RAPPORT

BTS SIO - E5

Situation professionnelle n°2

Déploiement et sécurisation d'un espace de stockage partagé collaboratif

03/02/2026

Contexte et Problématique :

Une PME possède des données dispersées sur plusieurs postes de travail, sans sauvegarde centralisée ni gestion des droits. Cette situation pose des risques critiques : perte de données en cas de panne disque, accès non autorisés à des documents confidentiels (RH, Direction), et saturation de l'espace de stockage par des fichiers personnels (vidéos, musiques). La demande : Centraliser les données sur un serveur sécurisé, garantir la redondance des disques, cloisonner les accès par service et contrôler le type de fichiers stockés.

NOM	DATE	TAMPON
CHERIF SOULEYMANE	03/02/2026	

SOMMAIRE :

1. LE CAHIER DES CHARGES :

1. Objectif principal :

L'objectif est de déployer un espace de stockage centralisé (File Server) sous Windows Server 2022 pour assurer la persistance, la confidentialité et l'intégrité des données de l'entreprise. Le service doit être capable de résister à une panne matérielle (disque) et d'empêcher tout accès non autorisé aux dossiers sensibles.

1.2. Choix techniques :

Environnement technologique :

- Hyperviseur : VMware Workstation 17 PRO
- Serveur : Windows Server 2022 (Rôle Serveur de fichiers, AD DS).
- Clients : Postes Windows 10 intégrés au domaine.
- Réseau : Contrôleur de domaine (AD), DNS, adressage IP statique serveur, PfSense.
- Stockage : 2 disques virtuels dédiés aux données (configuration RAID).

1.3. Prérequis :

- Un serveur Windows Server 2022 déjà promu Contrôleur de Domaine (AD DS).
- Deux disques durs virtuels vierges (non initialisés) de taille identique ajoutés à la VM.
- Un poste client Windows 10 joint au domaine pour les tests.
- Un compte administrateur du domaine.

1.4. Compétences :

Compétences du référentiel mises en œuvre :

- Analyse du cahier des charges d'un service à produire.
- Installation et configuration d'éléments d'infrastructure (Serveur de fichiers).
- Sécurisation des équipements et des usages (Permissions NTFS, ACL).
- Installation et configuration d'éléments de gestion du stockage (RAID, Quotas).
- Recueil d'informations sur une configuration et ses éléments (Tests de validation).

1.5. **Déroulement :**

Phase 1 : Fiabilisation du stockage (Disponibilité)

- Ajout de deux disques durs virtuels physiques au serveur (10Go).
- Configuration d'un volume en RAID 1 (Miroir) via le Gestionnaire de disques pour assurer la redondance des données en cas de panne physique d'un disque.

Phase 2 : Structuration et Gestion des identités

- Création d'une arborescence logique conforme à l'organigramme (Dossiers : Direction, Compta, Commun).
- Création des groupes de sécurité globaux dans l'Active Directory (G_Compta, G_Direction) et intégration des utilisateurs (dir_user et compta_user)

Phase 3 : Sécurisation des accès (Confidentialité)

- Désactivation de l'héritage des droits NTFS sur les dossiers racines.
- Application du principe de moindre privilège via les ACL (Access Control Lists) :
  - Direction : Accès total pour la direction, accès refusé pour les autres.
  - Public : Lecture seule pour les stagiaires, Modification pour les employés.
  - Validation technique : Vérification des accès effectifs (''Access Denied'') avec un compte utilisateur.

Phase 4 : Optimisation et Contrôle (Gestionnaire de ressources FSRM)

- Installation du rôle FSRM (File Server Resource Manager).
- Mise en place de Quotas stricts (limite de 500mo pour éviter la saturation).
- Configuration du Filtrage de fichiers : Interdiction d'enregistrer des extensions non professionnelles (.mp3, .avi, .exe,...) pour protéger le serveur contre les malwares et l'usage abusif.

1.6. **Contraintes :**

- **Contrainte technique** : Le serveur doit disposer de suffisamment de RAM pour supporter le rôle FSRM sans ralentissement.
- **Contrainte de sécurité** : L'héritage des droits NTFS doit être rompu sur les dossiers sensibles pour éviter les fuites de données.
- **Contrainte organisationnelle** : La structure des dossiers doit refléter exactement l'organigramme de la PME pour ne pas perturber les utilisateurs.

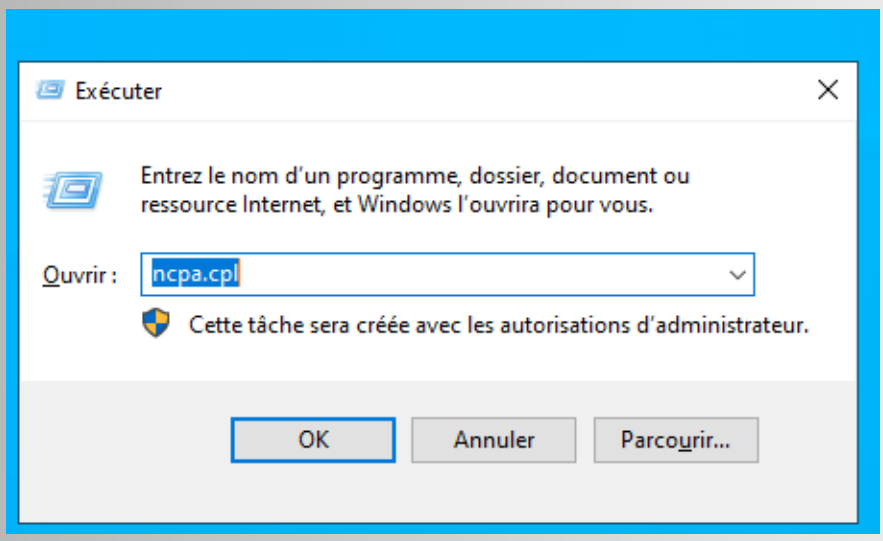
2. MISE EN OEUVRE :

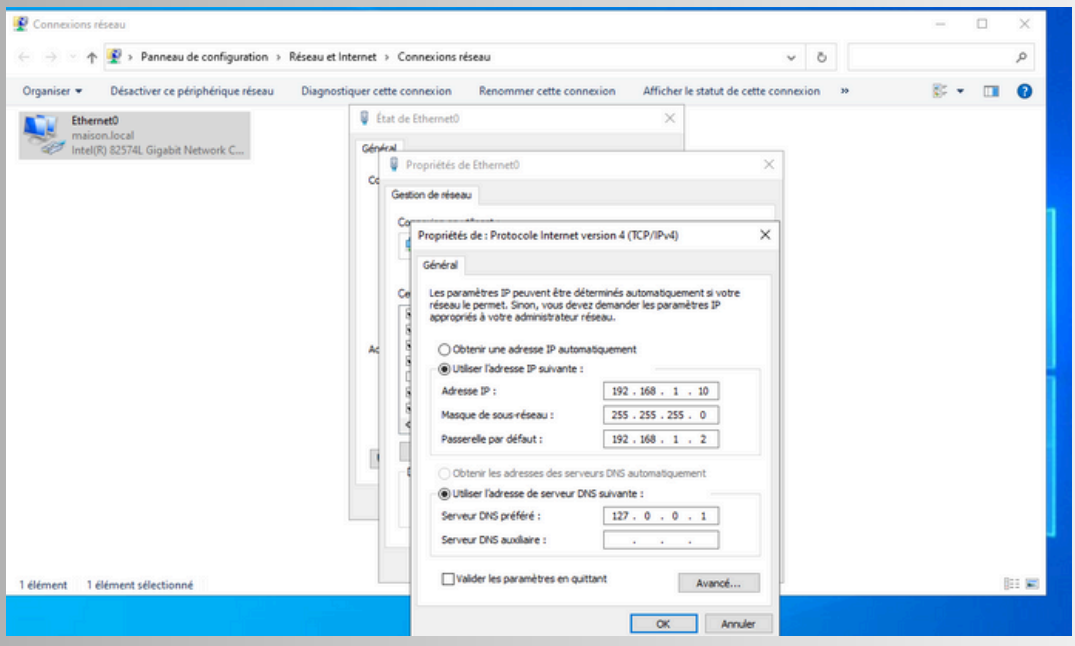
2.1. Etapes de configurations :

2.1.1. Configuration IP et connectivité

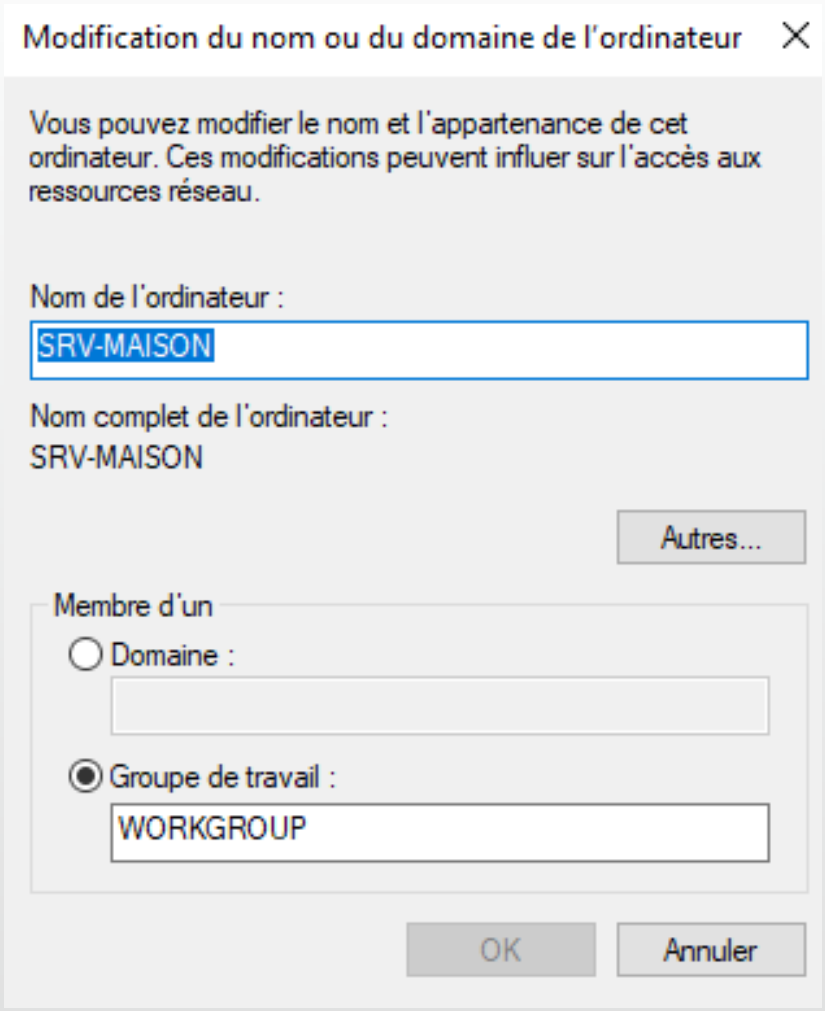
Configuration saisie :

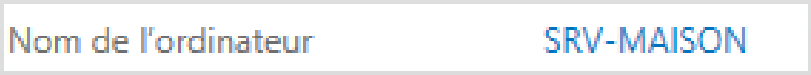
- IP : 192.168.1.10 (par exemple, dans le LAN de ton pfSense).
- Masque : 255.255.255.0
- Passerelle : 192.168.1.2 (L'IP LAN de ton pfSense).
- DNS : 127.0.0.1 (Le serveur sera son propre serveur DNS).



