Préparation de l’environnent de test : Deuxième partie

1. Introduction

Dans cet mission, nous avons réalisé le déploiement d’une infrastructure système sous environnement virtualisé (Vmware), incluant un serveur Windows, un pare-feu pfSense et un client Windows. L’objectif est de mettre en place les services Active Directory, DHCP, DNS ainsi que la gestion des utilisateurs, des groupes et des partages réseau.

2. Maquettage sous VMware

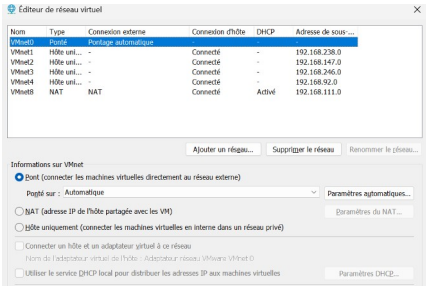
2.1 Configuration des réseaux

Les réseaux virtuels ont été configurés dans Vmware en associant chaque VLAN à un réseau vmnet distinct. Le réseau VMnet1 correspond au VLAN 10 (Serveurs), le réseau VMnet2 est associé au VLAN 20 (DMZ), le réseau VMnet3 correspond au VLAN 30 (Bureaux) et le réseau VMnet4 est dédié au VLAN 40 (Wifi_visiteurs). Un réseau supplémentaire en mode NAT (VMnet8) est utilisé pour fournir l’accès à Internet aux machines virtuelles. Cette correspondance permet de reproduire fidèlement la segmentation réseau définie dans l’architecture initiale.

Vmware → Modifier → Éditeur de réseau virtuel → Modifier le paramètres → Ajouter un réseau
Paramètres :

- Hôte uniquement
- Désactiver le service DHCP

On répète l’opération pour chaque "Vlan".

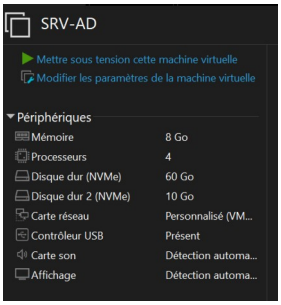


2.2 Création des machines virtuelles

Les machines virtuelles ont été créées avec les ressources nécessaires pour chaque rôle : serveur, pare-feu et client.

Installation du VM Windows Server

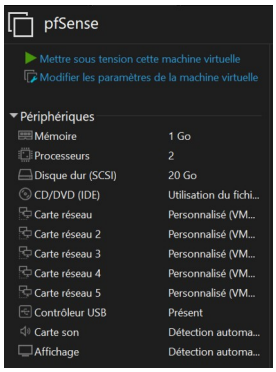
- Stockage : 60 go
- Stockage : 10 go
- Ram : 8 go
- Processeurs : 4
- Carte réseau : "Vlan Serveurs"



Installation du VM pFsense

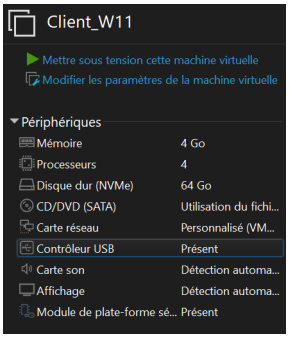
- Stockage : 20 go
- Ram : 1 go
- Processeurs : 2
- Carte réseau : Nat

-Carte réseau : "Tous les vlans"



Installation du VM client Windows 11

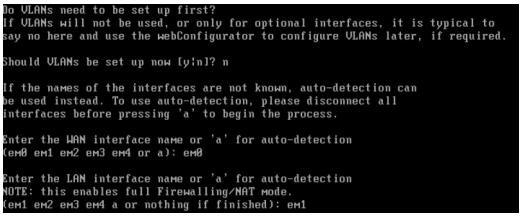
- Stockage : 64 go
- Ram : 4 go
- Processeurs : 4
- Carte réseau : "Vlan Bureaux"



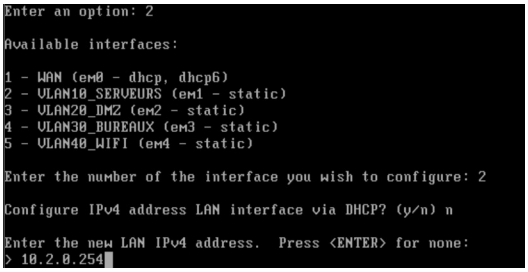
3. Installation et configuration de pfSense

3.1 Configuration initiale

Le pare-feu pfSense a été installé et configuré avec deux interfaces : WAN pour l'accès Internet et LAN pour le réseau interne.



