CPAM Ardèche / Greta Ardèche-Drôme

Active Directory

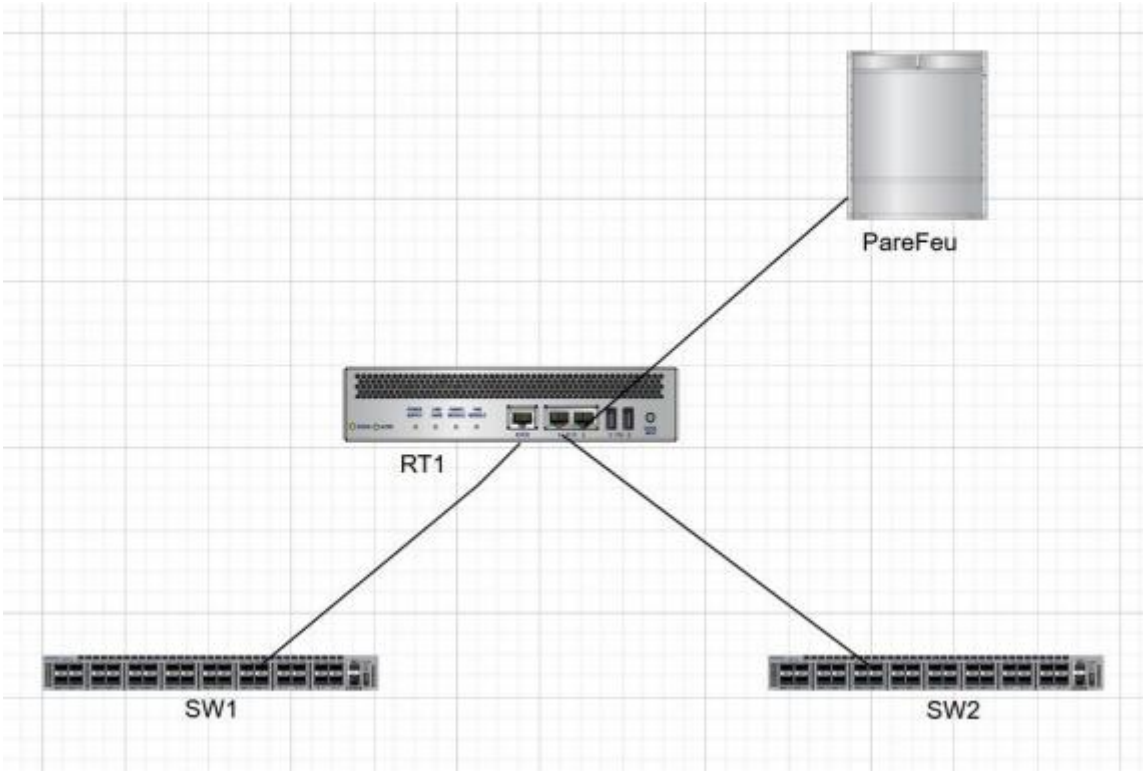
TP

Collet Valentin
BTS SIO-SISR / Session 2026

SOMMAIRE

Cahier des charges

Descriptifs de l'existant



L'infrastructure existante se compose d'un PareFeu, d'un routeur et deux switches.

L'infrastructure possède déjà un nom de domaine qui est au format : MySocVCt.fr.

De plus au niveau de l'organisations des services :

L'entreprise est composée de 6 services : organisés en deux sous-réseaux :

SR 1 : où se trouve le service technique et le service de recherche et développement

SR 2 : où se trouve la comptabilité, commercial, l'administration et enfin les ressources humaines.

Chaque service est composé de 6 utilisateurs, dont un chef/cadre.

Besoins

Afin de réaliser ce TP, il faut :

1. Deux VM Windows Server 2025 avec AD / DNS (afin d'assurer une redondance)
    - 60 go d'espaces de stockage prévu sur chaque VM avec 8Go de RAM alloué chacune.
2. Pfsense qui servira de routeur, pare-feu et assura le service DHCP au sein de l'infrastructure.

- Port AD : 389 (port de transfert de données standard)/636 (port de transfert de données sécurisées avec protocole TLS)
- Deux interfaces LAN pour deux sous-réseaux

3. Deux clients Windows (un pour chaque sous réseau)
4. Un plan des groupes et permissions de l'AD afin d'organiser et faciliter sa mise en œuvre

Contraintes

La principale contrainte est celle du temps dans un contexte de TP réaliser en centre de formation sur 16H de cours au total.

La mise en place d'un serveur AD implique aussi la présence d'un Domain Name Server (DNS) pour assurer son fonctionnement.

De plus, au cours de ce TP la configuration de l'Active Directory se fera selon la méthode AGDLP (Account, Global Groups, Domain Local groups, Permissions) qui permet de gérer les permissions dans l'AD et ainsi simplifier l'administration des utilisateurs et des ressources accessibles. Avec des permissions spécifiques selon les dossiers et les utilisateurs (cf schéma infrastructure AD).

Ressources

J'ai un poste de travail à disposition avec un hyperviseur de type 2 : Vmware Workstation afin de réaliser ce TP. Ce poste dispose d'un SSD de 500go et de 32Go de RAM pour assurer le bon fonctionnement des VM.

L'intervenant est ici aussi une personne ressource au cours de ce TP afin de me conseiller et répondre à mes questionnements.

Plusieurs cours sur l'active directory sont à ma disposition : allant de sa mise en place avec redondance (ce qui implique aussi un cours sur les DNS), puis un cours sur la méthode AGDLP me permettant d'avoir un AD organisé et logique.

Enfin l'infra existante implique un routeur à part, or j'ai choisi d'utiliser le PareFeu PfSense dans un souci de rapidité et praticité en tant que routeur comme vu pendant le TP, ce qui supprime un sous réseau 3 (entre PFsense et le routeur initiale).

Analyse

Descriptif des solutions

Service d'annuaire : est un système servant à stocker, organiser et gérer les informations d'un réseau informatique : **ressources** (dossiers, applications) et **utilisateurs** tout en y appliquant des politiques de sécurité. Le but étant de simplifier la gestion d'une infrastructure et de s'assurer de sa sécurité.

Active Directory : est la solution Microsoft de service d'annuaire, qui est basé sur LDAP. Celui-ci permet la gestion centralisée des **utilisateurs** et **groupe**, des **machines** et des **ressources réseaux** (imprimantes par exemple), de plus à la différence de LDAP il est possible de gérer les **stratégies de sécurité** (GPO / Group Policy Objects).

Celui-ci permettra une **authentification unique (SSO)** permettant d'accéder aux ressources réseaux avec un seul identifiant / mot de passe (ou carte agent + code PIN par exemple), une **gestion centralisée** pour administrer des utilisateurs, groupes et machines, l'**application de stratégie** (restriction d'utilisation des postes, scripts de login (par exemple des connexions réseaux après authentification). De plus la **sécurité** y est plus importante (chiffrement des données, possibilité d'audit et contrôle d'accès). Enfin ce service peut être intégré avec d'autres services : serveur Exchange (messagerie microsoft), Azure AD pour une solution AD sur le cloud.

Protocole Kerberos : est un **protocole d'authentification** utilisé par Active Directory où le client envoie son mot de passe à un service d'authentification sur le serveur AD, celui-ci délivre un ticket qui va permettre au client de s'authentifier

LDAP : (Lightweight Directory Access Protocol) est un protocole servant à agir avec un service d'annuaire (principalement utilisée pour des recherches rapides et un accès fréquent).

Celui-ci est organisé avec une structure sous forme **d'arbre** (dc = mysocvct, dc= fr), avec un **modèle objet** (utilisateurs, groupes, périphériques, poste, etc…) et attributs (nom, adresse, mot de passe)

Au niveau des protocoles utilisé : TCP/IP sur le port 389 pour les échanges standards ou 636 pour les transferts sécurisés par SSL/TLS.

Il va permettre une authentification dite centralisée (login / mot de passe), le stockage d'informations (sur les utilisateurs, groupes, postes, etc…), et l'intégration d'applications.

Dans notre cas j'utiliserais l'exemple d'un serveur LDAP open-source : OpenLDAP

Comparaison des solutions :

	OpenLDAP	AD	Analyse comparative
OS	Linux / Unix	Windows Server	
License	Open-source	Propriétaire (microsoft)	OpenLDAP ici a l'avantage de la gratuité
Cible	Infrastructure avec un environnement principalement orienté sur Linux , mais s'adapte tout de même très bien à des environnements mixtes	Infrastructure Windows, entreprises utilisant office 365 ou exchange	L'AD est plus adapté à des infrastructures Windows
Authentification	LDAP v3	LDAP + Kerberos (sécurisé via clé, pas de mot de passe clair)	X
Sécurité	Dépendante de la configuration (ex : TLS, SASL, ACL)	Elle y est intégrée avec Kerberos, (NTLM plus ancien),	Sécurité plus facilement gérée côté AD, mais tout aussi possible avec LDAP mais nécessitant une configuration plus complexe.
Structure	Arborescence	Arborescence LDAP + domaine, forêt et unités d'organisations (OU)	Plus de possibilité de trie et manipulations côté AD
Administration	En CLI ou via des outils tiers (phpldapadmin)	Via interface graphique intégrée ou en CLI (powershell principalement)	Facilité d'administration et configuration côté AD

Choix d'une solution

L'Active Directory sera la solution choisie, premièrement car celui-ci est à mettre en place dans le cadre du TP, de plus l'AD reste une solution plus simple à paramétrer dans un environnement d'entreprise orienté Windows, surtout qu'ici nos machines clients ont des OS Windows.

De plus, l'ajout des GPO, outils natif de l'AD permet la gestion de l'infrastructure plus efficacement en s'appliquant à des groupes.

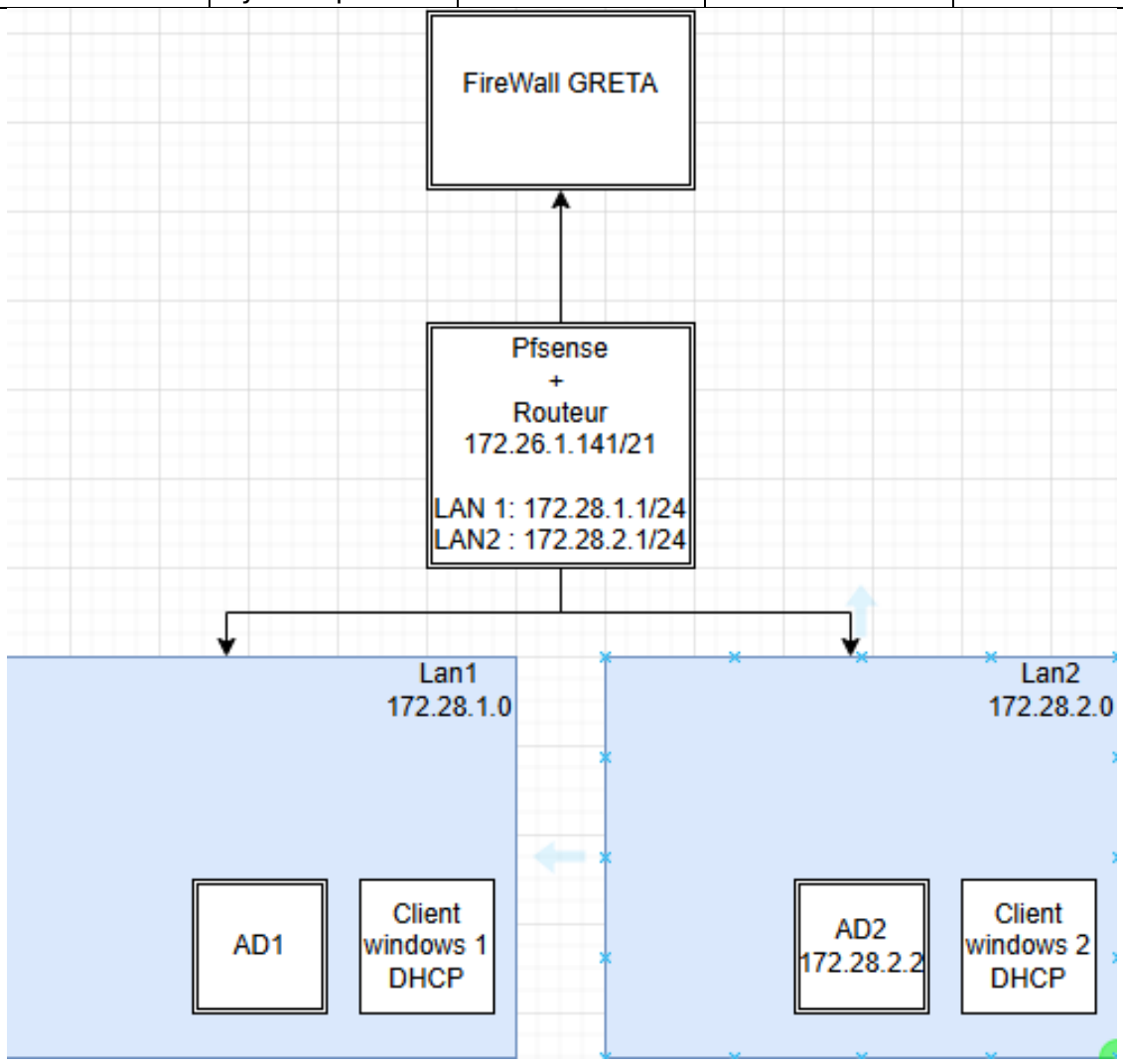
Enfin au niveau de la sécurité, les deux alternatives offrent des choix solides, mais l'AD de par sa sécurité intégrée renforcée pousse mon choix vers la solution de Microsoft.

