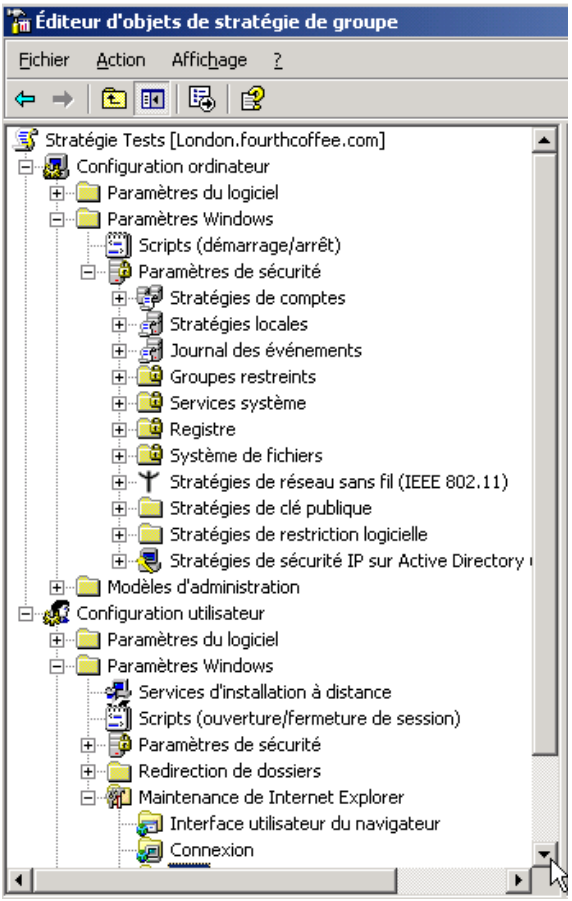
Les Stratégies de Groupes

Les stratégies de groupes, aussi appelées GPO, sont des outils de configuration de l'ordinateur ou de l'environnement utilisateur membres d'un domaine Active Directory.

Selon nos besoins, nous pouvons les affecter à un ensemble d'ordinateurs ou à un ensemble d'utilisateurs. Par exemple, il sera possible de dire "Je veux que tous ces ordinateurs aient tel programme installé" ou bien "Je veux que tous ces utilisateurs trouvent tel programme installé quel que soit l'ordinateur dont ils se servent".

En règle générale, la nature des paramètres applicables est différente selon que l'on s'adresse à un ordinateur ou à un utilisateur mais ce n'est pas toujours le cas, le déploiement de logiciels en est un exemple.

Que peuvent faire les stratégies de groupes?



Les stratégies de groupes peuvent entre autres (O veut dire paramètre ordinateur et U utilisateur) :

- Déployer, mettre à jour, désinstaller du logiciel (O, U).
- Imposer un script de démarrage ou d'arrêt aux machines ou bien d'ouverture ou de fermeture de session aux utilisateurs (O ou U).
- Imposer des stratégies de comptes : mots de passe (longueur, complexité, durée de vie), modalités de verrouillage de comptes, etc (O).

NB	Les stratégies de comptes doivent être attachées à l'objet domaine impérativement sinon, elles n'affectent que la base locale des machines. C'est un cas particulier.

- Paramétrer les droits spéciaux des utilisateurs, les options de sécurité (O).
- Paramétrer l'audit et les journaux Windows (O).
- Contrôler les services (O).
- Paramétrer le firewall (sous Vista et +) (O)
- Imposer des membres à des groupes locaux, cela s'appelle "Groupes restreints" (O).
- Imposer des permissions sur des fichiers (généralement système) et des entrées de registre (O).
- Interdire le lancement de certains programmes ou donner une liste exhaustive des programmes que l'on peut lancer, ce sont les restrictions logicielles (O, U).
- Gérer les certificats et les fonctionnalités qui y sont liées. Par exemple, gérer les agents de récupération EFS, interdire l'usage d'EFS (pour XP et +), installer des certificats d'Autorités de Certification Racine de Confiance (O, U pour cette dernière option, O pour les autres).
- Imposer du chiffrage aux réseaux Wi-Fi et créer des réseaux favoris (pour XP et +) (O).
- Faire installer son poste client à un utilisateur grâce à RIS (U).
- Rediriger le Bureau, Application Data, Mes Documents, le Menu Démarrer sur un partage réseau plutôt que de les laisser sur le poste local (U).
- Configurer Internet Explorer, par exemple imposer des Favoris (U).

