Avril 2026

Procédure
Graylog

BELLIOT Anne-Juliette

Sommaire

Pré-requis

Pour l'installation de Graylog, il est recommandé d'utiliser une machine sous Linux, telle que Debian ou Ubuntu.

Tout d'abord, nous devons paramétrer la carte réseau de notre machine.

Ici par exemple, notre adresse ip sera 192.168.22.1, avec un masque en /24, la passerelle est 192.168.22.254 et l'adresse du serveur DNS et 192.168.10.1

```
  GNU nano 8.4                                /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens192
iface ens192 inet static
        address 192.168.22.1
        netmask 255.255.255.0
        gateway 192.168.22.254
        # dns-* options are implemented by the resolvconf package, if installed
        dns-nameservers 192.168.10.1
```

Installation

L'installation se décompose en plusieurs parties :
-MongoDB pour la base de données
-Graylog Datanode, basé sur Opensearch, un moteur de recherche pour les données
-Graylog, le serveur principal pour recevoir, traiter et visualiser les données

Avant d'installer nos composants, nous pouvons mettre à jour notre machine.

```
root@srv-logs:~# apt update -y && apt upgrade -y
Atteint : 1 http://deb.debian.org/debian trixie InRelease
Réception de : 2 http://security.debian.org/debian-securi
Réception de : 3 http://deb.debian.org/debian trixie-upda
Réception de : 4 http://security.debian.org/debian-securi
Réception de : 5 http://security.debian.org/debian-securi
Réception de : 6 http://security.debian.org/debian-securi
406 ko réceptionnés en 0s (1 498 ko/s)
```

MongoDB

Nous allons commencer par l'installation de MongoDB. Tout d'abord, il faut installer les paquets gnupg et curl qui seront utiles par la suite.

```
root@srv-logs:~# apt install gnupg curl
```

Ensuite, nous effectuons cette commande afin d'importer la clé publique de MongoDB.

```
root@srv-logs:~# curl -fsSL https://www.mongodb.org/static/pgp/server-8.0.asc
 | gpg --dearmor -o /usr/share/keyrings/mongodb-server-8.0.gpg
```

Puis cette commande afin de créer un fichier de liste APT pour MongoDB, afin que le système sache où télécharger les paquets.

```
root@srv-logs:~# echo "deb [ signed-by=/usr/share/keyrings/mongodb-server-8.
0.gpg ] http://repo.mongodb.org/apt/debian bookworm/mongodb-org/8.0 main" |
tee /etc/apt/sources.list.d/mongodb-org-8.0.list
```

Nous pouvons alors installer le paquet MongoDB.

```
root@srv-logs:~# apt install mongodb-org -y
Installation de :
  mongodb-org

Installation de dépendances :
  mongodb-database-tools            mongodb-org-mongos
  mongodb-mongosh                   mongodb-org-server
  mongodb-org-database              mongodb-org-shell
  mongodb-org-database-tools-extra  mongodb-org-tools
```

Ensuite, nous faisons cette commande pour empêcher la mise à jour automatique de MongoDB. Cela pourrait en effet créer d'éventuels problèmes de compatibilité avec Graylog.

```
root@srv-logs:~# apt-mark hold mongodb-org
mongodb-org passé en figé (« hold »).
```

Pour finir, nous allons modifier la valeur de bindIp dans le fichier de configuration de MongoDB. Ainsi, ce dernier écoutera sur toutes les interfaces. Nous pouvons aussi mettre une adresse ip spécifique ou le nom d'une machine si le service devra écouter sur seulement une interface.

```
  GNU nano 8.4                    /etc/mongod.conf
  logAppend: true
  path: /var/log/mongodb/mongod.log

# network interfaces
net:
  port: 27017
  bindIp: 0.0.0.0
```

Nous pouvons, enfin, démarrer le service MongoDB.

```
root@srv-logs:~# systemctl daemon-reload
root@srv-logs:~# systemctl enable mongod.service
Created symlink '/etc/systemd/system/multi-user.target.wants/mongod.service'
 → '/usr/lib/systemd/system/mongod.service'.
root@srv-logs:~# systemctl start mongod.service
```

Graylog Data Node

Nous allons désormais passer à l'installation du Data Node. Ce dernier est un composant de Graylog qui gère le traitement et l'indexation des logs, en communiquant avec OpenSearch pour le stockage et les recherches.

Tout d'abord, nous téléchargeons le paquet Data Node à l'aide de ces deux commandes.

```
root@srv-logs:~# wget https://packages.graylog2.org/repo/packages/graylog-7.
0-repository_latest.deb
```

```
root@srv-logs:~# dpkg -i graylog-7.0-repository_latest.deb
```

Nous mettons à jour tous les paquets.

```
root@srv-logs:~# apt update
```

Et nous pouvons ensuite installer le Data Node de Graylog.

```
root@srv-logs:~# apt-get install graylog-datanode
```

Nous devons vérifier grâce à cette commande si la valeur du vm.max_map_count est supérieure ou égale à 262144.

```
root@srv-logs:~# cat /proc/sys/vm/max_map_count
1048576
```

Ici tout est bon. Si ce n'est pas le cas, il est possible de modifier cela grâce à cette commande.

```
root@srv-logs:~# echo 'vm.max_map_count=262144' | tee -a /etc/sysctl.d/99-graylog-datanode.conf
sysctl --system
```

Nous devons ensuite créer un mot de passe à l'aide de cette commande. Cela renvoie une chaîne de caractères aléatoire utilisée par Graylog pour chiffrer les informations sensibles du système.

```
root@srv-logs:~# openssl rand -hex 32
82e649c3f976d4965420434f7be737ea4ca17511df25782c201ad538f003ca39
```

Ce mot de passe doit être indiqué dans le fichier de configuration du Data Node.

Il est important de le garder aussi de côté car il sera par la suite à inscrire dans le fichier de configuration de Graylog.

```
  GNU nano 8.4   /etc/graylog/datanode/datanode.conf
# You MUST set a secret to secure/pepper the stored user passwo>
# Generate one by using for example: pwgen -N 1 -s 96
# ATTENTION: This value must be the same on all Graylog and Dat>
# Changing this value after installation will render all user s>
password_secret = 82e649c3f976d4965420434f7be737ea4ca17511df257>
```

Il faut ensuite ajouter une ligne qui définit la mémoire maximale utilisée par OpenSearch dans le Data Node, qui est généralement la moitié de la mémoire RAM du système.
Par exemple, si la machine a 8 GB de RAM, il faut mettre 4 GB.

```
opensearch_heap = 4g
```

Nous devons également modifier cette ligne pour la connexion avec la base de données.

```
mongodb_uri = mongodb://127.0.0.1:27017/graylog
```

L'ip 127.0.0.1 signifie que notre MongoDB est sur le même serveur, en localhost. C'est possible de mettre une autre ip si le service est sur une machine distante.

Enfin, nous pouvons redémarrer le service pour prendre en compte les changements.

```
root@srv-logs:~# systemctl daemon-reload
root@srv-logs:~# systemctl enable graylog-datanode.service
Created symlink '/etc/systemd/system/multi-user.target.wants/graylog-data
node.service' → '/usr/lib/systemd/system/graylog-datanode.service'.
root@srv-logs:~# systemctl start graylog-datanode.service
```

Graylog

Nous allons maintenant passer à l'installation de Graylog.

Tout d'abord, nous allons installer le paquet avec cette commande.

```
root@srv-logs:~# apt install graylog-server
Installation de :
  graylog-server
```

Ensuite, nous devons créer un mot de passe pour le compte administrateur de Graylog.
Pour effectuer cela, nous allons utiliser cette commande. Elle nous demande de rentrer le mot de passe, puis nous donne sa valeur chiffrée, afin que le mot de passe n'apparaisse pas en clair dans le fichier de configuration.

```
root@srv-logs:~# echo -n "Enter Password: " && head -1 </dev/stdin |
 tr -d '\n' | sha256sum | cut -d" " -f1
```

Voici la sortie de la commande :

```
Enter Password: graylog
4bbdd5a829dba09d7a7ff4c1367be7d36a017b4267d728d31bd264f63debeaa6
```

Nous pouvons désormais aller dans le fichier de configuration et rentrer cette valeur après root_password_sha2.
Nous allons également récupérer la valeur créée plus tôt, lors de l'installation du Data Node Graylog, que nous avons mise dans password_secret dans le fichier de configuration du Data Node.
Il faut la mettre également dans le paramètre password_secret du fichier de configuration de Graylog.

```
  GNU nano 8.4     /etc/graylog/server/server.conf
# ATTENTION: This value must be the same on all Graylog nodes in>
# Changing this value after installation will render all user se>
password_secret = 82e649c3f976d4965420434f7be737ea4ca17511df2578>

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

# You MUST specify a hash password for the root user (which you >
# system and in case you lose connectivity to your authenticatio>
# This password cannot be changed using the API or via the web i>
# modify it in this file.
# Create one by using for example: echo -n yourpassword | sha256>
# and put the resulting hash value into the following line
root_password_sha2 = 4bbdd5a829dba09d7a7ff4c1367be7d36a017b4267d>
```

Toujours dans le même fichier, nous pouvons définir la bind-address en 0.0.0.0:9000. Cela signifie que le serveur écoutera sur toutes les interfaces réseau sur le port 9000. De plus, c'est avec l'ip du serveur et ce numéro de port qu'on aura accès à l'interface web.

```
http_bind_address = 0.0.0.0:9000
```

Ensuite, nous modifions ces paramètres afin de définir la durée maximale de conservation ainsi que la taille maximale du journal de messages de Graylog, qui sert de stockage temporaire des logs avant leur traitement et leur indexation dans le Data Node.
Par exemple, nous pouvons mettre ces valeurs.

```
message_journal_max_age = 72h
message_journal_max_size = 30gb
```

Pour finir, nous allons modifier un paramètre dans le fichier graylog-server afin de définir la mémoire minimale et maximale allouée au serveur Graylog, généralement fixée à la moitié de la RAM du système. Il est recommandé de mettre la même valeur pour les deux afin d'optimiser les performances. Par exemple, si nous avons 8 giga de mémoire, les valeurs seront 4 et 4.

```
  GNU nano 8.4       /etc/default/graylog-server
# Path to a custom java executable. By default the java executab>
# bundled JVM is used.
#JAVA=/usr/bin/java

# Default Java options for heap and garbage collection.
GRAYLOG_SERVER_JAVA_OPTS="-Xms4g -Xmx4g -server -XX:+UseG1GC -XX>
```

Nous démarrons le service et l'installation est désormais terminée.

```
root@srv-logs:~# systemctl daemon-reload
root@srv-logs:~# systemctl enable graylog-server.service
Created symlink '/etc/systemd/system/multi-user.target.wants/gray
log-server.service' → '/usr/lib/systemd/system/graylog-server.ser
vice'.
root@srv-logs:~# systemctl start graylog-server.service
```

Configuration

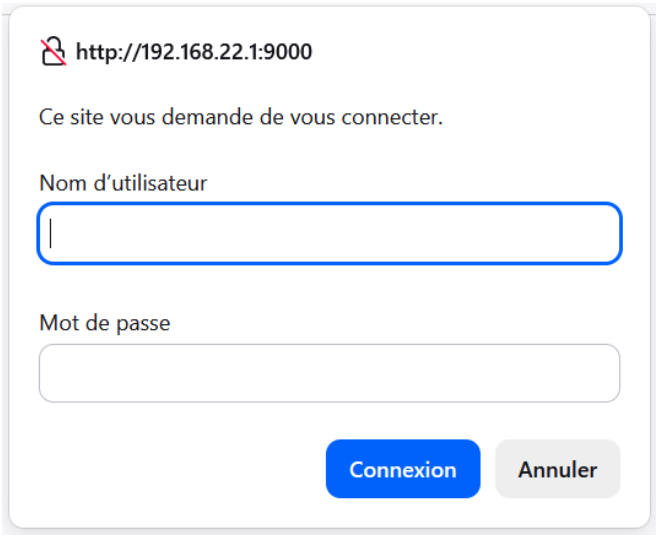
Nous allons passer désormais à la configuration de Graylog, à partir de son interface web.

Accès interface web

Pour pouvoir accéder pour la première fois à l'interface web de notre serveur Graylog, nous devons rentrer dans notre navigateur l'ip du serveur ainsi que le port. Par exemple, si l'ip est 192.168.22.1, la recherche sera celle-ci.

http://192.168.22.1:9000

Ensuite, un nom d'utilisateur et un mot de passe seront demandés.

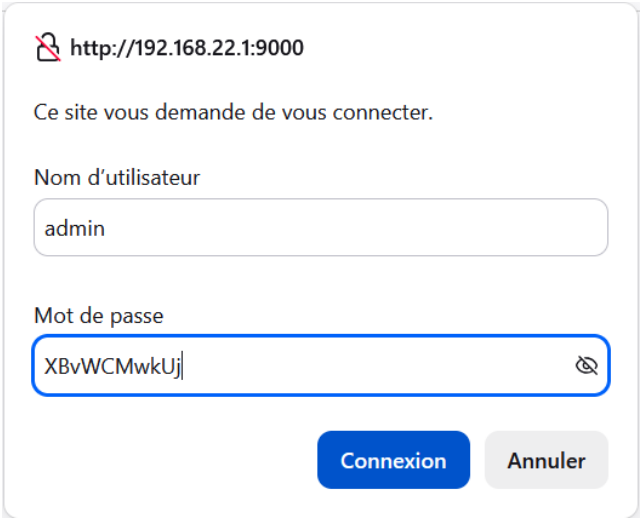


Il ne faut pas mettre le mot de passe créé lors de l'installation de Graylog, mais un mot de passe temporaire qu'on trouve dans notre machine à l'aide de cette commande.

```
root@srv-logs:~# tail /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 'XBvWCMwkUj'.
Try clicking on http://admin:XBvWCMwkUj@0.0.0.0:9000

================================================================================================================
```

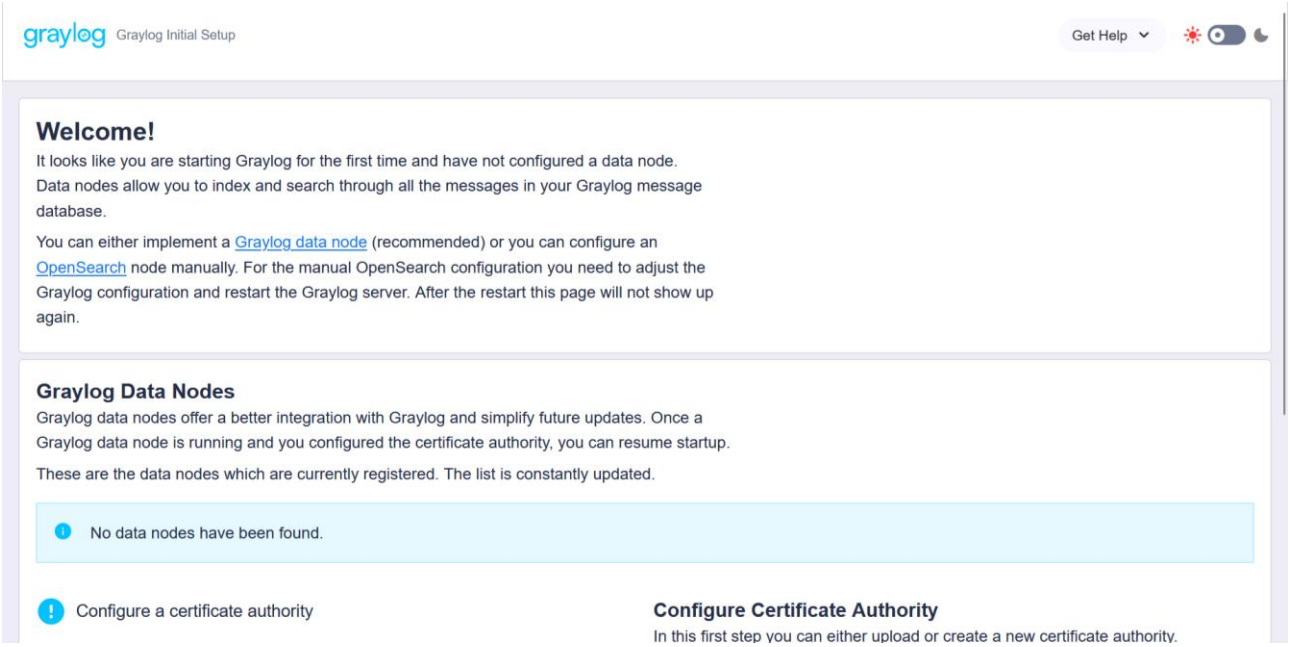
Ici, nous pouvons voir que le login est admin et le mot de passe est XBvWCMwkUj.