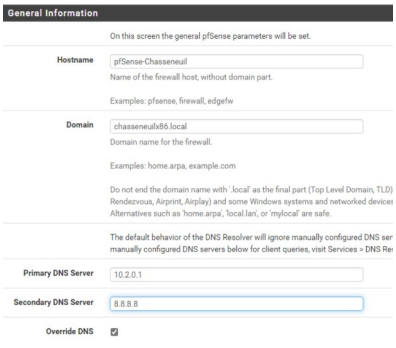
1) Assign interfaces
   vlan set : no
   wan : em0
   lan (serveur): em1

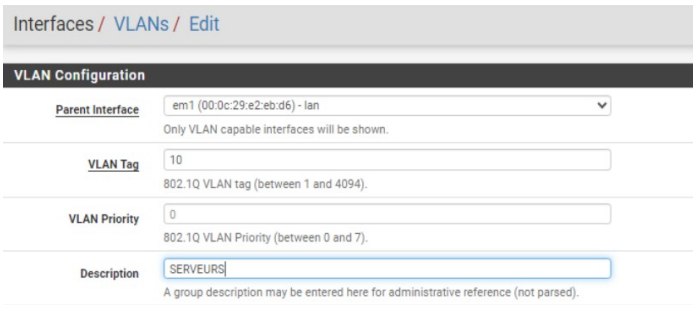


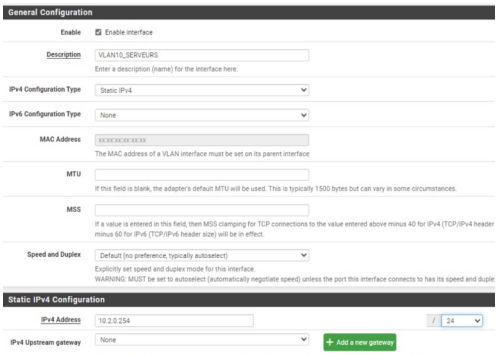
2) Set interfaces
   Sélectionner lan (serveur
      ipv4 : 10.2.0.254
      ipv6 : no

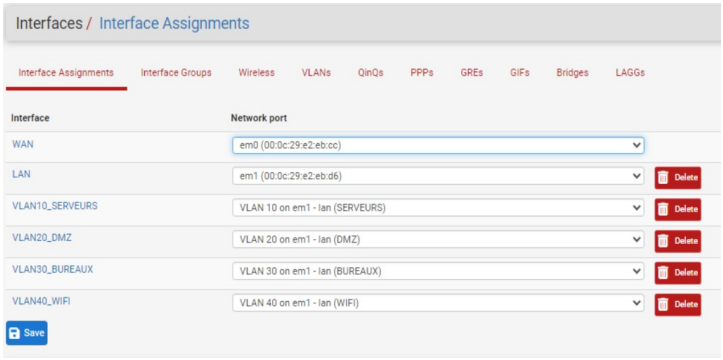
3.2 Configuration des VLANs

Un fois connecté en http avec l'IP du Lan (10.2.0.254) et compléter configuration initial pfSense, les VLANs ont été configurés afin de reproduire l'architecture réseau définie précedement.



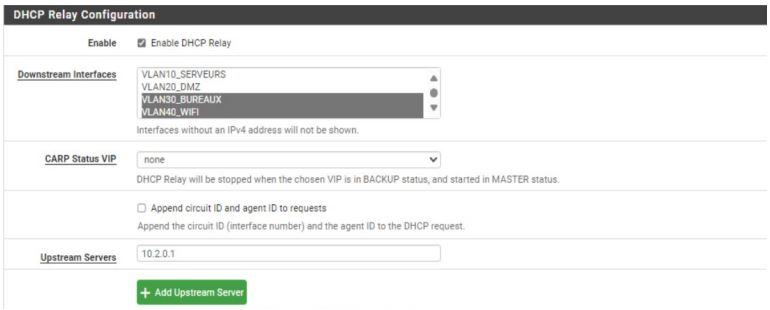






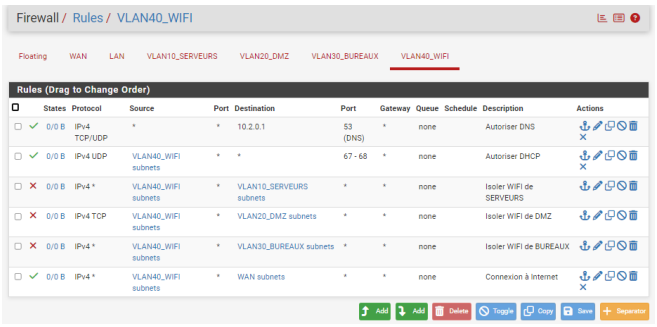
3.3 Configuration de DHCP relay

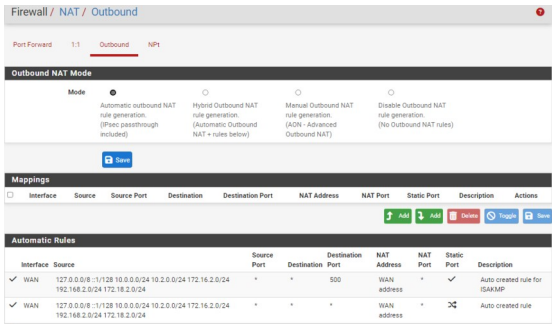
Le DHCP Relay a été configuré pour rediriger les requêtes DHCP vers le serveur Windows.



