

Active Directory Introduction (ultra-light, pas d'installation)

Dernière mise à jour : 29/10/22

Table des matières

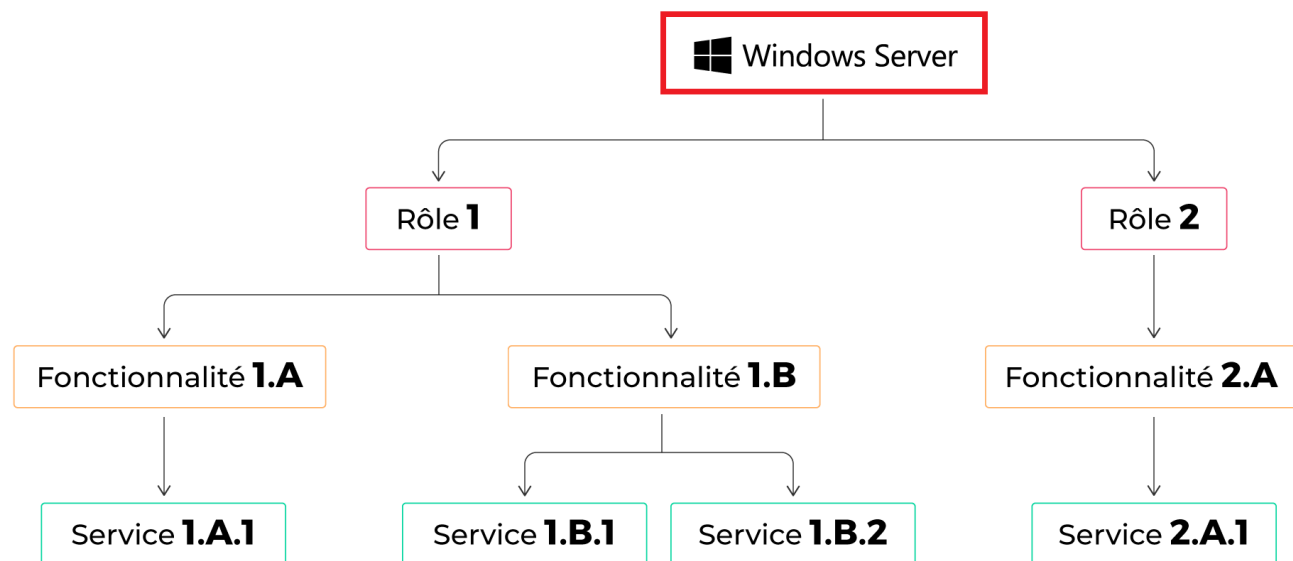
I. Configuration de rôles et services réseaux de base.....	2
II. Active Directory – Présentation.....	4

I. Configuration de rôles et services réseaux de base

Dans cette section nous allons découvrir les différents rôles et fonctionnalités disponibles sous Windows Server.

Un serveur Windows aura dans une entreprise un (ou plusieurs) **rôle(s)**. Ces rôles peuvent être de fournir/**héberger des fichiers**, gérer un annuaire (**Active Directory**), gérer des **certificats**, configurer votre réseau (**DHCP**) , etc. Pour être efficace, un rôle peut avoir besoin de **fonctionnalités**.

Chacun de ces rôles, pour fonctionner, va s'appuyer sur des **services**.



Sur Windows Server 2016 Standard on pourra ainsi installer les rôles suivants (liste non exhaustives) :

- Accès à distance et Services Bureau à distance
- Hyper-V
- Serveur **DHCP**
- Serveur **DNS**
- Serveur Web (IIS)
- Services **Active Directory**

- Services d'**impression**
- Service de **fichiers** et de stockage
- Service de **stratégie** et d'accès réseau
- Service WSUS (Windows Server Update Services)

II. Active Directory – Présentation

Le **système d'information** (SI) est un ensemble structuré de ressources permettant de collecter, stocker, traiter et **distribuer de l'information**, au travers d'un réseau informatique. Il permet donc de gérer et traiter de l'information au format numérique. Afin de garantir la **sécurité de ces informations**, il convient de mettre en œuvre des autorisations d'accès et des règles strictes qui assureront que les traitements sont correctement effectués par les personnes qui en ont le droit.