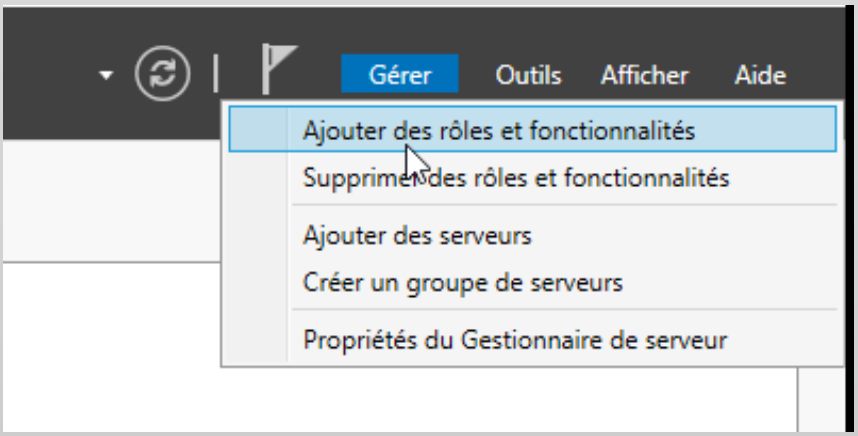


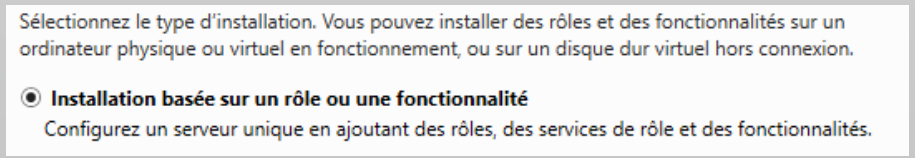
2.1.2. **Renommer le serveur**

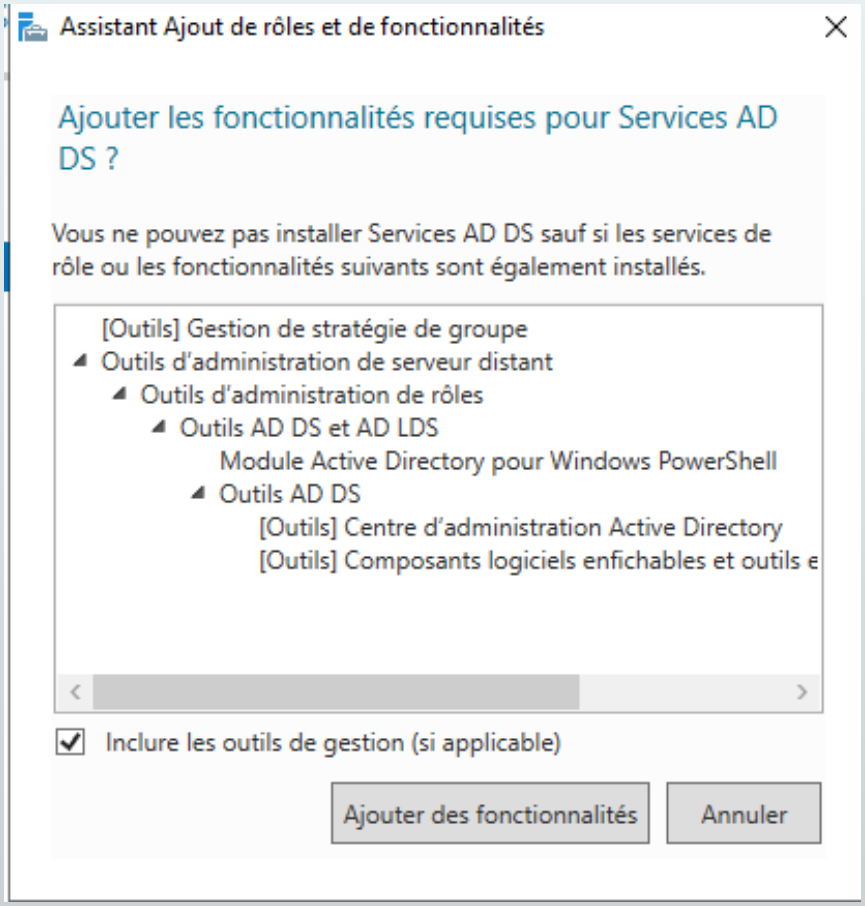


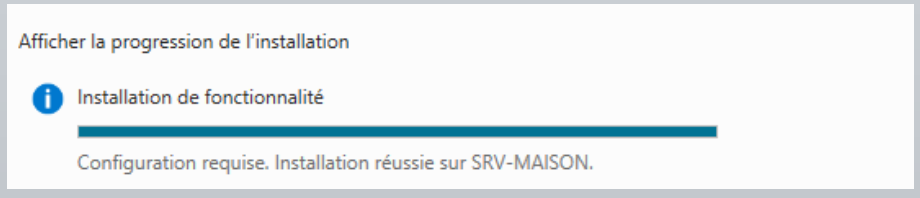


2.1.3. **Installation de l'Active Directory (AD DS)**

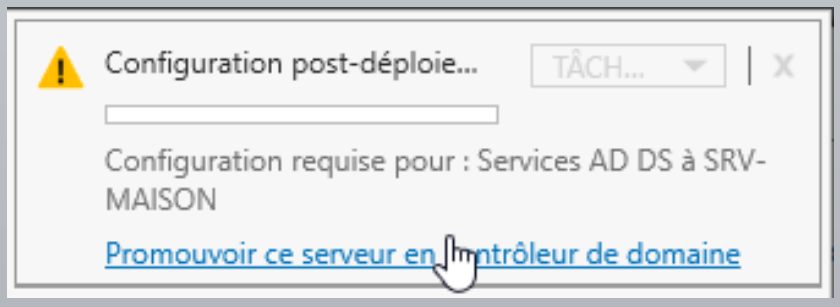


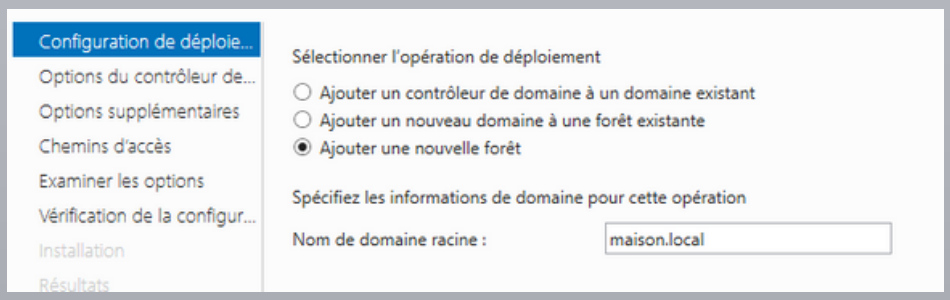


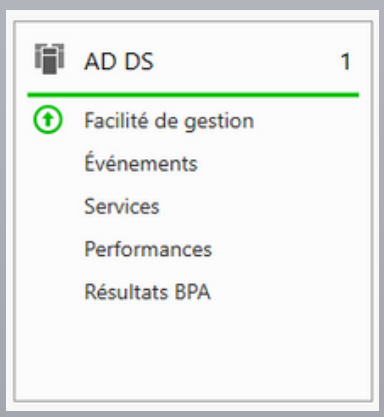




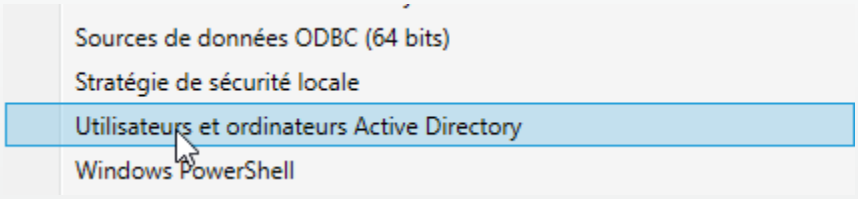
• Puis promotion du serveur en contrôleur de domaine en ajoutant une nouvelle foret

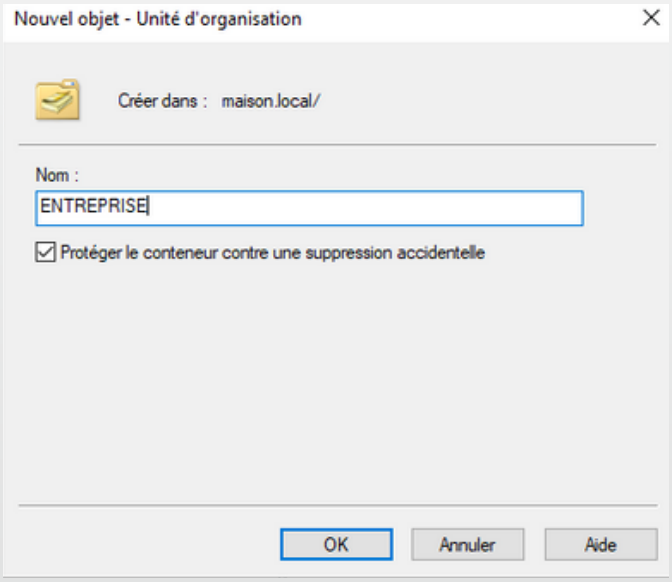




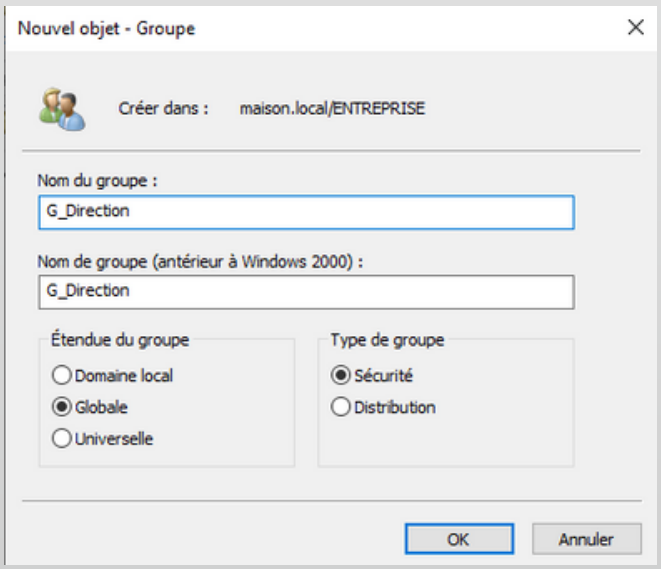


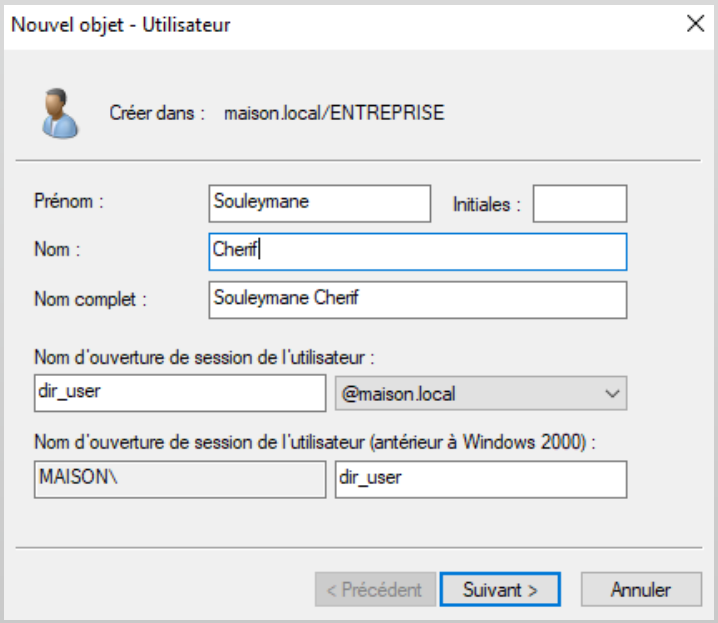
2.1.4. **Création de la structure dans l'AD (Utilisateurs et Groupes)**



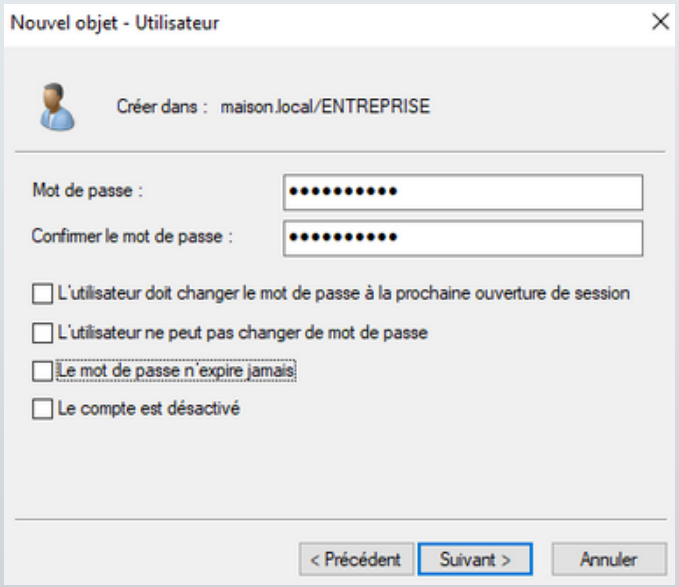


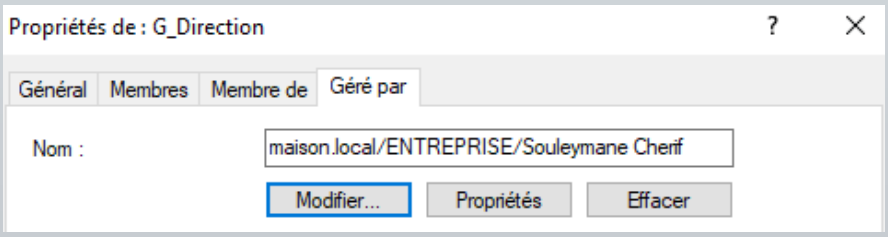
- Création groupes de sécurités + utilisateurs respectifs



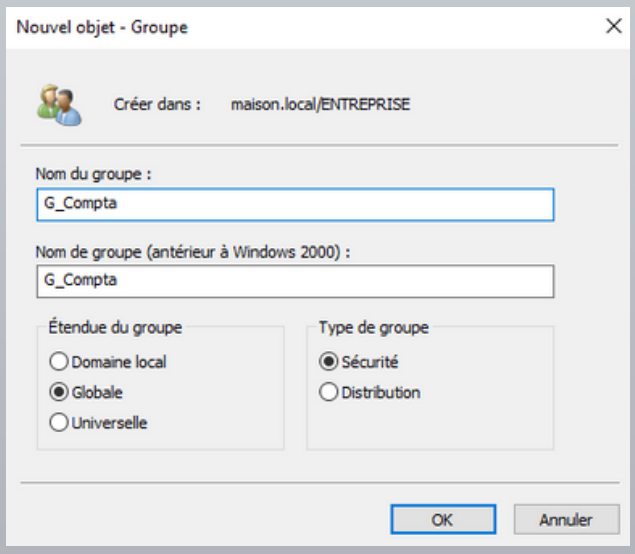


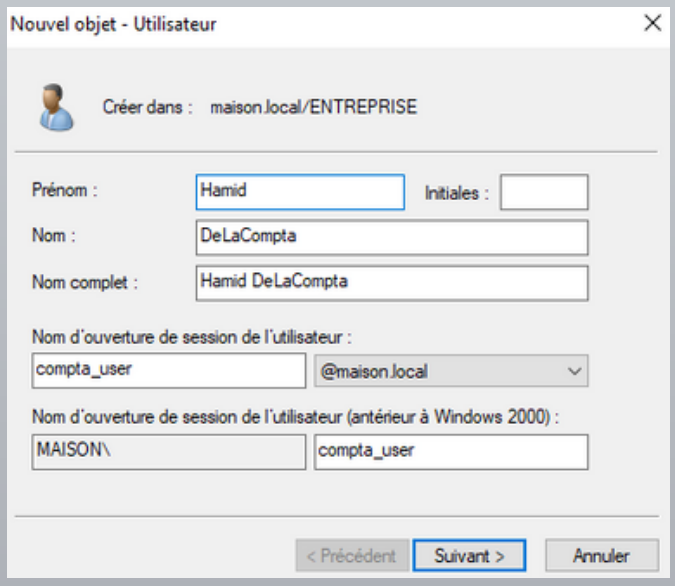
• Sécurisation des utilisateurs par mot de passe et attribution de la gestion du groupe



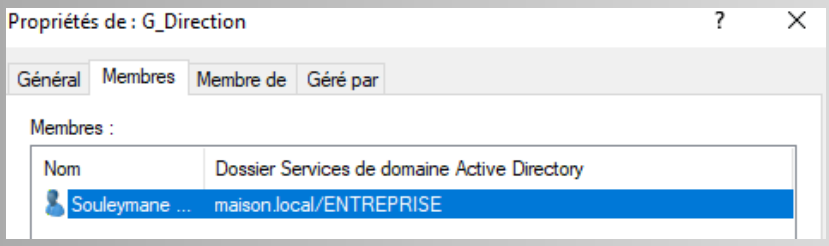


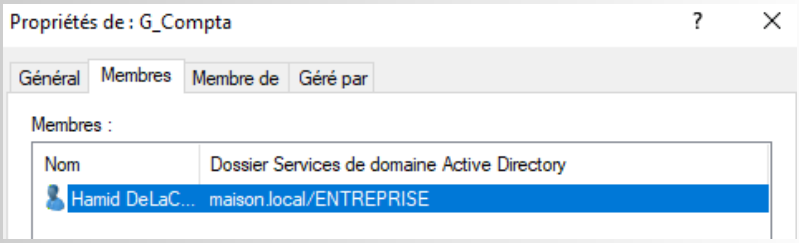
• Puis second





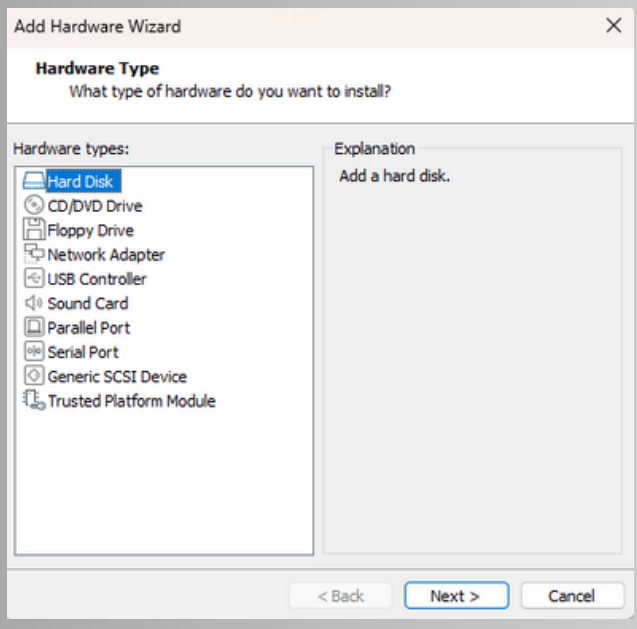
• Puis ajout des utilisateurs aux groupes respectifs

