



Guide d'Installation et de configuration de graylog server sous AlmaLinux

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

A - Installation et configuration de Graylog sous AlmaLinux ☀

Graylog est une puissante plateforme de gestion des journaux open-source conçue pour collecter, indexer et analyser les données de journal. Elle fournit aux utilisateurs des informations en temps réel sur les performances et la sécurité de leur système en permettant une recherche et une visualisation efficaces des données de journal. L'architecture de Graylog permet une évolutivité et une flexibilité, ce qui la rend adaptée à divers environnements, des petites entreprises aux grandes entreprises.

1. Préparer le système ☀

a) Mettre à jour le système

```
sudo dnf update -y
```

```
sudo dnf upgrade -y
```

b) Configurez un hostname unique pour le serveur Graylog

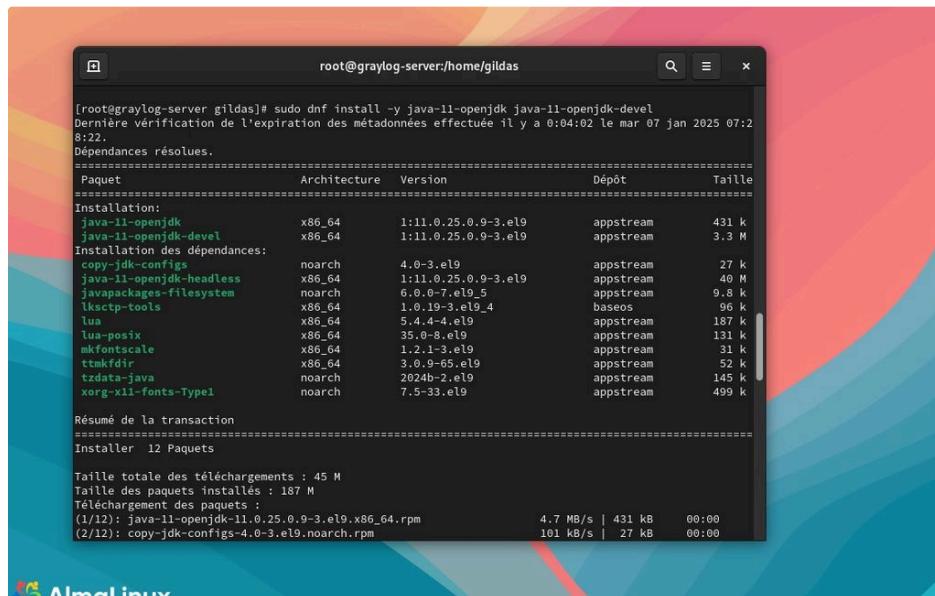
```
sudo hostnamectl set-hostname graylog-server
```

ⓘ Remplacez `graylog-server` par le nom de serveur souhaité.

2. Installer Java (JRE) ↗

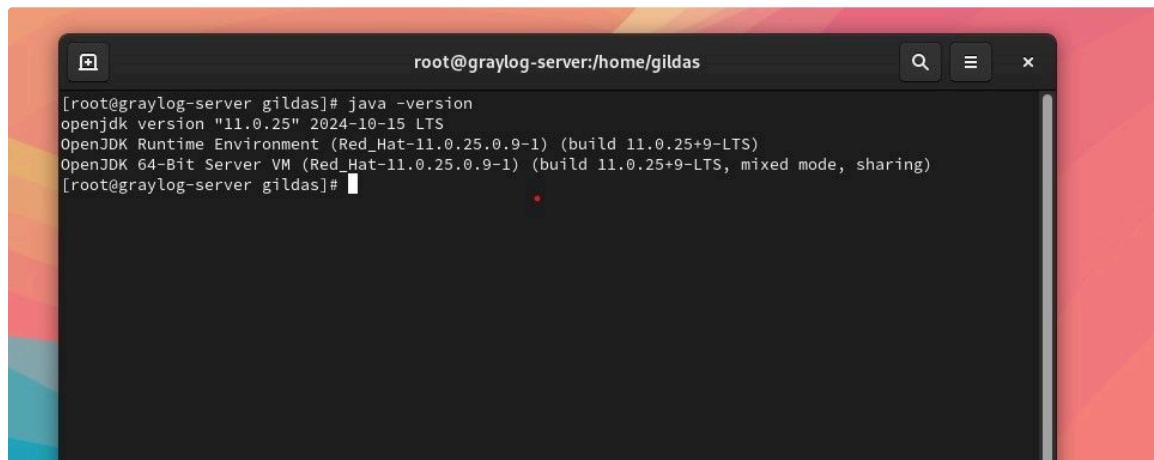
Avant d'installer et de configurer Graylog, assurez-vous que Java est installé sur votre système, car Graylog nécessite une machine virtuelle Java (JVM) pour fonctionner. Nous utiliserons OpenJDK 11, une version stable et compatible. Installez-le avec la commande suivante :

```
sudo dnf install -y java-11-openjdk java-11-openjdk-devel
```



- Vérifiez la version installée :

```
java -version
```



3. Télécharger et installer curl et pwgen ↗

```
sudo dnf install epel-release
```

```
sudo dnf install curl pwgen -y
```

4. Installer MongoDB

Graylog repose sur MongoDB pour le stockage de ses configurations et métadonnées. Assurez-vous que MongoDB est installé et configuré avant de poursuivre l'installation de Graylog.

