


جامعة الحسن الأول
UNIVERSITÉ HASSAN 1^{er}


Université Hassan 1^{er}
Faculté des Sciences et techniques de Settat
Département : MIA
LS-GI

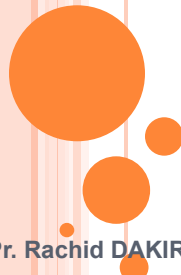


جامعة الحسن الأول
UNIVERSITÉ HASSAN 1^{er}

Filière : Génie Informatique

Module : Administration système et la sécurité





Pr. Rachid DAKIR

Année Universitaire : 2021-2022

Chapitre II : Administration système

LST : GI- AU : 2021-2022



Windows Server™
Active Directory





Active Directory

Professeur : Rachid DAKIR

LST : GI

A.U : 2021-2022

Chapitre II : Administration système

LST : GI- AU : 2021-2022

➤ Qu'est ce qu'un Active Directory

Active directory est un service d'annuaire permet de centraliser, de structurer et de contrôler, localiser et utiliser des ressources (Serveurs, Imprimantes, Utilisateurs dans un environnement Windows (2003/2008/2012 ou 2016) Server et de les stocker sur des objets.

Il permet aux utilisateurs de localiser et gérer ces ressources facilement d'une manière centralisée.



➔ L'objectif étant de centraliser deux fonctionnalités essentielles : l'**identification** et l'**authentification** au sein d'un système d'information (réseau d'ordinateurs qui utilisent le système Windows, macOS et encore Linux)

➔ Attribution et l'application de stratégies ainsi que l'installation de mises à jour critiques par les administrateurs.

Professeur : Rachid DAKIR

LST : GI

A.U : 2021-2022

Chapitre II : Administration système

LST : GI- AU : 2021-2022

➤ Les objectifs de l'AD

❑ **Administration centralisée et simplifiée** : La gestion des objets, notamment des comptes utilisateurs et ordinateurs est simplifiée, car tout est centralisé dans l'annuaire Active Directory. De plus, on peut s'appuyer sur cet annuaire pour de nombreuses tâches comme le déploiement de stratégies de groupe sur ces objets.

❑ **Unifier l'authentification** : Un utilisateur authentifié sur une machine pourra accéder aux ressources stockées sur d'autres serveurs ou ordinateurs enregistrés dans l'annuaire (à condition d'avoir les autorisations nécessaires). Ainsi, une authentification permettra d'accéder à tout un système d'information, c.-à-d un seul compte peut permettre un accès à tout le système d'information, ce qui est fortement intéressant pour les collaborateurs.

Administration
centralisée et
simplifiéeUnifier
l'authentification

Professeur : Rachid DAKIR

LST : GI

A.U : 2021-2022

Chapitre II : Administration système

LST : GI- AU : 2021-2022

➤ Les objectifs de l'AD

Lorsque un utilisateur veut accéder à un système d'information il doit dans un premier temps effectuer une procédure d'identification et d'authentification.

➔ **Identification** : est une phase qui consiste à établir l'identité de l'utilisateur. Elle permet répondre à la question : "Qui êtes vous ?". L'utilisateur utilise un identifiant (que l'on nomme "Compte d'accès", "Nom d'utilisateur" ou "Login" en anglais) qui l'identifie et qui lui est attribué individuellement. Cet identifiant est unique.

➔ **Authentification** est une phase qui permet à l'utilisateur d'apporter la preuve de son identité. Elle intervient après la phase dite d'identification. Elle permet de répondre à la question : "Êtes-vous réellement cette personne ?". L'utilisateur utilise un authentifiant ou "code secret" que lui seul connaît.

➔ **Autorisation** cumule l'identification et l'authentification afin d'accéder à un service. Quand une personne est autorisée, cela signifie qu'elle s'est préalablement enregistrée et que l'outil accorde l'accès à l'utilisateur. L'autorisation consiste à vérifier qu'une tentative de connexion est légitime. L'autorisation est accordée après une authentification réussie.

