

# IMPLANTATION DES DONNÉES

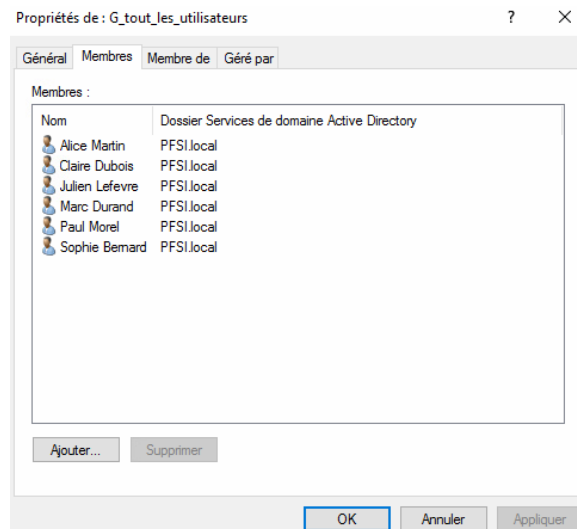
## Choix du système de gestion de fichiers (SGF)

Nous avons choisi **Windows Server 2016** comme système de fichiers, car il permet une gestion fine des permissions, une intégration complète à l'Active Directory (AD), et une facilité de déploiement via les stratégies de groupe (GPO). Le partage SMB est utilisé pour l'accès aux répertoires via le réseau.

## 1. Création des groupes dans l'Active Directory

Pour organiser les permissions d'accès aux répertoires partagés, on commence par créer les groupes de sécurité dans l'Active Directory:

- G\_service\_administratif -> Claire Dubois
- G\_service\_commercial -> Alice Martin et Julien Lefevre
- G\_service\_logistique -> Marc Durand
- G\_service\_rh -> Sophie Bernard
- G\_delegates\_syndicaux -> Paul Morel
- G\_tous\_les\_utilisateurs

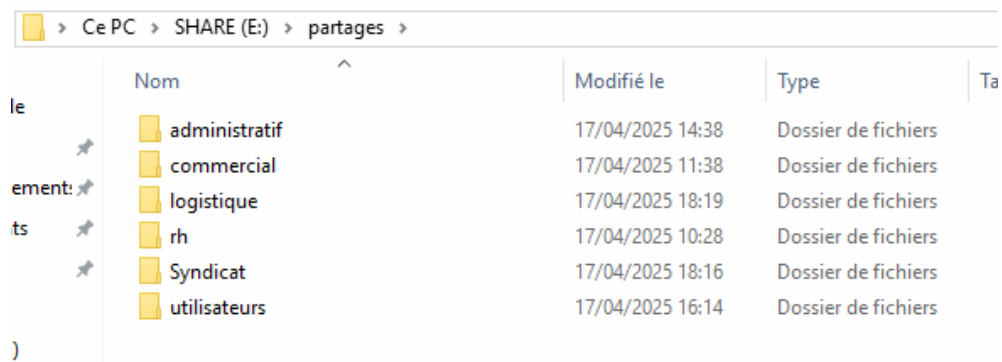


	Alice Martin	Utilisateur
	Claire Dubois	Utilisateur
	G_delegates_syndicaux	Groupe de séc...
	G_service_administratif	Groupe de séc...
	G_service_commercial	Groupe de séc...
	G_service_logistique	Groupe de séc...
	G_service_rh	Groupe de séc...
	G_tout_les_utilisateurs	Groupe de séc...
	Julien Lefevre	Utilisateur
	Marc Durand	Utilisateur
	Paul Morel	Utilisateur
	Sophie Bernard	Utilisateur

2. Création de l’arborescence des dossiers

Créer la structure suivante sur une partition dédiée (E:\partages) :

- E:\partages\administratif
- E:\partages\commercial\commandes
- E:\partages\logistique
- E:\partages\rh
- E:\partages\Syndicat
- E:\partages\utilisateurs\[nom utilisateur]

