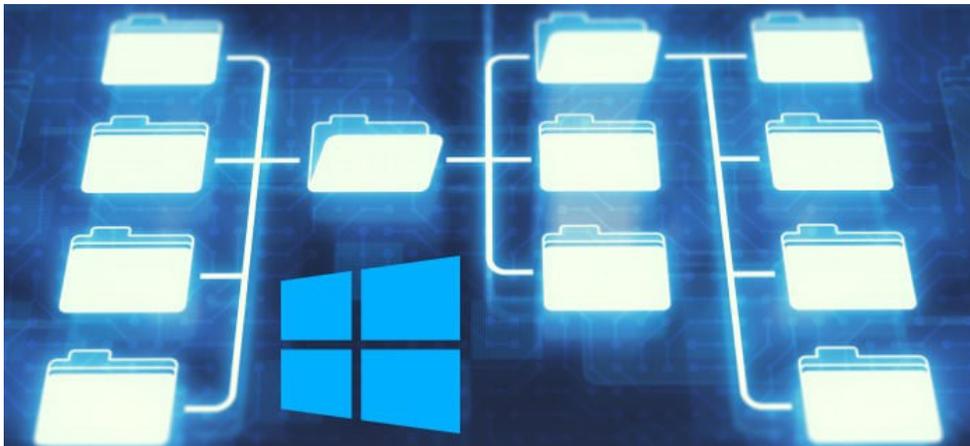


# Sécurisation de fichiers et dossiers sous Windows Server 2016



## SOMMAIRE

<u>1. Cahier des charges.....</u>	<u>3</u>
<u>2. Architecture des dossiers.....</u>	<u>4</u>
<u>3. Contexte.....</u>	<u>5</u>
<u>4. Mise en œuvre.....</u>	<u>6</u>
a) Intégration des clients dans un domaine.....	6
b) Groupes utilisateurs.....	8
c) Création des dossiers partagés.....	12
d) Autorisations.....	15
e) <u>Montage automatique du lecteur réseau.....</u>	<u>23</u>

## 1. Cahier des charges

L'établissement scolaire souhaite restructurer et sécuriser les dossiers partagés sur un serveur Windows.

Plusieurs types d'utilisateurs y auront accès : l'équipe administrative, les formateurs et les élèves.

Chaque groupe d'utilisateurs doit bénéficier de droits particuliers.

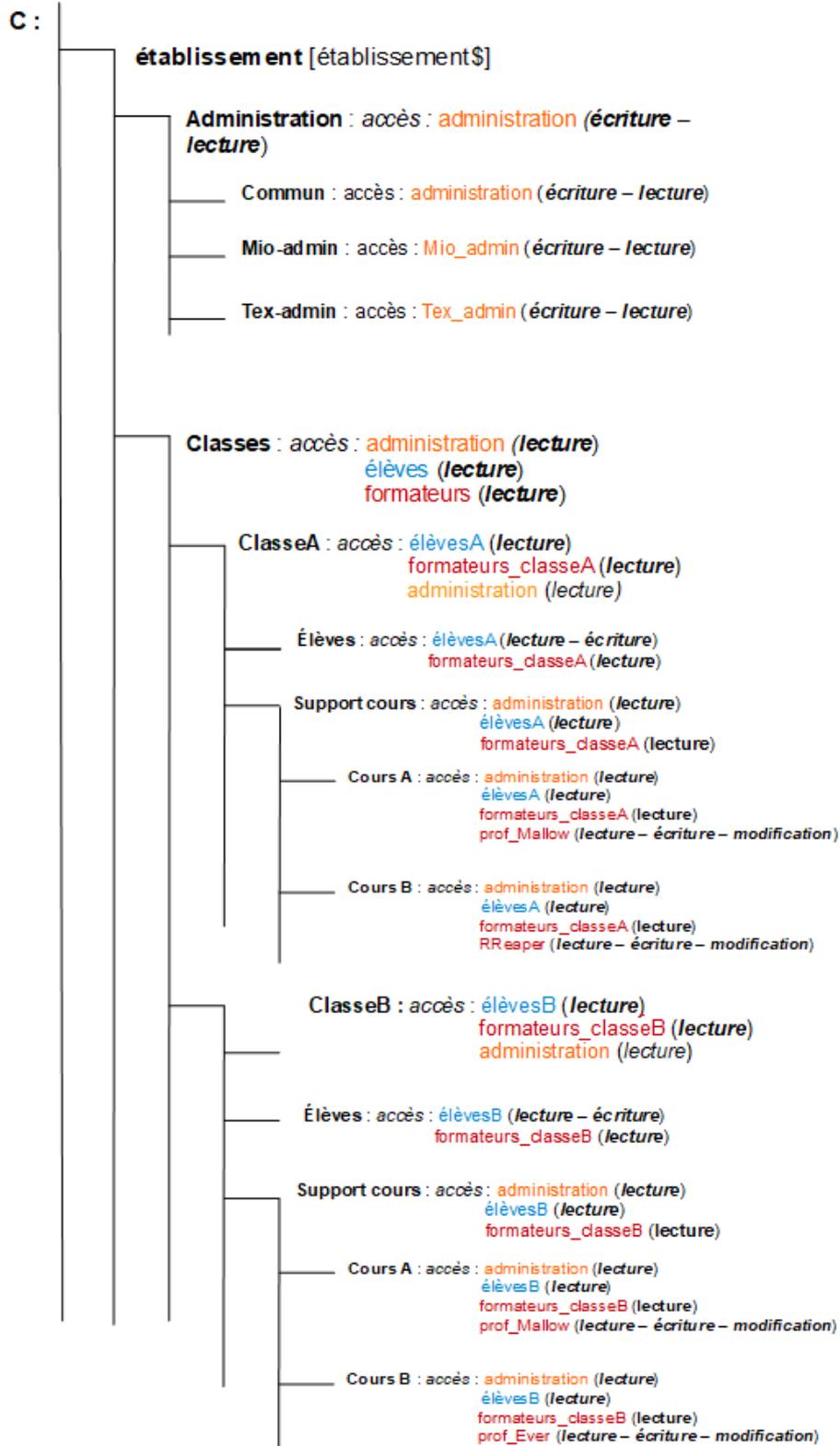
L'équipe administrative a un dossier dédié accessible uniquement à ce groupe. Chaque utilisateur de l'administration doit également posséder un dossier personnel, accessible seulement par lui. L'équipe administrative a aussi un droit de regard sur les supports des formateurs.

Les formateurs sont un deuxième groupe qui ont accès seulement à leurs classes. Ils ont des droits de lecture sur l'espace commun de chaque classe ainsi qu'aux supports d'autres formateurs de celles-ci. Ils possèdent, pour chaque classe dans laquelle ils interviennent, un dossier dans lequel ils peuvent ajouter et modifier du contenu.

Les élèves sont le troisième et dernier groupe d'utilisateur. Ils ont accès à leur dossier classe ainsi qu'aux supports des formateurs qu'ils ont en cours. Ils possèdent des droits d'ajout de documents dans un espace commun classe.

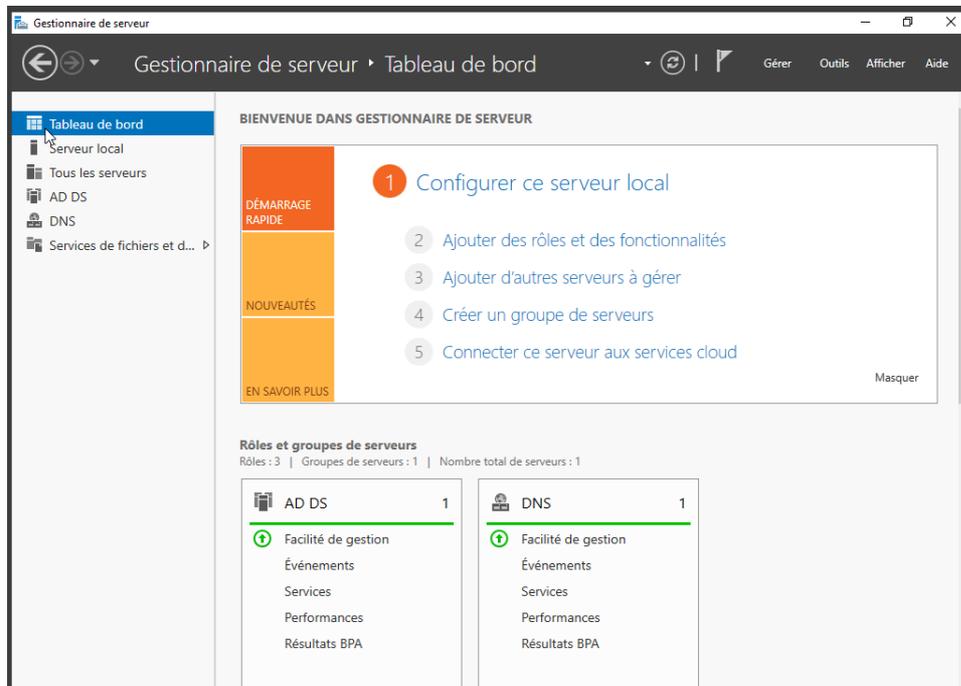
L'établissement souhaite que le montage des lecteurs réseaux soit paramétré pour être automatique.

## 2. Architecture des dossiers



### 3. Contexte

Dans cette situation, le serveur est installé et **Active Directory** est paramétré. Le domaine est nommé **“MIO”**.



Les postes clients sont tous sous Windows 10.

