LDAP

**Présentation et objectifs du cours**

Ce cours a pour objectif de vous présenter les annuaires LDAP et une implémentation libre proposant à la fois un serveur LDAP mais un ensemble d'outils clients : le projet OpenLDAP.

Vous allez découvrir à travers ce cours les notions liées aux annuaires LDAP. Vous apprendrez également comment mettre en œuvre un serveur OpenLDAP et utiliser les commandes clientes fournies par le projet

**Organisation du travail**

Le cours est divisé en deux parties majeures :

• une partie théorique concernant les annuaires LDAP

• une partie pratique présentant le projet OpenLDAP

La première partie est purement théorique. Elle présente les concepts liés à tous les annuaires LDAP. Il est indispensable de bien assimiler les notions qui y sont présentées car elles constituent la base de ce qui est présenté dans la seconde partie avec OpenLDAP.

Cette seconde partie présente comment mettre en place un annuaire. De nombreuses commandes seront utilisées, il est conseillé d'effectuer les manipulations en même temps sur l'ordinateur. Cette partie constitue en quelques sortes un exercice où il est expliqué pas à pas comment configurer et utiliser l'annuaire.

1. **Introduction**

L'informatique et la gestion de l'information prend une place de plus en plus importante dans notre société, particulièrement en entreprises. La multiplication des applications et des serveurs rend cette information difficile à maîtriser car très volitive et éparse. Ceci entraîne bien souvent une obsolescence, voire une incohérence des données stockées. Les annuaires LDAP offrent une réponse à ce problème en proposant de centraliser les informations et, par le biais d'un protocole standardisé, d'y connecter des applications clientes.

1. **Définition d'un annuaire**
2. **Qu'est-ce qu'un annuaire ?**

Vous utilisez fréquemment des annuaires : prenons l'exemple de l'annuaire téléphonique. Cet annuaire regroupe différentes entrées contenant chacune des informations particulières : nom, prénom, numéro de téléphone et adresse. Ces informations sont classées par département, puis par ville, puis enfin par nom.

Voici les caractéristiques communes aux annuaires :

• Un annuaire présente un **ensemble défini de données** (annuaire : nom, prénom, numéro de téléphone, adresse)

• Il **organise** ces données (annuaire : classées par département, villes, nom)

• Il offre un service de **consultation** (annuaire : diffusion au format papier)

• Il est **plus consulté** que mis à jour

• Il est **disponible** de manière permanente

Le standard LDAP tient compte de ces différentes caractéristiques. Nous verrons comment elles sont mises en œuvre au cours de la formation.

1. **Les concepts du protocole LDAP**
2. **Quatre modèles**

On a coutume de regrouper les caractéristiques et fonctionnalités de l'annuaire LDAP sous la forme de quatre modèles :

• Le modèle de nommage : définit comment l'information est stockée et organisée

• Le modèle fonctionnel : définit les services fournis par l'annuaire (recherche, ajout, ...)

• Le modèle d'information : définit le type d'informations stockées

• Le modèle de sécurité : définit les droits d'accès aux ressources

Ces différents points seront abordés au cours de la formation

1. **Un protocole**

LDAP signifie "Lightweight Directory Access Protocol".

LDAP est un protocole, ce qu'il signifie que son rôle est de présenter des informations. Un serveur LDAP agit en tant qu'intermédiaire entre une source de données et un client.

Nous verrons qu'en tant qu'intermédiaire il définit quelques conventions, notamment l'organisation des données qu'il présente qui sera sous forme hiérarchique, mais aussi un format d'échange standard.

LDAP fonctionne sur le port TCP 389 (par défault).

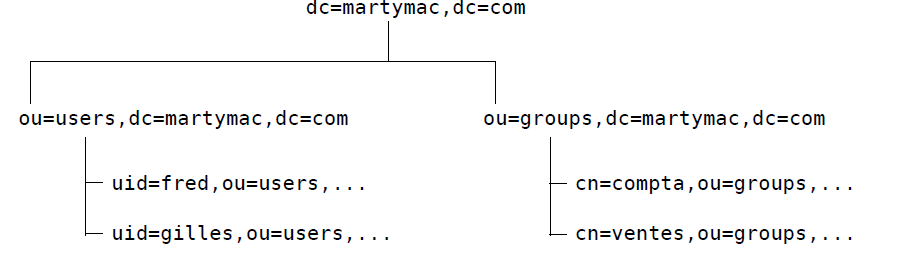
1. **Organisation des données (modèle de nommage)**
2. **Introduction**

Le modèle de nommage est la manière dont sont organisées les données dans l'annuaire.