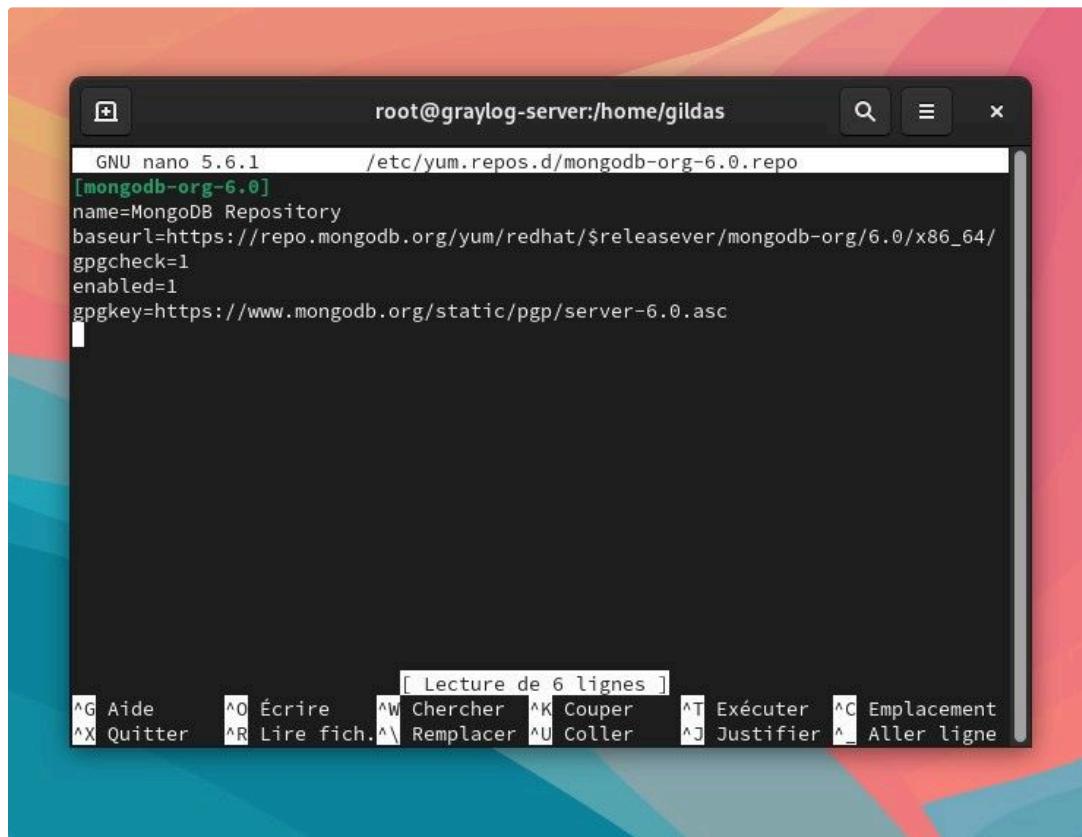
a) Ajouter le dépôt MongoDB

Créez un fichier pour le dépôt MongoDB :

```
sudo nano /etc/yum.repos.d/mongodb-org-6.0.repo
```

Ajoutez le contenu suivant :

```
[mongodb-org-6.0]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/$releasever/mongodb-org/6.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://www.mongodb.org/static/pgp/server-6.0.asc
```



The screenshot shows a terminal window titled "root@graylog-server:/home/gildas". The command "nano /etc/yum.repos.d/mongodb-org-6.0.repo" is running. The content of the file is displayed:

```
GNU nano 5.6.1      /etc/yum.repos.d/mongodb-org-6.0.repo
[mongodb-org-6.0]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/$releasever/mongodb-org/6.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://www.mongodb.org/static/pgp/server-6.0.asc
```

The terminal window has a dark background and light-colored text. At the bottom, there is a menu bar with French labels: "Aide", "Écrire", "Chercher", "Couper", "Exécuter", "Emplacement", "Quitter", "Lire fich.", "Remplacer", "Coller", "Justifier", and "Aller ligne".

i Faire **ctrl+x** pour enregistrer le fichier édité

b) Installer MongoDB

```
sudo dnf install -y mongodb-org
```

The terminal window shows the results of a package transaction. It lists 8 packages installed, totaling 132 MB download size and 567 MB installed size. The transaction summary includes the total time taken (00:13) and the MongoDB Repository status.

```
root@graylog-server:/home/gildas
mongodb-org-database x86_64 6.0.19-1.el9 mongodb-org-6.0 9.4 k
mongodb-org-database-tools-extra x86_64 6.0.19-1.el9 mongodb-org-6.0 14 k
mongodb-org-mongos x86_64 6.0.19-1.el9 mongodb-org-6.0 22 M
mongodb-org-server x86_64 6.0.19-1.el9 mongodb-org-6.0 30 M
mongodb-org-tools x86_64 6.0.19-1.el9 mongodb-org-6.0 9.3 k

Résumé de la transaction
=====
Installe 8 Paquets

Taille totale des téléchargements : 132 M
Taille des paquets installés : 567 M
Téléchargement des paquets :
(1/8): mongodb-org-6.0.19-1.el9.x86_64.rpm 64 kB/s | 9.3 kB 00:00
(2/8): mongodb-org-database-6.0.19-1.el9.x86_64 43 kB/s | 9.4 kB 00:00
(3/8): mongodb-org-database-tools-extra-6.0.19- 46 kB/s | 14 kB 00:00
(4/8): mongodb-database-tools-100.10.0-1.x86_64 3.4 MB/s | 24 MB 00:06
(5/8): mongodb-org-mongos-6.0.19-1.el9.x86_64.r 3.1 MB/s | 22 MB 00:07
(6/8): mongodb-org-tools-6.0.19-1.el9.x86_64.rp 23 kB/s | 9.3 kB 00:00
(7/8): mongodb-mongosh-2.3.8.x86_64.rpm 4.9 MB/s | 56 MB 00:11
(8/8): mongodb-org-server-6.0.19-1.el9.x86_64.r 4.8 MB/s | 30 MB 00:06

Total 9.9 MB/s | 132 MB 00:13
MongoDB Repository [ == ] --- B/s | 0 B --:-- ETA
```

c) Démarrer et activer MongoDB

```
sudo systemctl restart mongod
```

```
sudo systemctl enable mongod
```

