


CONFIGURATION ET GESTION D'UN DOMAINE

PARCOURS	SISR <input checked="" type="checkbox"/>	SLAM <input type="checkbox"/>
-----------------	---	--------------------------------------

Lieu de réalisation	Campus Montsouris	
Période de réalisation	Du : 14.06.2024	Au :
Modalité de réalisation	SEUL <input checked="" type="checkbox"/>	EN EQUIPE <input type="checkbox"/>

Intitulé de la mission	Configuration et gestion d'un domaine AD
Description du contexte de la mission	Configurer un domaine Active Directory et gérer les accès des utilisateurs à des dossiers partagés

Contraintes & Résultat	Ressources fournies / contraintes techniques / Résultats attendu
	VirtualBox, Windows Server 2022, Windows 11
Productions associées	Liste des documents produits et description

Modalités d'accès aux productions	Identifiants, mots de passe, URL d'un espace de stockage et présentation de l'organisation du stockage

Configuration et gestion d'un domaine AD

1. Configuration du rôle AD

La mission commence avec la configuration du rôle Active Directory sur la machine virtuelle accueillant le serveur Windows Server 2022.

2. Création du volume secondaire

La mission se poursuit avec la création d'un volume secondaire. Nous avons au préalable créer et ajouter, dans les paramètres VirtualBox, un disque physique de 5go à notre serveur. Dans le gestionnaire des disques, sélectionner le disque "non alloué", et à l'aide de l'assistant création d'un volume simple, créer un volume, appelé "fichiers", en format NTFS.

3. Création du dossier partagé

La création d'un dossier partagé sur le serveur se fait en allant dans "services de fichier et de stockage", présent par défaut sur le serveur. Puis aller dans "Partage", et faire un clic droit, et sélectionner "nouveau partage".

4. Gestion des droits d'accès

Afin de réglementer quel utilisateur a accès à quel partage, on va dans les propriétés de chaque partage créé. Par la suite, cliquer sur Modifier.

5. Entrée du client dans le domaine

Sur la machine du client, on adresse la machine afin qu'il se trouve dans le même réseau que celui du serveur AD (@réseau = 10.12.0.0/24). On peut soit le faire en automatique (DHCP), soit en statique. On choisit la seconde option.

De plus, on rajoute l'adresse du serveur AD en DNS.

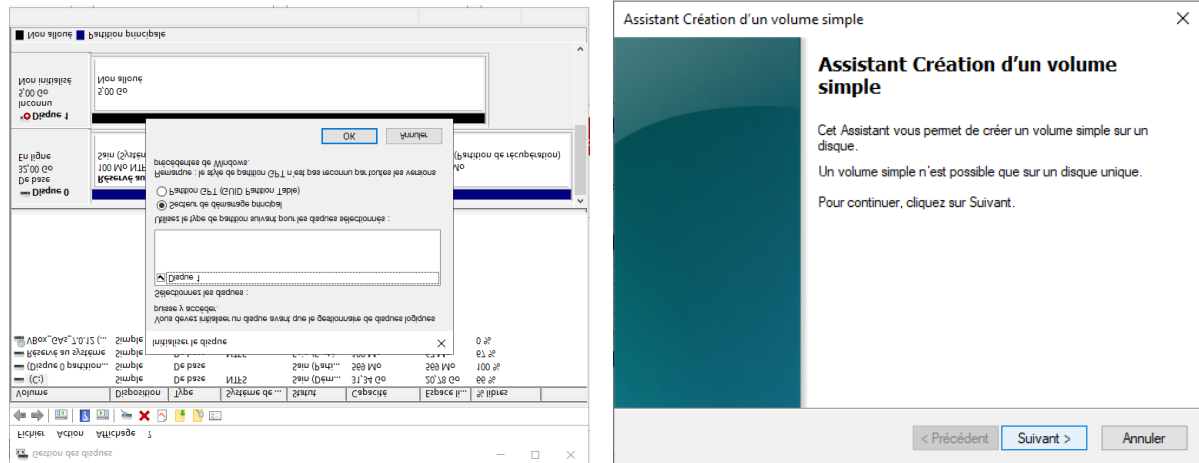
6. Evaluation des accès

Avec un utilisateur de chaque groupe (4 groupes, 15 utilisateurs), on test l'entrée dans le domaine en se connectant avec l'adresse, configurée en prénom.nom@nomdedomaine.lan. Puis, on connecte en lecteur réseau, dans l'explorateur de fichiers, les partages qu'on a créés (5 partages). En fonction du partage sur lequel l'utilisateur est, il a des droits en lecteur et écriture, seulement en lecture, les droits d'administration, ou n'a pas le droit d'accès au partage.

