Mise en place de GPO

Une **GPO** (*Group Policy Object*) est une règle Windows utilisée pour configurer et contrôler les paramètres des utilisateurs et des ordinateurs. Dans ce chapitre, nous allons voir comment configuré dans un premier temps l'environnement pour les GPO puis dans un second temps crée des exemple de GPO avec un logiciel en .MSI et en .EXE, puis le déploiement de règle et pour finir la mise en place automatique de partage réseaux.

Sommaire

Sommaire :

c)Création de la GPO

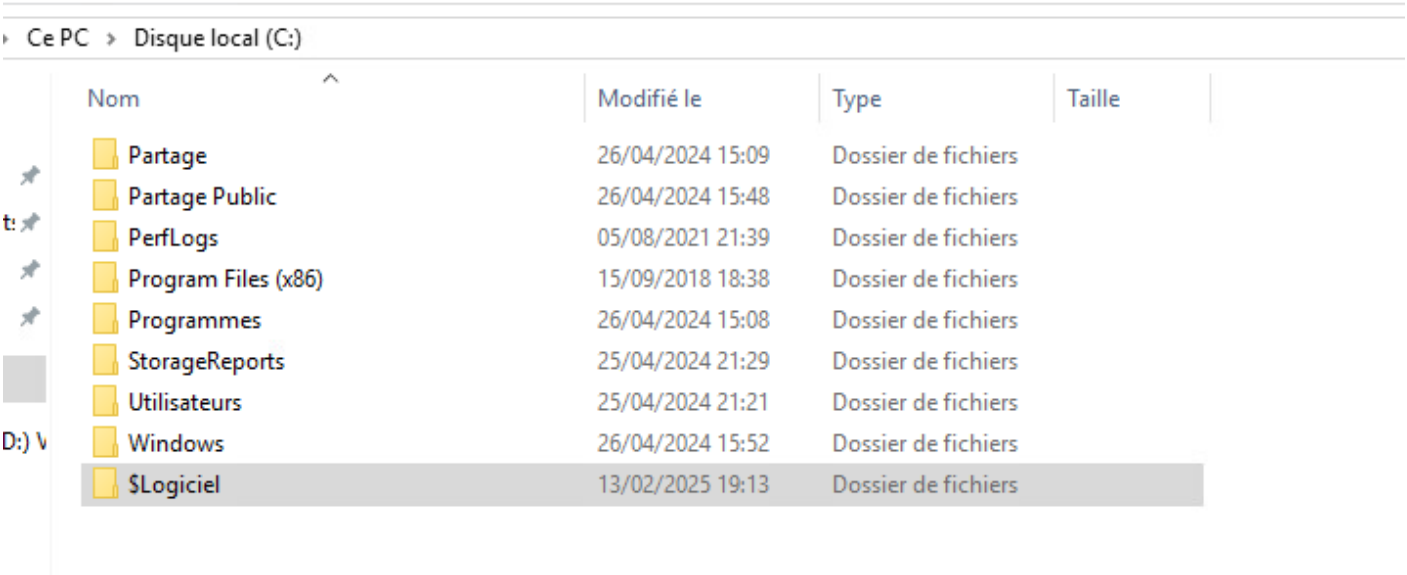
d)Test

1 - Configuration avant GPO

a) Création d’un dossier

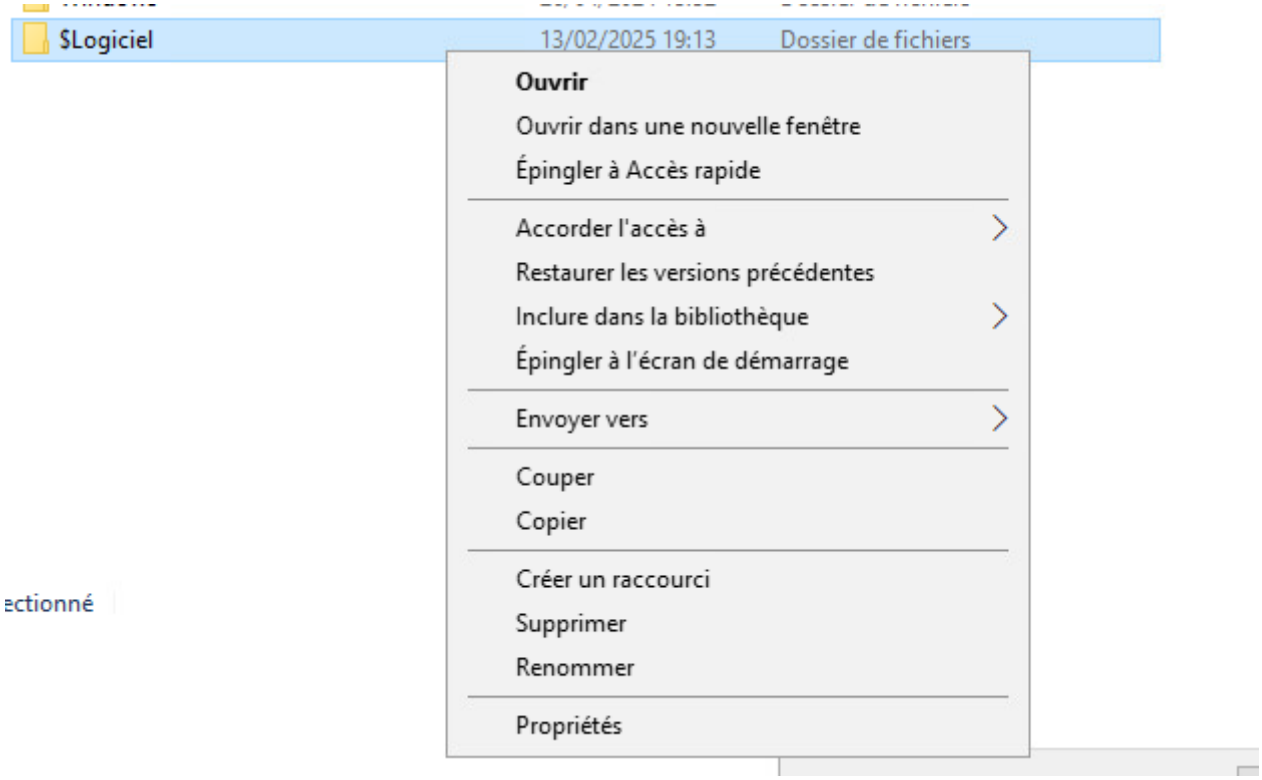
Dans un premier temps, nous allons créer un dossier qui va contenir des logiciels pour leur déploiement. Vous pouvez faire le dossier n'importe où, mais il est recommandé de le faire à la racine d'un volume :

Ici je le fais à la racine de C: en le nommant $Logiciel (le $ permet de rendre invisible le dossier pour les utilisateur).

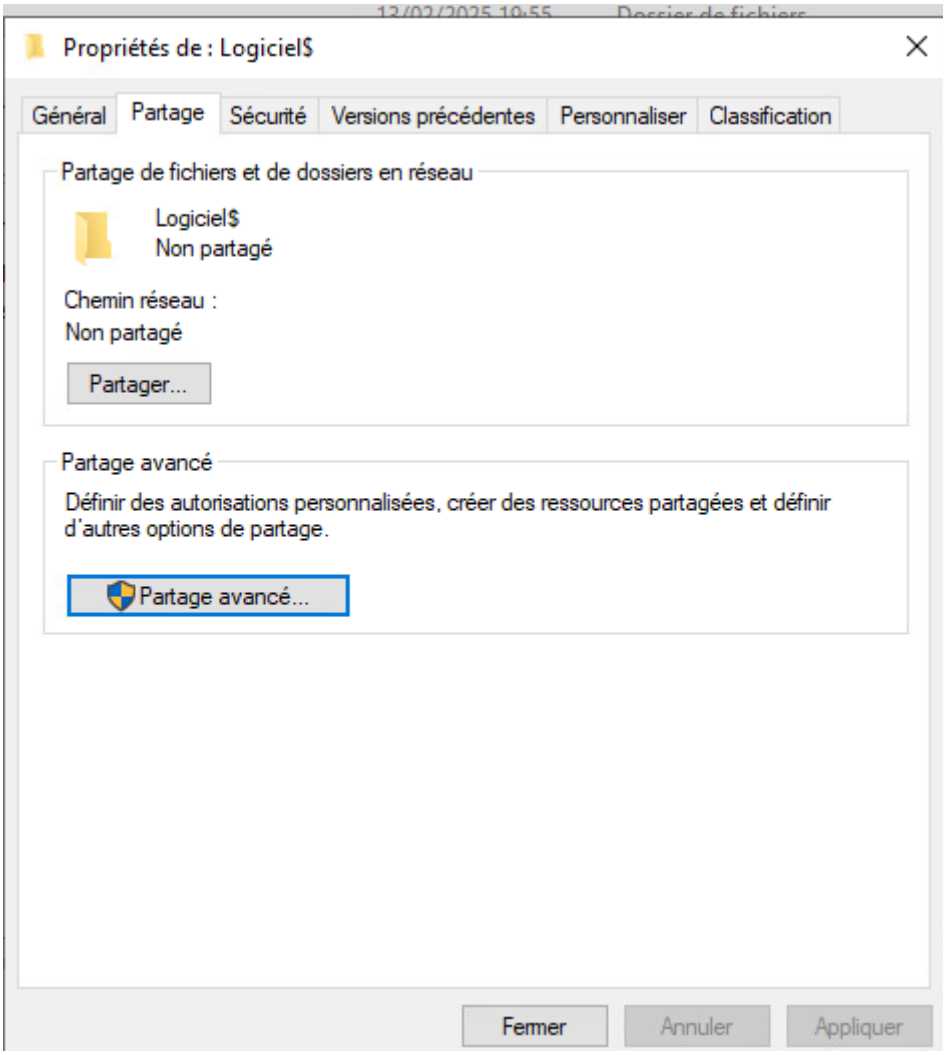


b) Partages

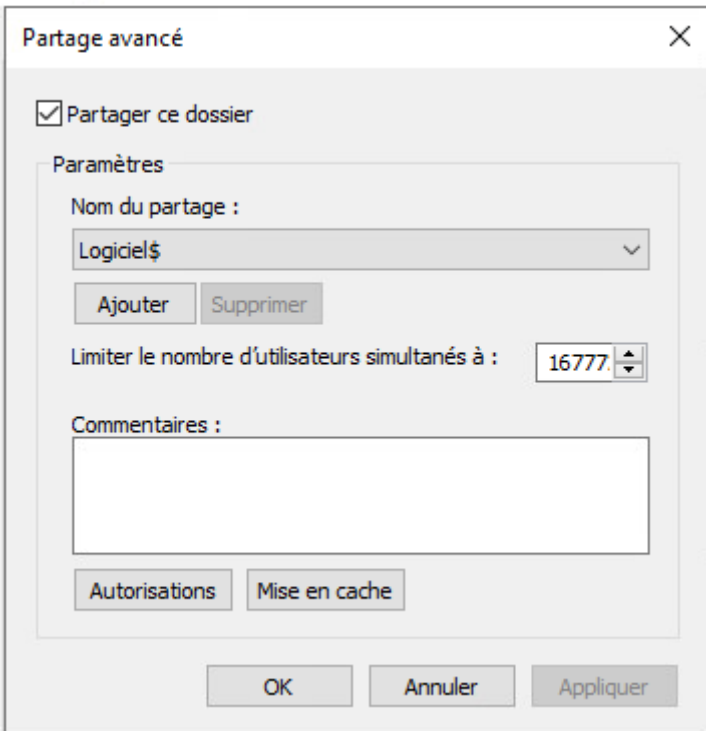
Puis je vais faire un clic droit dessus puis propriété pour pouvoir mettre en place le partage et les droits :



Nous allons aller dans l'onglet "Partage", puis cliquer sur "Partage avancé..." :