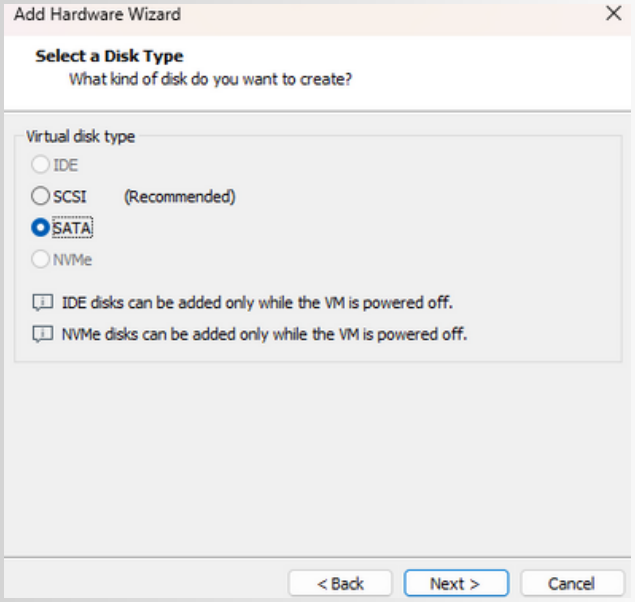


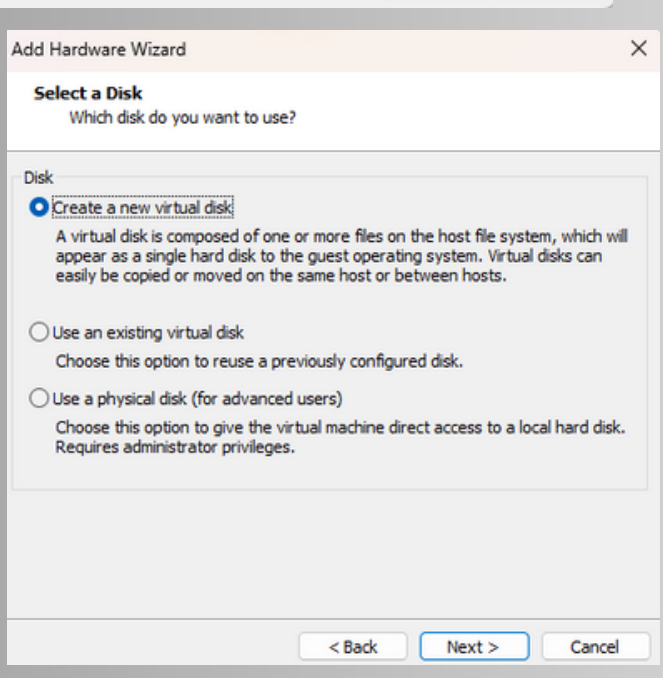


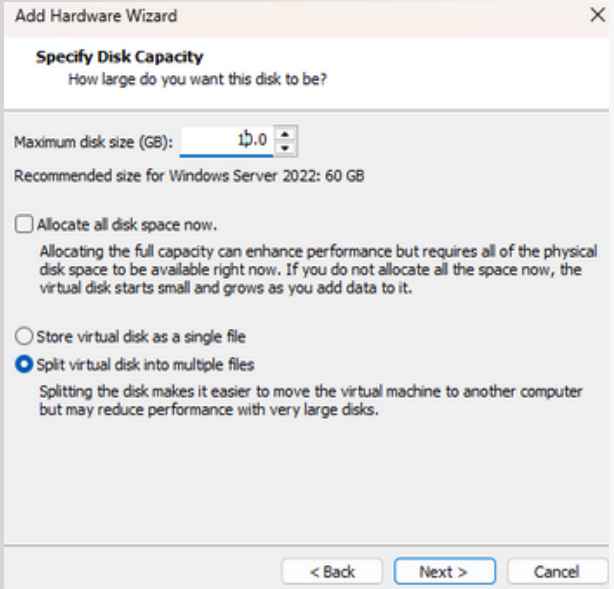
2.1.5. **Configuration du RAID 1 (Miroir) - ["Haute Disponibilité"]**

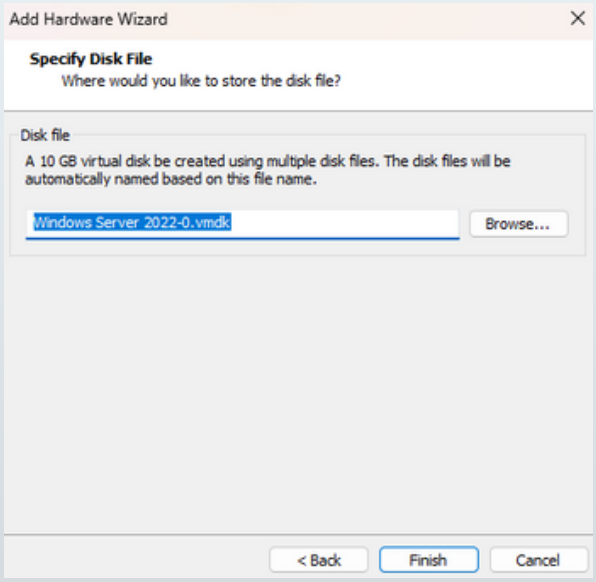
• Création de deux disques secondaires de 10Go

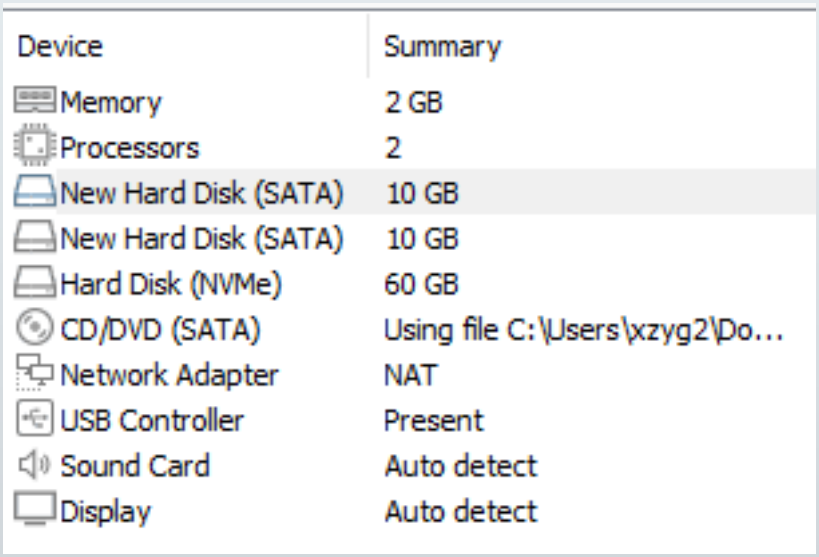




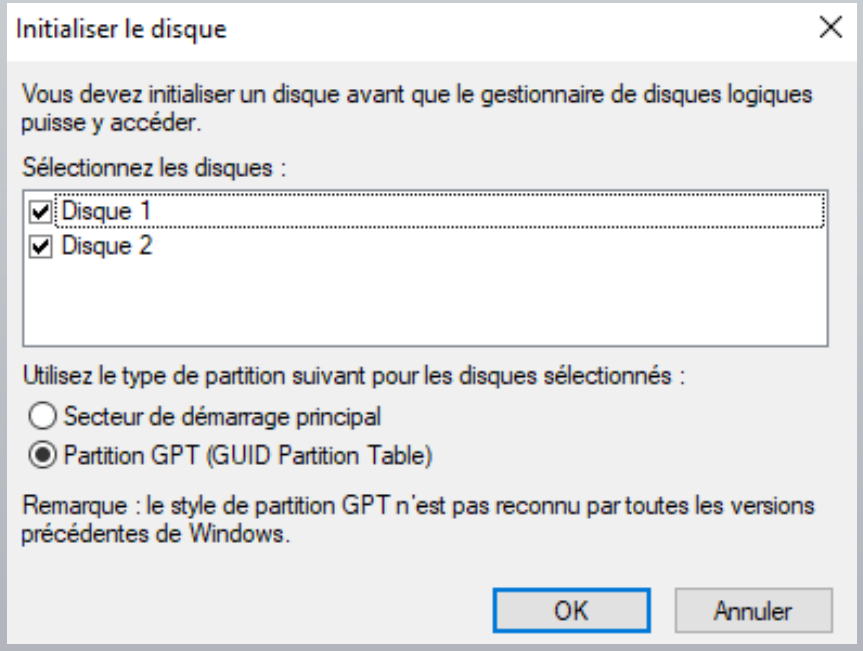




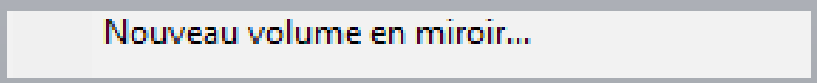


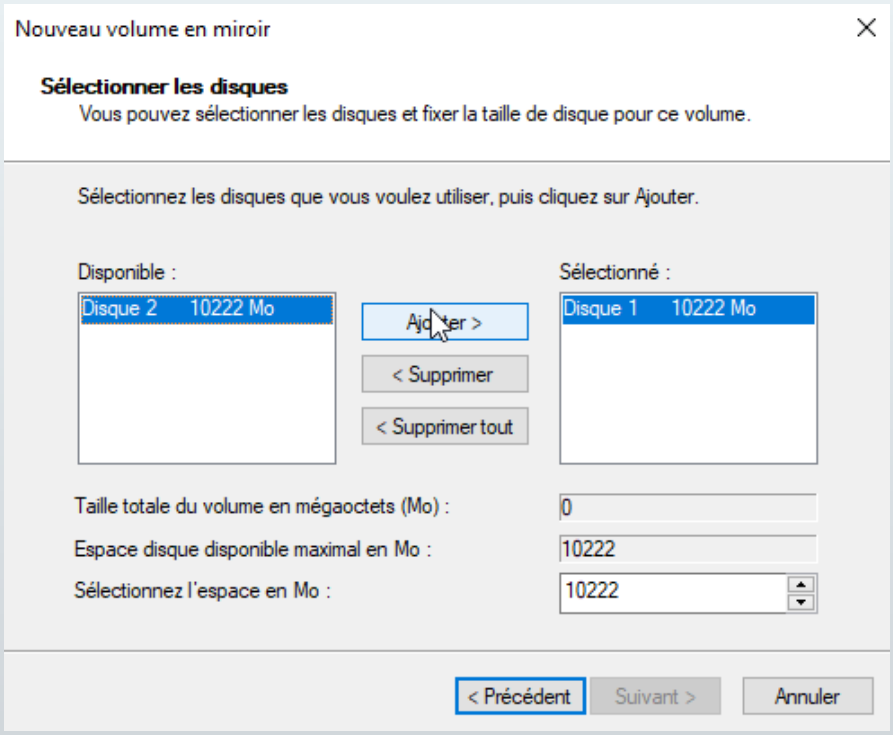


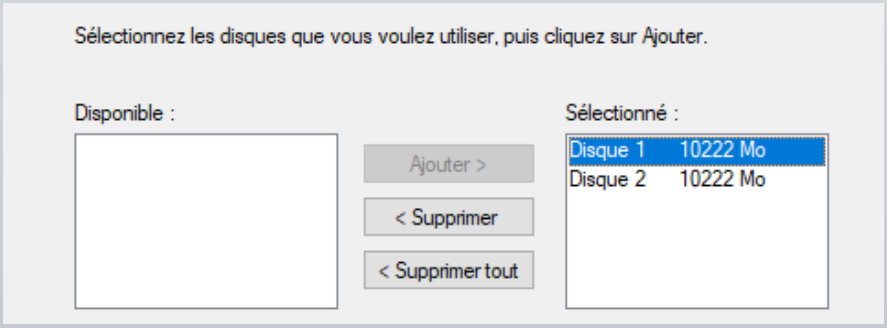
- Création du miroir

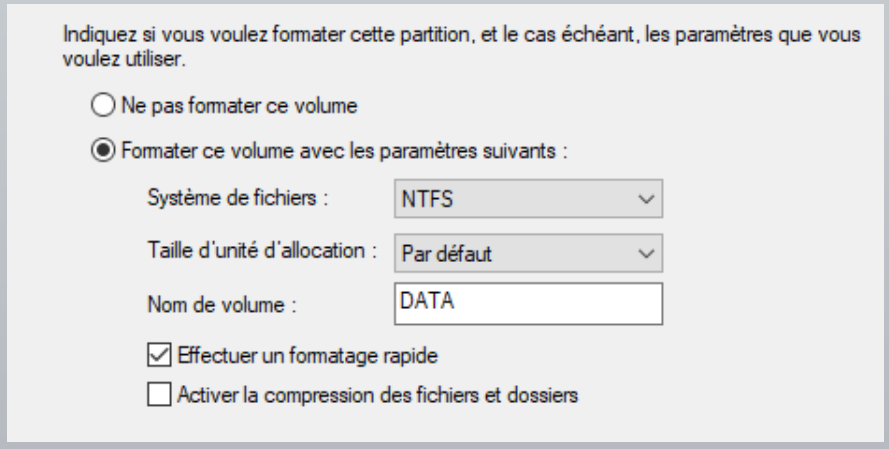


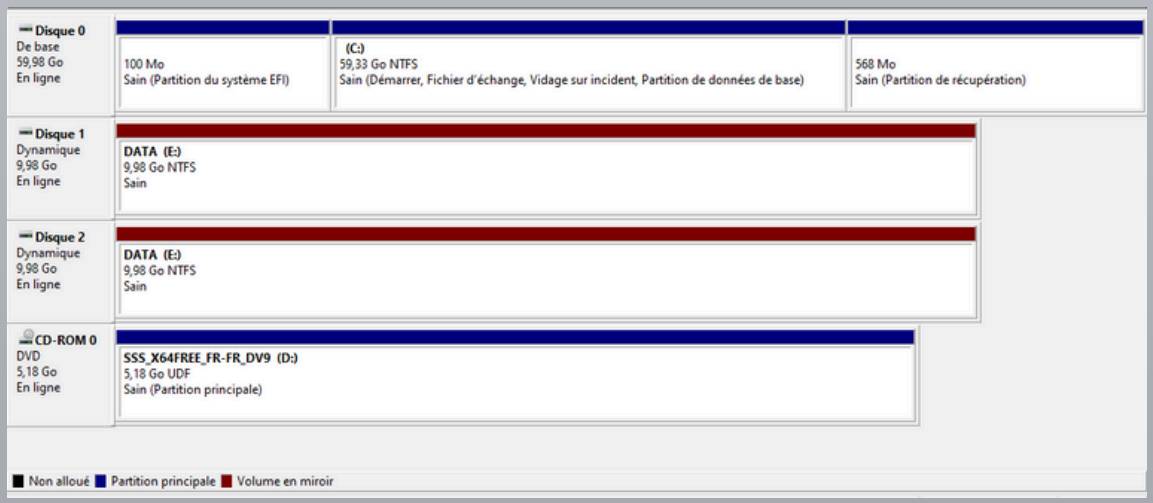
- Sur le disque 1



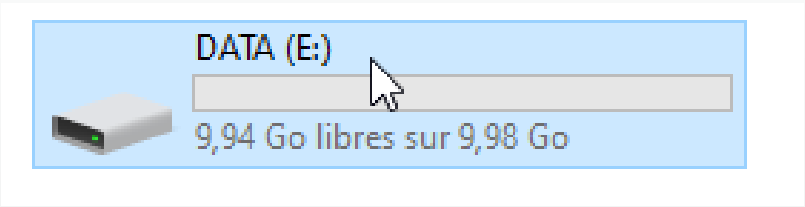

Nouveau volume en miroir
Sélectionner les disques
Vous pouvez sélectionner les disques et fixer la taille de disque pour ce volume.
Sélectionnez les disques que vous voulez utiliser, puis cliquez sur Ajouter.
Disponible :
Disque 2 10222 Mo
Ajouter >
< Supprimer
< Supprimer tout
Sélectionné :
Disque 1 10222 Mo
Taille totale du volume en mégaoctets (Mo) : 0
Espace disque disponible maximal en Mo : 10222
Sélectionnez l'espace en Mo : 10222
< Précédent
Suivant >
Annuler


Sélectionnez les disques que vous voulez utiliser, puis cliquez sur Ajouter.
Disponible :
Ajouter >
< Supprimer
< Supprimer tout
Sélectionné :
Disque 1 10222 Mo
Disque 2 10222 Mo

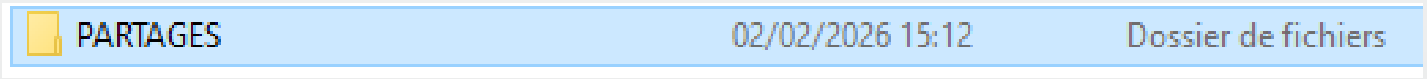

Indiquez si vous voulez formater cette partition, et le cas échéant, les paramètres que vous voulez utiliser.
Ne pas formater ce volume
Formater ce volume avec les paramètres suivants :
Système de fichiers : NTFS
Taille d'unité d'allocation : Par défaut
Nom de volume : DATA
Effectuer un formatage rapide
Activer la compression des fichiers et dossiers

