

# Onglet 1

## AP3-2 Domaine et découpage réseau

### Liens des réunions :

Réunion jour 1 :

[https://docs.google.com/document/d/1kcFSnpUjdO5TUHRticl6tr\\_wvy1jL2INwdKFKS9YIYE/edit?tab=t.0](https://docs.google.com/document/d/1kcFSnpUjdO5TUHRticl6tr_wvy1jL2INwdKFKS9YIYE/edit?tab=t.0)

Réunion Jour 2 :

<https://docs.google.com/document/d/1vYDEUxN4QqyOdFx0dDbYqK-dZaHt1BxJZ1et5tAeD94/edit?tab=t.0>

Réunion Jour 3 :

[https://docs.google.com/document/d/1rlA20oMFfa4M6y5qn\\_NhBitcMvSHql65NYpfWVm9g9k/edit?tab=t.0](https://docs.google.com/document/d/1rlA20oMFfa4M6y5qn_NhBitcMvSHql65NYpfWVm9g9k/edit?tab=t.0)

Réunion Jour 4 :

[https://docs.google.com/document/d/1ysXy7fUcEuMkdTdB19z2\\_aHpx4Ffw3yOLa\\_6ZhSmHYU/edit?tab=t.0](https://docs.google.com/document/d/1ysXy7fUcEuMkdTdB19z2_aHpx4Ffw3yOLa_6ZhSmHYU/edit?tab=t.0)

Réunion Jour 5 :

[https://docs.google.com/document/d/18nCA3u\\_lrNPYDUvTun9PEO1rHwRtQiGE6fJrQQEUzOU/edit?usp=sharing](https://docs.google.com/document/d/18nCA3u_lrNPYDUvTun9PEO1rHwRtQiGE6fJrQQEUzOU/edit?usp=sharing)

Réunion Jour 6 :

<https://docs.google.com/document/d/1Oorl7Xa-Dw9QDdhgWf2zDol76z-H0Jgb57sqWQ0K8vw/edit?usp=sharing>

Ajouter les switchs pour Enzo dans mRemoteNG et les routeurs pour Félicien.

schéma logique = mon physique avec les liens trunk, vlans, ip etc... et le

physique = mon physique avec les logiciels les noms etc ...

<https://trello.com/invite/b/68c9610f6526ae06f431817b/ATTI5e33d5bd7a4c69461359fe434d3de8a48DA20F77/ap3-2>

## **1. Infrastructure réseau – Routeur Cisco**

- Adressage IPv4 configuré et fonctionnel.
  - Accès sécurisé en SSH (pas de Telnet).
  - Compte administrateur modifié (mot de passe fort).
  - Câblage conforme au schéma réseau.
  - Communication avec Internet validée.
  - Communication avec le switch cœur opérationnelle.
  - Encapsulation DOT1Q fonctionnelle.
  - Système de sauvegarde des configurations actif (local + Nextcloud).
  - Upgrade OS/firmware du routeur effectué.
  - Documentation complète (config, procédures).
- 

## **2. Infrastructure réseau – Commutateur Cœur/Distribution**

- Adressage IPv4 configuré et fonctionnel.
- Accès SSH sécurisé, compte admin changé.
- Route par défaut configurée.
- Communication montante vers routeur et Internet OK.
- VLAN créés et propagés.
- VTP activé et opérationnel.

- Affectation des ports conforme au plan.
  - Communication avec switches d'accès validée.
  - Système mis à jour.
  - Documentation (config + procédures) réalisée.
  - Gestion des configurations (sauvegarde/Nextcloud).
- 

### **3. Infrastructure réseau – Commutateurs d'Accès**

- Adressage IPv4 configuré et fonctionnel.
  - SSH activé et accès admin sécurisé.
  - Route par défaut définie.
  - Communication Internet validée.
  - VLAN créés localement.
  - VTP configuré (client ou transparent selon design).
  - Ports affectés correctement aux VLAN (100/200/300).
  - Communication stable avec switch distribution.
  - Mise à jour système appliquée.
  - Documentation réalisée (configs, procédures).
  - Gestion des configurations assurée.
- 

### **4. Documentation et Organisation**

- Dossier technique complet rendu.
  - Contexte rappelé et cahier des charges respecté.
  - Schéma réseau **physique** validé.
  - Schéma réseau **logique** validé.
  - Plan d'adressage + plan de nommage conforme à la RFC1178.
  - Tableau de répartition des ports fourni.
  - Mise en place d'un système de gestion des mots de passe.
  - Plan de formation et transfert de compétences défini.
  - Outils de planification utilisés (Gantt, Trello...).
  - Répartition équitable des tâches entre membres.
  - Équipements en baie conformes.
  - Qualité du câblage validée.
- 

## 5. Proxmox & Active Directory

### Proxmox

- Dernière version installée (Proxmox VE latest).
- Adressage IPv4 configuré.
- Comptes admin distincts créés (pas d'usage unique root).
- Câblage conforme.
- Documentation Proxmox complète.
- Gestion des configurations assurée (backup VM, snapshot).

## Active Directory

- Domaine créé : m21X.1an conforme.
- Adressage IPv4 serveur défini.
- Découverte et documentation des vulnérabilités AD.
- GPO appliquées (fond d'écran, restrictions).
- Connexion réussie avec comptes utilisateurs.
- Profils itinérants opérationnels.
- Partages configurés :
  - Partage groupe (lecture/écriture/modif, pas suppression).
  - Partage global (direction seule).
  - Partage hors ligne avec VSS.
- Montage automatique des lecteurs réseau via GPO/script.
- Création des utilisateurs, groupes et OU conforme au fichier Excel.
- Documentation AD complète.
- Gestion des configurations (sauvegarde AD, export GPO).

# Plan TCP/IP

Les 3 dernières de chaque vlans sont les 3 ip des routeurs.

	VLAN	De	à	Masque
Handball	10	172.26.11.1	172.26.11.59	255.255.255.192
Basket	20	172.26.11.65	172.26.11.91	255.255.255.224
Volley	30	172.26.11.97	172.26.11.123	255.255.255.224
Direction	80	172.26.11.129	172.26.11.155	255.255.255.224
Danse	40	172.26.11.161	172.26.11.171	255.255.255.240
Tennis	50	172.26.11.177	172.26.11.179	255.255.255.248
Escrime	60	172.26.11.185	172.26.11.187	255.255.255.248
Football	70	172.26.11.193	172.26.11.195	255.255.255.248
Bowling	90	172.26.11.201	172.26.11.203	255.255.255.248
DMZ	18	172.26.11.209	172.26.11.219	255.255.255.240
Wifi	100	172.26.11.225	172.26.11.235	255.255.255.240
Visiteurs	110	172.26.11.241	172.26.11.243	255.255.255.248
Téléphonie	300	172.26.13.1	172.26.13.123	255.255.255.128
Impression	15	172.26.15.1	172.26.15.11	255.255.255.240
Administration	99	172.26.16.1	172.26.16.11	255.255.255.240
serveur	17	172.26.17.1	172.26.17.11	255.255.255.240



	Passerelle Routeur 1	Passerelle Routeur 2	Passerelle Routeur VIP
Handball	172.26.11.60	172.26.11.61	172.26.11.62
Basket	172.26.11.92	172.26.11.93	172.26.11.94
Volley	172.26.11.124	172.26.11.125	172.26.11.126
Direction	172.26.11.156	172.26.11.157	172.26.11.158
Danse	172.26.11.172	172.26.11.173	172.26.11.174
<b>Tennis</b>	172.26.11.180	172.26.11.181	172.26.11.182
Escrime	172.26.11.188	172.26.11.189	172.26.11.190
Football	172.26.11.196	172.26.11.197	172.26.11.198
Bowling	172.26.11.204	172.26.11.205	172.26.11.206
DMZ	172.26.11.220	172.26.11.221	172.26.11.222
Wifi	172.26.11.236	172.26.11.237	172.26.11.238
Visiteurs	172.26.11.244	172.26.11.245	172.26.11.246
Téléphonie	172.26.13.124	172.26.13.125	172.26.13.126
Impression	172.26.15.12	172.26.15.13	172.26.15.14
Administration	172.26.16.12	172.26.16.13	172.26.16.14
serveur	172.26.17.12	172.26.17.13	172.26.17.14



Nommage

**PC** → PC-Mercure-01, PC-Venus-02, PC-Terre-03

**Switchs** → SW-Orbite-01, SW-Galaxie-02

**Routeurs** → RT-Soleil, RT-Lune

**Serveurs** → SRV-Andromede(W2022-serveur), SRV-Nebuleuse

**VLANs** → VLAN-Planete, VLAN-Tellurique, VLAN-Gazeux

**Prises murales** → PR-Comete-01, PR-Astéroïde-02

Docu WSERVER/Proxmox

**Nom du serveur: SRV-Andromede**

**IP du serveur: 172.26.17.1**

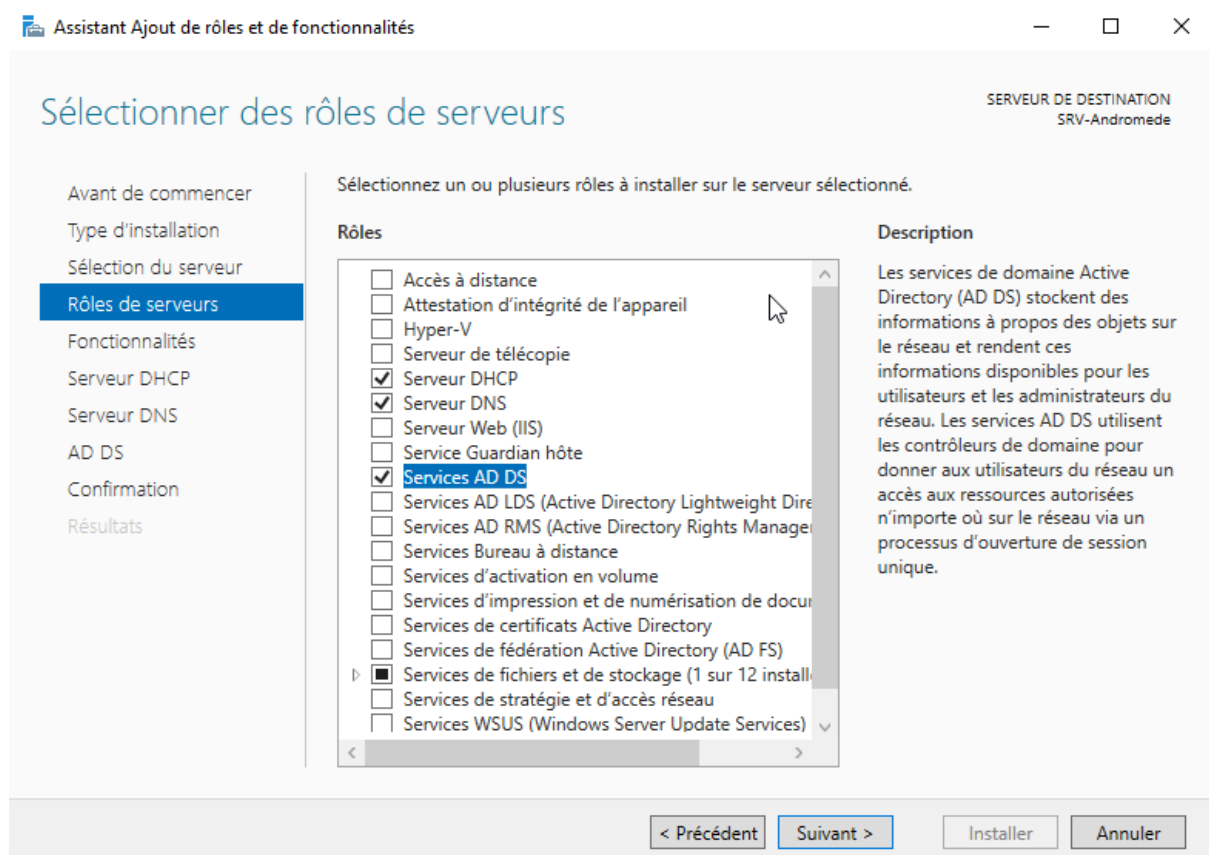
**IP du serveur proxmox: 172.26.17.11**

**Passerelle du serveur proxmox: 172.26.17.12**

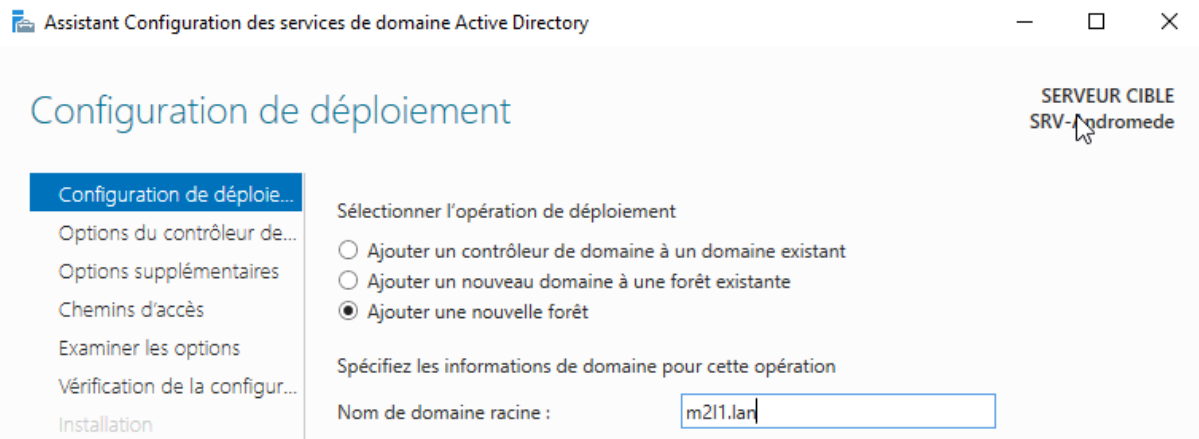
**Masquer du serveur: 255.255.255.240**

**Passerelle du serveur: 172.26.17.**

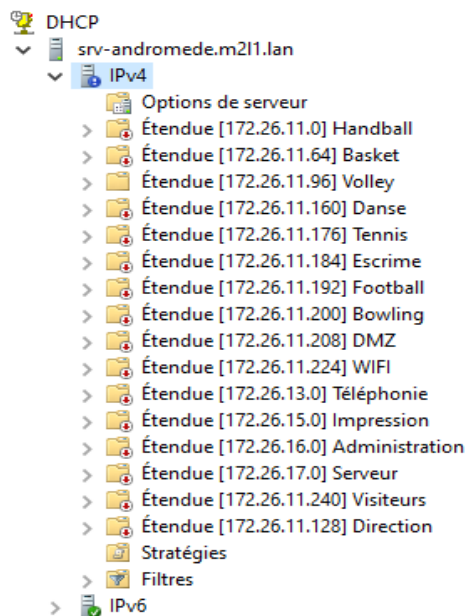
## Installation des services AD DS, Serveur DHCP et Serveur DNS



## Configuration du Active Directory (domaine m2l1.lan)

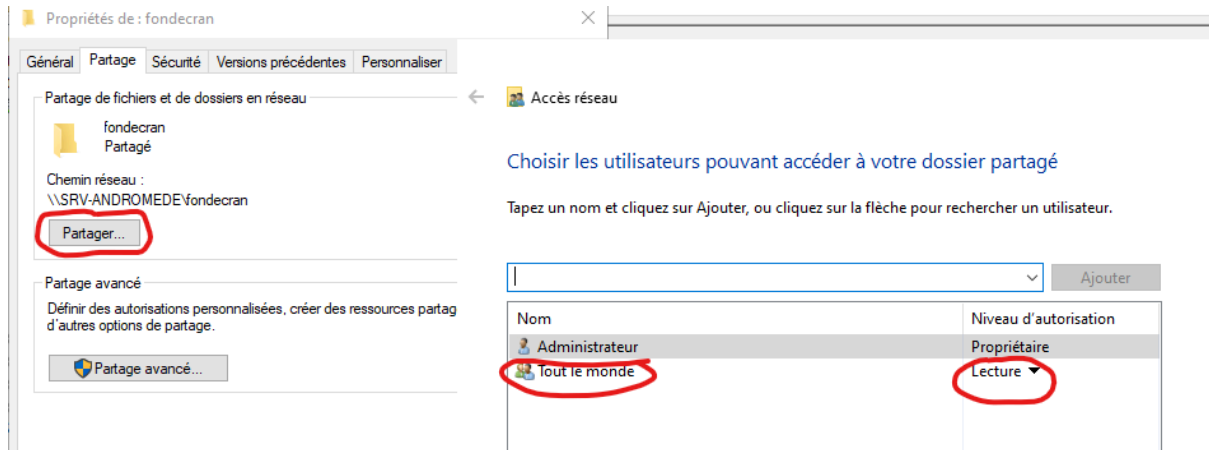


## Création des étendues (des vlans) sur le DHCP



## GPO Fond d'écran

Partager le fichier où se trouve les différents fonds d'écrans:



Créer les groupes pour chaque ligue dans AD:\*

Nom	Type	Description
Computers	Conteneur	Default container for upgr...
Tennis	Groupe	
Handball	Groupe	
Football	Groupe	
Escrime	Groupe	
Bowling	Groupe	
Basket	Groupe	
Danse	Groupe	
Volley	Groupe	

