

Présentation de Mon Projet 2

Sommaire :

Partie I : Mise en place de la Solution de Supervision Centreon

- 1.1. Prérequis et Mise à jour du système
- 1.2. Installation des dépôts et dépendances
- 1.3. Initialisation du serveur central
- 1.4. Sécurisation de la base de données (MariaDB)
- 1.5. Finalisation via l'interface Web
- 1.6. Initialisation des processus de collecte

Partie II : Supervision d'un Serveur Windows (SNMP)

- 2.1. Activation du service SNMP sur Windows Server
- 2.2. Configuration de la sécurité et des communautés
- 2.3. Ajout de l'hôte sur l'interface Centreon
- 2.4. Exportation de la configuration et vérification du statut

Partie III : Déploiement de l'Active Directory en Redondance

- 3.1. Concept de haute disponibilité (Haute Dispo)
- 3.2. Configuration du second contrôleur de domaine (DC2)
- 3.3. Réplication des Unités d'Organisation (UO) et Utilisateurs

Partie IV : Gestion de Parc et Ticketing avec GLPI

- 4.1. Préparation de l'environnement LAMP (Linux, Apache, MySQL, PHP)
- 4.2. Installation et configuration de la base de données
- 4.3. Déploiement des sources GLPI et gestion des droits
- 4.4. Configuration du serveur Web (VirtualHost)
- 4.5. Premier accès et interface de Ticketing

Partie V : Mise du DHCP sur le routeur

Partie VI : Mise en place du VPN sur Pfsense

Partie VII : Installation de cobian Backup sur DC1

Installation Centreon

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

Avec la commande « apt update && apt upgrade »

