

Windows Serveur et Active Directory

Sommaire:

1/ Matrice Permissions Groupe et utilisateur et Diagramme ULM

2/ Installation de Windows Serveur, Active Directory.

3/ Création des Unités d'organisation et des sous unité (UO)

4/ Création du script powershell des Unités d'organisation, groupes et utilisateurs a partir d'un fichier csv

5/ Création et Connexion des postes de travail

6/ Script automatisation sécurité

7/ Monter les lecteurs réseaux

8/ Monter les IMPRIMANTES

9/ Contrôleur DOMAINE Seconfaire et RéPLICATION

10/Création d'un Script Powershell Pour les Dossiers Imprimante et GPO

1/ Matrice Permissions Groupe et utilisateur et Diagramme ULM

Matrice des permissions pour les différents groupes d'utilisateurs et les dossiers partagés suivant l'établissement :

Établissement / Accès au dossier	Sièges 06	Gabres 06	Cascades 94	Hermitages 83
Sièges 06	Complet	Complet	Complet	Complet
Gabres 06	Aucun	Complet	Aucun	Aucun
Cascades 94	Aucun	Aucun	Complet	Aucun
Hermitages 83	Aucun	Aucun	Aucun	Complet

Matrice des permissions pour les différents groupes d'utilisateurs et les dossiers partagés :

Groupes / Dossiers	Médical M	Administratif S	Animation A?	Technique T	Compta P	Cadres X	Bibles Z
Cadres	Complet	Complet	Complet	Complet	Complet	Complet	Complet
Compta	Aucun	Complet	Lecture	Aucun	Complet	Aucun	Lecture
Animation	Lecture	Complet	Complet	Aucun	Aucun	Aucun	Lecture
Médical (Médecin, IDE, secrétaire médicale)	Complet	Complet	Lecture	Aucun	Aucun	Aucun	Lecture
Médical (AS et ASH)	Lecture	Complet	Lecture	Aucun	Aucun	Aucun	Lecture
Technique	Aucun	Complet	Lecture	Complet	Aucun	Aucun	Lecture
Autres	Aucun	Complet	Lecture	Aucun	Aucun	Aucun	Lecture

--	--	--	--	--	--	--	--	--

Voici la matrice des permissions spécifiques pour le siège :

Poste / Dossiers	Médical M	Administratif S	Animation A?	Technique T	Compta P	Cadres X	Bibles Z
DG et DRH	Lecture	Complet	Complet	Complet	Complet	Complet	Complet
Resp Technique	Aucun	Aucun	Aucun	Complet	Aucun	Aucun	Aucun
Chef Compta	Aucun	Aucun	Aucun	Aucun	Complet	Aucun	Aucun
Qualiticien	Lecture	Complet	Lecture	Lecture	Lecture	Lecture	Complet

DG et DRH : ont un accès complet à tous les dossiers sauf Médical où ils ont un accès en lecture seule.

Responsable Technique : a un accès complet uniquement aux dossiers Techniques.

Chef Comptabilité : a un accès complet uniquement aux dossiers Comptabilité.

Qualiticien : a un accès complet aux dossiers Administratif et Bibles, et un accès en lecture seule sur les autres dossiers.

Le réseaux aura donc comme dossier:

U: Dossier personnel des utilisateurs

M: Dossier Médical

S: Administratif

A: Animation

P: Compta

Z: Bibles

T: Technique

X: Cadres

Nous aurons donc comme groupes :

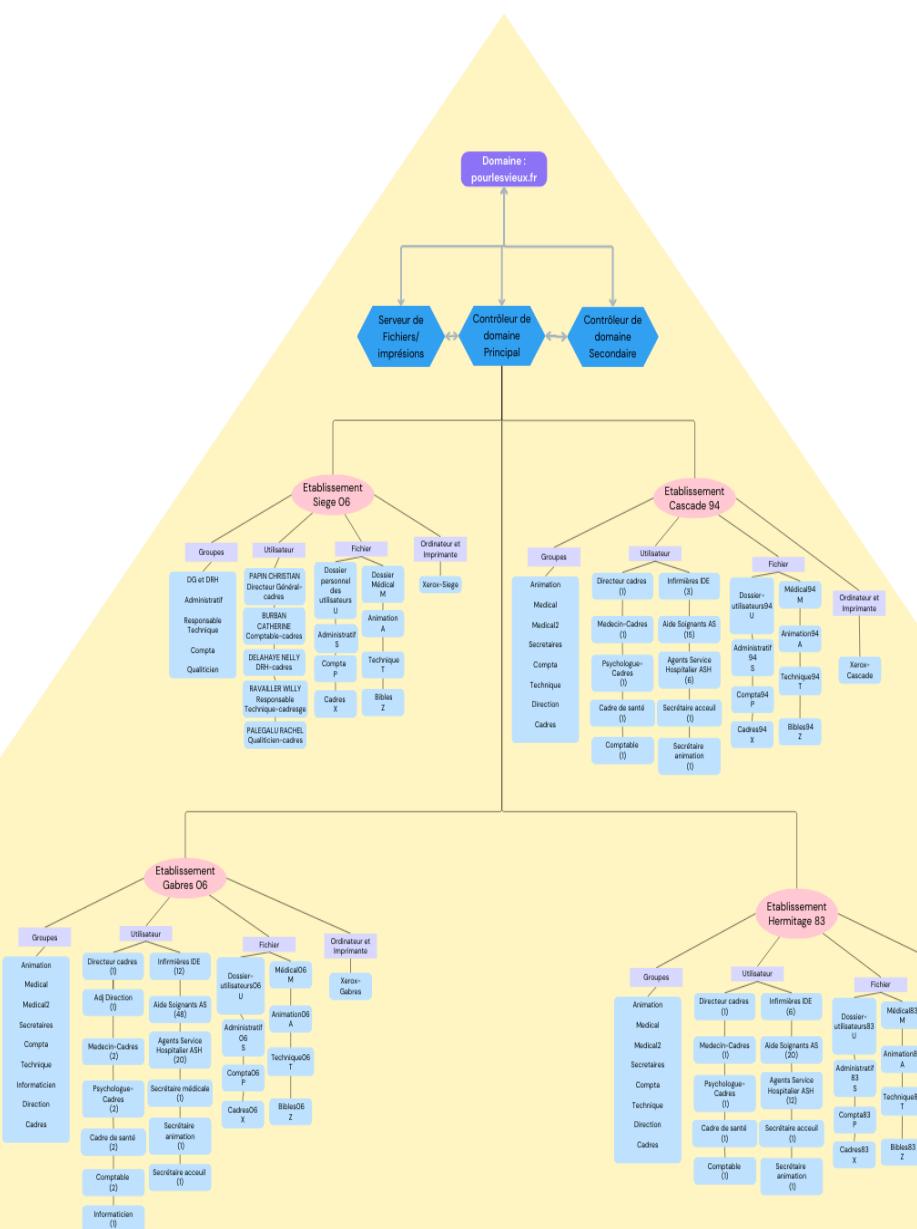
4 Groupes pour les Sites:

- Sièges 06
- Gabres 06
- Cascades 94
- Héritages 83

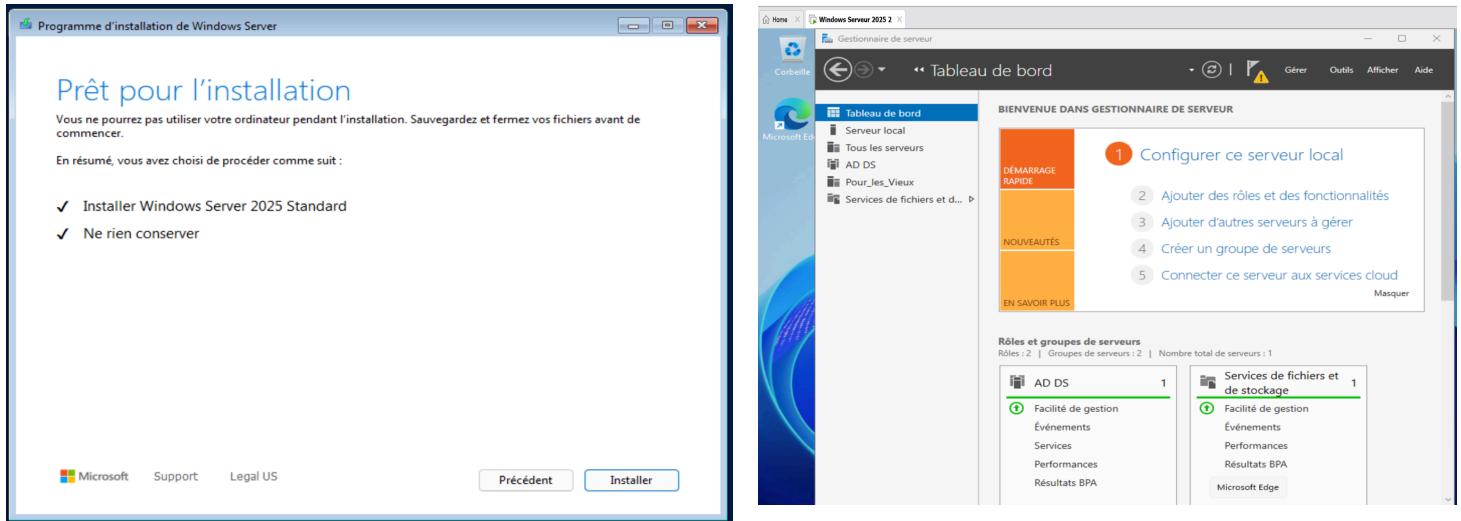
Groupes Pour les droits des fichiers:

- Animation
- Medical
- Medical2
- Secrétaires
- Compta
- Technique
- Informaticien
- Direction
- Cadres
- DG et DRH
- Administratif
- Responsable Technique
- Qualiticien

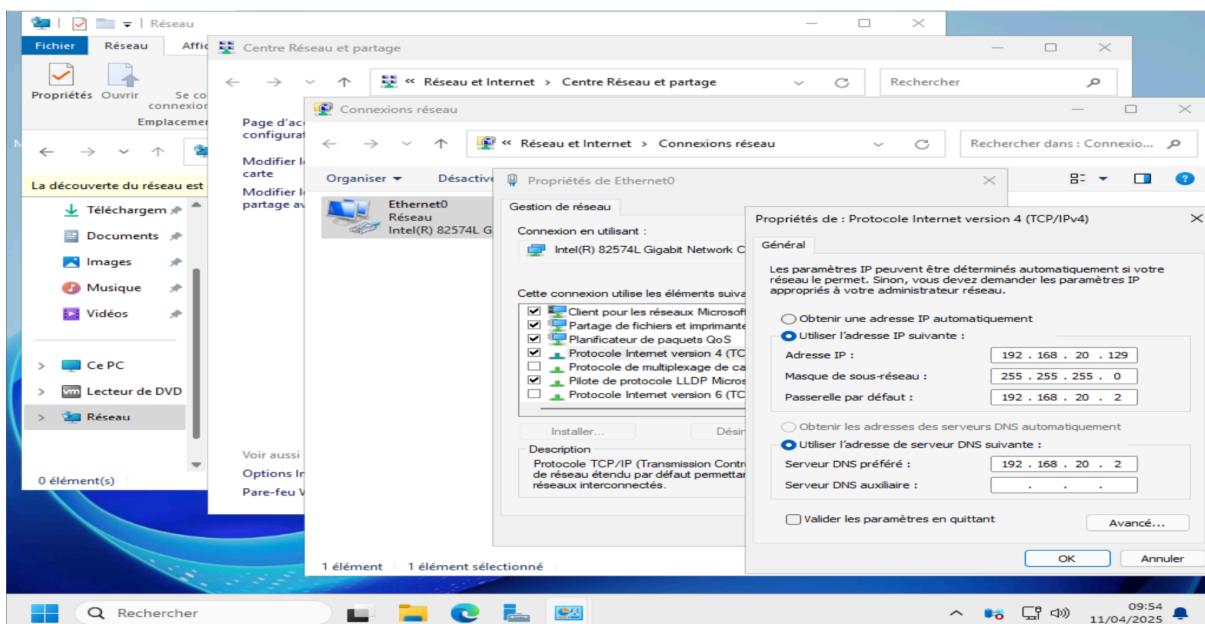
Diagramme ULM:



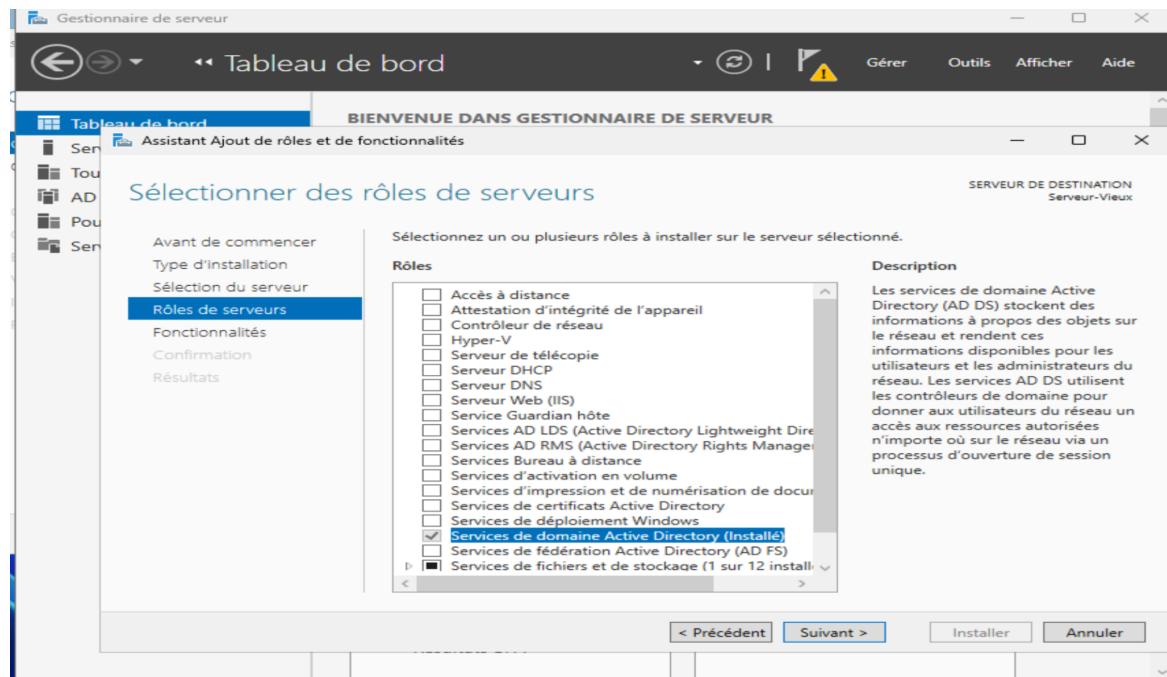
2/ Installation de Windows Serveur, Active Directory.



