



 **Student name:** Théophile Dutrey - Arthur Berret

 **Student class:** Cyber Groupe 1

 **Date:** 26/09/25

Exercise 2: Implement file access control

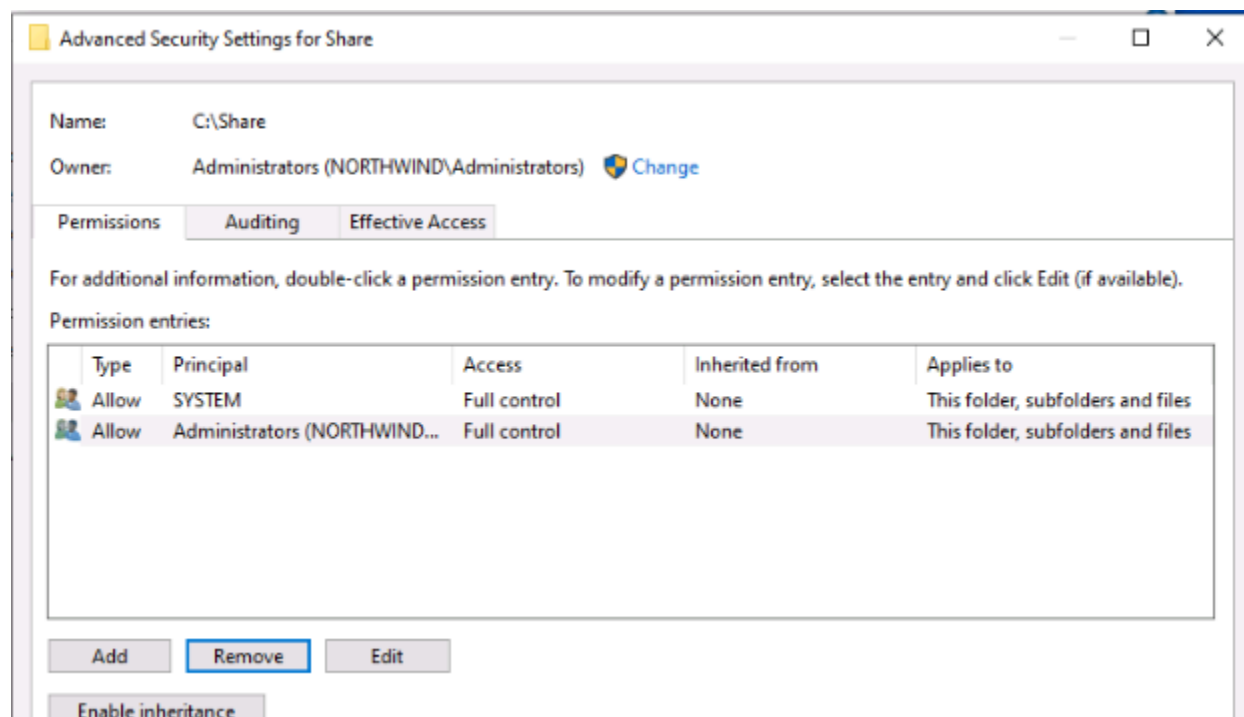
Task 2: Implement file permissions

Questions

1. Describe precisely how you implemented each rule. Make clear what change did you perform, especially regarding which user account your ACLs apply to, and which permissions did you grant.