Commençons maintenant :

```
Paramétrage de curl (7.88.1-10+deb12u14) ...
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 -Ls 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
démarré automatiquement

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

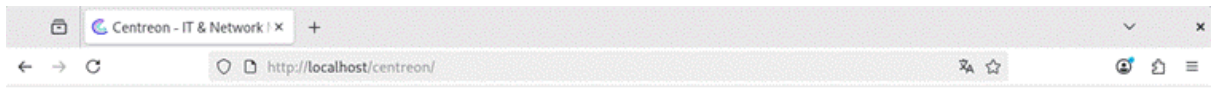
Etape 8 : Sécurisez l'accès root de la base de données avant
d'installer Centreon

Répondez OUI à toutes les questions sauf a « Disallow root
login remotely ? »

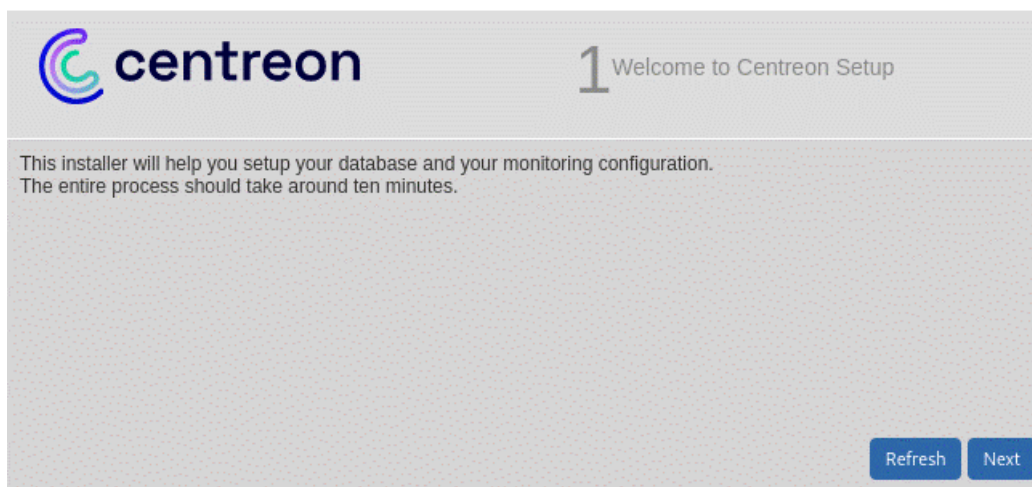
Il est aussi obligatoire de définir un nouveau mot de passe
root, ce mot de passe vous sera demandé pendant l'installation
Web.

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

Etape 9 : Démarrez le serveur Apache avec cette commande



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



Etape 11 : faites Next

centreon 2 Dependency check up

Module name	File	Status
MySQL	pdo_mysql.so	Loaded
GD	gd.so	Loaded
LDAP	ldap.so	Loaded
XML Writer	xmlwriter.so	Loaded
MB String	mbstring.so	Loaded
SQLite	pdo_sqlite.so	Loaded
INTL	intl.so	Loaded

Back Refresh Next

Etape 12 : faites Next

centreon 3 Monitoring engine information

Monitoring engine information

Centreon Engine Stats binary *

Centreon Engine var lib directory *

Centreon Engine Connector path

Centreon Engine Library (*.so) directory *

Centreon Plugins Path *

Back Refresh Next

Etape 13 : laissez les chemins par défaut et faites Next

centreon 4 Broker module information

Monitoring engine information

Centreon Broker etc directory *

Centreon Broker log directory *

Retention file directory *

Centreon Broker lib (*.so) directory *

Back Refresh Next

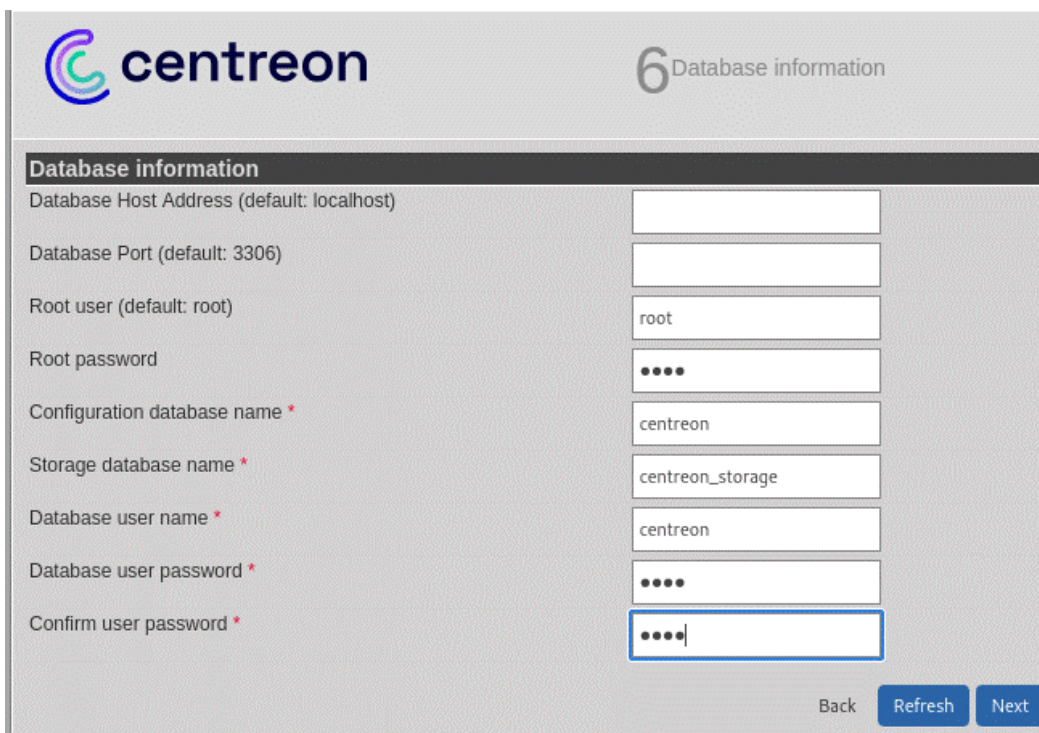
Etape 14 : Faire de nouveau Next



The screenshot shows the 'Admin information' step of the Centreon installation. The form includes fields for Login (admin), Password, Confirm password, First name (enzo), Last name (enzo), and Email (zoro.dev@gmail.com). The Email field is highlighted with a blue border. Navigation buttons 'Back', 'Refresh', and 'Next' are at the bottom right.

centreon	5 Admin information
Admin information	
Login	admin
Password *
Confirm password *
First name *	enzo
Last name *	enzo
Email *	zoro.dev@gmail.com
Back Refresh Next	

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



The screenshot shows the 'Database information' step of the Centreon installation. The form includes fields for Database Host Address, Database Port, Root user (root), Root password (masked with dots), Configuration database name (centreon), Storage database name (centreon_storage), Database user name (centreon), Database user password (masked with dots), and Confirm user password (masked with dots). The Confirm user password field is highlighted with a blue border. Navigation buttons 'Back', 'Refresh', and 'Next' are at the bottom right.

centreon	6 Database information
Database information	
Database Host Address (default: localhost)	
Database Port (default: 3306)	
Root user (default: root)	root
Root password
Configuration database name *	centreon
Storage database name *	centreon_storage
Database user name *	centreon
Database user password *
Confirm user password *
Back Refresh Next	

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



7 Installation

Currently installing database and generating cache... please do not interrupt this process.

Step	Status
Setting up configuration file	OK
Configuration database	OK
Storage database	OK
Creating database user	OK
Setting up basic configuration	OK
Partitioning database tables	OK
Generating application cache	OK

[Next](#)

Etape 17 : Faites Next


8 Modules installation

Module	Author	Version	
Centreon IT Edition Extensions	Centreon	25.10.2	<input checked="" type="checkbox"/>