Nous pouvons alors rentrer ces informations.

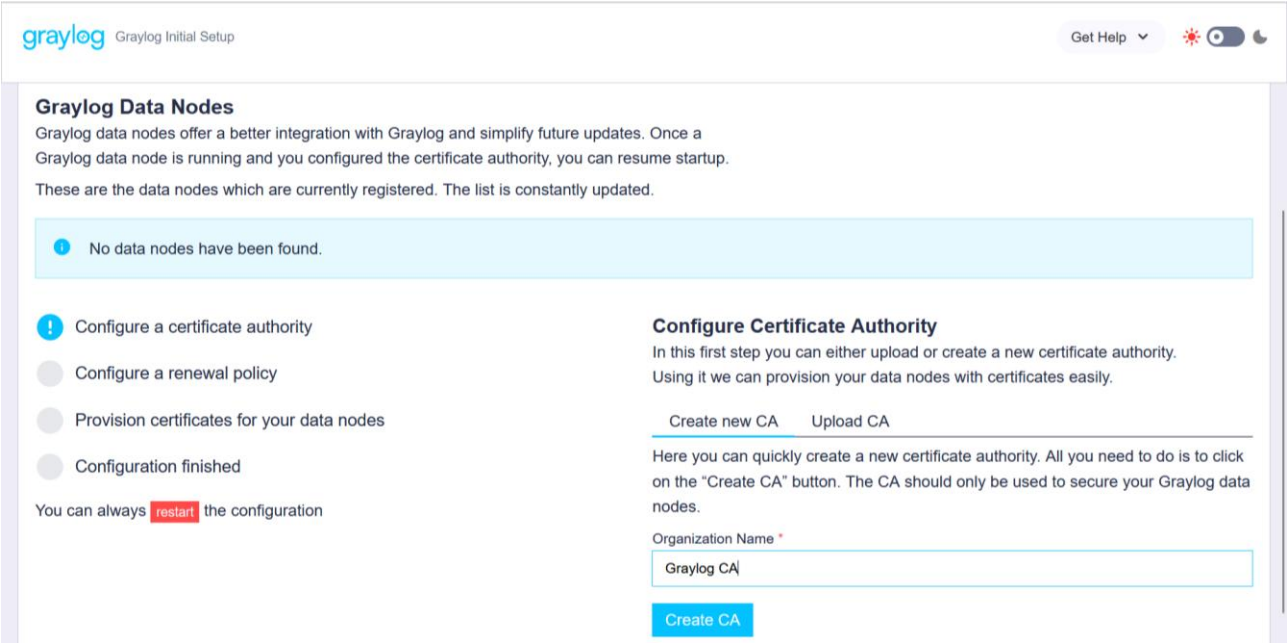


L'interface web sera alors accessible.

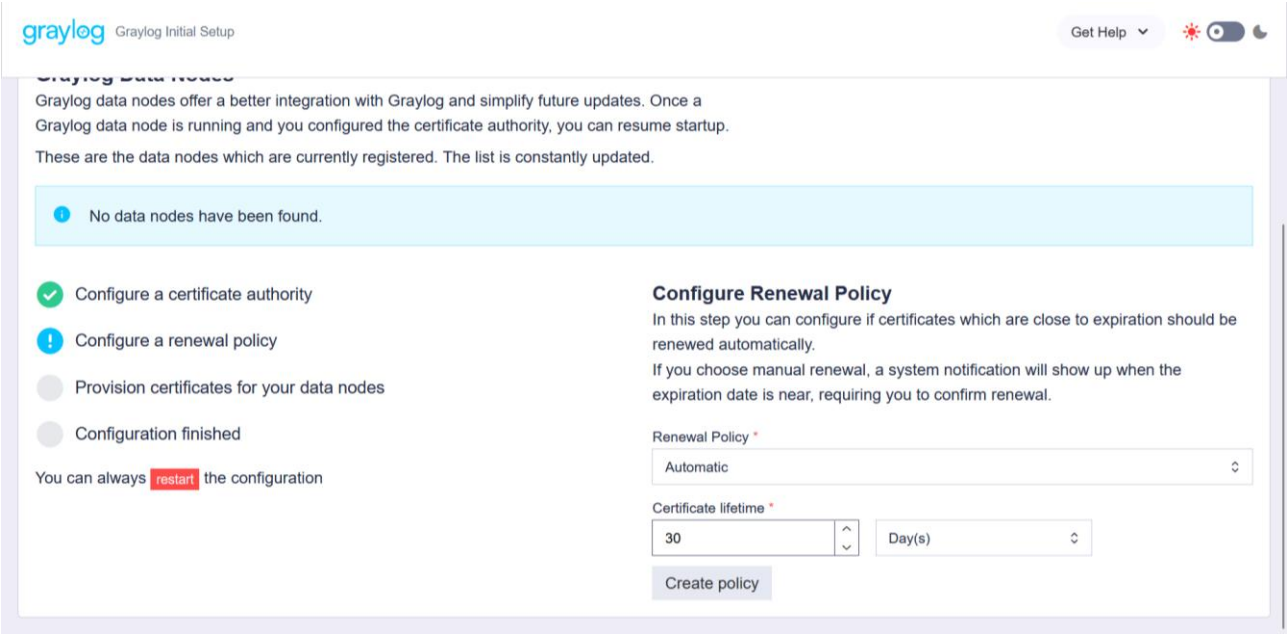
Lors de la première connexion à l'interface web, il est demandé de créer une autorité de certification. Cette dernière permettra ensuite à Graylog reconnaître le Data Node installé auparavant.



Il est possible de garder le nom par défaut ou bien de le changer.

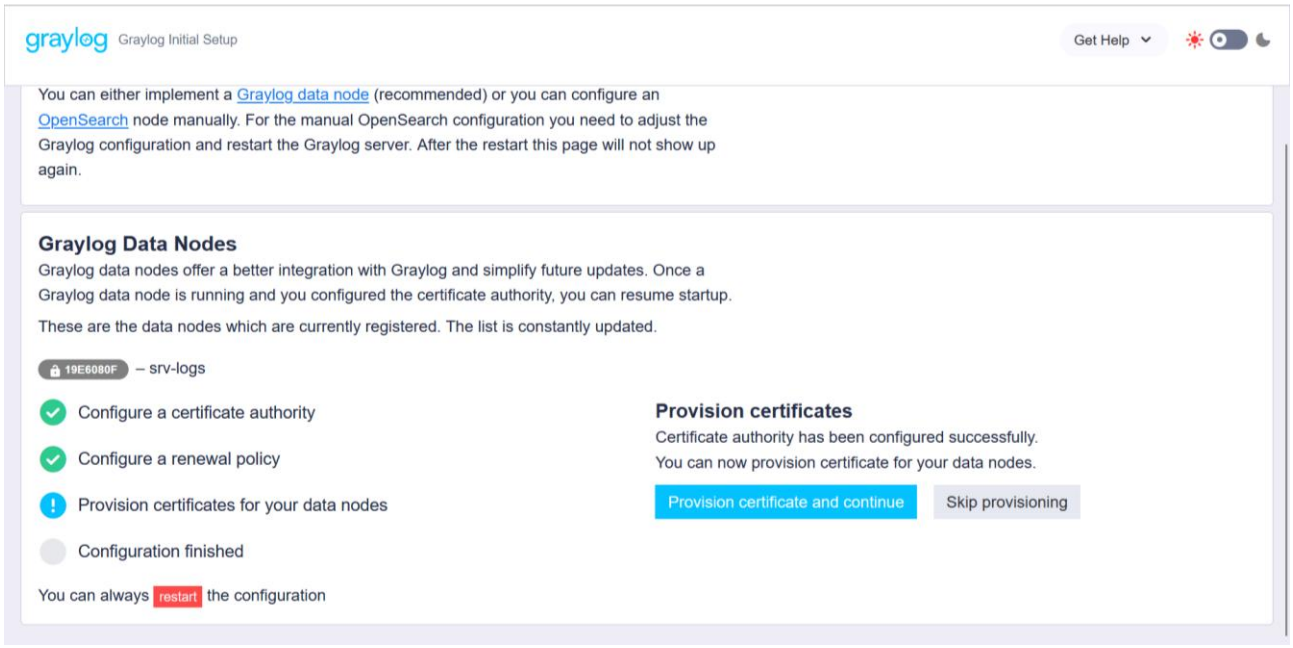


Ensuite, il faut définir quand les certificats doivent être renouvelés. Cela pourra être effectué automatiquement ou bien manuellement. Ici, 30 jours est la valeur par défaut.

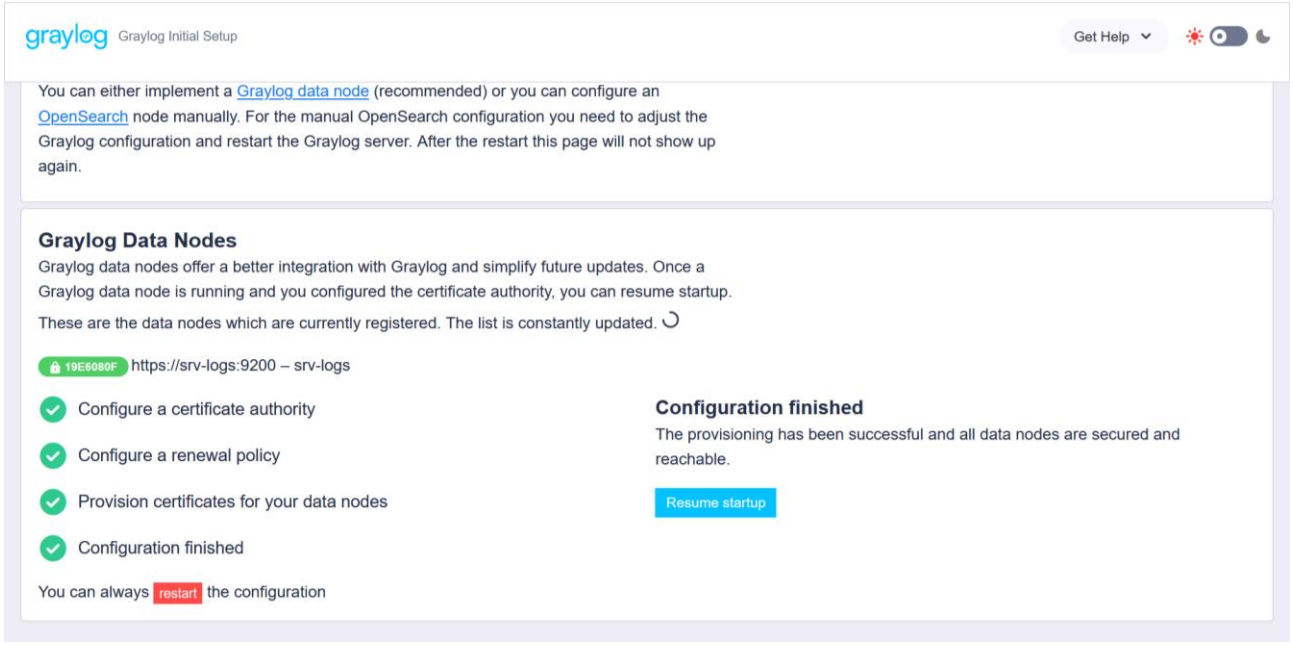


L'étape suivante consiste à provisionner un certificat pour le Data Node afin de sécuriser les communications avec Graylog.

Il suffit juste d'appuyer sur le bouton pour provisionner le certificat et continuer à la prochaine étape.

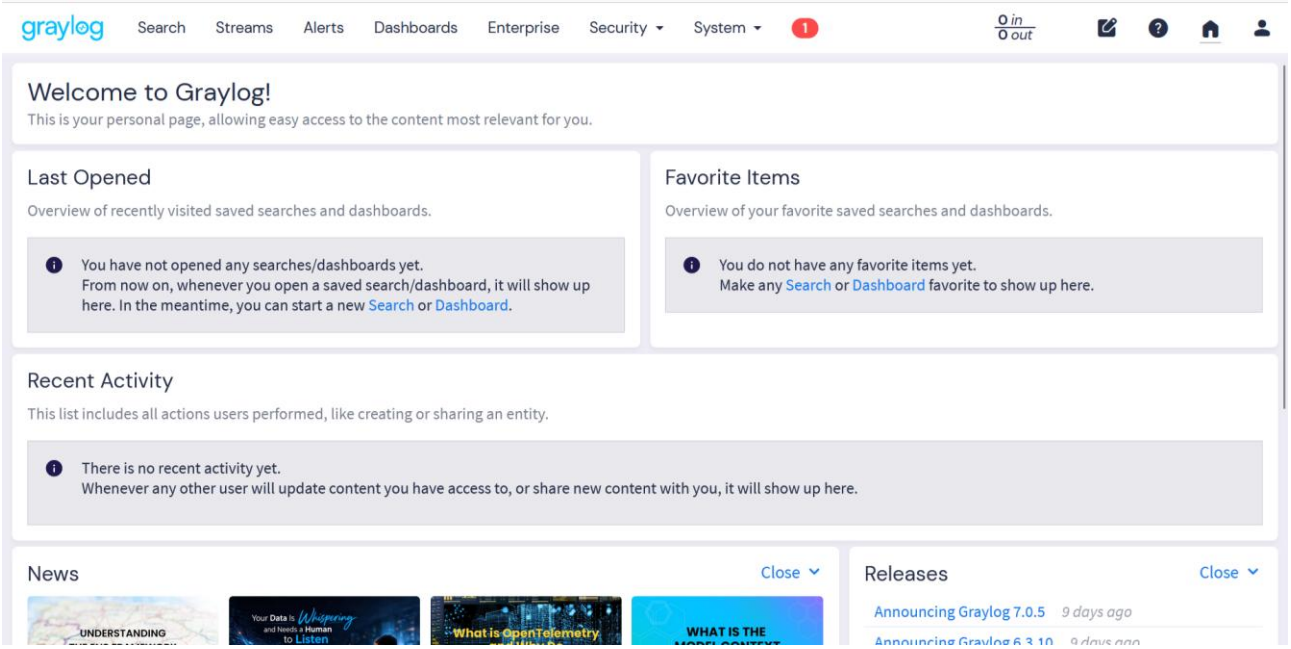


La configuration est terminée. Il n'y a plus qu'à rafraîchir la page pour aller sur la page de connexion.