Professeur : Rachid DAKIR

LST : GI

A.U : 2021-2022

L'authentification est une information qui consiste à vérifier les données

Chapitre II : Administration système

LST : GI- AU : 2021-2022

➤ Les objectifs de l'AD

❑ **Identifier les objets sur le réseau** : chaque objet enregistré dans l'annuaire est unique, ce qui permet d'identifier facilement un objet sur le réseau et de le retrouver ensuite dans l'annuaire.

Référencer les utilisateurs et ordinateurs

❑ **Référencer les utilisateurs et les ordinateurs** : l'annuaire s'apparente à une énorme base de données qui référence les utilisateurs, les groupes et les ordinateurs d'une entreprise. On s'appuie sur cette base de données pour réaliser de nombreuses opérations : authentification, identification, stratégie de groupe, déploiement de logiciels, etc.

Identifier les objets sur le réseau

- Fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows.
- Attribution et application de stratégies, la distribution de logiciels, et l'installation de mises à jour par les administrateurs.
- 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, etc.

Professeur : Rachid DAKIR

LST : GI

A.U : 2021-2022

Chapitre II : Administration système

LST : GI- AU : 2021-2022

► Les protocoles de l'AD

Le protocole principal de l'active directory qui permet d'accès aux annuaires (permet d'ajouter, de modifier et de supprimer des données enregistrées dans *Active Directory*, et qui permet en outre de rechercher et de récupérer ces données) est LDAP (389/TCP).

N'importe quelle application cliente conforme à LDAP peut être utilisée pour parcourir et interroger *Active Directory* ou pour y ajouter, y modifier ou y supprimer des données.

→ Un protocole qui permet de gérer des annuaires

Il existe d'autres protocoles sont indispensables au bon fonctionnement de l'AD :

- Kerberos : Il assure l'authentification de manière sécurisée avec un mécanisme de distribution de clés.
- DNS (Domain Name Server) : 53/TCP , Résolution, Dénomination,
- des objets AD
- SMTP : Simple mail Tranfer Protocol ,25/TCP, (Vérification que chaque utilisateur à son propose sessorin/ transfert des sessions , Emails de contact : dakir@info.ma
- RPC : Remote protocol call, responsable de la partie réplication entre deux domaines

Professeur : Rachid DAKIR

LST : GI

A.U : 2021-2022

Chapitre II : Administration système

LST : GI- AU : 2021-2022

► Les composants de l'Active Directory

□ Les objets :

Serveurs, domaines, sites, utilisateurs, ordinateurs, groupe, lien de site, imprimantes, dossier partagé...

Nom	Description
Ordinateur	Les ordinateurs clients intégrés au domaine, mais aussi les serveurs et les contrôleurs de domaine
Contact	Enregistrer des contacts, sans autorisation d'authentification
Groupe	Regrouper des objets au sein d'un groupe, notamment pour simplifier l'administration (attribution de droits à un service « Informatique » qui correspond à un groupe nommé « Informatique », par exemple)
Unité d'organisation	Dossier pour créer une arborescence et organiser les objets.
Imprimante	Ressource de type « Imprimante »
Utilisateur	Comptes utilisateurs qui permettent de s'authentifier sur le domaine, et accéder aux ressources, aux ordinateurs

Professeur : Rachid DAKIR

LST : GI

A.U : 2021-2022

Chapitre II : Administration système

LST : GI- AU : 2021-2022

► La structure de l'Active Directory

❑ Les classes et les attributs :

Au sein de l'annuaire Active Directory, il y a différents types d'objets, comme par exemple les utilisateurs, les ordinateurs, les serveurs, les unités d'organisation ou encore les groupes. En fait, ces objets correspondent à **des classes**, c'est-à-dire **des objets disposant des mêmes attributs**.

Certains objets peuvent être des containers d'autres objets :

➔ **Les groupes** permettront de contenir plusieurs objets de types utilisateurs afin de les regrouper et de simplifier l'administration.

➔ **Les unités d'organisation** sont des containers d'objets afin de faciliter l'organisation de l'annuaire et de permettre une organisation avec plusieurs niveaux.

