Présentation de Mon Projet 2

Sommaire :

Installation Centreon

Pour commencer je vous invite a mettre votre système a jour.

Avec la commande « apt update && apt upgrade »

Commençons maintenant :

```
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
root@debian:/home/enzo# apt update && apt install lsb-release ca-certificates apt-transport-https software-properties-common wget gnupg2 curl
```

Etape 1 : installez les dépendances

```
Paramétrage de curl (7.88.1-10+deb12u14) ...
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
root@debian:/home/enzo# curl -LsS https://r.mariadb.com/downloads/mariadb_repo_setup | sudo bash -s -- --os-type=debian --os-version=12 --mariadb-server-version="mariadb-10.11"
```

Etape 2 : Installez le dépôt de base de données

```
root@debian:/home/enzo# echo "deb https://packages.centreon.com/apt-standard/ $(lsb_release -sc)-25.10-stable main" | tee -a /etc/apt/sources.list.d/centreon-25.10-stable.list
deb https://packages.centreon.com/apt-standard/ bookworm-25.10-stable main
root@debian:/home/enzo# echo "deb https://packages.centreon.com/apt-plugins-stable/ $(lsb_release -sc) main" | tee /etc/apt/sources.list.d/centreon-plugins.list
```

Etape 3 : Installez le dépôt Centreon

```
root@debian:/home/enzo# wget -O- https://apt-key.centreon.com/ | gpg --dearmor | tee /etc/apt/trusted.gpg.d/centreon.gpg > /dev/null 2>&1
```

Etape 4 : Importez la clé du dépôt et lancez un « apt update »

```
root@debian:/home/enzo# apt install -y centreon-mariadb centreon
```

```
root@debian:/home/enzo# systemctl daemon-reload
```

```
root@debian:/home/enzo# systemctl restart mariadb
```

Etape 5 : Installez un serveur central centreon

```
root@debian:/home/enzo# hostnamectl set-hostname projetenzo
```

Etape 6 : Renommez votre nom d’hôte du serveur ici « projetenzo »

```
root@debian:/home/enzo# systemctl enable php8.2-fpm apache2 centreon cbd centengine gorgoned centreontrapd snmpd snmptrapd
root@debian:/home/enzo# systemctl enable mariadb
root@debian:/home/enzo# systemctl restart mariadb
```

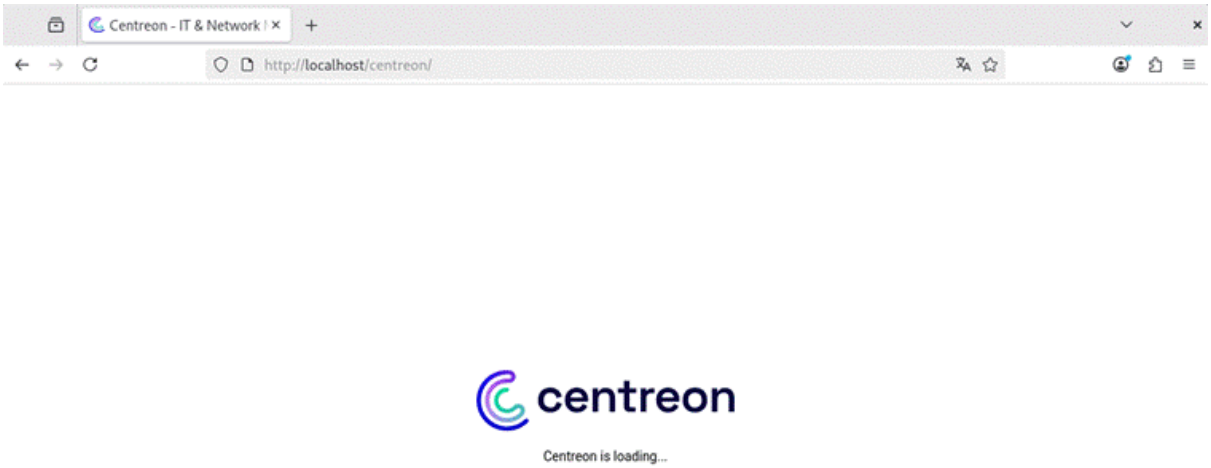
Etape 7 : exécutez cette commande pour que votre script démarre automatiquement

```
root@debian:/home/enzo# mariadb-secure-installation
```

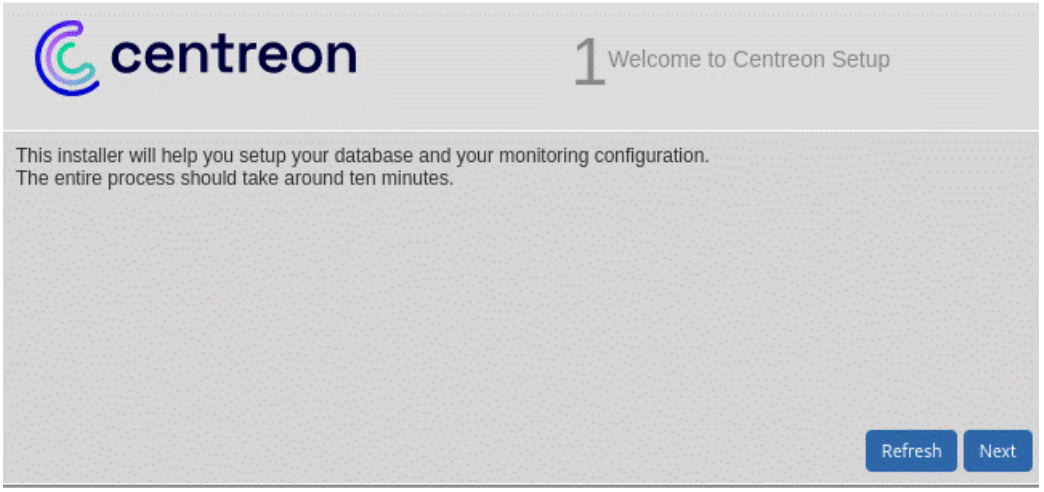
Etape 8 : Sécurisez l’accès root de la base de données avant d’installer Centreon
Répondez OUI à toutes les questions sauf a « Disallow root login remotely ? »
Il est aussi obligatoire de définir un nouveau mot de passe root, ce mot de passe vous sera demandé pendant l’installation Web.

```
root@debian:/home/enzo# systemctl start apache2
```

Etape 9 :Démarrez le serveur Apache avec cette comande



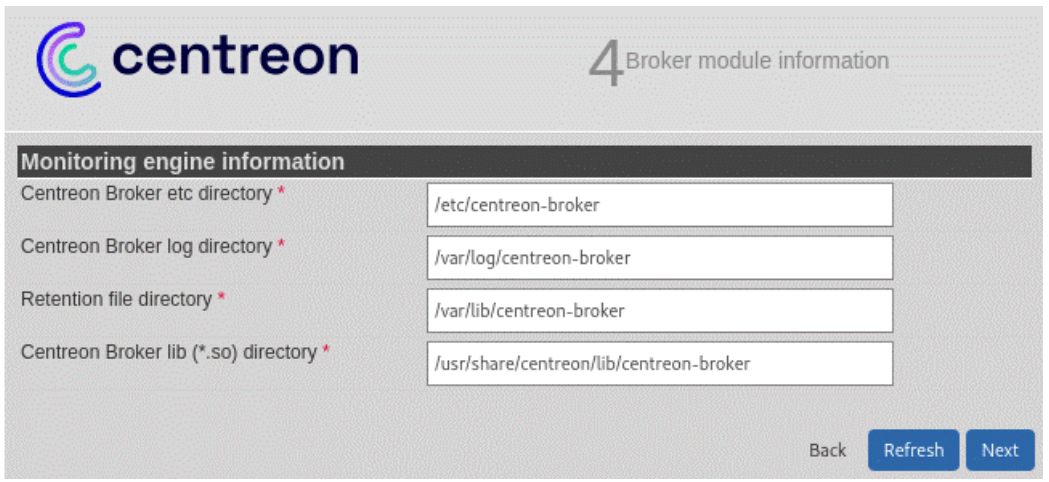
Etape 10 : rendez-vous sur la page web de Centreon pour continuer l'installation



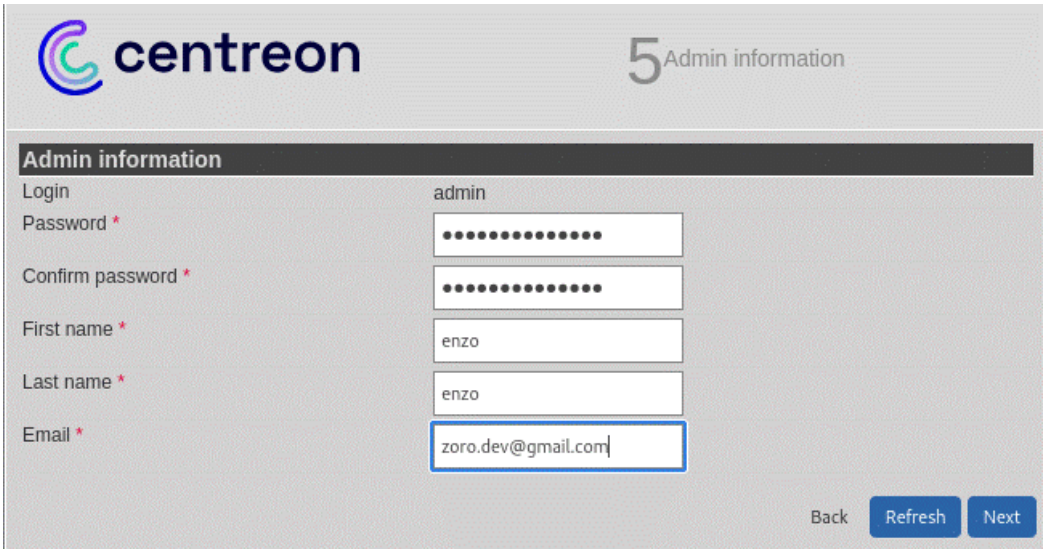
Etape 11 : faites Next

Etape 12 : faites Next

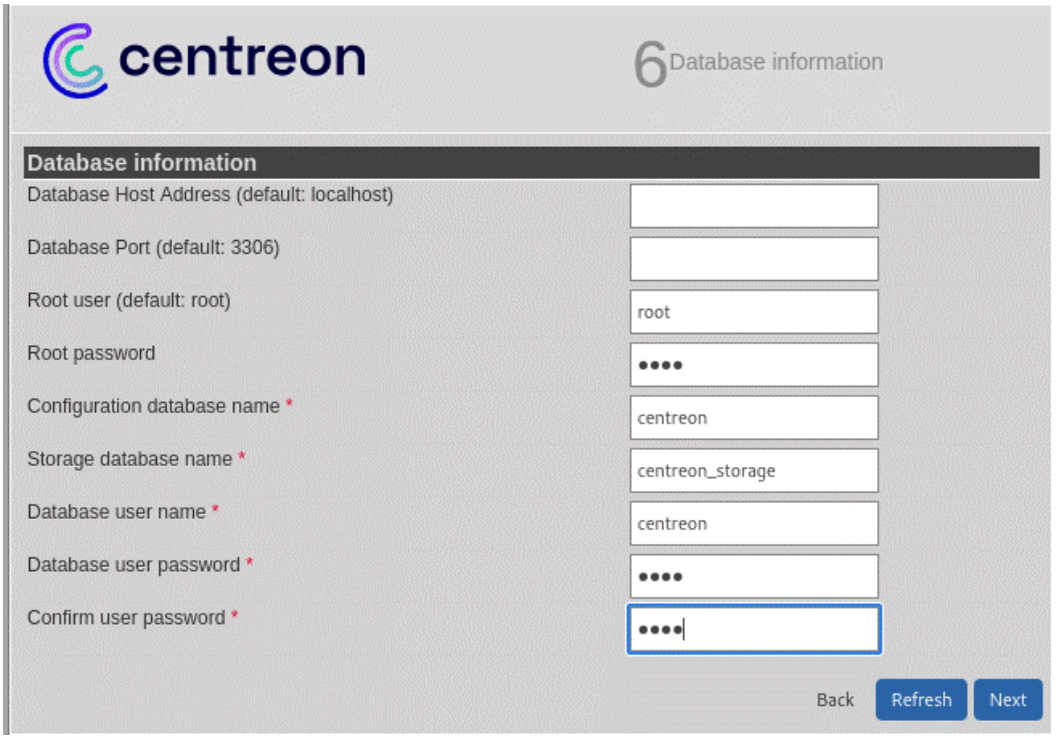
Etape 13 : laissez les chemins par défaut et faites Next



Etape 14 : Faire de nouveau Next

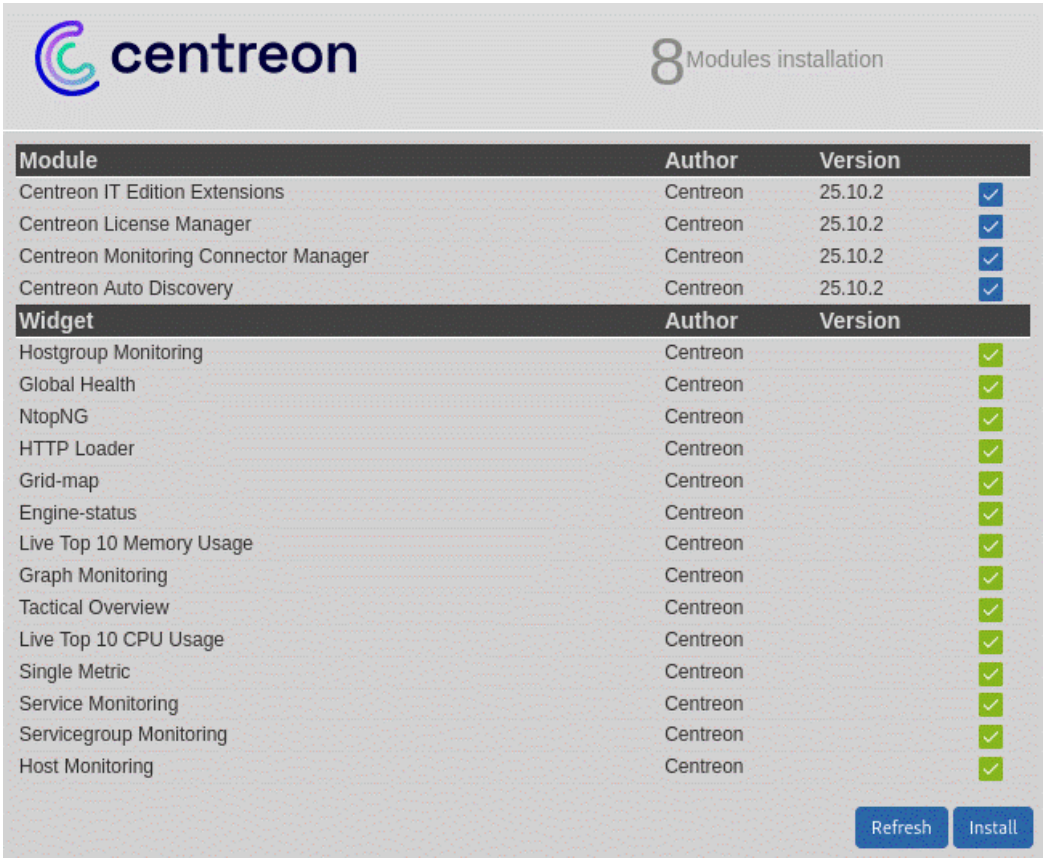


Etape 15 : Choisir un mot de passe robuste et remplir vos informations



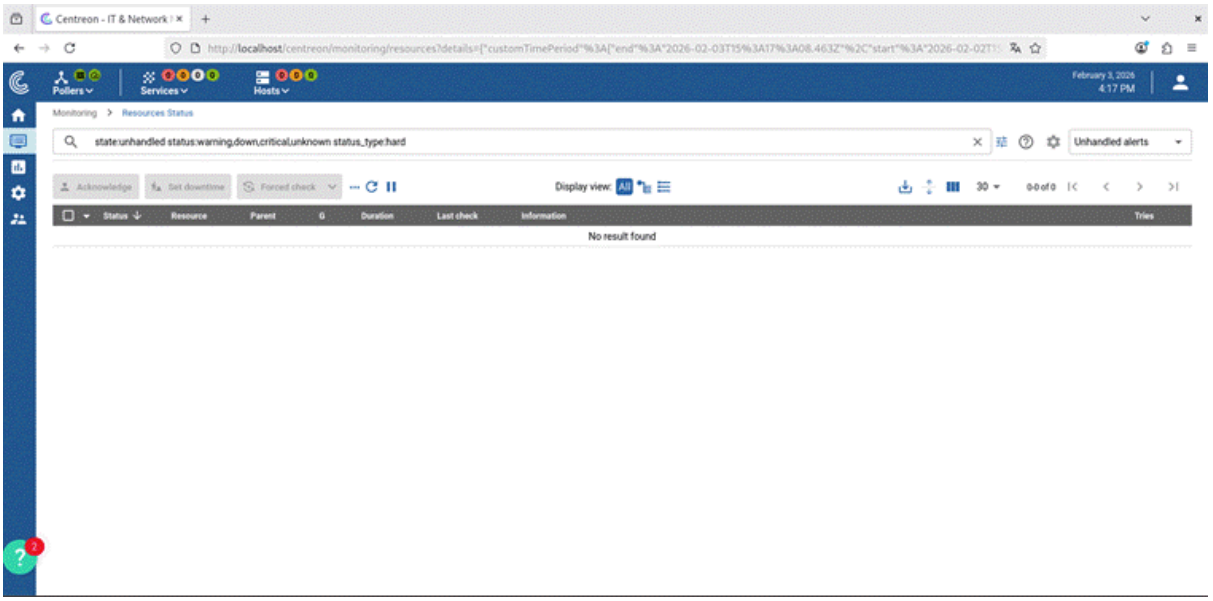
Etape 16 : Entrez votre mot de passe root et créer le nouveau mot de passe pour la base de donnée

Etape 17 : Faites Next



Etape 18 : Cliquez sur Install

Etape 19 : Faites Finish



Etape 20 : Vous voici sur l’interface Centreon

Initialisation de la supervision

Etape 1 :Pour démarrer les processus de supervision : Depuis l'interface web, rendez-vous dans le menu Configuration > Collecteurs.
Etape 2 :Sélectionnez le collecteur Central dans la liste et cliquez sur Exporter la configuration.
Etape 3 : Cochez Déplacer les fichiers générés en plus de la sélection par défaut et cliquez sur Exporter.
Etape 4 : Connectez-vous au serveur Central.

```
root@debian:/home/enzo# systemctl restart cbd centengine
```

Etape 5 : redémarrez les processus de collecte

```
root@debian:/home/enzo# systemctl restart gorgoned
```

Etape 6 : Redémarrez le service des tâches

```
root@debian:/home/enzo# systemctl start snmptrapd centreontrapd
```

