Auteur: P. Petit	*Titre: TD Administration Active Directory*	*Version: 1.0*
Date: 29/02/2004	Licence: Gnu Free Documentation Licence	Durée: 1h00

Administration d'Active Directory

Objectifs

- ràf

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 de travail sera dans le domaine.

Prérequis

ràf

Exercice 1: Création d'unité d'organisation

1. Il est possible de créer des unités d'organisation dans le domaine ou dans d'autres unités d'organisations. Créez une unité d'organisation **Promo** dans le domaine. Vérifiez qu'il n'est pas possible de créer une unité d'organisation dans le conteneur **Users**.
2. Créez des utilisateurs etu1, etu2, ..., eut5 dans Promo
3. Créez un utilisateur etu6 dans **Users** et déplacez le dans **Promo**.

Exercice 2: Délégation de contrôle

1. Nous souhaitons que l'utilisateur etu1 puisse réinitialiser le mot de passe des autres étudiants de l'unité d'organisation **Promo**. Pour cela, vous allez utiliser la délégation de contrôle. Rappelez les 3 paramètres d'une délégation de contrôle puis appliquer la.

Une délégation de contrôle :

- **délégue certaines tâches**
- **à certains utilisateurs**
- **sur les membres d'une unité d'organisation**

Une bonne pratique consiste à donner les droits à un groupe et à ajouter ou retirer les utilisateurs à ces groupes. Dans le cas présent, il faut créer un groupe initMDPEtu et lui déléguer la possibilité de réinitialiser les mots de passe de l'unité Promo. On ajoute ensuite ens1 à ce groupe.

2. Suite à des abus, etu1 perd sa délégation de contrôle. Ce rôle est maintenant dévolu à etu2. Expliquez ce que vous devez faire pour appliquer cette modification.

On ôte ens1 du groupe initMDPEtu et on y ajoute ens2.

Exercice 3: installation des consoles MMC sur une station de travail

1. Nous souhaitons que l'utilisateur auquel on a délégué l'administration puisse travailler depuis sa station de travail et non pas directement sur le serveur. Vérifiez que le jeu de consoles MMC d'une station de travail ne contient pas les consoles de gestion d'Active Directory.

Auteur: P. Petit	*Titre: TD Administration Active Directory*	*Version: 1.0*
Date: 29/02/2004	Licence: Gnu Free Documentation Licence	Durée: 1h00

2. Installer l'adminpak présent sur le CD d'installation de windows 2000 server et vérifier que les consoles de gestion d'active directory sont maintenant disponibles.

Exercice 4: Création d'un console de gestion personnalisée

1. Nous allons créer une console de gestion personnalisée permettant de gérer les mots de passe de l'unité d'organisation. Exécutez la commande **mmc.exe**.
2. Ajoutez ensuite le composant logiciel enfichable « utilisateurs et ordinateurs Active directory »
3. développez l'arborescence du domaine et cliquez sur **Promo** puis sur « nouvelle fenêtre à partir d'ici ». Fermez ensuite la fenêtre racine de façon à ne conserver que la nouvelle fenêtre.
4. Dans les options, changez le nom de la console en **Promo** et passez la console en mode utilisateur, accès limité, fenêtre unique. Refusez l'enregistrement des modifications.
5. Sauvez la console de façon à ce qu'elle apparaissent dans le menu « outils d'administration » de tous les utilisateurs.
6. Testez ensuite votre console en ouvrant une session en tant qu'utilisateur ayant le droit de réinitialiser les mots de passe des utilisateurs de **Promo**.

Exercice 5: Etude des autorisations Active Directory

1. Par défaut, le menu propriétés des unités d'organisations est en mode simplifié. Pour faire apparaître les onglets manquants, sélectionner le mode d'affichage avancé dans le menu affichage.
2. L'onglet sécurité des propriétés des unités d'organisations indique les droits qu'ont les utilisateurs sur l'unité. Consultez les ACL de l'unité d'organisation Departement.
3. L'utilisateur ayant le droit de réinitialiser les mots de passe apparaît mais son ACE est vide. Pourquoi ?

Il faut cliquer sur « Avancé » pour voir le détail des autorisations qu'à l'utilisateur.

Exercice 6: Audit

Exercice 7: Groupes locaux de domaine

1. A l'intérieur d'un domaine windows 2000, les groupes locaux de domaines sont très polyvalents: on les gère sur le contrôleur de domaine et ils sont utilisable sur tous les ordinateurs du domaine. Dans un domaine en mode mixte, il n'en est pas de même : lesgroupes locaux de domaine ne sont utilisables que sur les contrôleurs de domaine. Vérifiez que votre domaine est en mode natif en consultant les propriétés du domaine dans « utilisateurs et ordinateurs active directory ».
2. Créez les utilisateurs ad1, ad2, ad3 et ad4 sur le domaine.
3. On souhaite que certains utilisateurs du domaine (ad1, ad2 et ad3) soient administrateurs des stations de travail du domaine. Pour cela, créez un groupe local de domaine nommé SECURITE et incluez-y ad1, ad2 et ad3.

Le groupe est créé dans le domaine en utilisant la MMC « utilisateurs et ordinateurs Active

Directory ».

4. Sur les stations de travail, incluez le groupe MAIN dans le groupe des administrateurs de la station de travail.
5. Ouvrez une session sur la station de travail en tant qu'ad1, ad2 ou ad3 pour vérifier qu'ils ont bien les droits d'administration sur la station.

La création d'un nouveau compte utilisateur sur la station de travail est une bonne vérification.

6. Nous souhaitons retirer ce droit à ad3 et le donner à ad4. Comment doit-on procéder ?

On ôte ad3 du groupe MAINT et on y ajoute ad4. Cette action a été faite depuis le domaine sans intervention sur les stations de travail du domaine.

7. Citez d'autres façon de donner les droits d'administration sur les stations de travail et comparez les à celle que nous avons appliqué.

On peut inclure les utilisateurs directement dans le groupe des administrateurs des stations mais toute modification doit se faire sur les stations ce qui n'est pas vialbe si on gère un parc important.