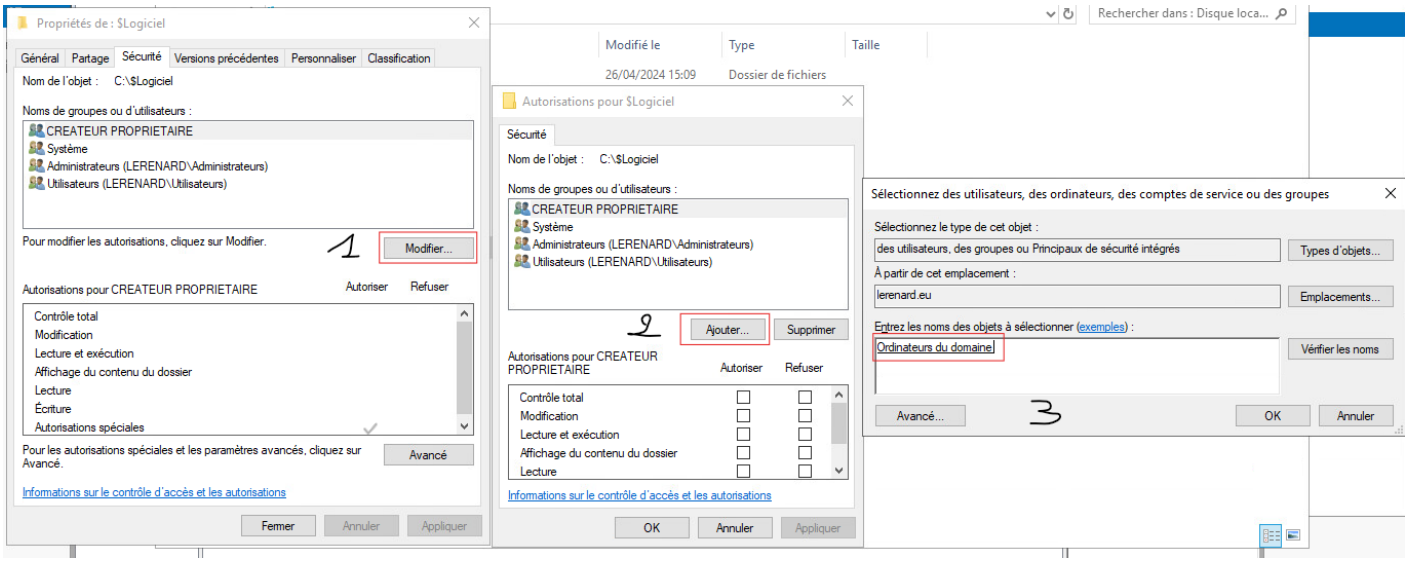
Nous n'allons rien toucher, puis faire "Appliquer", puis refermer :



Si c'est bien fait, vous allez voir "\\nom-de-votre-serveur\lepartage" et cela permettra de faire le déploiement d'application par la suite :

c) Mise en place des droits

On va aller dans "Sécurité", puis faire "Modifier". Une fois la fenêtre ouverte, on va faire "Ajouter...", on va rajouter "Ordinateurs du domaine" puis "OK" :



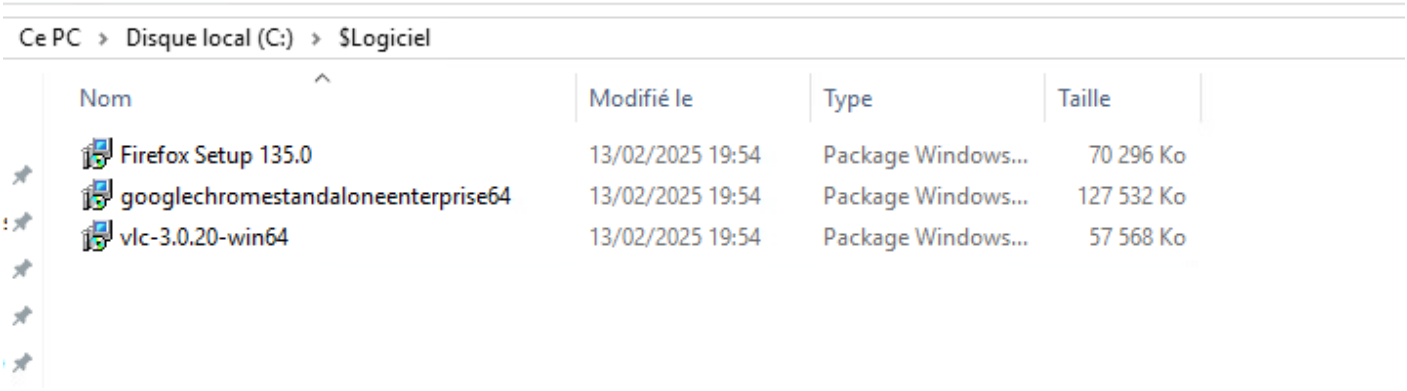
Une fois cela fait, on ne modifie rien et on fait "Appliquer", puis on fait "OK" et "Fermer".

2 - GPO avec .MSI

a) Mise en place des .MSI dans le dossier

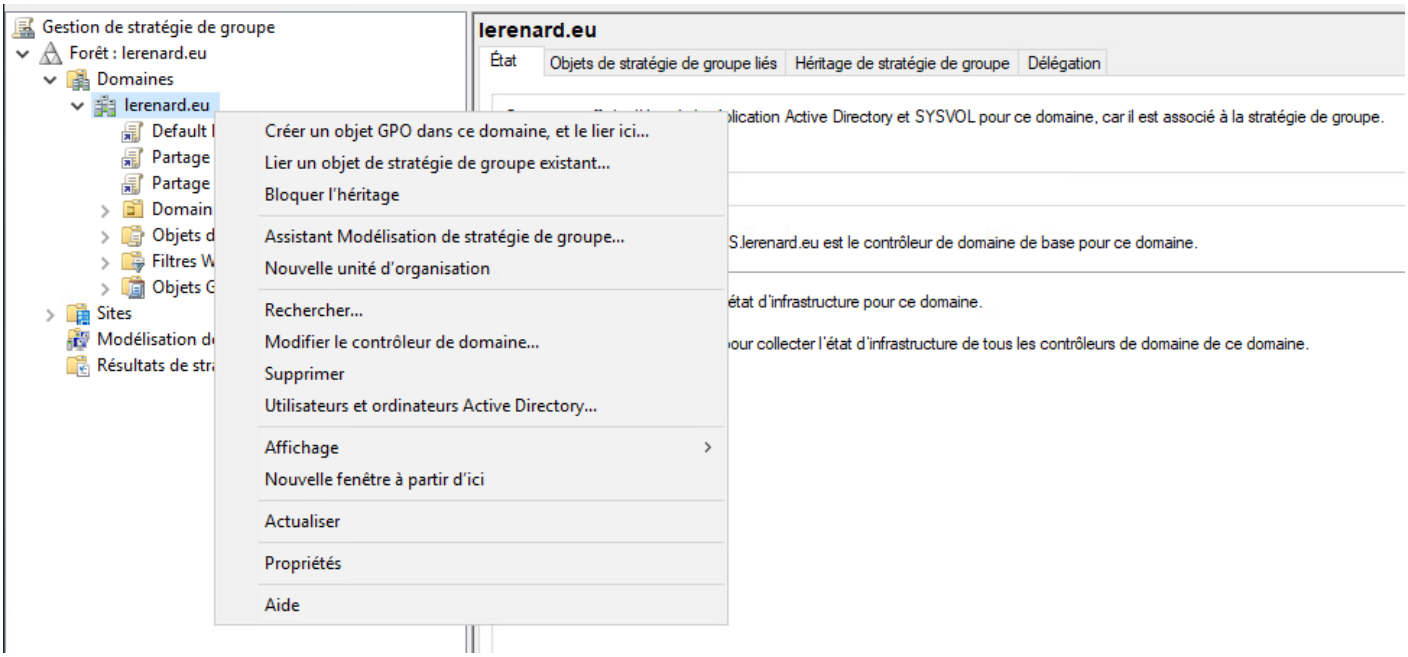
Nous allons dans cette partie téléchargé des .MSI.MSI. Les.MSI sont très pratiques car ils sont pré-configurés avec des commandes qui aident à automatiser l'installation du logiciel.

Ici je vais prendre Firefox, Chrome et VLC (pour les chercher, je cherche sur google "nom du logiciel". msi)" :

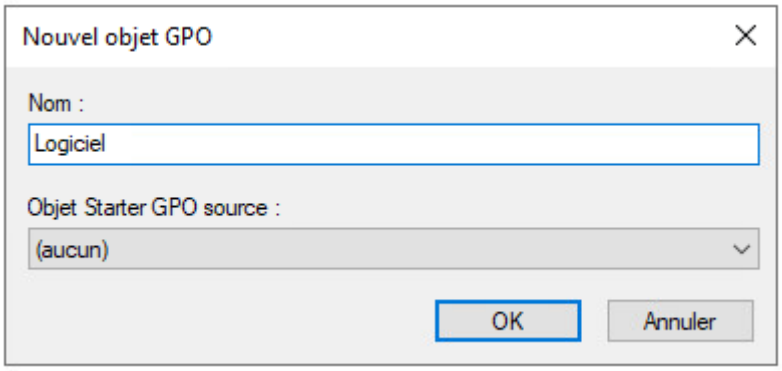


b) Création de la GPO :

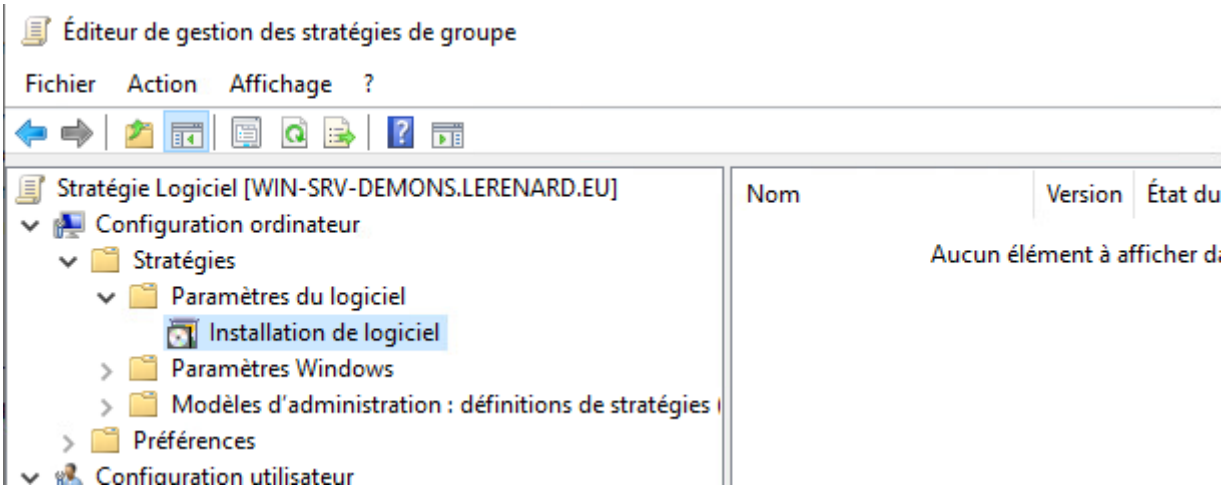
Pour créer la GPO, nous allons lancer "Gestion de stratégie de groupe", puis déplier chaque rubrique jusqu'à trouver notre domaine. Une fois le domaine trouvé, faites clic droit dessus et "Créer un objet GPO dans ce domaine, et le lier ici..." :



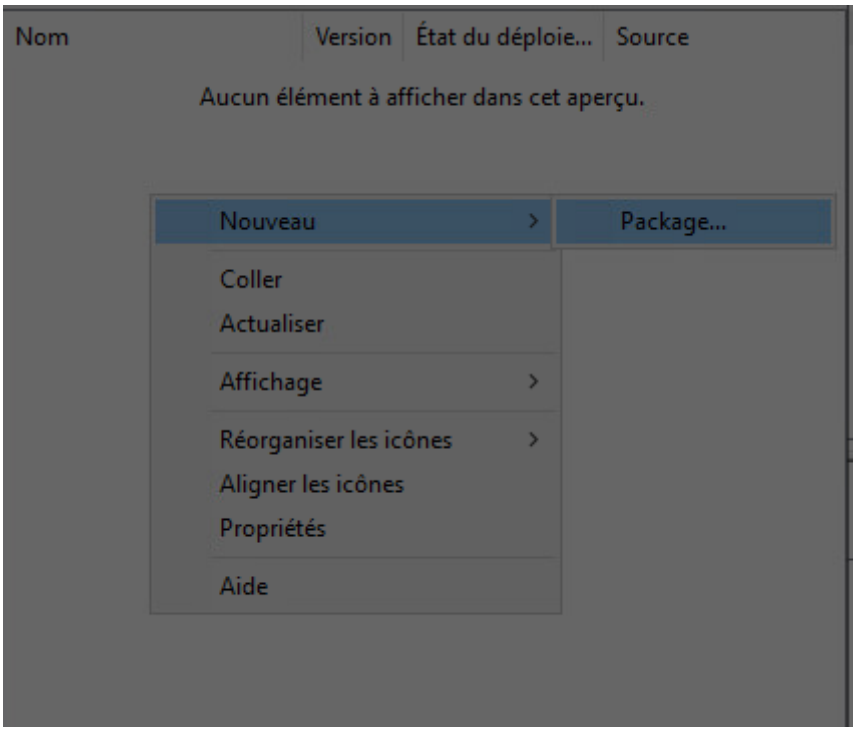
Vous lui donnez le nom que vous voulez, dans mon cas je la nomme logiciels pour l'exemple mais je vous conseille de faire un objet GPO pour chaque logiciel surtout en production :



