

Dans le cadre de mon projet E5, j'ai mis en place un **partage réseau centralisé** permettant aux utilisateurs d'accéder aux **fichiers et ressources** de l'entreprise tout en respectant des **règles strictes de permissions et de sécurité**. L'objectif était d'assurer une **gestion efficace et sécurisée des données**, en fonction des services et des utilisateurs

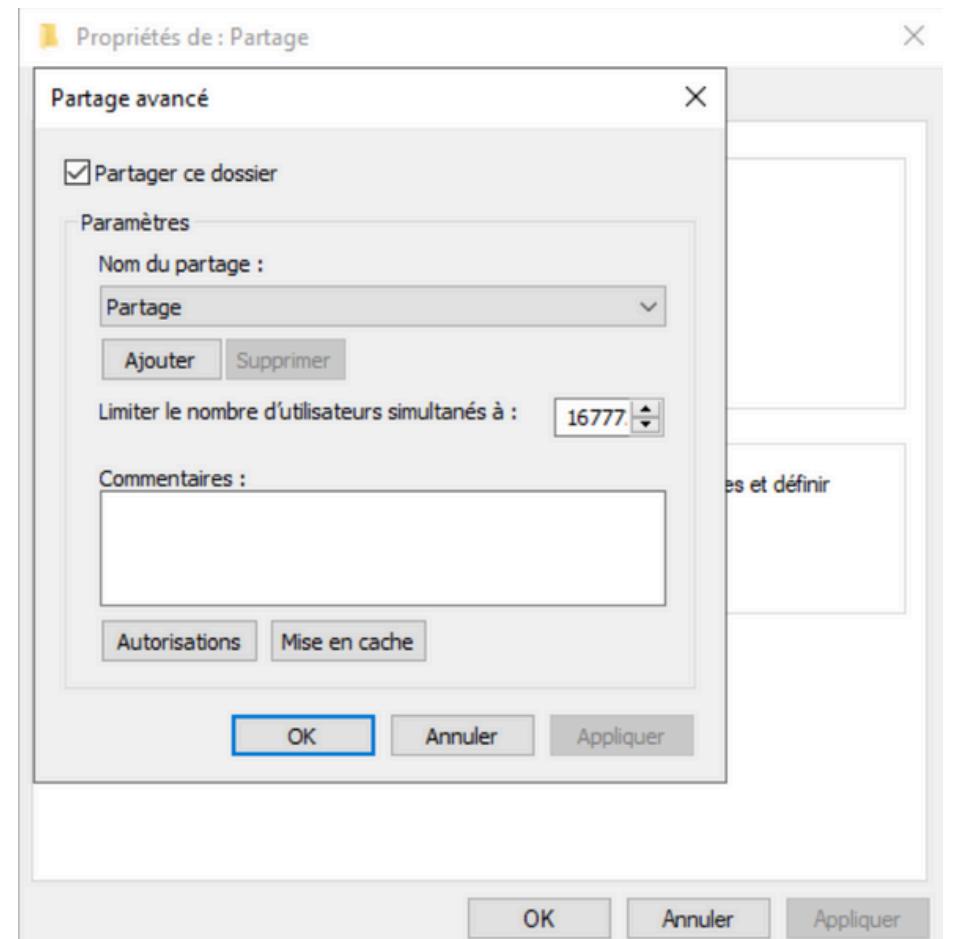
Contexte :

L'enjeu principal était de mettre en place un **serveur de partage de fichiers**, avec une structure clair et des **permissions adaptées** selon les besoins des utilisateurs et des groupes Active Directory. J'ai donc effectué les étapes suivantes pour tout mettre en place :