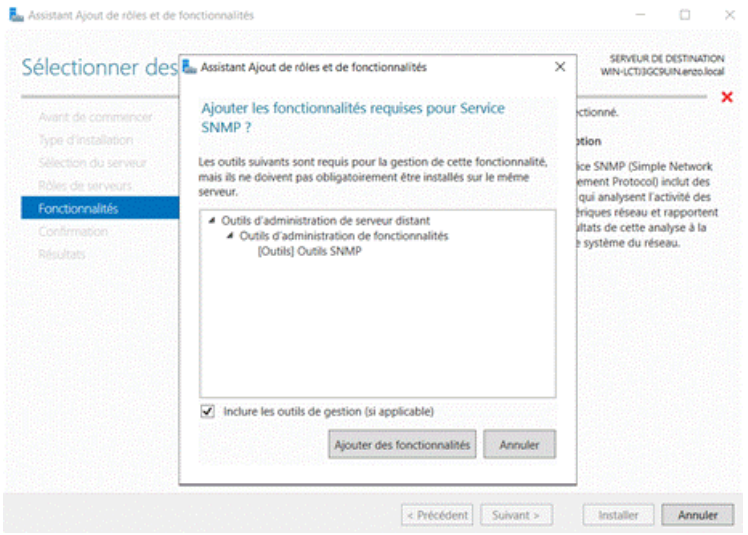
Etape 7 : Démarrez les services de supervision passive

```
root@debian:/home/enzo# systemctl start snmpd
```

Démarrer le démon SNMP

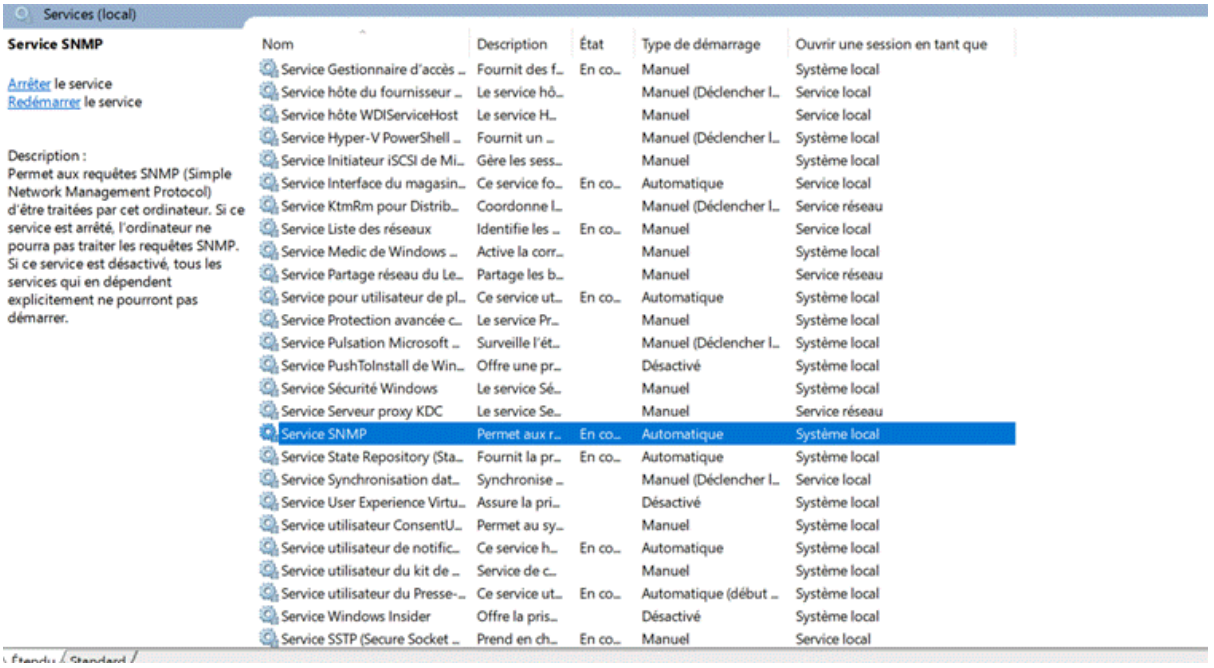
Superviser votre premier serveur Windows

Pour commencer, il faut que vous installiez le service SNMP sur votre Windows.
Pour ce faire il suffit d'allez dans ajoutez une fonctionnalité sur le gestionnaire de serveur, puis d'installer le service SNMP.



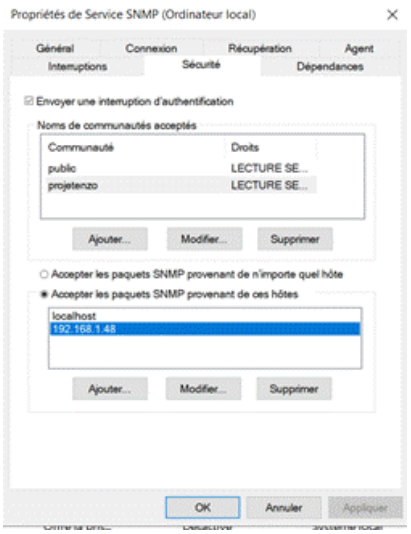
Etape 1 : Ajouter des fonctionnalités.

Etape 2 :Après l'installation de SNMP, vous devez procéder à sa configuration. Dans la barre de recherche, tapez services.msc et appuyez sur Entrée pour lancer le panneau Services. Recherchez le service SNMP dans la liste.

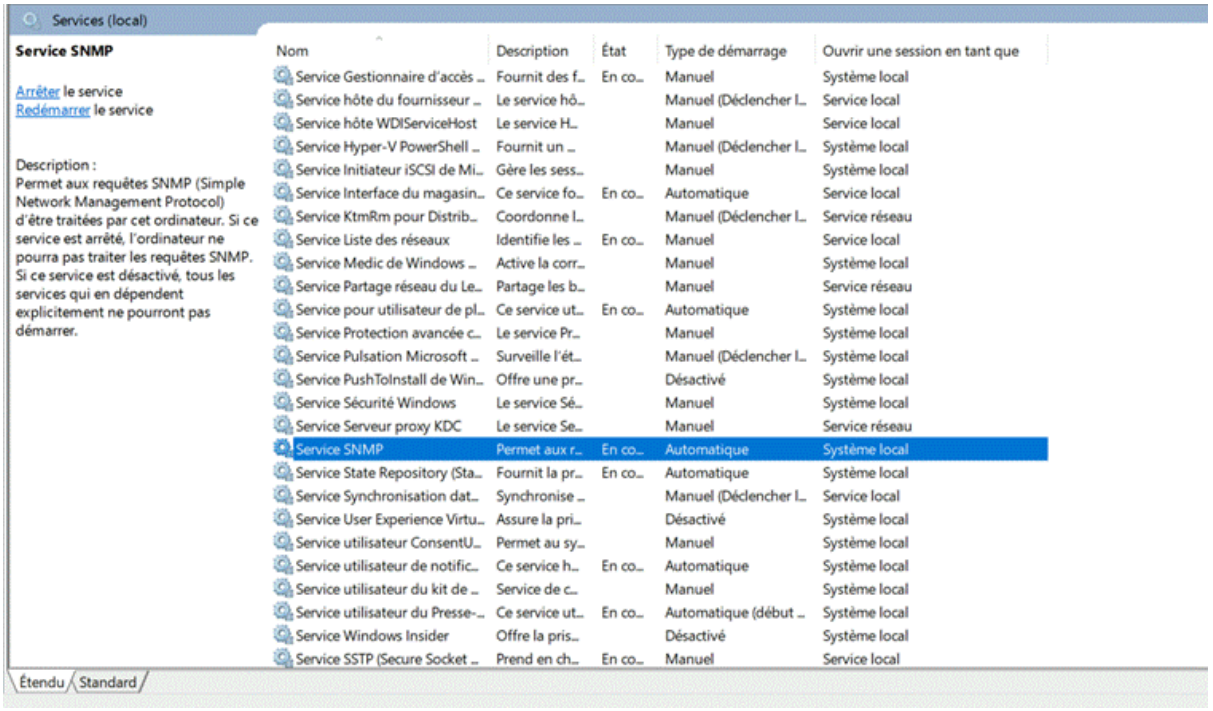


Etape 3 : Faire clic droit > propriété >Agent

Etape 4 : Rentré vos informations et cochez toutes les cases.
Puis faire Appliquer

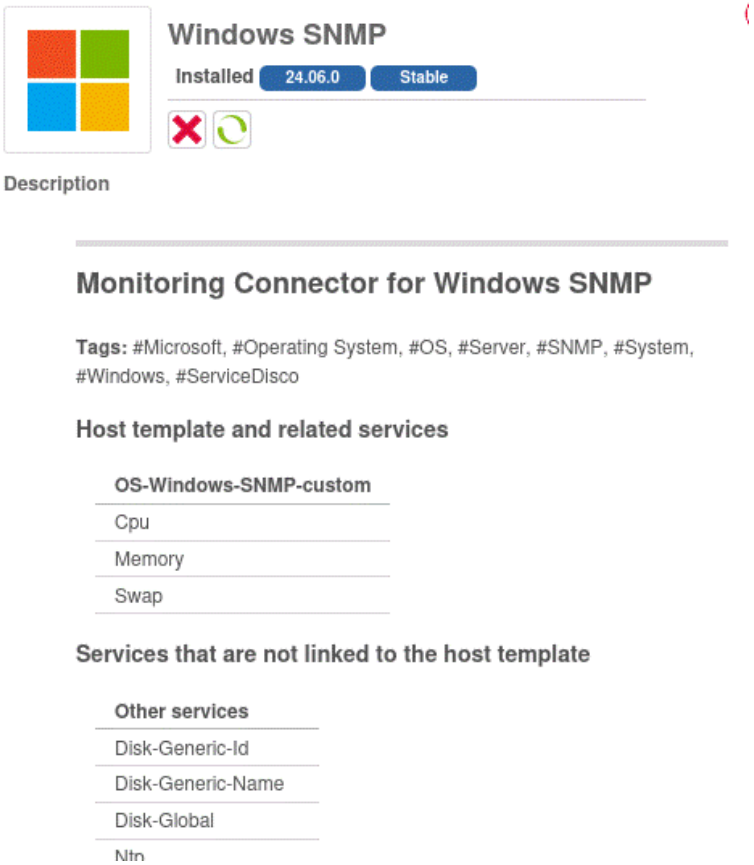


Etape 5 : Dans l'onglet Sécurité, renseignez la communauté SNMP dans la section Noms de communauté acceptés et choisissez l'option LECTURE SEULE. Sélectionnez ensuite Accepter les paquets SNMP de ces hôtes et ajoutez l'adresse IP du serveur Centreon.



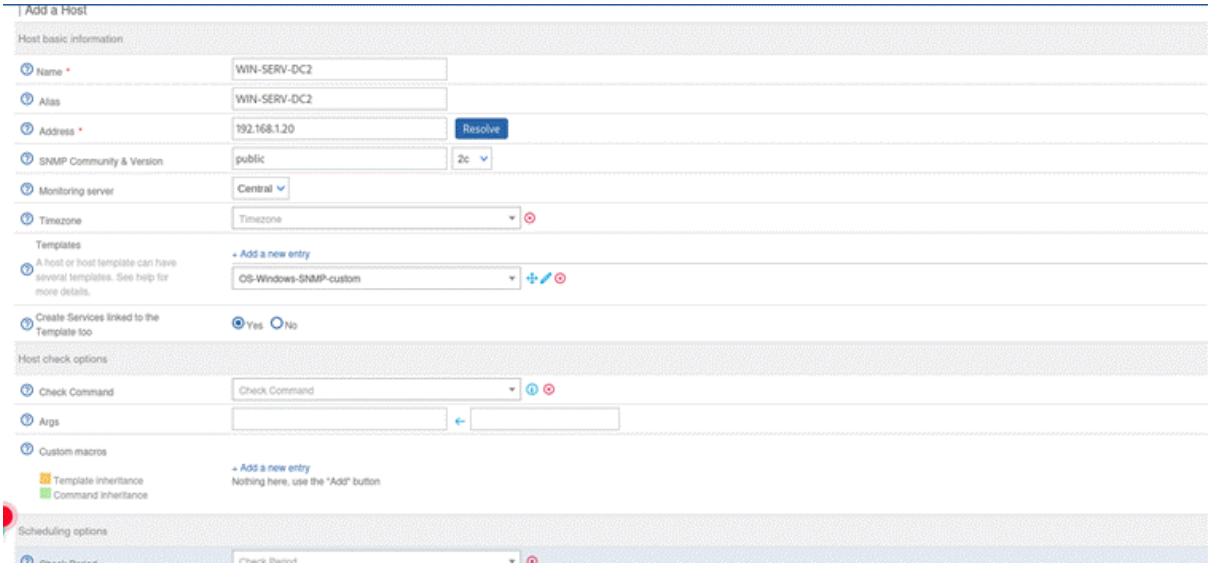
Etape 6 : Redémarrez le service SNMP

Dans l'interface Web de Centreon, accédez à Configuration > Connecteurs > Connecteurs de supervision et installez le connecteur de supervision Windows SNMP :



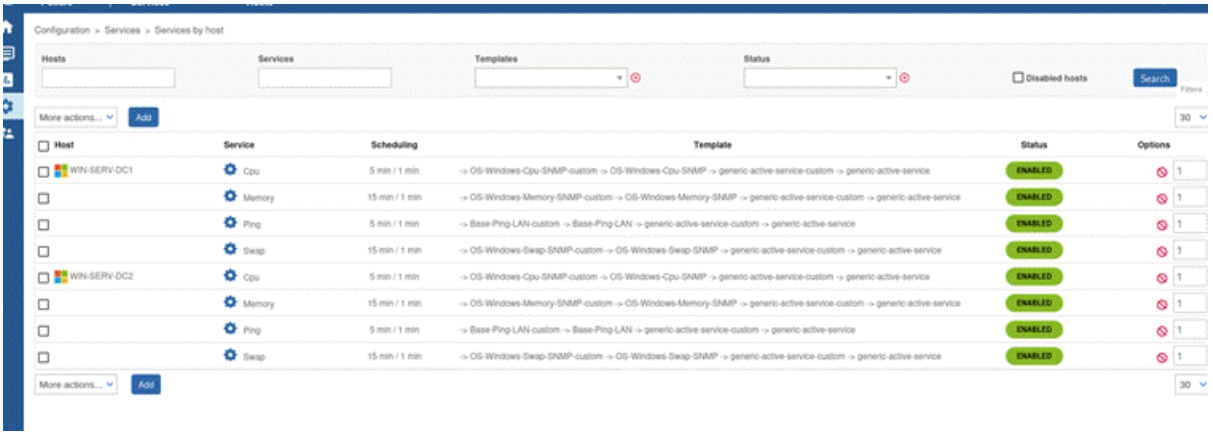
Étape 7 : Installez SNMP

Rendez-vous dans le menu Configuration > Hôtes > Hôtes (simplifiés) et cliquez sur Ajouter :



Étape 8 : Remplir avec vos informations comme ci-dessus ainsi que cliquez sur Ajouter une nouvelle entrée dans le champ Modèles, puis sélectionnez le modèle OS-Windows-SNMP-custom et enregistrez en cliquant sur Sauvegarder.

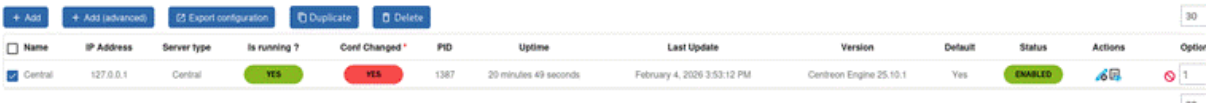
Rendez-vous dans le menu Configuration > Services > Services par hôte. Un ensemble d'indicateurs a été déployé automatiquement :



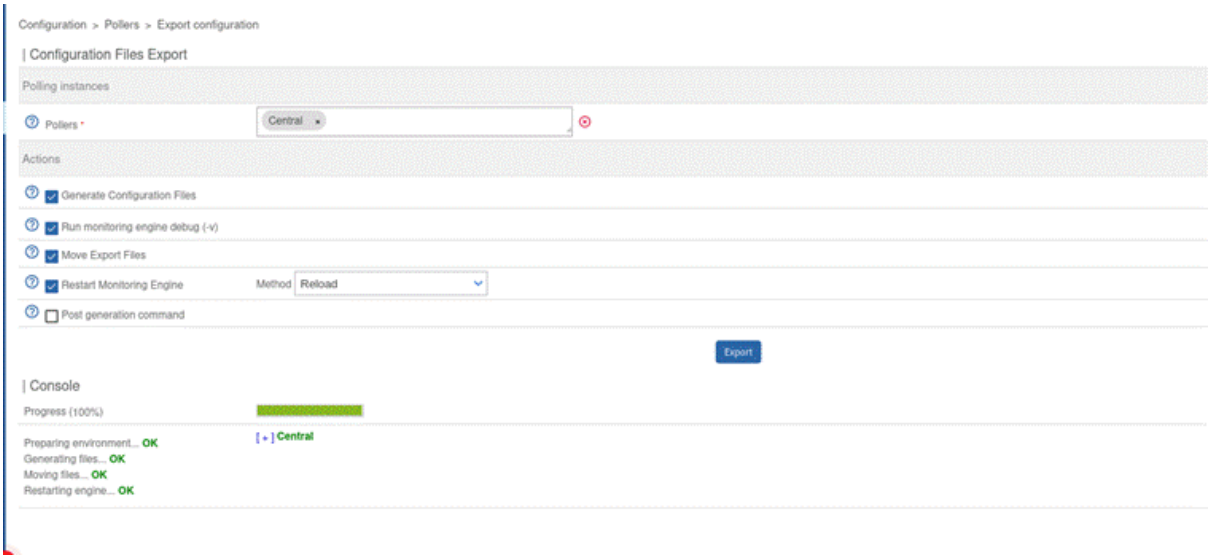
Allez à la page Configuration > Collecteurs > Collecteurs. La page affiche l'état de votre plateforme SaaS (collecteur Central) et de tous les collecteurs qui y sont reliés : les changements sont signalés dans la colonne Changement de configuration.

Sélectionnez le collecteur dont la configuration a changé.

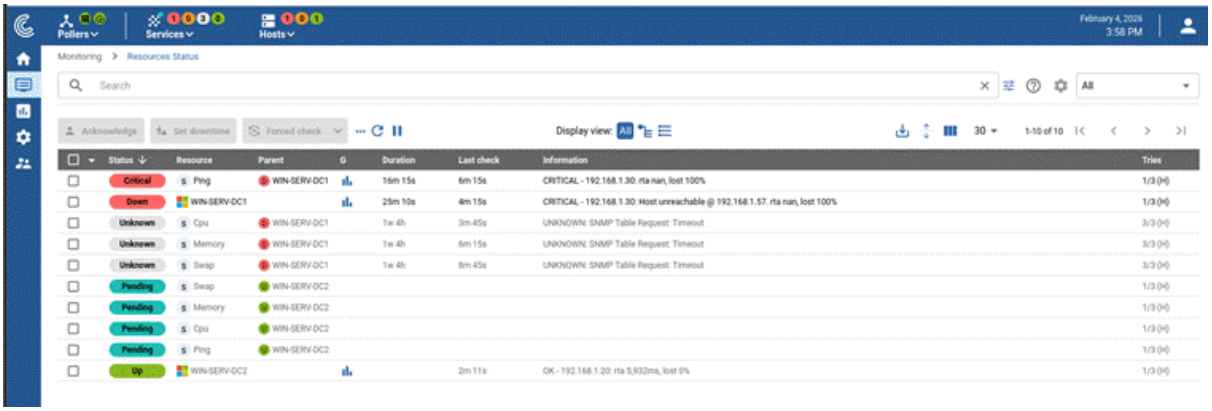
Cliquez sur Exporter la configuration.