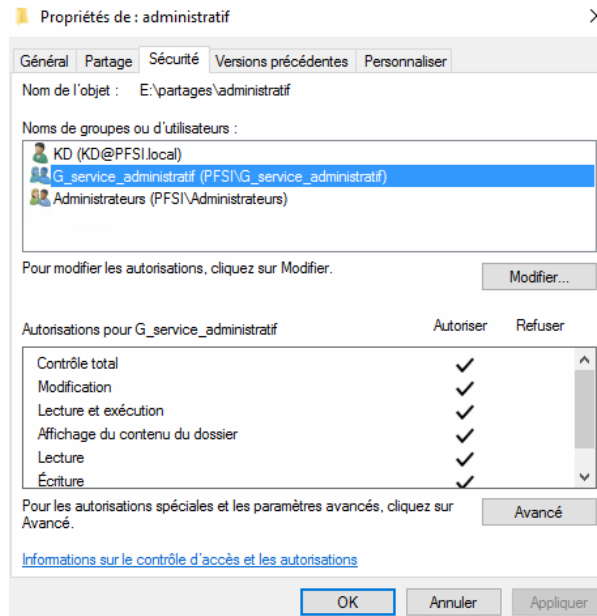


Groupe AD	Dossiers accessibles	Droits
G_service_administratif	Tous les répertoires communs	Lecture
G_service_commercial	Commercial	Lecture/Écriture
G_service_logistique	Logistique, Projets, Commandes (lecture)	Lecture/Écriture
G_service_rh	RH	Lecture/Écriture
G_delegates_syndicaux	Syndicat	Lecture/Écriture
Tous les utilisateurs	Syndicat	Lecture

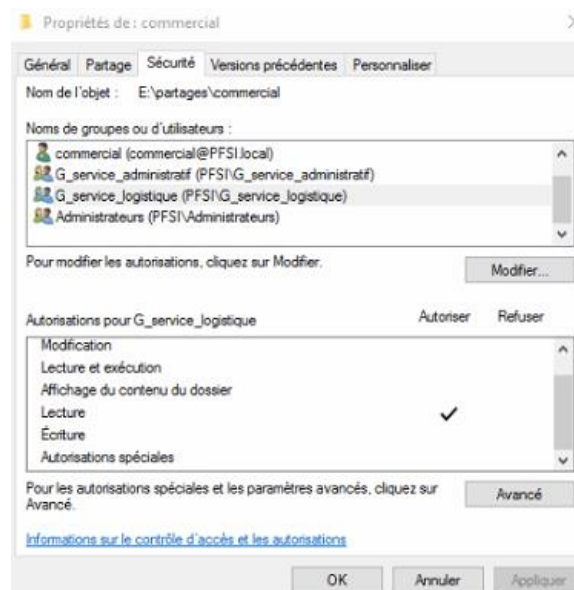
### 3. Partage des dossiers et configuration des permissions

Configurer les partages avancés et les autorisations NTFS comme suit :

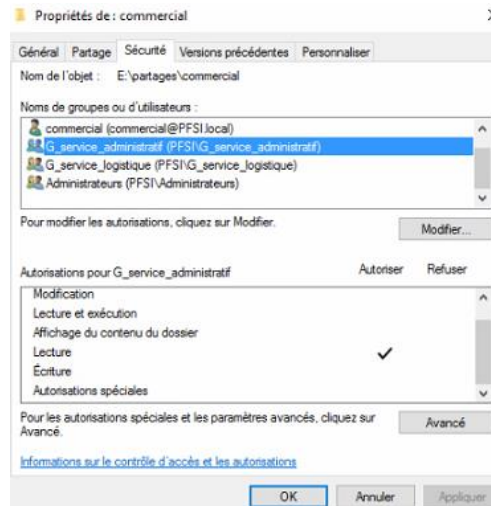
- Le service propriétaire a un accès complet à son dossier.



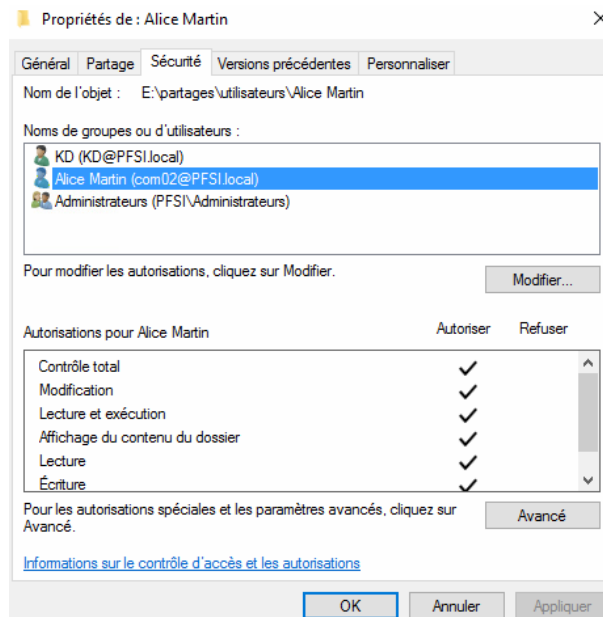
- Le service logistique a un accès en lecture au dossier commercial.