Nous commencerons par intégrer les clients dans le domaine puis créerons des utilisateurs et des dossiers partagés. Enfin nous attribuerons des autorisations aux utilisateurs pour les accès aux dossiers de l'établissement.

## 4. Mise en œuvre

### a) Intégration des clients dans un domaine

Nous renommons les différents PC clients.

#### Spécifications de l'appareil

Nom de l'appareil	Mallow
Nom complet de l'appareil	Mallow.mio.local
Processeur	11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz 2.42 GHz
Mémoire RAM installée	2,30 Go
ID de périphérique	AB5C276F- C83F-488C-969E-496865803F77
ID de produit	00330-80000-00000-AA722
Type du système	Système d'exploitation 32 bits, processeur x86
Stylet et fonction tactile	La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran

Copier

Renommer ce PC

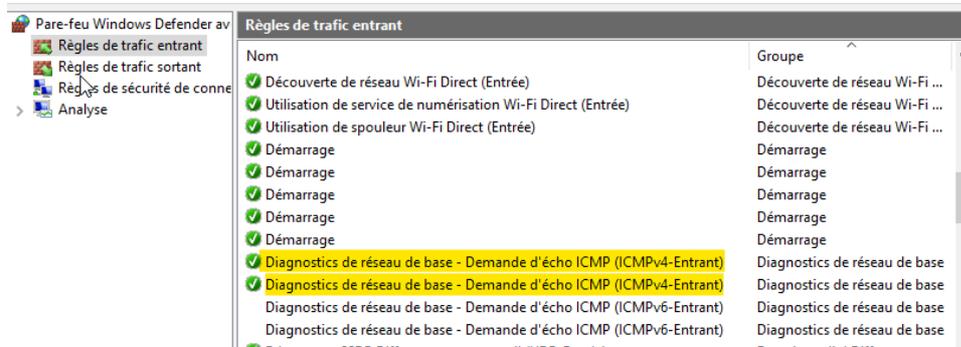
Puis, nous fixons les adresses IP afin que le client et serveur soient dans le même réseau.

The screenshot shows the Windows network settings interface. The main window is titled 'Modifier les paramètres IP' (Modify IP settings) for a network named 'Réseau non identifié'. The 'Manuel' (Manual) option is selected. The IPv4 settings are as follows:

- IPV4:  Activé
- Adresse IP: 192.168.10.2
- Longueur du préfixe de sous-réseau: 24
- Passerelle: 192.168.10.254
- DNS préféré: 192.168.10.1
- Autre DNS: (empty)

Buttons for 'Enregistrer' (Save) and 'Annuler' (Cancel) are visible at the bottom of the settings pane. The left sidebar shows the 'Paramètres' (Settings) menu with 'Réseau' (Network) selected.

Nous vérifions que le protocole ICMP IPV4 n'est pas bloqué par le parefeu. Les lignes **“Diagnostic de réseau de base - Demande d'écho ICMP (ICMPv4-Entrant)”** n'étaient pas en **“autoriser”**, nous les changeons donc d'état.



Arrivés à cette étape, avant de continuer, nous vérifions que le poste client et le serveur communiquent.

Pour cela, dans le terminal nous effectuons une requête **“ping”**. Nous faisons cette procédure sur le client en contactant le serveur puis du serveur vers le client.

- Vérification de communication entre poste client et serveur :

```
Microsoft Windows [version 10.0.19045.2364]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\sio2>ping 192.168.10.1

Envoi d'une requête 'Ping' 192.168.10.1 avec 32 octets de données :
Réponse de 192.168.10.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.10.1 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.10.1 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.10.1 : octets=32 temps=1 ms TTL=128

Statistiques Ping pour 192.168.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

--> ils communiquent

- Vérification de communication entre le serveur et le poste client :

```
Microsoft Windows [version 10.0.14393]
(c) 2016 Microsoft Corporation. Tous droits réservés.

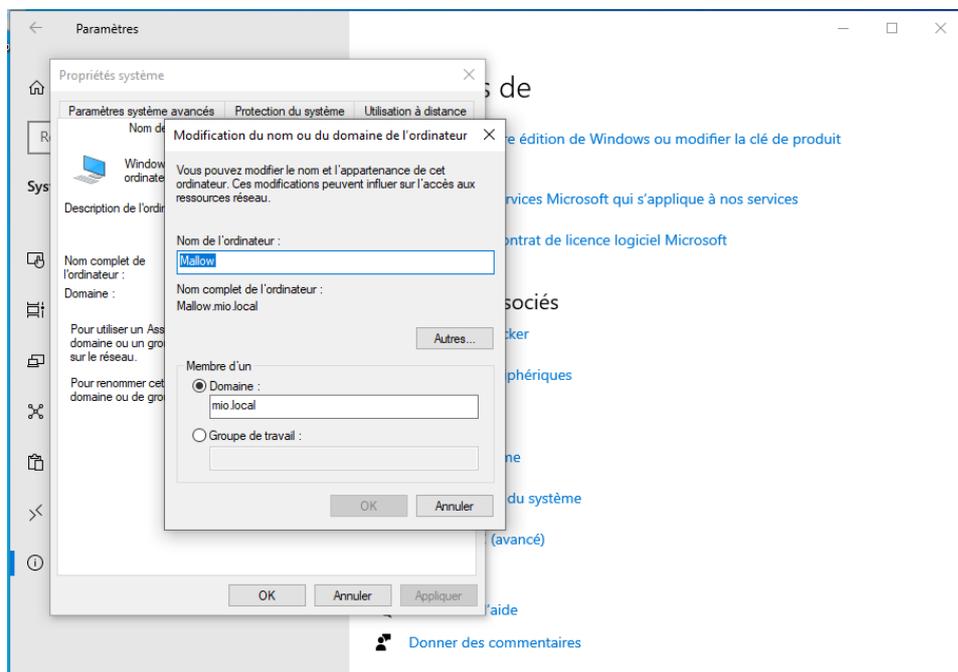
C:\Users\administrateur.MIO>ping 192.168.10.2

Envoi d'une requête 'Ping' 192.168.10.2 avec 32 octets de données :
Réponse de 192.168.10.2 : octets=32 temps=6 ms TTL=128
Réponse de 192.168.10.2 : octets=32 temps=4 ms TTL=128
Réponse de 192.168.10.2 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.10.2 : octets=32 temps=1 ms TTL=128

