Active Directory sur Windows Server – Collège Pasteur

Contexte du projet

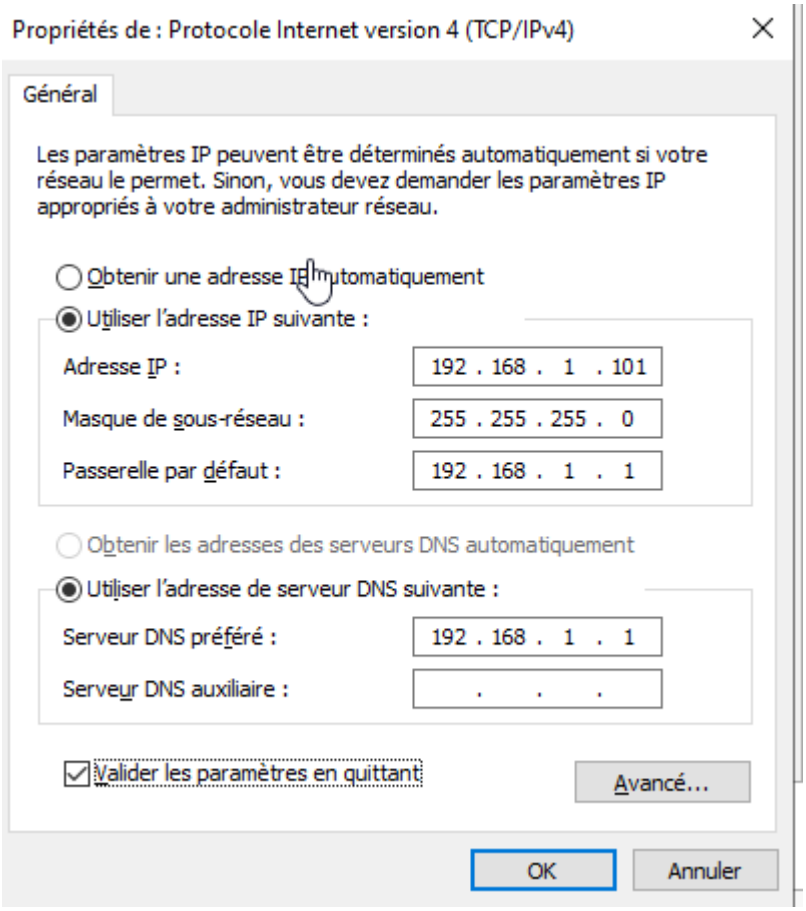
Déploiement d'un annuaire Active Directory pour un établissement scolaire (collège Pasteur, domaine clg-pasteur.lan) : contrôleur de domaine et DNS intégré, arborescence d'OU calquée sur l'organisation, gestion des comptes et groupes selon le modèle AGDLP, création de masse des élèves par import CSV, puis stratégies de groupe (GPO) pour restreindre les postes élèves et mapper les lecteurs réseau.

Objectif : centraliser l'authentification, l'organisation des objets et l'application des politiques sur l'ensemble des postes.

En production réelle, ce contrôleur serait un serveur physique (ou une VM sur hyperviseur) du LAN de l'établissement ; ici, le tout est monté sur une maquette virtualisée.

Adressage statique

Un contrôleur de domaine doit avoir une IP fixe : les clients et le DNS pointeront vers une adresse qui ne doit jamais changer.



On procède aux mises à jour de sécurité afin d'apporter les correctifs comblant les failles connues.

Schéma de la structure des OU pour une école nommée Pasteur

Les OU organisent l'annuaire et servent de cibles aux GPO. On calque l'arborescence sur l'organisation réelle : direction, professeurs, administratif, élèves.

```
clg-pasteur.lan
└── OU=College
    ├── OU=Utilisateurs
    |   ├── OU=Direction
    |   ├── OU=Professeurs
    |   ├── OU=Administratif
    |   └── OU=Eleves
    ├── OU=Groupes
    |   ├── OU=Global          (groupes GG_*)
    |   └── OU=DomainLocal     (groupes GDL_*)
    └── OU=Ordinateurs
        ├── OU=PC-Direction
        ├── OU=PC-Profs
        └── OU=PC-Salles
```

On commence par le renommage de la machine

```
PS C:\Users\Administrateur> Rename-Computer -NewName "SRV-DC01" -Restart
```

On renomme la machine avant la promotion : le nom d'un contrôleur de domaine ne se change pas facilement une fois le rôle installé.

On pointe le DNS vers le serveur lui-même

Active Directory repose entièrement sur le DNS. Le serveur doit s'interroger lui-même, car il devient le DNS du domaine.

```
PS C:\Users\Administrateur> Set-DnsClientServerAddress -InterfaceAlias "Ethernet0" -ServerAddresses 12
7.0.0.1
```

Installation du rôle AD :

On installe le rôle AD DS (le service d'annuaire) ainsi que ses outils d'administration.

Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

Promotion en contrôleur de domaine pour le collège Pasteur

La promotion crée la forêt et le domaine clg-pasteur.lan, installe le DNS intégré et définit le mot de passe DSRM (mode restauration des services d'annuaire).

```
Install-ADDSForest `
    -DomainName "clg-pasteur.lan" `
    -DomainNetbiosName "CLGPASTEUR" `
    -ForestMode "WinThreshold" `
```

