

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_-LFwlyGi9uVIMO09R2U/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

Nouvel objet - Unité d'organisation

Créer dans : remoteworks.local/

Nom :
POC-GPO

☒ Protéger le conteneur contre une suppression accidentelle

OK Annuler Aide

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 :

Environnement Sessions Contrôle à distance Profil des services Bureau à distance COM+

Général Adresse Compte Profil Téléphones Organisation Membre de Appel entrant

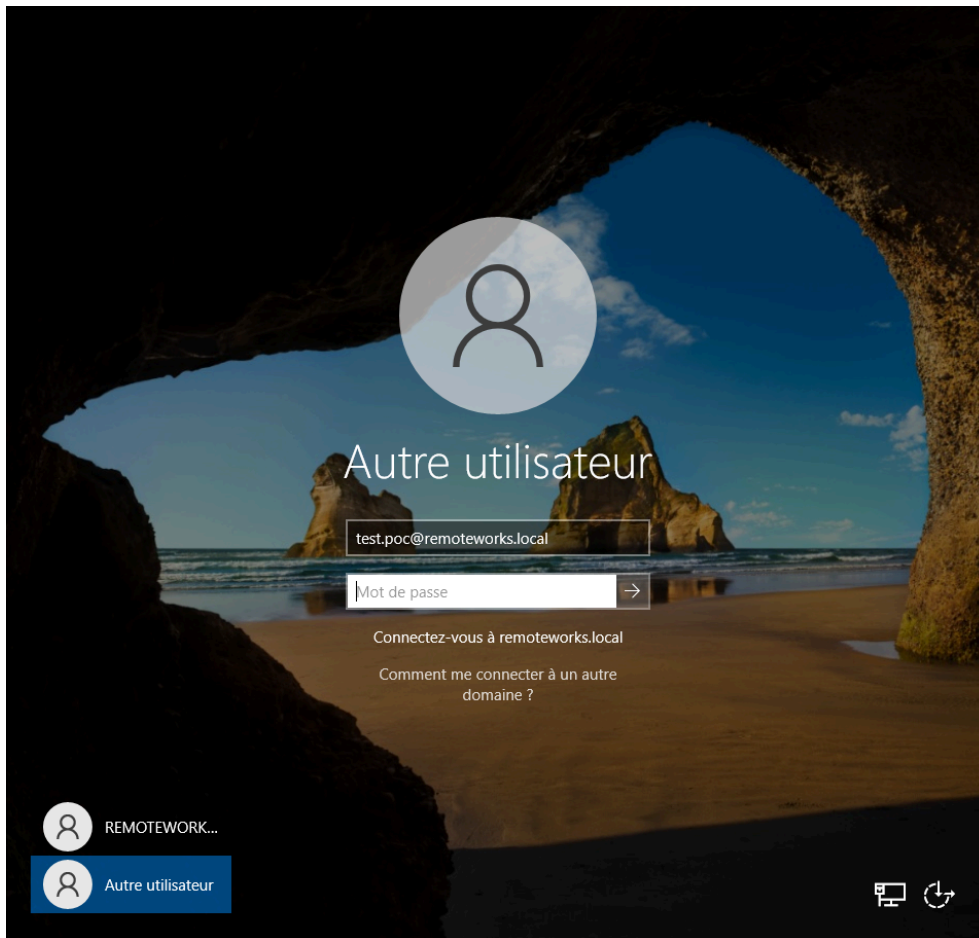
Nom d'ouverture de session de l'utilisateur :
test.poc @remoteworks.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
REMOTEWORKS\ test.poc

Horaires d'accès... Se connecter à...

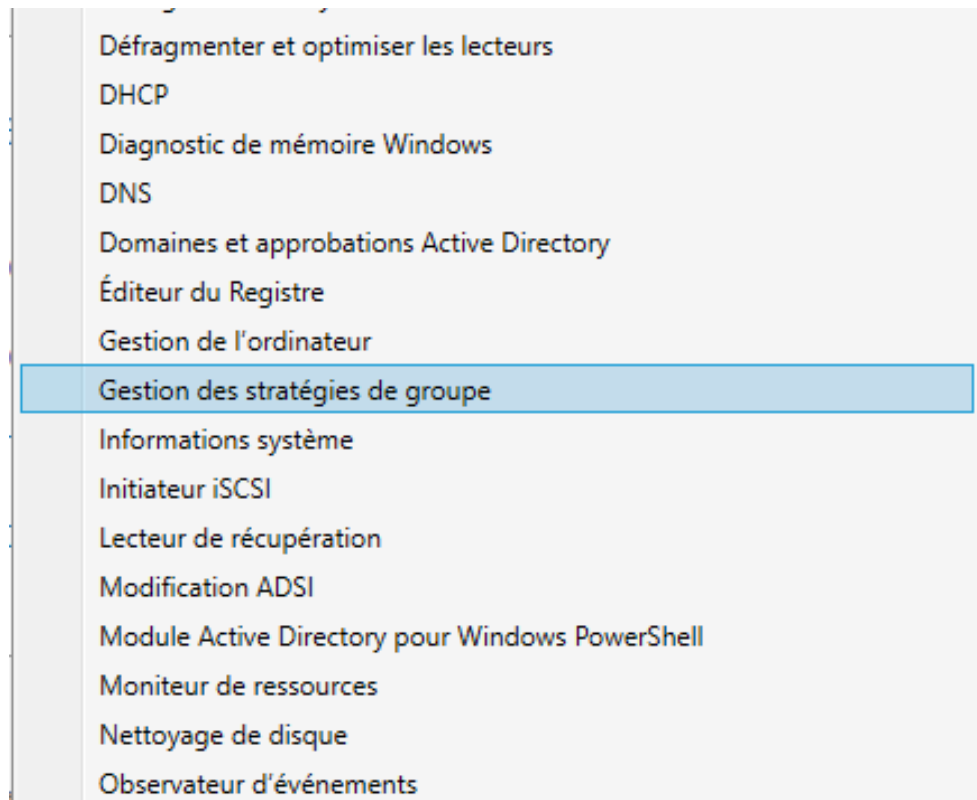
☐ Déverrouiller le compte

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 crée nos GPO :

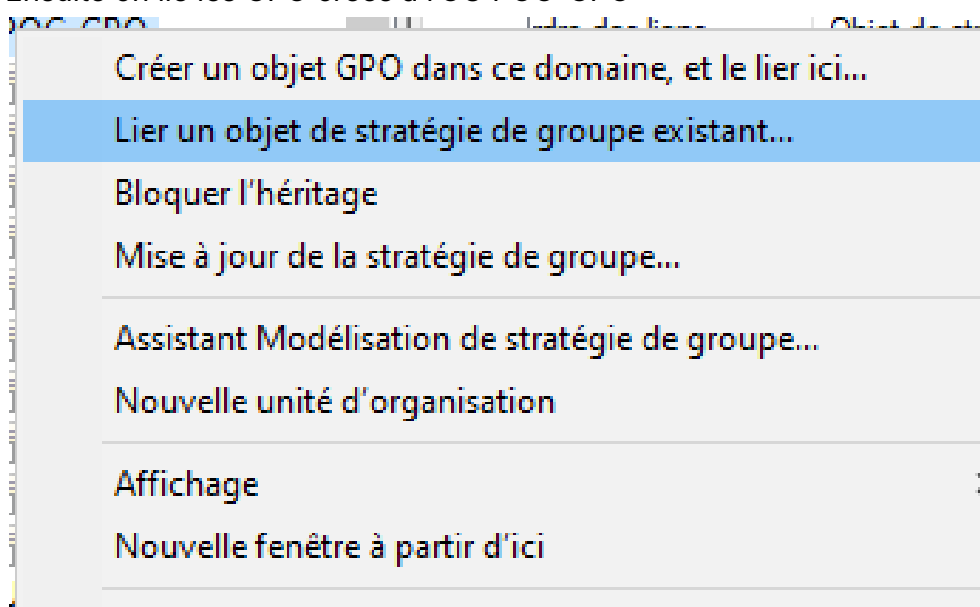
- SEC-User-NoPowerShell
- SEC-User-NoControlPanel
- SEC-Device-BlockUSB
- SEC-Session-LockedScreensaver
- SEC-User-NoCMD
- SEC-Firewall-Workstations
- APP-FirefoxESR-Hardening
- CORP-Wallpaper-BySite
- CORP-LegalBanner-Logon
- UX-StartMenu-Taskbar-Standard

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

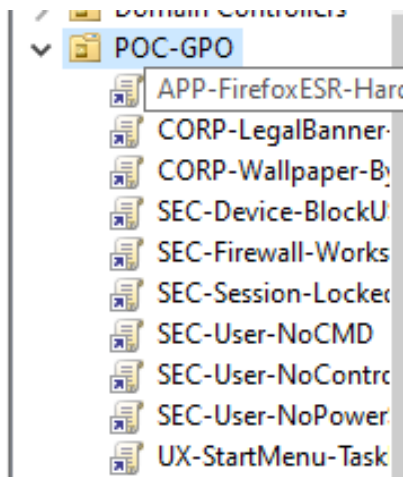
Résultat :



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



Résultat :

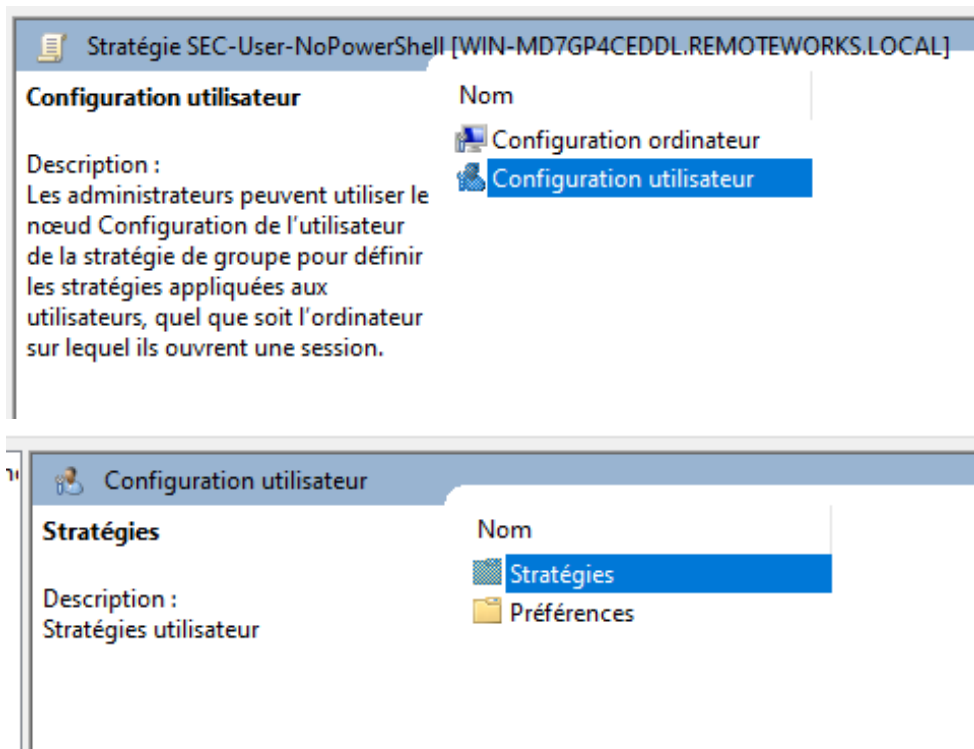


2. Configuration des GPO

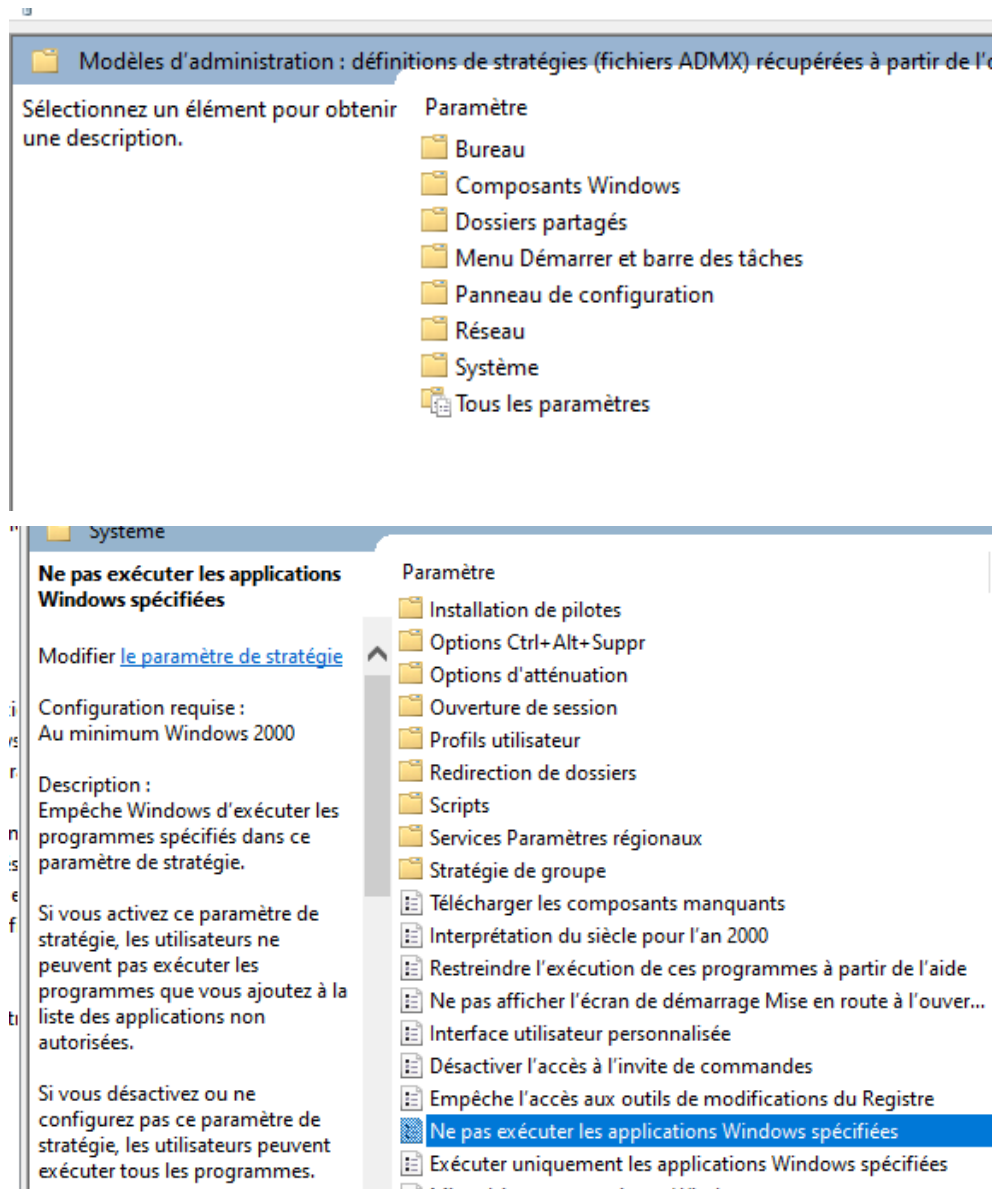
Maintenant on ajoute les règles à nos GPO créés pour qu'elles soient fonctionnelles.