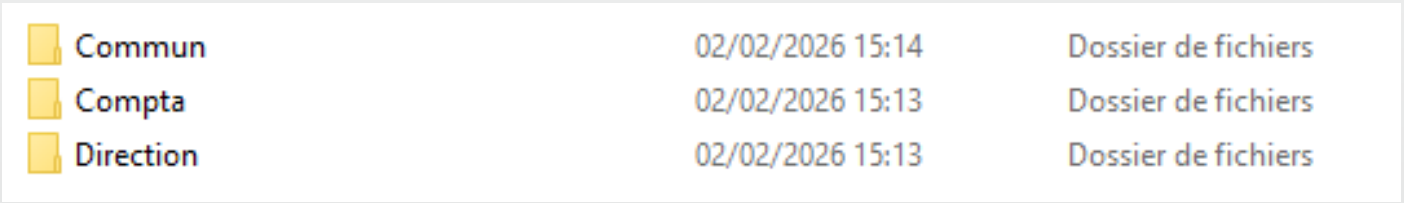

Disque 0
De base
59,98 Go
En ligne
100 Mo
Sain (Partition du système EFI)
(C:)
59,33 Go NTFS
Sain (Démarrer, Fichier d'échange, Vidage sur incident, Partition de données de base)
568 Mo
Sain (Partition de récupération)
Disque 1
Dynamique
9,98 Go
En ligne
DATA (E:)
9,98 Go NTFS
Sain
Disque 2
Dynamique
9,98 Go
En ligne
DATA (E:)
9,98 Go NTFS
Sain
CD-ROM 0
DVD
5,18 Go
En ligne
SSS_X64FREE_FR-FR_DV9 (D:)
5,18 Go UDF
Sain (Partition principale)
Non alloué
Partition principale
Volume en miroir

2.1.6. **Création de l'arborescence et Partage sur le disque “DATA”**

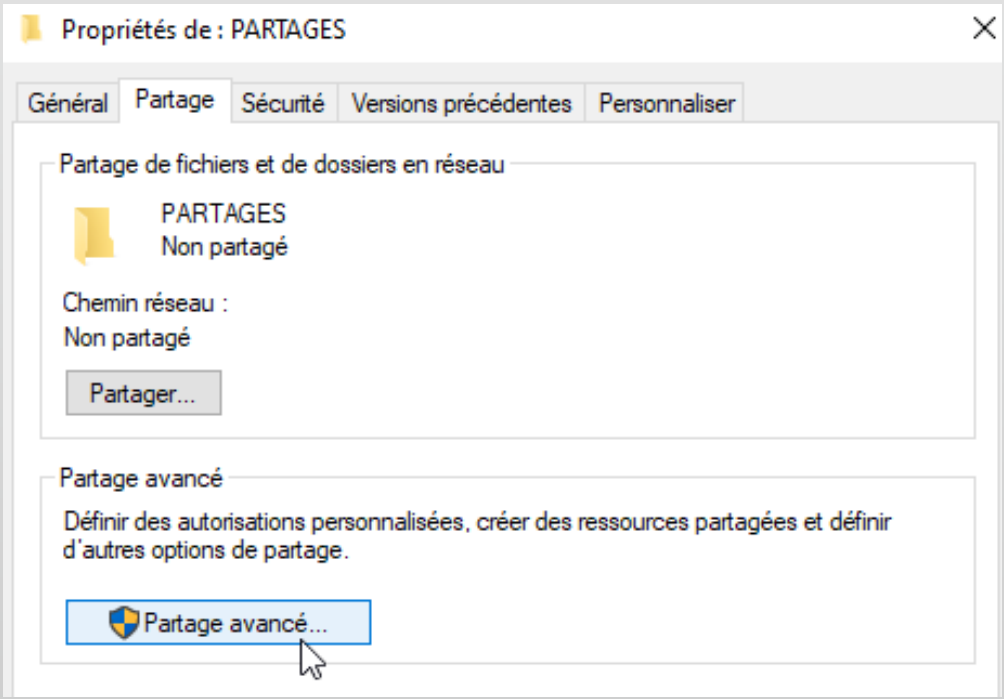


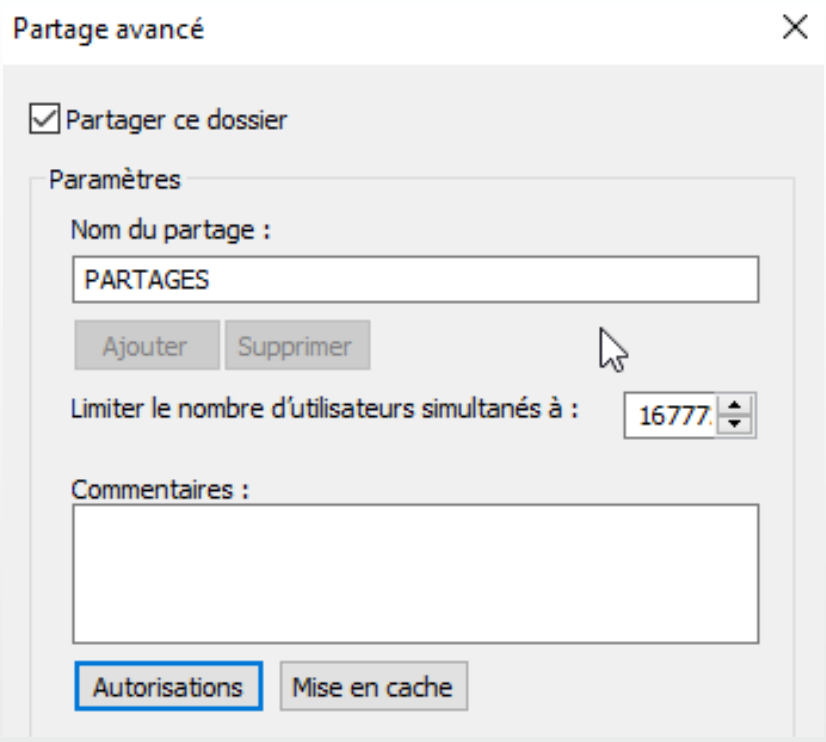
• Création d’un dossier racine nommé “PARTAGES” et de trois sous-dossiers



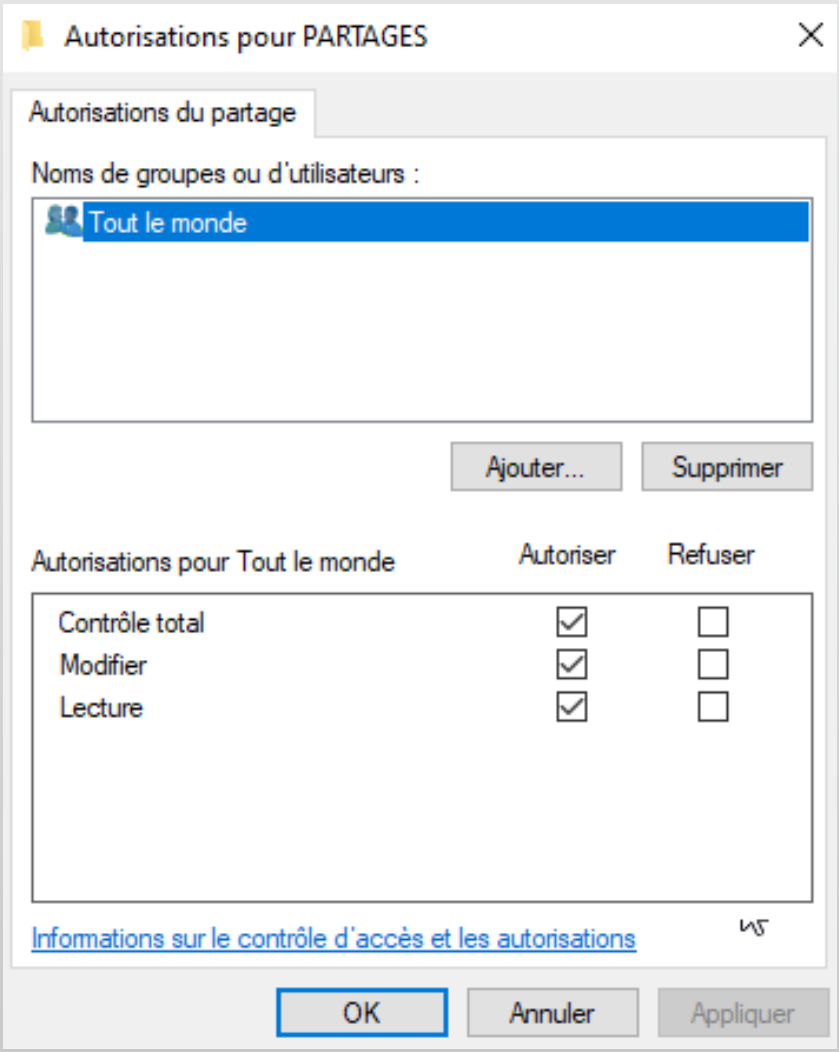


• Gestion du Partage (SMB)



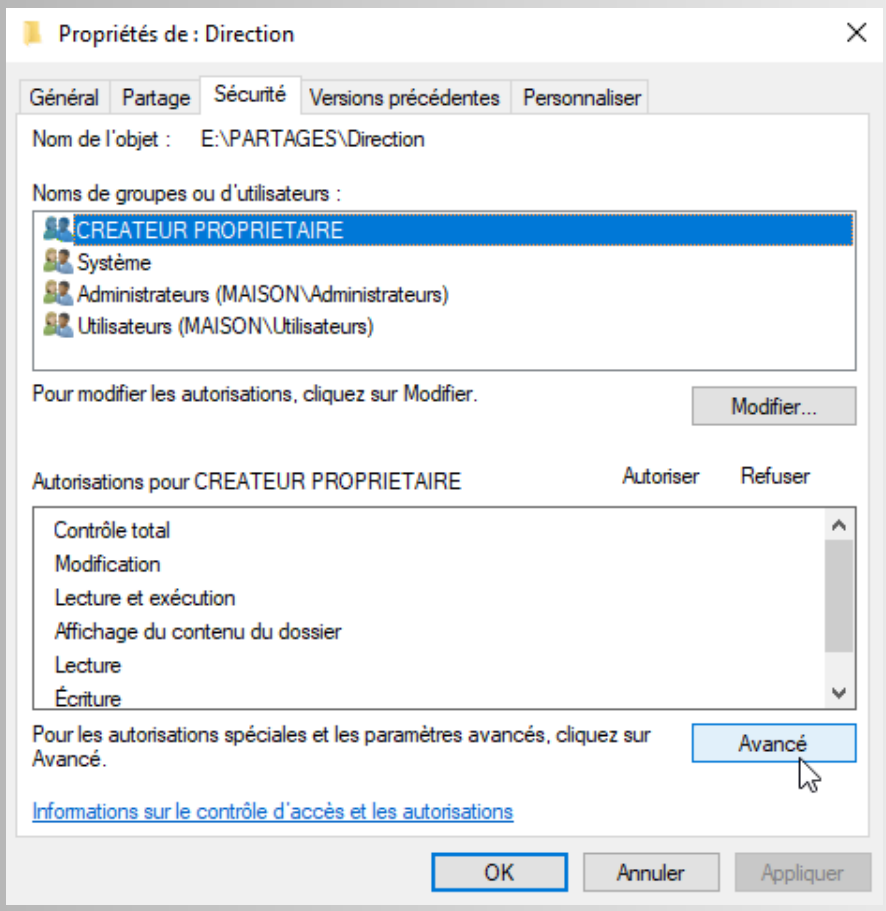


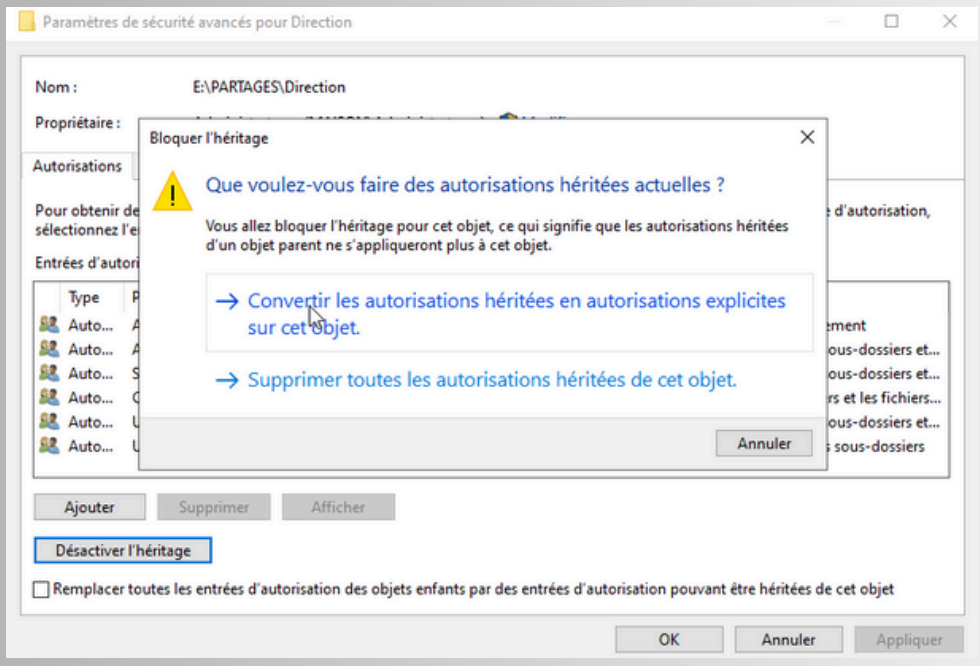
- Autorisation accordée a : “Tout le monde”



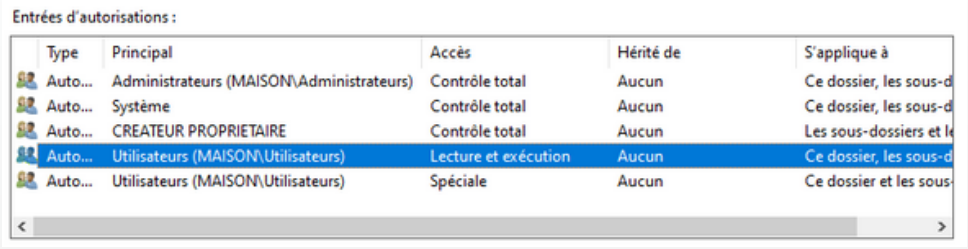
2.1.7. **Configuration des permissions NTFS**

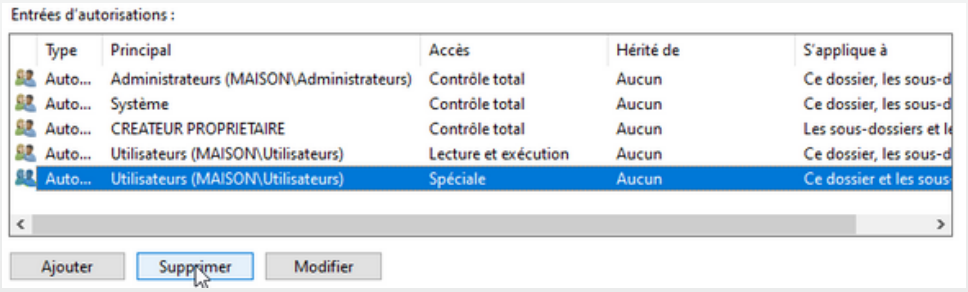
- Désactivation de l'héritage du dossier : "Direction"



