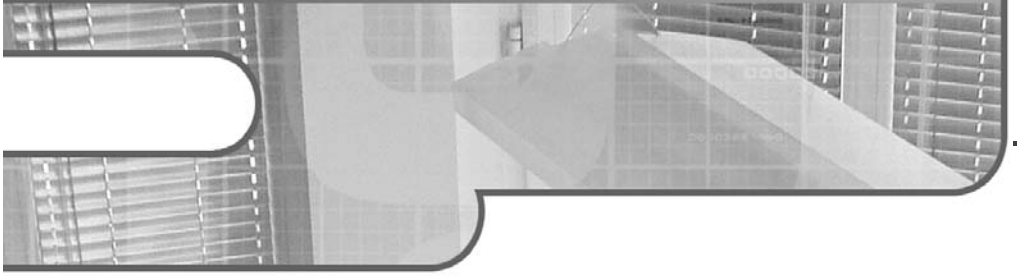

Chapitre 6
Stratégies de groupe et sécurité

1. Introduction

Dans le domaine informatique, la sécurité est un des éléments les plus sensibles. Le terme sécurité est large et il englobe une multitude de concepts. La sécurité physique des données de l'entreprise, l'intégrité des données informatiques, leur disponibilité et leur sauvegarde contribuent au maintien de l'existence de l'entreprise. La majorité des réseaux d'entreprise sont aujourd'hui connectés à Internet. Il existe deux grandes catégories : la sécurité domestique et la sécurité extérieure.

La sécurité domestique relève de toutes les manipulations maladroites ou intentionnelles qui peuvent nuire à l'intégrité du réseau local. La sécurité extérieure doit empêcher les attaques, virus et autres programmes malveillants d'agir. Ceux-ci sont majoritairement issus de l'extérieur de l'entreprise. Ces intrusions proviennent le plus souvent d'Internet ou de supports amovibles.

Maîtriser les stratégies de groupe dans les environnements Windows, c'est augmenter la capacité de sécurisation de l'entreprise. D'innombrables paramètres de stratégies liés à la sécurité des postes de travail et des serveurs ainsi que des données du réseau sont configurables avec les GPO.

Les politiques de sécurité varient d'une organisation à une autre, selon les besoins définis et l'activité de celle-ci. Une fois le niveau de sécurité déterminé, il est possible de configurer les stratégies de groupe correspondantes.

Lister et détailler toutes les options de sécurité et leur impact n'est pas l'objet de cet ouvrage. Nous allons plutôt nous concentrer sur les éléments principaux inhérents à la sécurité de Windows grâce aux stratégies de groupe.

Dans ce chapitre, nous présenterons les paramètres de sécurité considérés comme les plus importants. Nous expliquerons leurs actions et explorerons les différents niveaux des stratégies de sécurité.

2. Création du domaine et stratégies par défaut

Dans un domaine existant, les administrateurs habilités sont seuls responsables de la création de nouvelles stratégies de groupe, de leurs liaisons aux sites, aux domaines ou aux unités d'organisations et des paramètres qu'elles modifient.

Lors de la création d'un nouveau domaine, certaines opérations sont exécutées automatiquement dont la création des stratégies de groupe par défaut.

Initialement, lors de la promotion d'un serveur en contrôleur de domaine, l'unité d'organisation Domain Controllers est créée dans Active Directory. C'est dans cette unité d'organisation que seront hébergés les objets contrôleurs de domaine par défaut.

La stratégie de groupe Default Domain Policy est ensuite créée et liée au niveau du domaine. Cette GPO est la stratégie de domaine par défaut. Les paramètres définis s'appliquent à tous les objets contenus dans Active Directory.

Pour finir, la stratégie de groupe Default Domain Controllers Policy est créée et liée à l'unité d'organisation Domain Controllers. Cette GPO définit les paramètres de stratégies qui s'appliquent aux contrôleurs de domaine de l'entreprise.

Microsoft recommande de modifier uniquement les paramètres de sécurité de ces stratégies de groupe. Pour toute modification n'ayant aucun lien avec la sécurité, il est préférable de créer des GPO exclusives. Il est ensuite possible de les lier au niveau du domaine si nécessaire.

Remarque

Attention : si l'intégrité des stratégies de groupe Default Domain Policy et Domain Controllers Policy est altérée, il est très difficile de revenir en arrière !

2.1 La stratégie Default Domain Policy

La stratégie Default Domain Policy est liée au domaine Active Directory par défaut.

Le but principal de cette stratégie est de définir les politiques utilisées pour les comptes utilisateurs du domaine.

Voici les trois paramètres de stratégie qui nous intéressent :

– Politiques de mot de passe,
– Stratégies de verrouillage du compte,
– Stratégies des comptes Kerberos.

Ces trois paramètres définissent la façon dont les comptes utilisateurs vont fonctionner dans le réseau. Vous pouvez modifier directement la stratégie de groupe Default Domain Policy ou créer une nouvelle GPO pour configurer les paramètres de comptes utilisateurs de votre organisation. Une fois la GPO terminée, il suffit de la lier au domaine pour qu'elle fonctionne de la même façon que la stratégie par défaut Default Domain Policy.