3.4 Règles Firewall

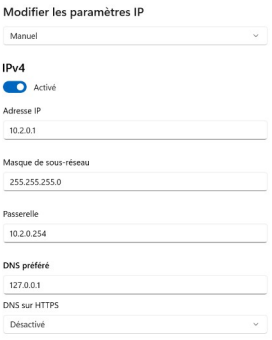
Des règles firewall ont été mises en place pour autoriser uniquement le DHCP, le DNS et l'accès Internet depuis le réseau WIFI tout en isolant les autres réseaux et le NAT sortant a été configuré afin de permettre aux réseaux internes d'accéder à Internet.





4. Installation et configuration Windows Server

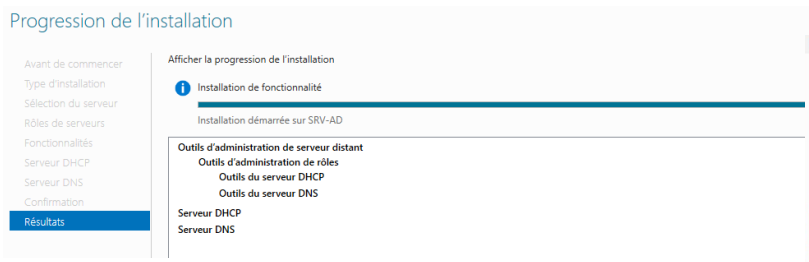
4.1 Paramétrage réseau

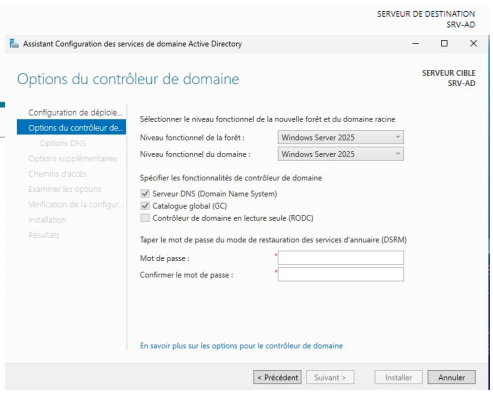


Le serveur Windows a été configuré avec une adresse IP fixe et utilisé comme serveur DNS principal.

4.2 Installation des rôles

Les rôles Active Directory, DHCP et DNS ont été installés via le gestionnaire de serveur. Ensuite, le serveur a été promu en contrôleur de domaine afin de centraliser l'authentification et la gestion des ressources.



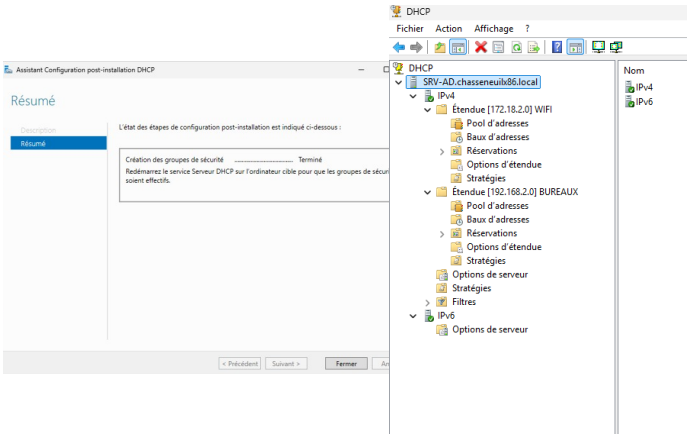


4.3 Configuration DHCP

Aprés finir la configuration post-installation, les étendues DHCP ont été configurées pour les réseaux Bureaux et WIFI avec les paramètres d'adressage correspondants.

