Mise en place d’un serveur de journalisation Graylog

Sommaire

Informations additionnelles

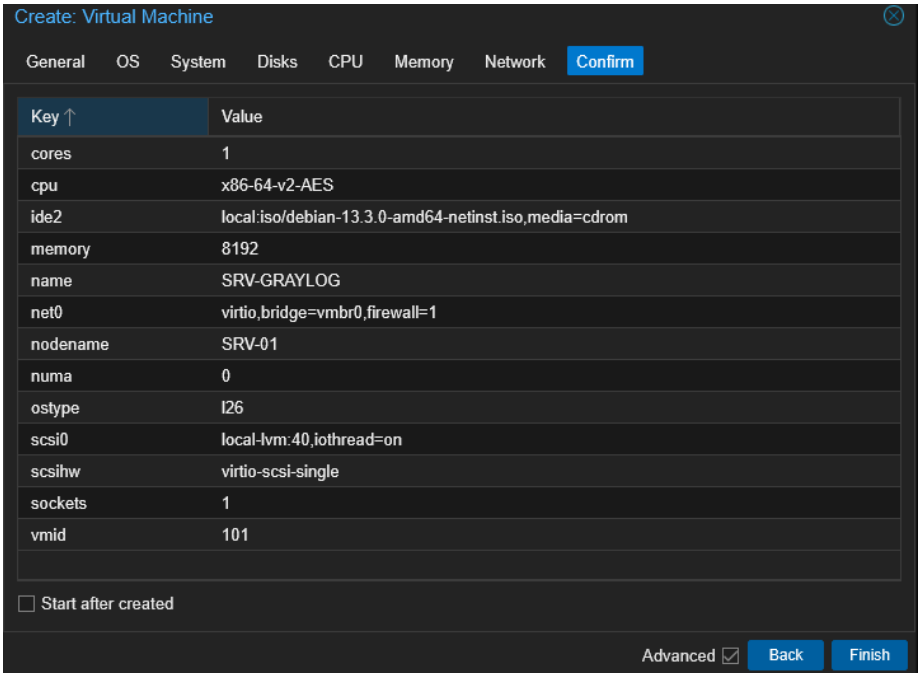
OS de la VM	Debian 13
Version de Graylog	6.2.12-1
MongoDB	7.0.30
OpenSearch	2.19.4
Rsyslog	8.2504.0-1
NXLog	nxlog-ce-3.2.2329

Partie 1 - Présentation de Graylog

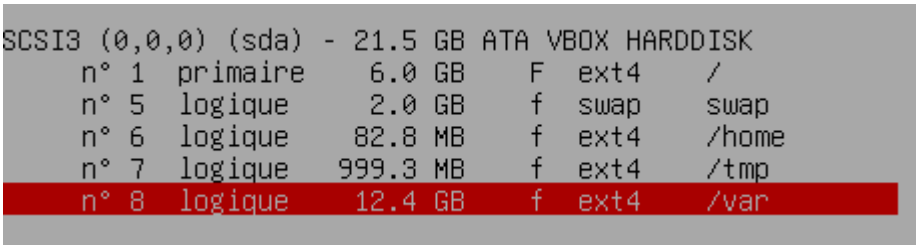
Graylog est une solution de gestion centralisée des logs qui permet de collecter, indexer et analyser vos données machine en temps réel. Elle offre des tableaux de bord visuels et un moteur de recherche puissant pour faciliter le débogage, la surveillance d'infrastructure et la détection d'incidents de sécurité. C'est un outil essentiel pour transformer des volumes massifs de données brutes en informations exploitables pour les équipes IT, DevOps et Sécurité.

Partie 2 - Prérequis

1) Une machine (8go minimum) avec Debian installé (SRV-01)



2) ⚠️ : Le partitionnement doit être réalisé de la façon suivante :



3) Ajouter la carte réseau privé hôte sur la machine depuis le proxmox (vmbr1)
4) Respecter l'adressage suivant :

Nom	@IP	Masque	Passerelle	DNS	Lié au domaine
SRV-GRAYLOG	192.168.30.15 192.168.150.15 (ens19)	/24	192.168.30.254	192.168.30.1	Oui

5) Nommer la machine comme ceci :

```
nano /etc/hostname
```

```
SRV-GRAYLOG.technova.local
```

```
nano /etc/hosts
```

```
127.0.0.1       localhost
```

```
127.0.0.1       localhost
192.168.30.15   SRV-GRAYLOG.technova.local      SRV-GRAYLOG

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

6) Il faudra également lier la machine au domaine technova.local.
7) Définir le serveur de temps suivant : timedatectl set-timezone Europe/Paris
8) Pensez à placer la machine dans le bon OU sur SRV-AD

Partie 3 - Identifiants et mots de passe

Nom	Identifiant	Mot de passe
Interface Graylog (défaut)	admin	Gromulax88!
Interface Graylog	aplantier	Zirkama63kk?
SRV-GRAYLOG (DEBIAN)	armel root	armel root

Partie 4 - Déploiement de Graylog et ses modules

Nous allons commencer par mettre à jour le cache des paquets ainsi que l'installation d'outils nécessaire pour la suite.

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

Sous partie 1 : Configuration de MongoDB

Téléchargez la clé GPG correspondante au dépôt MongoDB (version 7.0) :

```
curl -fsSL https://www.mongodb.org/static/pgp/server-7.0.asc | gpg -o
/usr/share/keyrings/mongodb-server-7.0.gpg --dearmor
```

Il faudra ensuite l'ajouter sur la machine :

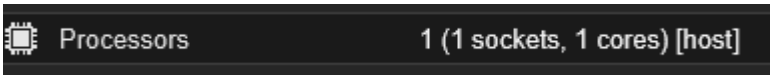
```
echo "deb [trusted=yes] http://repo.mongodb.org/apt/debian
bookworm/mongodb-org/7.0 main" | tee
/etc/apt/sources.list.d/mongodb-org.list
```

Une fois cela fait il faudra remettre à jour le cache des paquets et installer MongoDB

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

Avant d'effectuer des actions sur le service, il faudra activer "avx".

⚠️ : Penser à mettre le processeur en mode "host" sur proxmox.



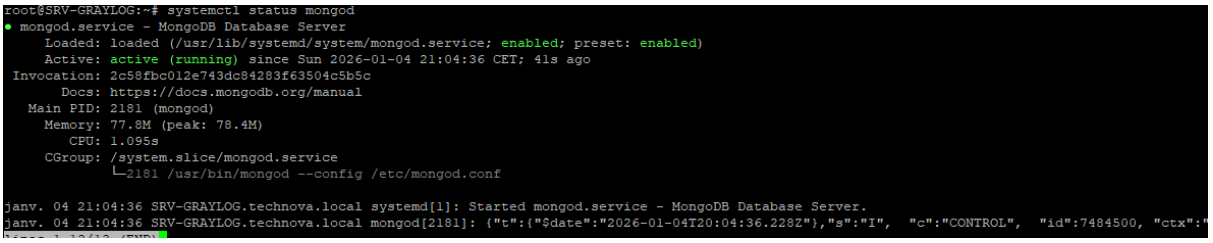

```
grep -o 'avx' /proc/cpuinfo
```

Une fois l'installation terminée, nous allons devoir relancer le service MongoDB et activer son démarrage automatique au lancement de la machine Debian.

```
systemctl daemon-reload
systemctl enable mongod.service
systemctl restart mongod.service
systemctl --type=service --state=active | grep mongod
```

Afin de vérifier si notre service est bien lancé on peut faire :

```
systemctl status mongod.service
```



Sous partie 2 : Configuration d'OpenSearch

Nous allons à présent installer OpenSearch. Commençons par l'ajout de la clé de signature pour les paquets d'OpenSearch :

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

Il faudra ensuite ajouter le dépôt OpenSearch afin de télécharger le paquet :

```
echo "deb [trusted=yes] https://artifacts.opensearch.org/releases/bundle/opensearch/2.x/apt stable main" | tee /etc/apt/sources.list.d/opensearch-2.x.list
```

Une fois cela fait, mettre à jour le cache de paquets :

```
apt update
```

Nous allons installer OpenSearch en définissant le mot de passe par défaut du compte Administrateur. Dans notre cas, il s'agira de "Gromulax88!".

```
env OPENSEARCH_INITIAL_ADMIN_PASSWORD="Gromulax88!" apt-get install -y opensearch
```

Une fois l'installation terminée, nous allons ouvrir le fichier de configuration afin d'effectuer la configuration minimale.