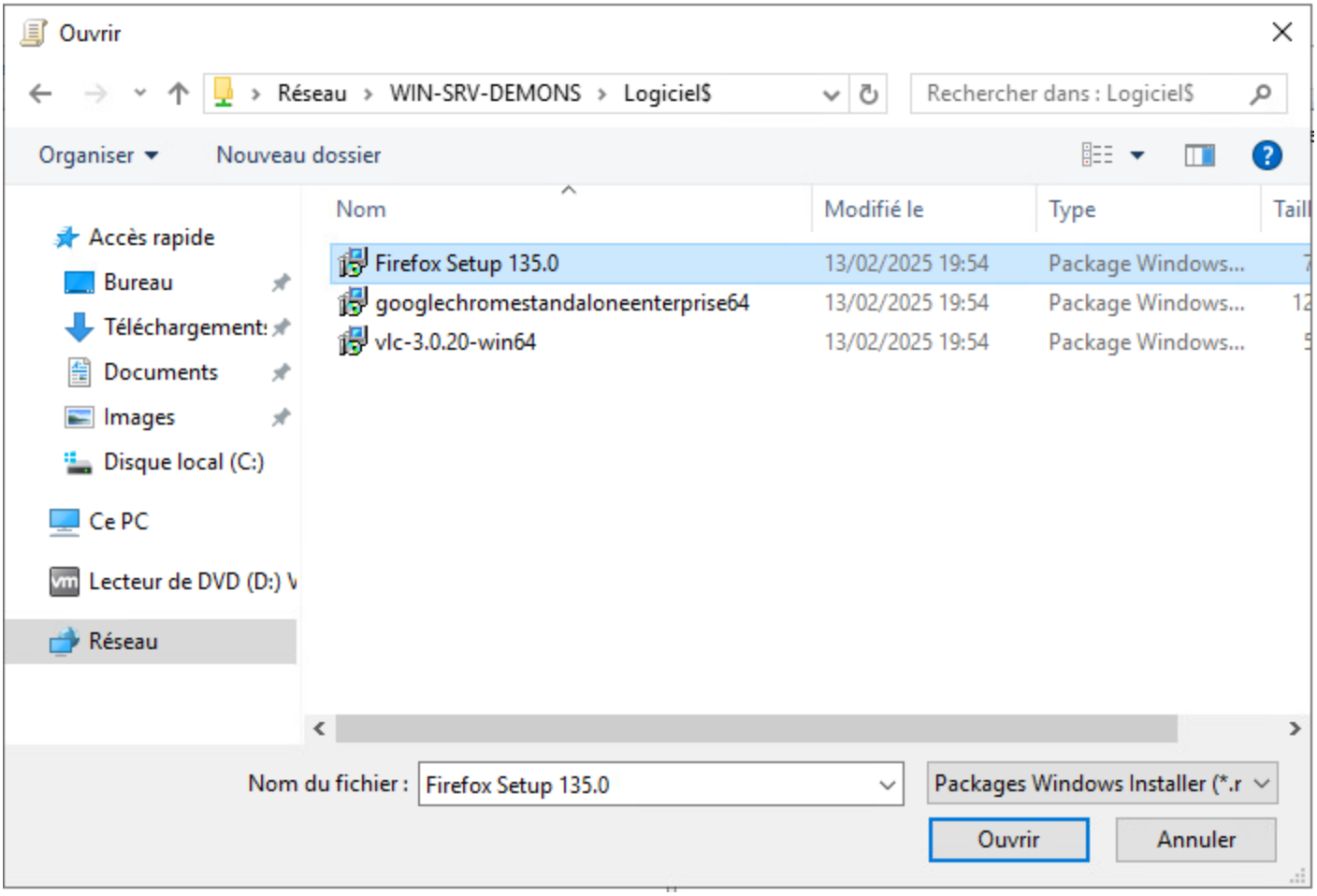
Une fois l'objet créé, nous allons faire un clic droit dessus puis "Modifier".



Une fois dans "installations de logiciel", nous allons faire clic droit soit sur "installation de logiciel", soit dans la zone "Aucun élément à afficher dans cet aperçu", puis "Nouveau>Package":

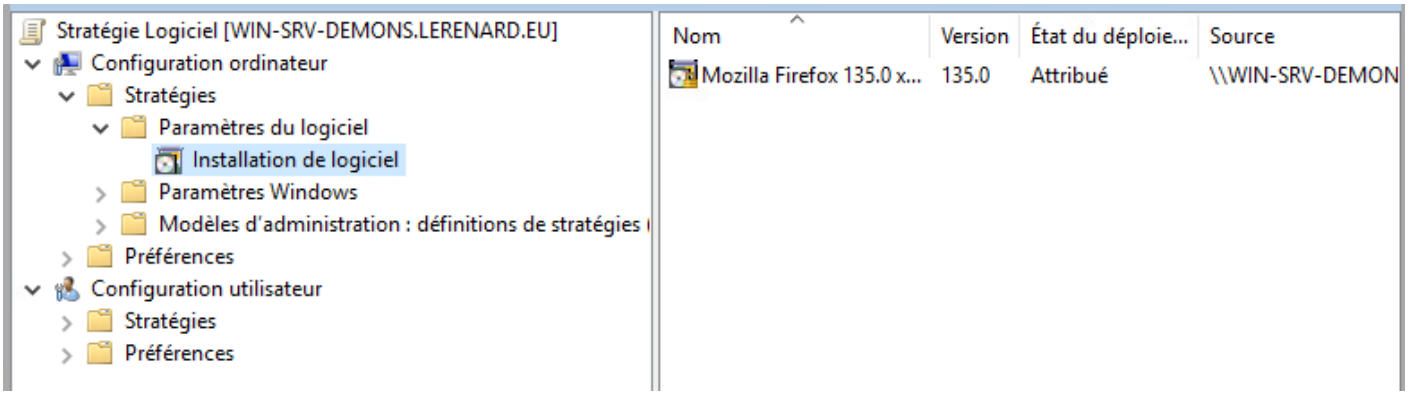


Cela va donc ouvrir une fenêtre "Ouvrir". Dans cette fenêtre, dans la barre du haut centrale, vous mettez le chemin réseau du dossier, dans mon cas "\\WIN-SRV-DEMONS\Logiciel$", puis sélectionnez un logiciel :



Vous laissez "attribué" puis faites "OK" :

On devrait voir cela :



Puis on répète l'opération pour les deux autres logiciels.

c) Test

Pour le test, nous allons aller sur une machine cliente, reliée au domaine pour faire dans l'invite de commande "gpupdate /force" pour forcer la recherche de gpo. Puis une fois redémarré, nous allons faire "gpresult /r" pour voir si la stratégie est visible :

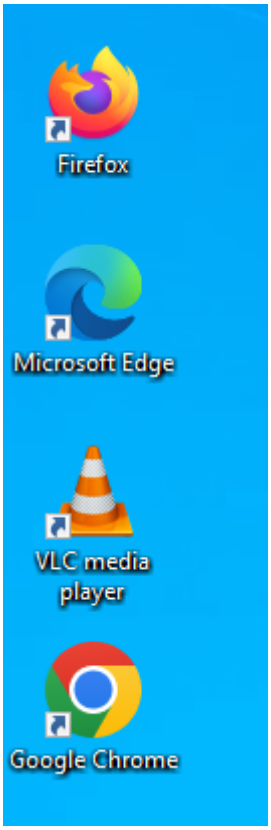
gpupdate /force :

```
C:\Users\Administrateur.LERENARD>gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.

Les avertissements suivants ont été rencontrés lors du traitement de la stratégie de l'ordinateur :

L'extension côté client de la stratégie de groupe Software Installation n'a pas pu appliquer un ou plusieurs paramètres
car les modifications doivent être traitées avant le démarrage système ou la connexion utilisateur. Le système attendra
la fin complète du traitement de la stratégie de groupe avant de procéder au prochain démarrage ou à la prochaine connex
ion pour cet utilisateur. Ceci peut entraîner un ralentissement du démarrage et des performances de démarrage du système
.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

Pour plus de détails, ouvrez le journal des événements ou exécutez GPRESULT /H GPReport.html depuis la ligne de commande
 pour accéder aux résultats de la stratégie de groupe.

Certaines stratégies d'ordinateurs activées peuvent uniquement être
exécutées pendant le démarrage.

OK pour redémarrer ? (O/N)o
Redémarrage de l'ordinateur...
```

Puis "gpresult /r"

```
Paramètre de l'ordinateur
-------------------------
    CN=WINDOWS-10-LOCA,CN=Computers,DC=lerenard,DC=eu
    Heure de la dernière application de la stratégie de groupe : 13/02/2025 à 21:01:41
    Stratégie de groupe appliquée depuis :      WIN-SRV-DEMONS.lerenard.eu
    Seuil de liaison lente dans la stratégie de groupe :   500 kbps
    Nom du domaine..................... : LERENARD
    Type de domaine.................... : Windows 2008 ou supérieur

    Objets Stratégie de groupe appliqués
    ------------------------------------
        Default Domain Policy
        Logiciel
```

Puis au bout d'un moment cela va redescendre tout seul :



3- Déploiement de .EXE

a)Mise en place des .exe dans le dossier

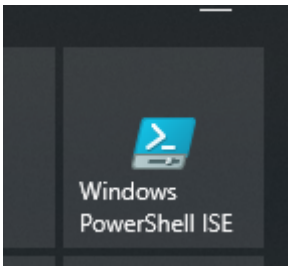
Pour cette partie, j'ai donc utilisé 7zip comme exemple, mais attention, ce n'est pas tous les exécutables qui peuvent fonctionner avec cette méthode. Par exemple, CrystalDiskInfo, qui permet de voir la vie des disques durs, ne peut être installé de cette façon.

J'ai donc téléchargé 7zip sur son site officiel, puis copier dans le dossier :

Nom	Modifié le	Type	Taille
7z2409-x64.exe	17/02/2025 00:39	Application	1 599 Ko
Firefox Setup 135.0.msi	16/02/2025 22:45	Package Windows...	70 296 Ko
googlechromestandaloneenterprise64.msi	16/02/2025 23:50	Package Windows...	127 532 Ko
vlc-3.0.18-win64.msi	16/02/2025 22:46	Package Windows...	57 730 Ko

b)Création du script

Après la copie de 7zip, nous allons donc ouvrir "Windows PowerShell ISE" :



