

Cours GPO

Ecrit par **Youenn DUVAL**

Mail: youenn@barbed.fr

Linkedin: [Youenn DUVAL](#)

Derniere mise à jour : **04/12/2025**

Note

Ce support de cours est issu de différents articles issu du site [IT-Connect](#). Parce que quand on trouve un truc bien fait, pourquoi réinventer la roue! (et en licence Creative Commons)

Table des matières

1. [La console GPMC](#)
2. [Présentation de la console GPMC](#)
 1. [Default Domain Policy](#)
 2. [Default Domain Controllers Policy](#)
3. [Les conteneurs Politiques, GPC et GPT dans l'Active Directory](#)
 1. [Présentation](#)
 2. [Group Policy Container \(GPC\)](#)
 3. [Group Policy Template \(GPT\)](#)
4. [GPO : magasin central et fichiers ADM, ADMX et ADML](#)
 1. [Les fichiers ADM et ADMX](#)
 2. [Les fichiers ADML](#)
 3. [Le magasin central \(PolicyDefinitions\)](#)
 4. [Fichiers ADMX pour Windows 10](#)
 5. [Fichiers ADMX pour Office, Firefox, Chrome, etc.](#)
5. [Créer sa première GPO](#)
 1. [Créer une stratégie de groupe](#)
 2. [Créer une liaison](#)
 3. [Tester la GPO](#)
6. [Les stratégies de groupe et l'option « Appliqué » \(Enforced\)](#)
 1. [Option "Appliqué" : explications](#)
7. [Les filtres WMI : syntaxe, exemples et création](#)
 1. [Où créer un filtre WMI pour une GPO ?](#)
 2. [Filtre WMI pour cibler un système d'exploitation](#)
 3. [Associer un filtre WMI à une GPO](#)
 4. [Exemples complémentaires](#)
8. [Forcer l'actualisation des GPO à distance sur une machine](#)
 1. [Utiliser la console GPMC](#)
 2. [Utiliser PowerShell et Invoke-GPUUpdate](#)
9. [Sauvegarde et restauration des stratégies de groupe \(GPO\)](#)

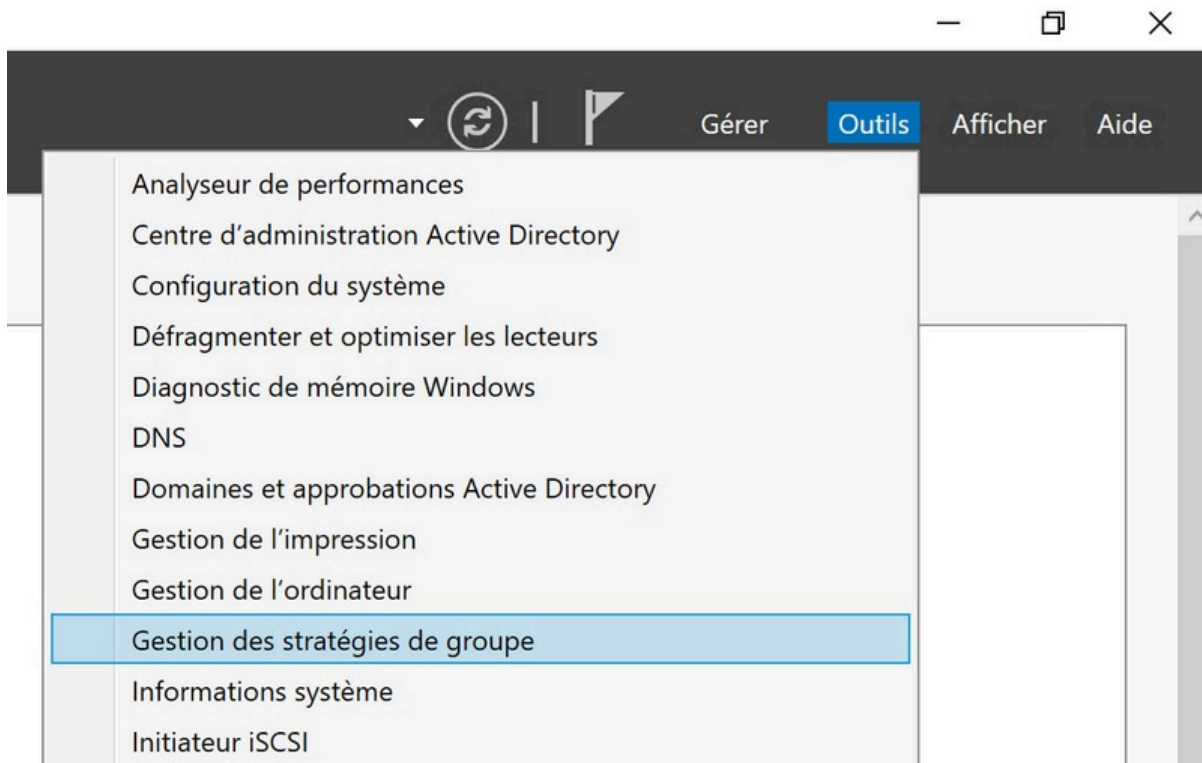
1. [Sauvegarder une GPO](#)
2. [Restaurer une GPO](#)
3. [Sauvegarder toutes les GPO avec PowerShell](#)
4. [Fusionner deux GPO](#)
10. [Comment appliquer une GPO sur un groupe spécifique ?](#)
 1. [Modifier le filtrage de sécurité d'une GPO](#)
11. [Comment bloquer une GPO pour un groupe spécifique ?](#)
 1. [Refuser l'accès à une GPO sur un groupe](#)
12. [Qu'est-ce qu'une GPO Starter ?](#)
 1. [Créer une GPO Starter](#)
 2. [Créer une GPO à partir d'une GPO Starter](#)
13. [Les préférences de stratégie de groupe](#)
 1. [Group Policy Preferences](#)
 2. [Que peut-on configurer avec les GPP ?](#)
 3. [Les différents types d'actions](#)
 1. [A. Action "Créer"](#)
 2. [B. Action "Remplacer"](#)
 3. [C. Action "Mettre à jour"](#)
 4. [D. Action "Supprimer"](#)
 4. [V. Le ciblage](#)
14. [GPO et Loopback processing](#)
 1. [Loopback processing](#)
15. [Exercice](#)
 1. [**Contexte général](#)
 2. [**Mission 1 — Analyse des besoins & rédaction d'un mini-cahier des charges**](#)
 3. [**Mission 2 — Recherche & sélection de GPO pertinentes**](#)
 1. [Sécurité du poste](#)
 2. [Corporatisme & identité visuelle](#)
 4. [**Mission 3 — Déploiement concret du POC**](#)
 5. [Livrable](#)

La console GMPC

Dans ce chapitre, je vais vous présenter **la console de gestion des stratégies de groupe, appelée également GPMC pour Group Policy Management Console**. Cette console est disponible sur tous les serveurs contrôleurs de domaine, mais elle peut être également installée sur un poste client sous Windows 10/11 (et les versions plus anciennes) grâce aux outils d'administration à distance (RSAT).

La connaissance de cette console et sa maîtrise représente une étape importante puisque nous allons l'utiliser tout au long de ce cours. En effet, il s'agit de LA console de gestion centralisée des stratégies de groupe sous Windows.

Pour commencer, ouvrez la console sur votre contrôleur de domaine : à partir du **Gestionnaire de serveur**, cliquez sur **"Outils"** puis **"Gestion des stratégies de groupe"** pour ouvrir la console.



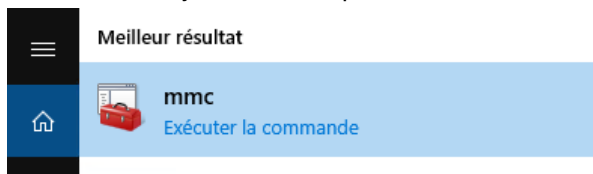
On peut l'ouvrir d'autres façon.

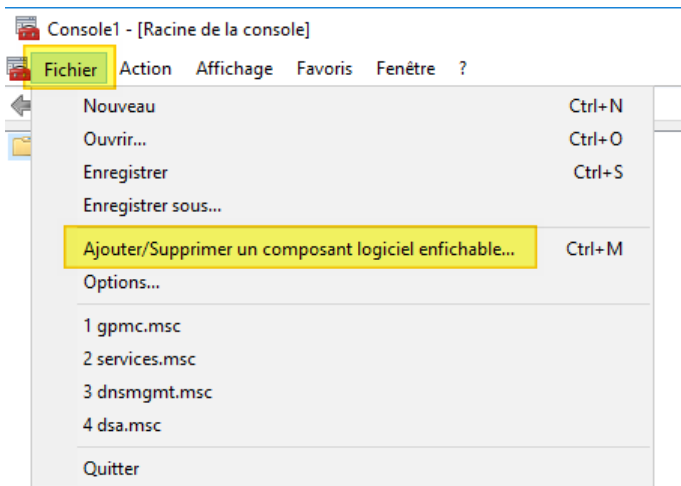
En appelant gpmmc.msc

```
Administrateur : Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Tous droits réservés.

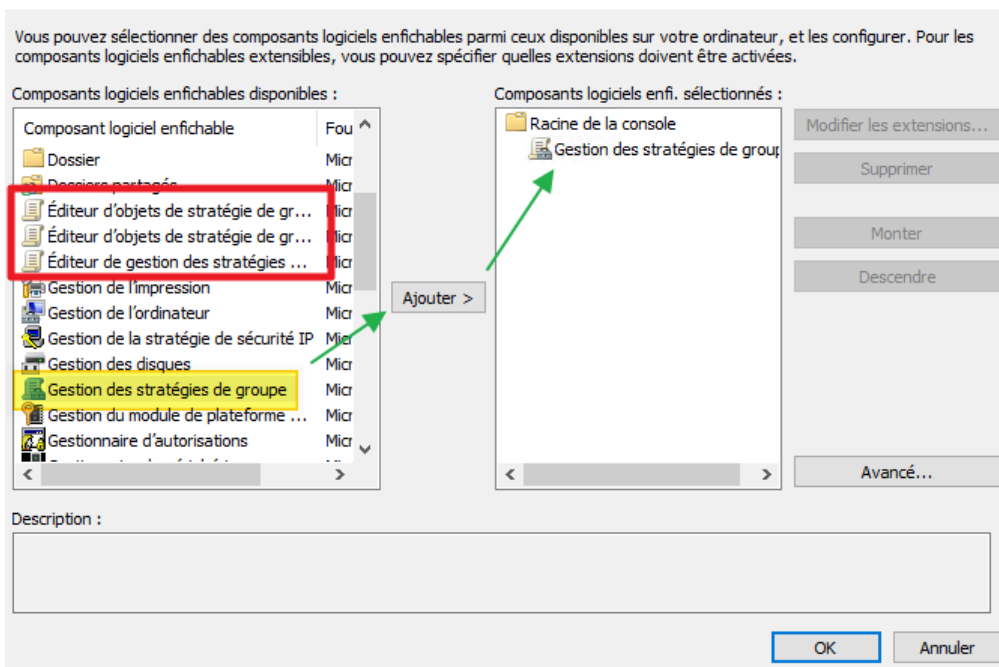
PS C:\Users\Administrateur.WIN-60QLRNDQVR7> gpmmc.msc
PS C:\Users\Administrateur.WIN-60QLRNDQVR7>
```

Ou encore en ajoutant le composant GPMC à une console MMC.





Ajouter ou supprimer des composants logiciels enfichables

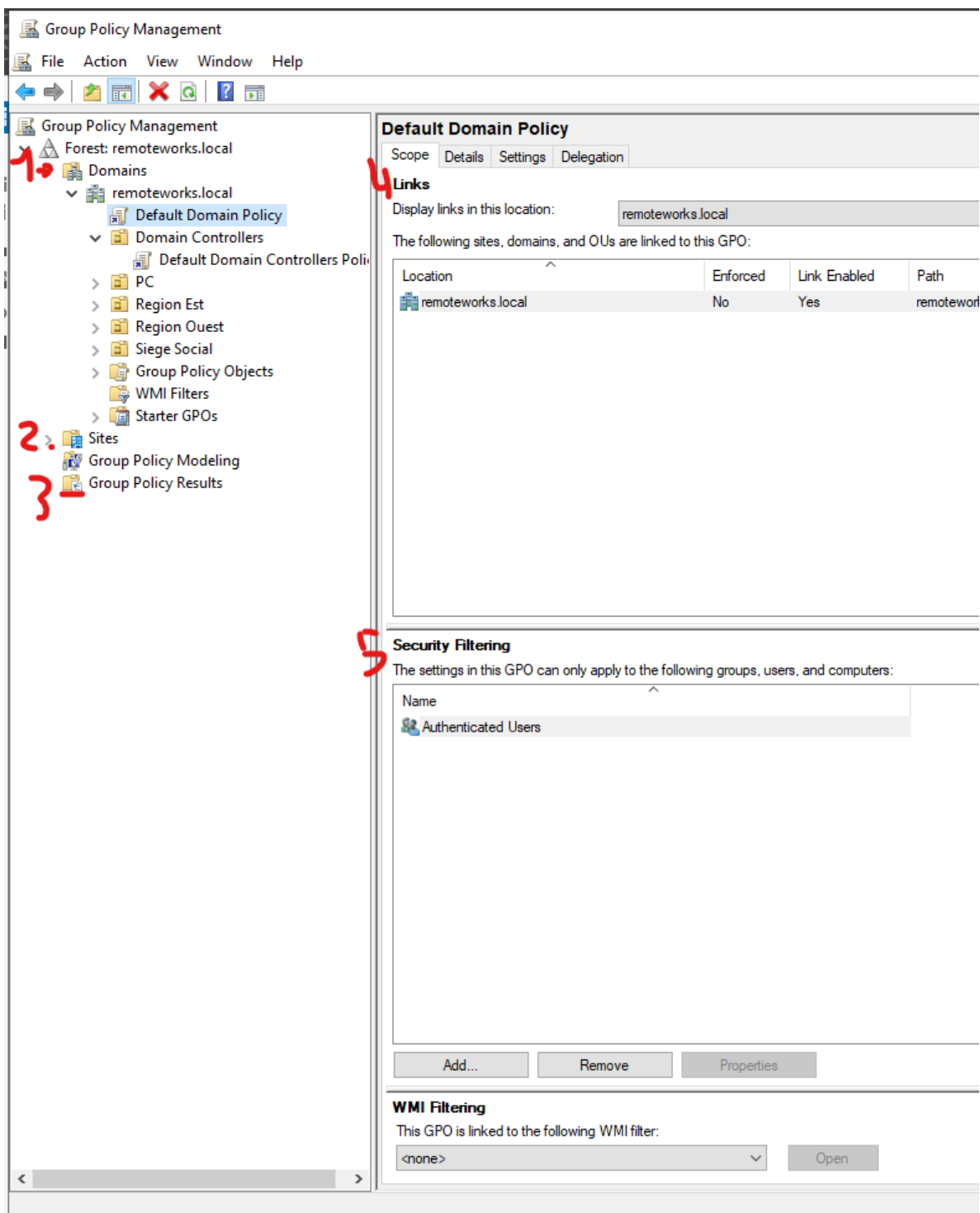


Présentation de la console GPMC

Maintenant que nous avons vu différentes façons d'accéder à cette fameuse console GPMC, je vais vous présenter les zones principales de la console. Il s'agit d'une étape importante puisque nous allons l'utiliser tout au long de ce cours.

La console suit la logique suivante : lorsque l'on sélectionne un élément sur la gauche, on accède à ses propriétés et sa configuration sur la droite.

Dans le cas d'une stratégie de groupe, cela nous donne :



[1] - Domaines : sous cette partie vous retrouvez l'ensemble des domaines de votre forêt, et pour chaque domaine l'ensemble des unités d'organisation. L'arborescence est identique à celle que vous avez définie en créant vos OU. La visualisation de cet arbre servira à venir positionner nos GPO sur les différentes OU.

Sous l'arborescence, nous apercevons notamment les deux stratégies de groupe intégrées par défaut à tout domaine Active Directory : *Default Domain Policy* et *Default Domain Controllers Policy*.

[2] - Sites : sous cette partie vous retrouvez vos différents sites Active Directory, à savoir par défaut uniquement l'élément "*Default-First-Site-Name*".

[3] - Résultats de stratégie de groupe : cette section est très importante, car elle permet d'exécuter une requête à distance sur un poste de travail pour visualiser quels sont les GPO appliquées sur ce poste et sur un utilisateur spécifique. Cela permet de récolter l'information à distance sans intervenir directement sur le poste.

[4] - Étendue, Détails, Paramètres et Délégation : ces différents onglets servent à accéder à la configuration de la GPO sélectionnée.

L'onglet "*Étendue*" sert à afficher les objets avec lesquels est liée la GPO sélectionnée, ainsi que le filtrage de sécurité et l'éventuel filtre WMI associé. Il est à noter qu'une GPO peut être liée à une OU, sans qu'elle s'applique forcément puisque le lien en lui-même peut être désactivé (d'où l'importance du champ "*Lien activé*").

L'onglet "*Détails*" affiche la date de création de la GPO, la date de dernière modification, le propriétaire, le numéro de version, l'état de la GPO et sa description si elle existe.

L'onglet "*Paramètres*" affiche tous les paramètres configurés au sein de la stratégie de groupe sélectionnée, ce qui est super pratique ! Enfin, l'onglet "*Délégation*" affiche les autorisations spécifiques sur cet objet GPO en matière d'administration.

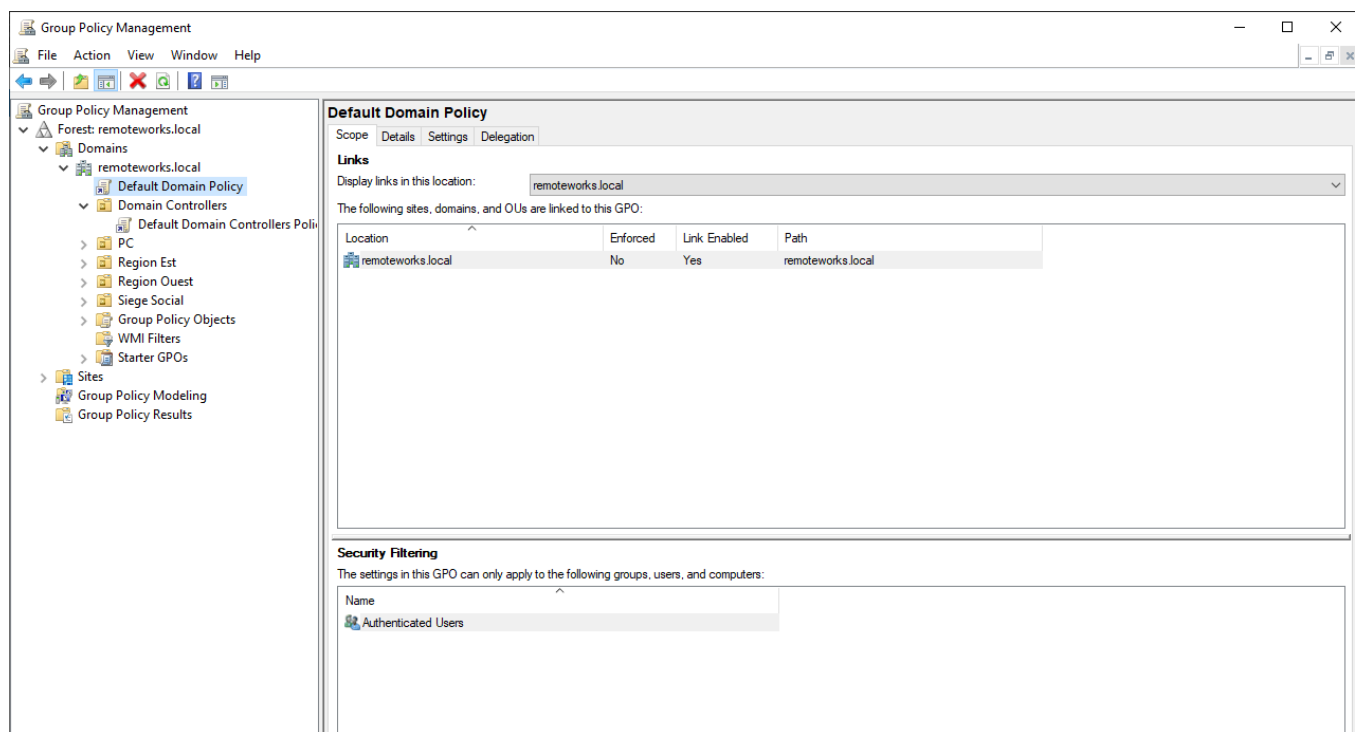
[5] - Filtrage de sécurité : de base la stratégie de groupe s'applique uniquement sur les objets enfants en fonction de son positionnement sur l'Active Directory, par exemple tous les objets enfants d'une OU. Avec le filtrage de sécurité, vous allez pouvoir appliquer la GPO uniquement sur un groupe de sécurité spécifique alors que par défaut celle-ci s'applique à tous les utilisateurs grâce au filtre "*Utilisateurs authentifiés*".

La présentation de la console va nous permettre de rentrer dans le vif du sujet afin de manipuler les différentes zones de cette console.

Default Domain Policy

La stratégie "**Default Domain Policy**" s'applique par défaut à la racine du domaine, c'est-à-dire au niveau le **plus haut**. De plus, elle contient comme filtrage de sécurité le groupe "Utilisateurs authentifiés" ce qui englobe tous les utilisateurs du domaine. **Par conséquent, ses paramètres s'appliquent à l'ensemble des ordinateurs et utilisateurs du domaine.**

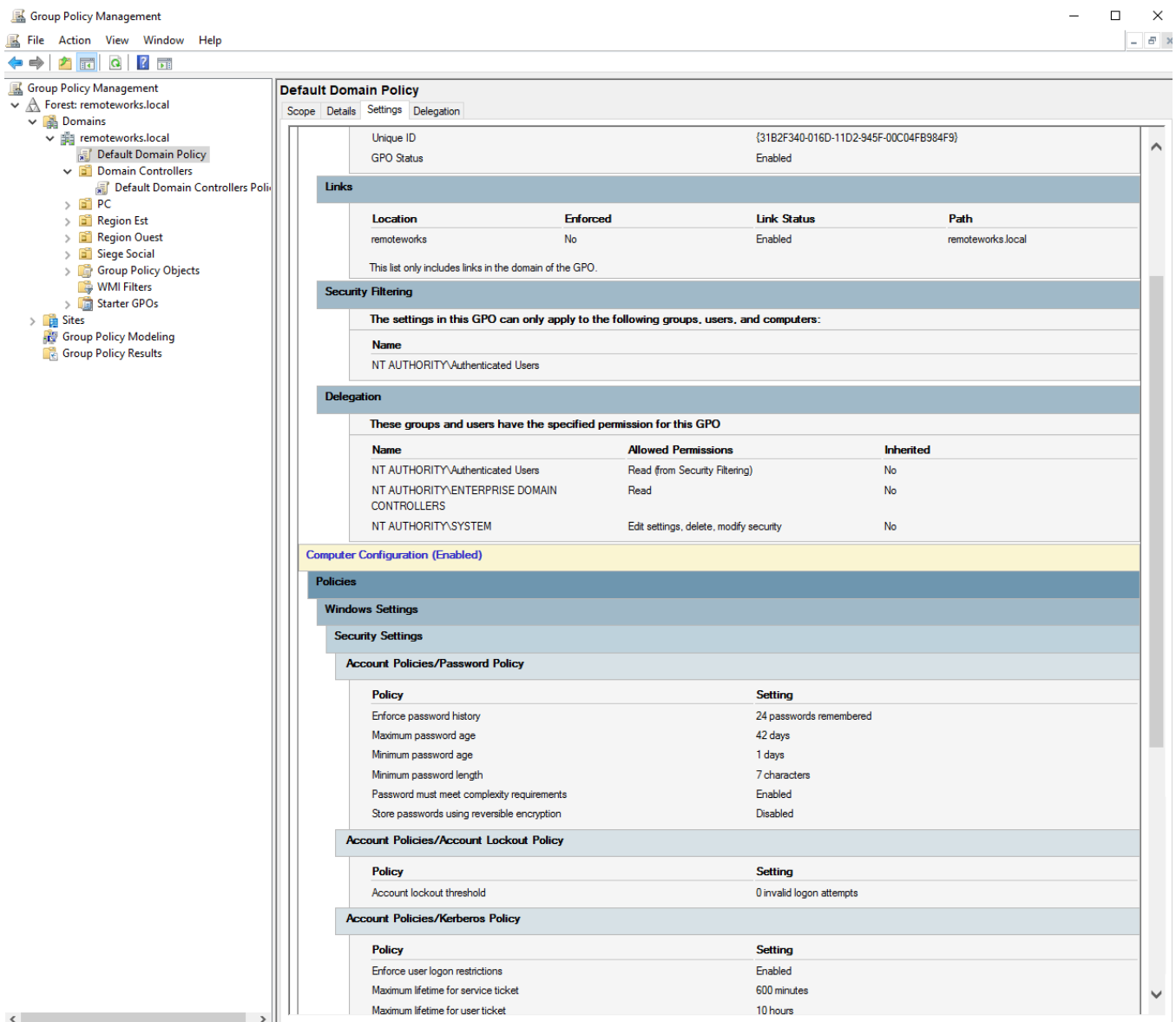
J'en profite pour préciser que lorsqu'une [GPO](#) s'affiche sous un conteneur, cela signifie qu'elle y est rattachée directement.



Que contient cette stratégie de groupe ?

La GPO "*Default Domain Policy*" contient exclusivement des paramètres de sécurité, et notamment pour la gestion des comptes utilisateurs : stratégie de mot de passe et de verrouillage de compte.

Ainsi, elle impose par défaut qu'un mot de passe soit d'une longueur minimale de 7 caractères et qu'il respecte les exigences en matière de complexité. Voici un aperçu au travers de la console GPMC :



En complément cette stratégie de groupe applique des paramètres liés à Kerberos, notamment pour définir la durée de vie maximale d'un ticket Kerberos pour un utilisateur, soit 10 heures par défaut.

