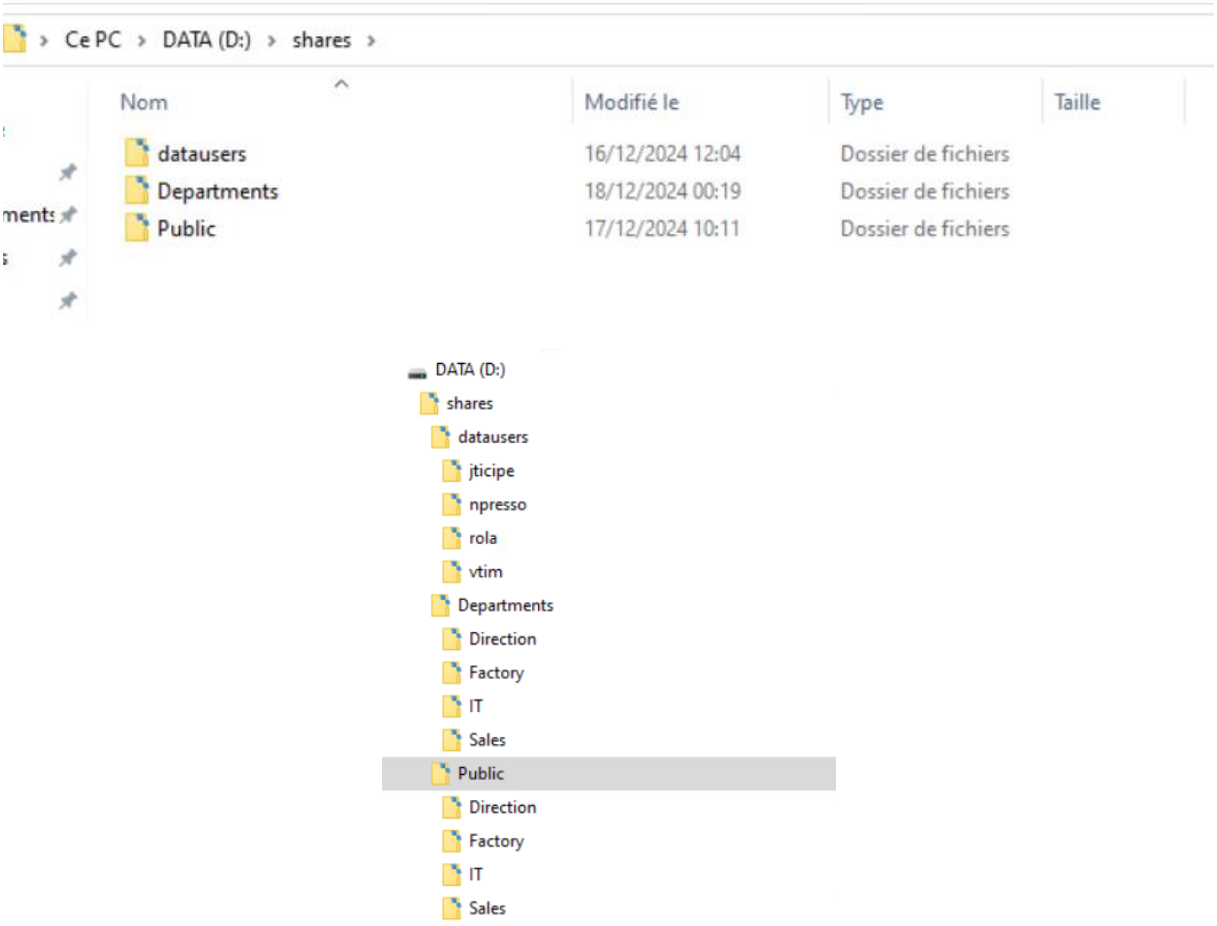
PAQUELET Etienne Groupe 11

KUT Suha

Jalon 23 : HQDCSRV File Server

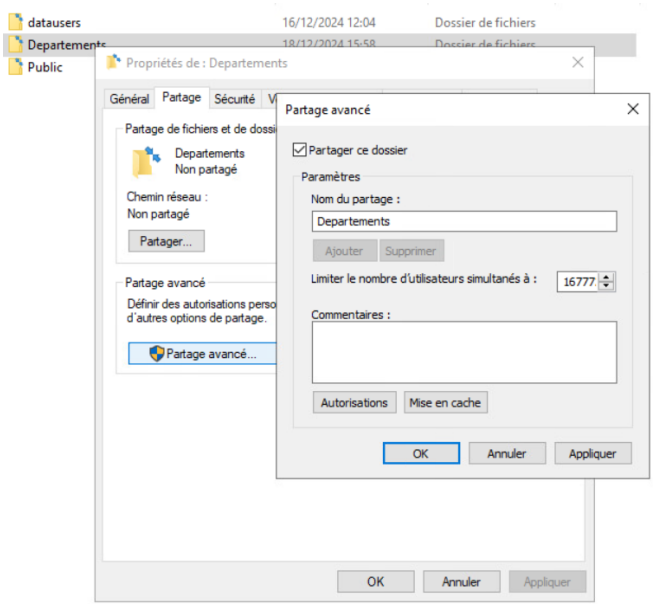
Dans ce jalon, nous allons vous présenter comment nous avons réalisé les partages de fichiers sur HQDCSRV.