Enfin, il est notable qu'OpenLDAP est une solution moins coûteuse qu'AD qui lui nécessite des licences Windows Server, ce qui serait à prendre en compte dans un cadre professionnel selon le budget de l'entreprise.

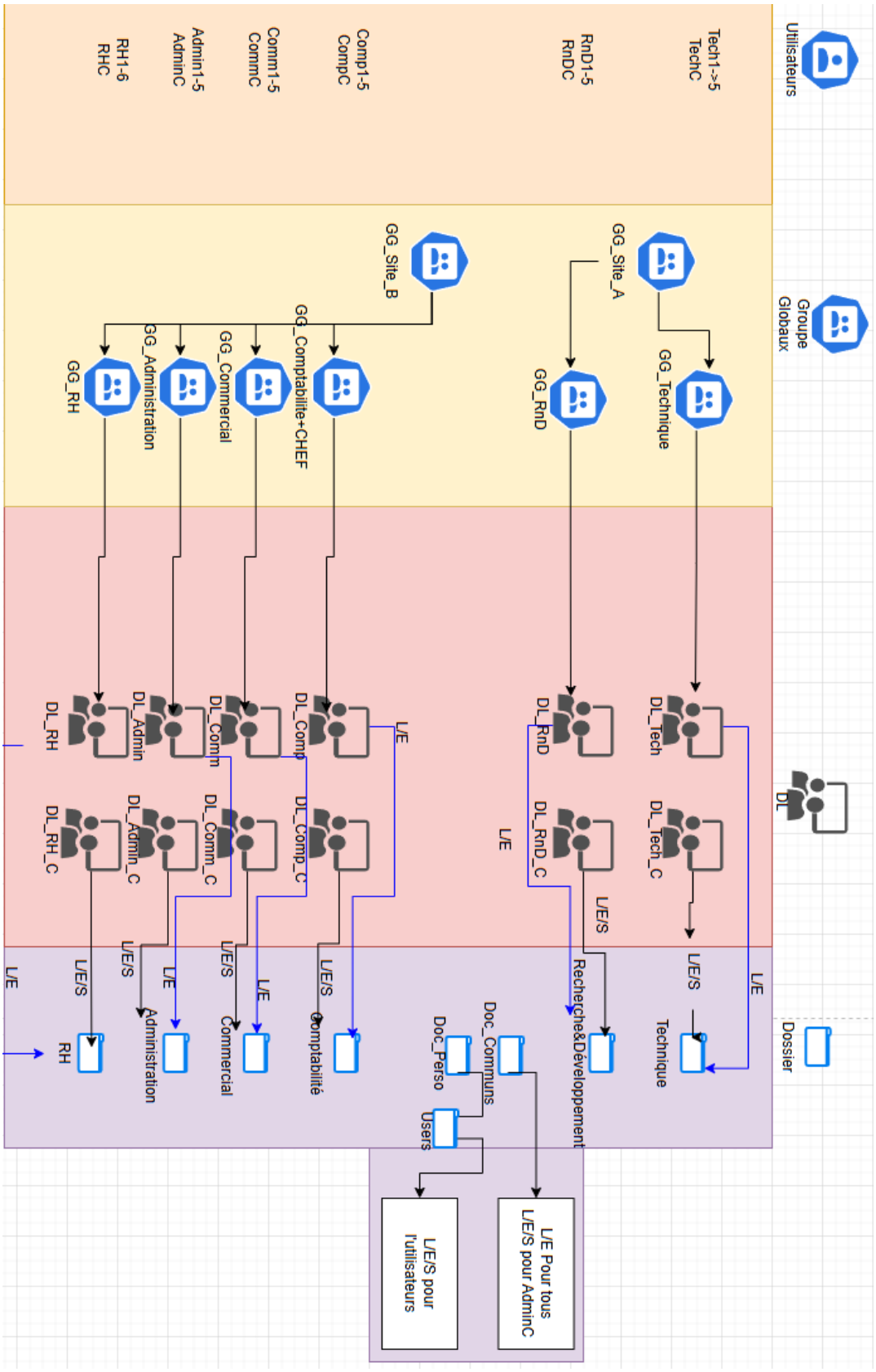
L'AD sera donc retenu grâce à sa facilité d'administration (GUI intégré et non pas en outils tiers ; ainsi que GPO).

Plan d'adressage et schéma AD

	Adresse	Mask	Passerelle	Interface
SR1	172.28.1.0	/24		172.28.1.1
SR2	172.28.2.0	/24		172.28.2.1
AD1+DNS1	172.28.1.2	/24	172.28.1.1	
AD2+DNS2	172.28.2.2		172.28.2.1	
Clients	Adresse dynamique	/24	Selon SR	



Voici le schéma de l'organisation de l'AD :



Etude de l'impact sur le SI existant

La mise en place d'un service d'annuaire type AD aura des impacts :

Techniques : l'AD va permettre la centralisation de la gestion des utilisateurs, des ordinateurs et ressources au sein du domaine, ce qui **simplifie** ladite gestion. De plus il va participer au renforcement de la **sécurité** du système informatique, via **le protocole d'authentification** Kerberos.

Organisationnels : en simplifiant l'administration des **utilisateurs et leurs droits**, ainsi que leur accès. De plus cela permet de faciliter l'instauration d'une architecture d'**accès aux ressources** avec des **droits NTFS.**

Humaines : La mise en place d'un service d'annuaire et redondant est une solution complexe nécessitant une **réflexion en amont** ainsi que des compétences particulières pour l'administrer.

Phasage de l'intervention

1) Installation des VMs : PareFeu, deux Windows serveur 2025 et deux clients Windows 10.
2) Mise en place du PareFeu PfSense
    a. Interface Wan
    b. Interface Lan 1 et plage DHCP
        i. Interface : 172.28.1.1/24
        ii. Plage DHCP : 172.28.1.10 – 172.28.1.253
    c. Interface Lan 2 et plage DHCP
        i. Interface : 172.28.2.1/24
        ii. Plage DHCP : 172.28.2.10 – 172.28.2.253
    d. Paramétrage règles PareFeu pour autoriser les protocoles nécessaires
        i. ICMP pour les tests entre LAN 1 et LAN 2
        ii. Port 636 et 389
    e.
    f. **TEST :**
        i. Sur clients Windows : ipconfig /all pour vérifier la bonne attribution d'une configuration DHCP
        ii. Sur clients Windows : ping client1 vers client2 et inversement pour s'assurer du bon fonctionnement du routage (celui-ci ne devrait pas poser un problème, les deux sous réseaux étant direct, le routage est donc automatique, si problème chercher côté règles de parefeu ou configuration ip des clients).
3) Installation DNS et son redondant

   a. Penser à paramétrer les adresses DNS sur le pfsense
   b. TEST :
      i. Sur Windows client 1 & 2 : bon fonctionnement du DNS1
         1. Nslookup Ads02.mysocvct.fr
      ii. Sur Windows client 1 & 2 : bon fonctionnement du DNS redondant
         1. Désactiver service DNS sur Windows Server 1
         2. Ping Ads01.mysocvct.fr
4) Installation AD et son redondant
5) Création de l'arborescence sur l'AD
   a. Utilisateurs
   b. Groupes globaux
   c. Groupes locaux
6) Politique de sécurité des mots de passe sur l'AD
   a. Test des politiques de mot de passe
7) Création des ressources (dossiers partagés)
8) Gestion des droits d'accès selon demande du TP
   a. Test des accès aux ressources, permission sur celle-ci.
9) Mise en place des GPO
   a. Test des gpos

Prévision des tests :

1) Test du DHCP
2) Test du routage et communication icmp
3) Test DNS
4) Test de connexion à des sessions utilisateurs AD
   a. Vérification des politiques de mot de passe (12 caractères, changement à la première authentification)
5) Vérification de l'accès aux ressources partagées
   a. Accès selon deux profil utilisateurs pour vérifier les permissions NTFS
6) Vérification des GPO

Déploiement

Le premier TP de 8h permettra la mise en place des VMs, du parefeu, des deux DNS, et un AD.

Sur les deux derniers TP de 4h : mise en place de l'AD redondant et administration de celui-ci selon les consignes.

Mise en place

1) Mise en place du PareFeu PfSense
    a. Configuration des interfaces

```
WAN (wan)       -> em0        -> v4/DHCP4: 192.168.1.32/24
LAN (lan)       -> em1        -> v4: 172.28.1.1/24
OPT1 (opt1)     -> em2        -> v4: 172.28.2.1/24
```

    b. Configuration DHCP

Primary Address Pool

Subnet	172.28.1.0/24	LAN 1
Subnet Range	172.28.1.1 - 172.28.1.254	
Address Pool Range	172.28.1.10 (From)	172.28.1.253 (To)

Primary Address Pool

Subnet	172.28.2.0/24	LAN 2
Subnet Range	172.28.2.1 - 172.28.2.254	
Address Pool Range	172.28.2.10 (From)	172.28.2.253 (To)

DNS Servers	172.28.1.2	
	172.28.2.2	LAN 1 + 2
	8.8.8.8	

    c. Paramétrage règles PareFeu pour autoriser les protocoles nécessaires

Floating | WAN | LAN | OPT1 — SUR LAN 1 & 2 (opt1)

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✓	3/230 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule
✓	30/1.39 GiB	IPv4 *	*	*	*	*	*	none		Default allow LAN to any rule

2) TEST :

a. Sur clients Windows : ipconfig /all pour vérifier la bonne attribution d'une configuration DHCP

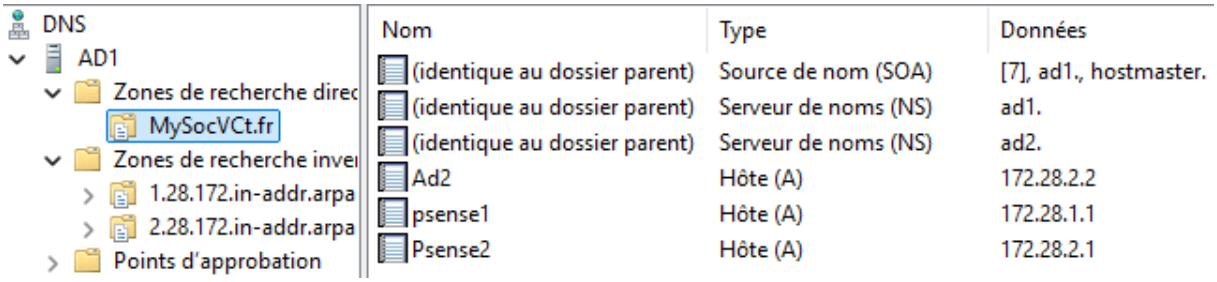
```
Suffixe DNS propre à la connexion. . . : home.arpa
Description. . . . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
Adresse physique . . . . . . . . . . . : 00-0C-29-F9-45-EC
DHCP activé. . . . . . . . . . . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . .: fe80::9dfd:d737:9208:7f01%9(préféré)
Adresse IPv4. . . . . . . . . . . . . .: 172.28.1.10(préféré)
Masque de sous-réseau. . . . . . . . . : 255.255.255.0
Bail obtenu. . . . . . . . . . . . . . : vendredi 10 octobre 2025 17:17:02
Bail expirant. . . . . . . . . . . . . : vendredi 10 octobre 2025 19:17:02
Passerelle par défaut. . . . . . . . . : 172.28.1.1
Serveur DHCP . . . . . . . . . . . . . : 172.28.1.1
IAID DHCPv6 . . . . . . . . . . . : 100666409
DUID de client DHCPv6. . . . . . . . : 00-01-00-01-30-79-9F-FF-00-0C-29-F9-45-EC
Serveurs DNS. . .  . . . . . . . . . . : 172.28.1.2
                                172.28.2.2
                                8.8.8.8
```

b. Sur clients Windows : ping client1 vers client2 et inversement pour s'assurer du bon fonctionnement du routage (celui-ci ne devrait pas poser un problème, les deux sous réseaux étant direct, le routage est donc automatique, si problème chercher côté règles de parefeu ou configuration ip des clients).

