1. Utilisateurs, Groupes et Unités d'organisation.

1.1. Création d'un utilisateur de domaine

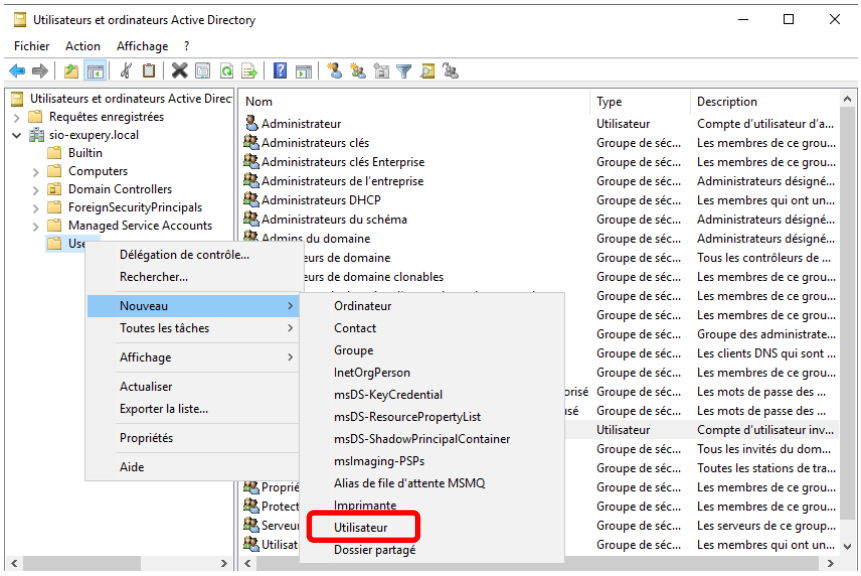
On distingue deux types de compte d'utilisateur :

- le **compte d'utilisateur local** dont les informations de compte résident dans le **SAM** (Secure Account Manager) local de tout ordinateur (station de travail, serveur membre d'un domaine ou d'un groupe de travail) ;
- le **compte d'utilisateur de domaine** qui est stocké dans l'**Active Directory**.

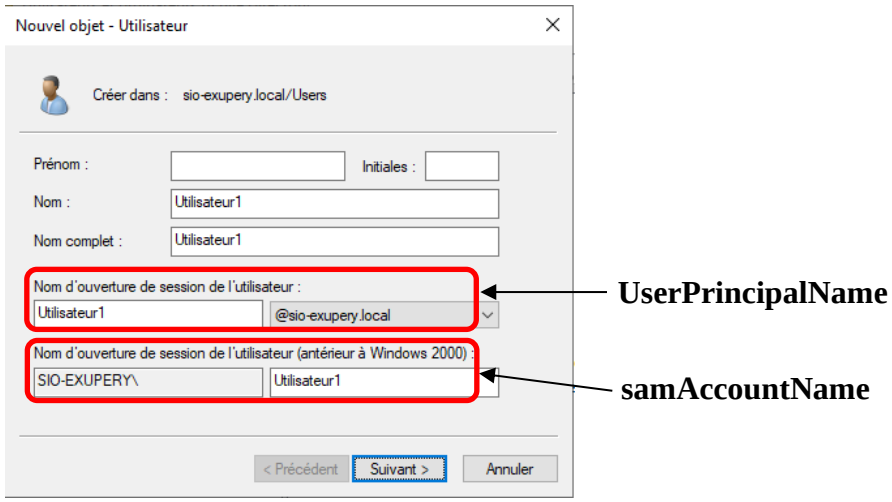
Un compte d'utilisateur de domaine peut se connecter sur n'importe quel ordinateur du domaine et accéder à toutes les ressources du domaine alors qu'un compte d'utilisateur local ne peut se connecter que sur l'ordinateur considéré.

A l'installation d'un serveur Windows Server 2022, deux comptes d'**utilisateurs locaux** sont automatiquement créés : le compte **Administrateur** et le compte **Invité** (désactivé).

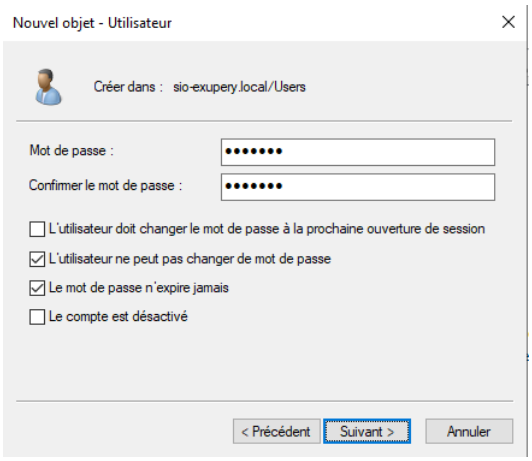
- Pour créer un utilisateur de domaine, ouvrez la console **Utilisateurs et ordinateurs Active Directory** en cliquant, dans le **Gestionnaire de serveur**, sur **Outils** puis sur **Utilisateurs et ordinateurs Active Directory**.
- Cliquez droit sur le conteneur **Users**, sélectionnez **Nouveau** puis **Utilisateur** :



- Tapez le **Nom** de l'utilisateur (Utilisateur1) ainsi que le **Nom d'ouverture de session** (2 manières de se connecter) :



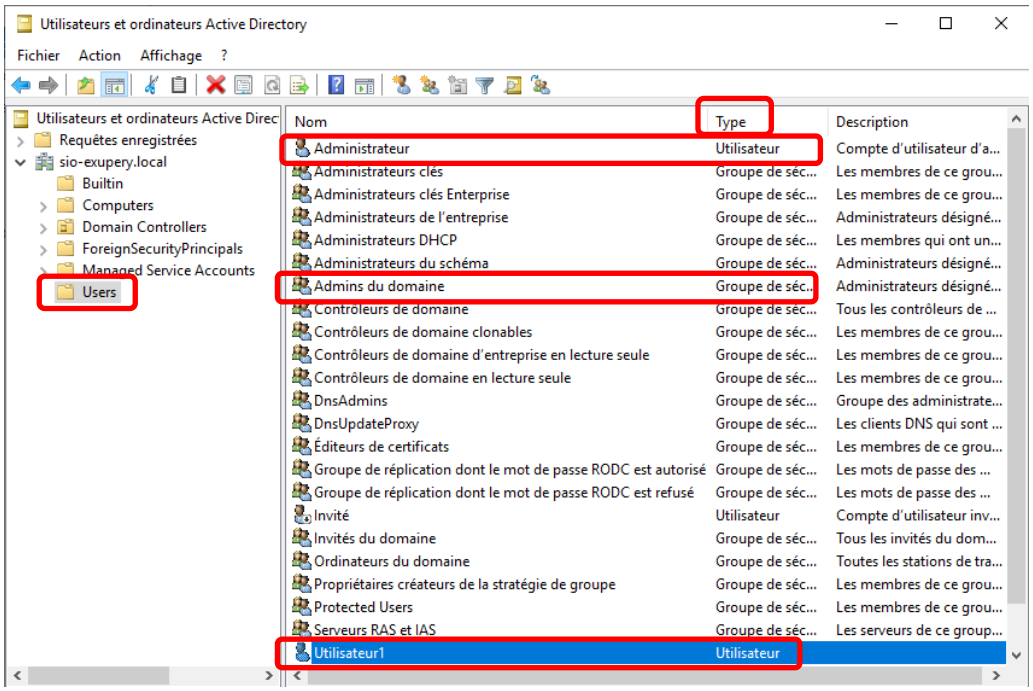
- Saisissez un mot de passe (Azerty0) puis confirmez-le. Vous êtes amené ensuite à préciser si l'utilisateur doit changer le mot de passe à la prochaine ouverture de session ou si l'utilisateur ne peut pas changer de mot de passe. Cochez **L'utilisateur ne peut pas changer de mot de passe** et **Le mot de passe n'expire jamais** :



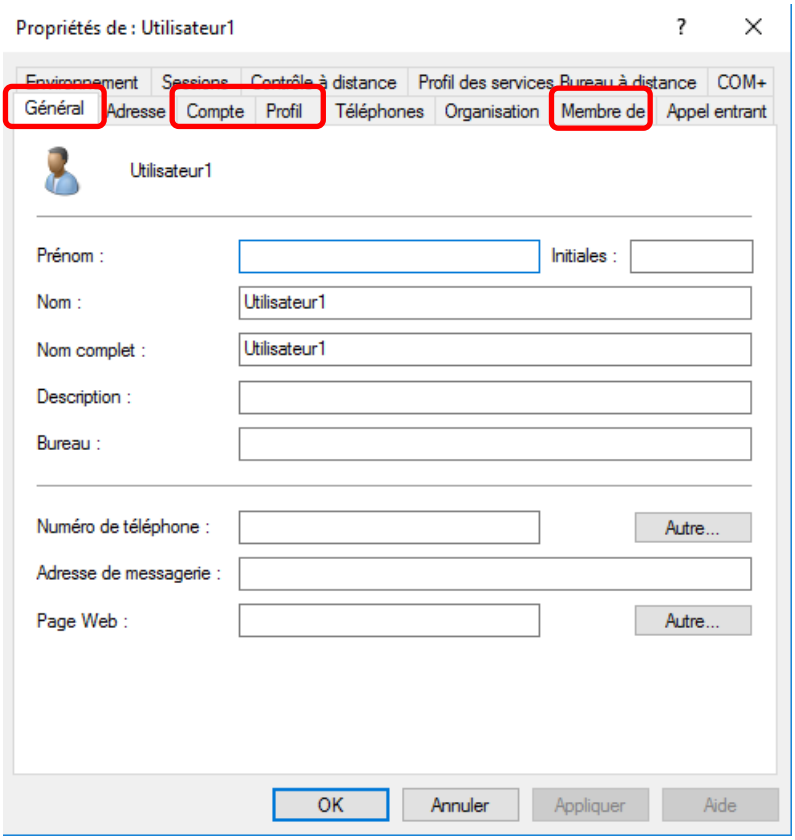
Par défaut, la stratégie locale sur un serveur Windows 2022 impose des mots de passe complexes respectant la règle suivante :

➔ Chaque mot de passe doit comporter au moins trois catégories de caractères parmi les 4 catégories suivantes : les lettres majuscules (A-Z), les lettres minuscules (a-z), les chiffres (0-9) et les caractères spéciaux (@ !$*-&…).

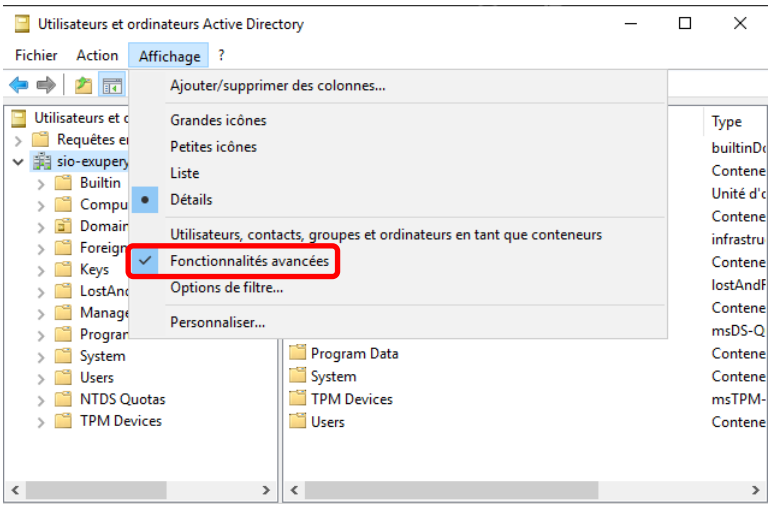
- Recherchez votre utilisateur dans **Utilisateurs et ordinateurs Active Directory** (conteneur **Users**) :



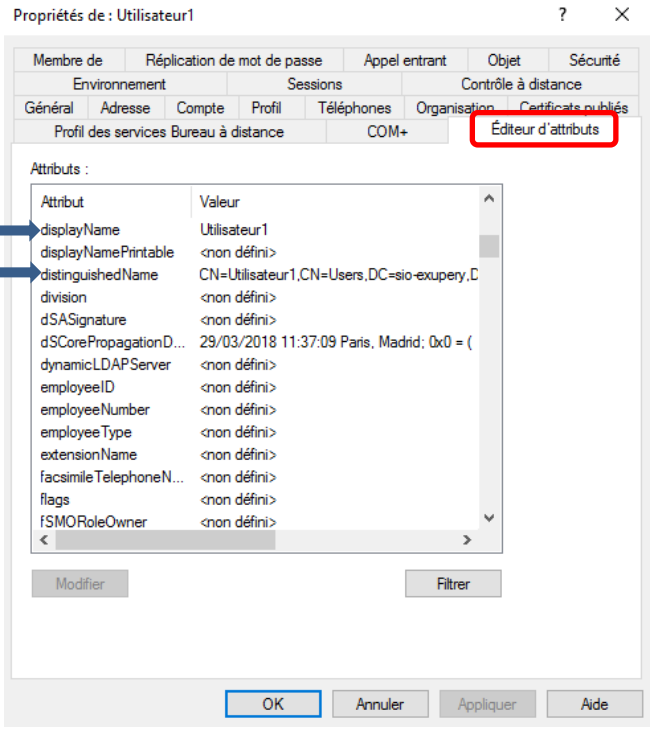
Pour modifier ou configurer les paramètres de l'utilisateur, vous pouvez double cliquer ou cliquer droit sur l'utilisateur et sélectionner **Propriétés**.



Certains onglets nécessitent l'affichage des fonctionnalités avancées. Dans la console **Utilisateurs et ordinateurs Active Directory**, cliquez sur le menu **Affichage** puis sur **Fonctionnalités avancées**.

