

# Chapitre 1

## -- Active Directory --

# CHAPITRE 1

## -- ACTIVE DIRECTORY --

### Rappel: groupe de travail et domaine:

- toutes les machines sous Windows sont par défaut dans un groupe de travail nommé « WORKGROUP », et qui permet de mettre en relation des machines d'un même groupe de travail, notamment pour le partage de fichiers,
- Mais il n'y a pas de notions d'annuaire, ni de centralisation avec ce mode de fonctionnement.

**→ Solution : Active Directory**

# CHAPITRE 1

## -- ACTIVE DIRECTORY --

### 1. Rappel: groupe de travail et domaine:

#### groupe de travail:

- - **Une base d'utilisateurs par machine** : appelée « base SAM », cette base est unique sur chaque machine et non partagée, ainsi, chaque machine contient sa propre base d'utilisateurs indépendante.
- - **Très vite inadapté dès que le nombre de postes et d'utilisateurs augmente**, car cela devient lourd en administration et les besoins différents.
- - **Création des comptes utilisateurs en nombre**, car chaque utilisateur doit disposer d'un compte sur chaque machine, les comptes étant propres à chaque machine.
- - **Manque de control et de sécurité** : chaque ordinateur peut devenir membre du groupe de travail sans authentication

# CHAPITRE 1

## -- ACTIVE DIRECTORY --

Rappel: groupe de travail et domaine:

### Domaine:

- - **Base d'utilisateurs, de groupes et d'ordinateurs centralisée.** Un seul compte utilisateur est nécessaire pour accéder à l'ensemble des machines du domaine.
- - **L'annuaire contient toutes les informations relatives aux objets,** tout est centralisé sur le contrôleur de domaine,
- - **Chaque contrôleur de domaine contient une copie de l'annuaire,** qui est maintenue à jour et qui permet d'assurer la disponibilité du service et des données qu'il contient. Les contrôleurs de domaine se répliquent entre eux pour assurer cela.
- - **Administration et gestion de la sécurité centralisée.**

# CHAPITRE 1

## -- ACTIVE DIRECTORY --

### 1. Introduction au service d'annuaire AD:

- Active Directory est un service d'annuaire utilisé pour stocker des informations relatives aux ressources réseau sur un domaine.
- il permet de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows.
- Il permet également l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour .
- Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés les imprimantes...
- Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation.

## CHAPITRE 4

### -- ACTIVE DIRECTORY --

#### 1. Introduction au service d'annuaire AD:

Administration  
centralisée et  
simplifiée

Unifier  
l'authentification

Identifier les  
objets sur le  
réseau

Référencer les  
utilisateurs et  
ordinateurs

## **CHAPITRE 4**

### **-- ACTIVE DIRECTORY --**

#### **2. Contrôleur de domaine:**

- Un contrôleur de domaine est le serveur sur lequel est installé Active Directory
- Il a comme rôle de traiter toutes les requêtes à sa destination; notamment:
  - vérifier les demandes d'authentification,
  - veiller à l'application des stratégies de groupe
  - stocker une copie de l'annuaire Active Directory...
- Un contrôleur de domaine est indispensable au bon fonctionnement du domaine, si on éteint le contrôleur de domaine ou qu'il est corrompu, le domaine devient inutilisable.

# CHAPITRE 1

## -- ACTIVE DIRECTORY --

### 2. Contrôleur de domaine:

- Le fichier de base de données NTDS.dit .<sup>.dll</sup>
- Sur chaque contrôleur de domaine, on trouve une copie de la base de données de l'annuaire Active Directory.
- Cette copie est symbolisée par un fichier « **NTDS.dit** » qui .<sup>.dll</sup> contient l'ensemble des données de l'annuaire.
- Le fichier NTDS.dit se trouve dans:  
  
