Active Directory :

L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc.

Active Directory existe depuis la version 2000, Le service d'annuaire Active Directory peut être mis en œuvre sur Windows 2000 Server, Windows Server 2003 et Windows Server 2008, il résulte de l'évolution de la base de compte plane SAM. Un serveur informatique hébergeant l'annuaire Active Directory est appelé « contrôleur de domaine ».

Active Directory stocke ses informations et paramètres dans une base de données centralisée. La taille d'une base Active Directory peut varier de quelques centaines d'objets pour de petites installations à plusieurs millions d'objets pour des configurations volumineuses.

Dans les premiers documents Microsoft mentionnant son existence, Active Directory s'est d'abord appelé NTDS (pour NT Directory Services, soit « Services d'annuaire de NT » en français). On peut d'ailleurs encore trouver ce nom dans la littérature couvrant le sujet ainsi que dans certains utilitaires AD comme NTDSUTIL.EXE par exemple, ou le nom du fichier de base de données NTDS.DIT.

Le protocole principal d'accès aux annuaires est LDAP qui permet d'ajouter, de modifier et de supprimer des données enregistrées dans Active Directory, et qui permet en outre de rechercher et de récupérer ces données. N'importe quelle application cliente conforme à LDAP peut être utilisée pour parcourir et interroger Active Directory ou pour y ajouter, y modifier ou y supprimer des données. Il utilise également DNS, LDAP, Kerberos V, SNTP, SMB/CIFS, MSRPC.

Les GPO

Les stratégies de groupe (ou GPO pour Group Policy Object) sont des fonctions de gestion centralisée de la famille Microsoft Windows. Elles permettent la gestion des ordinateurs et des utilisateurs dans un environnement Active Directory. Les stratégies de groupe font partie de la famille des technologies IntelliMirror, qui incluent la gestion des ordinateurs déconnectés, la gestion des utilisateurs itinérants ou la gestion de la redirection des dossiers ainsi que la gestion des fichiers en mode déconnecté.

Bien que les stratégies de groupe soient régulièrement utilisées dans les entreprises, elles sont également utilisées dans les écoles ou dans les petites organisations pour restreindre les actions et les risques potentiels comme le verrouillage du panneau de configuration, la restriction de l’accès à certains dossiers, la désactivation de l’utilisation de certains exécutables, etc.

Les stratégies de groupe peuvent contrôler des clés de registre, la sécurité NTFS, la politique de sécurité et d’audit, l’installation de logiciel, les scripts de connexion et de déconnexion, la redirection des dossiers, et les paramètres d’Internet Explorer. Les paramétrages sont stockés dans les stratégies de groupe. Chaque stratégie de groupe possède un identifiant unique appelé GUID (« Globally Unique Identifier »). Chaque stratégie de groupe peut être liée à un ou plusieurs domaines, site ou unité d’organisation Active Directory. Cela permet à plusieurs objets ordinateurs ou utilisateurs d’être contrôlés par une seule stratégie de groupe et donc de diminuer le coût d’administration globale de ces éléments.

Les stratégies de groupe utilisent des fichiers de modèle d’administration avec les extensions .ADM ou .ADMX qui décrivent les clés de registre modifiées par l’application des stratégies de groupe. Sur un ordinateur de travail, les modèles d’administration sont stockés dans le répertoire %WinDir%\Inf, alors que sur un contrôleur de domaine Active Directory, pour chaque domaine et pour chaque stratégie de groupe, ils sont stockés dans un répertoire individuel (Le « group policy template », ou GPT) au sein du répertoire Sysvol. Les fichiers .ADMX sont des fichiers basés sur le format XML et introduits par Windows Vista pour la gestion des stratégies de groupe.

Les stratégies de groupe sont analysées et appliquées au démarrage de l’ordinateur et pendant l’ouverture de session de l’utilisateur. Les ordinateurs rafraîchissent les paramètres transmis par les stratégies de groupe de façon périodique, généralement toutes les 60 ou 120

Lien utile <http://www.it-connect.fr/gpo-definir-un-utilisateur-administrateur-local-de-tous-les-pcs/>

Pour Screenshot d’utilisation

# Histoire des stratégies de groupe (GPO) dans Windows

* + - GPO signifie Group Policy Object soit stratégie de groupe.
    - Les GPO sont apparues avec Windows 2000 Server et AD 2000.
    - Les concepts abordés dans ce cours s’appliquent à toutes les versions d’Active Directory.
    - Les GPO remplacent les stratégies de sécurité que l’on trouvait dans Windows NT4.
    - Elles ont été considérablement enrichies depuis en terme de paramètres configurables et d’ergonomie des outils de gestion, d’édition et de maintenance.