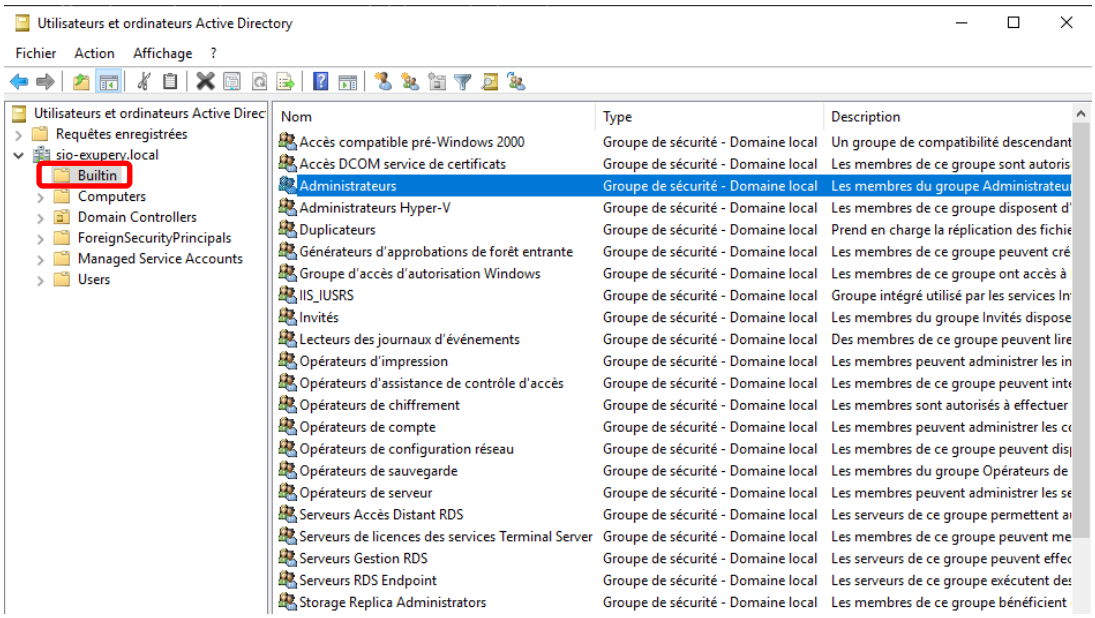


Réaffichez les propriétés de l'utilisateur Utilisateur1. L'onglet **Éditeur d'attributs** permet la visualisation et/ou la modification des attributs LDAP de l'objet.



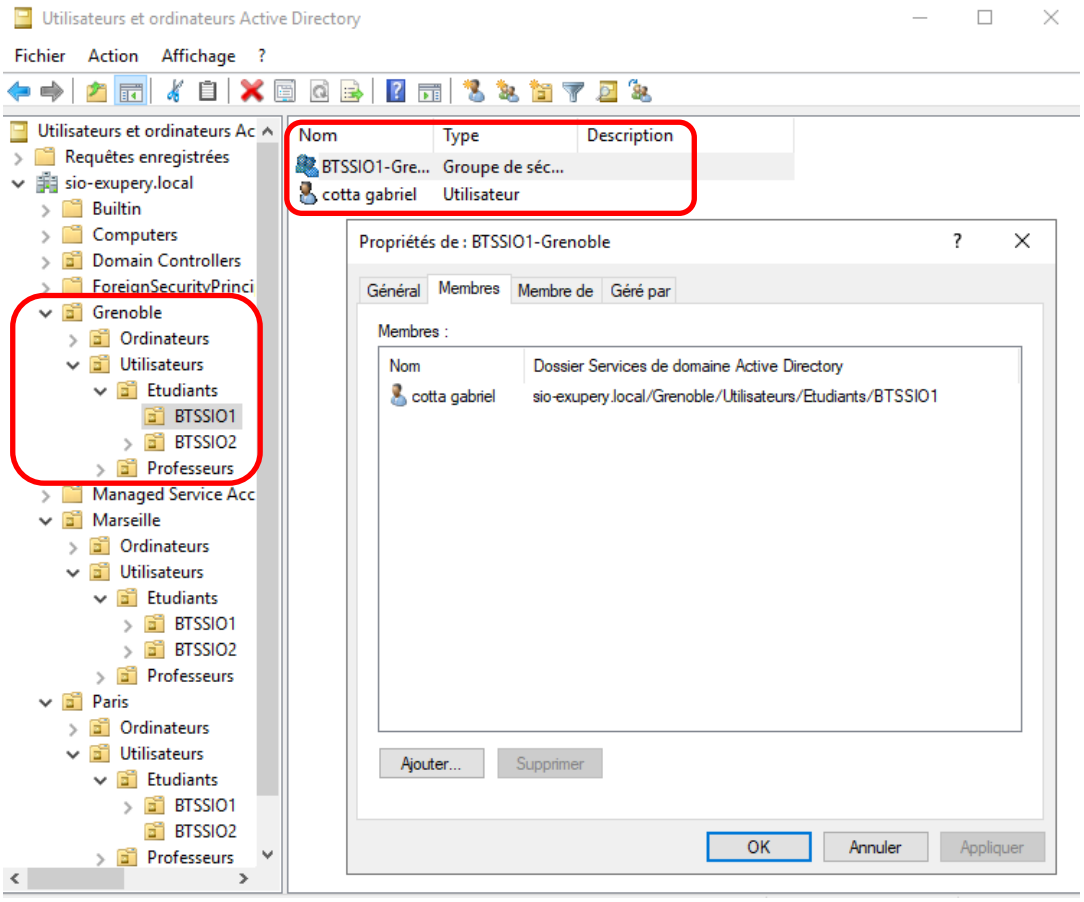
1.2. Les groupes prédéfinis de l'Active Directory

- Ouvrez le conteneur **Users**. Agrandissez la colonne **Type** (cf. page 2). Outre les **utilisateurs**, vous y trouvez les **groupes prédéfinis de l'Active Directory** **(Groupe de sécurité)**.
- Ouvrez le conteneur **Builtin**. Y figurent les **groupes Builtin** de l'Active Directory :

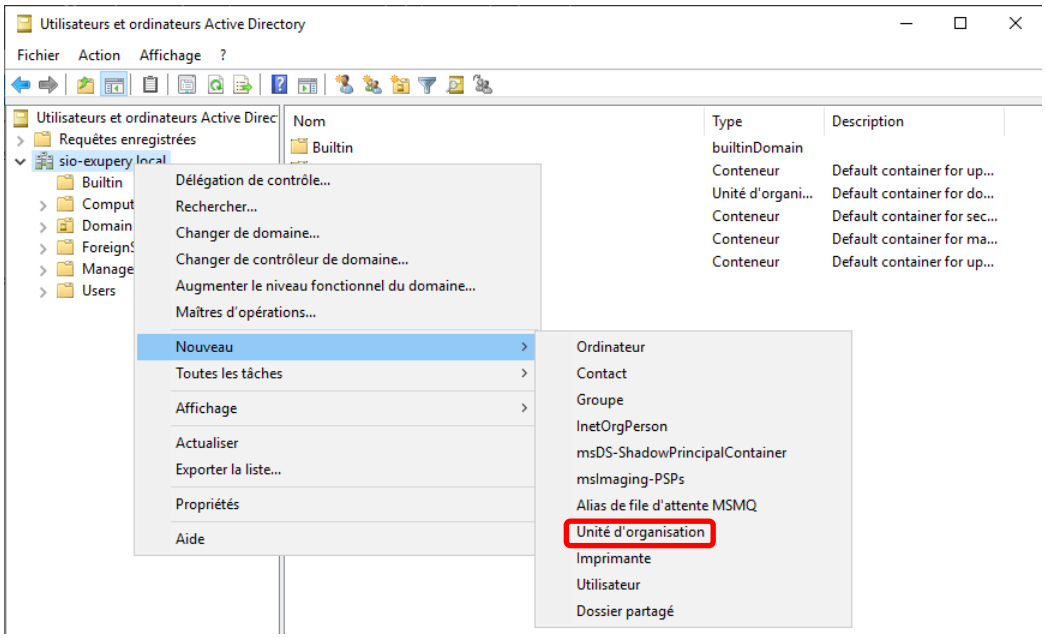


1.3. Création d'une unité d'organisation et d'un groupe d'utilisateurs

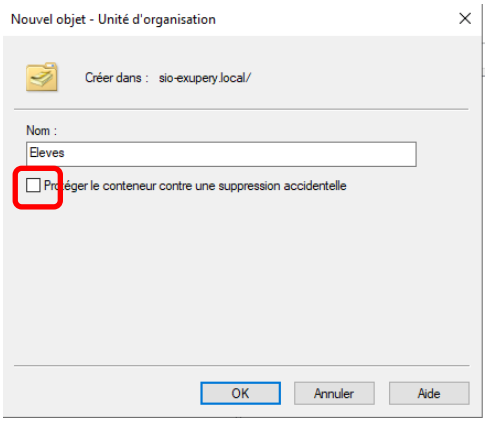
- Dans le but de faciliter la gestion des comptes utilisateurs, il est utile de créer des **groupes d'utilisateurs** afin de ne gérer qu'une seule entité plutôt que chaque utilisateur. L'utilisateur hérite, en effet, des autorisations accordées au groupe.
- Une **unité d'organisation** (**UO** ou **OU** en anglais) est un **conteneur** dans lequel on peut créer des **objets** (utilisateurs, groupes, ordinateurs, imprimantes) et sur lequel on peut appliquer des **stratégies de groupe** (cf. Chapitre 5). Les UO permettent d'organiser les objets de l'AD de manière hiérarchique afin de se rapprocher de l'organigramme logique de l'entreprise.



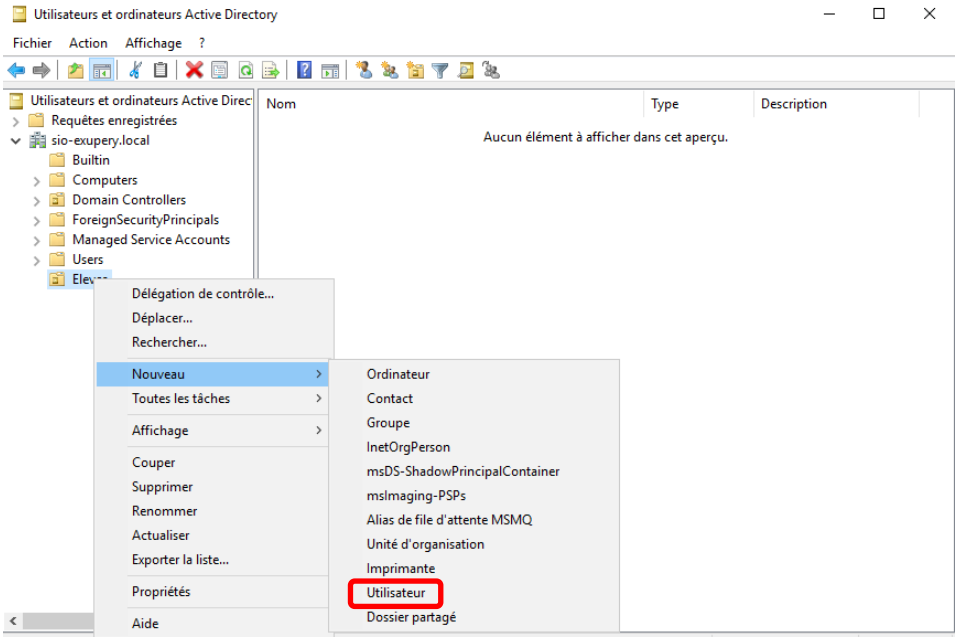
- Pour créer une unité d'organisation au même niveau que par exemple le conteneur **User**, cliquez droit sur le nom du domaine (**sio-exupery.local**), sélectionnez **Nouveau** puis **Unité d'organisation** :



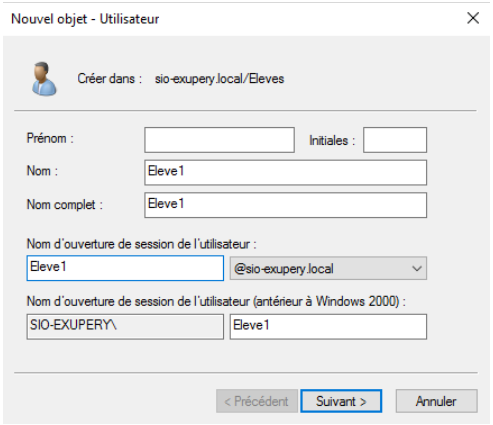
- Indiquez **Eleves** pour le nom de l'unité d'organisation et déprotégez l'unité d'organisation contre une suppression accidentelle :



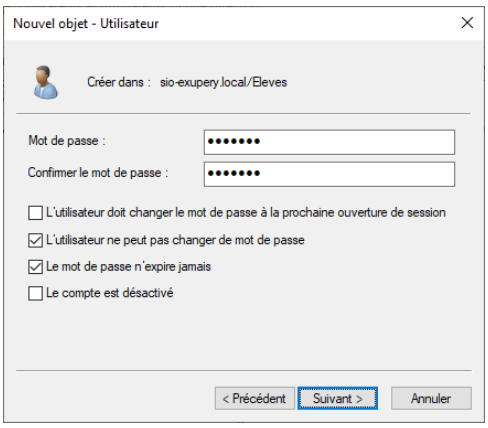
- Créez un nouvel utilisateur en cliquant droit sur l'UO **Eleves** :



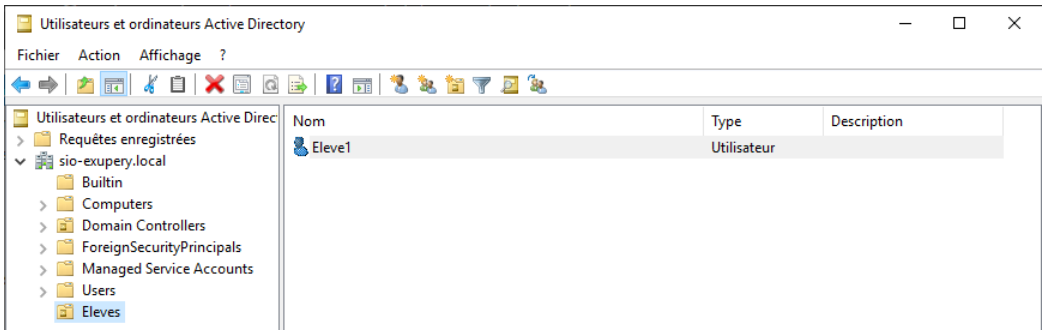
- Tapez le **Nom** de l'utilisateur (Eleve1) ainsi que le **Nom d'ouverture de session** :



