Le protocole LDAP

Septembre 2015

Introduction à LDAP

LDAP (*Lightweight Directory Access Protocol*, traduisez *Protocole d'accès aux annuaires léger* et prononcez "èl-dap") est un protocole standard permettant de gérer des annuaires, c'est-à-dire d'accéder à des bases d'informations sur les utilisateurs d'un réseau par l'intermédiaire de protocoles TCP/IP. Les bases d'informations sont généralement relatives à des utilisateurs, mais elles sont parfois utilisées à d'autres fins comme pour gérer du matériel dans une entreprise. Le protocole LDAP, développé en 1993 par l'université du Michigan, avait pour but de supplanter le protocole DAP (servant à accéder au service d'annuaire X.500 de l'OSI), en l'intégrant à la suite TCP/IP. A partir de 1995, LDAP est devenu un annuaire natif (*standalone LDAP*), afin de ne plus servir uniquement à accéder à des annuaires de type X500. LDAP est ainsi une version allégée du protocole DAP, d'où son nom de ***Lightweight** Directory Access Protocol*.

Présentation de LDAP

Le protocole LDAP définit la méthode d'accès aux données sur le serveur au niveau du client, et non la manière de laquelle les informations sont stockées. Le protocole LDAP en est actuellement à la version 3 et a été normalisé par l'IETF (Internet Engineering Task Force). Ainsi, il existe une RFC pour chaque version de LDAP, constituant un document de référence :

- RFC 1777 pour LDAP v.2 standard
- RFC 2251 pour LDAP v.3 standard

Ainsi LDAP fournit à l'utilisateur des méthodes lui permettant de :

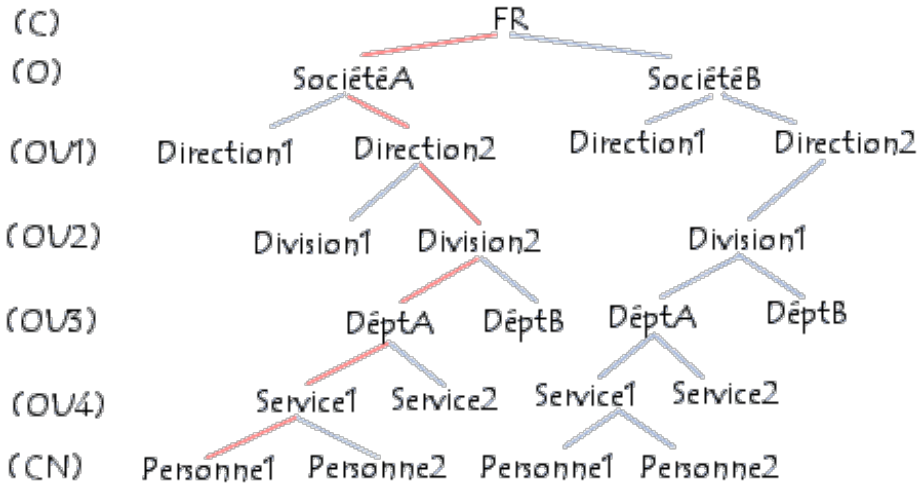
- se connecter
- se déconnecter
- rechercher des informations
- comparer des informations
- insérer des entrées
- modifier des entrées
- supprimer des entrées

D'autre part le protocole LDAP (dans sa version 3) propose des mécanismes de chiffrement (SSL, ...) et

d'authentification (SASL) permettant de sécuriser l'accès aux informations stockées dans la base.

L'arborescence d'informations (DIT)

LDAP présente les informations sous forme d'une arborescence d'informations hiérarchique appelée **DIT** (*Directory Information Tree*), dans laquelle les informations, appelées **entrées** (ou encore *DSE, Directory Service Entry*), sont représentées sous forme de branches. Une branche située à la racine d'une ramification est appelée racine ou suffixe (en anglais *root entry*). Chaque entrée de l'annuaire LDAP correspond à un objet abstrait ou réel (par exemple une personne, un objet matériel, des paramètres, ...). Chaque entrée est constituée d'un ensemble de paires clés/valeurs appelées **attributs**.



Les attributs des entrées

Chaque entrée est constituée d'un ensemble d'attributs (paires clé/valeur) permettant de caractériser l'objet que l'entrée définit. Il existe deux types d'attributs :

- **Les attributs normaux**: ceux-ci sont les attributs habituels (nom, prénom, ...) caractérisant l'objet
- **Les attributs opérationnels**: ceux-ci sont des attributs auxquels seul le serveur peut accéder afin de manipuler les données de l'annuaire (dates de modification, ...)

Une entrée est indexée par un **nom distinct** (**DN**, *distinguished name*) permettant d'identifier de manière unique un élément de l'arborescence. Un DN se construit en prenant le nom de l'élément, appelé *Relative Distinguished Name* (*RDN*, c'est-à-dire le chemin de l'entrée par rapport à un de ses parents), et en lui ajoutant l'ensemble des nom des entrées parentes. Il s'agit d'utiliser une série de paires clé/valeur permettant de repérer une entrée de manière unique. Voici une série de clés généralement utilisées :

- **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** (*organizational unit*), 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)
- ...

Ainsi un *Distinguished Name* sera de la forme :

```
uid=jeapil,cn=pillou,givenname=jean-francois
```

Le *Relative Distinguished Name* étant ici "*uid=jeapil*". Ainsi, on appelle **schéma** l'ensemble des définitions d'objets et d'attributs qu'un serveur LDAP peut gérer. Cela permet par exemple de définir si un attribut peut posséder une ou plusieurs valeurs. D'autre part, un attribut nommé *objectclass* permet de définir les attributs étant obligatoires ou facultatifs...

Consulter les données

LDAP fournit un ensemble de fonctions (procédures) pour effectuer des requêtes sur les données afin de rechercher, modifier, effacer des entrées dans les répertoires. Voici la liste des principales opérations que LDAP peut effectuer :

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

Le format d'échange de données LDIF

LDAP fournit un format d'échange (**LDIF**, *Lightweight Data Interchange Format*) permettant d'importer et d'exporter les données d'un annuaire avec un simple fichier texte. La majorité des serveurs LDAP supportent ce format, ce qui permet une grande interopérabilité entre eux. La syntaxe de ce format est la suivante :

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

Dans ce fichier, *id* est facultatif, il s'agit d'un entier positif permettant d'identifier l'entrée dans la base de données.

- chaque nouvelle entrée doit être séparée de la définition de l'entrée précédente à l'aide d'un saut de ligne (ligne vide)
- Il est possible de définir un attribut sur plusieurs lignes en commençant les lignes suivantes par un espace ou un tabulation
- Il est possible de définir plusieurs valeurs pour un attribut en répétant la chaîne *nom:valeur* sur des lignes séparées
- lorsque la valeur contient un caractère spécial (non imprimable, un espace ou *:*), l'attribut doit être suivi de *::* puis de la valeur encodée en base64

‹ Précédent

- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23

Suivant ›

Réalisé sous la direction de Jean-François PILLOU,
fondateur de CommentCaMarche.net.

Ce document intitulé « Le protocole LDAP » issu de **CommentCaMarche** (www.commentcamarche.net) est mis à disposition sous les termes de la licence Creative Commons. Vous pouvez copier, modifier des copies de cette page, dans les conditions fixées par la licence, tant que cette note apparaît clairement.