Service

- GLPI
- NextCloud
- Rsyslog et Loganalyzer
- NETBOX
- WINDOWS server

GLPI

Mise en place de glpi sur un serveur lap

apt install apache2

apt install php-{mysql,mbstring,curl,gd,xml,intl,ldap,apcu,xmlrpc,zip,bz2} -y

cd /var/www/

mkdir glpi

cd /etc/apache2/sites-available/

cp default-ssl.conf glpi-sssl.conf

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/glpi.key -out /etc/ssl/certs/glpi.crt
```

nano glpi-ssl.conf

```
<VirtualHost *:80>
        ServerName glpi.gsb.sio.jja
        Redirect permanent / https://glpi.gsb.sio.jja/
</VirtualHost>


<VirtualHost *:443>
        ServerAdmin webmaster@localhost
        ServerName glpi.gsb.sio.jja
        DocumentRoot /var/www/glpi/glpi

<Directory /var/www/glpi/glpi>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
</Directory>

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf

        #   SSL Engine Switch:
        #   Enable/Disable SSL for this virtual host.
        SSLEngine on

        #   A self-signed (snakeoil) certificate can be created by installing
        #   the ssl-cert package. See
        #   /usr/share/doc/apache2/README.Debian.gz for more info.
        #   If both key and certificate are stored in the same file, only the
        #   SSLCertificateFile directive is needed.
        SSLCertificateFile      /etc/ssl/certs/glpi.crt
        SSLCertificateKeyFile   /etc/ssl/private/glpi.key

        #   Server Certificate Chain:
```

a2enmode ssl

systemctl restart apache2

a2ensite glpi-ssl.conf

systemctl restart apache2

cd /tmp

```
wget https://github.com/glpi-project/glpi/releases/download/10.0.19/glpi-10.0.19.tgz
```

```
tar -xvzf glpi-10.0.19.tgz -C /var/www/glpi
```

```
# chown -R www-data /var/www/html_
```

```
e# chown -R www-data /var/www/glpi
```

a2dissite 000-default.conf

systemctl restart apache2

Pour enlever les erreur annexes avec php cookie etc:

Sur la bdd :

create database db_glpi;

```
GRANT ALL PRIVILEGES ON db_glpi.* TO admindb_glpi@'192.168.90.2' IDENTIFIED BY 'caribou';
FLUSH PRIVILEGES;
```

Étape 1 : Supprimer le fichier d’installation

Chemin :
`/var/www/html/glpi/install/install.php` *(ou* `/var/www/html/install/install.php` *si GLPI est à la racine)*

Commande (terminal) :

bash

Copier

```
sudo rm /var/www/html/glpi/install/install.php
```

> ⚠ Vérifiez d’abord que GLPI est bien installé et fonctionnel avant de supprimer ce fichier.

Étape 2 : Modifier la configuration PHP (`php.ini`)

Chemin du fichier `php.ini` (dépend de votre serveur) :

- Apache + PHP-FPM : `/etc/php/8.x/apache2/php.ini`
- Nginx + PHP-FPM : `/etc/php/8.x/fpm/php.ini`
  (Remplacez `8.x` par votre version de PHP, ex: `8.1`, `8.2`)

Ouvrir le fichier :

bash

Copier

```
sudo nano /etc/php/8.2/apache2/php.ini
```

Chercher et modifier :

ini

Copier

```
session.cookie_secure = On
session.cookie_httponly = On
```

> Si les lignes sont commentées (`;` au début), retirez le `;`.

NextCloud

INSTALLATION ET MISE EN PLACE DE NEXTCLOUD

L’installation sur les machine :

——————————————————————————————

Légende :

Rouge = commande

Vert = fichier de configuration

Noire = Explication

——————————————————————————————

Mise à jour de Debian 12

Mettre à jour la liste des paquets disponibles

sudo apt update Mettre à jour les paquets installés sudo apt upgrade -y

Mettre à jour les paquets installés

sudo apt upgrade -y

——————————————————————————————

Installation d'Apache

Installation des paquets Apache

sudo apt install apache2 -y

Démarrage du service Apache

sudo systemctl start apache2

Configuration du service pour qu’il soit actif à chaque reboot

sudo systemctl enable apache2

Confirmer le statut du service

systemctl status apache2

——————————————————————————————————————

Installation de MariaDB

Installation des paquets MariaDB

sudo apt install mariadb-server -y

Démarrage du service de base de données

sudo systemctl start mariadb

Configuration du service pour qu’il soit actif à chaque reboot

sudo systemctl enable mariadb

Confirmer le statut du service

——————————————————————————————————————

Installation de PHP

sudo apt install php php-cli php-mysql php-curl php-gd php-mbstring php-xml php-zip -y

——————————————————————————————————————

Téléchargement de Nextcloud

Se placer dans le répertoire des fichiers web Apache

cd /var/www/html

Télécharger la dernière version de unzip et Nextcloud

sudo apt install wget unzip -y
wget https://download.nextcloud.com/server/releases/latest.zip

Extraire l’archive

unzip latest.zip

Définir les bonnes permissions de fichier

sudo chown -R www-data:www-data nextcloud
sudo chmod -R 755 nextcloud

Supprimer l’archive téléchargée (optionnel)

rm latest.zip

———————————————————————————————————————

Création de la base de données pour Nextcloud

Connexion au serveur MariaDB

sudo mysql -u root -p

Dans MariaDB, exécuter

CREATE DATABASE nextclouddb;
GRANT ALL ON nextclouddb.* TO 'nextclouduser'@'localhost' IDENTIFIED BY 'votre_mot_de_passe';
FLUSH PRIVILEGES;
EXIT;

———————————————————————————————————————

Certif :

```
cp default-ssl.conf glpi-sssl.conf

openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/glpi.key -out /etc/ssl/certs/glpi.crt_
```

(a remplacer par le bon nom)

Configuration d'Apache pour Nextcloud

Créer un fichier de configuration pour Nextcloud

sudo nano /etc/apache2/sites-available/nextcloud.conf

Contenu du ficher de configuration

```
<VirtualHost *:80>
        ServerName next.marsallon.sio.jja
        Redirect permanent / https://next.marsallon.sio.jja/
</VirtualHost>



<VirtualHost *:443>
        ServerAdmin admin@next.marsallon.sio.jja
        DocumentRoot /var/www/html/nextcloud
        ServerName next.marsallon.sio.jja

        <Directory /var/www/html/nextcloud/>
                Options +FollowSymlinks
                AllowOverride ALL
                Require all granted
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/nextcloud_error.log
        CustomLog ${APACHE_LOG_DIR}/nextcloud_access.log combined

        SSLEngine on
        SSLCertificateFile /etc/ssl/certs/nexcloud.crt
        SSLCertificateKeyFile /etc/ssl/private/nextcloud.key




</VirtualHost>
```

Activer la configuration et les modules nécessaires

sudo a2ensite nextcloud.conf
 sudo a2enmod rewrite headers env dir mime

Le fichier dans le dns :

```
 GNU nano 7.2                                                    C
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns.marsallon.sio.jja. root.marsallon.sio.jja. (
                        20251124        ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.marsallon.sio.jja.
ns      IN      A       192.168.30.2
lamp    IN      A       192.168.30.3
lamp2   IN      A       192.168.30.4
lamp3   IN      A       192.168.30.5
lamp4   IN      A       192.168.30.6
glpi    IN      CNAME   lamp
HA      IN      CNAME   lamp3
mood    IN      CNAME   lamp2
next    IN      CNAME   lamp4
```

———————————————————————————————————

Redémarrer le serveur Apache

sudo systemctl restart apache2

———————————————————————————————————

Pourquoi 443 (ssl) ? =

Port 443 est le port par défaut pour le protocole **HTTPS**, utilisé pour sécuriser les connexions web. Il permet de chiffrer les données échangées entre votre navigateur et un serveur web, protégeant ainsi les informations sensibles

Pourquoi Debian 12 :

Je posséder déjà une template debian12 j'ai donc fait un clone, de plus j'ai de l'expérience sur debian 12.

Pourquoi j'ai utilisé mysql : Mysql est efficace, facile a mettre en place, et j'ai de expérience avec.

Pourquoi apache2 : Apache2 est efficace, facile a mettre en place, et j'ai de expérience avec.

Pourquoi php : PHP est efficace, facile a mettre en place, et j'ai de expérience avec.

Rsyslog et Loganalyzer

Mise en Place de LOGANALYZER

apt update && apt upgrade

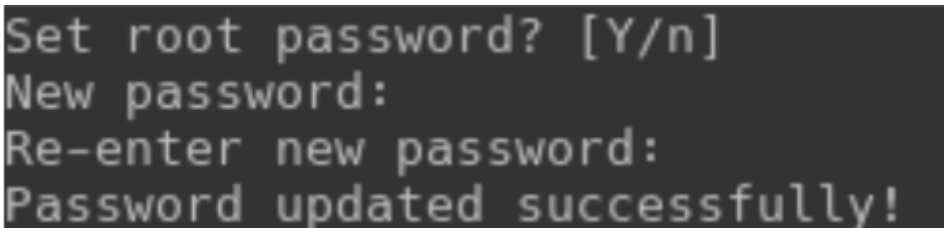
Ensuite, installez les services de base d'une pile « LAMP » (Linux Apache Mysql ou MariaDB PHP) et les modules de PHP nécessaires au bon fonctionnement de l'interface web Loganalyzer :

apt install apache2 mariadb-server php php-mysql php-gd

Sécurisez l'installation de mysql (mariadb) en définissant au compte root un mot de passe.

mysql_secure_installation

Ensuite on vous demande « Set root password ? [Y/n] ». Appuyez de nouveau sur la touche Entrée pour répondre « Oui » (Y = Yes) et définir un mot de passe pour l'utilisateur root (2 fois).

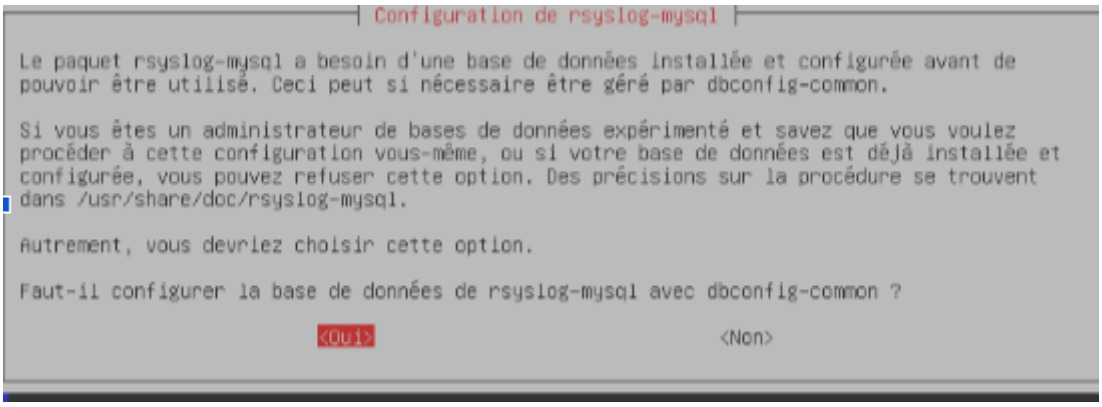


Password : Caribou

Pour toutes les questions qui suivront, appuyez sur Entrée pour valider.

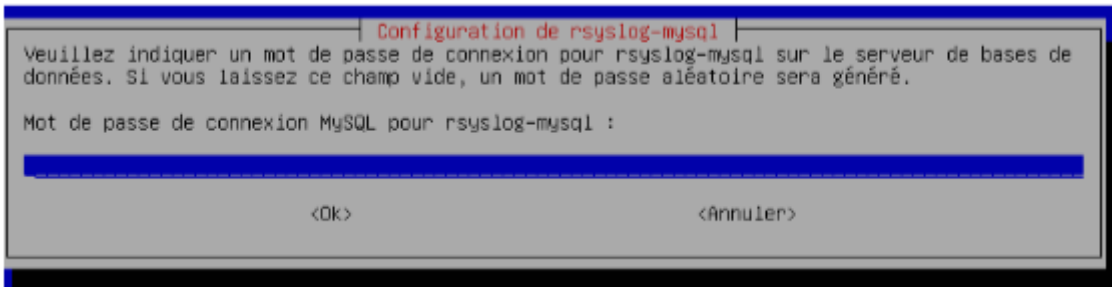
On termine la phase d'installation des services par le module mysql de rsyslog car nous allons héberger les journaux d'événements en base de données :

apt install rsyslog-mysql



Le dbconfig-common va alors s'occuper de créer une base de données appelée « Syslog » dont l'utilisateur « rsyslog » recevra les permissions adéquates pour interagir avec cette base.

Définissez un mot de passe pour l'utilisateur nommé « rsyslog » qui aura le contrôle total de la base de données Syslog :



Password : rsyslog

Poursuivons en activant la réception des logs sur le serveur dédié. Modifiez le fichier de configuration de rsyslog :

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

A la fin de ce même fichier, ajoutez la ligne suivante pour envoyer les logs directement à la base de données en renseignant le password que vous avez défini à l'utilisateur rsyslog à la place de « mdp user rsyslog » :

```
*.*
:ommysql:localhost,Syslog,rsyslog,rsyslog
```

Redémarrez le service rsyslog.

systemctl restart rsyslog

C'est tout pour la configuration de Rsyslog ! Passons maintenant à LogAnalyzer.

Placez vous dans le répertoire de votre choix, pour moi ça sera /tmp, et téléchargez la dernière version stable de LogAnalyzer.