Une fois sur la page de connexion, il faut spécifier non pas le mot de passe temporaire pour la première connexion mais le mot de passe qui a été configuré lors de l'installation de Graylog.

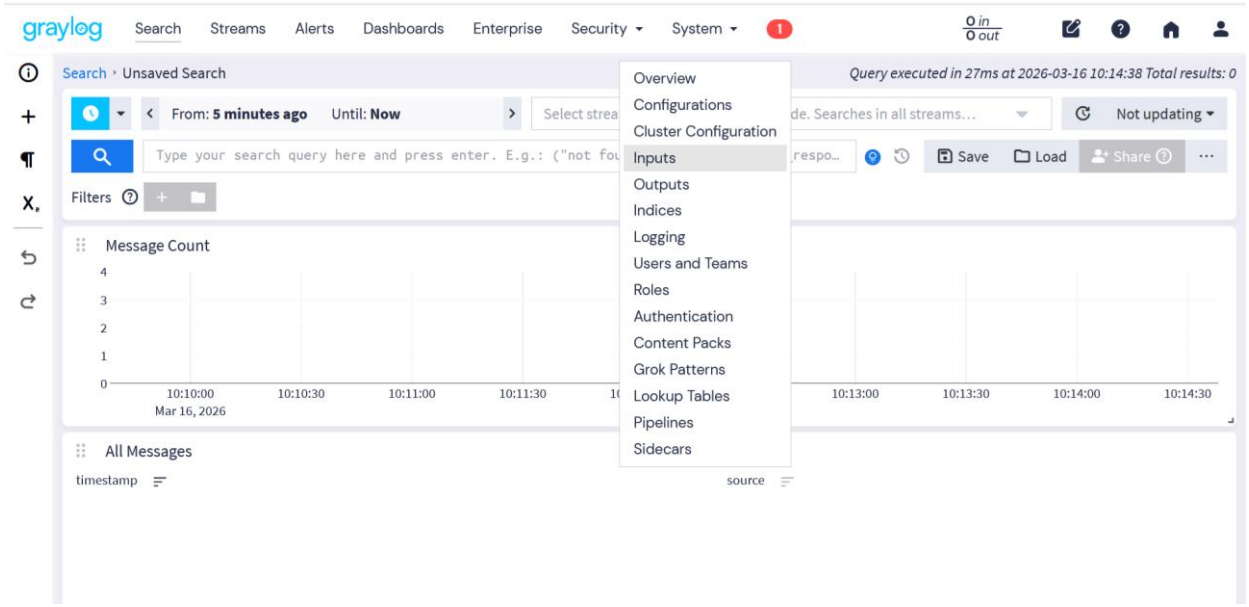
Nous arrivons alors sur la page principale de notre Graylog, que nous allons pouvoir configurer



Création d'inputs

Un Input est le point d'entrée des logs dans Graylog. Il sert à recevoir les messages envoyés par des sources externes, par exemple un serveur, une application ou un équipement réseau. Un input peut utiliser différents protocoles, comme Syslog ou encore GELF.

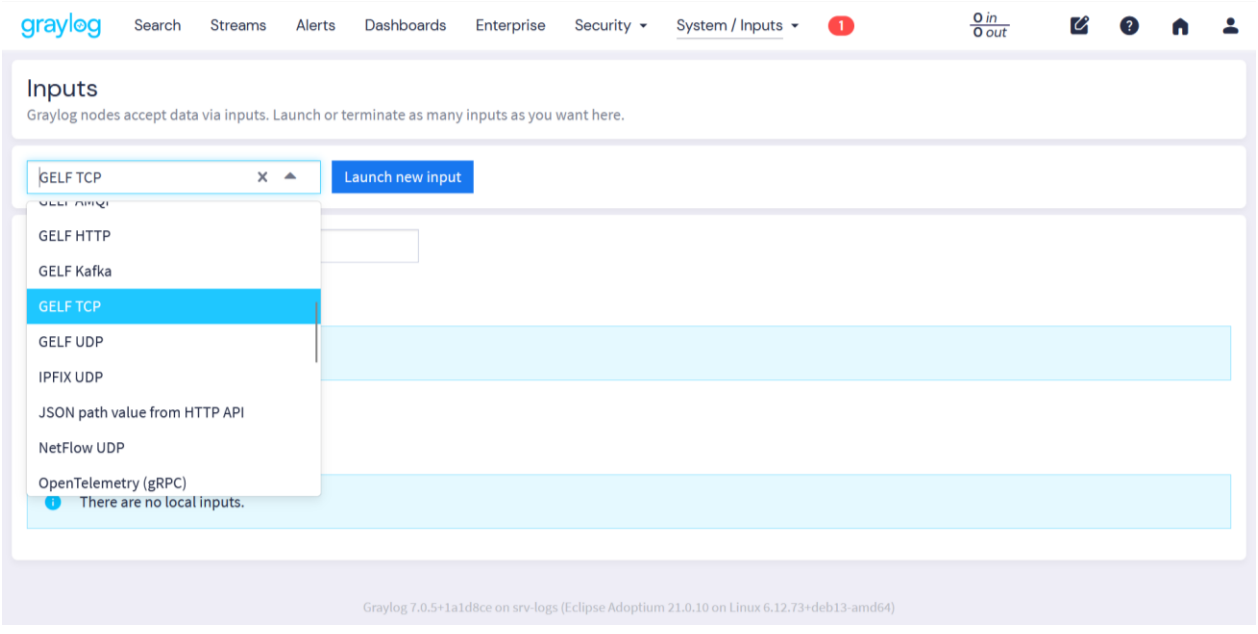
Pour créer un input, il faut tout d'abord aller dans System dans la barre de navigation, puis appuyer sur Inputs.



Ensuite, la création de l'input diffère selon le type de machine qui va envoyer ses logs.

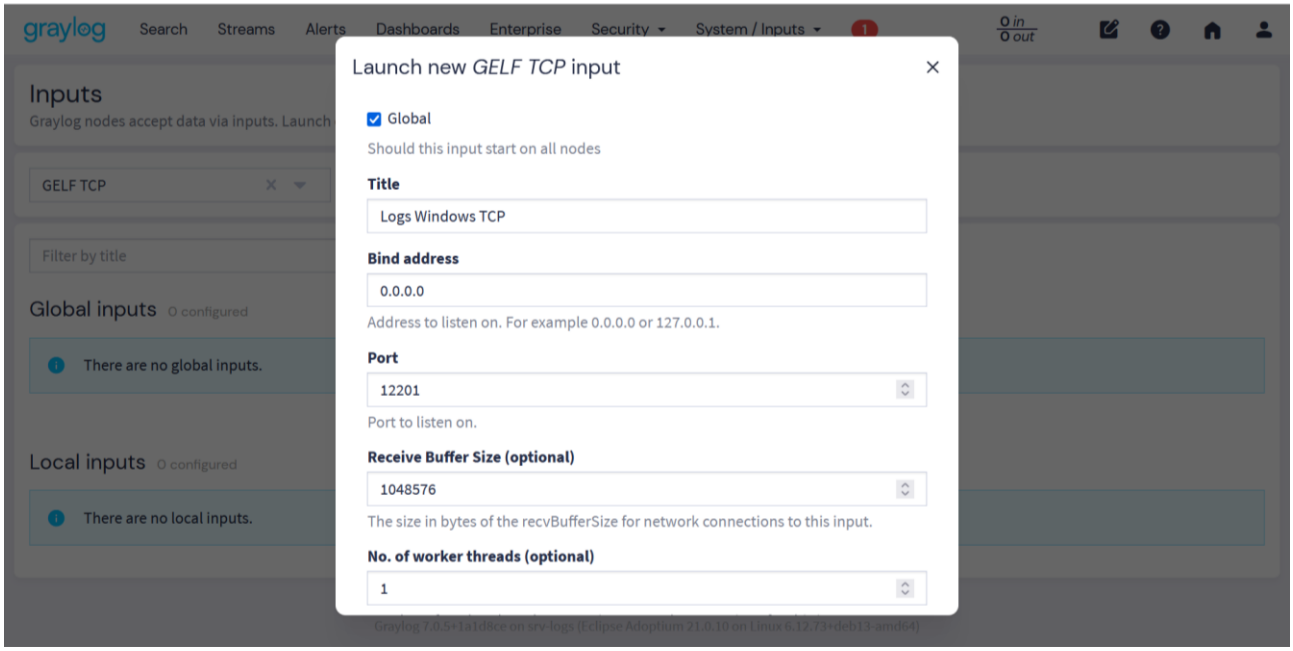
Windows

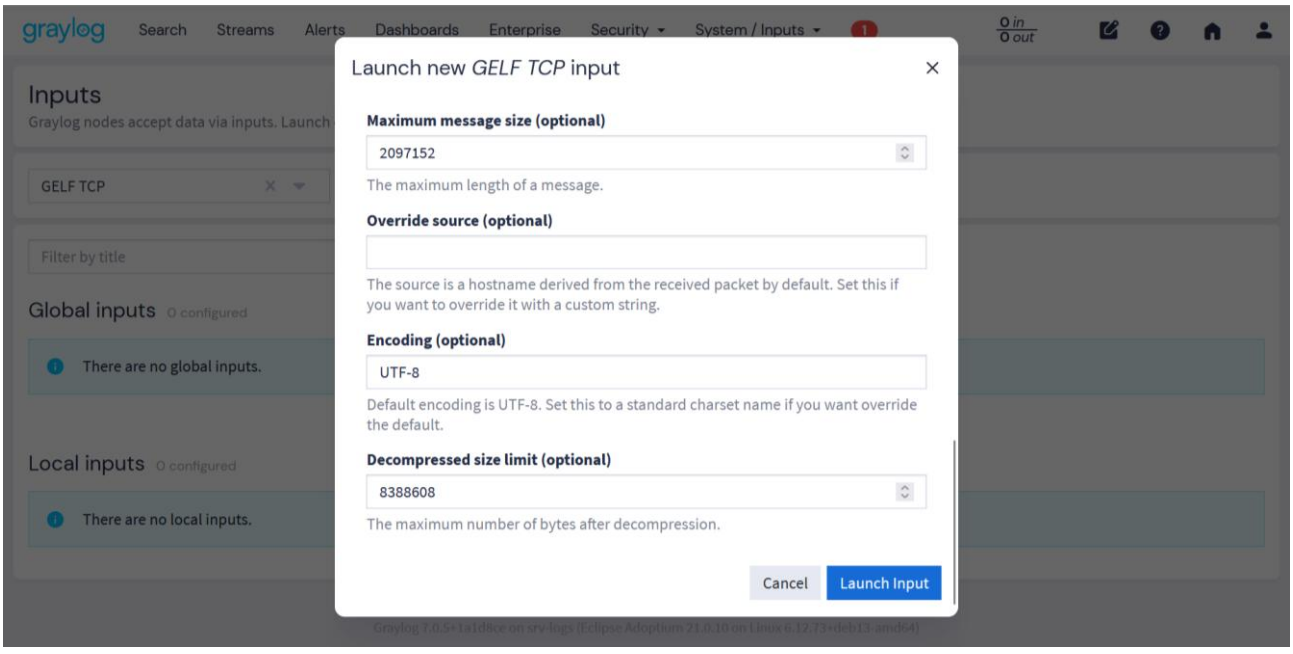
Pour un serveur sous Windows, nous allons choisir l'input GELF TCP dans le menu déroulant. En effet, ce protocole permet de récupérer facilement les journaux Windows avec un format structuré, fiable et complet, tout en garantissant que les messages ne seront pas perdus grâce à la transmission TCP.



Après avoir appuyé sur Launch new input, une fenêtre s'ouvrira. Nous pouvons alors paramétrer dans cette dernière les informations de notre input, notamment son nom. Le port peut être laissé par défaut, mais il est important de le noter car il sera utile par la suite. La bind address est 0.0.0.0 afin que toutes les machines puissent envoyer leurs logs à l'input avec le port correspondant.
Les autres options peuvent être laissées par défaut.

Nous pouvons alors lancer l'input.

