

Leçon 7 : Introduction aux GPO

Cette introduction aux GPO se base sur livre de référence (chapitre 3) :

[70-742] A. Warren, Exam Ref 70-742 : Identity with Windows® Server® 2016, 1st edition, Microsoft Press, March 2017

7.1 Introduction

La *stratégie de groupe* (**Group policy**) est un moyen important mis en place par les serveurs Windows Server afin de gérer de manière globale les politiques de configuration. Ainsi, il est possible de transmettre une politique de configuration déterminée à un ordinateur, un utilisateur ou un groupe de façon simple.

La stratégie de groupe est directement liée à la structure d'Active Directory. Ainsi, les paramètres que nous pouvons configurer sont *déployés* sur l'ensemble du domaine, sur les contrôleurs de domaine ou sur une unité d'organisation précise.

Les paramètres d'une stratégie de groupe, appelé *stratégie* (**Policy**) sont à sélectionner parmi les milliers d'option possibles. Les paramètres d'une stratégie peuvent porter sur des éléments très différents : ainsi, il est par exemple possible de désactiver l'utilisation de *regedit.exe*, le programme d'édition du registre ou encore, empêcher l'utilisateur d'atteindre le panneau de configuration.

Certains paramètres **sont applicables aux utilisateurs** (par exemple pour empêcher un utilisateur déterminé à modifier la configuration du système) alors que **d'autres sont applicables aux ordinateurs**. Nous en verrons quelques uns plus tard.

7.2 Les GPO

Une GPO²⁹ est une configuration reprenant une ou plusieurs stratégies et faisant partie d'une *stratégie de groupe*. La GPO s'applique à un ou plusieurs utilisateurs ou ordinateurs. Elle est déployée au niveau des postes et utilisateurs membres du domaine. Pour **créer ou modifier** une GPO, il faut utiliser l'outil de *Group Policy Management*

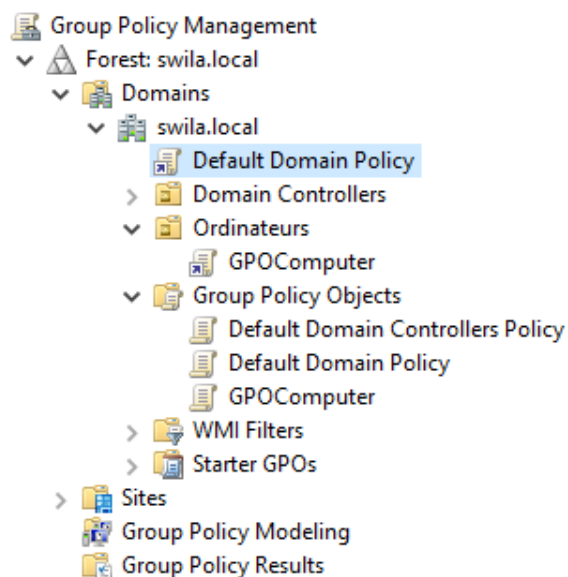


Figure 7.1 : Outil de gestion de stratégie de groupe

²⁹ Group Policy Object

Comme nous pouvons le voir sur la figure 7.1, dans le conteneur *Group Policy Object*, il y a 3 éléments : *Default Domain Policy*, *Default Domain Policy* et *GPOComputer* (qui est une stratégie créée).

Pour créer une nouvelle stratégie, il faut simplement faire un **clic-droit** sur ce conteneur et choisir **New**. Une fois le nom entré (par exemple *GPOComputer*), la stratégie est créée. Si nous souhaitons modifier la stratégie créée, il faut faire un **clic-droit** sur cette stratégie et choisir **Edit**.

Dès ce moment, on arrive dans l'outil d'édition de la stratégie de groupe. Sur la figure 7.2, on peut voir l'édition de la stratégie *Default Domain Policy*.

