pwgen
curl -fsSL https://www.mongodb.org/static/pgp/server-7.0.asc | gpg --dearmor -
o /usr/share/keyrings/mongodb-server-7.0.gpg
echo "deb [signed-by=/usr/share/keyrings/mongodb-server-7.0.gpg] https://
repo.mongodb.org/apt/debian bookworm/mongodb-org/7.0 main" | sudo tee /etc/apt/
sources.list.d/mongodb-org-7.0.list
```

```
root@Graylog:~# apt install -y gnupg wget curl uuid-runtime dirmngr pwgen
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
gnupg est déjà la version la plus récente (2.2.40-1.1+deb12u2).
wget est déjà la version la plus récente (1.21.3-1+deb12u1).
curl est déjà la version la plus récente (7.88.1-10+deb12u14).
uuid-runtime est déjà la version la plus récente (2.38.1-5+deb12u3).
dirmngr est déjà la version la plus récente (2.2.40-1.1+deb12u2).
pwgen est déjà la version la plus récente (2.08-2).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@Graylog:~# curl -fsSL https://www.mongodb.org/static/pgp/server-7.0.asc | gpg
--dearmor -o /usr/share/keyrings/mongodb-server-7.0.gpg
root@Graylog:~# echo "deb [signed-by=/usr/share/keyrings/mongodb-server-7.0.gpg] ht
tps://repo.mongodb.org/apt/debian bookworm/mongodb-org/7.0 main" | tee /etc/apt/sou
rces.list.d/mongodb-org-7.0.list
deb [signed-by=/usr/share/keyrings/mongodb-server-7.0.gpg] https://repo.mongodb.org
/apt/debian bookworm/mongodb-org/7.0 main
root@Graylog:~#
```

Étape 2.2 : Installation des paquets MongoDB

Après actualisation des index de paquets locaux, nous procédons à l'installation complète du métapaquet de la base de données relationnelle NoSQL.

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



Étape 2.3 : Activation et démarrage du service MongoDB

Nous configurons le gestionnaire de services `systemctl` pour forcer le démarrage persistant de MongoDB dès l'initialisation du noyau Linux, puis nous vérifions que son statut est bien opérationnel.

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

```
user@Graylog:~$ systemctl status mongod
● mongod.service - MongoDB Database Server
     Loaded: loaded (/lib/systemd/system/mongod.service; enabled; preset: enabl>
     Active: active (running) since Mon 2026-06-15 00:18:40 CEST; 2min 11s ago
       Docs: https://docs.mongodb.org/manual
   Main PID: 636 (mongod)
     Memory: 177.0M
        CPU: 844ms
     CGroup: /system.slice/mongod.service
             └─636 /usr/bin/mongod --config /etc/mongod.conf

Warning: some journal files were not opened due to insufficient permissions.
```

3. Installation et Configuration du Moteur d'Indexation OpenSearch

Étape 3.1 : Déclaration du dépôt OpenSearch

Les messages de logs collectés en masse par Graylog sont stockés et indexés au sein du moteur de recherche distribué OpenSearch (alternative open-source à Elasticsearch). Nous téléchargeons sa clé de confiance et déclarons la branche stable de son dépôt officiel dans la configuration APT.

```
curl -fsSL https://artifacts.opensearch.org/publickeys/opensearch.pgp | gpg --
dearmor -o /usr/share/keyrings/opensearch.gpg
echo "deb [signed-by=/usr/share/keyrings/opensearch.gpg] https://
artifacts.opensearch.org/releases/bundle/opensearch/2.x/apt stable main" | sudo
tee /etc/apt/sources.list.d/opensearch-2.x.list
```

```
root@Graylog:~# curl -fsSL https://artifacts.opensearch.org/publickeys/opensearc
h.pgp | gpg --dearmor -o /usr/share/keyrings/opensearch.gpg
root@Graylog:~# echo "deb [signed-by=/usr/share/keyrings/opensearch.gpg] https:/
/artifacts.opensearch.org/releases/bundle/opensearch/2.x/apt stable main" | tee
/etc/apt/sources.list.d/opensearch-2.x.list
deb [signed-by=/usr/share/keyrings/opensearch.gpg] https://artifacts.opensearch.
org/releases/bundle/opensearch/2.x/apt stable main
```

Étape 3.2 : Démarrage et validation d'OpenSearch

Une fois le paquet `opensearch` installé et son fichier de configuration `/etc/opensearch/opensearch.yml` ajusté (nommage du cluster, liaisons réseau), le service est démarré et validé.