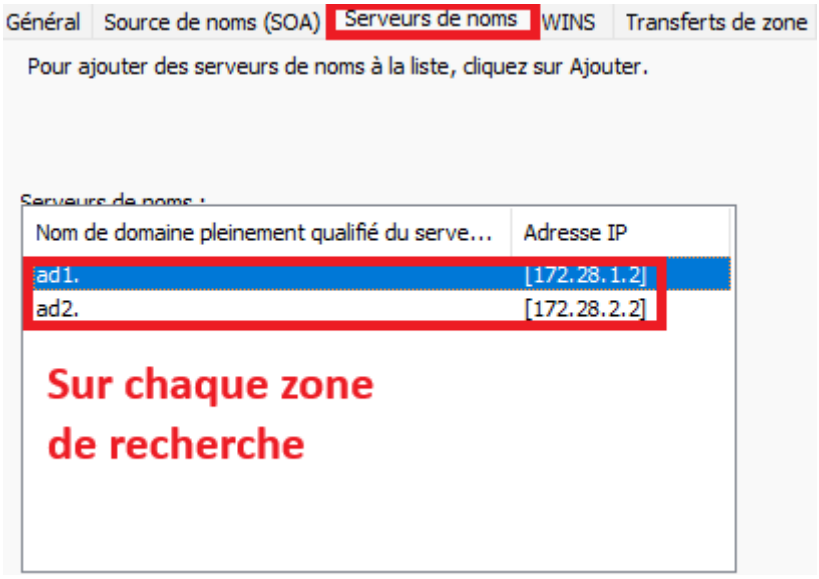
```
C:\Users\W10AD2>ping 172.28.1.10

Envoi d'une requête 'Ping'  172.28.1.10 avec 32 octets de données
Réponse de 172.28.1.10 : octets=32 temps<1ms TTL=127
Réponse de 172.28.1.10 : octets=32 temps<1ms TTL=127
Réponse de 172.28.1.10 : octets=32 temps<1ms TTL=127
```

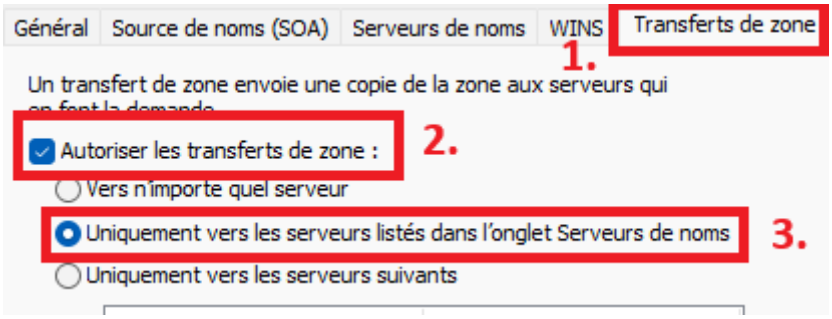
3) Installation DNS et son redondant

a. Configuration des RR

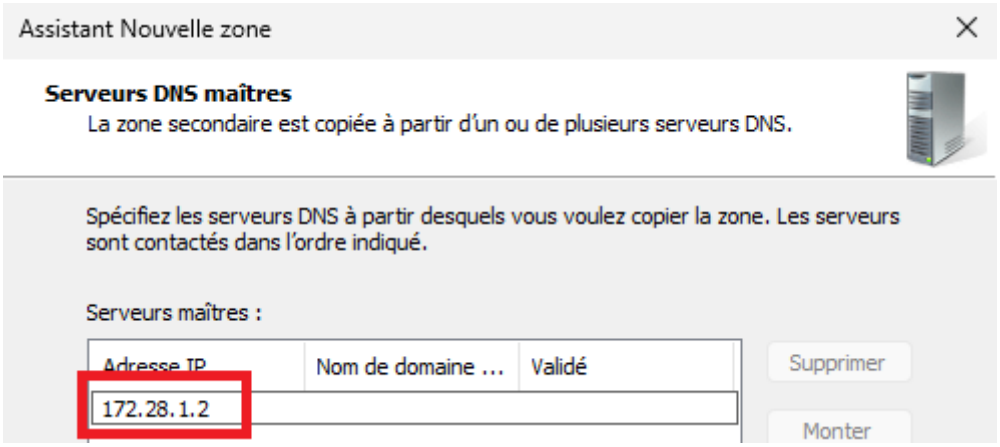


b. Configuration redondance





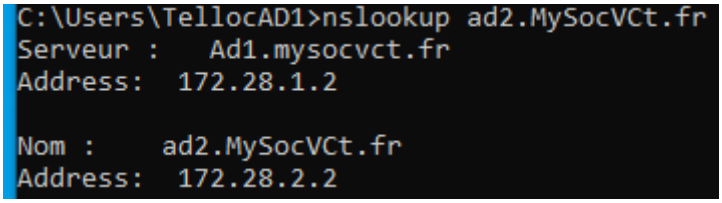
c. Configurer des **nouvelles zones secondaires** sur le serveur redondant



d. TEST :

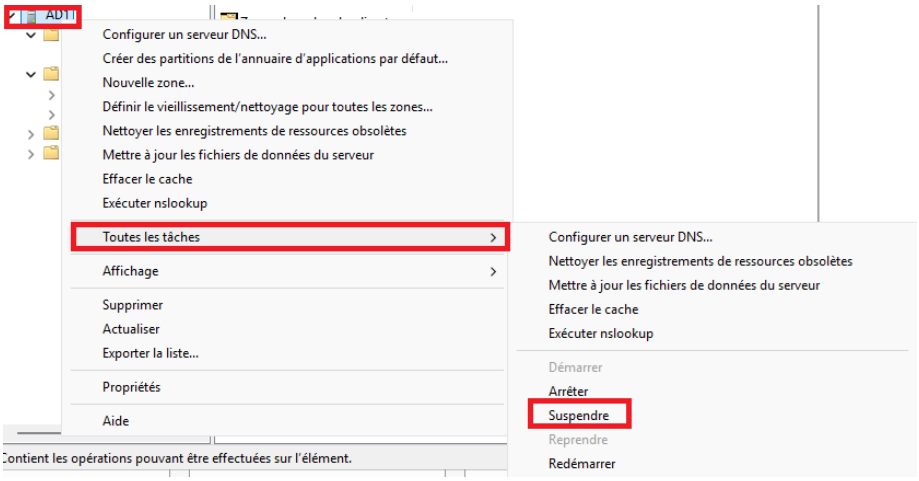
i. Sur Windows client 1 & 2 : bon fonctionnement du DNS1

1. Nslookup Ad2.mysocvct.fr



ii. Sur Windows client 1 & 2 : bon fonctionnement du DNS redondant

1. Désactiver service DNS sur Windows Server 1



2. Ping Ad1.mysocvct.fr (ping FQDN)

```
C:\Users\TellocAD1>ipconfig /flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.

C:\Users\TellocAD1>ping ad1.mysocvct.fr

Envoi d'une requête 'ping' sur ad1.mysocvct.fr [172.28.1.2] avec 32 octets de données :
Réponse de 172.28.1.2 : octets=32 temps<1ms TTL=128
Réponse de 172.28.1.2 : octets=32 temps<1ms TTL=128
Réponse de 172.28.1.2 : octets=32 temps<1ms TTL=128
Réponse de 172.28.1.2 : octets=32 temps<1ms TTL=128
```

```
C:\Users\TellocAD1>nslookup ad1.mysocvct.fr 172.28.2.2
Serveur :   UnKnown
Address:  172.28.2.2

Nom :    ad1.mysocvct.fr
Address:  172.28.1.2
```

4) Installation AD et son redondant

a. Installer le rôle AD DS

Via powershell : Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

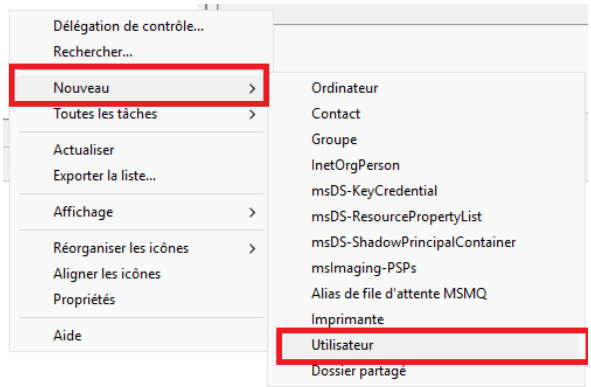
Redémarrer le serveur

b. Promouvoir le serveur en contrôleur de domaine AD DC

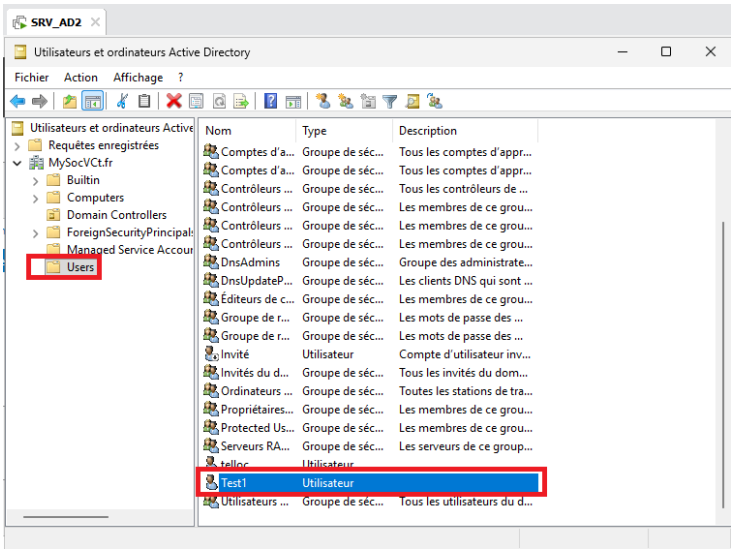
Via powershell : Install-ADDSForest -DomainName "MySocVCt.fr" -SafeModeAdministratorPassword (ConvertTo-SecureString "yourpassword" -AsPlainText -Force)

c. Test du bon fonctionnement redondance :

Je crée un utilisateur sur AD1 pour voir s'il est créé sur AD2 aussi : Clic droit dans **Utilisateurs et ordinateurs Active Directory** puis :



