Table of Contents

1.1. Histoire des stratégies de groupe (GPO) dans Windows

* GPO signifie Group Policy Object soit stratégie de groupe.
* Les GPO sont apparues avec Windows 2000 Server et AD 2000.
* Les concepts abordés dans ce cours s'appliquent à toutes les versions d'Active Directory.
* Les GPO remplacent les stratégies de sécurité que l'on trouvait dans Windows NT4.
* Elles ont été considérablement enrichies depuis en terme de paramètres configurables et d'ergonomie des outils de gestion, d'édition et de maintenance.

1.2. Avantages des stratégies de groupe (GPO)

* Les GPO permettent la configuration automatisée et centralisée des postes de travail et des serveurs Windows de votre environnement.
* Les GPO et leurs paramètres étant stockés dans AD et le dossier SYSVOL, la configuration des postes n'est plus stockée localement. Il suffit d'appliquer une GPO existante à un nouveau poste, et la configuration s'applique.
* Les configurations étant appliquées à des clés de registre particulières (clés « policies »), la suppression d'une GPO restaure les paramètres locaux appliqués avant les GPO.
* Il est en théorie possible de configurer n'importe quel paramètre par GPO.
* La configuration des postes est uniforme. De plus les GPO sont réappliquées à intervalle régulier.

1.3. Limites des stratégies de groupe (GPO)

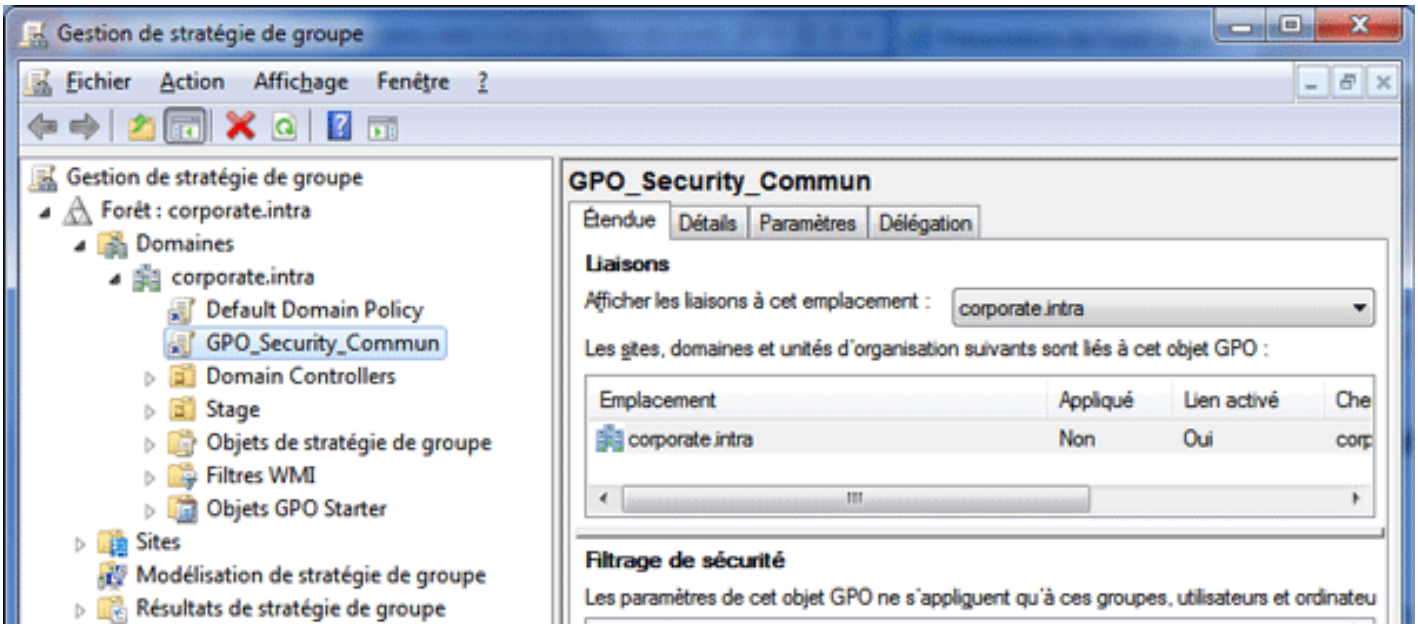
* La gestion des GPO n'est pas chose aisée. Il faut être sûr d'appliquer la ou les bonnes GPO aux bons ordinateurs et/ou utilisateurs. Beaucoup d'administrateurs sont confrontés à ce problème lorsqu'ils mettent en œuvre les GPO.
* La suite de ce cours explique les règles d'applications des GPO qui vous donneront tous les éléments à connaître afin de maîtriser la gestion (et donc l'application) des GPO.
* Un autre inconvénient des GPO est que si dans votre environnement, chaque poste ou chaque utilisateur nécessite une configuration particulière, les GPO ne sont plus réellement efficaces.

