Mise en place d’un Active Directory redondant d’entreprise - Proxmox

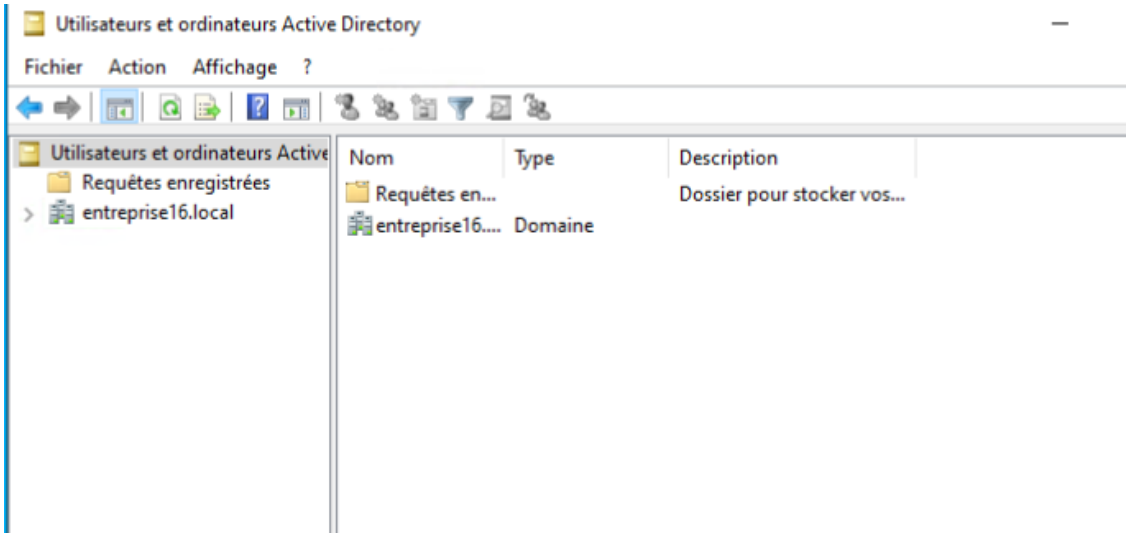
L’installation de l’Active Directory, la création du nom de domaine et la configuration du DHCP ne seront pas détaillées ici, car elles sont déjà expliquées dans le TP.

Creation d'utilisateurs

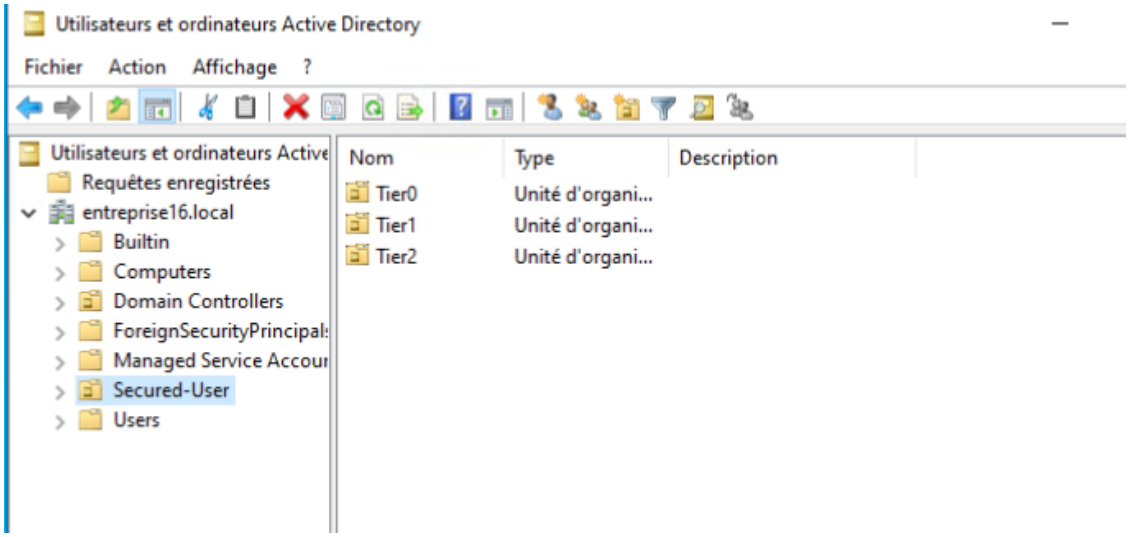
- Microsoft recommande une séparation des postes d’administration selon trois niveaux de sensibilité permettant de limiter les risques en cas de compromission :
    - Tier 0 : ressources critiques du SI (Contrôleurs de domaine, PKI, serveurs AD)
    - Tier 1 : administration des serveurs et applications (Serveurs Windows/Linux, hyperviseurs)
    - Tier 2 : postes utilisateurs
- L’objectif est d'éviter qu’un attaquant ayant compromis un poste utilisateur (Tier 2) puisse compromettre le domaine (Tier 0).
- Un administrateur ne doit jamais administrer un contrôleur de domaine depuis une machine jointe au domaine, car cela favoriserait :
    - la récupération de mots de passe administrateurs,
    - la possibilité d’escalade directe vers le Tier 0.

L’administration doit donc être réalisée depuis un poste d’administration dédié, ici appelé Admin, à l’aide d’un compte sécurisé AdminTier1.

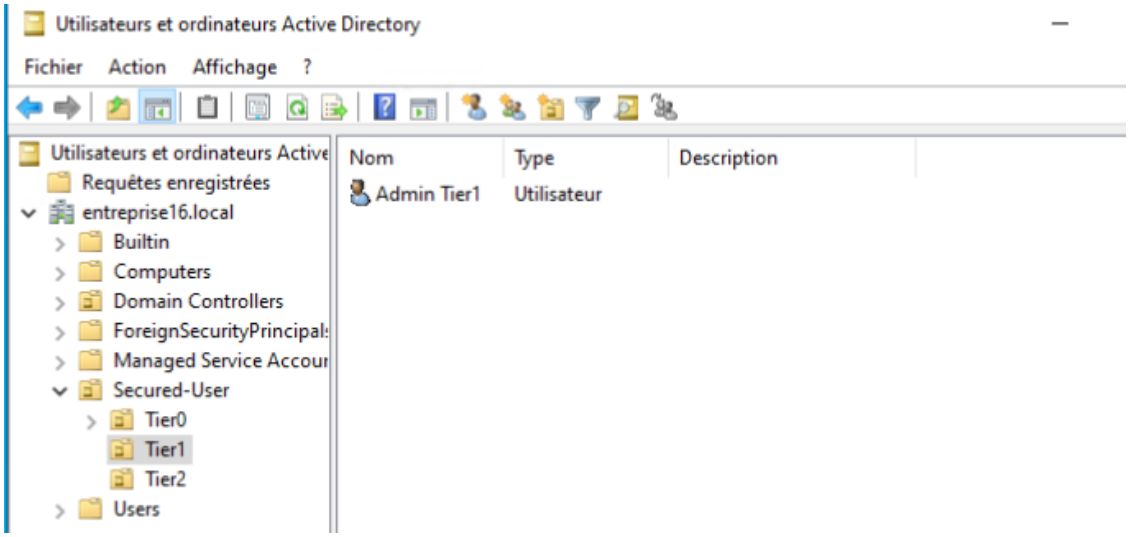
- Ce compte permettra notamment d’administrer :
    - Active Directory Users and Computers (ADUC),
    - les GPO,
    - le DNS,
    - le DHCP,
    - les scripts PowerShell AD.
- Pour ce faire voici les etapes pour creer l'utilisateur AdminTier1 dans l'UO Tier1:
    - Faut aller dans Utilisateurs et ordinateurs Active Directory dans la barre Windows:



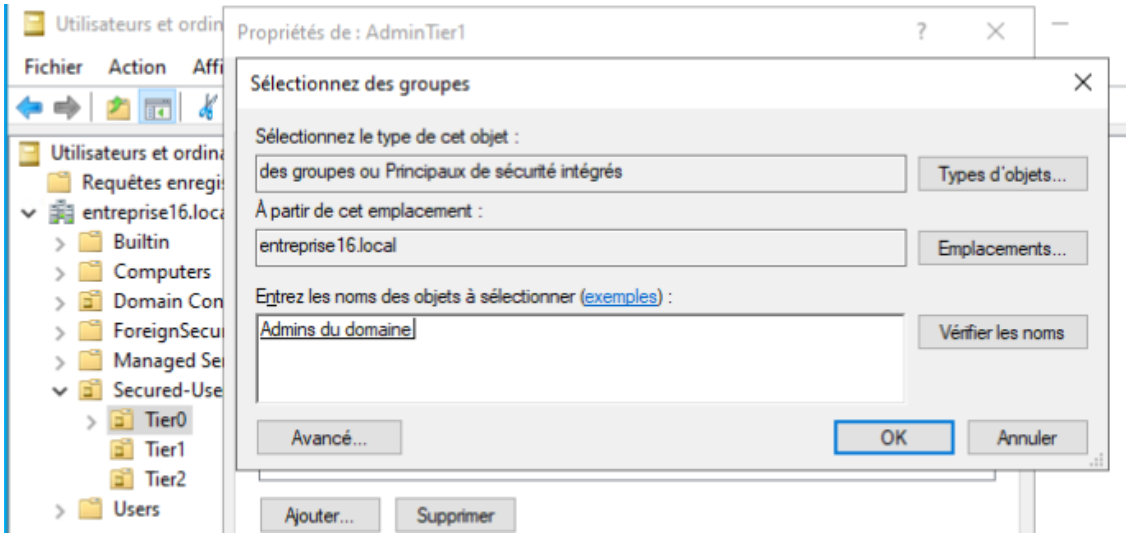
- Ensuite, on clique sur le nom de domaine pour déployer tous les dossiers.
- On se place dans le dossier Secured-Accounts, c'est là que nous avons mis nos UO.



