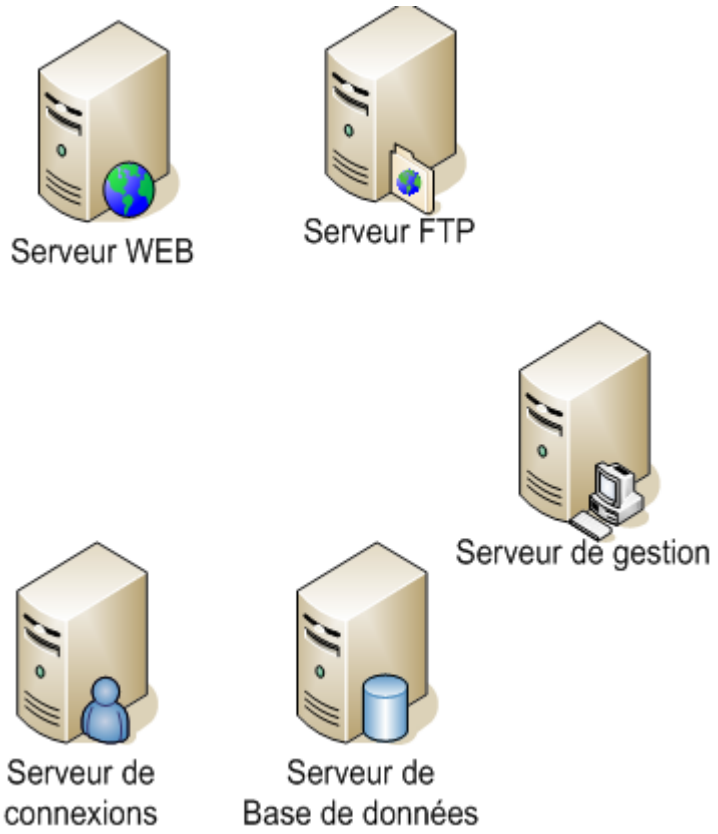
# Active Directory
# les services d’annuaire

# Utilisation

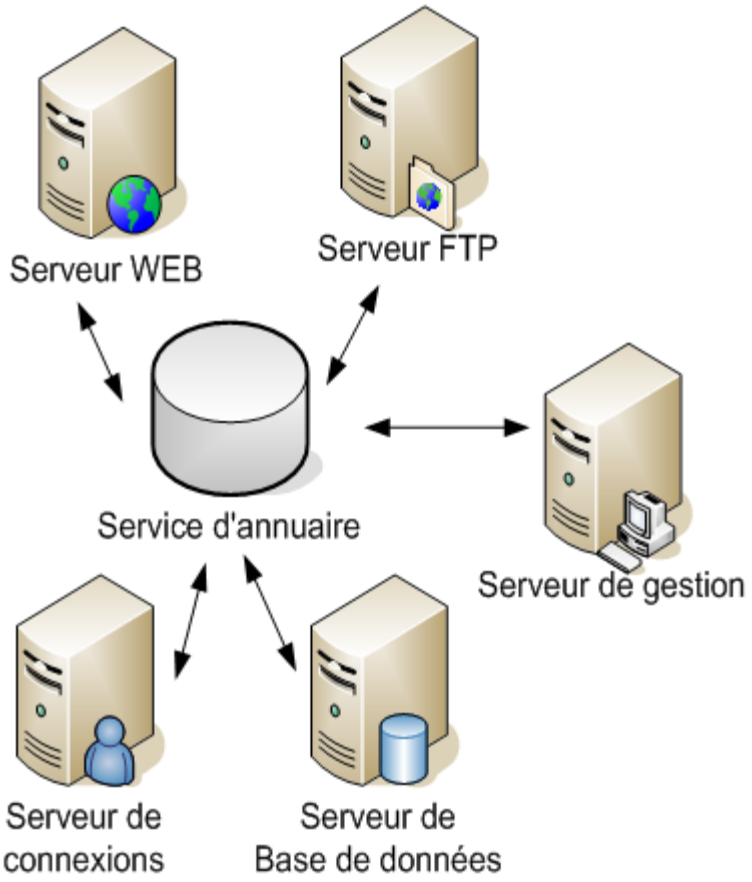
- Le serveur d'authentification a un annuaire pour l'identifiant et le mot de passe
- Les autres serveurs utilisent la même information dans des annuaires différents