Centreon License Manager	Centreon	25.10.2	<input checked="" type="checkbox"/>
Centreon Monitoring Connector Manager	Centreon	25.10.2	<input checked="" type="checkbox"/>
Centreon Auto Discovery	Centreon	25.10.2	<input checked="" type="checkbox"/>

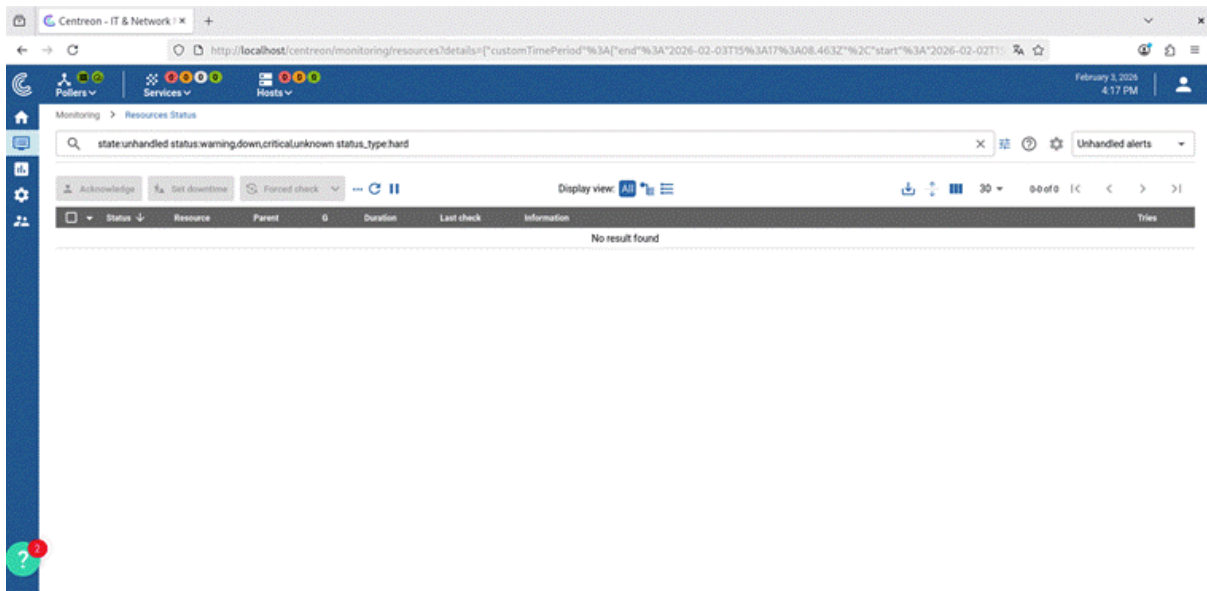
Widget	Author	Version	
Hostgroup Monitoring	Centreon		<input checked="" type="checkbox"/>
Global Health	Centreon		<input checked="" type="checkbox"/>
NtopNG	Centreon		<input checked="" type="checkbox"/>
HTTP Loader	Centreon		<input checked="" type="checkbox"/>
Grid-map	Centreon		<input checked="" type="checkbox"/>
Engine-status	Centreon		<input checked="" type="checkbox"/>
Live Top 10 Memory Usage	Centreon		<input checked="" type="checkbox"/>
Graph Monitoring	Centreon		<input checked="" type="checkbox"/>
Tactical Overview	Centreon		<input checked="" type="checkbox"/>
Live Top 10 CPU Usage	Centreon		<input checked="" type="checkbox"/>
Single Metric	Centreon		<input checked="" type="checkbox"/>
Service Monitoring	Centreon		<input checked="" type="checkbox"/>
Servicegroup Monitoring	Centreon		<input checked="" type="checkbox"/>
Host Monitoring	Centreon		<input checked="" type="checkbox"/>

[Refresh](#) [Install](#)

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

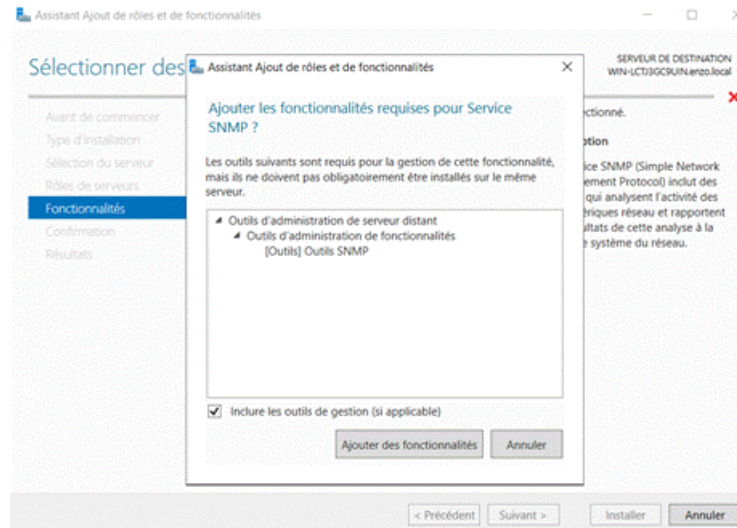
```
root@debian:/home/enzo# systemctl start snmpd
```

Démarrer le démon SNMP

Superviser votre premier serveur Windows

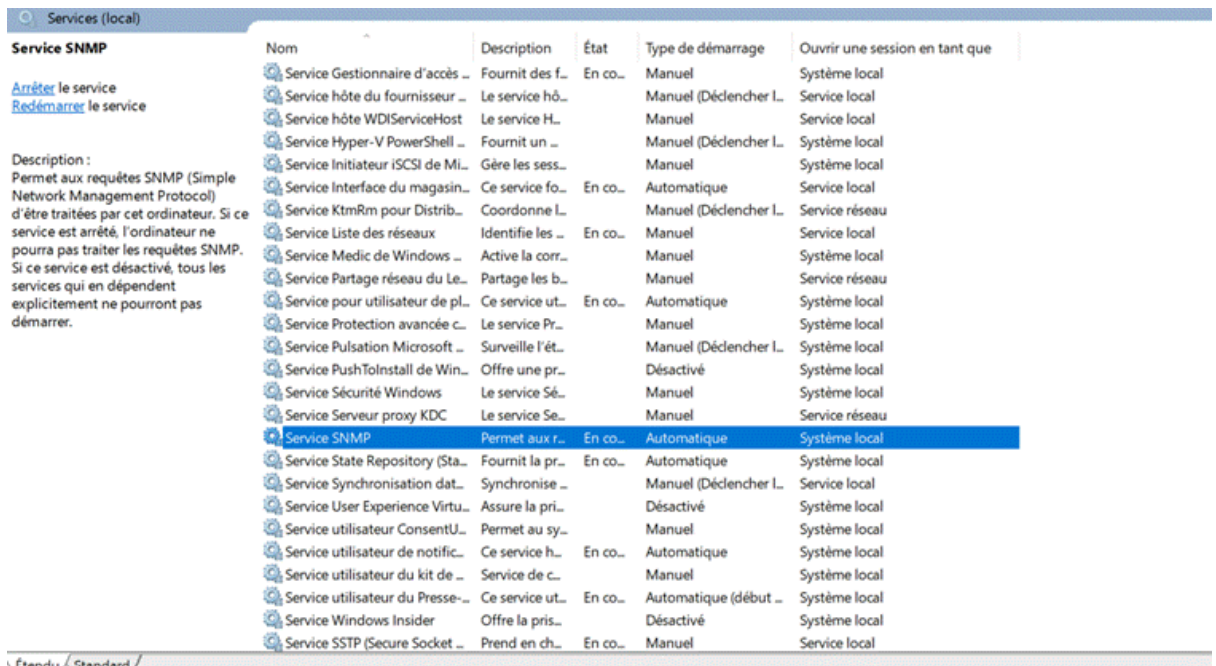
Pour commencer, il faut que vous installiez le service SNMP sur votre Windows.

Pour ce faire il suffit d'aller dans ajoutez une fonctionnalité sur le gestionnaire de serveur, puis d'installer le service SNMP.



Etape 1 : Ajouter des fonctionnalités.

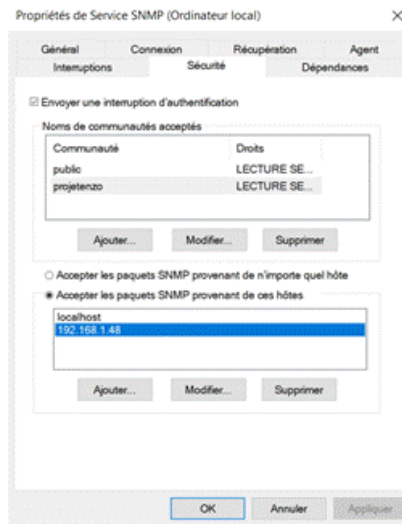
Etape 2 :Après l'installation de SNMP, vous devez procéder à sa configuration. Dans la barre de recherche, tapez services.msc et appuyez sur Entrée pour lancer le panneau Services. Recherchez le service SNMP dans la liste.



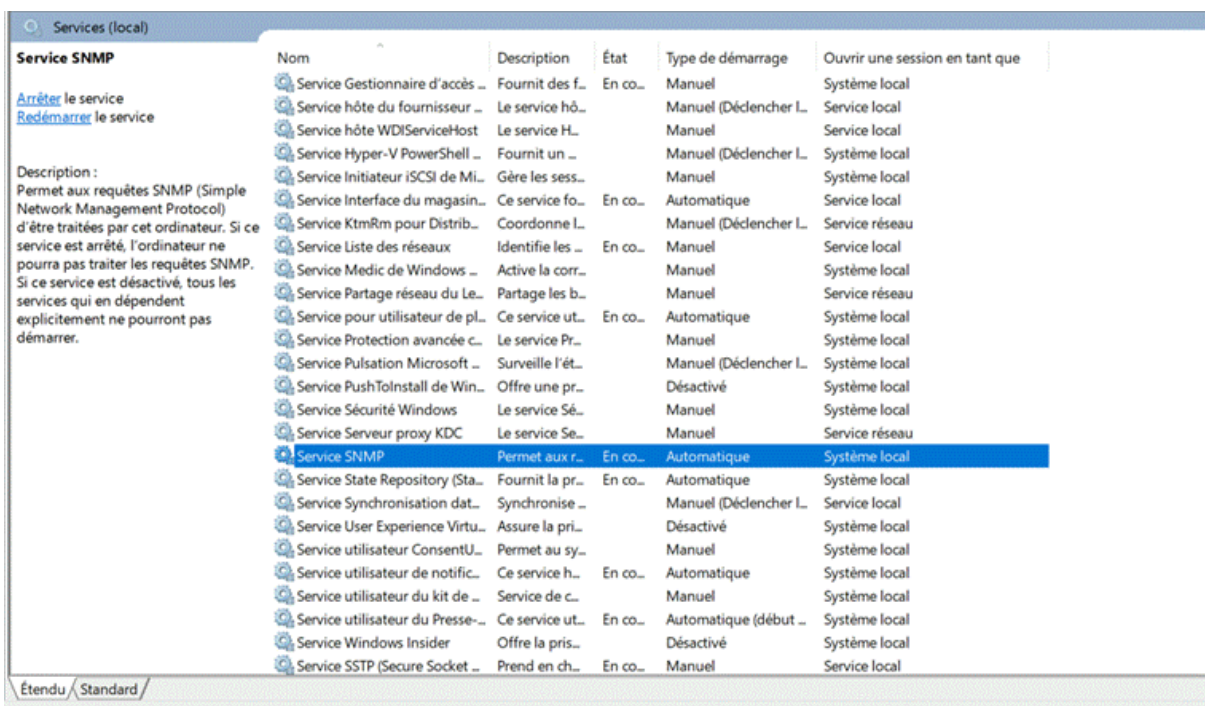
Etape 3 : Faire clic droit > propriété >Agent



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

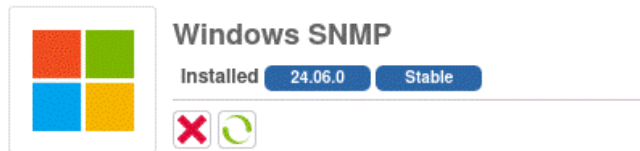


Etape 5 : Dans l'onglet Sécurité, renseignez la communauté SNMP dans la section Noms de communauté acceptés et choisissez l'option LECTURE SEULE. Sélectionnez ensuite Accepter les paquets SNMP de ces hôtes et ajoutez l'adresse IP du serveur Centreon.



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 :



Description

Monitoring Connector for Windows SNMP

Tags: #Microsoft, #Operating System, #OS, #Server, #SNMP, #System, #Windows, #ServiceDisco

Host template and related services

OS-Windows-SNMP-custom

Cpu

Memory

Swap

Services that are not linked to the host template

Other services

Disk-Generic-Id

Disk-Generic-Name

Disk-Global

NIn

Étape 7 : Installez SNMP

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

ADD a Host

Host basic information

Name * WIN-SERV-DC2

Alias WIN-SERV-DC2

Address * 192.168.1.20 [Resolve](#)

SNMP Community & Version public 2c

Monitoring server Central

Timezone Timezone

Templates

A host or host template can have several templates. See help for more details.

+ Add a new entry

OS-Windows-SNMP-custom

Create Services linked to the Template too Yes No

Host check options

Check Command Check Command

Args

Custom macros

+ Add a new entry

Nothing here, use the "Add" button

Scheduling options

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 :

Configuration > Services > Services by host

Hosts Services Templates Status Disabled hosts [SEARCH](#) Filter

More actions... [Add](#)

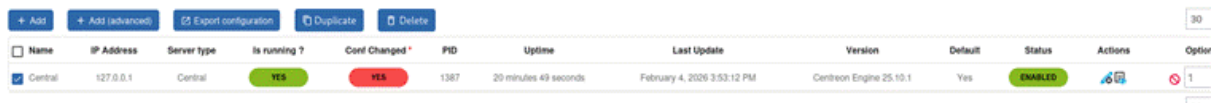