- Dans Tier1, on fait clic droit → Nouveau → Utilisateur.
- On remplit les champs (Admin, Tier1, AdminTier1), on met un mot de passe en décochant "changer le mot de passe", puis on clique sur Terminer.



- Ensuite, on ouvre les propriétés du compte et on l'ajoute au groupe Administrateurs du domaine(admins du domaine).



Une GPO (Group Policy Object), ou Objet de stratégie de groupe, est un ensemble de paramètres permettant aux administrateurs Active Directory de contrôler et de configurer automatiquement le comportement des postes clients, des utilisateurs, et parfois des serveurs au sein d'un domaine Windows.

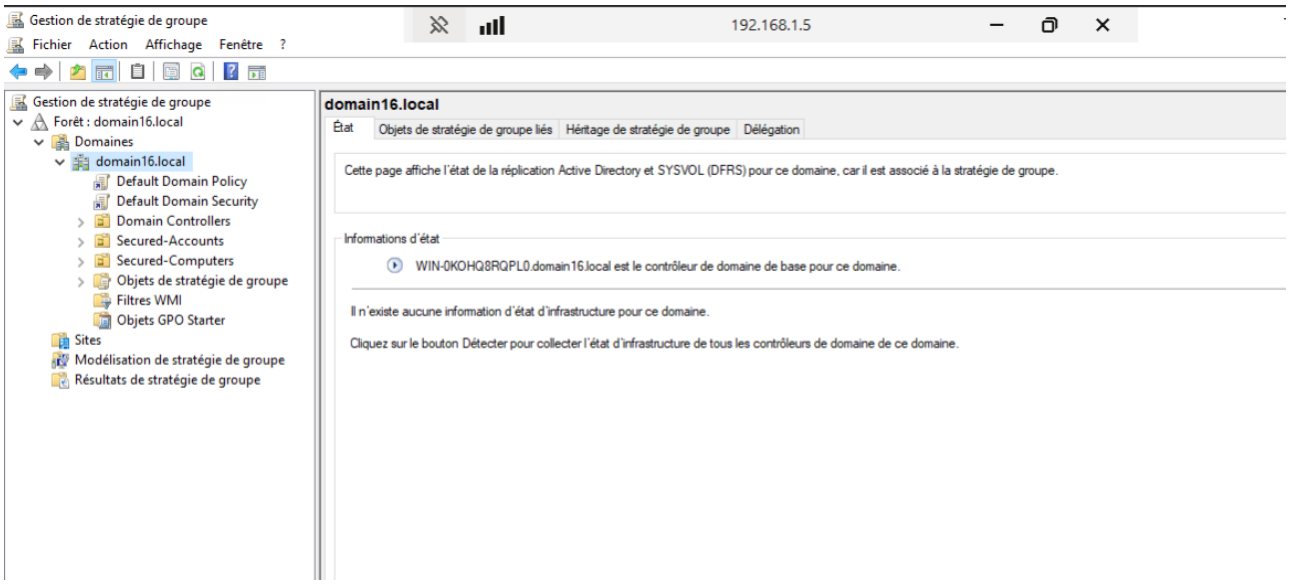
- Les GPO servent à appliquer des réglages centralisés, comme par exemple :
    - des paramètres de sécurité (mots de passe, verrouillages, restrictions),
    - des configurations système (fond d'écran, accès au panneau de configuration, scripts),
    - des déploiements de logiciels (via fichiers MSI),
    - des restrictions applicatives (PowerShell, CMD, installations).
- Elles sont hébergées dans l'Active Directory et s'appliquent automatiquement selon l'endroit où elles sont liées :
    - au niveau du domaine,
    - au niveau d'une Unité d'Organisation (UO),
    - ou au niveau d'un site.

VI/3 GPO Hardening postes utilisateurs

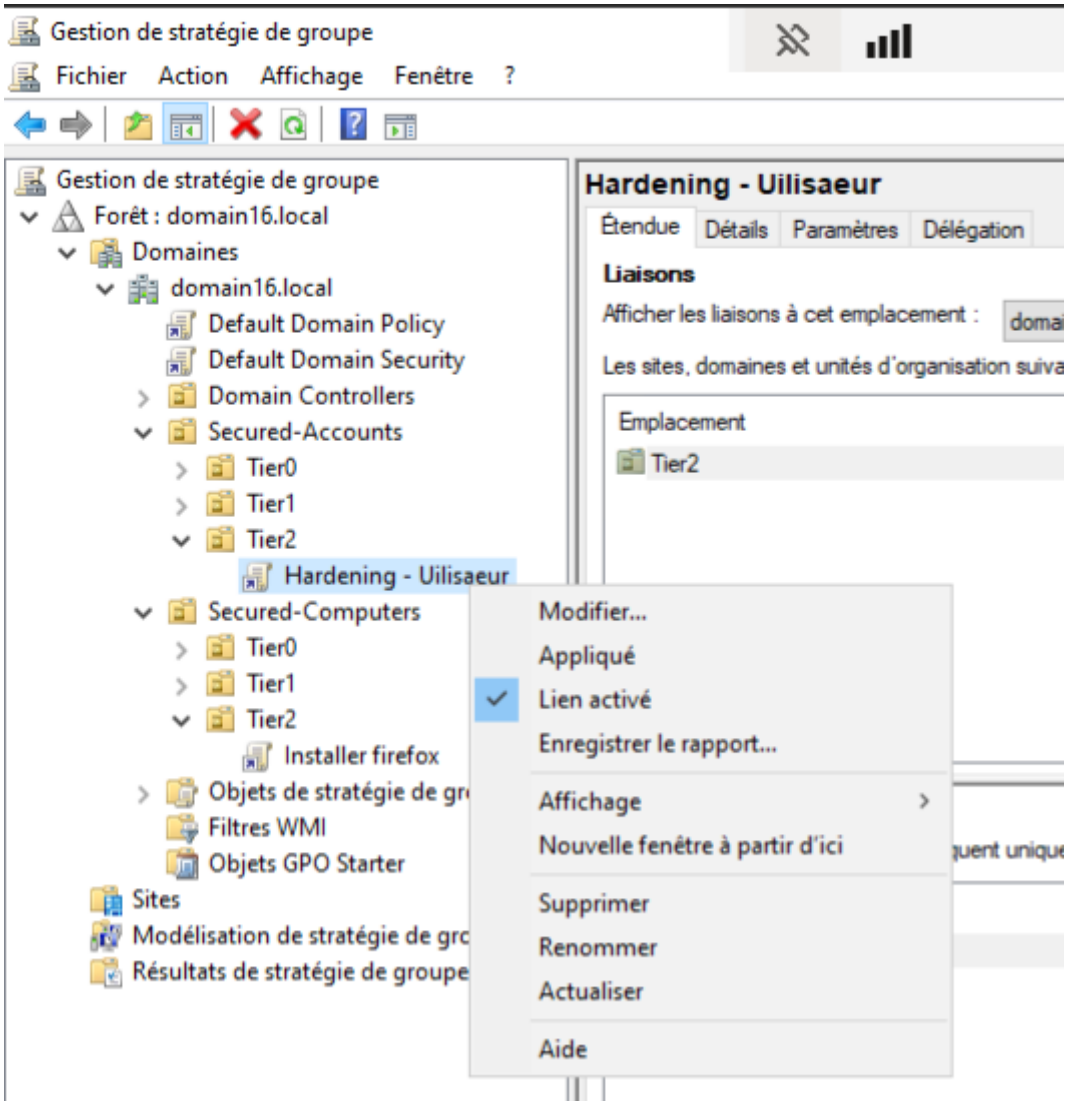
Moi, j'ai créé une seule GPO pour tout. Cependant, il est recommandé de créer différentes GPO pour chaque type de restriction, afin de faciliter la gestion et le dépannage.

