# Gouvernance des GPO avec une structure de sécurité multicouche

Écrit par Alvaro Vitta, consultant principal en solutions, Quest

## Introduction

La stratégie de groupe permet de configurer et de gérer de façon centralisée les systèmes d'exploitation, applications et paramètres des utilisateurs dans un environnement Microsoft Active Directory. La stratégie de groupe contrôle en partie ce que les utilisateurs peuvent et ne peuvent pas faire sur un système informatique. Elle intègre un système avec mots de passe complexes qui empêche les utilisateurs de choisir un mot de passe trop simple, connecte ou non au partage réseau les utilisateurs non identifiés à partir d'ordinateurs distants, et restreint l'accès à certains dossiers. Chaque ensemble de configurations de ce type est un « objet de stratégie de » (GPO, Group Policy Object).

Bien que les GPO soient conçus pour rationaliser les opérations informatiques et centraliser les stratégies de sécurité dans l'environnement Active Directory, comme tout autre système performant, ils peuvent faire l'objet d'une utilisation inappropriée ou être infiltrés pour contourner les contrôles de sécurité et accéder à des données sensibles. Certaines entreprises, de moyenne et de grande taille, possèdent des centaines voire des milliers de GPO déployés dans de environnements à très grande échelle, ce qui crée non seulement une menace interne majeure, mais également une large zone potentiellement soumise à des attaques, si les contrôles de sécurité compensatoires appropriés ne sont pas mis en place.

Ce livre blanc décrit comment les GPO peuvent faire l'objet d'une utilisation inappropriée ou être exploités lorsque des contrôles de sécurité adaptés ne sont pas mis en place. Il explique également comment implémenter une architecture de sécurité multicouche qui vous permet de détecter, signaler et prévenir tout accès non autorisé aux GPO.

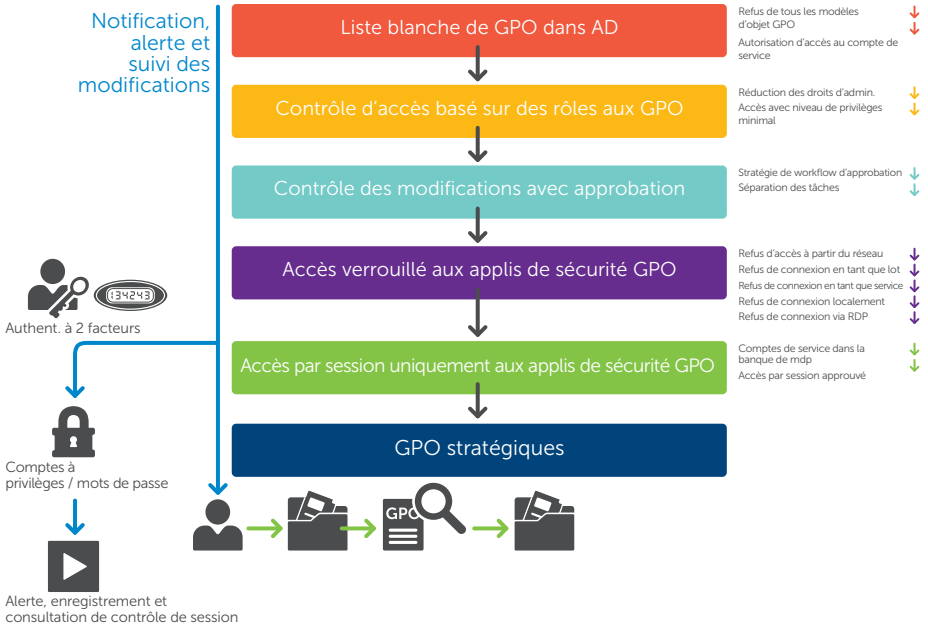


*Fig. 1. Structure de sécurité multicouche des GPO*

55 % des incidents de sécurité impliquent du personnel interne qui abuse de ses droits d'accès.[1]

## Exploitation des autorisations liées aux GPO

Sam Smith, nouvel administrateur informatique d'une entreprise de fabrication, a besoin d'installer un correctif sur un serveur de base de données Windows contenant une base de données SQL sensible avec des informations client confidentielles. Sam est administrateur de domaine et il ne peut pas se connecter à ce serveur SQL, car un GPO (**Deny log on locally**, Refus de connexion localement) a été configuré spécifiquement pour empêcher les administrateurs de domaine de se connecter à ce serveur SQL précis qui contient des détails personnels sur les clients. Au lieu de chercher à obtenir une approbation pour l'installation du correctif et de s'en charger durant la fenêtre de gestion du changement, le samedi, Sam décide de modifier le paramètre **Deny log on locally** (Refus de connexion localement) pour s'octroyer lui-même l'accès au serveur. Il désactive le GPO qui empêche les administrateurs de se connecter, puis se connecte pour installer le correctif. C'est alors que sa curiosité est attisée et qu'il décide de jeter un œil à certaines des informations sensibles sur les clients. Il va même jusqu'à en copier dans un dossier distinct. Ensuite, il modifie à nouveau le GPO pour réactiver le paramètre d'origine. Les modifications de paramétrage de GPO ne font pas l'objet d'un suivi dans les journaux de sécurité natifs. Par conséquent, un accès non autorisé n'est pas signalé jusqu'à ce qu'une révision d'audit de base de données ne soit effectuée six semaines plus tard.