Statistiques Ping pour 192.168.10.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 6ms, Moyenne = 3ms
```

--> ils communiquent

Enfin nous intégrons le poste dans le domaine Windows **MIO**.



Nous avons fini d'intégrer le poste client au serveur et au domaine AD DS.

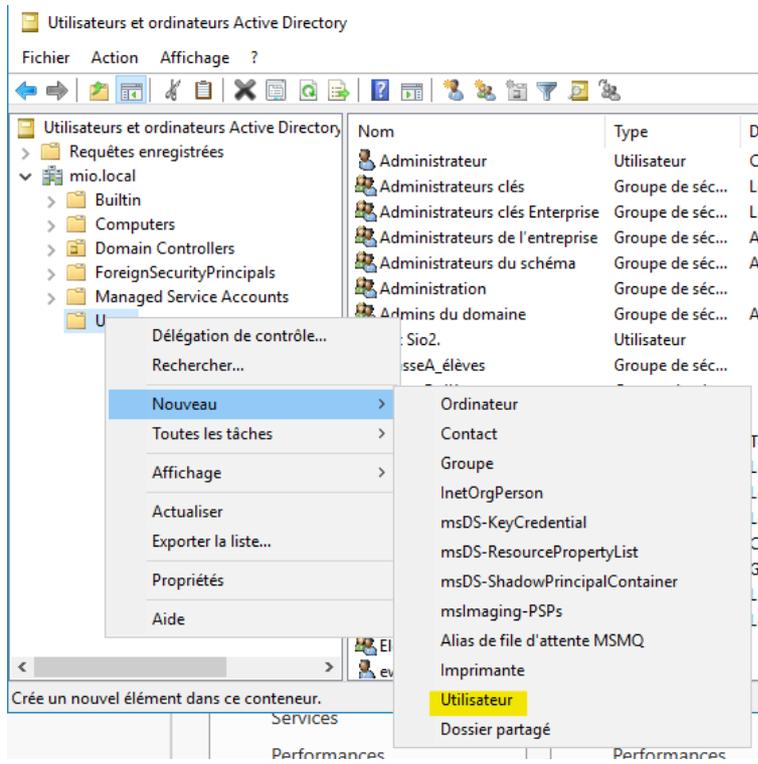
Nous allons créer quelques utilisateurs puis prendre un de ces derniers et vérifier si l'intégration du poste client dans le domaine est valide.

### ***b) Groupes utilisateurs***

Nous revenons sur notre poste serveur et dans notre gestionnaire serveur nous allons commencer à créer des utilisateurs pour le domaine MIO.

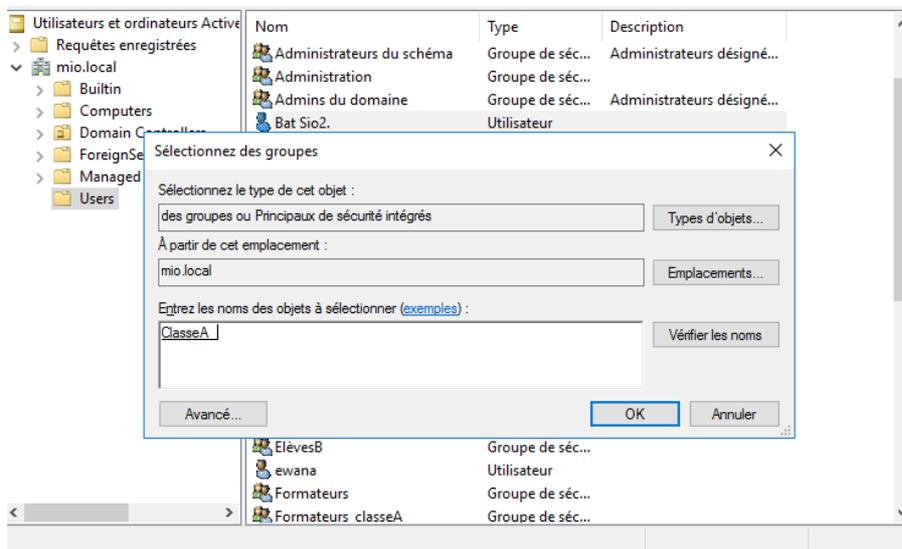
Nous allons dans "Outils", "Utilisateurs et ordinateurs Active Directory".

## Création d'un utilisateur :

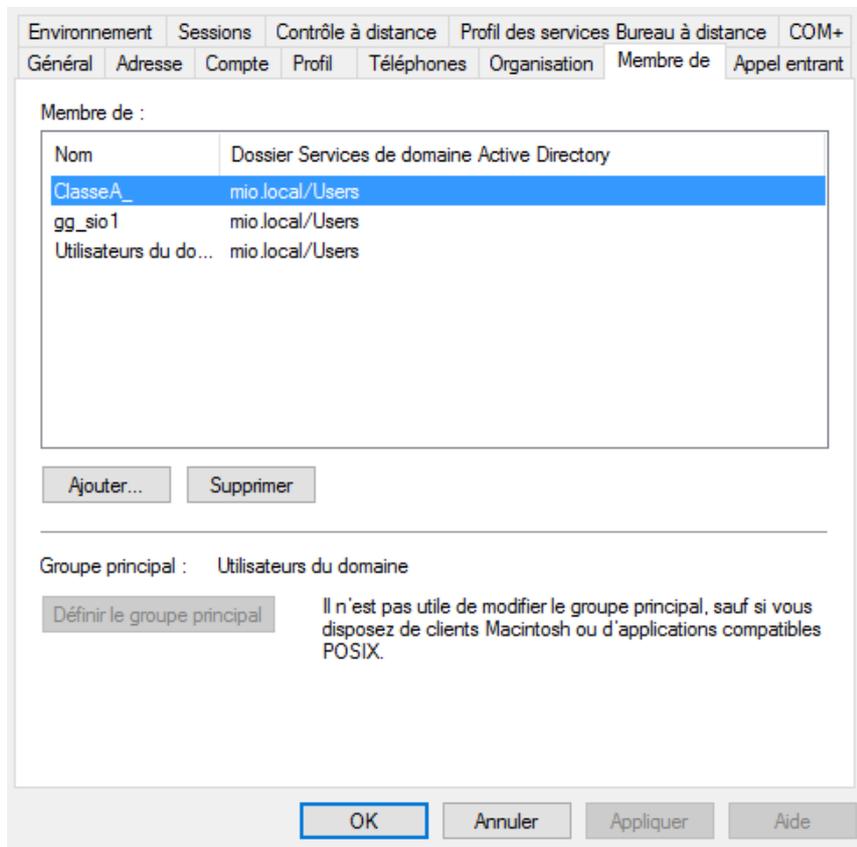


Il va y avoir des utilisateurs **formateurs**, des utilisateurs **élèves** et des utilisateurs de **l'administration**. Nous allons donc commencer à créer des groupes et y associer des utilisateurs.

Pour créer un groupe, il faut passer par le même chemin que pour un utilisateur. Il s'agit seulement de cliquer sur "**Groupe**" au lieu d'"**Utilisateur**" dans "**Nouveau**". Ensuite, nous allons ajouter des utilisateurs à un groupe. Pour cela, nous cliquons droit sur l'utilisateur : "**Ajouter à un groupe**". Nous entrons le nom du groupe.

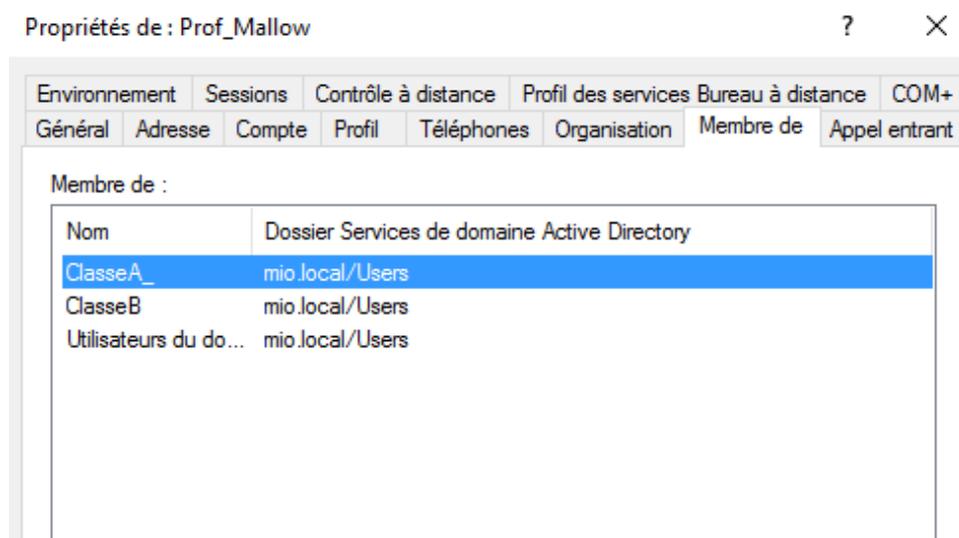


- Pour vérifier si l'utilisateur est dans un groupe donné, nous cliquons droit sur ce dernier : "Propriétés", onglet "membre de".



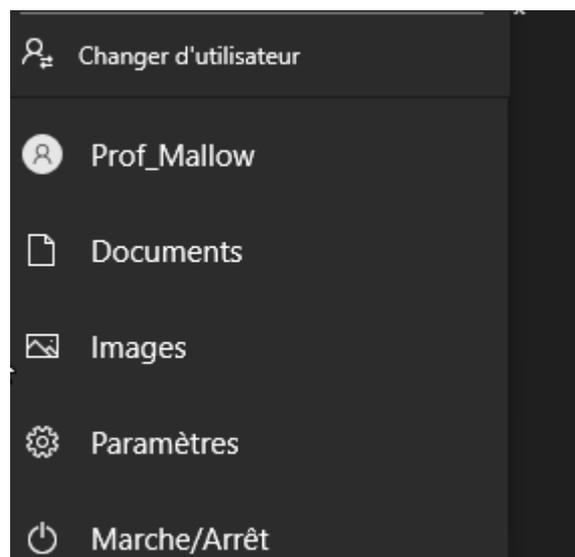