Bien que cela soit tentant, pour modifier la politique de mots de passe par exemple, **il est déconseillé de modifier la stratégie de groupe par défaut**. Si vous souhaitez modifier l'un des paramètres : créez une nouvelle GPO pour le modifier. **De nombreuses entreprises modifient ces deux stratégies de groupe par défaut, c'est une mauvaise pratique très répandue.**

Default Domain Controllers Policy

Au contraire de la première stratégie de groupe native, celle-ci s'applique directement sur l'unité d'organisation "Domain Controllers". Cette OU contient les objets ordinateurs correspondants aux contrôleurs de domaine de votre

domaine. Cela signifie que **cette GPO s'applique sur les contrôleurs de domaine et c'est tout.**

The screenshot displays the Group Policy Management console. On the left, the tree view shows the hierarchy: Group Policy Management > Forest: remoteworks.local > Domains > remoteworks.local > Default Domain Policy > Domain Controllers > Default Domain Controllers Policy. The main pane shows the configuration for the 'Default Domain Controllers Policy'.

Default Domain Controllers Policy
Data collected on: 1/4/2025 3:29:58 PM

General

Details

Domain	remoteworks.local
Owner	REMOTWORKS\Domain Admins
Created	1/2/2025 12:52:16 PM
Modified	1/2/2025 2:50:02 PM
User Revisions	0 (AD), 0 (SYSVOL)
Computer Revisions	5 (AD), 5 (SYSVOL)
Unique ID	{6AC1786C-016F-11D2-945F-00C04FB984F9}
GPO Status	Enabled

Links

Location	Enforced	Link Status	Path
Domain Controllers	No	Enabled	remoteworks.local/Domain Controllers

This list only includes links in the domain of the GPO.

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

Delegation

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Local Policies/User Rights Assignment

Policy	Setting
Access this computer from the network	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\ENTERPRISE

Que contient cette stratégie de groupe ?

Dans le même esprit que la précédente GPO, celle-ci contient des paramètres de sécurité. En fait, cette GPO a pour objectif de sécuriser un minimum les serveurs ayant le rôle de contrôleur de domaine. Dès qu'un nouveau contrôleur de domaine est ajouté à votre environnement, il se retrouve dans l'OU "*Domain Controllers*" donc il va hériter des paramètres de sécurité de cette GPO.

Parmi ces paramètres, nous retrouvons par exemple :

- Qui est autorisé à éteindre le serveur ?
- Qui est autorisé à ouvrir une session locale ?
- Qui est autorisé à modifier l'heure du système ?
- Qui est autorisé à gérer le journal d'audit et de sécurité ?
- Etc...

? Bien que cela puisse paraître anodin de limiter à certains groupes la modification de l'heure du système, cela ne l'est pas du tout. Pour rappel, le contrôleur de domaine jouera le rôle de source NTP pour la synchronisation de la date et l'heure des postes clients. En cas de décalage trop important, il y aura des problèmes d'authentification entre vos postes et votre contrôleur de domaine.

En résumé, je dirais qu'il est indispensable de connaître l'utilité de ces deux stratégies de groupe intégrées nativement à l'Active Directory, mais gardez à l'esprit qu'il est préférable de ne pas les modifier.

Les conteneurs Policies, GPC et GPT dans l'Active Directory

Présentation

Dans ce chapitre, nous allons aborder la notion de Policies, GPC et GPT : des éléments indispensables au bon fonctionnement des stratégies de groupe dans un environnement Active Directory.

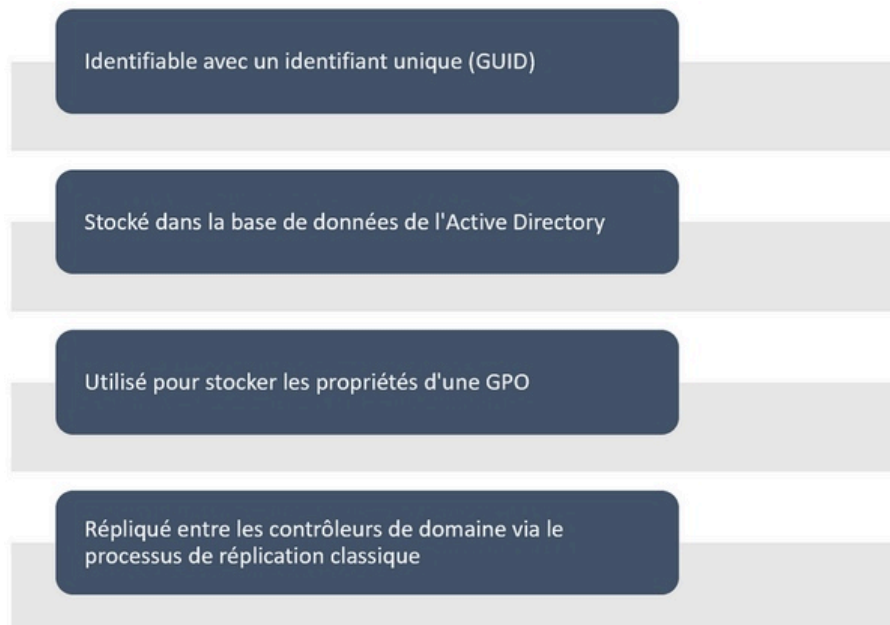
Chaque GPO est reliée à un container de stratégie de groupe appelé "*Group Policy Container*" (GPC) stocké directement dans l'Active Directory et un modèle de stratégie de groupe, en anglais "*Group Policy Template*" (GPT) qui se présente sous la forme d'un ensemble de fichiers stockés dans le répertoire SYSVOL.



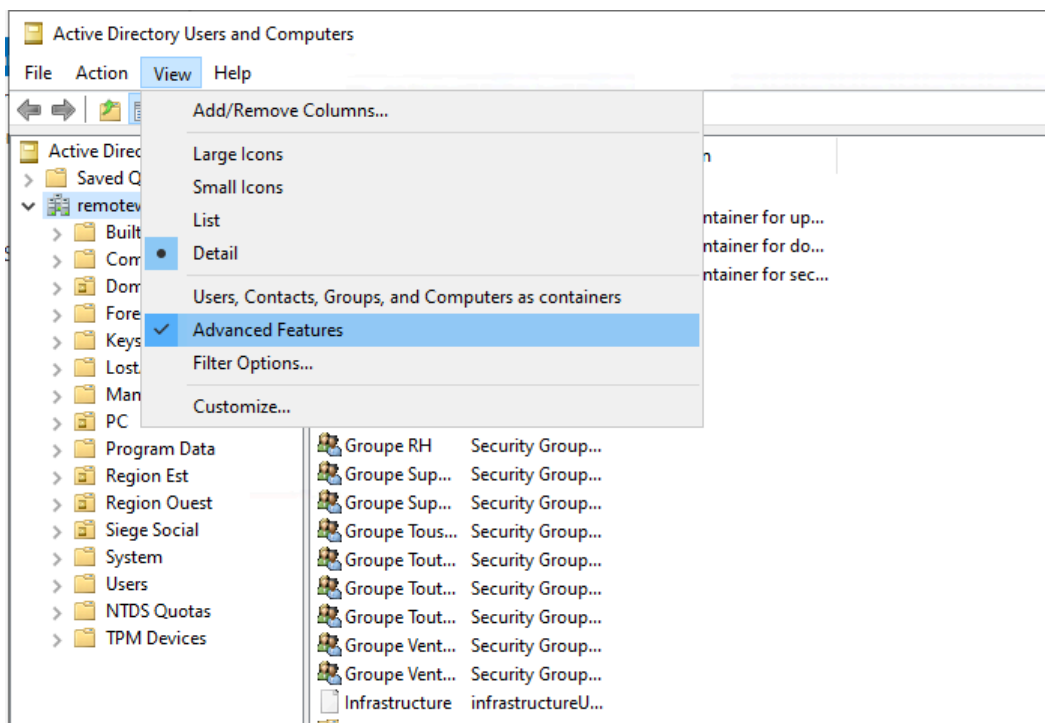
En fait, pour qu'une stratégie de groupe puisse être traitée par le poste client, deux éléments indispensables doivent être présents sur **le contrôleur de domaine qui a authentifié le poste client : le GPC et le GPT**. Pour assurer un bon fonctionnement, le GPC et le GPT de chaque GPO doivent être répliqués entre l'ensemble des contrôleurs de domaine.

Group Policy Container (GPC)

Pour chaque GPO créée, on peut utiliser la console "*Utilisateurs et ordinateurs Active Directory*" pour visualiser les informations de son container "GPC. Au niveau d'une GPO, on peut dire que le container de stratégie de groupe est :



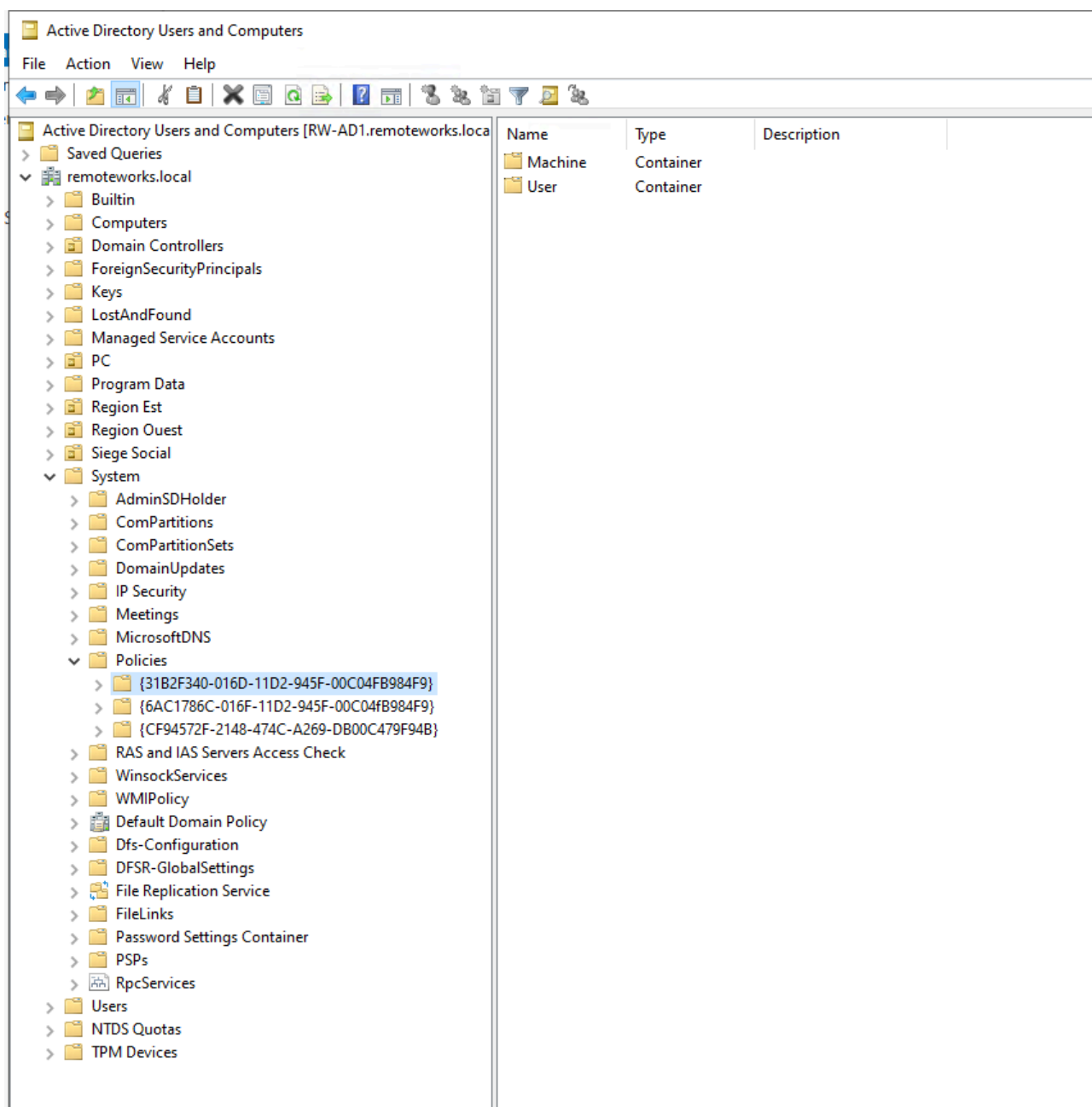
Pour voir en pratique ce que ça donne, ouvrez la console "**Utilisateurs et ordinateurs Active Directory**". Cliquez sur "**Affichage**" et "**Fonctionnalités avancées**" afin de pouvoir visualiser tous les containers de l'AD. La console va se recharger.



Parcourez comme suit : **System > Policies**.

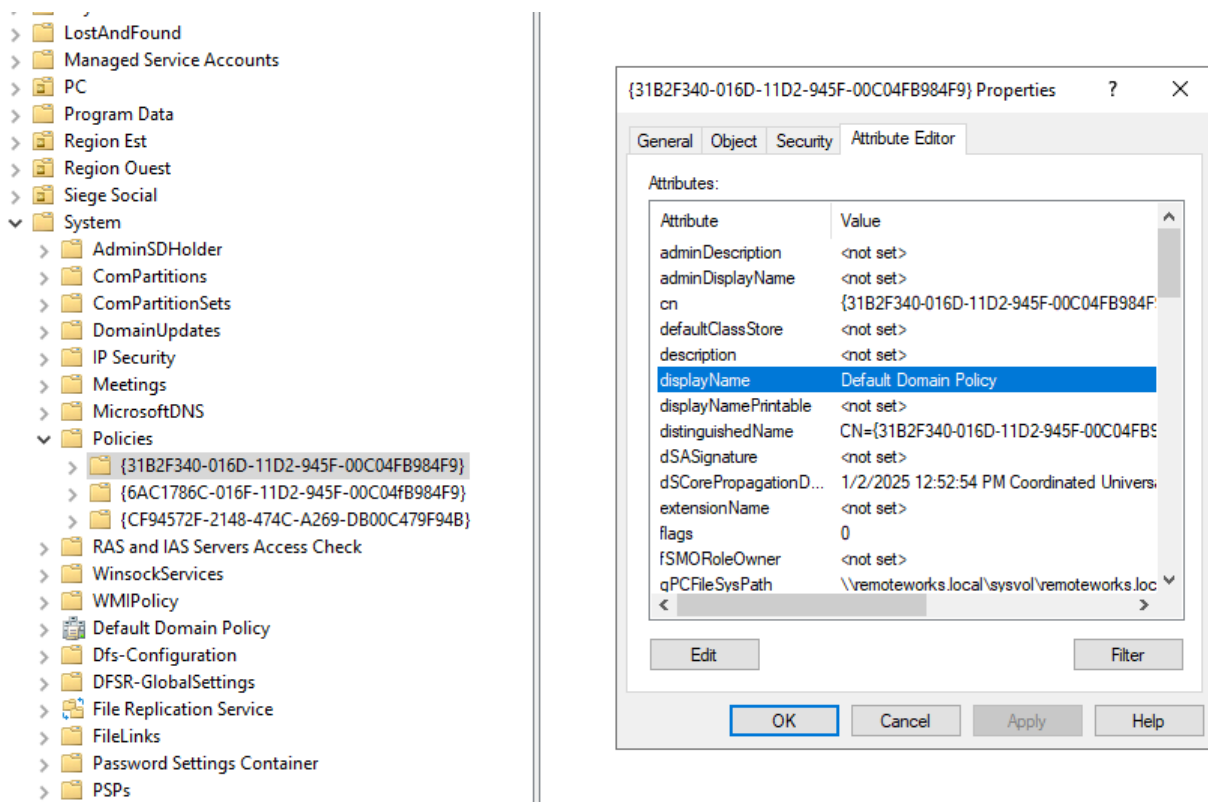
Sous "Policies", on retrouve un container par GPO, autrement dit on retrouve le GPC de chaque GPO existante sur votre domaine.

Le nom qui s'affiche, par exemple "03923E72-9557-412D-A642-781051C98BAE" sera le nom utilisé également pour le GPT au niveau de SYSVOL, mais nous verrons cela juste après.



Si vous effectuez un clic droit sur une GPO et que vous accédez aux propriétés, l'onglet "**Éditeur d'attributs**" vous donnera accès à de nombreuses propriétés au sujet de la GPO.

Simplement, nous pouvons voir le nom de la GPO c'est-à-dire le nom saisi lors de la création de l'objet via l'éditeur de stratégie de groupe. Ceci correspond à l'attribut *displayName*.



Un attribut qui est intéressant est "**gPCFileSysPath**" car celui-ci contient **le chemin vers le GPT de cette GPO**. Par exemple :

```
\\remoteworks.local\\sysvol\\remoteworks.local\\Policies\\{31B2F340-016D-11D2-945F-00C04FB984F9}
```

Enfin, l'attribut "*versionNumber*" vous donne le numéro de version de cette GPO. A chaque modification, ce numéro est incrémenté.

Intéressons-nous maintenant au *Group Policy Template* (GPT).

Group Policy Template (GPT)

Le template de stratégie de groupe (GPT) est un ensemble de fichiers et de dossiers stockés au sein du dossier partagé "SYSVOL", accessible à partir de tous les contrôleurs de domaine.

Pour la réplcation de ces éléments entre les différents DC du domaine, le service DFSR (*Distributed File System Replication*) est utilisé sur les versions récentes de Windows Server.

Identifiable avec un identifiant unique (GUID)

Stocké dans le SYSVOL

Utilisé pour stocker les fichiers de config de la GPO

Répliqué au travers de la réplcation SYSVOL

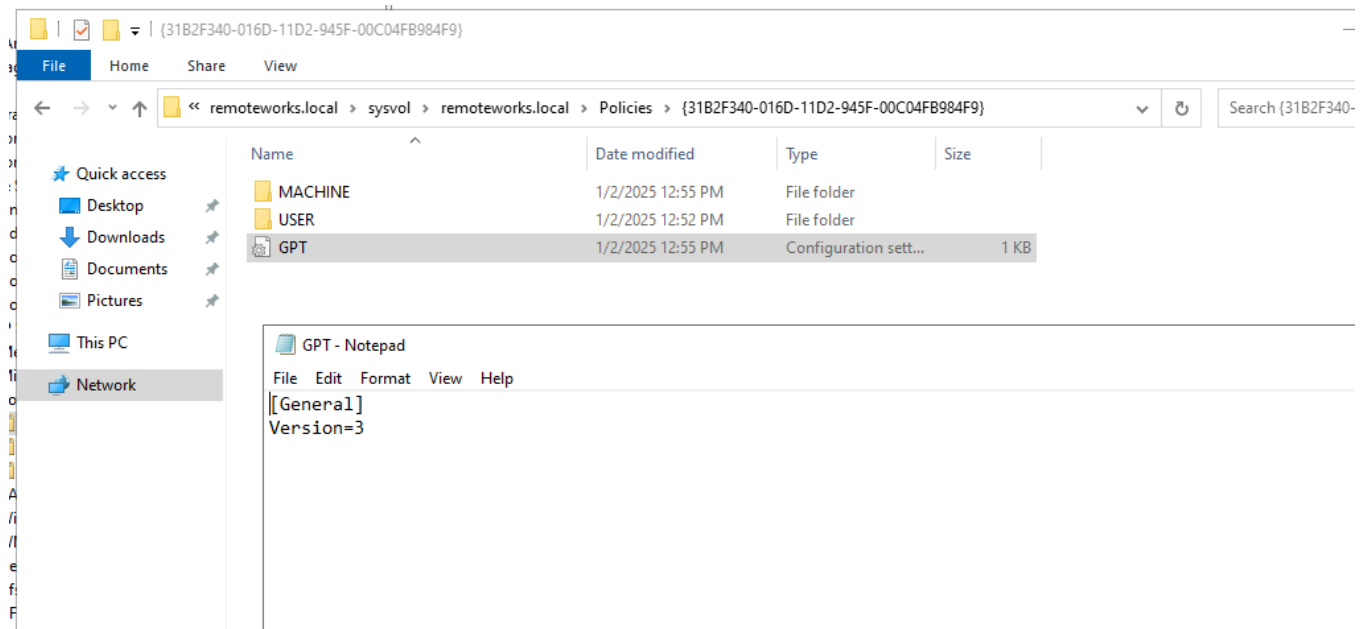
Si l'on accède au dossier SYSVOL du domaine, on remarque qu'il dispose d'un dossier "**Policies**" qui n'est pas sans rappeler le container de l'Active Directory. Par exemple, dans mon cas, cela donne le chemin suivant :

```
\\remoteworks.local\sysvol\remoteworks.local\Policies
```

Si l'on regarde à l'intérieur du dossier, on retrouve un dossier par GPO avec le même nom que l'on avait toute à l'heure dans l'AD pour chaque GPC. Au fait, **ce nom est le GUID de la GPO** 😊

À l'intérieur de chaque GPT, nous allons retrouver plusieurs éléments :

- **GPT.INI** : ce fichier contient uniquement le numéro de version du GPT, qui n'est pas forcément le même que le numéro de version du GPC. Cela va dépendre de l'état de la réplication.



- **MACHINE** : ce dossier stocke les fichiers de configuration correspondants aux paramètres de "Configuration Ordinateurs" définis dans la GPO en question.

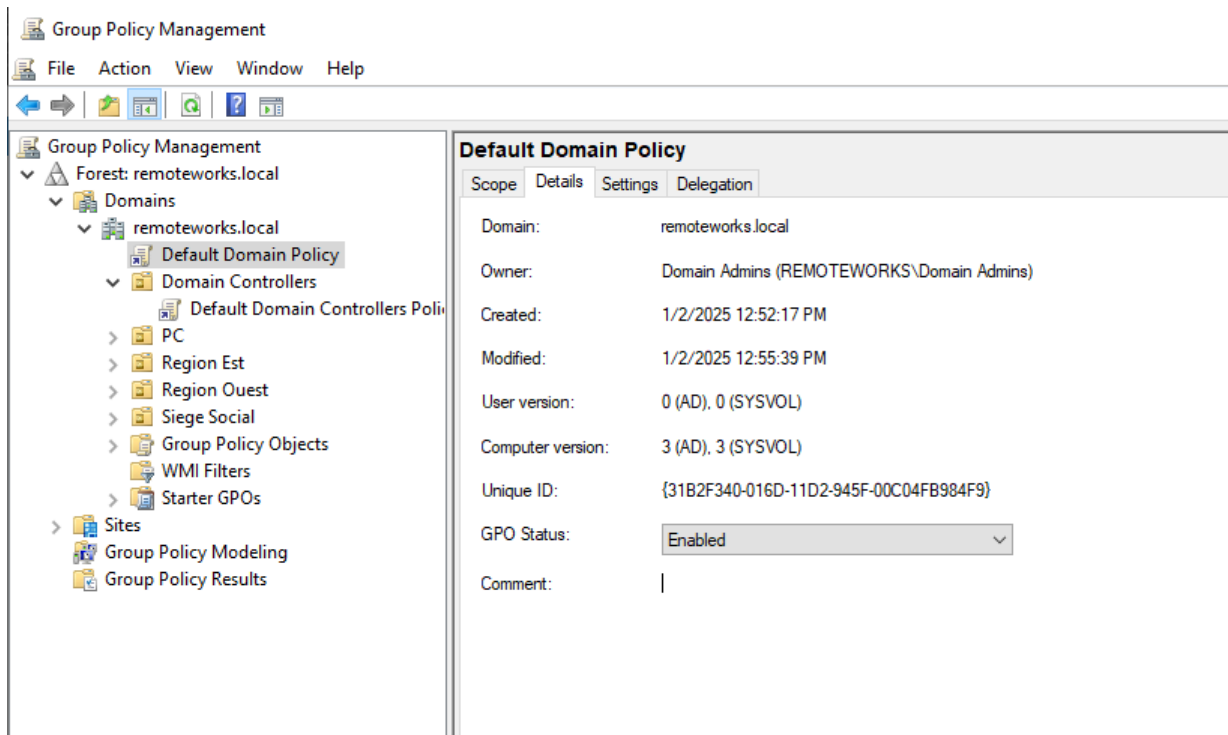
- **USER** : ce dossier stocke les fichiers de configuration correspondants aux paramètres de "Configuration Utilisateurs" définis dans la GPO en question.

Toutefois, dans les dossiers "MACHINE" et "USER" il y a le fichier "registry.pol" qui est présent dans les deux cas. Ce fichier contient les indications concernant les clés de registre à modifier, en fonction des paramètres configurés dans la GPO. A la lecture de ce fichier, le poste client sait quelle modification il doit apporter au registre.

Ensuite, nous avons par exemple les dossiers "*Scripts\Shutdown*" et "*Scripts\Startup*" sous "**MACHINE**" pour stocker un fichier Scripts.ini avec les informations sur le script à lancer, et éventuellement le script en lui-même. Dans le même esprit, nous avons pour la partie utilisateurs les dossiers "*Scripts\Logon*" et "*Scripts\Logoff*", pour les scripts liés à l'ouverture et la fermeture de session.

Pour finir ce chapitre, j'attire votre attention sur l'importance du numéro de version : il permet de savoir au poste client si une GPO a été modifiée, afin de récupérer la nouvelle version dans le cas où la version qu'il a appliquée est ancienne vis-à-vis de la version du contrôleur de domaine.

Lorsque l'on regarde les détails d'une GPO via la console GPMC, on remarque deux numéros de versions : AD et SYSVOL, ils correspondent respectivement au numéro de version du GPC et du GPT. Pour en savoir plus sur le contrôle du numéro de version, je vous orienter vers mon article à ce sujet : [GPO - Comparer les numéros de version](#)



GPO : magasin central et fichiers ADM, ADMX et ADML

Nous avons vu dans le chapitre précédent que les stratégies de groupe s'appuyaient sur un modèle de stratégie de groupe qui stockait ses fichiers dans le répertoire SYSVOL du domaine. **Maintenant, nous allons nous intéresser à d'autres fichiers utilisés pour les GPO : les fichiers ADM, ADMX et ADML, ainsi qu'au magasin central.**



Les fichiers ADM et ADMX

Windows Server est livré avec près de 200 fichiers ADMX, où chaque fichier correspond à un template d'administration. Ce fichier template va permettre d'ajouter des paramètres supplémentaires à l'éditeur de stratégie de groupe.