Tout d'abord, nous avons créé l'arborescence des partages :



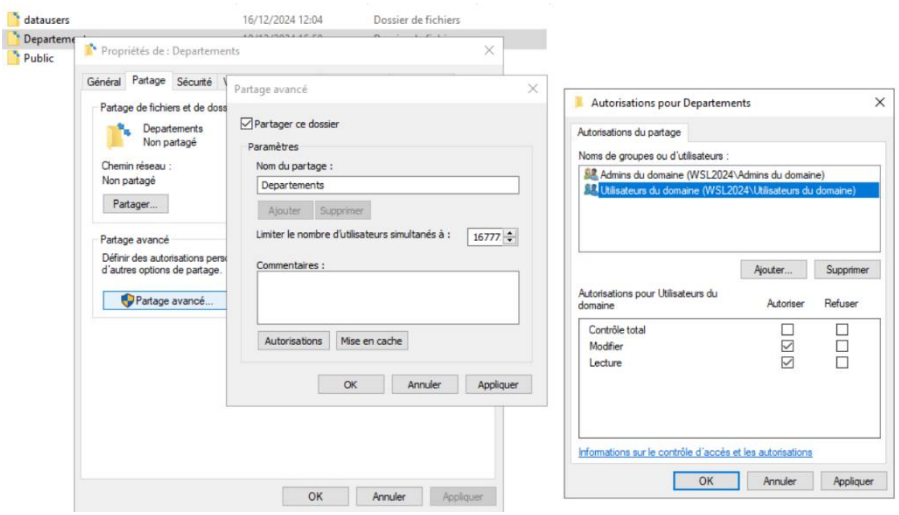
Une fois l'arborescence des dossiers créé, nous avons partagé les dossiers principaux :