```
nano /etc/opensearch/opensearch.yml
```

A l'intérieur de ce fichier, ajoutez les lignes suivantes :

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

⚠️Certaines lignes sont déjà présentes mais commentées. Vous pouvez les décommenter ou alors ajouter l'ensemble à la fin du fichier. Enregistrez et fermez ce fichier.

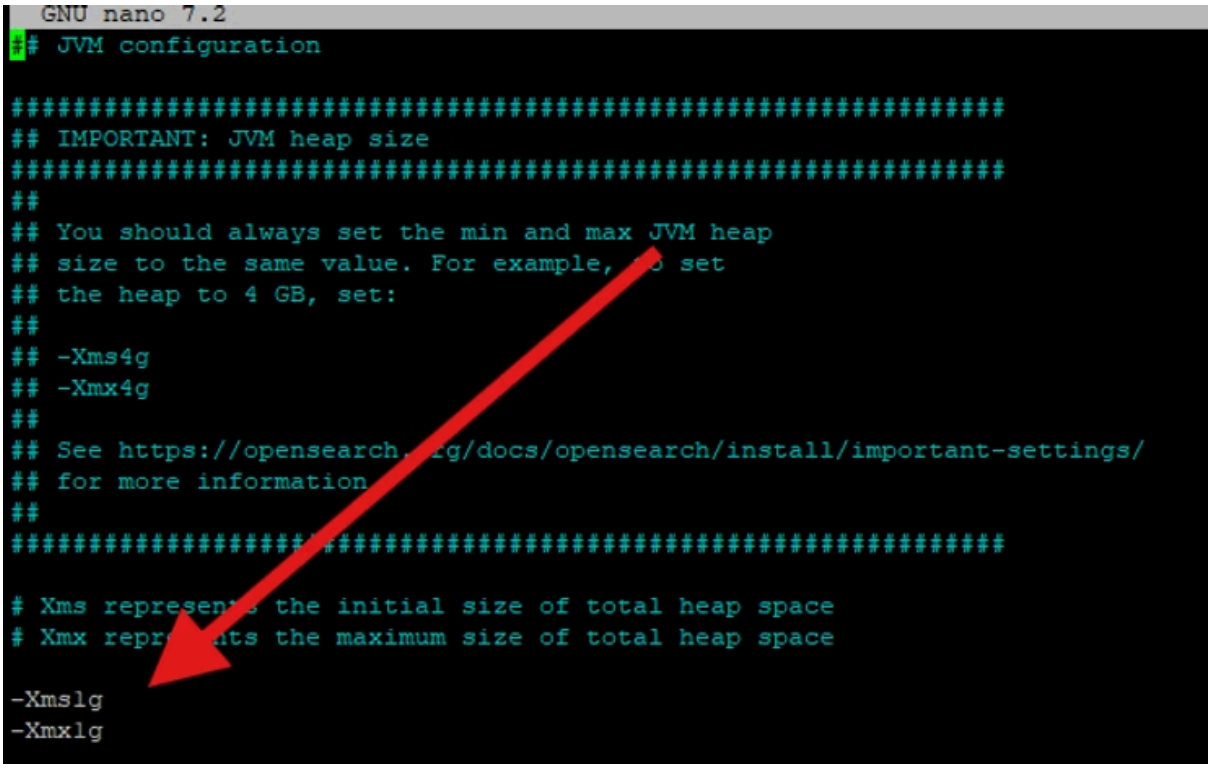
Enregistrez et fermez ce fichier.

Sous partie 3 : Configuration de Java (JVM)

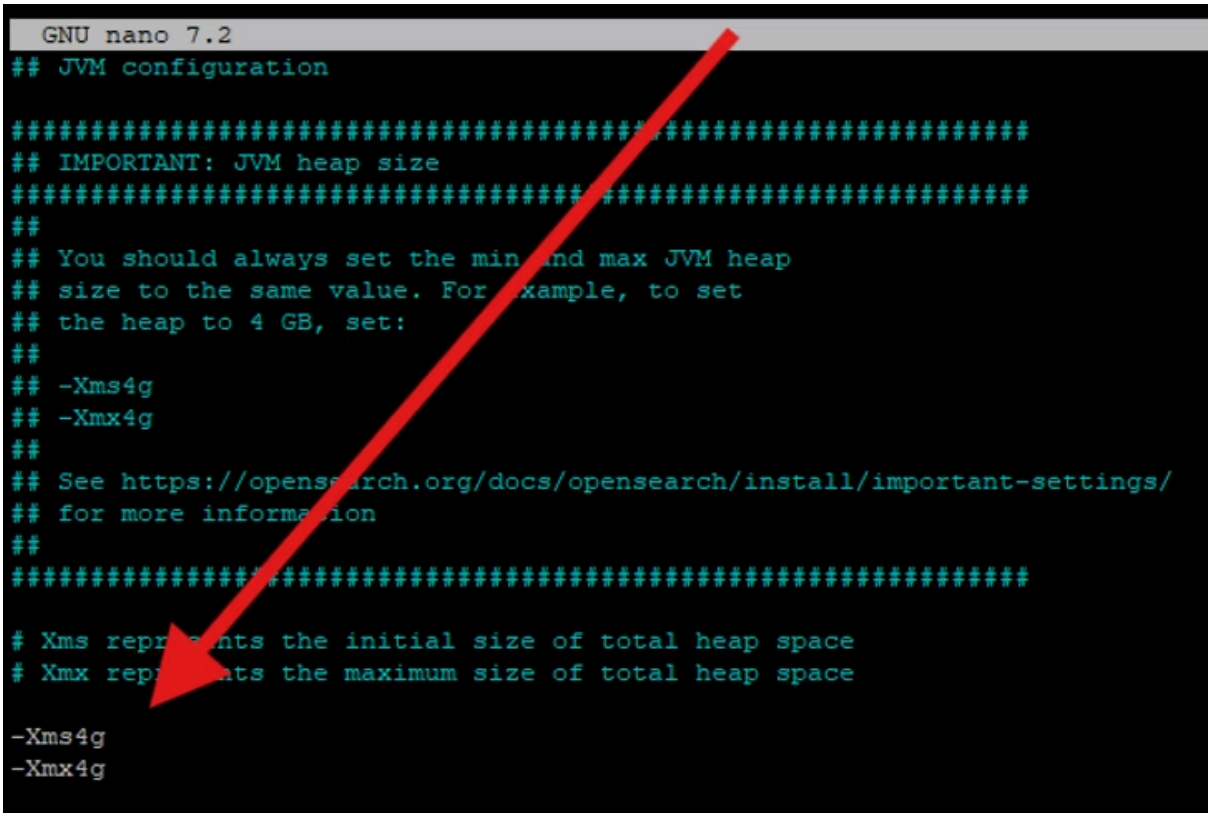
Il va falloir configurer Java Virtual Machine utilisé par OpenSearch afin d'ajuster la quantitée de mémoire utilisé par le service :

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

Nous avons alloué 8go à notre machine, et sur ces 8go nous voulons attribuer que 4go pour OpenSearch. Il faudra alors changer les paramètres suivant :



Par ceux-ci :



Il faudra ensuite enregistrer et fermer le fichier. Nous allons également vérifier la configuration du paramètre “max_map_count” qui définit la limite des zones de mémoire mappés par processus.

Nous allons fixer cette valeur à 262144 pour éviter les erreurs liées à la gestion de la mémoire.

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

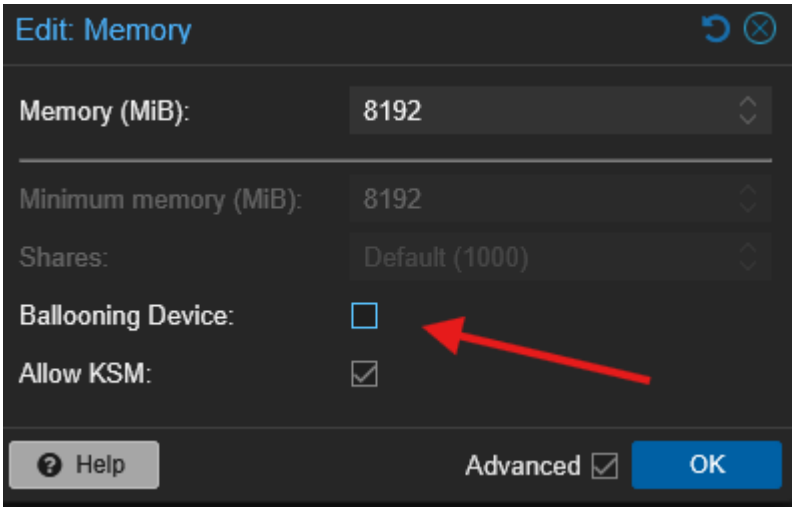
Nous allons ensuite terminer par désactiver le démarrage automatique d’OpenSearch et lancer le service associé.

```
systemctl daemon-reload
```

```
systemctl enable opensearch
```

```
systemctl restart opensearch
```

Il n’est pas impossible qu'à cette étape vous rencontreriez une erreur vous indiquant que vous n’avez pas assez de mémoire pour Java. Il faudra aller dans les paramètres de votre hyperviseur, et désactiver la mémoire dynamique.



Il faut donc décocher la case.

Votre OpenSearch aura correctement démarré :

```
root@SRV-GRAYLOG:~# systemctl restart opensearch
root@SRV-GRAYLOG:~# systemctl status opensearch
● opensearch.service - OpenSearch
     Loaded: loaded (/usr/lib/systemd/system/opensearch.service; enabled; preset: enabled)
     Active: active (running) since Sun 2026-01-04 21:31:44 CET; 3s ago
 Invocation: 3bd04184bd0142eeadfb2096d514a1c4
       Docs: https://opensearch.org/
   Main PID: 2956 (java)
      Tasks: 54 (limit: 9472)
     Memory: 4.3G (peak: 4.3G)
        CPU: 39.939s
     CGroup: /system.slice/opensearch.service
             └─2956 /usr/share/opensearch/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networkaddress.cache.nega
```

⚠️ : Le redémarrage peut parfois prendre 2 ou 3 minutes.

Vous allez pouvoir vérifier que java est bien été créée et comporte 4go de ram via la commande suivante :

```
top
```

```
top - 16:24:54 up  1:27,  2 users,  load average: 0,07, 0,20, 0,09
Tâches: 105 total,   1 en cours, 104 en veille,   0 arrêté,   0 zombie
%Cpu(s):  0,0 ut,  0,0 sy,  0,0 ni,100,0 id,  0,0 wa,  0,0 hi,  0,0 si,  0,0 st
MiB Mem :   7940,1 total,    185,5 libr,   5016,3 util,   3007,9 tamp/cache
MiB Éch :    977,0 total,    9[illegible]7 libr,      0,3 util.   2923,8 dispo Mem

    PID UTIL.      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TEMPS+ COM.
   2552 root       20   0       0      0      0 I   0,0   0,0   0:00.07 kworker/0:0-events
   2567 root       20   0       0      0      0 I   0,0   0,0   0:00.02 kworker/2:1-mm_percpu_wq
   2570 root       20   0       0      0      0 I   0,0   0,0   0:00.21 kworker/u8:1-events_unbound
   2728 root       20   0       0      0      0 I   0,0   0,0   0:00.11 kworker/u8:0-flush-8:0
   2730 root       20   0       0      0      0 I   0,0   0,0   0:00.02 kworker/2:0-events
   2732 root       20   0       0      0      0 I   0,0   0,0   0:0[illegible] kworker/u8:2-events_unbound
   3263 opensea+   20   0 8107824   4,4g  26660 S   0,0  56,8   1:02.90 java
   3498 root       20   0       0      0      0 I   0,0   0,0   0:00.01 kworker/u8:3-events_unbound
   3499 root       20   0       0      0      0 I   0,0   0,0   0:00.00 kworker/u8:4
   3500 root       20   0       0      0      0 I   0,0   0,0   0:00.04 kworker/u8:5-events_unbound
   3503 root       20   0       0      0      0 I   0,0   0,0   0:00.00 kworker/2:2-mm_percpu_wq
   3511 root       20   0   11708   5228   3304 R   0,0   0,1   0:01.65 top
```

Nous allons pouvoir passer à la dernière étape, l'installation de Graylog

TECHNOVA

Sous partie 4 : Installation de Graylog

Nous allons télécharger Graylog dans sa version 6.1

```
wget
https://packages.graylog2.org/repo/packages/graylog-6.2-repository_latest.deb
```

