

AD DS

# AD DS

- ❑ Active Directory est le **service d'annuaire** de Microsoft intégré aux versions serveur de Windows. Ce service d'annuaire est basé sur le protocole **LDAP** (Lightweight Directory Access Protocol). Ce protocole définit la méthode utilisée par le client pour l'interrogation de la base de données et permettra aux utilisateurs, entre autres, de se connecter/déconnecter au sein de ce qu'on appelle un **domaine**.
- ❑ L'objectif principal d'Active Directory est de fournir des **services centralisés** d'identification et d'authentification à un réseau informatique.
- ❑ Il répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les imprimantes, etc, qui seront appelés des « **objets** » et qui seront virtuellement stockés dans une base de données.
- ❑ L'intérêt d'avoir un Active Directory dans son réseau est qu'il va permettre de **hiérarchiser les ressources** de l'entreprise. Il va apporter une vision structurée de ses moyens en les organisant par **domaine**.

# Contrôleur de domaine

- ❑ La notion de domaine est **fondamentale** dans la compréhension d'Active Directory. Un domaine par définition est une « entité », **un ensemble logique d'objets** qui vont se partager le même annuaire. Il définit une zone d'administration dans le parc informatique. C'est sur ce domaine que les objets, utilisateurs, ordinateurs etc... seront authentifiés et donc, c'est à ce domaine qu'ils vont appartenir.
- ❑ **Un contrôleur de domaine** (DC) c'est le serveur Active Directory où seront stockées toutes les informations et paramètres dudit domaine, dans une base de données.
- ❑ Le contrôleur de domaine joue donc un rôle essentiel dans la gestion des « objets » Active Directory. Mais ça ne s'arrête pas là car chaque contrôleur peut jouer un rôle particulier dans la gestion du « domaine » ou de la « forêt ».

# Structure d' Active Directory

Active Directory est constitué de deux (2) structures : **une structure physique** et une **structure logique**.

## Structure Physique

La structure physique est tout site d'emplacement géographiquement définissable de votre annuaire Active Directory. Autrement-dit c'est l'emplacement physique des serveurs hébergeant le service AD.

## Structure Logique

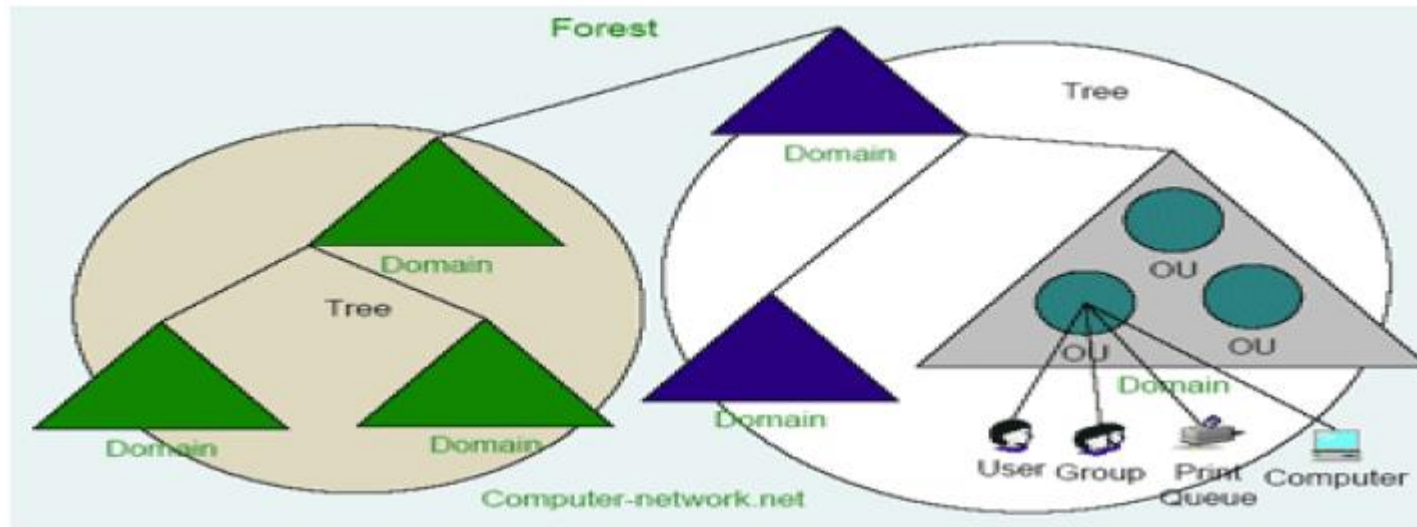
Elle représente l'architecture conceptuelle de votre annuaire. Elle est composée des suivants :

- **Objet** : c'est le plus petit élément du domaine. Il peut être un PC, un smartphone, une imprimante, un scanner, ...etc. Autrement dit c'est l'atome du domaine.
- **Ou (Organisation Unit)** : aussi appelée Unité d'Organisation, c'est un ensemble d'objets. C'est aussi un objet conteneur qui permet de hiérarchiser Active Directory.
- **Domaine** : le domaine est un ensemble d'Unité d'Organisation (OU).
- **Arborescence** : l'arborescence est un ensemble de domaines partageant le même espace de nom.
- **Forêt** : c'est un ensemble de domaines liés entre eux par des relations d'approbation.

# Structure d' Active Directory DS

Il existe 2 types de relation : une relation unidirectionnelle et une relation bidirectionnelle.

- Une relation d'approbation unidirectionnelle permet aux éléments d'un domaine d'accéder à un autre domaine sans une nouvelle authentification. La réciproque n'est pas vérifiée.
- Une relation d'approbation bidirectionnelle permet aux éléments des différents domaines d'accéder à l'autre domaine sans une nouvelle authentification et vice versa.



# LES STRATEGIES DE GROUPE (ou GPO Group Policy Object)

- ❑ L'intérêt d'utiliser des Unités d'Organisations pour **structurer son Active Directory**, c'est de pouvoir y appliquer des **stratégies de groupe**.
- ❑ Les stratégies de groupe (GPO) sont des **outils très puissants de configuration** de l'environnement applicables sur des ordinateurs et/ou des utilisateurs membres d'un domaine Active Directory.

Voici quelques exemples d'utilités des stratégies de groupe dans un domaine :

- Imposer des stratégies de compte (longueur d'un mot de passe, complexité...)
- Déléguer des tâches d'administration
- Empêcher le plug de médias amovibles
- Paramétrer la sécurité (pare-feu, stratégie VPN, Wifi...)
- ...

# TP AD DS

❑ Sous virtualBox:

- Installer et configurer AD DS sous Windows serveur 2012
- Créer deux (2) Unités d'Organisation qui seront « profs » et « étudiants ».
- Dans chacune des OU, créer des utilisateurs après avoir intégré les ordinateurs au domaine.
- Créer appliquer un GPO à OU étudiantS, Choisir la restriction « Empêcher l'accès au panneau de configuration... »