- Vérifiez que MongoDB est opérationnel :

```
sudo systemctl status mongod
```

The terminal window shows the status of the mongod service. It indicates the service is active (running) since January 07, 2025, at 07:29:53 EST. The service is managed by the mongod.service unit, which is a MongoDB Database Server.

```
root@graylog-server:/home/gildas
mongodb-org-database-tools-extra-6.0.19-1.el9.x86_64
mongodb-org-mongos-6.0.19-1.el9.x86_64
mongodb-org-server-6.0.19-1.el9.x86_64
mongodb-org-tools-6.0.19-1.el9.x86_64

Terminé !
[root@graylog-server gildas]# sudo systemctl restart mongod
sudo systemctl enable mongod
[root@graylog-server gildas]# sudo systemctl status mongod
● mongod.service - MongoDB Database Server
   Loaded: loaded (/usr/lib/systemd/system/mongod.service; enabled; preset: d>
   Active: active (running) since Tue 2025-01-07 07:29:53 EST; 19s ago
     Docs: https://docs.mongodb.org/manual/
   Main PID: 6478 (mongod)
      Memory: 70.0M
        CPU: 933ms
       CGroup: /system.slice/mongod.service
               └─6478 /usr/bin/mongod -f /etc/mongod.conf

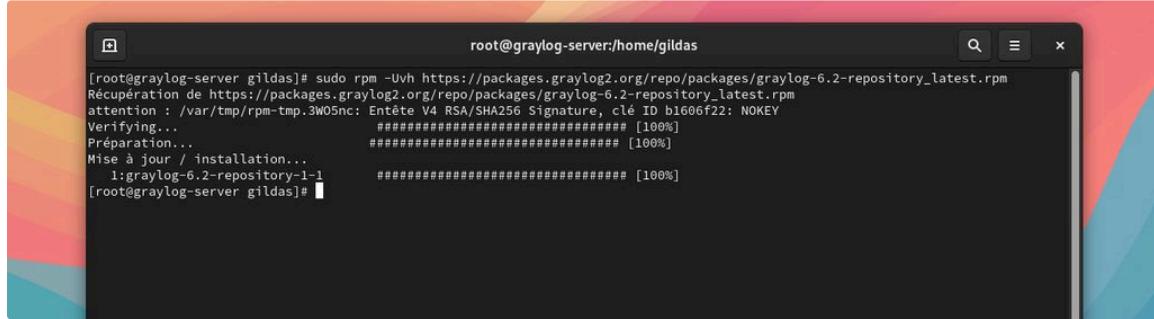
jan 07 07:29:53 graylog-server systemd[1]: Started MongoDB Database Server.
jan 07 07:29:53 graylog-server mongod[6478]: {"t":{"$date":"2025-01-07T12:29:53>

[root@graylog-server gildas]#
```

5. installation de graylog-server v6.2

a) Exécuter la commande ci-dessous pour ajouter le dépôt Graylog à votre système. La dernière version disponible du serveur Graylog est la v6.2 :

```
sudo rpm -Uvh https://packages.graylog2.org/repo/packages/graylog-6.2-repository_latest.rpm
```



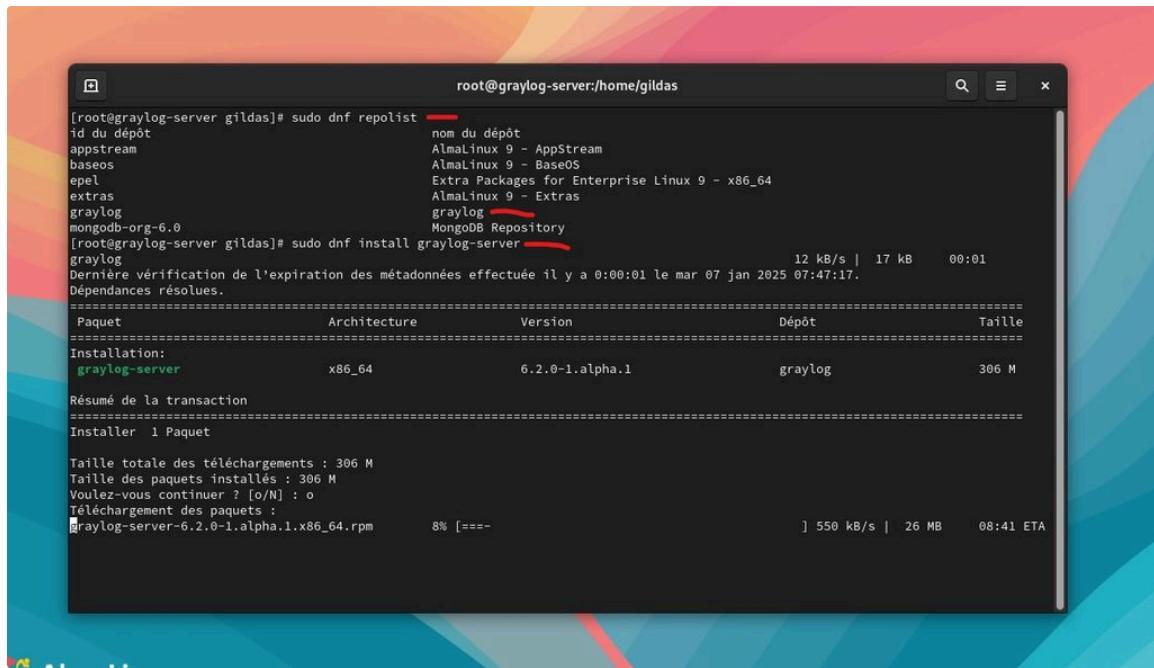
```
[root@graylog-server gildas]# sudo rpm -Uvh https://packages.graylog2.org/repo/packages/graylog-6.2-repository_latest.rpm
Récupération de https://packages.graylog2.org/repo/packages/graylog-6.2-repository_latest.rpm
attention : /var/tmp/rpm-tmp.3W05nc: Entête V4 RSA/SHA256 Signature, clé b1606f22: NOKEY
Verifier...
Préparation...
Mise à jour / installation...
  1:graylog-6.2-repository-1-1  #####
[root@graylog-server gildas]#
```

b) vérifier que le dépôt est bien présent et installer graylog-server

```
sudo dnf repolist
```