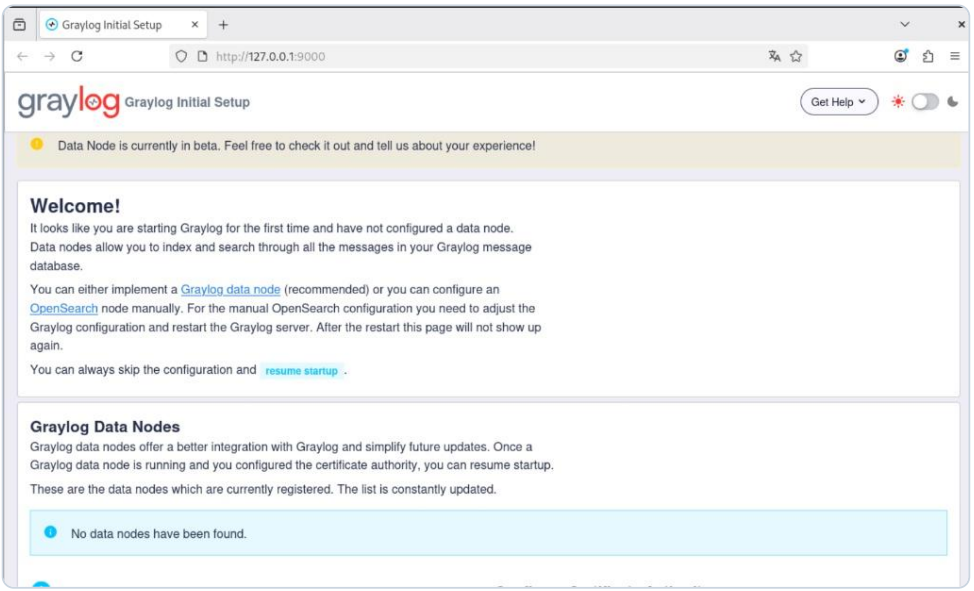
```
sudo systemctl enable opensearch
sudo systemctl start opensearch
sudo systemctl status opensearch
```

```
root@Graylog:~# systemctl status opensearch
● opensearch.service - OpenSearch
     Loaded: loaded (/lib/systemd/system/opensearch.service; enabled; preset: enabled)
     Active: active (running) since Mon 2026-06-15 00:55:41 CEST; 15s ago
       Docs: https://opensearch.org/
   Main PID: 3776 (java)
      Tasks: 65 (limit: 4613)
     Memory: 1.4G
        CPU: 29.106s
     CGroup: /system.slice/opensearch.service
             └─3776 /usr/share/opensearch/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networkaddress.ca
```

4. Initialisation Web et Configuration de Graylog Server

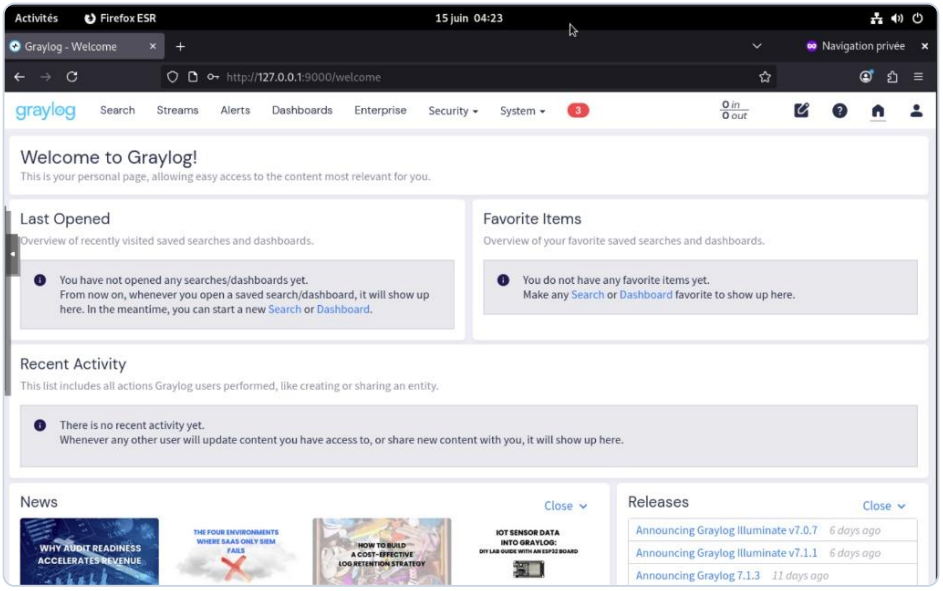