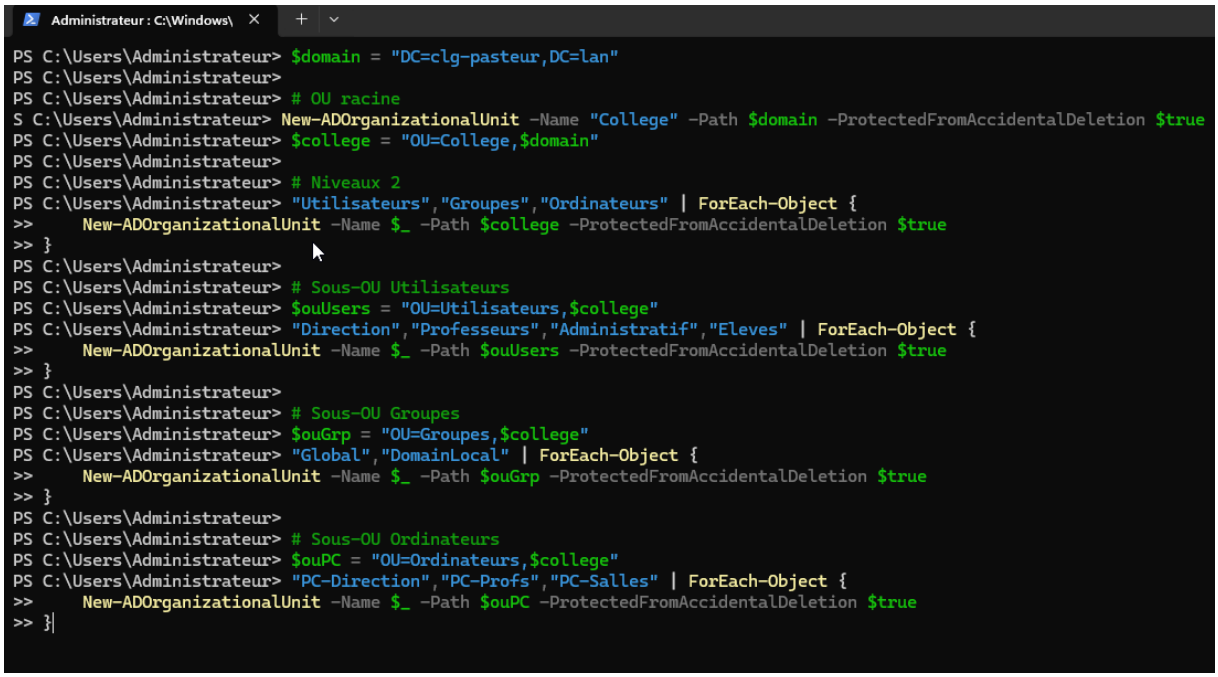
```
    -DomainMode "WinThreshold" `
    -InstallDns:$true `
    -DatabasePath "C:\Windows\NTDS" `
    -SysvolPath "C:\Windows\SYSVOL" `
    -LogPath "C:\Windows\NTDS" `
    -SafeModeAdministratorPassword (ConvertTo-SecureString "Yukinala30!" -
AsPlainText -Force) `
    -Force:$true
```

```
PS C:\Users\Administrateur> Install-ADDSForest `
>>     -DomainName "clg-pasteur.lan" `
>>     -DomainNetbiosName "CLGPASTEUR" `
>>     -ForestMode "WinThreshold" `
>>     -DomainMode "WinThreshold" `
>>     -InstallDns:$true `
>>     -DatabasePath "C:\Windows\NTDS" `
>>     -SysvolPath "C:\Windows\SYSVOL" `
>>     -LogPath "C:\Windows\NTDS" `
>>     -SafeModeAdministratorPassword (ConvertTo-SecureString "Dsrm_LabP@ss2025!" -AsPlainText -Force)
 `
>>     -Force:$true
```

Création des OU racines : utilisateurs, groupes et ordinateurs
On crée l'arborescence en PowerShell pour un déploiement reproductible. L'option ProtectedFromAccidentalDeletion empêche la suppression accidentelle d'une OU entière.

```
$domain = "DC=clg-pasteur,DC=lan"

# OU racine
New-ADOrganizationalUnit -Name "College" -Path $domain -
ProtectedFromAccidentalDeletion $true
$college = "OU=College,$domain"

# Niveaux 2
"Utilisateurs","Groupes","Ordinateurs" | ForEach-Object {
    New-ADOrganizationalUnit -Name $_ -Path $college -
ProtectedFromAccidentalDeletion $true
}

# Sous-OU Utilisateurs
$ouUsers = "OU=Utilisateurs,$college"
"Direction","Professeurs","Administratif","Eleves" | ForEach-Object {
    New-ADOrganizationalUnit -Name $_ -Path $ouUsers -
ProtectedFromAccidentalDeletion $true
}

# Sous-OU Groupes
$ouGrp = "OU=Groupes,$college"
"Global","DomainLocal" | ForEach-Object {
    New-ADOrganizationalUnit -Name $_ -Path $ouGrp -
ProtectedFromAccidentalDeletion $true
}
```

```
# Sous-OU Ordinateurs
$ouPC = "OU=Ordinateurs,$college"
"PC-Direction","PC-Profs","PC-Salles" | ForEach-Object {
    New-ADOrganizationalUnit -Name $_ -Path $ouPC -
ProtectedFromAccidentalDeletion $true
}
```



Création des groupes globaux et des groupes locaux
On applique le modèle AGDLP : les comptes vont dans des groupes Globaux (par fonction), les Globaux entrent dans des groupes Domain Local (par ressource), et c'est sur le Domain Local qu'on pose les droits. On évite ainsi d'attribuer des permissions directement aux comptes.

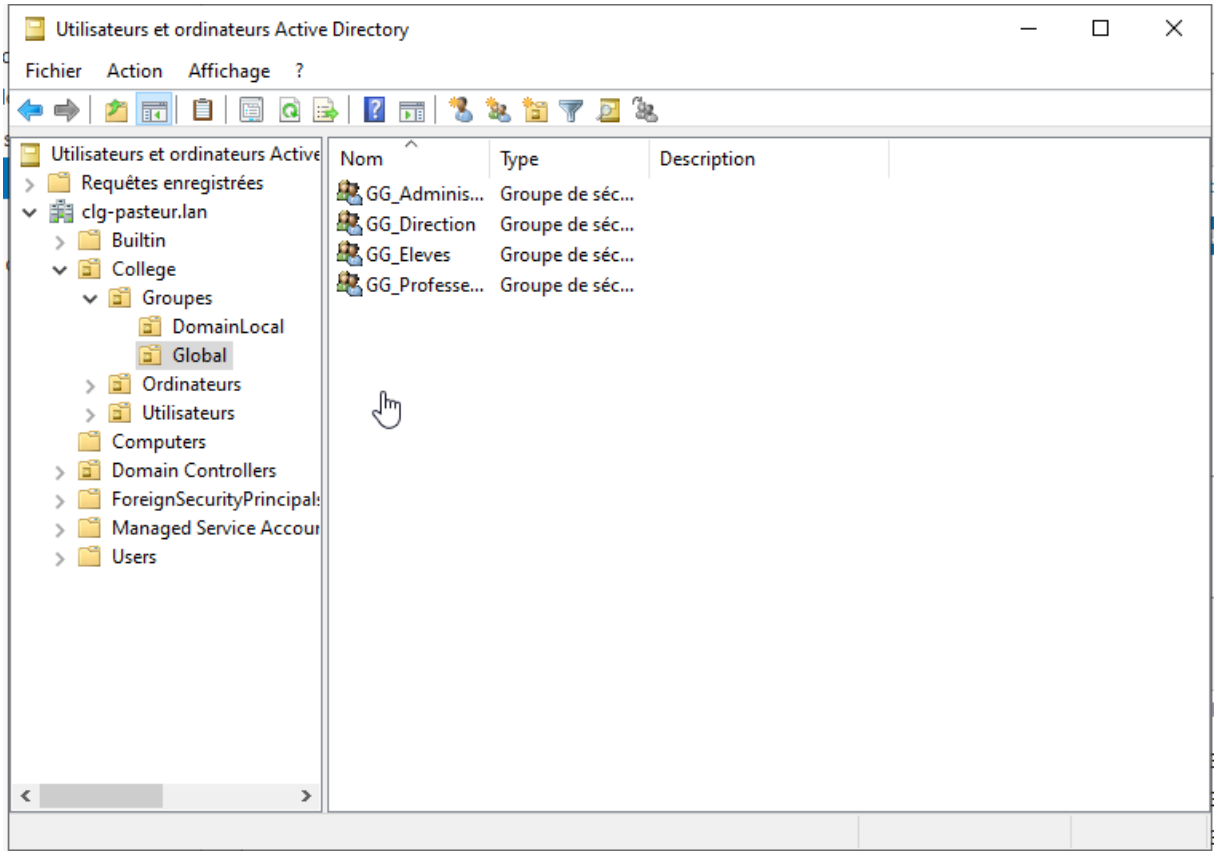
```
$ouGlobal = "OU=Global,OU=Groupes,$college"
$ouDL     = "OU=DomainLocal,OU=Groupes,$college"

# Groupes Globaux pour les postes de l’etablissement
"GG_Direction","GG_Professeurs","GG_Administratif","GG_Eleves" | ForEach-Object
{
    New-ADGroup -Name $_ -GroupScope Global -GroupCategory Security -Path
$ouGlobal
}

# Groupes Domain Local (ressources partagées)
"GDL_Partage_Profs_RW","GDL_Partage_Eleves_RW","GDL_Partage_Commun_R
O" | ForEach-Object {
    New-ADGroup -Name $_ -GroupScope DomainLocal -GroupCategory Security -
Path $ouDL
```