De plus, que ce soit dans la partie Ordinateur ou Utilisateur, on trouve ce que Microsoft appelle les Modèles d'Administration qui permettent d'effectuer des configurations correspondant à des options dans le registre machine ou utilisateur. Il est possible de charger des modèles supplémentaires (fichiers ADM ou ADMX depuis Windows 2008) par exemple ceux de Office, pour paramétrer une fonctionnalité ou application particulière.

Nature des stratégies de groupes

Un objet de stratégie de groupe (GPO pour Group Policy Object) est représenté à la fois par des données maintenues dans la base Active Directory et par des fichiers répliqués entre contrôleurs de domaines. La représentation physique est sans importance, les outils de manipulation des GPO nous la rendent transparente.

Pour que l'objet agisse, il faut le lier (link) à un ou plusieurs conteneurs. Les conteneurs en question peuvent être des objets Site, Domaine, OU.

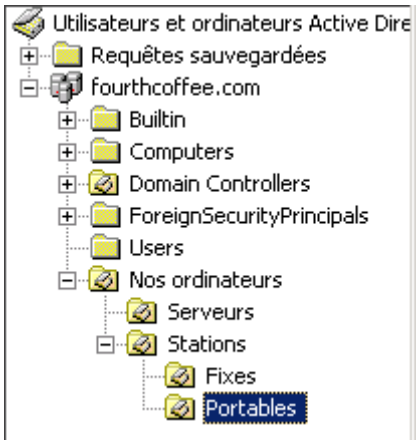
Les stratégies de groupes sont donc des objets Active Directory. Elles nécessitent donc un domaine AD et des ordinateurs Windows 2000 au minimum. En d'autres termes, les machines NT même membres d'un domaine AD ne subissent pas les stratégies de groupes et leurs utilisateurs non plus.

Il faut comprendre que l'essentiel du traitement de la GPO est fait par le client et non le contrôleur de domaine. C'est pourquoi une machine Windows 2000 va ignorer les paramètres ou fonctionnalités apparus dans XP.

Toujours dans le même ordre d'idées, si l'on a un parc mixte 2000, XP, Vista, c'est sur une station Vista qu'il faudra utiliser le programme de manipulation des stratégies (GPMC) afin de voir tous les paramètres de tous les OS. Si l'on créait la GPO depuis une machine 2000, l'on ne pourrait accéder qu'aux paramètres que connaissait Windows 2000.

Chronologie d'application des stratégies de groupes

Le principe de base est qu'un objet de GPO lié à un certain conteneur va agir sur les ordinateurs ou les utilisateurs présents dans ce conteneur et dans tous les conteneurs enfants. Par exemple :



Dans le domaine, une OU Stations contient deux OU filles Fixes et Portables. Si une GPO est attachée à Stations, elle va agir sur les ordinateurs dont le compte sera placé dans Stations mais aussi sur ceux dont le compte est placé dans Fixes ou Portables. Microsoft parle d'héritage ou de cascade de stratégies de groupes. De même si l'on attache une GPO à l'objet domaine (fourthcoffee.com), tous les objets du domaine vont la subir, quel que soit le conteneur dans lequel ils se trouvent.

NB	Il n'y a pas héritage des stratégies de groupes entre domaines d'une forêt. Bien que l'on puisse attacher à un conteneur une GPO créée dans un autre domaine, c'est bien le fait d'avoir lié la GPO à un conteneur du domaine courant qui lui permettra d'agir. Cette pratique n'est de toute façon pas recommandée et peu fiable, il vaut mieux importer la GPO dans le domaine.

On peut cependant modifier dans une certaine mesure ce comportement avec deux options. La première est le Blocage d'héritage qui est une propriété d'un conteneur et la seconde consiste à "forcer" un lien entre une GPO et un conteneur (assez bizarrement, Microsoft a traduit Force par Appliquer dans les versions françaises, ce qui n'a pas beaucoup de sens.). Nous reviendrons sur le fonctionnement de ces options.

Résolution des conflits

Les GPO sont appliquées dans un ordre précis.