L'utilisateur élève "Bat" a bien été ajoutée au groupe "ClasseA\_"

- Certains utilisateurs sont associés à plusieurs classes comme les professeurs. Ils sont donc présents dans plusieurs groupes.



- Pour vérifier que les utilisateurs sont bien actifs et que le poste client est bien associé au domaine **MIO**, nous ouvrons une nouvelle session au nom d'un des utilisateurs, ici **Prof\_Mallow**.

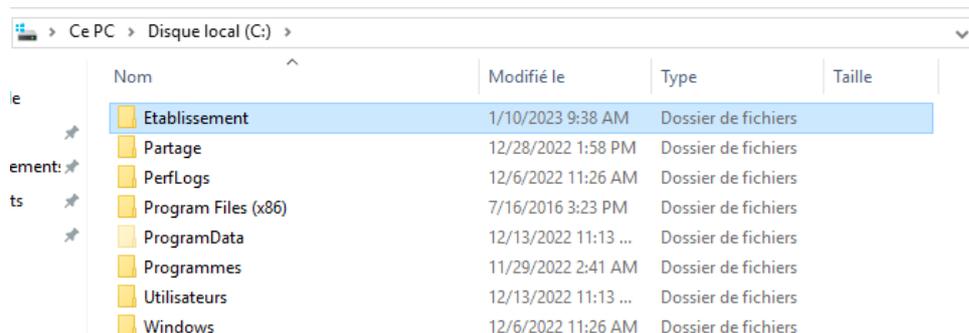
Nous avons pu nous connecter à sa session utilisateur. Nous pouvons donc en conclure que le poste client est bien lié au domaine et que l'utilisateur a été correctement ajouté.



### c) Création des dossiers partagés

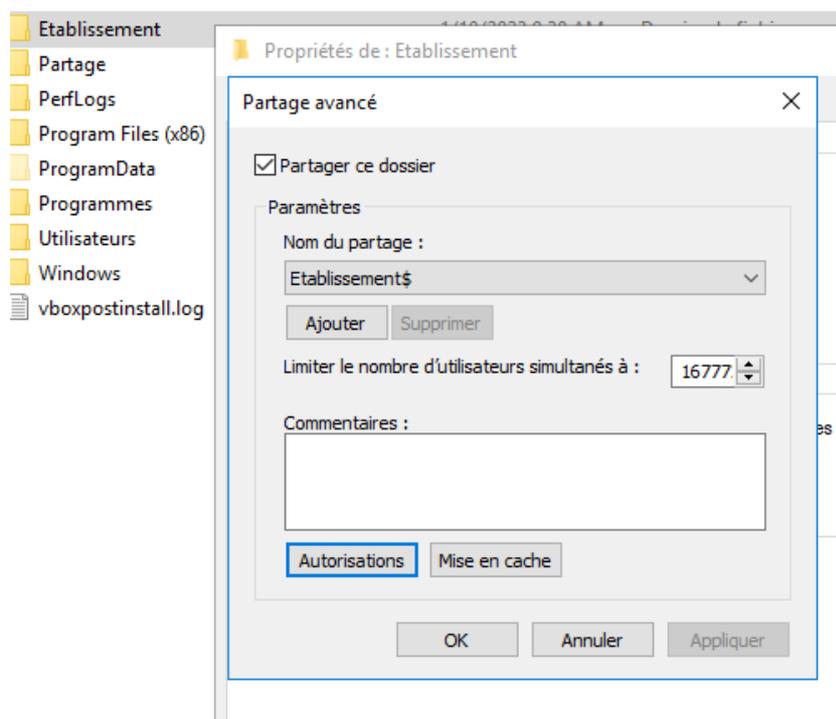
À présent que nous avons créé des utilisateurs et groupes d'utilisateurs, nous allons ajouter des dossiers que nous partagerons avec l'ensemble des utilisateurs. Dans le point suivant, nous nous concentrerons sur les droits d'accès à ces dossiers.

Nous créons tout d'abord un dossier "établissement" dans le **disque local C** de notre serveur :

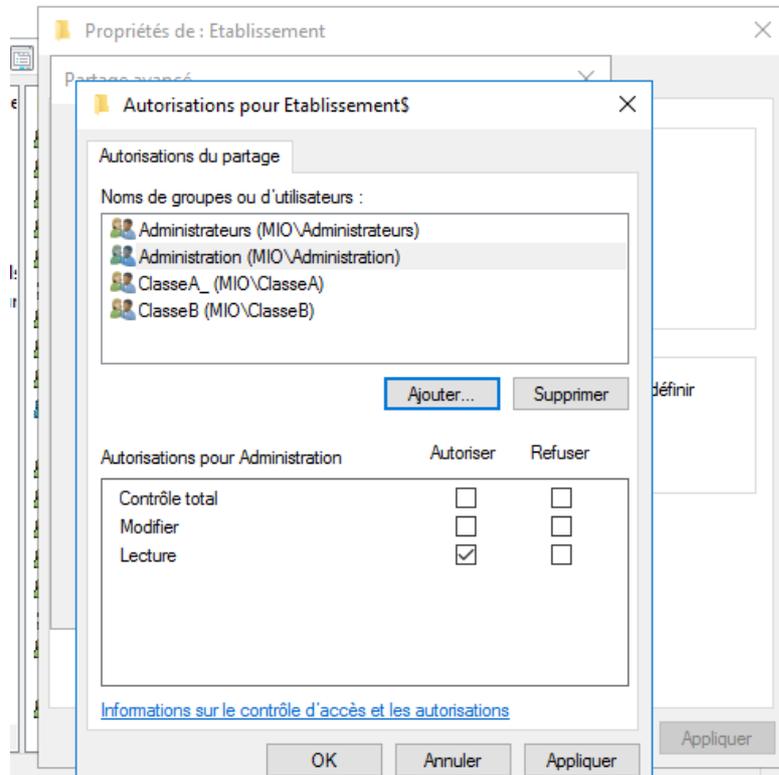


Ensuite, nous cliquons droit dessus, "Propriétés", onglet "Partage".

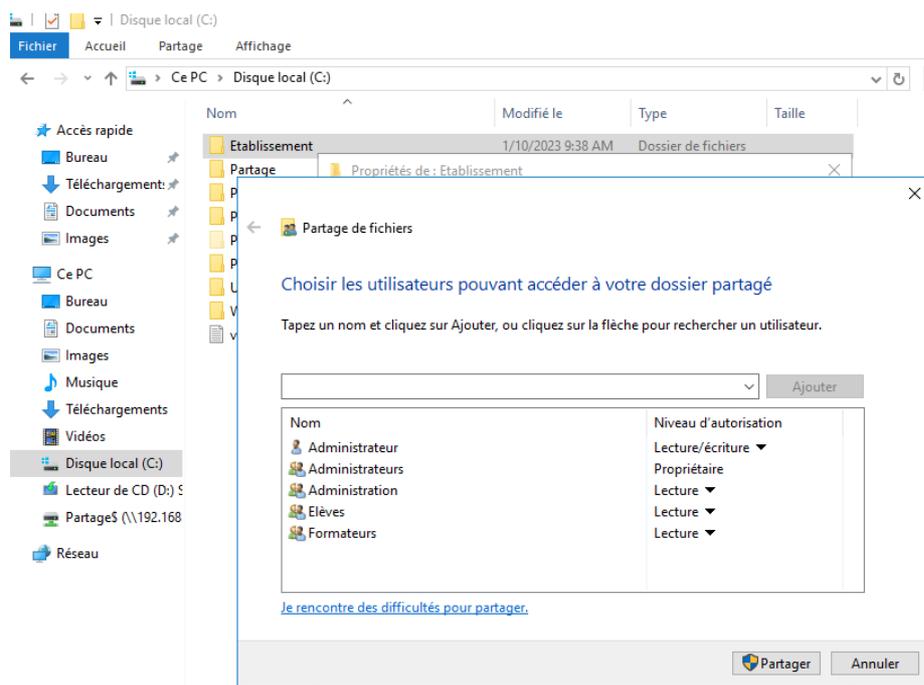
Sur cette fenêtre, nous cliquons sur "Partage avancé". Nous cochons "Partager ce dossier". Nous nommons le partage "Etablissement\$".



Nous cliquons ensuite sur “*Autorisations*” puis rajoutons les groupes de l’établissement. Seuls les administrateurs ont les autorisations “**modifier**” et “**contrôle total**”.

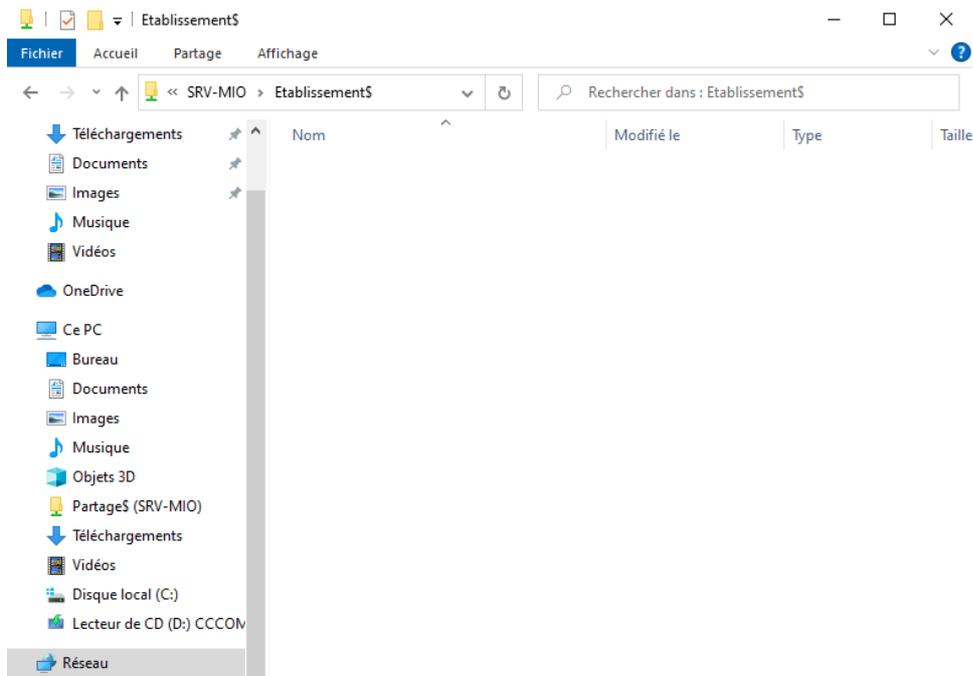


