IUT DE COLMAR

R304

Année 2022-23

Service d'annuaire

MARTIN BAUMGAERTNER

3 janvier 2023

Table des matières

1 CM 1 - 3 janvier 2023

1.1 Introduction

Active Directory est un service de gestion des identités et des accès qui est utilisé par les entreprises pour gérer les utilisateurs, les ordinateurs et les réseaux. Il permet de centraliser la gestion des utilisateurs et des groupes, et de contrôler l'accès aux ressources informatiques. Active Directory utilise un arbre hiérarchique de domaines pour stocker les informations sur les utilisateurs, les groupes et les ordinateurs de l'entreprise. Ces informations sont accessibles aux utilisateurs et aux ordinateurs autorisés dans le réseau, ce qui leur permet de se connecter aux ressources de l'entreprise et de les utiliser. Active Directory est souvent utilisé en conjonction avec le service de domaine de fichiers (DFS) pour permettre aux utilisateurs de trouver et d'accéder facilement aux fichiers partagés sur le réseau.

1.2 Les concepts de base

Voici quelques concepts de base à comprendre pour utiliser Active Directory :

- Domaine : un domaine est un ensemble de ressources informatiques qui partagent une base de données commune de comptes d'utilisateurs et de groupes. Un domaine est généralement associé à un nom de domaine DNS (par exemple, "example.com").
- Contrôleur de domaine : un contrôleur de domaine est un ordinateur qui exécute le service Active Directory et qui est chargé de stocker les informations sur les utilisateurs et les ordinateurs du domaine. Le contrôleur de domaine est également chargé de gérer les connexions aux ressources du domaine et de mettre à jour la base de données Active Directory.
- Arbre de domaines : un arbre de domaines est un ensemble hiérarchique de domaines qui partagent une base de données commune de comptes d'utilisateurs et de groupes. Les domaines dans un arbre de domaines sont liés les uns aux autres par des relations de confiance.
- Forêt de domaines : une forêt de domaines est un ensemble d'arbres de domaines qui partagent une base de données commune de comptes d'utilisateurs et de groupes. Les arbres de domaines dans une forêt de domaines sont liés les uns aux autres par des relations de confiance transitive.
- Organizational Unit (OU) : une OU est une unité organisationnelle dans Active Directory qui peut être utilisée pour organiser les objets de l'annuaire, tels que les utilisateurs, les groupes et les ordinateurs. Les OUs peuvent être utilisées pour appliquer des politiques de groupe et pour contrôler l'accès aux ressources du domaine.

— Groupe : un groupe est un objet dans Active Directory qui regroupe des utilisateurs et des ordinateurs. Les groupes sont utilisés pour gérer l'accès aux ressources du domaine et pour appliquer des politiques de groupe.
— Compte utilisateur : un compte utilisateur est un objet dans Active Directory qui représente un utilisateur de l'entreprise. Le compte utilisateur contient des informations sur l'utilisateur, telles que son nom, son adresse e-mail et son mot de passe.
— Compte ordinateur : un compte ordinateur est un objet dans Active Directory qui représente un ordinateur sur le réseau de l'entreprise. Le compte ordinateur est utilisé pour gérer l'accès de l'ordinateur aux ressources du domaine et pour appliquer des politiques de groupe.

1.3 Sécurité de la base Active Directory

La sécurité de la base Active Directory est cruciale pour garantir la confidentialité, l'intégrité et la disponibilité des informations stockées dans l'annuaire. Il existe plusieurs mesures de sécurité qui peuvent être mises en place pour protéger la base Active Directory :

— **Authentification forte** : il est recommandé d'utiliser des mots de passe sécurisés et de mettre en place une politique de mot de passe qui impose des exigences de longueur et de complexité. De plus, l'utilisation de méthodes d'authentification à deux facteurs peut renforcer la sécurité de l'authentification.
— **Chiffrement des communications** : il est important de chiffrer les communications entre les contrôleurs de domaine et les clients pour protéger les informations sensibles transitant sur le réseau. Le protocole LDAP (Lightweight Directory Access Protocol) peut être utilisé pour chiffrer les communications LDAP.
— **Gestion des droits d'accès** : il est essentiel de configurer les droits d'accès de manière à limiter l'accès aux informations sensibles aux seuls utilisateurs et groupes autorisés. Les Groupes de sécurité et les Organizational Units (OU) peuvent être utilisés pour gérer les droits d'accès aux ressources du domaine.
— **Sauvegarde et restauration** : il est important de mettre en place des sauvegardes régulières de la base Active Directory pour pouvoir la restaurer en cas de perte de données. Les sauvegardes doivent être effectuées sur un support de stockage sécurisé et être protégées par un mot de passe.
— **Mise à niveau de la sécurité** : il est important de maintenir Active Directory à jour avec les dernières mises à jour de sécurité pour protéger contre les vulnérabilités connues.

