PR01 – Mise en place d'un serveur de fichiers sous Windows

Sommaires :

Contexte :

Nous sommes chargés par notre établissement de restructurer et sécuriser les dossiers partagés sur un serveur Windows.

Objectifs :

1. Proposer une arborescence de dossiers répondant aux besoins de l'établissement.

2. Proposer des groupes d'utilisateurs avec 2 comptes par groupe répondant au besoin.

3. Mettre en œuvre la sécurité au niveau du système de fichiers (Onglet Sécurité) et de (Onglet Partage).

4. Mettre en place une méthode de montage automatique des lecteurs réseaux.

5. Montrer avec des tests significatifs, que les contraintes de sécurité du cahier des charges sont respectées.

Cahiers des charges :

L'établissement compte plusieurs classes, des formateurs et une équipe administrative.

Sécurisation demandée :

1) Les membres de l'équipe administrative ont un espace qui n'est accessible que par eux en écriture/lecture. Chacun dispose d'un espace personnel qui lui est propre et l'équipe dispose d'un espace commun accessible en lecture/écriture pour tous.

2) Chaque classe dispose d'un espace commun « élèves » et d'un espace commun à l'ensemble des professeurs de la classe dans lequel ceux-ci mettent à disposition des élèves, des supports de cours. Les élèves peuvent lire des documents dans l'espace professeurs, mais ne peuvent supprimer aucun document.

3) L'équipe administrative et les élèves ont accès en lecture à l'espace réservé aux professeurs d'une classe.

4) Les formateurs ont accès à l'espace commun « élèves » d'une classe, pour enregistrer un nouveau document ou faire « enregistrer-sous » pour créer une copie d'un document d'un élève. Ils ont bien sûr accès en lecture aux documents des élèves mais ne peuvent en aucun cas les supprimer.

5) Un élève ne peut pas supprimer ou modifier le document d'un autre élève.

Solution :

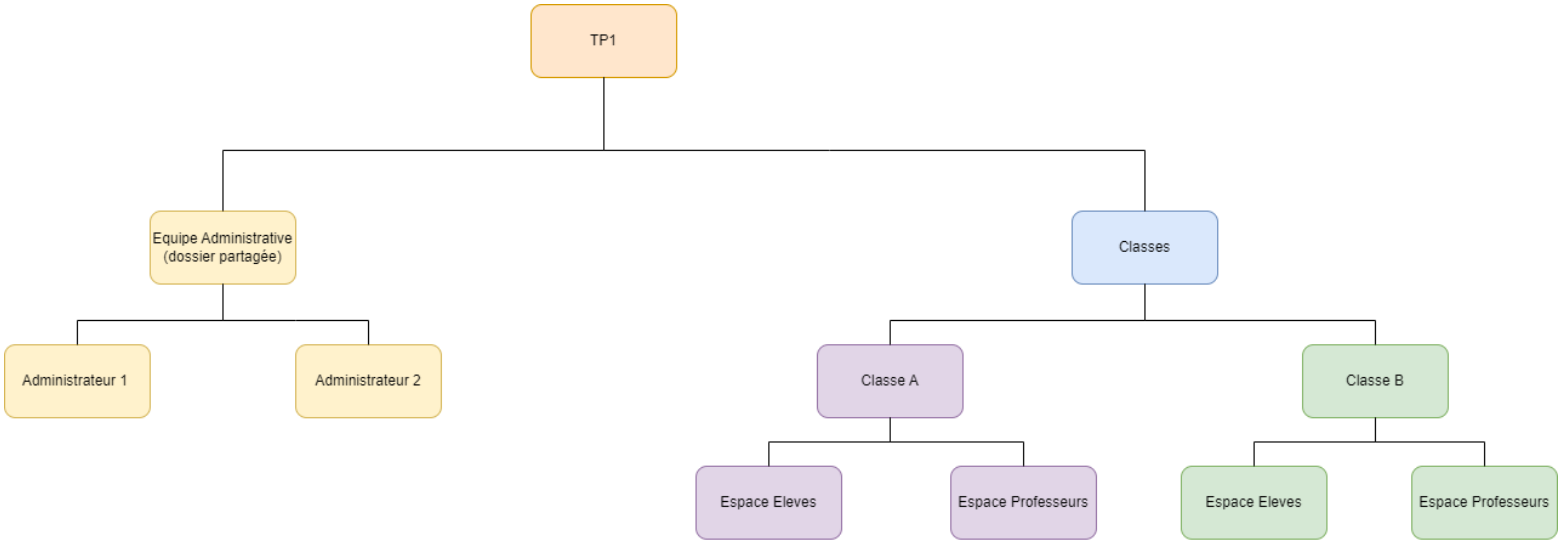
Pour répondre aux attentes de notre établissement, deux machines virtuelles seront créées : l'une pour héberger notre serveur Windows, et l'autre pour servir de poste de test.

Les dossiers et groupes/utilisateurs nécessaires seront ensuite créés et les mesures de sécurité appropriées seront mises en place pour assurer un bon partage des fichiers.

Pour finir, une GPO (Group Policy Object) sera implémentée.

Schéma ASI :

1) Arborescences des dossiers :



2) Groupes d'utilisateurs :

a) gg-EquipeAdministrative : Admin 1, Admin2
b) gg-ProfClasseA : Aurelien, Stephane
c) gg-ProfClasseB : Amadou, Virginie
d) gg-Eleve: George2, seb, leo, thomas
e) gg-ClasseA : George2, seb
f) gg-ClasseB : leo, thomas

Prérequis :

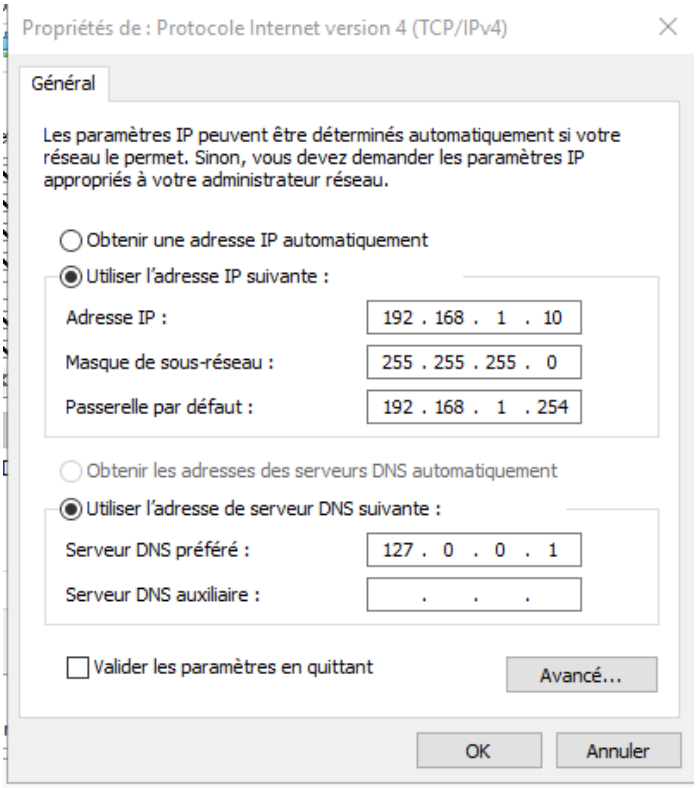
Nous commencerons par installer et configurer une machine virtuelle dédiée à notre serveur Windows 2019. Les services nécessaires, tels que l'activation de l'Active Directory, la création des dossiers, des groupes/utilisateurs, ainsi que la mise en place d'une GPO, seront ensuite configurés.

En parallèle, nous créerons une machine virtuelle pour un poste sous Windows 11 Pro afin d'effectuer les tests nécessaires à la validation du bon fonctionnement de notre infrastructure.

Pour cela nous allons utiliser Oracle VM, et les cartes réseau seront configurées en mode « Accès par pont ».

Configuration réseau du serveur et du poste client :

Configuration réseau du Serveur :



Nous lui attribuons une adresse IP fixe :

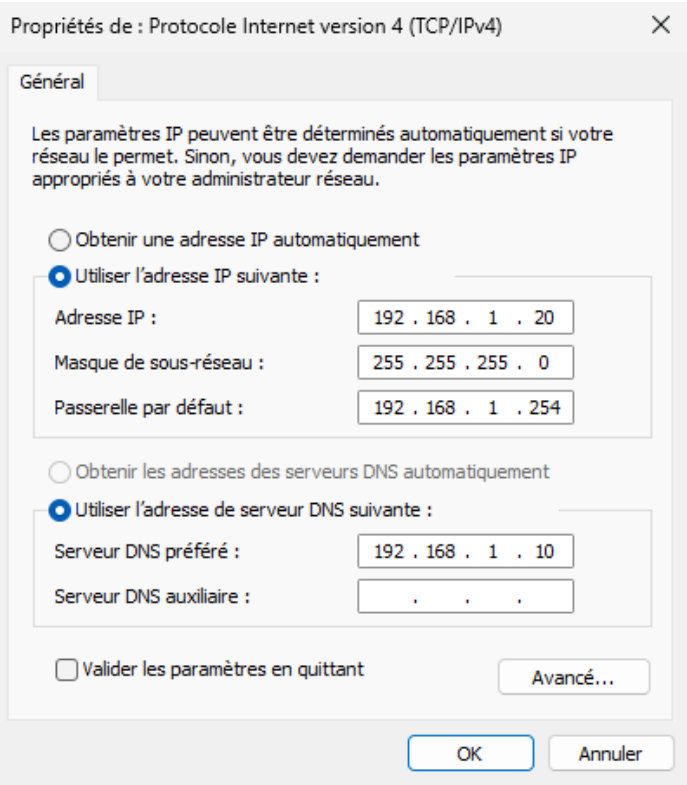
- 192.168.1.10

Pour le DNS on met l'adresse IP du contrôleur de domaine donc lui-même.

- 127.0.0.1

Ensuite on va désactiver la configuration par IpV6 dans le menu de réseau.

Configuration réseau du poste Client :



Nous lui attribuons une adresse IP fixe qui est sur le même réseau que le serveur :

- 192.168.1.20

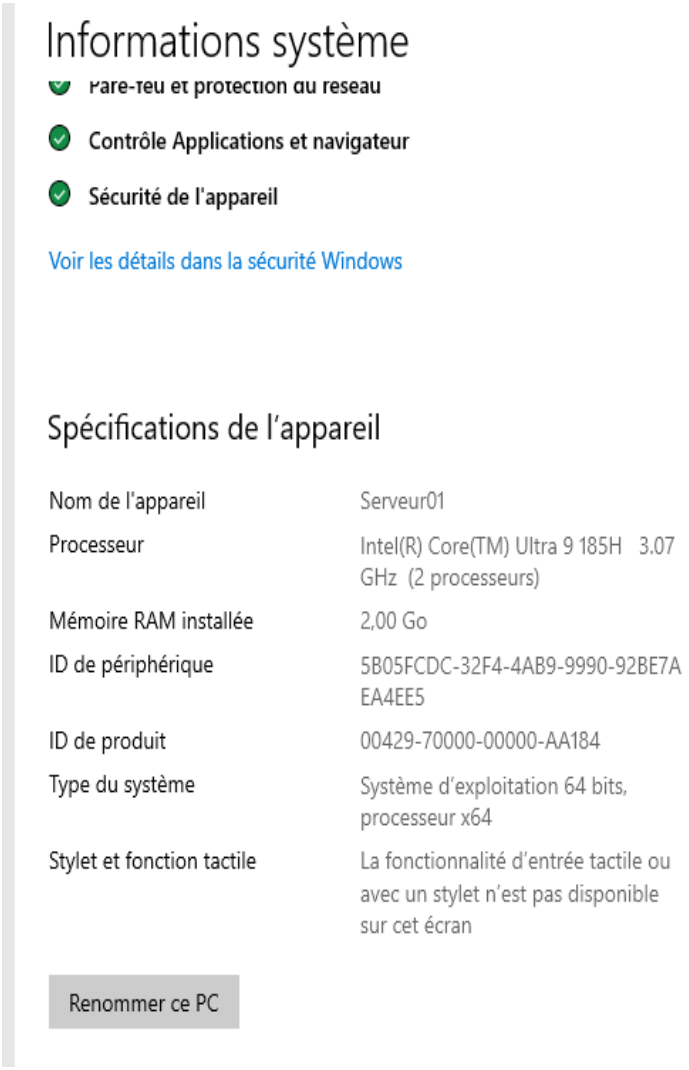
Pour le DNS on met l'adresse IP du contrôleur de domaine donc celle du serveur :

- 192.168.1.10

Maintenant que les interfaces réseau sont configurées, on pourra installer les services nécessaires.

Configuration du serveur :

Après le démarrage de Windows Server, il sera nécessaire de renommer l'ordinateur en « Serveur01 ».