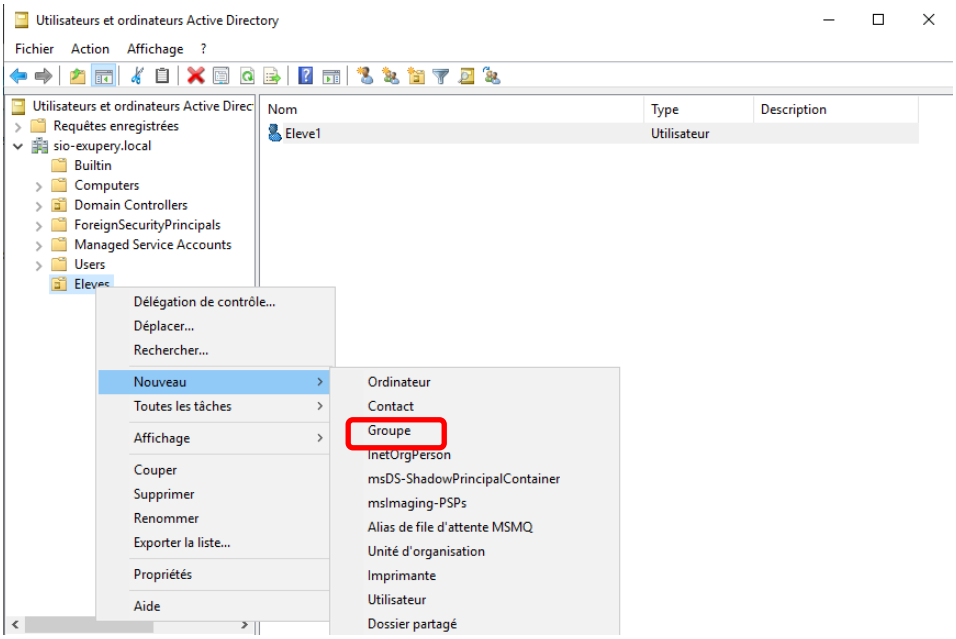
- Saisissez un **Mot de passe** (Azerty0) puis confirmez-le :



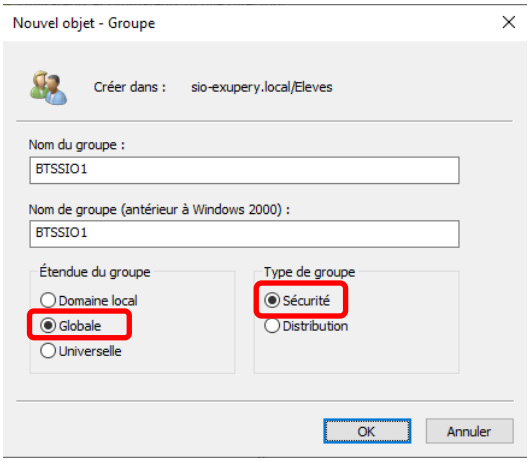
L'utilisateur **Eleve1** apparaît dans le conteneur **Eleves** :



- Pour créer un **groupe d'utilisateurs**, cliquez droit sur l'UO **Eleves**, sélectionnez **Nouveau** puis **Groupe** :

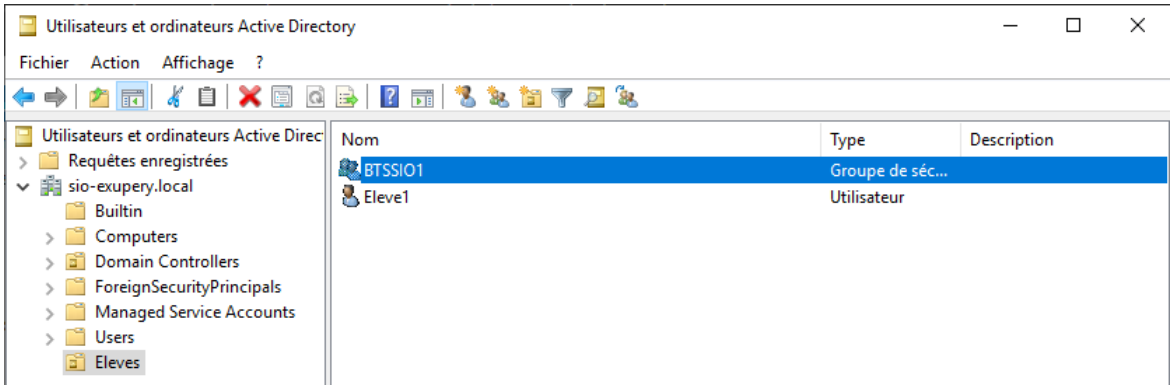


- Indiquez **BTSSIO1** pour le **Nom du groupe** et conservez la sélection par défaut pour l'**étendue du groupe (Globale)** ainsi que pour le type de groupe **(Sécurité)** :

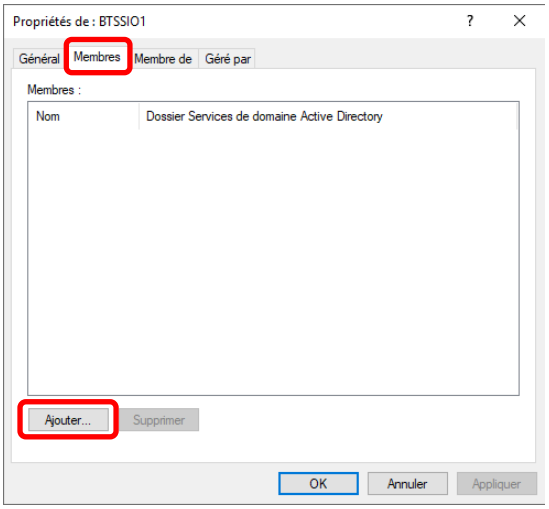


Cf. https://www.it-connect.fr/chapitres/les-differents-types-de-groupe-de-lactive-directory/ pour les différentes étendues et les différents types de groupe.

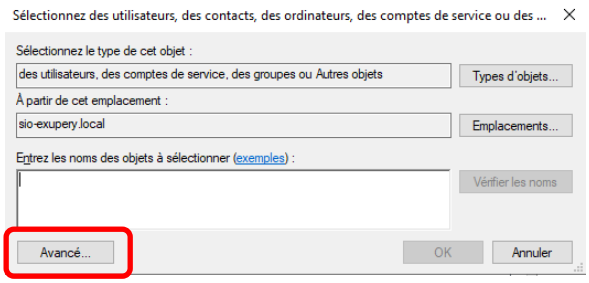
Le groupe d'utilisateurs **BTSSIO1** apparaît dans le conteneur **Eleves** :



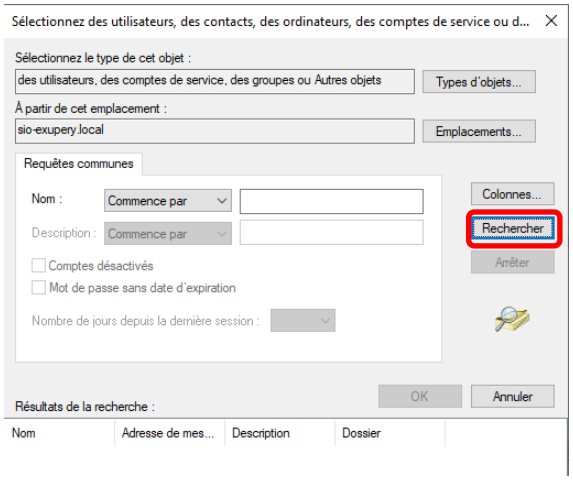
- Il s'agit maintenant d'ajouter l'utilisateur **Eleve1** au groupe **BTSSIO1**. Double cliquez sur le groupe **BTSSIO1,** cliquez sur l'onglet **Membres** puis sur **Ajouter** :



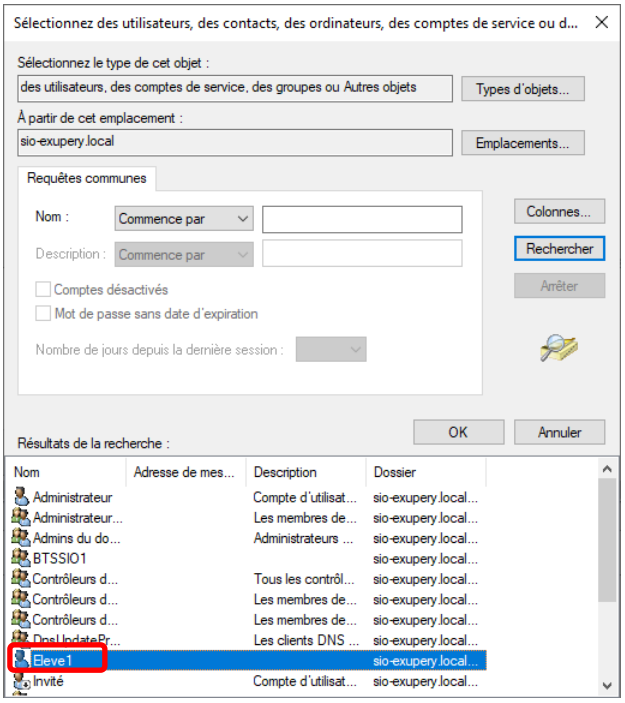
- Cliquez sur **Avancé** (la recherche de l'utilisateur se fera à partir du domaine **sio-exupery.local**) :



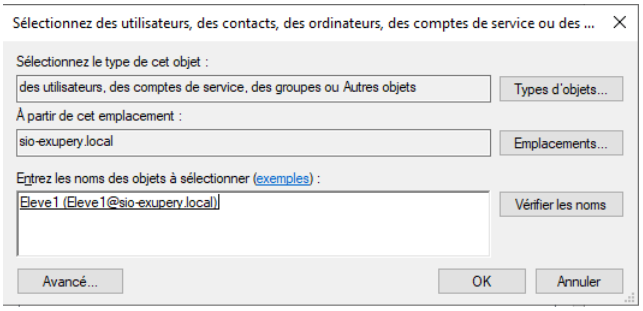
- Cliquez sur **Rechercher** :



- Double cliquez sur l'utilisateur **Eleve1** :

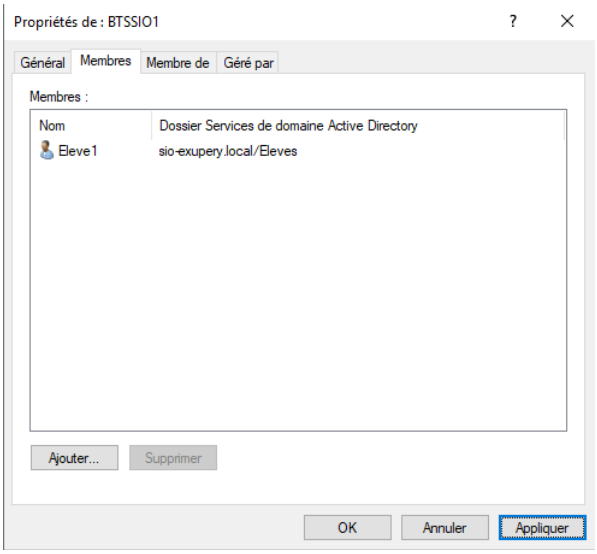


- Cliquez sur **OK** :

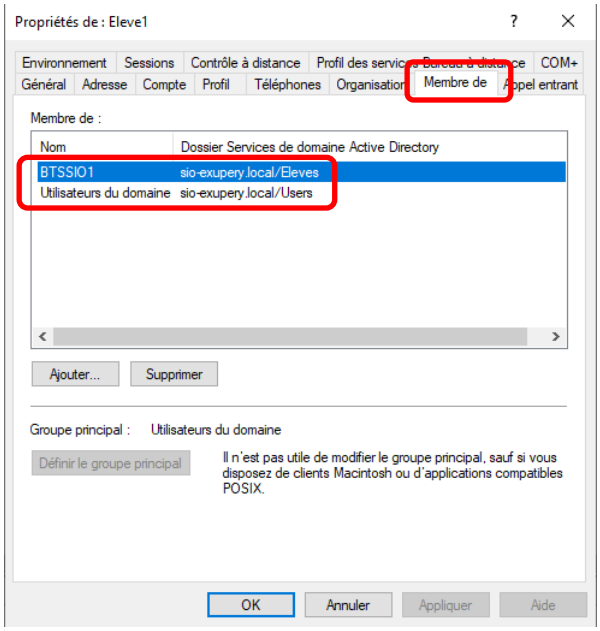


Vous pourriez entrer directement le nom de l'objet et cliquer sur **Vérifier les noms**.