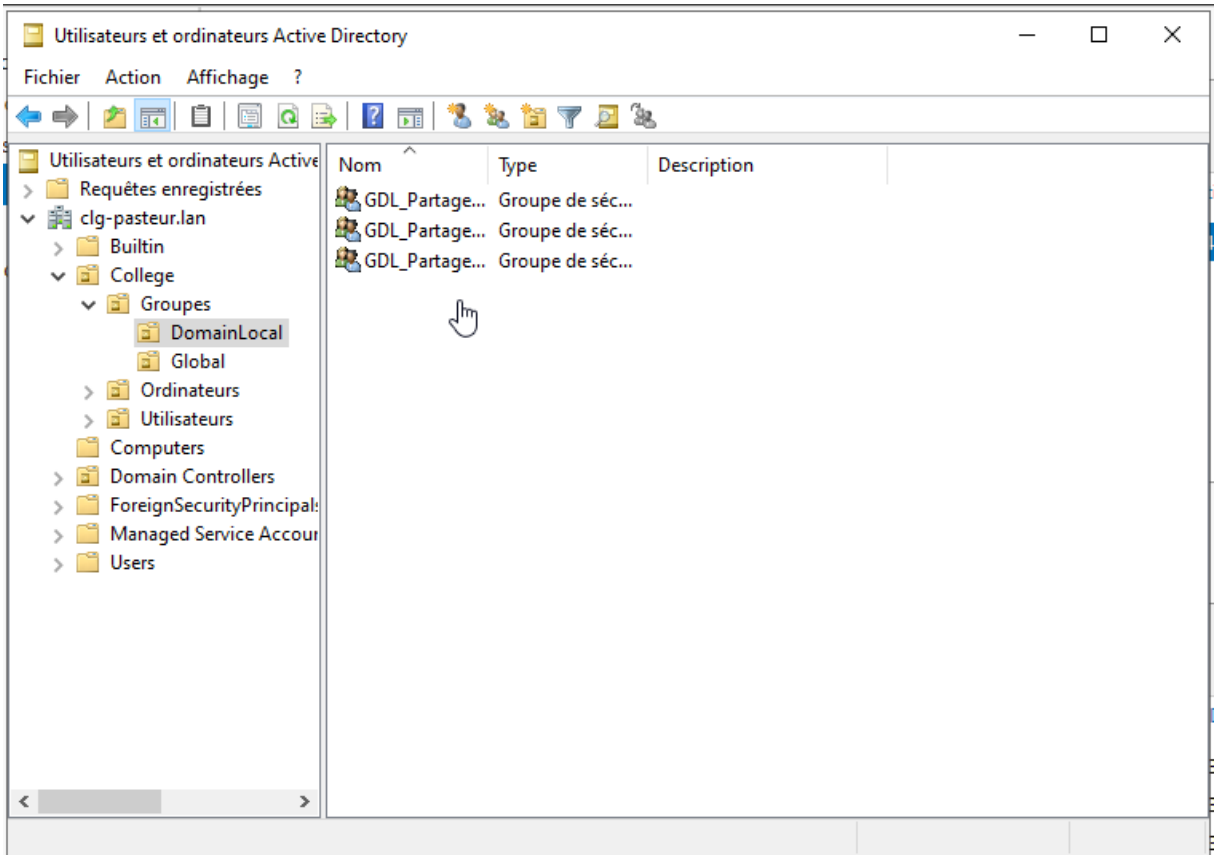
}

Imbrication AGDLP : les Globaux entrent dans les Domain Local
Add-ADGroupMember -Identity "GDL_Partage_Profs_RW" -Members "GG_Professeurs"
Add-ADGroupMember -Identity "GDL_Partage_Eleves_RW" -Members "GG_Eleves"
Add-ADGroupMember -Identity "GDL_Partage_Commun_RO" -Members "GG_Professeurs","GG_Direction"