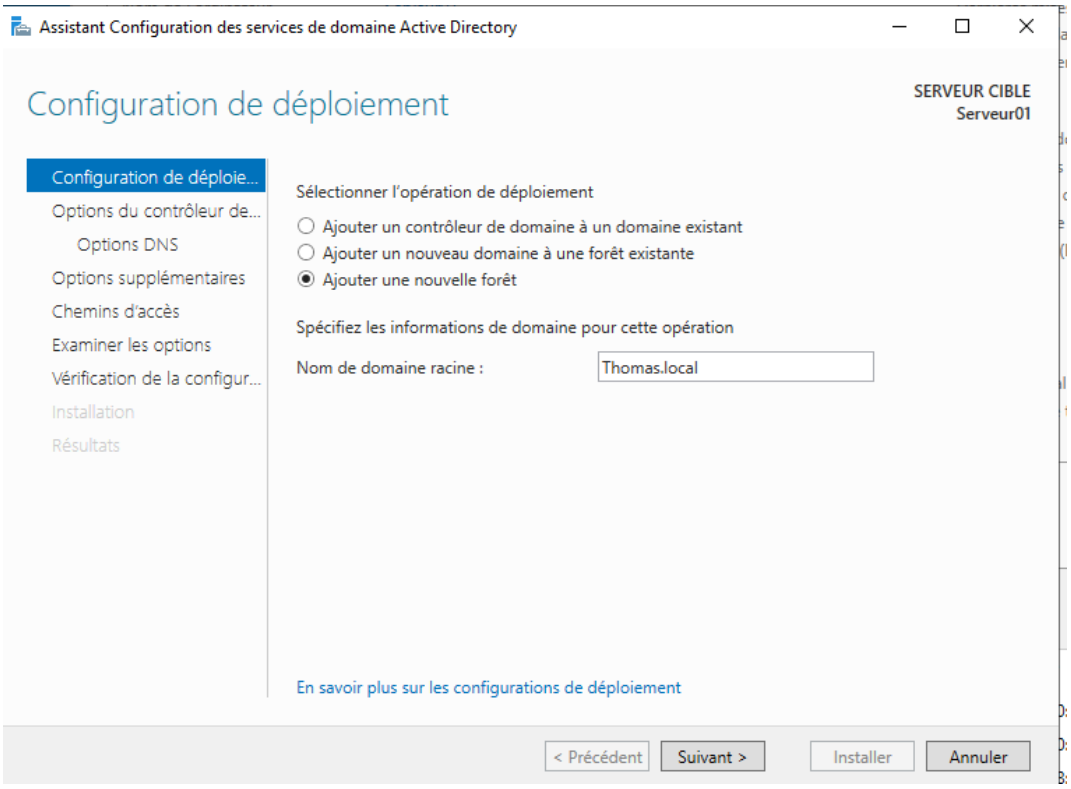


Création du domaine de l'active directory :

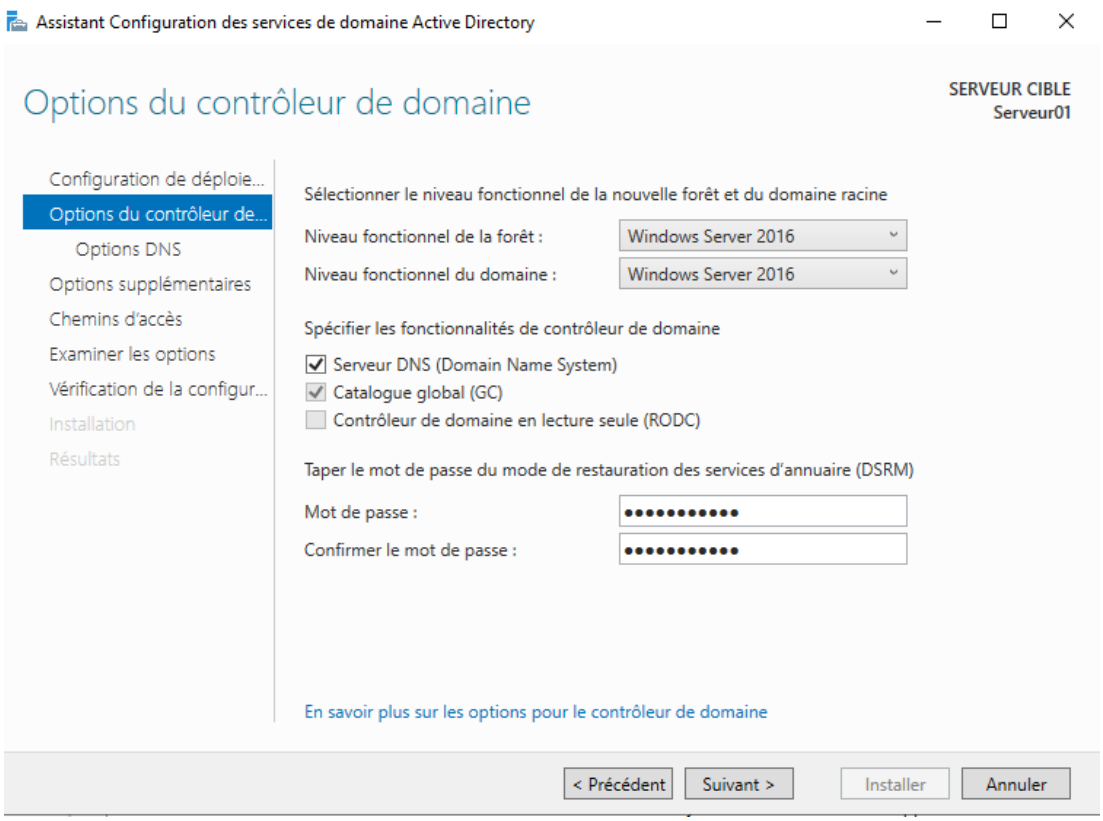
Via le gestionnaire de serveur, il faudra lancer l'assistant d'ajout de rôles et de fonctionnalités pour installer Active Directory, ce qui nous permettra de gérer notre serveur.

Ensuite nous créons un domaine qui s'appelle « Thomas.local ». Toutes les informations du serveur local sont visibles dans le Gestionnaire de Serveur.

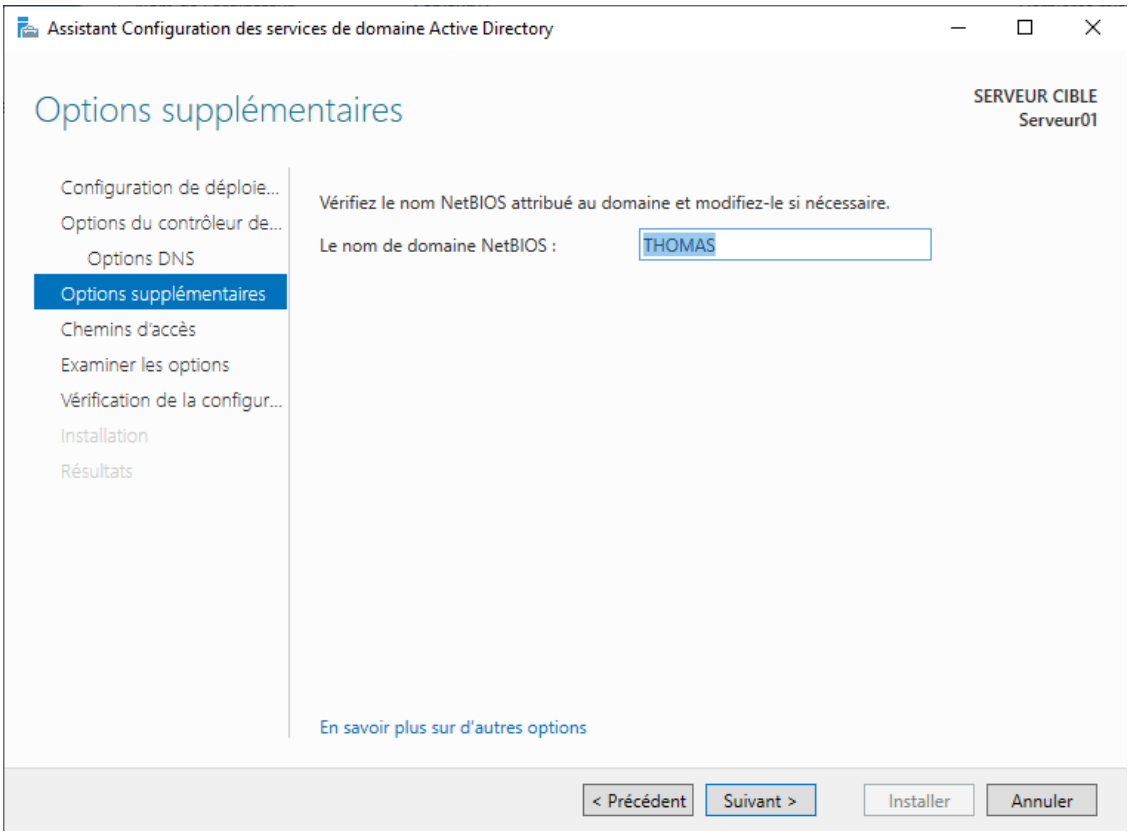
Le serveur Windows devient contrôleur de domaine, il va centraliser la base des comptes utilisateurs et va nous permettre d'administrer les ressources et les objets du domaine