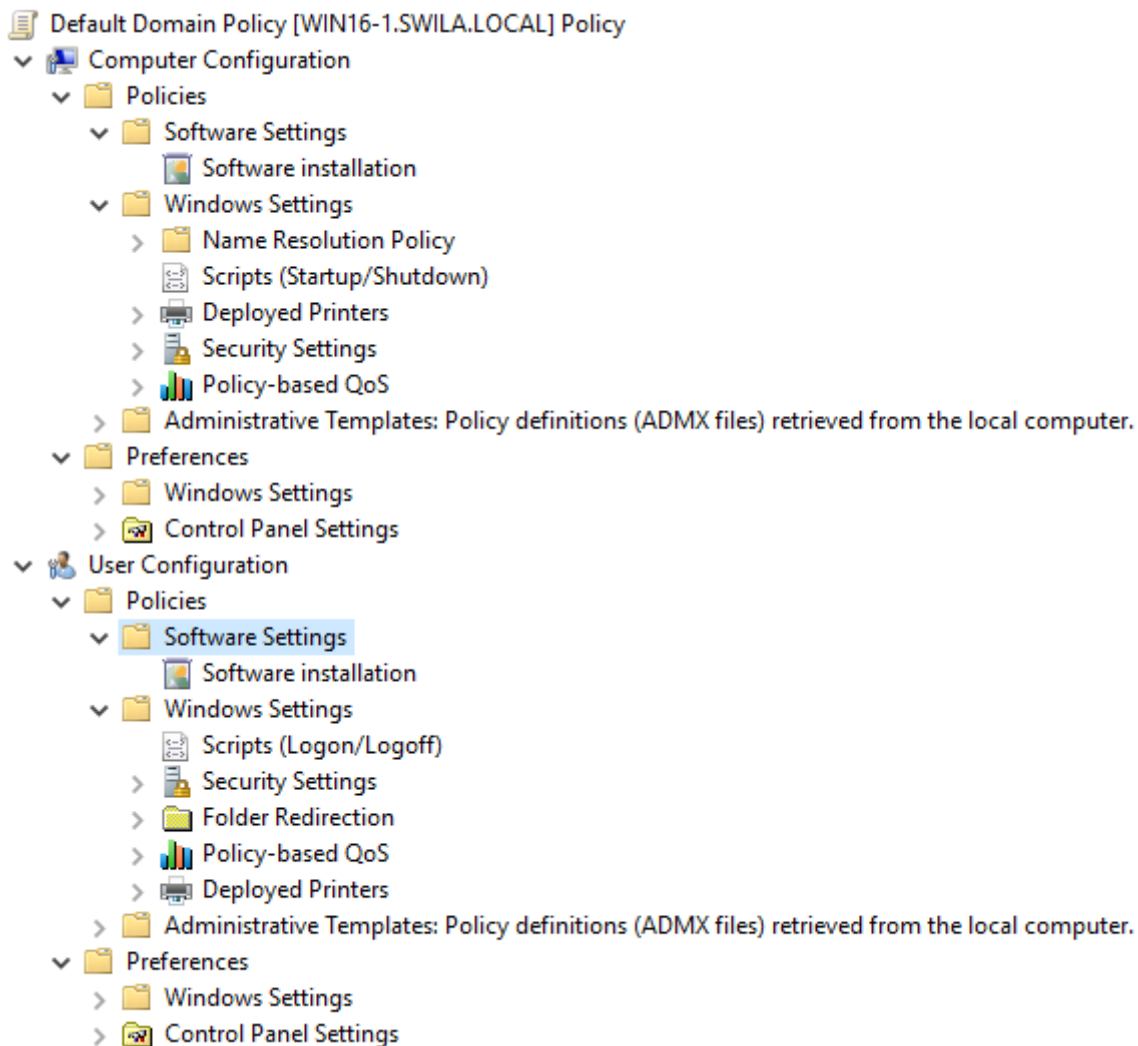


Figure 7.2 : Edition de stratégie *Default Domain Policy*

Dans le panneau de droite, on trouve toutes les stratégies configurables. Il y a des milliers de stratégies possibles et il faut dès lors faire son choix parmi celles qui sont proposées.

Sur la figure 7.3, on trouve les stratégies configurables de Uer Configuration\Administrative Templates\System. On remarque que les stratégies sont regroupées par thème (*Système*, *Accès au stockage amovible*, *Démarrage à chaud de Windows*, *Gestion de l'alimentation*, ...). A l'intérieur de chaque groupe, on retrouve les stratégies configurables. Chaque stratégie peut être *Not configured* (et

donc non modifiée par cette stratégie de groupe), *disabled* (désactivée) ou *enabled* (activée et donc prise en charge par la stratégie). Certaines stratégies, quand elles sont activées, nécessitent des éléments de configuration précis (comme par exemple le *délai d'expiration de mot de passe*).

Setting	State	Comment
Ctrl+Alt+Del Options		
Driver Installation		
Folder Redirection		
Group Policy		
Internet Communication Management		
Locale Services		
Logon		
Mitigation Options		
Power Management		
Removable Storage Access		
Scripts		
User Profiles		
Download missing COM components	Not configured	No
Century interpretation for Year 2000	Not configured	No
Restrict these programs from being launched from Help	Not configured	No
Do not display the Getting Started welcome screen at logon	Not configured	No
Custom User Interface	Not configured	No
Prevent access to the command prompt	Not configured	No
Prevent access to registry editing tools	Not configured	No
Don't run specified Windows applications	Not configured	No
Run only specified Windows applications	Not configured	No
Windows Automatic Updates	Not configured	No

Figure 7.3 : configuration de la stratégie de groupe

Ainsi, par exemple, nous pourrions configurer dans cette stratégie la **désactivation de l'invite de commande**. Il faut alors *activer* la stratégie *Prevent access to the command prompt*. Dans l'écran de configuration de cette stratégie, nous pouvons également désactiver le traitement des scripts (*disable the command prompt script processing*). Une fois cette stratégie active, l'utilisateur concerné par cette stratégie ne pourra plus accéder à l'invite de commande (l'invite de commande est la commande MS-DOS ou encore `cmd.exe`).