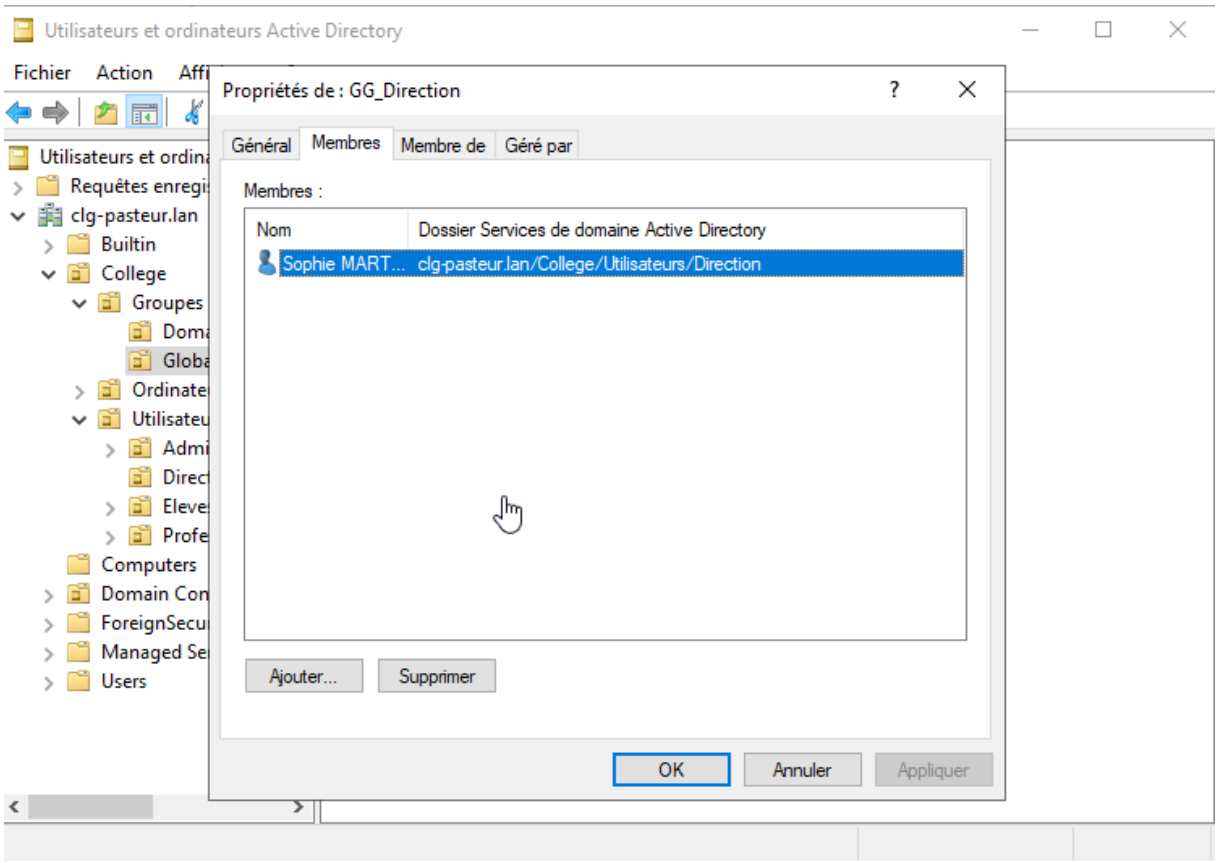
```
PS C:\Users\Administrateur> $ouGlobal = "OU=Global,OU=Groupes,$college"
PS C:\Users\Administrateur> $ouDL     = "OU=DomainLocal,OU=Groupes,$college"
PS C:\Users\Administrateur>
PS C:\Users\Administrateur> # Groupes Globaux (métiers)
PS C:\Users\Administrateur> "GG_Direction","GG_Professeurs","GG_Administratif","GG_Eleves" | ForEach-Object {
>>     New-ADGroup -Name $_ -GroupScope Global -GroupCategory Security -Path $ouGlobal
>> }
PS C:\Users\Administrateur>
PS C:\Users\Administrateur> # Groupes Domain Local (ressources)
PS C:\Users\Administrateur> "GDL_Partage_Profs_RW","GDL_Partage_Eleves_RW","GDL_Partage_Commun_RO" | ForEach-Object {
>>     New-ADGroup -Name $_ -GroupScope DomainLocal -GroupCategory Security -Path $ouDL
>> }
PS C:\Users\Administrateur>
PS C:\Users\Administrateur> # Imbrication AGDLP : les Globaux entrent dans les Domain Local
PS C:\Users\Administrateur> Add-ADGroupMember -Identity "GDL_Partage_Profs_RW"  -Members "GG_Professeurs"
PS C:\Users\Administrateur> Add-ADGroupMember -Identity "GDL_Partage_Eleves_RW" -Members "GG_Eleves"
PS C:\Users\Administrateur> Add-ADGroupMember -Identity "GDL_Partage_Commun_RO" -Members "GG_Professeurs","GG_Direction"
```

Vérification :
On contrôle que l'arborescence et les groupes sont bien créés.

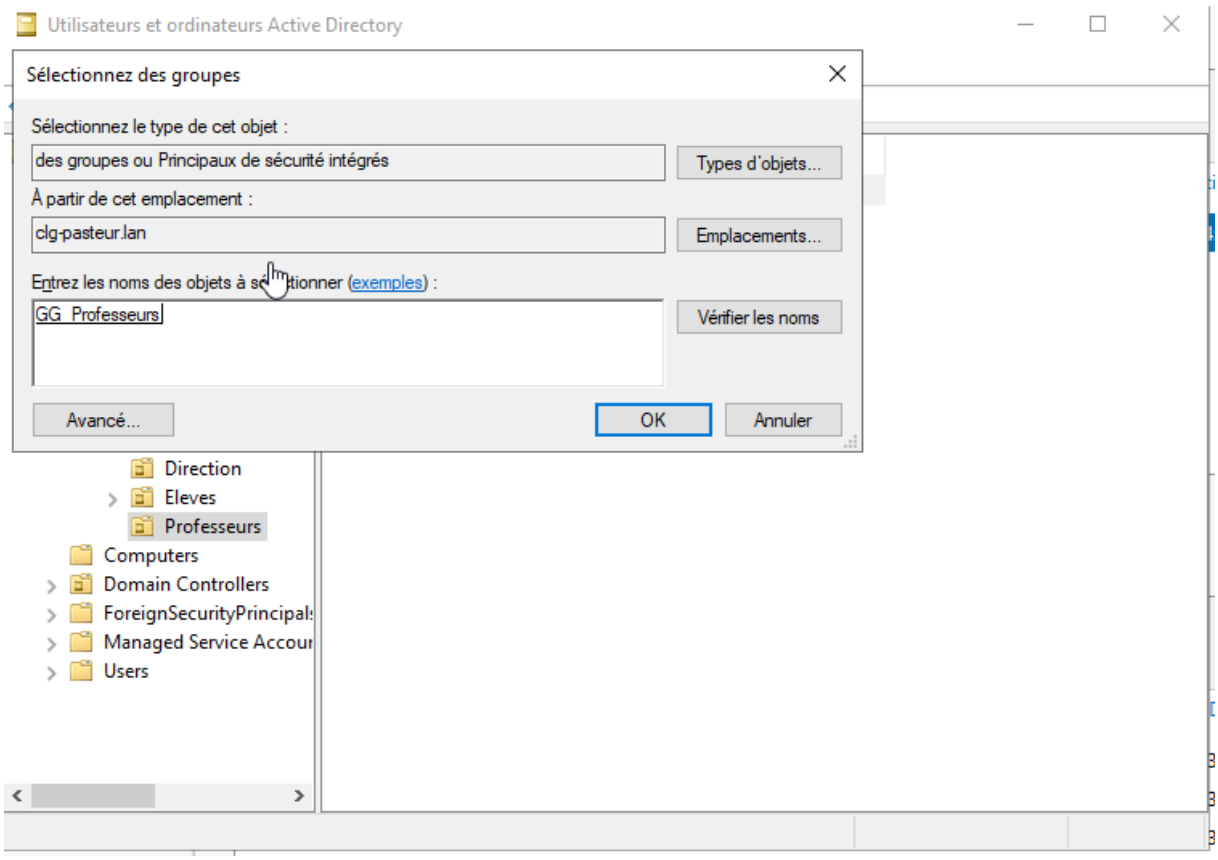




Ajout d'un utilisateur créé dans l'interface graphique au groupe global Direction
On illustre la gestion par console graphique, en complément des scripts.



