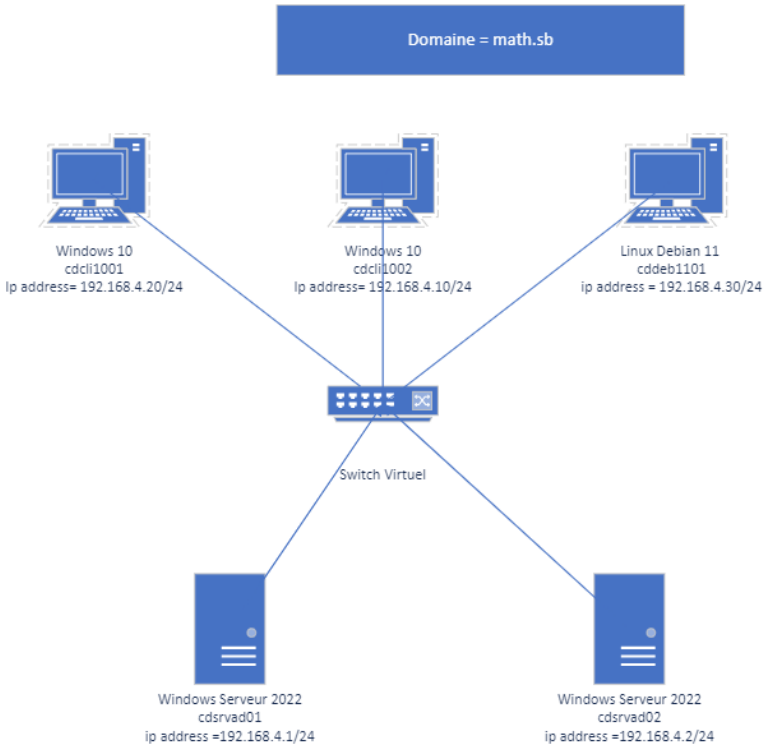
TD Active Directory phase 1

Table des matières



Installation et configuration d'Active Directory sur un serveur Windows 2022 :[1]

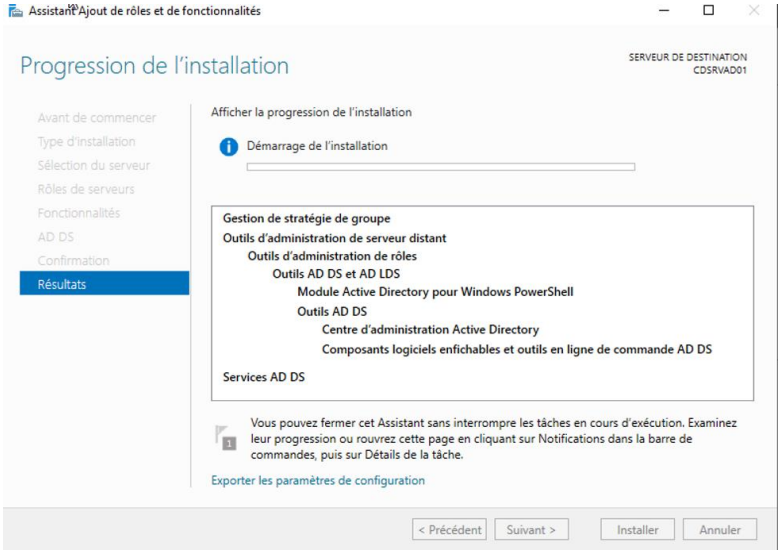
Étape 1 : Installation des rôles et fonctionnalités

- Ouvrir le "Gestionnaire de serveur" sur le serveur Windows 2022.
- Sélectionner "Gérer" dans le coin supérieur droit, puis choisir "Ajouter des rôles et fonctionnalités".

- Suivre l'assistant d'installation en sélectionnant "Installation basée sur un rôle ou une fonctionnalité".

- Cocher la case "Services AD DS".

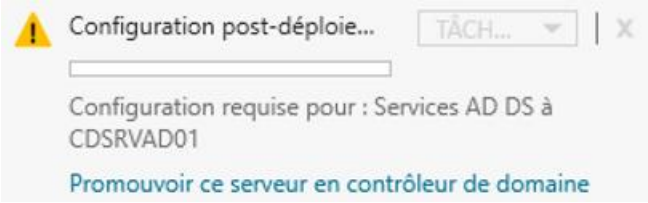
- Cliquer sur "Suivant" jusqu'à la fin de l'assistant, puis cliquer sur "Installer".



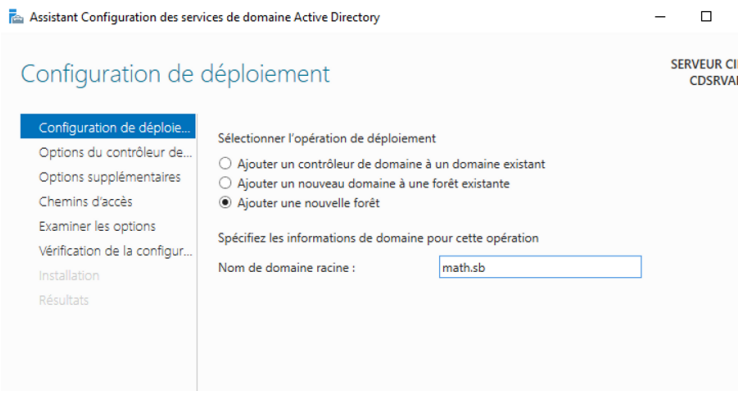
Justification : Cette étape installe les services Active Directory et DNS, nécessaires pour configurer et gérer un domaine Windows. C'est le point de départ pour la mise en place d'un environnement Active Directory.

Étape 2 : Configuration d'Active Directory

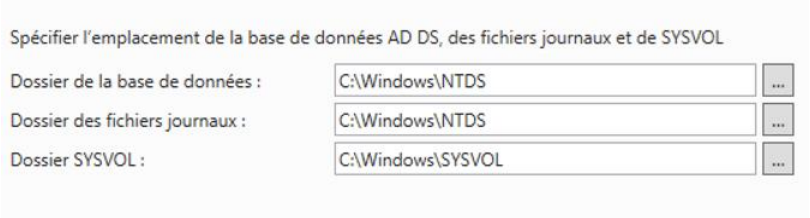
- Après l'installation des rôles et fonctionnalités, cliquer sur "Promouvoir ce serveur en contrôleur de domaine".

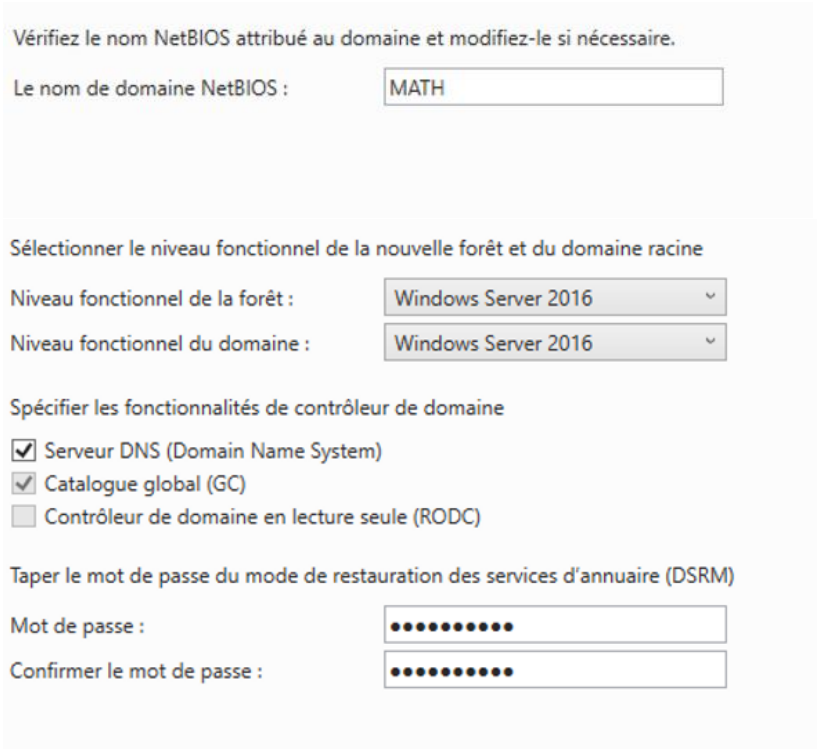


- Sélectionner "Ajouter une nouvelle forêt".
- Entrer le nom de domaine complet (FQDN) pour le domaine (ex : "math.sb").



- Choisir un mot de passe pour le mode restauration de service d'annuaire (DSRM).
- Laisser les fonctionnalités par défaut, le serveur DNS est indispensable.



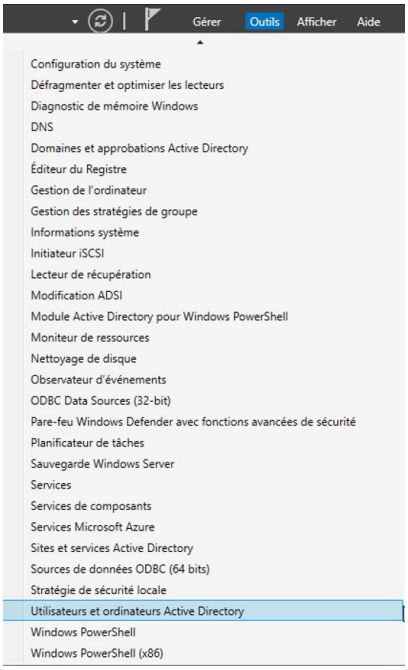


- Cliquer sur "Suivant" pour passer en revue les options sélectionnées, puis cliquer sur "Installer".

Justification : Cette étape configure Active Directory sur le serveur, en créant un nouvel annuaire pour stocker les informations sur les objets du domaine.

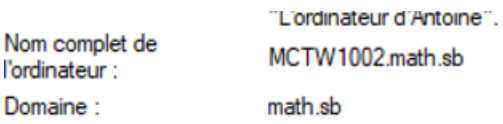
Étape 3 : Vérification de l'installation d'Active Directory

- Attendre que l'installation soit terminée et que le serveur redémarre.
- Ouvrir le "Gestionnaire de serveur".
- Vérifier dans la section "Outils" que les outils d'administration Active Directory sont disponibles (Utilisateurs et ordinateurs Active Directory, Sites et services Active Directory, etc.).