```
cd /tmp
wget
http://download.adiscon.com/loganalyzer/loganalyzer-
4.1.13.tar.gz
```

Une fois le téléchargement terminé, **décompressez les fichiers** :

```
tar -zxvf /tmp/loganalyzer-4.1.13.tar.gz
```

D'abord sortez du répertoire : cd .., **puis créez un répertoire loganalyzer »** à la racine du serveur web.

```
mkdir /var/www/html/loganalyzer
```

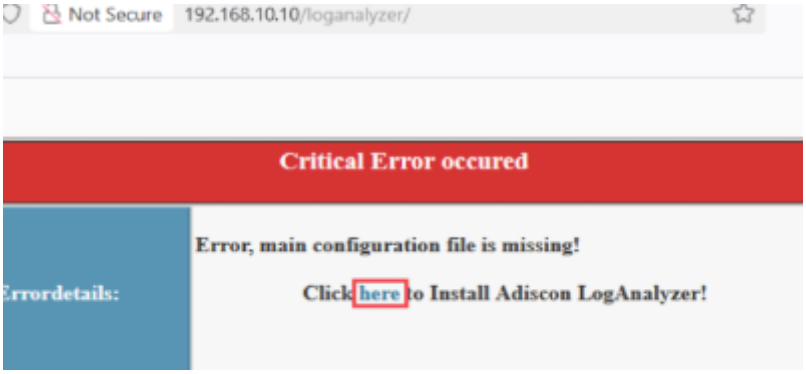
Copiez les fichiers requis dans ce nouveau répertoire :

```
cp -a /tmp/loganalyzer-4.1.13/src/*
/var/www/html/loganalyzer
```

```
chown -R www-data:www-data
/var/www/html/loganalyzer
```

Teste :

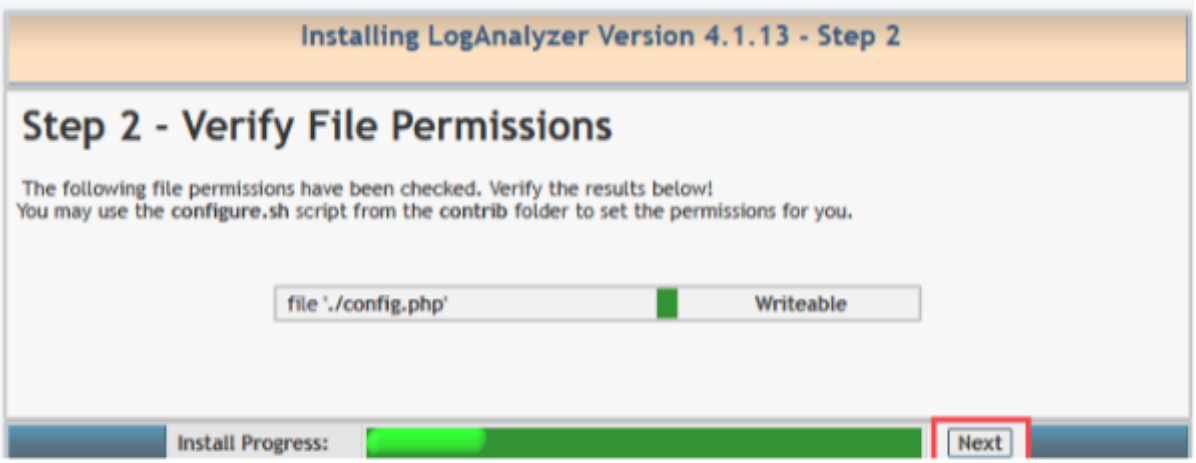
http://IP-serveur-syslog/loganayzer



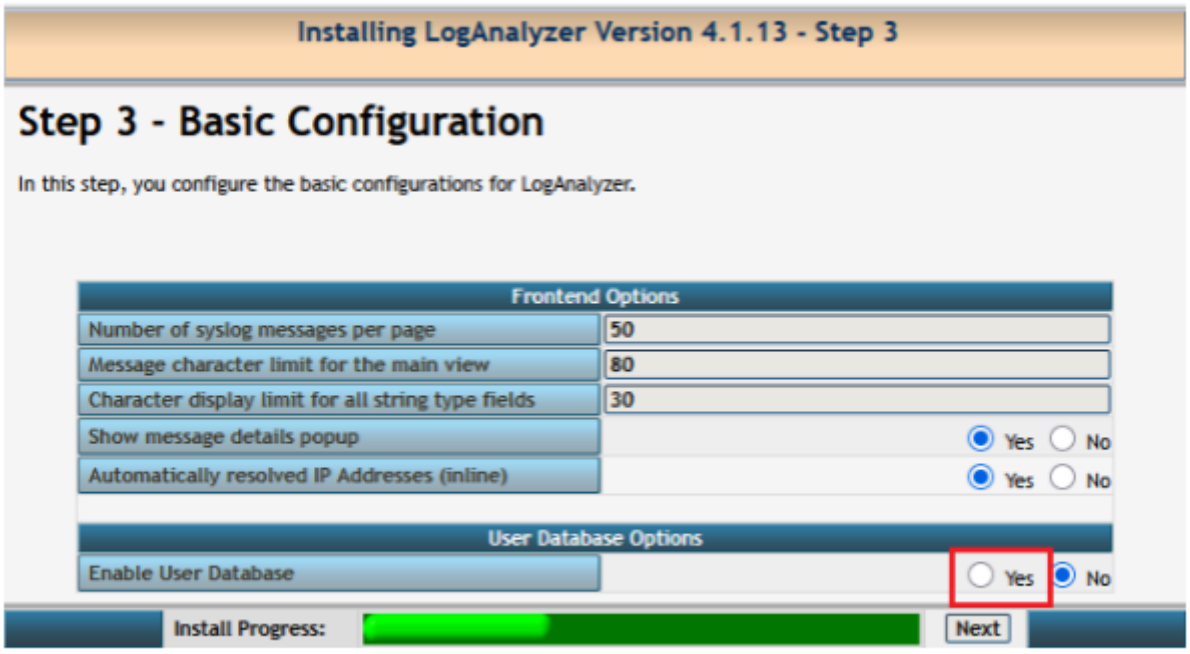
C’est NORMAL ! En effet nous n’avons pas encore initier l’installation de LogAnalyzer, il n’existe donc pas encore de fichier de configuration. Cliquez sur « here » pour lancer le setup.

A l’étape 1, on vous explique que le setup va vérifier si les pré-requis sont respectés. Cliquez sur « Next » .

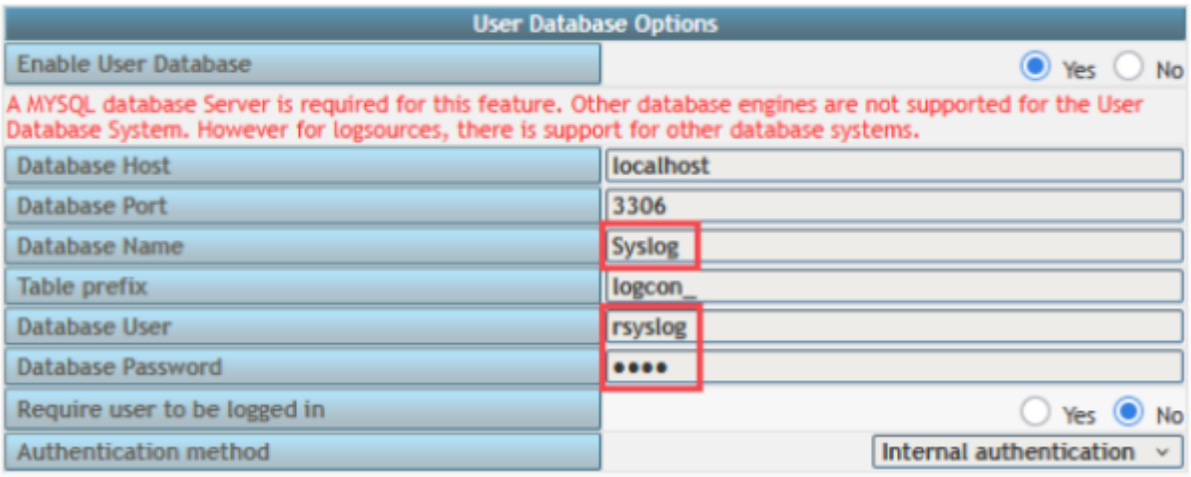
L’étape 2 contrôle les permissions sur les fichiers placés dans /var/www/html/loganalyzer. S’il n’y a pas d’erreur, cliquez sur « NEXT » sinon, relancez la commande « chown » précédemment décrite.



L’étape 3 est la configuration basique du logiciel. **Cochez la case « Yes »** de la question « Enable User Database » **pour renseigner les options de base de données.**



Dans la partie inférieure, **remplir les champs avec les informations de notre propre base de données Syslog** comme sur la capture ci-dessous. **Attention, pour le nom de la base de données il faut bien mettre un S majuscule.**
L'utilisateur sera **« rsyslog »** et le mot de passe que vous avez vous même défini au début.



Ces paramètres vont en réalité créer des tables supplémentaires dédiées à LogAnalyzer dans notre base de données Syslog. La partie « Table prefix » peut être laissée par défaut. Cliquez sur « Next ».

L'étape 4 indique que la connexion à la base de données définie à l'étape 3 a bien réussi et que les tables pour LogAnalyzer seront créées à l'étape suivante. Cliquez sur « Next ».

L'étape 5 valide la création des tables. Cliquez sur «Next ».

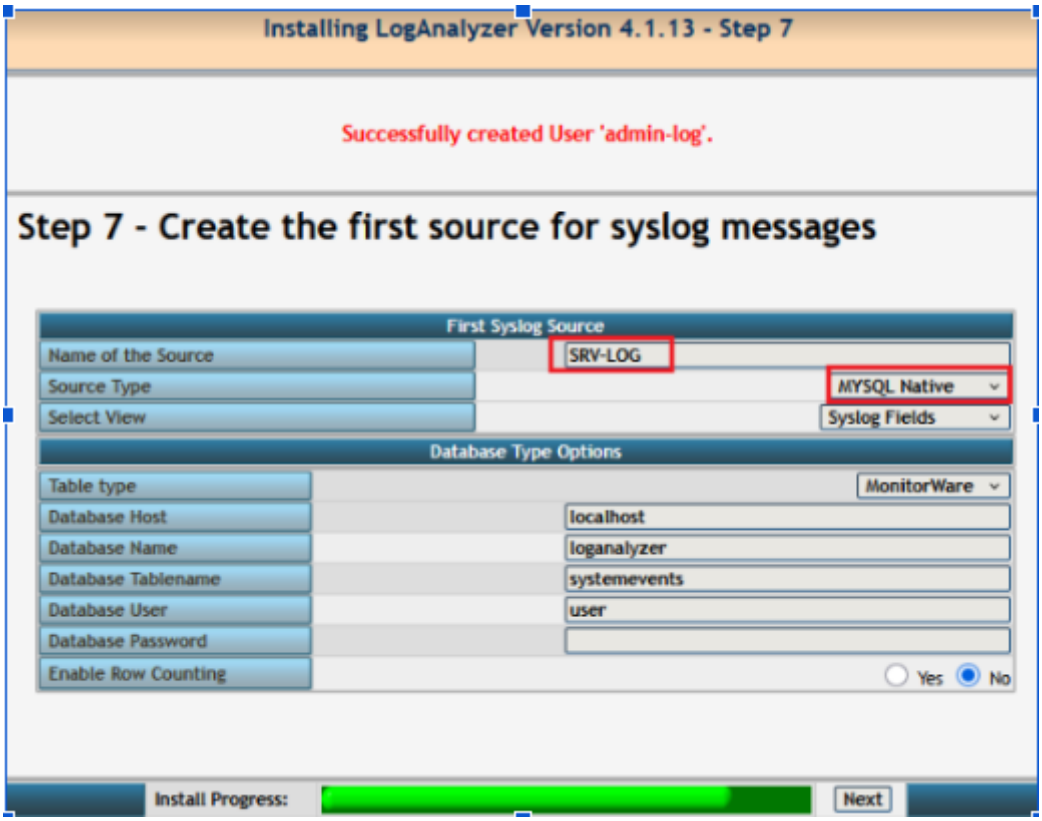
Prochaine étape, Créez un utilisateur pour se connecter à l'interface web de loganalyzer et définissez lui un mot de passe. Cliquez sur «Next ».

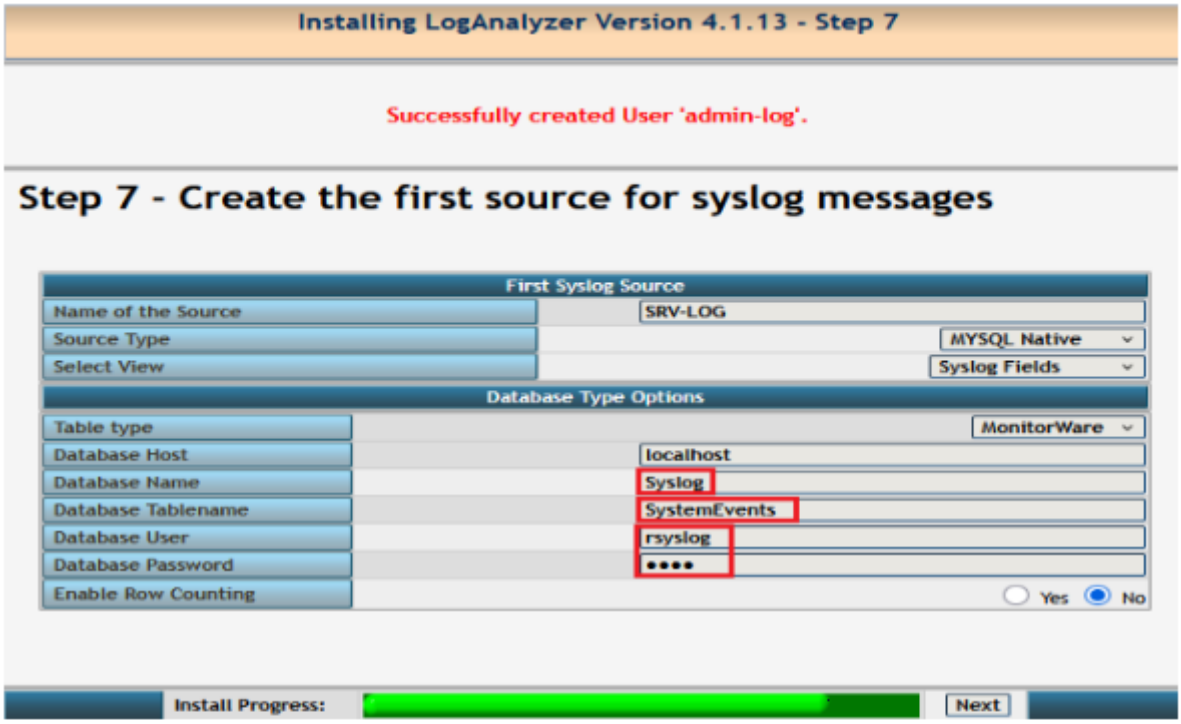
Créez un utilisateur pour se connecter à l'interface web de loganalyzer ell faut maintenant paramétrer la source des logs comme étant notre base de données. Renseignez le champ « Name of the Source » en indiquant ce que vous voulez, ici j'ai mis un nom de serveur par exemple.

Modifiez le champ « Source Type » en sélectionnant « MYSQL Native » ce qui déroule le menu inférieur des options de base de données.

Créez un utilisateur pour se connecter à l'interface web de loganalyzer ell faut maintenant paramétrer la source des logs comme étant notre base de données. Renseignez le champ « Name of the Source » en indiquant ce que vous voulez, ici j'ai mis un nom de serveur par exemple.

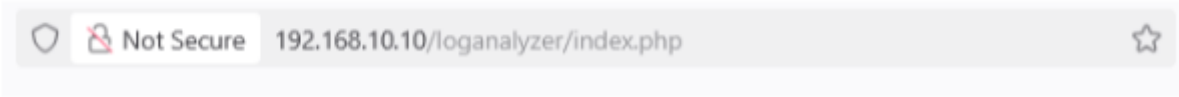
Modifiez le champ « Source Type » en sélectionnant « MYSQL Native » ce qui déroule le menu inférieur des options de base de données.


Installing LogAnalyzer Version 4.1.13 - Step 7
Successfully created User 'admin-log'.
Step 7 - Create the first source for syslog messages
First Syslog Source
Name of the Source
SRV-LOG
Source Type
MYSQL Native
Select View
Syslog Fields
Database Type Options
Table type
MonitorWare
Database Host
localhost
Database Name
loganalyzer
Database Tablename
systemevents
Database User
user
Database Password
Enable Row Counting
Yes
No
Install Progress:
Next



Terminez l'installation en cliquant sur « Finish! ».

Et là, **c'est le drame** ! Une page blanche WTF!



On ne panique pas ! C'est un bug connu de colonnes manquantes dans certaines tables de la base de données de syslog. Retournez sur votre serveur Debian, dans un terminal.

Connectez vous au service de base de données (juste écrire « mysql » si vous n'avez pas fait la sécurisation) :

