STRATÉGIES DE GROUPE (GPO)
MAPPAGE DE LECTEUR RÉSEAU

Déploiement automatisé du lecteur P: vers le namespace DFS

Mode opératoire — Procédure complète

Sasiraj GUNARATNARAJAH

BTS SIO — Option SISR

Année 2025 – 2026

Table des matières

1. Présentation

Ce document détaille la configuration des stratégies de groupe (GPO) pour le déploiement automatisé du mappage de lecteur réseau sur les postes clients du domaine pxdc.local. Cette documentation fait partie du projet d'infrastructure virtualisée sur Proxmox VE, dans le cadre du BTS SIO option SISR.

Les GPO (Group Policy Objects) permettent de configurer et d'appliquer automatiquement des paramètres sur l'ensemble des postes et utilisateurs du domaine Active Directory. Dans notre cas, nous allons déployer un mappage de lecteur réseau pointant vers l'espace de noms DFS \\pxdc.local\Partages, afin que chaque utilisateur dispose automatiquement d'un accès centralisé aux dossiers partagés de l'entreprise.

1.1 Prérequis

Composant	Détail
Serveur	WS-DC-1 (Windows Server 2025) — 192.168.20.10
Domaine	pxdc.local
DFS Namespace	\\pxdc.local\Partages (configuré précédemment)
Groupes de sécurité	GRP_Admin, GRP_Compta, GRP_Stagiaire, GRP_RH
Permissions NTFS	Configurées par groupe sur chaque dossier
Poste client	Windows 11 — 192.168.50.10 (LAN-PDT, OPT1)

1.2 Stratégie de mappage

Plutôt que de créer un lecteur différent par service (P:, Q:, R:, S:, T:), nous adoptons la bonne pratique entreprise : un seul lecteur mappé pour tous les utilisateurs, pointant vers la racine du namespace DFS. Les permissions NTFS, configurées dans la documentation précédente, assurent automatiquement l'isolation des données entre les services.

Paramètre	Valeur
Nom de la GPO	GPO_Mappage_Lecteurs
Lettre de lecteur	P:
Chemin UNC	\\pxdc.local\Partages
Libellé	Partage
Action	Créer
Reconnecter	Oui
Liée à	pxdc.local (tout le domaine)
Ciblage	Aucun (tous les utilisateurs du domaine)

💡 Avantage de cette approche : un seul lecteur réseau, un seul point d'entrée. L'utilisateur voit les

5 dossiers (Administration, Comptabilite, Stagiaire, RH, Commun) mais ne peut accéder qu'aux dossiers autorisés par son groupe de sécurité.

1.3 Compétences BTS SIO mobilisées

Bloc	Compétence
B1	Gérer le patrimoine informatique — Déploiement centralisé de configuration
B5	Administrer les systèmes — GPO, mappage lecteurs, Active Directory
B6	Cybersécurité — Contrôle d'accès par permissions NTFS et groupes AD

2. Création de la GPO

2.1 Ouverture de la console GPMC

Ouvrir la console Gestion des stratégies de groupe (GPMC) depuis le Gestionnaire de serveur > Outils, ou en tapant gpmc.msc dans le menu Démarrer.

Dans la console GPMC, développer l'arborescence : Forêt : pxdc.local > Domaines > pxdc.local.

2.2 Création de l'objet GPO

Effectuer un clic droit sur pxdc.local, puis sélectionner « Créer un objet GPO dans ce domaine, et le lier ici... ».