- Sur la machine Windows, accédez à "Paramètres" > "Système" > "Informations système" > "Modifier les paramètres" (à côté de "Nom de l'ordinateur, du domaine et du groupe de travail").
- Cliquez sur "Modifier" et sélectionnez "Adhérer à un domaine ou à un réseau professionnel".
- Entrez le nom complet du domaine Active Directory auquel vous souhaitez adhérer (par exemple, "math.sb").
- Vous serez invité à entrer les informations d'identification d'un compte. (par exemple, un compte d'administrateur de domaine).
- Une fois les informations d'identification vérifiées, cliquez sur "OK". Si tout se passe bien, vous recevrez un message confirmant que la machine a rejoint le domaine avec succès.
- Redémarrez la machine pour appliquer les changements.

Ne pas oublier dans les paramètres de la carte réseau de préciser l'adresse du serveur DNS qui est donc aussi l'adresse IP de L'AD.

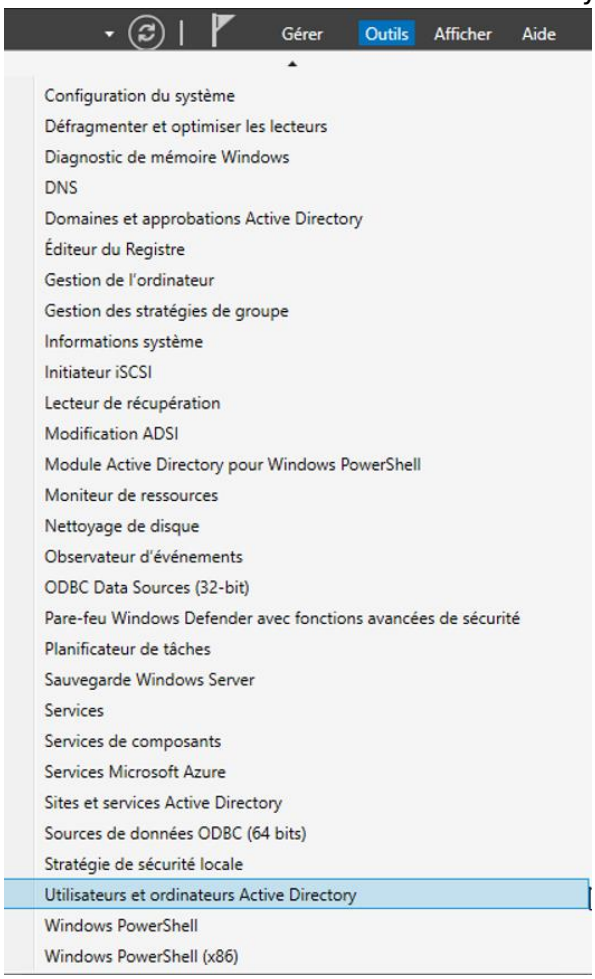


Justification : Cette vérification assure que l'installation d'Active Directory s'est déroulée correctement et que les outils d'administration nécessaires sont disponibles pour la gestion du domaine.

Création D’unité organisationnelle :

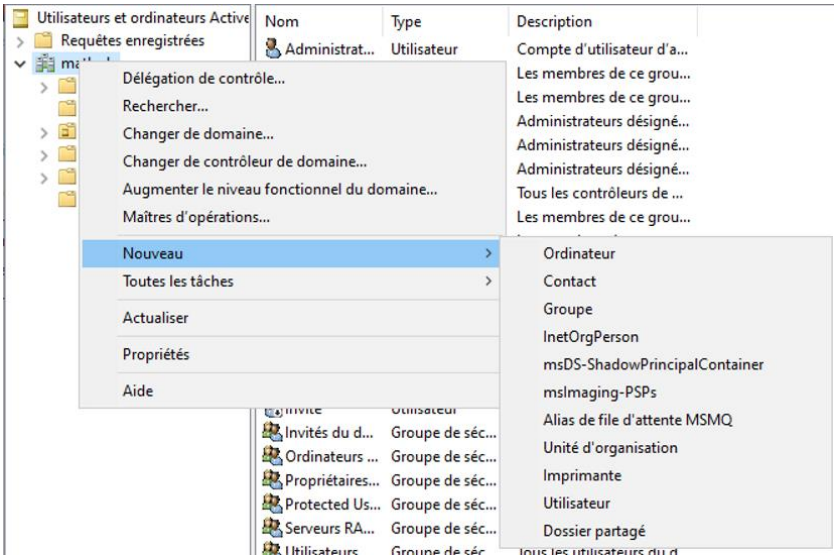
Étape 1 : Accès à la console d'administration Active Directory

- Ouvrez la console "Utilisateurs et ordinateurs Active Directory" en cliquant sur "Outils" dans le menu "Gestionnaire de serveur", puis en sélectionnant "Utilisateurs et ordinateurs Active Directory".

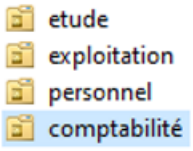


Étape 2 : Création des unités organisationnelles (OU)

- Dans la console "Utilisateurs et ordinateurs Active Directory", faites un clic droit sur le nom de votre domaine dans l'arborescence à gauche, puis sélectionnez "Nouveau" > "Unité d'organisation".

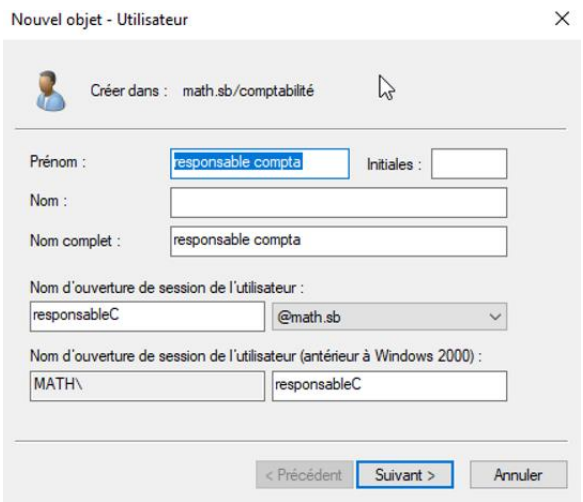


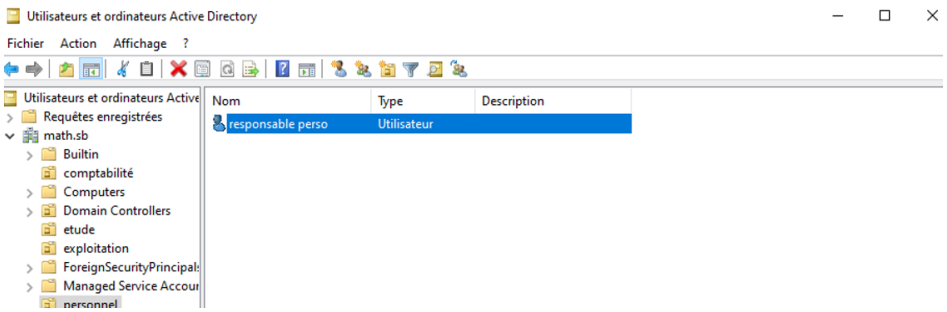
- Entrez le nom de l'unité organisationnelle pour le premier service, par exemple "Étude", puis cliquez sur "OK".
- Répétez cette étape pour créer une unité organisationnelle pour chaque service : "Exploitation", "Personnel" et "Comptabilité".



Étape 3 : Déplacement des utilisateurs et groupes dans les OU appropriées

- Pour chaque service, faites un clic droit sur l'unité organisationnelle correspondante que vous venez de créer, puis sélectionnez "Nouveau" > "Utilisateur" pour créer un utilisateur pour le responsable du service.
- Répétez cette étape pour chaque responsable de service.





Justification des étapes :

- **Accès à la console d'administration Active Directory :** Cela permet d'accéder à l'outil de gestion d'Active Directory où vous pouvez créer et organiser les objets, comme les unités organisationnelles.
- **Création des unités organisationnelles (OU) :** Chaque service de l'entreprise est représenté par une unité organisationnelle, ce qui permet de structurer l'organisation dans l'annuaire Active Directory.

Rôle :

- Le DNS dans Active Directory permet de résoudre les noms des appareils sur le réseau (ordinateurs, serveurs, imprimantes, etc.) en adresses IP et vice versa.
- Il fournit une résolution de noms dynamique.
- Le DNS est utilisé pour localiser les contrôleurs de domaine, les services de domaine, les serveurs d'impression et d'autres ressources dans l'environnement Active Directory.

Fonctionnement :

- Lorsqu'un client ou un serveur dans un domaine Active Directory a besoin de résoudre un nom DNS, il envoie une requête DNS au serveur DNS configuré sur sa machine.
- Si le nom demandé est dans la zone DNS du domaine, le serveur DNS répond avec l'adresse IP correspondante.
- Les enregistrements DNS spécifiques à Active Directory, tels que les enregistrements SRV, sont utilisés pour localiser les services AD, tels que les contrôleurs de domaine.

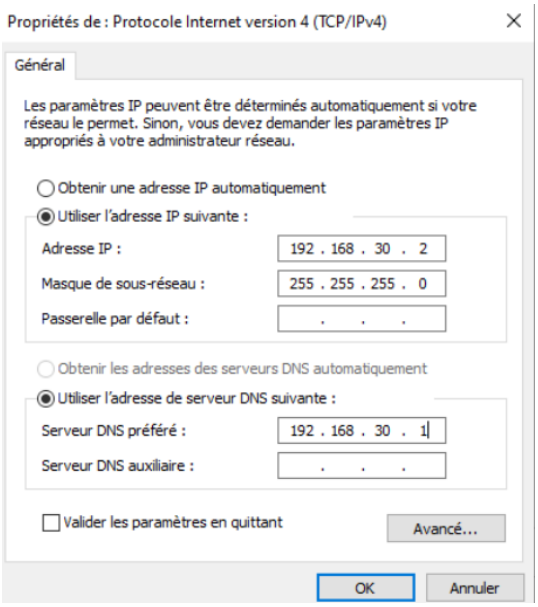
En résumé, le DNS dans Active Directory assure la résolution des noms et la localisation des services réseau, ce qui est essentiel pour le bon fonctionnement de l'infrastructure Active Directory.

