BTS Services informatiques aux organisations - SISR

Session 2025

E5 – Support et mise à disposition de services informatiques

Coefficient 4

DESCRIPTION DE LA REALISATION PROFESSIONNELLE

NOM et prénom du candidat :

Nathan VANDENBOSSCHE

Contexte de la réalisation professionnelle

- ***Layer Bureautique et Informatique*** *est une entreprise spécialisée dans la gestion d'infrastructures IT et la virtualisation, offrant des services essentiels pour répondre aux besoins de performance, sécurité et continuité des systèmes informatiques du client vdb-pro.*

- *La problématique principale réside dans le manque d'infrastructure pour accueillir les collaborateurs, malgré la présence d'un ESXi puissant.*

- *La solution choisie consiste à déployer une infrastructure hautement disponible et sécurisée, avec une réplication AD/DNS entre deux serveurs. Des scripts d'automatisation ont été utilisés pour la création d'unités organisationnelles, d'utilisateurs et de groupes afin d'optimiser la gestion des ressources et des permissions.*

Intitulé de la réalisation professionnelle

Mise en place d'une infrastructure Active Directory hautement disponible

Période de réalisation : 20/05/24 - 21/05/24 **Lieu :** Auxerre

Modalité : ☒ Individuelle ☐ En équipe

Principale(s) activité(s) concernée(s) :

- METTRE A DISPOSITION DES UTILISATEURS UN SERVICE INFORMATIQUE
- GERER LE PATRIMOINE INFORMATIQUE

Conditions de réalisation

- **Ressources présentes (situation avant la RP)**
  Un ESXi suffisamment puissant est disponible, mais aucune infrastructure n'a été créée pour accueillir des collaborateurs.

- **Résultats attendus (situation après la RP)**
  Une infrastructure hautement disponible, sécurisée et optimisée pour accueillir des collaborateurs.

- **Durée de réalisation**
  La mise en place de cette infrastructure m'a pris environ 2 jours, les scripts étant la partie la plus longue à réaliser.

Modalités d'accès à cette réalisation professionnelle.

https://portfolio.vdb-pro.fr *mdp : Cyb3r-M@P89$*

Partie 1 – Procédure de mise en œuvre

Dans le cadre de ma mission chez Layer Bureautique et Informatique, j'ai conçu une infrastructure Active Directory (AD) hautement disponible avec deux serveurs AD, l'un en mode graphique et l'autre en mode ligne de commande (server Core) pour le client vdb-pro. J'ai assuré la réplication entre ces serveurs pour garantir la redondance et la disponibilité continue des services. De plus, j'ai automatisé la création d'Unités Organisationnelles (OU) et d'utilisateurs à l'aide de scripts, simplifiant ainsi la gestion de l'AD.

Création des machines virtuelles (VM) dans ESXi

La virtualisation via ESXi permet de créer et gérer plusieurs machines virtuelles (VM) sur un seul serveur physique. En utilisant un hyperviseur comme ESXi, on peut isoler les différents services et rôles réseau dans des environnements séparés, ce qui est essentiel pour tester et sécuriser l'infrastructure. Cela réduit également les coûts matériels et améliore la gestion des ressources.

La création des VM dans ESXi permet de déployer un environnement virtuel sécurisé pour la mise en place des différents services (pare-feu, contrôleurs de domaine, client) dans une infrastructure isolée. Cela facilite la gestion, l'expérimentation et la restauration en cas d'erreur sans impacter un réseau physique.

Créer une VM dans ESXi implique de spécifier des paramètres comme l'allocation de mémoire vive (RAM), le nombre de cœurs CPU, et l'espace disque. Ces ressources sont ajustées selon les besoins de chaque service pour garantir des performances optimales. Une fois les VM créées, elles pourront être démarrées et configurées individuellement.

Schéma ESXi

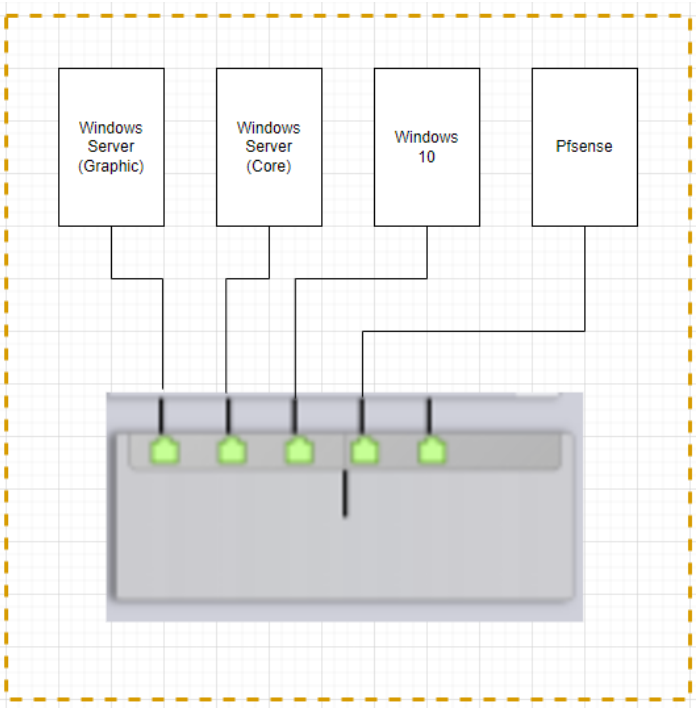
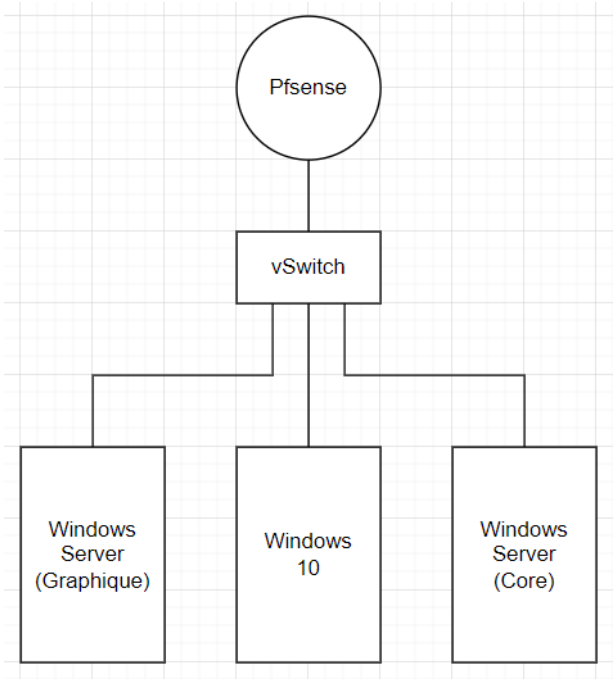


Schéma logique

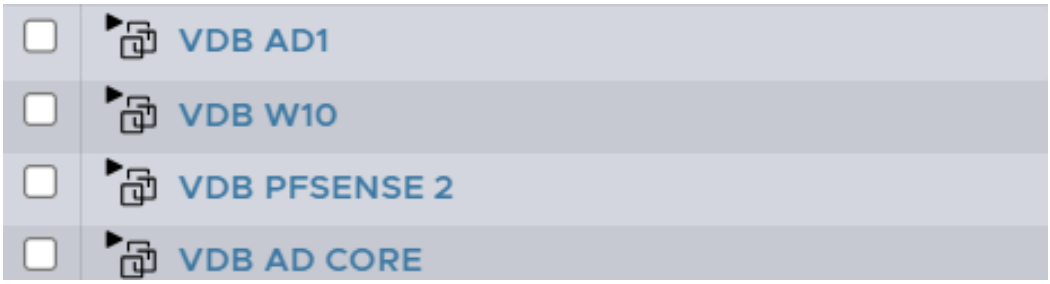


- **PfSense :** Joue le rôle de pare-feu pour filtrer le trafic et assurer la sécurité réseau.

- **Windows Server 2019 (GUI) :** Ce serveur est le contrôleur de domaine principal, il prend en charge les rôles AD (Active Directory) et DNS pour la gestion centralisée des ressources réseau.

- **Windows Server 2019 Core :** Servira de contrôleur de domaine secondaire et de serveur DNS répliqué, permettant la redondance et la résilience du service.

- **Windows 10 :** Client qui sera utilisé pour valider l'intégration et la connectivité dans le domaine Active Directory.



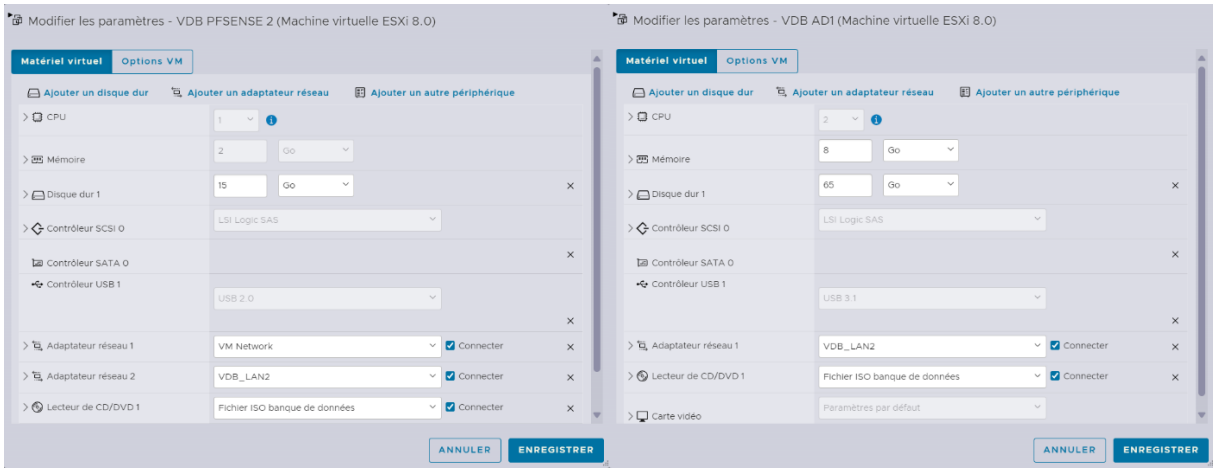
Configuration d'ESXi et des paramètres de VM (performance/réseau)

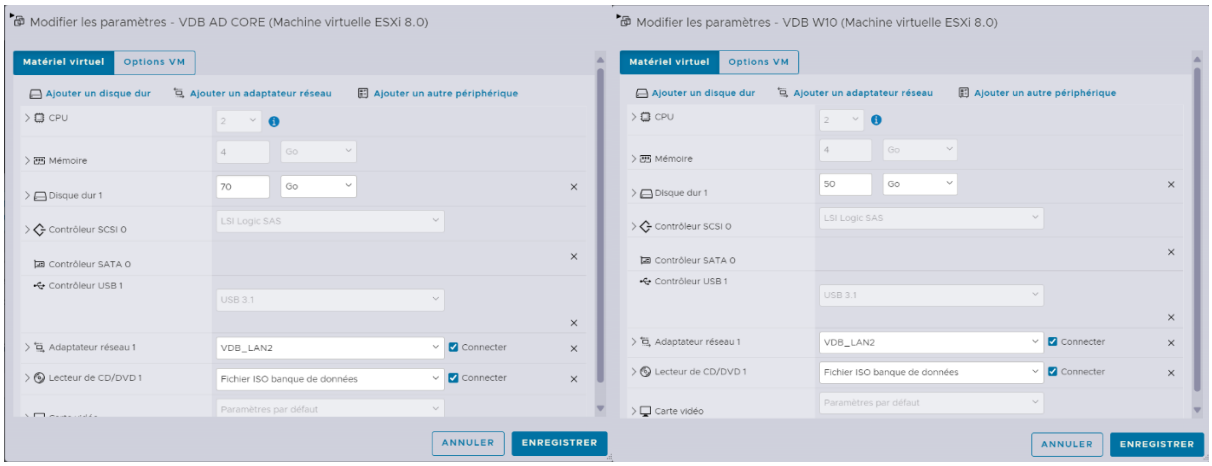
La configuration des ressources sur ESXi assure que les VM reçoivent les ressources nécessaires pour fonctionner sans ralentissement. Le réseau virtuel permet aux machines de communiquer en interne sans accès direct à Internet, assurant ainsi la sécurité et l'isolation de l'environnement.

Configurer ESXi et les paramètres des VM optimise l'allocation de ressources pour éviter les goulets d'étranglement et garantir un fonctionnement fluide de l'environnement. De plus, la configuration réseau permet aux VM de communiquer entre elles dans un environnement isolé.

Configuration des performances des VM dans ESXi :

Ajustement des ressources allouées aux VM (CPU, RAM, disque) selon les besoins du projet pour garantir une réactivité optimale.

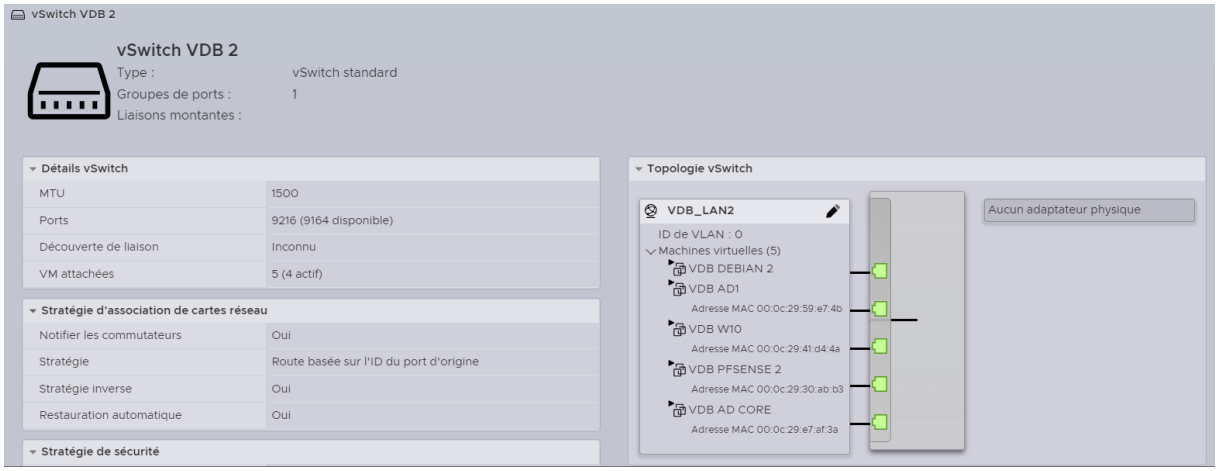




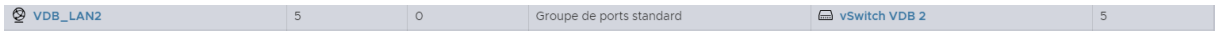
Paramètre supplémentaire que l'on peut configurer est l'allocation de mémoire, la réservation de ressources et la limitation d'IO pour chaque VM.

