installation-adds

```
        Mark Roderick
```

=[[=Active DirectoryAD DS==]]= permet de gérer les utilisateurs, objets
alternatif de Active Directory c'est LDAP=**Lightweight Directory Access Protocol**, est un protocole utilisé pour accéder et gérer les services d'annuaire sur un réseau TCP/IP
Installation AD DS

Active Directory (AD), c’est le cerveau et le système nerveux d’un réseau Windows. Sans lui, gérer un parc de 100 ordinateurs et 100 utilisateurs serait un cauchemar administratif.

---

1. C'est quoi, concrètement ?

Active Directory est un **service d'annuaire**. Imaginez un annuaire géant qui contient non seulement les noms des utilisateurs, mais aussi leurs mots de passe, leurs droits, leurs ordinateurs, les imprimantes du réseau, etc.

Ses deux rôles principaux sont :

1. **Authentification :** Vérifier que vous êtes bien qui vous prétendez être (Le "Login").
2. **Autorisation :** Vérifier que vous avez le droit d'accéder à telle ressource ou tel dossier.

---

2. La Structure Logique (La Hiérarchie)

L'AD organise les objets de manière hiérarchique, un peu comme des poupées russes :

- **Les Objets :** C'est l'unité de base (un utilisateur, un ordinateur, un groupe, une imprimante).
- **Les Unités d'Organisation (OU) :** Des "dossiers" pour ranger vos objets. C’est ici qu’on lie les **GPO**.
- **Le Domaine :** La limite administrative. Tous les objets partagent la même base de données (ex: `entreprise.local`).
- **L'Arbre (Tree) :** Un regroupement de domaines qui partagent un nom de racine commun.
- **La Forêt (Forest) :** Le niveau le plus haut. Elle regroupe tous les domaines. C'est la limite de sécurité ultime.

---

3. Les Composants Physiques

- **Le Contrôleur de Domaine (DC - Domain Controller) :** C'est le serveur qui héberge le service Active Directory. C'est lui qui répond quand vous tapez votre mot de passe.
- **Le Catalogue Global (GC) :** Un serveur qui contient une copie de tous les objets de la forêt (utile pour les recherches rapides).
- **La Réplication :** Si vous avez deux serveurs AD, ils se "parlent" en permanence pour que si vous changez un mot de passe sur le serveur A, le serveur B soit au courant instantanément.

---

4. Les 3 Piliers Techniques (Le moteur sous le capot)

Pour qu'Active Directory fonctionne, il s'appuie sur trois technologies standards :

1. **DNS (Le plus important) :** Sans DNS, l'AD ne fonctionne pas. Le DNS permet aux PC de trouver où se cache le Contrôleur de Domaine.
2. **LDAP (Lightweight Directory Access Protocol) :** C'est la langue parlée par l'AD pour lire et modifie les informations dans l'annuaire.
3. **Kerberos :** C'est le protocole de sécurité qui gère l'authentification via un système de "tickets" (très sécurisé).

---

5. Les outils de gestion

Pour administrer l'AD, vous utiliserez principalement ces consoles (accessibles via les outils RSAT) :

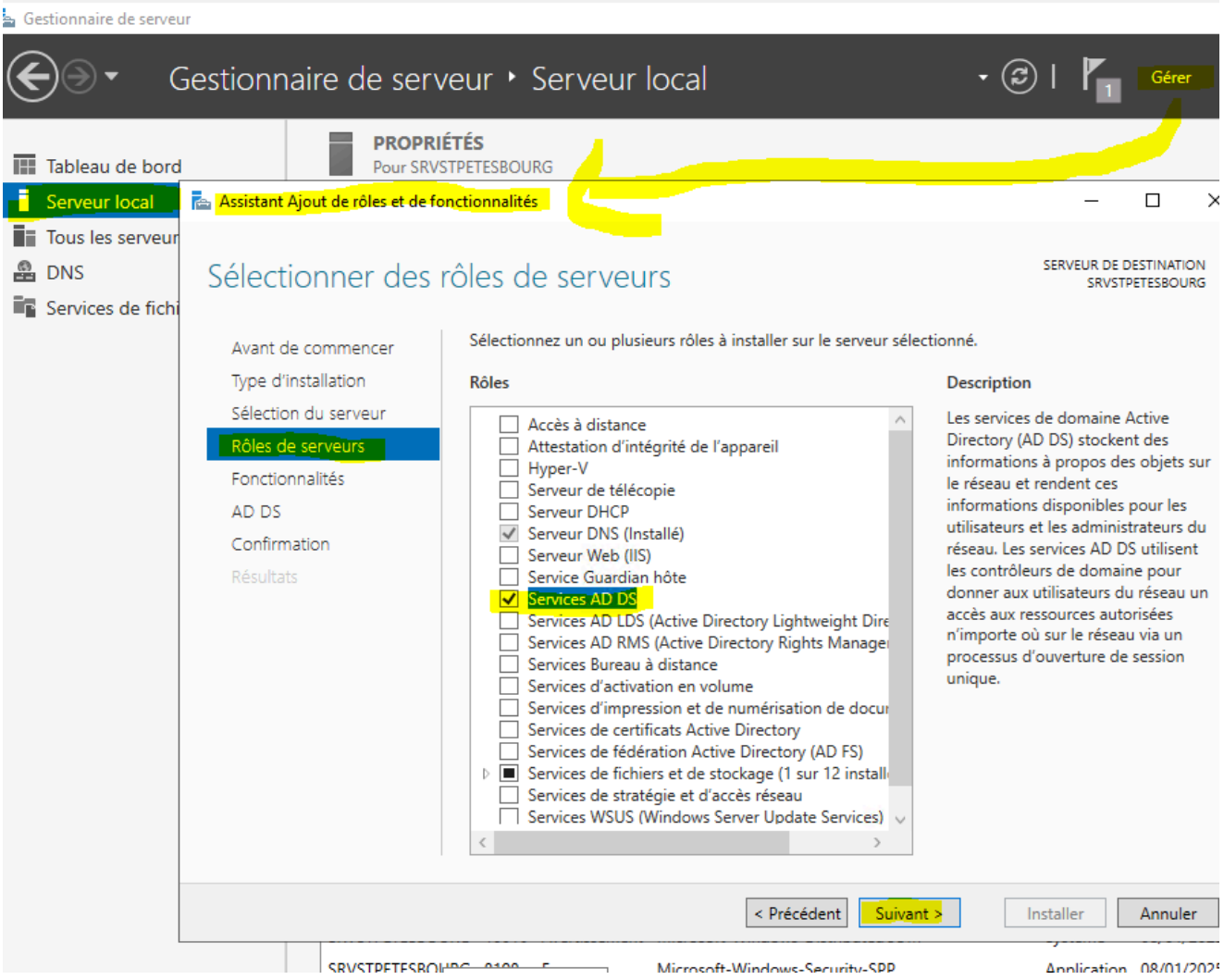
Outil	Nom de la console	Usage
ADUC	`dsa.msc`	Créer des utilisateurs, des groupes et des ordinateurs.
ADAC	(Centre d'admin)	Version moderne d'ADUC avec corbeille AD intégrée.
Sites et Services	`dssite.msc`	Gérer la réplication entre différents bureaux physiques.
Domaines et Approbations	`domain.msc`	Gérer les relations entre plusieurs domaines.

