WILD CODE SCHOOL

Les GPO

Que peut-on gérer avec les GPO ?

Plan

1 - Définition

2 - Règles de priorité

WILD CODE SCHOOL

Définition

Une définition

Les **objets de stratégies de groupes**, ou **GPO** (*Group Policy Object*) sont des collections virtuelles de politiques de sécurité.

- Possède un nom unique (comme un GUID).
- Permettent de gérer avec une méthode centralisée un parc informatique :
  - Gestion des ordinateurs et des utilisateurs
  - Gestion des politiques de sécurité (restriction d'utilisation)
  - Gestion de l'interface graphique
  - Déploiement de logiciels, de script, de service
  - Gestion des scripts de connexion
  - Redirection de dossiers…

Objectifs

- Méthode de gestion de configuration de parc informatique
- Permettent de définir une configuration cible de sécurité et d'installation

OS pris en compte

Les GPO sont fonctionnelles sur les ordinateurs ayant un OS Microsoft (client ou serveur).
Il existe des implémentations très partielles de clients GPO pour les environnements Linux. Mais :

- La plupart des modèles de GPO qui sont proposés dans la console de Gestion des Stratégies de Groupe ne seront pas pris en compte par les client GPO Linux.
- Si l'on affecte une GPO à un client qui ne peut pas l'interpréter, la GPO sera alors ignorée.

Constitution d'une GPO

Une GPO est constituée de trois composantes :

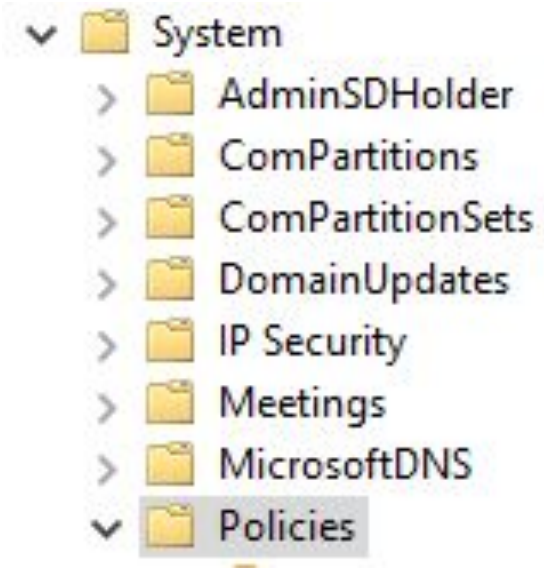
1. Une entrée LDAP
2. Le contenu de la GPO
3. Un attribut gPLink

L'entrée LDAP

L'entrée LDAP GPO est situé sous CN=Policies,CN=System,DC=xx,DC=xx dans la partition principale de l'AD.
Elle contient :

- Le nom
- le GUID
- Les droits d'édition de la GPO (potentielle délégation de droits)

-> Ce sont les informations administratives



Contenu d'une GPO

Le contenu de la GPO se trouve sur le serveur AD dans le partage SYSVOL.
Il contient dans un répertoire, dont le nom est le GUID, plusieurs fichiers d'instructions.
-> Les actions de la GPO.

Attribut gPlink

Cet attribut est affecté à une OU ou à un site AD.
Il rassemble plusieurs informations :

- L'identifiant de la GPO, le GUID
- Le chemin LDAP de la GPO
- L'ordre de traitement
- L'application ou non

Etat

En plus des caractéristiques d'une GPO vus précédemment, 2 types d'états existent :

- Forcée (*Enforced*) avec 2 possibilitées: oui ou non
- Active (*Enable*), qui peut avoir également l'état désactivée (*Disable*)

Etat forcé

Lorsqu'une GPO est "enforced", elle a la priorité sur les GPO appliquées à des niveaux inférieurs dans la hiérarchie AD.
ex.: une GPO appliquée à un domaine aura la priorité sur une GPO appliquée à une OU au sein de ce domaine.

Une GPO enforced :

- Ignore le blocage d'héritage
- Doit être utilisée très rarement
- Est typiquement réservée au Tier 0

État active

L'état "enabled" ou "disabled" d'une GPO détermine si elle est active ou non.

Link enabled vs GPO status enable ?

Link Enabled :
Cette option détermine si le lien entre une GPO et une OU est actif.
Si "Link Enabled" est désactivé -> la GPO ne s'appliquera pas aux objets dans cette OU, même si la GPO elle-même est activée (Enabled).
=> "Link Enabled" contrôle si le lien entre la GPO et l'OU est actif ou non.

GPO Status Enabled :
Etat de la GPO elle-même. Si elle est désactivée (Disabled), elle ne s'appliquera à aucun objet, indépendamment de l'état de ses liens.
Une GPO doit être activée (Enabled) pour qu'elle puisse s'appliquer.

WILD CODE SCHOOL

Règles de priorité

Stratégies locales

Les stratégies locales, sont un ensemble de configurations de sécurité et de gestion appliquées directement à un ordinateur individuel, sur les OS Microsoft. Elles sont définies localement sur chaque machine et ne dépendent pas d'une gestion centralisée par AD.