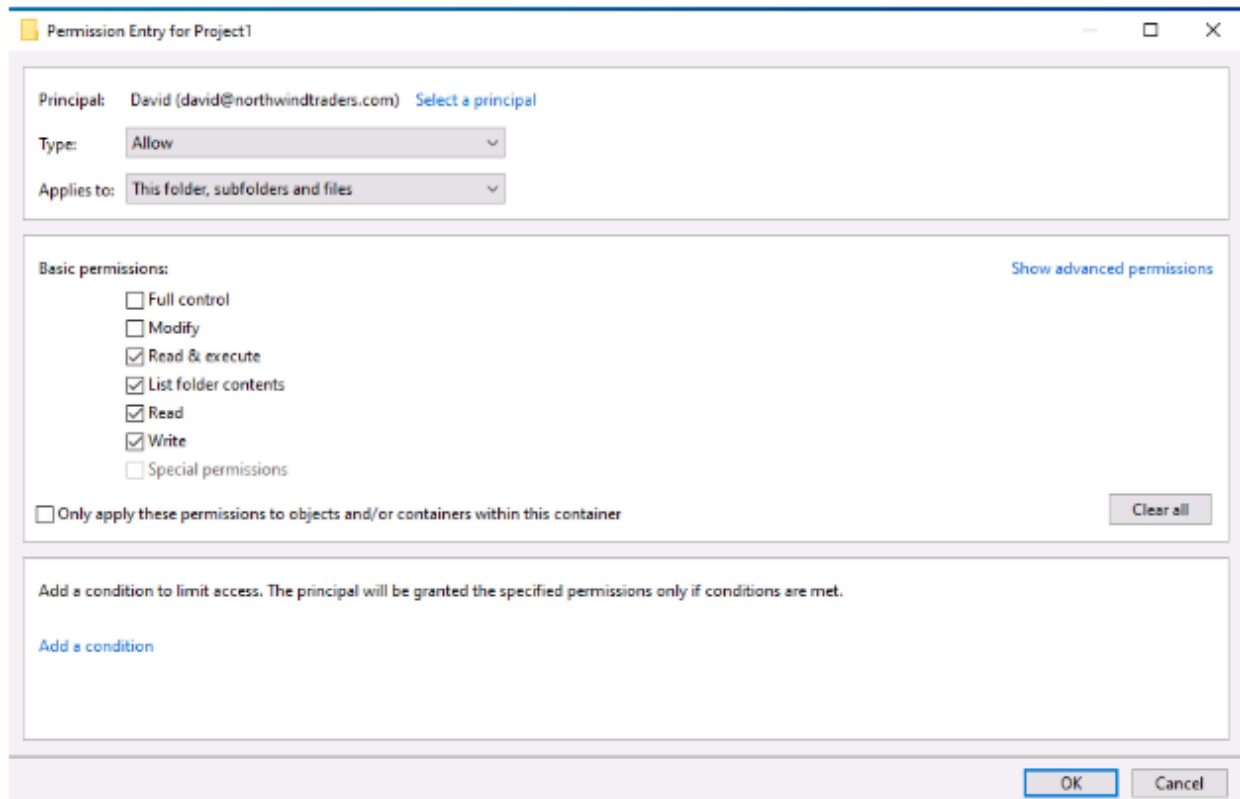
ID0:

Pour le dossier C:\Share, j'ai désactivé l'héritage des permissions afin d'obtenir une configuration indépendante. J'ai ensuite supprimé les entrées inutiles et conservé uniquement deux principaux : SYSTEM et Administrators (NORTHWIND\Administrators). Ces deux entités disposent du contrôle total sur le dossier ainsi que sur tous les sous-dossiers et fichiers. J'ai également activé l'option permettant de remplacer toutes les entrées de permissions des objets enfants afin que cette configuration s'applique uniformément à toute l'arborescence. Cette étape garantit que seuls les administrateurs et le système ont des droits complets sur le dossier racine et tout ce qu'il contient.