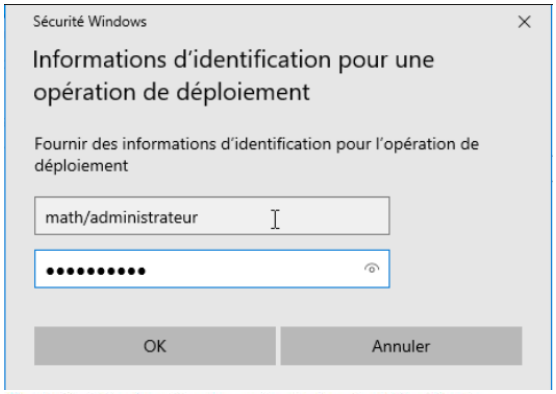
Mise en place serveur secondaire AD :

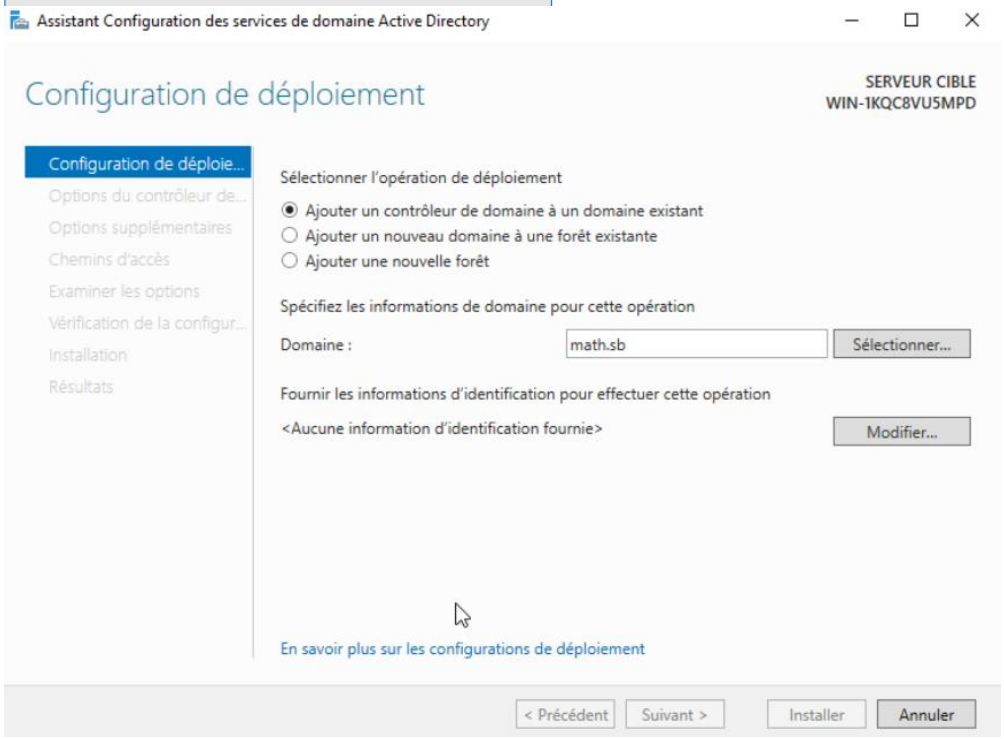
Pour commencer l'installation se fait exactement comme un serveur AD classique nous allons donc directement passer au vif du sujet la promotion du serveur AD et sa configuration :

Contrairement à l'installation d'un serveur AD, nous allons ici choisir « Ajouter un contrôleur de domaine à un domaine existant, nous devons bien évidemment préciser ce domaine math.sb et fournir un utilisateur qui est contenu dans l'annuaire de l'AD principale :

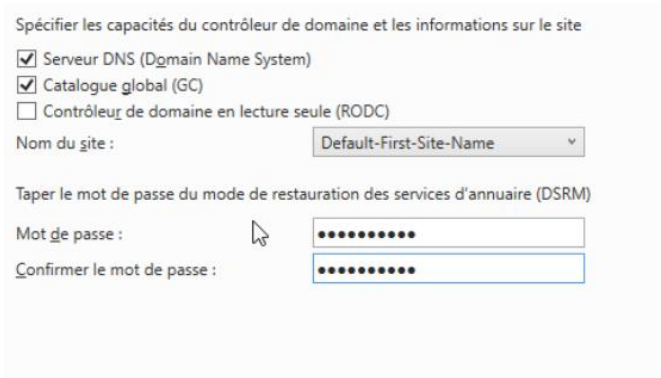
Il ne faut aussi surtout pas oublier de préciser en serveur DNS l'adresse du serveur AD sinon on ne pourra pas adhérer au domaine :





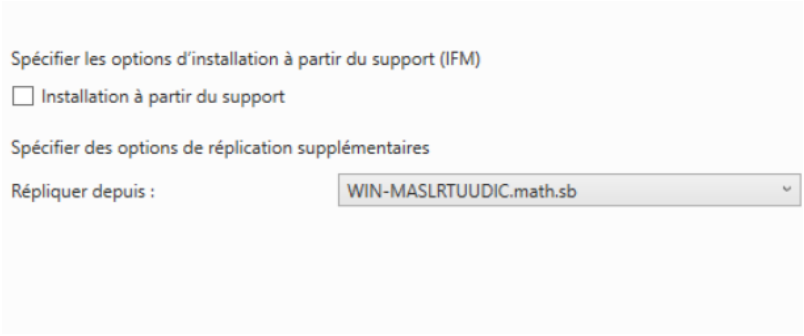


Une fois ceci fait il nous faudra rentrer le MDP du mode de restauration des services d'annuaire (DSRM) que l'on a défini sur l'AD principal. On laisse serveur DNS ce qui permettra si Windows server contenant AD et le serveur DNS principale tombe en panne que le serveur secondaire reprenne le relais.



Ensuite il nous faut préciser depuis quel serveur AD on réplique les données comme nous n'avons qu'un serveur à répliquer nous allons directement sélectionner notre serveur AD

principale :

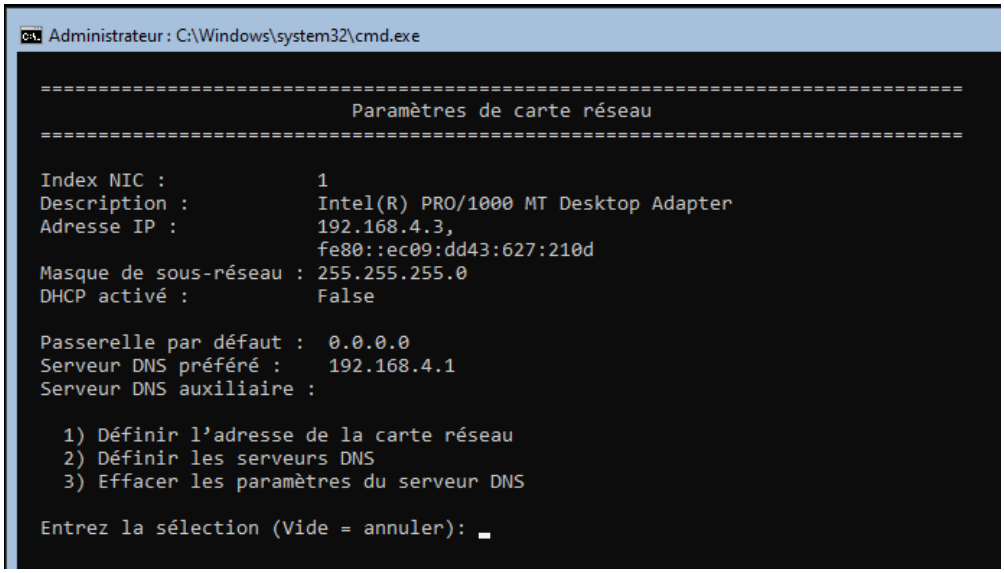


Maintenant si on regarde dans les appareils qui ont adhéré aux domaines on voit bien nos deux contrôleurs de domaines :

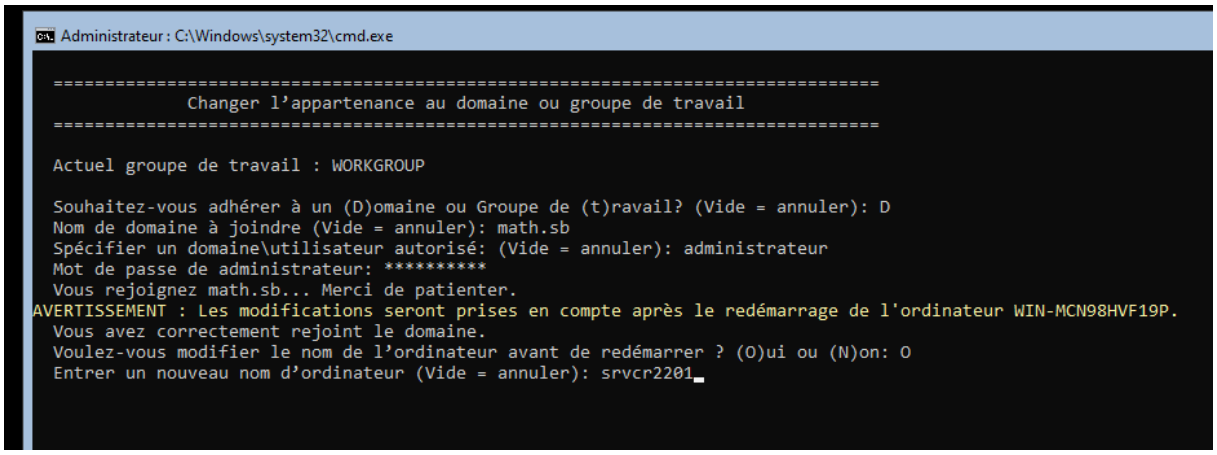
Nom	Type	Type de contrô...	Site	Description
WIN-1KQC8...	Ordinateur	GC	Default-First-Si...	
WIN-MASLR...	Ordinateur	GC	Default-First-Si...	

Mise en place serveur AD CORE :

Pour installer un serveur CORE tout d'abord ont choisi Windows server 2022 et non pas les Windows server (expérience de bureau). Une fois ceci fait nous allons configurer la carte réseau comme ceci, comme on peut le voir on met l'adresse IP le masque de sous-réseau la passerelle par défaut et l'adresse du serveur DNS.



L'adresse du serveur DNS est très importante c'est ce qui nous permet d'adhérer au domaine, nous allons d'ailleurs adhérer au domaine comme ceci :

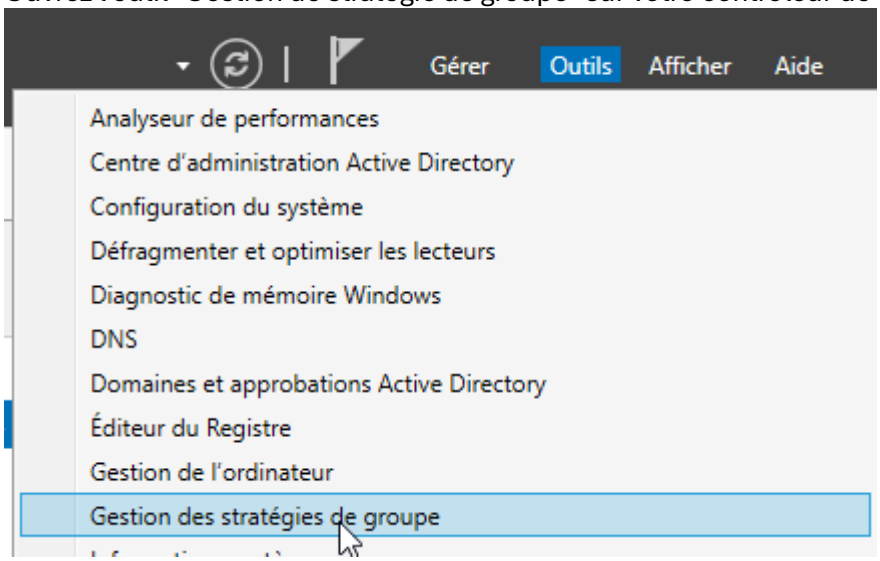


On voit ici qu'on rentre le nom de domaine du serveur AD « math.sb » on rentre ensuite un utilisateur qui est dans l'annuaire AD.

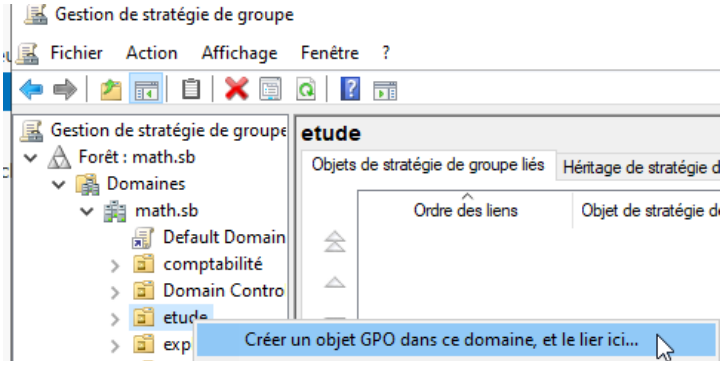
GPO :

Créer une GPO lié à l'unité d'organisation étude :

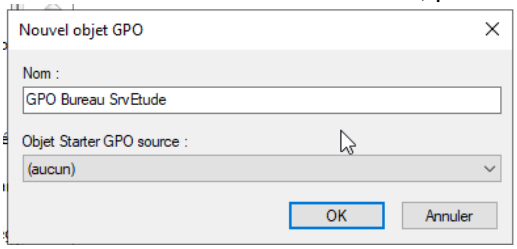
1. Ouvrez l'outil "Gestion de stratégie de groupe" sur votre contrôleur de domaine.



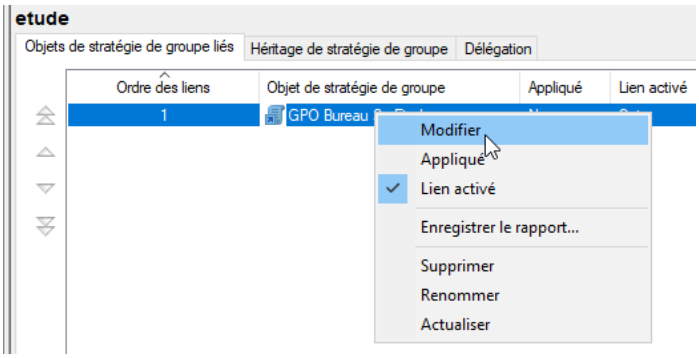
2. Créez une nouvelle GPO en cliquant avec le bouton droit sur l'unité d'organisation (UO) appropriée (dans ce cas, "Etude") et sélectionnez "Créer un objet GPO dans ce domaine, et le lier ici".



3. Nommez la nouvelle GPO, par exemple "GPO Bureau SrvEtude - Employés Seulement".

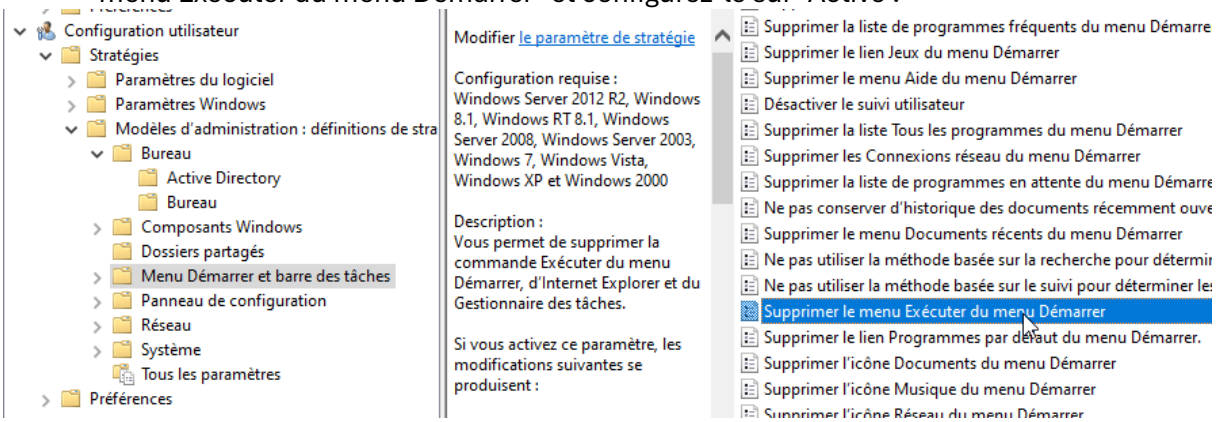


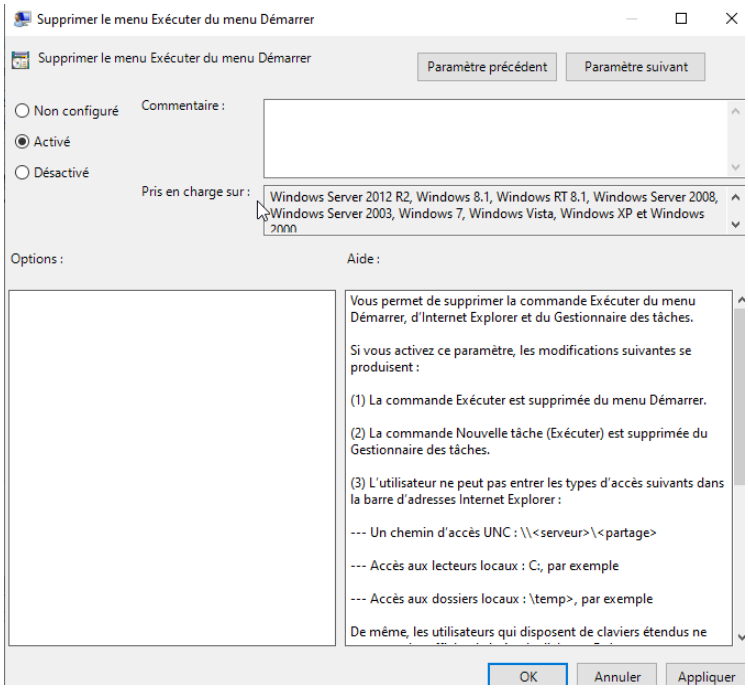
4. Faites un clic droit sur la GPO nouvellement créée et sélectionnez "Modifier".



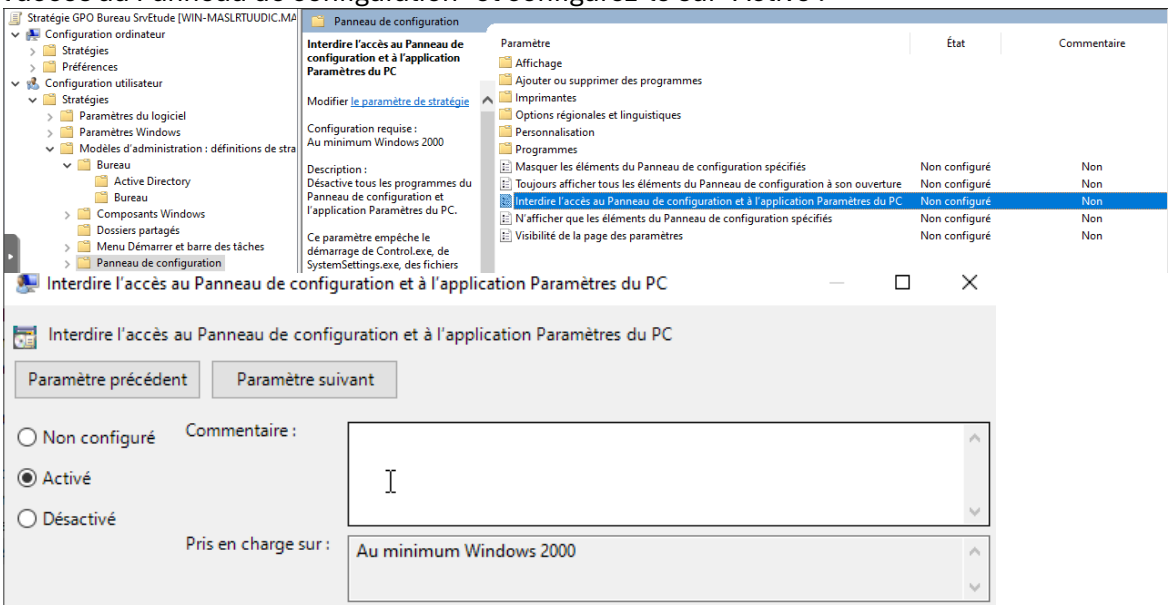
5. Dans l'éditeur de gestion de stratégie de groupe, naviguez jusqu'à "Configuration utilisateur" > "Modèles d'administration" > "Menu Démarrer et barre des tâches".