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*



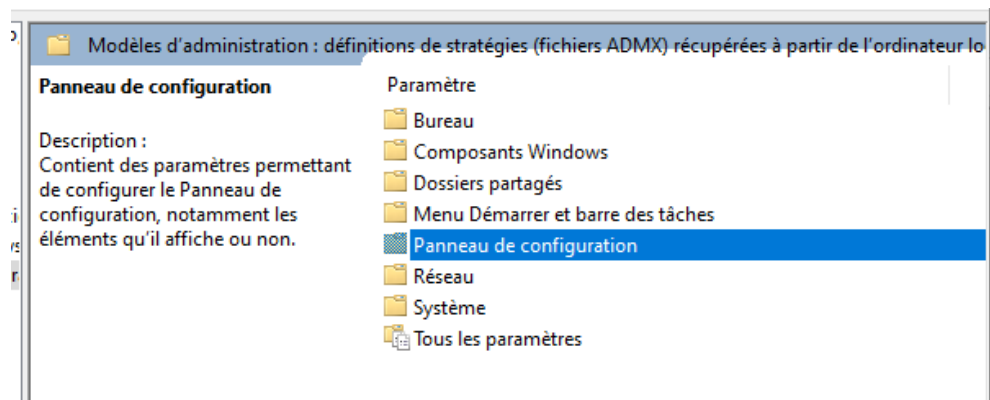
Et on y ajoute ces règles pour empêcher l'utilisation de PowerShell

Afficher le contenu

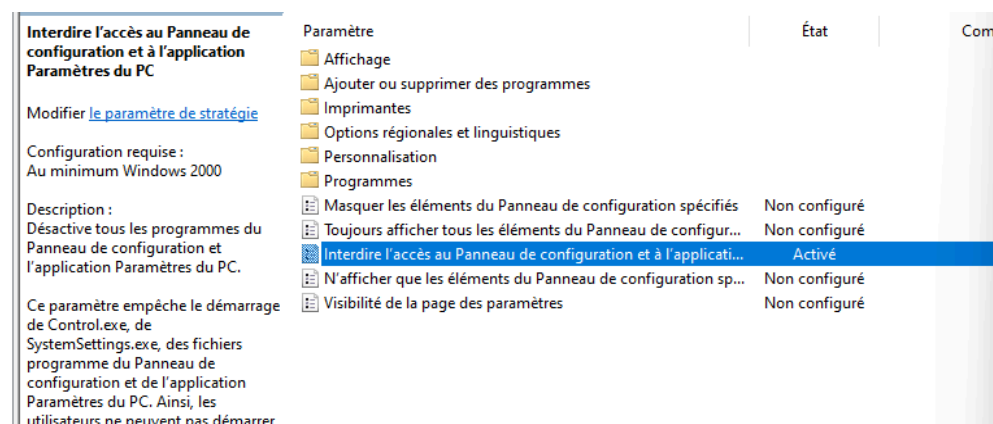
Liste des applications non autorisées	
Valeur	
powershell.exe	
pwsh.exe	
▶▶	

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*

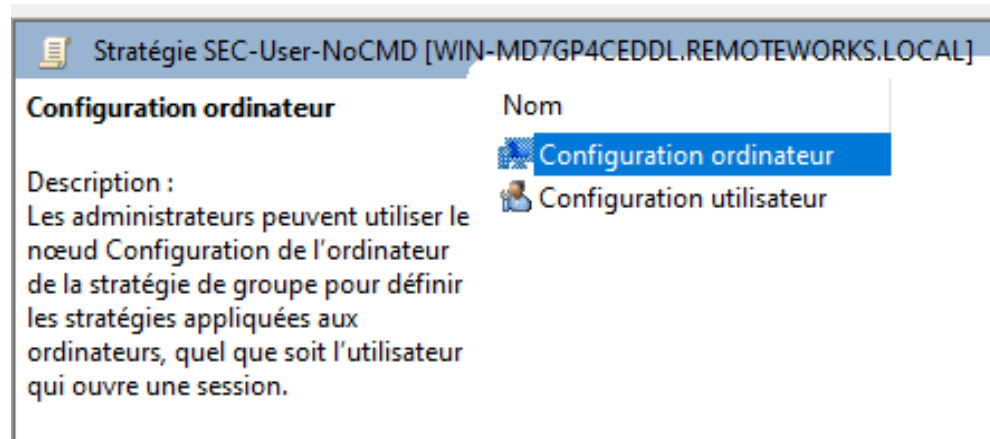


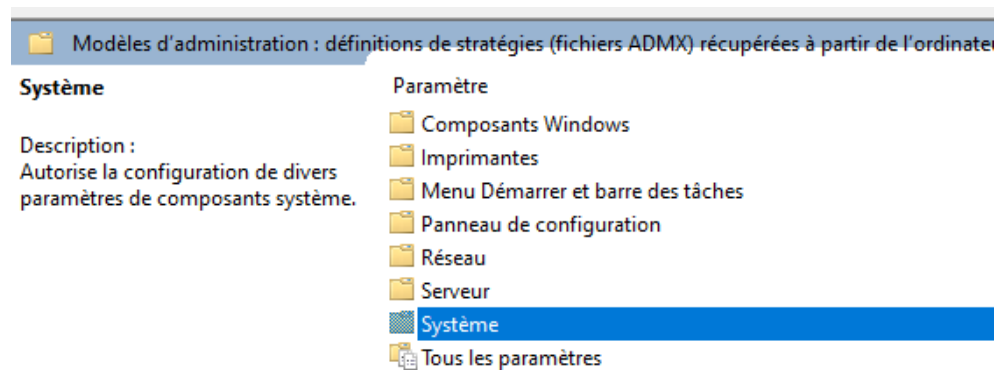
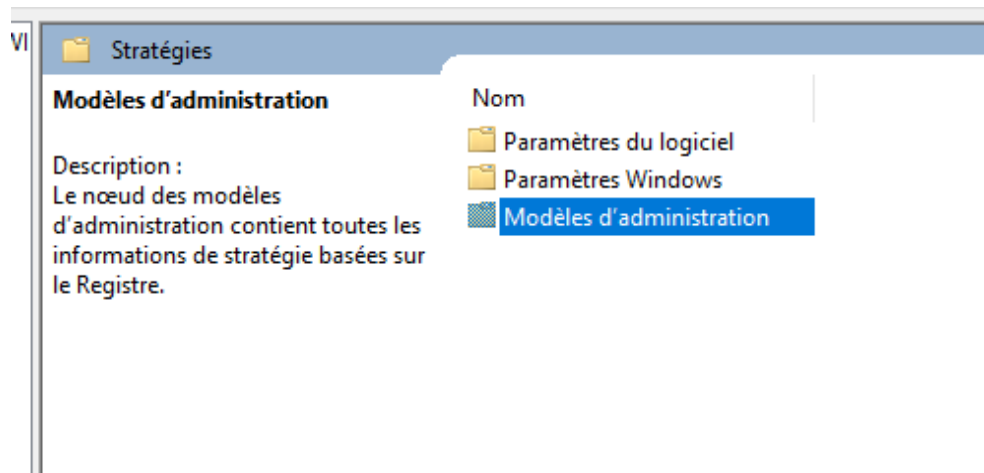
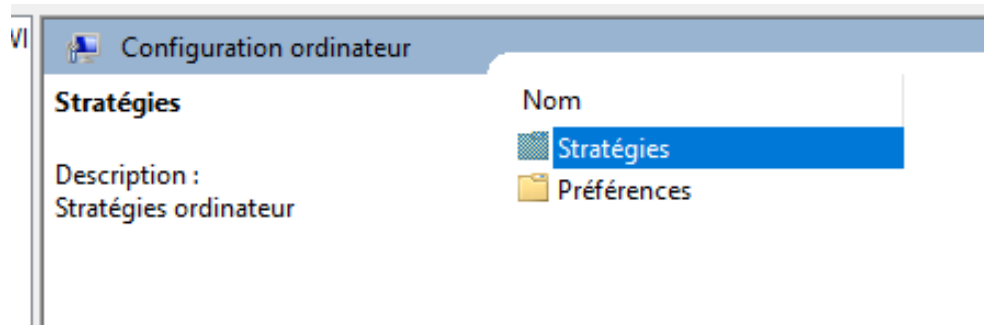
Puis on active *Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC*



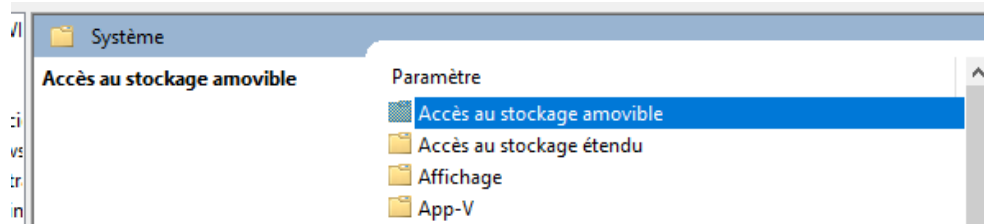
3- SEC-Device-BlockUSB

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 :

Disques amovibles : refuser l'accès en écriture	Paramètre	État	Cc
<p>Modifier le paramètre de stratégie</p> <p>Configuration requise : Au minimum Windows Vista</p> <p>Description : Ce paramètre de stratégie refuse l'accès en écriture aux disques amovibles.</p> <p>Si vous activez ce paramètre de stratégie, l'accès en écriture est refusé à cette classe de stockage amovible.</p> <p>Si vous désactivez ce paramètre de stratégie ou ne le configurez pas, l'accès en écriture est autorisé pour cette classe de stockage amovible.</p> <p>Remarque : pour exiger que les utilisateurs écrivent des données sur les disques de stockage protégés par BitLocker, activez le paramètre de stratégie « Refuser l'accès en écriture</p>	Définir le délai (en secondes) avant de forcer le redémarrage	Non configuré	
	CD et DVD : refuser l'accès en exécution	Non configuré	
	CD et DVD : refuser l'accès en lecture	Non configuré	
	CD et DVD : refuser l'accès en écriture	Non configuré	
	Classes personnalisées : refuser l'accès en lecture	Non configuré	
	Classes personnalisées : refuser l'accès en écriture	Non configuré	
	Lecteurs de disquettes : refuser l'accès en exécution	Non configuré	
	Lecteurs de disquettes : refuser l'accès en lecture	Non configuré	
	Lecteurs de disquettes : refuser l'accès en écriture	Non configuré	
	Disques amovibles : refuser l'accès en exécution	Non configuré	
	Disques amovibles : refuser l'accès en lecture	Activé	
	Disques amovibles : refuser l'accès en écriture	Activé	
	Toutes les classes de stockage amovible : refuser tous les acc...	Non configuré	
	Tout stockage amovible : permet l'accès direct pendant des ...	Non configuré	
	Lecteurs de bandes : refuser l'accès en exécution	Non configuré	
	Lecteurs de bandes : refuser l'accès en lecture	Non configuré	
	Lecteurs de bandes : refuser l'accès en écriture	Non configuré	
	Périphériques WPD : refuser l'accès en lecture	Non configuré	
	Périphériques WPD : refuser l'accès en écriture	Non configuré	

4- SEC-Session-LockedScreensaver

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

Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur	Paramètre
<p>Panneau de configuration</p> <p>Description : Contient des paramètres permettant de configurer le Panneau de configuration, notamment les éléments qu'il affiche ou non.</p>	Bureau
	Composants Windows
	Dossiers partagés
	Menu Démarrer et barre des tâches
	Panneau de configuration
	Réseau
	Système
	Tous les paramètres

Puis dans *Personnalisation*

Paramètre	État	Comr
Affichage		
Ajouter ou supprimer des programmes		
Imprimantes		
Options régionales et linguistiques		
Personnalisation		
Programmes		
Masquer les éléments du Panneau de configuration spécifiés	Non configuré	
Toujours afficher tous les éléments du Panneau de configur...	Non configuré	
Interdire l'accès au Panneau de configuration et à l'applicati...	Non configuré	
N'afficher que les éléments du Panneau de configuration sp...	Non configuré	
Visibilité de la page des paramètres	Non configuré	

















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 :

Paramètre	État	Cor
 Empêcher de modifier le modèle de couleurs	Non configuré	
 Empêcher de modifier le thème	Non configuré	
 Empêcher de modifier le style visuel des fenêtres et des bout...	Non configuré	
 Activer l'écran de veille	Activé	
 Empêcher la sélection de la taille de police du style visuel	Non configuré	
 Empêcher de modifier la couleur et l'apparence	Non configuré	
 Empêcher de modifier l'arrière-plan du Bureau	Non configuré	
 Empêcher de modifier les icônes du Bureau	Non configuré	
 Empêcher de modifier les pointeurs de la souris	Non configuré	
 Empêcher de modifier l'écran de veille	Non configuré	
 Empêcher de modifier les sons	Non configuré	
 Un mot de passe protège l'écran de veille	Activé	
 Dépassement du délai d'expiration de l'écran de veille	Activé	
 Forcer un écran de veille spécifique	Non configuré	
 Charger un thème spécifique	Non configuré	
 Forcer un fichier de style visuel spécifique ou forcer le style ...	Non configuré	

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\SYSTEM\remoteworks.local\Policies`

Si il y a déjà un dossier PolicyDefinitions il faut se rendre dedans sinon il faut le créer.














↑

« SYSVOL » remoteworks.local » Policies

▼

↺

Rechercher dans : Policies 🔍

	Nom	Modifié le	Type	Taille
<div>pide</div> <div>➤</div> <div>irgements: ➤</div> <div>ients ➤</div> <div>➤</div>	 {0EA3A554-89B5-4ED1-B36B-2906AC0D7...	04/12/2025 15:23	Dossier de fichiers	
	 {6AC1786C-016F-11D2-945F-00C04FB984...	02/12/2025 14:14	Dossier de fichiers	
	 {31B2F340-016D-11D2-945F-00C04FB984...	02/12/2025 14:14	Dossier de fichiers	2
	 {66B0DFC1-71A1-4ECB-9E97-EB0D37EB5...	04/12/2025 15:24	Dossier de fichiers	
	 {88F43E0F-6604-4887-899F-0C6B51999352}	04/12/2025 15:24	Dossier de fichiers	
	 {359F0E5D-E4A3-4DAF-B235-4A9BC4D8C...	04/12/2025 15:23	Dossier de fichiers	
	 {849CB941-98ED-4AD4-8365-29AEC2155F...	04/12/2025 15:24	Dossier de fichiers	
	 {6656A897-BF7D-4A8F-B936-B8C1BF271B...	04/12/2025 15:25	Dossier de fichiers	
	 {71697F84-AEB0-4045-99B5-E965EFD953...	04/12/2025 15:24	Dossier de fichiers	
	 {ADE98069-CEAD-40B2-8DBC-C68DDA46...	04/12/2025 15:25	Dossier de fichiers	
	 {BF4C3BFA-F199-4023-B1FE-14016C07A8...	04/12/2025 15:24	Dossier de fichiers	
	 {D3E9793A-56DC-477F-893D-2DD654BF8...	04/12/2025 15:23	Dossier de fichiers	
	 PolicyDefinitions	12/12/2025 09:51	Dossier de fichiers	

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

«

remoteworks.local

>

Policies

>

PolicyDefinitions

▼

↺

Rechercher dans : PolicyDefin... 🔍

	Nom	Modifié le	Type	Taille
<div><div><div>📁</div><div>fr-FR</div></div><div><div>📄</div><div>firefox.admx</div></div><div><div>📄</div><div>mozilla.admx</div></div></div>	fr-FR	12/12/2025 09:55	Dossier de fichiers	
	firefox.admx	12/12/2025 09:45	Fichier ADMX	237 Ko
	mozilla.admx	12/12/2025 09:45	Fichier ADMX	1 Ko

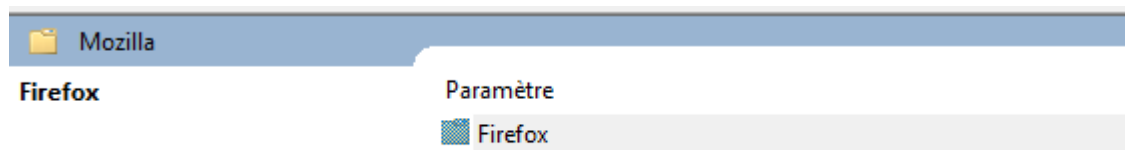
Ensuite on doit également y copier les fichier ADMX et ADML de Windows, pour se faire on suit le chemin C:\\Windows\\PolicyDefinitions et on copie l'intégralité des fichiers dans
 \\remoteworks.local\\SYSVOL\\remoteworks.local\\Policies\\PolicyDefinitions