Professeur : Rachid DAKIR

LST : GI

A.U : 2021-2022

Chapitre II : Administration système

LST : GI- AU : 2021-2022

► Les composants de l'Active Directory

Chaque objet dispose d'identifiants uniques qui sont représentés par deux attributs :

❖ DistinguishedName

Cet identifiant unique également appelé « DN » représente le chemin LDAP qui permet de trouver l'objet dans l'annuaire Active Directory. Lors de l'étude du protocole LDAP, nous avons déjà vu un exemple de DN.

Exemple :

- **Domaine** : uh1.ma
- **Unité d'organisation** où se trouve l'objet : informatique
- **Nom de l'objet** : sami

Le DN de cet objet utilisateur sera :

cn=sami,ou=informatique,dc=uh1,dc=ma

Professeur : Rachid DAKIR

LST : GI

A.U : 2021-2022

Chapitre II : Administration système		LST : GI- AU : 2021-2022								
<p>➤ Les composants de l'Active Directory</p> <p>Dans ce DN, on trouve un chemin qui permet de retrouver l'objet, différents éléments sont utilisés :</p> <table border="1"> <thead> <tr> <th>Identification de l'élément</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>cn</td> <td><i>CommonName</i> – Nom commun – Nom de l'objet final ciblé</td> </tr> <tr> <td>ou</td> <td><i>OrganizationalUnit</i> – Unité d'organisation</td> </tr> <tr> <td>dc</td> <td>Composant de domaine – Utilisé pour indiquer le domaine cible, avec un élément « dc » par partie du domaine</td> </tr> </tbody> </table> <p>➔ Chaque objet de l'annuaire est identifié par 3 paramètre :</p> <p>➔ Le DN peut être très long si l'arborescence de l'annuaire est importante et que l'objet se trouve au fin fond de cette arborescence. De plus, le DN peut changer régulièrement si l'objet est déplacé, ou si une unité d'organisation dont il dépend est renommée puisqu'il contient de manière nominative les objets.</p>			Identification de l'élément	Description	cn	<i>CommonName</i> – Nom commun – Nom de l'objet final ciblé	ou	<i>OrganizationalUnit</i> – Unité d'organisation	dc	Composant de domaine – Utilisé pour indiquer le domaine cible, avec un élément « dc » par partie du domaine
Identification de l'élément	Description									
cn	<i>CommonName</i> – Nom commun – Nom de l'objet final ciblé									
ou	<i>OrganizationalUnit</i> – Unité d'organisation									
dc	Composant de domaine – Utilisé pour indiquer le domaine cible, avec un élément « dc » par partie du domaine									
Professeur : Rachid DAKIR		LST : GI A.U : 2021-2022								

Chapitre II : Administration système		LST : GI- AU : 2021-2022
<p>➤ Les composants de l'Active Directory</p> <p>Chaque objet dispose d'identifiants uniques qui sont représentés par deux attributs :</p> <p>❖ Le GUID</p> <p>Identificateur global unique qui permet d'identifier un objet d'un annuaire Active Directory. Il correspond à l'attribut « ObjectGUID » dans le schéma Active Directory.</p> <p>Il est attribué à l'objet dès sa création et ne change jamais, même si l'objet est déplacé ou modifié. Le GUID suit un objet de la création jusqu'à la suppression. Codé sur 128 bits, le GUID d'un objet est unique au sein d'une forêt et il est généré par un algorithme qui garantit son unicité. Des informations aléatoires, d'autres non, comme l'heure de création de l'objet</p>		
Professeur : Rachid DAKIR		LST : GI A.U : 2021-2022

Chapitre II : Administration système

LST : GI- AU : 2021-2022

➡ Les composants de l'Active Directory

- Schéma :

Par défaut, tout annuaire Active Directory dispose de classes prédéfinies ayant chacune une liste d'attributs bien spécifique, et propre à tout annuaire, cela est défini grâce à un **schéma référentiel** .

Le schéma contient la définition de toutes les classes et de tous les attributs disponibles et autorisés au sein de votre annuaire.

➔ Le schéma Active Directory stocke la définition de tous les objets d'Active Directory (ex : nom, prénom pour l'objet utilisateur).

→ Le schéma comprend deux types de définitions : les classes d'objets et les attributs.

Classes : Computer, User, Group, UO, Printer, Shared Folder.....

