ACTIVE DIRECTORY
OUs, GROUPES ET DFS NAMESPACE

Organisation des services et partages réseau centralisés

Mode opératoire — Procédure complète avec captures d'écran

Sasiraj GUNARATNARAJAH

BTS SIO — Option SISR

Année 2025 – 2026

Table des matières

1. Présentation

Ce document détaille la procédure de mise en place d'une structure organisationnelle dans Active Directory (OUs, groupes, utilisateurs) et la configuration d'un espace de noms DFS (Distributed File System) pour centraliser les partages réseau de l'entreprise. Cette documentation fait partie du projet d'infrastructure virtualisée sur Proxmox VE, dans le cadre du BTS SIO option SISR.

L'espace de noms DFS permet de regrouper les dossiers partagés situés sur différents serveurs en un seul chemin d'accès logique. Les utilisateurs accèdent à tous les partages via un chemin unique (\\pxdc.local\Partages) sans connaître l'emplacement physique des données.

1.1 Prérequis

Composant	Détail
Serveur	WS-DC-1 (Windows Server 2022) — 172.16.1.10
Rôles installés	AD DS, DNS, DHCP
Domaine	pxdc.local
Réseau	LAN-SRV — 172.16.1.0/24 (vmbr1)
Pare-feu	pfSense (WAN : 192.168.1.100)

1.2 Structure organisationnelle cible

L'infrastructure Active Directory sera organisée en 4 unités d'organisation (OU) représentant les services de l'entreprise, chacune contenant un groupe de sécurité et des utilisateurs :

OU	Groupe	Utilisateurs
Administration	GRP_Admin	Patrick DURAND (PDG — accès à tous les groupes)
Comptabilité	GRP_Compta	Thomas ROUGET, Philippe ABADIE
Stagiaire	GRP_Stagiaire	Virginie RIGON, Laurent GUERIN
Ressources Humaines	GRP_RH	Sophie PALE, Sylvain NOIR

1.3 Structure DFS cible

```
\\pxdc.local\Partages\
    ├── Administration\    → accès GRP_Admin
    ├── Comptabilite\      → accès GRP_Compta
    ├── Stagiaire\         → accès GRP_Stagiaire
    ├── RH\                → accès GRP_RH
    └── Commun\            → accès Utilisateurs du domaine
```

1.4 Compétences BTS SIO mobilisées

Bloc	Compétence
B1	Gérer le patrimoine informatique — Organisation des ressources partagées
B5	Administrer les systèmes — AD, DFS, gestion des permissions NTFS
B6	Cybersécurité — Contrôle d'accès par groupes de sécurité

2. Création de la structure Active Directory

2.1 Création des Unités d'Organisation (OU)

Ouvrir la console Utilisateurs et ordinateurs Active Directory (dsa.msc). Clic droit sur le domaine pxdc.local > Nouveau > Unité d'organisation. Créer les 4 OUs :

1. Administration
2. Comptabilité
3. Stagiaire
4. Ressources Humaines

2.2 Création des groupes de sécurité

Dans chaque OU, clic droit > Nouveau > Groupe. Créer un groupe de sécurité globale pour chaque service :

OU	Nom du groupe	Étendue	Type
Administration	GRP_Admin	Globale	Sécurité
Comptabilité	GRP_Compta	Globale	Sécurité
Stagiaire	GRP_Stagiaire	Globale	Sécurité
Ressources Humaines	GRP_RH	Globale	Sécurité

2.3 Création des utilisateurs

Dans chaque OU, clic droit > Nouveau > Utilisateur. Créer les 7 comptes utilisateurs :

OU	Nom complet	Login	Mot de passe
Administration	Patrick DURAND	pdurand	sdfghjkl123/
Comptabilité	Thomas ROUGET	trouget	sdfghjkl123/
Comptabilité	Philippe ABADIE	pabadie	sdfghjkl123/
Stagiaire	Virginie RIGON	vrigon	sdfghjkl123/
Stagiaire	Laurent GUERIN	lguerin	sdfghjkl123/
Ressources Humaines	Sophie PALE	spale	sdfghjkl123/
Ressources Humaines	Sylvain NOIR	snoir	sdfghjkl123/

ℹ️ Les options « L'utilisateur doit changer le mot de passe à la prochaine ouverture de session » est décochée et « Le mot de passe n'expire jamais » est cochée (environnement de lab).

