Stratégies de groupes

Objectifs

- Utiliser et planifier les stratégies de groupe

Configuration initiale

Ce TD est à réaliser avec une station de travail windows 2000 pro et un serveur windows 2000 server. La station de travail sera appelée **station1**. Le serveur sera appelé **serveur1**. Le serveur sera contrôleur de domaine et la station sera dans le domaine.

Prérequis

- Administration d'active directory
- concepts sur les stratégies de groupe

Exercice 1: Stratégie locale de sécurité

1. Sur station 1, créez un utilisateur testloc (mot de passe: password).
2. Sur serveur1, créez un utilisateur test (mot de passe password)
3. Sur station1, utilisez l'outil « stratégie locale de sécurité » pour autoriser les utilisateurs testloc et test à modifier l'heure de la station de travail.
4. Tentez d'ouvrir une session sur le contrôleur de domaine en tant qu'utilisateur test. Que se passe-t-il ?

L'authentification réussit, le mot de passe est reconnu et accepté mais l'ouverture de la session est refusée parce que la stratégie locale de sécurité l'interdit.

5. Ouvrez une session en tant qu'administrateur et trouverez dans la stratégie de sécurité du contrôleur de domaine la liste des utilisateurs ou groupes autorisés à ouvrir une session sur le contrôleur de domaine. Ajoutez-y l'utilisateur test.

Attention: il s'agit de la stratégie de sécurité du contrôleur de domaine et pas de la stratégie de sécurité du domaine. Un administrateur compétent aurait créé un groupe LocalSession, aurait ajouté le groupe LocalSession aux utilisateurs pouvant ouvrir une session et aurait ensuite mis test dans LocalSession. C'est un principe de base de l'administration système windows 2000: on donne les permissions, les droits à des groupes et on gère qui a ces permissions et ces droits en ajoutant ou en otant les utilisateurs de ces groupes.

6. Tentez d'ouvrir une session en tant qu'utilisateur test sur le contrôleur de domaine. Que se passe-t-il ? Pourquoi ?

L'ouverture de session est refusée. C'est du au fait que les stratégies de groupe mettent un certain temps à se diffuser (#5 mn pour un contrôleur de domaine, #1h30 pour un ordinateur membre).

7. Forcez la propagation des stratégies de groupes à l'aide de la commande « secedit / refreshpolicy machine_policy ». Si l'aide en ligne apparaît, c'est que vous avez fait une faute de frappe.

Si la mise à jour concerne une stratégie machine, on utilise la commande indiquée. Pour une stratégie utilisateur, on utilise « secedit /refreshpolicy user_policy »

Auteur: P. Petit	*Titre: TD stratégies de groupes*	*Version: 1.0*
Date: 29/02/2004	Licence: Gnu Free Documentation Licence	Durée: 60 mn

Exercice 2: Stratégie de groupe dans active directory

1. Créez une unité d'organisation nommée **Departement**. Dans cette unité, créez des utilisateurs ens1, ens2, ..., ens5. Créez un utilisateur ensAdmin dans le conteneur Users.
2. On souhaite supprimer le menu exécuter à tous les utilisateurs de l'unité d'organisation Departement. Créez une stratégie de groupe implantant cette limitation (Propriétés de Departement/Stratégie de groupes).

Si la stratégie n'existe pas ailleurs, la création se fait en deux étapes: on clique sur nouveau pour la créer puis sur modifier pour placer les paramètres (« pas de menu exécuter » dans notre cas).

3. Vérifier en ouvrant une session sur la station de travail que cette modification s'applique bien à ens1, ... mais pas à ensadmin. Expliquez pourquoi.

Même problème depropagation des stratégies qu'à l'exercice précédent. Utilisez secedit pour forcer la propagation.

4. On souhaite appliquer un strategie de groupes aux utilisateurs du conteneur Users mais pas à ceux de l'unité d'organisation Departement. Est-ce possible ? Comment faire pour appliquer une strategie de groupe à tous les utilisateurs de Users, de département, ... ?

Users n'est pas une unité d'organisation, c'est un simple conteneur. Il n'est pas possible de définir de stratégie de groupe sur Users. Par contre, on peut définir une stratégie de groupe sur le domaine complet mais elle s'appliquera aussi à Departement. Il n'est donc pas possible de définir une stratégie de groupe qui ne s'applique qu'à Users. On peut par contre créer une stratégie de groupe au niveau du domaine. Elle s'appliquera à tous les utilisateurs du domaine mais les paramètres définis par les stratégies des unités d'organisation du domaine sera prioritaires sur elle. Cf ordre d'application des stratégies dans le cours.

5. On souhaite que tous les utilisateurs du domaine n'appartenant pas à l'unité d'organisation Departement n'aient pas d'item Exécuter dans leur menu démarrer. Comment procéder ? Mettez le en application.

On définit une stratégie de groupe au niveau du domaine qui enlève l'item Exécuter du menu Démarrer de tous les utilisateus du domaine. On définit une stratégie de groupe sur Departement qui impose l'item exécuter dans le menu Démarrer des utilisateurs de Departement.