6. Pour supprimer le menu Exécuter du menu Démarrer, double-cliquez sur "Supprimer le menu Exécuter du menu Démarrer" et configurez-le sur "Activé".

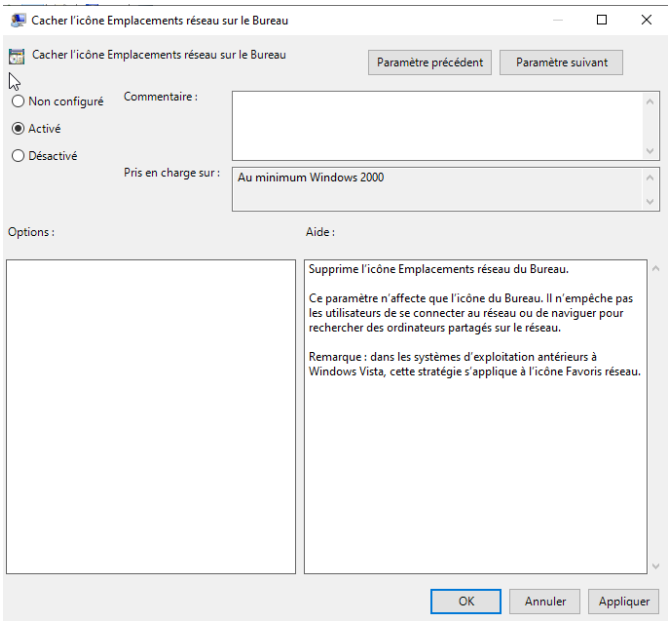




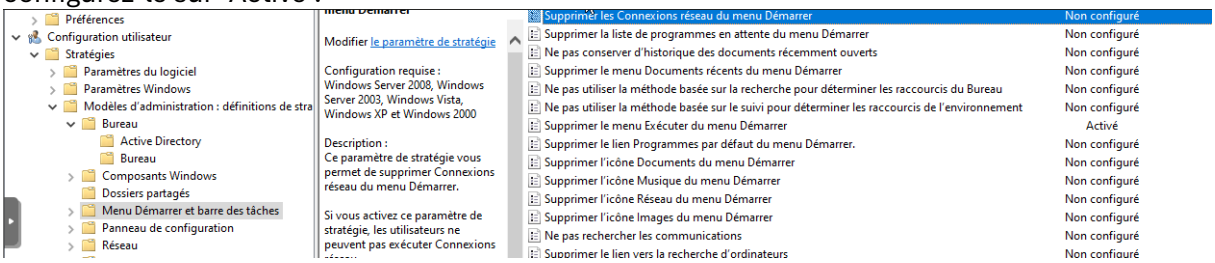
7. Pour empêcher l'accès au Panneau de configuration, double-cliquez sur "Masquer l'accès au Panneau de configuration" et configurez-le sur "Activé".

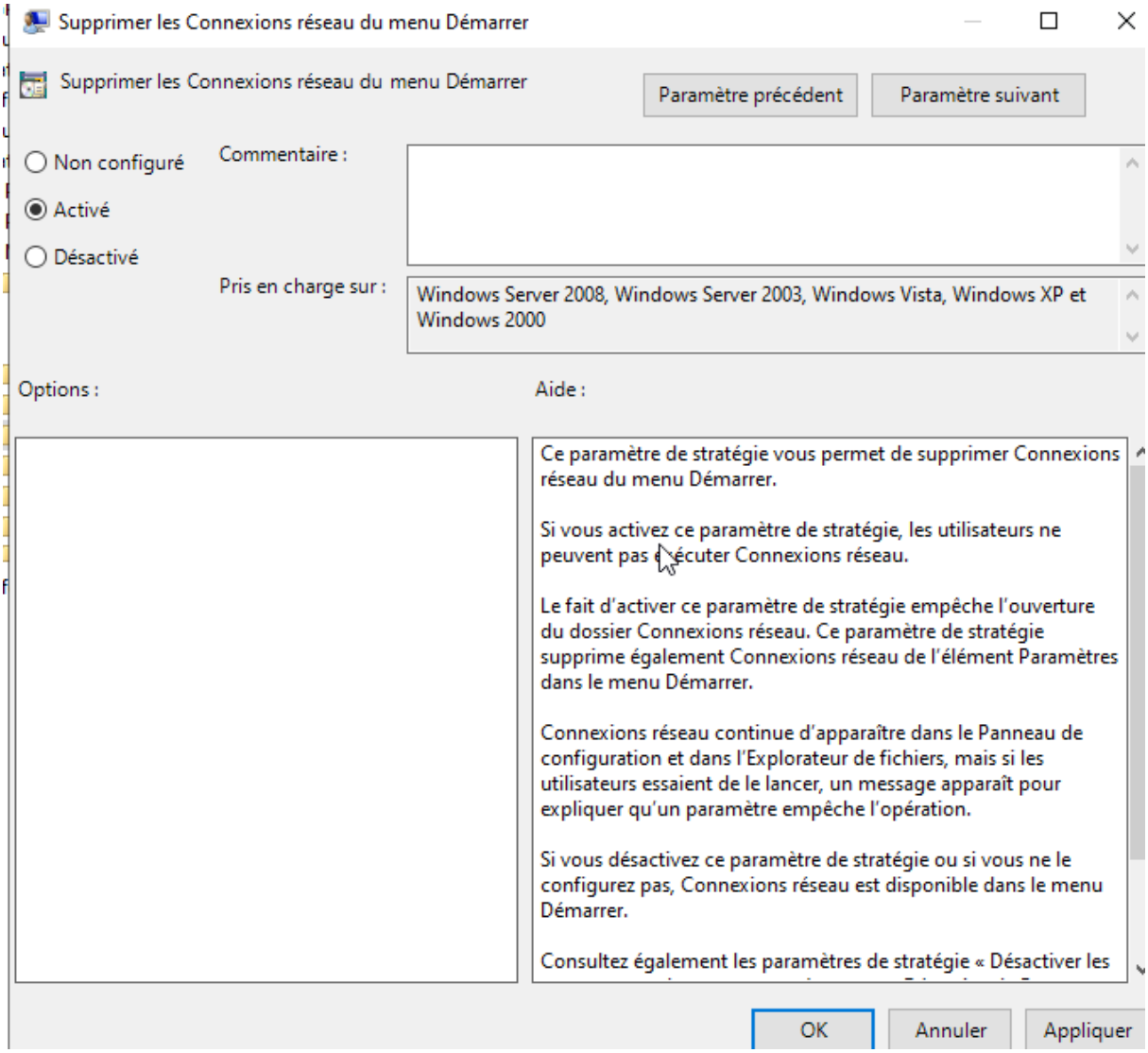


8. Pour cacher l'icône Favoris réseau sur le bureau, naviguez vers "Configuration utilisateur" > "Modèles d'administration" > "Composants Windows" > "Explorateur Windows" et double-cliquez sur "Masquer toutes les icônes du bureau" puis configurez-le sur "Activé" et sélectionnez "Favoris réseau".

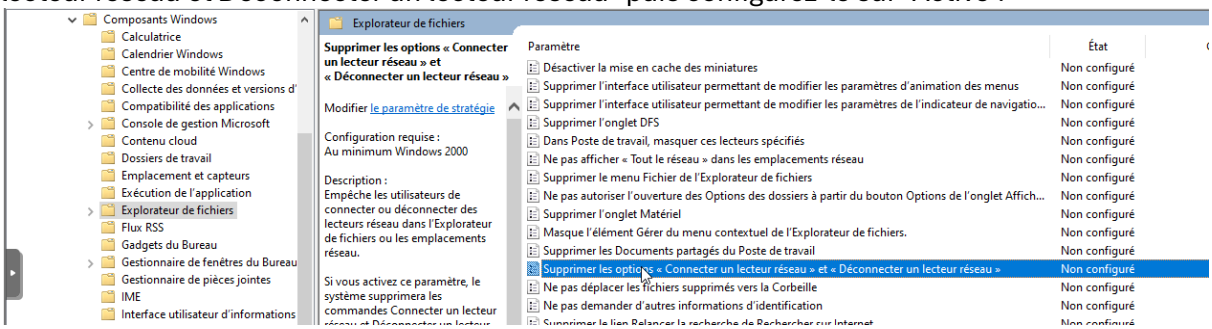


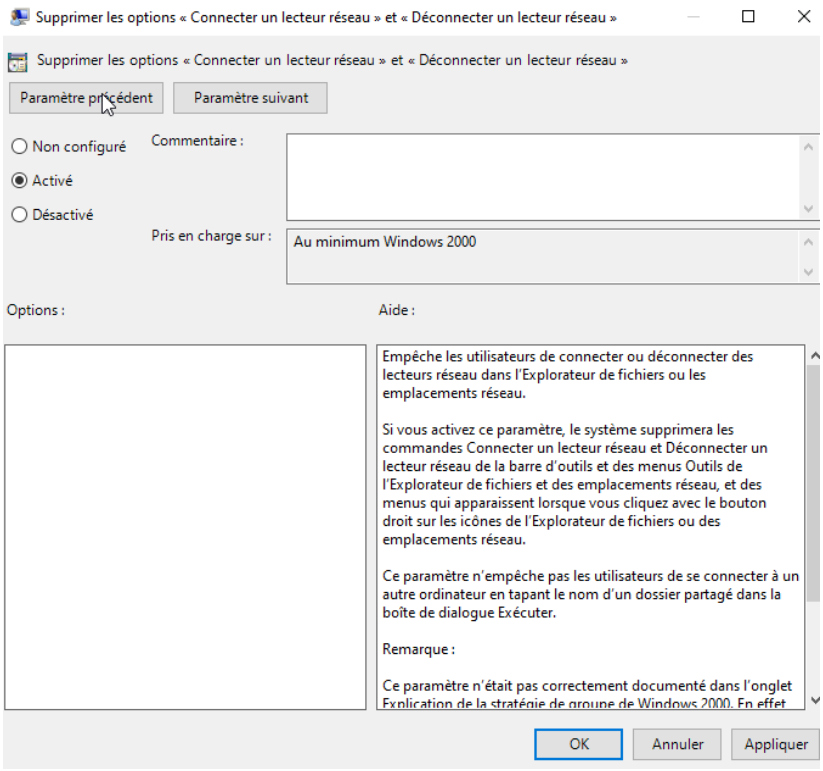
9. Pour supprimer les Connexions réseau du menu Démarrer, naviguez à "Configuration utilisateur" > "Modèles d'administration" > "Menu Démarrer et barre des tâches" et double-cliquez sur "Supprimer les Connexions réseau du menu Démarrer" puis configurez-le sur "Activé".





