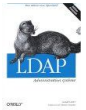
Service d'annuaire

Jean-François Berdjugin
Pierre-Alain Jacquot
Département SRC
L'Isle d'Abeau

Sources



- LDAP : Administration système de Gerald Carter, Sébastien Pujadas (Traduction)
- http://fr.wikipedia.org
- RFC : 2251-2256, 2829-2830
- Cours : Les services d'annuaire, Bruno Tesnière et Sylvain Sarméjeanne

Annuaire ?

- Larousse

  ANNUAIRE [anuɛr] n. M. (du lat. annuus, annuel; 1791). Recueil paraissant chaque année et contenant des reneignements de natures diverses (commerciaux, administratifs, scientifiques, etc, …) sur les événements de l'année précédente, des indications sur l'état du personnel, sur les abonnés d'un service public, sur les membre d'une société savante.

Annuaire ?

- Wikipédia

  Un annuaire est un système de stockage de données, dérivé des bases de données hiérarchisées, permettant en particulier de conserver les données pérennes, c'est-à-dire les données n'étant que peu mises à jour (historiquement, sur une base annuelle, d'où le nom), comme les coordonnées des personnes, des partenaires, des clients et des fournisseurs d'une entreprise. C'est pourquoi, grâce à des optimisations, un annuaire est beaucoup plus rapide en consultation qu'en mise à jour.

Annuaire ?

Ses caractéristiques :

- **Pérennité des données** (une base de donnée spécialisée)
- **Une organisation hiérarchique**, optimisée pour un accès rapide à de nombreuses informations, de petits volumes
- **Des entités** (ou objets) représentées dans l'annuaire pouvant avoir divers formats
- **Des accès simultanés** aux annuaires en consultation et en mise à jour
- **Un protocole d'accès** à l'annuaires

Annuaire vs SBBD

Un annuaire est une application se basant sur un SGBD afin de stocker et d'accéder aux enregistrements.

Un SGBD n'est pas forcement un annuaire

Annuaire répartis

- Sûreté => Réplication => Synchronisation
- Équilibrage de charge

=>

- les méta-annuaires avec réplication
- les méta-annuaires "virtuels« (pas de réplication)

Annuaires

Principales Types :

- **Annuaires multi-usages**
  - X 500
  - LDAP (Lightweight Directory Access Protocol)
  - UDDI (Universal Description Discovery and Integration)
- **Annuaires systèmes** :
  - Active Directory est compatible LDAP
  - NIS (Network Information System) un ancêtre
- Annuaires Internet (google, yahoo, …)
- Annuaires dédiés aux applications : Microsoft Exchange, Send Mail
- Internet Domaine Name Service
- Bases utilisateurs pour systèmes multi-utilisateurs (/etc/passwd, /etc/shadow, ..)

Norme X500

1988 conçu pour interconnecter tout type d'annuaire.

- Règle de nommage
- Protocoles d'accès dont DAP
- Méthode d'authentification

Trop lourd (X500, X501, X509, …)=>

Une version allégée de DAP : LDAP (le protocole) puis l'annuaire (natif, standalone).

Lightweight Directory Access Protocol

- LDAP est utilisé aussi bien pour un annuaire (standalone) que pour un protocole d'accès aux annuaires.
- Le protocole LDAP fournit un moyen standard pour effectuer des requêtes sur un annuaire.

Lightweight Directory Access Protocol

Concepts:

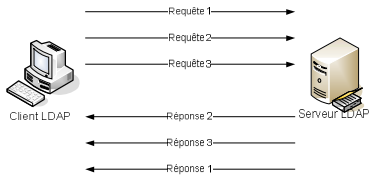
- Protocol LDAP : comment accéder à l'information de l'annuaire;
- Modèle d'information : le type des données de l'annuaire;
- Modèle de nommage : comment nommer les éléments de l'annuaire;
- Modèle fonctionnel : comment (méthodes) accéder à l'information;
- Modèle de sécurité : comment accès et données sont protégées;
- LDIF : un format d'échange;
- Modèle de réplication : comment la base est distribuée.
- Des API.

Protocole LDAP

Il définit la communication entre le client et le serveur :

- Connexion/Déconnexion
- Rechercher/Comparer
- Créer/Supprimer/Modifier

Le protocole permet le « pipelining » des requêtes



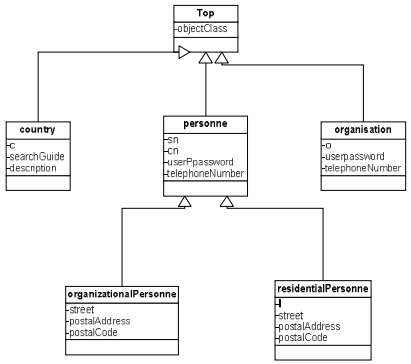
Protocole LDAP

- Ports : TCP/389 et TCP/636
- Choix de la méthode d'authentification
- Format d'un paquet de requête :
  - d'un numéro de message sur 3 octets
  - d'une séquence d'opérations
  - d'un champ optionnel de contrôle.
- Une opération se définit par :
  - son type sur 1 octet
  - la longeur (en nombre d'octets) de l'opération sur 1 octet
  - le contenu de l'opération, chaque opération ayant son propre format.
- Format d'un paquet de réponse :
  - d'un numéro de message sur 3 octets
  - du type de message sur 1 octet
  - de la longueur du message sur 1 octet
  - d'un code de retour sur 3 octets
  - du DN en question sur 2 octets
  - d'un message d'erreur en 2 octets
  - d'une éventuelle référence vers un ou plusieurs autres serveurs (séquence d'URL LDAP).

LDAP : Modèle d'information

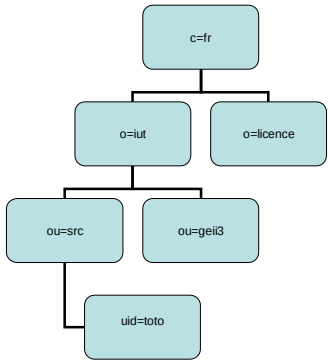
- Schéma : définitions relatives aux objets stockés dans l'annuaire (les classes d'objets leurs types et leur syntaxe)
- Les classes d'objet modélisent des objets réels ou abstraits (un nom, OID, attributs obligatoires, des attributs optionnels, un type)
- Attributs constituent les entrées de l'annuaire (nom, OID, mono ou multi-valués, une syntaxe et des règles de comparaison, un indicateur d'usage, un format ou une limite de taille)

LDAP : Modèle d'information



LDAP : modèle de nommage

- **D**irectory **I**nformation **T**ree : l'arbre
- **D**irectory **S**ervice **E**ntry : un nœud (un objet), un ensmeble de clef/valeur
- **D**istinguished **N**ame : un nom absolu (uid=toto, ou=src, o=iut, c=fr)
- **R**elative **D**istinguished **N**ame (uid=toto)

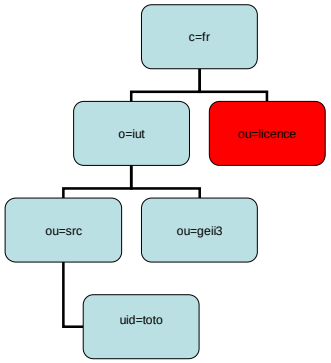


LDAP : modèle de nommage ?

Modèle hiérarchique

=>

A une profondeur donnée les nœud peuvent être de type différents



LDAP modèle de nommage

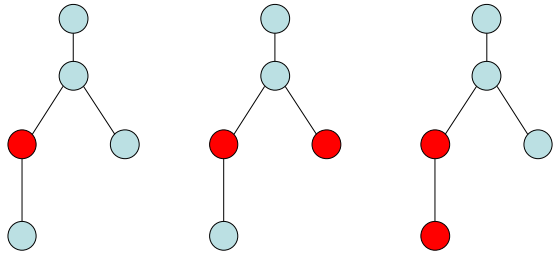
- Exemple d'ensemble clef valeur :
  - **uid** (userid), il s'agit d'un identifiant unique obligatoire
  - **cn** (common name), il s'agit du nom de la personne
  - **givenname**, il s'agit du prénom de la personne
  - **sn** (surname), il s'agit du surnom de la personne
  - **o** (organization), il s'agit de l'entreprise de la personne
  - **u** (organization), il s'agit du service de l'entreprise dans laquelle la personne travaille
  - **mail**, il s'agit de l'adresse de courrier électronique de la personne (bien évidemment)

LDAP : modèle fonctionnel

- Similaire au modèle UNIX
  - Opération/Description :
  - Abandon/Abandonne l'opération précédemment envoyées au serveur
  - Add /Ajoute une entrée au répertoire
  - Bind/Initie une nouvelle session sur le serveur LDAP
  - Compare/Compare les entrées d'un répertoire selon des critères
  - Delete/Supprime une entrée d'un répertoire
  - Extended/Effectue des opérations étendues
  - Rename/Modifie le nom d'une entrée
  - Search/Recherche des entrées d'un répertoire
  - Unbind/Termine une session sur le serveur LDAP
- Search et compare se font sous forme d'une requête composée de huit paramêtres

LDAP : modèle fonctionnel

- Notion de « scope »



Search scope base

Search scope on level search

Search scope subtree

Modèle de sécurité

- Un annuaire est un élément sensible
- Client hostile
  - Accès non autorisés
  - Modification non autorisées
- Menace réseau
  - Interceptions des mots de passe
  - Interceptions des données
  - Man in the midle

Modèle de sécurité

Il faut :
- Identifier le serveur
- Identifier le client
- Contrôler l'intégrité
- Contrôler l'accès

LDAP propose :
- Simple Authentification and Security Layer

LDAP peut aussi être utilisé au dessus de SSL ou TLS

LDAP ne propose pas de contrôle d'accès la liberté est laissée à l'implémentation

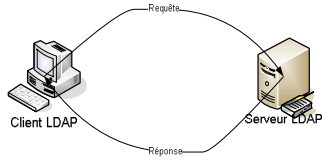
Lightweight Data Interchange Format

Format texte d'échange entre annuaire LDAP

[<id>]
dn: <distinguished name>
<attribut> : <valeur>
<attribut> : <valeur>
...