Ajout de Jean Denton dans le groupe Professeurs



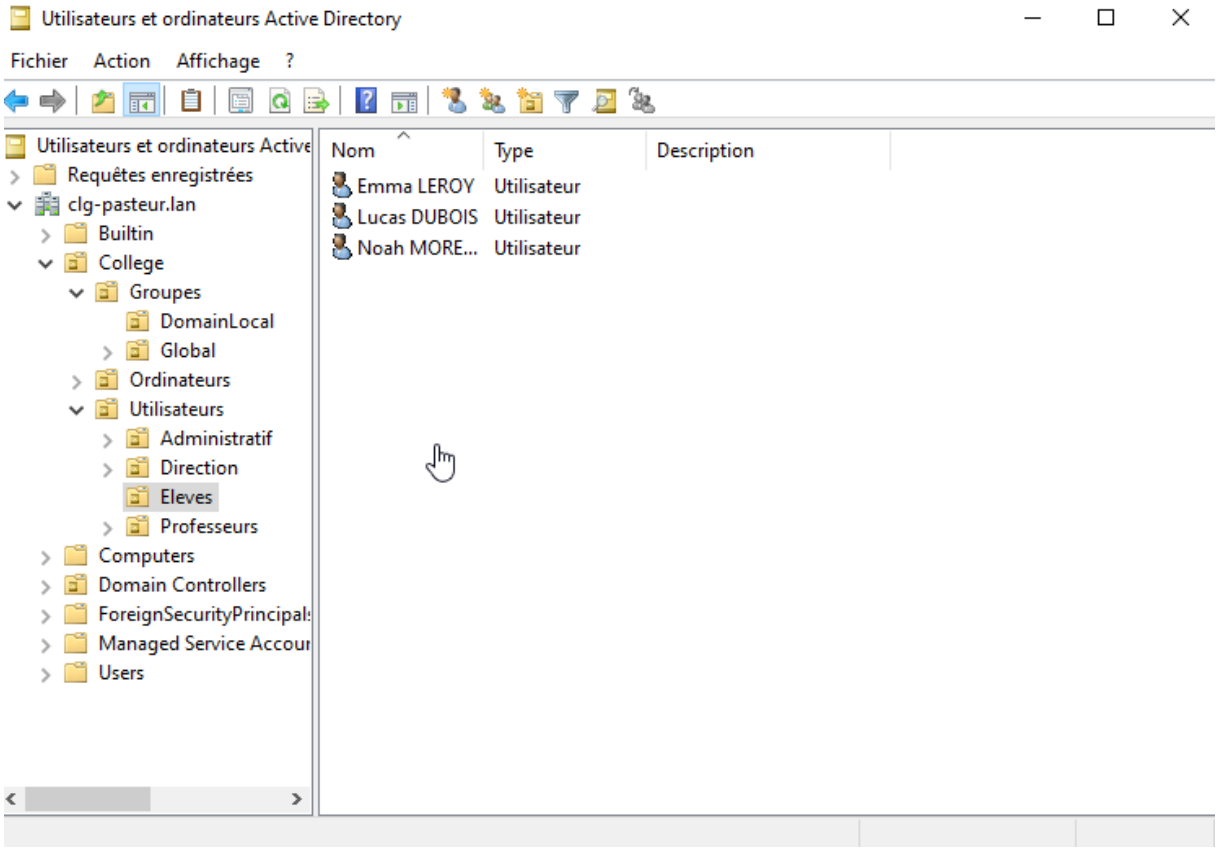
Création du fichier eleves.csv en PowerShell
On prépare un fichier CSV : la création des comptes élèves se fera en masse par import, pas un par un.

```
@'
Prenom,Nom,Login,Classe
Lucas,DUBOIS,l.dubois,6A
Emma,LEROY,e.leroy,6A
Noah,MOREAU,n.moreau,5B
'@ | Out-File "C:\Users\Administrateur\eleves.csv" -Encoding UTF8
```

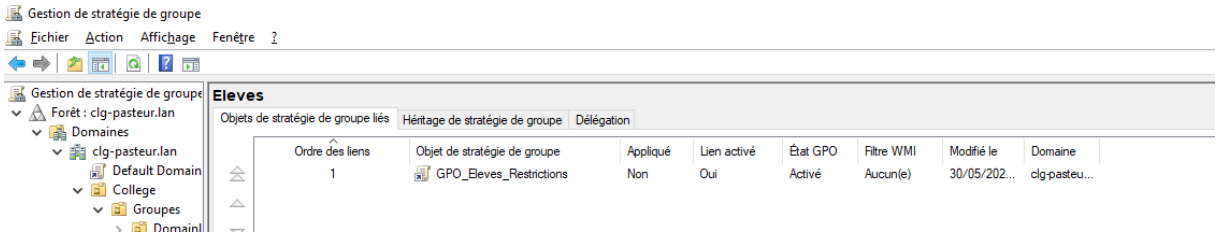
Importation du CSV créé précédemment :
On crée les comptes en masse depuis le CSV, avec changement de mot de passe imposé à la première connexion et ajout automatique au groupe GG_Eleves.

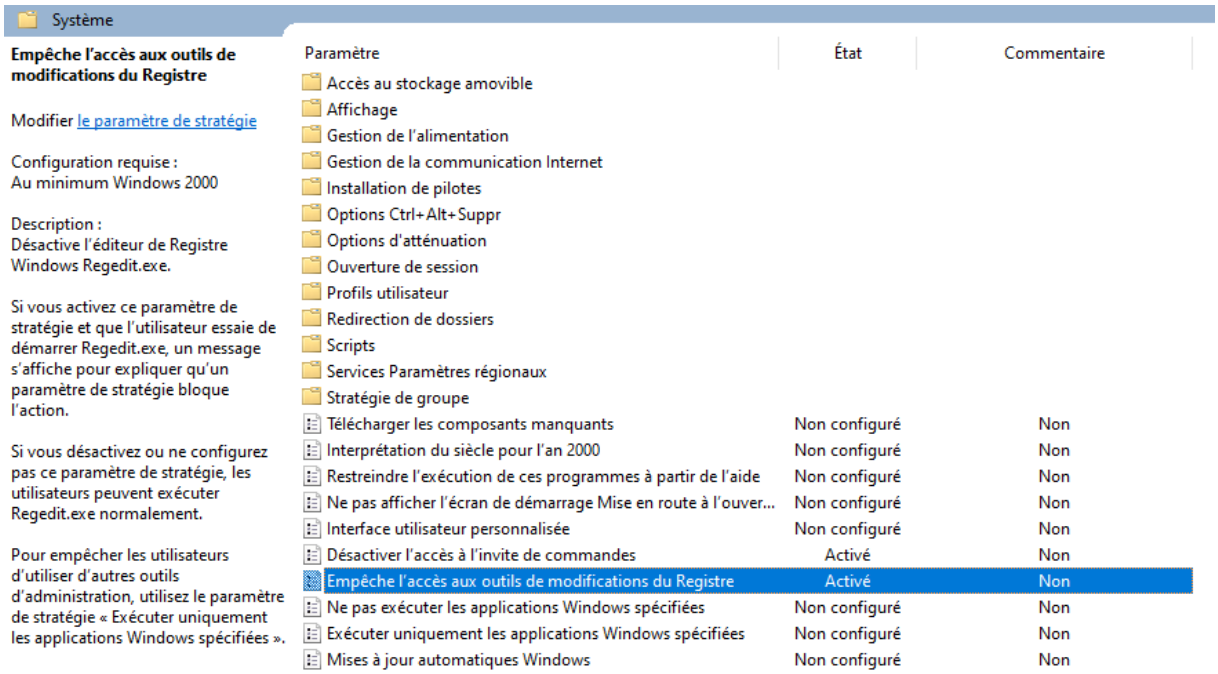
```
pwd = ConvertTo-SecureString "Yukinala30!" -AsPlainText -Force
$ouEleves = "OU=Eleves,OU=Utilisateurs,$college"

Import-Csv " C:\Users\Administrateur\eleves.csv" | ForEach-Object {
   New-ADUser `
      -Name "$($_.Prenom) $($_.Nom)" `
      -GivenName $_.Prenom -Surname $_.Nom `
      -SamAccountName $_.Login `
      -UserPrincipalName "$($_.Login)@clg-pasteur.lan" `
      -Department $_.Classe `
      -Path $ouEleves `
      -AccountPassword $pwd -Enabled $true -ChangePasswordAtLogon $true
   Add-ADGroupMember -Identity "GG_Eleves" -Members $_.Login}
```

