Présentation de l'Active Directory

L'Active Directory

C'est une solution propriétaire Microsoft. Cela permet de centraliser les identités, objets et les accès aux ressources d'une organisation (ordinateurs, imprimantes, partage de fichiers...).

Aujourd'hui il existe une version alternative "Cloud" ou plutôt SaaS appelée **Microsoft Entra ID**.

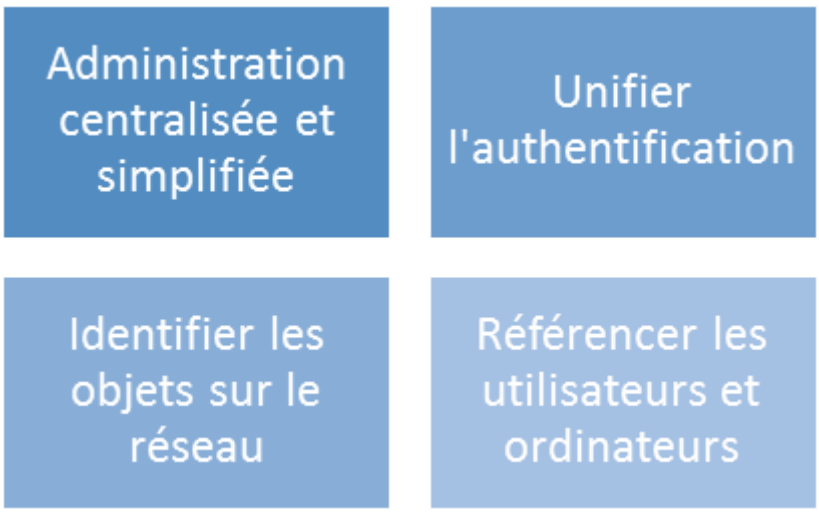
Ce service d'annuaire utilise le protocole LDAP (Lightweight Directory Access Protocol) de la couche 7 du modèle OSI.

Ce protocole s'appuie sur TCP/IP et par défaut il utilise les ports 389 et 3268.

Active Directory utilise également le protocole **DNS** afin d'identifier et enregistrer les objets. Il est donc primordiale de disposer d'une structure DNS stable et fiable pour son fonctionnement.

Les intérêts de l'annuaire

Présent dans la plupart des entreprises, les avantages de l'Active Directory ne sont plus un débat.



- **Centralisation et simplification de l'administration**

La création des utilisateurs, des permissions d'accès aux ressources et la gestion de politiques de configuration (GPO) sont définies et maintenues au niveau du domaine. Donc à partir d'un seul endroit, ce qui évite les répétition de configuration.

- **Authentification**

Les objets "utilisateurs" s'authentifient sur des objets "ordinateurs" qui sont eux même authentifié au domaine AD. Cela leur permet d'accéder (ou non en fonction des autorisations) à des ressources partagés sur d'autres ordinateurs/serveurs du domaine.

Egalement, un seul compte est utile pour se connecter sur des ordinateurs du domaine différents.

Autre point important, il existe de nombreuses applications qui permettent de s'appuyer sur l'authentification Active Directory et donc de simplifier encore plus la gestion des accès en entreprise !

- **Identification**

Comme indiquer précédemment, chaque objet est enregistré dans l'annuaire AD. Ces objets sont unique et facilement identifiables.

Toutes les ressources sont listées et il est très simple de "couper les accès" à une ressource en la désactivant par exemple.

- **Référencement**

L'annuaire AD étant une énorme base de données où tous les utilisateurs et ordinateurs de l'entreprise sont référencés, on s'appuie dessus pour réaliser les opérations d'authentification, d'identification, les déploiements de logiciels, les politiques de mot de passe...

La structure logique

- **Objets**

Les éléments utilisateurs, ordinateurs, serveurs ou encore les unités d'organisations, sont des **Objets** de l'annuaire.

Ces objets correspondent à des **classes** et chaque classe dispose **d'attributs**.

Exemple : un ordinateur est un objet de la classe Ordinateurs. Il dispose d'attributs spécifiques qu'un objet de la classe Utilisateur ne dispose pas et inversement.

- **Conteneurs**

Les conteneurs sont également des objets de l'annuaire, ces derniers servent à l'organisation et peuvent donc contenir d'autre objets.

Les groupes contiendront donc des objets de la classe Utilisateur ou Ordinateur par exemple.