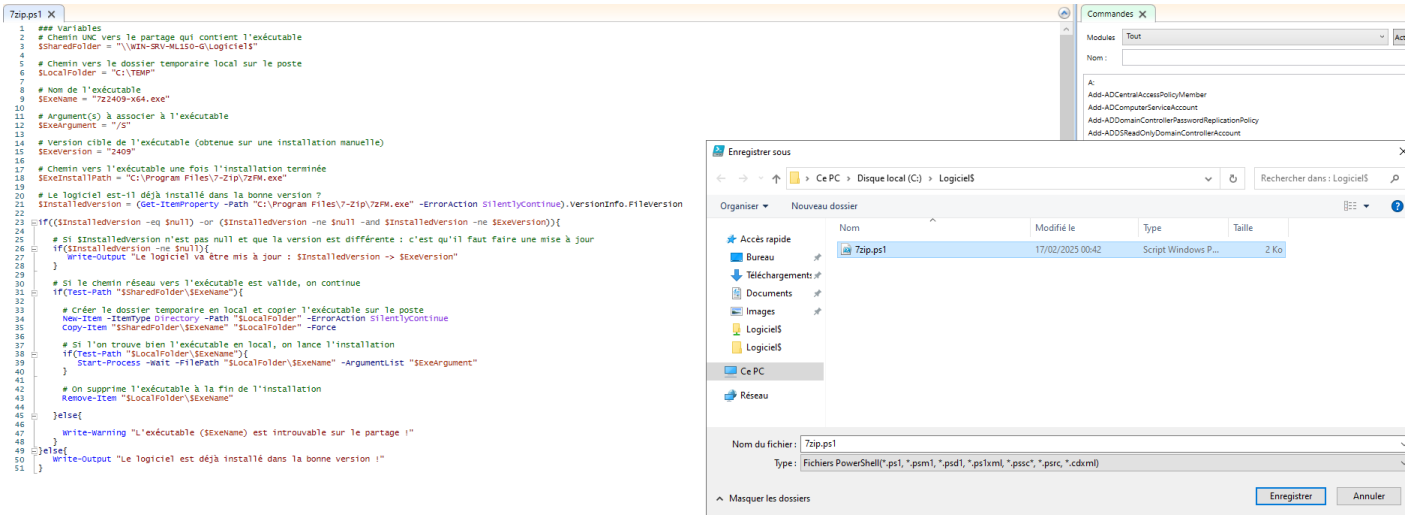
Une fois ouvert, nous allons donc y coller ça (bien sûr si vous installez un autre logiciel, modifiez cela pour le vôtre) :

```
### Variables
# Chemin vers le partage qui contient l'exécutable
$SharedFolder = "\\WIN-SRV-ML150-G\Logiciel$"

# Chemin vers le dossier temporaire local sur le poste
$LocalFolder = "C:\TEMP"

# Nom de l'exécutable
$ExeName = "7z2409-x64.exe"

# Argument(s) à associer à l'exécutable
$ExeArgument = "/S" # pour ordonné une installation silencieuse
```

```
# Version cible de l'exécutable (obtenue sur une installation manuelle)
$ExeVersion = "24.09"

# Chemin vers l'exécutable une fois l'installation terminée
$ExeInstallPath = "C:\Program Files\7-Zip\7zFM.exe"

# Le logiciel est-il déjà installé dans la bonne version ?
$InstalledVersion = (Get-ItemProperty -Path "C:\Program Files\7-Zip\7zFM.exe" -ErrorAction
SilentlyContinue).VersionInfo.FileVersion

if(($InstalledVersion -eq $null) -or ($InstalledVersion -ne $null -and $InstalledVersion -ne
$ExeVersion)){

   # Si $InstalledVersion n'est pas null et que la version est différente : c'est qu'il faut
faire une mise à jour
   if($InstalledVersion -ne $null){
      Write-Output "Le logiciel va être mis à jour : $InstalledVersion -> $ExeVersion"
   }

   # Si le chemin réseau vers l'exécutable est valide, on continue
   if(Test-Path "$SharedFolder\$ExeName"){

     # Créer le dossier temporaire en local et copier l'exécutable sur le poste
     New-Item -ItemType Directory -Path "$LocalFolder" -ErrorAction SilentlyContinue
     Copy-Item "$SharedFolder\$ExeName" "$LocalFolder" -Force

     # Si l'on trouve bien l'exécutable en local, on lance l'installation
     if(Test-Path "$LocalFolder\$ExeName"){
        Start-Process -Wait -FilePath "$LocalFolder\$ExeName" -ArgumentList "$ExeArgument"
     }

     # On supprime l'exécutable à la fin de l'installation
     Remove-Item "$LocalFolder\$ExeName"

   }else{

     Write-Warning "L'exécutable ($ExeName) est introuvable sur le partage !"
   }
}else{
```

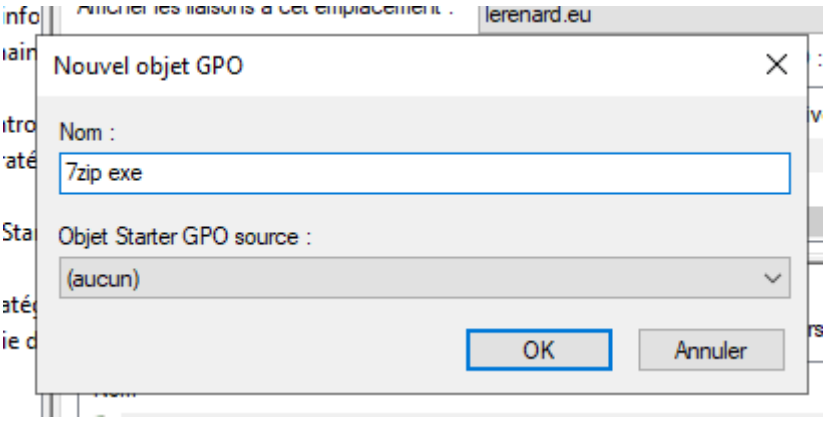
```
    Write-Output "Le logiciel est déjà installé dans la bonne version !"
}
```

Une fois cela copié, il faut l'enregistrer dans le dossier partagé, vous faites Ctrl+s ou Fichier > Enregistrer :

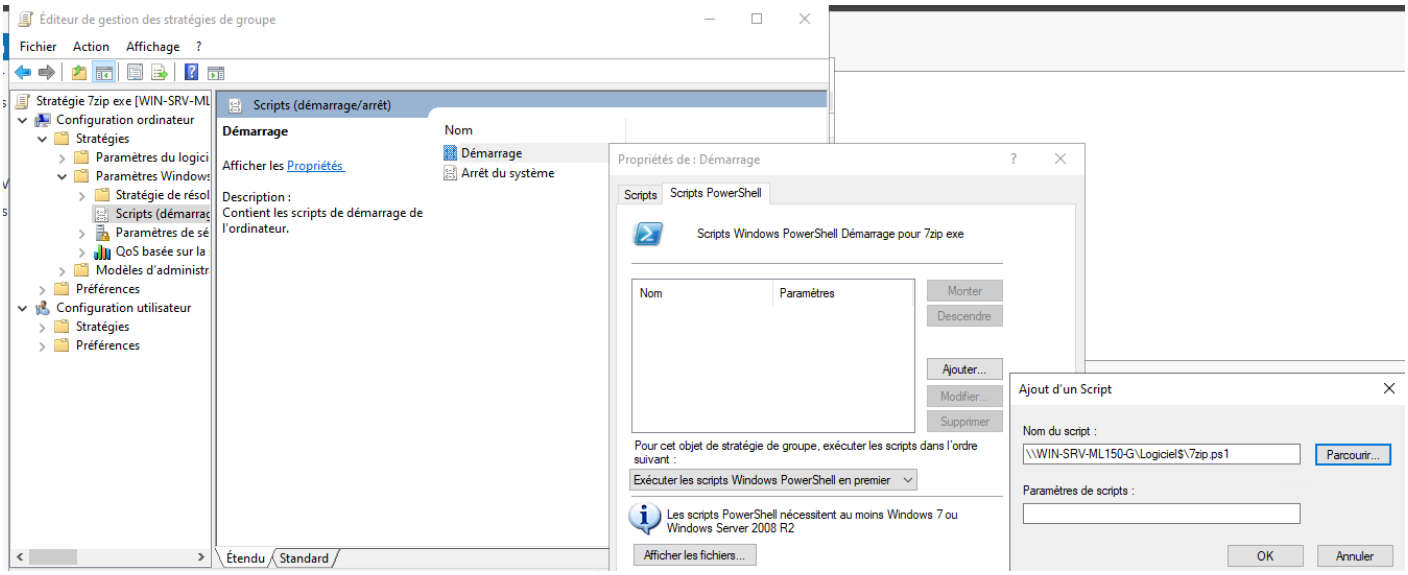


c)Création de la GPO

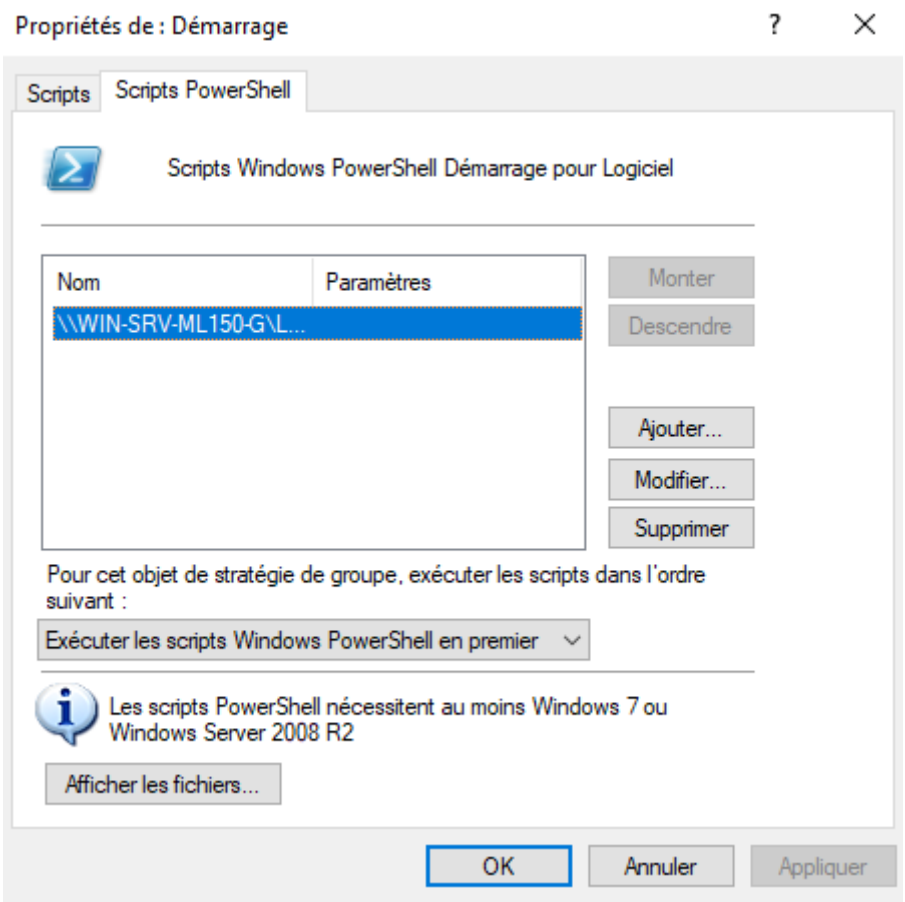
Comme pour les .MSI, nous allons crée une GPO que je vais noté celle fois si, 7zip.exe :



Puis nous allons aller dans "Configuration ordinateur > Paramètres Windows > Scripts (démarrage/arrêt) > Démarrage" et on double-clique sur "Démarrage". Une fois cela fait, on va dans l'onglet "Scripts PowerShell", on lui spécifie qu'il doit "Exécuter les scripts Windows PowerShell en premier" et on ajoute le script :