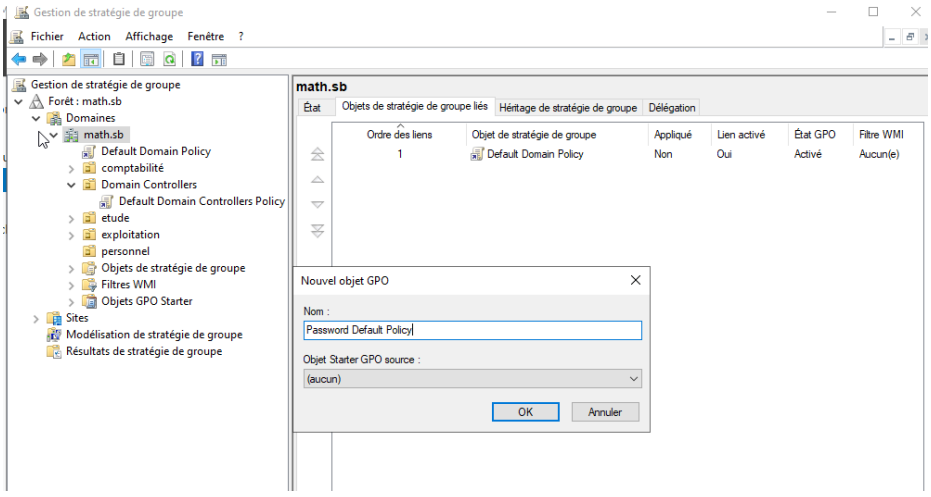
10. Pour supprimer "connecter un lecteur réseau" et "Déconnecter un lecteur réseau", naviguez vers "Configuration utilisateur" > "Modèles d'administration" > "Composants Windows" > "Explorateur Windows" et double-cliquez sur "Supprimer Connecter un lecteur réseau et Déconnecter un lecteur réseau" puis configurez-le sur "Activé".



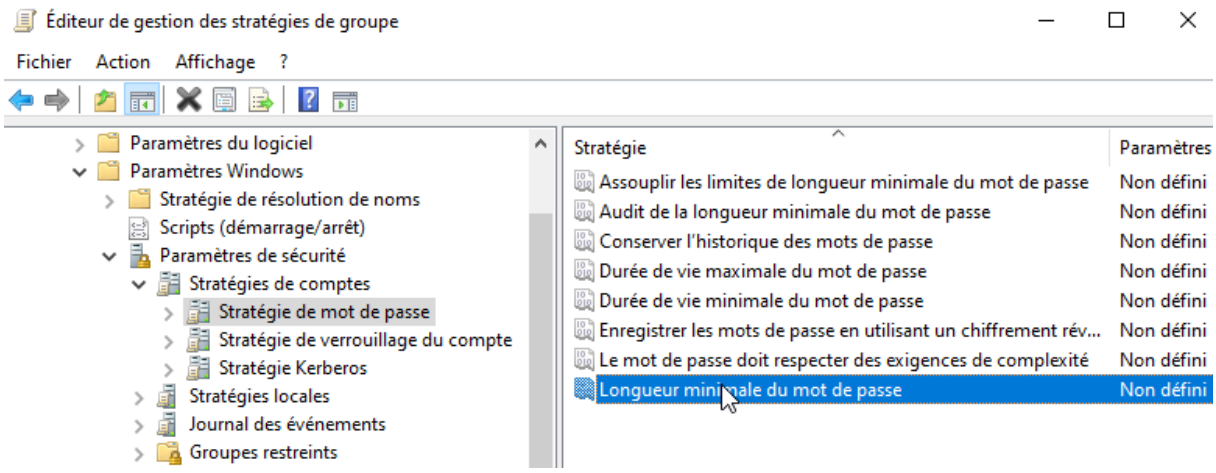


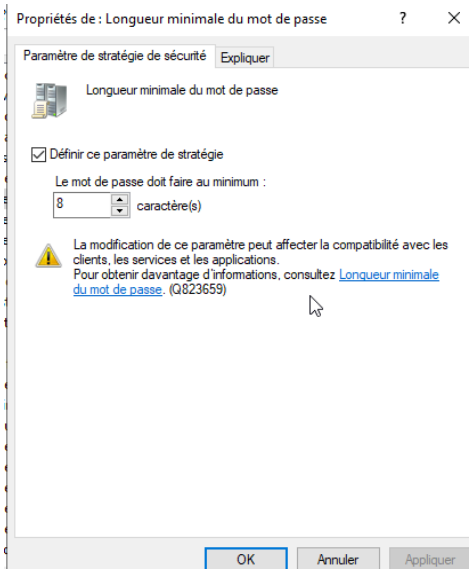
Stratégies de mot de passe :

Pour définir une stratégie de mot de passe global il suffit de créer une gpo pour le domaine math.sb :



Ensuite il faut aller dans paramètre Windows => paramètre de sécurité => Stratégie de mot de passe => longueur minimale du mot de passe :



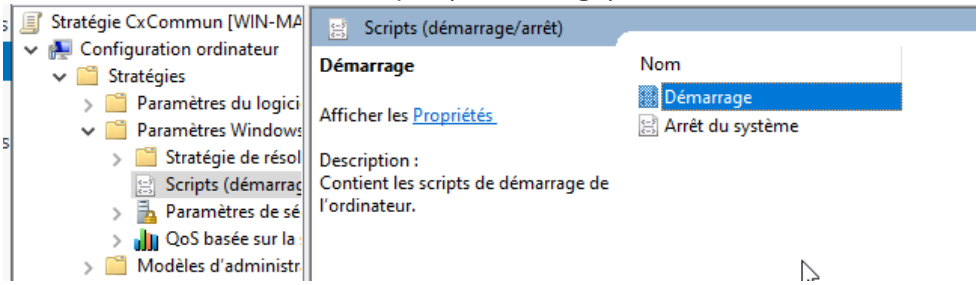


Il suffit de répéter l'opération pour une UO et mettre 6 caractères, la stratégie qui sera prise en compte c'est la stratégie la plus restrictive.
Donc, si la stratégie au niveau du domaine exige des mots de passe d'au moins 8 caractères, et que la stratégie au niveau de l'UO "Etude" exige des mots de passe d'au moins 6 caractères, alors la stratégie la plus restrictive sera appliquée.

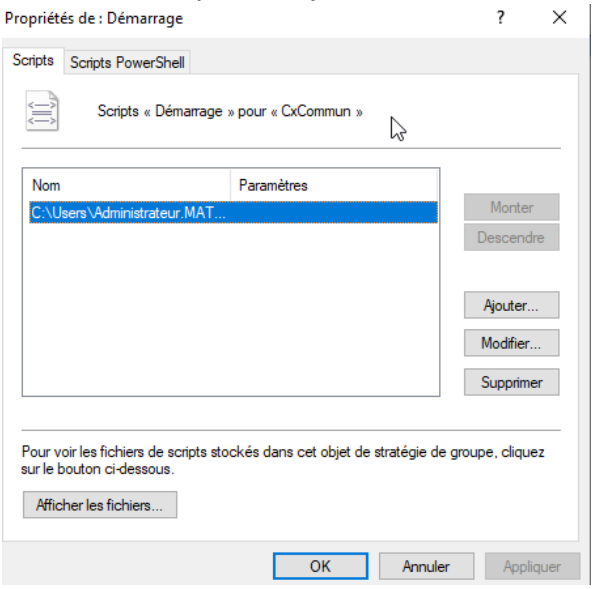
Création GPO script ouverture :

Nous allons créer un script en .bat qui aura uniquement cette ligne : « net use N: \\serveur\Commun »

Une fois le GPO créer dans le domaine math.sb nous allons dans Stratégies => Paramètres Windows => Scripts (Démarrage) :



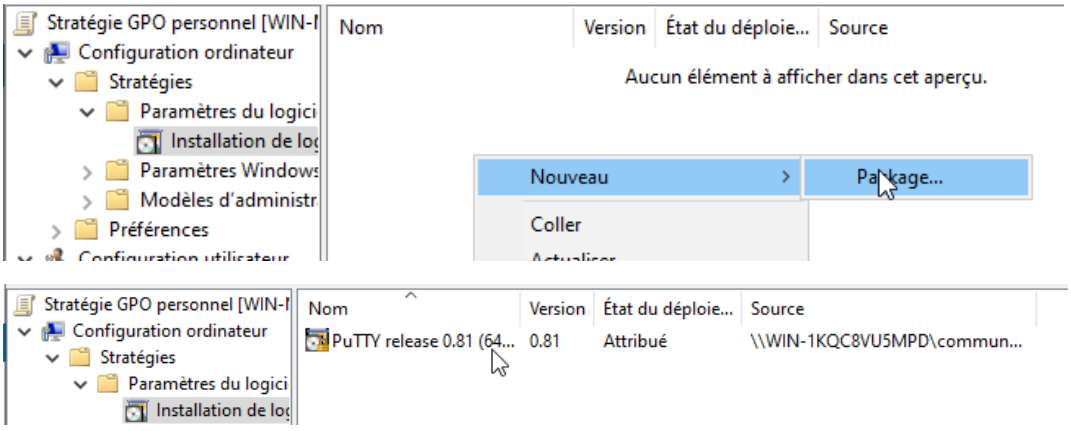
Ensuite on clique sur ajouter et on met l'emplacement du script :