Configuration réseau dans ESXi :

Création d'un vSwitch (vSwitch VDB 2) : Ce vSwitch permet de créer un réseau isolé pour les machines virtuelles (VM), assurant ainsi une sécurité accrue en restreignant l'accès aux VM et en empêchant toute communication non autorisée avec le réseau externe.



Création d'un groupe de ports (VDB_LAN2) : Ce groupe de ports est associé au vSwitch, offrant une interface de communication dédiée pour toutes les VM connectées. Il garantit une communication fluide et sécurisée entre les VM tout en optimisant la gestion du trafic réseau interne.



Configuration de PfSense pour isoler le réseau

PfSense est une solution pare-feu open source. Dans notre architecture, il protège et isole le réseau virtuel. Ce pare-feu sert également de routeur, permettant de filtrer le trafic entrant et sortant et d'autoriser uniquement les connexions nécessaires. Dans un environnement de production, cela limite l'exposition de l'infrastructure aux menaces extérieures.

Configurer PfSense avec une adresse **WAN** pour la connexion externe 10.5.0.29 et une adresse **LAN** pour le réseau interne 172.17.129.126. Les règles de pare-feu dans PfSense permettent de restreindre le trafic en fonction des besoins, et les règles NAT (Network Address Translation) permettent l'accès RDP sécurisé depuis l'extérieur.

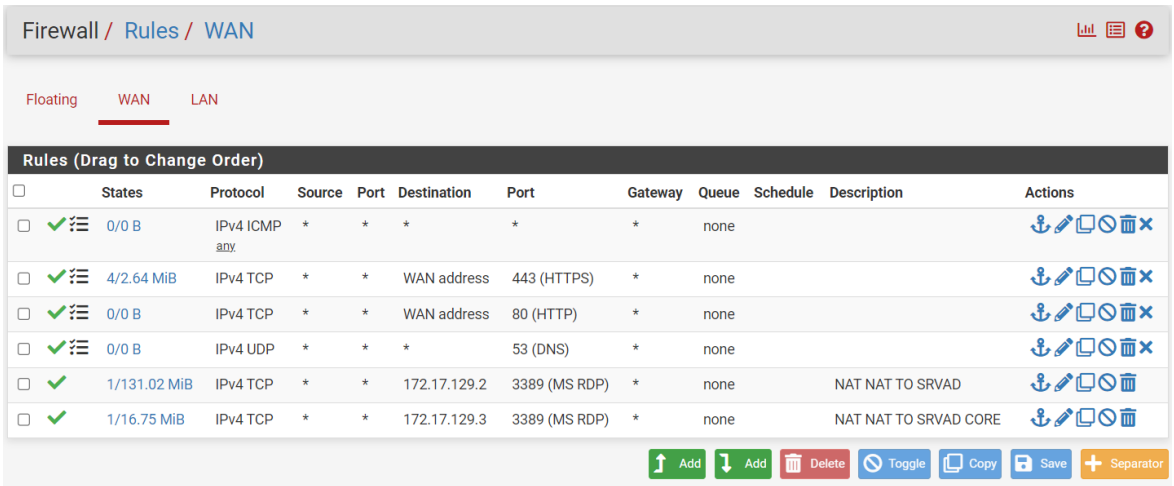
Paramètres réseau :

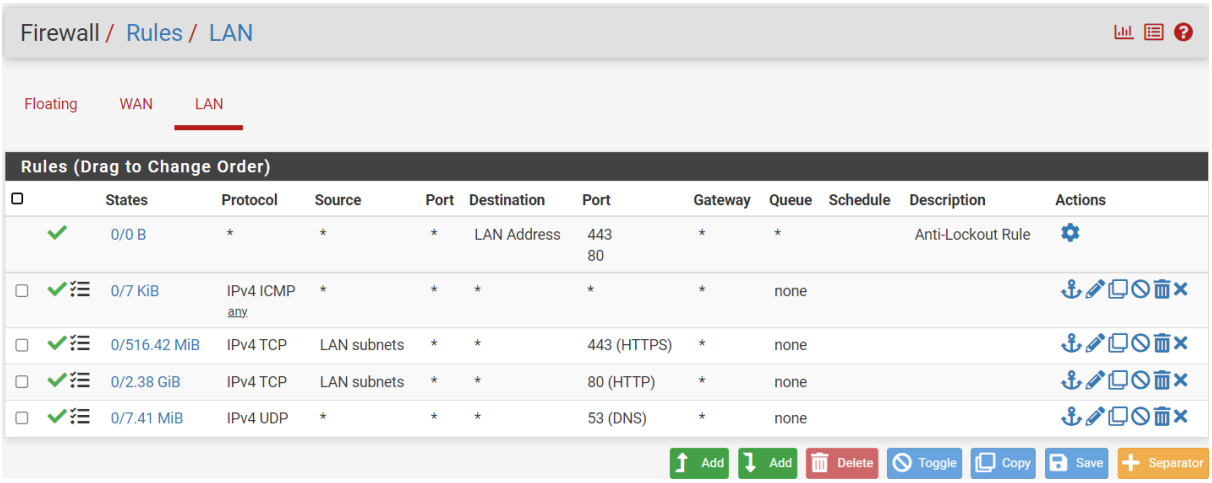
- **WAN :** Adresse IP 10.5.0.29 /16, connectée au réseau externe.
- **LAN :** Adresse IP 172.17.129.126 /25, pour le réseau interne entre les VM.

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense2 ***

WAN (wan)       -> vmx0       -> v4/DHCP4: 10.5.0.29/16
LAN (lan)       -> vmx1       -> v4: 172.17.129.126/25