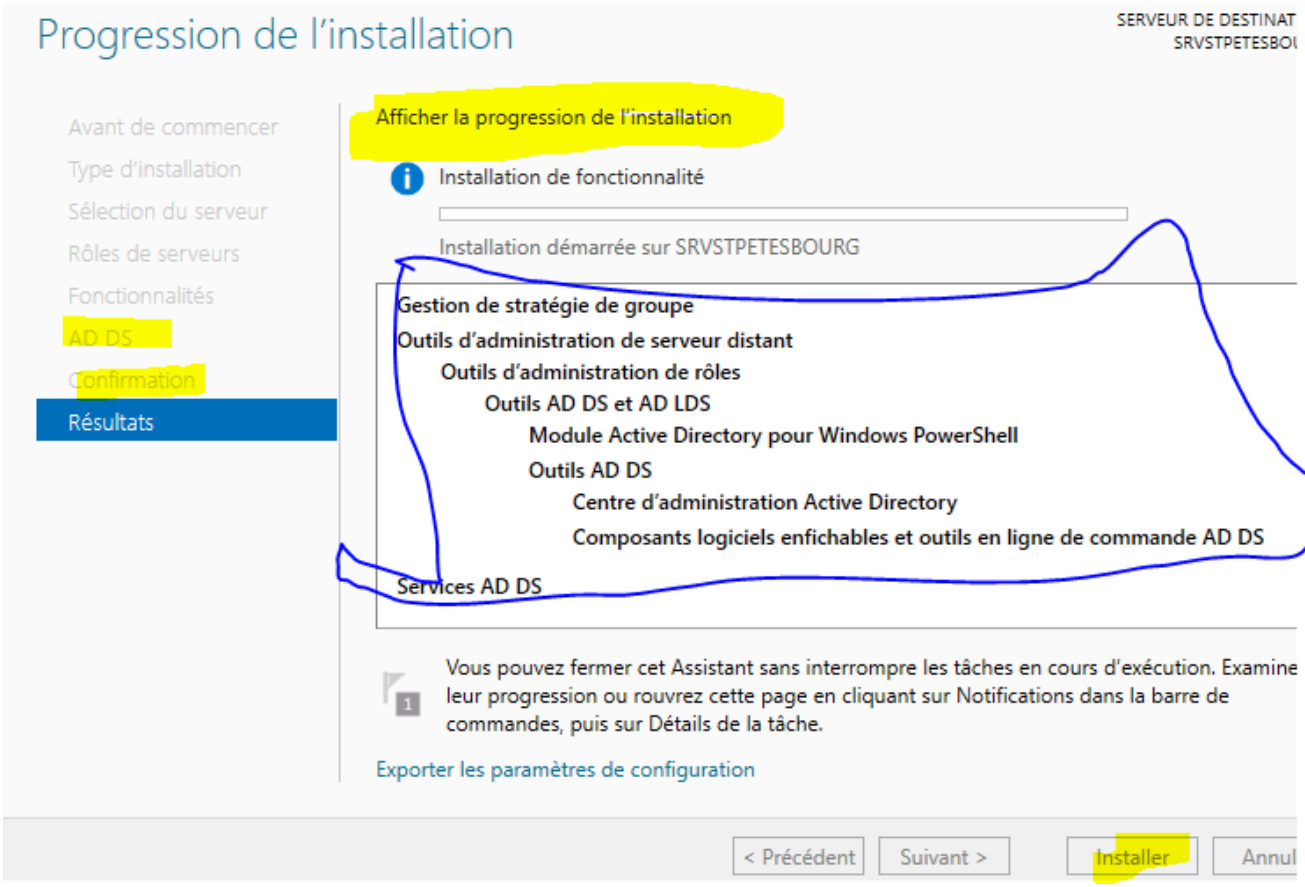
🚀 Le cycle de vie d'une session AD

Quand un utilisateur allume son PC le matin :

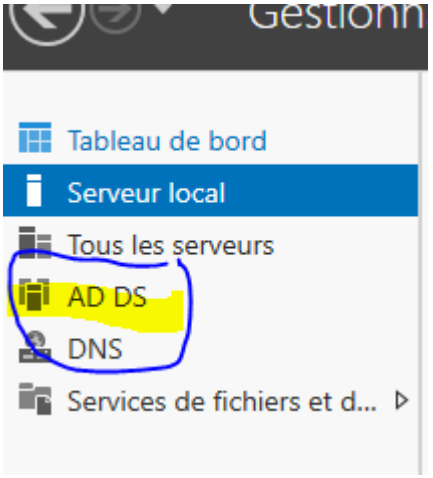
1. Le PC demande au **DNS** : *"Où est le contrôleur de domaine ?"*
2. Le DNS répond : *"Il est à l'adresse 192.168.1.10"*.
3. L'utilisateur tape son login/pass. Le PC contacte le DC via **Kerberos**.
4. Le DC vérifie et renvoie un "Ticket".
5. Le PC télécharge les **GPO** (fond d'écran, lecteurs réseaux) et ouvre la session.

> **Le conseil de l'expert :** Ne travaillez jamais directement sur le compte "Administrateur" du domaine pour vos tâches quotidiennes. Créez-vous un compte utilisateur standard et un compte admin séparé pour éviter les bêtises (ou les malwares).



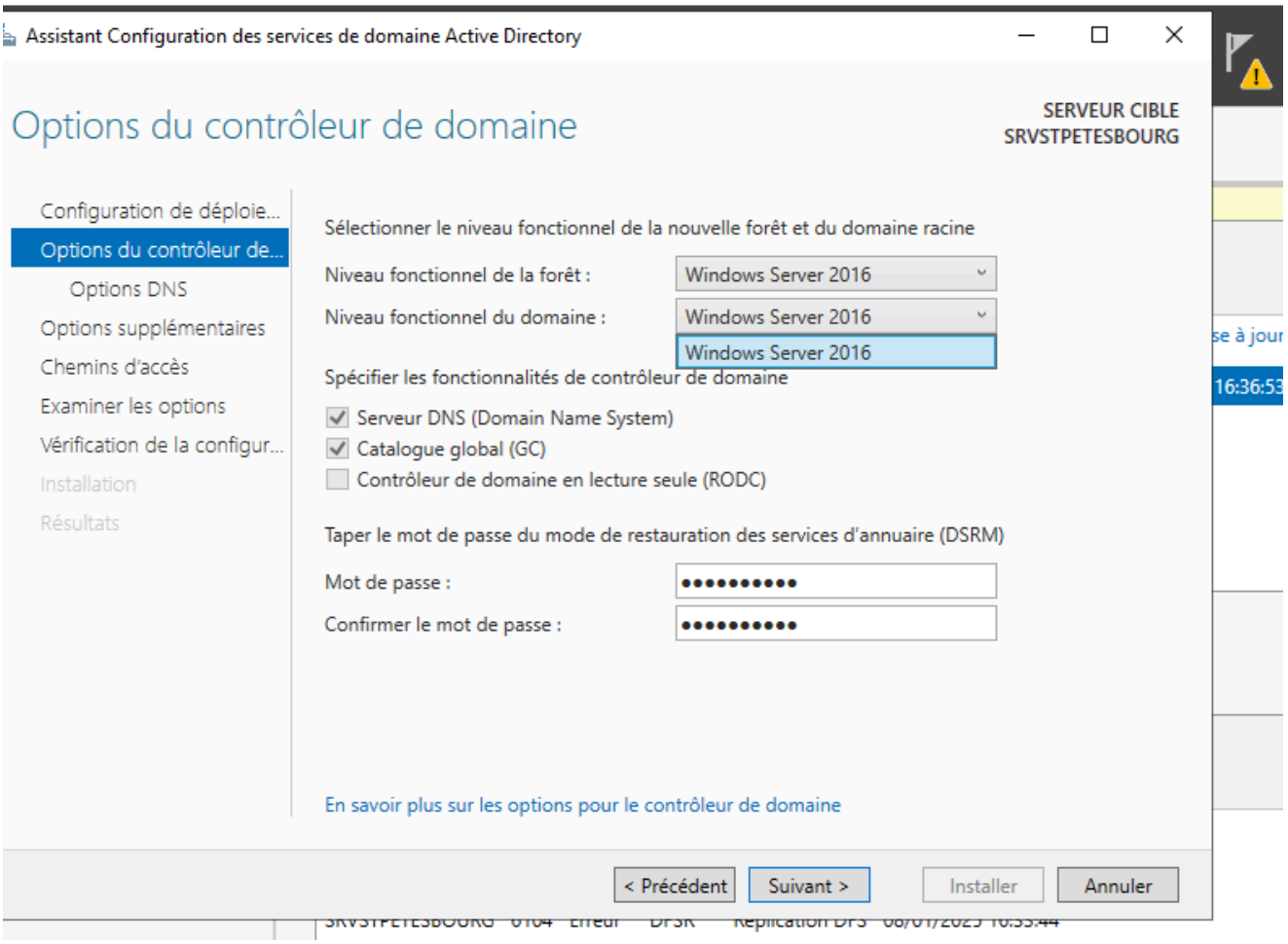


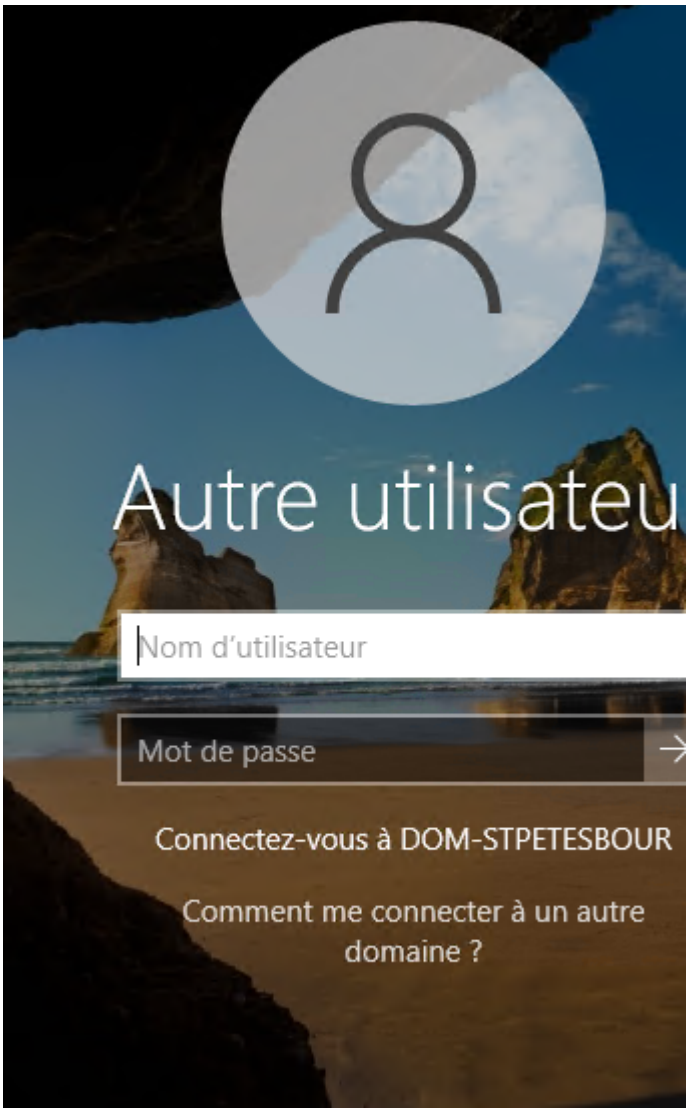
FIN de linstallation



mdp : Azerty123!

