

ACTIVE DIRECTORY

01. C'est quoi Active Directory !

L'Active Directory est un annuaire LDAP pour les systèmes d'exploitation Windows

Cet annuaire contient différents objets, de différents types (utilisateurs, ordinateurs, etc.).

L'objectif étant de centraliser deux fonctionnalités essentielles : l'identification et l'authentification au sein d'un système d'information.



Désormais, il est notamment lié au Cloud Microsoft, via Azure et Microsoft 365

Attention = Ancienne appellation de “ACTIVE DIRECTORY”

NTDS = NT Directory Services

déployer à l'époque sous windows NT !

Maintenant sous Windows Server !

02. Les intérêts d'un annuaire Active Directory sont :

Administration centralisée et simplifiée

Unifier l'authentification

Identifier les objets sur le réseau

Référencer les utilisateurs et ordinateurs

03. La Structure de l'Active Directory :

Les classes, les attributs, le schéma et les partitions d'annuaire

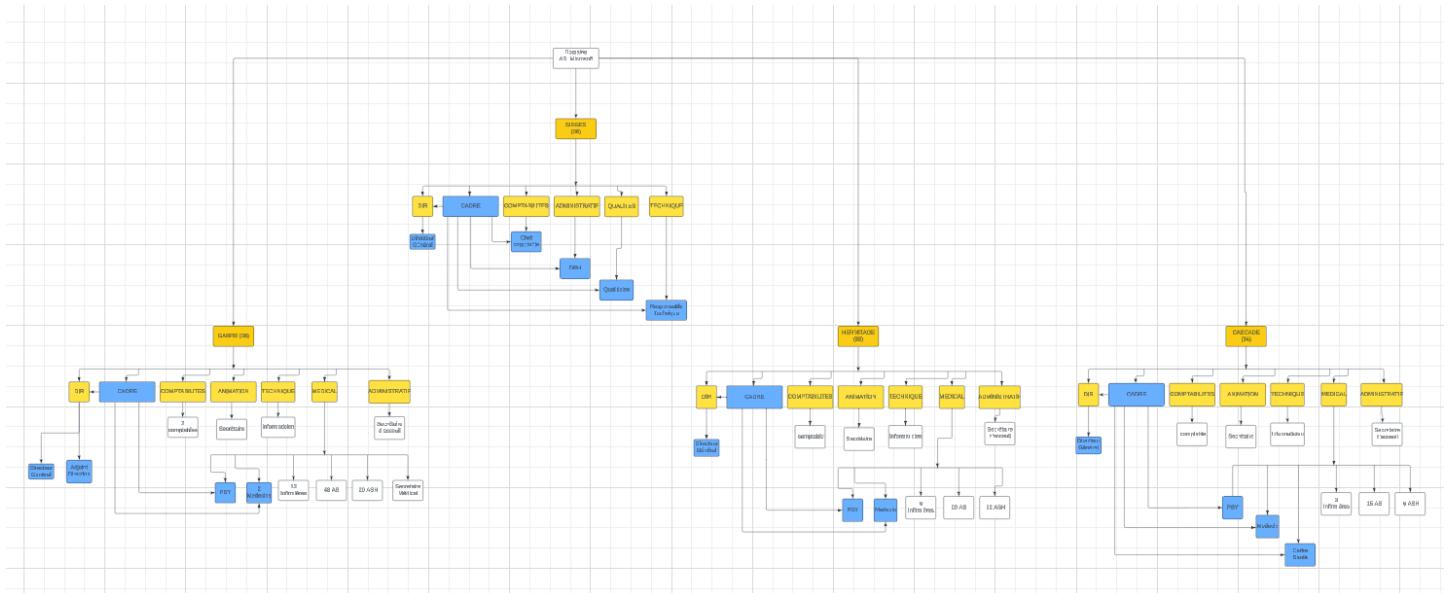
- **Les classes et les attributs** : les utilisateurs, les ordinateurs, les serveurs, les unités d'organisation ou encore les groupes. Ces objets correspondent à **des classes**, c'est-à-dire **des objets disposant des mêmes attributs**.
- **Le schéma** : Il contient la définition de toutes les classes et de tous les attributs disponibles et autorisés au sein de votre annuaire.
- **Les partitions d'annuaire** : Trois partitions, à savoir la partition de schéma, la partition de configuration et la partition domaine.

RUNTRACK

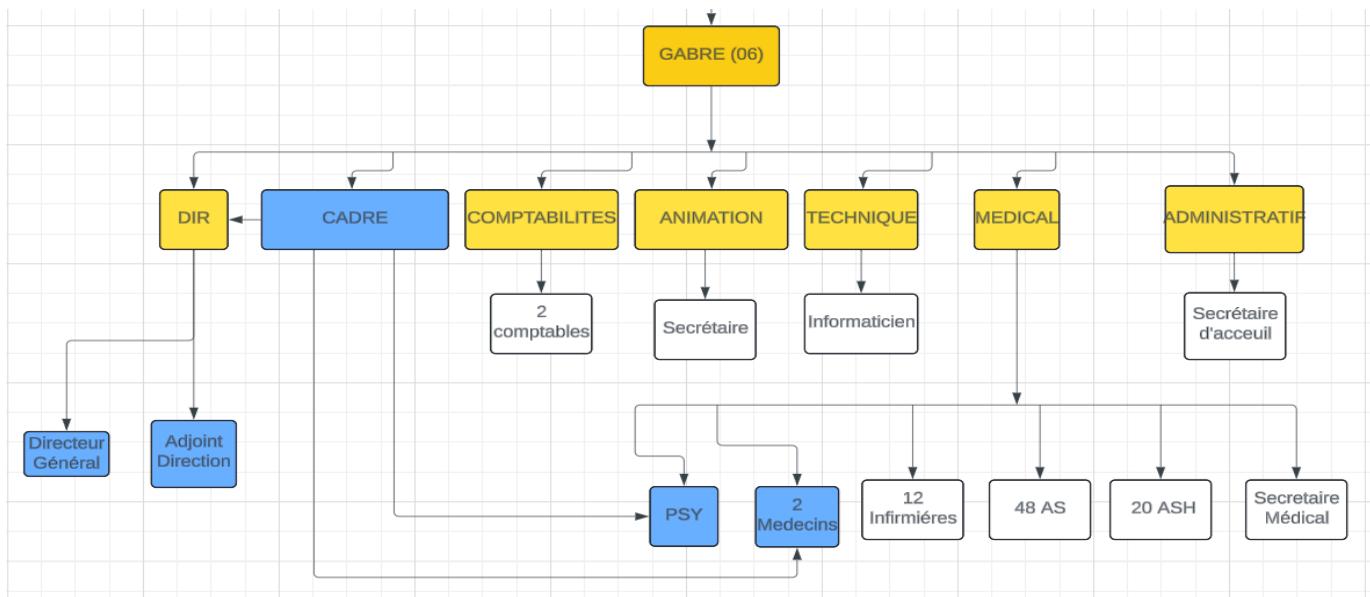
Job 0

Avant de vous lancer dans l'installation et la configuration de ce protocole **"complexe"**, préparez un document pour présenter **Active Directory**, son environnement, son fonctionnement et ses fonctionnalités, ses avantages et inconvénients. Trouvez aussi quelques cas pratiques de son utilisation en milieu professionnel...

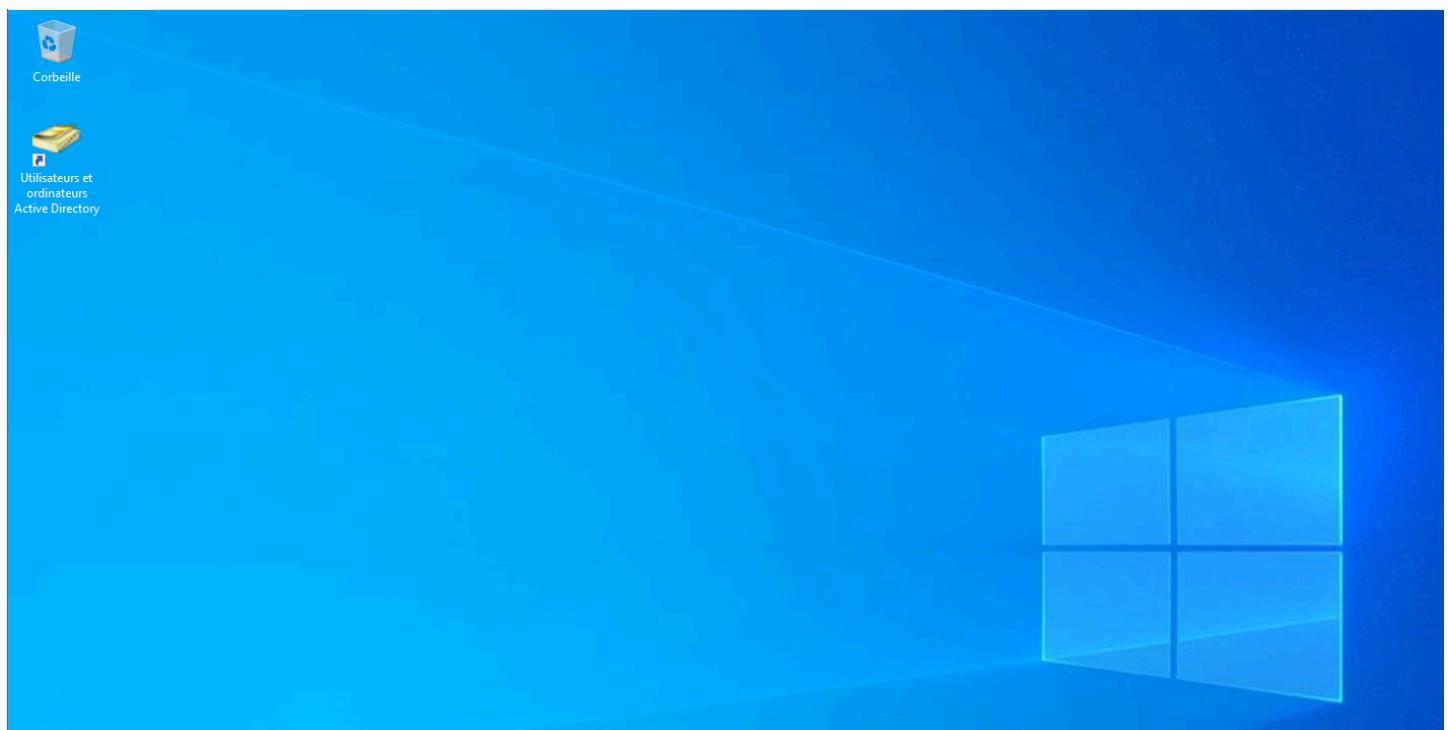
Document pour Organiser les OU d'Active Directory:



-Exemple d'un Organigramme pour la gestion d'un annuaire :

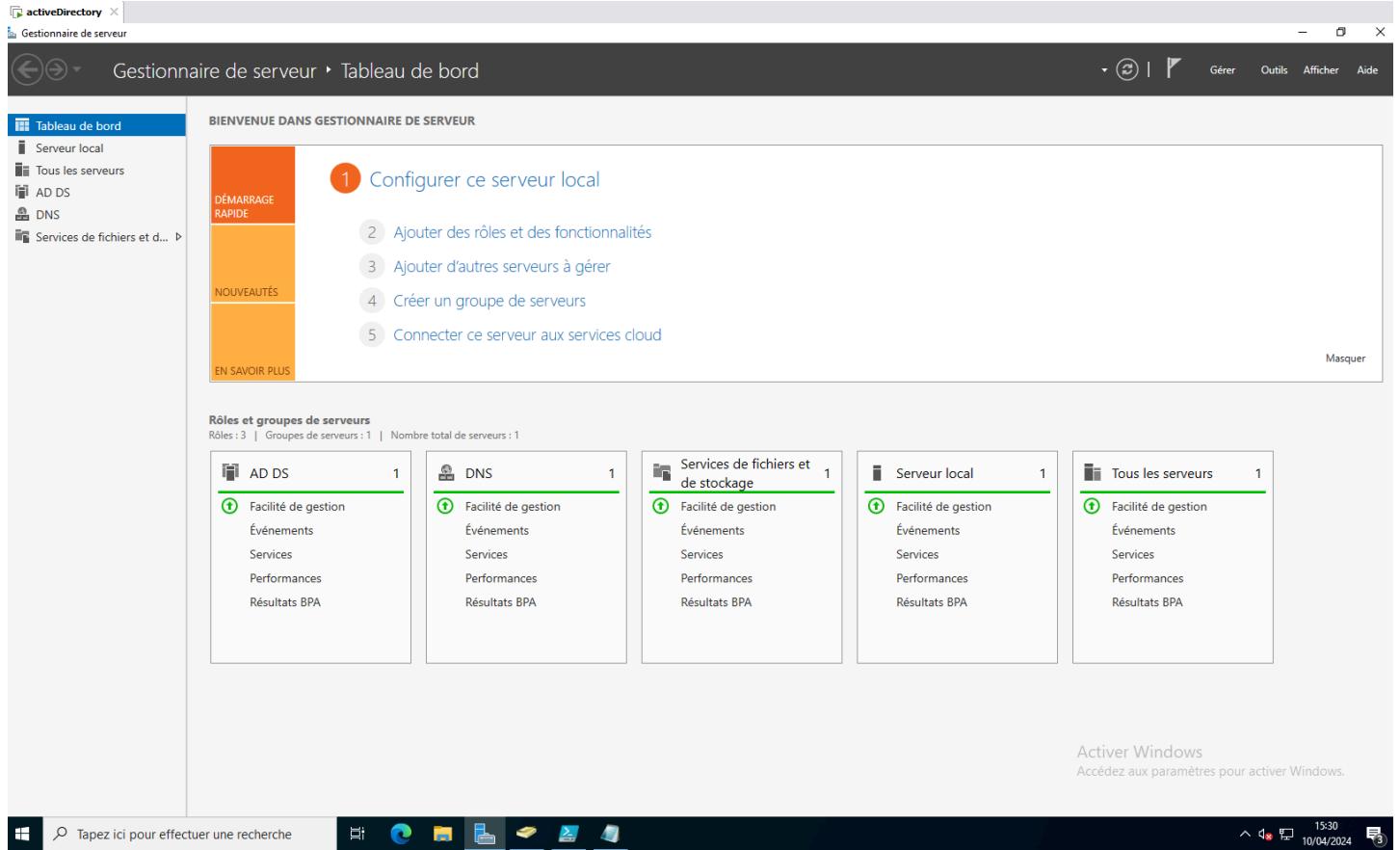


- VM Windows server installée:

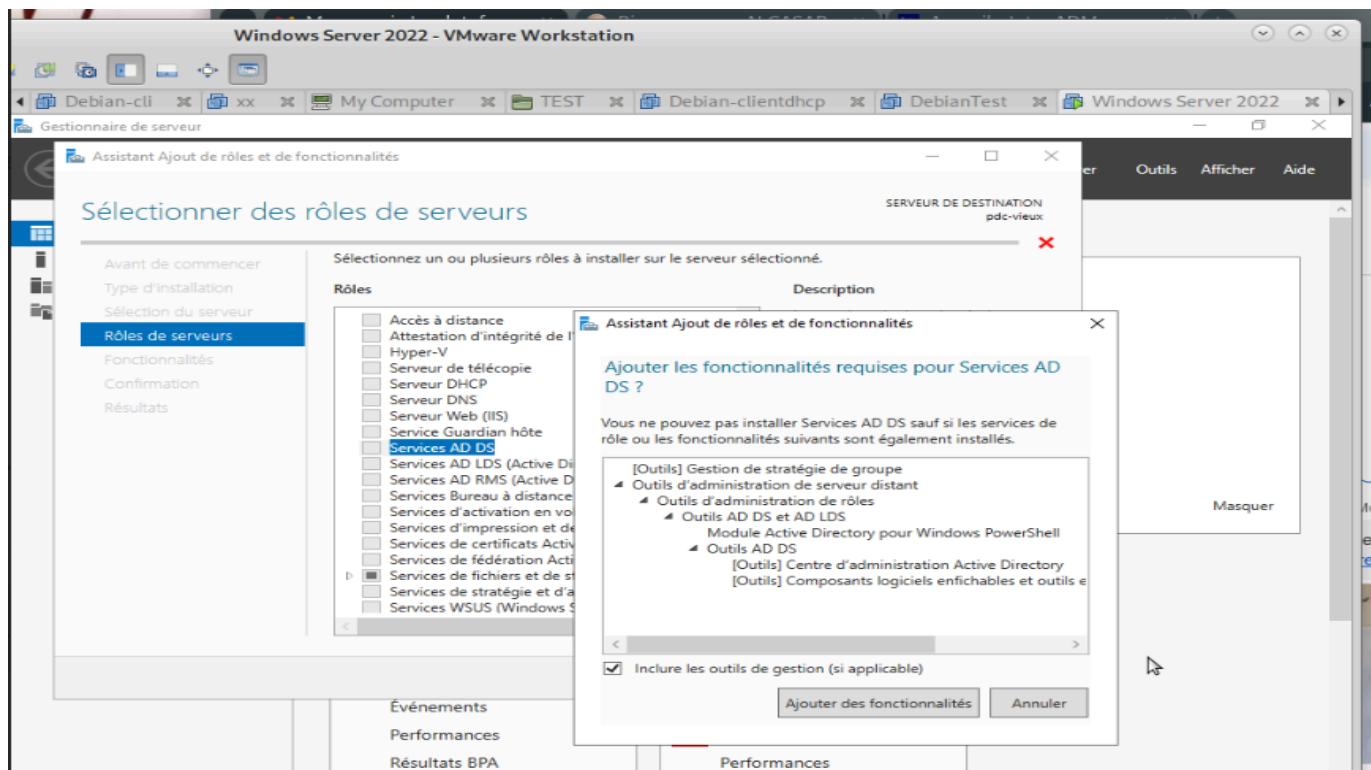


GESTIONNAIRE DE SERVEUR :

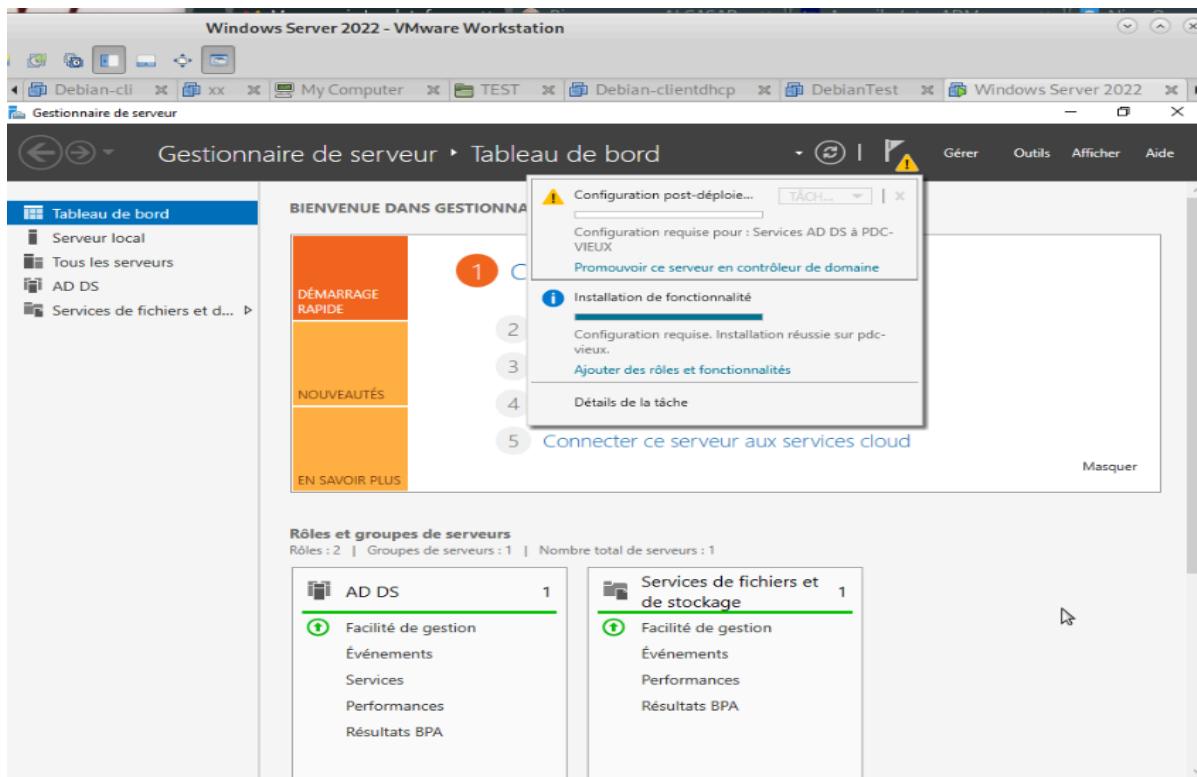
Installation :



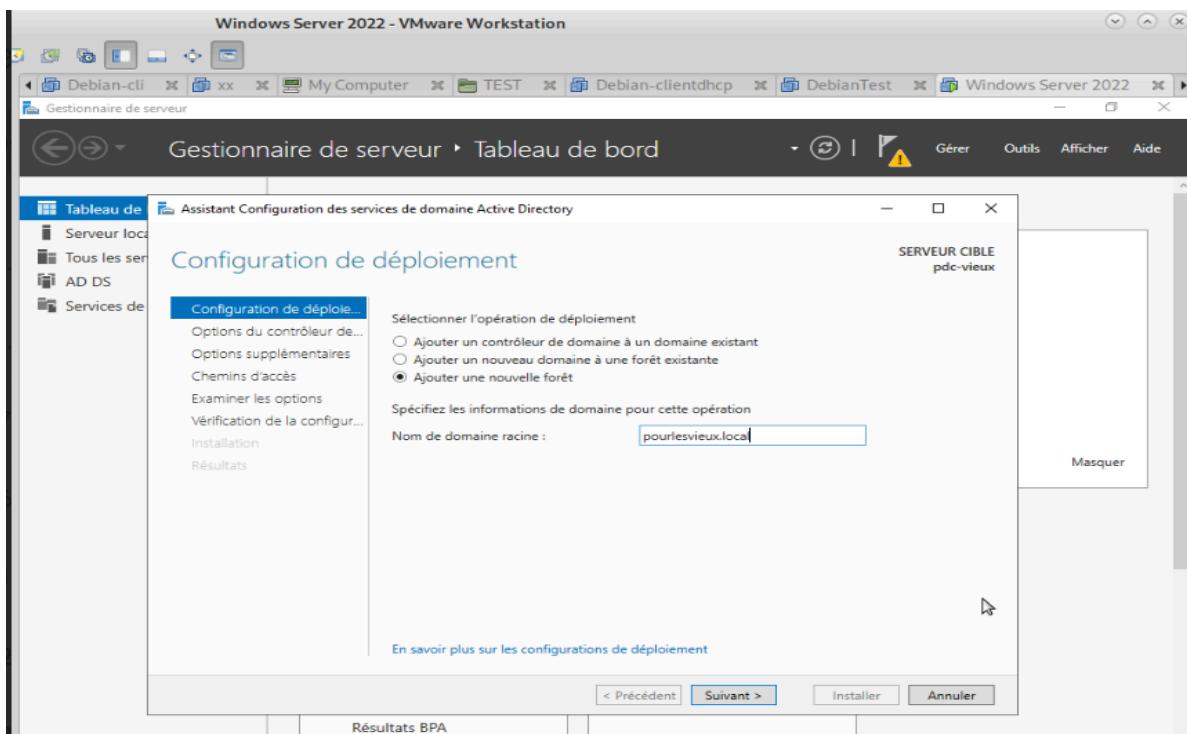
- Installation d'Active Directory :