# Avantages des stratégies de groupe (GPO)

* + - Les GPO permettent la configuration automatisée et centralisée des postes de travail et des serveurs Windows de votre environnement.
    - Les GPO et leurs paramètres étant stockés dans AD et le dossier SYSVOL, la configuration des postes n’est plus stockée localement. Il suffit d’appliquer une GPO existante à un nouveau poste, et la configuration s’applique.
    - Les configurations étant appliquées à des clés de registre particulières (clés « policies »), la suppression d’une GPO restaure les paramètres locaux appliqués avant les GPO.
    - Il est en théorie possible de configurer n’importe quel paramètre par GPO.
    - La configuration des postes est uniforme. De plus les GPO sont réappliquées à intervalle régulier.

# Limites des stratégies de groupe (GPO)

* + - La gestion des GPO n’est pas chose aisée. Il faut être sûr d’appliquer la ou les bonnes GPO aux bons ordinateurs et/ou utilisateurs. Beaucoup d’administrateurs sont confrontés à ce problème lorsqu’ils mettent en œuvre les GPO.
    - La suite de ce cours explique les règles d’applications des GPO qui vous donneront tous les éléments à connaître afin de maîtriser la gestion (et donc l’application) des GPO.
    - Un autre inconvénient des GPO est que si dans votre environnement, chaque poste ou chaque utilisateur nécessite une configuration particulière, les GPO ne sont plus réellement efficaces.

# Définition des stratégies de groupe (GPO)

* + - GPO signifie Group Policy Object.
    - Une GPO est un objet Active Directory, au même titre qu’un utilisateur, un ordinateur, ou une unité d’organisation.
    - Une GPO contient un ensemble de paramètres applicables à un utilisateur ou un ordinateur. Par exemple la désactivation du pare-feu ou la configuration d’Internet Explorer.
    - Les méta-informations des GPO sont stockées et répliquées via Active Directory. Les méta-informations sont entre autre le créateur de la GPO, les dates et heures des modifications, les autorisations NTFS, etc…
    - Les GPO elles-mêmes (qui ne sont que des dossiers et des fichiers), sont stockées et répliquées dans le dossier SYSVOL. Ces fichiers sont des fichiers .pol appliquant les modèles d’administration, ainsi que les fichiers de script, etc…
    - Pour rappel, le dossier SYSVOL est un dossier partagé entre les contrôleurs de domaine et avec les clients du domaine qui permet la réplication des fichiers nécessaires à Active Directory. Active Directory est un annuaire et ne peut pas stocker des fichiers et dossiers. Il se sert donc du dossier SYSVOL pour échanger les fichiers ne pouvant pas être stockés dans Active Directoy.
    - Les GPO sont liées à des objets Active Directory. Cette liaison détermine à quels utilisateurs ou ordinateurs les paramètres seront appliqués.Les seuls objets auxquels vous pouvez lier une GPO sont des Domaines, des Sites et des Unités d’organisation (OU).

Les stratégie de groupe dans un domain Microsoft Active Directory

La stratégie de GPO repose sur 2 termes : Centralisation et Configuration

**Centralisation**

Active Directory centralise deux grandes classes de paramètres :

* Les paramètres liés aux utilisateurs ( s’appliqunt aux utilisateurs dits « authentifiés » et prenant effet lors de l’ouverture de session
* Les paramètres liés aux ordinateurs ( s’appliquent aux ordinateurs enregistrés dans l’AD et s’appliquant lors du démarrage et du cycle de rafraichissement)

AD centralise une multitude de paramètres influant diectement sur ces deux catégories, faisant ainsi gagner aux administrateurs un temps précieux

**Configuration**

Prise en charge presque totale des mouvements de configurations. Les stratégies de groupe sont liées à la technoogie IntelliMirror qui leur fournit un certain nombre de fonctionnalités telle que :

* Fonctionnalités de configuration
* Fonctionnalités de modification
* Fonctionnalités liées aux comptes d’utilisateurs itinérants
* Fonctionnalités de disponibilités des données
* Fonctionnalités de disponibilité des logiciels

Une stratégie de groupe est un objet en tant que tel s’appliquant sur les deux catégories ci-dessus, les utilisateurs et les ordinateurs. Pour gérer ces stratégie, on utilise un outil nommés GPMC, *Group Policy Management Console.*

**1. Qu'est-ce qu'une stratégie de groupe ?**

1.1. Présentation des stratégies de groupe

Le terme Stratégie désigne la configuration logicielle du système par rapport aux utilisateurs. A la suite d’une installation de Windows, aucune stratégie n'est configurée, et tout est permis (en fonction des droits des groupes d'utilisateurs prédéfinis : Administrateurs, Utilisateurs, Utilisateurs avec pouvoir...).