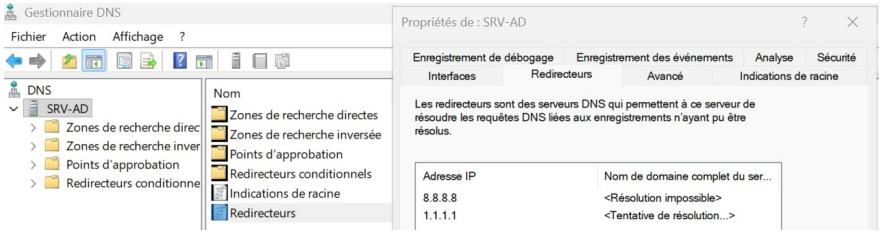
Nom : BUREAUX
- Plage : 192.168.2.100 → 192.168.2.200
- Masque : 255.255.255.0
- Passerelle : 192.168.2.254
- DNS : 10.2.0.1

- Nom : WIFI
- Plage : 172.18.2.100 → 172.18.2.200
- Masque : 255.255.255.0
- Passerelle : 172.18.2.254
- DNS : 10.2.0.1



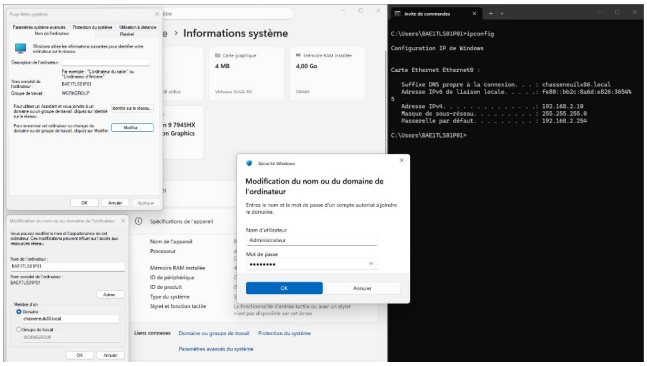
4.4 Configuration DNS

Le service DNS a été configuré avec des redirecteurs afin d'assurer la résolution des noms internes et externes.



5. Installation et configuration du poste client

Le client a été configuré en DHCP afin de recevoir automatiquement une adresse IP et les paramètres réseau et intégré au domaine Active Directory.

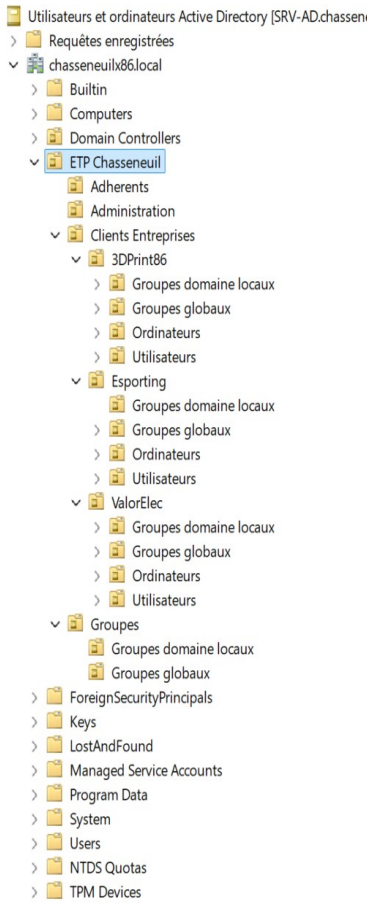


6. Création de l’Active Directory

Les unités d’organisation et les utilisateurs ont été créées automatiquement à l’aide de scripts PowerShell afin de structurer l’annuaire.

6.1 Création des OU

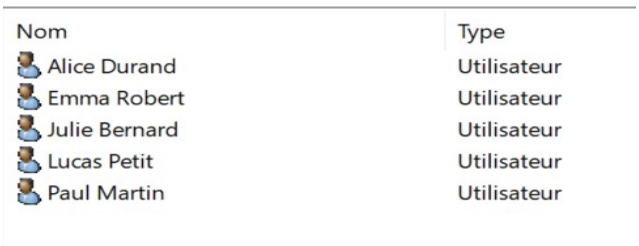
```
Import-Module ActiveDirectory

$domain = "DC=chasseneuilx86,DC=local"
# OU racine
New-ADOrganizationalUnit -Name "ETP Chasseneuil" -Path $domain
# OU principales
$base = "OU=ETP Chasseneuil,$domain"

New-ADOrganizationalUnit -Name "Administration" -Path $base
New-ADOrganizationalUnit -Name "Adherents" -Path $base
New-ADOrganizationalUnit -Name "Clients Entreprises" -Path $base
New-ADOrganizationalUnit -Name "Groupes" -Path $base

# OU Groupes global
New-ADOrganizationalUnit -Name "Groupes globaux" -Path "OU=Groupes,$base"
New-ADOrganizationalUnit -Name "Groupes domaine locaux" -Path "OU=Groupes,
$base"

# Entreprises
$entreprises = "Esporting","3DPrint86","ValorElec"

foreach ($ent in $entreprises) {
   $pathEnt = "OU=Clients Entreprises,$base"
   New-ADOrganizationalUnit -Name $ent -Path $pathEnt
   $entOU = "OU=$ent,$pathEnt"
   New-ADOrganizationalUnit -Name "Groupes globaux" -Path $entOU
   New-ADOrganizationalUnit -Name "Groupes domaine locaux" -Path $entOU
   New-ADOrganizationalUnit -Name "Utilisateurs" -Path $entOU
   New-ADOrganizationalUnit -Name "Ordinateurs" -Path $entOU
```



