DOCUMENTATION PROJET 2 BTS

Conception, déploiement et exploitation d'une infrastructure réseau sécurisée

1. Présentation de l'entreprise et du projet

1.1 VitaBigPharma est une entreprise du secteur pharmaceutique en pleine expansion. Pour accompagner sa croissance, elle a ouvert deux sites stratégiques : le siège à **Toulouse** (géré par l'étudiant A) et un centre opérationnel à **Marseille** (géré par l'étudiant B).

L'objectif de ce projet est de concevoir et déployer une infrastructure réseau et système complète, sécurisée et interconnectée, permettant une collaboration fluide entre les deux sites tout en garantissant la haute disponibilité des services critiques (ERP, Support IT, Supervision).

Les missions principales sont donc :

- **La centralisation :** Unifier la gestion des identités via Active Directory.
- **La sécurité :** Garantir la confidentialité des données pharmaceutiques et la traçabilité des accès.
- **Le télétravail :** Offrir un accès distant sécurisé aux collaborateurs nomades.
- **La continuité de service :** Assurer la disponibilité des services via la réplication et la supervision.

1.2 Architecture Technique et Adressage IP

L'organisation s'articule sur deux sites distincts :

- **Site de Toulouse (Siège Administratif) :** Regroupe la Direction, les Ressources Humaines et le pôle Finance. Ce site héberge l'ERP métier (**Dolibarr**).
- **Site de Marseille (Centre Technique) :** Accueille le service technique et le support informatique. Ce site centralise la gestion du parc et le ticketing (**GLPI**).

L'infrastructure repose sur une segmentation stricte des réseaux afin d'isoler les flux sensibles des flux utilisateurs. Chaque site est protégé par un pare-feu **pfSense/OPNSense** qui assure le routage, le filtrage et l'interconnexion VPN.

Le plan d'adressage (Côté Marseille) a été conçu pour permettre une scalabilité future tout en respectant les contraintes de sécurité

Zone	Sous-réseau	Passerelle (pfSense)	Description
WAN	Réseau Bridge/VMBR	DHCP / Statique	Accès Internet & VPN
LAN Serveurs	172.16.10.0/24	172.16.10.254	Contrôleur de domaine, GLPI, Supervision
LAN Clients	172.16.20.0/24	172.16.20.254	Postes collaborateurs (Débit limité à 5 Mb/s)
VPN Nomade	10.0.8.0/24	10.0.8.1	Clients distants (Télétravail)

Nom du Serveur	OS	Adresse IP	Rôle Principal
SRV-AD-MARS	Windows Server 2022	172.16.10.1	AD DS, DNS, Fichiers
SRV-GLPI-MON	Ubuntu 22.04 LTS	172.16.10.10	GLPI, Docker (Prometheus)

2 / Déploiement de l'Infrastructure Réseau (pfSense)

2.1 Choix et mise en œuvre du pare-feu

Initialement, la solution **OPNSense** a été retenue et maquettée pour la segmentation des réseaux (WAN, LAN Serveurs, LAN Collaborateurs). Cependant, au cours de la phase de déploiement et pour garantir une meilleure interopérabilité avec les configurations spécifiques du site de Toulouse, le choix s'est finalement porté sur **pfSense**.

Justification du changement :

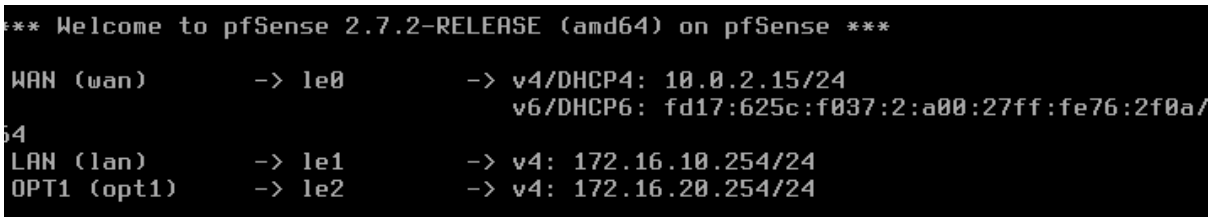
- **Stabilité des tunnels VPN :** Facilitation de l'interconnexion IPsec avec le site distant.
- **Gestion du Traffic Shaping :** Prise en main plus intuitive des *Limiters* pour appliquer la restriction de 5 Mb/s sur le LAN Collaborateurs.
- **Documentation :** Support communautaire plus vaste pour les problématiques avancées de liaison LDAP rencontrées.

2.2 Configuration des interfaces sur pfSense

Le pare-feu a été configuré avec trois cartes réseau virtuelles :

- **WAN (Adaptateur 1) :** Mode Accès par pont (Bridge) pour simuler la sortie Internet et permettre le montage des tunnels VPN.
- **LAN Serveurs (Adaptateur 2) :** Réseau interne (VLAN-SERVEURS) hébergeant les services AD et GLPI.

- **LAN Collaborateurs (Adaptateur 3) :** Réseau interne (VLAN-COLLAB) isolé, sur lequel la QoS est appliquée.

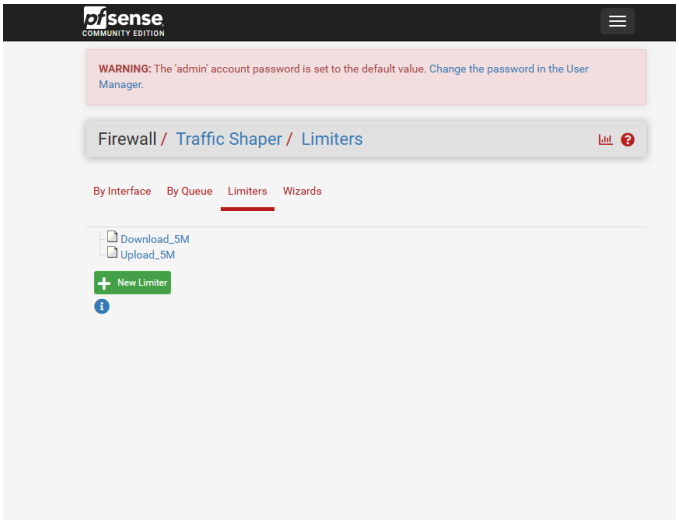


2.3 Mise en œuvre de la Qualité de Service (QoS) : Traffic Shaping

A. Création des limiters

La première étape a consisté à créer deux "tuyaux" virtuels (Limiters) dans le menu Firewall > Traffic Shaper > Limiters.

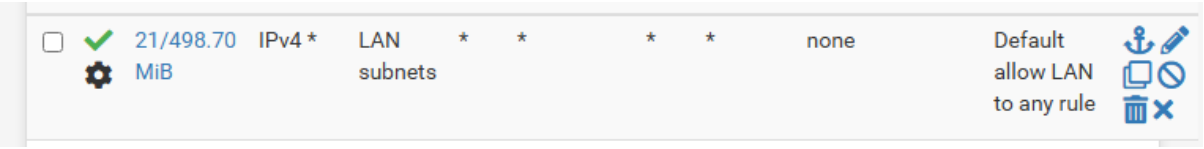
- **Upload_5M : Configuré à 5 Mbit/s pour le flux montant.**
- **Download_5M : Configuré à 5 Mbit/s pour le flux descendant.**



B. Application de la règle de filtrage

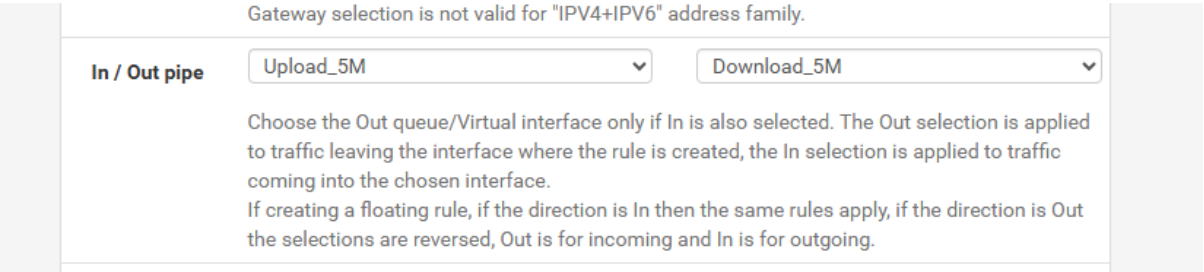
Une fois les "tuyaux" créés, il a fallu les activer en les associant à une règle de pare-feu sur l'interface LAN Collaborateurs.

1. **Sélection de la règle : J'ai édité la règle de passage par défaut (*Default allow LAN to any rule*).**



1. **Injection des Limiters :** Dans les paramètres avancés de cette règle, j'ai sélectionné le limiter Upload_5M pour le flux entrant (*In*) et Download_5M pour le flux sortant (*Out*).

Résultat : Tout appareil connecté sur ce VLAN est désormais bridé automatiquement par le pare-feu.



3. Services Windows et Active Directory

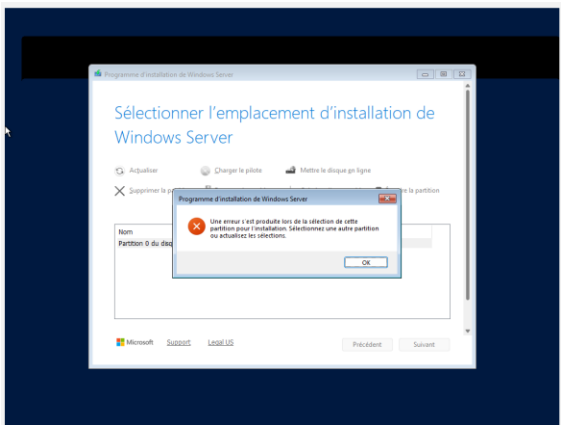
3.1 Préparation et Installation du Serveur

L'installation de **Windows Server 2022** a été effectuée sur une machine virtuelle dédiée. Lors de la phase d'installation, une problématique de partitionnement a été rencontrée, empêchant la création des volumes système.

Résolution via Diskpart : Pour débloquer l'installation, j'ai utilisé l'invite de commande (Maj + F10) pour réinitialiser le disque dur virtuel :

1. diskpart : Lancement de l'utilitaire.
2. select disk 0 : Sélection du disque principal.
3. clean : Effacement complet de la table de partition.
4. convert mbr : Conversion du disque en format MBR (compatible avec le mode BIOS de la VM).

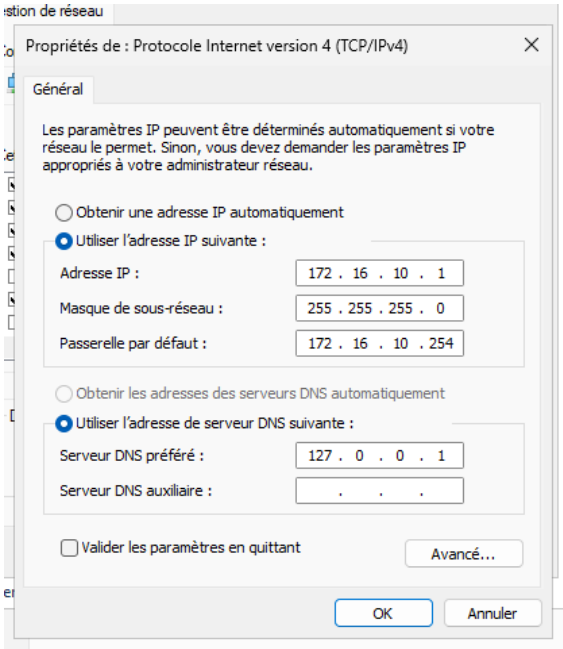
Justification technique : Cette manipulation a permis de repartir sur une base de stockage vierge et saine, indispensable avant la promotion du serveur.



3.2 Configuration Réseau et Promotion du domaine

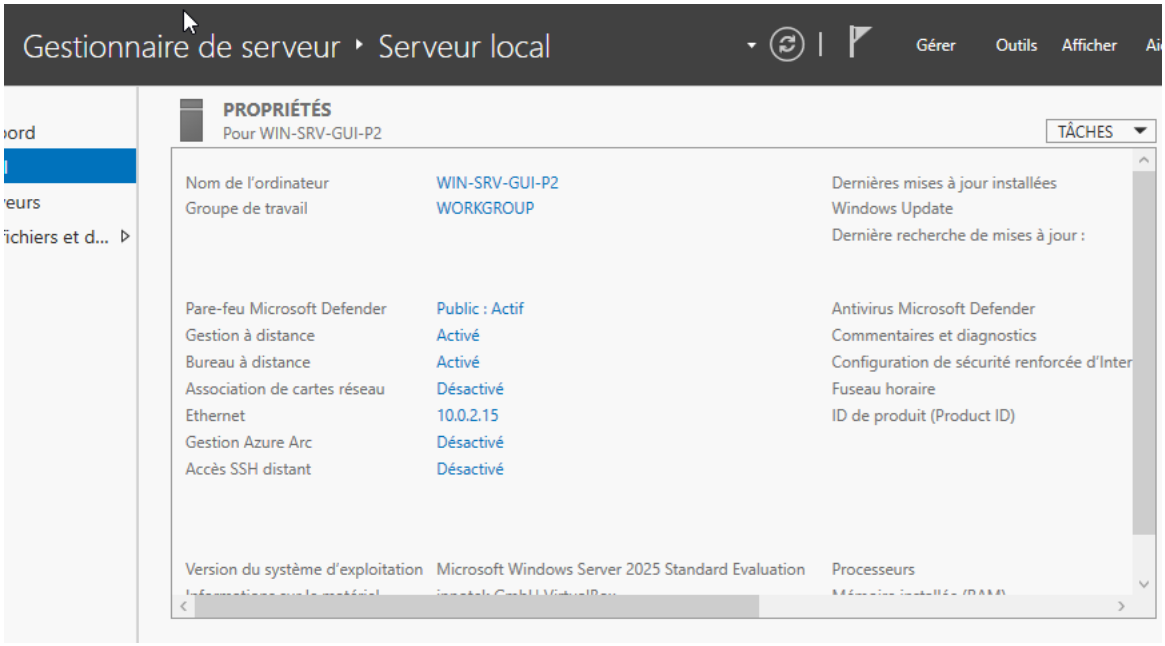
Avant de promouvoir le serveur en tant que Contrôleur de Domaine (DC), j'ai configuré les paramètres critiques suivants :

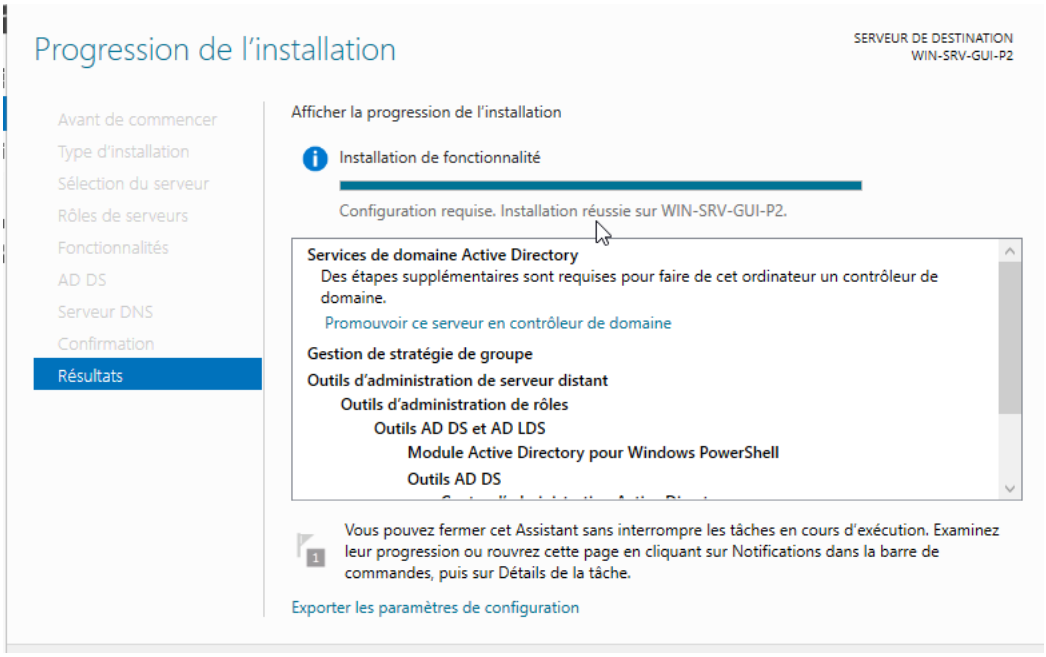
- **Adressage IP Statique : Fixation de l'IP à 172.16.10.1 pour garantir que les services DNS et d'authentification soient toujours joignables.**
- **Service DNS : Configuration du serveur pour qu'il pointe sur lui-même (127.0.0.1), car l'Active Directory est intrinsèquement lié au service DNS.**



