

Préparation de l'environnement 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

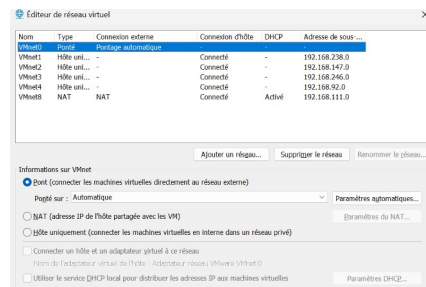
2.1 Configuration des réseaux

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".

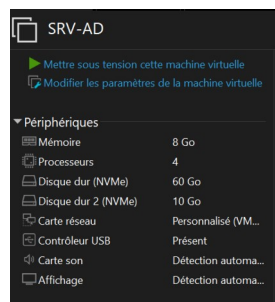


2.2 Création des machines virtuelles

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

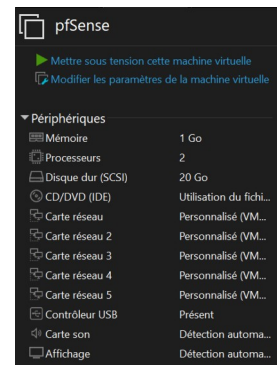
Installation du VM Windows Server

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



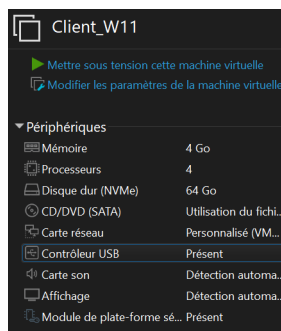
Installation du VM pFSense

- 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

```
No VLANs need to be set up first?  
If VLANs will not be used, or only for optional interfaces, it is typical to  
say no here and use the webConfigurator to configure VLANs later, if required.  
  
Should VLANs be set up now (y/n)? n  
  
If the names of the interfaces are not known, auto-detection can  
be used instead. To use auto-detection, please disconnect all  
interfaces before pressing 'a' to begin the process.  
  
Enter the WAN interface name or 'a' for auto-detection  
(em0 em1 em2 em3 em4 or a): em0  
  
Enter the LAN interface name or 'a' for auto-detection  
NOTE: this enables full Firewalling/NAT mode.  
(em1 em2 em3 em4 or nothing if finished): em1
```

```
Enter an option: 2  
  
Available interfaces:  
  
1 - WAN (em0 - dhcp, dhcp6)  
2 - VLAN10_SERVEURS (em1 - static)  
3 - VLAN20_DMZ (em2 - static)  
4 - VLAN30_BUREAUX (em3 - static)  
5 - VLAN40_WIFI (em4 - static)  
  
Enter the number of the interface you wish to configure: 2  
  
Configure IPv4 address LAN interface via DHCP? (y/n) n  
  
Enter the new LAN IPv4 address. Press <ENTER> for none:  
> 10.2.0.254
```

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 précédemment.

General Information

On this screen the general pfSense parameters will be set.

Hostname: pfSense-Chasseneuil

Domain: chasseneuil@local

Primary DNS Server: 10.2.0.1

Secondary DNS Server: 8.8.8.8

Override DNS:

Interfaces / VLANs / Edit

VLAN Configuration

Parent Interface: em1 (00:0c:29:e2:eb:d6) - lan

VLAN Tag: 10

VLAN Priority: 0

Description: SERVEURS

General Configuration

Enable: Enable interface

Description: VLAN10_SERVEURS

IPv4 Configuration Type: Static IPv4

IPv6 Configuration Type: None

MAC Address: [random]

MTU: [blank]

MSS: [blank]

Speed and Duplex: Default (no preference, typically autoselect)