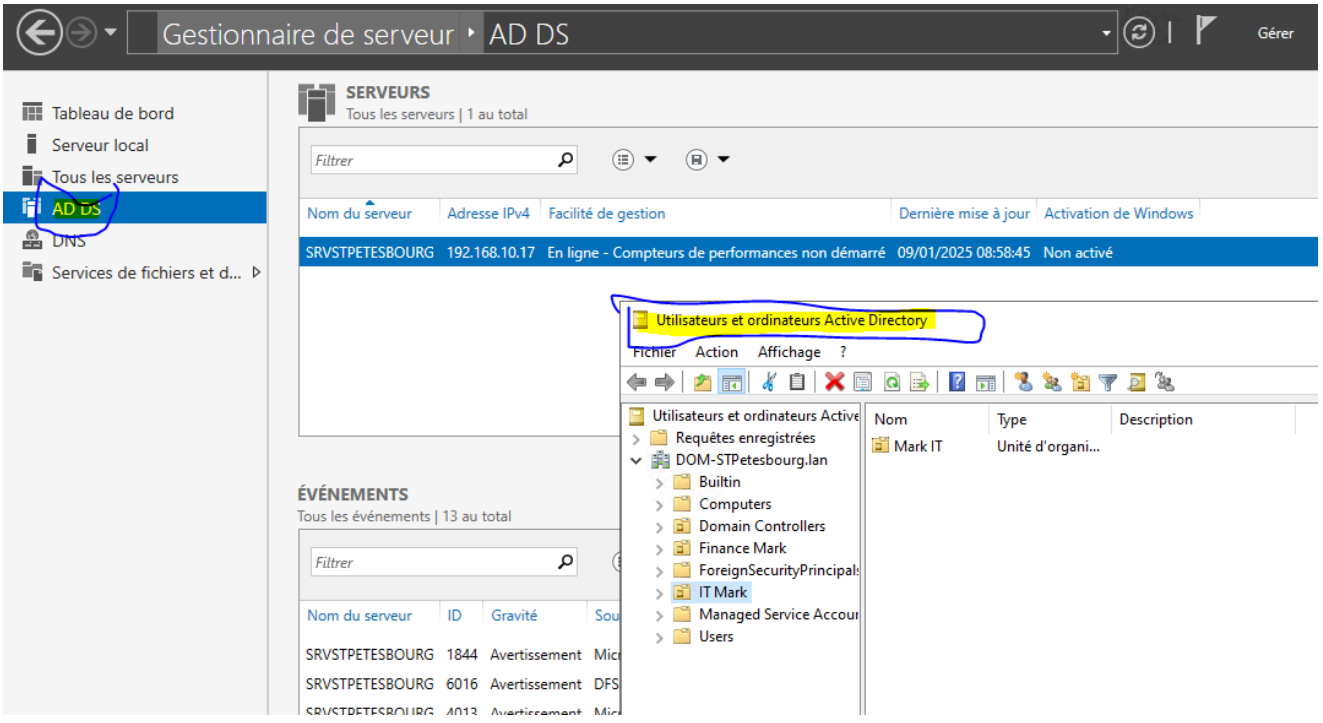
onnaire de serveur

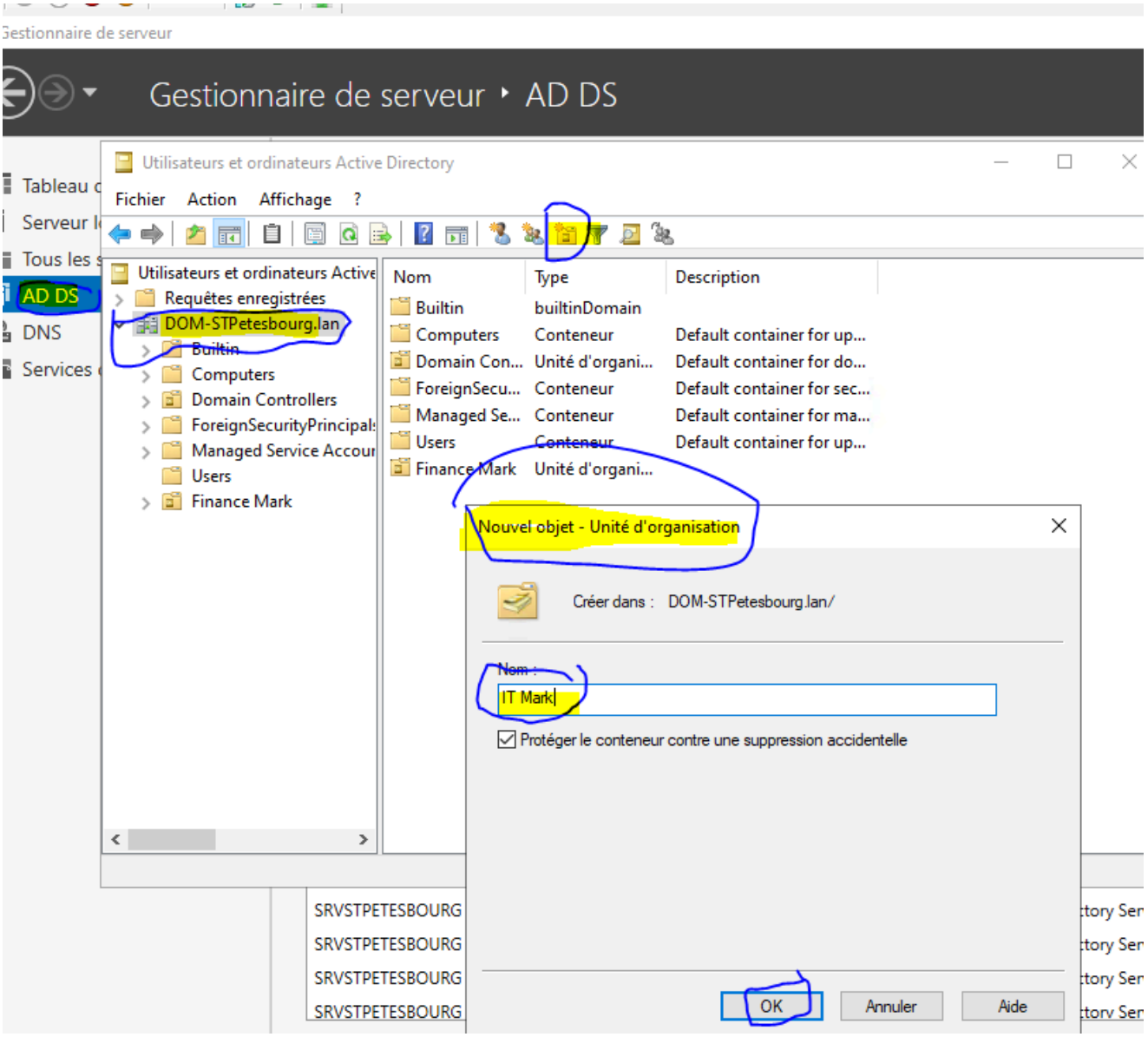




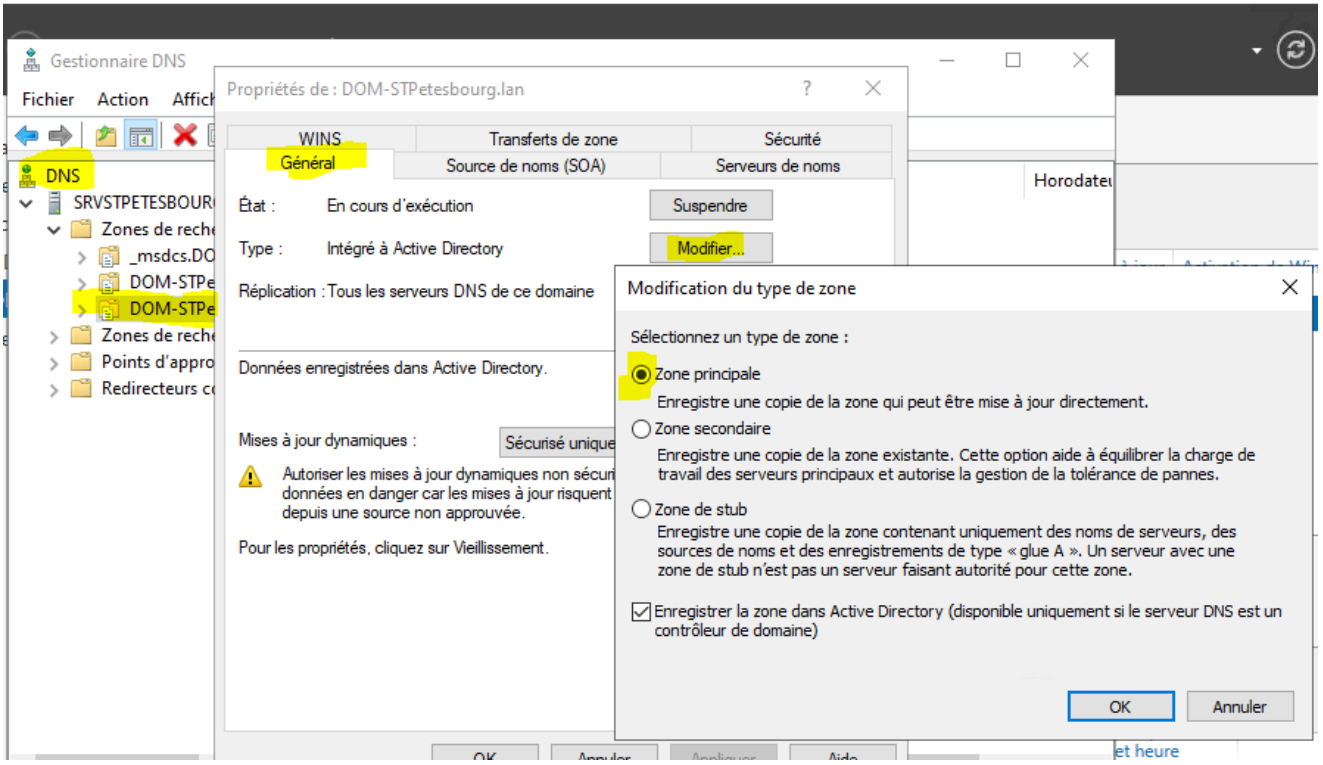
identifiant : administrateur
mdp: Azerty123! its actually Azerty123

gestionnaire de serveur AD DS
Pour ajouter un objet



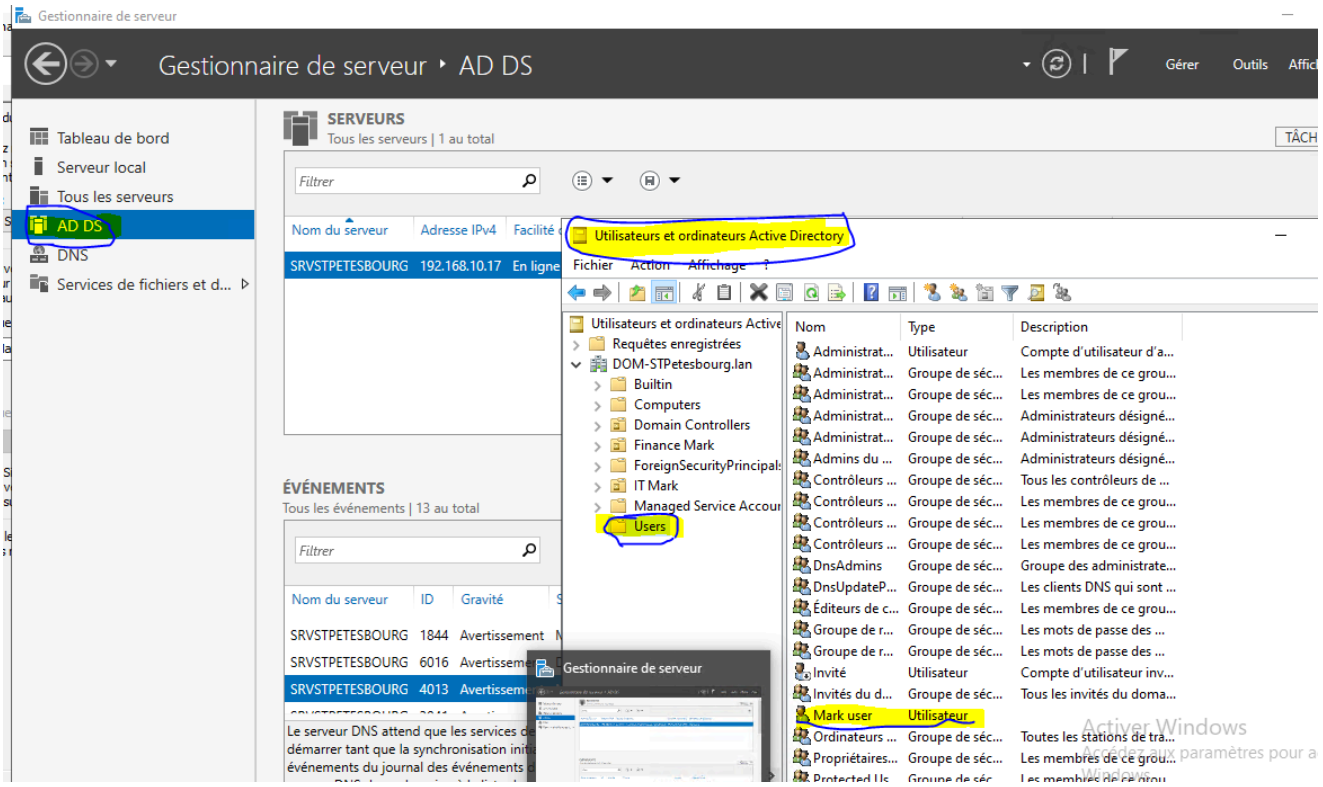

Gestionnaire de serveur
Gestionnaire de serveur ‣ AD DS
Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage ?
Utilisateurs et ordinateurs Active
Requêtes enregistrées
DOM-STPetesbourg.lan
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Users
Finance Mark
Nom Type Description
Builtin builtinDomain
Computers Conteneur Default container for up...
Domain Con... Unité d'organi... Default container for do...
ForeignSecu... Conteneur Default container for sec...
Managed Se... Conteneur Default container for ma...
Users Conteneur Default container for up...
Finance Mark Unité d'organi...
Nouvel objet - Unité d'organisation
Créer dans : DOM-STPetesbourg.lan/
Nom :
IT Mark
Protéger le conteneur contre une suppression accidentelle
OK
Annuler
Aide
SRVSTPETESBOURG
SRVSTPETESBOURG
SRVSTPETESBOURG
SRVSTPETESBOURG

RT


Gestionnaire DNS
Fichier Action
DNS
SRVSTPETESBOUR
Zones de reche
_msdcs.DO
DOM-STPe
DOM-STPe
Zones de reche
Points d'appro
Redirecteurs c
Propriétés de : DOM-STPetesbourg.lan
WINS
Transferts de zone
Sécurité
Général
Source de noms (SOA)
Serveurs de noms
État : En cours d'exécution
Suspendre
Type : Intégré à Active Directory
Modifier...
Réplication : Tous les serveurs DNS de ce domaine
Données enregistrées dans Active Directory.
Mises à jour dynamiques :
Sécurisé unique
Autoriser les mises à jour dynamiques non sécuri
données en danger car les mises à jour risquent
depuis une source non approuvée.
Pour les propriétés, cliquez sur Vieillissement.
Horodateu
Modification du type de zone
Sélectionnez un type de zone :
Zone principale
Enregistre une copie de la zone qui peut être mise à jour directement.
Zone secondaire
Enregistre une copie de la zone existante. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.
Zone de stub
Enregistre une copie de la zone contenant uniquement des noms de serveurs, des sources de noms et des enregistrements de type « glue A ». Un serveur avec une zone de stub n'est pas un serveur faisant autorité pour cette zone.
Enregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS est un contrôleur de domaine)
OK
Annuler