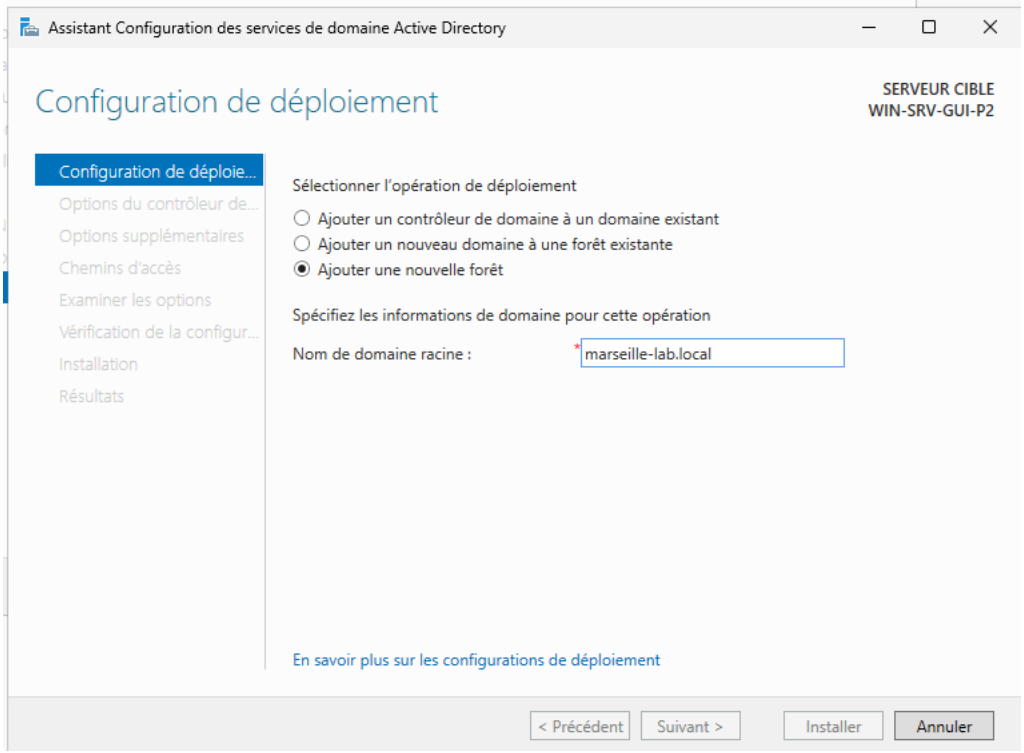
- **Promotion du Domaine : Le serveur a été promu pour créer la forêt et le domaine marseille-lab.local.**

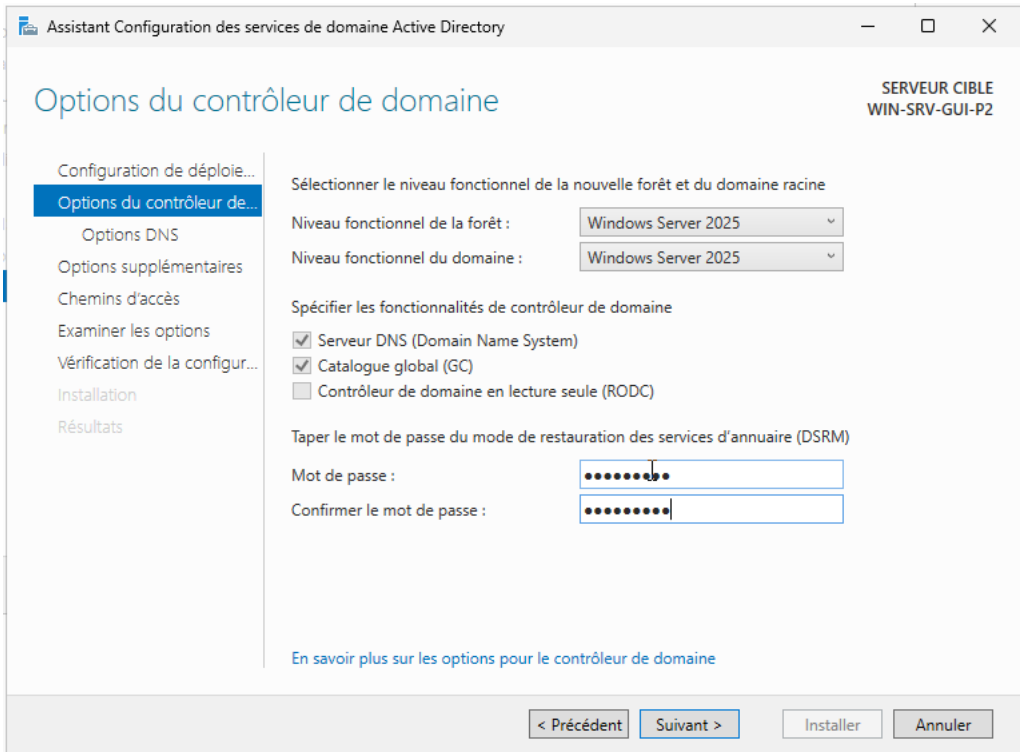
Avant la promotion du serveur, le **Bureau à Distance (RDP)** a été activé. Cette étape est cruciale pour permettre une administration distante fluide et sécurisée du contrôleur de domaine, sans avoir à dépendre de la console de l'hyperviseur (VirtualBox dans notre cas)

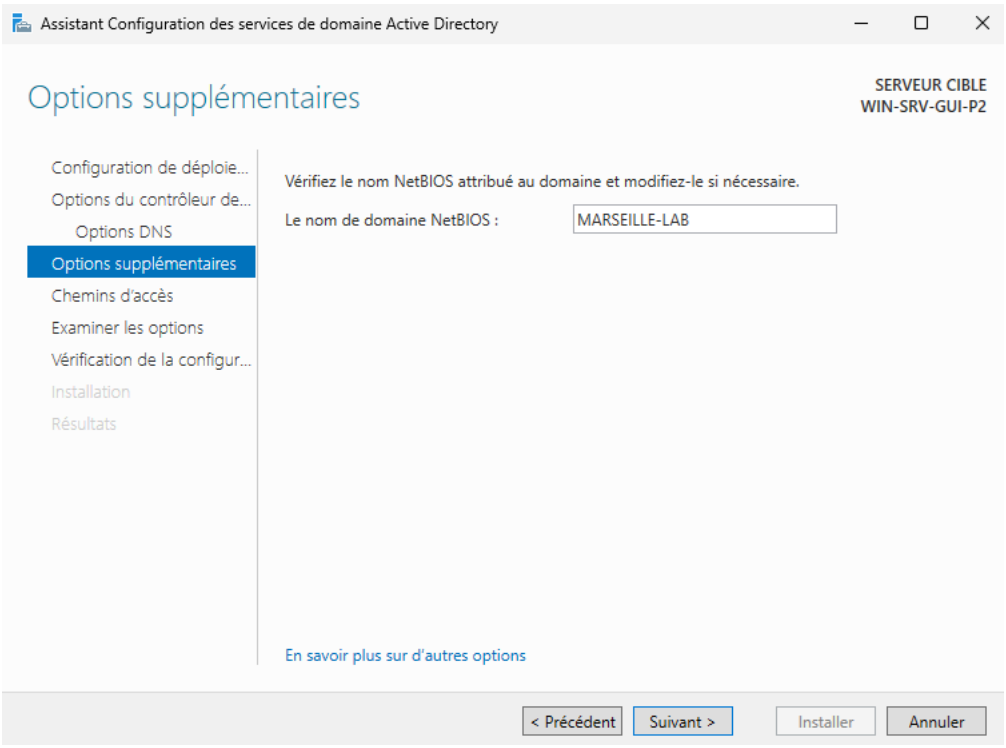




Ensuite, une fois le réseau opérationnel, le rôle **AD DS (Active Directory Domain Services)** a été installé et le serveur a été promu en tant que contrôleur de domaine pour la forêt « ***marseille-lab.local*** »








```
> 10.0.2.15
Serveur :   win-srv-gui-p2.marseille-lab.local
Address:  10.0.2.15

Nom :    win-srv-gui-p2.marseille-lab.local
Address:  10.0.2.15

> marseille-lab.local
Serveur :   win-srv-gui-p2.marseille-lab.local
Address:  10.0.2.15

Nom :    marseille-lab.local
Address:  10.0.2.15
```

3.3 Automatisation annuaire

Automatisation PowerShell

Pour gérer l'arrivée massive de collaborateurs, j'ai automatisé la création des comptes via un script **PowerShell** lié à un fichier CSV.

Fonctionnement du script :

- Création automatique des identifiants (prenom.nom).

- Placement des utilisateurs dans leurs Unités d'Organisation (OU) respectives (RH, Technique, etc.).
- Attribution immédiate aux groupes de sécurité pour gérer les permissions.

```
#1. Importation du module Active Directory

Import-Module ActiveDirectory

#2. Chemin du fichier CSV (Vérifie qu'il est bien sur ton C:)

$csvPath = "C:\users_marseille.csv" $users = Import-Csv -Path $csvPath -Delimiter
","

#3. Configuration du domaine

$DomainDNS = "marseille-lab.local"

foreach ($user in $users) { # Création du Login à partir de l'email (ex:
garcia.alex) $Login = ($user.Email.Split("@"))[0]

# Chemin corrigé : Support et Technique sont DANS SOCIETE-MARSEILLE
$TargetOU = "OU=$($user.OU),OU=SOCIETE-MARSEILLE,DC=marseille-lab,DC=local"

# Mot de passe complexe pour passer la sécurité GPO
$Password = ConvertTo-SecureString "Vitabig-2026!!" -AsPlainText -Force

try {
    # Création de l'utilisateur
    New-ADUser -Name "$($user.Prenom) $($user.Nom)" `
               -GivenName $user.Prenom `
               -Surname $user.Nom `
               -SamAccountName $Login `
               -UserPrincipalName "$($Login)@$DomainDNS" `
               -Path $TargetOU `
               -AccountPassword $Password `
               -Enabled $true `
               -ChangePasswordAtLogon $false

    # Ajout automatique au groupe (SUP_N1, SUP_N2, etc.)
    Add-ADGroupMember -Identity $user.Groupe -Members $Login

    Write-Host "SUCCÈS : $($Login) créé dans $($user.OU) et ajouté à
$($user.Groupe)" -ForegroundColor Green
```

```
}
catch {
    Write-Host "ERREUR pour $($Login) : $($_.Exception.Message)" -ForegroundColor
Red
}


}
```

```
                    -GivenName $user.Prenom `
                    -Surname $user.Nom `
                    -SamAccountName $Login `
                    -UserPrincipalName "$($Login)@$DomainDNS" `
                    -Path $TargetOU `
                    -AccountPassword $Password `
                    -Enabled $true `
                    -ChangePasswordAtLogon $false

        # Ajout automatique au groupe (SUP_N1, SUP_N2, etc.)
        Add-ADGroupMember -Identity $user.Groupe -Members $Login

        Write-Host "SUCCES : $($Login) créé dans $($user.OU) et ajouté à $($user.Grou
    }
    catch {
        Write-Host "ERREUR pour $($Login) : $($_.Exception.Message)" -ForegroundColor
    }
}
SUCCES : garcia.alex créé dans Support et ajouté à SUP_N1
SUCCES : bouazizi.imane créé dans Support et ajouté à SUP_N1
SUCCES : moretti.lucas créé dans Support et ajouté à SUP_N1
SUCCES : amine.youssef créé dans Support et ajouté à SUP_N1
SUCCES : kim.sarah créé dans Support et ajouté à SUP_N1
SUCCES : ramirez.diego créé dans Support et ajouté à SUP_N1
SUCCES : kowalczyk.anna créé dans Support et ajouté à SUP_N1
SUCCES : saidi.bilal créé dans Support et ajouté à SUP_N1
SUCCES : park.mina créé dans Support et ajouté à SUP_N1
SUCCES : petit.romain créé dans Support et ajouté à SUP_N1
SUCCES : hamdi.noura créé dans Support et ajouté à SUP_N2
SUCCES : bernardi.julien créé dans Support et ajouté à SUP_N2
SUCCES : mansour.farid créé dans Support et ajouté à SUP_N2
SUCCES : yilmaz.elif créé dans Support et ajouté à SUP_N2
SUCCES : faure.olivier créé dans Support et ajouté à SUP_N2
SUCCES : akhtar.sana créé dans Support et ajouté à SUP_N2
SUCCES : stojanovic.nikola créé dans Support et ajouté à SUP_N2
SUCCES : romano.paola créé dans Support et ajouté à SUP_N2
SUCCES : elmansouri.hamza créé dans Support et ajouté à SUP_N2
SUCCES : benoit.claire créé dans Support et ajouté à SUP_N2
SUCCES : aziz.omar créé dans Technique et ajouté à SUP_N3
SUCCES : renard.isabelle créé dans Technique et ajouté à SUP_N3
SUCCES : alvarez.sergio créé dans Technique et ajouté à SUP_N3
SUCCES : popov.vlad créé dans Technique et ajouté à SUP_N3
SUCCES : perreira.nathalie créé dans Technique et ajouté à SUP_N3
SUCCES : bouzidi.hicham créé dans Technique et ajouté à SUP_N3
SUCCES : nowak.marek créé dans Technique et ajouté à SUP_N3
SUCCES : abdullah.aisha créé dans Technique et ajouté à SUP_N3
SUCCES : dominguez.luis créé dans Technique et ajouté à SUP_N3
SUCCES : oconnell.kevin créé dans Technique et ajouté à SUP_N3
```

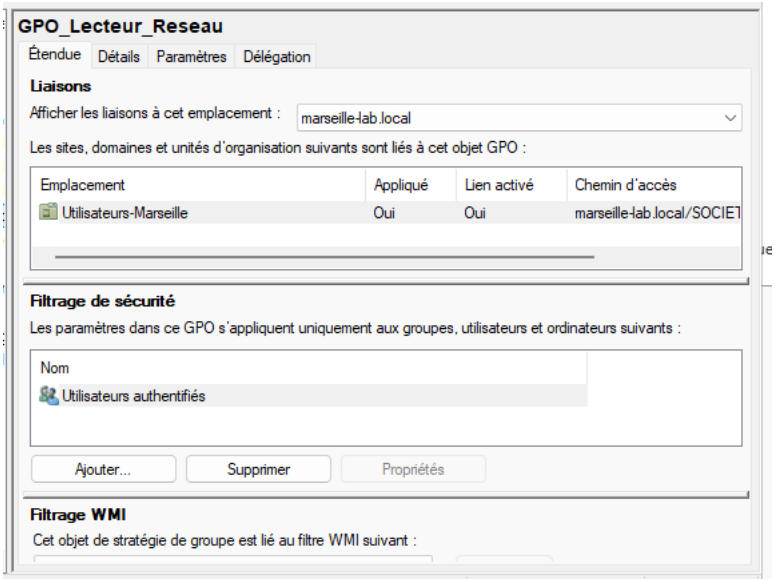
Création des utilisateurs OK

3.4 Déploiement des lecteurs réseau (GPO)

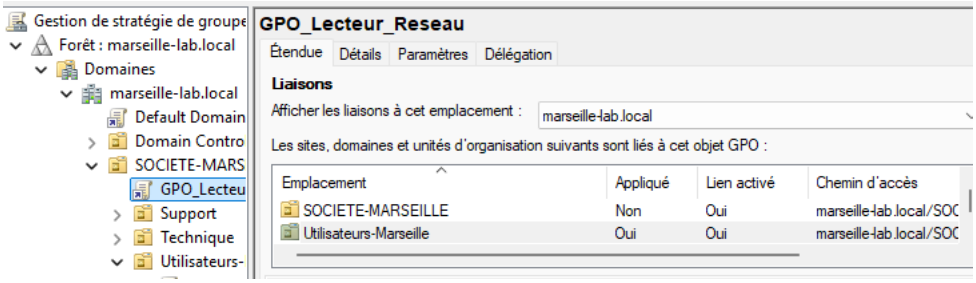
Pour centraliser les données des collaborateurs, j'ai mis en place un mappage automatique de lecteur réseau via une Stratégie de Groupe (GPO).

- Configuration : Dans l'éditeur de gestion des GPO, j'ai configuré : Configuration utilisateur > Préférences > Paramètres Windows > Mappage de lecteurs.
- Action : Création d'un lecteur réseau pointant vers le chemin UNC \\SRV-AD-MARS\Partage_Marseille.
- Lettre attribuée : Z:.

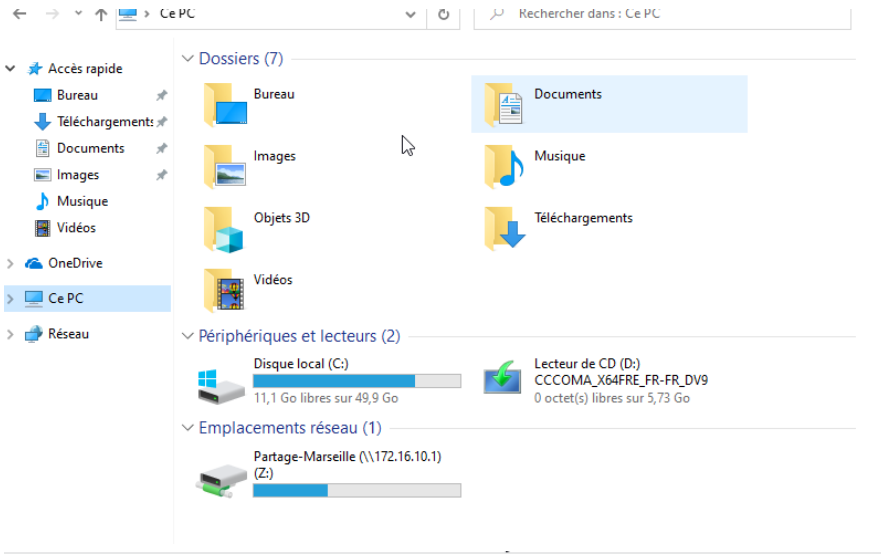
Résultat : À chaque ouverture de session, le lecteur réseau apparaît automatiquement dans l'explorateur de fichiers de l'utilisateur, facilitant le travail collaboratif.