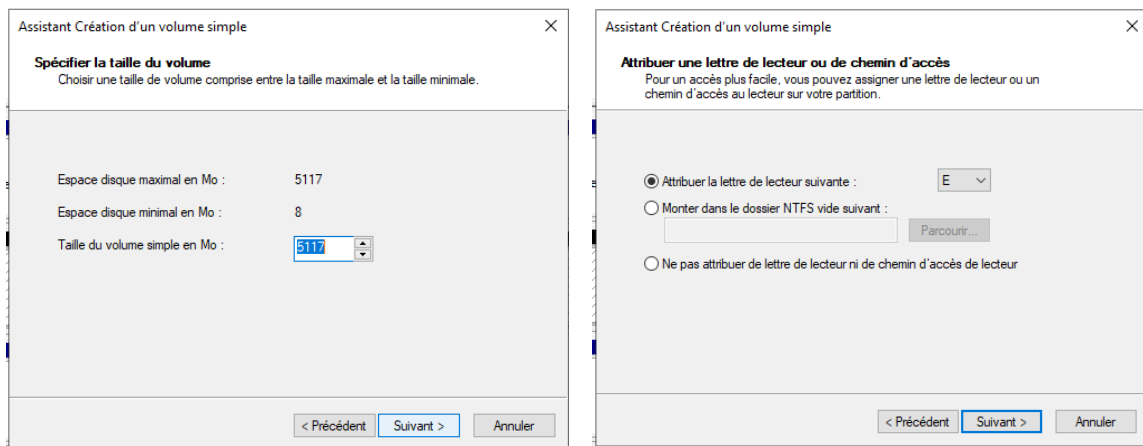
Configuration et gestion d'un domaine AD

1. Création de volume

Le disque physique secondaire de 5go a été rajouté auparavant dans les paramètres VirtualBox. Dans la VM, aller dans “gestionnaire des disques”, puis clic droit sur le disque secondaire, noté “non alloué”. Cliquer sur ok pour ouvrir l’assistant de création d’un volume simple. Cliquer sur Suivant.



Préciser la taille du disque physique que l’on souhaite allouer au volume logique. On choisit l’entièreté du disque. Cliquer sur Suivant. On choisit d’attribuer la lettre par défaut. Cliquer sur Suivant.



Configuration et gestion d'un domaine AD

On formate le disque avec le format par défaut NTFS, et on lui donne le nom de “fichiers”.

Assistant Création d'un volume simple

Formater une partition
Pour stocker des données sur cette partition, vous devez d'abord la formater.

Indiquez si vous voulez formater cette partition, et le cas échéant, les paramètres que vous voulez utiliser.

☐ Ne pas formater ce volume

☒ Formater ce volume avec les paramètres suivants :

Système de fichiers : NTFS

Taille d'unité d'allocation : Par défaut

Nom de volume : Nouveau nom

☒ Effectuer un formatage rapide

☐ Activer la compression des fichiers et dossiers

< Précédent Suivant > Annuler

Notre disque secondaire a un nouveau volume logique nommé “Fichiers”.

Assistant Création d'un volume simple

Fin de l'Assistant Création d'un volume simple

L'Assistant Création d'un volume simple est terminé.

Vous avez spécifié les paramètres suivants :

Type du volume : Volume simple
Disques sélectionnés : Disque 1
Taille du volume : 5117 Mo
Lettre de lecteur ou chemin d'accès : E:
Système de fichiers : NTFS
Taille d'unité d'allocation : Par défaut

Pour fermer cet Assistant, cliquez sur Terminer.

< Précédent Terminer Annuler

Disque 1	
De base	Fichiers
5,00 Go	5,00 Go NTFS
En ligne	Sain (Partition principale)

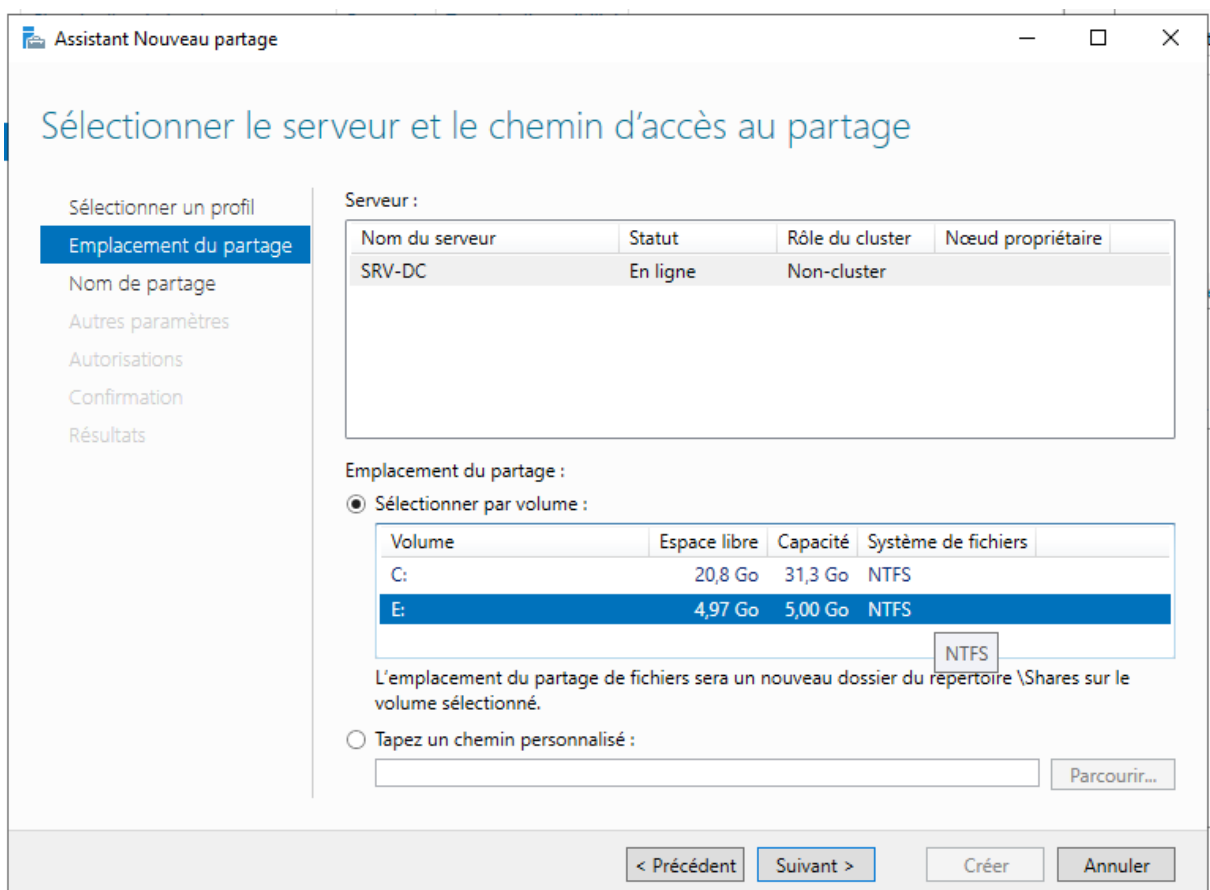
Configuration et gestion d'un domaine AD