Étape 4.1 : Assistant initial d'intégration des nœuds de données

Après installation du paquet applicatif principal `graylog-server` et génération des clés secrètes obligatoires (mots de passe chiffrés via `pwgen -N 1 -s 96`), nous accédons pour la première fois à l'interface d'initialisation web sur le port par défaut `http://127.0.0.1:9000`. L'assistant détecte l'absence temporaire de nœud de données lié.



Étape 4.2 : Accès au Tableau de Bord principal de Graylog

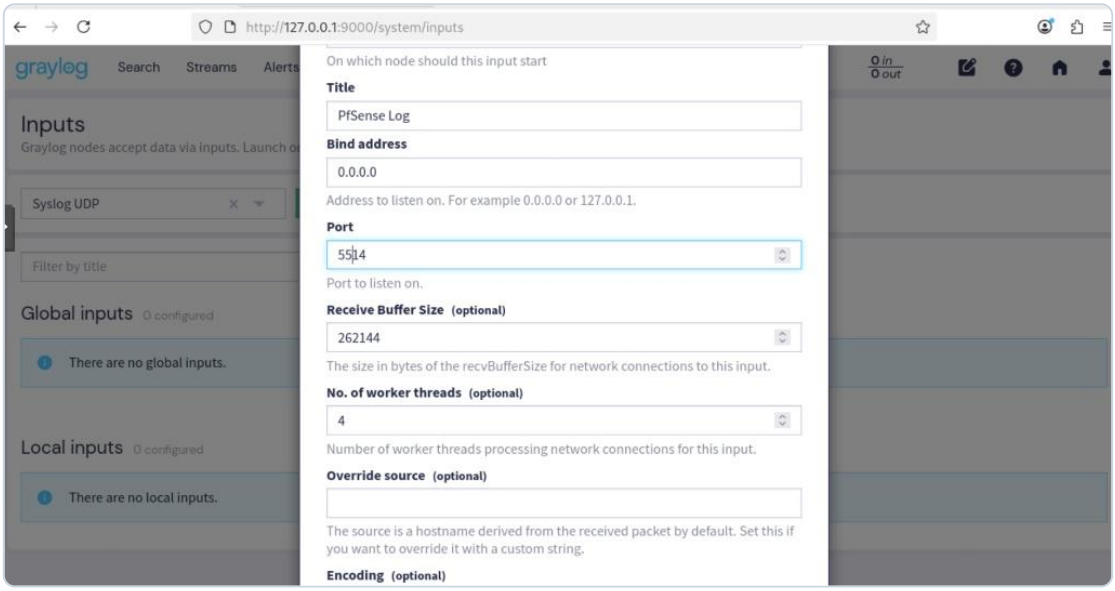
Une fois l'initialisation du fichier `graylog.conf` achevée et le service relancé, l'authentification s'effectue avec le compte super-administrateur. Nous arrivons sur la page d'accueil principale de la console web de Graylog, prête pour la réception de flux réseau.