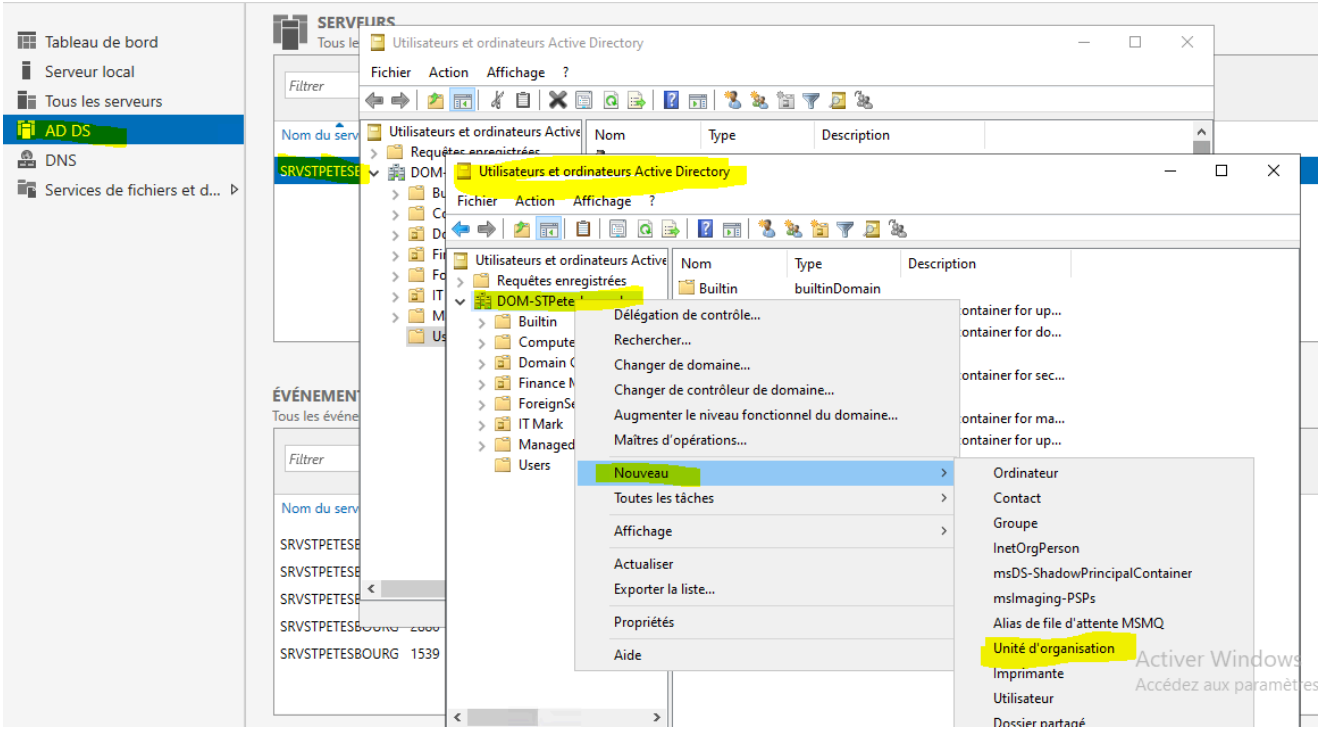
SUR AD DS

Sur gestionnaire de serveur, vous pouvez alors aller l'outil Gestionnaire « Utilisateurs et Ordinateurs » Puis créer votre 1er utilisateur !

