Exercice GPO

JOLIVEL-SAVAGE Raphaël
MÉNOURY Ethan

Lien du Google doc en cas de mauvais chargement du PDF :
https://docs.google.com/document/d/163tQLY-QaPQIYAfMry851Ou_-LFwlyGj9uVlMOO9R2U/edit?usp=sharing

Mission 1 — Analyse des besoins et rédaction d'un mini-cahier des charges

1. Risques actuels

- Sécurité faible et non homogène : mots de passe, pare-feu, antivirus, outils d'administration et configuration Firefox
- Configuration hétérogène entre postes et entre sites (Lyon, Paris, Lille), rendant l'audit difficile car cela provoque des comportements différents entre machines
- Perte de temps pour le support et pour les utilisateurs, car chaque correction ou installation est réalisée manuellement

2. Objectifs techniques

- Mettre en place un socle de sécurité standard (stratégie de mot de passe, verrouillage de session, firewall, restrictions des outils d'administration, contrôle de Firefox)
- Homogénéiser la configuration des postes et des profils utilisateurs via des GPO pour les paramètres système, les lecteurs réseau, les imprimantes et les raccourcis
- Centraliser la gestion des mises à jour et des modèles d'administration (WSUS, ADMX Windows/Firefox) et prévoir la sauvegarde/restauration des GPO

3. Plan GPO haut niveau en se basant sur des norme de nommage

Arborescence simplifiée

OU Postes
- Sous OU : Postes-Lyon, Postes-Paris, Postes-Lille

OU Utilisateurs
- Sous OU : Utilisateurs-Standard, Utilisateurs-Manager, Utilisateurs-IT

Au niveau du domaine

SEC-Domain-Baseline : paramètres de sécurité généraux du domaine (mots de passe, verrouillage de compte, Kerberos)
SEC-Firewall-Base : règles de pare-feu communes à tous les postes du domaine

Au niveau des OU Postes

SEC-Workstations-Hardening : durcissement des postes (désactivation PowerShell/cmd pour les utilisateurs standards, écran de veille verrouillé, USB...)
APPS-FirefoxESR-Config : configuration imposée de Firefox ESR

Au niveau des OU Utilisateurs

UX-Users-Standard : restrictions et ergonomie pour les utilisateurs standard (Menu de démarrage, barre des tâches, Store...)
UX-Managers : profil un peu plus ouvert pour les managers (même base mais avec moins de restrictions)

OU de test

POC-GPO : GPO de test appliquée sur une OU pour valider les paramètres avant de les lier aux OU de productions

Mission 2 — Recherche & sélection de GPO pertinentes

Sécurité du poste

Désactivation de PowerShell pour les utilisateurs standard
Restriction d'accès au panneau de configuration
Désactivation du stockage USB
Mise en place d'un écran de veille verrouillé obligatoire
Mise en place de GPO dédié à Firefox

Blocage de l'invite de commandes cmd pour les utilisateurs normaux
Durcissement du pare-feu Windows

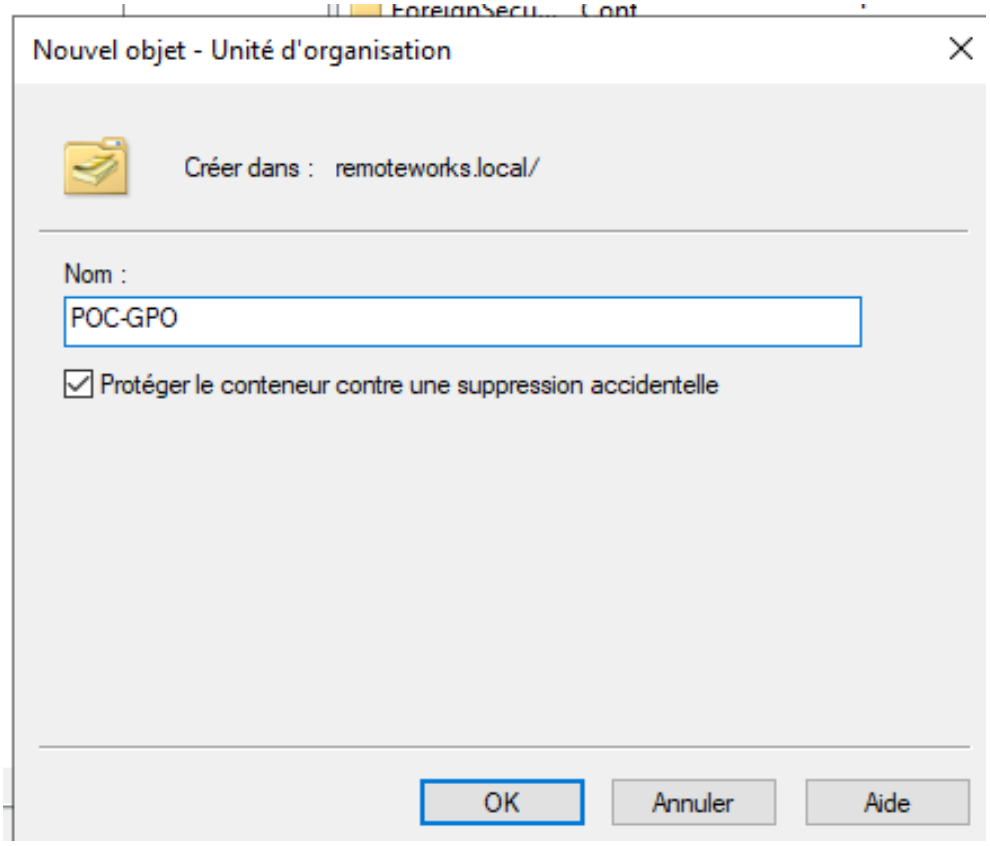
Corporatisme & identité visuelle

Messages légaux au login
Configuration du menu Start / barre des tâches
Désactivation Microsoft Store
Déploiement automatique de logiciels via GPO (MSI)

Mission 3 — Déploiement concret du POC

1. Préparer le POC (OU, poste, utilisateur)

On ouvre *Utilisateurs et ordinateurs Active Directory*.
Ici on crée une nouvelle OU : POC-GPO

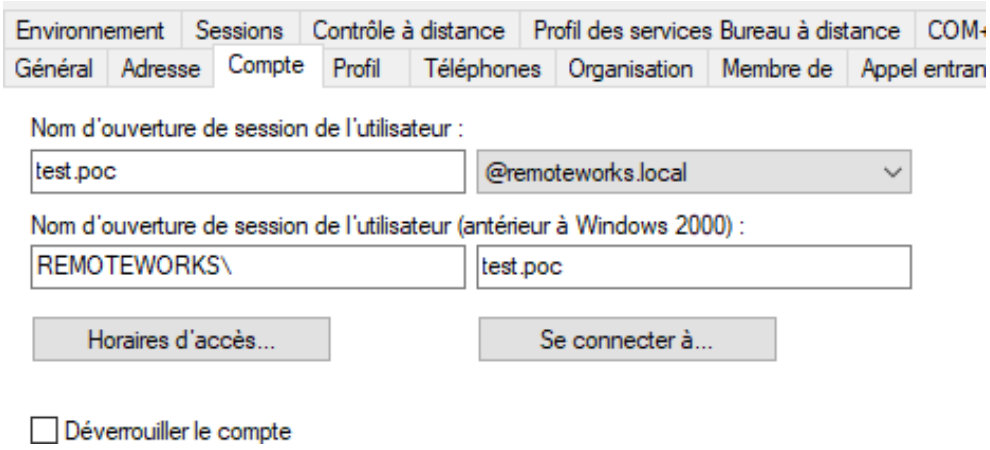


On coche la case *Protéger le conteneur contre une suppression accidentelle*

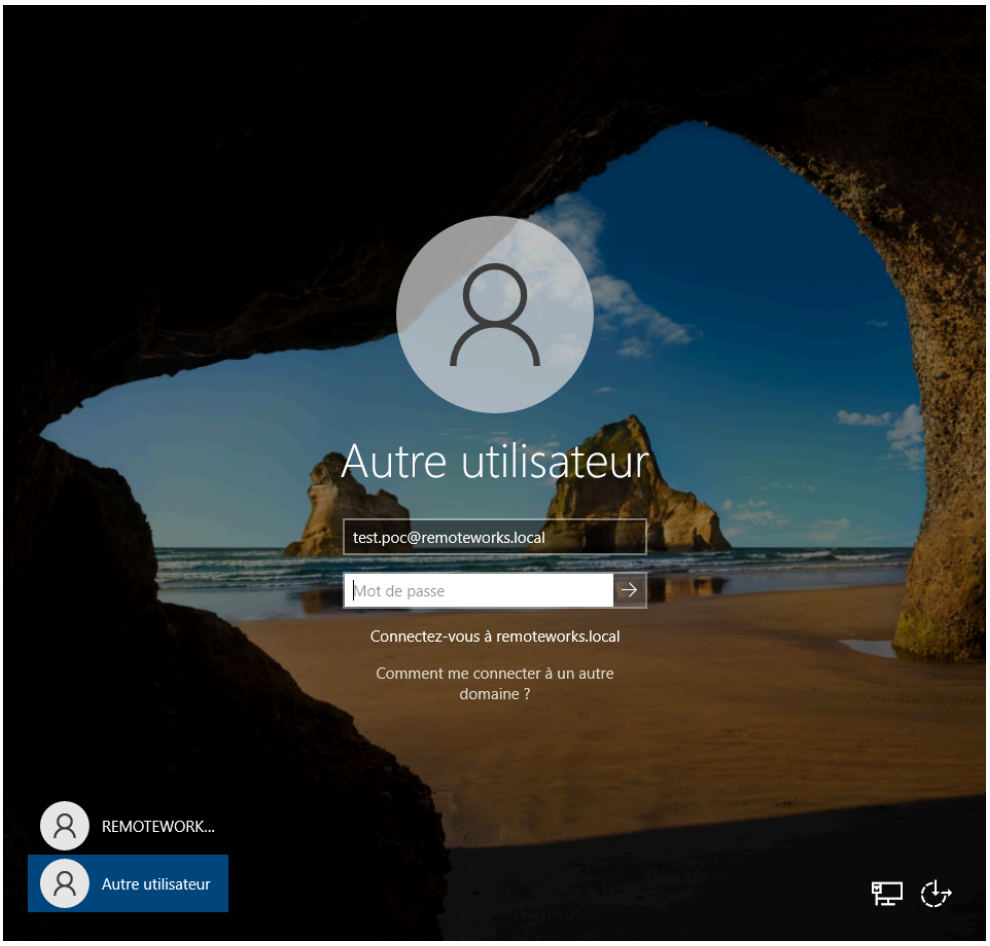
Ensuite dans cette OU on crée :

- un compte ordinateur
- un compte utilisateur de test

Ensuite on vérifie que le compte fonctionne en se connectant avec les identifiants :

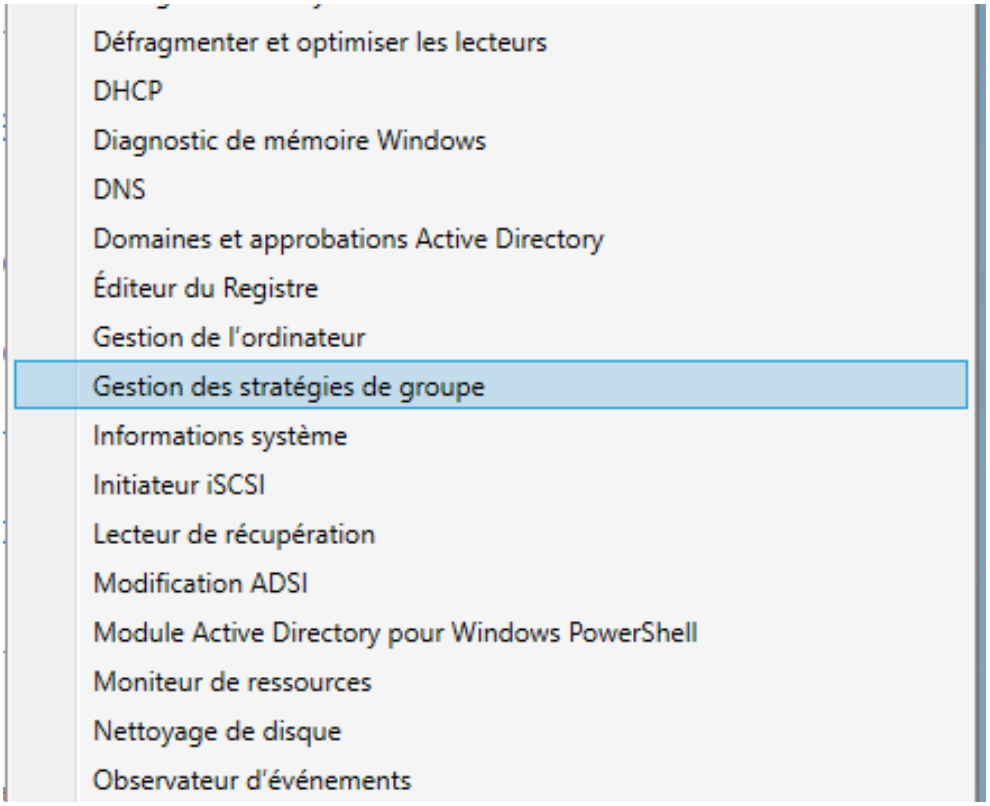


Pour se connecter on se déconnecte et on clique sur *Autre utilisateur*



Après avoir vérifié le bon fonctionnement, on retourne sur le compte administrateur.

On accède aux outils puis dans *Gestion des stratégies de groupe*.



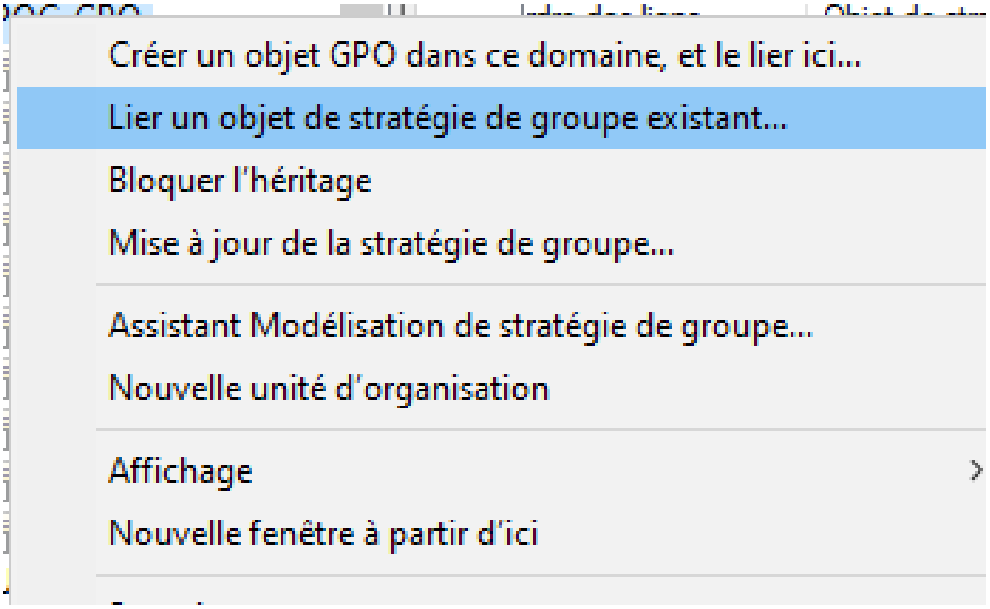
Puis on créer nos GPO :

- SEC-User-NoPowerShell
- SEC-User-NoControlPanel
- SEC-Device-BlockUSB
- SEC-Session-LockedScreensaver
- SEC-User-NoCMD
- SEC-Firewall-Workstations
- APP-FirefoxESR-Hardening
- CORP-Wallpaper-BySite
- CORP-LegalBanner-Logon
- UX-StartMenu-Taskbar-Standard

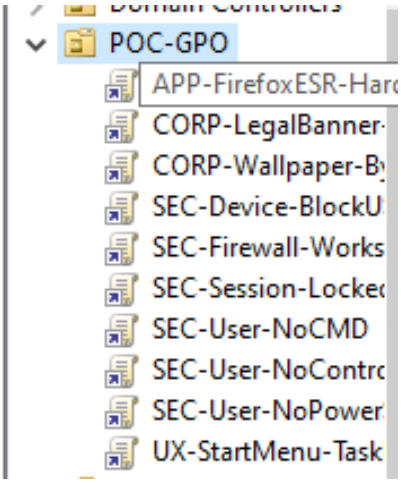
- SEC-Device-BlockBluetooth
- SEC-BitLocker-Workstations
- SEC-SmartScreen-Enable
- UX-Printers-AutoDeploy
- ADM-WSUS-Workstations

Résultat :

Ensuite on lie les GPO créés à l'OU POC-GPO



Résultat :

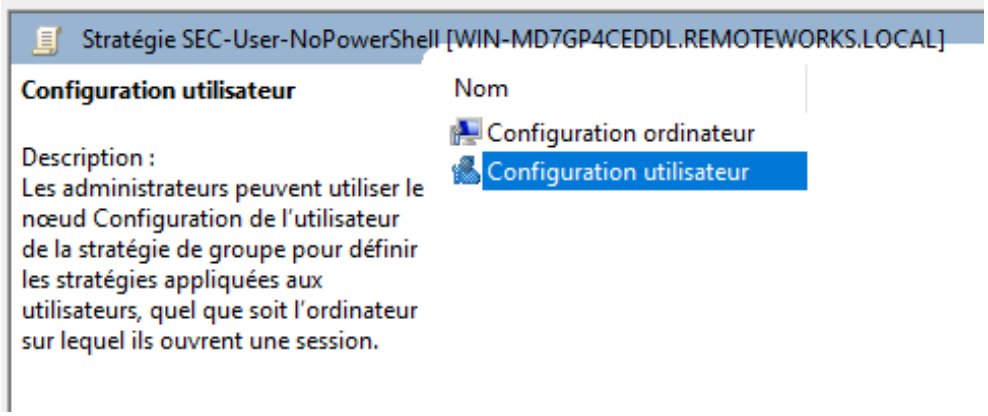


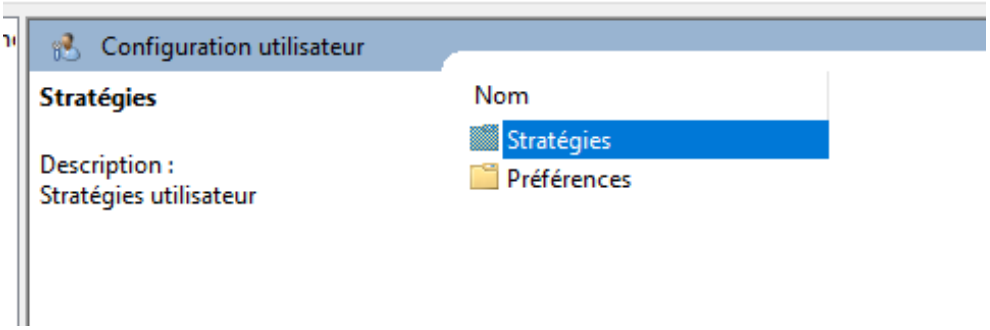
2. Configuration des GPO

Maintenant on ajoute les règles à nos GPO créés pour qu'elles soient fonctionnelles.