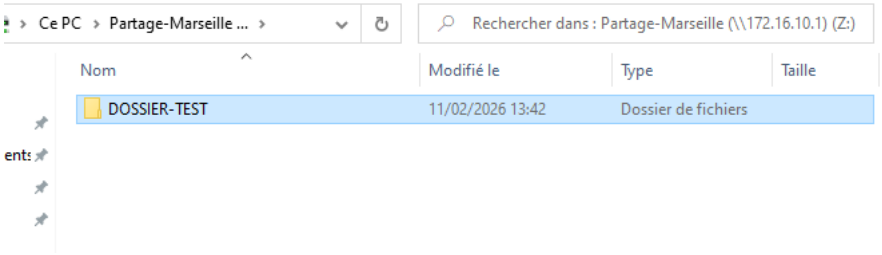


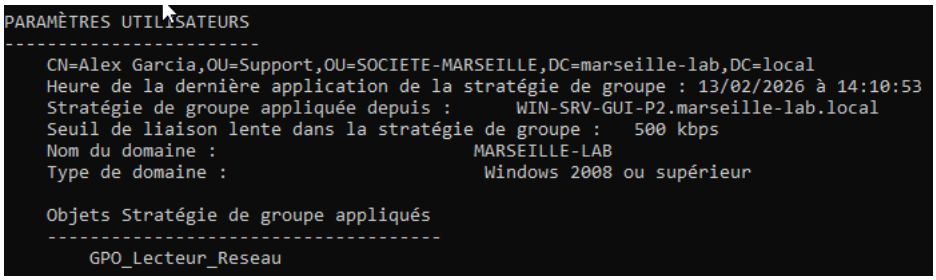
Une fois crée je positionne bien la GPO au niveau du Windows Server dans l'arborescence pour qu'elle soit prise en compte.



Ensuite il est possible de voir le lecteur depuis les sessions utilisateurs :







Bilan de l'étape "Stockage"

- **Disque C:** (Système) ⟶ Propre.
- **Disque E:** (Données) ⟶ Contient le partage.

3.5 Gestion du stockage et Quotas (Rôle FSRM)

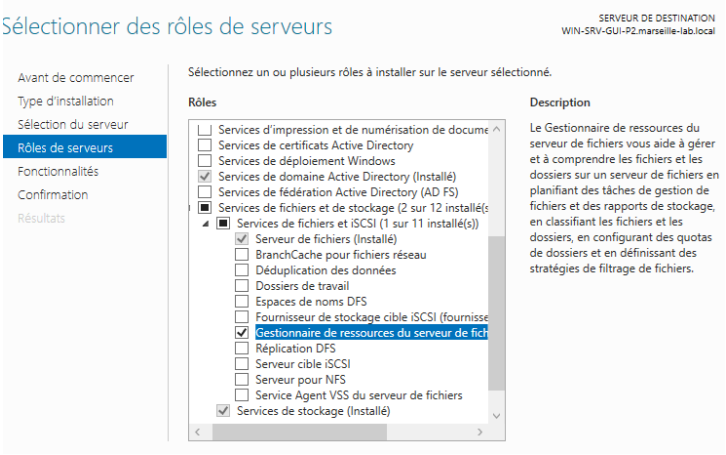
Afin d'éviter la saturation du disque serveur par les utilisateurs, j'ai déployé le rôle FSRM (*File Server Resource Manager*).

A. Mise en place de Quotas

J'ai configuré un Quota inconditionnel (Hard Quota) de 200 Mo sur le dossier partagé des collaborateurs. Le système interdit techniquement tout dépassement de cette limite.

Installation du rôle FSRM

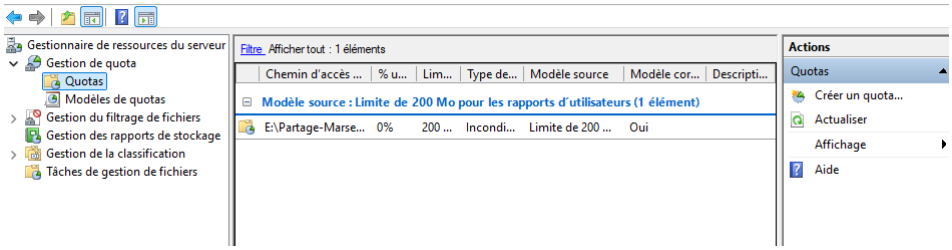
- Sur **Windows Server**, ouvrir le **Gestionnaire de serveur**.
- Cliquer sur **Gérer** (en haut à droite) > **Ajouter des rôles et fonctionnalités**.
- Faire **Suivant** jusqu'à la liste des "Rôles de serveurs".
- Dérouler la flèche **Services de fichiers et de stockage** > **Services de fichiers et iSCSI**.
- Cocher la case **Gestionnaire de ressources du serveur de fichiers**.
- Cliquer sur **Ajouter des fonctionnalités** (si demandé) > **Suivant** > **Installer**.



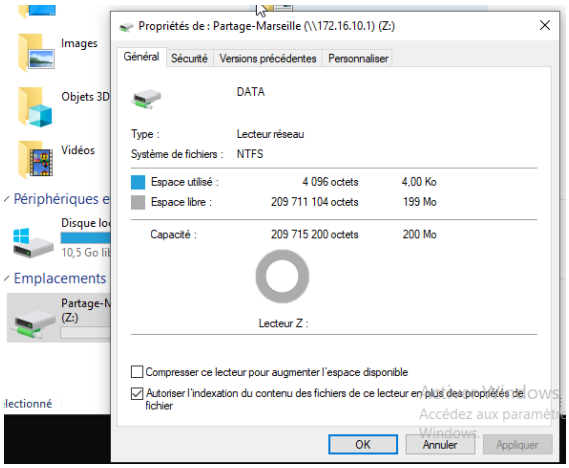
Ensuite je configure le quota :

Une fois FSRM :

1. **Outils** > **Gestionnaire de ressources du serveur de fichiers**.
2. **Gestion de quotas** > **Quotas**.
3. Dans la colonne de droite > **Créer un quota**.
4. **Chemin du quota** : Parcourir... > `E:\Partage-Marseille`.
5. **Propriétés** : Limité à 200Mo
6. Clique sur **Créer**.

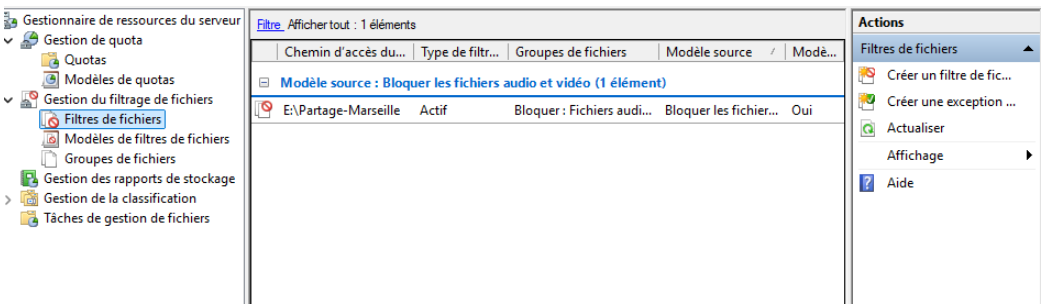


Test quota : Lecteurs Z avec le stockage donné OK

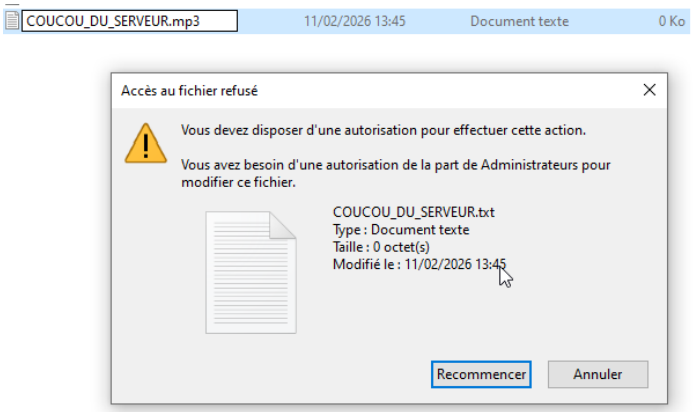


B. Filtrage : Interdiction stricte de stocker des fichiers multimédias (.mp3, .mp4). Un message d'erreur bloque toute tentative d'enregistrement non conforme.

1. (Dans la même fenêtre que pour configurer les quotas) Gestion **du filtrage de fichiers** > **Filtres de fichiers**.
2. **Créer un filtre de fichiers** (à droite)
3. **Chemin** : `E:\Partage-Marseille`.
4. **Propriétés** :
    a. **Bloquer les fichiers audios et vidéo**.
5. Clique sur **Créer**.



Test de créer un fichier en MP3 = Création fichier en txt et modification en MP3 = Message d'erreur

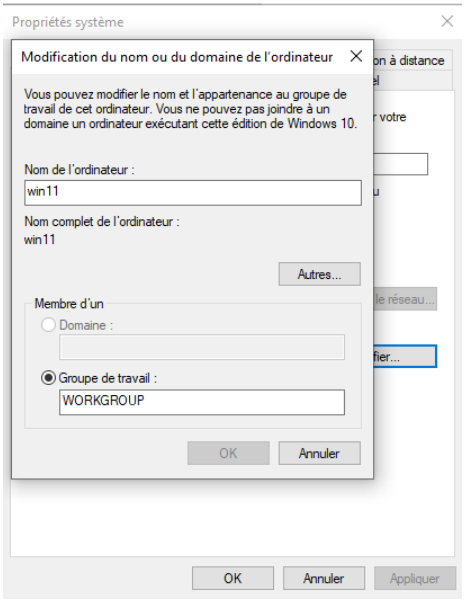


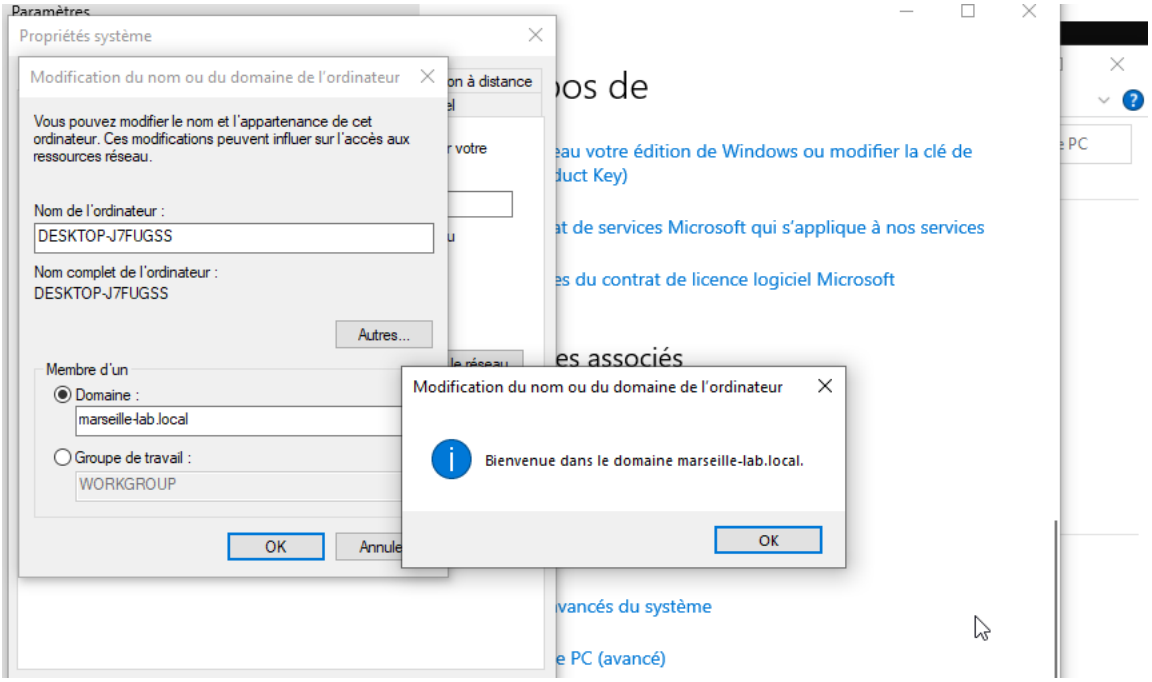
<u>Test effectué sur les dernières étapes pour vérifier le fonctionnement :</u>

- Test ping "marseille-lab.local OK
- Au lancement des sessions "domaine marseille-lab.local" affiché
- GPO fonctionnelle : lecteurs présents sur les sessions user (exemple ici sur la session garcia.alex, en créant un VM win11 et en se connectant au compte user)

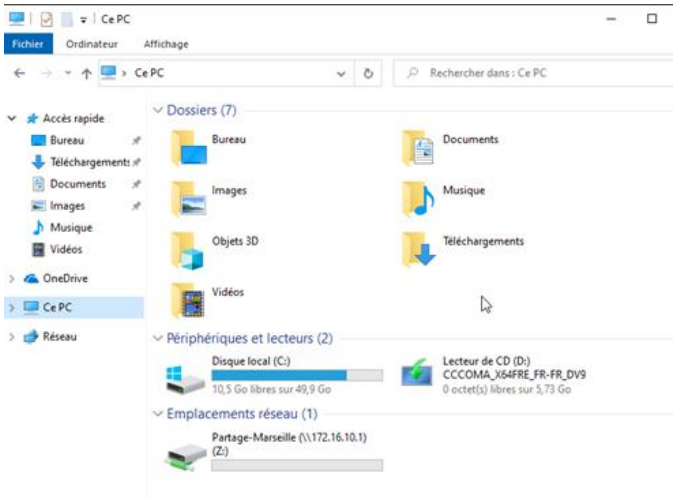
Pour rejoindre le domaine :

Création vm windows 11 + rejoindre le domaine





Résultat le lecteur est présent sur la session utilisateur :



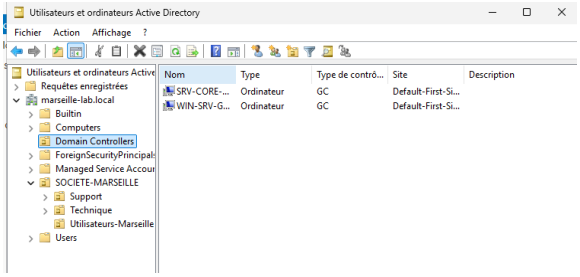
3.6 Haute disponibilité et Réplication

Un second contrôleur de domaine a été déployé sous **Windows Server Core**. La commande repadmin /showrepl a permis de valider la bonne synchronisation de l'annuaire entre les serveurs.

```
================================================================================
                        Paramètres de carte réseau
================================================================================

Index NIC :             6
Nom :                   Ethernet
Description :           Intel(R) PRO/1000 MT Desktop Adapter
Adresse IP :            172.16.10.2,
                        fe80::9842:2b16:766b:9ae1,
                        fd17:625c:f037:2:9be1:bebf:77c4:861c
Masque de sous-réseau : 255.255.255.0
DHCP activé :           False

Passerelle par défaut : 172.16.10.254 fe80::2
1er serveur DNS :       172.16.10.1
2e serveur DNS :
3e serveur DNS :

  1) Définir l'adresse de la carte réseau
  2) Définir les serveurs DNS
  3) Effacer les paramètres du serveur DNS
  4) Renommer la carte réseau

Entrez la sélection (Vide = annuler):
```

Réplication de l'ad

```
S C:\Users\vboxuser> Install-ADDSDomainController -DomainName "marseille-lab.local" -InstallDns -Credential (Get-Credential)


pplet de commande Get-Credential à la position 1 du pipeline de la commande
ournissez des valeurs pour les paramètres suivants :
redential
afeModeAdministratorPassword: **************
onfirmer SafeModeAdministratorPassword: **************

e serveur cible sera configuré en tant que contrôleur de domaine et redémarré à la fin de cette opération.
oulez-vous continuer en procédant à cette opération ?
O] Oui  [T] Oui pour tout  [N] Non  [U] Non pour tout  [S] Suspendre  [?] Aide (la valeur par défaut est « O ») : o
VERTISSEMENT : Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est
ntrouvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS
xistante, vous devez manuellement créer une délégation avec ce serveur DNS dans la zone parente pour activer une résolution
de noms fiable en dehors du domaine « marseille-lab.local ». Sinon, aucune action n'est requise.

VERTISSEMENT : Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est
ntrouvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS
xistante, vous devez manuellement créer une délégation avec ce serveur DNS dans la zone parente pour activer une résolution
de noms fiable en dehors du domaine « marseille-lab.local ». Sinon, aucune action n'est requise.


essage                                 Context           RebootRequired  Status
------                                 -------           --------------  ------
'opération s'est déroulée avec succès. DCPromo.General.3         False Success
```



W server core / Réplication OK

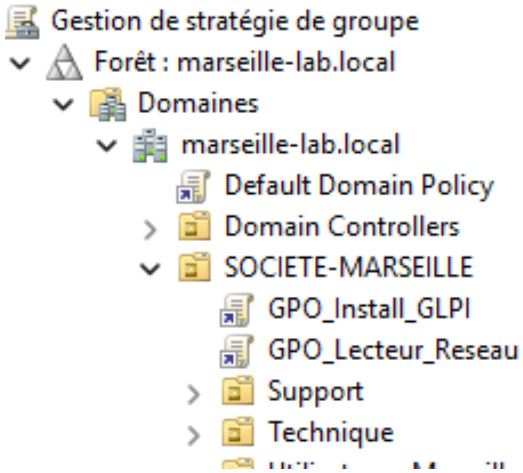
4. Système d'inventaire et d'assistance (GLPI)

Afin de répondre aux besoins de **VitaBigPharma** concernant le suivi du parc informatique, la mise en place d'une solution **GLPI** a été planifiée. Pour assurer un déploiement à grande échelle, la stratégie a été de préparer le parc d'ordinateurs avant même d'installer l'interface web.