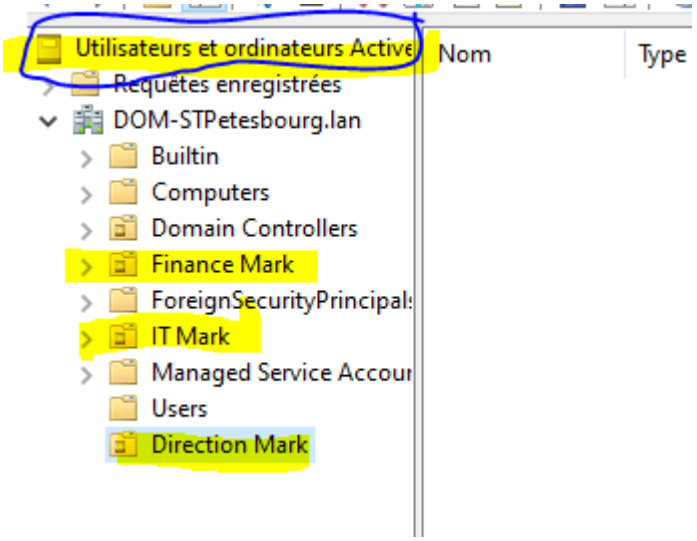


PARTIE 2

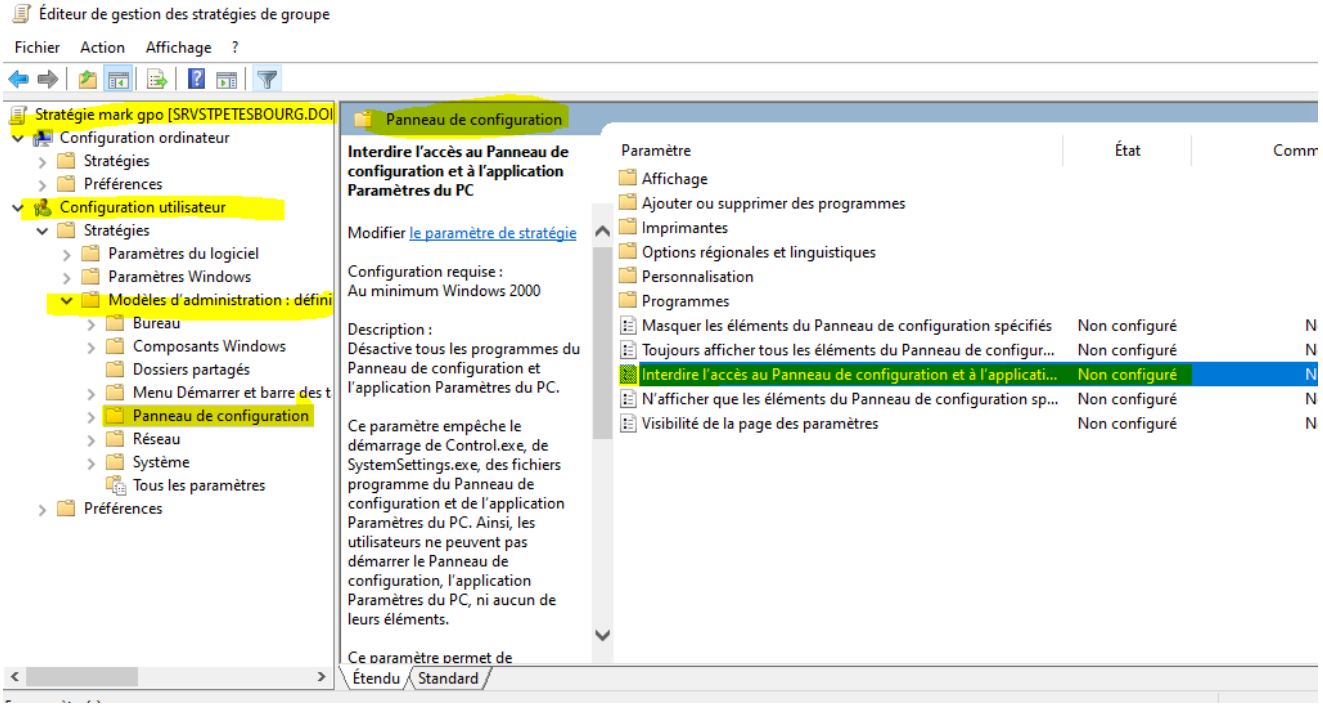
CREATION UNITAIRE DES UTILISATEURS



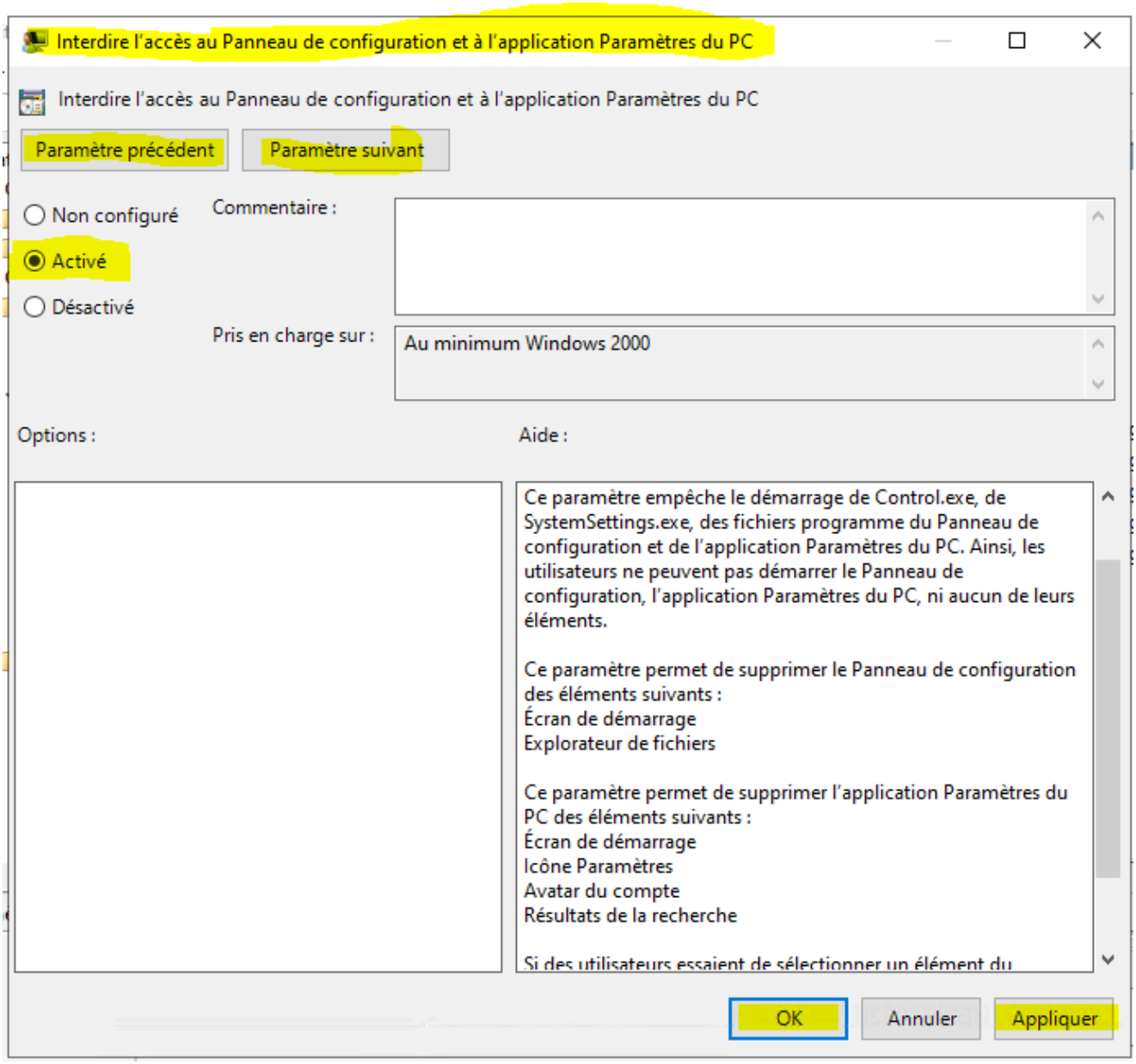
on creer 3 unités d'organisation



Exemple GPO (bloquer le panneau de configuration) : aller dans : gestion des sttratégie de groupe – l'unité d'organisation qui contient les utilisateurs – clic droit « créer un objet GPO dans ce domaine, et le lier ici » et le nommet celon le GPO qui vas être mis en place, ici « bloquer panneaux de configuration » - ensuite faire un clic droit sur le GPO – configuration utilisateur – modèles d'dministration – panneau de configuration – « interdire l'accès au panneau de configuration et à l'application spécifiés » et faire activé.



panneau de configuration

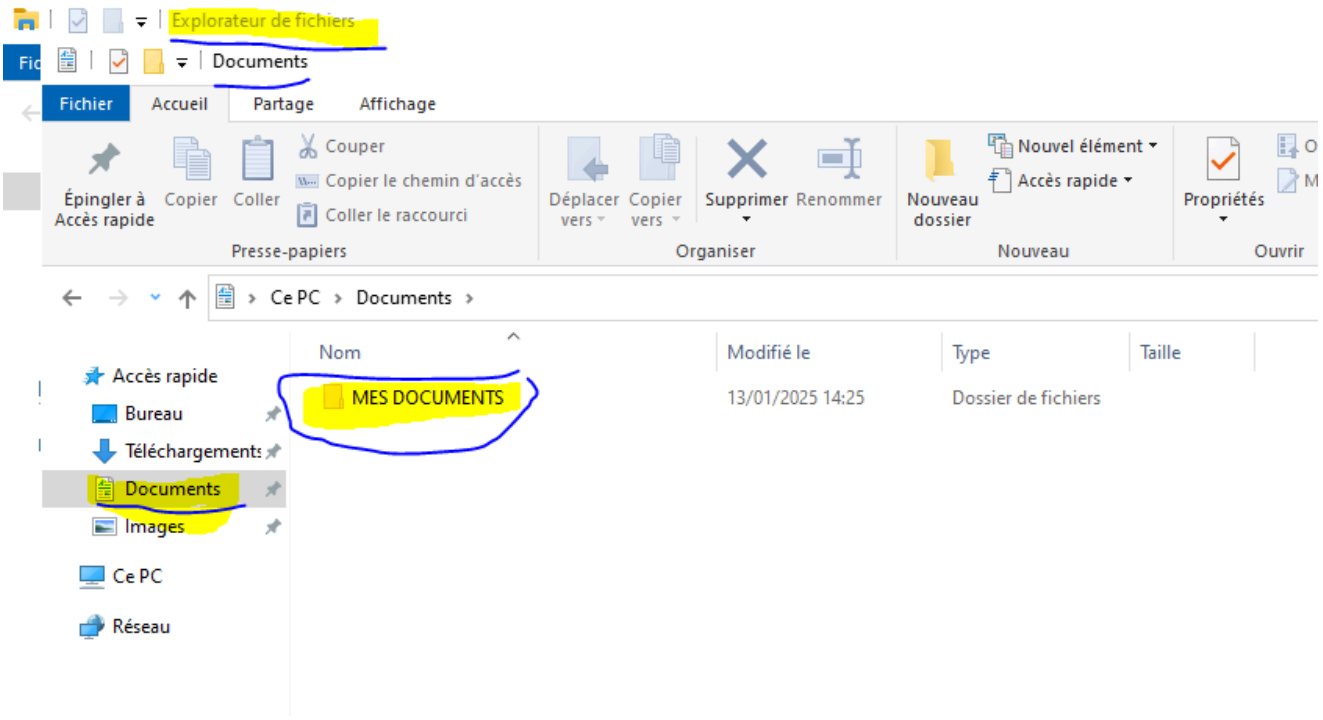


REDIRECTION DES **MES DOCUMENTS**

Pour que les dossiers « mes documents » des utilisateurs soient enregistrés sur le serveur sans que l'utilisateur n'ait de manipulations supplémentaires à effectuer.

1 – Créer un dossier partagé et donner des autorisations de partage aux utilisateurs authentifié

On creee un dossier dans documents dans l'explorateur des fichiers



Strategie de groupe Active Directory

Les **GPO** (*Group Policy Objects*) ou **Stratégies de Groupe** sont l'outil le plus puissant d'un administrateur Windows. Elles permettent de centraliser la configuration des utilisateurs et des ordinateurs au sein d'un domaine Active Directory.

---

1. Qu'est-ce qu'une GPO ?

Une GPO est un ensemble de paramètres de configuration. Au lieu de passer sur chaque poste pour changer un fond d'écran ou désactiver le panneau de configuration, vous créez une règle sur le serveur et elle s'applique à des milliers de machines instantanément.

On distingue deux grandes catégories dans une GPO :

- **Configuration Ordinateur :** S'applique au démarrage de la machine (ex: paramètres réseau, sécurité locale).
- **Configuration Utilisateur :** S'applique à l'ouverture de session (ex: lecteurs réseaux, paramètres Outlook).

---

2. La Hiérarchie d'application (LSDOU)

L'ordre dans lequel les stratégies s'appliquent est crucial, car la dernière stratégie appliquée écrase les précédentes en cas de conflit. C'est la règle **LSDOU** :

1. **L**ocal (Stratégie de la machine locale)
2. **S**ite (Niveau AD)

3. **D**omaine (Niveau AD)
4. **OU** (Unités d'Organisation - les dossiers dans votre AD)

> **Règle d'or :** Plus la stratégie est proche de l'objet (dans une OU profonde), plus elle a de poids.

---

3. Fonctionnement Technique

Une GPO est composée de deux parties :

- **GPC (Group Policy Container) :** L'objet visible dans l'Active Directory (contient le nom, l'ID, le statut).
- **GPT (Group Policy Template) :** Les fichiers réels stockés sur le dossier partagé `SYSVOL` des contrôleurs de domaine. C'est là que se trouvent les scripts et les fichiers `.pol`.

---

4. Gérer l'Héritage et les Exceptions

Parfois, vous voulez qu'une règle ne s'applique pas à tout le monde.

- **Blocage de l'héritage :** Une OU peut dire "Je ne veux pas des stratégies venant d'en haut".
- **Application forcée (Enforced) :** Une stratégie de haut niveau peut dire "Je m'applique quand même, même si l'héritage est bloqué en bas".
- **Filtrage de sécurité :** Vous pouvez appliquer une GPO uniquement à un groupe de sécurité spécifique plutôt qu'à toute l'OU.
- **Filtres WMI :** Permet d'appliquer une GPO selon des critères matériels (ex: "Appliquer uniquement si c'est un PC portable" ou "uniquement si c'est Windows 11").

---

5. Les outils indispensables

En tant qu'admin, tu dois connaître ces commandes par cœur :

Outil / Commande	Description
gpmc.msc	La console graphique pour créer et lier les GPOs.
gpupdate /force	Force la machine à aller chercher les nouvelles GPOs immédiatement.

Outil / Commande	Description
gpresult /r	Affiche quelles GPOs sont réellement appliquées sur le poste actuel.
rsop.msc	(Resultant Set of Policy) Interface graphique pour voir le résultat final des réglages.