1. **Une représentation hiérarchique des données**

LDAP organise les données de manière hiérarchique dans l'annuaire. Ceci signifie que toutes les informations découlent d'une seule et même "racine

Voici un exemple d'arborescence LDAP :



Cette arborescence est liée au nommage de chaque élément : un élément marque son appartenance à l'élément supérieur en en reprenant le nom, qu'il complète par le sien.

Ainsi, en étudiant simplement le nom de l'élément :**"cn=ventes,ou=groups,dc=martymac,dc=com"**

Il est possible de le situer dans la hiérarchie : il est situé sous l'élément "**ou=groups**" qui lui-même est situé sous l'élément "**dc=martymac,dc=com**".

* Termes à connaître

Avant de poursuivre, voici quelques termes à connaître :

• Chaque élément est appelé une **entrée** (an entry). Une entrée peut être un branchement (un **noeud**, a node) ou un élément terminal (une **feuille**, a leaf).

• Chaque élément possède un **DN** (Distinguished Name). Le DN est le nom complet de l'élément qui permet de le positionner dans l'arborescence. Il est unique dans l'annuaire.

Exemple : "cn=ventes,ou=groups,dc=martymac,dc=com"

• Chaque élément possède également un **RDN** (Relative Distinguished Name). Le RDN est la partie du **DN** de l'élément qui est relative au **DN** supérieur. Le RDN d'un élément ne permet pas de l'identifier de manière abolue dans l'annuaire. Exemple : "cn=ventes"

• La **racine** est l'élément supérieur de tous les autres, c'est la base de l'arborescence. On l'appelle **root** en anglais, parfois on parle de "**root DN**". Exemple : "dc=martymac,dc=com"

Les DN de chaque entrées sont composés au moins d'un attribut de l'élément (par exemple "cn" ou "uid") et de sa valeur. Un attribut est l'une des caractéristiques de cet élément.

Remarquez que la racine choisie ici est composée du nom du domaine où est hébergé notre serveur LDAP, martymac.com, décomposé en "dc" (Domain Components) pour obtenir dc=martymac,dc=com.

L'arbre se découpe ensuite en deux "ou" (Organisational Units) qui constituent deux branchements : "users" et "groups", dans lesquels nous trouvons ensuite les entrées feuilles de notre arbre : les utilisateurs et les groupes.

Chacune des entrées de notre arbre correspond à un type de donnée particulier, défini par une classe d'objet. Nous étudierons ces notions par la suite.

1. **Accéder à l'annuaire (modèle fonctionnel)**

Il existe plusieurs types d'opérations que l'on peut effectuer sur l'annuaire, voici les plus importantes :

• Rechercher une entrée suivant certains critères

• S'authentifier

• Ajouter une entrée

• Supprimer une entrée

• (Modifier une entrée)

• Renommer une entrée

Certaines de ces actions, notamment la recherche, nécessitent des outils particuliers pour nous faciliter l'accès à l'annuaire.

1. **Les données contenues dans l'annuaire (modèle d'information)**
2. **Les attributs**

Un attribut est une valeur contenue dans une entrée. Une entrée peut bien entendu contenir plusieurs attributs.

1. **Les classes d'ojets**

L'objectClass d'une entrée est un attribut qui permet de cataloguer cette entrée. Un objectClass définit un regroupement d'attributs **obligatoires** ou **autorisés** pour une entrée.

Une entrée peut posséder un ou plusieurs objectClass. Ce sont ces objectClass qui définissent la présence de tous les autres attributs.

1. **Le format LDIF**

Les données contenues dans l'annuaire sont présentées dans un certain format : il s'agit du format LDIF (LDAP Data Interchange Format - RFC 2849).

1. **La sécurité (modèle de sécurité)**

Lorsque vous mettez en place un annuaire d'entreprise, il convient de réfléchir au modèle de sécurité que vous souhaitez appliquer. LDAP fournit plusieurs mécanismes permettant de mener à bien votre projet.

Ex :

🡪 Le chiffrement des communications (SSL/TLS)

🡪SASL