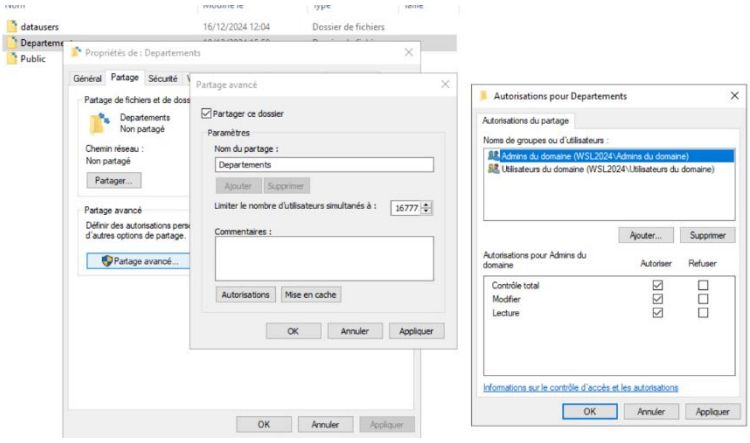
- Public
- Départements
- Datausers



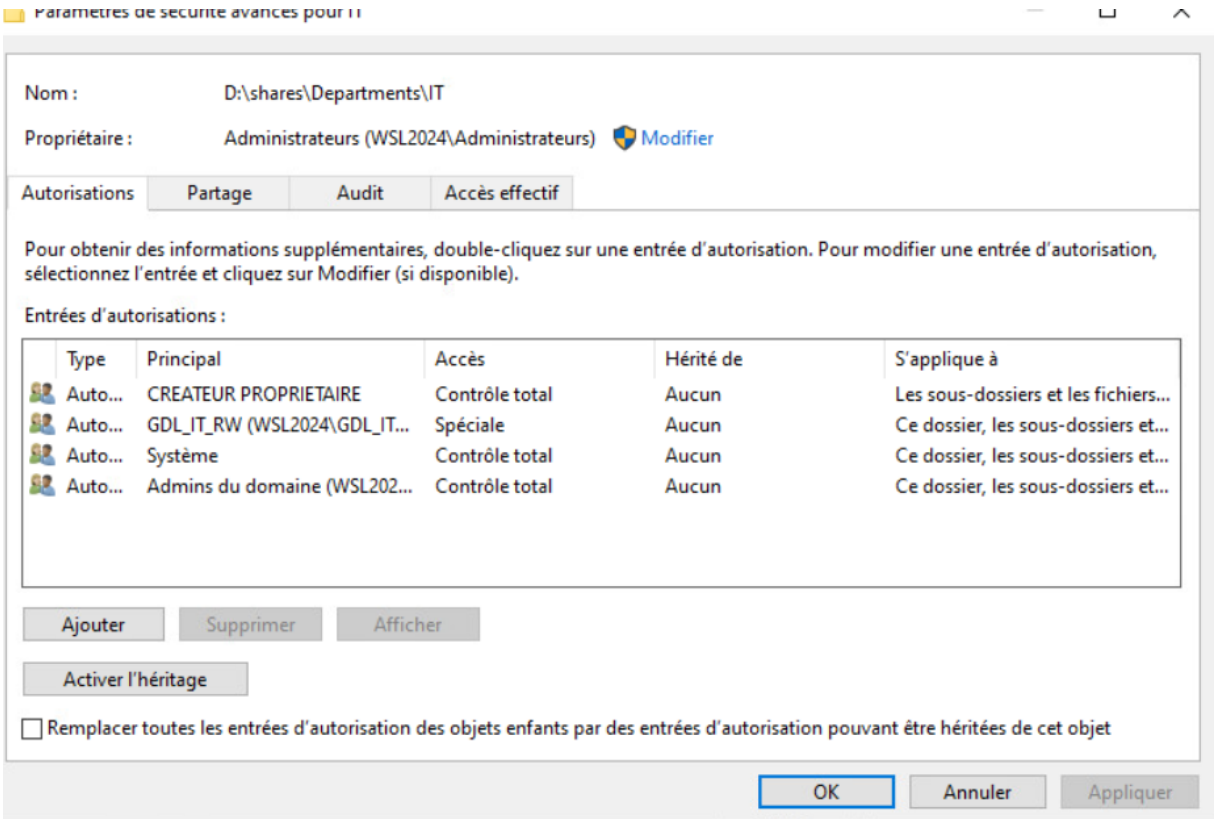
Une fois le partage activé, nous avons défini les autorisations suivantes :

- Les utilisateurs du domaine peuvent avoir accès en lecture/écriture au dossier partagé Départements et aux sous dossiers.
- Les administrateurs du domaine ont contrôle total.





Une fois cela fait, nous avons désactivé l'héritage des permissions sur les dossiers enfants de ces partages afin de distribuer des permissions personnalisées.