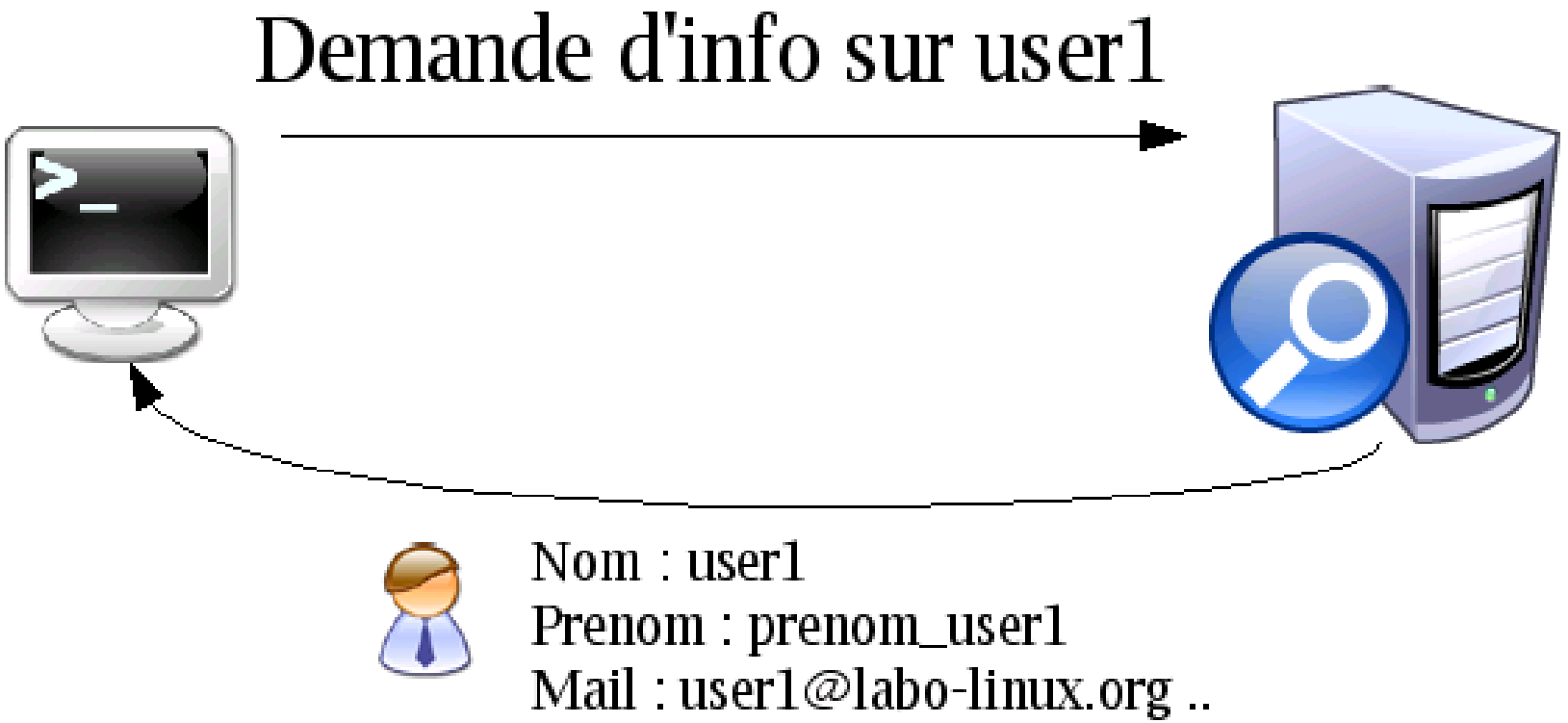
# Utilisation

- Meilleure administration, s'il y a toutes ces informations redondantes à un même endroit.