2.4 Appartenance aux groupes

Pour chaque utilisateur, clic droit > Propriétés > onglet Membre de > Ajouter le(s) groupe(s) correspondant(s) :

Utilisateur	Membre de
Patrick DURAND (PDG)	GRP_Admin + GRP_Compta + GRP_Stagiaire + GRP_RH
Thomas ROUGET	GRP_Compta
Philippe ABADIE	GRP_Compta
Virginie RIGON	GRP_Stagiaire
Laurent GUERIN	GRP_Stagiaire
Sophie PALE	GRP_RH
Sylvain NOIR	GRP_RH

💡 Patrick DURAND est le PDG, il est donc membre de tous les groupes pour avoir accès à l'ensemble des partages de l'entreprise.

2.5 Résultat dans Active Directory

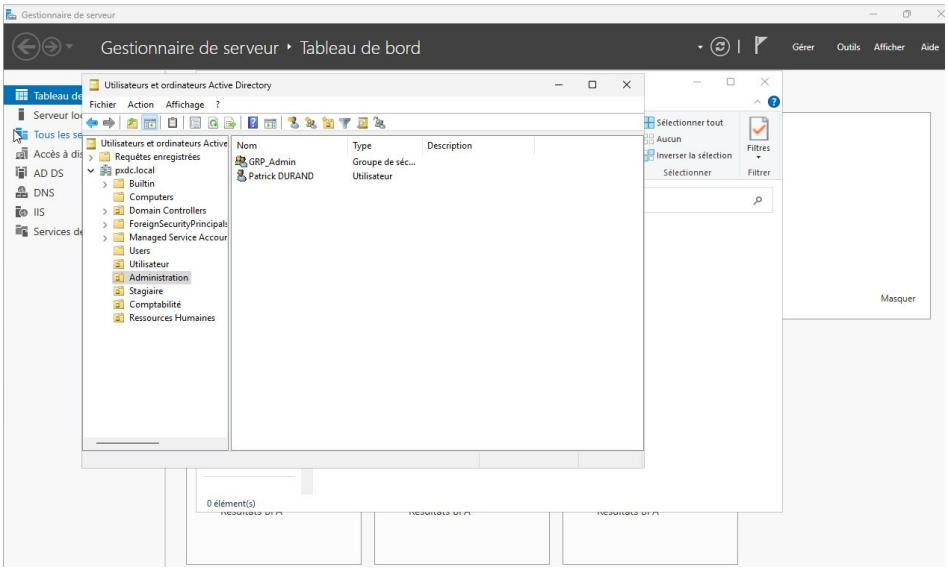

Figure 1 — Console AD : OU Administration avec le groupe GRP_Admin et l'utilisateur Patrick DURAND. Les 4 OUs sont visibles dans l'arborescence.

3. Installation du rôle DFS

3.1 Ajout du rôle Espaces de noms DFS

Ouvrir le Gestionnaire de serveur > Gérer > Ajouter des rôles et fonctionnalités. Suivre l'assistant :

5. Avancer jusqu'à « Rôles du serveur »
6. Développer Services de fichiers et de stockage > Services de fichiers et iSCSI
7. Cocher « Espaces de noms DFS »
8. Cliquer sur Installer