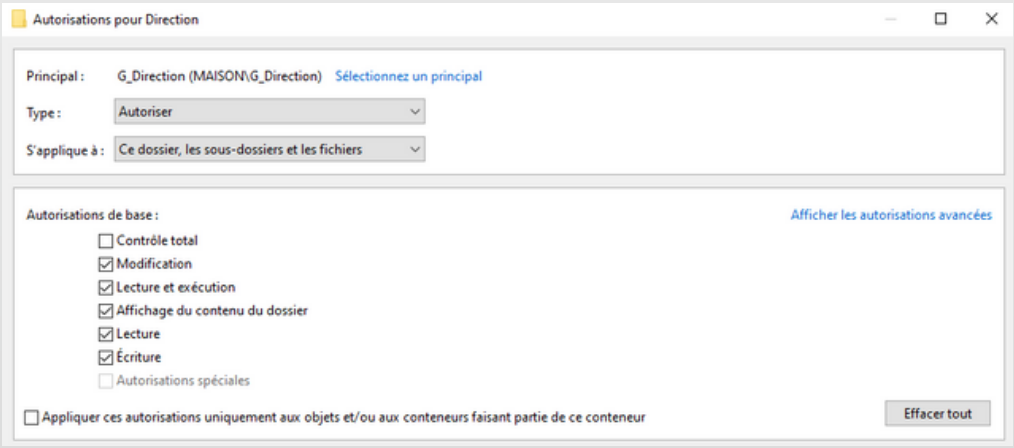


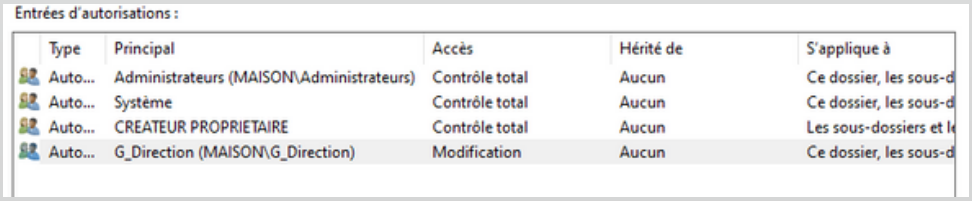
- Suppression des utlisateurs de la liste



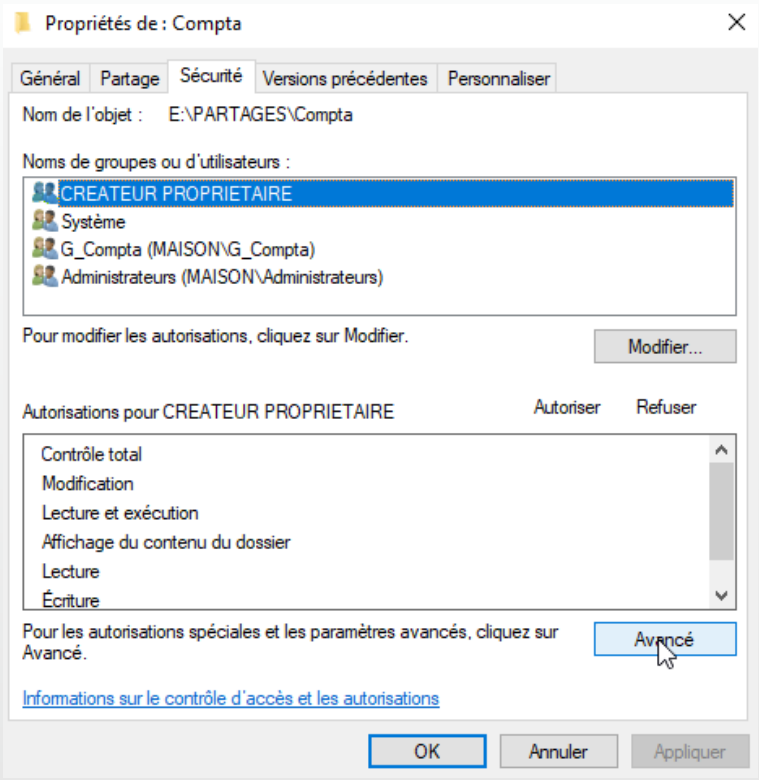


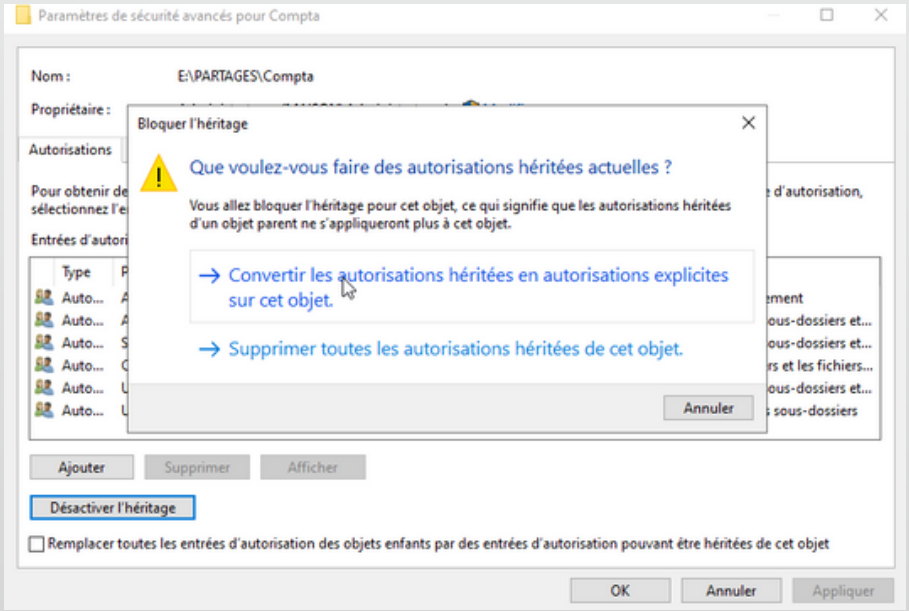
- Ajout du groupe : “G_Direction” a la liste



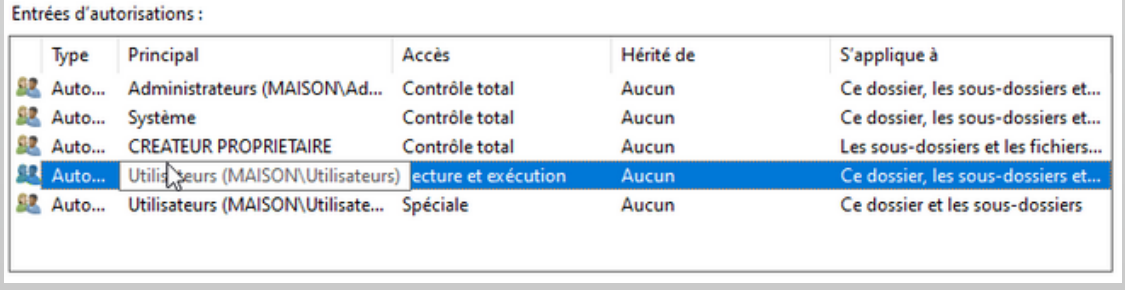


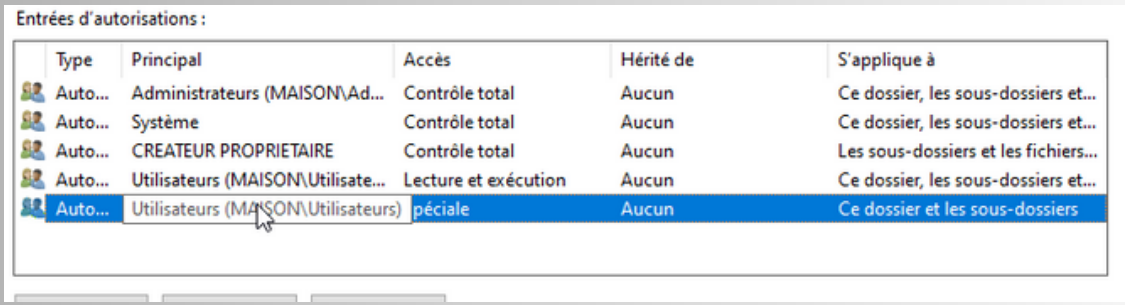
- Désactivation de l'héritage du dossier : "Compta"



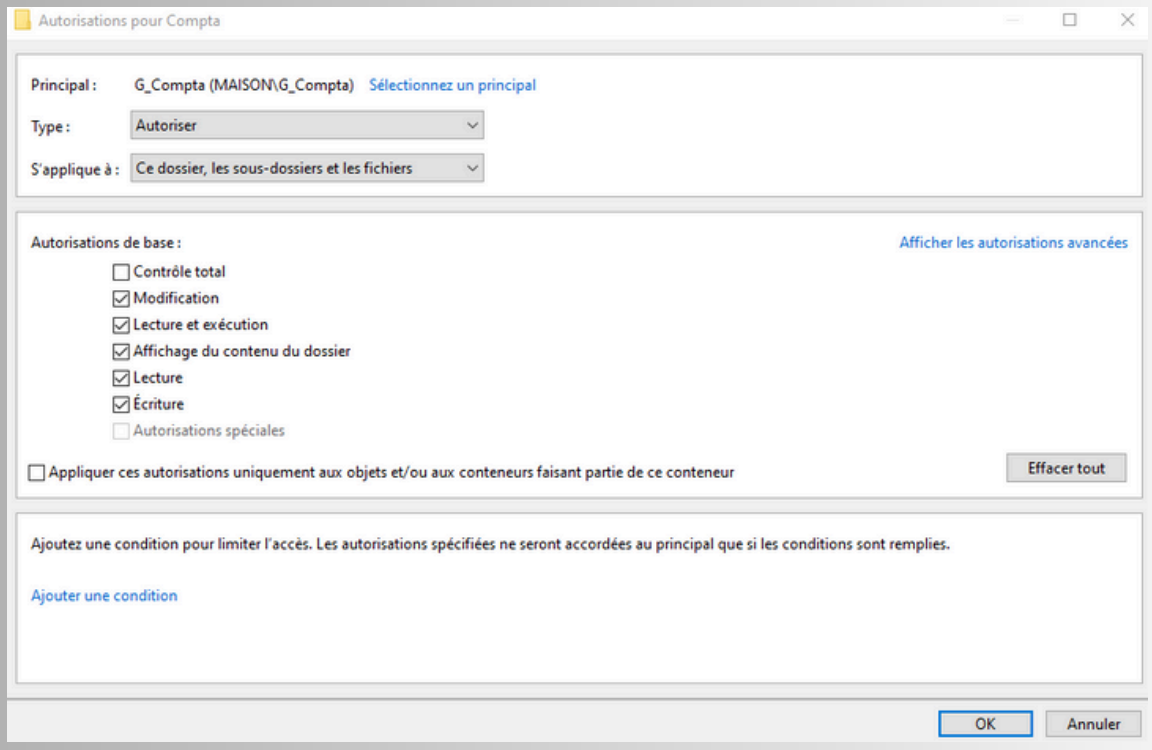


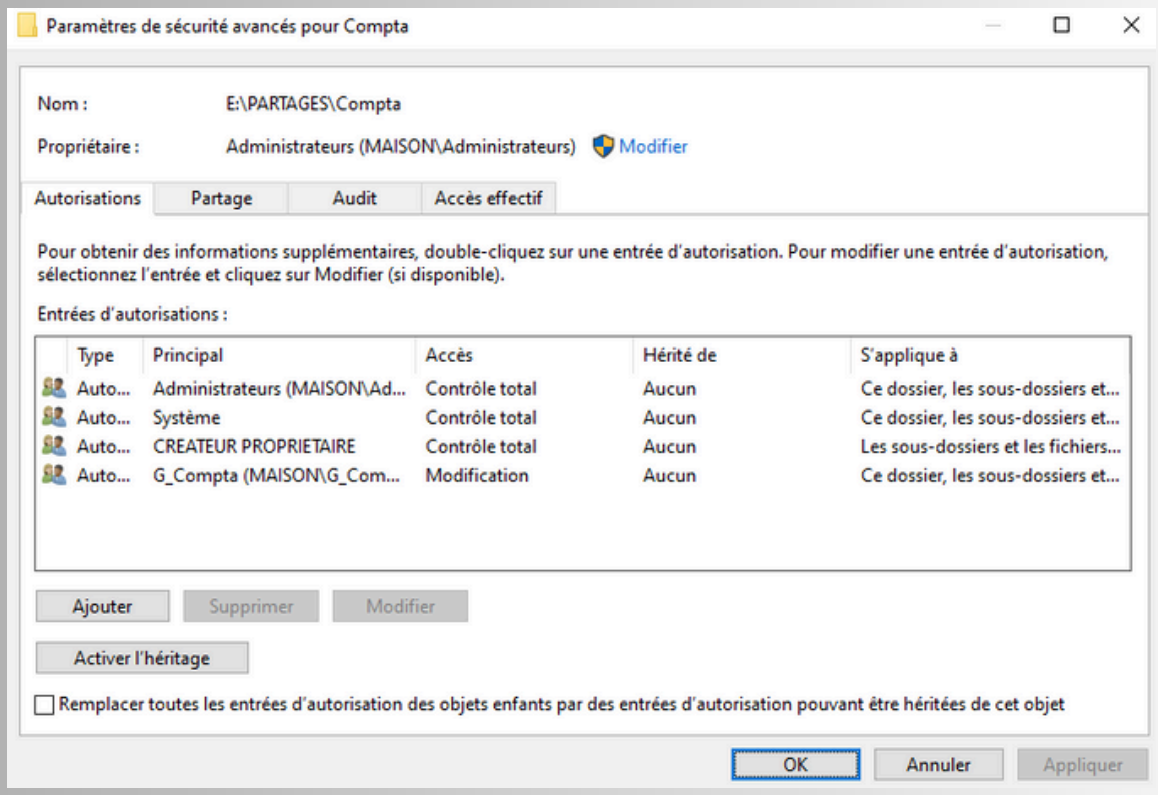
- Suppression des utlisateurs de la liste



