Les GPO

09/04/2015

# PRÉSENTATION

## Qu’est-ce qu’un GPO ?

Les objets de stratégies de groupes (GPO) sont des objets Active Directory (AD) permettant une configuration centralisée des ordinateurs et des serveurs Windows. Les fonctionnalités des stratégies de groupe englobent tout, du verrouillage des PC jusqu'à  la configuration de la sécurité et l'installation des logiciels. Ils sont associés à  la stratégie d'un domaine, d'un site ou d'une unité organisationnelle (OU).

## Utilisation des GPO

Plusieurs GPO peuvent s'appliquer à  un objet utilisateur ou à  un objet ordinateur, selon la place qu'ils occupent dans l'espace de noms AD. Les GPO sont hérités exactement comme le sont les autres objets et propriétés du domaine. Windows 2000 les traite de la manière suivante : il commence par traiter toute stratégie d'ordinateur local existante, puis tous les GPO de sites définis, les GPO au niveau du domaine et les GPO des OU. Microsoft utilise l'acronyme LSDOU pour cet ordre de priorité (c'est-à-dire Local, Site, Domain, puis OU). Il est possible de définir plusieurs GPO à  chaque niveau de cette hiérarchie. Il est possible de cocher une case au niveau de chaque conteneur - site, domaine et OU - pour bloquer l'héritage des GPO de niveau supérieur.

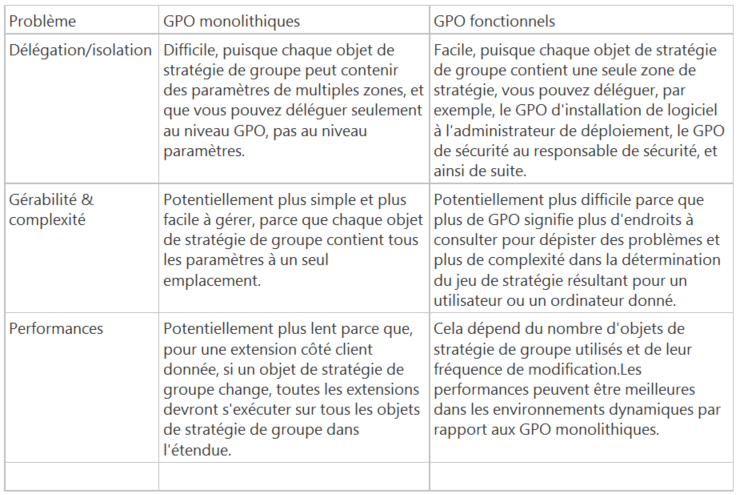
## Application des GPO

Seuls les objets utilisateur et ordinateur utilisent la stratégie de groupe. Au démarrage et à  l'arrêt, un ordinateur Windows traite les stratégies définies dans la partie Computer Configuration d'un GPO. A l'ouverture et la fermeture de session des utilisateurs, un utilisateur Windows traite les stratégies définies dans la partie User Configuration d'un GPO.

On peut également utiliser une stratégie de Modèles d'administration pour définir un rafraîchissement périodique des paramètres des GPO des utilisateurs et des ordinateurs. Celui-ci se produit, par défaut, toutes les 90 minutes.

De plus, il est possible d'appliquer de la sécurité à  des applications, avec l'élément Software Installation d'un GPO. Dans le cas où plusieurs applications sont publiez dans un GPO, dont la sécurité permet à  tous les utilisateurs authentifiés de l'utiliser. Il est possible de spécifier que seul certains groupes d'utilisateurs peuvent lire et voir ces applications.

## GPO monolithiques et GPO fonctionnels

Ils existent différentes façons d’implémenter des objets de stratégie de groupe. Les termes « monolithiques » et « fonctionnels » se réfèrent à la façon dont vous les concevez. Les objets de stratégie de groupe monolithiques contiennent des paramètres ayant de multiples origines. Par exemple, un GPO monolithique peut contenir des paramètres provenant des stratégies de modèles d'administration, de maintenance Internet Explorer et d'installation de logiciels, le tout dans un seul objet de stratégie de groupe. Par contraste, les objets de stratégie de groupe fonctionnels exécutent généralement une seule action. Par exemple, un objet de stratégie de groupe fonctionnel peut s'attacher seulement à l'installation de logiciel ou appliquer des paramètres de sécurité

## Cycle de traitement des GPO

Le traitement de la stratégie de groupe est une série complexe d'interactions impliquant de nombreuses parties de l’infrastructure Windows et Active Directory.