2.1. Définition des stratégies de groupe (GPO)

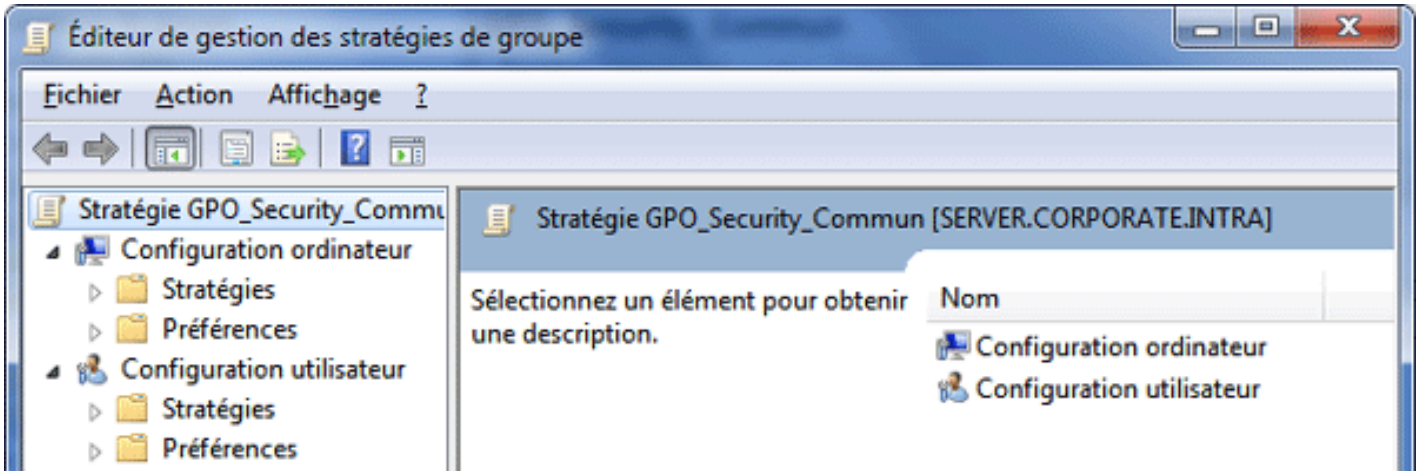
* GPO signifie Group Policy Object.
* Une GPO est un objet Active Directory, au même titre qu'un utilisateur, un ordinateur, ou une unité d'organisation.
* Une GPO contient un ensemble de paramètres applicables à un utilisateur ou un ordinateur. Par exemple la désactivation du pare-feu ou la configuration d'Internet Explorer.
* Les méta-informations des GPO sont stockées et répliquées via Active Directory. Les méta-informations sont entre autre le créateur de la GPO, les dates et heures des modifications, les autorisations NTFS, etc…
* Les GPO elles-mêmes (qui ne sont que des dossiers et des fichiers), sont stockées et répliquées dans le dossier SYSVOL. Ces fichiers sont des fichiers .pol appliquant les modèles d'administration, ainsi que les fichiers de script, etc…
* Pour rappel, le dossier SYSVOL est un dossier partagé entre les contrôleurs de domaine et avec les clients du domaine qui permet la réplication des fichiers nécessaires à Active Directory. Active Directory est un annuaire et ne peut pas stocker des fichiers et dossiers. Il se sert donc du dossier SYSVOL pour échanger les fichiers ne pouvant pas être stockés dans Active Directoy.