Créer 1 utilisateur par Ligue:

*C'est utilisateur serviront de test durant la configuration de l'AD*

User10 basket

User20 Tennis

User30 Escrime

User40 Danse

User50 Football

User60 Handball

User70 Bowling

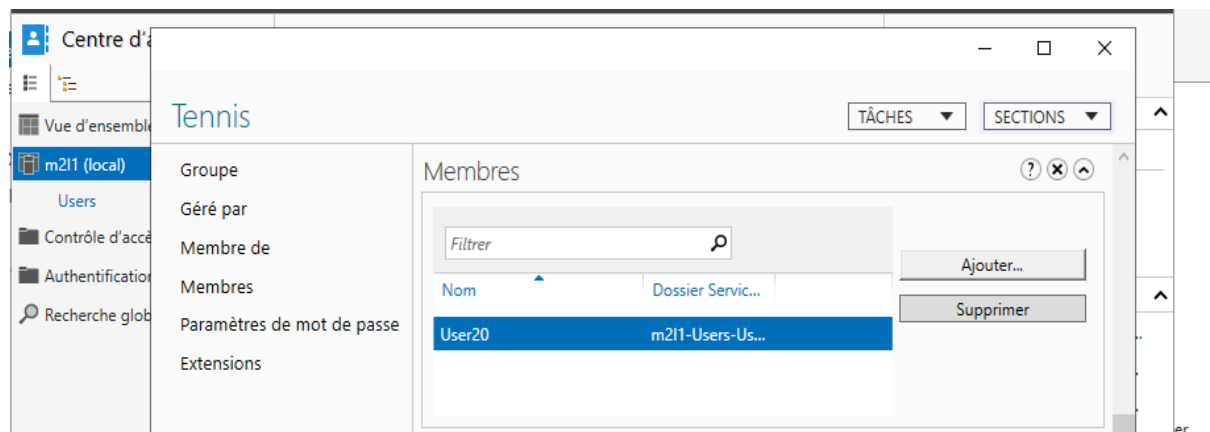


User Volley

Mpd par défaut Azerty11 puis changer en Azerty1234 lors de la première connexion

Nom	Type	Description
Utilisateurs DHCP	Groupe	Les membres qui ont un a...
User70	Utilisateur	
User60	Utilisateur	
User50	Utilisateur	
User40	Utilisateur	
Administrateur	Utilisateur	Compte d'utilisateur d'ad...
User10	Utilisateur	
User User	Utilisateur	
krbtgt	Utilisateur	Compte de service du cen...
Invité	Utilisateur	Compte d'utilisateur invité
User30	Utilisateur	
User20	Utilisateur	

Ajouter chaque utilisateur dans son groupe (ligue) dédié:

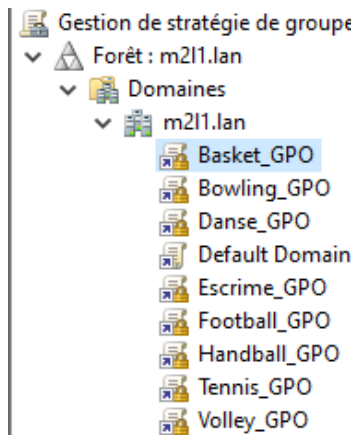


Ensuite aller dans Gestion des stratégies de groupes:

Ouvre Gestion de la stratégie de groupe (GPMC).

Clic droit sur le domaine m211.lan → Créer un objet GPO et le lier ici... puis donnez

lui un nom (Activer la GPO avec clic droit → Activer)



Clic droit sur votre GPO, puis Modifier

Configuration utilisateur → Préférences → Paramètres Windows → Fichiers.  
Nouveau → Fichier.

Action : **Remplacer**

Chemin source : **\\SRV-AD\fondcran\NOM\_IMAGE**

Chemin destination : **%USERPROFILE%\Images\NOM\_IMAGE**

Laisser par défaut (ne pas cocher Lecture seule / Masqué).

Dans commun cocher “Exécuter dans le contexte de sécurité de l'utilisateur connecté”


Valider.


Puis aller dans Configuration utilisateur → Modèle d'administration → Bureau → Bureau → Papier peint du Bureau

Activer

Nom du papier Peint

Mettre le chemin UNC:

 Papier peint du Bureau

 Papier peint du Bureau

☐ Non configuré    Commentaire :   
☒ Activé  
☐ Désactivé

Pris en charge sur :

Options :

Nom du papier peint :

Exemple : avec un chemin local :  
C:\windows\web\wallpaper\home.jpg

Exemple : avec un chemin UNC :  
\\Server\Share\Corp.jpg


Style du papier peint :

OK

Puis dans Configuration utilisateur → Préférences → Paramètre Windows → Fichier  
→ Clic Droit nouveau fichier

Propriétés de : dancer-5576002\_1920.jpg

Général    Commun

 Action :

Fichier(s) source :  ...

Fichier de destination :  ...

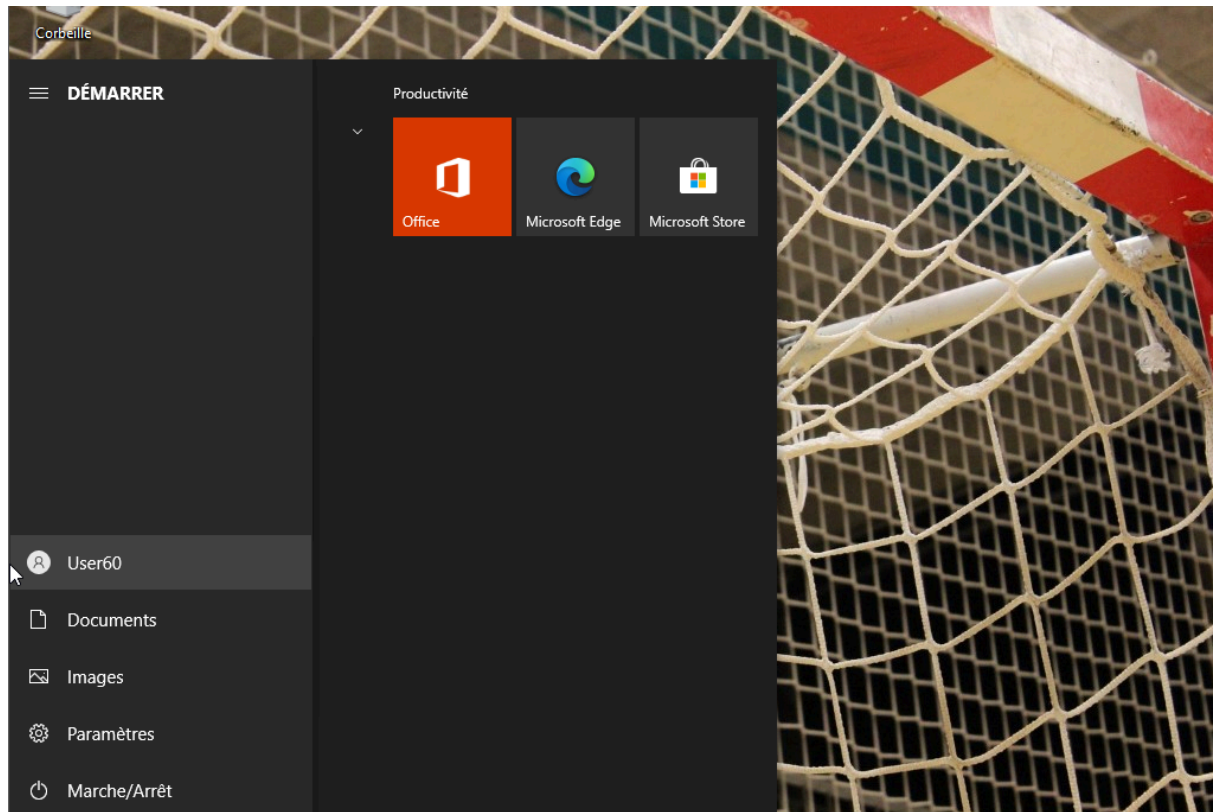
☐ Supprimer les erreurs sur les actions de fichiers individuels

Attributs

☐ Lecture seule  
☐ Masqué  
☐ Archiver

Puis dans la délégation de la GPO mettre les autorisations sur le groupe en question:  
**Lecture et Appliquer la stratégie de groupe.**

**Test avec User60:**



# Profils itinérants

## Créer le dossier de profils sur le serveur

Sur le serveur AD, créer un dossier sur un disque local (ex. D:) :

**D:\Profils**

Ce dossier contiendra les sous-dossiers des utilisateurs, créés automatiquement à la première connexion.

Clic droit sur le dossier → Propriétés → Partage

Cliquer sur Partager...

Ajouter Tout le monde (ou un groupe minimal pour le test) → autorisation Lecture/Écriture

Cliquer Partager puis Terminer

Chemin réseau accessible depuis les postes clients :

Toujours sur le dossier parent D:\Profils → Propriétés → Sécurité

Ajouter les groupes et utilisateurs suivants :

Administrateurs → Contrôle total

SYSTEM → Contrôle total

Authenticated Users → Lecture + Écriture

Ne pas cocher “Modification” ni “Contrôle total” sur le dossier parent

Activer l’héritage (dans Avancé)

## Définir le chemin du profil itinérant dans ADUC

Ouvrir Active Directory Users and Computers

Sélectionner un utilisateur → clic droit → Propriétés → Onglet Profil

Dans Chemin d’accès, saisir le chemin réseau vers le dossier partagé :

**\\SRV-AD\Profils\%username%**

User20


Compte	Profil
Organisation	Chemin d'accès ROMEDE\Profils\%username% :
Membre de	Dossier de base :

**%username%** permet de créer automatiquement le sous-dossier pour chaque utilisateur

**Test avec User40:**

Réseau > SRV-ANDROMEDE > Profils >

Rechercher dans : Profils

Nom	Modifié le	Type	Taille
 User40.V6	13/10/2025 09:12	Dossier de fichiers	

Le sous-dossier a bien été créé et je peux l'ouvrir et modifier son contenu.

## Partage 1 Groupe

Créer un dossier sur C: sur le serveur, aller dans propriété puis partage avancé.

Partage avancé

☒ Partager ce dossier

Paramètres

Nom du partage :  
 Partage\_Groupe\$

Ajouter Supprimer

Limiter le nombre d'utilisateurs simultanés à : 16777

Commentaires :

Autorisations Mise en cache

Autorisations pour Partage\_Groupe\$

Autorisations du partage

Noms de groupes ou d'utilisateurs :

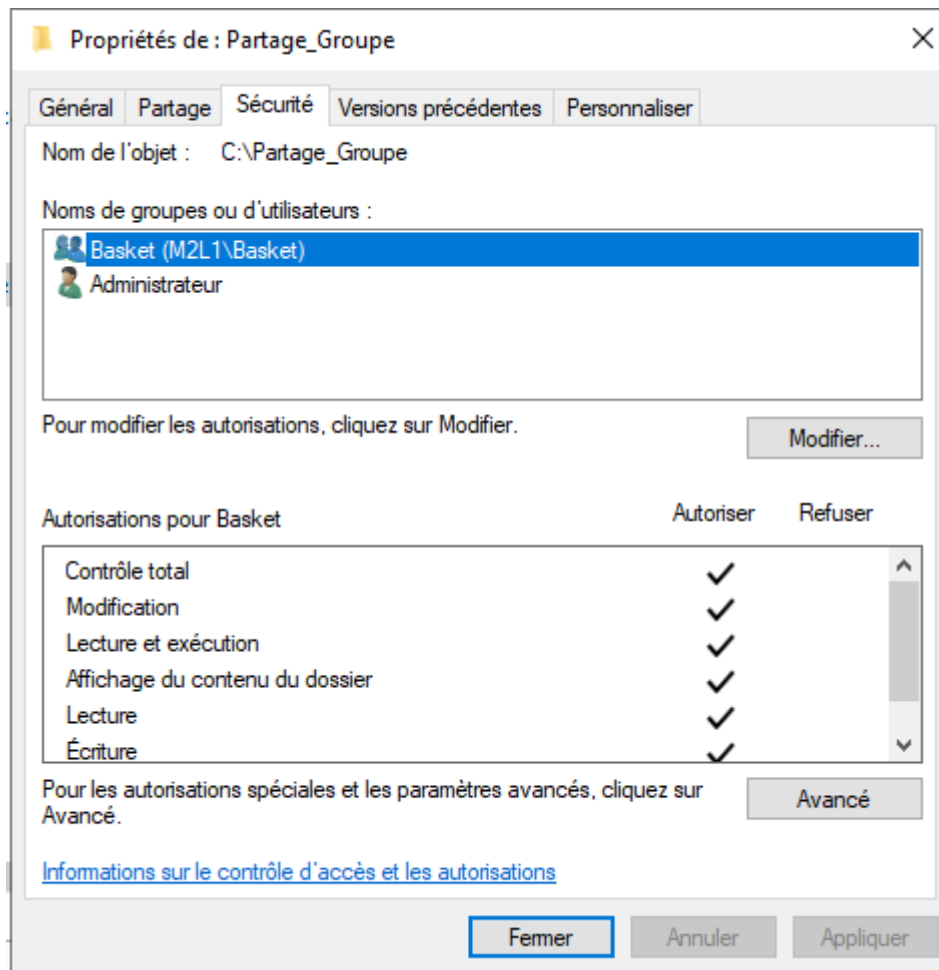
Basket (M2L1\Basket)

Ajouter... Supprimer

Autorisations pour Basket

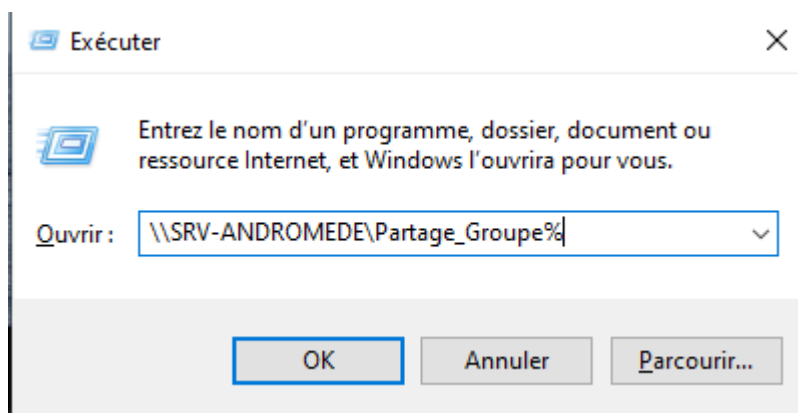
	Autoriser	Refuser
Contrôle total	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modifier	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lecture	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Puis aller dans Sécurité et mettre Administrateur et le groupe en question avec un contrôle total.

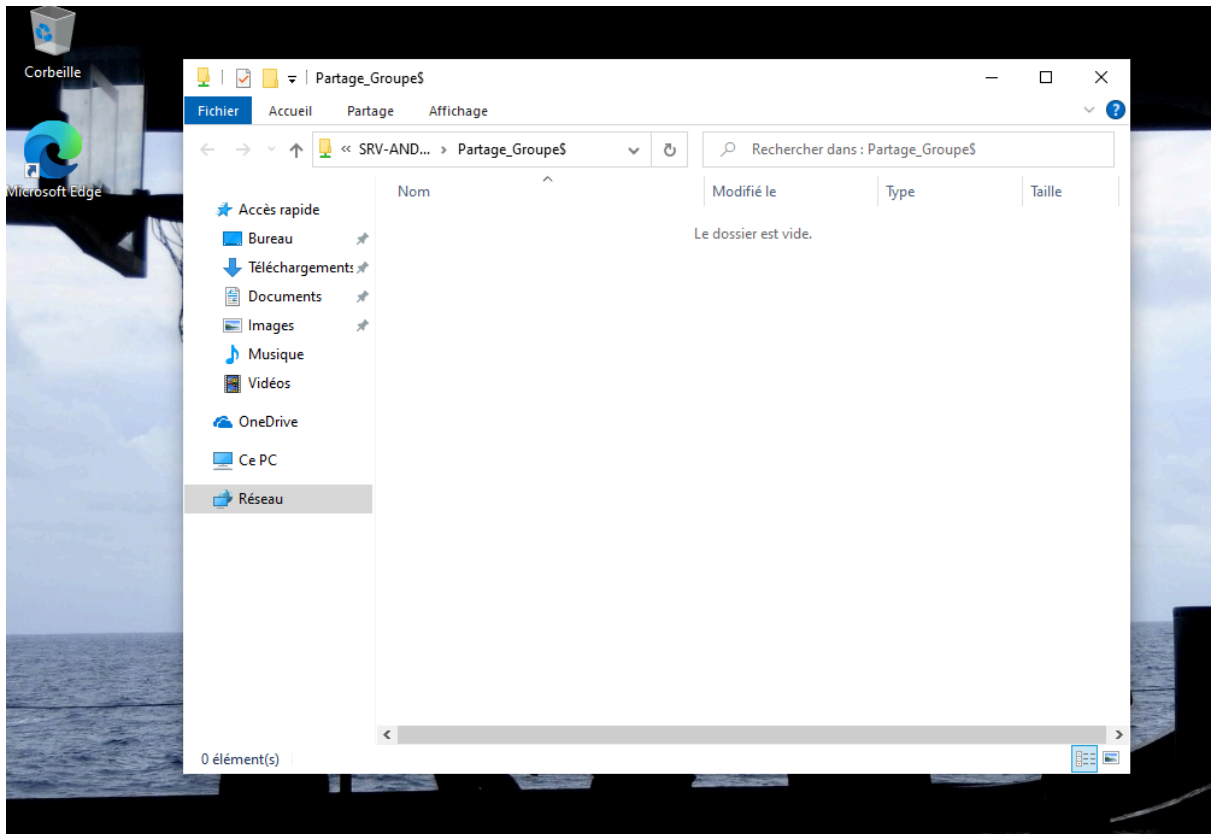


Aller sur un utilisateur de Basket (User 10 par exemple)