1. Stratégie locale. La stratégie locale n'est pas à proprement parler une GPO, ce sont les paramètres, essentiellement de sécurité, qu'un ordinateur, même autonome, va s'appliquer à partir du registre. On y accède avec l'outil GPEDIT.MSC mais en se connectant – lorsqu'il pose la question - à la base locale et non au domaine.
2. Site
3. Domaine
4..x OU

Pourquoi plusieurs fois OU ? Parce que si un compte ordinateur ou utilisateur se trouve dans une OU fille, dans notre exemple Portables, Windows va d'abord appliquer la/les GPO de Nos ordinateurs puis celle/celles de Stations et en fin celle/celles de Portable. On va donc du plus général au plus particulier.

Dans le cas où plusieurs GPO sont attachées au même conteneur, il faut déterminer explicitement leur ordre d'application en les ordonnant. Mais attention, la colonne Ordre des liens indique un poids et non un ordre. Ainsi c'est la GPO qui a la plus *petite* valeur dans l'ordre qui va l'emporter ! On peut mieux se rendre compte de la précédence en utilisant l'onglet Héritage du GPMC.

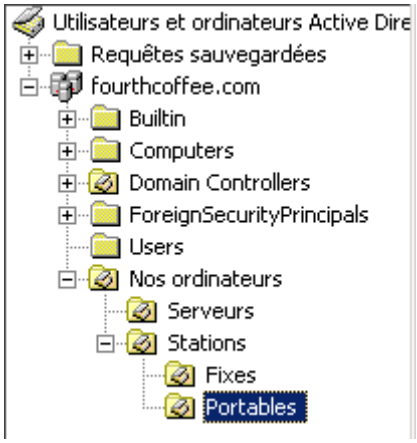
Donc Windows va chercher les GPO assignées et les applique tour à tour. Les principes suivants sont mis en œuvre :

- Si un paramètre défini par une GPO n'est pas contredit ensuite, il est appliqué.

- En revanche, en cas de contradiction, le *dernier paramètre appliqué l'emporte*.

NB	Certains paramètres ne sont pas de nature à en contredire d'autres. Par exemple, si une GPO dit "J'installe Word" et qu'un autre dit "J'installe Excel", bien que le même paramètre dise des choses différentes dans deux GPO, cela n'est pas une contradiction, les deux applications seront installées.

Par exemple, supposons que l'on attache une GPO à chacun des conteneurs Nos ordinateurs, Stations et Portables.



Nous manipulons deux paramètres : "Empêcher les utilisateurs d'installer des pilotes d'imprimante" et "Autoriser l'accès au CD-ROM uniquement aux utilisateurs ayant ouvert une session locale".

Premier cas de figure, un certain paramètre est affecté et n'est pas contredit :

	Empêcher installation pilote	**Autoriser CD-ROM en local seulement**
Nos ordinateurs		
Stations	Activé	
Portables		
Résultat	**Activé**	

Deuxième cas de figure, un certain paramètre est appliqué par une GPO et un autre paramètre l'est par une autre GPO.

	Empêcher installation pilote	**Autoriser CD-ROM en local seulement**
Nos ordinateurs		Activé
Stations	Activé	
Portables		
Résultat	**Activé**	**Activé**

Il n'y a pas contradiction, les deux paramètres s'appliquent.

Troisième cas de figure, un paramètre est contredit :

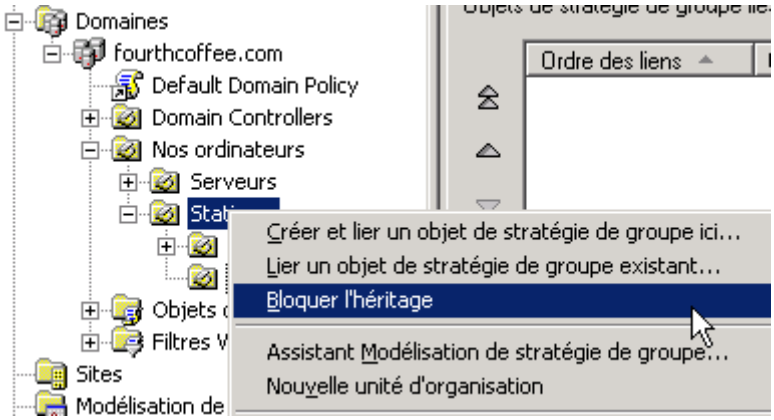
	Empêcher installation pilote	**Autoriser CD-ROM en local seulement**
Nos ordinateurs		
Stations	Activé	Activé
Portables	Désactivé	
Résultat	**Désactivé**	**Activé**

La dernière GPO ayant parlé a raison. Cela n'empêche pas l'autre paramètre qui n'a pas été contredit de s'appliquer. *Les conflits sont évalués paramètre par paramètre*.

