Chapitre 4

Pré-requis

☒Posséder des connaissances en Active Directory.

Objectifs

☒Définition de l'annuaire Active Directory.

☒Présentation des rôles FSMO.

☒Promotion d'un serveur membre en contrôleur de domaine.

☒Gestion de la corbeille AD et d'une stratégie de mot de passe affinée.

A. Introduction

Active Directory est un annuaire implémenté sur les systèmes d'exploitation Microsoft depuis Windows 2000 Server. Comme pour les autres annuaires, il s'appuie sur la norme LDAP. Beaucoup d'améliorations ont été apportées depuis. Il comprend généralement l'ensemble des comptes nécessaires à l'authentification des ordinateurs et utilisateurs d'une entreprise.

B. Vue d'ensemble d'Active Directory

Le rôle Services de domaine Active Directory contient des composants physiques et logiques.

Les composants physiques vont englober plusieurs éléments clés dans un domaine Active Directory. Ces derniers peuvent être matériels ou logiciels :

- Le contrôleur de domaine, qui contient une copie de la base de données Active Directory.
- La base de données et le dossier sysvol, qui vont contenir l'ensemble des informations d'Active Directory (propriétés des comptes utilisateurs, ordinateurs…). Chaque contrôleur de domaine du domaine Active Directory en contient une copie.
- Le serveur catalogue global, qui contient une copie partielle des attributs (nom, prénom, adresse de l'utilisateur…) des objets de la forêt. Il permet d'effectuer des recherches rapides sur un des attributs d'un objet d'un domaine différent de la forêt.

Tous ces composants fonctionnent avec des composants logiques, ces derniers permettent de mettre en place la structure Active Directory souhaitée.

Ainsi il est possible de trouver les composants suivants :

- Les partitions, qui sont des sections de la base de données Active Directory. Nous allons ainsi pouvoir trouver la partition de configuration, la partition de domaine, la partition DNS…
- Le schéma Active Directory, qui contient les attributs de tous les objets qui peuvent être créés dans Active Directory.
- Le domaine, il permet la mise en place d'une limite administrative pour les objets utilisateurs et ordinateurs.
- Une arborescence de domaine, elle contient une suite de domaine qui partage un espace de noms DNS contigu.

- La forêt Active Directory, qui contient l'ensemble des domaines Active Directory.
- Le site Active Directory, qui permet de découper un domaine en plusieurs parties, ceci afin de limiter et contrôler la réplication entre deux sites distants.
- L'unité d'organisation, qui permet d'appliquer une stratégie de groupe mais également de mettre en place une délégation.

1. Le domaine Active Directory

Un domaine Active Directory est un regroupement logique de comptes utilisateurs, ordinateurs ou de groupes. Les objets qui sont créés sont stockés dans une base de données présente sur tous les contrôleurs de domaine Active Directory. Cette base de données peut stocker plusieurs types d'objets :

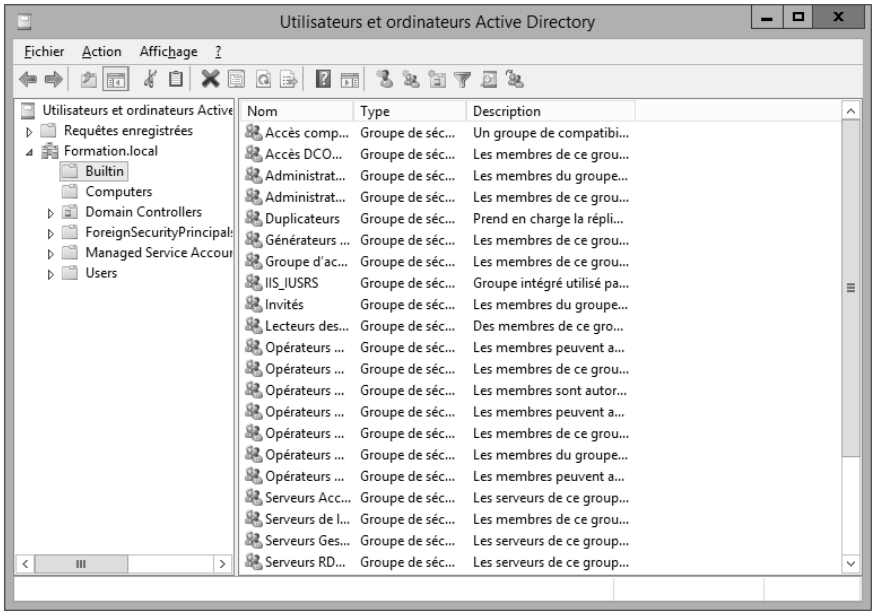
- Le compte utilisateur qui permet d'effectuer une authentification et d'autoriser des accès aux différentes ressources partagées. Il représente une personne physique ou une application.
- Le compte ordinateur qui permet d'authentifier la machine sur laquelle l'utilisateur ouvre une session.
- Enfin les groupes qui permettent de regrouper des comptes utilisateurs et ordinateurs dans le but de leur autoriser l'accès à une ressource, de mettre en place une délégation…