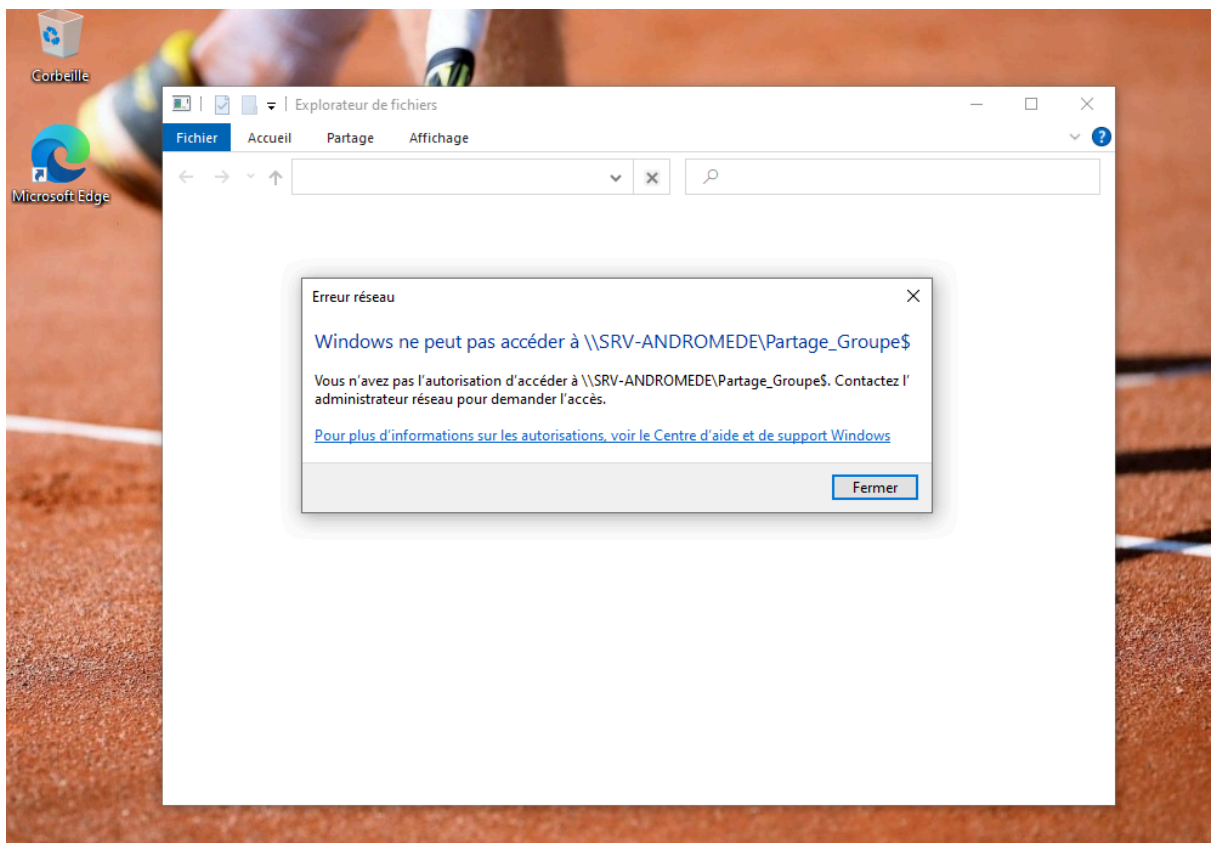
Win+r



On a bien accès au dossier, avec un contrôle total



**Même essai avec un utilisateur de Tennis(User20 par exemple)**

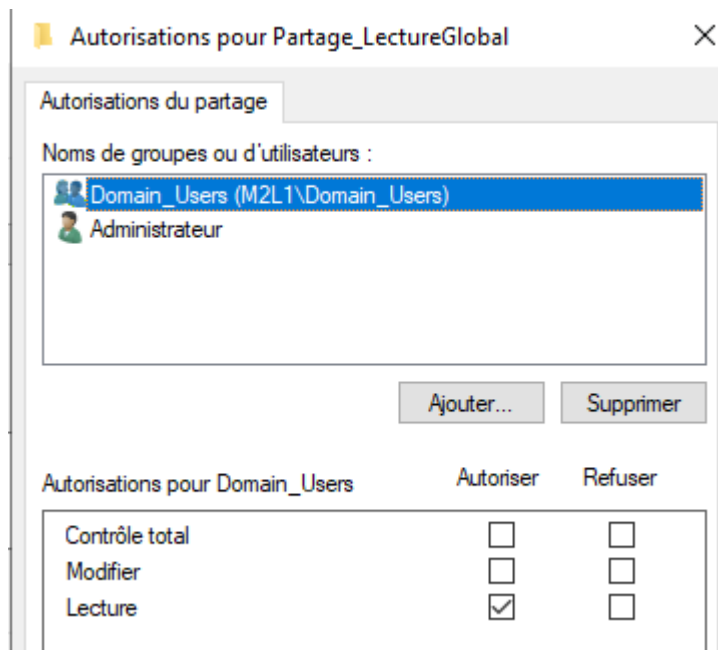
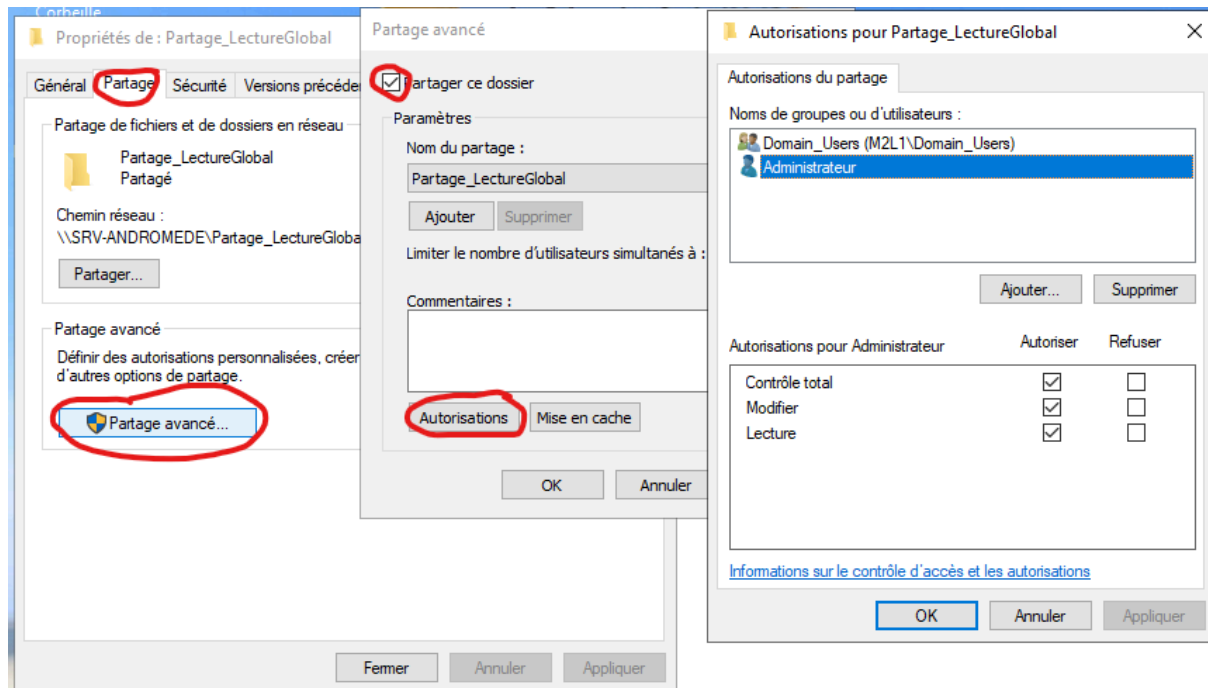




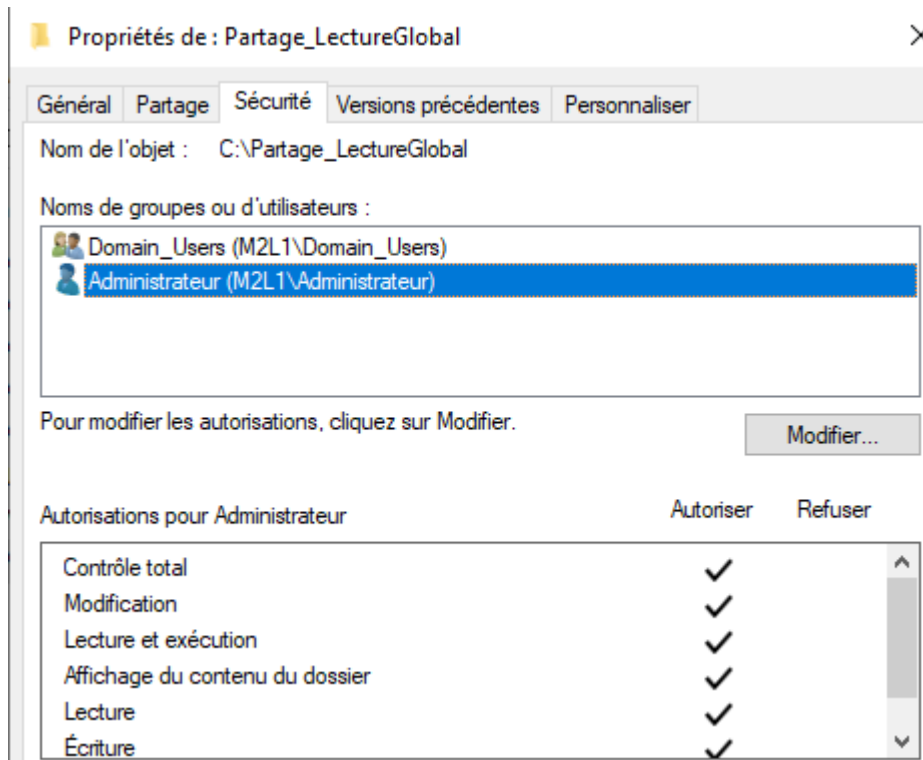
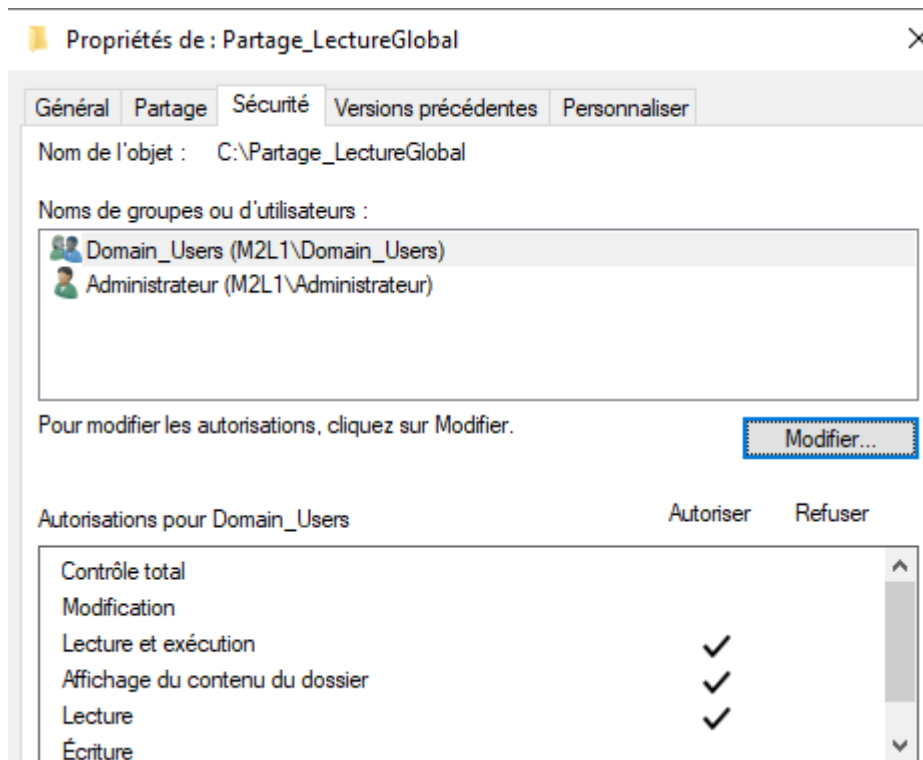
## Partage 2 Lecture Global

Les utilisateurs du domaine (sauf Administrateur) ont été ajouté dans un groupe: "Domain\_Users"

Créer un dossier sur C: puis:

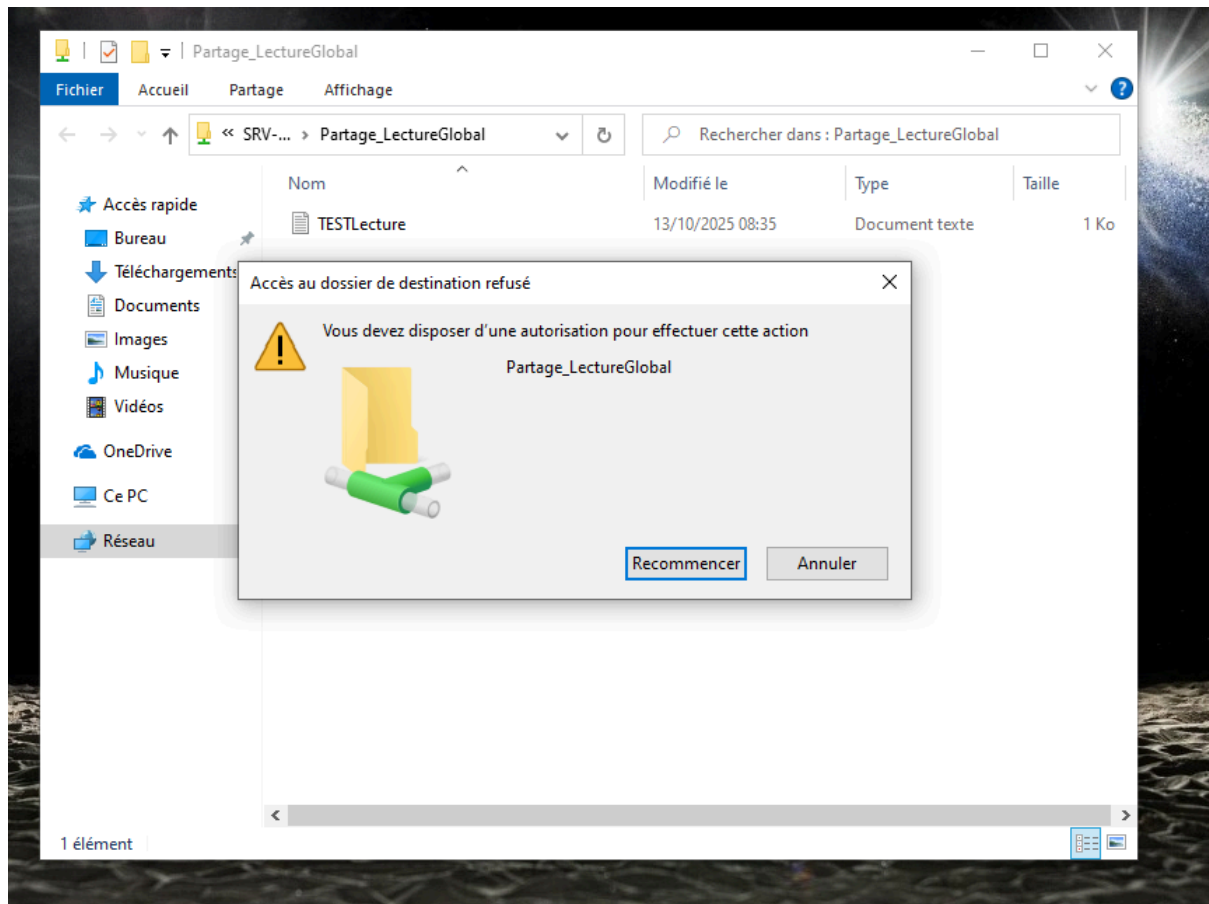


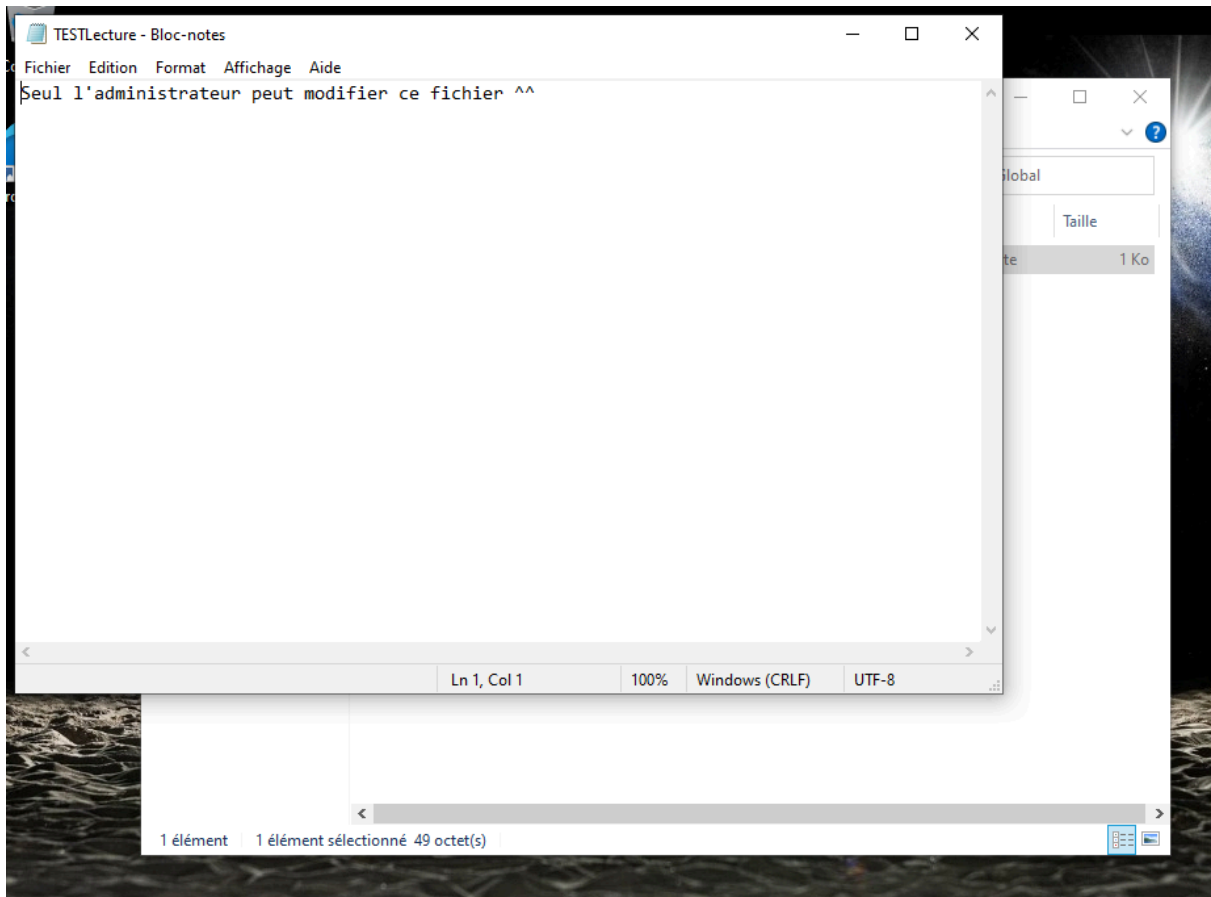
## Puis aller dans l'onglet **Sécurité**



Test depuis User40:

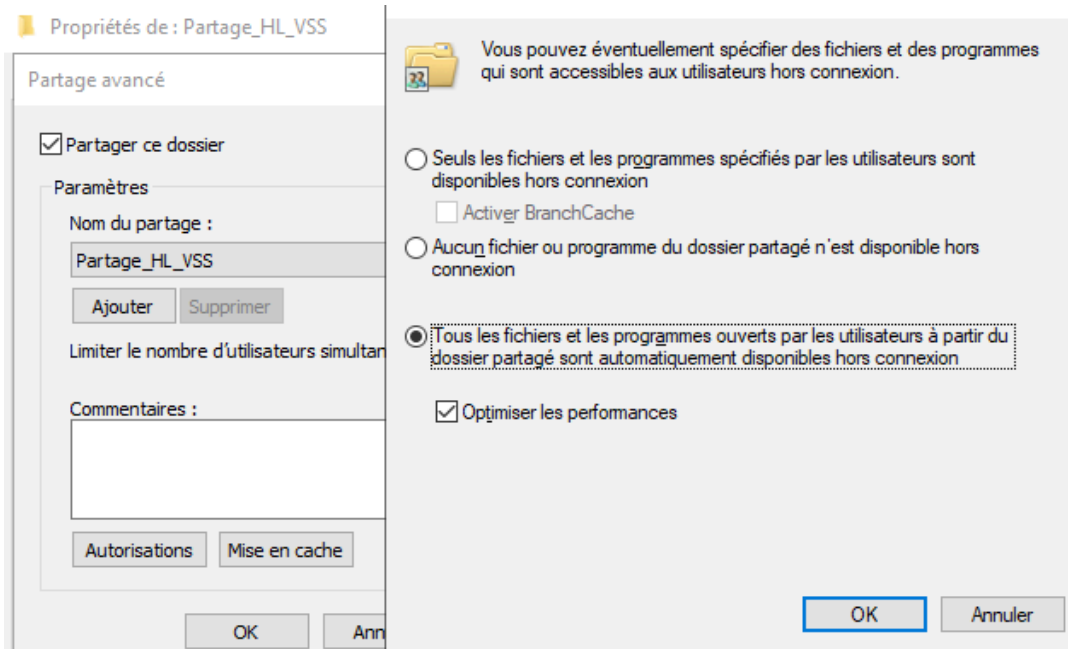
Impossible de créer un nouveau fichier dans le dossier mais nous pouvons lire le fichier TESTLect



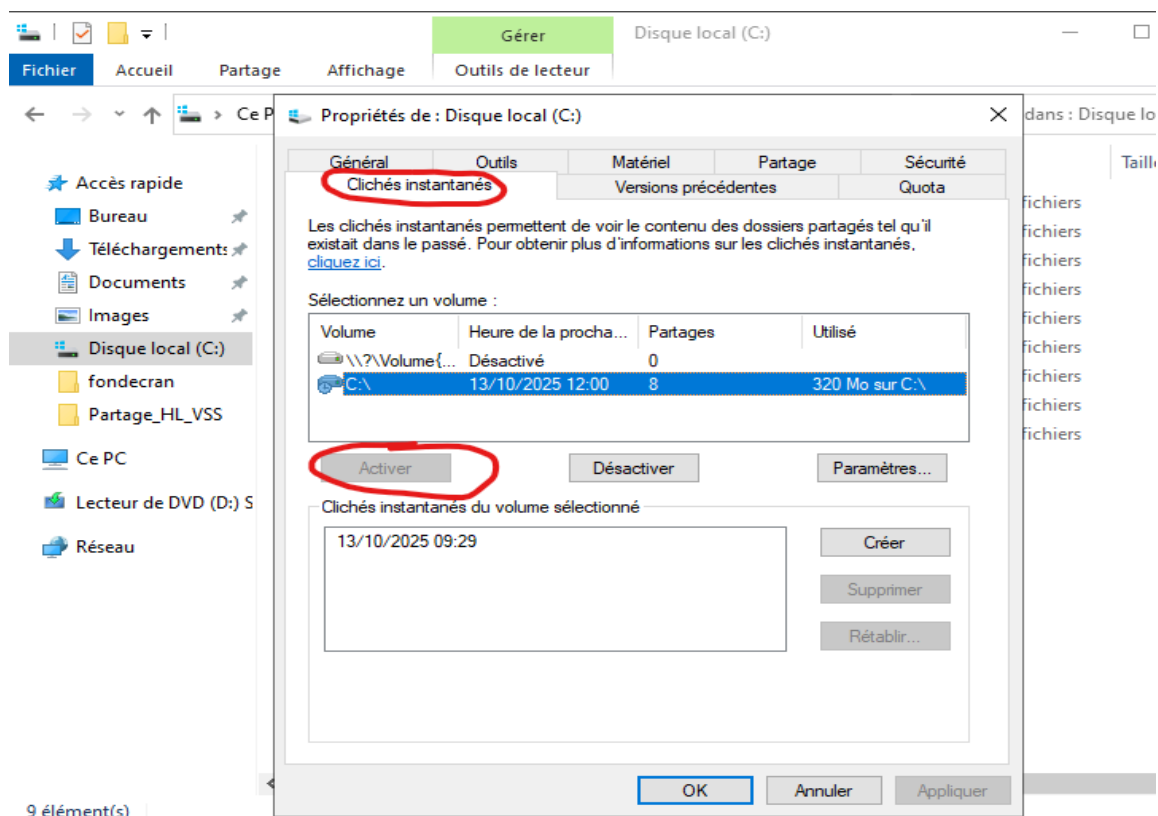


## Partage 3 Hors ligne + VSS

Créer un nouveau dossier dans C: puis donner les autorisations comme au partage précédent puis cliquer sur Mise en cache



Aller dans l'explorateur de fichier, clique droit sur le disque C:, **Propriétés**




Sur User40 j'accède au dossier et je vois deux fichiers txt. Clique droit sur un seul fichier par exemple Test3 → Toujours disponible hors connexion

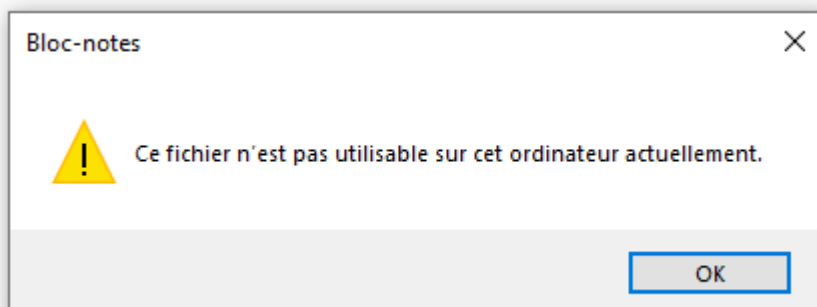
Un petit icône vert apparaît !

 nvtest	13/10/2025 09:33	Document texte	1 Ko
 Test3	13/10/2025 09:28	Document texte	1 Ko

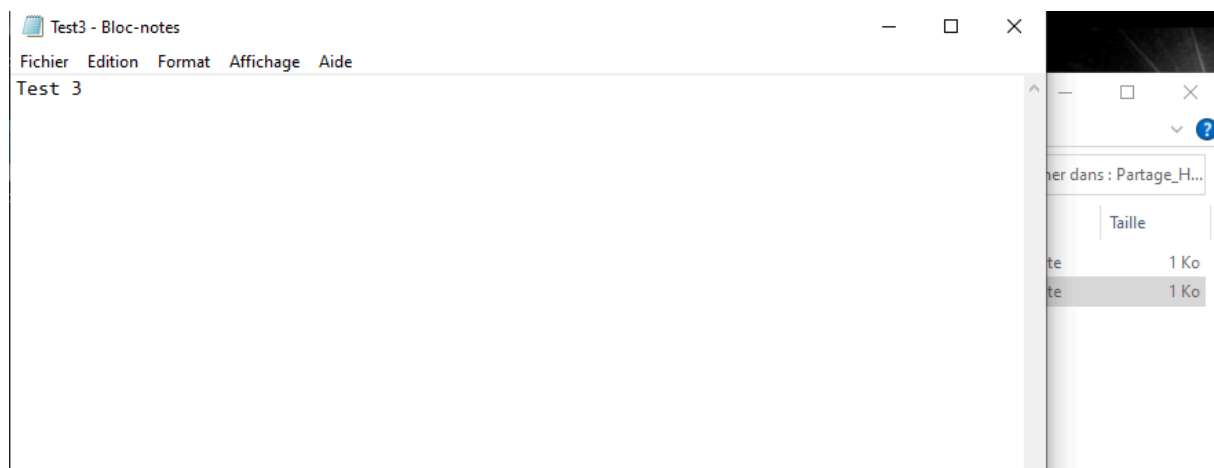
Je désactive ensuite la carte réseau et j'accède à nouveau au dossier:

 nvtest	13/10/2025 09:33	Document texte	1 Ko
 Test3	13/10/2025 09:28	Document texte	1 Ko

Désormais on a une croix grise qui est apparue sur nvtest. Lorsque l'on essaye de l'ouvrir:



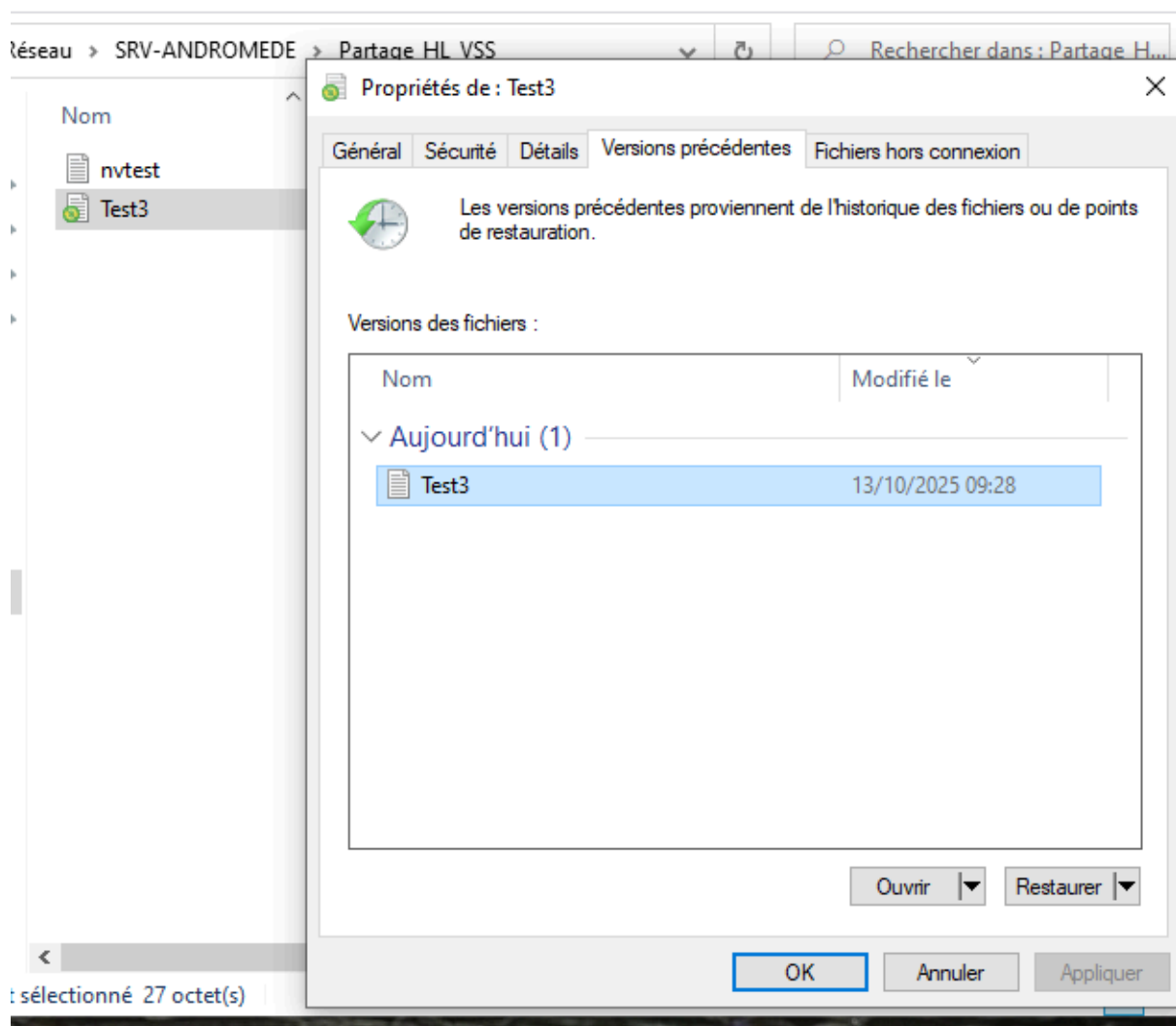
Et quand on ouvre Test3, la dernière version sauvegardé s'affiche:



**La connexion Hors ligne fonctionne bien !**

**Maintenant j'active à nouveau la carte réseau et je modifie le contenu du fichier Test3 via le compte Administrateur.**

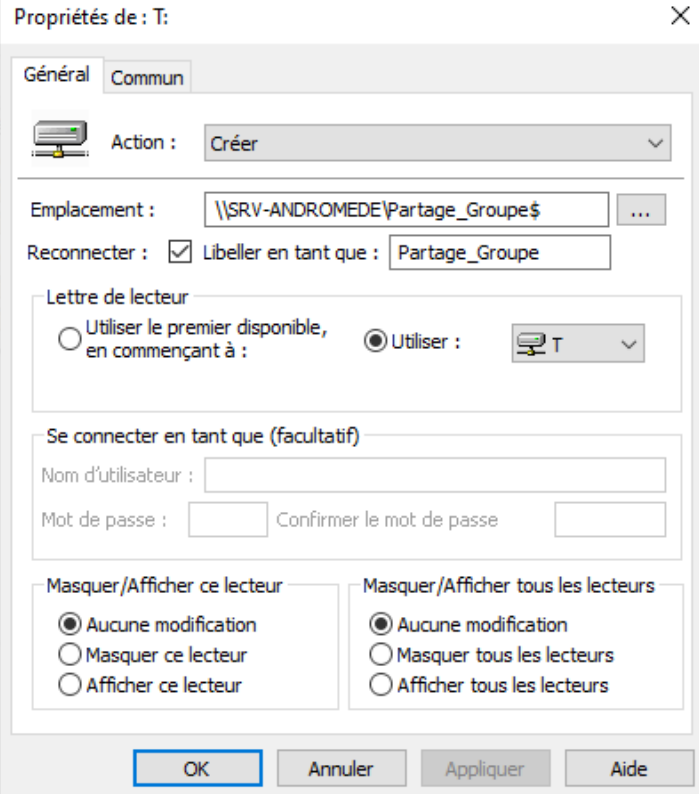
**Je retourne sur le dossier via User40, clique droit sur le fichier Test3, Version précédentes:**



**On a bien une version précédente qui est disponible. (VSS fonctionne)**

## Lecteur Réseau automatique

**Créer une nouvelle GPO, modifier-la et aller dans Configuration utilisateur → Préférences → Paramètres Windows → Mappages de lecteurs → Clique droit → Nouveau → Lecteur mappé**



The screenshot shows the 'Propriétés de : T:' dialog box with the 'Commun' tab selected. The 'Action' dropdown is set to 'Créer'. The 'Emplacement' field contains '\\SRV-ANDROMEDE\Partage\_Groupe\$'. The 'Reconnecter' checkbox is checked, and the 'Libeller en tant que' field contains 'Partage\_Groupe'. Under 'Lettre de lecteur', the 'Utiliser' radio button is selected, and the letter 'T' is chosen from the dropdown. The 'Se connecter en tant que (facultatif)' section has empty fields for 'Nom d'utilisateur' and 'Mot de passe'. At the bottom, there are four buttons: 'OK', 'Annuler', 'Appliquer', and 'Aide'.