7.2.1 Etendue

Une fois la stratégie de groupe définie, il faut déterminer à quels utilisateurs et/ou ordinateurs elle va s'appliquer. L'étendue peut être **le site, le domaine ou une unité d'organisation** définie dans Active Directory. L'étendue définit la *frontière d'application* de la stratégie. Ainsi, une stratégie s'appliquant sur une unité d'organisation déterminée se limitera aux éléments contenus (i.e. les descendants) dans cette unité. On remarque dès lors l'apparition d'une notion d'*héritage* : la stratégie s'applique à tous les éléments enfants. En conséquence, plusieurs stratégies peuvent s'appliquer. Par exemple, si nous définissons une stratégie au niveau du domaine et une stratégie au niveau d'une unité d'organisation, les deux stratégies s'appliquent aux objets enfants (effectivement, les objets contenus dans l'unité d'organisation héritent des deux stratégies). Il est possible de déterminer la stratégie appliquée sur un objet donné en utilisant le *jeu de stratégie résultant* (RSOP) qui évalue toutes les stratégies applicables.

Il est également possible de *limiter* la partie d'une stratégie en spécifiant, par exemple, les **Security Filtering**. Ce paramètre permet de limiter l'application de la stratégie à des groupes de sécurité définis (i.e. aux utilisateurs, ordinateurs, ... faisant partie ou non de ces groupes). La stratégie peut également s'appliquer sur base des *filtres WMI* qui mentionnent des caractéristiques du système d'exploitation (version, service pack, ...).

Par défaut, **Security Filtering** contient l'élément *Authenticated Users* (les utilisateurs authentifiés). Si vous modifiez cette option (en remplaçant par un groupe d'utilisateur précis par exemple), il faut impérativement donner au groupe *Domain Computers* un accès en lecture (READ) sur cette GPO, via l'onglet **Delegation > Advanced**. Sans cette action, la stratégie pourrait ne pas s'appliquer³⁰.

7.2.2 Prise en compte

Une fois la stratégie définie, liée et appliquée, il faut que celle-ci se déploie sur l'ensemble des ordinateurs membres du domaine. En fait, les stratégies sont mises en place *coté client*. Ainsi, les ordinateurs membres du domaine téléchargent les stratégies et les appliquent à leur propre configuration (modification du registre).

Les stratégies sont automatiquement téléchargées lorsque l'ordinateur démarre (stratégie *Computer Configuration*), lorsque l'utilisateur se connecte (stratégie *User Configuration*) et toutes les 90 à 120 minutes. Il est possible de demander à l'ordinateur client de mettre à jour sa stratégie en utilisant l'outil `GPUpdate.exe`. L'outil peut être exécuté sur le contrôleur de domaine ou sur le poste client.

7.2.3 Types de GPO

Il existe, depuis l'apparition de Windows Server 2000, la possibilité de définir une stratégie s'appliquant localement au serveur lui-même. Cette stratégie est particulièrement intéressante lorsque le serveur travaille en mode autonome (i.e. ne fait pas partie d'un domaine). Depuis Windows Server 2008, il est possible de définir *plusieurs* stratégies locales s'appliquant par exemple à des groupes d'utilisateur différents (i.e. les administrateurs, les non-administrateurs, ...). Ces stratégies locales sont accessibles au moyen de la console MMC si l'on ajoute le *composant snap-in* nommé *Group Policy Object*. Lors de l'ajout de ce composant, en cliquant sur **Browse**, il y a 2 onglets (Computers et Users), il est possible de spécifier le groupe auquel elle s'applique. Uniquement si l'ordinateur ne fait pas partie du domaine.

Dans un **domaine Active Directory**, deux GPO par défaut sont ajoutées :

- **Default Domain Policy** – Politique par défaut s'appliquant à tout le domaine installé (car elle est *liée* au domaine). Cette politique définit les contraintes de mot de passe et de sécurité qui sont appliquées pour tous les utilisateurs et ordinateurs. Il n'est pas recommandé de modifier cette politique (sauf pour modifier les éléments qu'elle configure comme la stratégie des mots de passe), il faut plutôt ajouter une nouvelle politique et lier celle-ci au domaine.
- **Default Domain Controllers Policy** – Cette politique est liée à la GPO *Domain Controllers* installée par Active Directory. Elle s'applique à tous les contrôleurs de domaine du domaine (car elle est *liée* à l'OU *Domain Controllers*). Cette politique définit donc les restrictions qui sont appliquées aux contrôleurs. Si d'autres restrictions ou configurations particulières doivent être prévues, il convient de modifier cette GPO.