<< Disque local (C:) > Windows > PolicyDefinitions					Rechercher dans : PolicyDefin...
	Nom	Modifié le	Type	Taille	
ide	en-US	08/05/2021 17:49	Dossier de fichiers		
	fr-FR	03/03/2022 04:50	Dossier de fichiers		
gements	ActiveXInstallService.admx	08/05/2021 10:15	Fichier ADMX	5	
nts	AddRemovePrograms.admx	08/05/2021 10:15	Fichier ADMX	5	
	AllowBuildPreview.admx	08/05/2021 10:15	Fichier ADMX	2	
definitions	AppCompat.admx	08/05/2021 10:15	Fichier ADMX	6	
	AppPrivacy.admx	08/05/2021 10:14	Fichier ADMX	35	
	appv.admx	08/05/2021 17:53	Fichier ADMX	35	
	AppxPackageManager.admx	08/05/2021 10:15	Fichier ADMX	6	
	AppXRuntime.admx	08/05/2021 10:15	Fichier ADMX	4	
	AttachmentManager.admx	08/05/2021 10:15	Fichier ADMX	6	
	AuditSettings.admx	08/05/2021 10:15	Fichier ADMX	2	
	AutoPlay.admx	08/05/2021 10:15	Fichier ADMX	4	
	AVSValidationGP.admx	08/05/2021 10:14	Fichier ADMX	3	
	Biometrics.admx	08/05/2021 10:15	Fichier ADMX	4	
	Bits.admx	08/05/2021 10:15	Fichier ADMX	56	
	Camera.admx	08/05/2021 10:15	Fichier ADMX	3	
	CEIPEnable.admx	08/05/2021 10:15	Fichier ADMX	2	
	CipherSuiteOrder.admx	08/05/2021 10:15	Fichier ADMX	2	
	CloudContent.admx	08/05/2021 10:15	Fichier ADMX	7	
	COM.admx	08/05/2021 10:15	Fichier ADMX	2	

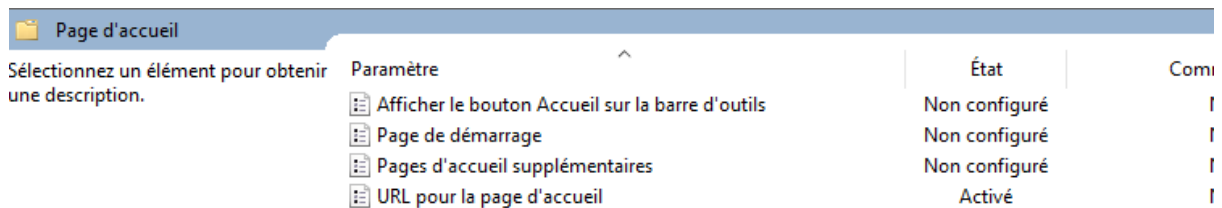
On modifie la GPO puis on se déplace dans *Configuration utilisateur > Stratégies > Modèles d'administration > Mozilla*

Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir du magasin centr	
Mozilla	Paramètre
	Composants Windows
	Imprimantes
	Menu Démarrer et barre des tâches
	Mozilla
	Panneau de configuration
	Réseau
	Serveur
	Système
	Tous les paramètres

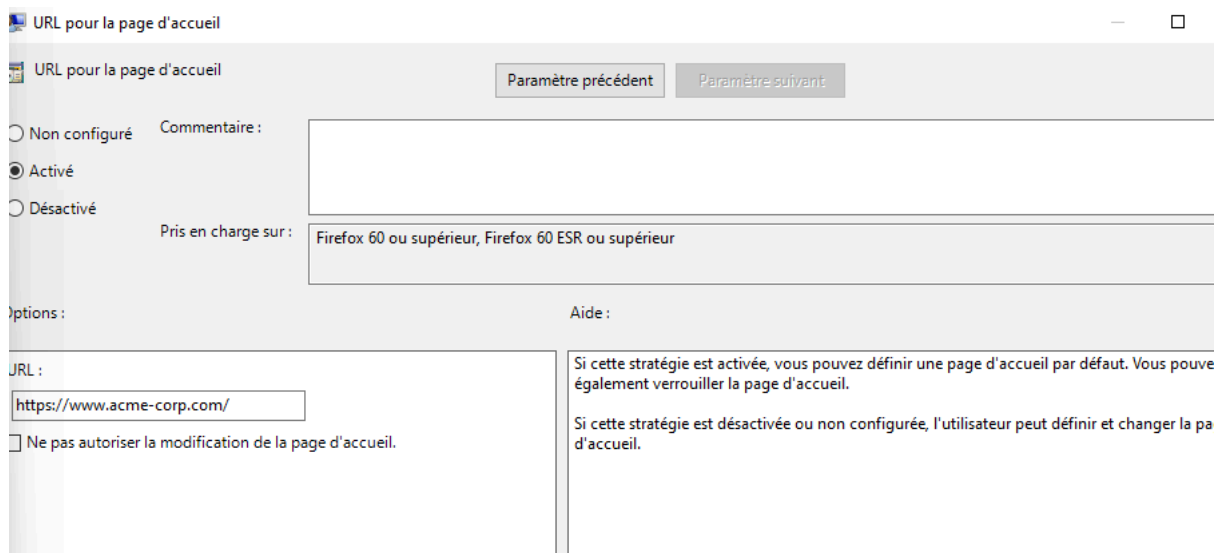
Puis Firefox



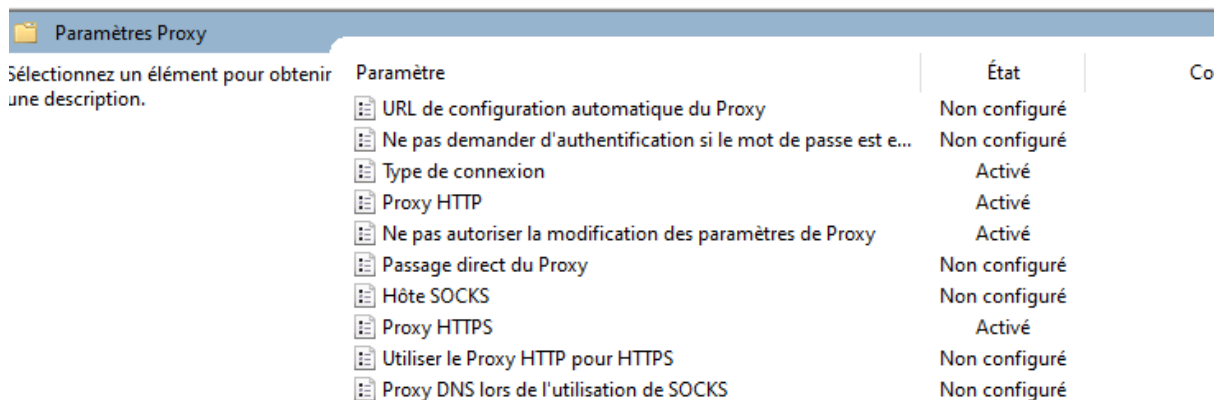
On va dans le dossier Page d'accueil et on active le paramètre URL pour la page d'accueil



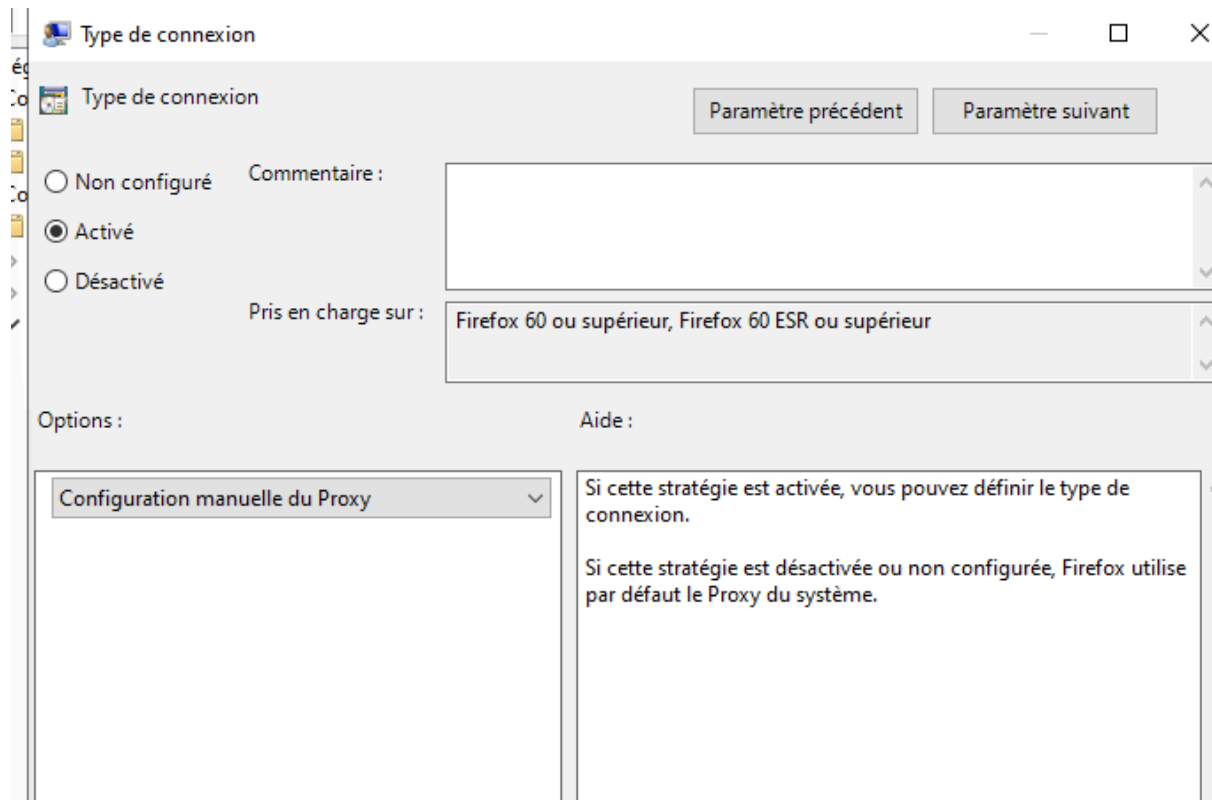
Et on y entre le lien du site web de l'entreprise



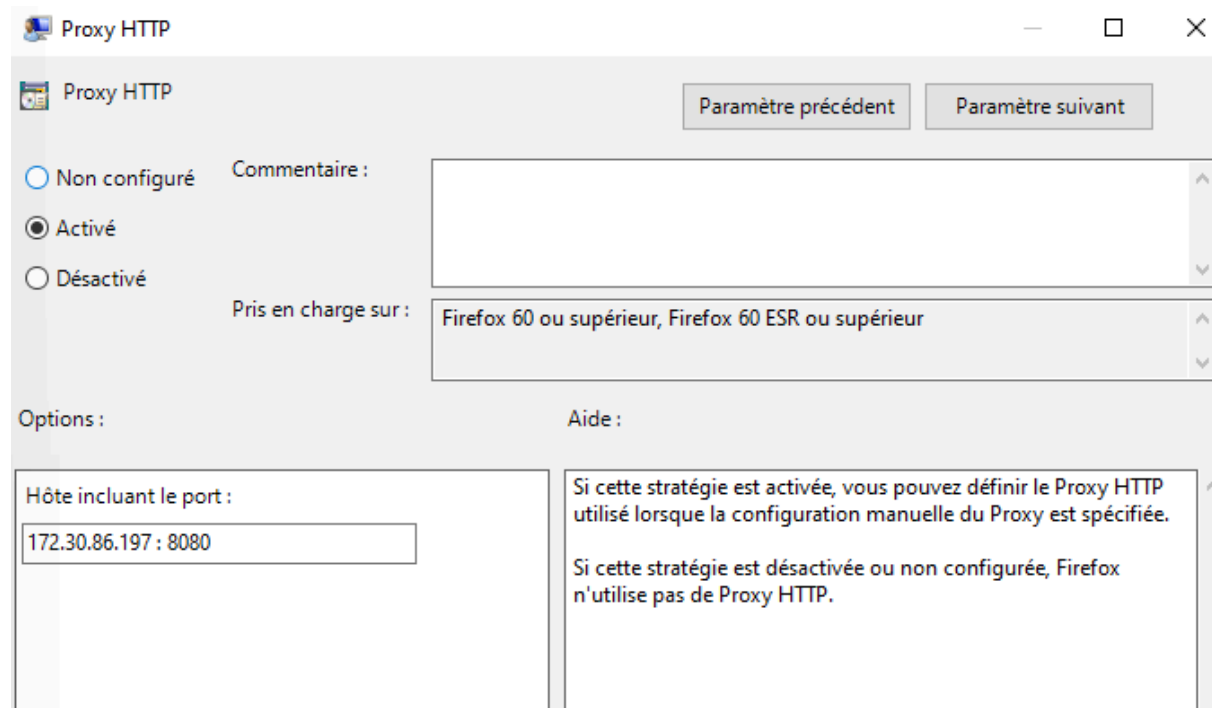
Ensuite on va dans les Paramètres Proxy



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

Extensions			
Sélectionnez un élément pour obtenir une description.	Paramètre	État	Com
	Gestion des extensions	Activé	
	Gestion des extensions (JSON sur une seule ligne)	Non configuré	
	Mise à jour des extensions	Non configuré	
	Extensions à installer	Activé	
	Empêcher les extensions d'être désactivées ou supprimées	Activé	
	Extensions à désinstaller	Non configuré	

6-SEC-User-NoCMD

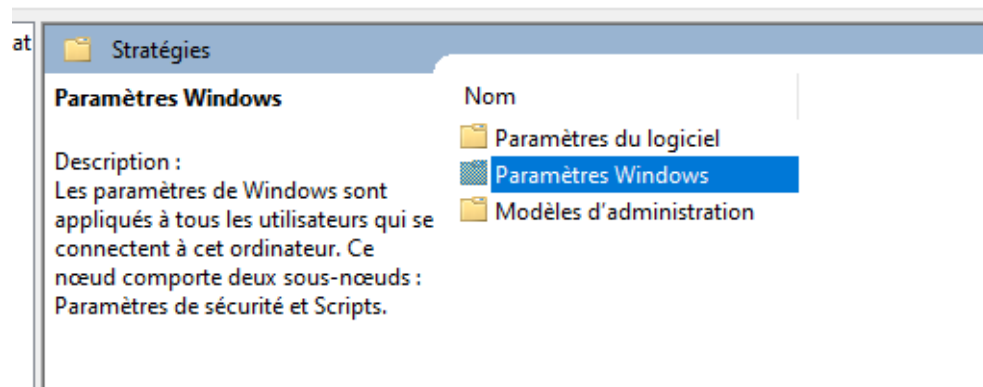
On modifie la GPO puis on se déplace dans Configuration utilisateur > Stratégies > Modèles d'administration > Système

On active l'option Désactiver l'accès à l'invite de commandes

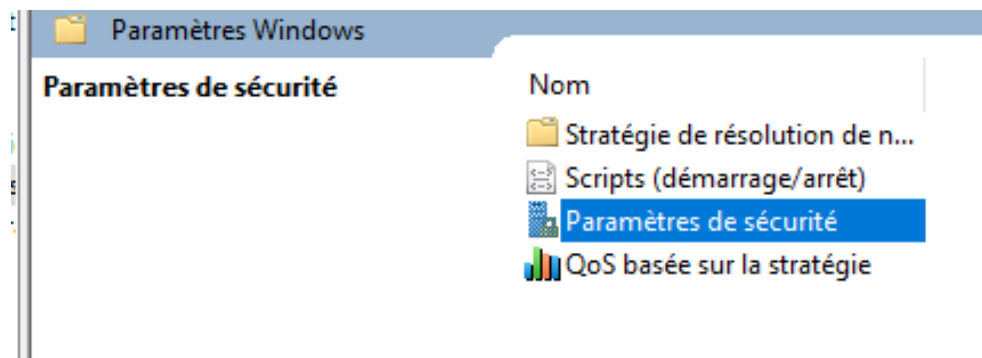
Système		
Désactiver l'accès à l'invite de commandes Modifier le paramètre de stratégie Configuration requise : Au minimum Windows 2000 Description : Ce paramètre de stratégie empêche les utilisateurs d'exécuter l'invite de commandes interactive, Cmd.exe. Ce paramètre de stratégie indique également s'il est permis d'exécuter ou non les fichiers de commandes (.cmd et .bat) sur l'ordinateur. Si vous activez ce paramètre de stratégie et que l'utilisateur essaie d'ouvrir une fenêtre de commande, le système affiche un message signalant qu'un paramètre bloque l'action. Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les utilisateurs peuvent exécuter normalement Cmd.exe et des fichiers de commandes. Remarque : n'empêchez pas l'exécution des fichiers de commandes sur l'ordinateur si celui-	Paramètre	État
	Accès au stockage amovible	
	Affichage	
	Gestion de l'alimentation	
	Gestion de la communication Internet	
	Installation de pilotes	
	Options Ctrl+Alt+Suppr	
	Options d'atténuation	
	Ouverture de session	
	Profils utilisateur	
	Redirection de dossiers	
	Scripts	
	Services Paramètres régionaux	
	Stratégie de groupe	
	Télécharger les composants manquants	Non configuré
	Interprétation du siècle pour l'an 2000	Non configuré
	Restreindre l'exécution de ces programmes à partir de l'aide	Non configuré
	Ne pas afficher l'écran de démarrage Mise en route à l'ouver...	Non configuré
	Interface utilisateur personnalisée	Non configuré
	Désactiver l'accès à l'invite de commandes	Activé
	Empêche l'accès aux outils de modifications du Registre	Non configuré
	Ne pas exécuter les applications Windows spécifiées	Non configuré
	Exécuter uniquement les applications Windows spécifiées	Non configuré
	Mises à jour automatiques Windows	Non configuré