```
mysql -u root -p
```

```
root@debian:/# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 73
Server version: 10.11.11-MariaDB-0+deb12u1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Saisissez les commandes suivantes (vous pouvez copier/coller tout le bloc d'un seul coup) qui vont ajouter les colonnes manquantes à la **table SystemEvents** :

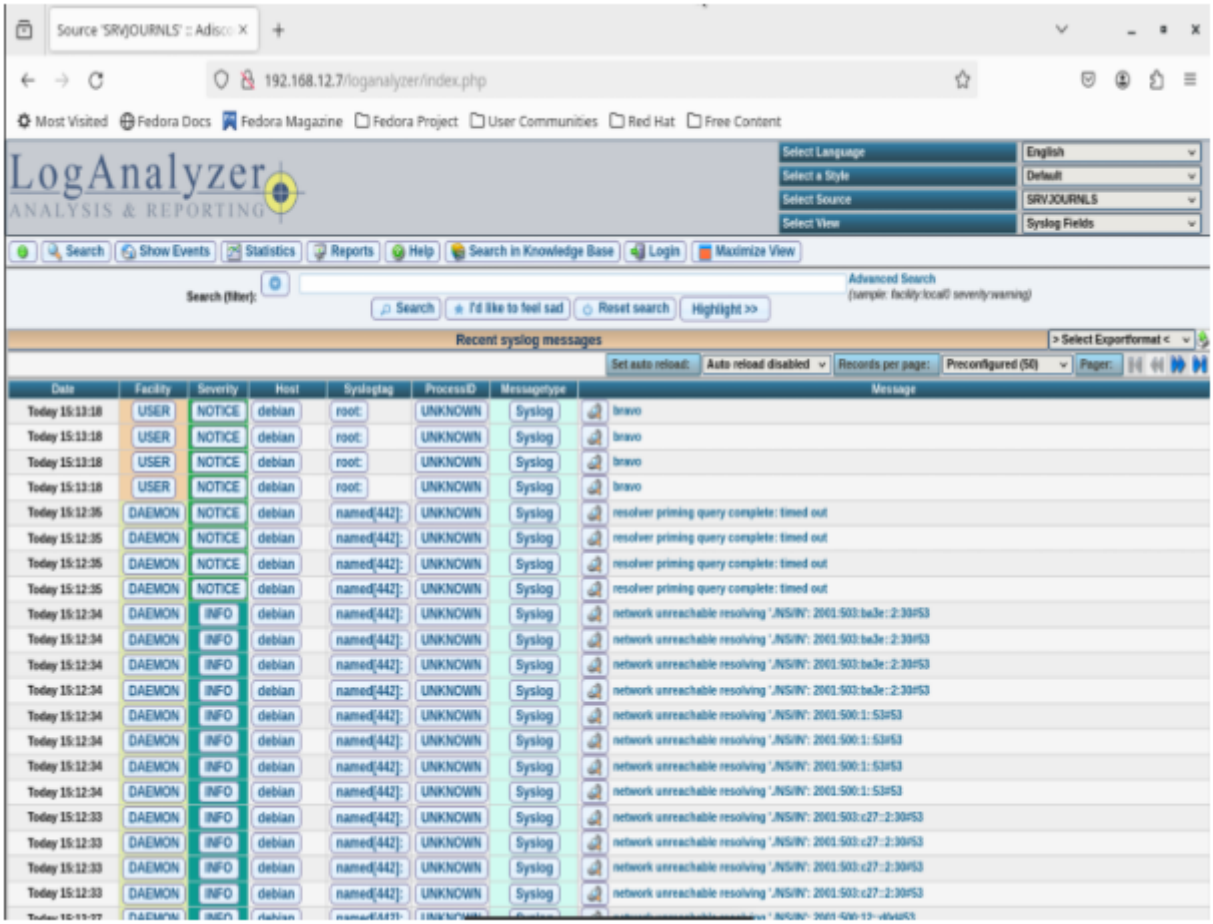
```
USE Syslog;
ALTER TABLE SystemEvents
ADD COLUMN checksum INT NOT NULL
DEFAULT 0,
ADD COLUMN processid VARCHAR(60) NOT
NULL DEFAULT 'UNKNOWN';
EXIT;
```

```
MariaDB [(none)]> USE Syslog;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [Syslog]> ALTER TABLE SystemEvents
    -> ADD COLUMN checksum INT NOT NULL DEFAULT 0,
    -> ADD COLUMN processid VARCHAR(60) NOT NULL DEFAULT 'UNKNOWN';
Query OK, 0 rows affected (0,017 sec)
Records: 0  Duplicates: 0  Warnings: 0

MariaDB [Syslog]> EXIT;
Bye
```

Retournez sur l'interface web de LogAnalyzer. Actualisez la page qui était blanche.