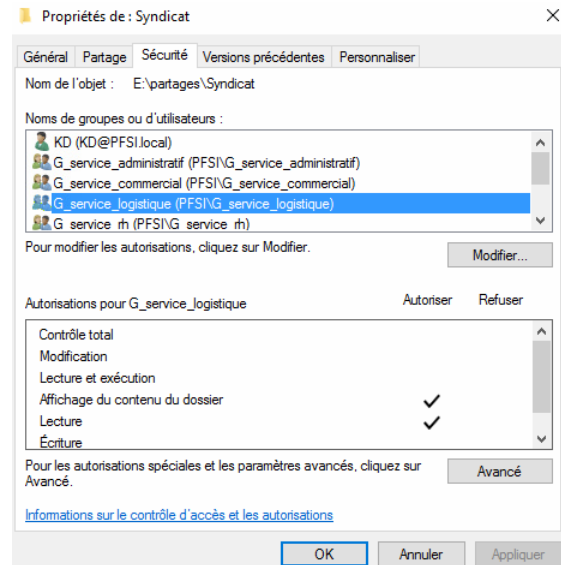
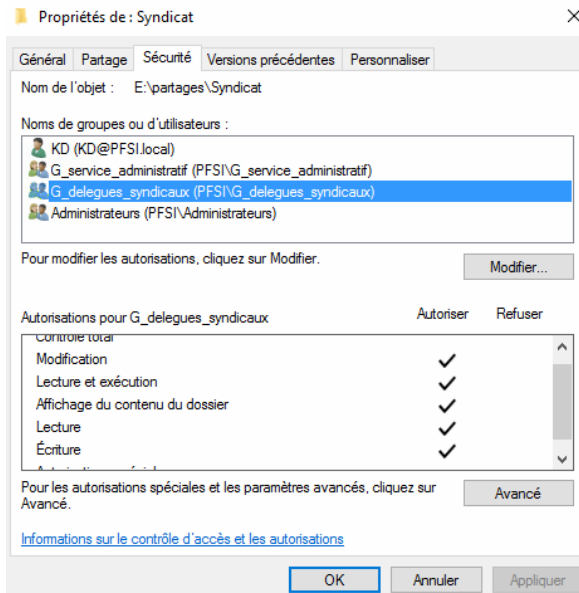
- Le service administratif a un accès en lecture à tous les dossiers. (exemple avec le dossier commercial)



- Les dossiers personnels ne sont accessibles que par l'utilisateur concerné.



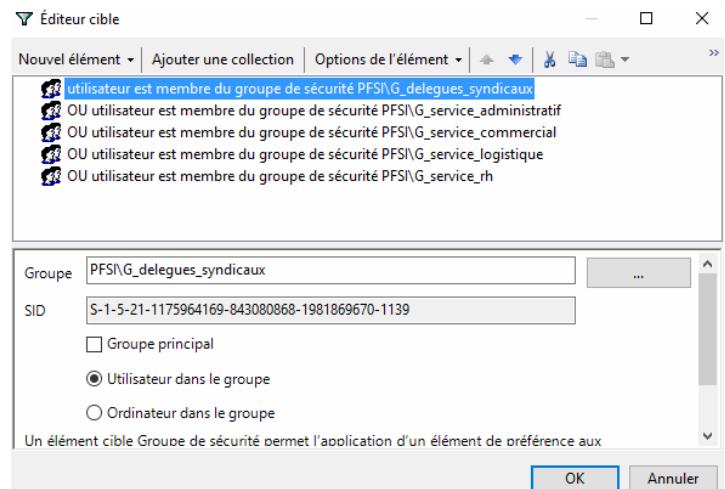
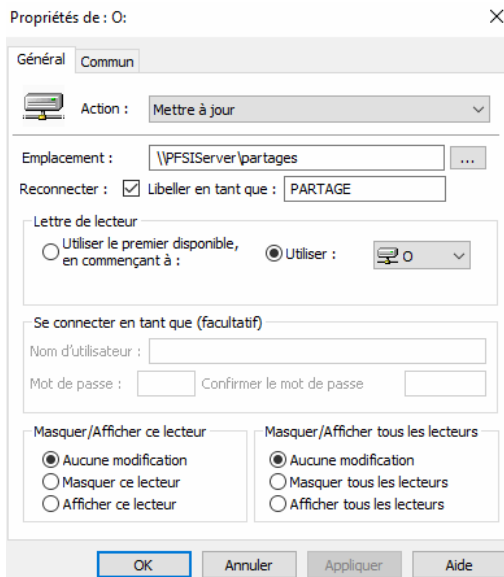
- Le dossier Syndicat est en lecture pour tous, modification pour les délégués syndicaux.