7- SEC-Firewall-Workstations

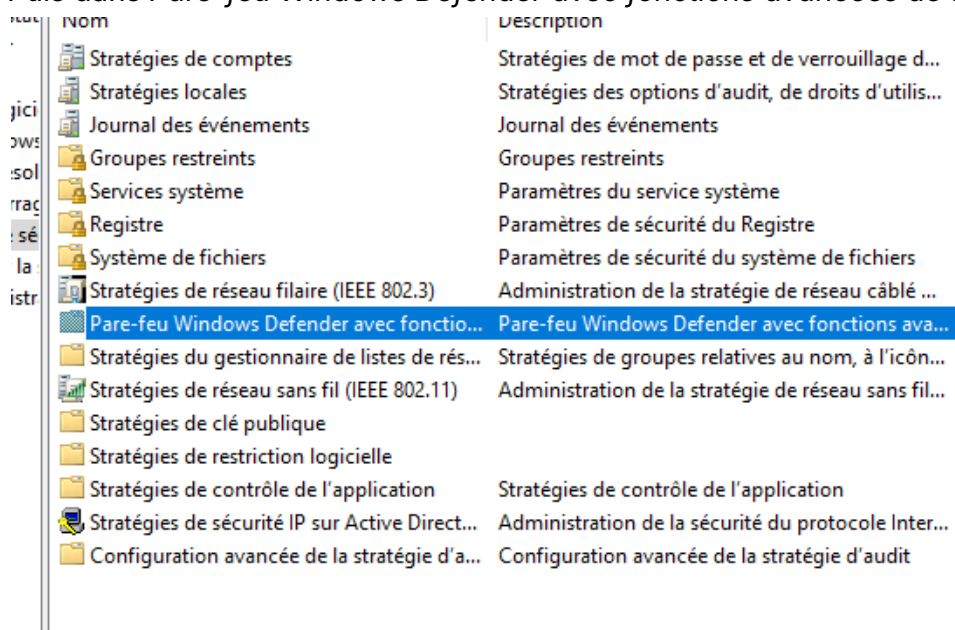
On modifie la GPO puis on se déplace dans Configuration ordinateur > Stratégies > Paramètres Windows



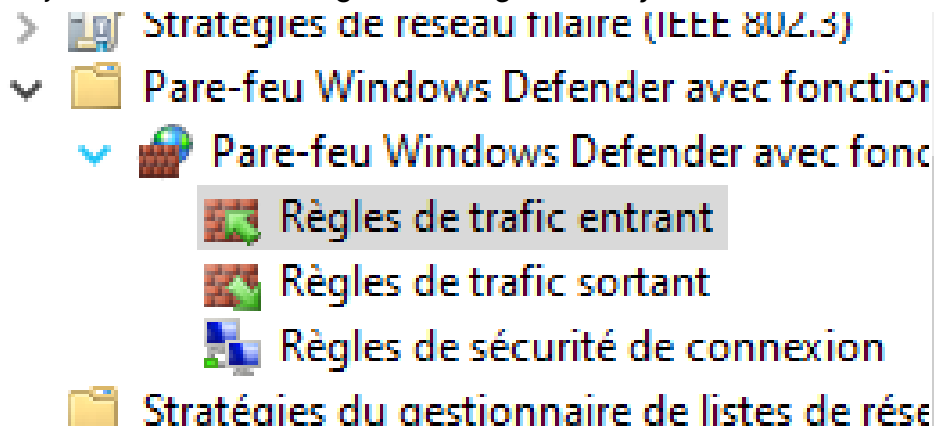
Puis dans *Paramètres de sécurité*



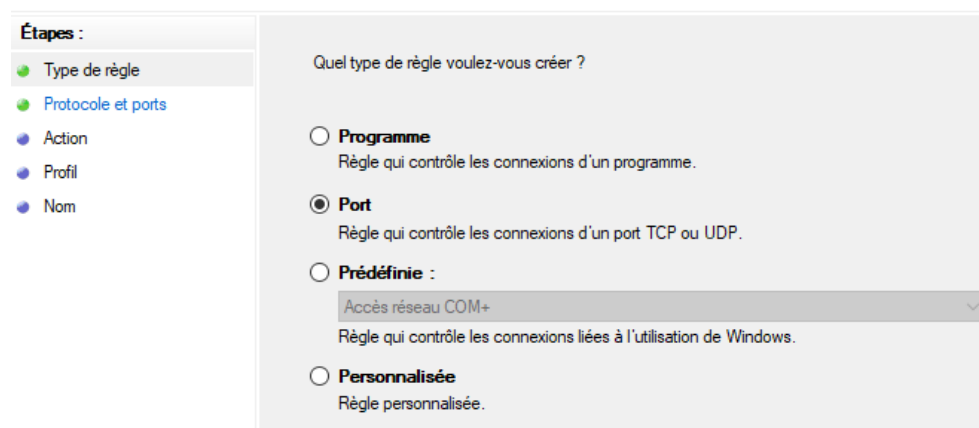
Puis dans *Pare-feu Windows Defender avec fonctions avancées de sécurité*



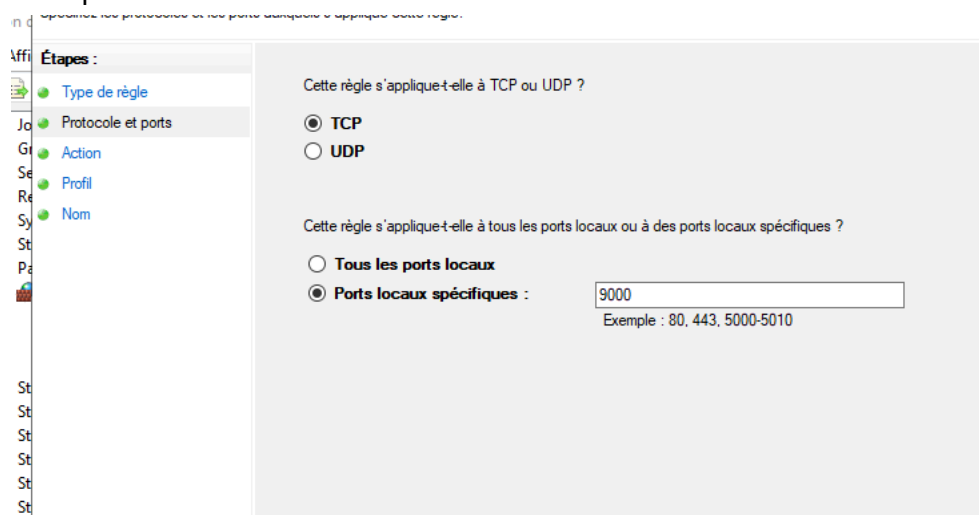
On ajoute une nouvelle règle dans *Règles de trafic entrant*



De type *Port*



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



On autorise la Connexion

Spécifiez une action à entreprendre lorsqu'une connexion répond aux conditions spécifiées dans la règle.

Étapes :

- Type de règle
- Protocole et ports
- Action**
- Profil
- Nom

Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?

☒ **Autoriser la connexion**
Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui ne le sont pas.

☐ **Autoriser la connexion si elle est sécurisée**
Cela comprend uniquement les connexions authentifiées à l'aide du protocole IPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles IPsec du nœud Règle de sécurité de connexion.

☐ **Bloquer la connexion**

Et on l'applique uniquement sur le Domaine

Appliquez les profils d'application à appliquer cette règle.

Étapes :

- Type de règle
- Protocole et ports
- Action
- Profil**
- Nom

Quand cette règle est-elle appliquée ?

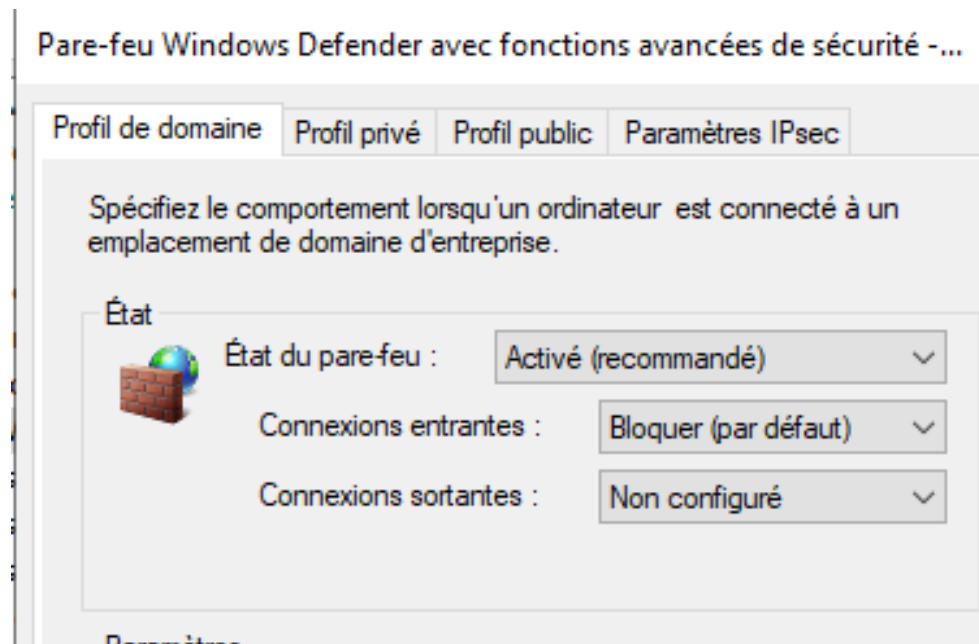
☒ **Domaine**
Lors de la connexion d'un ordinateur à son domaine d'entreprise.

☐ **Privé**
Lors de la connexion d'un ordinateur à un emplacement réseau privé, par exemple à domicile ou au bureau.

☐ **Public**
Lors de la connexion d'un ordinateur à un emplacement public.

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

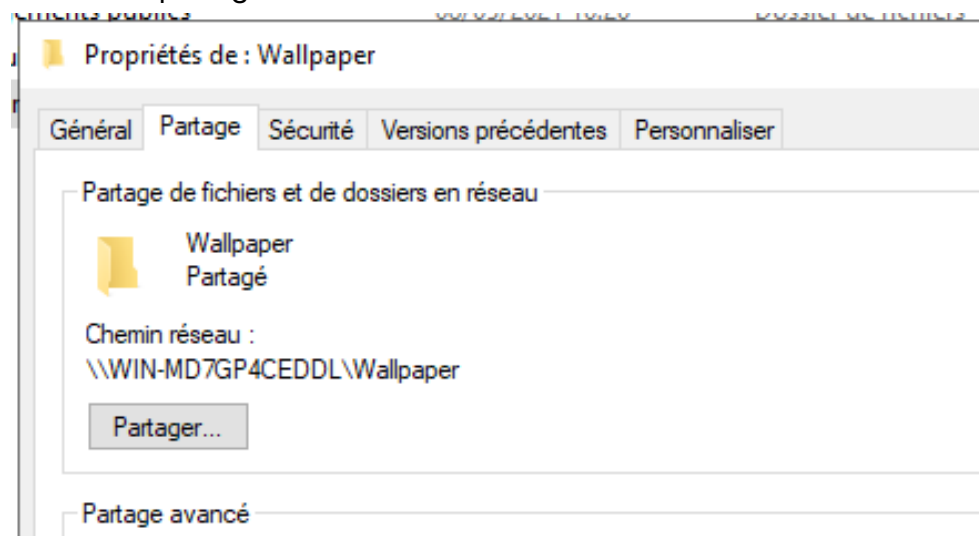


8- CORP-Wallpaper-BySite

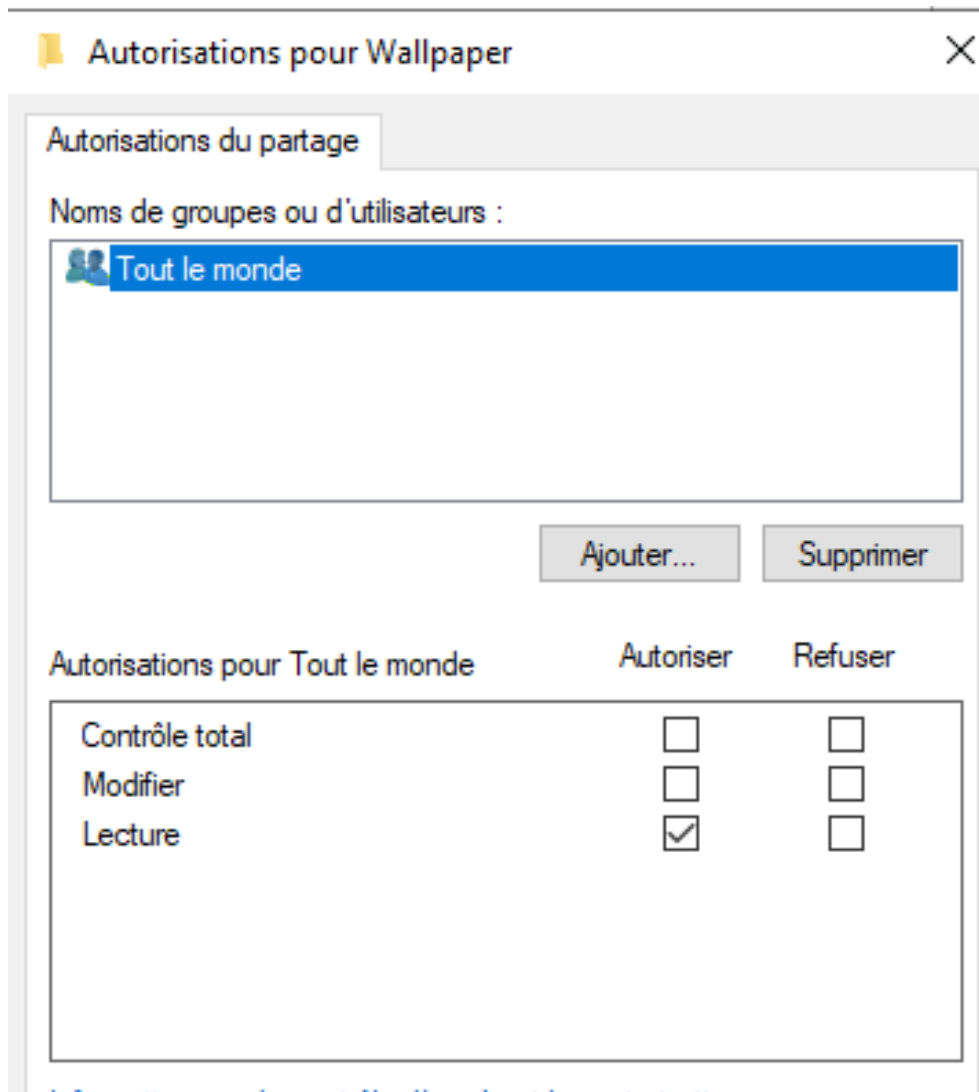
Pour appliquer un fond d'écran commun, il faut premièrement importer une image qui fera office de fond d'écran puis la mettre dans un dossier