Partition du système:\Windows\NTDS\ntds.dit

# CHAPITRE 1

## -- ACTIVE DIRECTORY --

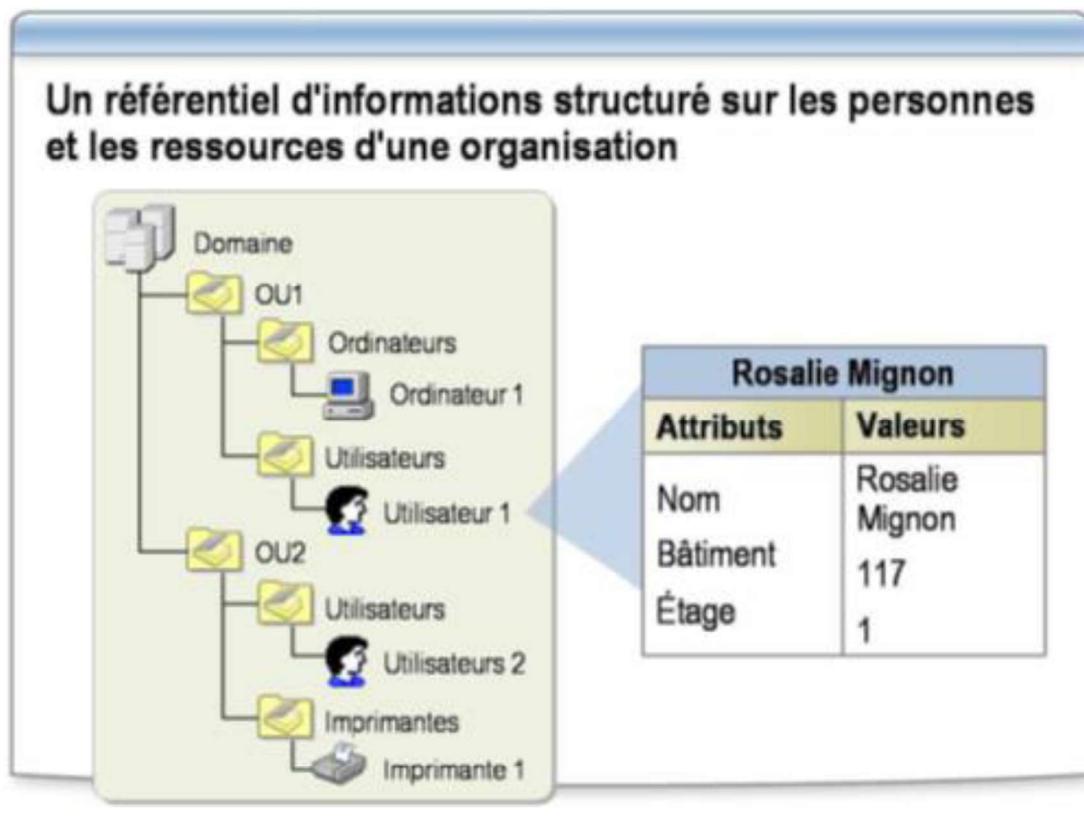
### 3. Structure d'Active Directory

- Une structure *Active Directory* (AD) est une organisation hiérarchisée d'objets.
- Les objets sont classés en trois grandes catégories :
  - les ressources (par exemple les imprimantes),
  - les services (par exemple le courrier électronique)
  - les utilisateurs (comptes utilisateurs et groupes).
- Chaque objet représente une entité unique — utilisateur, ordinateur, imprimante ou groupe — ainsi que ses attributs.
- Un objet est identifié de manière unique dans l'AD par son nom et possède ses propres attributs.

# CHAPITRE 1

## -- ACTIVE DIRECTORY --

### 3. Structure d'Active Directory



# CHAPITRE 1

## -- ACTIVE DIRECTORY --

### 3. Structure d'Active Directory

- Les types d'objets
  - Unité d'organisation:
- L'Unité d'Organisation ; Dans l'arborescence, ce sont des conteneurs qui permettent d'organiser les objets au sein d'un *domaine*.  
OU = unité d'orga
- Ces OU sont principalement utilisées pour permettre la délégation de droits et pour l'application de GPO.

