

Introduction

Ce TP est axé sur l'expérience pratique. L'approche adoptée guide étape par étape, en mettant en lumière tous les détails essentiels pour assurer un fonctionnement optimal. L'amélioration de l'installation sur divers aspects sera abordée au fur et à mesure. Il est recommandé de suivre les différentes manipulation dans l'ordre chronologique.

1. Installation et configuration.
2. Modification des paramètres par défaut.
3. Construire une DIT.
4. Modification du DIT.

Installation et configuration de OpenLDAP :

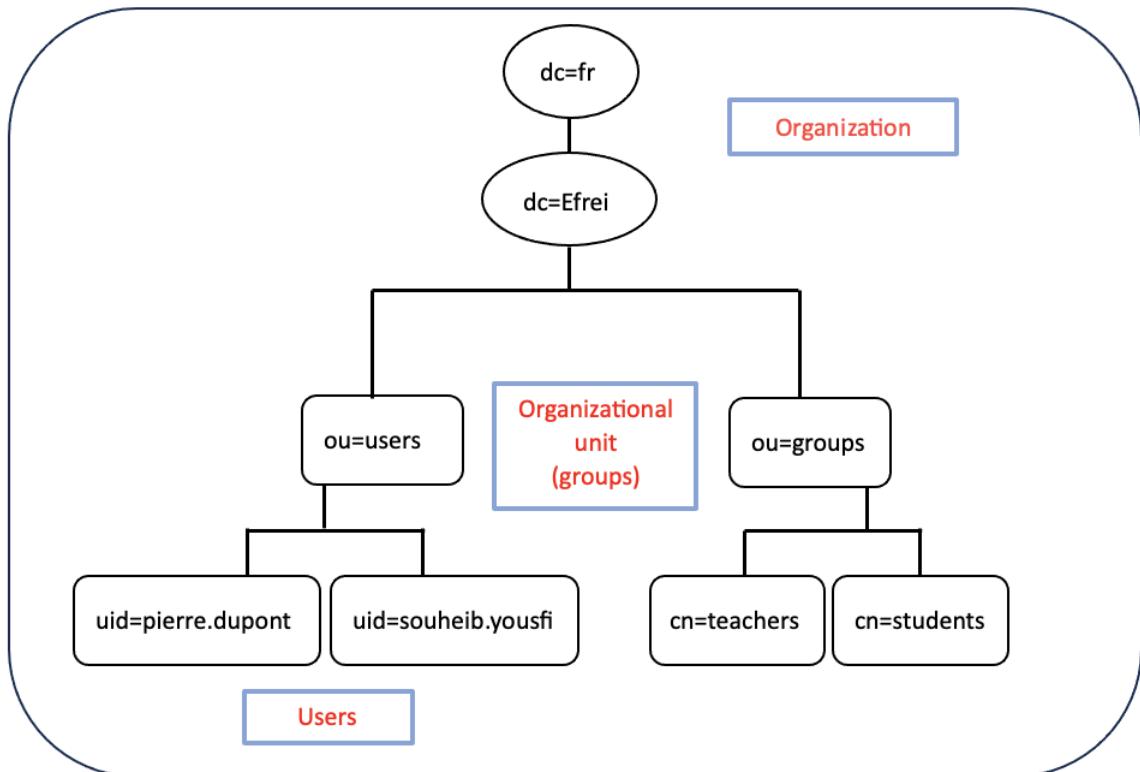
OpenLDAP, en tant qu'implémentation open-source du protocole LDAP (Lightweight Directory Access Protocol), offre un cadre robuste pour la mise en place d'un service d'annuaire. Un service d'annuaire, essentiel dans un réseau, constitue une base de données centralisée qui stocke et organise des informations sur les utilisateurs, les ressources et les entités.

L'organisation des données au sein d'OpenLDAP suit une structure hiérarchique arborescente. Cette hiérarchie permet une organisation logique et personnalisée des informations. Typiquement, les données du répertoire LDAP commencent par des entités de niveau supérieur telles que les pays, suivies par des subdivisions géographiques, des organisations, des unités organisationnelles, des personnes, et d'autres entités.