Static IPv4 Configuration

IPv4 Address: 10.2.0.254

IPv4 Upstream gateway: None

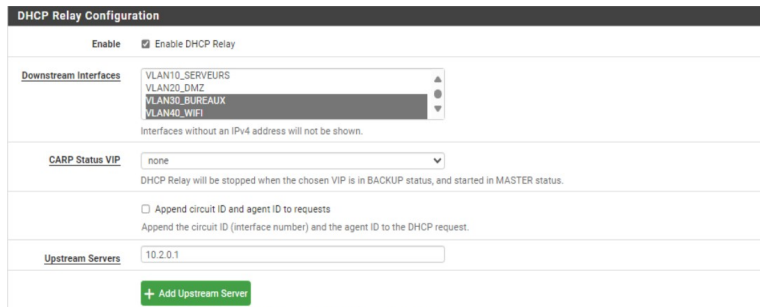
Interfaces / Interface Assignments

Interface	Network port
WAN	em0 (00:0c:29:e2:eb:cc)
LAN	em1 (00:0c:29:e2:eb:d6)
VLAN10_SERVEURS	VLAN 10 on em1 - lan (SERVEURS)
VLAN20_DMZ	VLAN 20 on em1 - lan (DMZ)
VLAN30_BUREAUX	VLAN 30 on em1 - lan (BUREAUX)
VLAN40_WIFI	VLAN 40 on em1 - lan (WIFI)

Save

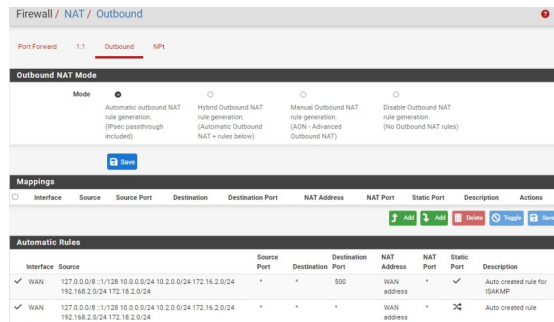
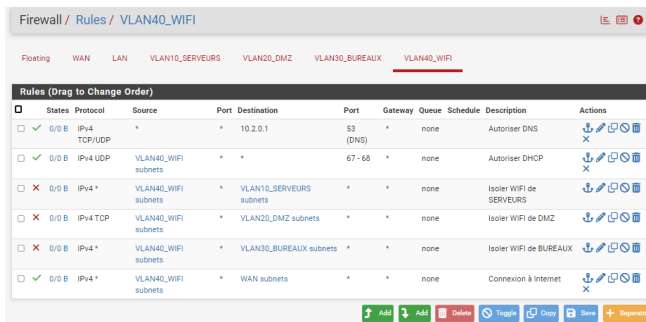
3.3 Configuration de DHCP relay

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.



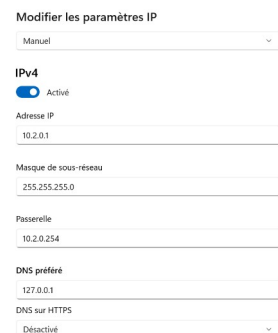
4. Installation et configuration Windows Server

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.



Progression de l'installation

- Avant de commencer
- Type d'installation
- Sélection du serveur
- Rôles de serveurs
- Fonctionnalités
- Serveur DHCP
- Serveur DNS
- Confirmation
- Résultats

Afficher la progression de l'installation

1 Installation de fonctionnalité

Installation démarrée sur SRV-AD

- Outils d'administration de serveur distant
- Outils d'administration de rôles
- Outils du serveur DHCP
- Outils du serveur DNS

Serveur DHCP

Serveur DNS

Assistant Configuration des services de domaine Active Directory

Options du contrôleur de domaine

Configuration de déploiement

Options du contrôleur de domaine

Options de rôle

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configuration

Installation

Résultats

Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine

Niveau fonctionnel de la forêt : Windows Server 2025

Niveau fonctionnel du domaine : Windows Server 2025

Spécifier les fonctionnalités de contrôleur de domaine

Serveur DNS (Domain Name System)

Catalogue global (GC)

Contrôleur de domaine en lecture seule (RODC)

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe : []

Confirmer le mot de passe : []