³⁰ <https://blogs.technet.microsoft.com/askds/2016/06/22/deploying-group-policy-security-update-ms16-072-kb3163622/>

7.2.4 Lier des GPO

Nous avons déjà vu comment il était possible de créer une nouvelle stratégie. Cependant, une fois la stratégie créée, il convient de la *lier* (i.e. l'appliquer) à un élément particulier d'Active Directory. Ainsi, pour réaliser cette opération de liaison, il faut, dans l'outil *Group Policy Management* (voir figure 7.1), faire un **clic-droit** sur l'élément auquel on souhaite appliquer la stratégie (le site, le domaine ou l'unité d'organisation) et choisir l'option **Link an Existing GPO**. Ensuite, il faut choisir la stratégie à appliquer.

Une fois liée, il est possible de spécifier les paramètres de filtre (filtrage *Security Filtering* et *WMI Filtering*) pour limiter la portée de la stratégie. Il est également possible de spécifier des paramètres de *délégation* (onglet *Delegation*). Ces paramètres mentionnent les utilisateurs (ou groupes) et autorisations applicables à la modification de cette stratégie. Ainsi, il est possible de définir une stratégie qui est gérée (i.e. déléguée) par quelqu'un d'autre. Il est ainsi possible de définir des administrateurs particuliers ayant des pouvoirs limités dans l'adaptation de la stratégie.

Les GPO sont mémorisées sur tous les contrôleurs de domaine dans le dossier %SystemRoot%\SYSVOL\Domain\Policies\GUID GPO. La GPO se matérialise en deux composants : un conteneur de stratégie de groupe et un modèle de stratégie de groupe. Ces fichiers sont répliqués entre les contrôleurs de domaine en cas de modification.

7.3 Paramètres d'une GPO

Les paramètres d'une GPO regroupent les stratégies que l'on peut activer. Comme dit précédemment, il y a des milliers de stratégies possibles.

Comme l'on peut le voir sur la figure 7.2, on distingue 2 sections principales : la *Computer configuration* et la *User Configuration*. A l'intérieur de chaque configuration, on trouve **les politiques** (i.e. politiques applicables) et **les Preferences** (nouvelles à partir de Windows Server 2008).

Les **Politiques** comprennent chacune les *Software Settings*, les *Windows Settings* et les *Administrative Templates*. Les *Software Settings* permettent une installation et un déploiement de programmes. Les *Windows Settings* permettent de définir des scripts, des paramètres de sécurité, rediriger des dossiers (dans le cas des utilisateurs), ... Il faut **bien distinguer les stratégies applicables à l'ordinateur et celles applicables à l'utilisateur**. Ainsi, la section *script* (présente des deux côtés) se comporte comme suit :

- Un script défini au niveau de la *Computer Configuration* s'exécute au démarrage ou à l'arrêt de la machine alors qu'aucun utilisateur n'est connecté
- Un script défini au niveau de la *User Configuration* s'exécute au démarrage ou à l'arrêt de la session de l'utilisateur (par conséquent, on sait qui se connecte et le script s'exécute avec les droits de ce dernier).

Dans l'élément *Administrative Templates*, on trouve des stratégies de configuration de l'environnement utilisateur ou ordinateur. Il est ainsi possible de limiter l'accès à certaines fonctionnalités : verrouillage de l'ordinateur, accès au panneau de configuration, ...

Etant donné le nombre de stratégies différentes (plusieurs milliers), elles sont présentées de manière hiérarchique dans des dossiers les regroupant logiquement.

Les **Préférences** sont des nouveaux éléments introduits à partir de Windows Server 2008 et Windows Vista. Elles permettent une gestion centralisée des variables d'environnement, de certaines applications, des disques réseaux, ... Ces préférences sont également intéressantes pour gérer les connexions aux imprimantes, ...

7.4 Etude de l'étendue d'une stratégie de groupe

Comme nous l'avons vu, plusieurs stratégies de groupe peuvent être applicables à un ordinateur ou un utilisateur. En effet, il est possible de *lier* une stratégie à un site, un domaine ou une unité d'organisation en sachant que celle-ci se propage à tous les éléments enfants (effet d'héritage).

Il est même possible de lier une stratégie de groupe à **plusieurs** unités d'organisation. Cette particularité peut s'avérer utile pour des unités d'organisation qui ne sont pas parentes (par exemple pour appliquer une même stratégie aux membres de l'unité *Professeur* et *Etudiant*).