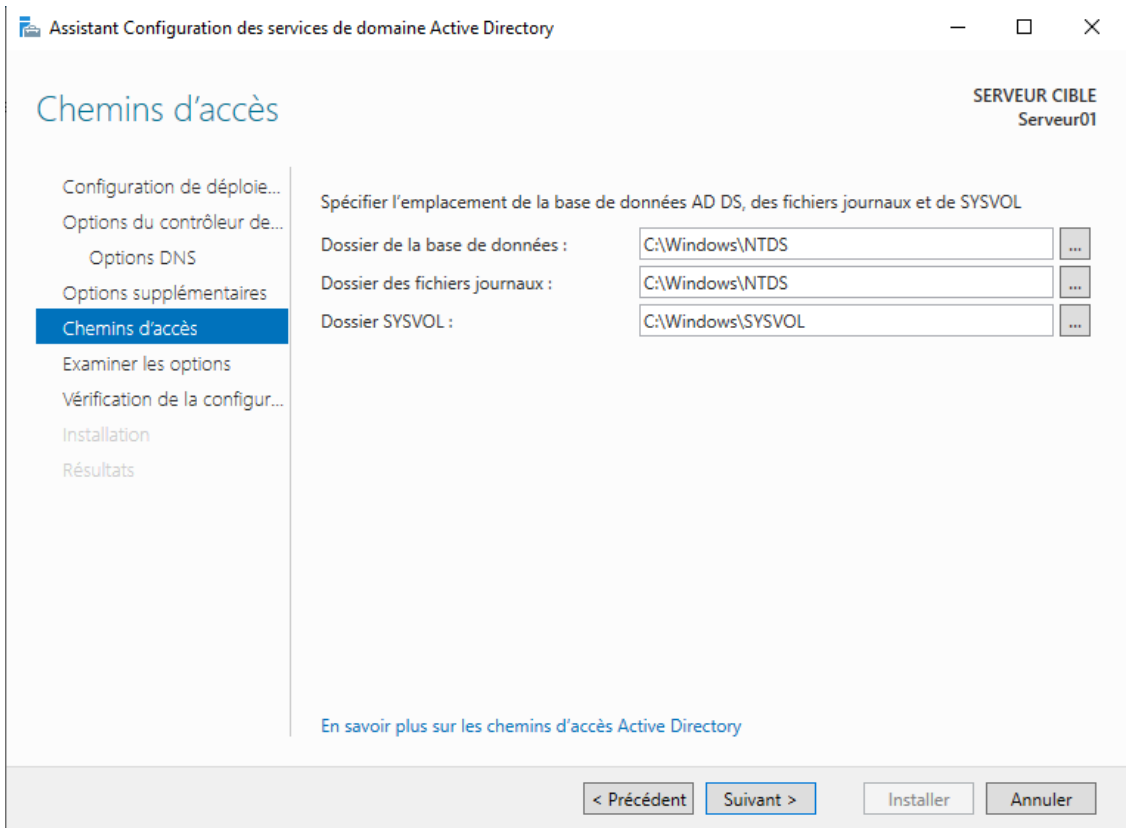
Création de la foret Thomas.local



Choix du niveau fonctionnel et du service DNS

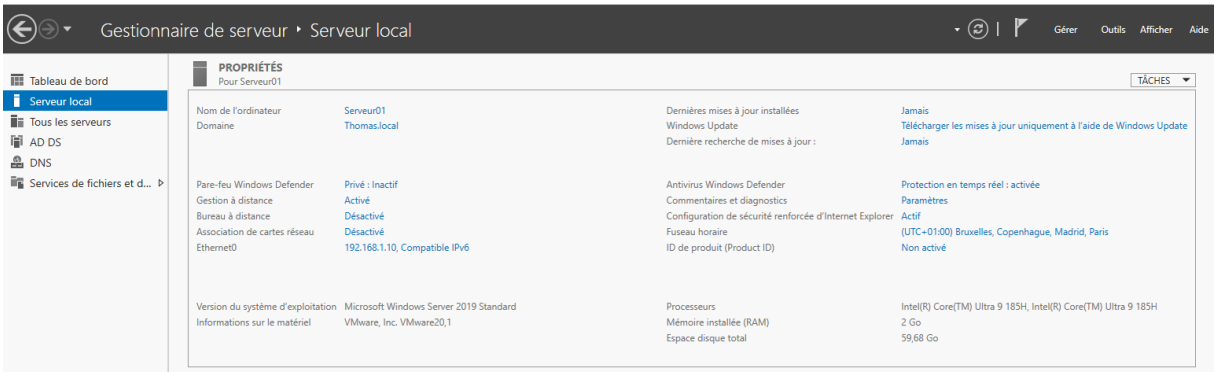


Choix du nom NetBIOS



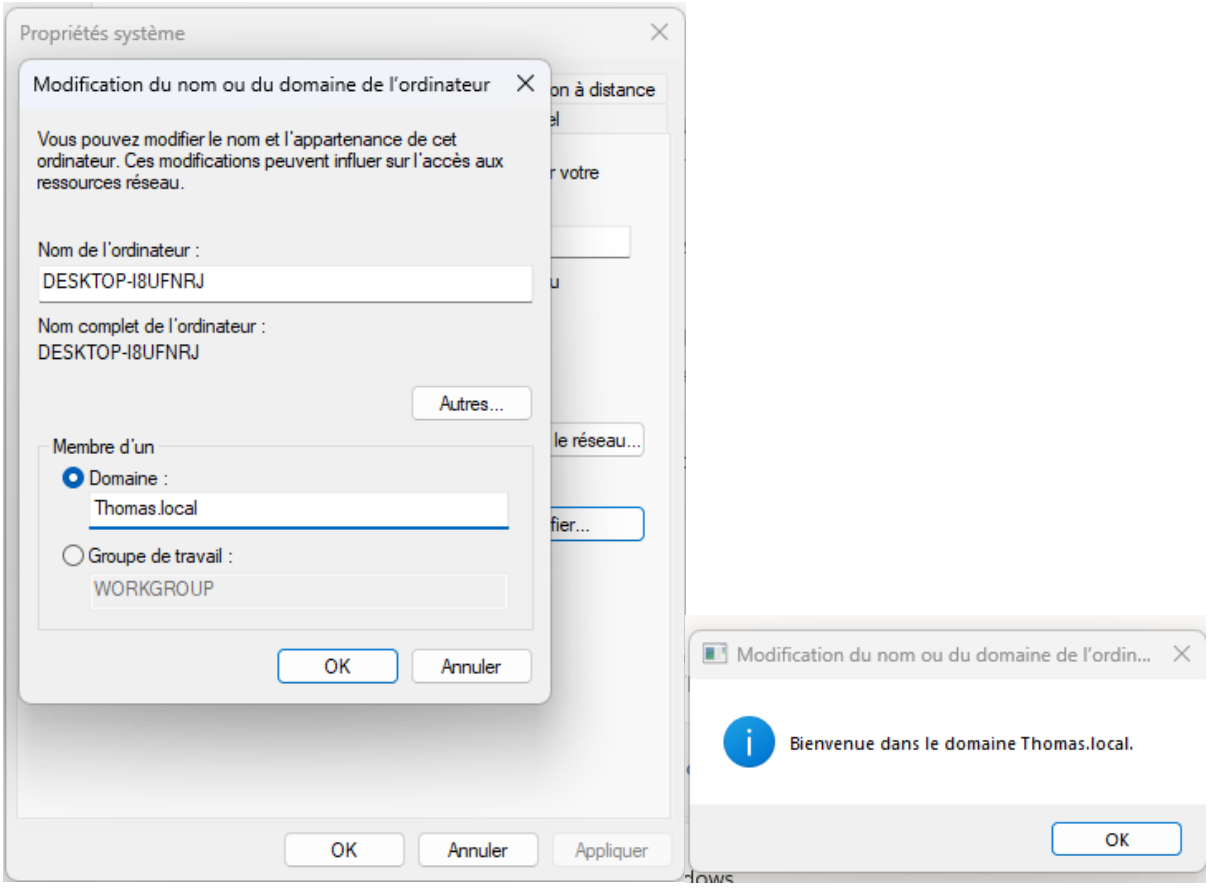
Choix des chemins d'accès

Nous avons plus qu'à vérifier la configuration et valider l'installation de notre domaine.



Notre Domaine et donc fonctionnel, nous allons maintenant faire rentrer le poste client dans le domaine :

Nous devons passer par les paramètres système et configurer le PC comme membre d'un domaine (ici, Thomas.local).

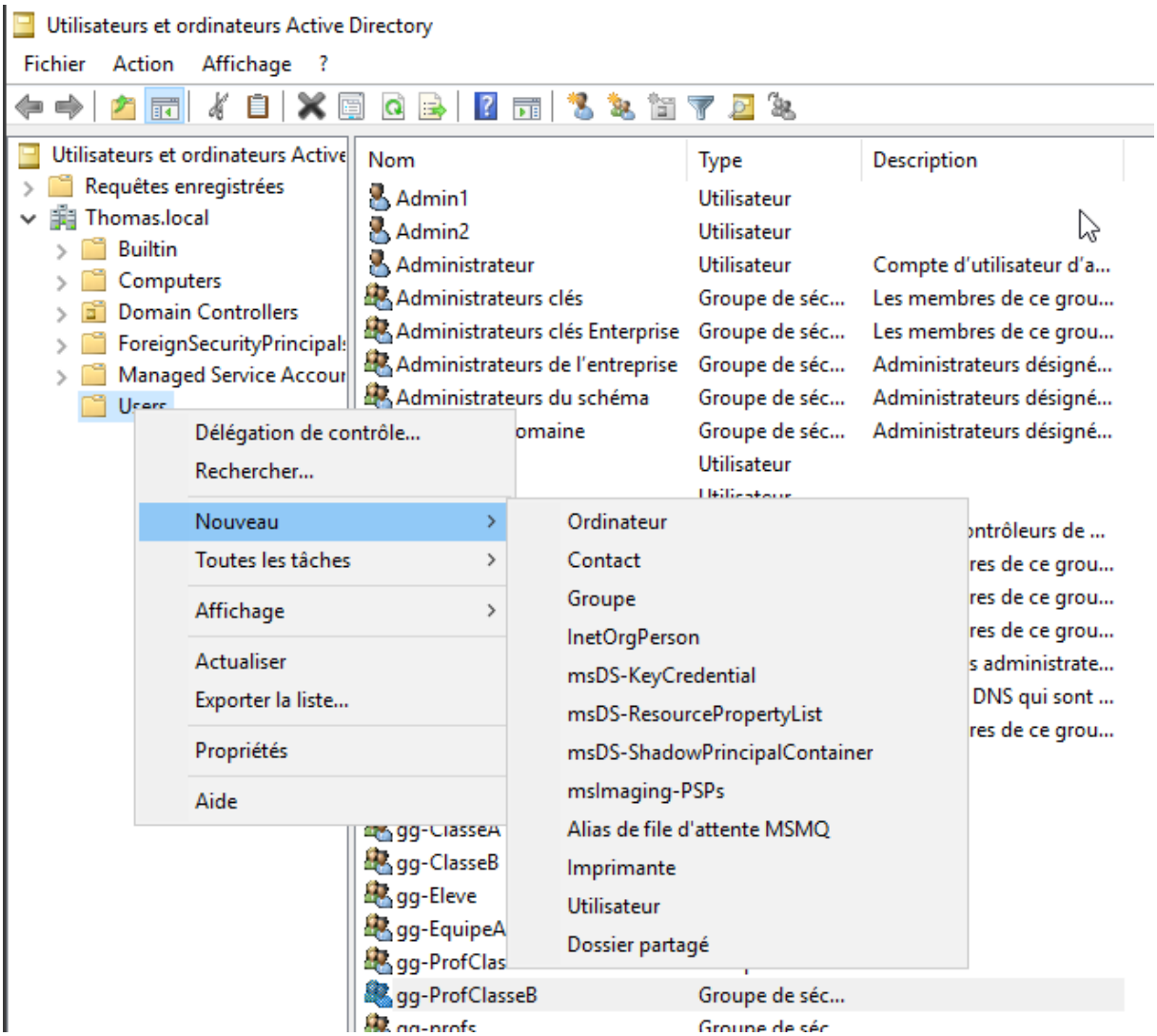


Maintenant, nous pouvons passer à la création de l'arborescence des répertoires, ainsi qu'à la gestion des rôles, des utilisateurs et de leurs groupes respectifs.

Création des utilisateurs / groupes

Pour créer un utilisateur il faut se rendre sur le Gestionnaire de serveur -> outils -> utilisateur et ordinateurs Active Directory

Il faut créer un utilisateur sur le dossier Users c'est également la que l'on pourra crée des groupes

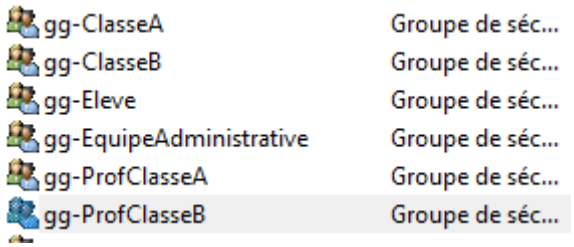


Il faudra donc remplir le Prénom et le nom d'ouverture de session,

Puis rajouter un mot de passe, qui peut être changé ou non en fonction des options.

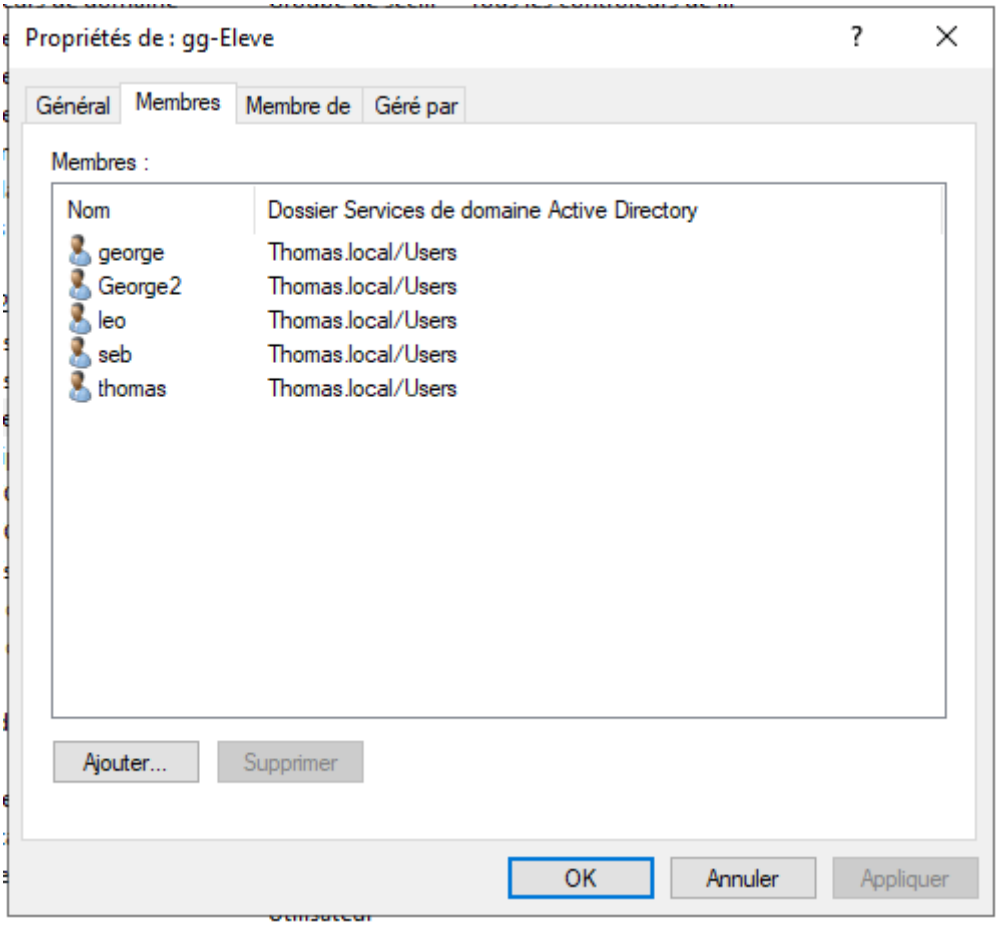
Une fois tous les utilisateurs créés, il faut créer des groupes.

On va créer des groupes globaux car on a un seul domaine ici.



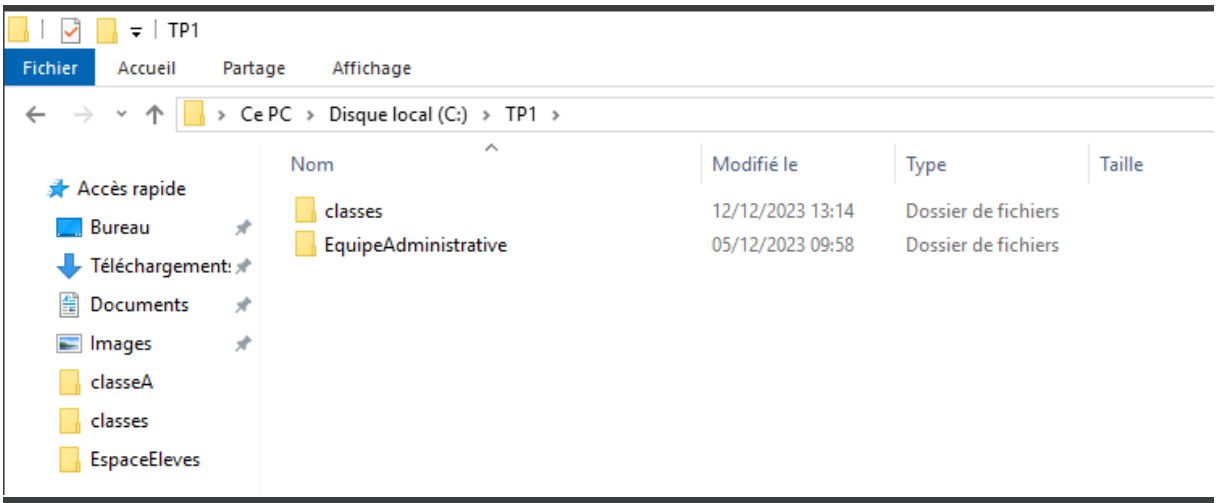
Puis ajouter les différents membres dans leur groupe respectifs