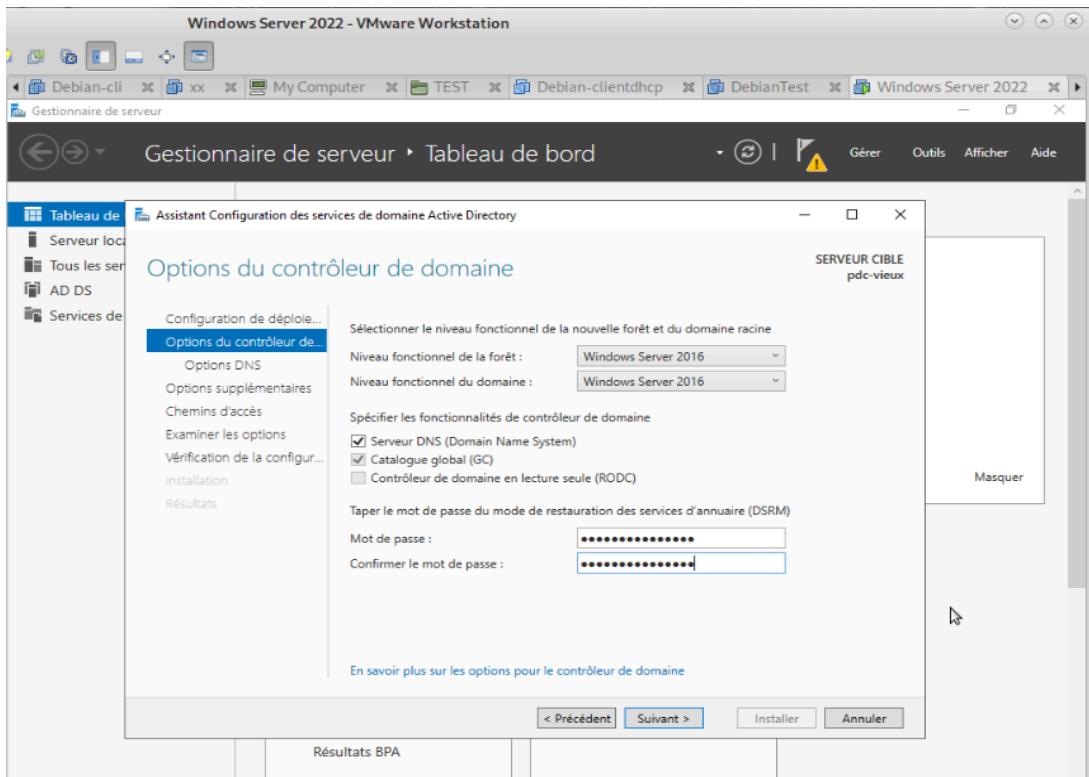
- Sélectionner AD DS



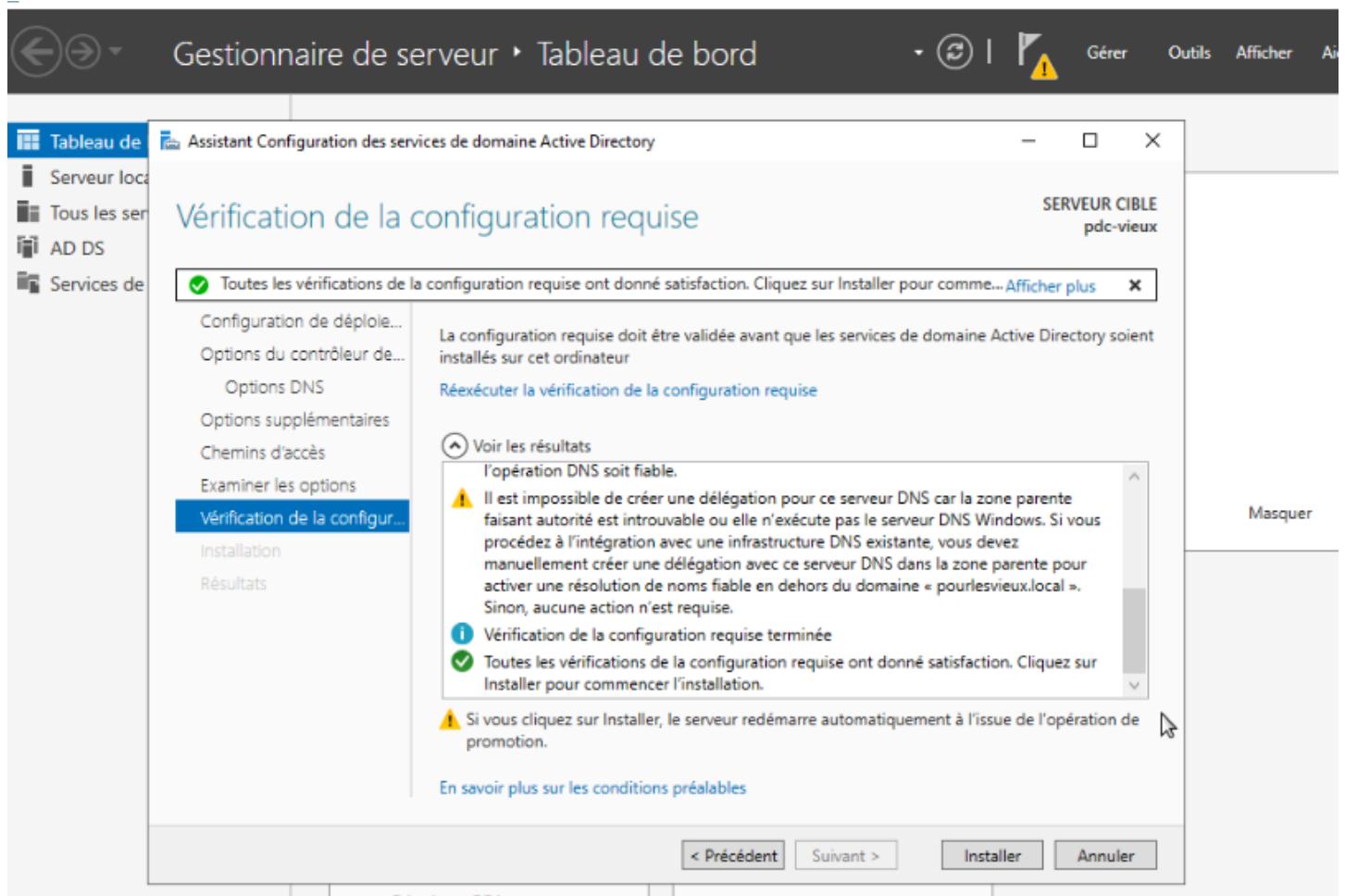
- Installation des fonctionnalités



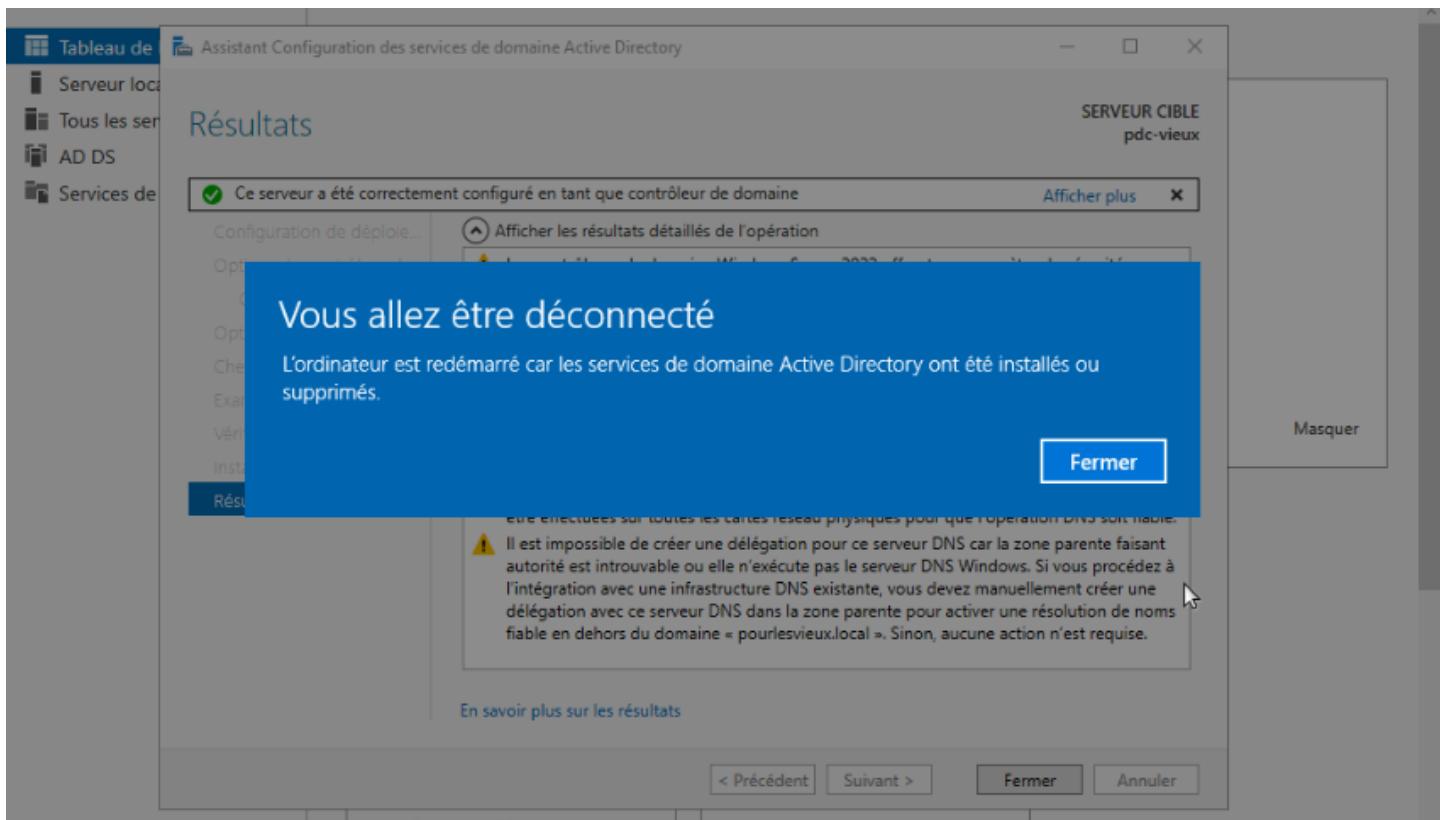
- Ajouter une nouvelle forêt



- Mettre un mot de passe (admin)



- Verification de la config requise



- Redémarrage de la VM

BIENVENUE DANS GESTIONNAIRE DE SERVEUR

DÉMARRAGE RAPIDE

- 1 Configurer ce serveur
- 2 Ajouter des rôles
- 3 Ajouter d'autres services
- 4 Créer un groupe
- 5 Connecter ce serveur

Rôles et groupes de serveurs

Rôles : 3 | Groupes de serveurs : 1 | Nombre total de serveurs

AD DS	1
Facilité de gestion	
Événements	
Services	
Performances	
Résultats BPA	

DNS	
Facilité de gestion	
Événements	
Services	
Performances	
Résultats	

Analyseur de performances
Centre d'administration Active Directory
Configuration du système
Défragmenter et optimiser les lecteurs
Diagnostic de mémoire Windows
DNS
Domaines et approbations Active Directory
Éditeur du Registre
Gestion de l'ordinateur
Gestion des stratégies de groupe
Informations système
Initiateur iSCSI
Lecteur de récupération
Modification ADSI
Module Active Directory pour Windows PowerShell
Moniteur de ressources
Nettoyage de disque
Observateur d'événements
ODBC Data Sources (32-bit)
Pare-feu Windows Defender avec fonctions avancées de sécurité
Planificateur de tâches
Sauvegarde Windows Server

pour ouvrir la console des gestion utilisateurs et ordi AD

Centre d'administration Active Directory

Centre d'administration Active Directory › pourlesvieux (local)

Vue d'ensemble

pourlesvieux (local)

Contrôle d'accès dynamique

Authentification

Recherche globale

Filtrer

Nom Type Description

Nom	Type	Description
Builtin	builtinDomain	
Computers	Conteneur	Default container for upgr...
Domain Controllers	Unité d'org...	Default container for dom...
ForeignSecurityPrincipals	Conteneur	Default container for secur...
Infrastructure	infrastructu...	
Keys	Conteneur	Default container for key o...
LostAndFound	lostAndFou...	Default container for orph...
Managed Service Accounts	Conteneur	Default container for man...
NTDS Quotas	msDS-Quo...	Quota specifications conta...
Program Data	Conteneur	Default location for storag...
System	Conteneur	Builtin system settings
TPM Devices	msTPM-Inf...	
Users	Conteneur	Default container for upgr...

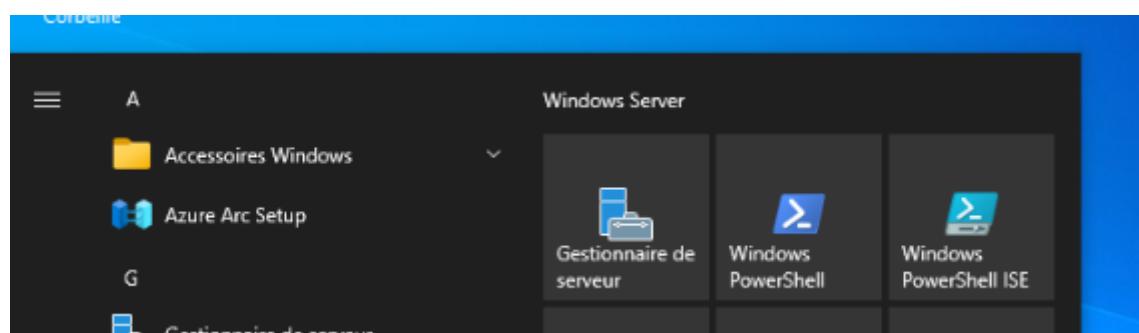
Builtin

Classe d'objets : builtinDomain Modifié le : 08/04/2024 07:33

Description :

Tâches

- Builtin
 - Nouveau
 - Supprimer
 - Rechercher sous ce noeud
 - Propriétés
- pourlesvieux (local)
 - Modifier le contrôleur de dom...
 - Augmenter le niveau fonction...
 - Augmenter le niveau fonction...
 - Activer la Corbeille...
- Nouveau
- Rechercher sous ce noeud
- Propriétés

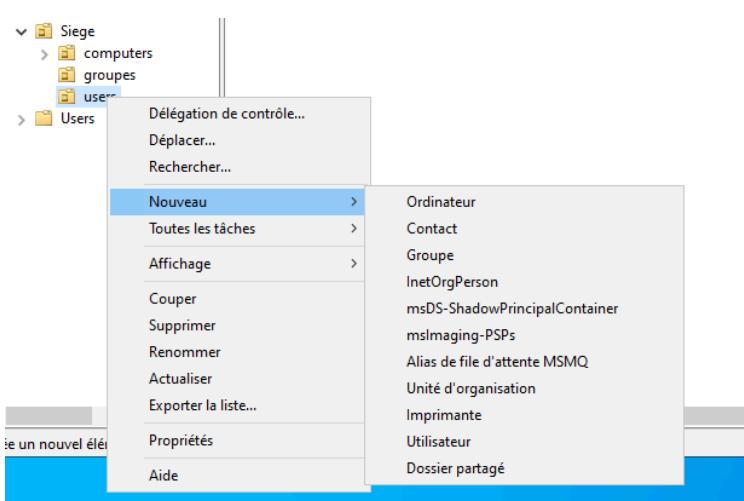


- Ouvrir PowerShell ISE

- **ACTIVE DIRECTORY installée :**

Job 2

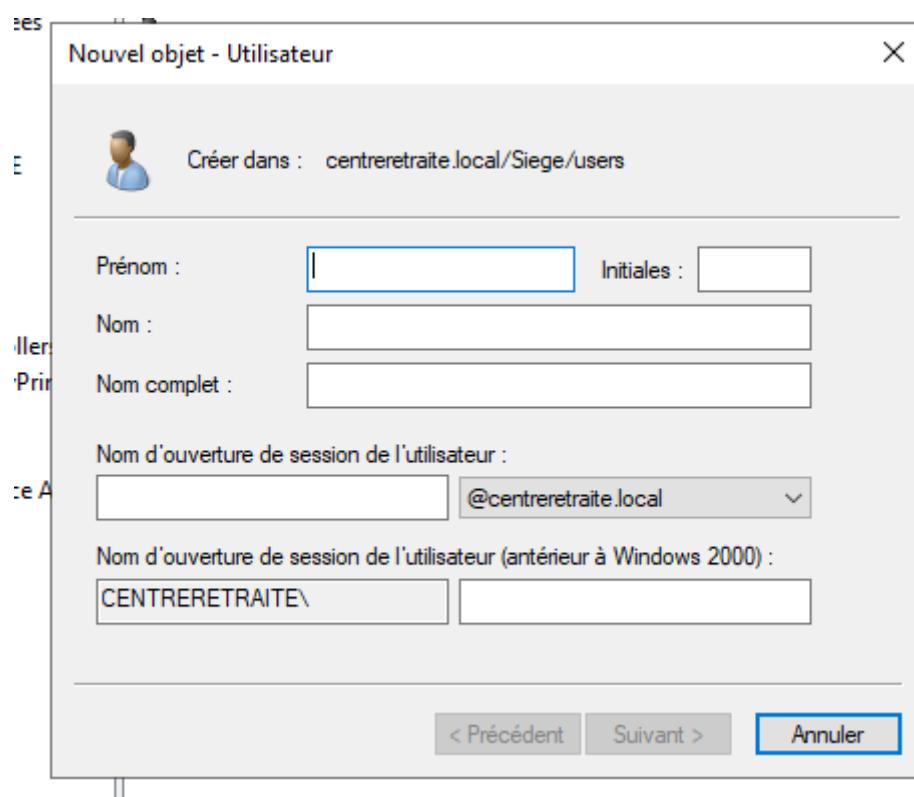
0.1 Créations des OU utilisateurs manuel et ou avec script:



Fichier Action Affichage ?

Nom	Type	Description
CATHERINE BURBAN	Utilisateur	Compte utilisateur pour CATHERINE BURBAN
CHRISTIAN PAPIN	Utilisateur	Compte utilisateur pour CHRISTIAN PAPIN
NELLY DELAHAYE	Utilisateur	Compte utilisateur pour NELLY DELAHAYE
RACHEL PALEGALU	Utilisateur	Compte utilisateur pour RACHEL PALEGALU
WILLY RAVAILLER	Utilisateur	Compte utilisateur pour WILLY RAVAILLER

- On peut créer les OU Users de deux façon soit manuellement :



- Ou bien avec un Script avec Powershell ISE :

```
Sans titre1.ps1 scriptCSVUserAD.ps1 X
1 # Spécifiez le chemin du fichier CSV contenant les données des utilisateurs
2 $CSVFile = "Utilisateurs.csv"
3
4 # Importez les données du fichier CSV
5 $CSVData = Import-Csv -Path $CSVFile -Encoding UTF8
6
7 # à mettre avant la boucle car le mot de passe première utilisation est le même pour tous au démarrage
8 $password = ConvertTo-SecureString -String "Azerty06!" -AsPlainText -Force
9
10 # Parcourez chaque ligne du fichier CSV
11 Foreach($Utilisateur in $CSVData){
12     # Récupérez les informations de chaque utilisateur à partir du CSV
13     $UtilisateurPrenom = $Utilisateur.PRENOM
14     $UtilisateurNom = $Utilisateur.NOM
15     $UtilisateurFonction = $Utilisateur.FONCTION
16     $UtilisateurEtablissement = $Utilisateur.ETABLISSEMENT
17     $username = $UtilisateurPrenom.ToLower() + "." + $UtilisateurNom.ToLower()
18
19
20     # Vérifiez si l'utilisateur existe déjà dans Active Directory
21     if (Get-ADUser -Filter {SamAccountName -eq $($UtilisateurNom.Substring(0,1))$UtilisateurPrenom}) {
22         Write-Warning "L'identifiant $($UtilisateurNom.Substring(0,1))$UtilisateurPrenom existe déjà dans l'AD"
23     }
24     else {
25
26
27         $userParams = @{
28             Name          = "$UtilisateurPrenom $UtilisateurNom"
29             SamAccountName = $username
30             UserPrincipalName = "$username@pourlesvieux.local"
31             GivenName    = $UtilisateurPrenom
32             Surname      = $UtilisateurNom
33             AccountPassword = $password
34             Enabled       = $true
35             Path          = "OU=Users,OU=$UtilisateurEtablissement,DC=centreretraite,DC=local"
36             Description   = "Compte utilisateur pour $UtilisateurPrenom $UtilisateurNom"
37             ChangePasswordAtLogon = $true
38         }
39         New-ADUser @userParams
40         Write-Output "Création de l'utilisateur : $($UtilisateurNom.Substring(0,1))$UtilisateurPrenom ($UtilisateurNom $UtilisateurPrenom)"
41     }
42 }
43 }
```

0.2 Créations des OU Groupes manuel et ou avec script:

Nom	Type	Description
SIE--Technique	Groupe de sécurité	
SIE--Qualiticien	Groupe de sécurité	
SIE--Direction	Groupe de sécurité	
SIE--Compta	Groupe de sécurité	
SIE--Cadres	Groupe de sécurité	
SIE--Admnistratif	Groupe de sécurité	

Nouvel objet - Groupe

Créer dans : centreretraite.local/Siege/groupes

Nom du groupe :

Nom de groupe (antérieur à Windows 2000) :

Étendue du groupe

Domaine local

Globale

Universelle

Type de groupe

Sécurité

Distribution

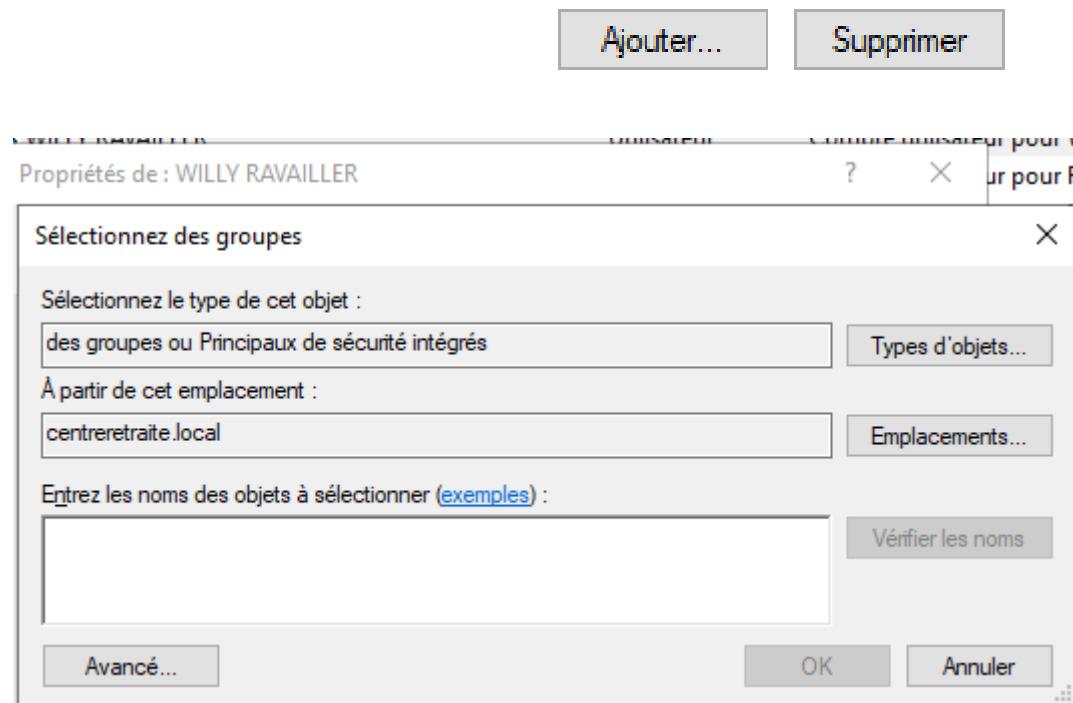
OK Annuler

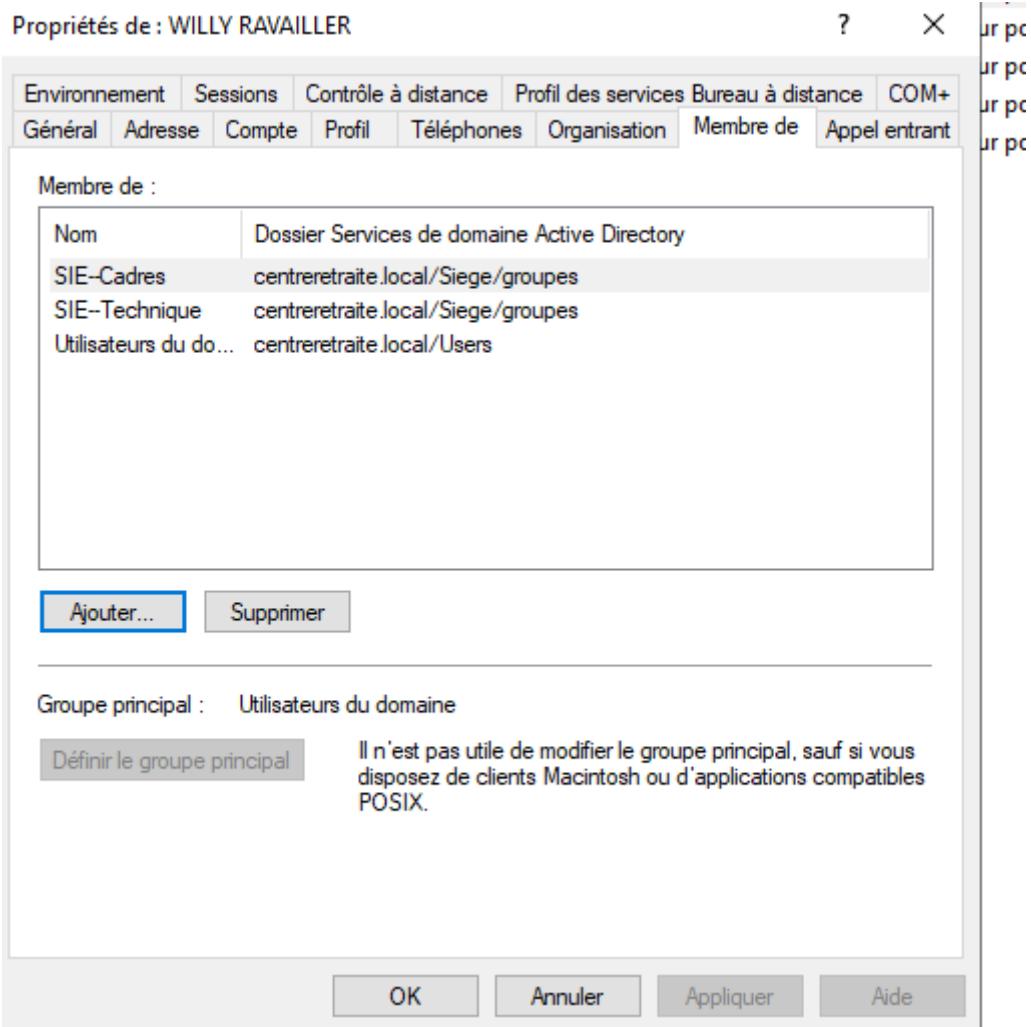
- une fois les OU groupes crée sa donne ceci :

The screenshot shows the Windows Active Directory Users and Computers interface. On the left, a navigation pane displays the organizational structure of the domain 'centreretraite.local'. Under the 'Siege' container, there are two sub-containers: 'computers' and 'groupes'. The 'groupes' container is selected. On the right, a list view shows six security groups with their names, types, and descriptions:

Nom	Type	Description
SIE--Technique	Groupe de sécurité	
SIE--Qualiticien	Groupe de sécurité	
SIE--Direction	Groupe de sécurité	
SIE--Compta	Groupe de sécurité	
SIE--Cadres	Groupe de sécurité	
SIE--Administratif	Groupe de sécurité	

- Pour intégrer un Users dans un groupe faut Double Cliquer sur un Users et dans l'icône [Membre défaut] cliquez sur :





- a la fin sa donne ceci :

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Utilisateurs et ordinateurs Active

- > Requêtes enregistrées
- centreretraite.local
 - > 06--GABRES
 - > 06--SIEGE
 - > 83--HERMITAGE
 - > 94--CASCADE
 - > Builtin
 - > Cascade
 - > computers
 - > groupes
 - > users
 - > Computers
 - > Domain Controllers
 - > ForeignSecurityPrincipal
 - > Gabres
 - > Hermitage
 - > Managed Service Account
 - > Siege
 - > computers
 - > groupes

Nom	Type	Description
SIE--Technique	Groupe de séc...	
SIE--Qualiticien	Groupe de séc...	
SIE--Direction	Groupe de séc...	
SIE--Compta	Groupe de séc...	
SIE--Cadres	Groupe de séc...	
SIE--Administratif	Groupe de séc...	

Job 3

Connectez ensuite ces postes à votre environnement Active Directory.

