Active Directory - AD

Active Directory (AD)

1. Présentation
Active Directory est un service d'annuaire développé par Microsoft pour les systèmes Windows. Il permet d'identifier les utilisateurs et les ordinateurs d'un parc informatique et de gérer leurs droits d'accès aux ressources.

Profil itinérant : profil stocké sur le serveur, qui conserve toute la configuration de la personne quel que soit le poste utilisé.

Annuaire : base de données spécialisée conçue pour stocker et organiser les informations sur les utilisateurs, machines, services et ressources d'un réseau. Elle permet de :
- retrouver rapidement une ressource ;
- gérer l'authentification et l'autorisation ;
- centraliser l'administration.

En recensant toutes ces informations, Active Directory constitue un noyau central qui permet de :
- retrouver et accéder à n'importe quelle ressource recensée ;
- avoir une représentation globale des ressources et des droits d'accès associés.
C'est donc un outil d'administration et de gestion centralisée du système d'information.

Active Directory permet de gérer de façon centralisée des réseaux allant de quelques PC à des réseaux d'entreprise répartis sur des sites géographiquement éloignés.

2. Prérequis
- Un serveur Windows Server avec le rôle AD DS, promu en contrôleur de domaine (via le Gestionnaire de serveur ou dcpromo).
- Par sécurité, au moins 2 contrôleurs de domaine pour assurer :
  - la tolérance aux pannes ;
  - la répartition des charges.
- Un serveur DNS sur le réseau (AD en dépend : enregistrements SRV).
- Le DNS de chaque machine doit être celui du domaine.

3. Caractéristiques
AD est avant tout un outil d'administration et d'authentification : il gère le système d'information et les accès des utilisateurs.

Répartition :
- répartition de l'annuaire sur le réseau ;
- réplication multi-maîtres : chaque contrôleur de domaine accepte les modifications, qui sont automatiquement copiées sur tous les autres contrôleurs du domaine (tolérance aux pannes et

répartition des charges) ;
- sécurisation de l'annuaire.

Recherche et indexation : basées sur le protocole LDAP (port 389), qui permet de communiquer avec un annuaire. Il définit comment un client peut :
- rechercher un utilisateur ;
- vérifier un mot de passe ;
- obtenir les informations d'un groupe ;
- ajouter, modifier ou supprimer des objets dans l'annuaire ;
- effectuer tout autre type d'interaction avec l'annuaire.

AD utilise le système de noms de domaine (DNS) pour localiser les services et échanger avec tout annuaire utilisant LDAP.

Protocoles utilisés : TCP/IP, DNS, DHCP, Kerberos (port 88), NTP (synchronisation du temps : Kerberos tolère 5 minutes d'écart maximum), LDAP.
Note : LDIF est un format de fichier d'échange, pas un protocole.

4. Structure logique
- Forêt : contient 1 à n arbres.
- Arbre : contient 1 à n domaines.
- Domaine : structure logique regroupant des ordinateurs partageant la même base d'annuaire. L'annuaire est géré au niveau du domaine. Il contient n unités d'organisation.
- Unité d'organisation (OU) : contient n objets (utilisateurs, ordinateurs, groupes).

Pour de très grandes organisations, plusieurs domaines peuvent être gérés. Sinon, un seul domaine suffit : cela dépend des besoins.

Éléments complémentaires :
- Catalogue global : index partiel de tous les objets de la forêt, pour les recherches inter-domaines.
- Rôles FSMO : 5 rôles à maître unique (maître de schéma, maître d'attribution des noms de domaine, émulateur PDC, maître RID, maître d'infrastructure).

5. Unités d'organisation (OU)
Une OU est une structure hiérarchique logique (et non physique) créée dans un domaine pour représenter une structure géographique ou les services de l'entreprise. Elle peut être fondée sur :
- l'administration ou les objets ;
- les zones géographiques ;
- les activités de l'entreprise ;
- les services de l'entreprise ;
- les projets.

Les OU se présentent comme des conteneurs (comme des dossiers). Elles servent à organiser les objets et à appliquer des GPO.
Les consoles d'administration permettent de tout gérer.

6. Groupes d'utilisateurs
Les groupes permettent d'attribuer les mêmes permissions à plusieurs utilisateurs. Différence : l'OU organise et applique des GPO, le groupe attribue des droits.

Il existe 2 types de groupes :
- Groupes de sécurité : gèrent l'accès aux ressources (ceux que vous allez utiliser).
- Groupes de distribution : envoient des messages à plusieurs personnes via un logiciel de messagerie (Exchange).

Étendues : global, domaine local, universel.
Bonne pratique AGDLP : Account → Global → Domain Local → Permission.

7. GPO
Les stratégies de groupe (Group Policy Objects) sont un outil essentiel d'AD : ce sont des paramètres applicables à des utilisateurs, des ordinateurs ou des groupes.
Elles se définissent au niveau d'un site, d'un domaine ou d'une unité d'organisation.
Ordre d'application : LSDOU (Local, Site, Domaine, OU).

Revision #4
Created 2026-03-23 16:05:30 UTC by Admin
Updated 2026-10-07 16:15:00 UTC by Admin