  Exemple : Effacer un compte utilisateur



# Utilisation



# Caractéristiques communes aux annuaires

- Un annuaire présente **un ensemble défini de données**
- Il **organise** ces données
- Il offre un service de **consultation**
- Il peut **protéger** les données
- Il est **plus consulté** que mis à jour
- Il est **disponible** de manière permanente

# ANNUAIRE OU BASE DE DONNEES ?

- **Ecritures** plus **rares** que lectures
- Mécanisme de **recherche** d'information **simple**
- Organisation des données de manière **hiérarchique** et non tabulaire
- Un annuaire doit être capable de **gérer l'authentification** des utilisateurs.

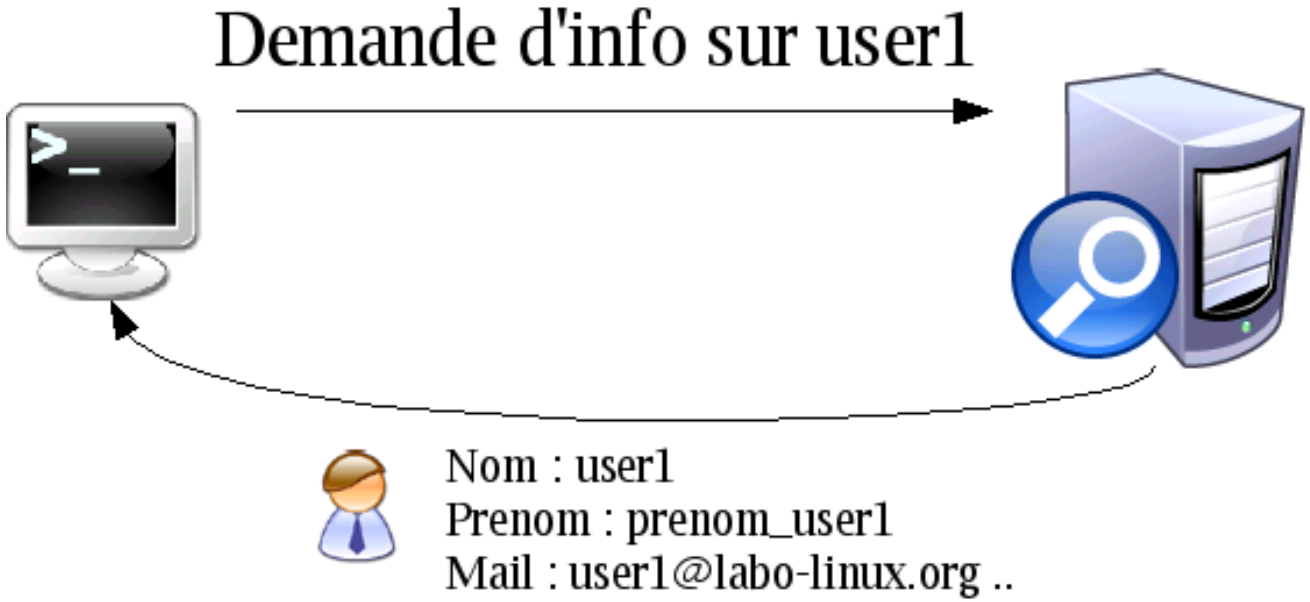
# Qu’avez-vous fait sous Active Directory?