0) Logout (SSH only)                  9) pfTop
1) Assign Interfaces                 10) Filter Logs
2) Set interface(s) IP address       11) Restart webConfigurator
3) Reset webConfigurator password    12) PHP shell + pfSense tools
4) Reset to factory defaults         13) Update from console
5) Reboot system                     14) Enable Secure Shell (sshd)
6) Halt system                       15) Restore recent configuration
7) Ping host                         16) Restart PHP-FPM
8) Shell
```

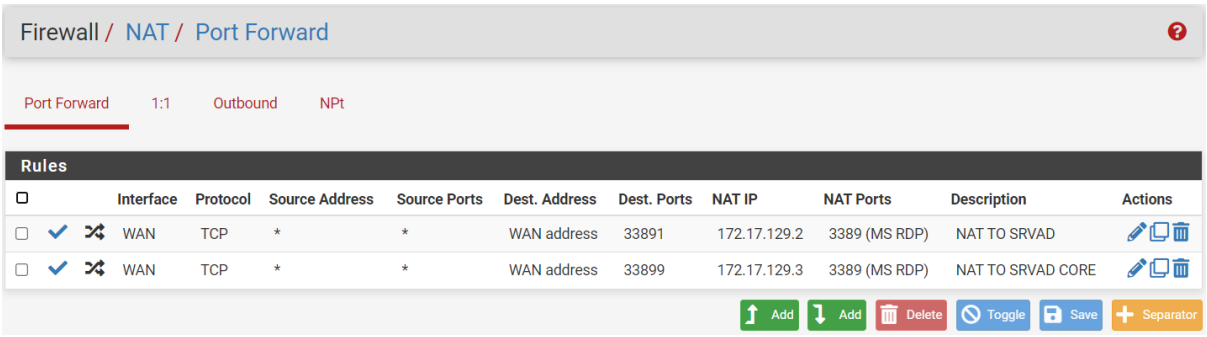
Règles PfSense :

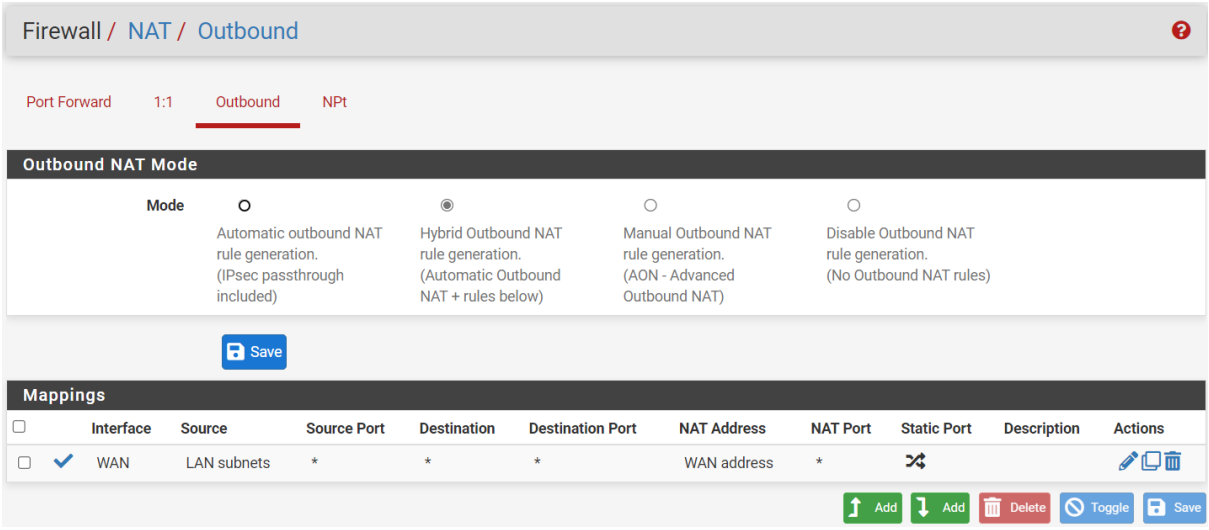
Rules : Configuration de règles de pare-feu pour contrôler l'accès et la circulation entre le réseau interne et externe.





NAT : Paramétrage de la redirection de port (RDP) pour accéder aux VM en interne depuis l'extérieur





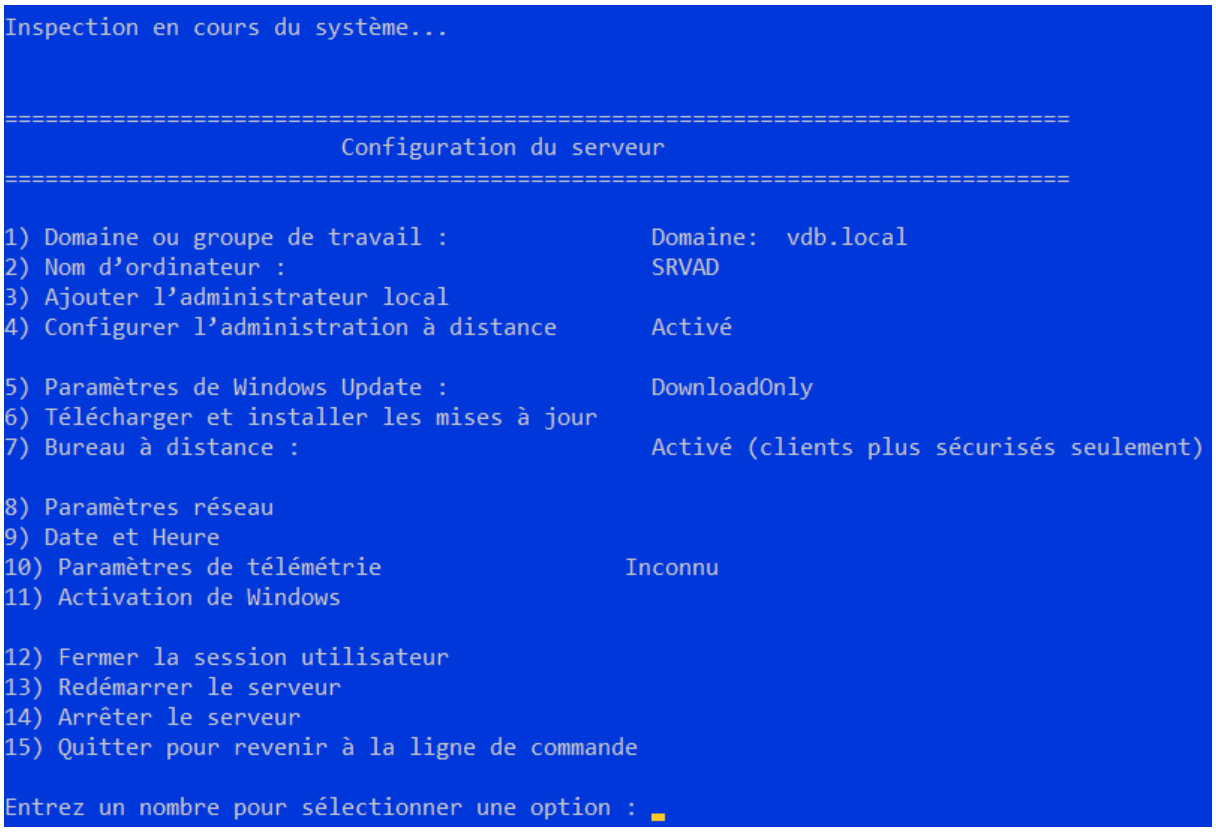
Installation et configuration de Windows Server 2022 (Interface graphique)

Le serveur Windows avec interface graphique est le principal contrôleur de domaine. L'interface facilite la gestion d'Active Directory, un service essentiel pour centraliser les utilisateurs, les groupes et les politiques de sécurité d'un réseau. C'est ce serveur qui initie le domaine vdb.local, fournissant les services d'authentification, de DNS et de DHCP.

Prise en main : Accès à la VM via ESXi pour effectuer les configurations de base.
Paramétrage réseau avec PowerShell « *sconfig* » : Configure l'adresse IP, la passerelle et le DNS pour que le serveur soit accessible aux autres machines.

Adresse IP : 172.17.129.2 /25
Passerelle : 172.17.129.126
DNS : Utilisation de l'adresse IP locale pour le DNS (172.17.129.2).

Activation de RDP : Permet d'utiliser le bureau à distance pour gérer le serveur de manière plus fluide. Activation de RDP via sconfig pour faciliter la gestion.

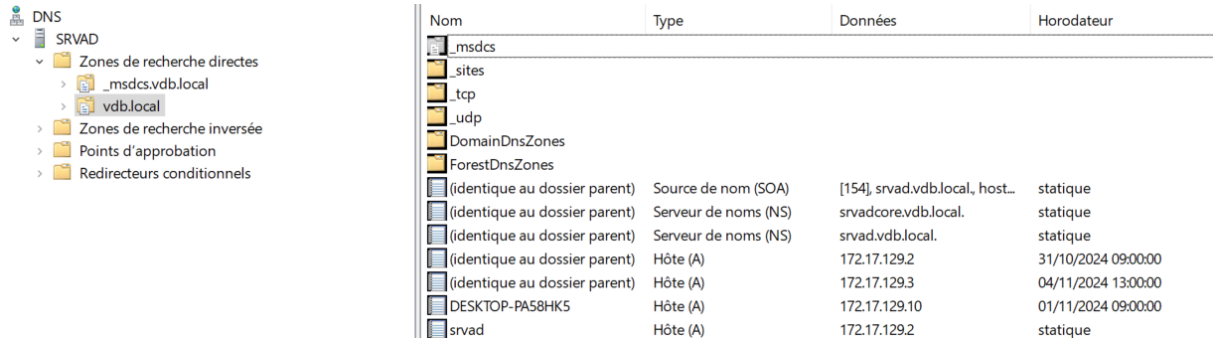


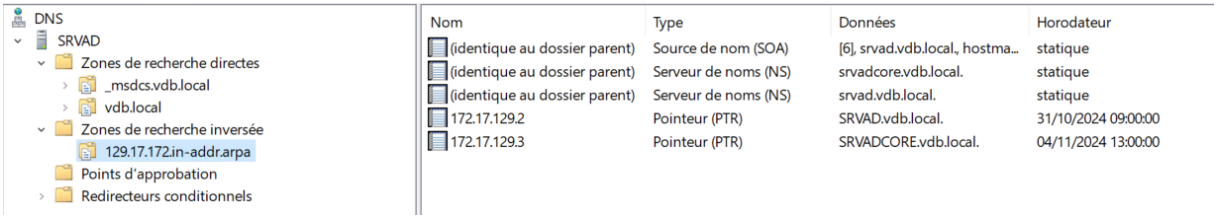
Installation des rôles DNS et AD DS (Active Directory Domain Services) :

Via le Gestionnaire de Serveur, les services AD et DNS sont installés. Le serveur est ensuite promu en tant que Domain Controller (DC), créant une forêt et un domaine vdb.local.

Le rôle de contrôleur de domaine et de DNS permet de gérer les ressources du domaine, les identités des utilisateurs, et de faciliter la résolution de noms. L'activation de RDP et les réglages réseau facilitent l'administration à distance.

Je configure donc les **zones DNS**, à la fois la **zone directe** (Forward Lookup Zone) et la **zone inversée** (Reverse Lookup Zone). Ces configurations sont essentielles pour assurer la résolution des noms dans notre infrastructure réseau, permettant aux machines de se trouver mutuellement de manière efficace.





Je procède à la promotion du serveur en tant que **contrôleur de domaine principal** dans **une nouvelle forêt** appelée **vdb.local**. Cette étape est cruciale pour la mise en place de notre infrastructure Active Directory, car elle établit un environnement centralisé pour la gestion des utilisateurs, des groupes, des ordinateurs, et des ressources au sein du réseau.

Je configure les **sites Active Directory** en ajoutant un **nouveau sous-réseau** (réseau LAN 2). L'objectif est d'assurer que tous les **contrôleurs de domaine** situés sur ce réseau soient automatiquement rattachés au **SiteA**.

Cela permet d'optimiser la **réplication Active Directory** en garantissant que le trafic réseau reste localisé et que les clients du réseau LAN 2 interagissent prioritairement avec les contrôleurs de domaine du SiteA, améliorant ainsi la performance et la résilience de l'infrastructure.

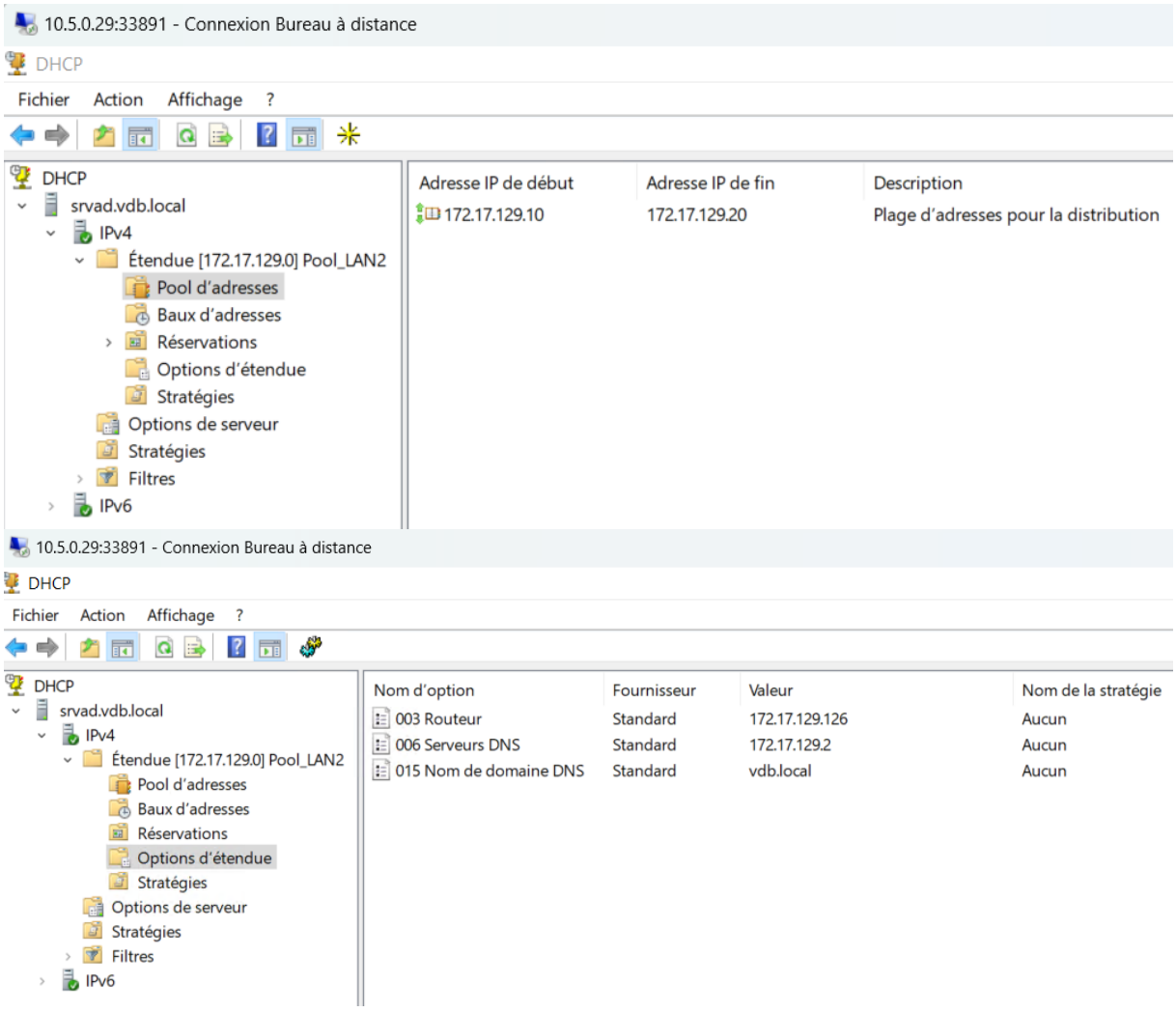
Configuration DHCP

Un serveur DHCP attribue automatiquement des adresses IP aux clients du réseau, simplifiant ainsi la gestion des configurations réseau, notamment pour les postes utilisateurs qui se connectent dynamiquement.

Dans le Gestionnaire DHCP, un pool d'adresses IP est créé pour le sous-réseau de l'environnement (par ex., 172.17.129.0/25). Le serveur DHCP attribuera ces adresses aux clients Windows 10, leur fournissant également l'adresse DNS du domaine.

Le DHCP garantit que les clients reçoivent des adresses IP valides et conformes à la topologie du réseau, simplifiant la configuration pour chaque nouvel utilisateur ou dispositif.

Configuration du pool d'adresses IP : Depuis le Gestionnaire DHCP, un pool d'adresses est défini pour le sous-réseau utilisé par les clients, par exemple 172.17.129.10 - 172.17.129.100. Le serveur DHCP transmet également l'adresse du DNS et l'adresse du routeur (gateway).



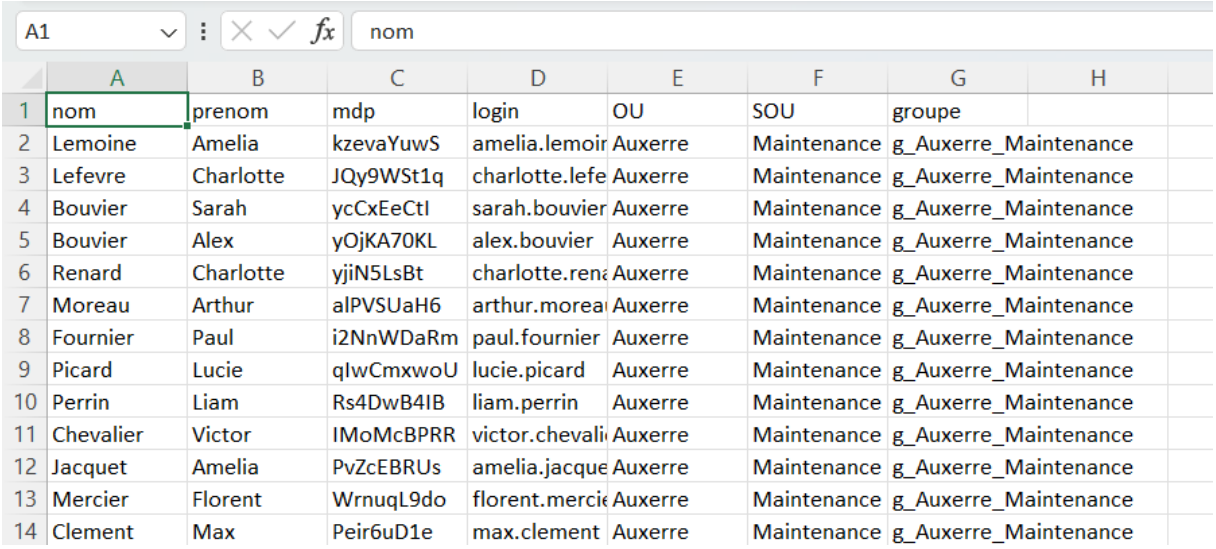
Je peux également configurer des réservations DHCP, ce qui permet de garantir que ces machines reçoivent toujours la même adresse IP, même si elles utilisent le protocole DHCP pour leur configuration réseau.

Création de scripts pour l'AD (OU, utilisateurs, groupes)

L'automatisation permet d'accélérer la création et la gestion des comptes et groupes dans l'Active Directory, évitant ainsi des opérations manuelles répétitives qui peuvent être sources d'erreurs. Cette étape est cruciale pour uniformiser la gestion des droits d'accès et la structure de l'annuaire.

J'ai créé plusieurs scripts PowerShell en utilisant l'IA comme aide afin d'automatiser la gestion d'Active Directory. Ces scripts permettent de créer automatiquement des Unités d'Organisation (OU) comme Technique et Maintenance, d'ajouter en masse des utilisateurs avec des informations prédéfinies (nom, mot de passe, login) et de gérer les groupes en y ajoutant les utilisateurs nécessaires.

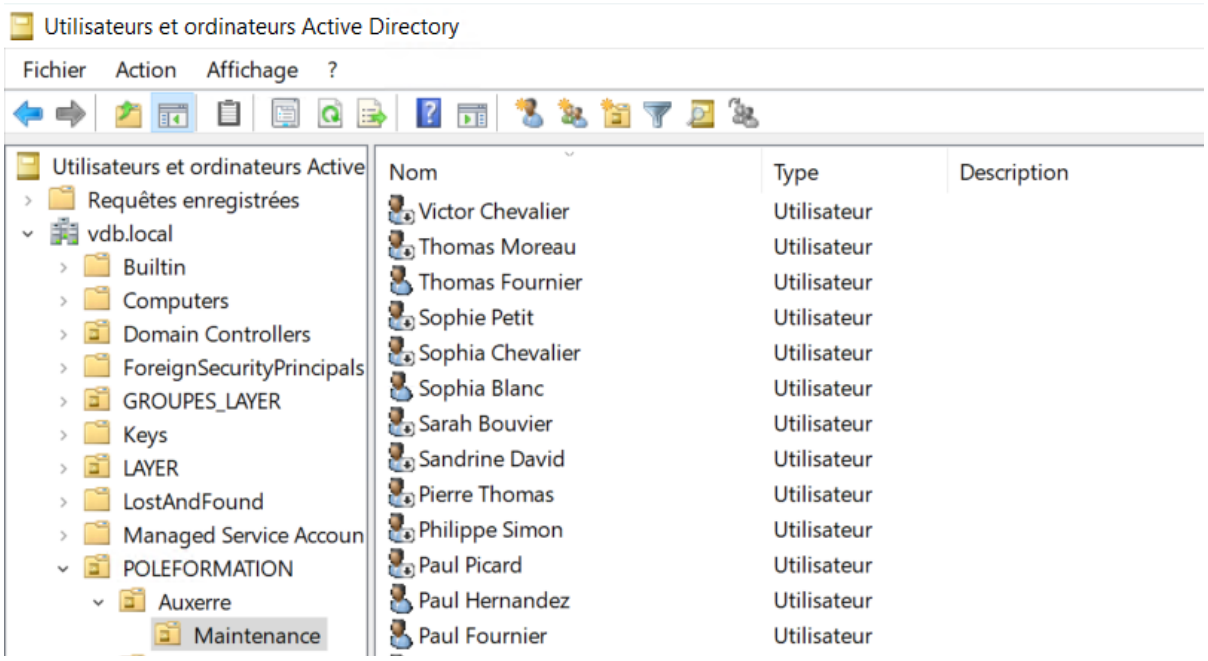
Voici un script PowerShell qui permet de créer des comptes utilisateurs en masse en important les informations depuis un fichier CSV. Ce script facilite la gestion des utilisateurs en automatisant leur création dans Active Directory avec des informations telles que le nom, le prénom, le login, le mot de passe, ainsi que les Unités d'Organisation (OU) et les groupes auxquels ils appartiennent.

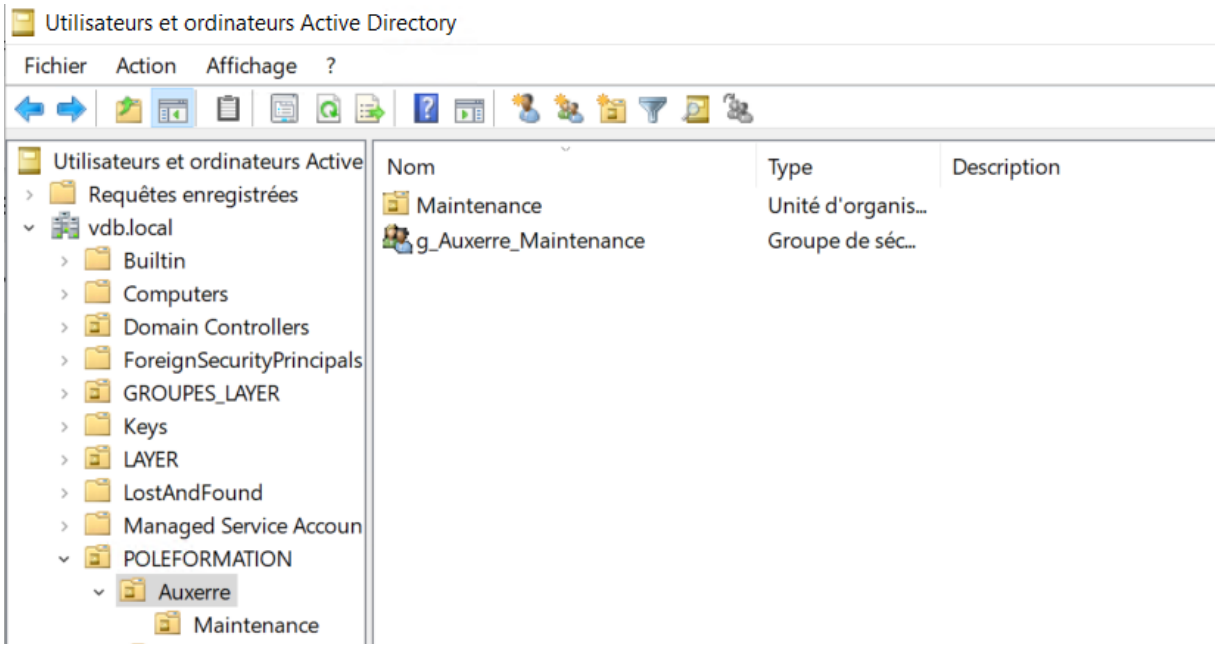


A1 | nom

	A	B	C	D	E	F	G	H
1	nom	prenom	mdp	login	OU	SOU	groupe	
2	Lemoine	Amelia	kzevaYuwS	amelia.lemoir	Auxerre	Maintenance	g_Auxerre_Maintenance	
3	Lefevre	Charlotte	JQy9WSt1q	charlotte.lefe	Auxerre	Maintenance	g_Auxerre_Maintenance	
4	Bouvier	Sarah	ycCxEeCtI	sarah.bouvier	Auxerre	Maintenance	g_Auxerre_Maintenance	
5	Bouvier	Alex	yOjKA70KL	alex.bouvier	Auxerre	Maintenance	g_Auxerre_Maintenance	
6	Renard	Charlotte	yjiN5LsBt	charlotte.rena	Auxerre	Maintenance	g_Auxerre_Maintenance	
7	Moreau	Arthur	alPVSUaH6	arthur.moreau	Auxerre	Maintenance	g_Auxerre_Maintenance	
8	Fournier	Paul	i2NnWDaRm	paul.fournier	Auxerre	Maintenance	g_Auxerre_Maintenance	
9	Picard	Lucie	qIwCmxwoU	lucie.picard	Auxerre	Maintenance	g_Auxerre_Maintenance	
10	Perrin	Liam	Rs4DwB4IB	liam.perrin	Auxerre	Maintenance	g_Auxerre_Maintenance	
11	Chevalier	Victor	IMoMcBPRR	victor.chevali	Auxerre	Maintenance	g_Auxerre_Maintenance	
12	Jacquet	Amelia	PvZcEBRUs	amelia.jacque	Auxerre	Maintenance	g_Auxerre_Maintenance	
13	Mercier	Florent	WrnuqL9do	florent.mercie	Auxerre	Maintenance	g_Auxerre_Maintenance	
14	Clement	Max	Peir6uD1e	max.clement	Auxerre	Maintenance	g_Auxerre_Maintenance	

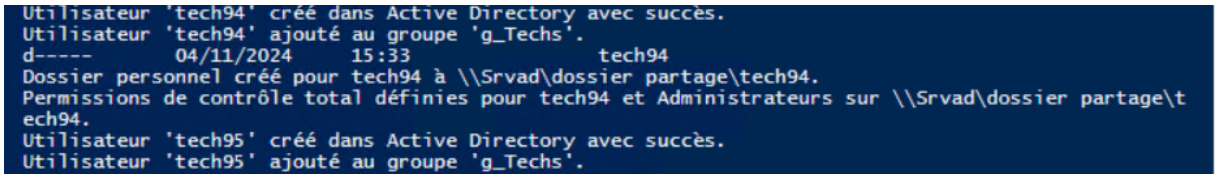
```
$users = Import-Csv -Path "C:\Users\Administrateur\Desktop\european_users_expanded.csv" -Delimiter ";"

