

## Installation et Utilisation de OpenLDAP sous Debian

### Présentation rapide

Une base **LDAP** est une base de données où les informations sont enregistrées de manière hiérarchique sous forme d'arbre et non sous forme tabulaire.

Une base LDAP est optimisée pour la lecture d'un nombre important de petits enregistrements et convient donc parfaitement pour stocker des annuaires ou des profils utilisateurs.

Le système LDAP utilise des **schémas** (/etc/ldap/schema) pour décrire des objets.

Chaque **objet** contient plusieurs **attributs** (obligatoire ou facultatifs). Et chaque objet peut **hériter** des attributs d'un autre objet. Exemple :

L'objet « person » a comme attributs : commonName, surname,..

L'objet fils « organizationalPerson » dérivé de l'objet « person » ajoute les attributs : title, PostalAddress,...

Les objets et les attributs sont **normalisés** pour assurer les échanges entre les logiciels.

Il est possible de modifier un schéma en rajoutant des attributs à un objet (déconseillé) ou en créant un nouvel objet (mieux), mais le mieux est de faire valider cette modification par l'IANA.

Chaque donnée enregistrée dans la base est identifiée par son **DN** (Distinguished Name). Ce DN est comparable au chemin complet d'un fichier. Exemple :  
dc=mondomaine,dc=fr

Pour ajouter ou modifier des données dans la base, il est possible d'utiliser le format **LDIF**.

### Installation

Paquets à installer :

```
# apt-get install ldap-server ldap-client
```

Ce qui installera en fait :

```
# apt-get install slapd ldap-utils
```

#### Écran (Titre en rouge) Message

Configuration de slapd Enter your DNS domain

Enter the name of organisation **mondomaine.com**

Admin password

#### Réponse

**mondomaine.com**

**mondomaine.com**

**xxxx**

Allow LDAPv2 protocol      **Oui \***

**\* J'ai été obligé d'autoriser la norme v2 pour les clients Win 2000.** Avec les clients Win NT, il n'y avait pas de problème.

## Configuration

Le fichier de configuration est :

```
/etc/ldap/slapd.conf
```

La ligne suivante permet d'autoriser l'utilisation de la norme V2 de LDAP.

```
allow bind_v2
```

La ligne suivante donne la racine de la base LDAP :

```
suffix "dc=mondomaine,dc=com"
```

La ligne suivante **qu'il faut ajouter manuellement** donne le login de l'administrateur (admin avec le rappel de la racine). Cette ligne et la suivante sont obligatoires pour avoir un accès root sur la base depuis un programme externe (ex : PHP)

```
rootdn "cn=admin,dc=mondomaine ,dc=com"
```

La ligne suivante **qu'il faut ajouter manuellement** donne le mot de passe en clair :

```
rootpw admin
```

Pour plus de sécurité, il est préférable de générer un mot de passe crypté en utilisant la commande :

```
# slappasswd  
New password:  
Re-enter new password:  
{SSHA}5y67xJ/t7esuGKUD7TQPcgykd8xiYMO2
```

Ensuite, il faut copier la chaîne cryptée à la place du mot de passe en clair

Paramétrage de l'accès en écriture de la base. Il faut indiquer le bon login et la racine de la base :

```
access to attribute=userPassword  
    by dn="cn=admin,dc=test,dc=com" write  
    by anonymous auth  
    by self write  
    by * none
```

Paramétrage de l'accès en lecture seule de la base. Il faut indiquer le bon login et la racine de la base :

```
access to *
  by dn="cn=admin,dc=test,dc=com" write
  by * read
```

## Démarrage du serveur (slapd)

Le serveur slapd se démarre d'une manière classique avec la commande :

```
# /etc/init.d/slapd restart
```

## Le format de fichier LDIF

Ce format de fichier est utilisé pour faire des imports / exports entre plusieurs bases ou pour modifier ou ajouter des données dans une base.

ATTENTION : Il est obligatoire de coder les données en UTF-8. Si lors de l'importation une erreur est rencontrée, celle-ci est abandonnée à l'endroit où elle en était.