Nous retournons sur la fenêtre précédente (“*Partage*”) et allons dans “*partager*”. Nous ajoutons les groupes qui vont être dans l’établissement.

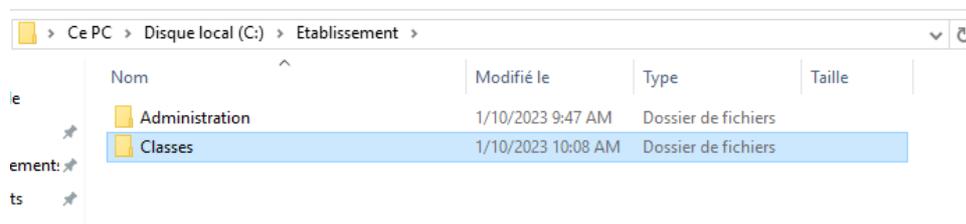


- Pour voir que le dossier a bien été partagé aux utilisateurs concernés, nous nous rendons sur 2 sessions différentes et vérifions que nous trouvons ce dossier.

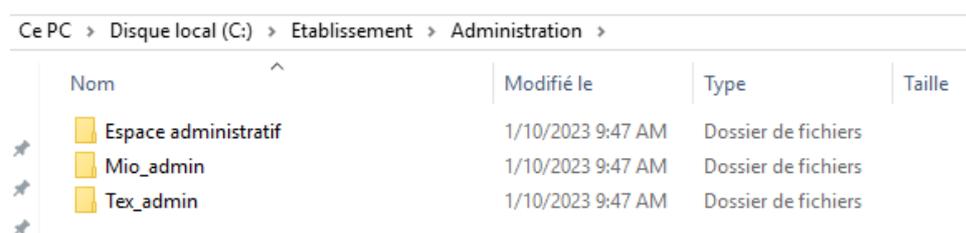
**PROF MALLOW** et **TSUBAKI** (élève classe A) --> ok



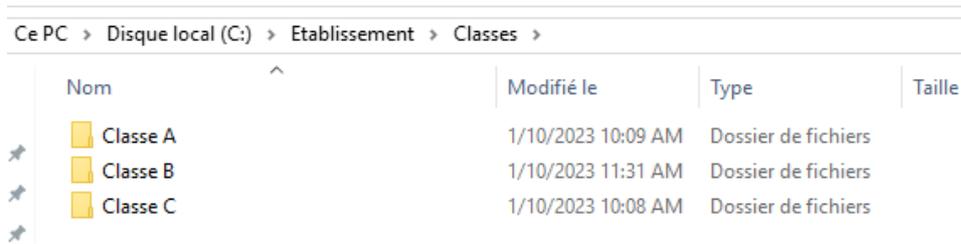
Nous avons terminé de partager le dossier “**Etablissement**”. A partir de maintenant, nous allons concevoir les sous-dossiers de la structure.



Dans “**Administration**” :

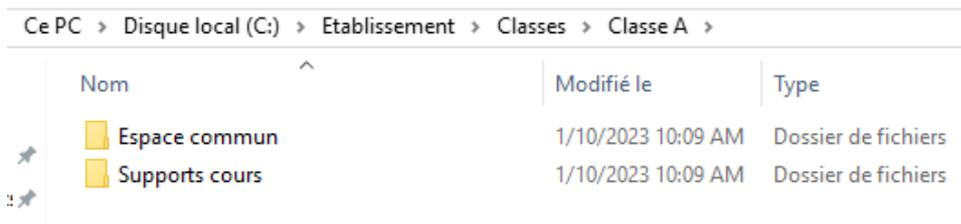


Classes” :



Nom	Modifié le	Type	Taille
Classe A	1/10/2023 10:09 AM	Dossier de fichiers	
Classe B	1/10/2023 11:31 AM	Dossier de fichiers	
Classe C	1/10/2023 10:08 AM	Dossier de fichiers	

Enfin dans une des classes (l'organisation est similaire pour toutes les classes) :



Nom	Modifié le	Type
Espace commun	1/10/2023 10:09 AM	Dossier de fichiers
Supports cours	1/10/2023 10:09 AM	Dossier de fichiers

Sur la session **Prof\_Mallow**, l'utilisateur voit et accède à tous les dossiers.

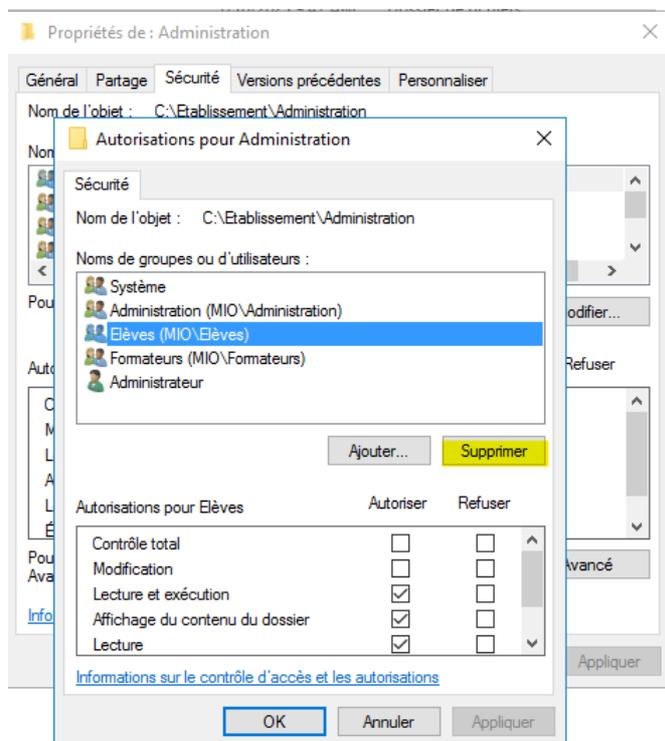
Cependant, pour respecter le cahier des charges, nous allons donner des autorisations spécifiques pour chaque groupe d'utilisateur.

#### **d) Autorisations**

Sur le serveur, nous allons attribuer des autorisations aux différents sous-dossiers d'”**Etablissement**”.

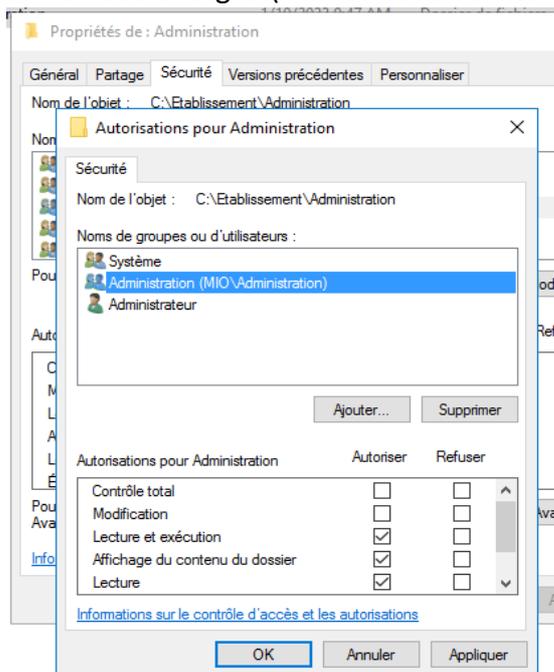
Prenons le sous-dossier “**Administration**”. Selon le cahier de charges, seuls les utilisateurs de l'administration ont accès à ce dossier.