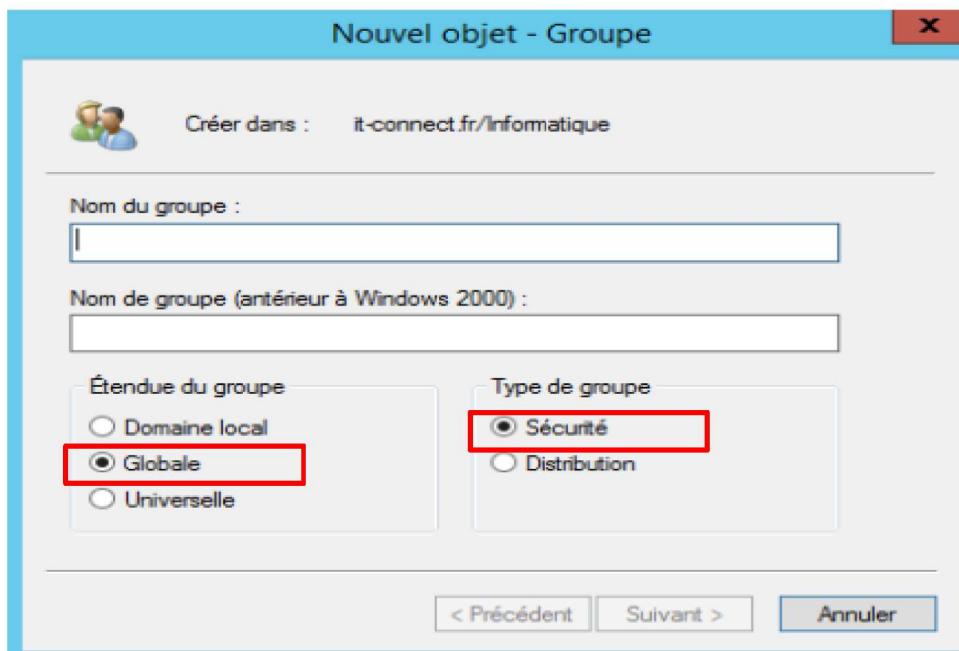
# CHAPITRE 1

## -- ACTIVE DIRECTORY --

### 3. Structure d'Active Directory

- Les types d'objets

- Groupe:



# CHAPITRE 1

## -- ACTIVE DIRECTORY --

### 3. Structure d'Active Directory

- Les types d'objets

- Groupe:

Il est destiné à établir des listes d'utilisateurs pour leur attribuer des droits ou des services. On distingue trois étendues de groupes :

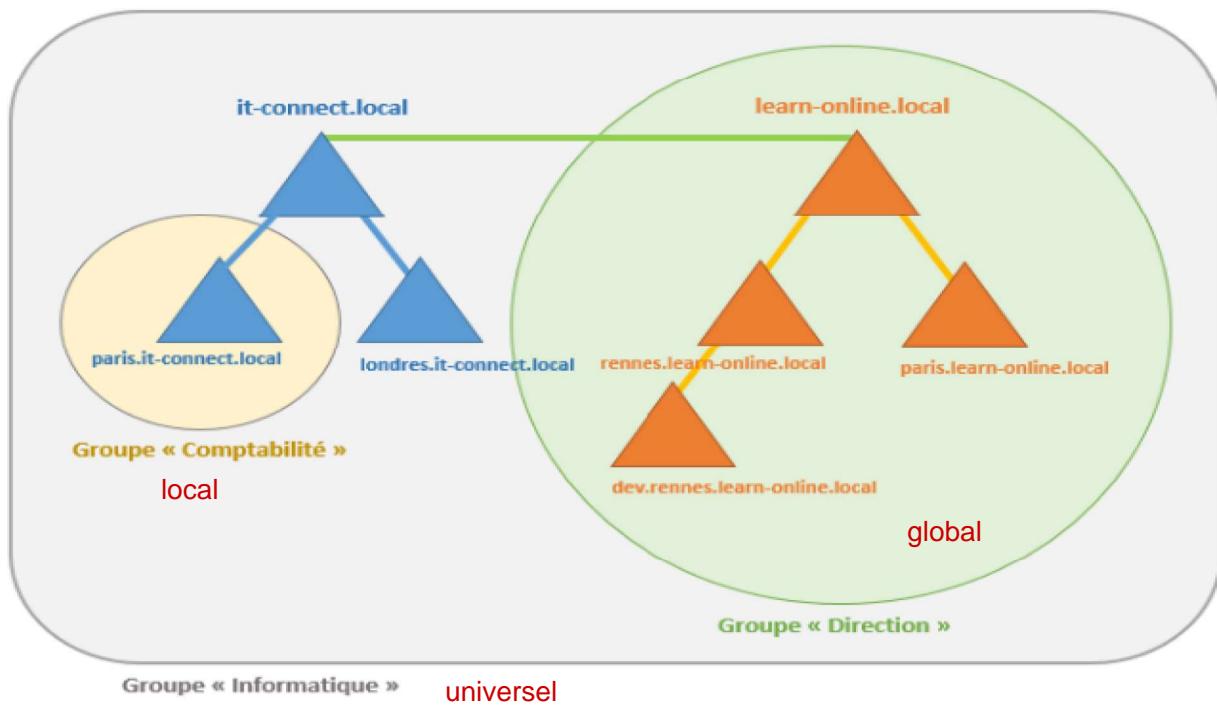
- Le groupe local : peut être utilisé uniquement dans le domaine dans lequel il est créé. Il peut être défini pour contrôler l'accès aux ressources uniquement au niveau du domaine local.
- Le groupe global Un groupe ayant une étendue « globale » pourra être utilisé dans le domaine local, mais aussi dans tous les domaines approuvés par le domaine de base
- groupe universel : à une portée maximale puisqu'il est accessible dans l'ensemble de la forêt, ce qui implique qu'il soit disponible sur tous les domaines de la forêt.

