Cours - Active Directory - Les stratégies de groupes

BTS SIO - Bloc 2 - SISR - Administration des systèmes et des réseaux

1. Stratégie locale et de domaine

1.1. Introduction

Dans le système de stratégies de groupe, **deux catégories peuvent être distinguées** : les **stratégies locales** et celles du **domaine**.

Les stratégies locales sont utilisées lors d'une approche individuelle des postes de travail.

Les stratégies de domaine sont indispensables pour configurer un parc entier d'ordinateurs clients en réseau de grande taille.

Il existe des façons d'approcher la gestion des stratégies de groupe au sein des différentes architectures Microsoft.

Si les administrateurs souhaitent utiliser les GPO au sein d'une architecture de type centralisée (appelée communément un Workgroup), l'unique moyen est de configurer une ou plusieurs stratégies locales sur chaque poste de travail.

Cette approche moins onéreuse génère cependant beaucoup de travail pour les responsables des structures informatiques.

Lorsque l'architecture est centralisée et gérée avec **Active Directory**, les **GPO** de domaines sont alors disponibles et pratiquement indispensables pour garantir une homogénéisation des GPO appliquées sur tout le parc.

1.2. Qu'est-ce qu'une stratégie de groupe ou GPO ?

Un **objet de stratégie de groupe** (GPO) **est un objet qui contient un ou plusieurs paramètres de stratégie qui eux-mêmes appliquent un paramètre de configuration pour les utilisateurs, les ordinateurs ou les deux.**

Les paramètres de stratégie de groupe sont des paramètres de configuration qui permettent aux administrateurs d'appliquer des paramètres en modifiant les paramètres du Registre spécifiques liés à l'utilisateur et spécifiques à l'ordinateur sur les ordinateurs basés sur un domaine. Vous pouvez regrouper des paramètres de stratégie de groupe pour créer des objets des stratégie de groupe, que vous pouvez ensuite appliquer aux utilisateurs et aux ordinateurs.

Une stratégie de groupe est également appelée **GPO** pour *Group Policy Object*.

1.3. Les paramètres des stratégie de groupes

Un paramètre de stratégie de groupe est le composant le plus précis de la stratégie de groupe. Il définit une modification de configuration spécifique à appliquer à un objet (un ordinateur, un utilisateur ou les deux) au sein des services de domaine Active Directory (AD DS) en général.

Une stratégie de groupe a des milliers de paramètres configurables. Ces paramètres peuvent affecter presque chaque zone de l'environnement informatique. Les paramètres ne peuvent pas tous être appliqués à toutes les versions antérieures des systèmes d'exploitation Windows Server et Windows clients. Chaque nouvelle version introduit de nouveaux paramètres et de nouvelles fonctions qui s'appliquent uniquement à cette version spécifique. Aujourd'hui, on compte plus de **3600 paramètres configurables**. Si un paramètre de stratégie de groupe est appliqué à un ordinateur qui ne peut pas le traiter, celui-ci l'ignore simplement.

La plupart des paramètres de stratégie ont trois états :

- **Non configuré**: l'objet de stratégie de groupe ne modifie pas la configuration existante de ce paramètre particulier pour l'utilisateur ou l'ordinateur.
- **Activé**: le paramètre de stratégie est appliqué.
- **Désactivé:** le paramètre de stratégie est spécifiquement inversé.

Par défaut, l'état **Non configuré** est affecté à la plupart des paramètres.

Certains paramètres ont des valeurs multiples ou leurs valeurs sont de type "chaîne de texte". Ceux-ci sont généralement utilisés pour fournir des détails de configurations spécifiques aux applications ou aux composants du système d'exploitation. Par exemple, un paramètre pourrait fournir l'URL de la page d'accueil de Windows Edge.

1.4. Structure des paramètres de stratégie de groupe

Il y a deux sections distinctes de paramètres de stratégie de groupe :

- Paramètres de l'utilisateur : il s'agit des paramètres qui modifient la ruche **HKEY** de l'utilisateur actuel dans le registre.
- Paramètres de l'ordinateur : il s'agit des paramètres qui modifient la ruche **HKEY** de l'ordinateur local dans le registre.

Les paramètres de l'utilisateur et de l'ordinateur ont chacun trois domaines de configuration qui sont illustrés dans le tableau suivant :

Domaine de configuration	Description
Paramètres logiciels	Comprennent les paramètres logiciels qui peuvent être déployés pour l'utilisateur ou l'ordinateur. Les logiciels qui sont déployés pour un utilisateur sont spécifiques à cet utilisateur. Les logiciels qui sont déployés pour l'ordinateur sont à la disposition de tous les utilisateurs de cet ordinateur.
Paramètres du systèmes d'exploitation Windows	Comprennent les paramètres de script et les paramètres de sécurité pour l'utilisateur et l'ordinateur et la maintenance Edge pour la configuration utilisateur.
Modèles d'administration	Comprennent des centaines de paramètres qui modifient le Registre afin de contrôler les divers aspects de l'environnement de l'utilisateur et de l'ordinateur. De nouveaux modèles d'administration peuvent être créés par Microsoft ou d'autres fournisseurs.

2. Les stratégies locales dans un Workgroup

Cf cours de première année : 1.2 Stratégies locales

3. Structure d'une stratégie de groupe

3.1. Introduction

Dans les versions antérieures à Windows Server 2008/2008 R2 et Vista/7, les fichiers ADM (modèles d'administration) étaient à l'origine des modèles d'administration configurables dans les stratégies de groupe. Les modifications des valeurs de registre faites par les fichiers ADM possédaient une syntaxe difficilement compréhensible et modifiable. Si les administrateurs voulaient personnaliser des valeurs de registre additionnelles à celles que Windows fournissait par défaut (les fichiers ADM standards), il était obligatoire de créer un fichier ADM personnalisé et cela nécessitait l'apprentissage de la syntaxe du langage de programmation.

L'enregistrement des fichiers ADM se faisait dans le répertoire de la stratégie de groupe dans laquelle il était créé, ajoutant à la taille de celle-ci environ 4 Mo. La réplication des contrôleurs de domaine était sensiblement alourdie par cette procédure engendrant une panne connue portant le nom de Sysvol bloat.

À partir de Windows Server 2008 et Windows Vista, une nouveauté dans le cadre de la gestion des modèles d'administration apparaît : les fichiers au format ADMX et ADML.

Les fichiers ADMX sont les successeurs des fichiers ADM présents dans les versions antérieures de Windows.

Programmés en langage XML, ces fichiers sont à l'origine des options constituant les modèles d'administration. Comme les fichiers ADM, les formats ADMX affectent la configuration de la base de registre des postes cibles. Les modifications des objets de stratégie de groupe se font dans l'interface de la console de gestion des stratégies de groupe, de façon identique au processus de configuration d'une GPO standard. Les fichiers ADMX définissent les paramètres du registre qui seront activés, désactivés ou modifiés sur les postes de travail cibles.

3.2. Fichiers ADM et ADMX

Les fichiers ADM ont pour but de générer les modifications de registre requises par le paramétrage des modèles d'administration dans les stratégies de groupe.

Leur gestion individuelle représente beaucoup de travail pour les administrateurs lorsqu'ils doivent en identifier un, le retrouver puis le dupliquer sur les postes de travail.

Les fichiers ADMX sont les successeurs des fichiers ADM ; leur structure a changé ainsi que leurs méthodes de gestion.

Lorsque nous sommes dans un environnement mixte, il est possible d'utiliser les nouvelles fonctionnalités.

Cependant, il est préférable de savoir que l'unique moyen de bénéficier de toutes les nouvelles fonctionnalités de Windows Server 2019 induit la migration de toutes les stations de travail vers, au minimum, Windows 10 et toutes les versions ultérieures.

En effet, un grand nombre de nouveaux paramètres est prévu pour fonctionner uniquement avec un niveau fonctionnel de domaine Server 2019. De plus, la plupart des nouvelles fonctionnalités qu'apporte la GPMC 3.0 sont exploitables si les postes clients sont en version Vista ou 7 au minimum.

Windows Vista et 7 contiennent près de 700 objets de stratégie à paramétrer, Windows XP n'en possède que 200. Lorsqu'un administrateur édite ou crée une stratégie de groupe, les paramètres disponibles dans le conteneur **Modèles d'administration** des nœuds **Configuration ordinateur** et **Configuration utilisateur** sont partagés entre ceux qui s'appliquent à Windows 7, 8.x et 10 et ceux qui s'appliquent aux versions antérieures.

Au sein d'un environnement qui inclut des versions mixtes de Windows, le paramétrage des GPO, plus particulièrement des modèles d'administration devra être fait en fonction des versions de Windows.

3.3. Fichiers ADMX et ADML

Les fichiers ADMX sont les éléments qui contiennent les paramètres de stratégie à définir dans la console de gestion des stratégies de groupe sous le nœud **Configuration ordinateur** et **Configuration utilisateur** - **Modèles d'administration**.

Chaque fichier ADMX correspond à un paramètre de stratégie pour une application spécifique.

Les fichiers ADMX contenant les paramètres de configuration du registre sont stockés dans le répertoire **%systemroot%\PolicyDefinitions** (**C:\Windows\PolicyDefinitions**) des contrôleurs de domaine et des postes de travail.

Chaque fichier ADMX implique la création d'un fichier ADML. Les fichiers ADML sont stockés dans un sous-répertoire du répertoire PolicyDefinitions (**C:\Windows\PolicyDefinitions**), dans le répertoire de la langue correspondante (fr-FR pour français).

Les fichiers ADM ne tenaient pas compte de la langue. Les fichiers ADMX bénéficient de leur fichier ADML qui permet d'afficher le paramètre de stratégie de groupe dans la langue désirée. Ainsi en créant un sous-répertoire dans le répertoire **%systemroot%\PolicyDefinitions** de la langue souhaitée **es-ES** puis en copiant les fichiers ADML en espagnol dans ce répertoire, si la langue espagnole est présente sur le système d'exploitation, les paramètres de GPO pourront être consultés et modifiés en espagnol.

3.4. Liens

Utilisez ce lien pour récupérer une documentation détaillée sur le fonctionnement des fichiers ADMX et ADML : http://technet.microsoft.com/fr-fr/library/cc772507%28WS.10%29.aspx

Utilisez ce lien si vous souhaitez créer vos propres fichiers ADMX. Le téléchargement du schéma ADMX vous aidera en fournissant le support de base pour la création de fichiers ADMX et ADML : http://go.microsoft.com/fwlink/?LinkId=86094

Ce lien vous permet l'accès à une documentation qui vous guidera lors de la création du fichier de base personnalisé : http://technet.microsoft.com/fr-fr/library/cc770905%28WS.10%29.aspx

Ce lien vous permettra de télécharger les modèles d'administration et les fichiers de préférence ADMX pour Windows Server 2016 : https://www.microsoft.com/fr-FR/download/details.aspx?id=48257

Ce lien vous permettra de télécharger les modèles d'administration ADM, ADMX et ADML pour Microsoft Office 2016 : https://www.microsoft.com/en-us/download/details.aspx?id=49030

3.5. Conclusion

Les objets de stratégie de groupe peuvent être utilisés sur des machines dans un **Workgroup**. Néanmoins **la charge administrative** pour gérer des postes dans un workgroup **est trop importante**, d'où **l'importance** de pouvoir **gérer** notre parc informatique de **manière centralisée avec Active Directory**.

La mise en place d'une infrastructure **Active Directory** impose une étape importante de réflexion et de planification sur l'arborescence de l'annuaire **AD**. Plus cette arborescence aura été réfléchie, plus son administration en termes de stratégie de groupe en sera facilitée. Une infrastructure AD impose une structure de résolution de noms, une synchronisation du temps de l'ensemble des machines du domaine avec le maître

d'opération **émulateur PDC** qui assure la gestion des GPO dans le domaine ainsi que la gestion du temps dans un domaine Active Directory.

Une stratégie de groupe est composée de deux fichiers, un fichier **ADMX** qui décrit la structure et les paramètres de registre de l'objet de stratégie de groupe et un fichier linguistique **ADML** qui lui permet d'afficher les paramètres ADMX associés dans une langue. Ces deux fichiers utilisent le langage XML, il est possible de migrer les anciens fichiers ADM avec ADMX Migrator. Vous aurez aussi la possibilité de personnaliser ou créer vos propres fichiers ADMX et ADML.

La puissance des modèles d'administration présente un intérêt supérieur en comparaison avec l'utilité des **filtres WMI**. Les modèles d'administration personnalisés permettent de configurer les postes de travail conformément aux attentes et aux besoins d'une entreprise.

La mise à disposition d'un **magasin central** renforce la centralisation des informations du réseau et permet la mise à jour de tous les contrôleurs de domaine grâce à la réplication.

Les filtres WMI sont quant à eux des outils très puissants puisqu'ils nous permettent de sélectionner encore plus finement des objets ordinateurs dans nos **OU**, grâce à des caractéristiques physiques. Plus votre connaissance des différentes parties du système que l'on peut filtrer augmente, plus vous pourrez utiliser WMI de manière efficace. Néanmoins, le filtrage par requête WMI prend du temps et de l'espace. Si trop de filtres WMI sont appliqués sur les postes au moment de l'application des stratégies de groupe, le réseau et les postes de travail seront alors ralentis de façon notable.

De plus, les requêtes WMI doivent être testées avant d'être déployées et appliquées de façon massive. Des requêtes WMI incorrectes peuvent sérieusement altérer le fonctionnement des stratégies de groupe et il est difficile de déterminer les causes exactes des pannes. Microsoft recommande de déployer les requêtes WMI dans vos laboratoires de test et de certifier leur bon fonctionnement avant de les intégrer aux systèmes en production.

Le nombre de paramètres configurés dans la console GPMC influence la rapidité des échanges de données sur le réseau.

4. GPO, AD et processus d'application

4.1. La clé est l'Active Directory

Les stratégies de groupe fonctionnent en corrélation étroite avec Active Directory. C'est dans l'Active Directory que sont liées les GPO pour qu'elles s'appliquent ensuite sur les postes clients.

La structure de l'Active Directory d'une entreprise, et plus particulièrement la structure des unités d'organisation, définit la façon dont il est possible de gérer les GPO.

La constitution de l'architecture Active Directory détermine la logique de création des stratégies de groupe. Il est intéressant de disposer d'un Active Directory scindé et organisé en concordance avec les différents secteurs d'activités de l'entreprise. Dans cette hypothèse, il sera plus facile de générer des stratégies de groupe orientées vers les besoins des utilisateurs et de les lier aux unités d'organisation correspondantes.

Il est recommandé également de maintenir la simplicité dans l'organisation des unités d'organisation. Une structure simple et compréhensible facilite la gestion des stratégies de groupe.

4.2. Création et cycle de vie d'une stratégie de groupe

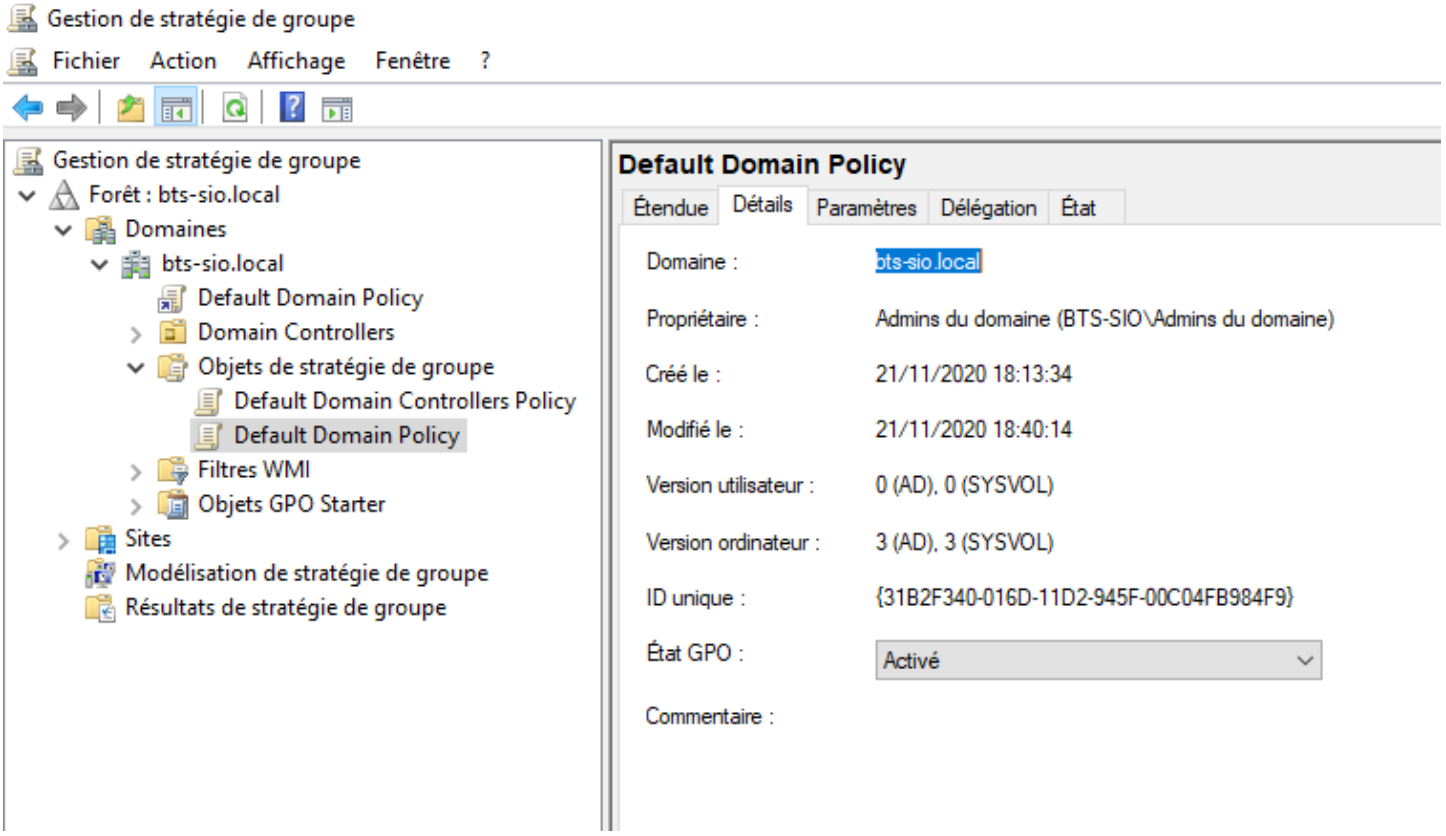
4.2.1. Localisation des GPO

Avant de vérifier la présence des stratégies de groupe dans la console GPMC, il est important de savoir qu'elles existent au sein des serveurs dès leur création. En effet, les fichiers qui constituent les stratégies de groupe sont stockés à plusieurs endroits des serveurs contrôleurs de domaine.

Certains événements se déroulent dans Active Directory lors de la création d'une stratégie dans la console de gestion des stratégies de groupe :

- Un identifiant global unique **GUID** (*Globally Unique Identifier*) est attribué à la GPO.
- Un conteneur de stratégie de groupe **GPC** (*Group Policy Container*) est créé dans la partition de domaine Active Directory.
- Un conteneur de modèles d'administration **GPT** (*Group Policy Template*) est créé dans le dossier SYSVOL\Policies du contrôleur de domaine émulateur **PDC** (*Primary Domain Controller*).