Propriétés de : T: X

Général Commun

Action : Créer

Emplacement : \\SRV-ANDROMEDE\Partage\_Groupe\$ ...

Reconnecter : ☒ Libeller en tant que : Partage\_Groupe

Lettre de lecteur

☐ Utiliser le premier disponible, en commençant à : ☐ Utiliser : T

Se connecter en tant que (facultatif)

Nom d'utilisateur :

Mot de passe :  Confirmer le mot de passe

Masquer/Afficher ce lecteur

☒ Aucune modification  
☐ Masquer ce lecteur  
☐ Afficher ce lecteur

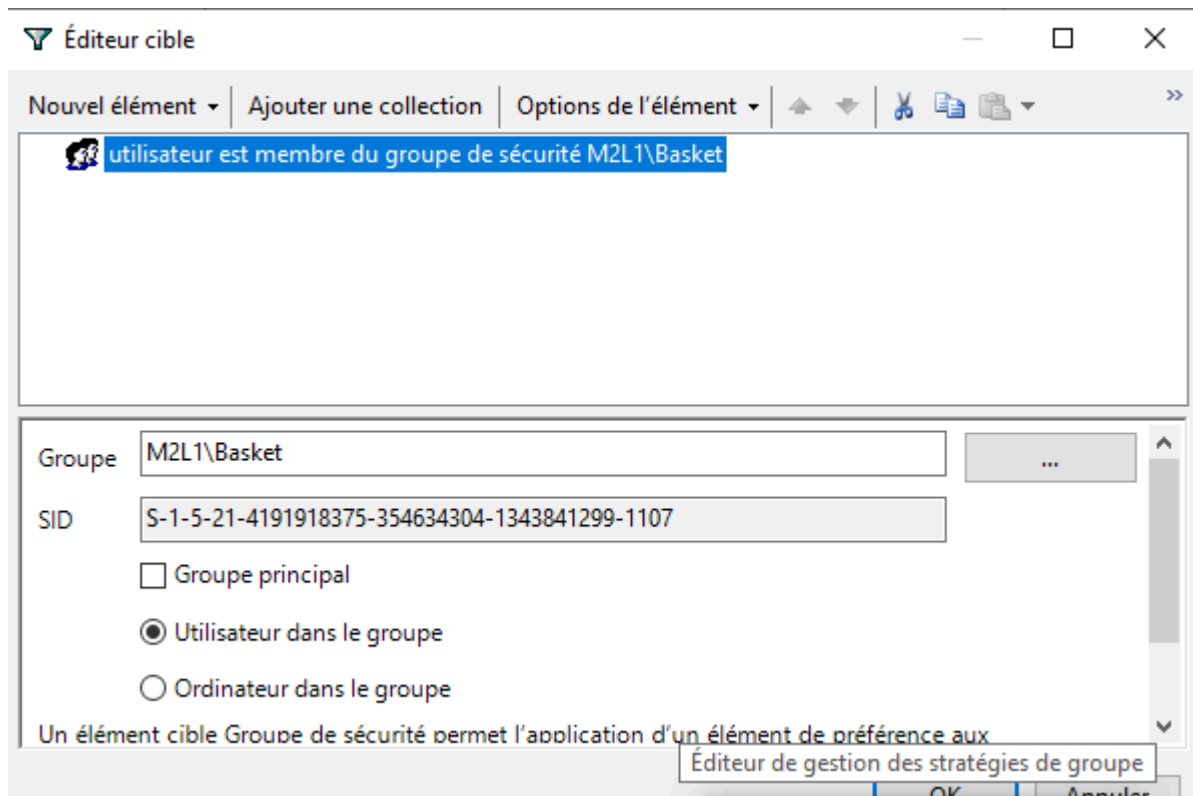
Masquer/Afficher tous les lecteurs

☒ Aucune modification  
☐ Masquer tous les lecteurs  
☐ Afficher tous les lecteurs

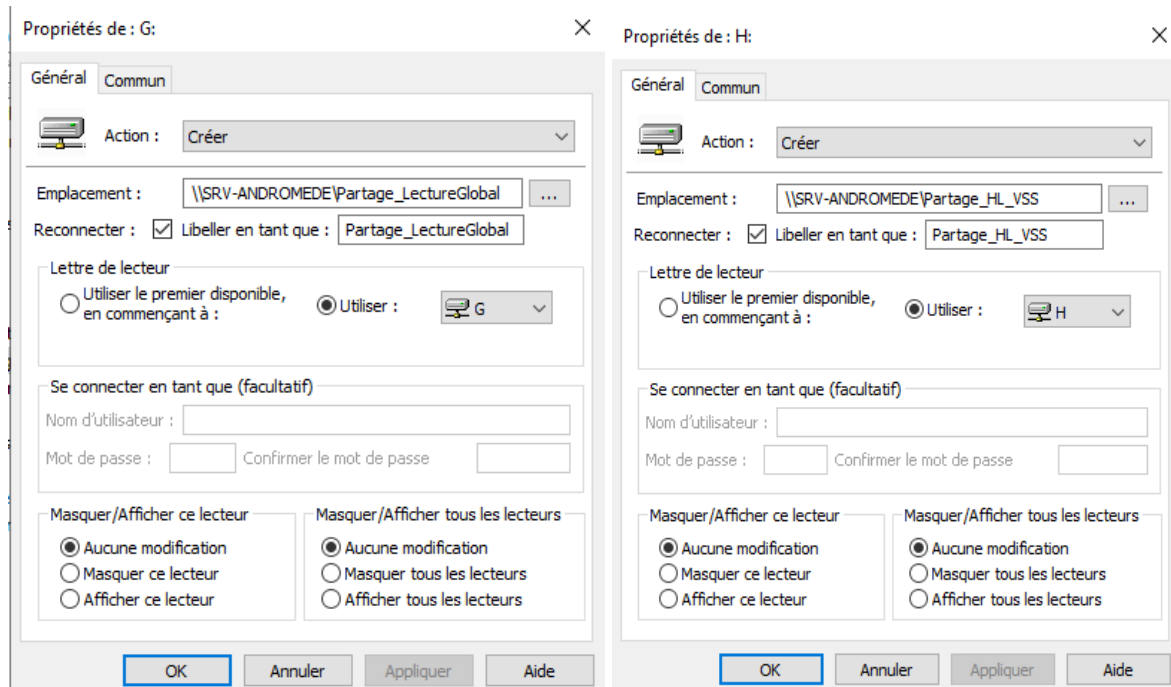
OK Annuler Appliquer Aide

**Dans onglet Commun, Ciblage au niveau de l'élément puis Ciblage. Mettre le groupe Basket.**

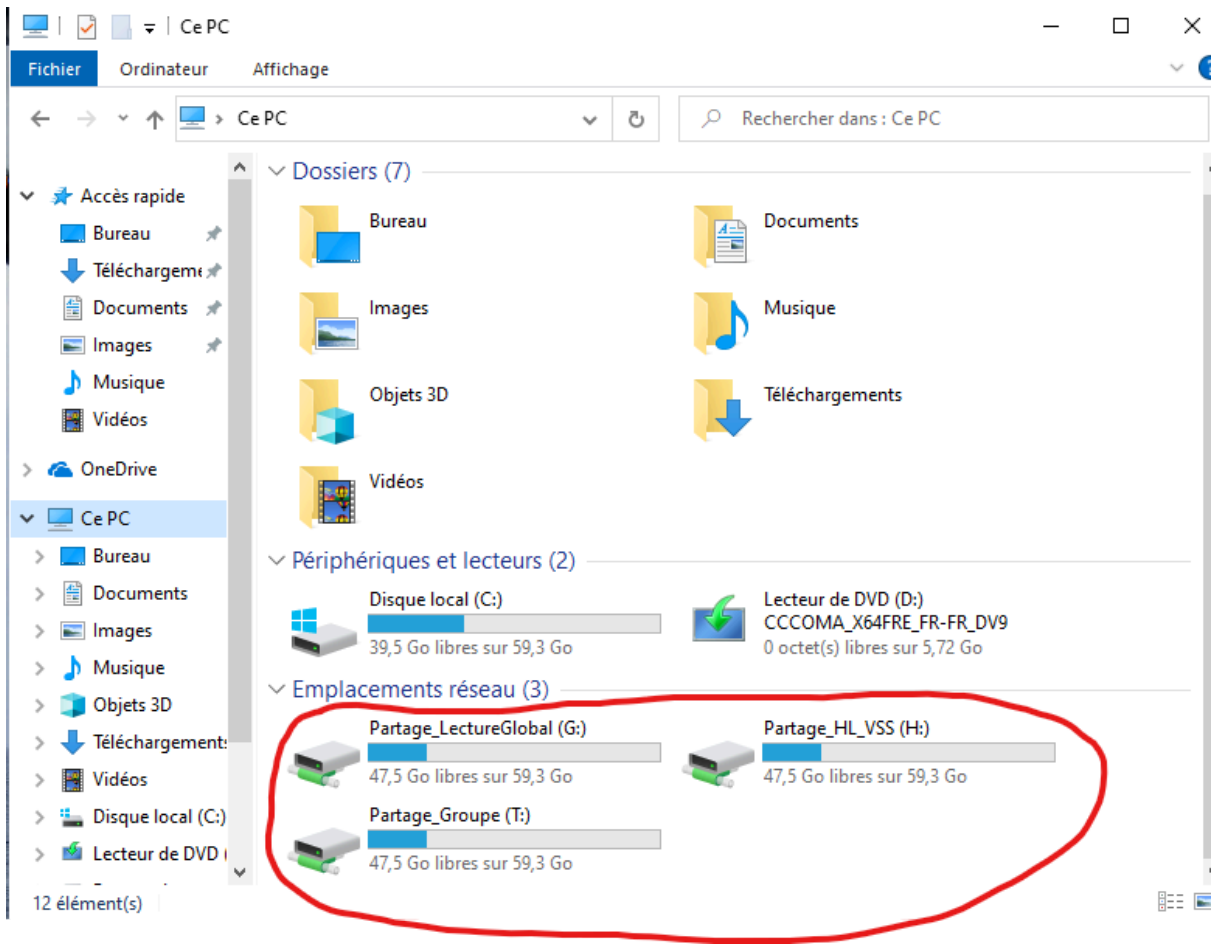




## Faire un nouveau Lecteur mappé pour le partage 2(G:) et 3(H:)



Test sur User10:





Lecteur G: Partage 2

 TESTLecture	13/10/2025 08:35	Document texte	1 Ko
---	------------------	----------------	------

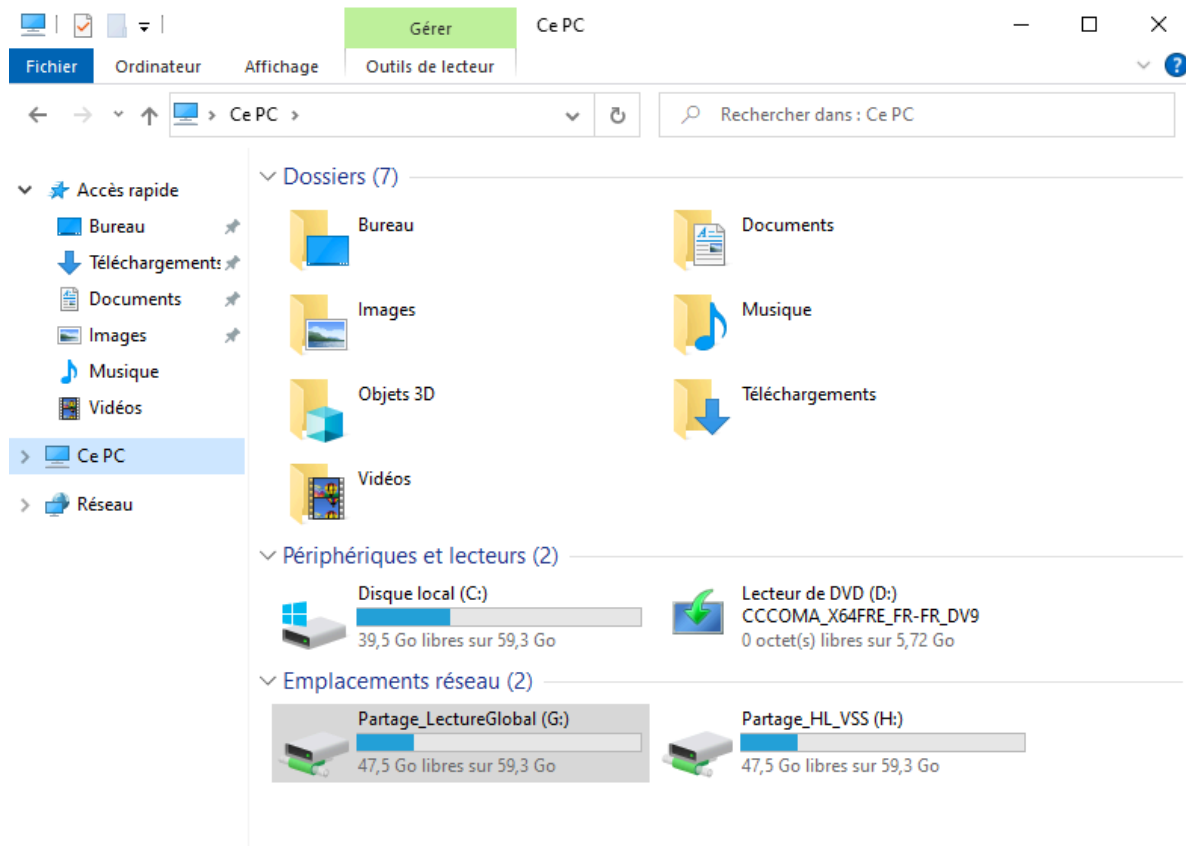
Lecteur T: Partage 1

 teets	14/10/2025 14:17	Document texte	1 Ko
---	------------------	----------------	------

Lecteur H: Partage 3

 nvtest	13/10/2025 09:33	Document texte	1 Ko
 Test3	13/10/2025 10:10	Document texte	1 Ko

## Test sur User30 qui ne voit lecteur T étant donné qu'il n'est partagé que pour le groupe Basket:



## Script: à mettre dans powershell

### Pour partager le script entre la VM et le pc installer VMware Tools

# Charger le module Active Directory

```
Import-Module ActiveDirectory
```

# Chemin vers le fichier CSV (converti depuis Excel)

```
$CSVPath = "C:\Users\Administrateur\Documents\ListeUser.csv"
```

