

# FICHE D'ACTIVITÉ : Mise en place d'un partage de fichiers avec permissions selon les services sous Active Directory Windows Server 2022

## Contexte de la mission

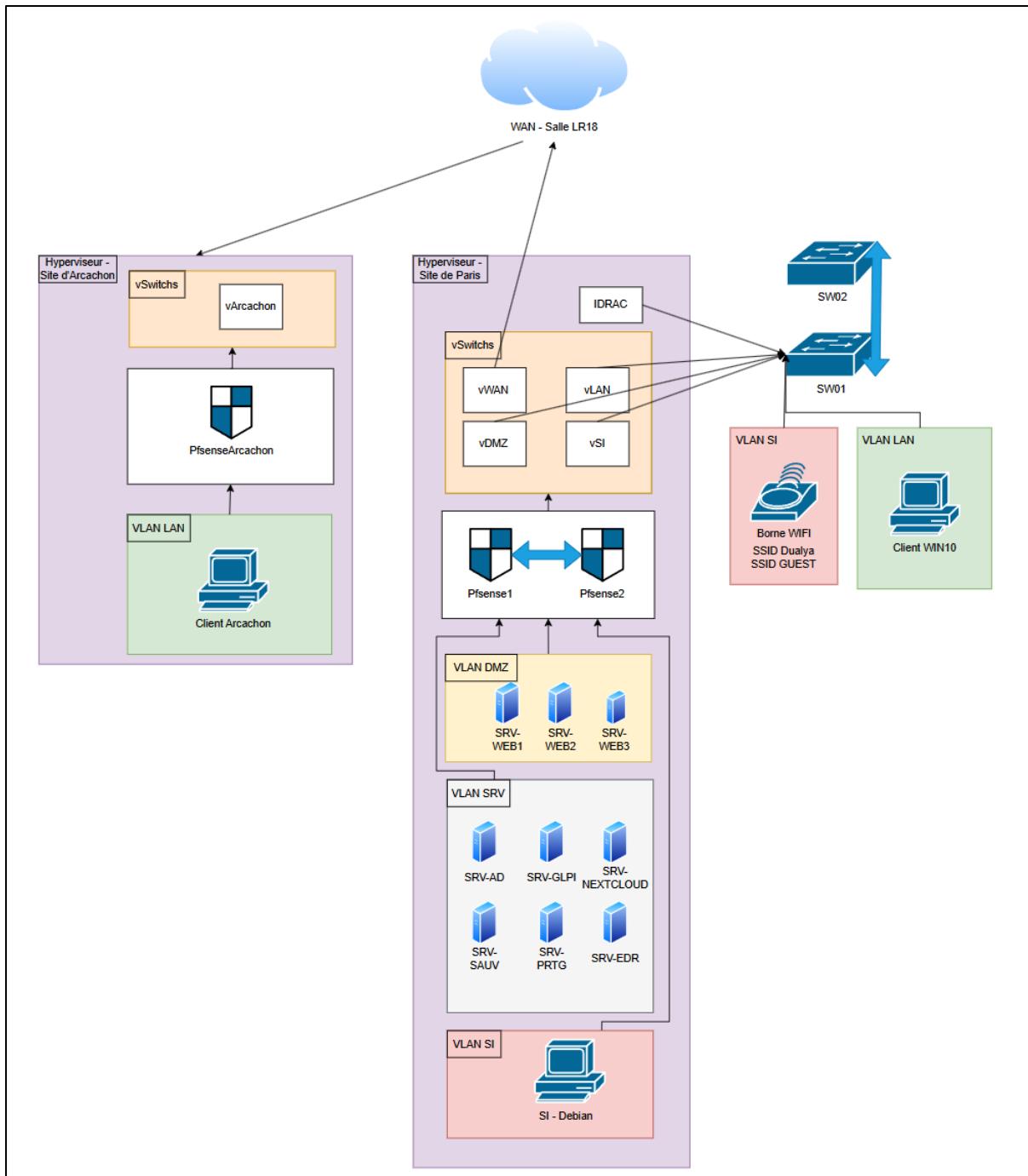
L'entreprise DUALYA souhaite centraliser ses documents sur un serveur de fichiers Windows Server, tout en assurant une sécurité optimale par service. Chaque service (Administration, Informatique, RH, Comptabilité et Direction) doit avoir accès à un dossier dédié avec des permissions restrictives, garantissant ainsi la confidentialité et l'intégrité des données.

L'entreprise DUALYA fait alors appel à notre société, Pear to Peer, afin de mettre en place leur infrastructure et ainsi nous confie cette mission. Nous serons également amené à modifier l'infrastructure, c'est pourquoi il est important de documenter chaque étape afin de ne rien omettre.