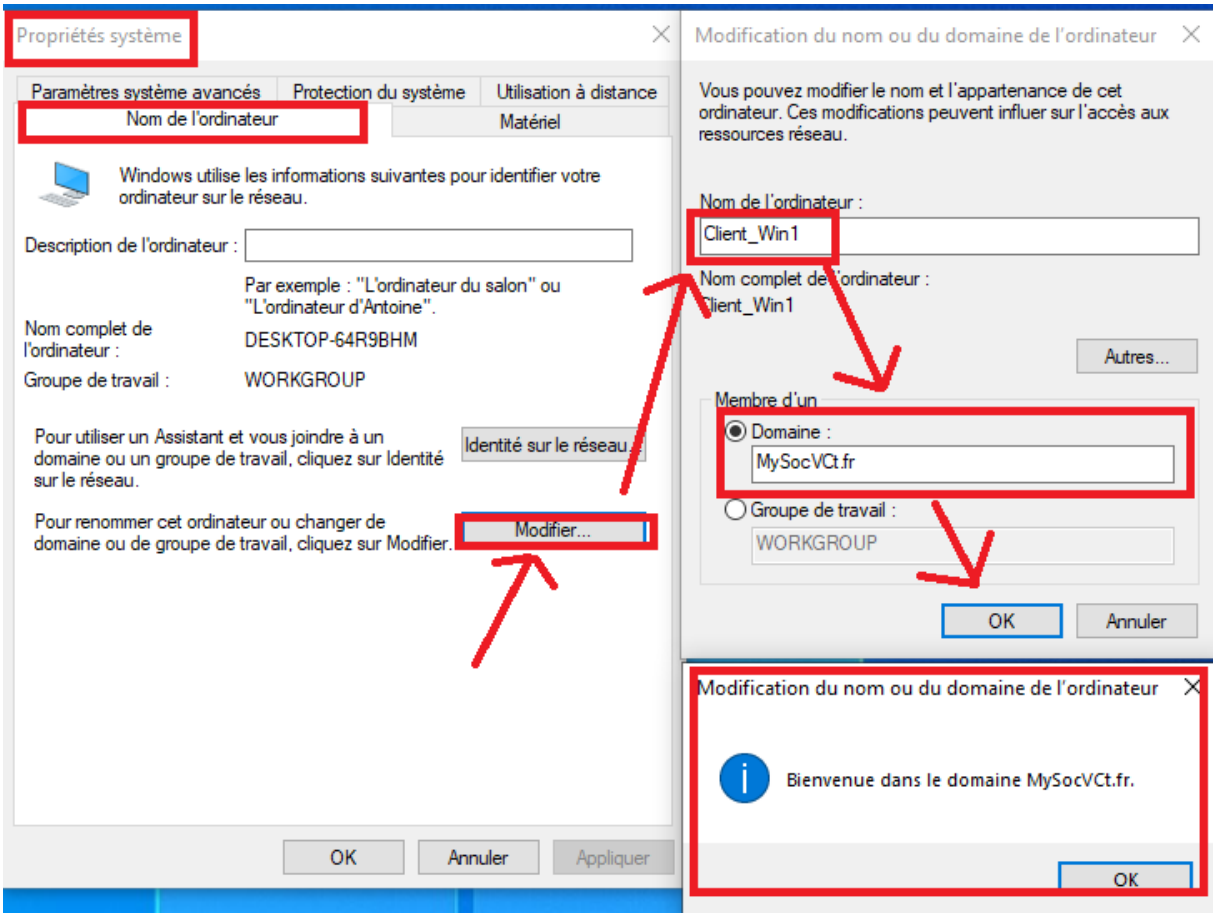
L'utilisateur Test s'appellera **Test1**, il réplique bien sur AD2 :



Puis, avec une commande PowerShell vérifier s'il y a des erreurs :

```
PS C:\WINDOWS\system32> repadmin /replsummary
Heure de début du résumé de la réplication : 2025-10-11 11:38:04

Début de la collecte des données pour le résumé de la réplication ;
cette opération peut prendre un certain temps :
  .....


DSA source              différence max    nb échecs %%   erreur
 AD1                        08m:45s    0 /   5    0
 AD2                        18m:37s    0 /   5    0


DSA de destination      différence max    nb échecs %%   erreur
 AD1                        18m:38s    0 /   5    0
 AD2                        08m:46s    0 /   5    0
```

5) Jonction poste Windows clients au domaine :



6) Création de l'arborescence sur l'AD
    a. Utilisateurs

Comme avec Test1, créer tous les Users selon tous les services :

, etc...

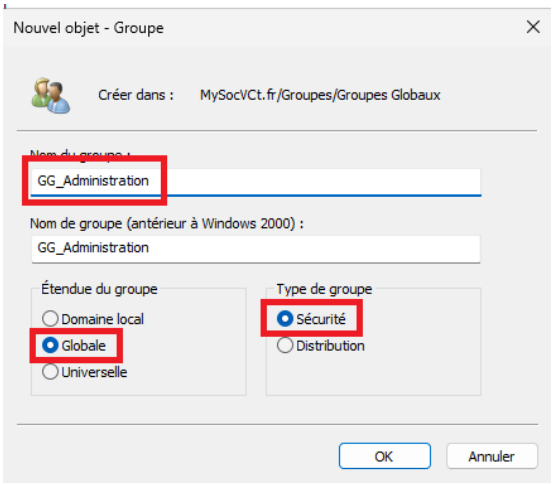
    b. Groupes globaux

Créer OU groupes globaux pour l'organisation, puis dedans :

Clic droit > nouveau > groupe

La convention sera :

1) GG_<Service>
2) GG_<Sercice>_Chef



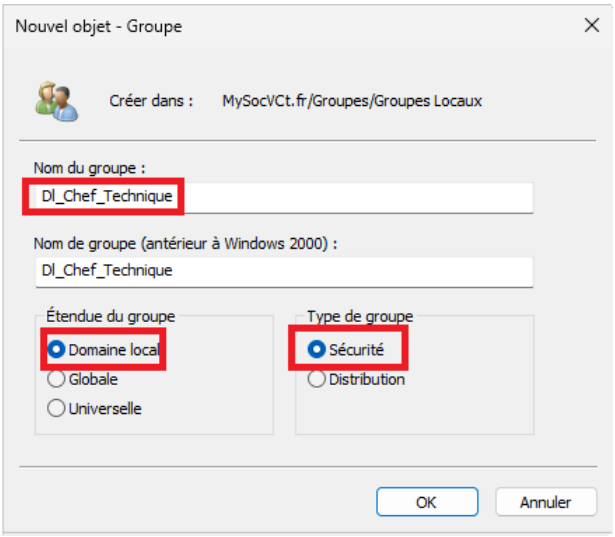
Ex :

GG_Administration	Groupe de sécurité - Global
GG_Administration_Chef	Groupe de sécurité - Global
GG_Commercial	Groupe de sécurité - Global
GG_Commercial_Chef	Groupe de sécurité - Global
GG_Comptabilite	Groupe de sécurité - Global
GG_Comptabilite_Chef	Groupe de sécurité - Global
GG_RD	Groupe de sécurité - Global
GG_RD_Chef	Groupe de sécurité - Global
GG_RH	Groupe de sécurité - Global
GG_RH_Chef	Groupe de sécurité - Global
GG_Technique	Groupe de sécurité - Global
GG_Technique_Chef	Groupe de sécurité - Global

c. Groupes locaux (DL)

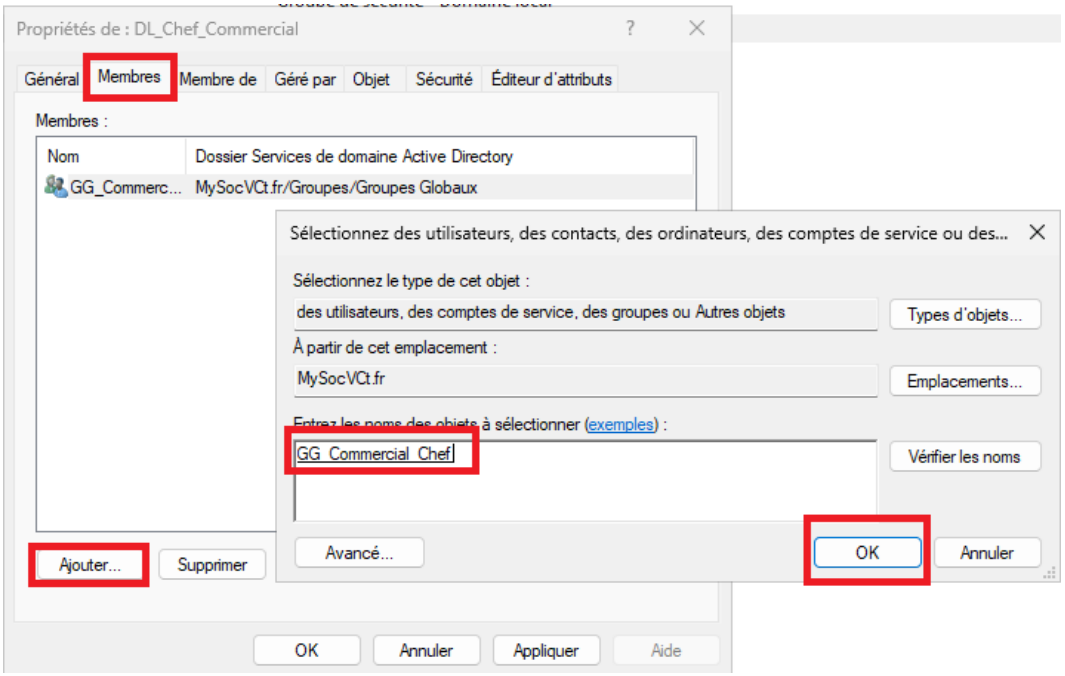
Comme précédemment, avec une convention :

3) DL_Chef_<Service>
4) DL_<Service>

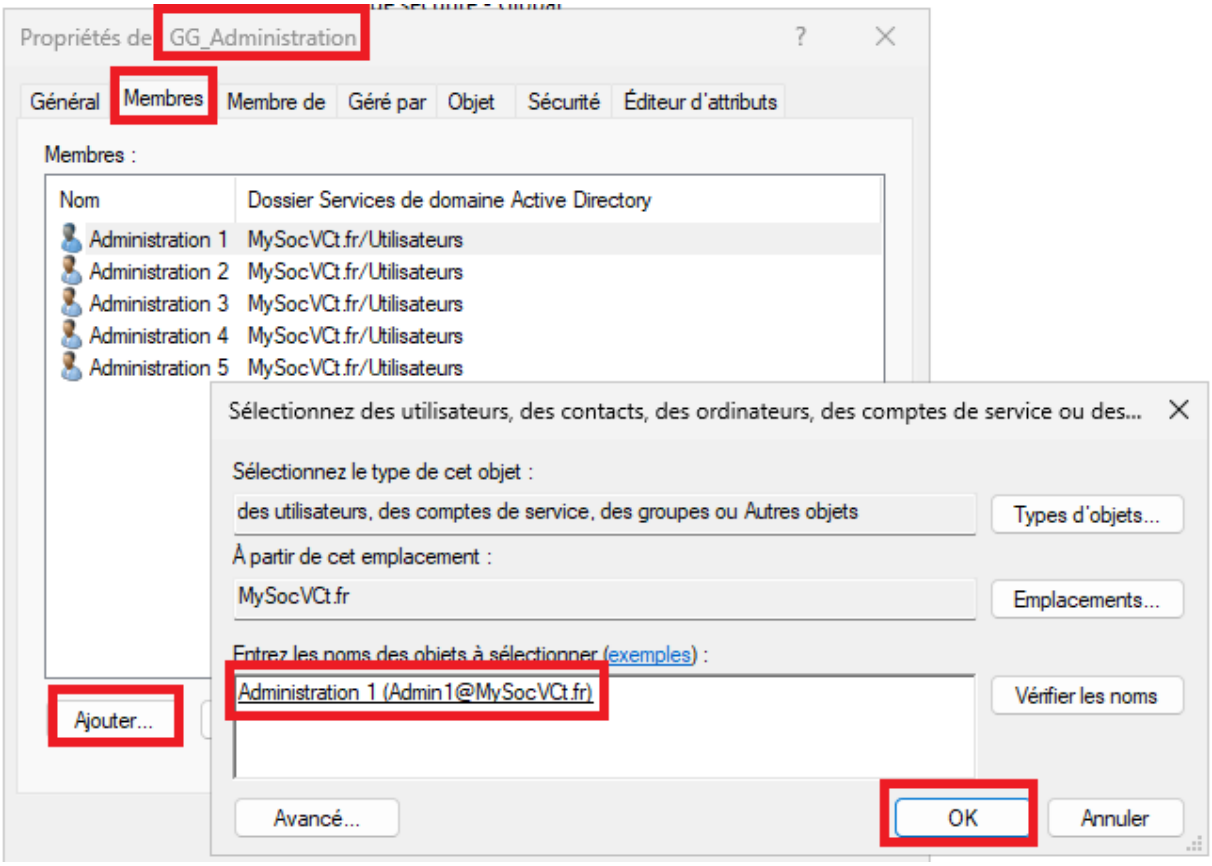


d. Attribution membre DL : groupes globaux de sécurité

Ici il faut attribuer les groupes globaux en tant que **membre** au groupe locaux.