Nous cliquons droit sur le dossier, “*Propriétés*”, onglet “*Sécurité*”, “*Avancé*”.  
 Nous **désactivons l’héritage** pour pouvoir modifier, supprimer des autorisations.

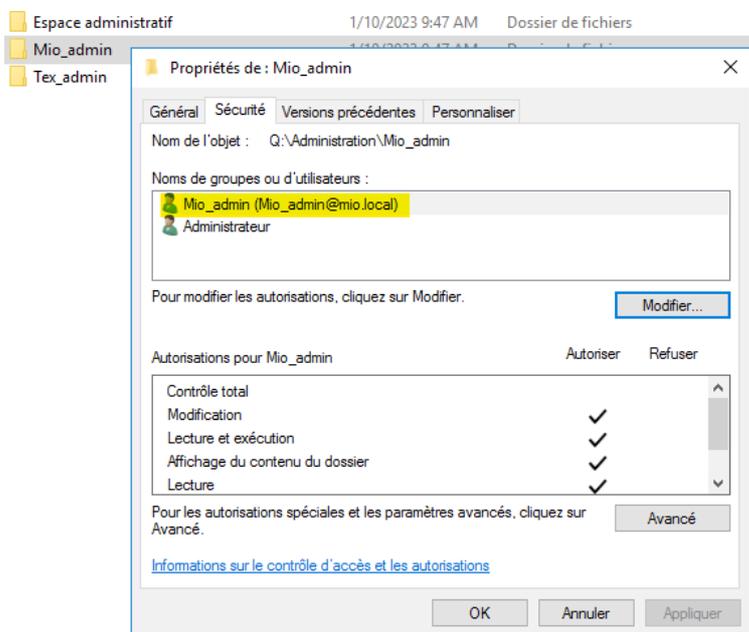


Après, dans “*Sécurité*”, “*Modifier*”, nous supprimons les groupes non autorisés.

Pour les groupes restants, nous vérifions les autorisations et ajustons au besoin selon le cahier des charges (cf ***Architecture des dossiers***)

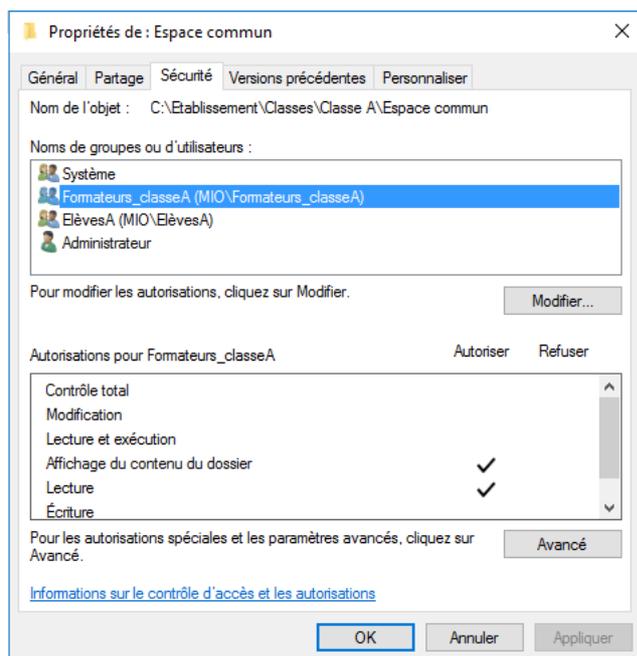


personne de l'administration a le droit à un espace personnel. Nous avons donc créé un dossier pour chaque utilisateur de l'administration et nous avons ajouté des **droits d'accès, d'écriture et de modification** seulement à la personne concernée.

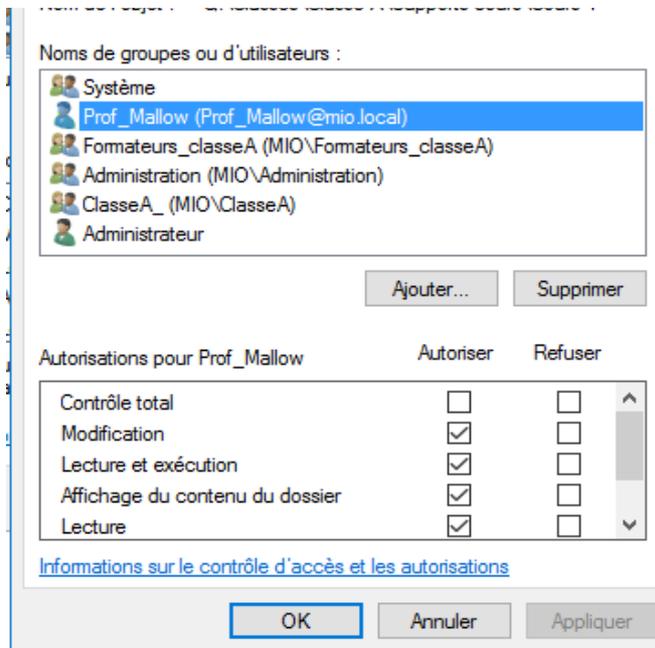


Dans les 2 classes, pour le dossier “**Espace commun**”, nous avons créé, sur le gestionnaire de serveur, des groupes formateurs pour chaque classe (ex : “**Formateurs\_classeA**”).

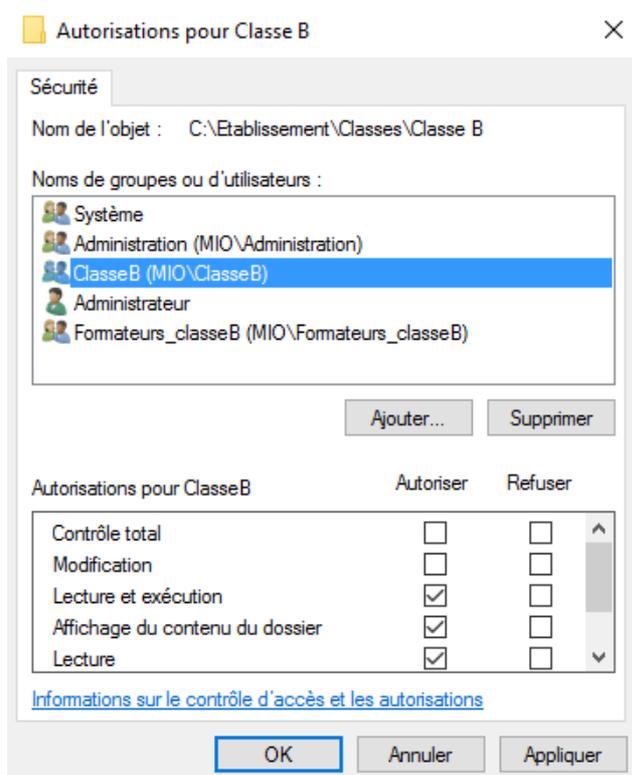
Les utilisateurs présents dans ce groupe auront les autorisations de **lecture** dans ce sous-dossier afin de visualiser et enregistrer les fichiers dont ils ont besoin.



r les dossiers des enseignants “**CoursA**”, “**CoursB**”, nous rajoutons des autorisations pour l’enseignant concerné : **écriture + modification**. En effet, nous partons du principe que chaque formateur peut ajouter ou supprimer des documents dans le dossier de son cours.



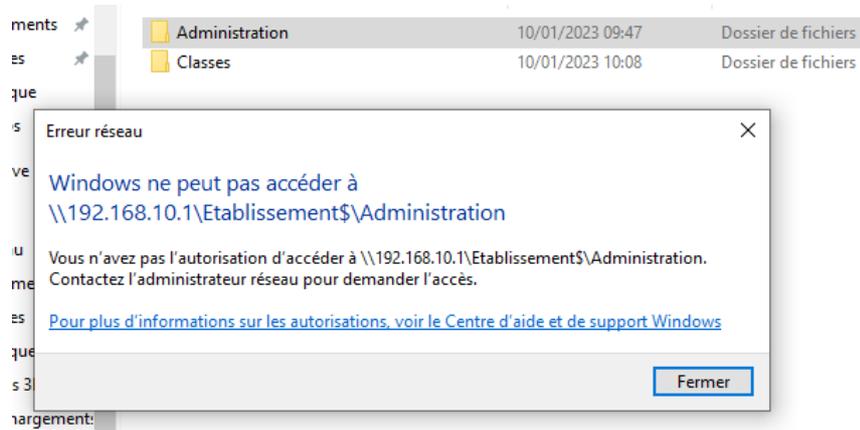
Les **élèves** ont accès seulement aux dossiers de leur classe.



