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

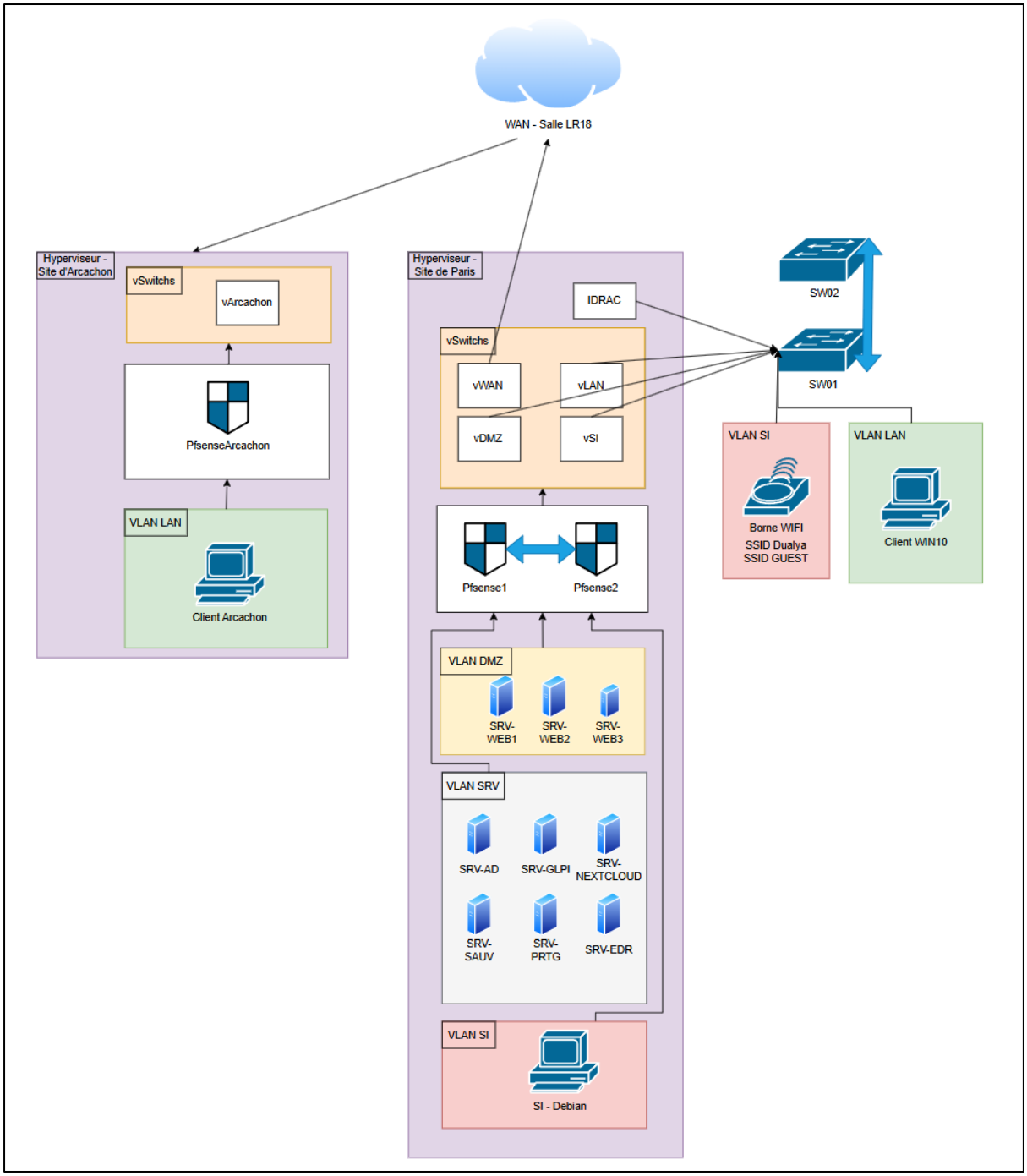
Contexte de la mission

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

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.