Créer une GPO désactivant le panneau de configuration et les paramètres pour les utilisateurs clients

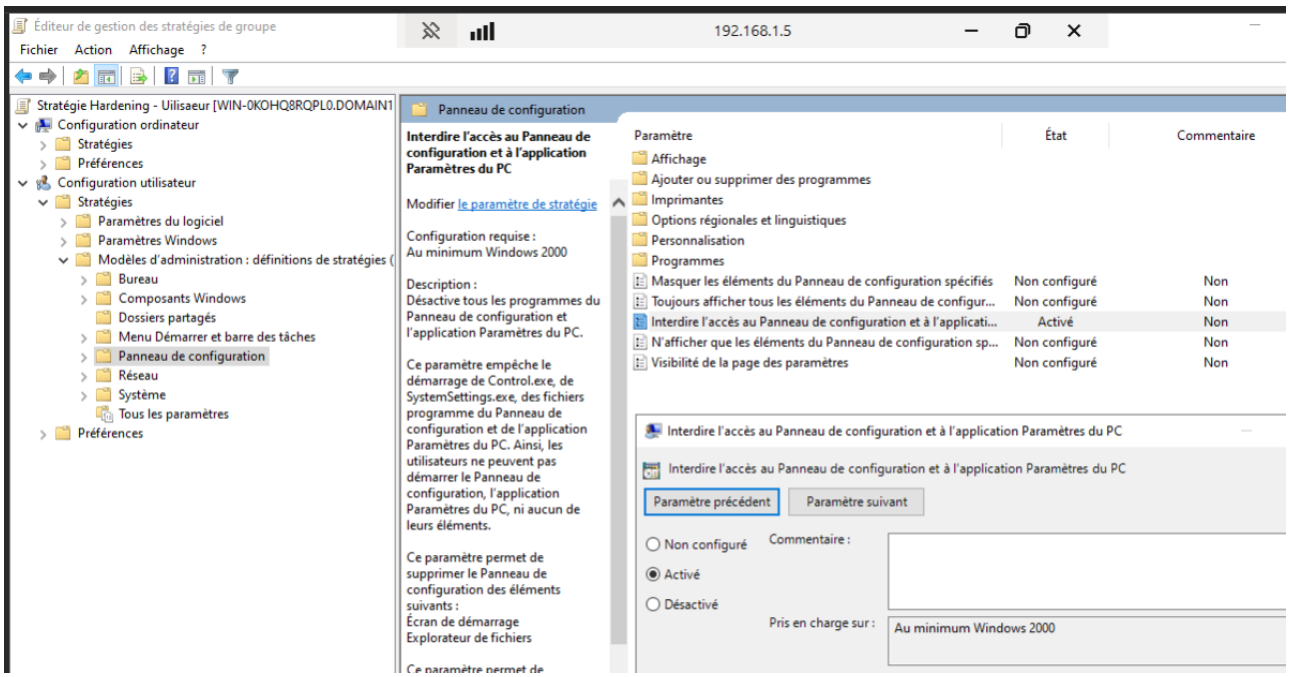
- Tout d'abord on rentre sur `Gestion de stratégie de groupe` et on se positionne au niveau de notre domaine, dans mon cas c'est `domain16.local`:



- Ensuite, on crée une nouvelle GPO en faisant un clic droit à l'endroit où se trouvent nos utilisateurs.
- On lui donne un nom clair, puis, une fois la GPO créée, il suffit de cliquer dessus et de sélectionner Modifier pour commencer la configuration. Dans mon cas je l'ai mis dans `Secured-Accounts` , dans `Tier2` .

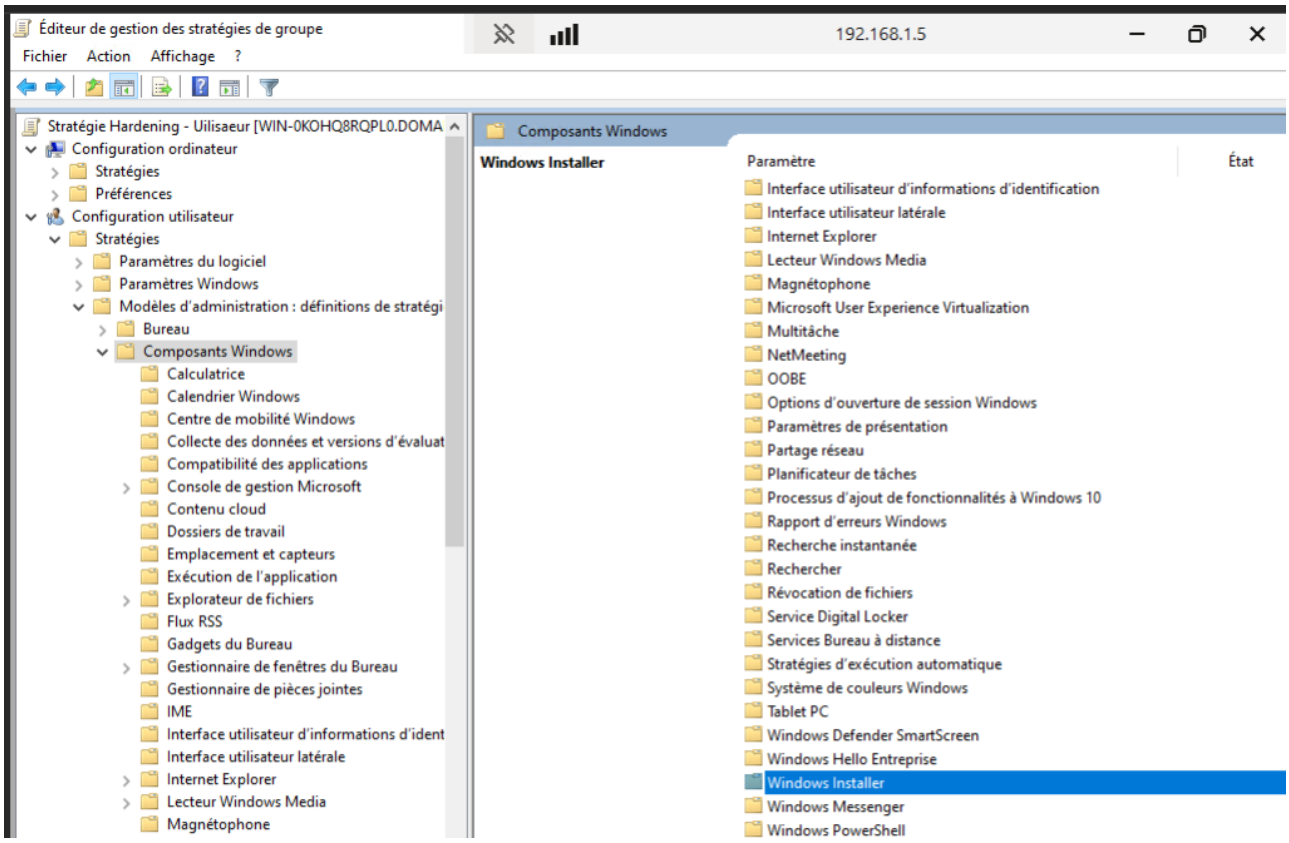


- Lorsque l'on clique sur Modifier, on accède directement à la configuration de la GPO.

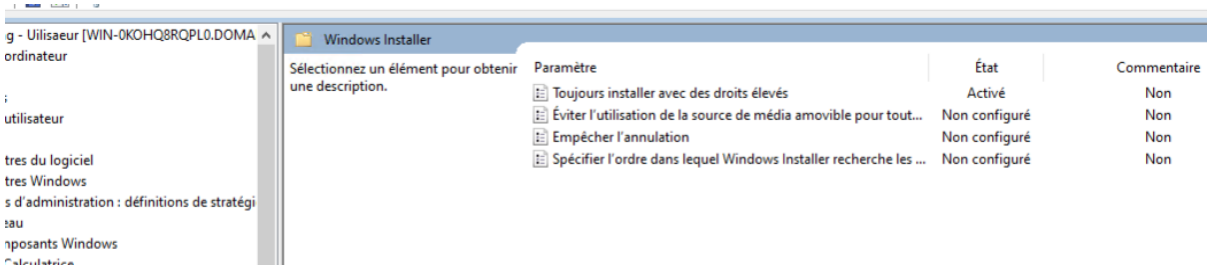
- Ici, nous voulons interdire l'accès au Panneau de configuration ainsi qu'aux Paramètres de Windows.
- Pour cela, on va dans :
    - Configuration de l'utilisateur → Stratégies → Modèles d'administration → Panneau de configuration.
- Ensuite, on sélectionne la règle "Interdire l'accès au Panneau de configuration et aux Paramètres du PC", puis on l'active.
- 