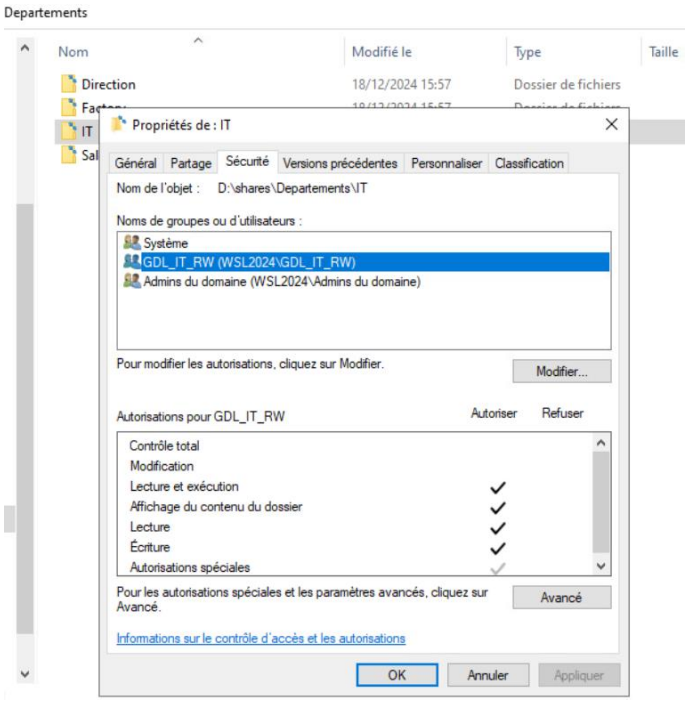


Voici les droits qui devaient etre mise en place en fonction des utilisateurs et de leurs groupes :

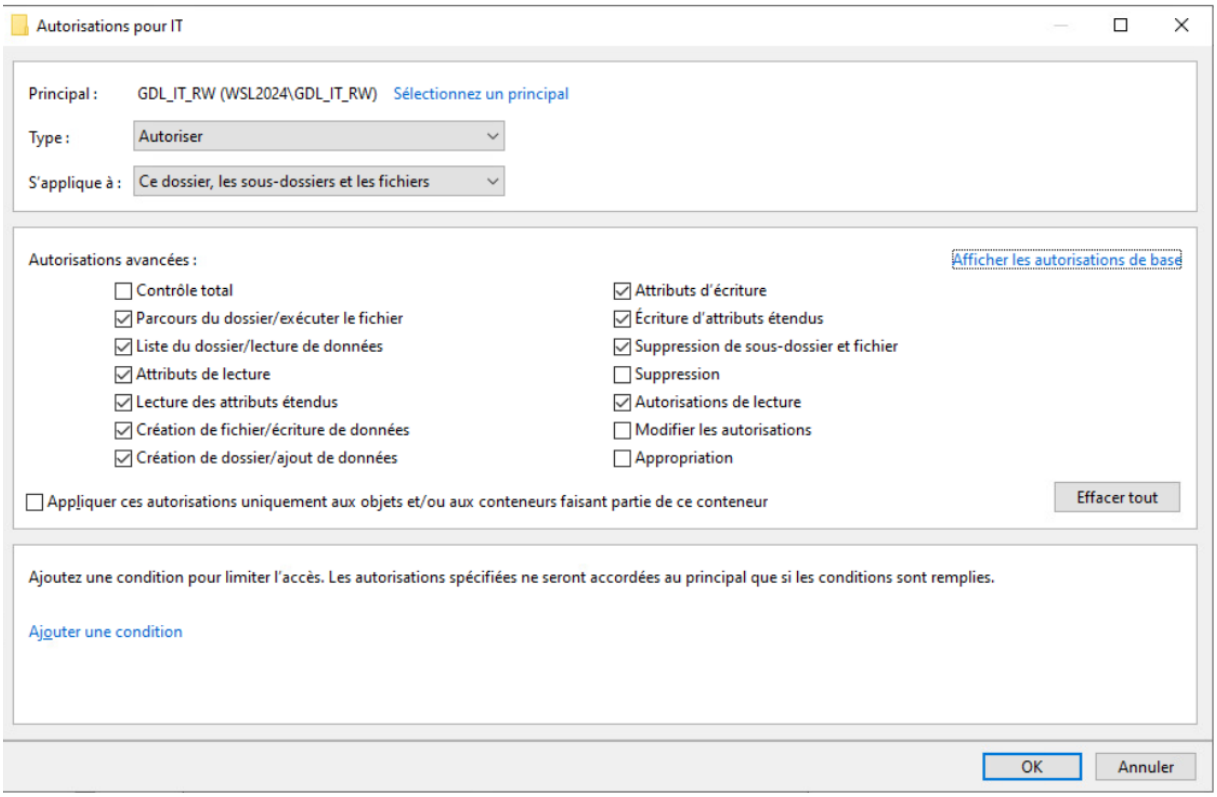
2. Department
- Located on D:\shares\Department
- Mounted with letter S:
- Users can only access their department folder
- Users can only see their department folder

3. Each department have a folder inside it named Public
- Located on D:\shares\Public
- Mounted with letter P:
- All users of the department have RW rights on this folder.