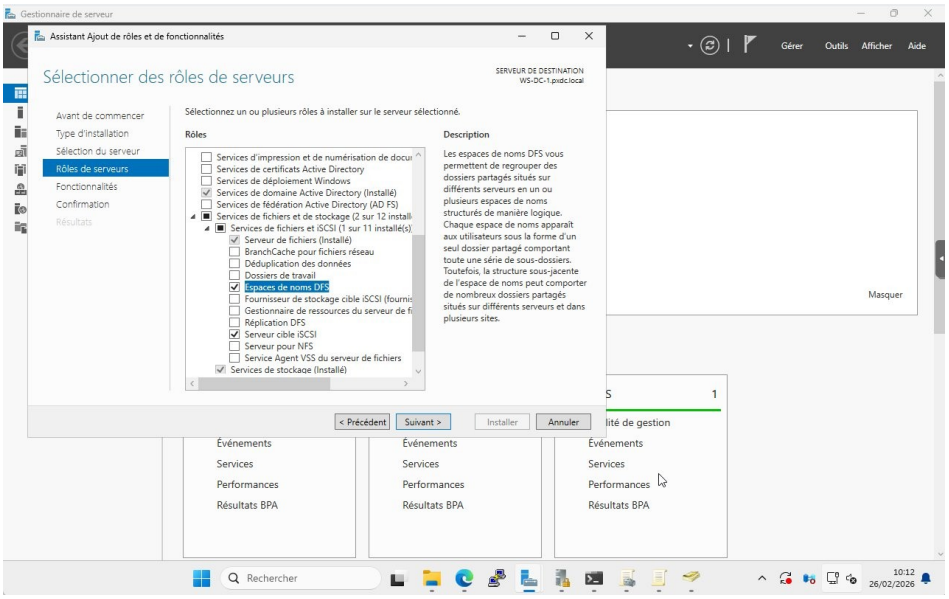

Figure 2 — Sélection du rôle « Espaces de noms DFS » dans l'assistant d'ajout de rôles

Attendre la fin de l'installation. Le rôle est maintenant disponible dans les outils d'administration.

4. Création des dossiers physiques

4.1 Arborescence sur le disque local

Créer les dossiers de partage sur le disque local du serveur. Ouvrir un cmd en administrateur :

```
mkdir C:\Partages\Administration
mkdir C:\Partages\Comptabilite
mkdir C:\Partages\Stagiaire
mkdir C:\Partages\RH
mkdir C:\Partages\Commun
```

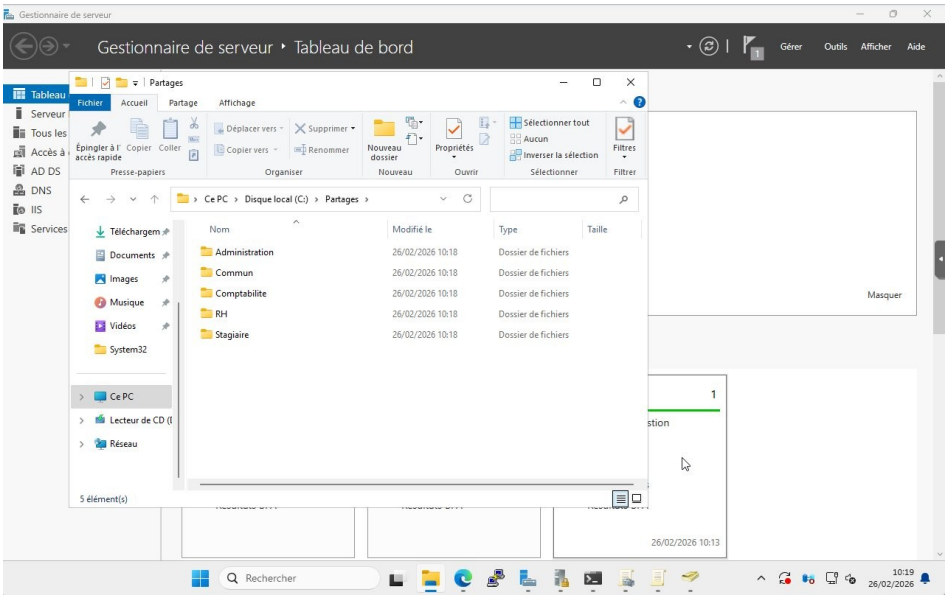

Figure 3 — Dossier C:\Partages avec les 5 sous-dossiers créés

5. Configuration de l'espace de noms DFS

5.1 Création du namespace

Ouvrir la console Gestion du système de fichiers distribués DFS (dfsmgmt.msc). Clic droit sur Espaces de noms > Nouvel espace de noms :