Pour installer RSYSLOG sur Fedora :

sudo dnf install rsyslog

sudo systemctl enable rsyslog

sudo systemctl start rsyslog

sudo systemctl status rsyslog

sudo nano /etc/rsyslog.d/50-remote.conf

#Envoi via UDP

. @adresse_ip_serveur:514

#Envoi via TCP

. @@adresse_ip_serveur:514

Remplacez adresse_ip_serveur par l’IP ou le nom du serveur de logs.

sudo systemctl restart rsyslog

```
sudo systemctl status rsyslog
```

NETBOX

MISE EN PLACE via docker :

Configuration des agent sur les différente machine debian :

Installation de netbox-agent sur Debian
Prérequis : NetBox accessible sur http://192.168.110.6:8080 — remplacez cette IP par celle de votre serveur NetBox si différente.

1.Installer les dépendances

```
apt install -y python3-pip dmidecode lshw
```

2.Installer netbox-agent

```
pip3 install netbox-agent==1.1.0 --break-system-packages
```

Puis faire :

```
apt --fix-missing install -y python3-pip dmidecode lshw
pip3 install netbox-agent==1.1.0 --break-system-packages mkdir -p /etc/netbox nano
/etc/netbox/netbox-agent.yml
```

3. Ajouter netbox_agent au PAF

```
echo 'export PATH=$PATH:/usr/local/bin:/usr/sbin' >> ~/.bashrc
source ~/.bashrc
```

4. Créer un token API dans NetBox
1. Connectez-vous sur NetBox
2. Cliquez sur votre nom d'utilisateur (en haut à droite) → API Tokens
3. Cliquez Add Token
4. Copiez le token généré (sans le mot Bearer)

5. Créer le fichier de configuration

```
mkdir -p /etc/netbox
nano /etc/netbox/netbox-agent.yml

yaml
netbox:
url: 'http://192.168.110.6:8080' # IP de votre serveur NetBox
token: 'VOTRE_TOKEN_ICI'
ssl_verify: false
virtual:
enabled: true
cluster_name: 'proxmox' # Nom exact du cluster dans NetBox
device:
server_role: 'Server'
network:
ignore_interfaces: "^(lo|docker|veth|br-)"
datacenter_location:
driver: 'cmd'
```

Important : le cluster_name doit correspondre exactement au nom du cluster dans NetBox → Virtualisation > Clusters.

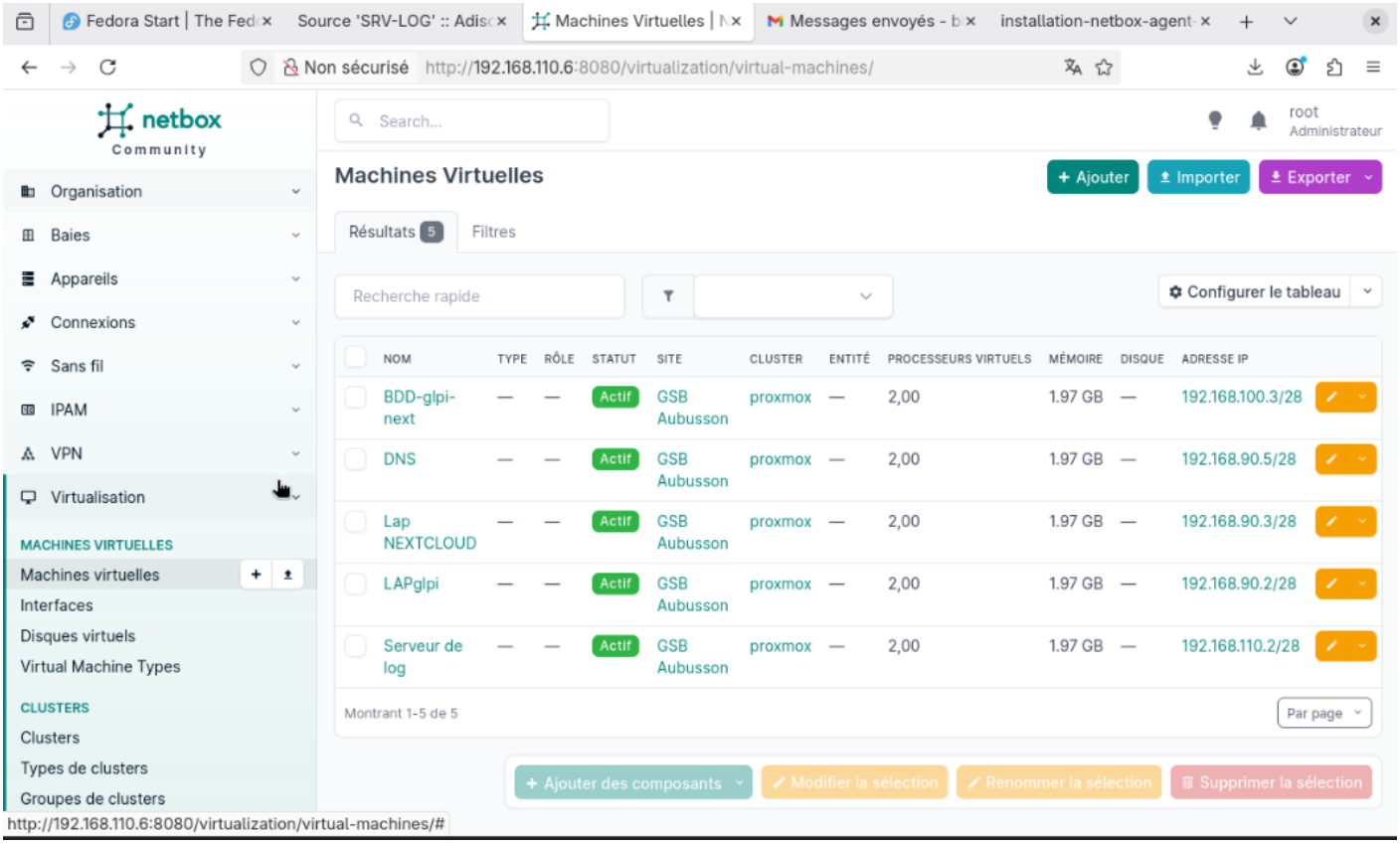
6. Tester l'envoi vers NetBox

```
PATH=$PATH:/usr/sbin netbox_agent -c /etc/netbox/netbox-agent.yml
```

Si vous voyez Finished updating NIC! à la fin, c'est bon

Normalement dans l'interface de NetBox on vois quelque chose de similaire (le nom c le nom de la machine)

Et pour avoir l'ip il faut aller dans modifier , décendre jusqu'a ip et choir la bonne IP



7. Automatiser avec un timer systemd (toutes les heures)

```
cat > /etc/systemd/system/netbox-agent.service << 'EOF'
[Unit]
Description=NetBox Agent
After=network.target
[Service]
Type=oneshot
Environment="PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
ExecStart=/usr/local/bin/netbox_agent -c /etc/netbox/netbox-agent.yml -u
EOF
cat > /etc/systemd/system/netbox-agent.timer << 'EOF'
[Unit]
Description=NetBox Agent toutes les heures
[Timer]
OnBootSec=5min
OnUnitActiveSec=1h
[Install]
WantedBy=timers.target
EOF
```

```
systemctl daemon-reload
systemctl enable --now netbox-agent.timer
```

Vérification :

```
systemctl status netbox-agent.timer
```

WINDOWS server

DOC WINDOWS CLIENT & WINDOWS SERVER

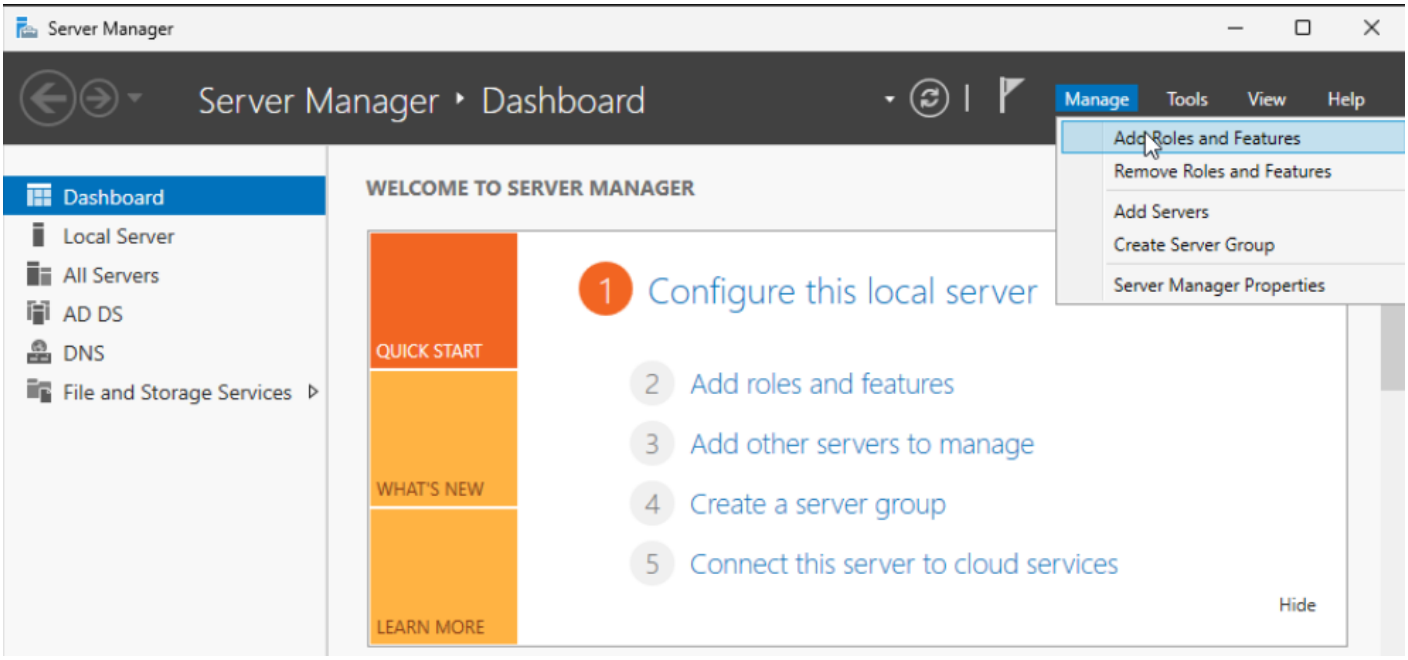
Objectifs :

- L’installation de **Active Directory**
- **Intégrer** un poste au domaine
- Création d’une **Stratégies de groupes** (GPO)