- Installer graylog-server :

```
sudo dnf install graylog-server
```



```
[root@graylog-server gildas]# sudo dnf repolist
id du dépôt
nom du dépôt
appstream AlmaLinux 9 - AppStream
baseos AlmaLinux 9 - BaseOS
epel Extra Packages for Enterprise Linux 9 - x86_64
extras AlmaLinux 9 - Extras
graylog graylog MongoDB Repository
mongodb-org-6.0 [root@graylog-server gildas]# sudo dnf install graylog-server
Dernière vérification de l'expiration des métadonnées effectuée il y a 0:00:01 le mar 07 jan 2025 07:47:17.
Dépendances résolues.
=====
Paquet Architecture Version Dépôt Taille
=====
Installation:
graylog-server x86_64 6.2.0-1.alpha.1 graylog 306 M
Résumé de la transaction
=====
Installer 1 Paquet

Taille totale des téléchargements : 306 M
Taille des paquets installés : 306 M
Voulez-vous continuer ? [o/N] : o
Téléchargement des paquets :
  graylog-server-6.2.0-1.alpha.1.x86_64.rpm      8% [====] 550 kB/s | 26 MB   08:41 ETA
```

c) configurer graylog-server

- Avec la commande `pwgen`, nous allons générer une clé chiffrée qui sera utilisée pour sécuriser les communications dans les fichiers de configuration du serveur Graylog.

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

```
[root@graylog-server gildas]# pwgen -N 1 -s 96
Y85iDMCGo1zHWe0tIw34F1qrGBqDvN7mAEZwib3r2tJ6yOGJAWXT9iN0IXeqhiWC6LK9SK2tj0W0XQhxCT9q4sh7dqFl5KN
[root@graylog-server gildas]#
```

- Copiez la clé générée, puis modifiez le fichier `/etc/graylog/server/server.conf` :

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

- Ensuite collez le mot de passe dans cette ligne :

i password_secret = <votre_clé_générée>

- Générez un mot de passe hashé pour l'utilisateur admin :

```
echo -n "VotreMotDePasseAdmin" | sha256sum
```

i Remplacez "VotreMotDePasseAdmin" par le mot de passe de votre choix pour votre administrateur.

```
[root@graylog-server gildas]# echo -n "VotreMotDePasseAdmin" | sha256sum
ba461213f9f3ca04446a6a4ad1f4108d1794a17d130d49d44dbd8b0067cb282d -
[root@graylog-server gildas]#
```

- Ajoutez le hash dans le fichier de configuration :

i root_password_sha2 = <hash_généré>

```
root@graylog-server:/home/gildas          /etc/graylog/server/server.conf      Modifié
GNU nano 5.6.1

# 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. encrypted log messages)
password_secret = Y85iDMCGo1zHWe0tIw34F1qrGBqDvN7mAEZwib3r2tJ6yOGJAWXT9iN0IXeqhiWC6LK9SK2tj0W0XQhxCT9q4sh7dqFl5KN

# 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 = ba461213f9f3ca04446a6a4ad1f4108d1794a17d130d49d44dbd8b0067cb282d

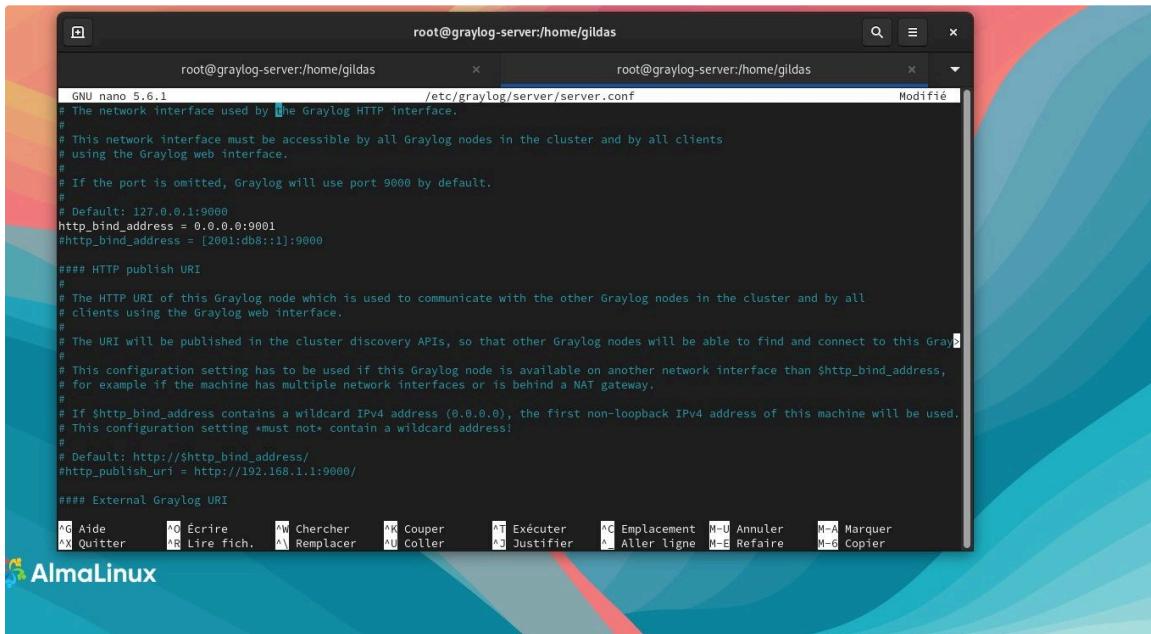
# The email address of the root user.
# Default is empty
#root_email = ""

# The time zone setting of the root user. See http://www.joda.org/joda-time/timezones.html for a list of valid time zones.
# Default is UTC
#root_timezone = UTC

# Set the bin directory here (relative or absolute)
# This directory contains binaries that are used by the Graylog server.
```

- Dans le même fichier, modifiez :

i) http_bind_address = 0.0.0.0:9001 (Le port par défaut est 9000, vous pouvez donc l'utiliser. De plus, au lieu de l'adresse IP 0.0.0.0, vous pouvez spécifier directement l'adresse IP de votre serveur.)



```
root@graylog-server:/home/gildas
GNU nano 5.6.1          /etc/graylog/server/server.conf
# 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 = 0.0.0.0:9001
$http_bind_address = [2001:db8::1]:9000

### HTTP publish URI
#
# The HTTP URI of this Graylog node which is used to communicate with the other Graylog nodes in the cluster and by all
# clients using the Graylog web interface.
#
# The URI will be published in the cluster discovery APIs, so that other Graylog nodes will be able to find and connect to this Graylog
# node.
#
# This configuration setting has to be used if this Graylog node is available on another network interface than $http_bind_address,
# for example if the machine has multiple network interfaces or is behind a NAT gateway.
#
# If $http_bind_address contains a wildcard IPv4 address (0.0.0.0), the first non-loopback IPv4 address of this machine will be used.
# This configuration setting *must not* contain a wildcard address!
#
# Default: http://$http_bind_address/
$http_publish_uri = http://192.168.1.1:9000

### External Graylog URI