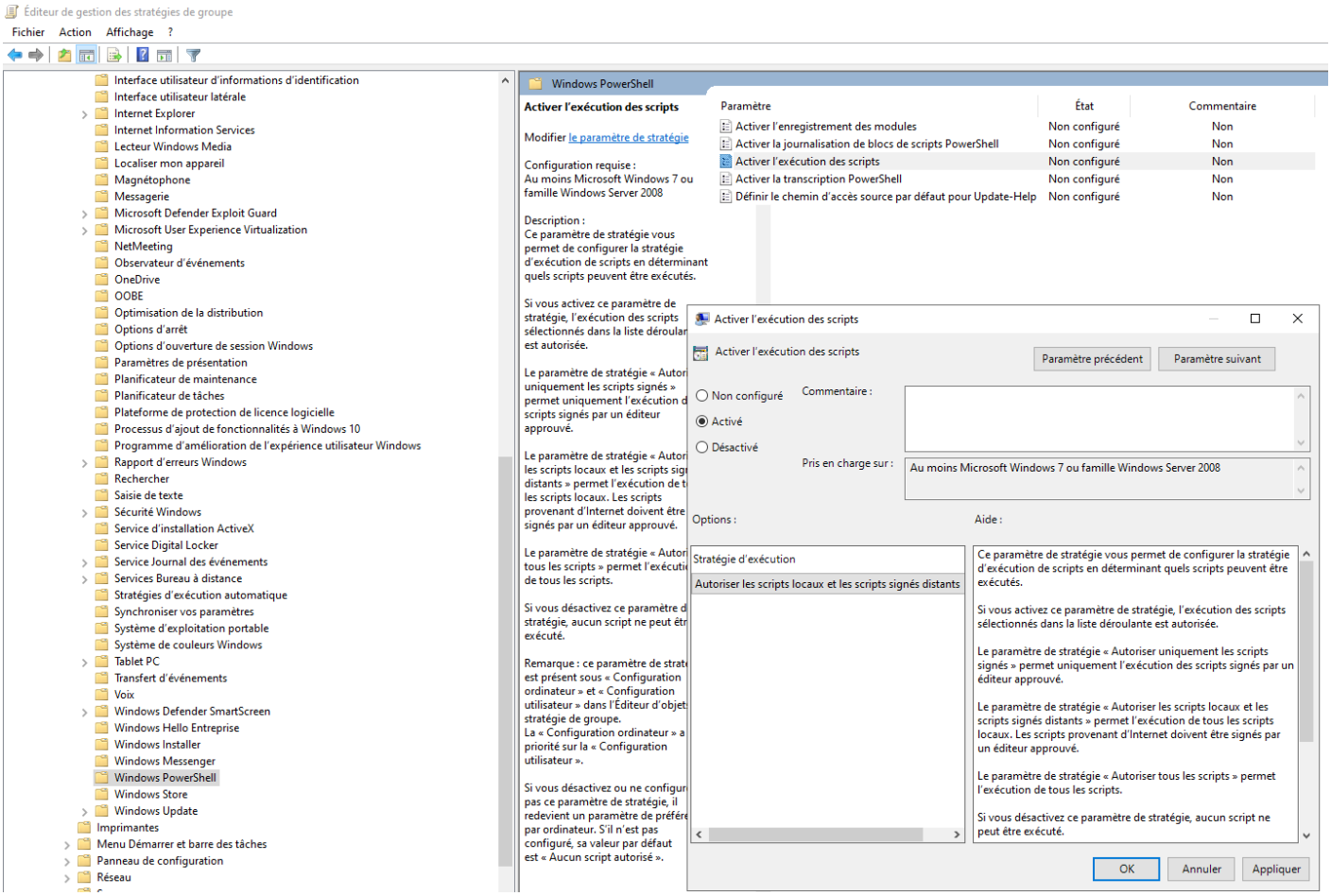
On fait donc "OK" puis "Appliqué :



Microsoft désactive par défaut les scripts pour des questions de sécurité, nous allons donc spécifier, dans la même GPO, l'activation de l'exécution des scripts :

```
Configuration ordinateur > Modèle d'administration > Composants Windows > Windows PowerShell
```

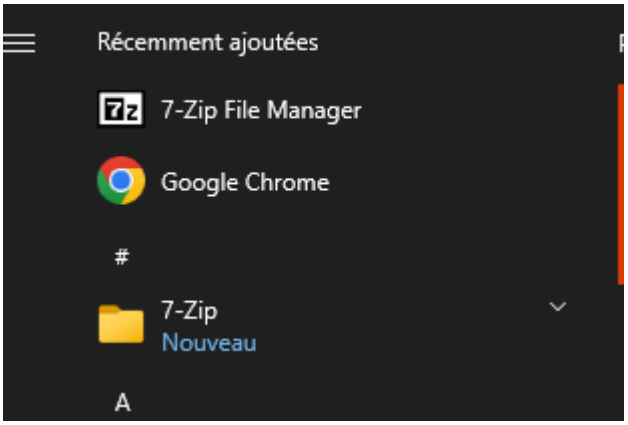
Une fois arrivés ici, nous allons ouvrir "Activer l'exécution des scripts" et cocher "Activé", puis faire "appliqué".



Nous n'avons plus rien à faire sur Windows Server et on passe maintenant à un client Windows 10.

D)Test

Ce test va être simple, on va juste redémarrer Windows et cela devrait redescendre tout seul. Dans mon cas, 7zip est redescendu tout seul assez rapidement :

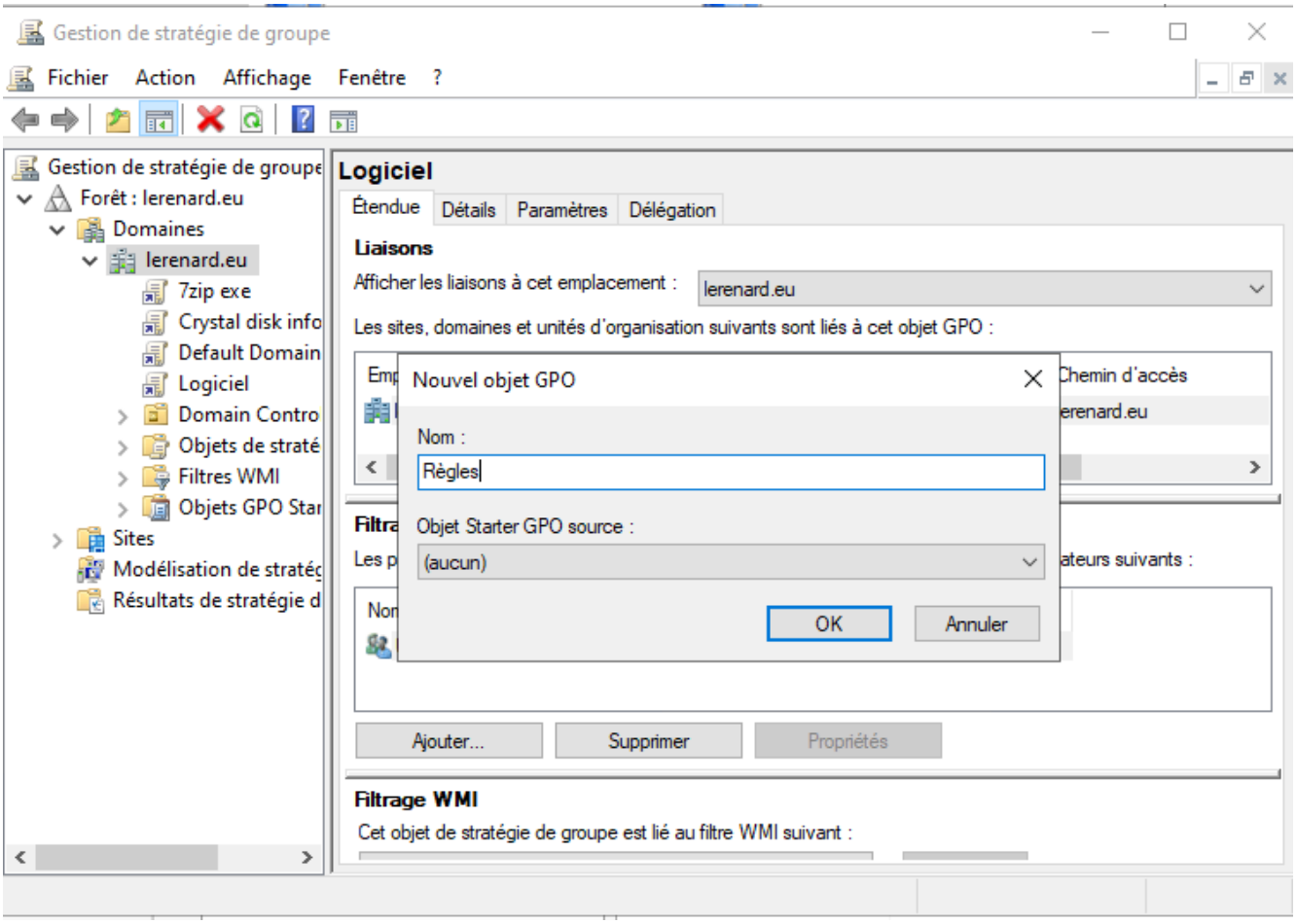


4- Déploiement de règle

a)Création de la GPO

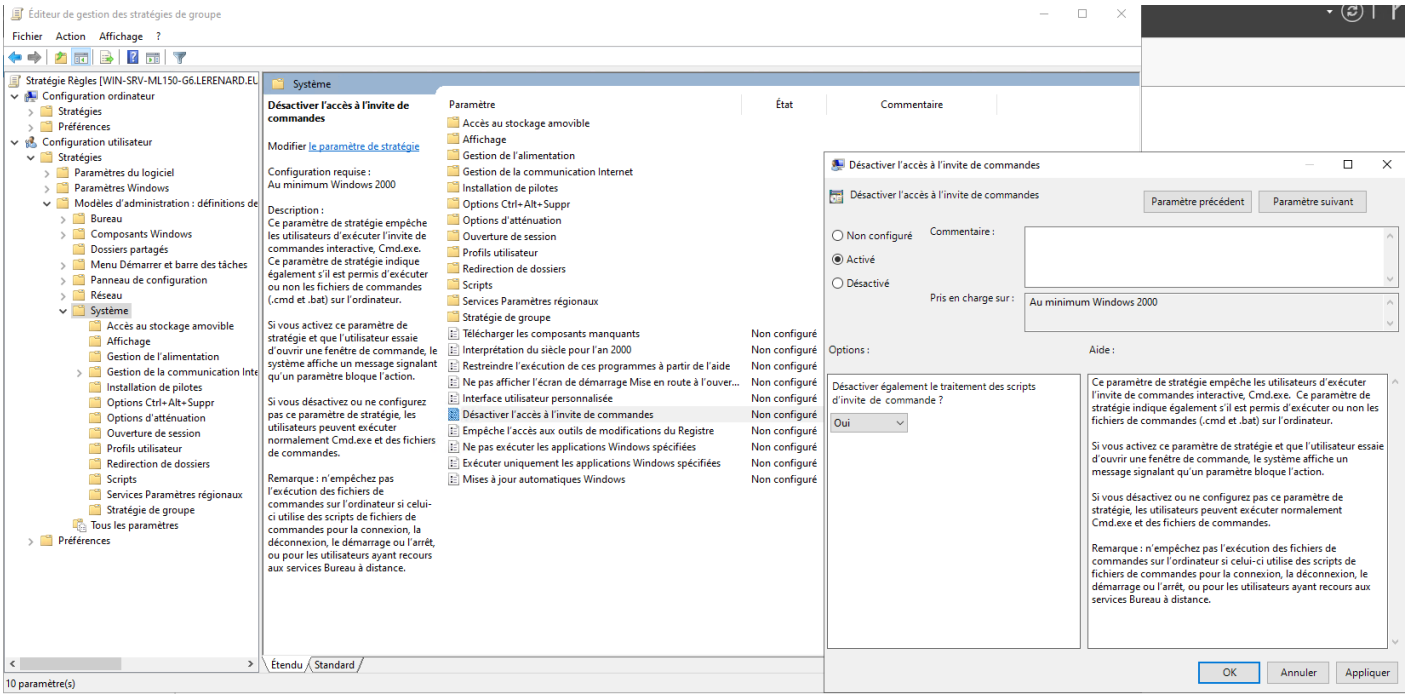
Dans cette partie, je vais bloquer l'accès à "l'invite de commandes" et changer l'image de fond du bureau.