1 – Installation de active Directory

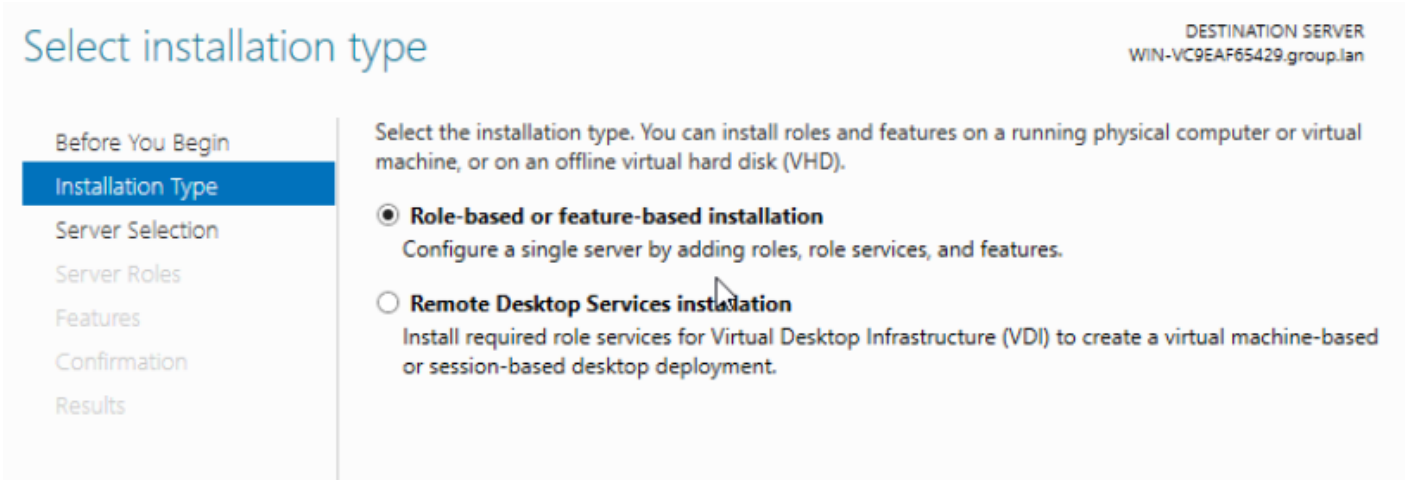
Étape 1 : Ajouter le rôle Active Directory

Allez dans le gestionnaire de serveur sur **Server Manager → Manage → Add Roles and features.**

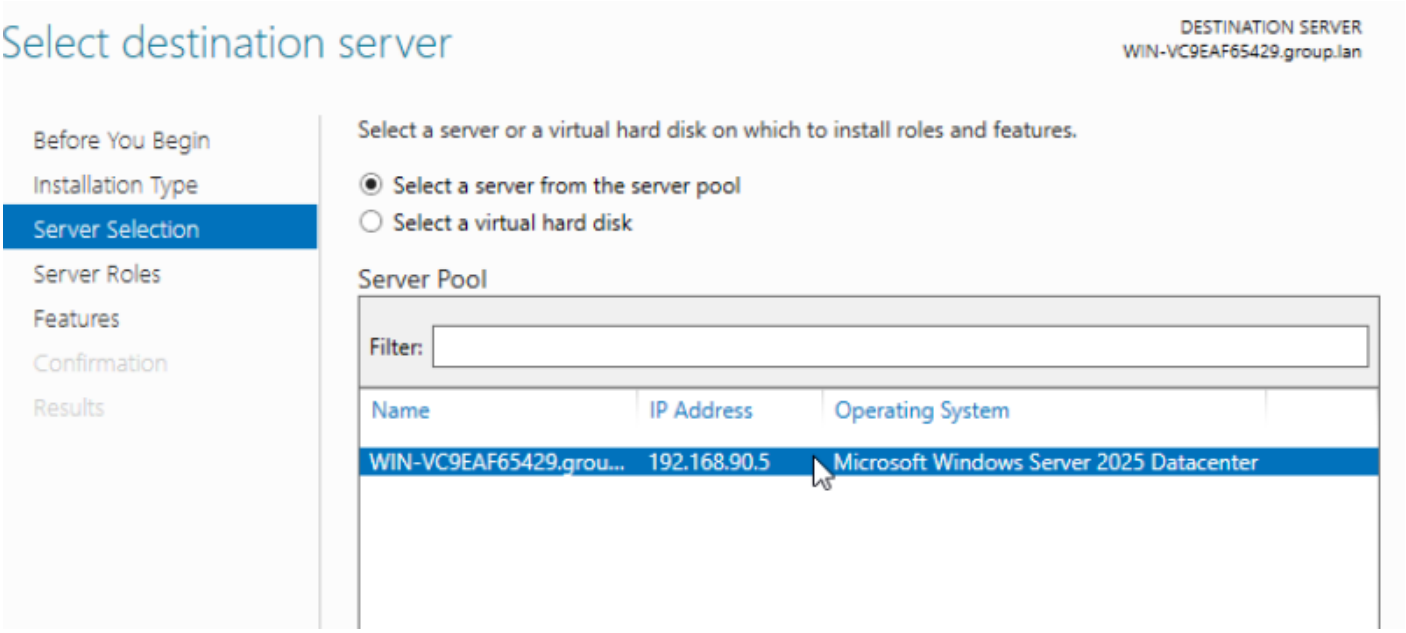


Étape 2 : Sélectionner le type d’installation :

Choisissez Installation basée sur un rôle ou en une fonctionnalité et faites suivants.

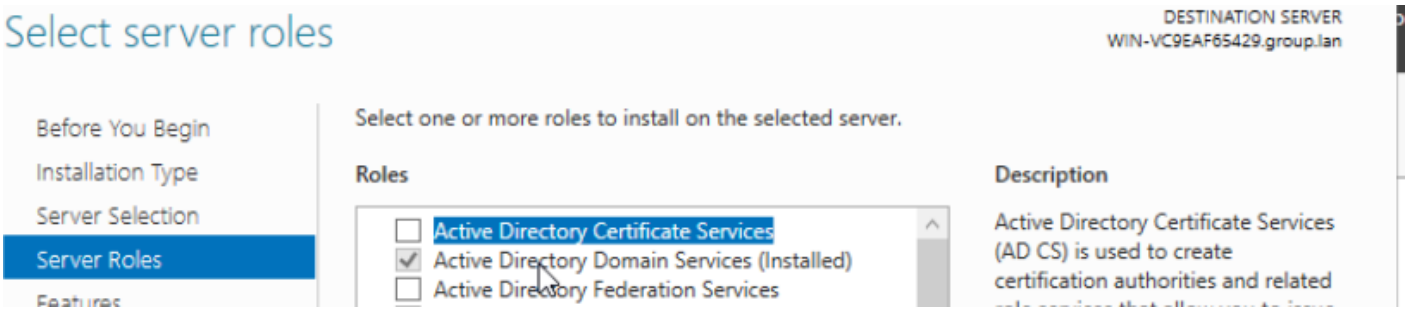


Étape 3 : Choisissez le serveur cible :



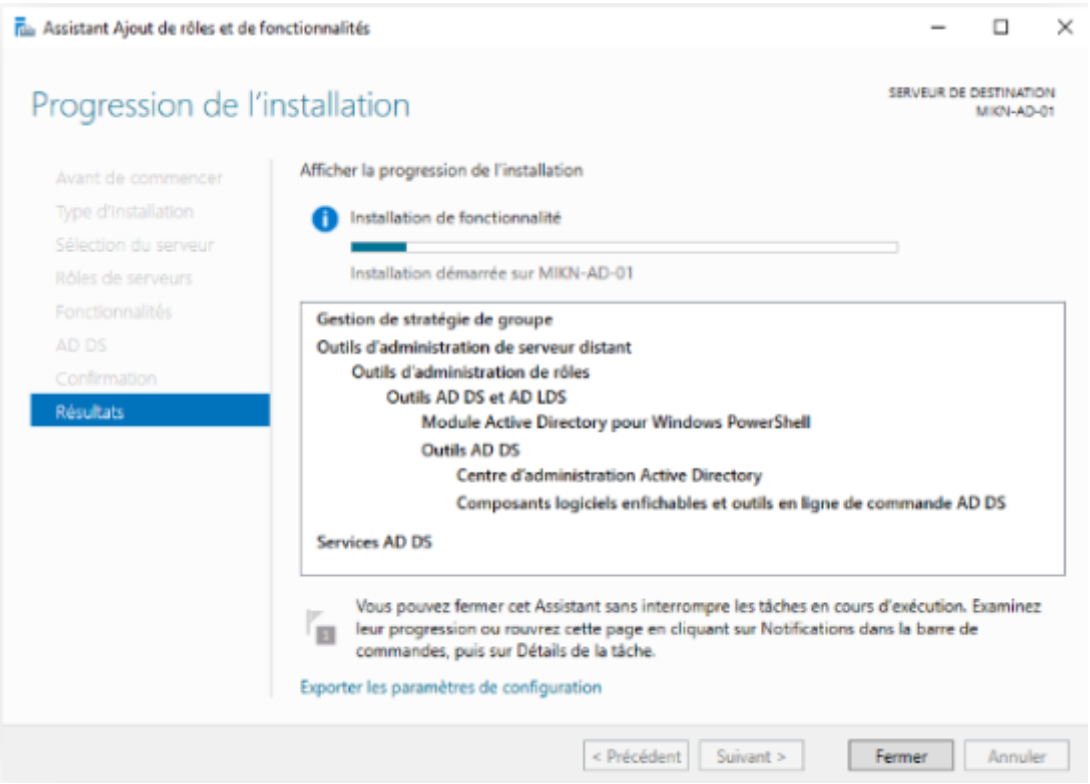
Étape 4 : Sélectionnez le rôle **Active Directory** (AD DS)

Dans la liste, cochez le Services de domaine **Active Director**y (AD DS) puis confirmez.



Étape 5 Finaliser l’Installation :

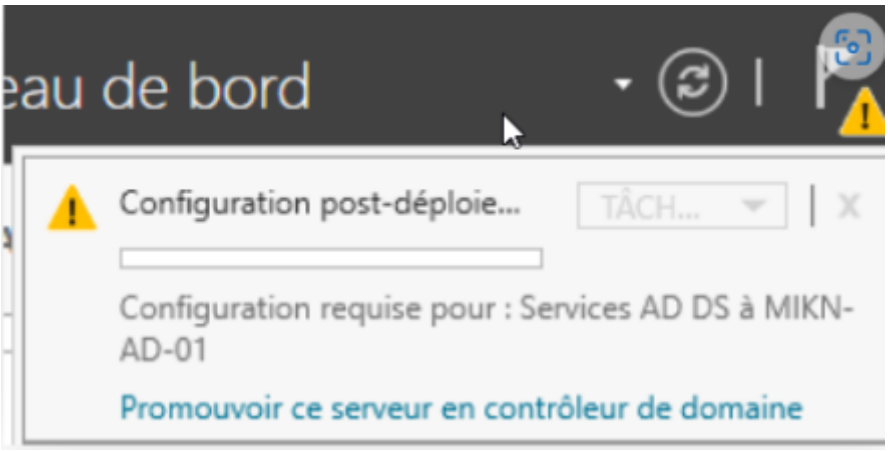
Une fois installer, le redémarrage se fera pas automatiquement faut d’abord promouvoir le serveur en tant que contrôleur de domaine.



Étape 6 : Promouvoir le Serveur en Contrôleur de domaine.

Lancer l'assistant :

Dans le gestionnaire de serveur, cliquez sur la notification indiquant que la configuration post-installation est nécessaire.