#### 4. Montage automatique des lecteurs via GPO

Créer une GPO dédiée pour le montage automatique des lecteurs réseau :

1. Ouvrir GPMC.msc.
2. Créer une GPO nommée "lecteur\_reseau".
3. Ajouter les lecteurs mappés via : Configuration utilisateur > Préférences > Lecteurs mappés.
4. Définir le ciblage pour chaque groupe AD concerné.



## 5. Politique de sauvegarde et risques

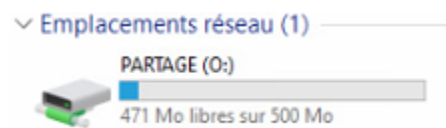
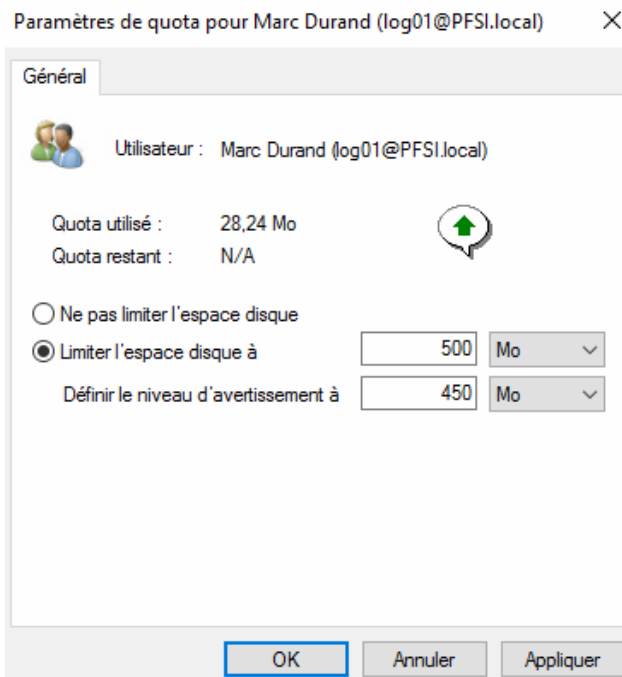
### 3. Politique de sécurité et analyse des risques

#### 3.1 Politique de sécurité actuelle

- **Sauvegarde :**
  - Uniquement les bases de données et les fichiers des services
- **Contrôle d'accès :**
  - Basé sur les groupes AD
- **Automatisation :**
  - Scripts de montage et répertoires via GPO
- **Quota :**
  - Défini par service pour éviter la saturation disque

### Gestion des quotas

La gestion des quotas permet de limiter l'espace disque utilisé par chaque utilisateur ou groupe sur le serveur de fichiers. Cela évite la saturation du disque dur et permet un contrôle plus précis des ressources utilisées par chaque service.



### 3.2 Risques encourus

Élément non sauvegardé	Risque potentiel
Données personnelles utilisateurs	Perte définitive des données critiques en cas de panne
Fichiers de configuration serveurs	Reconfiguration manuelle fastidieuse en cas de crash
Absence de redondance	Service indisponible en cas de défaillance matérielle
Sauvegardes non externalisées	Données vulnérables aux incidents locaux (incendie, vol...)

Il est fortement recommandé d'améliorer la politique de sauvegarde en incluant :

- Les répertoires personnels
- Les fichiers de configuration (export régulier)
- Une **sauvegarde externalisée** (Cloud, NAS distant, etc.)

### Conclusion

L'implantation des données de GSB sur un serveur de fichiers centralisé et sécurisé permet une organisation claire, un contrôle des accès rigoureux, et une automatisation des tâches de connexion. Cependant, la stratégie de sauvegarde doit être renforcée pour garantir la pérennité des services informatiques.

-