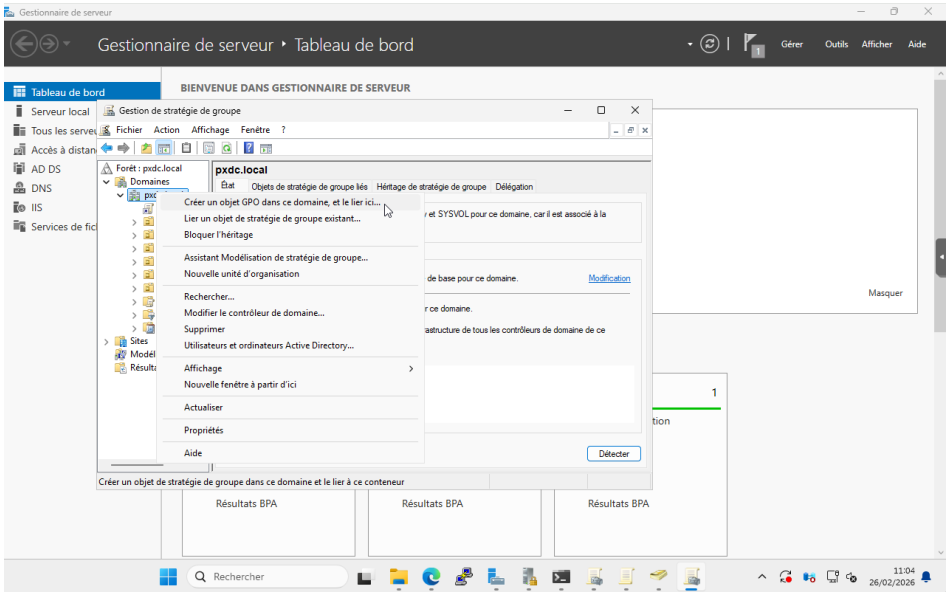

Figure 1 — Clic droit sur le domaine pxdc.local > Créer un objet GPO

Dans la boîte de dialogue « Nouvel objet GPO », saisir le nom de la GPO : GPO_Mappage_Lecteurs. Laisser l'objet Starter GPO source sur (aucun), puis cliquer sur OK.

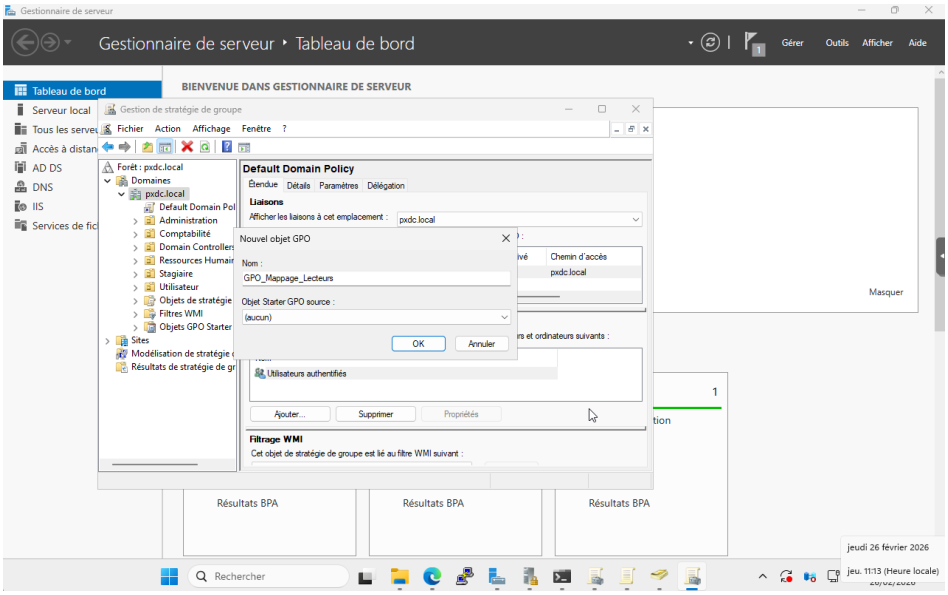

Figure 2 — Nom de la GPO : GPO_Mappage_Lecteurs

ℹ️ La GPO est créée et automatiquement liée à la racine du domaine pxdc.local. Elle s'appliquera donc à tous les utilisateurs et ordinateurs du domaine.

3. Configuration du mappage de lecteur

3.1 Édition de la GPO

Effectuer un clic droit sur GPO_Mappage_Lecteurs dans l'arborescence GPMC, puis sélectionner « Modifier ». L'éditeur de gestion des stratégies de groupe s'ouvre.

Naviguer dans l'arborescence suivante :

```
Configuration utilisateur
  └─ Préférences
       └─ Paramètres Windows
            └─ Mappages de lecteurs
```

3.2 Création du lecteur mappé

Effectuer un clic droit dans le panneau central de « Mappages de lecteurs », puis sélectionner Nouveau > Lecteur mappé.

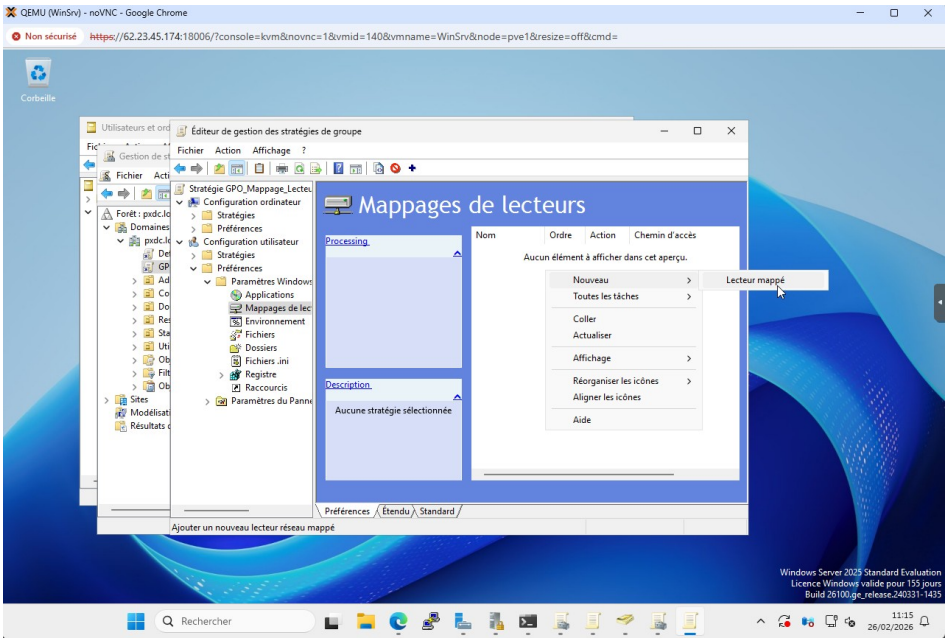

Figure 3 — Nouveau > Lecteur mappé dans l'éditeur GPO

3.3 Paramétrage du lecteur

Configurer les paramètres suivants dans la fenêtre « Propriétés de : P: » :

Paramètre	Valeur	Description
Action	Créer	Crée le lecteur à chaque connexion s'il n'existe pas
Emplacement	\\pxdc.local\Partages	Chemin UNC vers le namespace DFS
Reconnecter	Coché	Le lecteur persiste entre les sessions

Libellé	Partage	Nom affiché dans l'Explorateur de fichiers
Lettre de lecteur	P:	Utiliser > P

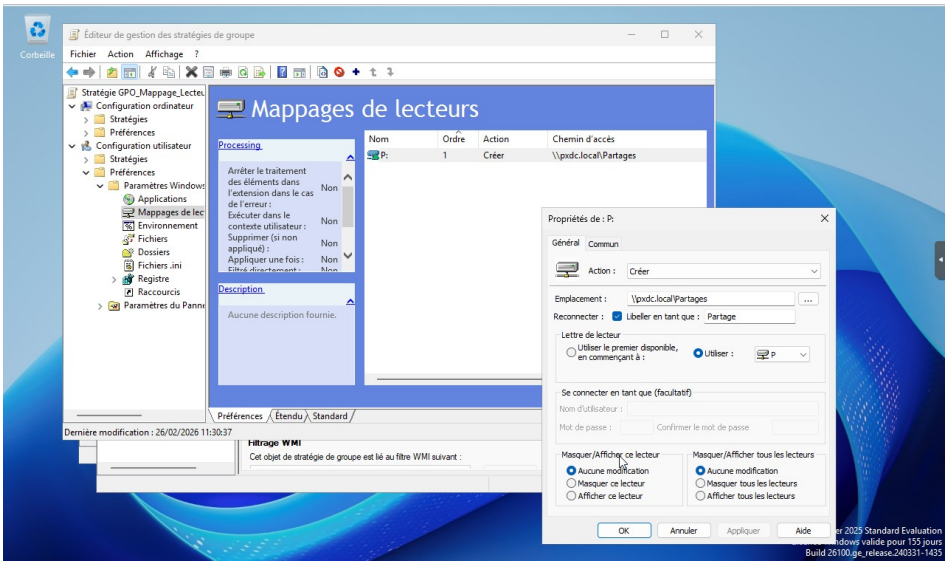

Figure 4 — Configuration complète du lecteur P: vers \\pxdc.local\Partages

Après validation, le lecteur P: apparaît dans la liste des mappages de lecteurs de la GPO avec l'action « Créer » et le chemin d'accès \\pxdc.local\Partages.