Documents publics	27/01/2025 15:29	Dossier de fichiers
Images publiques	05/12/2025 10:44	Dossier de fichiers
Musique publique	08/05/2021 10:20	Dossier de fichiers
Téléchargements publics	08/05/2021 10:20	Dossier de fichiers
Vidéos publiques	08/05/2021 10:20	Dossier de fichiers
Wallpaper	05/12/2025 10:44	Dossier de fichiers

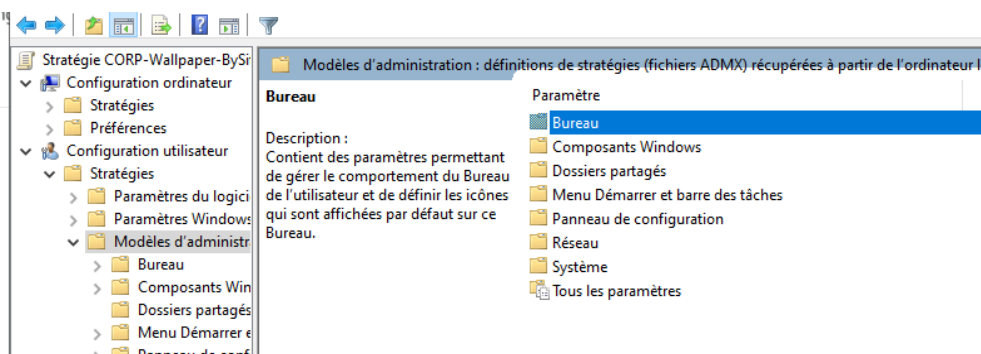
On le rend partageable :



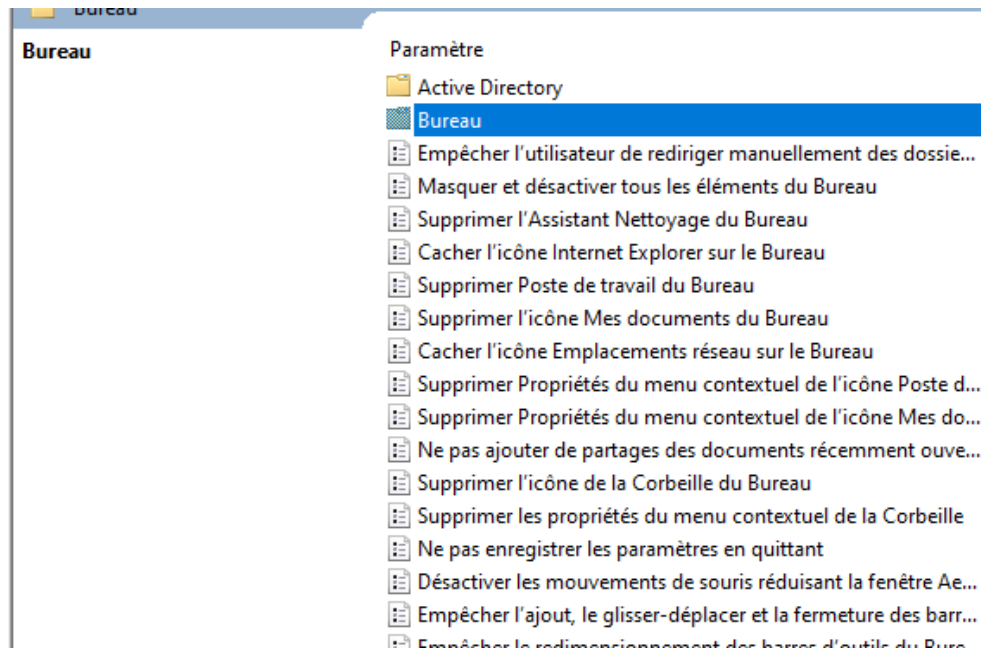
Et dans les paramètres du partage, bien vérifier que tout le monde à l'autorisation de lecture.



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



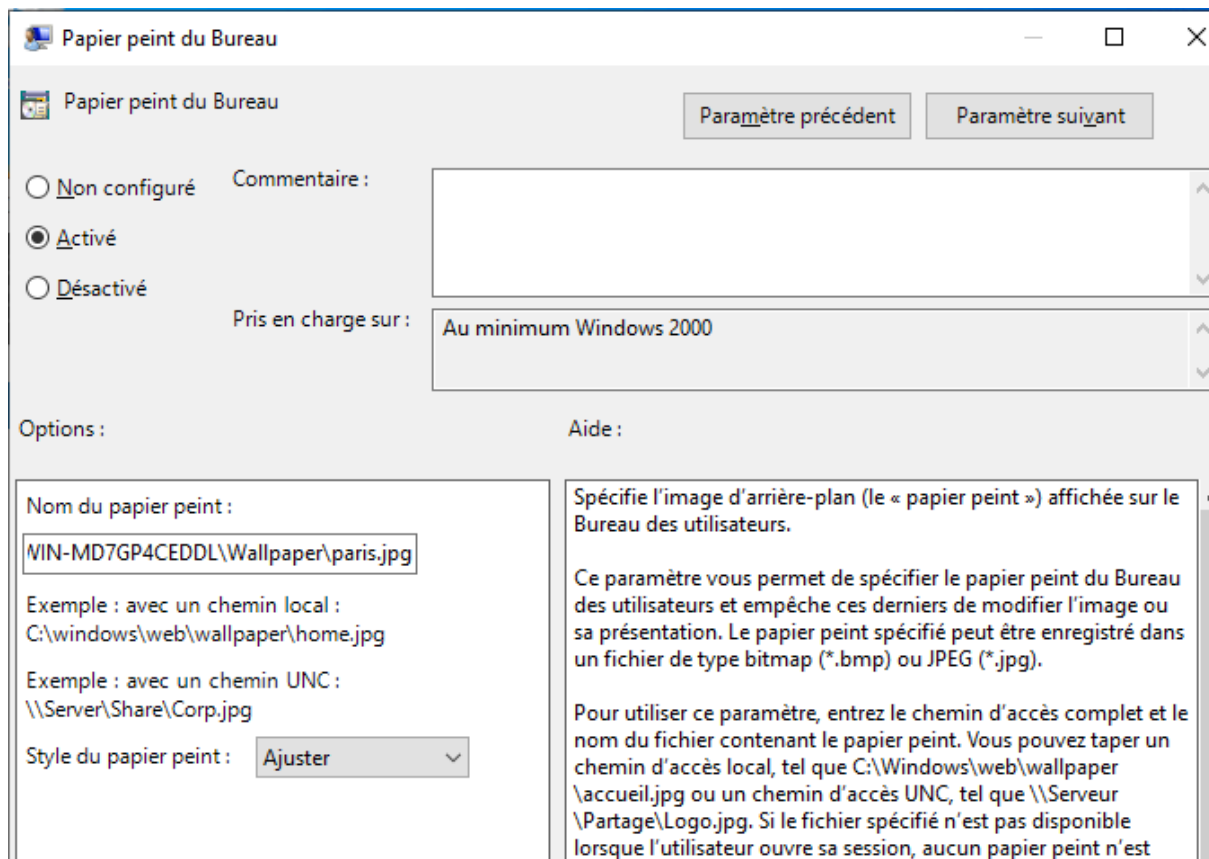
Puis dans Bureau



Et on active *Papier peint du Bureau*

Paramètre	État	Coti
Activer Active Desktop	Non configuré	
Désactiver Active Desktop	Non configuré	
Interdire les modifications	Non configuré	
Papier peint du Bureau	Activé	
Empêcher l'ajout d'éléments	Non configuré	
Empêcher la fermeture d'éléments	Non configuré	
Empêcher la suppression d'éléments	Non configuré	
Empêcher la modification d'éléments	Non configuré	
Désactiver tous les éléments	Non configuré	
Ajouter/supprimer des éléments	Non configuré	
N'autoriser que les papiers peints au format bmp	Non configuré	

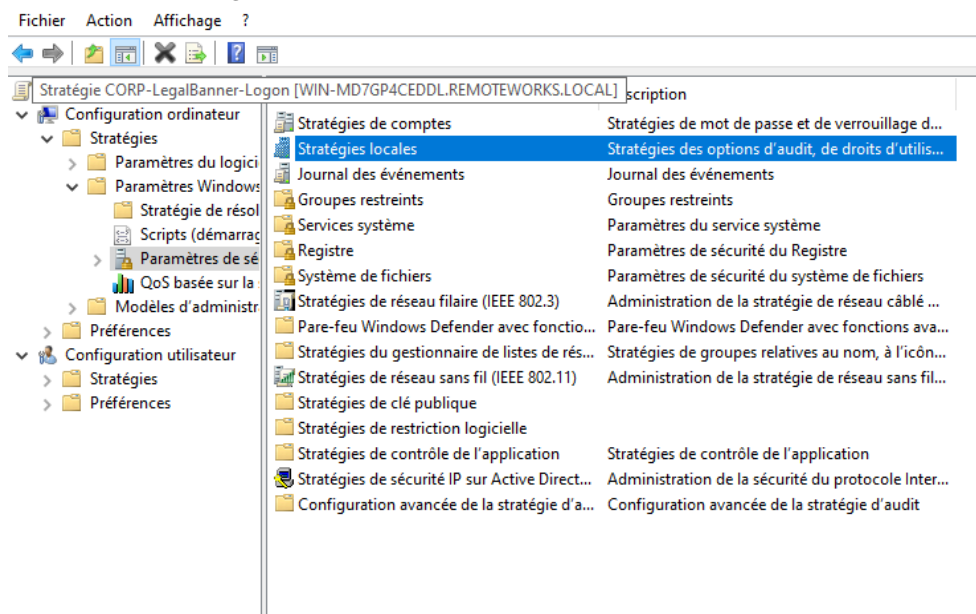
On entre le chemin d'accès du fond d'écran



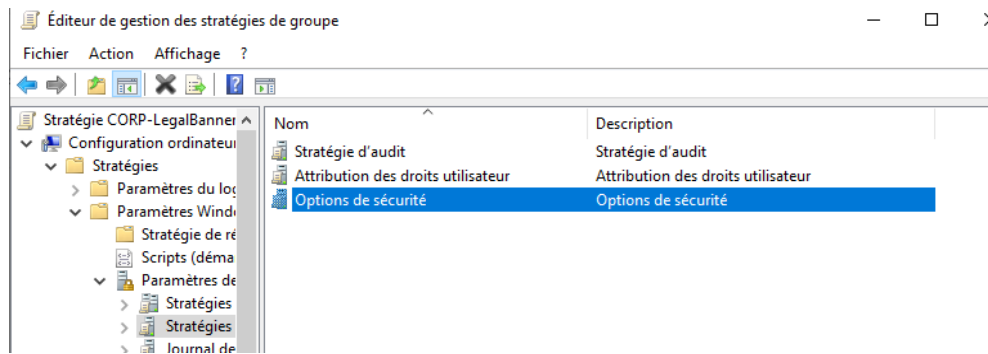
9- CORP-LegalBanner-Logon

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

Puis dans *Stratégies locales*

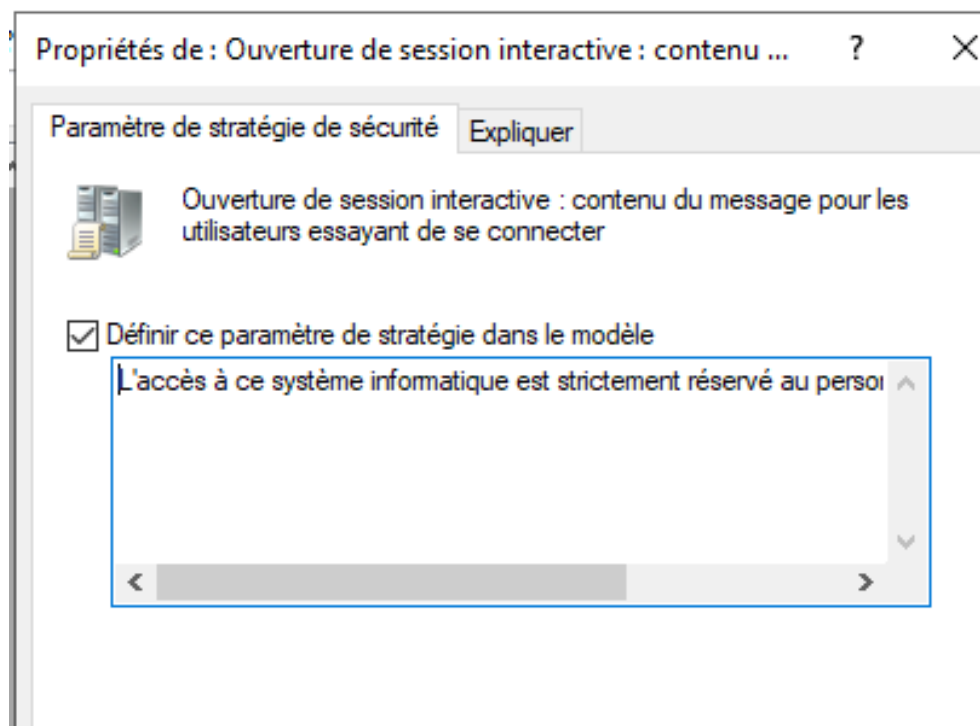


Et enfin dans *Options de sécurité*



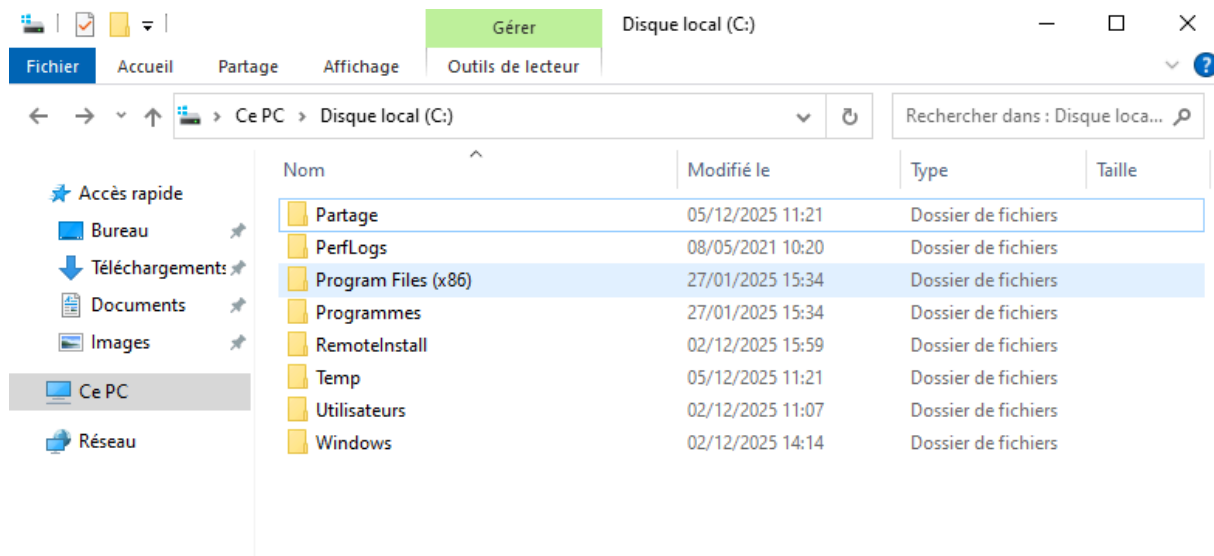
Ensuite on ouvre les propriétés d'*Ouverture de session interactive : contenu du message pour les utilisateurs essayant de se connecter*