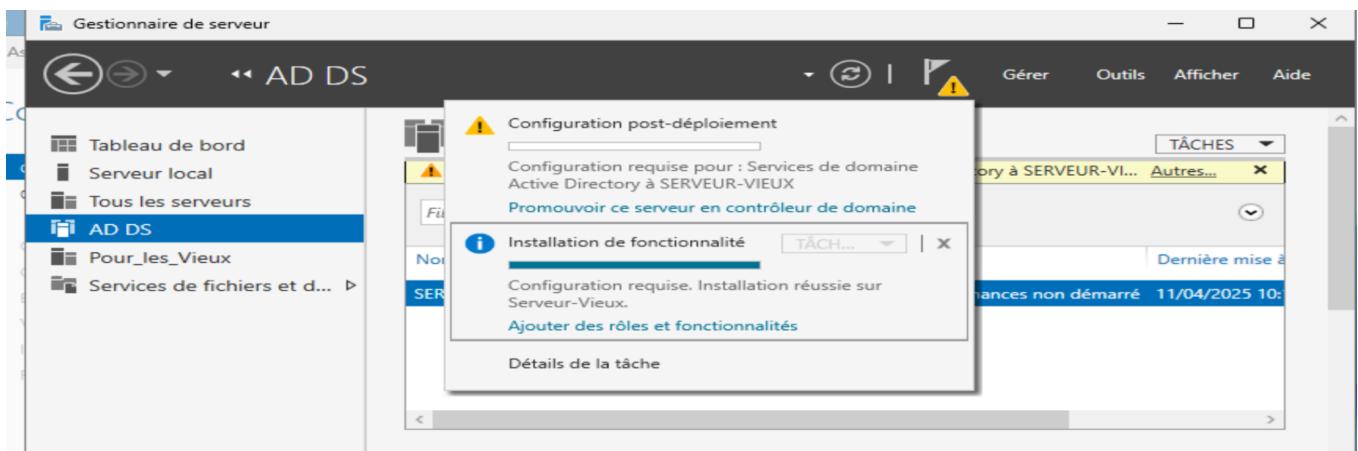
Je modifie mon adresse IP et DNS, je les mets en fixe :
dans réseau > paramètre > modifier les paramètres de la carte >
propriété > désactiver le IPV6 et modifier les paramètres de IPV4 en fixe



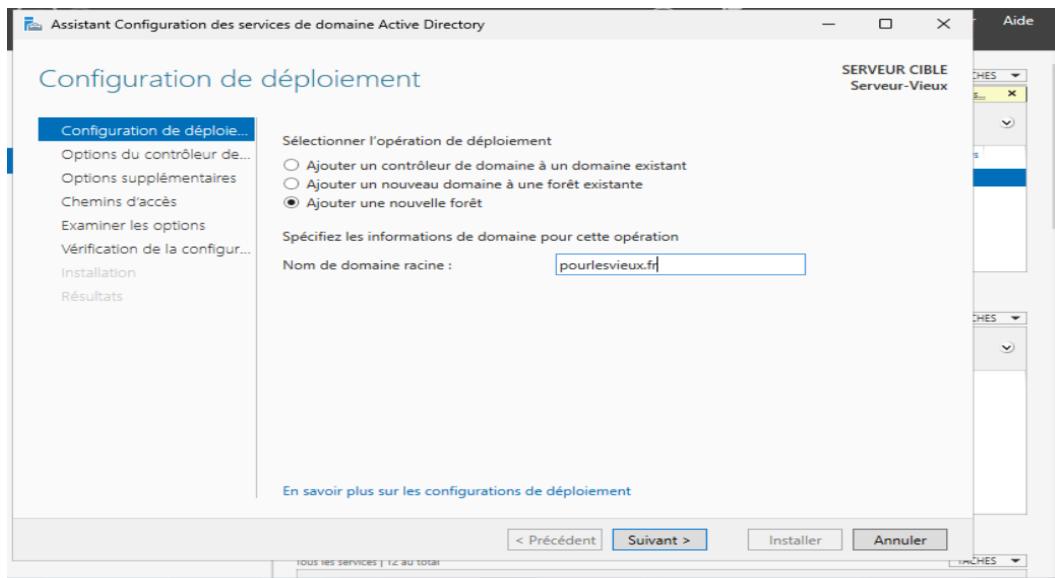
J'installe un Serveur Active Directory:



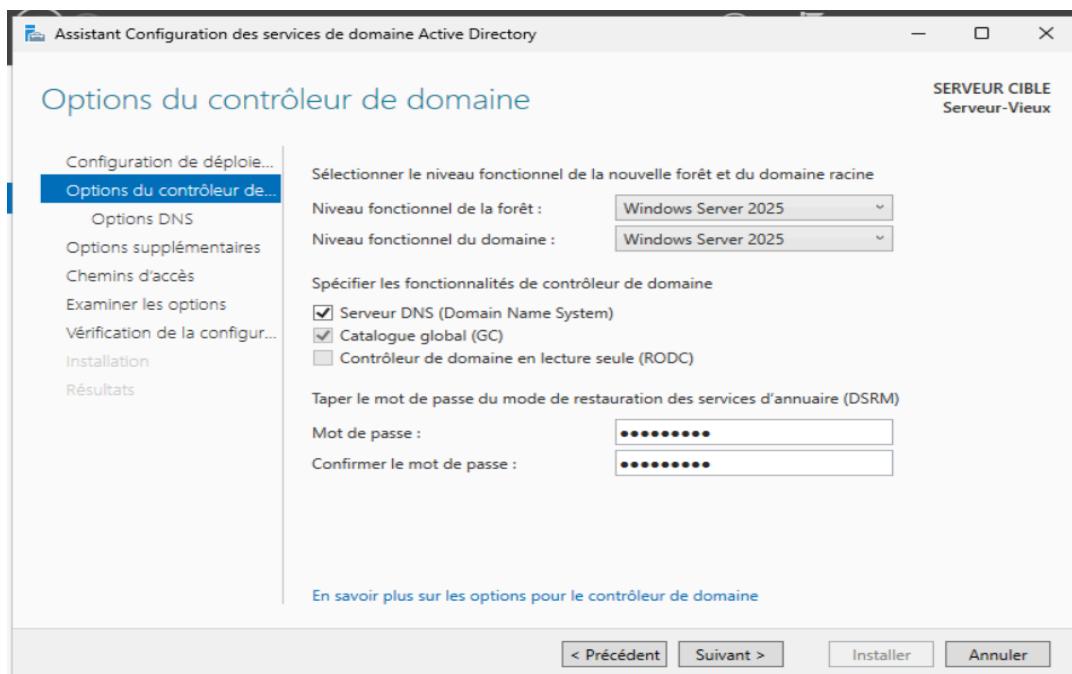
Je le Prometheus en contrôleur de domaine :



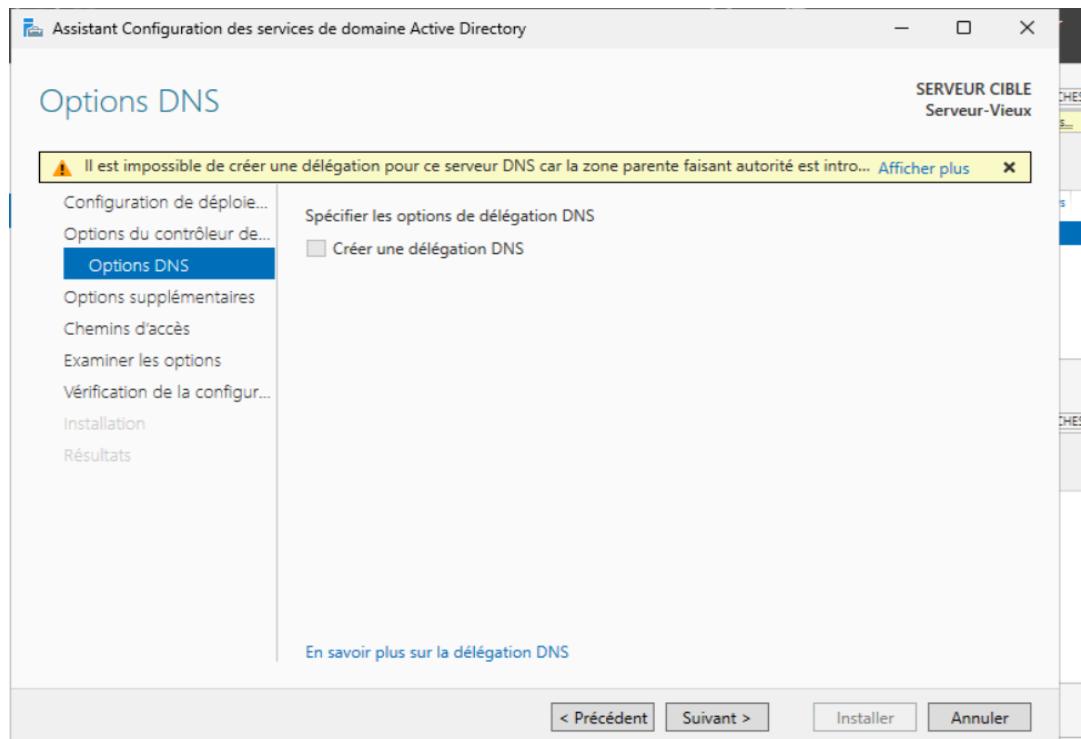
J'ajoute une forêt avec le nom de domaine :



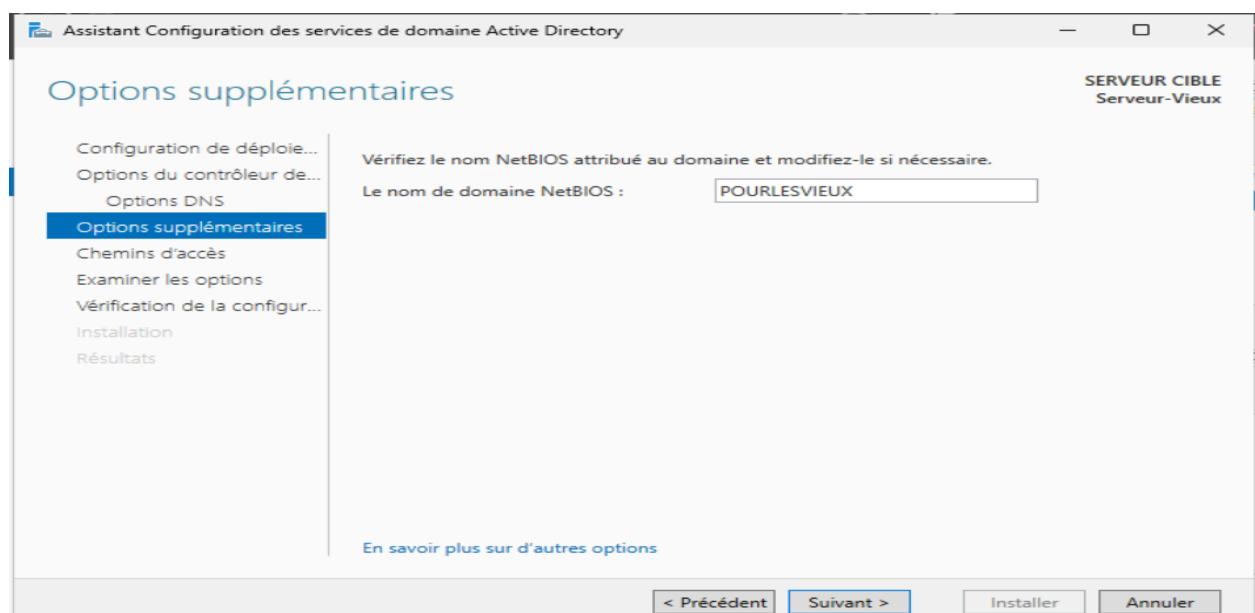
Je configure les options et je crée le mdp de restauration:



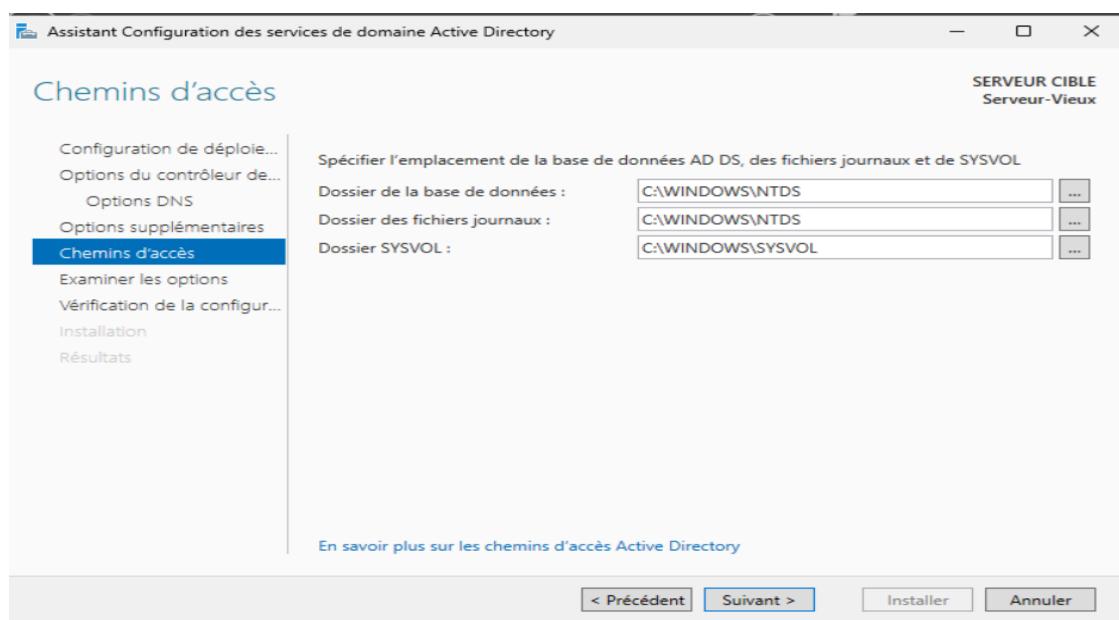
Comme il s'agit d'un nouveau serveur DNS pour une nouvelle zone, je continue sans créer un DNS:



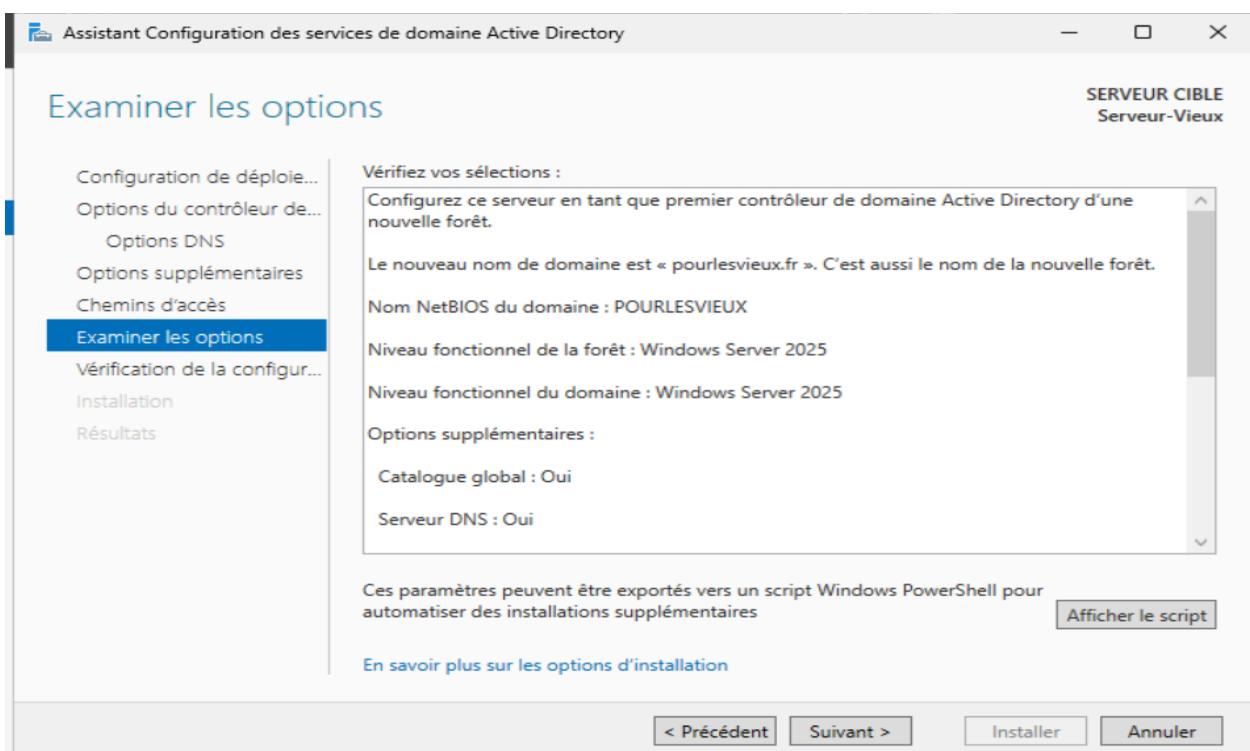
J'Indique un nom NETBIOS pour le domaine, à savoir un nom court et qui ne s'appuie pas sur DNS pour être résolu :



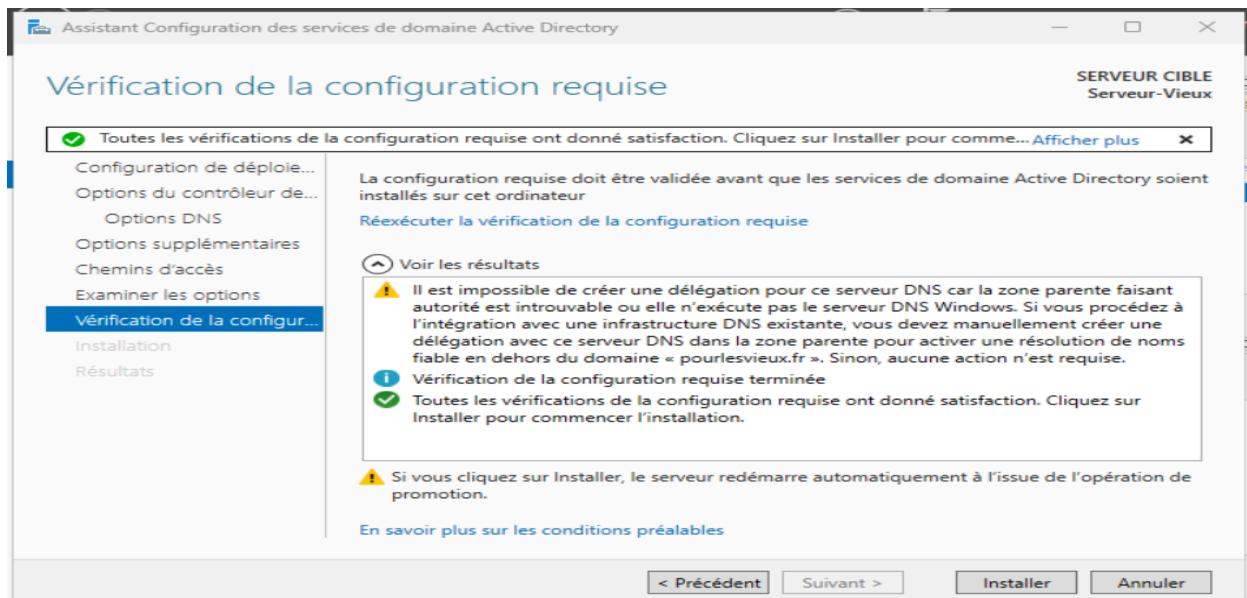
Je laisse les chemins par défaut et poursuis :



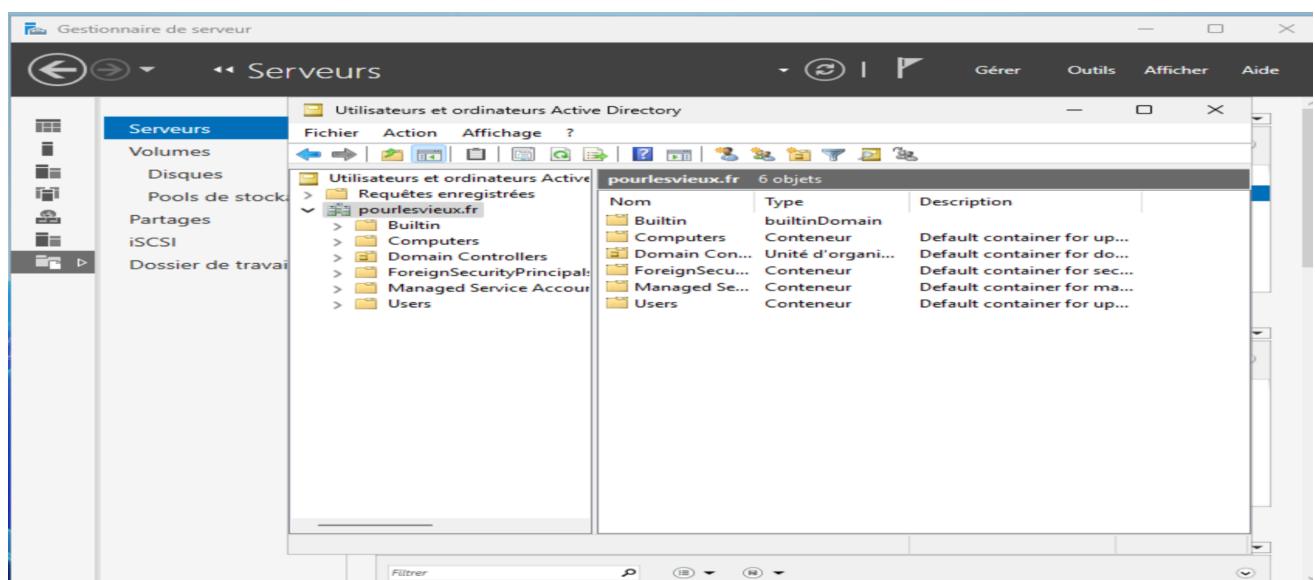
Je vérifie les options et continue :



Je finis en cliquant sur installer pour démarrer la création de votre domaine et la configuration du DC :



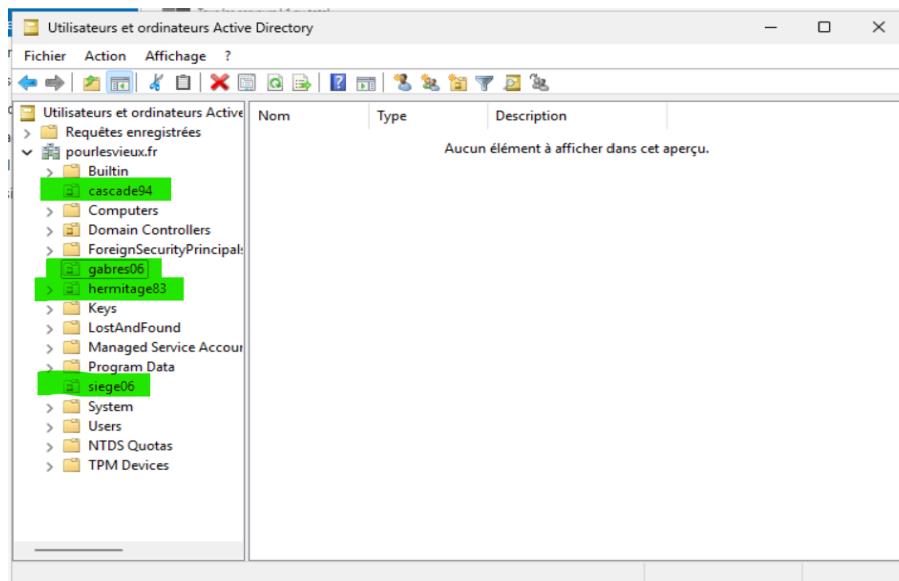
Dès lors que l'installation est terminée et que votre serveur a redémarré, vous pouvez commencer à utiliser votre domaine Active Directory, notamment avec les consoles "Utilisateurs et ordinateurs Active Directory" et "Centre d'administration Active Directory" qui servent à gérer les objets dans l'annuaire (utilisateurs, ordinateurs, serveurs, etc.).



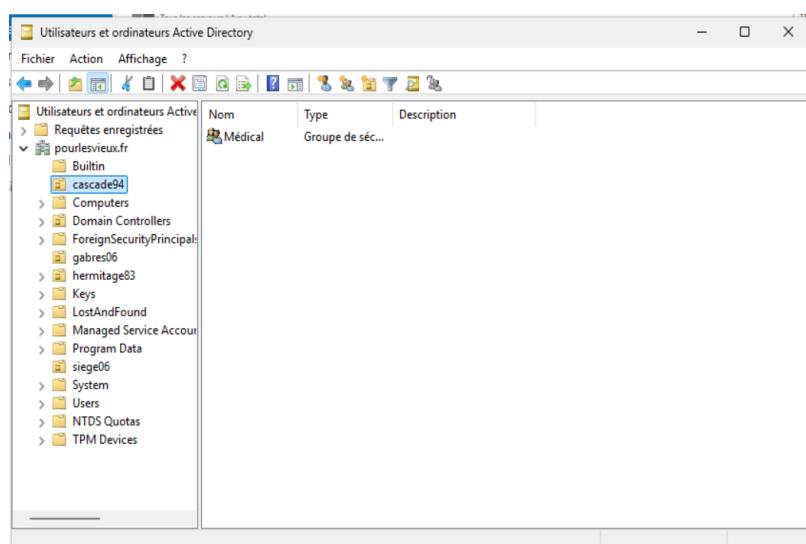
3/ Créeation des Unités d'organisation et des sous unité (OU)

Je commence par créer mes quatres unités organisationnelles, c'est-à-dire mes quatres agences.

dans outils > utilisateurs et ordinateurs actives directory>ajouter une unité organisationnel :