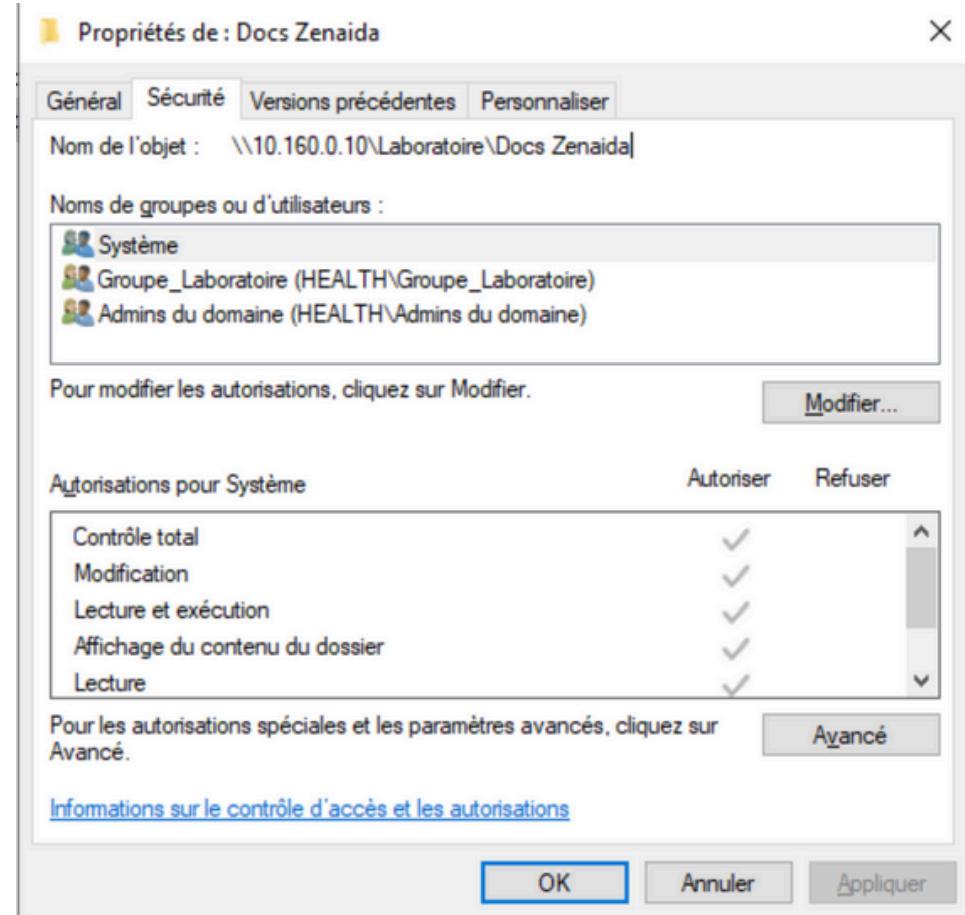
- **Création d'un partage réseau** sur le serveur dédié
- **Définition des permissions NTFS** pour garantir un accès restreint aux dossiers sensibles
- **Applications des droits d'accès** en fonction des groupes AD (lecture, écriture, modification)
- **Vérification et validation** des accès avec tout les utilisateurs

L'implémentation de ce partage réseau permet aux utilisateurs d'accéder aux fichiers nécessaires tout en respectant les restrictions de sécurité définies.

Accès au **partage réseau**  
depuis un compte utilisateur  
du domaine.