Nous avons vu que deux options permettaient d'intervenir sur le déroulement normal de l'héritage.

Bloquer l'héritage

La première est donc une propriété d'un conteneur, elle se nomme bloquer l'héritage.



L'effet est simple. Les GPO attachées aux conteneurs "supérieurs" sont ignorées.

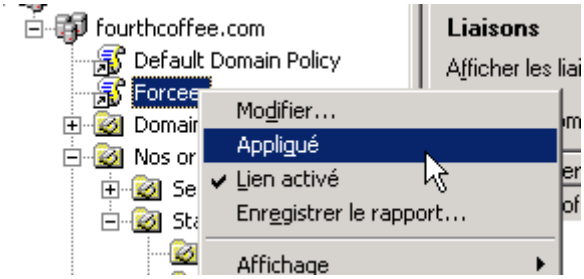
Par exemple, si nous bloquons l'héritage au niveau de l'OU Stations

	Empêcher installation pilote	**Autoriser CD-ROM en local seulement**
Nos ordinateurs		Activé
Stations		
Portables	Désactivé	
Résultat	**Désactivé**	

La GPO attachée à Nos ordinateurs n'est plus prise en compte. En revanche, évidemment, les GPO attachées à Stations ou aux OU contenues sont traitées normalement.

Force, Appliqué ou Ne pas outrepasser

Il se pourrait qu'un administrateur veuille qu'une règle soit absolument appliquée sur l'ensemble de son domaine ou autre conteneur et ne puisse être contredite. Une propriété du lien entre une GPO et un conteneur se nomme "Appliqué" dans la version française de 2003, "Ne pas outrepasser" dans 2000 et Force dans les versions américaines de 2003, ce qui nous paraît plus sensé.

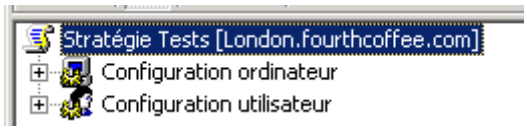


Si cette option est activée, alors

1. Les paramètres que contient la GPO ne peuvent pas être contredits par les GPO attachées aux conteneurs enfants.
2. La GPO est appliquée sans tenir compte de l'option Bloquer l'héritage des conteneurs enfants.

Objets subissant les stratégies

Une GPO comporte deux parties bien distinctes : une partie Ordinateur et une partie Utilisateur.



Imaginons la structure suivante :

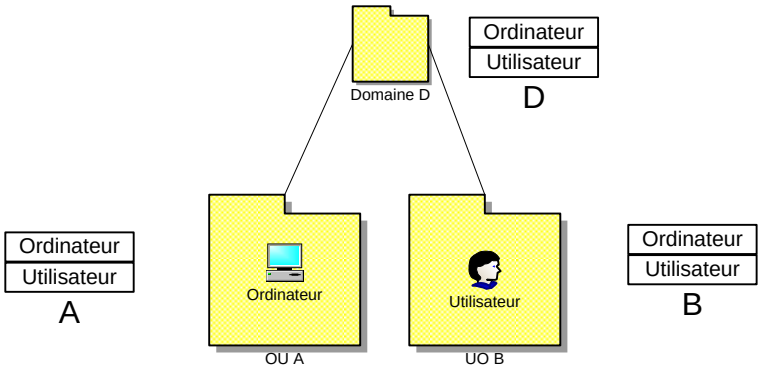


Figure 1

Un utilisateur dont le compte est dans l'OU B va allumer un ordinateur dont le compte est dans l'OU A et s'en servir. Quelles stratégies vont-elles être appliquées sachant qu'il y a une GPO (D, A, B) attachée à chaque conteneur et que dans une GPO il y a deux parties, Ordinateur (o) ou Utilisateur (u) ?