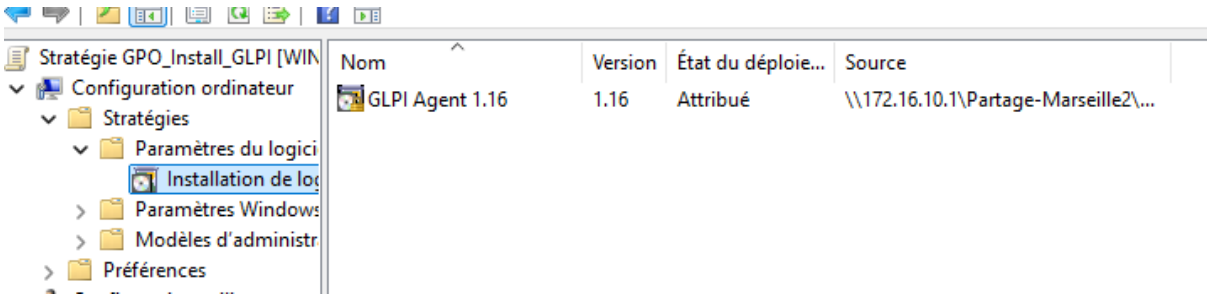
4.1 Déploiement via GPO de l'Agent GLPI

Déploiement par Stratégie de Groupe :

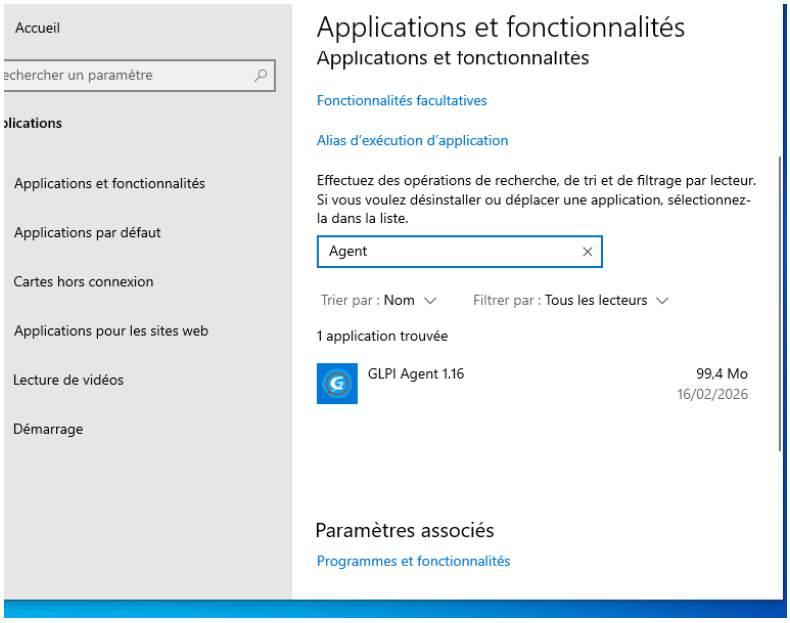
1. **Préparation :** J'ai placé le package d'installation (MSI) du **GLPI Agent** dans un dossier partagé accessible par tous les ordinateurs du domaine.
2. **Création de la GPO :** Dans l'éditeur de gestion des stratégies de groupe, j'ai créé une stratégie affectée à l'Unité d'Organisation des ordinateurs.



Pour distribuer l'agent sur le parc, j'ai créé une stratégie de déploiement de logiciel dans l'éditeur de gestion des stratégies de groupe : **Configuration ordinateur > Stratégies > Paramètres du logiciel > Installation de logiciel**. Le package MSI de l'agent a été placé sur un partage réseau accessible (\\172.16.10.1\Partage-Marseille2) et configuré avec l'état **"Attribué"**. Ainsi, l'agent s'installe silencieusement au démarrage de chaque poste client. *[Insérer ici ta capture image_c3c3f0.png]*



Test depuis une VM win11 Client :



4.2 Préparation de l'inventaire : Configuration de l'Agent GLPI via GPO

La distribution du logiciel GLPI Agent étant assurée par une Stratégie de Groupe (GPO), il était nécessaire de configurer ce dernier pour qu'il sache où envoyer ses données d'inventaire. J'ai donc utilisé cette même GPO pour injecter les paramètres directement dans le Registre Windows des postes clients.

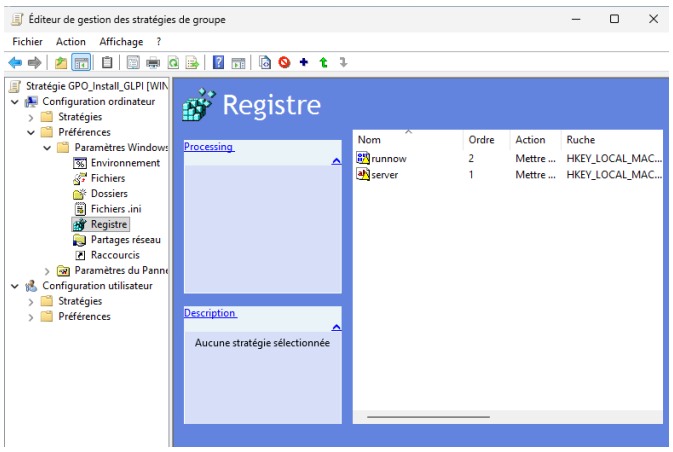
A. Configuration de l'adresse du serveur Dans l'éditeur de gestion des stratégies de groupe, Clic droit > Modifier (sur la gpo) > j'ai navigué vers : Configuration ordinateur > Préférences > Paramètres Windows > Registre J'ai créé un nouvel élément de registre avec les paramètres suivants : **Clic droit** dans la zone blanche à droite > Nouveau **> Élément Registre**.

- **Action :** Mettre à jour (Update). C'est l'option la plus pertinente : si la clé n'existe pas (nouvelle installation), Windows la crée. Si elle existe déjà (changement d'IP du serveur), Windows met simplement à jour la valeur.

- **Ruche :** HKEY_LOCAL_MACHINE. Cette ruche stocke les paramètres qui s'appliquent à l'ordinateur entier, peu importe l'utilisateur connecté. L'Agent GLPI étant un service fonctionnant en arrière-plan, il doit lire sa configuration au niveau de la machine.
- **Chemin de la clé :** SOFTWARE\GLPI-Agent
- **Nom de la valeur :** server (Mot-clé attendu par l'agent).
- **Type de valeur :** REG_SZ (Chaîne de caractères).
- **Données de la valeur :** http://172.16.10.10/glpi/ (L'URL du futur serveur GLPI).

B. Exécution immédiate de l'inventaire J'ai ensuite ajouté un second élément de registre de la même manière pour forcer le scan dès l'installation, sans attendre le délai aléatoire par défaut :

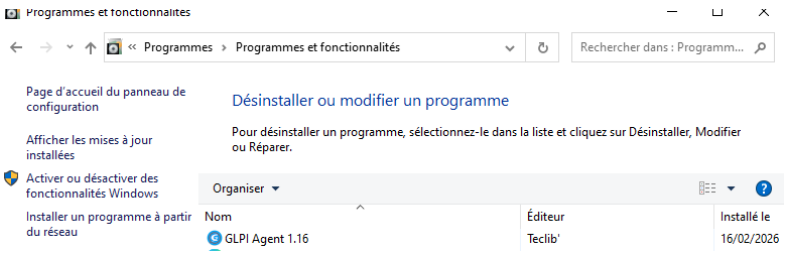
- **Action :** Mettre à jour
- **Ruche :** HKEY_LOCAL_MACHINE
- **Chemin de la clé :** SOFTWARE\GLPI-Agent
- **Nom de la valeur :** runnow (Interrupteur ordonnant un scan immédiat).
- **Type de valeur :** REG_DWORD (Valeur numérique).
- **Données de la valeur :** 1 (en Décimal).



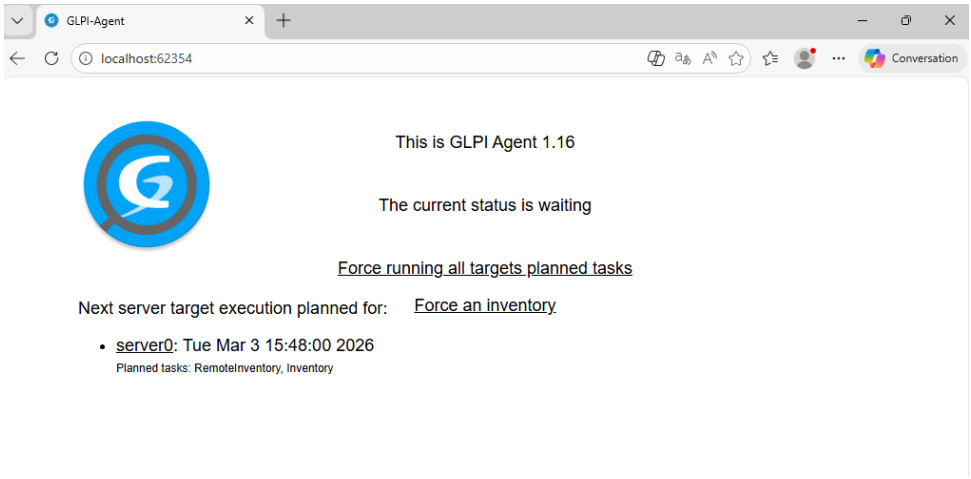
C. Validation sur le poste client

<u>Test sur la VM Client W11 :</u>

Programme présent :

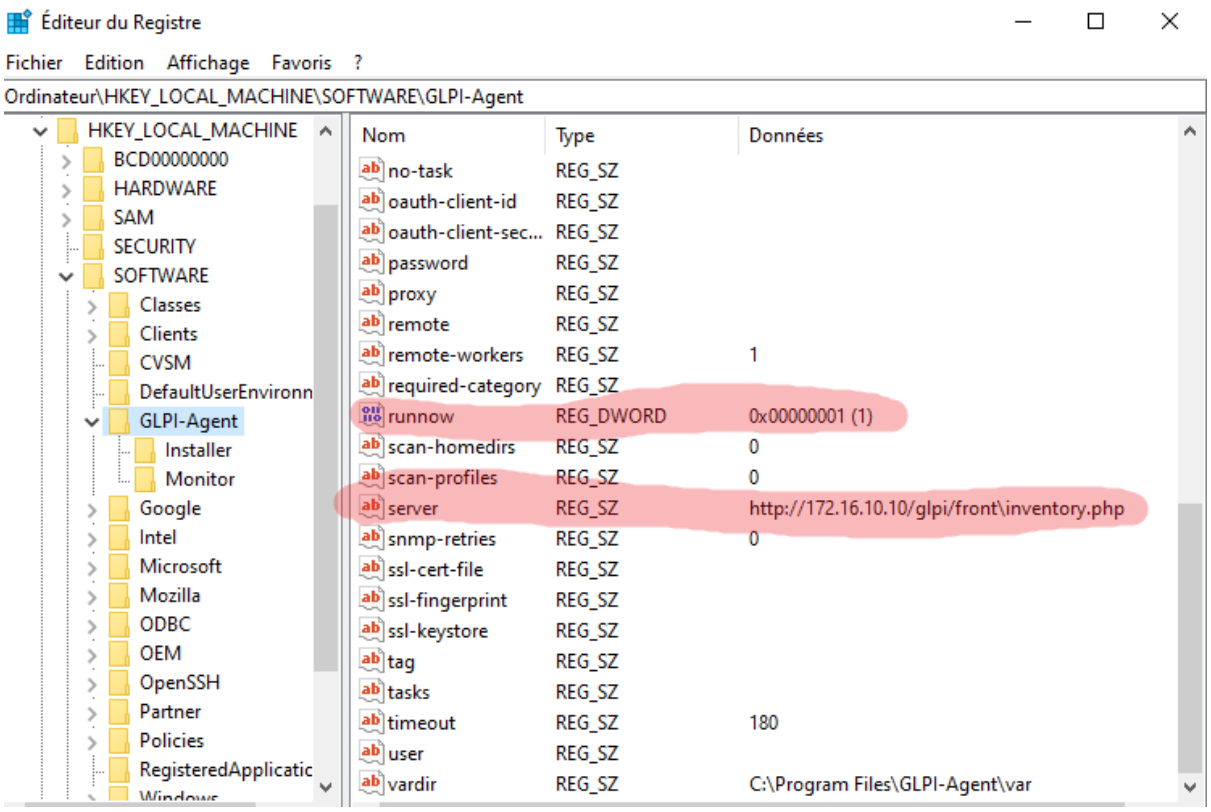


Agent GLPI accessible depuis l'url :



Pour m'assurer de la bonne application de la stratégie, j'ai démarré le poste client **Windows 11**. Après l'ouverture de session, j'ai lancé l'éditeur de registre (regedit) et navigué jusqu'au chemin HKEY_LOCAL_MACHINE\SOFTWARE\GLPI-Agent.

Résultat : Les clés server et runnow sont bien présentes et correctement renseignées, prouvant que le poste est prêt à contacter le serveur dès que celui-ci sera en ligne.



4.2 Mise en place serveur GLPI

A. Préparation serveur Ubuntu et Pile LAMP

Après avoir configuré une machine virtuelle sous **Ubuntu Server** avec l'adresse IP statique 172.16.10.10, j'ai pris la main à distance sur ce serveur via une connexion **SSH** établie depuis ma machine Windows Server.

