Contexte et objectif

Cette procédure décrit la mise en place d'un partage de fichiers sur un serveur Windows et l'attribution automatique d'un dossier personnel (home directory) à chaque utilisateur du domaine Active Directory.

Objectif : chaque utilisateur dispose, à son ouverture de session, d'un lecteur réseau personnel monté automatiquement (ex. lecteur Z:). Chaque utilisateur accède uniquement à son propre dossier ; aucun utilisateur ne peut lire ou modifier le dossier d'un autre.

Environnement de la maquette :

- Serveur : Windows Server 2022 contrôleur de domaine (AD DS, DNS) – nom : SRV-AD – IP : 192.168.1.200.
- Domaine Active Directory : talos.local
- Volume de stockage dédié aux données : E:
- Poste client : Windows 10 joint au domaine.

Prérequis

- Le rôle AD DS est installé et le domaine fonctionne (utilisateurs créés dans l'AD).
- Le rôle « Services de fichiers » est installé (recommandé pour l'énumération basée sur l'accès).
- Un volume de données disponible (ici E:) formaté en NTFS.
- Un compte administrateur du domaine pour réaliser la procédure.
- Au moins deux comptes utilisateurs de test dans l'AD pour valider l'isolation (ex. u.dupont et u.martin).

Principe : partage + NTFS

Deux niveaux de droits se cumulent. Le droit effectif est le plus restrictif des deux :

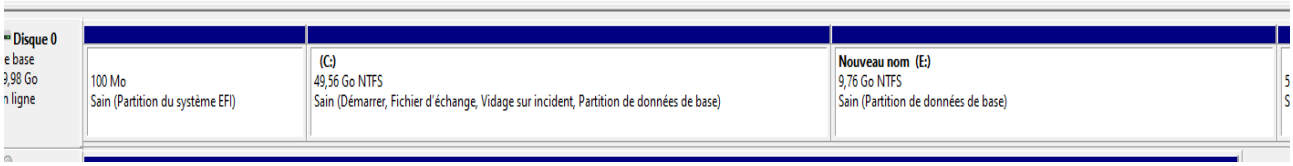
- Permissions de partage (SMB) : contrôlent l'accès via le réseau. On les laisse larges (Modifier) et c'est le NTFS qui filtre réellement.
- Permissions NTFS : contrôlent l'accès au niveau du système de fichiers. C'est ici que se fait l'isolation par utilisateur.

Le mécanisme clef : sur le dossier racine, on autorise les utilisateurs à créer leur dossier mais pas à parcourir ceux des autres, et on accorde au groupe CRÉATEUR PROPRIÉTAIRE le contrôle total uniquement sur les sous-dossiers. Quand l'AD crée automatiquement le dossier personnel (variable %username%), l'utilisateur en devient propriétaire et obtient le contrôle total sur son seul dossier.

Étape 1 Création de l'arborescence physique

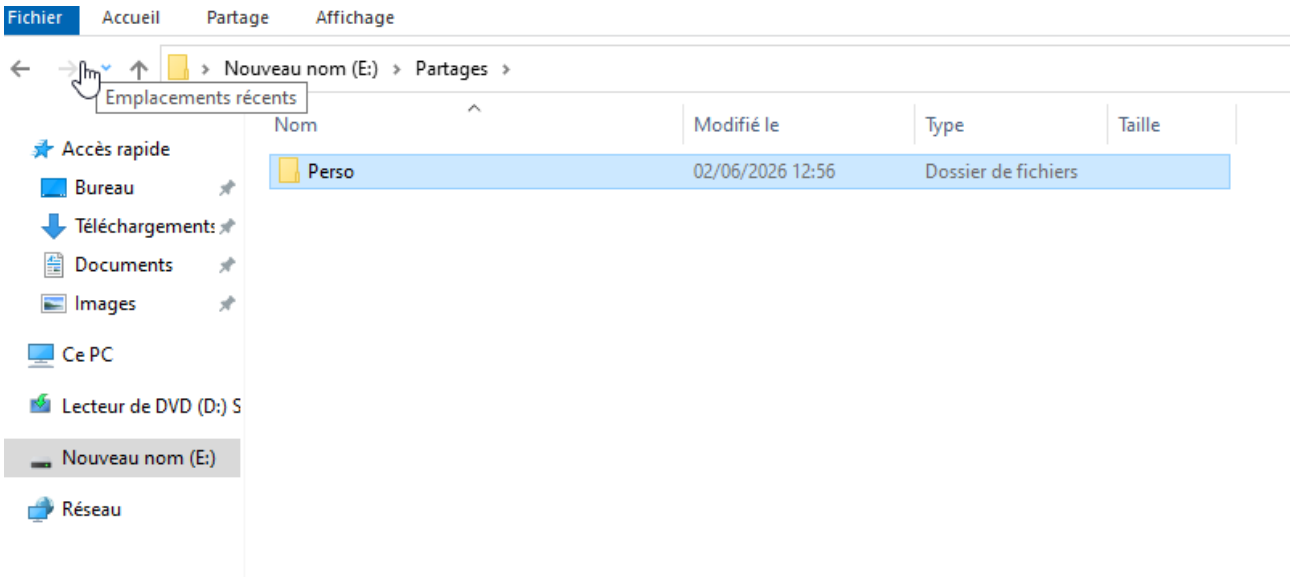
Sur SRV-AD, ouvrir l'Explorateur de fichiers.

