Installation et configuration d'Active Directory (AD)

Introduction

Active Directory (AD) est un service d'annuaire développé par Microsoft qui permet de gérer les utilisateurs, les ordinateurs et les ressources d'un réseau. Il est utilisé pour centraliser la gestion des droits d'accès, la sécurité et les politiques de groupe dans un environnement Windows. Ce TP consiste à installer Active Directory sur un Windows Server, à créer des utilisateurs et des groupes, et à tester la gestion des politiques.

Objectifs

1. Installer Active Directory sur un serveur Windows Server.
2. Configurer un domaine et un contrôleur de domaine.
3. Créer des utilisateurs et des groupes dans Active Directory.
4. Tester les fonctionnalités de Group Policy (stratégies de groupe).

Étapes réalisées

1. Installation d'Active Directory sur Windows Server :

1. **Installation du rôle "Active Directory Domain Services" (AD DS) :**
    - Ouvrez Server Manager et cliquez sur Add roles and features.
    - Sélectionnez Active Directory Domain Services dans la liste des rôles et cliquez sur Next.
    - Cliquez sur Install pour installer le rôle Active Directory Domain Services sur votre serveur.
2. **Promotion du serveur en contrôleur de domaine :**
    - Après l'installation, une notification apparaîtra dans Server Manager. Cliquez sur Promote this server to a domain controller.
    - Dans l'assistant Active Directory Domain Services Configuration, sélectionnez Add a new forest et entrez un nom de domaine, par exemple monentreprise.local.
    - Configurez les options DNS et le mot de passe pour le Mode de restauration des services d'annuaire (DSRM).
    - Cliquez sur Next et Install. Le serveur redémarrera automatiquement.

2. Configuration du domaine et du contrôleur de domaine :

1. **Vérification de la promotion du contrôleur de domaine :**

- Après le redémarrage du serveur, connectez-vous avec les identifiants du domaine Administrator.
- Ouvrez Active Directory Users and Computers pour vérifier que le domaine monentreprise.local a bien été créé.

2. **Vérification du service DNS :**
   - Active Directory utilise le service DNS pour localiser les contrôleurs de domaine. Vérifiez que le service DNS est bien configuré et fonctionne en exécutant la commande suivante :
   - nslookup monentreprise.local

3. Création d'utilisateurs et de groupes dans Active Directory :

1. **Création d'un utilisateur :**
   - Dans Active Directory Users and Computers, faites un clic droit sur le domaine monentreprise.local, puis cliquez sur New > User.
   - Entrez le prénom, le nom, le nom d'utilisateur et définissez un mot de passe pour l'utilisateur.
2. **Création d'un groupe :**
   - Dans Active Directory Users and Computers, faites un clic droit sur le domaine monentreprise.local, puis cliquez sur New > Group.
   - Donnez un nom au groupe, par exemple Administrateurs et définissez le type de groupe (groupe global ou local).
3. **Ajout d'un utilisateur à un groupe :**
   - Cliquez sur le groupe Administrateurs, puis sur l'onglet Members.
   - Cliquez sur Add, tapez le nom de l'utilisateur que vous souhaitez ajouter au groupe, puis cliquez sur OK.

4. Configuration des stratégies de groupe (Group Policy) :

1. **Accès à la gestion des stratégies de groupe :**
   - Ouvrez Group Policy Management depuis Server Manager.
   - Créez une nouvelle GPO (Group Policy Object) en cliquant sur Group Policy Objects et sélectionnez New.
   - Donnez un nom à la GPO, par exemple Paramètres de sécurité.
2. **Modification de la GPO pour appliquer des stratégies :**

- Clic droit sur la GPO Paramètres de sécurité et cliquez sur Edit.
- Dans l'éditeur Group Policy Management Editor, vous pouvez configurer différentes politiques, par exemple, imposer un mot de passe complexe ou interdire la connexion de certains utilisateurs.
    - Pour configurer la complexité du mot de passe, allez dans Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy.
    - Modifiez les paramètres selon vos besoins, par exemple Minimum password length à 8 caractères.

3. **Application de la GPO sur un ou plusieurs ordinateurs :**
    - Dans Group Policy Management, cliquez droit sur le domaine et sélectionnez Link an Existing GPO.
    - Sélectionnez la GPO créée (par exemple, Paramètres de sécurité) et liez-la à l'unité d'organisation (OU) souhaitée.

5. Vérification et tests :

1. **Vérification des utilisateurs et des groupes** :
    - Dans Active Directory Users and Computers, vérifiez que les utilisateurs et les groupes ont été créés correctement.
    - Testez la connexion avec un compte utilisateur en utilisant les identifiants définis précédemment.
2. **Vérification des stratégies de groupe** :
    - Sur un client Windows membre du domaine, ouvrez une fenêtre cmd et exécutez la commande suivante pour forcer la mise à jour des stratégies de groupe :
    - gpupdate /force
    - Vérifiez que les stratégies appliquées ont bien été prises en compte, par exemple, en vérifiant la complexité des mots de passe dans Panneau de configuration > Comptes d'utilisateurs > Modifier votre mot de passe.

Résultats obtenus

1. **Active Directory** a été installé et configuré sur le serveur avec succès.
2. Le domaine monentreprise.local a été créé et le serveur a été promu en contrôleur de domaine.

3. Les utilisateurs et groupes ont été créés avec succès dans Active Directory.
4. Les stratégies de groupe ont été configurées et appliquées pour renforcer la sécurité du domaine.

Conclusion

Ce TP m'a permis de comprendre le rôle et les fonctions d'Active Directory dans un environnement réseau. J'ai appris à installer et configurer Active Directory, à créer et gérer des utilisateurs et des groupes, et à appliquer des politiques de sécurité via Group Policy. Ces compétences sont essentielles pour gérer les utilisateurs et la sécurité d'une infrastructure informatique dans une organisation.