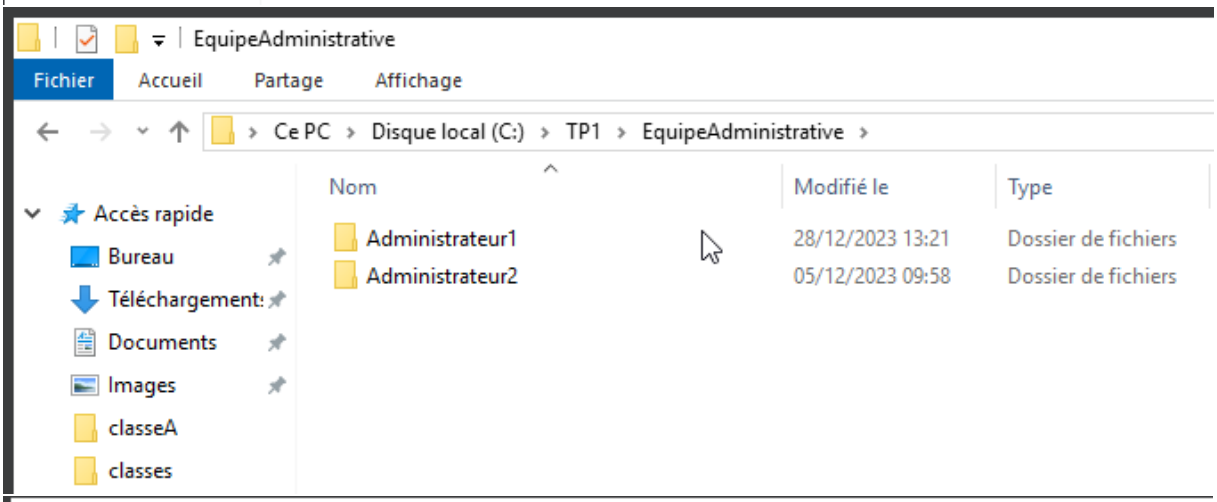
Exemple ici avec le groupe gg-Eleve :

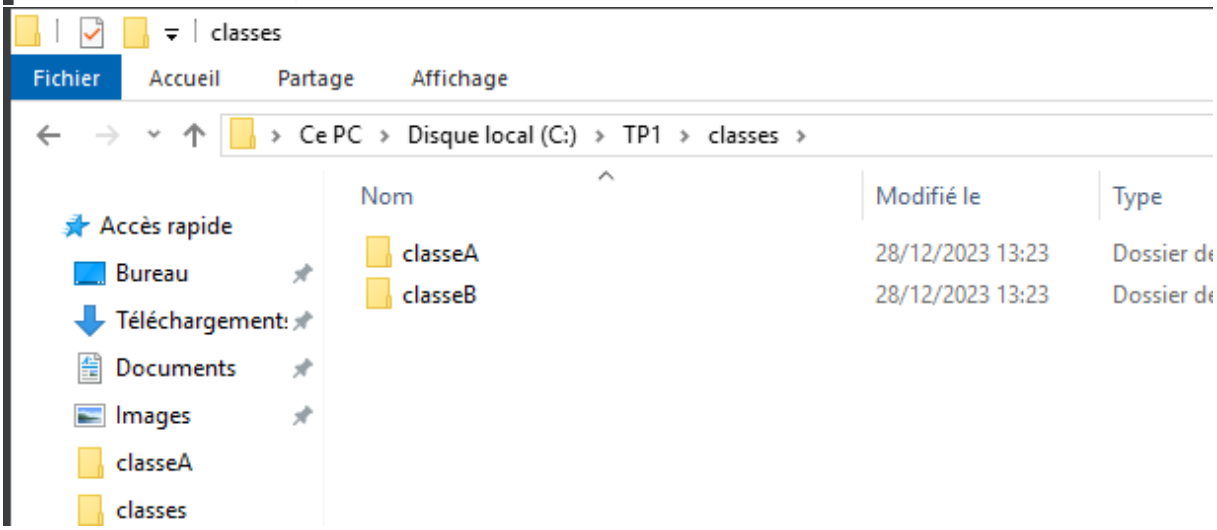


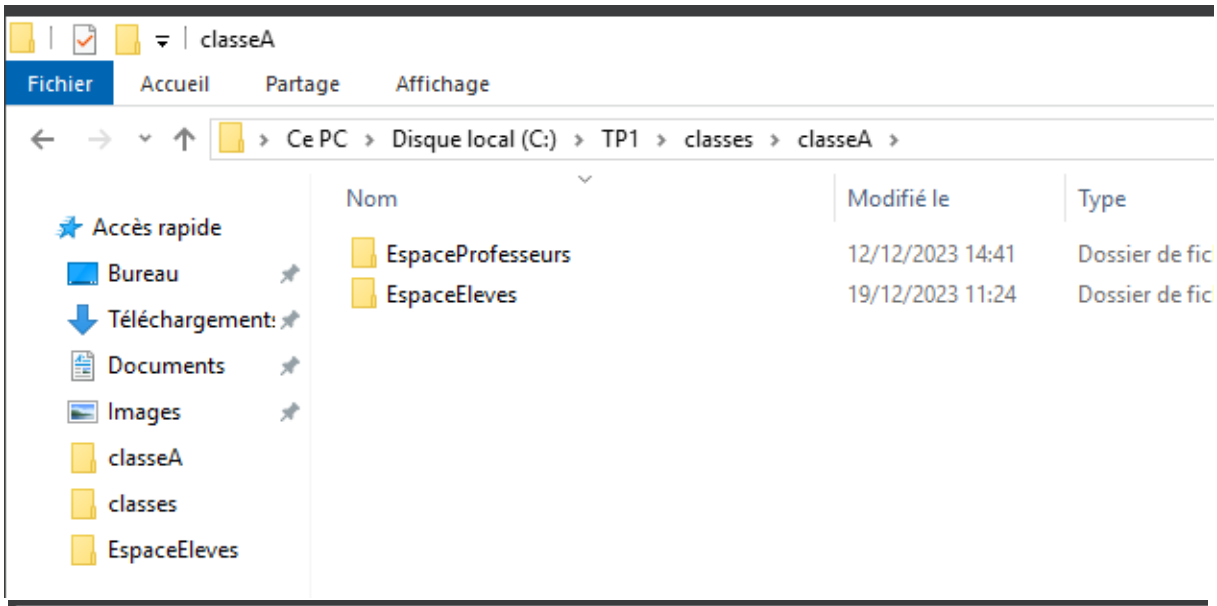
Création des dossiers

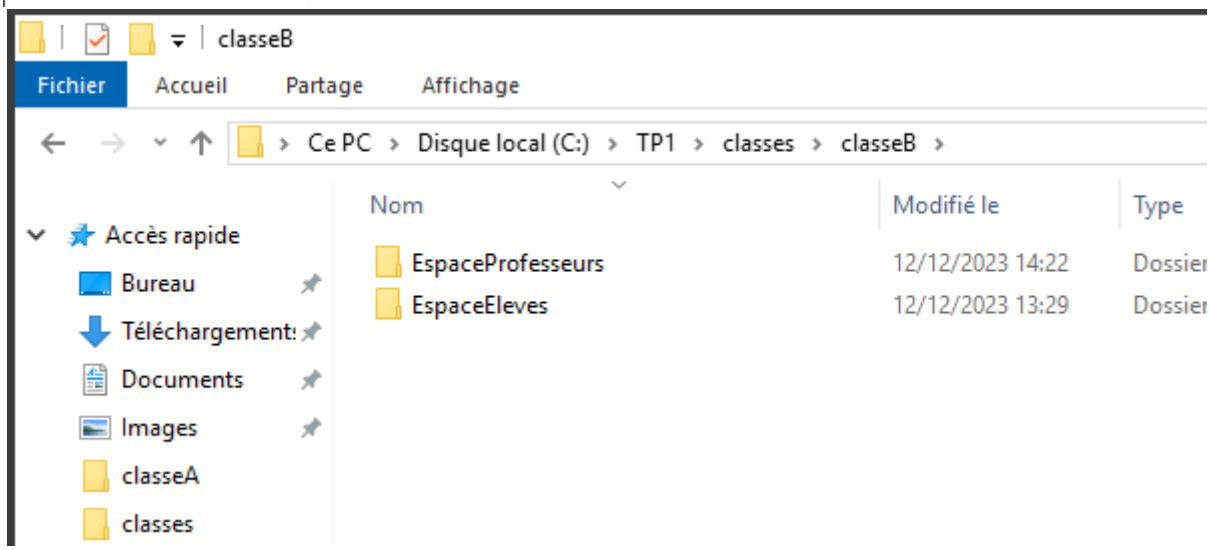
Maintenant que les utilisateurs et groupes sont créer, on va maintenant créer tous les dossiers nécessaires.


TP1
Fichier
Accueil
Partage
Affichage
Ce PC › Disque local (C:) › TP1 ›
Accès rapide
Bureau
Téléchargement
Documents
Images
classeA
classes
EspaceEleves
Nom
Modifié le
Type
Taille
classes
12/12/2023 13:14
Dossier de fichiers
EquipeAdministrative
05/12/2023 09:58
Dossier de fichiers


EquipeAdministrative
Fichier
Accueil
Partage
Affichage
Ce PC › Disque local (C:) › TP1 › EquipeAdministrative ›
Accès rapide
Bureau
Téléchargement
Documents
Images
classeA
classes
Nom
Modifié le
Type
Administrateur1
28/12/2023 13:21
Dossier de fichiers
Administrateur2
05/12/2023 09:58
Dossier de fichiers


classes
Fichier
Accueil
Partage
Affichage
Ce PC › Disque local (C:) › TP1 › classes ›
Accès rapide
Bureau
Téléchargement
Documents
Images
classeA
classes
Nom
Modifié le
Type
classeA
28/12/2023 13:23
classeB
28/12/2023 13:23



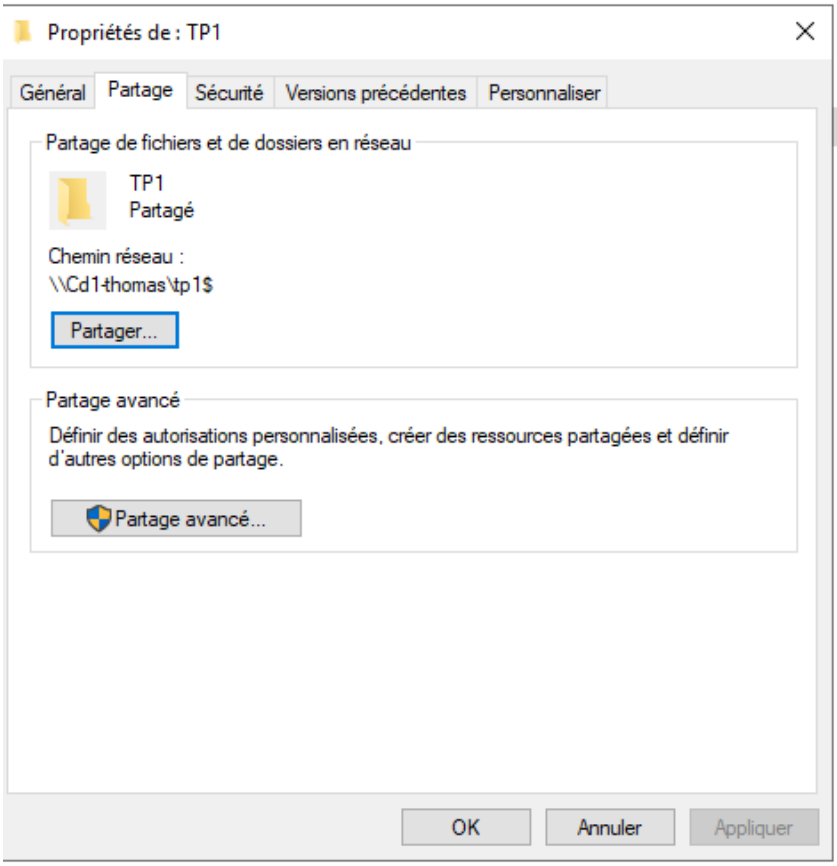


Partage et Sécurisation des dossiers (NTFS)

Ces dossiers sont accessibles et modifiable par tous, car aucun partage ni aucune sécurité n'est encore configurée.

L'accès doit être limité en fonction du statut de chaque individu au sein de l'école. Par exemple, un élève n'aura pas les mêmes droits qu'un professeur ou qu'un membre de l'équipe administrative. Nous allons nous baser sur le système de fichier NTFS pour cela.

Il faut partir du premier dossier, celui qui stocke tous les autres et avancer dans l'arborescence.