A moment du boot, l'ordinateur va s'appliquer les parties Ordinateur des GPO qui le concernent puis au moment du logon, l'ordinateur va aller chercher les parties Utilisateur des GPO qui concernent l'utilisateur. En d'autres termes :

Boot	Logon
Do + Ao	Du + Bu

Il est donc totalement inutile de définir des paramètres dans la partie Ordinateur d'une GPO attachée à un conteneur ne recevant que des utilisateurs, ils ne seront jamais lus.

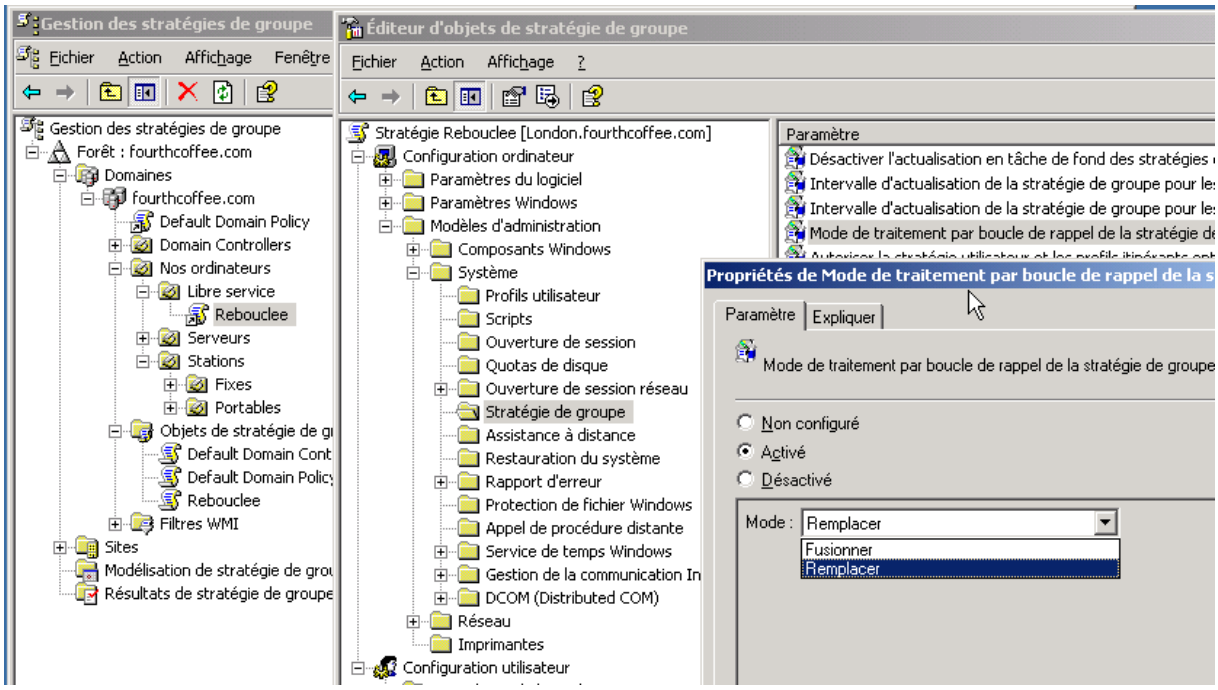
En revanche, l'inverse n'est pas toujours vrai.

Loopback, Rebouclage

On peut imaginer des circonstances dans lesquelles l'usage d'un certain ordinateur l'emporte sur qui s'en sert.

Par exemple : En règle générale dans une entreprise, les utilisateurs ont le droit de se servir du Panneau de Configuration. Mais il y a trois PC en libre service permettant d'accéder à l'Internet et sur lesquels il ne faudrait pas que les utilisateurs puissent modifier la configuration. Il serait donc souhaitable que sur ces trois PC, l'usage du Panneau de Configuration soit interdit. Or la désactivation du Panneau de Configuration est un paramètre de la partie Utilisateur d'une GPO. Il ne faut pas s'en servir dans une GPO attachée à une OU contenant les utilisateurs car cela leur interdirait le Panneau de Configuration sur toutes les machines. C'est là qu'intervient le rebouclage (Loopback).

Dans une GPO subie par un ordinateur, et donc dans la partie ordinateur (Configuration ordinateur / Modèles d'administration / Système / Stratégie de groupe), il est possible d'indiquer que cette GPO doit être "rebouclée" c'est-à-dire appliquée pour sa partie Utilisateur quand se produira le logon.