e. Attribution utilisateurs dans Groupes globaux



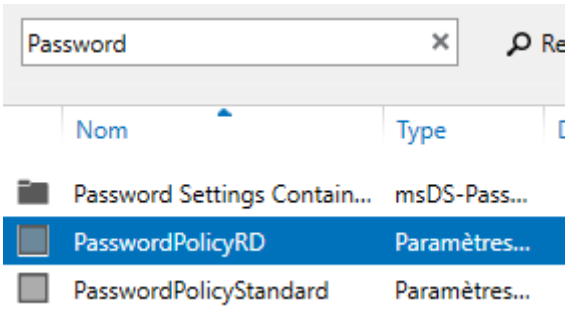
7) Politique de sécurité des mots de passe sur l'AD

J'utilise PowerShell pour créer deux PasswordPolicies :

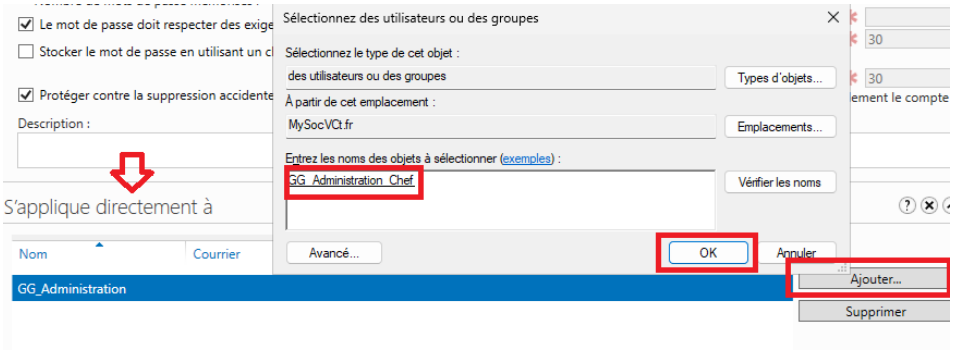
```
$policyParams = @{
  Name = "PasswordPolicyStandard"
  ComplexityEnabled = $true
  LockoutDuration = "00:30:00"
  LockoutObservationWindow = "00:30:00"
  LockoutThreshold = "0"
  MaxPasswordAge = "31.00:00:00"
  MinPasswordAge = "1.00:00:00"
  MinPasswordLength = "7"
  PasswordHistoryCount = "24"
  Precedence = "1" #PRIORITE SUR LES AUTRES
  ReversibleEncryptionEnabled = $false
  ProtectedFromAccidentalDeletion = $true
New-ADFineGrainedPasswordPolicy @policyParams
```

Il en faut une pour le service R&D et une pour le reste.

Puis il faut ajouter les groupes nécessaires dans les password policies sur le **centre d'administration AD :**



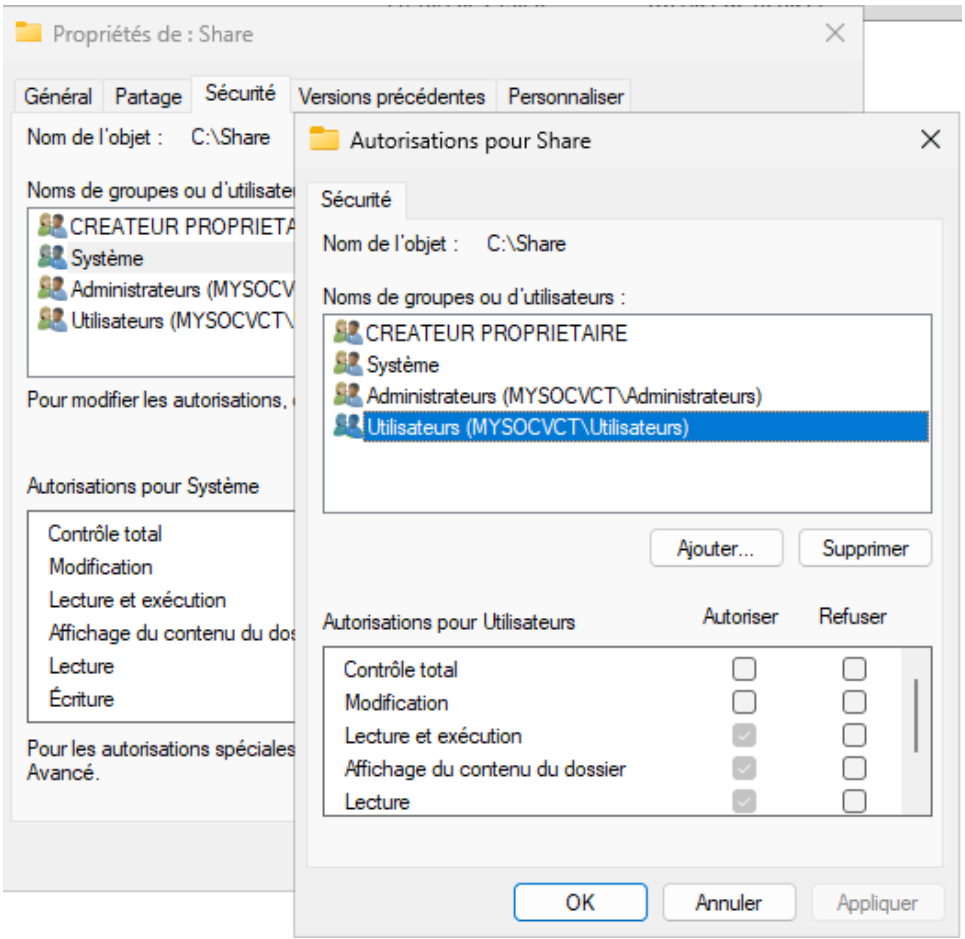
Sur **PasswordpolicyStandard** :Clic droit dessus > S'applique directement à + Ajouter :



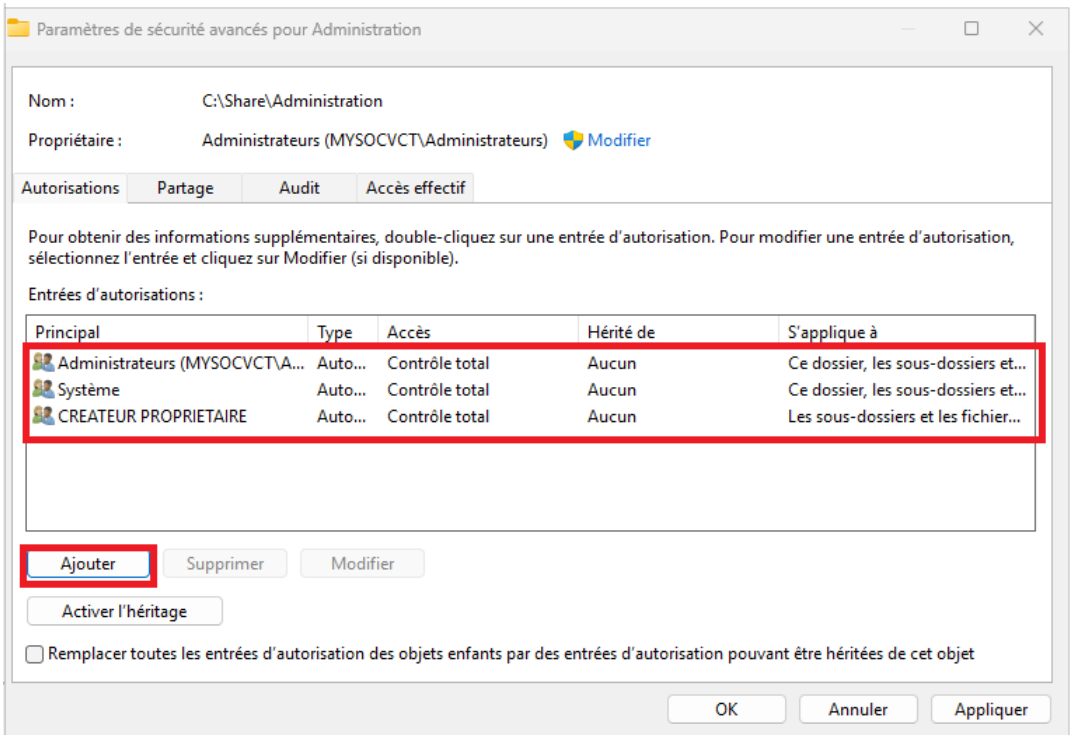
Faire ceci pour tous les GG sauf RD, puis répéter l'opération sur **PasswordPolicyRD** pour les GG_RD et GG_RD_Chef

8) Création des ressources (dossiers partagés) services

Je crée donc un dossier partage à la racine C:\ via **compmgmt > outils système > dossiers partagés > partages**

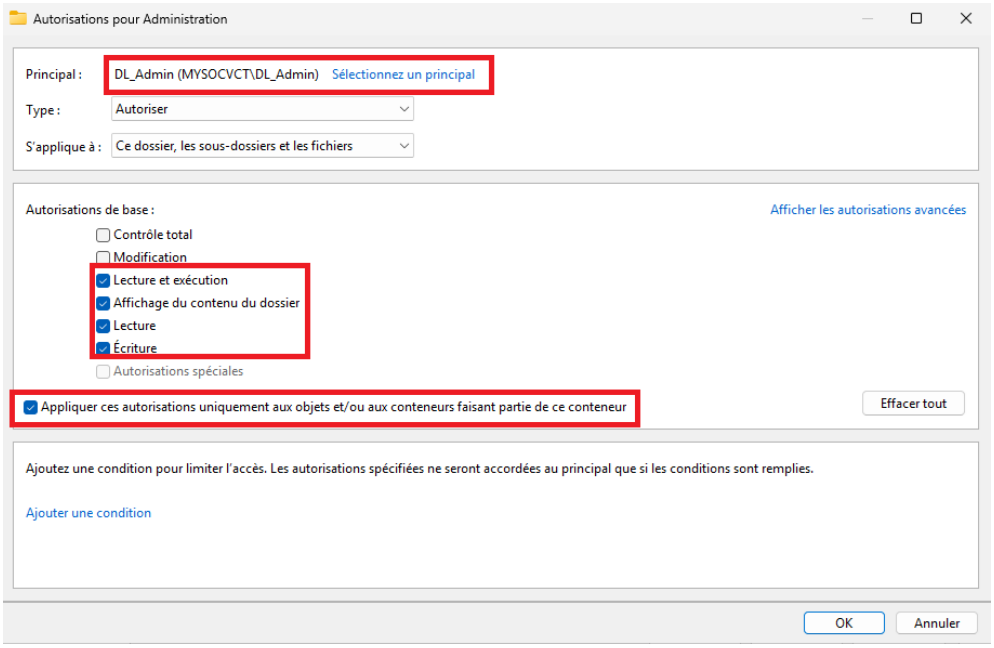


Désactiver l'héritage des permissions sur les dossiers: Cliquer droit sur le dossier > Propriétés > Sécurité > Avancé > Désactiver l'héritage > Convertir les permissions héritées en permissions explicites.