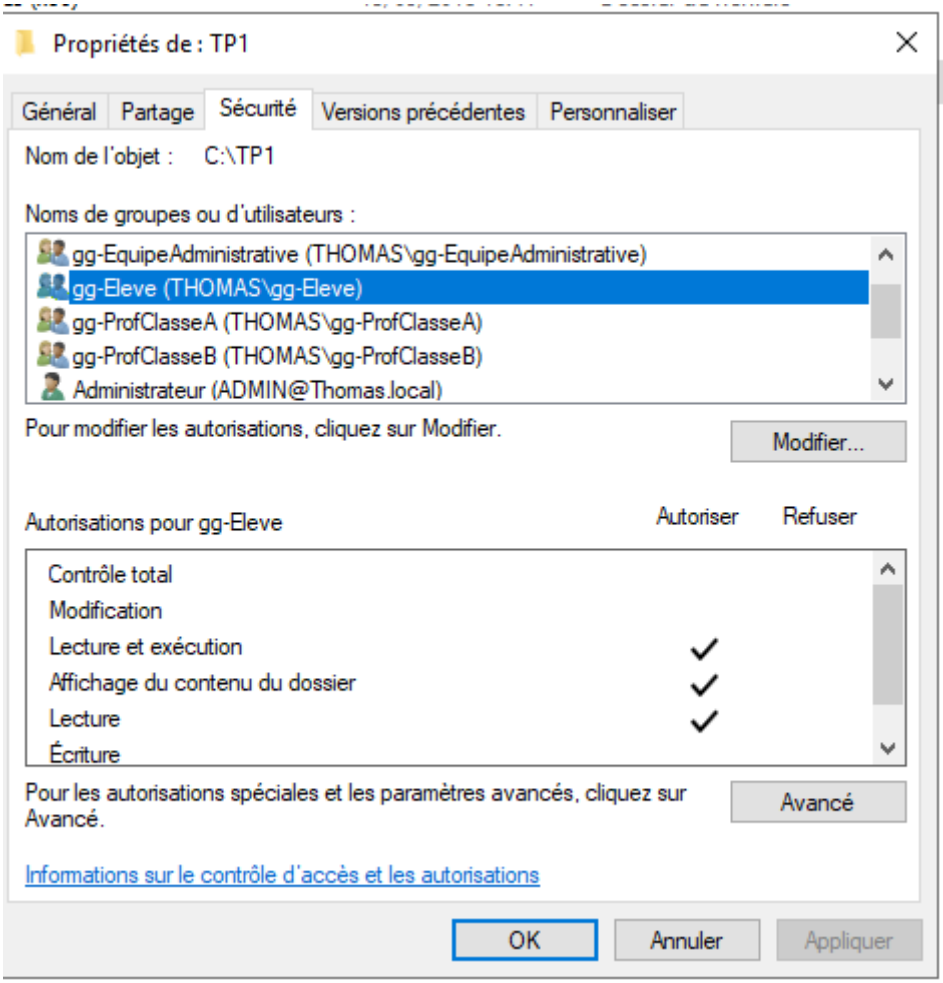


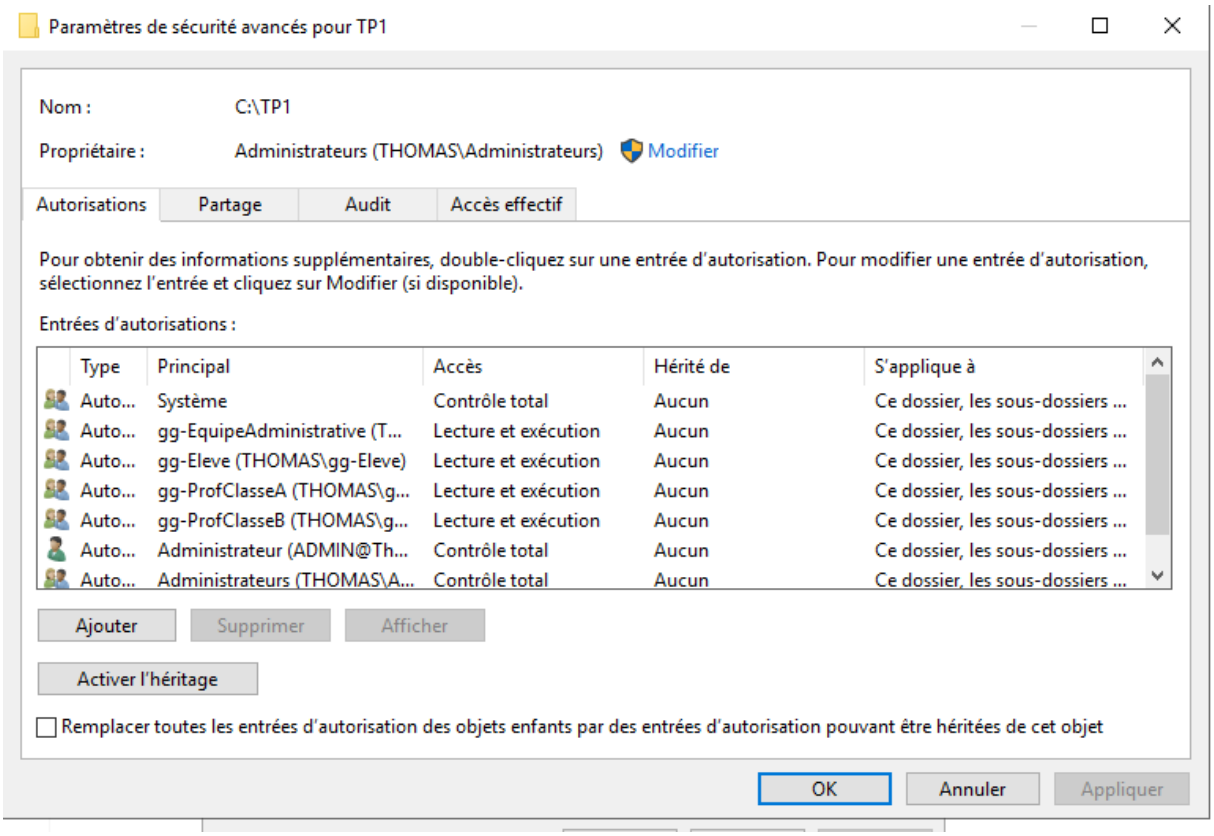
Le dossier TP1 a été partagé (il faut le cacher et on utilise $). Il n'est plus nécessaire de partager les autres dossiers individuellement, car le dossier racine est déjà partagé.

La prochaine étape consiste à sécuriser ces dossiers.

Pour cela on va devoir aller dans l'onglet sécurité afin de définir les droits de chacun et cela dans chaque dossier

Lors de la sécurisation il faudra penser à désactiver les héritages !


Propriétés de : TP1
Général
Partage
Sécurité
Versions précédentes
Personnaliser
Nom de l'objet : C:\TP1
Noms de groupes ou d'utilisateurs :
gg-EquipeAdministrative (THOMAS\gg-EquipeAdministrative)
gg-Eleve (THOMAS\gg-Eleve)
gg-ProfClasseA (THOMAS\gg-ProfClasseA)
gg-ProfClasseB (THOMAS\gg-ProfClasseB)
Administrateur (ADMIN@Thomas.local)
Pour modifier les autorisations, cliquez sur Modifier.
Modifier...
Autorisations pour gg-Eleve
Autoriser
Refuser
Contrôle total
Modification
Lecture et exécution
Affichage du contenu du dossier
Lecture
Écriture
Pour les autorisations spéciales et les paramètres avancés, cliquez sur Avancé.
Avancé
Informations sur le contrôle d'accès et les autorisations
OK
Annuler
Appliquer


Paramètres de sécurité avancés pour TP1
Nom : C:\TP1
Propriétaire : Administrateurs (THOMAS\Administrateurs) Modifier
Autorisations
Partage
Audit
Accès effectif
Pour obtenir des informations supplémentaires, double-cliquez sur une entrée d'autorisation. Pour modifier une entrée d'autorisation, sélectionnez l'entrée et cliquez sur Modifier (si disponible).
Entrées d'autorisations :
Type
Principal
Accès
Hérité de
S'applique à
Auto... Système Contrôle total Aucun Ce dossier, les sous-dossiers ...
Auto... gg-EquipeAdministrative (T... Lecture et exécution Aucun Ce dossier, les sous-dossiers ...
Auto... gg-Eleve (THOMAS\gg-Eleve) Lecture et exécution Aucun Ce dossier, les sous-dossiers ...
Auto... gg-ProfClasseA (THOMAS\g... Lecture et exécution Aucun Ce dossier, les sous-dossiers ...
Auto... gg-ProfClasseB (THOMAS\g... Lecture et exécution Aucun Ce dossier, les sous-dossiers ...
Auto... Administrateur (ADMIN@Th... Contrôle total Aucun Ce dossier, les sous-dossiers ...
Auto... Administrateurs (THOMAS\A... Contrôle total Aucun Ce dossier, les sous-dossiers ...
Ajouter
Supprimer
Afficher
Activer l'héritage
Remplacer toutes les entrées d'autorisation des objets enfants par des entrées d'autorisation pouvant être héritées de cet objet
OK
Annuler
Appliquer

Dans ce cas, tous les utilisateurs ont les mêmes droits : Lecture et exécution, affichage de contenu du dossier et lecture

Il faut donc faire la même chose sur tous les autres dossiers :

- EquipeAdministrative : Seul les membres de l'équipe administrative ont accès au dossier, ils ont accès à : Lecture et exécution, affichage de contenu du dossier et lecture

  Le dossier EquipeAdministrative est composée de deux dossiers :

  - Administrateur 1 : accessible uniquement par l'Admin1, il a accès à : La modification, lecture et exécution, affichage du contenu du dossier, lecture, écriture.

  - Administrateur 2 : accessible uniquement par l'Admin2, il a accès à : La modification, lecture et exécution, affichage du contenu du dossier, lecture, écriture

- Classes : tous les utilisateurs ont les mêmes droits : Lecture et exécution – Affichage de contenu du dossier – lecture

  Le dossier classe est composée de deux dossiers :

  - classeA : accessible uniquement par la classe A et les profs de la classe A, ils ont accès à : Lecture et exécution, affichage de contenu du dossier et lecture
  - classeB : accessible uniquement par la classe B et les profs de la classe B, ils ont accès à : Lecture et exécution, affichage de contenu du dossier et lecture

  L'équipe administrative a accès aux deux classes, avec les mêmes droits que les autres utilisateurs.

  Le dossier ClasseA est composée de deux dossiers :

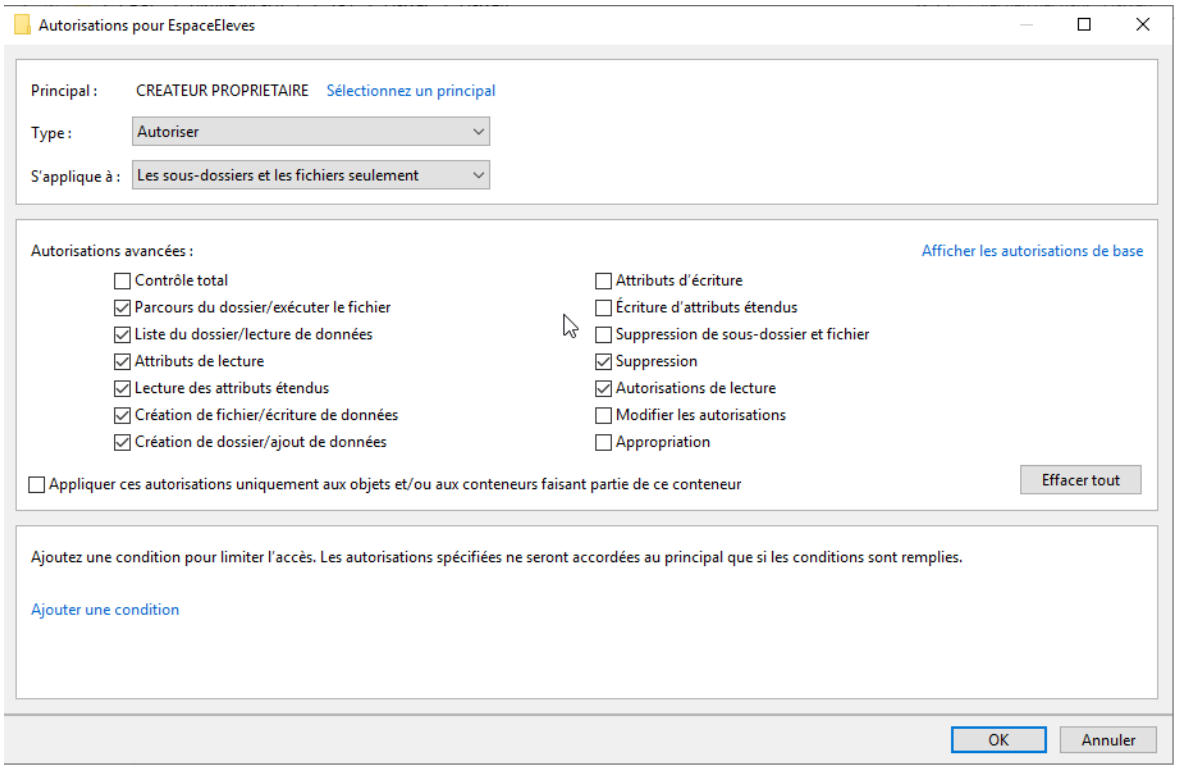
  - EspaceEleves : accessible uniquement par la classe A et les profs de la classe A ainsi que l'équipe administrative.
    L'équipe administrative a accès à : Lecture et exécution, affichage de contenu du dossier et lecture
    La classe A et les profs de la classe A ont accès à : Lecture et exécution, affichage de contenu du dossier et lecture et Autorisations spéciales (droit de créer des documents sans supprimer ceux dont on n'est pas propriétaire via créateur propriétaire)

  - EspaceProfesseurs : accessible uniquement par la classe A et les profs de la classe A ainsi que l'équipe administrative.
    L'équipe administrative et la classe A ont accès à : Lecture et exécution, affichage de contenu du dossier et lecture.
    Les profs de la classe A ont accès à : Lecture et exécution, affichage de contenu du dossier et lecture et Autorisations spéciales

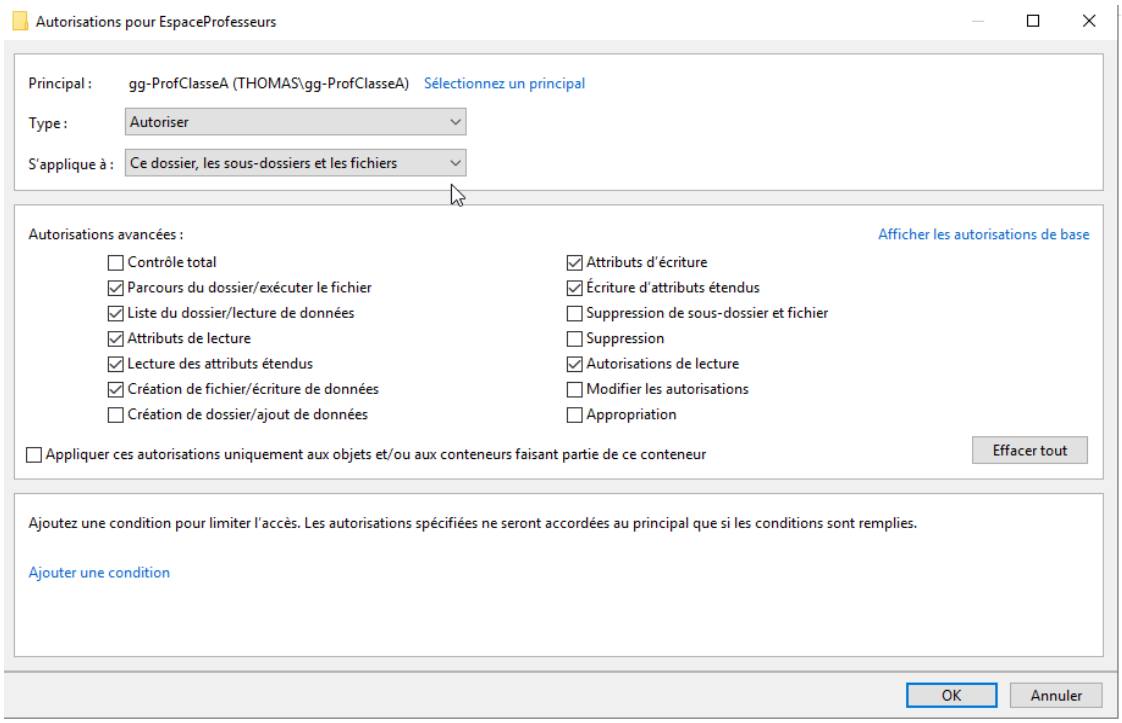
Pour ces deux dossiers on a mis en place un type particulier de groupe : Créateur Propriétaire

Lorsqu'une personne créée un dossier/fichiers elle devient automatiquement le créateur propriétaire de ce dossier/fichiers et obtiens des droits de contrôle spécial et total.