Sur le volume E:, créer le dossier qui contiendra tous les dossiers personnels :




```
E:\Partages\Perso
```

Le dossier Perso restera vide pour l'instant : les sous-dossiers utilisateurs seront créés automatiquement par l'AD à l'étape 8.



Étape 2 Création du partage masqué

On crée un partage masqué (suffixe $) : il n'apparaît pas dans le voisinage réseau, ce qui limite l'exposition.

Clic droit sur le dossier D:\Partages\Perso → Propriétés → onglet Partage.

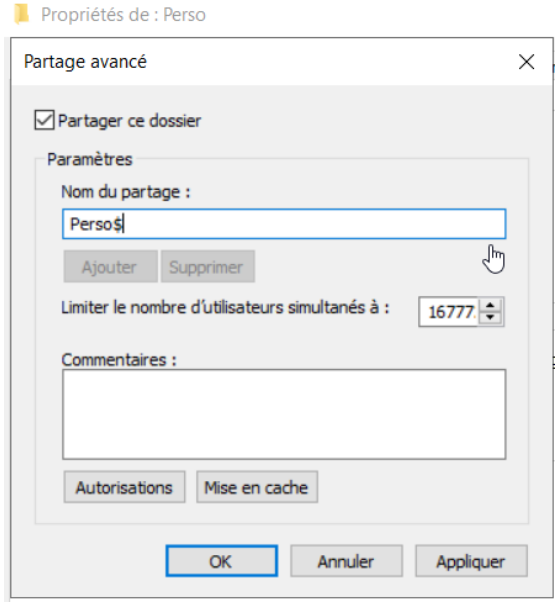
Cliquer sur Partage avancé.

Cocher Partager ce dossier.

Dans Nom du partage, saisir un nom masqué :

```
Perso$
```

Ne pas encore valider : passer aux permissions de partage (étape 3).



Étape 3 Permissions de partage

Dans la fenêtre Partage avancé, cliquer sur Autorisations.

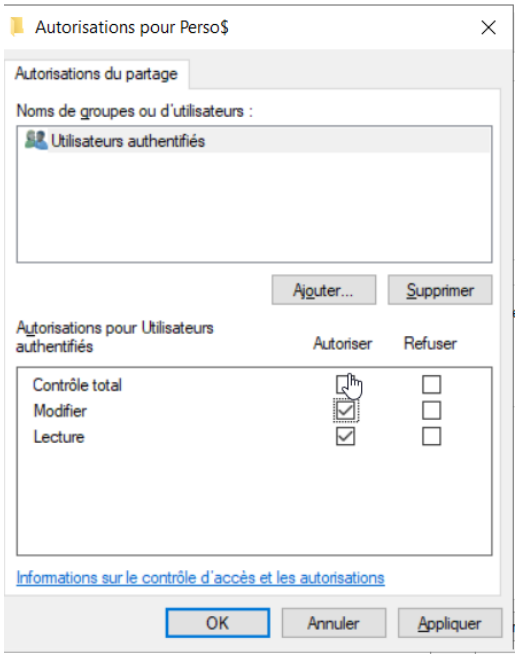
Supprimer le groupe Tout le monde.

Ajouter le groupe Utilisateurs authentifiés.

Lui accorder l'autorisation Modifier (Lecture + Modifier). Ne pas donner Contrôle total au niveau partage.