2. Les unités d'organisation

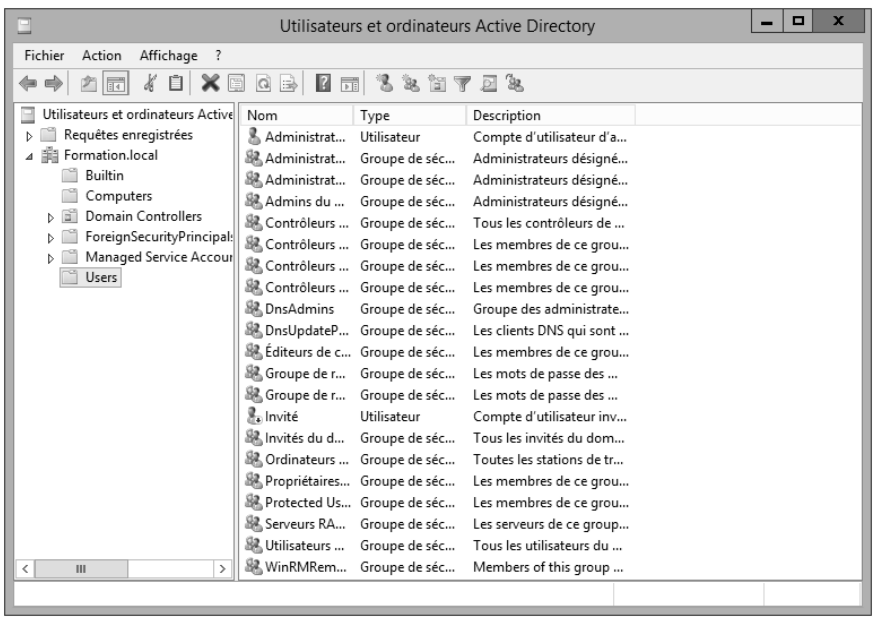
Les unités d'organisation (OU - *Organizational Unit*) sont des objets conteneurs qui permettent le regroupement de comptes utilisateur ou d'ordinateur. La création de ce type d'objet est généralement opérée afin d'assigner une stratégie de groupe à l'ensemble des objets présents dans le conteneur. Sa deuxième fonction est la mise en place d'une délégation afin de permettre à une personne différente de l'administrateur de gérer les objets présents dans le conteneur.

Ainsi les OU représentent une hiérarchie logique dans le domaine Active Directory (il est possible de les imbriquer, on parle alors d'OU parent et d'OU enfant). Il est par exemple possible de créer une unité d'organisation par ville (Aix, Paris...) ou même par type d'objet (utilisateur, ordinateur…). Lors de la création du domaine, des dossiers système et des unités d'organisation sont par défaut présents :

- **Dossier Builtin** : stocke les groupes par défaut : Administrateurs, Opérateurs d'impression…



- **Dossier Utilisateurs** : dossier par défaut lors de la création d'un nouvel utilisateur. Il contient par défaut le compte administrateur et les différents groupes administrateurs (Admins du domaine, Administrateurs de l'entreprise…).

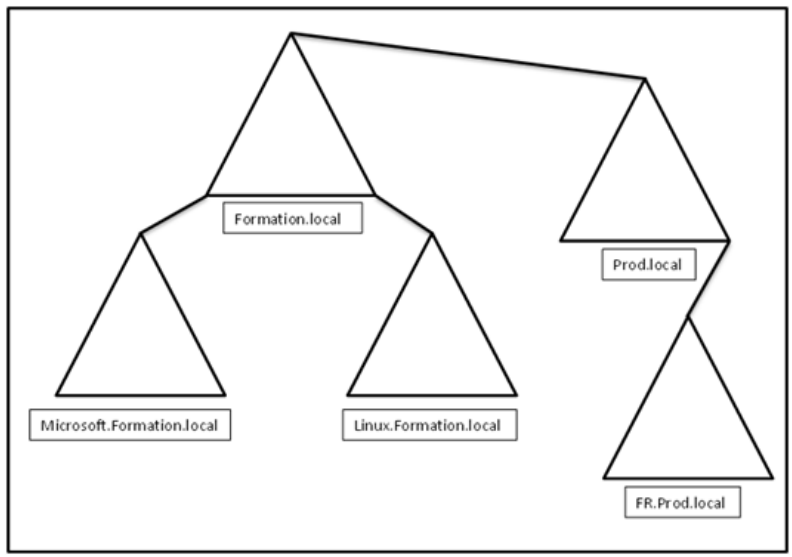


- **Dossier Computers** : répertoire par défaut, les comptes ordinateur sont positionnés à cet endroit lors de l'ajout de nouveaux postes de travail.
- **Unité d'organisation Domain Controllers** : emplacement par défaut pour les comptes des contrôleurs de domaine. Cette OU est la seule présente lors de la création du domaine. La stratégie de groupe Default Domain Controller Policy est positionnée sur cette unité d'organisation.