À un niveau élevé, le traitement de la Stratégie de groupe comprend deux parties. La première est appelée Noyau, ou traitement d'Infrastructure de Stratégie de groupe. Dans cette phase, un client de stratégie de groupe Windows interroge son contrôleur de domaine le plus proche pour déterminer la vitesse de lien au DC, où il se situe dans la hiérarchie Active Directory (c'est-à-dire de quel site, quel domaine et quelle l'unité d'organisation le client est membre), et quels objets de stratégie de groupe s'appliquent à l'ordinateur ou l'utilisateur actuellement connecté.(Il est important de noter que dans ce contexte un client peut être un serveur ou un poste de travail appartenant à un domaine Active Directory.)

Une fois la liste d'objets de stratégie de groupe créée, la phase suivante démarre : le traitement d'extension côté client (CSE, Client-Side Extension).Pendant la phase CSE, chaque CSE enregistré traite la liste d'objets de stratégie de groupe ayant des paramètres implémentés dans sa zone. Par exemple, le CSE Registre ou Modèle d'administration s'exécute systématiquement en premier et traite tous les objets de stratégie de groupe qui s'appliquent à l'ordinateur ou à l'utilisateur donné et qui ont une stratégie de registre implémentée en eux.

# OPTIMISATION

## Initialisation GPO au démarrage

1. La station de travail demande à  un serveur DNS de trouver un DC sur le site de la station de travail. Plus précisément, la station de travail demande au DNS l'enregistrement SRV. Cet enregistrement renvoie le nom du DC (dans le site) qui traite les demandes LDAP (Lightweight Directory Access Protocol) pour le domaine.
2. La station de travail établit une connexion par canal sécurisé avec le DC.
3. La station de travail envoie un ping au DC pour déterminer si la connexion réseau entre la station de travail et le DC (commutée, T1, par exemple) constitue une liaison réseau lente. (Par défaut, Windows 2000 juge lente une vitesse de transfert inférieure à  500 Kbps.)
4. La station de travail s'associe à  AD par LDAP.
5. La station de travail utilise LDAP pour interroger AD et obtenir une liste de tous les GPO reliés à  l'OU ou à  l'OU parent de la station de travail.
6. La station de travail utilise LDAP pour interroger AD et obtenir une liste de tous les GPO liés au domaine de la station de travail.
7. La station de travail utilise LDAP pour interroger AD et obtenir une liste de tous les GPO liés au site de la station de travail.
8. La station de travail utilise LDAP pour interroger le GPC (dans AD) et déterminer la voie vers le GPT de chaque GPO (dans Sysvol).
9. La station de travail lit le fichier gpt.ini qui réside dans le GPT de chaque GPO. Ce fichier liste le numéro de version actuel du GPO.
10. Les extensions côté client de la station de travail traitent les GPO qui ont été extraits.

Ces étapes ne représentent que le traitement des GPO spécifiques à  l'ordinateur, se produisant à  l'initialisation de l'ordinateur. Une fois l'utilisateur connecté au système, Win2K doit traiter les éventuels GPO spécifiques à  l'utilisateur. Pendant cette procédure, l'OS répète les étapes 4 à  10 (du point de vue du réseau, les étapes 1 à  3 ont déjà  été couvertes).

## Détection de liaison lente

L'activation de la détection de liaison lente signifie que moins d'extensions côté client travailleront au traitement des GPO et donc le temps de traitement GPO diminuera dans des conditions de liaison lente. On peut modifier la valeur liaison lente par défaut de 500 Kbps au moyen de la policy Group Policy slow link detection. (Cependant, augmenter le seuil pour forcer la détection de liaison lente n'est pas le meilleur moyen d'améliorer la performance de traitement GPO.)

## Version de GPO

Le GPC et le GPT de chaque GPO contiennent le numéro de version du GPO. Win2K augmente ce nombre chaque fois que l'on change le GPO. Les stations de travail XP et Win2K gardent un historique de chaque session de traitement GPO dans leurs registres locaux.

Par défaut, les extensions côté client ne traiteront pas un GPO si son numéro de version n'a pas changé. Quand le numéro de version d'un GPO est 0 (indiquant qu'il n'y a eu aucun paramétrage dans le GPO), les extensions côté client n'essaieront même pas de traiter le GPO. Le fait de forcer les extensions côté client à  traiter tous les GPO indépendamment du numéro de version, augmentera le temps de traitement.

## Traitement asynchrone

Par défaut, les opérations de traitement GPO de Windows sont synchrones : toutes les extensions côté client doivent finir de traiter les GPO de type machine (à  l'initialisation du système) avant que l'ordinateur ne présente le dialogue de connexion. De même, quand un utilisateur se connecte à  une unité Windows, les extensions côté client qui traitent les GPO au niveau utilisateur doivent terminer leur travail avant que l'utilisateur ne puisse prendre le contrôle du desktop et commencer à  travailler.

