**LDAP**

RFC 2251

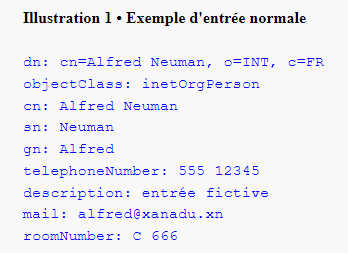
RFC 4511

1. **Annuaire**

* Annuaire = BDD spécialisée (mais annuaire uniquement optimisé pour la lecture)

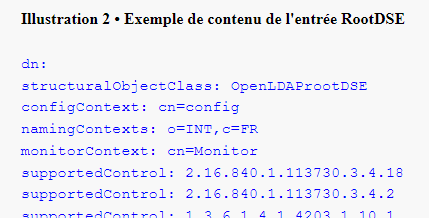
Permet de distribuer des certificats, d’authentifier des personnes…

* Historique des annuaires électroniques :
  + Unix /etc/passwd
  + NIS : network information services
  + DNS
  + Whois
  + X.500
  + LDAP : version allégée de DAP (accès au service d’annuaires X.500 de l’OSI)
* Vocabulaire :
  + Entrée = objet du monde réel (ex personne, imprimante, un ordinateur, une liste, un rôle…)
    - Entrées normales

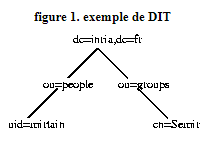


* + - Entrées opérationnelles : spécifique au serveur, permettent de le gérer

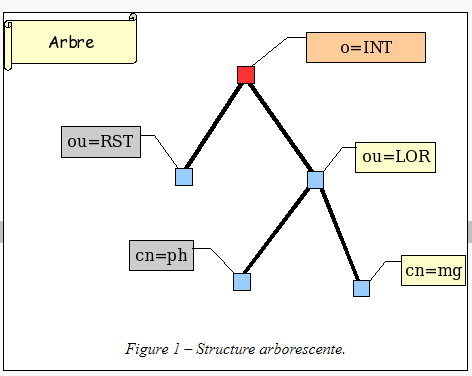
Chaque serveur possède une entrée "root Directory Specific Entry" : descriptions des arbres et des fonctionnalités du serveur



* + Directory Information Tree : Chaque nœud = une entrée



* + Nommage : identification des entrées



Accéder à une entrée :

* Un nom.
* Un chemin dans la BDD

**Nom distingué (DN)** = nom unique pour chaque entrée obtenu par construction = chemin d’accès

Exemple ici : le DN de l’entrée cn=mg est : **cn=mg, ou=LOR, o=INT, c=FR**

* + Attributs : Différentes informations d’une entrée : exemple cn…

Le nom des attributs est à la charge de l’administrateur mais o=INT et c=FR est figé.

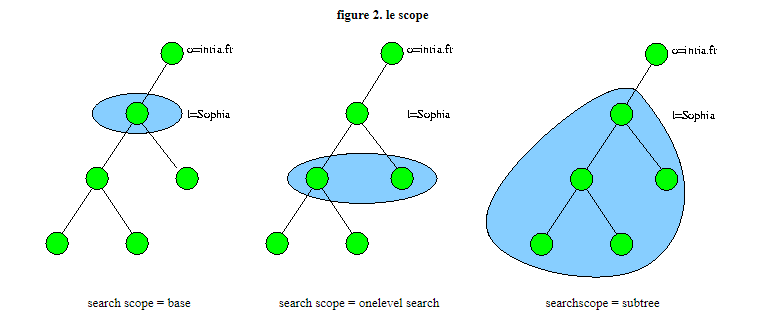
o : organization

ou : organizational unit

c : country

cn : common name

* Classe d’objet : moule d’une entrée :attributs possibles d’une entrée :
  + Liste d’attributs obligatoires
  + Liste d’attributs optionnels
  + 2 types :
    - Classe structurelle : une entrée découle de ce type
    - Classe auxiliaire : étend les attributs d’une entrée : héritage ?
* Schéma : définition des classes et attributs propres à un serveur, doit être publié
* Recherche :
  + Base= : base de la recherche (racine ou autre)
  + Profondeur : paramètre scope
    - Scope=base : profondeur = uniquement la base
    - Scope=one : profondeur = uniquement celles à un niveau de la base
    - Scope=sub : base+ tous les niveaux descendants



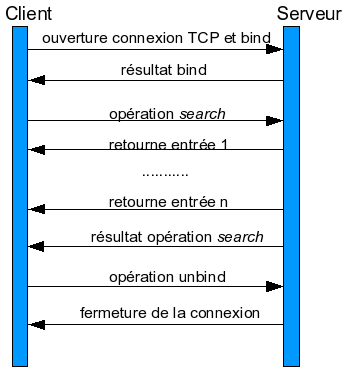
* Implémentation du protocole LDAP :
  + Dans la BDD Active directory de Microsoft
  + OpenLDAP
  + …

1. **Sécurité d’un annuaire :**

* SSL pour se connecter au serveur LDAP (certificats du serveur [et clients])
* Authentification diverses (login/mdp)
* Qui peut voir /modifier et quoi via ACL, suppose une authentification préalable

1. **Protocole LDAP**

* Données echangées au format BER : basic encoding rules (mais des fois ASCII, base64…)
* Utilise TCP ou TLS.



1. **Trames**
2. **Exemple**