6.1 Création des utilisateurs

Création des utilisateurs du service Administration. Le script est réutilisable pour les services restantes.

```
Import-Module ActiveDirectory

# Domaine
$domain = "DC=chasseneuilx86,DC=local"
# OU
$adminOU = "OU=Administration,OU=ETP Chasseneuil,$domain"
# Mot de passe sécurisé
$Password = ConvertTo-SecureString "Sio1234*" -AsPlainText -Force

# Liste utilisateurs
$admins = @(
   @{Nom="Durand"; Prenom="Alice"},
   @{Nom="Martin"; Prenom="Paul"},
   @{Nom="Bernard"; Prenom="Julie"},
   @{Nom="Petit"; Prenom="Lucas"},
   @{Nom="Robert"; Prenom="Emma"}
)
```



```
# Création utilisateurs
foreach ($user in $admins) {

   $login = ($user.Prenom.Substring(0,1) + $user.Nom).ToLower()

   New-ADUser `
      -Name "$($user.Prenom) $($user.Nom)" `
      -GivenName $user.Prenom `
      -Surname $user.Nom `
      -SamAccountName $login `
      -UserPrincipalName "$login@chasseneuilx86.local" `
      -Path $adminOU `
      -AccountPassword $Password `
      -Enabled $true `
      -PasswordNeverExpires $true
}
```

7. Création des groupes

7.1 Groupes globaux

Des groupes globaux ont été créés pour regrouper les utilisateurs par service selon la convention de nommage définie (GG_).

```
Import-Module ActiveDirectory

# VARIABLES
$domain = "DC=chasseneuilx86,DC=local"
$baseOU = "OU=ETP Chasseneuil,$domain"
$OU_Global = "OU=Groupes globaux,OU=Groupes,$baseOU"
$OU_DL  = "OU=Groupes domaine locaux,OU=Groupes,$baseOU"
$ENT_ESP_GG  = "OU=Groupes globaux,OU=Esporting,OU=Clients Entreprises,$baseOU"
$ENT_ESP_DL  = "OU=Groupes domaine locaux,OU=Esporting,OU=Clients Entreprises,$baseOU"

# GROUPES GLOBAUX
New-ADGroup -Name "GG_Administration" -GroupScope Global -GroupCategory Security -Path $OU_Global
New-ADGroup -Name "GG_Adherents" -GroupScope Global -GroupCategory Security -Path $OU_Global
New-ADGroup -Name "GG_Esporting" -GroupScope Global -GroupCategory Security -Path $ENT_ESP_GG
```

7.2 Groupes domaine local

Des groupes domaine local ont été créés pour gérer les droits d’accès aux ressources selon la convention DL_NomDossier_Droit.

```
# GROUPES DOMAINE LOCAL
New-ADGroup -Name "DL_Administration_M" -GroupScope DomainLocal -GroupCategory Security -Path $OU_DL
New-ADGroup -Name "DL_Adherents_M" -GroupScope DomainLocal -GroupCategory Security -Path $OU_DL
New-ADGroup -Name "DL_Commun_L" -GroupScope DomainLocal -GroupCategory Security -Path $OU_DL
New-ADGroup -Name "DL_Esporting_M" -GroupScope DomainLocal -GroupCategory Security -Path
$ENT_ESP_DL
```