# Créer l'OU racine si elle n'existe pas
if (-not (Get-ADOrganizationalUnit -Filter {Name -eq "POLEFORMATION"})) {
    New-ADOrganizationalUnit -Name "POLEFORMATION" -Path "dc=vdb,dc=local"
}

foreach ($user in $users) {
    # OU
    $ou = $user.OU
    $sou = $user.SOU

    # Vérifier et créer l'OU principale
    $ouPath = "ou=$ou,ou=POLEFORMATION,dc=vdb,dc=local"
    if (-not (Get-ADOrganizationalUnit -Filter {Name -eq $ou} -SearchBase "ou=POLEFORMATION,dc=vdb,dc=local")) {
        New-ADOrganizationalUnit -Name $ou -Path "ou=POLEFORMATION,dc=vdb,dc=local"
    }

    # Vérifier et créer l'OU secondaire
    $souPath = "ou=$sou,$ouPath"
    if (-not (Get-ADOrganizationalUnit -Filter {Name -eq $sou} -SearchBase $ouPath)) {
        New-ADOrganizationalUnit -Name $sou -Path $ouPath
    }

    # Groupe
    $group = $user.Groupe
    if (-not (Get-ADGroup -Filter {Name -eq $group} -SearchBase $ouPath)) {
        New-ADGroup -Name $group -Path $ouPath -GroupScope Global -GroupCategory Security
    }

    # Utilisateurs
    $nom = $user.Nom
    $prenom = $user.Prenom
    $login = $user.Login
    $mdp = $user.mdp

    # Créer l'utilisateur si non existant
    if (-not (Get-ADUser -Filter {SamAccountName -eq $login})) {
        New-ADUser -Name "$prenom $nom" `
                -Path $souPath `
                -SamAccountName $login `
                -AccountPassword (ConvertTo-SecureString $mdp -AsPlainText -Force) `
                -DisplayName "$prenom $nom" `
                -Enabled $true `
                -ChangePasswordAtLogon $true
    }
}
```

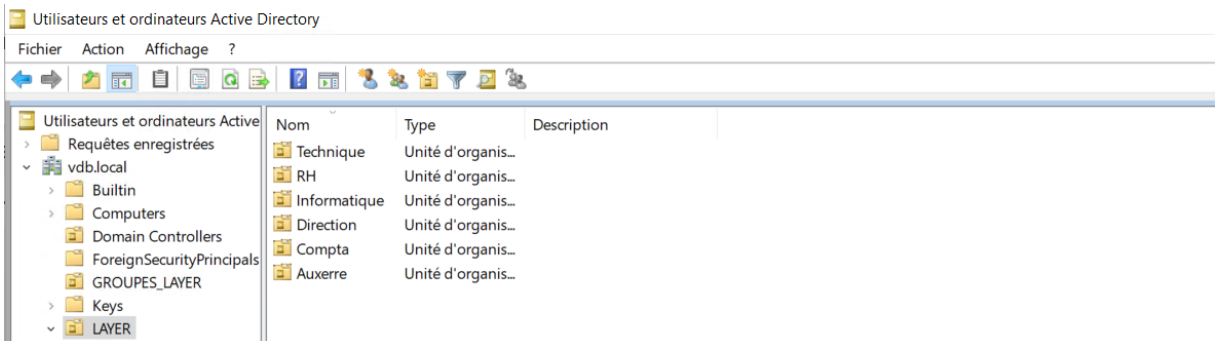

Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage ?
Utilisateurs et ordinateurs Active
Requêtes enregistrées
vdb.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
GROUPES_LAYER
Keys
LAYER
LostAndFound
Managed Service Accoun
POLEFORMATION
Auxerre
Maintenance
Nom
Type
Description
Victor Chevalier Utilisateur
Thomas Moreau Utilisateur
Thomas Fournier Utilisateur
Sophie Petit Utilisateur
Sophia Chevalier Utilisateur
Sophia Blanc Utilisateur
Sarah Bouvier Utilisateur
Sandrine David Utilisateur
Pierre Thomas Utilisateur
Philippe Simon Utilisateur
Paul Picard Utilisateur
Paul Hernandez Utilisateur
Paul Fournier Utilisateur

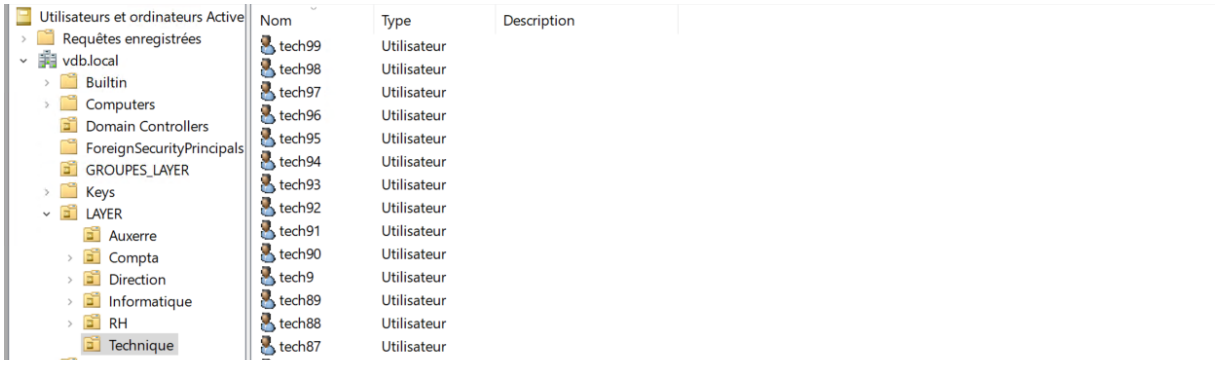

Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage ?
Utilisateurs et ordinateurs Active
Requêtes enregistrées
vdb.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
GROUPES_LAYER
Keys
LAYER
LostAndFound
Managed Service Accoun
POLEFORMATION
Auxerre
Maintenance
Nom
Type
Description
Maintenance Unité d'organis...
g_Auxerre_Maintenance Groupe de séc...

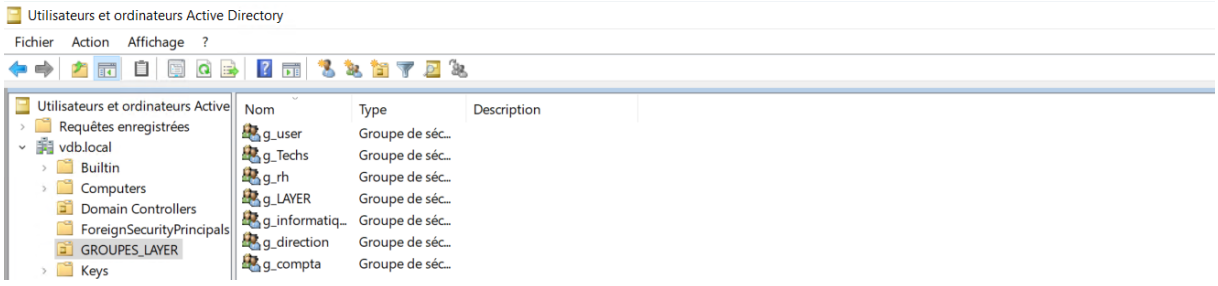
J'ai également créé des scripts toujours via IA permettant d'ajouter des utilisateurs directement via le script, sans avoir besoin de passer par un fichier CSV. Ces scripts sont conçus pour créer rapidement des comptes utilisateurs dans Active Directory en spécifiant directement les informations nécessaires telles que le nom, le prénom, le login, le mot de passe, ainsi que les groupes et les Unités d'Organisation (OU) auxquels ils doivent appartenir.

<u>Voir Script En Annexe</u>





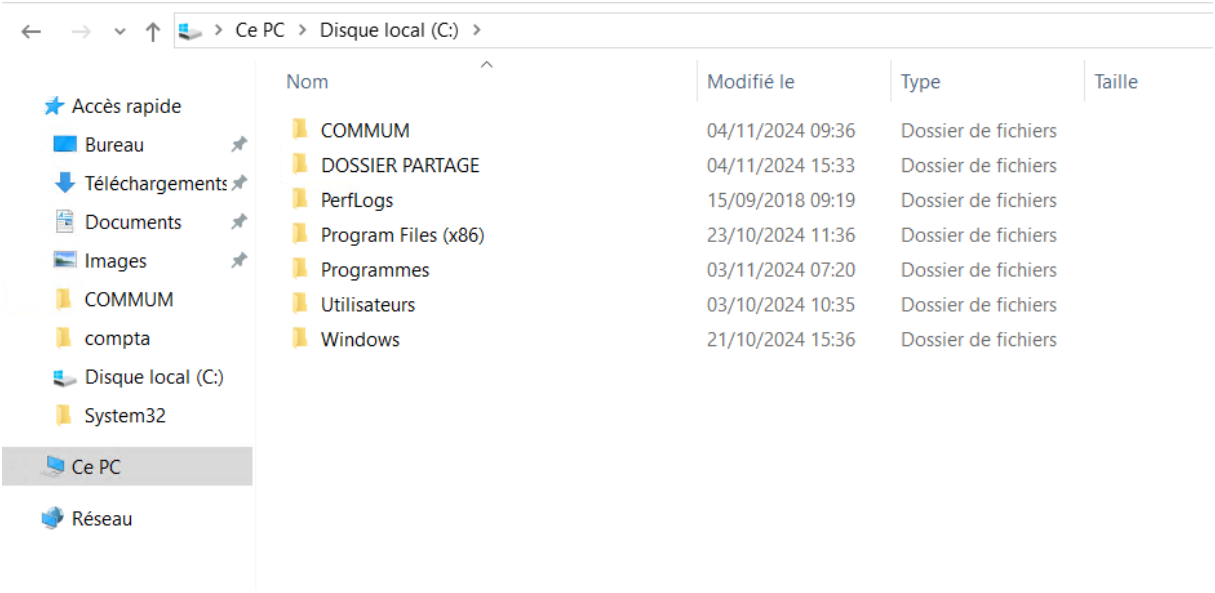


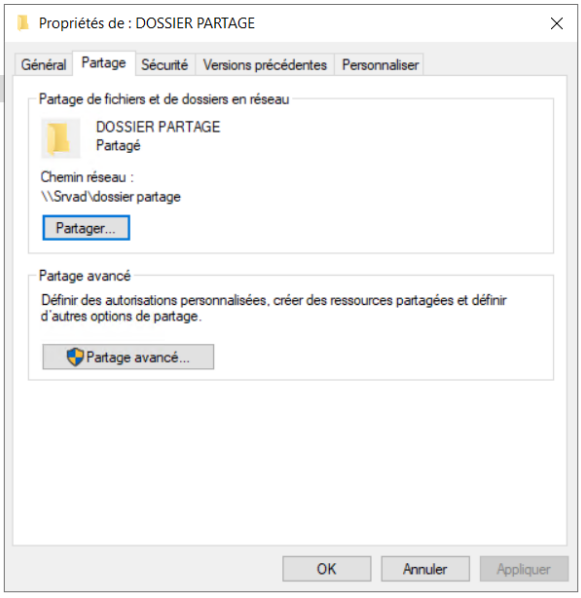


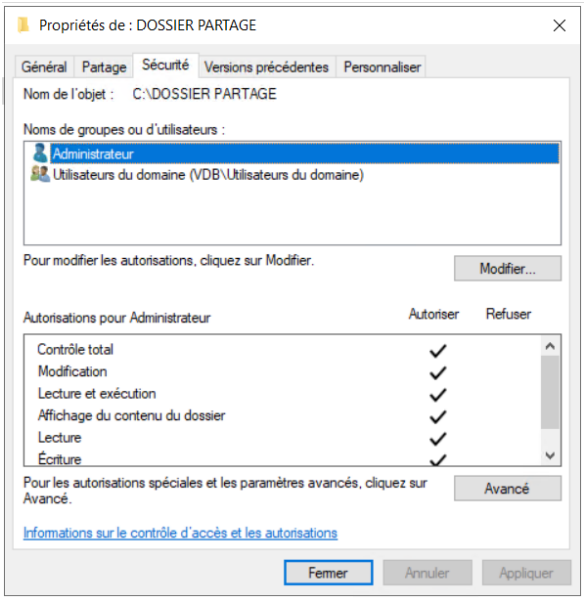
Le script que j'ai créé inclut également la création de dossiers personnels pour chaque utilisateur dans un dossier partagé réseau, tel que \\srvad\dossier_partage. Chaque utilisateur se voit attribuer un répertoire individuel qui lui est propre.

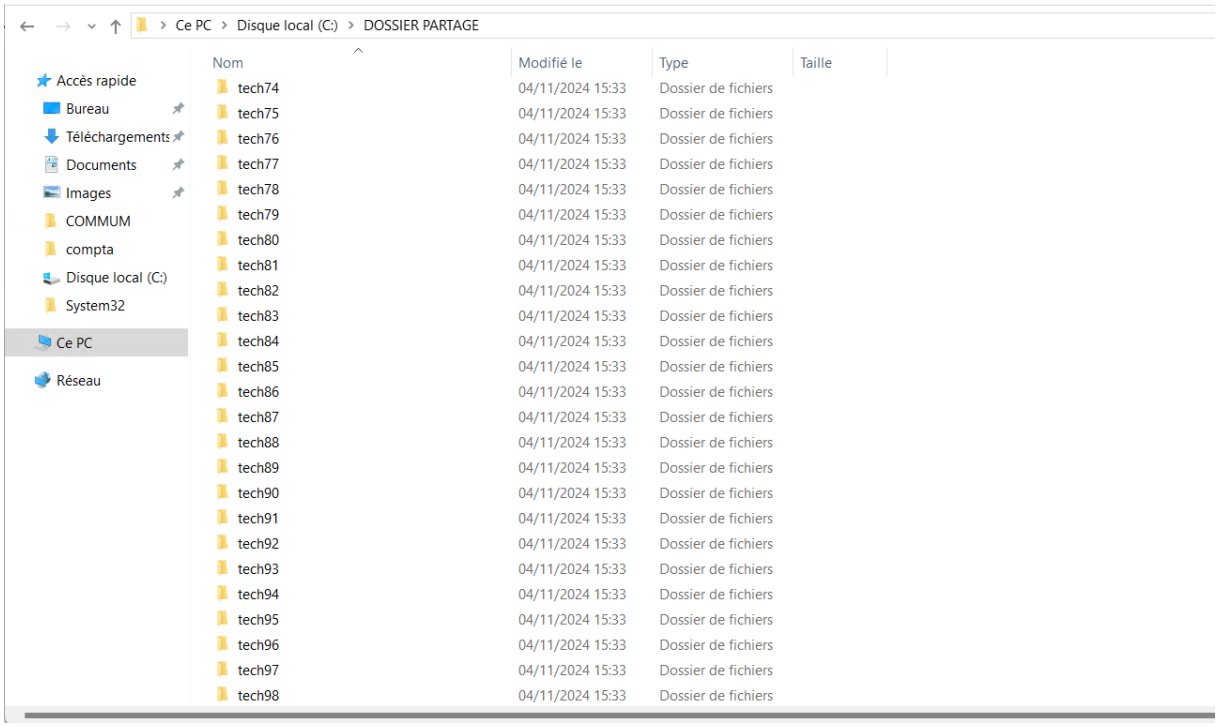
En parallèle, le script gère la configuration des droits ACL (Access Control List) sur ces dossiers personnels. Cela permet de définir des permissions d'accès précises pour chaque utilisateur, tout en assurant que le groupe Administrateurs ait des droits appropriés sur ces répertoires.

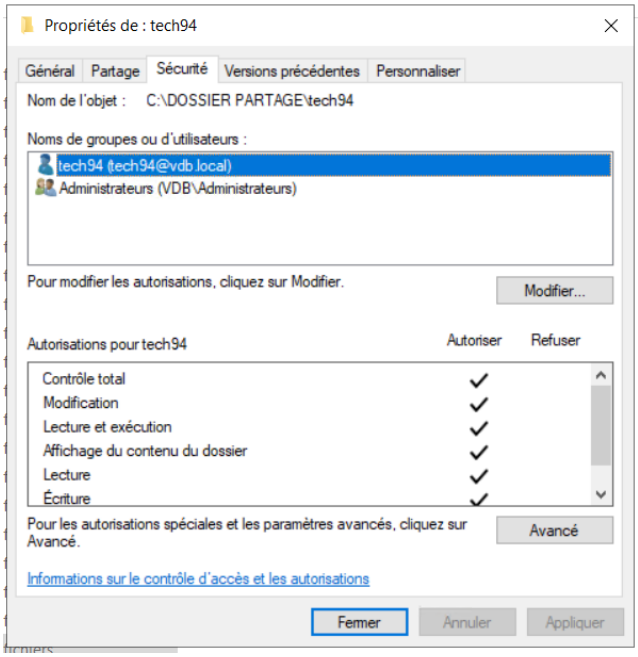
Ainsi, chaque utilisateur a son propre espace de stockage dans le réseau, avec des permissions adaptées à son rôle, tout en garantissant que les administrateurs conservent un contrôle total sur ces ressources partagées.











Cette automatisation rend la gestion des comptes beaucoup plus rapide et moins sujette aux erreurs. Les scripts permettent également de garder une structure d'AD homogène, essentielle pour une administration efficace et pour garantir la sécurité.

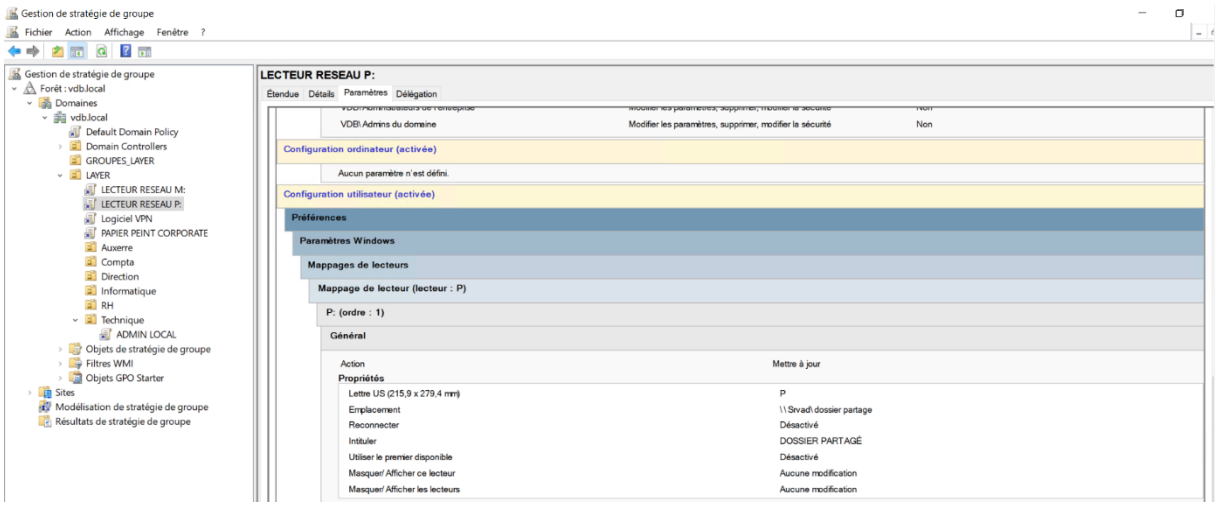
Configuration des GPO (Group Policy Objects)

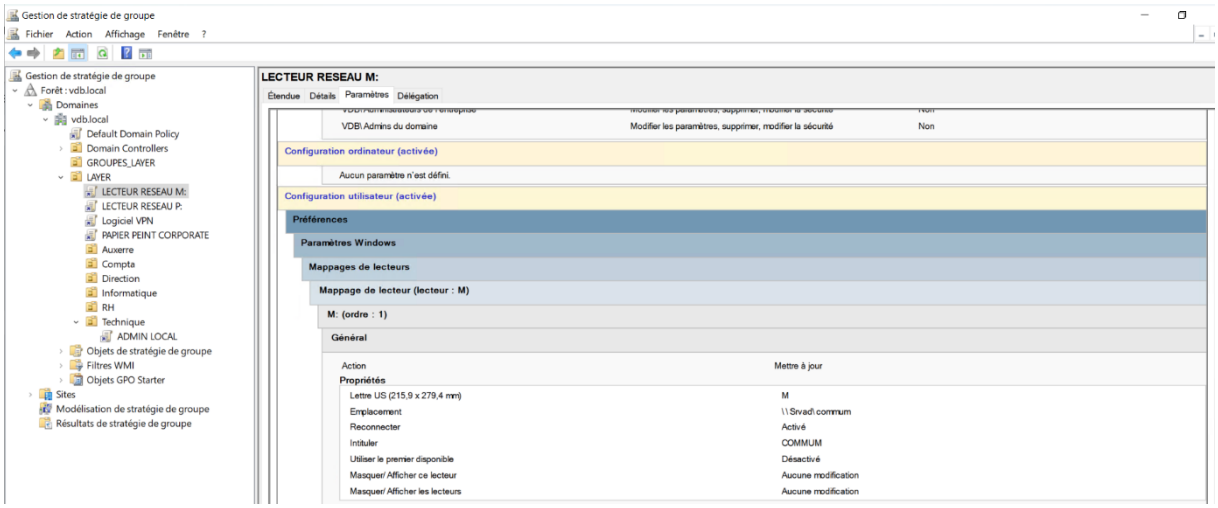
Les GPO permettent d'appliquer des politiques de sécurité, des restrictions et des configurations de manière centralisée aux utilisateurs et aux ordinateurs du domaine. Elles sont essentielles pour contrôler l'environnement utilisateur et s'assurer du respect des normes de sécurité.

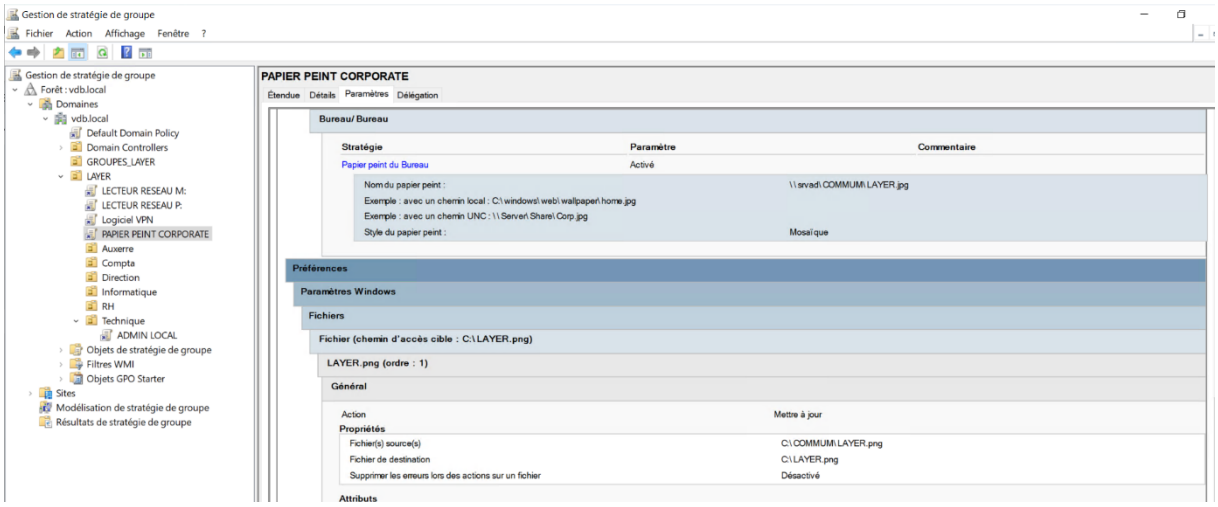
Les GPO peuvent être configurées dans le Gestionnaire de stratégie de groupe (GPMC) en spécifiant des paramètres comme les restrictions d'accès, les scripts de connexion et d'autres règles de sécurité. Les GPO sont ensuite appliquées aux OU ou aux groupes d'utilisateurs/ordinateurs spécifiques.

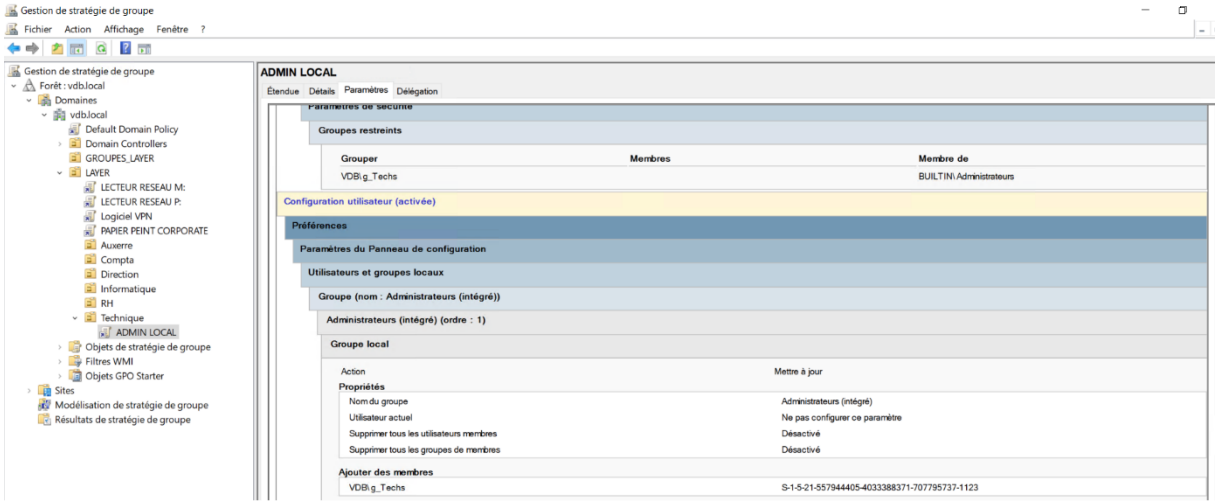
J'ai créé plusieurs **stratégies de groupe (GPO)** pour standardiser l'environnement utilisateur, telles que :

- **Lecteurs réseau** pour monter automatiquement des ressources partagées.
- **Papier peint corporate** pour appliquer un fond d'écran uniforme sur tous les postes.
- **Activation du compte local des techniciens en administrateur local** pour faciliter la gestion des machines par les techniciens.






Gestion de stratégie de groupe
Fichier Action Affichage Fenêtre ?
Gestion de stratégie de groupe
Forêt : vdb.local
Domaines
vdb.local
Default Domain Policy
Domain Controllers
GROUPES_LAYER
LAYER
LECTEUR RESEAU M:
LECTEUR RESEAU P:
Logiciel VPN
PAPIER PEINT CORPORATE
Auxerre
Compta
Direction
Informatique
RH
Technique
ADMIN LOCAL
Objets de stratégie de groupe
Filtres WMI
Objets GPO Starter
Sites
Modélisation de stratégie de groupe
Résultats de stratégie de groupe
PAPIER PEINT CORPORATE
Étendue Détails Paramètres Délégation
Bureau/ Bureau
Stratégie
Paramètre
Commentaire
Papier peint du Bureau
Activé
Nom du papier peint :
\\ srvad\ COMMUM\ LAYER.jpg
Exemple : avec un chemin local : C:\ windows\ web\ wallpaper\ home.jpg
Exemple : avec un chemin UNC : \\ Server\ Share\ Corp.jpg
Style du papier peint :
Mosaïque
Préférences
Paramètres Windows
Fichiers
Fichier (chemin d'accès cible : C:\LAYER.png)
LAYER.png (ordre : 1)
Général
Action
Mettre à jour
Propriétés
Fichier(s) source(s)
C:\ COMMUM\ LAYER.png
Fichier de destination
C:\ LAYER.png
Supprimer les erreurs lors des actions sur un fichier
Désactivé
Attributs


Gestion de stratégie de groupe
Fichier Action Affichage Fenêtre ?
Gestion de stratégie de groupe
Forêt : vdb.local
Domaines
vdb.local
Default Domain Policy
Domain Controllers
GROUPES_LAYER
LAYER
LECTEUR RESEAU M:
LECTEUR RESEAU P:
Logiciel VPN
PAPIER PEINT CORPORATE
Auxerre
Compta
Direction
Informatique
RH
Technique
ADMIN LOCAL
Objets de stratégie de groupe
Filtres WMI
Objets GPO Starter
Sites
Modélisation de stratégie de groupe
Résultats de stratégie de groupe
ADMIN LOCAL
Étendue Détails Paramètres Délégation
Groupes restreints
Grouper
Membres
Membre de
VDB\g_Techs
BUILTIN\Administrateurs
Configuration utilisateur (activée)
Préférences
Paramètres du Panneau de configuration
Utilisateurs et groupes locaux
Groupe (nom : Administrateurs (intégré))
Administrateurs (intégré) (ordre : 1)
Groupe local
Action
Mettre à jour
Propriétés
Nom du groupe
Administrateurs (intégré)
Utilisateur actuel
Ne pas configurer ce paramètre
Supprimer tous les utilisateurs membres
Désactivé
Supprimer tous les groupes de membres
Désactivé
Ajouter des membres
VDB\g_Techs
S-1-5-21-557944405-4033388371-707795737-1123

Installation de Windows 10

Les **stations de travail** (Windows 10) doivent être intégrées au domaine pour permettre aux utilisateurs de se connecter à l'aide de leurs identifiants Active Directory (AD). Cela simplifie également la gestion des permissions et des ressources auxquelles les utilisateurs peuvent accéder.

Windows 10 est utilisé pour simuler un poste de travail client, afin de vérifier l'intégration correcte au domaine, la fonctionnalité des services AD/DNS, ainsi que l'accès aux ressources et l'application des GPO.

Configuration du client DNS :

Chaque **poste de travail** est configuré pour utiliser l'adresse **DNS du serveur principal**. Cela garantit une résolution correcte des noms et permet la connexion au domaine sans problème.

Intégration au Domaine :

Pour intégrer une machine Windows 10 au domaine **vdb.local**, on utilise la commande **netdom join**, une méthode simple et rapide en ligne de commande pour rejoindre le domaine. Cela établit une connexion sécurisée entre le poste de travail et le contrôleur de domaine, facilitant ainsi la gestion centralisée des utilisateurs et des politiques.

Configuration de Windows Server 2022 Core

Le **serveur Core** sera configuré en tant que **contrôleur de domaine secondaire**, ce qui offrira une **redondance** pour les services **Active Directory** et **DNS**, contribuant ainsi à renforcer la résilience du domaine.

Prise en main :

La connexion initiale s'effectuera via **ESXi**, qui permet l'accès à la machine virtuelle.

Paramètres réseau via PowerShell :

Pour afficher les **adaptateurs réseau**, la commande utilisée est :