### Fichier LDIF pour ajouter des enregistrements

Voici la structure d'un fichier LDIF

```
dn: <distinguished name
  objectClass: <object class
  objectClass: <object class
  ...
  <attribute type:<attribute value
  <attribute type:<attribute value
  ...
```

Voici un exemple de fichier LDIF (AjoutRacine.ldif) pour créer la racine de l'arbre LDAP :

```
dn: dc=mondomaine,dc=com
objectClass: dcObject
objectClass: organization
o: Plastigray SAS
dc: plastigray
```

Commande pour ajouter la racine :

```
ldapadd -x -D "cn=admin,dc=mondomaine,dc=com" -w admin -f AjoutRacine.ldif
```

Voici un exemple de fichier LDIF (AjoutFiche.ldif) pour créer une nouvelle fiche :

```
dn: cn=Tony GALMICHE,dc=mondomaine,dc=com
objectClass: inetOrgPerson
cn: Tony GALMICHE
givenName: Tony
sn: GALMICHE
```

Commande pour ajouter la fiche :

```
ldapadd -x -D "cn=admin,dc=mondomaine,dc=com" -w admin -f AjoutFiche.ldif
```

## Fichier LDIF pour modifier des enregistrements

Les commandes de modification ont la syntaxe suivante :

```
dn: distinguished name
  changetype {{TYPE}}
  change operation identifier
  list of attributes...
...
-
  change operation identifier
  list of attributes
...

```

TYPE peu avoir l'une des valeurs suivantes :

- add (ajout d'une entrée),
- delete (suppression),
- modrdn (modification du RDN),
- modify (modification : add, replace, delete d'un attribut)

Le fichier « ModifFiche.ldif » ci-dessous permet d'ajouter le numéro de téléphone :

```
dn: cn=Tony GALMICHE,dc=mondomaine,dc=com
changetype: modify
add: telephonenumber
telephonenumber: 03 80 97 98 99

```

Commande pour modifier la fiche :

```
ldapadd -x -D "cn=admin,dc=mondomaine,dc=com" -w admin -f ModifFiche.ldif
```

## Fichier LDIF pour supprimer des enregistrements

Le fichier « SuppFiche.ldif » ci-dessous permet de supprimer une fiche :

```
dn: cn=Tony GALMICHE,dc=mondomaine,dc=com
changetype: delete

```

Commande pour supprimer la fiche :

```
ldapadd -x -D "cn=admin,dc=mondomaine,dc=com" -w admin -f SuppFiche.ldif
```

## Commande pour rechercher des enregistrements

Rechercher les enregistrements contenant un attribut objectclass (donc tous) depuis la racine :

```
ldapsearch -x -b "dc=mondomaine,dc=com" "objectclass=*"

```

Rechercher les enregistrements contenant un attribut cn dans la branche Eloyes :

```
ldapsearch -x -b "o=Eloyes,dc=mondomaine,dc=com" "cn=*"
```

Rechercher les enregistrements donc l'attribut dc se termine par gray depuis la racine :

```
ldapsearch -x -b "dc=mondomaine,dc=com" "dc=*gray"
```

## Sauvegarde et Restauration d'une base de données LDAP

La commande suivante permet de générer un fichier .LDIF contenant la base complète :

```
slapcat -l DumpLDAP.ldif -b "dc=mondomaine,dc=com"
```

## LDAP Browser

LDAP Browser est un programme en Java, permettant de consulter et de modifier une base LDAP :

<http://www-unix.mcs.anl.gov/gawor/ldap/>

## Exemples de scripts PHP

### Exemple de script PHP pour se connecter au serveur LDAP

```
$server="localhost";
$port="389";
$dn="dc=mondomaine,dc=com";
$rootdn="cn=admin,$dn";
$rootpw="admin";

$ds=ldap_connect($server,$port);
ldap_set_option($ds, LDAP_OPT_PROTOCOL_VERSION, 3);
$r=ldap_bind($ds,$rootdn,$rootpw)
    or die ("Impossible de se connecter au serveur ! \n");
echo "Authentification sur le serveur OpenLDAP -> OK \n\n";
```