## Comment une telle faille de sécurité est-elle possible ?

Malheureusement, des situations de ce type se produisent plus souvent qu'on ne le croit, que ce soit de façon accidentelle ou malveillante. En raison de la structure des autorisations de sécurité relativement aux GPO, tout administrateur de domaine peut modifier tout paramètre de sécurité GPO, et cela concerne même les paramètres censés empêcher précisément cette personne de faire certaines tâches. En outre, étant donné que les modifications de paramétrage de GPO ne sont pas suivies dans les journaux de sécurité natifs, il est impossible de surveiller de telles modifications même si vous utilisez des solutions de gestion des événements et des informations de sécurité (SIEM). Et vous ne pouvez pas empêcher que cela ne se reproduise à l'avenir, car vous n'avez aucun moyen de savoir précisément quel paramètre GPO a été modifié (valeurs antérieures et ultérieures), et vos administrateurs de domaine peuvent modifier les paramètres GPO comme bon leur semble.

## Structure de sécurité multicouche

Pour empêcher de telles failles (et de nombreuses autres), vous pouvez adopter une approche multicouche de la sécurité. Vous avez besoin d'un ensemble cohérent de contrôles de sécurité qui permettent

aux administrateurs de procéder à des modifications autorisées des paramètres GPO et, dans le même temps, qui empêchent tous intervenants externes et internes (notamment les administrateurs de domaine) d'apporter des modifications non autorisées.

Les couches de sécurité suivantes fonctionnent ensemble pour fournir les contrôles compensatoires de sécurité appropriés pour la gestion des accès aux paramètres GPO stratégiques :

- Liste blanche de GPO dans Active Directory
- Contrôle d'accès basé sur des rôles (RBAC) aux GPO
- Contrôle des modifications avec approbation
- Accès verrouillé aux applications de sécurité GPO
- Accès par session uniquement aux applications de sécurité GPO

## Liste blanche de GPO dans Active Directory

Tous les GPO sensibles (p. ex. ceux qui concernent l'ensemble d'un domaine, un contrôleur de domaine ou des applications stratégiques) sont ajoutés à la Liste de protection d'une application de sécurité tierce, avec fonctionnalités d'ajout des GPO à une liste blanche, notamment grâce à la solution Change Auditor for Active Directory. Cette solution de sécurité Windows offre une fonctionnalité qui permet un ajout en temps réel sur liste blanche et une surveillance des tentatives de modification non autorisée des paramètres GPO.

Seul un « compte de service GPO » spécifique, utilisé par une solution de sécurité (proxy) GPO tierce comme GPOAdmin et disposant de droits pour apporter des modifications aux GPO, est répertorié comme élément autorisé à modifier vos GPO les plus sensibles. Tous les autres comptes se voient automatiquement refuser l'accès pour apporter des modifications aux GPO (notamment les administrateurs de domaine). Les modifications autorisées sont possibles uniquement via l'interface GPOAdmin, ce qui fournit un modèle d'accès avec niveau de privilèges minimal et des contrôles de gouvernance appropriés concernant les modifications de GPO. L'utilisation d'une application de sécurité avec ajout des GPO à une liste blanche élimine les risques associés aux modifications quotidiennes non autorisées.

## Contrôle d'accès basé sur des rôles aux GPO

Bien que les autorisations de GPO natives soient conçues pour déléguer les autorisations aux GPO, ces autorisations créent parfois un conflit d'intérêts. Par exemple, un membre du groupe d'administrateurs de domaine peut, quand bon lui semble, apporter des modifications aux paramètres de sécurité GPO censés l'empêcher d'effectuer certaines tâches. Par conséquent, il peut être judicieux d'implémenter un modèle de contrôle d'accès basé sur des rôles, afin que les autorisations de GPO soient effectuées en dehors d'Active Directory et contrôlées par une solution de sécurité (proxy) GPO tierce comme GPOAdmin. GPOAdmin est une solution de gouvernance du cycle de vie pour les GPO. Cette solution fournit un modèle d'accès avec un niveau de privilèges minimal et vous permet de réduire le nombre d'administrateurs avec un accès trop libre aux paramètres GPO.