Valider (OK) puis fermer pour appliquer le partage.

Rappel : les permissions de partage sont volontairement larges ; l'isolation réelle est assurée par le NTFS à l'étape suivante.



Étape 4 Permissions NTFS sur le dossier racine

On définit ici les droits qui permettent la création automatique des dossiers personnels tout en isolant les utilisateurs.

Clic droit sur D:\Partages\Perso → Propriétés → onglet Sécurité → Avancé.

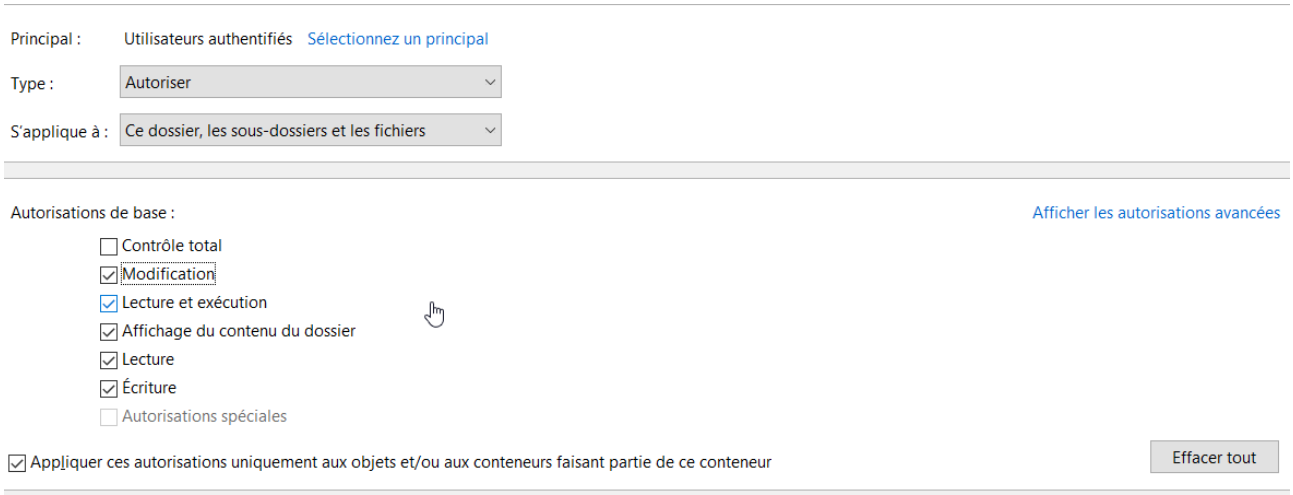
Désactiver l'héritage → choisir Convertir les autorisations héritées en autorisations explicites.

Configurer les entrées d'autorisation comme suit :

- Utilisateurs authentifiés : autorisations Afficher le contenu du dossier + Lecture + Création de dossier / ajout de données – appliqué à « Ce dossier seulement ».

Valider l'ensemble (OK).

Résultat attendu : un utilisateur peut créer son dossier dans Perso mais ne peut pas ouvrir ceux des autres. Le contrôle total « sous-dossiers et fichiers seulement » du CRÉATEUR PROPRIÉTAIRE garantit que le créateur de chaque dossier personnel (donc l'utilisateur) en maîtrise le contenu, sans hériter d'un accès sur les dossiers voisins.