## Table des matières

Contexte de la mission .....	1
Topologie logique de l'infrastructure .....	3
Veille effectuée avant-projet / étude et choix de la solution .....	4
Étape du projet.....	5
Liste du matériel / inventaire .....	6
Plan logique / physique / Schéma si nécessaire .....	6
Plan logique :.....	6
Plan physique :.....	6
Déroulement de la mission en lien avec les compétences .....	7
A. Création des groupes Active Directory en respectant la méthode AGDLP .....	7
1. Création des groupes globaux (GG_) pour chaque service.....	7
2. Création des groupes locaux de domaine (GDL_) en fonction des permissions .....	8
3. Ajout des groupes globaux dans les groupes locaux correspondants .....	9
4. Gestion des permissions spécifiques (exemple de la Direction et du dossier RH).....	10
B. Création des dossiers et permissions NTFS.....	11
C. Partage des dossiers via SMB.....	14
Amélioration continue possible (Revue régulière du projet, axes d'amélioration).....	15
Sensibilisation des collaborateurs.....	15
Conclusion.....	15

## Topologie logique de l'infrastructure



# Veille effectuée avant-projet / étude et choix de la solution

Avant de mettre en place cette solution, une étude des besoins a été réalisée :

- Analyse des services nécessitant un espace de stockage dédié.
- Étude des différentes méthodes de gestion des permissions sous Windows Server.
- Comparaison des stratégies de gestion des accès (AGDLP, permissions directes, groupes imbriqués).
- Vérification des solutions de sauvegarde adaptées pour garantir la disponibilité des fichiers en cas de panne ou de suppression accidentelle.

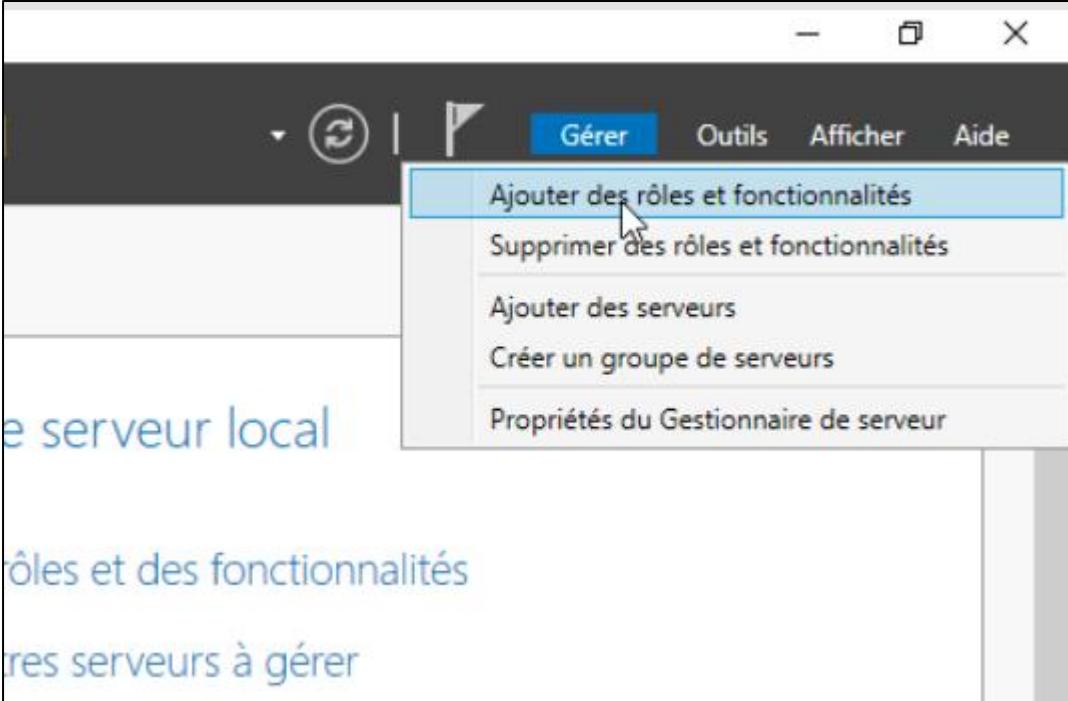
Après analyse, la méthode AGDLP (Account → Groupe Global → Groupe Domaine Local → Permission) a été retenue pour une gestion optimale et évolutive des droits d'accès. En effet, elle permet une **gestion claire, centralisée et évolutive des autorisations** : les utilisateurs sont ajoutés à des groupes globaux selon leur rôle ou service, puis ces groupes sont intégrés à des groupes de domaine local affectés aux permissions NTFS ou de partage sur les serveurs.

Cela **facilite l'audit, limite les erreurs humaines, et réduit les interventions manuelles** en cas de changement d'équipe ou de personnel. En séparant la logique métier (groupes globaux) de la logique technique (groupes locaux), AGDLP garantit une **meilleure sécurité, un meilleur cloisonnement des accès, et une administration simplifiée au quotidien**.