1) Création d'un dossier partagé

Aller dans “services de fichier et de stockage”, présent par défaut sur le serveur. Puis aller dans “Partage”, et faire un clic droit, et sélectionner “nouveau partage”.



On choisit le disque sur lequel créer le partage. Ici, celui de 5go.



Configuration et gestion d'un domaine AD

On donne un nom au partage et une description.

The screenshot shows the 'Assistant Nouveau partage' window with the 'Nom de partage' step selected in the left sidebar. The main area contains the following fields:

- Nom du partage :** A text box containing 'Partage'.
- Description du partage :** A text box containing 'Serveur de fichier sur le disque secondaire de 5go'.
- Chemin d'accès local au partage :** A text box containing 'E:\Shares\Partage'. Below it is a blue information icon and the text 'Si le dossier n'existe pas, il est créé.'
- Chemin d'accès distant au partage :** A text box containing '\\SRV-DC\Partage'.

At the bottom, there are four buttons: '< Précédent', 'Suivant >', 'Créer', and 'Annuler'.

On configure les paramètres additionnels.

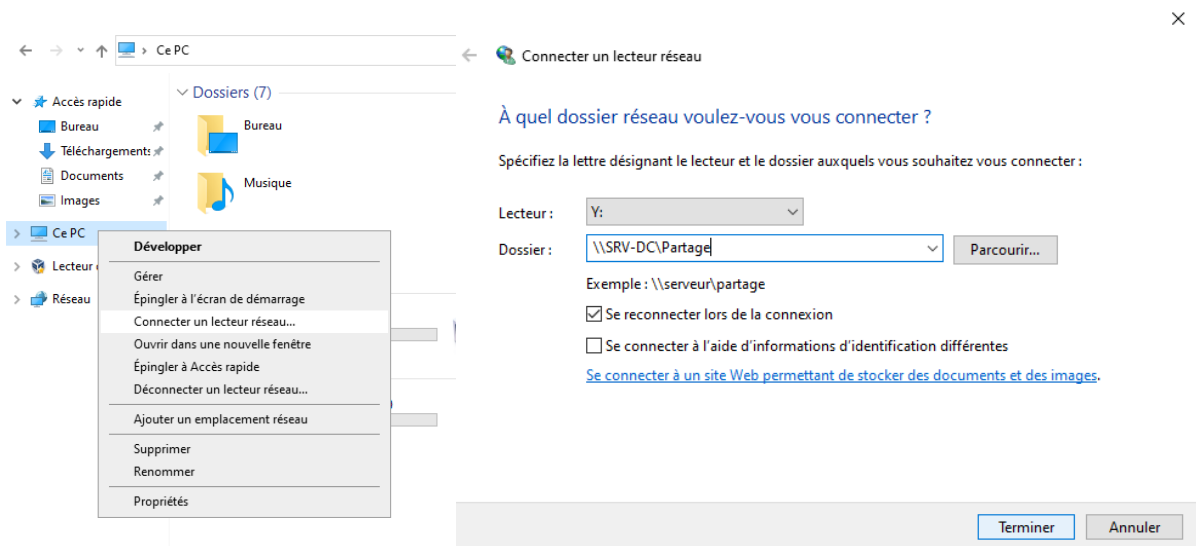
The screenshot shows the 'Assistant Nouveau partage' window with the 'Configurer les paramètres de partage' step selected in the left sidebar. The main area contains the following options:

- ☒ **Activer l'énumération basée sur l'accès**
L'énumération basée sur l'accès n'affiche que les fichiers et les dossiers dont un utilisateur possède les autorisations d'accès. S'il ne bénéficie pas d'autorisations en lecture (ou équivalentes) sur un dossier, Windows cache alors ce dernier de l'utilisateur.
- ☒ **Autoriser la mise en cache du partage**
La mise en cache met le contenu du partage à la disposition des utilisateurs hors connexion. Si la fonctionnalité BranchCache du service de rôle Fichiers réseau est installée, vous pouvez activer BranchCache sur le partage.
 - ☐ **Activer le cache de filiale (BranchCache) sur le partage de fichiers**
BranchCache permet aux ordinateurs d'une succursale de mettre en cache les fichiers téléchargés à partir de ce partage, puis de les rendre disponibles en toute sécurité pour les autres ordinateurs de la succursale.
- ☐ **Chiffrer l'accès aux données**
Lorsqu'il est activé, l'accès distant aux fichiers de ce partage est chiffré. Cela a pour effet de sécuriser les données contre tout accès non autorisé lors de leur transfert vers ou depuis le partage. Si cette case à cocher est activée et grisée, cela signifie qu'un administrateur a activé le chiffrement pour l'ensemble du serveur.