En savoir plus sur les options pour le contrôleur de domaine

< Précédent Suivant > Installer Annuler

4.3 Configuration DHCP

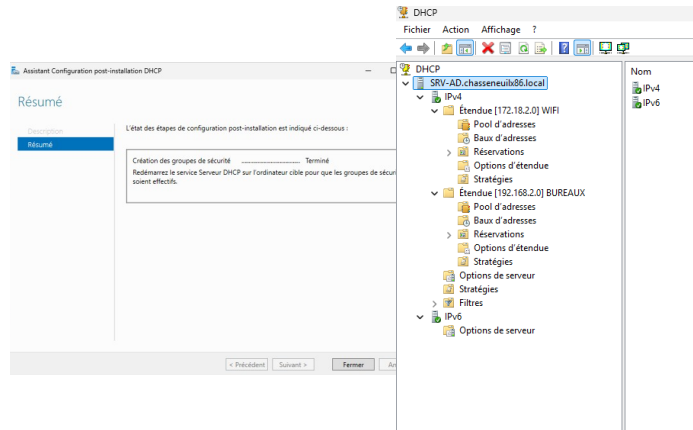
Après finir la configuration post-installation, les étendues DHCP ont été configurées pour les réseaux Bureaux et WIFI avec les paramètres d'adressage correspondants.

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

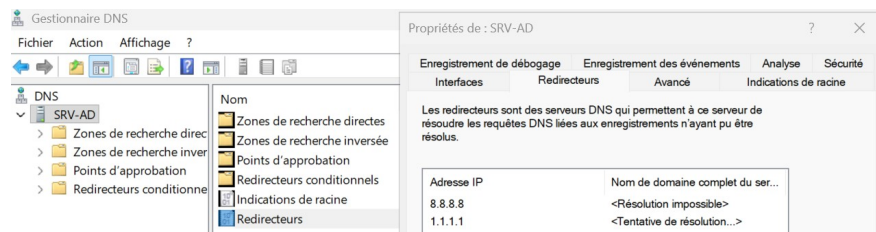
- Nom : WIFI

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



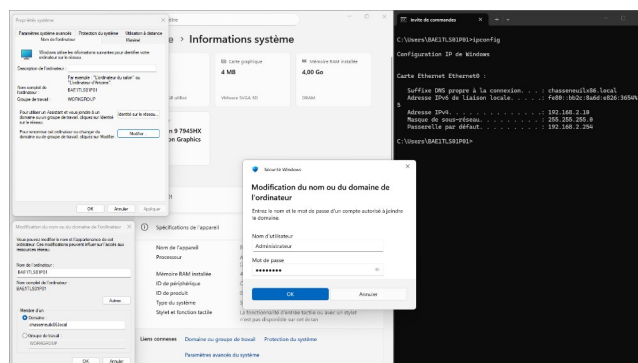
4.4 Configuration DNS

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 créés 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"}
)
```

Nom	Type
 Alice Durand	Utilisateur
 Emma Robert	Utilisateur
 Julie Bernard	Utilisateur
 Lucas Petit	Utilisateur
 Paul Martin	Utilisateur

```
# 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"
$SENT_ESP_GG = "OU=Groupes globaux,OU=Esporting,OU=Clients Entreprises,$baseOU"
$SENT_ESP_DL = "OU=Groupes domaine locaux,OU=Esporting,OU=Clients Entreprises,$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 $SENT_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_Communi_L" -GroupScope DomainLocal -GroupCategory Security -Path $OU_DL
New-ADGroup -Name "DL_Esporting_M" -GroupScope DomainLocal -GroupCategory Security -Path
$SENT_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_Commune_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 $_
```