- Ajout  d’utilisateurs
- Création de groupes d’utilisateurs
- Création d’unité d’organisation
- Ajout  d’ordinateurs

# AD est bien un annuaire

- Il recense tous les objets présents sur le réseau.
- Chaque objet est défini par un ensemble de données plutôt complètes :
  - Exemple : utilisateur

# Nécessité de normalisation




à 3 niveaux

1 Protocole d'échange

2 caractéristiques  des données

3 interfacer différents annuaires

# 1 Protocole d’échange

- Utilisation du protocole LDAP

  Lightweight

  Directory

  Access

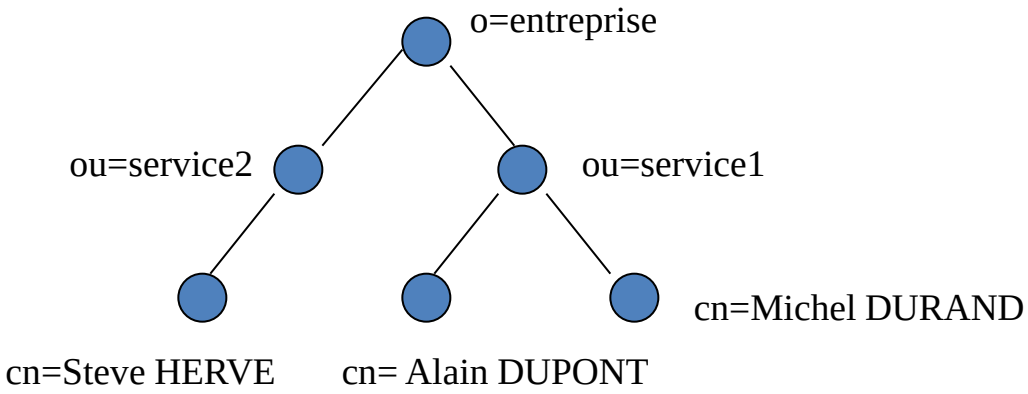
  Protocol

  Définit le format des trames échangées entre le client et le serveur.

# 2 caractéristiques des données (basé sur 4 modèles)

Le MODELE DE NOMMAGE définit l'organisation hiérarchique des données dans l'annuaire.

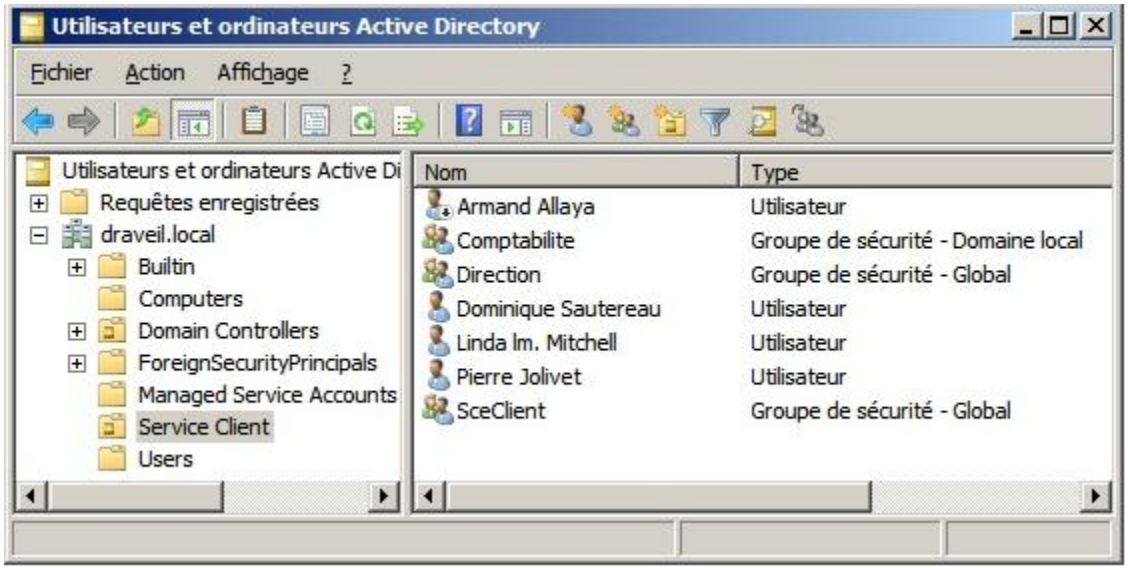
- **DIT** (Directory Information Tree)

