# TP5 : Installation et configuration d'un annuaire LDAP

EL GHORFI Rabii

LDAP signifie Lightweight Directory Access Protocol, c'est une version simplifiée du protocole X500. Vous pourrez trouver une présentation détaillée sur Wikipédia .

Pour expliquer rapidement, toutes les informations sont stockées dans un arbre. Vous devez déterminer l'arborescence des annuaires ou, autrement dit, des informations de l'arbre (Directory Information Tree) . Nous allons commencer ici avec un exemple simple contenant seulement 2 nœuds en plus de la racine :

- Le nœud "People" , où seront stockés vos utilisateurs
- Le nœud "Groups" , où seront enregistrés vos groupes

Vous devez commencer par déterminer ce que sera la racine de votre LDAP. Par défaut, votre arbre peut être déterminé à partir de votre domaine Internet. Si votre domaine est exemple.com , votre racine sera dc=exemple,dc=com .

Dans le cas où le nom de domaine déclaré sur la machine n'est pas celui que l'on souhaite utiliser, il faut modifier le nom dans les fichiers "/etc/hostname" et "/etc/hosts" et redémarrer le serveur AVANT l'installation des paquets.

# Installation

Avant tout, installons le daemon du serveur ldap (slapd) sur le serveur. Pour cela, il suffit d'installer les paquets **apt://slapd,ldap-utils**.

```
sudo apt-get install slapd
```

```
sudo apt-get install ldap-utils
```

On vous demandera votre mot de passe administrateur et votre nom de domaine. Renseignez-les. Parfois on ne vous demandera que le mot de passe et on ne vous demandera rien concernant le nom de domaine car l'installeur récupère directement le nom de domaine de la machine. Si vous souhaitez renseigner ces champs faites :

```
sudo dpkg-reconfigure slapd
```

Voici brièvement les réponses attendues pour une installation standard :

```
1.Passer la configuration d'OpenLDAP ? non
2.Nom de domaine ? example.com
3.Nom de votre société ? masociété
4.Quelle base de donnée ? hdb
5.Voulez-vous que la base de donnée soit effacée lorsque slapd est purgé ? oui
6.Supprimer les anciennes bases de données ? oui
7.Mot de passe administrateur ? VotreMotDePasse
8.Confirmer ce mot de passe ? VotreMotDePasse
9.Authoriser le protocol LDAPv2 ? non
```

Mais seulement quelques changements seront effectués sur la configuration par défaut. Tout le reste va se jouer dans le fichier `/etc/ldap/ldap.conf`.

Nous allons commencer par enregistrer le mot de passe administrateur (de LDAP) dans le fichier de configuration en éditant ce fichier. Ce serait une folie de vouloir enregistrer votre mot de passe en clair donc nous allons générer votre mot de passe en chiffré avec la commande : `sudo slappasswd`

On obtient quelque chose dans ce genre :

```
$ sudo slappasswd
New password:
Re-enter password:
{SSHA}d2BamRTgBuhC6SxC0vFGWol31ki8iq5m
```

Cet exemple montre la définition de votre mot de passe en utilisant le mot de passe "secret". (D'après l'implémentation de SSHA, votre résultat peut varier) .

Depuis Ubuntu Linux Intrepid Ibex, l'installation de slapd ne crée pas de fichier **slapd.conf**, tous les éléments de configuration sont désormais dans le dossier **/etc/ldap/slapd.d/**.

### Configuration du ficher ldap.conf

Éditez le fichier **/etc/ldap/ldap.conf** avec les droits administrateurs.
S'il n'est pas déjà présent, créez ce fichier avec les droits administrateurs. On renseigne alors les informations suivantes :

```
ldap_version 3
URI ldap://localhost:389
SIZELIMIT 0
TIMELIMIT 0
DEREF never
BASE dc=example, dc=com
```

Toutes les informations relatives a **slapd.d** (dossier remplaçant slapd.conf) sont maintenant inscrites au moment où on lance la commande *dpkg-reconfigure slapd*

## Remplir LDAP

L'annuaire a été créé lors de l'installation, il est maintenant temps de le remplir. Il sera rempli avec des entrées classiques qui seront compatibles avec la structure d'un annuaire (pour un annuaire partagé), avec les comptes classiques (pour une authentification Web par exemple) et avec les comptes Unix (posix).
L'annuaire LDAP peut être rempli par des fichiers ldif (ldif signifie ldap directory interchange format). Générez ce fichier d'exemple (init.ldif) :
La phrase "Générez ce fichier d'exemple" n'est pas claire. On ne comprend pas ce qu'on nous demande de faire véritablement. Créer un fichier n'importe où dans lequel on met ce fichier d'exemple ?

Effectivement il faut créer le fichier init.ldif, qu'on utilisera plus bas

```
$ vim ~/init.ldif
```

Contenu du fichier :

```
# fichier de données : ~/init.ldif
dn: dc=example,dc=com
objectClass: dcObject
objectClass: organizationalUnit
dc: example
ou: Example Dot Com

dn: ou=people,dc=example,dc=com
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=example,dc=com
objectClass: organizationalUnit
ou: groups

dn: uid=lionel,ou=people,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: lionel
sn: Porcheron
givenName: Lionel
cn: Lionel Porcheron
displayName: Lionel Porcheron
uidNumber: 1000
```

```
gidNumber: 10000
gecos: Lionel Porcheron
loginShell: /bin/bash
homeDirectory: /home/lionel
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: lionel.porcheron@example.com
postalCode: 31000
l: Toulouse
o: Example
mobile: +33 (0)6 xx xx xx xx
homePhone: +33 (0)5 xx xx xx xx
title: System Administrator
postalAddress:
initials: LP

dn: cn=example,ou=groups,dc=example,dc=com
objectClass: posixGroup
cn: example
gidNumber: 10000
displayName: Example group
```

Dans l'exemple ci-dessus, la structure de l'annuaire, c'est-à-dire un utilisateur et un groupe ont été créés. Dans d'autres exemples vous auriez pu voir le paramètre "objectClass: top" ajouté dans plusieurs entrées, mais c'est le comportement par défaut donc pas besoin de le mettre :)
Maintenant ajoutez vos entrées à LDAP :

- Arrêtez le daemon :
  `sudo /etc/init.d/slapd stop`
- Supprimer ce qui a été ajouté automatiquement à l'installation :
  `sudo rm -rf /var/lib/ldap/*`

Ajouter les données :
```
sudo slapadd -l ~/init.ldif
```

Si vous rencontrez le message type :
```
Entry (cn=example,ou=groups,dc=example,dc=com), attribute 'displayName' not allowed
slapadd: dn="cn=example,ou=groups,dc=example,dc=com" (line=46): (65) attribute 'displayName'
not allowed
```

Il faut commenter la ligne 46 comme ceci :
```
#displayName: Example group
```

Puis refaire :
```
sudo rm -rf /var/lib/ldap/*
```

Donner les droits de lecture aux fichiers de la base de données
```
sudo chown -R openldap:openldap /var/lib/ldap
```

N'oublions pas de relancer ldap :
```
sudo /etc/init.d/slapd start
```

Nous allons pouvoir vérifier que les données ont été correctement ajoutées avec les outils du paquet `ldap-utils`.
Pour effectuer une recherche dans les annuaires LDAP il vous suffit de faire :
```
ldapsearch -xLLL -b "dc=example,dc=com" uid=lionel sn givenName cn
dn: uid=lionel,ou=people,dc=example,dc=com
cn: Lionel Porcheron
sn: Porcheron
givenName: Lionel
```

Une rapide explication :

- -x désactive l'authentification SASL
- -LLL empêche l'affichage des informations LDIF
- -b indique la branche utilisée

NE PAS OUBLIER d'ajouter le user qui doit administrer le service ldap au group openldap à créer lors de l'installation du paquet ou bien de donner les bons droits sur les fichiers /etc/ldap/ldap.conf et /var/lib/ldap/*

# Utiliser votre serveur LDAP

Maintenant que votre serveur est prêt et démarré vous pouvez :

- Authentifier vos utilisateurs dans l'annuaire comme expliqué dans la documentation LDAPClientAuthentication
- Authentifier vos utilisateurs via une application web
- Utiliser l'annuaire comme une base de données pour votre client mail
- Et bien plus encore !!!

De manière plus concrète, il existe des solutions simples à installer et qui vous permettent un excellent accès à votre annuaire, que ce soit en visualisation comme en création/édition.

#### Pré-requis

- Avoir un serveur WEB installé, (php Apache ou LAMP).