2.2. Présentation de l'outil de gestion des stratégies de groupe (GPMC)

* GPMC signifie Group Policy Management Console, soit console de gestion des stratégies de groupe.
* GPMC est apparue comme un téléchargement facultatif avec Windows 2003 Server. Cet outil est dorénavant un outil d'administration intégré à Windows Server 2008, 2008R2 et 2012.
* GPMC permet de gérer tout ce qui concerne la gestion des GPO : Héritage, Blocage de l'héritage, Forcer les GPO, Filtrer les GPO, Délégation de l'administration des GPO, etc…
* En aucun cas cette console ne vous permet de modifier les paramètres qui seront appliqués par votre GPO, ni de gérer les OU ou les objets Active Directory.



* GPME signifie Group Policy Management Editor, soit éditeur de gestion des stratégies de groupe.
* GPME est l'outil qui permet de modifier le contenu des GPO, c'est-à-dire les paramètres qui seront appliqués aux postes cibles.
* Cette console se lance depuis GPMC.


Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie GPO_Security_Commu
Configuration ordinateur
Stratégies
Préférences
Configuration utilisateur
Stratégies
Préférences
Stratégie GPO_Security_Commun [SERVER.CORPORATE.INTRA]
Sélectionnez un élément pour obtenir une description.
Nom
Configuration ordinateur
Configuration utilisateur

3.1. Liaisons des stratégies de groupe (GPO)

* Les GPO sont liées à des objets Active Directory. Cette liaison détermine à quels utilisateurs ou ordinateurs les paramètres seront appliqués.
* Les seuls objets auxquels vous pouvez lier une GPO sont des Domaines, des Sites et des Unités d'organisation (OU).
* Cela signifie que pour appliquer les paramètres de GPO à des utilisateurs ou des ordinateurs particuliers, il faudra lier la GPO à l'OU, au domaine ou au site Active Directory contenant ces ordinateurs et utilisateurs.
* Il est impératif que l'OU, le domaine ou le site Active Directory auquel vous liez la GPO contienne des utilisateurs ou des ordinateurs pour que la GPO soit effective.
* La liaison qui lie une GPO à un site Active Directory, un domaine ou une OU est aussi un objet AD et permet donc l'application d'ACL. Cela signifie qu'il est possible de lier une même GPO à plusieurs objets Active Directory.
* On distinguera donc la liaison de l'application.

3.2. Application des stratégies de groupe (GPO)

* Une chose très importante à noter : Les GPO ne s'appliquent pas aux groupes Active Directory. En effet, si vous liez une GPO à une OU ne contenant que des groupes, aucun paramètre ne sera appliqué sur les clients.
* Les seuls objets Active Directory pouvant appliquer les paramètres de GPO sont les objets utilisateurs et ordinateurs contenus dans le site Active Directory, le domaine, ou l'OU auquel la GPO est liée.
* Les GPO étant elles-mêmes des objets AD, il est possible d'y appliquer des ACL.

3.3. Structure des stratégies de groupe (GPO)

* Une GPO contient toujours des paramètres de configuration ordinateur et des paramètres de configuration utilisateur.
* Les paramètres de configuration utilisateur ne s'appliquent qu'à des objets utilisateurs contenus dans l'OU à laquelle est liée la GPO.
* Les paramètres de configuration ordinateur ne s'appliquent qu'à des objets ordinateurs contenus dans l'OU à laquelle est liée la GPO.
* Par exemple, si vous créez une OU contenant des objets ordinateurs, que vous liez une GPO ne contenant que des paramètres utilisateurs à cette OU, alors il ne se passe rien.

3.4. All or nothing dans les stratégies de groupe (GPO)

* Une GPO fonctionne en mode All or Nothing, c'est-à-dire que vous ne pouvez pas filtrer un paramètre de la GPO pour qu'il ne s'applique pas sur un poste en particulier. Vous ne pouvez que filtrer la GPO entière.
* Il est uniquement possible de filtrer les paramètres de préférence.
* Il sera donc nécessaire de bien réfléchir au nombre de GPO à créer, et par là même au nombre et l'organisation de la structure d'OU.