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



10- UX-StartMenu-Taskbar-Standard

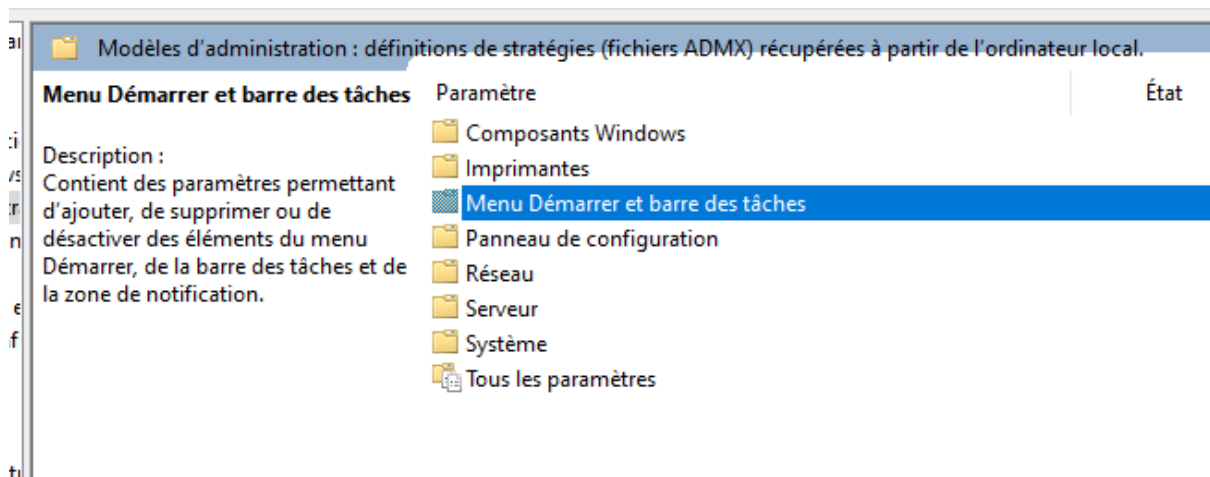
Premièrement on choisit les applications que l'on veut épingler sur notre barre de tâche. Puis on crée un dossier partagé comme pour le fond d'écran



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*

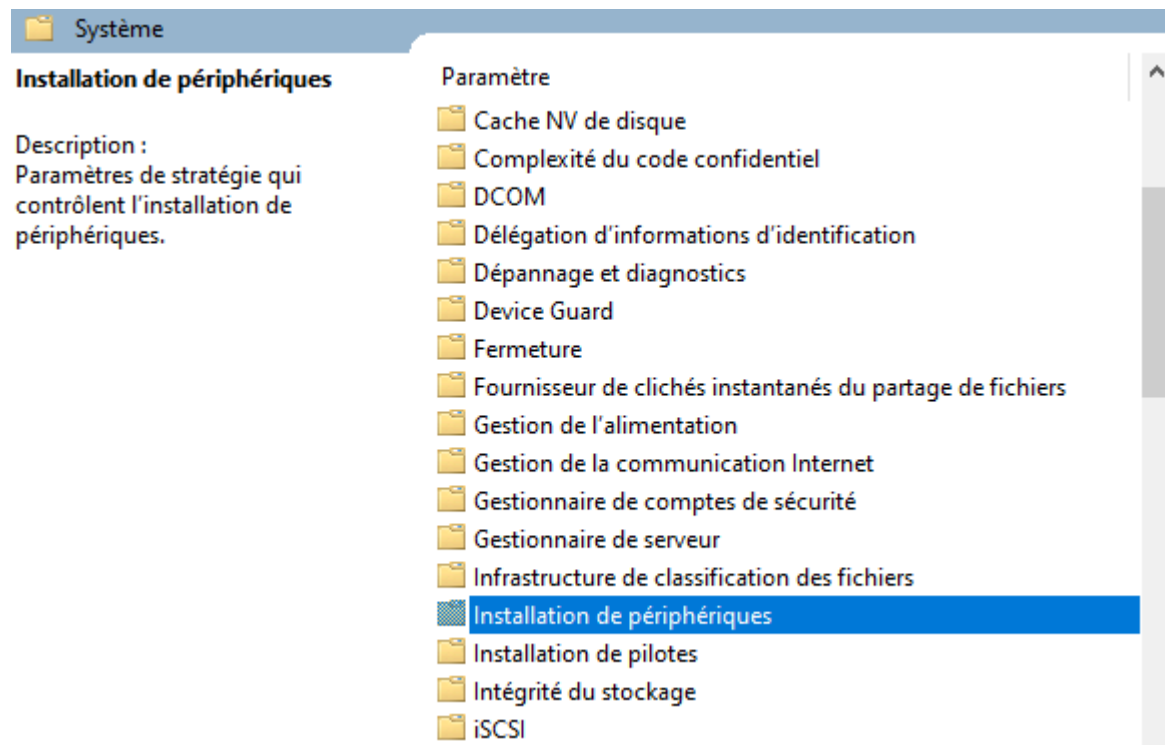


Puis on active *Disposition de l'écran de démarrage* et on y joint le chemin d'accès du fichier XML

Disposition de l'écran de démarrage		Paramètre précédent	Paramètre suivant
<input type="radio"/> Non configuré	Commentaire :		
<input checked="" type="radio"/> <u>A</u> ctivé			
<input type="radio"/> <u>D</u> ésactivé			
Pris en charge sur :		Au moins Windows Server 2016, Windows 10	
Options :		Aide :	
<div>Fichier de disposition de démarrage</div> <div>\\WIN-MD7GP4CEDDL\Partage\Standarc</div>		<p>Spécifie la disposition de l'écran de démarrage pour les utilisateurs.</p> <p>Ce paramètre vous permet de spécifier la disposition de l'écran de démarrage pour les utilisateurs et les empêche de modifier sa configuration. La disposition de l'écran de démarrage que vous spécifiez doit être stockée dans un fichier XML généré par l'applet de commande PowerShell Export-StartLayout. Pour utiliser ce paramètre, vous devez d'abord configurer manuellement la disposition de l'écran de démarrage d'un appareil selon l'apparence souhaitée. Après cela, exécutez l'applet de commande PowerShell Export-StartLayout sur ce même appareil. L'applet de commande génère un fichier XML représentant la disposition que vous avez configurée.</p> <p>Une fois le fichier XML généré et déplacé vers le chemin d'accès de fichier souhaité, entrez le nom et le chemin d'accès complet au fichier XML. Vous pouvez entrer un chemin d'accès local, tel que C:\StartLayouts\myLayout.xml, ou un chemin d'accès UNC, tel que \\Serveur\Partage\Layout.xml. Si le fichier spécifié n'est pas disponible lorsque l'utilisateur ouvre une session, la</p>	

11- SEC-Device-BlockBluetooth

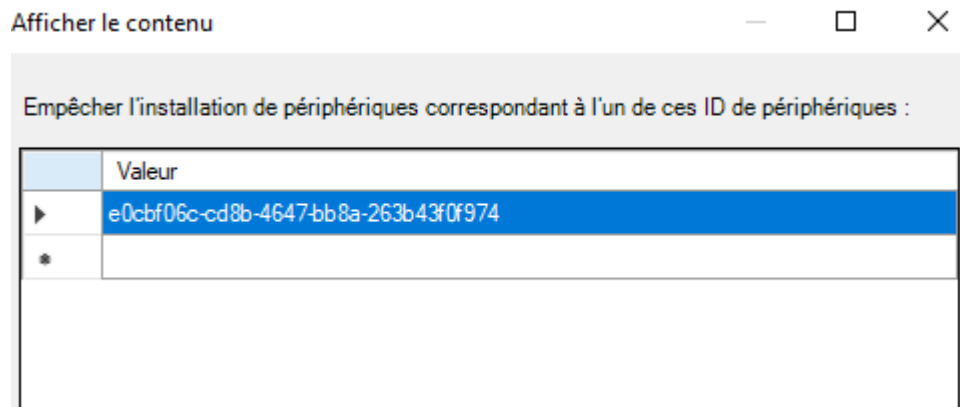
On modifie la GPO puis on se déplace dans *Configuration ordinateur > Stratégies > Modèles d'administration > Système > Installation de périphériques*



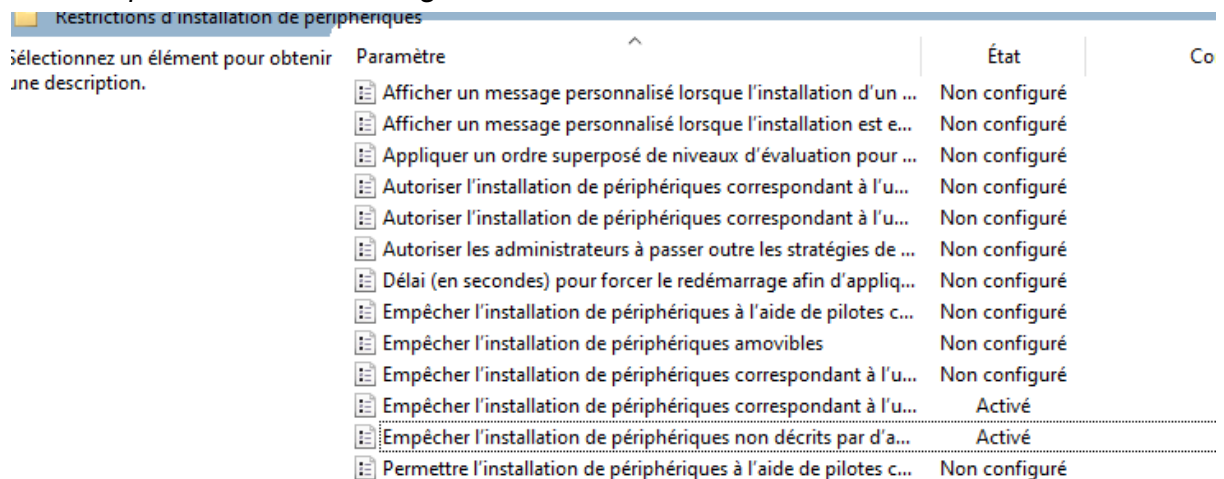
Puis dans *Restrictions d'installation des périphériques*

Installation de périphériques			
Sélectionnez un élément pour obtenir une description.	Paramètre	État	Comu
	Restrictions d'installation de périphériques		
	Accorder la même priorité à tous les pilotes signés numériq...	Non configuré	I
	Configurer le délai d'attente d'installation de périphérique	Non configuré	I
	Empêcher la création de point de restauration système lors ...	Non configuré	I
	Autoriser l'accès distant à l'interface Plug-and-Play	Non configuré	I
	Désactiver les bulles « Nouveau matériel détecté » pendant l...	Non configuré	I
	Ne pas envoyer de rapport d'erreurs Windows lors de l'instal...	Non configuré	I
	Empêcher Windows d'envoyer un rapport d'erreurs lorsqu'u...	Non configuré	I
	Empêcher la récupération des métadonnées de périphérique...	Non configuré	I
	Spécifier l'ordre de recherche des emplacements source des ...	Non configuré	I
	Spécifier le serveur de recherche de mises à jour de pilotes d...	Non configuré	I

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

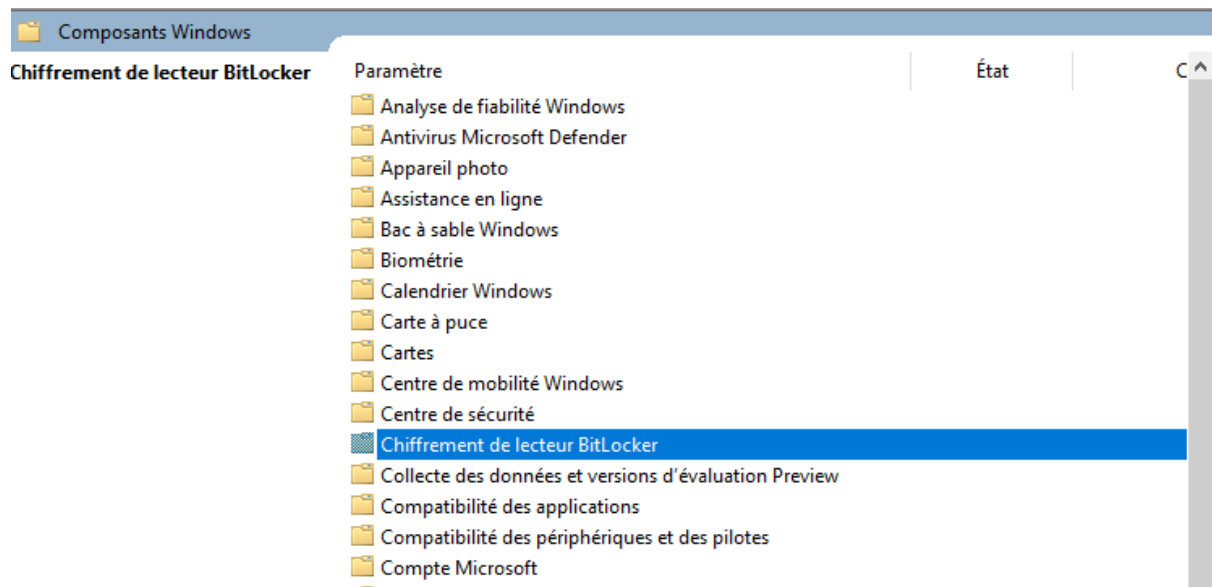


On active également l'option *Empêcher l'installation de périphériques non décrits par d'autres paramètres de stratégie*

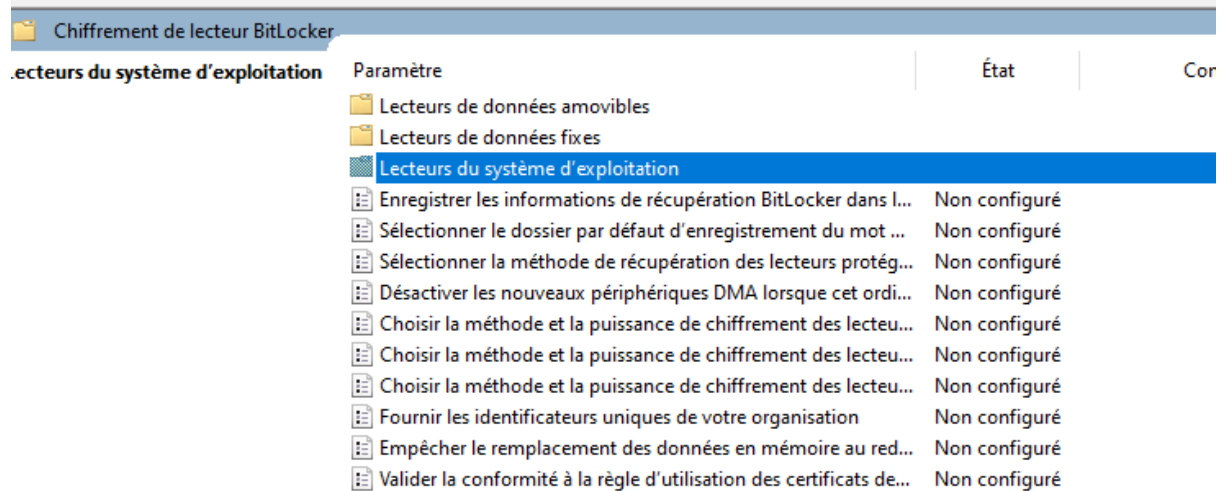


12- SEC-BitLocker-Workstations

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*

Exiger une authentification supplémentaire au démarrage

Exiger une authentification supplémentaire au démarrage Paramètre pré

☐ Non configuré Commentaire :
☒ Activé
☐ Désactivé

Pris en charge sur : Au minimum Windows Server 2008 R2 ou

Options : Aide

☒ Autoriser BitLocker sans un module de plateforme sécurisée compatible (re mot de passe ou une clé de démarrage sur un disque mémoire flash USB)

Paramètres pour les ordinateurs avec un module de plateforme sécurisée :

Configurer le démarrage du module de plateforme sécurisée :

Exiger le module de plateforme sécurisée

Configurer le code PIN de démarrage de module de plateforme sécurisée :

Exiger un code PIN de démarrage avec le module de plateforme sécurisée

Configurer la clé de démarrage de module de plateforme sécurisée :

Autoriser une clé de démarrage avec le module de plateforme sécurisée

Configurer le code PIN et la clé de démarrage de module de plateforme sécurisée :

Autoriser une clé et un code PIN de démarrage avec le module de plateforme sécurisée :

Ce p
supp
mod
BitLo

Rem
dém

Si vo
activ
com
dém
le le
l'acc
dispo
optio

Sur u
méth
de l'i
de n

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

Sélectionner la méthode de récupération des lecteurs fixes protégés par BitLocker

Sélectionner la méthode de récupération des lecteurs fixes protégés par BitLocker Paramètres

☐ Non configuré Commentaire :

☒ Activé

☐ Désactivé

Pris en charge sur : Au minimum Windows Server 2008 R2 ou Windows 7

Options : Aide :

☒ Autoriser les agents de récupération de données

Configurer le stockage par les utilisateurs des informations de récupération BitLocker :

Autoriser un mot de passe de récupération de 48 chiffres

Autoriser une clé de récupération de 256 bits

☐ Supprimer les options de configuration de l'Assistant d'installation de BitLocker

☒ Enregistrer les informations de récupération BitLocker dans les services de domaine Active Directory pour les lecteurs de données fixes

Configurer le stockage des informations de récupération BitLocker dans les services de domaine Active Directory :

Sauvegarder les mots de passe de récupération et les packages de clés

☒ N'activer BitLocker qu'une fois les informations de récupération stockées dans les services de domaine Active Directory pour les lecteurs de données fixes

Ce paramètre de stratégie protège les lecteurs fixes protégés par BitLocker. Ce paramètre de stratégie doit être configuré avant d'activer BitLocker.