Host	Service	Scheduling	Template	Status	Options
WIN-SERV-DC1	Cpu	5 min / 1 min	-> OS-Windows-Cpu-SNMP-custom -> OS-Windows-Cpu-SNMP -> generic-active-service-custom -> generic-active-service	ENABLED	1
	Memory	15 min / 1 min	-> OS-Windows-Memory-SNMP-custom -> OS-Windows-Memory-SNMP -> generic-active-service-custom -> generic-active-service	ENABLED	1
	Ping	5 min / 1 min	-> Base-Ping-LAN-custom -> Base-Ping-LAN -> generic-active-service-custom -> generic-active-service	ENABLED	1
WIN-SERV-DC2	Swap	15 min / 1 min	-> OS-Windows-Swap-SNMP-custom -> OS-Windows-Swap-SNMP -> generic-active-service-custom -> generic-active-service	ENABLED	1
	Cpu	5 min / 1 min	-> OS-Windows-Cpu-SNMP-custom -> OS-Windows-Cpu-SNMP -> generic-active-service-custom -> generic-active-service	ENABLED	1
	Memory	15 min / 1 min	-> OS-Windows-Memory-SNMP-custom -> OS-Windows-Memory-SNMP -> generic-active-service-custom -> generic-active-service	ENABLED	1
	Ping	5 min / 1 min	-> Base-Ping-LAN-custom -> Base-Ping-LAN -> generic-active-service-custom -> generic-active-service	ENABLED	1
	Swap	15 min / 1 min	-> OS-Windows-Swap-SNMP-custom -> OS-Windows-Swap-SNMP -> generic-active-service-custom -> generic-active-service	ENABLED	1

More actions... [Add](#)

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.

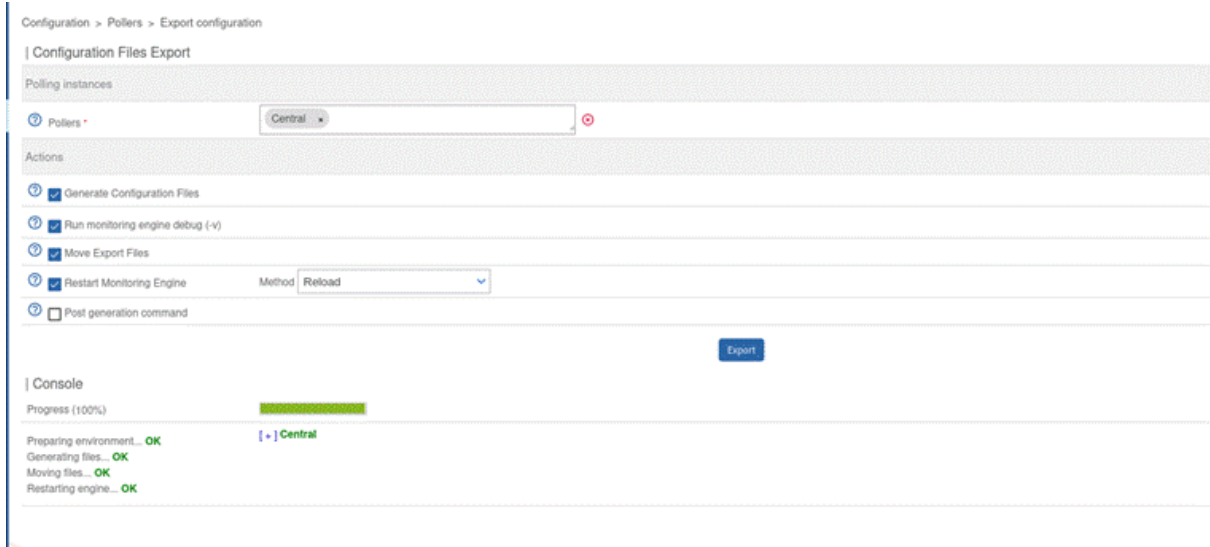
Sélectionnez le collecteur dont la configuration a changé.

Cliquez sur Exporter la configuration.



<input type="checkbox"/>	Name	IP Address	Server type	Is running ?	Conf Changed *	PID	Uptime	Last Update	Version	Default	Status	Actions	Optio
<input checked="" type="checkbox"/>	Central	127.0.0.1	Central	YES	YES	1387	20 minutes 49 seconds	February 4, 2026 3:53:12 PM	Centreon Engine 25.10.1	Yes	ENABLED		1

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.

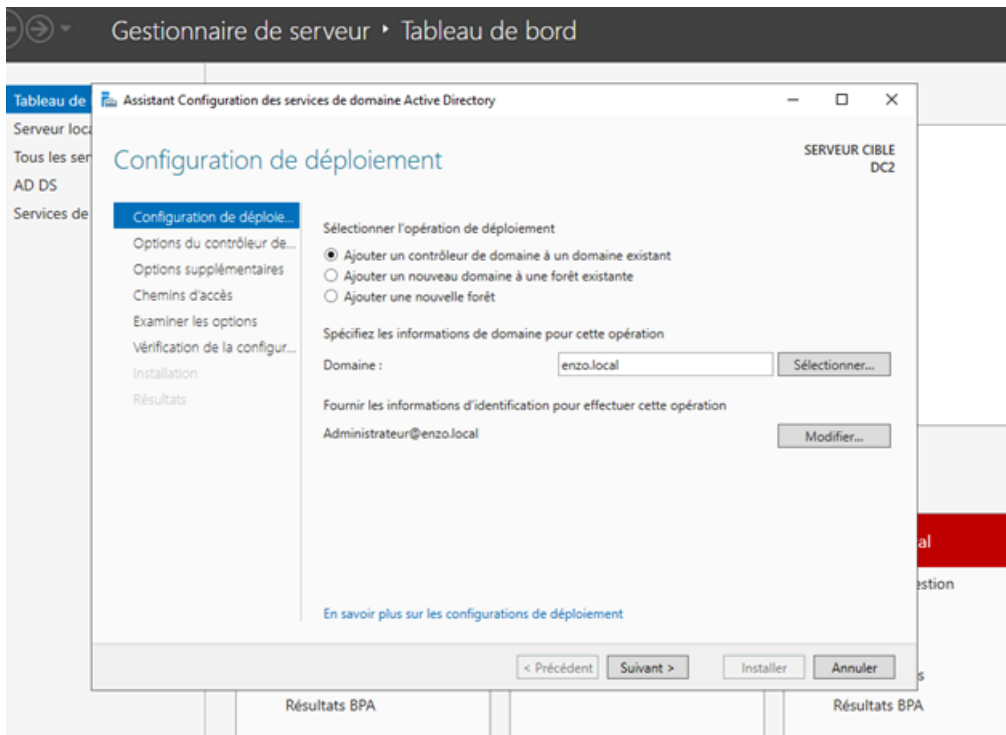


Rendez-vous dans le menu Monitoring > Status des Resources et positionnez le filtre sur Tous pour récupérer tous les indicateurs quel que soit leur état :

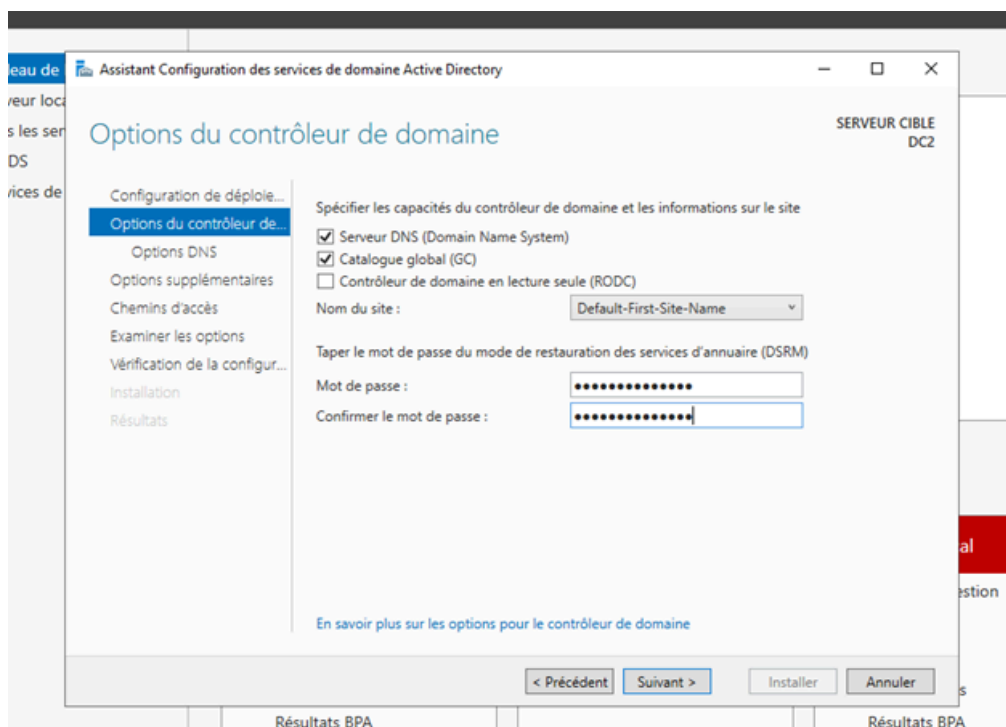
Status	Resource	Parent	Q	Duration	Last check	Information	Traces
Critical	Ping	WIN-SERV-DC1		15m 15s	6m 15s	CRITICAL - 192.168.1.30: rta nan, lost 100%	1/3 (0%)
Down	WIN-SERV-DC1			25m 10s	4m 15s	CRITICAL - 192.168.1.30: Host unreachable @ 192.168.1.57: rta nan, lost 100%	1/3 (0%)
Unknown	Cpu	WIN-SERV-DC1		1w 4h	3m 45s	UNKNOWN: SNMP Table Request: Timeout	3/3 (0%)
Unknown	Memory	WIN-SERV-DC1		1w 4h	6m 15s	UNKNOWN: SNMP Table Request: Timeout	3/3 (0%)
Unknown	Swap	WIN-SERV-DC1		1w 4h	8m 45s	UNKNOWN: SNMP Table Request: Timeout	3/3 (0%)
Pending	Swap	WIN-SERV-DC2					1/3 (0%)
Pending	Memory	WIN-SERV-DC2					1/3 (0%)
Pending	Cpu	WIN-SERV-DC2					1/3 (0%)
Pending	Ping	WIN-SERV-DC2					1/3 (0%)
Up	WIN-SERV-DC2				2m 11s	OK - 192.168.1.20: rta 5.932ms, lost 0%	1/3 (0%)

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

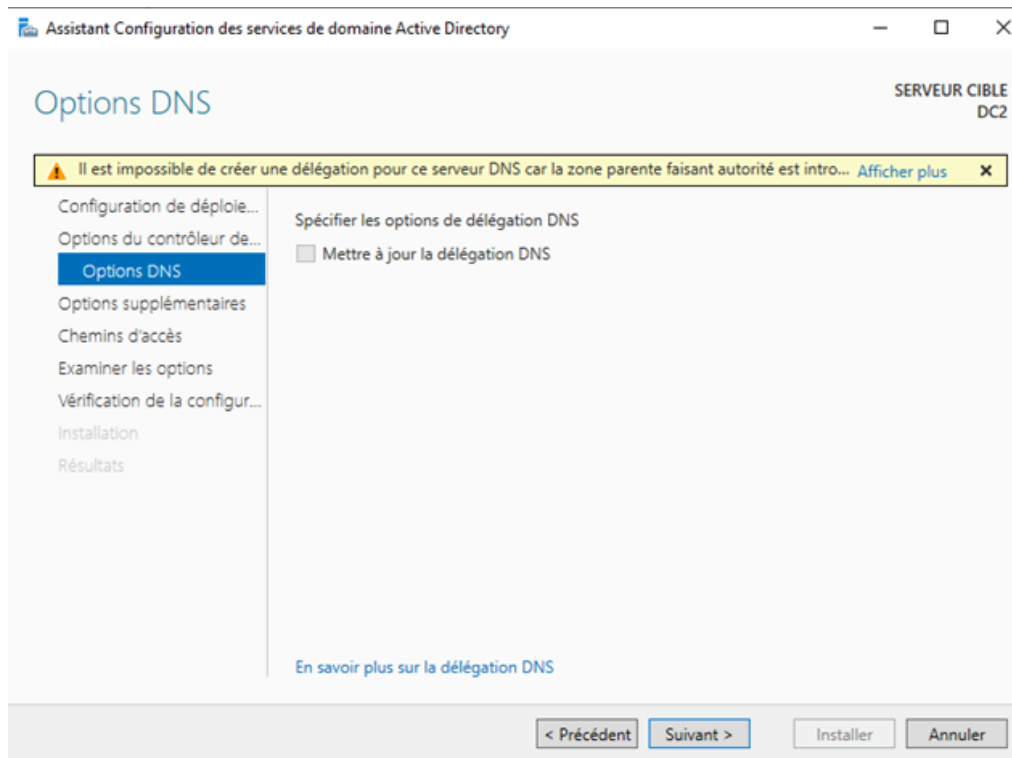
Déploiement d'un AD en redondance



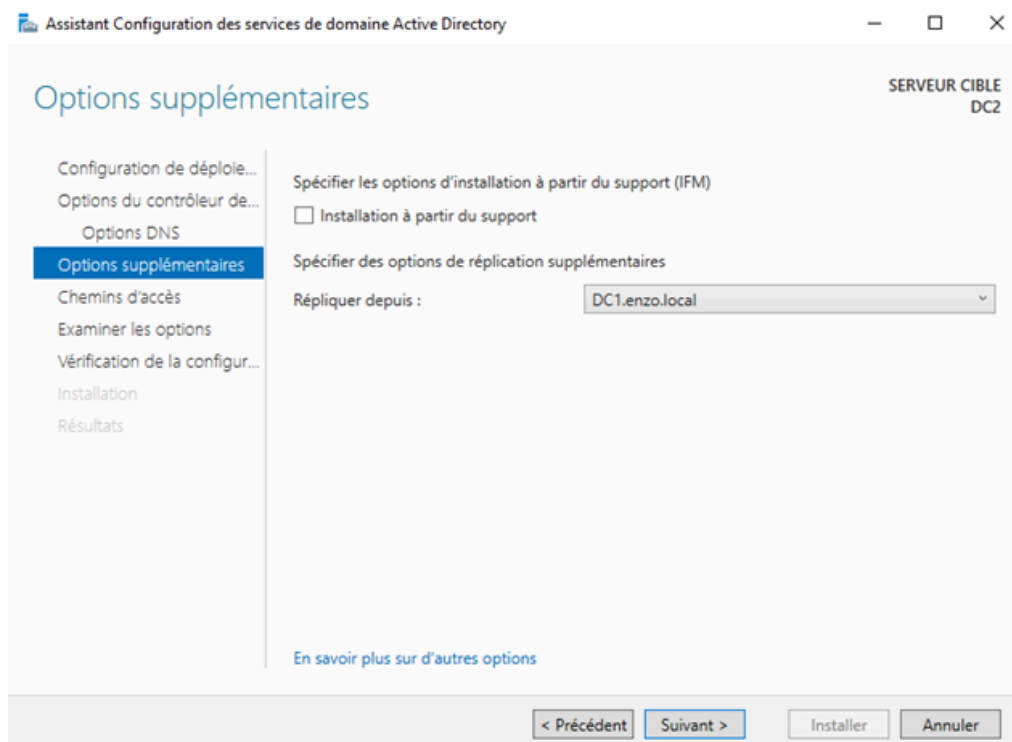
Etape 1 : Lors de l'installation de l'AD DS sélectionner « Ajouter un contrôleur de domaine à un domaine existant », puis entrer le nom de domaine enfin faites Suivant.



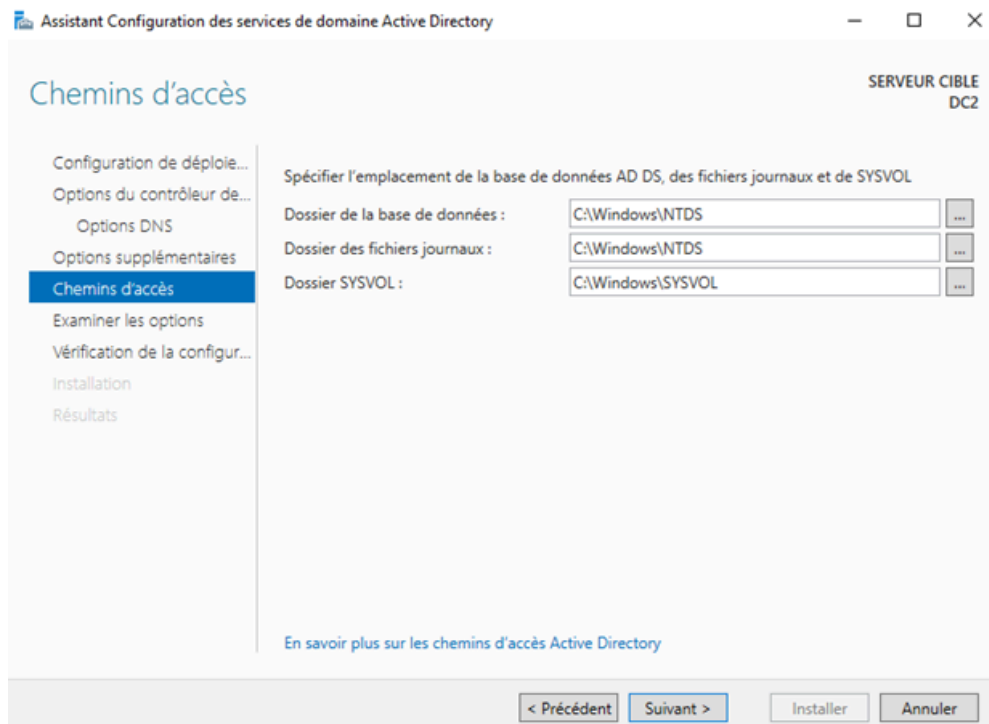
Etape 2 : Entrer un mot de passe robuste et faites Suivant.



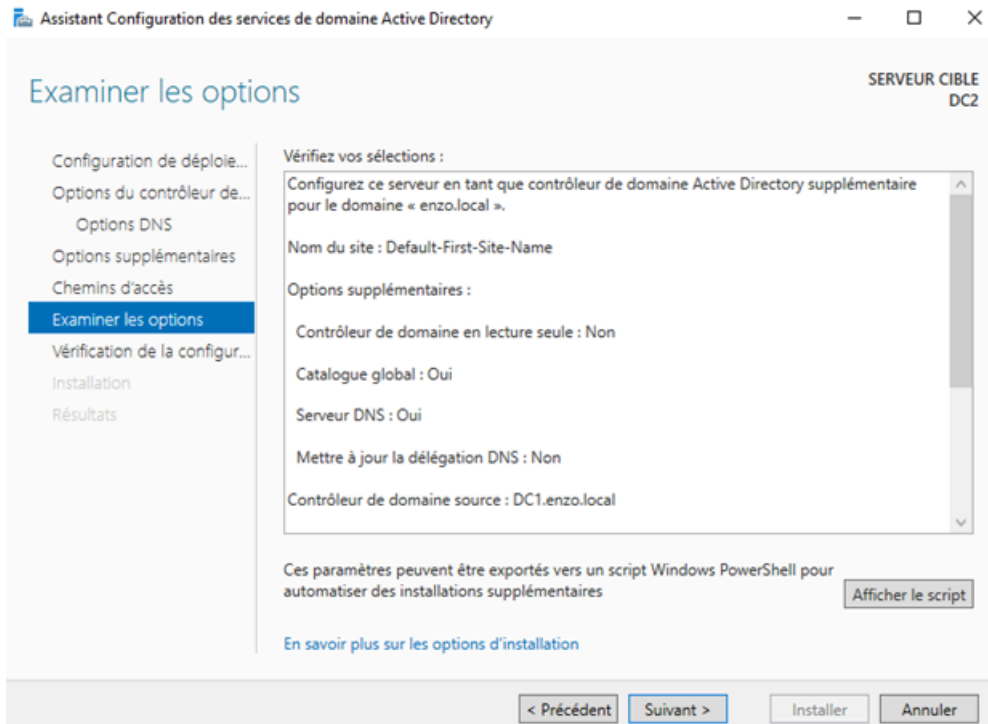
Etape 3 : sur cette page faites Suivant



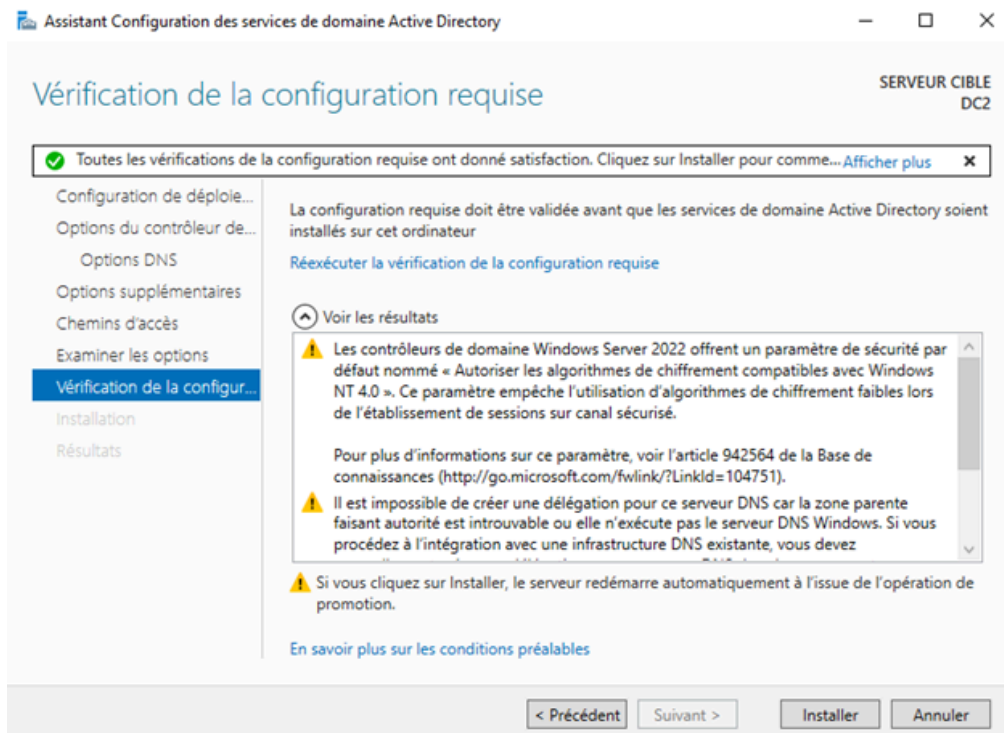
Etape 4 : Ici il faut sélectionner le FQDN de votre premier AD et faire Suivant



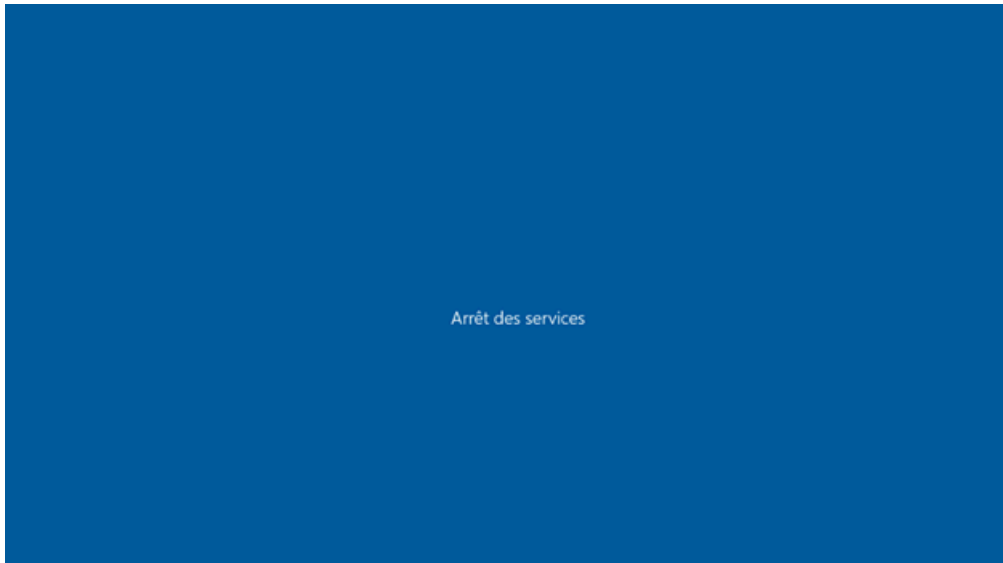
Etape 5 : Sur cette page faites Suivant



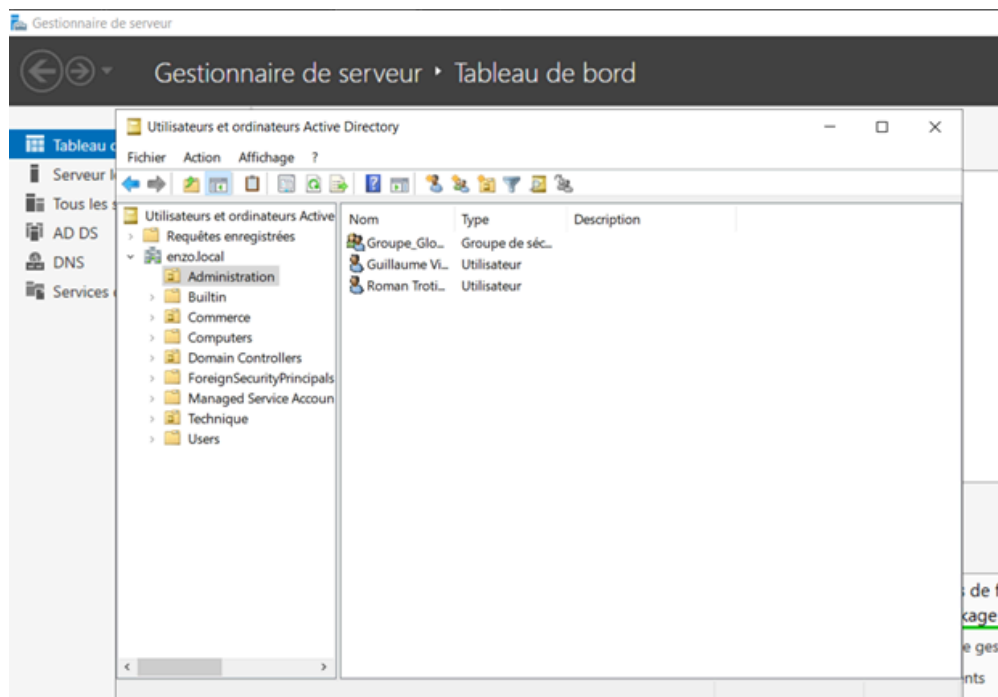
Etape 6 : Faire de nouveaux Suivant



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 signifie : 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.