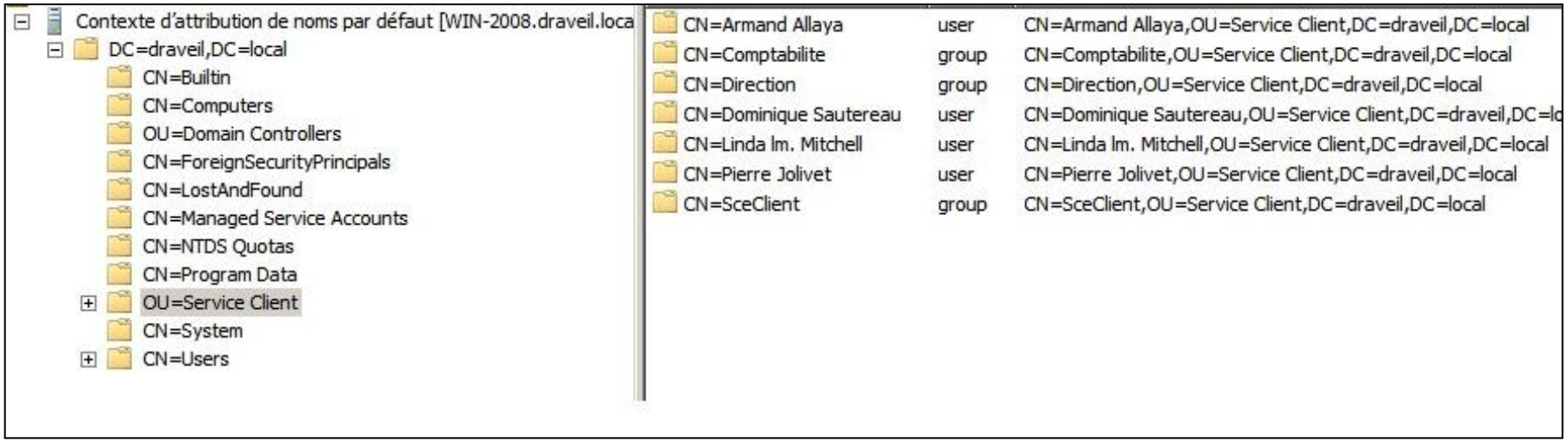



- **Identification d'une entrée (eq : un objet) : DN (Distinguished Name)**

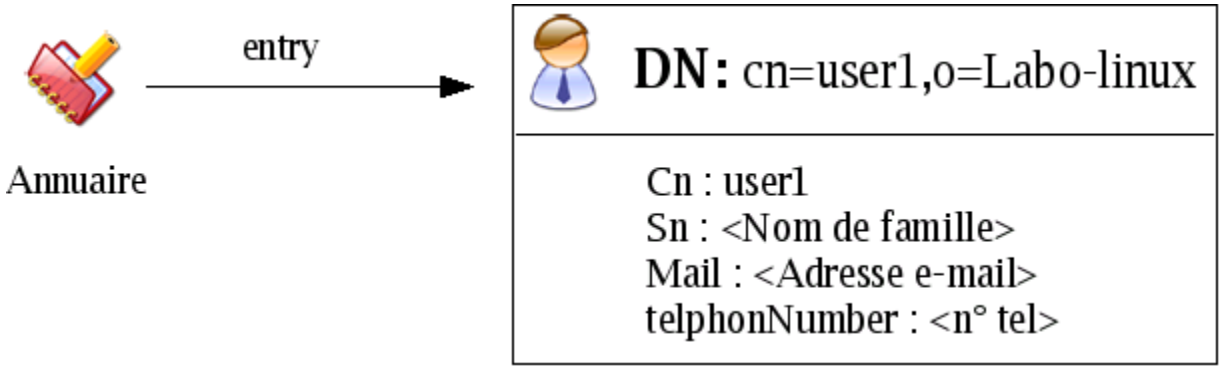
⟹ DN de l'objet Steve HERVE est : **cn=Steve HERVE, ou=service2, o=entreprise**

