Bonnes pratiques de stratégie de groupe

Bonnes pratiques de conception de la stratégie de groupe

La stratégie de groupe est un ensemble de paramètres du registre Windows qui contrôlent la sécurité, les audits et d'autres comportements opérationnels. La stratégie de groupe vous permet par exemple d'empêcher des utilisateurs d'accéder à certains fichiers ou à certains paramètres du système, d'exécuter des scripts lorsque le système démarre ou s'arrête, ou de forcer une page d'accueil particulière à s'ouvrir pour tous les utilisateurs du réseau. Ces bonnes pratiques relatives à la stratégie de groupe d'Active Directory vous aideront à protéger vos systèmes et à optimiser vos performances.

Ne modifiez ni la stratégie de domaine par défaut, ni la stratégie de contrôleur de domaine par défaut

Utilisez la stratégie de domaine par défaut uniquement pour les paramètres de comptes, de verrouillage de comptes, de mots de passe et d'authentification Kerberos, et mettez les autres paramètres dans d'autres GPO. La stratégie de domaine par défaut s'applique au niveau domaine, elle affecte donc tous les utilisateurs et ordinateurs du domaine.

Utilisez la stratégie de contrôleur de domaine par défaut uniquement pour la stratégie d'attribution des droits d'utilisateur et pour la stratégie d'audit, et mettez les autres paramètres dans d'autres GPO.

Cependant, même pour les stratégies mentionnées ci-dessus, il est préférable d'utiliser des GPO distinctes.

Créez une structure d'unités d'organisation (OU) bien conçue dans Active Directory

Une structure d'OU bien conçue permet d'appliquer plus facilement la stratégie de groupe et de remédier aux problèmes plus efficacement. Ne mélangez pas différents types d'objets AD dans les OU, mais séparez les utilisateurs et les ordinateurs dans leurs propres OU, puis créez des sous-OU pour chaque service ou fonction métier. Le fait de mettre les utilisateurs et les ordinateurs dans des OU distinctes facilite l'application des stratégies d'ordinateur à tous les ordinateurs et l'application des stratégies d'utilisateur à tous les utilisateurs. Il est plus facile de créer un GPO et de l'associer à plusieurs OU que de l'associer à une seule et d'avoir à gérer des ordinateurs ou des utilisateurs non concernés par la stratégie. Cependant, ne planifiez pas votre architecture d'OU en fonction seulement de la manière dont vous y associerez les stratégies de groupe.

Donnez aux GPO des noms descriptifs

S'il est possible d'identifier rapidement à quoi sert un GPO simplement en lisant son nom, l'administration de la stratégie de groupe s'en trouve grandement simplifiée. En donnant à un GPO un nom générique de type « paramètres pc », vous compliquez la tâche aux administrateurs systèmes. Vous pouvez par exemple utiliser les modèles d'appellation suivants :

- ✔ Stratégies de comptes d'utilisateur : U_<nom de la stratégie>
- ✔ Stratégies de comptes d'ordinateur : O_<nom de la stratégie>
- ✔ Stratégies de comptes d'ordinateur et d'utilisateur : OU_<nom de la stratégie>

Voici quelques exemples d'utilisation de ces règles d'appellation :

- ✔ U_StratégieRestrictionLogicielle
- ✔ U_InstallationLogiciels
- ✔ O_ParamètresBureau
- ✔ OU_ParamètresAudit

Créez chaque GPO selon sa fonction plutôt que selon les emplacements auxquels vous l'associez. Par exemple, si vous souhaitez un GPO doté de paramètres de renforcement des serveurs, n'y mettez que des paramètres de renforcement de serveurs et nommez-le d'une manière qui illustre cela.

Ajoutez des commentaires à vos GPO

En plus de trouver des noms appropriés, ajoutez des commentaires à chaque GPO, qui expliquent pourquoi il a été créé, son objectif et quels paramètres il contient. Ces informations pourront s'avérer d'une grande utilité quelques années plus tard.