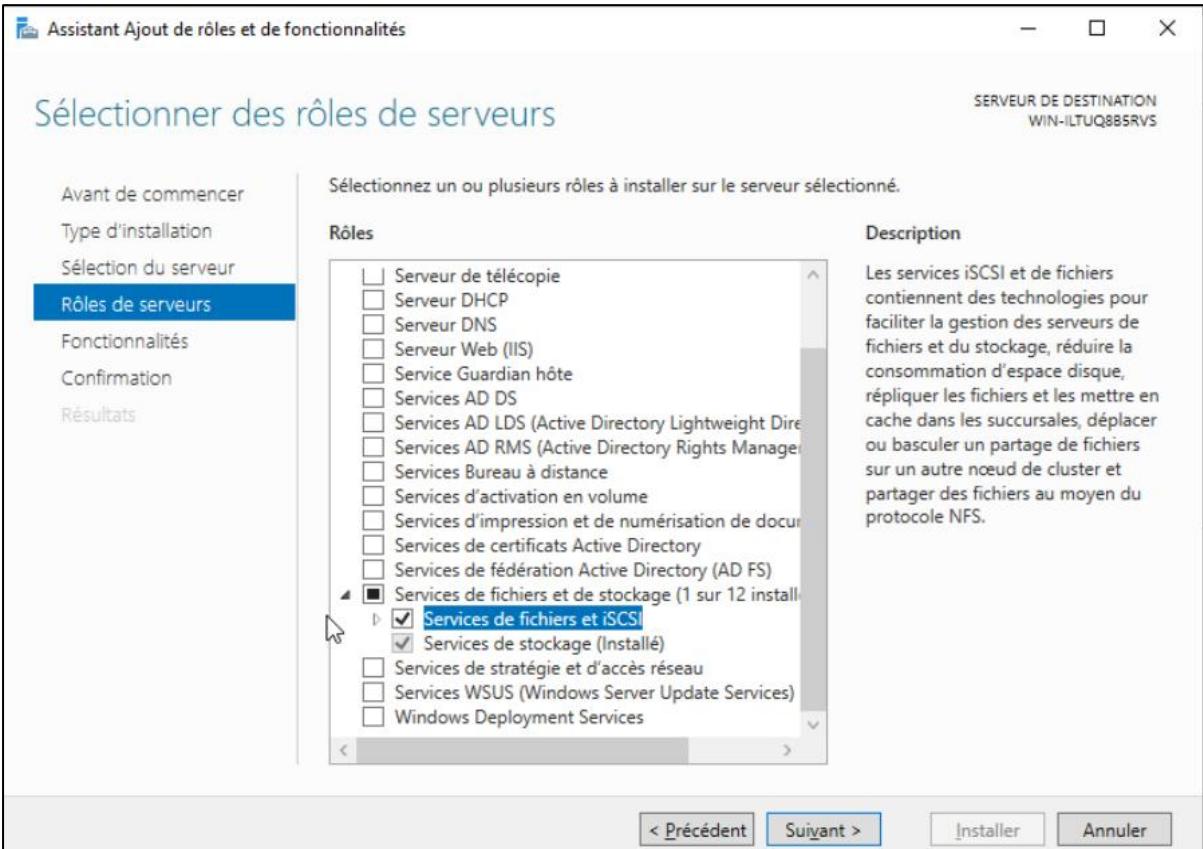
# Étape du projet

Les étapes suivantes ont été planifiées et réalisées :

1. Installation et configuration du rôle Serveur de fichiers sous Windows Server.



The screenshot shows the Windows Server Management Console. A context menu is open over a server node labeled 'Le serveur local'. The 'Ajouter des rôles et fonctionnalités' option is highlighted with a blue selection bar. Other options in the menu include 'Supprimer des rôles et fonctionnalités', 'Ajouter des serveurs', 'Créer un groupe de serveurs', and 'Propriétés du Gestionnaire de serveur'.

The screenshot shows the 'Assistant Ajout de rôles et de fonctionnalités' (Add Roles and Features Wizard). The title bar says 'Assistant Ajout de rôles et de fonctionnalités'. The main window is titled 'Sélectionner des rôles de serveurs' and shows the 'SERVEUR DE DESTINATION WIN-ILTUQ8B5RVS'. On the left, a navigation pane lists steps: 'Avant de commencer', 'Type d'installation', 'Sélection du serveur', 'Rôles de serveurs' (which is selected and highlighted in blue), 'Fonctionnalités', 'Confirmation', and 'Résultats'. The main area displays a table with two columns: 'Rôles' and 'Description'. The 'Rôles' column lists various server roles with checkboxes. The 'Description' column provides a detailed explanation for each role. In the 'Rôles' column, several checkboxes are checked, including 'Serveur de télécopie', 'Services AD DS', 'Services AD LDS (Active Directory Lightweight Directory Services)', 'Services AD RMS (Active Directory Rights Management Services)', 'Services Bureau à distance', 'Services d'activation en volume', 'Services d'impression et de numérisation de documents', 'Services de certificats Active Directory', 'Services de fédération Active Directory (AD FS)', 'Services de fichiers et de stockage (1 sur 12 installé)', 'Services de stockage (Installé)', 'Services de stratégie et d'accès réseau', 'Services WSUS (Windows Server Update Services)', and 'Windows Deployment Services'. The 'Description' column for the 'Services de fichiers et de stockage' role states: 'Les services iSCSI et de fichiers contiennent des technologies pour faciliter la gestion des serveurs de fichiers et du stockage, réduire la consommation d'espace disque, répliquer les fichiers et les mettre en cache dans les succursales, déplacer ou basculer un partage de fichiers sur un autre nœud de cluster et partager des fichiers au moyen du protocole NFS.'

Puis, en cliquant sur « Suivant » puis « Installer », le service de fichiers et de stockage sera installé sur le serveur.

2. Création des groupes Active Directory en respectant la méthode AGDLP.
3. Mise en place des permissions NTFS et des partages SMB.
4. Tests et validations des accès avec différents utilisateurs.
5. Documentation et sensibilisation des collaborateurs.
6. Mise en place d'une solution de sauvegarde automatique.

## Liste du matériel / inventaire

- Un serveur Windows Server 2022 avec Active Directory et le rôle Serveur de fichiers installé.
- Un réseau fonctionnel avec des clients sous Windows.
- Comptes utilisateurs et groupes AD préalablement configurés.
- Un NAS ou un autre support de stockage pour la sauvegarde des fichiers.
- Une infrastructure réseau sécurisée pour éviter les accès non autorisés.