```
Get-NetAdapter
```

Pour configurer l'**adresse IP**, le **masque** et la **passerelle**, on utilise les commandes suivantes :

```
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress "172.17.10.5" -PrefixLength 24 -DefaultGateway "172.17.10.1"
```

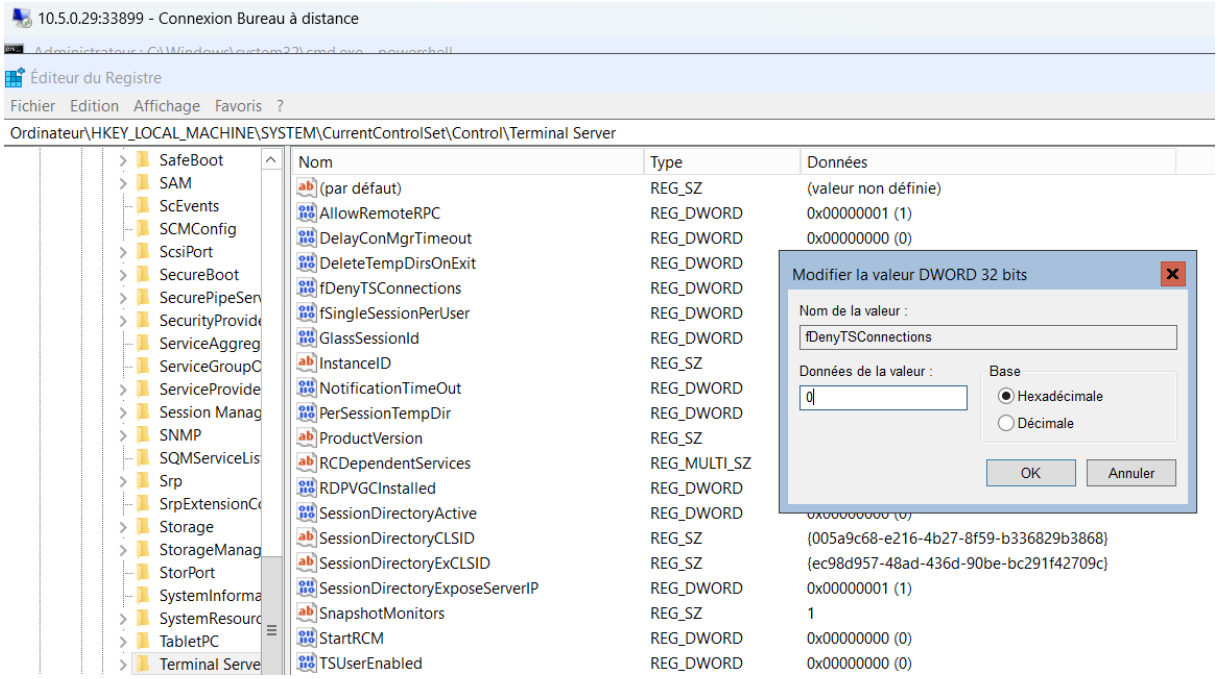
Pour spécifier le serveur DNS, la commande est :

```
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses "172.17.10.2"
```

Activation du bureau à distance :

Le bureau à distance est activé via une modification du registre. On utilise la commande suivante pour permettre les connexions RDP sur le serveur Core :

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t REG_DWORD /d 0 /f
```




```
PS C:\Users\Administrateur.VDB> Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server" | Select-Object fDenyTSConnections
>>

fDenyTSConnections
------------------
                0
```

Cela permet d'activer les connexions à distance et de gérer le serveur Core depuis une machine cliente.

Cette configuration prépare le serveur pour son rôle de contrôleur de domaine secondaire, tout en assurant une gestion réseau optimale et une facilité d'administration à distance.

Installation des services AD et DNS sur le serveur Core

La promotion du serveur **Core** en tant que **contrôleur de domaine secondaire** et en **serveur DNS répliqué** est essentielle pour garantir que les services **Active Directory** (AD) et **DNS** sont toujours disponibles, même en cas d'indisponibilité du serveur principal. Cela assure la **continuité du service** et minimise les risques d'interruptions pour les utilisateurs et les applications.

Installation des services AD et DNS :

1. **Commande pour installer les fonctionnalités AD et DNS** :
   Le serveur **Core** doit avoir les services nécessaires pour gérer l'Active Directory et le DNS. La commande suivante permet d'installer **Active Directory Domain Services** (AD-DS) et **DNS** :

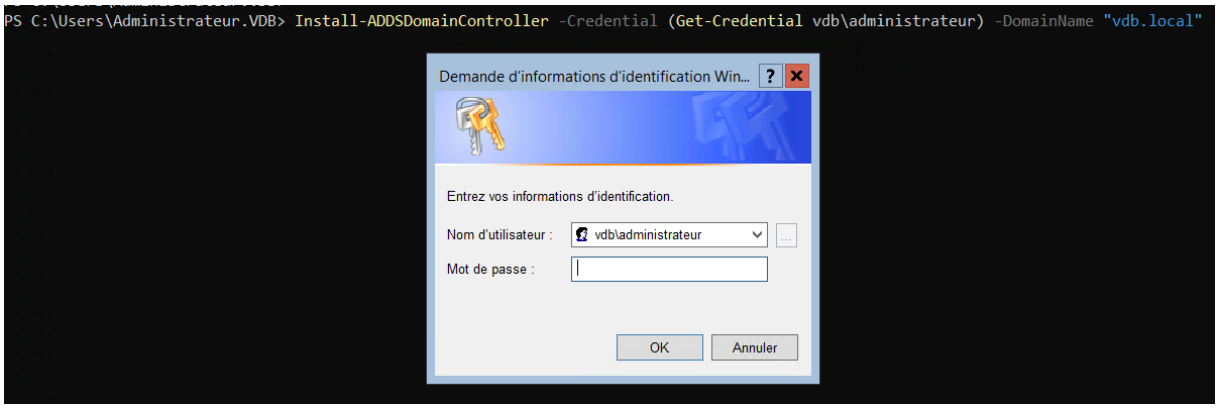
```
Install-WindowsFeature -Name AD-Domain-Services, DNS -IncludeManagementTools
```

Cette commande installe les services requis ainsi que les outils de gestion pour administrer le serveur AD et DNS.

Promotion du serveur Core en contrôleur de domaine secondaire :

Une fois les services installés, le serveur doit être promu en contrôleur de domaine secondaire pour assurer la **réplication**de l'AD et du DNS. La commande de promotion est la suivante :

```
Install-ADDSDomainController -Credential (Get-Credential vdb\administrateur) -DomainName "vdb.local"
```



- Cette commande démarre le processus de promotion et associe le serveur à l'AD existant dans le domaine **vdb.local**.
- **Get-Credential** vous invite à entrer les informations d'identification d'un utilisateur ayant les privilèges nécessaires (comme **administrateur**).
- Le serveur Core sera alors configuré pour répliquer les données du serveur principal et devenir un contrôleur de domaine secondaire.

L'objectif est de garantir que l'Active Directory et le DNS du serveur principal sont répliqués vers le serveur Core. Cela crée une **redondance** qui assure la disponibilité continue des services, même si le serveur principal devient indisponible.