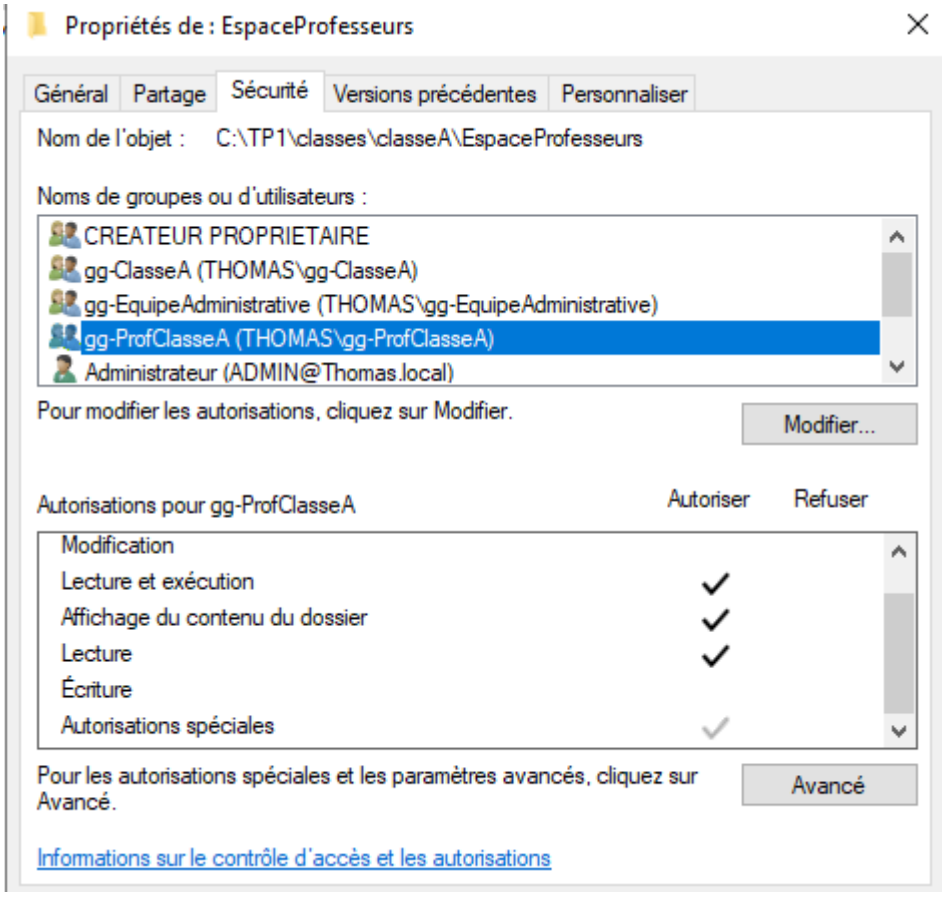
Ainsi personne ne peut modifier ou supprimer les fichiers de quelqu'un d'autres



Exemple :



Pour cela il suffit de cocher Création de fichier/écriture de données dans le groupe voulu, ici le groupe gg-ProfClasseA et grâce à Créateur propriétaire il aura les autorisations spéciales.



On a réalisé la même opération sur le groupe classeB !

Mise en place d'une GPO

On souhaite mettre en place une méthode de montage automatique des lecteurs réseaux.

On a plusieurs options :

- Utiliser un script de connexion pour monter automatiquement les lecteurs réseau lors de la connexion d'un utilisateur.

- Ou mettre en place une GPO

On va donc mettre en place une gpo qui permet d'établir des règles. Ici on va l'utiliser pour mapper automatiquement notre lecteur réseau du domaine sur les différents comptes utilisateurs du domaine lors du démarrage.

Pour la créer il faut se rendre dans le gestionnaire de serveur -> outils -> gestion des stratégies de groupe.

Il faut ensuite sélectionner le domaine où l'on souhaite faire la GPO et ordonner la création.

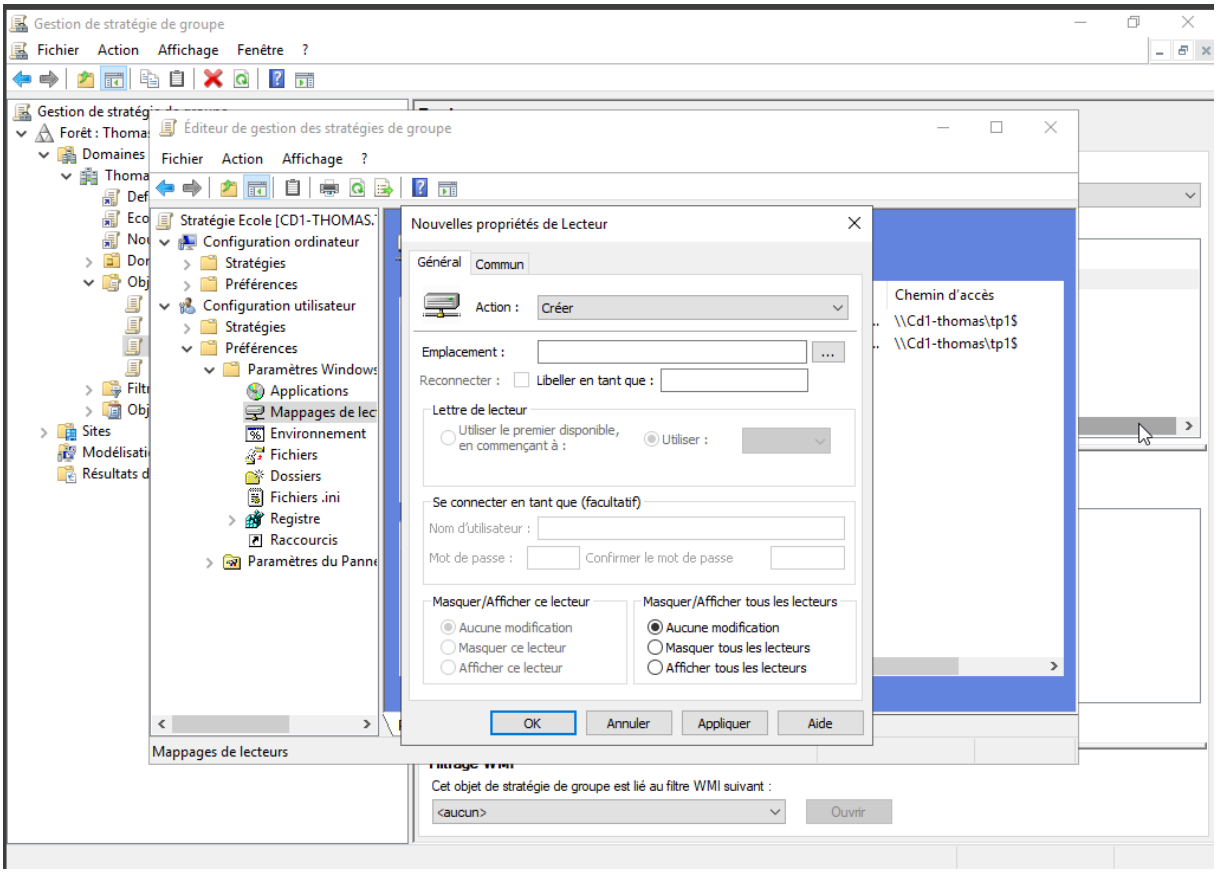
Puis se rendre sur la GPO crée et aller dans les modifications

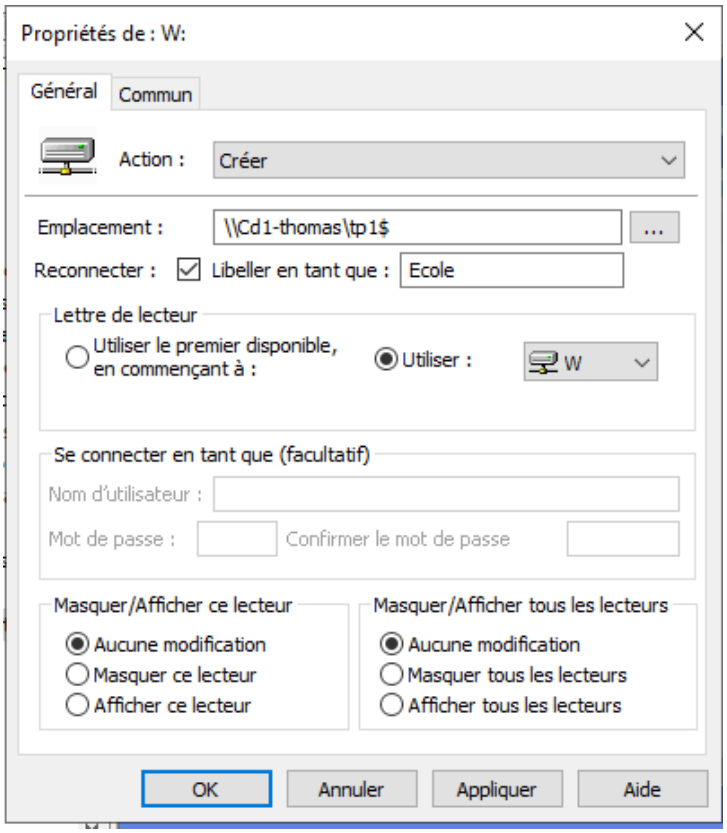
Ouvrir l'arborescence des dossiers Configuration utilisateurs -> Préférences -> Paramètres Windows puis mappage de lecteurs

Il faut ensuite faire nouveau puis lecteur mappé

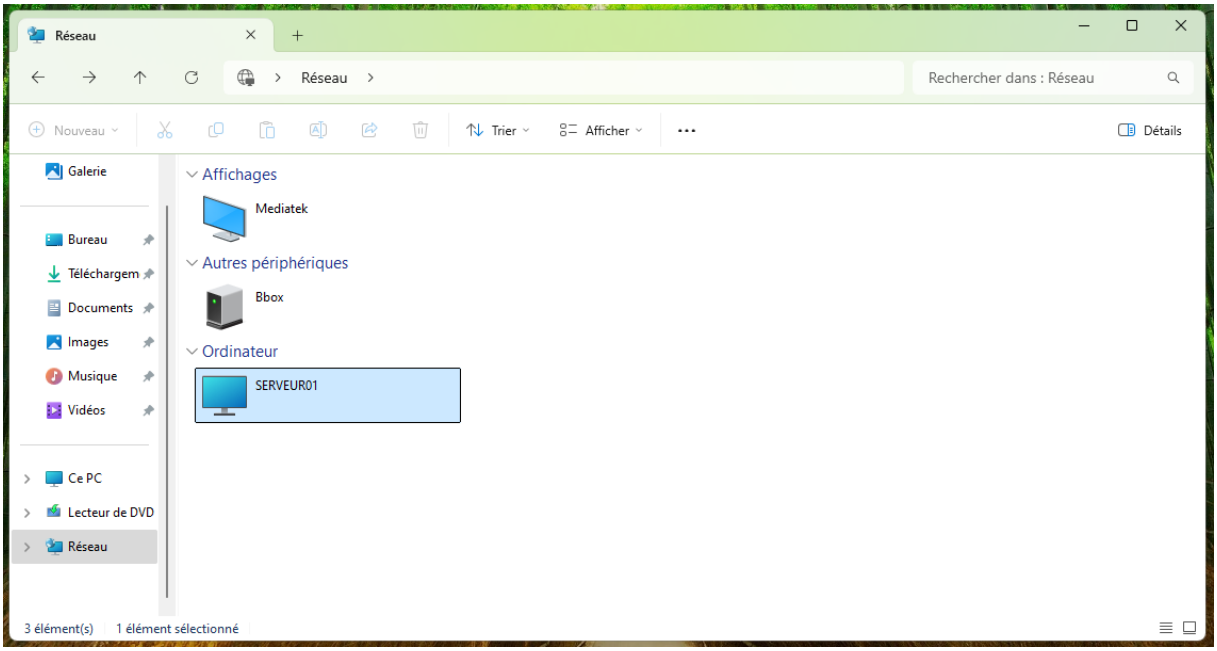
Il faudra ensuite renseigner les champs suivants :

- L'emplacement, correspondant au chemin du dossier choisit
- Un libellé, afin d'identifier clairement le lecteur accompagné de sa lettre, qui ne doit pas être utilisée.
- Sans oublier de cocher reconnecter, pour que l'utilisateur puisse voir le lecteur même après avoir redémarré sa session.