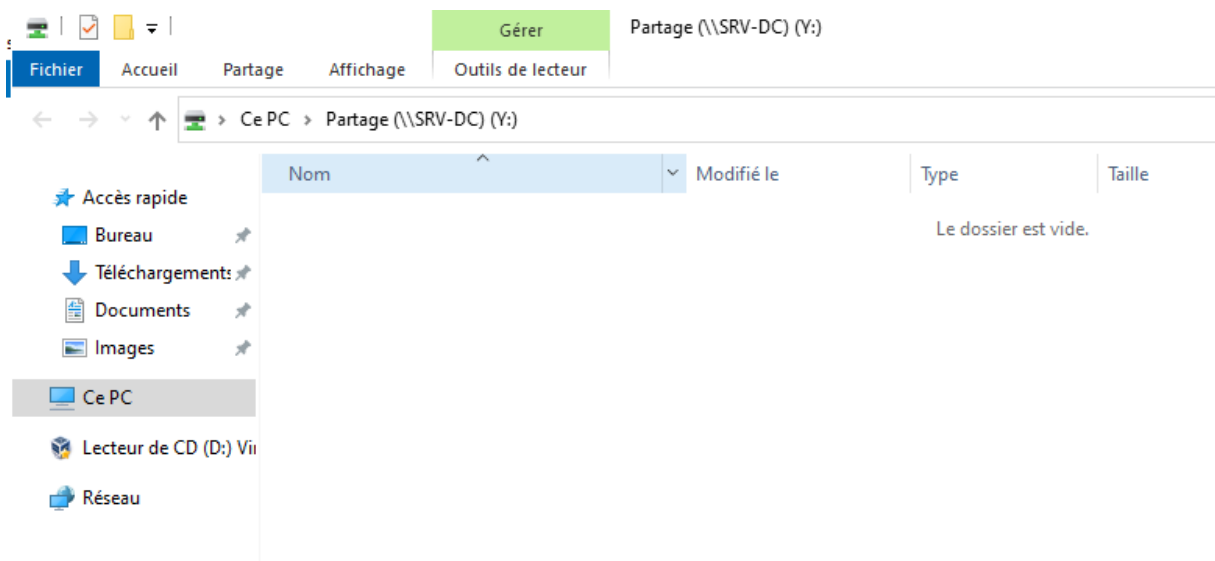
At the bottom, there are four buttons: '< Précédent', 'Suivant >', 'Créer', and 'Annuler'.

Configuration et gestion d'un domaine AD

Maintenant pour connecter un lecteur réseau, aller dans l'explorateur de fichiers Windows. Clic droit sur "Ce PC", sélectionner "connecter un lecteur réseau". Une nouvelle fenêtre s'ouvre, où il faut entrer le chemin du partage. Celui-ci est composé de 2 antislashes, le nom du serveur de fichiers, antislash, le nom du partage.



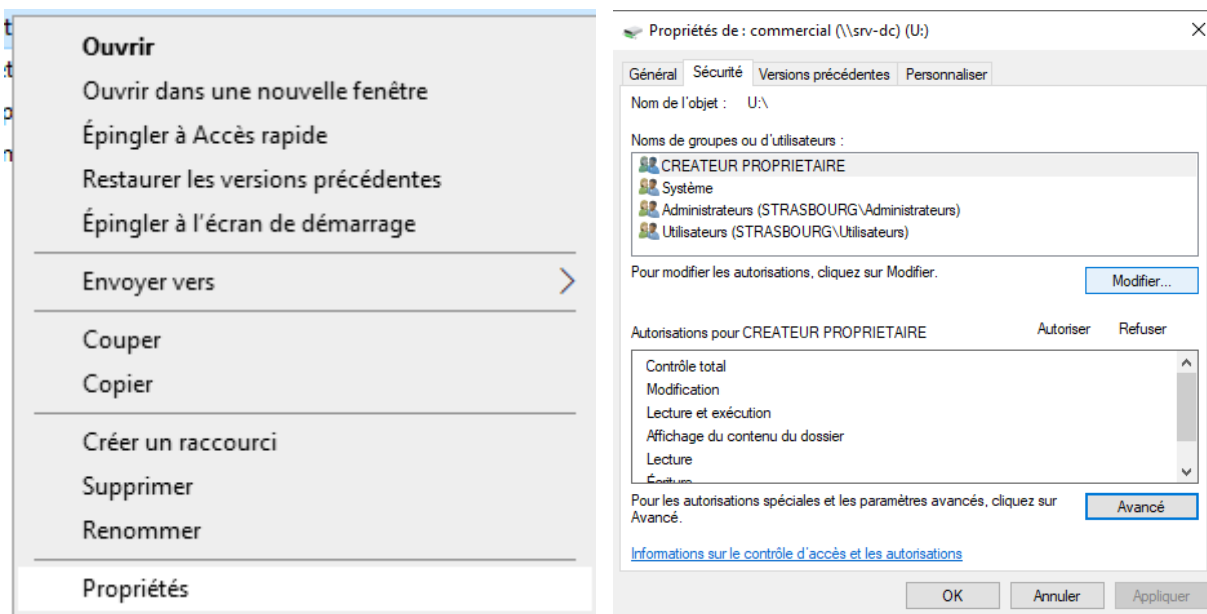
Nous avons bien accès au partage.



