

LDAP

lightweight directory access protocol



*Protocole d'accès à un **annuaire***

Base de données spécialisée avec une structure forte ...

... tout ce qui peut être nommé

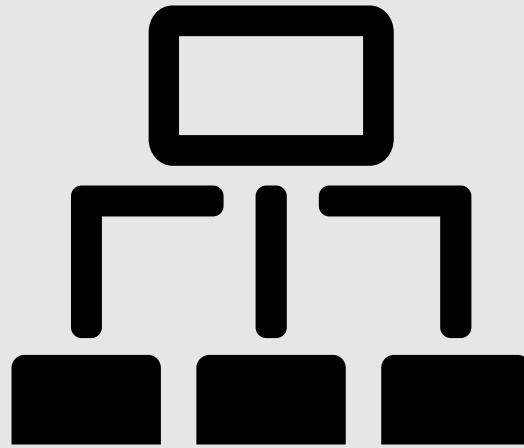
Un annuaire n'est pas un SGBD

LDAP fournit

protocole d'accès · un modèle d'informations
· conventions de nommage · modèle
fonctionnel, de sécurité et de duplication ·
API · LDIF



modèle de données



un nœud, une entrée · un nœud, un objet

La racine contient la description de l'arbre *rootDSE*

modèle de données |

***objectClass* (classe d'objet)**

nom, objectID,
attributs obligatoires / optionnels,
type (structurel | abstrait | auxiliaire)

Un attribut a : un nom, un OID, une syntaxe et un format de valeur

modèle de données ||

objectClass (classe d'objet)
objectID

normalisé ([RFC2256](#))
hiérarchie – héritage

2.5

1.3.6.1.4.1.4203 (openLDAP)

1.3.6.1.4.1.23162 (ÉSI)

modèle de données |||

Exemple *objectClass* : *inetOrgPerson* (*extrait de /etc/ldap/schema/inetorgperson.schema*)

```
objectclass ( 2.16.840.1.113730.3.2.2
  NAME 'inetOrgPerson'
    DESC 'RFC2798: Internet Organizational Person'
  SUP organizationalPerson
  STRUCTURAL
  MAY (
    audio $ businessCategory $ carLicense $
    departmentNumber $ displayName $ employeeNumber
    $ employeeType $ givenName $ homePhone $
    homePostalAddress $ initials $ jpegPhoto $ ... )
)
```

modèle de données ||||

Exemple *objectclass* et *attributetype*

(extraits de /etc/ldap/schema/core.schema)

```
objectclass ( 2.5.6.6 NAME 'person'  
    DESC 'RFC2256: a person'  
    SUP top STRUCTURAL  
    MUST ( sn $ cn )  
    MAY ( userPassword $ telephoneNumber $ seeAlso  
        $ description ) )  
  
attributetype ( 2.5.4.4 NAME ( 'sn' 'surname' )  
    DESC 'RFC2256: last (family) name(s) for which  
        the entity is known by'  
    SUP name )
```

Lorsque l'on insère une entrée, le serveur vérifie si la syntaxe est conforme → *schema checking*

modèle de données ||||

Chaque nœud a un identifiant unique
composé des attributs obligatoires

DN *distinguished name*

uid=fpignon, ou=construction, dc=example, dc=org

LDIF

LDAP Data Interchange Format

Format de représentation des données

import / export
modifications

Représentation des données

```
dn:cn=Marlene Sassøur,ou=student,dc=example,dc=be
objectclass: inetOrgPerson
cn: Marlene SASSOEUR
sn: Marlene
mail: marlene.sassoeur@dev.null
description: Elle me dit c'est Marlene sa soeur.
Avouez que c'est confusant .
```

Ajout, suppression de données

```
dn:cn=Marlene Sassøur,ou=student,dc=example,dc=be
changetype : modify
add : telephonenumber
telephonenumber : 123 45 67 89
```

```
dn:cn=Marlene Sassøur,ou=student,dc=example,dc=be
changetype : delete
```

modèle fonctionnel

Portée de la recherche
search scope

base
onelevel search
subtree

The image is a title card for 'Open LDAP'. It features a background photograph of an outdoor stone patio with several open books scattered across it. The patio is bordered by a black metal railing, and the surrounding area is covered in fallen autumn leaves. A semi-transparent green banner is overlaid across the middle of the image, containing the text 'Open LDAP' in a large, green, serif font.

Open LDAP

Open LDAP

Implémentation libre de LDAP

<http://openldap.org>

package : slapd, ldap-utils

dæmons : *slapd*, *slurpd*

Open LDAP |

Configuration

choix des schémas
`/etc/ldap/slapd.d`
utilitaires `ldapfoo`

Autres implémentations

Serveurs

OpenLDAP · Microsoft Active Directory ·
Netscape Directory Server ·

Clients

browsers · MS Windows · PAM LDAP · API
(perl, Java, ...)

([Liste](#))

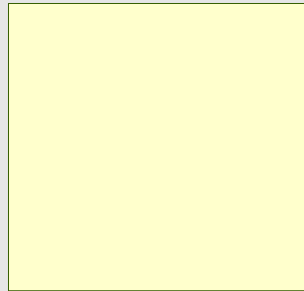
Références

[IANA enterprise numbers](#)

[OpenLDAP QuickStart](#)

[LinuxMag \(vieil\) article mongueurs](#)

Transparents dans le cadre de mes cours à HEB-ÉSI.
Ces slides sont sous licence CC-BY-NC-SA



Qui suis-je ?

Pierre Bettens (pbt)
pbettens@heb.be

<http://blog.namok.be> · <http://esi.namok.be>

Images

DeviantArt [inckurei](#) · Dieffi
The noun project [MikaDo Nguyen](#)