```

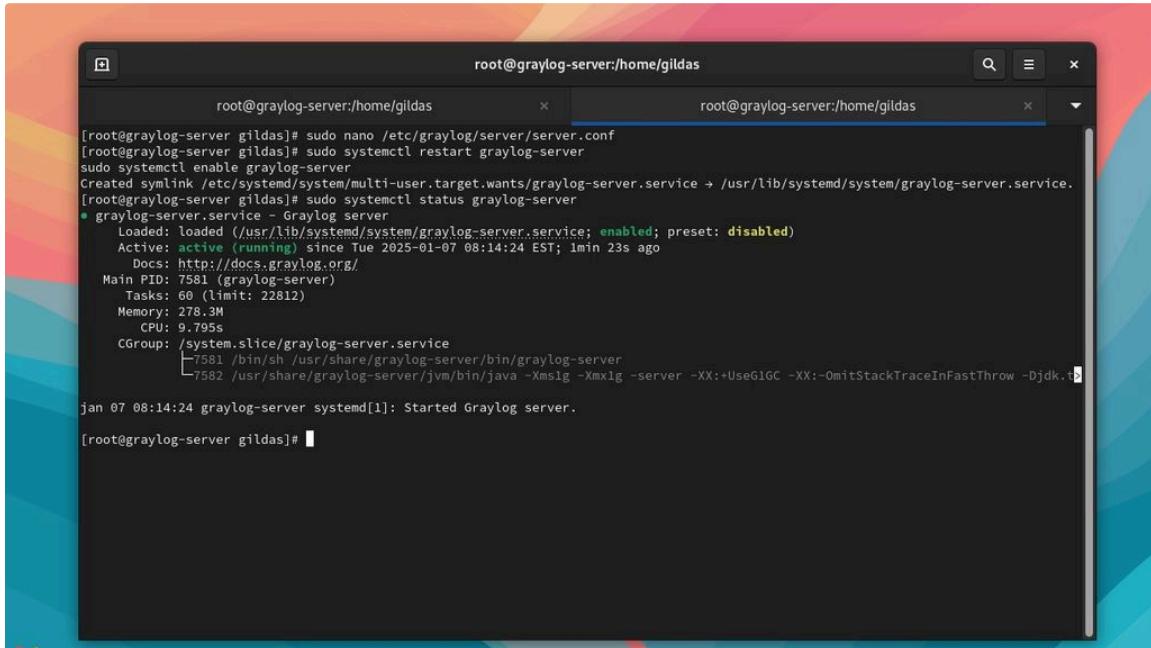
d) Activer et démarrer Graylog

```
sudo systemctl restart graylog-server
```

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

e) Vérifier le statut de Graylog

```
sudo systemctl status graylog-server
```



```
root@graylog-server:/home/gildas
root@graylog-server:gildas
[root@graylog-server gildas]# sudo nano /etc/graylog/server/server.conf
[root@graylog-server gildas]# sudo systemctl restart graylog-server
sudo systemctl enable graylog-server
Created symlink /etc/systemd/system/multi-user.target.wants/graylog-server.service → /usr/lib/systemd/system/graylog-server.service.
[root@graylog-server gildas]# sudo systemctl status graylog-server
● graylog-server.service - Graylog server
   Loaded: loaded (/usr/lib/systemd/system/graylog-server.service; enabled; preset: disabled)
   Active: active (running) since Tue 2025-01-07 08:14:24 EST; 1min 23s ago
     Docs: http://docs.graylog.org/
     Main PID: 7581 (graylog-server)
        Tasks: 60 (limit: 22812)
       Memory: 278.3M
          CPU: 9.795s
         CGroup: /system.slice/graylog-server.service
                   ├─7581 /bin/sh /usr/share/graylog-server/bin/graylog-server
                   └─7582 /usr/share/graylog-server/jvm/bin/java -Xms1g -Xmx1g -server -XX:+UseG1GC -XX:-OmitStackTraceInFastThrow -Djdk.t

jan 07 08:14:24 graylog-server systemd[1]: Started Graylog server.

[root@graylog-server gildas]#
```

[6. installation du datanode v6.2](#)