Le groupe d'utilisateurs **BTSSIO1** comprend l'utilisateur **Eleve1** :

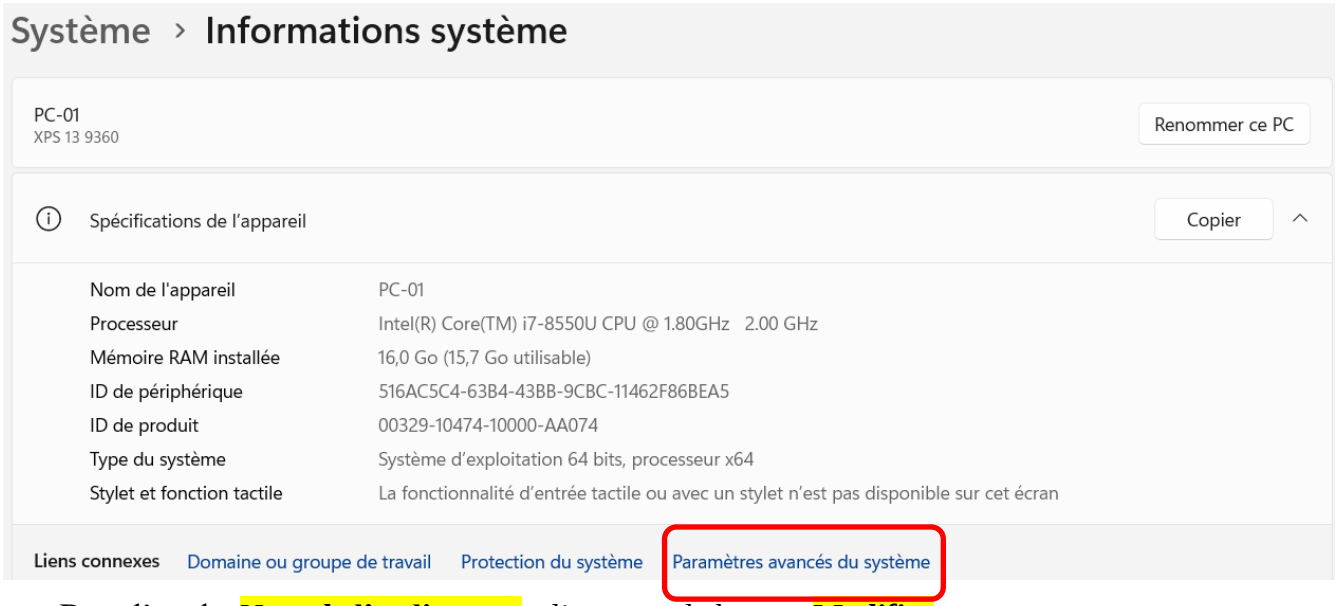


- Double cliquez sur l'utilisateur **Eleve1** et cliquez sur l'onglet **Membre de**. Cet utilisateur est membre du groupe d'utilisateurs **BTSSIO1** ainsi que du groupe prédéfini de l'Active Directory **Utilisateurs du domaine** :

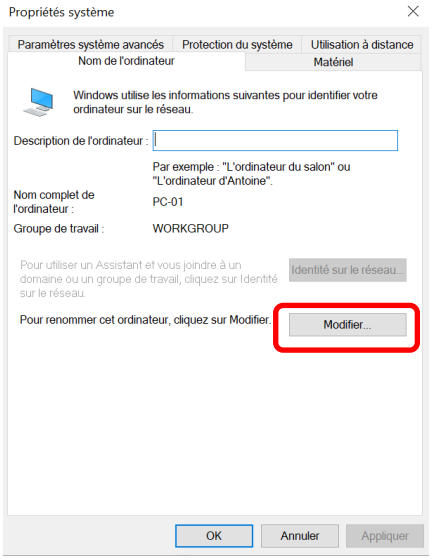


2. Inscription de WIN11 dans le domaine.

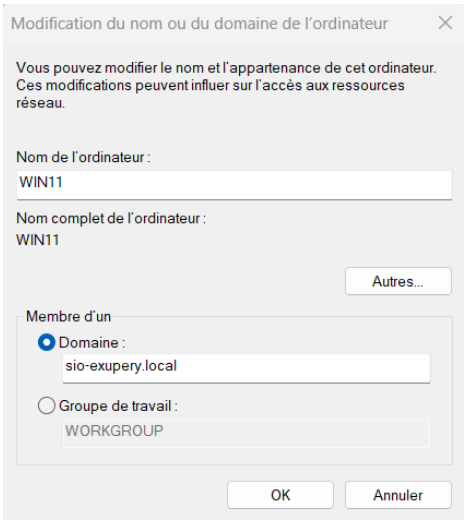
- A partir de la machine virtuelle **WIN11**, accédez à **Système** : cliquez droit sur le bouton **Démarrer**, sélectionnez **Système** (ou tapez Système dans la zone de recherche) puis cliquez sur **Paramètres avancés du système** :



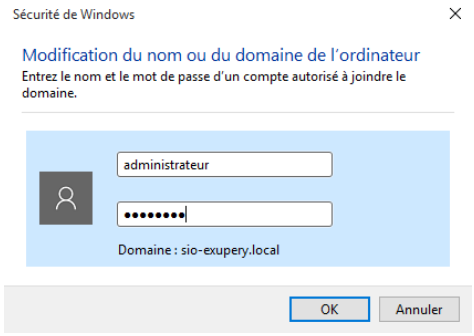
- Dans l'onglet **Nom de l'ordinateur**, cliquez sur le bouton **Modifier** :



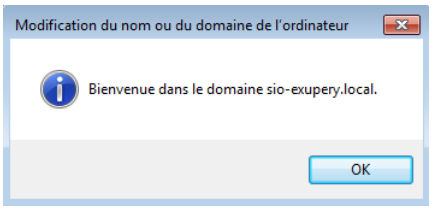
- Spécifiez le nom du domaine (**sio-exupery.local**) auquel vous voulez que l'ordinateur devienne membre :

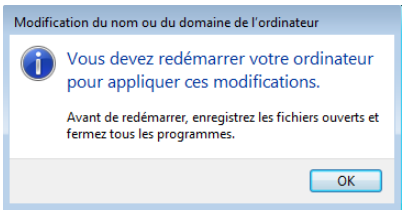


- Indiquez le nom et le mot de passe d'un compte autorisé à inscrire un ordinateur dans le domaine sio-exupery.local. Spécifiez le compte administrateur du serveur Windows 2022 :

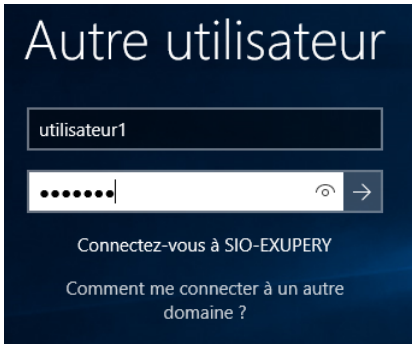


- Vous devez obtenir le message confirmant l'inscription de l'ordinateur dans le domaine. Un message d'avertissement vous précise que l'ordinateur doit redémarrer.

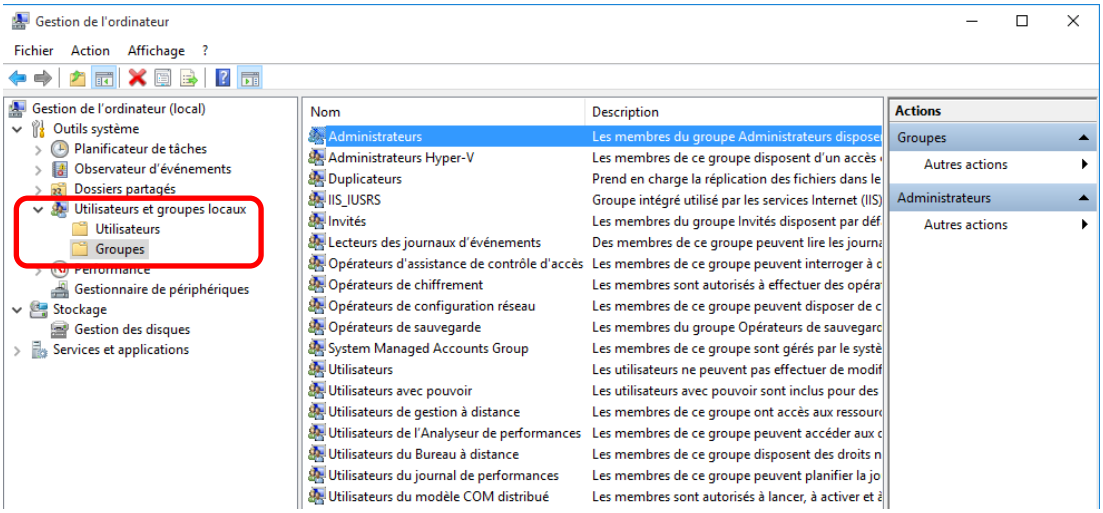




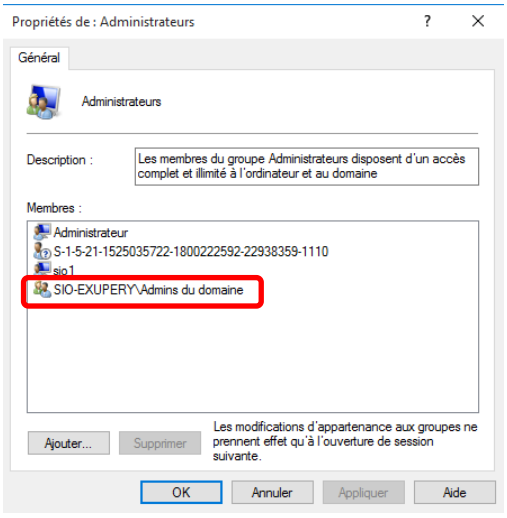
- Cliquez sur **Fermer** dans l'onglet **Nom de l'ordinateur** puis cliquez sur **Redémarrer maintenant**. Ouvrez ensuite une session depuis le domaine **sio-exupery** avec par exemple le compte **Utilisateur1** :

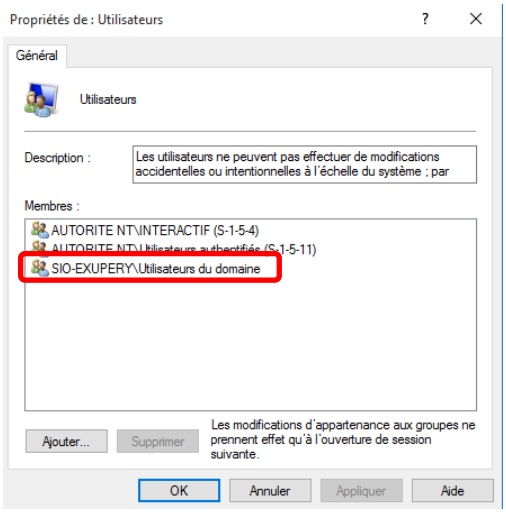


- Accédez à la liste des groupes prédéfinis sur un ordinateur local en cliquant droit sur **Ce PC** (VM WIN11) puis en sélectionnant **Gérer** (ou cliquer droit sur le bouton **Démarrer**). Dans **Gestion de l'ordinateur**, double cliquez sur **Utilisateurs et Groupes locaux** puis sur **Groupes** :

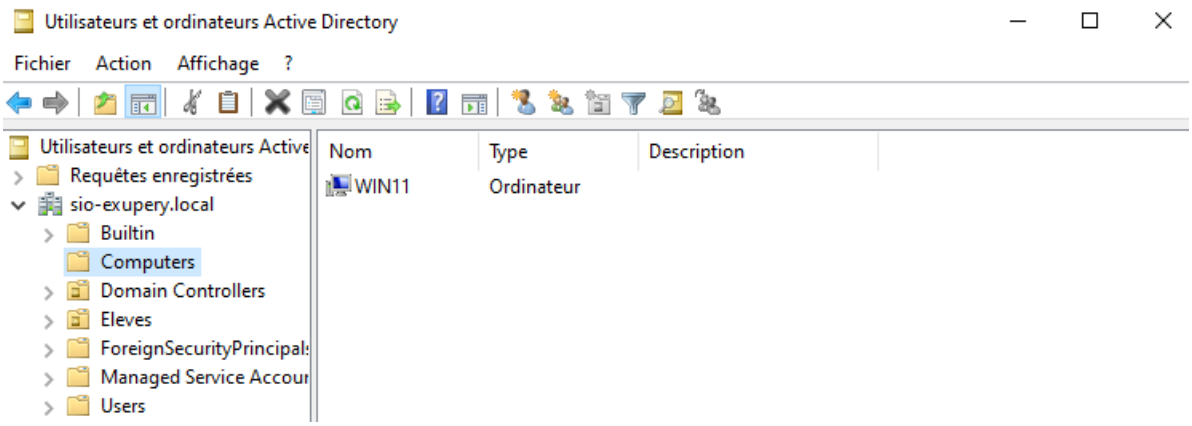


- Lorsqu'un ordinateur rejoint le domaine, le groupe **Admins de domaine** est automatiquement ajouté au groupe local **Administrateurs** et le groupe **Utilisateurs de domaine** est ajouté au groupe local **Utilisateurs**. Double cliquez sur les groupes locaux **Administrateurs** et **Utilisateurs** :





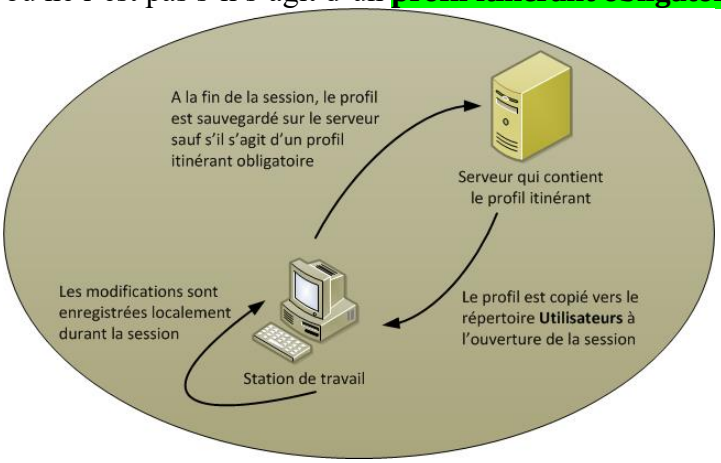
- A partir du serveur Windows 2022, accédez à **Utilisateurs et ordinateurs Active Directory** et cliquez sur **Computers** pour constater la présence de l'ordinateur WIN11 :



3. Profil itinérant et dossier de base.

On désigne par **profil utilisateur** l'ensemble des paramètres permettant de construire l'environnement personnel de l'utilisateur : paramètres du **Bureau**, entrées du menu **Démarrer**, dossier des **Favoris**, paramètres de l'**Explorateur de fichiers**…

Par défaut, le profil utilisateur est stocké en local (on parle alors de **profil utilisateur local**) dans un répertoire qui porte le nom du **login** et qui se trouve dans le répertoire **Utilisateurs** pour une station fonctionnant sous **Windows**.
Si l'utilisateur change d'ordinateur, la personnalisation du profil utilisateur n'est pas retrouvée sur le nouvel ordinateur. Pour pallier ce problème, **Windows 2022 Server**, comme ses prédécesseurs, permet d'enregistrer les profils des utilisateurs sur le serveur. On parle dans ce cas de **profil utilisateur itinérant**. Dès qu'un utilisateur se connecte sur un ordinateur, son profil est alors chargé du serveur en local puis le profil local est utilisé durant sa session. A la fin de sa session, le profil éventuellement modifié est sauvegardé, ou ne l'est pas s'il s'agit d'un **profil itinérant obligatoire**.