# CHAPITRE 1

## -- ACTIVE DIRECTORY --

### 3. Structure d'Active Directory

- Les types d'objets
  - Etendue de Groupe:



# CHAPITRE 1

## -- ACTIVE DIRECTORY --

### 3. Structure d'Active Directory

- Les types d'objets
  - Types de Groupe:

On distingue deux types de groupes :

- **Sécurité** Les groupes de sécurité permettent de gérer les autorisations d'accès aux ressources.
- Par exemple, si vous avez un partage sur lequel vous souhaitez donner des autorisations d'accès, vous pourrez utiliser un « *groupe de sécurité* » pour donner des autorisations à tous les membres de ce groupe.
- **Distribution:** L'objectif de ce type de groupe n'est pas de faire du contrôle d'accès, mais plutôt des listes de distribution. Par exemple, créer une liste de distribution d'adresses e-mail en ajoutant des contacts.
- De ce fait, ces groupes sont utilisés principalement par des applications de messagerie, comme Microsoft Exchange.

# CHAPITRE 1

## -- ACTIVE DIRECTORY --

### 4. Forêts, arborescences et domaines

- Domaine:
- Un domaine est constitué d'un ensemble d'Unités d'Organisation remplies d'objets de différentes classes : utilisateurs, ordinateurs, groupes, contrôleurs de domaine, etc.

Exemple:



# CHAPITRE 1

## -- ACTIVE DIRECTORY --

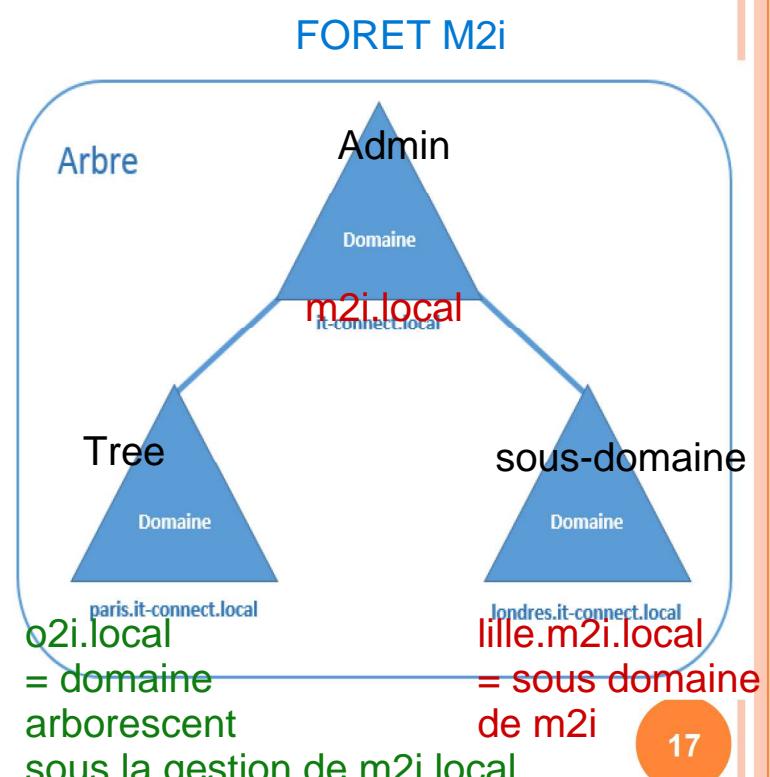
### 4. Forêts, arborescences et domaines

- Arbre:

Un arbre est la constitution d'un domaine principale et de ses sous domaines

Des entreprises ont plusieurs succursales, ce qui implique plusieurs sites sur différents emplacements géographiques.