## Plan logique / physique / Schéma si nécessaire

### Plan logique :

- Organisation des utilisateurs en groupes globaux (GG\_) par service.
- Attribution des droits via des groupes de domaine local (GDL\_).
- Permissions définies en fonction des besoins d'accès (CO, RW, RO).

### Plan physique :

- Un serveur de fichiers centralisé sous Windows Server 2022.
- Stockage des données sur un volume C:\Partages dédié aux partages.

# Déroulement de la mission en lien avec les compétences

## A. Création des groupes Active Directory en respectant la méthode AGDLP

### 1. Création des groupes globaux (GG\_) pour chaque service

- GG\_Admin
- GG\_Info
- GG\_RH
- GG\_Compta
- GG\_Direction Ajout des utilisateurs de chaque service dans leur groupe respectif.

Dans un premier temps, créons une OU « DUALYA » afin de regrouper tout nos utilisateurs et groupes et ainsi les séparer des groupes et utilisateurs Builtin.

The screenshot shows the Windows Server 2008 Active Directory Users and Computers (ADUC) console. The left pane displays a tree view of the directory structure under 'Utilisateurs et ordinateurs Active Directory'. A 'DUALYA' container is selected. The right pane is a table listing five global groups:

Nom	Type	Description
GG_Admin	Groupe de sécurité	
GG_Compta	Groupe de sécurité	
GG_Direction	Groupe de sécurité	
GG_Info	Groupe de sécurité	
GG_RH	Groupe de sécurité	

## 2. Création des groupes locaux de domaine (GDL\_) en fonction des permissions

Pour chaque service, trois groupes ont été créés :

- **CO (Contrôle Total)** : Gestion complète des fichiers et dossiers.
- **RW (Lecture-Écriture)** : Modification des fichiers sans suppression des permissions.
- **RO (Lecture Seule)** : Consultation des fichiers uniquement.

Exemple pour le service RH :

- GDL\_RH\_CO → contrôle total sur D:\Partages\RH
- GDL\_RH\_RW → lecture et écriture sur D:\Partages\RH
- GDL\_RH\_RO → lecture seule sur D:\Partages\RH

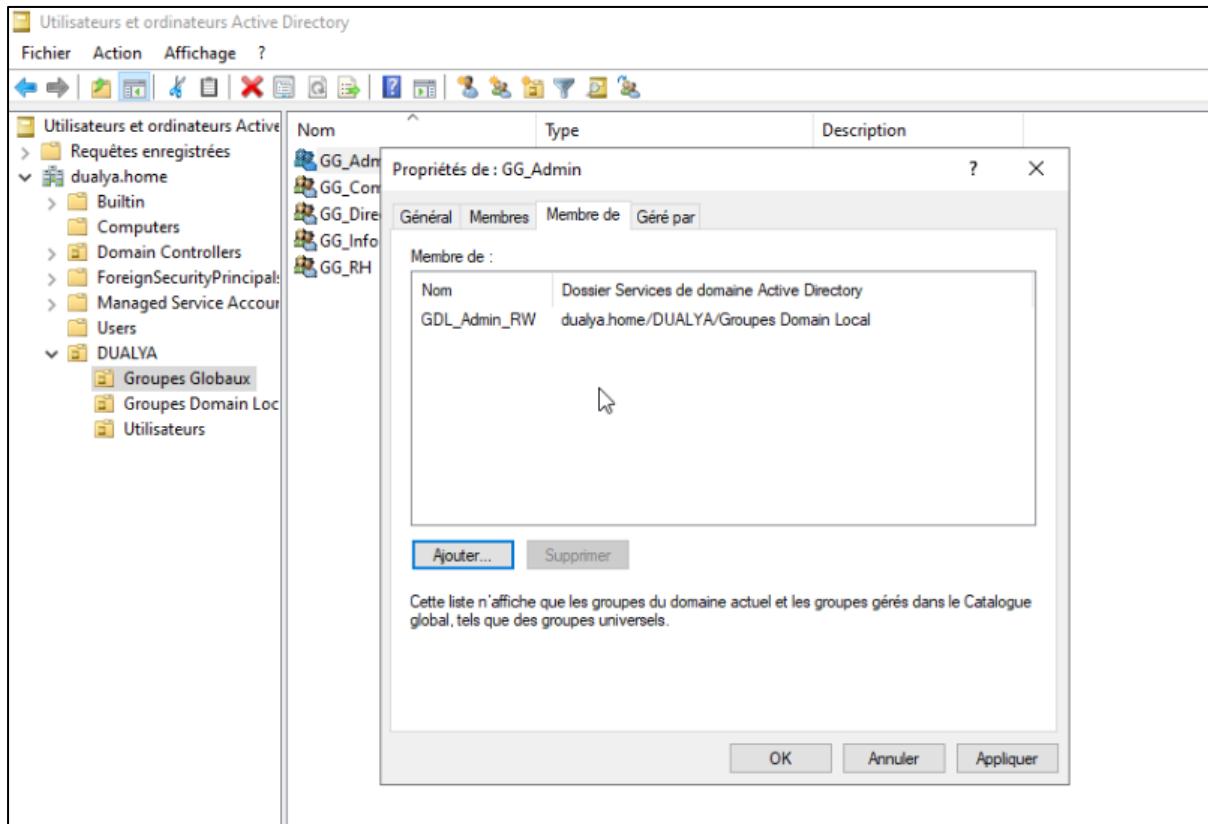
Même logique appliquée aux autres services :