Attibuts : Login, Descition, Name, Display name , Full name , Age,.....

Professeur : Rachid DAKIR

LST : GI

A.U : 2021-2022

Chapitre II : Administration système

LST : GI- AU : 2021-2022

➡ Les composants de l'Active Directory

- **Schéma :**

le schéma est protégé et les modifications contrôlées, puisque seuls les membres du groupe « **Administrateurs du schéma** » peuvent, par défaut, effectuer des modifications.

Le schéma comprend deux types de définitions :

- **Les classes d'objets** : Décrit les objets d'Active Directory qu'il est possible de créer. Chaque classe est un regroupement d'attributs.
- **Les attributs** : Ils sont définis une seule fois et peuvent être utilisés dans plusieurs classes

	Nom	Syntaxe	Ent	Description
Utilisateur et ordinateur act	<code>_acCspExpires</code>	Entier long intervalle	Actif	Account Expires
Schema Active Directory (S)	<code>_acCspAccountHistory</code>	Chaine Unicode	Actif	Account Name-History
Classes	<code>_acCspAggregate-Interv</code>	Entier long intervalle	Actif	ACS-Aggregate-Interv
Attributs	<code>_acCspAllocateRSP-PB</code>	Entier long intervalle	Actif	ACS-Allocate-RSP-PB
	<code>_acCspCacheTimeout</code>	Entier	Actif	ACS-Cache-Timeout
	<code>_acCspDirection</code>	Entier	Actif	ACS-Direction
	<code>_acCspOSM-DeadlineTime</code>	Entier	Actif	ACS-OSM-DeadlineTime
	<code>_acCspOSM-Priority</code>	Entier	Actif	ACS-OSM-Priority
	<code>_acCspOSM-Refresh</code>	Entier	Actif	ACS-OSM-Refresh
	<code>_acCspEnableACS-Service</code>	Boolean	Actif	ACS-Enable-ACS-Service
	<code>_acCspEnableRSP-Account</code>	Boolean	Actif	ACS-Enable-RSP-Account
	<code>_acCspEnableRSP-Messages</code>	Boolean	Actif	ACS-Enable-RSP-Messages
	<code>_acCspEventLog-Ent</code>	Entier	Actif	ACS-Event-Log-Ent
	<code>_acCspIdentName</code>	Chaine Unicode	Actif	ACS-Ident-Name

Classes : Computer, User, Group, UO, Printer, Shared Folder.....

Attibuts : Login, Descition, Name, Display name , Full name , Age,.....

Professeur : Rachid DAKIR

LST : GI

A.U : 2021-2022

Chapitre II : Administration système		LST : GI- AU : 2021-2022
<p>► Les composants de l'Active Directory</p>		
Nom de l'attribut dans le schéma	Nom de l'attribut dans la console Active Directory	Description
sAMAccountName	« Nom d'ouverture de session de l'utilisateur »	Valeur que devra utiliser l'objet pour s'authentifier sur le domaine
UserPrincipalName	« Nom d'ouverture de session de l'utilisateur » concaténé au nom du domaine sous la forme « @it-connect.local »	Nom complet de l'utilisateur avec le domaine inclus. Également appelé UPN
description	Description	Description de l'objet
mail	Adresse de messagerie	Adresse de messagerie attribuée à l'objet
adminCount	-	Égal à « 1 » s'il s'agit d'un compte de type « Administrateur », égal à « 0 » s'il ne l'est pas
DisplayName	Nom complet	Nom complet qui sera affiché pour cet utilisateur
givenName	Prénom	Prénom de l'utilisateur
logonCount	-	Nombre d'ouverture de session réalisée par cet objet
accountExpires	Date d'expiration du compte	Date à laquelle le compte ne sera plus utilisable (peut être vide)
ObjectSID	-	Identifiant de sécurité unique qui permet d'identifier un objet
pwdLastSet	-	Dernière fois que le mot de passe fût modifié
userAccountControl	-	État du compte – Une dizaine de codes différents sont possibles
Professeur : Rachid DAKIR		LST : GI A.U : 2021-2022