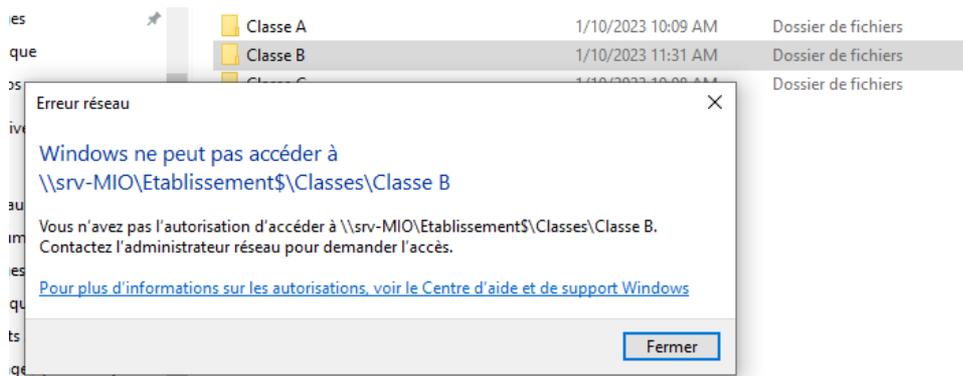
Après avoir paramétré les autorisations, nous vérifions qu'elles sont bien prises en compte chez divers utilisateurs.

- **Tsubaki** : élève de la classe A

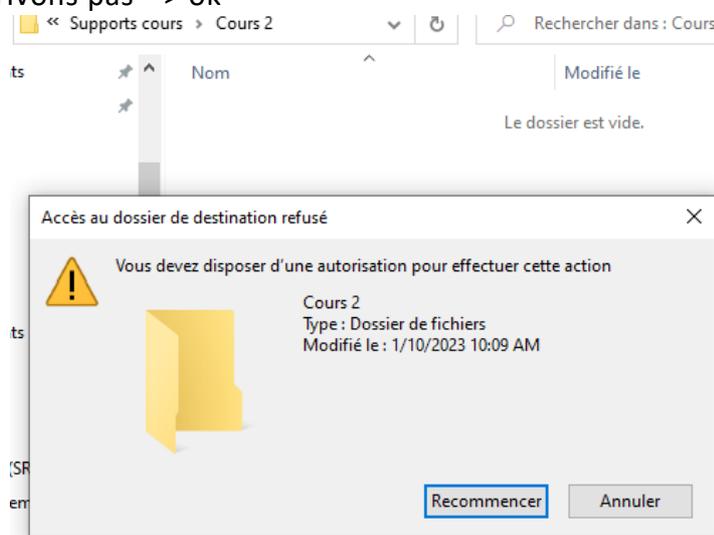
Accès à l'administration refusé --> ok



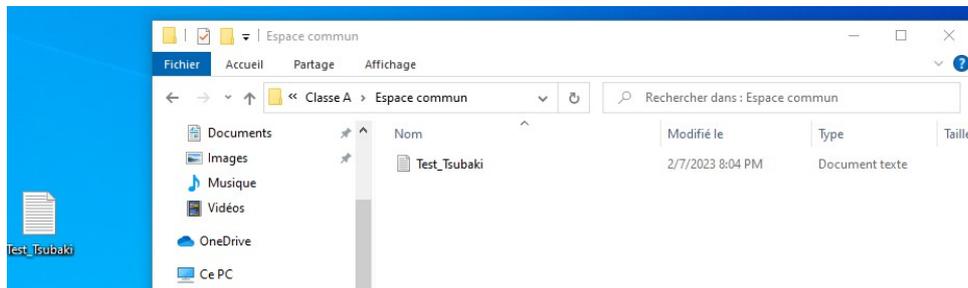
Nous tentons d'aller sur la classe B, nous n'y arrivons pas --> ok



Nous essayons de créer un fichier dans le cours 2 de la classe A, nous n'y arrivons pas --> ok

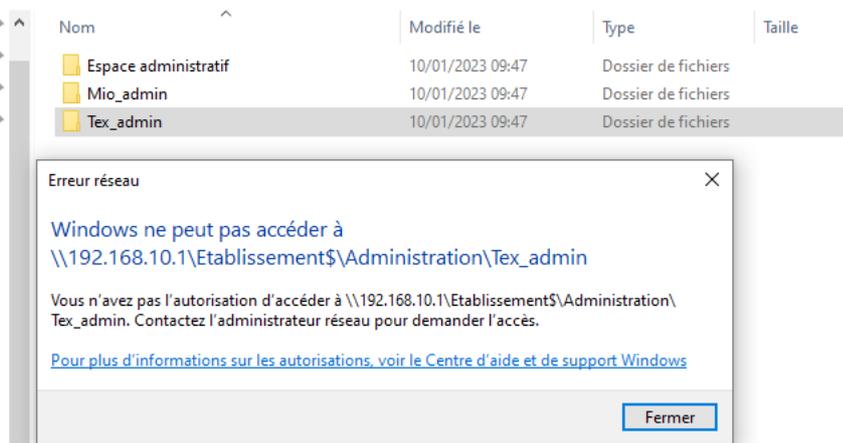


ans l'espace commun de la classe A, nous avons tenté d'ajouter un document créé par **Tsubaki** sur sa session. Cela fonctionne --> ok

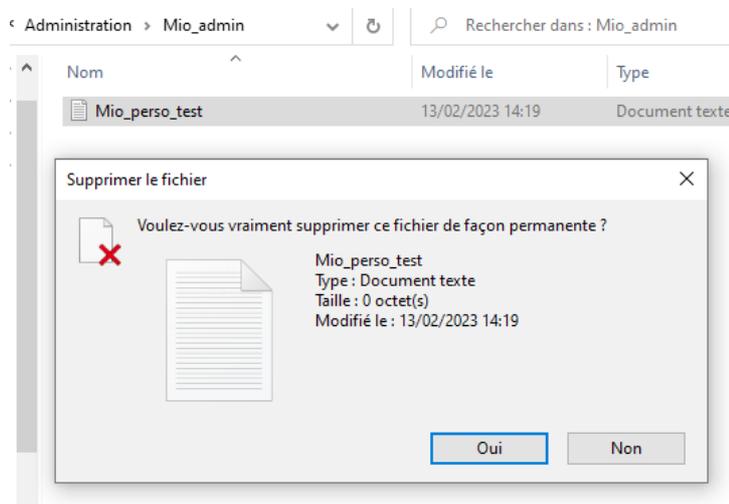


- Nous nous connectons à **Mio\_admin**, qui fait partie de l'administration.

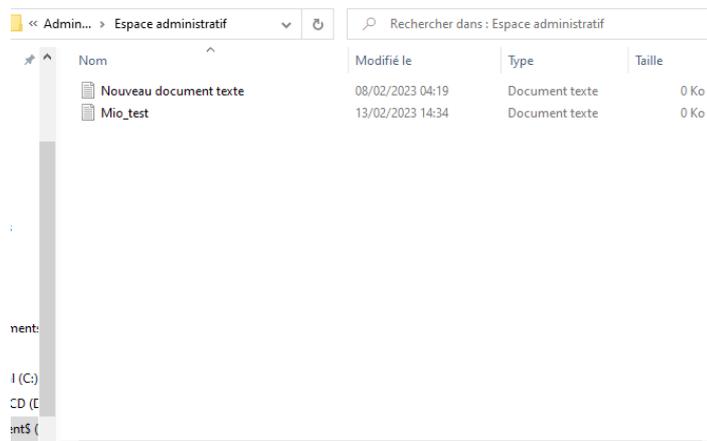
Nous pouvons aller dans le dossier **administration**. Nous essayons d'entrer dans le dossier personnel de **Tex\_admin**. Cela ne marche pas → ok



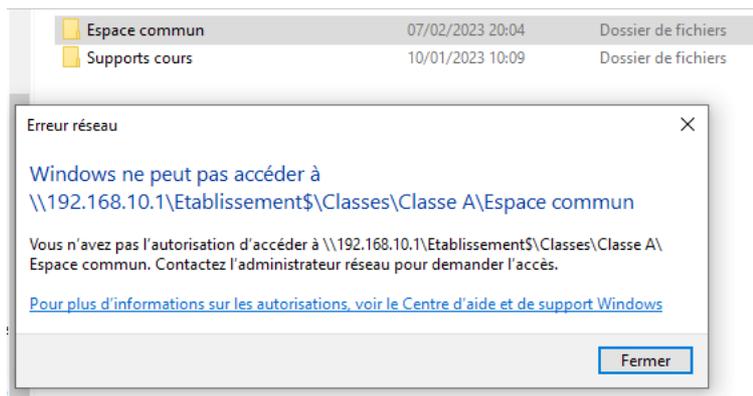
Nous pouvons accéder à son dossier personnel, y ajouter et supprimer des fichiers.



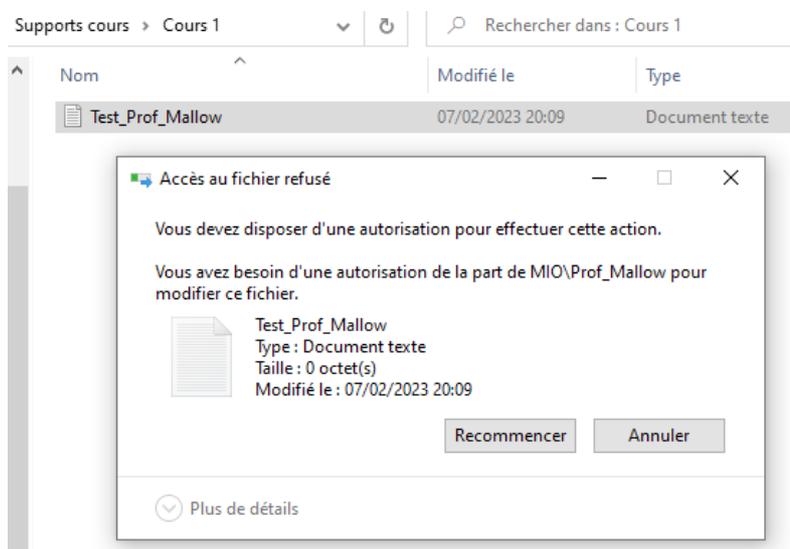
l'utilisatrice peut bien lire et ajouter des fichiers dans l'espace commun de l'administration.



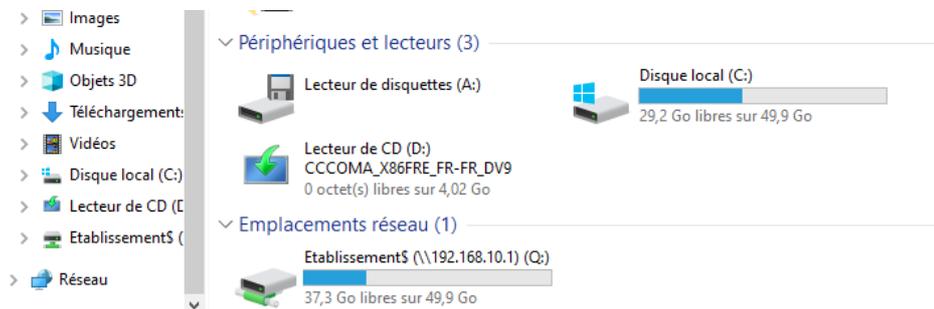
Cette utilisatrice accède aux classes mais ne peut pas entrer dans l'espace commun des élèves → ok



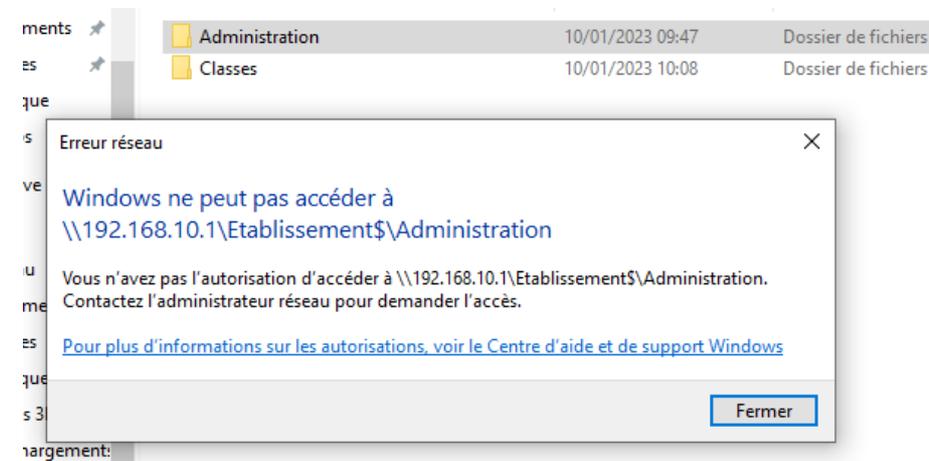
Enfin, nous pouvons aller dans les cours des différents formateurs mais nous ne pouvons pas supprimer les documents → ok