```
dpkg -i graylog-6.2-repository_latest.deb
```

```
apt update
apt install graylog-server
```

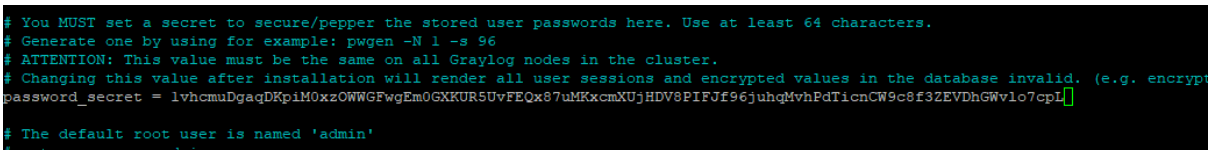
Avant de vouloir lancer Graylog, nous avons deux options à configurer. Le “passsword_secret” : C’est ce mot de passe qui est utilisé par Graylog pour sécuriser le stockage des mots de passe des utilisateurs. Elle doit être unique et aléatoire Le “root_password_sha2” : C’est le mot de passe par défaut de l’administrateur dans Graylog. Il est stocké sous forme d’un hash SHA-256 Pour le “password_secret” nous allons générer une clé de 96 caractères :

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

Copiez le résultat puis ouvrez le fichier suivant :

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

On va venir coller la clé à l’endroit prévu dans le fichier



Enregistrez et fermez le fichier.

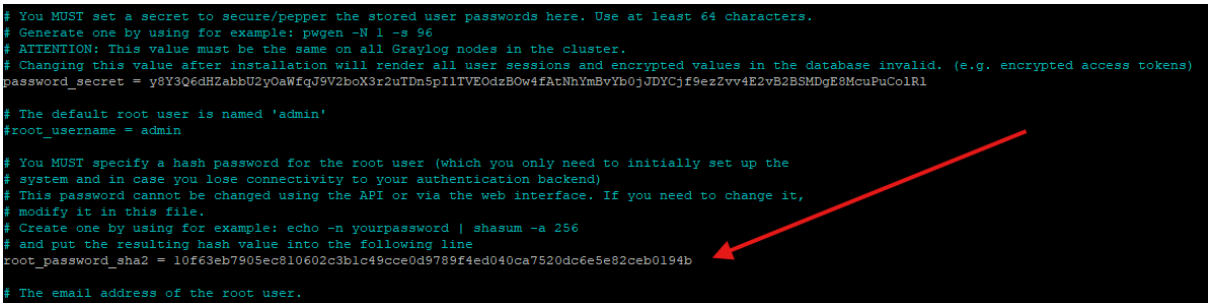
Pour le mot de passe secret :

```
echo -n "Gromulax88!" | shasum -a 256
```

Copiez la valeur retourné puis retirez le “-” à la fin.Le résultat est celui ci :

```
4cd4200c8b7abf59bfe5ce70a1c2ed56a75e041f1c89205d9401c0bab7e0d844
```

On retourne dans le fichier de configuration Graylog puis on va venir coller le mot de passe hashé à l'endroit prévu :



Profitez d'être dans ce fichier pour terminer la configuration :

Nous allons indiquer que l'interface web de Graylog soit accessible sur le port 9000 via toutes les IP La ligne est donc :

```
http_bind_address = 0.0.0.0:9000
```

Nous allons configurer l'option "elasticsearch_hosts" qui permet de déclarer notre instance locale OpenSearch.

Nous allons mettre la ligne suivante :

```
elasticsearch_hosts = http://127.0.0.1:9200
```

Une fois cela fait, enregistrez et fermez le fichier.

Nous allons activer Graylog pour qu'il démarre seul au prochaine démarrage de la machine

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

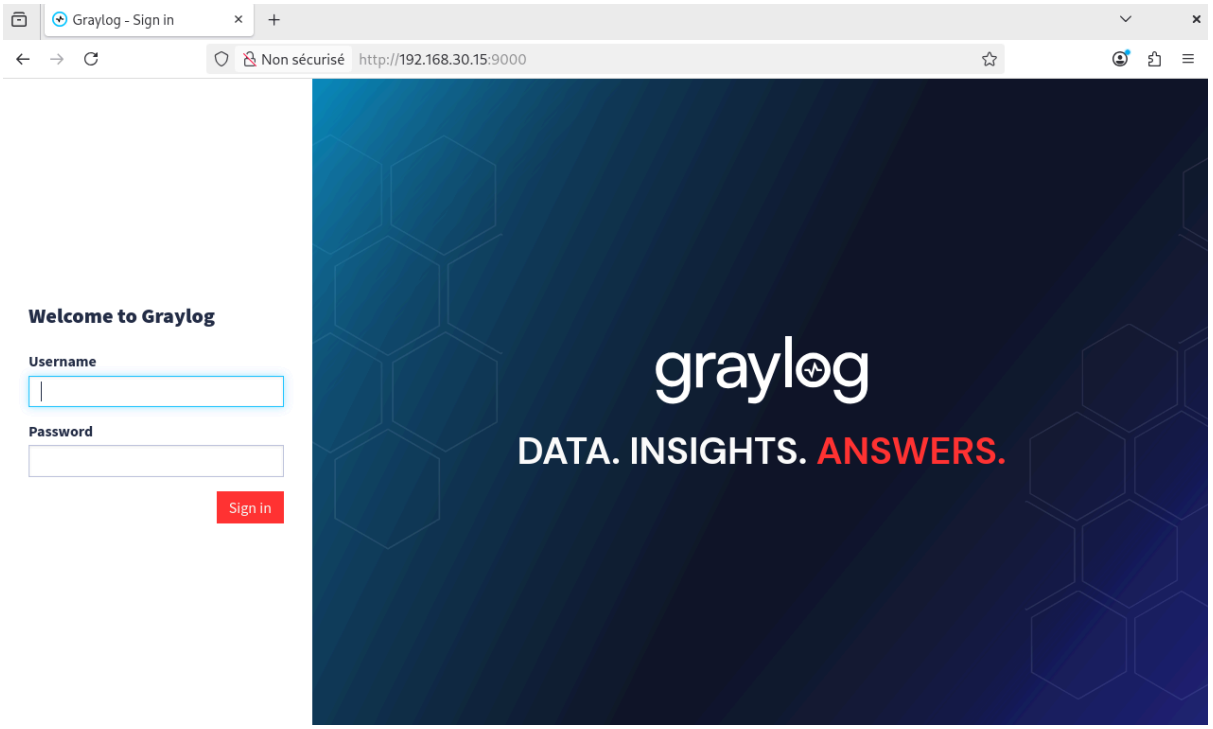
Avant la connexion à l'interface web, on peut vérifier que le service a bien démarré et au besoin redémarrer graylog :

```
systemctl restart graylog-server
```

```
systemctl status graylog-server.service
```

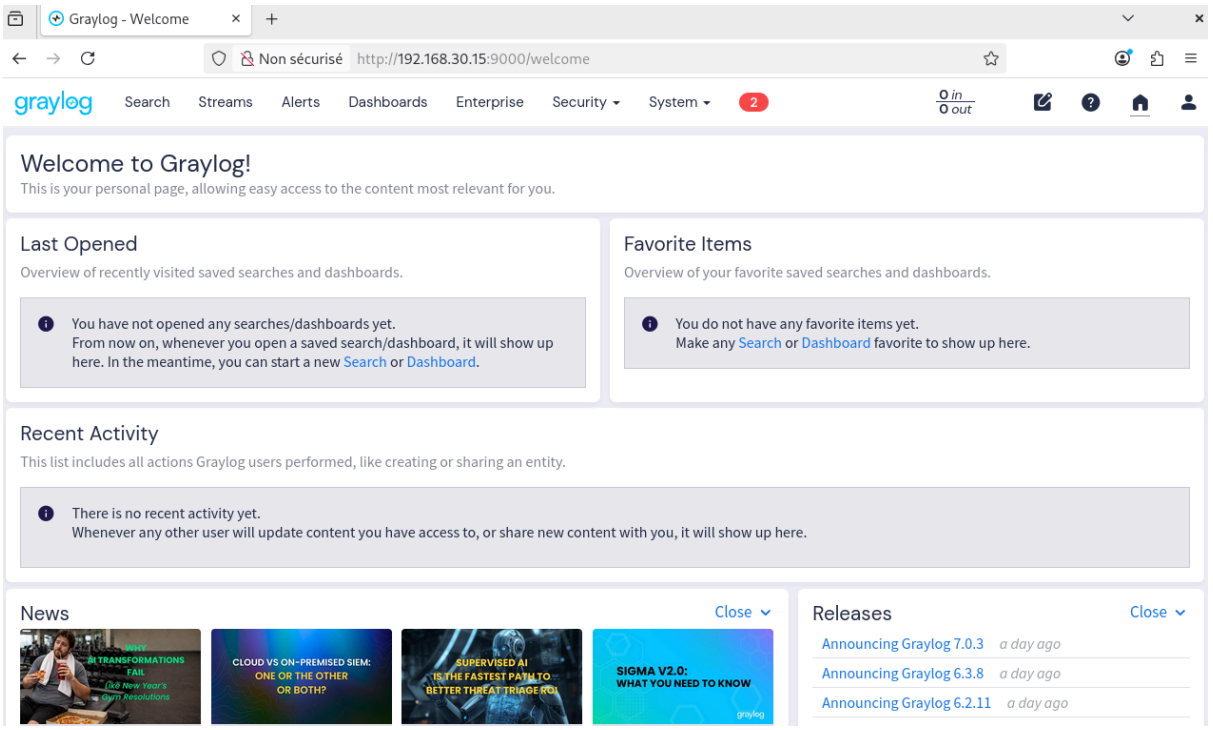
Nous allons alors pouvoir entrer l'adresse IP de notre serveur dans un navigateur pour nous connecter à l'interface graphique de Graylog. Il ne faudra pas oublier le port.