Il s'agit d'un paramètre de la partie Ordinateur de la stratégie car il faut bien que l'ordinateur le lise.

Si nous activons ce paramètre, deux options sont offertes, Fusionner ou Remplacer.

Voici leur fonctionnement si l'on suppose que, dans la Figure 1 page 6, la GPO A voit l'option de rebouclage activée.

Rebouclage	Boot	Logon
Sans	Do + Ao	Du + Bu
Fusionner	Do + Ao	Du + Bu + Au
Remplacer	Do + Ao	Au

Dans le mode Fusionner, la partie Utilisateur de la GPO subie par l'ordinateur est appliquée après ce que l'utilisateur subit normalement. Dans le mode remplacer, elle est appliquée à la place de ce que l'utilisateur subit normalement.

C'est donc bien l'emploi d'un certain ordinateur qui va imposer des paramètres utilisateur. Bien que d'usage peu fréquent ,ce dispositif permet de régler les problèmes particuliers que présentent les ordinateurs portables, en libre service ou dédiés à une application par exemple.

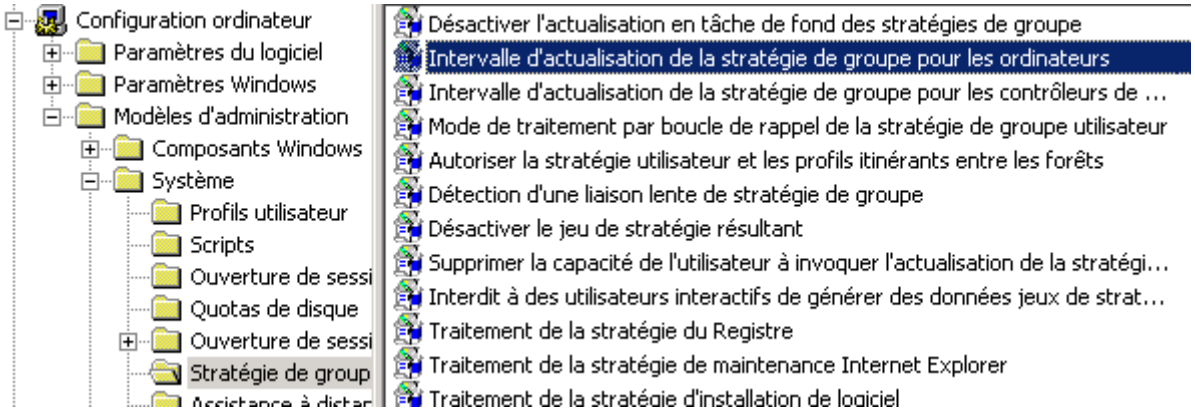
Application et Rafraichissement

Les GPO sont appliquées au boot pour la partie ordinateur et au logon pour la partie utilisateur.

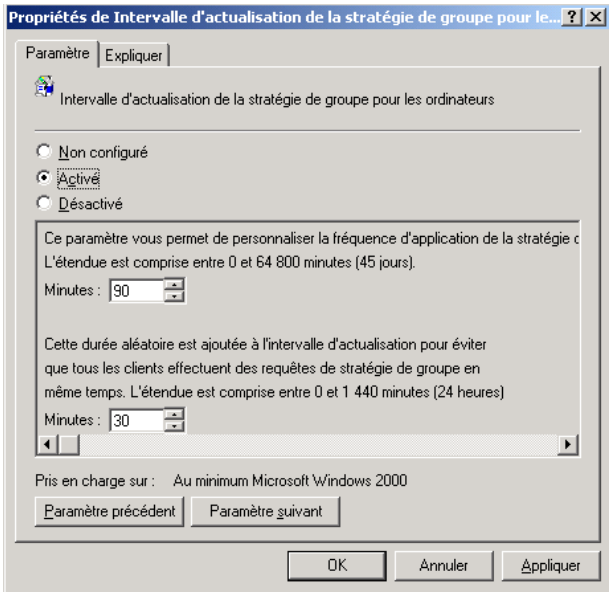
NB	Le traitement des stratégies est différent sur XP qui applique un procédé appelé Fast Logon ou Fast Boot (qui a été supprimé dans Vista). L'idée est de donner la main à l'utilisateur le plus vite possible. Donc XP ne va pas chercher les GPO quand il boot ni quand l'utilisateur se log s'il le fait immédiatement mais il ne le fera qu'à temps perdu (en général dans le 5 ou 10 minutes après le boot). Donc il applique les stratégies qu'il avait mises en cache avant le précédent shutdown. Si elles ont changé entretemps, l'ordinateur n'applique pas les changements, il rafraichira plus tard. Mais si des paramètres de la GPO ne sont pas rafraichissables, par exemple une installation de logiciel, alors il faudra rebooter la machine si c'est l'ordinateur qui subit la GPO ou rouvrir sa session si c'est l'utilisateur.