🚀 Meilleures Pratiques (Best Practices)

1. **Une GPO = Une fonction :** Ne créez pas une énorme GPO "Paramètres_Généraux". Créez une GPO "Sécurité_Mots_De_Passe", une GPO "Lecteurs_Réseaux", etc. C'est plus facile pour le dépannage.
2. **Désactivez les sections inutilisées :** Si votre GPO n'a que des paramètres "Utilisateurs", désactivez la partie "Ordinateur" pour accélérer le traitement.
3. **Évitez les GPO au niveau Domaine :** Préférez l'application au niveau des Unités d'Organisation (OU) pour plus de précision.
4. **Testez toujours :** Créez une OU "Test" avant de déployer une règle qui pourrait bloquer tout le réseau.

Le mappage de lecteur réseau via GPO est l'une des tâches les plus courantes et les plus utiles en administration système. Autrefois, on utilisait des scripts d'ouverture de session (des fichiers `.bat` avec la commande `net use`). Aujourd'hui, on utilise les **Préférences de Stratégie de Groupe (GPP)**, qui sont beaucoup plus puissantes et visuelles.

Voici un cours complet et pratique pour déployer des lecteurs réseaux.

---

1. Pourquoi utiliser les GPO pour les lecteurs réseaux ?

- **Zéro script :** Tout se fait via une interface graphique propre.
- **Ciblage précis :** Tu peux dire "Monte le lecteur `Z:` uniquement si l'utilisateur fait partie du groupe 'Comptabilité' ".
- **Nettoyage automatique :** Tu peux configurer la GPO pour supprimer le lecteur si l'utilisateur change de service.

---

2. Prérequis (Ce qu'il faut préparer avant)

1. **Un dossier partagé :** Tu dois avoir un dossier partagé sur un serveur de fichiers, et connaître son chemin UNC (ex: `\\Serveur-Fichiers\Partage_Compta`).

2. **Des droits NTFS et Partage :** Les utilisateurs cibles doivent avoir le droit de lire/écrire dans ce dossier.
3. **Une OU cible :** Les lecteurs réseaux s'appliquent aux **UTILISATEURS** (pas aux ordinateurs). Ta GPO devra donc être liée à une Unité d'Organisation (OU) qui contient tes utilisateurs.

---

3. Étape par Étape : Créer la GPO de Mappage

Étape 1 : Créer et lier la GPO

1. Ouvre la console de gestion des stratégies de groupe (`gpmc.msc`).
2. Fais un clic droit sur l'OU contenant tes utilisateurs (ex: `OU=Employes`) et choisis **Créer un objet GPO dans ce domaine, et le lier ici**.
3. Nomme ta GPO de façon claire : `GPO_MAP_Compta` .

Étape 2 : Éditer la GPO

1. Fais un clic droit sur `GPO_MAP_Compta` > **Modifier**.
2. Navigue dans cet arbre exact :

   👉 **Configuration utilisateur**

   👉 **Préférences**

   👉 **Paramètres Windows**

   👉 **Mappages de lecteurs**

Étape 3 : Configurer le lecteur réseau

1. Dans la zone de droite, fais un clic droit > **Nouveau** > **Lecteur mappé**.
2. Une fenêtre de propriétés s'ouvre. C'est ici que la magie opère.

---

4. Les 4 Actions de mappage (Très important ⚠️)

Dans la fenêtre, le premier menu déroulant s'appelle "Action". Il faut bien comprendre les différences :

Action	Ce que ça fait	Quand l'utiliser ?
Créer	Crée le lecteur s'il n'existe pas. Ne fait rien s'il existe déjà.	Rarement utilisé.

Action	Ce que ça fait	Quand l'utiliser ?
Mettre à jour	**(Le plus courant)** Crée le lecteur s'il n'existe pas. S'il existe, il met à jour ses paramètres.	C'est l'option recommandée par défaut.
Remplacer	Supprime le lecteur existant et le recrée.	Utile si tu as changé le chemin du serveur, mais cela coupe brièvement la connexion de l'utilisateur.
Supprimer	Supprime le lecteur `Z:` du poste.	Pour nettoyer les anciens lecteurs inutiles.

Configuration des autres champs :

- **Emplacement :** Le chemin UNC (ex: `\\Serveur1\Compta`).
- **Se reconnecter :** Coche cette case (équivalent du `/persistent:yes`).
- **Étiqueter en tant que :** Le nom qui s'affichera dans "Ce PC" (ex: `Dossier Comptabilité`).
- **Lettre de lecteur :** Choisis une lettre (ex: `M:`). Choisis l'option *Utiliser la lettre*.

---

5. Le "Ciblage au niveau de l'élément" (Le secret des Pros 🚀)

C'est la fonctionnalité la plus puissante des Préférences GPO. Au lieu de créer 10 GPO différentes pour 10 services, tu peux créer une seule GPO globale et définir des règles pour chaque lecteur.

1. Dans la fenêtre de ton lecteur mappé, va dans l'onglet **Commun** (Common).
2. Coche la case **Ciblage au niveau de l'élément** (Item-level targeting), puis clique sur le bouton **Ciblage...**.
3. Clique sur **Nouvel élément** > **Groupe de sécurité**.
4. Sélectionne le groupe AD `GRP_Comptabilite`.

Résultat : Ce lecteur réseau s'installera *uniquement* pour les utilisateurs qui sont membres du groupe "Comptabilité", même si la GPO est appliquée à toute l'entreprise !

---

6. Tester et Dépanner

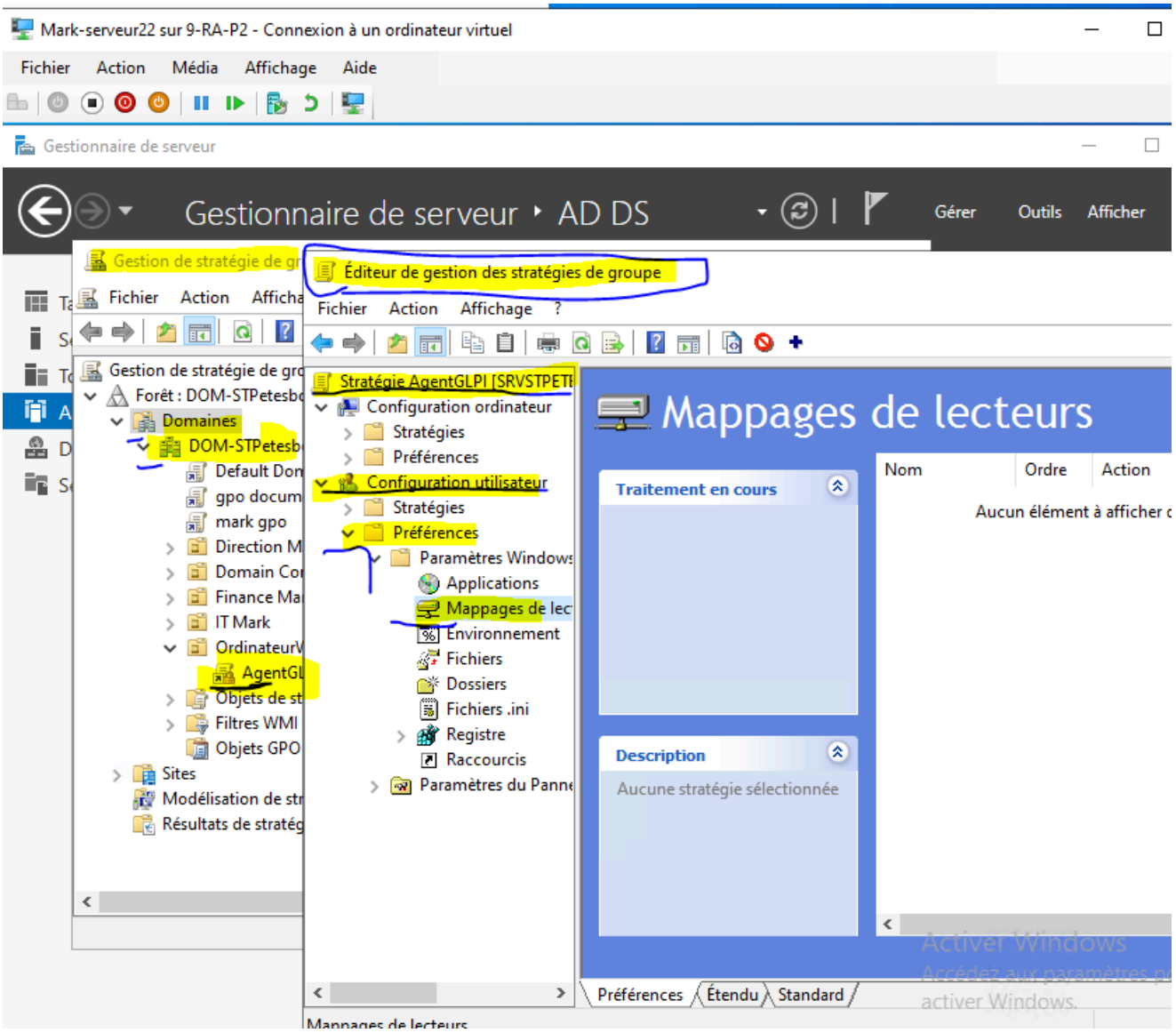
Une fois la GPO fermée, elle est active. Pour vérifier que ça fonctionne :