Configuration et gestion d'un domaine AD

2. Gestion des accès

Afin de régler quel utilisateur a accès à quel partage, on va dans les **propriétés** de chaque partage créé. Par la suite, cliquer sur **Modifier**.



Ici, il y a 4 groupes présents par défaut : utilisateurs, qui sont l'ensemble des utilisateurs créés par défaut dans l'Active Directory et ceux créés par la suite par l'administrateur, administrateurs, système et créateur propriétaire.

L'onglet sécurité nous permet d'ajouter ou de supprimer des groupes. Ici, nous allons ajouter des groupes de travail que l'on a auparavant créés dans notre active directory.

Ensuite, chaque groupe possède un niveau d'autorisation, illustré en 2 colonnes, celles d'autorisations ou d'interdictions, et concernant différentes actions : l'affichage, la lecture, l'écriture, la modification ou les droits totaux.

De base, le groupe par défaut "utilisateurs" possède des droits en écriture et lecture qui concernent tous les utilisateurs de l'AD. On retire ces droits en décochant les cases sous la colonne "Autoriser". Pour régler au cas par cas, on peut cocher ou décocher les cases dans les colonnes d'autorisation ou d'interdiction.

Ici, pour le dossier partagé "commercial", nous rajoutons les groupes "commercial", "direction". On attribue à ces deux groupes des droits en lecture et en écriture. De plus, l'utilisateur "responsable désigné" du groupe commercial se voit attribué l'entière responsabilité des droits, en cochant dans la colonne autorisé la ligne "contrôle total".

Configuration et gestion d'un domaine AD

Autorisations pour commercial (\srv-dc) (U:)

Sécurité

Nom de l'objet : U:\

Noms de groupes ou d'utilisateurs :

- Système
- Administrateurs (STRASBOURG\Administrateurs)
- commercial (STRASBOURG\commercial)**
- direction (STRASBOURG\direction)
- responsable commercial (STRASBOURG\responsable commerciale)

[Ajouter...] [Supprimer]

Autorisations pour commercial	Autoriser	Refuser
Contrôle total	<input type="checkbox"/>	<input type="checkbox"/>
Modification	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lecture et exécution	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Affichage du contenu du dossier	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lecture	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[Informations sur le contrôle d'accès et les autorisations](#)

[OK] [Annuler] [Appliquer]

De plus, on retire le groupe par défaut “utilisateurs” de chacun des dossiers partagés.

Propriétés de : secretariat (\\srv-dc) (W:)

Général Sécurité Versions précédentes Personnaliser

Nom de l'objet : W:\

Noms de groupes ou d'utilisateurs :

- direction (STRASBOURG\direction)
- secretariat avec responsable désigné (STRASBOURG\secretariat)
- responsable secretariat (STRASBOURG\responsable secretariat)
- Administrateurs (STRASBOURG\Administrateurs)

Pour modifier les autorisations, cliquez sur Modifier.

Modifier...

Autorisations pour CREATEUR PROPRIETAIRE

	Autoriser	Refuser
Contrôle total		
Modification		
Lecture et exécution		
Affichage du contenu du dossier		
Lecture		

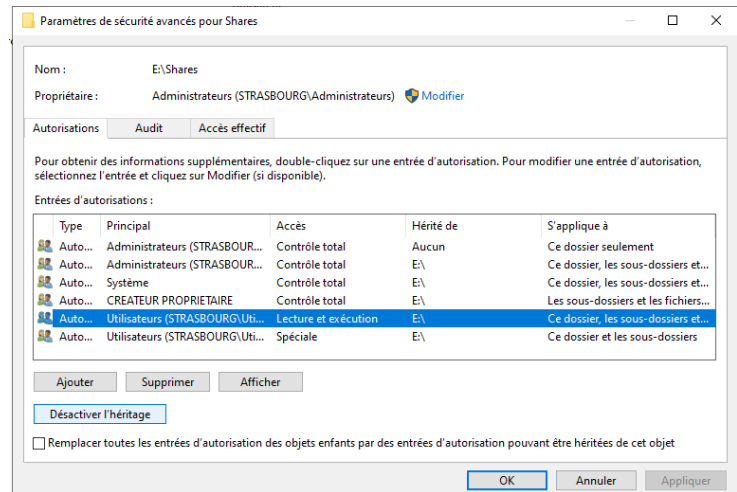
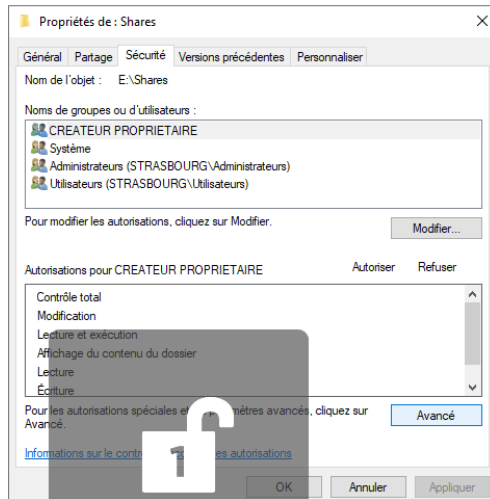
Pour les autorisations spéciales et les paramètres avancés, cliquez sur Avancé.

