

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_-LFwlyGj9uVIMO09R2U/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

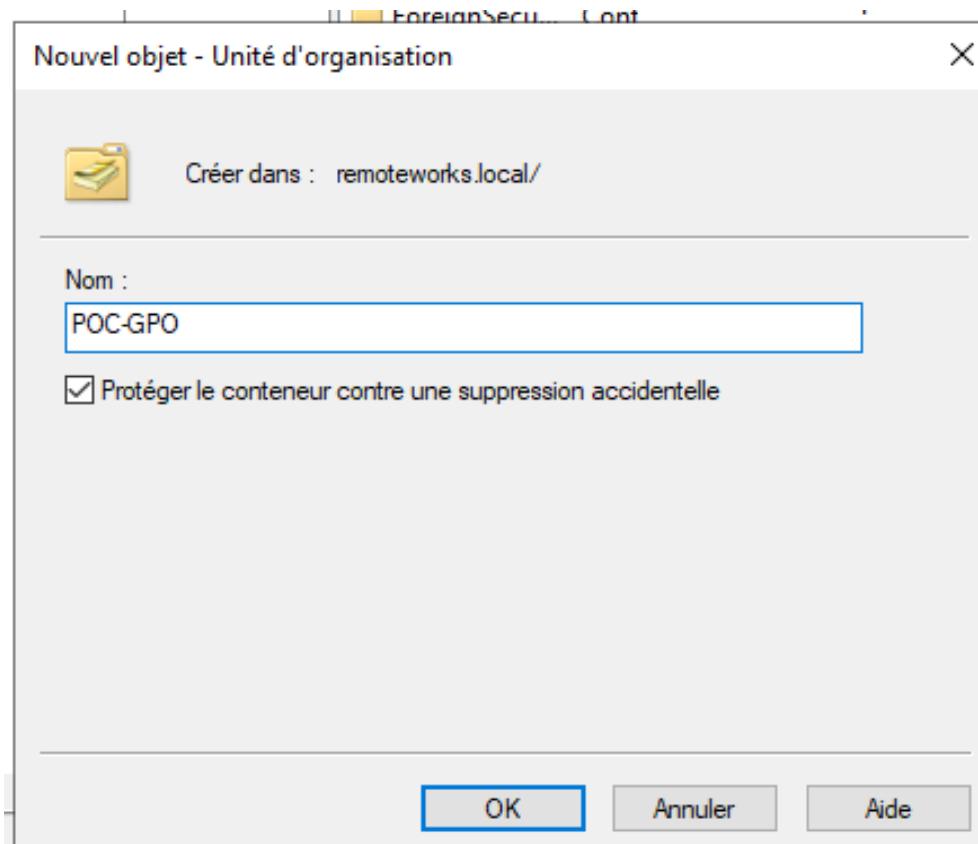
Corporatisme & identité visuelle

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 :

Environnement	Sessions	Contrôle à distance	Profil des services	Bureau à distance	COM+		
Général	Adresse	Compte	Profil	Téléphones	Organisation	Membre de	Appel entrant

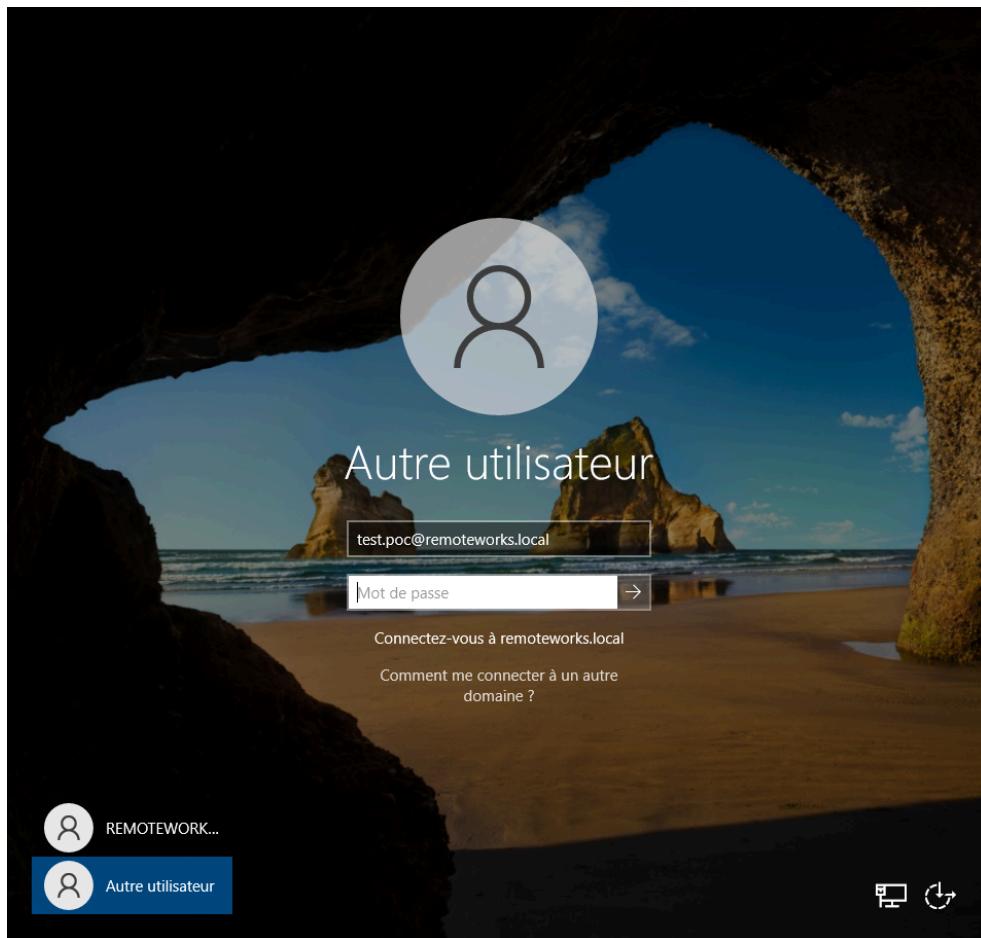
Nom d'ouverture de session de l'utilisateur :
test.poc @remoteworks.local

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*.

-
- Défragmenter et optimiser les lecteurs
DHCP
Diagnostic de mémoire Windows
DNS
Domaines et approbations Active Directory
Éditeur du Registre
Gestion de l'ordinateur
Gestion des stratégies de groupe
Informations système
Initiateur iSCSI
Lecteur de récupération
Modification ADSI
Module Active Directory pour Windows PowerShell
Moniteur de ressources
Nettoyage de disque
Observateur d'événements

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 :

Objets de stratégie de groupe dans remoteworks.local

Contenu Délégation

Nom

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

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

POC-GPO

Créer un objet GPO dans ce domaine, et le lier ici...

Lier un objet de stratégie de groupe existant...

Bloquer l'héritage

Mise à jour de la stratégie de groupe...

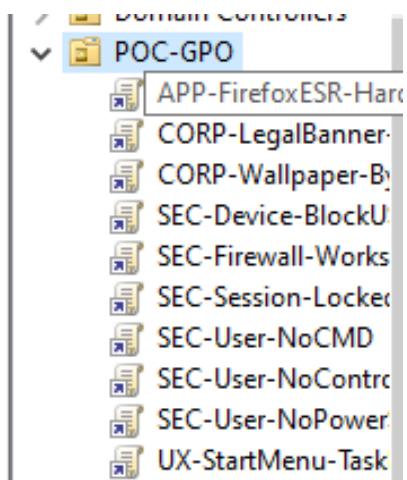
Assistant Modélisation de stratégie de groupe...

Nouvelle unité d'organisation

Affichage >

Nouvelle fenêtre à partir d'ici

Résultat :



2. Configuration des GPO

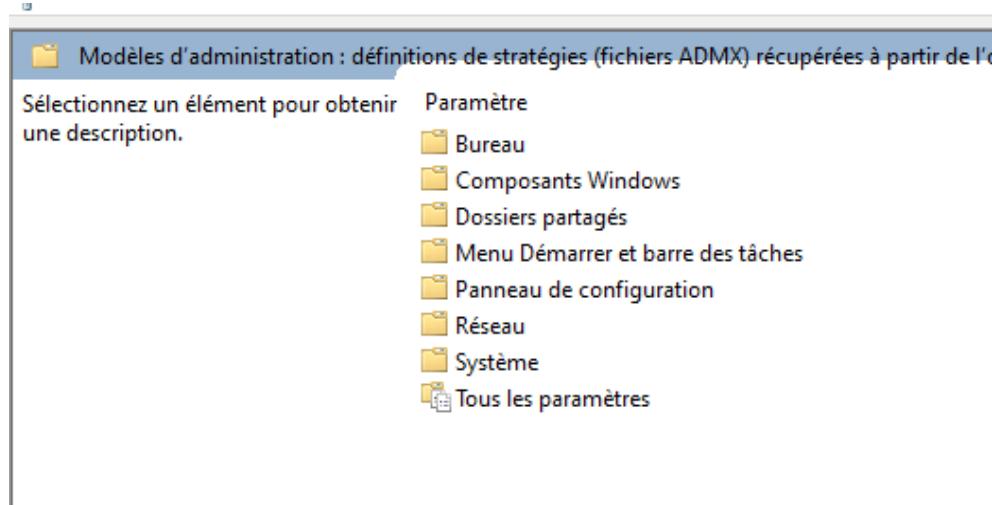
Maintenant on ajoute les règles à nos GPO créés pour qu'elles soient fonctionnelles.

1- SEC-User-NoPowerShell

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

The screenshot shows the "Stratégie SEC-User-NoPowerShell [WIN-MD7GP4CEDDL.REMOTEWORKS.LOCAL]" configuration. In the "Configuration utilisateur" section, the "Nom" is set to "Configuration utilitaire". The "Description" states: "Les administrateurs peuvent utiliser le nœud Configuration de l'utilisateur de la stratégie de groupe pour définir les stratégies appliquées aux utilisateurs, quel que soit l'ordinateur sur lequel ils ouvrent une session." In the "Stratégies" section, the "Nom" is set to "Stratégies". The "Description" is "Stratégies utilisateur".