Par exemple, très souvent on récupère les fichiers ADMX correspondants à la suite Microsoft Office pour pouvoir configurer Word, Excel, PowerPoint, etc... À l'aide d'une GPO. Par défaut, il n'y a pas de paramètres pour la suite Office, ce qui nécessite de réaliser un import manuel.

Note

Les modèles d'administration pour Office sont disponibles en téléchargement sur le site de Microsoft, au format ADMX pour les éditions 2007, 2010, 2013, 2016 et 2019 et au format ADM pour les éditions 2000 et 2003. Preuve que le format ADM est obsolète depuis plusieurs années.

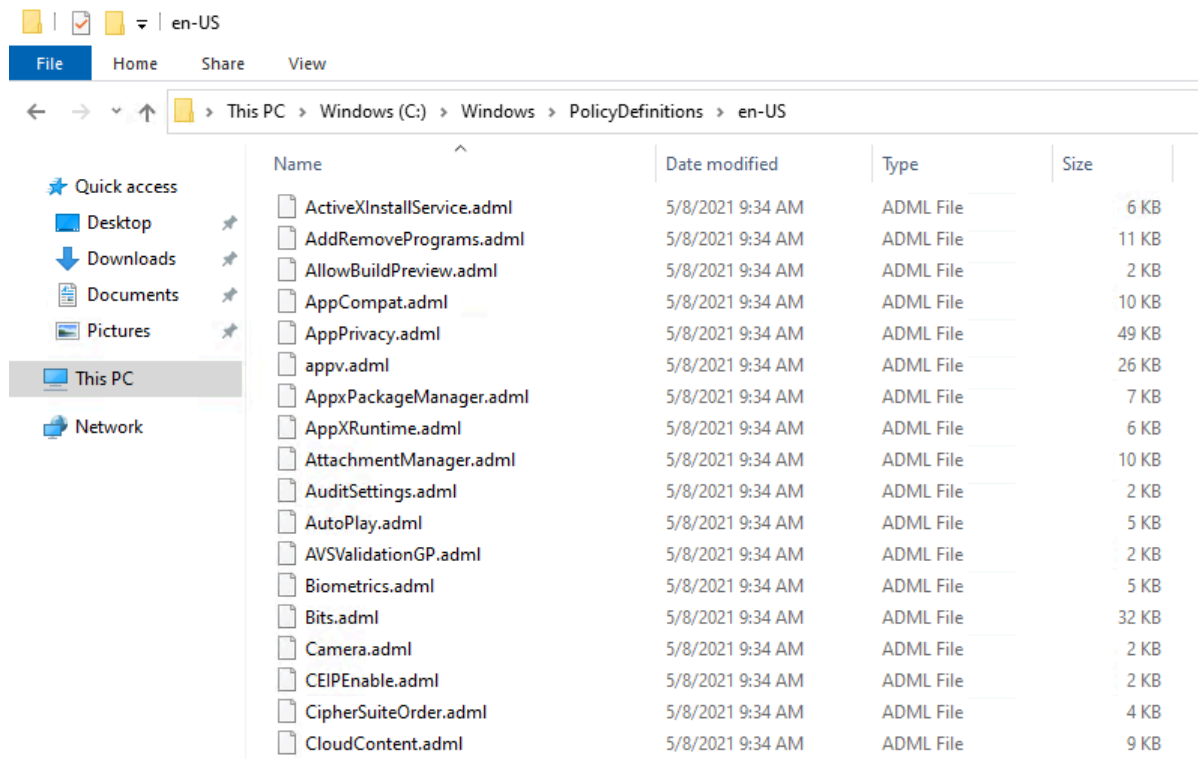
Les fichiers ADMX doivent être centralisés dans un espace de dépôt, le magasin central, que nous allons voir après, contrairement aux fichiers ADM qui sont plus contraignants. En effet, lorsque l'on utilisait les fichiers ADM, pour chaque

GPO créée, une copie du fichier ADM utilisé était copiée dans le GPT de la GPO. Cela pouvait représenter un espace de stockage important et surtout c'était lourd pour la réplication. **Résumé : les fichiers ADMX remplacent les fichiers ADM.**

Les fichiers ADML

Les fichiers ADML viennent en complément des templates d'administration (ADMX) afin de gérer la partie linguistique. Il s'agit ni plus ni moins que de fichiers de traduction.

Par exemple : lorsque Microsoft publie les fichiers ADMX pour Office, des fichiers de traduction de nombreuses langues sont intégrés au téléchargement. Ainsi, les nouveaux paramètres de GPO apparaîtront dans la langue correspondante au serveur local. Cela est appréciable lorsque la barrière de la langue est un problème.



Le magasin central (PolicyDefinitions)

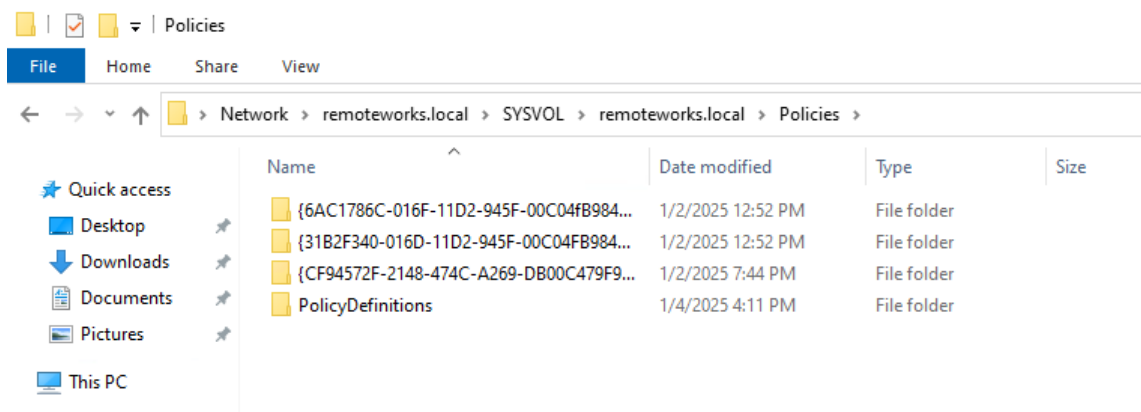
Le magasin central est un dossier qui est utilisé pour stocker les fichiers ADMX et ADML sur un domaine Active Directory. Le dossier correspondant au magasin central doit se nommer **PolicyDefinitions** et il doit être publié sur le partage SYSVOL à l'intérieur du dossier "*Politiques*" (vu précédemment pour le stockage des GPT).

Ainsi, nous devons créer le répertoire suivant :

```
C:\Windows\SYSVOL\domain\Polities\**PolicyDefinitions**
```

Quand une machine va lire les machines via le réseau, le chemin UNC sera le suivant :

```
\\remoteworks.local\SYSVOL\remoteworks.local\Polities\**PolicyDefinitions**
```



Pour pouvoir manipuler en même temps, je vous invite à créer ce dossier sur votre environnement. Cette action n'a pas d'impact sur la production. En complément et afin de pouvoir stocker les fichiers linguistiques (ADML), je vous invite à créer deux sous-dossiers :

```
en-US  
fr-FR
```

Cela nous permettra de stocker les fichiers de langue anglais et français.

Remarque :

Le magasin central inclus à Windows Server est stocké à l'emplacement suivant : **C:\Windows\PolicyDefinitions**, enfin plus précisément il utilise une variable d'environnement : `%systemroot%\PolicyDefinitions`.

Tous les fichiers ADMX et ADML natifs à Windows Server sont stockés à cet endroit. Néanmoins ce dossier est local et il n'est pas répliqué entre les contrôleurs de domaine, d'où la nécessité d'avoir un magasin central dans le dossier SYSVOL lorsque vous avez plusieurs contrôleurs de domaine.

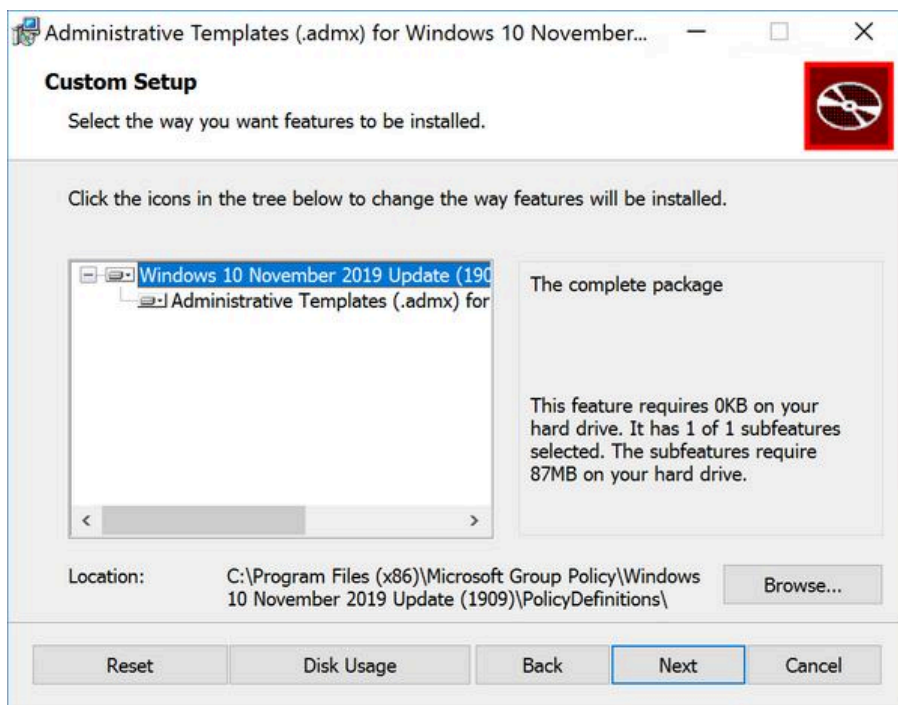
Tous les fichiers que nous allons ajouter par la suite seront à ajouter au dossier PolicyDefinitions de SYSVOL.

Fichiers ADMX pour Windows 10

À chaque fois qu'une nouvelle version de Windows 10 est publiée, Microsoft en propose pour actualiser les modèles d'administration dédiés à Windows 10. C'est l'occasion d'ajouter des paramètres supplémentaires afin d'offrir toujours plus de contrôle et possibilités avec les GPO.

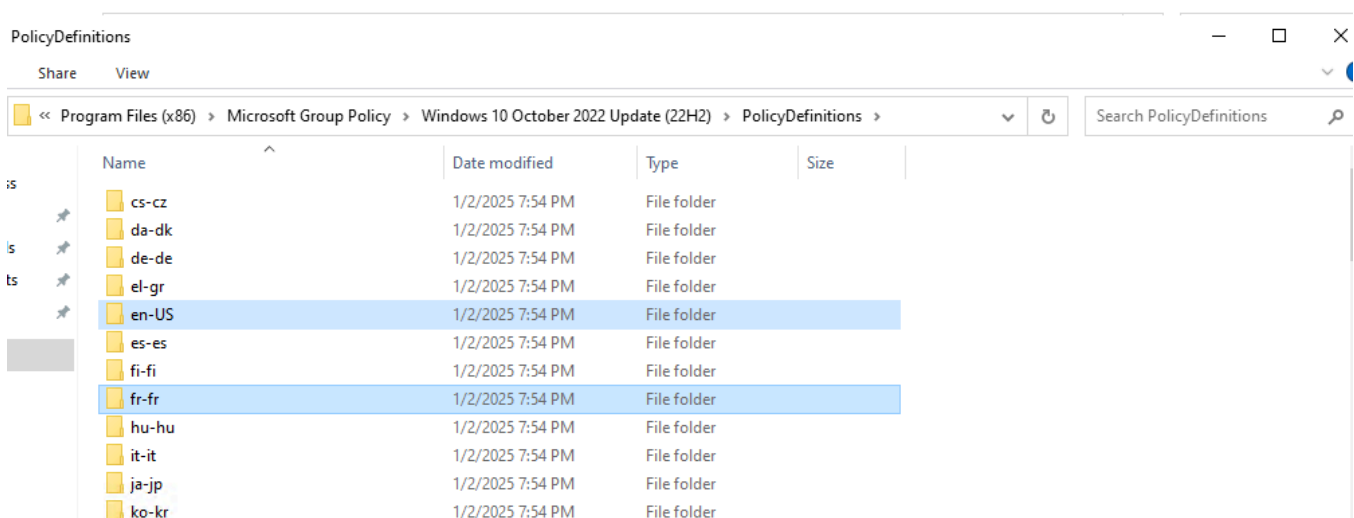
par exemple, les templates d'administration pour Windows 11 sont disponibles sur le site de Microsoft : [ADMX Windows 10](#)

Le téléchargement se présente sous la forme d'un fichier MSI, il faut réaliser l'installation sur un PC ou un serveur pour récupérer ensuite les fichiers ADMX et ADML.



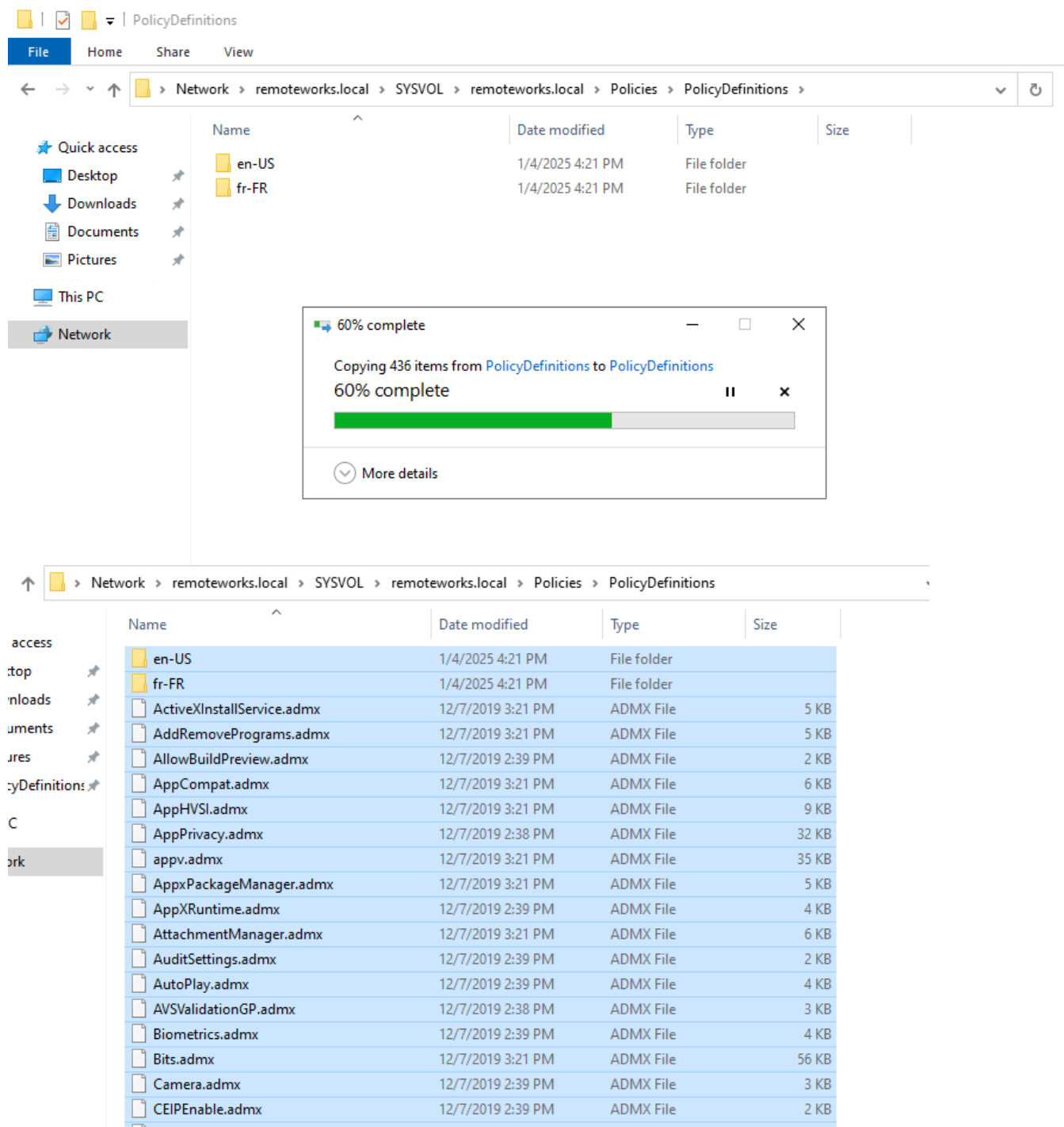
Lorsque l'installation est réalisée, les fichiers sont disponibles à l'emplacement suivant :

C:\Program Files (x86)\Microsoft Group Policy\Windows 10 October 2022 Update (22H2)\PolicyDefinitions



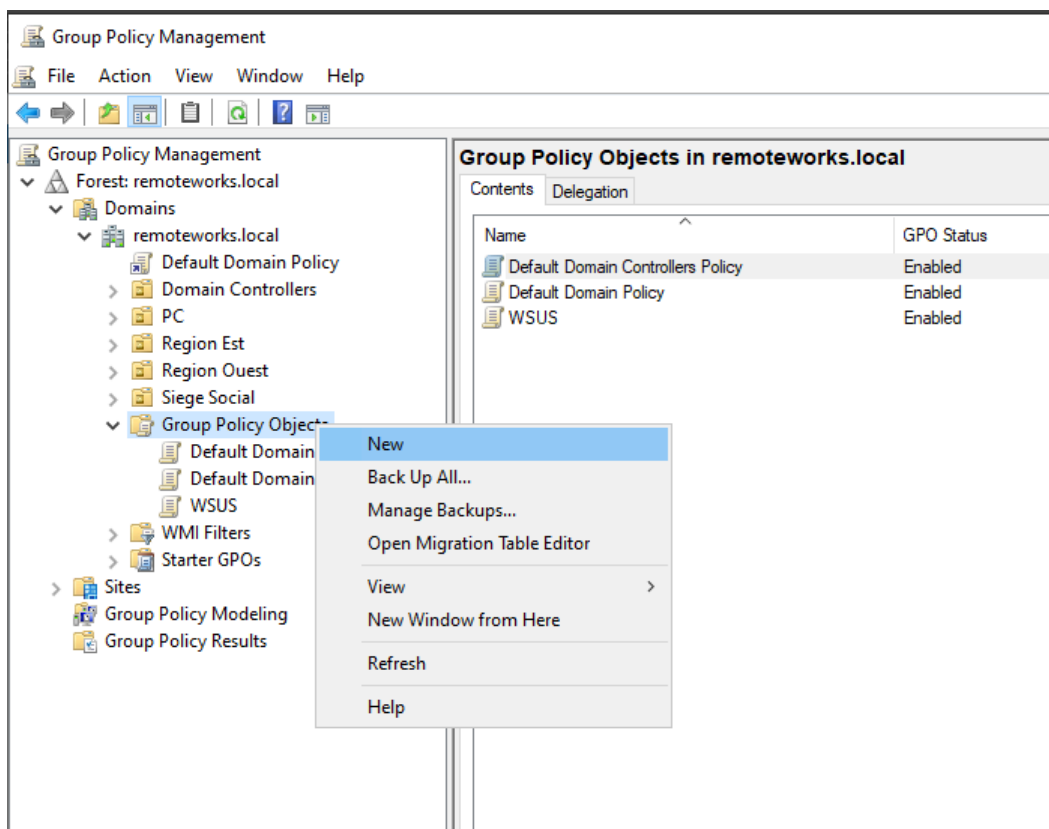
Copiez tous les fichiers ADMX, ainsi que les deux dossiers de langue "en-US" et "fr-fr" dans le dossier PolicyDefinitions. Pour rappel voici son emplacement :

\\remoteworks.local\SYSTEM\remoteworks.local\Policies\PolicyDefinitions



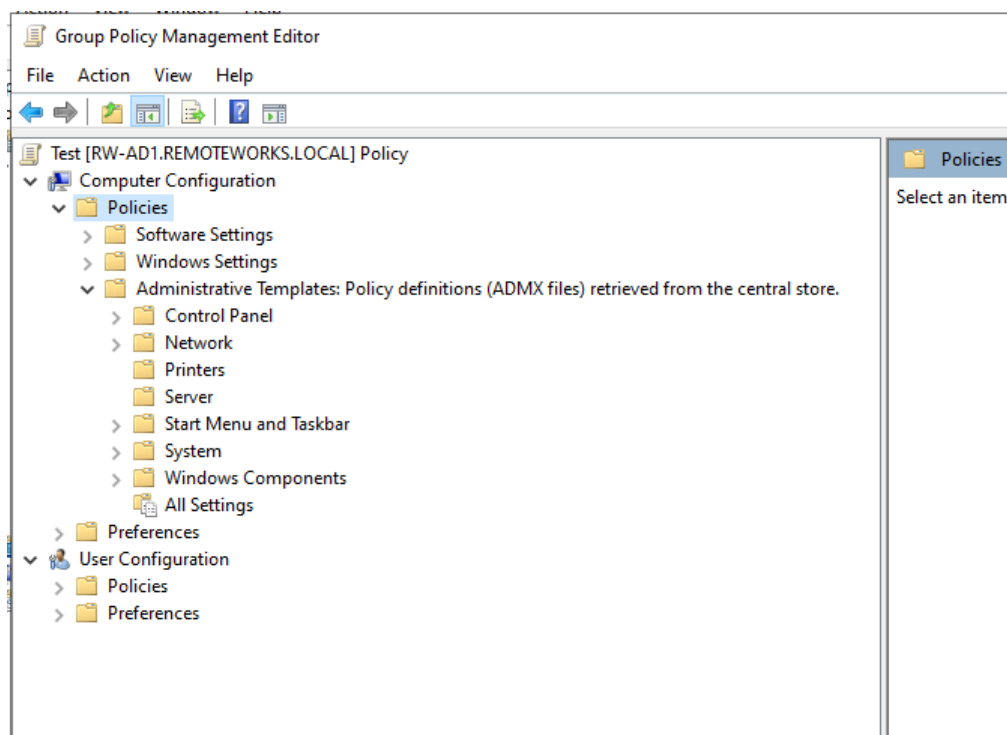
Voilà, vous venez d'importer de nouveaux fichiers ADMX sur votre domaine ! Plutôt simple.

Maintenant, si vous créez une nouvelle GPO à l'aide de la console GPMC... Via un clic droit sur "**Objets de stratégie de groupe**", puis "**Nouveau**". Donnez un nom, et ensuite modifiez la GPO via un clic droit puis "**Modifier**".



Si l'on déroule la partie "**Configuration ordinateur**" (ou Configuration utilisateur), on retrouve la partie "**Modèles d'administration**". Par défaut, dans cette partie nous retrouvons uniquement les modèles natifs et préchargés sur Windows Server. Désormais, dès que vous ajoutez des fichiers ADMX à votre dépôt centralisé, les paramètres de GPO viendront s'ajouter dans cette zone.

On remarque d'ailleurs la mention suivante : *définitions de stratégies (fichiers ADMX) récupérées à partir du magasin central*.



Les paramètres de Windows se noient un peu dans la masse, car il en existe déjà une multitude intégrée. Si l'on ajoute des fichiers ADMX pour des logiciels, ce sera visible plus facilement.

Fichiers ADMX pour Office, Firefox, Chrome, etc.

En complément de Windows, on retrouve très fréquemment en entreprise la suite Office, ainsi que les navigateurs Chrome et Firefox, voire même aussi la solution d'inventaire Fusion Inventory.

Voici quelques liens pour récupérer les fichiers ADMX associés :

- [ADMX pour Office 2016, Office 2019 et Office 365 ProPlus](#)
- [ADMX pour Mozilla Firefox \(version classique et ESR\)](#)
- [ADMX pour FusionInventory](#)
- [ADMX pour Google Chrome](#)

La procédure d'importation reste la même.

Créer sa première GPO

Jusqu'ici nous avons vu différentes notions théoriques, et nous avons vu comment utiliser la console de gestion des stratégies de groupe (GPMC) et importer des modèles d'administration. Cela nous avait d'ailleurs donné l'occasion de créer une première GPO, sans aller vraiment plus loin.

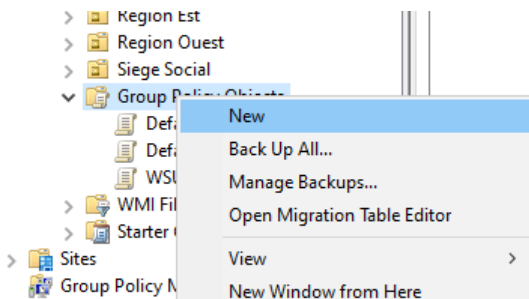
Dans ce chapitre, nous allons voir comment créer une GPO, et surtout comment configurer les paramètres qui s'y trouvent, pour enfin l'appliquer sur des utilisateurs et ordinateurs. Cela va permettre de valider ce que l'on a vu jusqu'ici avant de passer à la suite.