Nous avons donc ajouté les groupes de domaine LOCAL, en respectant la méthode AGDLP, en leurs ajoutant les permissions nécessaires pour que les utilisateurs puissent y avoir accès.

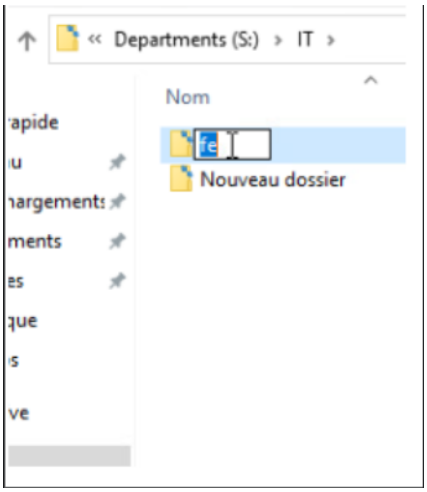


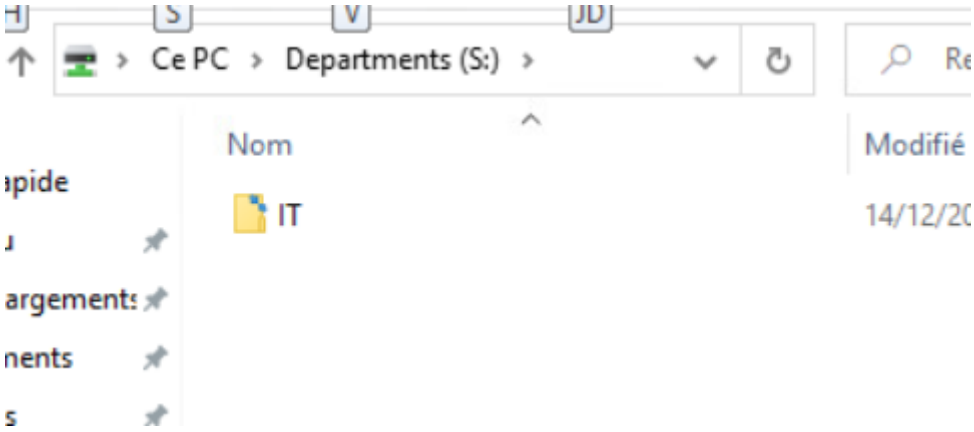
Il a aussi fallu modifier les autorisations avancées et décocher l'autorisation « suppression » et cocher l'autorisation « suppression des sous-dossiers et fichiers » pour empêcher les utilisateurs de supprimer le dossier parent.



Une fois cela configuré, nous avons déployé par GPO les lecteurs réseaux des dossiers partagés. Nous pouvons les voir sur HQCLT avec l'utilisateur Vincent TIM