Comme toute création de GPO, nous allons dans "Gestion de stratégie de groupe", puis crée une GPO que je nomme ici "Règles" (je vous conseille vivement en production de faire une GPO = une utilisation) :

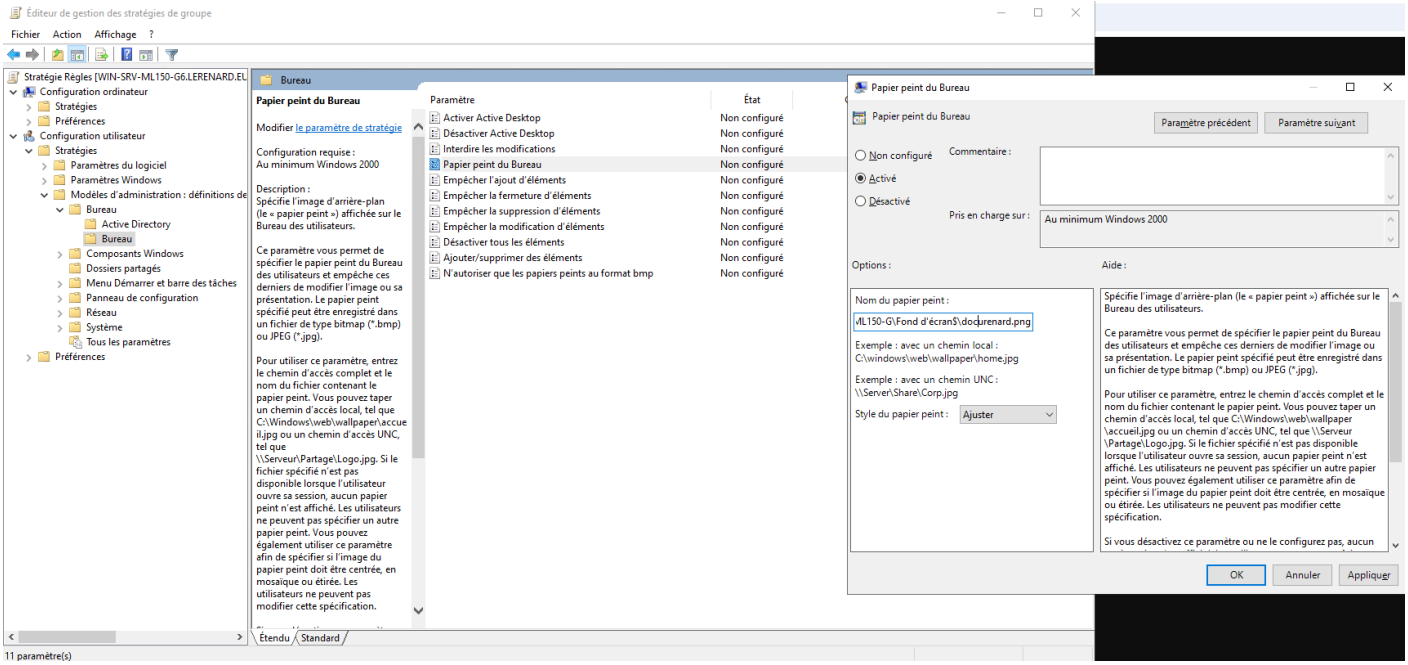


Puis nous allons rentrer dans la GPO. Pour changer des paramètres, c'est dans l'onglet "Configuration utilisateur".

Pour modifier la restriction de l'invite de commande, il faut aller dans "Configuration utilisateur>Stratégies>Modèles d'administrateur>Système", puis ouvrir "Désactiver l'accès à l'invite de commandes". Nous allons donc "Activer" cette règle puis faire "Appliquer" :



Maintenant, nous allons passer à la modification du fond d'écran. Nous allons donc aller dans "Configuration utilisateur>Stratégies>Modèles d'administration>Bureau>Bureau". Nous allons donc ouvrir "Papier peint du Bureau", puis indiquer un partage réseau qui contient l'image de votre choix. Dans mon cas j'ai créé un autre dossier avec les mêmes droits que le dossier Logiciel$ mais nommé Fond d'écran$.



Faites-appliquer puis nous allons passer au client,

b)Test

Une fois avoir redémarré ou démarré le client, nous pouvons constater que tout fonctionne :

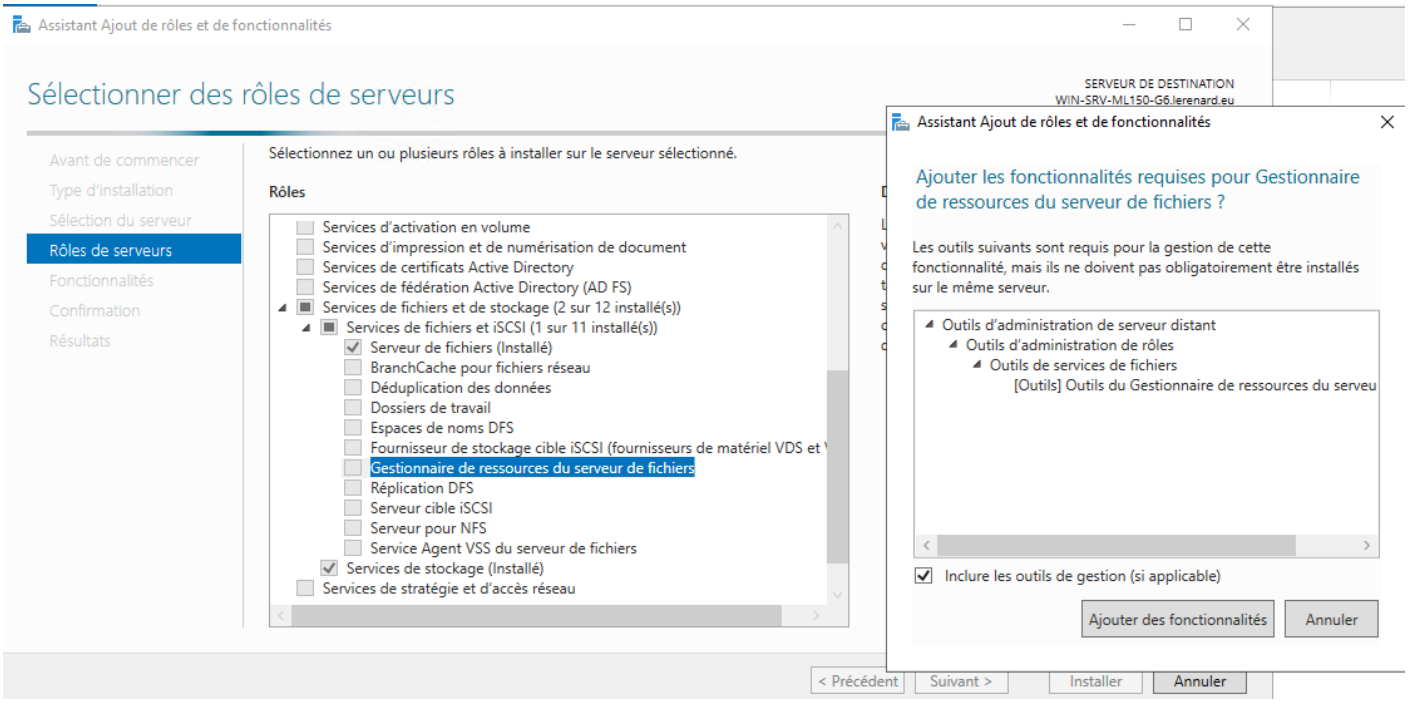

Corbeille
Firefox
Microsoft Edge
VLC media player
Google Chrome
DOCU
RENARD
Invite de commandes
Microsoft Windows [version 10.0.19045.2965]
(c) Microsoft Corporation. Tous droits réservés.
L'invite de commandes a été désactivée par votre administrateur.
Appuyez sur une touche pour continuer...

5- Déploiement de répertoire réseaux

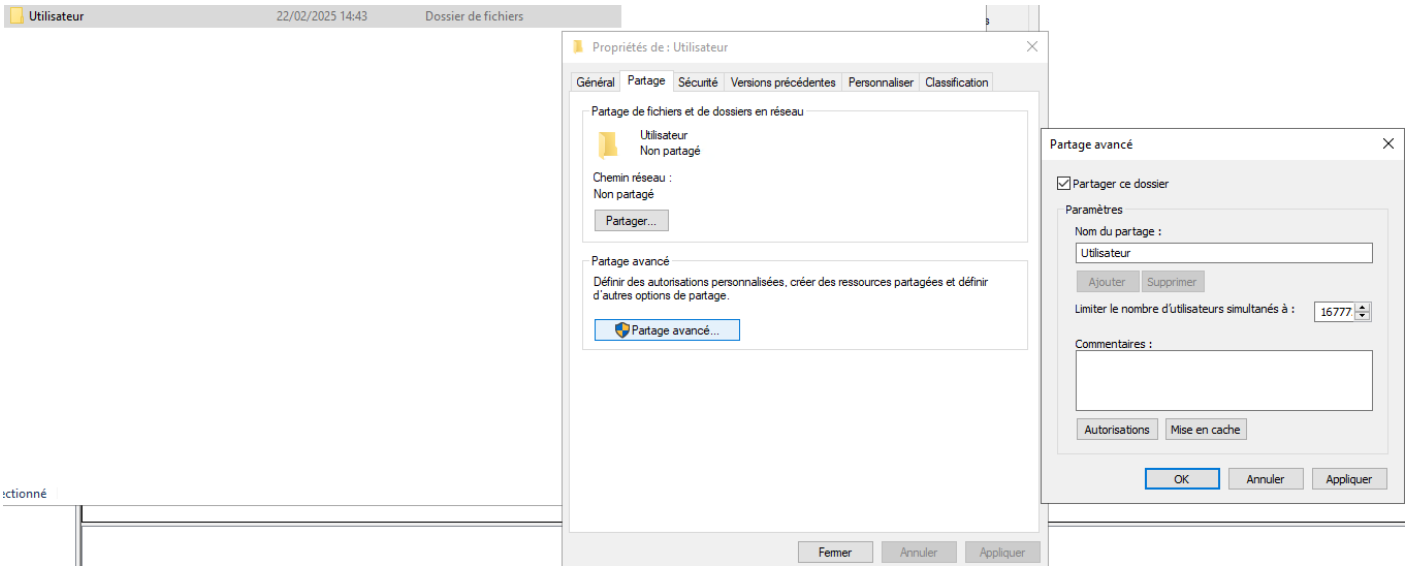
a)Création d'une GPO de lecteur partagé avec cota

Dans cette parti, nous allons crée une partage réseau avec cota. Ce partage sera "privé", c'est-à-dire que chaque utilisateur pourra mettre des documents ou autre sans que les autres les vois.

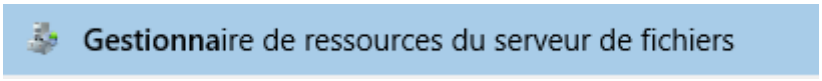
Pour ça, nous allons donc activé une option dans Windows Server, "Gestionnaire de ressources du serveur de fichiers" :



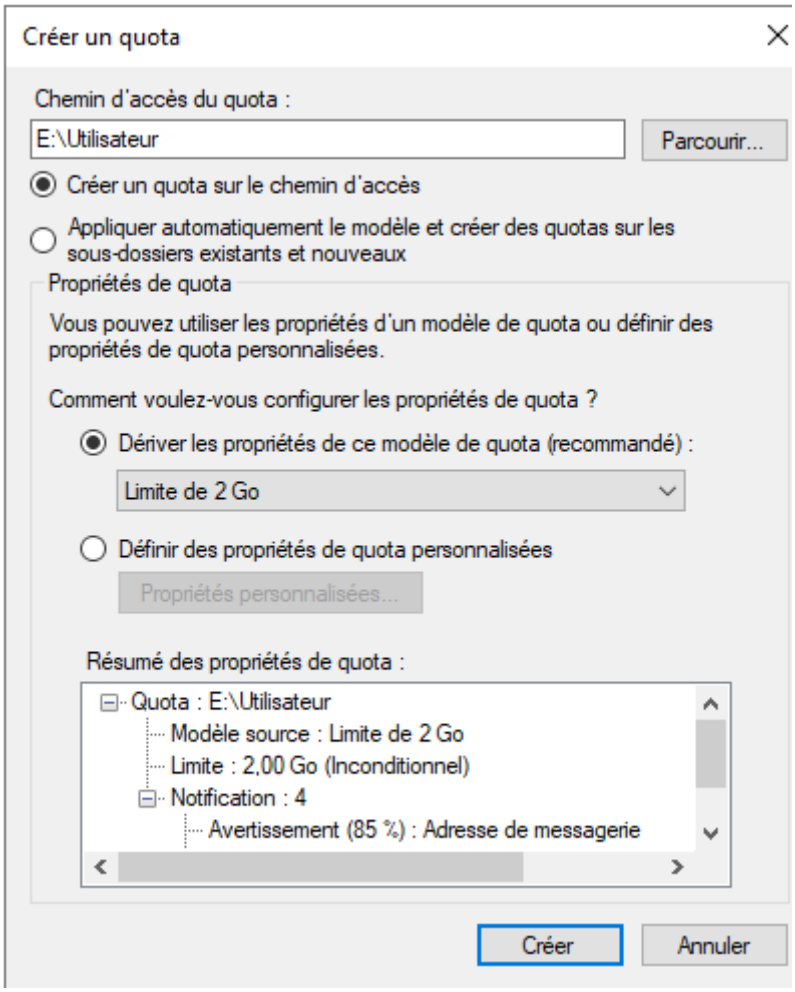
Une fois cela activé, nous allons créées le dossier qui va servir de base au partage, dans mon cas je l'ai nommé Utilisateur$ et que j'ai partagé en supprimant "Tout le monde" dans "Autorisation" et rajouté tous les droits à "Utilisateurs du domaine":



Une fois ce dossier créée, on ouvre "Gestionnaire de ressources du serveur de fichiers" :