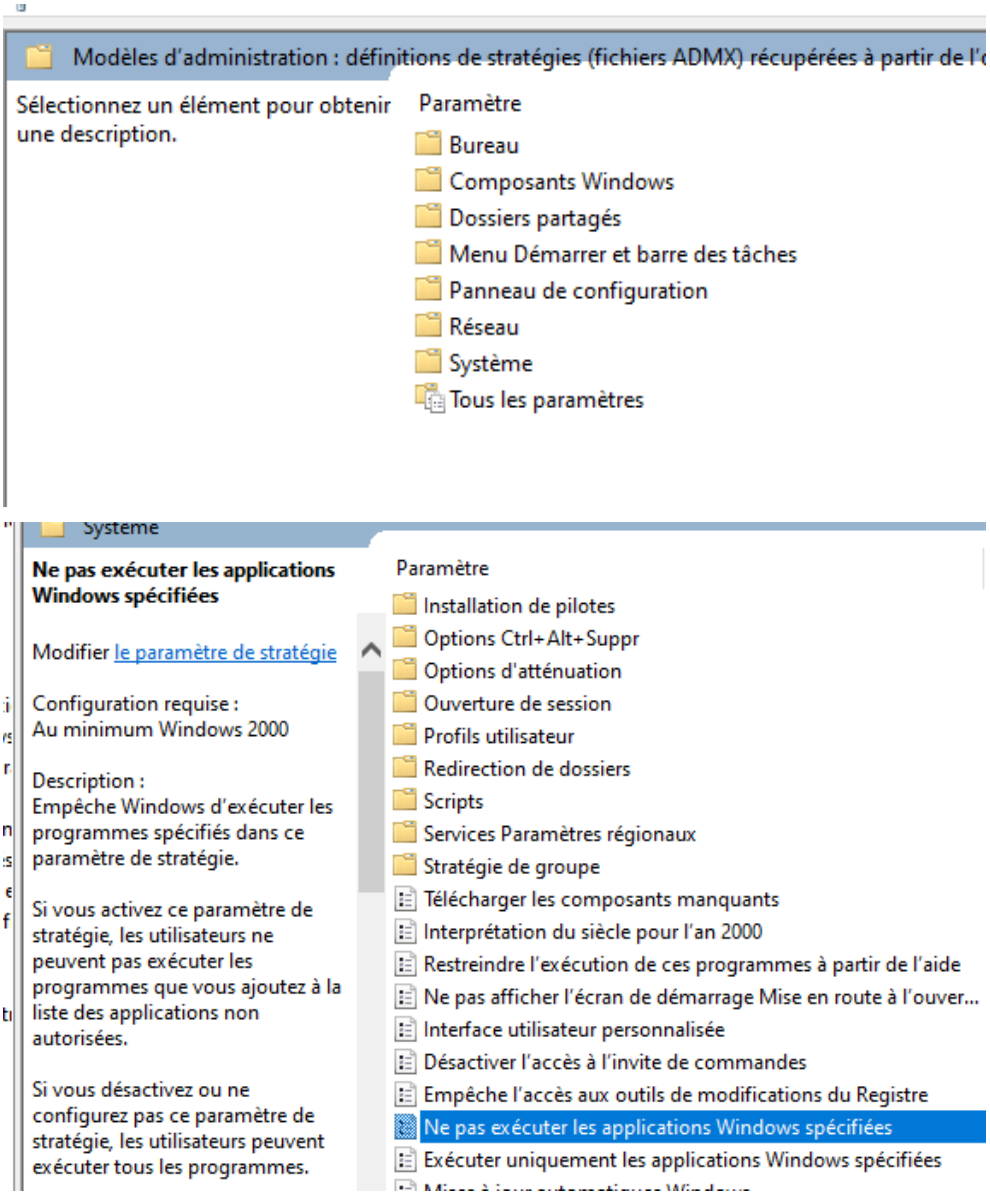
1- SEC-User-NoPowerShell

On modifie la GPO puis on se déplace dans *Configuration utilisateur* > *Stratégies* > *Modèles d'administration*





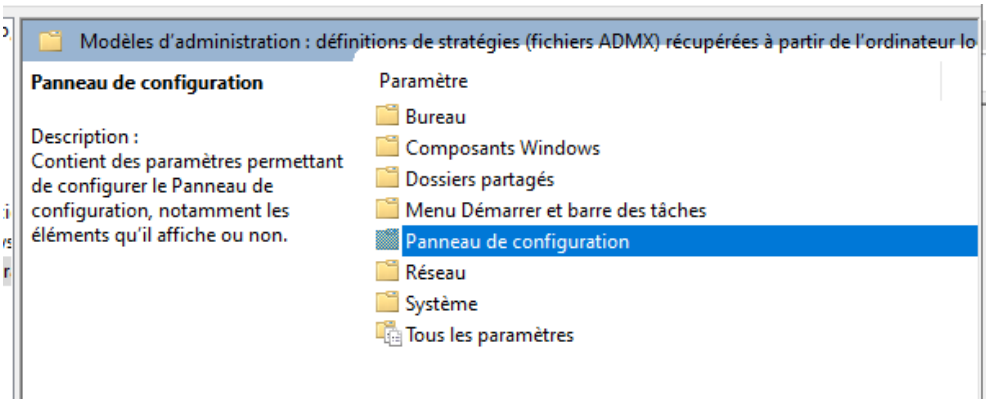
Ensuite on se déplace dans *Système* > *Ne pas exécuter les applications Windows spécifiés*



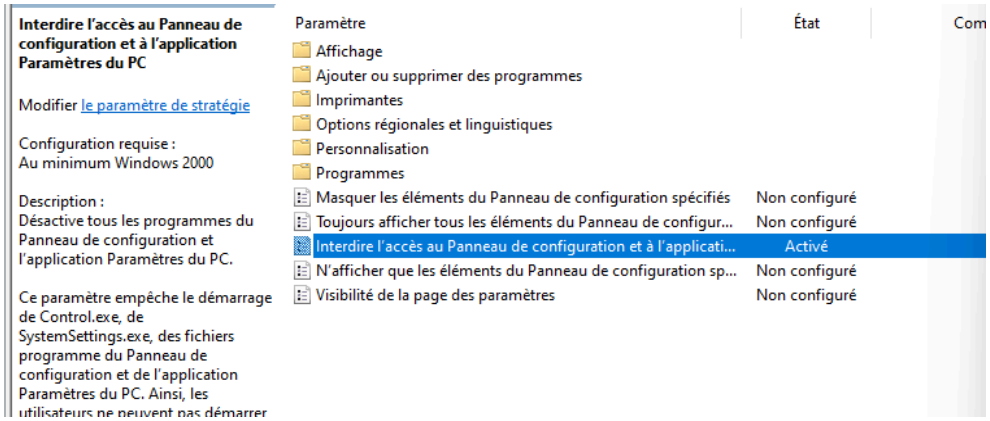
Et on y ajoute ces règles pour empêcher l'utilisation de PowerShell

2- SEC-User-NoControlPanel

On modifie la GPO puis on se déplace dans *Configuration utilisateur* > *Stratégies* > *Modèles d'administration* et puis dans *Panneau de configuration*

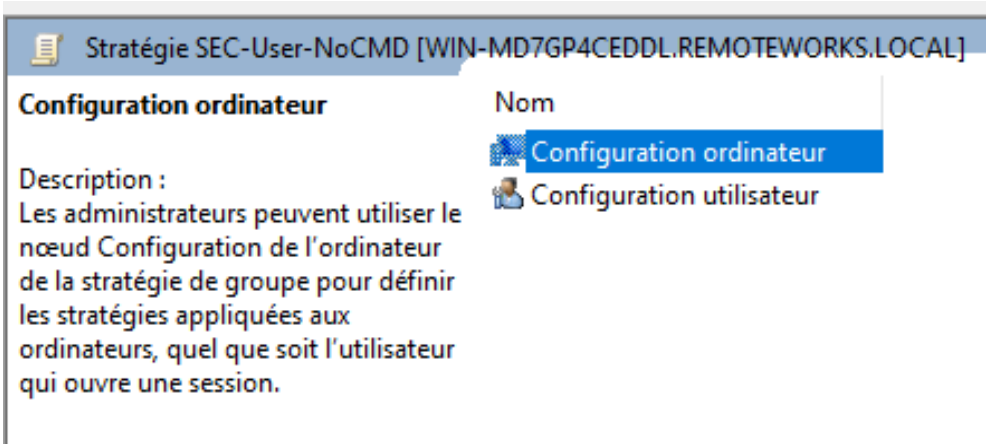


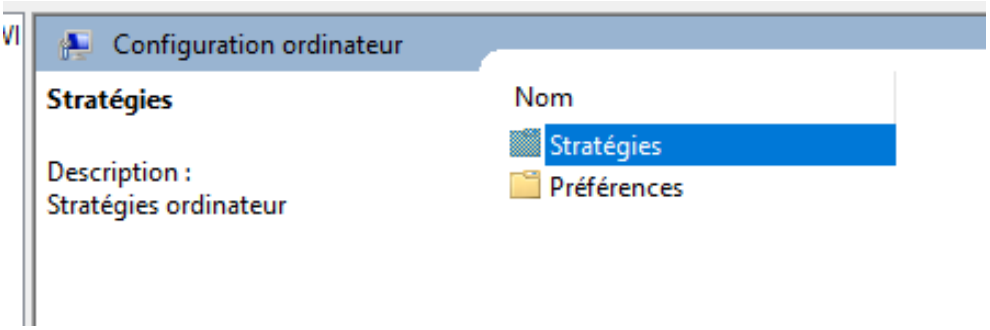
Puis on active *Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC*

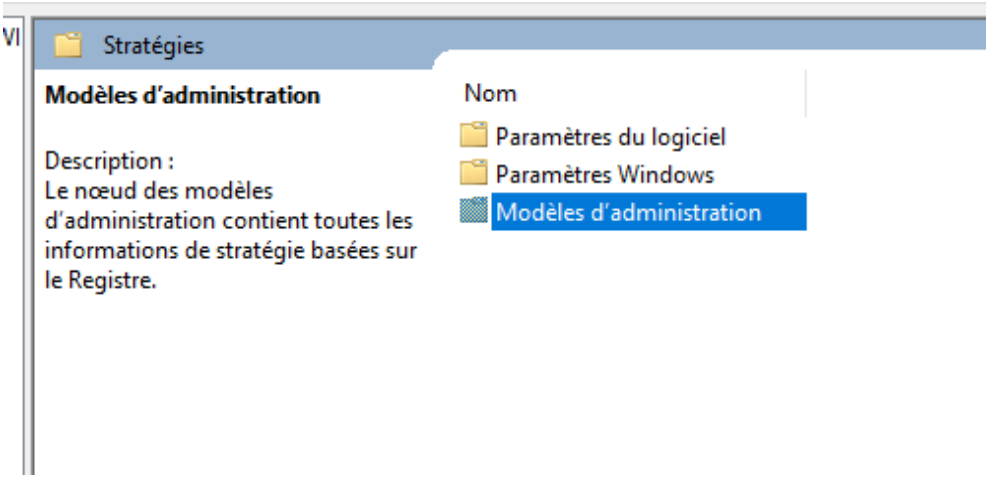


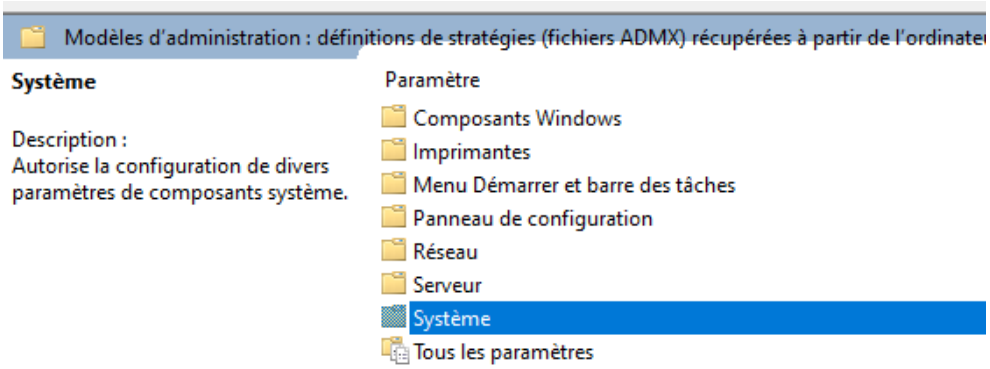
3- SEC-Device-BlockUSB

On modifie la GPO puis on se déplace dans *Configuration Ordinateur > Stratégies > Modèles d'administration > Système*

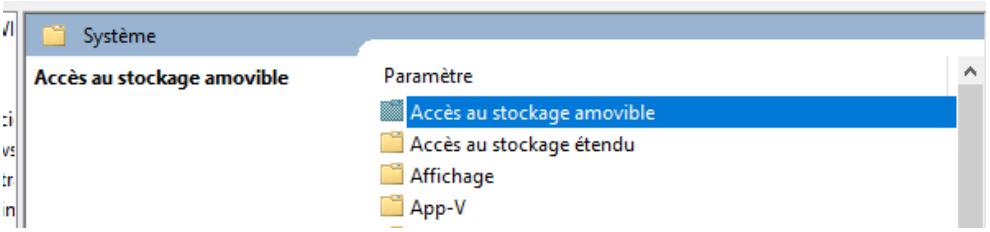






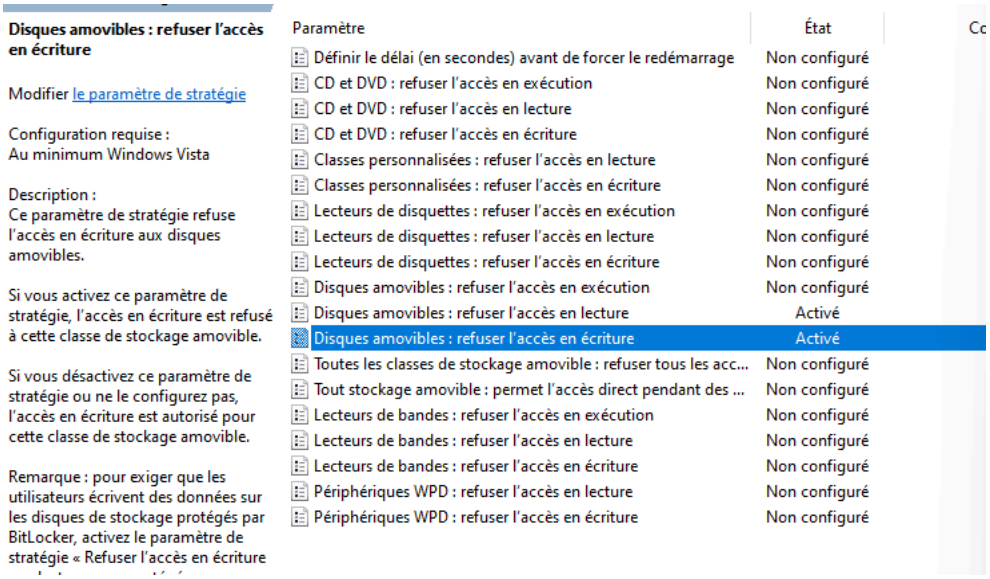


Ensuite on se déplace dans *Accès au stockage amovible*



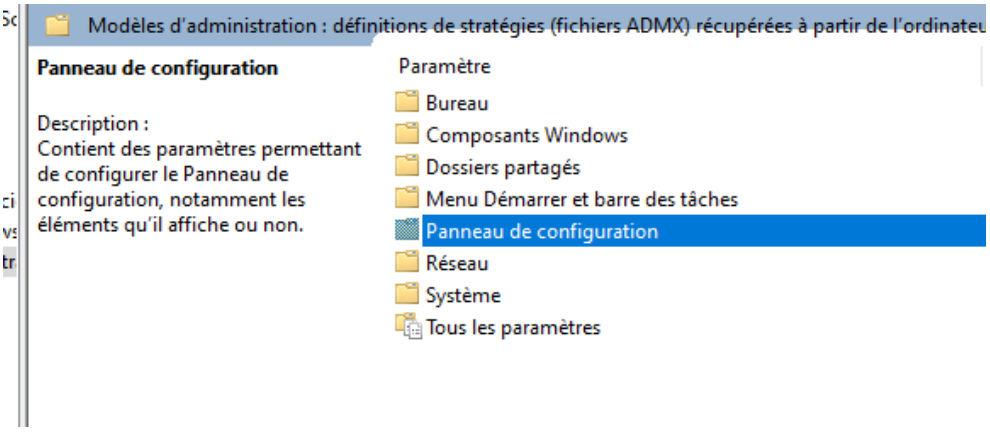
Puis on active :
→ *Disques amovibles : refuser l'accès en lecture*
→ *Disques amovibles : refuser l'accès en écriture*

Résultat :

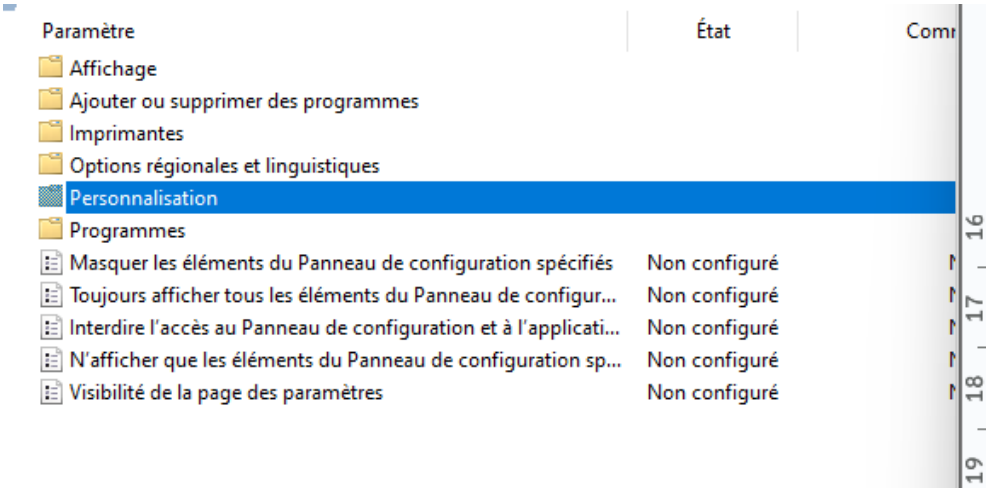


4- SEC-Session-LockedScreensaver

On modifie la GPO puis on se déplace dans *Configuration utilisateur* > *Stratégies* > *Modèles d'administration* > *Panneau de configuration*

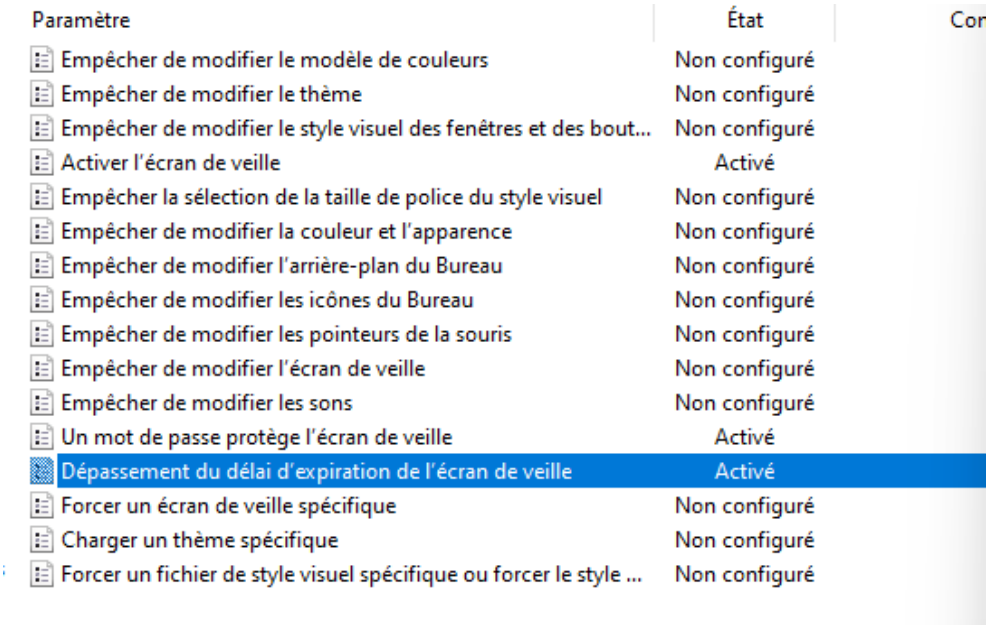


Puis dans *Personnalisation*



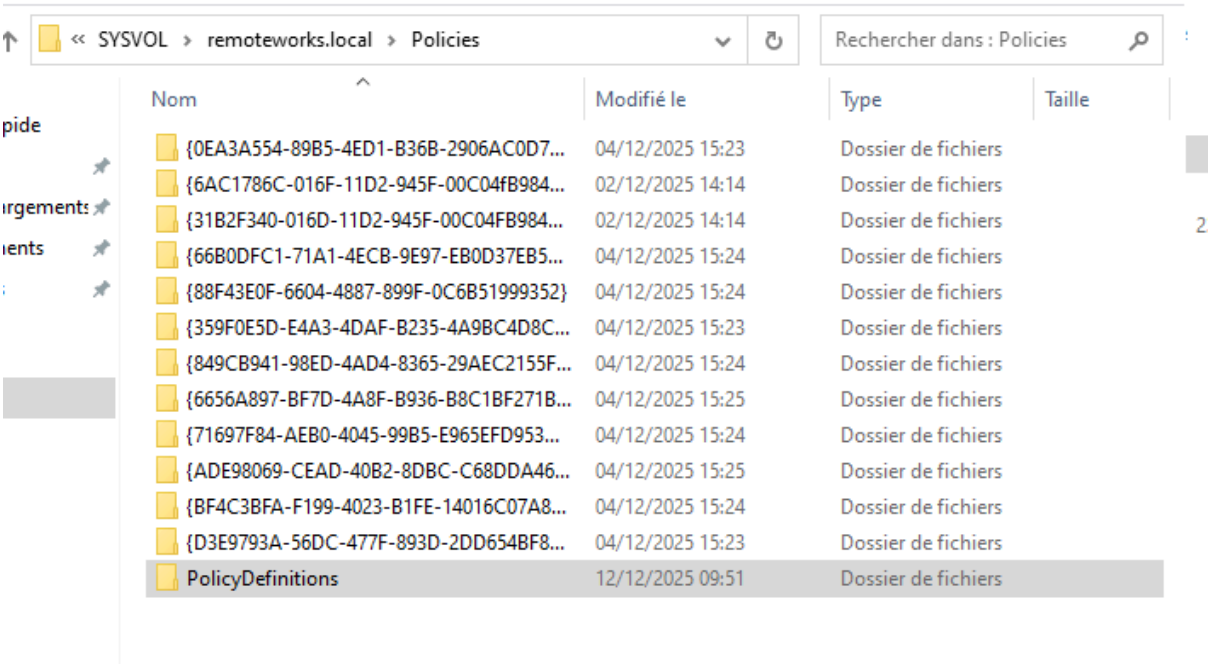
Et on active les paramètres :
Activer l'écran de veille
Un mot de passe protège l'écran de veille
Dépassement du délai d'expiration de l'écran de veille → 600 secondes par exemple