Les GPO sont ensuite rafraichies à un intervalle configurable aussi bien pour les ordinateurs membres ainsi que pour les contrôleurs de domaine par le paramètre "Intervalle d'actualisation…" dans la

rubrique Configuration ordinateur / Modèles d'administration / Système / Stratégie de groupe de la GPO elle-même.



Les paramètres en question permettent de configurer l'intervalle de rafraichissement et un délai aléatoire qui vient s'y ajouter Les valeurs par défaut sont respectivement de 90 et 30 minutes.



Paramètres non rafraichis

Certains paramètres ne sont pas rafraichis : les installations de logiciels, les redirections de répertoires, les configurations de profils itinérants (roaming profiles). Ils nécessitent donc une nouvelle ouverture de session quand ils se trouvent dans la partie Utilisateur de la GPO ou un nouveau reboot s'ils sont dans la partie Ordinateur (cas des installations de logiciels).

Rafraichissement forcé

Il est possible de forcer immédiatement le rafraichissement par les commandes suivantes :

Sous Windows 2000 : SECEDIT /REFRESHPOLICY suivi de soit MACHINE_POLICY soit USER_POLICY.

Après Windows 2000 : GPUDATE avec optionnellement /target:computer ou /target:user.

Assez curieusement, les documentations Microsoft ainsi que l'aide intégrée aux commandes sont fausses.

Cas particuliers

Liés au procédé de rafraichissement

Le principe de rafraichissement des stratégies est le suivant. Après le boot ou le logon, le moment venu, l'ordinateur va rechercher la liste des GPO à s'appliquer. Chaque GPO est dotée d'un numéro de version. Si de nouvelles GPO ont été définies ou si des numéros de versions ont changé, les GPO concernées sont appliquées.

Dans un cas de figure cela peut quand même laisser un ordinateur fonctionner avec des paramètres non conforme aux stratégies. Imaginons qu'après le boot, un utilisateur ait modifié dans le Registre une valeur normalement affectée par une GPO. Au moment du rafraichissement, comme la GPO qui définissait cette valeur n'a pas changé, l'ordinateur ne la réapplique pas.

C'est pour cela que Microsoft a prévu une options /force dans les commandes de rafraichissement. Elle va réappliquer toutes les GPO même si elles n'ont pas changé. On peut définir ce même comportement pour le rafraichissement automatique dans la rubrique "Configuration ordinateur / Modèles d'administration / Système / Stratégie de groupe" de la GPO elle-même.

Liés à Windows NT

Rappelons que Windows NT ne connaît pas la notion de Stratégies de Groupes. Donc, si l'on se sert d'une station NT, l'on ne subit pas du tout les Stratégies de Groupes (mais on subit bien les stratégies systèmes définies dans un NTCONFIG.POL).

En revanche, que se passe-t-il si l'on se sert d'une machine Windows 2000 ou au-delà et que le compte de la machine ou celui de l'utilisateur appartient à un domaine Active Directory alors que l'autre appartient à un domaine NT ?

Premier cas de figure : Le compte d'ordinateur est dans un domaine NT, le compte d'utilisateur dans un domaine AD. Lorsque l'utilisateur se connecte, l'ordinateur applique la partie Ordinateur (pas Utilisateur) de la Stratégie Système (ntconfig.pol) qu'il télécharge depuis le contrôleur de domaine. Puis il applique la partie Utilisateur (pas Ordinateur) des Stratégies de Groupes.

