Présentation d'Active Directory

Active Directory est le nom du **service d'annuaire de Microsoft**. Le terme de service d'annuaire doit être entendu au sens large, c'est-à-dire qu'il s'agit d'un annuaire référençant :

- des **personnes** (nom, prénom, numéro de téléphone, etc.)
- des STAs, des serveurs, des imprimantes, des applications, des bases de données, etc.

En permettant de recenser de nombreuses informations concernant le réseau, Active Directory constitue le moyeu central de toute l'architecture réseau. Cela permet :

- à un utilisateur de retrouver et d'accéder à n'importe quelle ressource recensée.
- d'avoir une représentation globale de l'ensemble des ressources et des droits/acccès associés et constitue de ce fait un outil d'administration et de gestion centralisé du réseau.

La structure d'Active Directory lui permet de gérer de **façon centralisée** des réseaux pouvant aller de quelques ordinateurs à des réseaux d'entreprises répartis sur de multiples sites éloignés géographiquement.

Pour utiliser Active Directory, il faut un ordinateur utilisant une version Windows Server 2k (2000, 2003, 2008, 2008 R2, 2012 R2) sur lequel est installé le **rôle Active Directory**. Il devient alors contrôleur de domaine.

Par sécurité, il doit y avoir au moins deux contrôleurs dans un domaine pour :

- assurer une **tolérance aux pannes**,
- et accessoirement une **répartition des charges**.

Caractéristiques d'Active Directory

Active Directory est un outil destiné aux utilisateurs mais dans la mesure où il permet une représentation globale de l'ensemble des ressources et des droits/accés associés il constitue également un outil d'administration et de gestion du réseau. Il fournit à ce titre des outils permettant de gérer :

- la **répartition** de l'annuaire sur le réseau : base d'annuaire distribuée ;
- sa **réplication** : tolérance aux pannes et répartition des charges ; toute modification d'annuaire est automatiquement copiée sur tous les contrôleurs de domaine d'un domaine
- la **sécurisation** de l'annuaire : le principal protocole d'authentification utilisé est Kerberos.

Comme les annuaires actuels, le mécanisme de recherche et d'index qui permet aux utilisateurs de localiser facilement des ressources publiées, est basé sur le protocole **LDAP** (Lightweight Directory Access Protocol).

Active Directory utilise le système de noms de domaine **DNS** afin d'échanger des informations avec n'importe quel annuaire qui utilise les protocoles LDAP. Il faut donc un serveur DNS sur le réseau.

Utilisation des protocoles TCP/IP

Le fonctionnement d'Active Directory est basé sur des protocoles standards de l'Internet :

- **TCP/IP** : famille de protocoles réseau Internet.
- **DNS** : gestion de l'espace de nom des domaines W2K. Les clients doivent utiliser le même serveur DNS car pour l'ouverture de session, le serveur DNS est consulté pour obtenir la liste du (des) serveur(s) de son domaine (enregistrement DNS de type SRV).
- **DHCP**: distribution de la configuration IP.
- **Kerberos** : authentification.
- **LDIF** : synchronisation de l'annuaire.
- **SNTP** : protocole de distribution de l'heure pour synchroniser les ordinateurs du réseaux. L'authentification Kerberos se base sur un ticket d'accès horodaté.
- **LDAP** : protocole d'accès à l'annuaire (recherche, etc.)

Structure logique d'AD : domaine, unité d'organisation (UO), forêt, arbre

Active Directory est composée de forêts, d'arbres, de domaines et d'unités d'organisation (UO).

- Une **forêt** contient un à n arbres

- Un **arbre** contient un à n domaines
- Un **domaine** contient n Unités d'Organisation
- Une **unité d'organisation** contient n objets

Un domaine est une structure logique (et non pas physique), qui regroupe de manière logique des ordinateurs, en partageant la même base d'annuaire. L'annuaire est géré au niveau du domaine : **« un domaine = un seul annuaire »** qui possède un nom de type DNS : "ma-soc.fr" Tous les contrôleurs de domaine de ce domaine ont le même annuaire (réplication).

Les relations d'approbation

Les relations d'approbation facilitent l'accès, pour un utilisateur d'un domaine, à une ressource d'un autre domaine car son compte sera approuvé. L'utilisateur aura accès aux ressources, en fonction des autorisations définies sans devoir s'authentifier à nouveau.

