**Introduction à Active Directory**

**Avantages de l'Active Directory**

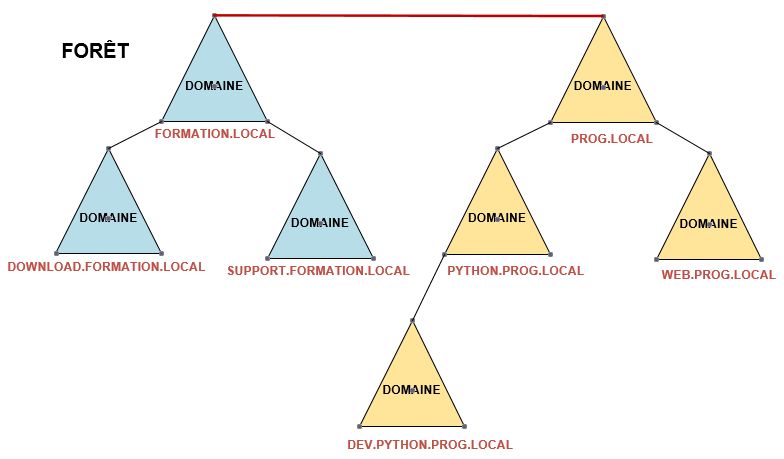
L'Active Directory facilite la centralisation des ressources et de la gestion, ainsi que l'authentification et l'autorisation des utilisateurs.

**Aperçu d’une structure**

Active Directory (AD) est une organisation hiérarchisée d'objets.

Les objets sont classés en trois grandes catégories:

* les ressources (exemple: ordinateurs, imprimantes)
* les services (exemple: courrier électronique)
* les utilisateurs et les groupes
* L'AD fournit des informations sur les objets, il organise et contrôle les accès.



Cette "Forêt" est constituée de deux "Arbres".

**Catalogue global**

Le catalogue global est l’ensemble de tous les objets d’une forêt AD DS (Active Directory Domain Services). Un serveur de catalogue global est un contrôleur de domaine qui enregistre une copie complète de tous les objets de l’annuaire pour son domaine hôte et une copie partielle en lecture seule de tous les objets pour tous les autres domaines de la forêt.

**Installation en mode graphique**

Dans la console "Gestionnaire de serveur" installer le rôle "Services AD DS"

* L'installation de l'Active Directory nécessite l'installation du rôle DNS
* L'installation de l'Active Directory exige un redémarrage.
* Après le redémarrage, nous devons compléter la post-installation afin de "promouvoir ce serveur en contrôleur de domaine".
* On doit choisir "Ajouter une nouvelle forêt" si c'est un nouveau domaine

**Partages administratifs (NETLOGON, SYSVOL)**

Après l'installation de l'Active Directory nous avons accès à deux partages

* \\formation.local\NETLOGON C:\Windows\SYSVOL\sysvol\FORMATION.LOCAL\scripts
* \\formation.local\SYSVOL C:\Windows\SYSVOL\sysvol

On remarque que le partage NETLOGON est un sous-dossier du partage SYSVOL.

Le partage SYSVOL est répliqué entre les contrôleurs de domaine.

Le partage SYSVOL contient deux dossiers

* \\formation.local\SYSVOL\FORMATION.LOCAL\**Policies**

**Ce dossier contient les GPO.**

* \\formation.local\SYSVOL\FORMATION.LOCAL\**scripts**

**Ce dossier contient les les scripts de logon.**

L'Active Directory a un nombre maximum d'objets (utilisateurs, groupes, ordinateurs) qu'il peut gérer.

Le nombre d'objet maximum est 2 147 483 393 = 231 – 255 = 2 147 483 648 – 255

**Présentations des unités d'organisations**

La console "Utilisateurs et ordinateurs Active Directory" contient les objets de l'Active Directory.

Par défaut, il existe seulement une "Unité d'organisation"

* Domain controllers contient les contrôleurs de domaine

Les autres objets de la console sont des "Conteneurs" et voici une courte liste

* Builtin contient que des groupes
* Computers contient des ordinateurs
* Users contient des utilisateurs et des groupes

**IMPOTANT: un administrateur peut ajouter des "Unité d'organisation" mais il ne peut pas ajouter des "Conteneurs".**

**Gestion des utilisateurs, des groupes et des ordinateurs**

La console "Utilisateurs et ordinateurs Active Directory" permet la gestion des utilisateurs, des groupes et des ordinateurs.

La console "Centre d'administration Active Directory" permet la gestion des utilisateurs, des groupes et des ordinateurs. Cette console est plus récente que la console UOAD (Utilisateurs et ordinateurs Active Directory).

**Groupes et leurs portées**

**Étendue du groupe**

* Les membres d'un groupe d'étendue "**Globale**" peuvent provenir uniquement du domaine local mais les membres peuvent accéder aux ressources de n'importe quel domaine.
* Les membres d'un groupe d'étendue "**Domaine local**" peuvent provenir de n'importe quel domaine mais les membres peuvent accéder qu'aux ressources du domaine local.
* Les membres d'un groupe d'étendue "**Universelle**" peuvent provenir de n'importe quel domaine et les membres peuvent accéder aux ressources de n'importe quel domaine.

**Type de groupe**

* Le type de groupe "**Sécurité**" permet de contrôler les accès aux différentes ressources.
* Le type de groupe "**Distribution**" est utilisé avec des logiciels de courriels comme Exchange.

**Gestion des droits utilisateurs**

La gestion des droits utilisateur se fait en utilisant les GPO.

Dans la section "Configuration ordinateur / Stratégies" on doit sélectionner

Paramètres Windows / Paramètres de sécurité / Stratégies locales / Attribution des droits utilisateur

**Canal sécurisé entre un ordinateur et le contrôleur de domaine**

Lorsqu'un ordinateur est joint au domaine un compte ordinateur est créé. Ce compte ordinateur possède un nom (sSMAccountName) et un mot de passe, ce mot de passe est enregistré sous forme de secret LSA (Local Security Account). Le mot de passe est changé à chaque 30 jours.

**"Active Directory" et Linux**

"Ubuntu 21.04" apporte l'intégration native de Microsoft Active Directory.

Ce n'est pas nouveau que de pouvoir joindre un ordinateur Linux à l'Active Directory, ce qui est nouveau avec "Ubuntu 21.04" c'est qu'il est possible de le faire pendant l'installation.