- GDL\_Admin\_CO, GDL\_Admin\_RW, GDL\_Admin\_RO
- GDL\_Info\_CO, GDL\_Info\_RW, GDL\_Info\_RO
- GDL\_Compta\_CO, GDL\_Compta\_RW, GDL\_Compta\_RO
- GDL\_Direction\_CO, GDL\_Direction\_RW, GDL\_Direction\_RO

Utilisateurs et ordinateurs Active Directory			
Fichier	Action	Affichage	?
Utilisateurs et ordinateurs Active			
> Requêtes enregistrées			
dualya.home			
> Builtin			
Computers			
> Domain Controllers			
> ForeignSecurityPrincipal:			
> Managed Service Accour			
Users			
DUALYA			
Groupes Globaux			
Groupes Domain Loc			
Utilisateurs			
	Nom	Type	Description
	GDL_Admin_FC	Groupe de sécurité - Domaine local	
	GDL_Admin_RO	Groupe de sécurité - Domaine local	
	GDL_Admin_RW	Groupe de sécurité - Domaine local	
	GDL_Compta_FC	Groupe de sécurité - Domaine local	
	GDL_Compta_RO	Groupe de sécurité - Domaine local	
	GDL_Compta_RW	Groupe de sécurité - Domaine local	
	GDL_Direction_FC	Groupe de sécurité - Domaine local	
	GDL_Direction_RO	Groupe de sécurité - Domaine local	
	GDL_Direction_RW	Groupe de sécurité - Domaine local	
	GDL_Info_FC	Groupe de sécurité - Domaine local	
	GDL_Info_RO	Groupe de sécurité - Domaine local	
	GDL_Info_RW	Groupe de sécurité - Domaine local	
	GDL_RH_FC	Groupe de sécurité - Domaine local	
	GDL_RH_RO	Groupe de sécurité - Domaine local	
	GDL_RH_RW	Groupe de sécurité - Domaine local	

### 3. Ajout des groupes globaux dans les groupes locaux correspondants

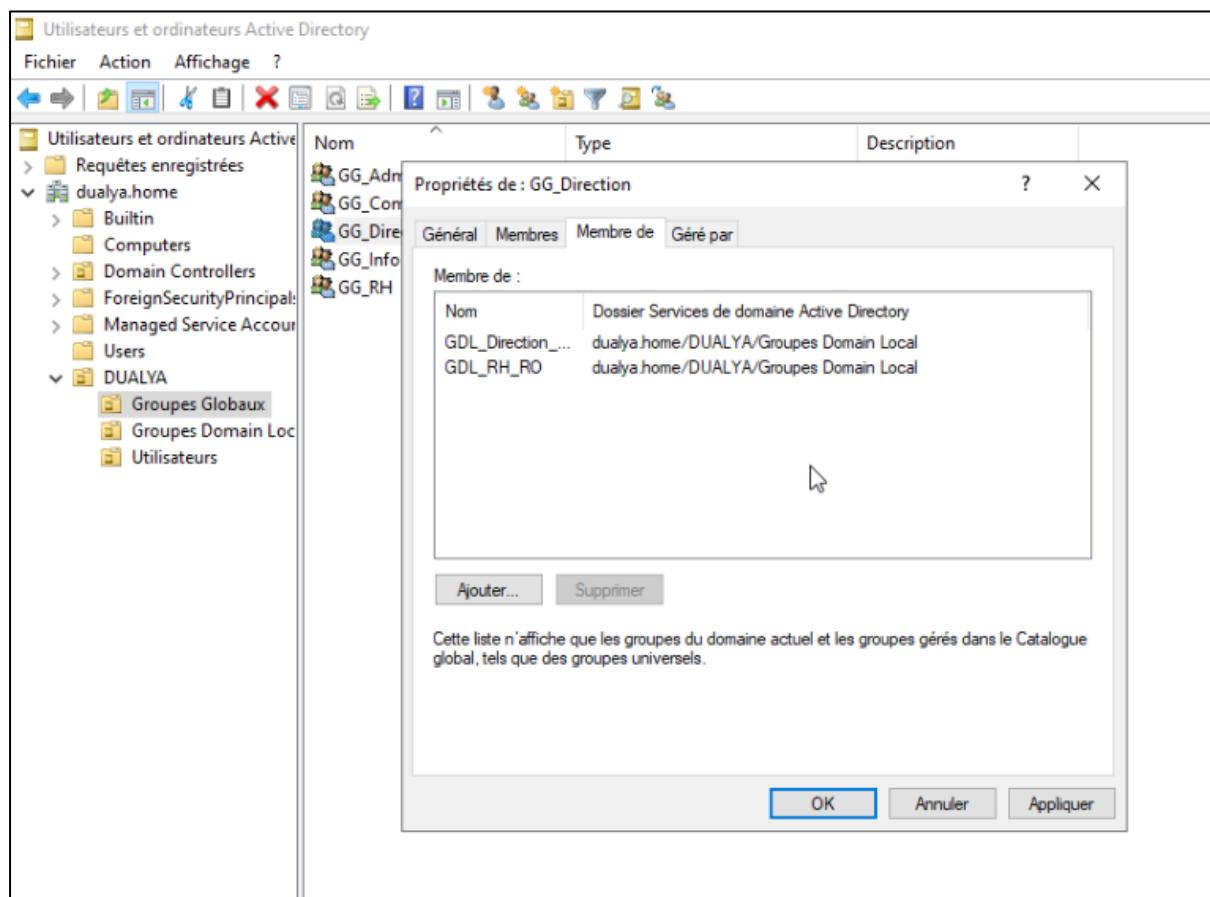
- GG\_Admin → GDL\_Admin\_RW
- GG\_Info → GDL\_Info\_RW
- GG\_RH → GDL\_RH\_RW
- GG\_Compta → GDL\_Compta\_RW
- GG\_Direction → GDL\_Direction\_RW



Répéter cette étape pour tous les groupes respectivement.

