ACTIVE DIRECTORY – NOTIONS DE BASE

SERVICES DE DOMAINE ACTIVE DIRECTORY
ACTIVE DIRECTORY DOMAIN SERVICES (AD DS)

ACTIVE DIRECTORY

ACTIVE DIRECTORY est un annuaire développé par Microsoft, utilisé sur les systèmes Windows Server. Il permet de fournir un système centralisé pour la gestion des utilisateurs, ordinateurs, et d'autre objets AD, ainsi que la gestion des ressources sur le réseau.

DOMAINE ACTIVE DIRECTORY

UN DOMAINE DANS ACTIVE DIRECTORY est une zone logique qui permet de regrouper et gérer des objets comme les utilisateurs, ordinateurs, groupes et ressources. Chaque domaine a sa propre base de données, ses politiques de sécurité, et peut être géré indépendamment ou dans une relation avec d'autres domaines.

CONTRÔLEUR DE DOMAINE

UN CONTRÔLEUR DE DOMAINE (DOMAIN CONTROLLER - DC) est un serveur Windows sur lequel le rôle AD DS (Active Directory Domain Services) est installé. Il a pour fonctions principales de :

- **Héberger une copie de la base de données Active Directory.**
- **Authentifier les utilisateurs et ordinateurs (connexion au réseau).**
- **Autoriser ou non l'accès aux ressources.**
- **Gérer de manière centralisée les objets AD.**
- **Répliquer automatiquement les données vers les autres contrôleurs de domaine dans le même domaine ou la même forêt.**

LA FORÊT AD

UNE FORET ACTIVE DIRECTORY est le niveau le plus haut dans la structure d'Active Directory.
Elle regroupe un ou plusieurs domaines qui partagent :

- **Le même schéma AD (structure des objets).**
- **La même configuration.**
- **Un catalogue global (répertoire pour rechercher des objets dans tous les domaines).**

Le premier domaine créé dans la forêt est appelé le domaine racine.

ARBORESCENCE DE DOMAINES

UNE ARBORESCENCE DE DOMAINES (ou *DOMAIN TREE*) est un ensemble de domaines Active Directory qui :

- **Partagent un espace de noms contigu.**
  EX :
  ➔ Parent : entreprise.local
  ➔ Enfant : marketing.entreprise.local
- **Sont liés par une relation d'approbation automatique de type parent/enfant.**
- **Cette relation est bidirectionnelle et transitive (les utilisateurs peuvent accéder aux ressources entre domaines selon les permissions).**

RELATION D'APPROBATION

LES RELATIONS D'APPROBATION (ou *TRUSTS*) sont des liens de confiance entre deux domaines Active Directory.
Elles permettent à un utilisateur d'un domaine d'accéder aux ressources d'un autre domaine, s'il a les autorisations nécessaires.

LES OBJETS AD

- **UNITÉ D'ORGANISATION :**
  - ➔ **Une unité d'organisation (ou ORGANIZATIONAL UNIT) est un objet de type conteneur qui peut regrouper plusieurs objets AD.**
  - ➔ **Elle permet d'implémenter une hiérarchisation dans l'annuaire AD.**
  - ➔ **Elle facilite l'administration et l'application des stratégies de groupes (GPOs).**

- **UTILISATEUR : Permet l'authentification des utilisateurs physiques qui ouvrent une session sur le domaine.**

- **GROUPE : Permet de rassembler différents objets (utilisateurs ou ordinateurs) qui doivent avoir un accès identique sur une ressource.**

- **ORDINATEUR : Permet l'authentification des postes physiques ou virtuels connectés au domaine.**

- **IMPRIMANTE : Utilisées pour simplifier le processus de localisation et de connexion aux imprimantes.**

- **DOSSIER PARTAGÉ : Permet de partager les ressources sur le domaine.**

STRUCTURE PHYSIQUE ET LOGIQUE

- **UNE STRUCTURE LOGIQUE représente l'organisation des objets AD (utilisateurs, groupes, ordinateurs) dans l'annuaire.**
  EX : Forêt, Arbre (arborescence), Domaine, Unité d'Organisation (OU).
- **UNE STRUCTURE PHYSIQUE concerne la répartition des serveurs et le trafic réseau.**
  EX : Contrôleurs de domaine, Sites, Liens de site.