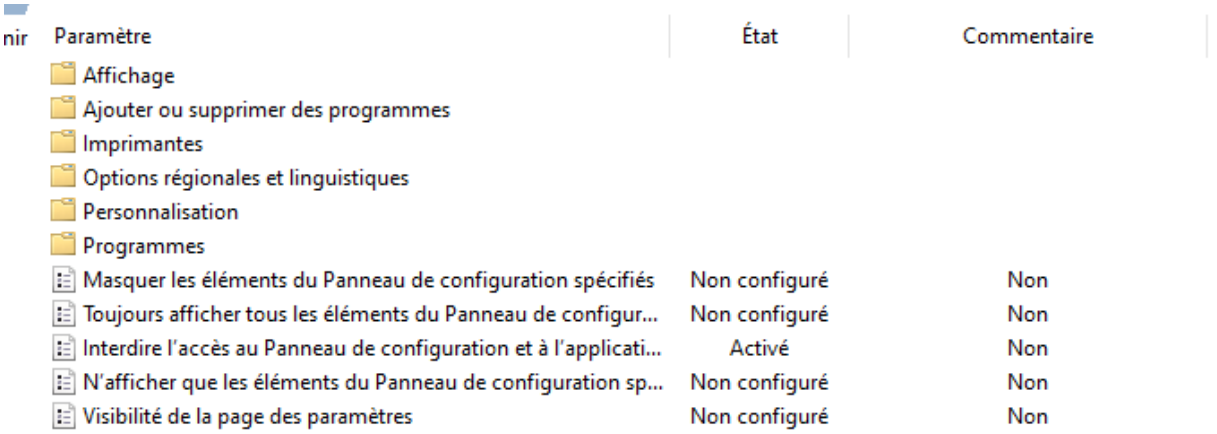
```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        27/05/2026     18:04                3D Objects
d-r---        27/05/2026     18:04                Contacts
d-r---        27/05/2026     18:13                Desktop
d-r---        27/05/2026     18:04                Documents
d-r---        28/05/2026     15:14                Downloads
d-r---        27/05/2026     18:04                Favorites
d-r---        27/05/2026     18:04                Links
d-r---        27/05/2026     18:04                Music
d-r---        27/05/2026     18:04                Pictures
d-r---        27/05/2026     18:04                Saved Games
d-r---        27/05/2026     18:04                Searches
d-r---        27/05/2026     18:04                Videos
-a----        30/05/2026     08:42             99 eleves.csv


PS C:\Users\Administrateur> $pwd = ConvertTo-SecureString "Yukinala30!" -AsPlainText -Force
PS C:\Users\Administrateur>
PS C:\Users\Administrateur> # On ne dépend plus de la session : on fige le DN complet
PS C:\Users\Administrateur> $college  = "OU=College,DC=clg-pasteur,DC=lan"
PS C:\Users\Administrateur> $ouEleves = "OU=Eleves,OU=Utilisateurs,$college"
PS C:\Users\Administrateur>
PS C:\Users\Administrateur> Import-Csv "C:\Users\Administrateur\eleves.csv" | ForEach-Object {
>>     New-ADUser `
>>         -Name "$($_.Prenom) $($_.Nom)" `
>>         -GivenName $_.Prenom -Surname $_.Nom `
>>         -SamAccountName $_.Login `
>>         -UserPrincipalName "$($_.Login)@clg-pasteur.lan" `
>>         -Department $_.Classe `
>>         -Path $ouEleves `
>>         -AccountPassword $pwd -Enabled $true -ChangePasswordAtLogon $true
>>     Add-ADGroupMember -Identity "GG_Eleves" -Members $_.Login
>> }
PS C:\Users\Administrateur>
```

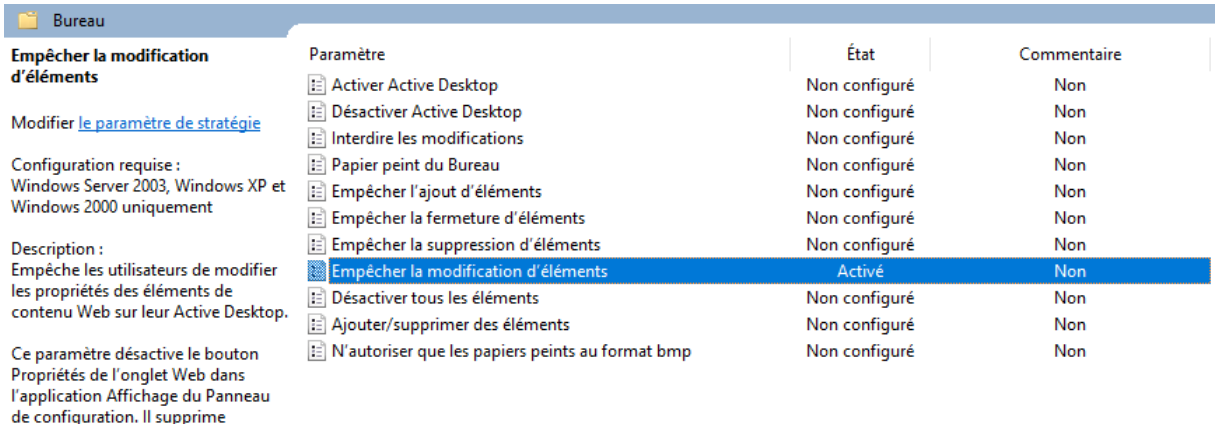


Création d'une GPO « Restriction élève » qui empêche l'accès au registre, à l'invite de commande, au panneau de configuration, et la modification du bureau, pour le groupe global Élèves.
On verrouille l'environnement des élèves (registre, invite de commande, panneau de configuration, bureau) pour limiter les manipulations et réduire la surface d'attaque sur les postes.