```
http://192.168.30.15:9000
```



Sous partie 5 : Configuration minimale de Graylog

Nous allons devoir nous connecter à l'interface à l'aide des identifiants présentés dans la partie mot de passe de la procédure.



Vous êtes désormais connecté à l'interface web de Graylog. Cependant pour plus de sécurité, nous voulons créer un compte utilisateur pour ne pas utiliser celui par défaut.

System → Users and Teams → Create user

First Name : Armel
Last Name : Plantier
Username : aplantier
E-Mail Address : aplantier@technova.local
Assign Roles : Admin
Password : Zirkama63kk?

Partie 5 : Envoie de log Linux sur Graylog via rsyslog

Nous allons paramétrer l'envoie de log depuis des machines linux, vers notre serveur Graylog.

Sous partie 1 : Création d'un Input pour Syslog

System → Inputs → Select input → Syslog TCP → Launch new input

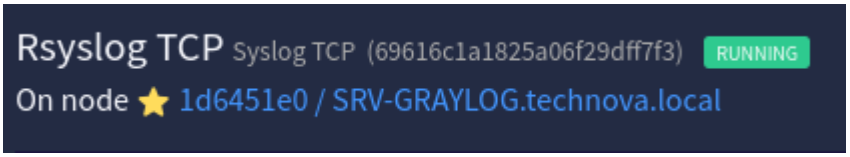
1) Title : Rsyslog TCP
2) Port : 1514
3) Store full message : Cochez la case

→ Launch Input

Vous devez retrouver ceci :

```
allow_override_date: true
bind_address: 0.0.0.0
charset_name: UTF-8
expand_structured_data: false
force_rdns: false
max_message_size: 2097152
number_worker_threads: 1
override_source: <empty>
port: 1514
recv_buffer_size: 1048576
store_full_message: true
tcp_keepalive: false
timezone: NotSet
tls_cert_file: <empty>
tls_client_auth: disabled
tls_client_auth_cert_file: <empty>
tls_enable: false
tls_key_file: <empty>
tls_key_password:********
use_null_delimiter: false
```

L'input doit être démarré :



Sous partie 2 : Création d'un index Linux

→ System → Indices → Create index set

Title : Linux Index
Description : Index pour les journaux Linux
Index prefix : linux_index

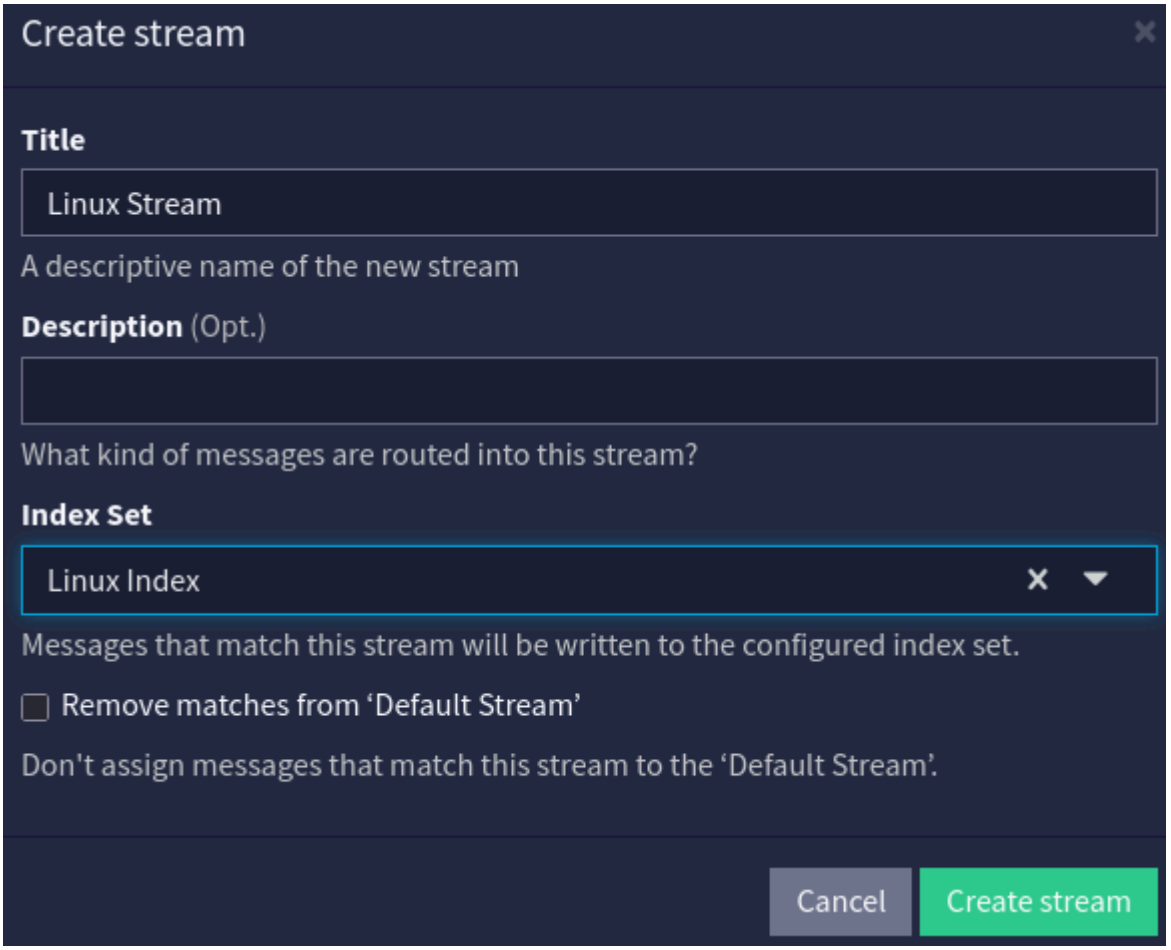
Il faudra ensuite valider avec "Create index set"

Sous partie 3 : Création d’un Stream

Pour créer le stream il faudra respecter les étapes suivantes :

Steams → Create stream :

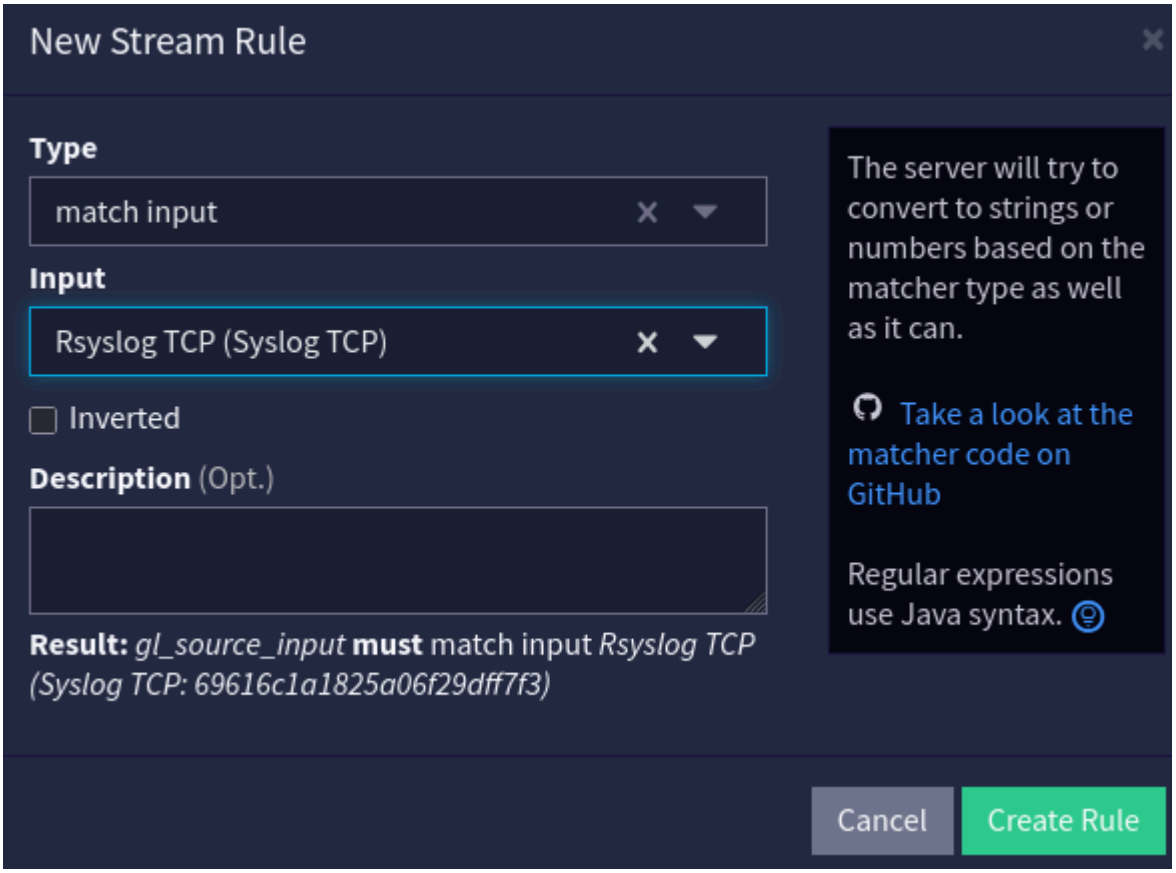
1) Title : Linux Stream
2) Index Set : Linux Index



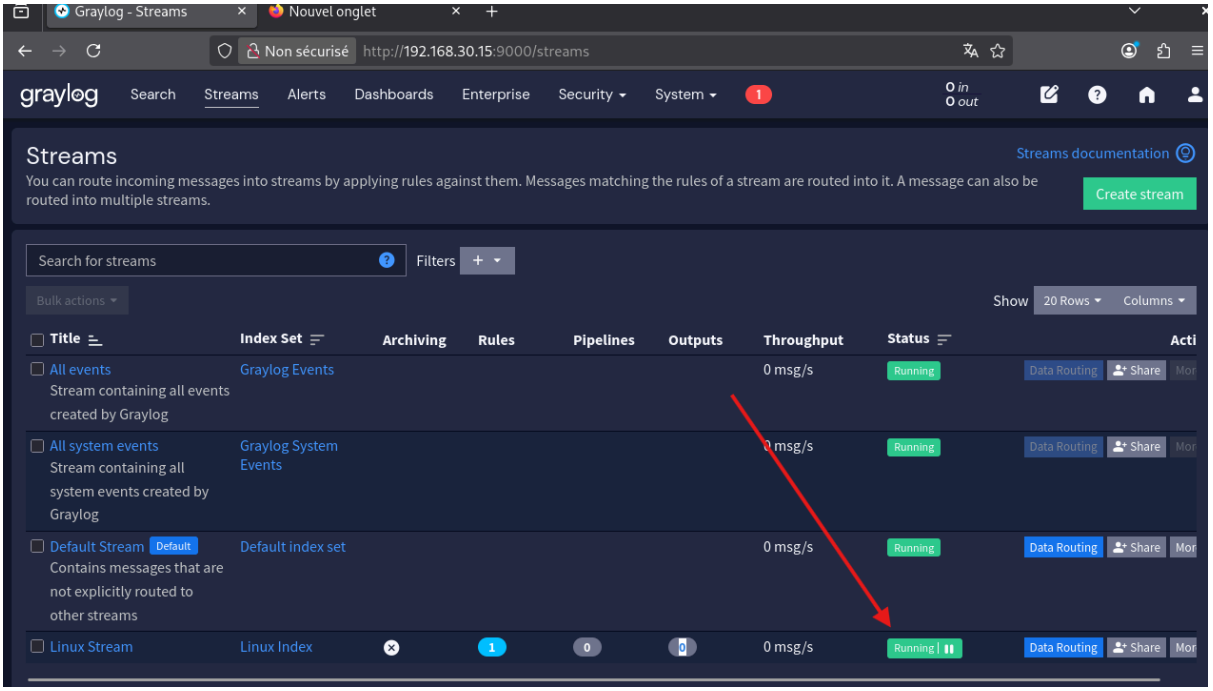
Il faudra ensuite créer le stream.

Ajoutons ensuite ensuite une règle de routage des messages :

→ More → Manage rules → Add stream rule



Votre nouveau Stream doit s'afficher dans la liste et il doit être sur l'état "Running". La bande passante de message indique "0 msg/s" car pour le moment, nous n'envoyons aucun journal vers l'Input Rsyslog UDP. Pour voir les journaux d'un stream, cliquez simplement sur son nom.



Tout est prêt du côté de Graylog. Passons à la suite, à savoir la configuration de la machine Linux.

Sous partie 4 : Installer et configurer Rsyslog sur Linux

Connectez-vous à la machine Linux et utilisez un compte utilisateur disposant des permissions pour élever ses privilèges (via sudo). Sinon, utilisez directement le compte "root".

Nous utiliserons le TNV-01