On peut vérifier que tout est fait correctement sur le PC serveur ainsi que sur celui de l'utilisateur si le lecteur réseau apparaît automatiquement à la connexion de la session dans les emplacements réseau du poste.



Tests significatifs :

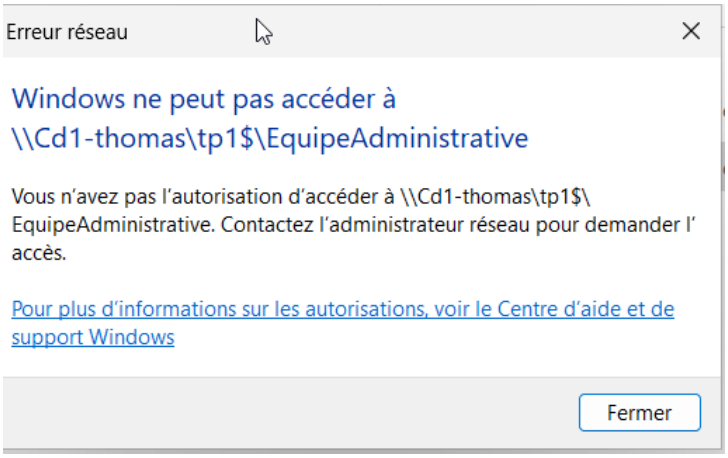
Voici un exemple de la procédure de vérification réalisée avec l'ensemble des utilisateurs :

Connexion avec le compte seb1 élève de la classe A :

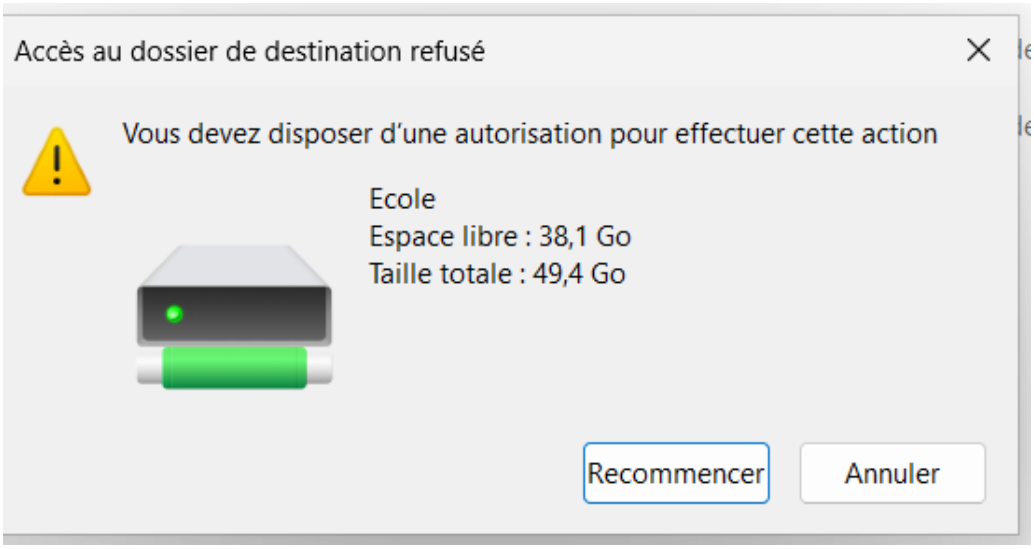
Seb@Thomas.local

Mot de passe :

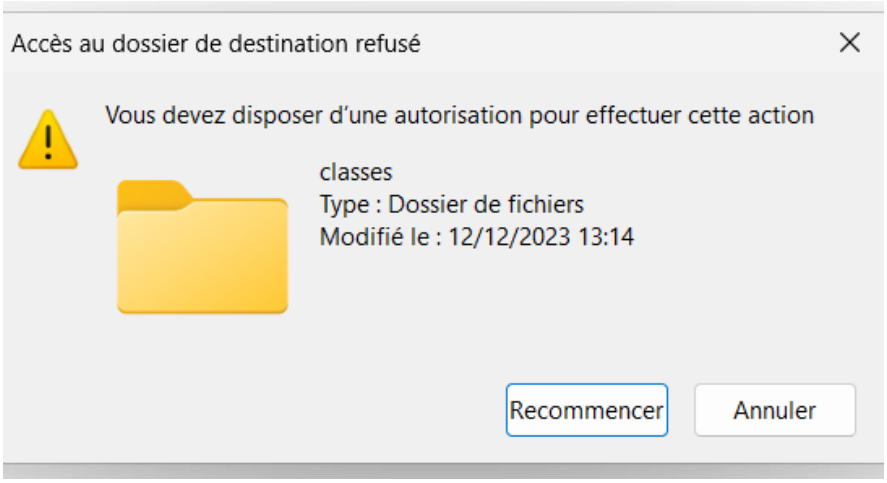
Accès dossier EquipeAdministrative :



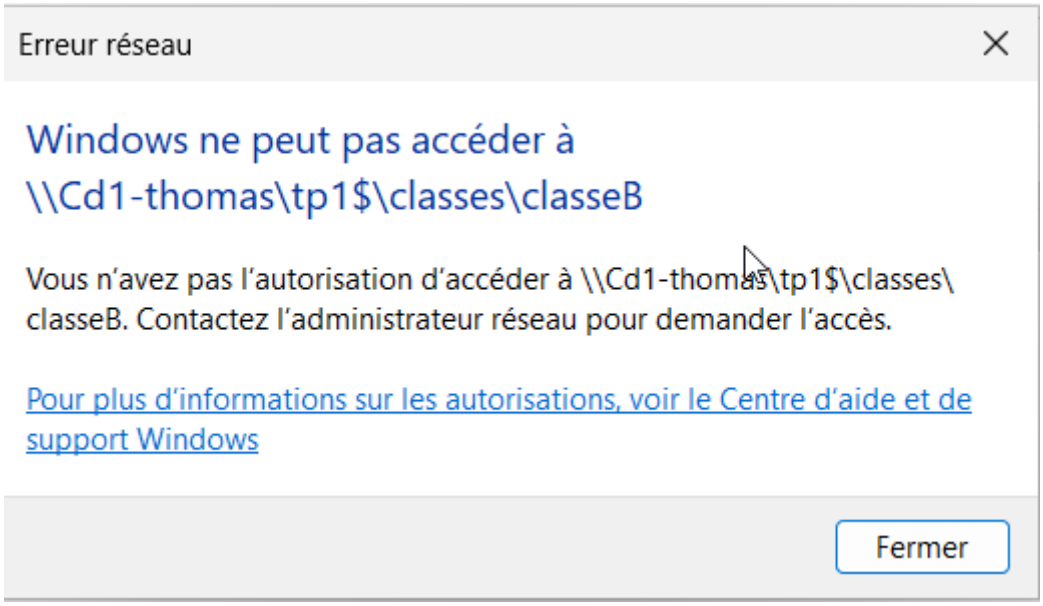
Essaie création d'un dossier dans le dossier TP1



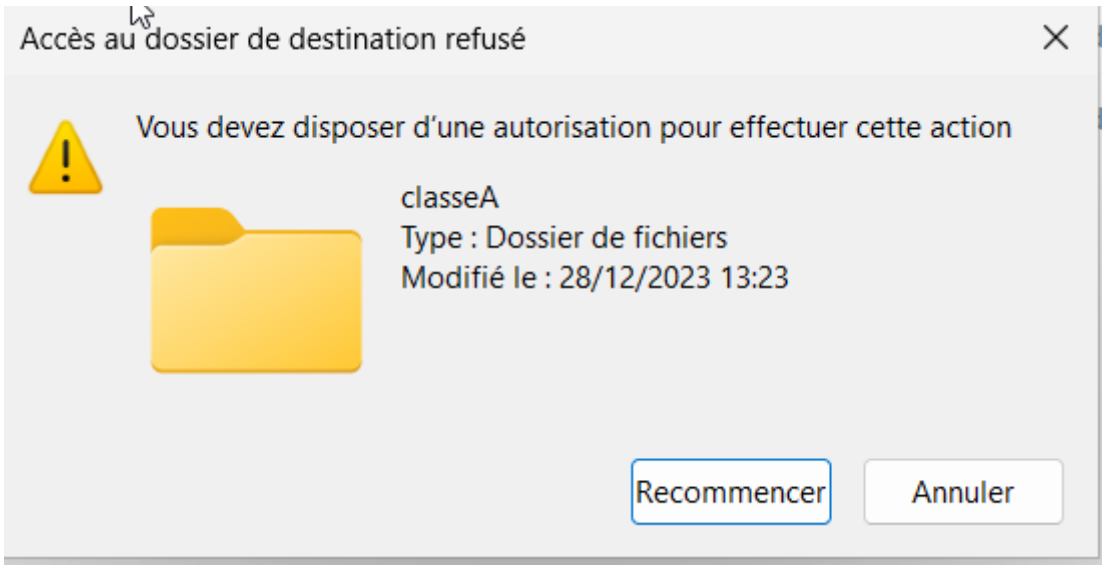
Essaie création d'un dossier dans le dossier classes



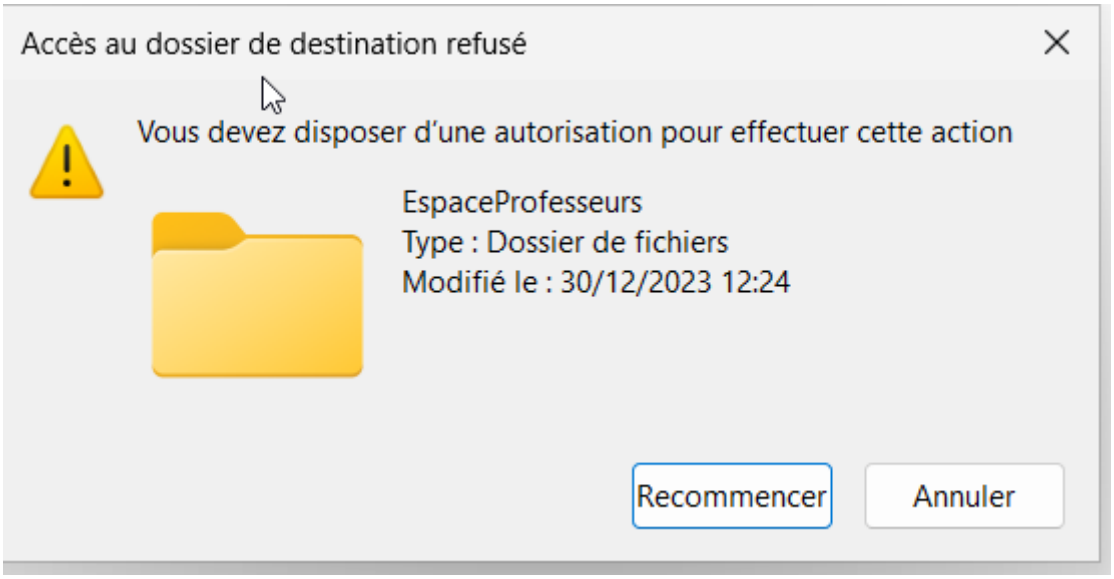
Accès dossier classeB :



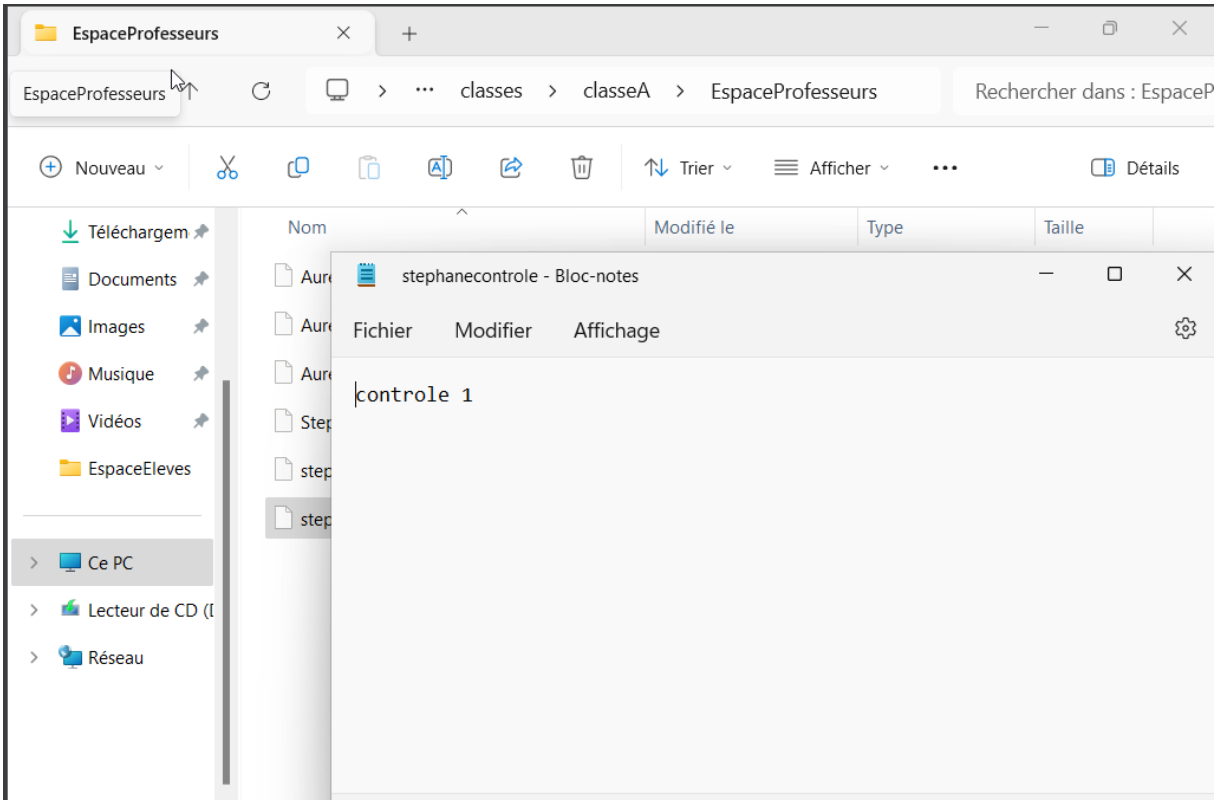
Essaie création d'un dossier dans le dossier classeA