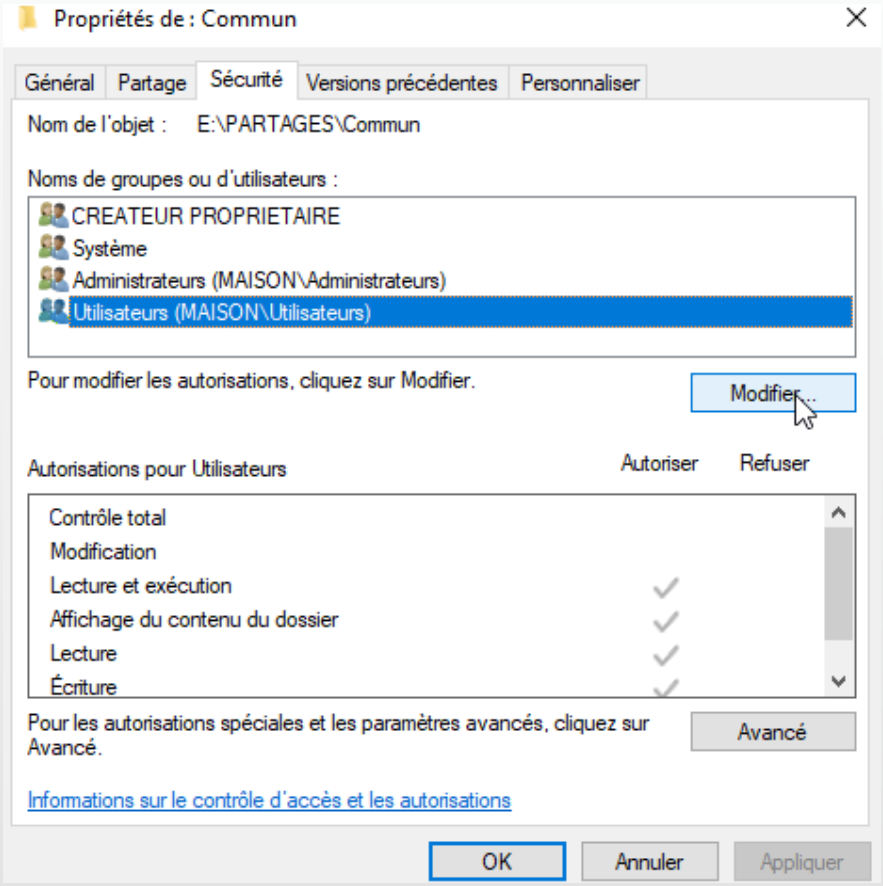


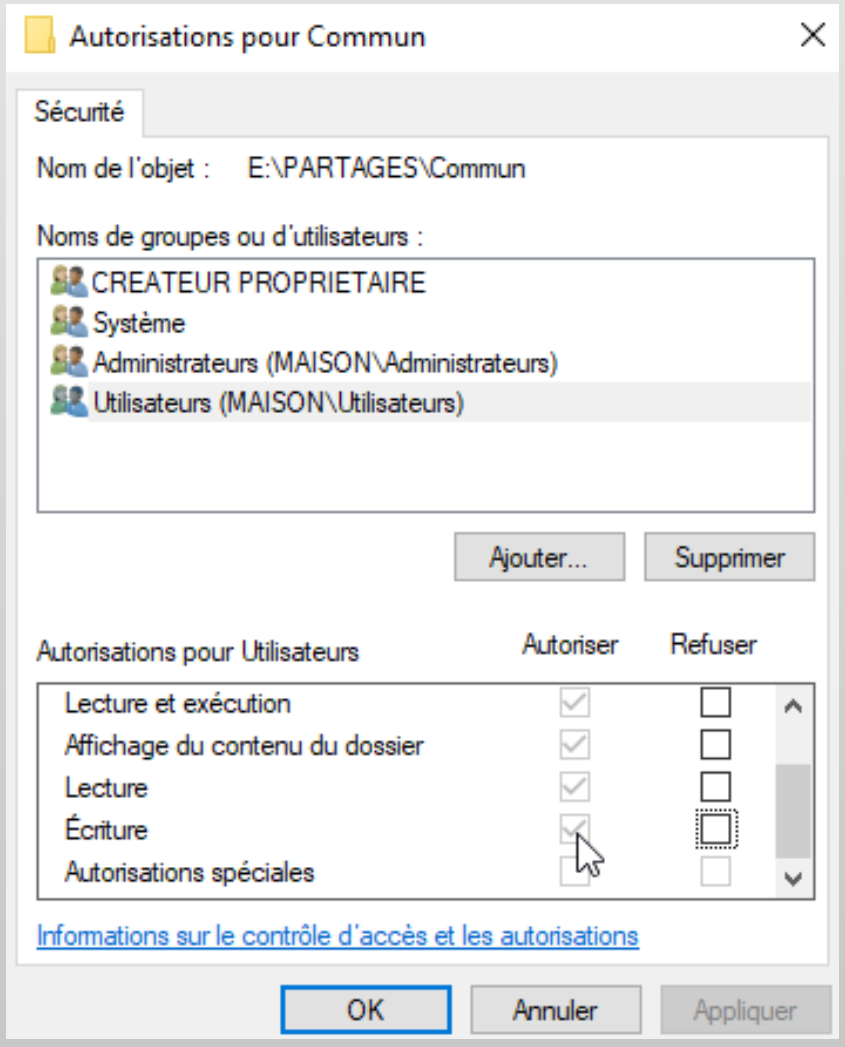
- Ajout du groupe : “G_Compta” a la liste





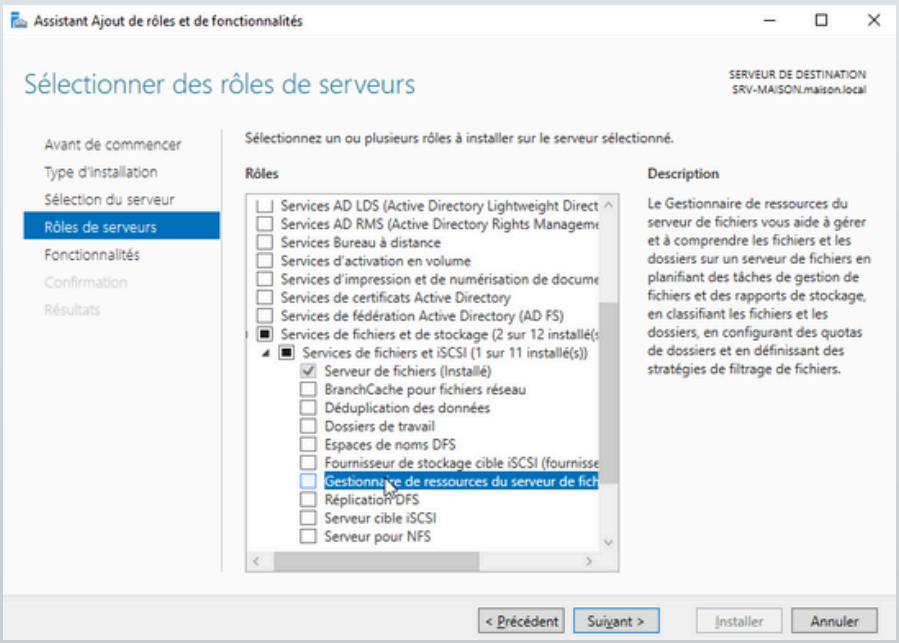
- Activation de la permission d' : "Ecriture" sur le dossier : "Commun"

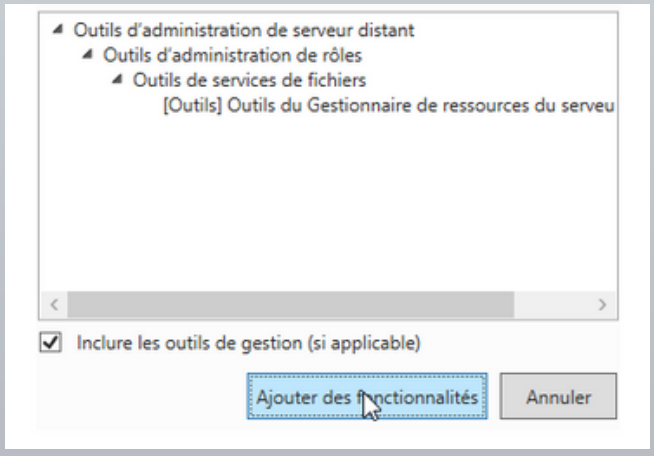


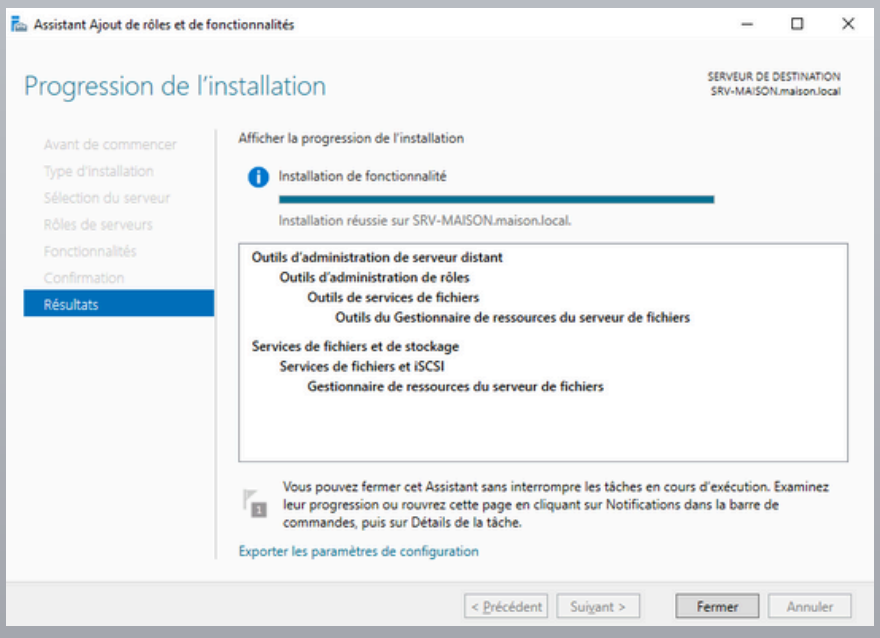


2.1.8. **Configuration du rôle FSRM (Gestionnaire de ressources du serveur de fichiers)**

- Installation “Gestionnaire de ressources du serveur de fichier (FSRM)

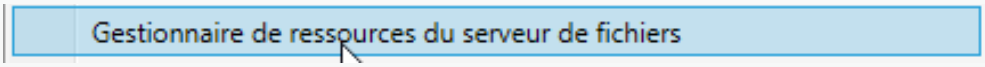


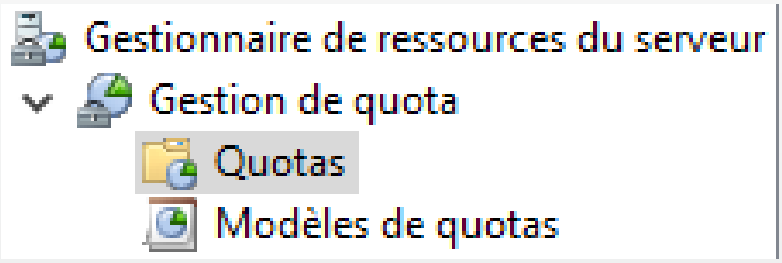




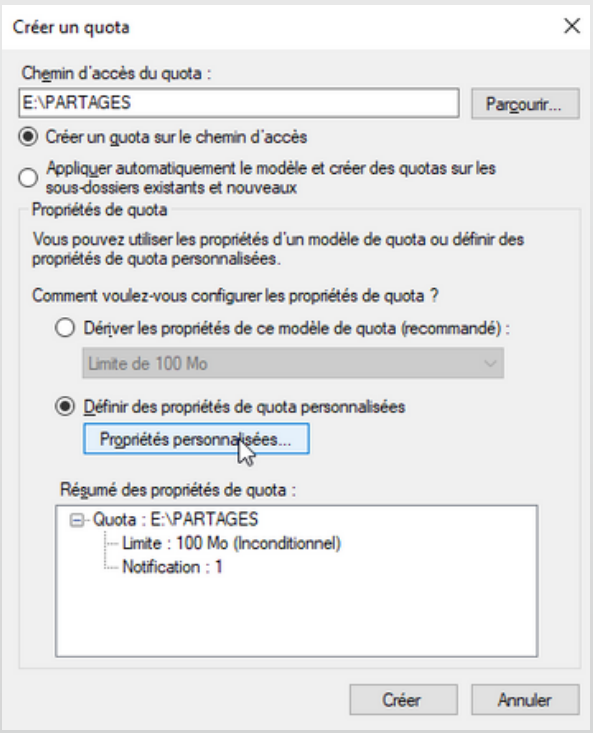
- Mise en œuvre du Quota (Disponibilité)

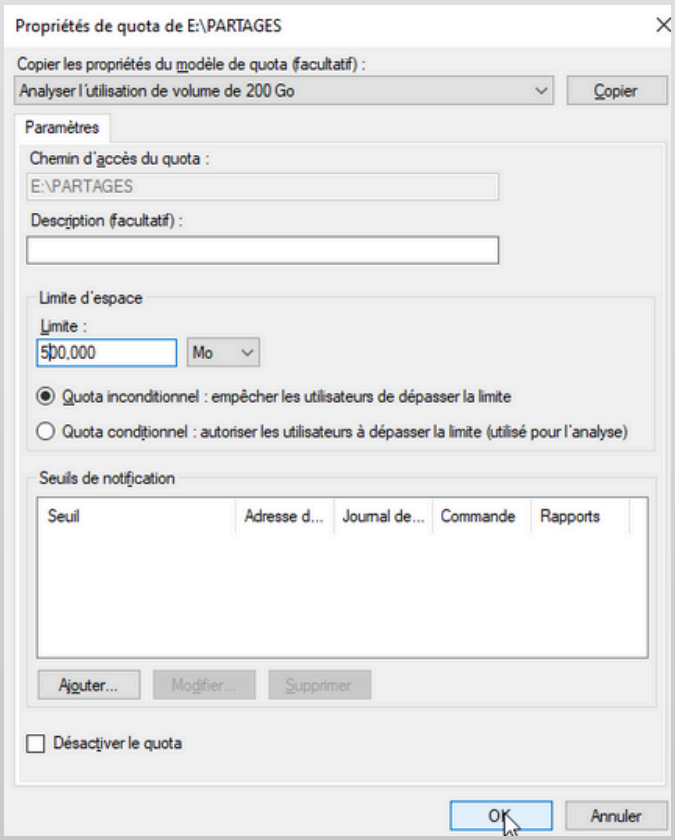
Evite qu'un utilisateur ne sature le disque

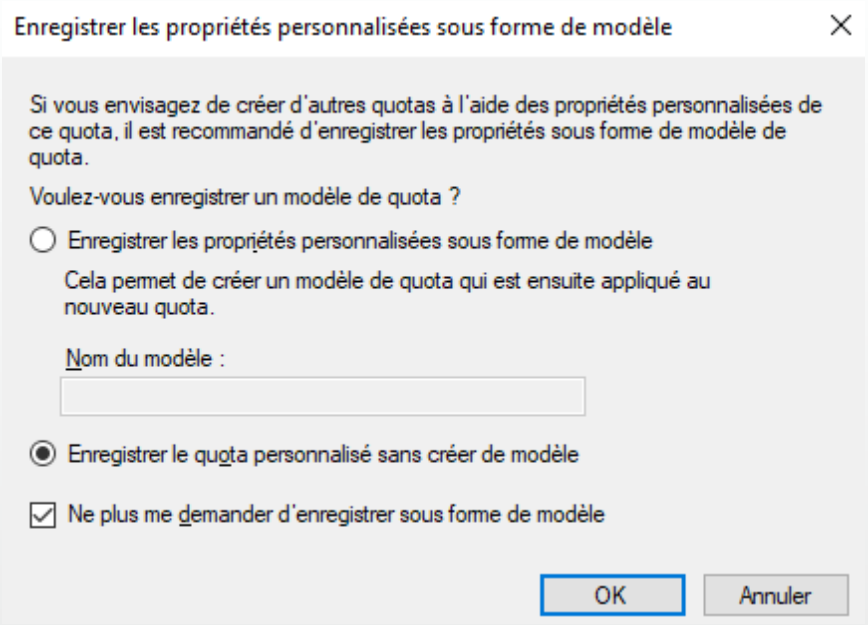




- Création d'un quota inconditionnel personnalisé de 500mo

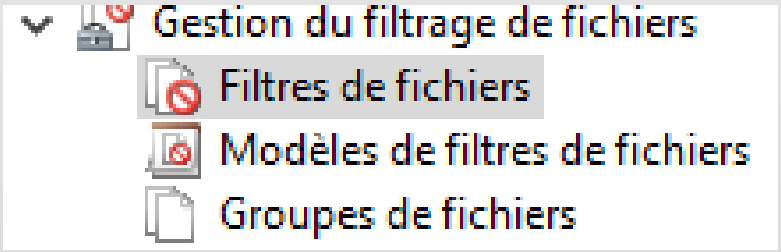




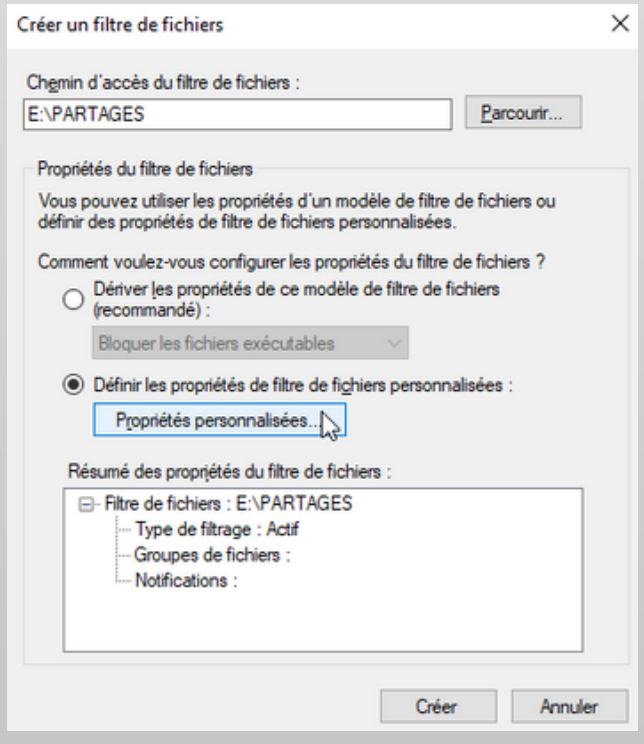


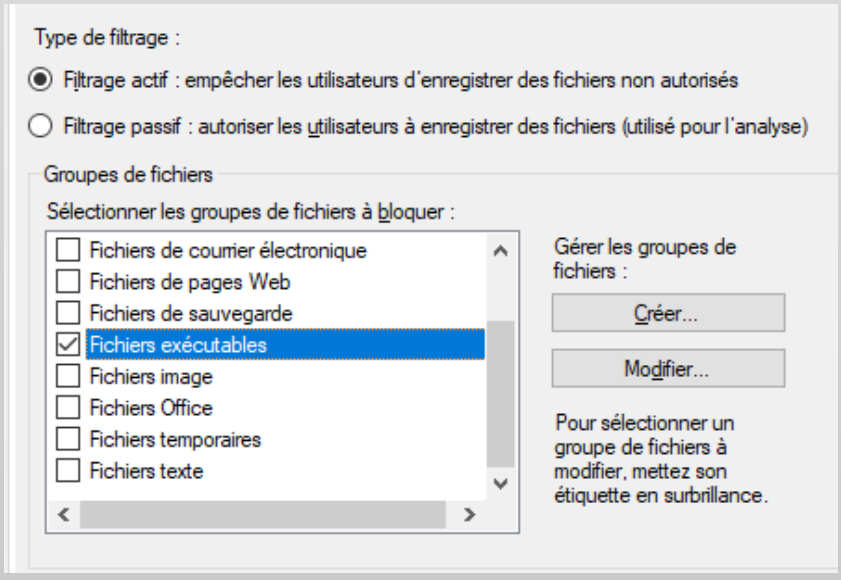
- Mise en œuvre du Filtrage de fichiers (Sécurité)