```
apt update
```

```
apt install rsyslog -y
```

On vérifiera l'état du service :

```
systemctl status rsyslog
```

On va pouvoir le configurer :

Rsyslog dispose d'un fichier de configuration principal situé à cet emplacement :

```
/etc/rsyslog.conf
```

En complément, le répertoire "/etc/rsyslog.d/" est utilisé pour stocker des fichiers de configuration supplémentaires pour Rsyslog. Dans le fichier de configuration principal, il y a une directive Include permettant d'importer tous les fichiers ".conf" situés dans ce répertoire. Ceci permet d'avoir des fichiers complémentaires pour configurer Rsyslog sans modifier le fichier principal.

Dans ce répertoire, vous devez utiliser des numéros pour définir l'ordre de chargement, parce que le chargement des fichiers se fait dans l'ordre alphabétique. Ainsi, le fait d'ajouter un préfixe numérique permet de gérer la priorité entre plusieurs fichiers de configuration. Ici, nous n'aurons qu'un seul fichier complémentaire, donc ce n'est pas gênant.

Dans ce répertoire, nous allons créer le fichier intitulé "10-graylog.conf" :

```
nano /etc/rsyslog.d/10-graylog.conf
```

Il faudra insérer cette ligne :

```
*.* @@192.168.30.15:1514;RSYSLOG_SyslogProtocol23Format
```

1) *.* : signifie qu'on doit envoyer tous les logs Syslog de la machine Linux vers Graylog
2) @ : indique que le transport est effectué en UDP. Il convient de préciser "@@" pour basculer en TCP.

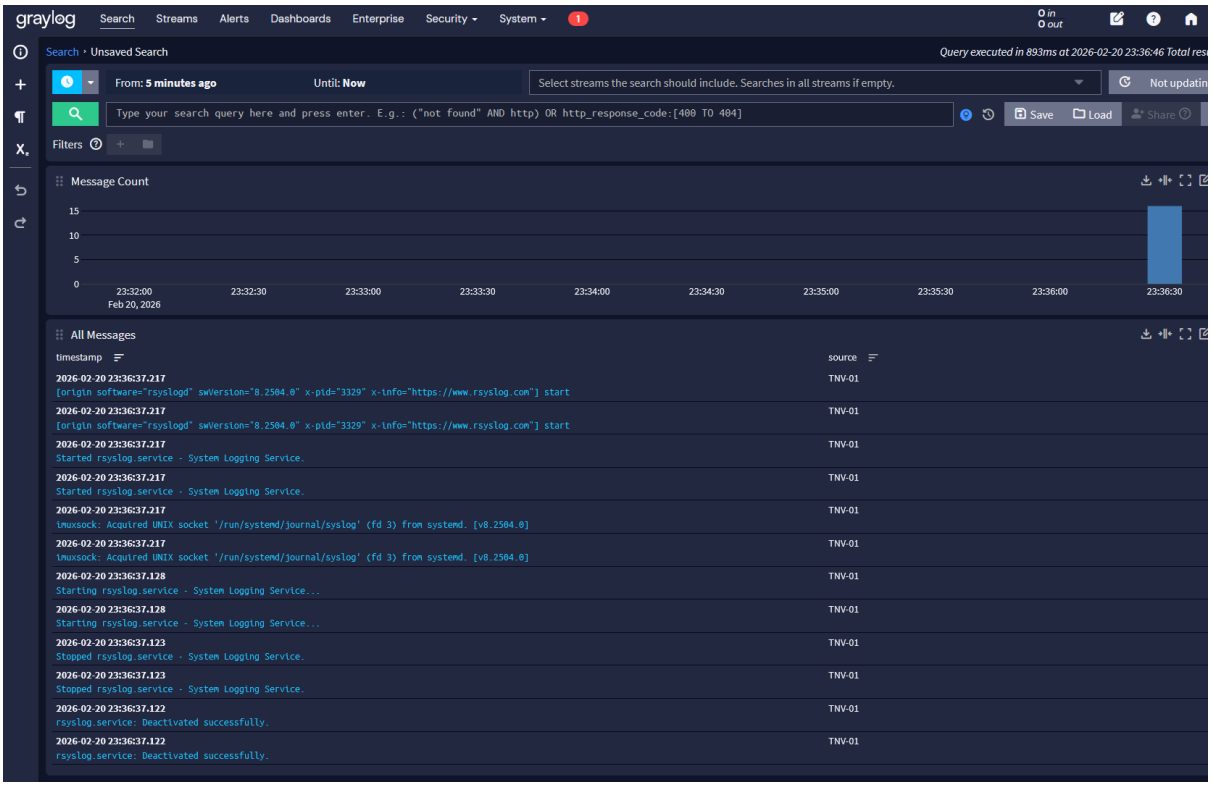
3) 192.168.10.220:1514 : indique l'adresse du serveur Graylog, ainsi que le port sur lequel on envoie les logs (correspondant à l'Input).

4) RSYSLOG_SyslogProtocol23Format : correspond au format des messages que l'on veut envoyer à Graylog.

```
systemctl restart rsyslog.service
```

Sous partie 5 : Afficher les logs Linux dans Graylog

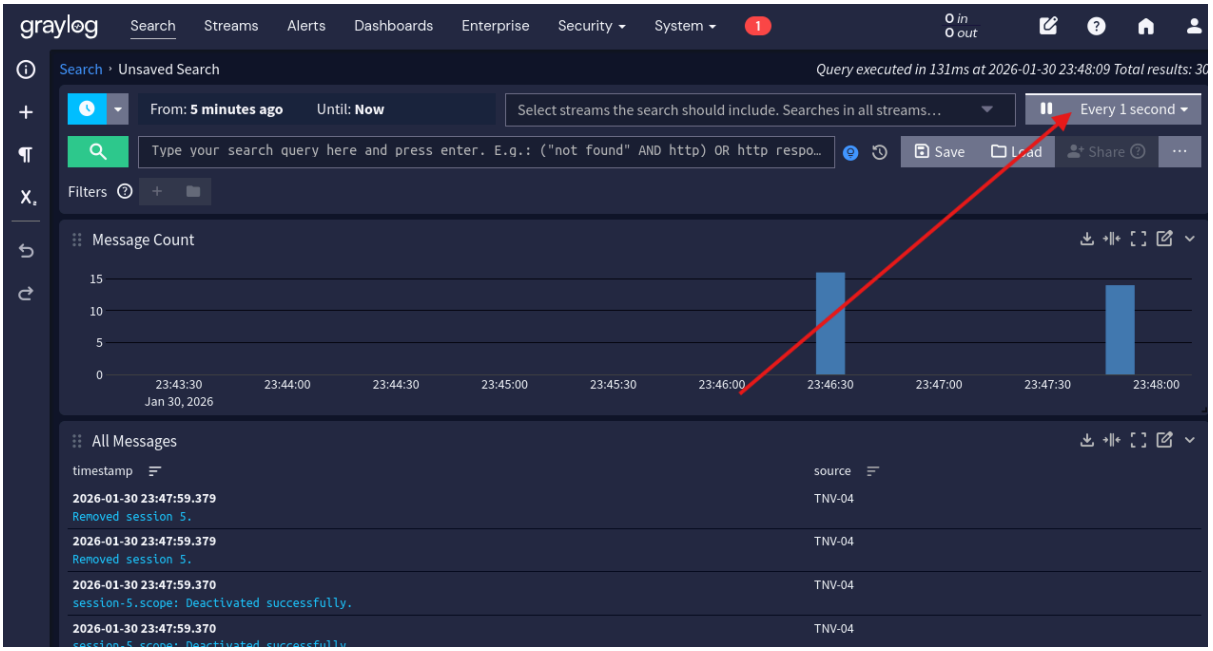
À partir de Graylog, vous pouvez cliquer sur "Streams" et sélectionner votre nouveau stream pour afficher les messages associés. Sinon, cliquez sur "Search" et effectuez la sélection de votre Steam et lancez une recherche.



Sous partie 6 : Identifier un échec de connexion SSH

A partir du TNV-01 (ou rsyslog est configuré) nous allons tenter une connexion SSH avec un mot de passe erroné.

Il faudra bien penser à définir le temps de rafraîchissement sur l'interface web :



Une fois la connexion tenté, nous devons apercevoir ceci :

Vous apercevez bien la connexion ssh qui à échoué et que le mot de passe entré n'est pas correcte.

Partie 6 : Envoie de log Windows Server sur Graylog via NXLog

Sous partie 1 : Créer un input NXLog dans Graylog

System → Inputs → GELF TCP → Launch new input

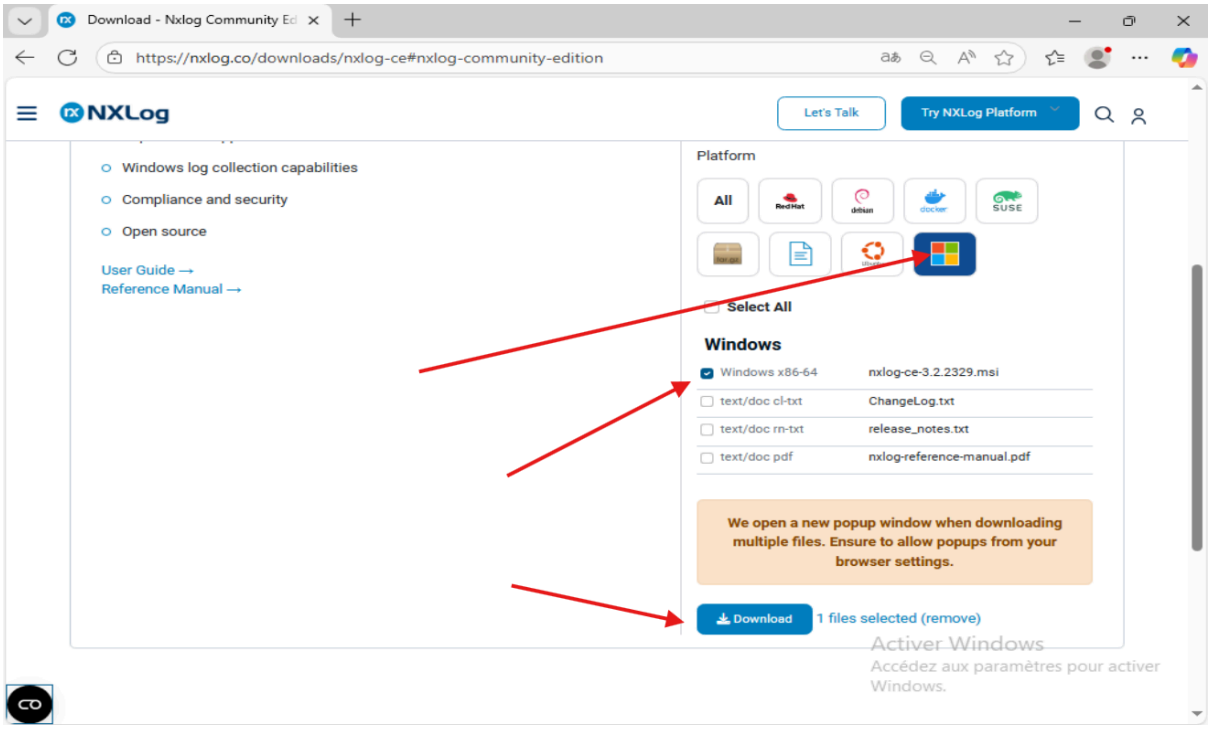
Title : NXLog TCP

→ Launch Input

L’input doit être en mode “running”

Sous partie 2 : Installer NXLOG sur Windows Server

Nous allons nous connecter sur notre SRV-AD puis il faudra télécharger NXLog via ce lien : https://nxlog.co/downloads/nxlog-ce#nxlog-community-edition



Il faudra ensuite exécuter le setup et suivre les instructions.

NXLog étant installé sur la machine, nous pouvons éditer son fichier de configuration situé à l'emplacement suivant :