Donc, une stratégie de groupe est identifiable par le GUID obtenu à sa création. Voici un exemple de GUID délivré pour l'une des GPO du domaine.



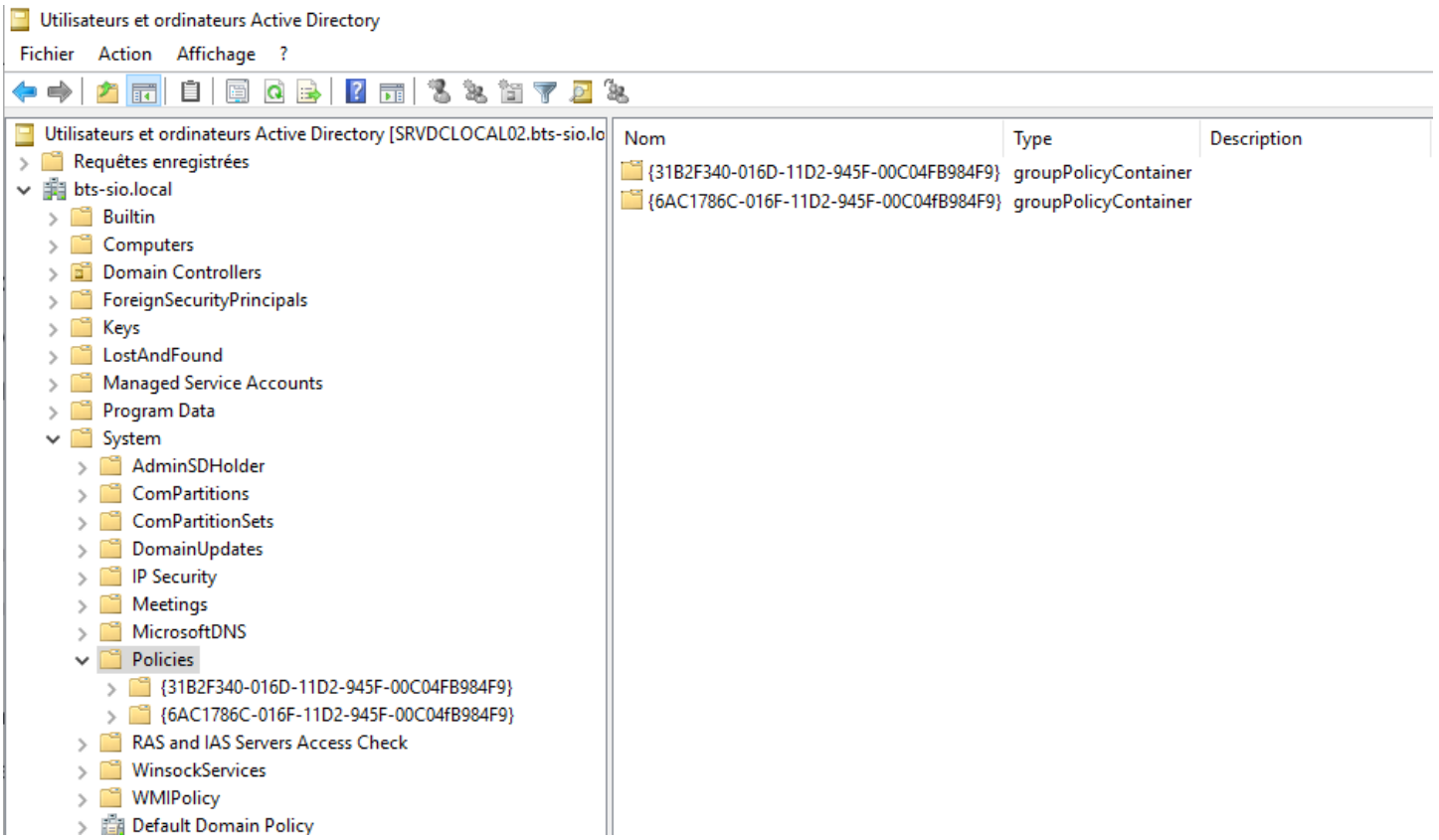
Par défaut, le GUID de la Default Domain Policy est toujours {31B2F340-016D-11D2-945F-00C04FB984F9} et celui de la Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04FB984F9} .

Le GUID (ou ID unique) garantit l'identité de la GPO dans le domaine et son unicité.

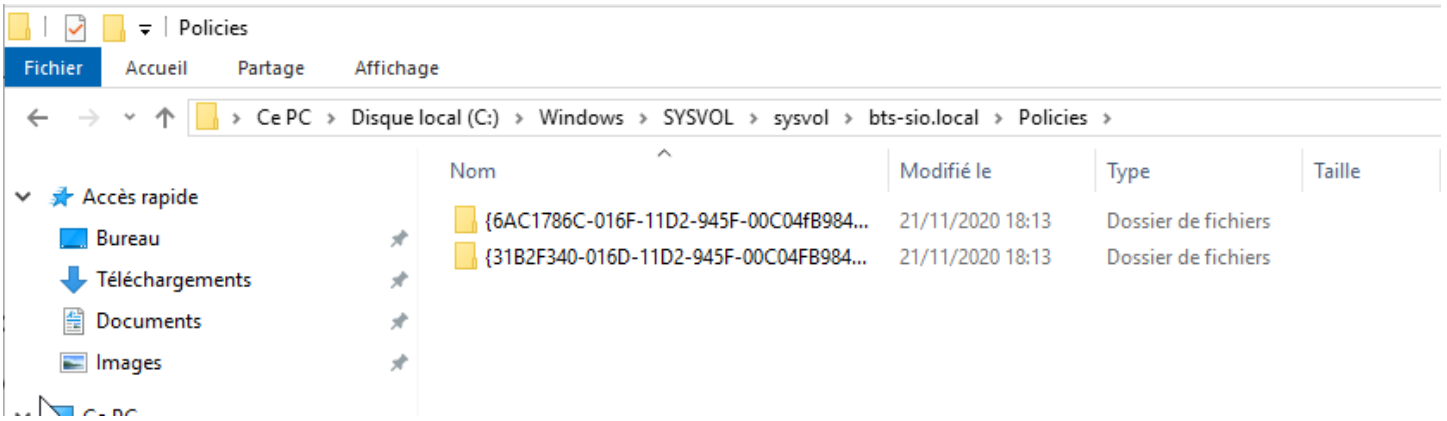
La stratégie de groupe est ensuite scindée en deux parties distinctes, GPC et GPT, qui sont stockées à deux endroits différents du contrôleur de domaine.

La GPC est stockée dans le conteneur **System\Policies** dans Active Directory. Il est nécessaire d'afficher les fonctionnalités avancées dans la console Utilisateurs et Ordinateurs Active Directory pour accéder au conteneur **Policies**.

L'illustration ci-dessous permet de voir le contenu du dossier **Policies**. Vous pouvez remarquer que les GPO sont répertoriées sous le GUID qui leur a été attribué lors de la création avec leur GPC.



Le GPT de chaque GPO est stocké dans le dossier SYSVOL\Policies du contrôleur de domaine principal. Les stratégies sont répertoriées par leur identifiant GUID au même titre que les GPC. Dans l'illustration, nous retrouvons le GPT de notre stratégie grâce à son GUID.



4.2.2. Permissions et droits d'accès sur les GPO

4.2.2.1. Création de GPO

Il faut disposer de certaines autorisations pour créer une stratégie de groupe.

Les utilisateurs ou groupes par défaut habilités à créer des objets GPO sont les membres des groupes **Administrateurs**, **Admins du Domaine** et **Administrateurs de l'entreprise**.

Le groupe **Propriétaires créateurs de la stratégie de groupe** fait partie de l'un des groupes de sécurité créés par défaut lors de la mise en place d'Active Directory. Ce groupe permet à ses membres de modifier les stratégies de groupe du domaine.

Une fois la stratégie de groupe créée, le seul utilisateur qui bénéficie des autorisations de modifications (écriture et suppression) est le propriétaire de l'objet. Cet utilisateur est en règle générale son créateur.

Cependant, les administrateurs du domaine et de l'entreprise possèdent des permissions explicites qui les autorisent à modifier les objets stratégie de groupe sans autorisation préalable du propriétaire. Leurs droits sont les plus élevés sur la totalité du domaine.

4.2.2.2. Consulter et modifier les autorisations

Les permissions concernant les stratégies de groupe sont gérées de plusieurs façons.

Les droits d'accès par défaut sont définis au moment de la création de la stratégie et sont consultables et modifiables de différentes manières.

La console de gestion des stratégies de groupe permet de modifier les autorisations des objets de stratégie de groupe de manière uniforme entre les différents éléments qui la constituent.

Il est possible de consulter les permissions des conteneurs GPC et/ou GPT d'une manière ciblée.

Attention, Microsoft recommande de n'utiliser que la console de gestion des stratégies de groupe pour modifier les permissions relatives à une stratégie de groupe. Il est pratiquement certain que la modification des permissions directement sur le conteneur GPC ou GPT d'une stratégie entraînera son dysfonctionnement.

Néanmoins, il est intéressant de connaître les différentes méthodes pour consulter et modifier les permissions des conteneurs GPC et GPT séparément.

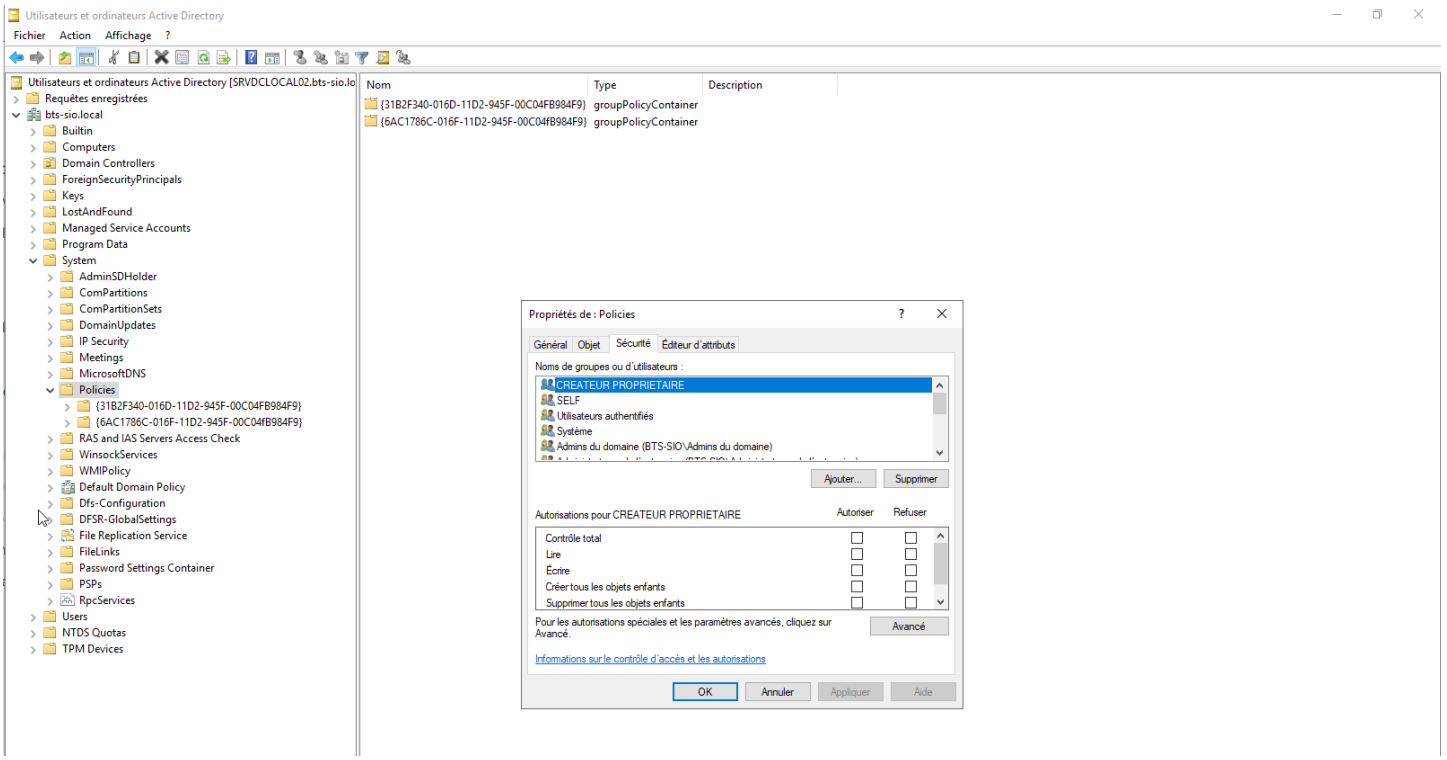
4.2.2.3. Le conteneur Policies dans Active Directory

Le conteneur **System\Policies** qui est accessible dans la console **MMC** (*Microsoft Management Console*) stocke les GPC de l'ensemble des stratégies de groupe du domaine.

Les permissions de ce dossier permettent de mettre en évidence les personnes et les groupes de sécurité du domaine qui disposent des autorisations de modifications.

L'édition des informations de sécurité de cet objet montre la présence des groupes **Administrateurs**, **Admins du domaine**, **Administrateurs de l'entreprise** et **Propriétaires créateurs de la stratégie de groupe**.

Voici une illustration des informations de sécurité du conteneur **Policies** dans Active Directory :



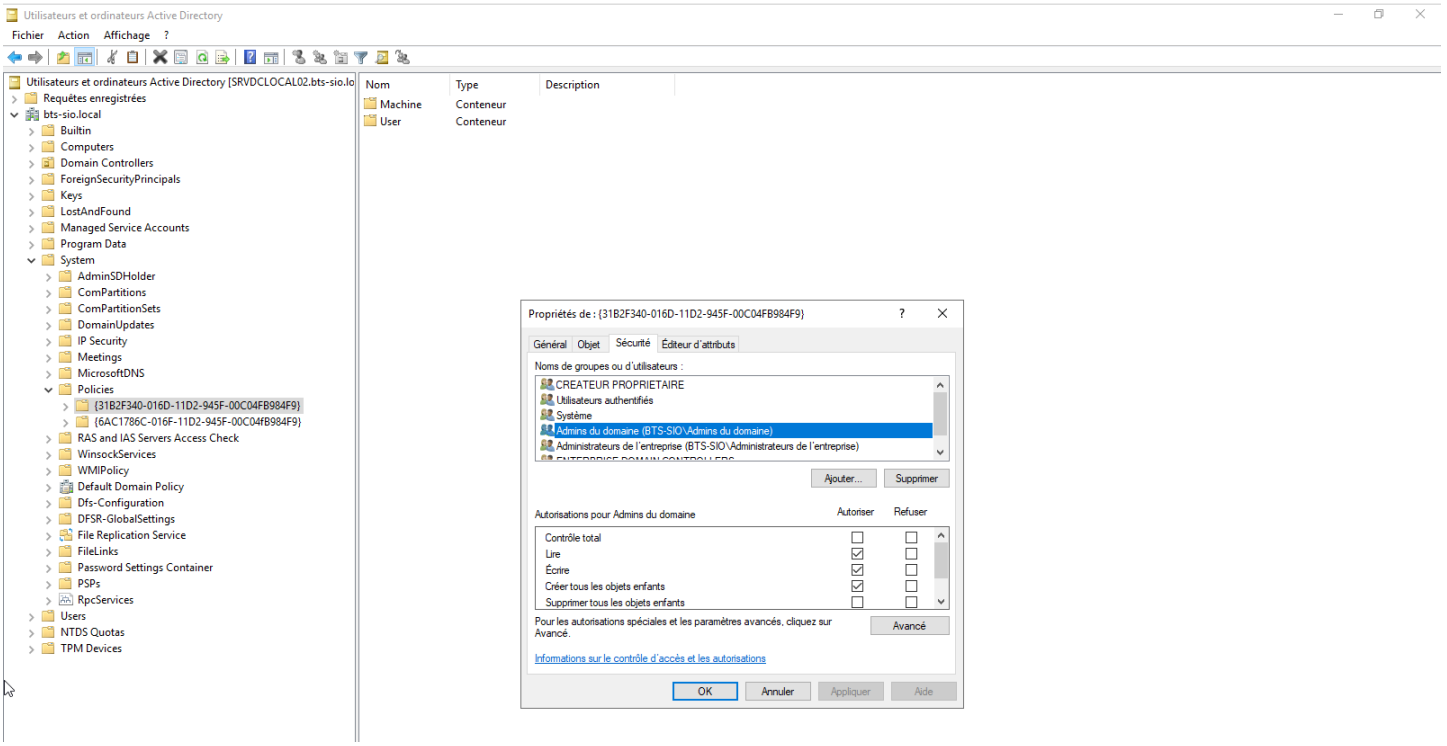
Les entités membres du groupe **Propriétaires créateurs de la stratégie de groupe** disposent uniquement des droits pour effectuer la création d'objets de stratégie de groupe. Ces droits sur ce répertoire permettent le stockage de la partie GPC des objets stratégie de groupe créés dans la GPMC.

Seuls les Administrateurs ont la possibilité de modifier le contenu du répertoire.

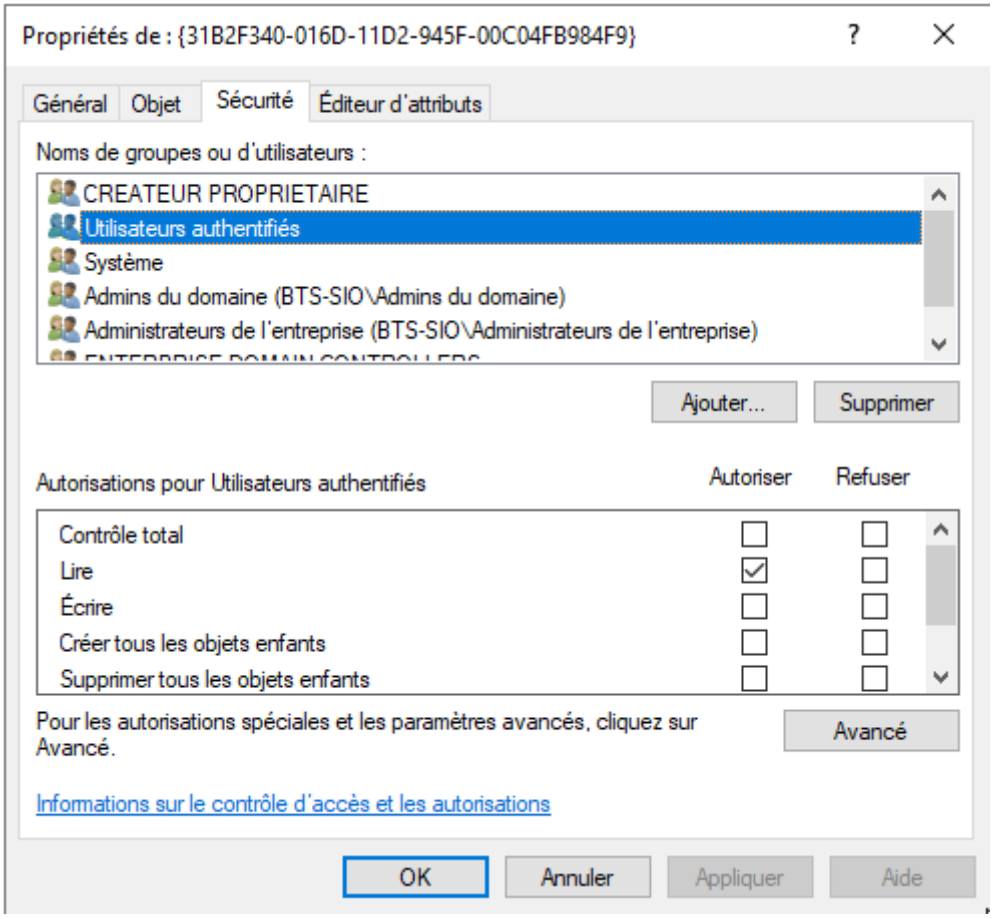
4.2.2.4. Le conteneur GPC

Les permissions du conteneur GPC sont accessibles depuis l'annuaire Active Directory. Les GPC des différentes stratégies sont localisées dans le conteneur **System\Policies** d'Active Directory. L'édition des propriétés de l'une des GPC permet d'obtenir les informations de sécurité de l'objet.

L'illustration suivante présente les propriétés de sécurité de notre stratégie de groupe identifiée par son GUID :



Concernant cette GPC, seuls les Administrateurs du domaine et de l'entreprise disposent des droits de lecture, d'écriture et de modification. Les utilisateurs authentifiés possèdent uniquement les droits de lecture, qui leur permettent d'exécuter et d'appliquer les paramètres de stratégie sur les postes clients.

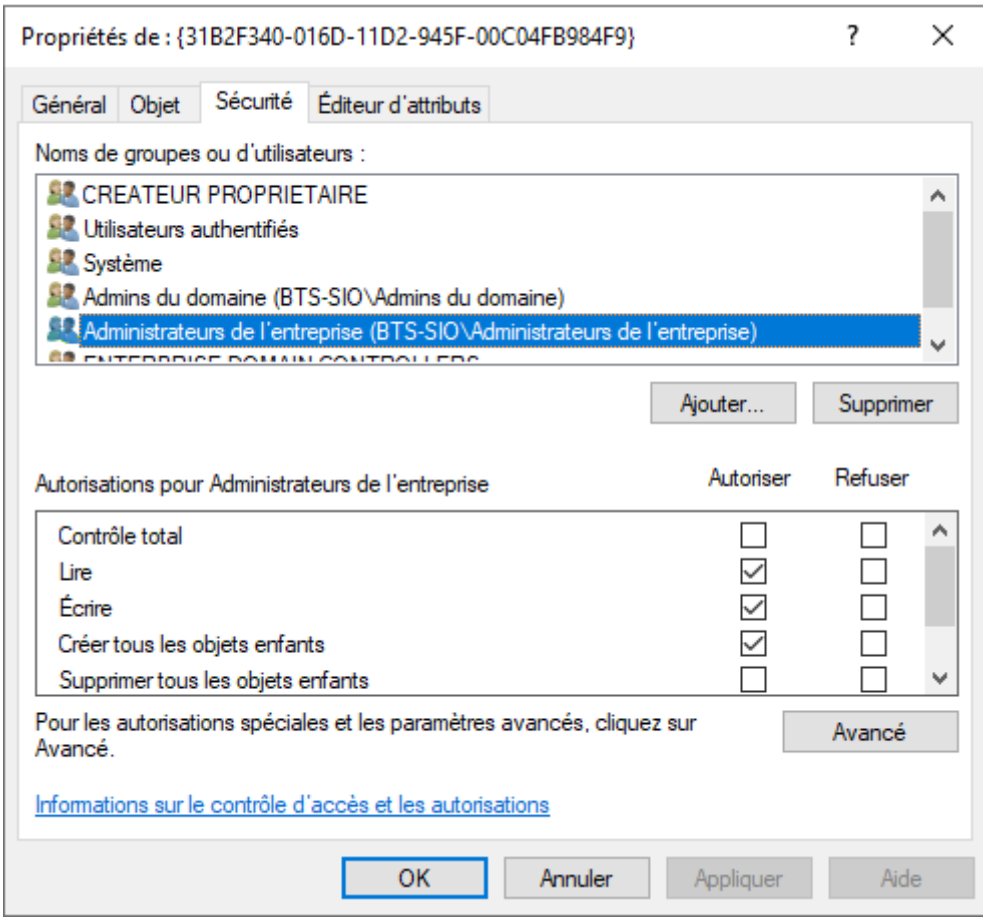


Il est possible d'ajouter ou de supprimer des utilisateurs et groupes dans l'onglet **Sécurité**. Il est important de rappeler que ces modifications ne seront pas répliquées sur l'objet GPT correspondant.

4.2.2.5. Le conteneur GPT

La consultation des permissions est basée sur les méthodes courantes de modification des autorisations des fichiers partagés. En effet, le conteneur GPT fait partie des répertoires enfants du partage SYSVOL des contrôleurs de domaine et fonctionne de la même façon qu'un répertoire classique. Il est possible d'éditer les propriétés du répertoire et de consulter ou modifier les informations de sécurité.

Voici une illustration des permissions de la GPT de notre stratégie de groupe :



4.2.3. Synchronisation des éléments GPC et GPT

Les éléments GPC et GPT sont les deux parties qui composent une stratégie de groupe.

Le conteneur de la stratégie de groupe et le modèle de la stratégie de groupe sont tous les deux répliqués entre tous les contrôleurs de domaine dans AD DS. Cependant, différents mécanismes de réplication sont utilisés pour ces deux éléments.

Le conteneur de la stratégie de groupe dans AD DS est répliqué par l'agent de duplication d'annuaire (DRA - *Directory Replication Agent*). L'agent de récupération de données utilise une topologie générée par le vérificateur de cohérence des connaissances (KCC), que vous pouvez définir ou affiner manuellement. Le résultat est que le conteneur de la stratégie de groupe est répliqué en quelques secondes à tous les contrôleurs de domaine dans un site et est répliqué entre les sites selon votre configuration de réplication intersite.

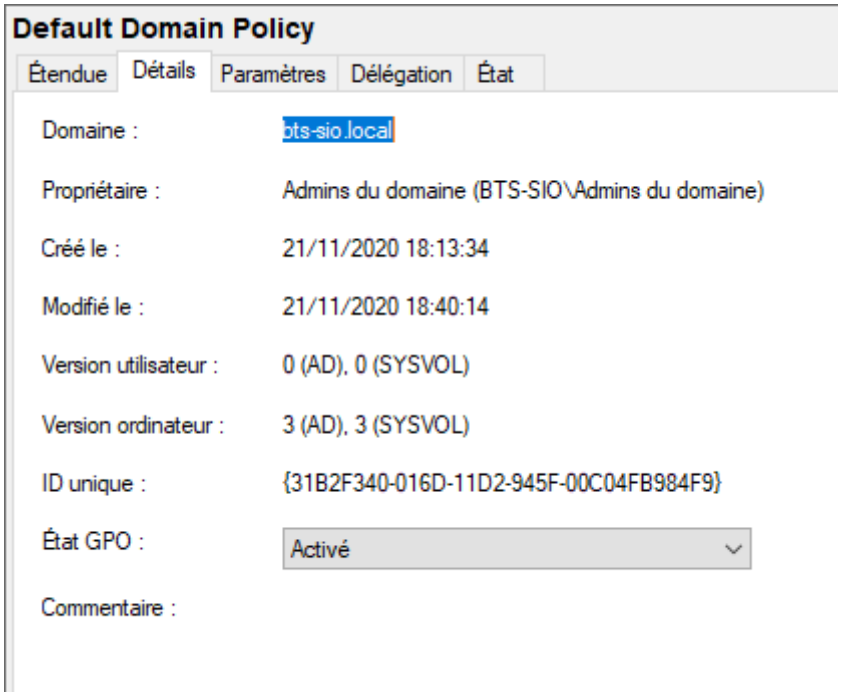
Le modèle de la stratégie de groupe dans le volume **SYSVOL** est répliqué à l'aide de l'une des deux technologies suivantes :

- Le service de réplication de fichiers **FRS** (*File Replication Service*) est utilisé pour répliquer le volume **SYSVOL** dans les domaines exécutant Windows Server 2008, Windows Server 2008 R2, Windows Server 2003, et Windows 2012.
- Si tous les contrôleurs de domaine exécutent Windows Server 2008 ou une version ultérieure, vous pouvez configurer la réplication du volume **SYSVOL** à l'aide de la réplication **DFS** (*Distributed File System*), qui est un mécanisme beaucoup plus efficace et plus fiable. Puisque le conteneur de la stratégie de groupe et le modèle de la stratégie de groupe sont répliqués séparément, il est possible qu'ils deviennent hors de synchronisation pendant une courte période.

Les stratégies de groupe appliquées à Windows 2000 et celles appliquées à Windows XP, Vista, 7 ou 8 ne tiennent pas compte des mêmes paramètres de synchronisation des éléments GPC et GPT.

Le client de stratégie de groupe peut identifier un objet de stratégie de groupe mis à jour par son numéro de version. Chaque objet de stratégie de groupe a un numéro de version qui est incrémenté chaque fois qu'une modification est faite. Le numéro de version est enregistré en tant qu'attribut de conteneur des stratégies de groupe et dans un fichier texte, GPT.ini, dans le dossier **Modèles de stratégie de groupe**. Le client de stratégie de groupe connaît le numéro de version de chaque objet de stratégie de groupe qu'il a précédemment appliqué. Si, pendant l'actualisation de la stratégie de groupe, le client de stratégie de groupe découvre que le numéro de version du conteneur de stratégie de groupe a été modifié, les extensions CSE sont informées que l'objet de stratégie de groupe est mis à jour.

Voici une illustration des numéros de version de notre stratégie de groupe :



Le système d'exploitation Windows 2000 comporte certaines limites car il n'applique les GPO que lorsque les deux éléments GPC et GPT sont synchronisés et utilisent le même numéro de version.

En conséquence, il est impératif que les deux systèmes de réplication (Active Directory et NTFRS ou DFS-R) soient en état de fonctionnement et coordonnés pour que les stratégies de groupe s'appliquent correctement sur les postes clients exécutant Windows 2000.

Les postes XP, Vista, 7, 8.x et 10 fonctionnent différemment. Lorsque la réplication Active Directory n'est pas programmée en même temps que la réplication NTFRS ou DFSR, les données GPC et GPT des contrôleurs de domaine peuvent ne pas correspondre durant l'intervalle de temps entre les deux réplications.

Ce phénomène n'empêche pas le traitement des stratégies sur les postes clients XP, Vista, 7, 8.x et 10 qui sont capables d'appliquer les paramètres contenus dans la GPC et ceux de la GPT alors que leurs numéros de version ne correspondent pas.

Lorsque les différentes réplications ont mis à jour les multiples contrôleurs de domaine et que les numéros de version ont changé, Windows détecte les modifications effectuées dans la GPO et applique les nouveaux paramètres de configuration.

Les numéros de version sont enregistrés en cache dans Windows et servent de référence pour les modifications des paramètres de stratégie. Lors de l'application d'une stratégie de groupe, un numéro de version identique à celui du cache indique qu'aucune modification n'est faite sur la GPO. Dans ce cas, le poste n'applique pas la GPO car les derniers paramètres appliqués sont les bons.

Un numéro de version différent indique au poste de travail que la stratégie a subi des modifications et qu'il est nécessaire de les télécharger et de les appliquer.

Pour les postes clients du réseau, les numéros de version sont indispensables pour signaler les modifications apportées aux stratégies de groupe.

Microsoft exige certaines conditions au fonctionnement et à l'application en bonne et due forme des stratégies de groupe sur les postes de travail :

- Les éléments GPC et GPT d'une même stratégie doivent être présents au sein des contrôleurs de domaine sur lesquels les stations sont authentifiées.
- Si le numéro de version inscrit dans la stratégie de groupe est différent de celui inscrit en cache dans le registre du poste de travail, Windows considère la stratégie comme mise à jour et décide d'en effectuer le traitement.

4.3. Application des stratégies sur les postes de travail

Afin de s'assurer du fonctionnement des GPO sur les postes des utilisateurs finaux, celles-ci doivent être appliquées selon certaines règles établies et respecter une hiérarchie définie.

Dans l'architecture d'un réseau, il existe plusieurs niveaux sur lesquels les stratégies de groupe peuvent s'appliquer.

L'ordre d'application est le suivant : stratégies locales, stratégies au niveau du site, stratégies au niveau du domaine et stratégies au niveau des unités d'organisation.

Dans ce livre, nous nous concentrons sur la gestion des stratégies de groupe dans un domaine Active Directory. Dans ce cas, l'ordre d'application prend effet à partir du site.

4.3.1. Niveaux d'application dans Active Directory

Nous pouvons considérer trois niveaux d'application différents dans Active Directory :

1. Site
2. Domaine
3. Unité d'organisation

4.3.1.1. GPO active au niveau site

Les stratégies liées au niveau des sites Active Directory affectent les utilisateurs en fonction du lieu de connexion.

Les utilisateurs existent ailleurs dans Active Directory mais récupèrent les paramètres GPO à partir de sites et services Active Directory. Afin de reconnaître sur quel site les utilisateurs se connectent, l'application vérifie à quel sous-réseau l'ordinateur appartient lors de l'attribution de l'adresse IP. Ces déclarations de sous-réseaux sont renseignées dans la console Sites et services Active Directory.

4.3.1.2. GPO active au niveau domaine

Lorsqu'une stratégie est liée au niveau domaine, elle affecte tous les utilisateurs et ordinateurs du domaine, toutes les UO et tous les sous-conteneurs UO.

4.3.1.3. GPO active au niveau unité d'organisation

Les stratégies appliquées au niveau unité d'organisation affectent les utilisateurs et ordinateurs présents dans l'UO ainsi que les objets créés dans les UO enfants.

4.3.2. Ordre d'application

Les stratégies de groupe s'appliquent dans l'ordre suivant :

1. Stratégies locales
2. Sites
3. Domaine
4. Unité d'organisation

4.3.3. Héritage des stratégies de groupe

Lorsqu'une GPO est liée à une OU dans Active Directory, les objets situés en dessous héritent des paramètres de stratégies de groupe venant du niveau supérieur.

Les stratégies sont cumulatives tant que les objets de stratégie modifiés n'entrent pas en conflit.

Les conflits de stratégies se produisent quand deux mêmes objets de stratégie sont modifiés dans deux GPO différentes.

Dans ce cas, la stratégie gagnante est la dernière qui est appliquée. Par exemple, si une GPO de domaine entre en conflit avec une GPO unité d'organisation, c'est la stratégie au niveau OU qui l'emporte. Cela concerne autant la configuration ordinateur que celle de l'utilisateur.

Quand un ordinateur démarre ou un utilisateur ouvre une session, le client de la stratégie de groupe examine l'emplacement de l'objet de l'ordinateur ou de l'utilisateur dans AD et évalue les objets de stratégie de groupe ayant l'étendue qui comprend l'ordinateur ou l'utilisateur.

Puis, les extensions CSE appliquent les paramètres de stratégie de ces objets de stratégie de groupe. Les stratégies sont appliquées séquentiellement, en commençant par celles qui sont liées au **Site**, suivies de celles liées au **Domaine**, puis celles liées aux **Unités d'organisation**, en partant de l'unité d'organisation de niveau supérieur jusqu'au dernier conteneur où se trouve l'objet. C'est une application superposée des paramètres ; ainsi un objet de

stratégie de groupe appliqué plus tard dans le processus, parce qu'il a une priorité supérieure, l'emporte sur les paramètres appliqués plus tôt dans le processus.

4.3.4. Bloquer l'héritage

Vous pouvez configurer un domaine ou une unité d'organisation pour empêcher l'héritage des paramètres de stratégie. Cette opération est appelée **blocage de l'héritage**.

4.3.5. Priorité des stratégies de groupes

Nous avons la possibilité de modifier la priorité des stratégies de groupe dans la console GPMC dans l'onglet **Objets de stratégie de groupe liés**.

Lorsque plusieurs stratégies de groupe sont liées à une même unité d'organisation, l'ordre d'application des stratégies de groupe s'effectue du bas vers le haut. La stratégie située en bas de liste sera appliquée en premier et ainsi de suite jusqu'en haut de la liste.

La priorité est indiquée sous forme de nombre dans la console GPMC, la priorité la plus élevée est définie par le nombre 1. Plus ce nombre augmente plus la priorité diminue.

4.4. Processus d'application des stratégies

4.4.1. Comprendre comment s'applique les GPO

Les stratégies de groupe possèdent un cycle de traitement particulier. Un certain nombre d'événements se déroulent depuis la création d'une GPO jusqu'à sa visibilité sur un poste de travail.

Le lieu de stockage des GPO, la partie liée à Active Directory et le chemin utilisé pour venir s'appliquer sur un poste de travail sont des éléments constituant le fonctionnement général des stratégies de groupe.

Lorsqu'une GPO vient d'être créée ou modifiée, elle ne s'applique pas directement sur les postes des conteneurs Active Directory auxquels elle est liée.

Les ordinateurs clients effectuent des requêtes plusieurs fois par jour afin de récupérer les paramètres de GPO qui leur sont destinés pour les traiter et les appliquer et les GPO sont diffusées à des moments spécifiques, selon des critères variables. C'est la phase de rafraichissement des stratégies de groupe qui est de 90 minutes par défaut.

Selon les versions de Windows que vous utilisez dans votre environnement (Windows 2000, XP, Vista, 7, 8.x et 10, Windows Server 2003, 2008, 2008 R2, 2012 R2, 2016 et 2019), les processus d'application et de récupération des GPO diffèrent. Les mécanismes d'application peuvent alors prêter à confusion.

Les règles d'application des GPO respectent une méthodologie stricte et sont définies par des paramètres inscrits par défaut. Il est cependant possible de modifier certains aspects de ces processus. Les temps d'attente entre les cycles d'application des stratégies de groupe peuvent être écourtés, les filtres WMI (*Windows Management Instrumentation*) peuvent être utilisés pour filtrer les ordinateurs cibles à partir de conditions précises. Les stratégies de groupe peuvent également traverser les forêts des environnements multiforêts. Mais il est important d'analyser les possibilités de modification offertes.

Dans cette partie du chapitre, nous abordons les principes d'application des stratégies de groupe, les différents cas de figure et approfondissons la compréhension de la chaîne d'événements depuis la création de la GPO à sa diffusion sur un poste de travail.

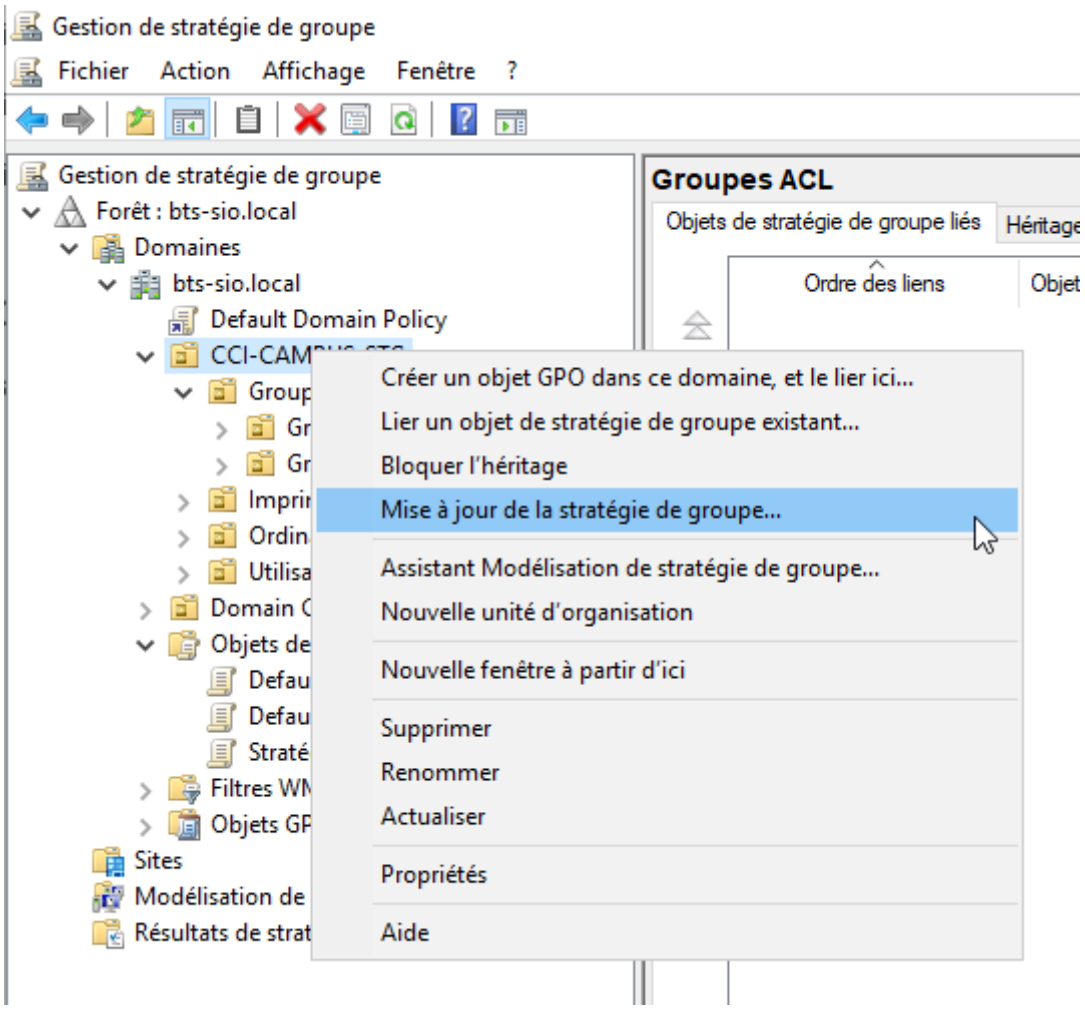
4.4.2. Principes généraux d'application des GPO

Il est important de rappeler que les GPO fonctionnent de la façon suivante :

- Création de la stratégie sur le serveur.
- Demande de récupération des paramètres de stratégies depuis le poste de travail.

Avec Windows Server 2003, 2008 et 2008 R2, il n'était pas possible de forcer l'application des GPO sur les postes clients depuis le serveur sans une application tierce.

Microsoft a intégré cette fonctionnalité dans Windows Server 2012, soit en utilisant une commande PowerShell **Invoke-GPupdate**, soit en utilisant une fonction qui a été rajoutée dans le menu contextuel de la console de stratégie de groupe lorsque l'on clique sur une OU : **Mise à jour de la stratégie de groupe**.



4.4.2.1. Processus d'application

4.4.2.1.1. Application initiale à l'ouverture de session

Les versions Windows 2000, Windows Server 2003, Windows Server 2008, 2008 R2 et Windows Server 2012, 2016 et 2019 récupèrent les paramètres de stratégie au moment de l'ouverture de session.

4.4.2.1.2. Application d'arrière-plan pour les ordinateurs membres du domaine

Les versions Windows 2000, Windows Server 2003, Windows Server 2008, 2008 R2 et 2012, 2016 et 2019, XP, Vista, 7, 8.x et 10 récupèrent les paramètres de stratégie environ 90 minutes après l'ouverture de session.

Ce paramètre peut être modifié dans une stratégie de groupe.

4.4.2.1.3. Application d'arrière-plan pour les contrôleurs de domaine

Les contrôleurs de domaine récupèrent les paramètres de stratégie toutes les 5 minutes, une fois la réplication Active Directory effectuée.

4.4.2.1.4. Application des stratégies de sécurité

L'extension de sécurité CSE (extension côté client) gère une exception importante aux paramètres de traitement de la stratégie par défaut. Les paramètres de sécurité sont ré-appliqués toutes les 16 heures, même si un objet de stratégie de groupe n'a pas changé.

Activez le paramètre de stratégie **Toujours attendre le réseau lors du démarrage de l'ordinateur et de l'ouverture de session** pour tous les clients Windows. Sans ce paramètre, les clients Windows XP, Windows Vista, Windows 7 et Windows 8 exécutent, par défaut, uniquement des actualisations en tâche de fond. Cela signifie qu'un client peut démarrer, et un utilisateur pourrait ensuite se connecter sans recevoir les dernières stratégies du domaine. Le paramètre est situé dans **Configuration ordinateur\Stratégies\Modèles d'administration\Système\Ouverture de session**.

Lors du déplacement d'un ordinateur ou d'un utilisateur d'une unité d'organisation à une autre, les processus d'application de GPO ne sont pas actifs en temps réel. Active Directory requiert un délai avant de détecter les modifications et de les appliquer.

Il existe donc plusieurs comportements concernant le principe d'application des stratégies de groupe, ces comportements sont liés à la version des systèmes d'exploitation installés sur les machines.

4.4.2.2. Processus d'application initial pour les versions Windows 2000 à 2019

Les stratégies de groupe sont divisées en deux parties distinctes, la configuration ordinateur et la configuration utilisateur.

La configuration ordinateur s'applique au démarrage des machines, avant la demande d'ouverture de session.

Les paragraphes suivants décrivent l'ordre des opérations du démarrage du poste à la demande d'ouverture de session utilisateur.

- Au démarrage de la machine, une requête DNS (*Domain Name System*) est effectuée pour trouver le nom d'un contrôleur de domaine qui va l'authentifier sur le réseau.
- Une fois le contrôleur de domaine trouvé, celui-ci indique à la machine à quel site Active Directory elle appartient, dans quel domaine elle est authentifiée et finalement dans quelle unité d'organisation elle est stockée.
- La configuration ordinateur est récupérée dans cet ordre, avant la demande d'ouverture de session.
- Une fois la stratégie appliquée, la fenêtre [Ctrl][Alt][Suppr] apparaît.
- Après l'authentification utilisateur validée par Active Directory, la partie configuration utilisateur de la GPO est récupérée dans le même ordre que précédemment : Site, Domaine et OU.
- Toutes les GPO utilisateurs qui concernent le client actuel sont appliquées à cet instant. Le Bureau de l'utilisateur apparaît uniquement après ce processus.
- L'ordre du procédé d'application des GPO : Site, Domaine et OU est appelé processus synchronisé.

4.4.2.3. Processus d'application initial pour les versions Windows XP et Vista

Dans le cas suivant, nous supposons que le poste de travail vient d'être intégré au domaine. C'est la première fois que les comptes ordinateurs et utilisateurs vont être authentifiés dans le domaine.

Le processus d'application des GPO va suivre la démarche de processus synchronisé, traité dans la partie précédente.

Au démarrage de la machine, les configurations des ordinateurs sont appliquées avant l'ouverture de session et les configurations utilisateurs après l'ouverture de session, juste avant l'affichage du Bureau. L'ordre d'application **Site**, **Domaine** et **Unité d'organisation** est maintenu.

Dans le cas de postes déjà actifs dans le domaine, la procédure d'application des stratégies de groupe est différente.

Sur la base d'un intervalle de **90 minutes** démarrant après l'ouverture de session, les GPO seront téléchargées et appliquées en arrière-plan jusqu'à la fermeture de session.

Les systèmes Windows 7, 8.x et 10 enregistrent les derniers paramètres de la stratégie ordinateur utilisée et les appliquent dès le démarrage des postes, bien que le réseau n'ait pas encore été détecté. À l'apparition de la fenêtre de commande [Ctrl][Alt][Suppr], toutes les nouvelles stratégies de groupe sont téléchargées sur le poste. Elles seront appliquées un peu plus tard après l'ouverture de session.

Microsoft a décidé de configurer les systèmes 7, 8.x et 10 de cette façon pour réduire les temps d'attente. Le démarrage du poste et l'ouverture de session utilisateur sont plus rapides car ils utilisent les dernières GPO utilisées, en quelque sorte en "cache".

Cela signifie que les GPO sont appliquées de manière asynchrone pour les environnements Windows 7, 8.x et 10.

Il existe cependant des particularités telles que les paramètres de sécurité et les modèles d'administration (fichiers qui mettent à jour le registre) téléchargés et appliqués quelques minutes après l'authentification utilisateur.

La terminologie Microsoft pour cette manière de procéder est appelée Fast Boot.

4.4.2.3.1. En résumé

Premier démarrage :

- Premier démarrage du poste après son intégration dans le domaine : application des paramètres de stratégie ordinateurs de façon synchronisée.
- Premier logon de l'utilisateur dans le domaine : application des paramètres de stratégie utilisateurs de façon synchronisée.

Pour les autres démarrages :

- À partir du deuxième démarrage du poste dans le domaine : application des derniers paramètres de stratégie ordinateurs utilisés avant la détection du réseau (procédé de mise en cache).
- À partir de la deuxième authentification utilisateur dans le domaine : téléchargement des nouveaux paramètres de stratégie et application de façon asynchrone.

4.4.2.4. Le Fast Boot

Le Fast Boot permet un gain de temps pour le démarrage du poste et l'ouverture de session utilisateur mais comporte aussi des désavantages.

L'application des GPO de façon asynchrone signifie que les changements ne sont pas visibles en temps réel. Plusieurs modifications nécessitent de redémarrer les postes pour qu'elles prennent effet. Il faut parfois redémarrer plusieurs fois les postes pour certaines modifications spécifiques (déploiement de logiciels et

redirection de dossiers). Le gain de temps au démarrage est donc altéré par les reboot que requièrent certaines modifications.

Les modifications de GPO utilisateurs demandent également de renouveler l'ouverture de session, une à deux fois en fonction des changements (répertoire Home, scripts d'ouverture de session, profils itinérants).

Il est possible de désactiver le Fast Boot sur les postes Windows XP, Vista, 7, 8.x et 10 pour qu'ils se comportent de la même manière que les environnements Windows 2000, Server 2003, 2008, 2008 R2, 2012, 2016 et 2019 (application des GPO de façon synchronisée).

Pour désactiver le Fast Boot et forcer l'application des GPO de façon synchronisée, il est nécessaire de créer une stratégie de groupe. Le composant à modifier se situe dans la section **Configuration ordinateur\Modèles d'administration\Système** puis configurez le paramètre **Exiger l'utilisation du démarrage rapide**. Ce paramètre n'affectera que les machines qui ont comme système d'exploitation Windows Server 2012, Windows 8 ou Windows RT au minimum.

Une telle stratégie va obliger les ordinateurs à détecter et télécharger les GPO et à les appliquer avant la commande d'ouverture de session [Ctrl][Alt][Suppr].

Lors de l'utilisation de démarrage rapide sur Windows 8 PC, vous verrez que les GPO qui sont ciblées lors de l'arrêt de l'ordinateur et le démarrage ne seront pas appliquées. Cela se produit parce que le noyau du système d'exploitation n'est pas totalement arrêté lors de l'utilisation de démarrage rapide. Il est plutôt en hibernation et reprend, ce qui contourne le traitement des GPO. Une fois l'utilisateur authentifié, les nouveautés ou modifications ne sont pas directement actives.

4.4.3. Appliquer les GPO manuellement

Dans certaines situations d'urgence ou lorsque vous n'avez pas le temps d'attendre la phase de rafraîchissement des stratégies de groupe pour qu'elles prennent effet d'elles-mêmes, vous pouvez utiliser des commandes qui vous permettront de forcer les stratégies de groupe sur les stations clientes.

Cette partie du chapitre liste les commandes ainsi que les actions correspondantes.

Afin de pouvoir éditer les commandes qui servent à forcer les GPO, il est obligatoire de disposer des droits administrateurs de la machine.

Les commandes sont réalisées dans l'éditeur de commande DOS (**Démarrer/Exécuter/cmd.exe**).

4.4.3.1. Commandes de Windows XP et les dernières versions

```
Gpupdate
```

Cette commande actualise consécutivement les stratégies utilisateurs et ordinateurs en cours.

```
Gpupdate /Target:Computer
```

Cette commande actualise les stratégies ordinateurs en cours.

```
Gpupdate /Target:User
```

Cette commande actualise les stratégies utilisateurs en cours.

```
Gpupdate /Logoff
```

Cette commande permet de vérifier si les paramètres de stratégies modifiés requièrent un reboot du poste pour être pris en compte.

```
Gpupdate /Boot
```

Cette commande permet de vérifier si les paramètres de stratégies modifiés requièrent un reboot du poste et redémarrent automatiquement le poste.

4.4.3.2. Commande depuis un serveur

La commande **Invoke-GPUpdate** est une applet de commande PowerShell. Cette dernière ne s'applique qu'à Windows Server 2012 et versions supérieures. Cette commande permet de rafraîchir les paramètres de sécurité qui sont définis sur des ordinateurs distants.

Détail de la syntaxe

```
Invoke-GPUpdate [[-Computer] <String>] [[-RandomDelayInMinutes] <Int32>] [-AsJob] [-Boot]
[-Force] [-LogOff] [-Target <String>]
```

- Le paramètre **[-AsJob]** nous permet d'exécuter l'applet comme en tâche de fond. Pour examiner le résultat de cette tâche, utilisez la commande **Receive-Job**.
- Le paramètre **[-Boot]** provoque un redémarrage de l'ordinateur après que les paramètres de stratégie de groupe ont été appliqués, si un redémarrage est nécessaire (par exemple les paramètres de stratégies d'installation du logiciel).
- Le paramètre **[-Force]** ré-applique l'ensemble des paramètres de stratégies de groupe.
- Le paramètre **[-LogOff]** provoque une déconnexion après l'application des paramètres de stratégies de groupe, si cela est nécessaire. Par exemple l'installation de logiciel pour la partie utilisateur, la redirection des dossiers.
- Le paramètre **[-RandomDelayInMinutes]** indique le délai, en minutes, que le planificateur de tâche attendra, et sur lequel un facteur est appliqué de manière aléatoire pour éviter une surcharge réseau. On peut spécifier des valeurs en minutes de 0 minute à 31 jours, soit 44 640 minutes.
- Le paramètre **[-Target]** nous permet de spécifier quel nœud de configuration l'administrateur souhaite mettre à jour : le nœud ordinateur ou utilisateur. Si ce paramètre n'est pas défini, les deux nœuds de configuration sont mis à jour.

La commande **Invoke-GPUpdate** ne supporte pas la planification d'une actualisation de la stratégie de groupe pour les ordinateurs fonctionnant sous Windows XP ou une version antérieure.

Afin d'utiliser cette commande, il faut au préalable que les règles de pare-feu suivantes soient définies sur chaque ordinateur afin de permettre les connexions distantes :

- Gestion à distance des tâches planifiées (RPC).
- Gestion à distance des tâches planifiées (RPC-EPMAP).
- Windows Management Instrumentation (WMI-IN).

Exemple

```
PS C:\> Invoke-GPUpdate -computer Portable01 -Target user -Force -LogOff
```

Cette commande permet de ré-appliquer l'ensemble des paramètres du nœud Utilisateur pour l'ordinateur Portable01.

5. Les outils de gestion des GPO

5.1. Administrer et gérer les GPO

L'administration des stratégies de groupe au sein d'une infrastructure Microsoft représente un des pôles majeurs de la gestion et du maintien de l'architecture réseau. Le déploiement massif de stratégies de groupe génère de nombreuses conséquences. En effet, la totalité de la chaîne informatique est impactée depuis les serveurs jusqu'aux postes de travail. Plusieurs moyens sont mis à disposition dans le but de réaliser les tâches d'administration relatives aux stratégies de groupe.

Une des méthodes envisageables est la connexion directe à l'un des contrôleurs de domaine du réseau. Dans ce cas, il est possible de créer et de gérer les stratégies à partir de la GPMC installée sur l'un d'eux.

Il est tout à fait possible d'exploiter les postes de travail installés avec XP ou Vista pour administrer le réseau de la même façon. Certains prérequis techniques doivent être respectés lorsque les administrateurs choisissent d'employer cette méthode.

La console de gestion des stratégies de groupe est un outil natif des systèmes d'exploitation Windows Server 2008, 2008 R2, 2012 et 2016. Aucune installation additionnelle n'est requise lorsque vous utilisez un contrôleur de domaine installé avec Server 2008 ou 2008 R2 ou 2012 ou 2016 ou 2019 pour administrer et gérer les stratégies de groupe.

Lorsque vous administrez les serveurs à partir de postes de travail Vista, 7 ou 8, il est nécessaire d'installer le pack RSAT (*Remote Server Administration Tool*) disponible en téléchargement sur le site de Microsoft.

Windows Vista dispose nativement de la console GPMC mais elle disparaît après l'installation du Service Pack 1.

Pour Windows 7, il existe deux packs d'administration : un pour la version RTM (*Release to Manufacturing*) et un pour le SP1 de Windows 7. Il est nécessaire de télécharger le pack RSAT de la même façon que pour Windows Vista. Les packs sont disponibles sur le site de Microsoft en téléchargement gratuit à l'adresse : http://www.microsoft.com/fr-fr/download/details.aspx?id=7887 pour la version SP1.

Microsoft met à disposition des administrateurs deux autres outils pour gérer et suivre le cycle de vie des stratégies de groupe : un ensemble de commandes PowerShell ainsi qu'une suite logicielle AGPM.

5.2. Gérer les GPO avec la console de gestion des stratégies de groupe GPMC 3.0

5.2.1. Implémenter la console GPMC 3.0

Selon la version de Windows Server installée sur les contrôleurs de domaine, l'utilisation de la GPMC est soumise à des conditions.

Les serveurs installés avec la version Entreprise de Windows Server 2008 et 2008 R2 ou la version Datacenter de Windows Server 2012 bénéficient de la console de gestion des stratégies de groupe dès la promotion du serveur au rang de contrôleur de domaine. Sur un serveur membre, il faudra installer la console de gestion des stratégies de groupe.

5.2.2. Installation de la fonctionnalité Gestion des de groupe

Cf document dédié

SISR4 - 04 - Cours - Active Directory - 07 - Gestion des GPO

5.2.3. Fonctionnalité de la console GPMC 3.0

Cf document dédié

SISR4 - 04 - Cours - Active Directory - 07 - Gestion des GPO