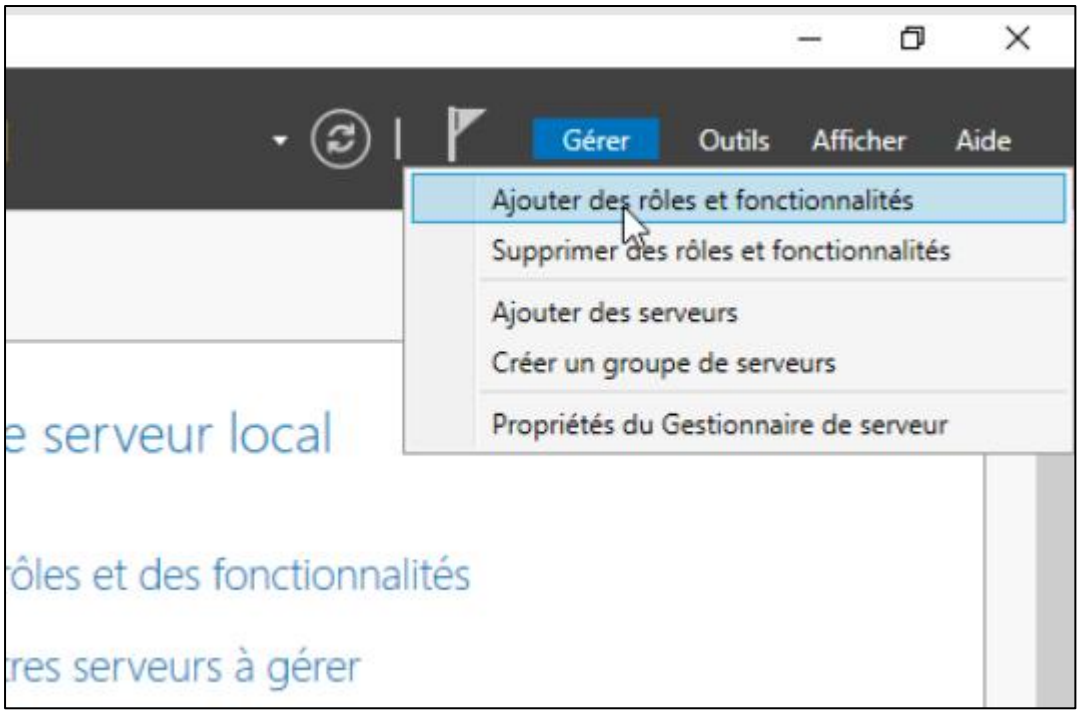
Après analyse, la méthode AGDLP (Account → Groupe Global → Groupe Domaine Local → Permission) a été retenue pour une gestion optimale et évolutive des droits d'accès. En effet, elle permet une **gestion claire, centralisée et évolutive des autorisations** : les utilisateurs sont ajoutés à des groupes 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.

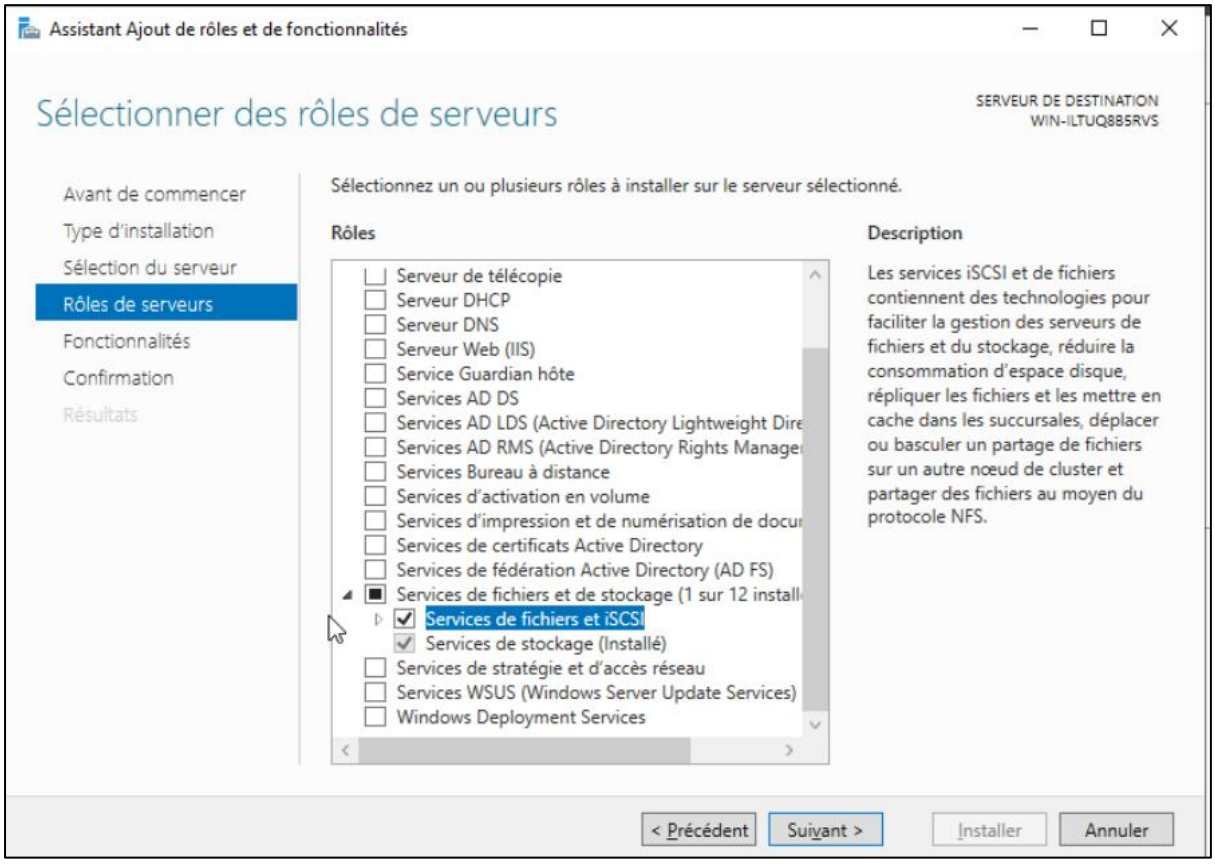
Cela **facilite l'audit**, **limite les erreurs humaines**, et **réduit les interventions manuelles** en cas de changement d'équipe ou de personnel. En séparant la logique métier (groupes globaux) de la logique technique (groupes locaux), AGDLP garantit une **meilleure sécurité**, un **meilleur cloisonnement**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