Dans le cadre de ce projet, notre objectif est de créer une arborescence spécifique dans OpenLDAP. Cette arborescence sera structurée de manière à démontrer la flexibilité offerte par LDAP pour organiser les données de manière cohérente. Nous allons configurer les niveaux d'entrées pour représenter le pays, l'organisation, l'unité organisationnelle, et les personnes.

À travers ce TP, les étudiants auront l'opportunité de se familiariser avec la configuration et la gestion de l'arborescence de répertoire dans OpenLDAP, renforçant ainsi leur compréhension pratique du fonctionnement d'un service d'annuaire basé sur LDAP.

Pour ce TP, nous allons créer l'arborescence suivante :



Un service d’annuaire traditionnel comprend un processus réseau qui traite les requêtes et une base de données stockée sur le système de fichiers. Dans le contexte d’OpenLDAP, le processus réseau est appelé slapd. L’utilisateur système associé à slapd est généralement openldap. La première étape consiste à l’installation de slapd dans les deux machines serveur et client. Pour faciliter le processus, la machine serveur sera connectée en remote à la machine client pour un affichage plus simple. La machine kali va être le serveur, et pierre le client dans une machine Ubuntu.

— Installation des packages :

- Commençons par préparer la machine du client pierre :

Ajouter un utilisateur pierre :

```
root@universite:/home/ubuntu/Desktop# adduser pierre
```

Lui donner les privilèges possibles :

```
root@universite:/home/ubuntu/Desktop# nano /etc/sudoers
pierre ALL=(ALL) ALL
root@universite:~# su - pierre
pierre@universite:~$
```

Changer le hostname :

```
pierre@Efrei:~/Desktop$ sudo hostnamectl hostname
[sudo] password for pierre:
Efrei.fr
```

- Installation de **slapd** et **ldap-utils** :

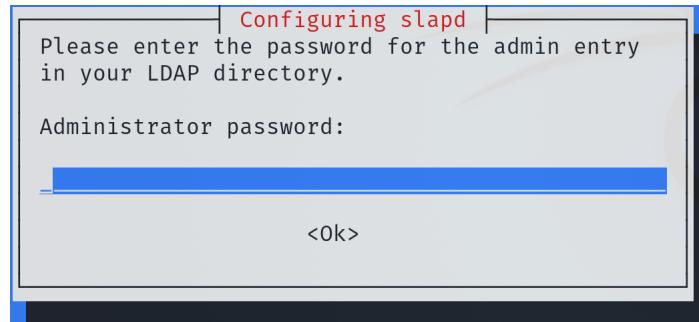
```

(kali㉿kali)-[~/Desktop]
$ hostname -I
10.0.2.15 192.168.56.20

(kali㉿kali)-[~/Desktop]
$ sudo apt-get install slapd ldap-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ldap-utils is already the newest version (2.4.59+dfsg-1).
ldap-utils set to manually installed.
Suggested packages:
  libsasl2-modules libsasl2-modules-gssapi-mit
  | libsasl2-modules-gssapi-heimdal
The following NEW packages will be installed:
  slapd
0 upgraded, 1 newly installed, 0 to remove and 377 not upgraded.
Need to get 1,445 kB of archives.
After this operation, 4,576 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y

```

pierre@Efrei:~\$ hostname -I
10.0.2.15 192.168.56.15
pierre@Efrei:~\$ sudo apt-get install slapd ldap-utils
[sudo] password for pierre:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ldap-utils is already the newest version (2.5.16+dfsg-0ubuntu0.22.04.2).
slapd is already the newest version (2.5.16+dfsg-0ubuntu0.22.04.2).
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
pierre@Efrei:~\$



- Configuration initiale :

Pour créer un squelette de configuration de slapd, nous allons utiliser la commande **dpkg-reconfigure** comme suit :

```

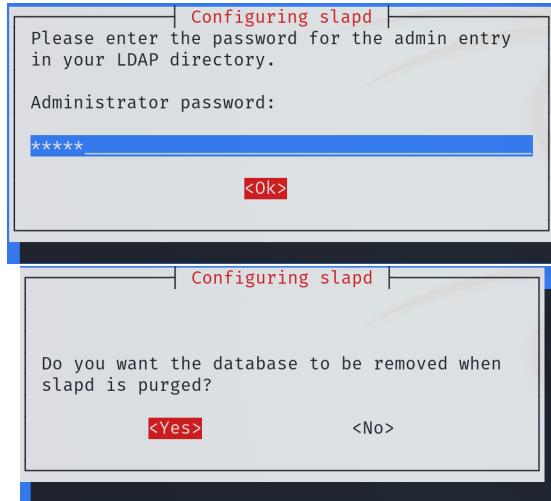
(kali㉿kali)-[~/Desktop]
$ sudo dpkg-reconfigure slapd