Cependant, cette liaison et cet héritage complexifient un peu la stratégie applicable à un élément. En effet, quels sont les éléments prioritaires ? Que se passe-t-il si des éléments contradictoires, de deux stratégies différentes sont définis ? Lesquels s'appliquent ?

7.4.1 Priorité

Pour connaître la priorité d'une GPO, il faut aller dans l'outil *Group Management Policy* et cliquer sur le conteneur souhaité (une unité d'organisation, le domaine, ...) et regarder l'onglet *Group Policy Inheritance*.

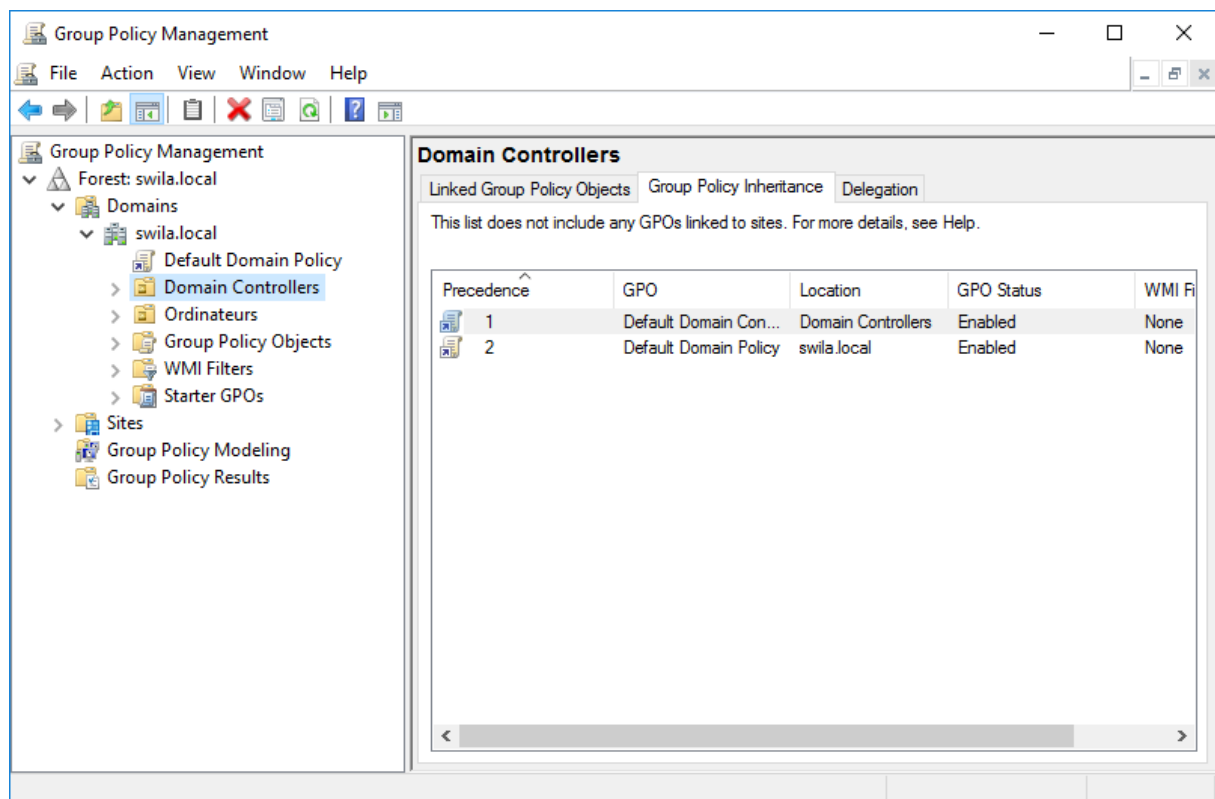


Figure 7.4 : Héritage des stratégies sur l'unité *Domain Controllers*

Comme nous pouvons le voir sur la figure 7.4, cet onglet renseigne les GPO applicables mais également leurs priorités. Il s'agit d'un élément important pour comprendre comment les stratégies définies vont effectivement s'appliquer sur les utilisateurs et ordinateurs membres du domaine. Dans notre exemple, nous remarquons que la GPO *Default Domain Controllers Policy* s'applique en premier (directement liée à l'unité d'organisation *Domain Controllers*) et ensuite, la GPO *Default Domain Policy* s'applique.

La priorité³¹ avec laquelle les GPOs s'appliquent est la suivante (plus le numéro est élevé, plus la priorité est importante) : «

1. L'objet de stratégie de groupe local (LPGO) est appliqué.
2. Les objets de stratégie de groupe (GPO) sont liés aux sites.
3. Les objets de stratégie de groupe (GPO) sont liés aux domaines.
4. Les objets de stratégie de groupe (GPO) sont liés aux unités d'organisation. Dans le cas d'unités d'organisation imbriquées, les GPO associés aux unités d'organisation parentes sont traités avant les GPO associés aux unités d'organisation enfants.