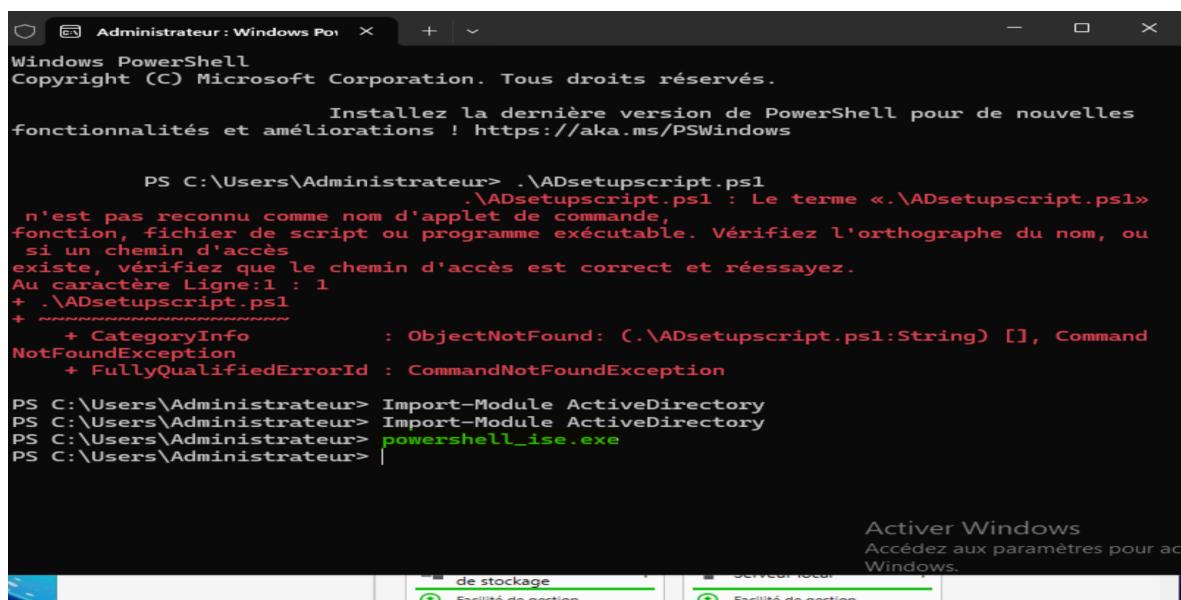


puis je rajoute les groupes qui me permettront de gérer les droits accès des utilisateurs :



4/ Création du script powershell des Unités d'organisation, groupes et utilisateurs a partir d'un fichier csv

J'ouvre le powershell_ise.exe pour faire mon script



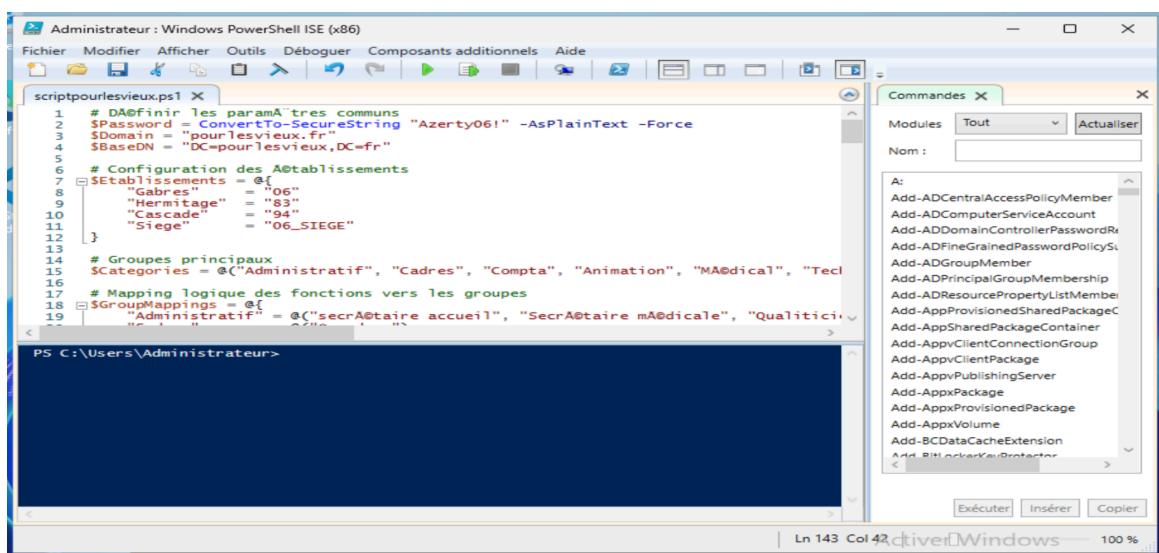
```
Administrator : Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindows

PS C:\Users\Administrateur> .\ADsetupscript.ps1
.\ADsetupscript.ps1 : Le terme «.\ADsetupscript.ps1»
n'est pas reconnu comme nom d'applet de commande,
fonction, fichier de script ou programme exécutable. Vérifiez l'orthographe du nom, ou
si un chemin d'accès
existe, vérifiez que le chemin d'accès est correct et réessayez.
Au caractère Ligne:1 : 1
+ .\ADsetupscript.ps1
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (.\ADsetupscript.ps1:String) [], Command
NotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\Administrateur> Import-Module ActiveDirectory
PS C:\Users\Administrateur> Import-Module ActiveDirectory
PS C:\Users\Administrateur> powershell_ise.exe
PS C:\Users\Administrateur>
```

Activer Windows
Accédez aux paramètres pour activer Windows.



```
Administrator : Windows PowerShell ISE (x86)
Fichier Modifier Afficher Outils Déboguer Composants additionnels Aide
```

```
scriptpourlesvieux.ps1 X
1 # Définir les paramètres communs
2 $Password = ConvertTo-SecureString "Azerty06!" -AsPlainText -Force
3 $Domain = "pourlesvieux.fr"
4 $BaseDN = "DC=pourlesvieux,DC=fr"
5
6 # Configuration des établissements
7 $Etablissements = @{
8     "Gabres"        = "06"
9     "Hermitage"     = "83"
10    "Cascade"       = "94"
11    "Siege"         = "06_SIEGE"
12 }
13
14 # Groupes principaux
15 $Categories = @("Administratif", "Cadres", "Compta", "Animation", "MAtériel", "Technique")
16
17 # Mapping logique des fonctions vers les groupes
18 $GroupMappings = @{
19     "Administratif" = @("secrétaire accueil", "Secrétaire mAtérale", "Qualité")
20 }
```

Commandes X

Modules Tout Actualiser

Nom :

A:

- Add-ADCentralAccessPolicyMember
- Add-ADComputerServiceAccount
- Add-ADDomainControllerPasswordPolicy
- Add-ADFineGrainedPasswordPolicy
- Add-ADGroupMember
- Add-ADPrincipalGroupMembership
- Add-ADResourcePropertyListMember
- Add-AppProvisionedSharedPackage
- Add-AppSharedPackageContainer
- Add-AppClientConnectionGroup
- Add-AppClientPackage
- Add-AppPublishingServer
- Add-AppxPackage
- Add-AppxProvisionedPackage
- Add-AppxVolume
- Add-BCDDataCacheExtension
- Add-BitLockerKeyProtector

Exécuter Insérer Copier

Ln 143 Col 42 drive:\Windows 100 %

```

# Importer le module Active Directory
Import-Module ActiveDirectory

# Definir les parametres communs
$Password = ConvertTo-SecureString "Azerty06!" -AsPlainText -Force
$Domain = "pourlesvieux.fr"

# Configuration des etablissements et departements
$Etablissements = @{
    "Gabres"      = "06"
    "Hermitage"   = "83"
    "Cascade"     = "94"
    "Siege"       = "06"
}

# Creation des OU principales formatees
foreach ($établissement in $Etablissements.Keys) {
    $dept = $Etablissements[$établissement]
    $ouName = "$établissement($dept)"
    $ouPath = "OU=$ouName,DC=pourlesvieux,DC=fr"

    # Creer l'OU principale avec le departement
    try {
        New-ADOrganizationalUnit -Name $ouName -Path "DC=pourlesvieux,DC=fr" -ErrorAction Stop
        Write-Host "OU $ouName creee"
    } catch {
        Write-Warning "L'OU $ouName existe deja"
    }

    # Creer les sous-OUs
    $subOUs = @("Utilisateurs", "Groupes", "Ordinateurs")
    foreach ($subOU in $subOUs) {
        try {
            New-ADOrganizationalUnit -Name $subOU -Path $ouPath -ErrorAction Stop
            Write-Host "Sous-OU $subOU creee dans $ouName"
        } catch {
            Write-Warning "La sous-OU $subOU existe deja dans $ouName"
        }
    }
}

```

Import les modules

Lie de Numéro de département à l'établissement

crée-les OU principal des établissements au format :

NomNumérodépartement
par exemple: Gabres06

Crée les Sous-OUs dans les établissements (Utilisateurs, Groupes , Ordinateurs)

```

41 # Creer les groupes departmentaux
42 $groupes = @("Administratif", "Cadres", "Compta", "Animation", "Medical", "Technique")
43 foreach ($groupe in $groupes) {
44     $nomGroupe = "$groupe$dept"
45     try {
46         New-ADGroup -Name $nomGroupe `-
47                     -GroupCategory Security `-
48                     -GroupScope Global `-
49                     -Path "OU-Groupes,$ouPath" `-
50                     -ErrorAction Stop
51         Write-Host "Groupe $nomGroupe cree"
52     } catch {
53         Write-Warning "Le groupe $nomGroupe existe deja"
54     }
55 }
56

57 # Definir les regles d'appartenance aux groupes
58 $groupMappings = @{
59     "Administratif" = "AS|ASH|secrétaire|Maitresse de Maison|Directeur|DRH|Qualiticien"
60     "Cadres"        = "cadres|cadre|Directeur|DRH|Qualiticien|responsable"
61     "Compta"        = "Comptable"
62     "Animation"     = "Animation"
63     "Medical"       = "Medecin|Psychologue|IDE|Infirmier"
64     "Technique"     = "technique|Informaticien"
65 }
66

67 # Importer le CSV et creer les utilisateurs
68 $users = Import-Csv -Path "./users.csv" -Delimiter ","
69

70 foreach ($user in $users) {
71     $baseEtablissement = $user.ETABLISSEMENT
72     $dept = $Etablissements[$baseEtablissement]
73     $ouName = "$baseEtablissement($dept)"
74     $fonction = $user.FONCTION
75

76     # Formater le nom d'utilisateur
77     $username = $($user.PRENOM.ToLower()) + "." + $($user.NOM.ToLower()) -replace '[éèààùù]', 'e' -replace '[ââîîôô]', 'a' -replace '[ââîîôô]', 'i' -replace '[ââññ]', 'o' -replace '[ââññ]', 'u'
78     $userOU = "OU=Utilisateurs,OU=$ouName,DC=pourlesvieux,DC=fr"

```

Création des groupes dans la sous-OU “groupes”

Création du mappings pour diriger les utilisateurs dans le bon groupes

Importé le fichier csv

Formatage des noms users

```

81 # Creer l'utilisateur
82 try {
83     New-ADUser -GivenName $user.PRENOM ` 
84         -Surname $user.NOM ` 
85         -Name "$($user.PRENOM) $($user.NOM)" ` 
86         -SamAccountName $username ` 
87         -UserPrincipalName "$username@$Domain" ` 
88         -AccountPassword $Password ` 
89         -Enabled $true ` 
90         -PasswordNeverExpires $false ` 
91         -ChangePasswordAtLogon $true ` 
92         -Path $userOU ` 
93         -ErrorAction Stop
94
95 Write-Host "Utilisateur $username cree dans $ouName"
96
97 # Determiner les groupes
98 $groupsToAdd = @()
99 foreach ($groupe in $groupMappings.Keys) {
100     if ($fonction -match $groupMappings[$groupe]) {
101         $groupsToAdd += "$groupe$dept"
102     }
103 }
104
105 # Ajouter aux groupes (en evitant les doublons)
106 $groupsToAdd = $groupsToAdd | Select-Object -Unique
107 foreach ($groupe in $groupsToAdd) {
108     try {
109         Add-ADGroupMember -Identity $groupe -Members $username -ErrorAction Stop
110         Write-Host " Ajoute au groupe $groupe"
111     } catch {
112         Write-Warning "Erreur d'ajout au groupe $groupe : $_"
113     }
114 }
115
116 } catch {
117     Write-Warning "Erreur lors de la creation de $username : $_"
118 }
119
120 Write-Host "Script execute avec succes !"

```

Création des users

Determiner les groupes de l'utilisateurs

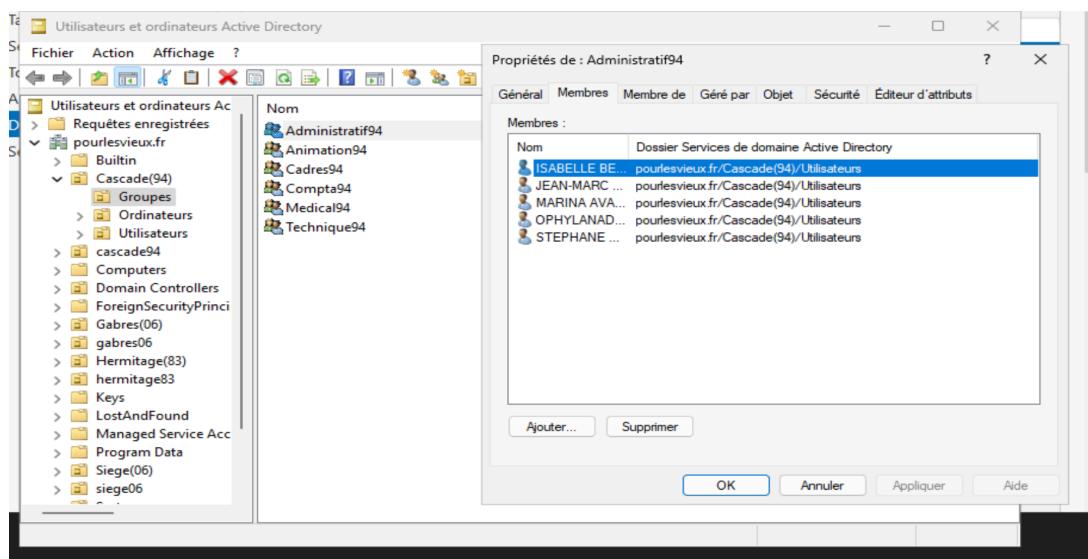
Ajouter au groupes l'utilisateurs en évitant les doublons