LES SITES AD

UN SITE ACTIVE DIRECTORY (AD) représente un emplacement physique du réseau où les ressources (serveurs, utilisateurs) sont proches en termes de connectivité réseau (bande passante élevée, faible latence).

En créant le découpage avec les sites AD, l'administration des réplications entre les sites est facilitée.

Chaque site est lié à un ou plusieurs sous-réseaux IP.

LE SCHÉMA AD

LE SCHÉMA AD Le schéma Active Directory (AD) est la structure qui définit :

- **Quels types d'objets peuvent exister dans l'annuaire (ex. : utilisateur, ordinateur, groupe).**
- **Quelles informations (attributs) peuvent être stockées pour chaque type d'objet.**

Le schéma est partagé par tous les domaines dans la forêt, et il peut être modifié (avec précaution).

Deux éléments du schéma :

➔ Classe d'objet : définit un type d'objet
EX : *user*, *computer*, *printer*.

➔ Attribut d'objet : définit les propriétés qu'un objet peut avoir
EX : *nom*, *mot de passe*, *adresse email*.

LA BASE DE DONNÉES NTDS

LA BASE DE DONNEES NTDS (ou magasin de données AD) est le fichier principal utilisé par Active Directory pour stocker toutes les informations sur les objets du domaine et les données de réplication entre les contrôleurs de domaine.Elle est stockée dans le fichier NTDS.dit. Le fichier se trouve généralement dans le répertoire C:\Windows\NTDS sur le contrôleur de domaine.

LES PARTITIONS AD (NTDS PARTITIONS)

Active Directory est organisé en quatre partitions principales qui permettent de diviser et gérer les différentes informations dans l'annuaire.

- **LA PARTITION DE DOMAINE : Elle contient les informations sur les objets du domaine, comme les utilisateurs, ordinateurs, groupes, etc. Chaque domaine a sa propre partition de domaine.**

- **LA PARTITION DE CONFIGURATION : Elle contient les informations sur la topologie de la forêt, telles que : les domaines, les liens entre contrôleurs de domaine, les sites et leurs configurations de réplication.**

- **LA PARTITION DE SCHÉMA : Elle définit les classes d'objets et les attributs associés. Un seul contrôleur de domaine dans la forêt a les droits d'écriture sur cette partition (souvent appelé le schéma maître). Les autres contrôleurs de domaine peuvent seulement lire ces informations.**

- **LA PARTITION D'APPLICATION : (ou PARTITION DNS) Elle contient la base de données DNS utilisée par Active Directory pour la résolution des noms dans la forêt.**

LES CINQS RÔLES FSMO

LES RÔLES FSMO (FLEXIBLE SINGLE MASTER OPERATIONS) sont des rôles critiques attribués à certains contrôleurs de domaine pour éviter les conflits et maintenir la cohérence dans la base de données Active Directory.

➔ **Rôles au niveau de la forêt (1 seul par forêt) :**

- **MAÎTRE DE SCHÉMA : Responsable de modifier le schéma AD (définition des objets et attributs). Un seul serveur dans toute la forêt peut faire cette opération.**
- **MAÎTRE DE DÉNOMINATION : Responsable de la création ou suppression de domaines dans la forêt. Il garantit l'unicité des noms de domaine.**

➔ **Rôles au niveau du domaine (1 seul par domaine) :**

- **MAÎTRE RID: Donne des blocs de RID aux autres contrôleurs de domaine. Le RID est utilisé pour créer des SID uniques pour chaque objet.**

- **MAÎTRE D'INFRASTRUCTURE: Met à jour les références vers les objets d'autres domaines. Il s'assure que les liens entre objets AD sont à jour même s'ils sont dans des domaines différents.**

- **MAÎTRE EMULATEUR PDC : Gère les changements de mot de passe, les verrouillages de comptes, et la synchronisation horaire.**

LA REPLICATION AD

LA REPLICATION ACTIVE DIRECTORY est le processus qui permet de synchroniser automatiquement les données entre les contrôleurs de domaine, afin de garantir que toutes les informations (utilisateurs, groupes, etc.) soient cohérentes dans toute la forêt.