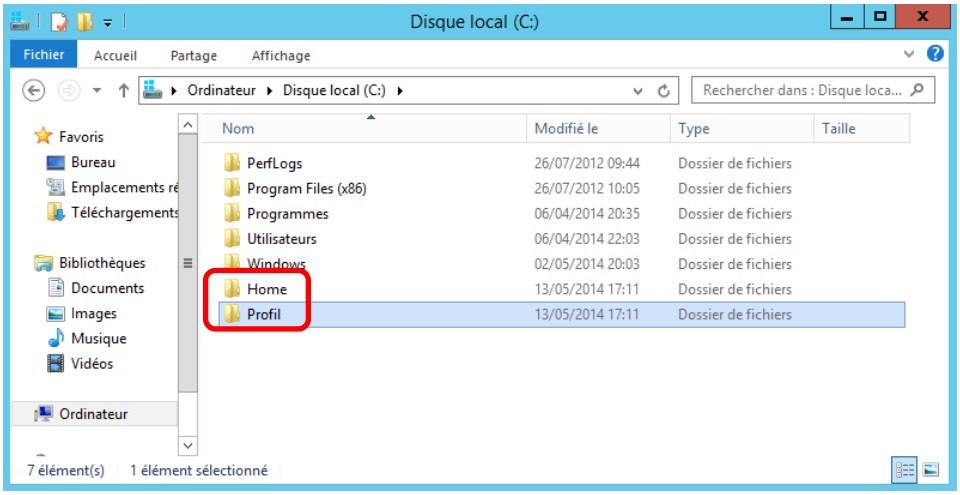


Pour créer un **profil itinérant obligatoire**, c'est-à-dire un profil itinérant dont les modifications ne sont pas enregistrées sur le serveur, il faut renommer le fichier **ntuser.dat** se situant dans le répertoire partagé côté serveur **utilisateurs\%username%** en **ntuser.man**.

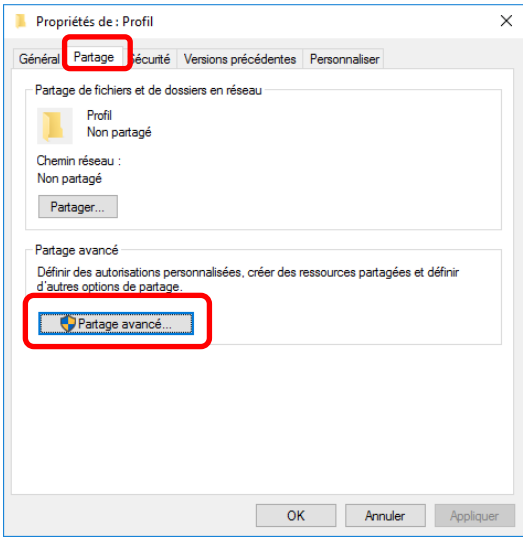
Dans un environnement Active Directory, une grande partie du profil de l'utilisateur peut être géré de manière efficace à l'aide des **stratégies de groupe** (cf. Chapitre 5).

3.1. Partage des répertoires Home et Profil et autorisations de partage

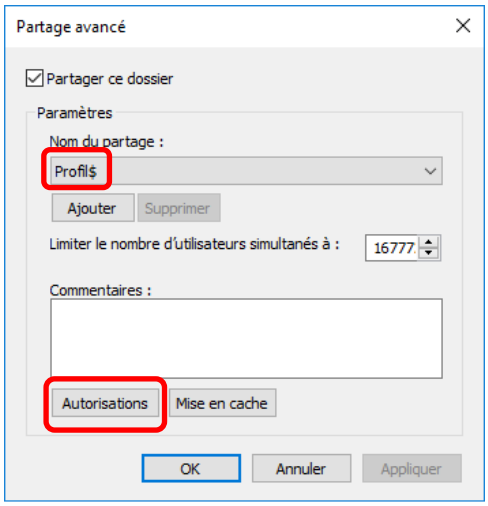
- Créez, à la racine du **Disque local (C:)** du serveur , le répertoire **Home** qui comportera les répertoires personnels des utilisateurs ainsi que le répertoire **Profil** qui recevra les profils itinérants des utilisateurs :

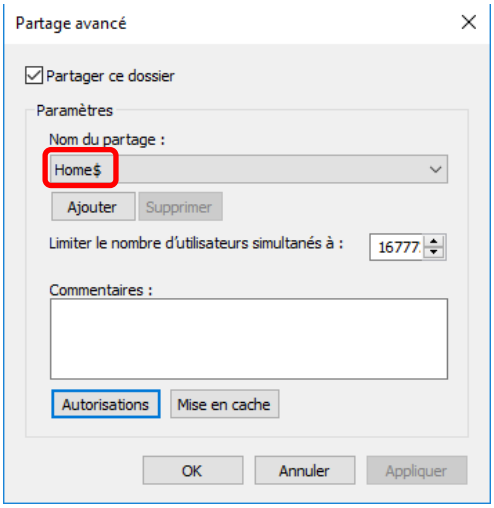


- Cliquez droit sur chaque répertoire et sélectionnez **Propriétés**. A partir de l'onglet **Partage**, cliquez sur **Partage avancé** afin de partager les deux répertoires :

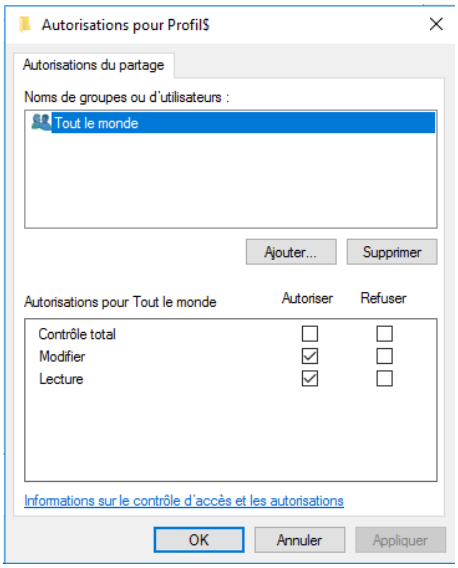


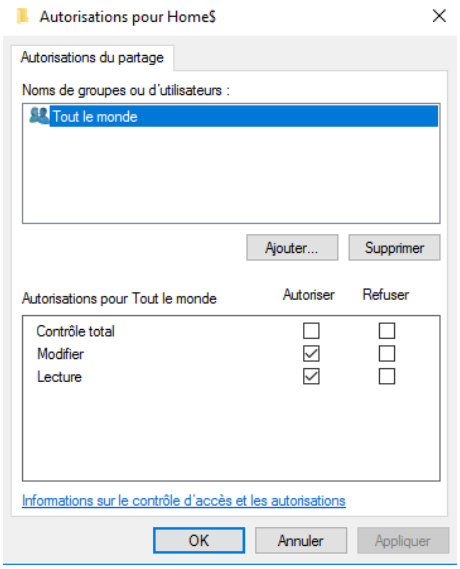
- Cochez **Partager ce dossier** et renseignez le **Nom du partage** (partage caché en ajoutant le caractère $ à la fin du nom de partage). Cliquez ensuite sur **Autorisations** :





- Pour ces deux répertoires, mettez les **autorisations de partage** à **Modifier** pour le groupe **Tout le monde** :





3.2. Autorisations de sécurité NTFS

Les **autorisations de partage** servent à définir les droits d'accès à un dossier via le réseau. Les **autorisations de sécurité NTFS** servent à définir les droits d'accès, via le réseau ou directement sur l'ordinateur, à un dossier ou à un fichier, qu'il soit partagé ou pas.

Les **autorisations de partages** offrent une sécurité moins grande que les **autorisations de sécurité NTFS** car ces dernières fonctionnent **aussi en local** et permettent de définir des **autorisations plus poussées**.

Le tableau suivant présente les **autorisations NTFS standards** existantes dans Windows Server 2022 :

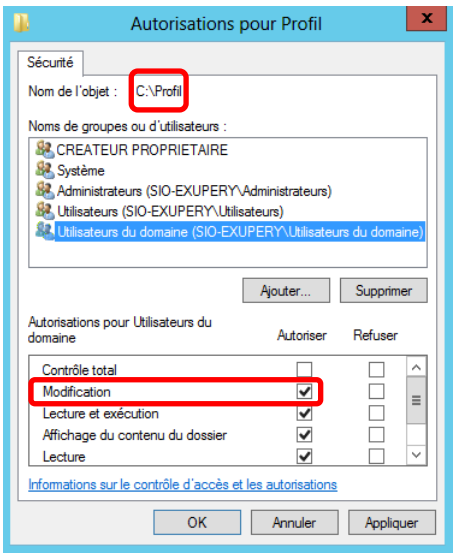
Affichage du contenu du dossier	Afficher le nom des fichiers et des sous-dossiers contenus dans un dossier sans avoir la possibilité de lire le contenu d'un fichier
Lecture	Permet l'affichage du contenu d'un dossier et permet de lire un fichier.
Écriture	Permet l'ajout ou la modification d'un fichier ou d'un dossier.
Lecture et exécution	Reprend l'autorisation de lecture et permet en plus l'exécution des programmes dans des dossiers.
Modification	Reprend l'autorisation de lecture, d'écriture, de lecture et exécution, d'affichage du contenu d'un dossier et permet en plus la **suppression**.
Contrôle total	Reprend l'autorisation de modification et permet en plus l'**appropriation**, la **modification des autorisations** et la **suppression de sous-dossiers et fichiers**.

En cliquant sur le bouton **Avancé**, on accède aux **autorisations spéciales** qui permettant d'affiner les autorisations standards.

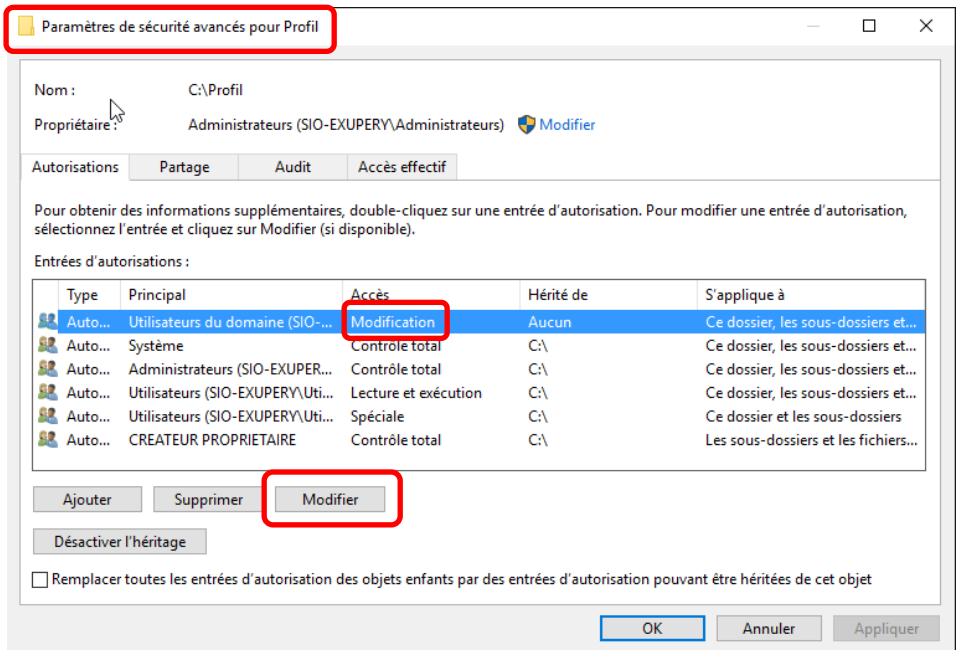
➔ En fait, chaque autorisation NTFS standard est basée sur les **autorisations spéciales** :

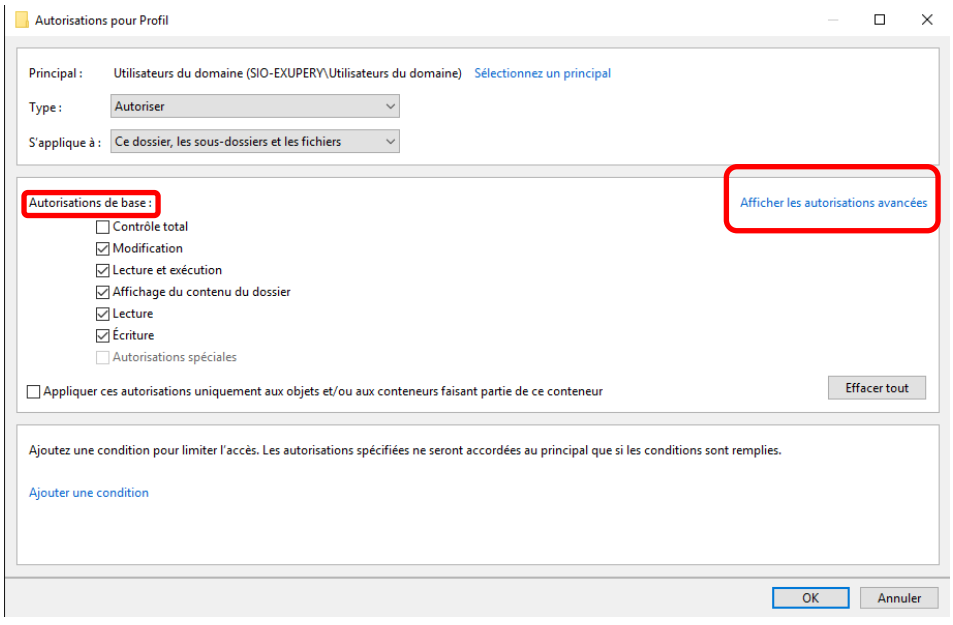
Autorisations standards / Autorisations spéciales	Lecture	Écriture	Lecture et exécution	Affichage du contenu d'un dossier	Modification	Contrôle total
Parcours du dossier/exécuter le fichier			x	x	x	x
Liste du dossier/lecture de données	x		x	x	x	x
Attributs de lecture	x		x	x	x	x
Lecture des attributs étendus	x		x	x	x	x
Création de fichier/écriture de données		x			x	x
Création de dossier/ajout de données		x			x	x
Attributs d'écriture		x			x	x
Écriture d'attributs étendus		x			x	x
Suppression de sous-dossier et fichier						x
Suppression					x	x
Autorisations de lecture	x	x	x	x	x	x
Modifier les autorisations						x
Appropriation						x