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



The screenshot shows the 'Ne pas exécuter les applications Windows spécifiées' policy under the 'Système' node. The description states: 'Empêche Windows d'exécuter les programmes spécifiés dans ce paramètre de stratégie.' The details pane shows the following information:

- Configuration requise : Au minimum Windows 2000
- Description : Empêche Windows d'exécuter les programmes spécifiés dans ce paramètre de stratégie.
- Si vous activez ce paramètre de stratégie, les utilisateurs ne peuvent pas exécuter les programmes que vous ajoutez à la liste des applications non autorisées.
- Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les utilisateurs peuvent exécuter tous les programmes.

To the right is a list of parameters:

- 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
- Interprétation du siècle pour l'an 2000
- Restreindre l'exécution de ces programmes à partir de l'aide
- Ne pas afficher l'écran de démarrage Mise en route à l'ouvert...
- Interface utilisateur personnalisée
- Désactiver l'accès à l'invite de commandes
- Empêche l'accès aux outils de modifications du Registre
- Ne pas exécuter les applications Windows spécifiées** (highlighted)
- Exécuter uniquement les applications Windows spécifiées

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

The screenshot shows the 'Liste des applications non autorisées' dialog box. It contains a table with the following data:

	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*

Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local

Panneau de configuration

Description : Contient des paramètres permettant de configurer le Panneau de configuration, notamment les éléments qu'il affiche ou non.

Paramètre

- Bureau
- Composants Windows
- Dossiers partagés
- Menu Démarrer et barre des tâches
- Panneau de configuration**
- Réseau
- Système
- Tous les paramètres

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

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

Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC

Paramètres du PC

Description : Désactive tous les programmes du Panneau de configuration et l'application Paramètres du PC. Ce paramètre empêche le démarrage de Control.exe, de SystemSettings.exe, des fichiers programme du Panneau de configuration et de l'application Paramètres du PC. Ainsi, les utilisateurs ne peuvent pas démarre

3- SEC-Device-BlockUSB

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

Stratégie SEC-User-NoCMD [WIN-MD7GP4CEDDL.REMOTEWORKS.LOCAL]

Configuration ordinateur

Description : Les administrateurs peuvent utiliser le nœud Configuration de l'ordinateur de la stratégie de groupe pour définir les stratégies appliquées aux ordinateurs, quel que soit l'utilisateur qui ouvre une session.

Nom
■ Configuration ordinateur
■ Configuration utilisateur

Configuration ordinateur

Stratégies

Description : Stratégies ordinateur

Nom

- Stratégies
- Préférences

Stratégies

Modèles d'administration

Description : Le noeud des modèles d'administration contient toutes les informations de stratégie basées sur le Registre.

Nom

- Paramètres du logiciel
- Paramètres Windows
- Modèles d'administration

Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur

Système

Description : Autorise la configuration de divers paramètres de composants système.

Paramètre

- Composants Windows
- Imprimantes
- Menu Démarrer et barre des tâches
- Panneau de configuration
- Réseau
- Serveur
- Système**
- Tous les paramètres

Ensuite on se déplace dans *Accès au stockage amovible*

Système

Accès au stockage amovible

Paramètre

- Accès au stockage amovible
- Accès au stockage étendu
- Affichage
- App-V

Puis on active :

- *Disques amovibles : refuser l'accès en lecture*
- *Disques amovibles : refuser l'accès en écriture*

Résultat :

Paramètre	État
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*

Paramètre
Bureau
Composants Windows
Dossiers partagés
Menu Démarrer et barre des tâches
Panneau de configuration
Réseau
Système
Tous les paramètres

Puis dans *Personnalisation*

Paramètre	État	Com
Affichage	Non configuré	16
Ajouter ou supprimer des programmes	Non configuré	17
Imprimantes	Non configuré	18
Options régionales et linguistiques	Non configuré	19
Personnalisation	Non configuré	
Programmes	Non configuré	
Masquer les éléments du Panneau de configuration spécifiés	Non configuré	
Toujours afficher tous les éléments du Panneau de config...	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 boutons	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\SYSVOL\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
pide	{0EA3A554-89B5-4ED1-B36B-2906AC0D7...	04/12/2025 15:23	Dossier de fichiers	
rgement:	{6AC1786C-016F-11D2-945F-00C04fB984...	02/12/2025 14:14	Dossier de fichiers	
ients	{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
e	fr-FR	12/12/2025 09:55	Dossier de fichiers	
ments:	firefox.admx	12/12/2025 09:45	Fichier ADMX	237 Ko
s	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...

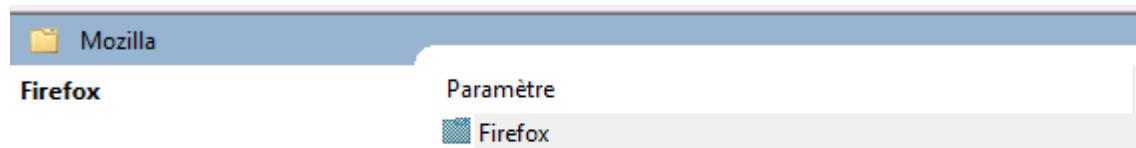
Nom	Modifié le	Type	Taille
en-US	08/05/2021 17:49	Dossier de fichiers	
fr-FR	03/03/2022 04:50	Dossier de fichiers	
ActiveXInstallService.admx	08/05/2021 10:15	Fichier ADMX	5
AddRemovePrograms.admx	08/05/2021 10:15	Fichier ADMX	5
AllowBuildPreview.admx	08/05/2021 10:15	Fichier ADMX	2
AppCompat.admx	08/05/2021 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 central

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

Sélectionnez un élément pour obtenir une description.	Paramètre	État	Com
	Afficher le bouton Accueil sur la barre d'outils	Non configuré	I
	Page de démarrage	Non configuré	I
	Pages d'accueil supplémentaires	Non configuré	I
	URL pour la page d'accueil	Activé	I

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

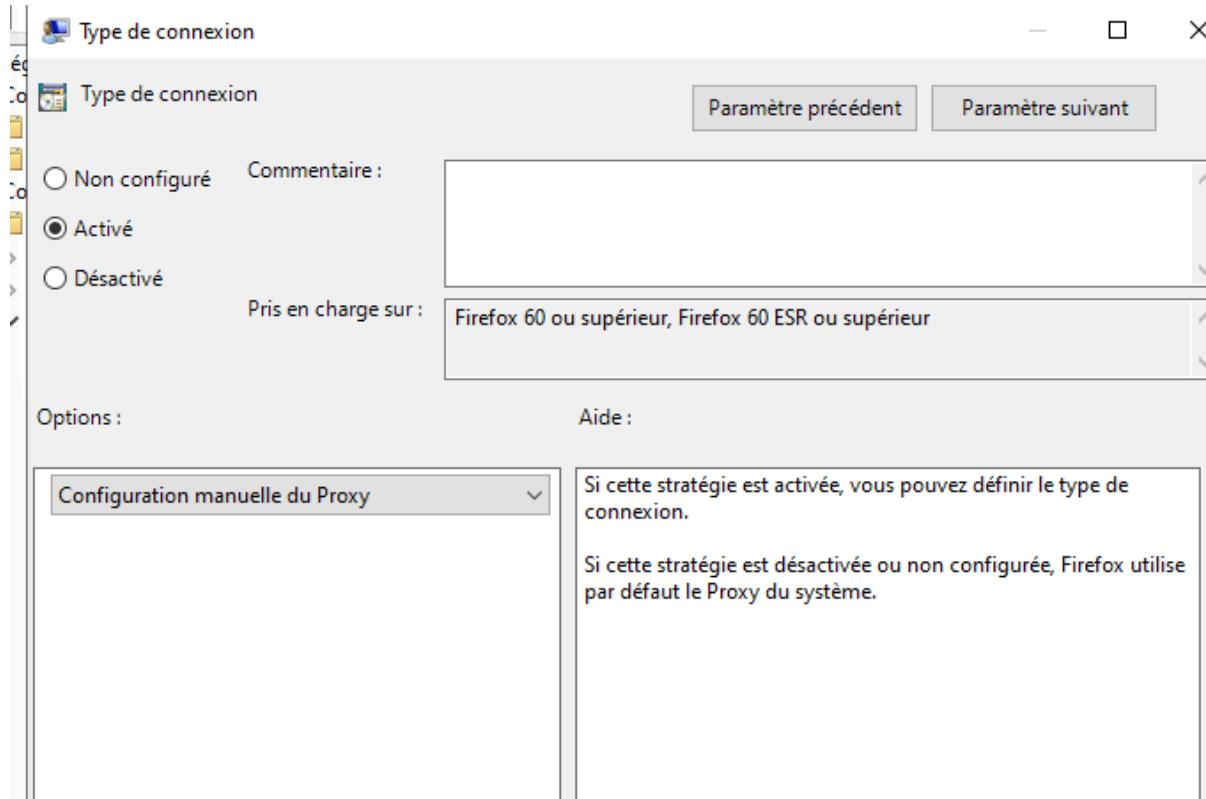
The screenshot shows the configuration dialog for "URL pour la page d'accueil". It has two tabs: "Paramètre précédent" and "Paramètre suivant". The "Paramètre suivant" tab is selected. It shows the following settings:

- State: Activé (radio button selected)
- Commentaire: (empty text area)
- Pris en charge sur: Firefox 60 ou supérieur, Firefox 60 ESR ou supérieur
- URL: https://www.acme-corp.com/ (text input field)
- Options: Ne pas autoriser la modification de la page d'accueil.
- Aide: (two columns of text describing the URL setting)