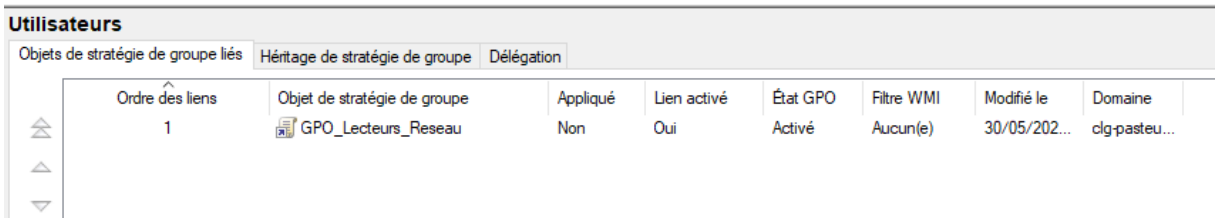



Système
Empêche l'accès aux outils de modifications du Registre
Modifier le paramètre de stratégie
Configuration requise :
Au minimum Windows 2000
Description :
Désactive l'éditeur de Registre Windows Regedit.exe.
Si vous activez ce paramètre de stratégie et que l'utilisateur essaie de démarrer Regedit.exe, un message s'affiche pour expliquer qu'un paramètre de stratégie bloque l'action.
Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les utilisateurs peuvent exécuter Regedit.exe normalement.
Pour empêcher les utilisateurs d'utiliser d'autres outils d'administration, utilisez le paramètre de stratégie « Exécuter uniquement les applications Windows spécifiées ».
Paramètre
État
Commentaire
Accès au stockage amovible
Affichage
Gestion de l'alimentation
Gestion de la communication Internet
Installation de pilotes
Options Ctrl+Alt+Suppr
Options d'atténuation
Ouverture de session
Profils utilisateur
Redirection de dossiers
Scripts
Services Paramètres régionaux
Stratégie de groupe
Télécharger les composants manquants Non configuré Non
Interprétation du siècle pour l'an 2000 Non configuré Non
Restreindre l'exécution de ces programmes à partir de l'aide Non configuré Non
Ne pas afficher l'écran de démarrage Mise en route à l'ouver... Non configuré Non
Interface utilisateur personnalisée Non configuré Non
Désactiver l'accès à l'invite de commandes Activé Non
Empêche l'accès aux outils de modifications du Registre Activé Non
Ne pas exécuter les applications Windows spécifiées Non configuré Non
Exécuter uniquement les applications Windows spécifiées Non configuré Non
Mises à jour automatiques Windows Non configuré Non

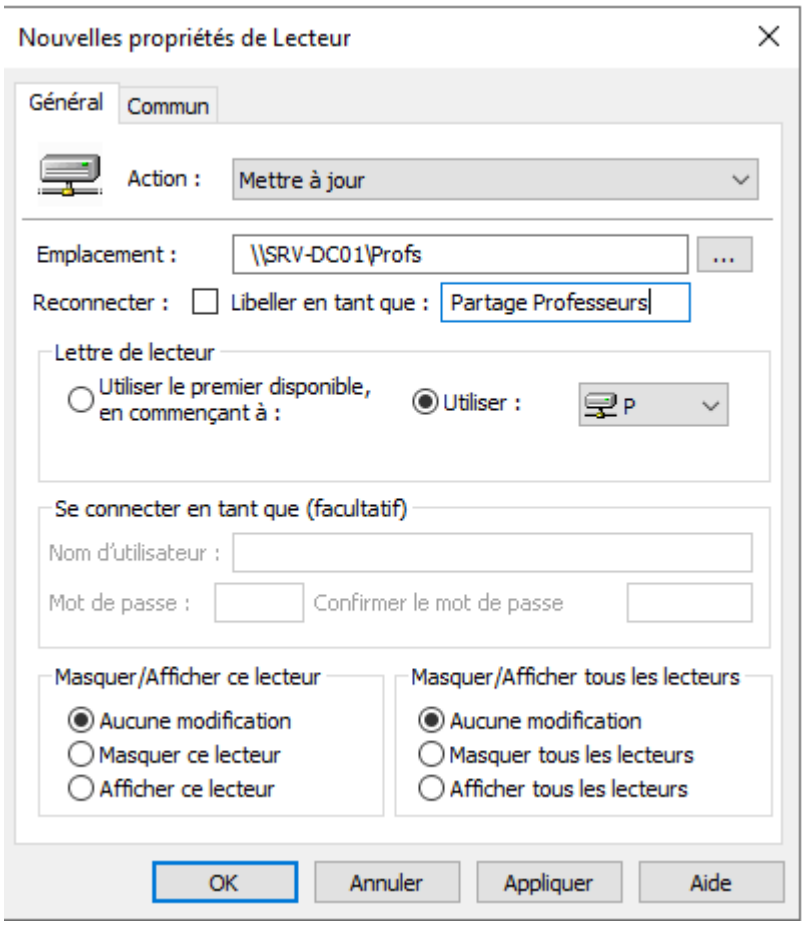

nir
Paramètre
État
Commentaire
Affichage
Ajouter ou supprimer des programmes
Imprimantes
Options régionales et linguistiques
Personnalisation
Programmes
Masquer les éléments du Panneau de configuration spécifiés Non configuré Non
Toujours afficher tous les éléments du Panneau de configur... Non configuré Non
Interdire l'accès au Panneau de configuration et à l'applicati... Activé Non
N'afficher que les éléments du Panneau de configuration sp... Non configuré Non
Visibilité de la page des paramètres Non configuré Non