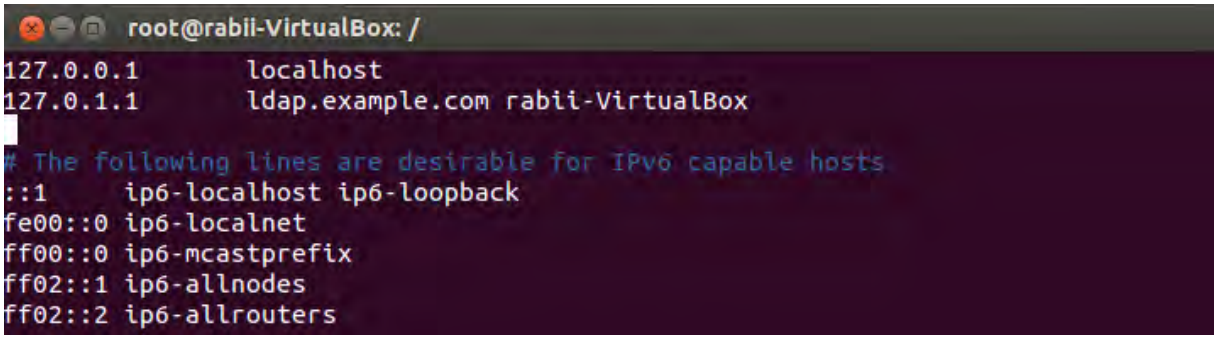
Tapez la commande suivante :

```
sudo apt-get install php5
```

**Configuration du fichier etc/hosts**

Etant donné que la machine linux sera membre de votre domaine, vous devez donc modifier le nom de votre machine. Pour cela, modifier le fichier "/etc/hosts" pour y indiquez le nom de le nom de domaine de la machine en plus du nom par défaut. Syntaxe : [nom de domaine] [nom de la machine Ubuntu]

```
gedit /etc/hosts
```




Remplacer la ligne:
127.0.1.1 rabii-VirtualBox
Par:
127.0.1.1 ldap.example.com rabii-VirtualBox

Maintenant, notre machine Ubuntu possède 2 noms :

- rabii-VirtualBox: Le nom normal de la machine
- ldap.example.com : Le nom de domaine de la machine

**Installation de phpldapadmin :**

L'interface Web utilisée dans ce TP n'est pas compatible avec la version 13.10 d'Ubuntu, à titre d'information : La version 13.10 n'est pas une version LTS (du moins, à l'heure actuelle) alors que la version 12.04 l'est.

Pour installer cette interface web, tapez simplement la commande suivante :

```
sudo apt-get install phpldapadmin
```

Note : Etant donné qu'il s'agit d'une interface web codée en PHP, le serveur Web Apache sera automatiquement installé avec le module PHP ainsi que les autres dépendances requises par ces composants.

**Autoriser OpenLDAP dans le parefeu :**

Pour commencer, lister les applications disponibles comme ceci :

```
sudo ufw app list
```

Maintenant que vous savez comment est nommé le serveur LDAP, autoriser le en tapant ceci :

```
sudo ufw allow "OpenLDAP LDAP"
```

Note : Cette commande autorisera cette application pour les 2 versions du protocol TCP/IP :
La règle a été ajoutée
La règle a été ajoutée (v6)

**Activer le parefeu et vérification :**

Pour commencer, vérifier l'état du pare-feu en tapant la commande suivante :

```
sudo ufw status
```

Si le pare-feu est activé, les applications autorisées dans le pare-feu s'afficheront également. Dans le cas contraire, vous pouvez l'activer en tapant la commande suivante. Note : Le pare-feu n'est pas activé par défaut sous Ubuntu 12.04 LTS.

```
sudo ufw enable
```

Une fois le pare-feu activé, Ubuntu vous affichera le message suivant : Le pare-feu est actif et lancé au démarrage du système

Vérifiez ensuite que l'application "OpenLDAP LDAP" est bien autorisée dans le pare-feu.

```
sudo ufw status
```

Si cette application apparait dans la liste, c'est que celle-ci est bien autorisée par le pare-feu.