```
enzo@enzo-VMware-Virtual-Platform:~$ sudo apt install apache2
```

Installation de apache2

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

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 php-zip 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/glpi
<VirtualHost *:80>
  ServerName GLPI
  DocumentRoot /var/www/glpi/public

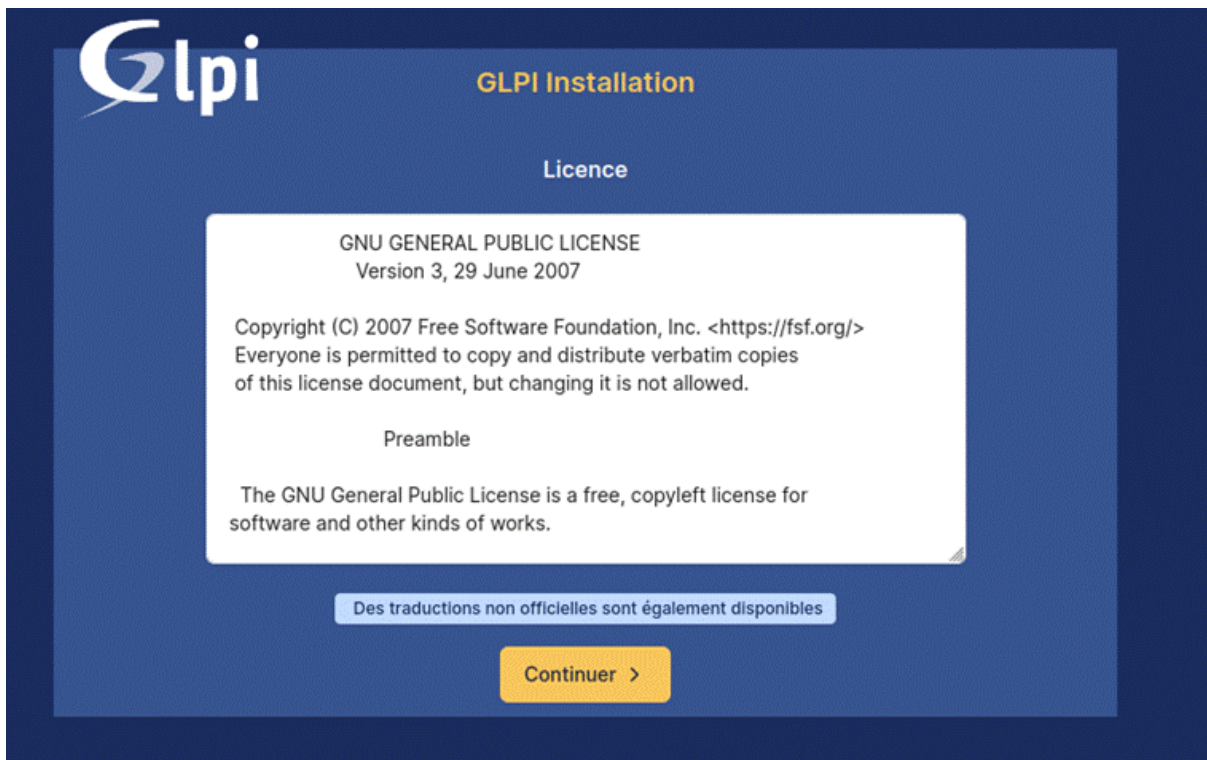
  <Directory /var/www/glpi/public>
    Require all granted
    RewriteEngine On

    # 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



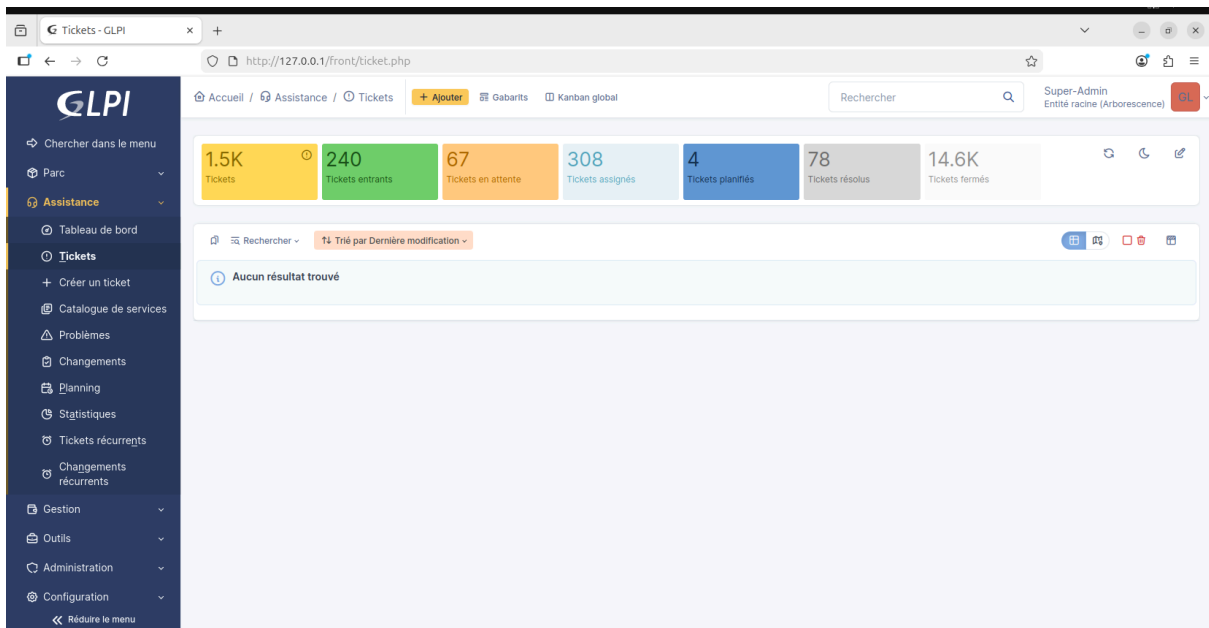
Cliquer sur continuer



Puis Utiliser GLPI



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



Voici l'interface de ticketing.

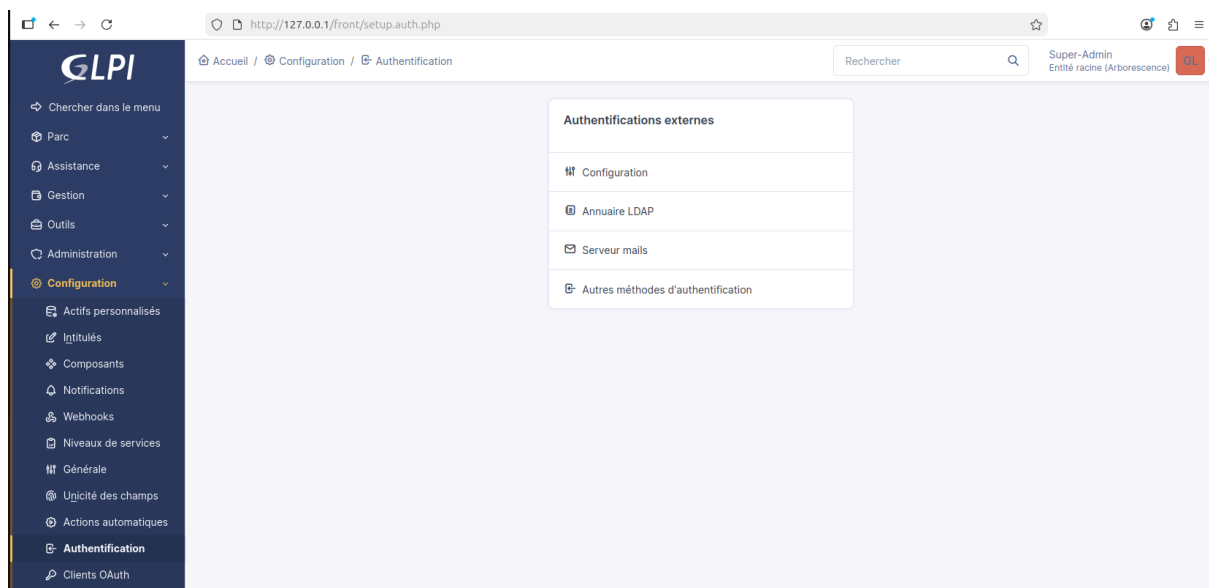
Configuration de l'authentification LDAP via l'Active Directory

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.

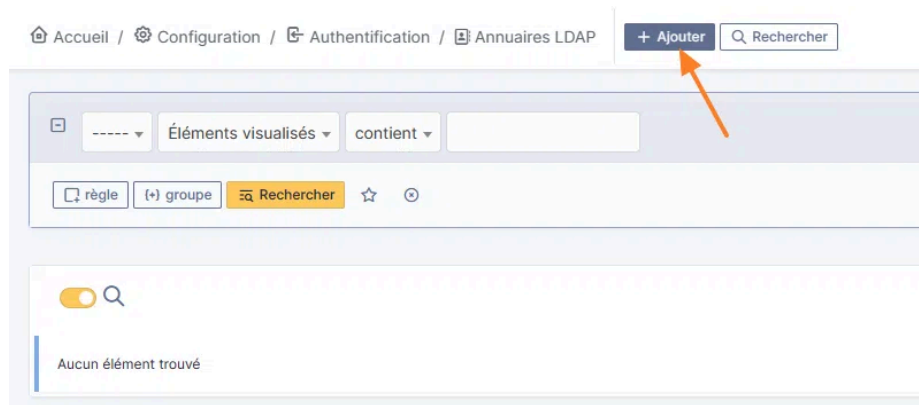
```
sudo apt-get update  
sudo apt-get install php-ldap
```

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".

GLPI

Accueil / Configuration / Authentification / Annuaire LDAP + Ajuster

Rechercher Super-Admin Entrée racine (Arborescence)

Annuaire LDAP - ActiveDirectory - ID 1

Annuaire LDAP

- Tester
- Utilisateurs
- Groupes
- Informations avancées
- Réplicats
- Historique 8
- Tous

Nom: ActiveDirectory

Serveur par défaut: Oui

Activé: Oui

Serveur: 192.168.1.20

Port (par défaut 389): 389

Commentaires:

Filtre de connexion:

BaseDN: OU=Technique,DC=enzo,DC=local

Utiliser bind: Oui

DN du compte (pour les connexions non anonymes): ENZO/DC2

Mot de passe du compte (pour les connexions non anonymes): *****

Effacer:

Champ de l'identifiant: userprincipalname

Champ de synchronisation: ?

Supprimer définitivement Sauvegarder

Créé le 2026-03-17 14:48 Dernière mise à jour le 2026-03-17 16:16

Information

Élément modifié: ActiveDirectory

Remplir vos informations comme cela.

Annuaire LDAP - ActiveDirectory - ID 1

Annuaire LDAP

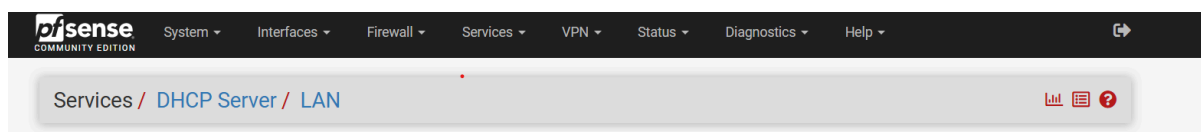
- Tester
- Utilisateurs
- Groupes
- Informations avancées
- Réplicats
- Historique 8
- Tous

Test LDAP Serveur : ActiveDirectory

- Flux TCP**
Connexion à 192.168.1.20 sur le port 389 réussie
- Base DN**
Base DN "OU=Technique,DC=enzo,DC=local" configurée
- LDAP URI**
Vérification de l'URI LDAP réussie
- Connexion Bind**
Authentification réussie
- Chercher (50 premiers résultats)**
Recherche réussie (4 entrées trouvées)

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

LAN

General DHCP Options

DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny Unknown Clients	<input type="text" value="Allow all clients"/> <small>When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.</small>