Ne définissez pas les GPO au niveau domaine

Chaque objet de stratégie de groupe défini au niveau domaine sera appliqué à tous les objets utilisateurs et ordinateurs. Certains paramètres peuvent alors être appliqués à des objets auxquels vous ne les destiniez pas. Pour cette raison, le seul GPO à définir au niveau domaine est la stratégie de domaine par défaut. Il est préférable d'appliquer les autres stratégies à un niveau plus granulaire.

Appliquez les GPO au niveau racine d'OU

L'application de GPO au niveau OU permet aux sous-OU d'hériter de ces stratégies, il n'est donc pas nécessaire d'associer la stratégie à chaque sous-OU. Si vous souhaitez que certains utilisateurs ou ordinateurs n'héritent pas d'un paramètre, vous pouvez les mettre dans leur propre OU et appliquer la stratégie à cette OU directement.

N'utilisez pas les dossiers racines Utilisateurs ou Ordinateurs dans Active Directory

Ces dossiers ne sont pas des OU, ils ne peuvent donc pas être associés à des GPO. La seule manière d'appliquer des stratégies à ces dossiers est de les associer au niveau domaine, mais comme nous l'avons expliqué, vous devez éviter cela. Par conséquent, dès qu'un nouvel objet utilisateur ou ordinateur apparaît dans ces dossiers, déplacez-le immédiatement dans l'OU appropriée.

Ne désactivez pas les GPO

Si un GPO est associé à une OU et que vous ne souhaitez pas l'appliquer, supprimez le lien, plutôt que de désactiver le GPO. La suppression du lien d'une OU ne supprime pas le GPO, mais ses paramètres ne sont plus appliqués. La désactivation du GPO empêche son application à tout le domaine, ce qui peut provoquer des problèmes si vous utilisez cette stratégie de groupe dans une autre OU, elle ne s'y appliquera plus.

Mettez en œuvre la gestion des modifications pour la stratégie de groupe

La stratégie de groupe peut devenir incontrôlable si vous permettez à tous vos administrateurs d'effectuer toutes les modifications qu'ils veulent. Mais il peut s'avérer difficile de suivre les modifications apportées à la stratégie de groupe, car les journaux de sécurité n'offrent pas une visibilité totale sur ce qui a été modifié et comment. Consultez le Guide de référence rapide sur l'audit de la stratégie de groupe pour savoir comment suivre les modifications apportées à la stratégie de groupe (https://www.netwrix.com/group_policy_auditing_quick_reference_guide.html).

Les modifications les plus importantes apportées aux GPO doivent être discutées avec la direction et documentées en détail. De plus, vous devez définir des alertes e-mail pour les modifications apportées aux GPO critiques, car vous devez être informé dès que possible de telles modifications afin d'éviter toute indisponibilité système. Pour cela, vous pouvez utiliser des scripts PowerShell ou, ce qui est plus pratique, un logiciel d'audit informatique comme Netwrix Auditor for Active Directory (https://www.netwrix.fr/active_directory_auditing.html).

Évitez de bloquer l'héritage et la mise en œuvre des stratégies

Avec une bonne structure d'OU, vous évitez d'avoir à bloquer l'héritage et la mise en œuvre des stratégies. Ces paramètres peuvent rendre plus difficiles la gestion des GPO et la résolution des problèmes connexes. Le blocage de l'héritage et de la mise en œuvre des stratégies ne sont jamais nécessaires si la structure des OU est bien conçue.Create each GPO according to its purpose rather than where you're linking it to. For example, if you want to have a GPO that has server hardening settings in it, put only server hardening settings in it and label it as such.