```
C:\Program Files\nxlog\conf\nxlog.conf
```

En complément de la configuration déjà présente dans le fichier "nxlog.conf", vous devez ajouter ces lignes à la fin :

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

# Déclarer le serveur Graylog
<Extension gelf>
    Module        xm_gelf
</Extension>

# Sortie vers Graylog en TCP
<Output graylog_tcp>
    Module        om_tcp
    Host          192.168.30.15
    Port          12201
```

```
    OutputType    GELF_TCP
</Output>

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

1) **im_msvistalog** : il s'agit du module déclaré comme entrée (Input) pour récupérer les journaux dans l'Observateur d'événements de Windows, compatible à partir de Windows Server 2008 et Windows Vista. Il est toujours compatible avec les dernières versions, à savoir Windows 11 et Windows Server 2025. Pour les versions antérieures à Windows Server 2008, utilisez le module "im_mseventlog"

2) **om_udp** : il s'agit du module déclaré comme sortie (Output graylog_tcp). Dans ce bloc, vous devez modifier l'adresse IP, car elle correspond au serveur Graylog (192.168.0.220) et éventuellement le port. Nous utilisons le type de sortie "GELF_TCP" pour rester cohérent vis-à-vis de l'Input déclaré dans Graylog.

3) **Route 1** : il s'agit d'une règle « de routage » dans NXLog pour prendre ce qui correspond à l'Input "in" (les logs Windows) et les envoyer vers la sortie "graylog_tcp", à savoir notre Graylog.

Sauvegardez les changements et redémarrez le service NXLog à partir d'une console PowerShell ouverte en tant qu'administrateur (ou via la console Services).

```
Restart-Service nxlog
```

Sous partie 3 : Affinage des règles de collecte de NXLog

Par défaut, NXLog va envoyer tous les événements de tous les journaux de Windows vers notre puits de logs Graylog. Il est possible d'affiner la configuration de NXLog, de façon très précise, pour envoyer les events de certains journaux uniquement ou ceux correspondants à certains critères.

Ce lien peut être utile : https://docs.nxlog.co/userguide/configure/filtering.html

Voici un exemple, où nous venons modifier l'Input dans la configuration de NXLog pour transmettre à Graylog uniquement les événements du journal "Sécurité".

La configuration sera alors comme ceci :

```
# Récupérer les journaux de l'observateur d'événements (Filtre Sécurité
```

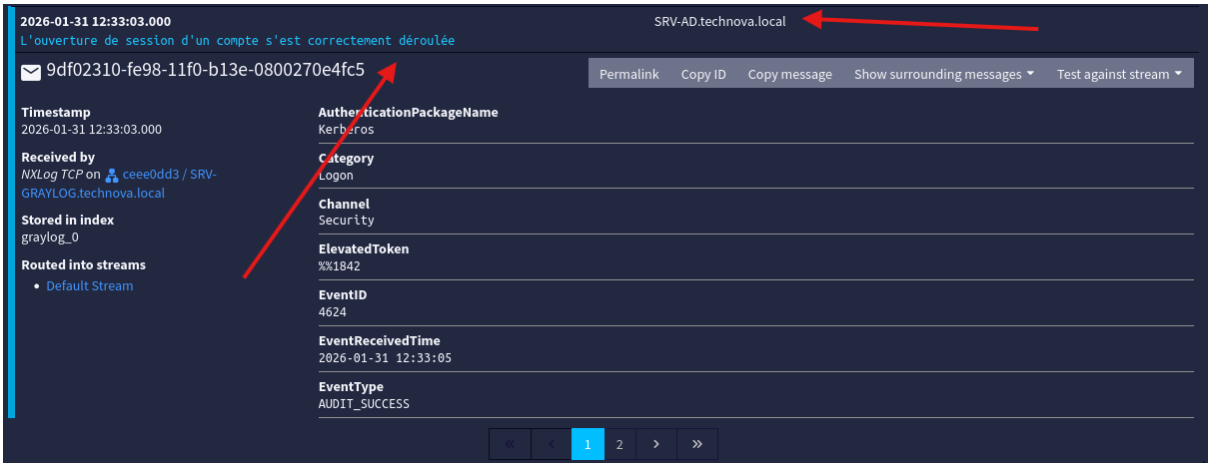
```
uniquement)
<Input in>
    Module      im_msvistalog
    <QueryXML>
        <QueryList>
            <Query Id='1'>
                <Select Path='Security'>*</Select>
            </Query>
        </QueryList>
    </QueryXML>
</Input>

# Déclarer le serveur Graylog
<Extension gelf>
    Module        xm_gelf
</Extension>

# Sortie vers Graylog en TCP
<Output graylog_tcp>
    Module        om_tcp
    Host          192.168.30.15
    Port          12201
    OutputType    GELF_TCP
</Output>

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

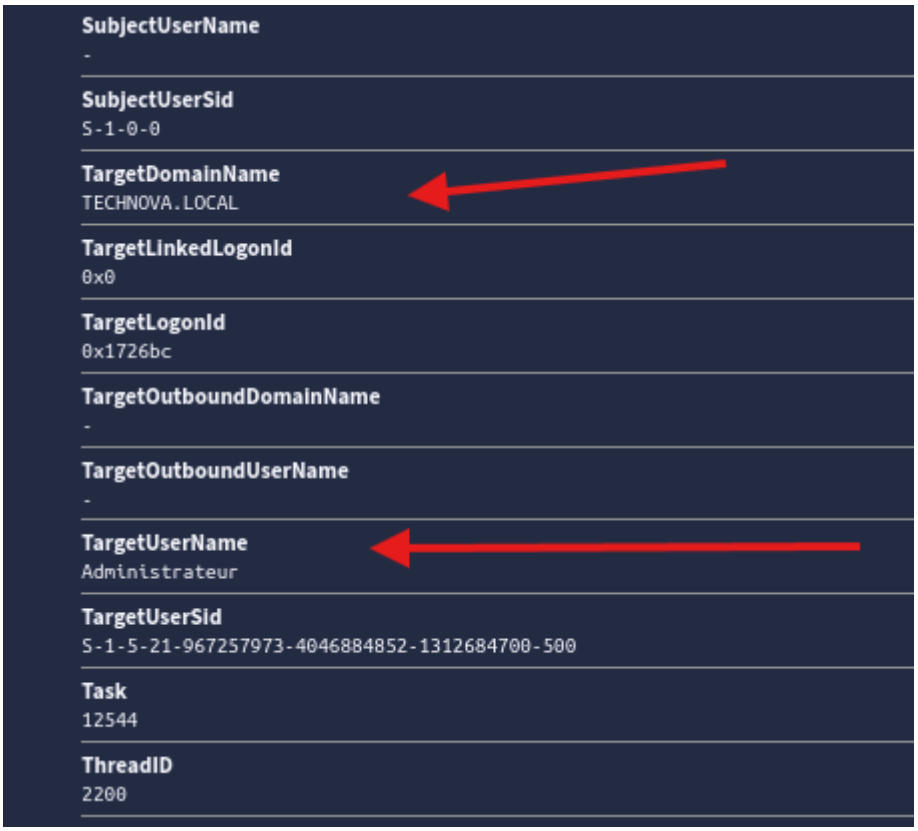
```
Restart-Service nxlog
```

Sous partie 4 : Vérification de la réception des logs

Suite à la configuration de Graylog et de l'agent NXLog sur la machine Windows, les journaux doivent désormais être envoyés vers Graylog ! Pour le vérifier, cliquez simplement sur "Search" dans le menu de Graylog.

