

Les annuaires

Présentation

Un annuaire est une base de données centralisée dont la fonction est de retourner les attributs d'un objet via une fonction de recherche.

Les objets sont de différents types

Un objet utilisateur possédant les attributs (nom, prénom, numéro de téléphone, etc.)

Un objet imprimante possédant les attributs (nom, adresse IP, localisation...)

Un ordinateur (nom, adresse IP, localisation...)

Un groupe d'utilisateurs

Les annuaires applicatifs

Lotus Notes

MS Exchange

Les annuaires système/réseau

Sun NIS

Microsoft AD

Les annuaires multi-usages

X.500 pour les opérateurs télécom

LDAP

LDAP

Lightweight Directory Access Protocol est un annuaire multi-usage qui est construit sur 7 fonctions :

Le protocole

Le modèle **d'information**

Le modèle **de nommage**

Le modèle **fonctionnel**

Le modèle **de sécurité**

Le modèle **de duplication**

Les API de développement

Le protocole

C'est un protocole sur le mode client-serveur utilisant le port TCP 389 ou TCP 636 en mode SSL/TLS.

Le modèle fonctionnel

Ce modèle décrit comment on accède aux données et comment on les manipule.

Il possède des instructions de base comme : add, delete, modify, rename, search, bind (connexion), unbind (déconnexion)

Le modèle de sécurité

Il protège l'accès aux données via l'authentification et le chiffrement des connexions. Il permet de spécifier qui accède aux données et avec quels droits.

Le modèle de duplication

Il permet la duplication et la synchronisation des données entre plusieurs serveurs LDAP.

Les API de développement

Elles permettent le développement d'application permettant de manipuler l'annuaire et de l'interroger.

Le modèle d'information

Il définit comment les objets doivent être stockés.

1. Le schéma représente l'ensemble des définitions (le squelette) qui concerne les objets.
2. Les classes d'objets qui représentent des objets réels (utilisateur, imprimante, organisation...) et des objets abstraits comme root directory specific entry (rootDSE) qui contient des attributs auxquels seul le serveur peut accéder afin de les manipuler.

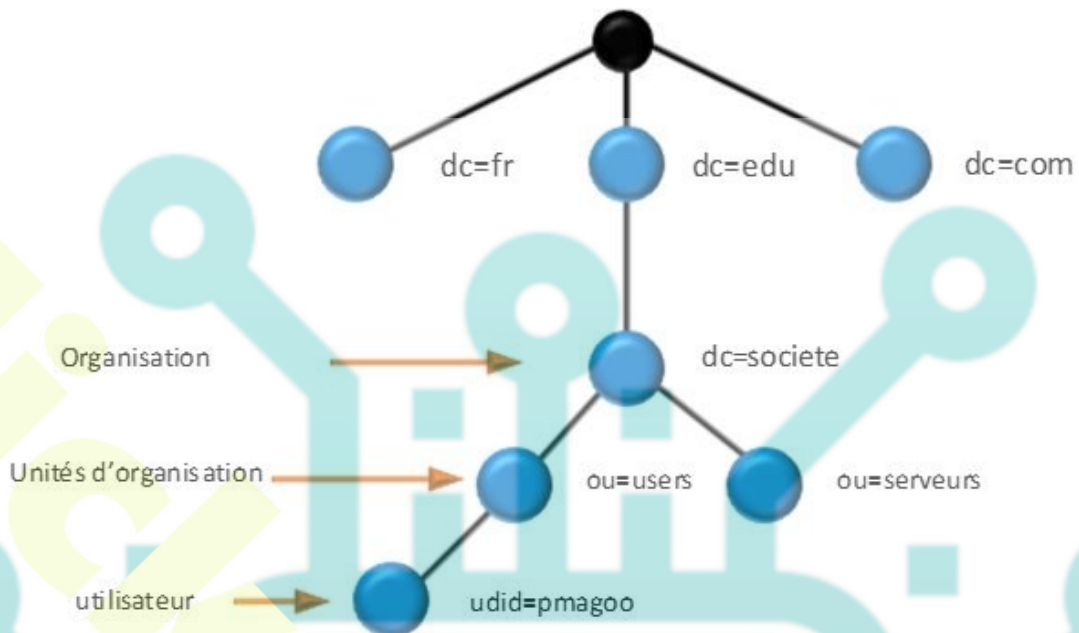
Les classes d'objets possèdent des attributs.

Exemple

```
dn: cn=Pierre Magoo, o=societe, c=FR
objectClass: inetOrgPerson
cn: Pierre Magoo
sn: Magoo
gn: Pierre
telephoneNumber: 11 11 11 11 11
description: webmaster
mail: m.magoo@societe.fr
```

Le modèle de nommage

Il définit comment sont organisés les objets suivant une structure nommée DIT (Directory Information Tree)



LDIF

LDIF (LDAP Data Interchange Format) est un format d'échange de données, qui permet de visualiser ou de modifier le contenu d'un annuaire.

Les données sont sous forme d'un fichier texte.

Exemple

```

dn: cn=Pierre Magoo,ou=users,o=societe,c=fr
changetype: add
cn: Pierre Magoo
sn: Magoo
mail: pmagoo@societe.fr
telephoneNumber: 11 11 11 11 11
objectClass: organizationalPerson
objectClass: person
objectClass: top
  
```