fin du script

Je lance le script dans le PowerShell_ISE

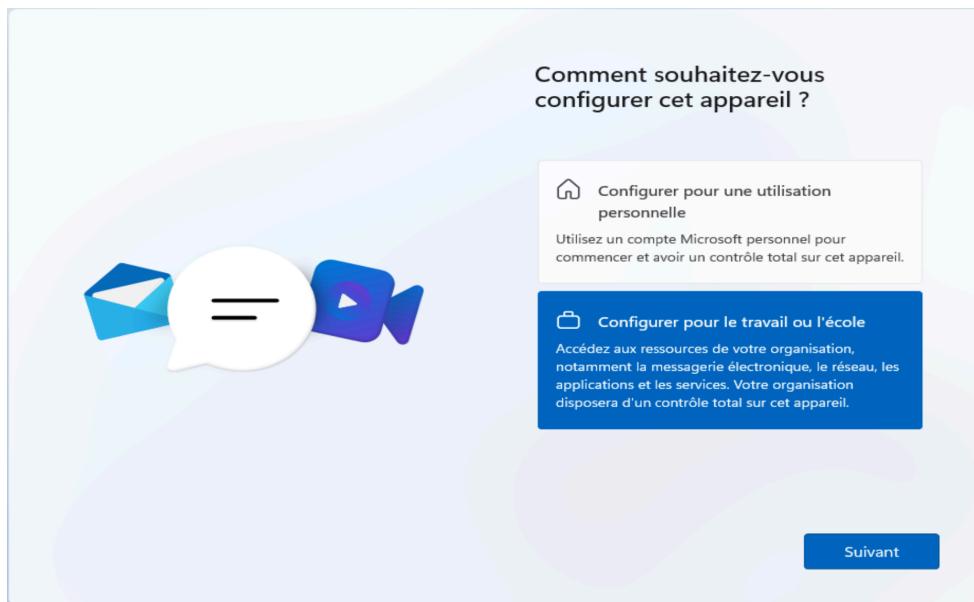
```
Ajoute au groupe Administratif83
Utilisateur roland.parfait cree dans Hermitage(83)
Ajoute au groupe Technique83
Utilisateur charlotte.pic cree dans Hermitage(83)
Ajoute au groupe Administratif83
Ajoute au groupe Cadres83
Utilisateur fanny.portanier cree dans Hermitage(83)
Utilisateur julie.rhem cree dans Hermitage(83)
Ajoute au groupe Medical83
Utilisateur armelle.sanseau cree dans Hermitage(83)
Ajoute au groupe Administratif83
Utilisateur catherine.burban cree dans Siege(06)
Ajoute au groupe Cadres06
Ajoute au groupe Compta06
Utilisateur nelly.delahaye cree dans Siege(06)
Ajoute au groupe Administratif06
Ajoute au groupe Cadres06
Utilisateur rachel.palegalu cree dans Siege(06)
Ajoute au groupe Administratif06
Ajoute au groupe Cadres06
Utilisateur christian.papin cree dans Siege(06)
Ajoute au groupe Administratif06
Ajoute au groupe Cadres06
Utilisateur willy.ravailler cree dans Siege(06)
Ajoute au groupe Technique06
Ajoute au groupe Cadres06
Script execute avec succes !
PS C:\Users\Administrateur>
```

Je peux voir que les UO, sous UO , GPO et User ont bien été créée.

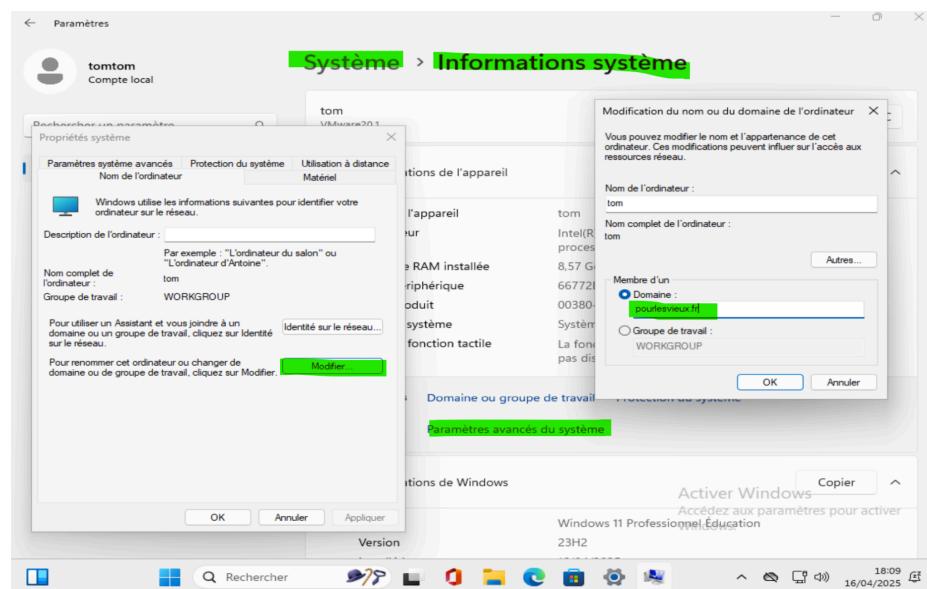


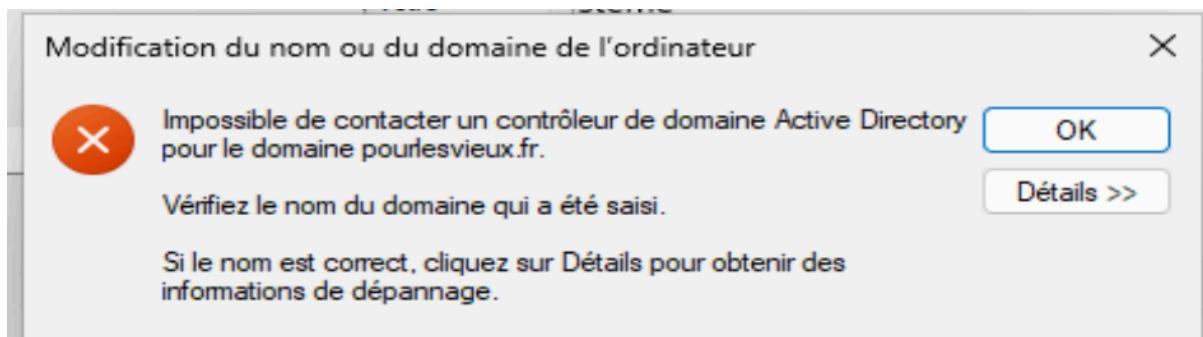
5/ Crédit et Connexion des postes de travail

J'installe un windows 11 configurer en environnement entreprise



Dans système > information système > paramètre avancer du système > modifier > mettre le nom de domaine du serveur.





Si un message d'erreur apparaît pour le DNS, il faut dans la carte réseau modifier le DNS de IPv4 et mettre le DNS du serveur.

Paramètre du serveur:

Modifier les paramètres IP

IPv4

Activé

Adresse IP: 192.168.20.129

Masque de sous-réseau: 255.255.255.0

Passerelle: 192.168.20.2

DNS préféré: 192.168.20.129

DNS sur HTTPS: Désactivé

Autre DNS: 8.8.8.8

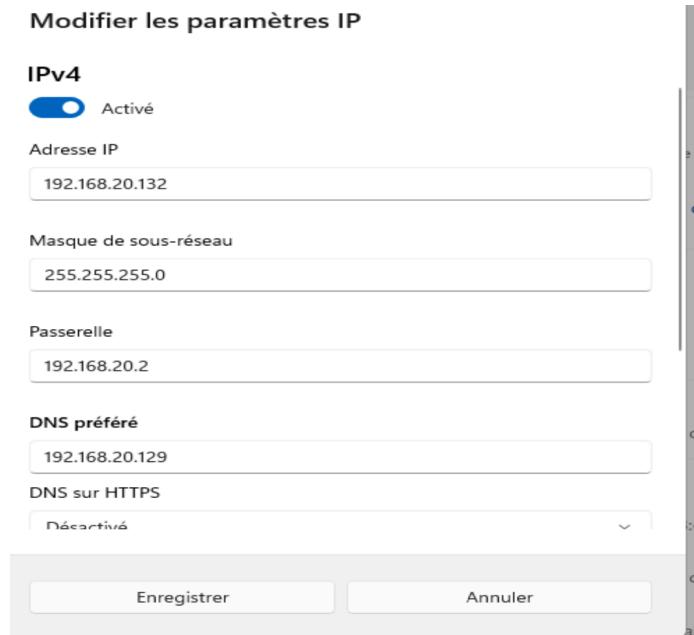
DNS sur HTTPS: Désactivé

IPv6

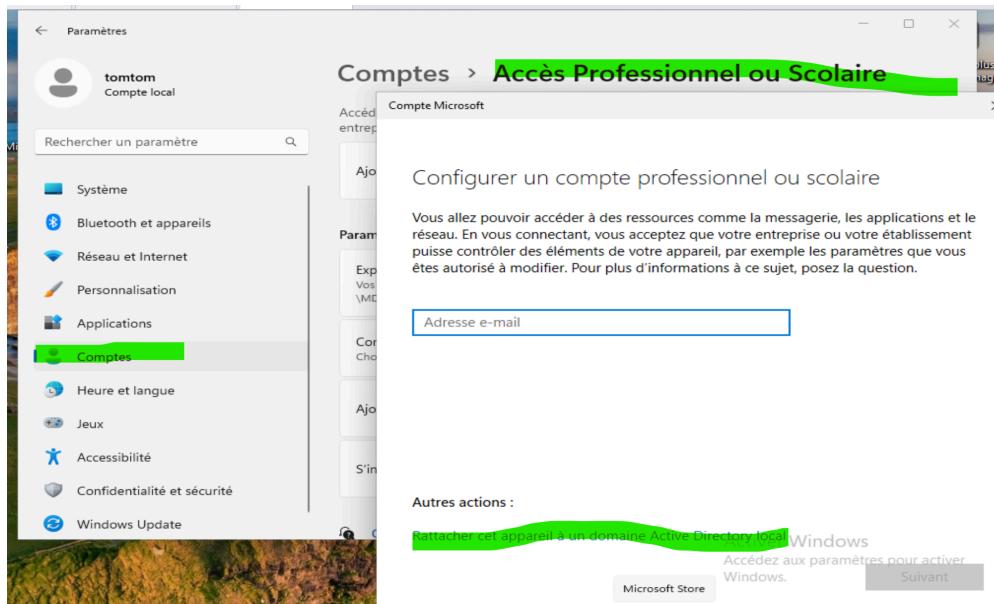
Désactivé

Enregistrer Annuler

Paramètre du client :



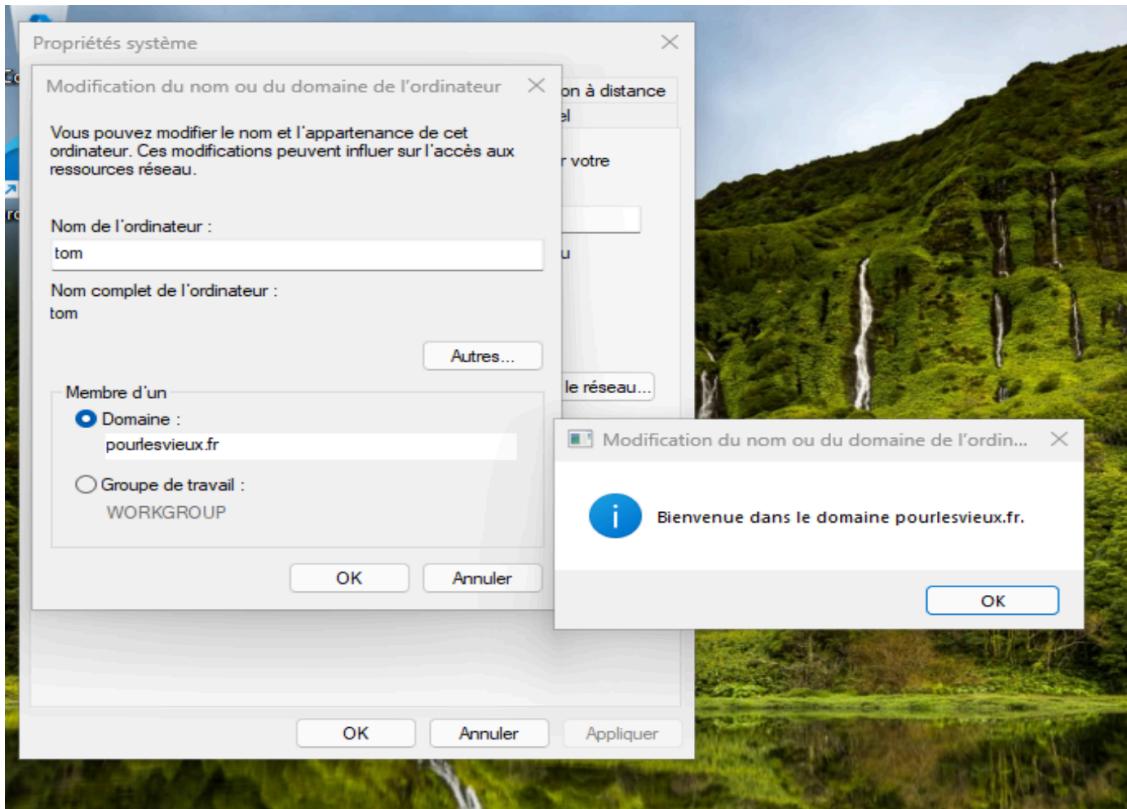
Pour me connecter au serveur je vais dans:
paramètre> comptes > ajouter un compte professionnel ou scolaire> se connecter > rattacher cet appareil a un domain Active Directory local



Je rentre les identifiants de connections:

Identifiant connection: Administrateur

Mon mdp admin



Cette opération peut prendre quelques minutes.

N'éteignez pas votre PC.

Cella

configure m'as
séssio...

The screenshot shows the Windows Settings interface under the 'Comptes' (Accounts) section. On the left, a sidebar lists various settings categories: Système, Bluetooth et appareils, Réseau et Internet, Personnalisation, Applications, Comptes (which is selected and highlighted in blue), Heure et langue, Jeux, Accessibilité, Confidentialité et sécurité, and Windows Update. The main pane displays the user profile for 'Administreuteur' (Administrator) at 'pourlesvieux.fr'. The profile picture is a placeholder. The user's name is listed as 'POURLESVIEUX\ADMINISTRATEUR' with the full email 'POURLESVIEUX\Administreuteur' and the role 'Administrateur'. Below the profile, there are five sections: 'Vos informations' (Your information), 'E-mail et comptes' (Email and accounts), 'Options de connexion' (Connection options), 'Autres utilisateurs' (Other users), and 'Sauvegarde Windows' (Windows backup). Each section has a brief description and a right-pointing arrow indicating further options.