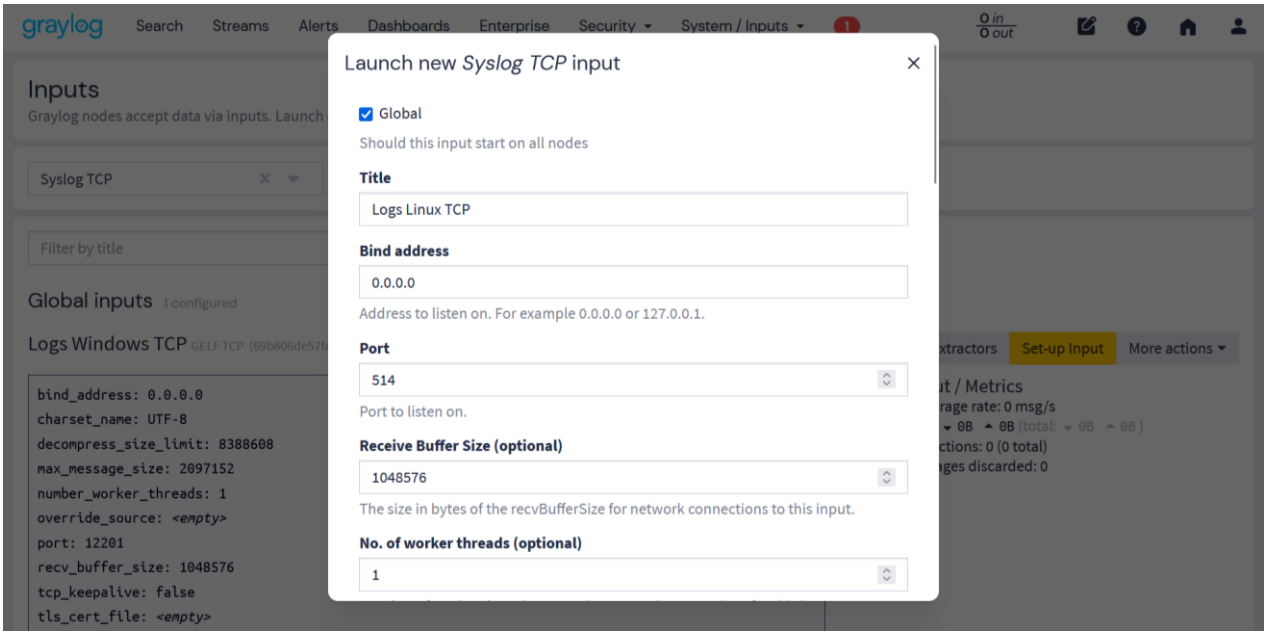




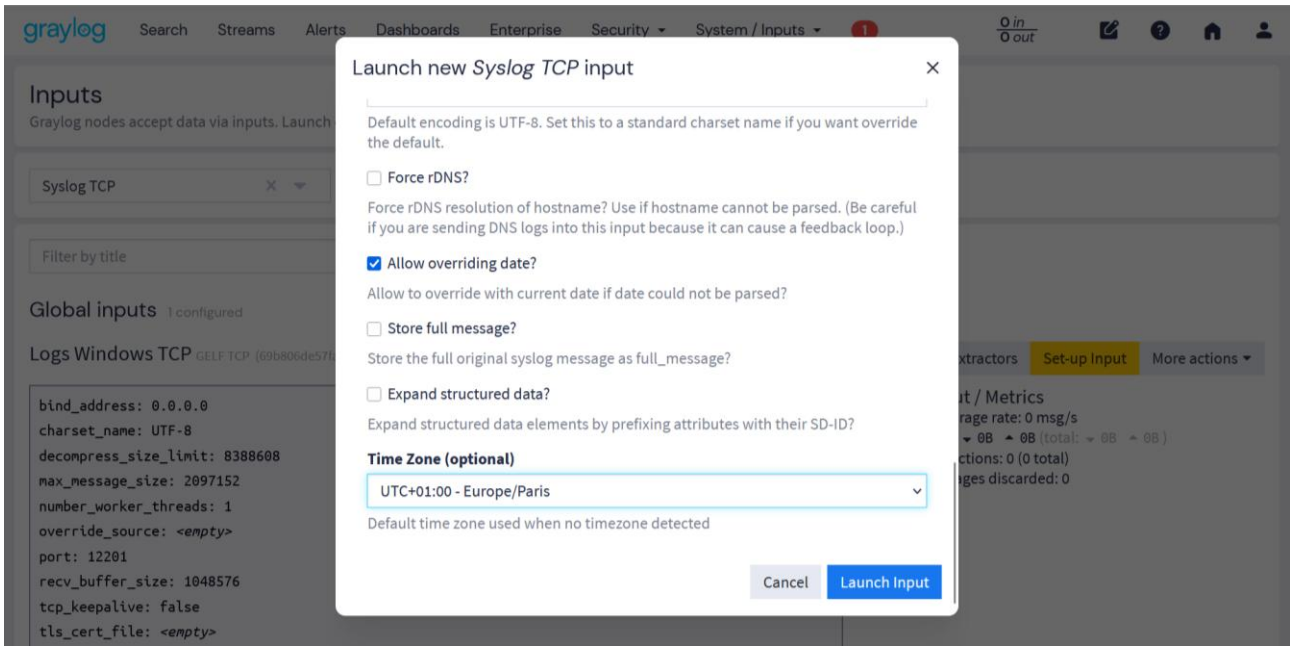
Linux

Pour les machines qui sont sous Linux, la création d'input est légèrement différente.
Il faudra choisir l'option Syslog TCP. En effet, Syslog est un protocole standard sur Linux pour l'envoi de journaux système, ce qui permet à Graylog de collecter facilement les logs des différentes distributions Linux.

Nous donnons tout d'abord un nom à notre input, puis nous paramétrons la bind-address à 0.0.0.0.
Nous pouvons également laisser le port et les autres options par défaut.

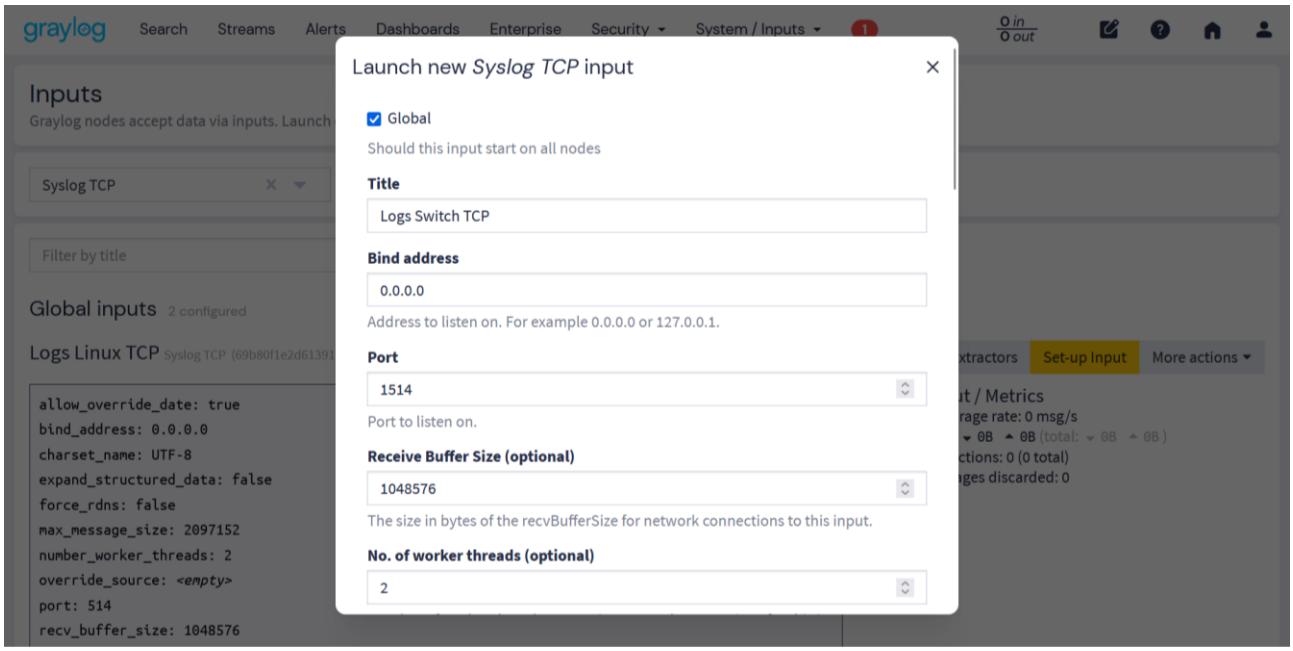


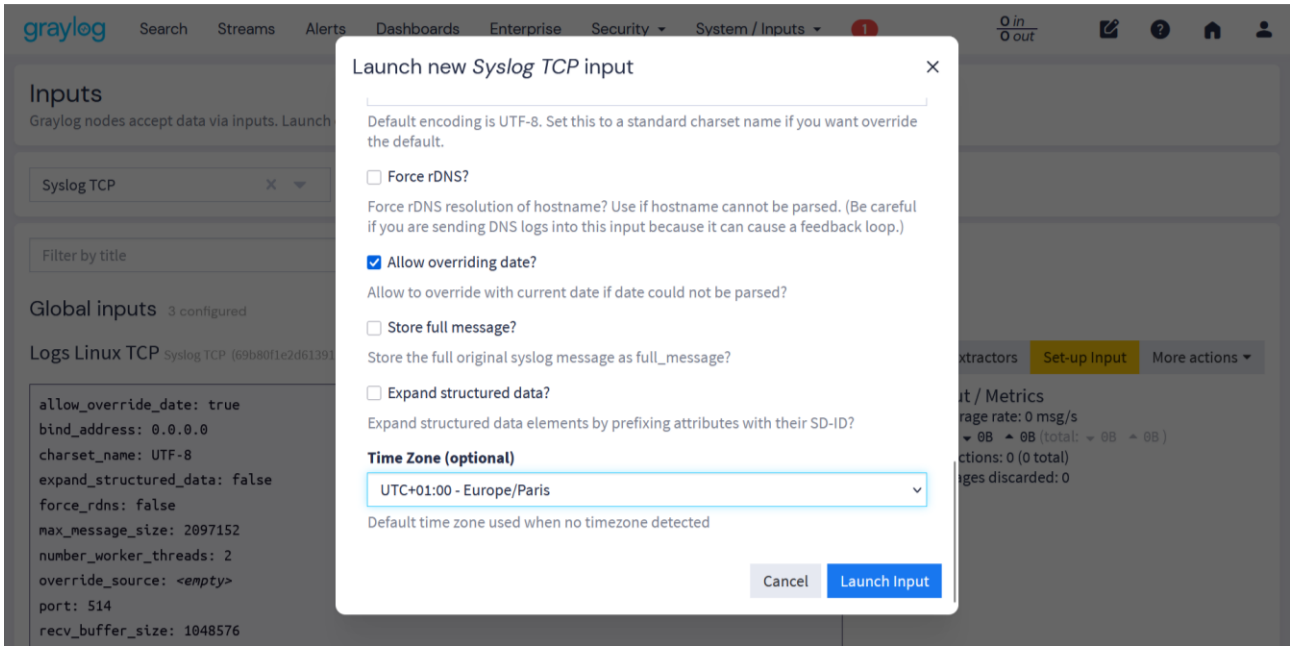
Tout à la fin, il est possible de changer le fuseau horaire pour le mettre à la bonne heure, ici celle de Paris.
Une fois cela effectué, nous pouvons lancer l'input.



Switch

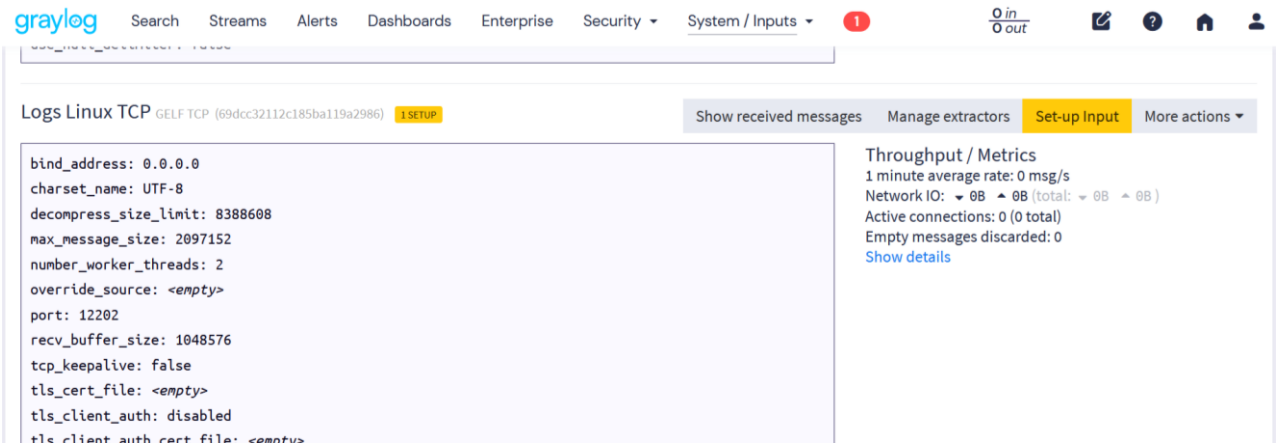
Pour les switchs, il faut faire pareil que pour un serveur Linux mais il faut changer le port afin que deux inputs n'aient pas le même numéro de port.



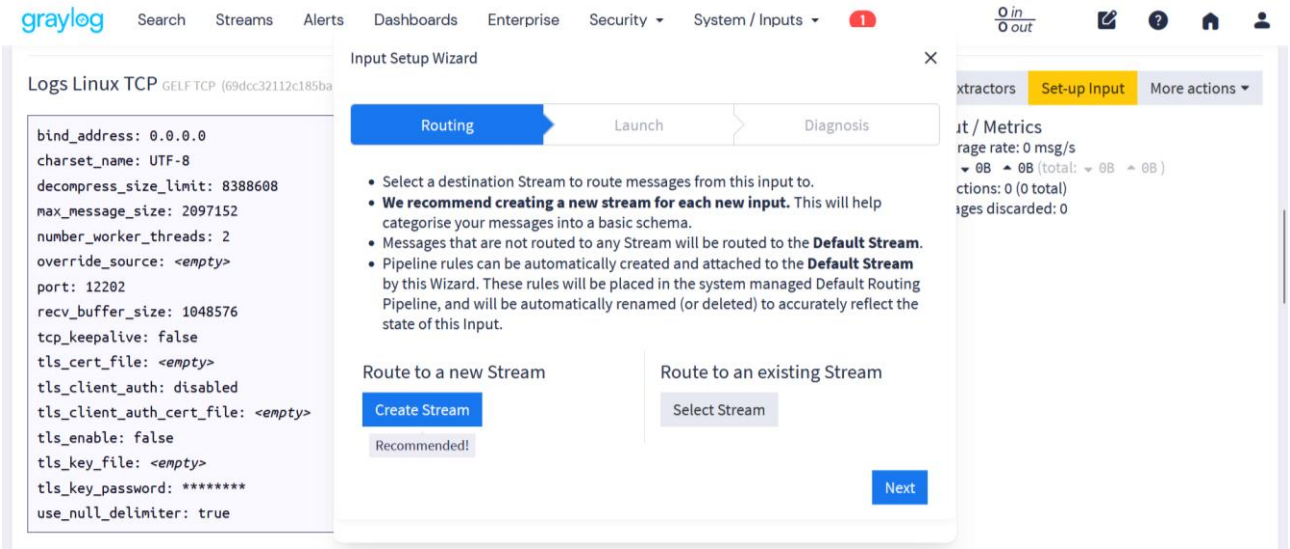


Démarrer les inputs

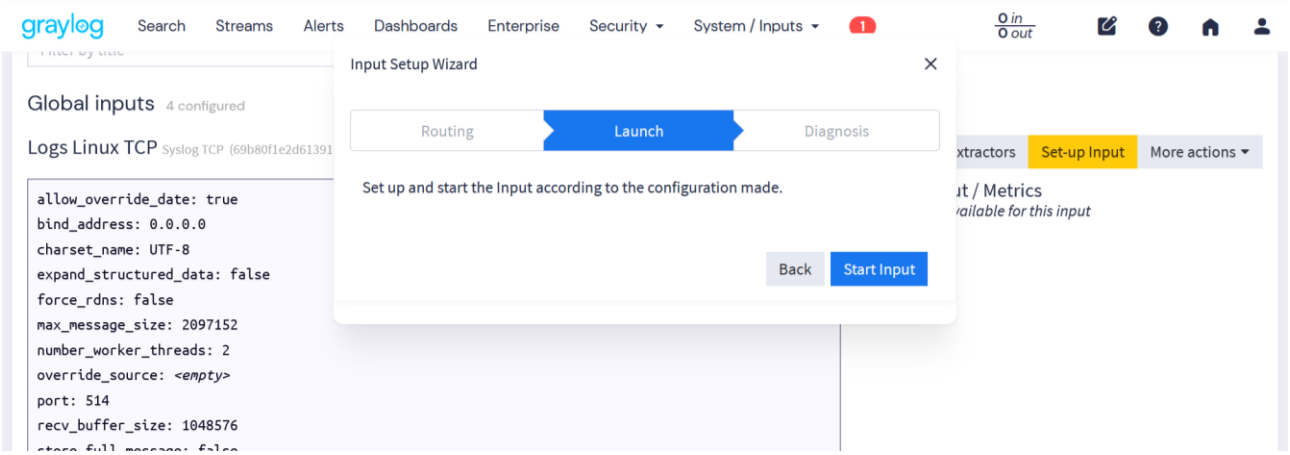
Nous pouvons désormais démarrer nos inputs.
Pour cela, nous devons appuyer sur Set-up input.