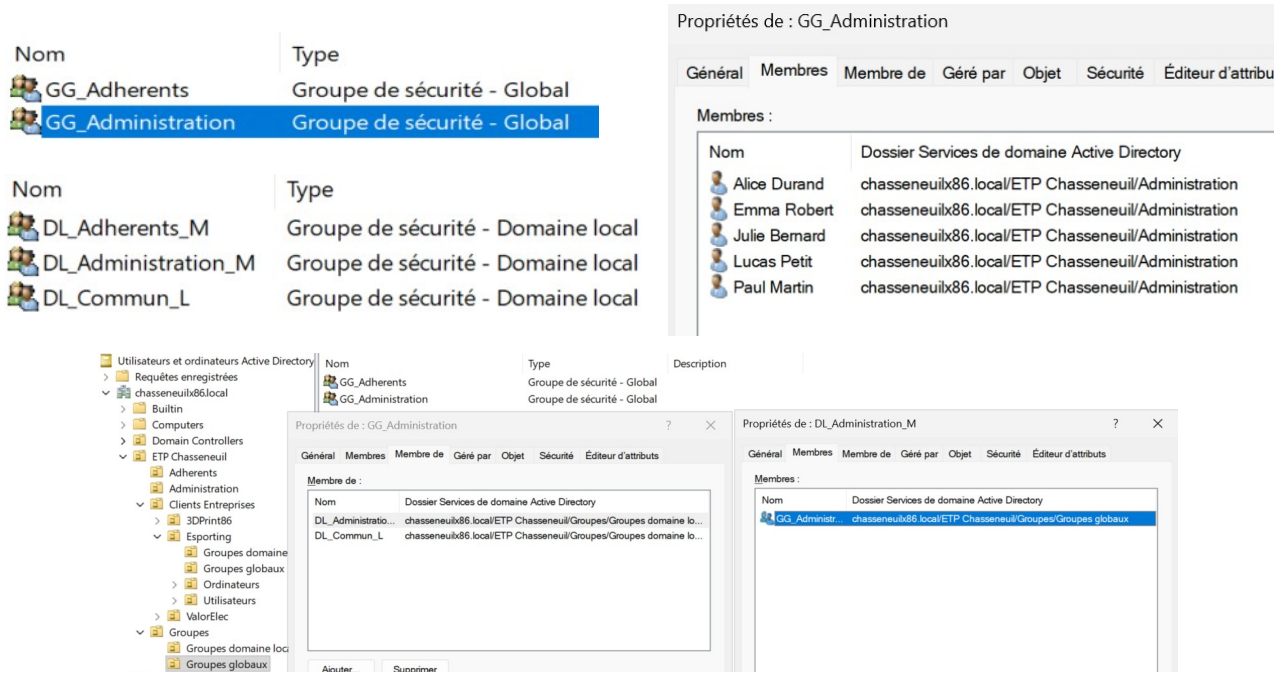
7.3 Imbrication des groupes

Les groupes globaux ont été intégrés dans les groupes domaine locaux afin d’appliquer la méthode AGDLP.

```
# IMBRICATION
Add-ADGroupMember -Identity "DL_Administration_M" -Members "GG_Administration"
Add-ADGroupMember -Identity "DL_Adherents_M" -Members "GG_Adherents"
Add-ADGroupMember -Identity "DL_Commun_L" -Members
"GG_Administration","GG_Adherents","GG_Esporting"
```

7.4 Ajout des utilisateurs aux groupes globaux

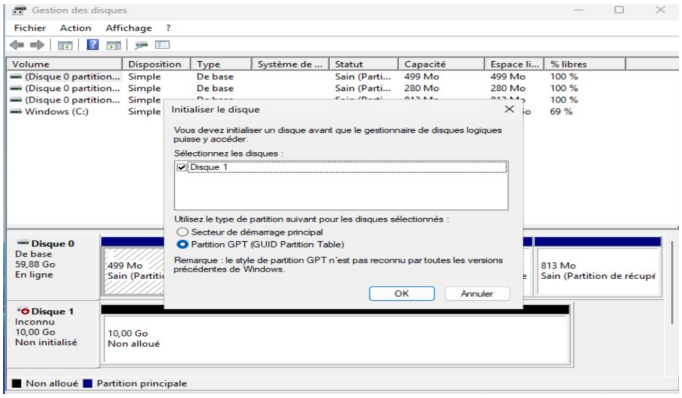
```
# VARIABLES
$domain = "DC=chasseneuilx86,DC=local"

$OU_Admin = "OU=Administration,OU=ETP Chasseneuil,$domain"
$OU_Adherents = "OU=Adherents,OU=ETP Chasseneuil,$domain"
$OU_Ent_Esp = "OU=Utilisateurs,OU=Esporting,OU=Clients Entreprises,OU=ETP Chasseneuil,$domain"
# AJOUT UTILISATEURS → GROUPES GLOBAUX

# Administration
Get-ADUser -Filter * -SearchBase $OU_Admin | ForEach-Object {
   Add-ADGroupMember -Identity "GG_Administration" -Members $_
}

# Adherents
Get-ADUser -Filter * -SearchBase $OU_Adherents | ForEach-Object {
   Add-ADGroupMember -Identity "GG_Adherents" -Members $_
}
# Esporting
Get-ADUser -Filter * -SearchBase $OU_Ent_Esp | ForEach-Object {
   Add-ADGroupMember -Identity "GG_Esporting" -Members $_
}
```

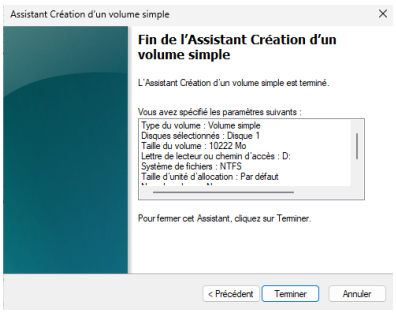


8. Mise en place des partages

8. 1. Création d'un nouveau disque

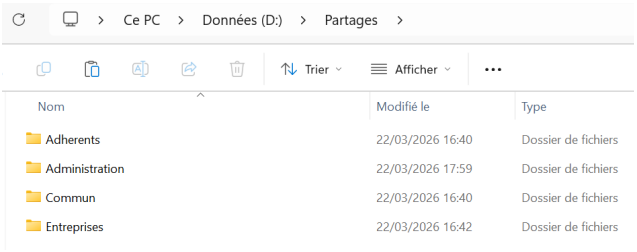
Un nouveau disque a été initialisé, partitionné et formaté en NTFS afin de créer un espace de stockage dédié aux partages réseau.