La case à cocher « Autoriser les agents de récupération de données » doit être cochée pour que les agents de récupération de données puissent être ajoutés à la stratégie de groupe. Guide de déploiement de BitLocker : Ajout d'informations sur l'ajout d'agents de récupération de données.

Dans « Configurer le stockage des informations de récupération BitLocker », indiquez le type de mot de passe de récupération à utiliser.

Sélectionnez « Supprimer les options de configuration de l'Assistant d'installation de BitLocker » pour empêcher les utilisateurs d'activer BitLocker sur un lecteur protégé par BitLocker. La récupération utilise les informations de récupération pour le lecteur sont ajoutées à la stratégie de groupe.

Dans « Enregistrer les informations de récupération BitLocker dans les services de domaine Active Directory pour les lecteurs de données fixes », indiquez le type de mot de passe de récupération à utiliser.

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

Choisir la méthode et la puissance de chiffrement des lecteurs (Windows 10 [Version 1511] et ultérieur)

☐ Non configuré Commentaire :

☒ Activé

☐ Désactivé

Pris en charge sur : Au moins Windows Server 2016, Windows 10

Options :

Sélectionner la méthode de chiffrement pour les lecteurs du système d'exploitation :

XTS AES 128 bits (par défaut)

Sélectionner la méthode de chiffrement pour les lecteurs de données fixes :

XTS AES 128 bits (par défaut)

Sélectionner la méthode de chiffrement pour les lecteurs de données amovibles :

AES-CBC 128 bits (par défaut)

Aide :

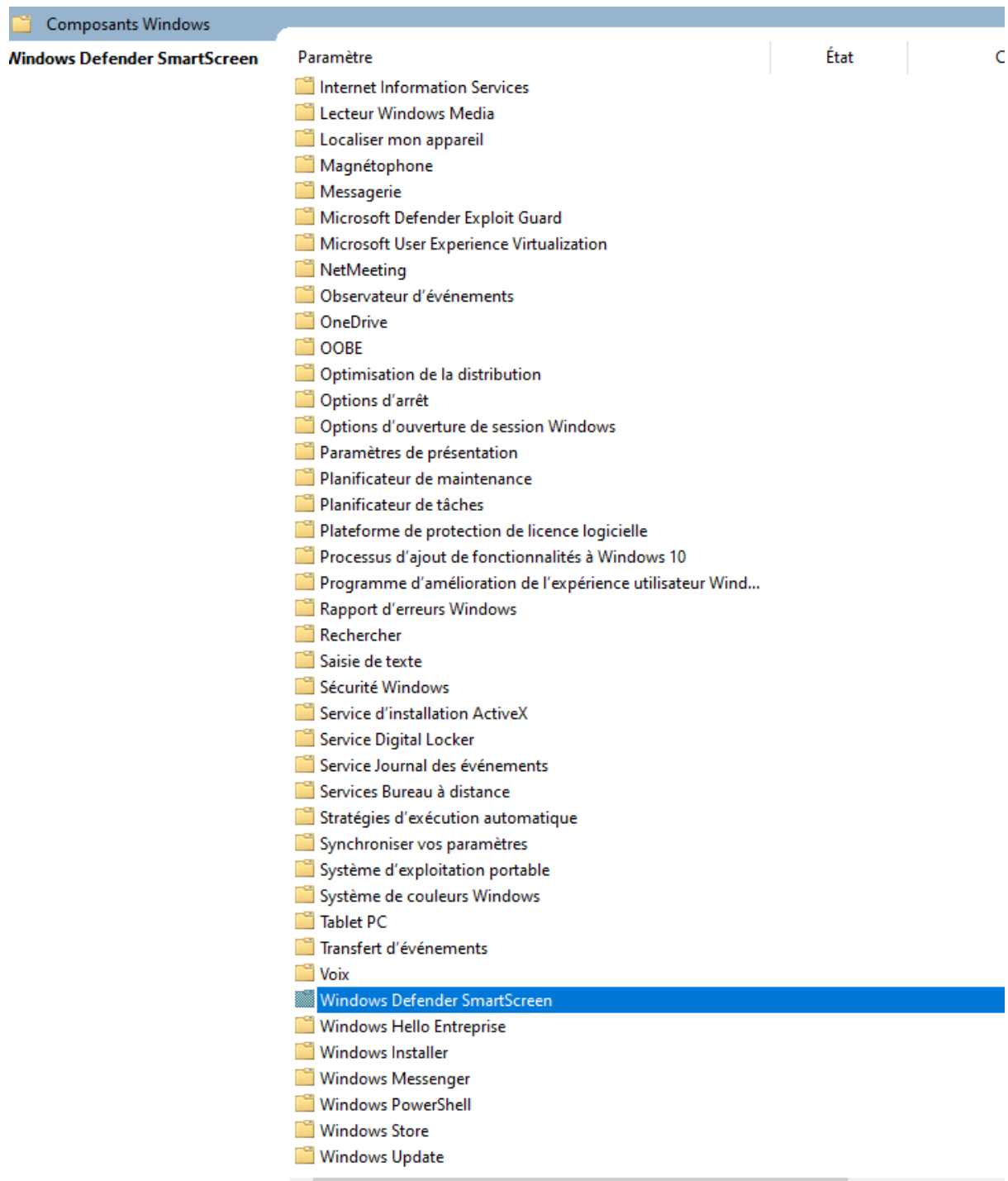
Ce paramètre de stratégie utilisé par le chiffrement vous activez BitLocker. Le lecteur est déjà chiffré ou

Si vous activez ce paramètre de chiffrement et la puissance des lecteurs de système d'exploitation. Pour les lecteurs du système l'algorithme AES-XTS. Pour les lecteurs de données fixes et amovibles, l'algorithme AES-CBC 128 bits si le lecteur est utilisé (Windows 10 [Version 1511]).

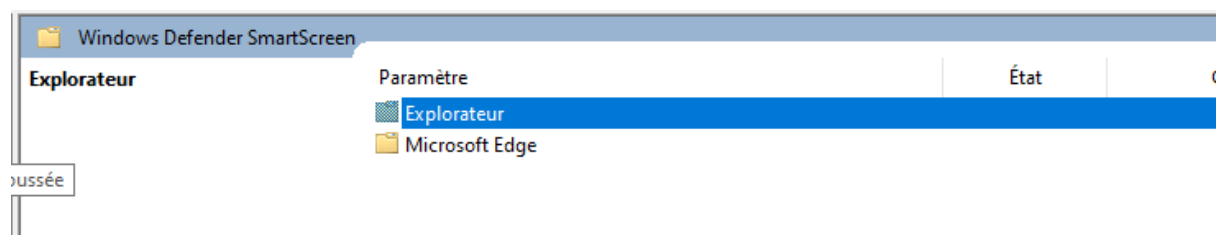
Si vous désactivez ce paramètre, le lecteur n'est pas chiffré avec la même force

13- SEC-SmartScreen-Enable

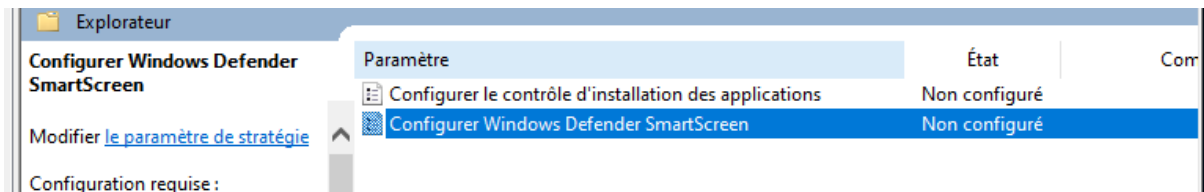
On modifie la GPO puis on se déplace dans Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows Defender SmartScreen