```
}
```

The screenshot displays the Active Directory console with several windows open. On the left, a tree view shows the hierarchy: Utilisateurs et ordinateurs Active Directory > Requêtes enregistrées > chasseneuilx86.local > Builtin > Computers > Domain Controllers > ETP Chasseneuil > Adherents > Administration > Clients Entreprises > 3DPrint86 > Esporting > Groupes domaine > Groupes globaux > Ordinateurs > Utilisateurs > ValorElec > Groupes > Groupes domaine local > Groupes globaux.

Three windows show group properties:

- Propriétés de : GG_Administration**: Shows the 'Membres' tab with a list of users: Alice Durand, Emma Robert, Julie Bernard, Lucas Petit, and Paul Martin, all with domain paths like chasseneuilx86.local/ETP Chasseneuil/Administration.
- Propriétés de : DL_Administration_M**: Shows the 'Membres' tab with a list of users: DL_Administratio... and DL_Commune_L, with domain paths like chasseneuilx86.local/ETP Chasseneuil/Groupes/Groupes domaine lo...
- Propriétés de : DL_Administration_M**: Shows the 'Membres' tab with a list of users: GG_Administr... with a domain path like chasseneuilx86.local/ETP Chasseneuil/Groupes/Groupes globaux.

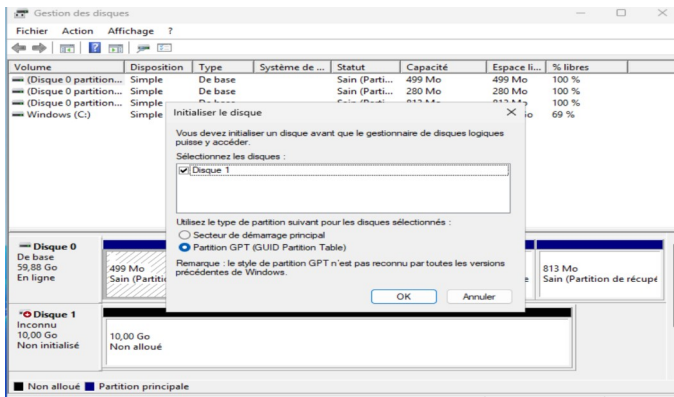
Two other windows show a list of groups:

Nom	Type
GG_Adherents	Groupe de sécurité - Global
GG_Administration	Groupe de sécurité - Global
DL_Adherents_M	Groupe de sécurité - Domaine local
DL_Administration_M	Groupe de sécurité - Domaine local
DL_Commune_L	Groupe de sécurité - Domaine local

8. Mise en place des partages

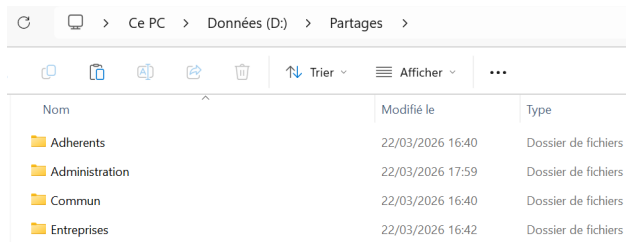
8.1. Création d'un nouveau disque

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_Communic_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"
```

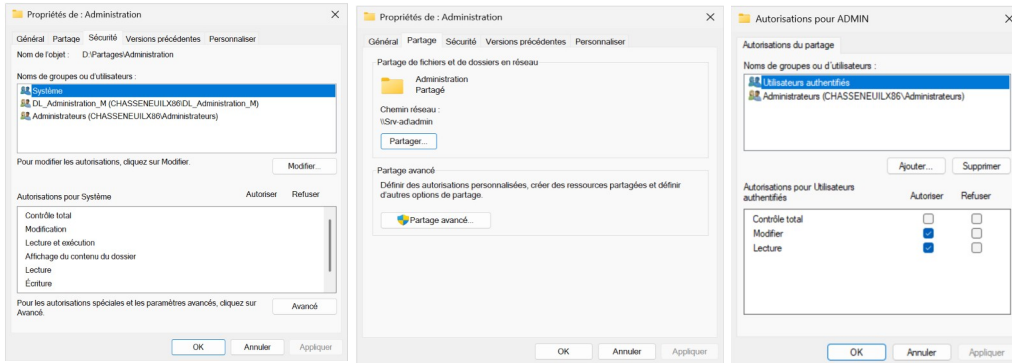
```
New-SmbShare -Name "ADHERENTS" -Path "D:\Partages\Adherents" -FullAccess "Administrateurs"
New-SmbShare -Name "COMMUN" -Path "D:\Partages\Commun" -FullAccess "Administrateurs"
New-SmbShare -Name "ESPORTING" -Path "D:\Partages\Entreprises\Esporting" -FullAccess "Administrateurs"
```