# Le DIT Active Directory



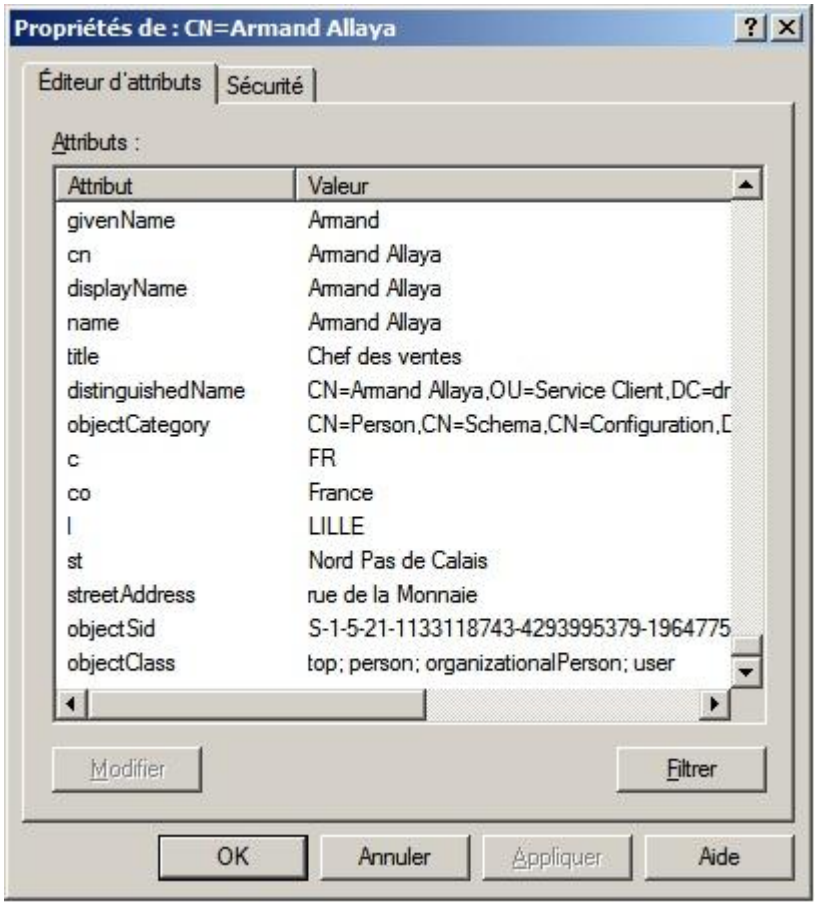



# Le modèle d'information




- Entry = élément de base de l'annuaire
- Ensemble d'attributs qui identifient un objet
- L'objet est identifié par son DN

# Le modèle d'information Active Directory



# Le modèle fonctionnel

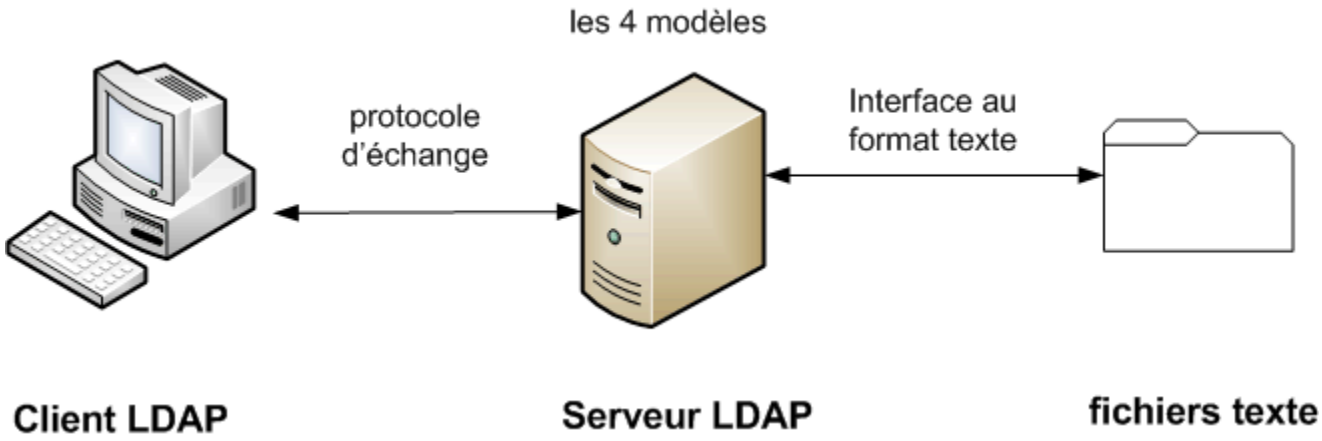
Ce sont les services fournis par l'annuaire.