Ignore Denied Clients	<input type="checkbox"/> Ignore denied clients rather than reject <small>This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.</small>
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request <small>This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting</small>

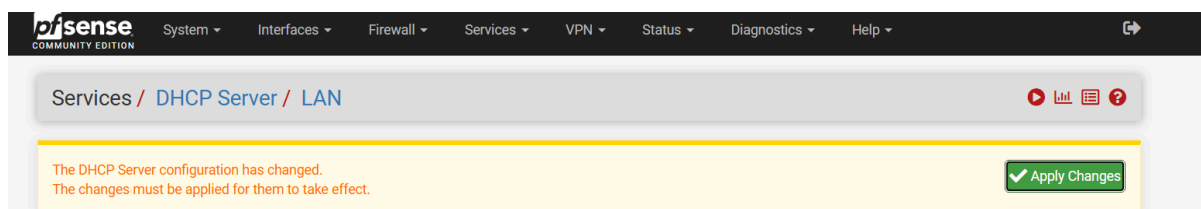
Cliquer sur enable le serveur DHCP sur le Lan

Primary Address Pool

Subnet	192.168.1.0/24
Subnet Range	192.168.1.1 - 192.168.1.254
Address Pool Range	<input type="text" value="192.168.1.100"/> <input type="text" value="192.168.1.245"/> From To <small>The specified range for this pool must not be within the range configured on any other address pool for this interface.</small>

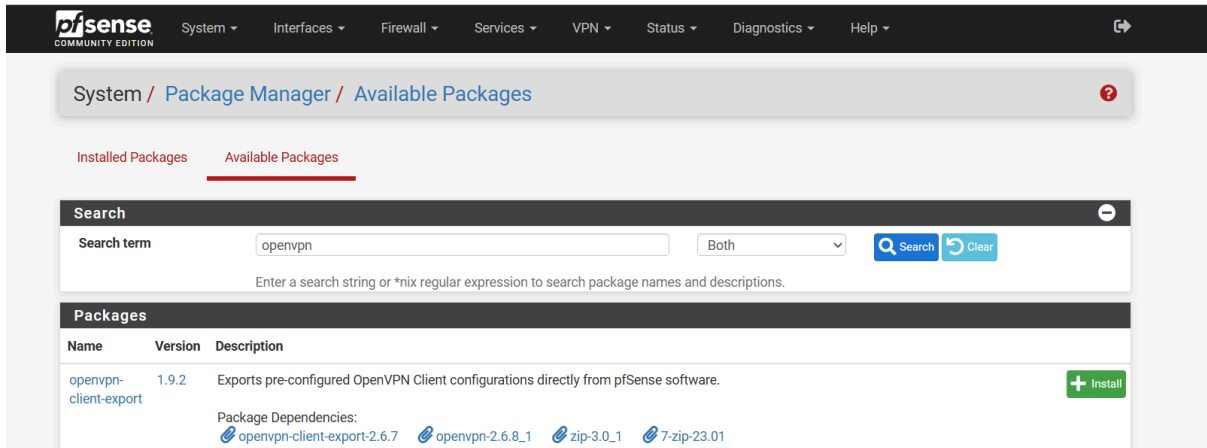
Additional Pools

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

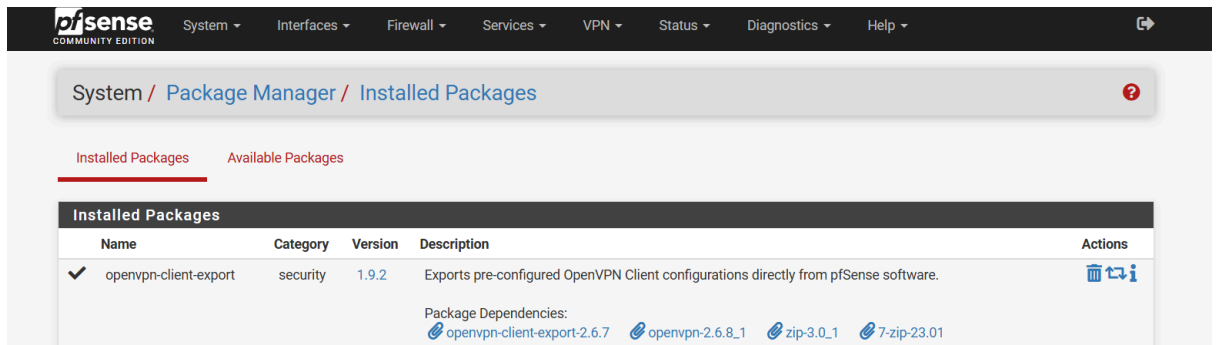


Le serveur DHCP est maintenant créé il suffit d'appliquer les changements.

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

System / Certificate / Authorities / Edit

Authorities Certificates Revocation

Create / Edit CA

Descriptive name
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '.

Method

Trust Store Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

Remplir avec vos informations

Create / Edit CA

Descriptive name
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '.

Method

Trust Store Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

Key type

The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm
The digest method used when the CA is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Lifetime (days)

Common Name
The following certificate authority subject components are optional and may be left blank.

Country Code

State or Province

Une fois créée vous le retrouver ici

Non sécurisé 192.168.1.35/system_canager.php Résumer

System / Certificate / Authorities

Authorities Certificates Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
VPN-CA	<input checked="" type="checkbox"/>	self-signed	0	ST=Gard, O=CyberDoc, L=Nimes, CN=internal-ca, C=FR Valid From: Thu, 26 Mar 2026 15:13:30 +0000 Valid Until: Sun, 23 Mar 2036 15:13:30 +0000	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Refresh"/> <input type="button" value="Delete"/>

Ensuite allez dans VPN / OpenVPN / Servers

VPN / OpenVPN / Servers 🔍 📄 ?

[Servers](#) [Clients](#) [Client Specific Overrides](#) [Wizards](#) [Client Export](#)

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
-----------	-----------------	----------------	---------------	-------------	---------

[+ Add](#)

Faire add et remplir avec vos informations comme si dessous