3.5. Ordre d'application des stratégies de groupe (GPO)

* Lorsqu'un ordinateur démarre, ou qu'un utilisateur ouvre une session, les paramètres correspondant

(Configuration ordinateur et utilisateur) sont appliqués dans l'ordre suivant :

1. Stratégie locale (cf. gpedit.msc).
2. GPO au niveau du site.
3. GPO au niveau du domaine.
4. GPO au niveau de l'OU.
5. GPO au niveau des sous-OU.

* Si aucun conflit n'est détecté, tous les paramètres de GPO s'appliquent aux objets utilisateurs et ordinateurs contenus dans le site, le domaine et les OU.
* S'il y a un conflit, c'est le paramètre (et uniquement le paramètre en conflit) de la dernière GPO appliquée (soit la plus proche de l'utilisateur ou de l'ordinateur) qui s'applique.

3.6. Héritage des stratégies de groupe (GPO)

* Par définition, une GPO est liée à des Sites, des domaines, ou des OU.
* Tous les objets utilisateurs et ordinateurs contenus dans les sous-OU héritent des GPO liées à des objets de niveau supérieur dans la hiérarchie Active Directory.
* Cela signifie qu'un objet stocké dans une sous-OU peut hériter de plusieurs GPO.
* Si aucun conflit n'est détecté dans les différentes GPO, tous les paramètres de toutes les GPO s'appliquent.
* S'il y a un conflit, c'est le paramètre en conflit de la dernière GPO appliquée qui s'applique.

3.7. Bloquer l'héritage des stratégies de groupe (GPO)

* Si vous ne souhaitez pas que vos ordinateurs et utilisateurs d'une OU donnée appliquent les GPO héritées, vous pouvez bloquer l'héritage des GPO.
* Les GPO liées à des OU, Domaines, et Sites supérieurs ne seront plus appliquées.
* Cependant, on ne peut pas bloquer une GPO forcée.

3.8. Forcer les stratégies de groupe (Option Appliqué)

* Si un administrateur veut imposer une GPO au niveau du Domaine par exemple sans qu'un administrateur délégué puisse aller à l'encontre des paramètres (c'est-à-dire de configurer des paramètres entrant en conflit, ou de bloquer l'héritage), l'administrateur peut forcer l'application de sa GPO.
* Aucune GPO ne pourra aller à l'encontre de la GPO forcée.
* Si deux GPO sont forcées à des niveaux différents de l'arborescence d'unités d'organisation, alors l'ordre d'application est inversé, et c'est la GPO la plus en haut de l'arborescence qui est appliquée.
* Attention, dans la version française de GPMC, cette option a été traduite « Appliqué ». C'est une erreur, et pensez bien à n'utiliser cette option que si vous souhaitez forcer la GPO.

3.9. Filtrage NTFS des stratégies de groupe (GPO)

* La GPO étant un objet AD, il est possible d'y appliquer des ACL.
* Les autorisations « lire » et « appliquer la stratégie de groupe » permettent de filtrer les GPO au niveau NTFS.
* Si dans une OU donnée, vous ne souhaitez pas appliquer les GPO à un certain nombre de machines ou utilisateurs, sans pour cela créer de nouvelles OU, vous pouvez refuser l'application de la GPO à ce groupe, ou autoriser l'application de la GPO uniquement pour un groupe.

* Par défaut, le groupe utilisateurs authentifiés est autorisé à appliquer toutes les GPO.
* Afin de déterminer quels utilisateurs ou ordinateurs appliquent les GPO, Active Directory vérifie les autorisations d'accès à la GPO, mais uniquement pour les utilisateurs stockés dans l'unité d'organisation.
* On parle de filtrage NTFS des GPO. Le groupe ne doit pas être obligatoirement stocké dans la même unité d'organisation.
* Par exemple, dans une unité d'organisation donnée, il existe tous les utilisateurs du domaine. Vous n'avez pas l'autorisation de créer de nouvelles unités d'organisation. On vous demande d'appliquer une GPO uniquement aux comptables. Théoriquement, la GPO s'appliquera à tous les utilisateurs de l'unité d'organisation. La solution consiste à simplement autoriser uniquement le groupe des comptables à lire et appliquer la GPO.
* Attention, mélanger le filtrage par OU et NTFS peut rendre la tâche ardue.
* Les ACL permettent aussi de déléguer la gestion des GPO, par exemple pour permettre à un utilisateur de modifier une GPO sans pour cela récupérer les droits administrateur.