9. Serveur : sélectionner WS-DC-1 (pxdc.local)
10. Nom de l'espace de noms : Partages
11. Type : Espace de noms de domaine (chemin : \\pxdc.local\Partages)
12. Cliquer sur Créer

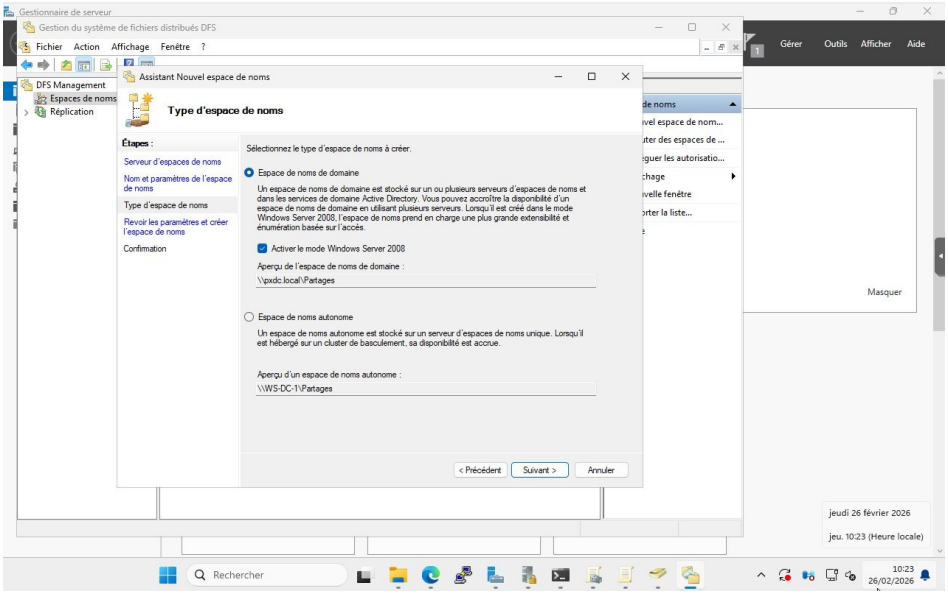

Figure 4 — Assistant de création : espace de noms de domaine \\pxdc.local\Partages

5.2 Ajout des dossiers dans le namespace

Clic droit sur \\pxdc.local\Partages > Nouveau dossier. Pour chaque dossier, renseigner le nom puis cliquer sur Ajouter pour définir la cible de dossier :

Nom du dossier	Cible (chemin UNC)	Dossier local
Administration	\\pxdc.local\Administration	C:\Partages\Administration
Comptabilite	\\pxdc.local\Comptabilite	C:\Partages\Comptabilite
Stagiaire	\\pxdc.local\Stagiaire	C:\Partages\Stagiaire
RH	\\pxdc.local\RH	C:\Partages\RH
Commun	\\pxdc.local\Commun	C:\Partages\Commun

Lors de la création de la cible, utiliser le bouton Parcourir > Nouveau dossier partagé pour créer automatiquement le partage SMB associé :