0.1 Récupérer l'IP de la VM Windows server

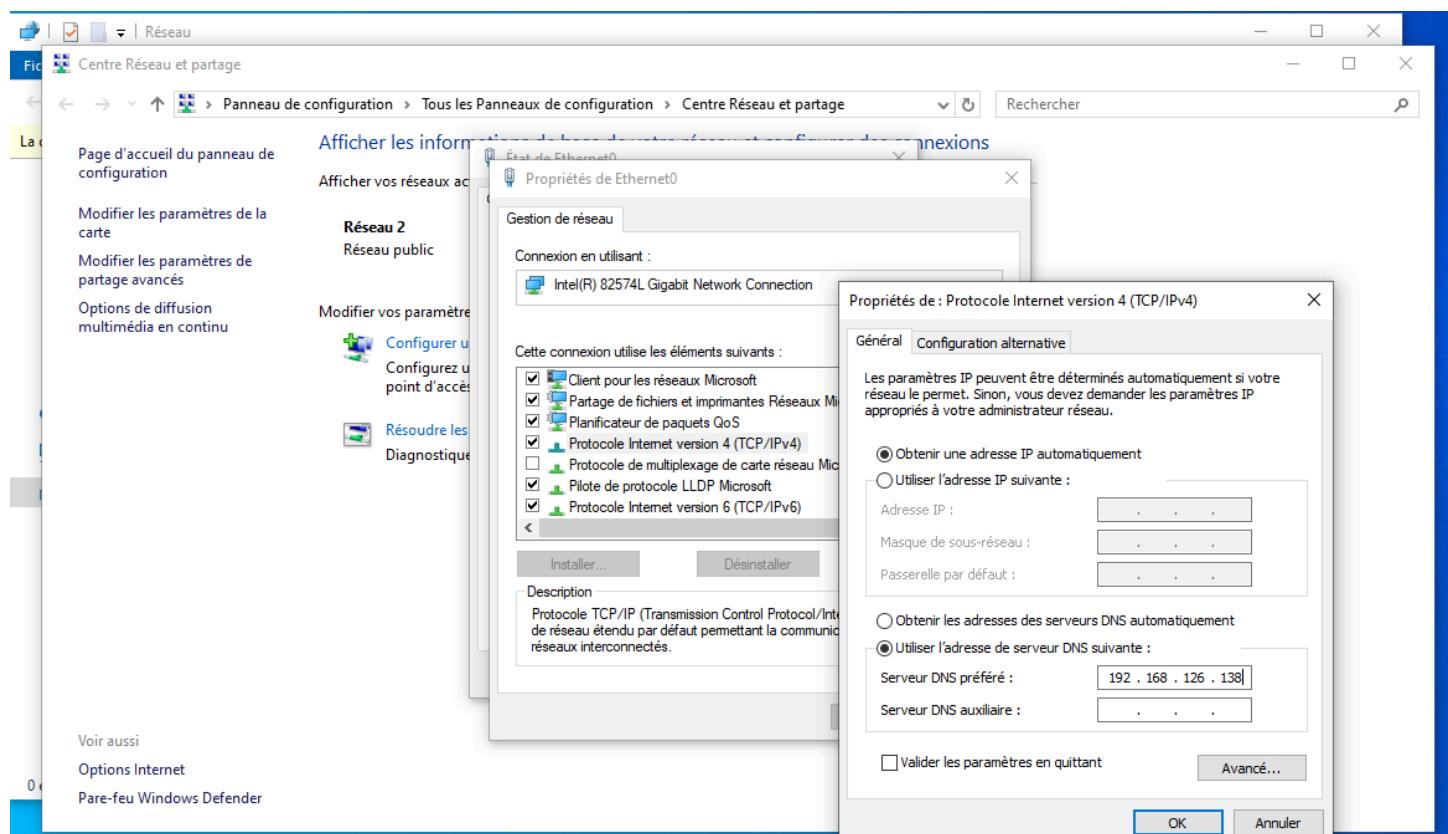
```
PS C:\Users\Administrateur> ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion . . . . . : localdomain
    Adresse IPv6 de liaison locale . . . . . : fe80::4f12:dc06:48c2:9350%15
    Adresse IPv4 . . . . . : 192.168.126.138
    Masque de sous-réseau . . . . . : 255.255.255.0
    Passerelle par défaut . . . . . : 192.168.126.2
```

0.2 puis la mettre dans la VM de windows Client :

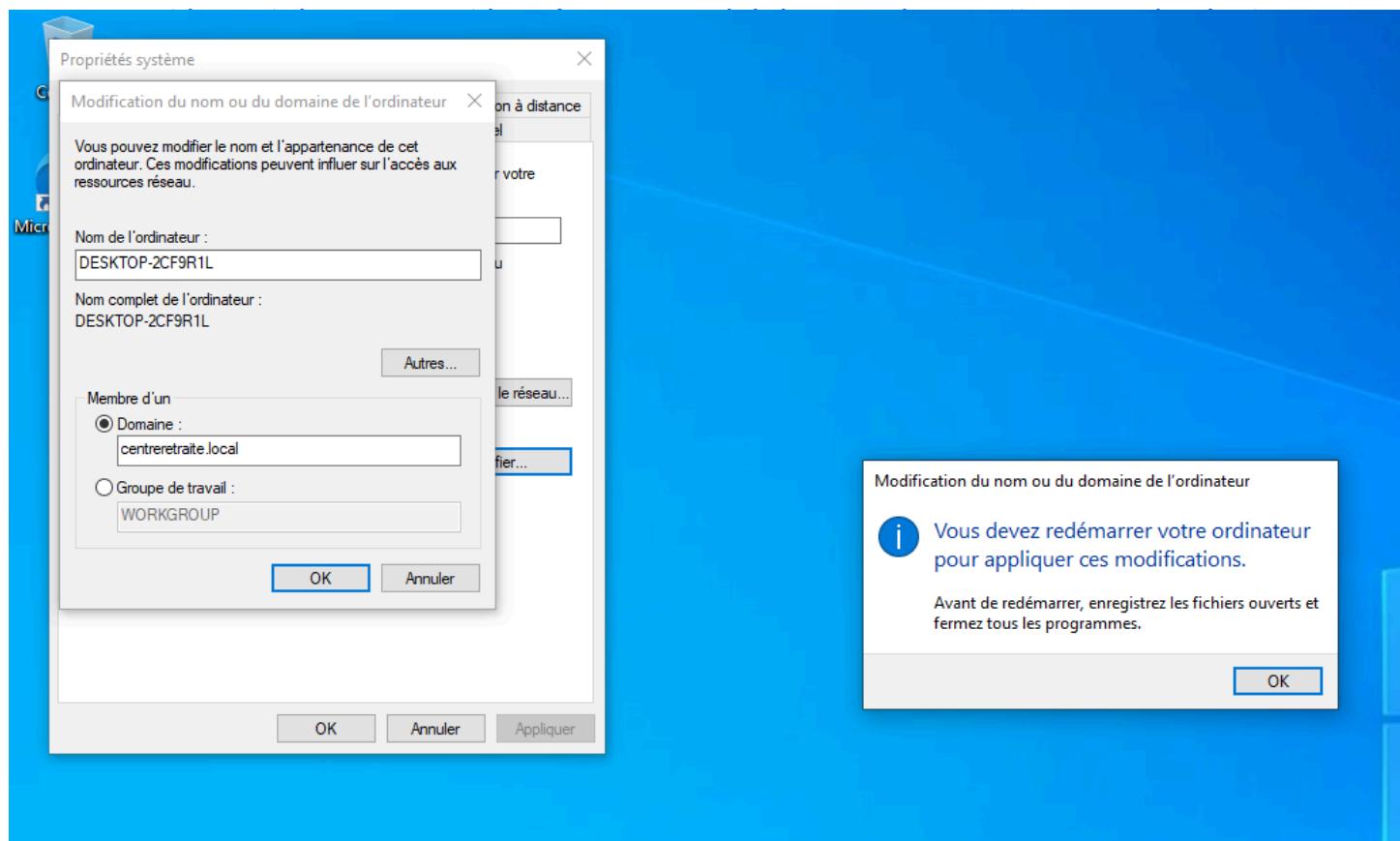


Puis dans la même VM mettre en membre du domaine le serveur DNS :

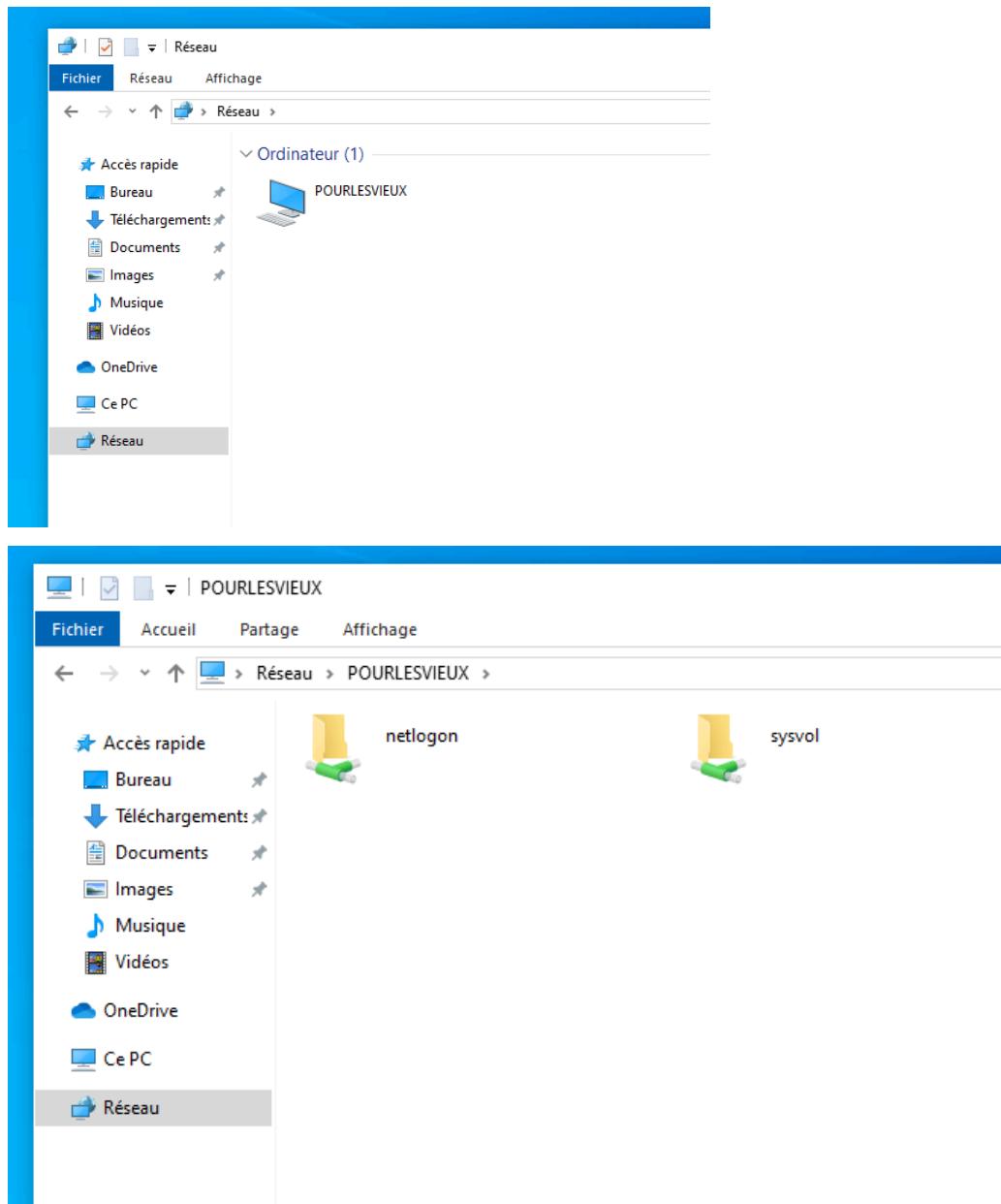
ATTENTION !

Lors de saisie du nom d'utilisateur bien indiquer le nom complet de connexion qui est pour cette exemple

CENTRERETRAITE\Administrateur



On peut voir sur VM Client dans “Réseau” la présence de la connexion vers VM Active directory :



- On retrouve le nom de l'ordinateur Client connecter a Active Directory

The screenshot shows the "Utilisateurs et ordinateurs Active Directory" snap-in. The left navigation pane shows a tree structure under "centretrretraite.local": "Requêtes enregistrées", "centretrretraite.local" (expanded to show "06--GABRES", "06--SIEGE", "83--HERMITAGE", "94--CASCADE", "BuiltIn", "Cascade", "Computers", "Domain Controllers", "ForeignSecurityPrincipal", and "Gabres"). The right pane is titled "Nom" and lists "DESKTOP-2CF9R1L".

nota: script pour remove retirée la sécurité supprimée “OU”

Set-ADOrganizationalUnit -Identity "OU=94--CASCADE,DC=centreretraite,DC=local" -ProtectedFromAccidentalDeletion \$false

```
scriptCSVUserAD.ps1 ScriptRemove.ps1 X
1 Set-ADOrganizationalUnit -Identity "OU=06--GABRES,DC=centreretraite,DC=local" -ProtectedFromAccidentalDeletion $false
2 Set-ADOrganizationalUnit -Identity "OU=06--SIEGE,DC=centreretraite,DC=local" -ProtectedFromAccidentalDeletion $false
3 Set-ADOrganizationalUnit -Identity "OU=83--HERMITAGE,DC=centreretraite,DC=local" -ProtectedFromAccidentalDeletion $false
4 Set-ADOrganizationalUnit -Identity "OU=94--CASCADE,DC=centreretraite,DC=local" -ProtectedFromAccidentalDeletion $false
```

Tableau de bord gestionnaire de serveur :