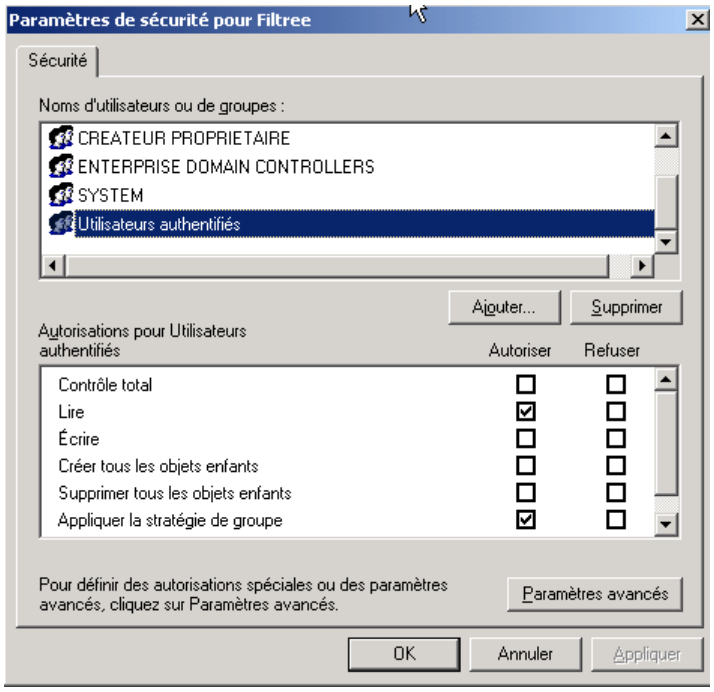
Deuxième cas de figure : Le compte d'ordinateur est dans un domaine AD et le compte d'utilisateur dans un domaine NT. Lorsque l'ordinateur boot, il s'applique la partie Ordinateur des Stratégies de Groupe et quand l'utilisateur se connecte, l'ordinateur lui applique la partie Utilisateur de la Stratégie Système.

Filtrage

Le filtrage est utile quand nous devons attacher une GPO à un conteneur dans lequel se trouvent à la fois des comptes (utilisateurs ou ordinateurs) qui devraient subir la GPO et d'autres qui ne le devraient pas.

Par groupe de sécurité

Le principe est simple. Les GPO sont dotées d'une ACL. Pour qu'un compte d'ordinateur ou d'utilisateur se voit appliquer une GPO, il faut qu'il ait à la fois le droit de lire la GPO et le droit de se l'appliquer.



L'ACL par défaut d'une GPO prévoit globalement que les Administrateurs ont tous les droits dessus et que le groupe spécial Utilisateurs authentifiés a le droit "Lire et Appliquer la stratégie de groupe".

Étant donné que tout compte d'utilisateur ou d'ordinateur appartient au groupe Utilisateurs authentifiés, il subira la GPO.

Si l'on veut restreindre l'application de la GPO à un sous ensemble d'utilisateurs ou d'ordinateurs, il suffit de :

1. Créer un groupe
2. Y placer les comptes concernés
3. Supprimer Utilisateurs authentifiés de l'ACL de la GPO
4. Ajouter dans l'ACL de la GPO le groupe en question avec les permissions "Lire et Appliquer la stratégie de groupe".

NB	Il est, la plupart du temps, prudent de refuser l'application des GPO sur les administrateurs, en particulier si la GPO impose des restrictions.. Il suffit pour cela de cocher l'option "Refuser" de la permission "Appliquer la stratégie" des groupes administrateurs.

Par filtre WMI

Les filtres WMI, apparus avec XP, permettent d'écrire des requêtes WMI qui détermineront si une machine s'applique ou pas la GPO.

Le traitement du filtre WMI étant fait au niveau du client et non du contrôleur de domaine, les machines Windows 2000 ne le prennent pas en compte. En d'autres termes, si une OU contient à la fois des ordinateurs XP, 2003 et 2000 et qu'on lui attache une GPO d'installation de logiciel mais que celle-ci restreigne l'installation aux seuls ordinateurs ayant au moins 10 Go de libre sur le disque C:, les machines 2000 vont s'installer l'application quel que soit l'espace disque.

Note	Il ne peut y avoir qu'un seul filtre WMI par GPO. Par conséquent, si l'on veut appliquer une GPO à des machines répondant à des cas différents de filtres WMI, il faut faire deux GPO identiques mais auxquelles on attache des filtres WMI différents.