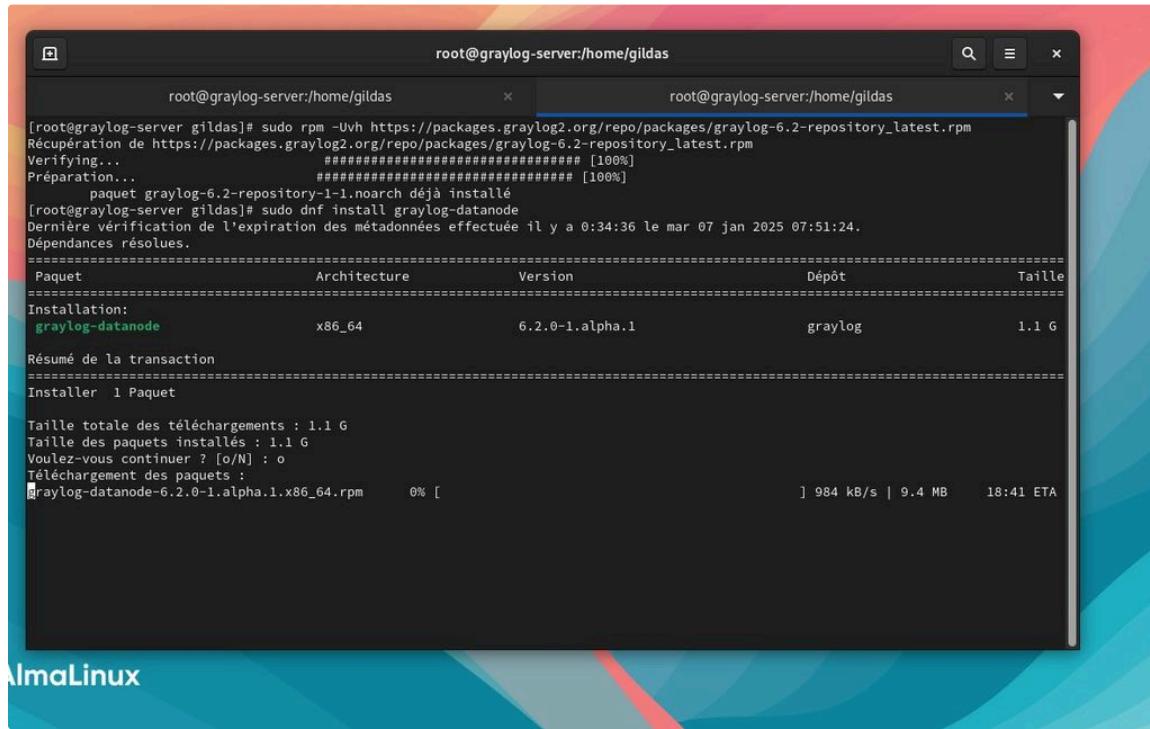
Un **datanode** dans un serveur Graylog joue un rôle essentiel dans la gestion du stockage des logs, le traitement des données, ainsi que dans l'amélioration des performances et de la disponibilité des informations.

À partir de la version 5.0 de Graylog, il est recommandé d'utiliser **datanode** comme support pour la base de données. Cette solution est plus stable et fiable pour ces versions. Pour les versions antérieures à 5.0, d'autres options comme **OpenSearch** ou **Elasticsearch** sont également compatibles et souvent privilégiées.

- **Télécharger et Installez le package Data Node v6.2**

```
sudo rpm -Uvh https://packages.graylog2.org/repo/packages/graylog-6.2-repository_latest.rpm
```

```
sudo dnf install graylog-datanode
```



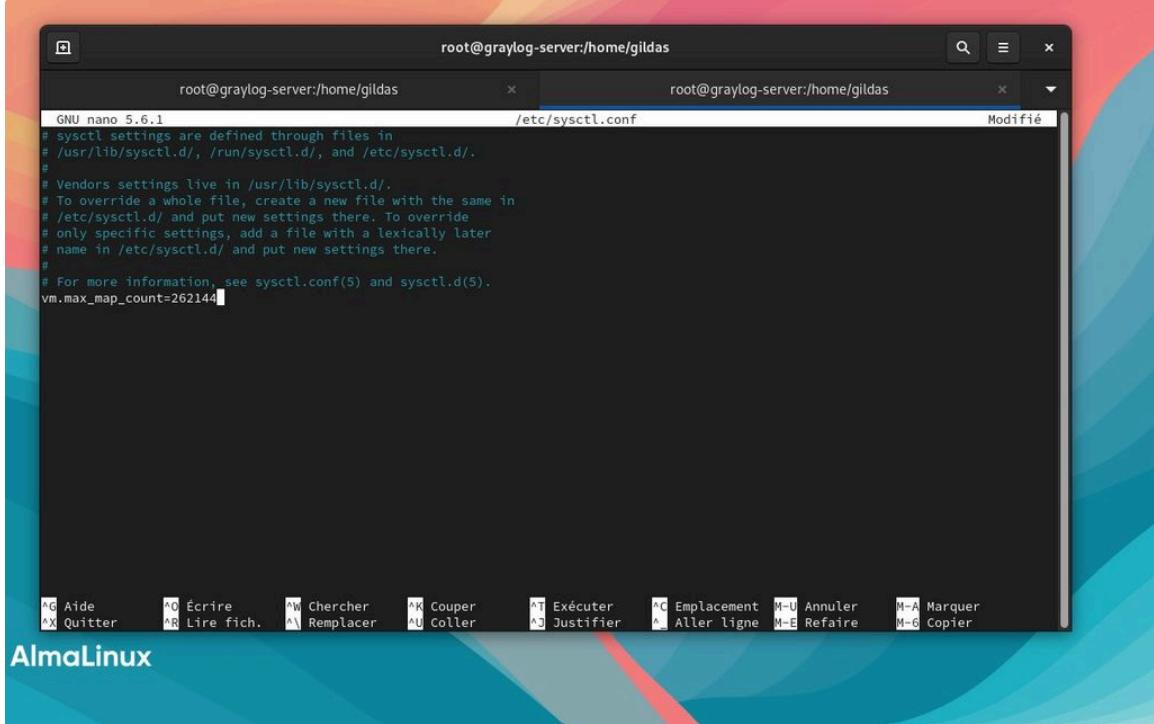
- **Vérification du paramètre Linux `vm.max_map_count`**

Vérifiez que le paramètre Linux `vm.max_map_count` est configuré à au moins 262144. Pour ce faire, exécutez la commande suivante :

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

Pour augmenter cette valeur si elle ne correspond pas aux besoins, ajoutez la ligne suivante à `nano /etc/sysctl.conf` :

```
vm.max_map_count=262144
```



Pour recharger ce paramètre de configuration, exécutez la commande suivante :

```
sudo sysctl -p
```

- **Clé secrète Datanote.**

- Accédez au fichier de configuration de Graylog Server.

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

-Ensuite copiez simplement la clé secrète existante :

password_secret = <Votre clé existante >

-configurez le fichier /etc/graylog/datanode/datanode.conf .

Mettez à jour le fichier de configuration du datanode en y ajoutant la clé copiée précédemment dans Graylog Server.