Ainsi, on pourrait résumer comme suit : le traitement des objets de stratégie de groupe (GPO) repose sur le principe selon lequel **le dernier qui écrit gagne**, et les GPO qui sont traitées ensuite ont priorité sur ceux qui ont été traités précédemment. »

Bien sûr, lorsque plusieurs GPO sont liées au même conteneur (à la même unité d'organisation par exemple), la priorité est définie par l'ordre des liens (montré dans l'onglet *Objets de stratégie de groupe liés*, premier onglet de la fenêtre figure 7.4).

Il est possible de modifier cet ordre de plusieurs manières. La première est la possibilité est l'option **Block Inheritance** sur un conteneur donné (une unité d'organisation par exemple). Ce faisant, cette unité n'hérite plus d'aucune autre GPO et seules les GPO directement liées à cette unité dans l'ordre mentionné s'appliquent. **Dans la plupart des cas, ce n'est pas une bonne manière de fonctionner³²**. Il convient de limiter l'utilisation de cette possibilité lorsque celle-ci s'avère vraiment indispensable. Si nous reprenons l'exemple de la figure 7.4, bloquer l'héritage reviendrait à n'avoir que la seule GPO *Default Domain Controllers Policy* active sur l'unité.

Une autre méthode pour modifier l'ordre de priorité est d'utiliser l'**option Enforced** d'une GPO. Dans ce cas, cette GPO *Enforced* se voit gratifiée de la priorité la plus grande. A nouveau, si dans notre exemple nous activons cette option sur la GPO *Default Domain Policy*, les priorités d'application des GPO sont, à nouveau, chamboulées : la GPO *Default Domain Policy* s'applique d'abord. **Attention !** L'option *Enforced* est prioritaire sur la possibilité de bloquer l'héritage. De plus, activer cette option sur une GPO définie à un niveau supérieur est toujours prioritaire sur l'activation de l'option sur une GPO définie dans l'objet courant (ainsi, activer *Enforced* sur la GPO *Default Domain Policy* et *Default Domain Controllers Policy* implique un ordre de priorité suivant : *Default Domain* puis *Default Controllers*). Ce choix est finalement assez logique, cela permet à une entreprise de définir une politique de sécurité globale appliquée à toute l'entreprise et non modifiable par un administrateur local (en charge de la gestion des stratégies d'une GPO, d'une branche de l'entreprise, ...).

³¹ Extrait de [http://technet.microsoft.com/fr-fr/library/cc757050\(v=ws.10\).aspx](http://technet.microsoft.com/fr-fr/library/cc757050(v=ws.10).aspx)

³² Ainsi, appliquer cette option **doit être une exception**, plutôt qu'une règle.

7.4.2 Application

Nous avons vu précédemment qu'il était possible de restreindre l'application d'une GPO en utilisant les options de filtres. Cette possibilité permet, par exemple, d'appliquer une GPO à un groupe de sécurité donné ou un type d'ordinateur défini. Par contre, il est souvent intéressant d'**exclure un groupe** d'une GPO afin que celle-ci ne s'applique jamais aux membres de ce groupe. Pour y arriver, il faut passer par l'onglet *Delegation* sur une GPO (qui permet normalement de déléguer la gestion d'une unité à un groupe donné). Il est possible de modifier le droit associé (via l'option *Advanced*) sur l'unité et cocher *Deny* pour la permission *Apply group policy* (qui refusera l'application de la stratégie).

Il est également possible de définir des filtres dans la section *WMI Filtering* pour restreindre l'application d'une GPO à une configuration donnée. Des exemples de tels filtres sont donnés sur le site suivant : <https://docs.microsoft.com/en-us/windows/access-protection/windows-firewall/create-wmi-filters-for-the-gpo>.

Ainsi, pour cibler les ordinateurs dont la configuration est Windows 10 ou Windows Server 2016, il est possible d'utiliser la requête WMI suivante (tirée du livre de référence [70-742]) :

```
Select * FROM Win32_OperatingSystem WHERE Version LIKE "10.%"
```

Ainsi la GPO ne s'applique alors qu'à ces seules configurations.

Enfin, il est également possible (via l'option *GPO Status* dans l'onglet *Details*) d'activer ou désactiver des paramètres définis dans la *Computer Configuration* ou de la *User Configuration* d'une GPO. Ainsi, une GPO peut être en état *Enabled* et donc tous les paramètres sont traités durant le déploiement, *All settings disabled* ainsi cette GPO n'est pas utilisée ou encore *computer configuration disabled* ou *user configuration disabled*. L'utilisation de ces options est à réserver à des cas très spécifiques !