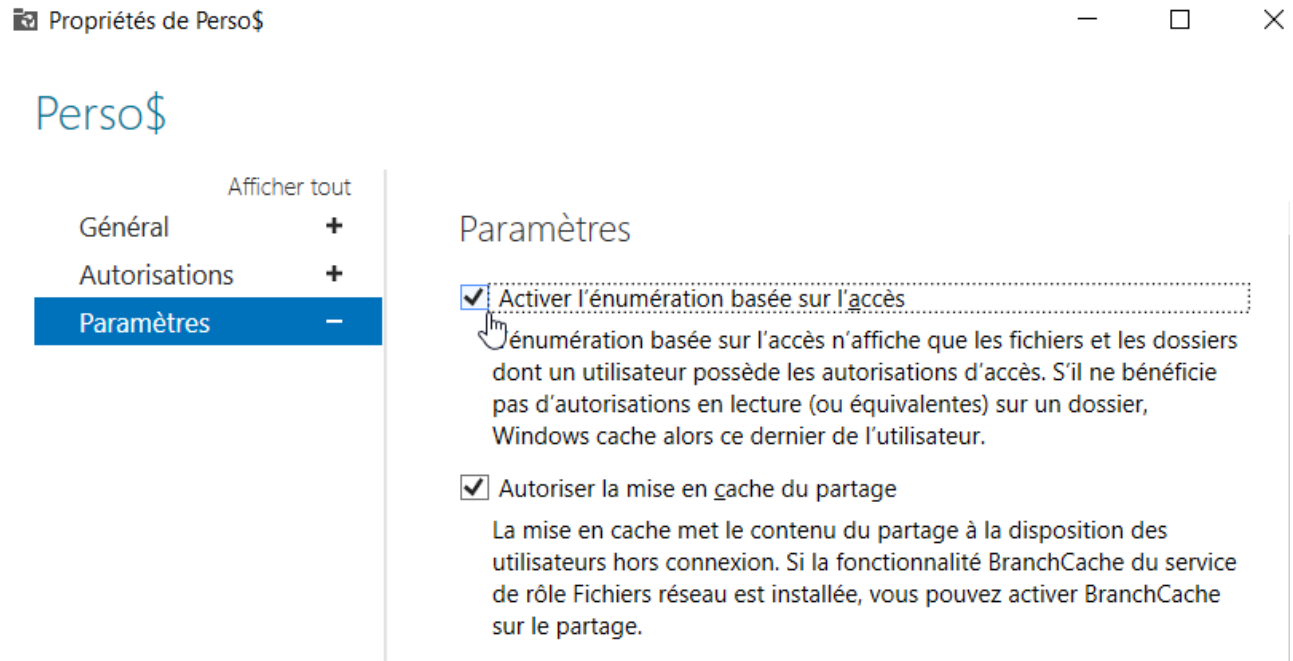


Étape 5 Énumération basée sur l'accès (ABE)

L'ABE masque les dossiers auxquels l'utilisateur n'a pas accès : il ne voit que son propre dossier dans le partage.

Ouvrir le Gestionnaire de serveur → Services de fichiers et de stockage → Partages.

Clic droit sur le partage Perso$ → Propriétés → Paramètres.



Étape 6 Affectation du dossier personnel dans l'AD

C'est l'étape qui déclenche la création automatique du dossier et le montage du lecteur réseau.

Ouvrir Utilisateurs et ordinateurs Active Directory.

Double-cliquer sur un utilisateur crée jean dupont → onglet Profil.

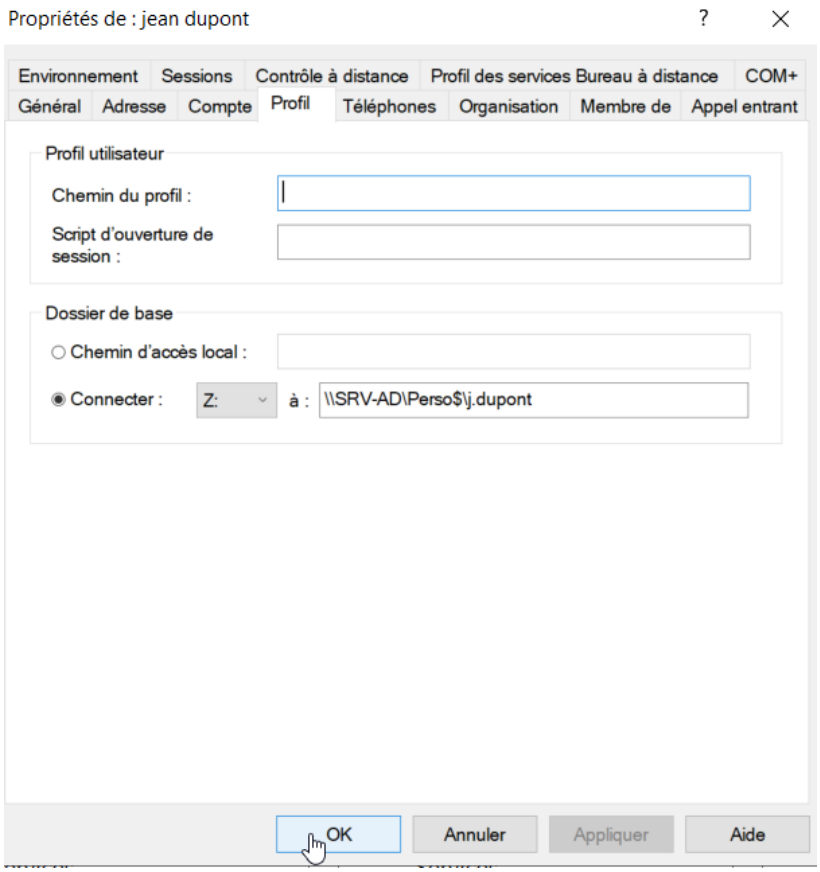
Dans la zone Dossier de base (home folder), sélectionner Connecter.