### Exemple de script PHP pour rechercher des enregistrements

```
$sr=ldap_search($ds,$dn,"(objectclass=*)");
if ($sr) {
    $info=ldap_get_entries($ds,$sr);
    echo $info["count"]." enregistrements dans OpenLDAP \n";
    for ($i=0;$i<=$info["count"];$i++) {
        echo "$i - ".$info[$i]["dn"]." \n";
    }
}
```

### Liste partielle des attributs de la classe « organization »

Attribut	Description
----------	-------------

businessCategory	Activité professionnelle d'une entreprise ou d'une personne
c	Code du pays en deux lettres (respectant le standard ISO 3166)
cn	Nom de l'objet (common name)
description	Description de l'objet
distinguishedName	Nom distingué (utilisé par d'autres attributs par héritage)
facsimileTelephoneNumber	Numéro de fax
givenName	Prénom de la personne
houseIdentifier	Identifiant d'un bâtiment
initials	Initiales d'une personne
internationalSDNNumber	Numéro ISDN
l	localité de l'objet (géographique)
member	Distinguished Name des membres
name	Nom (utilisé par d'autres attributs par héritage)
o	Nom de l'organisation
objectClass	Classe d'objets
ou	Unité organisationnelle (branche de l'organisation)
owner	Nom du propriétaire de l'objet
postalAddress	Adresse postale (sans le code postal)
postalCode	Code postal
postalOfficeBox	Boîte aux lettres (postale)
presentationAddress	Adresse réseau de la présentation de l'objet (généralement une URL vers la présentation en ligne)
protocolInformation	Attribut complémentaire à presentationAddress pour définir le protocole à utiliser
registeredAddress	Adresse postale pour des envois de courriers recommandés et de colis
seeAlso	DN d'objets complémentaires
serialNumber	Numéro de série de l'objet
sn	Nom de famille de la personne (surname)
st	Etat ou région (state)
streetAddress	Nom de la rue et assimilé (boulevard, ...)
telephoneNumber	Numéro de téléphone
title	Titre de la personne (différent de fonction)
uid	Identifiant unique de l'objet
userPassword	Mot de passe de l'utilisateur

## Liste partielle des attributs de la classe « inetOrgPerson »

Nom	Sémantique	Mono	Obl	Lecture	Utilisation
cn	nom(s) complet(s) (d'usage) sans accent		O	RI	Ordre : Nom, Prénom. Attention : pas d'accent pour simplifier les recherches. Voir aussi displayName. Exemple : "Bugale Jerome"
displayName	nom complet avec accents				Version accentuée de la valeur principale de cn. Exemple : "Bugalé Jérôme"
employeeType	type de personnel		D ?	RI ?	Définir les grandes familles ?
facsimileTelephoneNumber	Numéro de fax			RI	Format E 123 (cf Références)
givenName	Prénom	M		D RI	idem sn. Exemple : "Jérôme"
l					localité de l'objet (géographique)
labeledURI	Page personnelle			RI	

mail	adresse mel canonique	M	RI ?	
mobile	numéro de téléphone mobile		RI	Format E 123 (cf Références)
o				Nom de l'organisation
ou				Unité organisationnelle (branche de l'organisation)
postalAddress	Adresse postale		RI	Adresse complète. Attention au format ("\$" séparateur, voir RFC2256)
postalCode	Code postal			
preferredLanguage	langue préférée	M	RI	cf RFC2068
sn	Nom		O RI	Contient le nom d'usage. Il est possible d'ajouter le nom de famille (nom patronymique) en seconde valeur. Tout caractère diacritique. Première lettre en majuscule. Voir aussi cn. Exemple : "Bugalé".
st				Etat ou région (state)
telephoneNumber	numéro de téléphone fixe		RI	Format E 123 (cf Références)
title	titre		RI	Responsabilité ; président, directeur, ... (cf Harpège ?). Code ou intitulé complet ?
uid	identifiant unique	M	D R	utilisé comme rdn, contenu indifférent mais aussi court que possible
userCertificate	certificat X509		A ?	