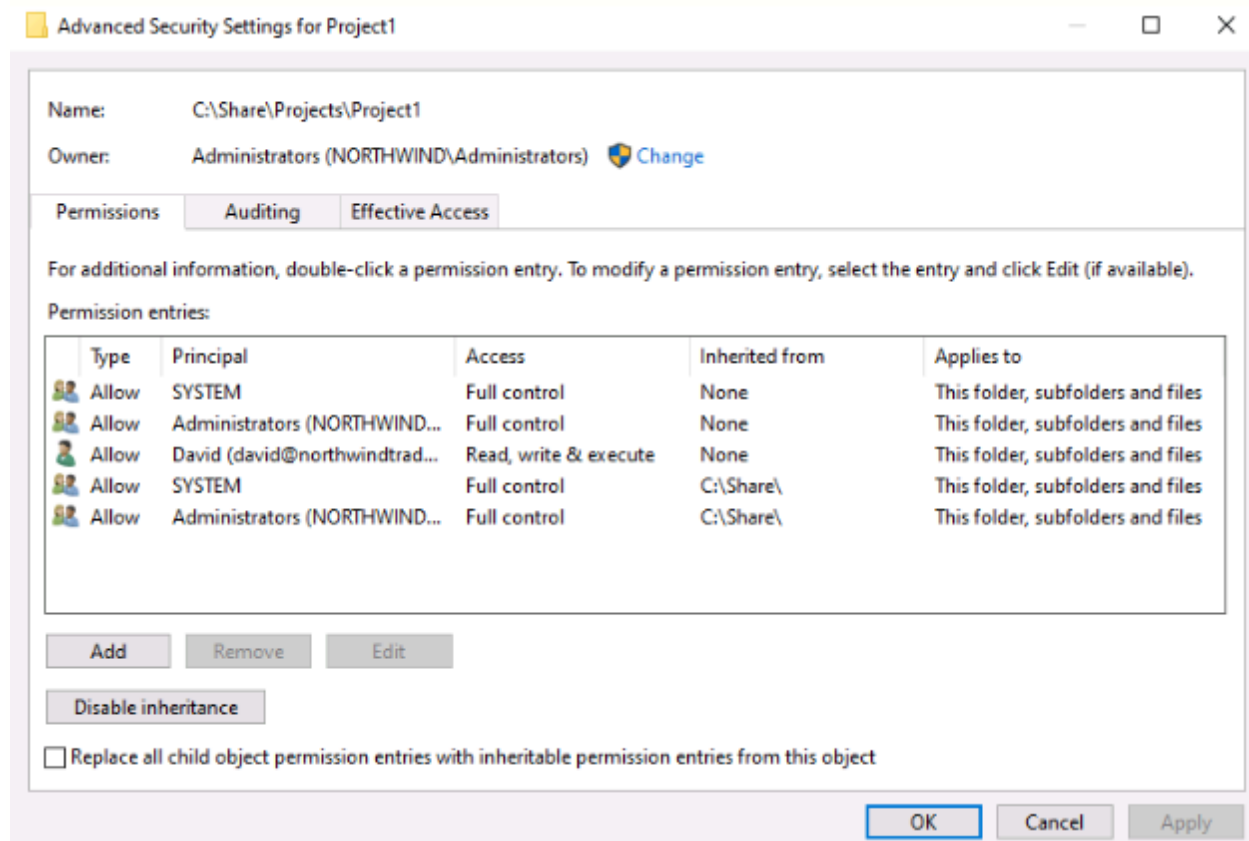


ID1:

Pour le dossier C:\Share\Projects\Project1, j'ai désactivé l'héritage des permissions puis supprimé les entrées inutiles afin de garder un contrôle précis. J'ai ensuite ajouté l'utilisateur NORTHWIND\david comme principal. J'ai configuré ses droits de manière à lui permettre de lire et exécuter, de lister le contenu, de lire, d'écrire, de créer des fichiers et des sous-dossiers. En revanche, j'ai explicitement veillé à ce qu'il ne puisse pas supprimer de fichiers ou de sous-dossiers. Ainsi, David dispose des permissions nécessaires pour travailler sur le projet, sans risque de suppression accidentelle ou volontaire de données.



Module 1 – Lab 2 – lab title



ID2:

Pour le dossier C:\Share\Users, j'ai supprimé l'héritage afin d'avoir une configuration indépendante des permissions parent. J'ai conservé uniquement SYSTEM et Administrators avec un contrôle total. J'ai ensuite ajouté le groupe Authenticated Users et configuré leurs droits de façon à ce qu'ils puissent uniquement lister le contenu du dossier, c'est-à-dire voir quels sous-dossiers existent, sans pouvoir y accéder directement. Pour ce faire, j'ai coché uniquement les autorisations de type lecture (list folder, read attributes, read extended attributes, read permissions), et j'ai restreint l'application à This folder only. De cette manière, les utilisateurs authentifiés peuvent voir la structure du dossier Users, mais ne peuvent pas entrer dans les sous-dossiers sans autorisations explicites.