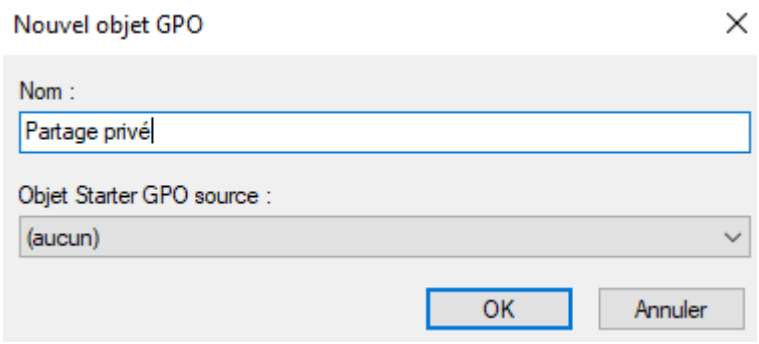


Nous allons dans "Gestion de quota>Quotas" et clic droit et "Créer un quota". Ici je vais utilisé une une propriétés de modèle de quota déjà créer qui est de 2go. J'ai spécifier mon dossier en local dans un premier temps et dans un second temps le quota à appliqué puis "Créer" :



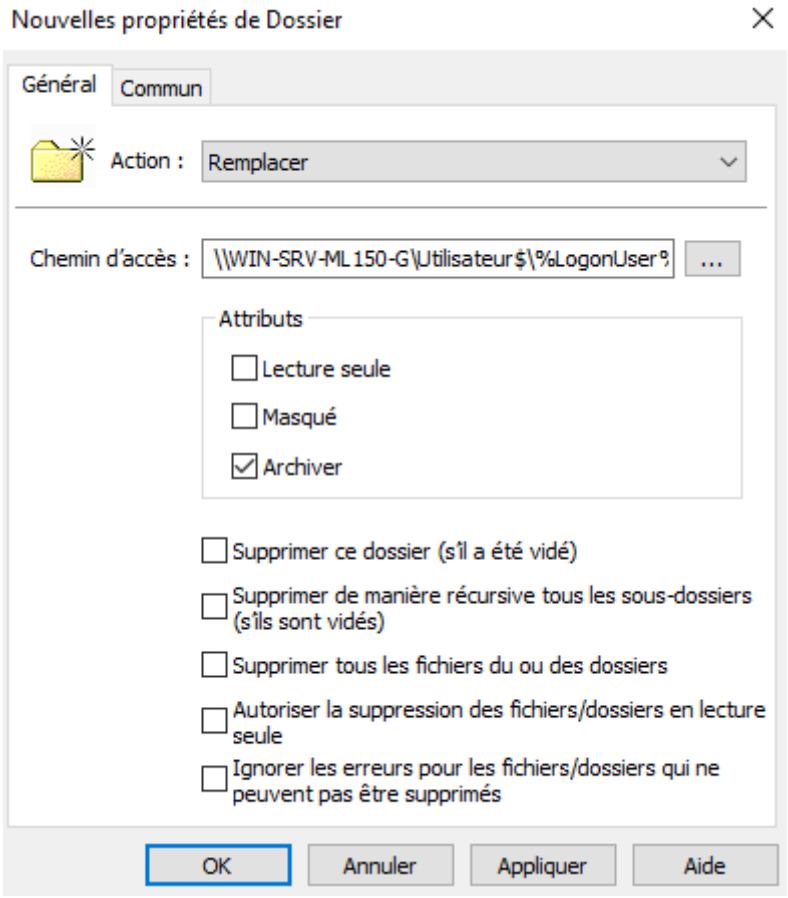
Chemin d'accès du quota	% utilisé	Limite	Type de quota	Modèle source	Modèle correspondant
Modèle source : Limite de 2 Go (1 élément)					
E:\Utilisateur$	0%	2,00 Go	Inconditionnel	Limite de 2 Go	Oui

Nous passons maintenant à la création de la GPO et je vais la nommé dans mon cas "Partage privé" :

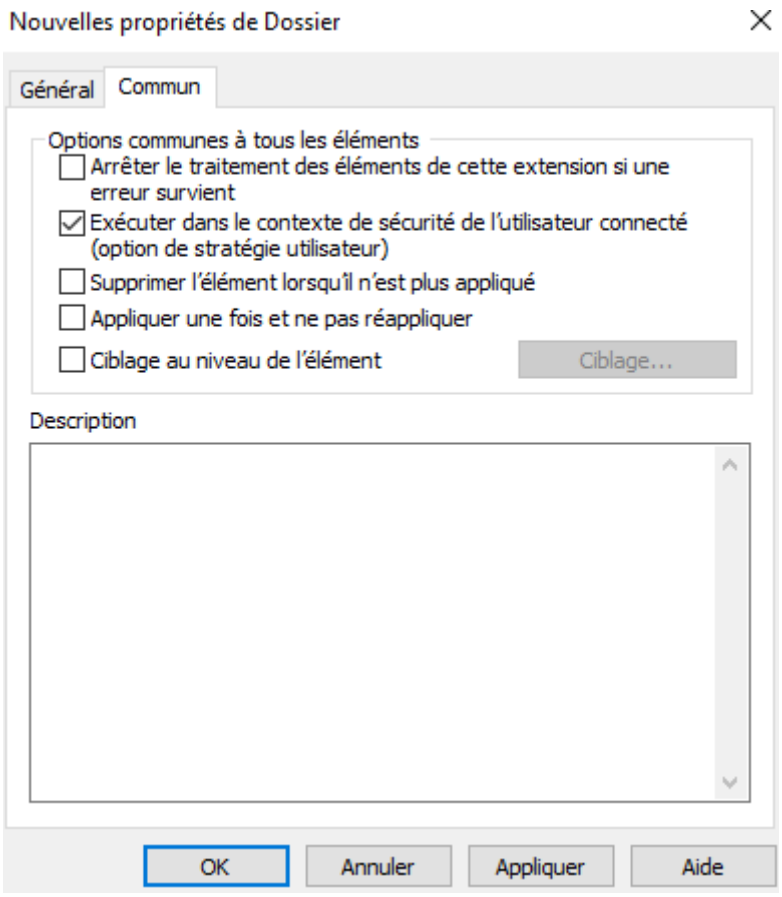


On arrive donc dans la GPO. Allez dans « Configuration Utilisateur>Préférences>Dossier » et faite clic droit « Nouveau>Dossiers» :

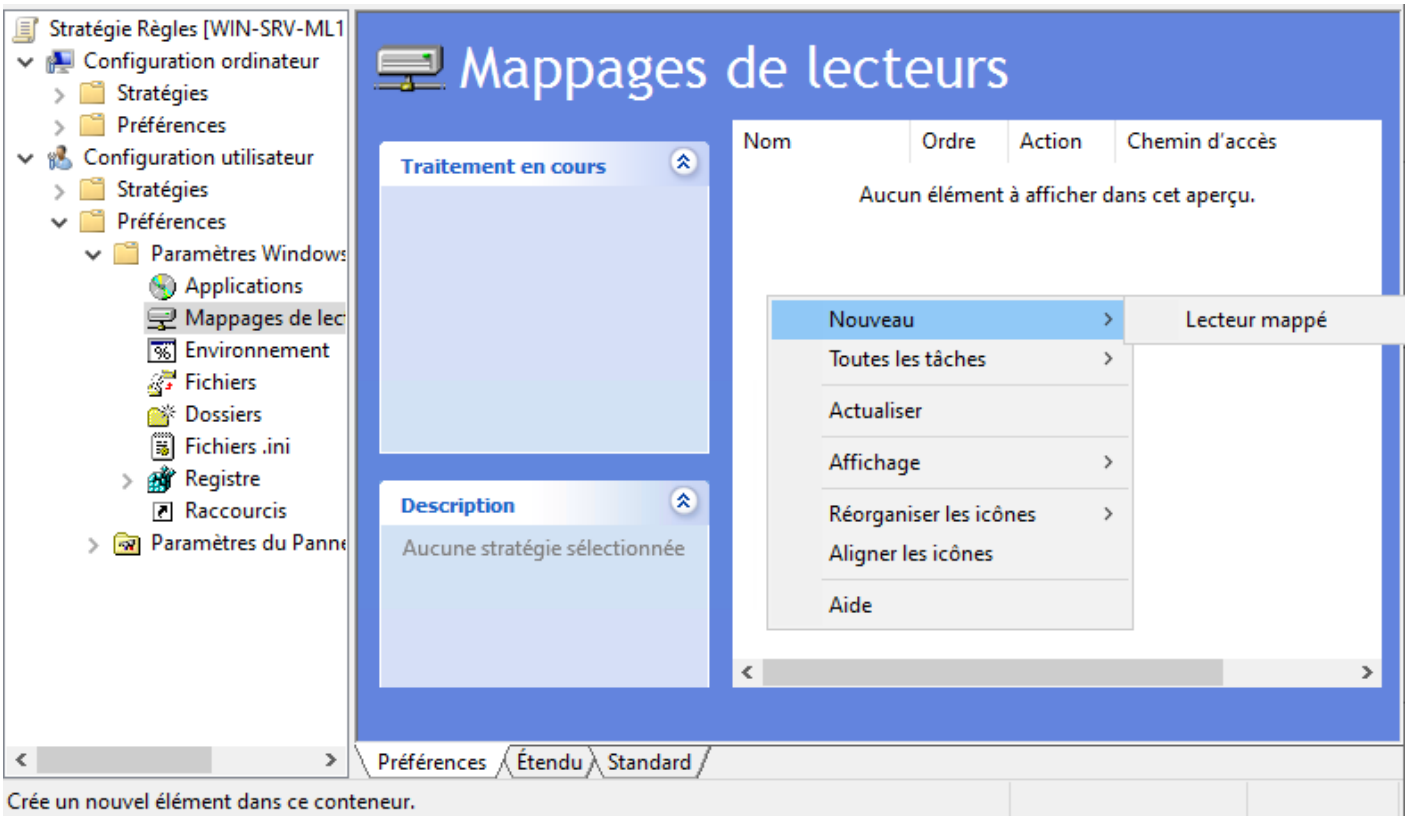
Nous allons donc mettre comme "Action" "Remplacer" puis comme "Chemin d'accès" le chemin réseau du dossier partagé suivie de "%LogonUser%" qui permet de crée un dossier automatiquement quand un utilisateur se connectera :



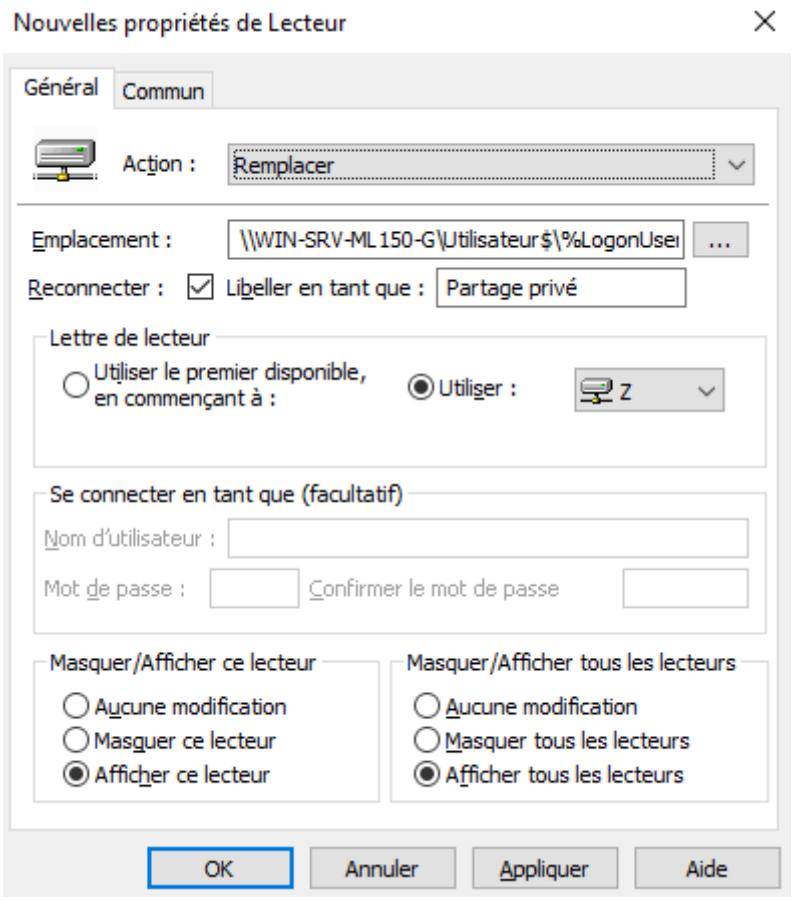
Et pour des questions de sécurité, nous allons allé dans l'onglet "Commun et coché "Exécuter dans le contexte de sécurité de l'utilisateur connecté" :