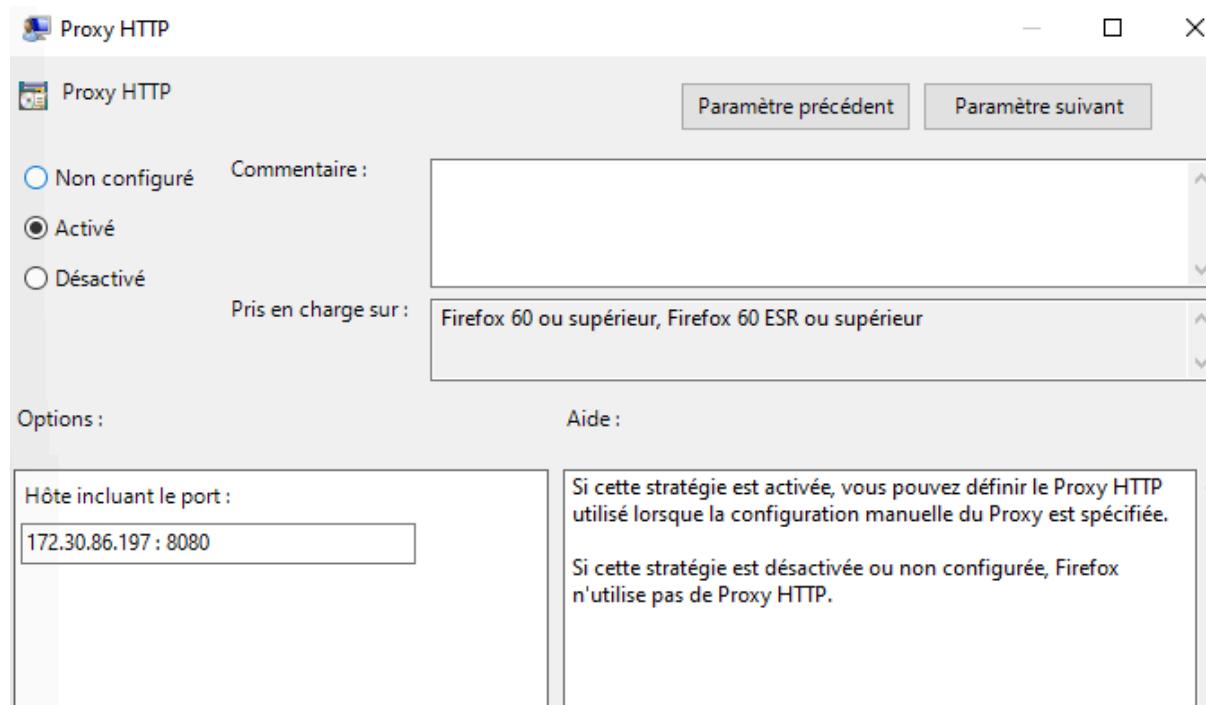
Ensuite on va dans les Paramètres Proxy

Sélectionnez un élément pour obtenir une description.	Paramètre	État	Co
	URL de configuration automatique du Proxy	Non configuré	
	Ne pas demander d'authentification si le mot de passe est e...	Non configuré	
	Type de connexion	Activé	
	Proxy HTTP	Activé	
	Ne pas autoriser la modification des paramètres de Proxy	Activé	
	Passage direct du Proxy	Non configuré	
	Hôte SOCKS	Non configuré	
	Proxy HTTPS	Activé	
	Utiliser le Proxy HTTP pour HTTPS	Non configuré	
	Proxy DNS lors de l'utilisation de SOCKS	Non configuré	

Puis on active Type de connexion et on choisit 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

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

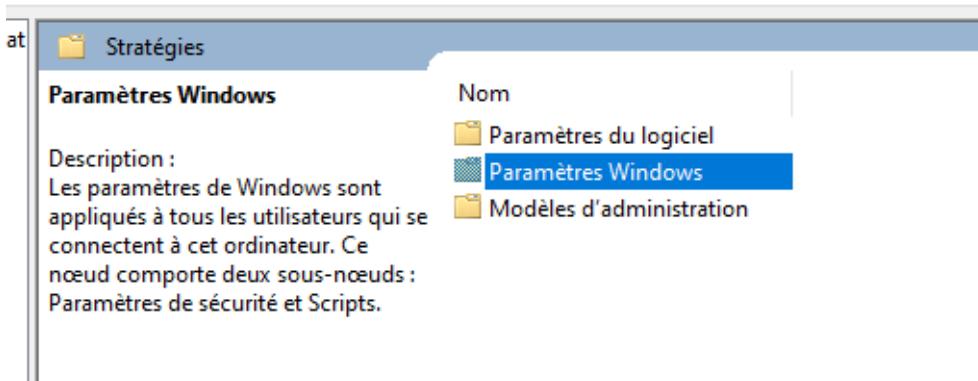
On modifie la GPO puis on se déplace dans *Configuration utilisateur > Stratégies > Modèles d'administration > Système*

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

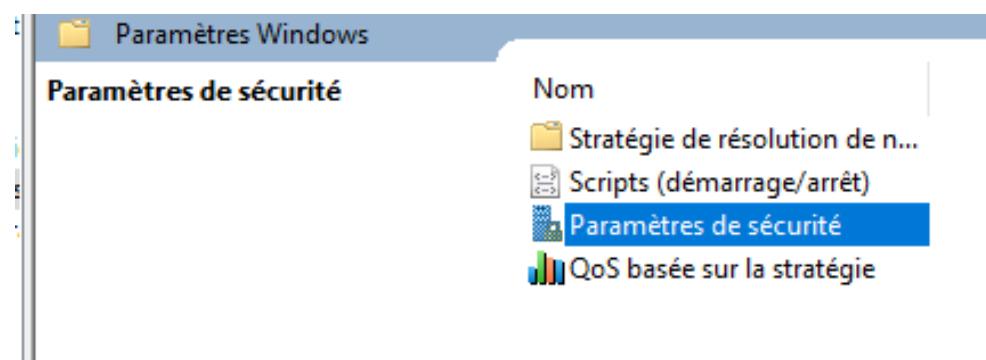
Paramètre	État
Accès au stockage amovible	Non configuré
Affichage	Non configuré
Gestion de l'alimentation	Non configuré
Gestion de la communication Internet	Non configuré
Installation de pilotes	Non configuré
Options Ctrl+Alt+Suppr	Non configuré
Options d'atténuation	Non configuré
Ouverture de session	Non configuré
Profils utilisateur	Non configuré
Redirection de dossiers	Non configuré
Scripts	Non configuré
Services Paramètres régionaux	Non configuré
Stratégie de groupe	Non configuré
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'ouvert...	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

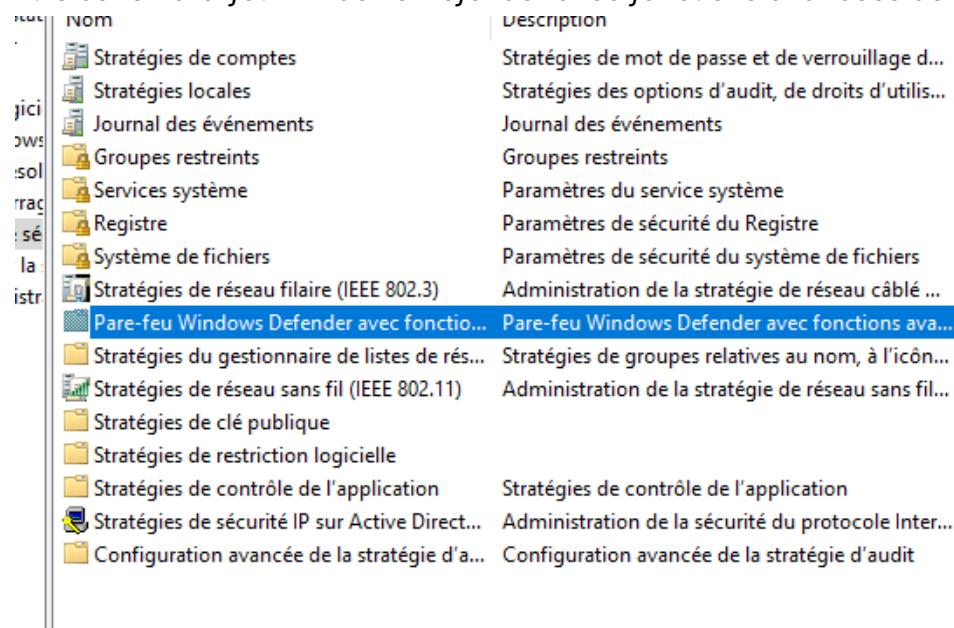
On modifie la GPO puis on se déplace dans *Configuration ordinateur > Stratégies > Paramètres Windows*



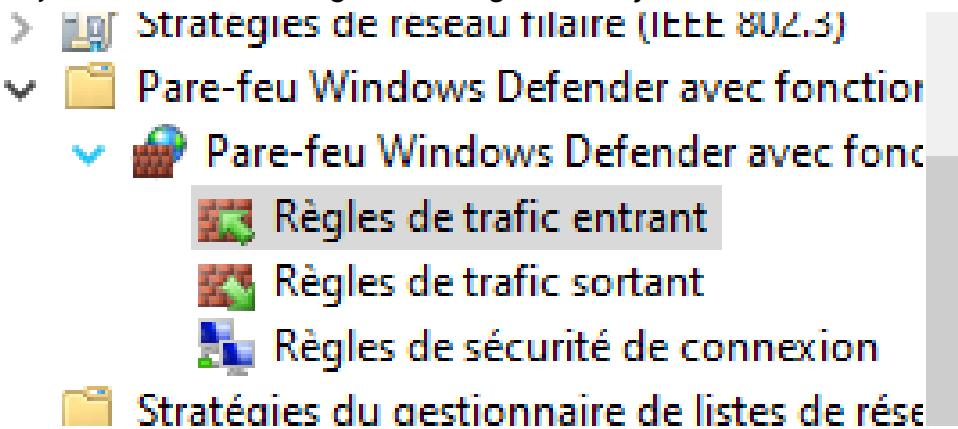
Puis dans *Paramètres de sécurité*



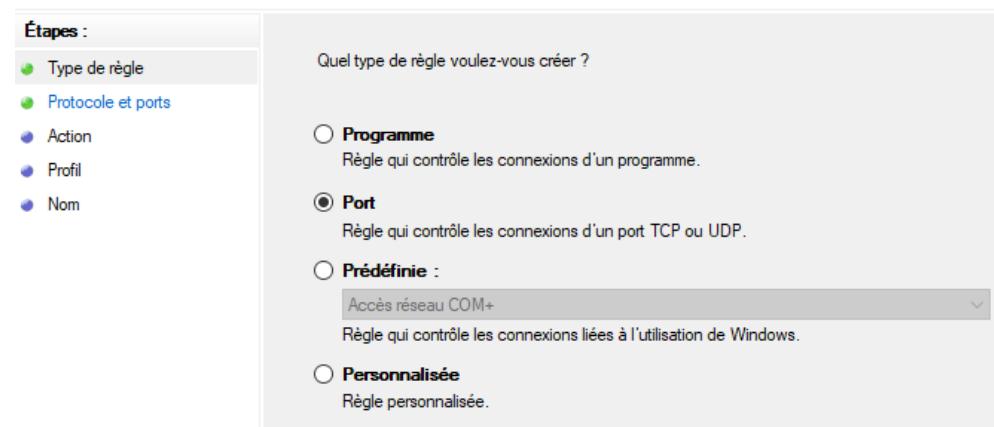
Puis dans *Pare-feu Windows Defender avec fonctions avancées de sécurité*