Module 1 – Lab 2 – lab title

Permission Entry for Users

Principal: Authenticated Users [Select a principal](#)

Type: Allow

Applies to: This folder only

Advanced permissions: [Show basic permissions](#)

<input type="checkbox"/> Full control	<input type="checkbox"/> Write attributes
<input type="checkbox"/> Traverse folder / execute file	<input type="checkbox"/> Write extended attributes
<input checked="" type="checkbox"/> List folder / read data	<input type="checkbox"/> Delete subfolders and files
<input checked="" type="checkbox"/> Read attributes	<input type="checkbox"/> Delete
<input checked="" type="checkbox"/> Read extended attributes	<input checked="" type="checkbox"/> Read permissions
<input type="checkbox"/> Create files / write data	<input type="checkbox"/> Change permissions
<input type="checkbox"/> Create folders / append data	<input type="checkbox"/> Take ownership

☐ Only apply these permissions to objects and/or containers within this container

[Add a condition](#)

OK Cancel

Advanced Security Settings for Users

Name: C:\Share\Users

Owner: Administrators (NORTHWIND\Administrators) [Change](#)

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Administrators (NORTHWIND...	Full control	None	This folder, subfolders and files
Allow	Authenticated Users	Read	None	This folder only

Add Remove Edit

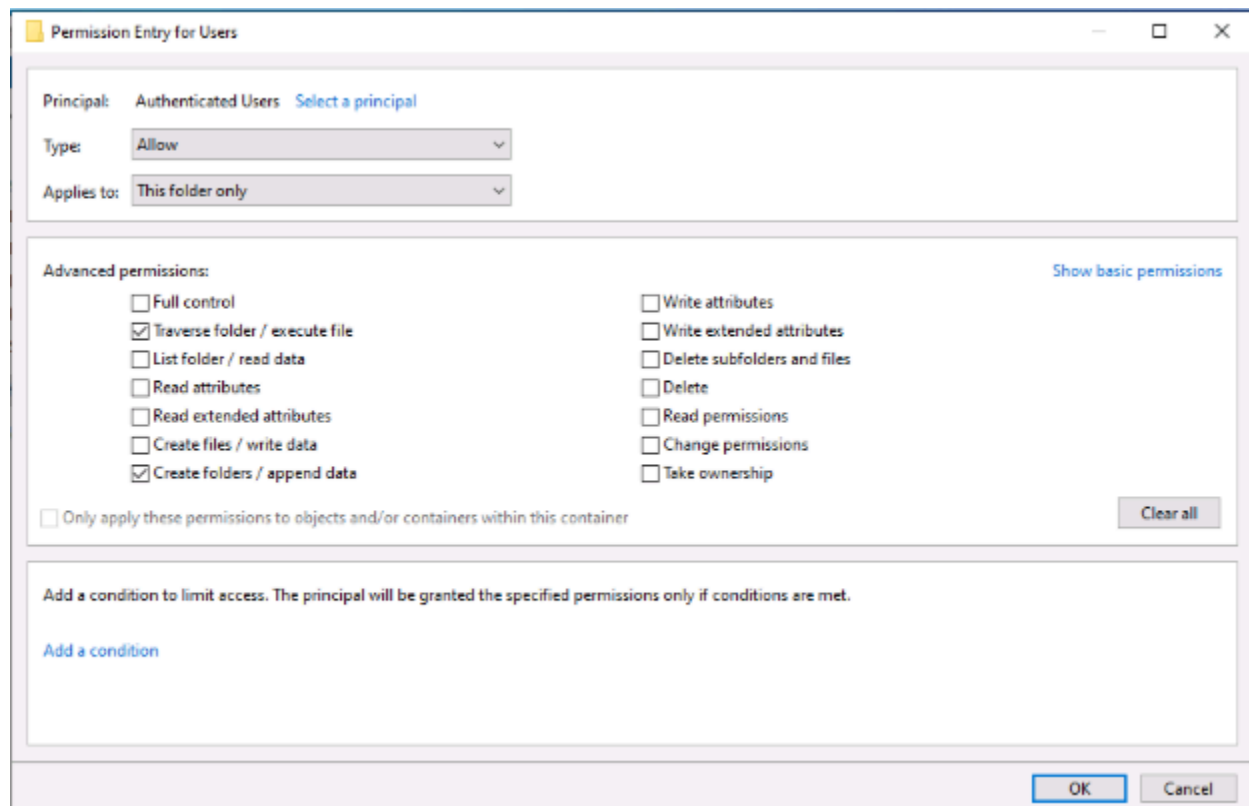
Enable inheritance

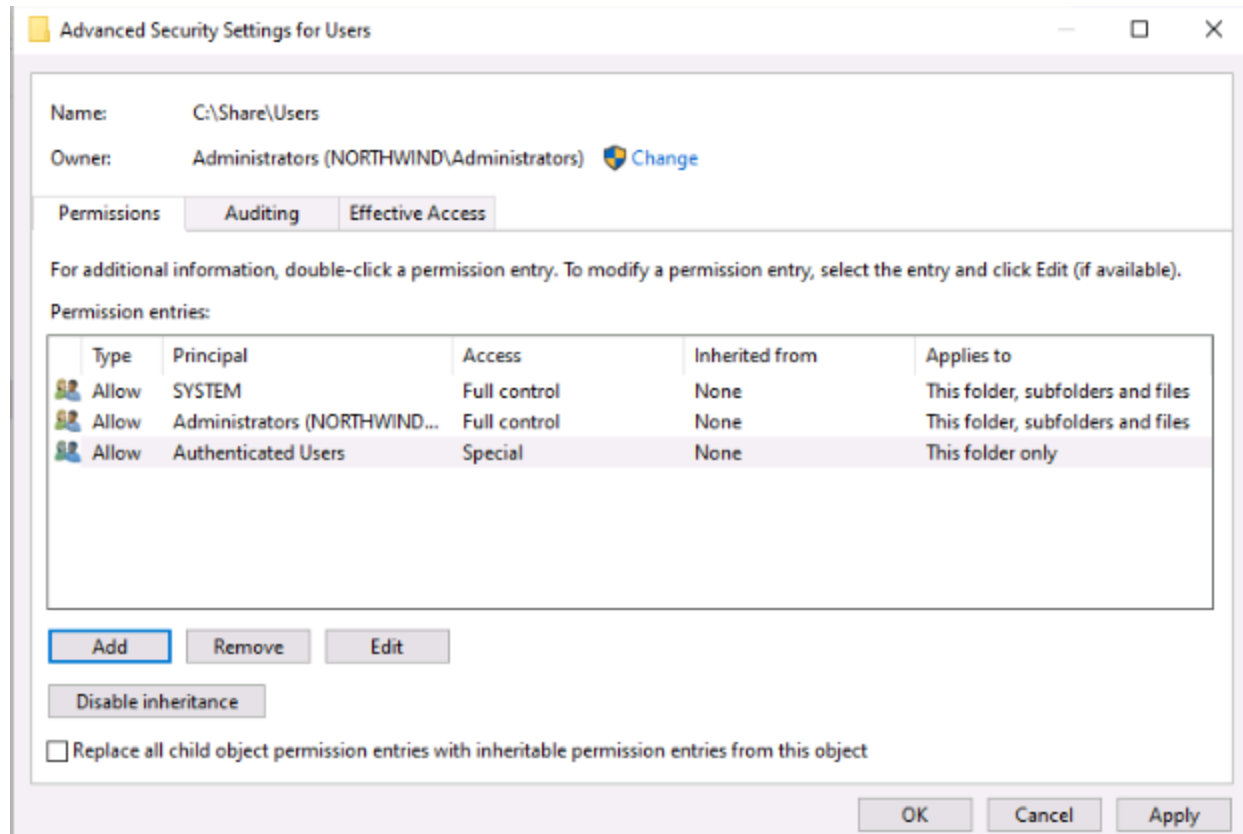
☐ Replace all child object permission entries with inheritable permission entries from this object

OK Cancel Apply

ID3:

Toujours sur le dossier C:\Share\Users, j'ai ajouté une règle supplémentaire pour le groupe Authenticated Users afin de leur donner le droit de créer de nouveaux dossiers enfants. Pour cela, j'ai attribué l'autorisation Create folders / append data, appliquée à This folder only. Cela permet à chaque utilisateur de créer son propre dossier personnel dans Users. Grâce au mécanisme de Windows, les nouveaux dossiers héritent automatiquement des permissions par défaut : SYSTEM et Administrators conservent le contrôle total, et le CREATOR OWNER (l'utilisateur qui a créé le dossier) reçoit également un contrôle total sur son propre dossier. Cela garantit que chaque utilisateur peut travailler dans son propre répertoire sans interférer avec ceux des autres.