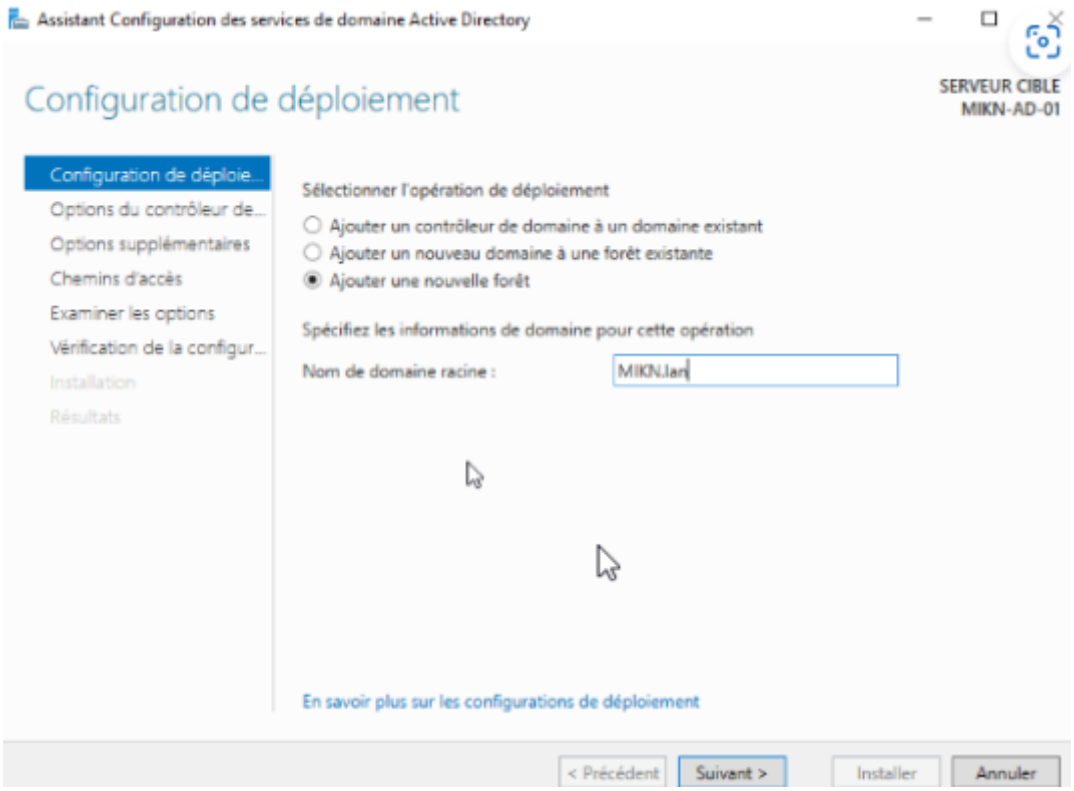


Créez un nouveau domaine :

Choisissez

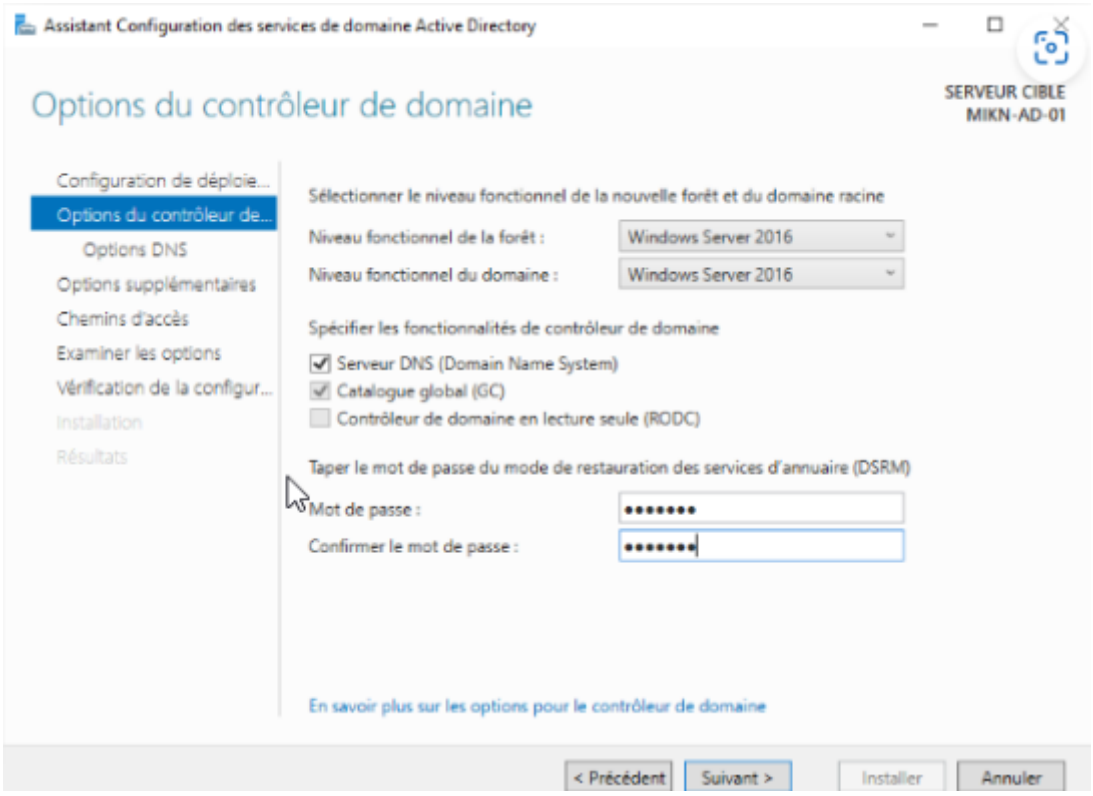
Ajouter une nouvelle forêt.

Entrez le nom de domaine racine comme **mondomaine.lan** (Par exemple).

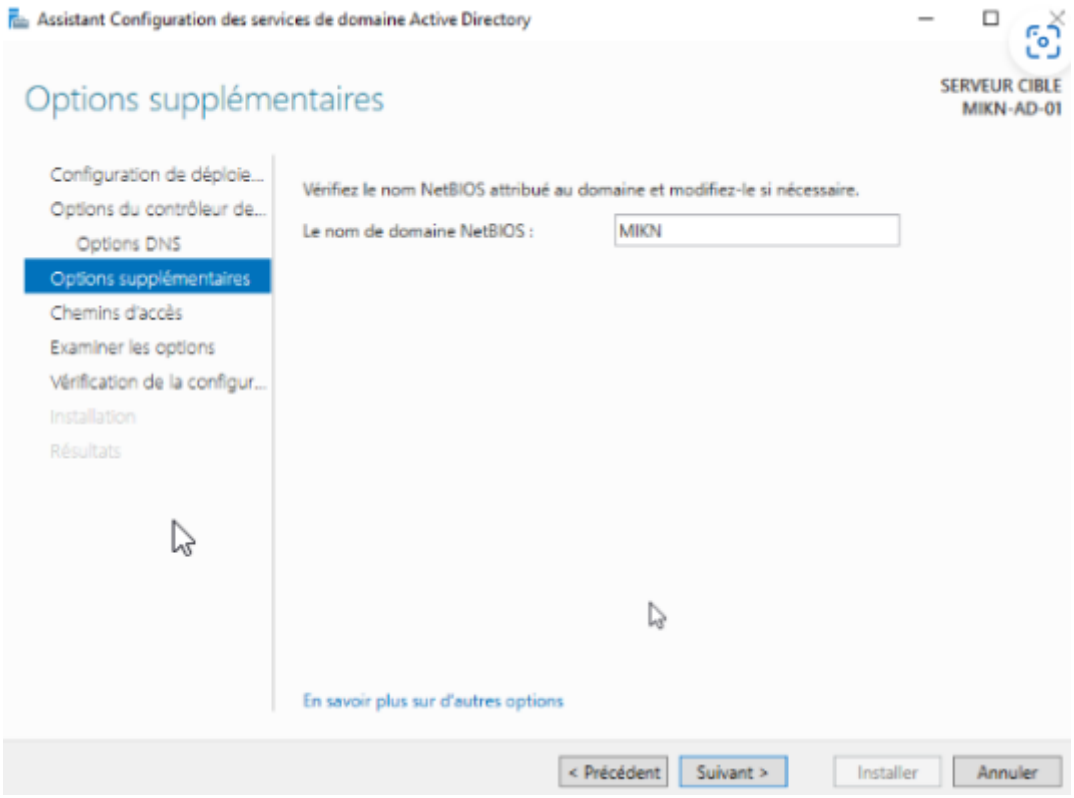


Configurer les options du domaine :

Configurez un mot de passe pour le mode de restauration des services d’annuaire.



Vérifiez bien le **nom NetBIOS** proposé et ajustez-le si nécessaire.



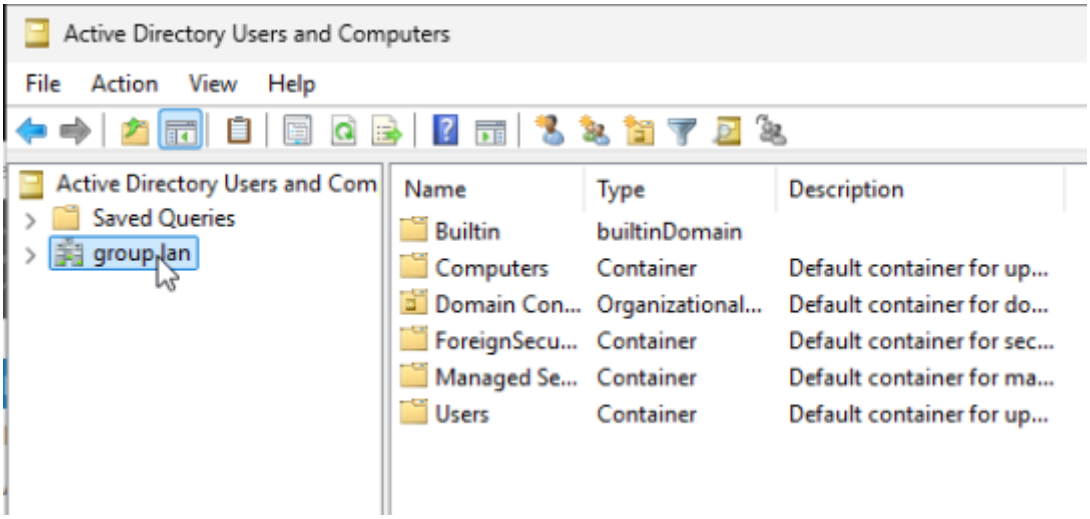
Valider et Installer :

Laissez l'assistant valider la config.

Cliquez sur **installer**. Le serveur redémarrera automatiquement.

Étape 7 : Vérifier l'installation

Testez le domaine :



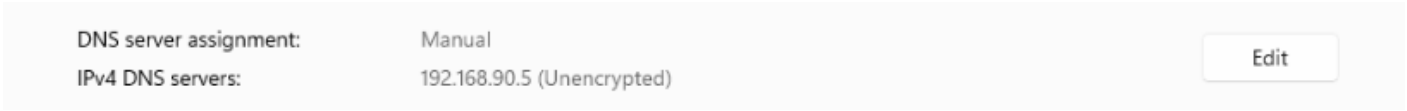
2 - Intégrer un poste au domaine

Étape 1 : Rendez vous sur votre machine Cliente

Étape 2 : Allez dans Network and settings :

Étape 3 : Allez dans Internet :

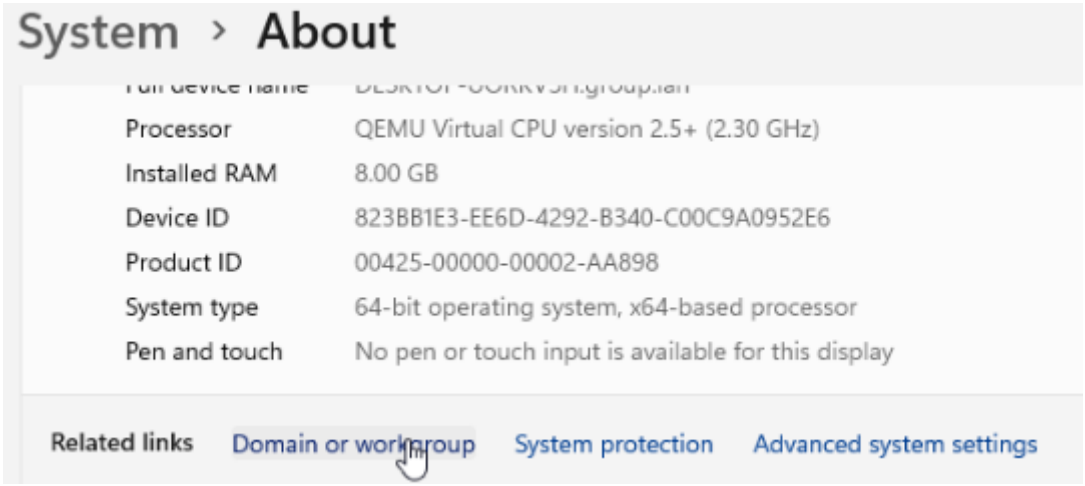
Adressez configurez votre machine correctement (IP), si c'est déjà fait remplacez alors le DNS de votre machine cliente par l'adresse IP de de votre Windows Server.