Choisir une lettre de lecteur, par exemple Z:.

Dans le champ À, saisir le chemin UNC avec la variable %username% :

```
\\SRV-AD\Perso$\%username%
```

Valider (OK).



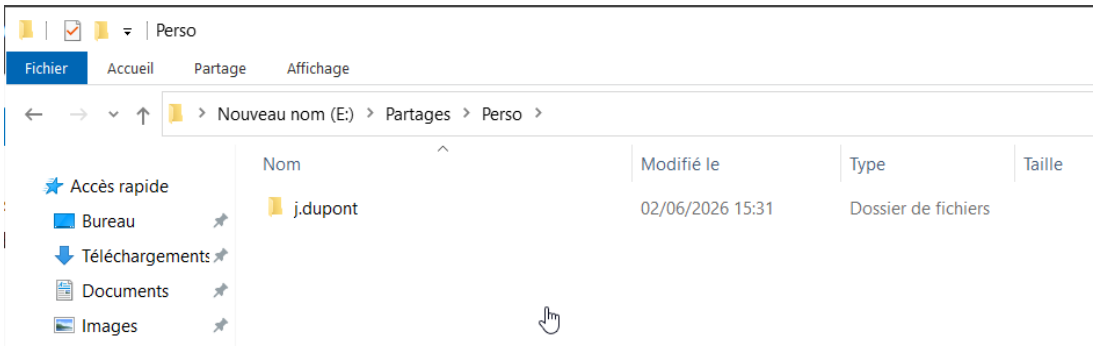
À la validation, Windows remplace %username% par l'identifiant de connexion (ex. u.dupont), crée automatiquement le sous-dossier correspondant dans D:\Partages\Perso et positionne l'utilisateur comme propriétaire avec contrôle total sur ce seul dossier.

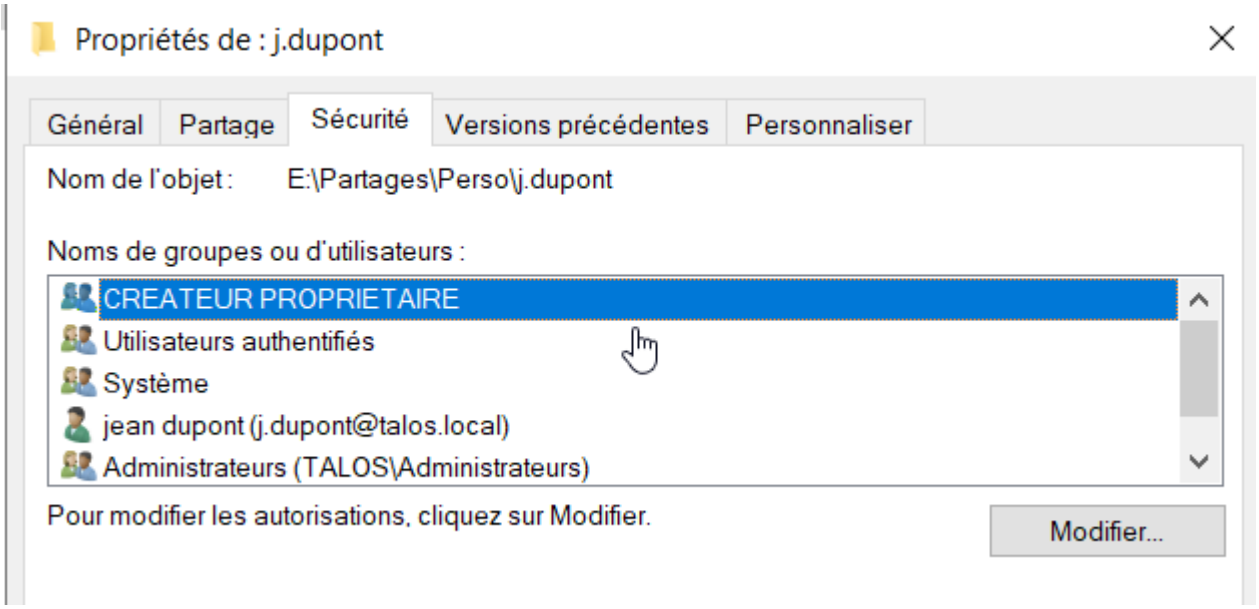
Étape 7 Vérification côté serveur

Retourner dans D:\Partages\Perso : le sous-dossier au nom de l'utilisateur a été créé automatiquement.