Il sera ensuite proposé de créer un stream. Nous pouvons passer cette étape et directement appuyer sur Next. En effet, les streams pourront être créé un peu plus tard.



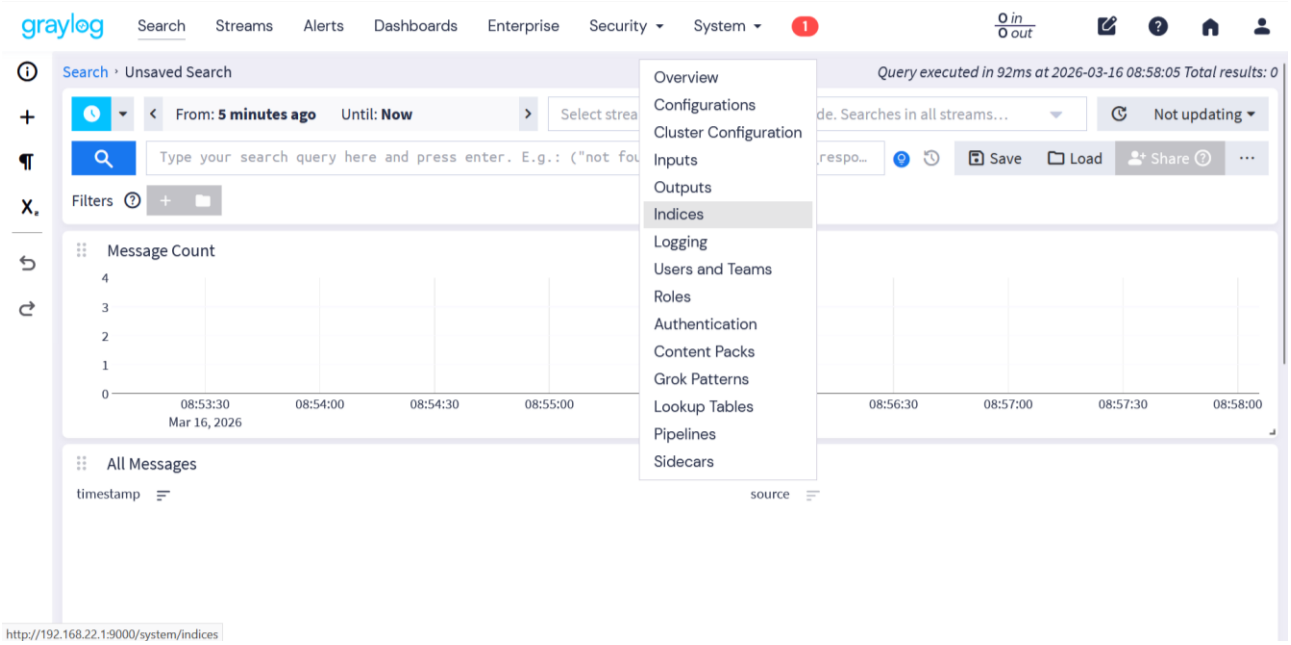
Ensuite, nous pouvons appuyer sur Start Input, puis Back. L'input sera alors démarré.



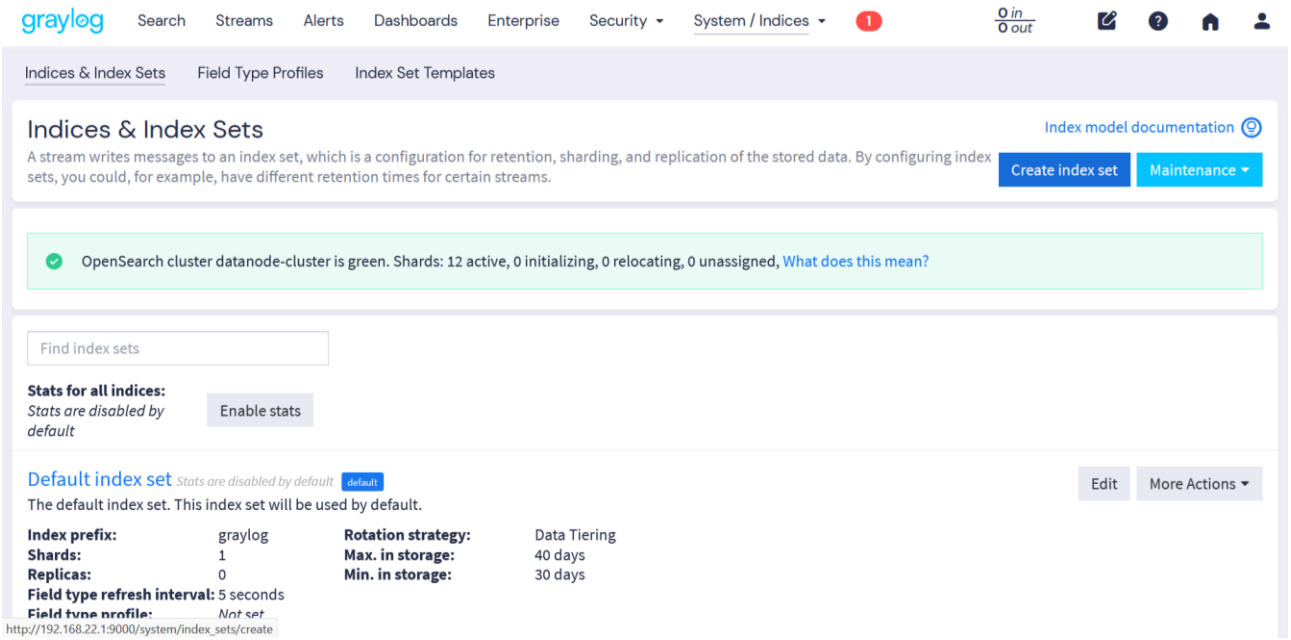
Création d'index

Un Index est l'endroit où les logs sont réellement stockés. Les données sont gérées par Graylog Data Node, basé sur OpenSearch.
Un message ne peut pas être contenu dans plusieurs index.
Il n'est pas obligatoire de créer un index car il en existe déjà un par défaut.

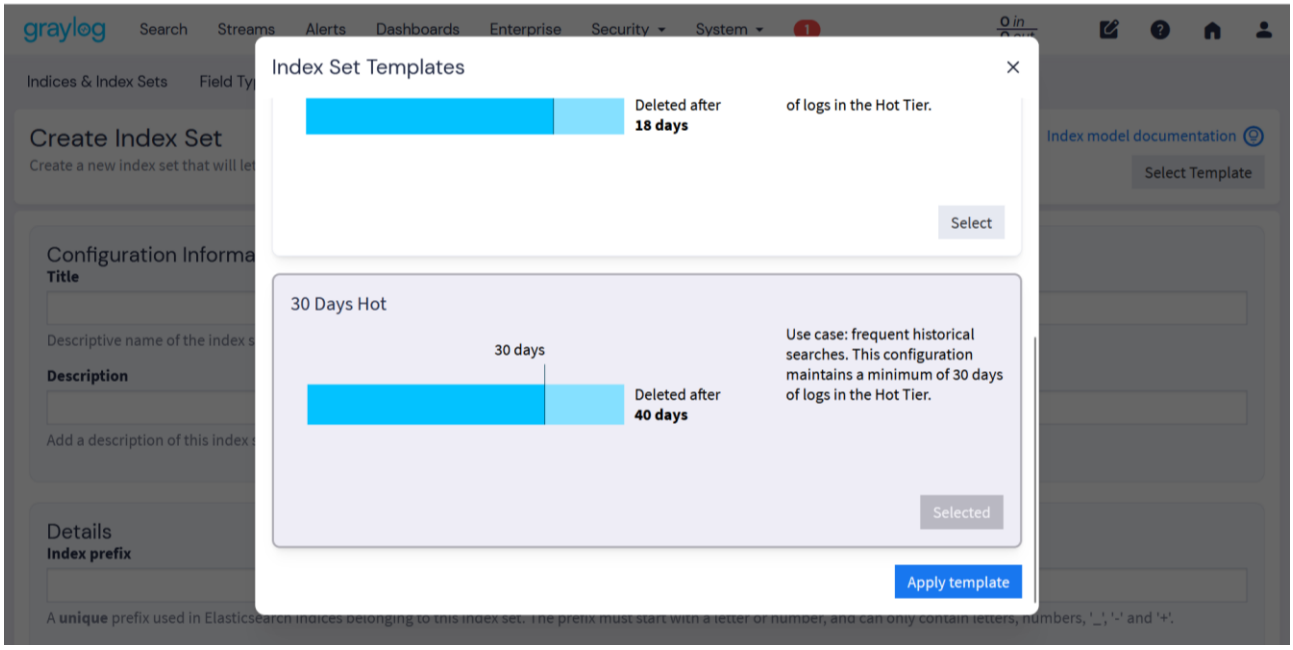
Pour créer un index, il faut d'abord aller dans l'onglet System puis Indices.



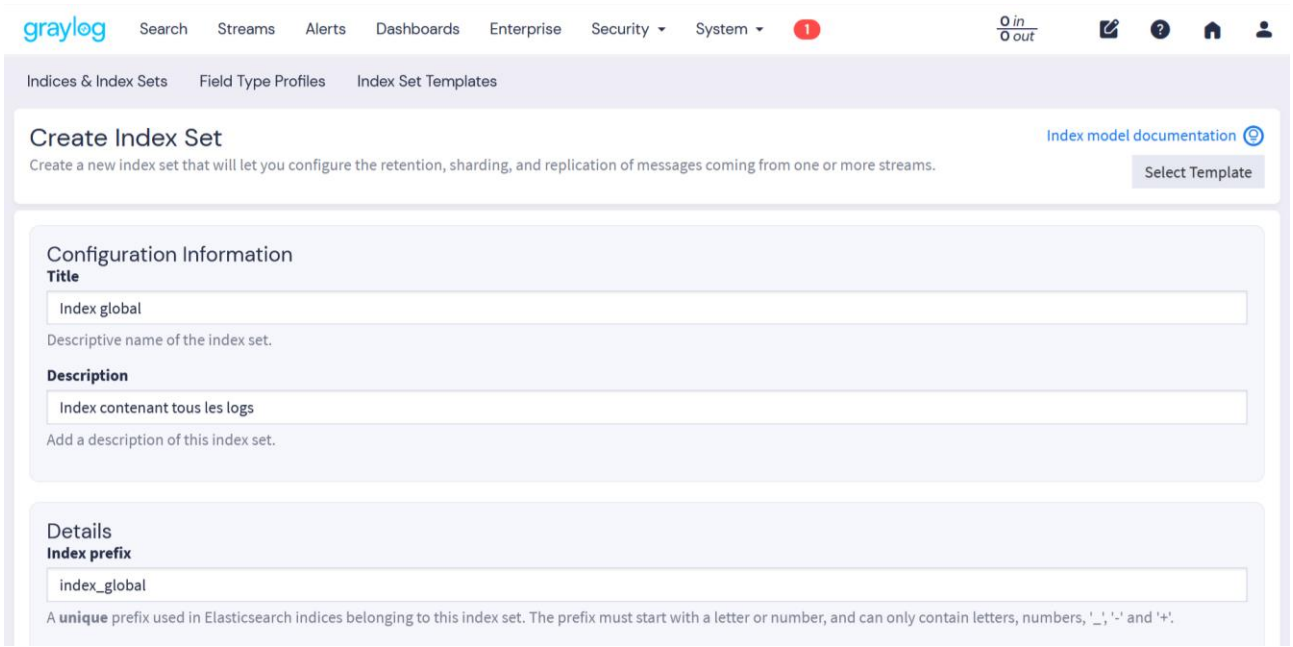
Ensuite, nous pouvons appuyer sur Create Index Set.



Nous devons choisir pour combien de temps nos logs seront stockés dans notre index.
Ce paramètre pourra être modifiable par la suite, mais pour l'instant nous pouvons choisir 30 jours.



Nous devons lui donner un titre, éventuellement une description, et un préfixe unique qui définira l'index.
Les autres options peuvent être laissées par défaut.



Enfin, nous pouvons valider tout en bas de la page.

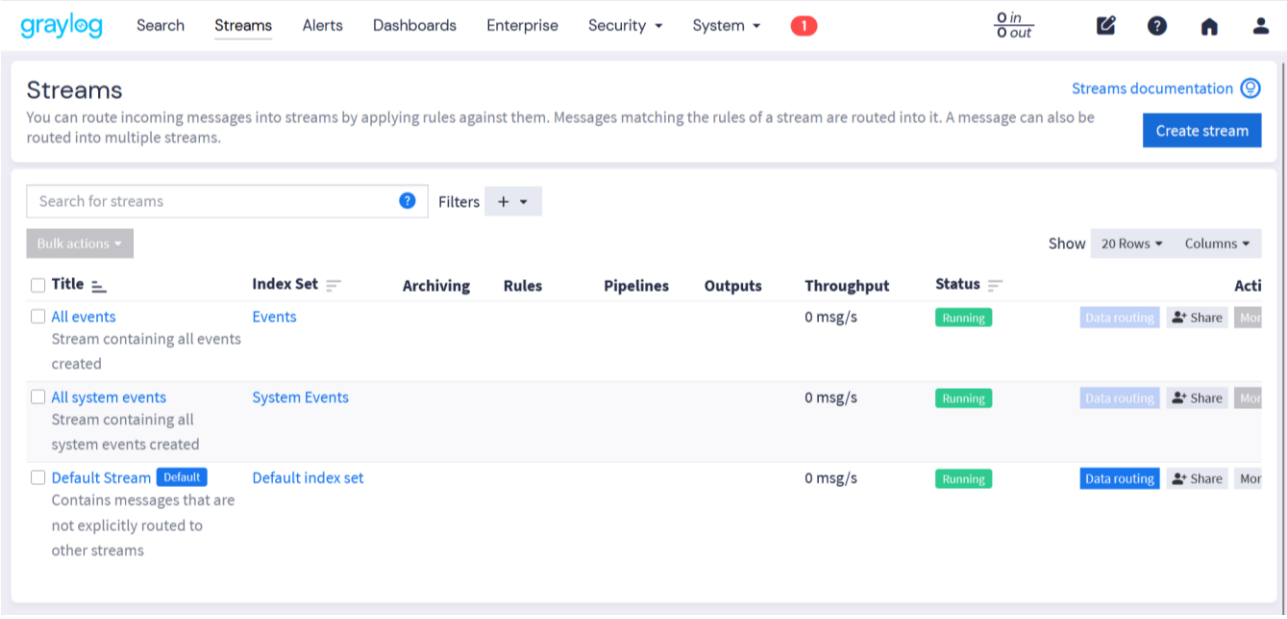
Création de streams

Un Stream sert à filtrer et organiser les logs une fois qu'ils sont reçus. Il permet d'appliquer des règles sur les messages afin de déterminer à quel groupe ils appartiennent.
Un message peut être compris dans plusieurs streams.