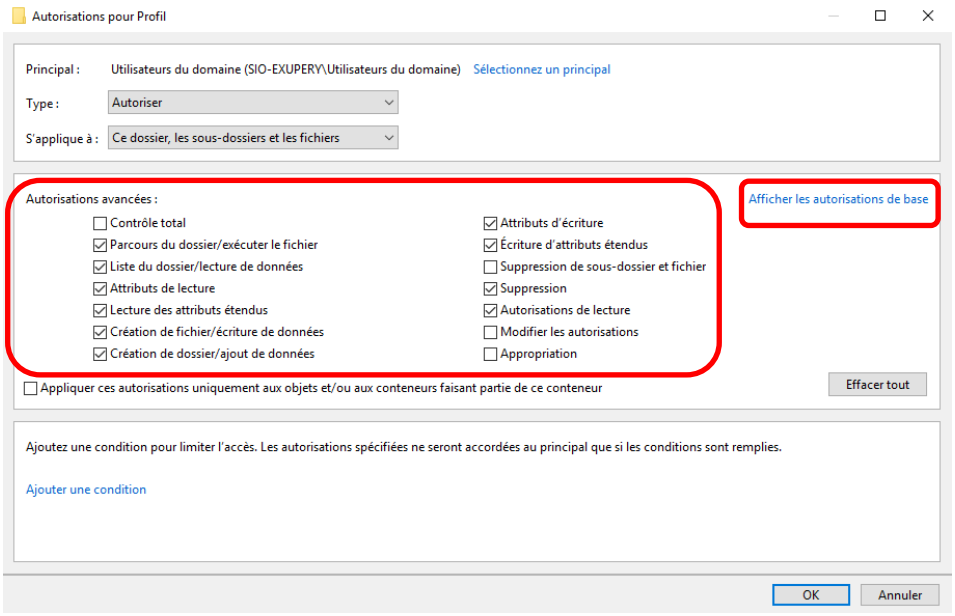
Exemple d'autorisations spéciales :



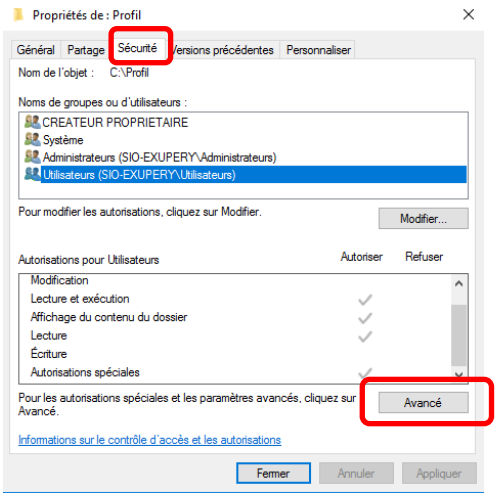
L'autorisation de sécurité standard **Modification,** accordée ci-dessus aux membres du groupe **Utilisateurs du domaine** sur le répertoire **Profil**, correspond aux **autorisations spéciales** suivantes :



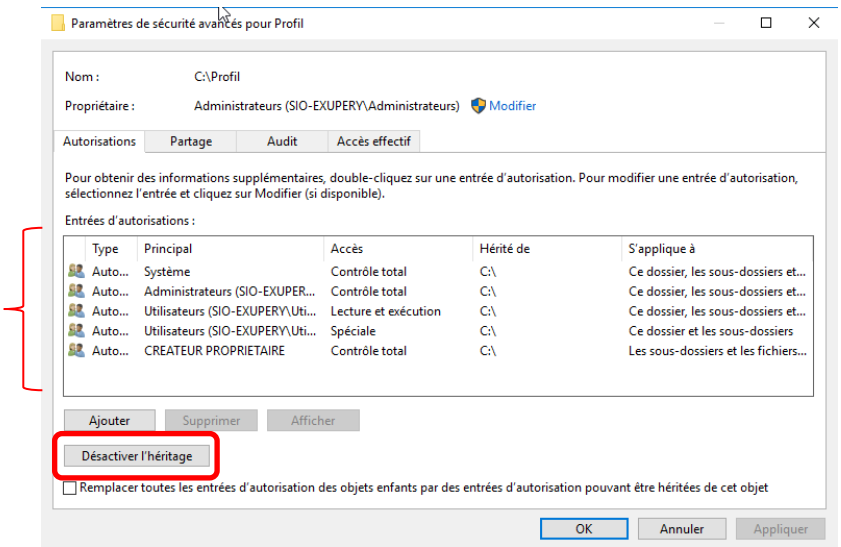




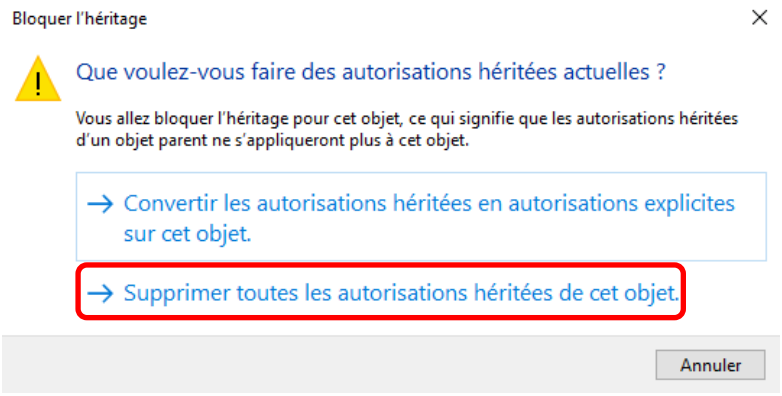
- Dans l'onglet **Sécurité** des propriétés du répertoire **Profil**, cliquez sur **Avancé** afin de définir les **autorisations de sécurité NTFS** :



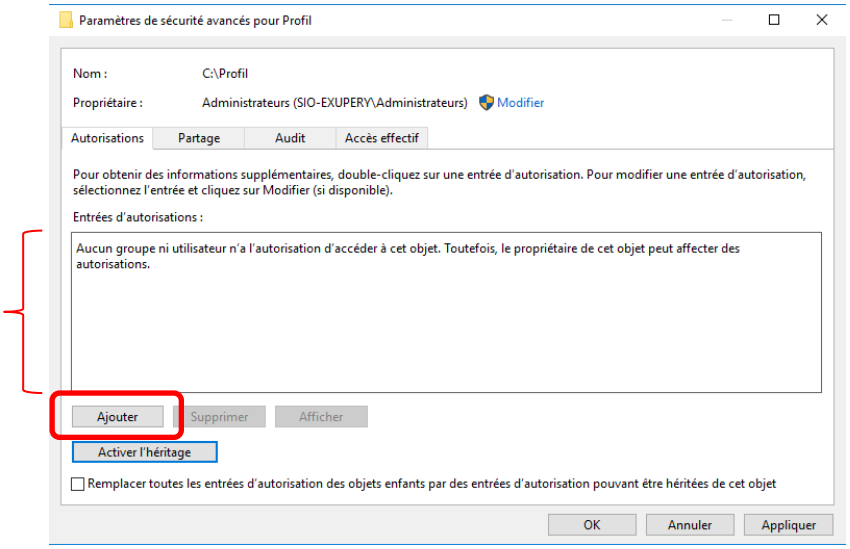
- Cliquez sur **Désactiver l'héritage** :



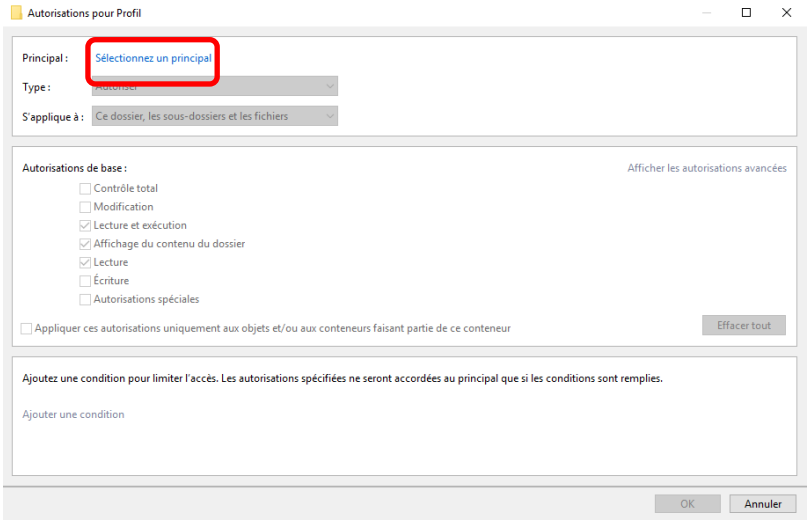
- Cliquez sur **Supprimer toutes les autorisations héritées de cet objet** :



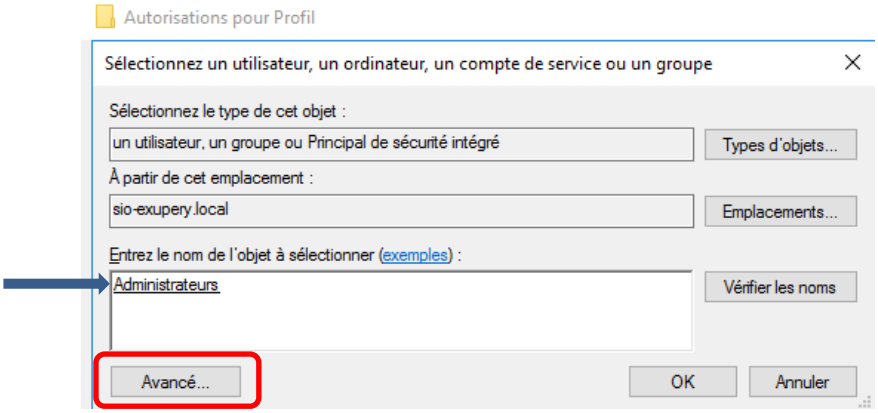
- Cliquez sur le bouton **Ajouter** :



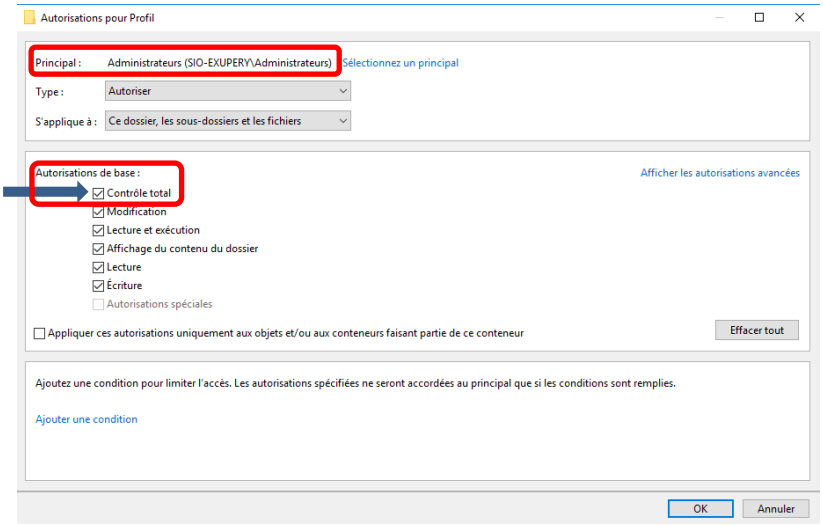
- Cliquez sur **Sélectionnez un principal** :



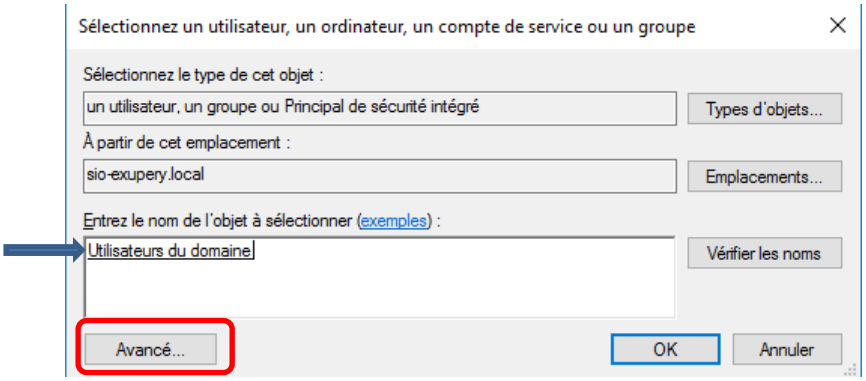
- Sélectionnez le groupe **Administrateurs** avec les boutons **Avancé** et **Rechercher** :



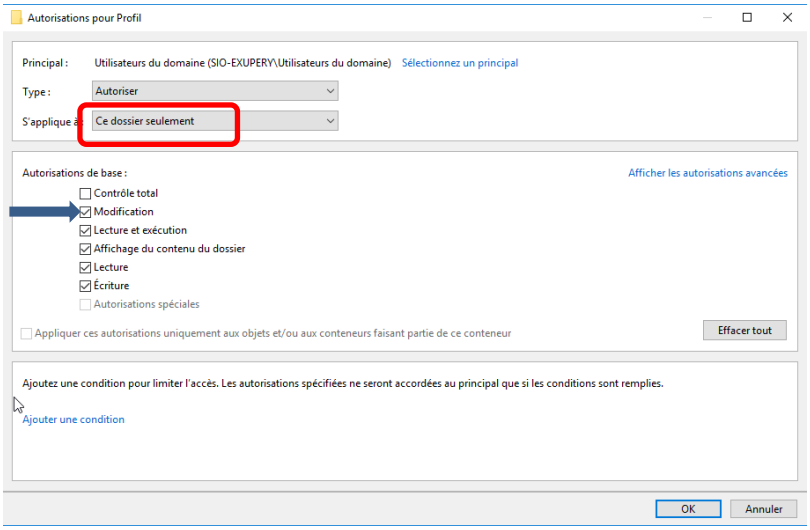
- Attribuez **Contrôle total** au groupe **Administrateurs** :