Gestionnaire de serveur › Tableau de bord

BIENVENUE DANS GESTIONNAIRE DE SERVEUR

DÉMARRAGE RAPIDE

1 Configurer ce serveur local

2 Ajouter des rôles et des fonctionnalités

3 Ajouter d'autres serveurs à gérer

4 Créer un groupe de serveurs

5 Connecter ce serveur aux services cloud

Masquer

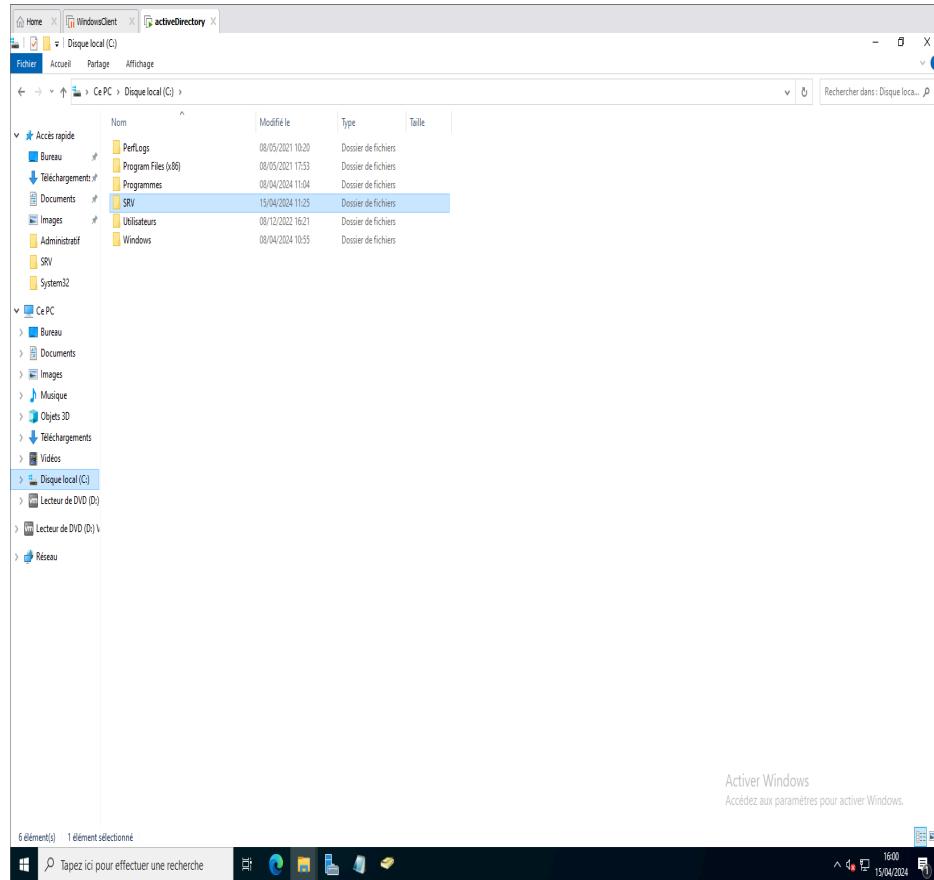
Rôles et groupes de serveurs

Rôles : 3 | Groupes de serveurs : 1 | Nombre total de serveurs : 1

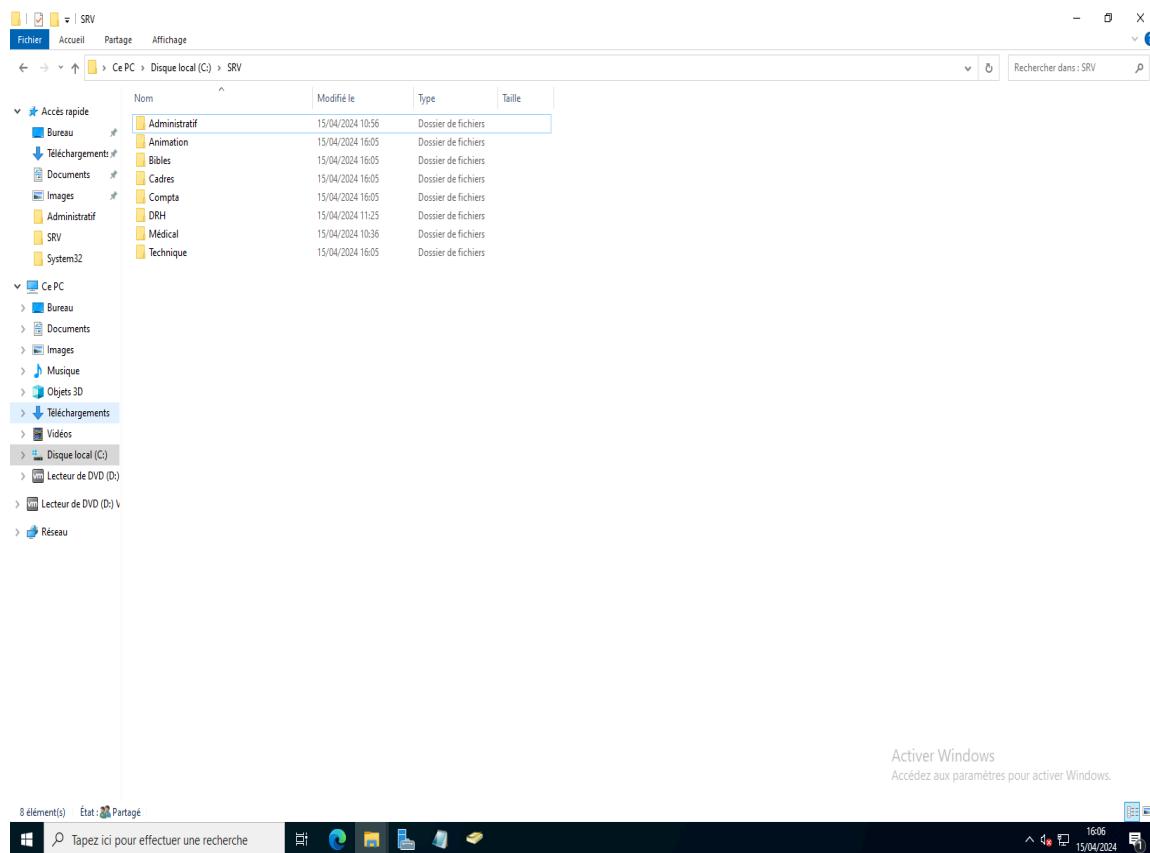
Role	Count
AD DS	1
DNS	1
Services de fichiers et de stockage	1
Serveur local	1
Tous les serveurs	1

- **Création des fichiers à partagé sur chaque utilisateur :**

Dans la VM Active Directory créée dans le lecteur C:\ un dossier SRV



puis dans ce même fichier créé les dossiers concernant les poste d'utilisateur :



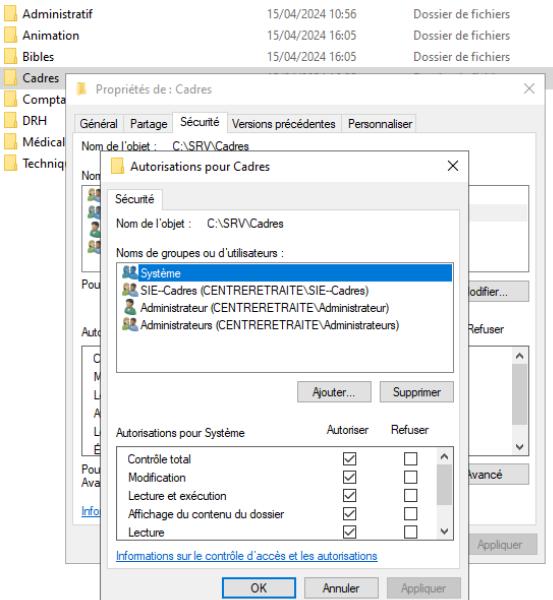
Puis **partager** chaque dossier :

Onglet Sécurité pour créer le lien d'utilisateurs du dossier cadres ci dessous:

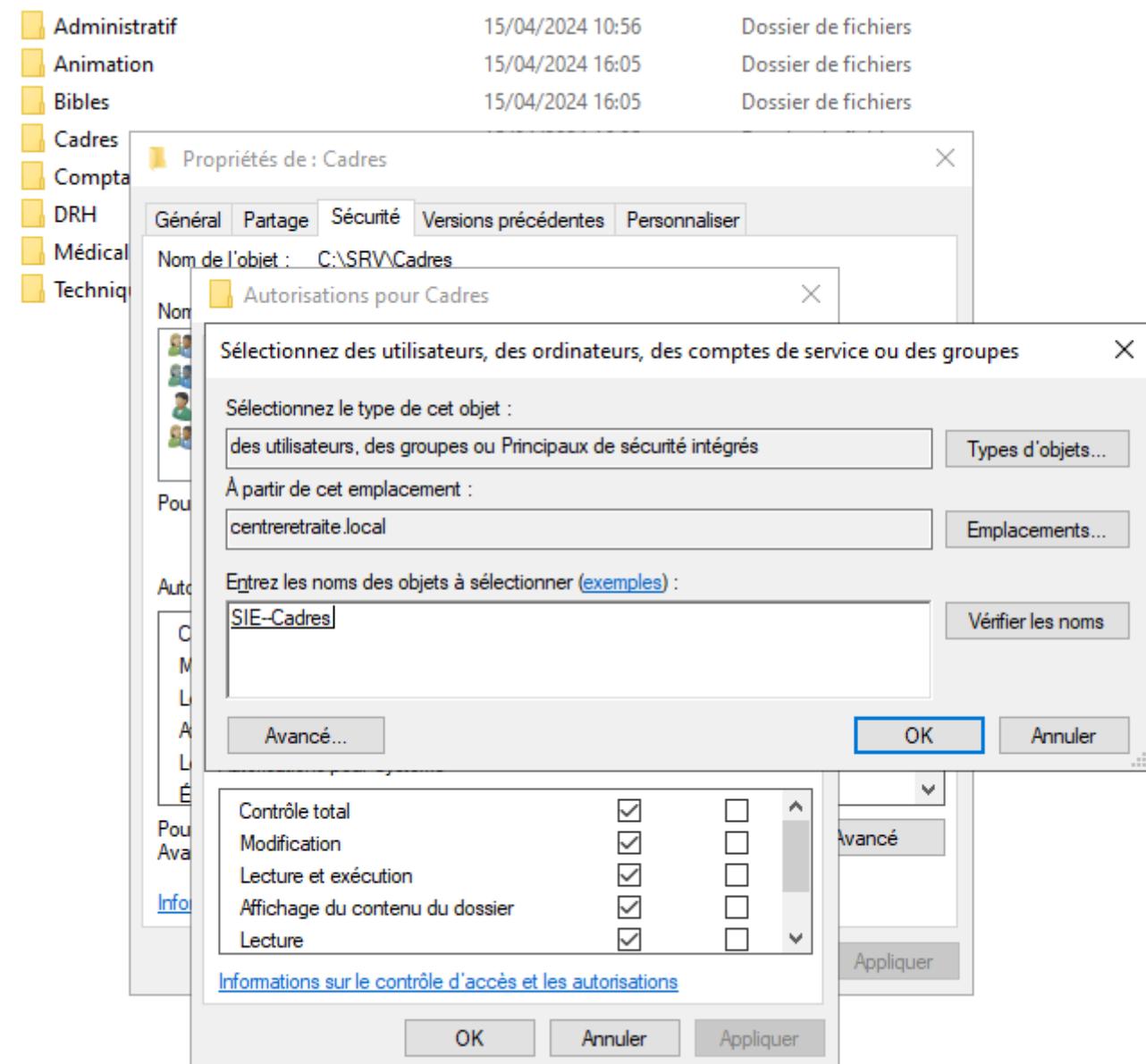
Nota : Ne pas oublier de supprimer les héritages sur avancées et sa vous permettra de supprimer le partage de Tout le Monde

The screenshot shows a Windows File Explorer window with a list of folders in the background. In the foreground, a 'Propriétés de : Cadres' (Properties of : Cadres) dialog box is open. The 'Sécurité' (Security) tab is selected. The 'Nom de l'objet' (Object name) is listed as 'C:\SRV\Cadres'. Under 'Noms de groupes ou d'utilisateurs' (Names of groups or users), 'Tout le monde' (Everyone) is selected. A note says 'Pour modifier les autorisations, cliquez sur Modifier.' (To modify permissions, click on Modify). Below this, under 'Autorisations pour Tout le monde' (Permissions for Everyone), all checkboxes are checked: 'Contrôle total' (Full control), 'Modification' (Modify), 'Lecture et exécution' (Read & execute), 'Affichage du contenu du dossier' (Read the contents of the folder), 'Lecture' (Read), and 'Écriture' (Write). A link 'Informations sur le contrôle d'accès et les autorisations' (Information about access control and permissions) is provided. At the bottom, there are 'Fermer' (Close), 'Annuler' (Cancel), and 'Appliquer' (Apply) buttons.