L'utilisation de cette option garantit l'intégrité de la stratégie Default Domain Policy et ne prend pas plus de temps à configurer. Dans ce cas, il est impératif de prendre en compte les principes de précédence des GPO.

2.1.1 Les paramètres de stratégies du domaine

Il existe cinq paramètres de stratégie qui, une fois modifiés, ne prennent effet que si la GPO est liée au niveau du domaine. Voici la liste de ces paramètres et leurs fonctions :

- Forcer la déconnexion des comptes : il est possible de définir les plages horaires pendant lesquelles les comptes Active Directory des utilisateurs fonctionnent. Passé la limite, les utilisateurs sont automatiquement déconnectés de leurs sessions.
- Comptes : renommer le compte administrateur local. Vous pouvez renommer le nom du compte administrateur local du poste.
- Comptes : renommer le compte invité. Vous pouvez l'utiliser pour renommer le compte invité sur les postes de travail.
- Comptes : statut du compte administrateur. Cette option fonctionne à partir des versions Windows Server 2003 et supérieures. Vous pouvez désactiver le compte administrateur local sur les postes de travail.
- Comptes : statut du compte invité. Cette option fonctionne à partir des versions Windows Server 2003 et supérieures. Vous pouvez désactiver le compte invité sur les postes de travail.

Remarque

Ces paramètres de stratégie ne fonctionnent que s'ils sont appliqués au domaine entier.

2.1.2 Modifier la Default Domain Policy ou en créer une nouvelle

Il est possible de modifier directement la Default Domain Policy pour configurer le comportement des comptes utilisateurs du domaine ou de créer une stratégie à part entière et de la lier au niveau du domaine.

Si vous choisissez de créer une nouvelle GPO pour configurer les comptes utilisateurs, le problème de la précédence des GPO se pose. Or, nous avons étudié que la dernière GPO qui s'applique est celle qui a la priorité la plus élevée. Il faudra donc changer la précédence de la stratégie des comptes utilisateurs pour qu'elle s'applique en dernier, après la Default Domain Policy. Sinon, les paramètres de configuration des comptes utilisateurs ne prendront pas effet sur les postes de travail car ils seront annulés et remplacés par ceux de la Default Domain Policy.

Il est recommandé de modifier la Default Domain Policy directement pour les paramètres de stratégies des comptes utilisateurs. Il faut penser à lui attribuer le niveau de précédence le plus élevé, et éviter l'apparition de conflit car elle aura la priorité sur les autres GPO du domaine.

2.2 Stratégie Default Domain Controllers Policy

Dans un domaine Active Directory, tous les serveurs promus au rang de contrôleurs de domaine sont automatiquement intégrés à l'unité d'organisation Domain Controllers.

La stratégie Default Domain Controllers Policy créée par défaut à la mise en place du domaine définit les paramètres de stratégie qui s'appliquent à tous les contrôleurs de domaine contenus dans l'unité d'organisation Domain Controllers.

Vous pouvez également créer une nouvelle GPO pour configurer les contrôleurs de domaine et lui attribuer le plus haut niveau de précédence pour qu'elle s'applique après la stratégie par défaut. Mais il est recommandé d'utiliser la Default Domain Controllers Policy disponible à cet effet.

2.3 Réparer les stratégies par défaut

Il arrive que les stratégies de groupe soient corrompues et ne fonctionnent plus correctement. Il est recommandé d'utiliser les sauvegardes des stratégies par défaut faites idéalement avant les premières modifications.

Si aucune sauvegarde n'a été effectuée, Windows Server 2008, 2008 R2 et 2012 proposent des outils en ligne de commande qui permettent de restaurer les stratégies de groupe à leur état initial. Ces commandes fonctionnent à partir de la version 2003 de Windows Server et offre les fonctionnalités suivantes : restauration de la stratégie Default Domain Policy ou de Default Domain Controllers Policy ou les deux ensembles.

Pour effectuer une restauration des stratégies de domaine par défaut, il faut être connecté au serveur contrôleur de domaine principal avec les droits d'administration requis.

Une fois authentifié, éditez une fenêtre de commande DOS et tapez la commande **DCGPOFIX** en choisissant un des paramètres suivants :

– **`DCGPOFIX /Target:Domain`** pour restaurer la Default Domain Policy.

– **`DCGPOFIX /Target:DC`** pour restaurer la Default Domain Controllers Policy.

– **`DCGPOFIX /Target:BOTH`** pour restaurer les deux.

Toutefois, **DCGPOFIX** ne fonctionne pas si le schéma Active Directory a subi des modifications depuis l'installation du contrôleur de domaine. Par exemple pour installer Exchange Server quelle que soit la version installée, le schéma Active Directory doit être modifié. Il en est de même pour System Center Configuration Manager.

Dans ce cas, utilisez la commande suivante :

– **`GPOFIX /ignoreschema`** pour ignorer les modifications du schéma.

Astuce

*Pour restaurer les GPO par défaut d'un contrôleur de domaine Windows Server 2000, vous pouvez télécharger l'outil **RecreateDefPol** sur le site de Microsoft.*