Puis je peux me connecter avec ma session
Identifiant: anne.buisine@pourlesvieux.fr
Password par défaut: Azerty06!



Autre utilisateur

anne.buisine@pourlesvieux.fr

•••••••|

✉ ➔

Connectez-vous à pourlesvieux.fr

Comment me connecter à un autre domaine ?

mtom



Autre utilisateur

anne.buisine@pourlesvieux.fr

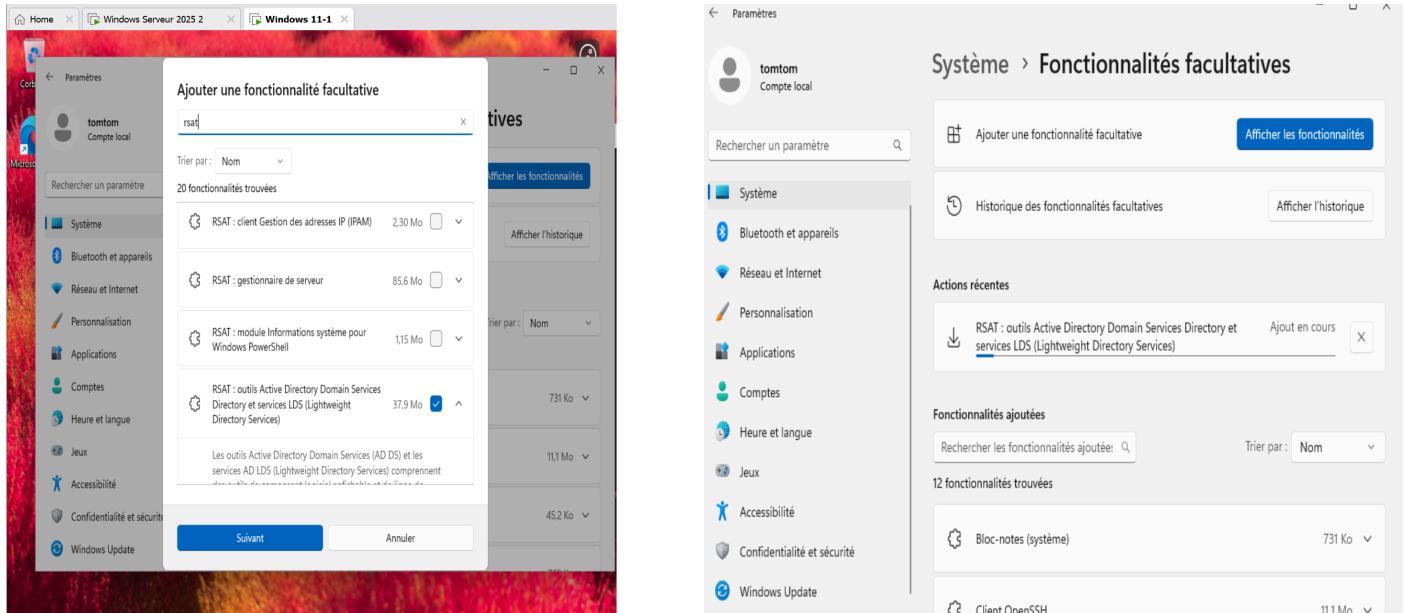
✉ ➔

Connectez-vous à pourlesvieux.fr

Comment me connecter à un autre domaine ?

Annuler

(pas obligatoire):
Je dois aussi Ajouter le module RSAT a windows 11



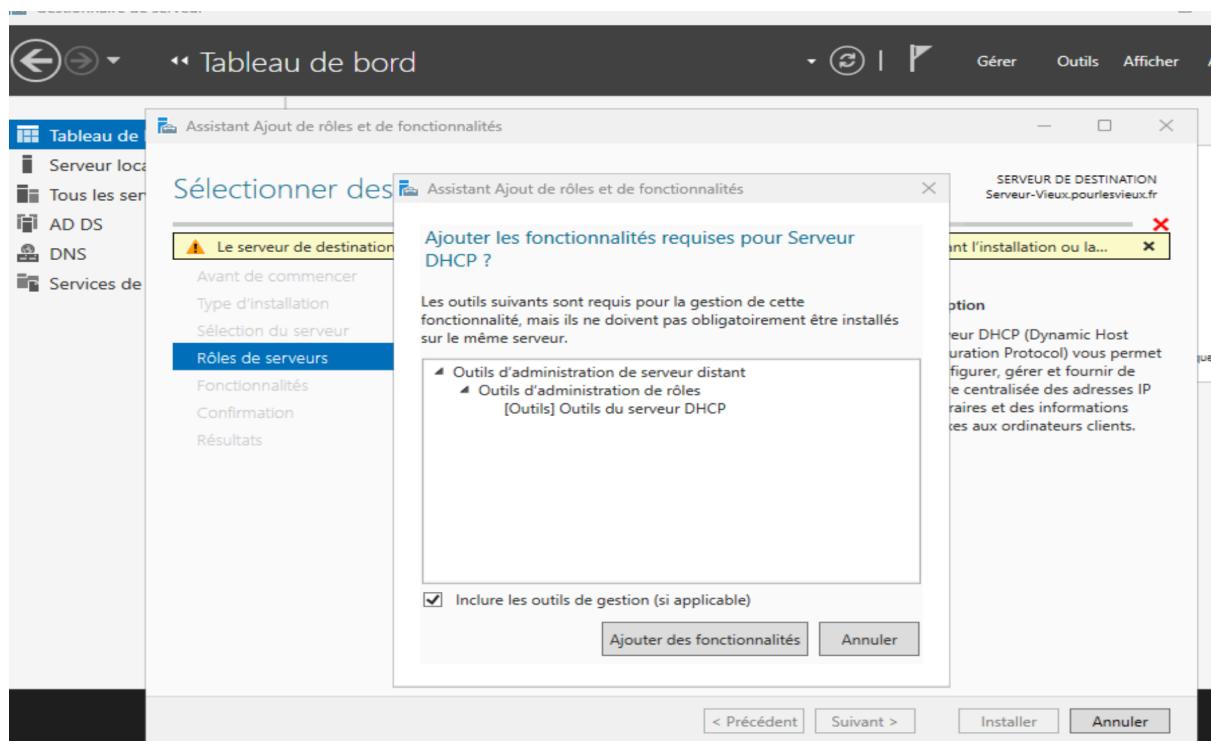
Je vérifie qu'il a bien été installé et je redémarre

```
Sélection Administrateur : Windows PowerShell
PS C:\Windows\system32> Get-WindowsCapability -Name RSAT* -Online | Select-Object -Property DisplayName, State
DisplayName                               State
-----
RSAT : outils Active Directory Domain Services Directory et services LDS (Lightweight Directory Services) Installed
RSAT : Module PowerShell pour Azure Stack HCI      NotPresent
RSAT : utilitaires d'administration de chiffrement de lecteur BitLocker NotPresent
RSAT : outils des services de certificats Active Directory NotPresent
RSAT : outils du serveur DHCP                    NotPresent
RSAT : outils du serveur DNS                    NotPresent
RSAT : outils de clustering de basculement     NotPresent
RSAT : outils de services de fichiers          NotPresent
RSAT : outils de gestion de stratégie de groupe NotPresent
RSAT : client Gestion des adresses IP (IPAM)    NotPresent
RSAT : outils LLDP Data Center Bridging        NotPresent
RSAT : outils de gestion du contrôleur de réseau NotPresent
RSAT : outils d'équilibrage de charge réseau    NotPresent
RSAT : outils de gestion de l'accès à distance  NotPresent
RSAT : outils des services Bureau à distance   NotPresent
RSAT : gestionnaire de serveur                 Installed
RSAT : Outils de gestion des services de migration du stockage NotPresent
Outils d'administration de serveur distant : module de réplica de stockage pour Windows PowerShell NotPresent
RSAT : module Informations système pour Windows PowerShell NotPresent
RSAT : outils d'activation en volume           NotPresent
RSAT : outils Windows Server Update Services   NotPresent

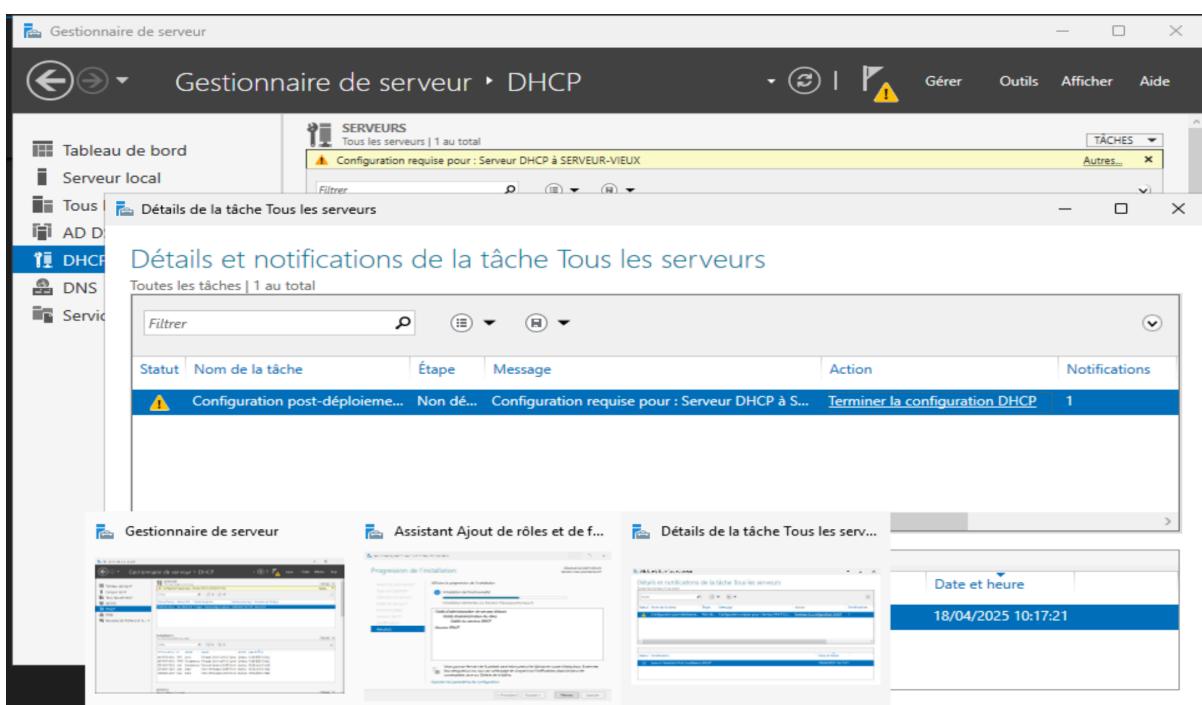
PS C:\Windows\system32>
```

(Pour pouvoir ce connecter avec un adresse dynamique)

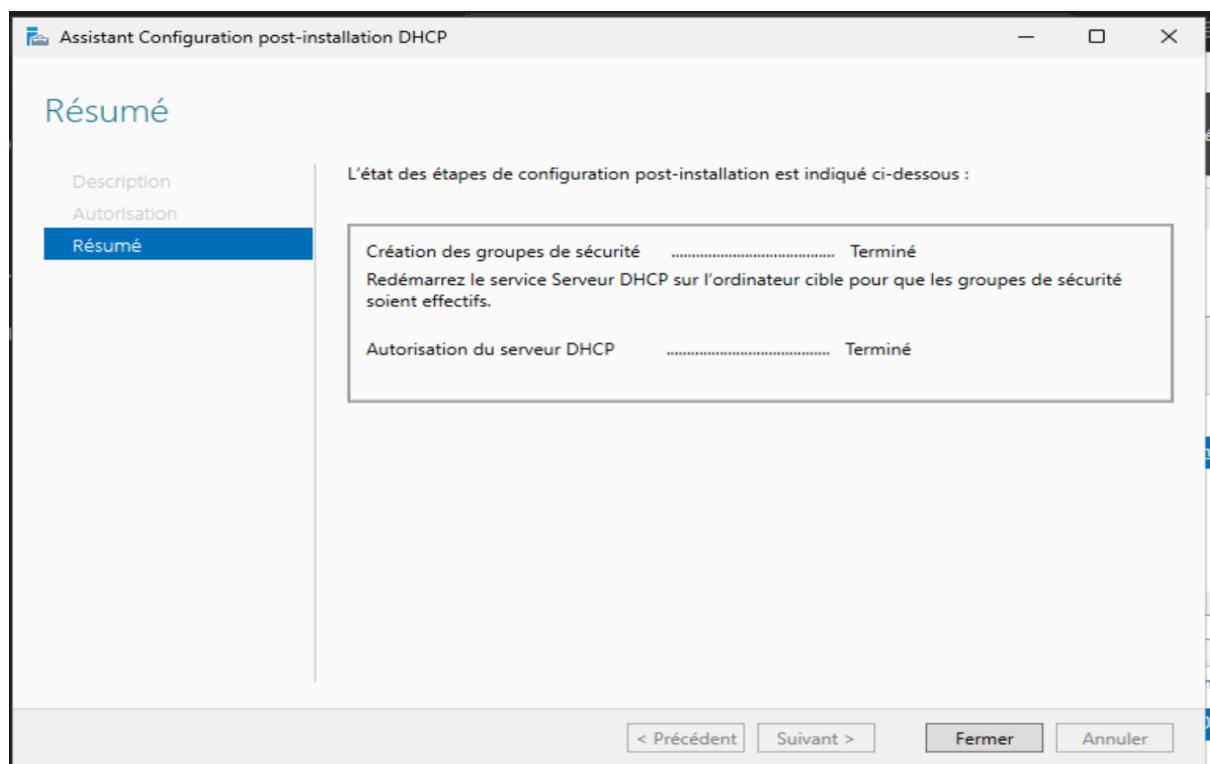
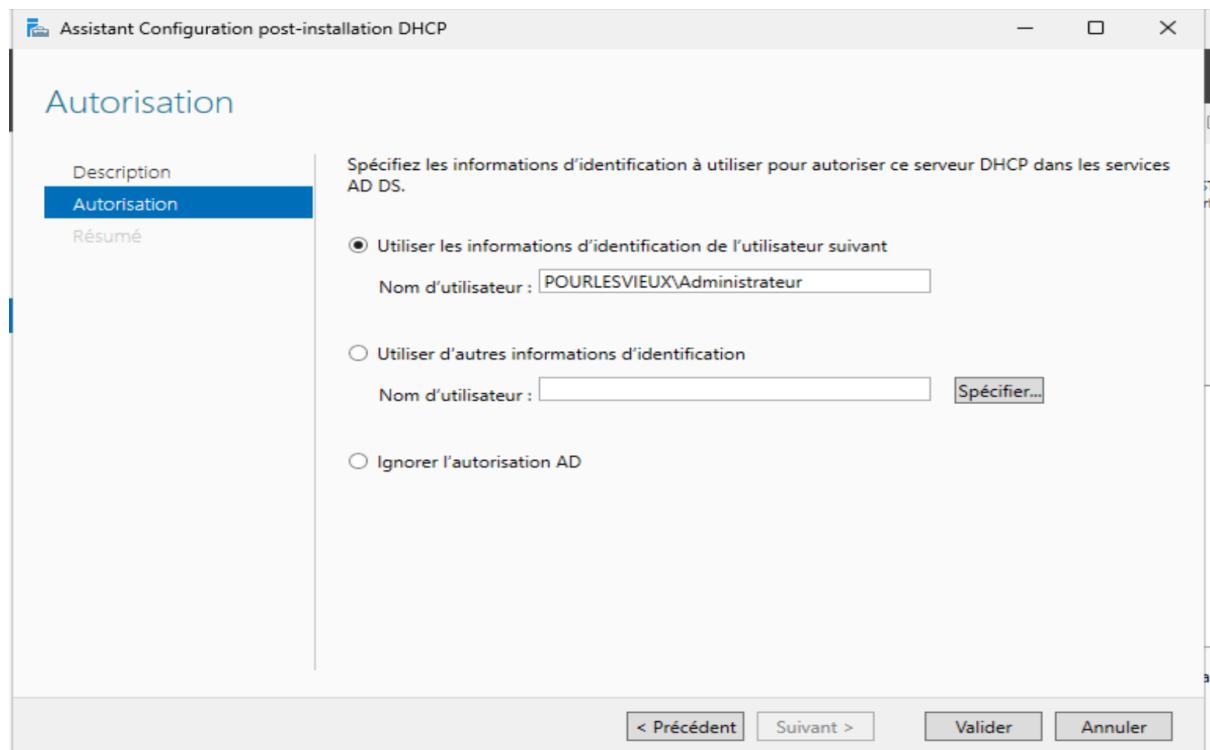
J'installe un serveur DHCP sur mon Windows Serveur