#### 4. Gestion des permissions spécifiques (exemple de la Direction et du dossier RH)

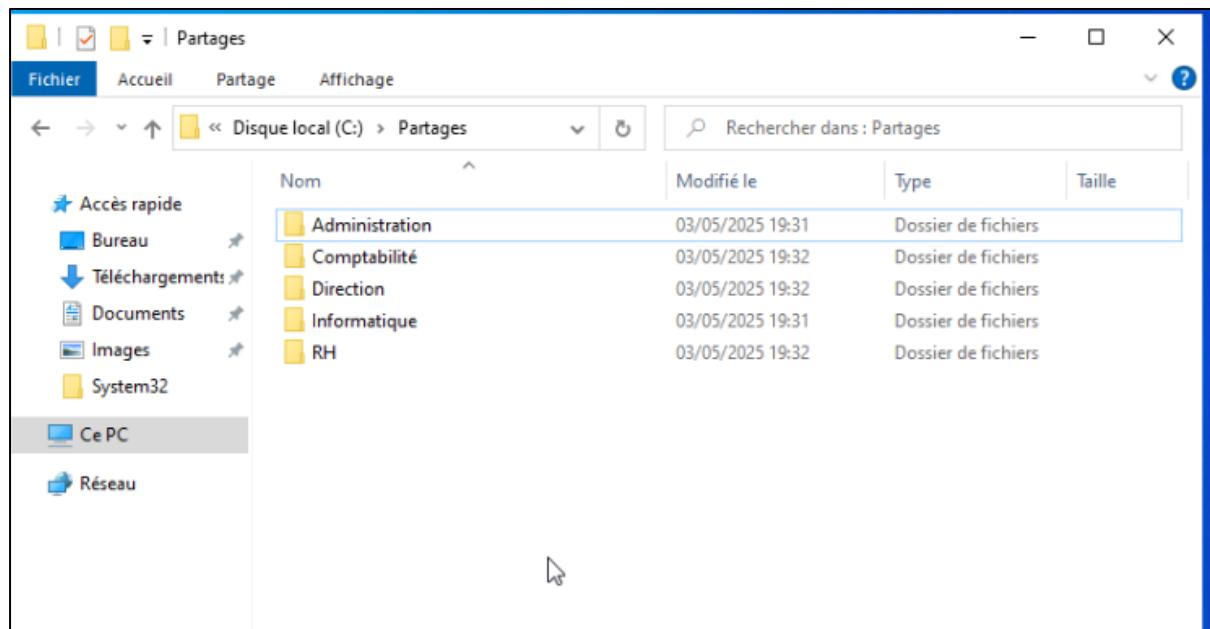
- La Direction doit avoir un accès en lecture seule au dossier RH.
- Plutôt que d'attribuer directement les permissions aux utilisateurs de la Direction, on applique la méthode AGDLP :
  - Ajouter GG\_Direction dans GDL\_RH\_RO.
  - GDL\_RH\_RO ayant une permission lecture seule (RO) sur D:\Partages\RH, tous les membres de GG\_Direction peuvent accéder en lecture seule à ce dossier.



## B. Création des dossiers et permissions NTFS

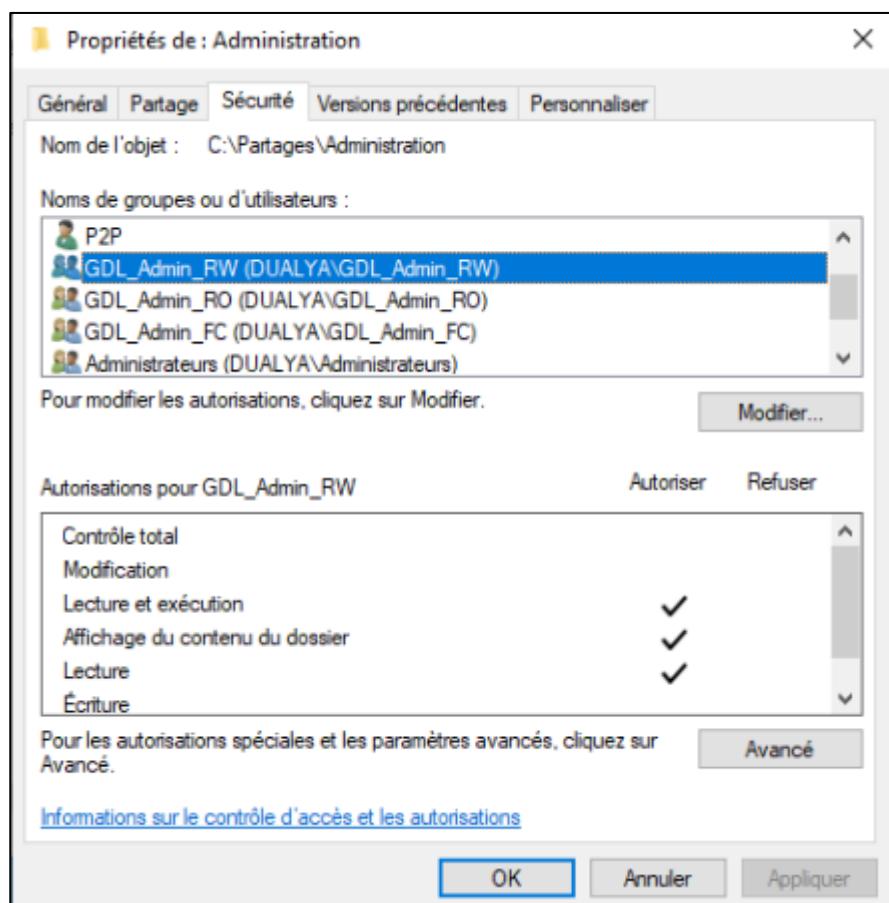
### 1. Crédation de la structure des dossiers :