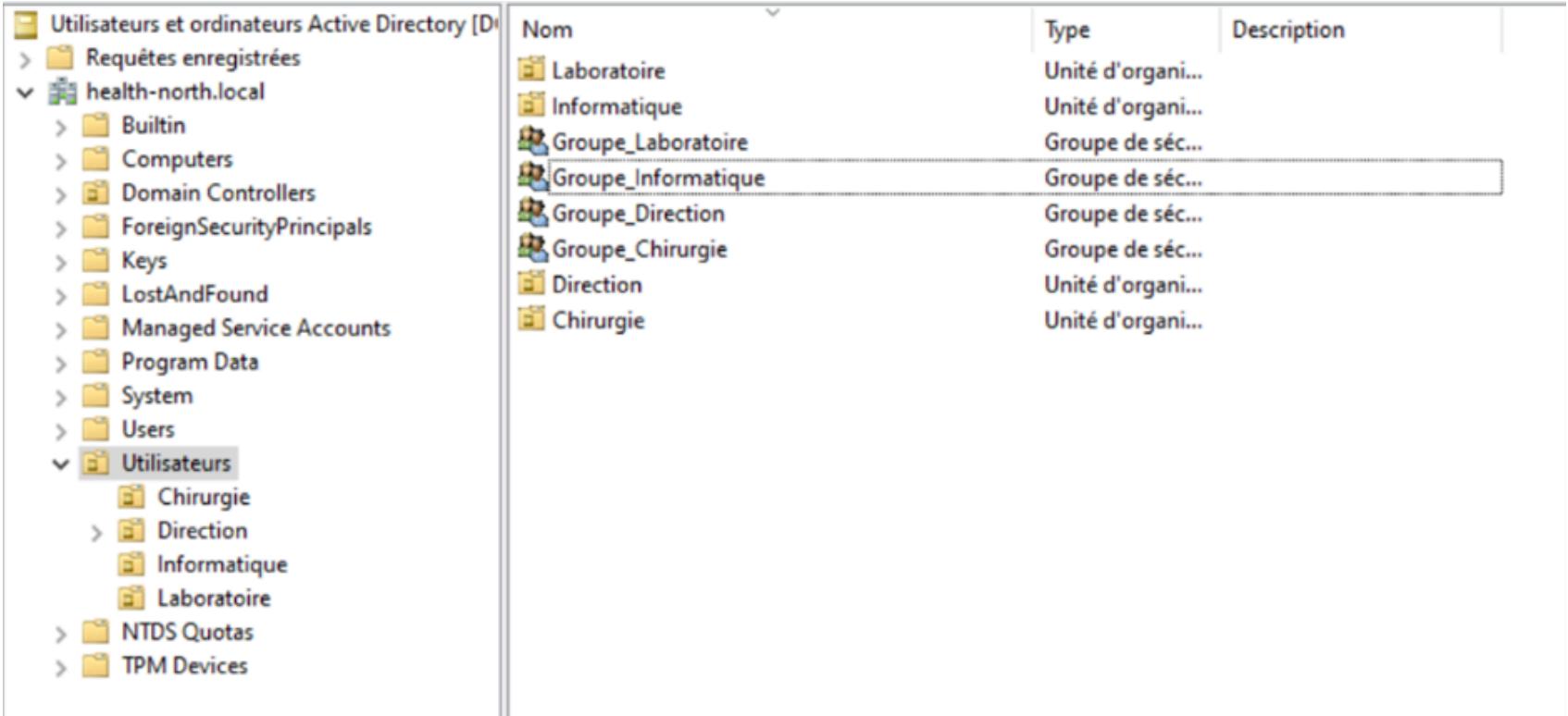


Paramètres de **partage avancés du dossier** "Partage" accessible à tout les utilisateurs. Ce dossier constitue le point de départ pour le partage réseau de l'entreprise dans le cadre du projet.



Aperçu des **permissions NTFS** appliqués au dossier “Docs Zenida”.  
L'accès est restreint au groupe “Groupe\_Laboatoire”, garantissant une séparation des accès entre les services.

Les administrateurs du domaine conservent un contrôle total pour la gestion et la maintenance.



The screenshot shows the Windows Active Directory Users and Computers snap-in. On the left, a navigation pane lists various Active Directory containers and objects. Under 'Utilisateurs et ordinateurs Active Directory [D]', 'health-north.local' is expanded, showing 'Utilisateurs' (selected), 'Requêtes enregistrées', and several system and service accounts. Under 'Utilisateurs', there are three OUs: 'Chirurgie', 'Direction', and 'Informatique'. A context menu is open over the 'Utilisateurs' container, with 'Ajouter un groupe' highlighted.

**Vue de l'Active Directory avec l'organisation des OU et des groupes.** Cette structure permet d'attribuer des permissions spécifiques aux partages réseau, comme illustré précédemment avec le "Groupe\_Laboratoire".

Nom	Type	Description
Laboratoire	Unité d'organis...	
Informatique	Unité d'organis...	
Groupe_Laboratoire	Groupe de séc...	
<b>Groupe_Informatique</b>	<b>Groupe de séc...</b>	
Groupe_Direction	Groupe de séc...	
Groupe_Chirurgie	Groupe de séc...	
Direction	Unité d'organis...	
Chirurgie	Unité d'organis...	

**Vue de l'Active Directory avec l'organisation des OU et des groupes.** Cette structure permet d'attribuer des permissions spécifiques aux partages réseau, comme illustré précédemment avec le "Groupe\_Laboratoire".

Erreur réseau

Windows ne peut pas accéder à \\10.160.0.10\Chirurgie

Vous n'avez pas l'autorisation d'accéder à \\10.160.0.10\Chirurgie. Contactez l'administrateur réseau pour demander l'accès.

[Pour plus d'informations sur les autorisations, voir le Centre d'aide et de support Windows](#)

Fermer

Test d'accès depuis un poste client :  
Un poste **sans les permissions requises** qui essaye d'accéder au dossier “Chirurgie” mais l'accès lui est refusé. Cela démontre l'application de la **bonne gestion des droits et des permissions**.