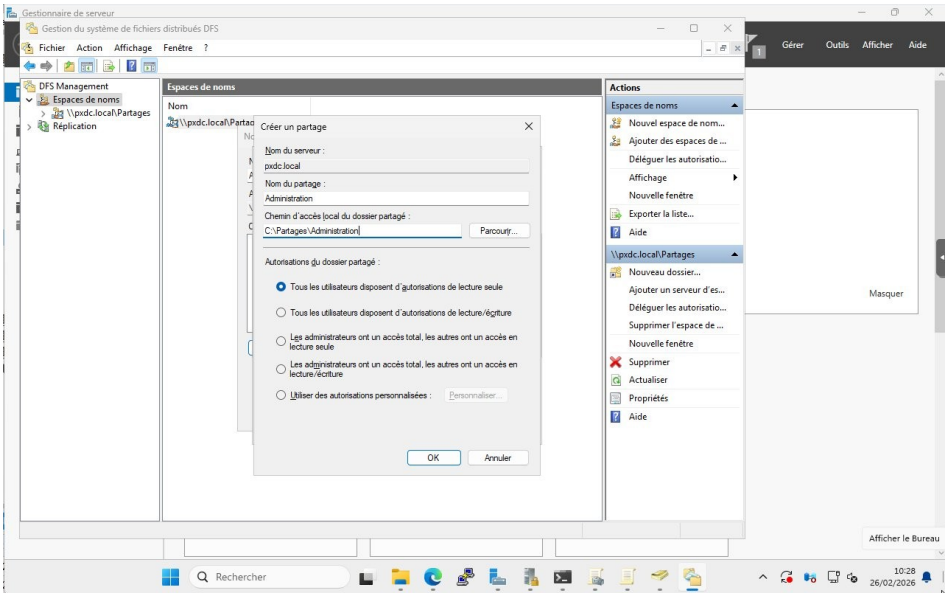

Figure 5 — Création du partage Administration avec le chemin local C:\Partages\Administration

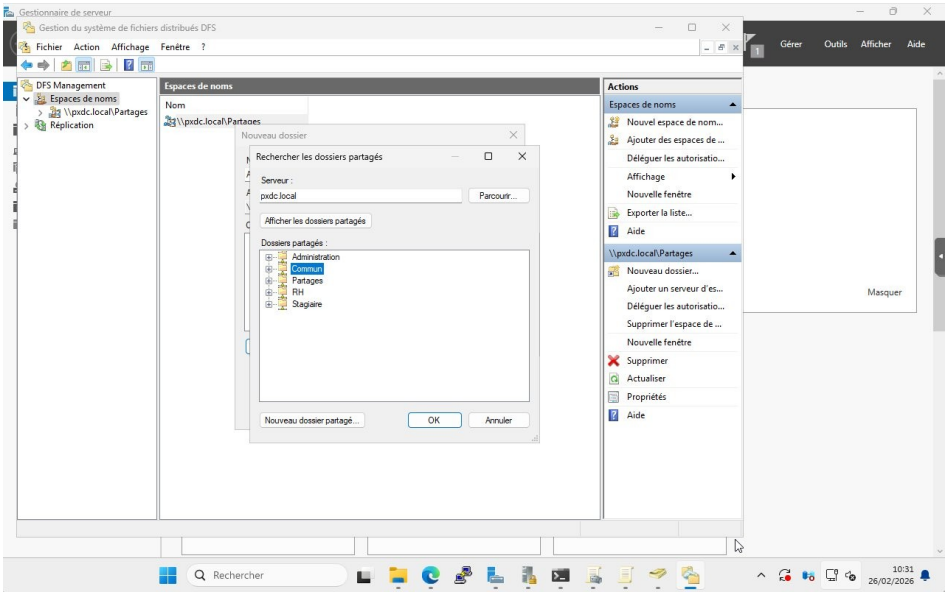

Figure 6 — Liste des dossiers partagés disponibles sur le serveur (Administration, Commun, RH, Stagiaire)

5.3 Résultat dans la console DFS

Une fois les 5 dossiers ajoutés, la console DFS affiche l'arborescence complète du namespace :