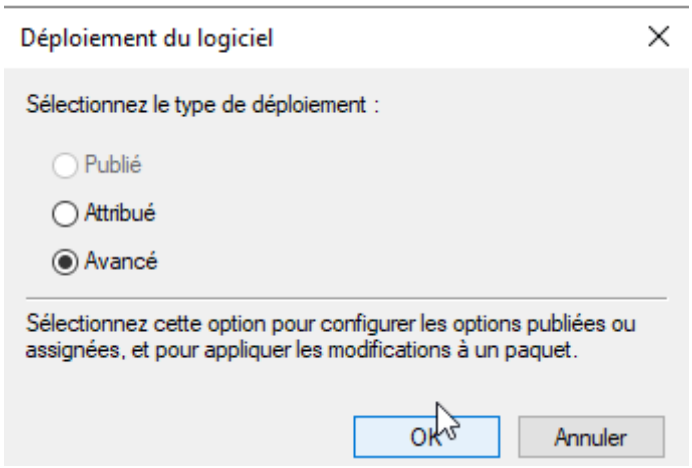
Voilà maintenant toute nos sessions aux démarrages se connecterons au lecteur réseau N :

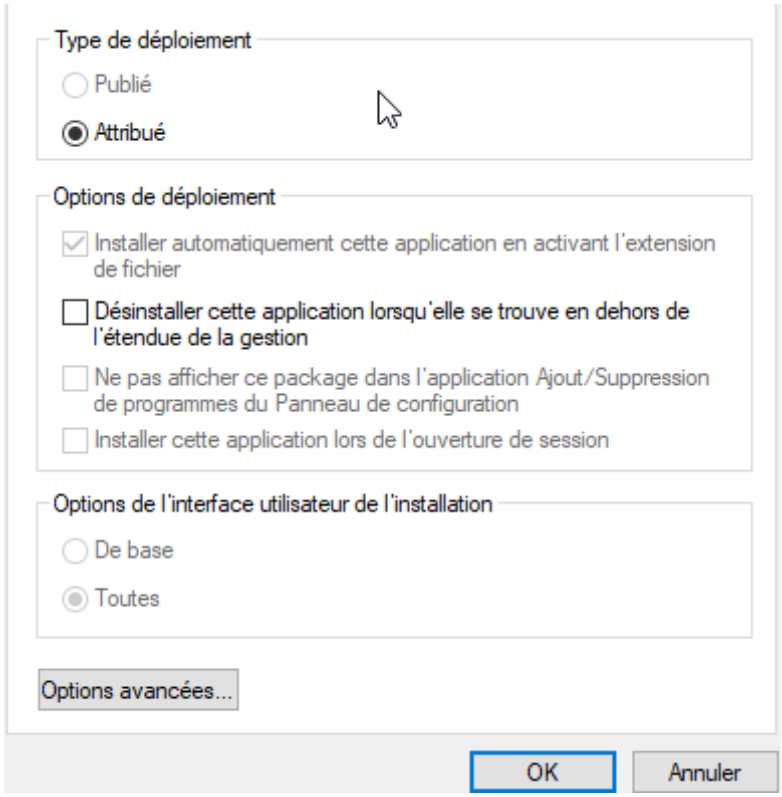
Création GPO Pour déployé application :

Une fois la GPO créer dans L'UO personnel nous allons dans Stratégies => Paramètres du logiciel => Installation logiciel une fois ici on fait clique droit nouveau => Package et on met le chemin UNC pour accéder à l'application que l'on veut installer au lancement d'une session dans l'UO personnel :

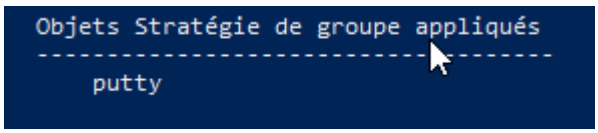


Dans déploiement du logiciel il faut choisir avancé pour pouvoir changer des paramètres si nécessaire, dans notre cas ce n'est pas nécessaire et nous allons mettre Attribué.



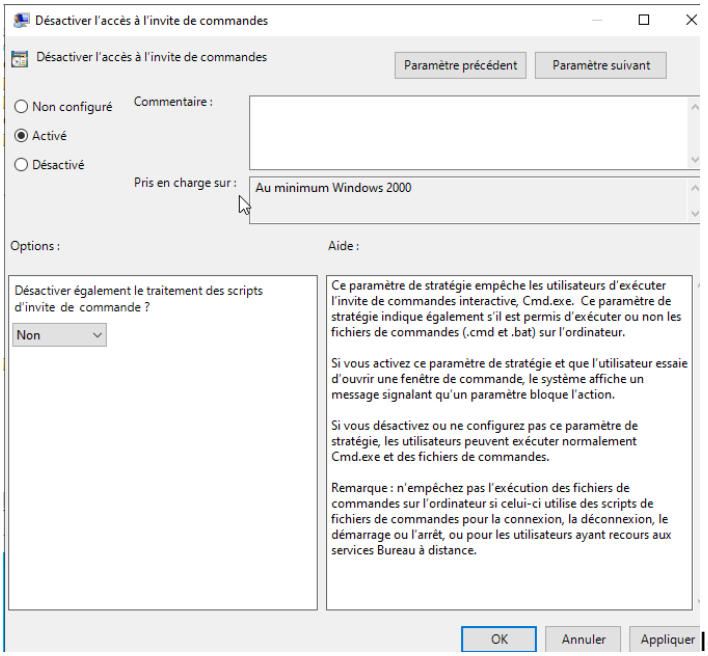


Et voilà tous les utilisateurs dans l'UO "personnel" auront PuTTY d'installer sur leur session

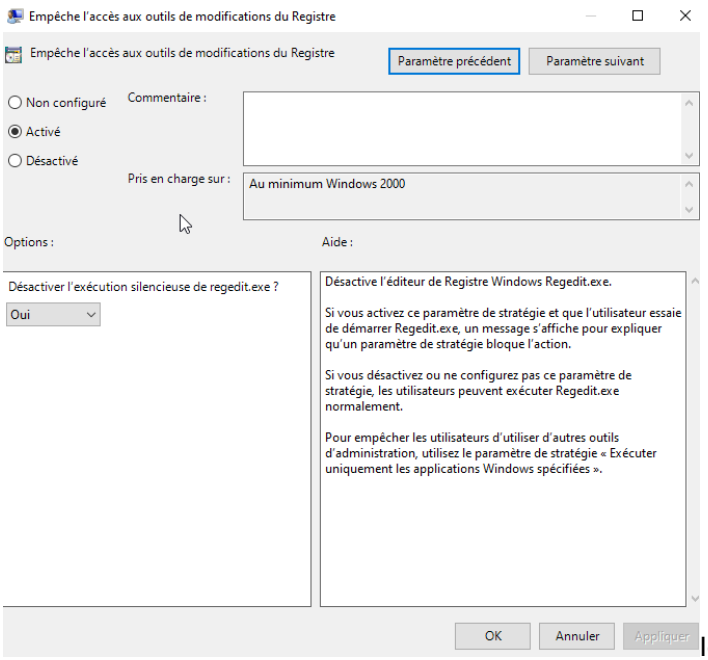


GPO accès strict minimum au bureau Windows :

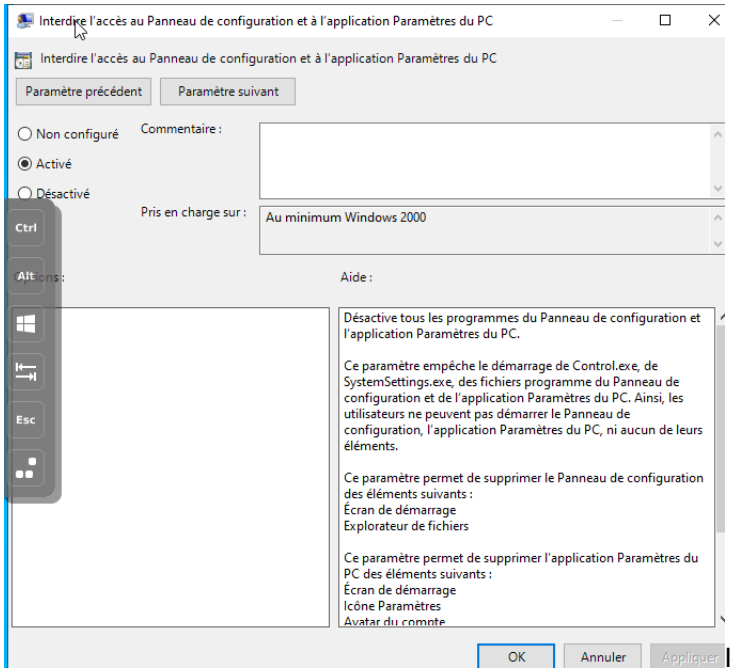
Pour faire ceci on empêche l'exécution, la recherche d'application, l'accès à l'invite de commande, les services, les registres et l'accès au panneau de configuration :