Les Unités d'Organisations (OU) sont également des conteneurs d'objet. Par défaut, des OU sont présentes dans l'annuaire. Il convient à l'administrateur d'en ajouter afin de créer une structure

avec plusieurs niveaux qui simplifieront l'administration générale de l'Active Directory.

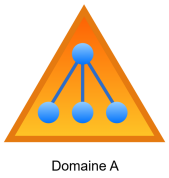
Il faut voir les OU comme des dossiers qui permettent de ranger les objets.

- **Domaine**

Un domaine est une zone d'administration regroupant plusieurs objets et ressources qui partagent un annuaire commun.

Dans le même principe que DNS, Active Directory utilise le principe de l'arborescence inversée. Ainsi, un domaine ajouté à un domaine existant sera "enfant" du premier.

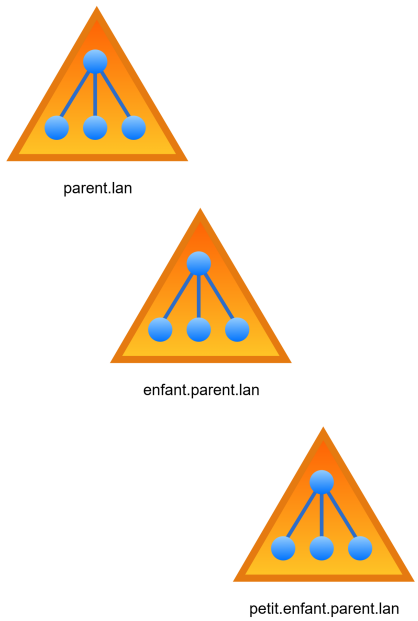
Conventionnellement, les domaine Actives Directory sont représenté par des triangles.



- **Arbre**

L'arbre représente l'ensemble hiérarchique des domaine parent + enfant. Il est possible pour un domaine enfant d'avoir lui aussi un ou plusieurs autres domaine enfant. Cela formera donc une hiérarchie de domaine dont la base du nom reprendra toujours celle du domaine racine/parent : domaineEnfant.domaineParent.lan

Cette ensemble forme donc l'arbre Active Directory.



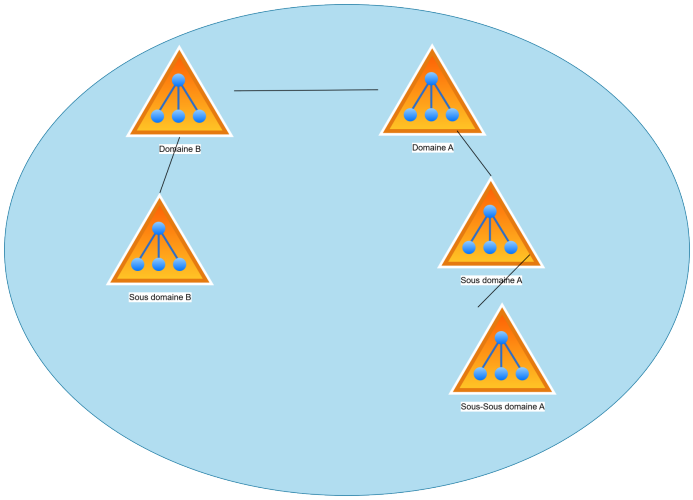
- **Forêt**

C'est la représentation complète de tous les arbres représentant eux mêmes tous les domaine parents + enfants.

Tous les domaines d'une forêt partagent :

- Une configuration commune
- Une étendue de recherche global
- Des relations d'approbations

Lorsque l'on crée un nouveau domaine dans un nouvelle forêt, on crée ce que l'on appelle le **domaine racine**.



- **Le schéma**

Le schéma Active Directory contient toutes les définitions de tous les objets de l'annuaire. Un schéma est créé par défaut à la création d'un domaine, il évoluera au fil du temps en fonction des besoins ou pour répondre à des prérequis d'applications (exemple Microsoft Exchange).

Attention toutefois, la modification du schéma doit être réalisé avec précaution car tous les objets seront impactés par les modifications.

Il existe d'ailleurs un groupe de sécurité "Administrateur du schéma" dont il faut être membre afin de réaliser les modifications.

Revision #1
Created 2025-10-29 15:43:37 UTC by Corentin Roche
Updated 2025-10-29 15:43:45 UTC by Corentin Roche