# Importer les utilisateurs depuis le CSV

```
$users = Import-Csv -Path $CSVPath
```

# Chemin de création des utilisateurs (racine du domaine)

```
$OU = "DC=m2l1,DC=lan"
```

```
# Mot de passe par défaut
```

```
$DefaultPassword = "Azerty11"
```

```
# Fonction pour nettoyer le téléphone
```

```
function Clean-Phone($phone) {
```

```
    if ($phone) { return ($phone -replace '[^0-9\+\s\-\,]', '') } else { return "" }
```

```
}
```

```
# Fonction pour nettoyer le code postal
```

```
function Clean-PostalCode($cp) {
```

```
    if ($cp) { return ($cp -replace '[^0-9A-Za-z]', '') } else { return "" }
```

```
}
```

```
# Boucle sur chaque utilisateur
```

```
foreach ($user in $users) {
```

```
    # Vérifie que les champs nécessaires existent
```

```
    if (-not $user.Prenom -or -not $user.Nom) {
```

```
        Write-Host " ⚠ Champs Prénom ou Nom manquant pour une ligne, passage au suivant."
        -ForegroundColor Yellow
```

```
        continue
```

```
    }
```

```
$prenom = $user.Prenom.Trim()
```

```
$nom = $user.Nom.Trim()
```

```
$sam = ($prenom + "." + $nom).ToLower()
```

```
$upn = "$sam@m2l1.lan"
```

```
# Vérifie si l'utilisateur existe déjà
```

```
if (Get-ADUser -Filter { SamAccountName -eq $sam } -ErrorAction SilentlyContinue) {
```

```
    Write-Host " ⚠ L'utilisateur $sam existe déjà, passage au suivant." -ForegroundColor Yellow  
    continue  
}
```

```
# Création minimale de l'utilisateur
```

```
try {
```

```
    New-ADUser `
```

```
        -SamAccountName $sam `
```

```
        -UserPrincipalName $upn `
```

```
        -Name "$prenom $nom" `
```

```
        -GivenName $prenom `
```

```
        -Surname $nom `
```

```
        -DisplayName "$prenom $nom" `
```

```
        -Title $user.Type `
```

```
        -EmployeeID $user.ID `
```

```
        -Description $user.IDescription `
```

```
        -OfficePhone (Clean-Phone $user.Tel) `
```

```
        -StreetAddress $user.Rue `
```

```
        -City $user.Ville `
```

```
        -PostalCode (Clean-PostalCode $user.CP) `
```

```
        -Path $OU `
```

```
        -AccountPassword (ConvertTo-SecureString $DefaultPassword -AsPlainText -Force) `
```

```
        -ChangePasswordAtLogon $true `
```

```
        -Enabled $true
```

```

Write-Host "✅ Utilisateur créé : $prenom $nom" -ForegroundColor Green
}

catch {

    Write-Host "❌ Erreur création utilisateur $prenom $nom : $_" -ForegroundColor Red

    continue

}

# Ajout au groupe selon le secteur (avec DN complet)

switch -Regex ($user.Secteur) {

    "Volley"    { $GroupDN = "CN=Volley,OU=OU_Volley,DC=m2l1,DC=lan" }

    "Basket"    { $GroupDN = "CN=Basket,OU=OU_Basket,DC=m2l1,DC=lan" }

    "Handball"  { $GroupDN = "CN=Handball,OU=OU_Handball,DC=m2l1,DC=lan" }

    "Danse"     { $GroupDN = "CN=Danse,OU=OU_Danse,DC=m2l1,DC=lan" }

    "Direction" { $GroupDN = "CN=Direction,OU=OU_Direction,DC=m2l1,DC=lan" }

    default     { $GroupDN = $null }

}

if ($GroupDN) {

    try {

        Add-ADGroupMember -Identity $GroupDN -Members $sam

        Write-Host "✅ $sam ajouté au groupe $($user.Secteur)" -ForegroundColor Green

    }

    catch {

        Write-Host "❌ Erreur ajout de $sam au groupe $($user.Secteur) : $_" -ForegroundColor Red

    }

} else {

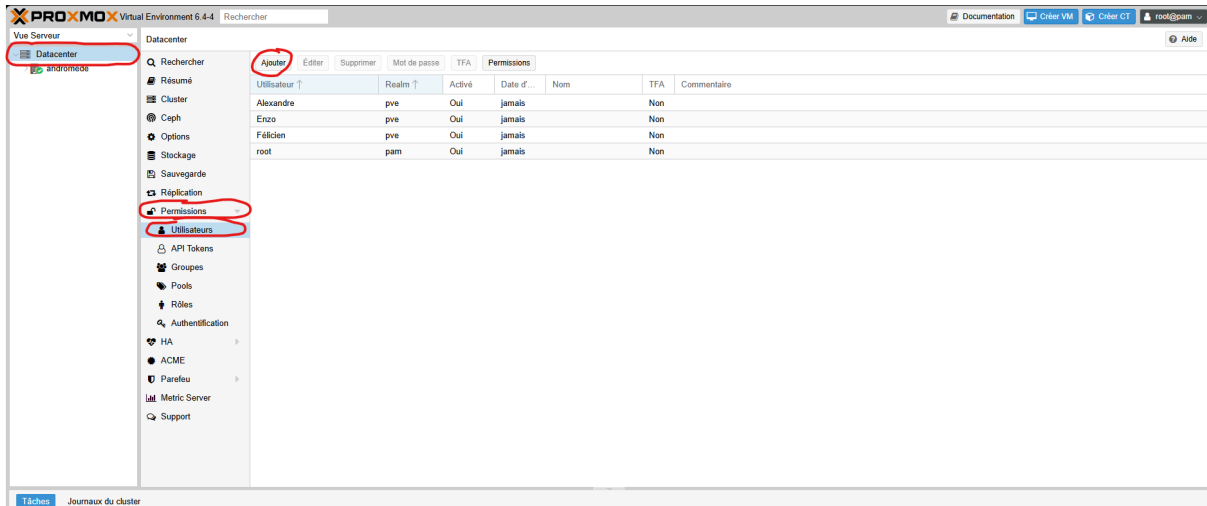
    Write-Host "⚠️ Aucun groupe trouvé pour $sam ($($user.Secteur))" -ForegroundColor Yellow
}

```

}

}

Pour créer des utilisateurs (Admin) dans proxmox il suffit de commencer par créer les utilisateurs voulu comme ceci Datacenter > permissions > Utilisateurs > Ajouter



**Ajouter: Utilisateur**

Utilisateur:  Prénom:

Realm: Proxmox VE authentica Nom:

Mot de passe:  E-Mail:

Confirmer le mot de passe:

Groupe:

Date d'expiration: never

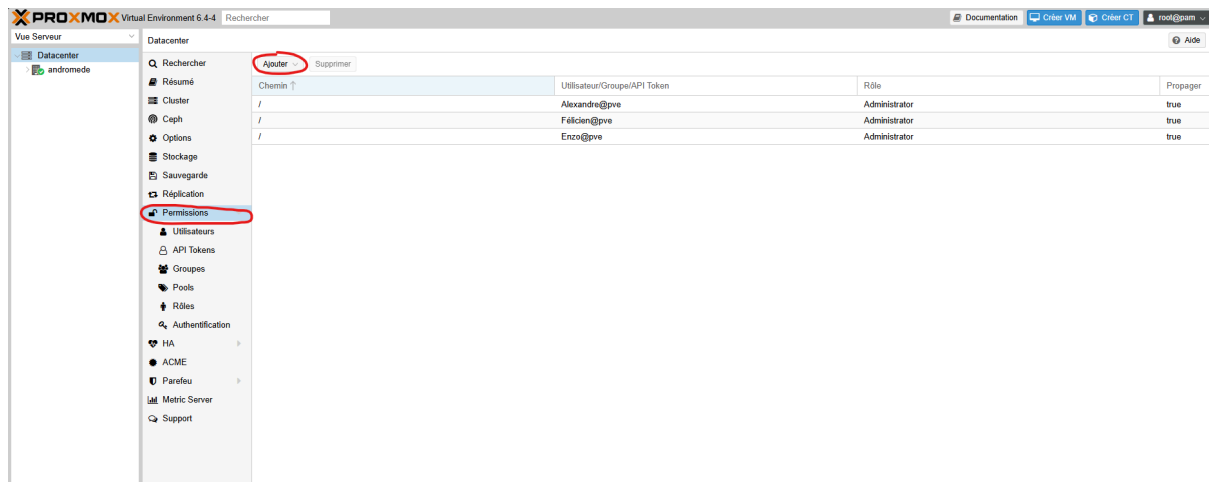
Activé: ☒

Commentaire:

Avancé ☐ **Ajouter**

Puis lui donner un Nom d'utilisateur et un mot de passe.

Pour ajouter des permissions aux utilisateurs aller dans Datacenter > Permissions > Ajouter



Puis sélectionner le chemin racine l'utilisateur dont nous voulons modifier les permissions et en rôle Administrator.

Ajouter: Permissions de l'utilisateur

Chemin: /

Utilisateur: Enzo@pve

Rôle: Administrator

Propager: ☒

Aide Ajouter



# Docu Routeur

```
! =====
! CONFIGURATION ROUTEUR SOLEIL
! =====
```

```
enable
configure terminal
```

```
hostname Soleil          ! Nom du routeur
no ip domain-lookup      ! Désactive la résolution DNS inutile
```

```
banner motd #
Accès réservé aux administrateurs autorisés.
#                       ! Message d'avertissement d'accès
```

```
clock timezone CET 1 0    ! Configure le fuseau horaire
exit
```

```
! --- Sécurité et utilisateur ---
configure terminal
username Administrateur privilege 15 secret Azerty11
! Créer un utilisateur administrateur avec mot de passe chiffré et privilège maximal
```

```
! --- Configuration SSH sécurisée ---
ip domain-name m2l1.lan
crypto key generate rsa modulus 4096  ! Génère une clé RSA pour SSH (4096 bits)
ip ssh version 2                      ! Force SSH version 2
ip ssh time-out 60                    ! Timeout SSH de 60 secondes
ip ssh authentication-retries 2       ! Deux tentatives d'authentification max
```

```
line vty 0 4
transport input ssh                ! Autorise uniquement SSH (pas Telnet)
login local                        ! Utilise la base d'utilisateurs locale
exec-timeout 10 0                  ! Déconnexion automatique après 10 minutes
exit
end
```

```
! --- Configuration des interfaces VLANs (Trunk et sous-interfaces) ---
configure terminal
```

```
interface g0/0/0
no ip address
no shutdown
! Interface principale en mode trunk (pas d'adresse IP)
```

```
! === VLANs et sous-interfaces ===
interface g0/0/0.10
encapsulation dot1Q 10
ip address 172.26.11.60 255.255.255.192
```

```
ip helper-address 172.26.17.1
no shutdown
! VLAN 10 : réseau 172.26.11.0/26
```

```
interface g0/0/0.20
encapsulation dot1Q 20
ip address 172.26.11.92 255.255.255.224
ip helper-address 172.26.17.1
no shutdown
! VLAN 20 : réseau 172.26.11.64/27
```

```
interface g0/0/0.30
encapsulation dot1Q 30
ip address 172.26.11.124 255.255.255.224
ip helper-address 172.26.17.1
no shutdown
! VLAN 30 : réseau 172.26.11.96/27
```

```
interface g0/0/0.80
encapsulation dot1Q 80
ip address 172.26.11.156 255.255.255.224
ip helper-address 172.26.17.1
no shutdown
! VLAN 80 : réseau 172.26.11.128/27
```

```
interface g0/0/0.40
encapsulation dot1Q 40
ip address 172.26.11.172 255.255.255.240
ip helper-address 172.26.17.1
no shutdown
! VLAN 40 : réseau 172.26.11.160/28
```

```
interface g0/0/0.50
encapsulation dot1Q 50
ip address 172.26.11.180 255.255.255.248
ip helper-address 172.26.17.1
no shutdown
! VLAN 50 : réseau 172.26.11.176/29
```

```
interface g0/0/0.60
encapsulation dot1Q 60
ip address 172.26.11.188 255.255.255.248
ip helper-address 172.26.17.1
no shutdown
! VLAN 60 : réseau 172.26.11.184/29
```

```
interface g0/0/0.70
encapsulation dot1Q 70
```

```
ip address 172.26.11.196 255.255.255.248
ip helper-address 172.26.17.1
no shutdown
! VLAN 70 : réseau 172.26.11.192/29
```

```
interface g0/0/0.90
encapsulation dot1Q 90
ip address 172.26.11.204 255.255.255.248
ip helper-address 172.26.17.1
no shutdown
! VLAN 90 : réseau 172.26.11.200/29
```

```
interface g0/0/0.18
encapsulation dot1Q 18
ip address 172.26.11.220 255.255.255.240
ip helper-address 172.26.17.1
no shutdown
! VLAN 18 : réseau 172.26.11.208/28
```

```
interface g0/0/0.100
encapsulation dot1Q 100
ip address 172.26.11.236 255.255.255.240
ip helper-address 172.26.17.1
no shutdown
! VLAN 100 : réseau 172.26.11.224/28
```

```
interface g0/0/0.110
encapsulation dot1Q 110
ip address 172.26.11.244 255.255.255.248
ip helper-address 172.26.17.1
no shutdown
! VLAN 110 : réseau 172.26.11.240/29
```

```
interface g0/0/0.300
encapsulation dot1Q 300
ip address 172.26.13.124 255.255.255.128
ip helper-address 172.26.17.1
no shutdown
! VLAN 300 : réseau 172.26.13.0/25
```

```
interface g0/0/0.15
encapsulation dot1Q 15
ip address 172.26.15.12 255.255.255.240
ip helper-address 172.26.17.1
no shutdown
! VLAN 15 : réseau 172.26.15.0/28
```

```
interface g0/0/0.99
```

```
encapsulation dot1Q 99
ip address 172.26.16.12 255.255.255.240
ip helper-address 172.26.17.1
no shutdown
! VLAN 99 : réseau 172.26.16.0/28
```

```
interface g0/0/0.17
encapsulation dot1Q 17
ip address 172.26.17.12 255.255.255.240
ip helper-address 172.26.17.1
no shutdown
! VLAN 17 : réseau 172.26.17.0/28
```

```
! --- ACL pour NAT ---
access-list 1 permit 172.26.11.0 0.0.0.63
access-list 1 permit 172.26.11.64 0.0.0.31
access-list 1 permit 172.26.11.96 0.0.0.31
access-list 1 permit 172.26.11.128 0.0.0.31
access-list 1 permit 172.26.11.160 0.0.0.15
access-list 1 permit 172.26.11.176 0.0.0.7
access-list 1 permit 172.26.11.184 0.0.0.7
access-list 1 permit 172.26.11.192 0.0.0.7
access-list 1 permit 172.26.11.200 0.0.0.7
access-list 1 permit 172.26.11.208 0.0.0.15
access-list 1 permit 172.26.11.224 0.0.0.15
access-list 1 permit 172.26.11.240 0.0.0.7
access-list 1 permit 172.26.13.0 0.0.0.127
access-list 1 permit 172.26.15.0 0.0.0.15
access-list 1 permit 172.26.16.0 0.0.0.15
access-list 1 permit 172.26.17.0 0.0.0.15
! Autorise les réseaux internes pour la traduction NAT
```

```
ip nat inside source list 1 interface g0/0/1 overload
! PAT (NAT surcharge) vers l'interface externe
```

```
! --- Définition des interfaces NAT ---
interface range g0/0/0.10 - 0.300
ip nat inside
exit
```

```
interface g0/0/1
ip address dhcp
ip nat outside
no shutdown
! Interface WAN externe, reçoit une IP publique via DHCP
```

```
! --- Route par défaut ---
ip route 0.0.0.0 0.0.0.0 172.21.159.254
```

! Route vers la passerelle du FAI

end

write memory

! Sauvegarde de la configuration

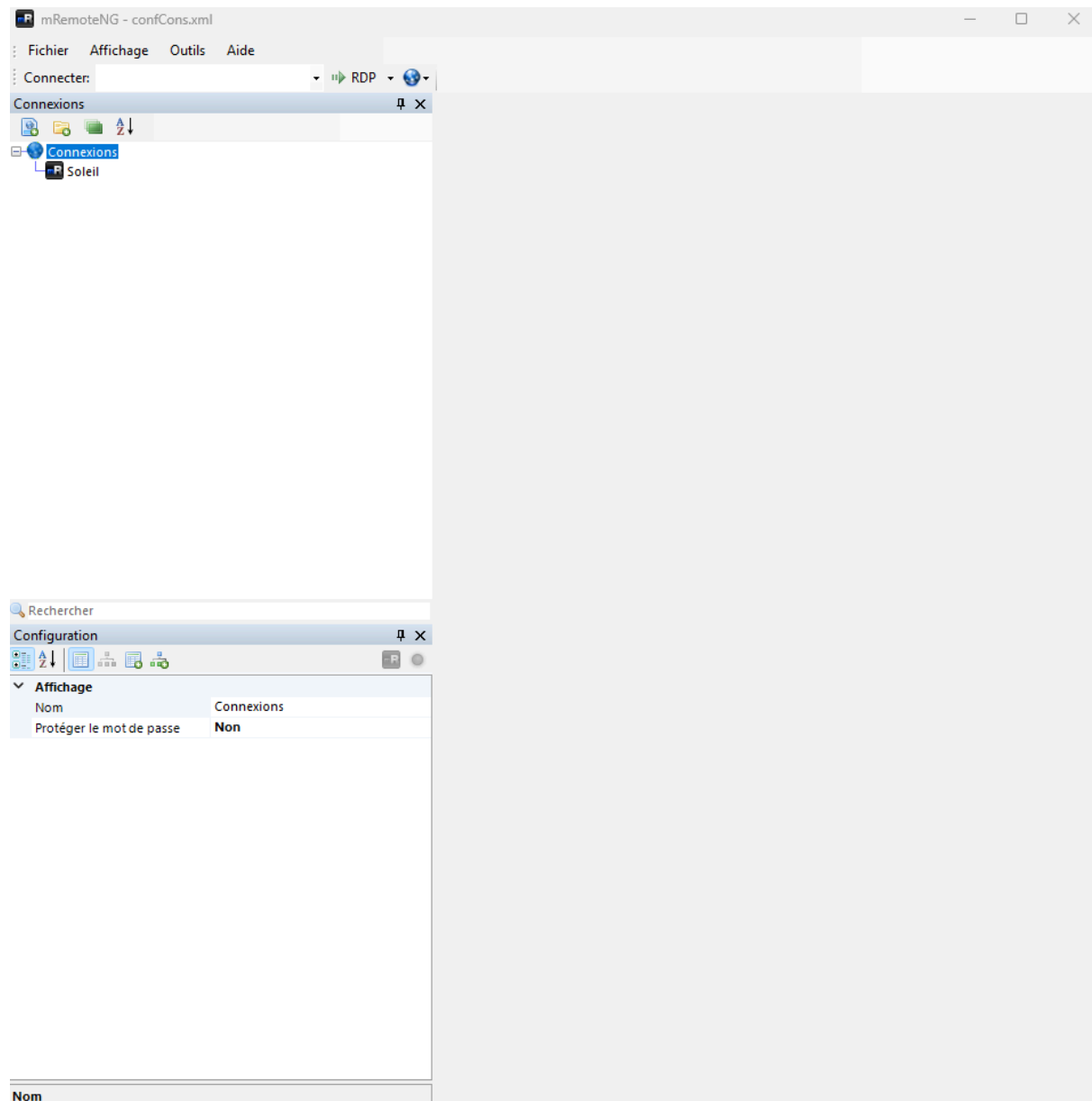
Pour ce qui est de la backup il suffit d'installer TFTP64 comme dans le TP.