Les stratégies de groupe ou GPO (Group Policies Object) permettent de configurer des restrictions d'utilisation de Windows où des paramètres à appliquer soit sur un ordinateur donné soit sur un compte utilisateur donné. Il est ainsi possible d’agir sur :

• La définition d’un environnement adapté : Il est possible par exemple de rediriger certains répertoires leurs contenus

• Le déploiement de logiciels : **Une automatisation complète de l’installation des programmes sur les postes clients est possible en fonction du profil de l’utilisateur**

• L’application des paramètres de sécurité : Le contexte de sécurité de l’environnement utilisateur peut être modifier

Voici un exemple de stratégie de groupe :

• Menu Démarrer et Barre des tâches

1. Suppression du menu Documents dans le menu Démarrer

2. Suppression des Connexions réseau et accès distant du menu Démarrer

3. Suppression du menu Exécuter dans le menu Démarrer

4. Désactivation de la fermeture de session dans le menu Démarrer

5. Désactivation de la commande Arrêter

• Panneau de configuration

1. Désactivation du Panneau de configuration

2. Masque de certaines applications du Panneau de configuration

• Système

1. Activation des quotas de disque

2. Désactivation des outils de modifications du Registre

3. Désactivation de l'invite de commandes

• Internet Explorer

1. Désactivation de la modification des paramètres de la page de démarrage

1.2. Scripting

**Les GPO permettent en outre de spécifier des scripts de démarrage** (que l’ordinateur exécutera au lancement de Windows avant qu’un utilisateur ne se soit loguer), ainsi que des **scripts d’ouverture de session** (exécutés quand un utilisateur se logue). Grâce aux scripts d’ouverture de session il est possible notamment de créer des lecteurs réseau (c’est à dire une lettre de lecteur que l’on associe en réalité à un partage réseau) selon les groupes et les utilisateurs.

Les scripts de démarrage s’exécutent en mode synchrone ( les uns après les autres sans que le login ne soit possible avant la fin de leur exécution) et de façon invisible. D’un autre côté, les scripts d’ouverture de session s’exécutent en mode asynchrone (tous en même temps au moment du login) mais restent eux aussi invisibles.

Les scripts peuvent être placés sur n’importe quel DC (contrôleur de domaine) du domaine ( et ce grâce au phénomène de réplication), dans le sous répertoire du domaine destiné aux scripts et qui se situe dans le partage SYSVOL.

Voici un exemple de script :

Set objNetwork = Wscript.CreateObject(«WScript.Network») objNetwork.MapNetworkDrive«G:», «\\NomOrdinateur\NomOrdinateur Data» msgbox «Votre script a fonctionné ! »

1.3. Création d'une GPO à l'aide de la console gpedit.msc

La console gpedit.msc permet de créer des stratégies de groupe, son nom de fichier est : %systemroot%\system32\gpedit.msc. Celle-ci récupère ses informations à différents niveaux : dans les fichiers dont l’extension est .adm, dans la base de registre et dans deux fichiers nommés registry.pol. L’ensemble de ces éléments seront détaillés dans la suite de notre étude.

Voici un diagramme qui détaille le fonctionnement de gpedit.msc :

1.4. Installation de la console de gestion des stratégies de groupe

La console de gestion des stratégies de groupe (GPMC, Group Policy Management Console) Microsoft permet l’uniformisation de la gestion des stratégies de groupe au sein d’une organisation. Avant que celle-ci ne fasse son apparition, il était nécessaire d’utiliser plusieurs outils Microsoft pour gérer les stratégies de groupe. La console GPMC réunit désormais dans une seule console toutes les fonctionnalités nécessaires.

Grâce à la console GPMC, la gestion des stratégies de groupe est facilitée : comprendre, déployer, gérer et résoudre des problèmes liés aux implémentations de stratégie de groupe sont désormais des tâches qui ne posent pas de soucis. La GPMC permet par ailleurs d’automatiser des opérations de stratégie de groupe à l'aide de scripts.

La console GPMC contrôle les stratégies de groupe Windows 2000 et Windows Server 2003. Les fonctionnalités majeures proposées par la console GPMC sont :

• une interface graphique utilisateur qui facilite l’utilisation des GPO

• l'importation et l'exportation ainsi que le copier/coller des objets de stratégie de groupe

• le filtrage par le langage WMI (Windows Management Instrumentation)

• la sauvegarde et la restauration des objets de stratégie de groupe

• la présence d’un module de vérification des stratégies résultantes (RSoP, resultant set of policy)

• l'utilisation de scripts pour les tâches associées aux stratégies de groupe

• la génération de rapports

• la gestion simplifiée de la sécurité liée aux stratégies de groupe

Dans certains cas, il est nécessaire de modifier le fonctionnement des GPO, par exemple dans le cas où la machine est en accès libre. Le paramètre de GPO « Bouclage » permet à l’ordinateur de prendre lui-même en compte la partie Utilisateur de la GPO qu’il utilise, ces paramètres éliminent les paramètres de GPO normalement appliqués par le login de l’utilisateur. Ainsi un environnement utilisateur très limité par exemple pourra être défini quel que soir l’utilisateur logué.

1.7. Stockage des paramètres d'une GPO

Lorsqu’une GPO est définit, les paramétrages de cette dernière sont stockés dans la base de registre dans les branches suivantes :

• HKEY\_CURRENT\_USER\Software\Policies\Microsoft

• HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies

• HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft

• HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies