esprit

Se former autrement

Le service d'annuaire
Niveau: 4ème

Unité Pédagogique: Réseaux

Module : Services et administration des réseaux

cdio

CONCEIVE DESIGN IMPLEMENT OPERATE

Enropean Accreditation of Engineering Programmes EUR-ACE®

Délivré par Cti Commission des Titres d'Ingénieur

CONFÉRENCE DES GRANDES ÉCOLES

A.U: 2020/2021

Structure du Module: SAR

- Service WEB
- Service de messagerie
- Service de résolution de noms
- Service d’annuaire
- Service de supervision
- HA&LB

Plan


Definition & Concepts
L’annuaire LDAP
Les modèles de l’annuaire

Definition & Concepts

Exemples d'annuaires courants

- annuaire téléphonique : Les Pages Jaunes
- carnet d'adresses
- catalogue de vente

Annuaire informatique:

- gérer un grand nombre d'utilisateurs
- organisation des documents en dossiers et répertoires
- accéder à tous les serveurs, à toutes les applications et à toutes les ressources par le biais d'une ouverture de session unique.

- Un annuaire global célèbre très utilisé : DNS
  - il a un espace de nommage uniforme
  - il est distribué entre des serveurs coopérants

Definition & Concepts

- Un annuaire est un conteneur d'informations organisées
- ⇒ un système de stockage de données
- Organisé d'une manière hiérarchique
- Dérivé des **BDD relationnelles**

Un annuaire ➔ une base de données

Mais

Une base de données ➔ un annuaire

Definition & Concepts

Annuaire Electronique VS Base de données

1. Les données sont stockées de **manière hiérarchique** dans l'annuaire, tandis que les bases de données dites "**relationnelles**" stockent les enregistrements de façon tabulaire

2. Un annuaire électronique est conçu pour être consulté, bien plus que mis à jour. Le rapport **lecture** sur **écriture** est donc **plus élevé** dans les annuaires.

3. **L'extensibilité dans l'annuaire**: L'ajout d'attributs, l'équivalent des champs dans les bases de données relationnelles, est facile à réaliser. Il ne nécessite pas, par exemple, de reconstruction de la base.

Definition & Concepts
Caractéristiques

- **Dynamique** : Les informations peuvent être mises à jour en temps réel simplement par un administrateur
- **Souple** : Il est facile de rajouter de nouveaux attributs.
- **Sécurisé** : Les annuaires permettent de contrôler l'accès aux informations par différents critères.
- **Personnalisé** : la possibilité de définir la façon de présenter les données.

L'annuaire LDAP

LDAP Lightweight Directory Access Protocol

- **Héritier de l'annuaire X500 (proposé par l'ISO)**
  - Standard conçu par les opérateurs télécom pour interconnecter leurs annuaires téléphoniques
  - X500 adapté à l'internet ➔ LDAP (même modèle de schéma,. . .)

- **LDAP a été proposé en 1995 :**
  - Standard d'annuaire au dessus de TCP/IP
  - Un client commence une session LDAP en se connectant sur le port TCP 389 du serveur.
  - Version 3 actuellement (RFC 2251)

L’annuaire LDAP
Objectifs

- Fournir aux utilisateurs des informations fiables, facilement accessibles
- Permettre aux utilisateurs de mettre à jour eux-mêmes leurs informations personnelles
- Rendre les informations accessibles de façon contrôlée
- Eviter la redondance d’informations : un seul annuaire pour l’ensemble des services
- Faciliter la gestion (administration) des postes de travail, des équipements réseau

L’annuaire LDAP
Terminologies

- **Objet** : Un objet est un ensemble particulier d’attributs qui représente quelque chose de concret ,trois grandes catégories d’objets :