Créer une stratégie de groupe

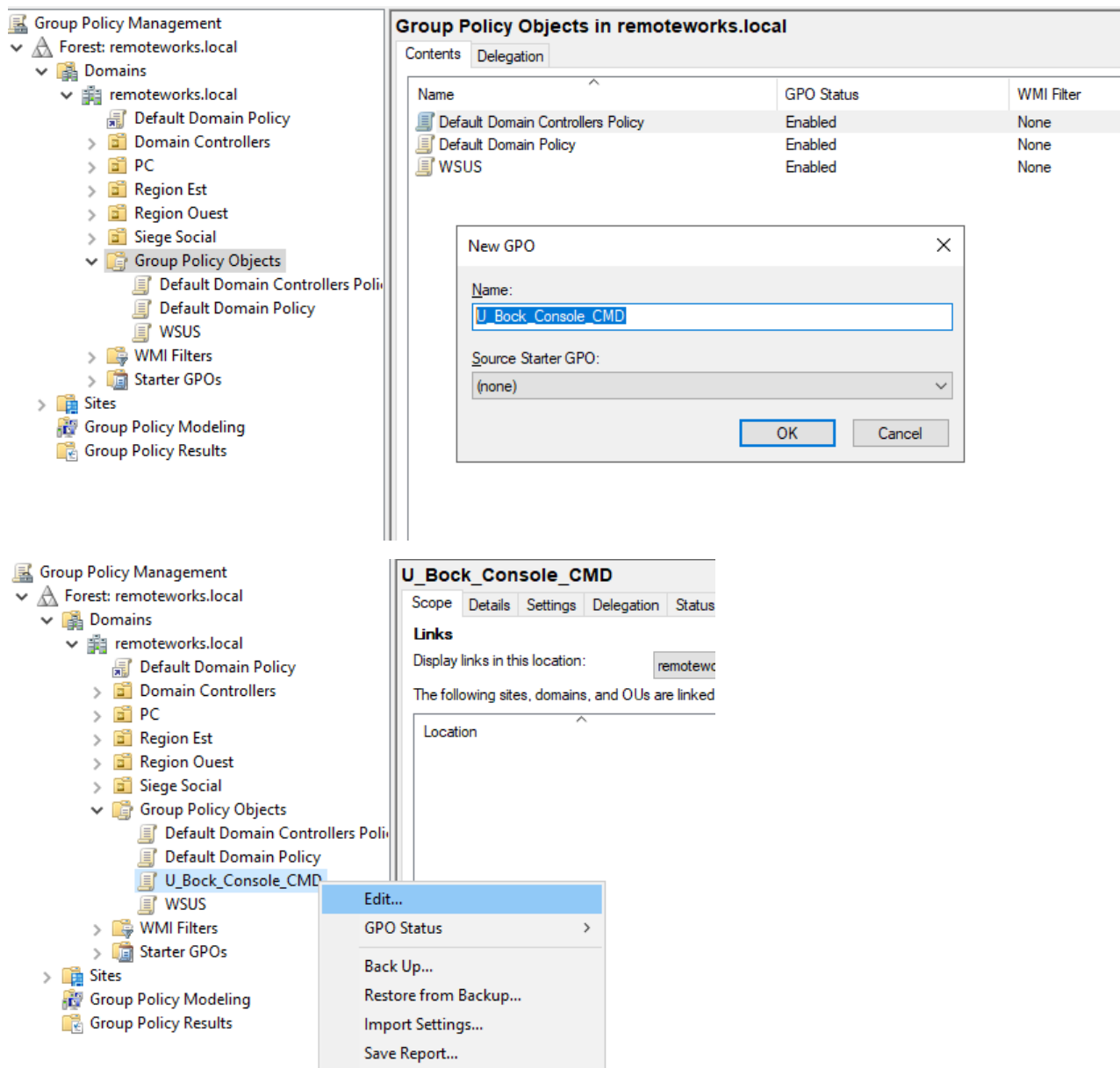
Sur votre contrôleur de domaine, ouvrez la console GPMC.

Sur "**Objets de stratégie de groupe**", effectuez un clic droit et cliquez sur "**Nouveau**".

Dans cet exemple, je vous propose de créer une stratégie de groupe pour bloquer l'utilisation de l'invite de commande (*console cmd*) dans certaines sessions utilisateurs. Cette action simple est très répandue en entreprise.



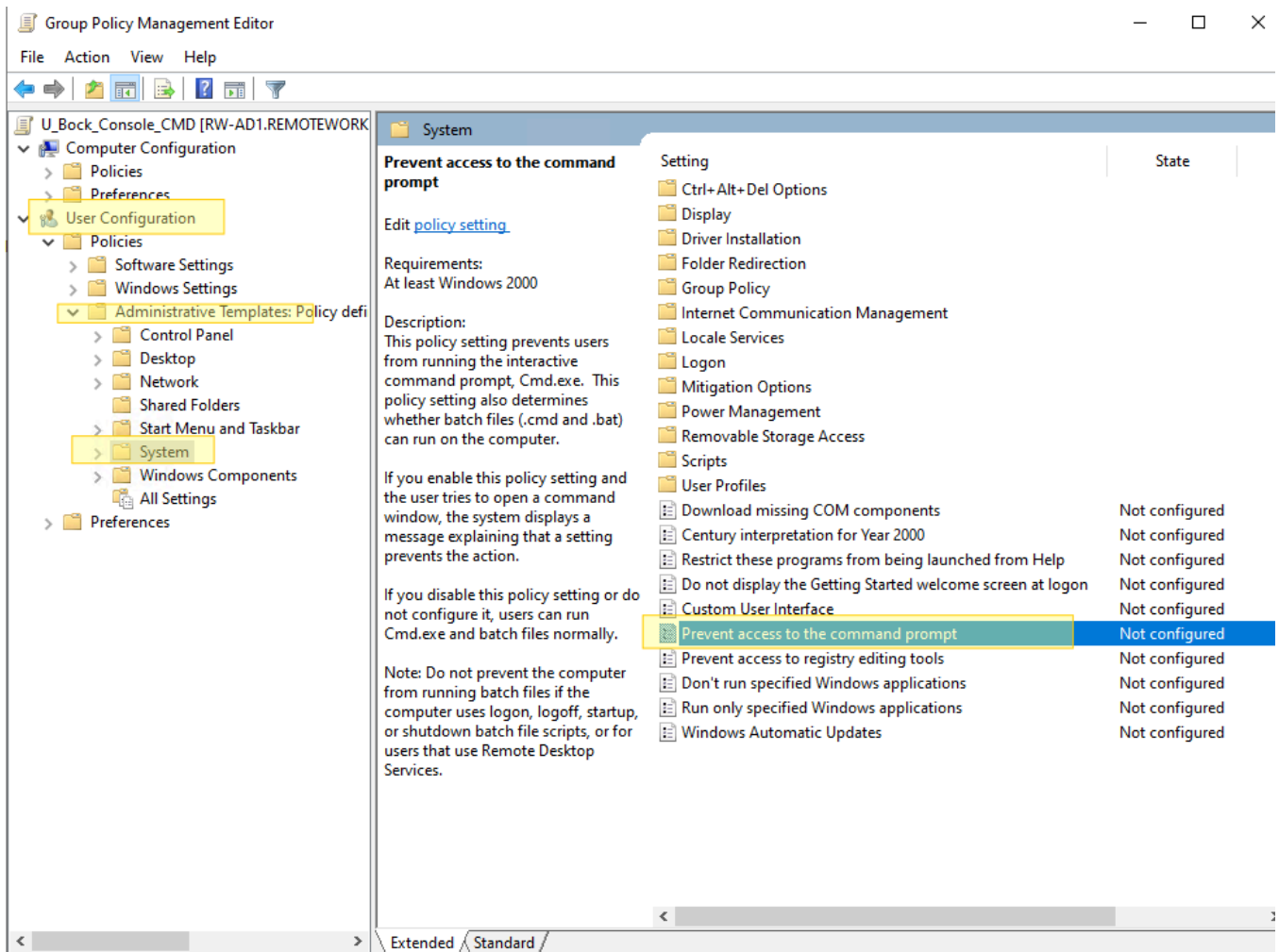
Indiquez un nom pour cette GPO, par exemple "U_Bock_Console_CMD" mais vous pouvez mettre ce que vous voulez. Le "U" étant là en préfixe pour indiquer qu'il s'agit d'une GPO qui va agir au niveau Utilisateur. Cliquez sur "OK" pour valider.



Une fenêtre "Éditeur de gestion des stratégies de groupe" va s'ouvrir, cela permet de configurer la GPO. Autrement dit, c'est ici que l'on va activer ou configurer certains paramètres à appliquer sur les utilisateurs (ou les ordinateurs).

L'objectif maintenant va être de trouver le paramètre qui permet de désactiver l'accès à l'invite de commandes. Pour cela, il n'y a pas d'autres solutions que de chercher... Mais une recherche rapide sur Internet est souvent efficace pour trouver le nom du paramètre au sein d'un tuto ou sur un forum...

Voici le chemin vers notre fameux paramètre : **Configuration utilisateur > Stratégies > Modèles d'administration > Système > Désactiver l'accès à l'invite de commandes**. Double-cliquez dessus.



Les fenêtres de configuration sont présentées de la même façon pour la majorité des paramètres. Nous retrouvons tout d'abord dans le haut, deux boutons : "*Paramètre précédent*" et "*Paramètre suivant*" pour naviguer entre les paramètres sans fermer et rouvrir une nouvelle fenêtre.

Nous avons également le champ "**Pris en charge sur :**" qui donne des indications (plus ou moins précises) sur la compatibilité de ce paramètre avec les différentes versions de Windows [1].

Juste à gauche, nous avons trois boutons, que vous retrouverez sur tous les paramètres que l'on pourrait qualifier de "booléen" : **soit on active, soit on désactive, ou alors on ne configure pas et dans ce cas c'est le paramétrage par défaut de Windows qui s'appliquera** (à moins que ce paramètre soit géré dans une autre GPO).

L'aide [2] indiquée en dessous à droite, **va vous expliquer quel sera l'impact si ce paramètre est activé, désactivé ou si il n'est pas configuré** (le comportement par défaut sera indiqué). Cette aide est vraiment très utile !

Enfin, certains paramètres proposent des options. C'est le cas de celui-ci. Si vous activez ce paramètre, il ne sera pas possible d'utiliser la console CMD avec les comptes utilisateurs ciblés. Néanmoins, l'option "**Désactiver également le traitement des scripts d'invite de commande**" est intéressante puisqu'elle permet (lorsqu'elle est définie sur "Non") d'autoriser l'exécution des scripts CMD.

Par exemple : si vos utilisateurs doivent exécuter un script de connexion qui va monter des lecteurs réseau, il ne faudra pas désactiver cette option.

Concernant, notre configuration, activez ce paramètre et validez.

Prevent access to the command prompt

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on: At least Windows 2000

Options:

Disable the command prompt script processing also?

No

Help:

This policy setting prevents users from running the interactive command prompt, Cmd.exe. This policy setting also determines whether batch files (.cmd and .bat) can run on the computer.

If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.

If you disable this policy setting or do not configure it, users can run Cmd.exe and batch files normally.

Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Remote Desktop Services.

OK Cancel Apply

Vous pouvez fermer ensuite la console de modification de cette GPO.

Vous revoilà dans la console GPMC : cliquez sur la GPO "U_Bloquer_Console_CMD", puis sur la droite cliquez sur l'onglet "Paramètres". **Déroulez ensuite sous "Configuration utilisateur", vous verrez que cela offre la possibilité de voir rapidement la configuration contenue dans cette GPO.**

The screenshot shows the Group Policy Management console with the 'U_Bock_Console_CMD' GPO selected. The left pane shows the hierarchy: Forest: remoteworks.local > Domains > remoteworks.local > Group Policy Objects > U_Bock_Console_CMD. The right pane shows the configuration details for this GPO.

U_Bock_Console_CMD

Scope: Details Settings Delegation Status

Details

Domain	remoteworks.local
Owner	REMOTWORKS\Domain Admins
Created	1/4/2025 4:30:56 PM
Modified	1/4/2025 4:36:00 PM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	0 (AD), 0 (SYSVOL)
Unique ID	{1B8B3CD-4C55-46FA-BCF4-C958646DF6F6}
GPO Status	Enabled

Links

Location	Enforced	Link Status	Path
None			

This list only includes links in the domain of the GPO.

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

Delegation

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No
REMOTWORKS\Domain Admins	Edit settings, delete, modify security	No
REMOTWORKS\Enterprise Admins	Edit settings, delete, modify security	No

Computer Configuration (Enabled)

No settings defined.

User Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

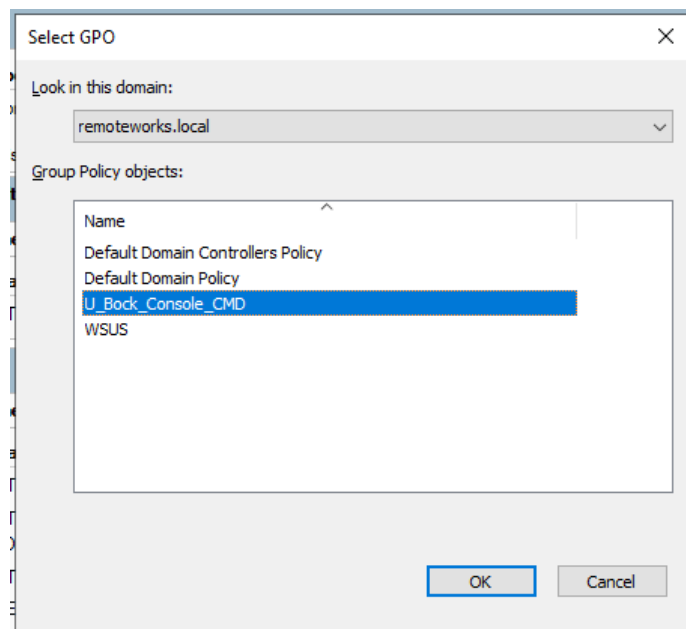
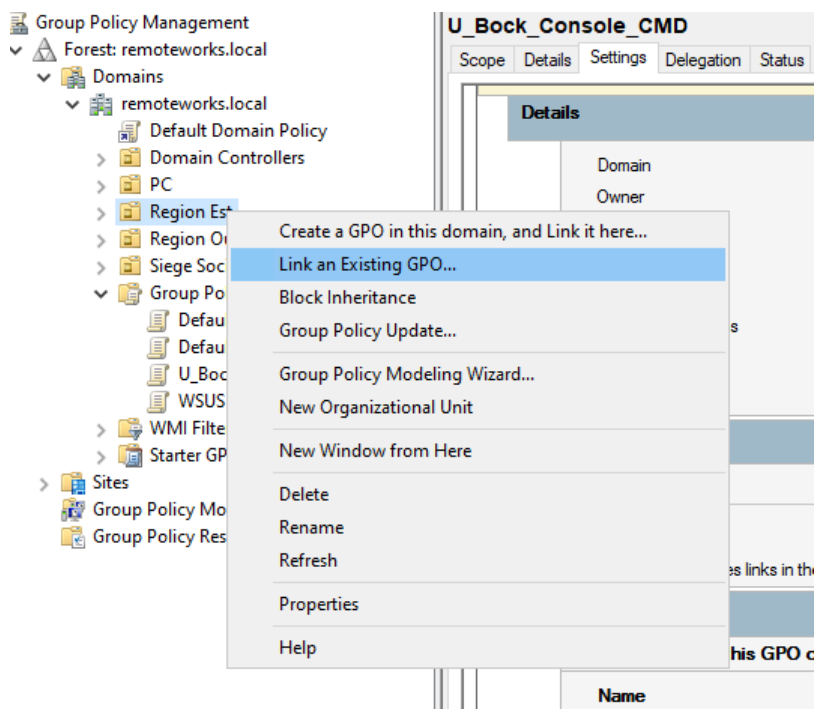
Policy	Setting	Comment
Prevent access to the command prompt	Enabled	
Disable the command prompt script processing also?	No	

Créer une liaison

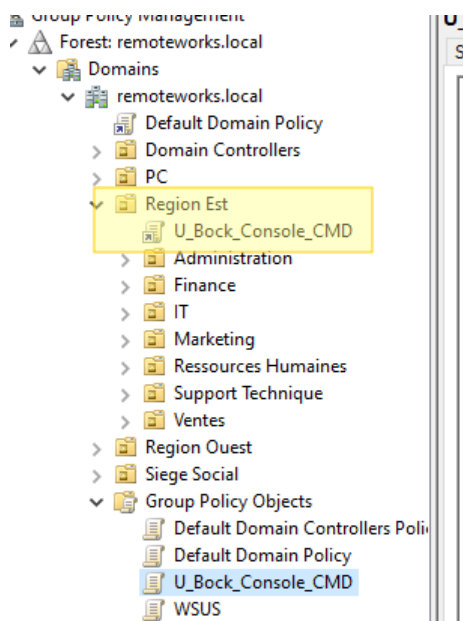
En l'état, notre stratégie de groupe ne sert à rien puisqu'elle s'applique sur aucun objet. Il va falloir la positionner au niveau de l'annuaire [Active Directory](#) : soit sur le domaine pour bloquer CMD dans toutes les sessions (pas top pour les sessions Administrateurs), soit sur une ou plusieurs OU spécifiques.

Par exemple, si l'on a une OU "Personnel" qui contient différentes sous-OU (Region Est, Ouest etc) cela s'avère pertinent. **Pour créer une liaison entre une GPO et une unité d'organisation, effectuez un clic droit sur l'OU et cliquez sur "Lier un objet de stratégie de groupe existant".**

Il y a plusieurs méthodes pour créer une liaison, un simple glisser-déposer pourrait fonctionner aussi.



La liaison étant maintenant créée, on remarque qu'un raccourci s'est ajouté juste sous l'OU "Region Est".



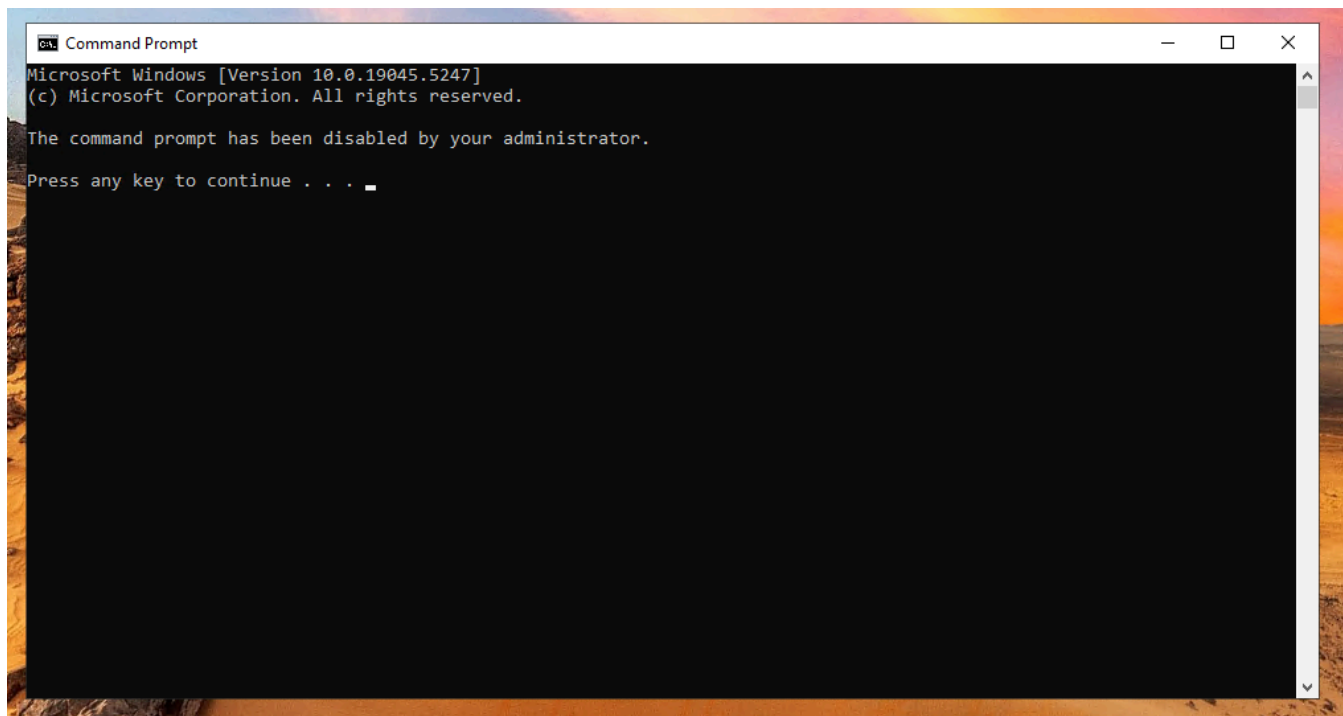
Maintenant, il ne reste plus qu'à tester la GPO sur un compte utilisateur ?

Tester la GPO

Sur un poste qui est dans le domaine, nous allons ouvrir une session d'un utilisateur dont le compte se situe dans l'OU "Personnel" ou dans l'une des sous-OU de "Personnel".

Une fois la session ouverte, je vous invite à lancer une invite de commandes. Et là, surprise : **l'invite de commandes a été désactivé par votre administrateur.**

Conclusion : notre stratégie de groupe fonctionne bien !



Il s'agissait de la première fois où cet utilisateur ouvrait la session sur ce poste de travail. Dans le cas où la session existerait déjà, il se peut que la GPO ne s'applique pas immédiatement. Il existe un temps de rafraîchissement pour les stratégies de groupe, ce qui est d'autant plus vrai pour les stratégies ordinateurs qui s'appliquent généralement au démarrage de la machine.

Pour forcer l'actualisation des stratégies de groupe sur un poste, que ce soit pour les paramètres ordinateurs ou utilisateurs, il y a une commande magique et qu'il est indispensable de connaître : gpupdate /force. Cette commande est associée à l'utilitaire Group Policy Update.

Si vous êtes prêt, on passe à la suite, on va regarder plus en détail les options qui s'offrent à nous...

Les stratégies de groupe et l'option « Appliqué » (Enforced)

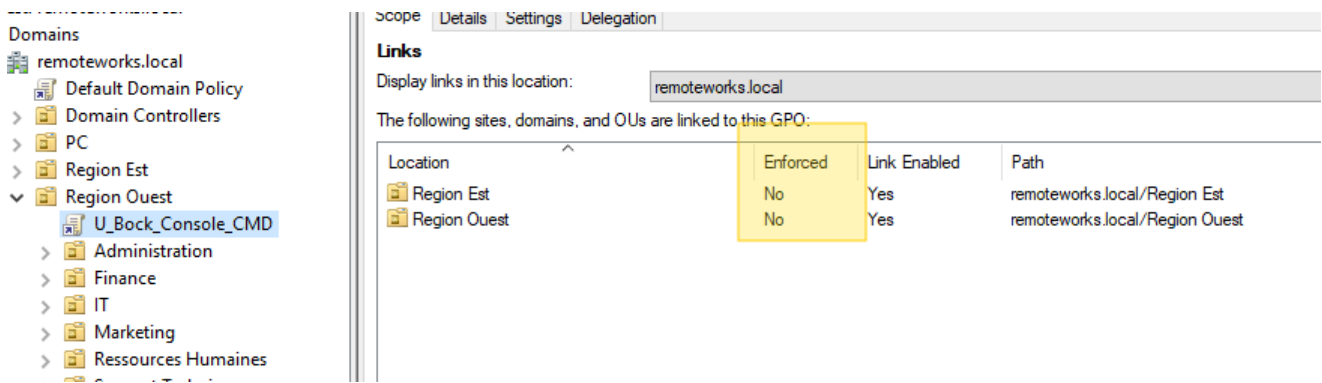
Dans le chapitre précédent, nous avons vu comment créer et appliquer notre première GPO. Les plus curieux d'entre vous ont peut-être remarqué que dans les propriétés de la liaison, il y avait un paramètre intitulé "Appliqué". Compte tenu de l'importance de ce paramètre et du mauvais usage qui en est fait, j'ai décidé de lui consacrer un chapitre.

Option "Appliqué" : explications

Je vais reprendre la GPO créée précédemment, et qui je vous le rappelle, fonctionnait parfaitement sur le poste client.

Dans la console GPMC, lorsque je clic sur la GPO, sur la droite au sein de l'onglet "*Étendue*", nous avons la partie "*Liaisons*". Dans cette partie, nous retrouvons autant de lignes que la GPO a de liaisons. Autrement dit, si la GPO est liée à 5 unités d'organisations différentes, il y aurait 5 lignes, chaque liaison ayant ses propres paramètres.

La question que l'on peut se poser : comment cela se fait-il que la GPO fonctionnait sur le poste client alors que le paramètre "Enforced" est sur "No" ?



La réponse est plutôt simple : ce n'est pas ce paramètre qui indique si la GPO s'applique ou non. Par contre, si le paramètre "**Lien activé**" était sur "**Non**" là je peux vous garantir qu'elle ne s'appliquerait pas.

En fait, l'option "Appliqué" est très mal traduite ! Avant traduction, en anglais donc, le terme est : *Enforced*.

Imaginons que nous avons une GPO contenant des paramètres de sécurité sensibles et qui doivent être impérativement appliqués sur l'ensemble des postes, le tout sans qu'il soit possible de remplacer ces paramètres. Alors, activez l'option "Appliqué". Même si la GPO s'applique au niveau du domaine, qu'elle active un paramètre, qui est lui-même désactivé dans une autre GPO positionnée sur l'OU où se trouve l'objet cible, ce sera la GPO "Enforced" qui gagnera.

Nous verrons plus tard la notion d'héritage, mais en temps normal si l'on désactive l'héritage des GPO sur une OU, vont s'appliquer uniquement les GPO liées directement sur l'OU. **Sauf que si une GPO est Enforced, elle s'appliquera même si l'héritage est désactivé !**

Cette option doit être utilisée à bon escient, et surtout ne l'activez pas par défaut, cela est plus source de problèmes qu'autre chose. Si une GPO ne s'applique pas, le problème est sûrement ailleurs.

****Maintenant que vous connaissez le véritable intérêt de l'option "Appliqué", s'il vous plaît, ne faites pas partie de ceux qui l'activent sur toutes les stratégies de groupe !**

Les filtres WMI : syntaxe, exemples et création

Nous avons vu jusqu'ici qu'il était possible de lier une stratégie de groupe à une unité d'organisation, à un domaine ou encore à un site directement, mais cela peut montrer ses limites. En effet, imaginez que l'on ait une unité d'organisation nommée "Ordinateurs" et qui contient tous les PC de l'entreprise.

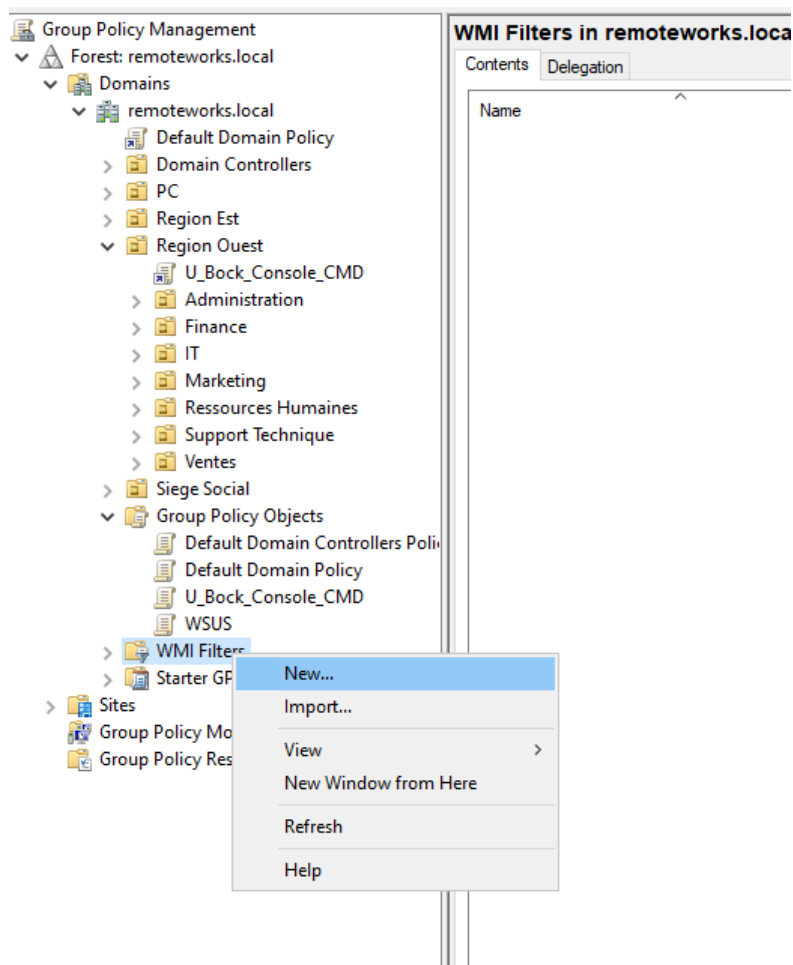
Dans cette OU, nous pourrions retrouver des objets ordinateurs avec des postes sous Windows 8 et Windows 10.

Dans certains cas, on peut avoir besoin d'appliquer une stratégie de groupe uniquement aux PCs dont le système d'exploitation est Windows 10. C'est là que le filtre WMI intervient, c'est ce que nous allons voir dans ce chapitre au travers différents exemples.

Où créer un filtre WMI pour une GPO ?

La première question que l'on se pose c'est : où est-ce que je vais pouvoir créer le filtre WMI ? Pour cela, rendez-vous dans la console GPMC (*Éditeur de stratégie de groupe*).

Ensuite, effectuez un clic droit sous "**Filtres WMI**" et cliquez sur "**Nouveau**".



Filtre WMI pour cibler un système d'exploitation

Pour commencer, nous allons créer un filtre WMI qui va permettre de cibler une version spécifique de Windows, par exemple **cibler uniquement les postes sous Windows 10**.

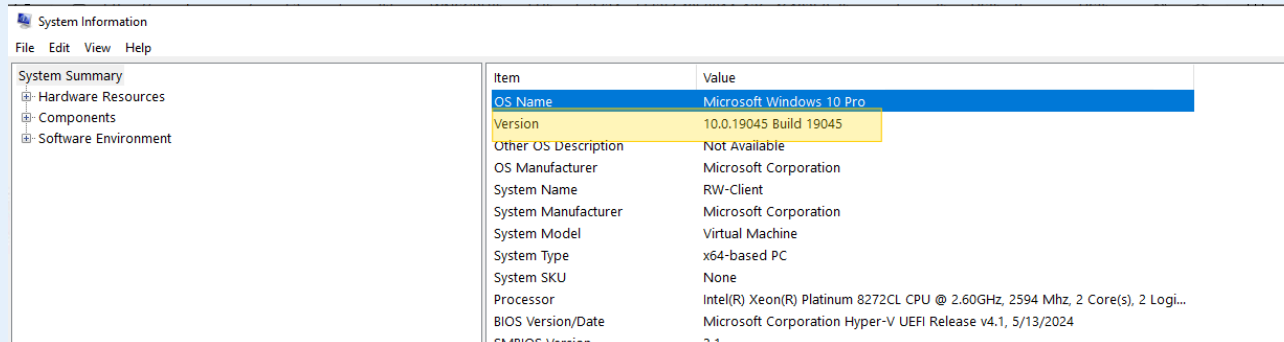
Pour cibler une version précise de Windows, nous avons besoin de connaître son numéro de version.

Concernant Windows 10 et les versions antérieures, voici un récapitulatif :

Système d'exploitation	Numéro de version
Windows XP – 32 bits	5.1
Windows XP – 64 bits	5.2
Windows Vista	6.0
Windows 7	6.1
Windows 8	6.2
Windows 8.1	6.3
Windows 10 (1709)	10.0.16299
Windows 10 (1803)	10.0.17134
Windows 10 (1809)	10.0.17763
Windows 10 (1903)	10.0.18362

 **Note**

Vous pouvez récupérer la version de votre OS en allant dans le system information



The screenshot shows the 'System Information' window. On the left, under 'System Summary', the 'Components' section is expanded. The main pane displays a list of system items and their values. The 'Version' item is highlighted in yellow, showing '10.0.19045 Build 19045'. Other items include OS Name (Microsoft Windows 10 Pro), Other OS Description (Not Available), OS Manufacturer (Microsoft Corporation), System Name (RW-Client), System Manufacturer (Microsoft Corporation), System Model (Virtual Machine), System Type (x64-based PC), System SKU (None), Processor (Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz, 2594 Mhz, 2 Core(s), 2 Logi...), BIOS Version/Date (Microsoft Corporation Hyper-V UEFI Release v4.1, 5/13/2024), and SMBIOS Version (3.1).

Item	Value
OS Name	Microsoft Windows 10 Pro
Version	10.0.19045 Build 19045
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	RW-Client
System Manufacturer	Microsoft Corporation
System Model	Virtual Machine
System Type	x64-based PC
System SKU	None
Processor	Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz, 2594 Mhz, 2 Core(s), 2 Logi...
BIOS Version/Date	Microsoft Corporation Hyper-V UEFI Release v4.1, 5/13/2024
SMBIOS Version	3.1

Pour les versions "Windows Server", il y a également un numéro de version à chaque fois :

Système d'exploitation	Numéro de version
Windows Server 2003 R2	5.2
Windows Server 2008	6.0
Windows Server 2008 R2	6.1
Windows Server 2012	6.2
Windows Server 2012 R2	6.3
Windows Server 2016 (1607)	10.0.14393
Windows Server 2016 (1709)	10.0.16299
Windows Server 2019 (1809)	10.0.17763

A la lecture des deux tableaux ci-dessus, **vous remarquerez que certains numéros de versions sont identiques entre les éditions clientes et les éditions serveurs Windows**. Comment faire pour les différencier malgré tout ?

Note

Dans les deux cas, ce numéro de version est stocké dans l'Active Directory au sein de chaque objet de type ordinateur, si vous avez besoin de vérifier.

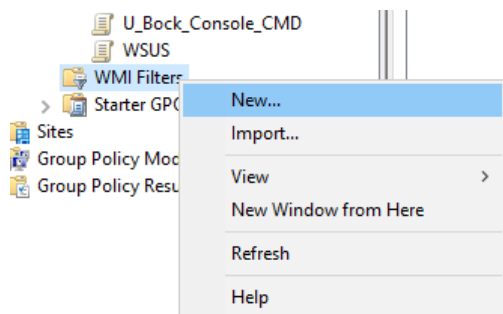
Nous allons utiliser un second paramètre nommé "**ProductType**" qui lorsqu'il est égal à "1" cible les éditions clientes de Windows. Lorsqu'il est à "2" il cible les serveurs contrôleurs de domaine et à "3" il cible les autres serveurs.

Vu que chaque version de Windows 10 dispose de son propre numéro de version, nous pouvons soit cibler une version spécifique de Windows 10, soit cibler toutes les versions de Windows 10 d'un coup puisqu'il commence à chaque fois par "10.0".

Maintenant, revenez sur la fenêtre de création de notre nouveau filtre WMI.

Commencez par indiquer un nom, par exemple : *Windows_10_Only*. Profitons-en pour indiquer une description également.

Ensuite, nous allons devoir créer une requête, c'est grâce à elle que nous allons pouvoir créer notre filtre pour retenir que les objets ordinateurs qui correspondent à Windows 10.



 A screenshot of the 'New WMI Filter' dialog box. It has a 'Name' field with 'Windows_10_Only', a 'Description' field with 'Only on windows 10 (all versions)', and a 'Queries' section. The 'Queries' section contains a table with columns 'Namespace' and 'Query'. To the right of the table are buttons for 'Add', 'Remove', and 'Edit'. At the bottom are 'Save' and 'Cancel' buttons. The 'Add' button is highlighted with a yellow box.

Concernant la requête WMI, elle sera construite de cette façon :

```
SELECT * FROM <Classe WMI> WHERE <Propriété> = <Valeur>
```

Pour la "classe WMI", nous allons utiliser **Win32_OperatingSystem**, ce qui nous donne accès à la propriété **"Version"**. Nous allons devoir vérifier la valeur de cette propriété.

Ce qui nous donne, pour sélectionner tous les PC Windows 10 (toutes versions)

```
SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0%" AND ProductType="1"
```

En plus de ce que l'on vient de voir précédemment, on ajoute l'opérateur "LIKE" en plus et un "%" après le numéro de version pour prendre toutes les "sous-versions" éventuelles.

Il faut alors valider la requête et cliquer sur **"Enregistrer"** pour valider la création du filtre.

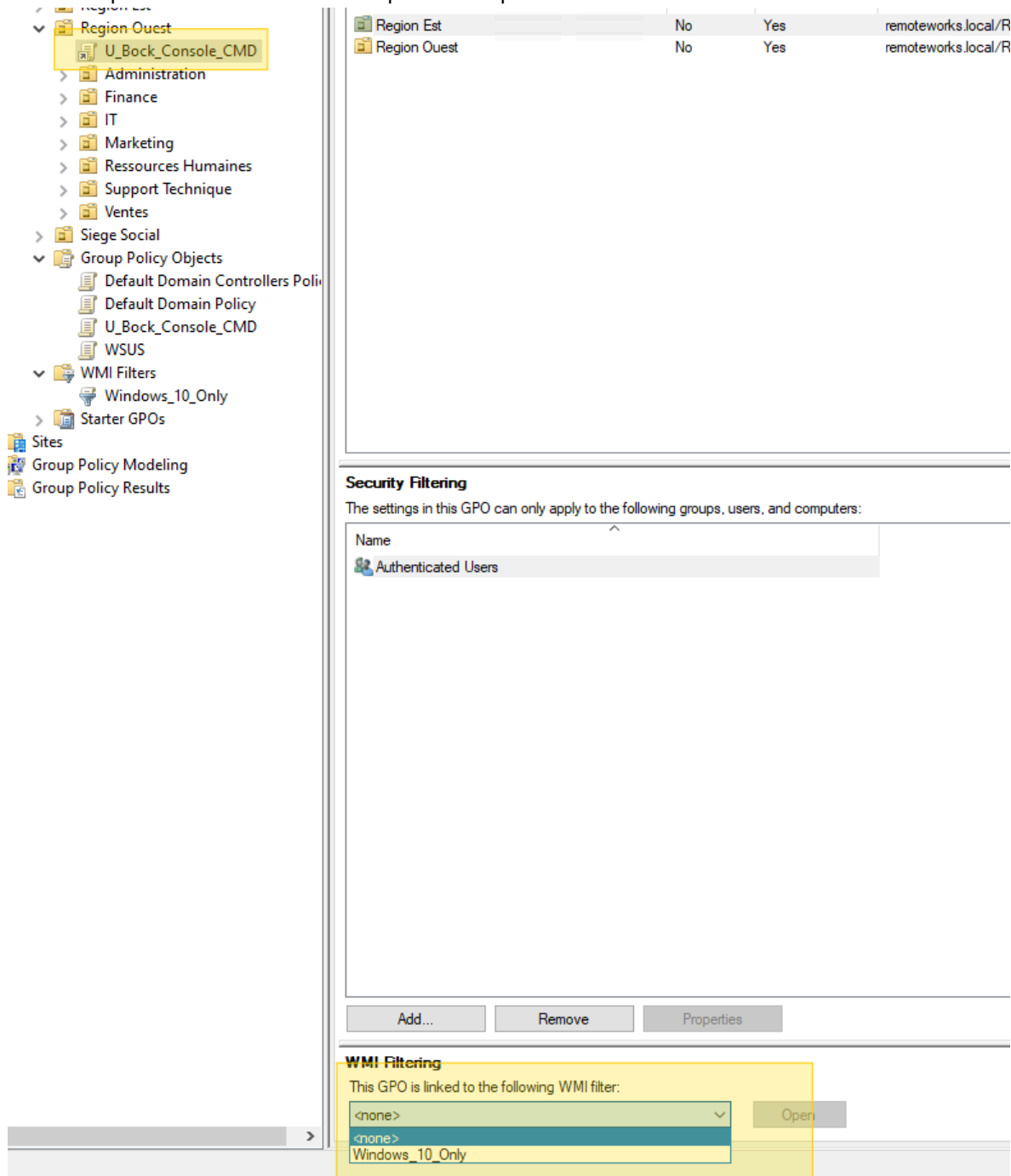
 A screenshot of the 'WMI Query' dialog box. It has a 'Namespace' field with 'root\cimv2' and a 'Browse...' button. Below it is a 'Query' text area containing the SQL query: 'SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0%" AND ProductType="1"'. At the bottom are 'OK' and 'Cancel' buttons.

Maintenant, il ne reste plus qu'à voir comment l'associer à une GPO.

Associer un filtre WMI à une GPO

Un filtre WMI ne s'applique à une GPO que lorsqu'il y a une liaison entre les deux. Pour réaliser cette opération, dans la console GPMC, cliquez sur votre GPO. Ensuite, vérifiez que vous êtes bien sur l'onglet "Étendue".

Dans le bas de la fenêtre, vous devriez voir la zone "*Filtrage WMI*". Grâce à la liste déroulante, sélectionnez votre filtre WMI et cliquez sur "Oui" sur la fenêtre qui s'affiche pour valider.



À partir de ce moment-là, le filtrage WMI va s'appliquer sur votre GPO. Si cela ne fonctionne pas, il faudra vérifier votre requête.

Exemples complémentaires

Pour finir ce chapitre, voici quelques exemples supplémentaires pour vous aider dans la construction de vos requêtes :

- **Sélectionner tous les PC Windows 10 en 32 bits**

```
SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0%" AND ProductType="1" AND OSArchitecture = "32-bit"
```

- **Sélectionner tous les PC Windows 7**

```
SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "6.1%" AND ProductType="1"
```

- Sélectionner tous les serveurs sous [Windows Server 2016/2019](#)

```
SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.%" AND (ProductType = "2" OR ProductType = "3" )
```

Comme nous devons sélectionner les serveurs avec le *ProductType* à "2" et à "3" pour prendre tous les serveurs, cela ajoute de la complexité à la requête, on doit coupler l'usage du "AND" (ET) et du "OR" (OU).

- Sélectionner tous les objets ordinateurs avec un OS 64 bits (processeur 64 bits)

```
SELECT * FROM Win32_Processor WHERE AddressWidth = "64"
```

- Sélectionner tous les PC dont le nom commence par "PC-PORTABLE-"

```
SELECT Name FROM Win32_ComputerSystem WHERE Name LIKE "PC-PORTABLE-%"
```

- Sélectionner tous les PC Windows 8 et Windows 8.1 (soit deux versions différentes) :

```
SELECT * FROM Win32_OperatingSystem WHERE (Version LIKE "6.2%" OR Version LIKE "6.3%") AND ProductType = "1"
```

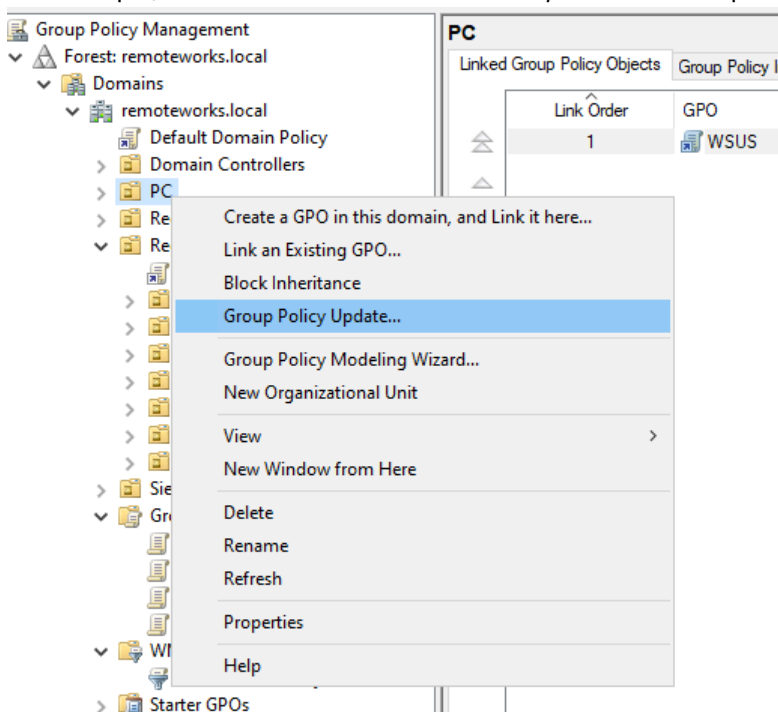
Forcer l'actualisation des GPO à distance sur une machine

Lorsqu'il s'agit de forcer l'actualisation des stratégies de groupe sur un poste afin de tester un nouveau paramètre ou d'appliquer en urgence une nouvelle configuration, il y a plusieurs méthodes pour réaliser cette opération à distance. On parlera de **Remote Group Policy Update**.

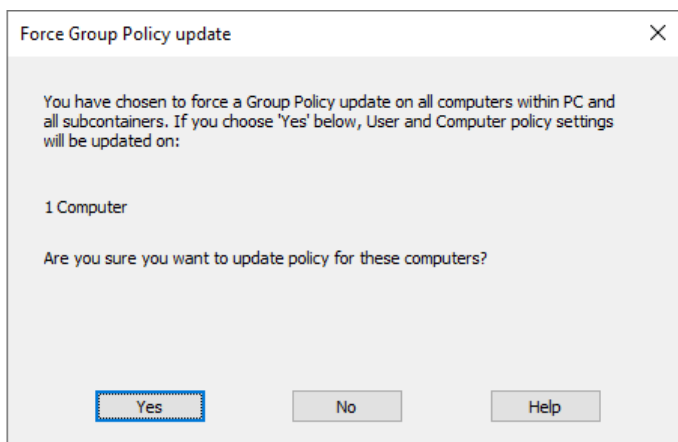
Utiliser la console GPMC

La méthode la plus répandue est celle intégrée à la console GPMC. Vous pouvez sélectionner une unité d'organisation dans l'arborescence (plus ou moins haut dans la hiérarchie) pour déclencher une actualisation des [GPO](#) à distance.

Par exemple, via un clic droit sur l'OU "IT - Computers" et en cliquant sur "**Mise à jour de la stratégie de groupe**".

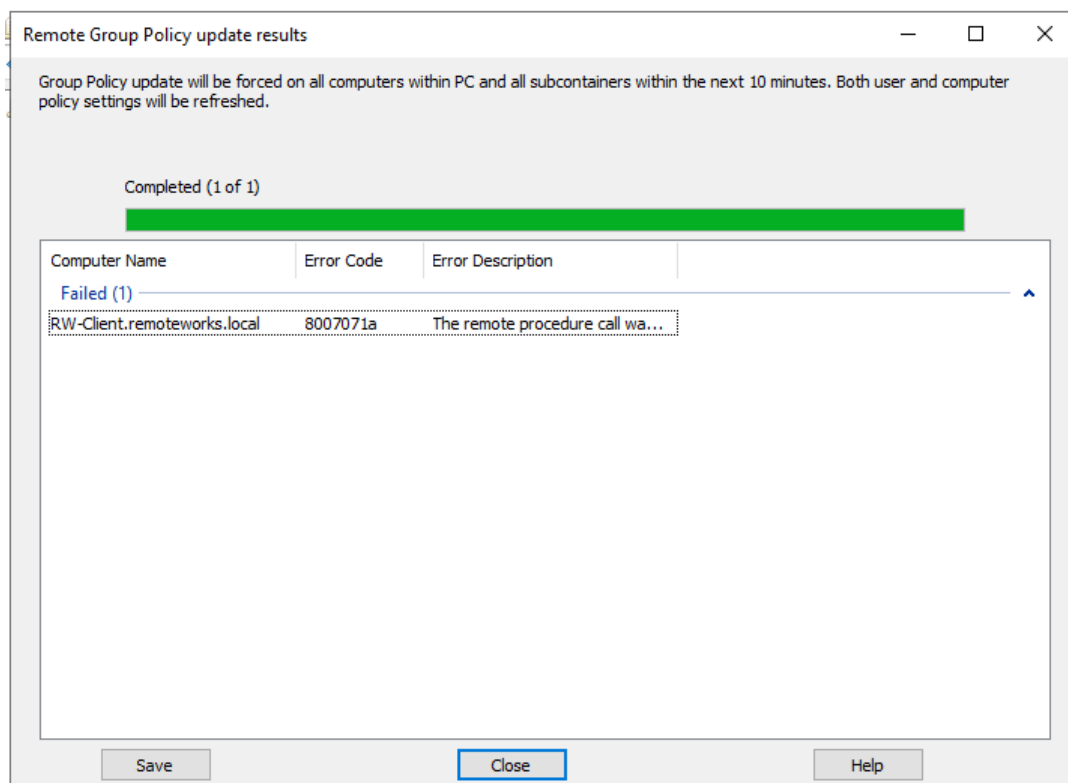


Une fenêtre va s'ouvrir pour vous indiquer le nombre de postes ciblés. Cliquez sur "Oui" pour lancer l'opération.



Vous allez être déçu, mais il y a des chances pour que ça ne fonctionne pas : le pare-feu de Windows bloque le flux par défaut. Si vous utilisez une protection Endpoint sur vos postes clients et qu'il gère le pare-feu, il va falloir y jeter un coup d'œil également.

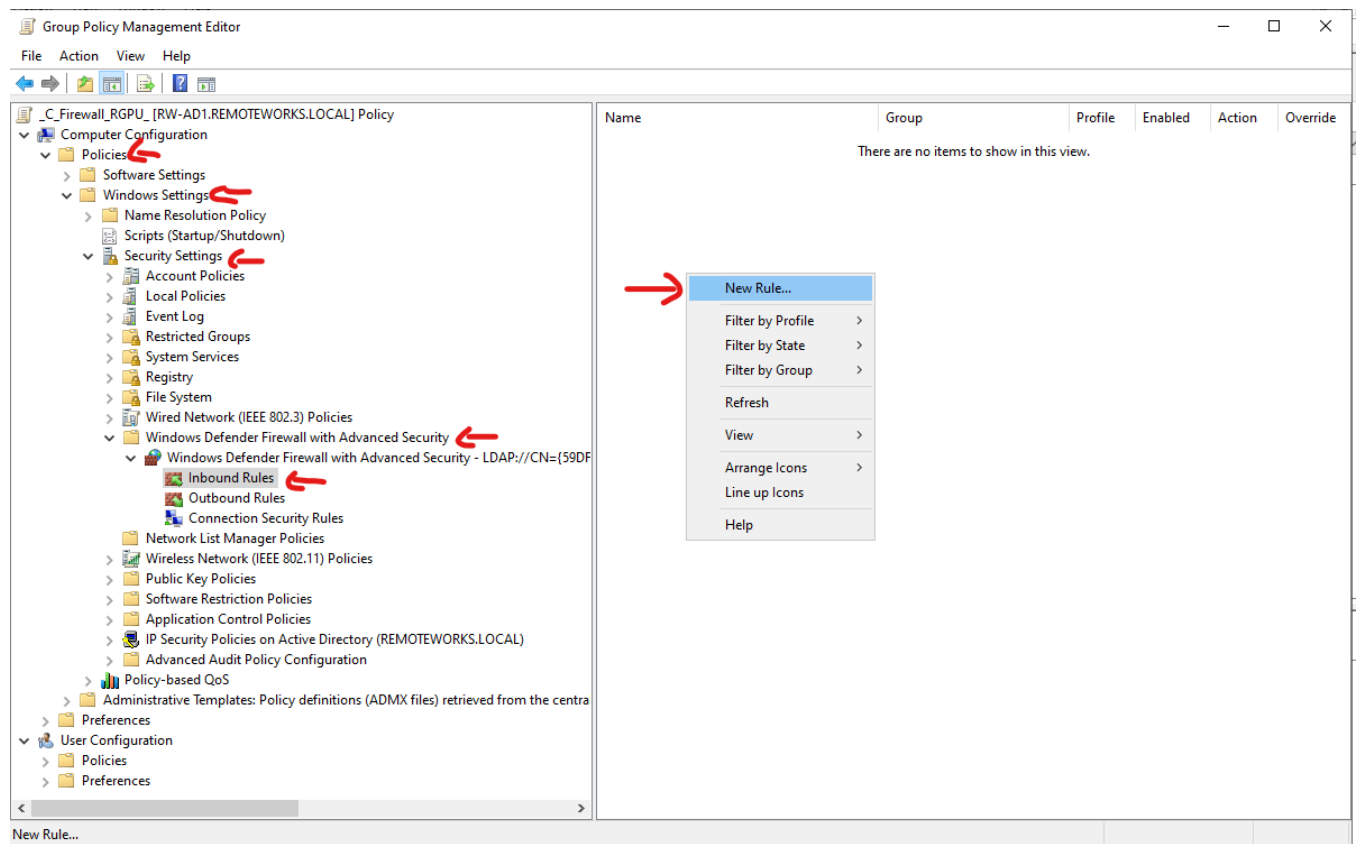
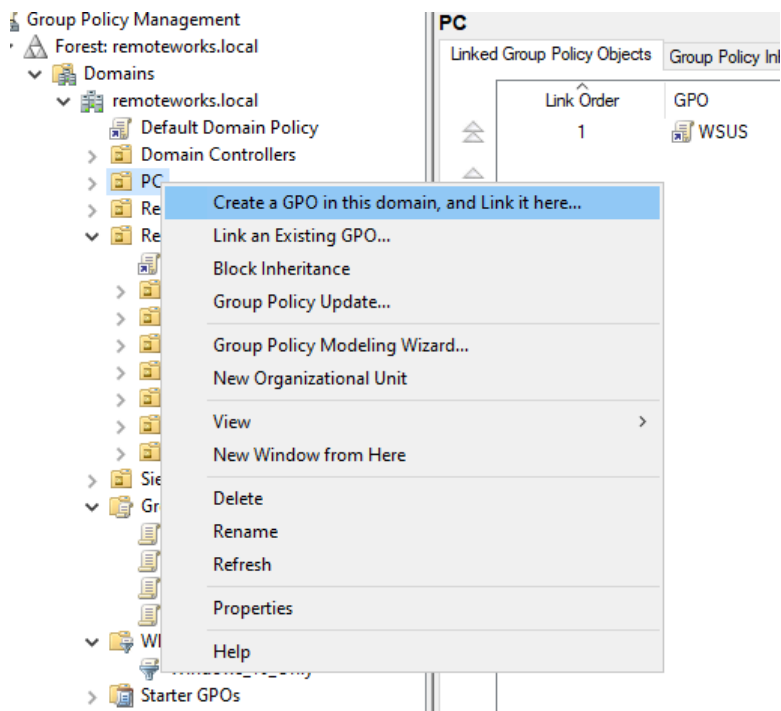
L'erreur 8007071A "L'appel de procédure distante a été annulé" va s'afficher sur chaque ligne. Sauf si le pare-feu est désactivé sur le poste client, ce qui n'est pas recommandé.