3. La forêt Active Directory

Une forêt est constituée d'un ou plusieurs domaines Active Directory. On parle de domaine racine pour le premier domaine de la forêt, de plus ce dernier donne son nom à la forêt. Dans notre maquette le domaine racine est Formation.local, la forêt a donc le nom de ce dernier, soit Formation.local. On trouve dans une forêt Active Directory une seule configuration et un seul schéma, ceux-ci sont partagés par l'ensemble des contrôleurs de domaine présents dans la forêt. Elle a également pour but la mise en place d'une frontière de sécurité, les autres forêts n'ont aucun droit sur elle et aucune donnée n'est répliquée à l'extérieur de la forêt.

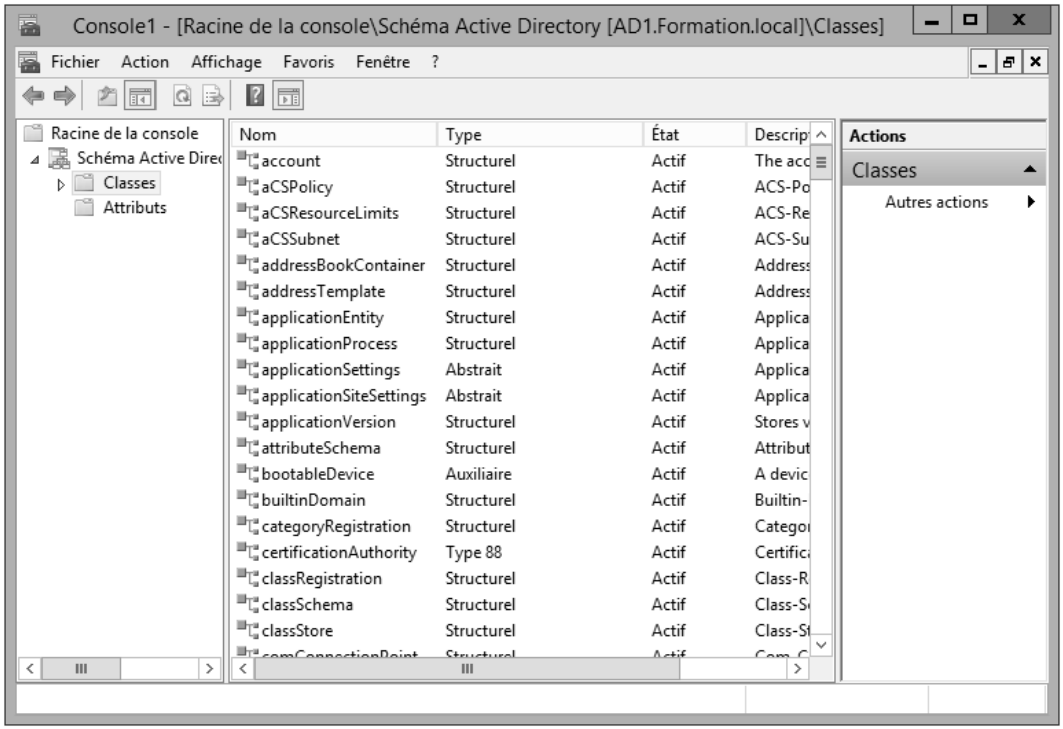
Une forêt Active Directory est donc composée d'une suite de domaines appelée également une arborescence de domaines, ces derniers partagent un espace de noms contigu. La relation entre les domaines d'une même arborescence est de type parent/enfant. Un domaine qui dispose d'un espace de noms différent fait partie d'une arborescence différente.



Le domaine représente lui aussi une limite de sécurité car l'objet utilisateur qui permet l'authentification d'une entité (personne physique de l'entreprise…) est défini par domaine. Ce dernier contient au moins un contrôleur de domaine, deux étant recommandés pour des raisons de disponibilité. Ce type de serveur a la responsabilité de l'authentification des objets utilisateurs et ordinateurs dans un domaine AD.

4. Le schéma Active Directory

Le schéma Active Directory est un composant qui permet de définir les objets ainsi que leurs attributs pouvant être créés dans Active Directory. Lors de la création d'un nouvel objet, le schéma est utilisé afin de récupérer les attributs de ce dernier et leurs syntaxes (booléen, entier...).



Ainsi, lors de la création de l'objet, l'annuaire Active Directory connaît chaque attribut et le type de données à stocker. Lors de migration Active Directory ou en cas d'installation de certaines applications (Exchange, etc.) le schéma doit être mis à jour. Cette opération vise à rajouter des objets et leurs attributs qui pourraient être par la suite créés (exemple : une boîte mail). Cette opération ne peut être effectuée que sur un contrôleur de domaine ayant le rôle de maître de schéma, l'utilisateur qui effectue l'opération doit être membre du groupe Administrateur du schéma. Après avoir apporté la modification, cette dernière est répliquée à l'ensemble des contrôleurs de domaine de la forêt.

Par défaut le logiciel enfichable Schéma Active Directory est caché. Pour pouvoir l'activer, il est nécessaire de taper la commande **regsvr32 schmmgmt.dll** dans la console **Exécuter**.