Faite appliqué puis on passe de Dossiers à Mappages de lecteur et faire clic droit "Nouveau>Lecteur mappé" :



Comme dis précédemment, dans "Action" on sélectionne "Remplacer" puis comme "Chemin d'accès" le chemin réseau du dossier partagé suivie de "%LogonUser%" qui permet de sélectionné automatiquement le dossier de l'utilisateur connecté. Puis dans mon cas j'ai donner comme nom à ce lecteur "Partage privé" qui aura comme lettre fixe Z:. Et pour finir, on coche "Afficher ce lecteur" et "Afficher tous les lecteurs" :

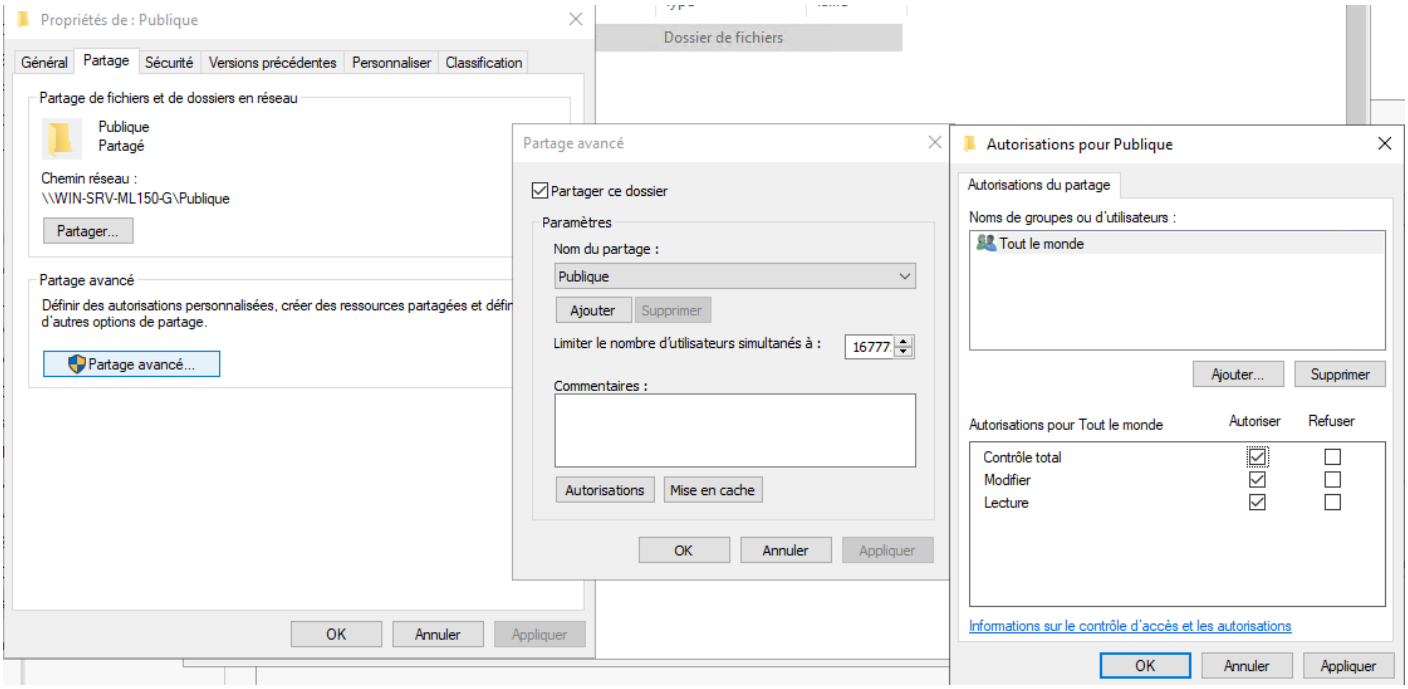


On fait appliqué.

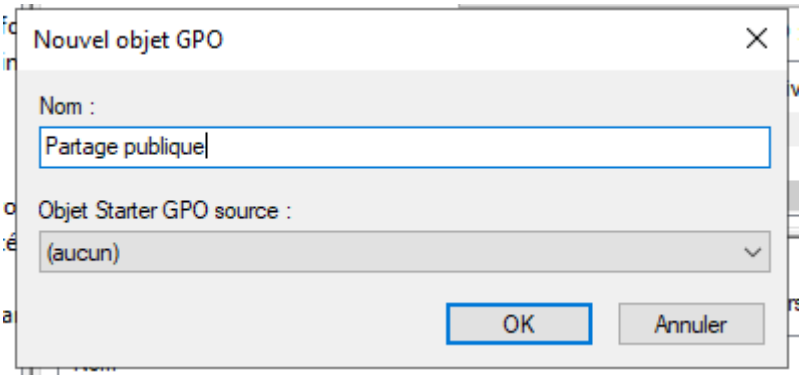
b)Création d'une GPO de dossier sans cota

Dans cette second parti, nous allons crée une partage réseau sans cota. Ce partage sera "publique", c'est-à-dire que chaque utilisateur verra ce que tous le monde mets dans ce lecteur.

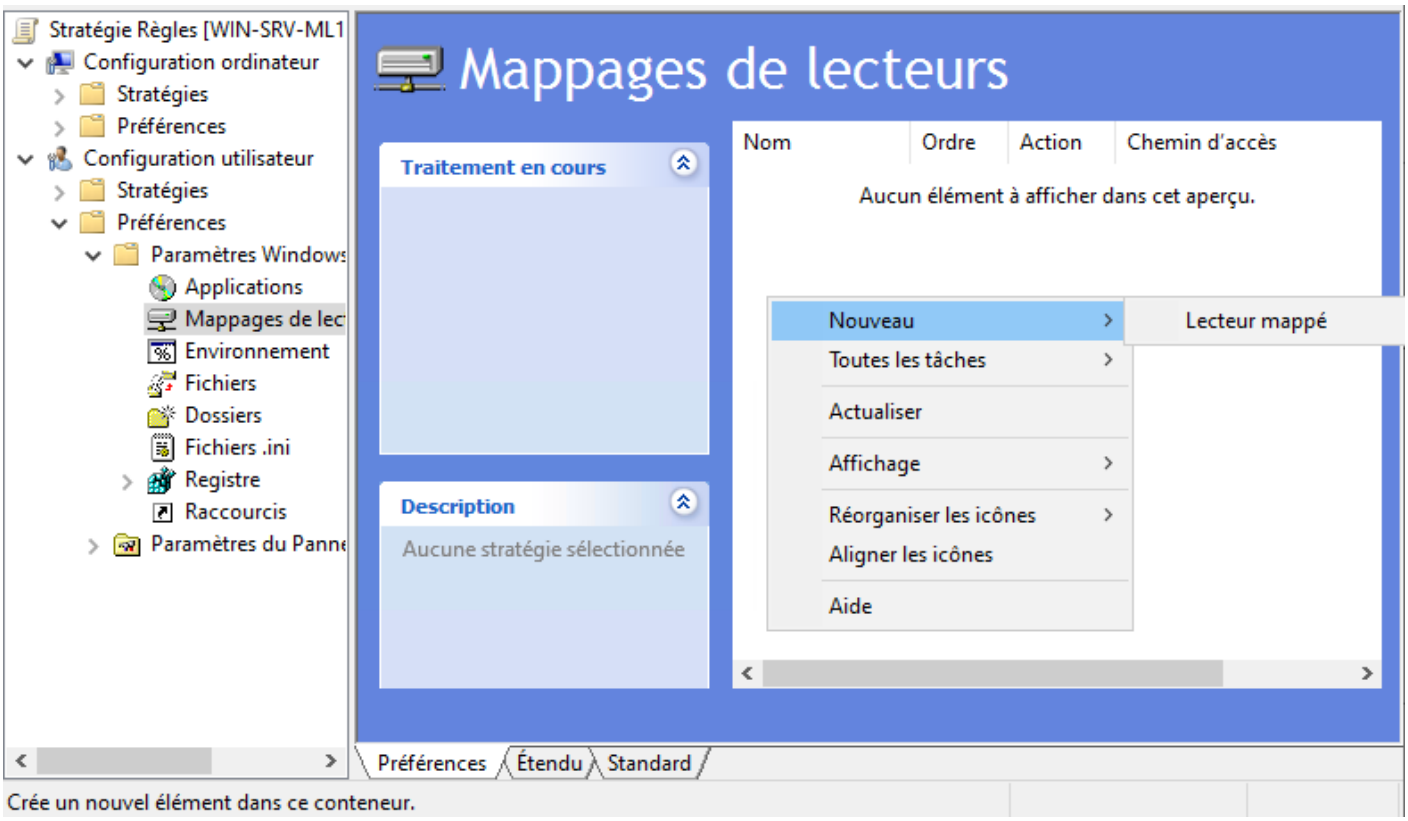
Nous allons créées le dossier qui va servir de base au partage, dans mon cas je l'ai nommé publique et partagé en autorisant tous à "Tout le monde":



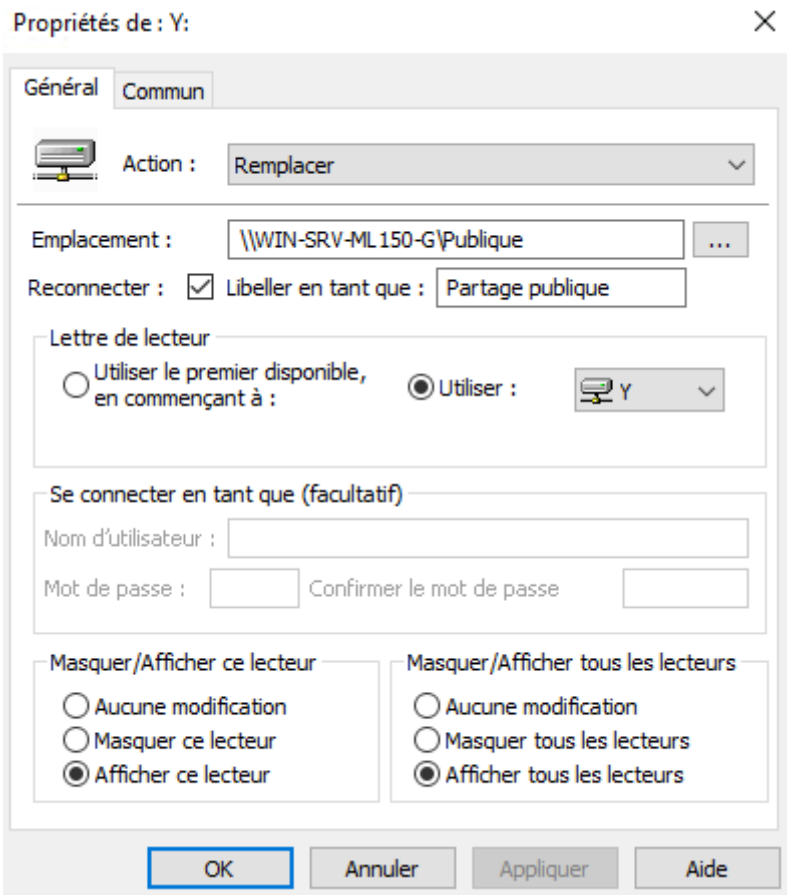
Nous passons maintenant à la création de la GPO et je vais la nommé dans mon cas "Partage publique" :



On arrive donc dans la GPO. Allez dans « Configuration Utilisateur>Préférences>Paramètres WIndows>Mappages de lecteur" et faire clic droit "Nouveau>Lecteur mappé" :



Comme dis précédemment, dans "Action" on sélectionne "Remplacer" puis comme "Chemin d'accès" le chemin réseau du dossier partagé. Puis dans mon cas j'ai donner comme nom à ce lecteur "Partage privé" qui aura comme lettre fixe Y: (on ne peut pas donner Z: comme précédemment car cela créera un conflit de lettre) . Et pour finir, on coche "Afficher ce lecteur" et "Afficher tous les lecteurs" :



On fait appliqué.

c)Test

Pour ce test, j'effectue un simple gpupdate dans powershell :