[Informations sur le contrôle d'accès et les autorisations](#)

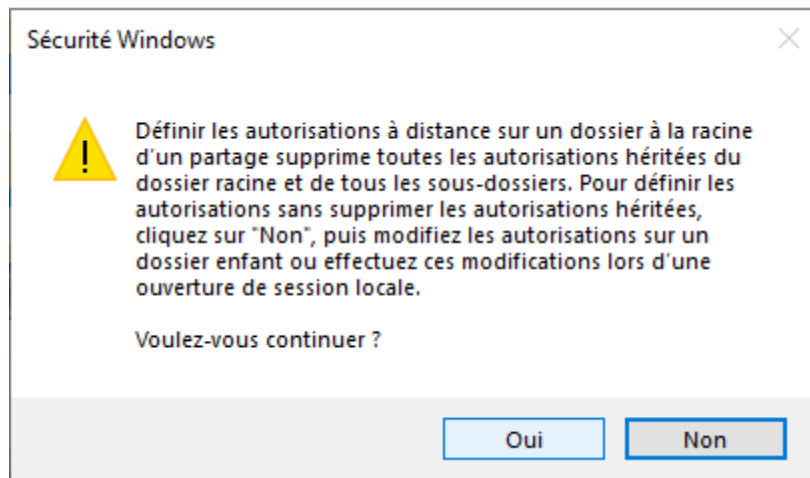
OK Annuler Appliquer

Configuration et gestion d'un domaine AD

Sur certains dossiers partagés, on ne peut par défaut supprimer le groupe utilisateurs. Il faut désactiver l'option d'héritage des autorisations. Pour cela, aller dans l'onglet "avancé", puis sélectionner les groupes utilisateurs et cliquer sur "désactiver l'héritage".



On valide en cliquant sur "oui".