Share SMB:

Afin que les permissions NTFS configurées sur le dossier C:\Share soient effectivement prises en compte par les autres machines du domaine, il est nécessaire de publier ce dossier comme partage réseau SMB. Sans cette étape, les clients (ex. WIN-CLI1 ou WIN-SRV1) n'accèdent pas au bon répertoire et ne peuvent donc pas appliquer les règles de sécurité définies. L'analyse du serveur via Server Manager → File and Storage Services → Shares a montré que seuls les partages système standards (NETLOGON et SYSVOL) existaient par défaut. Aucun partage Share n'était présent. Cela expliquait pourquoi les tests réalisés depuis les autres postes ne reflétaient pas les restrictions mises en place. Pour corriger cela, un nouveau partage SMB a été créé :

Lancement de l'assistant New Share Wizard dans le Server Manager.

Sélection du profil SMB - Quick.

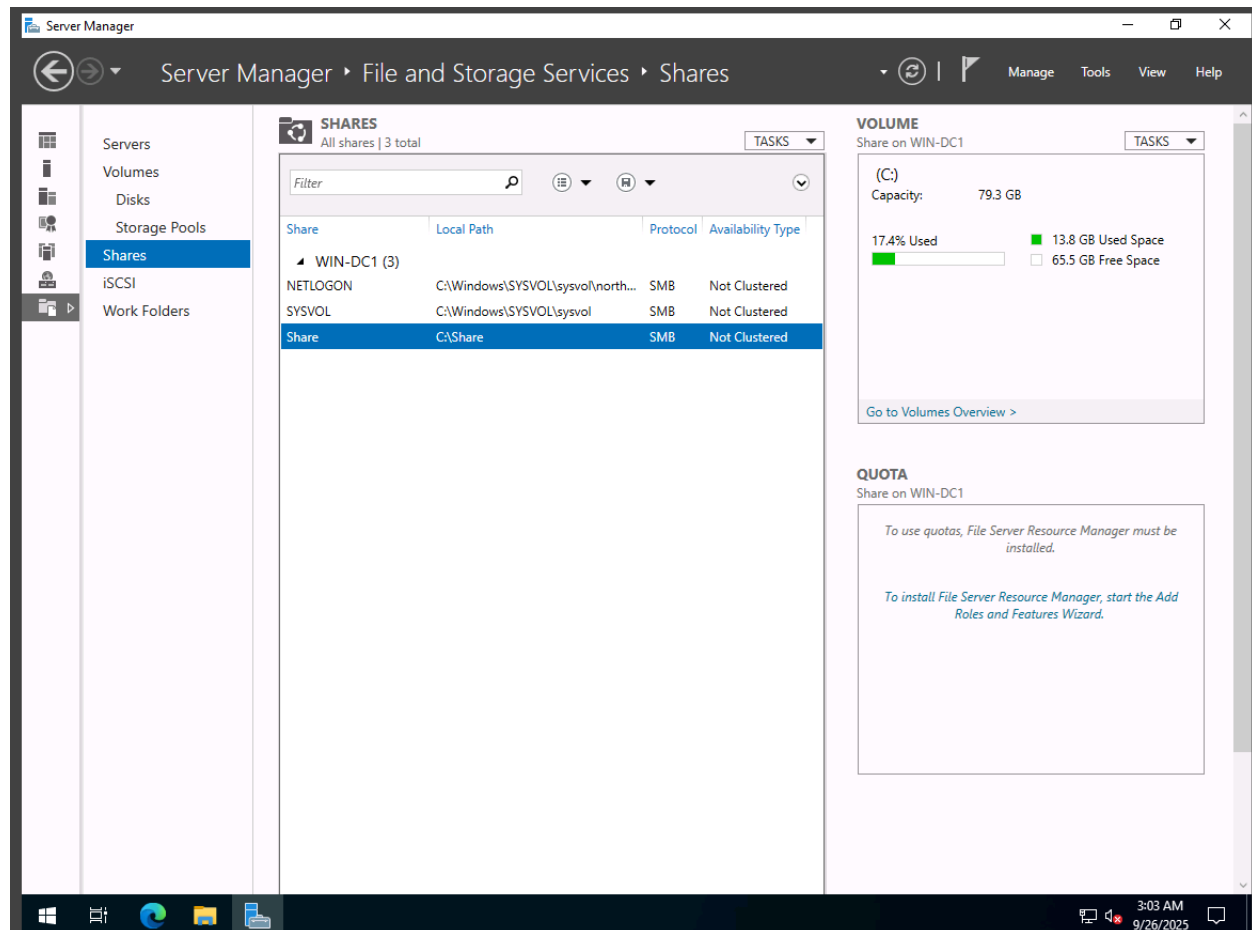
Définition du chemin personnalisé vers C:\Share