7.4.3 La boucle de rappel

Parfois, on souhaite modifier la stratégie qui s'applique à l'utilisateur en fonction de l'ordinateur sur lequel il se connecte. Par exemple, un ordinateur particulier, sur lequel un logiciel précis tourne pourrait disposer de protection différente au niveau de la configuration utilisateur.

Or, la stratégie utilisateur s'applique quelque soit l'ordinateur sur lequel il se connecte. Afin de pouvoir personnaliser la stratégie utilisateur en fonction de l'ordinateur, Active Directory supporte le concept de *boucle de rappel*.

C'est une stratégie *Computer Configuration* visible dans `Policies\Administrative Templates\System\Group Policy\Configure user Group Policy loopback processing mode`. Ce paramètre peut être *not configured*, *enabled* ou *disabled*. Une fois *activé (enabled)*, cette stratégie propose deux modes de fonctionnement : **replace** qui permet de ne pas tenir compte de la stratégie actuelle de l'utilisateur mais de traiter tous les utilisateurs sur base de la configuration utilisateur de cette stratégie ; **merge** qui permet d'ajouter des nouvelles stratégies à la stratégie utilisateur (uniquement applicable à la connexion sur cet ordinateur). La boucle de rappel sera étudiée plus précisément dans une leçon ultérieure.

7.5 Déterminer la stratégie appliquée

Comme nous l'avons décrit, les stratégies applicables à l'utilisateur et à l'ordinateur peuvent être multiples, héritées, liées, et parfois, des configurations viennent compliquer les choses comme les options *Enforced* ou *block inheritance* sans oublier l'activation de *la boucle de rappel* ou encore les *filtres*. Tous ces mécanismes rendent difficile l'analyse en cas de défaillance d'une configuration.

En effet, il est dès lors peu aisé d'identifier clairement les stratégies qui sont appliquées à un utilisateur donné. Pour ce faire, il est possible de déterminer le *jeu de stratégie résultant* (RSoP pour *Result Set of Policies*) qui analyse et déduit la stratégie appliquée. RSoP peut envoyer une requête à un ordinateur concernant la stratégie appliquée à celui-ci ou à un utilisateur qui se connecterait sur ce dernier. Le rapport est intéressant pour analyser et comprendre ce qui se passe.

Cet outil existe en deux versions : dans la console *Group Policy Management* (figure 7.4), on peut voir, comme dernière option sur la gauche, l'élément **Group Policy Results**. Grâce à cette option, il est possible en faisant un **clic-droit** sur le panneau de droite de choisir l'option **Group Policy Results Wizard**. Une fois les options spécifiées, le système affiche un rapport précisant la stratégie appliquée.

La seconde version de l'outil est un *programme exécutable nommé* `gpresult.exe`. Ce programme rédige un rapport HTML mentionnant la stratégie applicable en fonction des options activées. L'aide de cet outil est disponible ici : `gpresult.exe /?`.

7.6 Quelques stratégies courantes

7.6.1 Connexion à des dossiers partagés

Un des grands avantages de l'utilisation des GPO est la possibilité de **connecter automatiquement** les lecteurs réseaux des utilisateurs sans devoir faire les modifications manuellement à l'intérieur de chaque session.

Pour ce faire, il y a 2 méthodes : l'utilisation d'un **script d'ouverture de session** et l'utilisation de la commande `net use` vue précédemment. Cette méthode était utilisée pour connecter les lecteurs réseaux sur des systèmes antérieur à Windows Vista / Windows Server 2008. L'autre méthode est de passer par les **préférences** dans la stratégie. Nous allons présenter les deux.

En ce qui concerne le **script**, il faut aller dans `User Configuration\Policies\Windows Settings\Scripts\Logon` et puis ajouter un nouveau script à l'emplacement proposé (ou bien dans un chemin réseau accessible). Les scripts supportés sont les scripts batch (fichier `.bat`) ou Powershell pour des ordinateurs clients Windows 7 et suivants (fichier `.ps1`).

En ce qui concerne les **préférences**, il faut aller dans `User Configuration\Preferences\Windows Settings\Drive Maps`. Il convient alors d'ajouter un nouveau mappage en mentionnant, comme emplacement, un chemin réseau `\\SERVEUR\Partage`.