Une fois installé et configuré je me connecte en ssh depuis ma vm windows server :

Et je lance ceci :

Bash
```
sudo apt update && sudo apt upgrade -y
(mise à jour)
```

Une fois que la première commande a terminé, on installe le serveur web (Apache), la base de données (MariaDB) et le langage de programmation de GLPI (PHP) avec toutes ses extensions obligatoires :

```
sudo apt install -y apache2 mariadb-server php php-cli php-mysql php-xml php-curl php-gd php-mbstring php-intl php-bz2 php-zip php-ldap php-apcu
```

- **Apache2** : Le serveur web qui va afficher les pages de GLPI sur les navigateurs de tes utilisateurs.
- **MariaDB** : Le moteur de base de données qui va stocker tous les tickets et l'inventaire de tes PC.
- **PHP** : Le langage dans lequel GLPI est codé, avec ses "extensions" (xml, curl, gd...) qui permettent à GLPI de générer des graphiques, de lire des fichiers, etc

B. Configuration de la base de données

```
sudo mysql

CREATE DATABASE glpidb;

CREATE USER 'glpiuser'@'localhost' IDENTIFIED BY 'Azerty123!';

GRANT ALL PRIVILEGES ON glpidb.* TO 'glpiuser'@'localhost';

FLUSH PRIVILEGES;

EXIT;
```

```
No VM guests are running outdated hypervisor (qemu) binaries on this host.
admin-mars@srv-mars-glpi:~$ sudo mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.14-MariaDB-0ubuntu0.24.04.1 Ubuntu 24.04

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)]> CREATE DATABASE glpidb;
Query OK, 1 row affected (0,001 sec)

MariaDB [(none)]> CREATE USER 'glpiuser'@'localhost' IDENTIFIED BY 'Azerty123!';
Query OK, 0 rows affected (0,004 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON glpidb.* TO 'glpiuser'@'localhost';
Query OK, 0 rows affected (0,004 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,002 sec)

MariaDB [(none)]> EXIT;
```

C. Installation GLPI:

Téléchargement et mise en place :

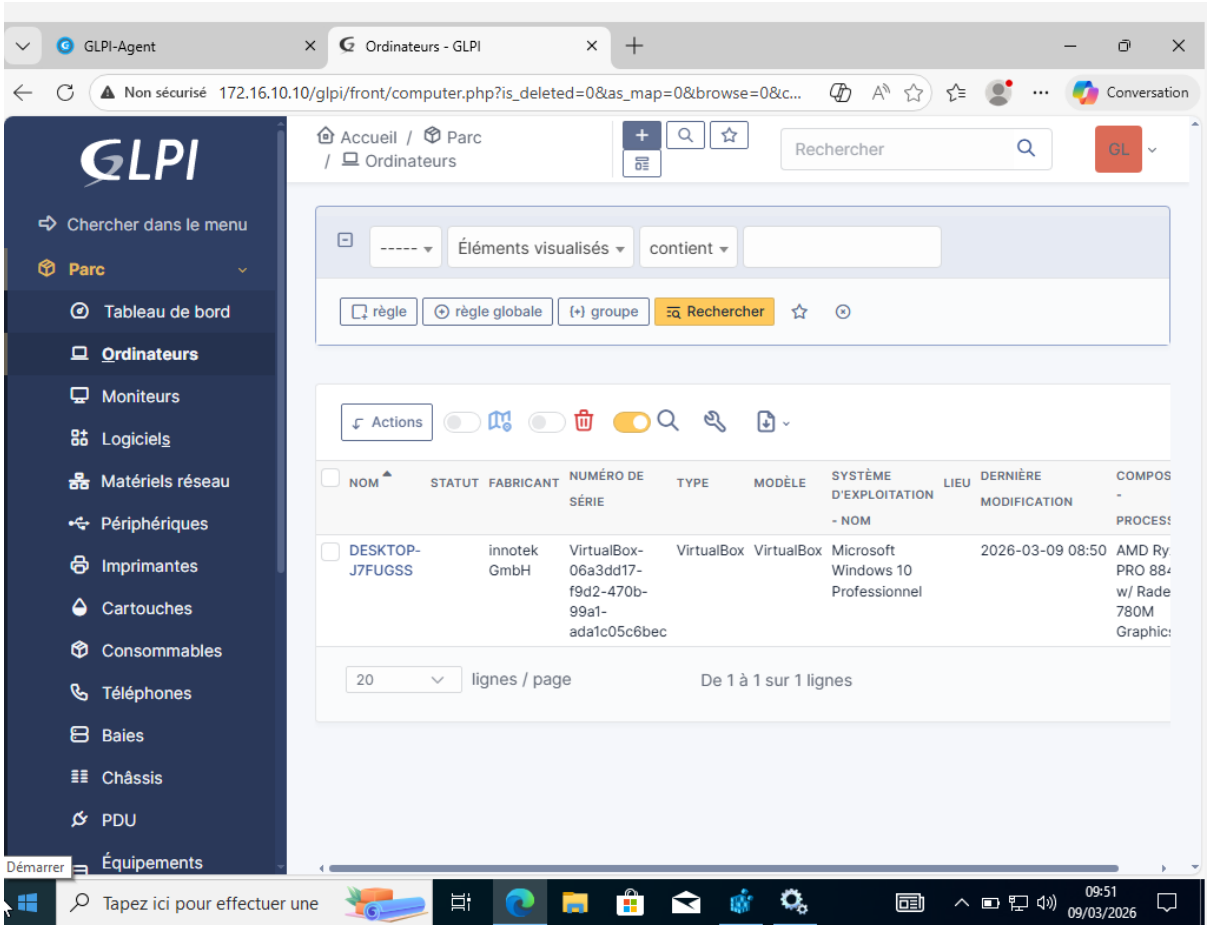
```
cd /tmp && wget https://github.com/glpi-
project/glpi/releases/download/10.0.23/glpi-10.0.23.tgz

tar -xzf glpi-10.0.23.tgz

sudo mv glpi /var/www/html/
```

Attribution des permissions : J'ai octroyé les droits d'écriture au service web (www-data) sur le dossier d'installation, une étape indispensable pour permettre la réception des fichiers XML envoyés par les agents d'inventaire :

```
sudo chown -R www-data:www-data /var/www/html/glpi &&

sudo chmod -R 755 /var/www/html/glpi
```

Configuration graphique : L’installation s’est achevée depuis un navigateur :

L'URL http://172.16.10.10/glpi. La liaison avec la base de données s'est faite avec succès en utilisant les identifiants glpiuser / Azerty123!. J'ai par la suite activé les modules d'inventaire natifs dans l'interface d'administration.



Le PC remonte bien dans l'inventaire du GLPI

Erreur rencontrée :

- **Correction de l'URL de communication :**
  - Détection d'une erreur **404 Not Found** due à un caractère spécial (%5C) dans l'URL.
  - Modification de la base de registre Windows (`Regedit`) dans `HKEY_LOCAL_MACHINE\SOFTWARE\GLPI-Agent` (ou `WOW6432Node`).
  - Remplacement de l'anti-slash (`\`) par un slash (`/`) pour obtenir l'URL correcte : `http://172.16.10.10/glpi/front/inventory.php`.
- **Tests de connectivité :** Validation de la communication via des commandes `ping` et via l'interface locale de l'agent (`http://localhost:62354`).
- **Forçage de l'inventaire :** Utilisation de la commande "Force Inventory" pour déclencher la remontée immédiate des données matérielles et logicielles vers le serveur.

4. Résultat final

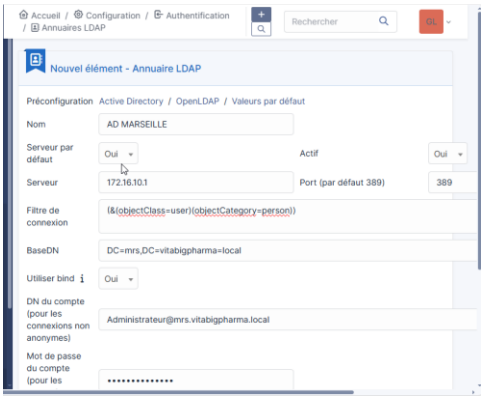
- **Validation :** L'ordinateur Windows 11 apparaît désormais correctement dans le menu **Parc > Ordinateurs** de GLPI.
- **Données collectées :** Remontée automatique des informations système (processeur, RAM, disques, logiciels installés, etc.).

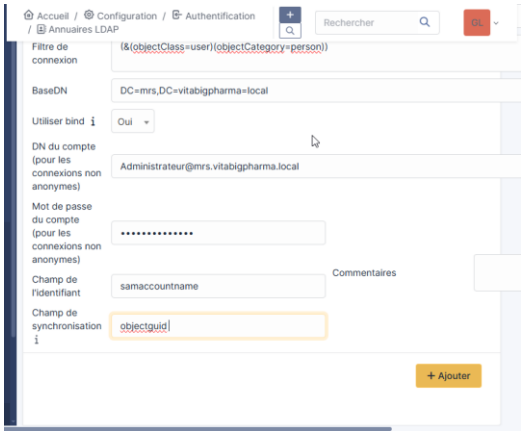
4.4 Démarche d'intégration de l'annuaire (LDAP) et Analyse technique

Afin d'optimiser l'expérience des utilisateurs de **VitaBigPharma** et de centraliser la gestion des mots de passe, j'ai entrepris de lier le serveur GLPI au contrôleur de domaine Windows Server via le protocole **LDAP** (Lightweight Directory Access Protocol). L'objectif était de permettre une authentification unique (SSO).

A. Configuration initiale Le prérequis technique ayant été validé lors de l'installation du serveur web (présence du module php-ldap), j'ai paramétré la liaison dans l'interface de GLPI :

- **Serveur :** L'adresse IP du contrôleur de domaine (172.16.10.1).
- **Port :** 389 (Port standard LDAP non chiffré).
- **Base DN :** Le chemin de l'annuaire (DC=marseille-lab,DC=local).
- **Root DN (Compte de liaison) :** Un compte administrateur autorisé à lire l'annuaire



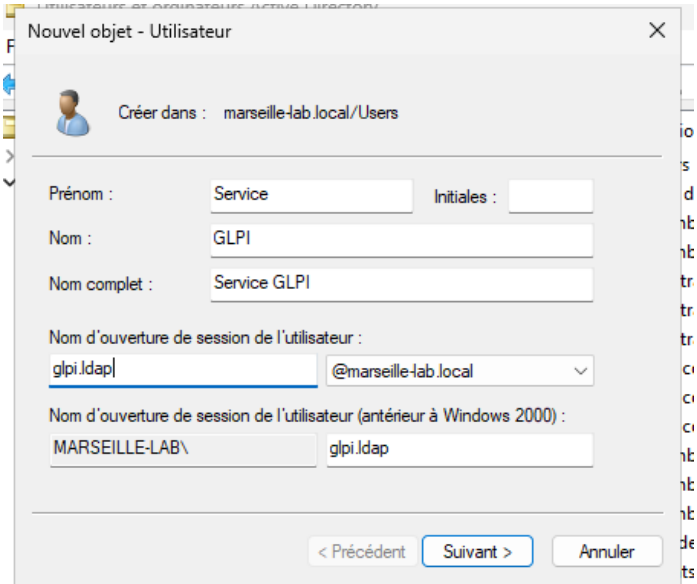


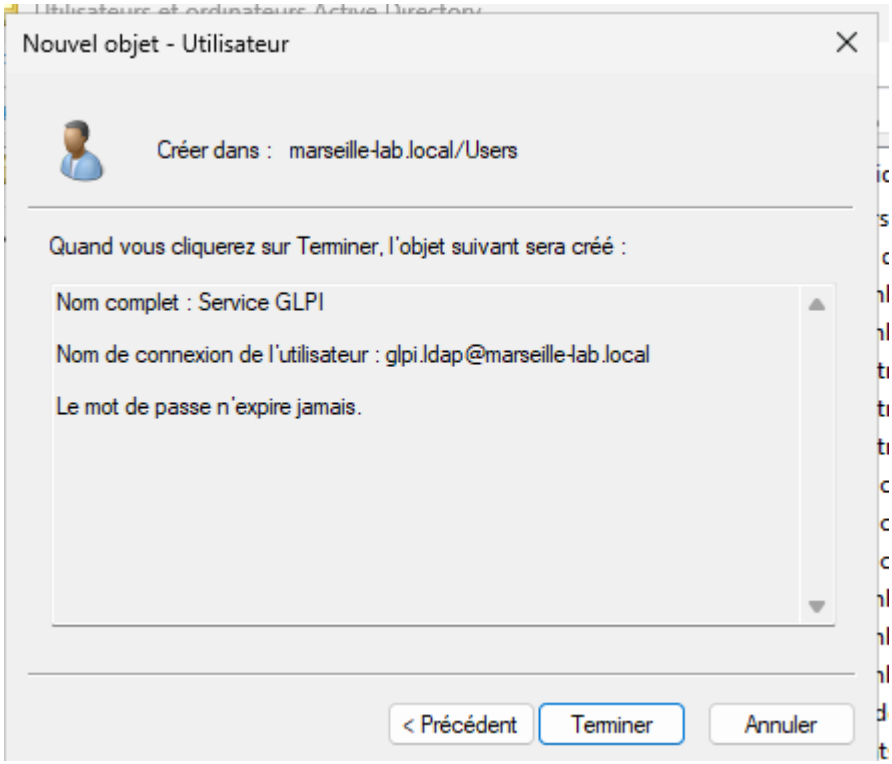
B. Incidents rencontrés et Démarche de résolution (Troubleshooting) Lors des tests de connexion à l'annuaire, des erreurs de communication et de synchronisation sont apparues. J'ai donc mis en place une démarche de diagnostic rigoureuse, documentée par des captures d'écran :

1. **Vérification syntaxique :** J'ai analysé et modifié à plusieurs reprises la syntaxe du *Base DN* et du *Root DN* pour m'assurer qu'il n'y avait pas d'erreur de formatage (ex: utilisation de l'UPN vs format Distinguished Name complet).

2. **Analyse des flux réseau :** J'ai vérifié que le pare-feu du Windows Server et les règles de routage (pfSense) ne bloquaient pas les requêtes sur le port 389 entre le VLAN Serveurs (Ubuntu) et le VLAN Management (AD).

3. **Test de création d'un nouvel utilisateur mais toujours sans effet**





- **Création d'un compte de service :** `glpi.ldap` dans l'AD.
- **Paramétrage GLPI :** * Hôte : `172.16.10.1` / Port : `389`.
    - BaseDN : `DC=marseille-lab,DC=local`.
    - DN du compte : `glpi.ldap@marseille-lab.local`.
    - Filtre de connexion : `(&(objectClass=user)(objectCategory=person))`.

4. Lors des tests, le message suivant a été identifié via le terminal Ubuntu (`ldapsearch`) :

Erreur : `Strong(er) authentication required (8)` **Code DSID :** `0C09035C`

- **Analyse :** Le serveur Windows refuse les connexions "Simple Bind" (en clair) et exige une signature LDAP ou un chiffrement SSL/TLS pour garantir l'intégrité des données.

J'ai donc ensuite mené toutes les actions ci-dessous une par une pour trouver le blocage :

- **Côté Windows Server (GPO & Registre) :**

- Modification de la stratégie de groupe (**GPO**) : Désactivation de l'exigence de signature de serveur LDAP (*Contrôleur de domaine : exigences de signature de serveur LDAP* positionné sur "Aucun").
- Modification du **Registre Windows** : Passage de la clé `LdapServerIntegrity` à `0` pour forcer l'acceptation des liaisons simples.
- Désactivation du **Pare-feu Windows** pour lever tout blocage réseau.

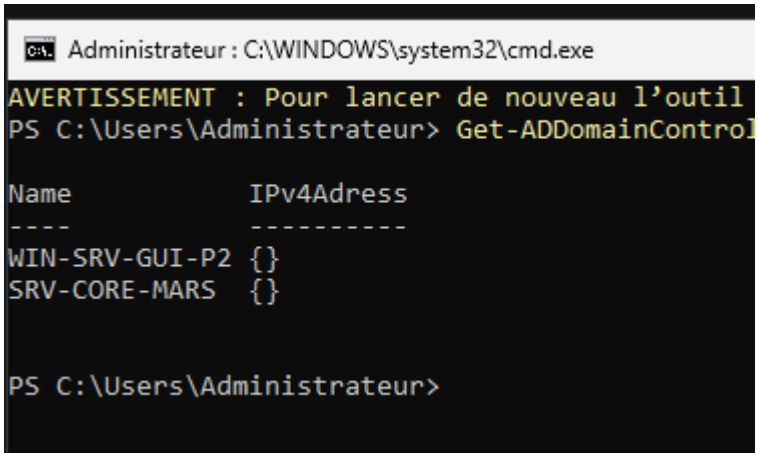
- **Côté Ubuntu (Client LDAP) :**
  - Installation de l'extension PHP : `sudo apt install php-ldap`.
  - Modification du fichier `/etc/ldap/ldap.conf` : Ajout de `TLS_REQCERT never` pour autoriser les connexions vers des serveurs sans certificat vérifié.
  - Activation du mode **Debug** dans GLPI pour tenter d'isoler l'erreur PHP.
- **Variantes de connexion testées :**
  - Utilisation du port **3268** (Catalogue Global) au lieu du 389.
  - Tentative de connexion sécurisée **LDAPS** sur le port **636**.
  - Utilisation du nom **FQDN** (`WIN-SRV-GUI-P2.marseille-lab.local`) à la place de l'IP.

C. Bilan et Perspectives Malgré ces nombreuses investigations et les ajustements réalisés, la liaison LDAP n'a pas pu être finalisée de manière stable dans le temps imparti pour le projet. Cependant, cette étape m'a permis d'approfondir mes connaissances sur la structure complexe d'un annuaire Active Directory et sur le débogage de flux réseau inter-serveurs. La finalisation de cette tâche reste la perspective d'évolution prioritaire pour finaliser le système d'information.

Solution préconisée : Pour une mise en production réelle, l'installation d'une **Autorité de Certification (AD CS)** sur Windows serait nécessaire pour activer le LDAPS (port 636) avec un certificat SSL valide, seule méthode acceptée par le serveur pour lever l'erreur de "Stronger Authentication".

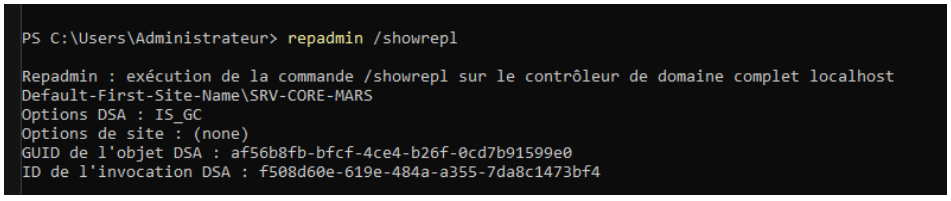
Phase de contrôle : Validation de la Haute Disponibilité (Active Directory)

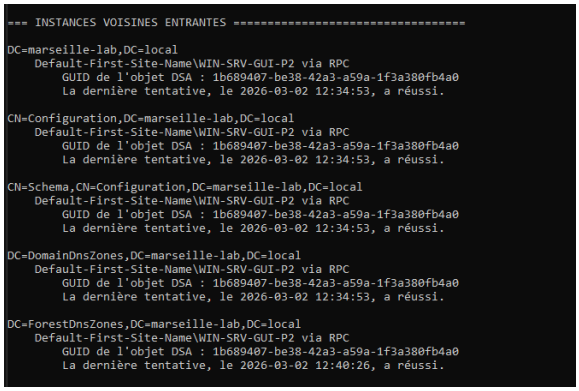
1. **Vérification de la topologie du domaine** Depuis une invite de commande PowerShell avec élévation de privilèges, j'ai interrogé l'annuaire pour lister les contrôleurs reconnus par le domaine.



