Active Directory

Présentation d'Active Directory :

Introduction :

Active Directory (AD) est un outil d'administration et de gestion de réseau.

Il est un annuaire (ou base de données) qui répertorie et organise les informations concernant le monde Microsoft (utilisateurs, machines, applications).Il regroupe un ensemble de services qui permettent de mettre en lien les utilisateurs avec les ressources réseau dont ils ont besoin pour mener à bien leurs missions. **AD ne concerne QUE Microsoft.**

La base de données (ou annuaire) contient des informations stratégiques sur votre environnement, notamment les utilisateurs et ordinateurs qui le composent et les différentes autorisations d'accès. Par exemple, la base de données peut compter 100 comptes d'utilisateurs, avec des informations telles que le poste occupé par chaque personne, son numéro de téléphone et son mot de passe. Elle recense aussi les autorisations dont ces personnes disposent.

Les informations qui sont répertoriées dans l'AD sont appelées "objets AD", ils sont regroupés principalement en six catégories :

1. Utilisateurs (les comptes utilisateurs)
2. Ordinateur (ordinateur clients du domaine, serveur et contrôleur de domaines)
3. Contact (contact sans authentification)
4. Unité d'organisation (dossier pour créer une arborescence)
5. Imprimante
6. Groupes (listes d'utilisateurs pour l'attribution des droits et/ou services)

A noter que tous les objets sont classés en groupe et sous-groupe pour en simplifier l'administration.

L'organisation des objets AD :

Ils sont regroupés en Domaines (entité autonome de gestion).
Dans le domaine les objets AD sont classés en unités d'organisation (ou Organizational Unit), c'est un conteneur administratif qui peut renfermer des utilisateurs, des groupes et des ordinateurs.

Stratégie de groupe (Group Policy Objects) ils permettent de restreindre des actions comme les accès à certaines ressources ou dossiers, l'attribution des droits ou l'utilisation à certains exécutables.

Le GPO peut s'appliquer à l'ensemble des domaines ou unités d'organisation.

Environnement :

Lorsqu'on se réfère à l'organisation de l'Active Directory, on parle d'arborescence AD.
Un arbre AD correspond à un domaine et toutes ses ramifications (domaines enfants).

L'arbre AD fait partie d'un plus grand ensemble qu'on appelle une forêt.
Une forêt AD comprend donc à la fois le domaine racine (root domain) mais aussi l'ensemble des domaines enfants, la forêt contient donc tous ces arbres.

Afin de permettre aux utilisateurs d'un domaine d'accéder aux ressources d'un autre domaine, l'AD utilise un mécanisme de relations d'approbation.
Ces relations d'approbation permettent d'accorder des permissions dans un domaine différent de celui qui contient le domaine de l'utilisateur.

Les relations d'approbation peuvent être de nature multiple :

- intra forêt
- inter forêt
- inter sous domaines de plusieurs forêts par exemple

Ce qui signifie qu'un utilisateur d'un domaine peut avoir des permissions dans n'importe quel domaine de la forêt mais aussi que chaque domaine connaît les relations qu'il a avec les autres domaines de la forêt.

Une architecture AD repose sur les Domain Controllers (serveurs, annuaires) qui sont des serveurs avec un système d'exploitation de la famille Windows Server.

L'architecture AD se base sur plusieurs Domain Controller qui vont synchroniser les données d'annuaires entre eux assurant ainsi la cohérence des informations dans toute la forêt. Ils assurent les communications entre les utilisateurs et les domaines comme les processus d'ouverture de session d'utilisateurs, l'authentification et les recherches d'annuaire.

A noter qu'il existe un type particulier de Domain Controller qui est le RODC (Read Only Domain Controller) il est utilisé dans le cas des sites distants permettant aux utilisateurs d'accéder aux ressources réseau beaucoup plus rapidement tout en garantissant la sécurité et l'intégrité de l'Active Directory.

Protocoles :

- **LDAP (Lightweight Directory Access Protocol)** : LDAP est le protocole principal utilisé par Active Directory pour permettre l'accès aux informations d'annuaire.
  Il fournit des opérations de lecture et d'écriture pour interagir avec les données stockées dans Active Directory, telles que les utilisateurs, les groupes et les ressources réseau.
  LDAP est utilisé pour l'authentification des utilisateurs, la recherche d'informations dans l'annuaire et la gestion des objets d'annuaire.

- **DNS :** sans le DNS l'Active Directory ne fonctionnera pas. C'est d'ailleurs pour ça que lors de la mise en place d'un domaine, l'installation du serveur DNS est proposée.

  Le protocole DNS est utilisé pour la résolution des noms, ce qui permet aux postes clients de localiser les contrôleurs de domaine au sein de votre système d'information. De la même manière, lorsque l'on souhaite joindre un client au domaine, on utilise un nom comme « *it-connect.local* », ce qui implique une requête DNS pour savoir quelle est l'adresse IP correspondante à ce nom, vous serez alors redirigé vers votre contrôleur de domaine qui traitera la requête.

- **Kerberos** :
  Kerberos est un protocole d'authentification sécurisé utilisé par Active Directory pour valider l'identité des utilisateurs et des ordinateurs.
  Il repose sur des tickets d'authentification chiffrés pour établir et valider les sessions sécurisées entre les clients et les serveurs.
  Kerberos est essentiel pour assurer un accès sécurisé aux ressources réseau et garantir l'intégrité des communications dans un environnement Active Directory.

Les avantages et inconvénients d’Active Directory :

Avantages	Description
Centralisation des données	Toutes les informations relatives aux utilisateurs, ordinateurs, groupes, etc., sont stockées en un seul endroit, facilitant ainsi leur gestion et leur accessibilité.
Authentification unique	Les utilisateurs peuvent utiliser leurs identifiants AD pour accéder à différents services et ressources, réduisant ainsi la nécessité de gérer plusieurs mots de passe.
Contrôle d'accès	Permet de définir des politiques de sécurité et des autorisations granulaires pour contrôler l'accès aux ressources réseau, renforçant ainsi la sécurité.
Gestion des stratégies de groupe (GPO)	Les stratégies de groupe permettent de configurer et de déployer des paramètres système pour les utilisateurs et les ordinateurs, simplifiant ainsi la gestion des configurations système.
Intégration avec d'autres services Microsoft	Active Directory s'intègre étroitement avec d'autres produits et services Microsoft tels que Exchange Server, SharePoint et Office 365, offrant une expérience utilisateur cohérente.

Inconvénients	Description
Complexité de déploiement et de maintenance	La mise en place et la maintenance d'Active Directory peuvent être complexes, nécessitant des compétences spécialisées et des ressources dédiées.
Coût de licence	Bien qu'Active Directory soit inclus dans les éditions serveur de Windows, certaines fonctionnalités avancées ou l'intégration avec d'autres produits peuvent entraîner des coûts supplémentaires.
Dépendance vis-à-vis de Microsoft	Active Directory étant un produit propriétaire de Microsoft, les organisations qui l'utilisent peuvent être verrouillées dans l'écosystème Microsoft, limitant ainsi leurs options de fournisseurs.
Sécurité et vulnérabilités	Comme tout logiciel, Active Directory est sujet à des vulnérabilités de sécurité qui nécessitent des mises à jour régulières et une surveillance constante pour maintenir un niveau de sécurité adéquat.
Évolutivité limitée	Bien qu'Active Directory puisse gérer des environnements de petite à grande taille, les déploiements à très grande échelle peuvent nécessiter une planification minutieuse et des configurations spécifiques pour assurer une performance optimale.