8.2 Création de l'arborescence

L'arborescence des dossiers partagés a été créée sur un disque dédié.



8.3 Attribution des droits NTFS

Les droits NTFS ont été appliqués en associant les groupes domaine locaux aux dossiers correspondants.

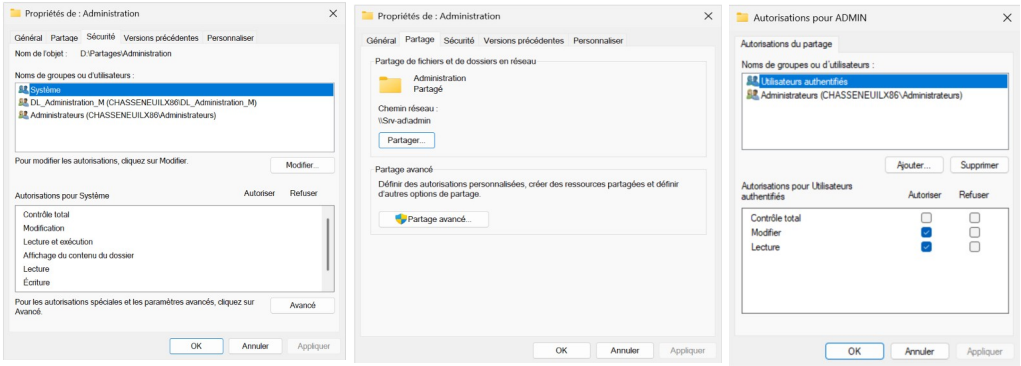
```
Import-Module ActiveDirectory

# DROITS NTFS

# Administration
icacls "D:\Partages\Administration" /inheritance:r
icacls "D:\Partages\Administration" /grant:r "SYSTEM:(F)"
icacls "D:\Partages\Administration" /grant:r "Administrateurs:(F)"
icacls "D:\Partages\Administration" /grant:r "chasseneuilx86\DL_Administration_M:(M)"

# Adherents
icacls "D:\Partages\Adherents" /inheritance:r
icacls "D:\Partages\Adherents" /grant:r "SYSTEM:(F)"
icacls "D:\Partages\Adherents" /grant:r "Administrateurs:(F)"
icacls "D:\Partages\Adherents" /grant:r "chasseneuilx86\DL_Adherents_M:(M)"

# Commun
icacls "D:\Partages\Commun" /inheritance:r
icacls "D:\Partages\Commun" /grant:r "SYSTEM:(F)"
icacls "D:\Partages\Commun" /grant:r "Administrateurs:(F)"
icacls "D:\Partages\Commun" /grant:r "chasseneuilx86\DL_Commun_L:(R)"

# Esporting
icacls "D:\Partages\Entreprises\Esporting" /inheritance:r
icacls "D:\Partages\Entreprises\Esporting" /grant:r "SYSTEM:(F)"
icacls "D:\Partages\Entreprises\Esporting" /grant:r "Administrateurs:(F)"
icacls "D:\Partages\Entreprises\Esporting" /grant:r "chasseneuilx86\DL_Esporting_M:(M)"
```

8.4 Création des partages SMB

Les partages réseau ont été configurés avec des droits adaptés en supprimant l'accès par défaut et en ajoutant les groupes autorisés.

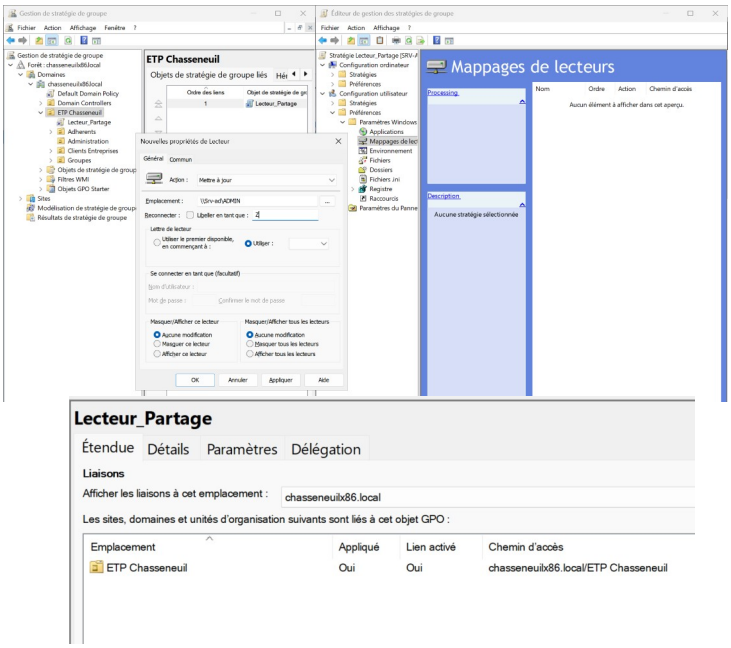
```
# DROITS SMB

New-SmbShare -Name "ADMIN" -Path "D:\Partages\Administration" -FullAccess "Administrateurs"
```