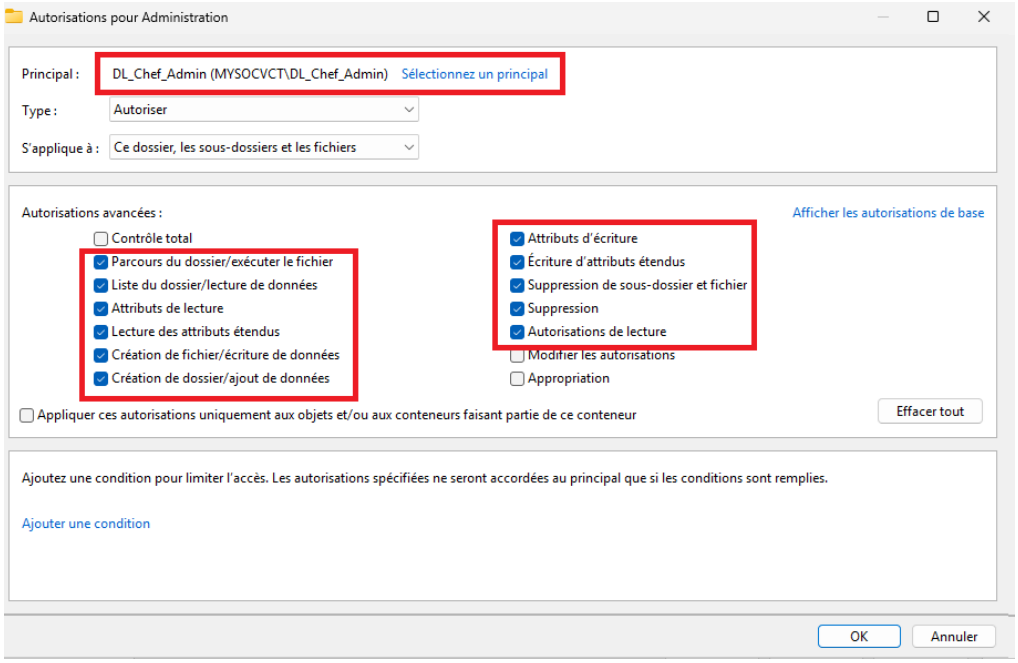


Puis pour chaque **dossier service** y ajouter le **DL_<Service>** Correspondant en gérant les autorisations

/ ! \ Penser à cocher **« Appliquer ces autorisations… »** pour que les utilisateurs du groupe puissent **supprimer leurs propres objets**

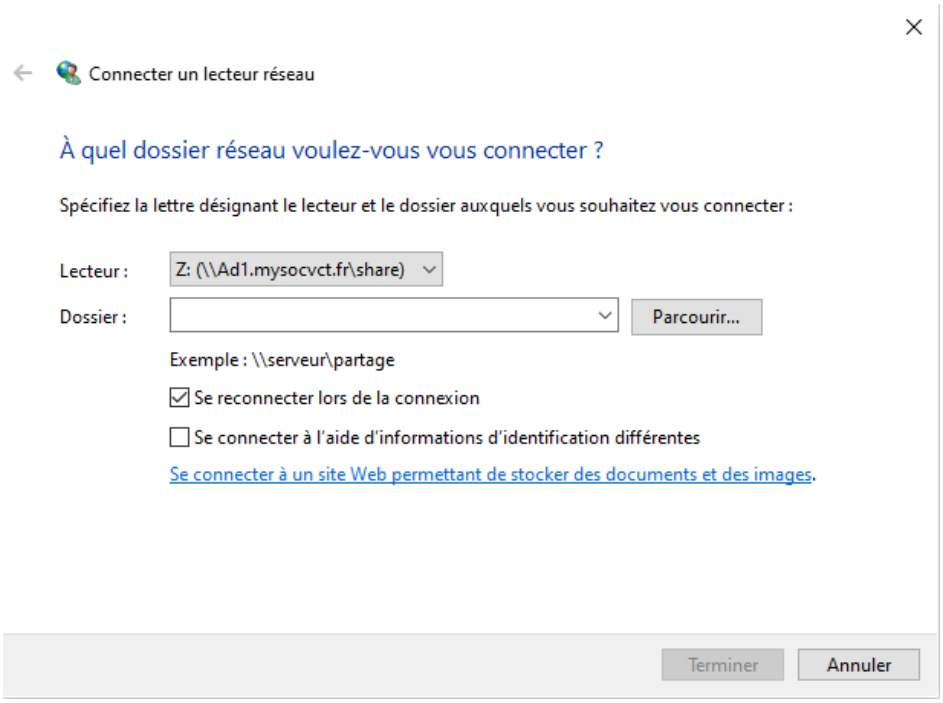


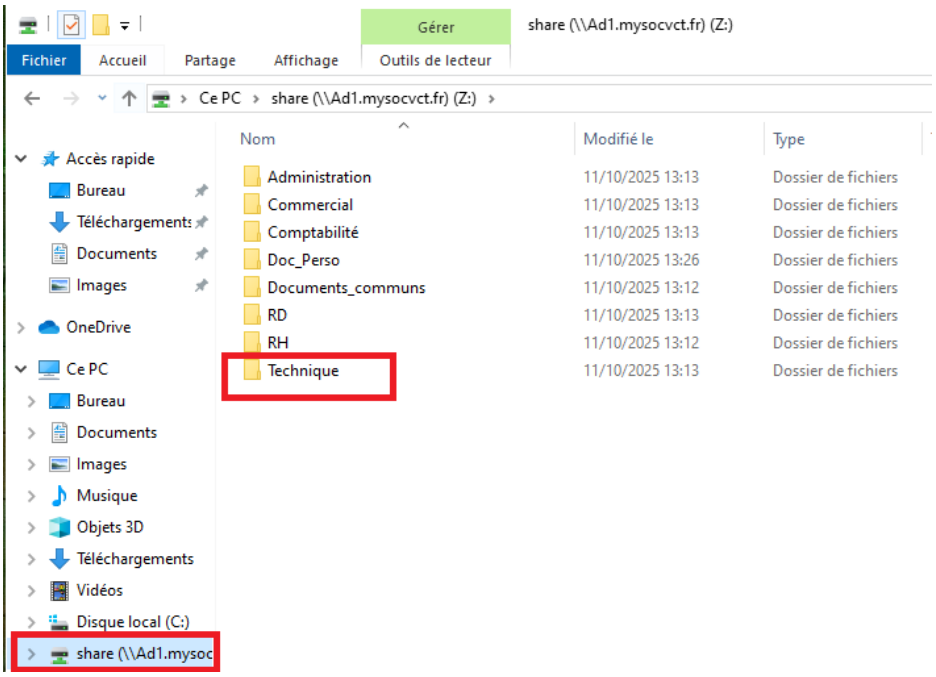
Puis pour le **chef** :



9) Test

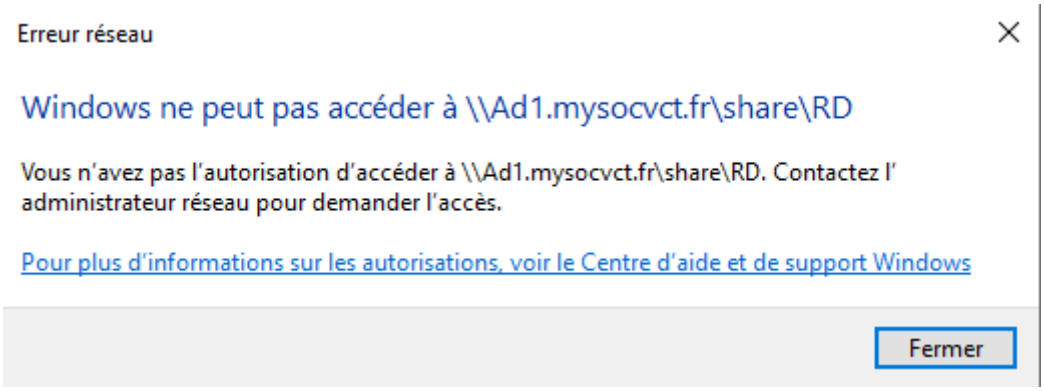
Connecter un lecteur réseau sur client Windows (par exemple Tech1)



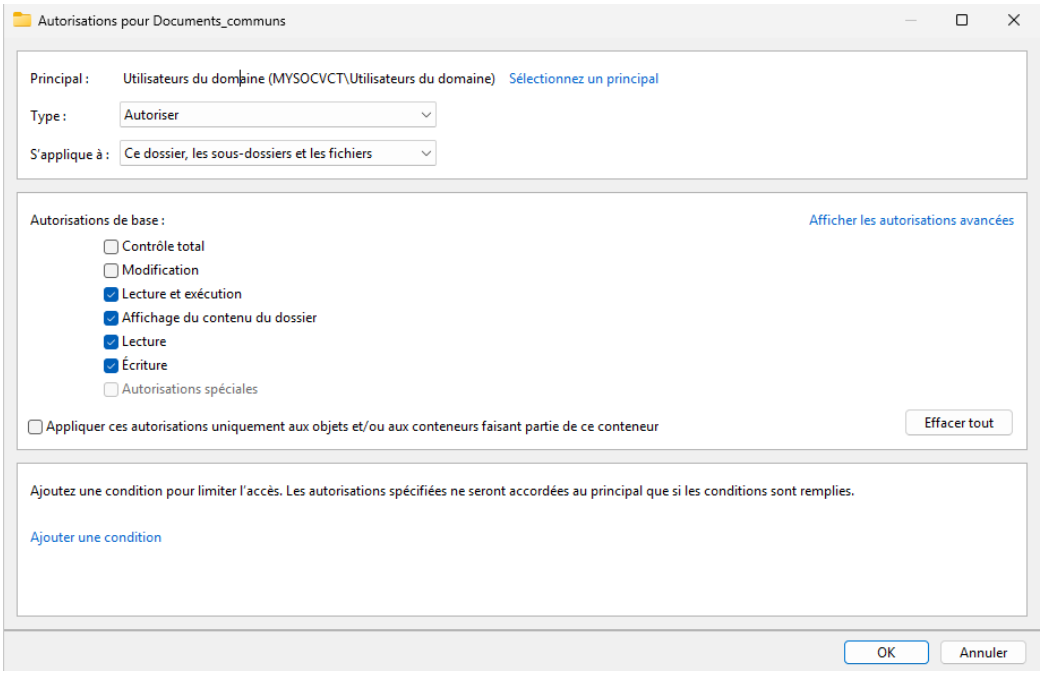


Vérifier l'accès au dossier technique : OK.

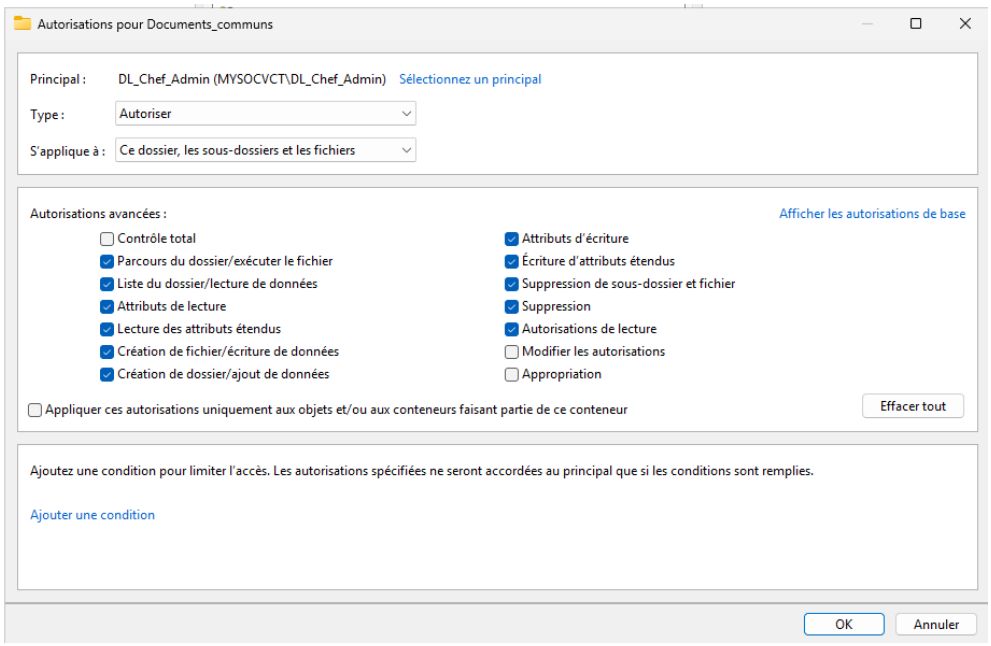
Vérifier l'accès aux autres dossiers services : NON :