Impact de la redondance :

La mise en place de cette redondance pour **l'Active Directory** et le **DNS** assure non seulement une **résilience accrue** de l'infrastructure, mais elle permet également une **continuité de service** sans interruption pour les utilisateurs et le réseau en cas de défaillance du serveur principal.

Ainsi, ce processus rend le serveur Core pleinement opérationnel en tant que contrôleur de domaine et serveur DNS secondaire, tout en offrant une haute disponibilité pour l'infrastructure Active Directory.

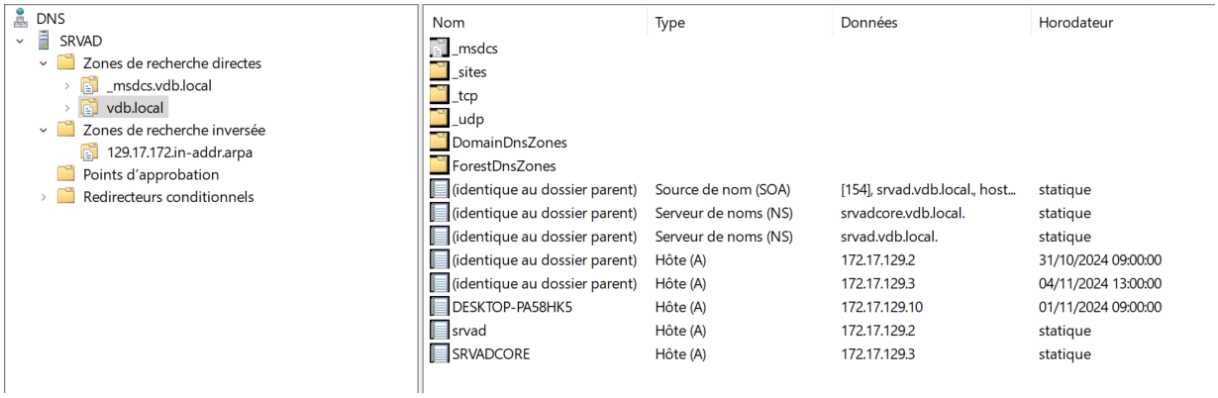
Partie 2 – Validation

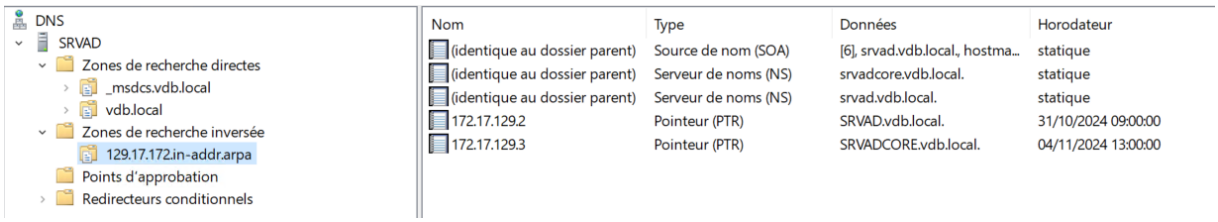
Vérifications de la Réplication

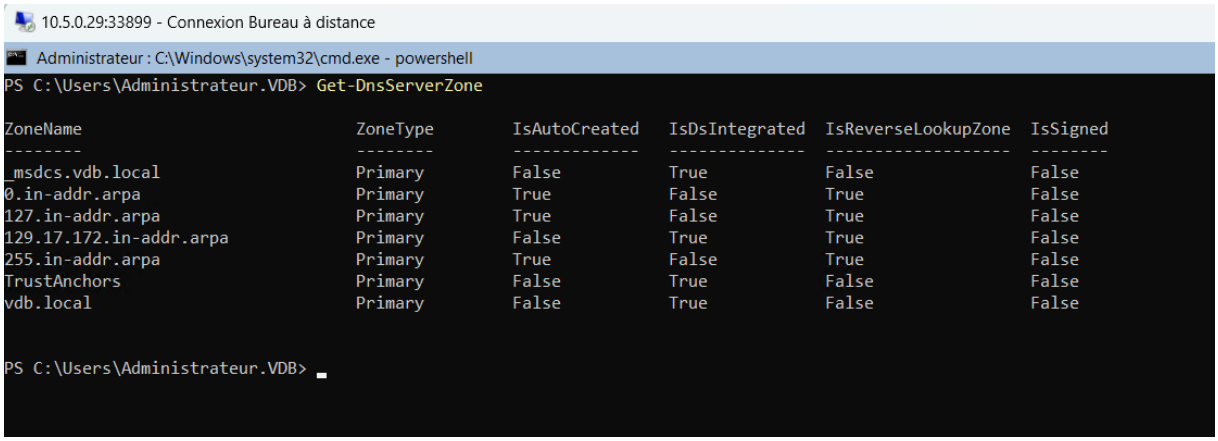
Il est essentiel de vérifier régulièrement la **réplication** entre les contrôleurs de domaine pour assurer la **cohérence** et la **disponibilité** des données dans l'Active Directory (AD) et les services DNS. Cela garantit que les informations sur les utilisateurs, groupes et autres objets AD, ainsi que les enregistrements DNS, sont bien synchronisées entre tous les contrôleurs de domaine, assurant une gestion fluide et une authentification correcte.

Vérification de la réplication DNS :

- Vérifier que les enregistrements DNS sur les contrôleurs de domaine sont synchronisés est crucial pour garantir que la résolution des noms fonctionne correctement.
- **Commande de vérification DNS** : Utilisez des outils comme **nslookup** ou **dnscmd** pour vérifier que les enregistrements DNS sont répliqués entre les serveurs DNS.

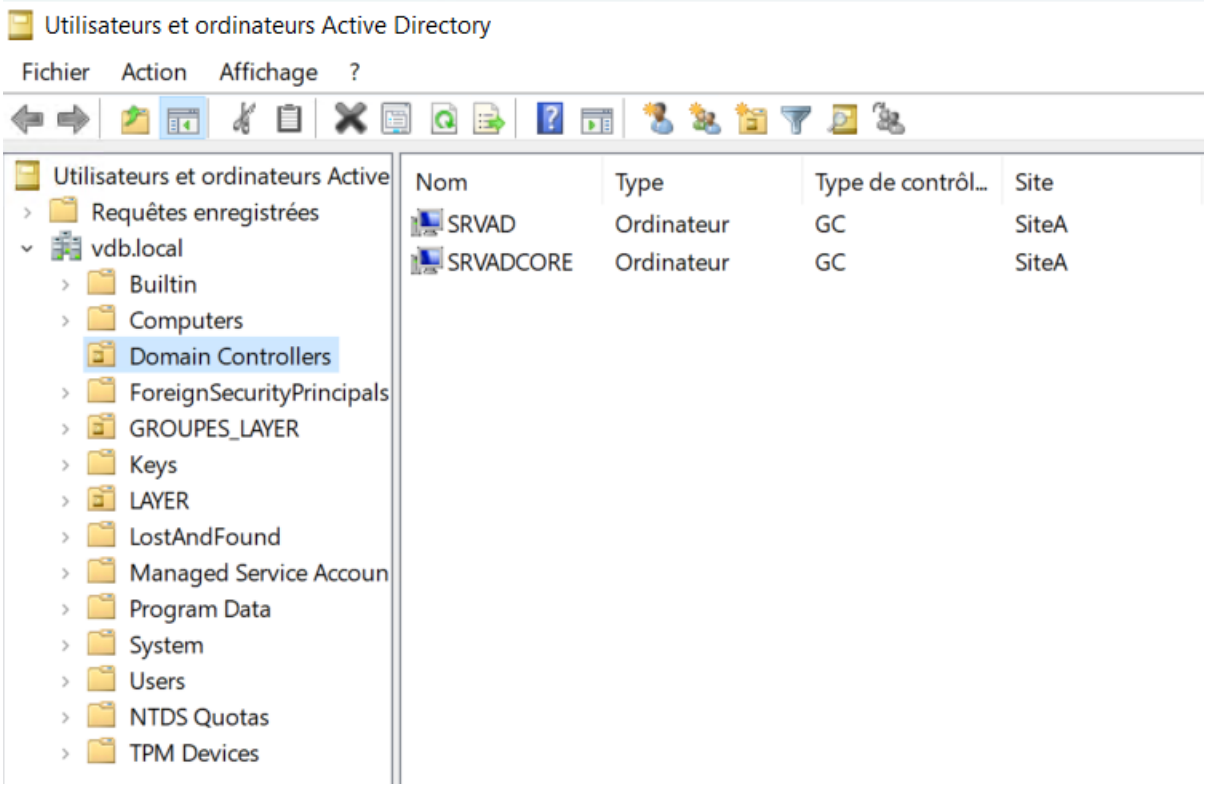






Vérification de la réplication de l'Active Directory :

- Il est important de confirmer que **les utilisateurs**, **les groupes** et **les autres objets AD** sont bien répliqués entre les contrôleurs de domaine.




```
PS C:\Users\Administrateur.VDB> Get-ADOrganizationalUnit -Filter * | Select-Object Name, DistinguishedName
>>

Name               DistinguishedName
----               -----------------
Domain Controllers OU=Domain Controllers,DC=vdb,DC=local
LAYER              OU=LAYER,DC=vdb,DC=local
Compta             OU=Compta,OU=LAYER,DC=vdb,DC=local
RH                 OU=RH,OU=LAYER,DC=vdb,DC=local
Direction          OU=Direction,OU=LAYER,DC=vdb,DC=local
Informatique       OU=Informatique,OU=LAYER,DC=vdb,DC=local
Technique          OU=Technique,OU=LAYER,DC=vdb,DC=local
GROUPES_LAYER      OU=GROUPES_LAYER,DC=vdb,DC=local
Auxerre            OU=Auxerre,OU=LAYER,DC=vdb,DC=local


PS C:\Users\Administrateur.VDB> _
```

- **Commande de vérification AD** : La commande suivante permet de vérifier l'état de la réplication des objets AD :

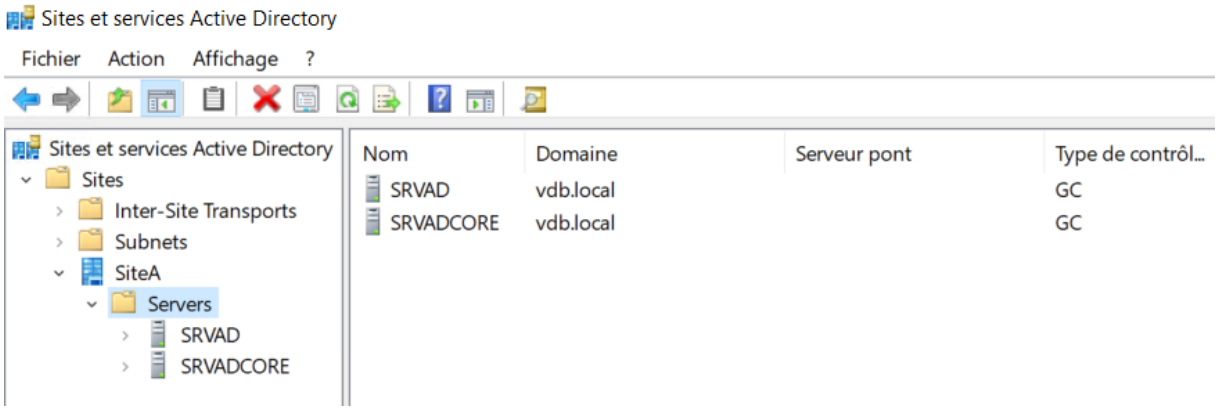
repadmin /replsummary

```
PS C:\Users\Administrateur.VDB> repadmin /replsummary
>>
Heure de début du résumé de la réplication : 2024-11-04 15:55:59

Début de la collecte des données pour le résumé de la réplication ;
cette opération peut prendre un certain temps :
  .....


DSA source              différence max    nb échecs %%   erreur
 SRVAD                      01m:27s    0 /   5    0
 SRVADCORE                  05m:39s    0 /   5    0


DSA de destination      différence max    nb échecs %%   erreur
 SRVAD                      05m:39s    0 /   5    0
 SRVADCORE                  01m:27s    0 /   5    0


PS C:\Users\Administrateur.VDB>
```

Cette commande fournit un résumé de la réplication des contrôleurs de domaine, indiquant si la réplication a réussi ou échoué, ainsi que des détails sur les erreurs potentielles.

Vérification des Sites et Sous-Réseaux :

- Il est également important de vérifier que les **configurations de sites** AD et **les sous-réseaux** associés sont correctement configurés et répliqués. Les sites et sous-réseaux permettent de contrôler la manière dont la réplication se fait entre les contrôleurs de domaine en fonction de leur emplacement géographique et réseau.



Commandes de vérification de la réplication :

1. **repadmin /replsummary** : Cette commande fournit un aperçu de l'état global de la réplication entre tous les contrôleurs de domaine dans le domaine. Elle aide à identifier les problèmes de réplication, y compris les erreurs de connexion et les divergences de données.

2. **w32tm /query /status** : Cette commande permet de vérifier l'état de la **synchronisation du temps** entre les serveurs. La synchronisation horaire est essentielle pour éviter les erreurs liées à des horloges de serveurs désynchronisées, ce qui peut affecter la réplication AD.

```
PS C:\Users\Administrateur.VDB> w32tm /query /status
>>
Indicateur de dérive : 0(Aucun avertissement)
Couche : 2 (Référence secondaire, synchronisée par (S)NTP)
Précision : -23 (119.209ns par battement)
Délai de racine : 0.0015947s
Dispersion de racine : 10.0213984s
ID de référence : 0xAC118102 (IP de la source :  172.17.129.2)
Heure de la dernière synchronisation réussie : 04/11/2024 15:59:24
Source : SRVAD.vdb.local
Intervalle d'interrogation : 7 (128s)

PS C:\Users\Administrateur.VDB>
```

3. **w32tm /resync** : Si des problèmes de synchronisation du temps sont détectés, cette commande force la **synchronisation de l'horloge** entre le serveur local et un serveur NTP (Network Time Protocol), garantissant ainsi la précision de l'heure pour la réplication et les services AD.