Je configure le serveur DHCP:



Je vais dans “terminer la configuration” :



Assistant Nouvelle étendue

Plage d'adresses IP
Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.

Paramètres de configuration pour serveur DHCP

Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début :

Adresse IP de fin :

Paramètres de configuration qui se propagent au client DHCP.

Longueur :

Masque de sous-réseau :

< Précédent Suivant > Annuler

Il peut utiliser l'adresse pendant 8 jours

Assistant Nouvelle étendue

Durée du bail
La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.

La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.

De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.

Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.

Limitée à :

Jours : Heures : Minutes :

< Précédent Suivant > Annuler

Je définit ma passerelle

Assistant Nouvelle étendue

Routeur (passerelle par défaut)
Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.

Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP :

<input type="text" value="192.168.20.129"/>	<input type="button" value="Ajouter"/> <input type="button" value="Supprimer"/> <input type="button" value="Monter"/> <input type="button" value="Descendre"/>
---	---

< Précédent Suivant > Annuler

Serveurs

Volumes

D... Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Part... < > [] [] [] [] [] [] [] [] [] [] [] []

iSCS... Utilisateurs et ordinateurs Ac... Nom Type Description

Dos... > Requêtes enregistrées > Builtin builtinDomain Default container for up...

> pourlesvie > Délégation de contrôle... Unité d'organisation

> Builtin Rechercher... Unité d'organisation

> Cascad Changer de domaine... Conteneur

> cascad Changer de contrôleur de domaine... Unité d'organisation

> Compu Augmenter le niveau fonctionnel du domaine... Conteneur

> Domai Maîtres d'opérations... Unité d'organisation

> Foreign Nouveau Unité d'organisation

> Gabres Rechercher... Unité d'organisation

> gabres Changer de domaine... Conteneur

> Hermit Affichage Unité d'organisation

> Grc Actualiser infrastructureUpdate

> Orc Exporter la liste... Conteneur

> Util Groupe de sécurité - Domaine local Default container for ke...

> hermit lostAndFound Default container for or...

> Keys Conteneur Default container for ma...

> LostAn Groupe de sécurité - Domaine local Quota specifications co...

> Manag msDS-QuotaContainer Conteneur

> Progra Unité d'organisation Default location for stor...

> SiegeC Unité d'organisation

> siege06 Conteneur

> System Builtin system settings

Assistant Délégation de contrôle

Utilisateurs ou groupes

Sélectionnez un ou plusieurs groupes ou utilisateurs auxquels vous voulez déléguer le contrôle.

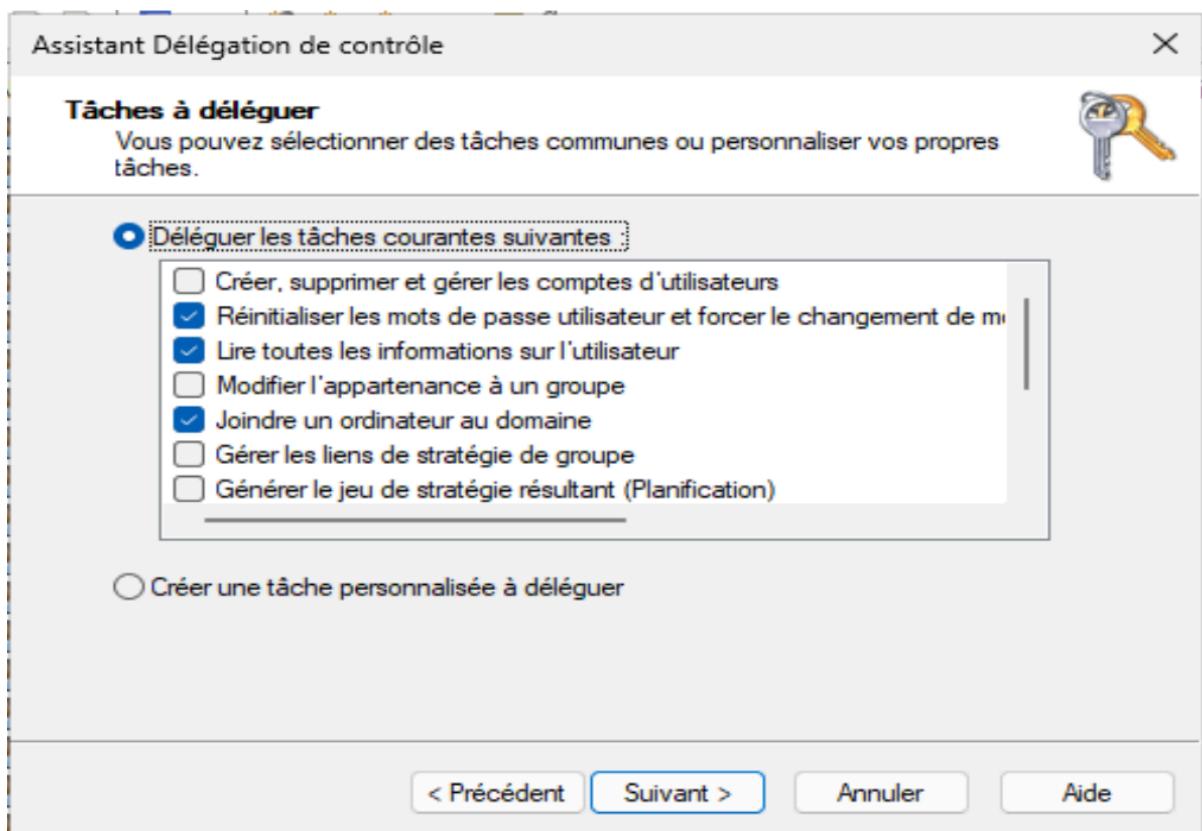


Utilisateurs et groupes sélectionnés :

Utilisateurs authentifiés (AUTORITE NT\Utilisateurs authentifiés)

Ajouter... Supprimer

< Précédent Suivant > Annuler Aide



6/ Script automatisation sécurité

```
1 # Comptes inactifs depuis plus de 30 jours
2 $DaysInactive = 30
3 $InactiveDate = (Get-Date).AddDays(-$DaysInactive)
4
5 $InactiveUsers = Get-ADUser -Filter {LastLogonDate -lt $InactiveDate -and Enabled -eq $true} -Properties LastLogonDate |
6 | Select-Object Name, SamAccountName, LastLogonDate |
7 | Sort-Object LastLogonDate
8
9 $ReportPath = "C:\Audit\Comptes_Inactifs_$(Get-Date -Format 'yyyyMMdd').csv"
10 $InactiveUsers | Export-Csv -Path $ReportPath -NoTypeInformation -Encoding UTF8
11
12 Write-Host "Rapport des comptes inactifs généré : $ReportPath"
13
14
15 # Doubloons de noms et emails
16 $AllUsers = Get-ADUser -Filter * -Properties DisplayName, Mail
17
18 # Doubloons de noms complets
19 $DuplicateNames = $AllUsers | Group-Object DisplayName | Where-Object { $_.Count -gt 1 }
20 $DuplicateNames | ForEach-Object {
21     Write-Warning "Doubloon détecté pour le nom : $($_.Name)"
22     $_.Group | Select-Object SamAccountName, DisplayName
23 }
24
25 # Doubloons d'adresses email
26 $DuplicateEmails = $AllUsers | Where-Object { $_.Mail } | Group-Object Mail | Where-Object { $_.Count -gt 1 }
27 $DuplicateEmails | ForEach-Object {
28     Write-Warning "Doubloon d'email détecté : $($_.Name)"
29     $_.Group | Select-Object SamAccountName, Mail
30 }
31
32 # Export CSV
33 $DuplicateReport = "C:\Audit\Doublons_AD_$(Get-Date -Format 'yyyyMMdd').csv"
34 $DuplicateNames + $DuplicateEmails | Export-Csv -Path $DuplicateReport -NoTypeInformation -Encoding UTF8
35
36
37 # Surveiller les connexions entre 20h et 6h
38 $AfterHoursStart = 20
39 $AfterHoursEnd = 6
40
41
42 $RecentLogons = Get-ADUser -Filter {LastLogonDate -gt (Get-Date).AddDays(-1)} -Properties LastLogonDate
43
44 foreach ($User in $RecentLogons) {
45     if ($User.LastLogonDate) {
46         $Hour = $User.LastLogonDate.Hour
47         if ($Hour -ge $AfterHoursStart -or $Hour -le $AfterHoursEnd) {
48             Write-Warning "Connexion en dehors des heures normales : $($User.SamAccountName) à $($User.LastLogonDate)"
49             # Envoyer une alerte par email
50             Send-MailMessage -To "security@pourlesvieux.fr" -Subject "Alerte Connexion" -Body "Utilisateur $($User.Name) connecté à $($User.LastLogonDate)" -From "noreply@pourlesvieux.fr" -SmtpServer "smtp.pourlesvieux.fr"
51         }
52     }
53 }
54
55
56 # Trouver les utilisateurs avec trop de priviléges
57
58 Get-ADUser -Filter * -Properties MemberOf | Where-Object {
59     $_.MemberOf -match "Domain Admins|Enterprise Admins|Schema Admins" -and $_.Enabled -eq $true
60 } | Select-Object Name, SamAccountName
61
62
63 # Détecter les modifications récentes de GPO
64
65 Get-WinEvent -LogName "Microsoft-Windows-GroupPolicy/Operational" -MaxEvents 20 |
66 Where-Object { $_.Id -eq 4016 } |
67 Select-Object TimeCreated, Message
68
69
70 # Vérifier les services vulnérables
71
72 Get-Service | Where-Object {
73     $_.StartType -eq "Automatic" -and $_.Status -eq "Running" -and $_.Name -match "TermService|Spooler|WinRM"
74 } | Select-Object Name, DisplayName
```

crée un csv des compte inactif depuis X temps

crée un csv des compte en double

Envie un mail d'alerte en cas de connexion après les heures défini de travail de travail