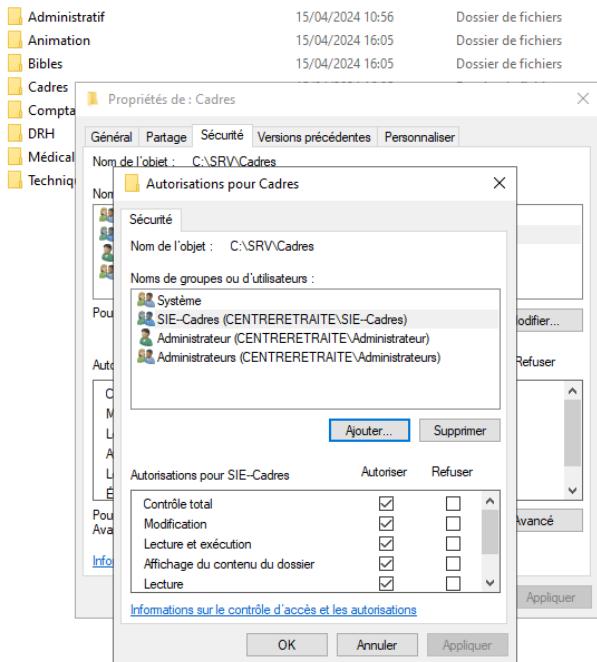
cliquez sur Modifier :



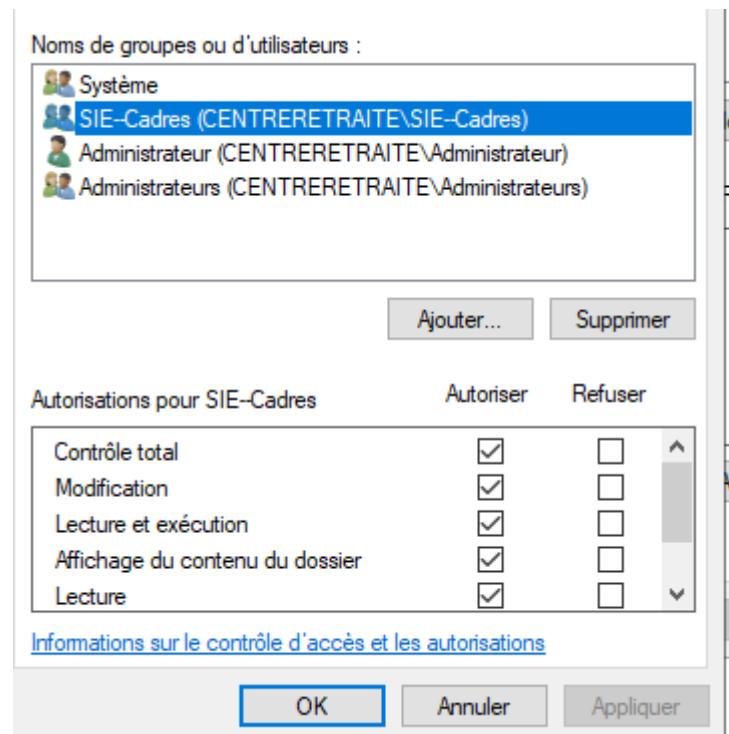
puis rechercher le nom des objets crée sur actives directory concernant Les OU Groupes :



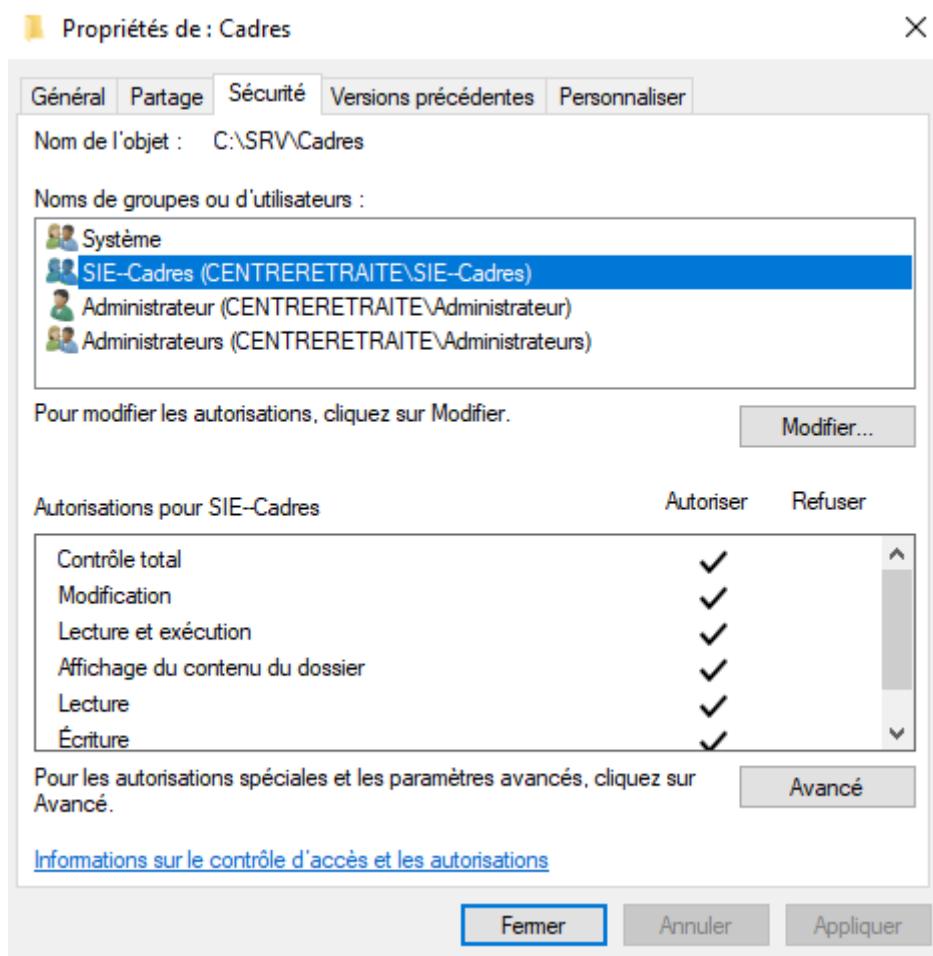
sa doit afficher ceci dans la fenêtre de l'OU doit être apparent sur la fenêtre :



Puis donner ci dessous les autorisations qui concernent les utilisateurs qui auront accès au dossier :



à la fin ça doit donner ceci :



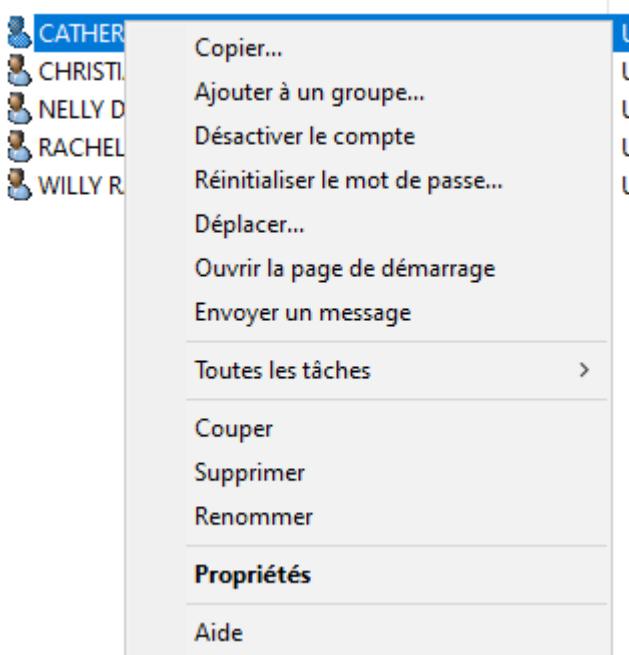
puis on va sur **utilisateur de AD** :

The screenshot shows the 'Utilisateurs et ordinateurs Active Directory' window. The left navigation pane shows the structure: 'Utilisateurs et ordinateurs Active' > 'centreretraite.local' > '06--Gabres' > 'users'. The main pane displays a table of users:

Nom	Type	Description
CATHERINE BURBAN	Utilisateur	Compte utilisateur pour CATHERINE BURBAN
CHRISTIAN PAPIN	Utilisateur	Compte utilisateur pour CHRISTIAN PAPIN
NELLY DELAHAYE	Utilisateur	Compte utilisateur pour NELLY DELAHAYE
RACHEL PALEGALU	Utilisateur	Compte utilisateur pour RACHEL PALEGALU
WILLY RAVAILLER	Utilisateur	Compte utilisateur pour WILLY RAVAILLER

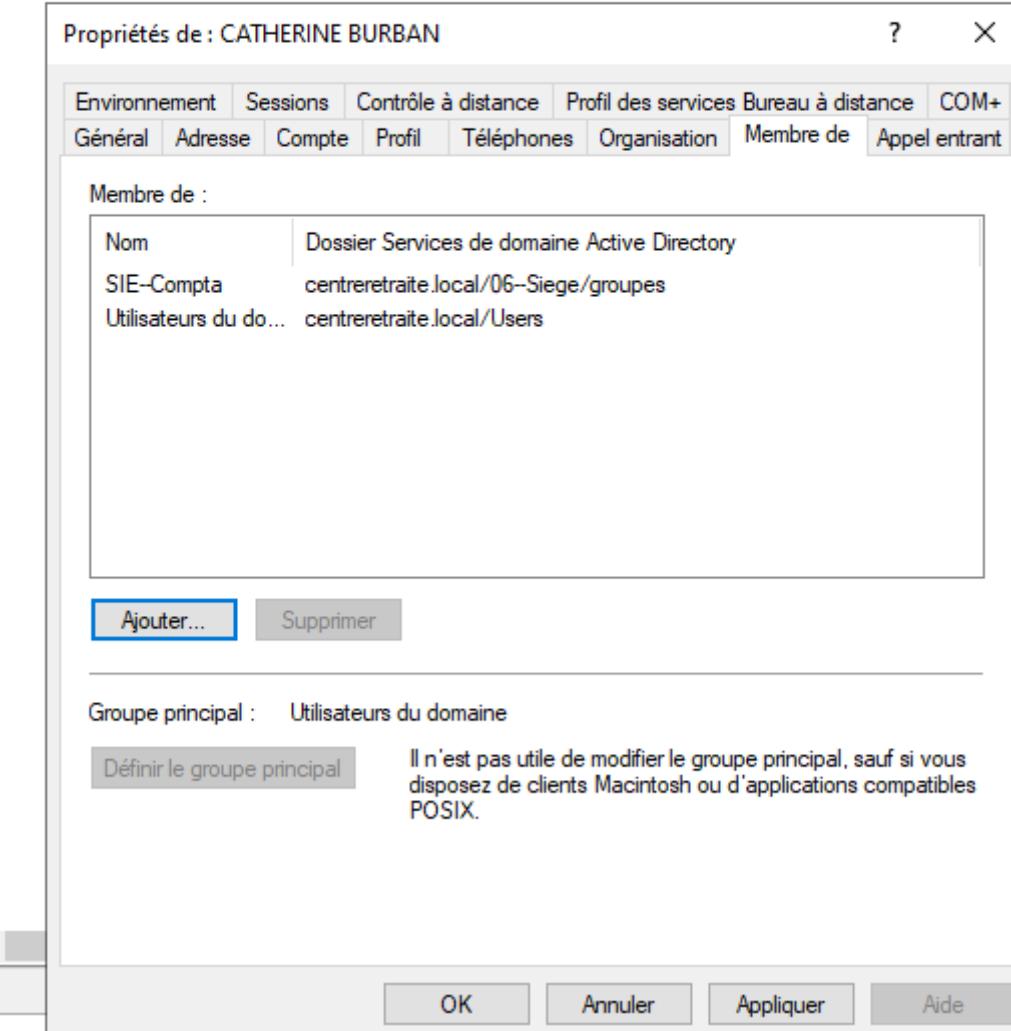
on va **sélectionner** un Utilisateur cadres dans cette exemple tous sont cadres prenoms **Catherine BURBAN** comme exemple :

- **Clique droit** sur le nom et on sélectionne **Propriétés** :



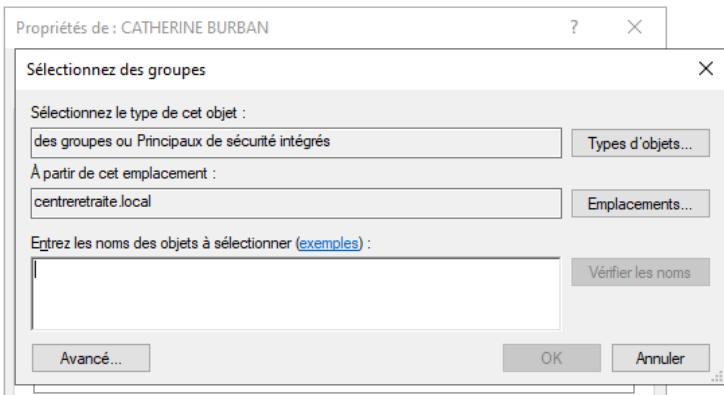
puis on sélectionne **Membres de :**

Nom	Type	Description
CATHERINE BURBAN	Utilisateur	Compte utilisateur pour CATHERINE BURBAN
CHRISTIAN PAPIN	Utilisateur	Compte utilisateur pour CHRISTIAN PAPIN
NELLY DELAHAYE	Utilisateur	Compte utilisateur pour NELLY DELAHAYE
RACHEL PALEGALU	Utilisateur	Compte utilisateur pour RACHEL PALEGALU
WILLY RAVAILLER	Utilisateur	Compte utilisateur pour WILLY RAVAILLER

