**Stratégie de groupe locale avec Windows**

Le service "Client de stratégie de groupe" (gpsvc) est responsable de l’application des paramètres configurés par les administrateurs pour l’ordinateur et pour les utilisateurs.

Les fichiers ADMX et ADML

* les fichiers ADMX sont dans le dossier c:\windows\PolicyDefinitions
* les fichiers ADML sont dans le dossier c:\windows\PolicyDefinitions\fr-FR

les fichiers ADML sont des fichiers spécifiques à la langue

On peut ajouter des fichiers ADMX et ADML supplémentaires.

Microsoft distribue des fichiers ADMX et ADML pour "**Office 365 - Office 219 - Office 216**".

**Administrative Template files (ADMX/ADML) and Office Customization Tool for Microsoft 365 Apps for enterprise, Office 2019, and Office 2016**

* admintemplates\_x64\_5191-1000\_en-us.exe
* office2016grouppolicyandoctsettings.xlsx

Microsoft distribue des fichiers ADMX et ADML pour "Edge Chromium".

* MicrosoftEdgePolicyTemplates.zip

Google distribue des fichiers ADMX et ADML pour "Chrome".

* policy\_templates.zip

**Lien entre stratégie de groupe locale et le registe**

La "Stratégie de groupe locale" permet de configurer des restrictions pour l'utilisation de Windows en spécifiant des paramètres à appliquer à l'ordinateur ou à l'utilisateur.

Lorsqu'on configure un paramètre de la stratégie de groupe locale on modifie une clé de registre.

Les clés du registre pour la "Configuration utilisateur":

* HKEY\_CURRENT\_USER\Software\Policies
* HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies

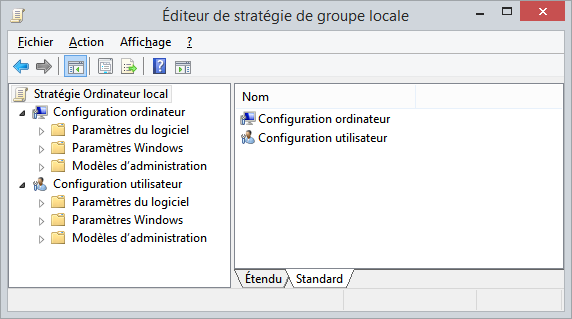
Les clés du registre pour la "Configuration ordinateur":

* HKEY\_LOCAL\_MACHINE\Software\Policies
* HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies

"Windows Serveur 2019" et "Windows 10" permettent de configurer environ 4500 stratégies.

**Les paramètres qui sont dans les Stratégies ne peuvent pas être modifiés par l'utilisateur.**

On démarre l'éditeur de stratégie de groupe locale avec gpedit.msc.



**GPEDIT.MSC et la "Configuration ordinateur**"

* Lorsque l’on configure la partie "**Configuration ordinateur**", elle s’applique que si la GPO est liée à une OU contenant des ordinateurs.
* Les paramètres de la stratégie de l'ordinateur sont appliqués lors du démarrage du poste et mis à jour aux 90 minutes avec un décalage aléatoire compris entre 0 et 30 minutes sur les postes clients mais aux 5 minutes sur le contrôleur de domaine.

Les fichiers POL pour la configuration ordinateur

* %ALLUSERSPROFILE%\ntuser.pol
* %windir%\system32\GroupPolicy\Machine\Registry.pol

**GPEDIT.MSC et la "Configuration utilisateur"**

* Lorsque l’on configure la partie "**Configuration utilisateur**", elle s’applique que si la GPO est liée à une OU contenant des utilisateurs.
* Les paramètres de la stratégie utilisateur sont appliqués à l'ouverture d'une session et mis à jour aux 90 minutes avec un décalage aléatoire compris entre 0 et 30 minutes sur les postes clients mais aux 5 minutes sur le contrôleur de domaine.

Les fichiers POL de la configuration utilisateur

* %USERPROFILE%\ntuser.pol
* %windir%\system32\GroupPolicy\User\Registry.pol

Les outils avec une interface graphique

* **gpedit.msc** est l’éditeur de stratégie de groupe locale
* **rsop.msc**

Cet outil affiche le jeu de stratégies résultant (RSoP).

Cet outil ne permet pas de sauvegarder le résultat.

RSOP (Resultant Set of Policy)

Les programmes sans interface graphique

* **gpresult.exe**

Cet outil de ligne de commande affiche le jeu de stratégies résultant (RSoP).

Cet outil permet de sauvegarder le résultat de la commande dans un fichier HTML.

* **gpupdate.exe**

Cet outil met à jour les paramètres de stratégie de groupe.