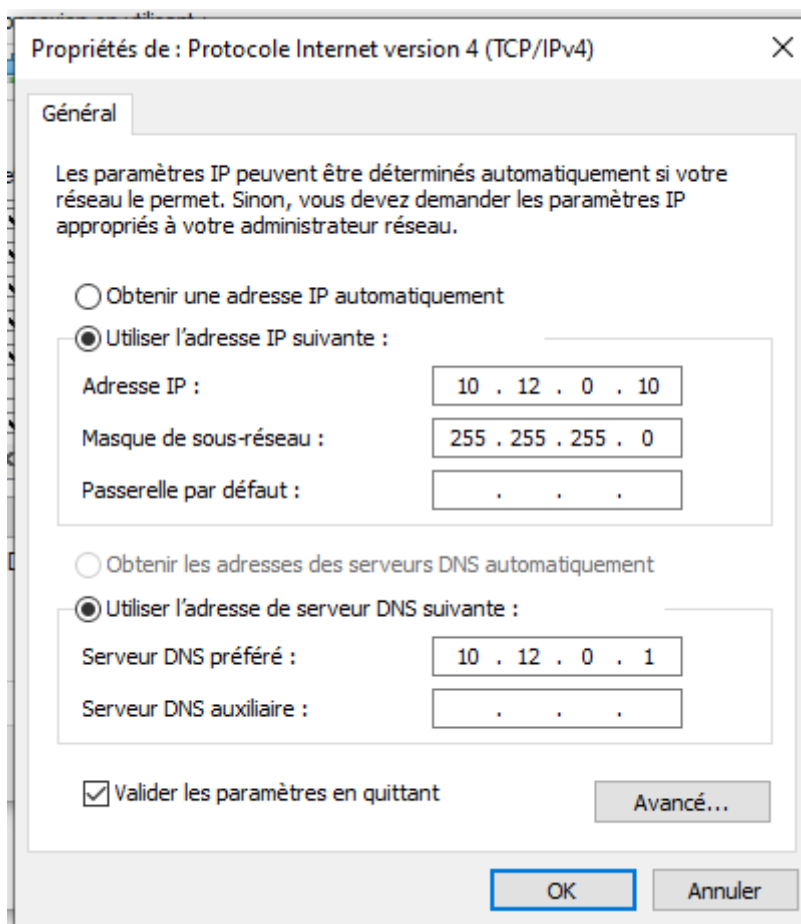


Configuration et gestion d'un domaine AD

A) Entrée dans le domaine

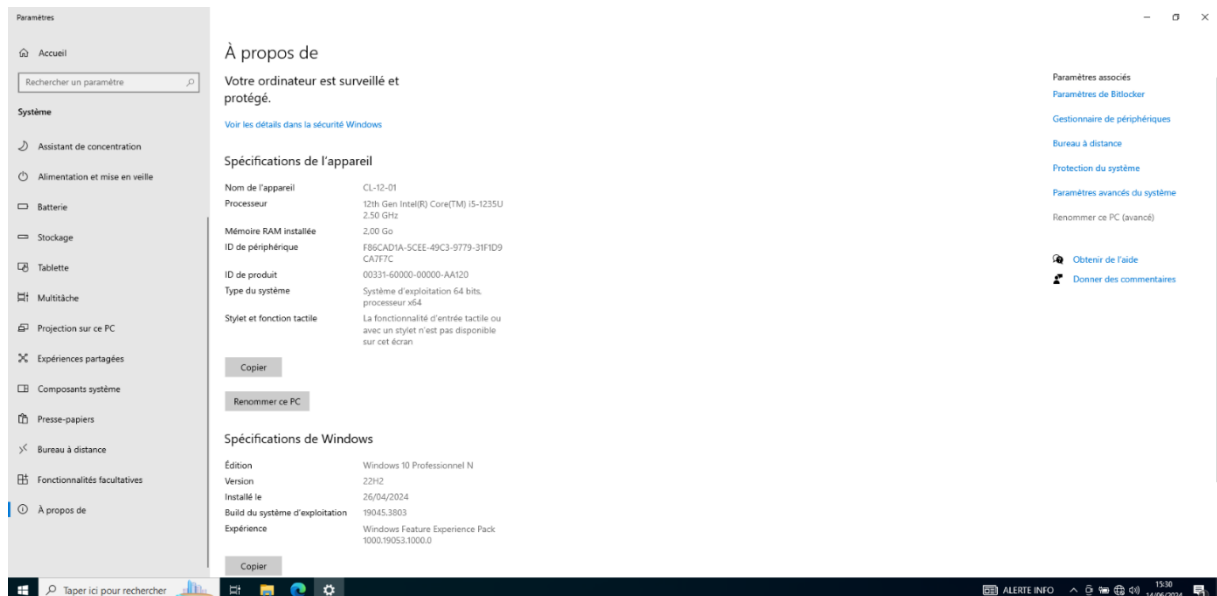
On adresse le client afin qu'il se trouve dans le même réseau que celui du serveur AD (@réseau = 10.12.0.0/24). On peut soit le faire en automatique (DHCP), soit en statique. On choisit la seconde option.

De plus, on rajoute l'adresse du serveur AD en DNS.

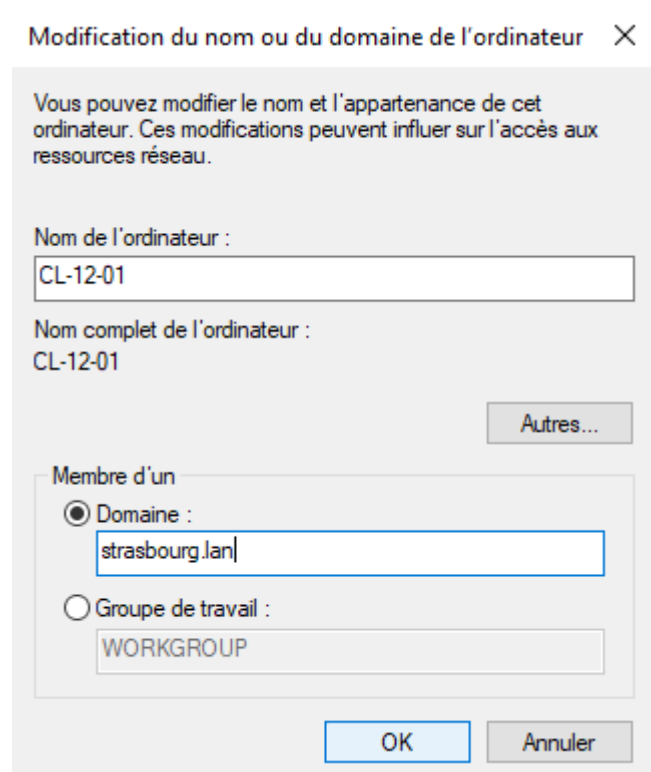
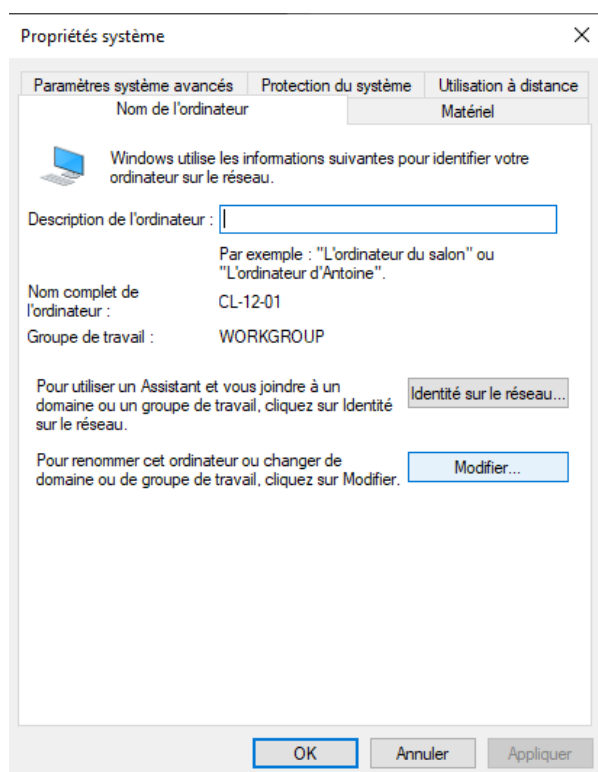


Configuration et gestion d'un domaine AD

Par la suite, aller dans **paramètres**, puis à **propos de**, puis sur “renommer ce pc (avancé)”.