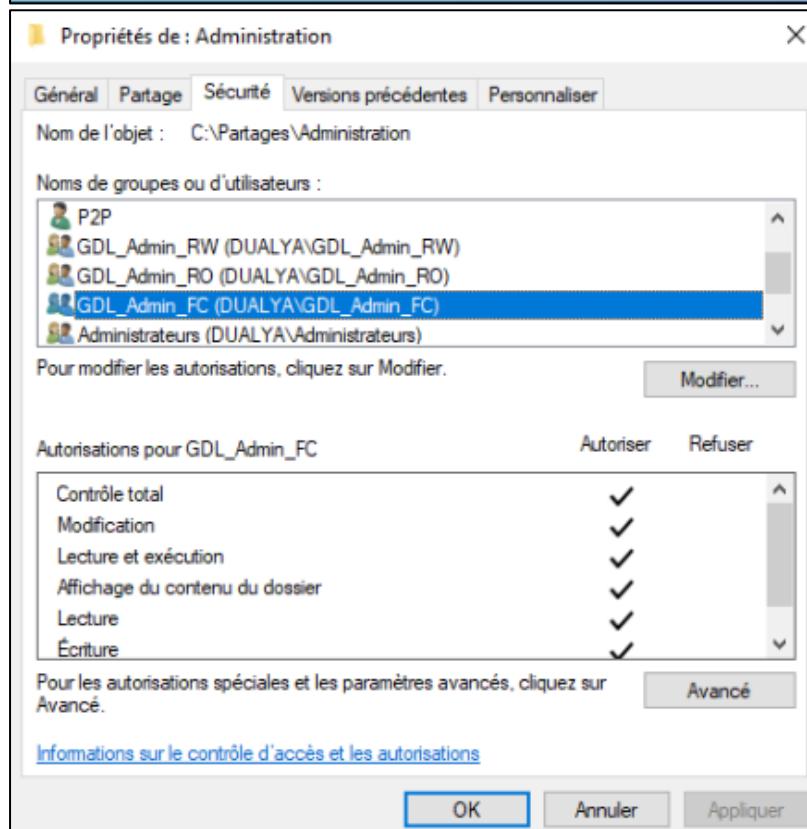
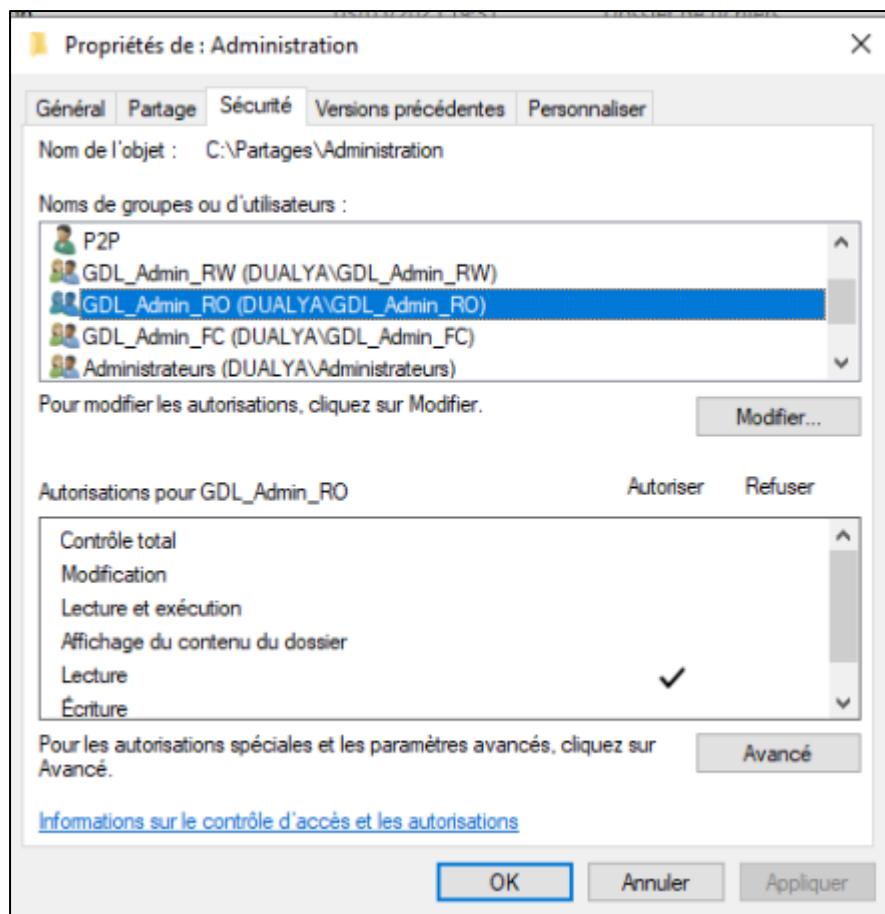
- o C:\Partages\Administration
- o C:\Partages\Informatique
- o C:\Partages\RH
- o C:\Partages\Comptabilité
- o C:\Partages\Direction



