JOB 0 : Documentation

Luka FRANCOIS

Véronique ABELLA

Kaïs FRAOUCENE

Romain ABDOUH

SOMMAIRE

I/ Qu'est-ce qu' Active Directory ?

Active Directory (AD) est un s**ervice d'annuaire qui fonctionne sur Microsoft Windows Server**. Sa fonction principale consiste **à permettre aux administrateurs de gérer les permissions et de contrôler l'accès aux ressources du réseau**.

Dans Active Directory, les **données sont stockées sous forme d'objets (ex : OU ou Unité d'Organisation, Ordinateur, Utilisateurs, Groupe)**. Ceux-ci comprennent les utilisateurs, les groupes, les applications et les périphériques. Ils sont **classés en fonction de leur nom et de leurs attributs.**

L'Active Directory est aussi un **bon outil pour la gestion des parcs informatiques**. En effet, il permet, s'il est bien configuré, de **savoir dans quel service se situe une machine** par exemple.

II/ Les environnements possibles

Il est possible de créer **divers environnements** grâce à Active Directory :

1. **Environnement à un seul domaine Active Directory**

À l'aide d'un déploiement Active Directory unique, nous pouvons **synchroniser les utilisateurs et les groupes d'un seul domaine** Active Directory.

2. **Environnement Active Directory à domaines multiples, forêt unique**

À l'aide d'un déploiement à domaines multiples, forêt unique, nous pouvons **synchroniser des utilisateurs et des groupes à partir de multiples domaines Active Directory au sein d'une forêt unique**.

3. **Environnement Active Directory à forêts multiples avec relations d'approbation**

Dans un déploiement Active Directory à forêts multiples avec relations d'approbation, nous pouvons **synchroniser des utilisateurs et des groupes provenant de plusieurs domaines Active Directory dans des forêts où une relation d'approbation bidirectionnelle existe entre les domaines**.

4. **Environnement Active Directory à forêts multiples sans relations d'approbation**

Dans un déploiement Active Directory à forêts multiples sans relations d'approbation, nous pouvons **synchroniser des utilisateurs et des groupes provenant de plusieurs domaines Active Directory dans des forêts sans relation d'approbation entre les domaines**.

III/ Son fonctionnement

Voici une vue d'ensemble de son fonctionnement :

Active Directory fonctionne comme un **service centralisé de gestion des identités dans un environnement Windows**.

1. Structure hiérarchique

Active Directory est **organisé de manière hiérarchique en unités logiques appelées domaines**. **Chaque domaine peut contenir des objets** tels que des utilisateurs, des groupes, des ordinateurs et des ressources partagées

2. Services principaux

- **Service d'annuaire : Stocke les informations sur les objets du domaine**, telles que les utilisateurs, les groupes et les ordinateurs. Il **fournit une base de données centralisée et hiérarchique** pour ces informations.

- **Service d'authentification : Vérifie l'identité des utilisateurs et des ordinateurs qui tentent d'accéder aux ressources du réseau**. Il **assure la sécurité** en vérifiant les informations d'identification des utilisateurs.

- **<u>Service de stratégie de groupe (GPO) :</u> Gère les paramètres de configuration pour les utilisateurs et les ordinateurs dans le domaine**. Les stratégies de groupe peuvent être utilisées pour **définir des règles de sécurité, des paramètres système et des configurations d'applications**.

- **<u>Service de réplication :</u> Synchronise les données entre les contrôleurs de domaine** pour **assurer la cohérence de la base de données** Active Directory.

1. **Contrôleurs de domaine**

Les contrôleurs de domaines sont des serveurs exécutant le service Active Directory. Chaque domaine a **au moins un contrôleur de domaine qui stocke une copie de la base de données** Active Directory pour ce domaine.

2. **Authentification et autorisation**

Lorsqu'un utilisateur ou un ordinateur se connecte au réseau, il est authentifié par le service d'authentification Active Directory. Une fois authentifié, il **peut accéder aux ressources réseau pour lesquelles il est autorisé en fonction des autorisations définies** dans Active Directory.