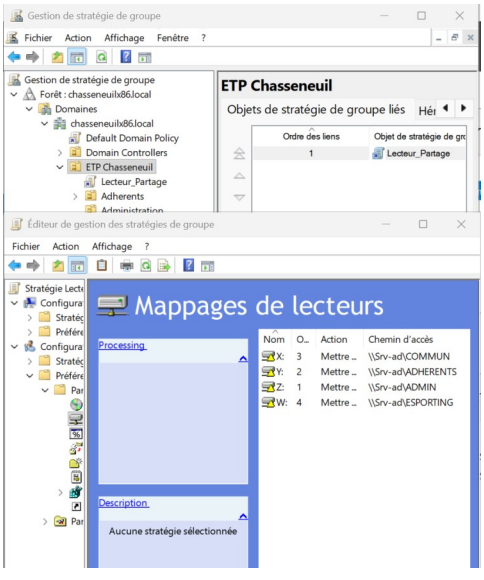
```
New-SmbShare -Name "ADHERENTS" -Path "D:\Partages\Adherents" -FullAccess "Administrateurs"
New-SmbShare -Name "COMMUN" -Path "D:\Partages\Commun" -FullAccess "Administrateurs"
New-SmbShare -Name "ESPORTING" -Path "D:\Partages\Entreprises\Esporting" -FullAccess "Administrateurs"


# Revocation de "Tout le monde"
Revoke-SmbShareAccess -Name "ADMIN" -AccountName "Everyone" -Force -ErrorAction SilentlyContinue
Revoke-SmbShareAccess -Name "ADHERENTS" -AccountName "Everyone" -Force -ErrorAction SilentlyContinue
Revoke-SmbShareAccess -Name "COMMUN" -AccountName "Everyone" -Force -ErrorAction SilentlyContinue
Revoke-SmbShareAccess -Name "ESPORTING" -AccountName "Everyone" -Force -ErrorAction SilentlyContinue

# Attribution aux "Utilisateurs authentifiés"
Grant-SmbShareAccess -Name "ADMIN" -AccountName "Utilisateurs authentifiés" -AccessRight Change -Force
Grant-SmbShareAccess -Name "ADHERENTS" -AccountName "Utilisateurs authentifiés" -AccessRight Change -Force
Grant-SmbShareAccess -Name "COMMUN" -AccountName "Utilisateurs authentifiés" -AccessRight Read -Force
Grant-SmbShareAccess -Name "ESPORTING" -AccountName "Utilisateurs authentifiés" -AccessRight Change -Force
```



9. Mise en place des lecteurs réseau par GPO

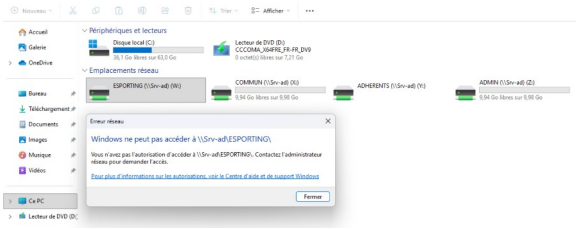
Les lecteurs réseau ont été déployés automatiquement via une stratégie de groupe afin de faciliter l'accès aux ressources.

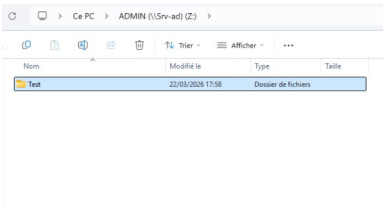




10. Tests

Des tests ont été réalisés afin de valider le bon fonctionnement de l'infrastructure : attribution DHCP, résolution DNS, accès aux partages et respect des droits utilisateurs.





12. Conclusion

Cet atelier a permis de déployer une infrastructure complète intégrant Active Directory, la gestion des utilisateurs et des ressources ainsi que l’automatisation des tâches. L’ensemble des services fonctionne conformément aux attentes.