Vous devriez voir de premiers journaux arriver, ce qui aura pour effet de faire un pic de logs. Je vous recommande de cliquer sur le bouton mis en évidence sur l'image ci-dessous pour rafraîchir la liste automatiquement toutes les 5 secondes (par défaut).
L'image ci dessous provient d’un log de connexion au compte “Administrateur” sur le PC-01





Nous avons bien nos logs qui remontent.

Partie 7 : Envoie de log Windows Client sur Graylog via NXLog

Cette partie demande davantage de configuration car nous voulons déployer NXLog sur l'ensemble des postes clients. Nous allons automatiser la tâche par GPO.

Nous voulons donc installer NXLog ainsi qu'avoir le bon fichier de configuration. Cela se fera à l'aide de notre partage "Deploy" créée dans une procédure précédente.

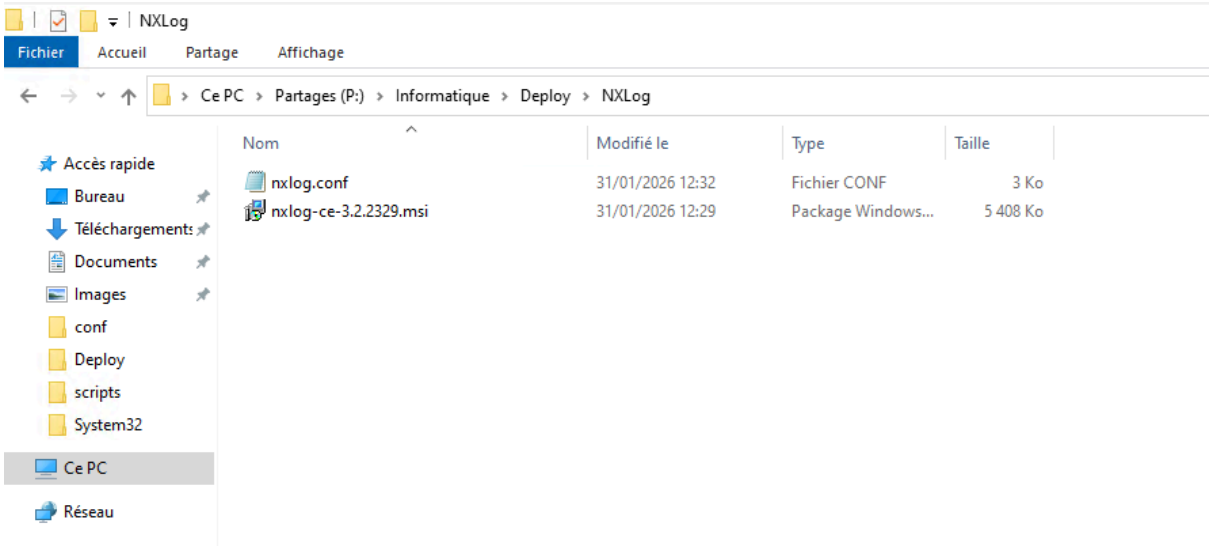
Sous partie 1 : Configuration du partage

Nous allons donc commencer par déposer le fichier d'installation NXLog :

```
P:\Informatique\Deploy\NXLog\nxlog-ce-3.2.2329.msi
```

Il faudra ensuite ajouter le fichier de configuration dans le dossier NXLog

⚠️ : Attention à bien désactiver l'héritage dans les options de partages du dossier NXLog



Pour rappel, voici le contenu du fichier :

```
Panic Soft
#NoFreeOnExit TRUE

define ROOT     C:\Program Files\nxlog
define CERTDIR  %ROOT%\cert
define CONFDIR  %ROOT%\conf\nxlog.d
define LOGDIR   %ROOT%\data

include %CONFDIR%\\*.conf
define LOGFILE  %LOGDIR%\nxlog.log
LogFile %LOGFILE%

Moduledir %ROOT%\modules
CacheDir  %ROOT%\data
```

```
Pidfile   %ROOT%\data\nxlog.pid
SpoolDir  %ROOT%\data

<Extension _syslog>
    Module      xm_syslog
</Extension>

<Extension _charconv>
    Module      xm_charconv
    AutodetectCharsets iso8859-2, utf-8, utf-16, utf-32
</Extension>

<Extension _exec>
    Module      xm_exec
</Extension>

<Extension _fileop>
    Module      xm_fileop

    # Check the size of our log file hourly, rotate if larger than 5MB
    <Schedule>
        Every   1 hour
        Exec    if (file_exists('%LOGFILE%') and \
                   (file_size('%LOGFILE%') >= 5M)) \
                    file_cycle('%LOGFILE%', 8);
    </Schedule>

    # Rotate our log file every week on Sunday at midnight
    <Schedule>
        When    @weekly
        Exec    if file_exists('%LOGFILE%') file_cycle('%LOGFILE%', 8);
    </Schedule>
</Extension>

# Snare compatible example configuration
# Collecting event log
# <Input in>
#     Module      im_msvistalog
# </Input>
#
# Converting events to Snare format and sending them out over TCP syslog
# <Output out>
#     Module      om_tcp
#     Host        192.168.1.1
#     Port        514
```

```
#     Exec        to_syslog_snare();
# </Output>
#
# Connect input 'in' to output 'out'
# <Route 1>
#     Path        in => out
# </Route>

# Récupérer les journaux de l'observateur d'événements (Filtre Sécurité
uniquement)
<Input in>
    Module      im_msvistalog
    <QueryXML>
        <QueryList>
            <Query Id='1'>
                <Select Path='Security'>*</Select>
            </Query>
        </QueryList>
    </QueryXML>
</Input>

# Déclarer le serveur Graylog
<Extension gelf>
    Module        xm_gelf
</Extension>

# Sortie vers Graylog en TCP
<Output graylog_tcp>
    Module        om_tcp
    Host          192.168.30.15
    Port          12201
    OutputType    GELF_TCP
</Output>

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

La partie concernant le partage est prête.

Sous partie 2 : Configuration de la GPO

Nous allons utiliser la GPO “GPO_Deploy_Logiciel” déjà présente sur l’OU “02_Postes_de_Travai”

Notre GPO est prête à être modifié :

Configuration ordinateur → Stratégies → Paramètres du logiciel → Installation de logiciel → Clique droit → Nouveau → Package

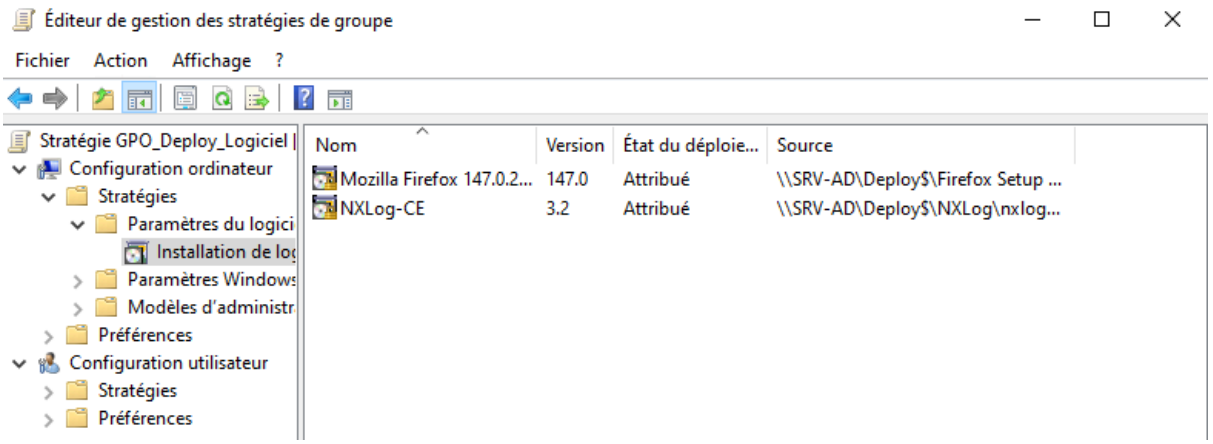
Il faudra ensuite se connecter au partage :