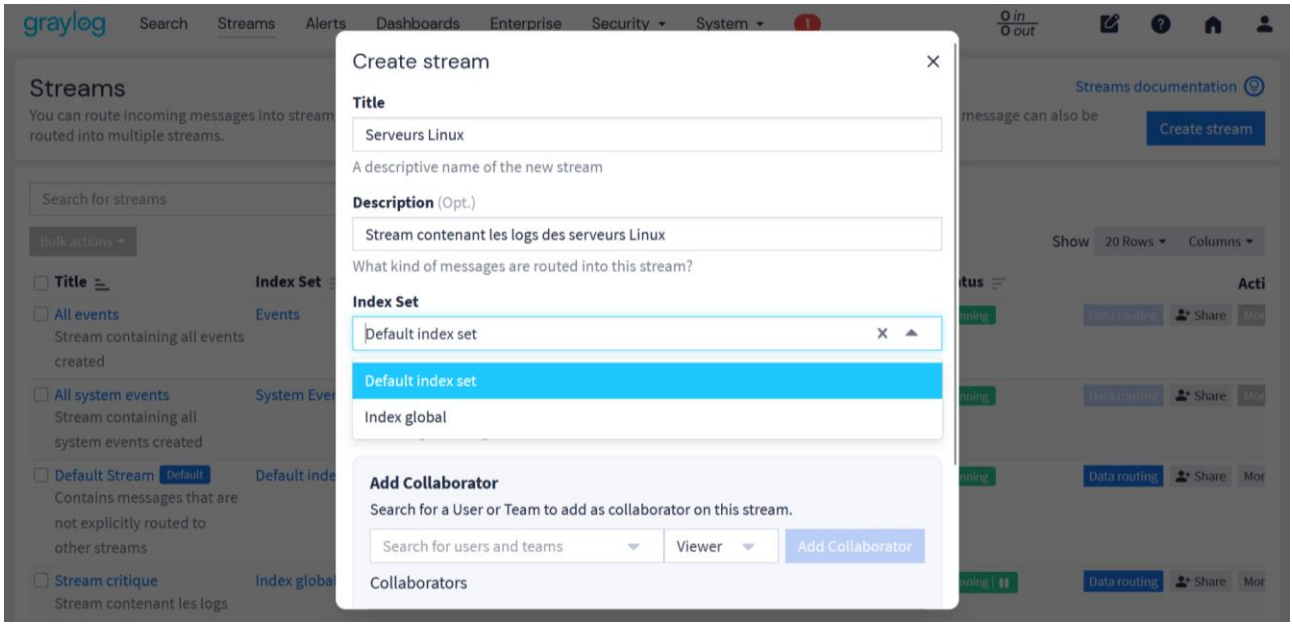
Ici, pour l'exemple, nous allons créer un stream pour un type de machine, puis un stream pour les logs liés aux comptes utilisateurs de l'Active Directory.

Pour commencer, il faut aller dans l'onglet Streams dans la barre de navigation. Nous pouvons voir que des streams par défaut sont déjà créés.

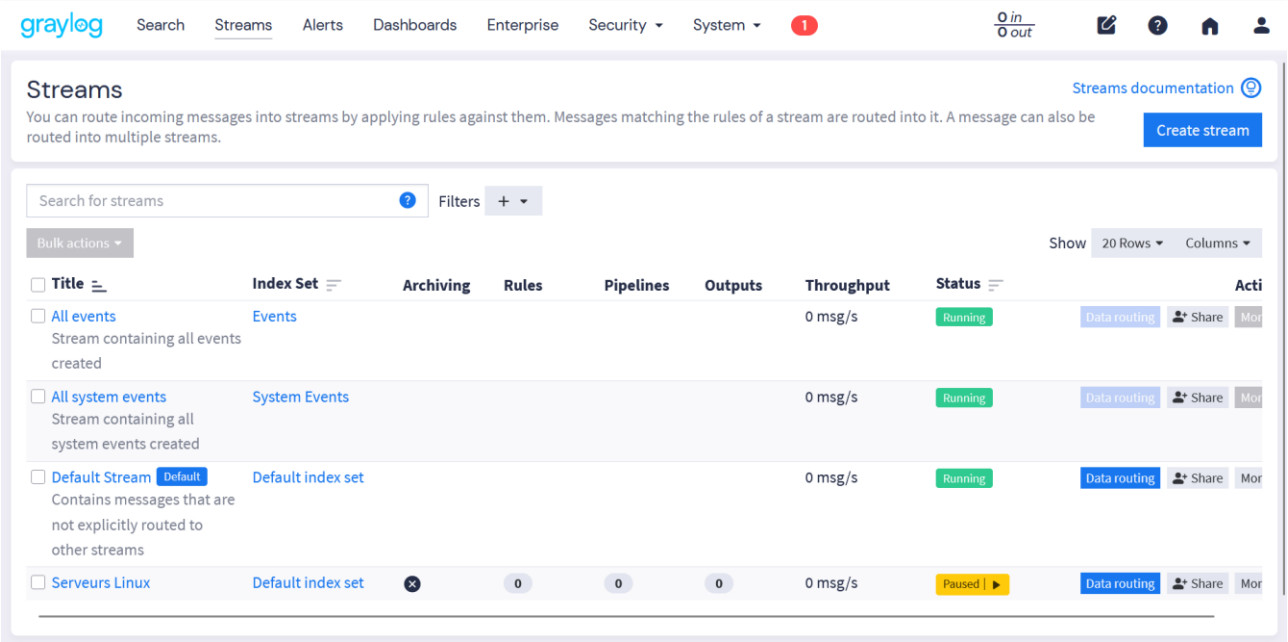
Pour créer un nouveau stream, nous pouvons appuyer sur Create stream.



Ensuite, nous pouvons lui donner un nom, une brève description, et choisir l'index qui stockera les logs du stream, celui par défaut ou celui que nous venons de créer.

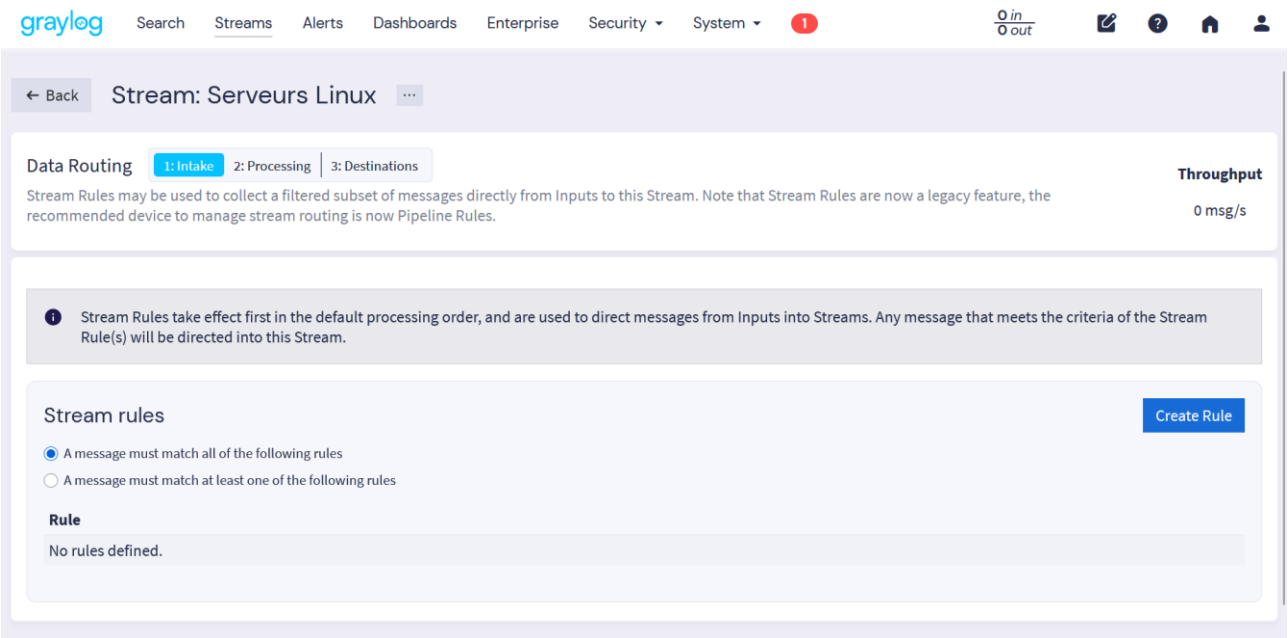


Notre nouveau stream apparaît dans la liste des Streams.

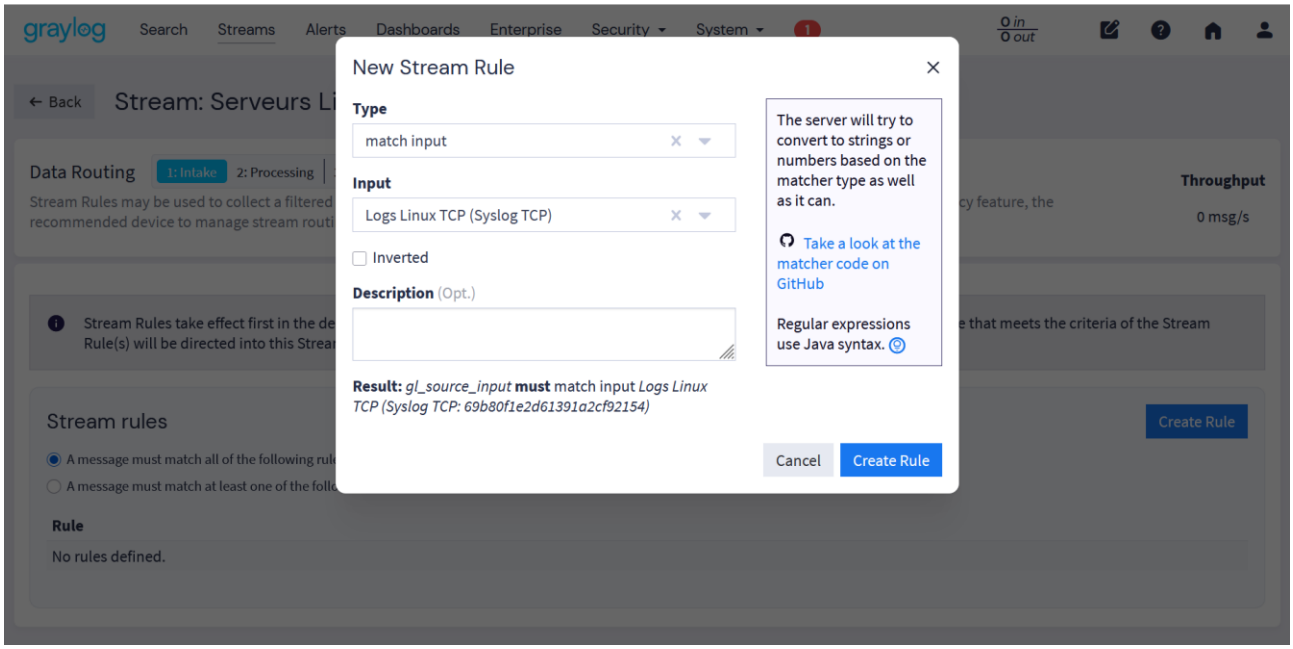


Nous allons alors mettre en place une règle.

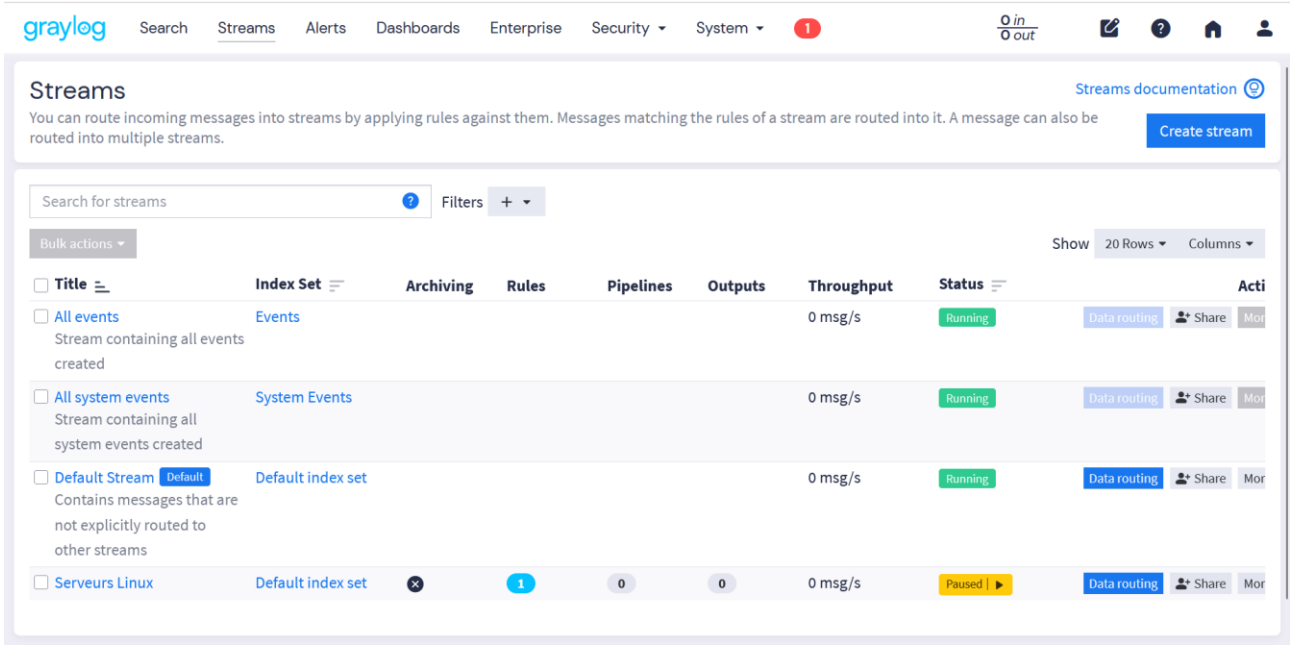
Pour cela, nous allons sur Data Routing, puis Create Rule.



Nous devons alors paramétrer la règle comme cela : le type doit être match input, et l'input celui qui reçoit les logs de nos serveurs Linux. Cela signifie que tous les messages qui sont reçus par notre input Logs Linux TCP seront dans ce stream.
Il est possible de mettre une description et une fois cela terminé, nous pouvons donc valider la règle en appuyant sur Create rule et retourner dans nos streams.



Nous allons pouvoir démarrer notre stream en appuyant sur le bouton Paused en jaune. Le statut passera alors en Running, et nous pourrons aller voir les logs reçus dans le stream en appuyant dessus.