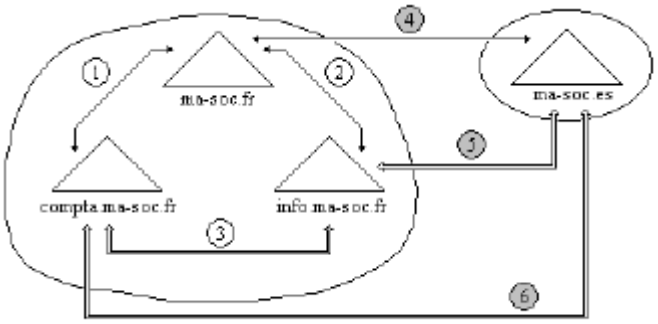
Des **relations d'approbation** sont créées automatiquement et hiérarchiquement entre domaine d'un même arbre. Un arbre est constitué d'un ensemble de domaines et de sous-domaines qui partagent un **espace de nom contigu**.

Les relations d'approbation doivent être créées manuellement entre différent arbres.

Les relations d'approbation sont **transitives**.

Tous les domaines d'une forêt partagent le même **catalogue global**.

Exemple :



Il y a dans cet annuaire Active Directory il y a deux espaces de noms :

- "ma-soc.fr", avec 2 domaines enfants (compta.ma-soc.fr & info.ma-soc.fr),
- "ma-soc.es" (Espagne), sans domaine enfant.

On a **deux arbres** mais **une seule forêt** qui regroupe ces deux arbres.

Relations d'approbation automatiques et hiérarchiques : 1 & 2

Relation d'approbation établie manuellement : 4

Relations d'approbation implicites (transitivité) : 3, 5 & 6

Schéma Active Directory

Le Schéma du service d'annuaire Active Directory contient les définitions de tous les objets, tels que les ordinateurs, les utilisateurs et les imprimantes. Il existe deux types de définitions dans le schéma :

- les classes d'objets décrivent les objets d'annuaire qui peuvent être créés.
- les attributs de chaque classe d'objet

Les utilisateurs peuvent rechercher des objets dans Active Directory en recherchant des attributs spécifiques. **Exemple :** un utilisateur peut rechercher une imprimante dans un bâtiment donné en effectuant une recherche sur l'attribut **Emplacement** de la classe d'objet des imprimantes.

Il n'y a qu'un seul schéma pour l'ensemble de la forêt, schéma qui est stocké dans la base de données AD.

Le catalogue global

C’est un référentiel d'informations qui contient un sous-ensemble d’attributs relatifs à tous les objets Active Directory. Il s'agit des attributs qui sont les plus fréquemment utilisés dans les requêtes (par exemple, le prénom, le nom, le nom d'ouverture de session et le mot de passe d'un utilisateur).

Un serveur de catalogue global est un contrôleur de domaine qui conserve une copie du catalogue global et traite les requêtes qui lui sont destinées.

Le catalogue global remplit deux rôles d'annuaire importants, il permet à un utilisateur :

- d'ouvrir une session sur le réseau en fournissant à un contrôleur de domaine des informations sur l’adhésion aux différents groupes lorsqu'un processus d'ouverture de session est lancé ;
- de trouver des informations d'annuaire dans la forêt entière, quel que soit l’emplacement des données.

Unité d'organisation (OU – Organizational Unit)

Pour de très grandes organisations ou pour permettre une séparation et un cloisonnement des pouvoirs d'administration, il peut y avoir une gestion de plusieurs domaines. Sinon un seul domaine suffit et l'utilisation des unités d'organisation permet de gérer d'organiser l'annuaire pour qu'il corresponde aux besoins de l'organisation.

Une **unité d'organisation** est une structure hiérarchique logique (et non pas physique), créée dans un domaine pour représenter une structure géographique ou des services de l'entreprise. Les unités d’organisation peuvent être fondées sur :

- l’administration ou les objets
- les zones géographiques
- les activités de l’entreprise
- les services de l’entreprise
- des projets

Les **OU** sont des conteneurs (des “dossiers”) dans lesquels on peut **créer** des objets, définir des **stratégies de groupe** et **déléguer droits d’administration**.