```
\\SRV-AD\Deploy$\NXLog
```

⚠️ : L'héritage doit être activé.

Il faudra ensuite sélectionner le fichier nxlog.msi

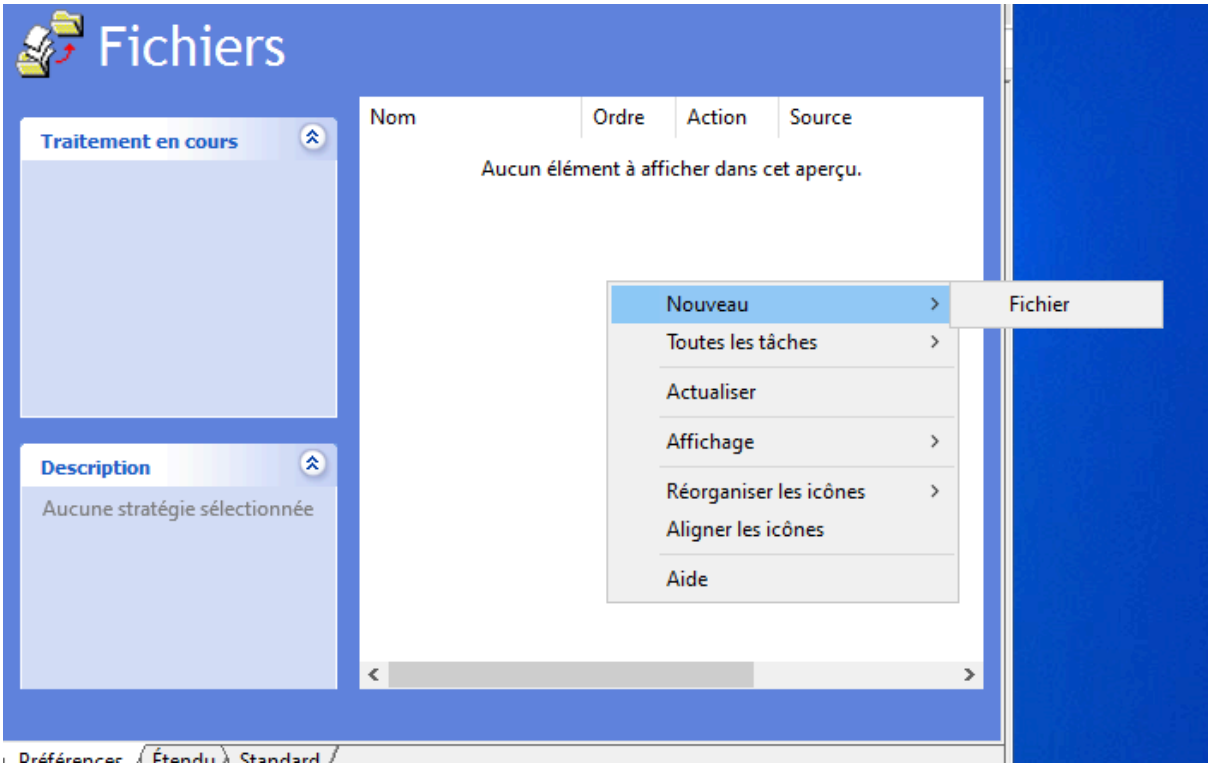
→ Mode Attribué



La configuration de l’installation est terminée, il faut ensuite configurer le déploiement du fichier de configuration.

Dans la même fenêtre :

Configuration ordinateur → Préférences → Paramètres Windows → Fichiers



Action : Remplacer
Fichier source : \\SRV-AD\Deploy$\NXLog\nxlog.conf
Fichier de destination : C:\Program Files\nxlog\conf\nxlog.conf

→ Ok

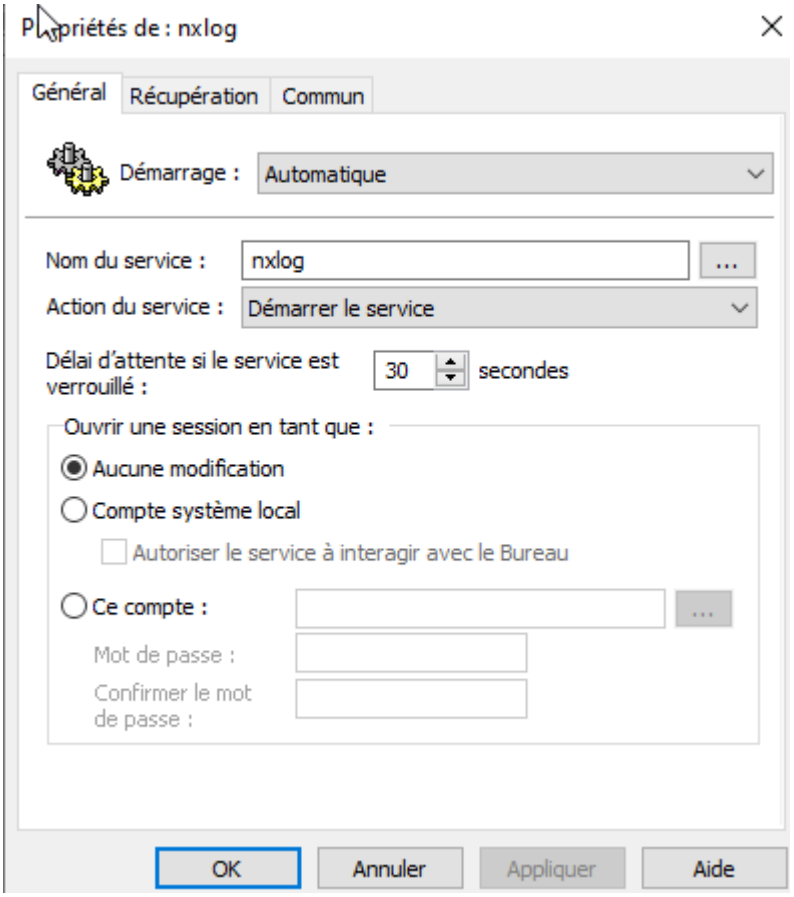
Il faudra juste configurer le démarrage automatique du service NXLog :

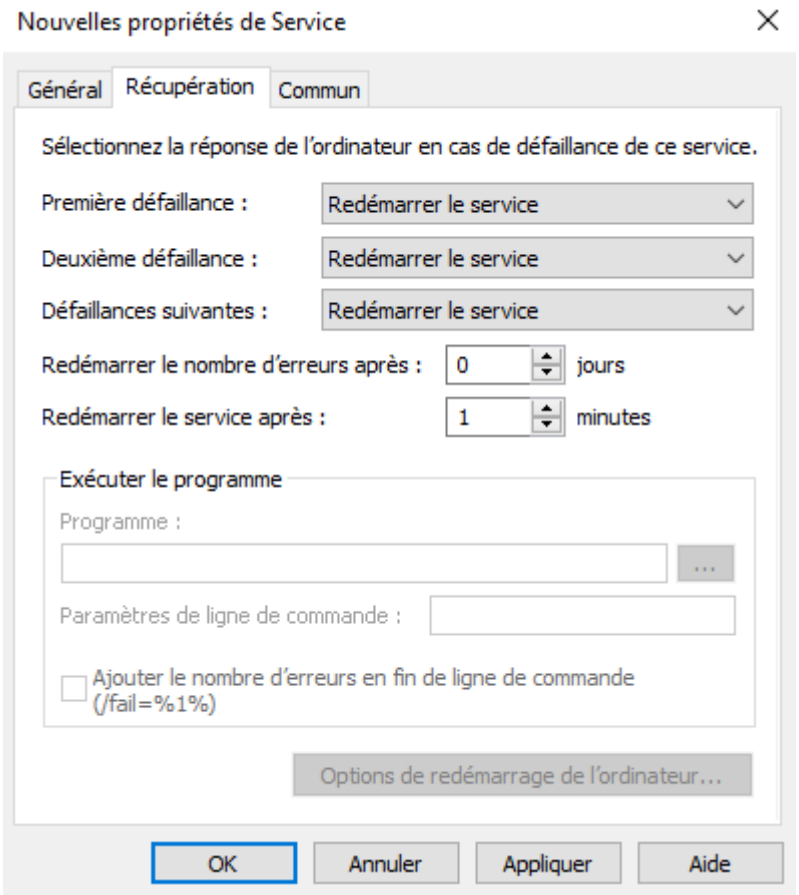
Configuration ordinateur → Préférences → Paramètres du panneau de configuration → Services

Il faudra ensuite suivre les étapes suivantes :

Nouveau → Service :

Démarrage : Automatique
Nom du service : nxlog
Action du service : Démarrer le service
Onglet “Récupération” : Redémarrer le service (pour les 3 options)


Propriétés de : nxlog
Général
Récupération
Commun
Démarrage :
Automatique
Nom du service :
nxlog
Action du service :
Démarrer le service
Délai d'attente si le service est verrouillé :
30
secondes
Ouvrir une session en tant que :
Aucune modification
Compte système local
Autoriser le service à interagir avec le Bureau
Ce compte :
Mot de passe :
Confirmer le mot de passe :
OK
Annuler
Appliquer
Aide


Nouvelles propriétés de Service
Général
Récupération
Commun
Sélectionnez la réponse de l'ordinateur en cas de défaillance de ce service.
Première défaillance :
Redémarrer le service
Deuxième défaillance :
Redémarrer le service
Défaillances suivantes :
Redémarrer le service
Redémarrer le nombre d'erreurs après :
0
jours
Redémarrer le service après :
1
minutes
Exécuter le programme
Programme :
Paramètres de ligne de commande :
Ajouter le nombre d'erreurs en fin de ligne de commande (/fail=%1%)
Options de redémarrage de l'ordinateur...
OK
Annuler
Appliquer
Aide

Pour terminer la configuration de la GPO, nous allons modifier le Pare-feu des PC Clients.

Configuration ordinateur → Stratégies → Paramètres Windows → Paramètres de sécurités → Pare-feu Windows Defender avec fonctions avancées → Règles de trafic sortant → Nouvelle règle

1) Port
2) TCP et Ports dist. spéc. : 12201
3) Autoriser la connexion
4) Cochez : Domaine / Privé / Public
5) Nom : Graylog Output

Sous partie 3 : Vérification finale de la GPO

Pour tester sur un PC Client :

1. Allumez un PC client
2. Ouvrez une invite de commande (CMD) en admin et tapez : gpupdate /force.
3. Redémarrez le PC. (L'installation de logiciel ne se fait qu'au démarrage, avant l'écran de login).
    - Note : Le démarrage sera un peu plus long que d'habitude ("Installation du logiciel géré...").
4. Une fois connecté :
    - Vérifiez que le dossier C:\Program Files\nxlog existe.
    - Vérifiez que le fichier nxlog.conf à l'intérieur est bien le vôtre (regardez l'IP 192.168.30.15 dedans).

On remarque bien l'arrivé de log sur Graylog

```
timestamp                                                        source
2026-02-21 15:20:31.000                                          TNV-02.technova.local
Privilèges spéciaux attribués à la nouvelle ouverture de ses
2026-02-21 15:20:31.000                                          TNV-02.technova.local
L'ouverture de session d'un compte s'est correctement déroulée
2026-02-21 15:19:19.000                                          TNV-02.technova.local
Privilèges spéciaux attribués à la nouvelle ouverture de ses
2026-02-21 15:19:19.000                                          TNV-02.technova.local
L'ouverture de session d'un compte s'est correctement déroulée
2026-02-21 15:17:23.000                                          TNV-02.technova.local
Privilèges spéciaux attribués à la nouvelle ouverture de ses
2026-02-21 15:17:23.000                                          TNV-02.technova.local
L'ouverture de session d'un compte s'est correctement déroulée
2026-02-21 15:17:23.000                                          TNV-02.technova.local
Privilèges spéciaux attribués à la nouvelle ouverture de ses
2026-02-21 15:17:23.000                                          TNV-02.technova.local
L'ouverture de session d'un compte s'est correctement déroulée
2026-02-21 15:17:23.000                                          TNV-02.technova.local
Privilèges spéciaux attribués à la nouvelle ouverture de ses
2026-02-21 15:17:23.000                                          TNV-02.technova.local
L'ouverture de session d'un compte s'est correctement déroulée
2026-02-21 15:17:22.000                                          TNV-02.technova.local
Privilèges spéciaux attribués à la nouvelle ouverture de ses
2026-02-21 15:17:22.000                                          TNV-02.technova.local
L'ouverture de session d'un compte s'est correctement déroulée
```