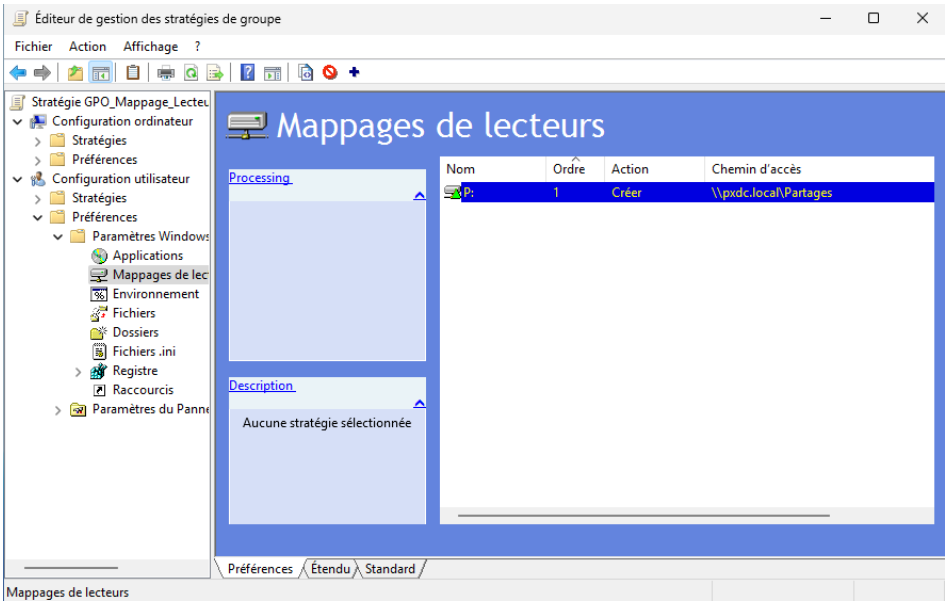

Figure 5 — Lecteur P: configuré dans la GPO

⚠️ Ne pas utiliser de chemin direct comme \\WS-DC-1\Partages. Toujours utiliser le chemin du namespace DFS (\\pxdc.local\Partages) pour garantir la transparence en cas de changement de serveur.

4. Application et vérification

4.1 Forcer l'application de la GPO

Après avoir validé la configuration, forcer l'application immédiate de la GPO sur le serveur :

```
gpupdate /force
```

Sur un poste client joint au domaine, la GPO s'appliquera automatiquement à la prochaine connexion de l'utilisateur, ou après exécution de gpupdate /force.

4.2 Vérification sur un poste client

Après jonction du poste Windows 11 au domaine pxdc.local et connexion avec le compte pdurand (PDG, membre des 4 groupes de sécurité), le lecteur P: (Partage) apparaît automatiquement dans l'Explorateur de fichiers.

Le lecteur P: donne accès aux 5 dossiers du namespace DFS :