Nous allons créer une stratégie de groupe pour autoriser ce flux. Pour cela, créez une nouvelle GPO et nommez-la "C_Firewall_RGPU" par exemple. Elle contiendra des paramètres de configuration "Ordinateur" puisque cela concerne le pare-feu.

Modifiez la GPO, et parcourez comme suit : **Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Pare-feu Windows avec fonctions avancées de sécurité > Règles de trafic entrant.**

Lorsque vous êtes sur le dernier item, sur la partie de droite de la console réalisez un clic droit et cliquez sur "**Nouvelle règle**".



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

Rule Type

Predefined Rules

Action

What type of rule would you like to create?

☐ Program

Rule that controls connections for a program.

☐ Port

Rule that controls connections for a TCP or UDP port.

☒ Predefined:

Windows Management Instrumentation (WMI)

Rule that controls connections for a Windows experience.

☐ Custom

Custom rule.

< Back

Next >

Cancel

New Inbound Rule Wizard

Predefined Rules

Select the rules to be created for this experience.

Steps:

Rule Type

Predefined Rules

Action

Which rules would you like to create?

The following rules define network connectivity requirements for the selected predefined group. Rules that are checked will be created. If a rule already exists and is checked, the contents of the existing rule will be overwritten.

Rules:

Name	Rule Exists	Profile
<input checked="" type="checkbox"/> Windows Management Instrumentation (DCOM-In)	No	All
<input checked="" type="checkbox"/> Windows Management Instrumentation (WMI-In)	No	All
<input checked="" type="checkbox"/> Windows Management Instrumentation (ASync-In)	No	All

< Back

Next >

Cancel

New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Predefined Rules
- Action**

What action should be taken when a connection matches the specified conditions?

☒ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
[Customize...](#)

☐ **Block the connection**

< Back **Finish** Cancel

Sélectionnez ensuite "**Prédéfinie**" et dans la liste déroulante prenez "**Infrastructure de gestion Windows**". Cela va permettre d'activer les trois règles contenues dans ce groupe.

Répétez l'opération en ajoutant une nouvelle règle. Cette fois-ci, sélectionnez "**Gestion à distance des tâches planifiées**".

New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type**
- Predefined Rules
- Action

What type of rule would you like to create?

☐ **Program**
Rule that controls connections for a program.

☐ **Port**
Rule that controls connections for a TCP or UDP port.

☒ **Predefined:**
Remote Scheduled Tasks Management
Rule that controls connections for a Windows experience.

☐ **Custom**
Custom rule.

< Back **Next >** Cancel

À la fin, vous devez obtenir ceci :

Name	Group	Profile	
✓ Remote Scheduled Tasks Management (R...	Remote Scheduled Tasks Ma...	All	'
✓ Remote Scheduled Tasks Management (R...	Remote Scheduled Tasks Ma...	All	'
✓ Windows Management Instrumentation ...	Windows Management Instr...	All	'
✓ Windows Management Instrumentation ...	Windows Management Instr...	All	'
✓ Windows Management Instrumentation ...	Windows Management Instr...	All	'

Si tout est bon, il ne reste plus qu'à lier la GPO pour qu'elle s'applique vos postes afin de configurer le pare-feu. Ensuite, vous avez deux options :

- Soit patienter que la stratégie de groupe s'actualise automatiquement sur vos postes
- Soit forcer la mise à jour en intervenant sur la machine et en exécutant la commande "gpupdate /force". Il faudra redémarrer le poste.

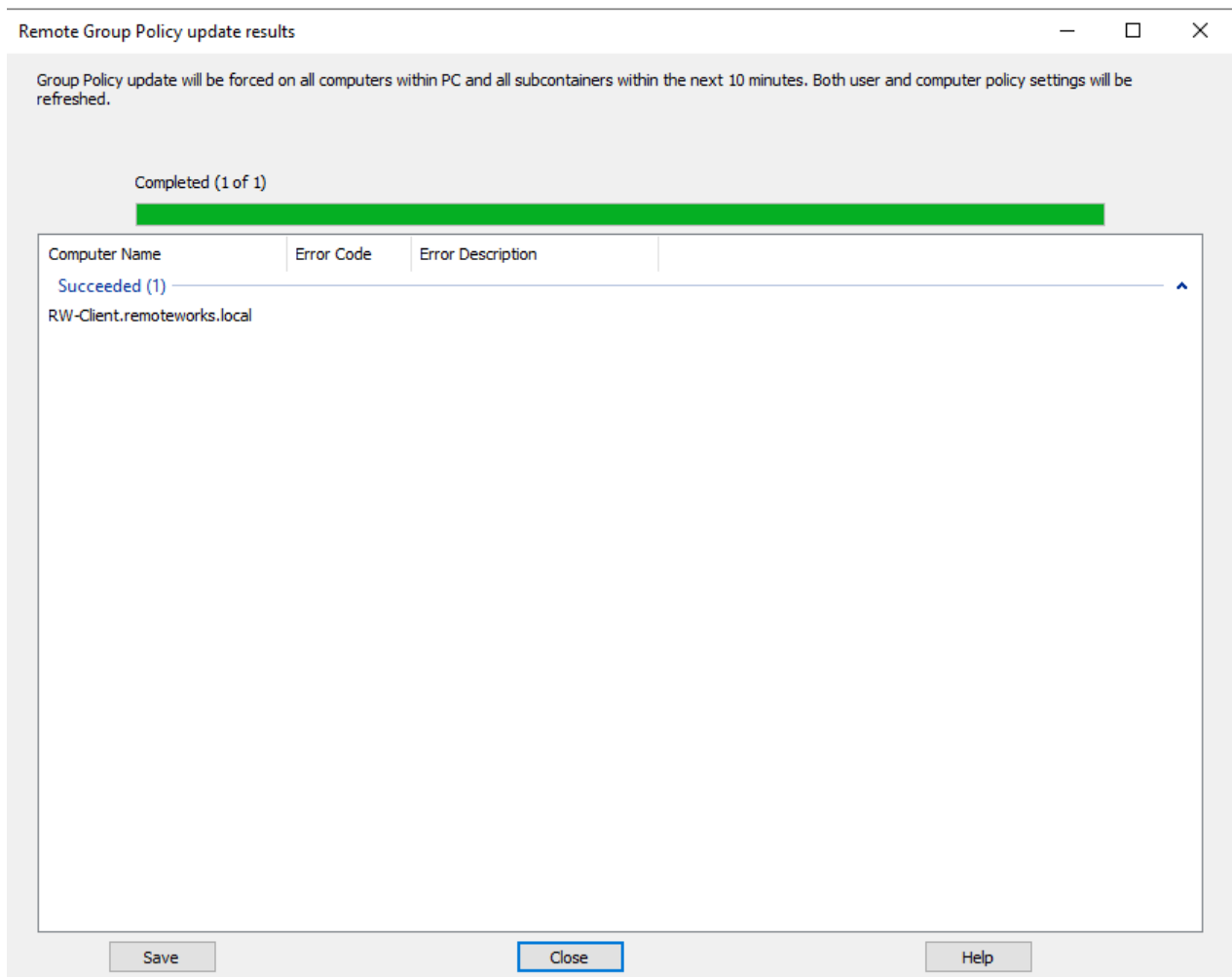
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.5247]
(c) Microsoft Corporation. All rights reserved.

C:\Users\youenn>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\youenn>
```

Quoi qu'il en soit, une fois que la GPO sera déployée sur le poste, l'actualisation des GPO à distance doit fonctionner. Par exemple, on peut le constater ci-dessous avec le PC qui est passé sur l'état "Réussite". L'autre PC ne risque pas de fonctionner, car il est toujours dans l'AD, mais il n'existe pas : d'où l'importance de faire le tri dans l'annuaire.



Soit vous pouvez enregistrer les résultats ou tout simplement fermer.

Warning

Attention : cette action réalisée à distance n'est pas transparente au niveau du poste client. Si un utilisateur est connecté sur le poste, il verra l'invite de commande s'exécuter à l'écran pour exécuter l'utilitaire *gpupdate*. Cela est plus ou moins rapide et discret en fonction des performances de votre PC/infrastructure.

Utiliser PowerShell et Invoke-GPUdate

Depuis [Windows Server 2012](#), Microsoft a intégré la commande PowerShell "*Invoke-GPUdate*" pour réaliser une actualisation des GPO à distance sur un poste cible.

Cette alternative est intéressante notamment, car on peut l'intégrer dans un script donc cela offre beaucoup plus de souplesse que la console GPMC.

Pour utiliser cette commande, il faudra indiquer l'ordinateur cible au sein du paramètre `-Computer`. Vous pouvez utiliser le nom FQDN de la machine ou son nom NetBIOS.

```
invoke-gpupdate -computer rw-client -RandomDelayInMinutes 0
```

Lorsque le paramètre `RandomDelayInMinutes` est à zéro, l'actualisation sera déclenchée immédiatement. Grâce à ce paramètre, **il est possible de "planifier" la mise à jour jusqu'à 31 jours** puisque la valeur maximale est 44640 minutes.

Exemple :

```
PS C:\Users\youenn> invoke-gpupdate -computer rw-client -RandomDelayInMinutes 0
PS C:\Users\youenn>
```

On pourrait ajouter à la commande le paramètre `"-Target"` avec la valeur `"User"` pour actualiser seulement les paramètres de l'utilisateur. Idem avec la valeur `"Computer"` pour les paramètres de l'ordinateur.

Grâce à cette commande, on peut très facilement actualiser la GPO sur l'ensemble des ordinateurs de l'AD grâce à ces deux lignes :

```
$Computers = Get-ADComputer -Filter *
$Computers | ForEach-Object -Process { Invoke-GPUUpdate -Computer $_.Name -RandomDelayInMinutes 0 -Force }
```

Attention, cela peut s'avérer dangereux en termes de charge, selon le nombre de machines dans votre annuaire. Prenez une sélection plus restreinte si besoin en agissant sur la commande `Get-ADComputer`.

La bonne nouvelle c'est que cette commande nécessite les mêmes règles de firewall que la première méthode



Nous venons de voir les deux méthodes principales pour actualiser les GPO à distance sur une ou plusieurs machines.

Sauvegarde et restauration des stratégies de groupe (GPO)

Dans ce chapitre, je vous propose d'aborder la notion de sauvegarde et de restauration des stratégies de groupe. Sauvegarder une GPO a plusieurs intérêts :

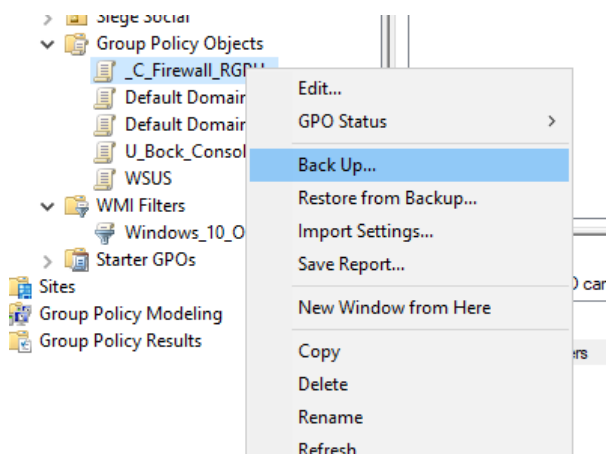
- Avant d'apporter des changements importants, afin de faciliter le retour-arrière
- Réimporter les paramètres d'une [GPO](#) au sein d'une autre GPO, sur le même domaine ou un autre domaine
- Se protéger contre les éventuelles suppressions accidentelles

Nous allons voir comment sauvegarder une GPO, comme la restaurer, mais aussi comment sauvegarder toutes les stratégies de groupe grâce à PowerShell, ce qui permet également d'automatiser cette tâche.

Sauvegarder une GPO

Sur votre serveur, ouvrez la console GPMC (*Gestion de stratégie de groupe*). Ensuite, déroulez **"Objets de stratégie de groupe"** dans la console : la liste des GPO de votre domaine va apparaître.

Si, par exemple, on souhaite sauvegarder la GPO `"C_Firewall_RGPU"` que l'on a créé dans un précédent chapitre, il suffit de faire un clic droit dessus et de cliquer sur **"Sauvegarder..."**.



Un assistant s'ouvre, il y a deux choses à renseigner :

- L'emplacement, c'est-à-dire le dossier dans lequel il faut stocker la [sauvegarde](#)
- La description, par exemple le nom de la GPO ou la date de sauvegarde

Le dossier créé aura pour nom un identifiant (type GUID), ce n'est pas très parlant mais nous verrons que c'est facilement exploitable.

Lorsque vous avez renseigné les deux champs, ou en tout cas à minima l'emplacement, cliquez sur "**Sauvegarder**".

Back Up Group Policy Object

Enter the name of the folder in which you want to store backed up versions of this Group Policy Object (GPO). You can back up multiple GPOs to the same folder.

Note: Settings that are external to the GPO, such as WMI filters and IPsec policies, are independent objects in Active Directory and will not be backed up.

To prevent tampering of backed up GPOs, be sure to secure this folder so that only authorized administrators have write access to this location.

Location:

C:\backup_gpo

Browse...

Description:

backup_GPO_date

Back Up

Cancel

Backup

Backup progress:

Status:

GPO: _C_Firewall_RGPU_...Succeeded

OK

Cancel

Ensuite, si l'on regarde au niveau du stockage ce que ça donne, on remarque bien la présence d'un nouveau dossier correspondant à la sauvegarde notre GPO. A l'intérieur, on retrouve les différents fichiers de notre GPO.

{A63BCA00-0E37-4A4C-A92E-E2BE4902E96C}

File

Home

Share

View

←

→

↶

↷

This PC

>

Windows (C:)

>

backup_gpo

>

{A63BCA00-0E37-4A4C-A92E-E2BE4902E96C}

>

Quick access

Desktop

Downloads

Documents

Pictures

PolicyDefinitions

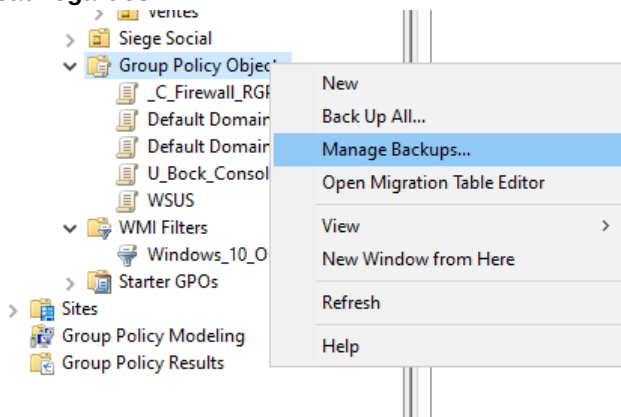
This PC

Network

Name	Date modified	Type	Size
DomainSysvol	1/4/2025 6:33 PM	File folder	
Backup	1/4/2025 6:33 PM	XML Document	6 KB
gpreport	1/4/2025 6:33 PM	XML Document	21 KB

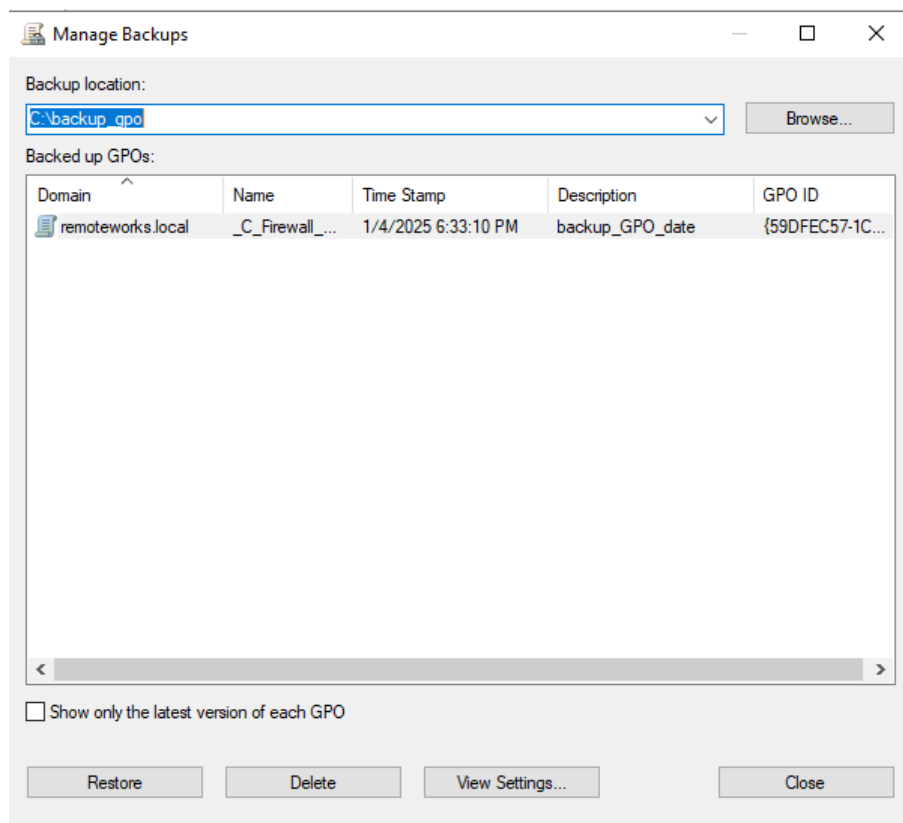
Restaurer une GPO

Maintenant, intéressons-nous à la restauration d'une GPO à partir d'une sauvegarde. Toujours dans la console GPMC, cette fois-ci, effectuez un clic droit directement sur "**Objets de stratégie de groupe**" puis cliquez sur "**Gérer les sauvegardes**".



Ensuite, il faut indiquer le chemin vers le dossier où se situe la sauvegarde votre GPO. L'idéal est de centraliser les sauvegardes dans un même dossier, sans faire de sous-dossier car il ne serait pas pris en compte.

L'utilitaire va afficher la liste des sauvegardes trouvées, vous pouvez avoir plusieurs sauvegardes pour la même GPO. Ce qui donne :



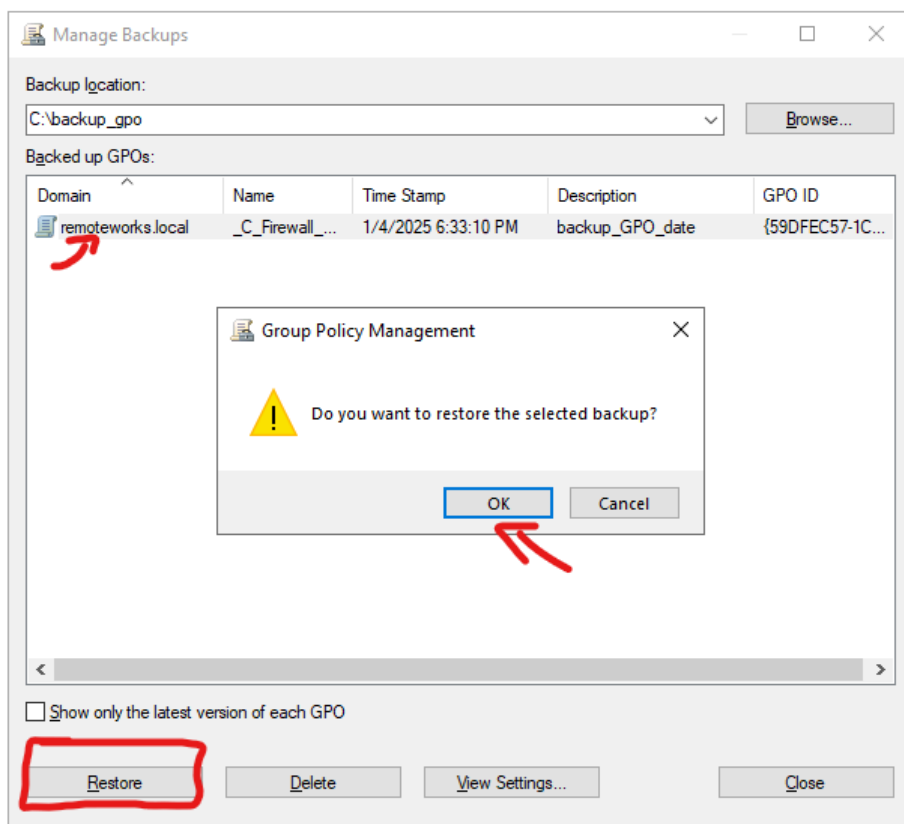
Dans le cas où vous avez plusieurs versions pour la même GPO, vous pouvez cocher la case "**N'afficher que la dernière version des objets GPO**" pour épurer l'affichage.

Pour restaurer une sauvegarde, c'est simple :

- 1 - On sélectionne la sauvegarde dans la liste
- 2 - On clic sur le bouton "Restaurer"
- 3 - On clic sur "OK" pour déclencher la restauration de la sauvegarde

Note : si la GPO n'existe plus dans votre infrastructure, elle sera créée. Si elle existe toujours, elle sera écrasée pour revenir à l'état antérieur.

Avant de déclencher l'opération, si vous ne savez pas trop quelle version restaurer, vous pouvez sélectionner une sauvegarde et cliquer sur "**Afficher les paramètres**" pour voir le contenu de cette version.



Concernant la restauration d'une GPO il est à noter que :

- Cela ne restaure pas les liaisons de la GPO - **il faudra recréer les liens manuellement**
- Cela ne restaure pas le filtre WMI s'il n'existe plus (un filtre WMI peut être exporté via un clic droit dessus)
- Les autorisations visibles dans l'onglet "Délégation" sont restaurées

Si ces éléments ne sont pas restaurés, cela implique bien sûr qu'ils ne sont pas inclus à la sauvegarde.

Sauvegarder toutes les GPO avec PowerShell

Nous venons de voir comment sauvegarder une GPO via la console GPMC mais cela n'est pas très efficace s'il y a besoin de sauvegarder un ensemble de GPO de façon régulière.

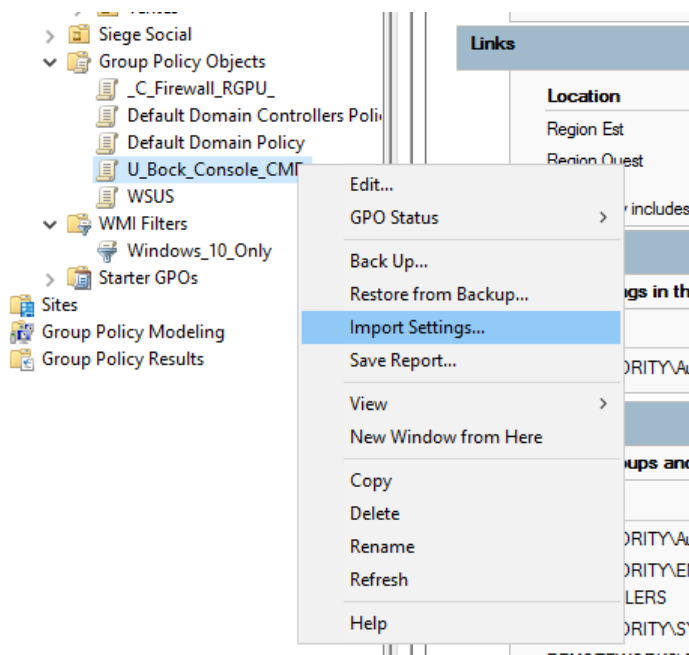
Grâce au module PowerShell "GroupPolicy" on peut aisément manipuler les stratégies de groupe en ligne de commande. Une seule ligne suffit pour sauvegarder toutes les GPO :