Résultat :

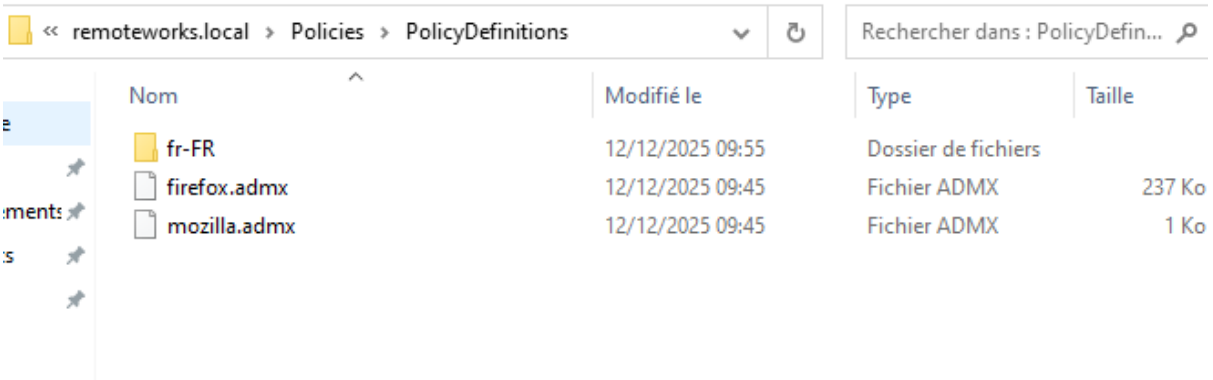


5- APP-FirefoxESR-Hardening

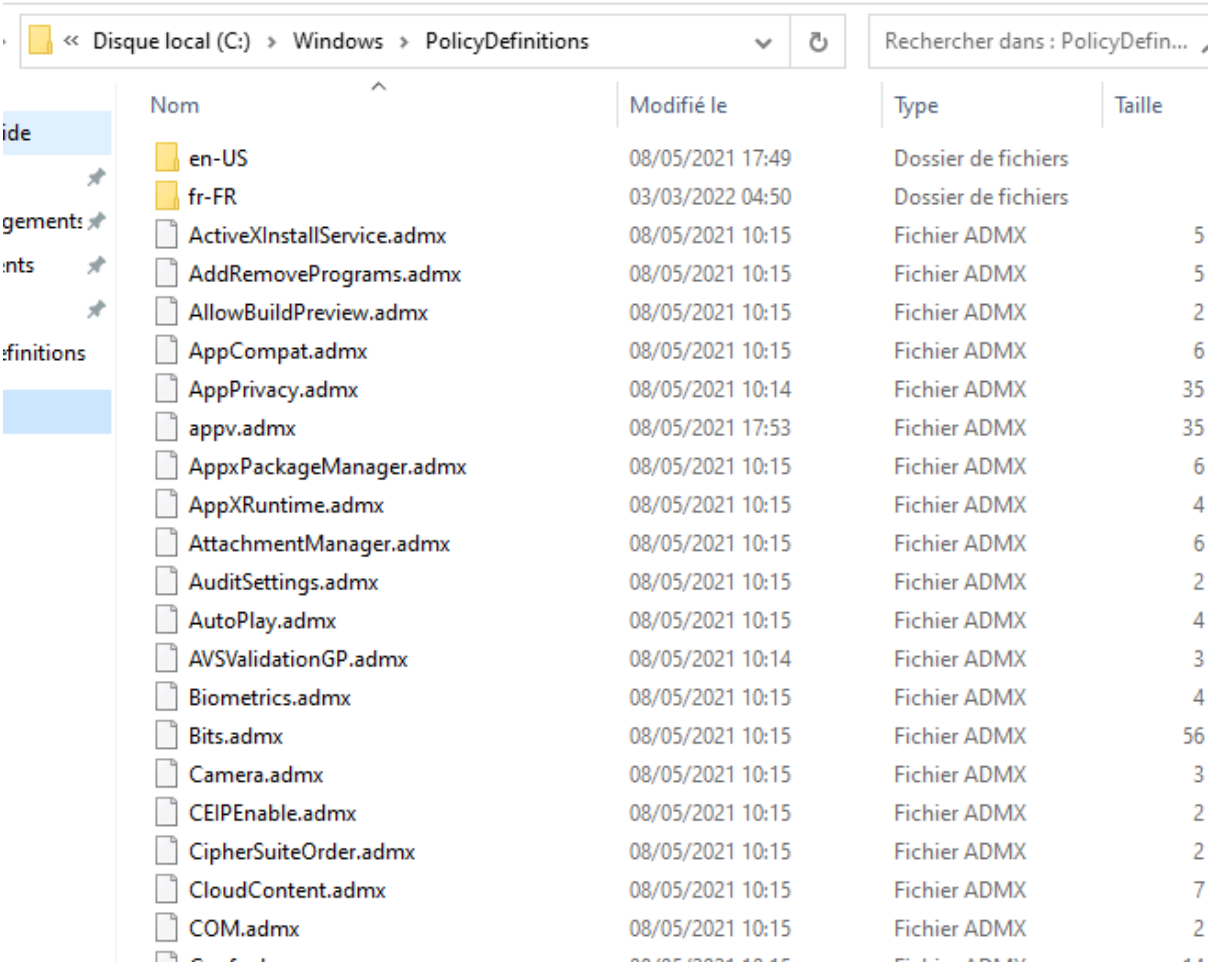
On se rend à l'adresse suivante : https://github.com/mozilla/policy-templates/releases
Et on télécharge le fichier ZIP sur notre serveur. Une fois téléchargé on extrait le fichier puis on se rend au chemin suivant :
\\remoteworks.local\SYSVOL\remoteworks.local\Policies
Si il y a déjà un dossier PolicyDefinitions il faut se rendre dedans sinon il faut le créer.



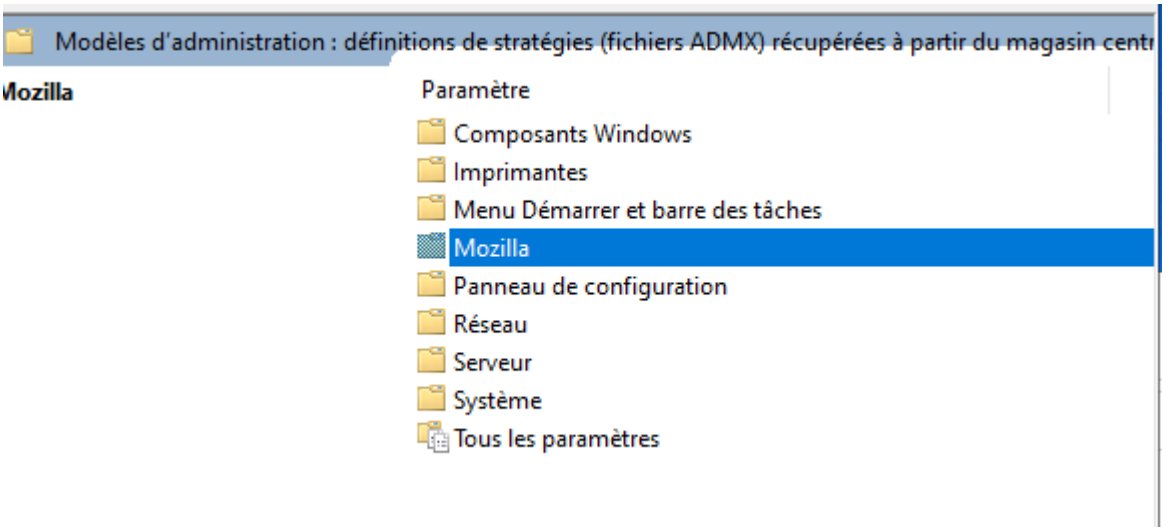
Ensuite on copie les fichiers .admx et le dossier de langue fr-FR (avec les fichiers .adml) dans le dossier PolicyDefinitions.



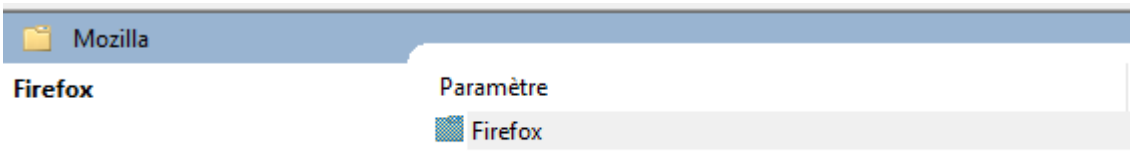
Ensuite on doit également y copier les fichier ADMX et ADML de Windows, pour se faire on suit le chemin C:\\Windows\PolicyDefinitions et on copie l'intégralité des fichiers dans *\\remoteworks.local\SYSVOL\remoteworks.local\Policies\PolicyDefinitions*



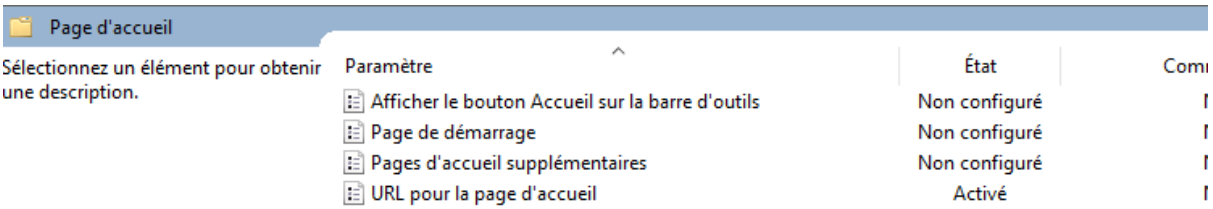
On modifie la GPO puis on se déplace dans *Configuration utilisateur* > *Stratégies* > *Modèles d'administration* > *Mozilla*



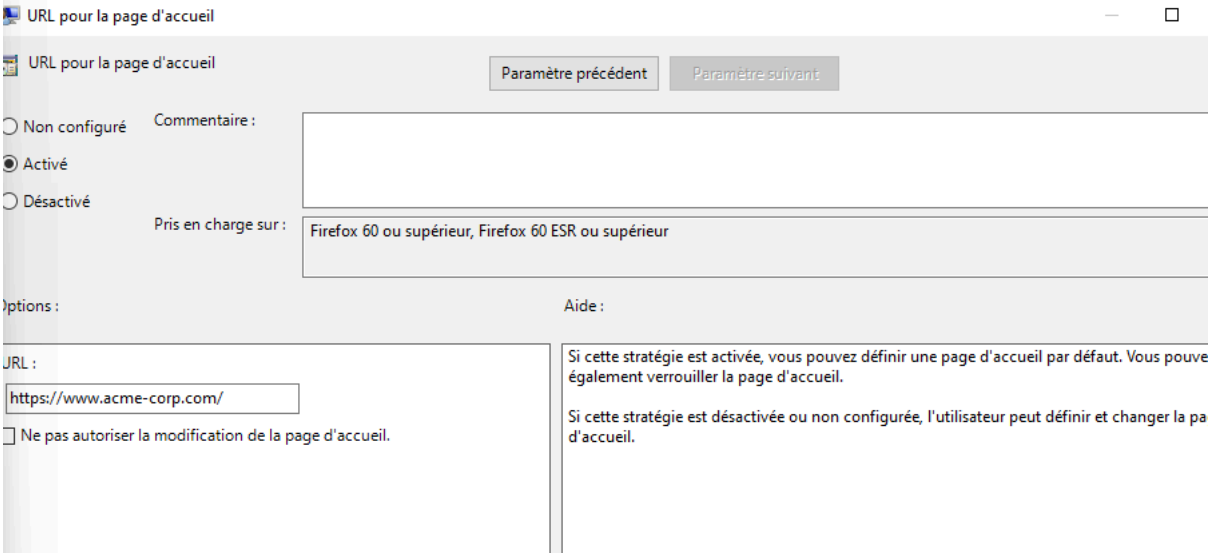
Puis Firefox



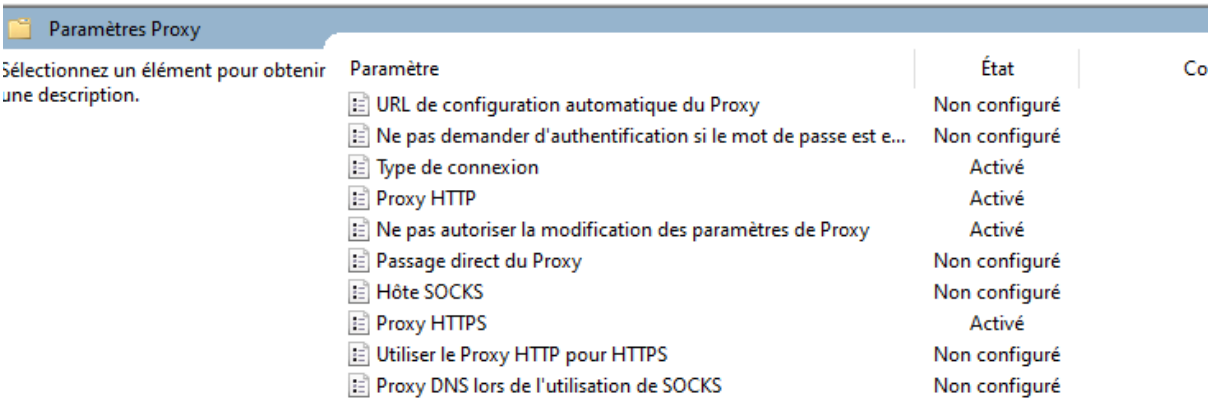
On va dans le dossier Page d'accueil et on active le paramètre URL pour la page d'accueil



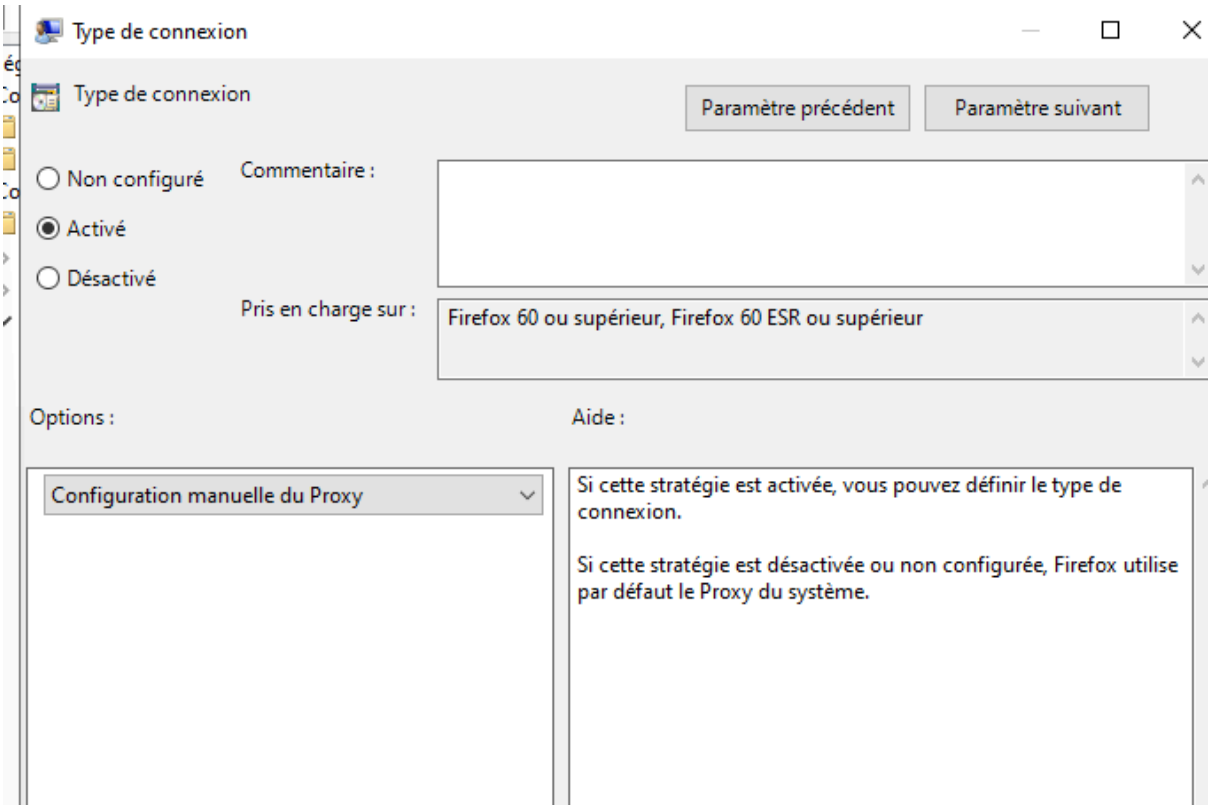
Et on y entre le lien du site web de l'entreprise



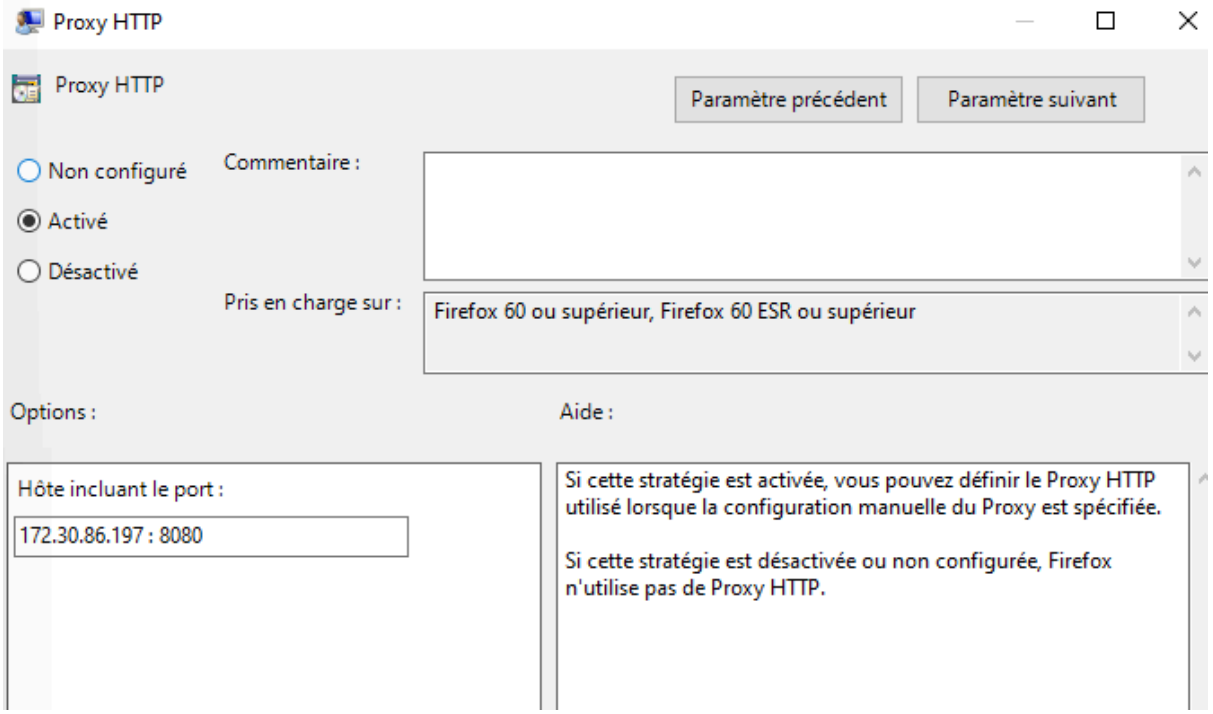
Ensuite on va dans les Paramètres Proxy



Puis on active Type de connexion et on choisi Manuel

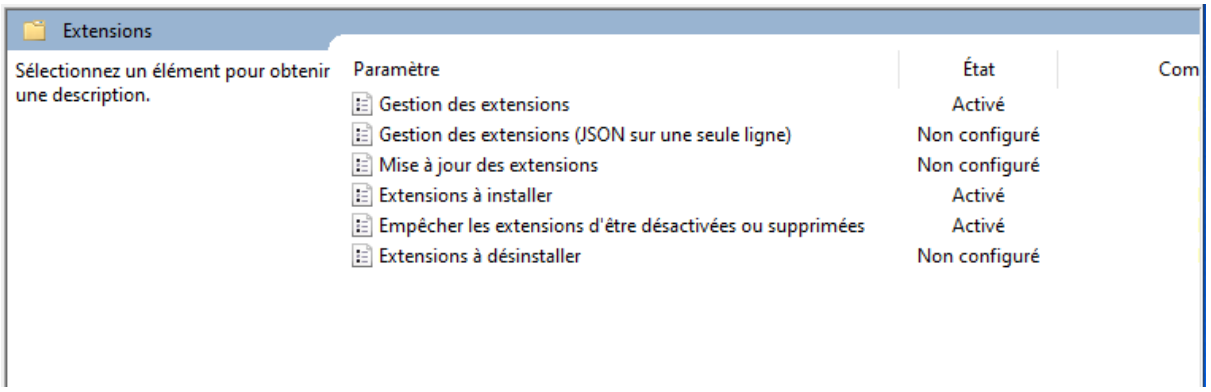


On active également Proxy HTTP et Proxy HTTPS et on y entre l'ip de notre machine avec le port 8080