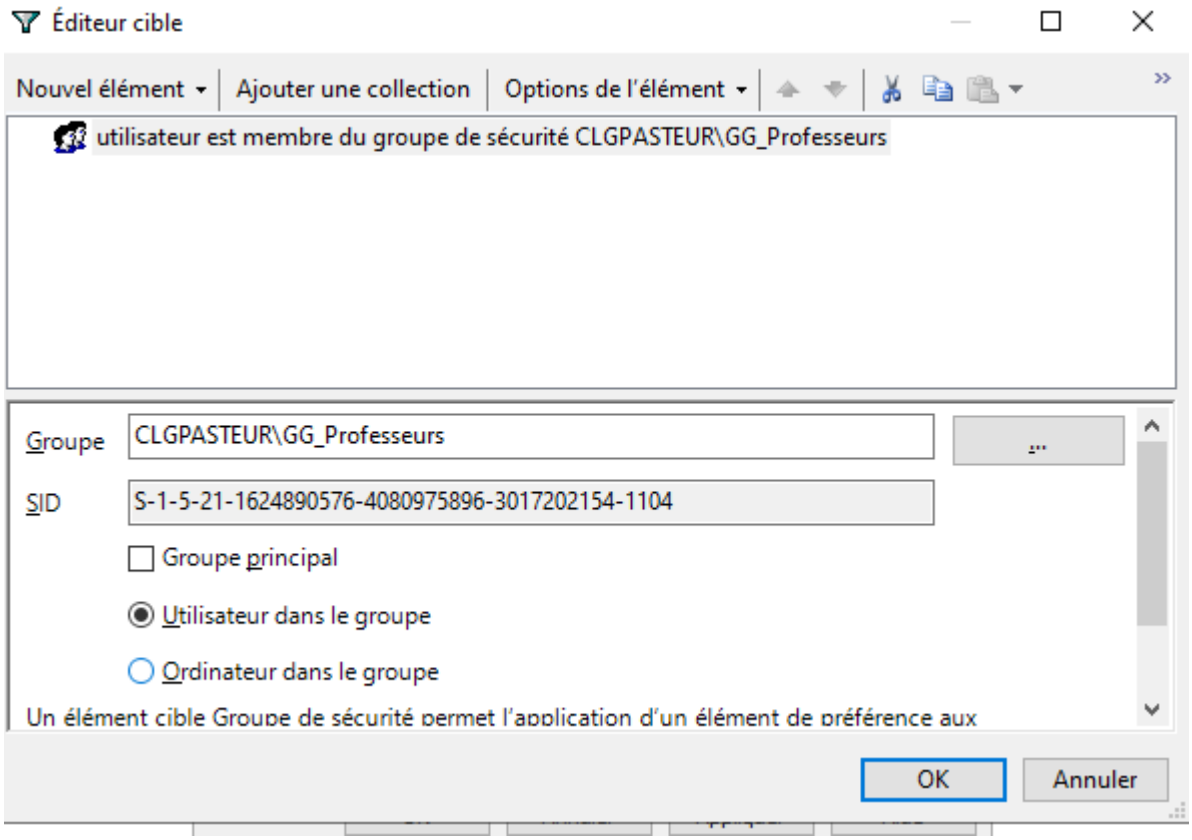

Bureau
Empêcher la modification d'éléments
Modifier le paramètre de stratégie
Configuration requise :
Windows Server 2003, Windows XP et Windows 2000 uniquement
Description :
Empêche les utilisateurs de modifier les propriétés des éléments de contenu Web sur leur Active Desktop.
Ce paramètre désactive le bouton Propriétés de l'onglet Web dans l'application Affichage du Panneau de configuration. Il supprime
Paramètre
État
Commentaire
Activer Active Desktop Non configuré Non
Désactiver Active Desktop Non configuré Non
Interdire les modifications Non configuré Non
Papier peint du Bureau Non configuré Non
Empêcher l'ajout d'éléments Non configuré Non
Empêcher la fermeture d'éléments Non configuré Non
Empêcher la suppression d'éléments Non configuré Non
Empêcher la modification d'éléments Activé Non
Désactiver tous les éléments Non configuré Non
Ajouter/supprimer des éléments Non configuré Non
N'autoriser que les papiers peints au format bmp Non configuré Non

Passons à la création d'une GPO « Lecteurs réseau » dans l'OU Utilisateurs : un lecteur personnel pour les élèves, un pour les professeurs, et un dernier commun aux membres de GG_Professeurs ou GG_Direction.
Les lecteurs réseau sont mappés automatiquement à l'ouverture de session selon le groupe : chaque profil retrouve son espace, sans intervention manuelle sur les postes.

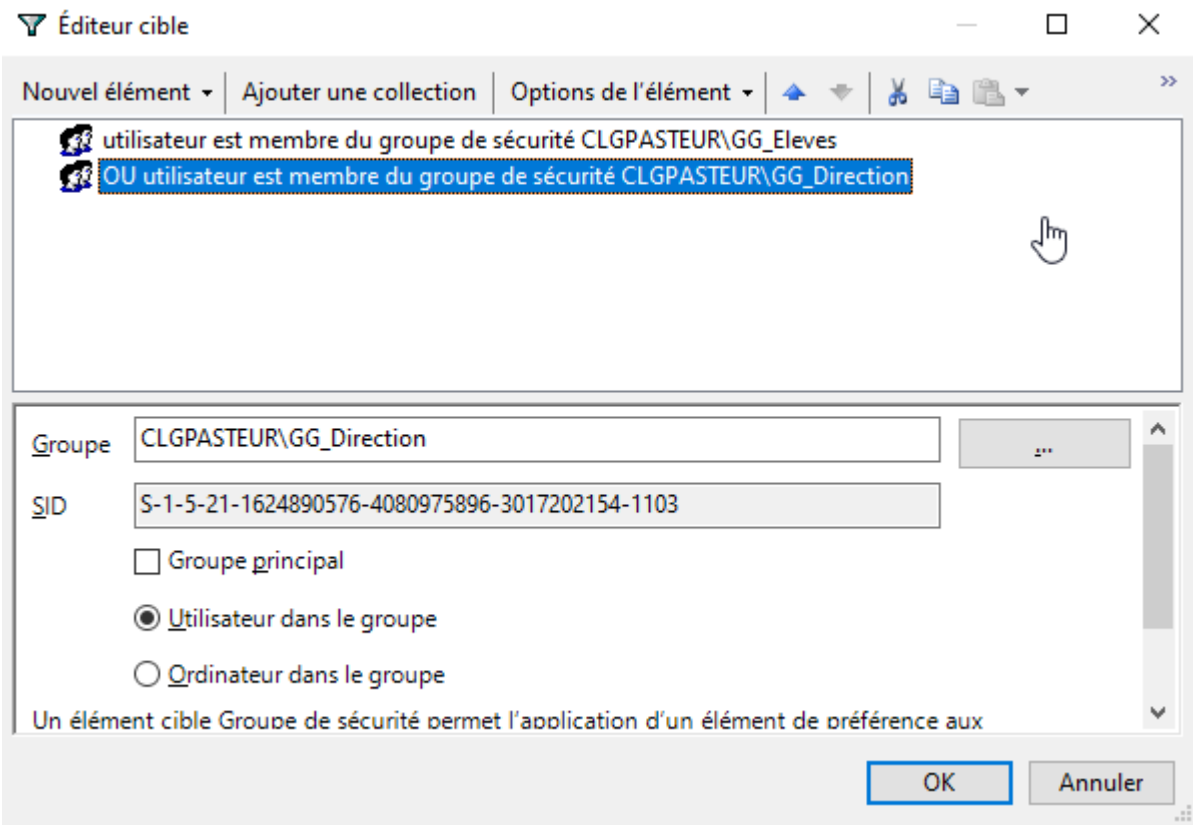


Configuration utilisateur → Préférences → Paramètres Windows → Mappages de lecteurs.





On fait de même pour le lecteur commun Direction ou Professeurs, en mettant l'opérateur à OU dans les options de l'élément.
Le ciblage par élément (opérateur OU sur l'appartenance aux groupes) conditionne le mappage à l'appartenance Direction ou Professeurs.



Test avec un client Windows 10 joint au domaine (mot de passe : Yukinala30 !)
Validation côté client : un poste Windows 10 rejoint le domaine doit récupérer l'authentification AD, les GPO et les lecteurs mappés.

Changement du DNS puis jointure au domaine
Le client doit utiliser le DNS du domaine (le serveur AD) pour localiser le contrôleur, sinon la jointure échoue.

```
PS C:\Users\ssss> Set-DnsClientServerAddress -InterfaceAlias "Ethernet0" -Se
rverAddresses 192.168.1.101
```

Rename-Computer -NewName "PC-SALLE-01" -Restart

Jointure au domaine Pasteur

```
PS C:\Users\ssss> Add-Computer -DomainName "clg-pasteur.lan" `
>>     -OUPath "OU=PC-Salles,OU=Ordinateurs,OU=College,DC=clg-pasteur,DC=lan
" `
>>     -Credential (Get-Credential) `
>>     -Restart
```