2. Définition des permissions NTFS :

- Suppression de "Tout le monde" pour éviter les accès non contrôlés.
- Ajout des groupes GDL\_ correspondants avec les permissions adaptées.



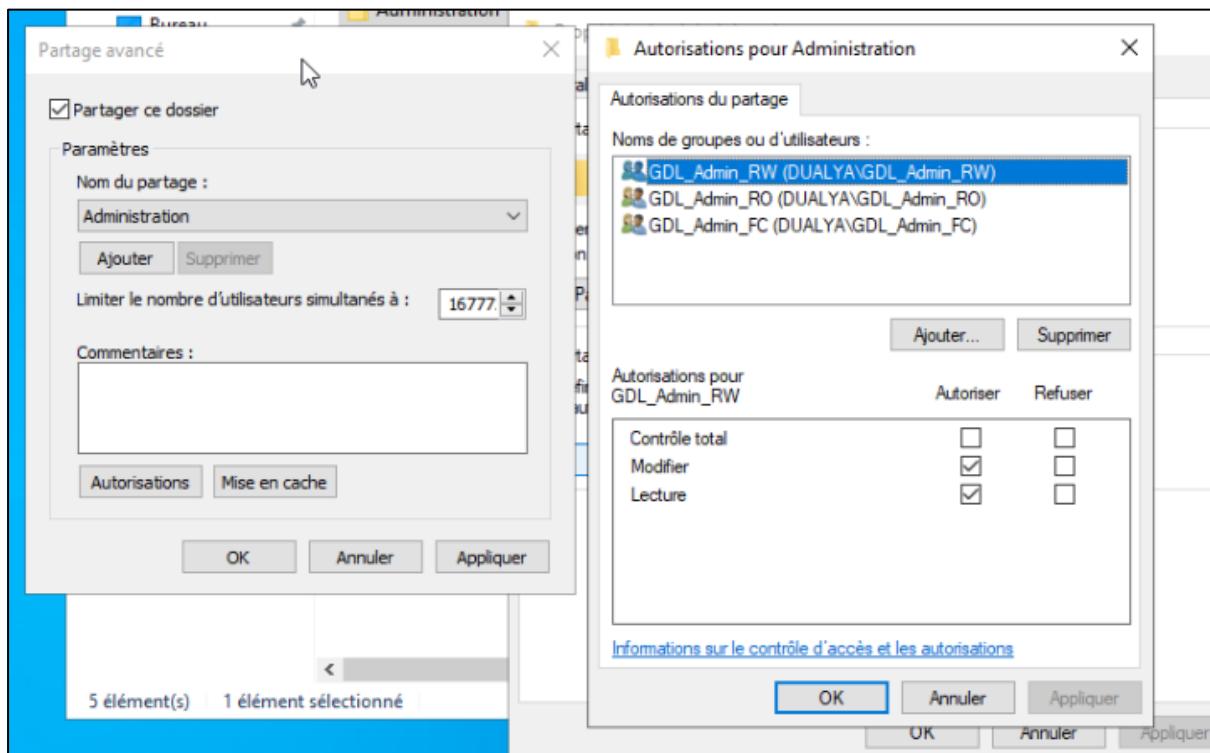


Répéter ces étapes pour chaque services, respectivement.

## C. Partage des dossiers via SMB

### 1. Partage de chaque dossier :

- o Clic droit → Propriétés → Partage avancé → Partager ce dossier.
- o Suppression de "Tout le monde", puis ajout des groupes GDL\_ correspondants avec les bons droits.



Répéter cette étape pour chaque partage, respectivement, selon le service concerné.

## Amélioration continue possible (Revue régulière du projet, axes d'amélioration)

- Mise en place de scripts PowerShell pour automatiser l'ajout de nouveaux utilisateurs et la gestion des permissions.
- Surveillance des accès aux fichiers via les journaux d'événements Windows.
- Intégration d'une solution de sauvegarde et de restauration rapide des fichiers.

## Sensibilisation des collaborateurs

- Explication de la politique de sécurité mise en place.
- Formation des utilisateurs à la bonne gestion des fichiers.
- Sensibilisation aux risques liés aux droits d'accès non maîtrisés.

## Conclusion

Cette activité m'a permis d'approfondir mes connaissances en gestion des droits d'accès et en administration Windows Server. L'application de la méthode AGDLP assure une gestion évolutive et sécurisée. La gestion des accès spécifiques (comme la lecture seule pour la Direction sur RH) permet une administration flexible et rapide. Cette approche me sera utile pour administrer des infrastructures IT de manière professionnelle. Par la suite, j'ai pu utiliser la méthode AGDLP dans le monde professionnel dans une mission de mise en place d'un SHAREPOINT pour l'entreprise.