Chapitre II : Administration système		LST : GI- AU : 2021-2022
<p>► Les composants de l'Active Directory</p>		
<p>❑ Catalogue :</p> <p>Le catalogue global est un contrôleur de domaine qui dispose d'une version étendue de l'annuaire <u>Active Directory</u>. En fait, comme tout contrôleur de domaine, il dispose d'une copie complète de l'annuaire Active Directory de son domaine, mais en supplément il dispose de :</p> <ul style="list-style-type: none"> → Un répliqua partiel pour tous les attributs contenus dans tous les domaines de la forêt → Toutes les informations sur les objets de la forêt ▪ <u>Le catalogue global contient une partie des attributs les plus utilisés de tous les objets Active Directory.</u> ▪ <u>Il contient les informations nécessaires pour déterminer l'emplacement de tout objet de l'annuaire.</u> ▪ <u>Il regroupe des éléments provenant de l'ensemble de la forêt, c'est en quelque sorte un annuaire central.</u> ▪ <u>Capable de localiser des objets dans l'ensemble de la forêt, car il a une vue d'ensemble sur tous les objets. Les contrôleurs de domaine classique s'appuieront sur lui pour justement localiser des objets dans une forêt.</u> 		
Professeur : Rachid DAKIR		LST : GI A.U : 2021-2022

Chapitre II : Administration système

LST : GI- AU : 2021-2022

Les composants de l'Active Directory

Catalogue :

Le catalogue global est un point central dans un environnement où il y a plusieurs domaines, puisqu'il doit faire le lien entre tous les objets de tous les domaines de la forêt.

Lorsqu'il n'y a qu'un seul domaine dans la forêt, le catalogue global perd tout son intérêt, car les autres contrôleurs de domaine sauront « se débrouiller seul ».

Le catalogue global assure quatre fonctions clés auprès du système Active Directory et pour « venir en aide » aux autres contrôleurs de domaine de la forêt, à savoir :



Professeur : Rachid DAKIR

LST : GI

A.U : 2021-2022

Chapitre II : Administration système

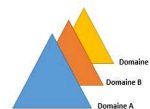
LST : GI- AU : 2021-2022

Les composants de l'Active Directory

Catalogue :

Exemple :

Deux contrôleurs de domaine se trouvent au sein du domaine A, un contrôleur de domaine « standard » et un second qui dispose du rôle de « catalogue global ».



→ Le contrôleur AD standard disposera de la partition d'annuaire du domaine A

→ Le contrôleur de domaine catalogue global dispose des partitions d'annuaire du domaine A, mais aussi du domaine B et du domaine C

Le premier contrôleur de domaine créé au sein d'une forêt est automatiquement catalogue global. Autrement dit, lorsque vous montez un Active Directory, vous créez automatiquement un nouveau domaine dans une nouvelle forêt, ce qui implique que le contrôleur de domaine soit catalogue global.

Professeur : Rachid DAKIR

LST : GI

A.U : 2021-2022

Chapitre II : Administration système	LST : GI- AU : 2021-2022
<p>➤ Les composants de l'Active Directory</p> <ul style="list-style-type: none"> ▪ Les partitions d'annuaire <p>La base de données Active Directory est divisée de façon logique en trois partitions de répertoire (appelé « Naming Context »).</p> <ul style="list-style-type: none"> ▪ La partition de schéma : Contient l'ensemble des définitions des classes et attributs d'objets, qu'il est possible de créer au sein de l'annuaire Active Directory. Cette partition est unique au sein d'une forêt. ▪ La partition de configuration : Contient la topologie de la forêt (informations sur les domaines, les liens entre les contrôleurs de domaines,etc.). Cette partition est unique au sein d'une forêt. ▪ La partition de domaine : Contient les informations de tous les objets d'un domaine (ordinateur, groupe, utilisateur, etc.). Cette partition est unique au sein d'un domaine. 	
Professeur : Rachid DAKIR	LST : GI A.U : 2021-2022