Interdit le stockage de fichier non-professionnel ou dangereux



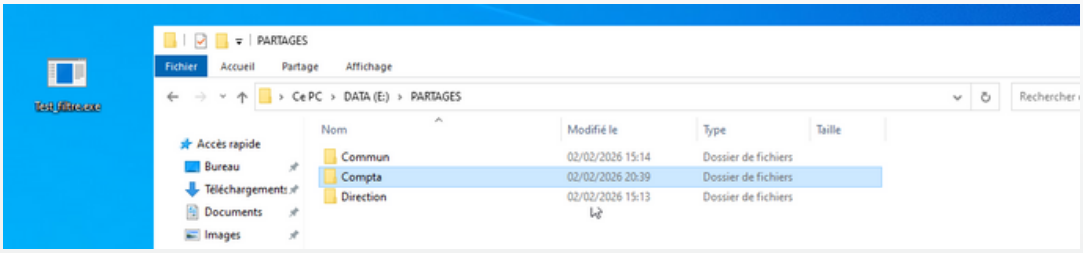
- Création d'un filtre de fichiers personnalisé

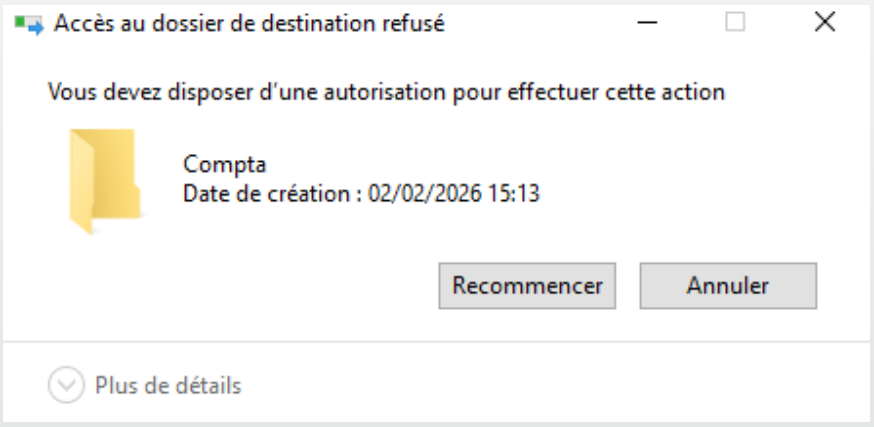




- Resultat :

Le fichier “test” exécutable est impossible a copier dans le dossier “Compta”.





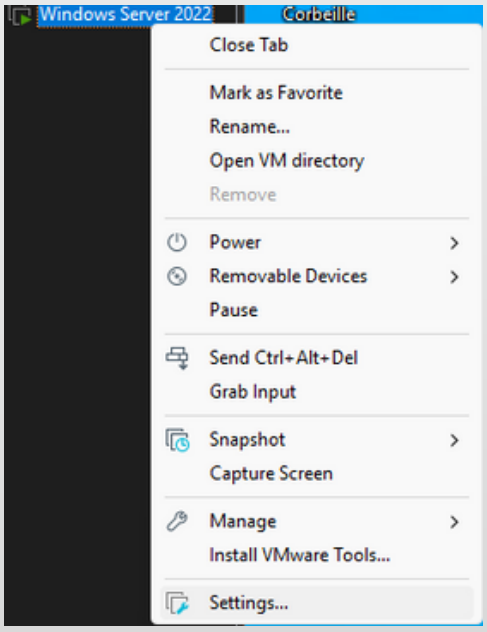
3. TESTS ET RECETTES :

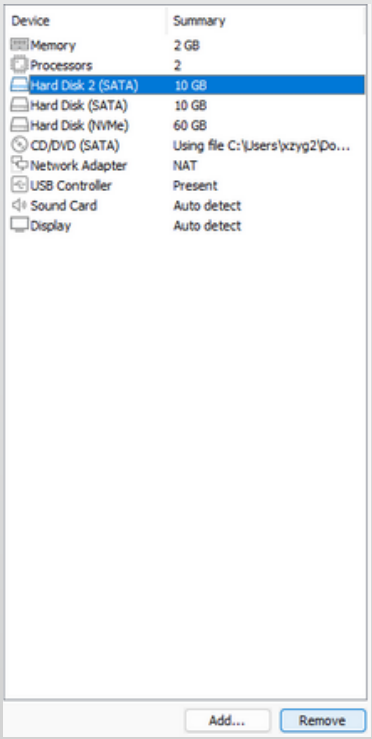
3.1. TESTS ET VÉRIFICATIONS

3.1.1. Vérification de la tolérance aux pannes (RAID 1)

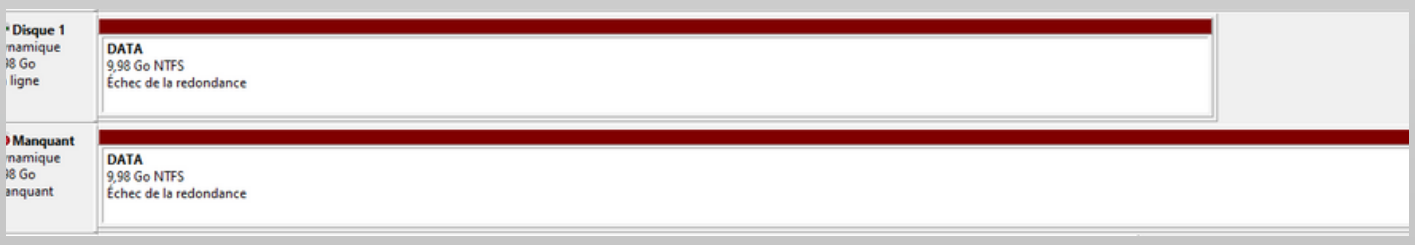
- Hypothèse : "Que se passe-t-il si l'un de mes disques tombe en panne physiquement ?"

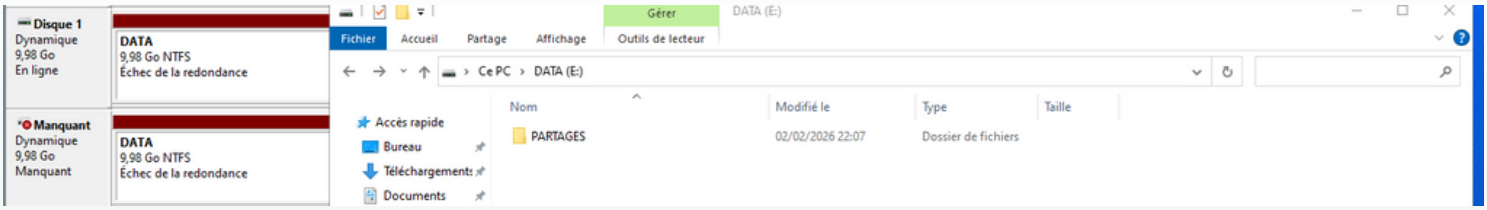
- Action : "Simulation d'une panne par déconnexion à chaud du disque secondaire dans l'hyperviseur."





- Observation : "Le gestionnaire de disques affiche l'état Échec de la redondance. Le système reste opérationnel (Continuité de service)."



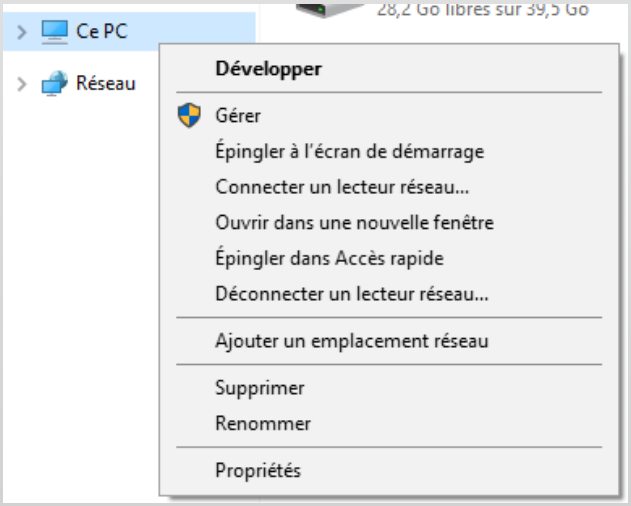


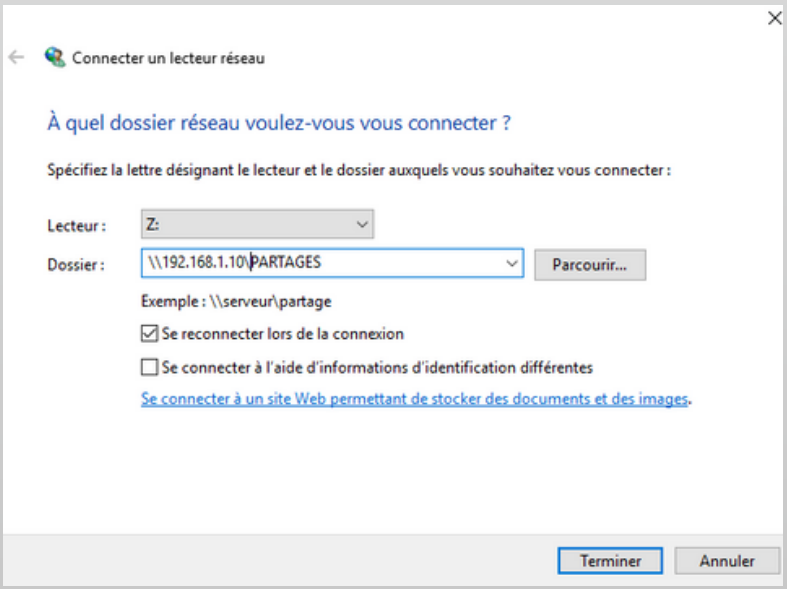
- Conclusion : "L'objectif de haute disponibilité est atteint : aucune donnée n'est perdue et le serveur n'a pas eu besoin de redémarrer."

→ La possibilité de remettre la redondance en marche s'effectue par l'ajout d'un nouveau disque (la procédure n'est pas traitée ici)

3.1.2. **Vérification de la confidentialité (ACL NTFS)**

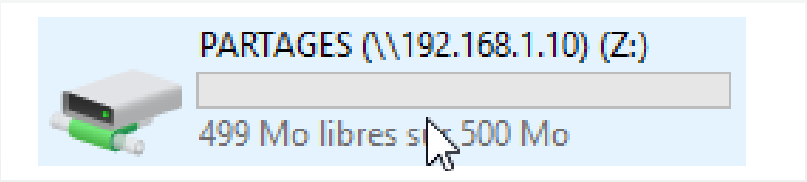
- Hypothèse : "Les fichiers sont-ils partagés chez tous les utilisateurs sélectionnés ?"
- Action : "Création d'une VM Windows 10 Pro connectée au domaine et connexion au lecteur réseau."

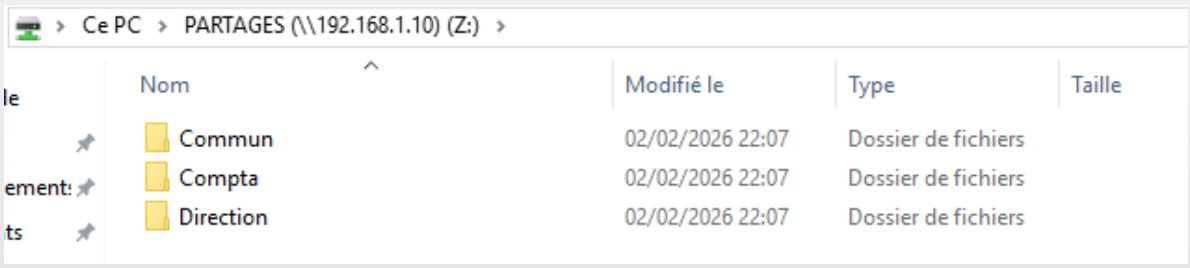


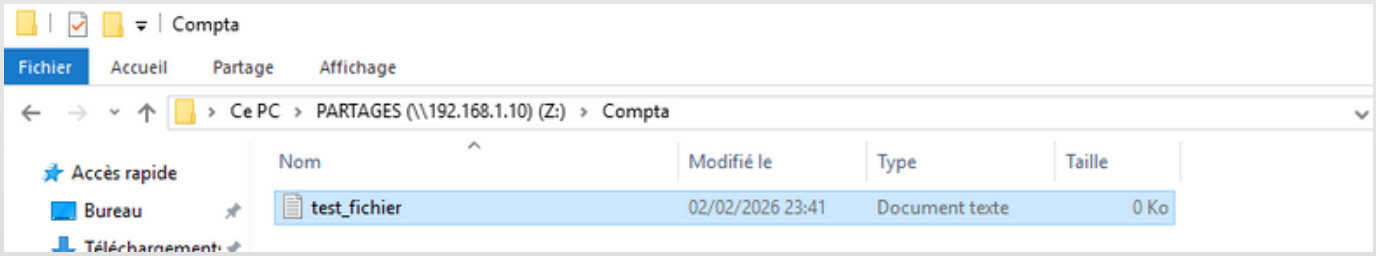


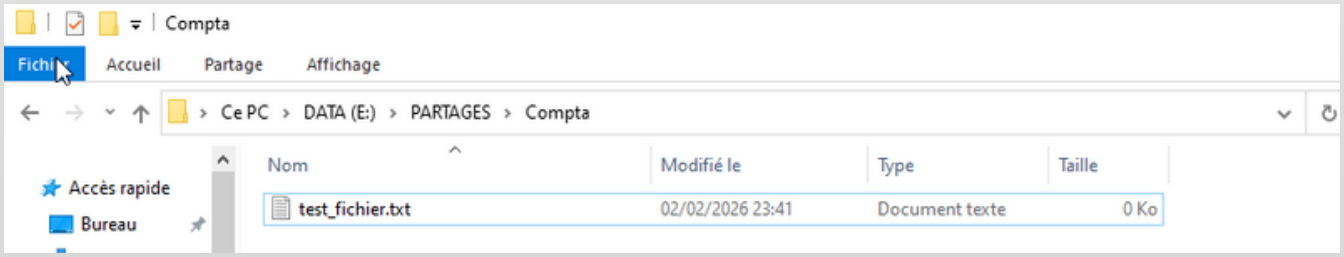
- Observation : "Le lecteur réseau se présente et le gestionnaire de fichiers affiche bien les trois dossier principalement contenu dans le dossier “PARTAGES”.