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.

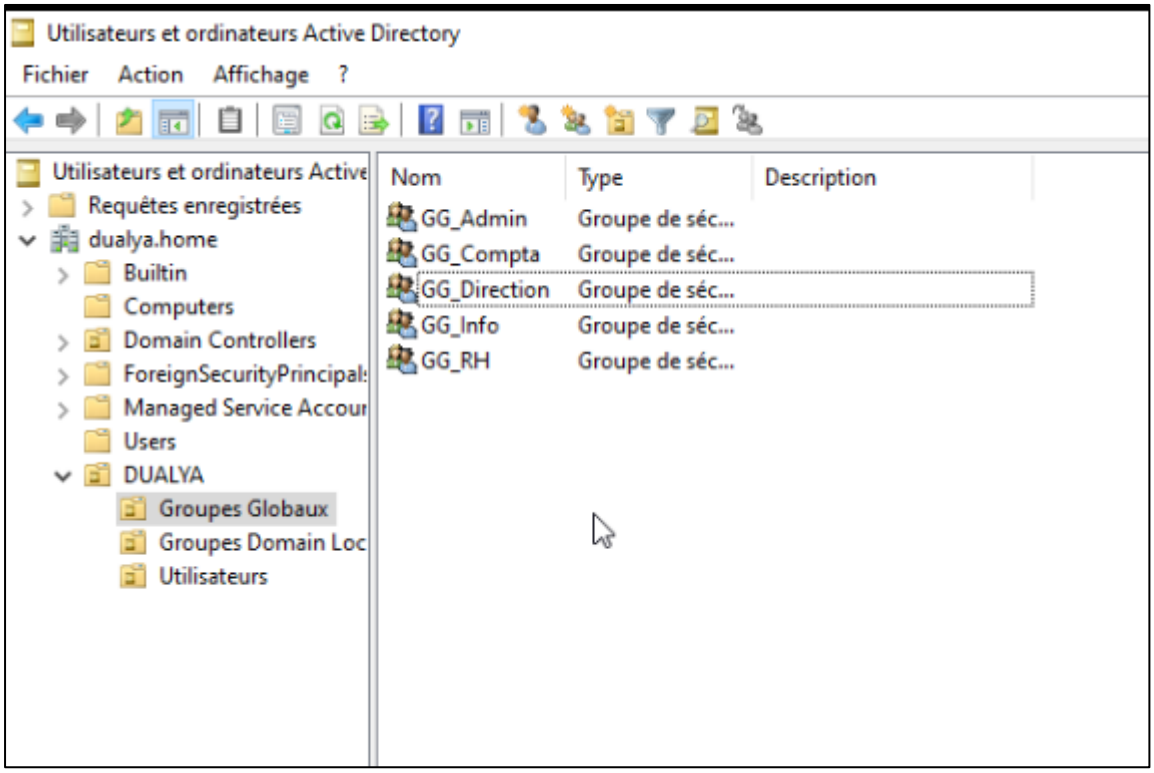
Déroulement de la mission en lien avec les compétences

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.



2. Création des groupes locaux de domaine (GDL_) en fonction des permissions

Pour chaque service, trois groupes ont été créés :