Selon l'importance de ces sites, on pourra envisager de créer un ou plusieurs sous-domaines au domaine principal



Autre entreprise (Afpa)  
= une autre foret

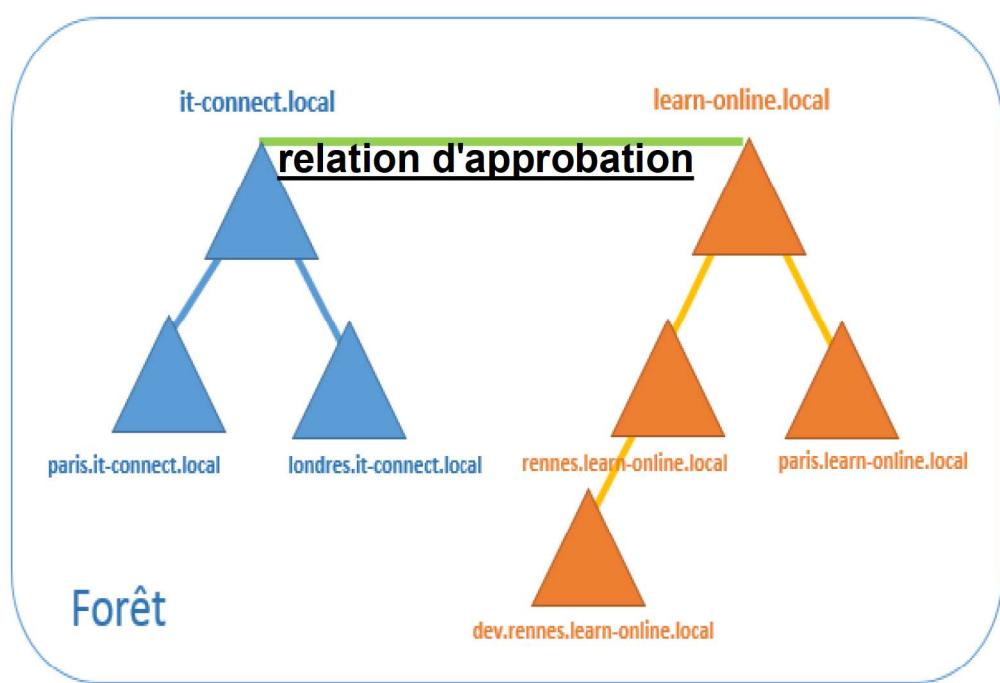
Trust (partage) entre 2 domaines de forets différentes  
ou également entre 2 forêts selon besoins

# CHAPITRE 1

## -- ACTIVE DIRECTORY --

### 4. Forêts, arborescences et domaines

- Forêt:
- une forêt est un regroupement d'une ou plusieurs arborescences de domaine



## CHAPITRE 1

### -- ACTIVE DIRECTORY --

#### 4. Forêts, arborescences et domaines

- Forêt:
- Les avantages d'une forêt sont:
  - la forêt facilite les communications entre les domaines,
  - Création de relations entre les différents domaines de la forêt
  - Simplification de l'administration et flexibilité des utilisateurs.
  - Tous les arbres d'une forêt partagent un schéma d'annuaire commun
  - Tous les domaines d'une forêt partagent un « *Catalogue Global* » commun.