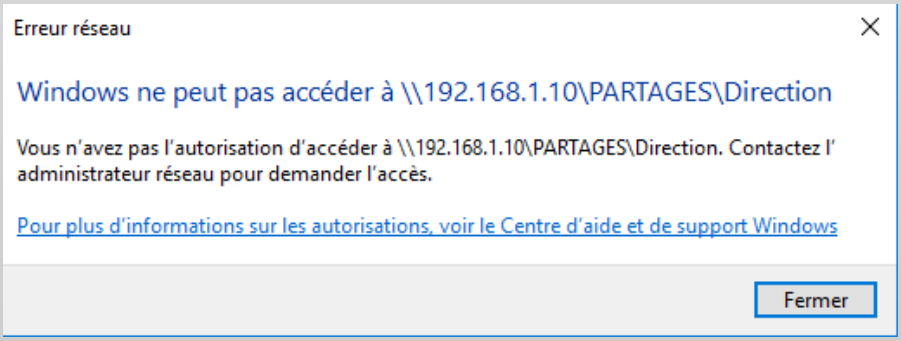
La création de fichiers dans “Compta” est possible.
L’acces a “Directon” est interdit
Et “Commun est accessible. "

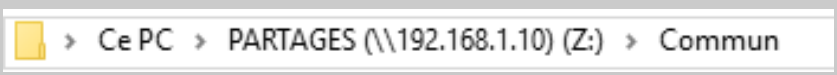












- Conclusion : "L'objectif de confidentialité est atteint : les utilisateurs ont bien accès aux dossiers partagés."

→ La mise en marche de la VM Windows 10 Pro n'a pas été montré ici.

3.1.3. Vérification des Quotas (FSRM)

- Hypothèse : "Que se passe-t-il si l'on créer un fichier plus grand que la limite fixée ?"

- Action : "Simulation de la création d'un fichier de 600mo via PowerShell."

→ Le pourquoi de l'utilisation de PowerShell est expliqué dans "Incidents".

```
PS C:\Users\Administrateur> fsutil file createnew E:\Partages\Commun\fichier_test.dat 600000000
Erreur :  Espace insuffisant sur le disque.
PS C:\Users\Administrateur>
```

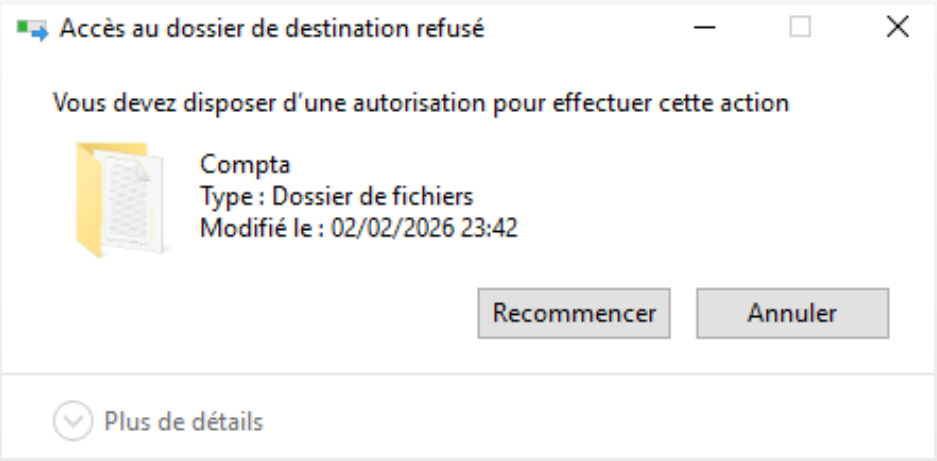
- Observation : "Les règles de quotas agissent de façon conforme à ce qui était demandé. Le fichier ne peux être créer "

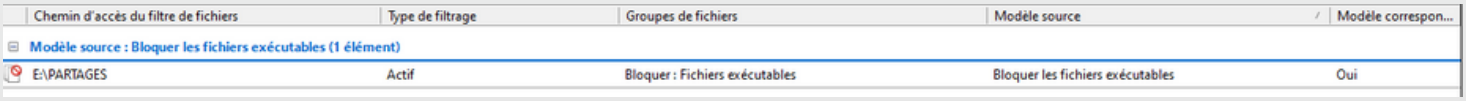
- Conclusion : "L'objectif de quotas est atteint : les fichiers trop volumineux ne peuvent être créer, la saturation des disques est géré."

3.1.4. Vérification des Filtrages

- Hypothèse : "Que se passe-t-il si l'on essaye d'importer un fichier considéré "indésirable" par les règles de filtrage dans le dossier "Compta" ?"

- Action : "Création du fichier "logiciel_interdit.exe" et tentative de copie dans le dossier "Compta"





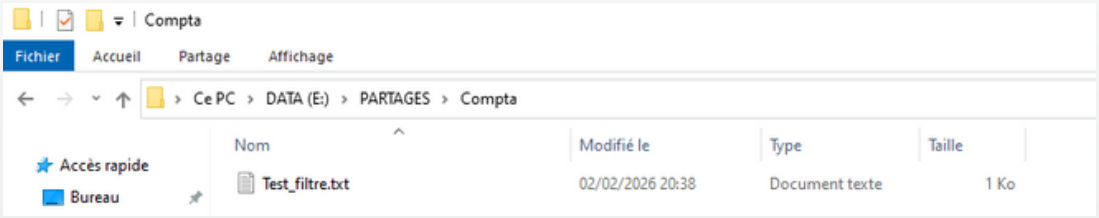
Chemin d'accès du filtre de fichiers	Type de filtrage	Groupes de fichiers	Modèle source	Modèle correspon...
Modèle source : Bloquer les fichiers exécutables (1 élément)				
E:\PARTAGES	Actif	Bloquer : Fichiers exécutables	Bloquer les fichiers exécutables	Oui

- Observation : "Les règles de filtrage ont bien été appliquée lors de la copie du fichier “indésirable”. Le dossier est sain et sauf. "
- Conclusion : "L'objectif de filtrage est atteint : aucun fichier non conforme ne peut être ajoute aux dossier concernés par le règles de filtrage."

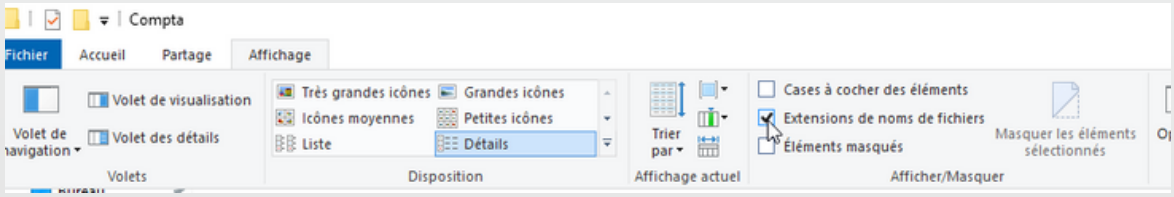
3.2. INCIDENTS

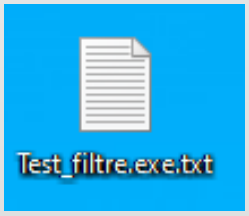
3.2.1. Incident n°1 :

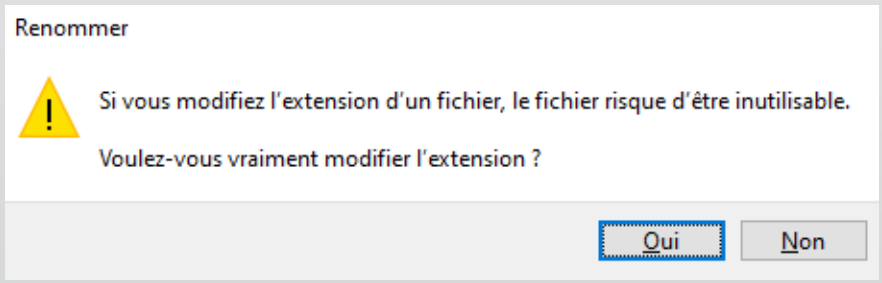
- Le dossier “Compta” autorisait la copie du fichier « test »

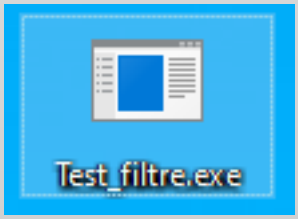


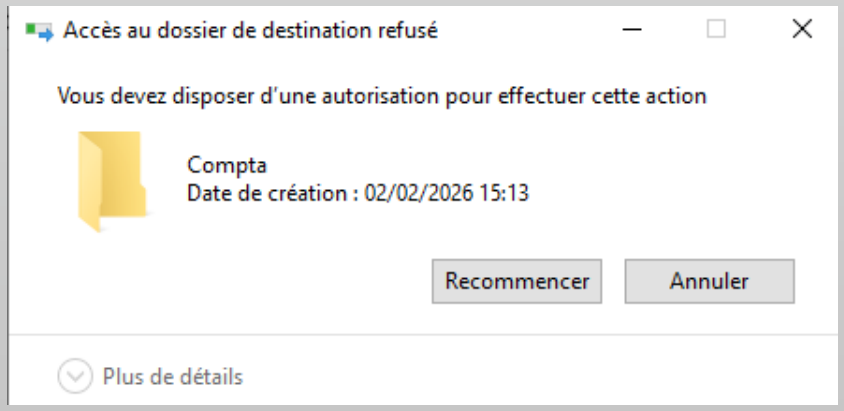
- Activer l’option “Extension de noms de fichiers” dans “Affichage” du gestionnaire de fichiers









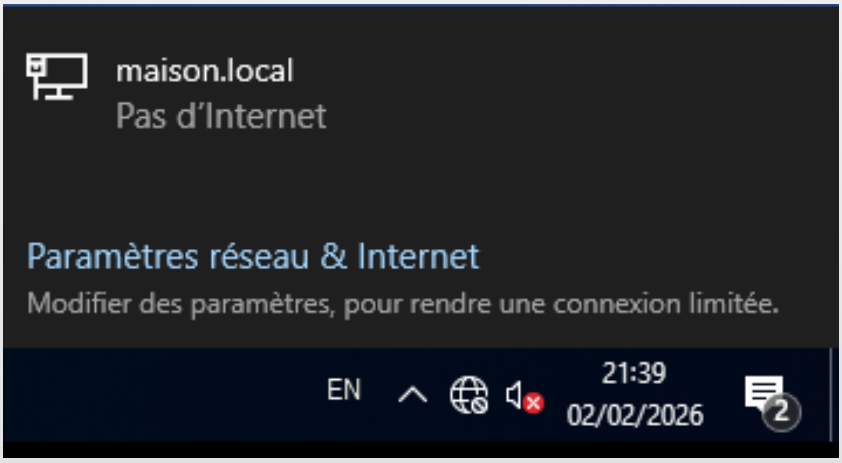


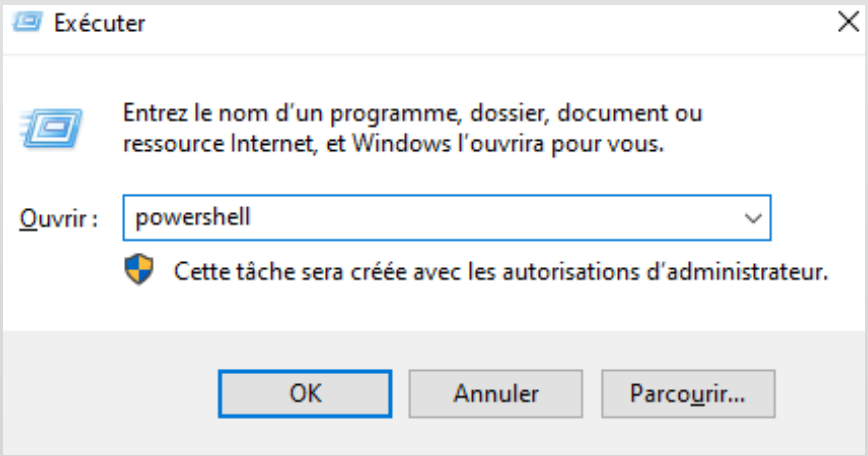
3.2.2. **Incident n°2 :**

La VM Windows Server ne reçoit pas l'internet du PfSense (no route to host quand ping 8.8.8.8). Donc création du fichier test via PowerShell.

```
Enter a host name or IP address: 8.8.8.8

ping: sendto: No route to host
ping: sendto: No route to host
ping: sendto: No route to host
^CVMware Virtual Machine - Netgate Device ID: 73caec097108974ade18
```






```
S C:\Users\Administrateur> fsutil file createnew E:\Partages\Commun\fichier_test.dat 600000000
rreur :  Espace insuffisant sur le disque.
S C:\Users\Administrateur>
```

4. POINTS FUTURS A POUSSER :

- **L'alerte par mail ou Log**

→ *Lorsqu'un utilisateur essaye de déposer un fichier "indésirable" un mail est envoyé a la personne désignée. Ceci est une preuve de "Journallisatoin et d'Audit.*

- **La Corbeille Active Directory**

→ *Cette fonctionnalité permet une restauration rapide des objets supprimés par erreur, sans avoir à restaurer une sauvegarde complète de l'état du système.*

- **L'Audit des accès aux fichiers**

→ Permet de tracer les actions sensibles comme la suppression de document et donc d'en connaitre son auteur.

- **La Double Authentification (2FA) sur le VPN**

→ *Renforce l'authentification. Même si le mot de passe d'un employé est volé, l'attaquant ne peut pas entrer sans le code unique sur le téléphone.*

- **Le Failover DNS / DHCP**

→ *L'objectif est d'éliminer le 'Single Point of Failure' (Point de défaillance unique). Si le serveur 1 tombe, le serveur 2 prend le relais instantanément.*"

5. BILAN :

5.1. **Bilan Technique**

La mise en œuvre de ce serveur de fichiers sous Windows Server 2022 a permis de répondre point par point aux exigences du cahier des charges initial. L'utilisation du RAID 1 (Miroir) garantit une tolérance aux pannes matérielles, assurant la disponibilité immédiate des données. La gestion rigoureuse des permissions NTFS et la rupture de l'héritage ont permis d'instaurer un cloisonnement strict des accès, respectant ainsi le principe de confidentialité des données sensibles de l'entreprise (Direction, Comptabilité).

5.2. **Optimisation et Maîtrise des Ressources**

Au-delà de la simple gestion des droits, l'installation du rôle FSRM a apporté une couche de contrôle indispensable. La mise en place de quotas inconditionnels prévient la saturation du stockage, tandis que le filtrage de fichiers actifs protège le serveur contre l'usage abusif de l'espace disque (fichiers non professionnels) et réduit les vecteurs de risques liés aux fichiers exécutables.

5.3. **Apport Personnel et Analyse**

Cette mission m'a permis de consolider mes compétences en administration de services de domaine (AD DS) et de comprendre l'importance d'une structure de données organisée pour les utilisateurs finaux. J'ai appris à anticiper les erreurs humaines (suppression accidentelle, saturation disque) et à automatiser la politique de sécurité de l'entreprise via les outils natifs de Microsoft.

5.4. **Ouverture vers la Cybersécurité (Lien vers l'E6)**

Si l'infrastructure interne est désormais sécurisée et robuste, la problématique de l'accès à ces données pour les collaborateurs nomades reste entière. L'exposition de ces services sur Internet représenterait un risque majeur (attaques par force brute, interception de données).

→ **Transition** : C'est pourquoi, dans la continuité de cette sécurisation, l'étape suivante (E6) portera sur la mise en place d'un tunnel sécurisé VPN (OpenVPN) via le pare-feu pfSense, afin de garantir une authentification forte et un chiffrement des flux pour tout accès distant au serveur de fichiers.