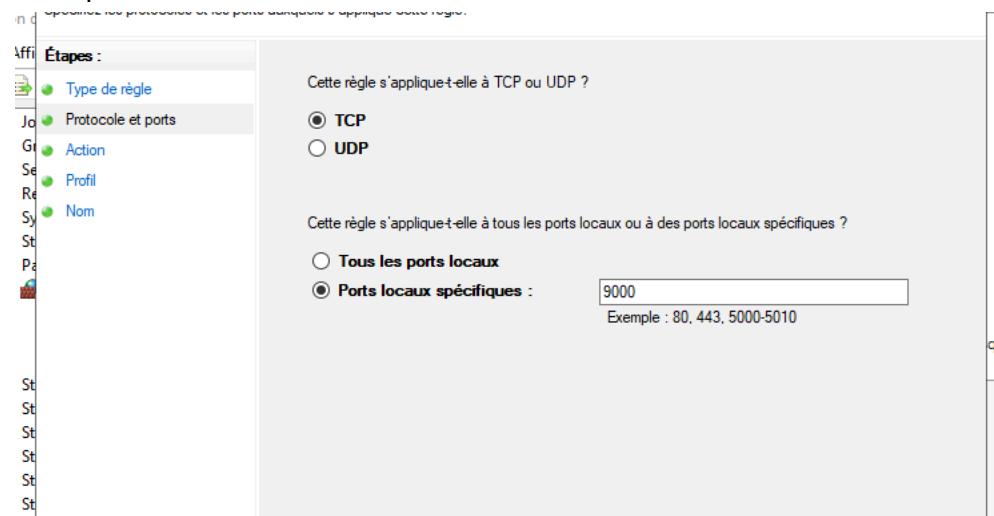
On ajoute une nouvelle règle dans *Règles de trafic entrant*



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

~~Appliquer les profils suivants à l'application cette règle.~~

Étapes :

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

Quand cette règle est-elle appliquée ?

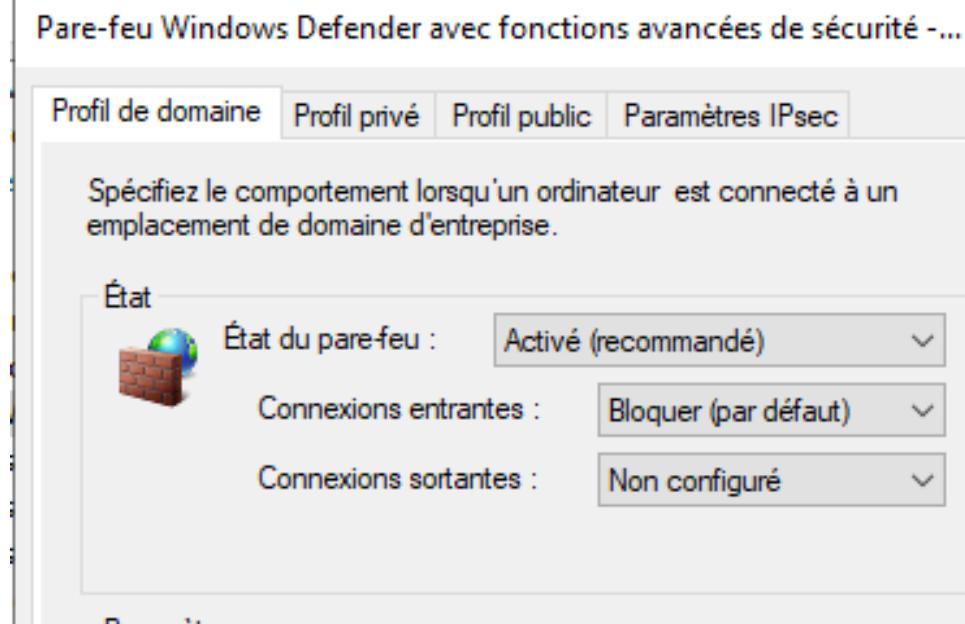
Domaine
Lors de la connexion d'un ordinateur à son domaine d'entreprise.

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

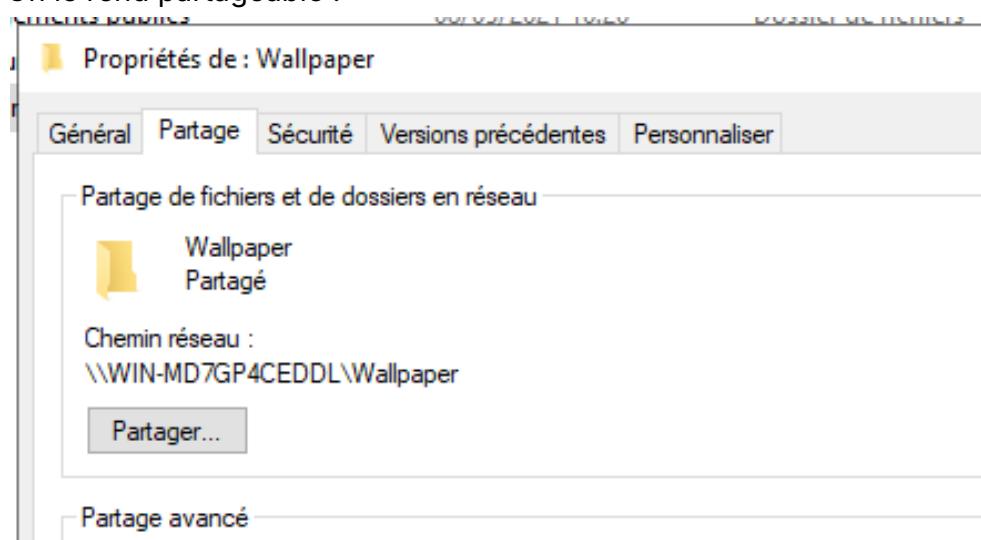


8- CORP-Wallpaper-BySite

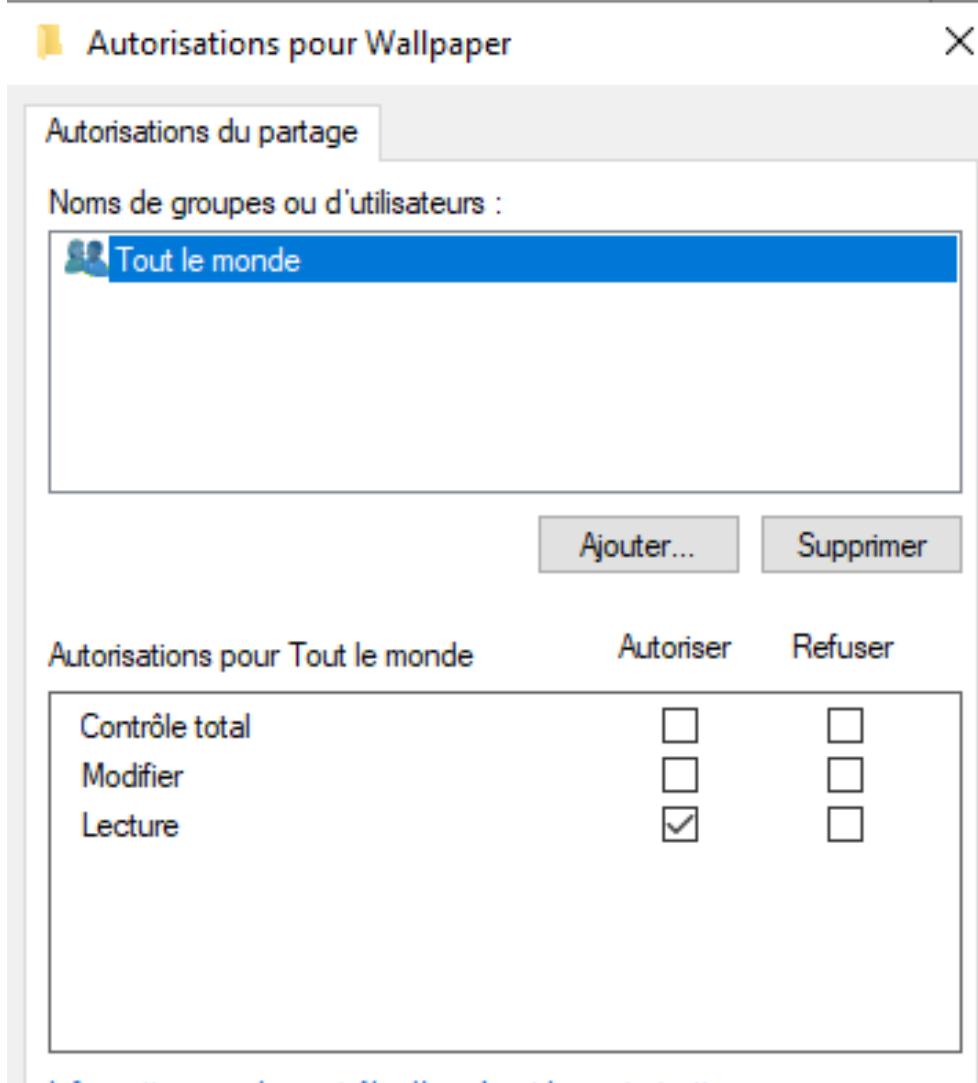
Pour appliquer un fond d'écran commun, il faut premièrement importer une image qui fera office de fond d'écran puis la mettre dans un dossier

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*

Stratégie CORP-Wallpaper-BySi

Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local

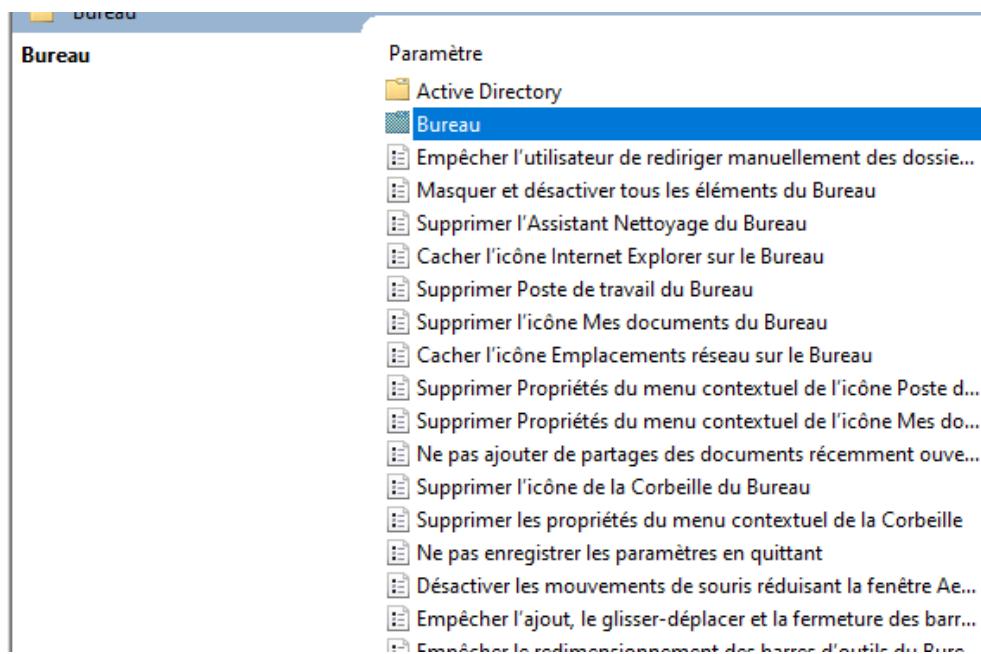
Bureau

Description : Contient des paramètres permettant de gérer le comportement du Bureau de l'utilisateur et de définir les icônes qui sont affichées par défaut sur ce Bureau.

Paramètre

- Bureau**
- Composants Windows
- Dossiers partagés
- Menu Démarrer et barre des tâches
- Panneau de configuration
- Réseau
- Système
- Tous les paramètres

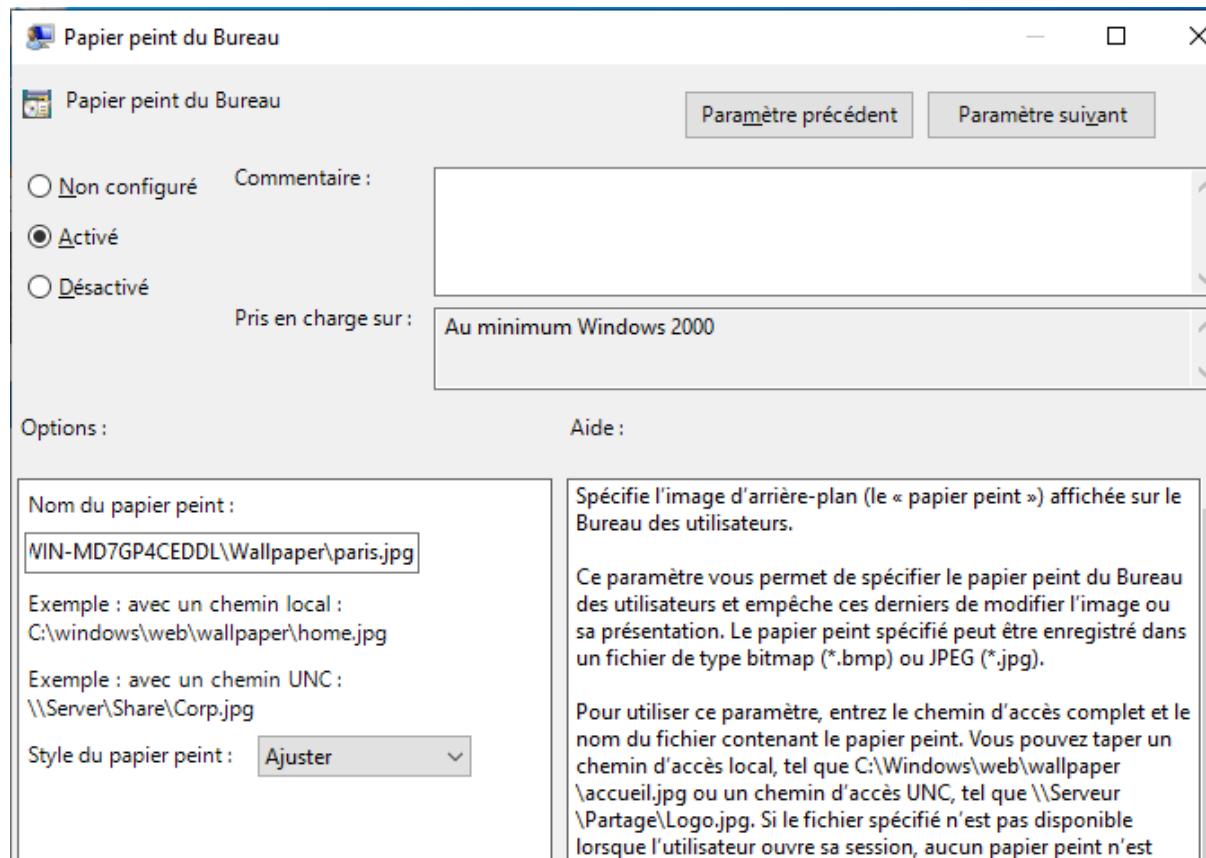
Puis dans Bureau



Et on active *Papier peint du Bureau*

Paramètre	État	Cor
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	

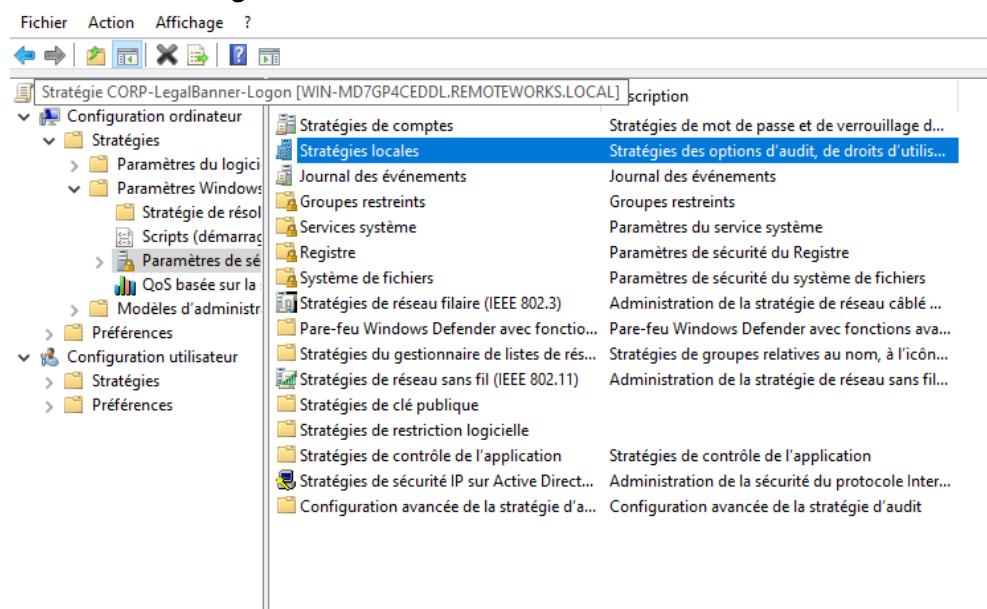
On entre le chemin d'accès du fond d'écran



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*

The screenshot shows the 'Éditeur de gestion des stratégies de groupe' window. In the left navigation pane, under 'Stratégie CORP-LegalBanner', the 'Options de sécurité' node is selected. The right pane displays a table with three rows:

Nom	Description
Stratégie d'audit	Stratégie d'audit
Attribution des droits utilisateur	Attribution des droits utilisateur
Options de sécurité	Options de sécurité

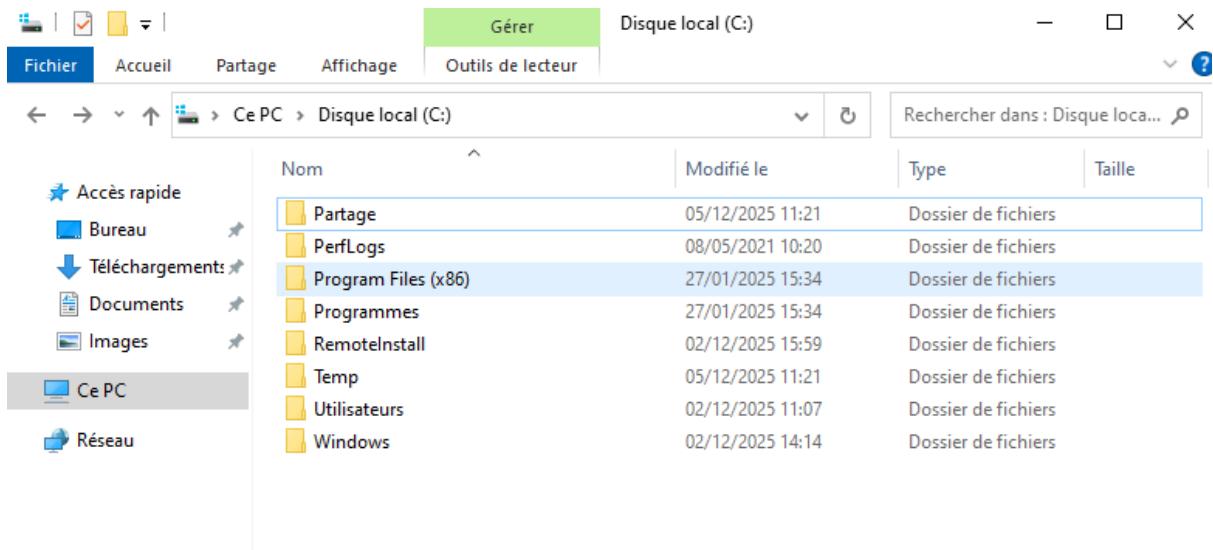
Ensuite on ouvre les propriétés d'*Ouverture de session interactive : contenu du message pour les utilisateurs essayant de se connecter*

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

The screenshot shows the 'Propriétés de : Ouverture de session interactive : contenu ...' dialog box. The title bar says 'Propriétés de : Ouverture de session interactive : contenu ...'. The main area is titled 'Paramètre de stratégie de sécurité' with a 'Expliquer' button. On the left, there is a server icon. The main content area shows the parameter name 'Ouverture de session interactive : contenu du message pour les utilisateurs essayant de se connecter'. Below it, a checked checkbox says 'Définir ce paramètre de stratégie dans le modèle'. A text input field contains the message: 'L'accès à ce système informatique est strictement réservé au perso...'. There are scroll bars on the right side of the input field.

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*

The screenshot shows the Group Policy Management Editor. The left pane displays the navigation tree under 'Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local'. The 'Menu Démarrer et barre des tâches' node is selected. The right pane shows the 'Paramètre' (Parameter) list, which includes 'Composants Windows', 'Imprimantes', 'Menu Démarrer et barre des tâches' (selected), 'Panneau de configuration', 'Réseau', 'Serveur', 'Système', and 'Tous les paramètres'.

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

The screenshot shows the 'Disposition de l'écran de démarrage' (Start Screen Layout) configuration page. At the top, there are three radio button options: 'Non configuré' (Not configured), 'Activé' (Enabled), and 'Désactivé' (Disabled). The 'Activé' option is selected. Below this, there is a 'Commentaire:' (Comment) field which is empty. Underneath the radio buttons, it says 'Pris en charge sur:' (Supported on:) followed by 'Au moins Windows Server 2016, Windows 10'. On the right side of the screen, there are two buttons: 'Paramètre précédent' (Previous setting) and 'Paramètre suivant' (Next setting). At the bottom left, there is an 'Options:' (Options) section containing a 'Fichier de disposition de démarrage' (Start screen layout file) input field with the value '\\WIN-MD7GP4CEDDL\Partage\Standarc'. On the right side, there is an 'Aide:' (Help) section with detailed text explaining the parameter and its usage.

Disposition de l'écran de démarrage

Paramètre précédent Paramètre suivant

Non configuré Commentaire :

Activé

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

Options : Aide :

Fichier de disposition de démarrage
\\WIN-MD7GP4CEDDL\Partage\Standarc

Spécifie la disposition de l'écran de démarrage pour les utilisateurs.

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.

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

11- SEC-Device-BlockBluetooth

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

The screenshot shows the 'Système' folder expanded in the navigation pane. Under 'Installation de périphériques', there is a detailed list of parameters:

- Cache NV de disque
- Complexité du code confidentiel
- DCOM
- Délégation d'informations d'identification
- Dépannage et diagnostics
- Device Guard
- Fermeture
- Fournisseur de clichés instantanés du partage de fichiers
- Gestion de l'alimentation
- Gestion de la communication Internet
- Gestionnaire de comptes de sécurité
- Gestionnaire de serveur
- Infrastructure de classification des fichiers
- Installation de périphériques** (highlighted in blue)
- Installation de pilotes
- Intégrité du stockage
- iSCSI

Puis dans *Restrictions d'installation des périphériques*

The screenshot shows the 'Restrictions d'installation de périphériques' configuration page. On the left, a note says 'Sélectionnez un élément pour obtenir une description.' The main area lists various policy settings with their current status:

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

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

Afficher le contenu

Empêcher l'installation de périphériques correspondant à l'un de ces ID de périphériques :

	Valeur
▶	e0cbf06c-cd8b-4647-bb8a-263b43f0f974
*	

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

Restrictions d'installation de périphériques

Sélectionnez un élément pour obtenir une description.	Paramètre	État	Co
	Afficher un message personnalisé lorsque l'installation d'un ...	Non configuré	
	Afficher un message personnalisé lorsque l'installation est e...	Non configuré	
	Appliquer un ordre superposé de niveaux d'évaluation pour ...	Non configuré	
	Autoriser l'installation de périphériques correspondant à l'u...	Non configuré	
	Autoriser l'installation de périphériques correspondant à l'u...	Non configuré	
	Autoriser les administrateurs à passer outre les stratégies de ...	Non configuré	
	Délai (en secondes) pour forcer le redémarrage afin d'appliq...	Non configuré	
	Empêcher l'installation de périphériques à l'aide de pilotes c...	Non configuré	
	Empêcher l'installation de périphériques amovibles	Non configuré	
	Empêcher l'installation de périphériques correspondant à l'u...	Non configuré	
	Empêcher l'installation de périphériques correspondant à l'u...	Activé	
	Empêcher l'installation de périphériques non décrits par d'a...	Activé	
	Permettre l'installation de périphériques à l'aide de pilotes c...	Non configuré	

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*

Paramètre	État	C
Analyse de fiabilité Windows		
Antivirus Microsoft Defender		
Appareil photo		
Assistance en ligne		
Bac à sable Windows		
Biométrie		
Calendrier Windows		
Carte à puce		
Cartes		
Centre de mobilité Windows		
Centre de sécurité		
Chiffrement de lecteur BitLocker		
Collecte des données et versions d'évaluation Preview		
Compatibilité des applications		
Compatibilité des périphériques et des pilotes		
Compte Microsoft		

Puis dans Lecteurs du système d'exploitation

Paramètre	État	Cor
Lecteurs de données amovibles		
Lecteurs de données fixes		
Lecteurs du système d'exploitation		
Enregistrer les informations de récupération BitLocker dans l...	Non configuré	
Sélectionner le dossier par défaut d'enregistrement du mot ...	Non configuré	
Sélectionner la méthode de récupération des lecteurs protég...	Non configuré	
Désactiver les nouveaux périphériques DMA lorsque cet ordi...	Non configuré	
Choisir la méthode et la puissance de chiffrement des lecteu...	Non configuré	
Choisir la méthode et la puissance de chiffrement des lecteu...	Non configuré	
Choisir la méthode et la puissance de chiffrement des lecteu...	Non configuré	
Fournir les identificateurs uniques de votre organisation	Non configuré	
Empêcher le remplacement des données en mémoire au red...	Non configuré	
Valider la conformité à la règle d'utilisation des certificats de...	Non configuré	

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

Ce p
supp
mod
BitLc

Rem
dém

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

Sur t
métal
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

Paramètre

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 fixe

La case à cocher « Au minimum Windows Server 2008 R2 ou Windows 7 » indique que ce paramètre de stratégie protège les lecteurs fixes

Dans « Configurer le stockage des informations de récupération BitLocker », indiquez si vous souhaitez autoriser un mot de passe de récupération de 48 chiffres ou une clé de récupération de 256 bits

Sélectionnez « Supprimer les options de configuration de l'Assistant d'installation de BitLocker » pour empêcher les utilisateurs de configurer BitLocker sur un lecteur. Les utilisateurs doivent utiliser la fonctionnalité de BitLocker dans l'assistant d'installation pour configurer BitLocker sur un lecteur

Dans « Enregistrer les informations de récupération BitLocker dans les services de domaine Active Directory pour les lecteurs de données fixes », indiquez si vous souhaitez sauvegarder les mots de passe de récupération et les packages de clés dans les services de domaine Active Directory

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

The screenshot shows the 'Choisir la méthode et la puissance de chiffrement des lecteurs' (Select encryption method and power settings) GPO editor page. It includes the following sections:

- Options :** A section with three radio buttons:
 - Non configuré
 - Activé
 - Désactivé
- Commentaire :** An empty text input field.
- Pris en charge sur :** A dropdown menu showing "Au moins Windows Server 2016, Windows 10".
- Aide :** A large text area containing the following information:

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 de chiffrement pour les lecteurs de système d'exploit. Pour les lecteurs du système d'exploit, l'algorithme AES-XTS. Pour les lecteurs de données fixes et amovibles, l'algorithme AES-CBC 128 bits si le lecteur est utilisé avec Windows 10 (version 1511).

Si vous désactivez ce paramètre, le lecteur est chiffré avec l'algorithme AES 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

Composants Windows

Windows Defender SmartScreen	Paramètre	État	C
Internet Information Services			
Lecteur Windows Media			
Localiser mon appareil			
Magnétophone			
Messagerie			
Microsoft Defender Exploit Guard			
Microsoft User Experience Virtualization			
NetMeeting			
Observateur d'événements			
OneDrive			
OOBE			
Optimisation de la distribution			
Options d'arrêt			
Options d'ouverture de session Windows			
Paramètres de présentation			
Planificateur de maintenance			
Planificateur de tâches			
Plateforme de protection de licence logicielle			
Processus d'ajout de fonctionnalités à Windows 10			
Programme d'amélioration de l'expérience utilisateur Wind...			
Rapport d'erreurs Windows			
Rechercher			
Saisie de texte			
Sécurité Windows			
Service d'installation ActiveX			
Service Digital Locker			
Service Journal des événements			
Services Bureau à distance			
Stratégies d'exécution automatique			
Synchroniser vos paramètres			
Système d'exploitation portable			
Système de couleurs Windows			
Tablet PC			
Transfert d'événements			
Voix			
Windows Defender SmartScreen			
Windows Hello Entreprise			
Windows Installer			
Windows Messenger			
Windows PowerShell			
Windows Store			
Windows Update			

Puis on va dans Explorateur

Windows Defender SmartScreen

Explorateur	Paramètre	État	C
Explorateur	Explorateur		
	Microsoft Edge		

On active le paramètre Configurer Windows Defender SmartScreen

Explorateur	Paramètre	État	Com
Configurer Windows Defender SmartScreen	Configurer le contrôle d'installation des applications	Non configuré	
Modifier le paramètre de stratégie	Configurer Windows Defender SmartScreen	Non configuré	

Configuration requise :

Et on active l'option Avertir et empêcher tout contournement

Configurer Windows Defender SmartScreen

Paramètre précédent

Non configuré Commentaire :

Activé

Désactivé Pris en charge sur : Au minimum Windows Server 2012, Windows 8 ou Wi

Options : Aide :

Choisissez l'un des paramètres suivants :

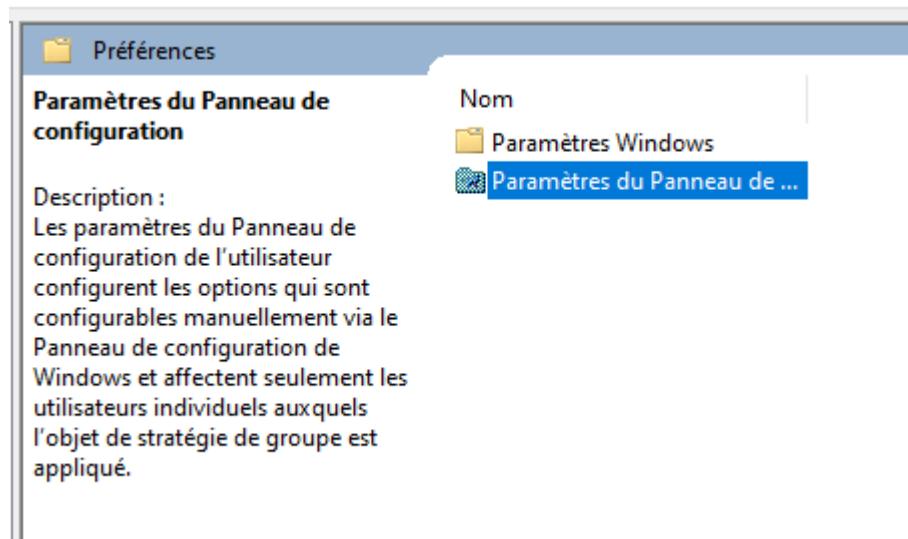
Avertir et empêcher tout contournement

Cette stratégie vous permet d'activer ou Défender SmartScreen. SmartScreen aide avertissant les utilisateurs avant qu'ils n'i programmes potentiellement malveillan d'Internet. Cet avertissement se présente boîte de dialogue interstitielle qui s'affic d'une application téléchargée à partir d'I reconnue ou connue pour être malveilla dialogue n'est affichée pour les applicati suspectes.

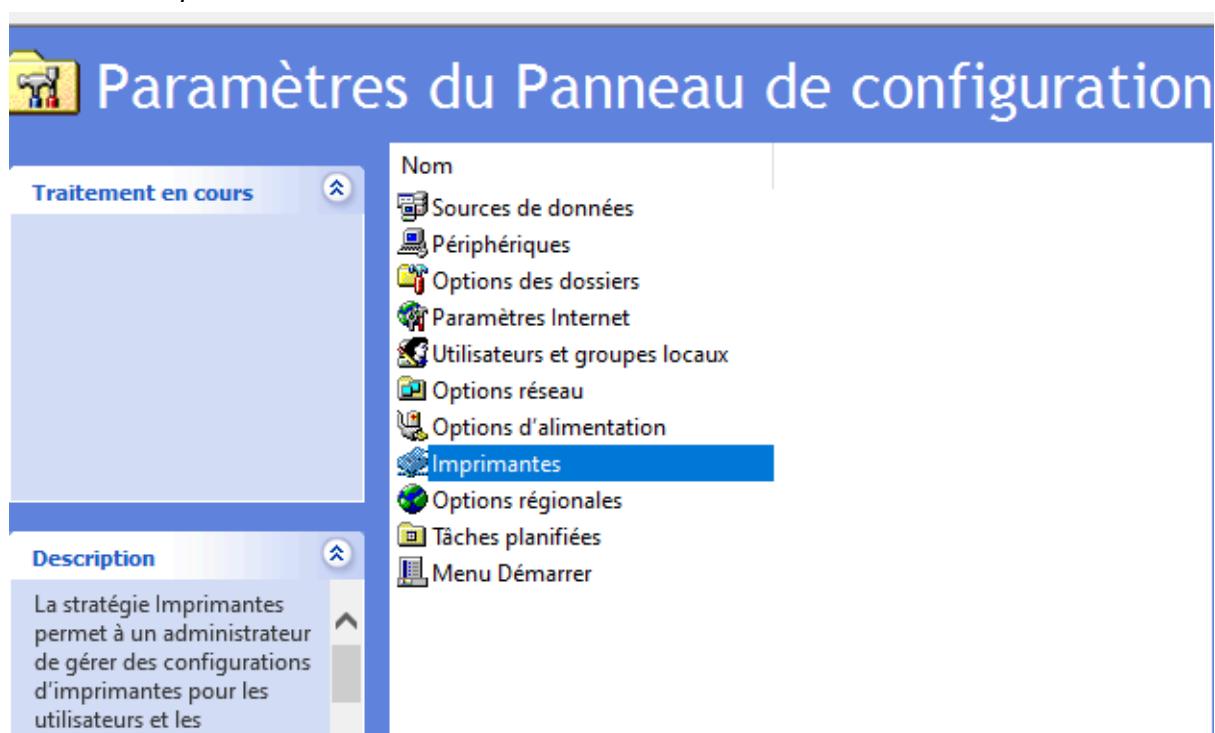
Certaines informations sont envoyées à et programmes exécutés sur les PC avec activée.

14 - UX-Printers-AutoDeploy

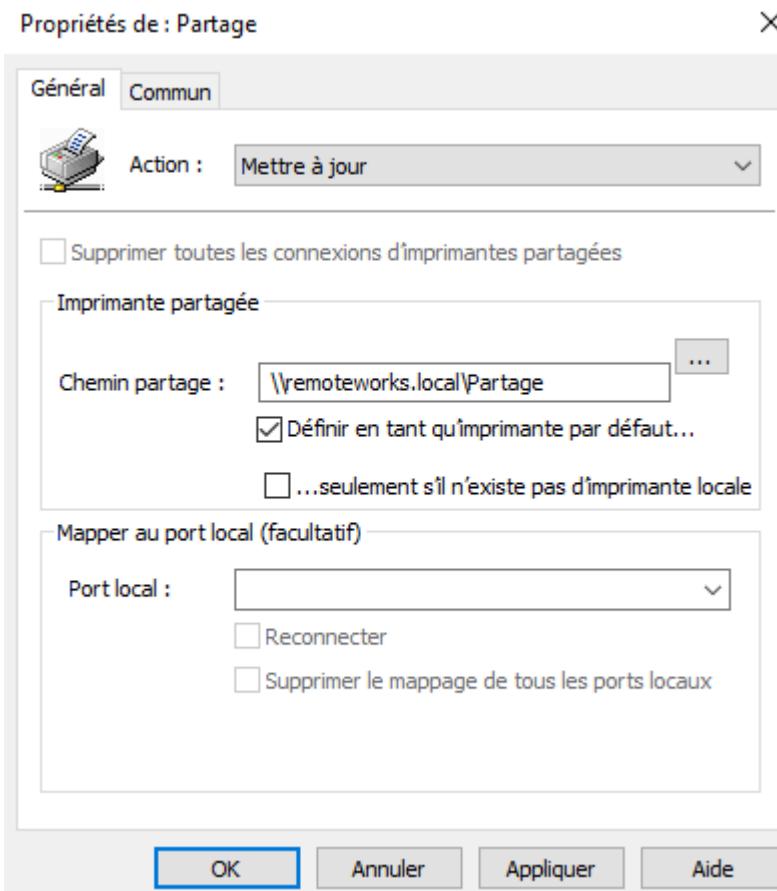
On modifie la GPO puis on se déplace dans *Configuration utilisateur > Préférences > Paramètres du Panneau de configuration*



Puis dans *Imprimantes*



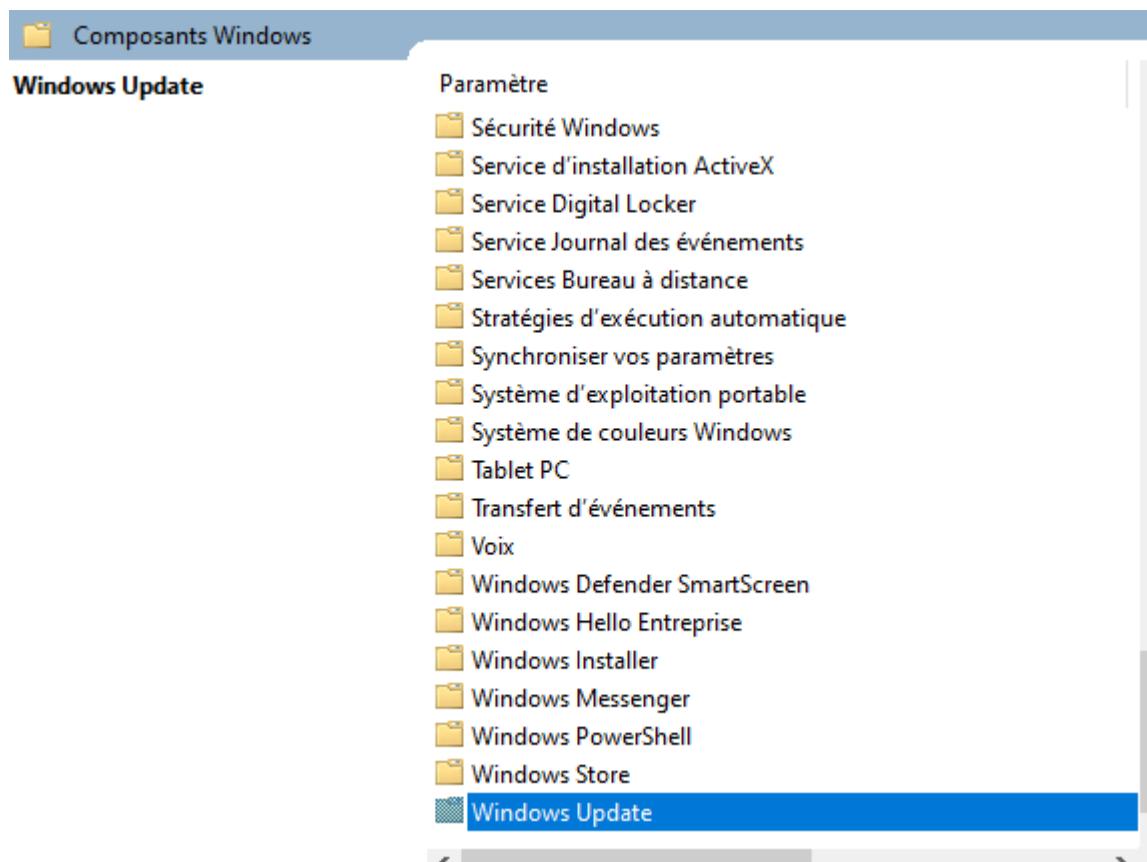
On clique droit sur Nouveau > *Imprimante Partagé*