Créer une GPO pour empêcher les utilisateurs clients d'installer des logiciels

- Puisque nous utilisons une seule GPO regroupant toutes les restrictions, il suffit simplement d'ajouter la règle correspondante dans cette GPO.
- On va sur:
    - Configuration de l'utilisateur → Stratégies → Modèles d'administration → Composants Windows → Windows Installer

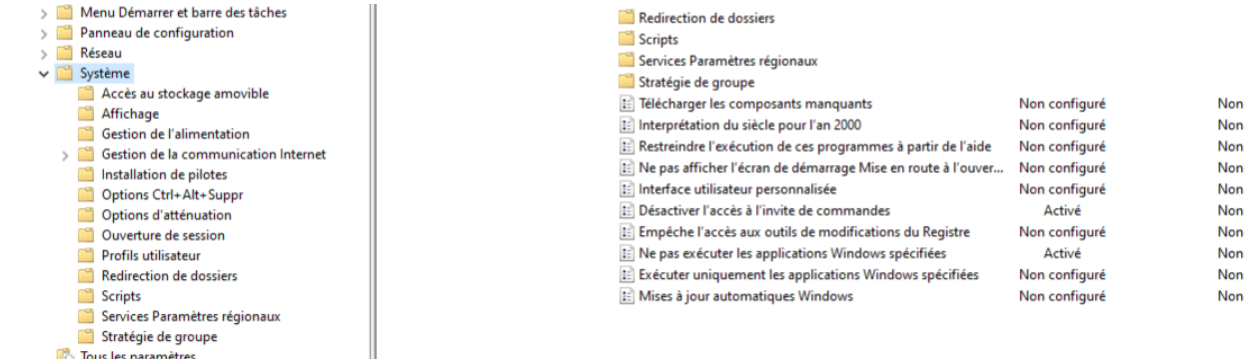


- On active l'option toujours installer avec des droits élevés:

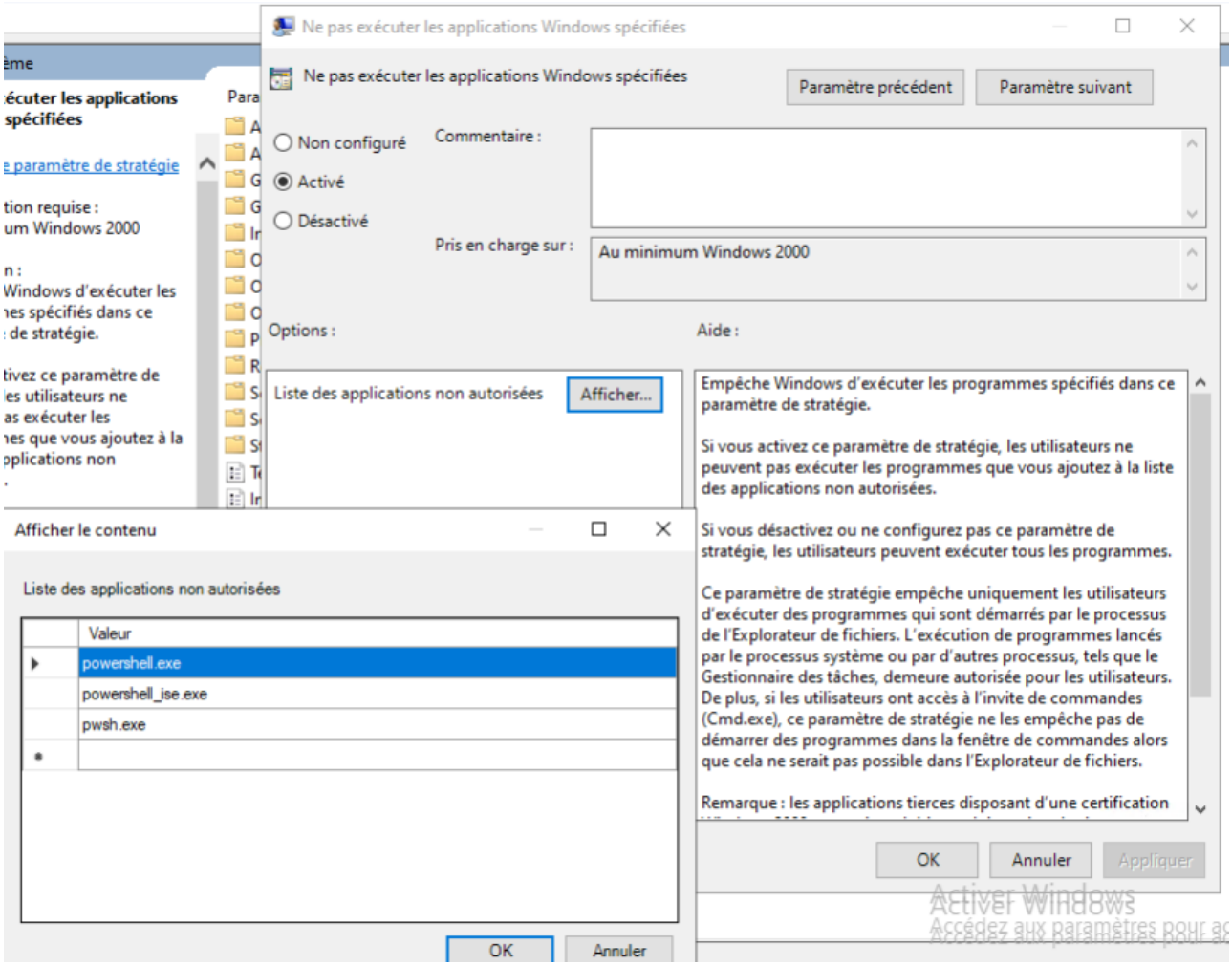


Créer une GPO pour empêcher les utilisateurs clients d'accéder à l'invite de commande ainsi qu'au PowerShell

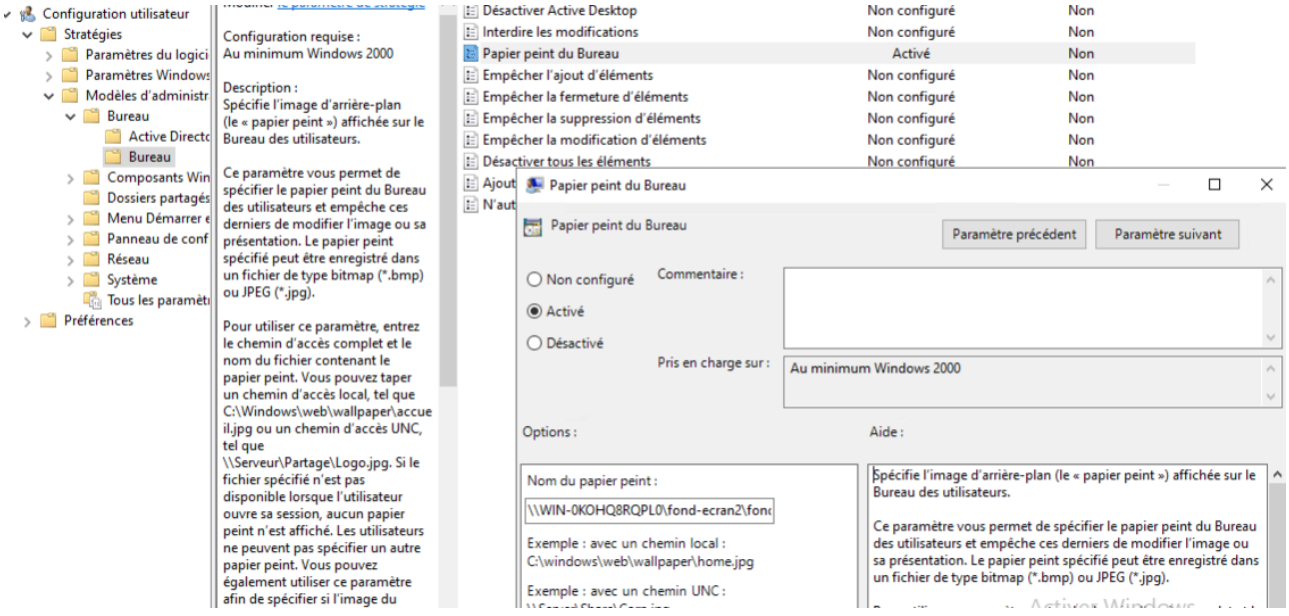
- Pour se faire on se replace sur COnfiguration de l'utilisateur:
  - Configuration de l'utilisateur → Stratégies → Modèles d'administration → Système



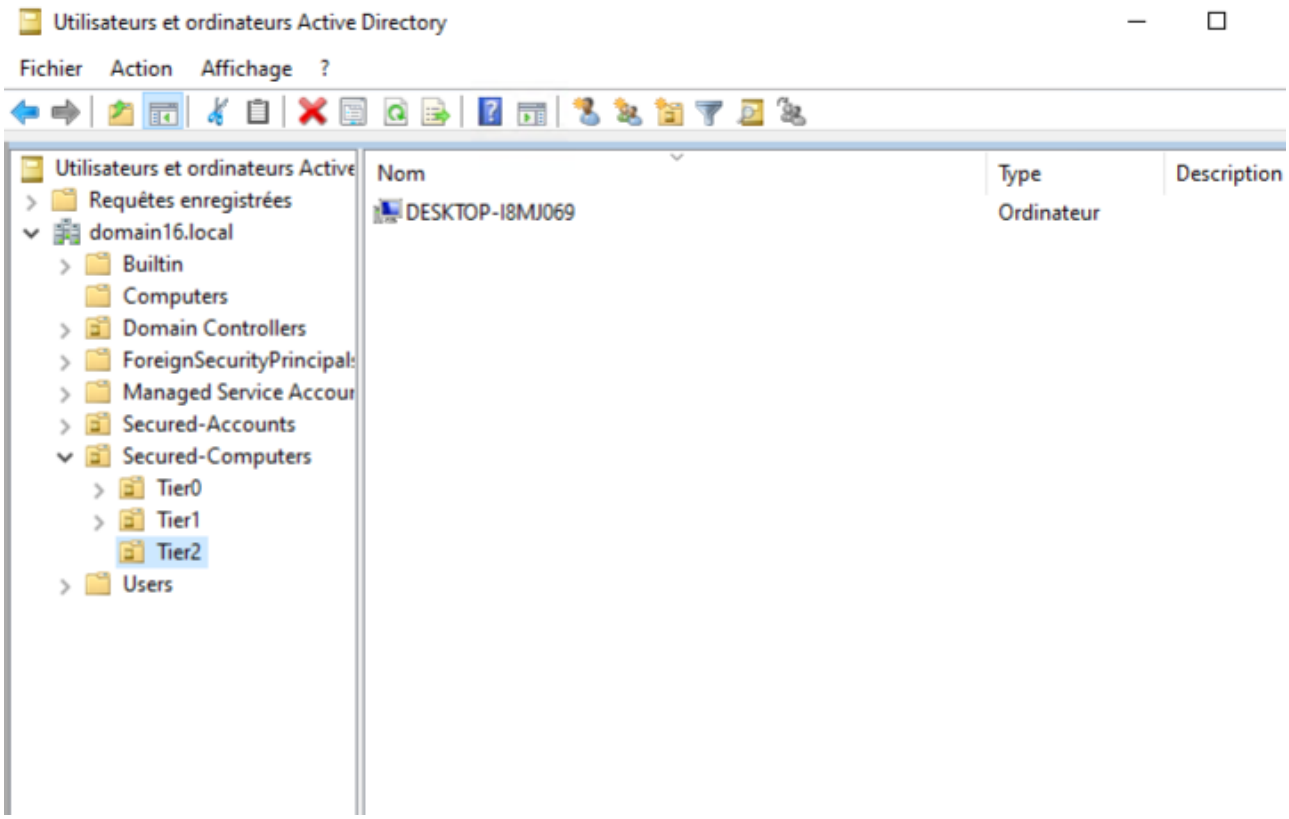
- On active l'option desactiver l'accés à l'invite de commande
- Et dans l'option "Ne pas exécuter les applications spécifiées", on met powershell.

- 

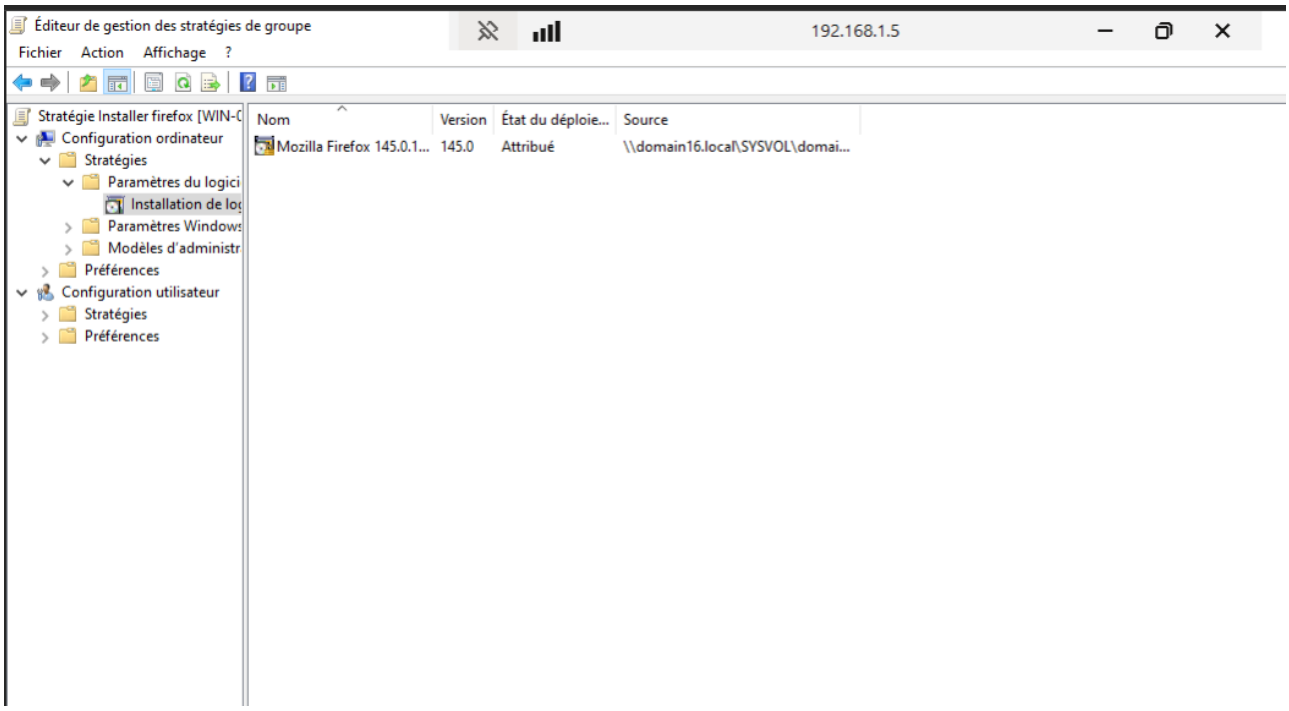
Créer une GPO pour forcer le fond d'écran des sessions utilisateurs client

- Pour cette etape on se place sur:
  - Configuration de l'utilisateur → Stratégies → Modèles d'administration → Bureau → Bureau
- Dans l'option "Fond d'écran du Bureau", on sélectionne Activé et on indique le chemin réseau vers le dossier partagé contenant le fond d'écran. Le dossier partagé doit être accessible automatiquement à chaque session de l'utilisateur.
- 

VI/4 GPO spécifique : déploiement de logiciel

- Pour cet exemple, nous allons déployer Firefox. Nous avons placé le fichier d'installation dans le dossier C:\Windows\SYSVOL\domain\software (le dossier software a été créé et contient le logiciel Firefox).
- Tout d'abord, nous allons déplacer le poste client qui se trouve dans Computers vers l'UO que nous avons créée, Secured-Computers, plus précisément dans Tier2.
- 

- Une fois déplacé, on se rend dans Gestion des stratégies de groupe pour créer une nouvelle GPO dans Secured-Computers, sous Tier2.
- Une fois la GPO créée et nommée, on clique sur Modifier et on va dans :
  - Configuration de l'ordinateur → Stratégies → Parametre du logiciel
- À cet endroit, on fait un clic droit → Nouveau → Package et on sélectionne le logiciel via le chemin réseau : \domain16.local\SYSVOL\domain16.local\software (et non pas le chemin local C:\Windows\SYSVOL\domain\software). Le chemin local est lié au chemin réseau, et c'est ce dernier qu'on attribue pour que le déploiement fonctionne correctement \domain16.local\SYSVOL\domain16.local\software\Firefox....