[Servers](#) [Clients](#) [Client Specific Overrides](#) [Wizards](#) [Client Export](#)

General Information

Description
A description of this VPN for administrative reference.

Disabled Disable this server
Set this option to disable this server without removing it from the list.

Mode Configuration

Server mode

Backend for authentication

Device mode
tun mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
tap mode is capable of carrying 802.3 (OSI Layer 2.)

Endpoint Configuration

Protocol

Interface
The interface or Virtual IP address where OpenVPN will receive client connections.

Local port
The port used by OpenVPN to receive client connections.

Cryptographic Settings [Explorateur de fichiers](#)

Cryptographic Settings

TLS Configuration Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

Automatically generate a TLS Key.

Peer Certificate Authority

Peer Certificate Revocation list No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

OCSP Check Check client certificates with OCSP

Server certificate
Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.

DH Parameter Length
Diffie-Hellman (DH) parameter set used for key exchange. [i](#)

ECDH Curve
The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.

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	<div style="border: 1px solid #ccc; padding: 5px;"><ul style="list-style-type: none">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)<li style="background-color: #f0f0f0;">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)</div> <p>Available Data Encryption Algorithms Click to add or remove an algorithm from the list</p>	<div style="border: 1px solid #ccc; padding: 5px;"><ul style="list-style-type: none">AES-256-CBC</div> <p>Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list</p>
Fallback Data Encryption Algorithm	<div style="border: 1px solid #ccc; padding: 5px;"><p>AES-256-CBC (256 bit key, 128 bit block) ▼</p><p>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.</p></div>	
Auth digest algorithm	<div style="border: 1px solid #ccc; padding: 5px;"><p>SHA256 (256-bit) ▼</p><p>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.</p></div>	
Hardware Crypto	<div style="border: 1px solid #ccc; padding: 5px;"><p>No Hardware Crypto Acceleration ▼</p></div>	
Certificate Depth	<div style="border: 1px solid #ccc; padding: 5px;"><p>One (Client+Server) ▼</p><p>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.</p></div>	

Tunnel Settings	
IPv4 Tunnel Network	<div style="border: 1px solid #ccc; padding: 5px;"><p>10.0.8.0</p><p>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.</p><p>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.</p></div>