Cochez les cases suivantes (voir la section Options d'export) : Générer les fichiers de configuration Lancer le débogage du moteur de supervision (-v) Déplacer les fichiers générés Redémarrer l'ordonnanceur. Utilisez la méthode : Recharger : lorsque vous avez créé, supprimé ou modifié des objets supervisés Redémarrer : lorsque vous avez apporté des changements à la communication entre un collecteur et la plateforme SaaS, ou à la configuration du moteur de collecte. Un redémarrage prend plus de temps qu'un rechargement. Cliquez sur Exporter. Un log de l'export s'affiche.



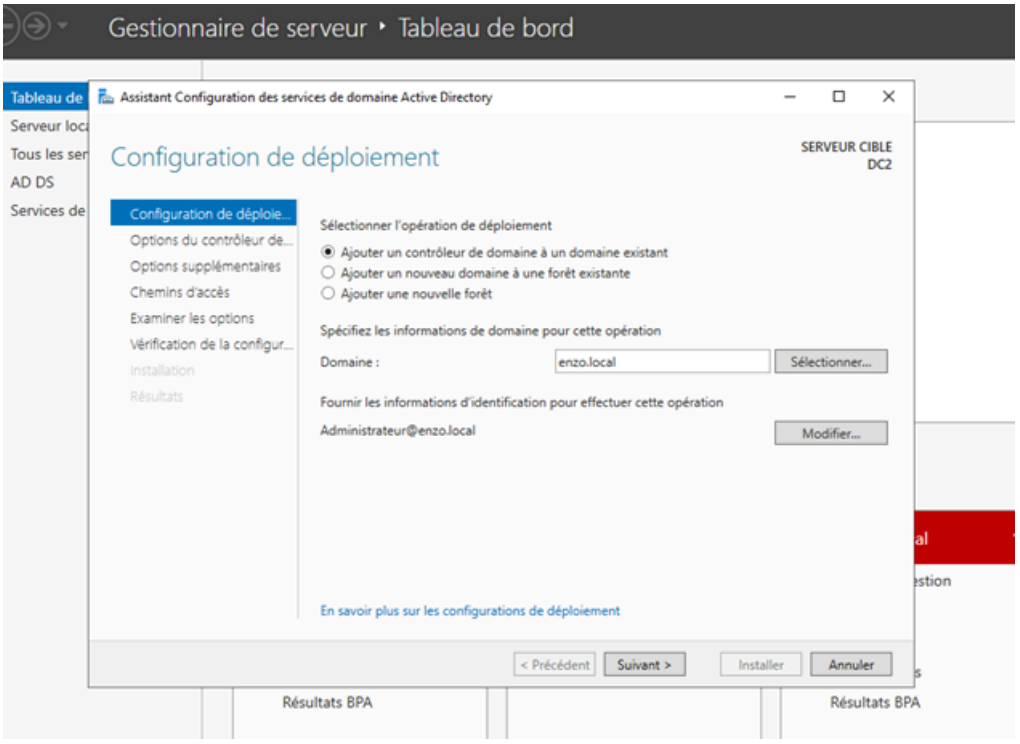
Rendez-vous dans le menu Monitoring > Status des Resources et positionnez le filtre sur Tous pour récupérer tous les indicateurs quel que soit leur état :



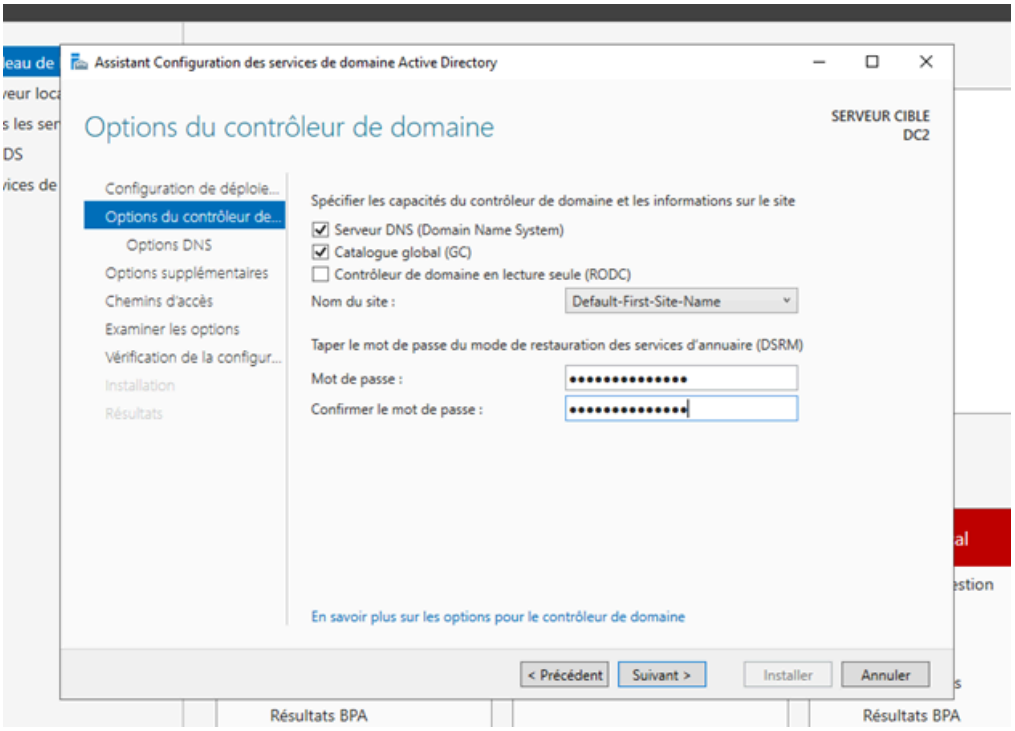
Nous pouvons voir que mon WIN-SERV-DC2 est bien Up.

.

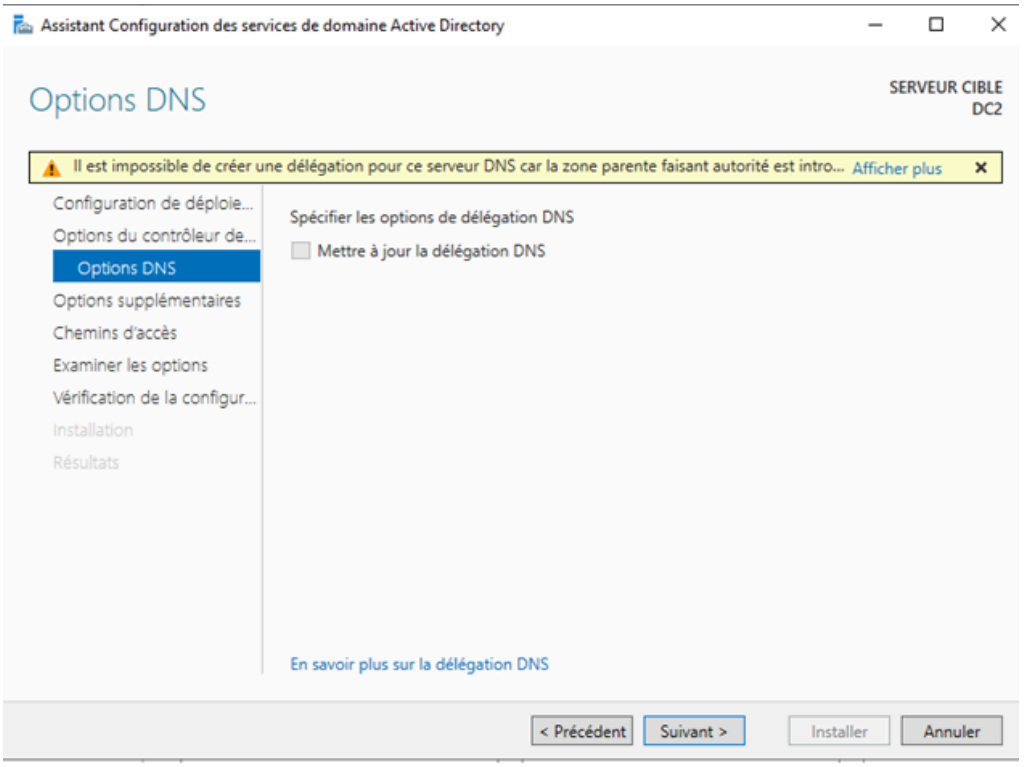
Déploiement d’un AD en redondance



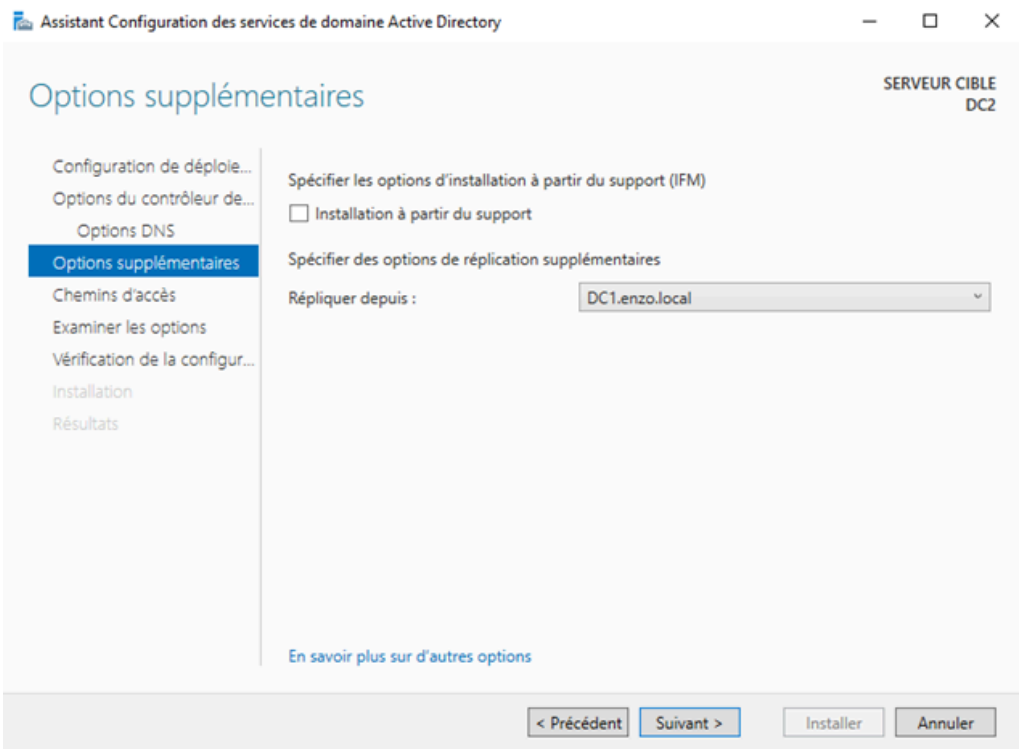
Etape 1 : Lors de l’installation de l’AD DS sélectionner « Ajouter un contrôleur de domaine à un domaine existant », puis entrer le nom de domaine enfin faites Suivant.



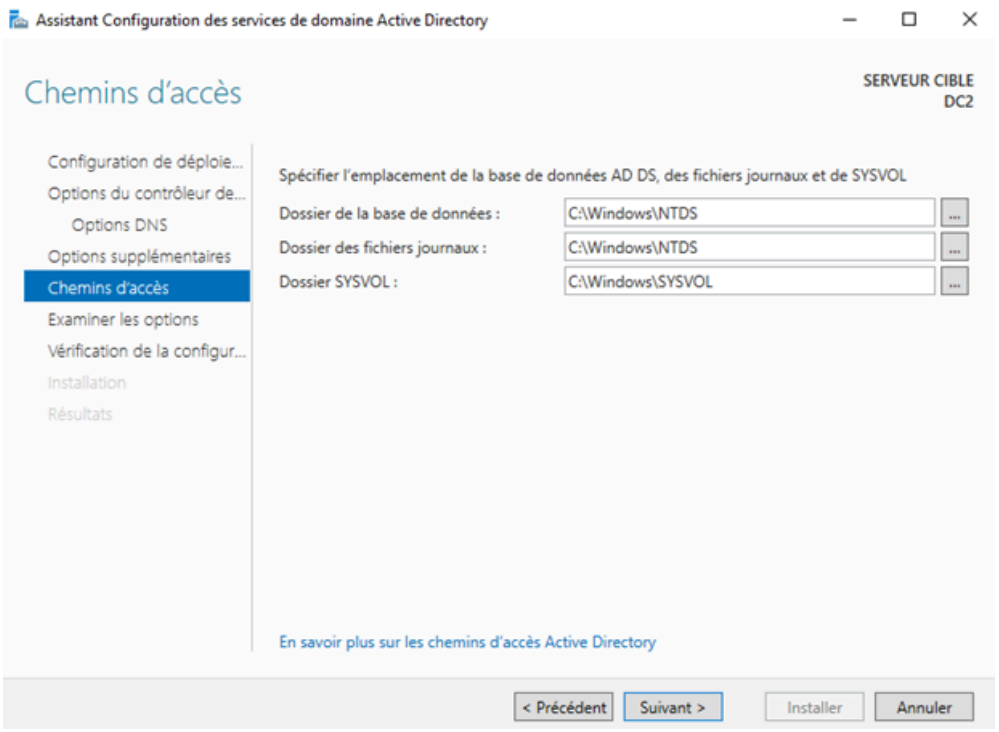
Etape 2 : Entrer un mot de passe robuste et faites Suivant.



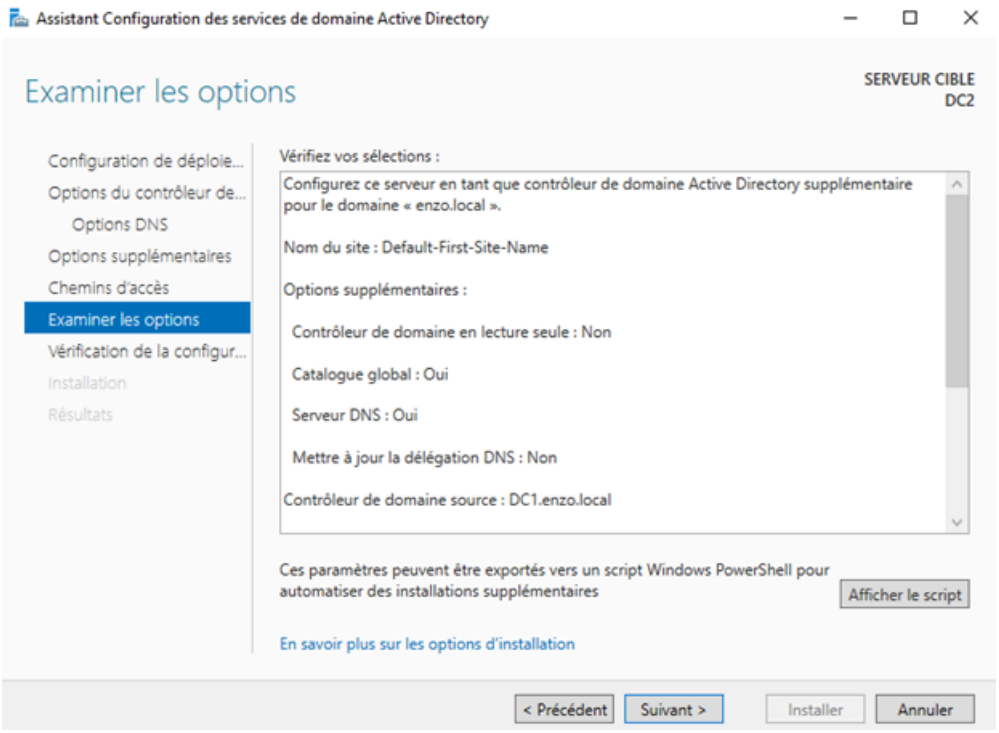
Etape 3 : sur cette page faites Suivant



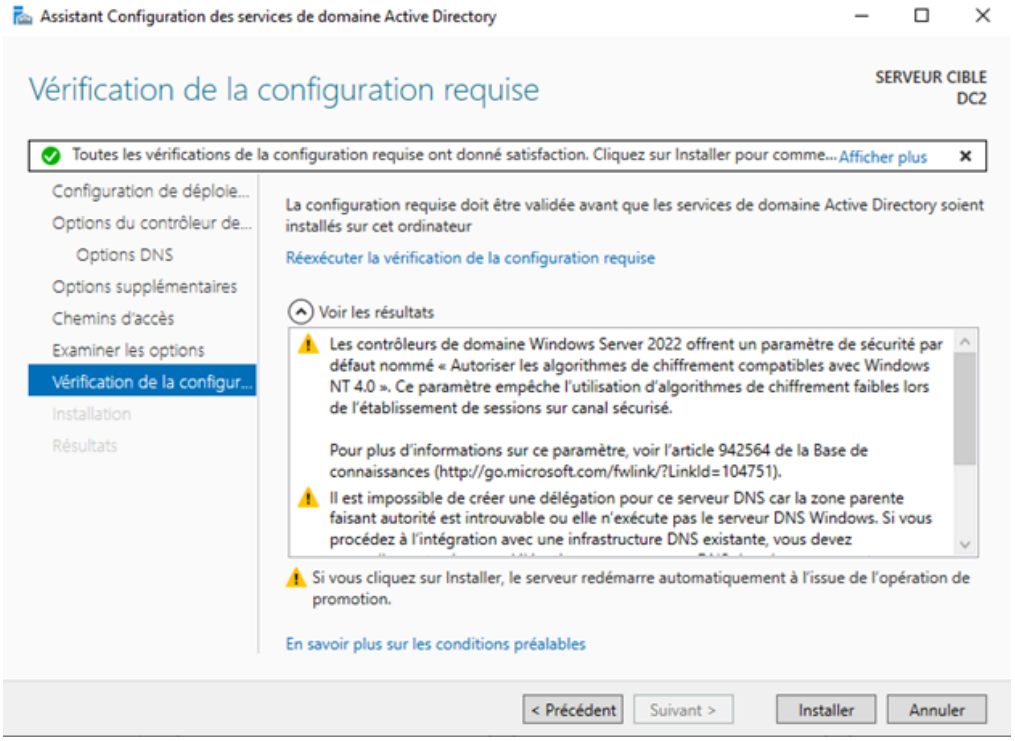
Etape 4 : Ici il faut sélectionner le FQDN de votre premier AD et faire Suivant