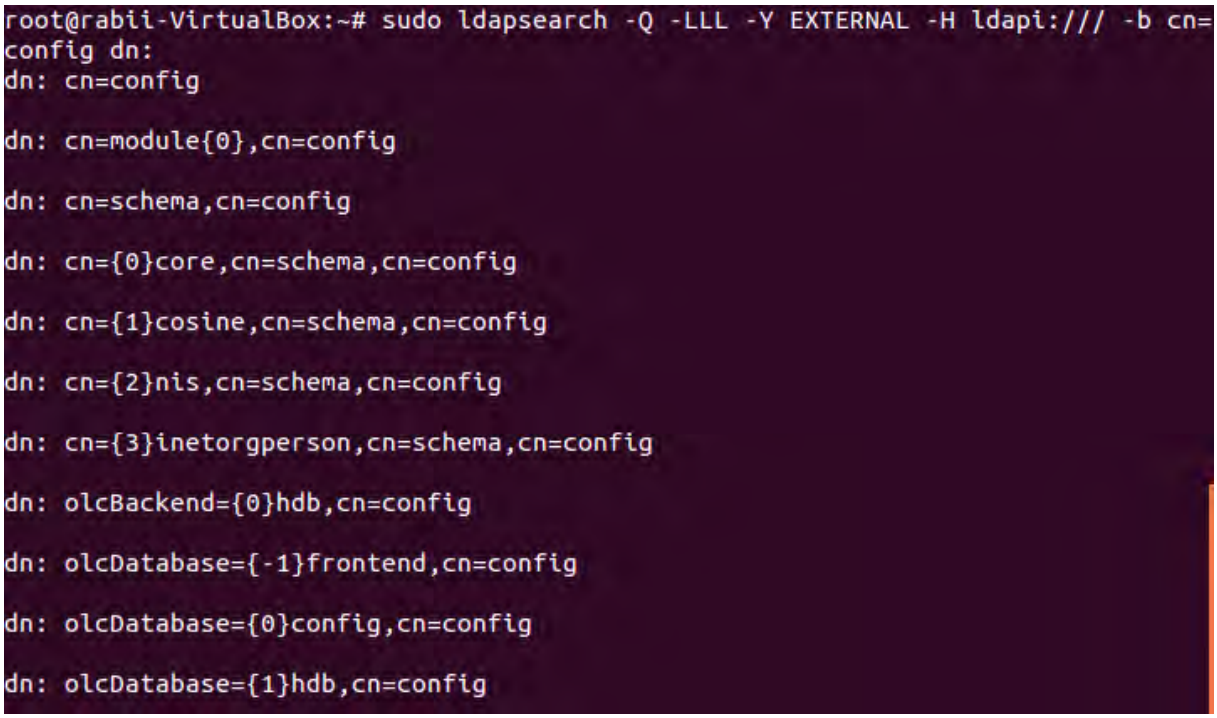
```
root@rabii-VirtualBox:~# sudo ufw status
État : actif

Vers                       Action      Depuis
----                       ------      ------
OpenLDAP LDAP              ALLOW       Anywhere
OpenLDAP LDAP (v6)         ALLOW       Anywhere (v6)
```

**Test de la connexion au serveur :**

Pour tester la connexion au serveur LDAP, nous allons utiliser les outils en ligne de commandes "OpenLDAP utilities (ldap-utils)" que nous avons installé au début du TP.

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config dn:
```

Si tout se passe bien, vous devriez obtenir ceci




**Connexion à l'interface Web phpLDAPadmin**

phpLDAPadmin se connecte à notre serveur LDAP pour pouvoir ajouter ou supprimer ou modifier les informations du serveur. Avant de pouvoir ouvrir l'interface graphique de phpLDAPadmin assurer vous que :

Le serveur web est lancé :

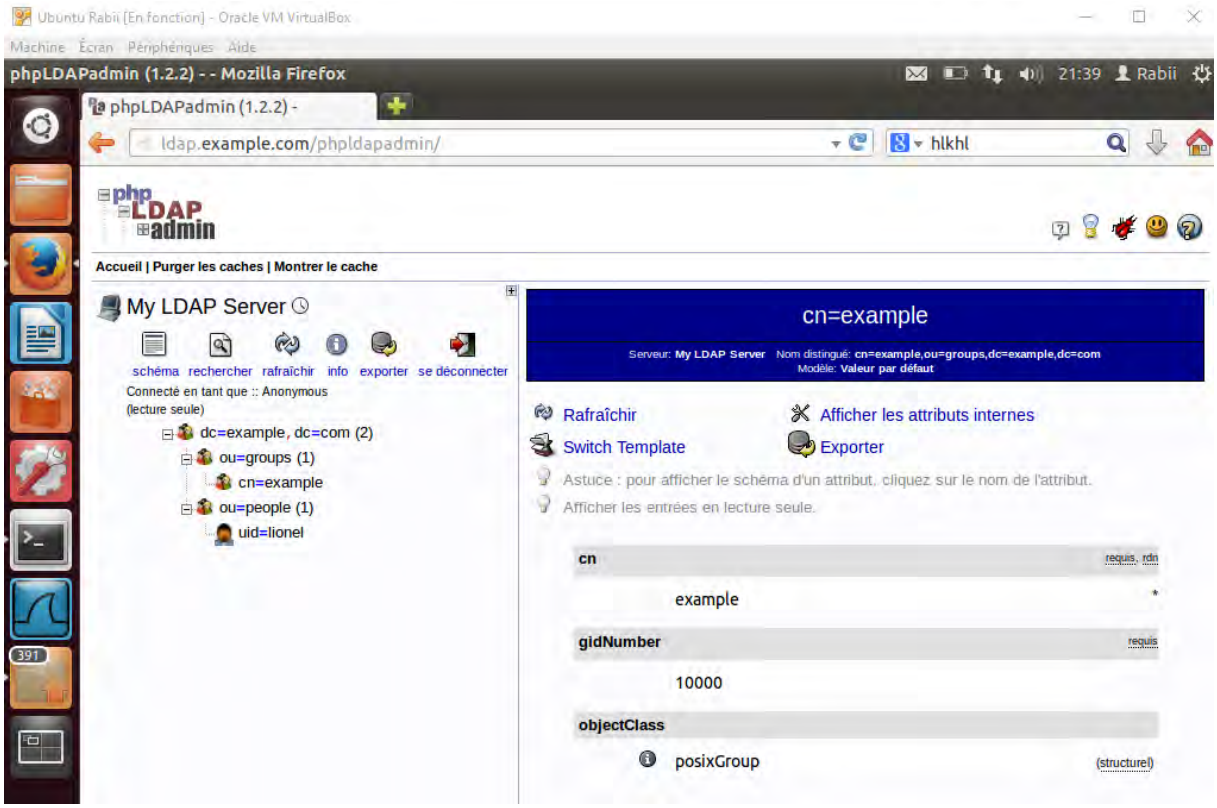
```
sudo /etc/init.d/apache2 start
```

Le serveur ldap est lancé :