Redondance d'AD en binome

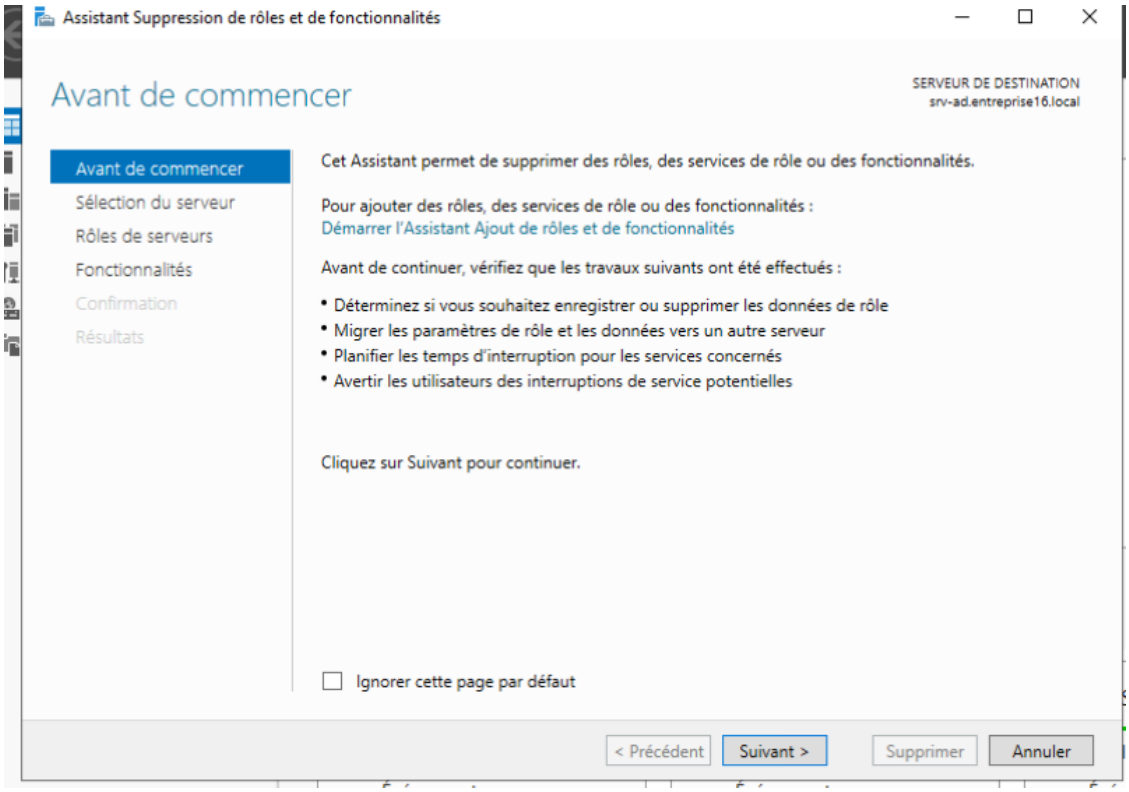
- Avant le déploiement en binôme, il a fallu s'assurer que les deux environnements Proxmox soient configurés de manière identique :
  - Même plan d'adressage réseau (LAN en 192.168.1.0/24)
  - pfSense configuré en 192.168.1.1
  - Deux serveurs AD avec adresses fixes (étudiant A : 192.168.1.5, étudiant B : 192.168.1.6)
  - Un domaine commun(on va voir comment on fait)

Domaine en coummun

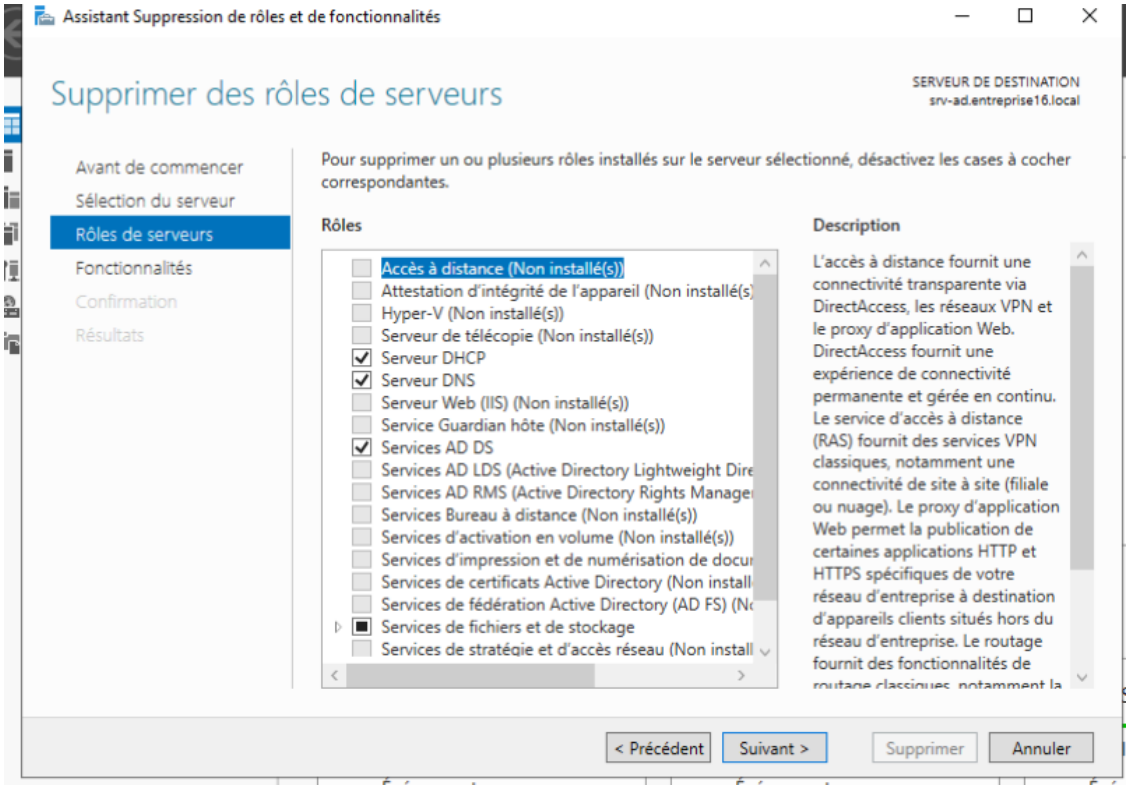
- Au début du TP, chaque étudiant avait installé son propre Active Directory avec un domaine différent. Lors de la mise en binôme, il fallait obligatoirement travailler dans un domaine commun, ce qui a nécessité la rétrogradation des deux serveurs AD.

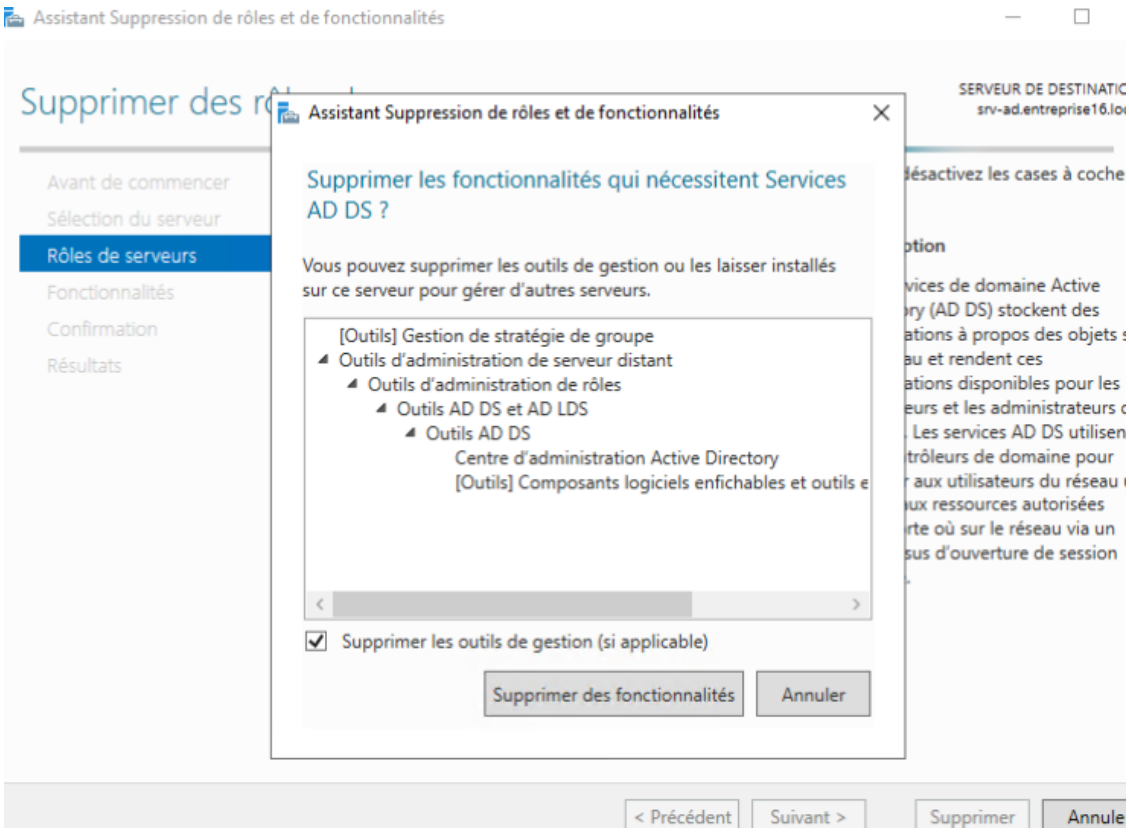
Rétrogradation de mon AD(AD-A)

- De mon côté, j'ai rétrogradé mon serveur pour qu'il ne soit plus contrôleur de domaine et redevienne un serveur standard:
  - J'ai ouvert le Gestionnaire de serveur, puis je me suis placé dans Gérer en haut à droite pour cliquer sur Supprimer des rôles et fonctionnalités.