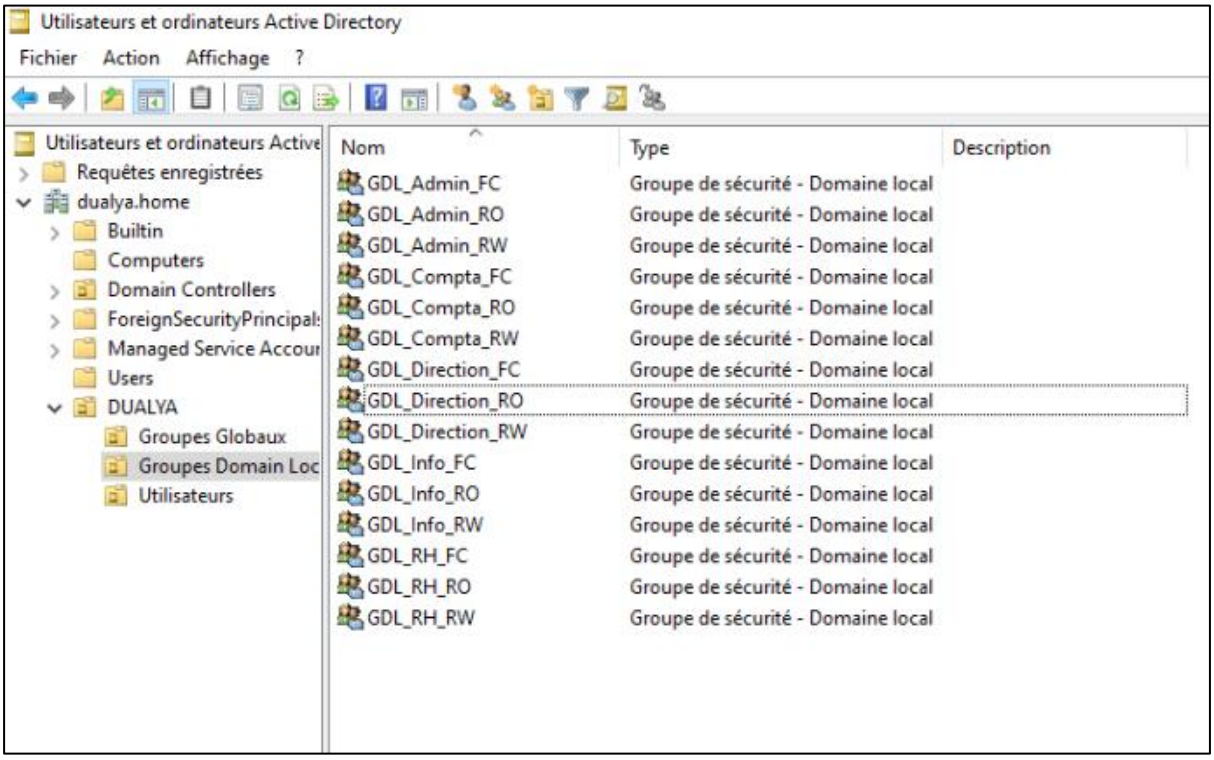
- **CO (Contrôle Total)** : Gestion complète des fichiers et dossiers.
- **RW (Lecture-Écriture)** : Modification des fichiers sans suppression des permissions.
- **RO (Lecture Seule)** : Consultation des fichiers uniquement.

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

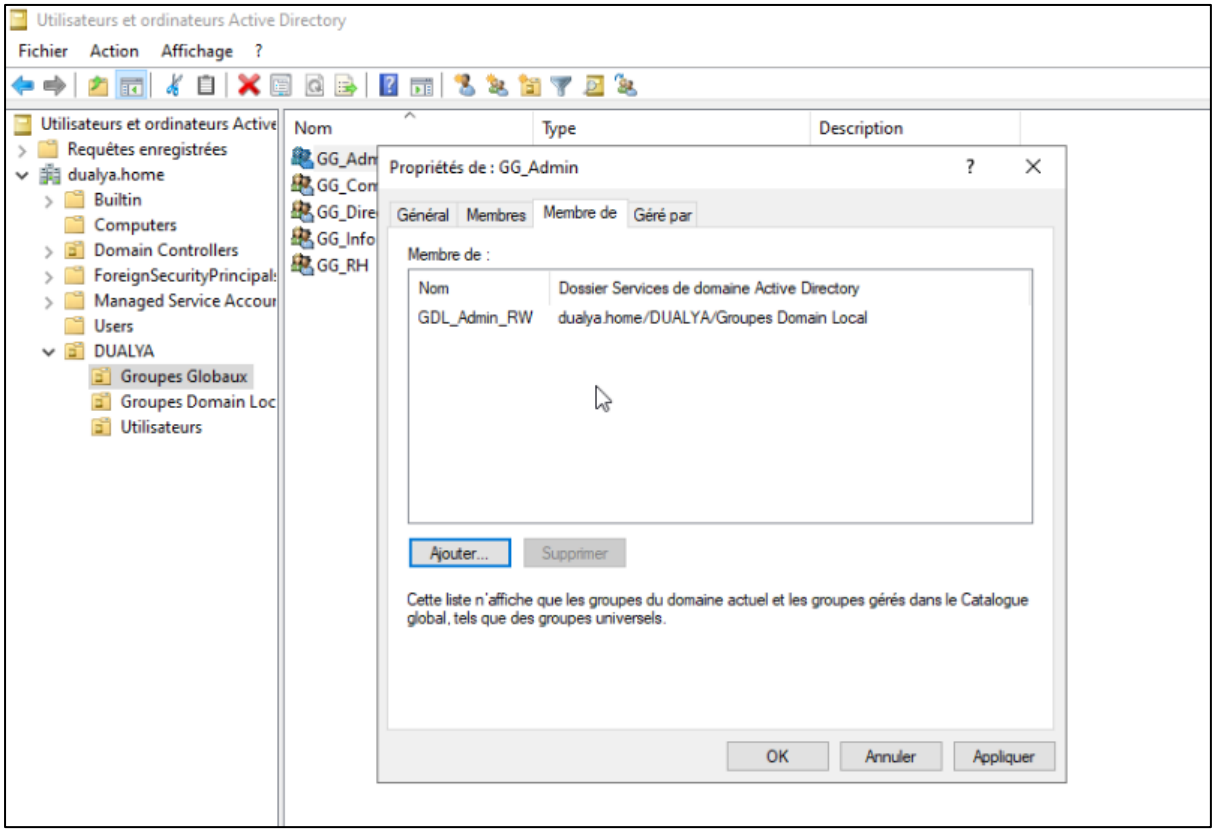
Même logique appliquée aux autres services :