Si le traitement de nombreux GPO retarde sensiblement le démarrage du système ou la connexion de l'utilisateur, on peut configurer Win2K pour qu'il traite les GPO de manière asynchrone (au moyen des policies Apply Group Policy for computers asynchronously during startup et Apply Group Policy for users asynchronously during logon.)

Toutefois, un GPO qui n'a pas terminé le traitement au moment où un utilisateur se connecte, risque de ne pas entrer en action avant la prochaine connexion de l'utilisateur - un « trou » qui pourrait poser un problème pour des catégories Group Policy comme Software Installation et Folder Redirection.

(XP comporte une fonction Fast logon optimization, et donc le traitement GPO de XP est asynchrone par défaut. Par conséquent, les extensions côté client sur une unité XP pourraient bien ne pas finir de traiter tous les GPO avant qu'un système ne présente la boîte de dialogue de connexion ou ne permette à  un utilisateur d'accéder au desktop, et Software Installation et Folder Redirection demandent en principe deux connexions avant d'entrer en vigueur.)

## Paramètre de la GPO

Dans chaque GPO, on peut définir des paramètres qui s'appliquent aux ordinateurs ou aux utilisateurs. Mais il n'est pas nécessaire de définir les deux dans un GPO donné. Par conséquent, la première et la plus simple démarche pour améliorer la performance consiste à  désactiver les paramètres au niveau ordinateur ou au niveau utilisateur inutilisés d'un GPO. Ainsi, les extensions coté clients ne prendront pas la peine de chercher les paramètres non-existants, ce qui allège le cycle de traitement.

Un autre moyen de garder la maîtrise des temps de traitement GPO consiste à  instaurer un intervalle maximum pour l'exécution des scripts. Comme l'on peut appliquer des GPO multiples à  un utilisateur ou un ordinateur donné, on pourrait avoir plusieurs scripts s'exécutant l'un après l'autre. Mais des scripts défectueux ou mal programmés pourraient s'interrompre ou s'exécuter indéfiniment.

Pour atténuer ce genre de problème, on peut définir un temps maximum d'exécution de tous les scripts.

## Limiter les GPO

L'action la plus élémentaire consiste à  limiter le nombre de GPO qu'un ordinateur ou utilisateur doit traiter au démarrage ou à  la connexion (Limiter à une dizaine).Lors de la première utilisation, le temps d’attente est plus long parce que les extensions côté client doivent appliquer initialement tous les paramètres. Après le cycle de traitement initial, les redémarrages système et les connexions utilisateur qui suivront ne traiteront que les GPO qui ont changé (sauf si vous les forcez à  procéder autrement).

## Limiter les groupes de sécurité

L'utilisation des groupes de sécurité (les groupes locaux, globaux ou universels AD contenant des ordinateurs ou des utilisateurs) peut affecter le traitement GPO. On peut recourir aux groupes de sécurité pour filtrer les effets des GPO - par exemple, quand on veut n'appliquer un GPO niveau domaine qu'à  un petit nombre d'utilisateurs ou d'ordinateurs.

Mais le filtrage par les groupes de sécurité se paie en performances. En effet, plus il y a d'ACE (access control entries) associées à  un GPO, plus l'extension côté client du GPO doit travailler pour savoir si un ordinateur ou un utilisateur appartient à  l'un des groupes soumis au filtrage.

Donc, en maintenant les ACL des GPO courts et concis, on améliore (ou tout au moins on maintient) les performances. Il ne faut pas utiliser systématiquement les ACL pour filtrer les GPO de chaque ordinateur ou utilisateur.

## Limiter les liens multidomaines

Les performances sont aussi affectées par l'utilisation de GPO liés au travers de frontières de domaines. Chaque GPO appartient à  un domaine AD et le GPC et le GPT du GPO résident sur les DC de ce domaine.

Supposons que l'on ait une forêt d'AD multidomaines. On pourrait lier un GPO d'un domaine (domaine A) à  un autre domaine de la forêt (domaine B). Mais quand un ordinateur ou un utilisateur du domaine B traite le GPO qui se trouve dans le domaine A, les extensions côté client de l'ordinateur du domaine B doivent traverser les relations d'approbation dans la forêt, pour accéder au GPC et au GPT du GPO.

Une telle opération est plus coûteuse en matière de performances que le fait de communiquer avec des GPO dans le même domaine. De plus, si l'ordinateur du domaine B ne peut pas trouver un DC du domaine A dans le même site AD, il lui faudra peut-être traverser des liens WAN pour atteindre un DC et traiter le GPO.

Il vaut donc mieux éviter de lier des GPO en franchissant des frontières de domaines. Il est préférable de copier un GPO défini d'un domaine dans un autre.