1. Connecte-toi sur un PC client avec un utilisateur cible.

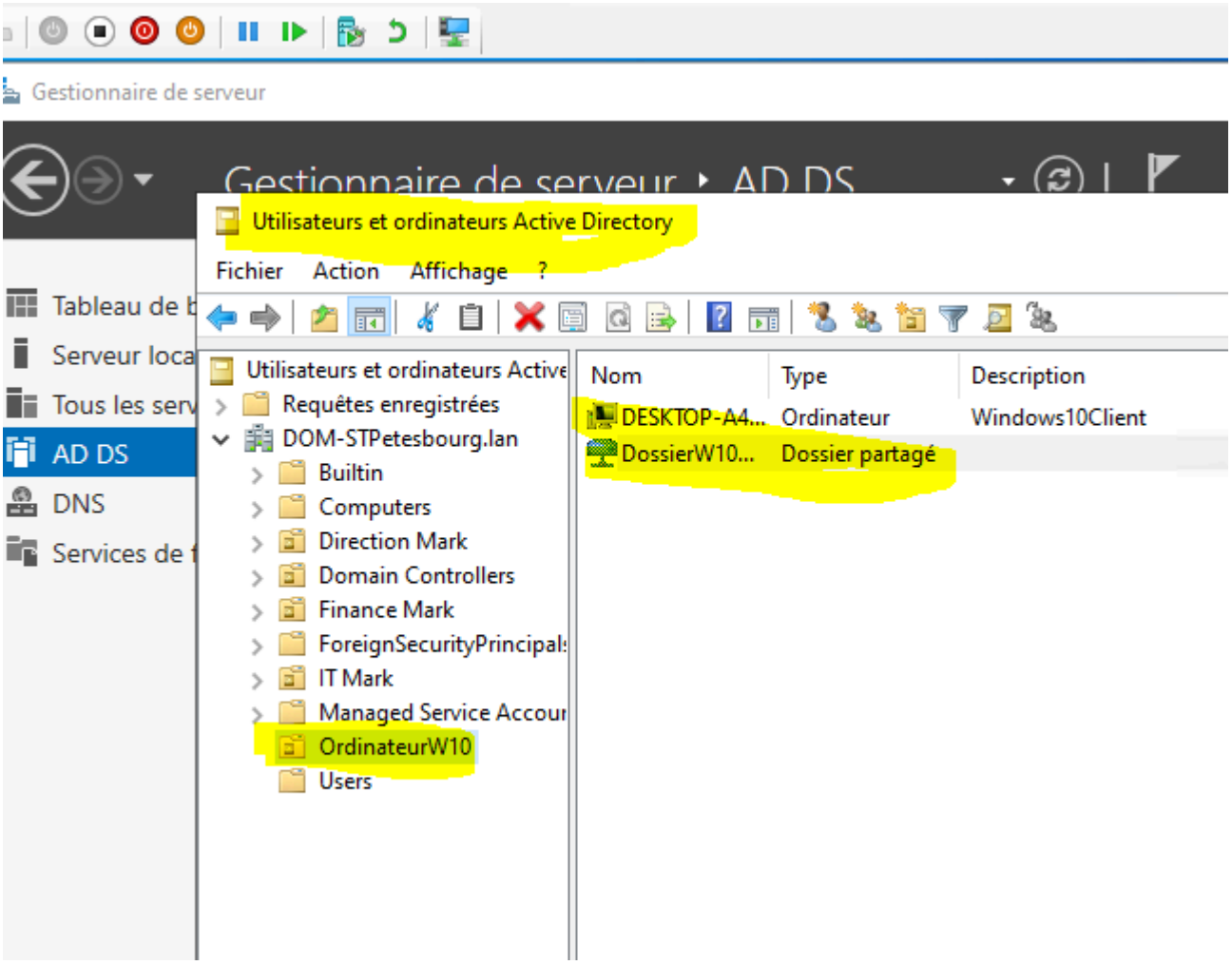
2. Ouvre l'invite de commande (cmd) et tape : `gpupdate /force` (pour forcer la mise à jour des GPO).
3. Ouvre l'explorateur de fichiers : le lecteur réseau devrait apparaître instantanément.

En cas de problème (Dépannage) :

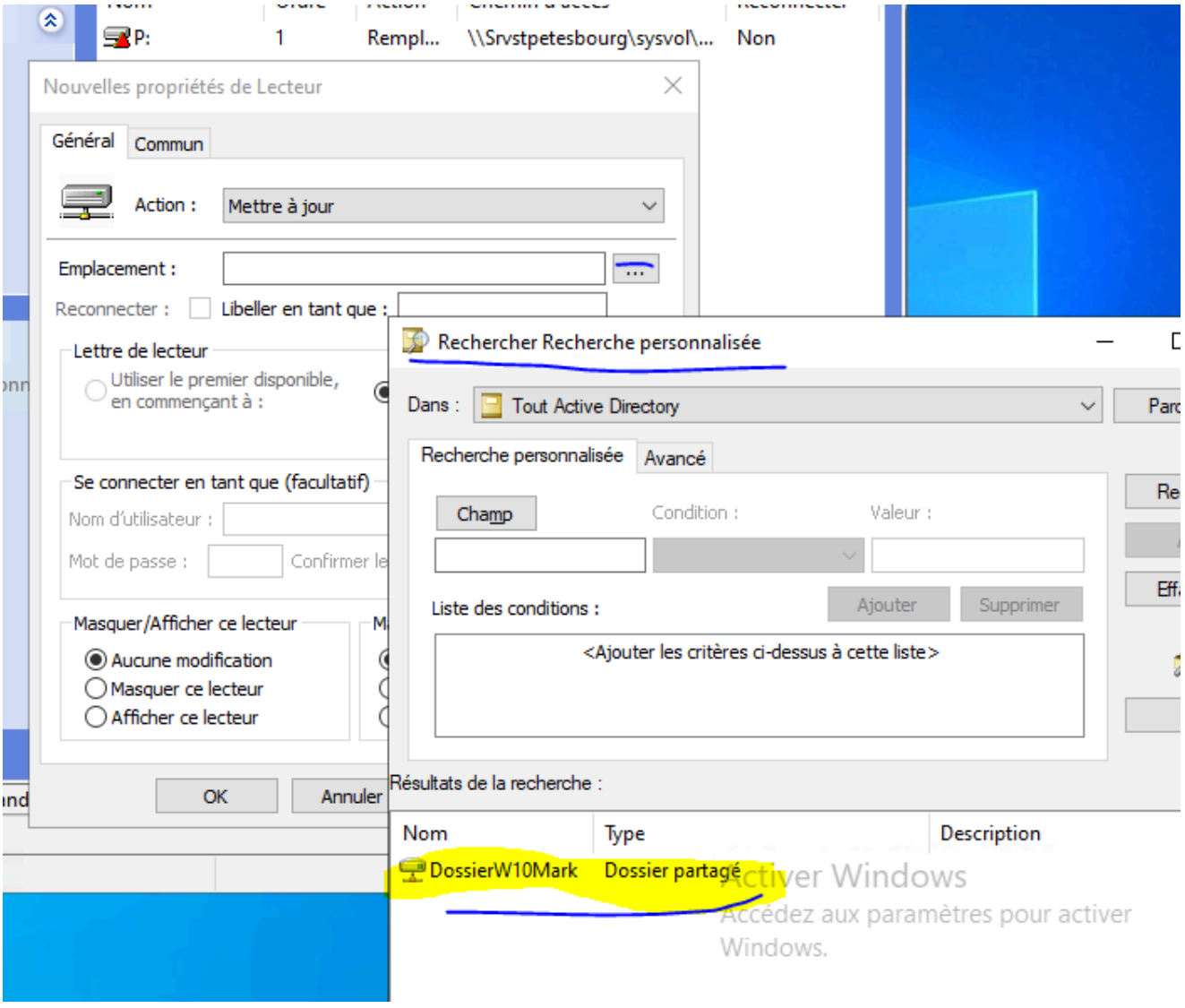
- **Le lecteur ne monte pas :** L'utilisateur a-t-il les droits NTFS pour lire le dossier partagé ? Si le dossier lui est interdit, la GPO ne montera pas le lecteur.
- **Mauvaise OU :** Ta GPO est-elle bien appliquée sur une OU qui contient l'**Utilisateur** et non l'**Ordinateur** ? (Rappel : les mappages se font dans "Configuration Utilisateur").
- **Vérifier la GPO :** Tape `gpresult /r` dans le cmd du client pour voir si `GPO_MAP_Compta` fait bien partie des GPO appliquées.



utilisateur



parcours le dossier partager



lecteur mapper