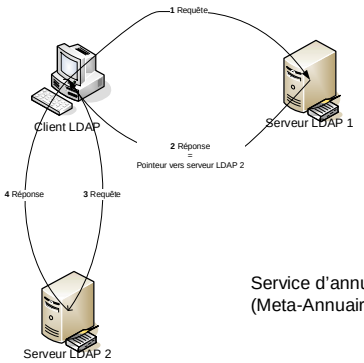
dn: uid =toto, ou = src, ou=iut, c =fr
cn: Nom
givenName: Prénom
sn: Surnom
telephoneNumber: +06 06 06 06
telephoneNumber: +07 07 07 07
mail: Prenom.Nom@example.com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top

Topologie LDAP



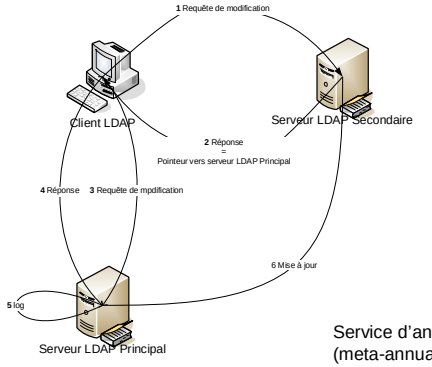
Serveur d'annuaire local

Topologie LDAP



Service d'annuaire local avec références
(Meta-Annuaire Virtuel)

Topologie LDAP



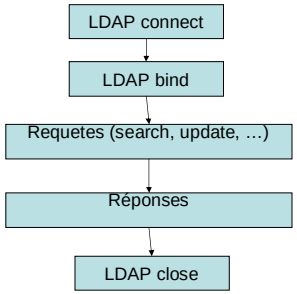
Problème lors des mises à jour

Service d'annuaire avec réplication
(meta-annuaire avec réplication)

API LDAP

- Dans tous les langages du moment
- Exemple PHP :

```
$ds=ldap_connect("127.0.0.1");
…
$r=ldap_bind($ds);
…
$dn="dc=fctice,dc=fr";
$filtre = "sn=T*";
$sr=ldap_search($ds, $dn,
    $filtre);
…
$info = ldap_get_entries($ds,
    $sr);
…
ldap_close($ds);
```



Universal Description Discovery and Integration

UDDI permet de localiser le service Web recherché

- Norme de l'OASIS (Organization for the Advancement of Structured Information Standards)
- Basée sur XML
- Destinée aux services Web (un ensemble de norme et protocoles pour l'échange de données entre applications)
  - Plus particulièrement dans le cadre du architecture de type SOA (Service Oriented Architecture)
- Repose sur SOAP (Simple Object Access Protocol) un protocole de RPC orienté objet et utilisant XML. SOAP est utilisé au dessus de HTTP ou SMTP ou autre protocole applicatif.

Universal Description Discovery and Integration

Dans la pratique :

- Les pages blanches comprennent la liste des entreprises ainsi que des informations associées à ces dernières. Nous y retrouvons donc des informations comme le nom de l'entreprise, ses coordonnées, la description de l'entreprise mais également l'ensemble des ses identifiants.

=>

- Les pages jaunes recensent les services web de chacune des entreprises sous le standard WSDL (Web Services Description Language).

=>

- Les pages vertes fournissent des informations techniques précises sur les services fournis. Ces informations concernent les descriptions de services et d'information de liaison ou encore les processus métiers associés.

Active Directory

Active Directory est une technologie Microsoft qui repose sur le protocole LDAP mais aussi sur d'autres protocoles (DNS, Kerberos, SMTP, SMB/CIFS, MSRPC).

Le modèle de données et un dérivé de la norme X500.

Network Information Service/NIS+

- Objectif centralisation des comptes sur un réseau local
- Composants
  - Domaines : des machines qui partagent les mêmes cartes identifié par un nom
  - Cartes : les éléments d'information
  - Démons : les processus serveurs (binding)
  - Utilitaires : ypcat, ypwhich, ypinit, makedbm, …

Nommage à « plat » et sécurité => NIS+ (très rare)

Domain Name System

- Portée globale
- Correspondance entre une adresse IP est un nom d'hôte
- Enregistrements :
  - SOA, NS
  - A,AAA
  - PTR
  - CNAME
  - MX, SRV

Conclusion

- Systèmes nombreux avec une norme qui l'emporte : LDAP

- Toujours une portée
  - Locale : base de compte
  - …
  - Globale : DNS
- Protocole
- Modèle :
  - d'information
  - de nommage
  - fonctionnel
  - (sécurité et duplication)