  -les ressources (par exemple les imprimantes),

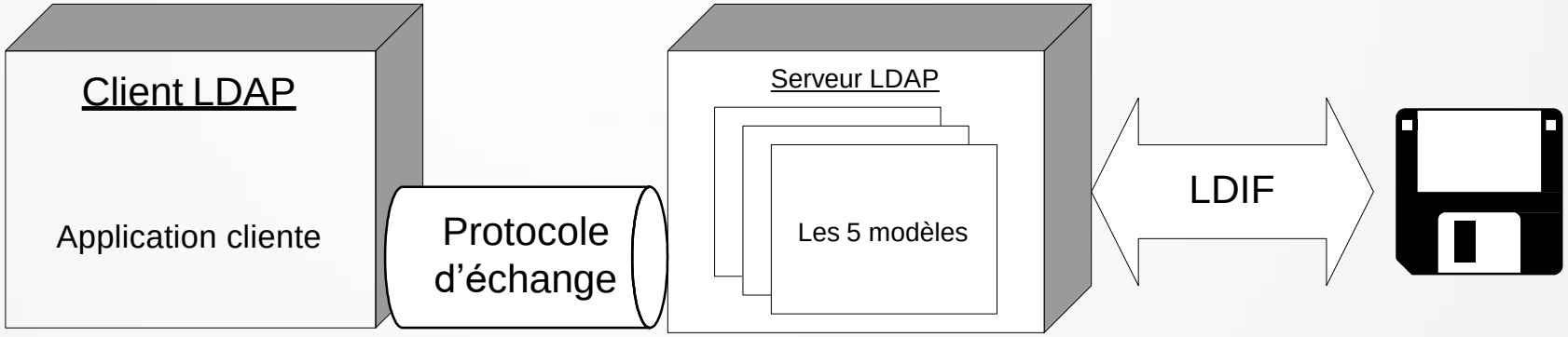
  -les services (par exemple le courrier électronique),

  -les utilisateurs (comptes utilisateurs et groupes).

- **Attribut:** Un attribut est un élément de données qui décrit un certain aspect d’un objet.
- **Conteneur** : C’est simplement une enveloppe, qui renferme des objets et d’autres conteneurs.
- **Le schéma:** correspond à tout ce qui constitue l’annuaire : les objets, les attributs, les conteneurs

L’annuaire LDAP

- **Le protocole d’échange d’informations**
- **La nature des données : 5 modèles**
- **Les interfaces : LDIF**



L’annuaire LDAP

L’annuaire LDAP définit 5 modèles

- **un modèle d’information**: le type de données contenues dans l’annuaire
- **un modèle de nommage:** comment l’information est organisée et référencée
- **un modèle fonctionnel**: une syntaxe des requêtes permettant l'interrogation de la base et la mise à jour des informations
- **un modèle de sécurité**: comment les données et les accès sont protégés
- **un modèle de duplication:** comment la base est répartie entre serveurs et aussi :

1. le protocole ➔ comment on accède à l’annuaire
2. les API ➔pour développer des applications clientes
3. LDIF ➔ un format d’échange de données

L’annuaire LDAP

La structure d'une entreprise se compose en deux parties distinctes : physique et logique.
Physique par son organisation géographique en différents sites et logique par sa hiérarchie.

Bien souvent, on attribue un sous-réseau IP à un site physique d'une entreprise.
Un domaine, contrairement à un site, mappe la structure logique de l'organisation.

Les modèles de l'annuaire
Le modèle d'information

- Définit le type de données pouvant être stocké dans l'annuaire
- Entrée/objet→ élément de base de l'annuaire; elle contient les informations sur un objet de l'annuaire
  - contient les données
  - regroupe un ensemble d'attributs

attribu	description
cn	« common name » ou nom commum
o	« organization name » ou nom de l'organisation
gn	« given name » ou le surnom
l	« locality name » ou nom de la localité
st	« state name » ou nom de l'état
ou	« organisational unit » ou unité d'organisation
dc	« domain component » ou nom de domaine

Les attributs classiques de LDAP

Les modèles de l'annuaire
Le modèle d'information

Client	
Type d'attribut	Valeur d'attribut
cn:	Ziggy NIGHT
uid	Znight
telnumber	0388123456
mail	Ziggy.night@gmail.co
solde	1000000

Exemple d'entrée

Les modèles de l’annuaire
Le modèle d’information

Une unité d'organisation:

- est une organisation logique permettant de regrouper les différents objets au sein d'un domaine.
- répond à des besoins administratifs, permet de:
  -déléguer des pouvoirs à certains utilisateurs,
  -simplifier la sécurité en limitant la visibilité des ressources.

Les modèles de l'annuaire
Le modèle d'information

- Exemples de classes d'objet :
  - ✓ une entreprise (*o*)
  - ✓ ses différents départements(*ou*)
  - ✓ ses employés (organizationalPerson)
  - ✓ ses imprimantes (devices)
  - ✓ ses groupes de travail(groupofnames)

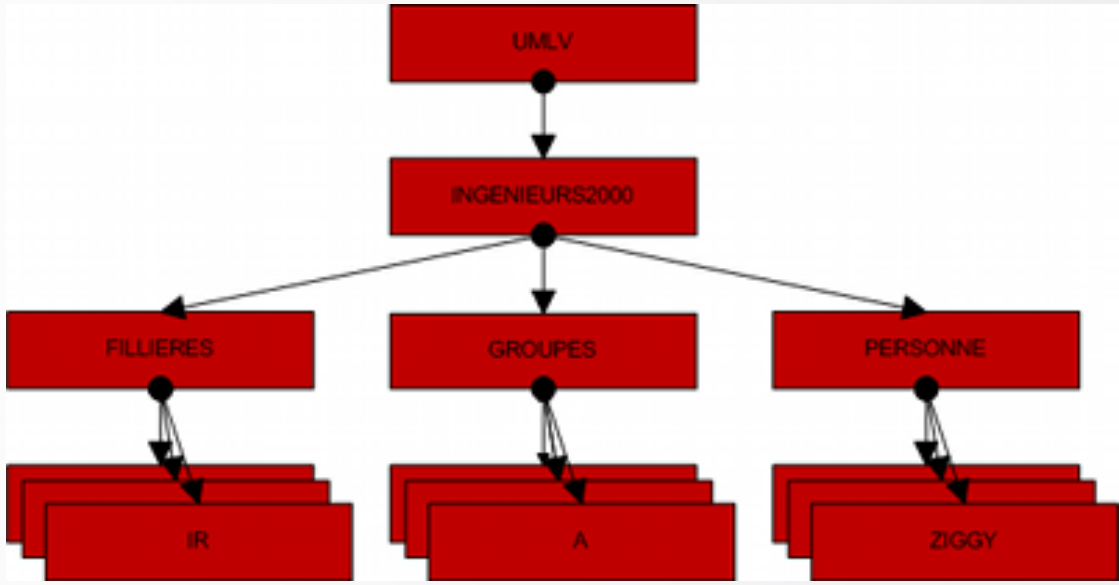
- Toutes les classes d'objets et leurs attributs sont définis dans un schéma (arbre)

- Chaque entrée de l'annuaire fait obligatoirement référence à une **classe d'objet** du **schéma**

Les modèles de l'annuaire

Le modèle de nommage

- Il définit comment sont organisées les entrées de l'annuaire et comment elles sont référencées
- Cette organisation est représentée par le **Directory Information Tree** → (DIT)
- Classification des entrées dans une arborescence hiérarchique
  - comparable au système de fichier UNIX



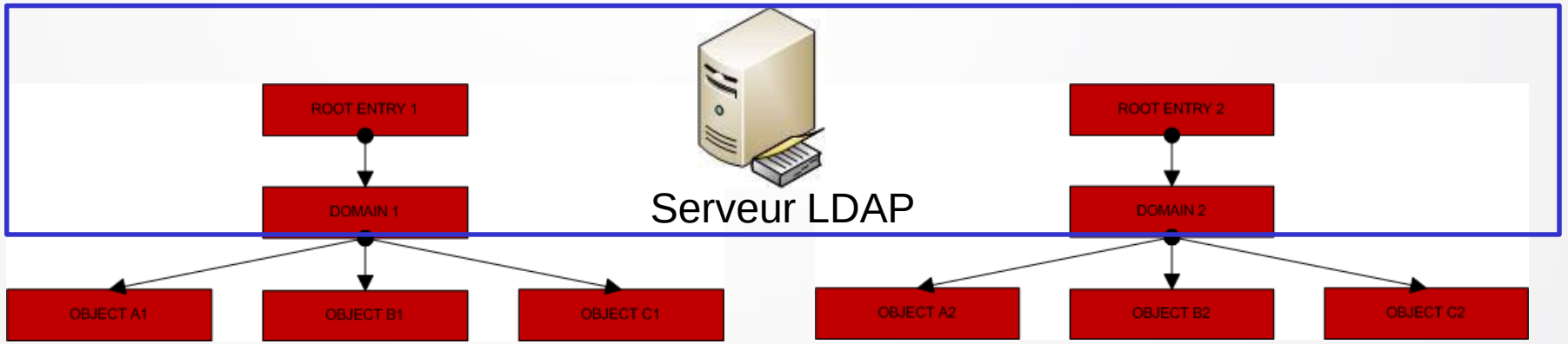
Exemple de Directory Information Tree (DIT)

Les modèles de l'annuaire

Le modèle de nommage

- Une « Root Entry » correspond à l'espace de nommage géré par le serveur

- Un serveur LDAP peut gérer plusieurs arbres (donc plusieurs « Root Entry »)



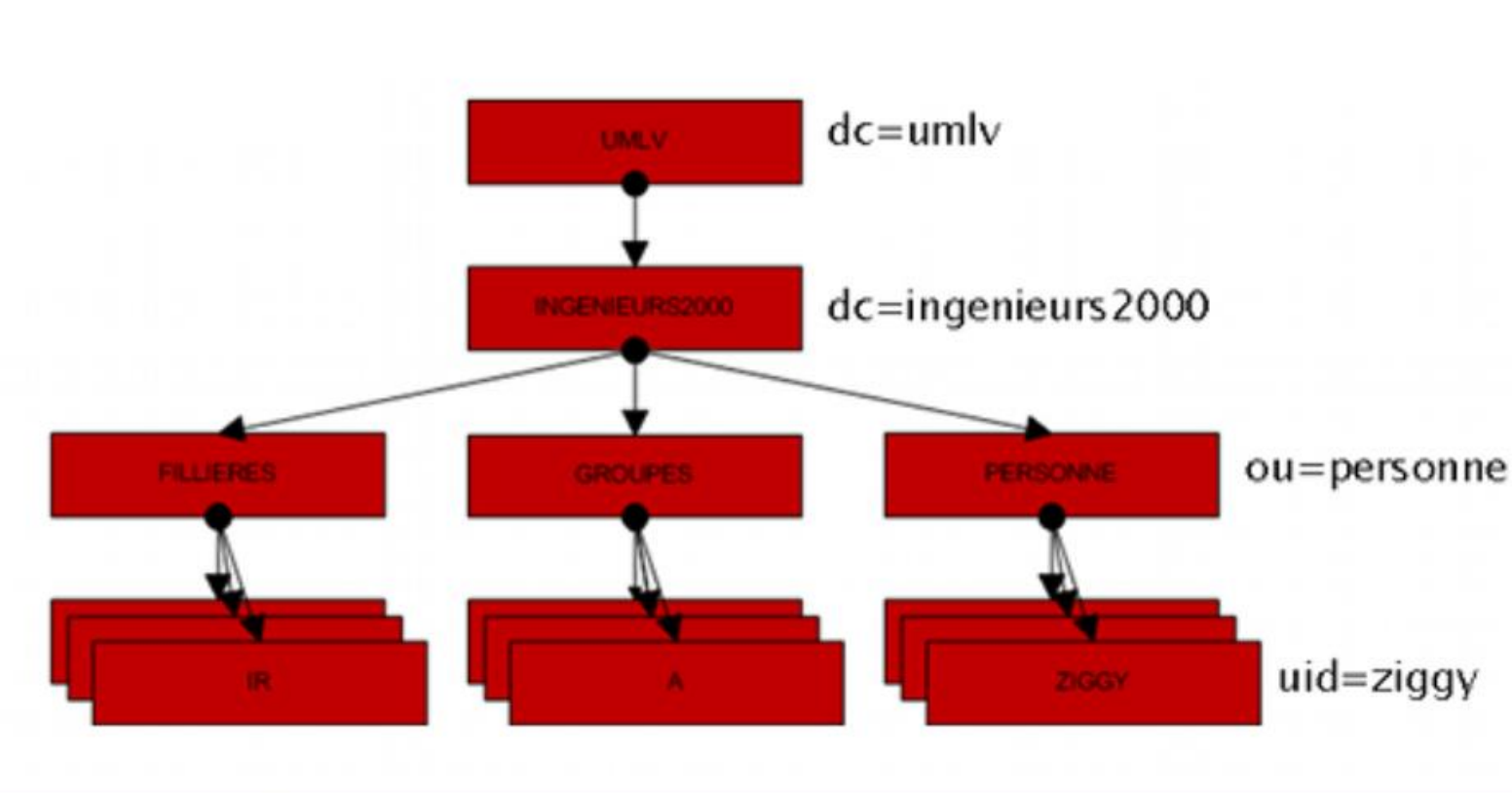
Les modèles de l'annuaire

Le modèle de nommage

- Distinguish Name (DN) ➔ référence de manière **unique** une entrée du DIT
- Equivalent du path d'un fichier UNIX
- DN ➔ constitué d'un ensemble d'attributs et de leurs valeurs provenant de chacune des entrées parentes mises bout à bout.
- Chaque composant du DN est appelé « Relative Distinguish Name » (RDN)

Les modèles de l'annuaire

Le modèle de nommage: schéma



DN de l'entrée ziggy = [uid=ziggy, ou=personne, dc=ingenieurs2000, dc = umlv]

- On doit s'assurer que 2 entrées du DIT n'aient pas le même DN

Les modèles de l'annuaire
Le modèle fonctionnel

- Il décrit :
  - les moyens d'accès aux données
  - les opérations applicables aux données

- Les opérations possibles sont :
  - opérations d'interrogation ➔ search
  - opérations de comparaison ➔ compare
  - opérations de mise à jour ➔ add, delete, rename, modify
  - opérations d'authentification et de contrôle ➔ bind, unbind, abandon

Les modèles de l'annuaire
Le modèle de sécurité

- Il décrit le moyen de protéger les données de l'annuaire

- La sécurité se fait à plusieurs niveaux
  - ✓ par l'authentification pour se connecter au service
  - ✓ par un modèle de contrôle d'accès au données
  - ✓ par le chiffrement des communications

Les modèles de l'annuaire

Le modèle de sécurité

- Pour **l'authentification**, LDAPv3 propose plusieurs choix:
  - ✓ Anonymous authentification ➔ accès sans authentification
  - ✓ Root DN authentification ➔ accès administrateur
  - ✓ Mot de passe + SSL ou TLS➔ accès chiffré
  - ✓ Certificats sur SSL ➔ accès avec échange de clé (publique/privée)

- **Le contrôle d'accès** ➔ droit d'accès aux données (lecture, écriture, recherche, comparaison)

- **Chiffrement** ➔ utilisation de SSL ou TLS

Les modèles de l'annuaire
Le modèle de duplication

- Il définit comment dupliquer l'annuaire sur d'autres serveurs

- Intérêt de **dupliquer un serveur LDAP** :
  - ✓ pallier une panne de l'un des serveurs, coupure de réseaux, …
  - ✓ répartir la charge du service
  - ✓ garantir une qualité de service (temps de réponse)

Les logiciels

- Les logiciels serveurs
  - Active Directory
  - Lotus Domino
  - OpenLDAP
- Les logiciels clients
  - Microsoft Outlook, NetMeeting
  - Netscape Communicator
  - LDAP Browser

REF: Marc OLORY – LDAP et les services d'annuaire