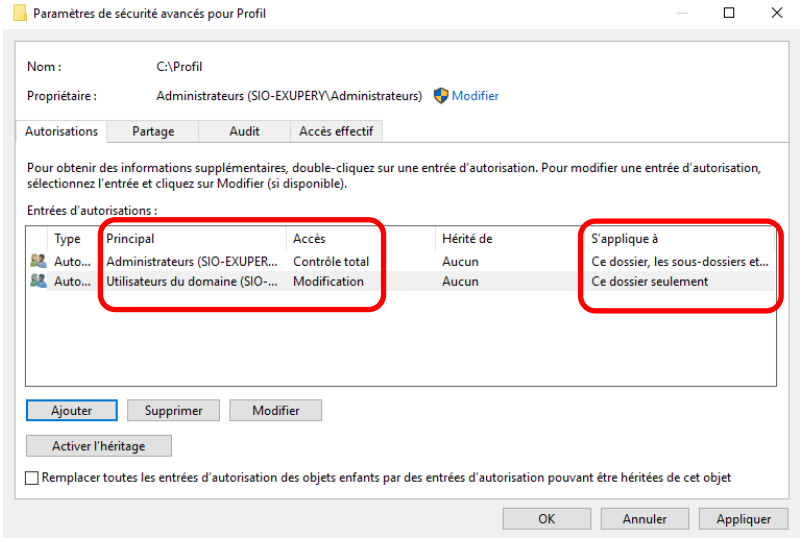
- Ajoutez de manière analogue le groupe **Utilisateurs du domaine** :



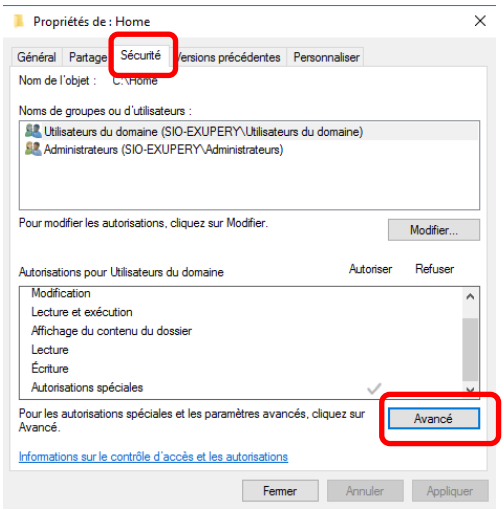
- Définissez les permissions NTFS de manière à ce que le groupe **Utilisateurs du domaine** ait accès au dossier **Profil** en **Modification** mais uniquement sur **Ce dossier seulement** (pas sur les sous dossiers). En effet, un utilisateur ne doit pas accéder avec cette autorisation de sécurité NTFS au répertoire Profil des autres utilisateurs :



- Cliquez enfin sur **Appliquer** et **OK**.

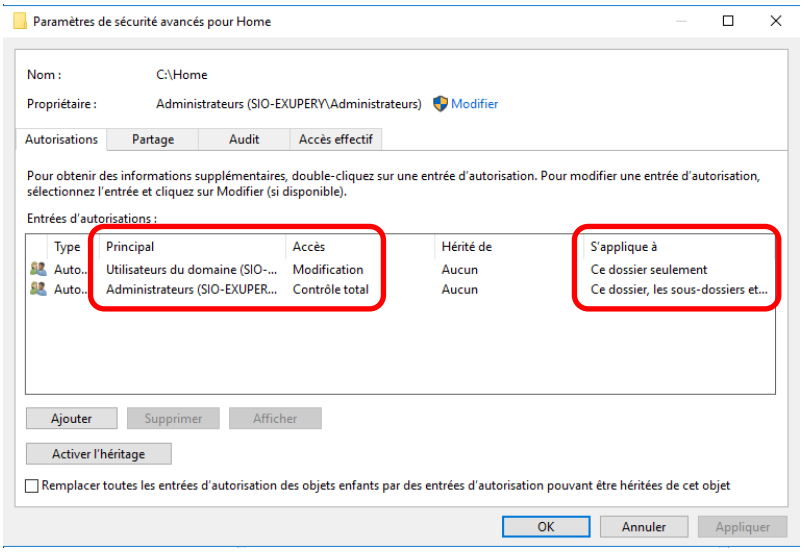


- Procédez de la même manière pour le répertoire **Home** en cliquant sur **Avancé** depuis l'onglet **Sécurité** puis en désactivant l'héritage.



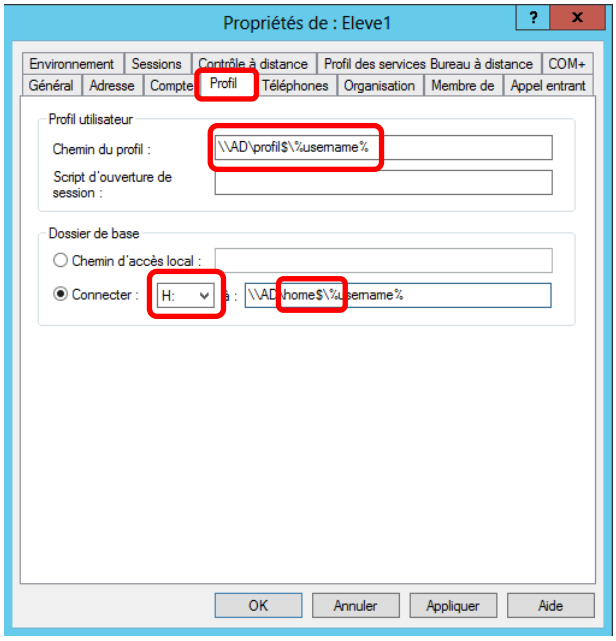
Définissez les permissions NTFS de manière à ce que le groupe **Utilisateurs du domaine** ait accès au dossier **Home** en **Modification** mais uniquement sur **Ce dossier seulement** (pas sur les sous dossiers). En effet, un utilisateur ne doit pas accéder avec cette autorisation de sécurité NTFS aux répertoires

personnels des autres utilisateurs. Attribuez **Contrôle total** au groupe **Administrateurs** pour ce dossier et à ses sous-dossiers.



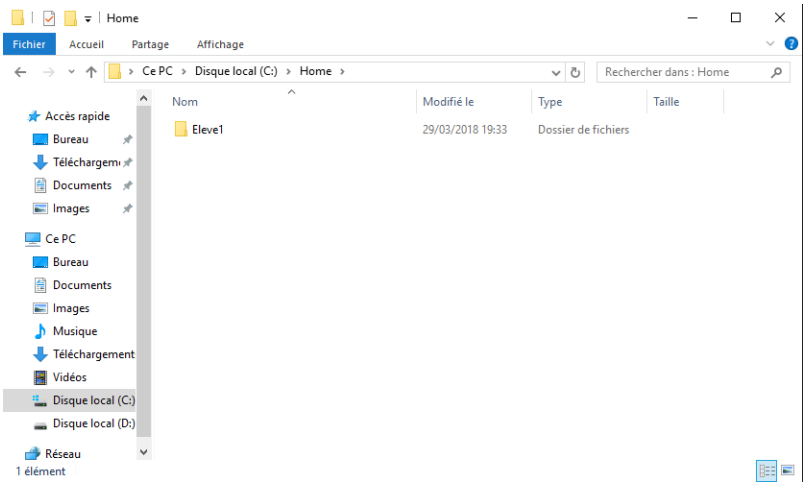
3.3. Onglet Profil de l'objet Utilisateur

- Indiquez, dans l'onglet **Profil**, le **Chemin du profil** sur le serveur ainsi que le **Dossier de base** pour l'utilisateur **Eleve1**. Le nom de l'utilisateur est remplacé par la variable d'environnement **%username%**. Après validation, c'est la valeur de la variable qui apparaît.



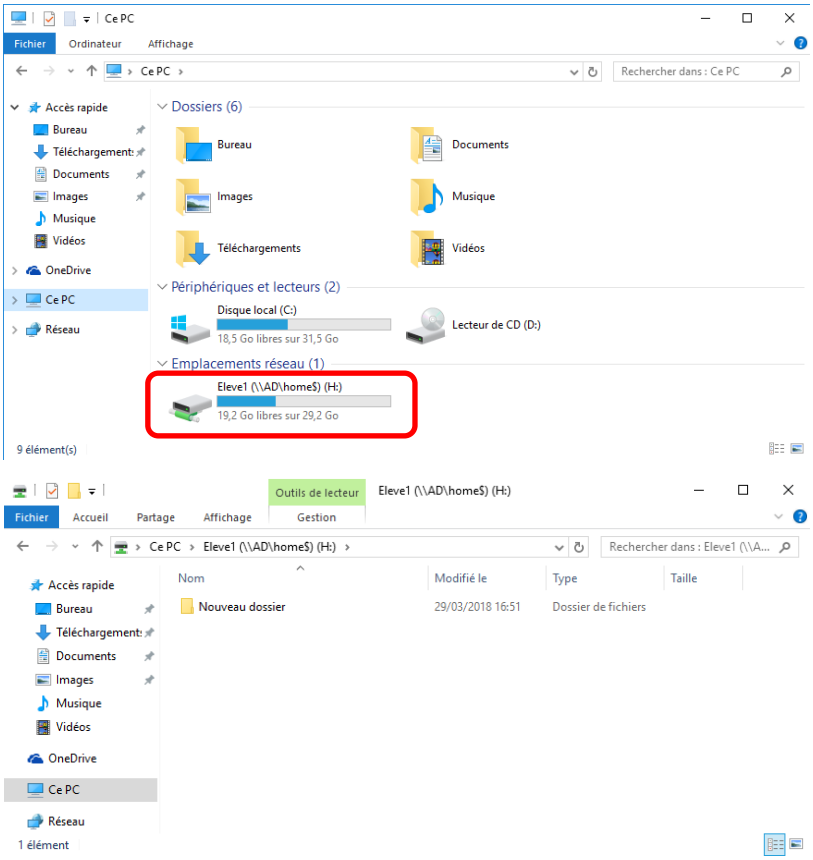
Chemin UNC pour accéder à la ressource partagée

- Constatez la création du répertoire personnel de l'utilisateur **Eleve1** :

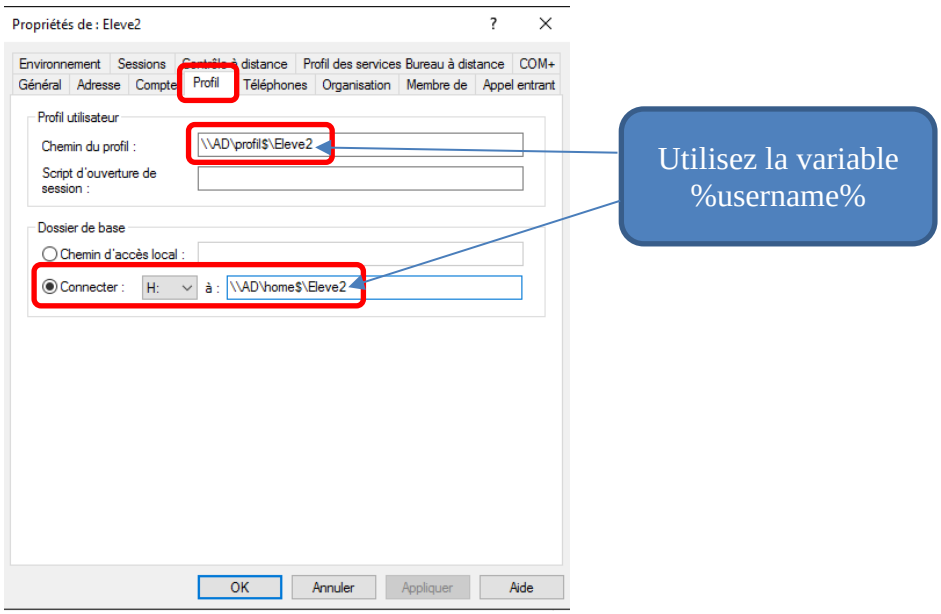


- Ouvrez une session **Eleve1** depuis WIN11

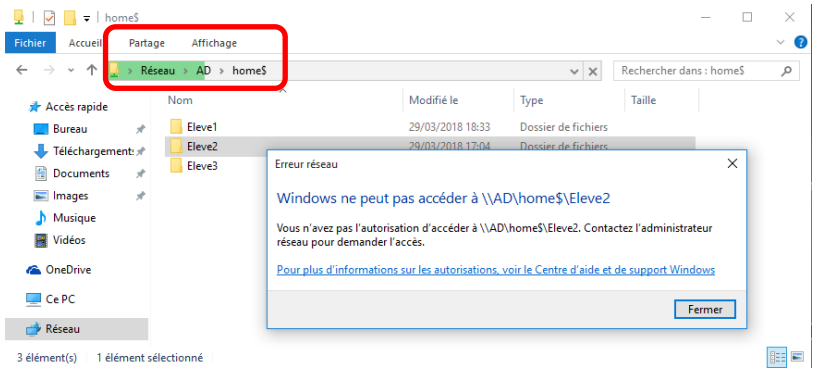
- Constatez la présence du lecteur réseau permettant l'accès au répertoire personnel de l'utilisateur :



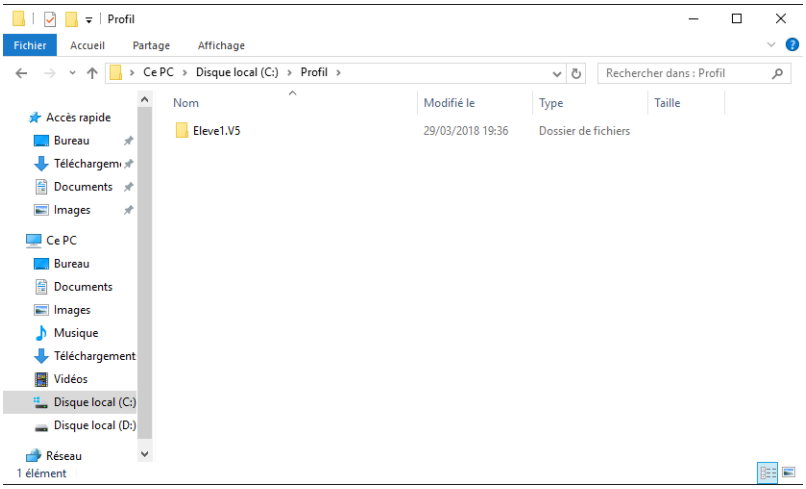
- Créez dans l'annuaire un utilisateur **Eleve2** membre du groupe **BTSSIO1** et complétez l'onglet **Profil** :



- Vérifiez depuis WIN11 que l'utilisateur **Eleve1** n'ait pas accès aux répertoires des autres utilisateurs (cf. pages 20 et 21).