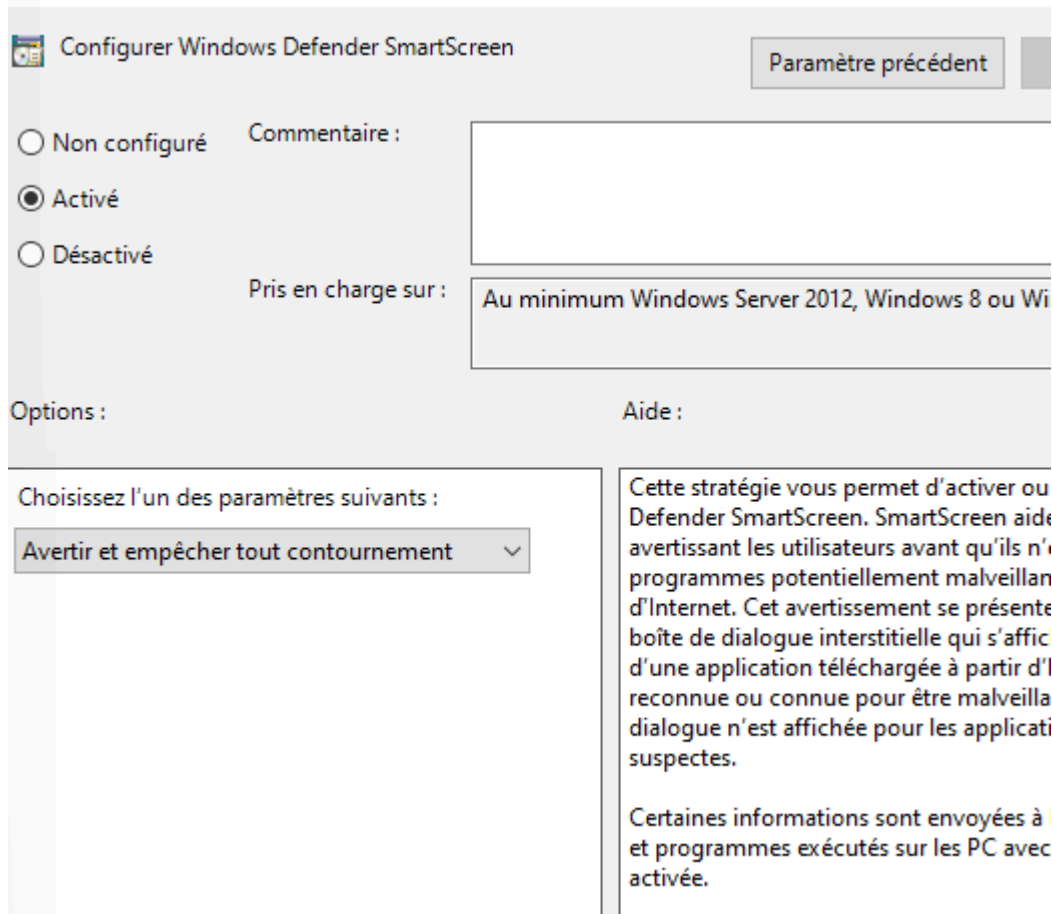
Puis on va dans Explorateur



On active le paramètre Configurer Windows Defender SmartScreen

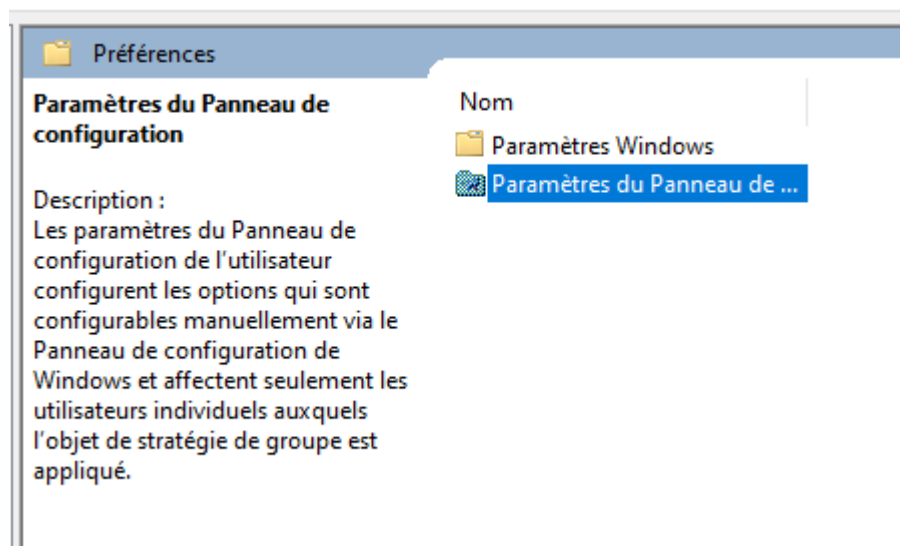


Et on active l'option Avertir et empêcher tout contournement

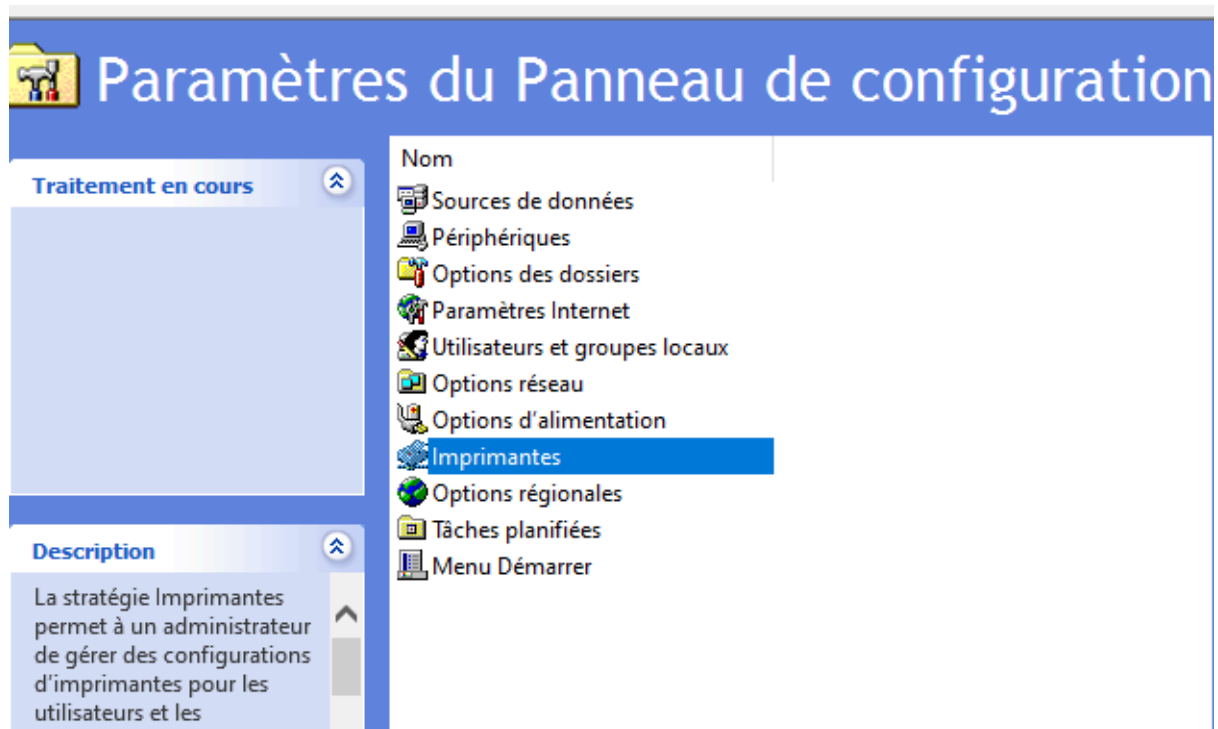


14 - UX-Printers-AutoDeploy

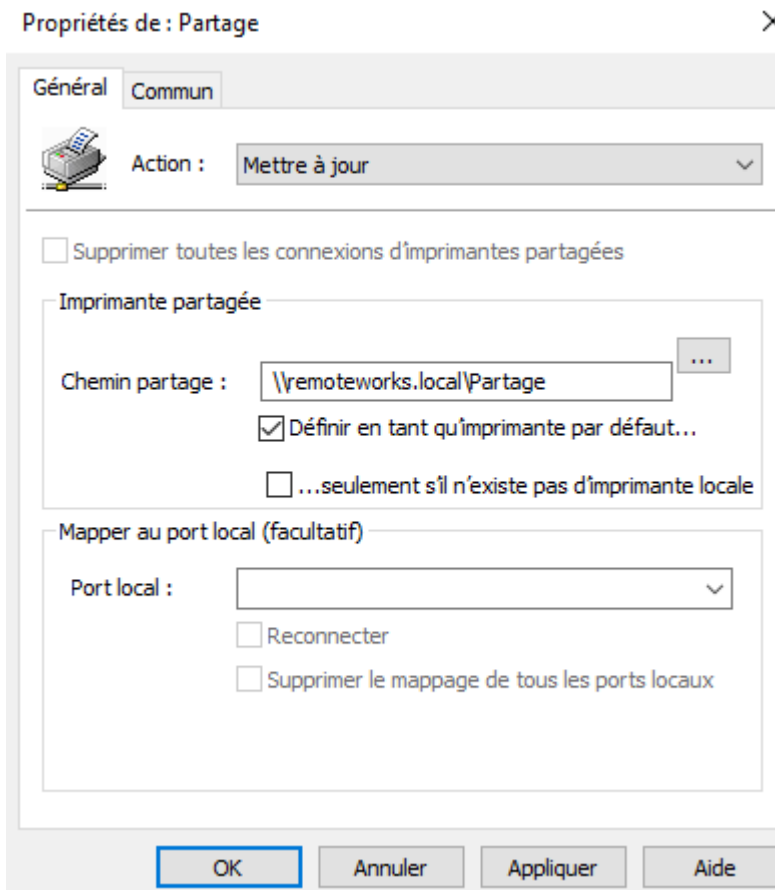
On modifie la GPO puis on se déplace dans *Configuration utilisateur > Préférences > Paramètres du Panneau de configuration*



Puis dans *Imprimantes*



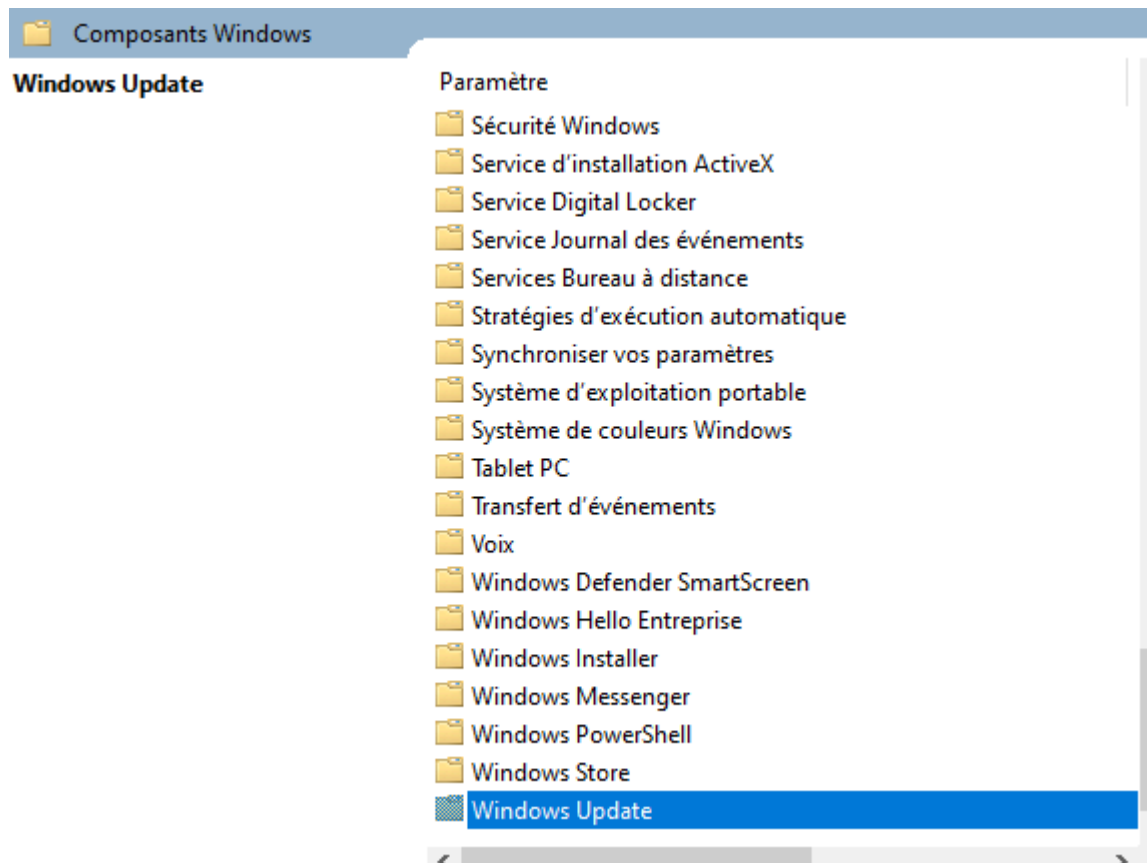
On clique droit sur Nouveau > *Imprimante Partagé*



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*.

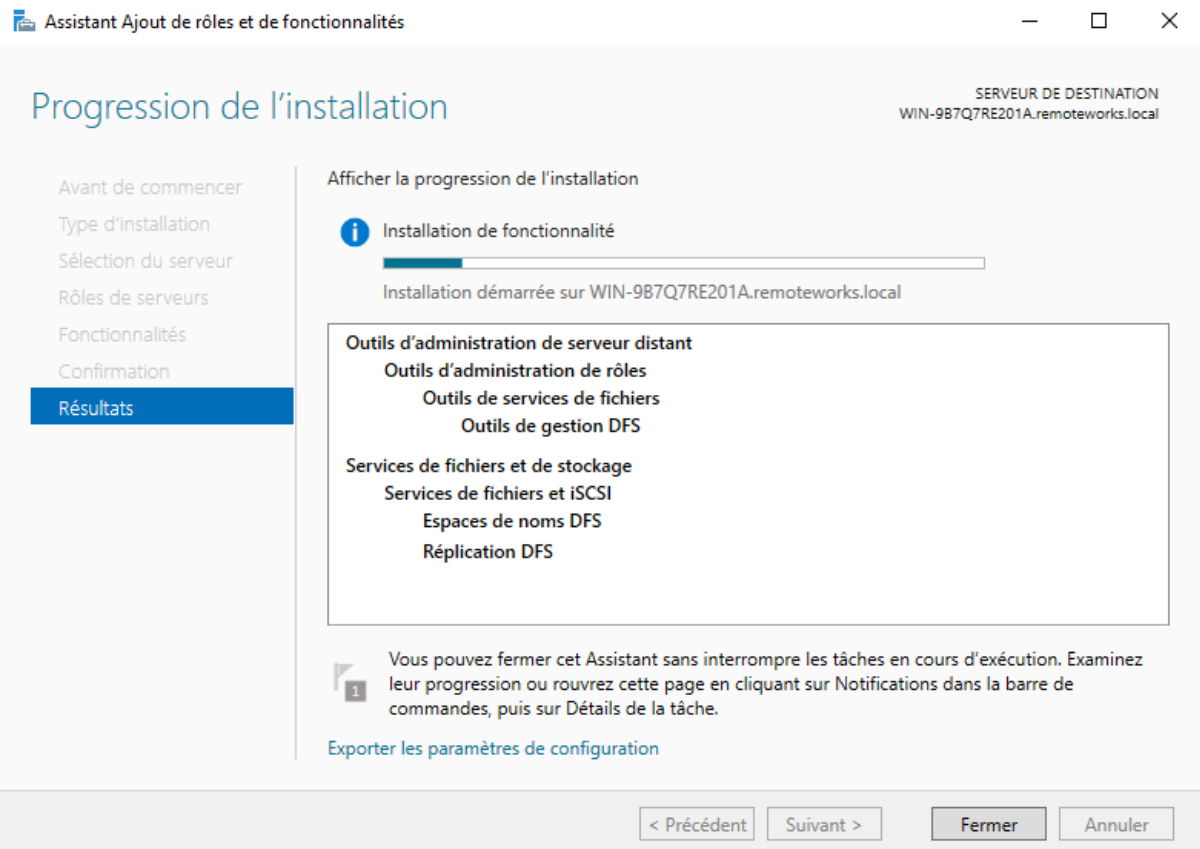
On sélectionne *Installation basée sur un rôle ou fonctionnalité*.

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

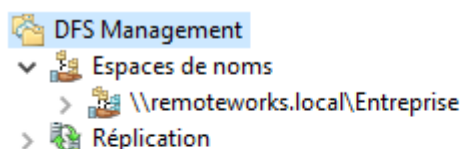
1. On ouvre *Gestion du système de fichier distribué DFS*
2. Clic droit sur *Espaces de noms* → *Nouvel espace de noms*.
3. On sélectionne le serveur.
4. On choisie un nom (exemple : *Entreprise*).

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:



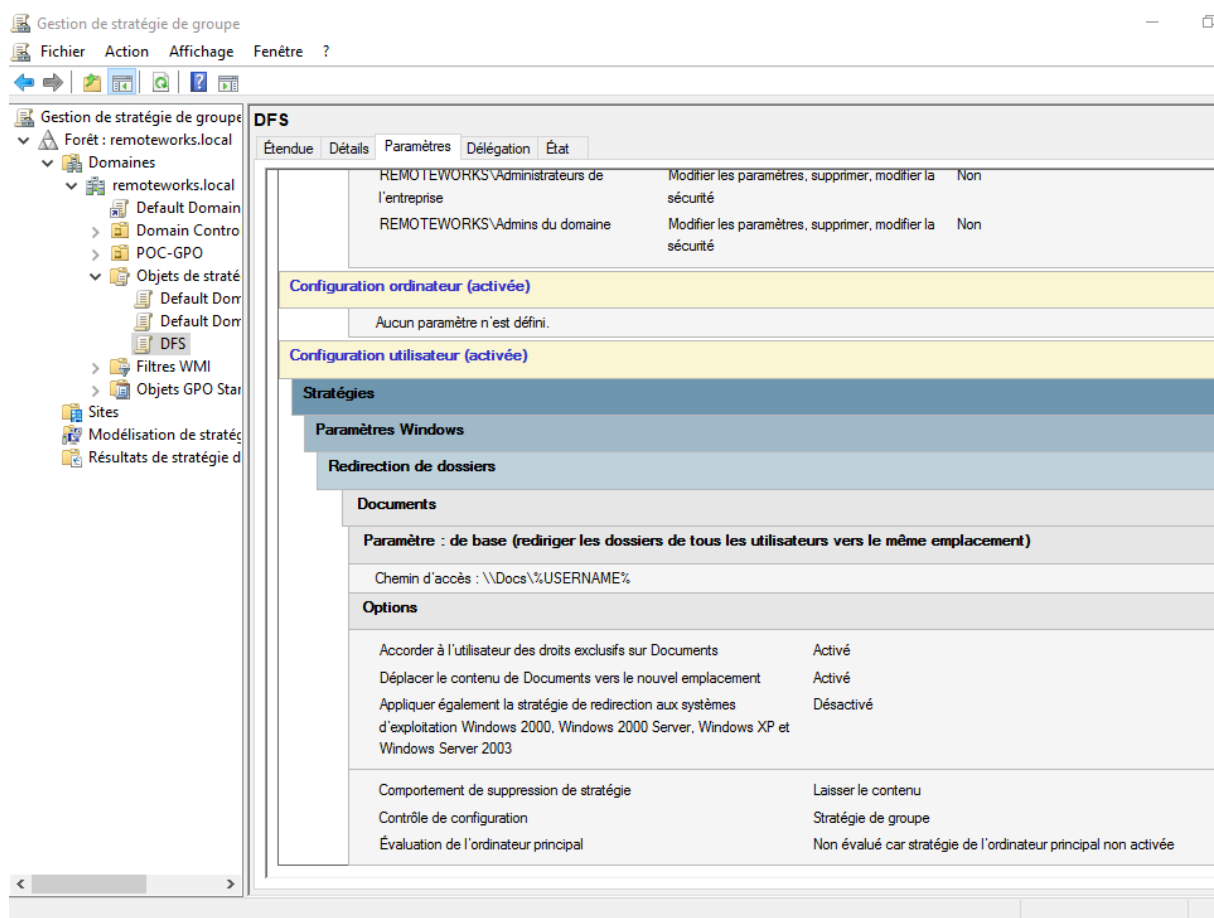
Ajouter des dossiers au Namespace

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.



Spécifier l'emplacement intranet du service de mise à jour Microsoft

Spécifier l'emplacement intranet du service de mise à jour Microsoft Paramètre précédent Paramètre suivant

☐ Non configuré Commentaire :
☒ Activé
☐ Désactivé

Pris en charge sur : Au minimum Windows XP Professionnel Service Pack 1 ou Windows 2000 Service Pack 3, à l'exclusion de

Options : Aide :

Configurer le service de Mise à jour pour la détection des mises à jour :

http://WIN-MD7GP4CEDDL:8530

Configurer le serveur intranet de statistiques : http://WIN-MD7GP4CEDDL:

Définir le serveur de téléchargement alternatif : http://WIN-MD7GP4CEDDL:

(exemple: https://IntranetUpd01)

☐ Téléchargez les fichiers sans URL dans les métadonnées si un serveur de téléchargement alternatif est défini.

☐ Do not enforce TLS certificate pinning for Windows Update client for detecting updates

Select the proxy behavior for Windows Update client for detecting updates:

Utiliser uniquement le proxy système pour détecter les mises à jour (par défaut)

Specifies an intranet server to host updates from Microsoft Update service to automatically update computers on your network.

This setting lets you specify a server on your network to function as the Automatic Updates client will search this service for updates. You can set both values to be the same server name value can be specified to configure Windows Update Agent to download updates from an alternate download server instead of the intranet update service.

To use this setting, you must set two server name values: the server name value that the Automatic Updates client detects and downloads updates, and the server name value that the Automatic Updates client uses to upload statistics. You can set both values to be the same server name value can be specified to configure Windows Update Agent to download updates from an alternate download server instead of the intranet update service.

If the status is set to Enabled, the Automatic Updates client connects to the intranet Microsoft update service (or alternate download server), instead of the Internet, to search for and download updates. Enabling this setting means that your organization doesn't have to go through a firewall to get updates, and it provides an opportunity to test updates before deploying them.

If the status is set to Disabled or Not Configured, and if Automatic Updates is disabled by policy or user preference, the Automatic Updates client cannot connect to the Internet to search for updates.

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.

```

gpupdate /force
...
stratégie d'ordinateur s'est terminée sans erreur.
stratégie utilisateur s'est terminée sans erreur.
  
```

```
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.