Dans le directory on met le répertoire ou le fichier de configuration doit arriver par exemple le bureau.

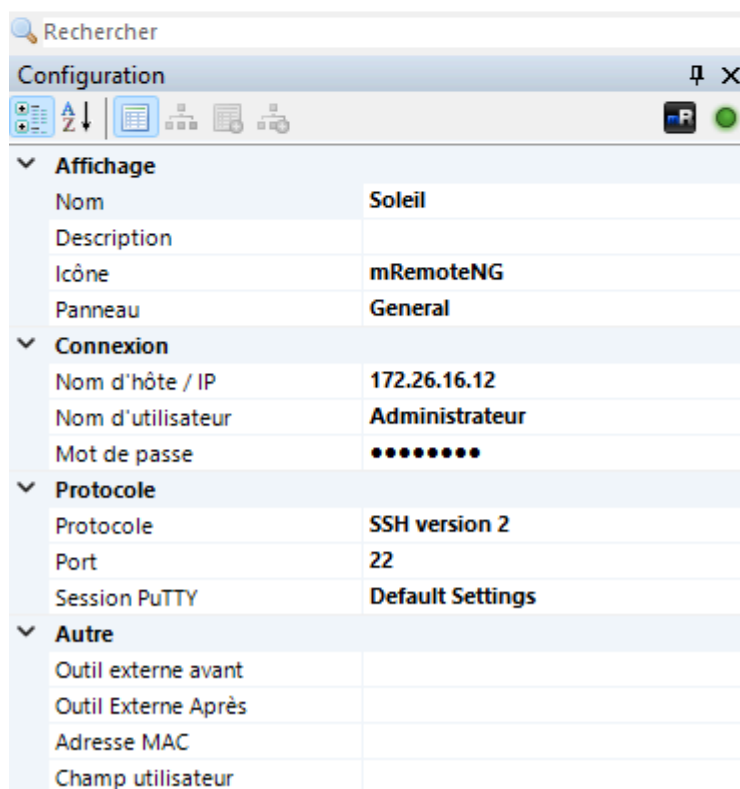
Puis dans le routeur on écrit copy running-config tftp: puis l'ip de la machine hôte.

Pour se connecter en ssh au routeur, j'ai utilisé le logiciel mRemoteNG.

il se présente comme ceci :



pour se connecter au routeur, il faut faire Fichier > ajouter une connexion puis rentrer les différents paramètres :



Nom



Contexte AP

# Contexte du projet

La Maison des Ligues de Lorraine (M2L) héberge différentes ligues sportives régionales et leur fournit un ensemble de services numériques (accès Internet, messagerie, impression, hébergement de serveurs, etc.). Jusqu'à présent, l'ensemble des structures utilisait un **réseau unique**, ce qui entraîne des problèmes de sécurité, en particulier avec la présence de visiteurs connectés via le réseau Wi-Fi et l'utilisation croissante d'équipements mobiles.

Afin d'améliorer la **sécurité, la gestion des flux réseau et la qualité de service**, une réorganisation complète de l'infrastructure informatique est prévue. Ce projet vise notamment à :

- Mettre en place une **segmentation réseau par VLAN** (postes fixes, postes nomades, téléphonie IP) afin de cloisonner les flux.
- Installer un **nouveau domaine Active Directory** sous Windows Server 2025, hébergé sur un hyperviseur Proxmox, pour remplacer l'ancienne architecture et centraliser l'authentification, la gestion des utilisateurs et les services essentiels (AD, DNS, DHCP).
- Mettre en place une politique de **sécurité renforcée** :
  - utilisateurs limités sur leurs postes,
  - stockage des données centralisé et non local,
  - intégration de stratégies de groupe (GPO),
  - détection et correction des vulnérabilités.
- Créer une organisation de **partages réseau** :
  - partages de groupe pour chaque ligue (basket, hand, volley),
  - un partage global réservé à la direction,
  - montage automatique à la connexion des utilisateurs,
  - gestion des accès hors ligne et historisation.
- Sécuriser et administrer le réseau via un **nouveau routeur Cisco** et des commutateurs compatibles 802.1Q.

- Préparer la mise en place d'une **DMZ** pour héberger des services accessibles depuis l'extérieur (notamment un serveur HTTPS).

Dans le cadre de ce projet, il est également demandé de :

- Planifier et documenter l'ensemble des tâches techniques,
- Réaliser un plan de réseau détaillé,
- Fournir des notices techniques (VLAN, sauvegardes de configurations),
- Rédiger un document récapitulatif sur les GPO, scripts et configurations spécifiques,
- Tester l'ensemble de la solution mise en œuvre (séparation des flux, intégration au domaine, accès aux services).

Ce projet s'inscrit dans une démarche de **modernisation et de sécurisation de l'infrastructure IT** de la M2L, afin d'accompagner la croissance des besoins numériques des ligues et de garantir un environnement fiable, évolutif et sécurisé.

# Cahier des charges

# Cahier des charges

## Projet : Mise en place d'un domaine et découpage du réseau – M2L

---

### 1. Présentation du projet

La Maison des Ligues de Lorraine (M2L) héberge de nombreuses ligues sportives régionales et met à leur disposition différents services numériques (accès Internet, impression, téléphonie IP, messagerie, etc.).

Actuellement, l'ensemble des équipements informatiques est relié à un **réseau unique**, ce qui engendre des problèmes de sécurité et de gestion des flux, notamment avec l'usage de postes nomades via le Wi-Fi.

Le projet a pour but de **moderniser et sécuriser l'infrastructure informatique** grâce à la mise en place :

- d'une **segmentation réseau par VLAN**,
  - d'un **nouveau domaine Active Directory sous Windows Server 2025**,
  - d'une **gestion centralisée des utilisateurs et des ressources**,
  - d'une **sécurisation des données et des configurations réseau**.
- 

### 2. Objectifs

- Séparer les flux réseau en plusieurs VLAN (postes fixes, postes nomades, téléphonie IP).
- Créer un **nouveau domaine Active Directory** **m2lX.lan** avec gestion des utilisateurs et des groupes (Basket, Hand, Volley).
- Déployer un **serveur Windows Server 2025** sous Proxmox avec les rôles AD, DNS et DHCP.
- Mettre en place des **partages réseau sécurisés et automatiques** selon les droits des ligues et de la direction.

- Garantir la **sécurité des données** (pas de stockage local, accès hors ligne, historisation).
  - Sauvegarder les configurations routeur/commutateur sur un espace réservé aux administrateurs (serveur + Nextcloud).
  - Identifier et corriger les vulnérabilités Active Directory (via documentation et bonnes pratiques).
- 

### 3. Périmètre du projet

#### Inclus :

- Installation et configuration d'un serveur Windows Server 2025.
- Création et test des VLAN (100 postes fixes, 200 postes nomades, 300 téléphonie IP).
- Mise en place de l'Active Directory, DNS, DHCP.
- Création des utilisateurs et affectation des GPO (fond d'écran, restrictions, droits limités).
- Configuration des partages réseau et automatisation via scripts/GPO.
- Sauvegarde des configurations routeur/commutateur.
- Documentation technique et démonstration finale.

#### Exclus (mais prévus dans missions ultérieures) :

- Mise en place complète de la DMZ et du serveur HTTPS accessible depuis l'extérieur.
  - Déploiement avancé de la QoS pour la téléphonie IP.
- 

### 4. Contraintes

- Utiliser des commutateurs Cisco compatibles 802.1Q.
- Utiliser un routeur Cisco pour la nouvelle architecture.

- Respecter la structure de l'adressage et des VLAN fournis.
  - Utiliser uniquement des images libres de droit pour les fonds d'écran utilisateurs.
  - Les utilisateurs ne doivent pas disposer de droits administrateurs sur leur poste.
  - Toutes les configurations doivent être documentées et sauvegardées.
- 

## 5. Livrables attendus

- **Plan de réseau détaillé** (réalisé sous Visio).
  - **Notice technique VLAN** (configuration + tests).
  - **Notice technique sauvegarde switch/routeur.**
  - **Documentation GPO et scripts** (restrictions, montage automatique des partages, configuration spécifique).
  - **Rapport sur les vulnérabilités Active Directory** et les solutions proposées.
  - **Présentation orale et démonstration** de la solution (intégration postes au domaine, tests VLAN, séparation des flux, accès HTTPS en DMZ).
- 

## 6. Validation et réception

La validation se fera lors d'une **démonstration pratique** devant le professeur, comprenant :

- Connexion au réseau depuis postes fixes et nomades.
- Intégration de postes Windows 10/11 au domaine.
- Accès par comptes utilisateurs avec fonds d'écran spécifiques et restrictions.
- Accès aux partages réseau selon droits.
- Preuve de la séparation des flux VLAN.
- Accès à l'URL HTTPS en DMZ (si inclus).
- Vérification des sauvegardes de configurations.





# Schéma réseau physique

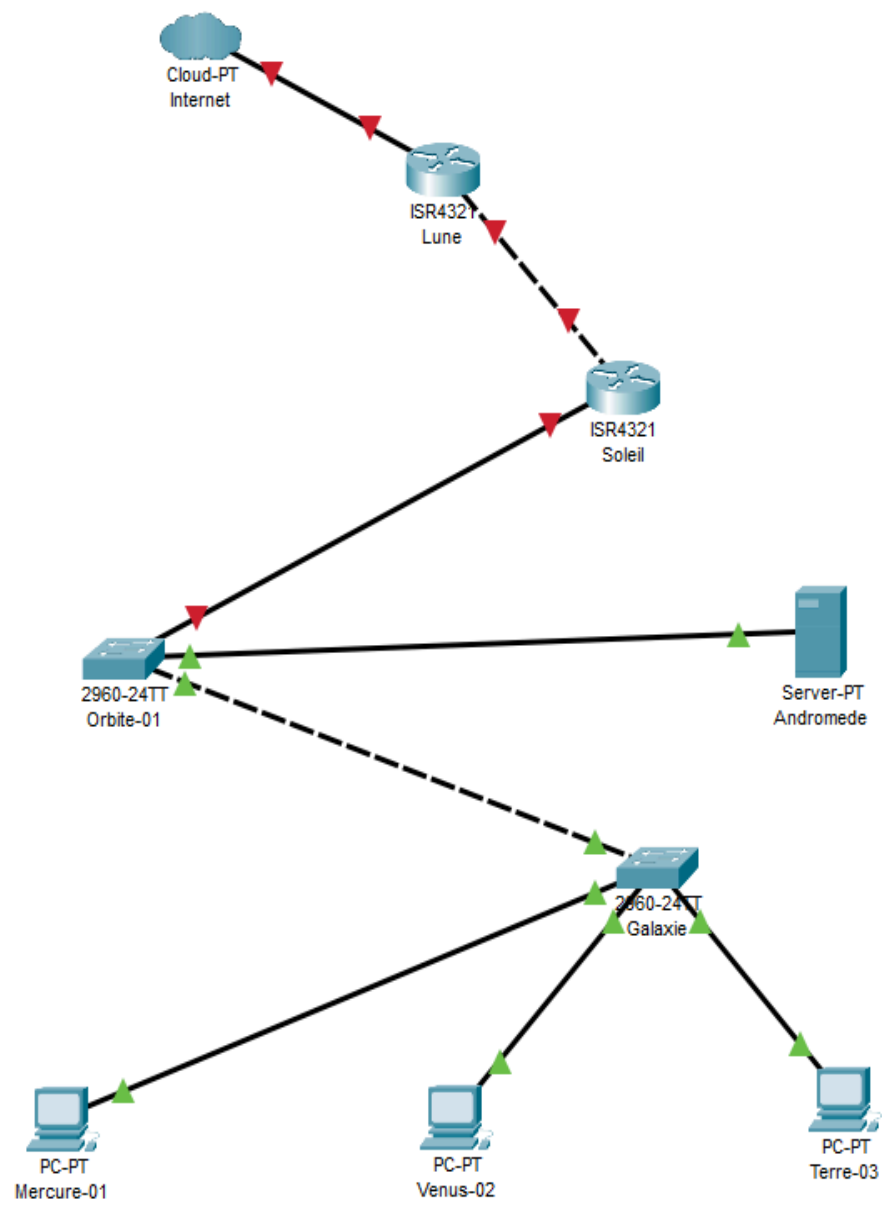
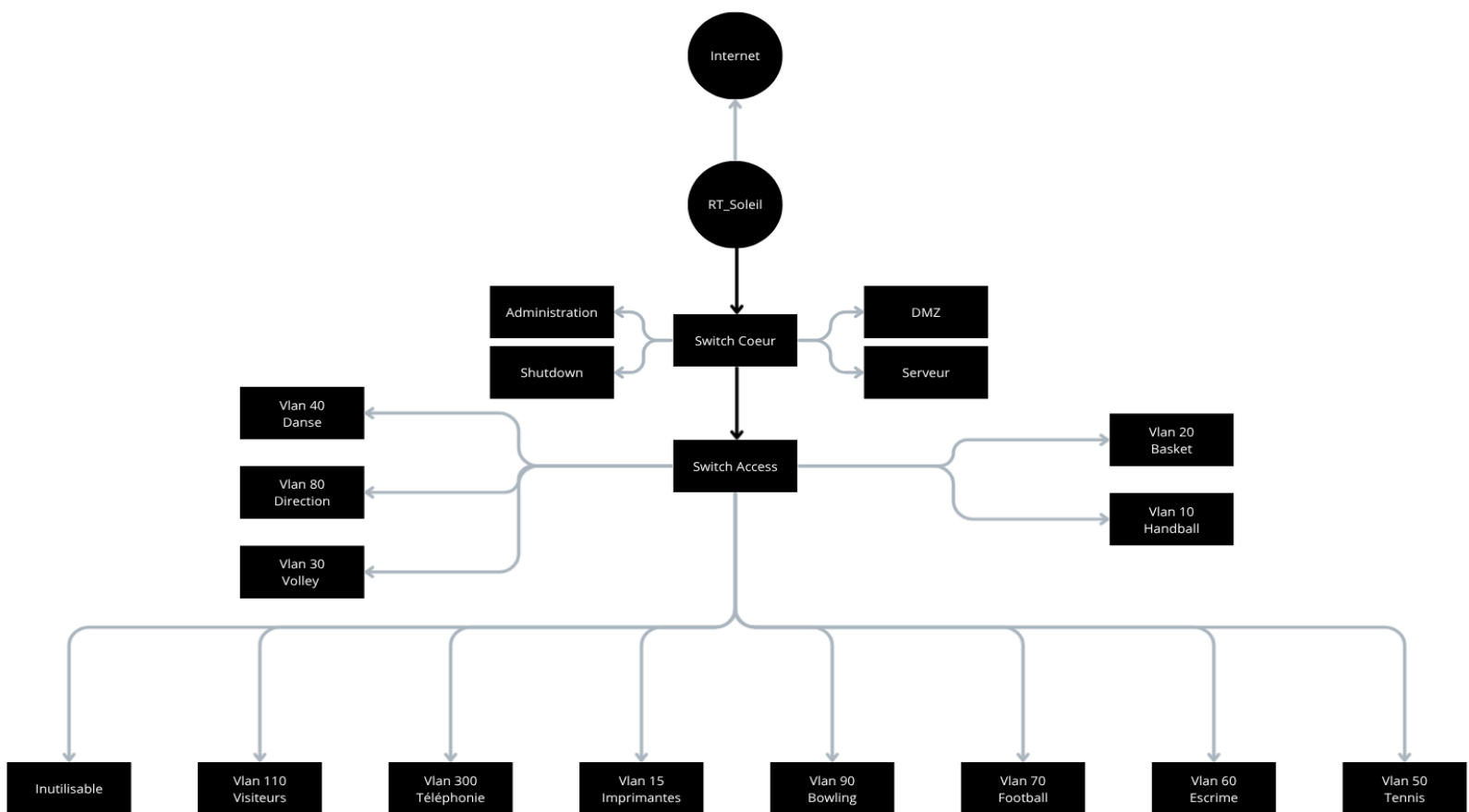


schéma réseau logique



# Tableau des ports

interface G1/0/1 Trunk -> SW Cœur	interface G1/0/3 Vlan 20	interface G1/0/5 Vlan 80	interface G1/0/7 Vlan 50	interface G1/0/9 Vlan 70	interface G1/0/11 Vlan 15	interface G1/0/13 Vlan 300	interface G1/0/15 Vlan 110	interface G1/0/17 ShutDown	interface G1/0/19 ShutDown	interface G1/0/21 ShutDown	interface G1/0/23 ShutDown
--	--------------------------------	--------------------------------	--------------------------------	--------------------------------	---------------------------------	----------------------------------	----------------------------------	----------------------------------	----------------------------------	----------------------------------	----------------------------------