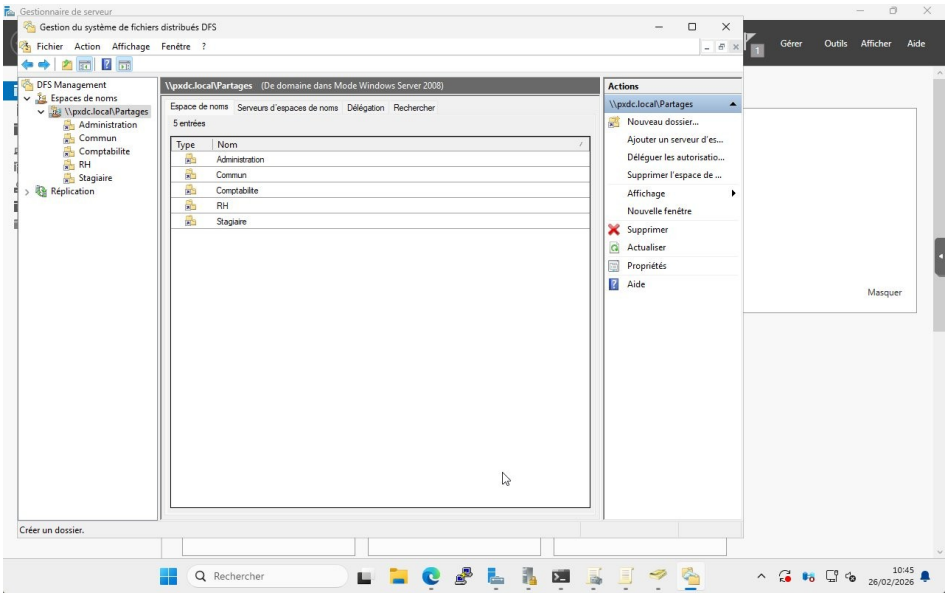

Figure 7 — Console DFS : namespace \\pxdc.local\Partages avec les 5 dossiers (Administration, Commun, Comptabilite, RH, Stagiaire)

6. Configuration des permissions NTFS

6.1 Principe de sécurité

Les permissions NTFS permettent de contrôler l'accès aux dossiers au niveau du système de fichiers. Chaque dossier de service est accessible uniquement par le groupe de sécurité correspondant. Le dossier Commun reste accessible à tous les utilisateurs du domaine.

Pour chaque dossier dans C:\Partages, effectuer les opérations suivantes : clic droit > Propriétés > onglet Sécurité > Modifier > Ajouter le groupe correspondant et supprimer le groupe Utilisateurs générique.

6.2 Matrice des permissions

Dossier	Groupe autorisé	Permission	Utilisateurs génériques
Administration	GRP_Admin	Contrôle total	Supprimé
Comptabilite	GRP_Compta	Contrôle total	Supprimé
Stagiaire	GRP_Stagiaire	Contrôle total	Supprimé
RH	GRP_RH	Contrôle total	Supprimé
Commun	Utilisateurs du domaine	Lecture/Écriture	Conservé

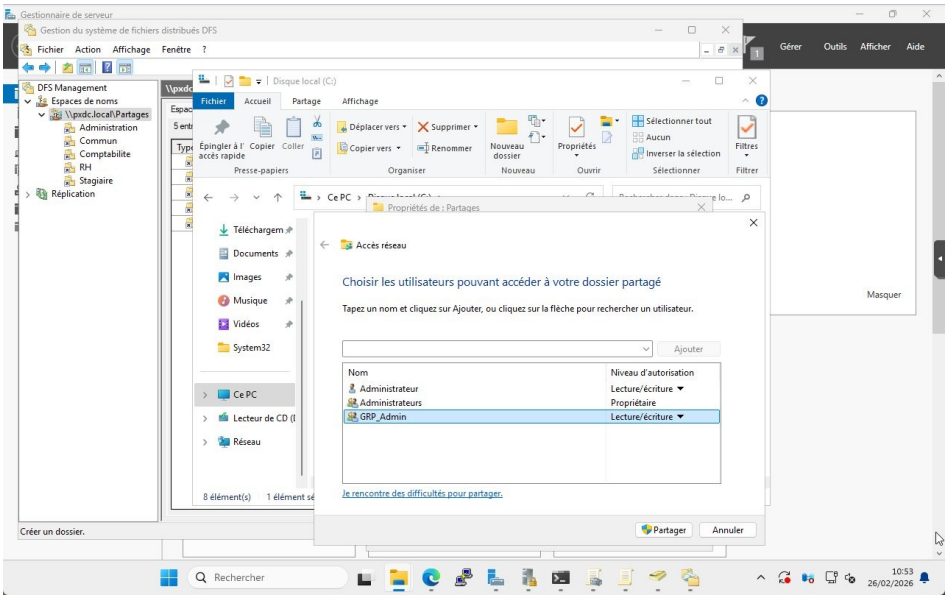

Figure 8 — Configuration des permissions de partage avec GRP_Admin en lecture/écriture

⚠️ Patrick DURAND (PDG) a accès à tous les dossiers car il est membre des 4 groupes. Les autres utilisateurs n'ont accès qu'à leur dossier de service + le dossier Commun.