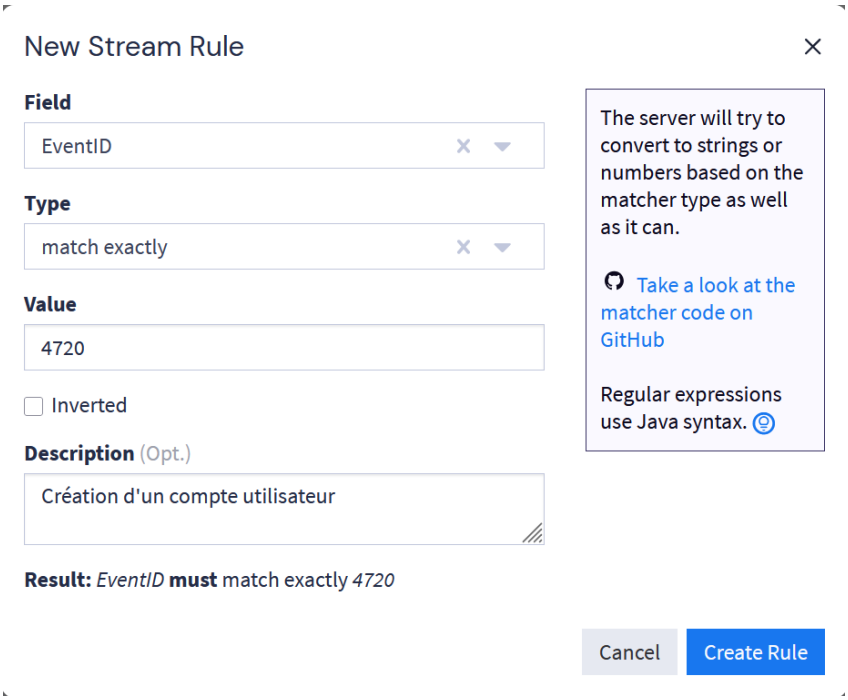


De la même manière, nous pouvons créer un stream qui filtre les messages qui sont liés à des modifications de compte dans un Active Directory.

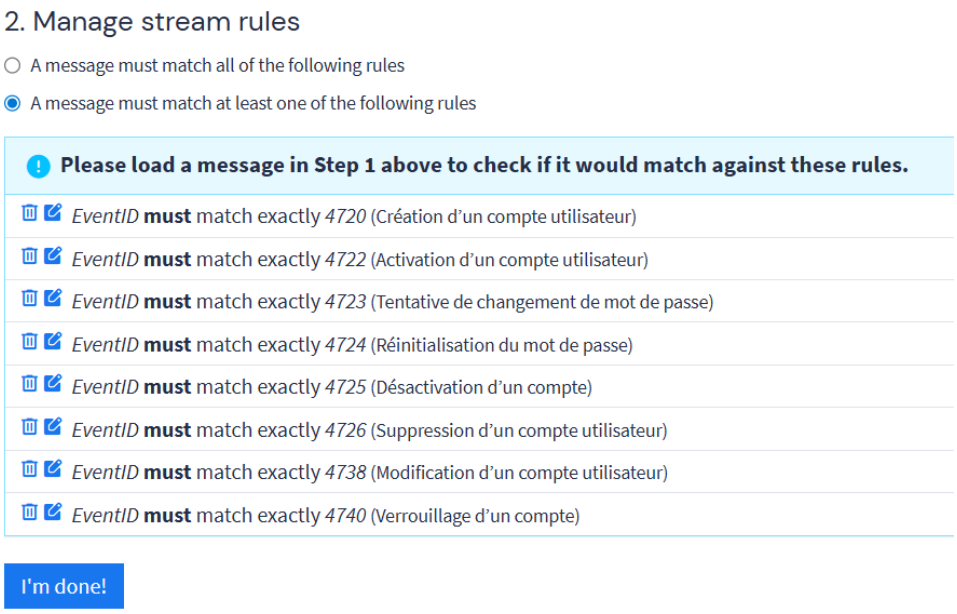
Tout d'abord, nous créons un nouveau stream.

Ensuite, nous allons définir des règles afin de filtrer uniquement les logs correspondant à la modification d'un compte Active Directory. Pour cela, nous utiliserons les EventID, qui sont des numéros uniques associés à chaque événement et qui permettent de savoir précisément quelles actions ont été réalisées. Ces derniers sont générés par Windows.

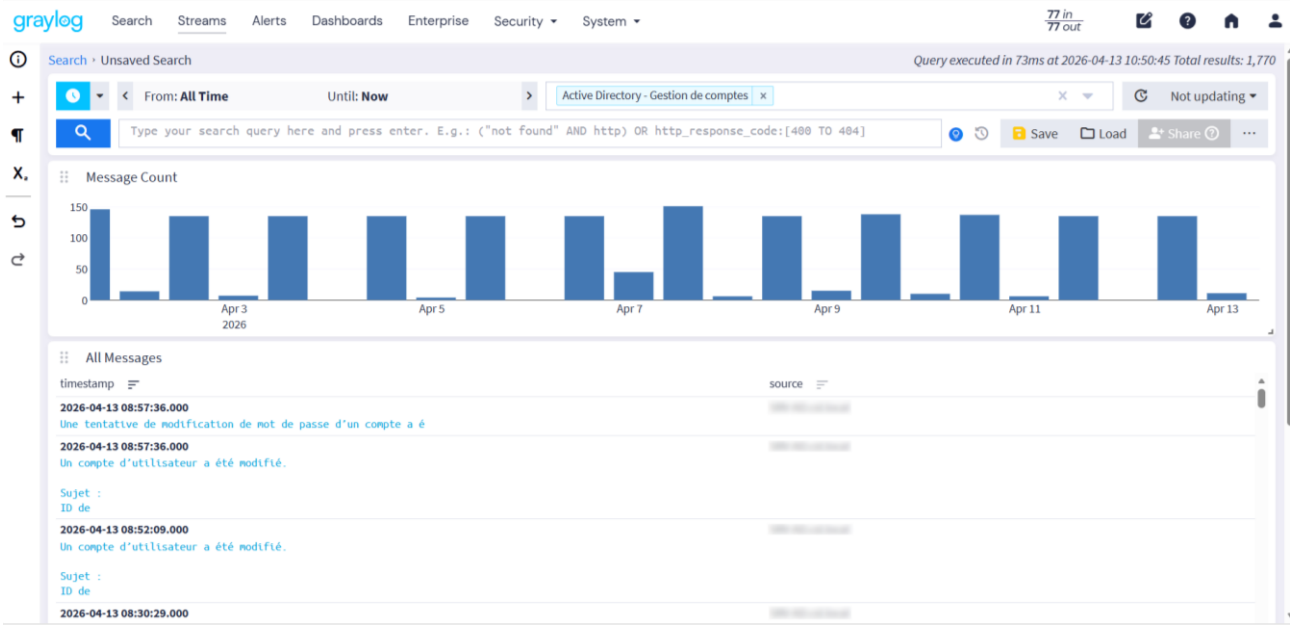
Pour cela, il faut aller dans Data Routing et Create Rule. Nous mettons alors EventID comme field, puis nous souhaitons qu'il corresponde exactement à la valeur 4720, donc nous mettons match exactly comme type et 4720 comme value. Nous pouvons ajouter une description si besoin.



Les règles à paramétrer sont celle-ci.
Nous choisissons "A message must match at least one of the following rules" afin de prendre en compte tous les logs correspondant à l'un des critères définis, puisqu'un événement ne peut être associé qu'à un seul EventID.



Enfin, nous démarrons le stream et nous pouvons alors voir nos logs triés.

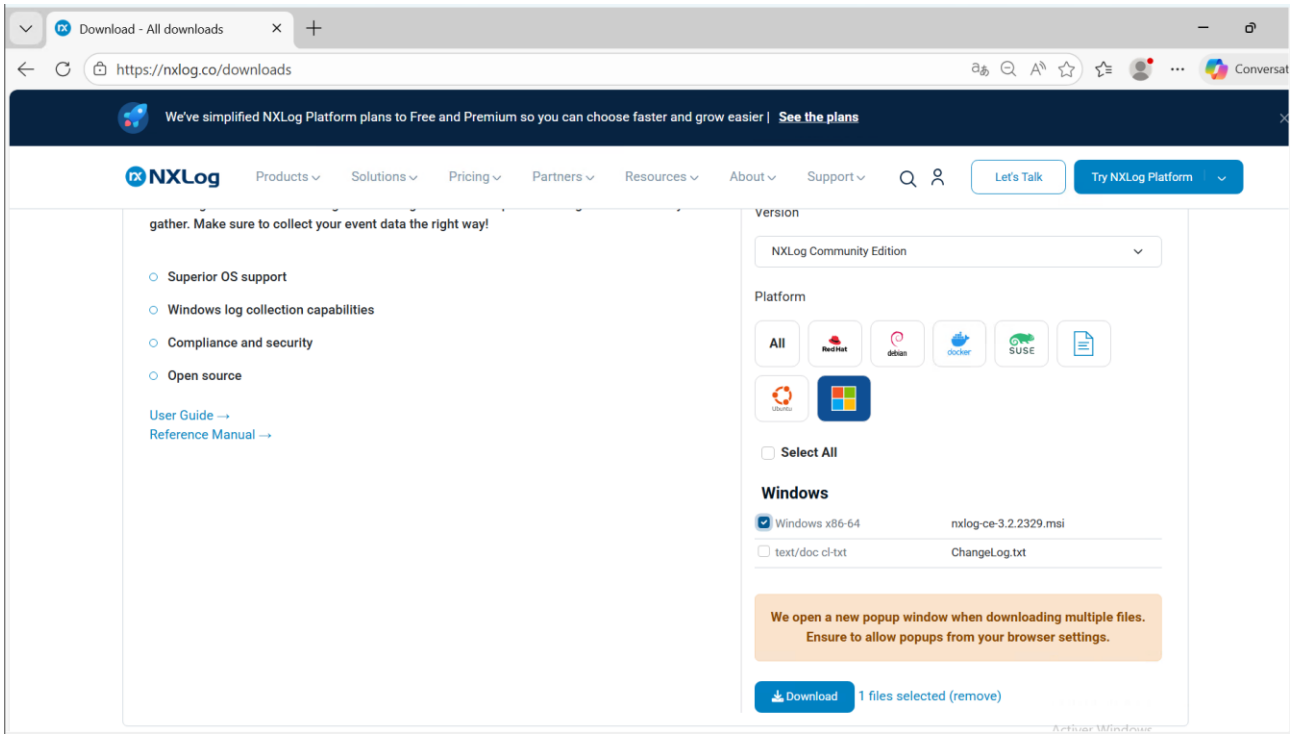


Mise en place de l'envoi des logs

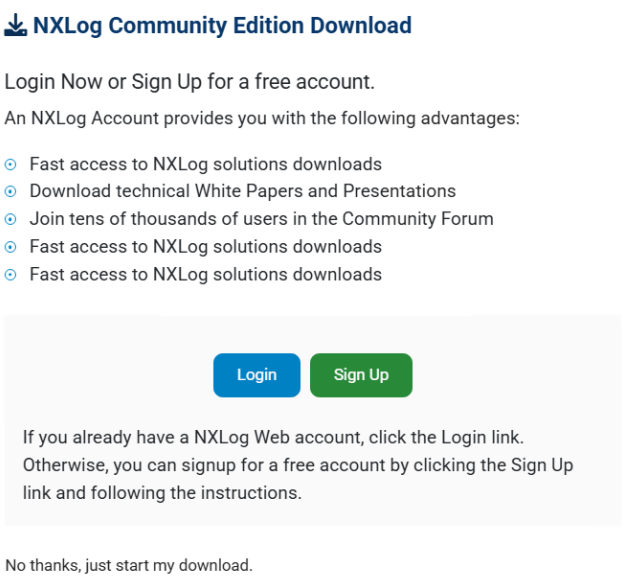
Une fois nos inputs et streams créés, nous devons configurer nos machines de façon que les logs soient envoyés vers notre serveur Graylog.

Configuration sur Windows

Sur Windows, nous allons utiliser le logiciel NXLog.
Pour cela, nous pouvons nous connecter sur notre serveur Windows et télécharger NXLog depuis ce lien : https://nxlog.co/downloads



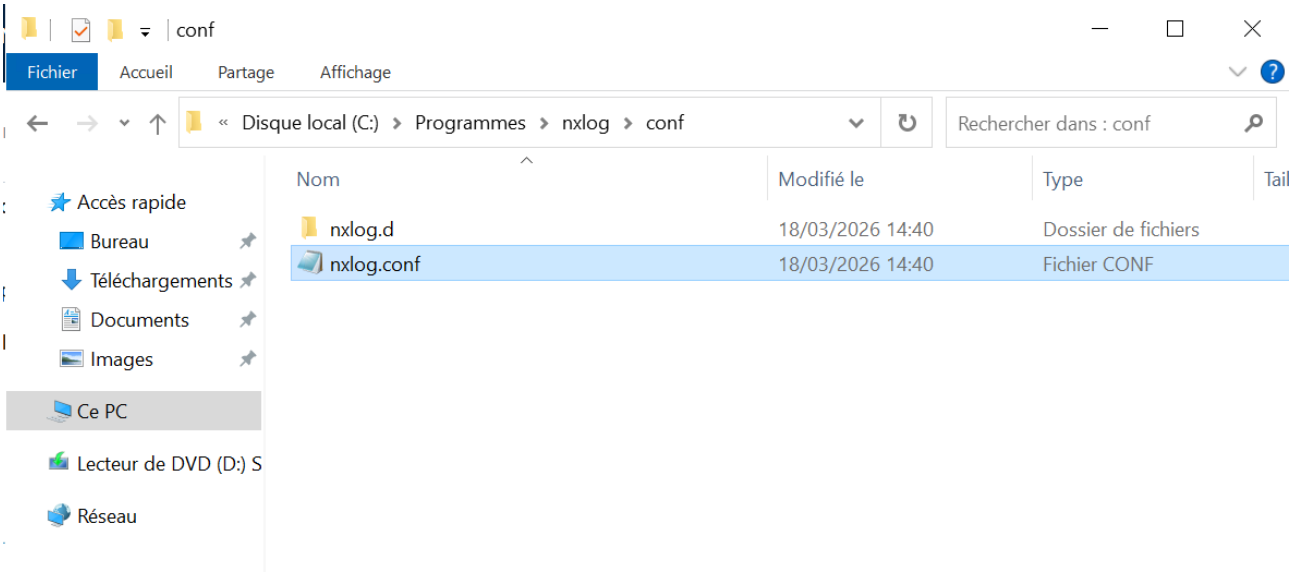
Il faut sélectionner la version Community Edition, la plateforme Windows et Windows x86-64.
Ensuite, nous pouvons appuyer sur Download.
Si un compte est demandé, il est possible de contourner en cliquant en bas à gauche.



Nous pouvons alors commencer l'installation de NXLog.

Il suffit de suivre les instructions de l'assistant, il n'y a encore rien à paramétrer.

Une fois l'installation terminée, nous pouvons éditer le fichier de configuration de NXLog.



