Présentation d'Active Directory

- Gestion des utilisateurs et des ressources dans un domaine Active Directory
- Questions

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 (2008, 2008 R2, 2012 R2, 2016, 2019, 2022) 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.

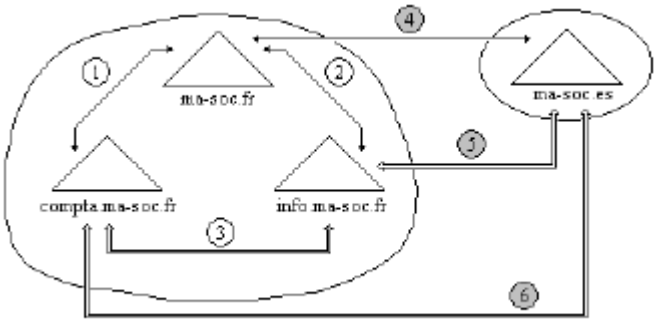
Des **relations d'approbation** sont créées automatiquement et hiérarchiquement entre domaine d'un même arbre. Un arbre est constitué d'un ensemble de domaines et de sous-domaines qui partagent un **espace de nom contigu**.

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**.

La gestion des licences Windows

L'utilsation des logiciels Windows nécessite l'acquisition d'une licence d'utilisation :

- une licence pour chaque client (Windows 10, 11)
- une licence pour chaque serveur Windows Server (2019, 2022)
- une licence d'accès client CAL pour chaque STA qui accède au serveur

La gestion des utilisateurs et des ordinateurs

La console d'administration **Utilisateurs et ordinateurs Active Directory** permet de gérer plusieurs types d'objets. Cette console contient les dossiers suivants :

- Le dossier **Builtin** contient les groupes par défaut avec une étendue de domaine local.
- Le dossier **Computers** contient les comptes d'ordinateurs des stations clientes appartenant au domaine.
- Le dossier **Domain Controllers** contient les contrôleurs du domaine.
- Le dossier **Users** est le conteneur par défaut des utilisateurs du domaine.

Les groupes d'utilisateurs

Les groupes d'utilisateurs permettent de rassembler des utilisateurs devant bénéficier des mêmes droits ou autorisations. Il existe 2 types de groupe :

- les groupes de **sécurité** pour gérer l'accès aux ressources et que vous allez utiliser,
- les groupes de **distribution** (pour envoyer des messages à plusieurs utilisateurs avec le logiciel de messagerie Exchange).

Il y a 3 étendues de groupe :

- **Global** : pour organiser les comptes utilisateurs et avoir des autorisations dans tous domaines. Cela sert à regrouper des utilisateurs ayant des besoins similaires en termes d'accès aux ressources.(Ex. : le groupe **Utilisateurs du domaine**)
- **Domaine local** : pour définir des autorisations à des ressources du domaine local (Ex. : le groupe Administrateurs)
  * **Universelle** : pour regrouper les comptes d'utilisateurs de n'importe quel domaine et assigner des autorisations dans n'importe quel domaine.

Attention : les stations Windows ainsi que les serveurs Windows membre d'un domaine conservent une **gestion locale des comptes**, c'est à dire la gestion d'utilisateurs locaux et de groupes locaux.

La gestion d'un domaine peut se faire par niveau de fonctionnalité afin de pouvoir intégrer des serveurs **anciens** avec des serveurs plus **récents**.

En mode natif il est possible d'imbriquer des groupes dans d'autres groupes, c'est à dire qu'un groupe peut être membre d'un autre groupe.

Un utilisateur peut être membre de plusieurs groupes.

Démarche d'utilisation des groupes

- Les groupes **globaux** reflètent l'organisation de l'entreprise.
- Les groupes **locaux de domaine** sont à utiliser pour gérer les autorisations sur des ressources bien déterminées.

Démarche préconisée par Microsoft (dans un contexte de domaine unique, sans forêt) :

- **AGDLP**, qui signifie : Account, Global group, Domain Local group, Permission.

On ne met pas d'autorisations d'accès directement sur les utilisateurs sauf si l'utilisateur est vraiment unique (dossier personnel / répertoire de base).

Les profils d'utilisateurs

Un profil utilisateur contient tous les informations qui définissent l'environnement de travail d'un l'utilisateur.

- le fichier **ntuser.dat** contenant le profil dans le dossier **Documents and settings**,
- le profil est construit localement la première fois à partir du profil **Default user**,
- Le profil **errant** : il s'agit de retrouver son profil sur n'importe quelle station. Pour cela il faut modifier les propriétés du compte en indiquant dans l'onglet Profil le chemin réseau **UNC** existant (utilisation de la variable %username% pour la création automatique du dossier \\serveur\profiles\%username%)

Le répertoire de base (dossier personnel) peut être créé automatiquement en utilisant la variable %username% sur les partitions NTFS (CT pour l'administrateur et l'utilisateur).