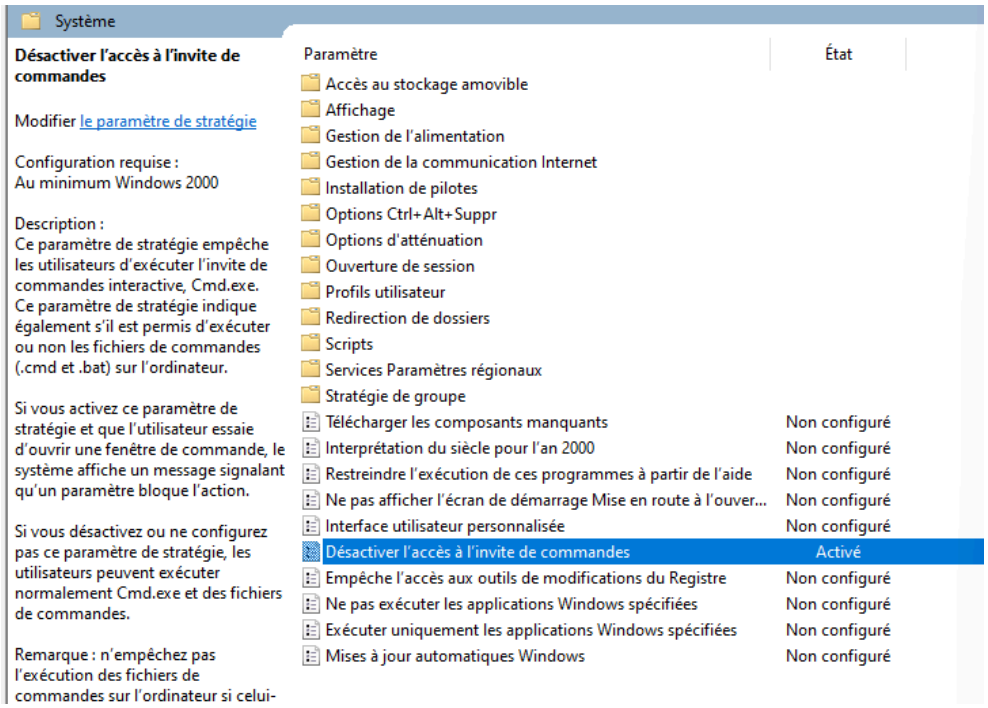
Et pour finir on active l'option Ne pas autoriser la modification des paramètres de Proxy.

Ensuite on va dans le dossier Extensions et on active Gestion des extensions, Extensions installer et Empêcher les extensions d'être désactivées ou supprimées



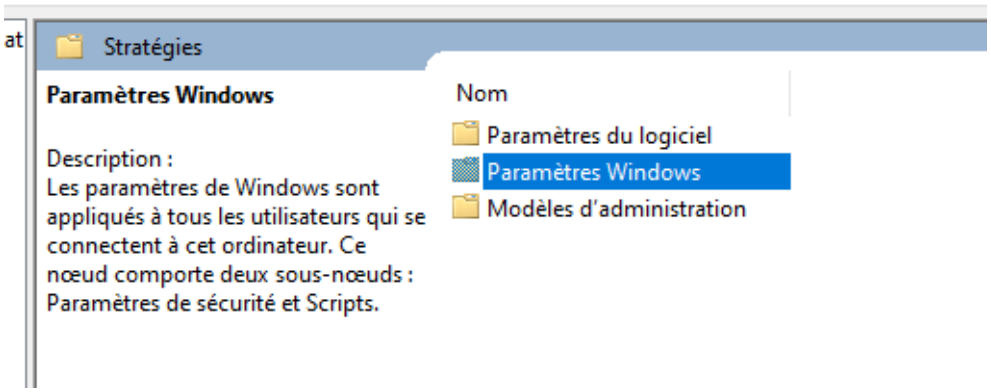
6-SEC-User-NoCMD

On modifie la GPO puis on se déplace dans *Configuration utilisateur > Stratégies > Modèles d'administration > Système*
On active l'option *Désactiver l'accès à l'invite de commandes*

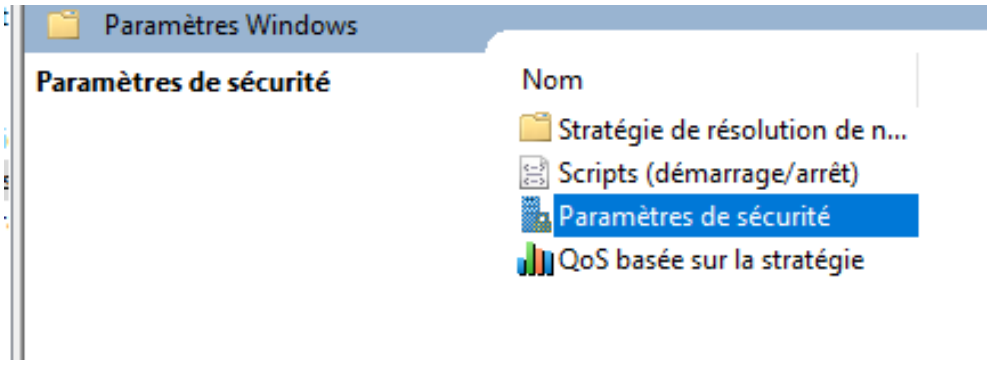


7- SEC-Firewall-Workstations

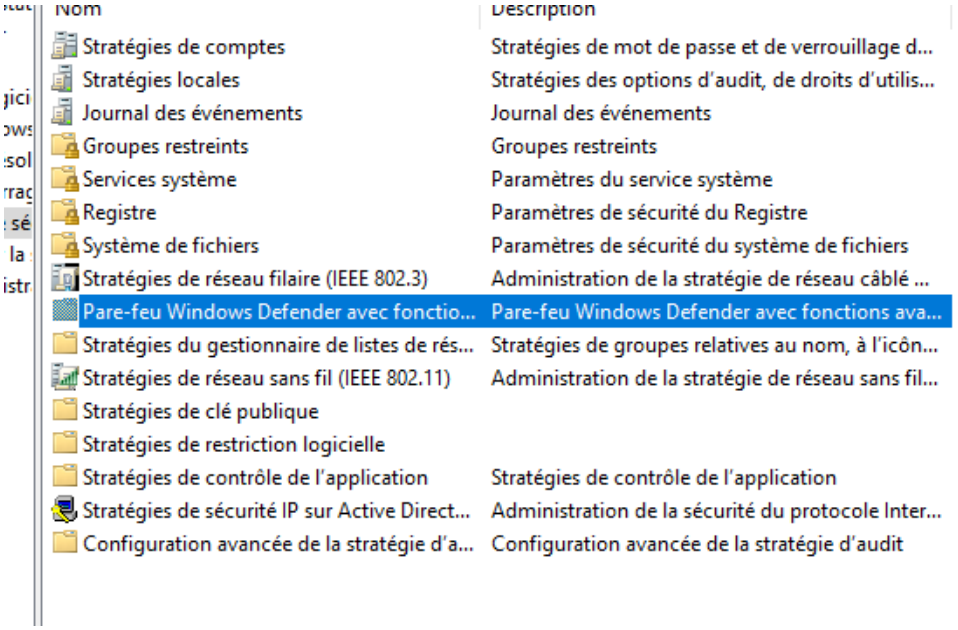
On modifie la GPO puis on se déplace dans *Configuration ordinateur > Stratégies > Paramètres Windows*



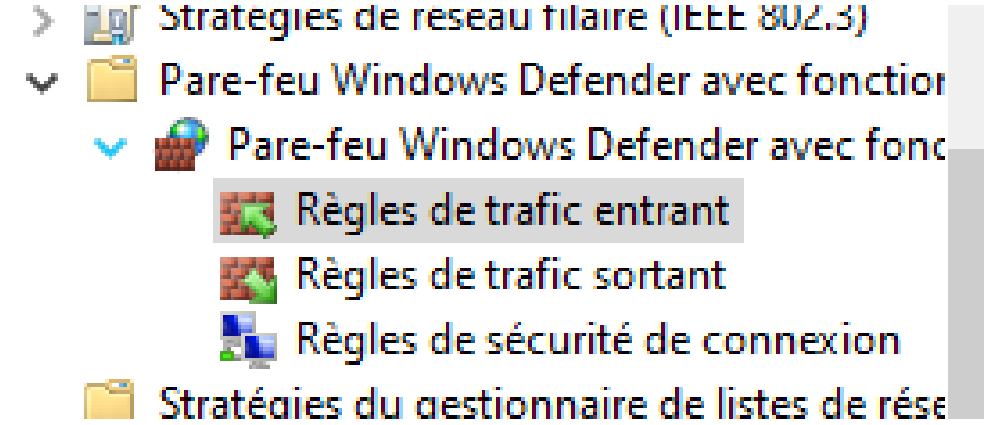
Puis dans *Paramètres de sécurité*



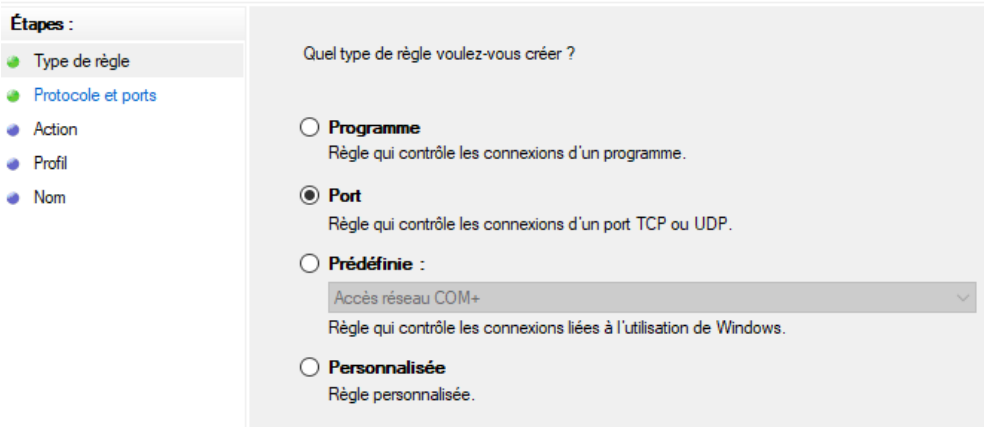
Puis dans *Pare-feu Windows Defender avec fonctions avancées de sécurité*



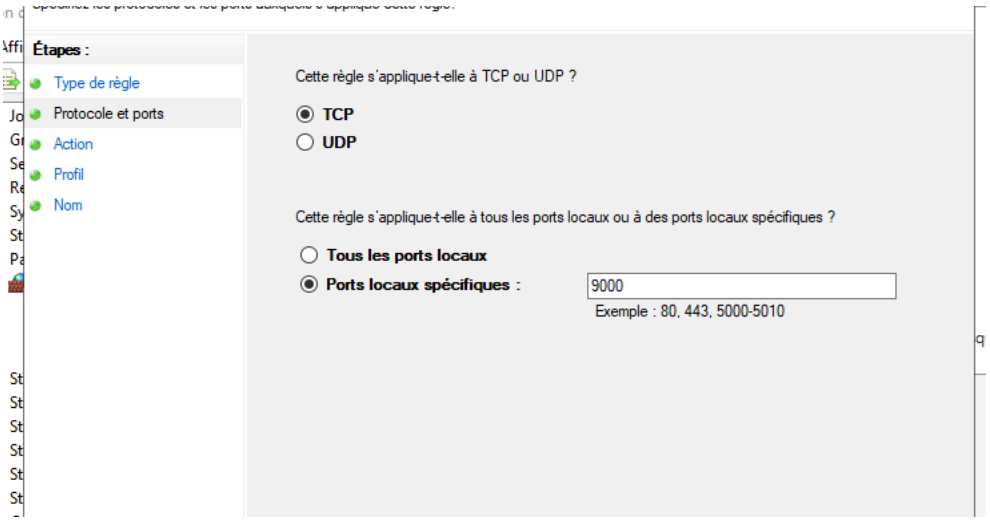
On ajoute une nouvelle règle dans *Règles de trafic entrant*



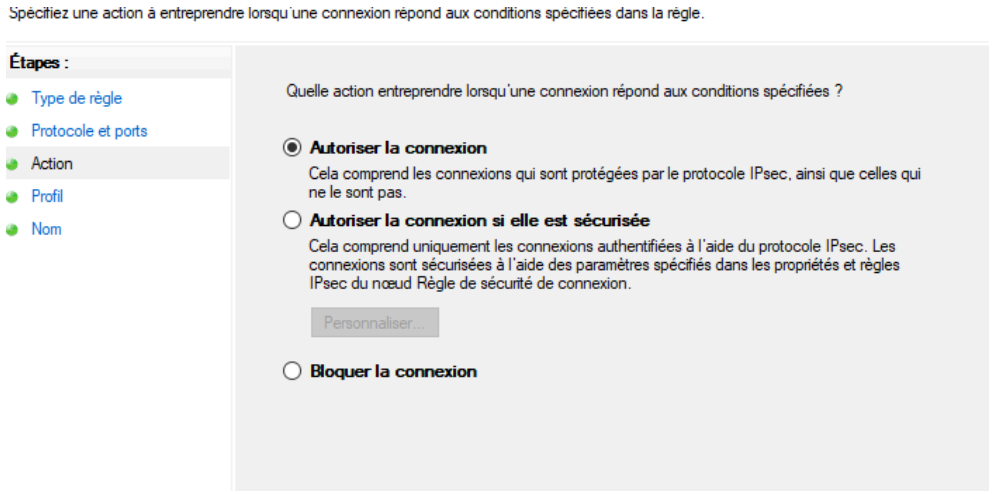
De type *Port*



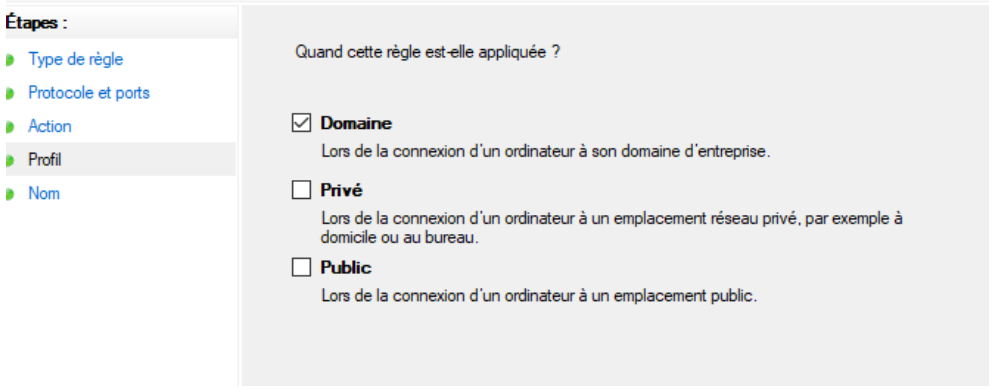
On laisse le Protocole TCP et en Ports locaux spécifiques on peut entrer 9000 par exemple



On autorise la Connexion

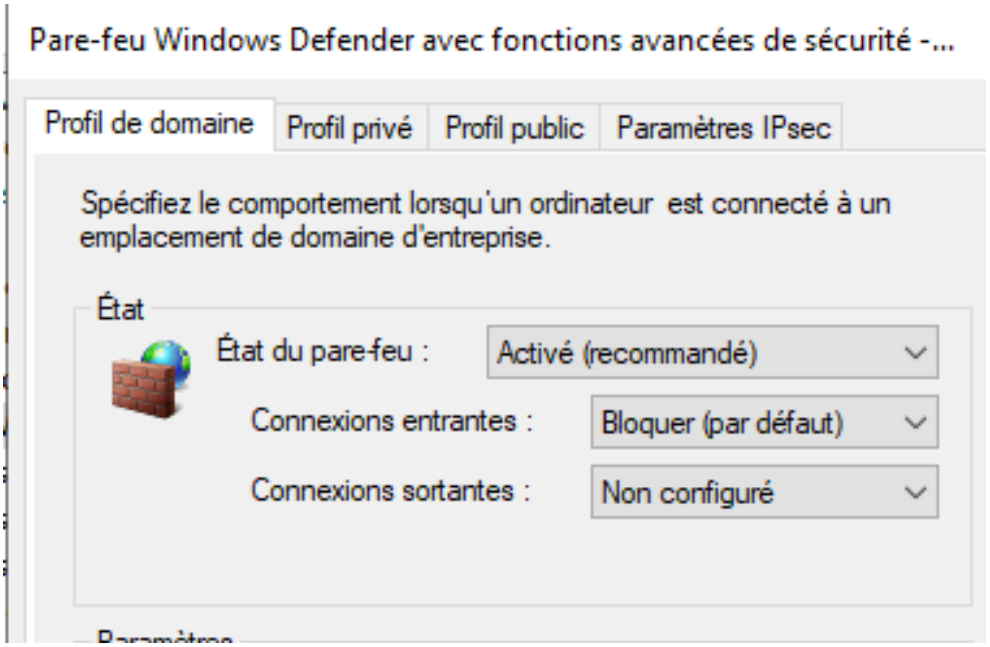


Et on l'applique uniquement sur le Domaine



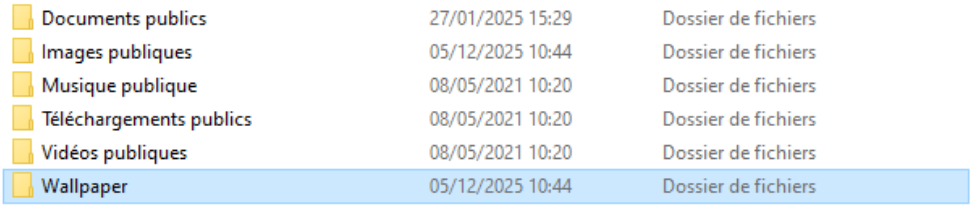
Ensuite on lui donne un nom et on enregistre cette nouvelle règle

On doit également modifier les Propriétés du Pare-feu Windows Defender et bloquer les Connexion entrante par défaut