10) Création des partages Documents communs



Puis pour chef_admin :

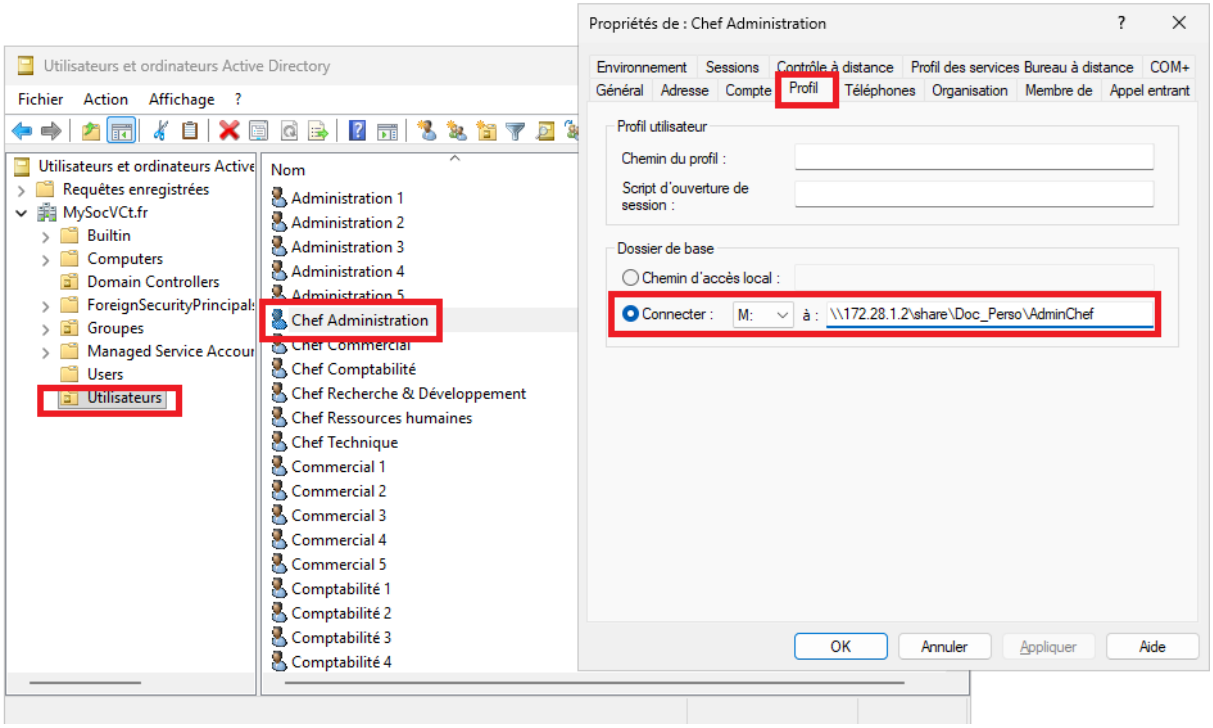


11) TEST doc communs

Accéder au dossier <Service> avec un membre de GG_<Service correspondant> puis, vérifier si les autres services renvoient bien une erreur d'accès, puis créer un fichier et le **supprimer**. Vérifier que la suppression ne fonctionne pas sur un objet dont l'utilisateur n'est pas le créateur.

12) Partage des documents personnels

Pour cela :



13) Test doc perso

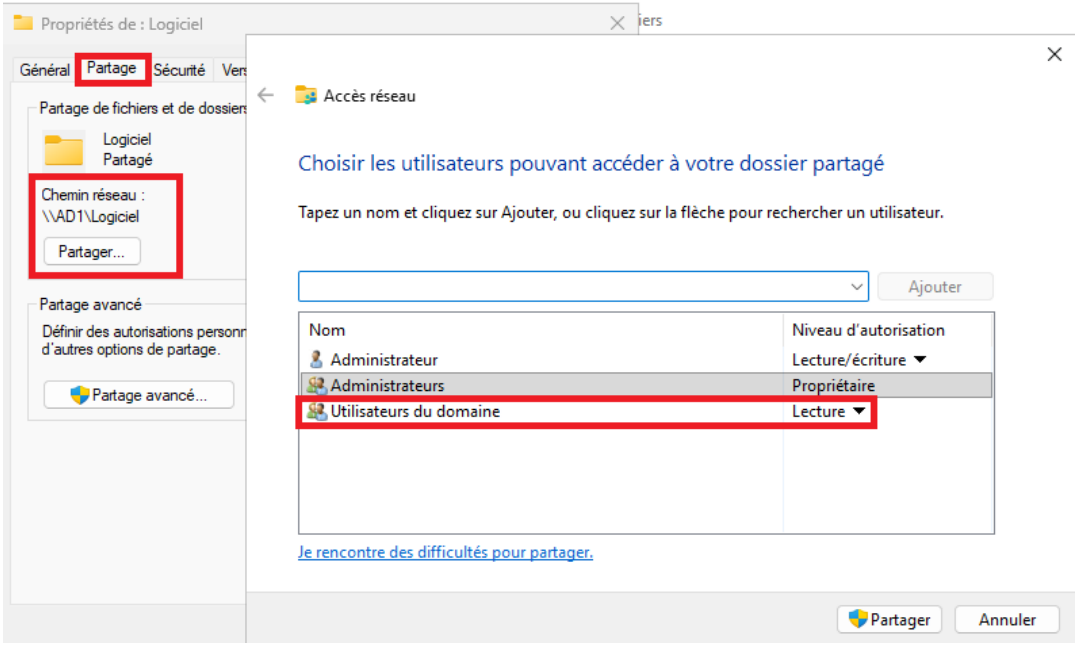
Essayer d'accéder au doc perso de l'utilisateur : OK, puis créer un fichier et le supprimer.

Vérifier que les autres sont inaccessibles.

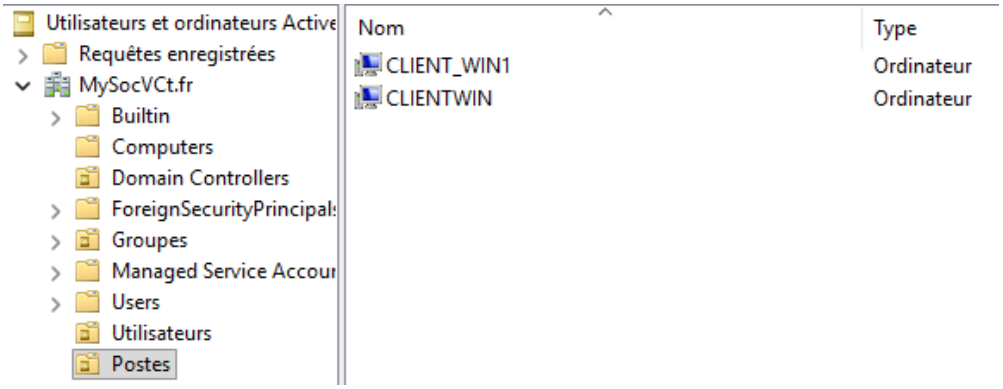
14) Mise en place des GPO

a. Firefox :

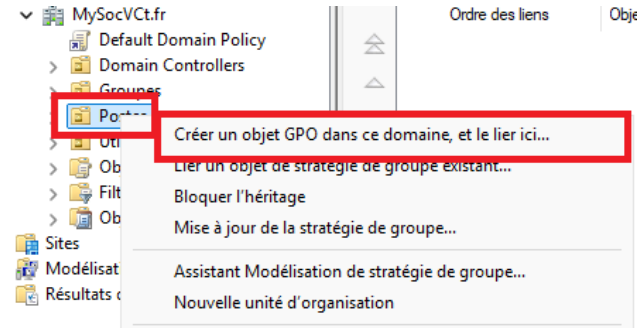
Je commence par créer un dossier partagé avec l'exe **.MSI** de **firefox** (version **ESR**)



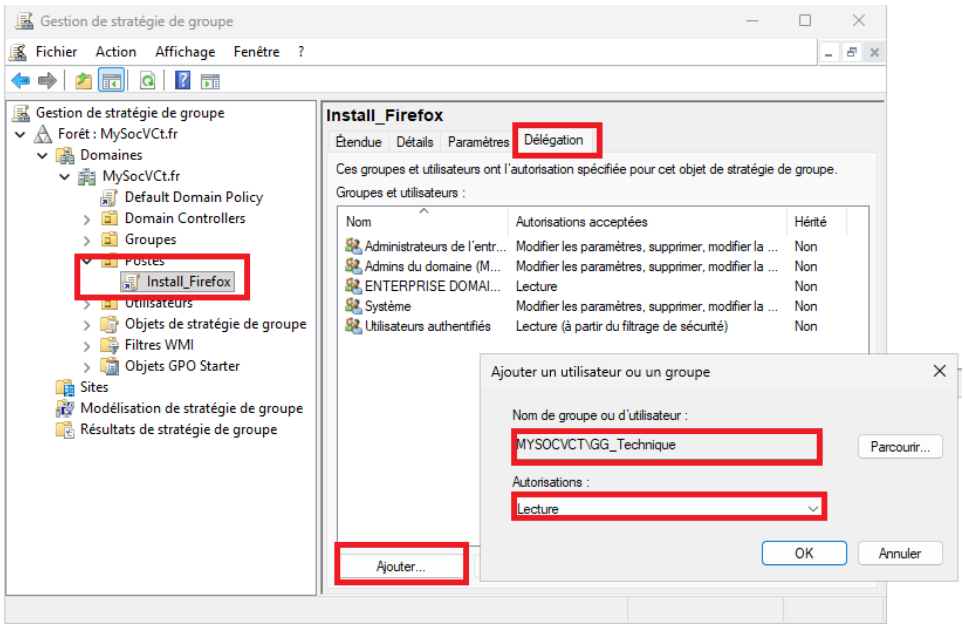
Puis, il faut créer une OU avec les postes dedans :

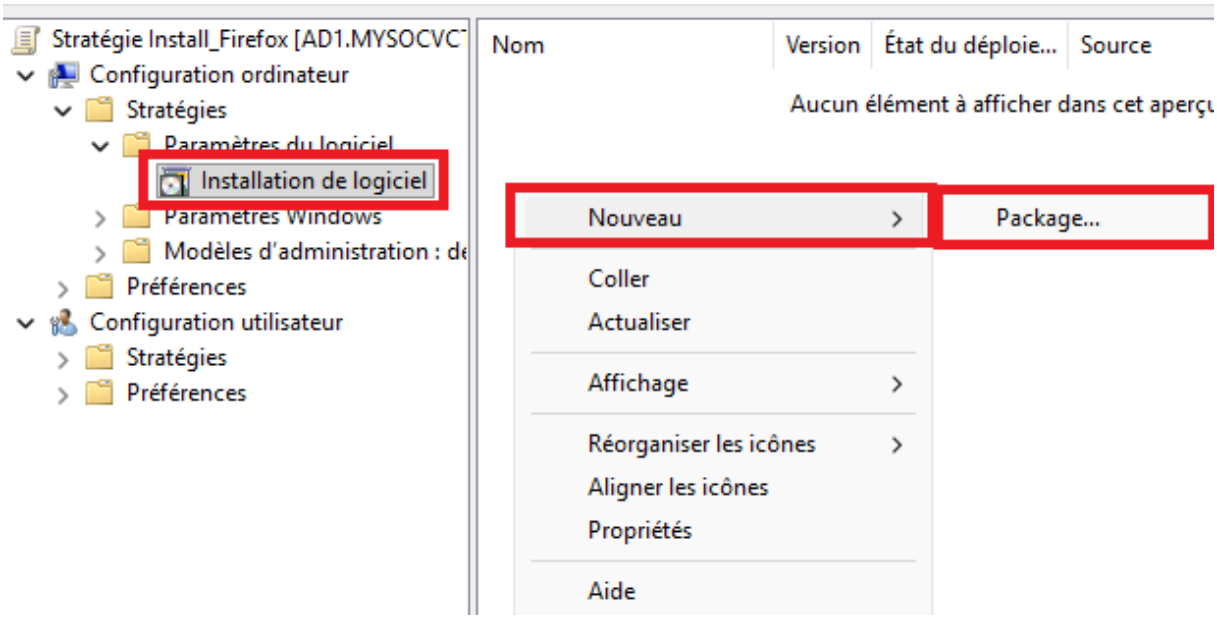


Enfin dans le **gestionnaire de stratégie de groupe :**

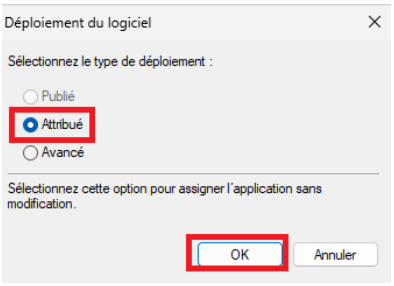


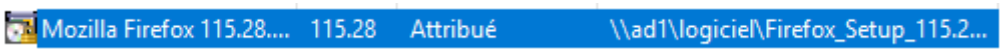
Il est aussi possible de le faire via GPO et tâche planifiée.