# CHAPITRE 1

## -- ACTIVE DIRECTORY --

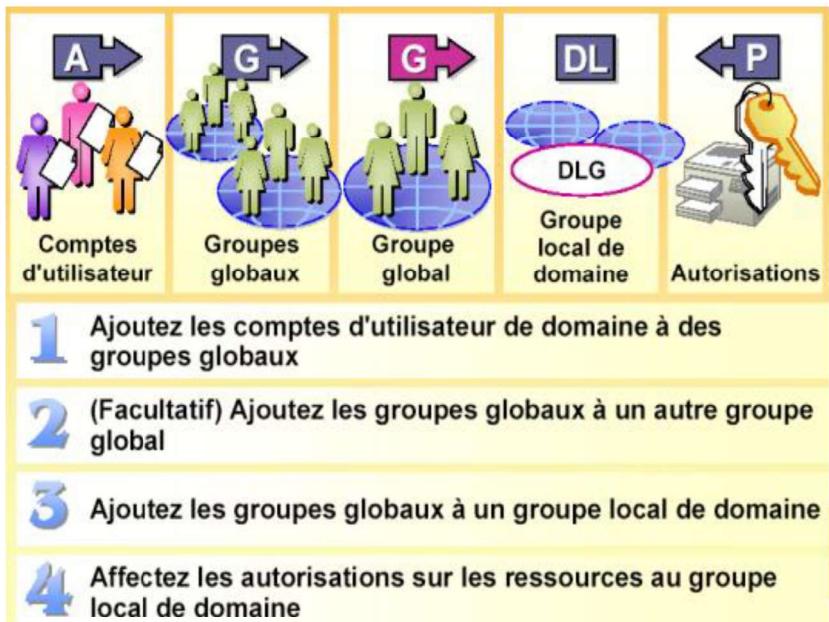
### 4. Forêts, arborescences et domaines

#### Stratégies AGDLP

- **AGDLP** (Accounts, Global, Domain Local, Permissions) est une stratégie d'affectation des droits sous Windows server,

- Elle consiste à:

- Ajouter des comptes utilisateurs à un groupe global
- Ajouter le groupe global dans un groupe domaine local
- Attribuer les autorisations au groupe de domaine local



# CHAPITRE 1

## -- ACTIVE DIRECTORY --

### 5. Les Profils utilisateurs dans AD:

- Profil Standard:
- Windows maintient un profil pour chaque utilisateur ouvrant une session:  
Profil standard
- Le dossier du profil contient des données et des réglages spécifiques à l'utilisateur, comme l'historique de navigation, les documents, les photos, ...
- Les profils standard sont associés à un poste de travail donné.
- Si un même utilisateur ouvre une session sur un autre poste ou sur un poste virtuel, il n'y retrouvera pas les données associées à son profil.

# CHAPITRE 1

## -- ACTIVE DIRECTORY --

### 5. Les Profils utilisateurs dans AD:

- Profil itinérant:
- Les profils itinérants s'appuient sur le stockage des données utilisateurs sur un serveur réseau plutôt que sur un poste de travail.
- Lorsque le client ouvre une session, Windows copie ses données depuis le réseau, sur le poste local.
- A la fermeture de session, Windows copie les modifications apportées au profil sur le serveur. Ce processus vise à garantir que le profil utilisateur est à jour à l'ouverture de session suivante, sur un poste physique comme virtuel.
- Les profils itinérants améliorent la mobilité des utilisateurs et permettent la centralisation des données de profils utilisateurs.
- À partir de Windows Server 2000, il est possible de créer des profils itinérants ,

# CHAPITRE 1

## -- ACTIVE DIRECTORY --

### 5. Les Profils utilisateurs dans AD:

- **Profil Obligatoire:**

- Un profil obligatoire est un profil imposé à l'utilisateur et qui est en lecteur seul.
- En effet lorsqu'un utilisateur modifie son profil il ne sera pas enregistré lors de la fermeture de la session.

#### Etapes de configuration:

- Créer un dossier « ProfilObligatoire » et partager le en réseau.
- affecter ce profil aux comptes d'utilisateurs , pour cela afficher les propriétés de votre compte d'utilisateur à partir de la console Utilisateurs et ordinateurs Active Directory.
- Dans l'onglet Profil, rentrez le chemin du profil: \\serveur\ProfilObligatoire\%Username% pour l'option Chemin du profil.
- Pour rendre le profil obligatoire il faut renommer le fichier **ntuser.dat** en **ntuser.man** dans le répertoire « ProfilObligatoire »

# CHAPITRE 1

## -- ACTIVE DIRECTORY --

### 6. Prérequis pour installer AD:

Un ordinateur équipé de Microsoft® Windows Server. 2016 Standard ou Datacenter.

- 4 Go de RAM
- 60 Go d'espace disque disponible au minimum.
- Une partition ou un volume formaté avec le système de fichiers NTFS. La partition NTFS est nécessaire pour le dossier SYSVOL.
- Les privilèges administratifs nécessaires
- Protocole TCP/IP installé et configuré pour utiliser le système DNS avec IP fixe
- Un serveur DNS qui fait autorité pour le domaine DNS