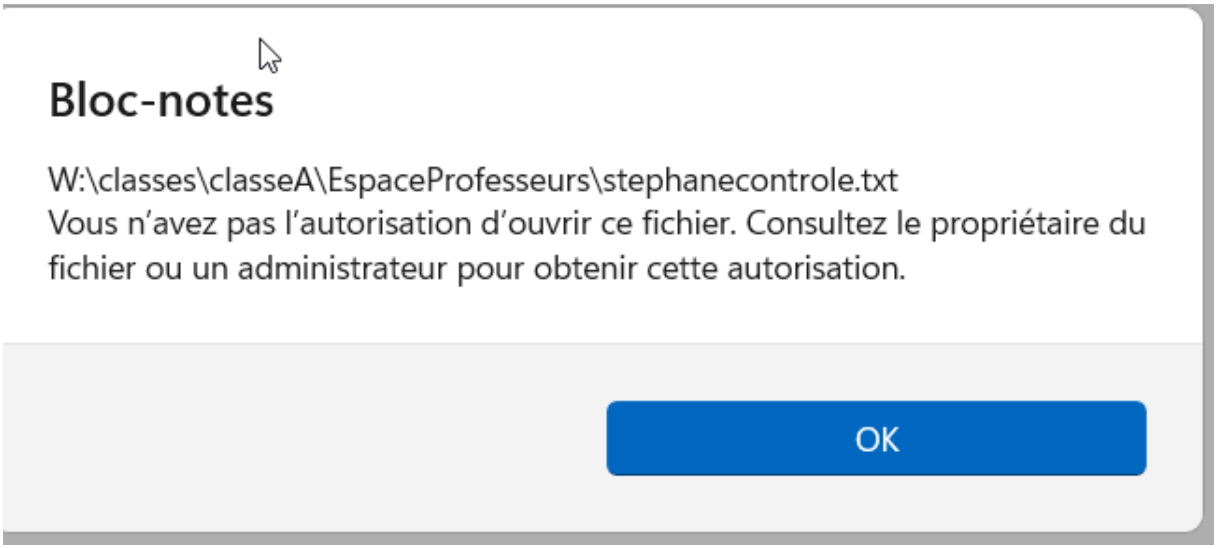
Essaie création d'un dossier dans le dossier EspaceProfesseurs



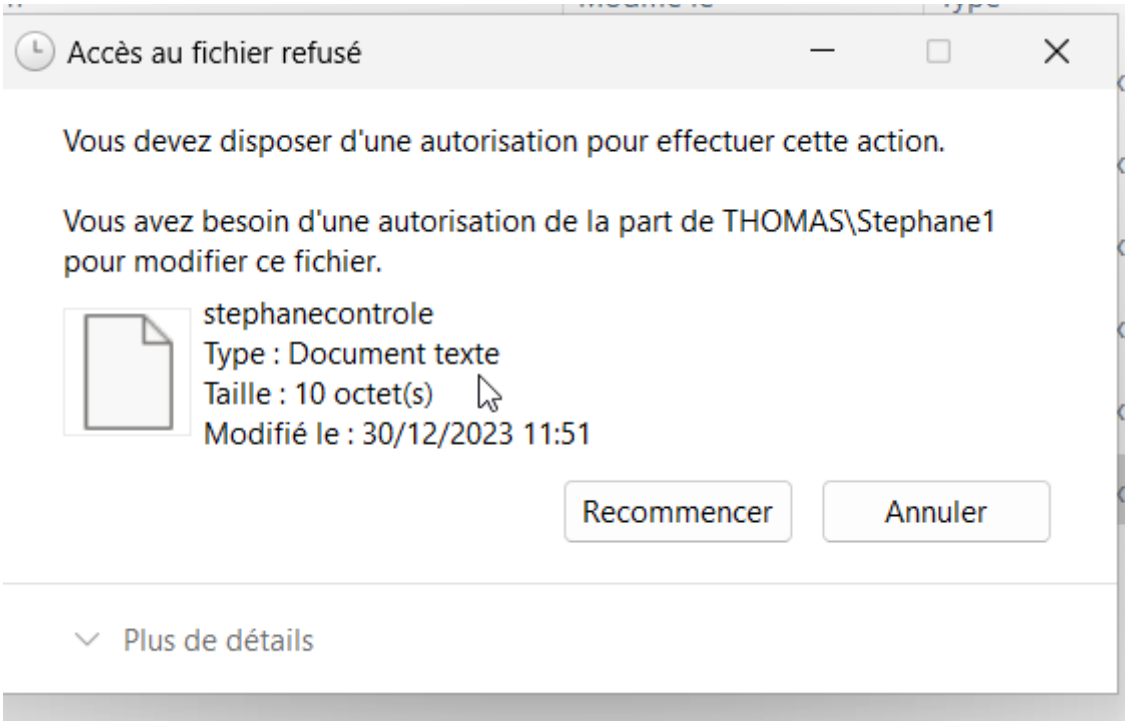
Lecture d’un document créé par un professeurs



Modification du fichier et lorsque l’on veut l’enregistrer impossible, voici le message afficher

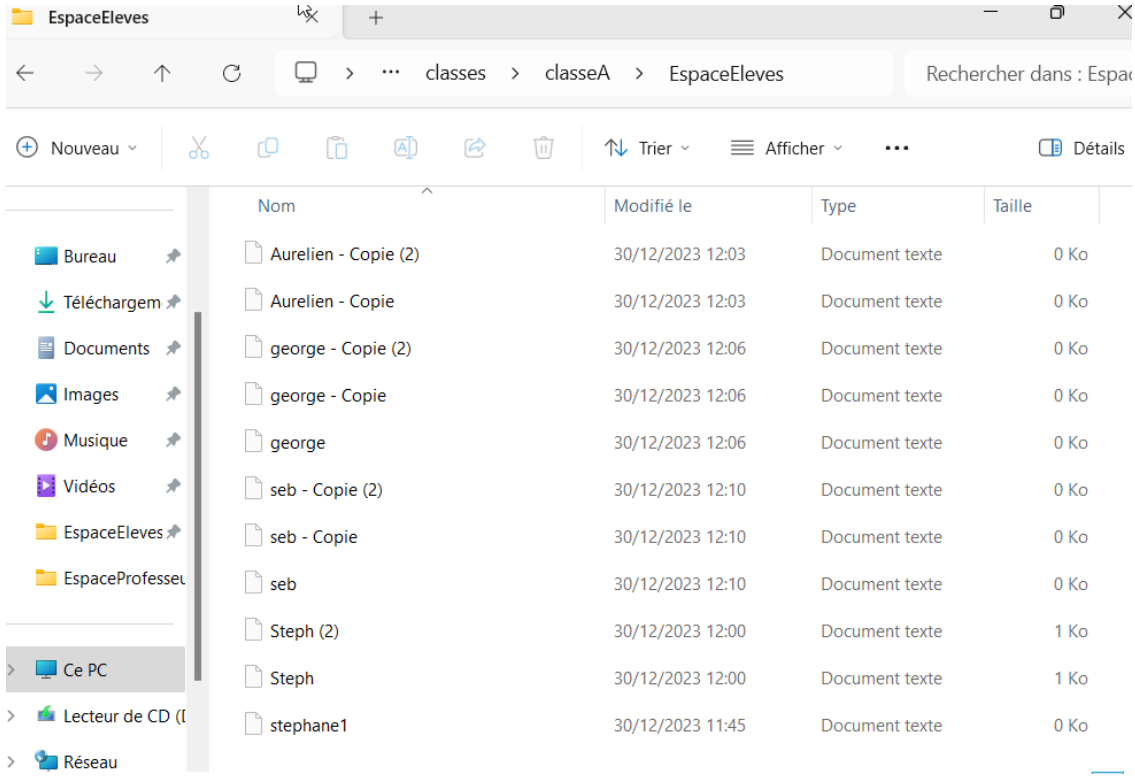


Impossible également de supprimer le fichier

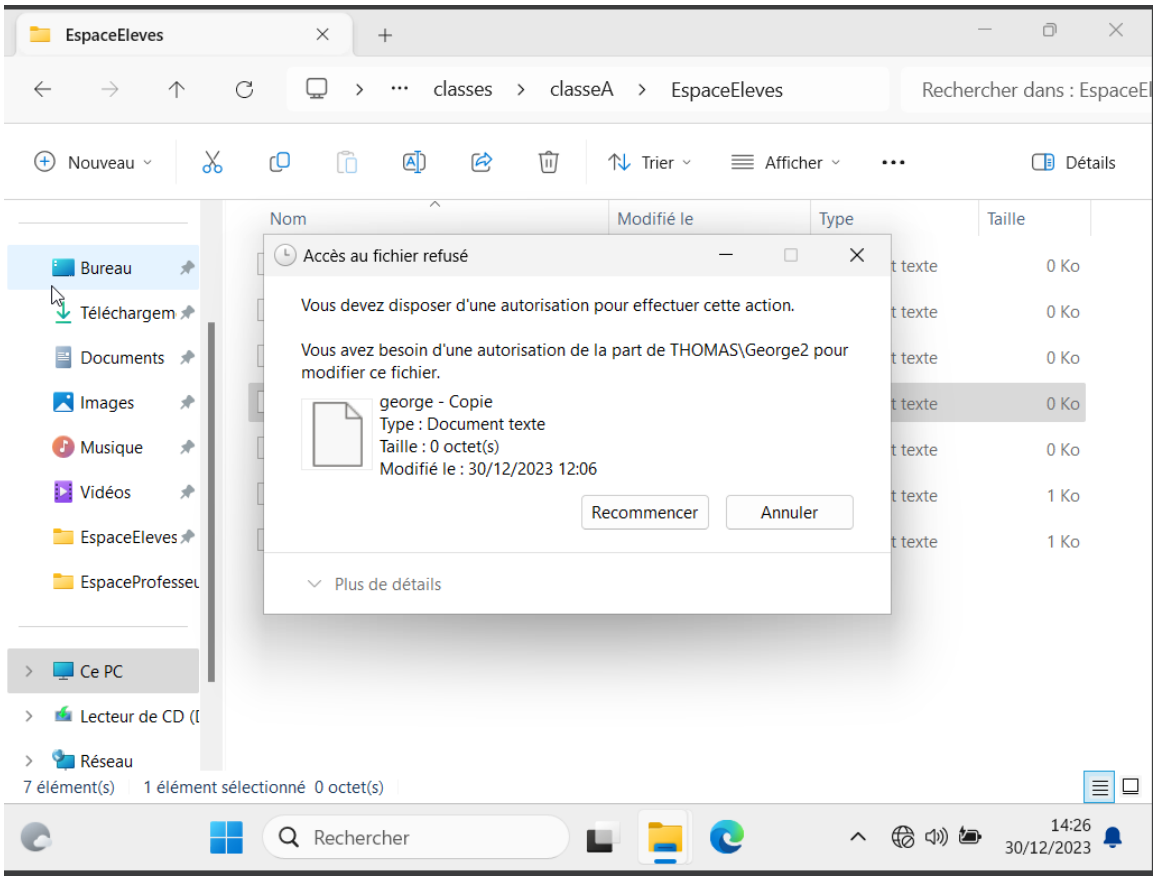


Dans le dossier élève seb1 peut créer, modifier et supprimer ses propres fichiers mais pas ceux des autres, il peut juste les lires.

Les professeurs peuvent également poser des documents dans ce dossier et lire les documents des élèves.



Exemple avec un documents crée par George2 (suppression impossible / ni modification)



Tests réalisés avec tous les utilisateurs afin de bien valider que les différentes contraintes de sécurité du cahier des charges sont respectées.

Et c'est bien le cas ici, on peut donc le déployer !

Conclusion :

Pour restructurer et sécuriser les dossiers partagés sur notre serveur Windows, nous avons suivi une série d'étapes :

- Création d'une nouvelle arborescence de dossiers répondant aux besoins de notre établissement.
- Définition et configuration de groupes d'utilisateurs avec deux comptes par groupe pour garantir un accès approprié.
- Implémentation des mesures de sécurité au niveau du système de fichiers et des paramètres de partage pour contrôler l'accès et les permissions.
- Mise en place d'une méthode de montage automatique des lecteurs réseaux, facilitant l'accès aux ressources partagées.
- Réalisation de tests significatifs pour vérifier que toutes les contraintes de sécurité spécifiées dans le cahier des charges sont respectées.

Nous avons utilisé deux machines virtuelles : une pour héberger le serveur Windows et une autre pour les tests. Les dossiers et groupes d'utilisateurs nécessaires ont été créés, et les mesures de sécurité adaptées ont été appliquées. Enfin, une GPO (Group Policy Object) a été mise en place pour gérer centralement les paramètres de sécurité. Cette approche assure une gestion sécurisée et efficace des dossiers partagés, en conformité avec les exigences de notre établissement.