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

💡 password_secret = <Clé copiée dans le serveur Graylog.>

```
root@graylog-server:/home/gildas
GNU nano 5.6.1
/etc/graylog/datanode/datanode.conf
# * The backslash character must be escaped as a double backslash. For example:
#
# path=c:\\docs\\doc1
#
# 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 DataNode from init scripts or similar.
node_id_file = /etc/graylog/datanode/node-id

# location of your data-node configuration files - put additional files like manually created certificates etc. here
config_location = /etc/graylog/datanode

# 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 and DataNode nodes in the cluster.
# Changing this value after installation will render all user sessions and encrypted values in the database invalid. (e.g. encrypted password_secret = jXTSOLVnNLgKsJcBzgjR0gfjh36hLTks5hWT294jrQBQ6RoI0jUf6bGnND9em9HPVfPDQVegS0QgNrAxW3GExdyAs2k642)
password_secret = jXTSOLVnNLgKsJcBzgjR0gfjh36hLTks5hWT294jrQBQ6RoI0jUf6bGnND9em9HPVfPDQVegS0QgNrAxW3GExdyAs2k642

# 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 =
```

AlmaLinux

- **Démarrer et activer Graylog-DataNode.**

```
sudo systemctl enable graylog-datanode.service
sudo systemctl restart graylog-datanode
```

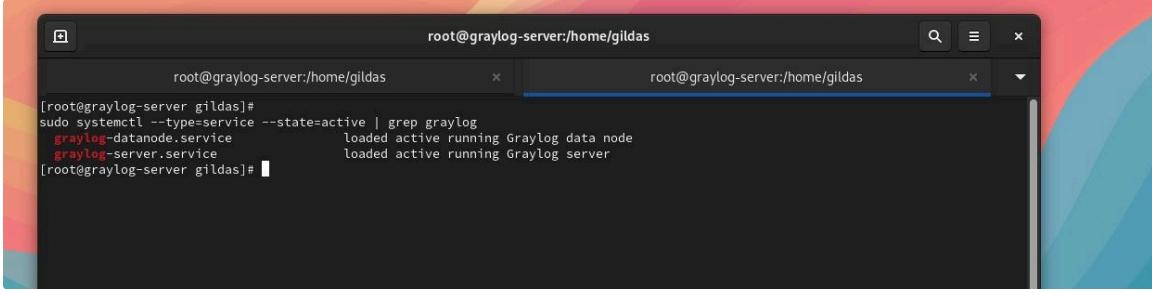
- **Vérifier le statut**

```
sudo systemctl restart graylog-datanode
sudo systemctl status graylog-datanode
```

```
root@graylog-server:/home/gildas
root@graylog-server:gildas
[root@graylog-server gildas]# sudo nano /etc/graylog/datanode/datanode.conf
[root@graylog-server gildas]# sudo systemctl enable graylog-datanode.service
sudo systemctl start graylog-datanode
Created symlink /etc/systemd/system/multi-user.target.wants/graylog-datanode.service → /usr/lib/systemd/system/graylog-datanode.service.
[root@graylog-server gildas]# sudo systemctl status graylog-datanode
● graylog-datanode.service - Graylog data node
   Loaded: loaded (/usr/lib/systemd/system/graylog-datanode.service; enabled; preset: disabled)
   Active: active (running) since Tue 2025-01-07 09:10:47 EST; 11s ago
     Docs: http://docs.graylog.org/
     Main PID: 8008 (java)
        Tasks: 52 (limit: 22812)
       Memory: 521.7M
          CPU: 14.249s
         CGroup: /system.slice/graylog-datanode.service
             └─8008 /usr/share/graylog-datanode/jvm/bin/java -Dlog4j.configurationFile=file:///etc/graylog/datanode/log4j2.xml -Xms1g
jan 07 09:10:47 graylog-server systemd[1]: Started Graylog data node.
[root@graylog-server gildas]#
```

Vérifiez que les deux services sont bien présents et fonctionnent correctement.

```
sudo systemctl --type=service --state=active | grep graylog
```



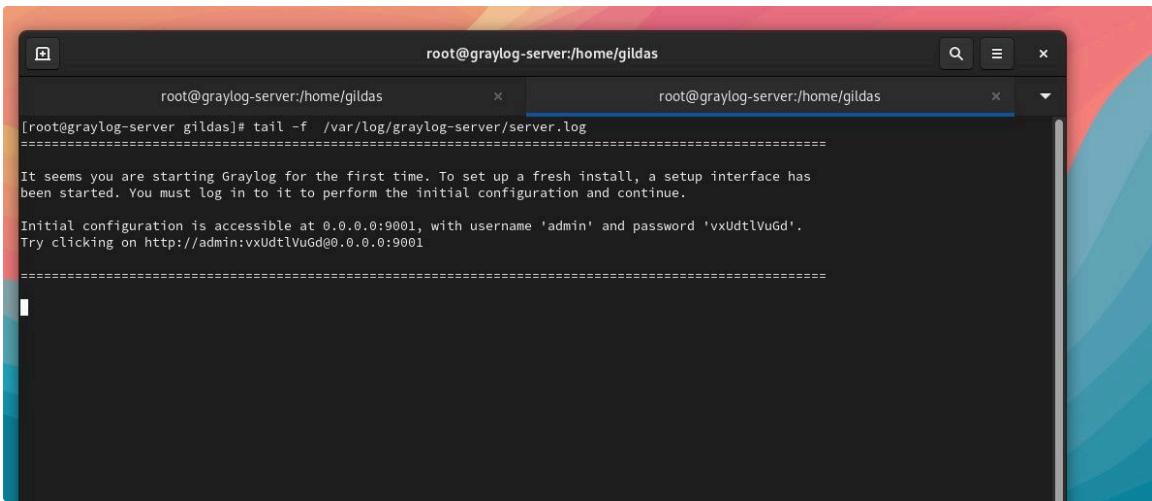
```
root@graylog-server:/home/gildas
[root@graylog-server gildas]# sudo systemctl --type=service --state=active | grep graylog
graylog-datanode.service          loaded active running Graylog data node
graylog-server.service            loaded active running Graylog server
[root@graylog-server gildas]#
```

7. Première connexion à l'interface graphique Graylog ↗

Lors de la première connexion à l'interface graphique, Graylog génère un mot de passe temporaire. Après cette connexion initiale, vous pourrez utiliser le mot de passe administrateur que vous avez configuré.