## Contrôles des modifications avec approbation

Lorsque vous établissez une liste blanche de GPO et un modèle de contrôle d'accès basé sur des rôles aux GPO, vous devez configurer un processus automatisé qui permet la séparation des tâches à l'aide de workflows d'approbation, afin que la personne qui modifie un paramètre GPO soit différente de la personne qui approuve le déploiement de la modification du GPO dans l'environnement de production. Cela peut paraître évident, mais il s'agit toujours d'une opération qui doit être gérée et implémentée de manière officielle.

## Accès verrouillé aux applications de sécurité GPO

Lorsque vous utilisez des applications de sécurité GPO tierces, comme Change Auditor for Active Directory et GPOAdmin, pour contrôler les modifications apportées au GPO, ces applications deviennent critiques. Il est par conséquent important de protéger également ces solutions de sécurité contre tout accès non autorisé. Pour ajouter cette couche de sécurité, il vous suffit d'ajouter une stratégie de sécurité GPO à votre liste blanche et de l'appliquer aux serveurs hébergeant vos applications de sécurité. Utilisez les paramètres suivants :

**Deny logon as a batch (Refuser la connexion en tant que lot), Deny access from network (Refus d'accès depuis le réseau), Deny logon as service (Refus de connexion en tant que service), Deny logon locally (Refus de connexion localement) et Deny logon via RDP (Refus de connexion via RDP)**

69 % des utilisateurs à privilèges déclarent que les outils de sécurité ne fournissent pas suffisamment d'informations sur les incidents.[2]

Une architecture de sécurité multicouche vous permet de détecter, de signaler et d'empêcher tout accès non autorisé aux GPO.

## Accès par session uniquement aux applications de sécurité GPO

Pour créer un accès sécurisé dédié aux administrateurs de serveur, afin qu'ils effectuent des tâches de maintenance régulières sur les applications de sécurité GPO tierces, vous devez fournir un accès contrôlé via une connexion par bureau à distance chiffrée à partir d'une « jumpbox » comme TPAM (The Privileged Appliance and Modules), qui peut également être équipée d'un système d'authentification à deux facteurs comme Quest Defender pour plus de sécurité. À partir de la jumpbox, qui est une appliance renforcée, et une fois que la session temporaire a été approuvée par le ou les approbateurs appropriés, un membre autorisé de l'équipe peut établir la connexion au serveur d'application de sécurité GPO tierce pour la réalisation de tâches de maintenance spécifiques. Toutes les opérations de la session sont enregistrées et peuvent être consultées à la demande, afin de détailler toutes les opérations effectuées sur le serveur.

## Conclusion

Des incidents de sécurité relatifs aux GPO peuvent malheureusement se produire dans toutes les entreprises, de façon accidentelle ou intentionnelle. Étant donné que les journaux de sécurité intégrés ne fournissent pas suffisamment d'informations et que les autorisations natives souffrent d'un réel manque de flexibilité, vous avez besoin d'une structure de sécurité multicouche qui intègre les capacités de solutions de sécurité GPO tierces pour détecter, signaler et empêcher les incidents de sécurité GPO qui compromettent les données précieuses de votre organisation.

## À propos de l'auteur

Alvaro Vitta est consultant principal en solutions et spécialiste de la sécurité chez Quest. Depuis plus de 15 ans, Alvaro évalue, conçoit, teste et déploie des solutions de sécurité pour des plateformes sur site ou basées sur le Cloud dans de grandes entreprises des secteurs privé et public. Les domaines concernés par les solutions sont la gestion des accès et des identités, Active Directory, la gouvernance, les risques et la conformité dans les entreprises internationales. Alvaro possède différentes certifications, notamment CISSP, CISSO, MCSE et ITIL.

[1] *« 2015 Data Breach Investigations Report » (Rapport d'enquête 2015 sur les violations de données), Verizon, avril 2015, http://www.verizonenterprise.com/DBIR/2015*

[2] *« Privileged User Abuse and the Inside Threat » (Abus de l'utilisateur à privilèges et menace interne), Raytheon Company, mai 2014, http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf.*

## PROFIL DE QUEST

Quest aide ses clients à réduire les tâches d'administration fastidieuses afin qu'ils puissent se concentrer sur l'innovation nécessaire pour faire avancer leur entreprise. Les solutions Quest® sont évolutives, économiques et faciles à utiliser, et elles offrent un niveau d'efficacité et de productivité sans pareil. Quest invite sa communauté internationale à rejoindre ses efforts d'innovation, et réitère son engagement envers la satisfaction de ses clients. Quest continuera d'accélérer la mise à disposition des solutions les plus complètes pour la gestion du Cloud Azure, des SaaS, de la sécurité, de la mobilité des collaborateurs et de l'exploitation des bases de données.



En cas de questions sur l'utilisation de ce document, nous vous invitons à contacter :

**Quest Software Inc.**
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656, États-Unis

Veuillez vous rendre sur notre site Web (www.quest.com) pour obtenir nos coordonnées à l'échelle locale et internationale.