```
Get-GPO -Domain remoteworks.local -All | Backup-GPO -Path "C:\backup_gpo"
```

Fusionner deux GPO

Pour finir, je souhaitais partager avec vous une astuce : si vous souhaitez fusionner deux GPO, c'est-à-dire prendre les paramètres d'une GPO et les importer dans une autre pour ne faire qu'un, cela est possible. Vous devez :

- 1 - Réaliser une sauvegarde de la GPO qui contient les paramètres que vous souhaitez récupérer
- 2 - Effectuer un clic droit sur la GPO cible, et cliquer sur "*Importer des paramètres*"



3 - Suivez l'assistant ensuite pour charger votre sauvegarde et les paramètres seront intégrés à votre GPO existante, ce qui permet de fusionner des GPO

4 - Supprimez si vous le souhaitez la GPO source

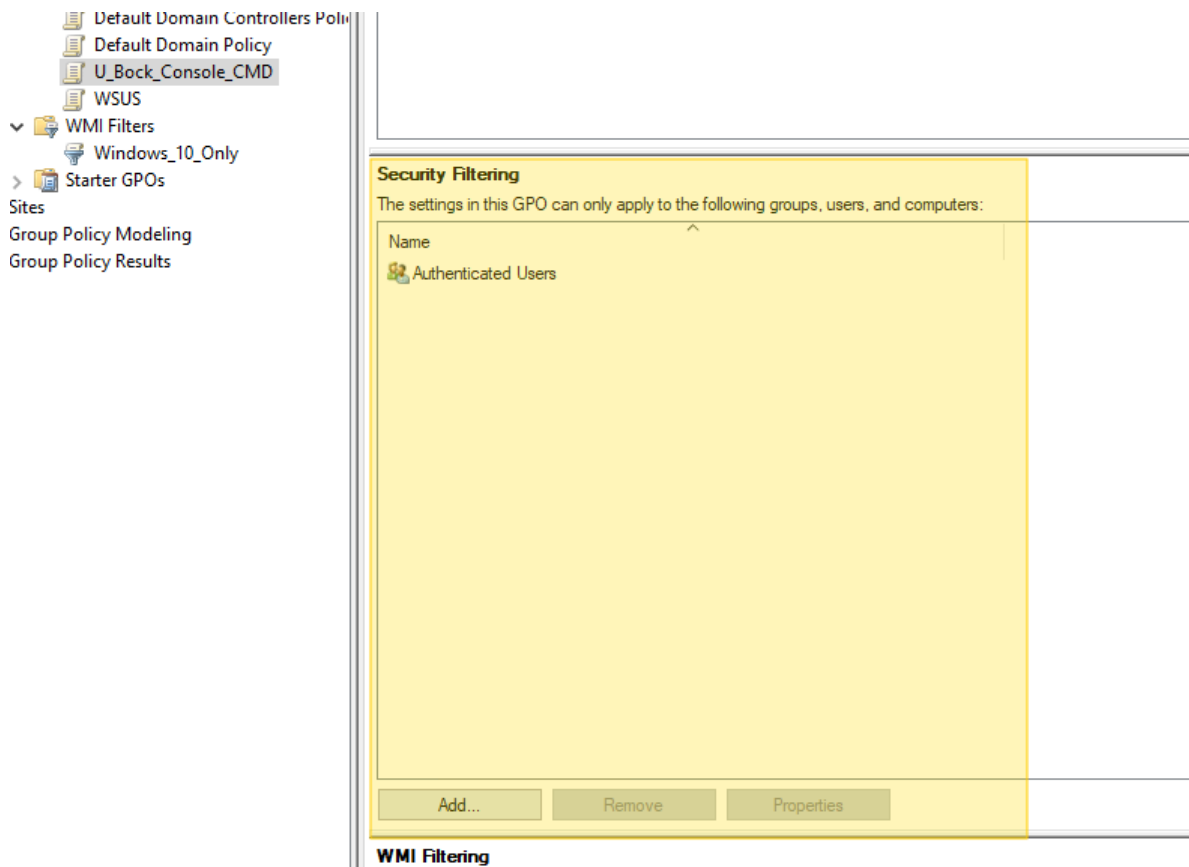
Comment appliquer une GPO sur un groupe spécifique ?

Plutôt que de vous parler de la notion de délégation qui n'est pas spécialement utilisée dans les TPE/PME, mais qui s'adresse plutôt aux équipes très conséquentes, je préfère vous parler du filtrage de sécurité d'une GPO. Cela est pratique et ça peut servir donc c'est encore mieux !

Par défaut, lorsque l'on crée une stratégie de groupe, le filtrage "**Utilisateurs authentifiés**" s'applique. Cela signifie que la GPO s'applique à l'ensemble des utilisateurs qui se connectent sur une machine.

Note

Les comptes administrateurs sont également considérés comme "*Utilisateurs authentifiés*". Être admin ne donne pas le droit d'être exclu du scope des GPO.



On peut ajuster ce filtrage de sécurité pour cibler certains utilisateurs spécifiques, si le fait de jouer avec les liaisons et les filtres WMI n'est pas suffisant pour réaliser le ciblage.

Modifier le filtrage de sécurité d'une GPO

Pour modifier le filtrage de sécurité d'une GPO à partir de la console GPMC, il faut commencer par **sélectionner la GPO dans l'arborescence**. Ensuite, sur la partie droite, nous retrouvons la zone "**Filtrage de sécurité**" avec la valeur par défaut "**Utilisateurs authentifiés**" clairement visible.

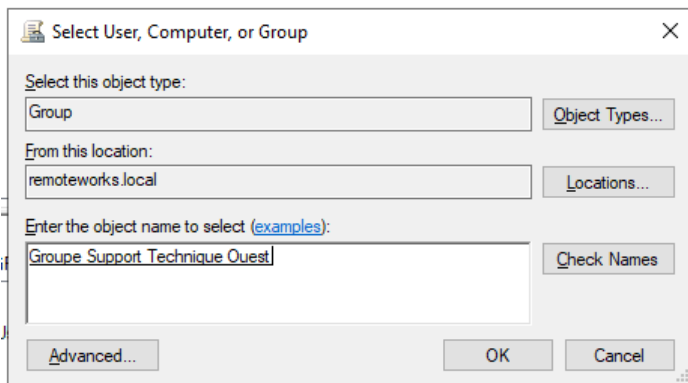
L'objectif va être d'ajouter un groupe de sécurité qui contient les utilisateurs (ou ordinateurs) que vous souhaitez cibler avec votre GPO, à la place du groupe "Utilisateurs authentifiés".

Procédez de cette façon :

- 1 - Cliquez sur le bouton "Ajouter"
- 2 - Saisissez le nom de votre groupe de sécurité
- 3 - Cliquez sur "Vérifier les noms" pour valider le nom saisi
- 4 - Cliquez sur "OK" pour valider

Remarques :

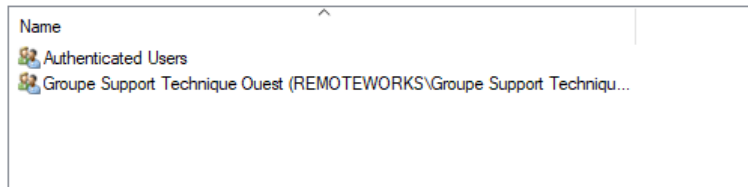
- Il est tout à fait possible d'ajouter plusieurs groupes
- Pour simplifier la gestion, vous pouvez créer un groupe de sécurité dédié à cette GPO



Ensuite, dans le filtrage de sécurité le groupe que vous venez d'ajouter va apparaître, en complément du groupe **"Utilisateurs authentifiés"**. Je vous invite à supprimer ce groupe du coup en cliquant dessus et en cliquant sur le bouton **"Supprimer"**. Vous devriez obtenir ceci :

Security Filtering

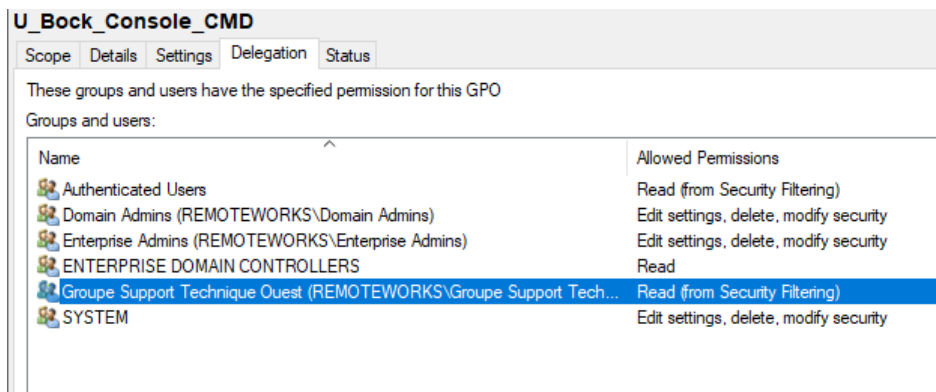
The settings in this GPO can only apply to the following groups, users, and computers:



Il est à noter que les autorisations attribuées dans le filtrage de sécurité sont reportées dans l'onglet **"Délégation"** de la GPO avec la mention **"Lecture (à partir du filtrage de sécurité)"**.

Concrètement, **cela signifie que les membres du groupe "Comptables" peuvent lire cette GPO, les paramètres vont donc s'appliquer sur les objets membres du groupe**. Les utilisateurs qui ne sont pas de ce groupe auront un accès refusé lorsqu'ils vont tenter de lire la GPO, ce qui va empêcher que les paramètres de la GPO s'appliquent.

Cette méthode, bien que pratique, doit être utilisée à bon escient et lorsque vous rencontrez des problèmes sur une GPO qui ne s'applique pas, il faudra penser à vérifier le filtrage de sécurité et notamment les membres contenus dans le groupe.



Pour que la configuration fonctionne, il faut ajouter le groupe **"Utilisateurs authentifiés"** si il n'y est pas déjà, en lecture dans l'onglet **"Délégation"**, même si la GPO ne doit plus s'appliquer aux utilisateurs authentifiés. Au sein de l'onglet **"Délégation"**, cliquez sur le bouton **"Ajouter"** en bas à gauche. Ensuite, recherchez **"Utilisateurs authentifiés"** et validez.

A partir de là, il ne restera plus qu'à tester la GPO en se connectant sur un PC avec un compte pour qui la GPO doit s'appliquer et un autre pour lequel elle ne doit pas s'appliquer (mais qui est quand même ciblé via la liaison) afin de valider le bon fonctionnement ?

Enfin, **je tiens à préciser que si vous modifiez le filtrage de sécurité, cela s'applique sur la GPO directement, et donc sur toutes les liaisons de la GPO**. Il n'y a pas de gestion de la sécurité par liaison, mais bien une gestion globale, c'est important de le savoir.

Dans le chapitre suivant, nous allons voir comment faire l'inverse, à savoir : **comment bloquer une GPO pour un groupe spécifique ?**

Comment bloquer une GPO pour un groupe spécifique ?

Alors que nous venons de voir comment appliquer une GPO sur un groupe spécifique dans le chapitre précédent, maintenant nous allons traiter un autre cas : si l'on souhaite appliquer une GPO à tous les utilisateurs sauf certains, comment faire ? Il va falloir leur refuser l'accès à la GPO, voyons comment faire.

Refuser l'accès à une GPO sur un groupe

Dans l'éternelle console GPMC, il va falloir commencer par sélectionner la GPO dans la liste. Ensuite, **nous allons accéder directement à l'onglet "Délégation"** : et oui, le filtrage de sécurité permet de donner l'accès à une [GPO](#), mais ne permet pas de gérer le refus.

L'objectif va être de bloquer l'accès au groupe "*Direction*" à cette GPO qui s'applique sur tout le personnel de l'entreprise jusqu'ici.

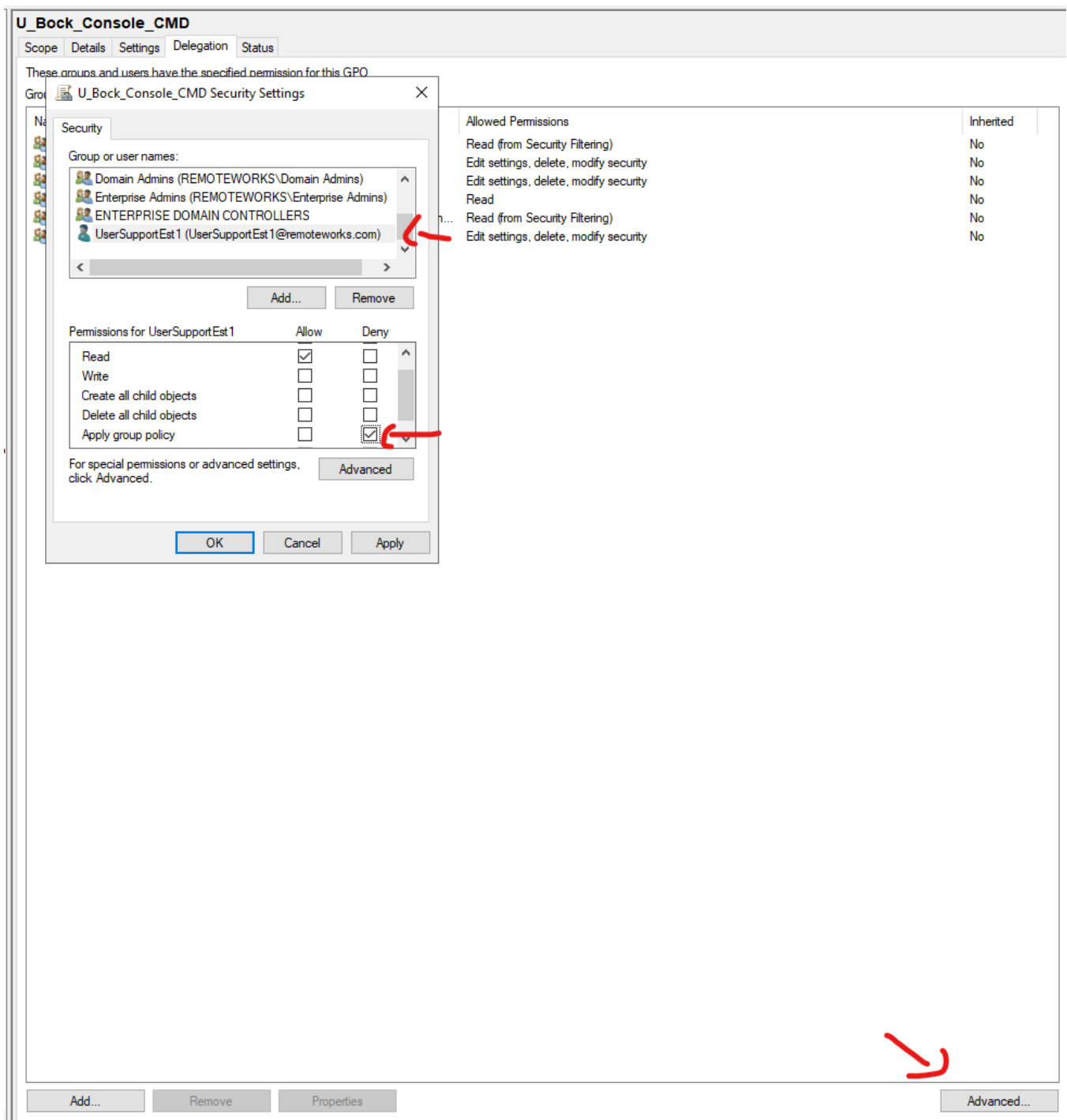
Au sein de l'onglet "**Délégation**", cliquez sur le bouton "**Avancé**" en bas à droite.

Cela va ouvrir **les paramètres de sécurité de la GPO et nous donner accès en direct aux permissions**. Nous allons ajouter le groupe "*Direction*" à cet endroit, pour cela il faut cliquer sur le bouton "*Ajouter*".

Maintenant que le groupe de sécurité "*Direction*" apparaît, il va falloir lui attribuer les bons droits :

- **Le droit "Lire" doit rester sur "Autoriser", comme c'est le cas actuellement**
- **Le droit "Appliquer la stratégie de groupe" doit être sur "Refuser"**

Ce qui donne :



Si c'est bon pour vous, il reste à valider. Un message d'avertissement va s'afficher pour **vous indiquer que le refus est prioritaire sur l'autorisation**. En bref, si un utilisateur est dans le groupe "Direction", le refus s'appliquera dessus même s'il est dans un autre groupe autorisé.

L'autorisation que l'on vient de définir apparaît comme "Personnalisé" dans la liste.

Groupe Support Technique Ouest (REMOTWORKS\Groupe Support Tech...	Read (from Security
SYSTEM	Edit settings, delete,
UserSupportEst1 (REMOTWORKS\UserSupportEst1)	Custom

L'opération s'arrête ici, comme d'habitude, il ne reste plus qu'à réaliser des tests de bon fonctionnement. Là, c'est à vous de jouer !

Qu'est-ce qu'une GPO Starter ?

Jusqu'ici, nous avons vu ensemble les stratégies de groupe "classiques" que l'on peut créer directement à partir de la console GPMC. Il y a un autre type de GPO qu'il est possible de créer, il s'agit de la "GPO Starter", mais alors à quoi

ça sert ? Comme son nom peut le laisser penser, **il s'agit d'une GPO qui va servir de point de départ pour créer une ou plusieurs autres GPO ; autrement dit il s'agit d'un template.**

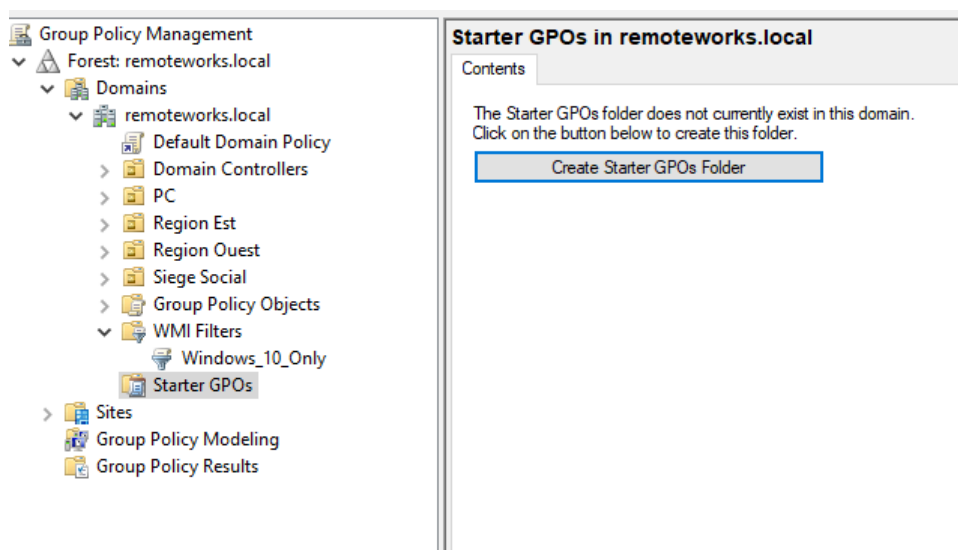
Il est alors possible d'utiliser une GPO Starter comme base pour créer une ou plusieurs GPO, cela peut-être utile si vous avez plusieurs variantes d'une même GPO à créer, mais que la base doit être commune, car vous avez à chaque fois des paramètres identiques. Vous créez cette base, et ensuite vous l'utilisez pour créer vos GPO afin d'ajouter seulement les paramètres spécifiques.

Note

Si l'on utilise une GPO Starter pour créer une GPO, et que l'on modifie ensuite la GPO Starter, cela ne va pas remettre à jour automatiquement toutes les GPO qui ont utilisé ce template. Le template est vraiment utilisé au départ lors de la création de la GPO, puis il n'y a plus de lien entre les deux objets par la suite.

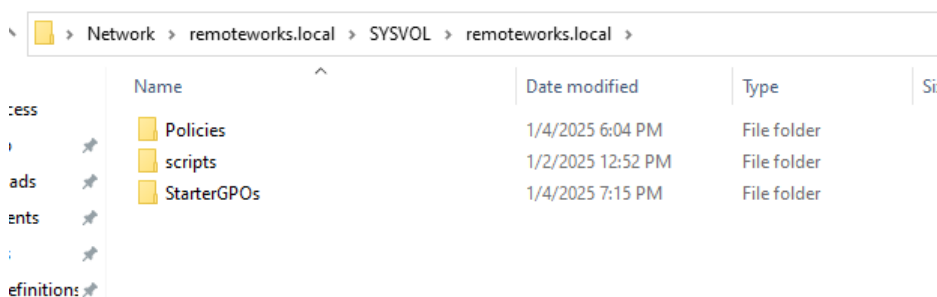
Créer une GPO Starter

À l'aide de la console GPMC, on retrouve ces GPO sous le container "**Objets GPO Starter**". De base, il faut initialiser les GPO Starter, il suffit de cliquer sur le bouton "**Créer le dossier des objets GPO Starter**". Vous verrez que par défaut il y en a 2, enfin ce nombre peut évoluer en fonction de la version de votre console GPMC.

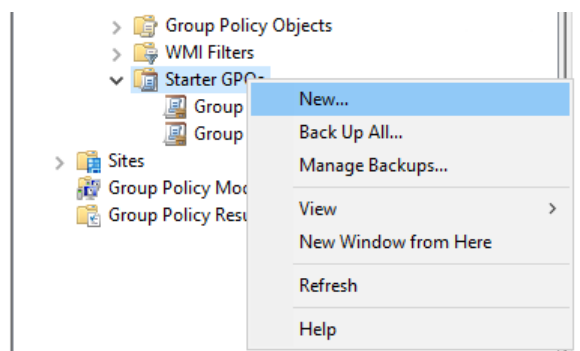


Concrètement, cela va générer

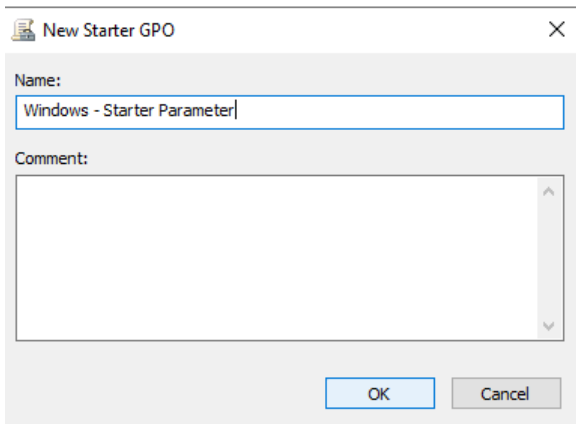
un nouveau dossier au sein du SYSVOL de votre domaine:



Ensuite, pour créer une nouvelle GPO Starter, il n'y a rien de compliqué : un clic droit sur "**Objets GPO Starter**" puis "**Nouveau**" sera suffisant pour ouvrir la fenêtre de création.



Donnez un nom à votre objet et pensez à indiquer un commentaire, puis validez. La GPO va ensuite être listée dans la liste des GPO Starter.



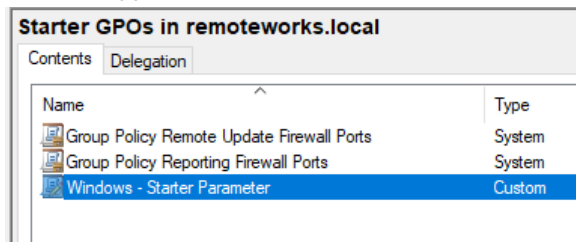
New Starter GPO

Name:
Windows - Starter Parameter

Comment:

OK Cancel

La GPO apparaît bien dans la liste.



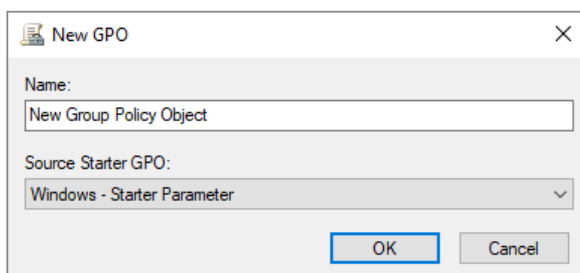
Name	Type
Group Policy Remote Update Firewall Ports	System
Group Policy Reporting Firewall Ports	System
Windows - Starter Parameter	Custom

Maintenant, il ne reste plus qu'à modifier cette GPO Starter et à la configurer comme n'importe quelle autre GPO. Néanmoins, les GPO Starter ne permettent pas de définir des paramètres de type "Préférences". Bien entendu, il n'est pas possible de lier cette GPO Starter sur une OU, le domaine ou un site de votre arborescence : il s'agit seulement d'un template.

Il est à noter que les GPO Starter peuvent être sauvegardées, sur le même principe que pour les GPO standards.

Créer une GPO à partir d'une GPO Starter

Si vous créez une GPO (classique) via la console GPMC, vous verrez qu'il y a l'option "**Objet Starter GPO source**" et que dans la **liste déroulante on retrouve bien la GPO Starter que l'on vient de créer**. Il suffit de la choisir et de valider.



New GPO

Name:
New Group Policy Object

Source Starter GPO:
Windows - Starter Parameter

OK Cancel

Le fait d'avoir sélectionné une GPO Starter lors de la création, cela implique que la GPO que vous venez de créer contient déjà des paramètres : elle contient tous ceux définis dans la GPO Starter au moment de la création.

Les préférences de stratégie de groupe

Avec Windows Server 2008, Microsoft a introduit des paramètres supplémentaires aux stratégies de groupe afin d'offrir des possibilités supplémentaires. **Il s'agit des préférences de stratégie de groupe, que l'on appelle également Group Policy Preferences (GPP).**

Pour rappel, lorsqu'un paramètre est défini dans une GPO et qu'il s'applique sur un utilisateur ou un poste, ce paramètre est forcé et ne peut pas être modifié par l'utilisateur. **Avec les préférences, c'est différent. En effet, ces paramètres sont déployés, mais peuvent être modifiés.**

Group Policy Preferences

Afin de mieux cerner les préférences de stratégies de groupe, voici ce que l'on peut en dire :

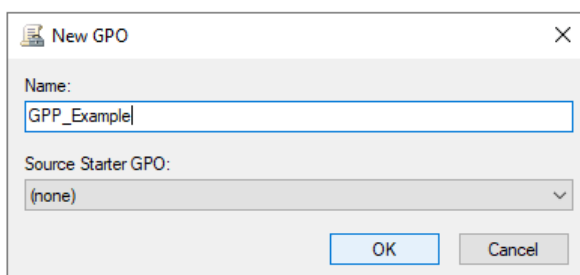
- Comme pour les paramètres d'une stratégie de groupe classique, elles existent pour **les ordinateurs et les utilisateurs**
- Les préférences sont configurables directement à partir de la **console classique GPMC**
- La **configuration déployée peut-être modifiée** par l'utilisateur
- Par défaut, si l'on **supprime une GPP qui s'applique sur un poste**, cela **ne supprime pas la configuration déployée par cette GPP**, contrairement aux paramètres classiques qui reviendraient à leur état initial
- Les **paramètres GPP sont différents des paramètres classiques**