Le retour de la commande confirme que le serveur principal (WIN-SRV-GUI-P2) et le serveur Core (SRV-CORE-MARS) sont tous deux parfaitement enregistrés en tant que contrôleurs légitimes de la forêt.

2. Validation de la réplication inter-serveurs Avoir deux serveurs ne suffit pas, ils doivent partager la même base de données. J'ai donc exécuté l'utilitaire de diagnostic de réplication : repadmin /showrepl.





Bilan : Cette vérification me garantit que si le serveur principal de Marseille venait à tomber en panne, le serveur Core prendrait immédiatement le relais pour l'authentification des utilisateurs et la résolution DNS, assurant ainsi la continuité d'activité pour VitaBigPharma.

5. Sauvegarde et Sécurisation des données

L'objectif de cette étape est de sécuriser les données critiques du serveur de fichiers Windows (site de Marseille) en effectuant une sauvegarde déportée. Pour des raisons de performance et de sécurité, j'ai choisi de déployer un serveur sous Linux.

5.1 Déploiement du serveur de sauvegarde (Debian Core) Connexion au serveur windows :

J'ai installé une machine virtuelle sous **Debian "Headless"** (sans interface graphique). Ce choix technique présente un double avantage : la réduction de l'empreinte matérielle (économie de RAM et CPU) et la diminution de la surface d'attaque du serveur.

- **Configuration réseau :** Le serveur a reçu une adresse IP statique (172.16.10.20) configurée sur son interface réseau (enp0s3 via le fichier /etc/network/interfaces) pour garantir sa joignabilité permanente sur le réseau interne.

5.2 Interopérabilité Windows/Linux (Protocole CIFS)

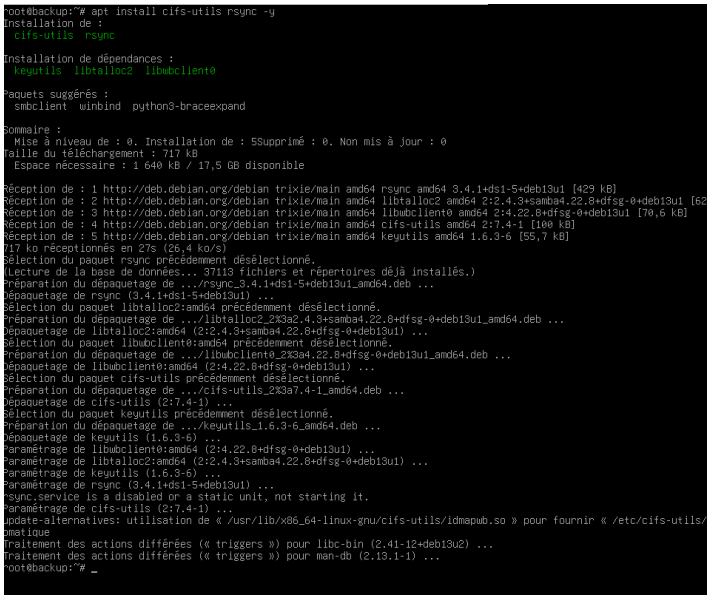
```
mount -t cifs //172.16.10.1/Partage-Marseille /mnt/partage_windows -o
username=Administrateur
```

Mount = lier les deux

Cifs = protocole de windows pour le partage de fichiers

172.16.10.1 = WS

Validation : Cette commande confirme que le réseau interne fonctionne, que Linux communique avec l'Active Directory, et que le partage de fichiers est opérationnel.



- Le réseau interne fonctionne.
- Le Linux communique avec l'AD.
- Le partage de fichiers est opérationnel.

5.3 Scripting et Automatisation (Bash & Rsync)

Pour éviter de lancer les sauvegardes manuellement, j'ai développé un script Bash automatisé s'appuyant sur l'outil de synchronisation **rsync**. L'avantage de rsync est qu'il effectue une sauvegarde incrémentielle : il ne copie que les blocs de données modifiés depuis la dernière exécution, ce qui réduit considérablement la charge réseau.

Contenu du script (/root/backup.sh) :

“

```
#!/bin/bash
```

```
# Configuration

SOURCE="/mnt/partage_windows/"

DESTINATION="/backup/marseille/"

LOG="/var/log/backup.log"

DATE=$(date "+%Y-%m-%d %H:%M:%S")


echo "--- Début de la sauvegarde : $DATE ---" >> $LOG


# Synchronisation avec rsync

# -a : archive (garde les droits)

# -v : bavard (écrit ce qu'il fait)

# --delete : efface sur Linux ce qui a été supprimé sur Windows

rsync -av --delete $SOURCE $DESTINATION >> $LOG 2>&1


echo "--- Sauvegarde terminée ---" >> $LOG
```

“

J'ai ensuite rendu ce script exécutable via la commande :

```
chmod +x /root/backup.sh
```

Chmod = modifier les droits d’un fichier

+x = transformer le texte en fichier executable

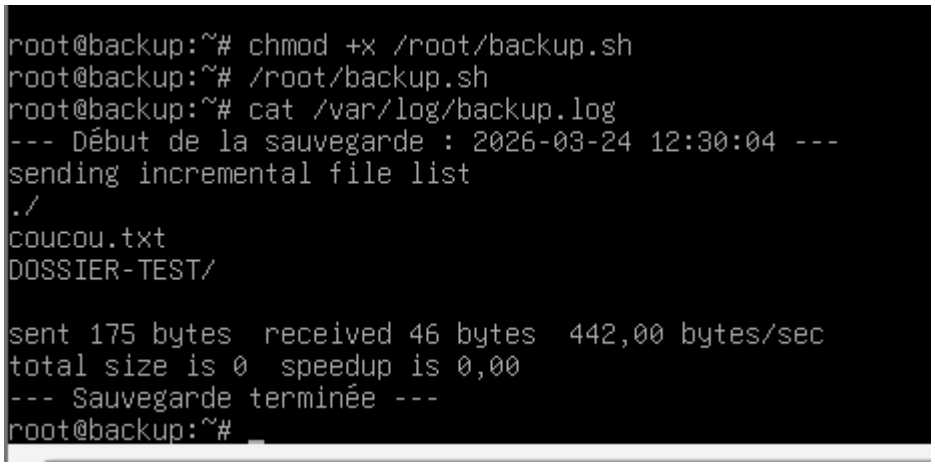
Ce qui permet au système de l'exécuter comme un programme à part entière.

Et je peux lancer la sauvegarde manuelle avec celle-ci :

```
/root/backup.sh
```

Après le lancement de sauvegarde : je vérifie si cela fonctionne bien avec

```
cat /var/log/backup.log
```

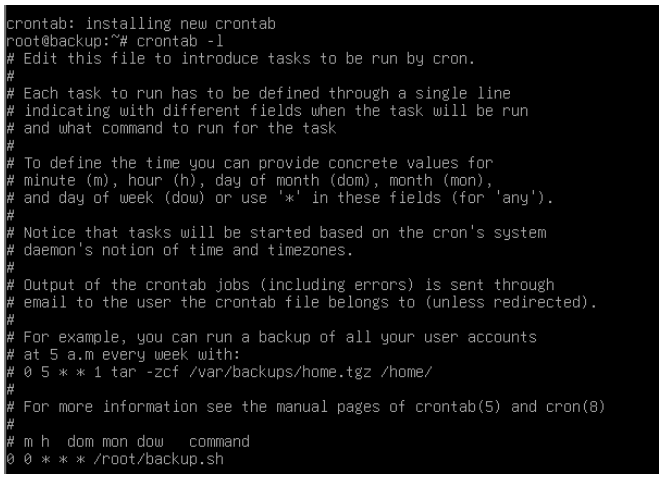


- **L'outil :** `rsync`, qui est la référence pour la sauvegarde incrémentielle (il ne copie que ce qui a changé, donc c'est très rapide).
- **La sécurité :** utilisation d'un serveur Linux sans interface graphique = réduction des ressources nécessaires (RAM/CPU) et la surface d'attaque.
- **L'automatisation :** Grâce à `cron`, la sauvegarde se fait toute seule sans intervention humaine.

5.4 Planification et Supervision (Cron)

Pour finaliser l'automatisation, j'ai planifié l'exécution de ce script de manière autonome en l'ajoutant aux tâches planifiées du système via la commande `crontab -e`. J'ai ajouté la ligne suivante pour déclencher la sauvegarde quotidiennement à minuit :

```
0 0 * * * /root/backup.sh
```



Chaque jour à minuit la commande backup s'exécutera.

6. Sécurisation de l'infrastructure et Audit

Afin de garantir la protection des données de VitaBigPharma face aux cybermenaces, j'ai mis en place une politique de sécurité réseau stricte, suivie d'un audit de vulnérabilité de l'annuaire central.

6.1 Filtrage des flux réseau (Pare-feu pfSense)

L'objectif sur le réseau LAN de Marseille a été d'appliquer le principe du moindre privilège pour limiter les vecteurs d'attaque latéraux. J'ai configuré les règles de pare-feu sur l'interface LAN du pfSense, traitées dans cet ordre de priorité (de haut en bas) :

1. Autorisation du flux de sauvegarde (SMB / CIFS) :
    - Action : PASS
    - Source : 172.16.10.20 (Serveur Backup Debian)
    - Destination : 172.16.10.1 (Serveur de fichiers AD)
    - Port : TCP 445 (MS-DS)
    - Justification : Cette règle autorise exclusivement le serveur de sauvegarde Linux à venir lire les données du serveur Windows. Tout autre poste tentant d'utiliser ce port de manière illégitime sera soumis aux règles inférieures.

2. **Restriction du protocole ICMP (Ping) :**

- **Action :** BLOCK
- **Source :** LAN Subnets
- **Destination :** ANY
- **Justification :** Le blocage des requêtes ICMP permet de dissimuler la topologie du réseau interne. Cela ralentit considérablement la phase de reconnaissance d'un attaquant potentiel (scans réseau) depuis une machine compromise.

3. **Règle par défaut (Default Allow) :**

- Maintien d'une règle d'autorisation générale pour les autres services non critiques, positionnée en bas de liste pour que les règles de blocage spécifiques soient traitées en priorité.

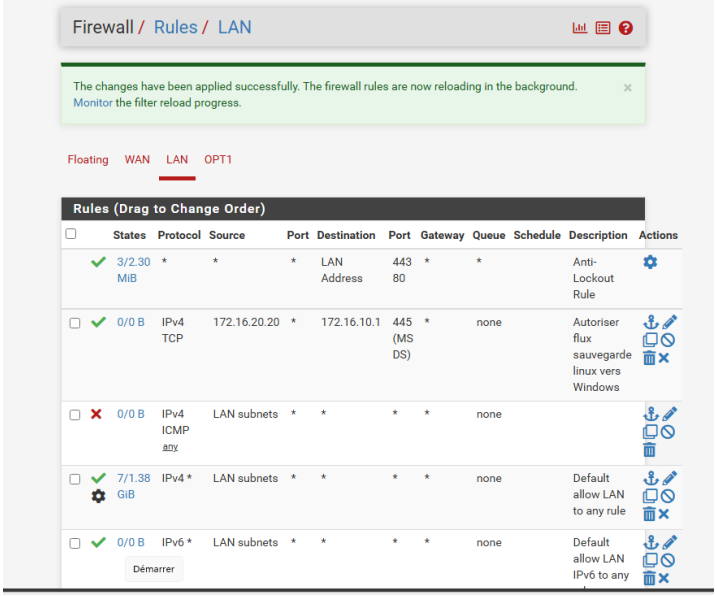
Objectif

Appliquer le principe du **moindre privilège** sur le réseau LAN de Marseille pour limiter les vecteurs d'attaque.

Configuration du filtrage (Firewall Rules)

J'ai configuré les règles sur l'interface LAN du pfSense dans cet ordre de priorité :

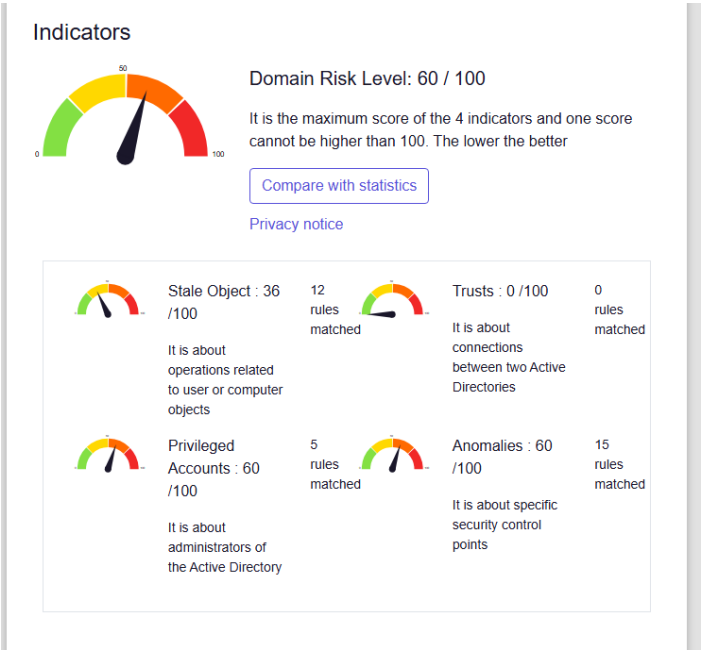
1. **Autorisation du flux de sauvegarde (SMB)** :
    a. **Action** : PASS
    b. **Source** : `172.16.10.20` (Serveur Backup)
    c. **Destination** : `172.16.10.1` (Serveur AD/Fichiers)
    d. **Port** : TCP 445 (MS-DS)
    e. *Justification* : Ce flux est indispensable au bon fonctionnement du script de sauvegarde.
2. **Restriction du protocole ICMP (Ping)** :
    a. **Action** : BLOCK
    b. **Source** : LAN Subnets
    c. **Destination** : ANY
    d. *Justification* : Interdire le ping vers l'extérieur permet de dissimuler les machines du réseau interne lors de tentatives de scan ou de reconnaissance depuis le WAN.
3. **Règle par défaut (Default Allow)** :
    a. Maintien de l'accès général pour les autres services, tout en sachant que les règles précédentes (plus spécifiques) sont traitées en priorité.



6.2 Audit de sécurité Active Directory (PingCastle)

La compromission de l'Active Directory équivalant à la compromission totale de l'entreprise, j'ai réalisé un audit de sécurité automatisé à l'aide de l'outil de référence **PingCastle**.

A. Analyse du rapport d'audit Le scan initial a révélé un niveau de risque global ("Domain Risk Level") évalué à **60 / 100**.



Ce score s'explique principalement par les configurations de rétrocompatibilité activées par défaut sous Windows Server, qui ne répondent plus aux standards de sécurité modernes.

B. Remédiations et Plan d'action Face à ce constat, j'ai adopté une démarche de "Hardening" (durcissement) en ciblant les vulnérabilités par ordre de criticité :

1. **Correction immédiate (Privileged Accounts) :** La faille la plus critique remontée par le rapport concernait mon compte Administrateur (mots de passe, stratégies de verrouillage). J'ai immédiatement appliqué des mesures correctives pour verrouiller cet accès à hauts privilèges.

2. **Plan de remédiation (Anomalies) :** L'indicateur d'anomalies à 60/100 souligne la présence de protocoles obsolètes et vulnérables, tels que **SMBv1** ou la résolution de noms **LLMNR**. N'ayant pas pu tous les corriger dans le temps imparti, j'ai prévu une phase de durcissement ultérieure. Ces protocoles devront être désactivés globalement sur le parc à l'aide de nouvelles Stratégies de Groupe (GPO).

7. Supervision de l'infrastructure (Prometheus)

Afin d'anticiper les pannes et de surveiller l'état de santé du système d'information, j'ai mis en place une solution de supervision basée sur Prometheus.