Puis sélectionner le .msi avec l'adresse réseau et :



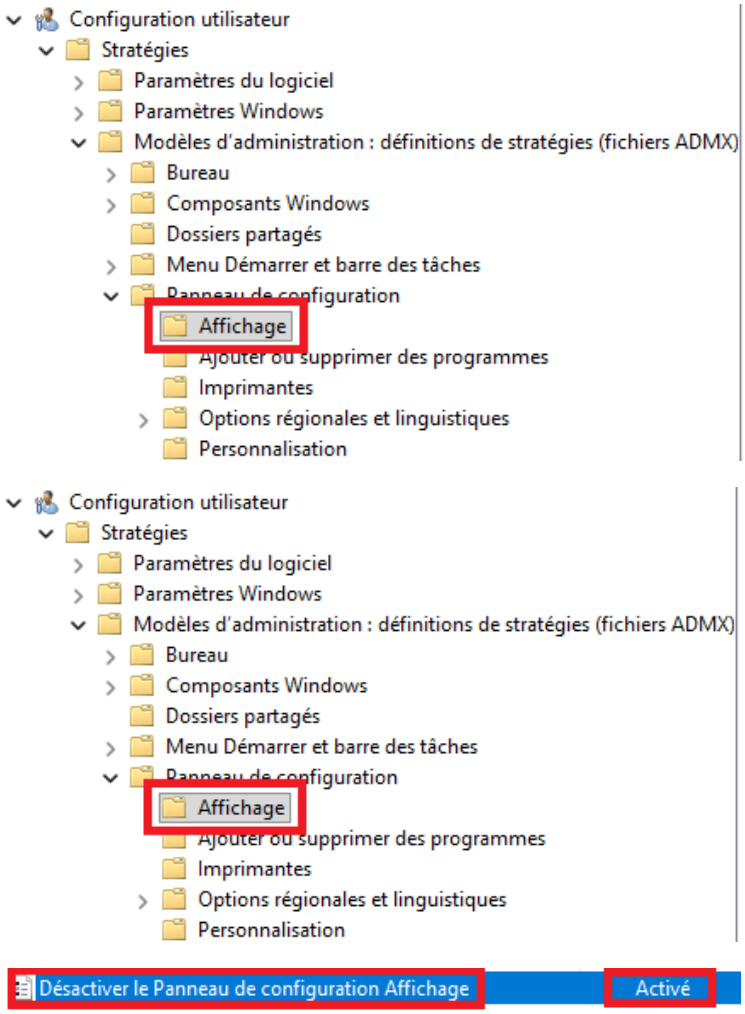


Pour tester la GPO :

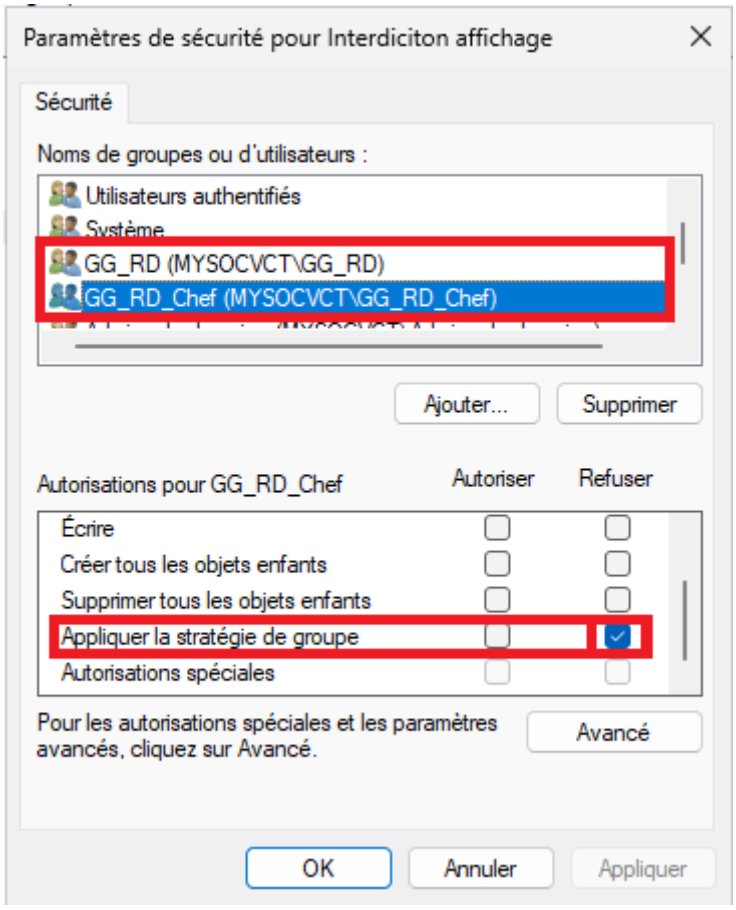
Sur un poste avec utilisateurs Tech1 : sur la cmd, taper gpupdate /force, pour mettre à jour les stratégies.

b. Interdiction de la modification de l'affichage

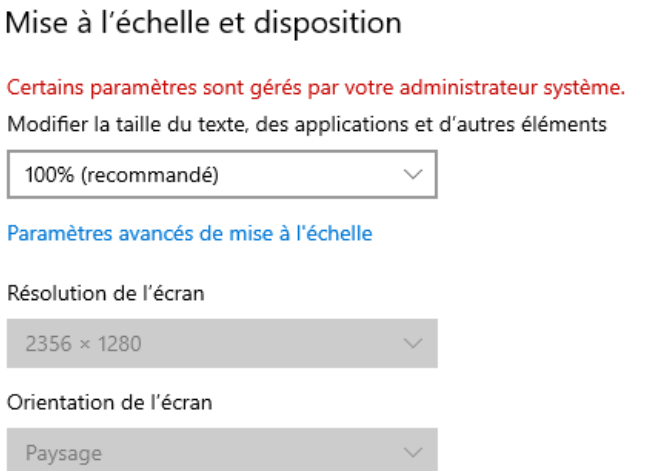
Toujours dans la mise à jour des stratégies, créer une nouvelle GPO, intitulée « Interdiction affichage », l'éditer :



Régler les groupes, afin que la GPO s'applique à tous sauf au service RD , pour cela dans l'onglet **délégation>avancé** de la GPO, ajouter les deux groupes RD avec le refus :

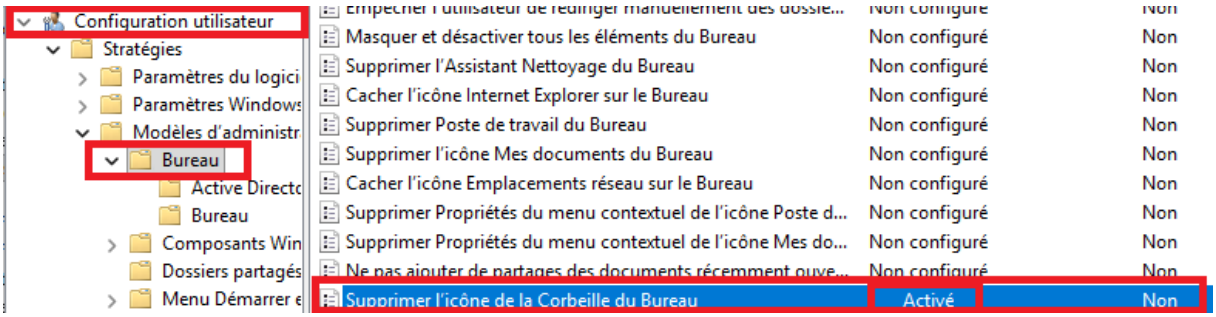


Pour tester, il suffit de faire un gpupdate /force et vérifier :

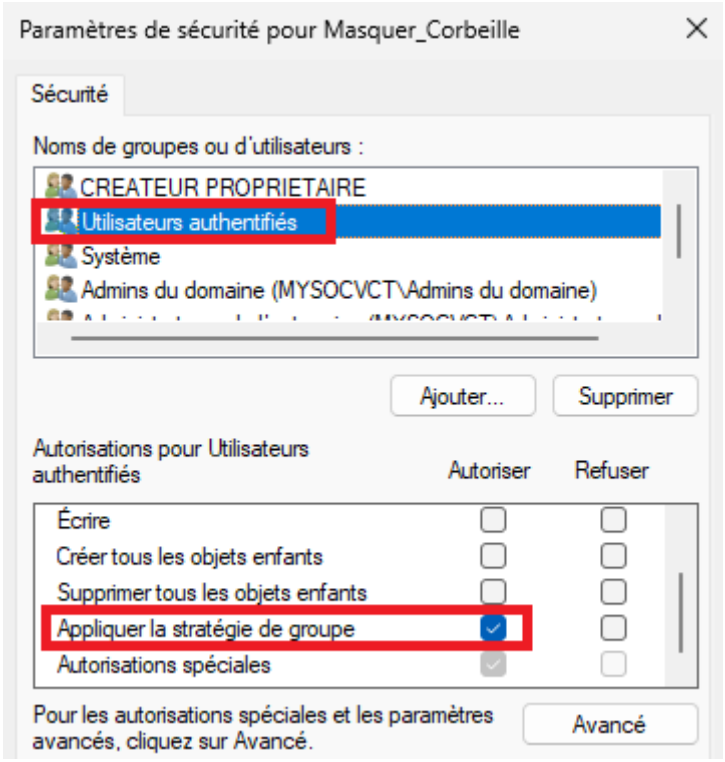


c. GPO pour masquer la corbeille

Pour cela toujours dans le gestionnaire de stratégie de groupe, créer une gpo sous l'OU utilisateurs intitulée : Masquer_Corbeille puis :



Vérifier au niveau des utilisateurs concernées :



Vérifier son bon fonctionnement après l'avoir activée avec un gpupdate /force sur un poste.

Rapport de tests

Les tests sont réalisés et documentés dans la procédure, en suivant l'ordonnancement du phasage de l'intervention.

Premièrement il s'agit de vérifier la bonne attribution des configuration DHCP et communications des intermédiaires au sein du réseau (ping). Ensuite, de s'assurer du bon fonctionnement du DNS et son redondant (via les commandes nslookup, et en réessayant via ping après avoir désactiver le service DNS du serveur 1).

Puis, les tests vont concerner la création des utilisateurs, la politique de mot de passe, et leurs accès à des ressources spécifiques. Et enfin, la bonne application des GPO.

Ces tests sont faits à l'aide de deux clients Windows 10.

Rapport de déploiement

Le déploiement s'est déroulé « sans accroc » avec la mise en place d'un serveur AD/DNS et redondant. Ce qui correspond à deux VM Windows serveur 2025.

Enfin celui-ci a une architecture d'AD (utilisateurs -> groupes de sécurité globaux -> groupe locaux -> ressources) et des règles GPO appliqués permettant l'administration des postes et des utilisateurs.

Bilan

Conclusion :

Cette procédure m'a permis d'améliorer ma maîtrise et mes connaissances à propos de l'Active Directory de manière générale mais aussi la création de dossiers partagés avec la gestion des permissions selon la méthode AGDLP, que j'ai pu m'approprier grâce à ce TD, tout comme les GPO.

Auto évaluation :

Je pense pouvoir m'améliorer sur l'organisation et la gestion du temps, malgré le loupé d'un TD de 4h, j'ai pu rattraper le travail de chez moi.