Utilisez des petits GPO pour simplifier l'administration

Les petits GPO facilitent la résolution des problèmes, la gestion, la conception et l'implémentation. Voici quelques moyens de scinder les GPO en stratégies plus petites :

- ✔ Paramètres du navigateur
- ✔ Paramètres de sécurité
- ✔ Paramètres d'installation des logiciels
- ✔ Paramètres AppLocker
- ✔ Paramètres réseau
- ✔ Mappage des lecteurs

Gardez cependant à l'esprit que les GPO de grande taille dotés de nombreux paramètres requièrent moins de traitement lors de la connexion (les systèmes ayant moins de requêtes à effectuer pour obtenir les informations de GPO). Le chargement de nombreux petits GPO peut prendre plus de temps. Cependant, les GPO de grande taille peuvent présenter des conflits de paramètres qu'il faudra résoudre, et vous devrez faire attention à l'héritage des GPO.

Accélérez le traitement des GPO en désactivant les configurations d'ordinateurs et d'utilisateurs inutilisées

Si un GPO est assorti de paramètres d'ordinateur mais pas de paramètres d'utilisateur, vous devez désactiver la configuration utilisateur de ce GPO afin d'améliorer les performances de traitement de la stratégie de groupe lors de la connexion aux systèmes. Voici d'autres facteurs qui peuvent entraîner des temps de démarrage et de connexion lents :

- ✔ Scripts de connexion téléchargeant des fichiers volumineux
- ✔ Scripts de démarrage téléchargeant des fichiers volumineux
- ✔ Mappage de lecteurs de base éloignés
- ✔ Déploiement d'énormes pilotes d'imprimante via les préférences de la stratégie de groupe
- ✔ Surutilisation du filtrage de la stratégie de groupe selon l'appartenance aux groupes AD
- ✔ Utilisation excessive des filtres WMI (Windows Management Instrumentation) (voir la section suivante pour plus d'informations)
- ✔ Dossiers personnels d'utilisateurs appliqués via le GPO

Évitez d'utiliser beaucoup de filtres WMI

WMI comprend de très nombreuses classes grâce auxquelles vous pouvez décrire presque tous les paramètres utilisateur et ordinateur. Cependant, l'utilisation de nombreux filtres WMI ralentit la connexion et entraîne une mauvaise expérience utilisateur. Efforcez-vous d'utiliser des filtres de sécurité avec WMI, lorsque c'est possible, car ils nécessitent moins de ressources.

Réservez le traitement en boucle à des cas d'utilisation spécifiques

Le traitement en boucle limite les paramètres utilisateur à l'ordinateur auquel s'applique le GPO. Le traitement en boucle est couramment utilisé sur les serveurs de terminaux : les utilisateurs se connectent à un serveur et vous devez appliquer des paramètres utilisateur spécifiques lorsqu'ils se connectent uniquement à ces serveurs. Vous devez créer un GPO, activer le traitement en boucle et appliquer le GPO à l'OU qui contient les serveurs.

Utilisez « gpresult » pour résoudre les problèmes de GPO

La commande gpresult affiche les informations de stratégie de groupe pour un utilisateur et un ordinateur distants. De plus, elle réduit le temps nécessaire au traitement du GPO. Cette commande est disponible uniquement sous Windows 10 et Windows Server 2016. L'utilitaire gpresult comporte de nombreux paramètres ; vous pouvez les consulter en entrant la commande « gpresult /? ».

Utilisez la gestion avancée des stratégies de groupe (AGPM)

AGPM offre des fonctions d'édition des GPO, de contrôle de version et de suivi des modifications. Elle fait partie du Microsoft Desktop Optimization Pack (MDOP) for Software Assurance et peut être téléchargée sur https://www.microsoft.com/en-us/download/details.aspx?id=54967 (https://www.microsoft.com/en-us/download/details.aspx?id=54967).

Sauvegardez vos stratégies de groupe

Configurez une sauvegarde quotidienne ou hebdomadaire des stratégies à l'aide de scripts PowerShell ou d'une solution tierce, de sorte qu'en cas d'erreur de configuration, vous puissiez toujours restaurer vos paramètres.

Bonnes pratiques relatives aux paramètres de GPO

Limitez l'accès au Panneau de configuration Windows

Il est important de limiter l'accès au Panneau de configuration, même si l'utilisateur n'est pas un administrateur sur la machine Windows. Vous pouvez bloquer tous les accès au Panneau de configuration ou autoriser un accès limité à des utilisateurs spécifiques grâce aux stratégies suivantes :

- ✔ Masquer les éléments du Panneau de configuration spécifiés
- ✔ Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC
- ✔ N'afficher que les éléments du Panneau de configuration spécifiés
- ✔ Interdisez les supports amovibles.

Les supports amovibles peuvent être dangereux. En branchant un disque infecté sur votre système, quelqu'un peut diffuser des logiciels malveillants sur l'ensemble du réseau. Dans un environnement de bureau, il est préférable de désactiver totalement les disques amovibles en utilisant la stratégie « Empêcher l'installation de périphériques amovibles ». Vous pouvez aussi désactiver les DVD, les CD et même les lecteurs de disquettes si vous le souhaitez, mais en priorité les lecteurs amovibles.

Désactivez les mises à jour automatiques des pilotes de votre système

Les mises à jour des pilotes peuvent causer de sérieux problèmes : elles peuvent provoquer des erreurs Windows, des baisses de performances ou même le redoutable écran bleu de la mort. Les utilisateurs ordinaires ne peuvent pas désactiver les mises à jour, car cette fonction est automatisée. Avec la stratégie « Désactiver la recherche de pilotes de périphériques Windows Update », vous pouvez modifier les paramètres de la stratégie de groupe Windows de manière à désactiver les mises à jour automatiques des pilotes. Vous devez toutefois spécifier les ID matériel des appareils pour lesquels vous souhaitez arrêter les mises à jour. Vous trouverez cette information dans le Gestionnaire de périphériques.

Veillez à restreindre l'accès à l'invite de commande

L'invite de commande est très utile aux administrateurs système, mais entre de mauvaises mains, elle peut devenir une catastrophe car elle donne aux utilisateurs la possibilité d'exécuter des commandes qui peuvent endommager votre réseau. Il est donc préférable de la désactiver pour les utilisateurs ordinaires. À cette fin, vous pouvez utiliser la stratégie « Désactiver l'accès à l'invite de commande ».

Désactivez le redémarrage forcé de vos serveurs

Lorsque Windows Update est activé, Windows vous incite à redémarrer le système après une mise à jour. Mais certains utilisateurs n'éteignent pas leur ordinateur lorsqu'ils quittent leur travail… si leur ordinateur est redémarré de force par Windows Update, ils peuvent perdre leurs fichiers non sauvegardés. Vous pouvez utiliser les paramètres de la stratégie de groupe pour désactiver définitivement ces redémarrages forcés.

Désactivez les installations de logiciels via AppLocker et la stratégie de restriction logicielle.

Il existe de nombreuses façons d'empêcher les utilisateurs d'installer de nouveaux logiciels sur leur système. Ceci réduit les tâches de maintenance et évite le nettoyage nécessaire en cas d'installation inadéquate. Vous pouvez empêcher l'installation de logiciels en modifiant les paramètres d'AppLocker et ceux de la stratégie de groupe de restriction logicielle, et en interdisant l'exécution de certaines extensions (par exemple « .exe »).

Désactivez NTLM dans votre infrastructure réseau

NTLM est utilisé pour les ordinateurs membres d'un groupe de travail et pour l'authentification locale. Dans un environnement Active Directory, l'authentification Kerberos doit être préférée à NTLM, car ce protocole d'authentification est plus robuste : il utilise l'authentification mutuelle plutôt que la méthode stimulation/réponse du NTLM. NTLM présente de nombreuses vulnérabilités connues et utilise une cryptographie plus faible, il est donc très vulnérable aux attaques par force brute. Désactivez l'authentification NTLM sur votre réseau en configurant la stratégie de groupe de manière à n'autoriser que l'authentification Kerberos, mais assurez-vous d'abord que les applications Microsoft et tierces de votre réseau ne nécessitent pas d'authentification NTLM.