- 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



3. Ajout des groupes globaux dans les groupes locaux correspondants

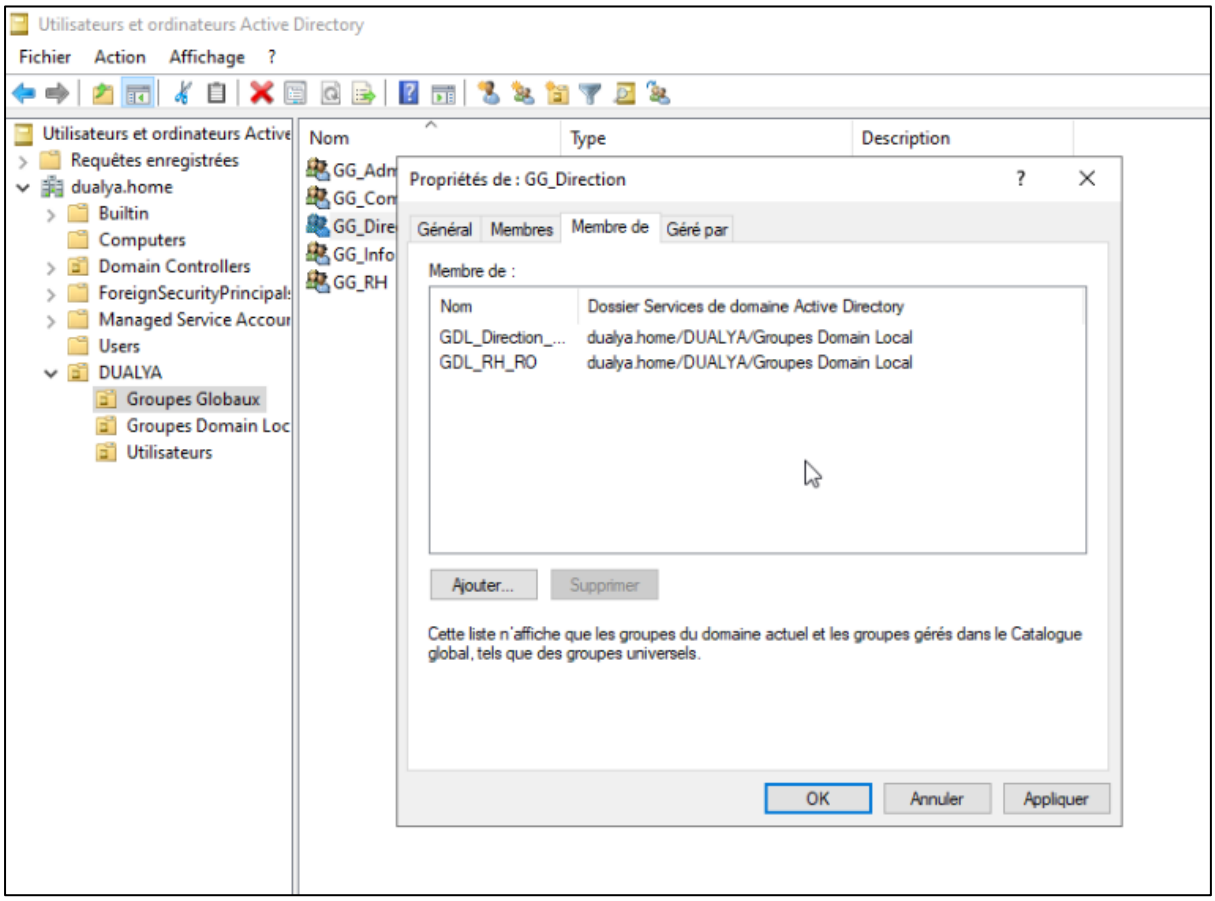
- GG_Admin → GDL_Admin_RW
- GG_Info → GDL_Info_RW
- GG_RH → GDL_RH_RW
- GG_Compta → GDL_Compta_RW
- GG_Direction → GDL_Direction_RW



Répéter cette étape pour tous les groupes respectivement.

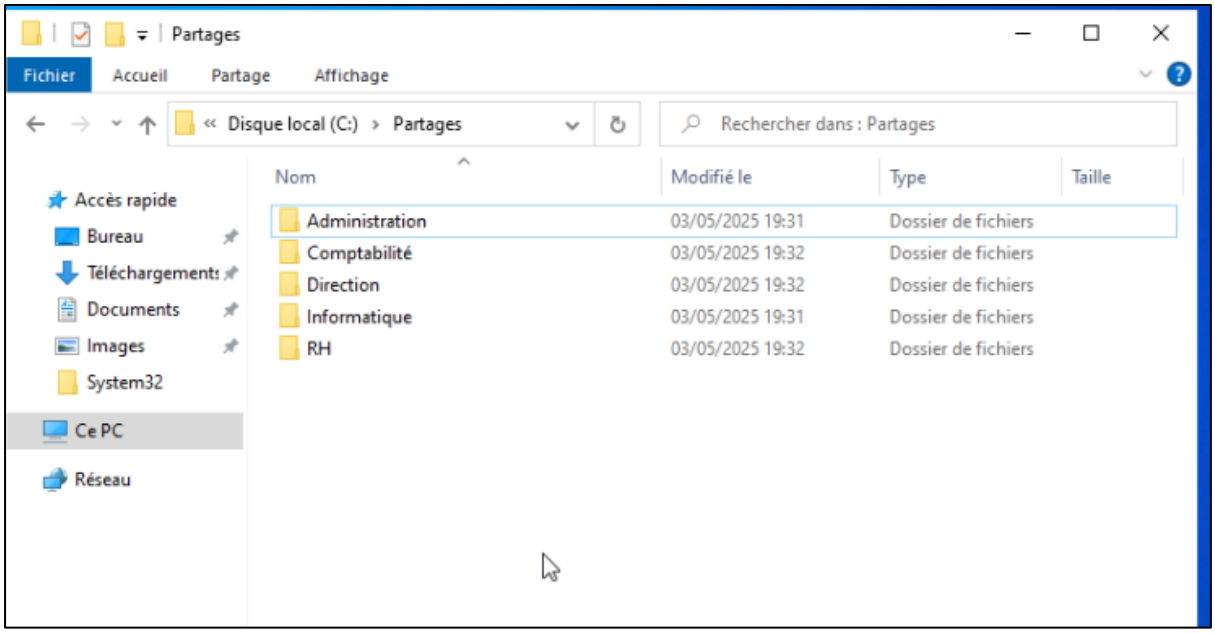
4. Gestion des permissions spécifiques (exemple de la Direction et du dossier RH)

- 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.