IPv6 Tunnel Network	<div style="border: 1px solid #ccc; padding: 5px;"><p></p><p>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.</p></div>
Redirect IPv4 Gateway	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)	<div style="border: 1px solid #ccc; padding: 5px;"><p>192.168.1.0</p><p>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</p></div>

Concurrent connections
Specify the maximum number of clients allowed to concurrently connect to this server.

Allow Compression
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
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

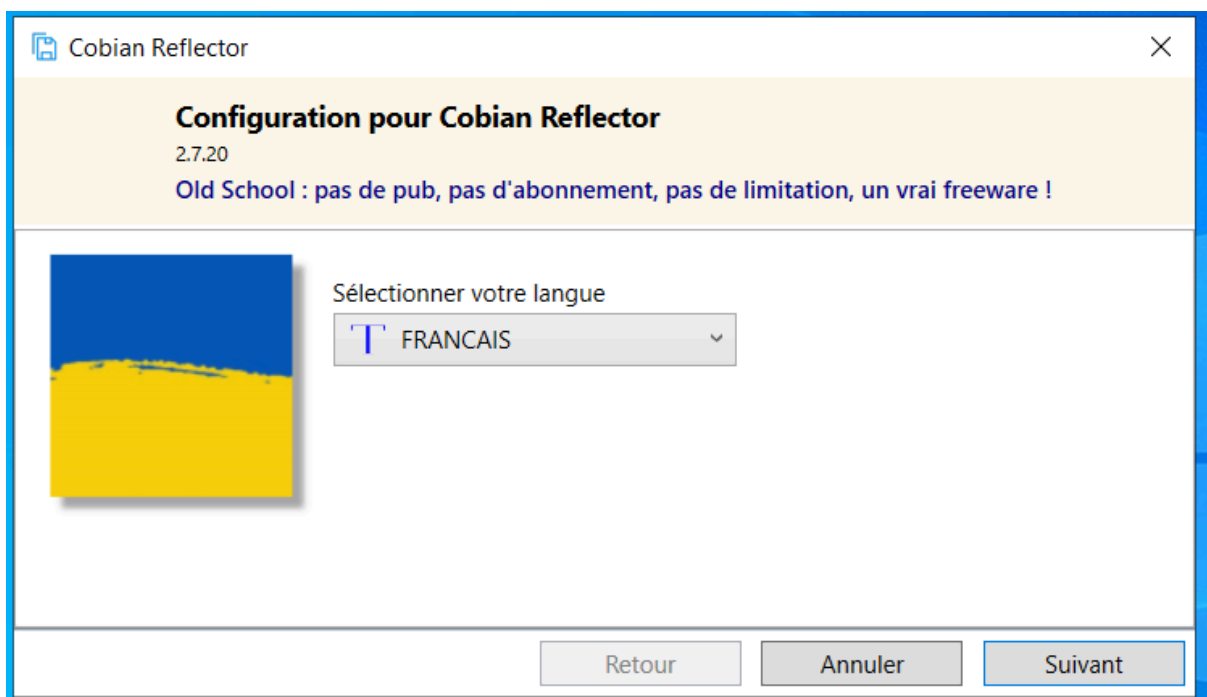
OpenVPN Servers

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	

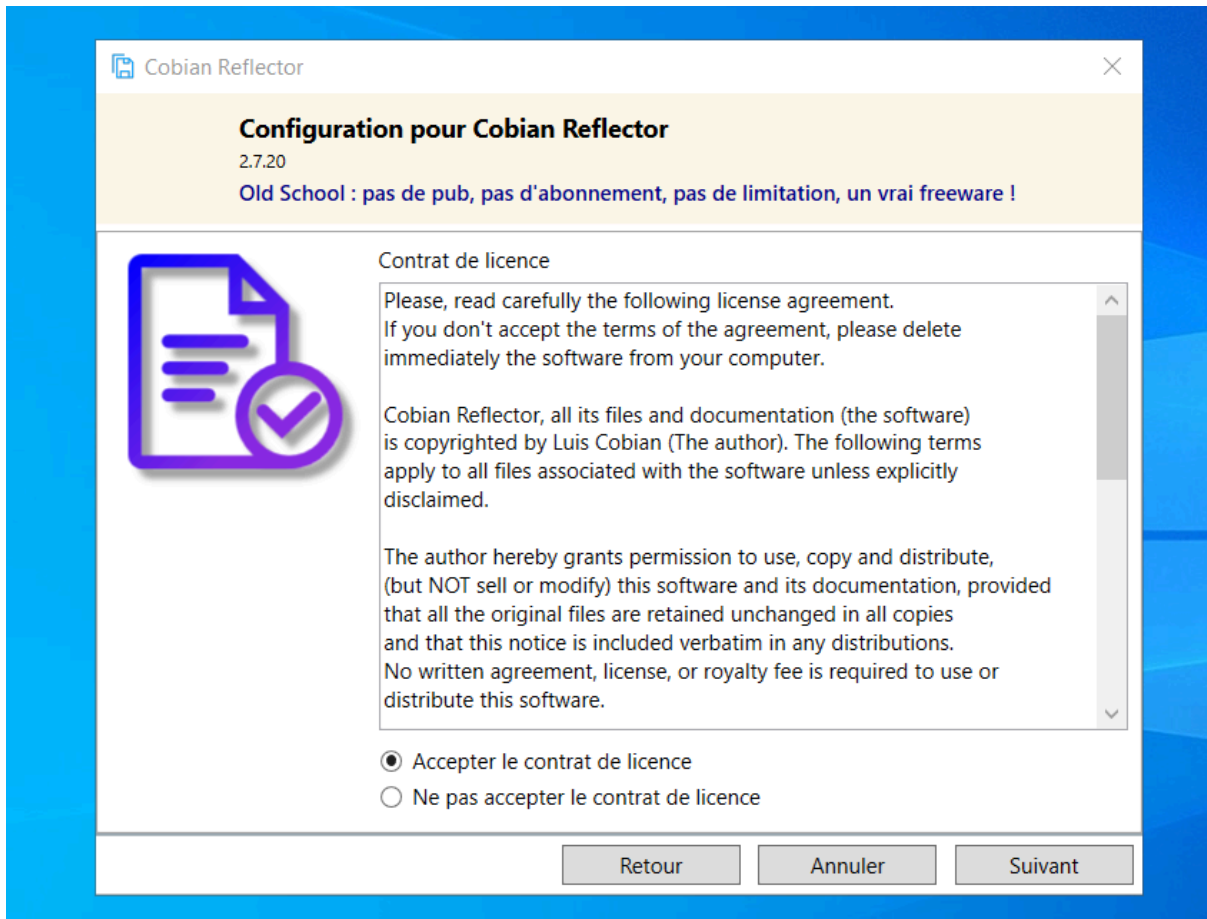
Add

Installation de Cobian

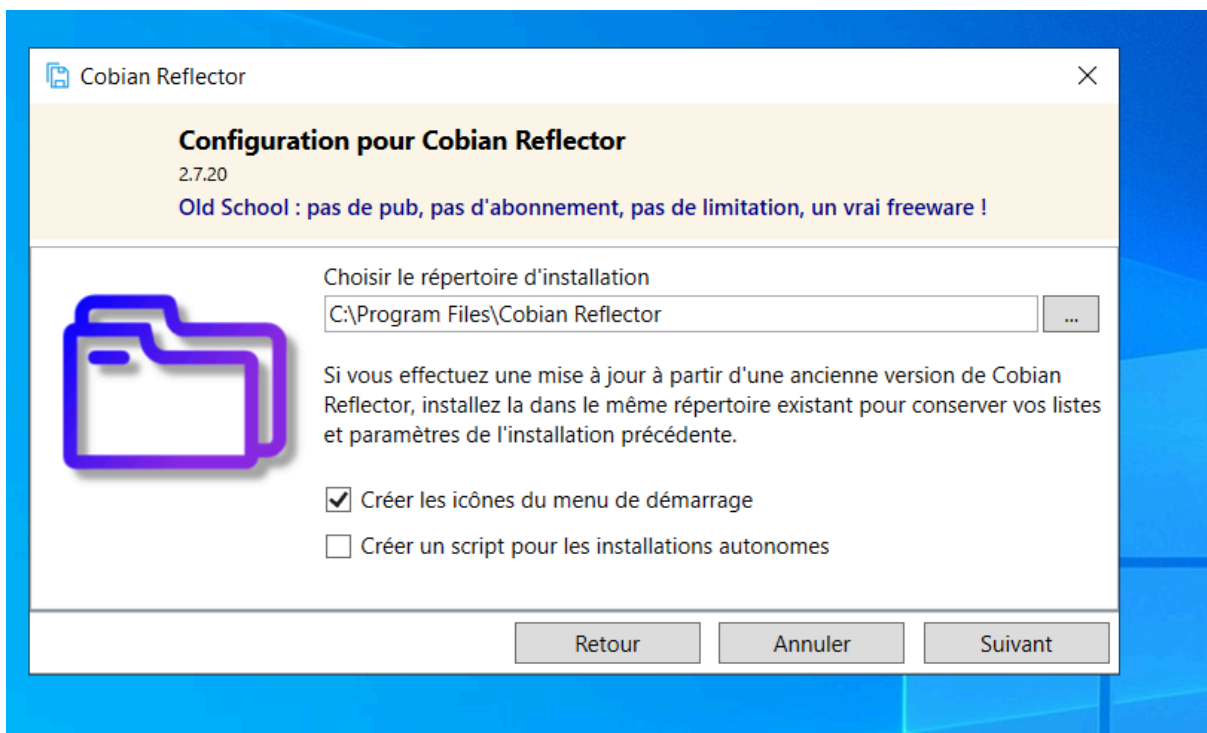
Rendez-vous sur le site officiel de Cobian Backup
Téléchargez la dernière version (Cobian Reflector de
préférence)



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



Accepter le contrat de licence et faire suivant




Faire suivant

Cobian Reflector

Configuration pour Cobian Reflector

2.7.20
Old School : pas de pub, pas d'abonnement, pas de limitation, un vrai freeware !



Type d'installation

- En tant qu'application (pas de démarrage automatique)
- En tant qu'application (démarrage automatique pour l'utilisateur actuel)
- En tant qu'application (démarrage automatique pour tous les utilisateur
- En tant que service

Installation du service

- Installer sous le compte système local
- Installer sous un compte standard

Nom d'utilisateur (DOMAINE\utilisateur) Mot de passe

Démarrer automatiquement l'interface utilisateur

Cliché instantané des volumes

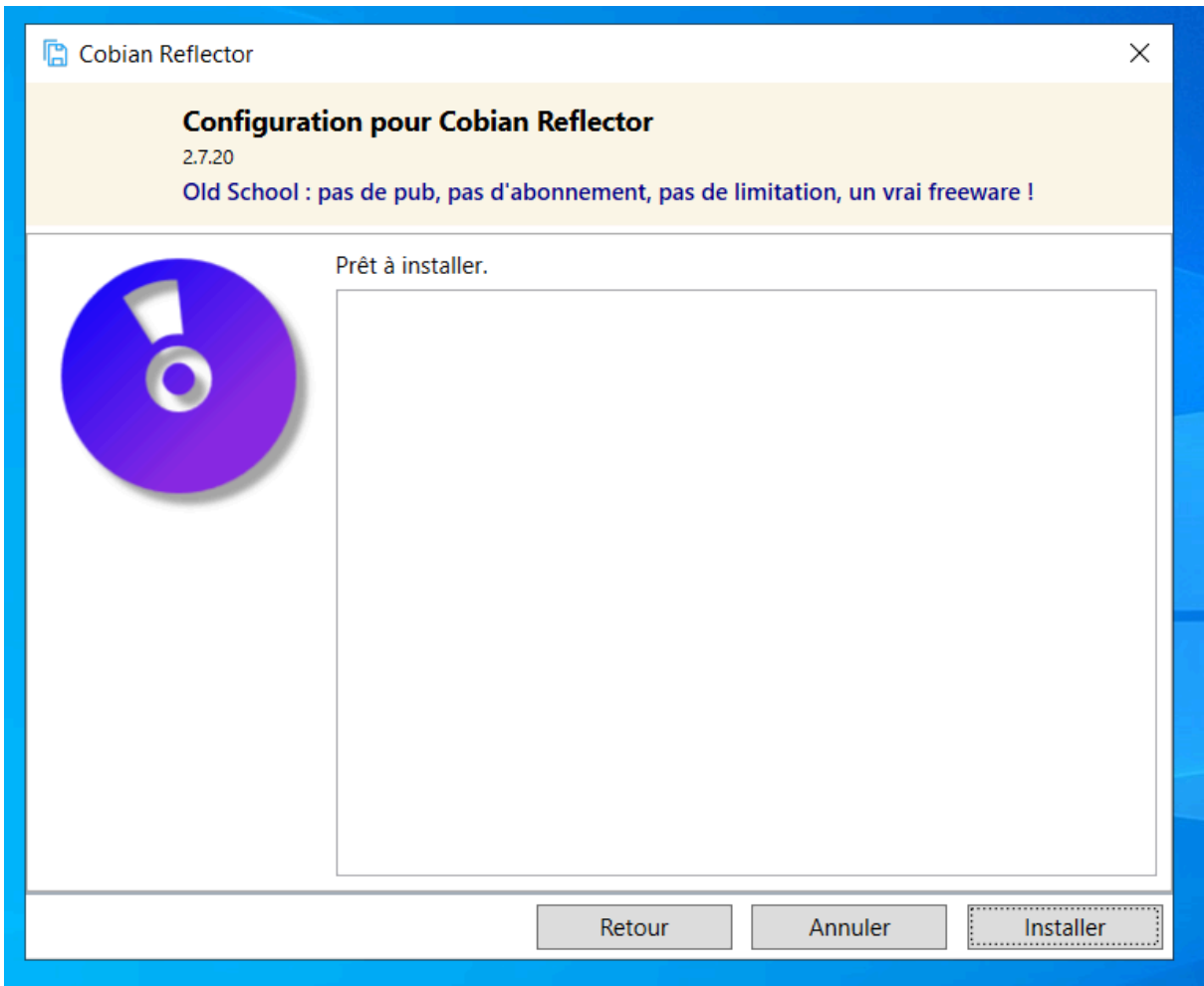
Installer le service de Volume Shadow Copy

Cobian Reflector

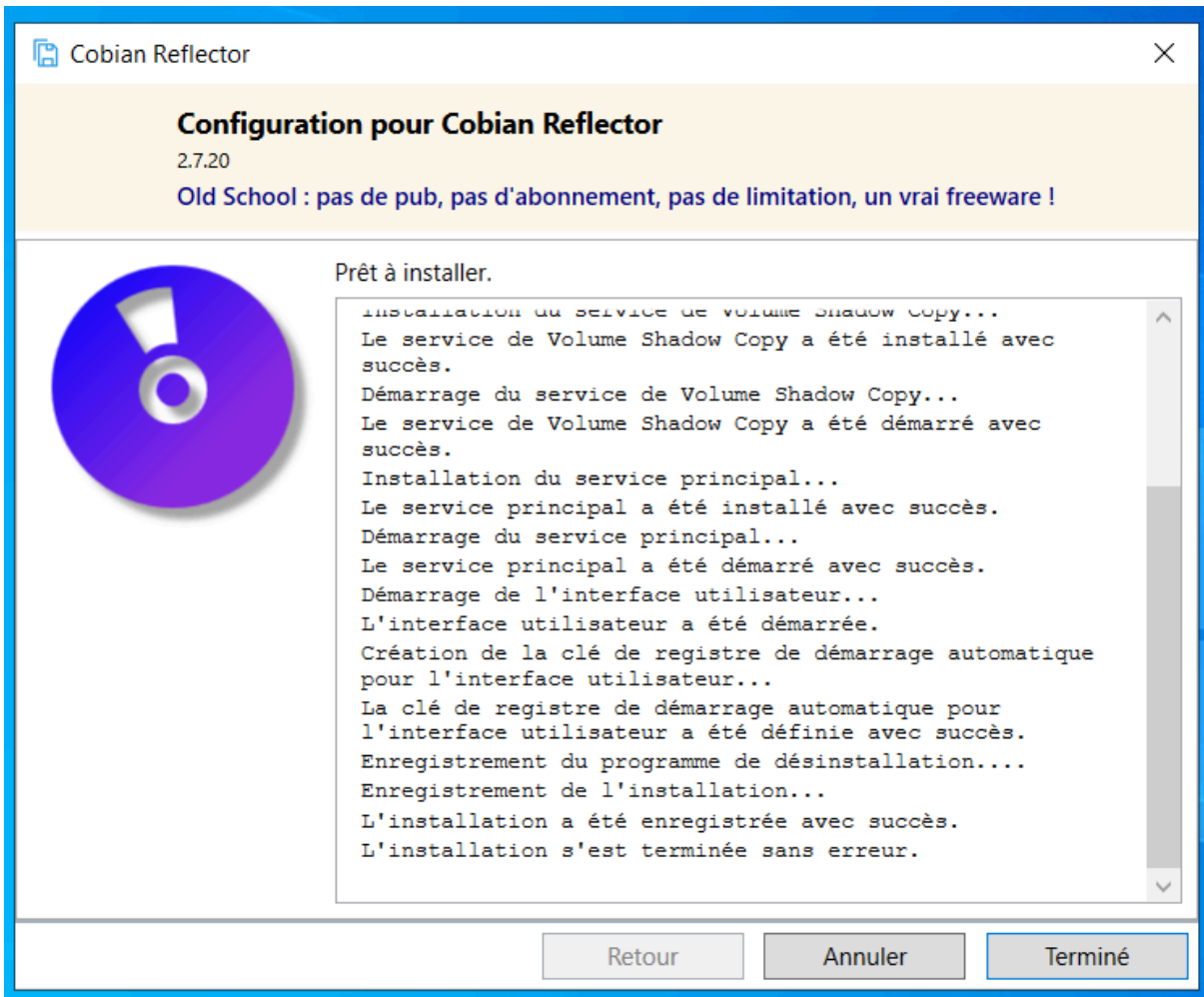
Configuration pour Cobian Reflector
2.7.20
Old School : pas de pub, pas d'abonnement, pas de limitation, un vrai freeware !
Type d'installation

Annuler Suivant

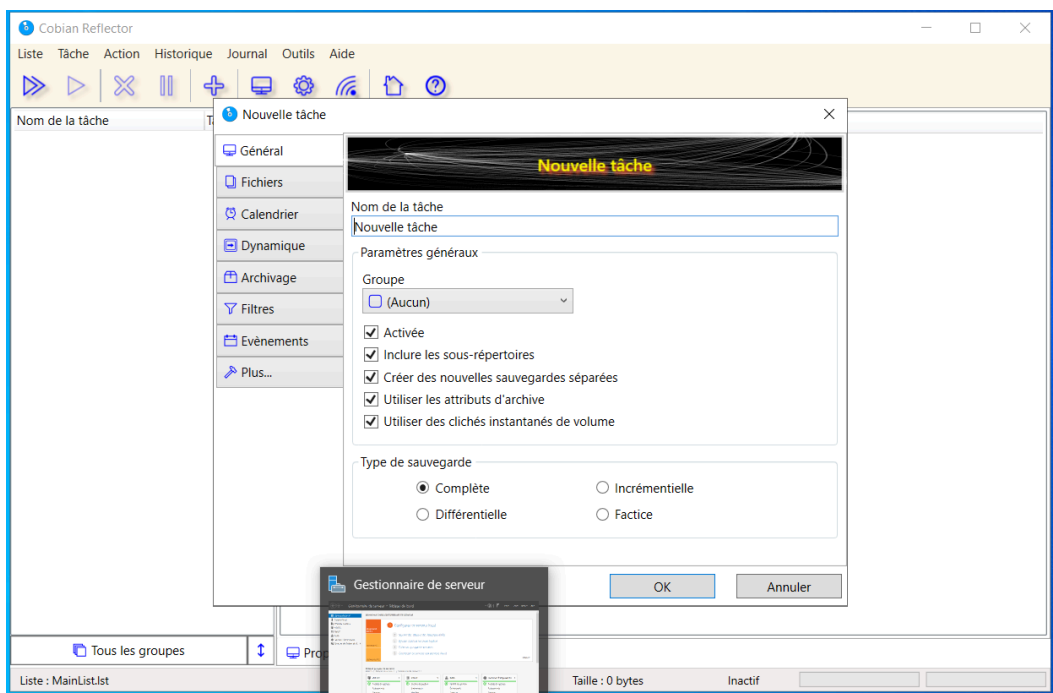
Ici installez bien en tant que service.



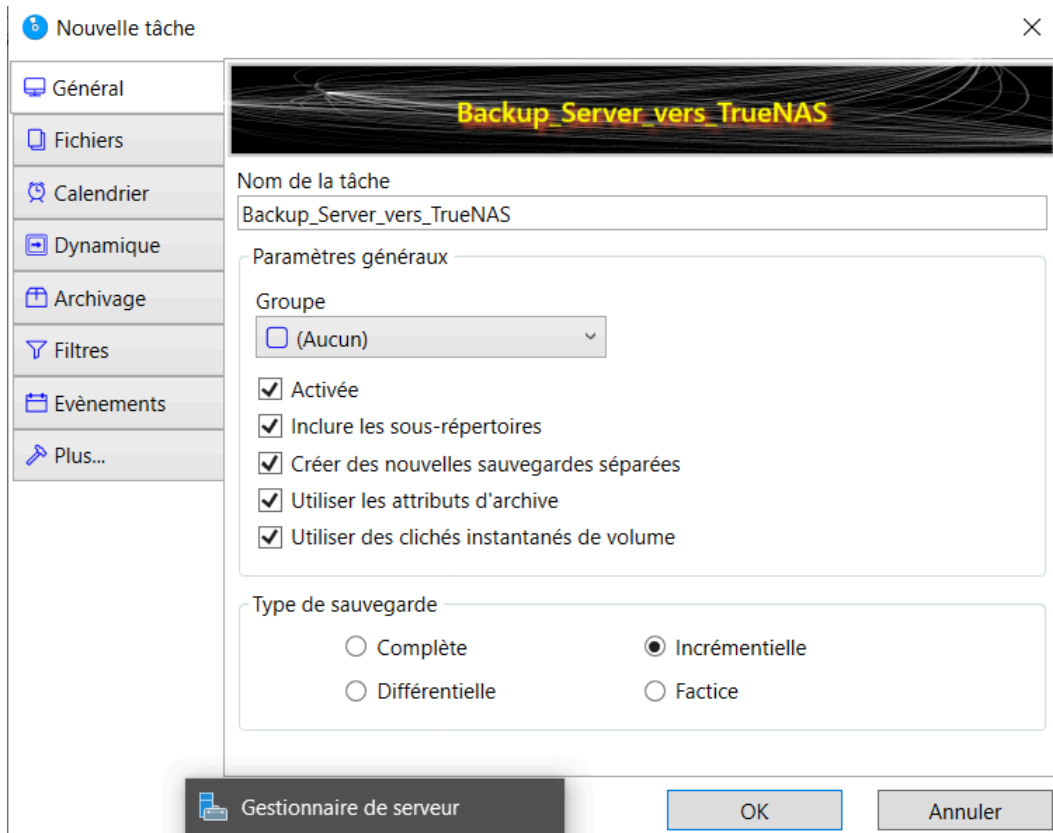
Et faire Installer



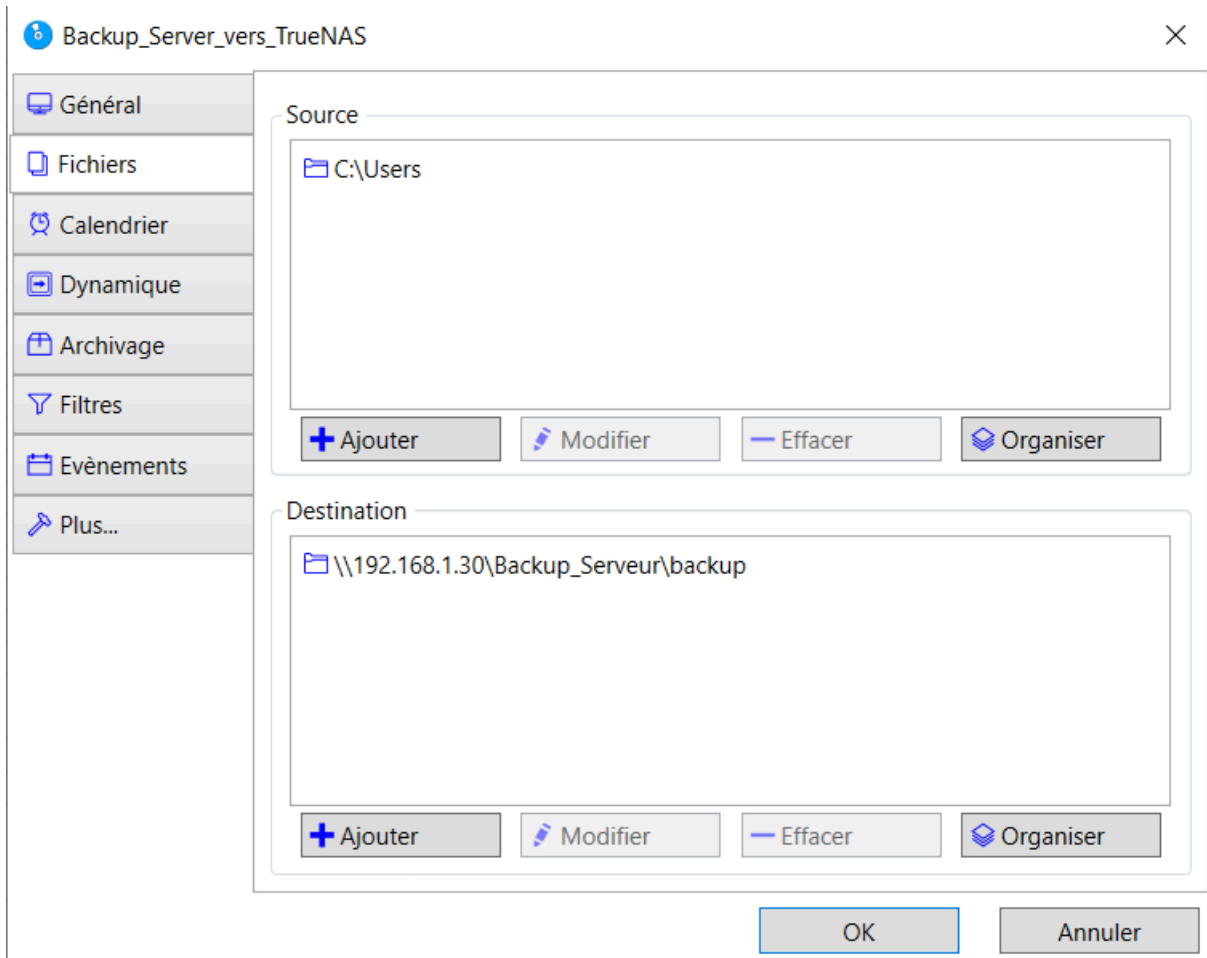
L'installation s'est faite sans erreur. Faire Terminé



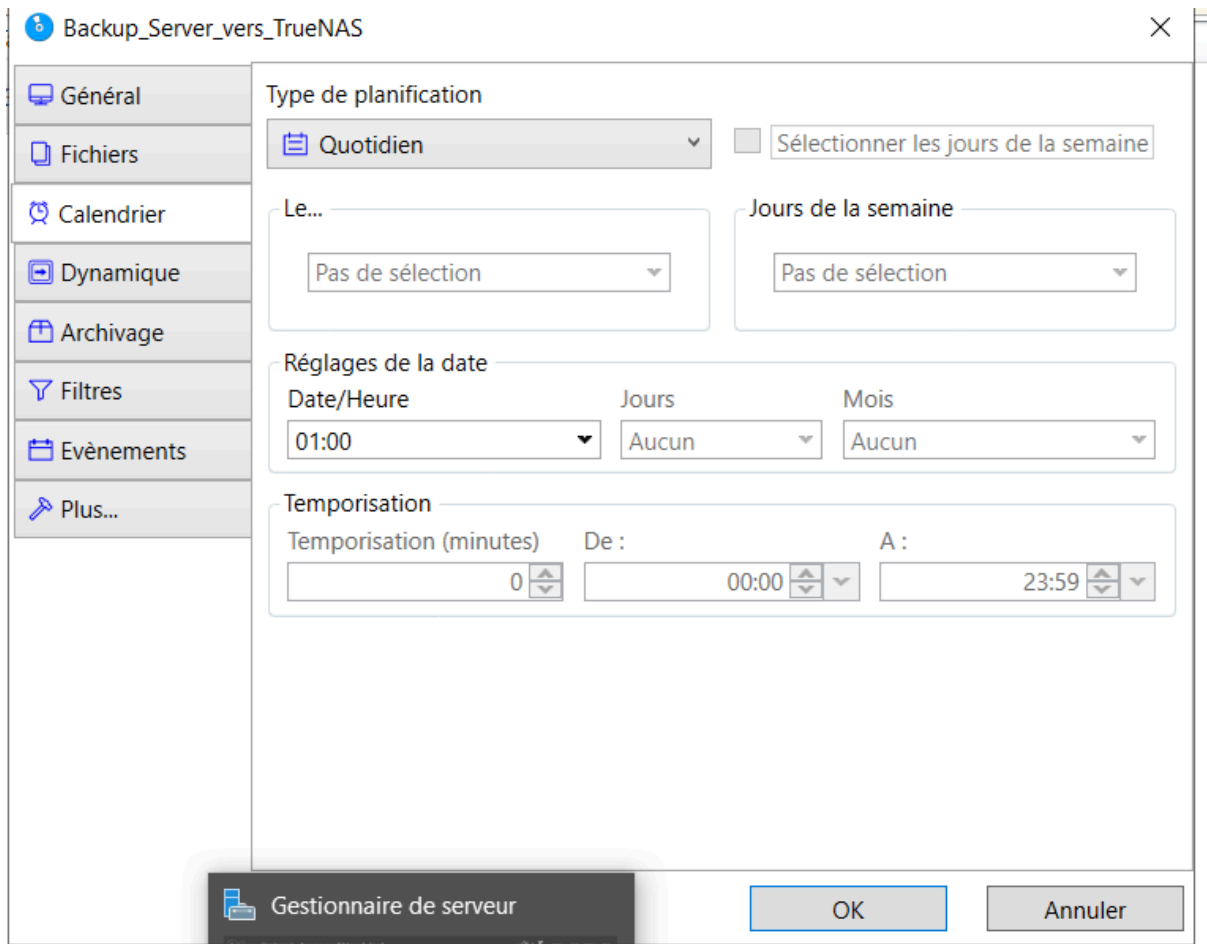
Ouvrez l'application Cobian Reflector et créez une nouvelle tâche.



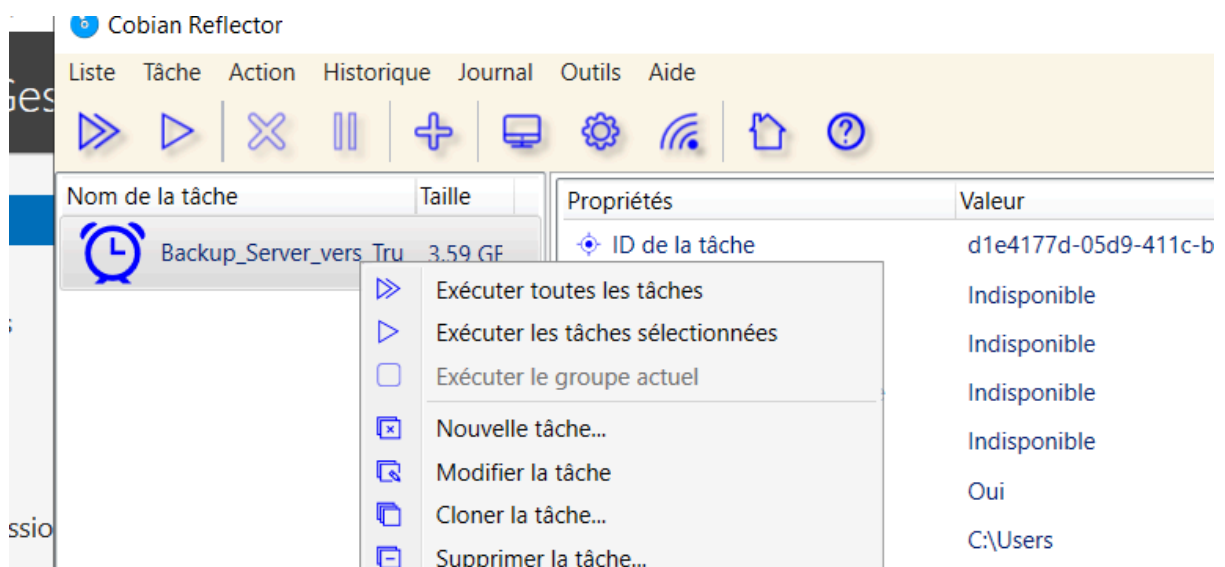
Remplir le nom de votre tâche et choisir le type de sauvegarde
Incrémentielle



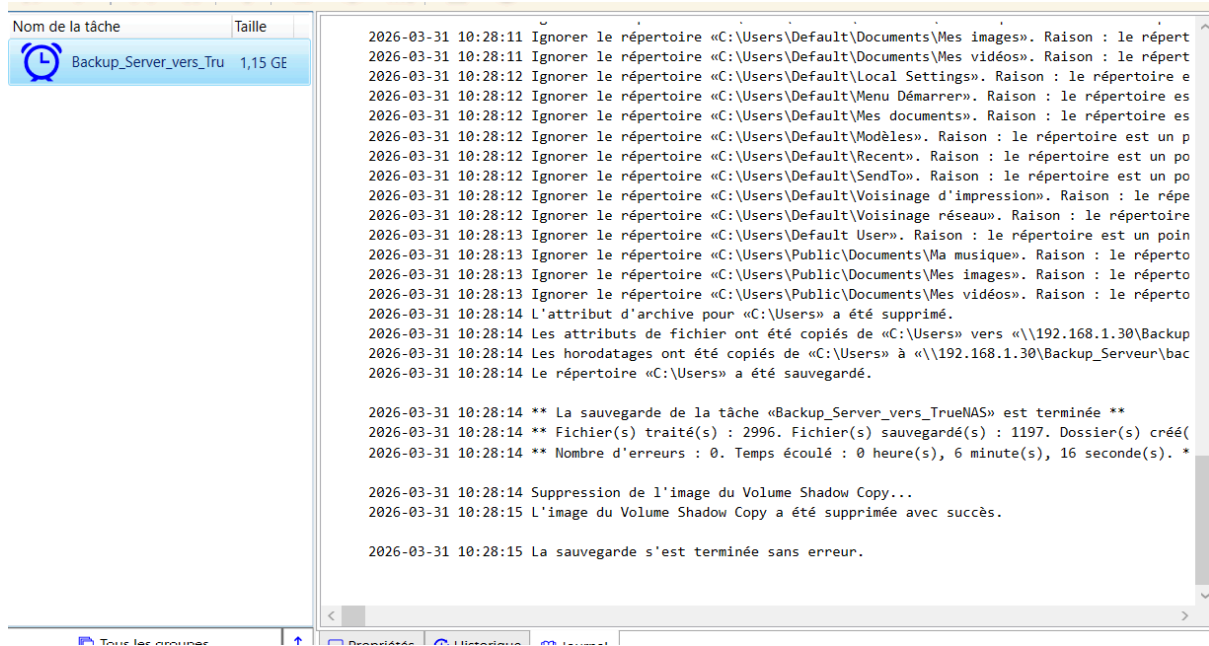
Entrez vos sources (dossier du windows serveur) et en destination votre TrueNas



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 été exécuté sans erreur, la sauvegarde est donc en place sur le dossier de backup

Enzo
ALCARAZ
SIO 2