- Ensuite, on clique sur Suivant à deux reprises, on appuie sur AD DS pour arriver avec l'assitant, puis on clique sur Supprimer des fonctionnalités:





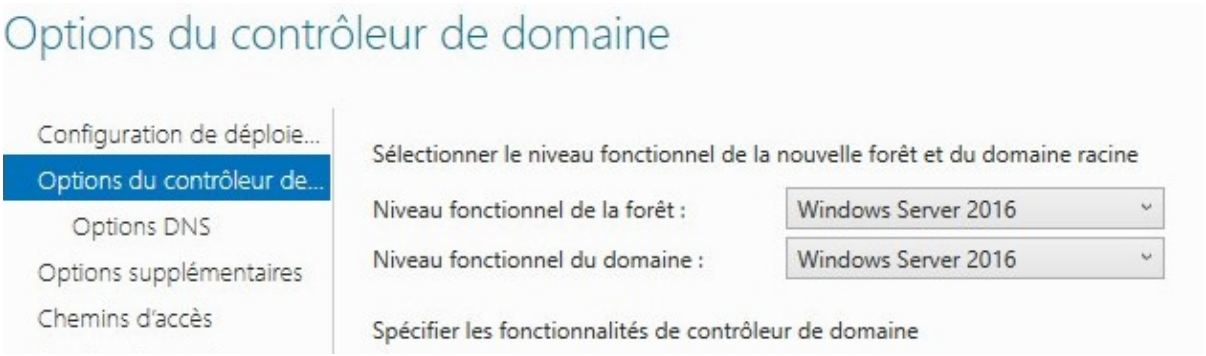
- Une erreur lors de la validation va alors s'afficher à l'écran, on vous indique que le serveur doit être rétrogradé avant de pouvoir supprimer ce rôle. Cliquez sur "Rétrograder le contrôleur de domaine", un second assistant va s'exécuter.
- On coche forcer la suppression de ce controleur de domaine ensuite sur suivant.
- Ya un avertissement on met suivant, on laisse par defaut et on met suivant.
- On creer un mot de passe (on peut reutiliser le meme)
- On clique sur retrograder et on attends
- Ensuite on confime et on met supprimer pour redemarer.

Promotion des serveurs Active Directory après rétrogradation

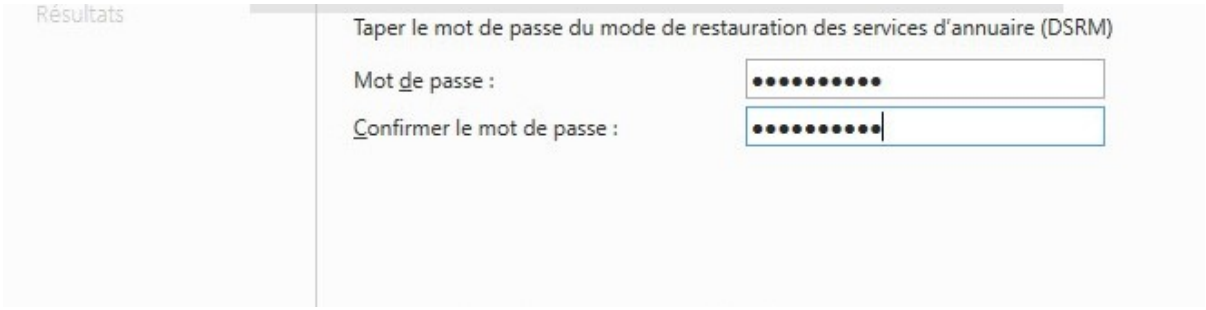
- Une fois le serveur redémarré, on ouvre le Gestionnaire de serveur, on clique sur le drapeau en haut à droite et on sélectionne Promouvoir ce serveur en contrôleur de domaine.

- Une fois dedans, on arrive sur configuration de déploiement et la on selectionne "ajouter une nouvelle forêt"

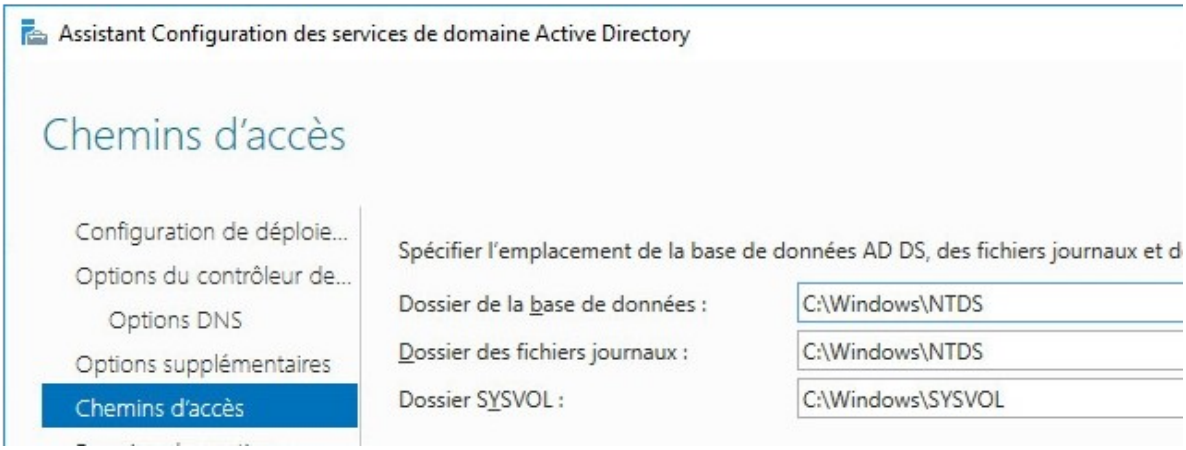
- On arrive sur les options du controleur de domaine et on met les options suivantes:



- Dans la meme etape on met un mot de passe:



- Sur option de DNS on met suivant, pour le NetBios on met suivant.
- Sur le chemain d'access on laisse par defaut:



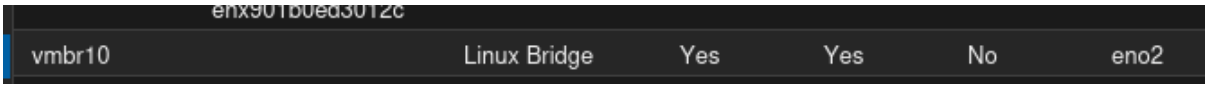
- Dans Examiner les options, on vérifie les paramètres puis on clique sur Suivant.
- On attend la fin de l'installation, puis le système redémarre automatiquement.