Elle fonctionne grâce à des objets de connexion, qui sont unidirectionnels (réplication dans un seul sens).

Il existe deux types de réplication :

➔ **LA RÉPLICATION INTRASITE : dans un même site AD.**

- **Très rapide et non compressée, car elle se fait sur des liens réseau locaux.**
- **Après une modification, une notification est envoyée après 15 secondes au 1er partenaire.**
- **Ensuite, une nouvelle notification est envoyée chaque 3 secondes aux autres partenaires.**
- **Le DRA (Directory Replication Agent) effectue alors le transfert des données modifiées.**

➔ **LA RÉPLICATION INTERSITE : entre sites AD différents.**

- **Plus lente et compressée, pour économiser la bande passante WAN.**
- **Chaque site désigne un contrôleur de domaine comme "tête de pont".**
- **Les têtes de pont sont responsables de la réplication entre sites.**
- **Le rôle ISTG (InterSite Topology Generator) crée les objets de connexion nécessaires pour organiser cette réplication.**

PREREQUIS POUR LA PROMOTION D'UN SERVEUR EN CONTROLEUR DE DOMAINE

- **Système de fichiers NTFS : Les partitions du disque doivent être formatées en NTFS (et non FAT32).**
- **Nom de l'ordinateur : Le nom du poste doit être défini avant la promotion.**
- **Configuration réseau : L'adresse IP doit être configurée (fixe de préférence), avec masque, passerelle et DNS (le DNS correctement configuré, souvent en pointant vers lui-même ou un DNS AD déjà existant).**
- **Serveur DNS : Le serveur doit pointer vers un serveur DNS fonctionnel, ou installer DNS lors de la promotion.**
- **Nom du domaine : Définir un nom de domaine valide.**

LES OPTIONS DE PROMOTION

Lors de la promotion d'un serveur, trois choix sont possibles :

- **Ajouter un contrôleur de domaine à un domaine existant : Permet d'ajouter un contrôleur de domaine secondaire ou un RODC (*Read-Only Domain Controller*).**
- **Ajouter un nouveau domaine à une forêt existante : Permet de créer un domaine enfant ou une nouvelle arborescence.**
- **Ajouter une nouvelle forêt : Crée une nouvelle forêt Active Directory avec un nouveau domaine racine.**

CONTROLEUR DE DOMAINE EN LECTURE SEULE (RODC-READ ONLY DOMAIN CONTROLLER)

UN RODC est un contrôleur de domaine spécial qui possède une copie en lecture seule de la base Active Directory.

Il est utilisé principalement dans des sites distants (ex. : une agence ou filiale).

Il permet d'authentifier localement les utilisateurs, sans risquer de modification dans AD.

CONTROLEUR DE DOMAINE SECONDAIRE/SUPPLÉMENTAIRE (ADDITIONAL DOMAIN CONTROLLER - ADC)

UN CONTROLEUR DE DOMAINE SECONDAIRE (ou ADC) est un serveur ajouté à un domaine existant, qui contient une copie complète de l'annuaire AD.
Il assure la répartition des charges, la réplication, la tolérance aux pannes et le partage des requêtes d'authentification.
Contrairement au RODC, il a des droits de lecture et écriture sur la base AD.

SYSVOL

SYSVOL (System Volume) est un dossier partagé sur les contrôleurs de domaine Windows, qui contient les fichiers nécessaires à la gestion et à la configuration d'un domaine Active Directory.
Il est utilisé pour répliquer des données importantes (comme les stratégies de groupe et les scripts de connexion) entre tous les contrôleurs de domaine d'un même domaine.
La réplication de SYSVOL est essentielle pour garantir que tous les contrôleurs de domaine disposent des mêmes fichiers.

La réplication se fait via :

- **➔ FRS (ancien, Windows Server 2000/2003).**
- **➔ DFSR (nouveau, depuis 2008), plus rapide et fiable.**

LA RÉTROGRADATION

LA RETROGRADATION d'un contrôleur de domaine (DC) consiste à retirer le rôle Active Directory Domain Services (AD DS) du serveur.
Cette opération convertit le serveur d'un contrôleur de domaine vers un serveur membre (dans un domaine) ou un serveur autonome (hors domaine), selon le cas.