1.4 Le DNS dans Active Directory

Le Domain Name System (DNS) est un service qui permet de traduire les noms de domaine en adresses IP. Dans un environnement Active Directory, le DNS joue un rôle crucial dans la résolution des noms d'hôtes et d'autres ressources du réseau.

Le DNS fonctionne en utilisant une hiérarchie de serveurs DNS qui se répartissent les responsabilités de résolution de noms. Les serveurs DNS de niveau supérieur, appelés serveurs racines, sont responsables de la résolution des noms de premier niveau, tels que ".com" et ".org". Les serveurs DNS de niveau inférieur, appelés serveurs autoritatifs, sont responsables de la résolution des noms de domaines spécifiques, tels que "example.com".

Dans un environnement Active Directory, le serveur DNS autoritatif est généralement le contrôleur de domaine. Le contrôleur de domaine utilise le DNS pour publier les informations de service, telles que l'adresse IP du contrôleur de domaine et les informations de service Kerberos. Les clients Active Directory utilisent le DNS pour trouver les ressources du réseau, telles que les partages de fichiers et les imprimantes.

Il est important de configurer correctement le DNS dans un environnement Active Directory pour assurer une résolution de nom fiable et une communication efficace entre les différents éléments du réseau.

1.5 Les stratégies de groupe en Active Directory

Les stratégies de groupe sont des ensembles de règles et de paramètres qui permettent de configurer et de contrôler les ordinateurs et les utilisateurs d'un domaine Active Directory. Les stratégies de groupe sont appliquées à des objets de l'annuaire, tels que les utilisateurs, les groupes et les ordinateurs, et sont utilisées pour définir les paramètres de sécurité, de stratégie de réseau et de stratégie de système.

Il existe deux types de stratégies de groupe en Active Directory :

— **Stratégies de groupe de niveau utilisateur** : ces stratégies s'appliquent aux utilisateurs et définissent les paramètres de l'environnement de travail, tels que les paramètres de bureau et de stratégie de sécurité.
— **Stratégies de groupe de niveau ordinateur** : ces stratégies s'appliquent aux ordinateurs et définissent les paramètres du système d'exploitation, tels que les paramètres de stratégie de sécurité et de stratégie de réseau.

Les stratégies de groupe sont appliquées aux objets de l'annuaire en fonction de leur appartenance à un groupe ou à une OU. Les paramètres de la stratégie de groupe peuvent être hérités de manière descendante dans l'arborescence de l'annuaire, ce qui permet de configurer de manière centralisée les paramètres de l'ensemble des objets d'un domaine.

Les stratégies de groupe sont un outil puissant pour la gestion des ordinateurs et des utilisateurs dans un environnement Active Directory et permettent de configurer de manière centralisée les paramètres de l'ensemble des objets d'un domaine.

1.6 Concept de l'active directory

L'Active Directory est un service de répertoire qui permet la gestion centralisée des informations de l'entreprise, telles que les utilisateurs, les ordinateurs et les imprimantes. Il utilise le protocole LDAP (Lightweight Directory Access Protocol) pour permettre l'accès à ces informations. LDAP est un protocole de réseau qui permet de lire et de modifier les informations stockées dans un annuaire de données, comme l'Active Directory. En utilisant LDAP, les applications peuvent accéder et gérer les informations de l'annuaire de manière standardisée et sécurisée.

1.7 Les rôles FSMO dans Active Directory

Les rôles FSMO (Flexible Single Master Operations) sont des rôles de domaines spéciaux dans un environnement Active Directory qui sont détenus par un seul contrôleur de domaine dans un domaine donné. Il y a cinq rôles FSMO différents qui peuvent être affectés à des contrôleurs de domaine différents dans un environnement Active Directory :

- **Rôle du maître unique de l'annuaire (RID)** : Ce rôle est responsable de la distribution de séries uniques de numéros de sécurité (SID) et de numéros de réplication de l'identificateur (RID) aux nouveaux comptes d'objets de l'annuaire créés dans le domaine.
- **Rôle du maître unique de la stratégie de groupe (PDC)** : Ce rôle est responsable de la mise à jour de la stratégie de groupe et de la synchronisation des horloges dans le domaine.
- **Rôle du maître unique de la hiérarchie de noms (PDN)** : Ce rôle est responsable de l'ajout et de la suppression de domaines de l'annuaire.
- **Rôle du maître unique de la stratégie de noms (PDN)** : Ce rôle est responsable de la modification de la stratégie de noms et de la définition de la stratégie de noms par défaut pour le domaine.
- **Rôle du maître unique de la base de données de certification (PDC)** : Ce rôle est responsable de la révocation de certificats et de la gestion de la base de données de certification de l'annuaire.

Il est recommandé de répartir ces rôles sur plusieurs contrôleurs de domaine pour assurer la redondance et la disponibilité des fonctionnalités associées à chaque rôle.