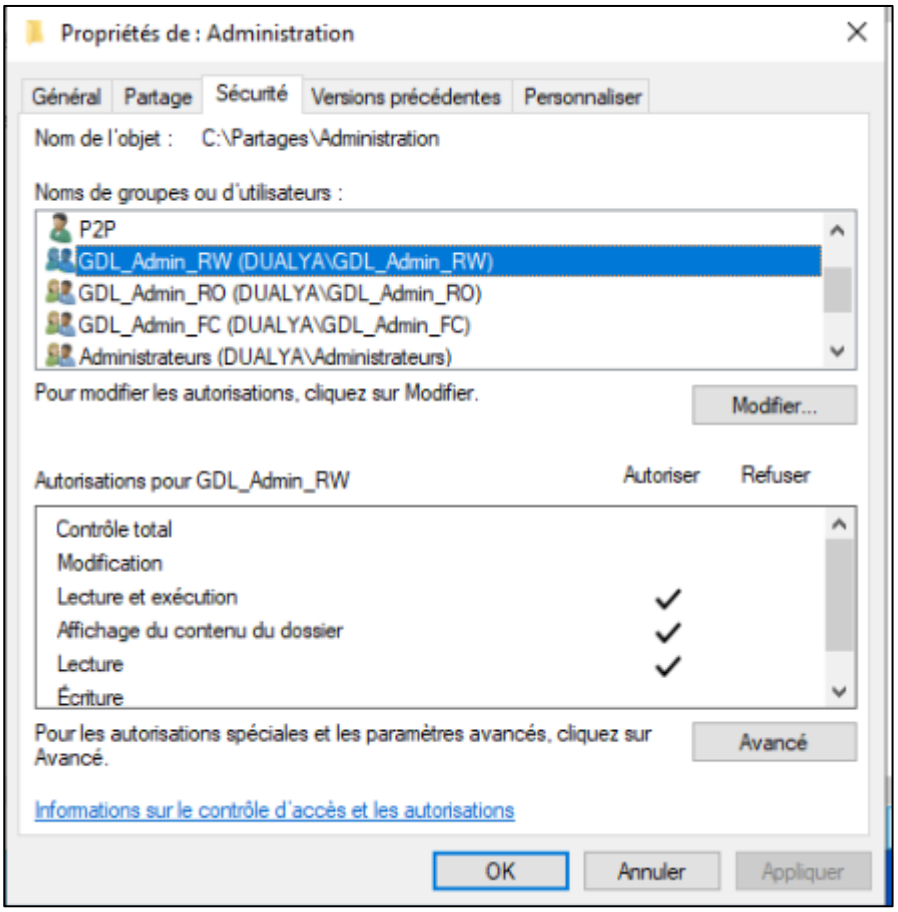


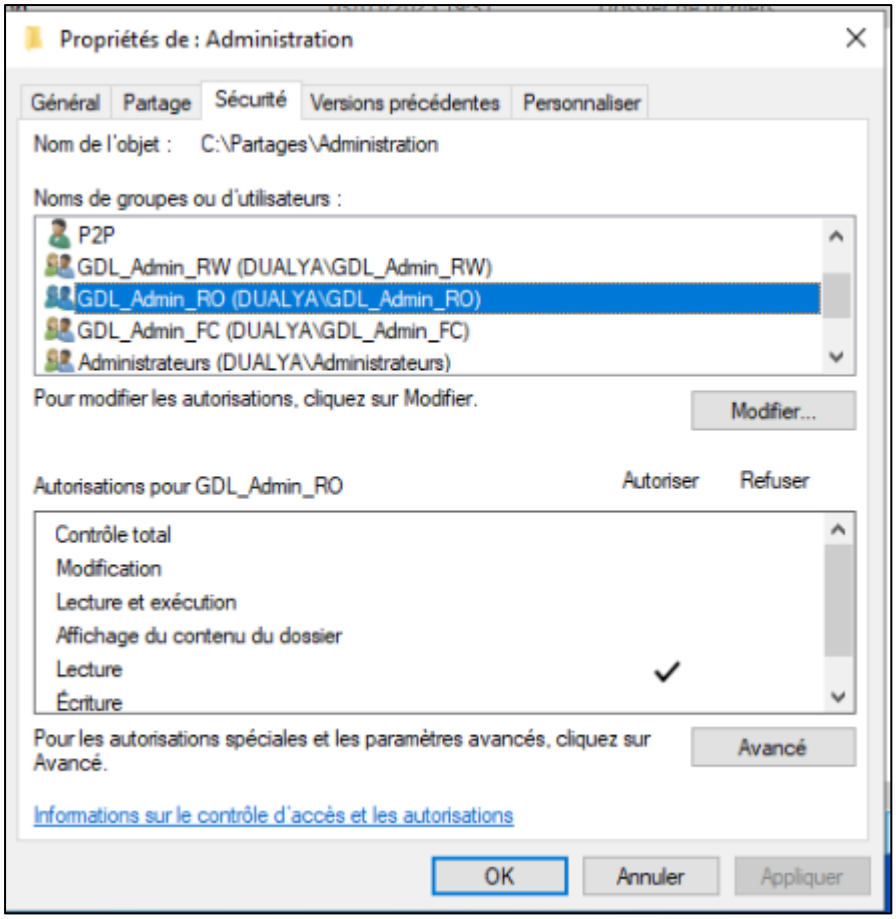
B. Création des dossiers et permissions NTFS