Exercice 3: Délégation de l'administration d'une stratégie de groupes

1. Consultez les ACL des objets de stratégie de groupe (Departement/propriété/stratégie de groupe/propriété) et indiquer à qui s'applique la stratégie de groupe, qui a le droit de la modifier et qui a le droit d'en créer d'autres.
2. Faites en sorte que l'utilisateur ensadmin puissse modifier la strategie mais pas en créer d'autres. Ouvrez une session en tant qu'ensadmin pour le vérifier. Comment sont les boutons « Nouveau » ?

Le bouton nouveau es grisé puisque l'utilisateur ensAdmin n'a pas le droit de créer de nouvelles stratégies.

3. Faites en sorte que l'utilisateur ensadmin puisse créer des stratégies de groupes et les associer à l'unité Departement sans avoir le droit de le faire ailleurs (pour le domaine ou pour d'autres unités)

Il suffit de lui donner le droit ad hoc dans les ACL.

4. La stratégie de groupe liée à Departement s'applique-t-elle a ensadmin ?

Non car ensAdmin n'appartient pas à Departement. Une stratégie de groupe s'applique aux objets des conteneurs auxquels elle est liée. Dans le cas présent, la stratégie s'applique aux compes utilisateurs présents dans Departement.

Exercice 4: Suppression d'une stratégie de groupes

1. Supprimer l'une des stratégies de groupe de Departement. On vous propose deux choix : « supprimer la liaison » ou « supprimer la liaison et la strategie ». Expliquer les conséquences de chacun de ces choix.

On peut supprimer le lien seul ou supprimer le lien et l'objet GPO. Si on supprime le lien, l'objet GPO peut être lié à d'autres unités d'organisation. Si on supprime le lien et l'objet GPO, ce dernier est complètement détruit et ne peut plus être utilisé (lié) à d'autres unités d'organisation.

Exercice 5: Planification des stratégies de groupes

1. Proposer et implantez les unités d'organisations, les strategies de groupe, ... permettant de répondre au cahier des charges suivant:
   - les utilisateurs du domaine sont soit des membres du personnel ou des étudiants
   - les membres du personnel sont soit des enseignants, soit des personnels administratifs
   - les étudiants sont soit des étudiants de Miage, soit des étudiants d'ASR
   - les étudiants ne doivent pas pouvoir changer leur mot de passe
   - les utilisateurs ont tous le château de chambord en fond d'écran
   - les étudiants de miage ne doivent pas avoir de menu permettant de connecter ou de déconnecter un lecteur réseau
   - Les étudiants de miage ont un paysage d'automne en fond d'écran. Les étudiants d'ASR ont une colline herbeuse comme fond d'écran
   - une sercrétaire (sec1) peut réinitialiser les mots de passe des étudiants
   - un enseignant (ens1) peut gérer les comptes des étudiants (et notamment en créer) Il peut aussi appliquer des stratégies de groupe aux étudiants.

On est obligé de créer des unités d'organisation pour regrouper des comptes (utilisateurs ou ordinateurs) auxquels on veut appliquer un traîtement commun : soit des paramètres via les stratégies de groupe, soit déléguer des tâches administratives sur ces comptes via la délégation de contrôle.

Du cahier des charges, on déduit que les comptes des enseignants et des personnes administratifs ont les mêmes particularités et contraintes. On ne les séparera donc pas dans des unités d'organisation distinctes.

Auteur: P. Petit	*Titre: TD stratégies de groupes*	*Version: 1.0*
Date: 29/02/2004	Licence: Gnu Free Documentation Licence	Durée: 60 mn

Les étudiants sont par contre répartis en deux groupes qui ont des particularités propres. Nous allons donc adopter l'organisation suivante:

- **une unité d'organisation Departement**
- **dans Departement, deux unités d'organisation: Personnel et Etudiants**
- **dans Etudiants, deux unités d'organisation : Miage ASR.**
- **Une stratégie de groupe sur Departement qui impose le fond d'écran Chambord**
- **Une stratégie de groupe sur Etudiants qui empêche le changement de mot de passe**
- **Une stratégie de groupe sur ASR qui impose le fond d'écran herbeux (qui vaut mieux qu'un fond d'écran barbu à la « big brother is watching you »)**
- **une strategie de groupe sur Miage qui impose le fond d'écran d'automne**
- **une strategie de groupe sur Miage qui supprimer les items permettant de connecter/déconnecter des lecteurs réseau. On aurait pu regrouper les deux propriétés (fond d'écran et connecter) dans une seule stratégie mais il est considérer comme une bonne pratique d'avoir des stratégies clairement identifiables jouant des rôles clairs et cohérent avec des noms parlants. Cela facilite leur réutilisation.**
- **On créera un groupe initMDPEtu et on utilisera la délégation de contrôle sur Etudiants pour donner le droit de réinitialiser les mots de passe à initMDPEtu. On ajoutera sec1 à initMDPEtu.**
- **On créera un groupe gestionCompteEtu et on utilisera la délégation de contrôle sur Etudiants pour donner le droit de gérer les comptes à gestionCompteEtu. On ajoutera ens1 à initMDPEtu.**