Stratégies locales vs GPO

Stratégies locales :

- Spécifique à chaque ordinateur individuel
- En workgroup (sans domaine) et en domaine
- Console locale **gpedit.msc**

GPO :

- Centralisées via l'AD
- Uniquement en domaine
- Console serveur **gpmc**
- Priorité sur les stratégies locales

Priorité des GPO sur l'AD

Lorsqu'un ordinateur dans un domaine AD démarre ou lorsqu'un utilisateur se connecte, les politiques sont appliquées dans l'ordre suivant :

- Local : D'abord, les stratégies locales sont appliquées.
- Site : Ensuite, les GPO associées au site AD sont appliquées.
- Domaine : Les GPO de niveau domaine sont appliquées après celles du site.
- OU: Les GPO des OU sont appliquées, en commençant par l'OU parent la plus élevée et en descendant jusqu'à l'OU la plus spécifique.

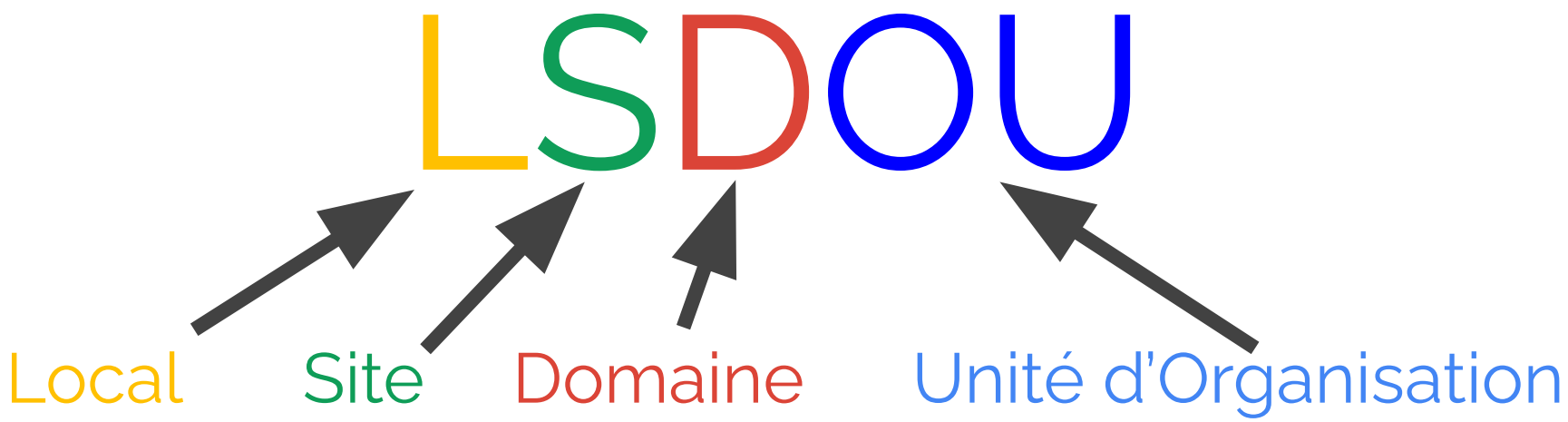
=> concept **d'héritage**

Détail sur l'héritage

Blocage d'héritage :
Les OU peuvent être configurées pour bloquer l'héritage des GPO des niveaux supérieurs.

Configuration **GPO Enforced** :
Une GPO marquée comme "Enforced" écrasera les politiques des niveaux inférieurs, même si l'héritage est bloqué.

Priorité des GPO sur l'AD



Fonctionnement sur une OU

Ordre déterminé :
On peut spécifier manuellement un ordre de priorité.

LIFO (*Last In, First Out*) :
La dernière GPO liée est traitée en premier.
Si 2 GPO ont des paramètres qui se chevauchent, le paramètre de la dernière GPO traitée prévaudra.

Filtrage et Sécurité :
Les paramètres de sécurité et le filtrage (sécurité ou WMI) influence l'application d'une GPO.

Filtrage de sécurité

Une GPO ne s'applique que si :

- Elle est liée à un site / domaine / OU
- ET l'objet AD possède le droit :
  - Read
  - Apply Group Policy

Ces droits sont gérés via le filtrage de sécurité.

Un groupe de filtrage particulier

Le groupe Authenticated Users a le droit Apply Group Policy => Tous les utilisateurs et tous les ordinateurs authentifiés reçoivent la GPO.

Pour restreindre une GPO :

- Retirer l'application du groupe Authenticated Users
- Ajouter un groupe de sécurité AD (Utilisateur ou Ordinateur)
- Lui donner le droit Lecture + Apply Group Policy

Bonnes pratiques

- Ne pas modifier les GPO de domaine par défaut (default domain policy)
- Se baser sur une hiérarchie d'OU
- Avoir une nomenclature descriptive
- Ne pas utiliser les dossiers de base « users » et « computers »
- Supprimer un lien de GPO au lieu de le désactiver
- Ne pas bloquer l'héritage
- Utiliser de petite GPO
- Utiliser les gestion avancées de mot de passe
- Désactiver les configurations « ordinateurs » ou « utilisateurs » inutilisées

Conclusion

Composants d'une GPO :

- Entrée LDAP
- Contenu de la GPO
- Attribut gPLink

Priorité LSDOU

Bonnes pratiques