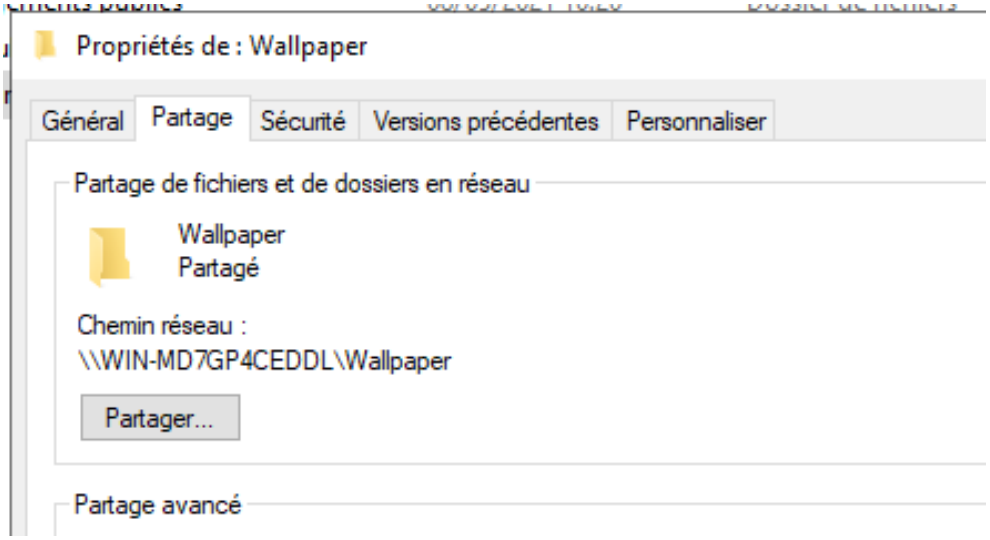


8- CORP-Wallpaper-BySite

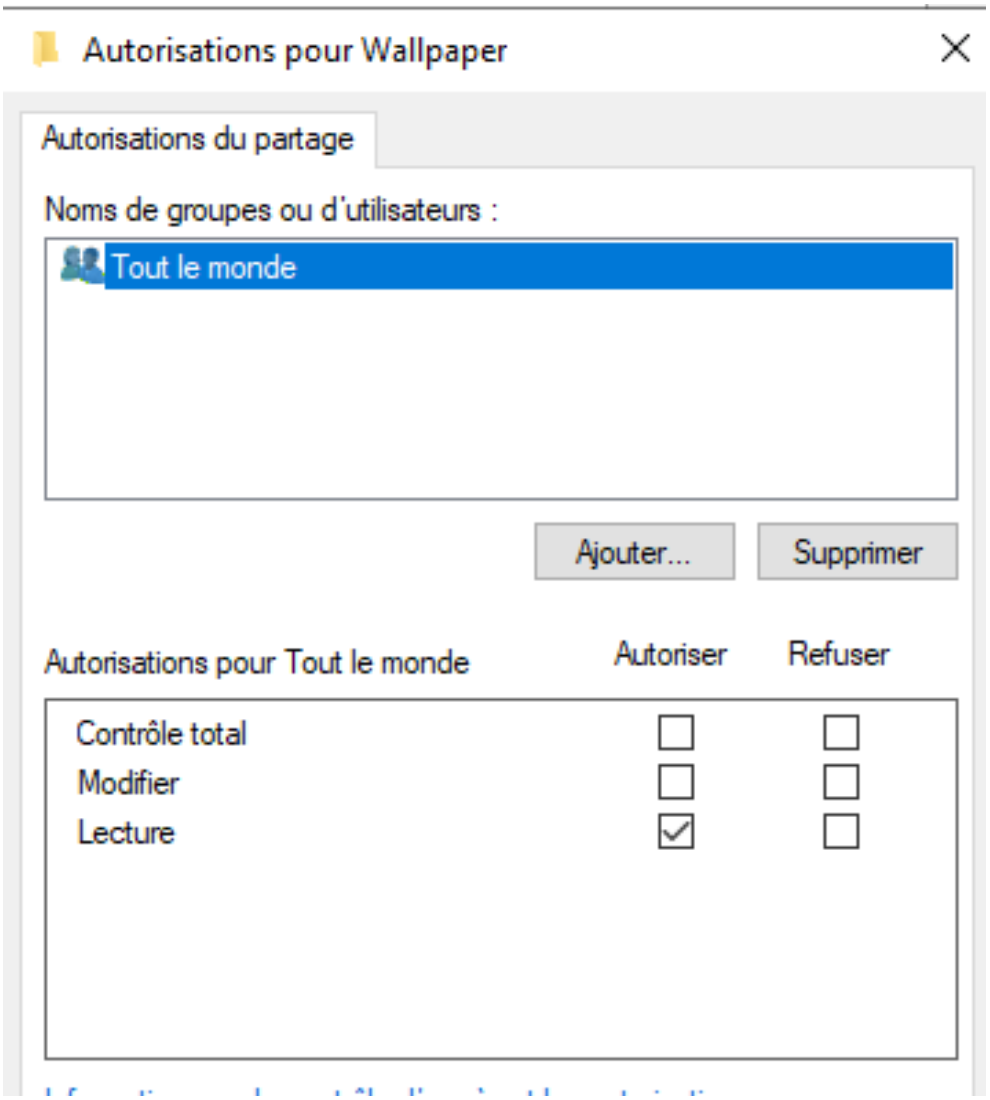
Pour appliquer un fond d'écran commun, il faut premièrement importer une image qui fera office de fond d'écran puis la mettre dans un dossier



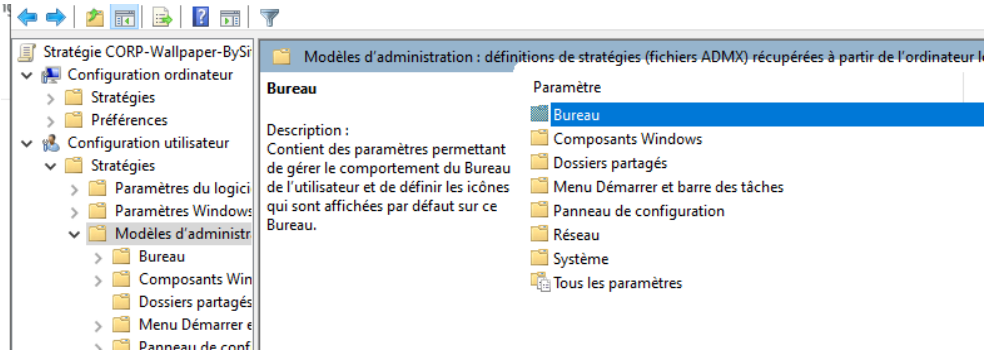
On le rend partageable :



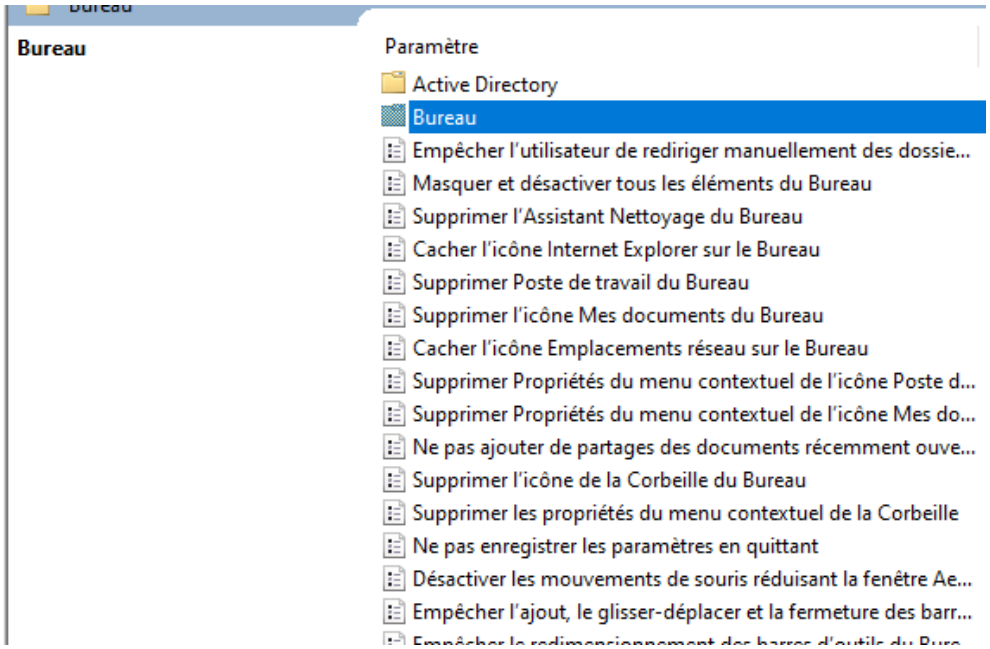
Et dans les paramètres du partage, bien vérifier que tout le monde à l'autorisation de lecture.



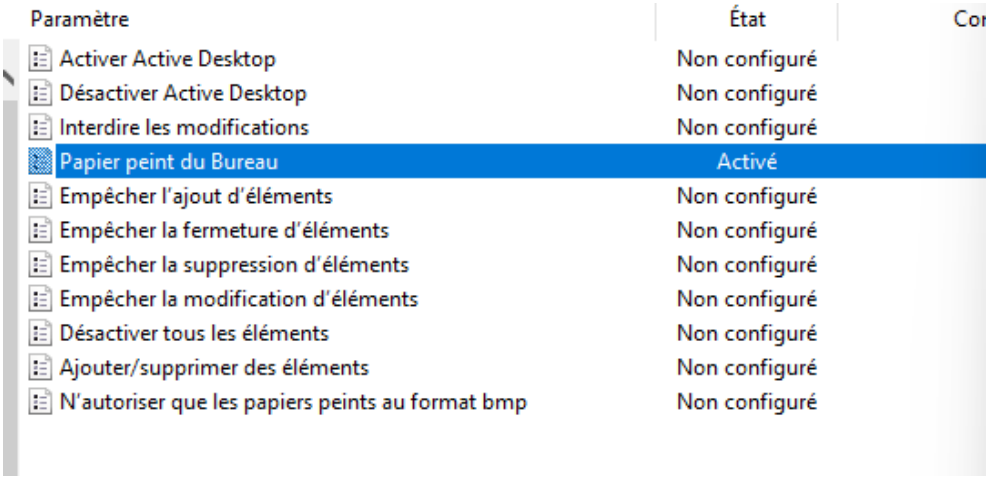
On modifie la GPO puis on se déplace *Configuration Utilisateur > Stratégies > Modèles d'administration > Bureau*



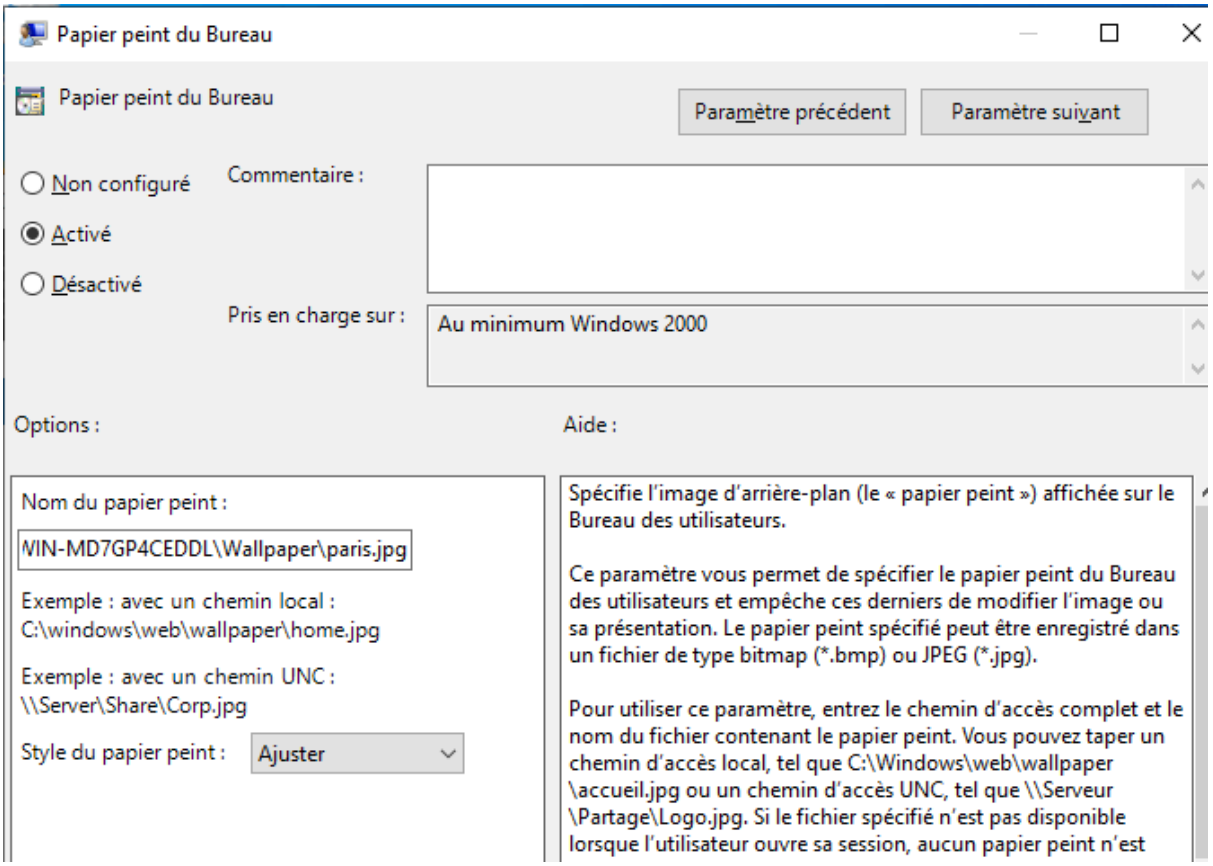
Puis dans Bureau



Et on active *Papier peint du Bureau*



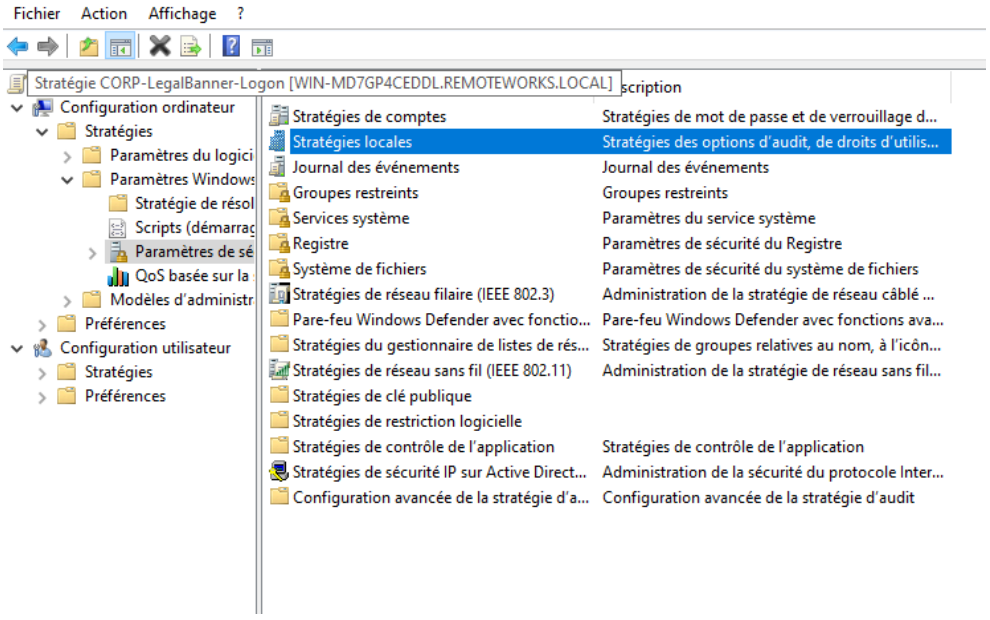
On entre le chemin d'accès du fond d'écran



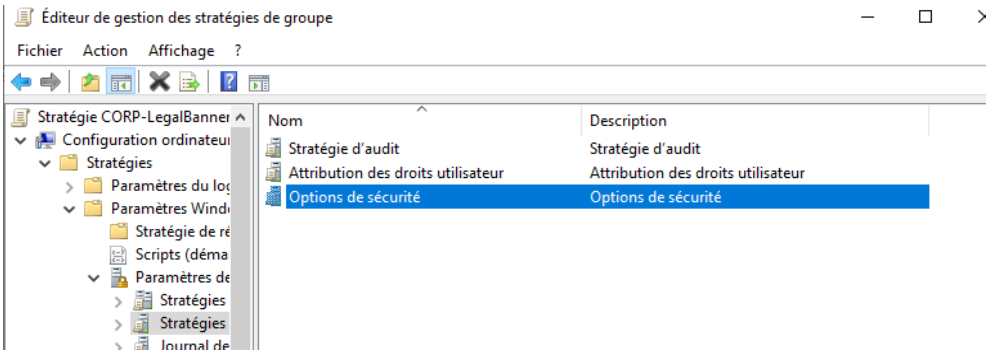
9- CORP-LegalBanner-Logon

On modifie la GPO puis on se déplace dans *Configuration ordinateur* > *Stratégies* > *Paramètres Windows* > *Paramètres de sécurité*

Puis dans *Stratégies locales*

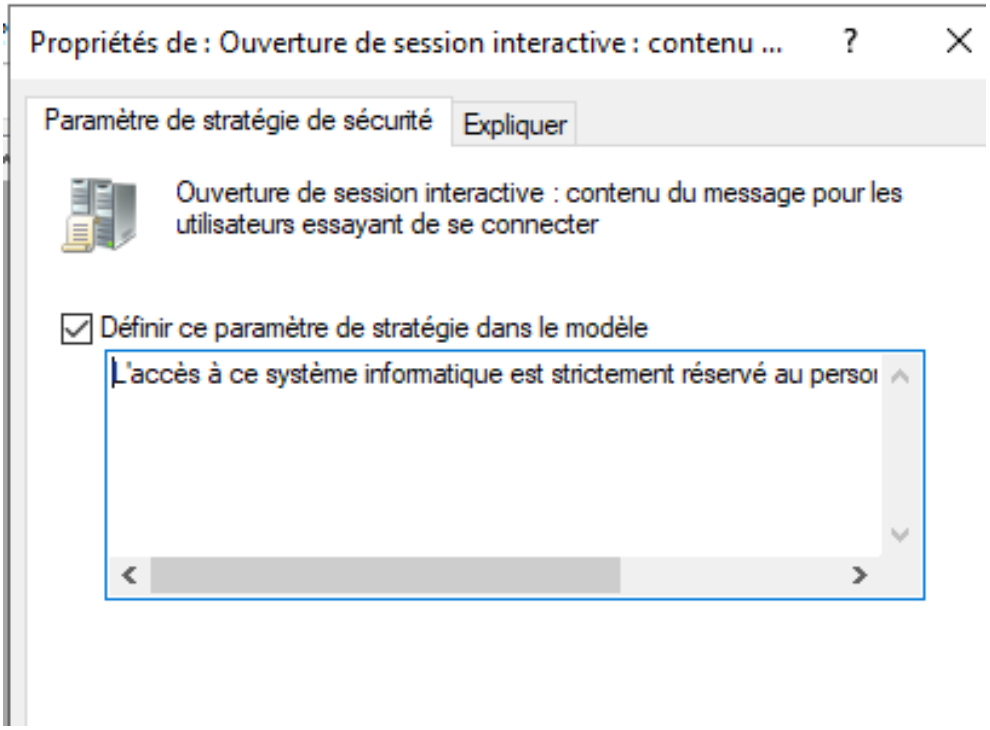


Et enfin dans *Options de sécurité*



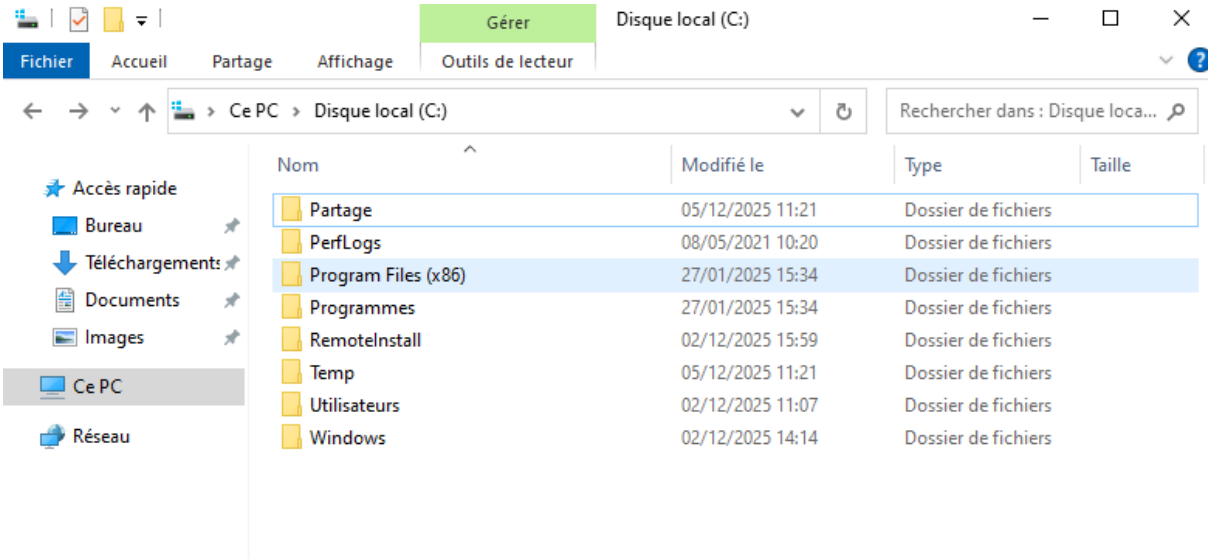
Ensuite on ouvre les propriétés d'*Ouverture de session interactive : contenu du message pour les utilisateurs essayant de se connecter*

Puis on entre un texte qui s'affiche lors de la connexion des utilisateurs



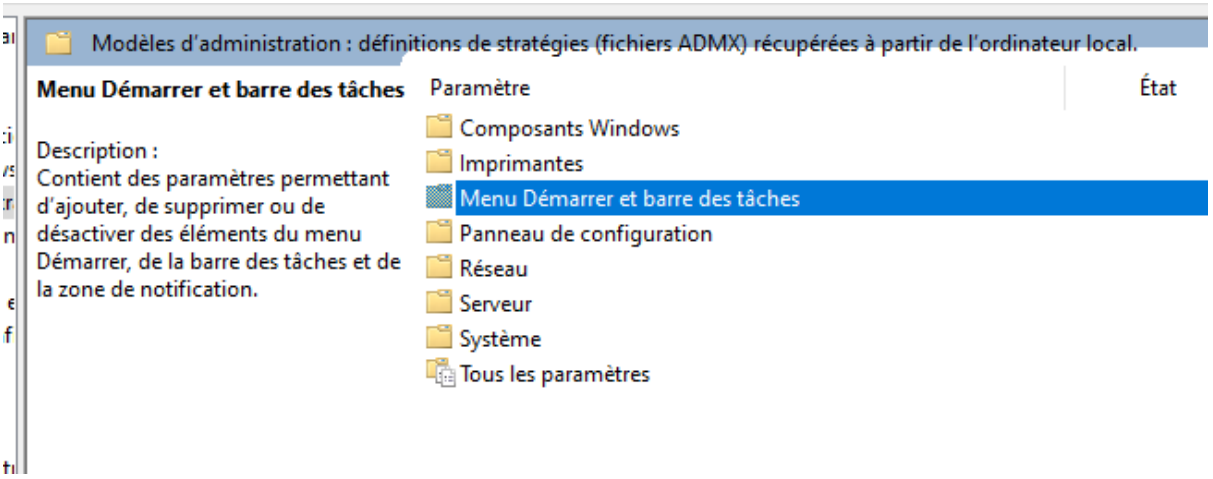
10- UX-StartMenu-Taskbar-Standard

Premièrement on choisit les applications que l'on veut épingler sur notre barre de tâche. Puis on crée un dossier partagé comme pour le fond d'écran

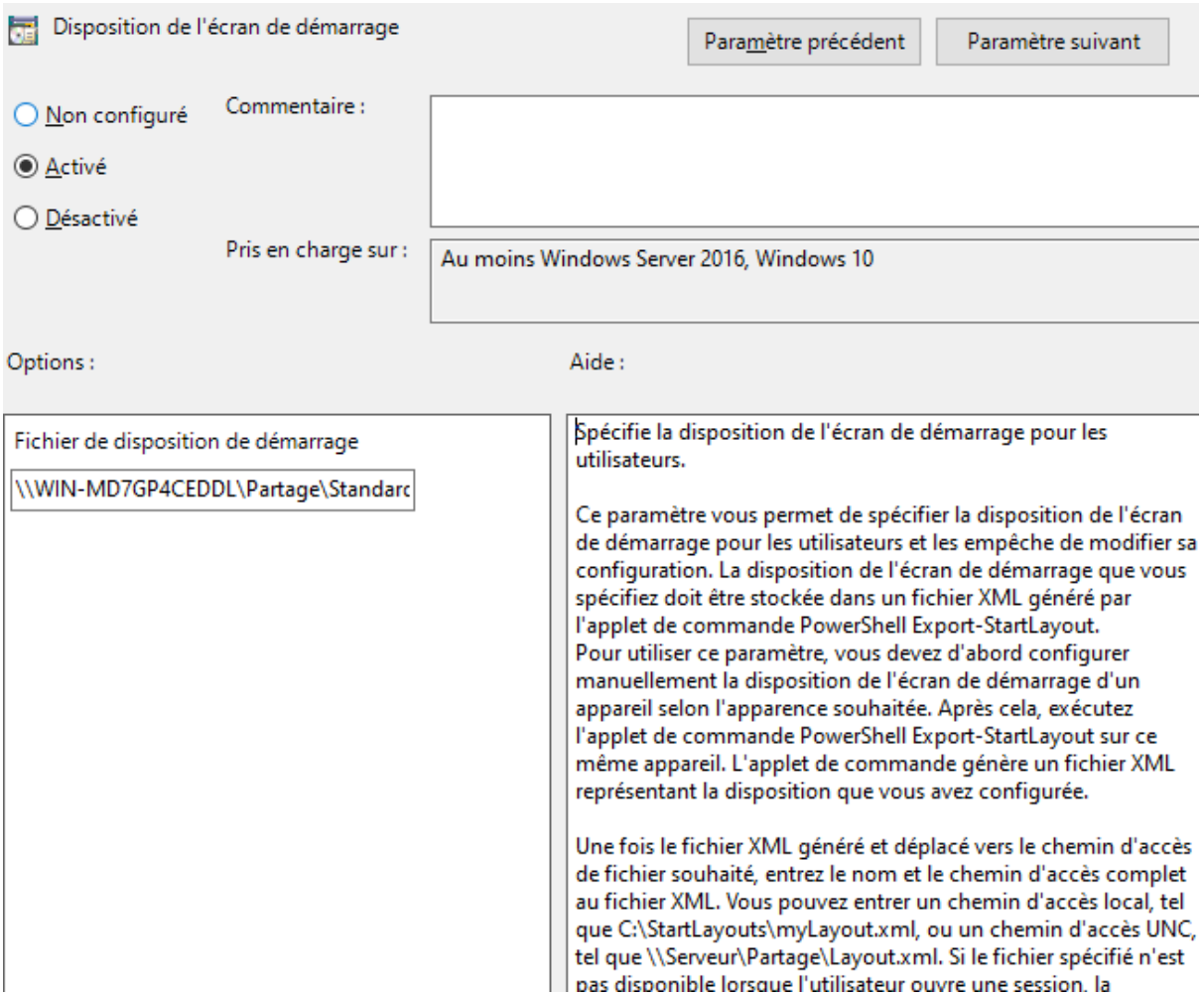


Puis dans le powershell, on exécute la commande suivante :
Export-StartLayout -Path "C:\Partage\StandardLayout.xml"

On modifie la GPO puis on se déplace dans *Configuration ordinateur* > *Stratégies* > *Modèle d'administration* > *Menu Démarrer et barre des tâches*

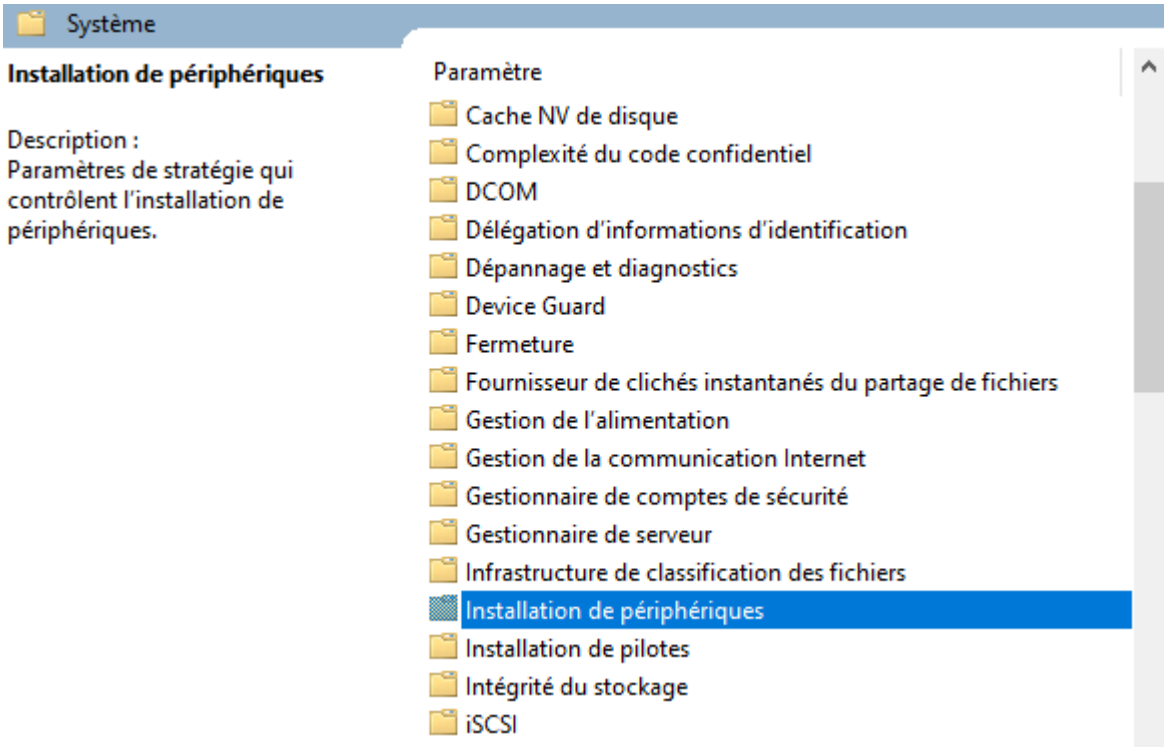


Puis on active *Disposition de l'écran de démarrage* et on y joint le chemin d'accès du fichier XML

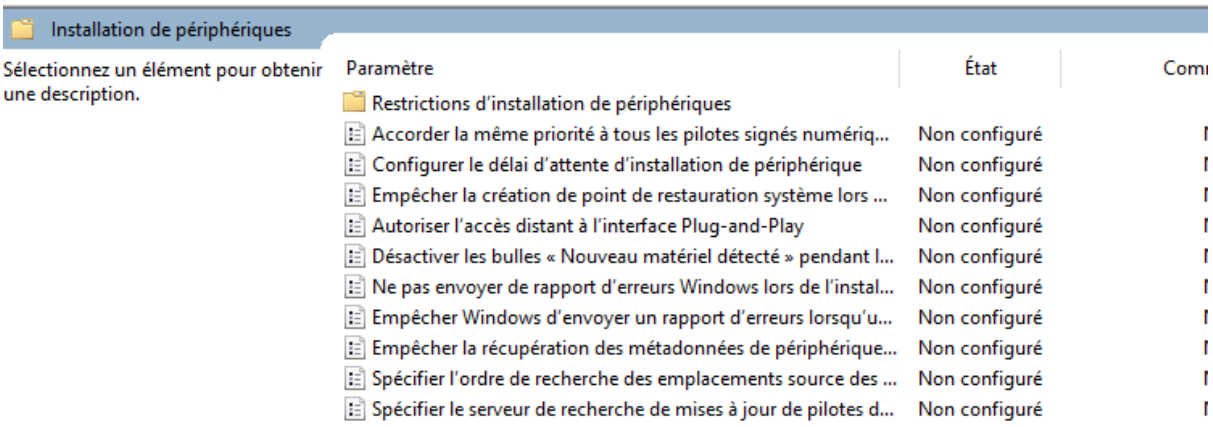


11- SEC-Device-BlockBluetooth

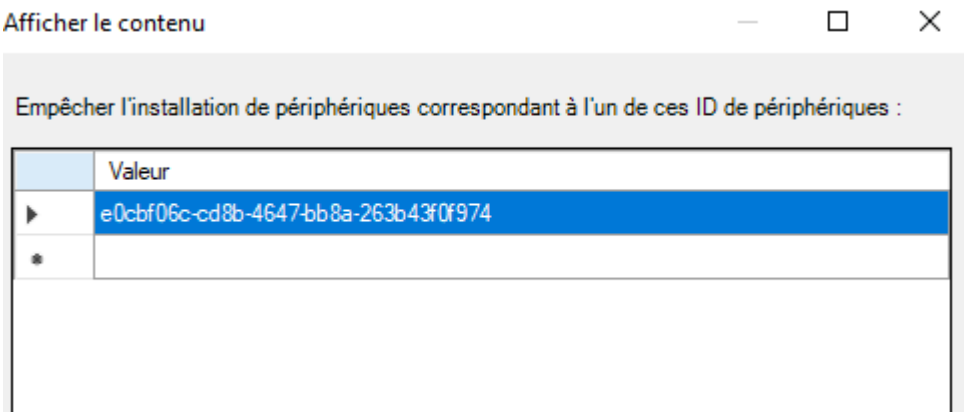
On modifie la GPO puis on se déplace dans *Configuration ordinateur > Stratégies > Modèles d'administration > Système > Installation de périphériques*



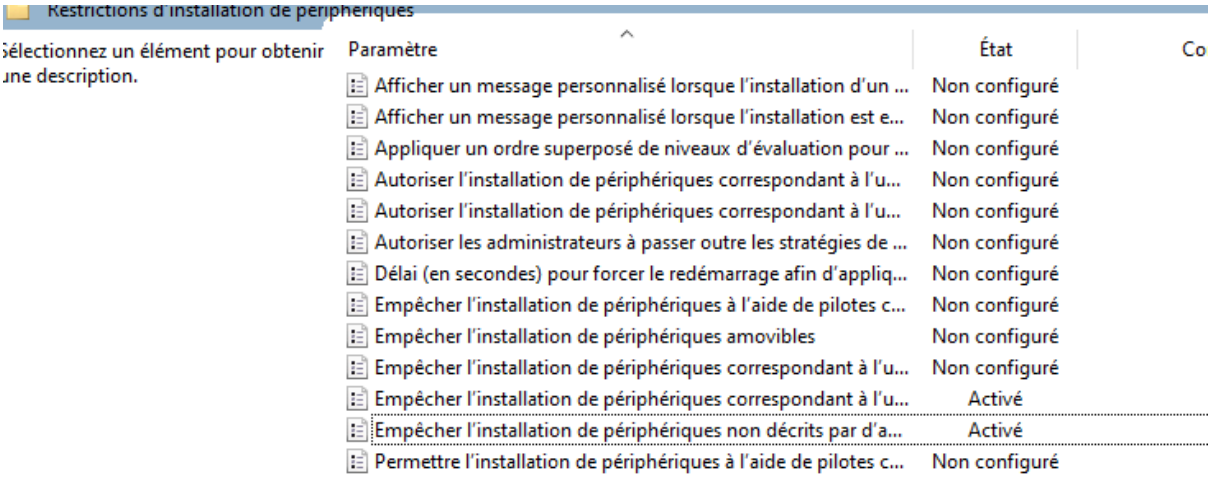
Puis dans Restrictions d'installation des périphériques



On active l'option *Empêcher l'installation de périphériques correspondant à l'un de ces ID de périphériques* et on entre le GUID de la classe Bluetooth sur Windows

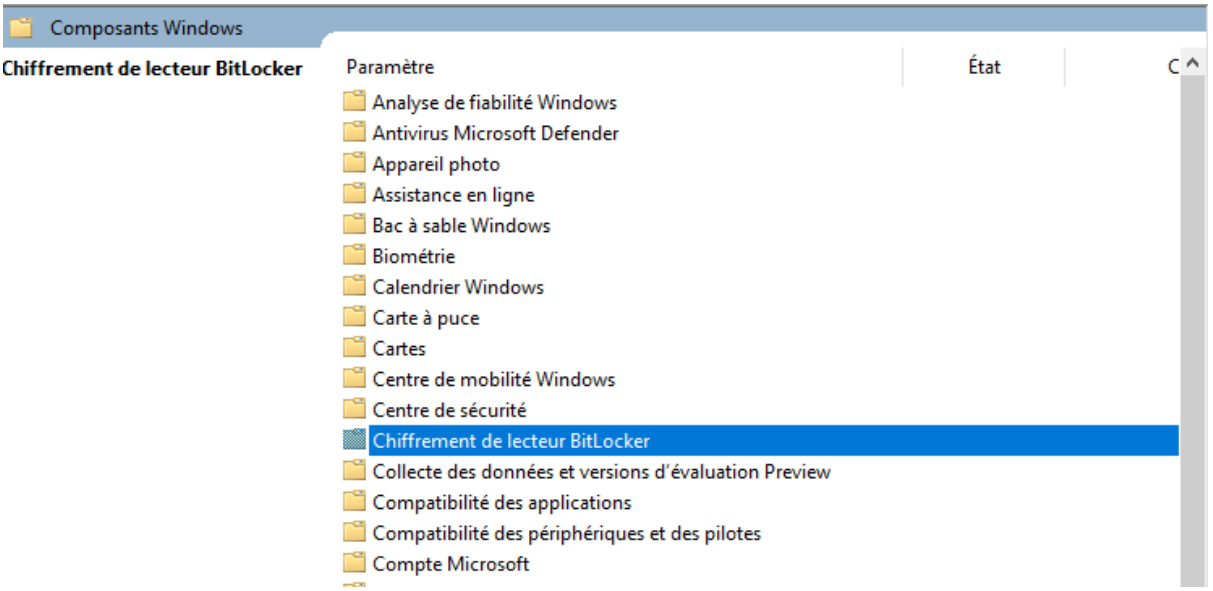


On active également l'option *Empêcher l'installation de périphériques non décrits par d'autres paramètres de stratégie*

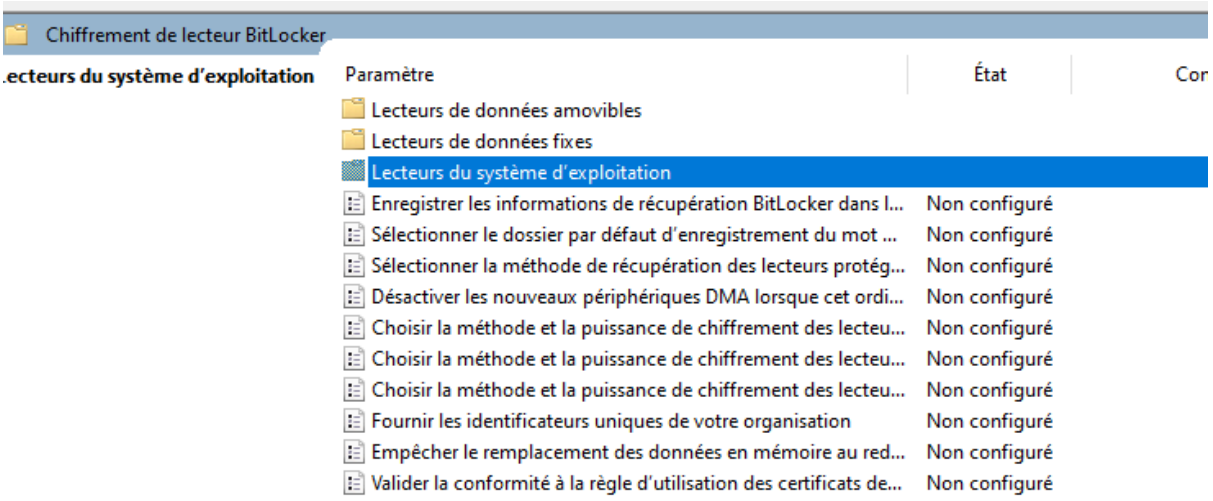


12- SEC-BitLocker-Workstations

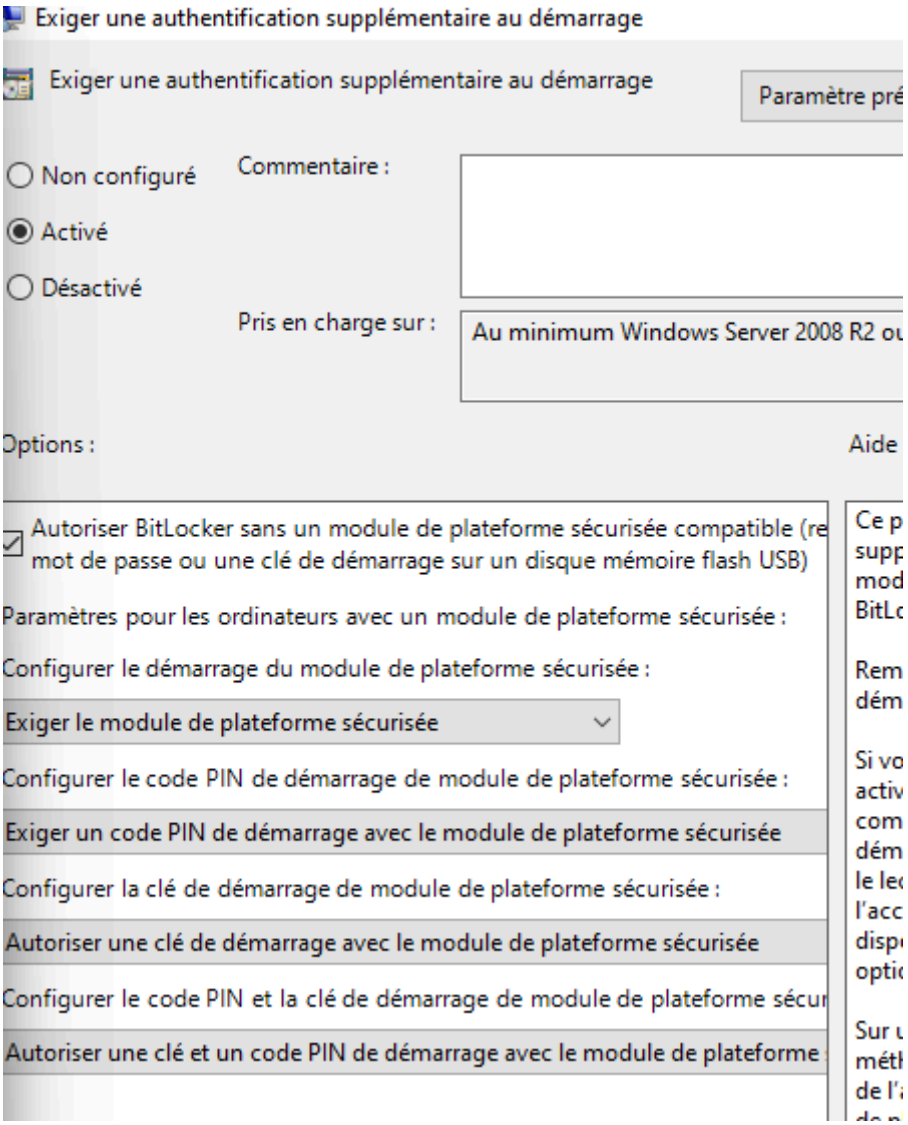
On modifie la GPO puis on se déplace dans *Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Chiffrement de lecteur Bitlocker*



Puis dans Lecteurs du système d'exploitation

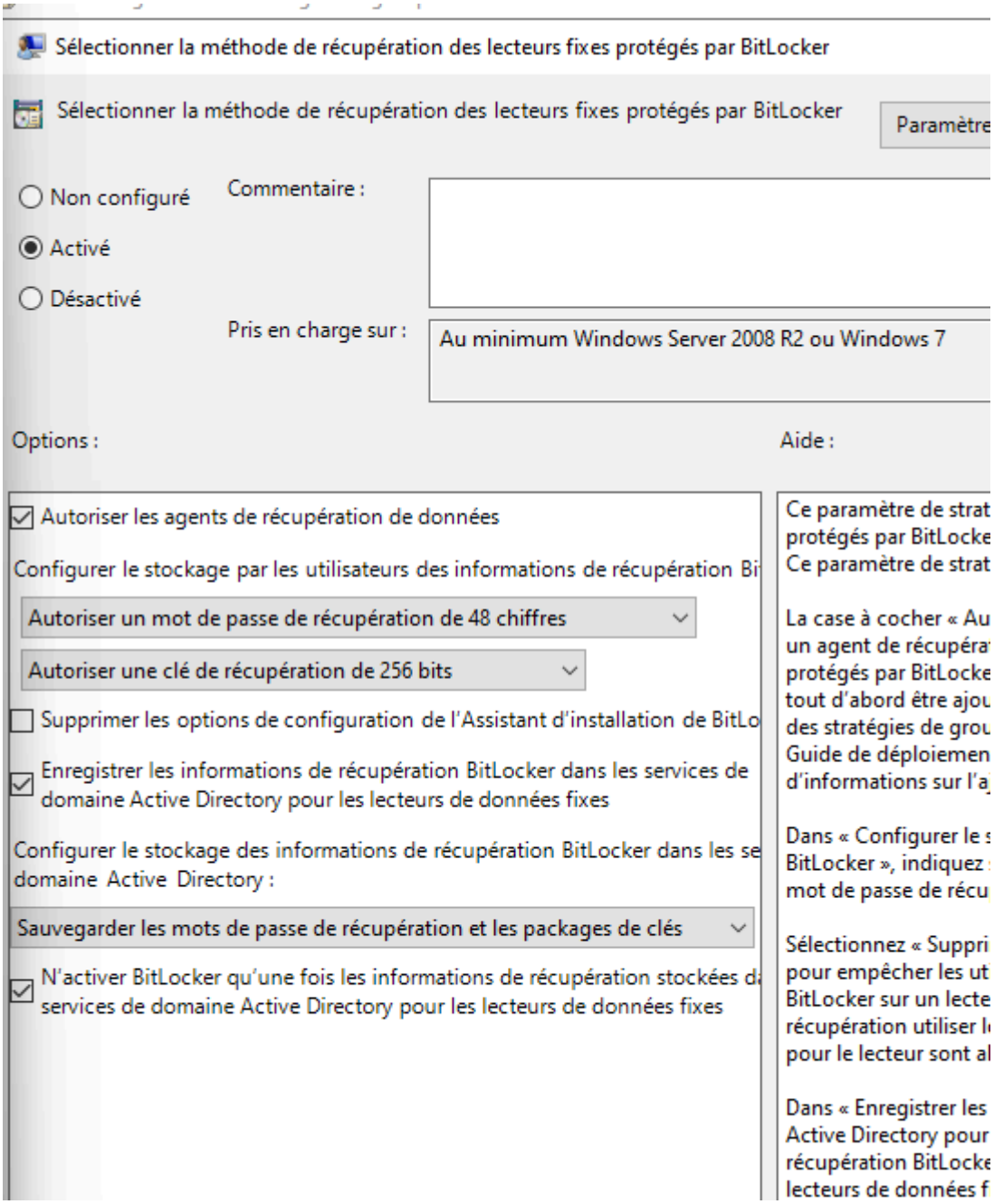


On active le paramètre *Exiger une authentification supplémentaire au démarrage*, *Exiger le module de plateforme sécurisé* et *Exiger un code PIN de démarrage avec le module de plateforme sécurisée*

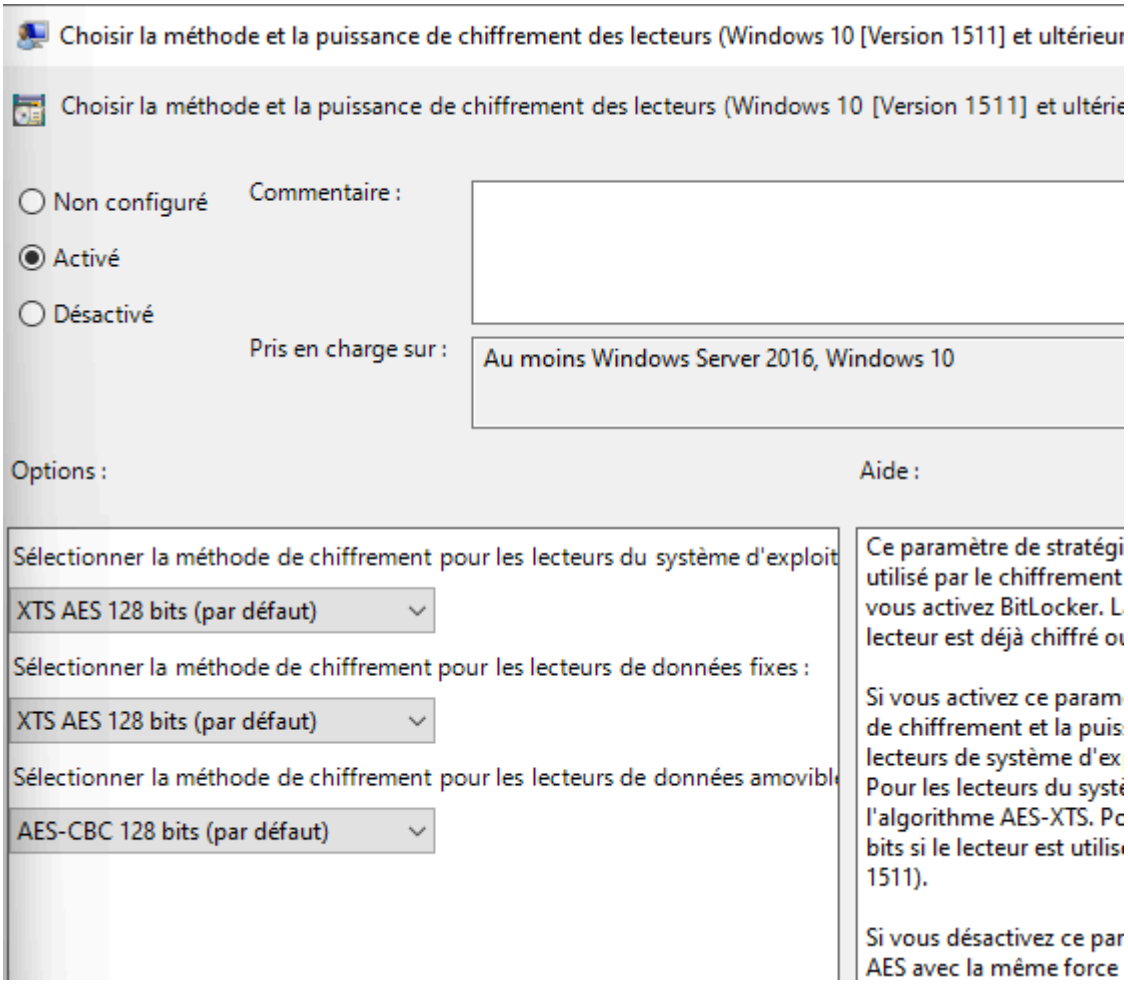


Ensuite on va dans le dossier Lecteurs de données fixes et on active le paramètres Sélectionner la méthode de récupération des lecteurs fixes protégés par Bitlocker et

on active les options suivantes

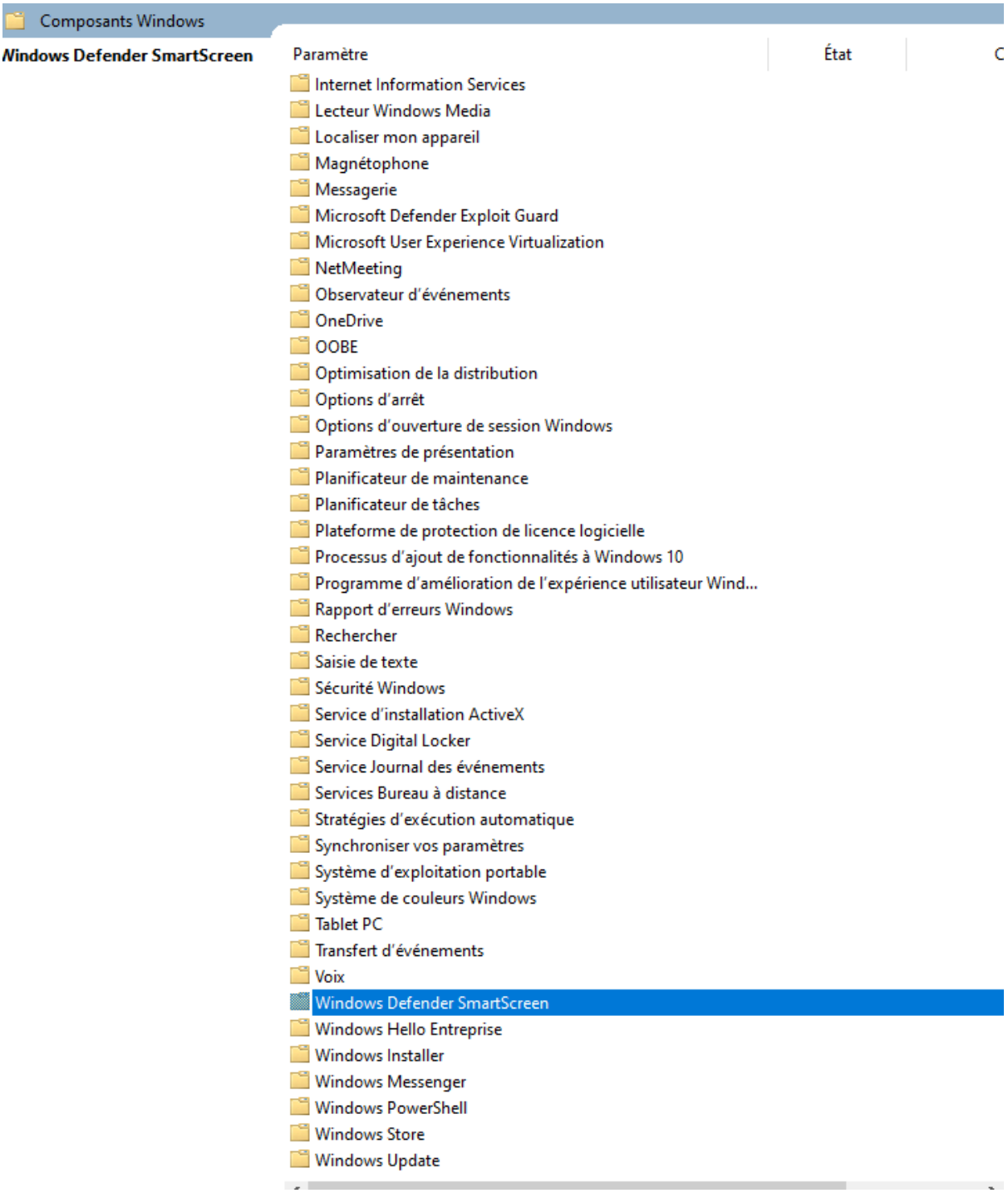


Pour finir on retourne dans le dossier global Chiffrement de lecteur Bitlocker et on active l'option Choisir la méthode et la puissance de chiffrements des lecteurs

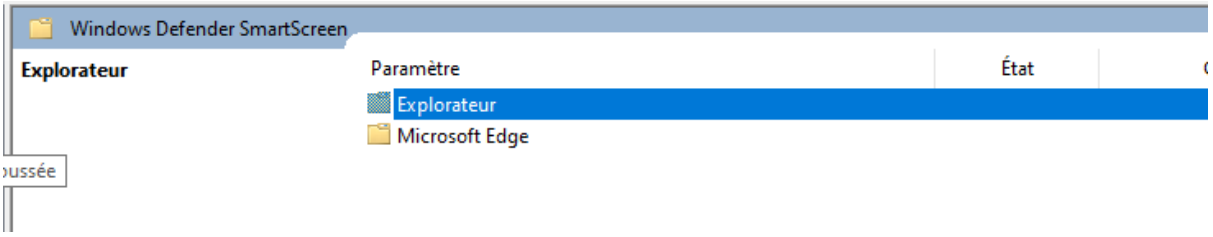


13- SEC-SmartScreen-Enable

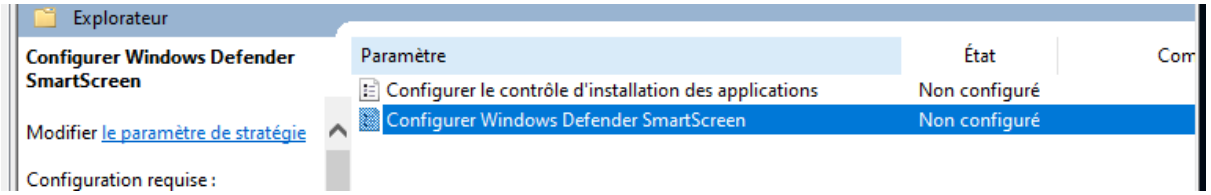
On modifie la GPO puis on se déplace dans Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows Defender SmartScreen



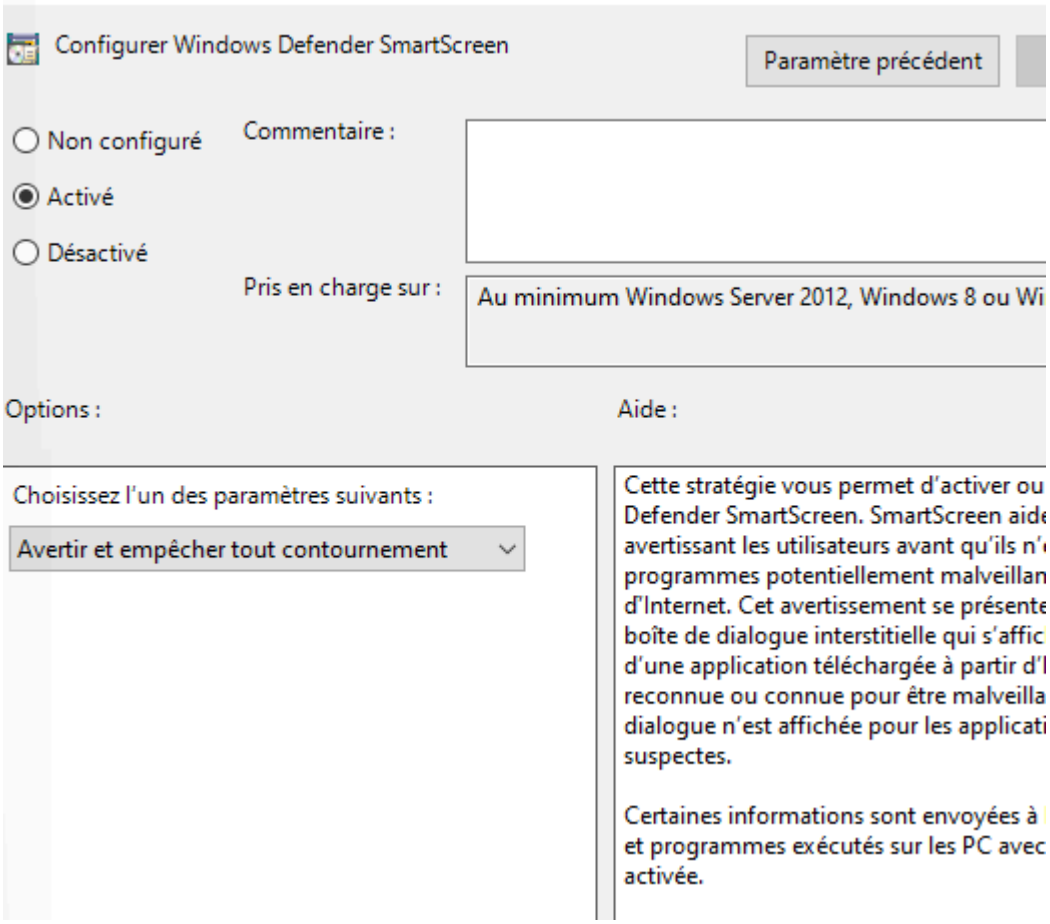
Puis on va dans Explorateur



On active le paramètre Configurer Windows Defender SmartScreen

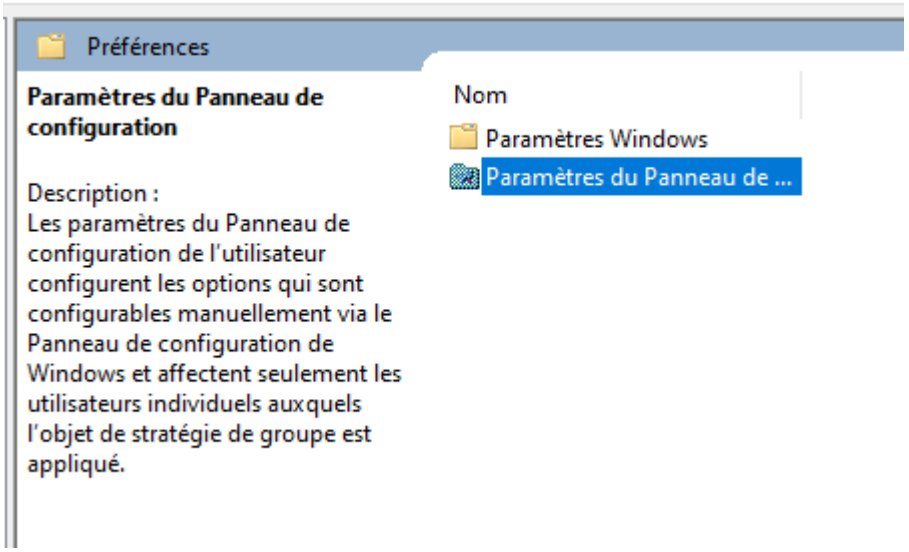


Et on active l'option Avertir et empêcher tout contournement

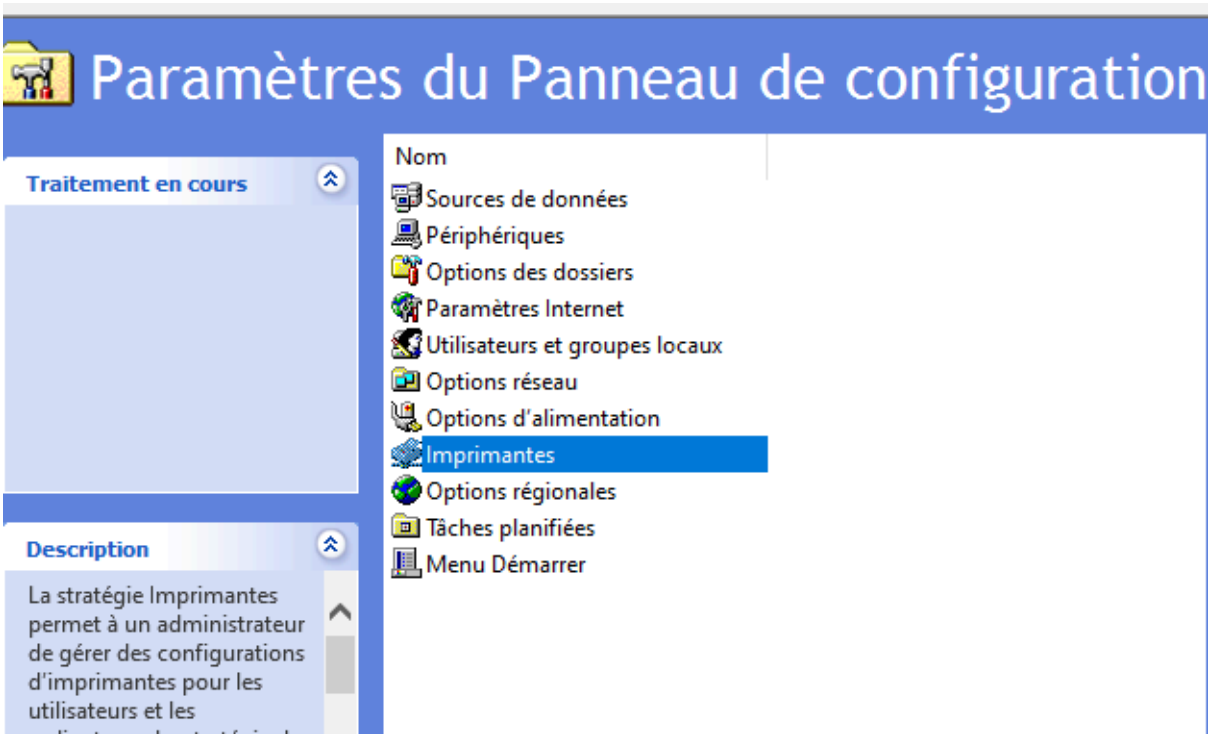


14 - UX-Printers-AutoDeploy

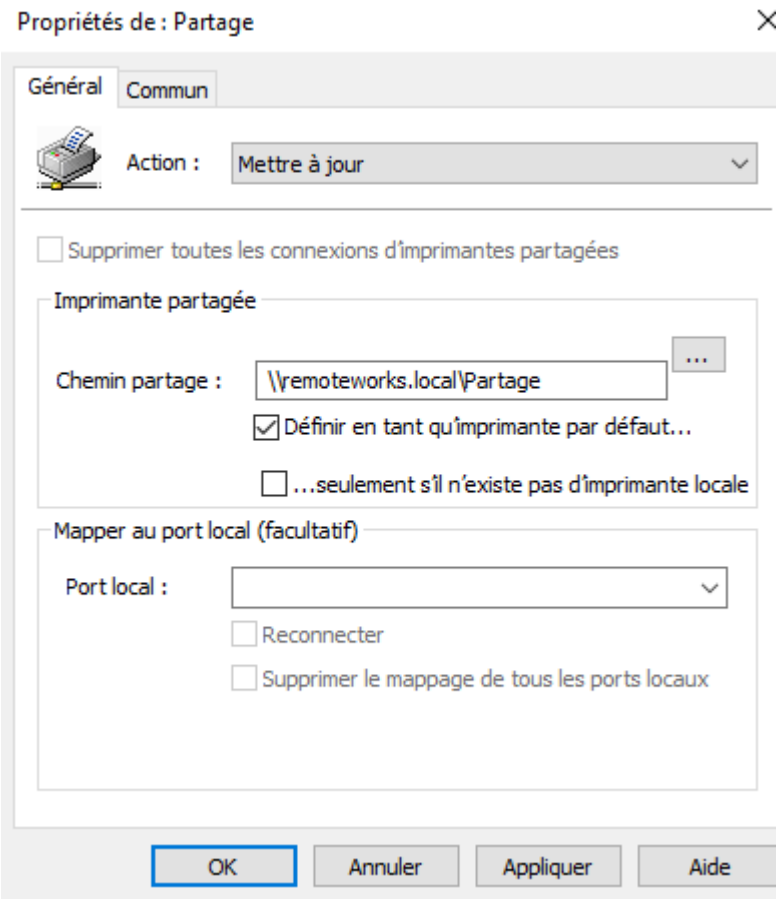
On modifie la GPO puis on se déplace dans *Configuration utilisateur > Préférences > Paramètres du Panneau de configuration*



Puis dans *Imprimantes*



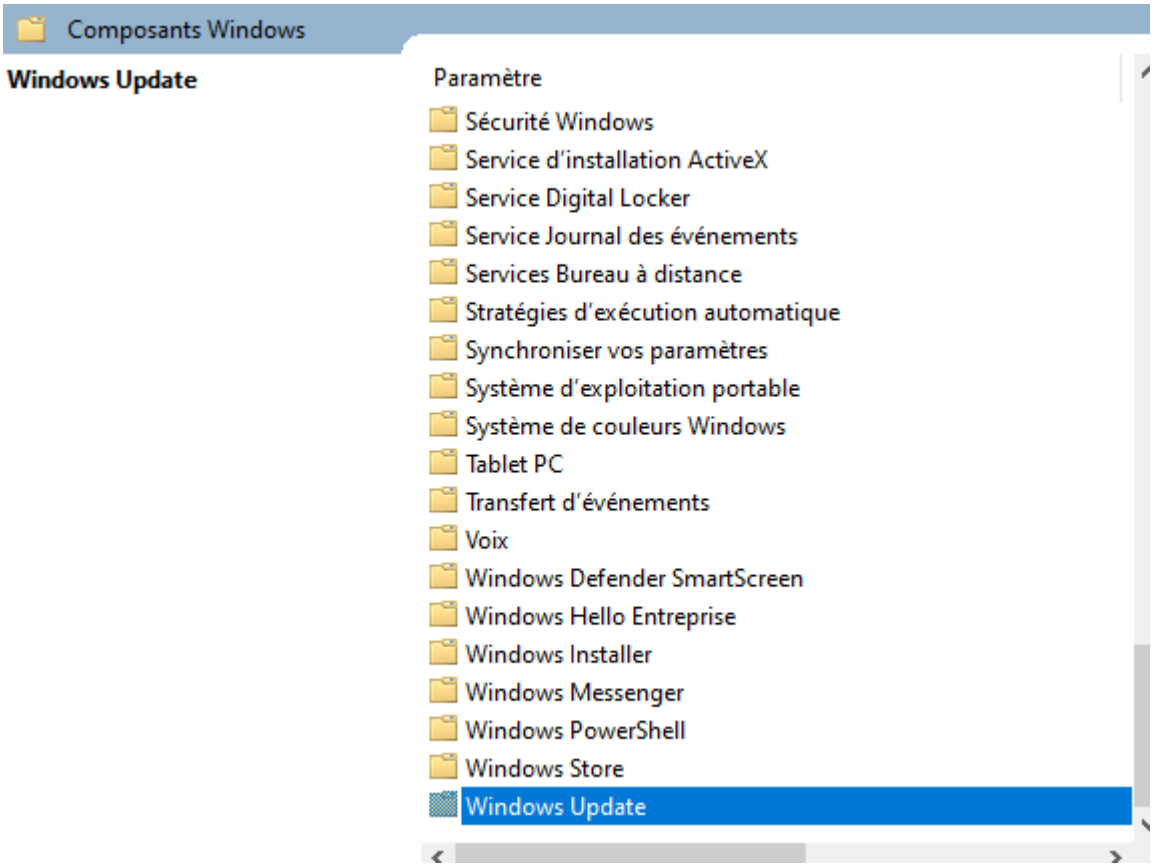
On clique droit sur Nouveau > *Imprimante Partagé*



On met l'action Mettre à jour et entre le chemin de partage de l'imprimante. On l'a définit également par défaut.

15- ADM-WSUS-Workstations

On modifie la GPO puis on se déplace dans *Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows Update*



Puis on active le paramètre Spécifier l'emplacement intranet du service de mise à jour Microsoft
Et on y entre le lien de notre serveur WSUS avec le port 8530 (port de base pour WSUS)

Installer DFS sur le serveur

Dans le Server Manager, on ouvre *Ajouter des rôles et fonctionnalités*.

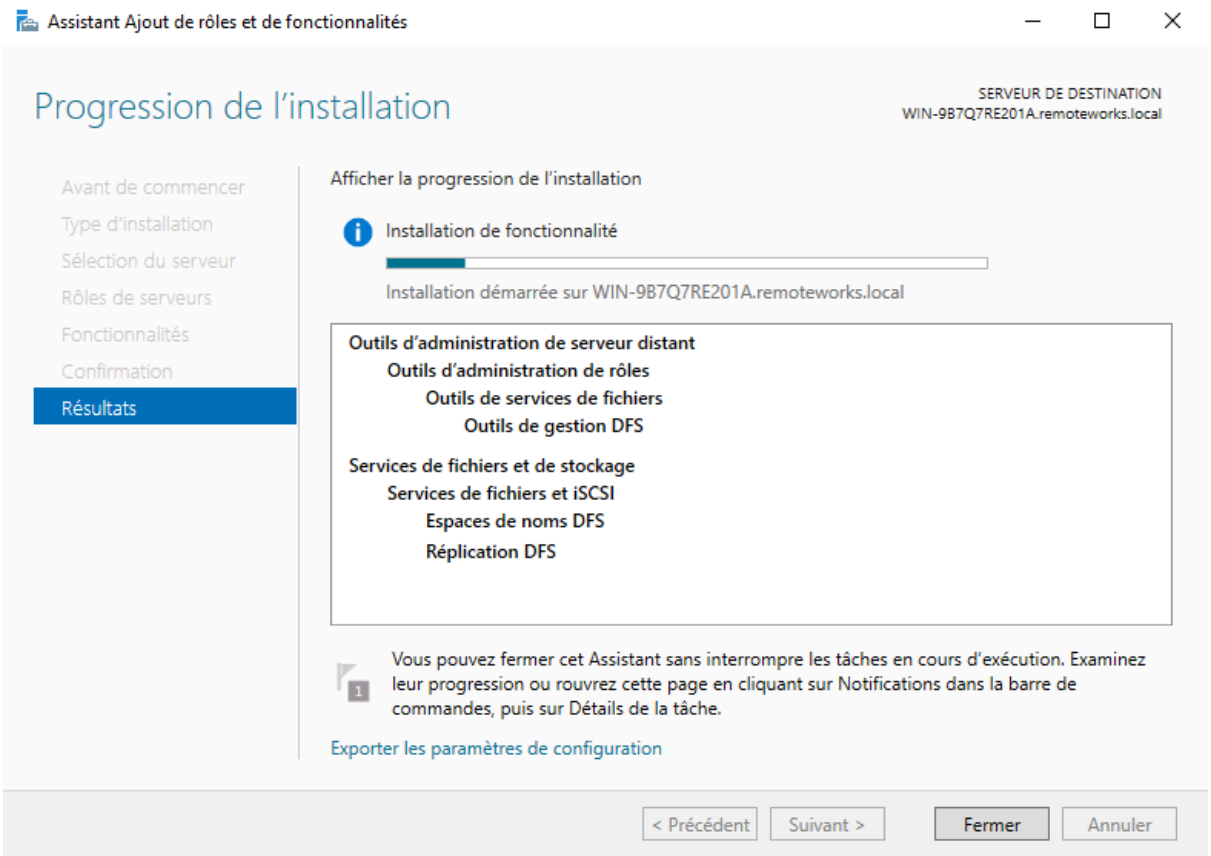
On sélectionne *Installation basée sur un rôle ou fonctionnalité*.

On coche *Services de fichiers et de stockage → Services de fichiers et iSCSI*.

Sous Services de fichiers, on coche :

- *Espaces de noms DFS*
- *Réplication DFS*
-

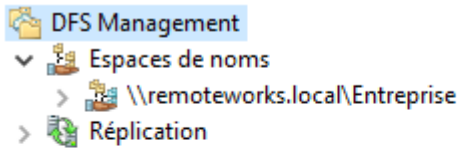
On clique sur Installer et on attend la fin de l'installation.



Créer un Namespace DFS

1. On ouvre *Gestion du système de fichier distribué DFS*
2. Clic droit sur *Espaces de noms* → *Nouvel espace de noms*.
3. On sélectionne le serveur.
4. On choisie un nom (exemple : *Entreprise*).
5. On configure les permissions :
Exemple : *Les administrateurs ont un accès total, les autres ont un accès en lecture seule*.
6. On termine l'assistant.

Résultat:



Ajouter des dossiers au Namespace

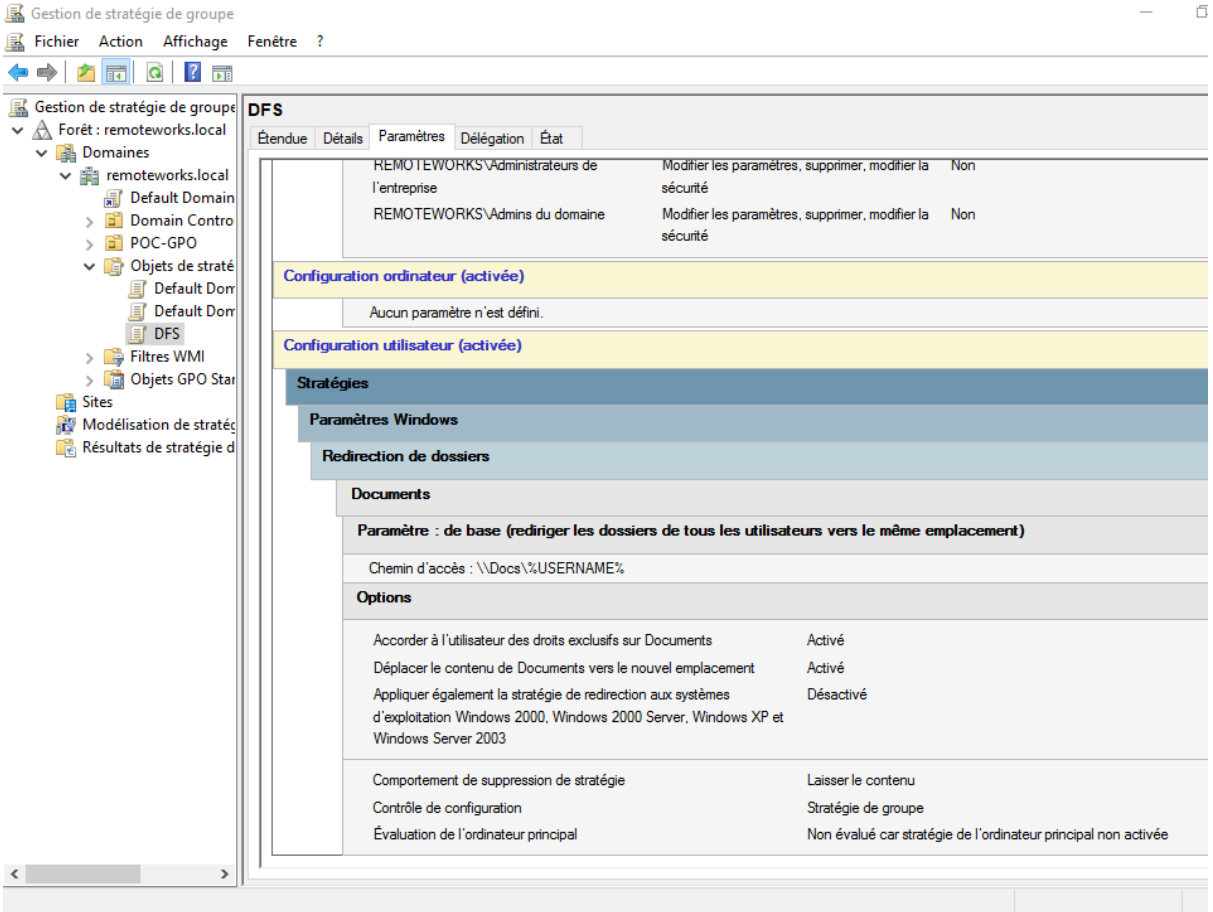
1. Dans DFS Management, on fais un clic droit sur *Espace de noms* → *Nouveau Dossier*.

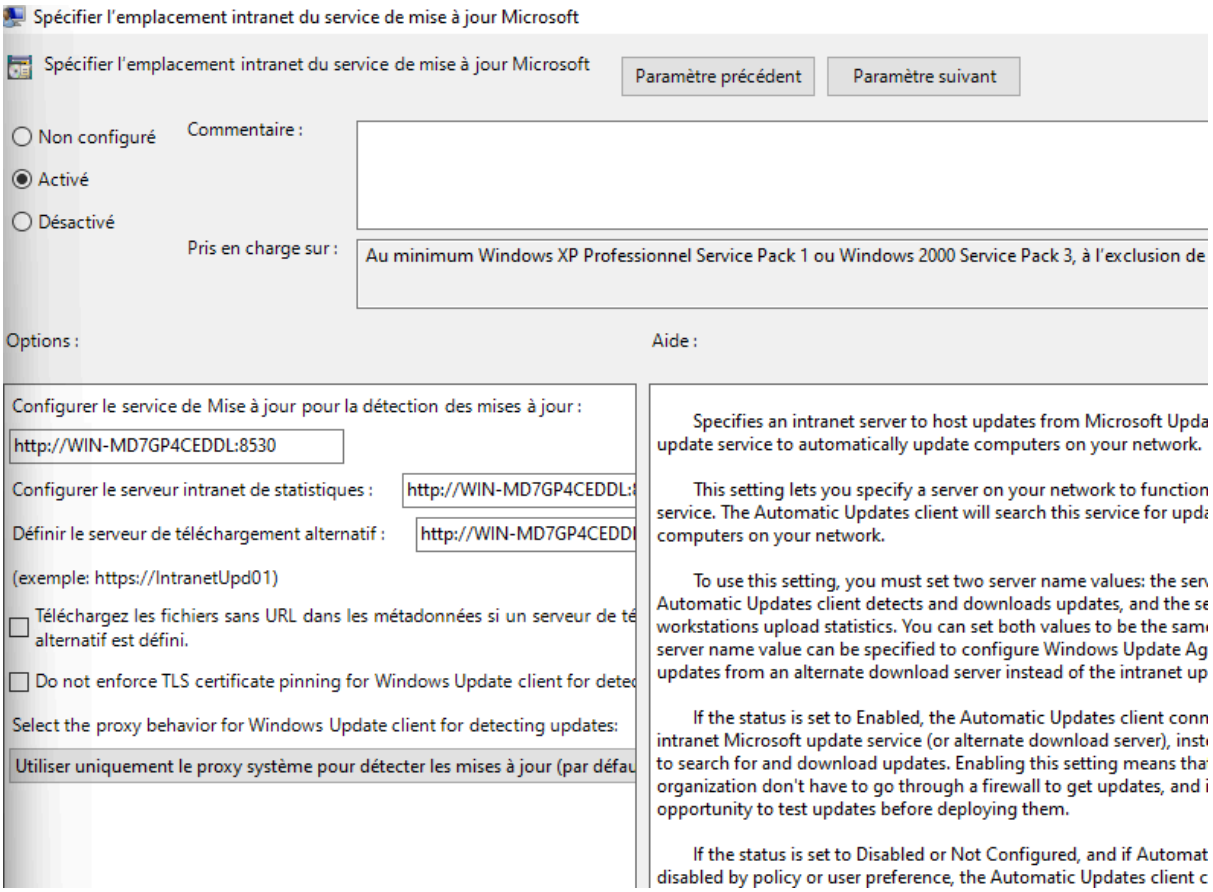
2. On donne un nom au dossier (ex : *Docs*).
3. On clique sur *OK* pour ajouter des chemins physiques (Exemple : *Serveur1**Docs* ou *Serveur2**Docs*)
4. On peut configurer la réplication DFS si on veut que les fichiers soient synchronisés entre serveurs.

Configurer la redirection de dossiers via GPO

1. Dans le Server Manager, ouvrir Gestion des stratégies de groupe.
2. On crée une nouvelle GPO.
3. On navigue vers :
Configuration Utilisateur → Stratégies → Paramètres Windows → Redirection de dossier
4. On choisit le dossier à rediriger (ex : Documents).
5. Clic droit → *Propriétés → De Base - Rediriger les dossiers de tout le monde vers le même emplacement*.
6. Dans *Emplacement du dossier cible*, on choisit *Rediriger vers l'emplacement suivant*.
7. On met le chemin DFS qu'on a créé, par exemple : *Docs*\%USERNAME%

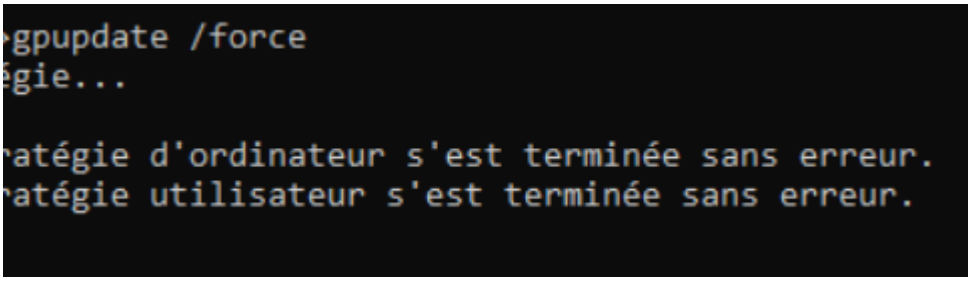
8. On applique les permissions automatiquement si nécessaire.





4. Vérifiez leur application

On se connecte à notre compte test et on ouvre l'invite de commande et on y entre successivement les 2 commandes suivantes.




```
gpresult /h C:\rapport.html
```

Une fois la deuxième commande exécutée le fichier est créé et il suffit de voir si nos GPO y sont bien appliquées.