3.10. Filtrage WMI des stratégies de groupe (GPO)

* Les GPO peuvent aussi appliquer des scripts WMI à des fins de filtrage.
* WMI signifie Windows Management Instrumentation, et est un système utilisant un langage de requête très proche de SQL (il s’appelle WQL) afin de récupérer toutes les informations matérielles et logicielles d’un système local ou distant.
* Cela vous permet de créer des conditions d’application des GPO comme par exemple analyser l’espace libre restant, le type de processeurs, ou le débit réseau.
* Un seul script WMI peut être appliqué par GPO, mais un même script peut contenir plusieurs conditions (requêtes).

3.11. Actualisation des stratégies de groupe (GPO)

{jcomments on}Les GPO sont actualisées sur les postes clients dans les cas suivants :

* Au démarrage de l’ordinateur pour la configuration ordinateur.
* A l’ouverture de session pour la configuration utilisateur.
* Toutes les 5 minutes sur un contrôleur de domaine (valeur par défaut mais modifiable).
* Toutes les 90 minutes sur un poste non contrôleur de domaine (valeur par défaut mais modifiable).
* Lorsque la commande GPUPDATE est exécutée (l’équivalent est SECEDIT /REFRESHPOLICY sur les versions de Windows antérieures à Windows XP et 2003). Cette commande demande au contrôleur de domaine les modifications apportées aux GPO depuis la dernière actualisation.
* La commande GPUPDATE /FORCE force le téléchargement intégral des GPO même si les paramètres sont déjà appliqués. De plus cette commande informera l’utilisateur ou l’administrateur qu’un redémarrage ou qu’une fermeture de session est nécessaire pour que les GPO soient appliquées dans leur totalité.
* Certains paramètres nécessite un redémarrage ou une ouverture de session pour s’appliquer. C’est le cas par exemple pour les scripts et l’installation de logiciels.
* Dans tous les cas, la meilleure façon de s’assurer que les GPO sont bien appliquées est de redémarrer l’ordinateur client.

3.12. Temps de latence de l'application des GPO

* Il est important de noter que le temps de latence de l'application des GPO varie considérablement d'un environnement à un autre.
* Le temps de latence des GPO représente le temps existant entre la création de la GPO et la disponibilité de cette GPO pour les ordinateurs ciblés. Par exemple, je crée une GPO à 12h, je lance un GPUPDATE sur un poste client, et rien ne se passe (étant sûr de la bonne configuration de ma GPO).
* Lorsque l'on crée une GPO, celle-ci est stockée dans Active Directory pour les métadonnées, et dans le

dossier SYSVOL pour les fichiers POL, les scripts et autres fichiers de configuration. Active Directory et le dossier stockés sous forme de réplicas sur tous les contrôleurs de domaine de votre domaine. La réplication Active Directory se charge de mettre à jour Active Directory et le dossier SYSVOL sur tous les contrôleurs de domaine. Il est donc impératif :

1. Soit d'attendre la fin de la réplication Active Directory sur tous les contrôleurs de domaine (le temps de réplication d'Active Directory est dépendant de la structure de sites Active Directory : plus la structure est complexe, plus le temps de réplication est long!).
2. Soit de forcer la réplication Active Directory en lançant la commande REPADMIN /SYNCALL sur le contrôleur de domaine où a été créé la GPO.

* Pensez donc bien à être un peu patient. D'expérience, ce temps de latence peut varier de quelques secondes à un quarantaine de minutes.

3.13. Maintenance des GPO

Les outils suivants permettent la maintenance des GPO. Par maintenance, comprenez l'explication de la non application d'une GPO. Pourquoi tel utilisateur n'applique pas les bons paramètres de GPO sur le bon ordinateur.