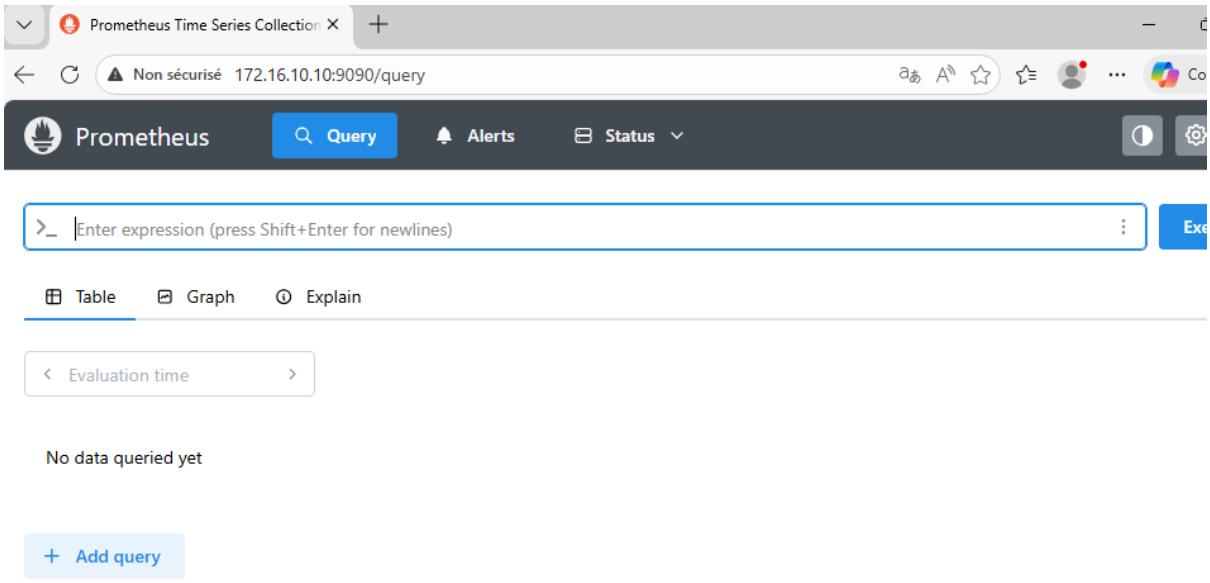
Pour héberger ce service, j'ai choisi de réutiliser la machine virtuelle Linux (Ubuntu) hébergeant déjà GLPI. Ce choix technique se justifie par trois critères :

- Optimisation des ressources : Éviter la création d'une machine virtuelle supplémentaire permet d'économiser la mémoire RAM et les ressources CPU de l'hyperviseur.
- Centralisation : Le serveur Linux devient la véritable "Tour de contrôle" du site de Marseille, gérant à la fois l'inventaire matériel (GLPI) et la surveillance en temps réel.
- Stabilité : Prometheus, étant développé pour des environnements UNIX, s'exécute nativement avec de meilleures performances sous Linux.

7.1 Préparation de l'environnement (Docker et Node Exporter)

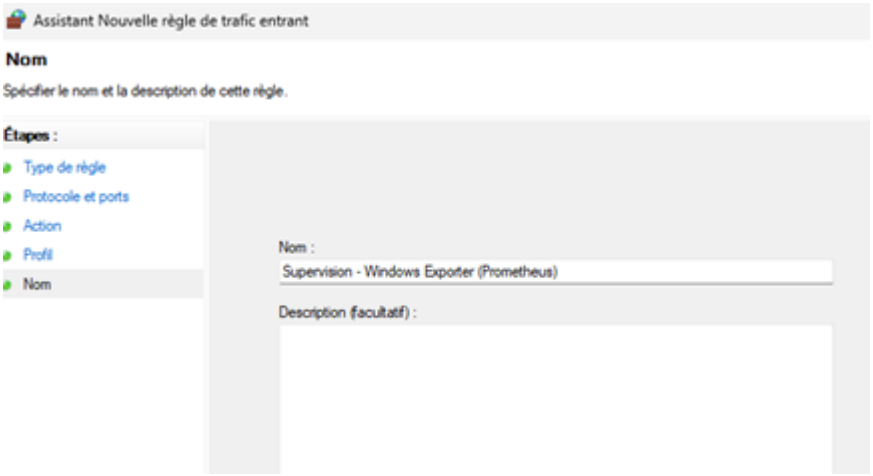
L'installation de Prometheus a été réalisée via la technologie de conteneurisation **Docker**, permettant d'isoler l'application du reste du serveur (GLPI).

```
sudo apt update

sudo apt install docker.io -y

sudo systemctl enable --now docker
```



Pour que Prometheus puisse surveiller le serveur Linux lui-même (consommation CPU, RAM, espace disque), j'ai installé l'agent **Node Exporter** (qui écoute sur le port 9100) :

```
sudo apt install prometheus-node-exporter -y

sudo systemctl enable --now prometheus-node-exporter
```

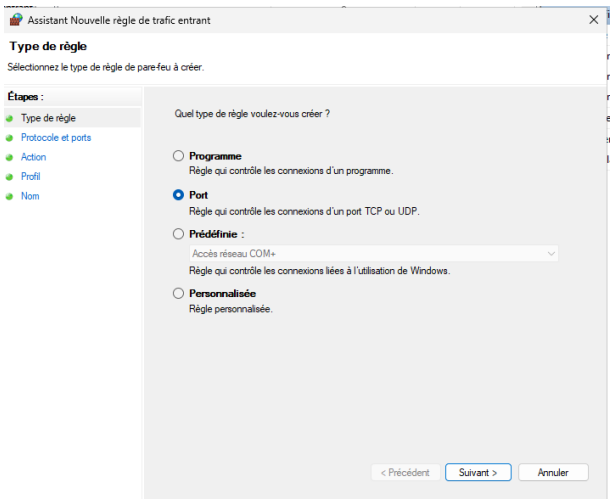


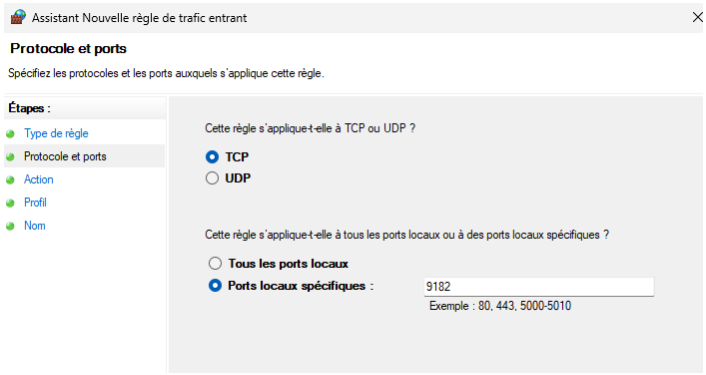
7.2 Déploiement de l'agent sur Windows Server

Afin de remonter les métriques du contrôleur de domaine (Active Directory), j'ai dû installer un agent spécifique pour l'environnement Microsoft.

1. **Téléchargement et Installation :** Je me suis rendu sur le dépôt GitHub officiel de la communauté Prometheus (https://github.com/prometheus-community/windows_exporter/releases) pour télécharger la dernière version de l'utilitaire **Windows Exporter** au format .msi. J'ai ensuite exécuté cet installateur sur le serveur 172.16.10.1. Cet agent traduit les données du serveur Windows pour qu'elles soient compréhensibles par Prometheus.

2. **Ouverture des flux :** Pour permettre à Prometheus de venir interroger cet agent, j'ai créé une nouvelle règle de trafic entrant dans le **Pare-feu Windows Defender** avec une autorisation stricte sur le port TCP **9182**.





7.3 Configuration du serveur Prometheus

Il a ensuite fallu indiquer au serveur Prometheus où se trouvaient les agents à interroger. J'ai créé un dossier de configuration (mkdir -p ~/prometheus_config) et édité le fichier de configuration principal prometheus.yml via l'éditeur **Nano** :

```
global:
 scrape_interval: 15s # Fréquence de récupération des données


scrape_configs:
 - job_name: 'Linux_Marseille_GLPI'
  static_configs:
   - targets: ['172.16.10.10:9100'] # IP locale (Node Exporter)


 - job_name: 'Windows_Server_AD'
  static_configs:
   - targets: ['172.16.10.1:9182'] # IP du contrôleur de domaine (Windows Exporter)
```

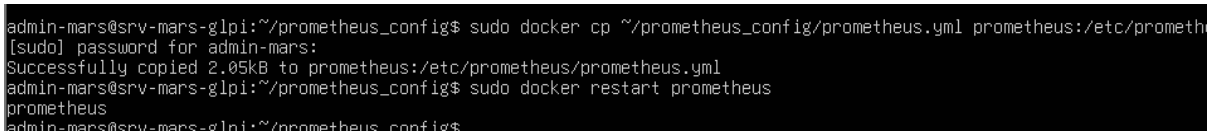
Et je modifie ensuite le fichier .yml : “nano prometheus.yml” grâce à nano je peux créer le fichier et je peux ensuite le modifier.

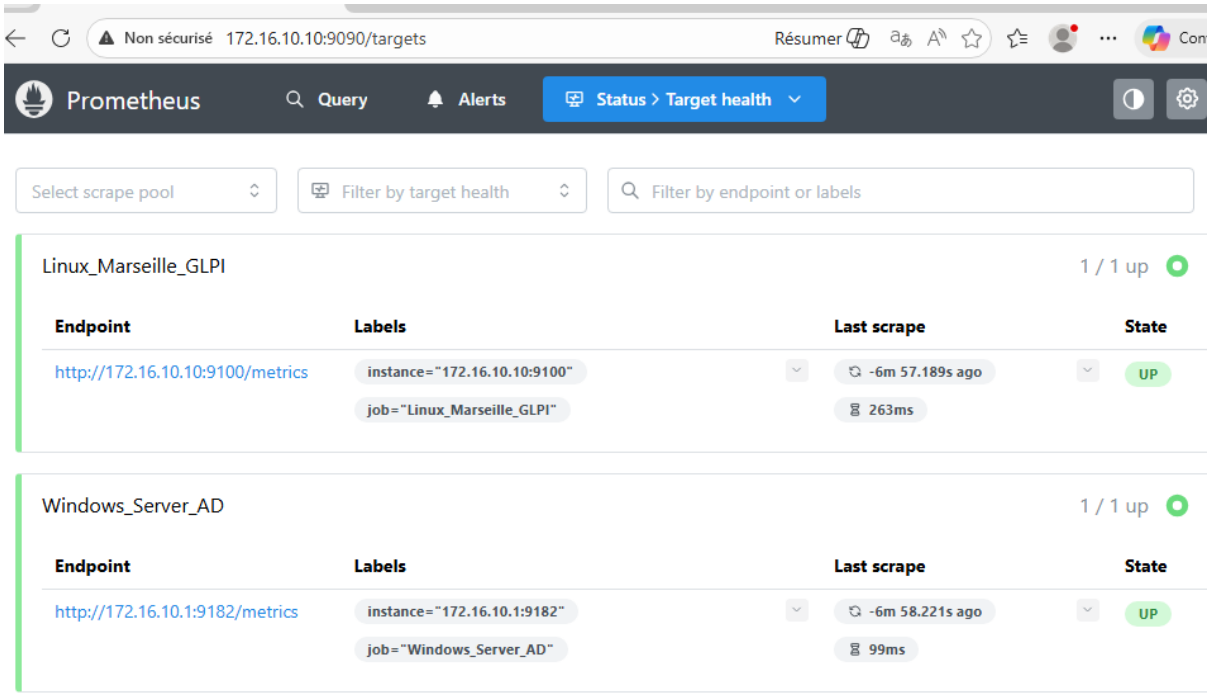
“

```
global:
  scrape_interval: 15s # Fréquence de récupération des données
```

```
scrape_configs:
  - job_name: 'Linux_Marseille_GLPI'
    static_configs:
      - targets: ['172.16.10.10:9100'] # IP locale de l'hôte pour node-exporter


  - job_name: 'Windows_Server_AD'
    static_configs:
      - targets: ['172.16.10.1:9182'] # IP du contrôleur de domaine
```

Je copie ensuite le fichier dans le conteneur et redémarre ensuite prometheus pour que les changements soient appliqués :





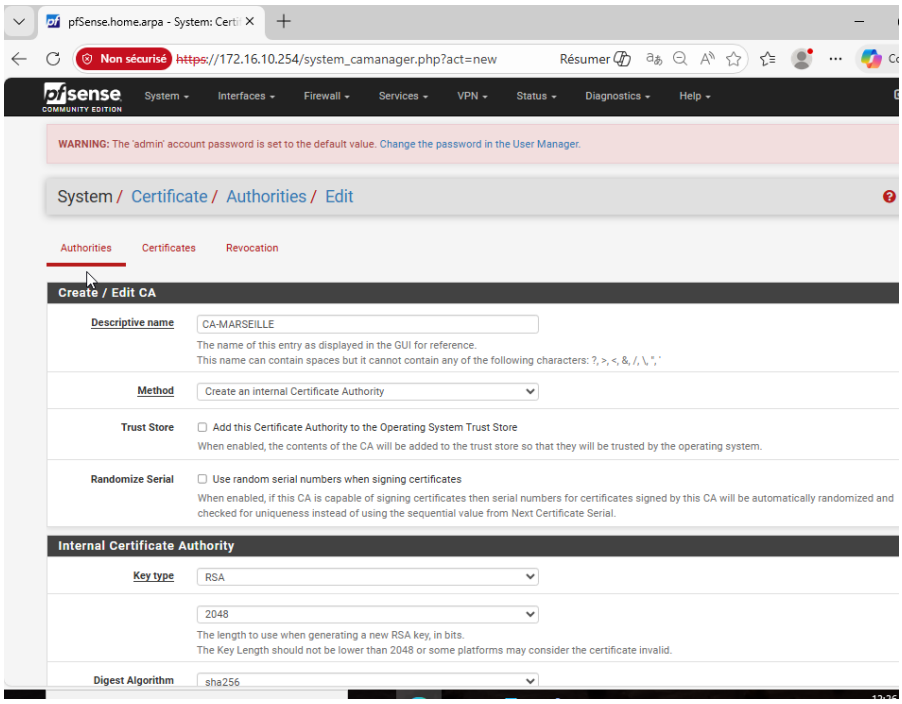
8. Sécurisation des accès distants (VPN Nomade)

Afin de permettre aux collaborateurs de **VitaBigPharma** travaillant en déplacement ou en télétravail d'accéder de manière sécurisée aux ressources internes (Serveur de fichiers, GLPI, Intranet), j'ai mis en place un serveur VPN Nomade (Remote Access) en utilisant le protocole **OpenVPN** intégré au pare-feu pfSense.

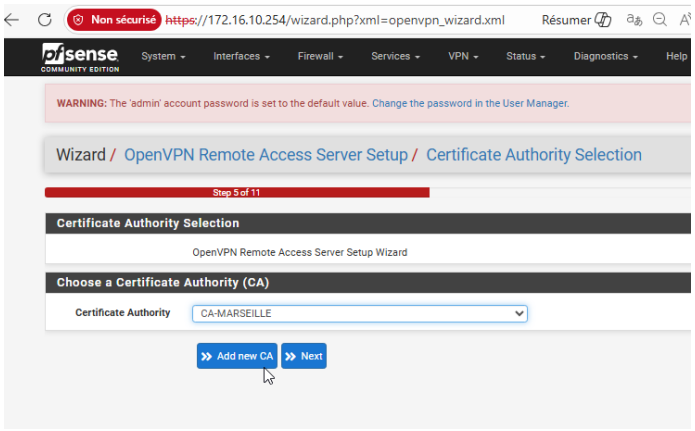
8.1 Infrastructure Cryptographique (PKI)

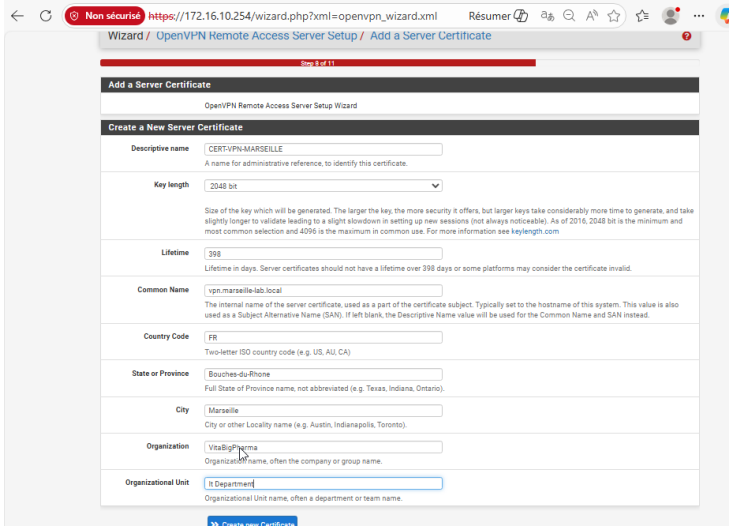
La sécurité d'un VPN repose sur des certificats numériques. Avant de configurer le tunnel, j'ai dû créer une infrastructure à clé publique (PKI) interne :

1. **L'Autorité de Certification (CA) :** Création d'une entité nommée CA-MARSEILLE dans le gestionnaire de certificats de pfSense. Elle sert de tiers de confiance pour signer et valider toutes les connexions.



2. **Le Certificat Serveur :** Génération d'un certificat serveur (CERT-VPN-MARSEILLE) signé par la CA précédente, permettant d'identifier formellement le pare-feu pfSense auprès des clients.