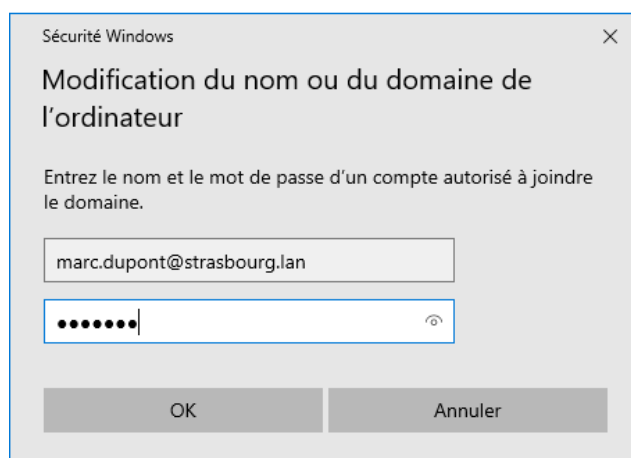


Aller sur **Modifier**, puis rajouter le nom du domaine dans la fenêtre qui s'ouvre. Ici, il s'agit du domaine *strasbourg.lan*.

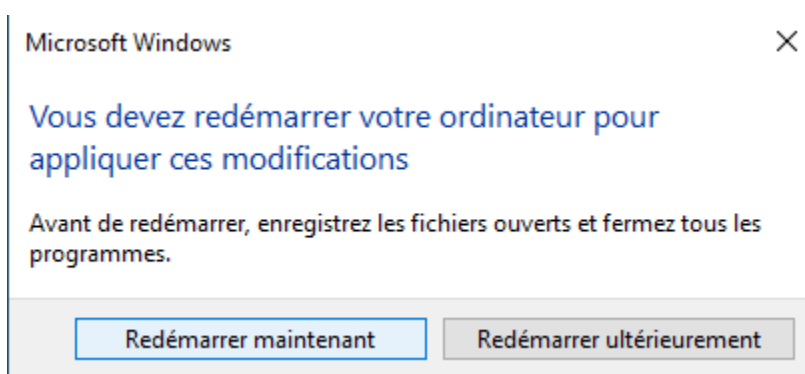
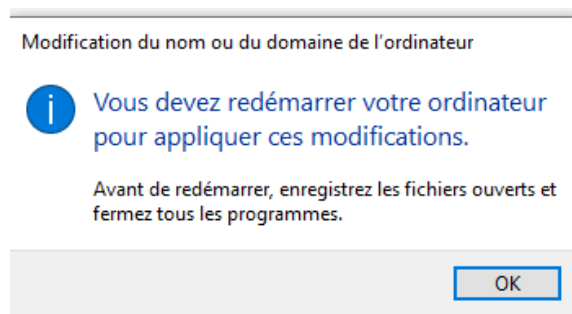
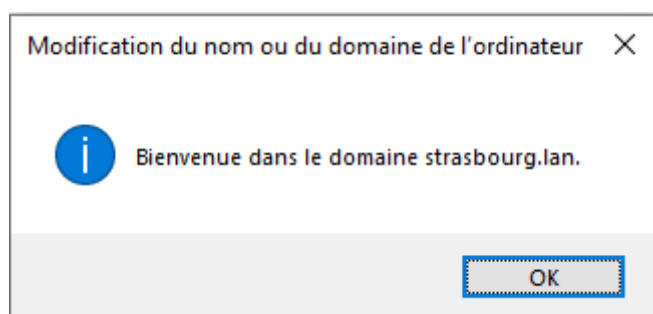


Configuration et gestion d'un domaine AD

Une nouvelle fenêtre s'ouvre, on entre l'identifiant d'un des utilisateurs que nous avons configurés plus haut, avec son mot de passe.



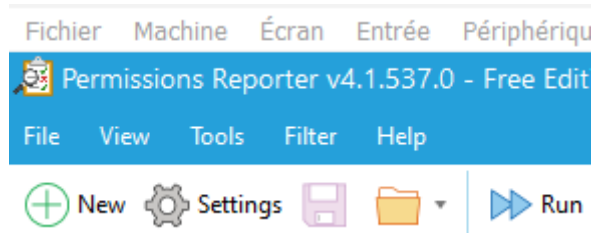
L'entrée dans le domaine est un succès. Un redémarrage est nécessaire.



Configuration et gestion d'un domaine AD

B) Audit des accès

Afin d'auditer les droits d'accès (ACL), on installe l'outil "Permissions Reporter". Lorsque celui-ci est installé, on clique sur "Run".



Lorsque l'analyse est finie, l'outil nous propose une vue sur l'entièreté des permissions des différents dossiers et fichiers du système. Parmi eux, ceux du disque principal C:\ et du disque secondaire E:\, accueillant nos dossiers partagés.

Dans ce dernier, on peut voir les 5 dossiers partagés que nous avons paramétrés auparavant : commercial, commun, comptabilité, direction et secrétariat.

General

PATH: E:\\$RECYCLE.BIN
OWNER: BUILTIN\Administrateurs
MODIFIED: 21/06/2024 09:23:16
SUBFOLDER COUNT: 1
INHERITED: No
SCAN STATE: Complete

Permissions

Type	Inherited	Account	Basic Permissions	Scope
Allow	No	BUILTIN\Administrateurs	Full control	This folder, subfolders, and files
Allow	No	AUTORITE NT\Système	Full control	This folder, subfolders, and files
Allow	No	BUILTIN\Utilisateurs	Special	This folder only

Subfolders 5 total 1 immediate 1 non-inheriting 1 immediate non-inheriting

Name	Owner	Inherited	Subfolders	Subfolders (Total)	Subfolders Not Inheriting
S-1-5-21-1760288615-1551125...	BUILTIN\Administrateurs	No	4	4	0