On met l'action Mettre à jour et entre le chemin de partage de l'imprimante. On l'a définie 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.

Assistant Ajout de rôles et de fonctionnalités

Progression de l'installation

SERVEUR DE DESTINATION
WIN-9B7Q7RE201A.remoteworks.local

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

Afficher la progression de l'installation

Installation de fonctionnalité

Installation démarrée sur WIN-9B7Q7RE201A.remoteworks.local

Outils d'administration de serveur distant

- Outils d'administration de rôles
- Outils de services de fichiers
- Outils de gestion DFS

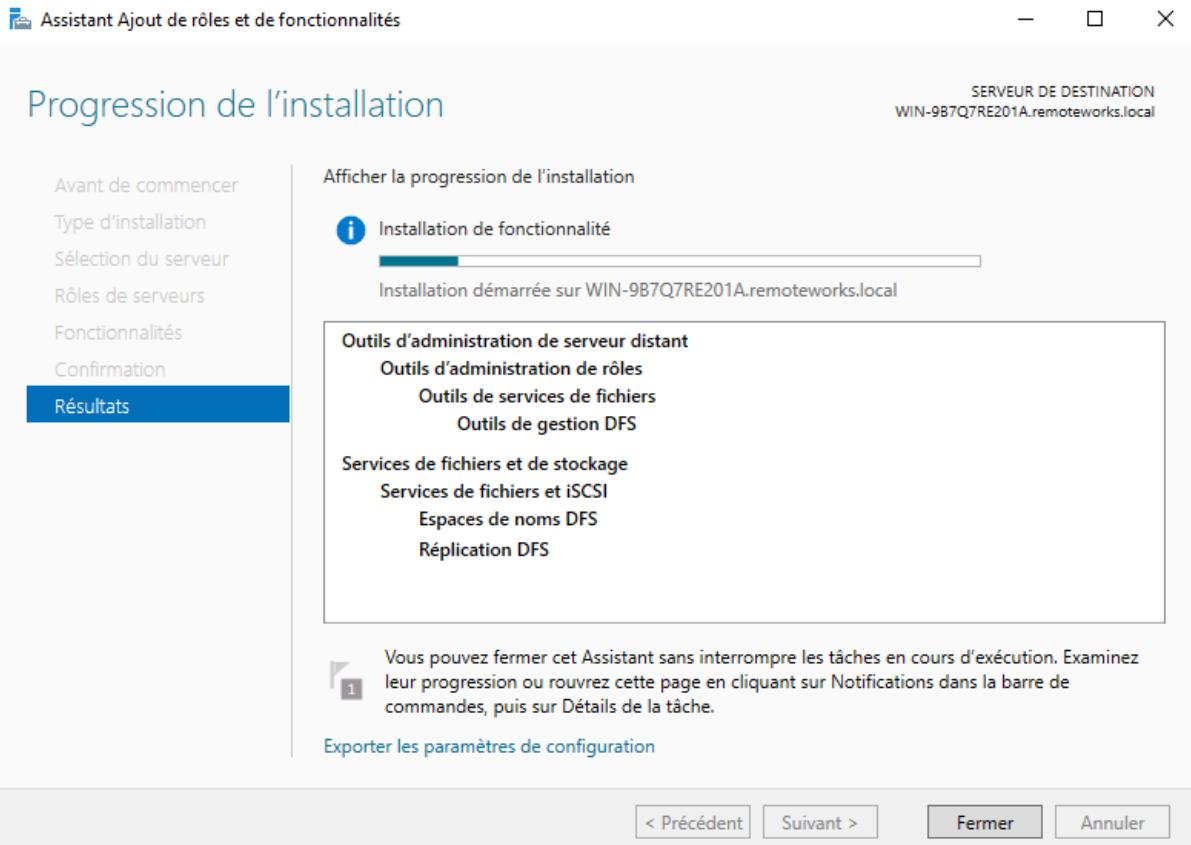
Services de fichiers et de stockage

- Services de fichiers et iSCSI
- Espaces de noms DFS
- Réplication DFS

Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

Exporter les paramètres de configuration

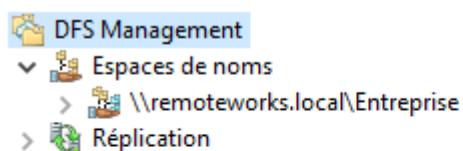
< Précédent Suivant > Fermer Annuler



Créer un Namespace DFS

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

Résultat:



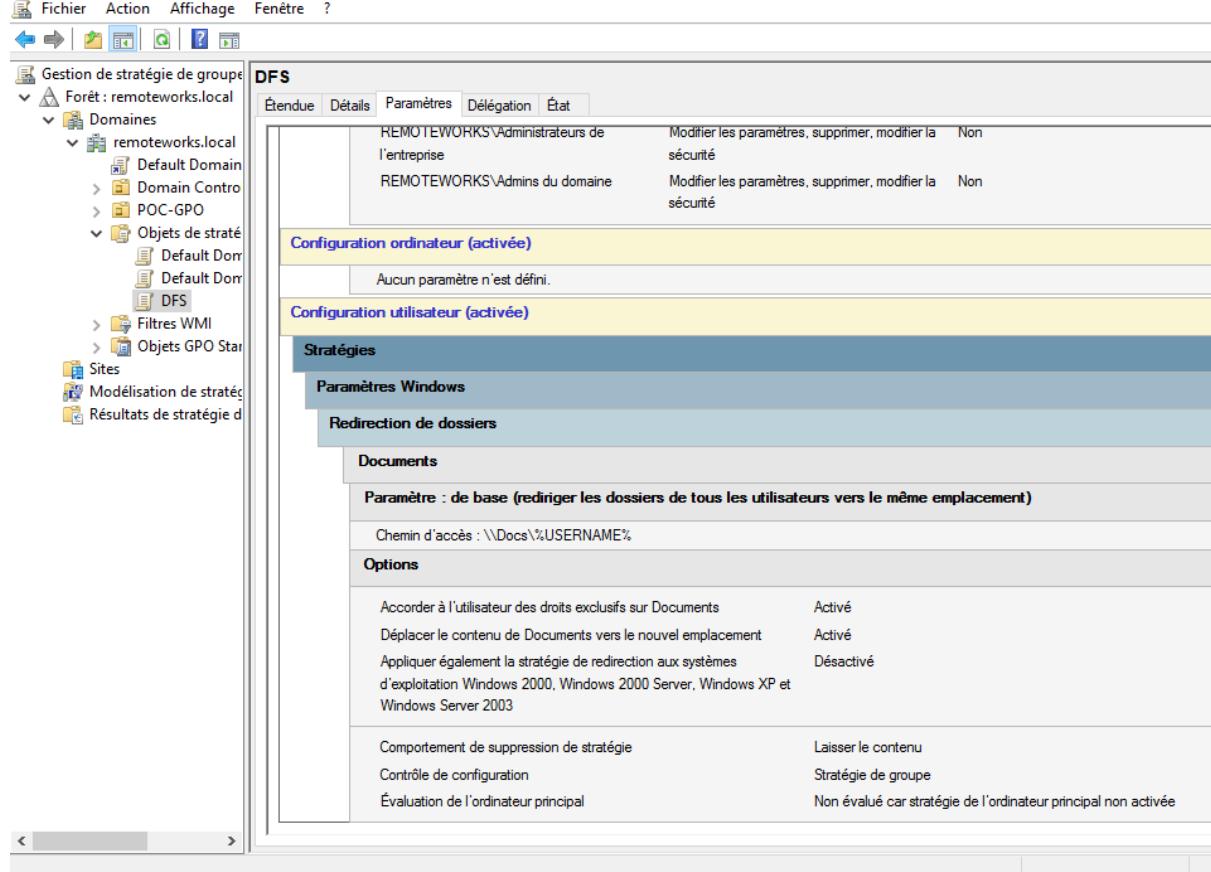
Ajouter des dossiers au Namespace

- 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

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 :

Configurer le serveur intranet de statistiques :

Définir le serveur de téléchargement alternatif :
(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 detection

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 Microsoft Update service (or alternate download server). The Automatic Updates client will search this service for updates on your network.

To use this setting, you must set two server name values: the server name that the Automatic Updates client detects and downloads updates, and the server name that workstations upload statistics. You can set both values to be the same if you want. This 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 Microsoft update service (or alternate download server) instead of the intranet Microsoft update service (or alternate download server), instead of connecting directly to the Microsoft update service. Enabling this setting means that workstations don't have to go through a firewall to get updates, and it gives users 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 connects to the Microsoft update service (or alternate download server) instead of the Microsoft update service.

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
Régie...
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.