Nous devons ajouter ces lignes à la fin du fichier.

```
# Récupérer les journaux de l'observateur d'événements
<Input in>
    Module      im_msvistalog
</Input>

# Déclarer le serveur Graylog (selon input)
<Extension gelf>
    Module      xm_gelf
</Extension>

<Output graylog_tcp>
    Module      om_tcp
    Host        192.168.22.1
    Port        12201
    OutputType  GELF_TCP
</Output>

# Routage des flux in vers out
 <Route 1>
     Path in => graylog_tcp
 </Route>
```

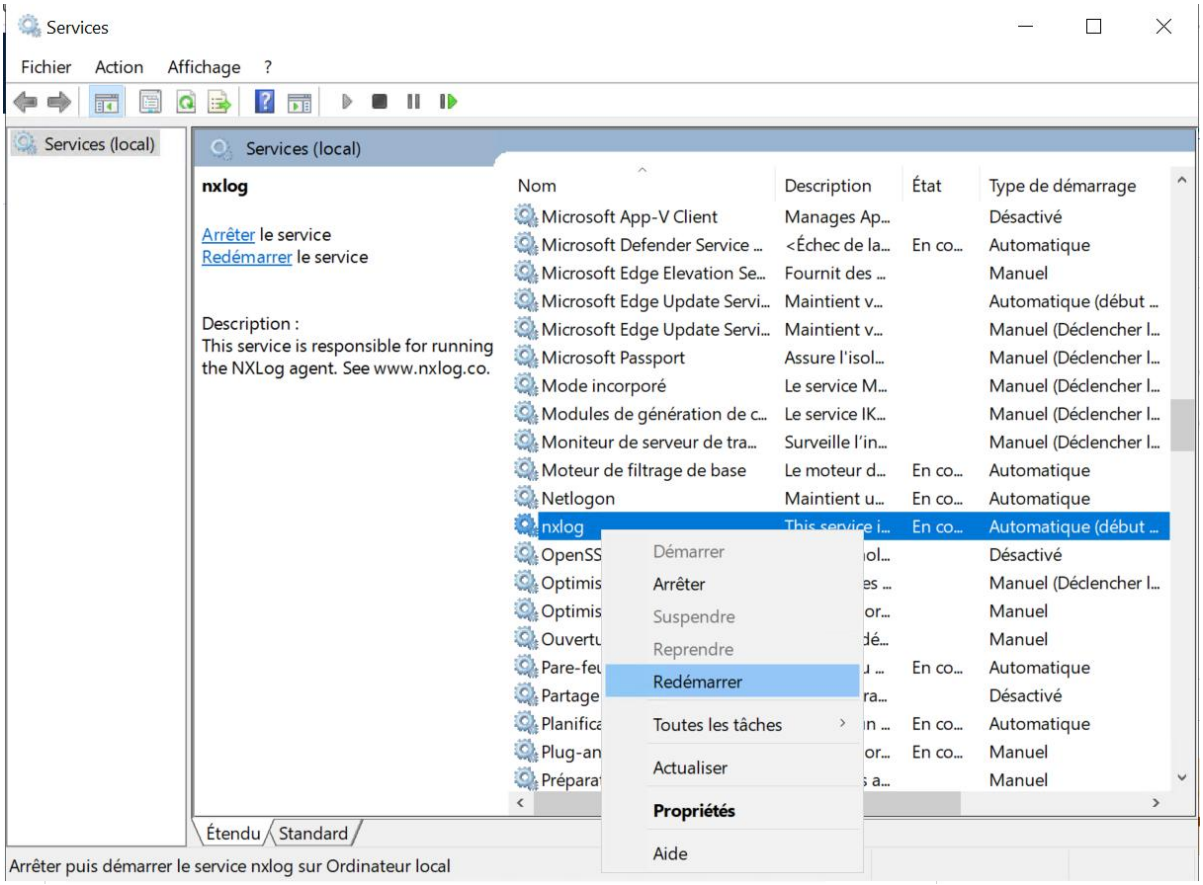
nxlog.conf - Bloc-notes

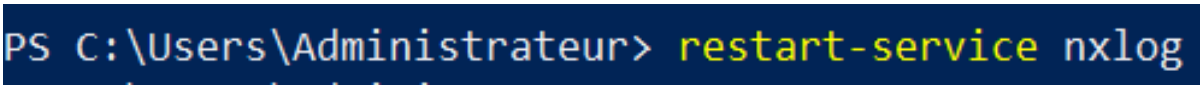
Fichier Edition Format Affichage Aide

```
# Récupérer les journaux de l'observateur d'événements
<Input in>
    Module      im_msvistalog
</Input>

# Déclarer le serveur Graylog (selon input)
<Extension gelf>
    Module        xm_gelf
</Extension>

<Output graylog_tcp>
    Module        om_tcp
    Host          192.168.22.1
    Port          12201
    OutputType    GELF_TCP
</Output>

# Routage des flux in vers out
 <Route 1>
     Path in => graylog_tcp
 </Route>
```

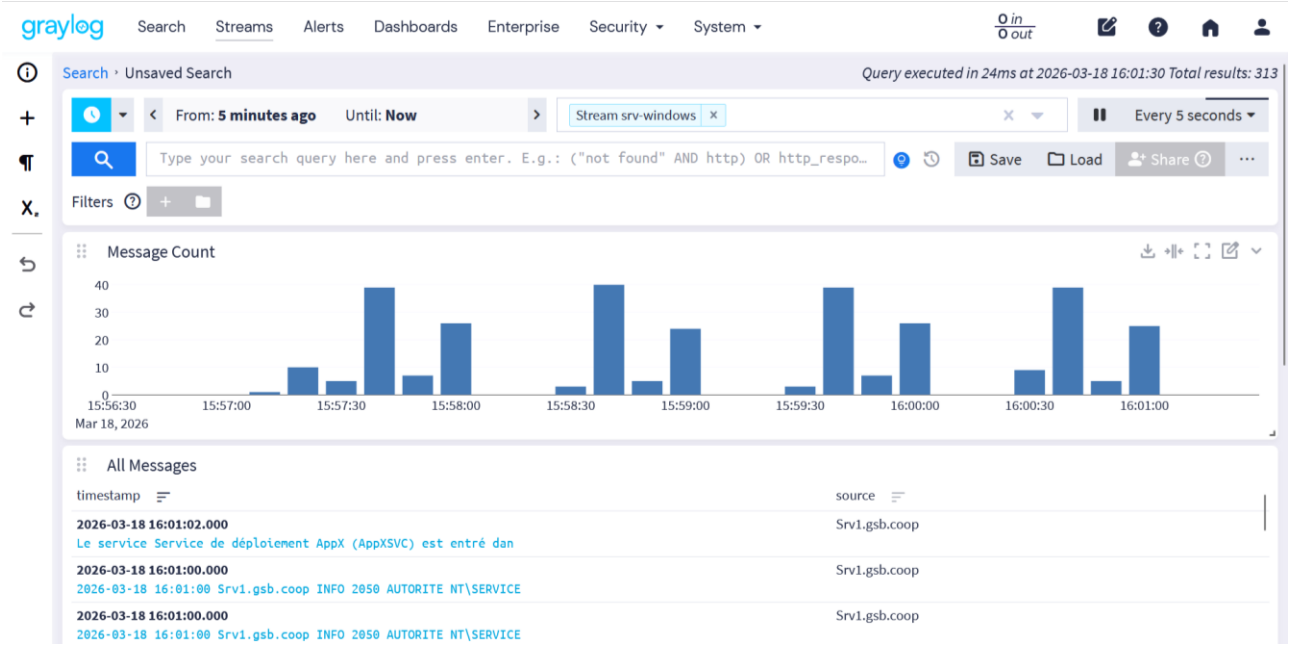
Ces paramètres correspondent au serveur Graylog ainsi qu'à l'input Windows déjà créé. Ils doivent alors être modifié selon le paramétrage du serveur.

Enfin, il faut sauvegarder le fichier et redémarrer le service NXLog, en PowerShell ou bien depuis la console Services.





En vérifiant, nous pouvons voir que les logs sont bien envoyés sur notre serveur Graylog.



Configuration sur Linux

Pour envoyer les logs d'un serveur Linux à notre Graylog, nous allons utiliser Rsyslog.

Sur notre serveur Linux, nous pouvons d'abord mettre à jour la machine et installer rsyslog si le paquet n'est pas déjà installé.

```
root@nas-omv:~# apt update -y && apt upgrade -y
root@nas-omv:~# apt install rsyslog
```

Ensuite, nous devons créer un fichier intitulé 10-graylog.conf dans le répertoire de rsyslog.
Dans ce dernier, nous inscrivons cette ligne.

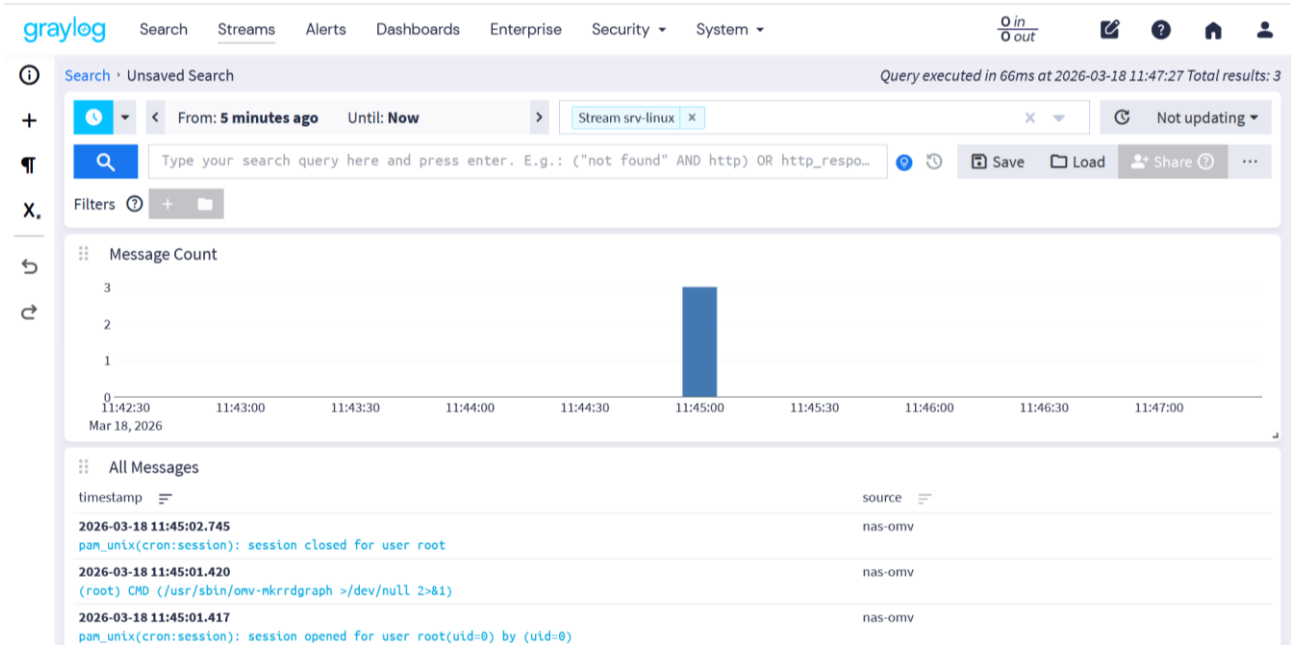
```
  GNU nano 7.2     /etc/rsyslog.d/10-graylog.conf
*.* @@192.168.22.1:514;RSYSLOG_SyslogProtocol23Format
```

Elle est à modifier en fonction du paramétrage du serveur Graylog. Ici, *.* signifie qu'on veut envoyer tous les logs de la machine à Graylog. Ensuite, les @@ signifient que le transport s'effectue en TCP. L'ip doit être celle du serveur Graylog et le port celui qui est spécifié pour l'input Linux.

Enfin, nous redémarrons rsyslog.

```
root@nas-omv:~# systemctl restart rsyslog.service
```

Nous pouvons désormais voir nos logs dans notre stream Linux.



Configuration sur Switch

Pour envoyer les logs depuis un switch, il y a seulement quelques commandes à effectuer.
Cependant, elles diffèrent en fonction de la marque et du modèle du switch.
Dans ces exemples, le niveau de logs du switch est configuré à informational (niveau 6). Il existe 8 niveaux de logs, allant de 0 (emergencies) à 7 (debugging). Lorsqu'un niveau est configuré, le switch remonte tous les messages à partir de ce niveau. Le niveau informational est le plus adapté à un usage courant : il couvre les événements significatifs du réseau tout en évitant la surcharge de messages générée par le niveau debugging.

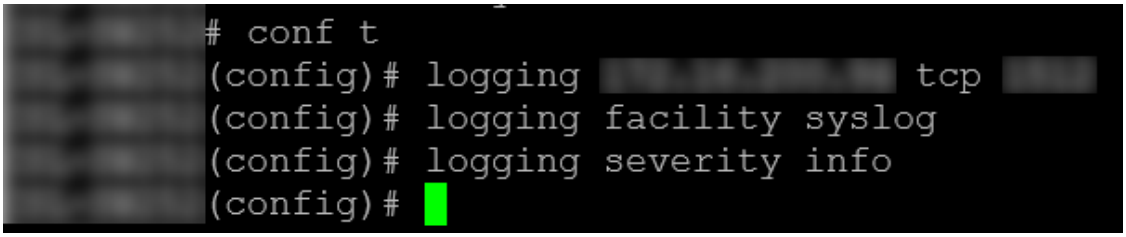
Cisco

Sur un switch Cisco, la configuration s'effectue depuis le mode de configuration du terminal. Il faut ensuite saisir la commande logging en précisant successivement le mot-clé host suivi de l'adresse IP du serveur Graylog, le mot-clé transport suivi du protocole utilisé, puis le mot-clé port suivi du numéro de port correspondant à l'input Graylog dédié aux switchs.

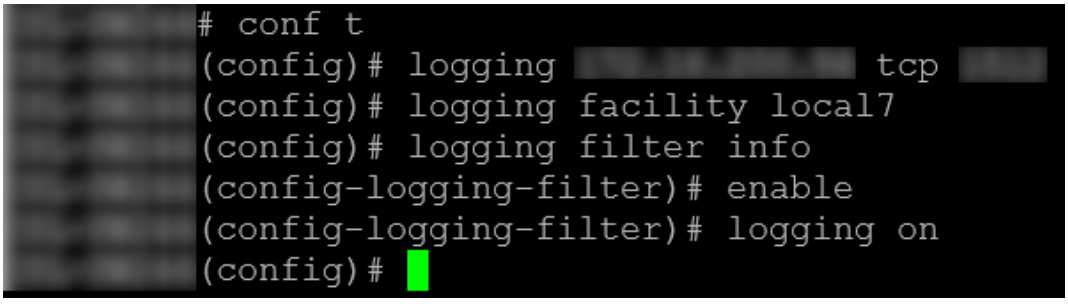
```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#logging host 192.168.22.1 transport tcp port 1514
Router(config)#logging trap informational
Router(config)#logging facility local7
Router(config)#logging on
```

Aruba

Sur un switch Aruba, voici les commandes à effectuer.
Il n'y a pas besoin d'indiquer le paramètre à chaque fois, mais simplement de donner l'ip suivi du protocole et du port. Il n'est pas non plus obligatoire de mettre la commande logging on.



Selon le modèle du switch, les commandes peuvent être les suivantes.



Changer fuseau horaire graylog

Si l'interface de Graylog n'affiche pas la bonne heure alors que le serveur est bien dans le bon fuseau horaire, il faut ajouter cette ligne dans le fichier de configuration de graylog.

```
  GNU nano 8.4     /etc/graylog/server/server.conf

# The time zone setting of the root user. See http:
# Default is UTC
root_timezone = Europe/Paris
```

Ensuite, il faut redémarrer le service Graylog.

```
root@srv-logs:~# systemctl restart graylog-server.service
```