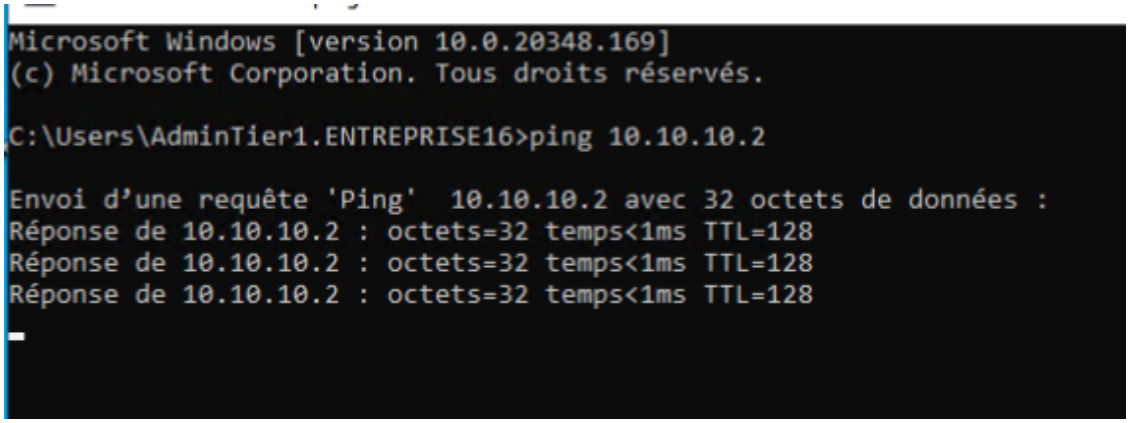
Pour AD-B

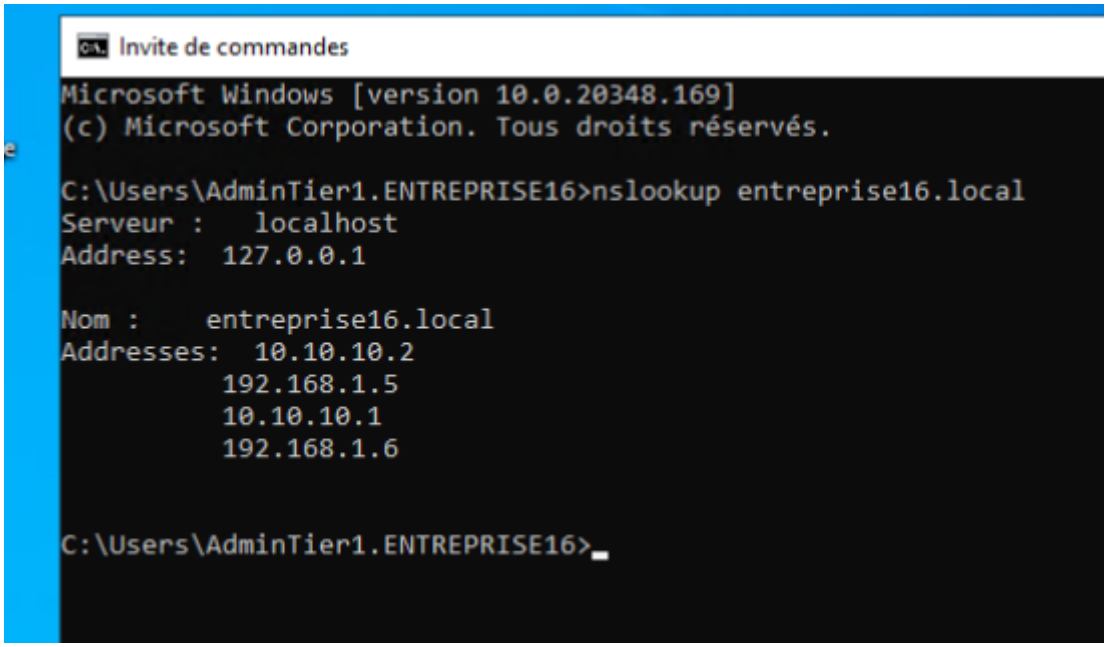
- Pour AD-B, il faut faire la même procédure de rétrogradation et de promotion. La différence est que, lors de la promotion, il ne faut pas créer une nouvelle forêt, mais rejoindre un domaine existant

(entreprise16.local), afin que les deux serveurs fassent partie du même domaine pour la redondance.

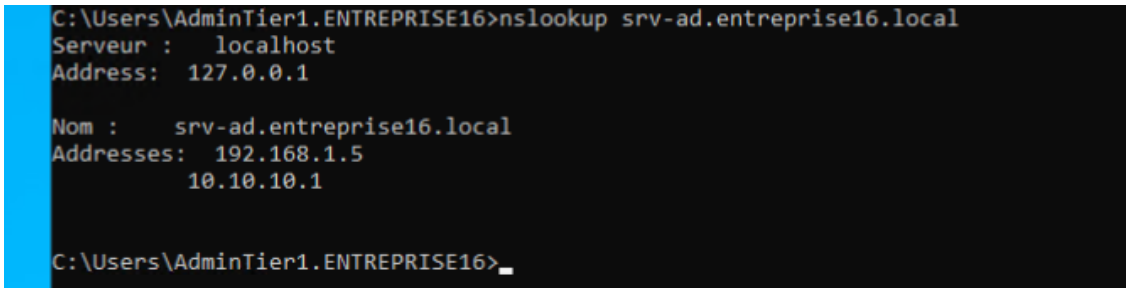
Création d'un réseau inter-site et connectivité

- Pour permettre la communication entre nos deux contrôleurs de domaine (AD-A et AD-B), nous avons configuré un réseau point-à-point et ajouté une deuxième carte réseau sur chaque VM.
- Les deux serveurs Proxmox sont reliés par un câble Ethernet sur l'interface physique eno2.
  - Le pont virtuel vmbr10 est associé à cette interface (eno2), ce qui permet aux machines virtuelles connectées à vmbr10 de communiquer directement via ce câble.
  - 

- Configuration IP :
  - AD-A : 10.10.10.1/30 avec le premier DNS de 127.0.0.1 et le deuxiemme de AD-B
  - AD-B : 10.10.10.2/30 avec le premier DNS de AD-A et le deuxiemme 127.0.0.1
  - Pas de gateway configurée sur cette carte réseau.
- Pour tester la connectivité il suffit juste de pinger les deux machines entre eux.
  - Le ping de AD-A vers AD-B:
    - 

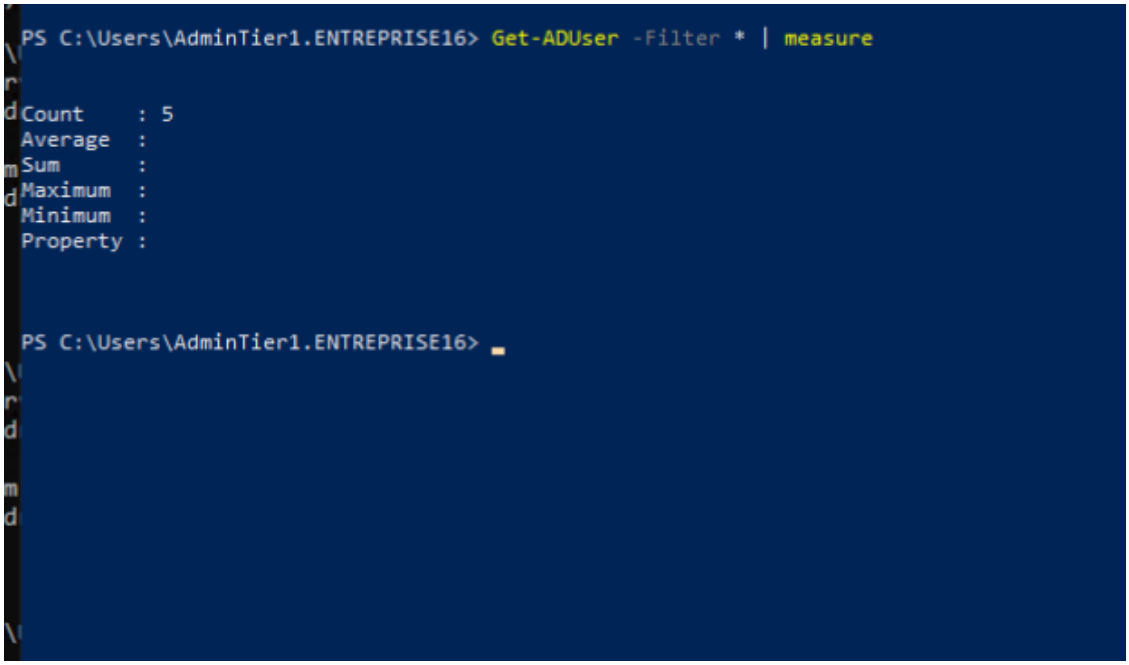
- On verifie aussi les resolutions DNS depuis AD-B avec les commandes
  - nslookup entreprise16.local
    - 

  - nslookup SRV-AD(AD-A).entreprise16.local



Vérifier la réplication et la redondance

- L'objectif ici est de s'assurer que les deux contrôleurs de domaine (AD-A et AD-B) ont les mêmes données et que la réplication fonctionne correctement.
- Sur AD-A et AD-B, exécuter les commandes suivantes :
  - repadmin /replysummary
  - repadmin /showrepl
- Sur le AD-A et AD-B exécuter:
  - Get-ADUser -Filter * | measure
    - Les deux AD doivent renvoyer le même nombre d'utilisateurs, confirmant que la réplication fonctionne.



- Depuis un client du LAN de A exécuter:
  - whoami /fqdn
  - nltest /dsgetdc:entreprise16.local
  - Ça doit tomber parfois sur l'AD-A et AD-B
- Depuis un client du LAN de B refaire de meme et faut avoir le meme resultat.

Test en cas de panne

- Éteindre AD-A puis refaire les tests depuis les clients.
  - L'AD actif doit être AD-B >> Rallumer AD-A, éteindre AD-B, refaire les tests.
  - L'AD actif doit être AD-A.

Cela permet de vérifier que la redondance fonctionne et que les services restent accessibles même si un DC tombe.