5. Collecte et Intégration des Flux de Logs (Input Configuration)

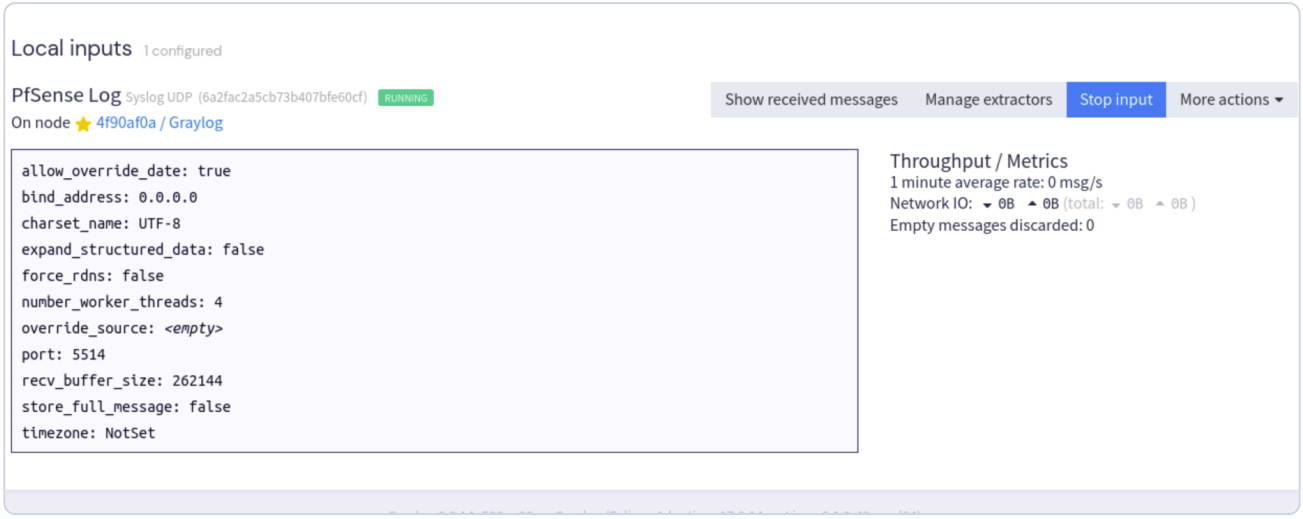
Étape 5.1 : Création de la passerelle de réception (Input Syslog UDP)

Pour collecter les messages distants, nous déclarons un point d'écoute (Input) sur le serveur de logs. Dans la console Graylog, nous naviguons dans **System > Inputs**, sélectionnons un type d'entrée **Syslog UDP** et configurons ses propriétés : titre explicite `PfSense Log`, liaison sur l'adresse d'écoute globale `0.0.0.0` et assignation d'un port réseau d'écoute dédié non standard comme le port `5514`.



Étape 5.2 : Validation de l'activation et de l'état de l'Input

Une fois enregistrée, l'entrée s'initialise et passe instantanément au statut vert **RUNNING**. Les paramètres réseau configurés (taille du tampon mémoire, threads de traitement, port d'écoute) sont listés et le compteur de débit (Throughput) se tient prêt à comptabiliser les messages entrants par seconde.



6. Interconnexion : Routage des Logs depuis le Pare-feu pfSense

La phase finale consiste à configurer l'équipement source pour exporter ses événements vers le collecteur de données Graylog. Au niveau de l'interface d'administration de notre pare-feu pfSense, nous naviguons dans l'onglet de gestion des journaux (**Status > System Logs > Settings**).

Dans la section **Remote Log Servers**, nous renseignons l'adresse IP fixe de notre serveur de centralisation Graylog suivie du port d'écoute configuré précédemment : `10.50.50.45:5514`. Enfin,

nous sélectionnons spécifiquement la nature des événements à exporter en cochant les cases **System Events** (événements liés au système d'exploitation de la passerelle) et **Firewall Events** (historique des paquets filtrés, bloqués ou autorisés par les règles du pare-feu), puis nous sauvegardons la configuration pour ouvrir le flux continu.