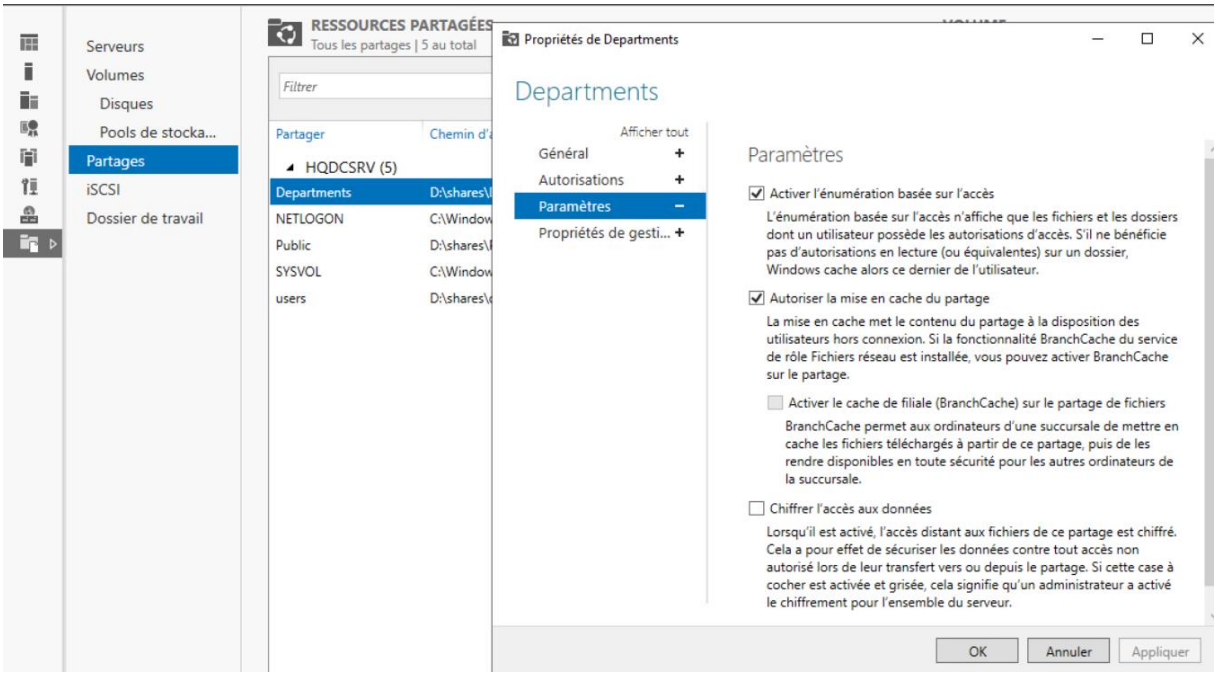
Nous pouvons ensuite accéder à ces partages depuis l'utilisateur Vincent TIM avec les autorisations configurées



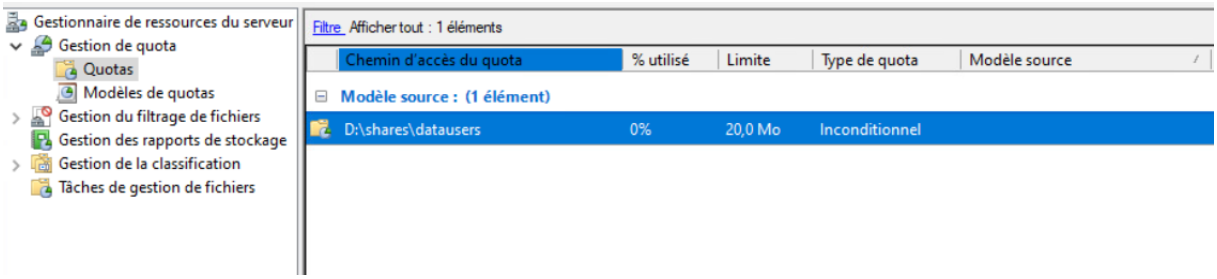


Afin que les utilisateurs ne puissent voir les dossiers des autres utilisateurs et départements, nous avons activé l'ABE (Access Based Enumeration). Cette fonctionnalité permet aux dossiers d'être visibles des utilisateurs ayant des droits dessus. Ainsi, si un utilisateur n'a pas de droits d'accès configuré sur un dossier partagé, il ne verra pas ce dossier partagé. En d'autre termes, L'ABE permet de masquer automatiquement les dossiers auxquels un utilisateur n'a pas les **droits d'accès**. Voici comment nous l'avons configuré :

Dans le gestionnaire de serveurs, nous sommes allés dans « Services de fichiers » puis « partages ». Nous sommes allés dans les propriétés et dans l'onglet paramètre, nous avons activé cette fonctionnalité.



Afin de limiter les utilisateurs à un quota de 20 MB, nous avons installé le gestionnaire des ressources du serveur de fichier. Celui-ci nous a permis de déclarer un quota de 20 Mo sur les dossiers présent dans le partage datausers.



Il fallait également interdire les fichiers exécutables dans ces dossiers. Pour cela, toujours dans ce gestionnaire dans « Gestion du filtrage de fichier », nous avons définis une règle interdisant l'utilisation de fichiers exécutables.