3. **Administration**

Active Directory est **géré à l'aide d'outils d'administrations** tels que l'**outil Utilisateurs et Ordinateurs Active Directory** (ADUC) et l'**outil Utilitaire de gestion Active Directory** (ADSI). Ces outils permettent aux administrateurs de **créer, modifier** et **supprimer des objets du domaine**, ainsi que de **gérer les autorisations** et de **réplication pour assurer la sécurité et la cohérence des informations dans le réseau**.

IV/ Ses avantages

Active Directory offre plusieurs avantages pour la gestion des identités et des accès dans un environnement Windows.

Voici ses principaux avantages :

1. **Centralisation des identités :** Active directory **centralise les informations** sur les utilisateurs, les groupes et les ordinateurs **dans un annuaire unique**, ce qui **simplifie la gestion des identités et des accès**.

2. **Authentification unique :** Les utilisateurs peuvent **utiliser les mêmes identifiants** (nom d'utilisateur et mot de passe) **pour accéder à toutes les ressources du réseau intégrées à Active Directory**.

3. **Gestion des autorisations :** Active Directory **permet aux administrateurs de définir des autorisations granulaires** (permettant de spécifier des privilèges ciblés pour un utilisateur ou un groupe d'utilisateurs) **pour les utilisateurs et les groupes, contrôlant ainsi leur accès aux ressources du réseau**.

4. **Stratégies de groupe :** Les stratégies de groupes **permettent aux administrateurs de définir et de gérer des configurations**

5. **Sécurité renforcée :** Active Directory **offre des fonctionnalités de sécurité avancées** telles que la gestion des certificats, l'authentification à deux facteurs et le contrôle d'accès basé sur les rôles pour **protéger les ressources sensibles du réseau**.

6. **Réplication et redondance : Les données Active Directory sont répliquées** entre plusieurs contrôleurs de domaine pour **assurer la disponibilité et la redondance**

des informations, même en cas de panne d'un serveur.

7. **Intégration avec d'autres services Microsoft : Active Directory s'intègre avec d'autres services Microsoft** tels que Exchange Server, SharePoint, etc., **offrant ainsi une gestion unifiée des identités et des accès** pour l'ensemble de l'écosystème Microsoft.

8. **Facilité de gestion :** Active Directory est **géré à l'aide d'outils d'administration conviviaux** (qui simplifient les tâches administratives) tels que l'Utilitaire de gestion Active Directory (ADUC), qui **simplifient les tâches courantes de gestion des identités et des accès**.

V/ Ses inconvénients

Malgré les avantages qu'offre Active Directory pour la gestion des identités et des accès dans un environnement Windows, il existe également des inconvénients :

1. **Complexité de déploiement et de maintenance :** La **mise en place et la configuration initiales d'Active Directory peuvent être complexes**, surtout dans les environnements de grande taille. De plus, **la maintenance continue** (gestion des mises à jour, sauvegardes, correctifs de sécurité) **nécessite une expertise technique**.
2. **Coût :** Active Directory peut **entraîner des coûts significatifs**, non seulement pour l'acquisition de licences logicielles, mais également pour le matériel et les ressources humaines nécessaires à sa mise en oeuvre et sa gestion.

3. **Dépendance vis-à-vis de Windows :** Active Directory est une technologie de Microsoft, donc celle-ci est **étroitement liée aux produits Microsoft** et **fonctionne principalement dans un environnement Windows**. Cela p**eut limiter la flexibilité et la portabilité** pour les organisations qui souhaitent utiliser des systèmes d'exploitation ou des applications non-Microsoft.

4. **Risque de sécurité :** Comme toute **infrastructure informatique centralisée, Active Directory présente des risques de sécurité potentiels**, telles que des attaques par force brute (généralement effectuées par des programmes informatiques automatisés et qui génèrent des milliers ou plus de combinaisons de mots de passe), les failles de sécurité et les accès non autorisés.

5. **Évolutivité limitée :** Bien qu'Active Directory puisse évoluer pour prendre en charge des environnements de grande taille, il **peut devenir plus complexe à mesure que le nombre d'utilisateurs, de groupes et de ressources augmente**. Cela **peut rendre la gestion plus difficile** et nécessiter des efforts supplémentaires pour maintenir les performances et la disponibilité du système.