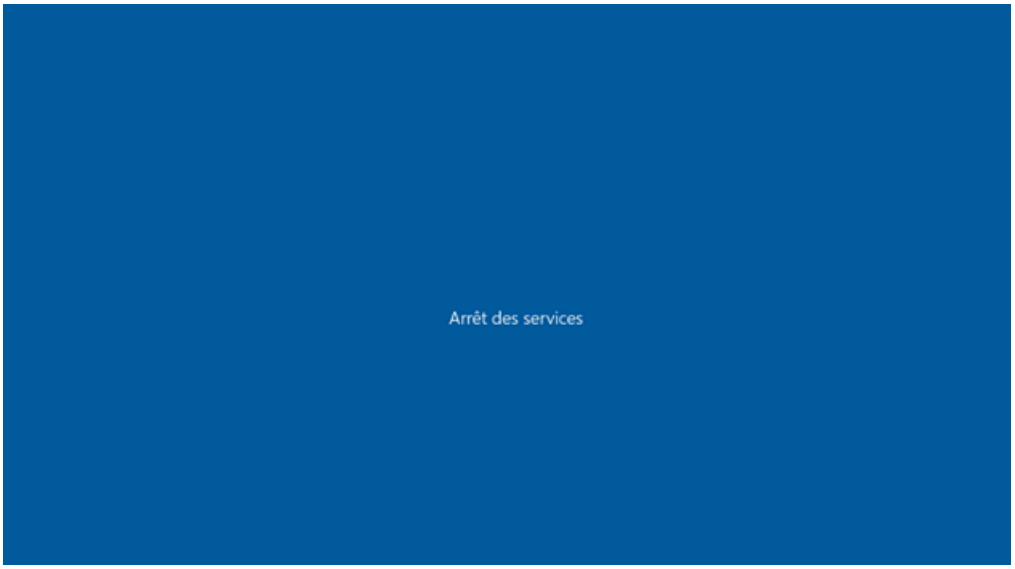
Etape 5 : Sur cette page faites Suivant



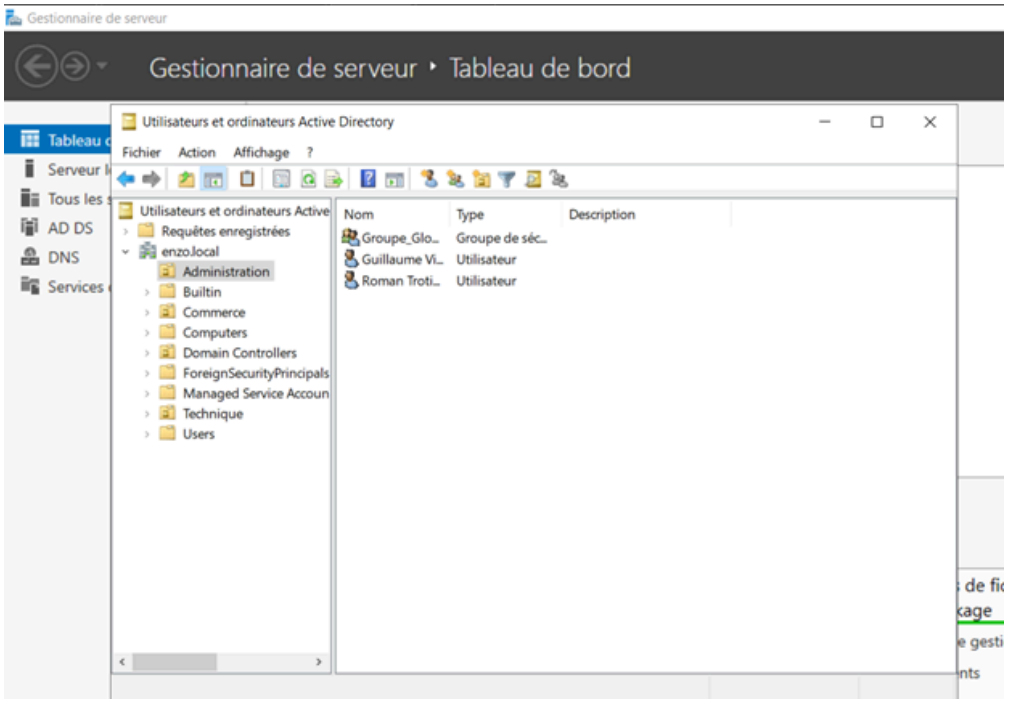
Etape 6 : Faire de nouveaux Suivant



Etape 7 : Cliquer sur Installer



Etape 8 : Le Windows Server redémarre



Étape Finale : Vous voici enfin sur l’AD ici nous pouvons retrouver mes UO et Utilisateur du domaine, la redondance est maintenant fini.

Installation de GLPI

Avant d'installer GLPI, il va falloir préparer la machine ou le serveur qui va l'accueillir. Pour pouvoir déployer efficacement le logiciel nous aurons besoin d'un serveur LAMP. L'acronyme LAMP signigie : Linux Apache Mysql PHP C'est un ensemble de logiciels qui a plusieurs fonctions :

Linux : est le système de base

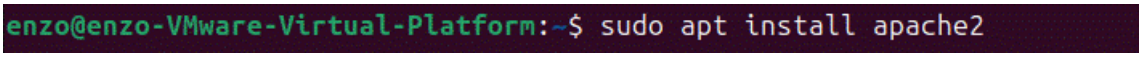
Apache : est un serveur web frontal, il va permettre de répondre aux requêtes des navigateurs pour l'affichage des pages web

MySQL : est un système de gestion de base de données, nous pouvons également utiliser MariaDB qui est un équivalent

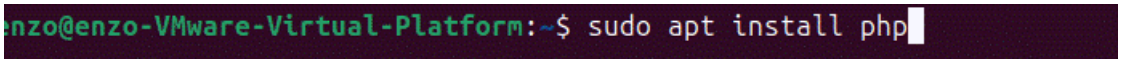
PHP : est un langage informatique qui permet la génération de pages web dynamique. Ce dernier va également nous permettre de communiquer avec MySQL. Il faudra également mettre son système à jour, histoire de ne pas avoir de soucis avec quelconque dépendances. Il est possible de le faire avec la commande suivante :

sudo apt update && sudo apt upgrade -y

Tous ces services sont des prérequis, car GLPI est une application qui sera accessible et gérée/utilisée depuis un navigateur.



Installation de apache2



Installation de php

```
enzo@enzo-VMware-Virtual-Platform:~$ sudo apt install php-mysql
```

Installation de Php-mysql

```
enzo@enzo-VMware-Virtual-Platform:~$ sudo apt install php-curl php-gd php-intl php-json php-mbstring php-xml php-zip php-intl php-bcmath php-phar phpzip php-bz2
```

Installation des instances de php

```
enzo@enzo-VMware-Virtual-Platform:~$ sudo apt install mysql-server
```

Installation de mysql-server

```
enzo@enzo-VMware-Virtual-Platform:~$ sudo mysql_secure_installation
```

Installation de mysql_secure_installation

```
Press y|Y for Yes, any other key for No: y
```

```
Remove anonymous users? (Press y|Y for Yes, any other key for No) : Y
```

Répondre Y

```
enzo@enzo-VMware-Virtual-Platform:~$ sudo mysql
```

Configurer mysql

```
mysql> CREATE DATABASE GLPI;
Query OK, 1 row affected (0,02 sec)
```

```
mysql> CREATE USER 'admin'@'localhost' IDENTIFIED BY 'Enzo123.';
```

```
mysql> GRANT ALL PRIVILEGES ON GLPI.* TO 'admin'@'localhost';
```

```
mysql> FLUSH PRIVILEGES;
```

Remplir avec vos informations

```
enzo@enzo-VMware-Virtual-Platform:~$ wget https://github.com/glpi-project/glpi/releases/download/11.0.2/glpi-11.0.2.tgz
```

Installation de GLPI

```
enzo@enzo-VMware-Virtual-Platform:~$ sudo tar -xzf glpi-11.0.2.tgz -C /var/www/
```

Décompresser le fichier

```
enzo@enzo-VMware-Virtual-Platform:/$ sudo chmod -R 755 /var/www/glpi
```

Donnez les bonnes permissions

```
enzo@enzo-VMware-Virtual-Platform:/$ sudo chown -R www-data:www-data /var/www/glpi
```

Changer le propriétaire

```
enzo@enzo-VMware-Virtual-Platform:/$ sudo nano /etc/apache2/sites-available/glpi.conf
```

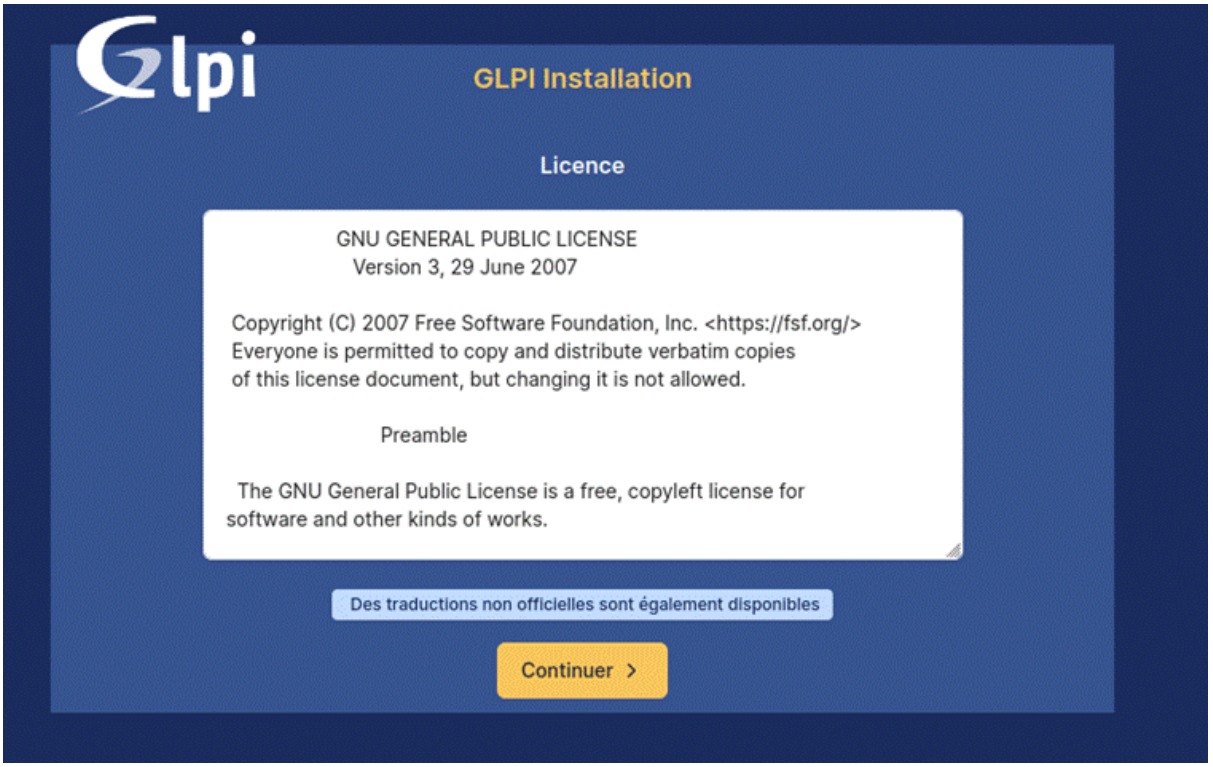
Ouvrez le fichier glpi.conf

```
 GNU nano 7.2                                          /etc/apache2/sites-available/glp
<VirtualHost *:80>
        ServerName GLPI
        DocumentRoot /var/www/glpi/public

        <Directory /var/www/glpi/public>
                Require all granted
                RewriteEngine On

                # Ensure authorization headers are passed to PHP.
                # Some Apache configurations may filter them and break usage of API, CalDAV, ...
                RewriteCond %{HTTP:Authorization} ^(.+)$
                RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
                # Redirect all requests to GLPI router, unless file exists.
                RewriteCond %{REQUEST_FILENAME} !-f
                RewriteRule ^(.*)$ index.php [QSA,L]
        </Directory>
</VirtualHost>
```

Modifier avec vos informations

```
enzo@enzo-VMware-Virtual-Platform:/$ sudo a2ensite glpi.conf
Enabling site glpi.
To activate the new configuration, you need to run:
  systemctl reload apache2
enzo@enzo-VMware-Virtual-Platform:/$ sudo a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
  systemctl restart apache2
enzo@enzo-VMware-Virtual-Platform:/$ sudo systemctl reload apache2
```

redémarrer vos services et lancer 127.0.0.1 sur votre navigateur de recherche.



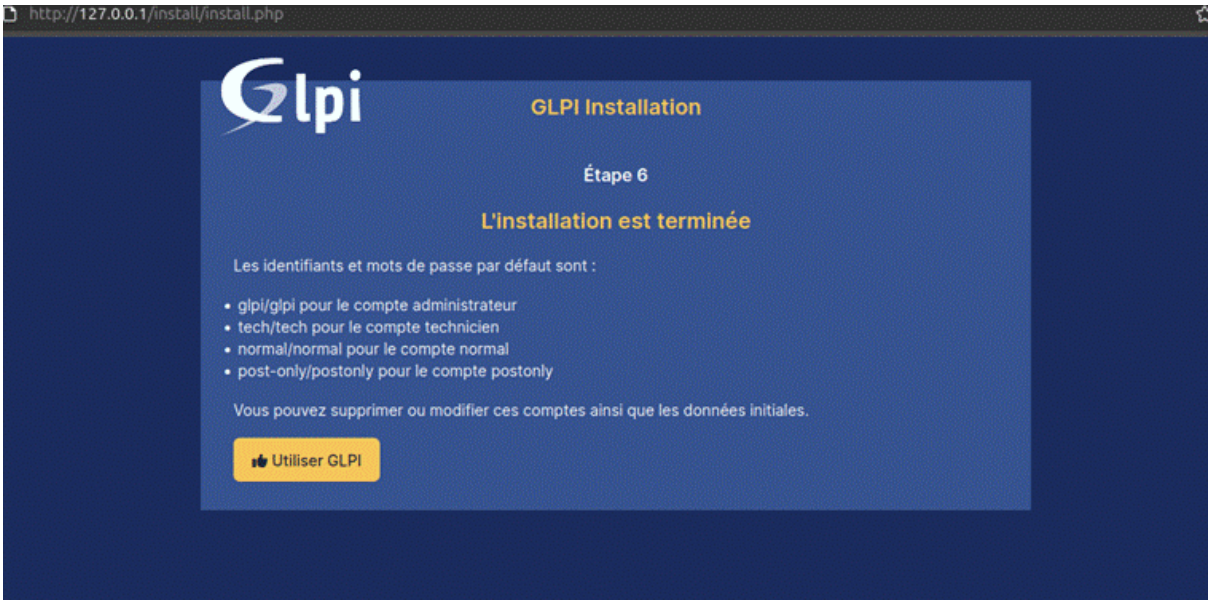
Vous voici sur l’interface de GLPI

Faire Installer

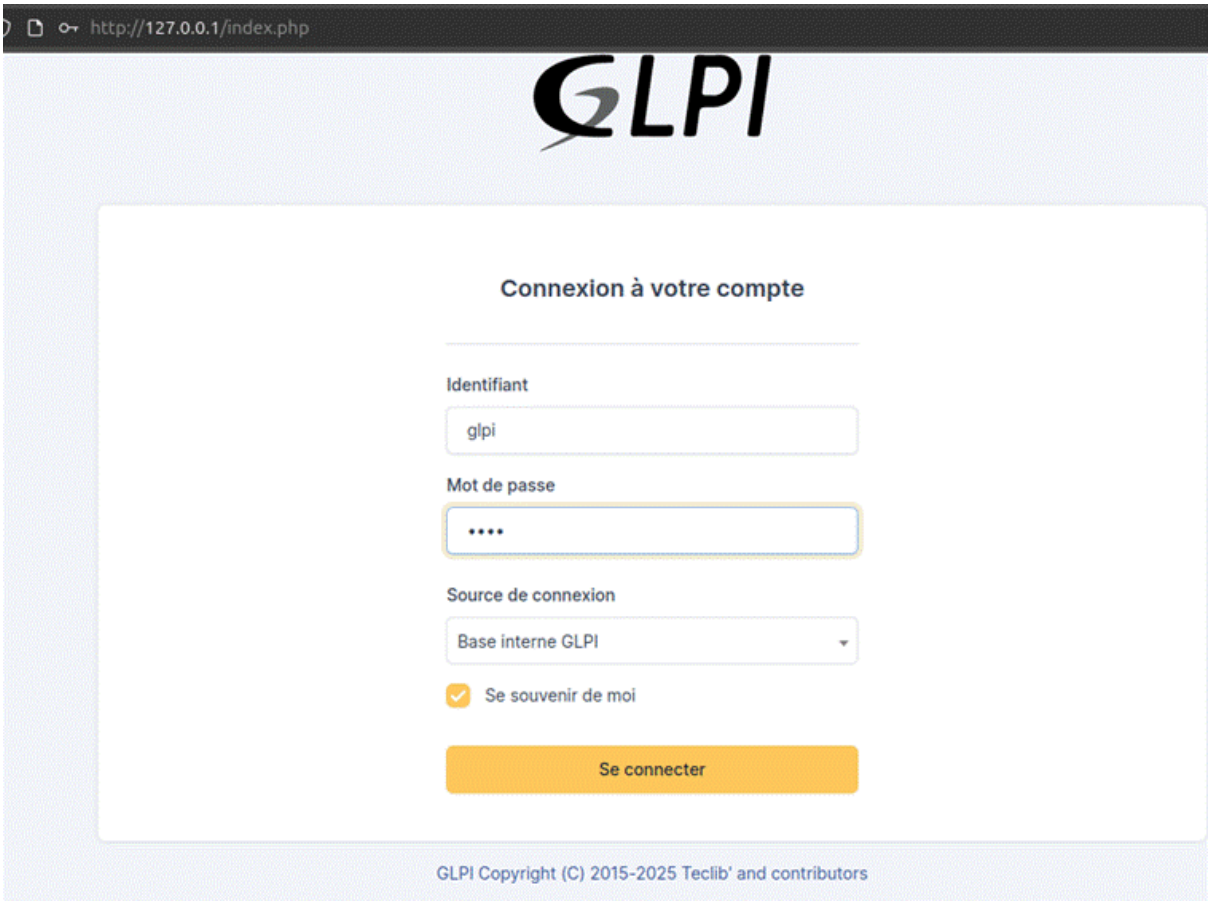
Entre les logins de mysql

Initialisation de la base de données

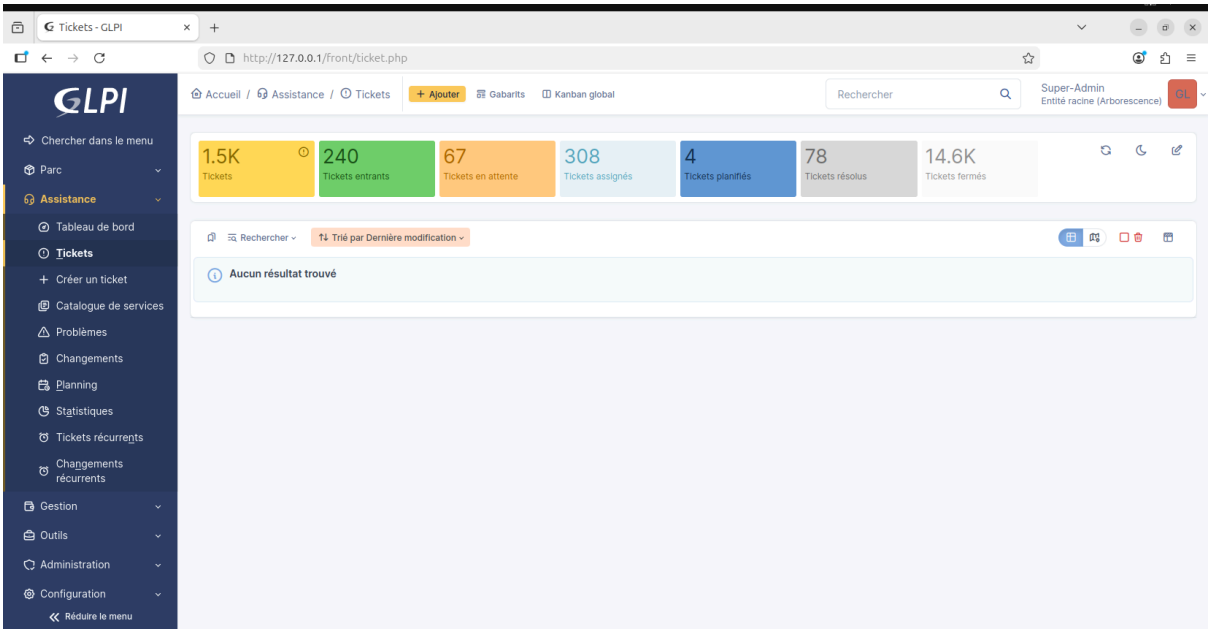
Cliquer sur continuer



Puis Utiliser GLPI



Entrer les identifiant par défait glpi / glpi
Et vous voici dans l'interface de GLPI



Voici l'interface de ticketing.

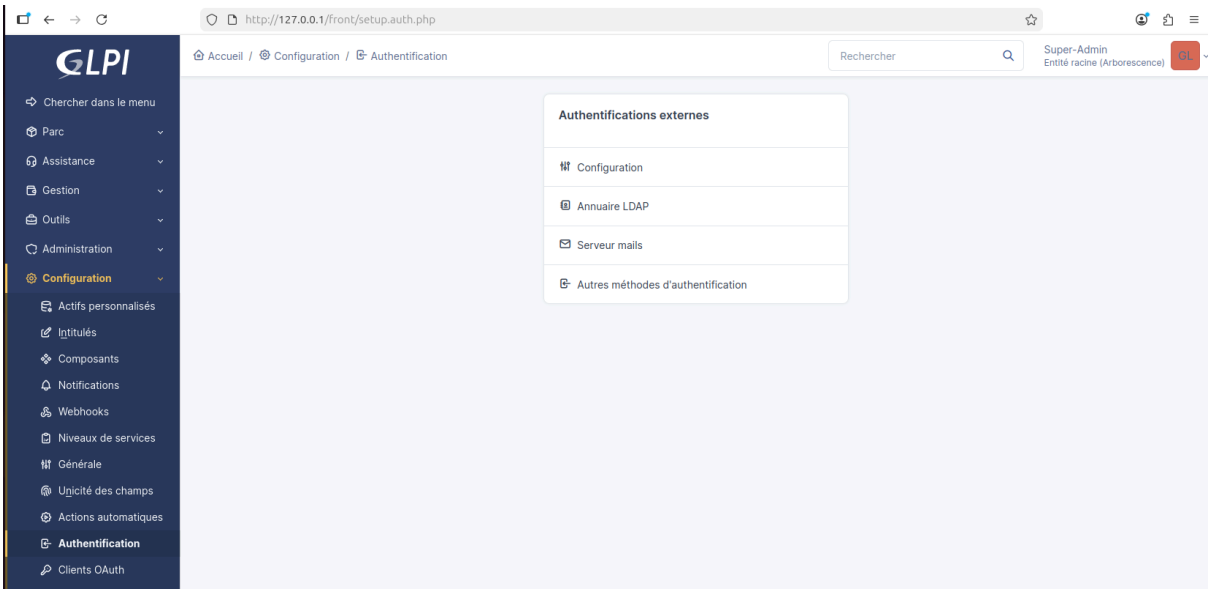
Configuration de l’authentification LDAP via l’Active Directory

Connectez-vous à votre serveur GLPI et exécutez les deux commandes suivantes pour mettre à jour le cache des paquets et procéder à l'installation de l'extension.

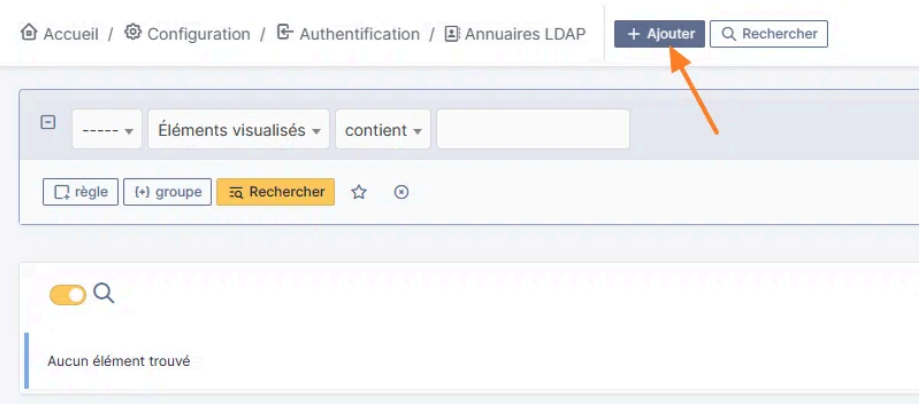
```
sudo apt-get update
sudo apt-get install php-ldap
```

Cette extension sera installée et activée dans la foulée. Vous n'avez pas besoin de relancer le serveur.

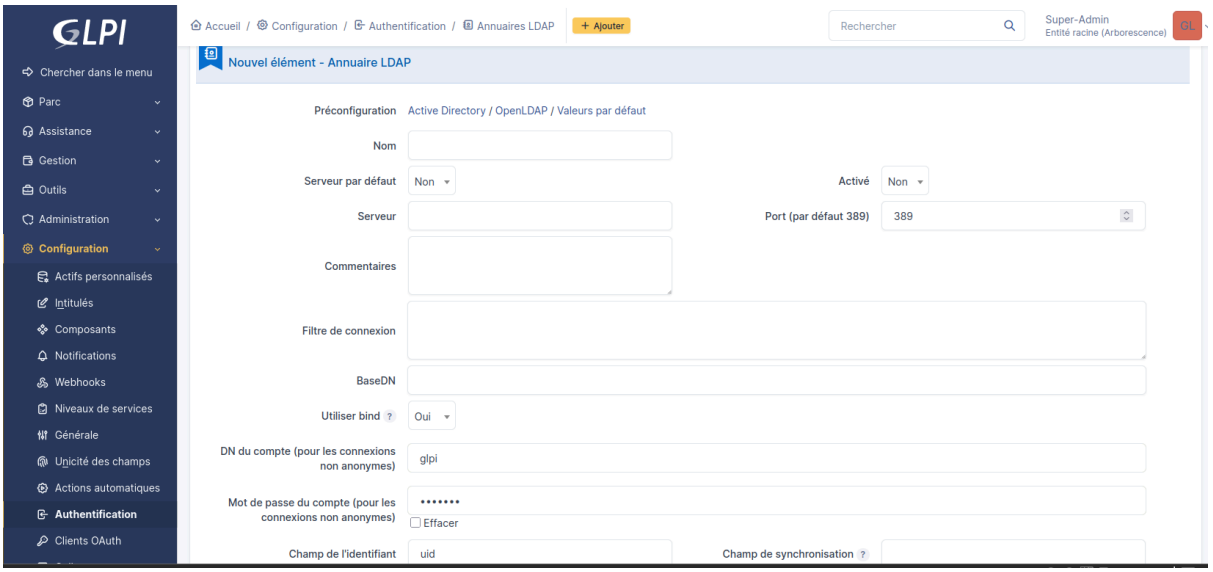
Désormais, nous allons ajouter notre annuaire Active Directory à GLPI. Connectez-vous à GLPI avec un compte administrateur, puis dans le menu "Configuration", cliquez sur "Authentification".

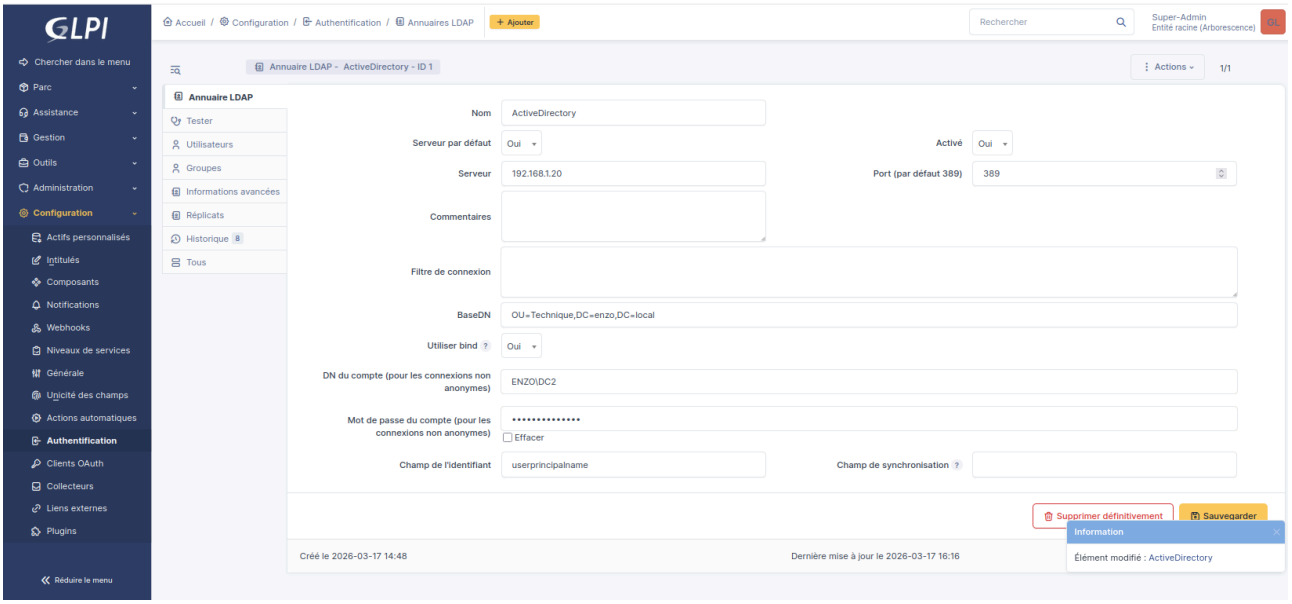


Au centre de l'écran, cliquez sur "Annuaire LDAP"

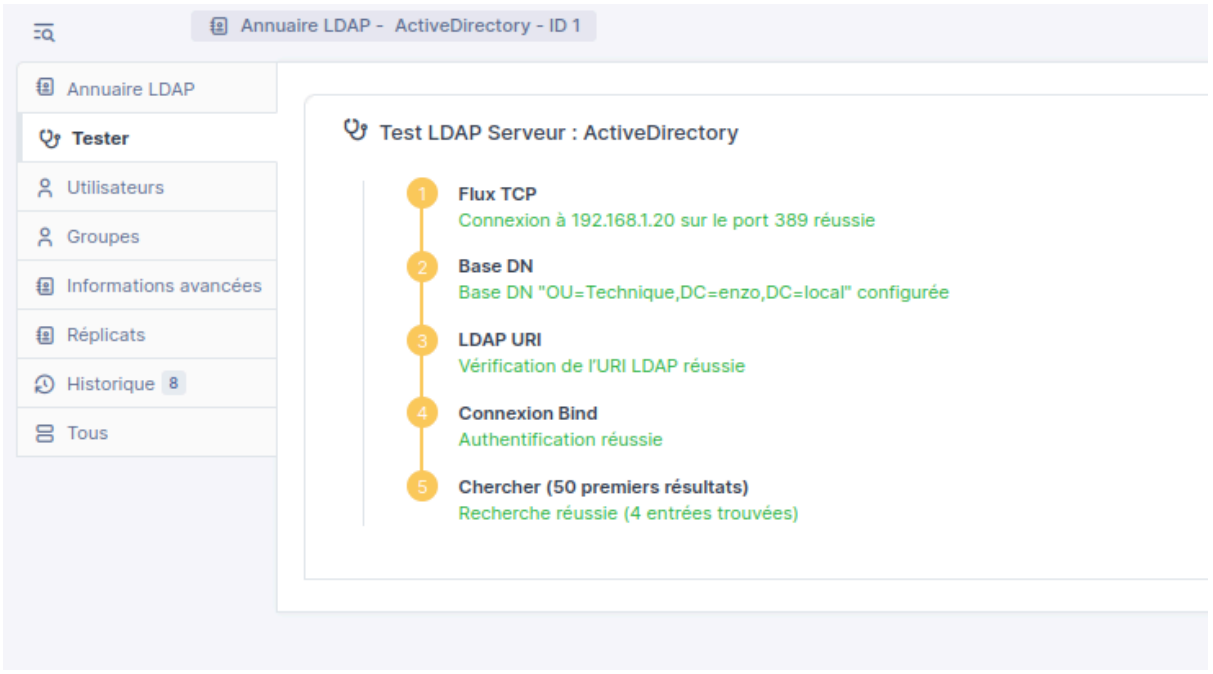


Puis, cliquez sur le bouton "Ajouter".



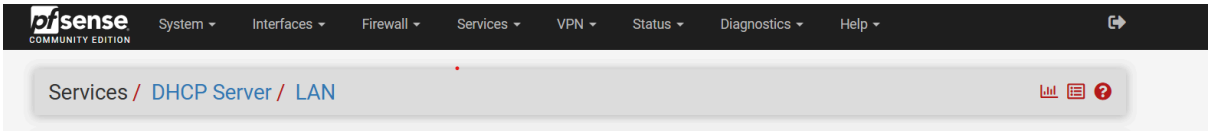


Remplir vos informations comme cela.

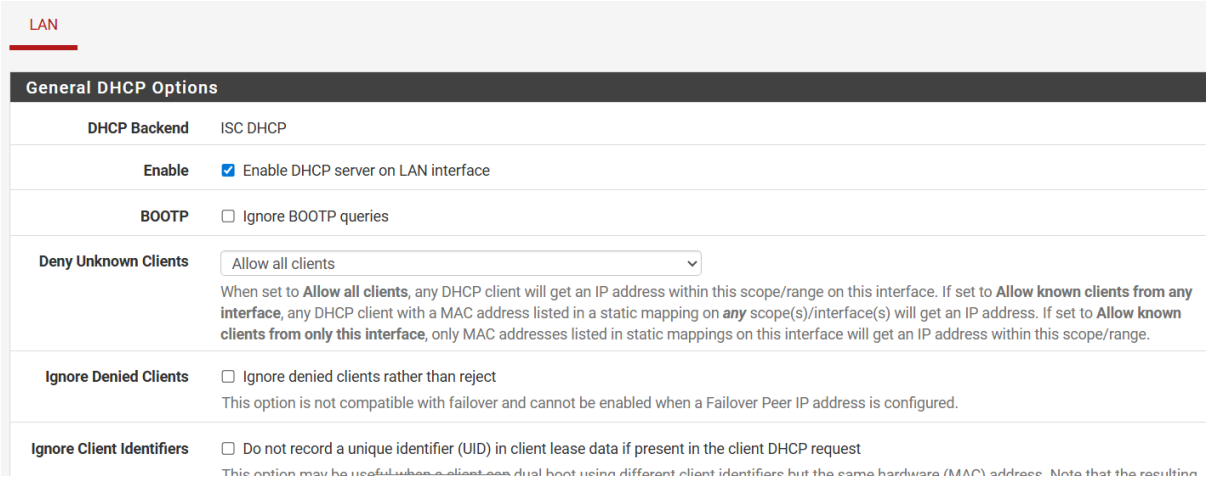


Vérifier que le test soit bon avant de continuer

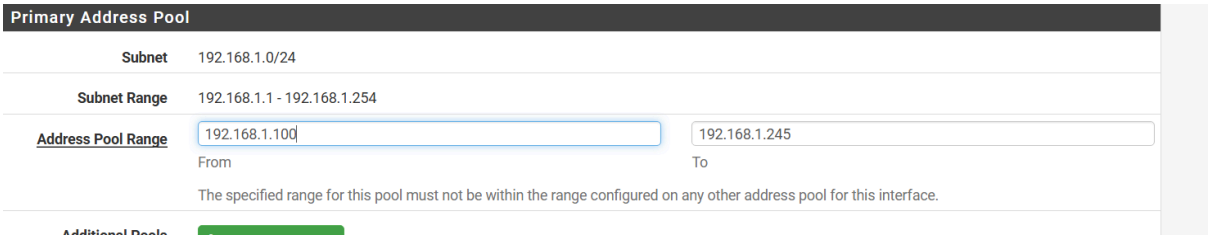
Mise en place du DHCP sur Pfsense



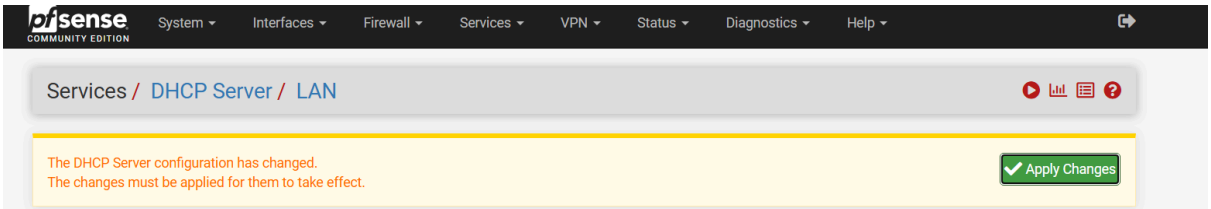
Pour commencer rendez-vous sur Services / DHCP Server / LAN



Cliquer sur enable le server DHCP sur le Lan

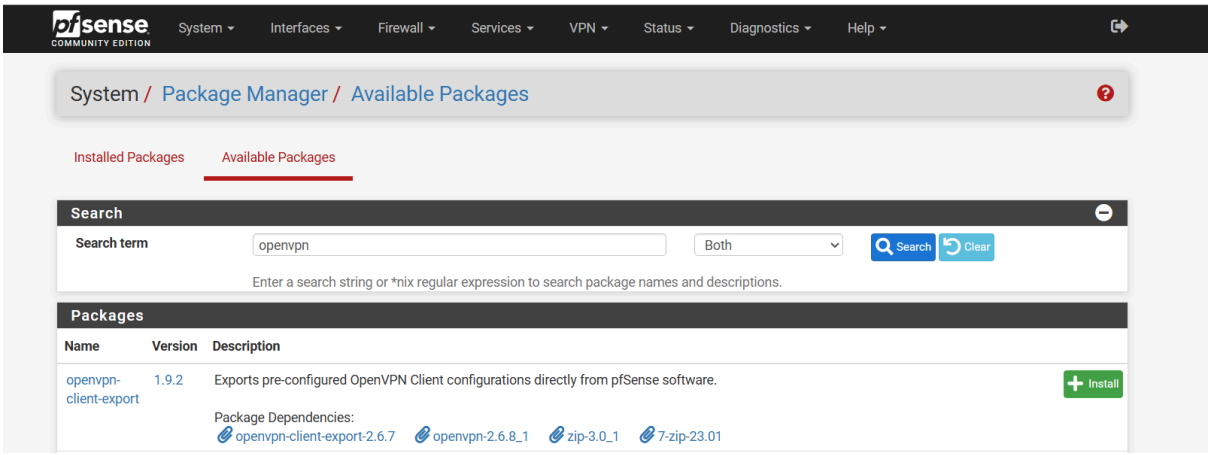


Ici entrer votre plage d'IP que le serveur DHCP va pouvoir attribuer. Et cliquer sur Save

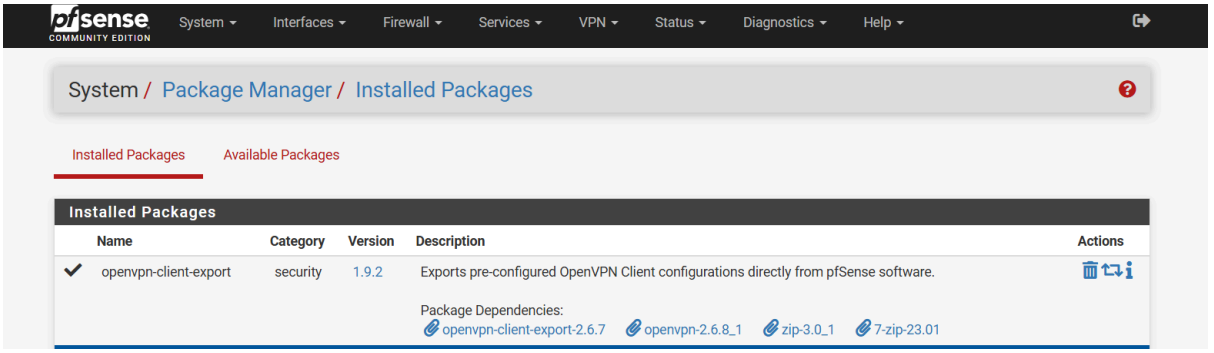


Le serveur DHCP est maintenant créé il suffit d'appliquer les changements.

Mise en place d’un VPN

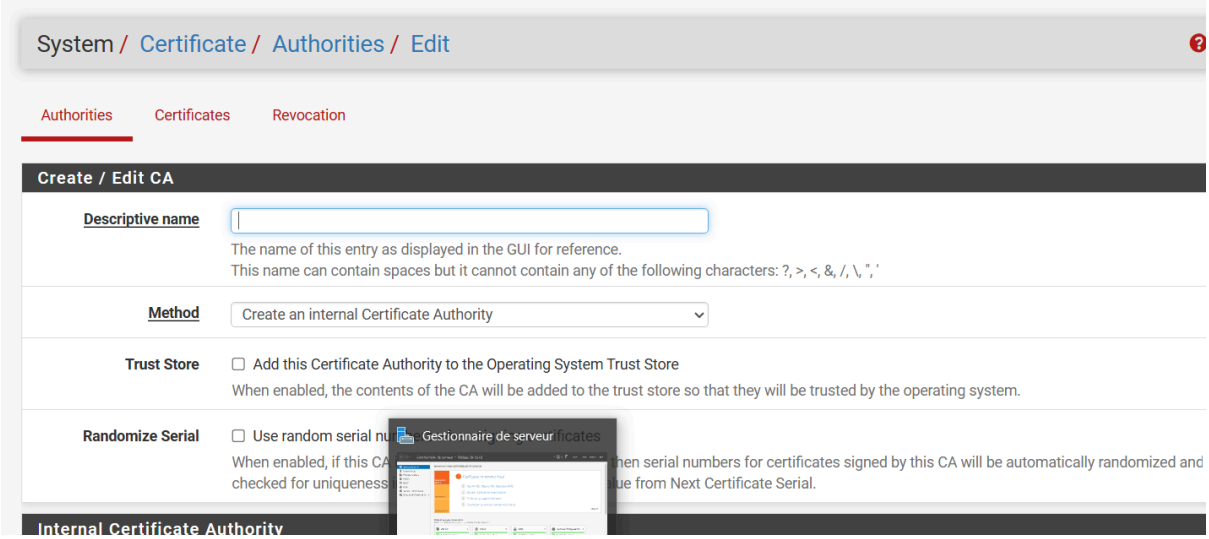


1. Connectez-vous à l'interface web de pfSense
2. Allez dans **System → Package Manager**
3. Cliquez sur l'onglet **Available Packages**
4. Recherchez **"openvpn-client-export"**
5. Cliquez sur **Install** puis confirmez

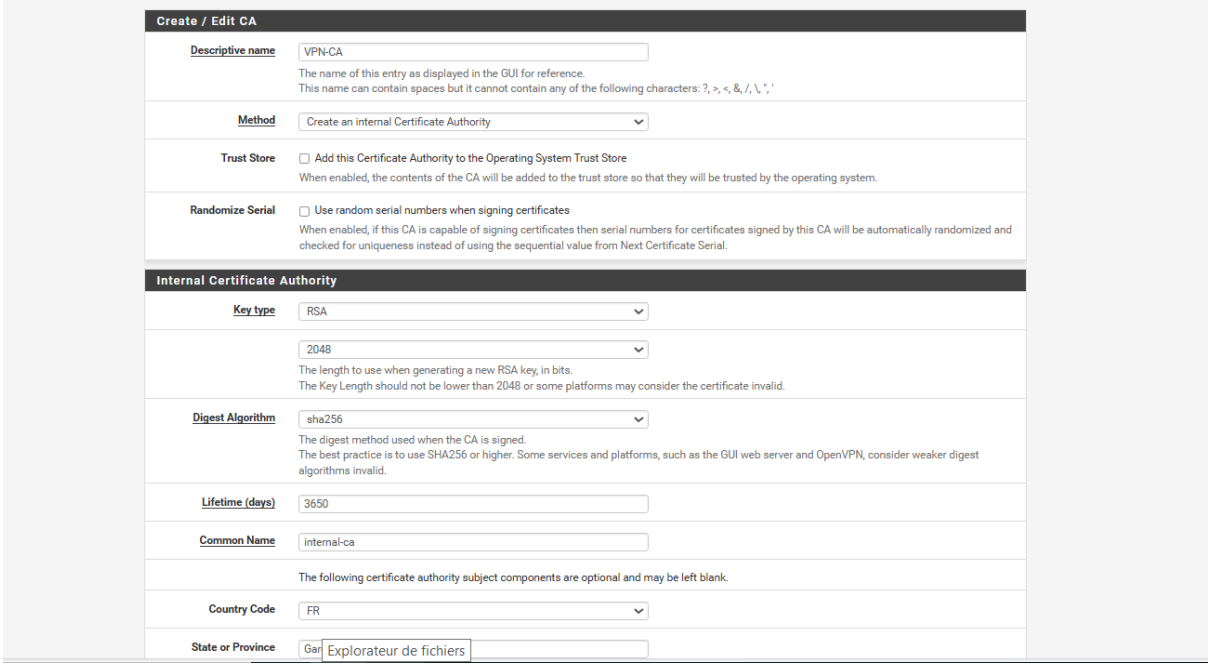


Le package doit apparaître dans l'onglet "Installed Packages" une fois l'installation terminée.

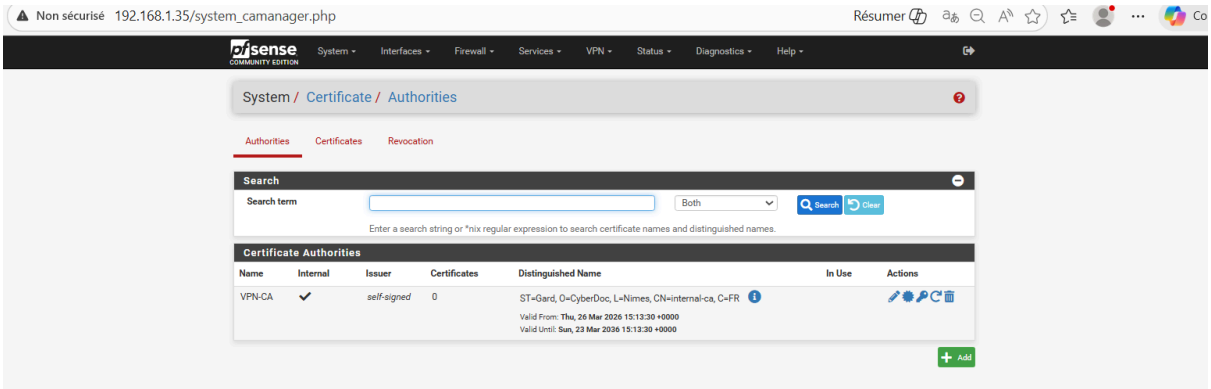
Aller maintenant dans System / Certificates / Authorities



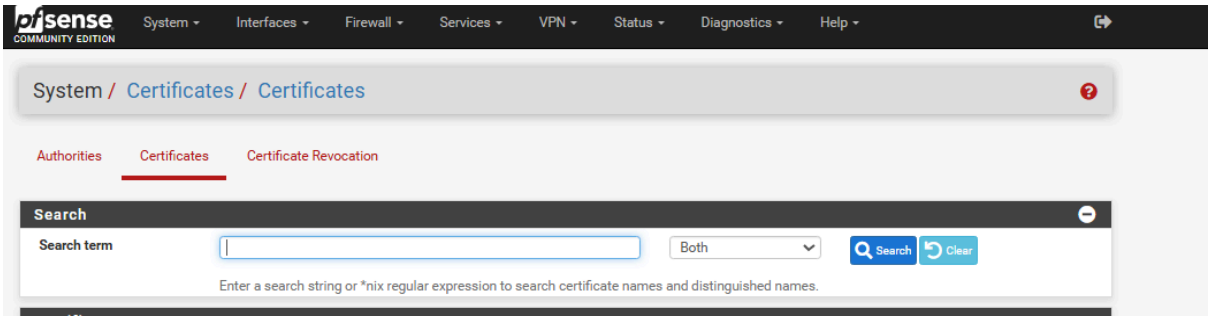
Remplir avec vos informations



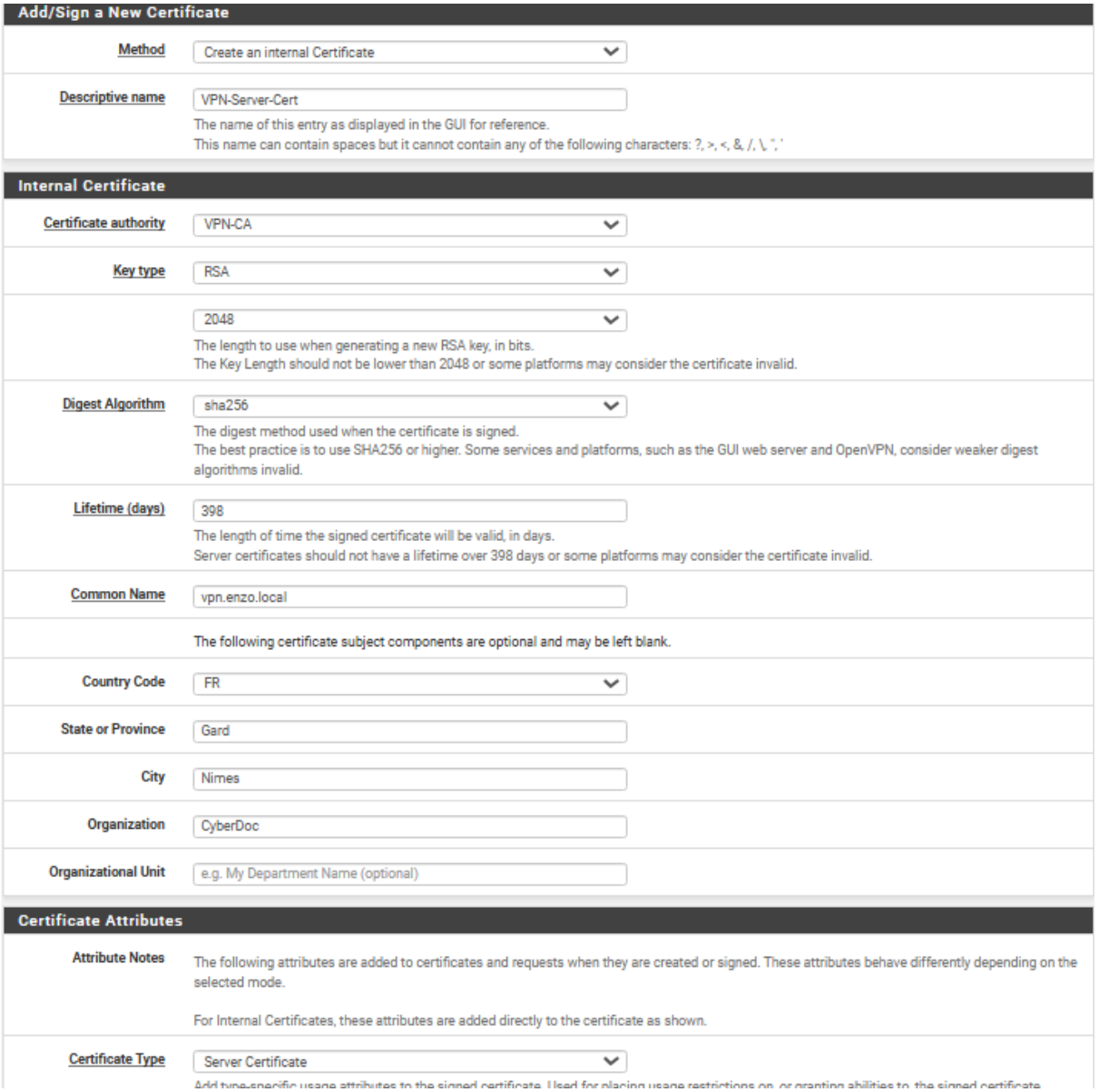
Une fois créée vous le retrouver ici



Dans System / Certificates / Certificates

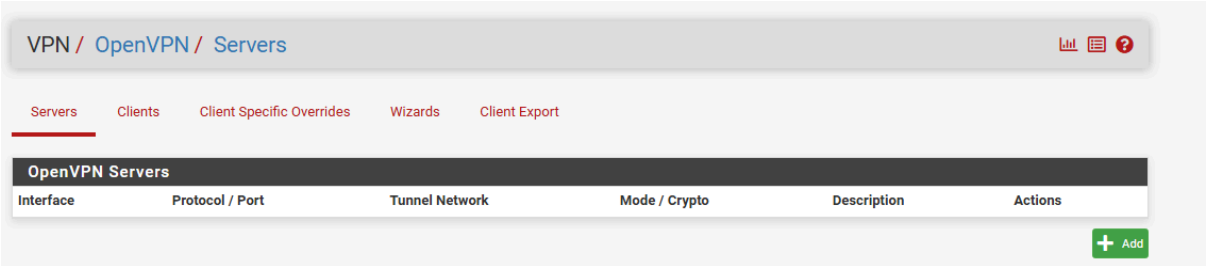


Faites Add et configurer le certificat

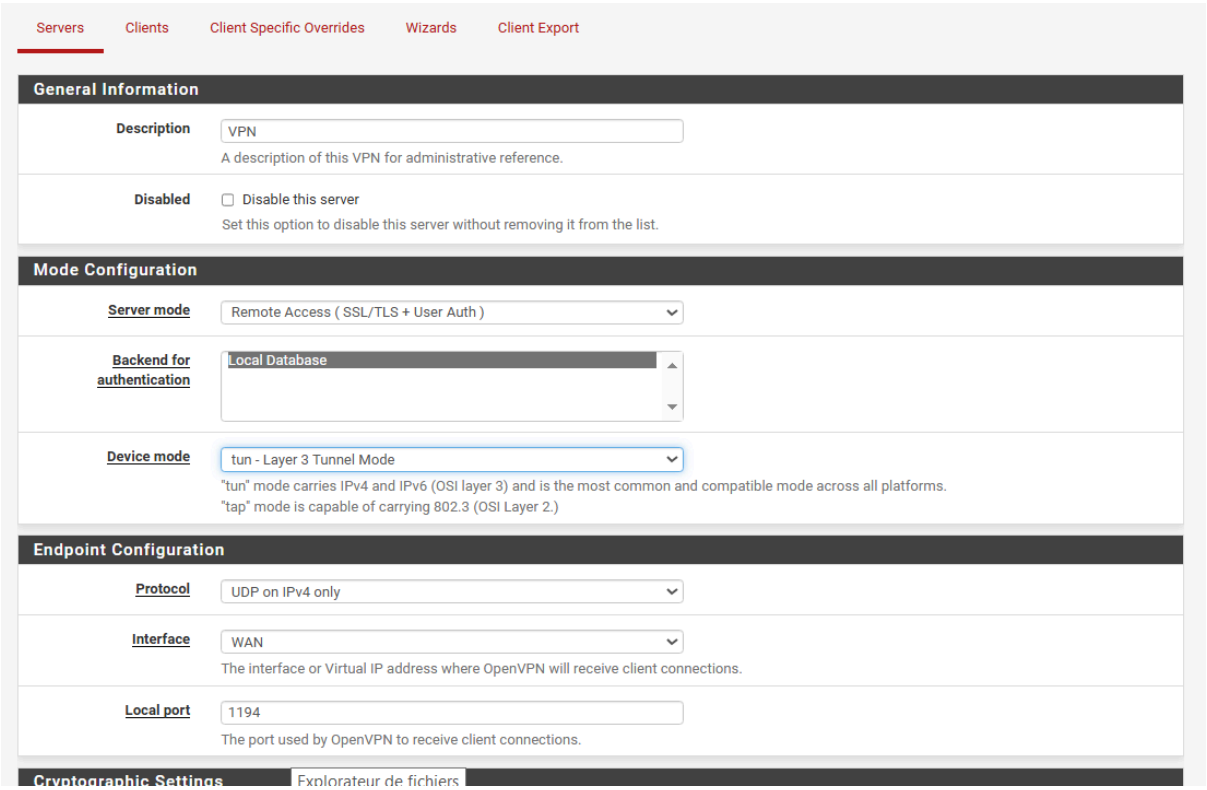


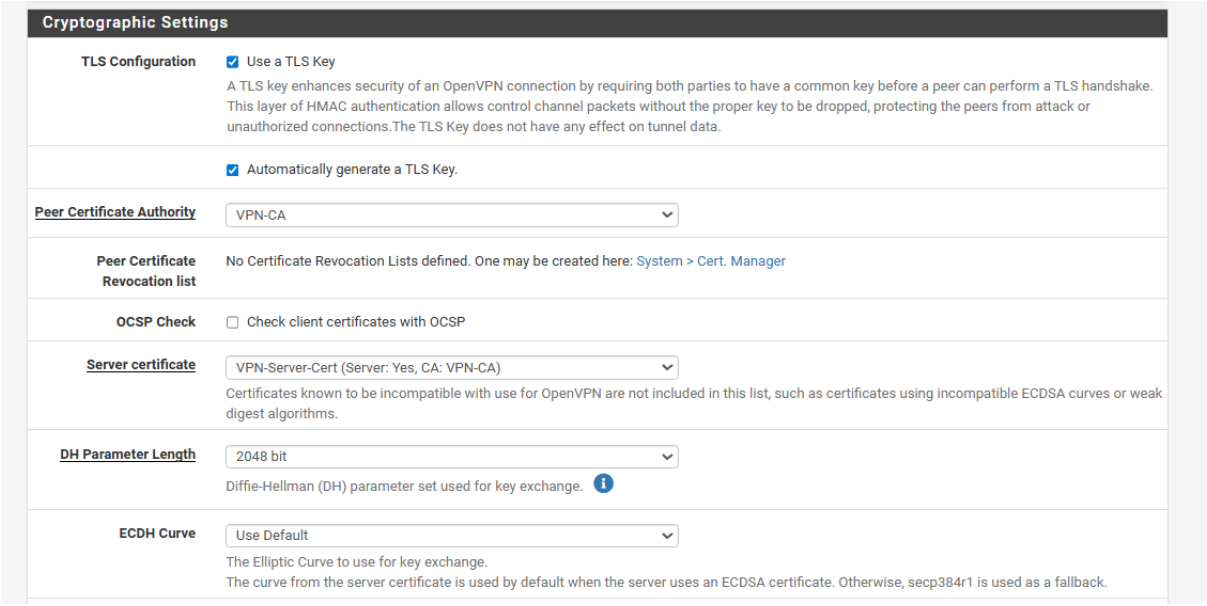
Remplir avec vos informations

Ensuite allez dans VPN / OpenVPN / Servers



Faire add et remplir avec vos informations comme si dessous





The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.

Data Encryption Algorithms

Available Data Encryption Algorithms:
AES-192-CFB1 (192 bit key, 128 bit block)
AES-192-CFB8 (192 bit key, 128 bit block)
AES-192-GCM (192 bit key, 128 bit block)
AES-192-OFB (192 bit key, 128 bit block)
AES-256-CBC (256 bit key, 128 bit block)
AES-256-CFB (256 bit key, 128 bit block)
AES-256-CFB1 (256 bit key, 128 bit block)
AES-256-CFB8 (256 bit key, 128 bit block)
AES-256-GCM (256 bit key, 128 bit block)
AES-256-OFB (256 bit key, 128 bit block)

Available Data Encryption Algorithms
Click to add or remove an algorithm from the list

Allowed Data Encryption Algorithms:
AES-256-CBC

Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list

The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode.

Fallback Data Encryption Algorithm

AES-256-CBC (256 bit key, 128 bit block)

The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.

Auth digest algorithm

SHA256 (256-bit)

The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.

Hardware Crypto

No Hardware Crypto Acceleration

Certificate Depth

One (Client+Server)

When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.

Tunnel Settings

IPv4 Tunnel Network

10.0.8.0

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.

IPv6 Tunnel Network

This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

Redirect IPv4 Gateway

☐ Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway

☐ Force all client-generated IPv6 traffic through the tunnel.

IPv4 Local network(s)

192.168.1.0

IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network

Concurrent connections	10 Specify the maximum number of clients allowed to concurrently connect to this server.
Allow Compression	Refuse any non-stub compression (Most secure) Allow compression to be used with this VPN instance. Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack. Asymmetric compression allows an easier transition when connecting with older peers.
Push Compression	☐ Push the selected Compression setting to connecting clients.
Type-of-Service	☐ Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Inter-client communication	☐ Allow communication between clients connected to this server
Duplicate Connection	☐ Allow multiple concurrent connections from the same user When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session. Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.

Client Settings

Dynamic IP	☑ Allow connected clients to retain their connections if their IP address changes.
Topology	Subnet -- One IP address per client in a common subnet Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

Ping settings Explorateur de fichiers

VPN / OpenVPN / Servers

Servers | Clients | Client Specific Overrides | Wizards | Client Export

OpenVPN Servers

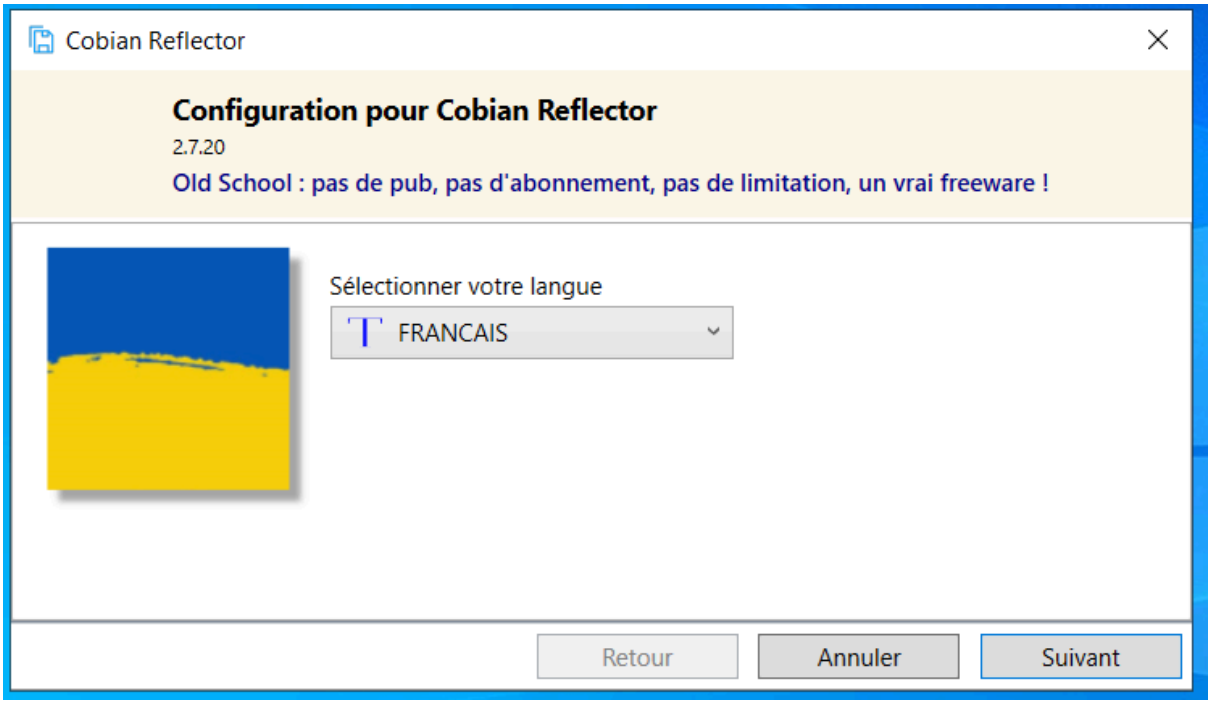
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.0.8.0/24	**Mode:** Remote Access (SSL/TLS + User Auth) **Data Ciphers:** AES-256-CBC **Digest:** SHA256 **D-H Params:** 2048 bits	VPN	

+ Add

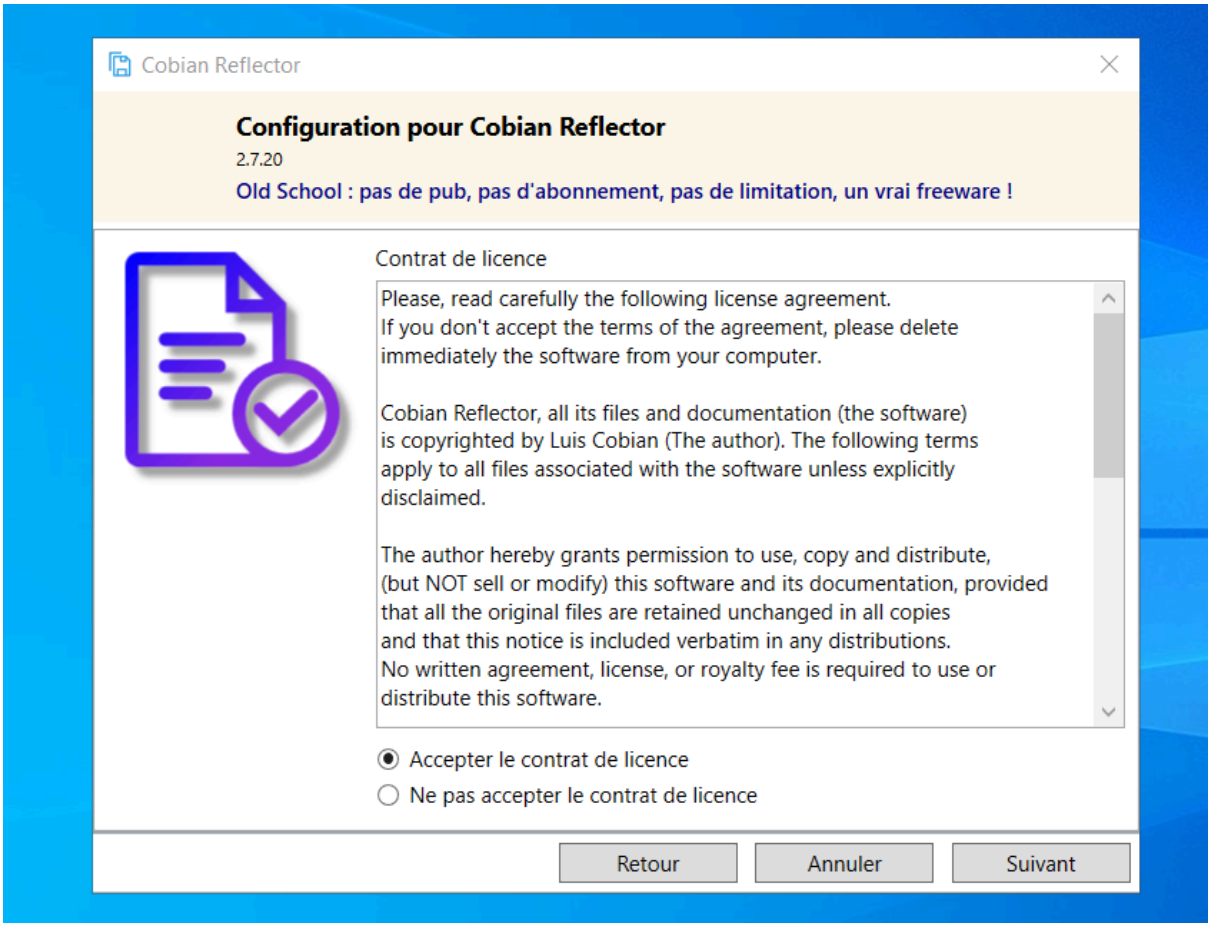
Installation de Cobian

Rendez-vous sur le site officiel de Cobian Backup

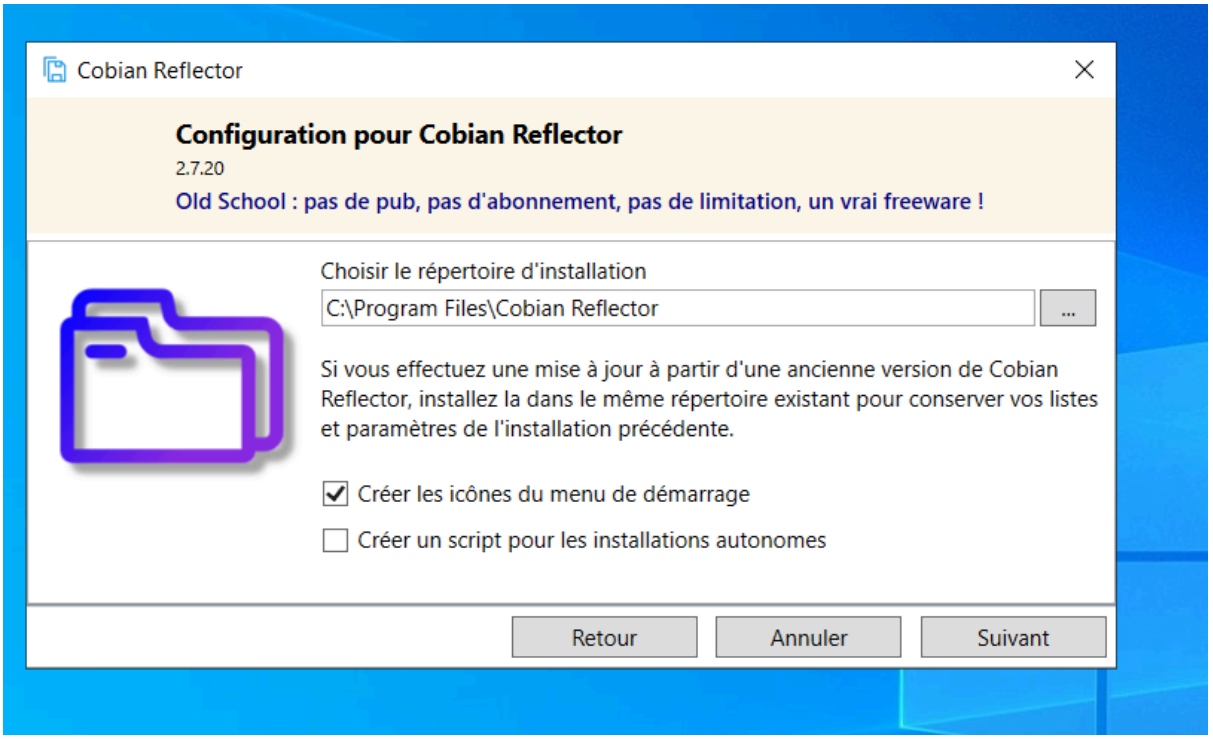
Téléchargez la dernière version (Cobian Reflector de préférence)



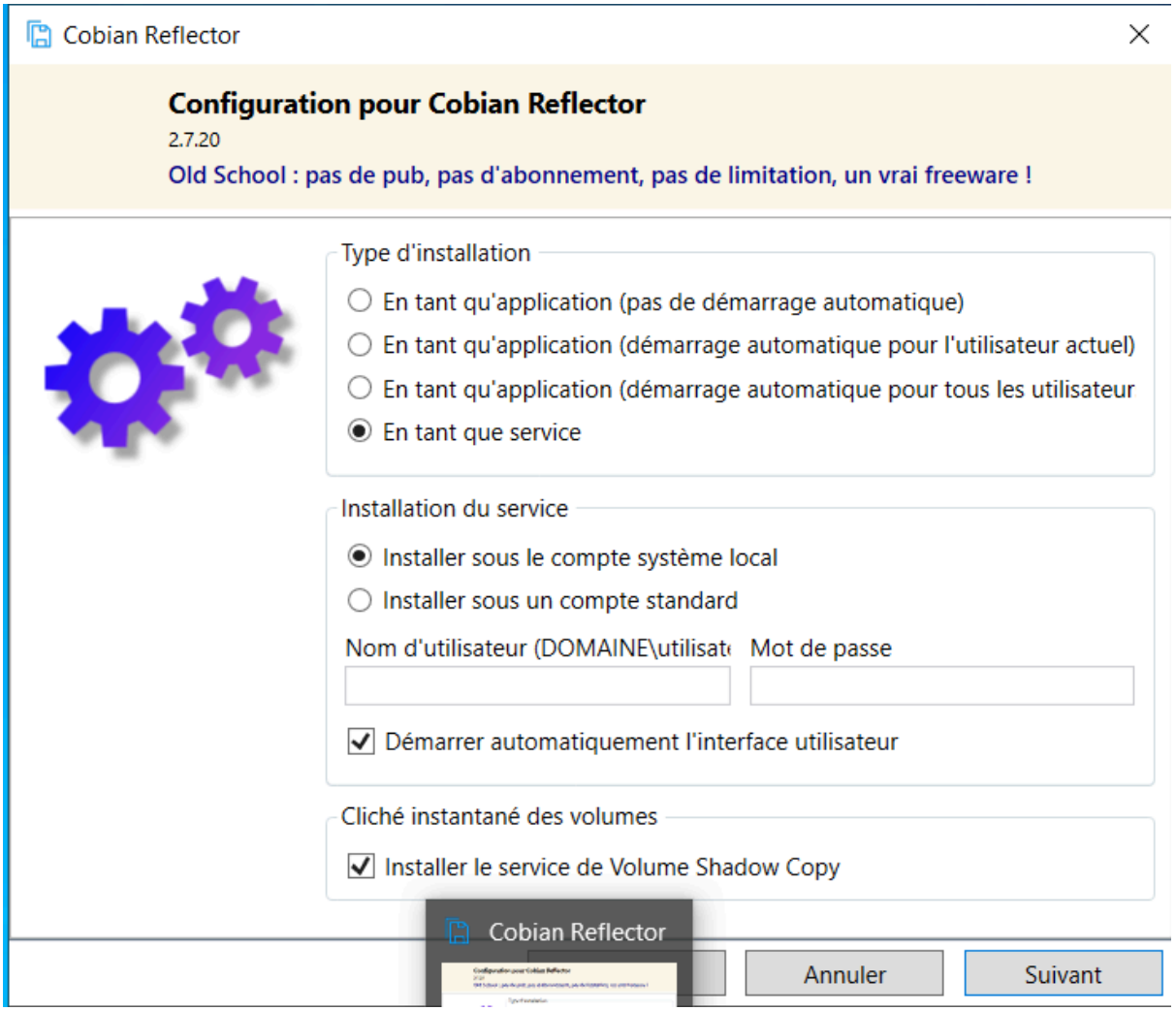
Une fois sur le .exe, sélectionnez votre langue et faites suivant



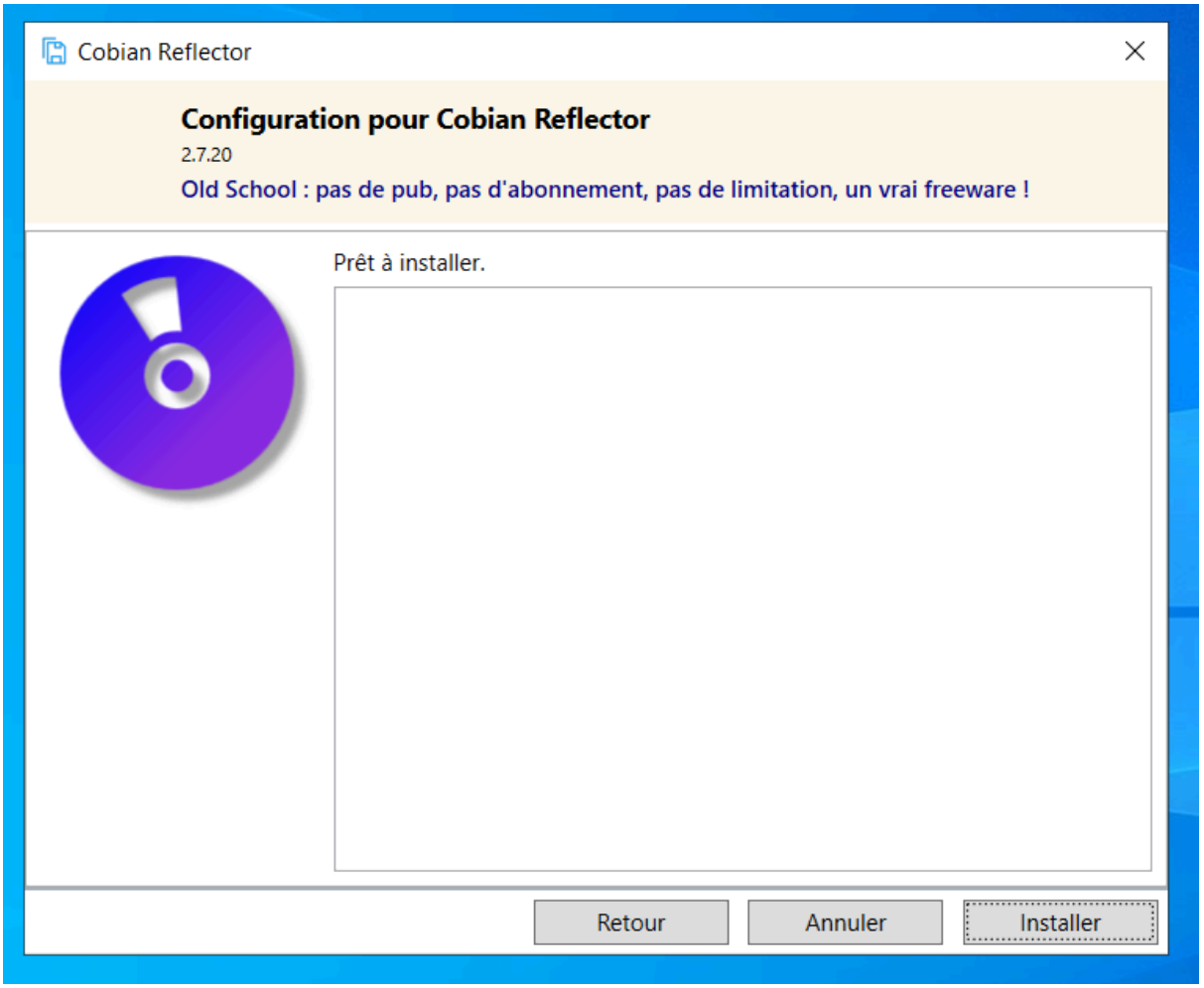
Accepter le contrat de licence et faire suivant