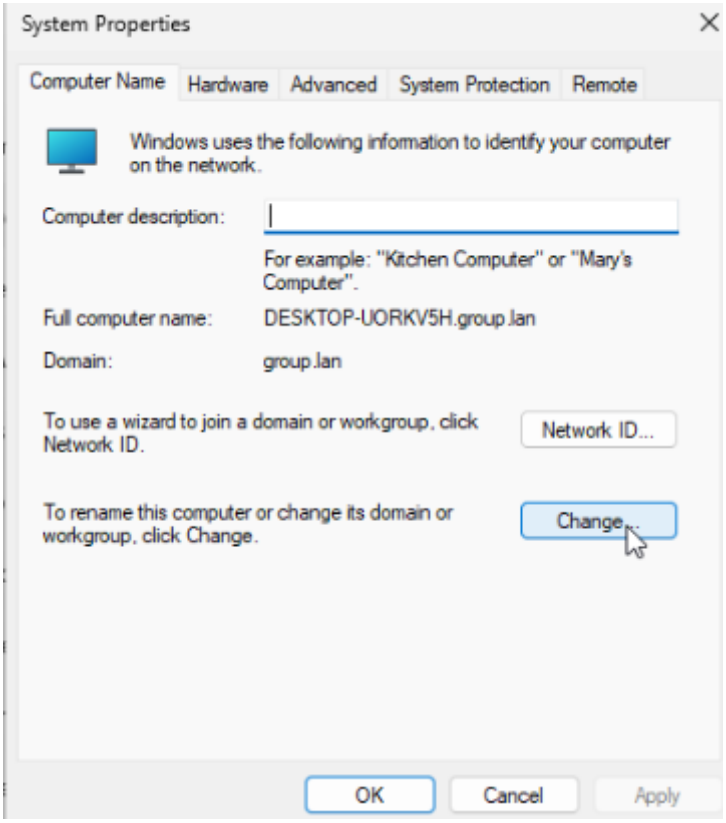


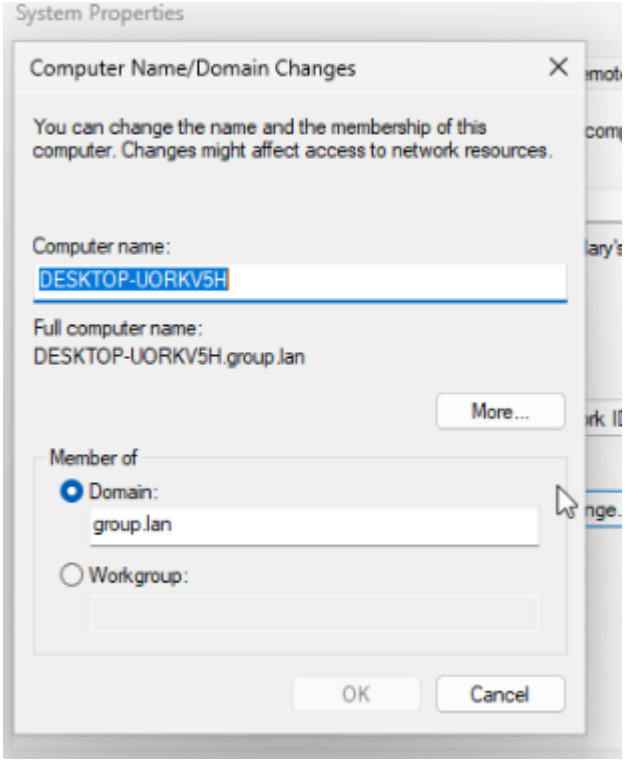
Étape 4 : Ajouter votre machine dans le domaine :

Allez dans **Systeme → About → Domain or workgroup → renommez ce poste ou changer le domaine ...etc** cliquez sur **Change..** puis ajouter votre **nom de domaine** préalablement créer.

(Suivez les capture suivante)







3 – Création d’une stratégie de groupe

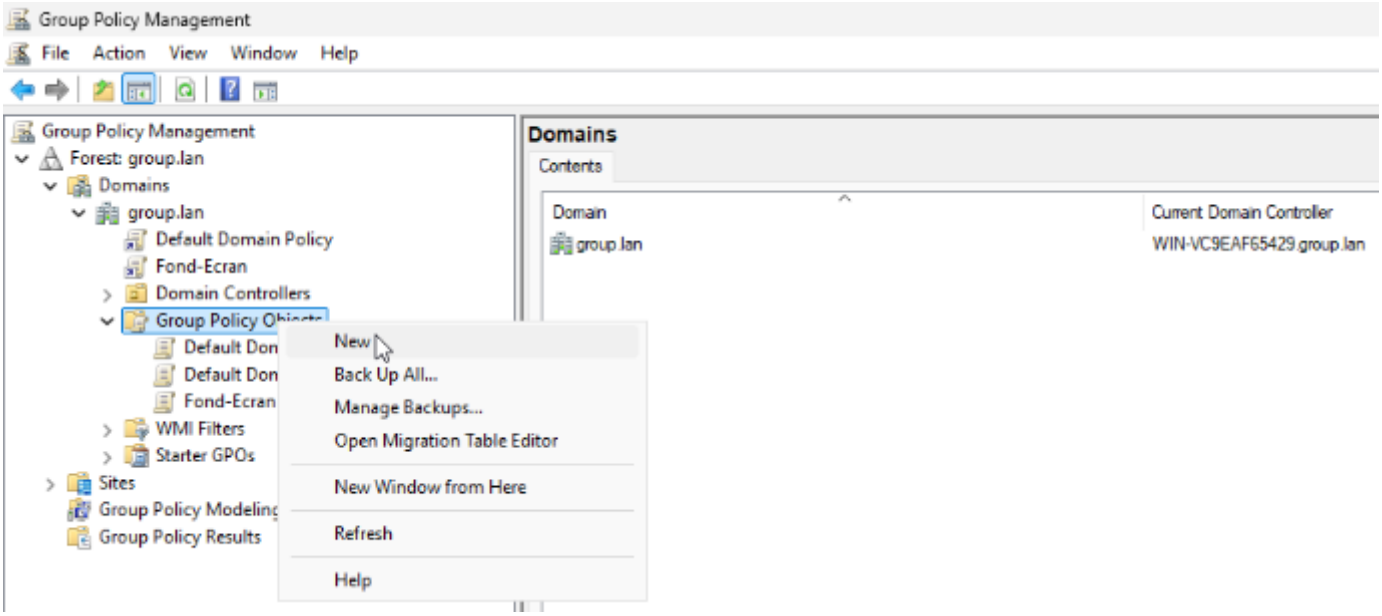
Étape 1 : Vous deviez disposer d’une image

Sélectionner votre image puis mettez dans le chemin suivant :

Ce PC → Disque local (C) → Windows → SYSVOL → sysvol → mondomaine.lan → scripts → Dossier qui contient l’image.

Étape 2 : Créer votre GPO

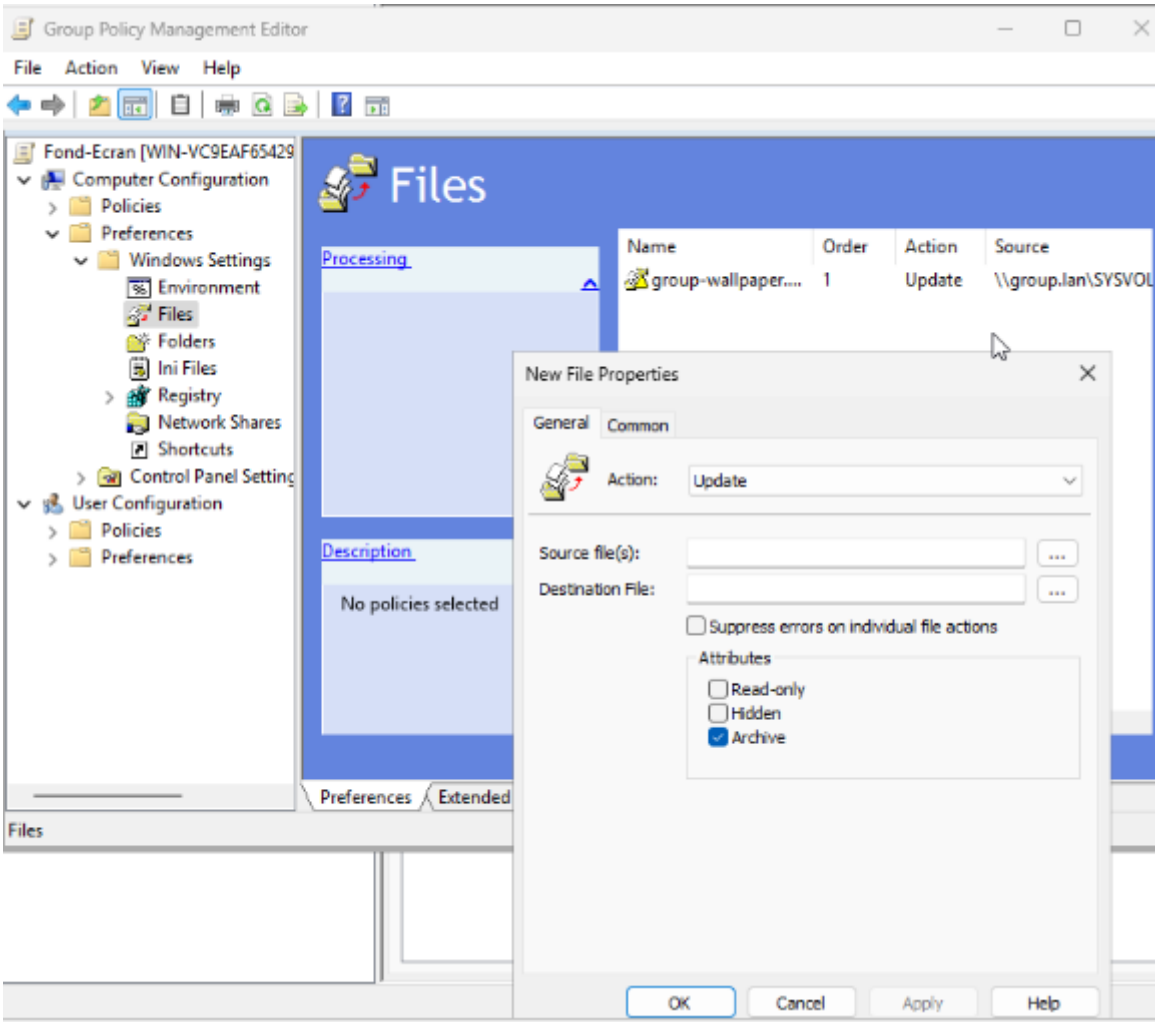
Rendez vous dans **Group Policy Management**, une fois dans le répertoire faites un clic droit sur **Group Policy Objects** et créer votre Stratégies de Groupes.