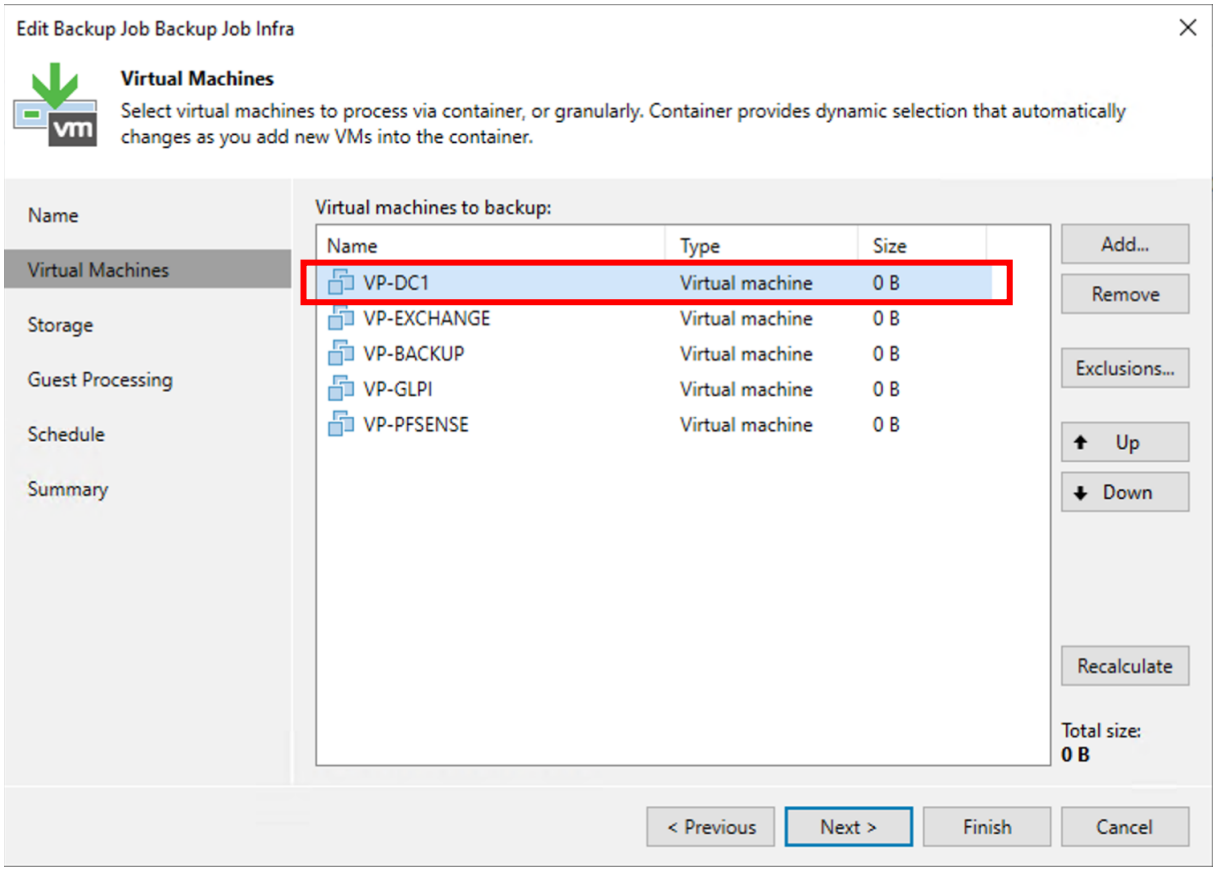
Importance de la réplication et de la vérification de la synchronisation :

La réplication garantit que les utilisateurs et groupes peuvent **s'authentifier** et **accéder** aux ressources indépendamment du contrôleur de domaine auquel ils se connectent. Cela permet de maintenir une **continuité des services** et évite les interruptions de service dues à une divergence des données entre les contrôleurs de domaine.

Les **vérifications de synchronisation** permettent de détecter tout problème de **latence** ou de divergence de données, assurant ainsi que les deux serveurs restent parfaitement alignés.

Gérer le patrimoine informatique

L'ensemble du patrimoine informatique est rigoureusement recensé à l'aide d'un outil de gestion des actifs, assurant une traçabilité complète de l'infrastructure. La redondance du service Active Directory est assurée grâce à la réplication entre un contrôleur de domaine principal (interface graphique) et un contrôleur secondaire sous Windows Server Core, garantissant la disponibilité continue des services d'annuaire et DNS. Les référentiels et bonnes pratiques sont respectés pour assurer une gestion cohérente des droits, attribués selon les habilitations des utilisateurs. La continuité de service est renforcée par la solution de sauvegarde Veeam, déployée par l'entreprise, qui permet des sauvegardes régulières et fiables. Les restaurations sont testées et validées, assurant un retour rapide à la normale en cas d'incident. Enfin, tout écart vis-à-vis des règles d'usage des ressources numériques est systématiquement détecté et signalé pour maintenir un environnement sécurisé et conforme.



Partie 3 – Veille technologique

Afin de garantir la pérennité, la sécurité et l'efficacité de l'infrastructure mise en place, plusieurs axes d'amélioration sont envisagés pour optimiser les performances, la gestion des ressources et renforcer la résilience des services. Voici un aperçu des évolutions possibles pour cette infrastructure fraîchement configurée :

Amélioration des ressources et de l'isolation réseau :

- **Allocation dynamique des ressources** : Grâce à ESXi, il est possible d'ajuster automatiquement les ressources allouées à chaque machine virtuelle en fonction de ses besoins, optimisant ainsi les performances et l'efficacité.
- **Isolation réseau renforcée** : La mise en place de VLANs (Virtual LANs) permet de segmenter davantage les sous-réseaux internes, offrant ainsi une meilleure sécurité et une gestion plus fine du trafic réseau entre les différentes zones de l'infrastructure.

Amélioration de la gestion du trafic et des services réseau :

- **Segmentation avancée du trafic** : En ajoutant des règles spécifiques, il est possible de séparer plus efficacement le trafic interne par type de service, comme les requêtes DNS ou les authentifications AD, améliorant ainsi la sécurité et la gestion des flux réseau.
- **Serveur DHCP sur pfSense** : Configurer pfSense en tant que serveur DHCP permet de gérer dynamiquement les adresses IP des machines virtuelles, réduisant la dépendance à un serveur Windows pour cette fonction et offrant davantage de flexibilité et de contrôle sur la distribution des adresses.

Amélioration de la configuration DHCP :

- **Temps de bail optimisé** : Réduire le temps de bail pour les réseaux à forte mobilité, où les appareils se connectent fréquemment et temporairement, permet une gestion plus dynamique des adresses IP et une utilisation plus efficace des ressources réseau.
- **Redondance DHCP (Failover)** : Mettre en place un serveur DHCP secondaire en mode failover pour assurer la continuité du service en cas de défaillance du serveur principal, garantissant ainsi une distribution ininterrompue des adresses IP et la résilience du réseau.

Amélioration de la gestion des ressources et de la sécurité :

- **Attribution de permissions spécifiques** : Ajouter des commandes **Set-ACL** dans les scripts pour appliquer des permissions personnalisées sur les ressources partagées, assurant ainsi un contrôle d'accès précis en fonction des rôles et des besoins des utilisateurs.
- **Gestion des mots de passe** : Générer des mots de passe temporaires pour les nouveaux utilisateurs et configurer l'obligation de modification lors de leur première connexion, renforçant ainsi la sécurité et garantissant que chaque utilisateur choisisse un mot de passe personnel et sécurisé.

Amélioration de la gestion des groupes et de l'automatisation :

- **Groupes de sécurité GPO** : Associer des **GPO** spécifiques aux groupes de sécurité **Active Directory** pour affiner le contrôle d'accès, en appliquant des politiques de sécurité adaptées à chaque groupe d'utilisateurs ou de machines.
- **Scripts automatisés** : Déployer automatiquement des imprimantes réseau ou des unités mappées via des scripts, simplifiant ainsi la gestion des ressources et garantissant une configuration cohérente et rapide sur toutes les stations de travail.

Amélioration de l'intégration et de la gestion des profils utilisateurs :

- **Scripts d'intégration** : Mettre en place un script de pré-configuration pour automatiser le processus de jonction des machines au domaine, réduisant ainsi les erreurs manuelles et accélérant le déploiement.
- **Redirection de profil utilisateur** : Configurer la redirection des profils utilisateurs vers un serveur dédié pour centraliser et sécuriser les données utilisateurs, tout en facilitant la gestion des profils dans un environnement de domaine.

Centralisation des logs et surveillance :

- Mettre en place une **solution de gestion des logs centralisée** SexiLog pour collecter, analyser et alerter sur des événements de sécurité ou des dysfonctionnements dans l'infrastructure.
- Configurer des **alertes proactives** avec par exemple **PRTG** pour avertir en temps réel des problèmes éventuels sur les serveurs, les services AD/DNS ou les machines clients.

Gestion des mises à jour et patching :

- Installer un **serveur WSUS** pour centraliser les mises à jour Windows et assurer qu'aucun patch de sécurité ne soit omis.
- Installer un **logiciel tiers** pour centraliser les mises à jour de l'infrastructure et assurer qu'aucun patch de sécurité ne soit omis.

Sauvegarde et récupération de données :

- Intégrer une **solution de sauvegarde automatique** pour les données sensibles et les configurations critiques de l'infrastructure (comme les bases de données AD, DNS et les fichiers partagés).
- Tester et affiner régulièrement le processus de **récupération après sinistre (DRP)** afin de garantir la résilience de l'infrastructure en cas de défaillance majeure.

Conclusion

Ces améliorations futures permettraient non seulement d'optimiser les performances, la sécurité et la fiabilité de l'infrastructure, mais aussi d'envisager une évolutivité à long terme en s'adaptant aux besoins croissants de l'entreprise. Chaque étape sera évaluée et mise en œuvre de manière progressive pour garantir une infrastructure stable et résiliente.

ANNEXE

```
# Paramètres de base pour créer plusieurs utilisateurs
$nomDeBase = "tech"  # Nom de base des utilisateurs
$nombreUtilisateurs = 100  # Nombre d'utilisateurs à créer
$cheminDeBase = "\\Srvad\dossier partage"  # Chemin de base pour les dossiers personnels

# Variable pour définir dynamiquement le chemin de l'OU pour les utilisateurs dans AD
$ouPath = "OU=Technique,OU=LAYER,DC=vdb,DC=local"  # Modifie ce chemin si nécessaire
$ouName = "Technique"  # Nom de l'OU cible à vérifier et créer si nécessaire

# Chemin de l'OU pour les groupes
$groupOUPath = "OU=GROUPES_LAYER,DC=vdb,DC=local"  # OU spécifique pour les groupes

# Mot de passe pour chaque utilisateur
$motDePasse = "btssio89$"

# Nom du groupe ou de l'utilisateur administrateur ayant le contrôle
$administrateur = "Administrateurs"  # Nom du groupe administrateur local

# Variable pour définir dynamiquement le groupe dans lequel ajouter les utilisateurs
$groupName = "g_Techs"  # Nom du groupe à créer et auquel ajouter les utilisateurs

# Vérifier si l'OU pour les utilisateurs existe et la créer si elle est absente
if (-Not (Get-ADOrganizationalUnit -Filter {Name -eq $ouName} -SearchBase
"OU=LAYER,DC=vdb,DC=local" -ErrorAction SilentlyContinue)) {
New-ADOrganizationalUnit -Name $ouName -Path "OU=LAYER,DC=vdb,DC=local"
Write-Host "L'OU '$ouName' a été créée dans 'OU=LAYER,DC=vdb,DC=local'."
} else {
Write-Host "L'OU '$ouName' existe déjà dans 'OU=LAYER,DC=vdb,DC=local'."
}

# Vérifier si le groupe existe dans l'OU pour les groupes et le créer si nécessaire
if (-Not (Get-ADGroup -Filter {Name -eq $groupName} -SearchBase $groupOUPath -ErrorAction
SilentlyContinue)) {
New-ADGroup -Name $groupName -GroupScope Global -Path $groupOUPath -GroupCategory
Security
Write-Host "Le groupe '$groupName' a été créé dans '$groupOUPath'."
} else {
Write-Host "Le groupe '$groupName' existe déjà dans '$groupOUPath'."
}

# Boucle pour créer chaque utilisateur avec un numéro incrémental
for ($i = 1; $i -le $nombreUtilisateurs; $i++) {
# Définir les informations de l'utilisateur
$samAccountName = "$nomDeBase$i"  # Exemple : user1, user2, user3...
$userPrincipalName = "$samAccountName@vdb.local"
$repertoirePersonnel = Join-Path -Path $cheminDeBase -ChildPath $samAccountName

# Création de l'utilisateur dans Active Directory
New-ADUser `
-Name $samAccountName `
```

```
-Path $ouPath `
-AccountPassword (ConvertTo-SecureString $motDePasse -AsPlainText -Force) `
-UserPrincipalName $userPrincipalName `
-SamAccountName $samAccountName `
-Enabled $true

Write-Host "Utilisateur '$samAccountName' créé dans Active Directory avec succès."

# Ajouter l'utilisateur au groupe spécifié
Add-ADGroupMember -Identity $groupName -Members $samAccountName
Write-Host "Utilisateur '$samAccountName' ajouté au groupe '$groupName'."

# Vérifier si le dossier personnel existe déjà
if (-Not (Test-Path -Path $repertoirePersonnel)) {
# Créer le répertoire personnel
New-Item -ItemType Directory -Path $repertoirePersonnel -Force
Write-Host "Dossier personnel créé pour $samAccountName à $repertoirePersonnel."
} else {
Write-Host "Le dossier personnel pour $samAccountName existe déjà à $repertoirePersonnel."
}

# Récupérer les ACL du dossier personnel
$acl = Get-Acl -Path $repertoirePersonnel

# Désactiver l'héritage et supprimer les permissions héritées
$acl.SetAccessRuleProtection($true, $false)

# Supprimer toutes les règles d'accès existantes
$acl.Access | ForEach-Object { $acl.RemoveAccessRuleAll($_) }

# Ajouter les droits de contrôle total pour l'utilisateur
$userAccessRule = New-Object
System.Security.AccessControl.FileSystemAccessRule("$samAccountName", "FullControl",
"ContainerInherit,ObjectInherit", "None", "Allow")
$acl.AddAccessRule($userAccessRule)

# Ajouter les droits de contrôle total pour les administrateurs
$adminAccessRule = New-Object
System.Security.AccessControl.FileSystemAccessRule("$administrateur", "FullControl",
"ContainerInherit,ObjectInherit", "None", "Allow")
$acl.AddAccessRule($adminAccessRule)

# Appliquer les modifications ACL sur le dossier
Set-Acl -Path $repertoirePersonnel -AclObject $acl

Write-Host "Permissions de contrôle total définies pour $samAccountName et $administrateur sur
$repertoirePersonnel."
}
```