- Administration
- Commun
- Comptabilite
- RH
- Stagiaire

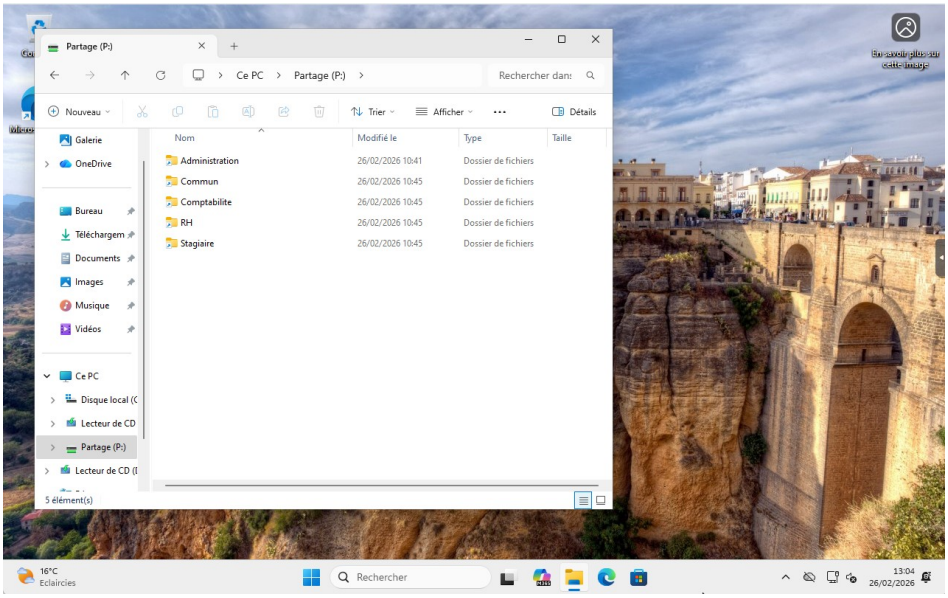

Figure 6 — Lecteur P: (Partage) sur le poste Windows 11, connecté en tant que pdurand

💡 Patrick DURAND (PDG) a accès à tous les dossiers car il est membre des 4 groupes de sécurité (GRP_Admin, GRP_Compta, GRP_Stagiaire, GRP_RH). Les autres utilisateurs ne verront le contenu que des dossiers autorisés par leur groupe + le dossier Commun.

5. Matrice de tests des accès

Le tableau suivant résume le comportement attendu lors de l'accès au lecteur P: selon le profil de l'utilisateur connecté :

Utilisateur	Service	Administration	Comptabilite	Stagiaire	RH	Commun
pdurand	PDG	✅	✅	✅	✅	✅
trouget	Compta	❌	✅	❌	❌	✅
pabadie	Compta	❌	✅	❌	❌	✅
vrigon	Stagiaire	❌	❌	✅	❌	✅
lguerin	Stagiaire	❌	❌	✅	❌	✅
spale	RH	❌	❌	❌	✅	✅
snoir	RH	❌	❌	❌	✅	✅

ℹ️ Le contrôle d'accès est entièrement géré par les permissions NTFS configurées sur les dossiers. La GPO se contente de mapper le lecteur P: sans filtrage supplémentaire.

6. Résumé de l'architecture

6.1 Vue d'ensemble

Le schéma suivant résume le flux complet, de la GPO jusqu'aux données :

```
GPO_Mappage_Lecteurs (liée à pxdc.local)
  │
  └── Lecteur P: → \\pxdc.local\Partages (DFS Namespace)
        │
        ├── Administration\  → GRP_Admin
        ├── Comptabilite\    → GRP_Compta
        ├── Stagiaire\       → GRP_Stagiaire
        ├── RH\              → GRP_RH
        └── Commun\          → Utilisateurs du domaine
```

6.2 Avantages

- Un seul lecteur réseau (P:) pour tous les utilisateurs, simple et intuitif
- Chemin DFS transparent : si le serveur de fichiers change, aucune modification de la GPO nécessaire
- Permissions NTFS par groupe : l'isolation des données est gérée au niveau du système de fichiers
- Maintenance simplifiée : ajout d'un nouveau service = créer un dossier + un groupe, sans modifier la GPO
- Scalable : fonctionne identiquement avec 5 ou 50 dossiers de service

7. Synthèse et points de vérification

#	Point de vérification	Statut
1	Console GPMC ouverte (gpmc.msc)	✅
2	GPO GPO_Mappage_Lecteurs créée	✅
3	GPO liée au domaine pxdc.local	✅
4	Mappage lecteur P: configuré vers \\pxdc.local\Partages	✅
5	Action = Créer, Reconnecter = Oui, Libellé = Partage	✅
6	Pas de ciblage (tous les utilisateurs)	✅
7	gpupdate /force exécuté sur le serveur	✅
8	Test poste Windows 11 : lecteur P: visible	✅
9	Test accès pdurand : 5 dossiers accessibles	✅

La GPO de mappage de lecteur réseau est configurée, active et validée sur le domaine pxdc.local. Chaque utilisateur qui se connecte sur un poste du domaine voit automatiquement le lecteur P: (Partage) dans son Explorateur de fichiers, avec un accès contrôlé par les groupes de sécurité Active Directory et les permissions NTFS.