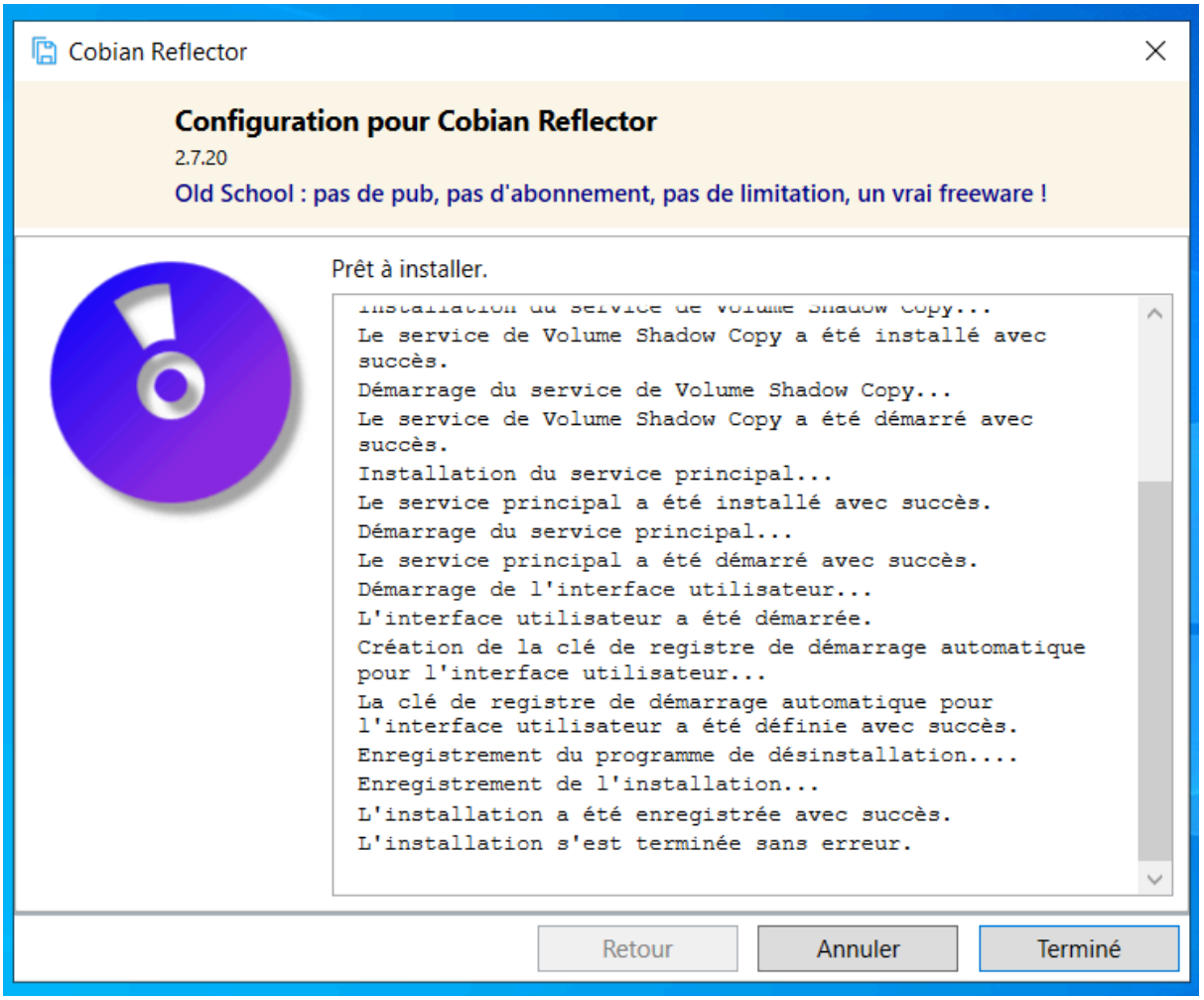
Faire suivant



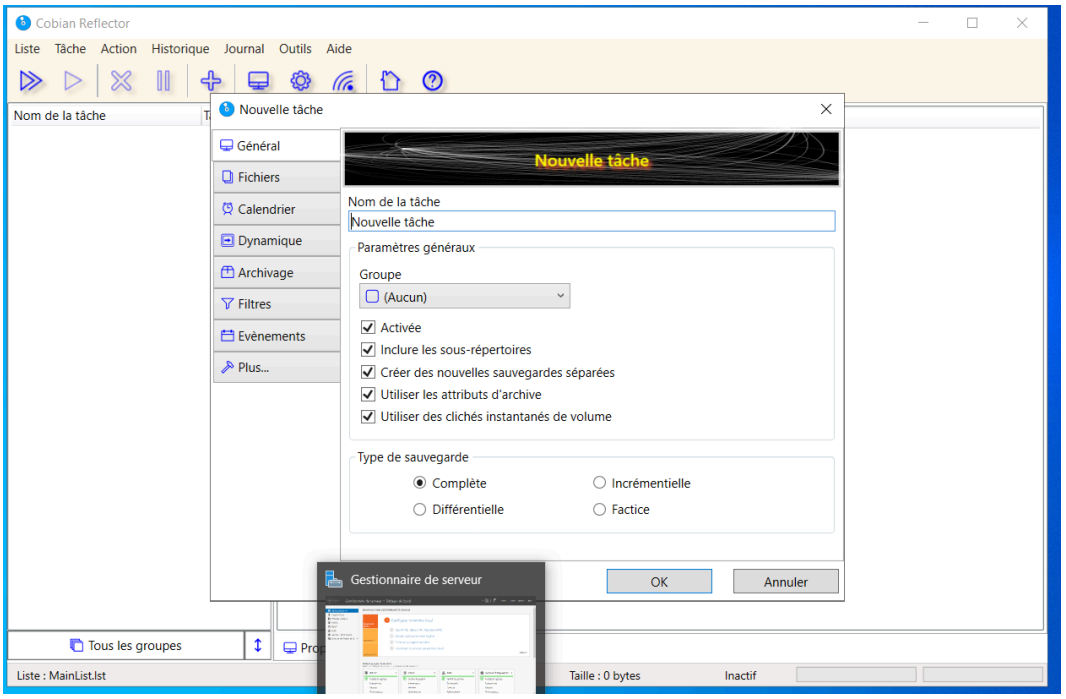
Ici installez bien en tant que service.



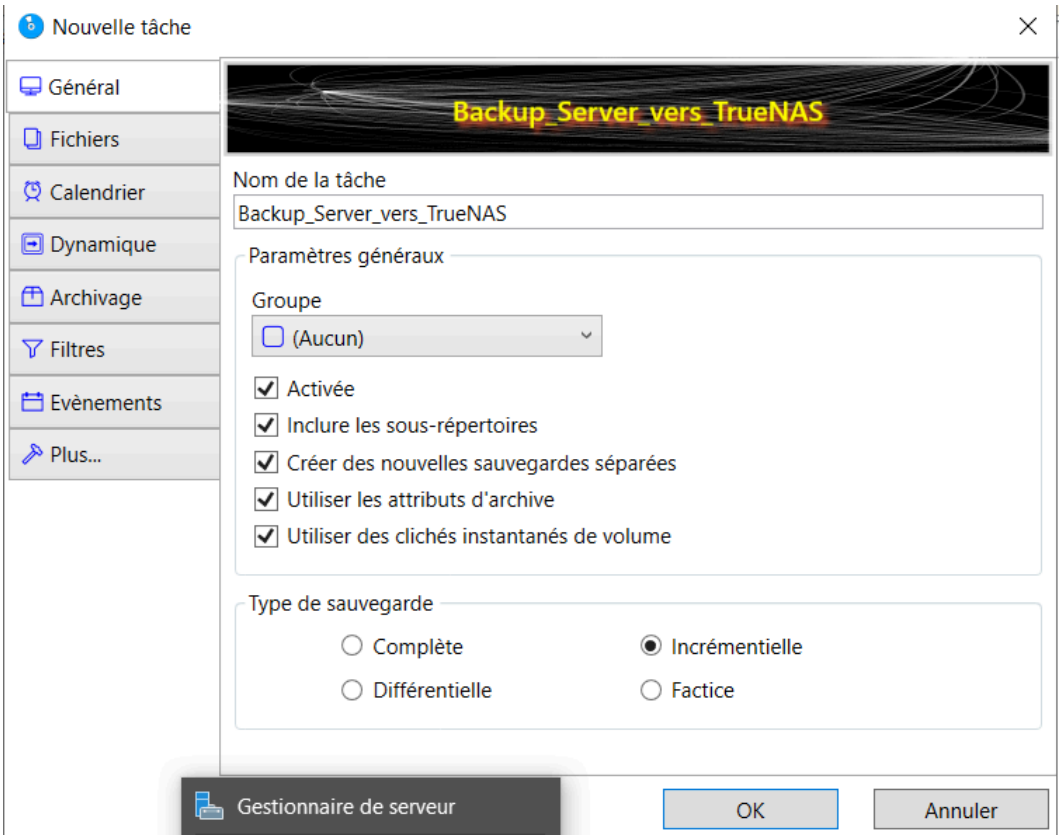
Et faire Installer



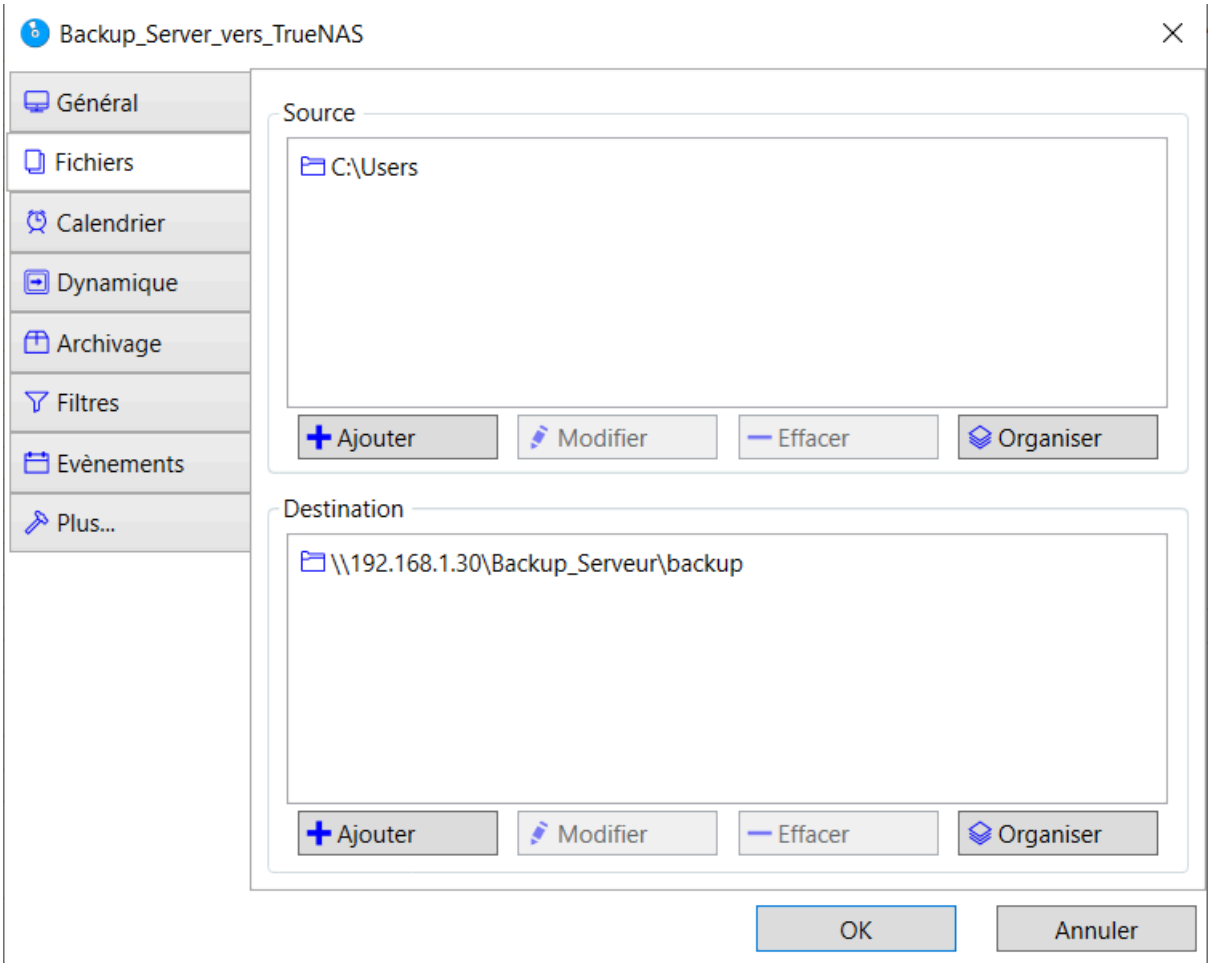
L’installation s’est faite sans erreur. Faire Terminé



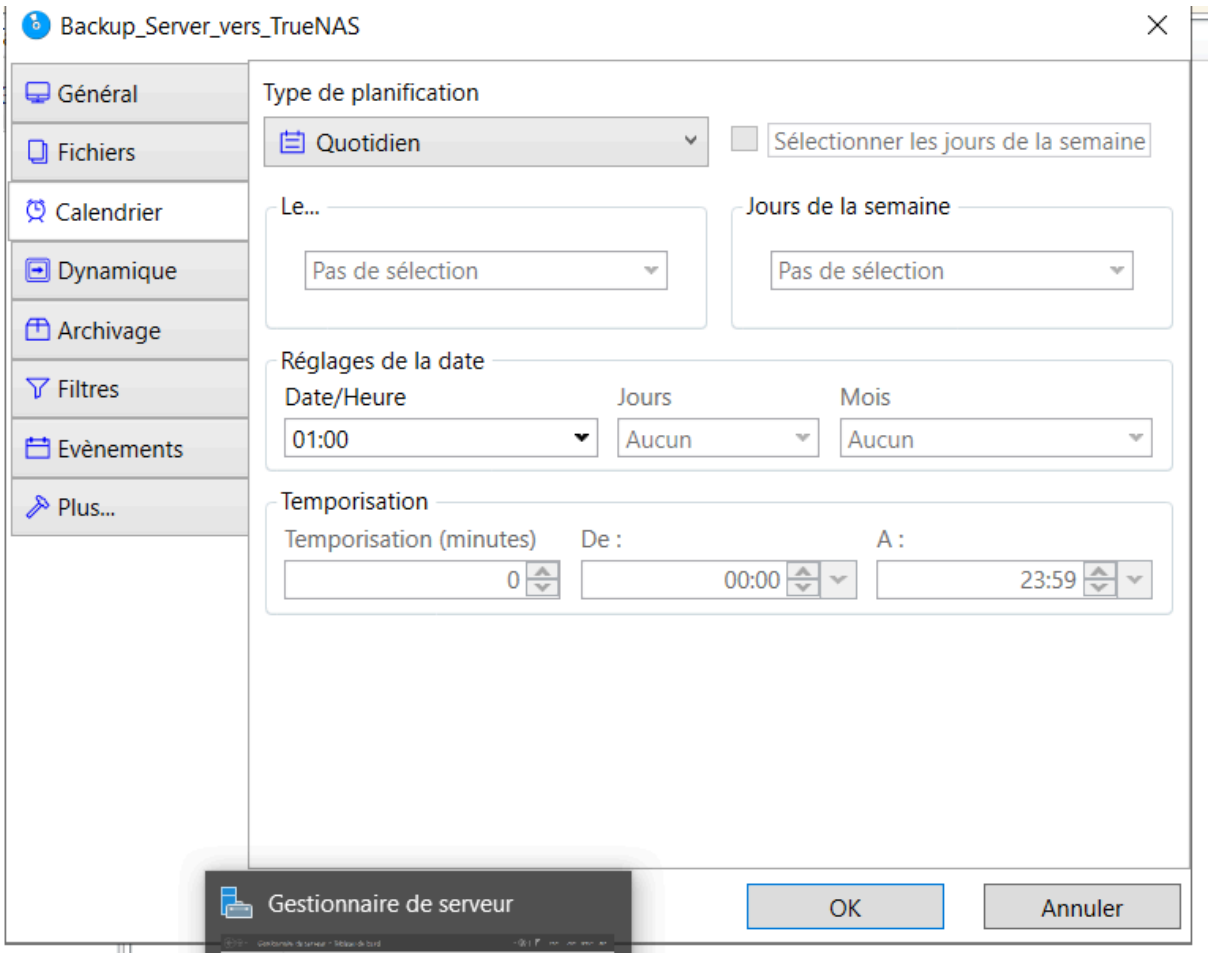
Ouvrez l’application Cobian Reflector et créez une nouvelle tâche.



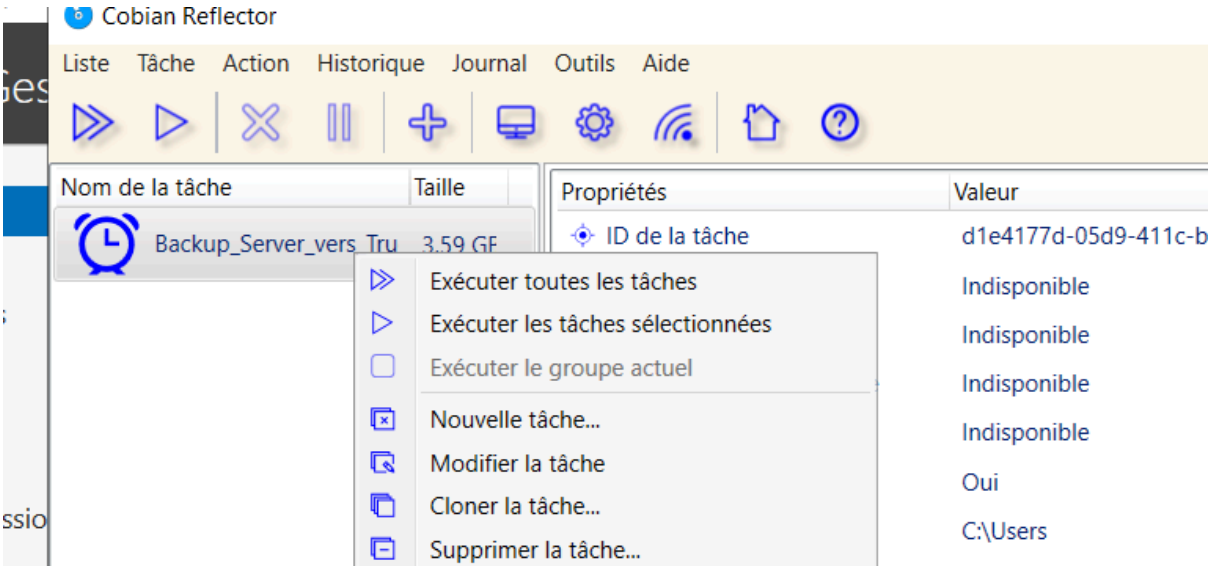
Remplir le nom de votre tâche et choisir le type de sauvegarde Incrémentielle



Entrez vos sources (dossier du windows serveur) et en destination votre TrueNas



Ici j'ai géré la planification de la sauvegarde pour tous les jours à 01h du matin



Maintenant il faut exécuter la tâche

la tâche à était exécuté sans erreur, la sauvegarde est donc en place sur le dossier de backup

Enzo
ALCARAZ
SIO 2