Clic droit sur ce sous-dossier (ex. u.dupont) → Propriétés → Sécurité.

Vérifier que seuls figurent : l'utilisateur (Contrôle total), SYSTÈME et Administrateurs. Aucun autre utilisateur ne doit apparaître.

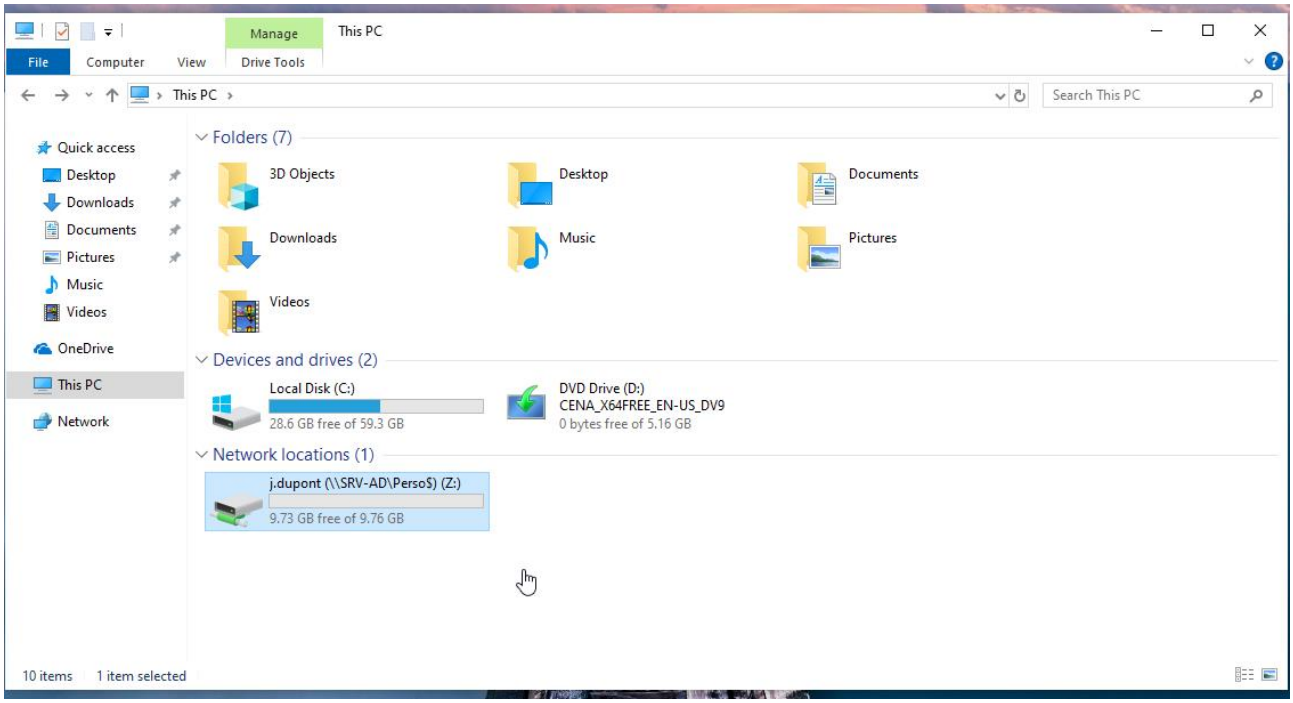




Étape 8 Test côté client

Sur un poste client joint au domaine, ouvrir une session avec j.dupont.

Ouvrir l'Explorateur : le lecteur Z: est monté automatiquement et pointe sur le dossier personnel.



Créer un fichier test dans Z: pour confirmer le droit d'écriture.

Test d'isolation : tenter d'accéder au dossier d'un autre utilisateur via :

```
\\SRV-AD\Perso$\u.martin
```