Attribution du nom de partage Share, ce qui permet d'y accéder en réseau via \WIN-DC1\Share.

Vérification des permissions du partage et suppression d'entrées génériques éventuelles (comme Everyone: Read) pour ne conserver que la cohérence avec les ACL NTFS définies (ID0 à ID3).

Dès lors, la structure C:\Share est disponible comme ressource partagée et les règles de sécurité configurées s'appliquent bien aux utilisateurs lorsqu'ils se connectent via le réseau. Les clients du domaine n'ont pas besoin de recréer un

dossier local C:\Share, ils utilisent uniquement le partage SMB publié depuis le contrôleur de domaine.



Task 3: Test permissions on the "Projects" folder

Questions

1. Explain the mechanism which allows to restrict permissions on files they own.

Dans le modèle de sécurité de Windows, basé sur le Discretionary Access Control (DAC), le créateur d'un fichier ou d'un dossier en devient automatiquement le propriétaire. Ce statut particulier confère un droit implicite : le propriétaire peut toujours modifier les autorisations (ACL) appliquées à son objet, même si celles-ci ne lui accordent pas le contrôle total. Autrement dit, un utilisateur reste en mesure de réattribuer des droits sur ses propres fichiers, ce qui limite l'efficacité des restrictions définies par un administrateur.

Pour contrer ce comportement et éviter qu'un utilisateur ne contourne les règles de sécurité, il est possible de modifier la gestion de la propriété par défaut. Une pratique courante consiste à attribuer la propriété non pas au créateur, mais à un compte ou un groupe administrateur (par exemple Administrators ou SYSTEM). Cette mesure peut être configurée au moyen des stratégies de sécurité locales ou, dans un environnement de domaine, via des stratégies de groupe (GPO). Ainsi, la

capacité d'un utilisateur à modifier les permissions de ses propres fichiers est neutralisée, garantissant un contrôle administratif strict des droits d'accès.

Task 4: Test permissions on the "Users" folder

Questions

1. Explain the mechanism which sets the permissions of the creator of a file or folder.

Lorsque qu'un utilisateur crée un fichier ou un dossier dans Windows, le système applique automatiquement les règles de contrôle d'accès définies sur le dossier parent. Ces règles incluent notamment une entrée spéciale appelée CREATOR OWNER. L'entrée CREATOR OWNER est un identificateur particulier dans les listes de contrôle d'accès (ACL). Elle ne correspond pas à un utilisateur précis, mais représente dynamiquement le compte qui crée l'objet. Ainsi :

- Lorsqu'un utilisateur crée un fichier ou un dossier, l'entrée CREATOR OWNER est remplacée par cet utilisateur dans les autorisations effectives.
- Par défaut, Windows attribue au propriétaire de l'objet un contrôle total sur celui-ci, ce qui lui permet de gérer son contenu et ses permissions.
- Les permissions appliquées au créateur dépendent donc de la présence et de la configuration de l'entrée CREATOR OWNER dans le dossier parent.

Ce mécanisme garantit que l'utilisateur qui crée un objet dispose des droits nécessaires pour l'utiliser immédiatement, tout en permettant aux administrateurs de définir à l'avance quel niveau d'accès sera attribué aux créateurs.