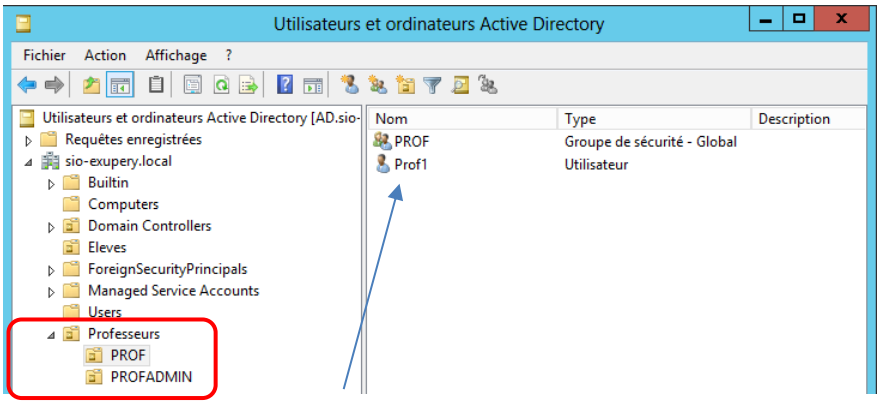
- Fermez la session de l'utilisateur **Eleve1** et constatez la présence de son profil itinérant dans le répertoire **Profil** du serveur :



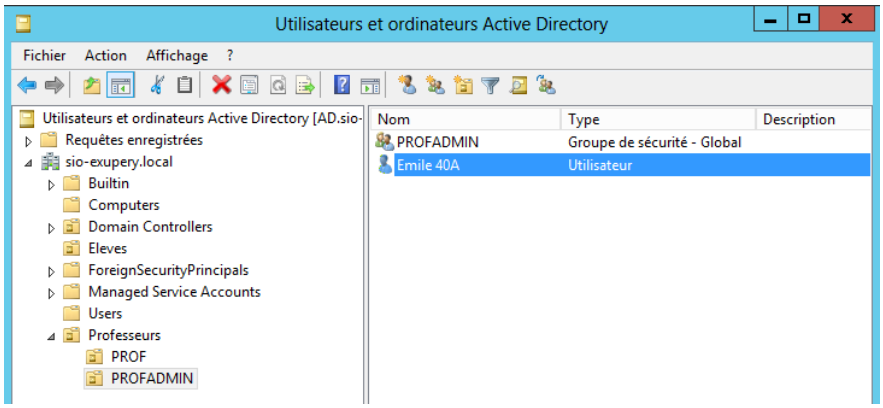
4. Structuration de l'annuaire.

L'annuaire contient pour le moment l'unité d'organisation **Eleves**. Il s'agit maintenant de créer l'UO **Professeurs** dans laquelle on créera deux autres UO se nommant **PROF** et **PROFADMIN**. Dans chacune d'entre elles, nous créerons respectivement les groupes **PROF** et **PROFADMIN**. L'objectif sera d'appliquer des **stratégies de groupe** sur les différentes UO créées (cf. Chapitre 5).

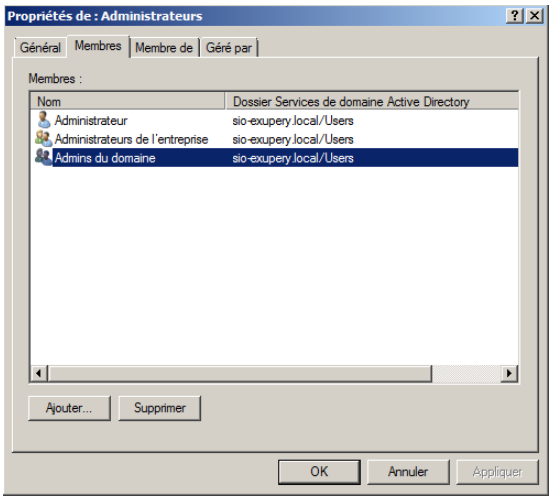
- Créez les UO **Professeurs**, **PROF** et **PROFADMIN** ainsi que les groupes **PROF** et **PROFADMIN** comme indiqué ci-dessous :



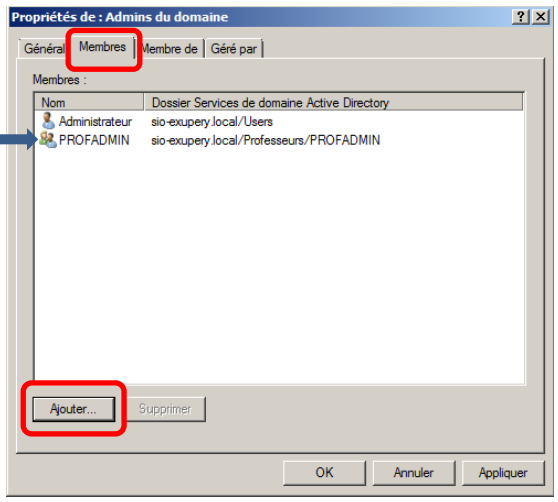
- Dans l'UO **PROF**, créez l'utilisateur **Prof1** membre du groupe **PROF**.
- Renseignez l'onglet **Profil** de la même manière que pour **Eleve1** (profil itinérant et dossier de base).
- Dans l'UO **PROFADMIN**, créez l'utilisateur **Emile 40A** membre du Groupe **PROFADMIN**. Renseignez également l'onglet **Profil** (profil itinérant et dossier de base).



Le groupe **Admins du domaine** (Users) est membre du groupe **Administrateurs** (conteneur Builtin) :



- Ajoutez le groupe **PROFADMIN** au groupe **Admins du domaine** (conteneur **Users**) :



5. Partage des répertoires communs C-SIO1 et C-PROF.

Il s'agit de procéder à la création et au partage de deux répertoires communs. Le premier, **C-SIO1**, sera à la disposition de l'ensemble des élèves membres du groupe **BTSSIO1** ainsi que des professeurs, et le second, **C-PROF**, sera réservé aux professeurs qu'ils soient membres du groupe **PROF** ou du groupe **PROFADMIN**.

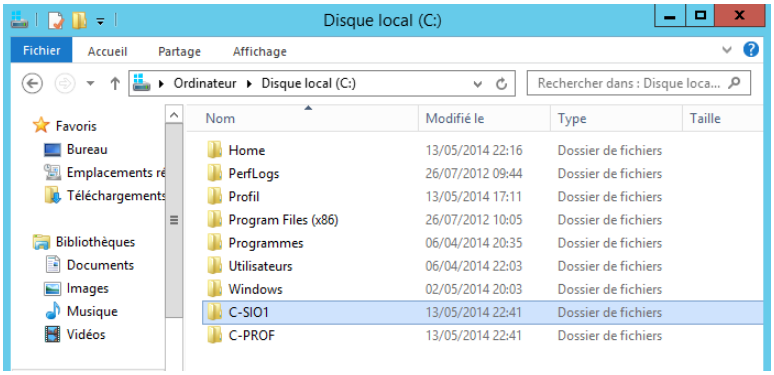
Pour ces deux répertoires, les **autorisations de partage** seront mises à **Modifier** pour le groupe **Tout le monde**.

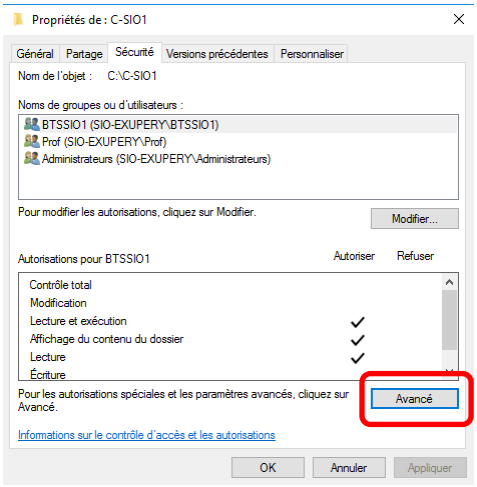
Les **autorisations de sécurité NTFS** sont les suivantes :

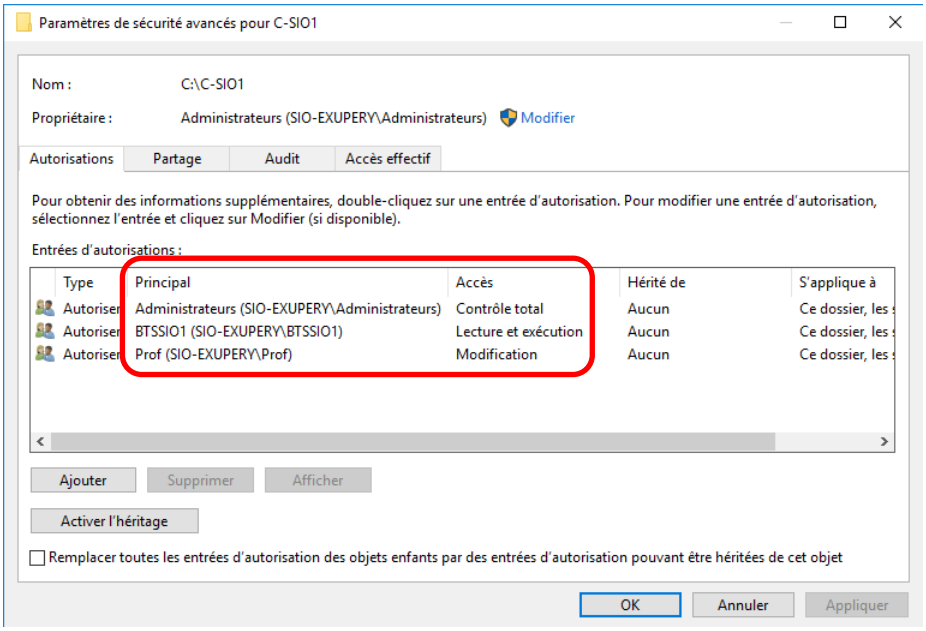
Dossier	Permissions NTFS
C:\C-SIO1	Administrateurs : **CT**, BTSSIO1 : **Lecture et Ecriture**, PROF : **Modifier**
C:\C-PROF	Administrateurs : **CT**, PROF : **Modifier**

Rappel : le groupe **PROFADMIN** fait partie du groupe **Admins du domaine** donc du groupe **Administrateurs**.

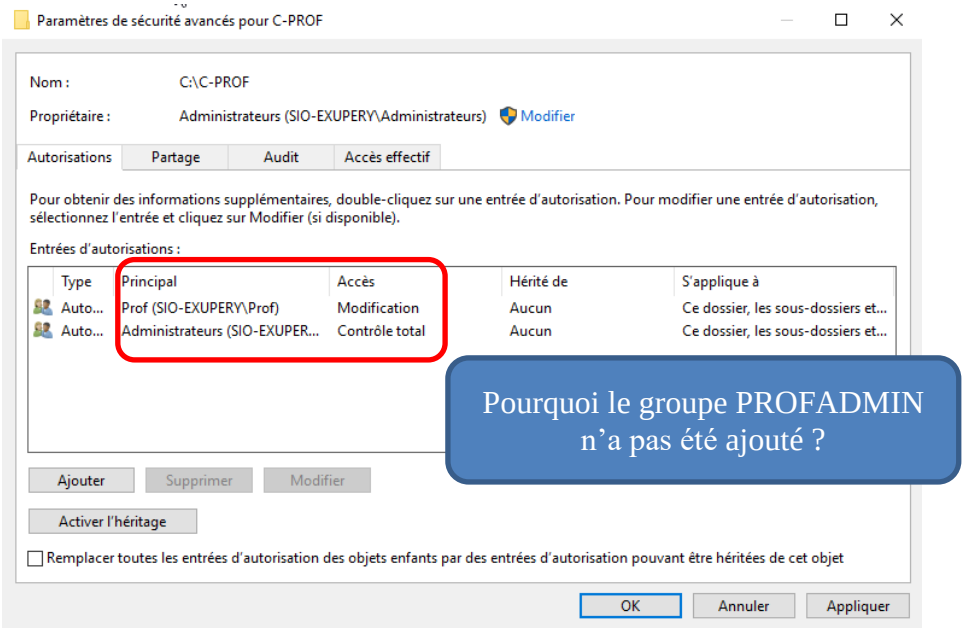
- Créez, à la racine du **Disque local (C:)**, le répertoire **C-SIO1**. Partagez le dossier et définissez les autorisations de partage indiquées au-dessus du tableau ci-dessus. Dans l'onglet **Sécurité**, cliquez sur **Avancé**, désactivez l'héritage et définissez les autorisations de sécurité suivant les indications du tableau ci-dessus :







- Créez, à la racine du **Disque local (C:)**, le répertoire **C-PROF**. Partagez le dossier et définissez les autorisations de partage (cf. page précédente). Dans l'onglet **Sécurité**, cliquez sur **Avancé**, désactivez l'héritage et définissez les autorisations de sécurité (cf. tableau page précédente) :



➔ Vous pouvez ajouter le groupe **PROFADMIN** mais il est de toute manière membre du groupe **Administrateurs** puisqu'il est membre du groupe **Admins du domaine**.