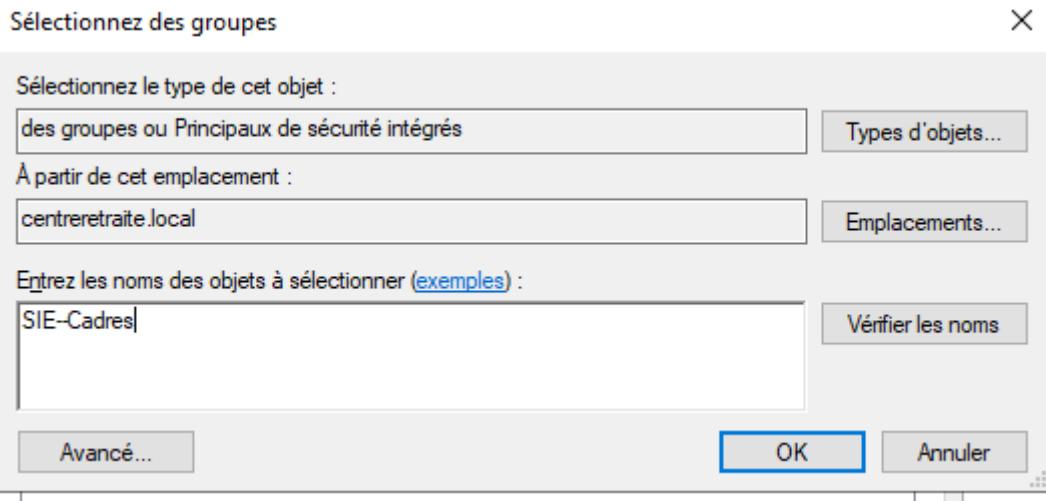


Cliquez sur AJOUTER :

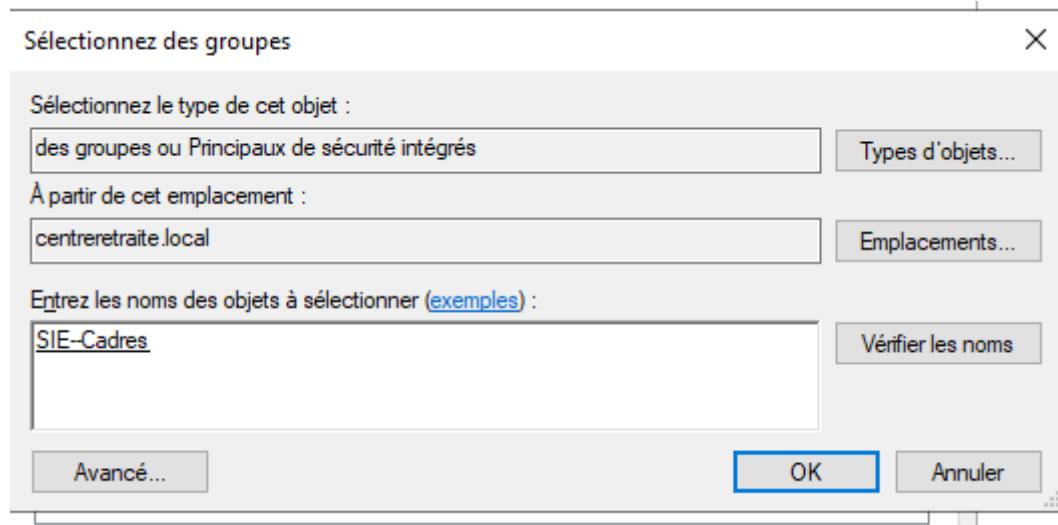
Nom	Type	Description
CATHERINE BURBAN	Utilisateur	Compte utilisateur pour CATHERINE BURBAN
CHRISTIAN PAPIN	Utilisateur	Compte utilisateur pour CHRISTIAN PAPIN
NELLY DELAHAYE	Utilisateur	Compte utilisateur pour NELLY DELAHAYE
RACHEL PALEGALU	Utilisateur	Compte utilisateur pour RACHEL PALEGALU
WILLY RAVAILLER	Utilisateur	Compte utilisateur pour WILLY RAVAILLER



et remplissez la fenêtre du nom de L'**OU Groupes** à partager avec Catherine :



Puis on clique sur **Vérifier les NOMS** : nota lorsqu'ils trouvent le groupe il le surligne et faut cliquez sur OK :



et le Dossier de service d'AD est visible Catherine fais parti de L'OU Groupes et pourra voir et Modifier les dossiers Cadres:

Propriétés de : CATHERINE BURBAN

Membre de :

Nom	Centre
SIE-Cadres	centreerretraite.local/06-Siege/groupes
SIE-Compta	centreerretraite.local/06-Siege/groupes
Utilisateurs du do...	centreerretraite.local/Users

Ajouter... Supprimer

Groupe principal : Utilisateurs du domaine

Il n'est pas utile de modifier le groupe principal, sauf si vous disposez de clients Macintosh ou d'applications compatibles POSIX.

OK Annuler Appliquer Aide

Appliquer et OK!

On peut vérifier elle partage bien le dossier Cadres :

Propriétés de : CATHERINE BURBAN

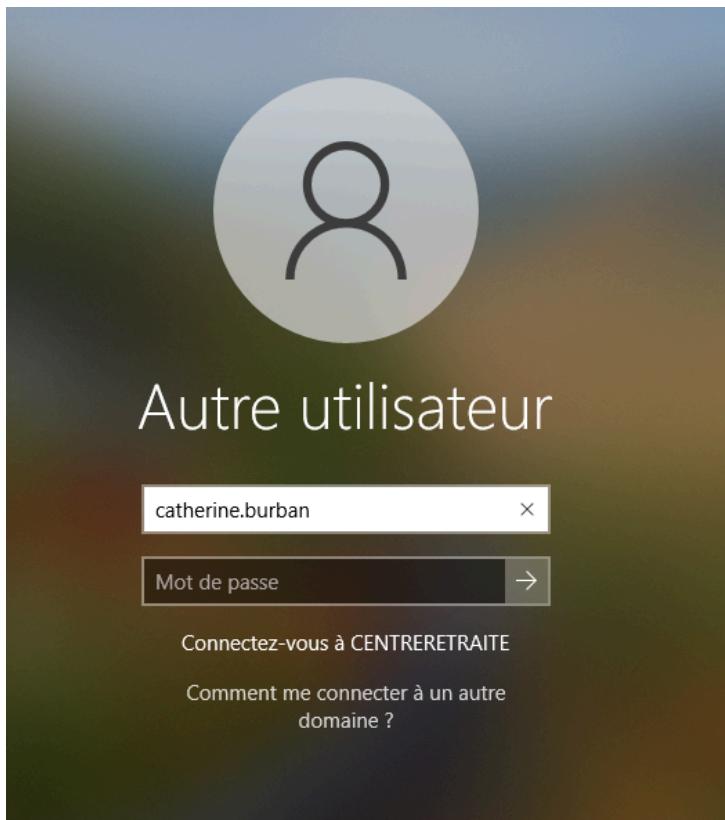
Membre de :

Nom	Centre
SIE-Cadres	centreerretraite.local/06-Siege/groupes
SIE-Compta	centreerretraite.local/06-Siege/groupes
Utilisateurs du do...	centreerretraite.local/Users

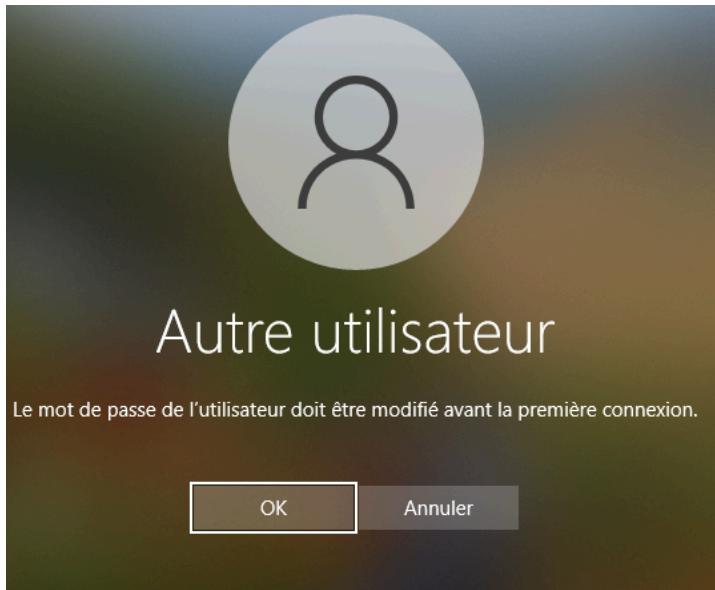
Ajouter... Supprimer

OK Annuler Appliquer Aide

On va ouvrir la cession de **Catherine** sur la **VM Windows client** et on vérifie que les dossiers concernant **Catherine** lui sont bien partagés:



mdp Azerty06! premiere utilisation puis demande du nouveau mot de passe:





Autre utilisateur

catherine.burban

••••••••

••••••••••

•••••••••••



Connectez-vous à CENTRERETRAITE

Comment me connecter à un autre
domaine ?

Annuler

MDP : Laplateforme.io

cession créé :

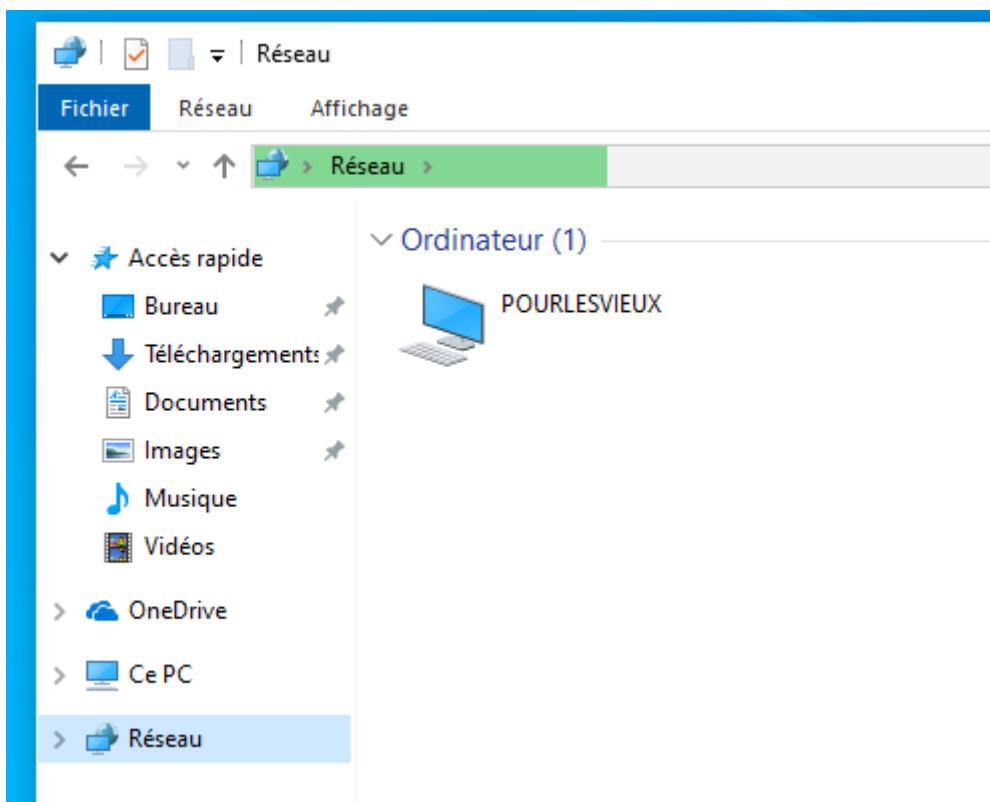


CENTRERETRAITE\catherine.burban

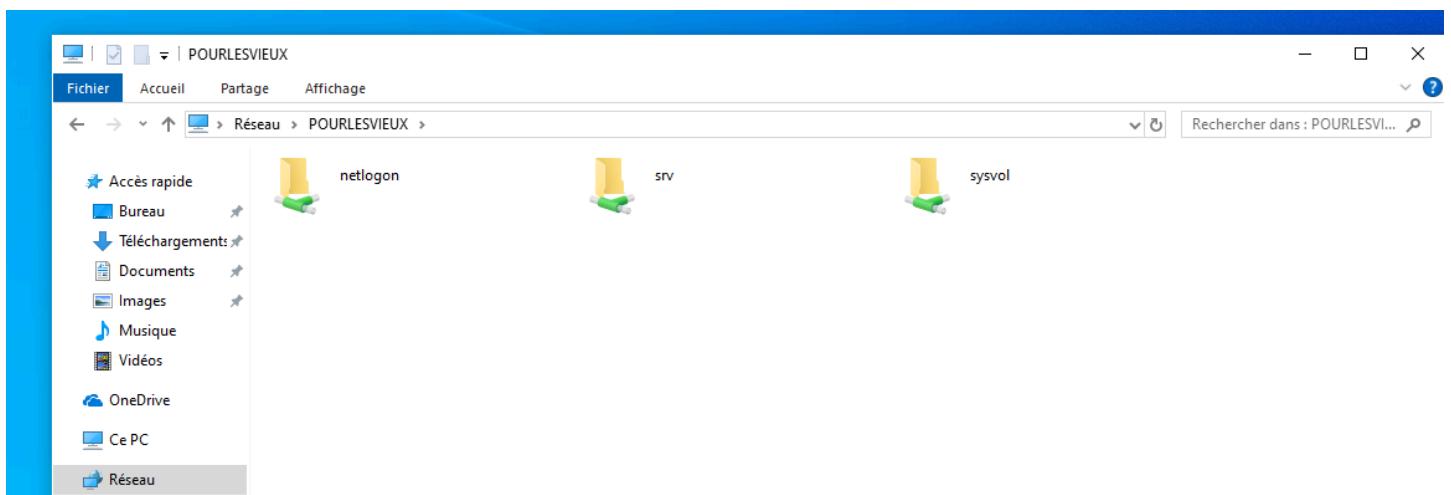
Mot de passe



Montage du Réseau :



on peut voir le dossier partagé **SRV** de la VM AD :



On peut voir que le compte **Catherine** qui peut accéder au **Dossier Cadres et Compta** :