```
sudo /etc/init.d/slapd start
```

Enfin ouvrir le lien suivant sur votre navigateur web :

```
Ldap.example.com/phpldapadmin
```




**Problème : Memory Limit low**

Si lorsque vous allez sur l'interface web de phpldapadmin, vous avez cette erreur : Memory Limit low. Your php memory limit is low - currently 16M . Éditer en admin le fichiers php.ini :

```
cd /etc/php5/apache2/
sudo nano php.ini
```

trouvez la section suivante et changez la valeur memory_limit = 16M en mettant 50M :

```
;;;;;;;;;;;;;;;;;;;
; Resource Limits ;
;;;;;;;;;;;;;;;;;;;

max_execution_time = 30     ; Maximum execution time of each script, in seconds
max_input_time = 60 ; Maximum amount of time each script may spend parsing   request data
;max_input_nesting_level = 64 ; Maximum input variable nesting level
memory_limit = 50M      ; Maximum amount of memory a script may consume (16MB)
```

Il suffit ensuite de recharger la configuration de apache pour que la modification soit prise en compte :

```
sudo /etc/init.d/apache2 reload
```

puis relancer votre serveur ldap :

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

# Réplication des données LDAP

Le service LDAP peut vite devenir un service hautement critique dans votre système d'information : tout dépend (ou peut dépendre) de LDAP :

- Authentification
- Autorisation
- Mail
- …

Ce serait donc une bonne idée de créer un système redondant. Le mini HOWTO ci-dessous vous permettra de le faire.

**Introduction**

Avec OpenLDAP 2.2 (sur Breezy et Dapper), la réplication est basée sur une communication maître-esclave.

**ATTENTION**

Vous devez vous rappeler que les modifications devraient toujours être faites sur le maître ! Si vous modifiez un esclave, les modifications seront perdues dès la synchronisation suivante :/

**Le maître**
Sur le maître, vous devez modifier la section "base de donnée" du fichier de configuration `/etc/ldap/slapd.conf` pour ajouter une instruction de réplication. L'exemple suivant montre une réplication sur le serveur `ldap-2.example.com` avec le Manager *user* et le mot de passe *secret*. Le fichier de log est l'emplacement où les données seront stockées avant d'être envoyées sur le(s) serveur(s) esclave(s).

Comment faire pour les versions ou le fichier slapd.conf n'existe plus, comme c'est dit plus haut??

```
replica uri=ldap://ldap-2.example.com:389 binddn="cn=Manager,dc=example,dc=com"
bindmethod=simple
credentials=secret

replogfile      /var/lib/ldap/replog
```

Il ne reste plus qu'a redémarrer votre serveur LDAP :)

**Le(s) Esclave(s)**

Sur le(s) serveur(s) esclave(s) , il vous suffit d'autoriser votre serveur maître à mettre à jour la base de donnée LDAP. Pour cela ajoutez les lignes suivantes dans votre `/etc/ldap/slapd.conf` à la section base de données :

```
updatedn        cn=Manager,dc=example,dc=com
updateref       ldap://ldap-1.example.com
```

Redémarrez votre serveur LDAP (l'esclave).