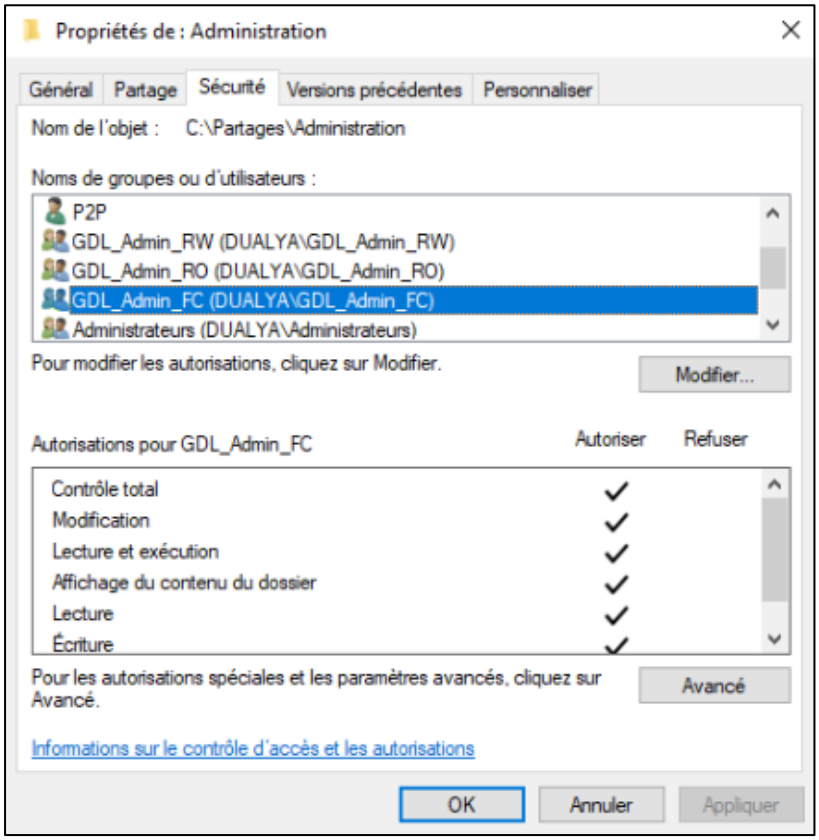
1. Création de la structure des dossiers :
    - C:\Partages\Administration
    - C:\Partages\Informatique
    - C:\Partages\RH
    - C:\Partages\Comptabilité
    - C:\Partages\Direction



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.



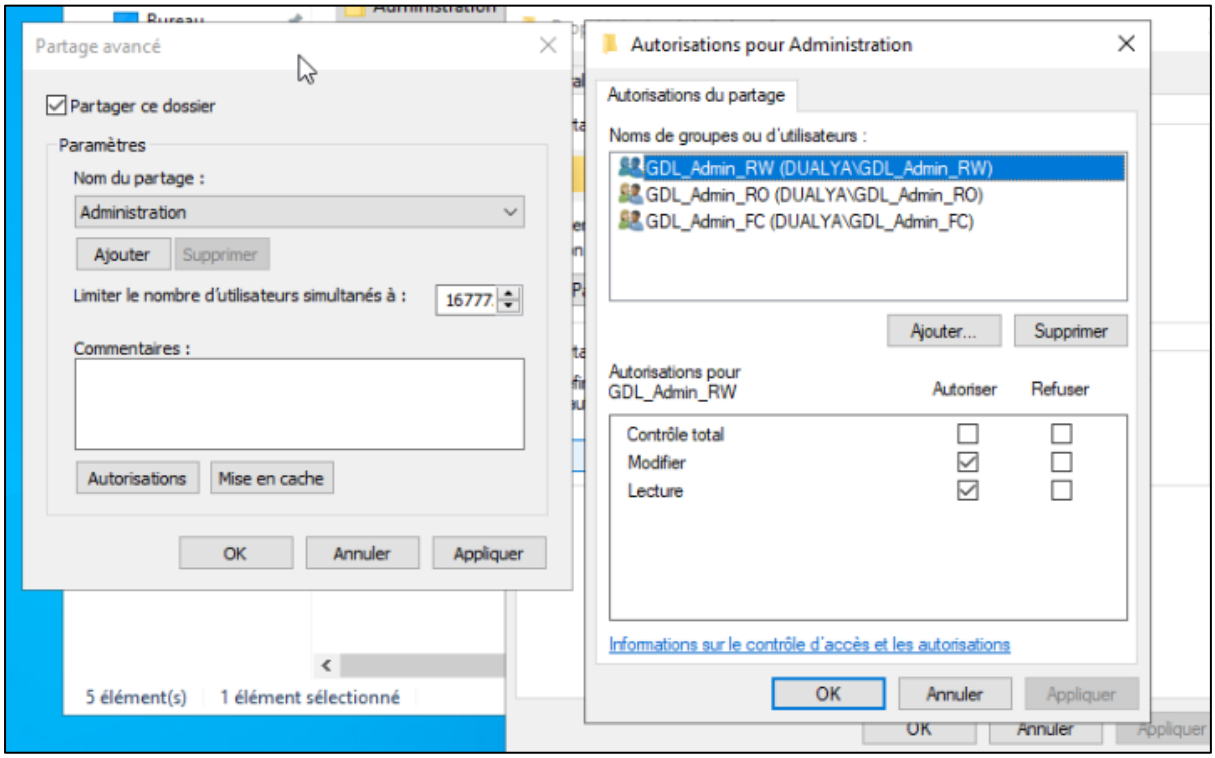




Répéter ces étapes pour chaque services, respectivement.

C. Partage des dossiers via SMB

1. Partage de chaque dossier :
    - Clic droit → Propriétés → Partage avancé → Partager ce dossier.
    - 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.