Les opérations que l'on peut effectuer :

- Rechercher une entrée selon certains critères
- S'authentifier
- ajouter une entrée
- supprimer ou modifier une entrée
- renommer une entrée

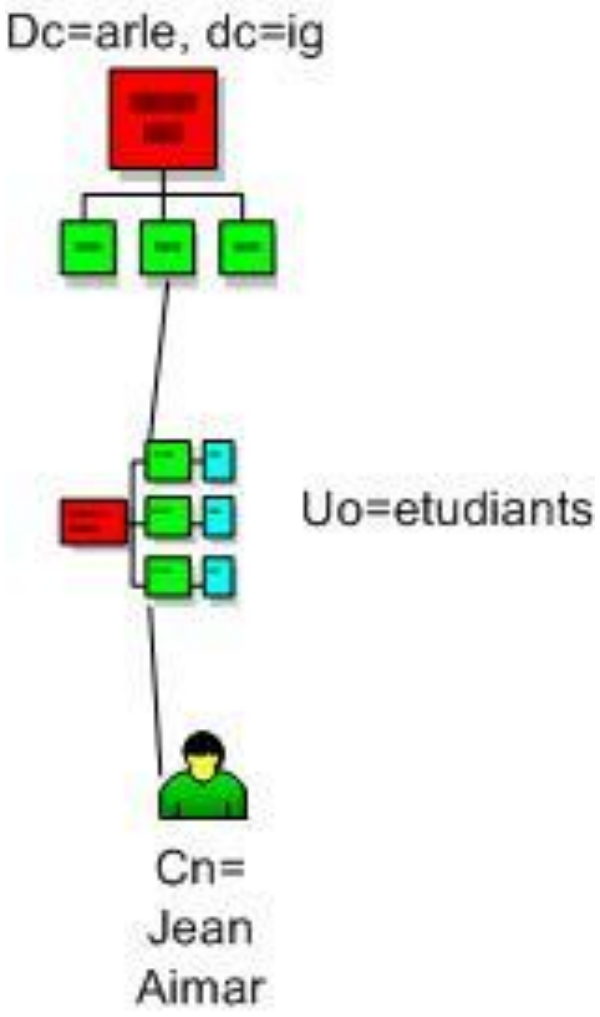
# Le modèle de sécurité

# Interface texte : le format LDIF




- **LDAP Data Interchange Format (LDIF) est le standard de représentation des entrées sous forme texte**
- **Utilisé pour afficher ou modifier les données de la base suivant deux modes :**
  - **faire des imports/exports de base,**
  - **faire des modifications sur des entrées.**

# Exemple de fichier LDIF




```
# Création du noeud racine
      dn: dc=arle,dc=ig
      dc: arle
      objectClass: dcObject
      objectClass: organizationalUnit
      ou: Arle Point Ig

# Création de l' ou etudiants
      dn: ou=etudiants,dc=arle,dc=ig
      ou: etudiants
      objectClass: organizationalUnit


# Création de Jean Aimar
      dn: cn=Jean Aimar,ou=etudiants,dc=arle,dc=ig
      objectClass: inetOrgPerson
      cn: Jean Aimar
      sn: Aimar
      mail: jaimar@wanadoo.fr
      telephoneNumber: 06 33 42 67 44
      telephoneNumber: 03 44 25 62 46
      departmentNumber: stsig
```