Switch Access

interface G1/0/2 Vlan 10	interface G1/0/4 Vlan 30	interface G1/0/6 Vlan 40	interface G1/0/8 Vlan 60	interface G1/0/10 Vlan 90	interface G1/0/12 Vlan 15	interface G1/0/14 Vlan 300	interface G1/0/16 Vlan 110	interface G1/0/18 ShutDown	interface G1/0/20 ShutDown	interface G1/0/22 ShutDown	interface G1/0/24 ShutDown
--------------------------------	--------------------------------	--------------------------------	--------------------------------	---------------------------------	---------------------------------	----------------------------------	----------------------------------	----------------------------------	----------------------------------	----------------------------------	----------------------------------

interface G1/0/1 Trunk -> RT1	interface G1/0/3 Trunk -> SW Access	interface G1/0/5 Trunk -> DMZ	interface G1/0/7 Trunk -> Serveur	interface G1/0/9 Trunk -> Serveur	interface G1/0/11 Vlan 99	interface G1/0/13 Vlan 99	interface G1/0/15 Vlan 99	interface G1/0/17 ShutDown	interface G1/0/19 ShutDown	interface G1/0/21 ShutDown	interface G1/0/23 ShutDown
-------------------------------------	--	-------------------------------------	---	---	---------------------------------	---------------------------------	---------------------------------	----------------------------------	----------------------------------	----------------------------------	----------------------------------

Switch Cœur

interface G1/0/2 Trunk -> RT2	interface G1/0/4 Trunk -> DMZ	interface G1/0/6 Trunk -> DMZ	interface G1/0/8 Trunk -> Serveur	interface G1/0/10 Vlan 99	interface G1/0/12 Vlan 99	interface G1/0/14 Vlan 99	interface G1/0/16 Vlan 99	interface G1/0/18 ShutDown	interface G1/0/20 ShutDown	interface G1/0/22 ShutDown	interface G1/0/24 ShutDown
-------------------------------------	-------------------------------------	-------------------------------------	---	---------------------------------	---------------------------------	---------------------------------	---------------------------------	----------------------------------	----------------------------------	----------------------------------	----------------------------------

# Conf Switch Coeur

```
enable
configure terminal
```

```
hostname Orbite-01
no ip domain-lookup
ip domain-name m2l.local
```

```
! Comptes & SSH (ASCII)
enable secret Agpeit30
username admin privilege 15 secret Azerty11
```

```
crypto key generate rsa modulus 2048
ip ssh version 2
line vty 0 4
transport input ssh
login local
exec-timeout 10 0
```

```
! Passerelle & IP de management
ip default-gateway 172.26.16.12
```

```
! ===== VTP (pour propager les VLAN depuis le SW-COEUR== !
vtp domain M2L-VTP
vtp mode server
vtp password FreeAccess
vtp version 2
```

```
! ===== VLANs =====
vlan 10
name HANDBALL
exit
vlan 15
name IMPRESSION
exit
vlan 17
name SERVEUR
exit
vlan 18
name DMZ
exit
vlan 20
name BASKET
exit
vlan 30
name VOLLEY
exit
vlan 40
name DANSE
```



```
exit
vlan 50
name TENNIS
exit
vlan 60
name ESCRIME
exit
vlan 70
name FOOTBALL
exit
vlan 80
name DIRECTION
exit
vlan 90
name BOWLING
exit
vlan 99
name ADMINISTRATION
exit
vlan 100
name WIFI
exit
vlan 110
name VISITEUR
exit
vlan 300
name TELEPHONIE
exit
```

! ===== IP SWITCH-COEUR ===== !

```
interface vlan 99
description *****MANAGEMENT SW-COEUR-01*****
ip address 172.26.16.10 255.255.255.240
no shutdown
exit
```

! ===== LIEN VERS LE ROUTEUR 1 ===== !

```
interface GigabitEthernet1/0/1
description *****LIEN VERS LE ROUTEUR 1*****
switchport mode trunk
no shutdown
exit
```

! ===== LIEN VERS LE ROUTEUR 2 ===== !

```
interface GigabitEthernet1/0/2
description *****LIEN VERS LE ROUTEUR 2*****
switchport mode trunk
no shutdown
```

exit

! ===== LIEN VERS LE SWITCH D'ACCES ===== !

```
interface GigabitEthernet1/0/3
description *****LIEN VERS LE SWITCH D'ACCES*****
switchport mode trunk
exit
```

! ===== LIEN VERS LES SERVEURS DMZ ===== !

```
interface range GigabitEthernet1/0/4-6
description *****LIEN VERS LES SERVEURS DMZ*****
switchport mode trunk
no shutdown
exit
```

! ===== LIEN VERS LES SERVEURS ===== !

```
interface range GigabitEthernet1/0/7-9
description *****LIEN VERS LES SERVEURS*****
switchport mode trunk
no shutdown
exit
```

! ===== LIEN VERS L'ADMINISTRATION ===== !

```
interface range GigabitEthernet1/0/10-16
description *****ADMINISTRATION*****
switchport mode access
switchport access vlan 99
no shutdown
exit
```

! ===== PORT SHUTDOWN ===== !

```
interface range GigabitEthernet1/0/17-24
description *****SHUTDOWN*****
shutdown
exit
```

wr

# Conf Switch Accès

```
enable
configure terminal
```

```
hostname Galaxie-02
no ip domain-lookup
ip domain-name m2l.local
```

```
! Comptes & SSH (ASCII)
enable secret Agpeit31
username admin privilege 15 secret Djn42N25dfL8
```

```
crypto key generate rsa modulus 2048
```

```
ip ssh version 2
line vty 0 4
transport input ssh
login local
exec-timeout 10 0
```

```
! Passerelle & IP de management (SVI VLAN120)
ip default-gateway 172.26.16.12
```

```
! VTP : client (le cœur propage les VLAN)
vtp domain M2L-VTP
vtp mode client
vtp password FreeAccess
vtp version 2
```

```
! ===== IP SWITCH-ACCES ===== !
interface Vlan 99
description *****MANAGEMENT SW-ACCES-01*****
ip address 172.26.16.9 255.255.255.240
no shutdown
```

```
! ===== LIEN VERS LE SWITCH COEUR ===== !
interface GigabitEthernet1/0/1
description *****LIEN VERS LE SWITCH COEUR*****
switchport mode trunk
no shutdown
```

```
! ===== HANDBALL (VLAN 10) ===== !
interface GigabitEthernet1/0/2
description *****LIGUE_HANDBALL *****
switchport mode access
switchport access vlan 10
no shutdown
```

```
! ===== LIGUE BASKET (VLAN 20) ===== !
```

```
interface GigabitEthernet1/0/3
description *****LIGUE_BASKET*****
switchport mode access
switchport access vlan 20
no shutdown
```

! ===== LIGUE VOLLEY (VLAN 30) ===== !

```
interface GigabitEthernet1/0/4
description *****LIGUE_VOLLEY*****
switchport mode access
switchport access vlan 30
no shutdown
```

! ===== DIRECTION (VLAN 80) ===== !

```
interface GigabitEthernet1/0/5
description *****DIRECTION*****
switchport mode access
switchport access vlan 80
no shutdown
```

! ===== LIGUE DANSE (VLAN 40) ===== !

```
interface GigabitEthernet1/0/6
description *****LIGUE_DANSE*****
switchport mode access
switchport access vlan 40
no shutdown
```

! ===== LIGUE TENNIS (VLAN 50) ===== !

```
interface GigabitEthernet1/0/7
description *****LIGUE_TENNIS*****
switchport mode access
switchport access vlan 50
no shutdown
```

! ===== LIGUE ESCRIME (VLAN 60) ===== !

```
interface GigabitEthernet1/0/8
description *****LIGUE_ESCRIME*****
switchport mode access
switchport access vlan 60
no shutdown
```

! ===== LIGUE FOOTBALL (VLAN 70) ===== !

```
interface GigabitEthernet1/0/9
description *****LIGUE_FOOTBALL *****
switchport mode access
switchport access vlan 70
no shutdown
```

! ===== LIGUE BOWLING (VLAN 90) ===== !

```
interface GigabitEthernet1/0/10
description *****LIGUE_BOWLING*****
switchport mode access
switchport access vlan 90
no shutdown
```

! ===== IMPRIMANTE (VLAN 15) ===== !

```
interface range GigabitEthernet1/0/11-12
description *****IMPRIMANTE*****
switchport mode access
switchport access vlan 15
no shutdown
```

! ===== TELEPHONIE (VLAN 300) ===== !

```
interface range GigabitEthernet1/0/13-14
description *****TELEPHONIE*****
switchport mode access
switchport access vlan 300
no shutdown
```

! ===== VISITEUR FILAIRE (VLAN 110) ===== !

```
interface range GigabitEthernet1/0/15-16
description *****VISITEUR*****
switchport mode access
switchport access vlan 110
no shutdown
```

! ===== PORTS INUTILISÉS ===== !

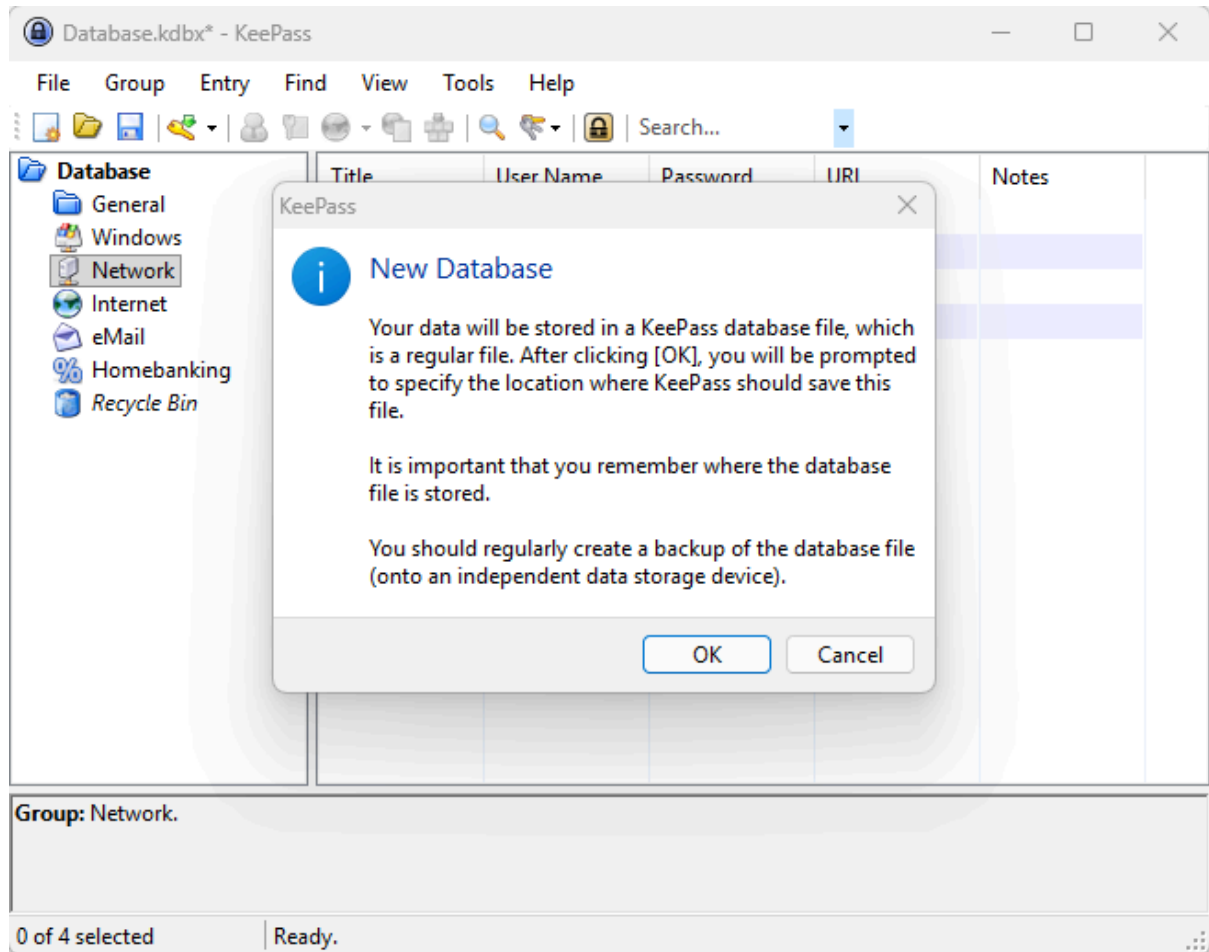
```
interface range GigabitEthernet1/0/17-24
description *****SHUTDOWN*****
shutdown
```

# Keepass

Mot de passe keepass : ErFGuiPOINC15307!#fCazpo29,

J'ai choisi le logiciel KeePass pour la gestion des mots de passe.

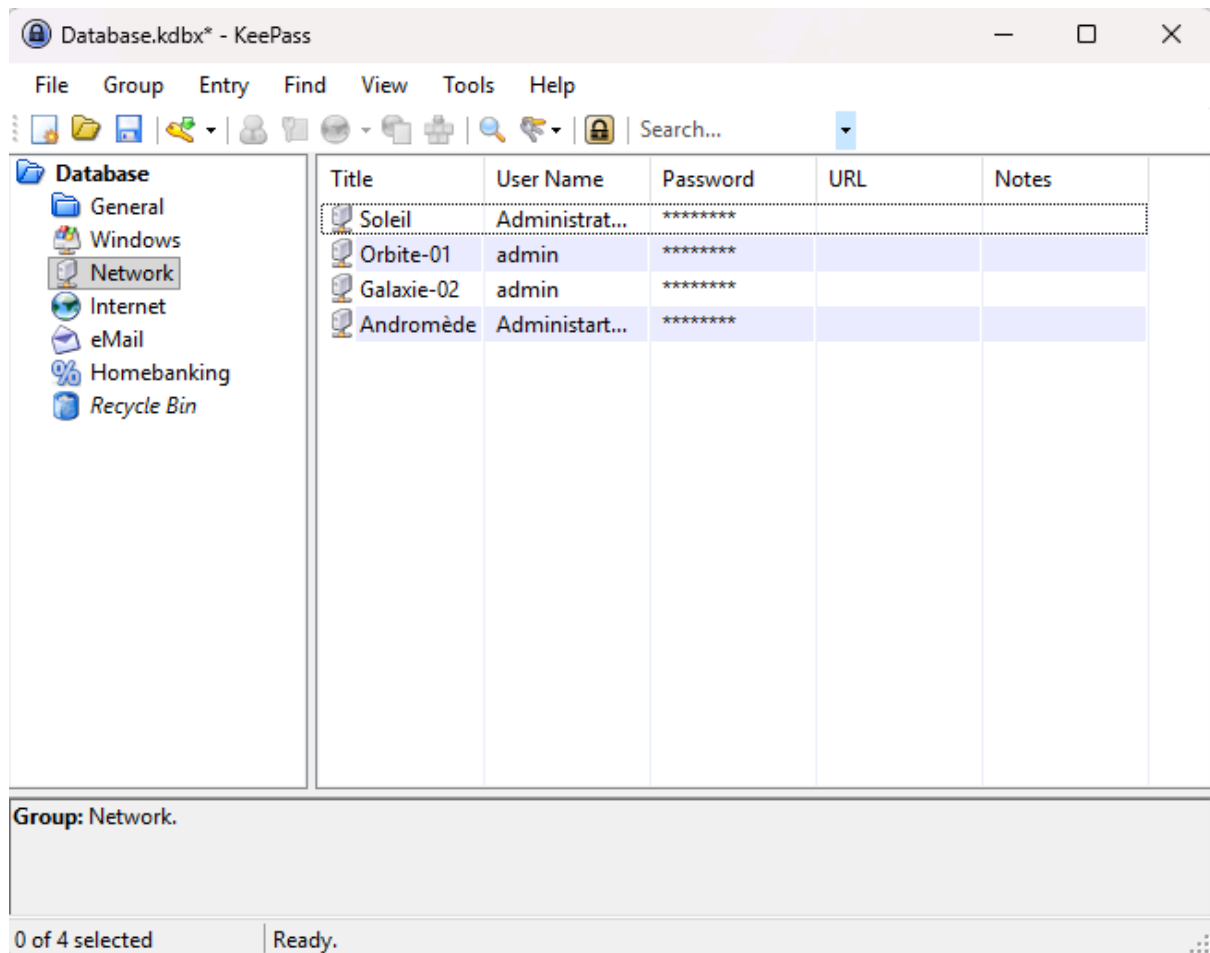
voici une courte présentation :



Il faut d'abord créer une base de données des mots de passe.

puis une fois cela fait, il faut ajouter les mots de passes correspondant aux machines ou aux utilisateurs :





Une fois cela terminé les mots de passe sont enregistrés dans un coffre fort qui est la base de données protégée par un gros mot de passe.