Étape 3 : Modifier votre GPO

Faites un clique droit sur votre **Stratégies de Groupes** qui vient d’être créer, **configuration computer → preferences → Windows Settings → Files.**

Faites un **clique droit** sur l’espace vide puis **new file**

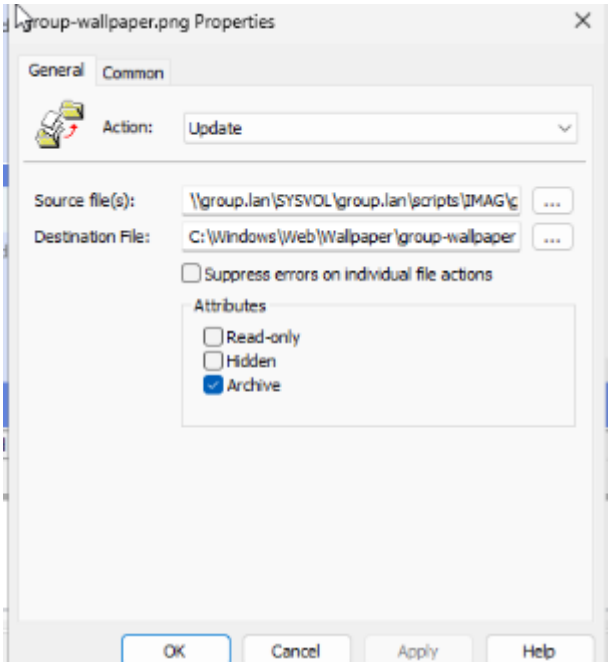


Vérifiez que l'action soit toujours **update,** ensuite dans « **Sources file(s)** » Mettez le chemin réseau de l'emplacement de l'image :

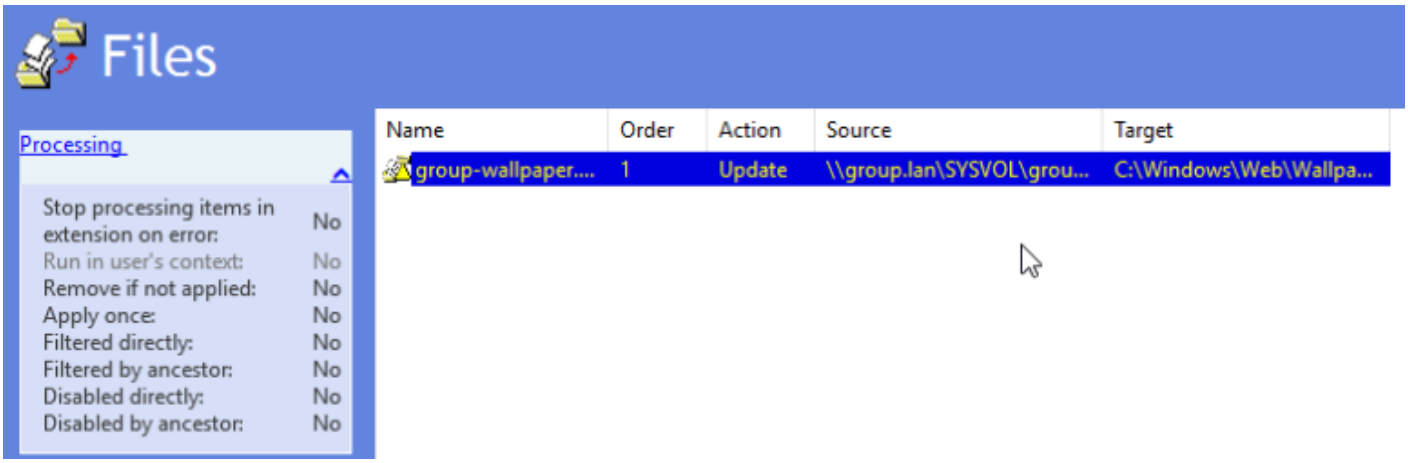
\\mondomaine.la**n**\SYSVOL\mondomaine.lan\scripts\Dossiercontenantlimage\Imageellemême

Dans Destination File :

c:\\Windows\Web\Wallpaper\Imageellemême

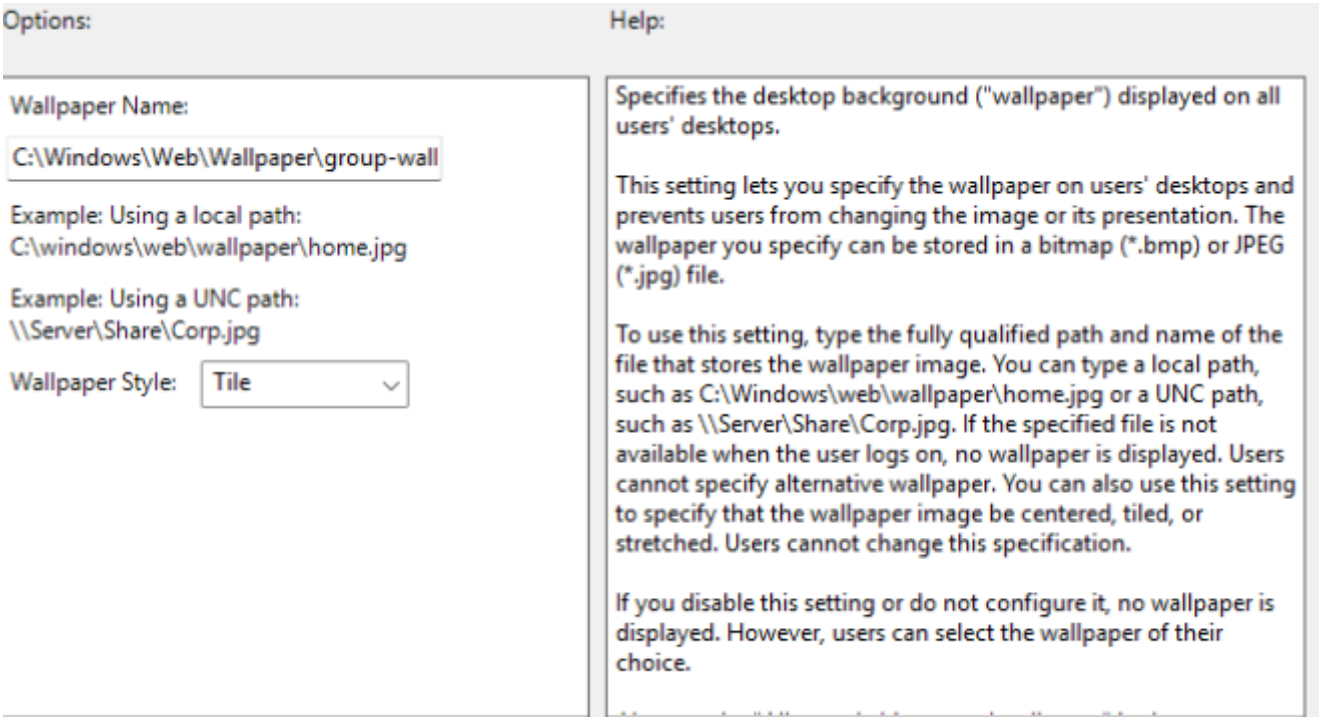


Appliquez votre modification, le résulta attendue devrait ressembler a ceci :



Ensuite configurer le **User Configuration :**

Policy → Admin Temp → Desktop → Desktop Wallpaper

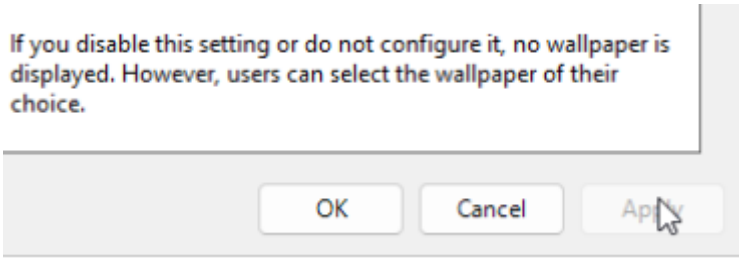


Dans le **Wallpaper Name :**

Collez le chemin qui mène vers la destination qui a été défini au par-avant.

Dans Wallpaper Style : Centrer (Tile)

Une fois prêt, appliquer la modification.

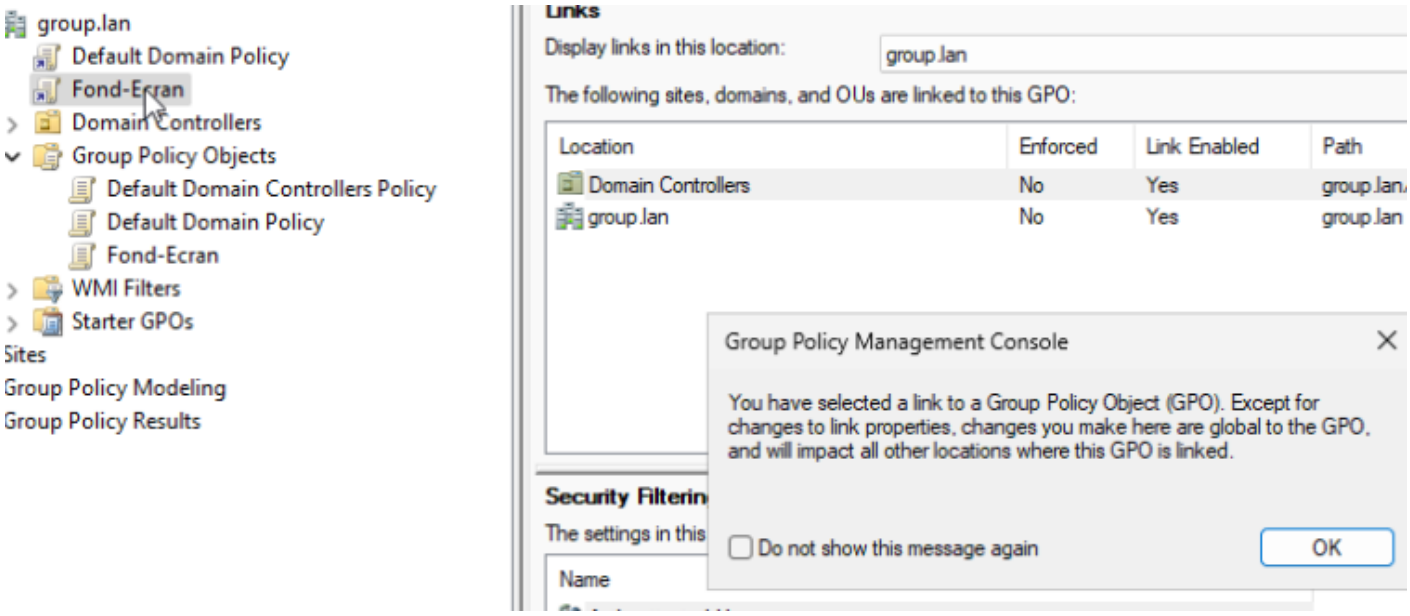


Retournez dans **Group Policy Management.**

Étape 4 : Liée votre GPO à votre domaine :

Cliquez sur votre **Stratégies de groupes** → **Cliquez** sur votre nom de domaine en haut → Link an Existing GPO… → Stratégies de groupes ;

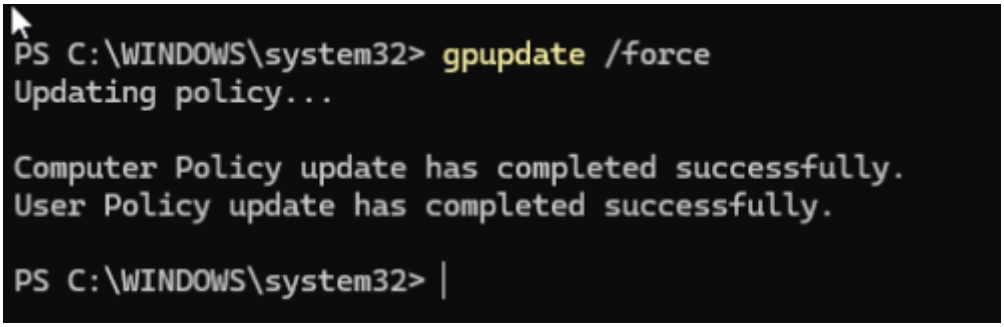
Pour vérifiez **Cliquez** sur votre Stratégies de groupes mise en place.



Étape 5 : Appliquez votre GPO par Powershell

Sur votre Windows Server et votre Windows client faites la commande suivante :

gpupdate /force



Parfait !