Le mot de passe temporaire est généralement disponible dans les fichiers logs de Graylog. Pour l'afficher, utilisez la commande suivante

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



```
root@graylog-server:/home/gildas
root@graylog-server:/home/gildas
[root@graylog-server gildas]# 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 0.0.0.0:9001, with username 'admin' and password 'vxUdtlVuGd'.
Try clicking on http://admin:vxUdtlVuGd@0.0.0.0:9001
=====
```

- Finaliser la configuration via l'interface web ↗

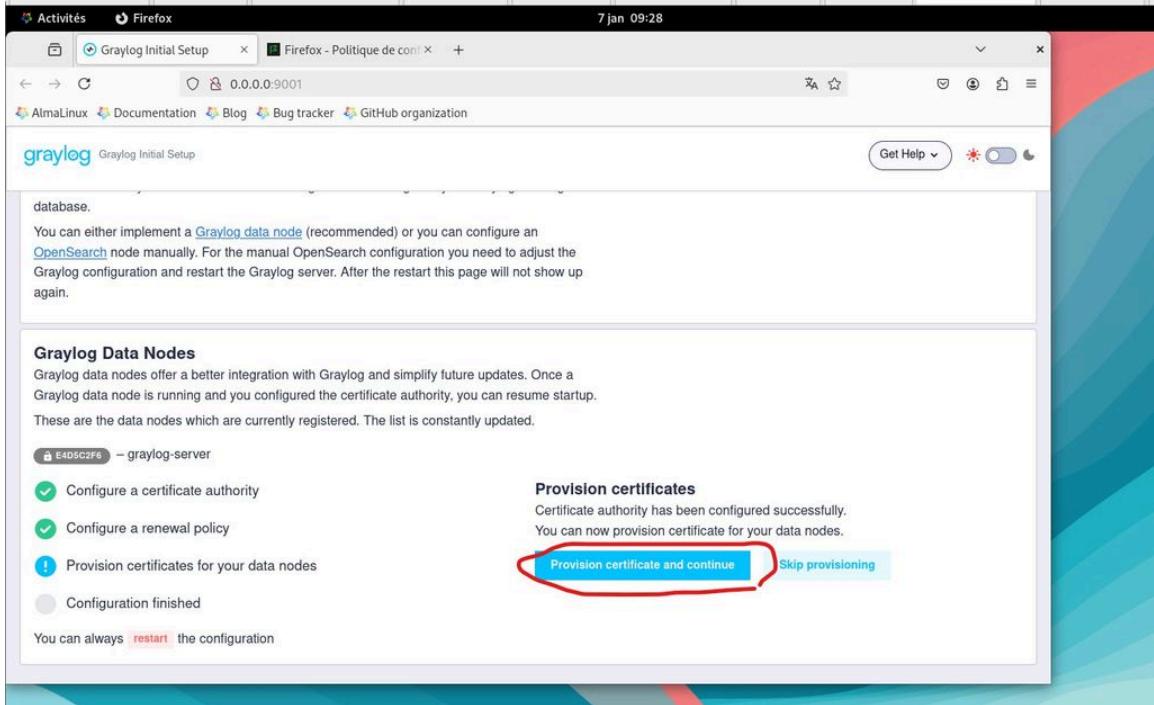
- ⓘ Créer un certificat pour le datanode

The screenshot shows the 'Configure Certificate Authority' section of the Graylog Initial Setup. It includes a list of steps: 'Configure a certificate authority' (marked with a green checkmark), 'Configure a renewal policy' (unchecked), 'Provision certificates for your data nodes' (unchecked), and 'Configuration finished' (unchecked). Below this, a note says 'You can always [restart](#) the configuration'. To the right, there's a 'Configure Certificate Authority' panel with a 'Create new CA' tab selected. It contains fields for 'Organization Name' (set to 'Graylog CA') and a 'Create CA' button, which is circled in red.

ⓘ Définir une politique de renouvellement des certificats dépend de vos besoins. Par défaut, le renouvellement automatique se produit tous les 30 jours.

The screenshot shows the 'Configure Renewal Policy' section of the Graylog Initial Setup. It includes a list of steps: 'Configure a certificate authority' (marked with a green checkmark), 'Configure a renewal policy' (unchecked), 'Provision certificates for your data nodes' (unchecked), and 'Configuration finished' (unchecked). Below this, a note says 'You can always [restart](#) the configuration'. To the right, there's a 'Configure Renewal Policy' panel with a 'Renewal Policy' dropdown set to 'Automatic' and a 'Certificate lifetime' input field containing '30' with a dropdown menu for 'Day(s)'. A 'Create policy' button is circled in red.

ⓘ Attribuer le certificat à notre **datanode est une étape cruciale et obligatoire pour assurer le bon fonctionnement du serveur. Ce processus peut prendre quelques minutes, donc **patiemment** attendez que toutes les étapes de configuration soient terminées avant de continuer.**



Bienvenue sur l'interface de Graylog !

A screenshot of the Graylog main interface. At the top, there's a navigation bar with links for Search, Streams, Alerts, Dashboards, Enterprise, Security, and System. A notification badge '1' is visible on the System icon. Below the navigation, a 'Welcome to Graylog!' message says 'This is your personal page, allowing easy access to the content most relevant for you.' Under 'Last Opened', it says 'You have not opened any searches/dashboards yet.' A note says '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.' In the 'Recent Activity' section, it says 'There is no recent activity yet.' A note says 'Whenever any other user will update content you have access to, or share new content with you, it will show up here.'

V - Conclusion ↗

Votre serveur Graylog est opérationnel sous AlmaLinux ! Profitez pleinement de ses fonctionnalités pour centraliser, indexer et analyser vos journaux via une interface intuitive et unique. Cette centralisation est essentielle pour une surveillance efficace et une gestion optimale des incidents, assurant ainsi le suivi des performances système et une identification rapide des problèmes.

Les sections suivantes détaillent la configuration et l'envoi des journaux de vos machines Linux et serveurs Windows vers votre serveur Graylog. Cette étape garantit l'acheminement correct de toutes vos données de journalisation, offrant une vue d'ensemble complète 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)