* GPOTool : Cet outil en ligne de commande permet de valider la bonne cohérence de la structure de la GPO. GPOTool vérifie le stockage de méta-informations des GPO dans AD et la bonne structure des fichiers dans SYSVOL.
* GPResult est une commande permettant de visualiser sur les postes clients les GPO qui lui sont appliquées, ainsi qu'un visuel des paramètres appliqués. L'option /H, permet l'affichage du rapport au format HTML. Cet outil permet de diagnostiquer quels paramètres sont appliqués et par quelle GPO.
* Résultats de la stratégie de groupe : Cet outil est similaire à GPResult sauf qu'il est complètement graphique et se lance depuis GPMC. Tous les rapports sont affichés au format HTML.
* Observateur d'évènements : Outil de troubleshooting courant, il vous permet de vérifier les causes de non-application sur les clients. Les sources des ID les plus courantes pour les GPO sont USERENV et SCECLI pour les problèmes relatifs aux GPO et leur application.

4.1. Configuration ordinateur et utilisateur

* Comme vu précédemment, un objet GPO contient 2 grands jeux de configuration, un pour l'utilisateur, un pour l'ordinateur.
* Pour simplifier, on peut dire que la configuration utilisateur applique des clés de registre dans HKCU, et que la configuration ordinateur applique des clés de registre dans HKLM.
* La configuration utilisateur s'applique à l'ouverture de session et « suit » l'utilisateur quelque soit l'ordinateur sur lequel il se connecte. Elle s'applique seulement si le site Active Directory, le domaine, ou l'OU auquel est liée la GPO contient des objets utilisateurs.
* La configuration ordinateur s'applique au démarrage de l'ordinateur et est valable pour tous les utilisateurs qui ouvrent une session.Elle s'applique seulement si le site Active Directory, le domaine, ou l'OU auquel est liée la GPO contient des objets ordinateurs.

4.2. Paramètres de stratégie

* Les paramètres de stratégie existent depuis Windows 2000
* Ils permettent de paramétrer des clés de registre, de configurer des paramètres de sécurité, d'installer des logiciels, de déployer des scripts et tout autre paramètres de configuration. Par exemple, vous pouvez définir des permissions NTFS sur vos postes clients depuis les GPO, désactiver des services, ou gérer les groupes locaux…
* Ces paramètres peuvent être configurés pour ne pas être modifiables par les utilisateurs et les administrateurs locaux.
* Ces paramètres sont pris en charge par Windows XP (si les paramètres lui sont applicables bien sûr).

4.3. Structure des paramètres de stratégie

Les stratégies sont divisées en 3 grandes parties :

* Installation de logiciel : permet de déployer des logiciels dans votre réseau grâce au package MSI.
* Paramètres de sécurité : permet de configurer les paramètres de sécurité des utilisateurs ou ordinateurs (permissions NTFS, droits des utilisateurs, gestion des groupes locaux, gestion des certificats, des stratégies de mot de passe, etc…).
* Modèles d'administration : on touche directement au registre. Tous les paramètres configurables par le registre peuvent être configurés par GPO.

4.4. Stratégies de préférences (GPP)

* Les stratégies de préférences existent depuis Windows 2008.
* Elles permettent de créer et de gérer des objets de types fichiers, dossiers, imprimantes locales, raccourcis, etc…
* Ces paramètres sont modifiables par les utilisateurs.
* Ces paramètres ne sont pas pris en charge par Windows XP en natif. Il faut installer le Client Side Extension, qui est un logiciel (mise à jour) gratuit téléchargeable sur le site de Microsoft.
* Petit regret : Microsoft ne propose ce logiciel qu'au format EXE et pas MSI, ce qui le rend difficile à déployer par GPO (Installation de logiciels).

4.5. Fichiers ADM et ADMX

* Les fichiers adm et admx sont les fichiers de définition des paramètres des modèles d'administration.

* Les fichiers adm sont l'ancienne génération, alors que les fichiers admx sont arrivés avec Windows Server 2008r2
* Ces fichiers sont modifiables. On peut aussi en ajouter des personnalisés ou en télécharger sur le site des éditeurs de logiciels (Office chez Microsoft par exemple).
* Cela signifie que si le paramètre que vous souhaitez configurer sur votre poste client n'existe pas nativement dans la GPO, vous pouvez le rajouter et étendre les possibilités des GPO.