Vous l'aurez compris, vis-à-vis des paramètres de stratégie de groupe, les préférences apportent plus de souplesse et offrent une façon supplémentaire d'administrer son parc informatique.

Que peut-on configurer avec les GPP ?

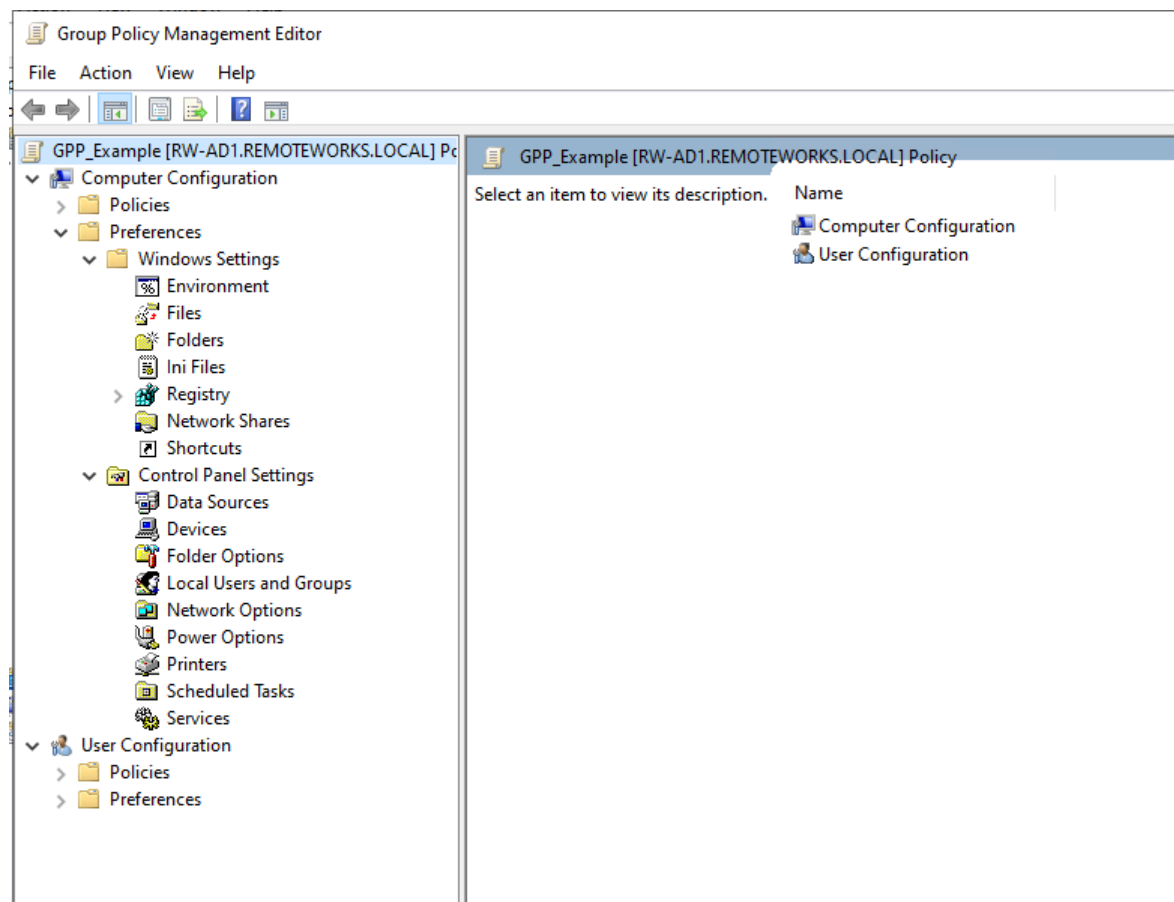
Lorsque l'on édite une stratégie de groupe, les préférences sont regroupées dans une section dédiée avec différentes sous-catégories. Maintenant, nous allons voir ce qu'il est possible de configurer via une GPP.

Créez une nouvelle [GPO](#) via la console GPMC pour que l'on regarde cela ensemble. Ensuite, éditez cette GPO.



Ensuite, que ce soit au niveau de la "**Configuration ordinateur**" ou de la "**Configuration utilisateur**", on retrouve un container "**Préférences**" : c'est sous ce container que se trouvent tous les paramètres GPP.

Au total, nous avons une vingtaine d'items, qui de par leur nom donne une idée de ce à quoi ils peuvent servir. Voyez par vous-même :



Pour que ce soit plus parlant et plus clair, voici quelques tâches que l'on peut réaliser grâce à une GPP :

- Déployer ou supprimer **une imprimante** sur la session d'un utilisateur
- Copier, écraser ou supprimer **un fichier** sur un ordinateur
- Créer un nouveau dossier ou supprimer **un dossier** existant
- Mapper **un lecteur réseau**
- Ajouter, modifier ou supprimer **une clé de registre**
- Créer un **nouveau raccourci** sur la session d'un utilisateur ou sur le "Bureau Public", par exemple
- Gérer **les variables d'environnement**
- Créer, supprimer et modifier **une tâche planifiée**
- Gérer **les utilisateurs et groupes locaux** d'un poste de travail
- Etc.

En fait de manière générale, on peut toujours réaliser trois actions : création, modification (de deux façons) ou suppression. L'action doit être choisie au moment où l'on définit le paramètre. Nous y reviendrons.

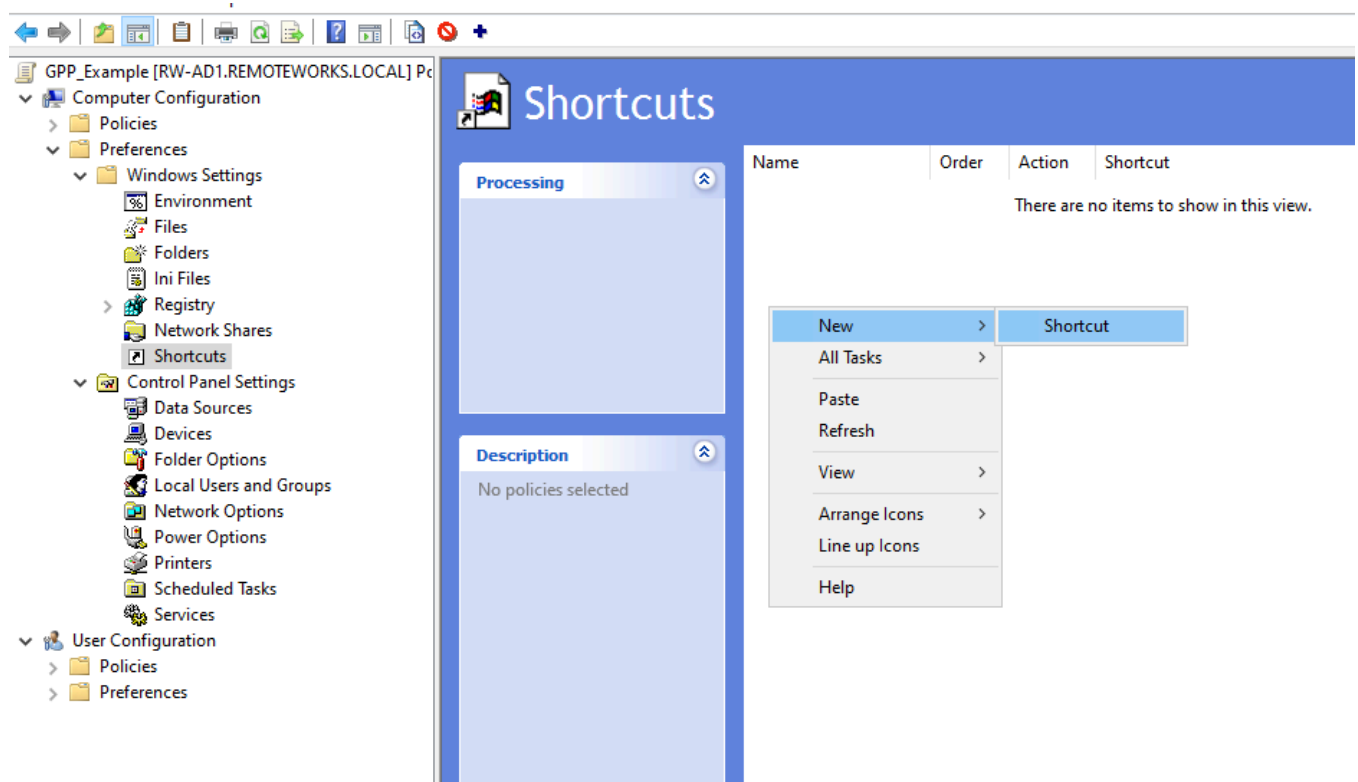
Pour créer une nouvelle configuration dans une GPP, il suffit de sélectionner l'item, par exemple "**Raccourcis**" et dans la fenêtre qui s'affiche à droite, de faire un clic droit puis "**Nouveau**".

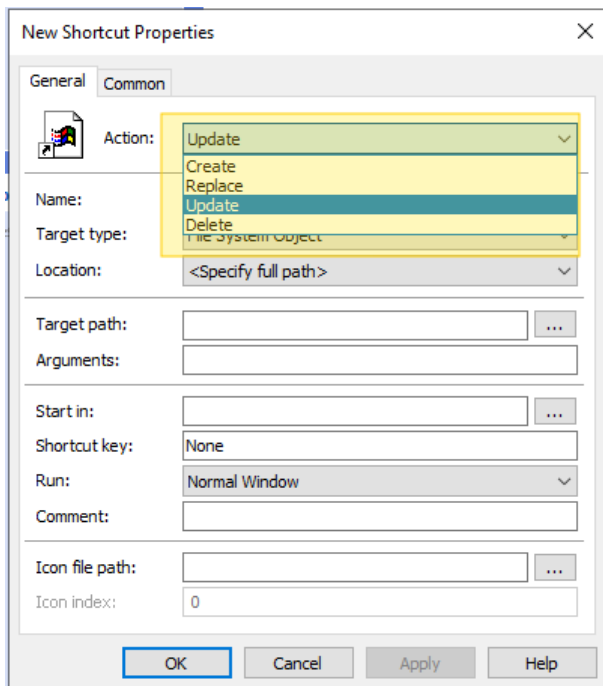
Vous verrez ensuite que le processus est spécifique à chaque item, bien qu'il y ait des points communs, mais cela est totalement différent des paramètres classiques où, pour la plupart, il suffit d'activer ou désactiver.

Les différents types d'actions

Comme je le disais précédemment, lorsque l'on crée une nouvelle configuration, on a le choix entre plusieurs actions. D'ailleurs, c'est le premier champ du formulaire et les valeurs proposées seront toujours les mêmes : **Créer**, **Remplacer**, **Mettre à jour** et **Supprimer**.

Exemple avec un raccourcis.





Plus précisément, voici des informations sur ces quatre actions :

A. Action "Créer"

Cette action doit être utilisée seulement pour créer quelque chose qui n'existe pas. Par exemple, pour ajouter un raccourci sur un PC s'il n'existe pas, s'il existe déjà et que vous souhaitez le modifier, n'utilisez pas cette action. Si l'objet cible existe déjà, le paramètre sera ignoré.

B. Action "Remplacer"

Cette action permettra de **supprimer l'objet existant et d'ajouter le nouveau à la place** avec les paramètres définis dans votre GPP. C'est sûrement l'action la moins utilisée.

C. Action "Mettre à jour"

Il s'agit de l'action par défaut et c'est celle qui est la plus utile. Si le paramètre que vous souhaitez mettre à jour n'existe pas, il sera créé automatiquement. S'il existe déjà, il sera mis à jour afin d'intégrer les nouveaux paramètres de votre GPP. En fait, cette action se rapproche du mode de fonctionnement d'une GPO : la configuration du poste sera mise à jour pour correspondre à ce qui est défini dans la GPP, tout en offrant la possibilité à l'utilisateur de modifier la configuration.

D. Action "Supprimer"

Comme son nom l'indique, **cette action sert à supprimer un objet créé par une GPP**, par exemple un fichier ou un raccourci. Souvenez-vous que lorsqu'une GPP n'est plus appliquée sur un ordinateur/utilisateur, cela ne supprime pas ce qu'elle a créé : cela est logique d'un sens, car imaginait si vous supprimez un dossier créé par GPP alors que l'utilisateur a stocké des données à l'intérieur... Cependant, pour permettre de supprimer ce qui n'est plus utilisé, par exemple une tâche planifiée, une clé de registre, etc... **Il faudra mettre à jour votre GPP pour utiliser l'action "Supprimer" à la place de "Mettre à jour" (ou autre) afin de faire le nettoyage.**

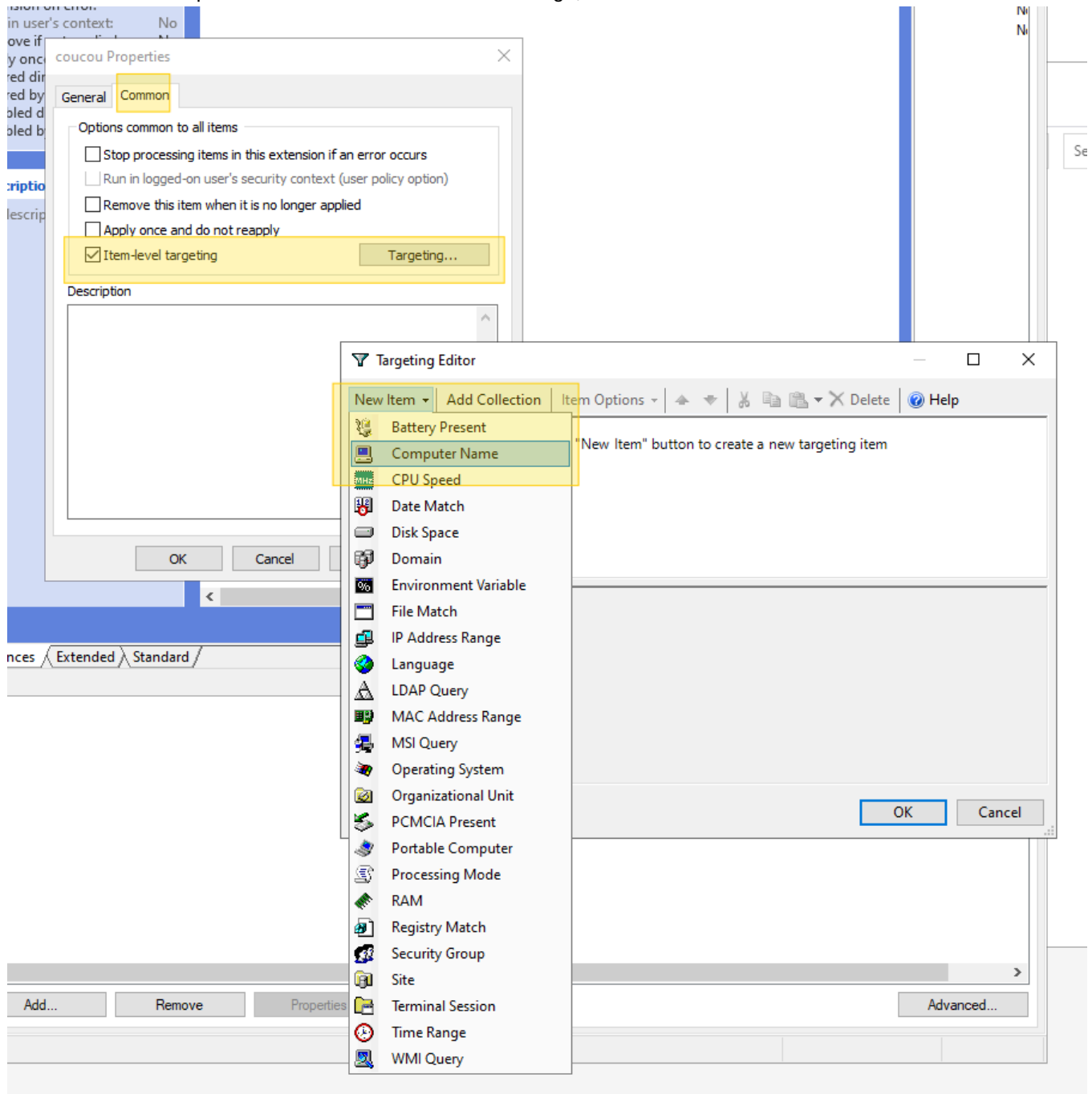
V. Le ciblage

En termes de ciblage, nous avons pu voir qu'une GPO peut s'appliquer sur une OU, un domaine ou encore un site, et qu'ensuite on peut réaliser un ciblage en jouant avec le filtrage de sécurité ou encore avec un filtre WMI. Avec les GPP on peut aller beaucoup plus loin, avec un ciblage qui peut se baser sur une multitude de critères, et ce, pour chaque paramètre de GPP créé.

Lorsque l'on crée une nouvelle configuration, il y a l'onglet "**Commun**" qui regroupe des paramètres communs à toutes les configurations GPP. C'est à ce niveau que l'on retrouve l'option "**Ciblage au niveau de l'élément**", qui, lorsqu'elle est active donne accès au bouton "**Ciblage**".

Ensuite dans l'éditeur de cible, vous allez pouvoir définir différents critères. Par exemple, créer un ciblage par rapport au nom de l'ordinateur, à la version du système d'exploitation, en fonction de l'appartenance de l'ordinateur ou de l'utilisateur à un groupe de sécurité spécifique, mais aussi par rapport à l'espace disque restant sur un volume spécifique d'un PC, à la langue du système, à la quantité de RAM ou encore en fonction d'une plage horaire.

Il y a des possibilités infinies puisque l'on peut définir plusieurs critères dans le même ciblage, avec des conditions différentes : ET / OU - EST / N'EST PAS. Je vous recommande tout de même de ne pas en abuser et de réaliser des tests de performance suite à l'utilisation du ciblage, notamment si vous commencez à cumuler les critères.



Avec ce chapitre, mon objectif était de vous proposer une vue d'ensemble des préférences de stratégie de groupe, notamment pour bien comprendre le fonctionnement et avoir une idée des possibilités offertes. Pour la suite, les fenêtres de configuration ayant chacune leurs spécificités, il serait intéressant de les utiliser dans des cas pratiques : comment déployer des lecteurs réseau, des imprimantes, etc. via les GPP.

GPO et Loopback processing

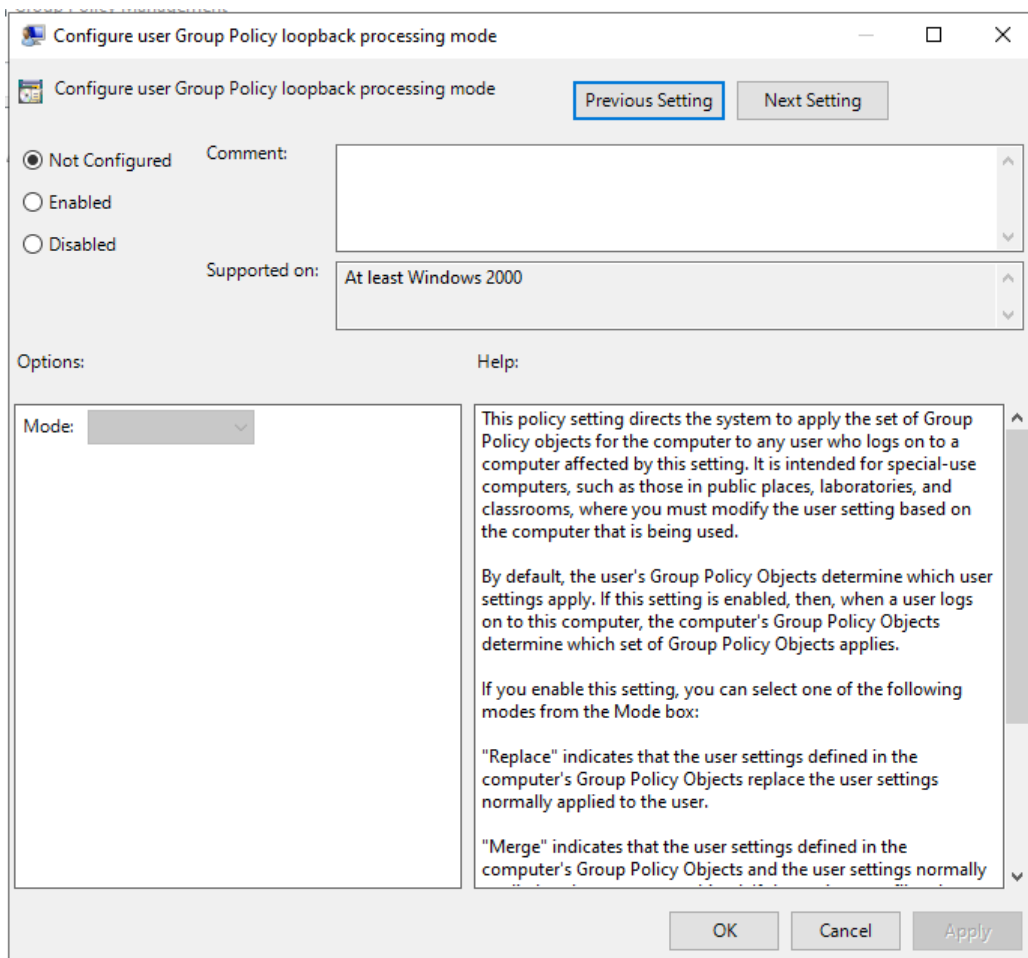
Lorsque l'on manipule et déploie des stratégies de groupe, il y aura forcément un moment où l'on entend parler de la notion de **"Loopback processing"**, ou en français **"Traitement par boucle de rappel"**. Le concept qui se cache derrière ce terme pose souvent des problèmes de compréhension : raison de plus pour vous en parler dans ce cours afin que ce soit bien compris.

Loopback processing

Lorsque l'on **édite une stratégie de groupe, la configuration se découpe en deux parties** : d'une part la section "*Configuration ordinateur*" et d'autre part la section "*Configuration utilisateur*". Si l'on veut appliquer des paramètres sur un ensemble de PC, nous allons modifier les paramètres de "*Configuration ordinateur*" et sur le même principe pour la partie utilisateur. Logique me direz-vous.

Par conséquent, lorsqu'un utilisateur ouvre une session sur un poste du domaine, les paramètres de [GPO](#) qui ciblent la machine sur laquelle il se connecte vont s'appliquer, ainsi que les paramètres de GPO qui ciblent le compte de l'utilisateur en lui-même. Ce cumul de paramètres va s'appliquer.

Cependant, ce mode de fonctionnement peut être impacté par le *Loopback Processing*. Tout d'abord, le traitement par boucle de rappel fait référence au paramètre de GPO suivant : **Configuration de l'ordinateur/Modèles d'administration/Système/Stratégie de groupe/Configurer le mode de traitement par bouclage de la stratégie de groupe utilisateur** (en anglais : *Configure user Group Policy loopback processing mode*).



Prenons un exemple : vous souhaitez que des paramètres utilisateurs s'appliquent seulement lorsqu'un utilisateur se connecte sur les machines contenues dans une OU spécifique. **Comment faire puisqu'il s'agit de paramètres de "Configuration utilisateur" et que notre GPO s'applique sur des objets ordinateurs ?** En activant le *Loopback processing*, nous allons **pouvoir faire en sorte que les paramètres qui s'appliquent sur l'utilisateur ne sont pas ceux appliqués sur l'objet utilisateur directement, mais ceux appliqués au niveau de l'objet ordinateur**. Subtile.

Ainsi, lorsqu'un utilisateur se connecte sur l'un des PC en question, il va recevoir des paramètres utilisateurs spécifiques à la connexion sur cet ordinateur. **Que se passe-t-il dans le cas où l'utilisateur a déjà certains paramètres configurés dans une GPO qui s'applique directement sur son objet AD ?** Lorsque l'on active le mode de traitement de la boucle de rappel dans la GPO (paramètre ci-dessus), il y a deux choix :

- **Remplacer (replace)** : les paramètres "utilisateurs" de la GPO ordinateur remplacent ceux de la GPO utilisateur, complètement.
- **Fusionner (merge)** : les paramètres "utilisateurs" des deux GPO sont fusionnés. S'il y a un conflit, c'est la valeur de la GPO qui s'applique sur l'ordinateur qui l'emporte.

Pour le *loopback processing* il y a deux cas d'usage intéressants :

- **Sur un serveur RDS** pour appliquer des paramètres spécifiques aux utilisateurs lorsqu'ils se connectent sur ce serveur de sessions
- **Sur un ensemble de postes de travail** où doivent s'appliquer des paramètres supplémentaires, par exemple des paramètres complémentaires lorsque la personne utilise un PC portable

La notion de *loopback processing* offre une flexibilité supplémentaire dans la gestion des stratégies de groupe, et il est très important de la connaître et de la comprendre. Cela peut s'avérer utile si vous avez besoin de réaliser un debug de GPO car il peut arriver que ce paramètre explique un comportement qui semblait anormal.

Exercice

****Contexte général**

Vous êtes nouvellement recruté(e) en tant qu'alternant administrateur/trice systèmes dans l'entreprise **ACME Solutions**, une ESN de 100 employés présente sur 3 sites (Lyon, Paris, Lille).

Le DSI souhaite renforcer :

- la **sécurité** des postes clients
- l'**homogénéité** du parc informatique
- la **conformité** vis-à-vis des normes internes
- le **contrôle des navigateurs**, notamment Firefox
- la **réduction des incidents liés à une mauvaise configuration**

Le parc informatique utilise :

- Active Directory Windows Server 2019-2022
- 100 postes Windows 10/11
- Firefox ESR comme navigateur standard

Votre mission : proposer, justifier et déployer un **ensemble cohérent de GPO avancées**, puis fournir un **POC (Proof of Concept)** fonctionnel.

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

Rédigez un document expliquant :

1. Les risques actuels sur les postes (sécurité, configuration hétérogène, productivité).
2. Vos objectifs techniques.
3. Un plan de déploiement GPO haute-niveau (schéma d'OU, ordre de priorité, etc.)

Mission 2 — Recherche & sélection de GPO pertinentes

Vous devez proposer **au moins 10 GPO avancées**, réparties en :

Sécurité du poste

Exemples possibles :

- 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 a Firefox(**obligatoire celle la!**)

Corporatisme & identité visuelle

- Fond d'écran imposé selon le site

- 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

Sur un environnement Windows Server + client Windows :

1. Créez une OU **POC-GPO**
2. Ajoutez un poste et un utilisateur de test
3. Créez et appliquez 10 GPO **minimum** parmi votre sélection
4. Vérifiez leur application via :
 - `gpupdate /force`
 - `gpresult /h rapport.html`
5. Documentez vos observations (captures obligatoires)

Livrable

Rédaction d'un document explicitant votre travail sur les 3 missions.

Pour la mission 3 il faudra fournir une documentation de la mise en place (screenshot et commentaire).

Fournissez également une sauvegarde des GPO que vous avez mis en place.