L'élément central d'un système d'information est l'**annuaire des ressources**. Il centralise les identités et les regroupe afin de simplifier la mise en œuvre de règles d'accès à l'information. Cet annuaire permettra également de s'assurer que les personnes utilisent des ressources matérielles (ordinateurs, imprimantes...) qui répondent elles aussi à des règles de fonctionnement strictes.

Nous allons étudier **Microsoft Active Directory** qui est l'annuaire de ressources le plus utilisé en entreprise. Son fonctionnement est natif pour les ordinateurs ayant des environnements Windows et peut aussi fonctionner avec Linux. Toutefois les systèmes d'exploitation UNIX n'auront pas accès à l'ensemble des fonctionnalités et sa mise en place grâce à Samba est plus complexe. Samba est un logiciel d'interopérabilité qui implémente le protocole propriétaire de fichiers Microsoft **SMB (Server Message Block ; SaMBa)**. La version 3 permettra ainsi d'intégrer des machines Linux en tant que membre d'un **domaine** (ensemble d'ordinateurs reliés à Internet et possédant une caractéristique commune, par exemple « .com » qui s'appliquait à l'origine aux domaines enregistrés par des entités commerciales). La dernière version 4 permettra de mettre en place un service de contrôleur de domaine Active Directory.

Active Directory va donc stocker dans une base de données (qui peut être distribuée sur un ou plusieurs contrôleurs de domaine) les renseignements relatifs aux ressources réseau d'un domaine (comptes utilisateurs, serveurs, postes de travail, dossiers partagés, imprimantes, etc.). Son objectif est de centraliser l'identification et l'authentification d'un réseau de postes clients. Il permettra aussi de créer et gérer des stratégies de groupe, installer des logiciels et assurer leurs mises à jour, etc.

Nous allons par la suite beaucoup parler d'**objets** qui composeront notre Active Directory et seront des types suivants :

- **Ressources** (poste de travail, imprimante, dossier partagé, etc...)
- **Utilisateurs** (comptes individuels ou des groupes qui rassembleront plusieurs utilisateurs avec des droits et des services associés)
- **Services** (courrier électronique par exemple)

Chaque **objet** représente une **entité unique** (utilisateur, ordinateur, imprimante, etc...) et possède une **identification unique** (son nom) et des attributs. Certains objets peuvent être des conteneurs et ainsi englober d'autres objets.

Un Active Directory (AD) permettra de répertorier de quelques centaines à plusieurs millions d'objets, nous pourrons ensuite « interroger » notre annuaire pour par exemple connaître la liste de toutes les imprimantes de marque HP sur un site géographique donné.

Les **attributs de l'objet** sont les **caractéristiques** et les **informations** que l'objet peut contenir. Ils seront défini par un schéma (qui spécifiera notamment le type d'objets pouvant être stockés dans l'AD). Chaque attribut peut être utilisé dans plusieurs classes d'objets de schémas différents. Ces objets de schéma existent pour permettre au schéma d'être étendu ou modifié si nécessaire. Toutefois la désactivation ou la modification de ces objets peut avoir de graves conséquences car elle entraîne des modifications fondamentales dans la structure de l'AD. Toute modification sera automatiquement propagée dans Active Directory et une fois créé, l'objet de schéma ne peut plus être supprimé (il peut seulement être désactivé), donc portez une attention toute particulière à la création ou modifications de vos schémas.

Les **Unités Organisationnelles** (UO ou OU :Organisational Unit) sont des conteneurs qui seront constitués d'objets hiérarchisés. Ils permettront la délégation de droits ainsi que l'application de nos stratégies de groupe (GPO). On pourra structurer et hiérarchiser nos utilisateurs au sein de notre domaine.

Cf CasFictifsAD.pdf pour illustrer ce que représente l'annuaire AD.