7.6.2 Ouvrir une session sur le contrôleur de domaine

Il est parfois utile de permettre à certains utilisateurs d'ouvrir une session locale sur le contrôleur de domaine. Pour activer cette option, il faut modifier une GPO existante : **Default Domain Controllers Policy**. L'élément à modifier se trouve dans : `Computer Configuration\Policies\Windows`

Settings\Security settings\Local Policies\User Rights Assignment\Allow log on locally. **Attention, il convient d'ajouter les utilisateurs / groupes souhaités sans modifier les valeurs déjà définies !**

7.6.3 Ne pas afficher le dernier utilisateur connecté

On remarque que, par défaut, le système mentionne le dernier utilisateur connecté sur la machine. Ce comportement peut être déroutant sur des ordinateurs partagés. Dès lors, il faut modifier la stratégie suivante : Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name.

Attention ! Il s'agit d'une stratégie sur l'ordinateur, elle s'applique donc aux objets ordinateurs d'Active Directory. Elle doit donc être placée dans une branche contenant de tels objets.

7.6.4 Redirection des dossiers

Comme nous l'avons vu, le profil de l'utilisateur reprend toutes ses informations. Depuis le passage en domaine, il convient de mentionner un chemin réseau pour le profil de l'utilisateur. Nous avons également vu que lors de la connexion en utilisant un profil itinérant, celui-ci était copié sur la machine locale, géré localement, puis recopié sur le serveur lors de la déconnexion. Enfin, nous avons également vu que **plusieurs versions** du profil (suffixées par « .V2 » ou « .V6 ») peuvent être créées suivant la version du système.

Le problème est que, plus le profil grossit (nouveaux documents, fichiers importants sur le bureau, ...), plus le temps de connexion grandit également. Une solution à ce problème est de *rediriger* les dossiers importants (Bureau, Mes documents, ...) dans un espace réseau. De cette manière, ces informations ne sont plus recopiées sur chaque machine, elles restent sur le serveur et la modification est réalisée directement depuis cet endroit. De plus, elles sont communes à toutes les versions du profil.


Ainsi, il est tout à fait possible de préciser une stratégie pour rediriger ces dossiers. Il faut modifier le paramètre suivant : User Configuration\Policies\Windows Settings\Folder Redirection et choisir les modifications souhaitées. Il convient, bien sûr, de préciser un chemin réseau vers l'emplacement souhaité.

Pour que la modification soit effective dans tous les cas, il faut également ajouter une stratégie sur les ordinateurs concernés : Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure folder redirection policy processing.

7.6.5 Et le reste ...

Il existe des milliers de stratégies possibles et il n'est pas possible de les détailler toutes ici. Il est parfois difficile de trouver une stratégie voulue. C'est pourquoi Microsoft a introduit une option de filtrage sur la branche *Administrative Templates*. Cette option est particulièrement intéressante pour trouver une stratégie dans l'ensemble. Pour l'activer, il suffit de faire un **clic-droit** sur *Administrative Templates* puis **Filter Options**.

7.7 Exercices

1. Empêcher les membres des catégories *étudiants* et *e-learning* d'avoir accès à l'outil d'édition du registre. **Créez une seule GPO liée aux OUs concernées.**
2. Empêcher tous les utilisateurs, excepté les membres de la catégorie *informatique*, de lancer l'invite de commande. **Limitez aux utilisateurs concernés en utilisant les filtrages de sécurité (Security Filtering) uniquement.**
3. Créer un partage réseau `SharedSocial` et connecter les membres de la catégorie *social* à ce partage **en utilisant un script batch** (lecteur `X:`, accès en modification pour *social*, inaccessible pour les autres). Ajoutez une GPO Ordinateur « *Configure Logon Script Delay* » à 0 minute, sur les postes clients (VM Windows 10).
4. Pour protéger la stratégie des mots de passe du domaine, arrangez-vous pour que celle-ci soit toujours prioritaire (en 1^{ère} position dans l'onglet *Group Policy Inheritance*).
5. Permettre aux membres de la catégorie *informatique* d'ouvrir une session locale sur le contrôleur de domaine
6. Pour des questions de sécurité, on ne souhaite pas voir apparaître le nom de la dernière personne connectée sur les postes clients (VM Windows 10).
7. Réaliser une redirection de dossier (tous) pour les membres de la catégorie *travaux* de sorte que les dossiers soient placés dans leur profil. Ainsi, leur bureau devra se trouver dans `CGData\<login>\Desktop` (et ainsi de suite pour tous les dossiers).
8. Créer un partage réseau `SharedPublic` et connecter tous les utilisateurs à ce partage au moyen d'une préférence (lecteur , tout le monde en lecture, *direction* en modification).
9. Pour s'amuser : restrictions pour les membres de la catégorie *juridique* :
 - a. Supprimer : l'accès au menu contextuel de la barre des tâches, Supprimer l'horloge,
 - b. Le bureau : supprimer tous les éléments du bureau
 - c. Système : Désactiver le verrouillage de l'ordinateur ; supprimer le gestionnaire des tâches