Chercher les user avec trop de droit detecte les modification GPO

Vérifie les services vulnérables

7/ Monter les lecteurs réseaux

Je crée un script qui me permet de monter les réseaux et faire le mapping

```
19 # Import du module nécessaire pour les partages réseau
20 Import-Module SmbShare
21
22 # Configuration de base
23 $Domain = "pourlesvieux.fr"
24 $BasePath = "\\serveurvieux\pourlesvieux.fr" # Remplacez par votre serveur réel
25 $LogPath = "C:\Logs\MountDrives_$(Get-Date -Format 'yyyyMMdd').log"
26
27 # Fonction pour logger les actions
28 function Write-Log {
29     param (
30         [string]$Message,
31         [string]$Level = "INFO"
32     )
33     $Timestamp = Get-Date -Format "yyyy-MM-dd HH:mm:ss"
34     $LogMessage = "[${Timestamp}] [{${Level}}] ${Message}"
35     Add-Content -Path $LogPath -Value $LogMessage
36 }
37
38 # Fonction pour monter un lecteur réseau
39 function Mount-NetworkDrive {
40     param (
41         [string]$DriveLetter,
42         [string]$NetworkPath,
43         [bool]$Persistent = $true,
44         [string]$Description = ""
45     )
46
47     # Vérifier si le lecteur est déjà mappe
48     if (Test-Path "${DriveLetter}:") {
49         Write-Log "Le lecteur ${DriveLetter}: est déjà mappe" -Level "WARNING"
50         return
51     }
52
53     # Vérifier si le partage existe
54     if (-not (Test-Path $NetworkPath)) {
55         Write-Log "Le partage réseau $NetworkPath n'est pas accessible" -Level "ERROR"
56         return
57     }
58
59     try {
60         # Monter le lecteur
61         $Result = New-PSDrive -Name $DriveLetter -PSProvider FileSystem -Root $NetworkPath -Persist:$Persistent -Scope Global -Description $Description -ErrorAction Stop
62
63         Write-Log "Lecteur ${DriveLetter}: mappe avec succès vers $NetworkPath ($Description)"
64         return $true
65     }
66     catch {
67         Write-Log "Erreur lors du mapping de ${DriveLetter}: vers $NetworkPath - $_" -Level "ERROR"
68         return $false
69     }
70 }
71
72 # Détection du département de l'utilisateur (à partir du nom de l'ordinateur ou autre méthode)
73 $ComputerName = $env:COMPUTERNAME
74 $UserDept = "06" # Valeur par défaut, à adapter selon votre logique
75
76 # Exemple de détection du département à partir du nom de l'ordinateur
77 if ($ComputerName -match "83") { $UserDept = "83" }
78 elseif ($ComputerName -match "94") { $UserDept = "94" }
79
80 Write-Log "Département détecté : $UserDept"
81
82 # Monter les lecteurs selon la configuration
83 $DriveMappings = @(
84     @{Letter = "U"; Path = "$basePath\Utilisateurs\$env:USERNAME"; Description = "Dossier personnel" },
85     @{Letter = "M"; Path = "$basePath\Medical_$UserDept"; Description = "Dossier Medical" },
86     @{Letter = "A"; Path = "$basePath\Administratif_$UserDept"; Description = "Administratif/Animation" },
87     @{Letter = "T"; Path = "$basePath\Technicien_$UserDept"; Description = "Technicien" }
88 )
```

```
# Application des mappages
foreach ($Mapping in $DriveMappings) {
    Mount-NetworkDrive -DriveLetter $Mapping.Letter -NetworkPath $Mapping.Path -Description $Mapping.Description
}

# Verification finale
$MappedDrives = Get-PSDrive -PSProvider FileSystem | Where-Object { $_.DisplayRoot -like "\\"* }
Write-Log "Recapitulatif des lecteurs mappes :"
$MappedDrives | ForEach-Object {
    Write-Log " $($_.Name): $($_.DisplayRoot)"
}

# Optionnel : Ajouter au script de login utilisateur
Write-Host "Montage des lecteurs reseau termine"
Write-Host "U: Votre dossier personnel"
Write-Host "M: Dossier Medical"
Write-Host "S: Administratif/Animation"
Write-Host "P: Comptabilite"
Write-Host "Z: Bibles et procedures"
Write-Host "T: Documents techniques"
Write-Host "X: Documents cadres"

# Fin du script
```

8/ Monter les IMPRIMANTES

```
# Configuration de base
$LogPath = "\\serveur\logs\Imprimantes_\$(Get-Date -Format 'yyyyMMdd').log"
$PrintServer = "SRV-IMPRIMANTES" # Nom de votre serveur d'impression
|
# Tableau de correspondance etablissement -> imprimantes
$PrintersMapping = @{
    "Gabres(06)" = @("IMP-GABRES-01", "IMP-GABRES-RECEPTION")
    "Hermitage(83)" = @("IMP-HERMITAGE-ETAGE1", "IMP-HERMITAGE-ACCUEIL")
    "Cascade(94)" = @("IMP-CASCADE-BUREAUX", "IMP-CASCADE-INFIRMERIE")
    "Siege(06)" = @("IMP-SIEGE-COMPTA", "IMP-SIEGE-RH", "IMP-SIEGE-DIRECTION")
}

# Imprimantes communes a tous les etablissemets
$CommonPrinters = @("IMP-COLOR-COMMUNE", "IMP-NOIRBLANC-COMMUNE")

# Fonction de logging
function Write-Log {
    param ([string]$message, [string]$level = "INFO")
    $timestamp = Get-Date -Format "yyyy-MM-dd HH:mm:ss"
    $logMessage = "[${timestamp}] [$level] $message"
    Add-Content -Path $LogPath -Value $logMessage
}

# Fonction pour installer une imprimante
function Install-Printer {
    param (
        [string]$printerName,
        [bool]$setAsDefault = $false
    )

    $printerPath = "\\$PrintServer\$printerName"

    try {
        # Vefier si l'imprimante est deja installée
        if (Get-Printer -Name $printerPath -ErrorAction SilentlyContinue) {
            Write-Log "Imprimante $printerName déjà installée"
            return $true
        }
    }

    # Installation de l'imprimante
    Add-Printer -ConnectionName $printerPath -ErrorAction Stop
    Write-Log "Imprimante $printerName installée avec succès"

    # Definir comme imprimante par defaut si demande
    if ($setAsDefault) {
        Set-Printer -Name $printerPath -Shared $false -ErrorAction Stop
        Write-Log "Imprimante $printerName définie comme défaut"
    }

    return $true
}
catch {
    Write-Log "échec installation $printerName : $_" -level "ERROR"
    return $false
}

# Detection de l'établissement de l'utilisateur
function Get-UserEstablishment {
    # Methode 1 : Par nom de machine (si convention de nommage)
    $computerName = $env:COMPUTERNAME
    foreach ($etab in $PrintersMapping.Keys) {
        if ($computerName -match $etab.Split('(')[0]) {
            return $etab
        }
    }

    # Methode 2 : Par groupe AD de l'utilisateur (plus fiable)
    $userGroups = (Get-ADUser $env:USERNAME -Properties MemberOf).MemberOf
    foreach ($etab in $PrintersMapping.Keys) {
        $etabName = $etab.Split('(')[0]
        if ($userGroups -match "Grp-$etabName") {
            return $etab
        }
    }
}

# Valeur par default si non detecte
return "Siege(06)"

# Detection si utilisateur fait partie du siege
function Test-IsSiegeUser {
    $userGroups = (Get-ADUser $env:USERNAME -Properties MemberOf).MemberOf
    return ($userGroups -match "Grp-Siege" -or $userGroups -match "Domain Admins")
```

```
125 | 
126 # 4. Si utilisateur du siege, installer toutes les imprimantes
127 if ($isSiegeUser) {
128     Write-Log "Utilisateur du siege - installation de toutes les imprimantes"
129     foreach ($etab in $PrintersMapping.Keys) {
130         if ($etab -ne $userEtab) {
131             foreach ($printer in $PrintersMapping[$etab]) {
132                 Install-Printer -printerName $printer
133             }
134         }
135     }
136 }
137 
138 # 5. Verification finale
139 $installedPrinters = Get-Printer | Where-Object { $_.Type -eq "Connection" }
140 Write-Log "Imprimantes installées : $($installedPrinters.Count)"
141 $installedPrinters | ForEach-Object { Write-Log " - $($_.Name)" }
142 
143 Write-Log "Deploiement des imprimantes terminé"
```

9/ Contrôleur DOMAINE SECONDAIRE ET RÉPLICATION

1. Préparation du serveur

Installation des rôles nécessaires

powershell

Copy

Download

```
Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools  
Import-Module ADDSDeployment
```

2. Promotion en contrôleur de domaine secondaire

powershell

Copy

Download

```
Install-ADDSDomainController  
    -NoGlobalCatalog:$false  
    -CreateDnsDelegation:$false  
    -CriticalReplicationOnly:$false  
    -DatabasePath "C:\Windows\NTDS"  
    -DomainName "votredomaine.com"  
    -InstallDns:$true  
    -LogPath "C:\Windows\NTDS"  
    -NoRebootOnCompletion:$false  
    -SiteName "Default-First-Site-Name"  
    -SysvolPath "C:\Windows\SYSVOL"  
    -Force:$true
```

```
Administrator : C:\WINDOWS\system32\cmd.exe

Carte Ethernet Ethernet0 :

Suffixe DNS propre à la connexion... : localdomain
Adresse IPv6 de liaison locale... : fe80::1e07:c599:428f:fa57%3
Adresse IPv4... : 192.168.20.128
Masque de sous-réseau... : 255.255.255.0
Passerelle par défaut... : 192.168.20.2
PS C:\Users\Administrateur> install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
----- ----- ----- {Services de domaine Active Directory, Ges...
True    No       Success           {Services de domaine Active Directory, Ges...

PS C:\Users\Administrateur> Import-Module ADDSDeplolement
Import-Module : Le module «ADDSDeplolement» spécifié n'a pas été chargé, car aucun fichier de module valide n'a été trouvé dans un répertoire de module.
Au caractère Ligne:1 : 1
+ Import-Module ADDSDeplolement
+ ~~~~~
+ CategoryInfo          : ResourceUnavailable: (ADDSDeplolement:String) [Import-Module], FileNotFoundException
+ FullyQualifiedErrorId : Modules_ModuleNotFound,Microsoft.PowerShell.Commands.ImportModuleCommand

PS C:\Users\Administrateur> Install-ADDSDomainController

applet de commande Install-ADDSDomainController à la position 1 du pipeline de la commande
Fournissez des valeurs pour les paramètres suivants :
DomainName: pourlesvieux.fr
SafeModeAdministratorPassword: *****
```

3. Vérification de la réPLICATION

Vérifier l'état de la réPLICATION

powershell

Copy

Download

```
repadmin /showrepl
repadmin /replsummary
```

Forcer la réPLICATION IMMÉDIATE

powershell

Copy

5. Surveillance continue

Script de surveillance de la réPLICATION

powershell

Copy

Download

```
$replicationStatus = repadmin /showrep
$errors = $replicationStatus | Select-String "failed"

if ($errors) {
    Send-MailMessage -To "admin@votredomaine.com"
        -Subject "ALERTE RéPLICATION AD"
        -Body "Problèmes de réPLICATION détectés:`n$errors"
        -From "noreply@votredomaine.com"
        -SmtpServer "smtp.votredomaine.com"

    # Tentative de réparation automatique
    repadmin /syncall /AdeP
}
```

10/Creation d'un Script Powershell Pour les Dossier imprimante et GPO (a finir)

voir le script

The screenshot shows a Windows PowerShell ISE window titled "Script_Gpo_ou_dossier.ps1". The code in the editor is as follows:

```
313 } Import-UsersFromCSV -EtablissementName $EtabName -BaseDN $BaseDN -Password $Password
314 }
315 }
316 Write-Host "`nConfiguration terminee avec succes !" -ForegroundColor Green
```

The output pane displays the results of the script execution:

```
Traitement de l'établissement : Cascade
Dossier cree : C:\Partages\Bibles_94
AVERTISSEMENT : Erreur lors de la creation/config du dossier Bibles_94 : Exception lors de l'appel de « AddAccessRule » avec < 1 > argument(s) : « Impossible de traduire certaines ou toutes les références d'identité. »
Dossier cree : C:\Partages\Cadres_94
AVERTISSEMENT : Erreur lors de la creation/config du dossier Cadres_94 : Exception lors de l'appel de « AddAccessRule » avec < 1 > argument(s) : « Impossible de traduire certaines ou toutes les références d'identité. »
Dossier cree : C:\Partages\Technique_94
AVERTISSEMENT : Erreur lors de la creation/config du dossier Technique_94 : Exception lors de l'appel de « AddAccessRule » avec < 1 > argument(s) : « Impossible de traduire certaines ou toutes les références d'identité. »
Dossier cree : C:\Partages\Medical_94
AVERTISSEMENT : Erreur lors de la creation/config du dossier Medical_94 : Exception lors de l'appel de « AddAccessRule » avec < 1 > argument(s) : « Impossible de traduire certaines ou toutes les références d'identité. »
Dossier cree : C:\Partages\Utilisateur_94
Dossier cree : C:\Partages\Compta_94
AVERTISSEMENT : Erreur lors de la creation/config du dossier Compta_94 : Exception lors de l'appel de « AddAccessRule » avec < 1 > argument(s) : « Impossible de traduire certaines ou toutes les références d'identité. »
Dossier cree : C:\Partages\Administratif_94
AVERTISSEMENT : Erreur lors de la creation/config du dossier Administratif_94 : Exception lors de l'appel de « AddAccessRule » avec < 1 > argument(s) : « Impossible de traduire certaines ou toutes les références d'identité. »
Dossier cree : C:\Partages\Animation_94
AVERTISSEMENT : Erreur lors de la creation/config du dossier Animation_94 : Exception lors de l'appel de « AddAccessRule » avec < 1 > argument(s) : « Impossible de traduire certaines ou toutes les références d'identité. »
AVERTISSEMENT : Fichier CSV introuvable : C:\Users\Cascade.csv

Configuration terminee avec succes !
```

The status bar at the bottom indicates "Terminé" (Completed).

The screenshot shows a Windows File Explorer window with the following details:

Path: Ce PC > Disque local (C:) > Partages

Search bar: Rechercher dans : Partages

Table Headers:

Nom	Modifié le	Type	Taille
-----	------------	------	--------

Data Rows:

Administratif_06	22/04/2025 00:53	Dossier de fichiers	
Administratif_83	22/04/2025 00:54	Dossier de fichiers	
Administratif_94	22/04/2025 00:54	Dossier de fichiers	
Animation_06	22/04/2025 00:53	Dossier de fichiers	
Animation_83	22/04/2025 00:54	Dossier de fichiers	
Animation_94	22/04/2025 00:54	Dossier de fichiers	
Bibles_06	22/04/2025 00:53	Dossier de fichiers	
Bibles_83	22/04/2025 00:54	Dossier de fichiers	
Bibles_94	22/04/2025 00:54	Dossier de fichiers	
Cadres_06	22/04/2025 00:53	Dossier de fichiers	
Cadres_83	22/04/2025 00:54	Dossier de fichiers	
Cadres_94	22/04/2025 00:54	Dossier de fichiers	