Chapitre II : Administration système	LST : GI- AU : 2021-2022
<p>➤ La structure de l'Active Directory</p> <ul style="list-style-type: none"> ❑ Structure logique : <p>La structure logique d'Active Directory offre une méthode efficace pour concevoir une hiérarchie</p> <ul style="list-style-type: none"> ▪ Domaine : est un ensemble d'ordinateurs et/ou d'utilisateurs qui partagent une même base de données d'annuaire et chaque domaine est identifié par un nom ▪ Unité d'organisation : est un objet conteneur utilisé pour organiser les objets au sein du domaine. ▪ Arborescence : est un ensemble de domaines partageant un nom commun. ▪ Forêt : est un ensemble de domaines (ou d'arborescences) n'ayant pas le même nom commun mais partageant un schéma et un catalogue global commun. 	
Professeur : Rachid DAKIR	LST : GI A.U : 2021-2022

Chapitre II : Administration système

LST : GI- AU : 2021-2022

► La structure de l'Active Directory

□ Structure logique :

▪ Domaine :

Ensemble d'ordinateurs et/ou d'utilisateurs qui partagent une même base de données d'annuaire et chaque domaine est identifié par un nom



→ Regroupement logique de comptes utilisateurs, ordinateurs ou de groupes. Les objets qui sont créés sont stockés dans une base de données annuaire

→ Au sein du domaine schématisé ci-dessus, on retrouvera tout un ensemble d'Unités d'Organisation remplies d'objets de différentes classes : utilisateurs, ordinateurs, groupes, contrôleurs de domaine, etc.

Professeur : Rachid DAKIR

LST : GI

A.U : 2021-2022

Chapitre II : Administration système

LST : GI- AU : 2021-2022

► La structure de l'Active Directory

□ Structure logique :

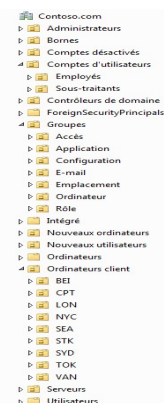
▪ Unité d'organisation :

Ce sont des conteneurs permettent de regrouper des objets dans un domaine.

On crée des unités d'organisation pour :

- ❖ Déléguer des autorisations administratives
- ❖ Appliquer la stratégie de groupe

→ conteneur utilisé pour organiser les objets au sein du domaine.



Professeur : Rachid DAKIR

LST : GI

A.U : 2021-2022

Chapitre II : Administration système

LST : GI- AU : 2021-2022

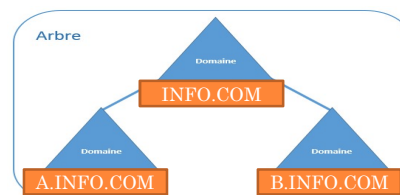
► La structure de l'Active Directory

□ Structure logique :

▪ Arbre :

Lorsqu'un domaine principal contient plusieurs sous-domaines on parle alors d'arbre, où chaque sous-domaine au domaine racine représente une branche de l'arbre.

- ❖ Un arbre est un regroupement hiérarchique de plusieurs domaines.
- ❖ Partage même nom commun comme arbre



Professeur : Rachid DAKIR

LST : GI

A.U : 2021-2022

Chapitre II : Administration système

LST : GI- AU : 2021-2022

► La structure de l'Active Directory

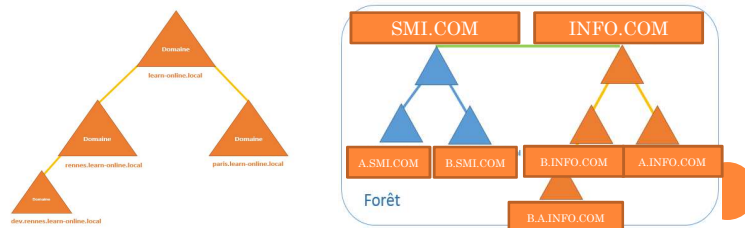
□ Structure logique :

▪ Forêt :

Une forêt est un regroupement d'une ou plusieurs arborescences de domaine, autrement dit d'un ou plusieurs arbres.

Ces arborescences de domaine sont indépendantes et distinctes bien qu'elles soient dans la même forêt.

- ❖ Les différentes arborescences d'une forêt ne partagent pas le même espace de nom et la même structure.



Professeur : Rachid DAKIR

LST : GI

A.U : 2021-2022