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
```

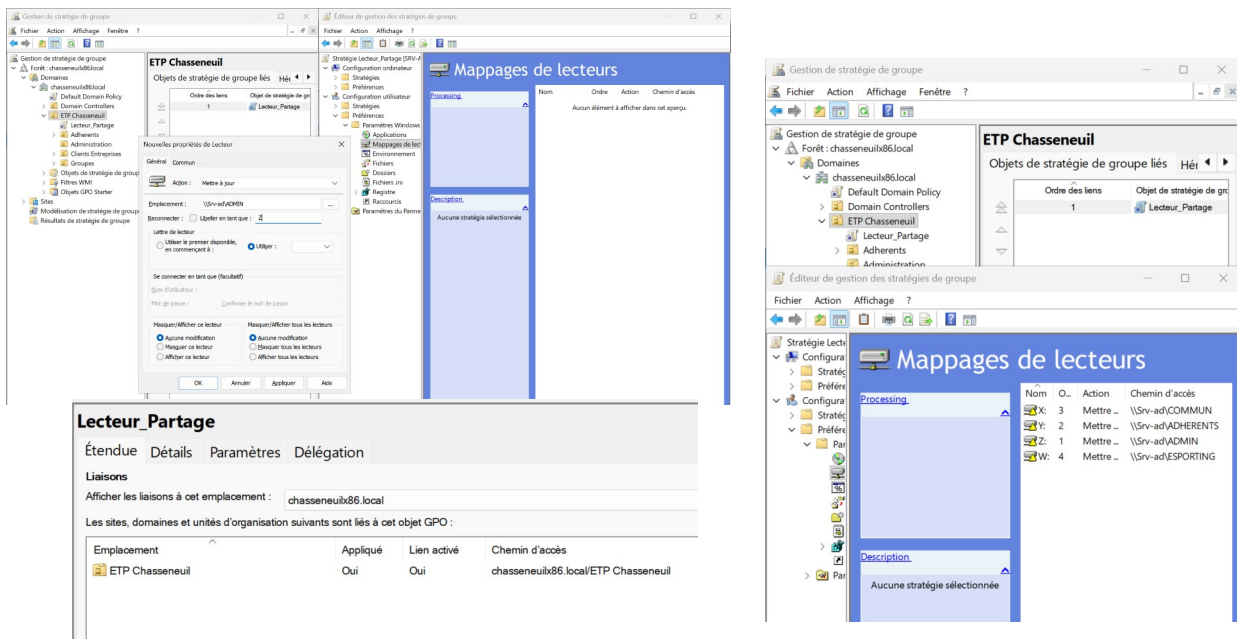
Attribution aux "Utilisateurs authentifiés"

```
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
```



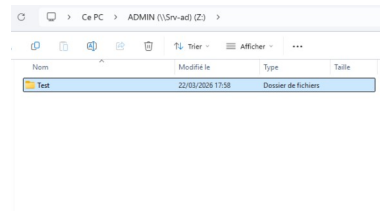
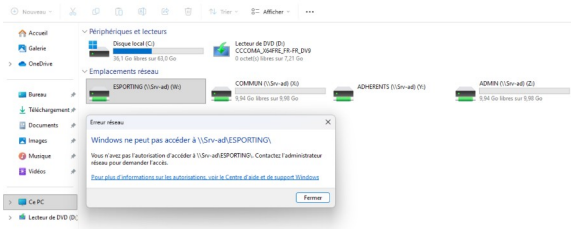
9. Mise en place des lecteurs réseau par GPO

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.