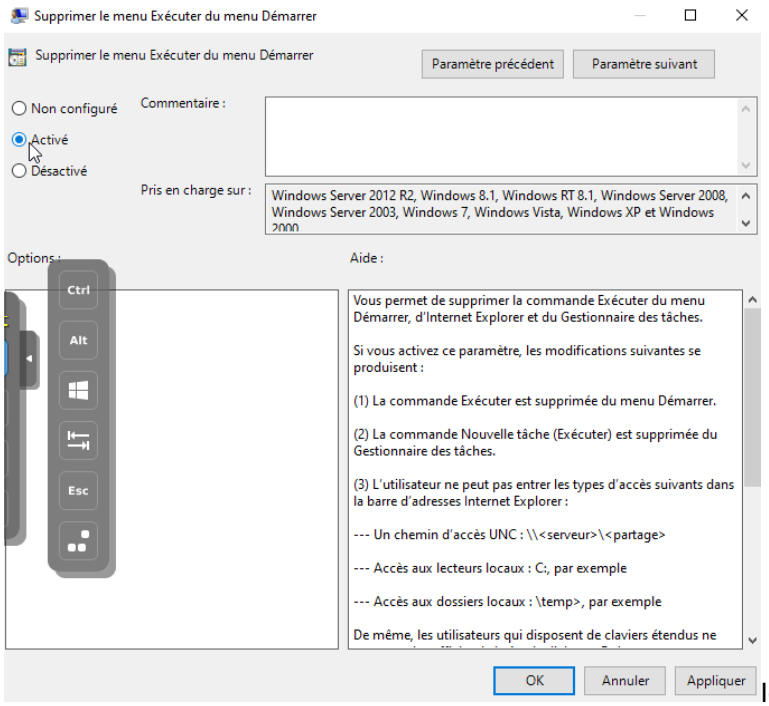
Ici on désactive l'invite de commande



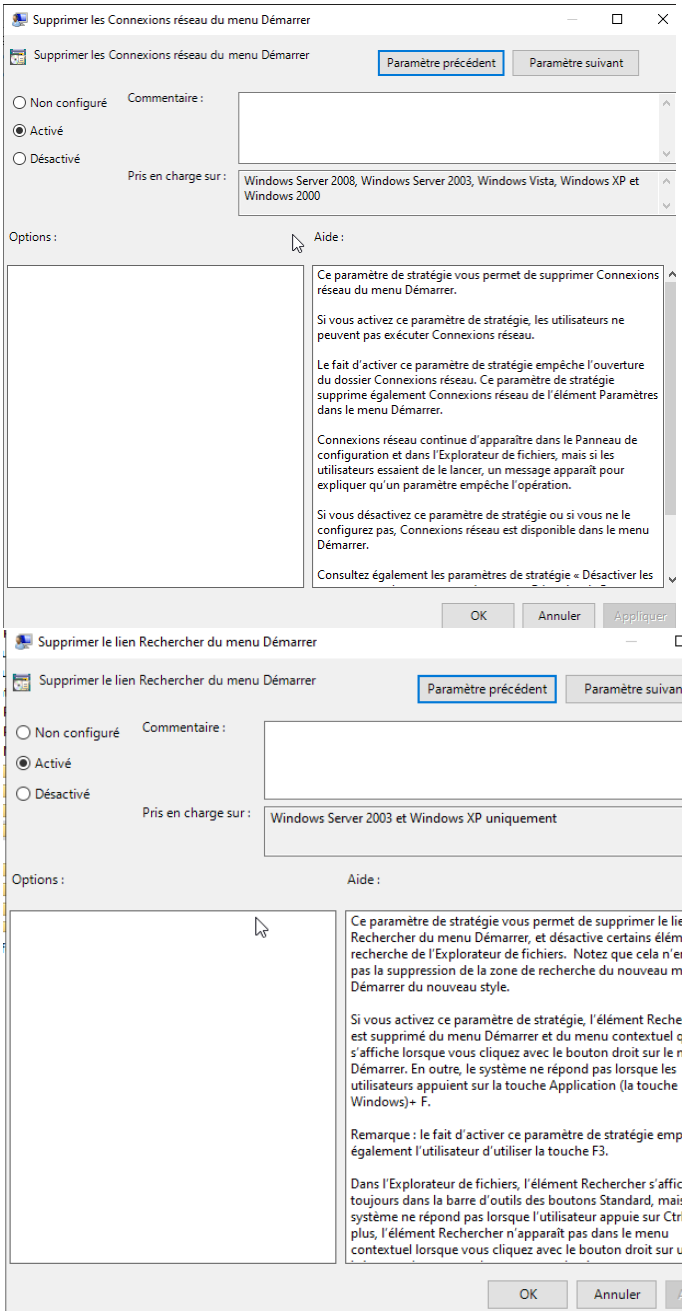
Ici on empêche l'accès au registre



Ici on empêche l'accès aux paramètres et aux panneaux de configuration

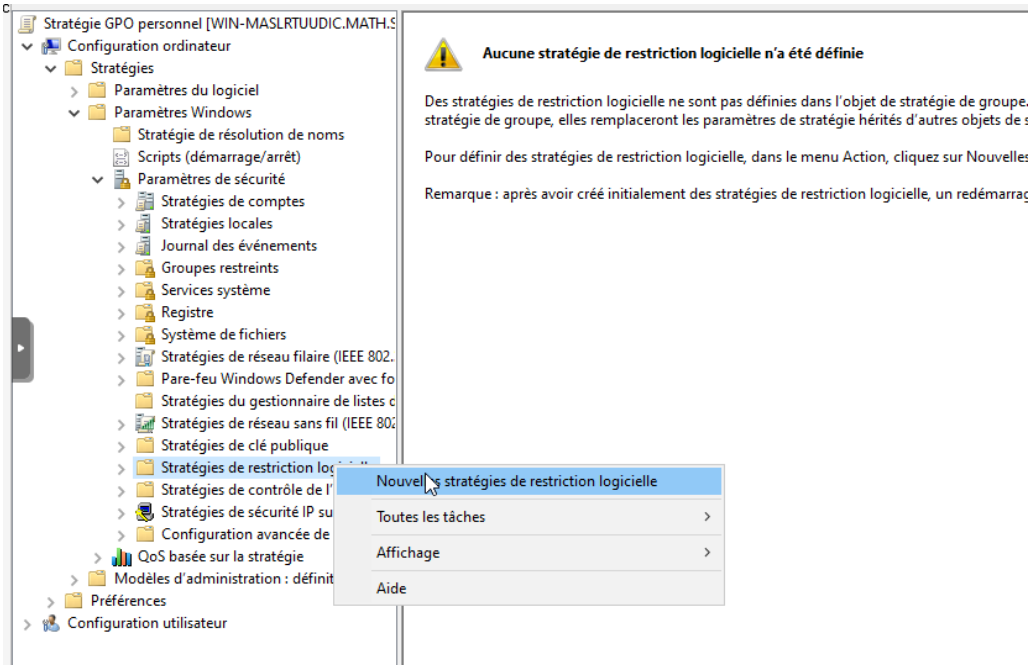


Ici on supprime l'accès au menu exécuter pour mettre des chemins UNC par exemple.

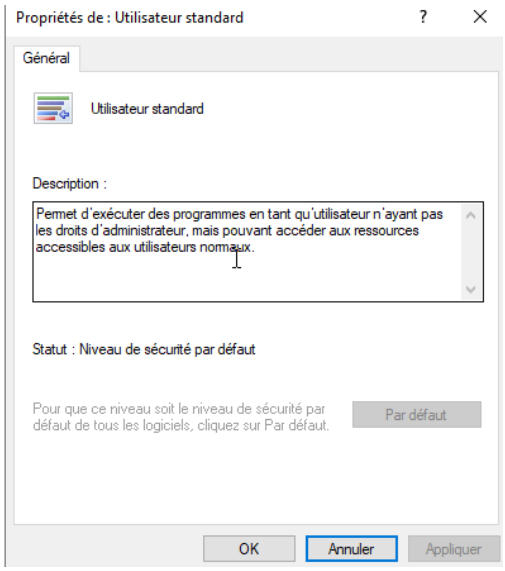


On ne peux plus faire de recherche dans le menu démarrer

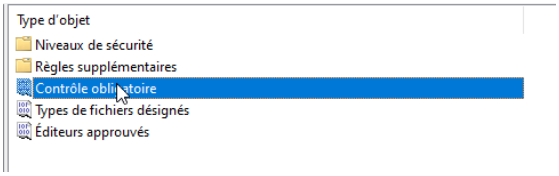
Pour empecher l'execution nous allons allez ici et créer une strategie de restriction logicielle :



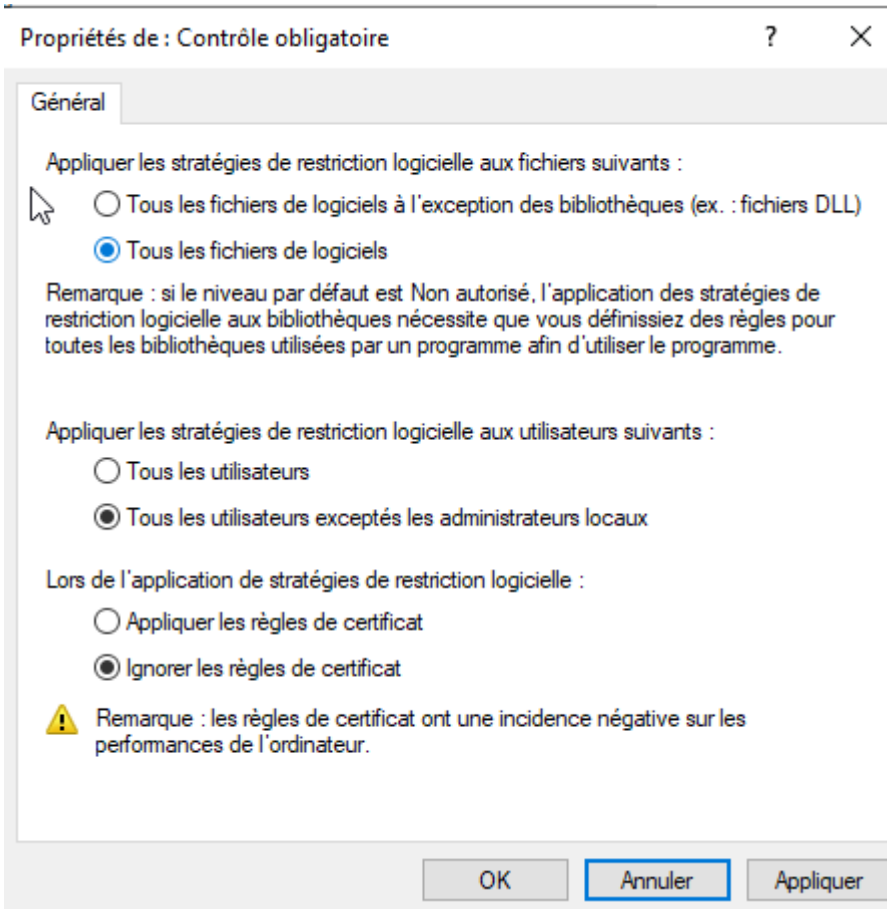
Nous allons donner les droits d'exécution pour n'importe quel utilisateur pour l'instant :



Nous allons ensuite dans contrôle obligatoire :



Ensuite on applique ces paramètres pour empêcher l'exécution de n'importe quel logiciel par un utilisateur et non pas par un administrateur :



Mettre l'option tous les fichiers de logiciels peuvent provoquer des ralentissements, mais notre GPO est prête !