7. Validation du namespace DFS

7.1 Test d'accès au namespace

Pour valider le bon fonctionnement, ouvrir l'Explorateur de fichiers et accéder au chemin UNC du namespace :

Chemin : \\pxdc.local\Partages

Les 5 dossiers doivent apparaître dans l'Explorateur :

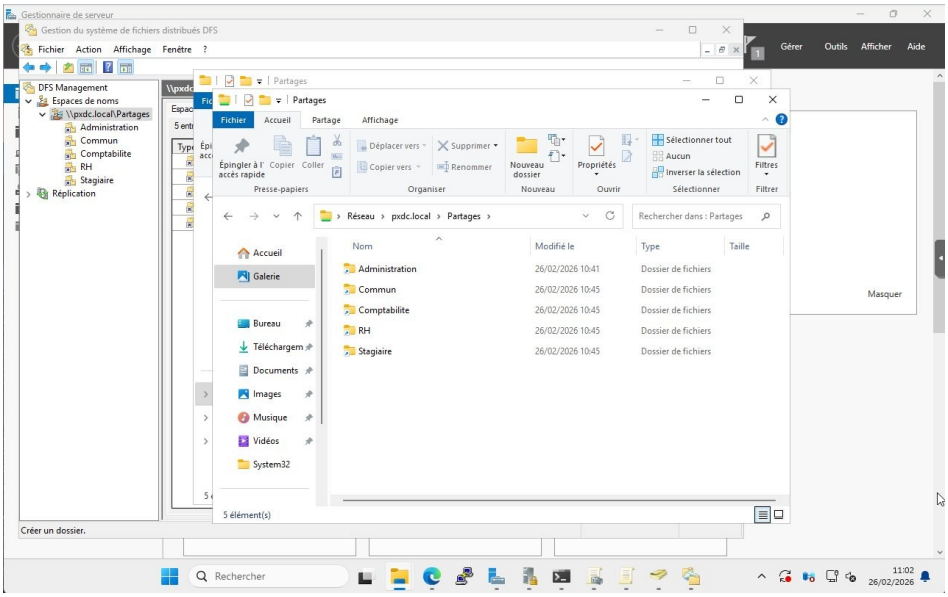

Figure 9 — Accès au namespace \\pxdc.local\Partages via l'Explorateur — les 5 dossiers sont visibles

7.2 Tests d'accès par utilisateur

Pour vérifier l'isolation des permissions, se connecter avec différents comptes AD et tenter d'accéder aux dossiers :

Utilisateur	Administration	Comptabilite	Stagiaire	RH	Commun
pdurand (PDG)	✅	✅	✅	✅	✅
trouget	❌	✅	❌	❌	✅
vrigon	❌	❌	✅	❌	✅
spale	❌	❌	❌	✅	✅

💡 Ce test pourra être effectué depuis le poste client Windows 11 une fois celui-ci joint au domaine, pour valider le fonctionnement de bout en bout.

8. Synthèse et points de vérification

#	Point de vérification	Statut
1	4 OUs créées (Administration, Comptabilité, Stagiaire, RH)	✅
2	4 groupes de sécurité créés (GRP_Admin, GRP_Compta, GRP_Stagiaire, GRP_RH)	✅
3	7 utilisateurs créés et affectés aux bons groupes	✅
4	Patrick DURAND membre des 4 groupes	✅
5	Rôle Espaces de noms DFS installé	✅
6	5 dossiers créés dans C:\Partages	✅
7	Namespace \\pxdc.local\Partages créé (type domaine)	✅
8	5 dossiers ajoutés dans le namespace avec cibles	✅
9	Permissions NTFS configurées par groupe	✅
10	Accès au namespace validé depuis l'Explorateur	✅

L'espace de noms DFS est désormais opérationnel. Les utilisateurs du domaine pxdc.local peuvent accéder à leurs dossiers de service via le chemin unique \\pxdc.local\Partages. L'accès est contrôlé par les groupes de sécurité Active Directory, garantissant l'isolation des données entre les différents services.