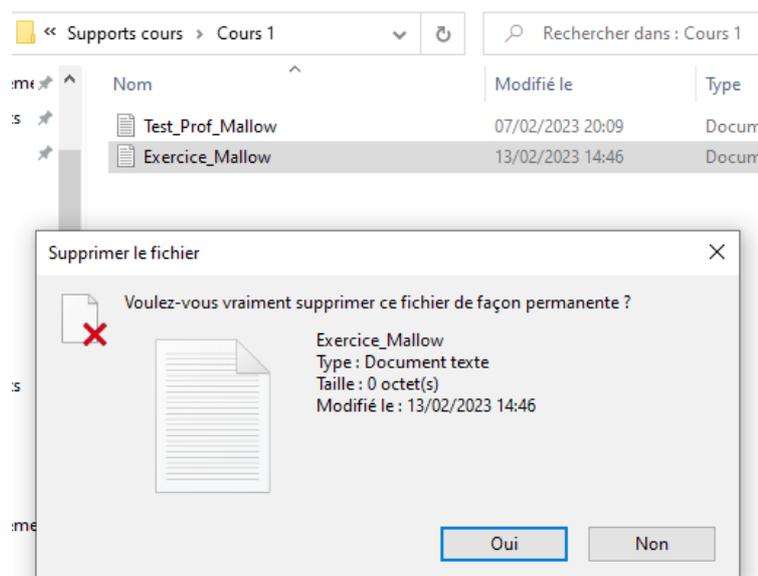
us nous connectons sur la session **Prof\_Mallow** qui est formatrice dans la classe A et la classe B → ok



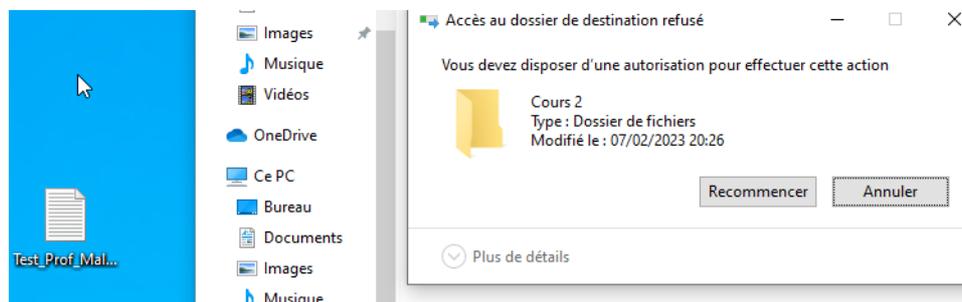
Accès à l'administration refusé --> ok



Nous pouvons aller dans les 2 classes et pour chaque dossier de son cours, nous arrivons à y mettre des fichiers et les supprimer.



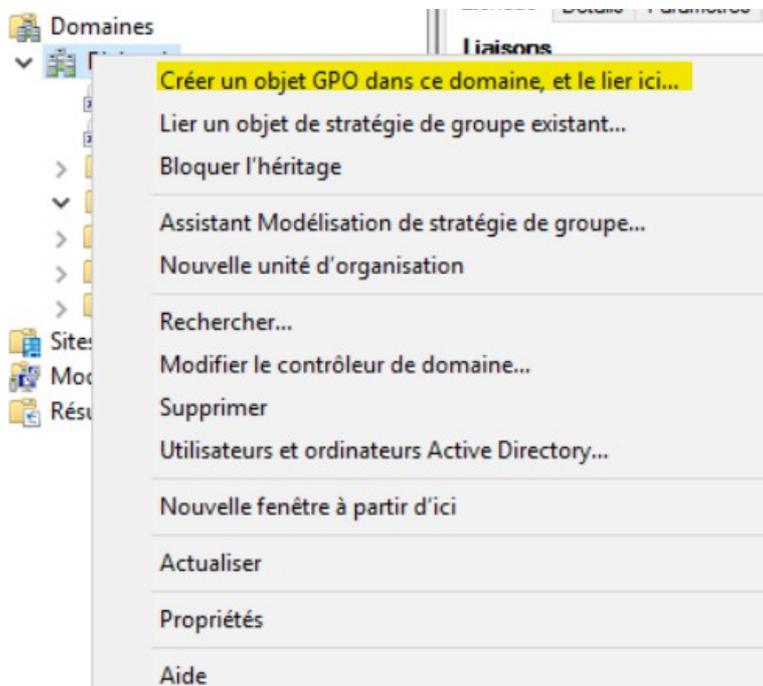
us essayons de transférer un document de **Prof\_Mallow** vers le cours 2. C'est impossible --> ok

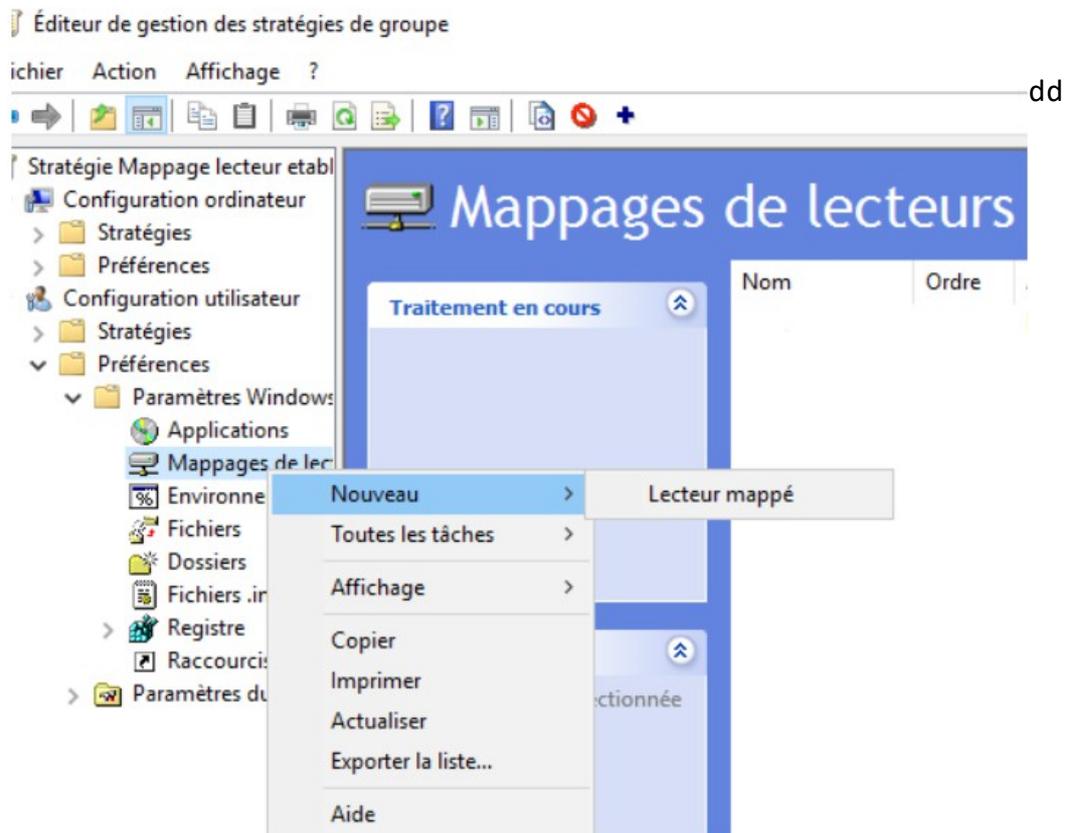


### e) Montage automatique du lecteur réseau

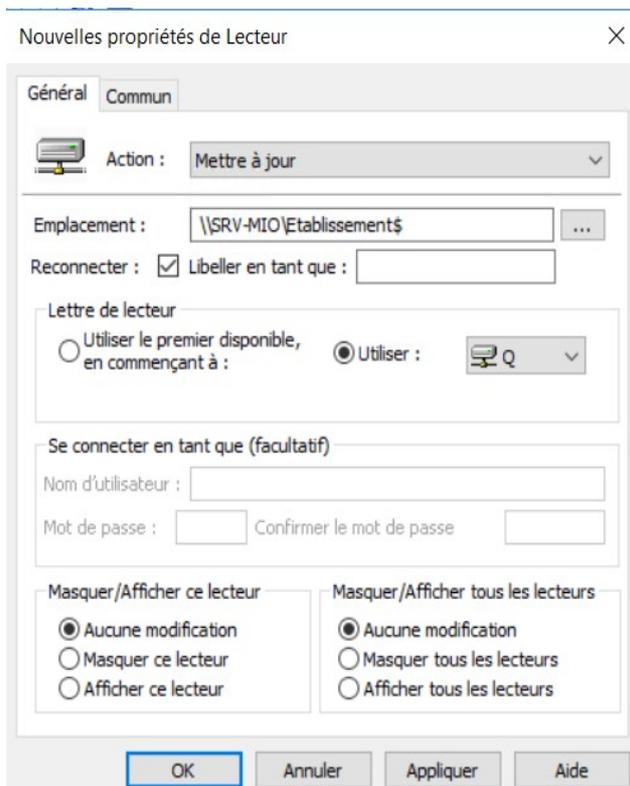
Lorsqu'un nouvel utilisateur est ajouté, nous souhaitons que le lecteur réseau soit monté automatiquement. Pour cela, nous allons créer une GPO (une stratégie de groupe).

Dans la gestion de stratégie de groupe, dans notre domaine, nous ajoutons une nouvelle stratégie

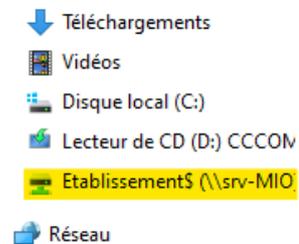




Nous renseignons les données du lecteur réseau



Après avoir appliqué, nous démarrons une machine client avec une nouvelle session utilisateur. Dans l'explorateur de fichiers, nous voyons que le lecteur réseau est remonté.



Nous en avons donc terminé avec la création et le paramétrage de l'établissement tel que demandé dans le cahier des charges. Pour chaque étape effectuée, des vérifications ont été réalisées pour attester du bon fonctionnement des manipulations.

Si la lecture de ce document soulève des questions, nous vous prions de nous contacter à l'adresse mail suivante : [emilie.wanaverbecq@esicad.org](mailto:emilie.wanaverbecq@esicad.org)