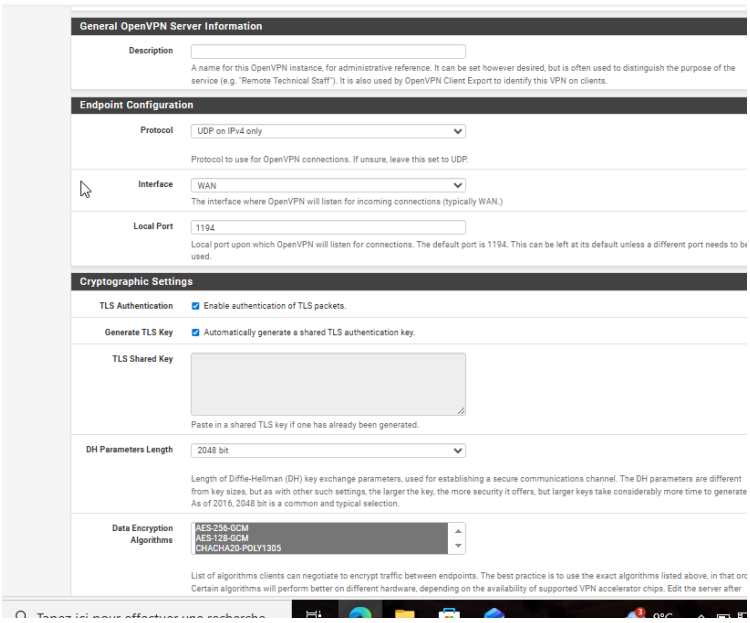


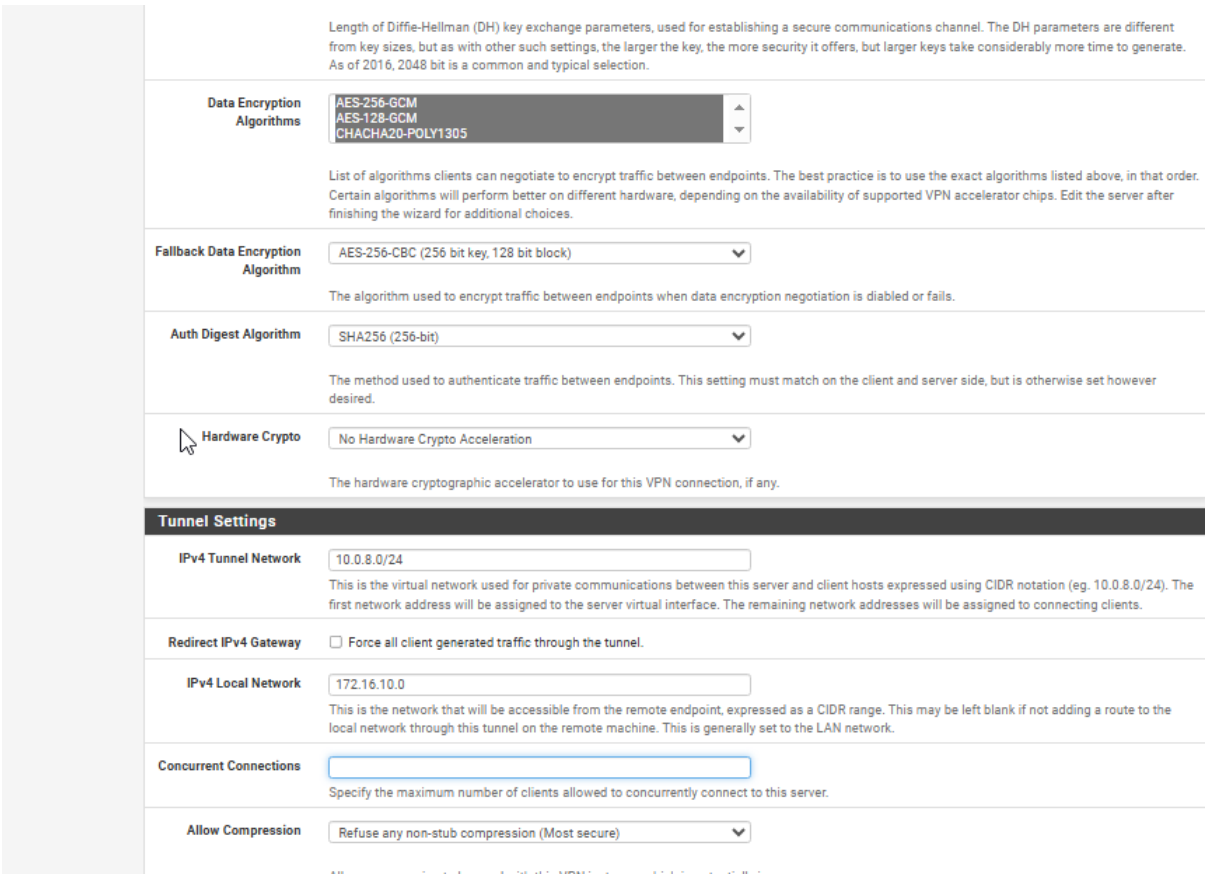
8.2 Configuration du Serveur OpenVPN

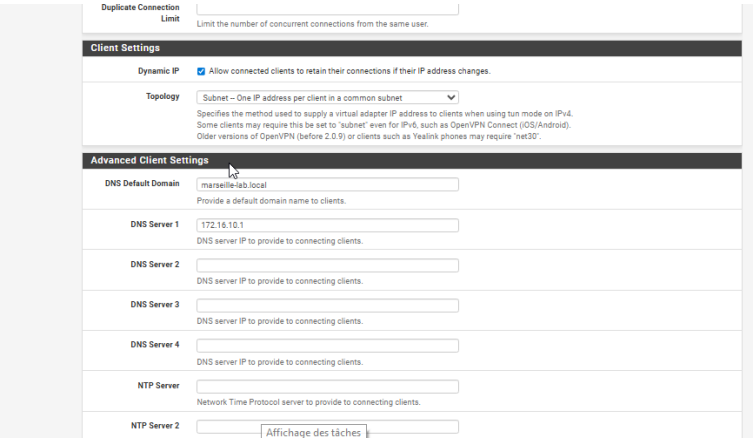
J'ai utilisé l'assistant de configuration (Wizard) pour paramétrer le serveur VPN avec les éléments techniques suivants :

- **Protocole et Interface :** Écoute sur l'interface WAN en utilisant le protocole **UDP** sur le port standard **1194**.
- **Chiffrement :** Utilisation de l'algorithme robuste AES-256-GCM pour garantir la confidentialité des données transitant par le tunnel.
- **Réseau virtuel (Tunnel Network) :** 10.0.8.0/24. C'est la plage d'adresses IP qui sera distribuée virtuellement aux télétravailleurs.
- **Réseau local (Local Network) :** 172.16.10.0/24. J'indique au VPN quel réseau physique il doit rendre accessible aux nomades.

- **Paramètres DNS :** J'ai configuré le serveur VPN pour qu'il pousse l'adresse IP du contrôleur de domaine (172.16.10.1) et le suffixe DNS (marseille-lab.local) aux clients. C'est une étape cruciale pour que les utilisateurs puissent joindre les serveurs par leur nom et non juste par leur IP.





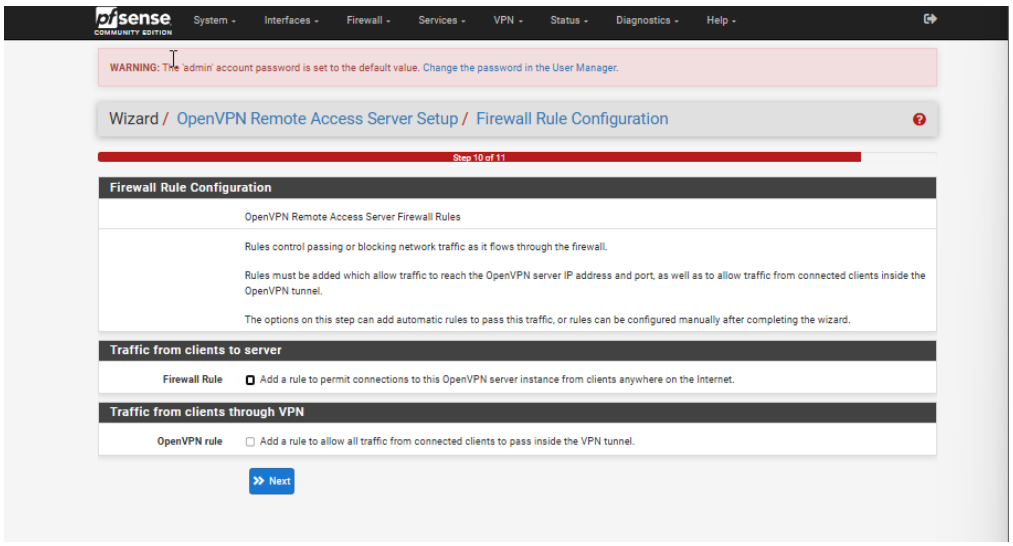


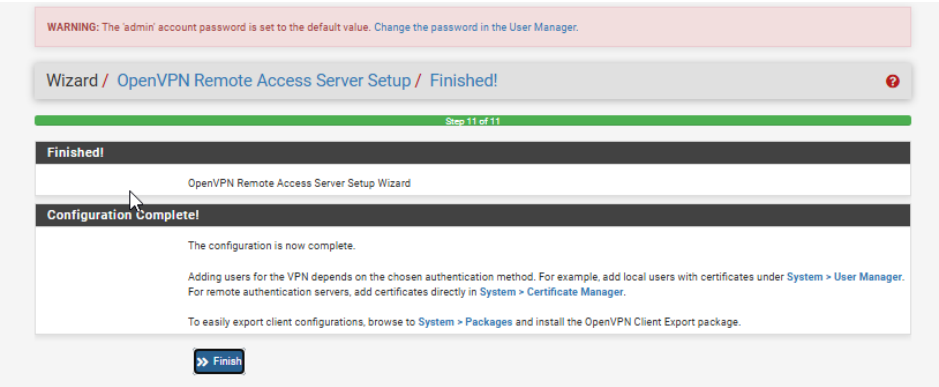
8.3 Automatisation des règles de Pare-feu

Pour que le trafic puisse circuler, j'ai autorisé la création automatique des règles de pare-feu lors de la finalisation de l'assistant (cocher les deux cases) :

1. **Firewall Rule (Traffic from clients to server) :** Création d'une règle sur l'interface WAN autorisant les connexions entrantes depuis Internet sur le port UDP 1194. Sans cette règle, le pare-feu rejetterait les tentatives de connexion VPN.

2. **OpenVPN rule (Traffic from clients through VPN) :** Création d'une règle dans le nouvel onglet "OpenVPN", autorisant les clients virtuels (le réseau 10.0.8.0/24) à circuler vers le LAN de Marseille pour accéder aux services (GLPI, AD, Partages).





8.4 Déploiement et Procédure Utilisateur

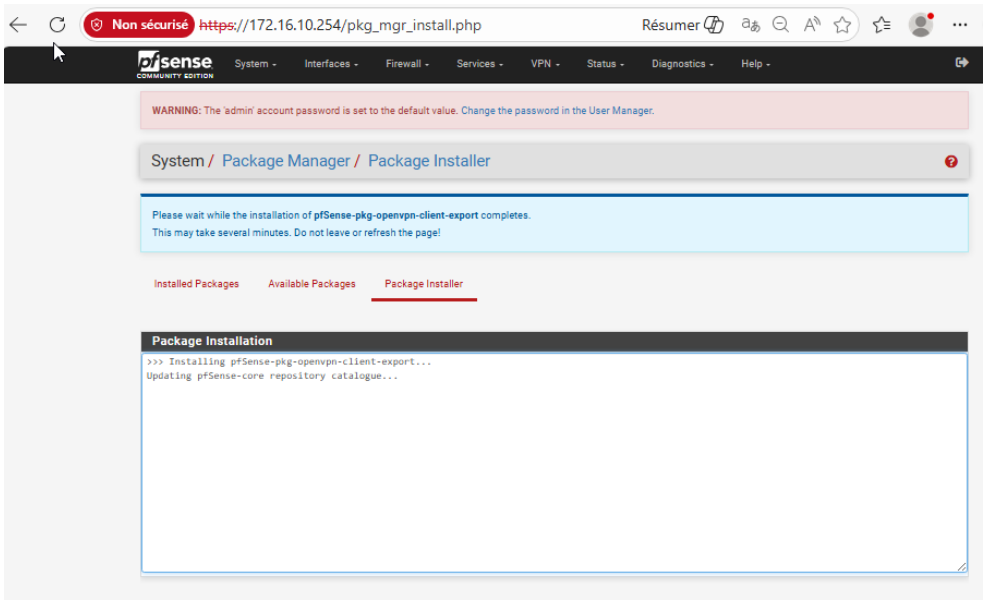
Pour simplifier l'intégration d'un nouveau collaborateur nomade, j'ai installé le paquet additionnel **openvpn-client-export** via le gestionnaire de paquets de pfSense.

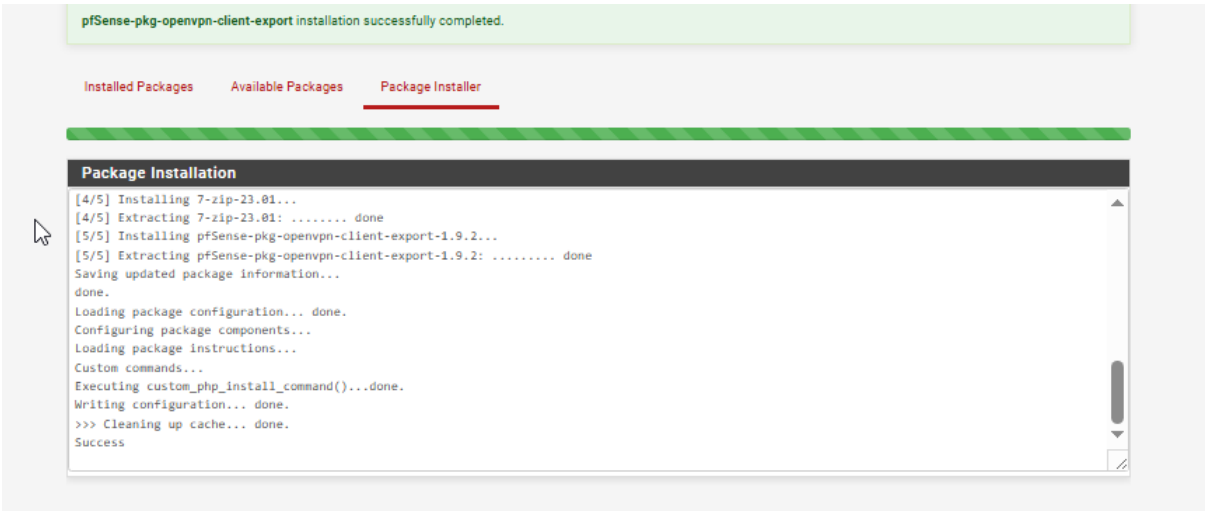
Lorsqu'un utilisateur (ex: *j.dupont* ou *u.nomade*) a besoin d'un accès, la procédure est la suivante :

A. Côté Administration (Création de l'identité) :

1. Création d'un compte utilisateur local dans System > User Manager.
2. Génération automatique d'un certificat personnel ("clé" numérique unique) lié à cet utilisateur et signé par CA-MARSEILLE.
3. Exportation de son profil de connexion préconfiguré depuis VPN > OpenVPN > Client Export (format *.ovpn*).

B. Côté Utilisateur (Le "Kit de connexion") : Je fournis au collaborateur le logiciel client officiel (OpenVPN Connect) ainsi que son fichier .ovpn personnel. L'utilisateur n'a aucune configuration technique à réaliser. Il lui suffit d'importer le fichier dans l'application, de saisir son mot de passe, et son poste se retrouve virtuellement connecté au réseau de l'entreprise, avec un accès complet aux serveurs comme s'il était physiquement au bureau.





Conclusion Générale et Perspectives d'évolution

La conception et le déploiement de l'infrastructure de VitaBigPharma sur le site de Marseille m'ont permis de mettre en œuvre un système d'information complet, hautement disponible et répondant aux exigences strictes d'une entreprise moderne.

Bilan des réalisations :

Au cours de ce projet, j'ai pu valider l'intégration de différents environnements (Windows Server, Ubuntu, Debian) autour de services critiques pour l'entreprise :

- Gestion des identités et du parc : Déploiement d'un annuaire Active Directory redondant couplé à une solution GLPI automatisée par Stratégies de Groupe (GPO).
- Sécurisation des données : Mise en place de règles de quotas (FSRM), d'audits de vulnérabilité (PingCastle) et de sauvegardes déportées automatisées (Rsync/Cron).
- Supervision et Mobilité : Surveillance proactive des ressources via Prometheus et sécurisation du télétravail grâce à un tunnel VPN Nomade (OpenVPN).

À ce jour, le site principal de Marseille est opérationnel, sécurisé, et son architecture a été pensée pour être facilement scalable.

Perspectives d'évolution : L'interconnexion multisite

L'entreprise VitaBigPharma étant en pleine expansion, le prochain grand défi technique concerne la collaboration inter-agences. Si les collaborateurs nomades bénéficient déjà d'un accès sécurisé via le VPN Client-à-Site déployé, la communication directe avec la seconde succursale (le site de Toulouse hébergeant l'ERP) constitue la suite logique du projet.

L'évolution prioritaire serait la mise en place d'un VPN Site-à-Site (via IPsec ou OpenVPN). Cette interconnexion permanente entre les pare-feux pfSense des deux agences permettrait de créer un réseau unifié et transparent. Sur le plan technique, ce tunnel permettrait d'établir une relation d'approbation et une réplication Active Directory entre les deux sites. Les collaborateurs de Toulouse pourraient ainsi s'authentifier de manière centralisée, accéder aux partages de fichiers communs et utiliser le service d'assistance GLPI de Marseille sans jamais faire transiter leurs données en clair sur Internet. L'infrastructure actuelle a été rigoureusement documentée et dimensionnée pour accueillir cette évolution majeure.