**exemples**

* Il est possible de gérer l'accès aux périphériques amovibles (USB, CD-RW, DVD-RW, ...)

si on modifie un des nombreux paramètres dans

Configuration ordinateur / Modèles d'administration / Système / Accès au stockage amovible

* Il est possible de modifier la liste des utilisateurs qui peuvent changer le fuseau horaire

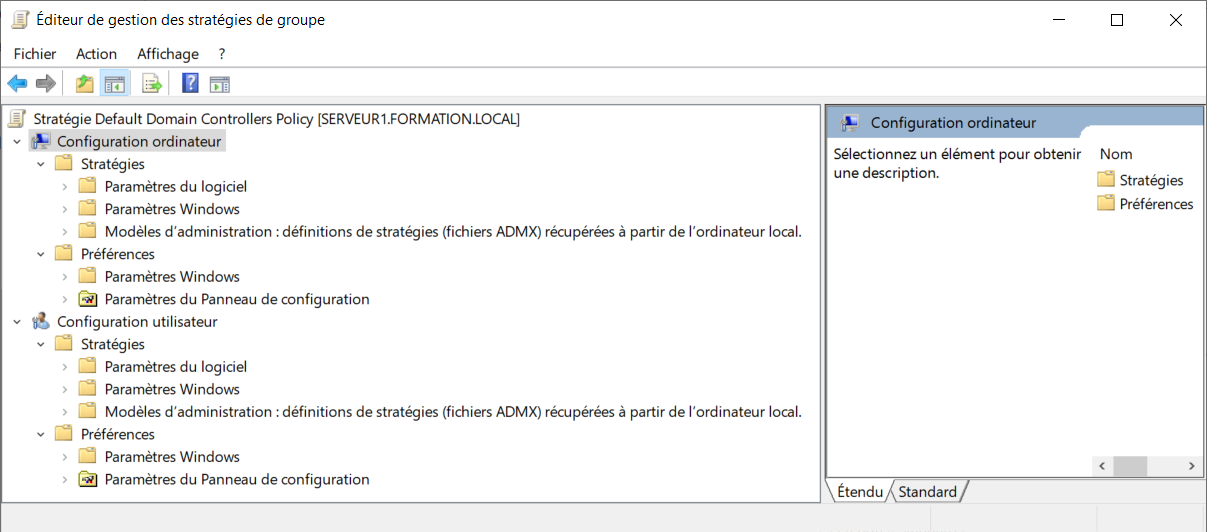
si on modifie le paramètre "Changer le fuseau horaire" dans

Configuration ordinateur / Paramètres Windows / Paramètres de sécurité /

Stratégies locales / Attribution des droits utilisateur

**Les GPO dans un domaine**

Les stratégies de groupe permettent une gestion centralisée des ordinateurs et des utilisateurs dans un environnement Active Directory.



Dans un domaine, un administrateur peut configurer des Stratégies et des Préférences.

Les paramètres qui sont dans les Préférence peuvent être modifiés par l'utilisateur.

Une GPO peut être liée

* à une OU 🡺 on la voit sous la OU
* à plusieurs OU 🡺 on la voit sous chaque OU
* à aucune OU 🡺 on la voit seulement dans la section OSG (Objets de stratégie de groupe)

Les GPO sont emmagasinées dans SYSVOL.

Dans un domaine, il existe deux GPO par défaut:

* Default Domain Policy
* Default Domain Controllers Policy



**Documentation sur l'ordre d'exécution des GPO**

L'ordre d'exécution des GPO respecte la formule LSDOU.

L pour Locale

S pour Site

D pour Domaine

OU pour "Unité d'organisation"

**Les bonnes pratiques pour la gestion des GPO**

1. Ne modifiez pas les stratégies "**Default Domain Policy**" et "**Default Domain Controller Policy**".

Si vous devez modifier des paramètres dans ces stratégies, vous devez créer d'autres stratégies.

1. Votre structure Active Directory doit faciliter l'application des stratégies.

La conception d’UO a une incidence sur le déploiement des stratégies de groupe.

Il est important de ne pas mélanger les comptes utilisateurs et ordinateurs dans une même UO.

Ne gardez pas les utilisateurs et les ordinateurs dans les conteneurs "**Users**" et "**Computers**".

1. Vous devez donner des noms significatifs à vos stratégies.

Les stratégies qui s'appliquent à des utilisateurs **U\_nom\_de\_la\_GPO**

Les stratégies qui s'appliquent à des ordinateurs **C\_nom\_de\_la\_GPO**

Les préférences qui s'appliquent à des utilisateurs **PU\_nom\_de\_la\_GPO**

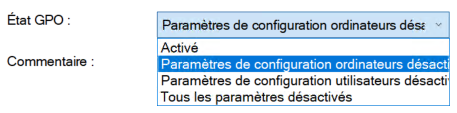
Les préférences qui s'appliquent à des ordinateurs **PC\_nom\_de\_la\_GPO**

1. Il est recommandé d'ajouter des commentaires à vos stratégies.
2. Vous ne devez pas créer des stratégies au niveau du domaine.

Parce que les stratégies s'appliquent à tous les utilisateurs et à tous les ordinateurs du domaine.

1. Il est préférable de créer plusieurs petites stratégies.
2. Pour augmenter la vitesse d'application des stratégies

Il faut désactiver les paramètres de configuration ordinateurs si la stratégie n'a aucun paramètre dans la section "**Configuration ordinateur**".



Il faut désactiver les paramètres de configuration utilisateurs si la stratégie n'a aucun paramètre dans la section "**Configuration utilisateur**".