```

Configuring slapd
If you enable this option, no initial configuration or database will be created for you.
Omit OpenLDAP server configuration?
<Yes> <No>

Configuring slapd
The DNS domain name is used to construct the base DN of the LDAP directory. For example, 'foo.example.org' will create the directory with 'dc=foo, dc=example, dc=org' as base DN.
DNS domain name:
Efrei.fr
<Ok>

Configuring slapd
Please enter the name of the organization to use in the base DN of your LDAP directory.
Organization name:
Efrei
<Ok>



À l'issue de cette étape, la racine `dc=Efri,dc=fr` est créée. L'étape suivante est liée, il s'agit de vérifier l'attribut *organization* pour cette racine.

- Tests Fonctionnels :

Pour commencer, vérifiez la version de votre serveur :

```
(kali㉿kali)-[~/Desktop]
$ slapd -VV
```

Démarrez le service slapd et vérifiez le port d'écoute 389.

```
(kali㉿kali)-[~/Desktop]
$ sudo service slapd status
[sudo] password for kali:
● slapd.service - LSB: OpenLDAP standalone server (Li>
    Loaded: loaded (/etc/init.d/slapd; generated)
    Drop-In: /usr/lib/systemd/system/slapd.service.d
              └─slapd-remain-after-exit.conf
    Active: inactive (dead)
      Docs: man:systemd-sysv-generator(8)
lines 1-6/6 (END)

(kali㉿kali)-[~/Desktop]
$ sudo service slapd start

(kali㉿kali)-[~/Desktop]
$ sudo service slapd status

(kali㉿kali)-[~/Desktop]
$ sudo netstat -laptun | grep slapd
tcp        0      0  0.0.0.0:389                 0.0.0.0:*          LISTEN      13586/slapd
tcp6       0      0  :::389                          :::*           LISTEN      13586/slapd
```

L'affichage de l'annuaire est permis par l'outil `ldapsearch`. Les options `-H`, qui définit l'URL, et `-b`, qui définit la racine à parcourir, sont nécessaires.

En cas d'absence de ces arguments, les arguments par défaut doivent être définis en modifiant le fichier `ldap.conf` ainsi que le localhost qui sera nommé Efri.fr dans `/etc/hosts`. Essayez de consulter votre annuaire avec `ldapsearch -x -H ldap ://@ip_server -D "cn=admin,dc=Efri,dc=fr" -W` avant la modification de `ldap.conf` et après.

```
GNU nano 5.9                                     /etc/hosts *
127.0.0.1      localhost Efri.fr
127.0.1.1      kali

GNU nano 5.9                                     /etc/ldap/ldap.conf *
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE   dc=example,dc=com
#URI    ldap://ldap.example.com ldap://ldap-provider.example.com:666
BASE   dc=Efri,dc=fr
URI    ldap://Efri.fr
#SIZELIMIT 12
#TIMELIMIT 15
#DEREF   never
# TLS certificates (needed for GnuTLS)
TLS_CACERT  /etc/ssl/certs/ca-certificates.crt
```

L'affichage de l'annuaire révèle la présence de la racine du serveur *Distinguished Name* : DN préalablement configurée et créée.

```
(kali㉿kali)-[~/Desktop]
└─$ ldapsearch -x
# extended LDIF
#
# LDAPv3
# base <dc=Efrei,dc=fr> (default) with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# Effrei.fr
dn: dc=Efrei,dc=fr
objectClass: top
objectClass: dcObject
objectClass: organization
o: Effrei
dc: Efrei

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

- **-x** : Utilise l'authentification simple au lieu de SASL. (Simple Authentication and Security Layer).
- **-H** : Spécifie l'URI du serveur, par exemple Efrei.fr.
- **-D** : Spécifie le DN de l'utilisateur, par exemple cn=admin,dc=Efrei,dc=fr.
- **-w** : Spécifie le mot de passe de l'utilisateur pour l'authentification simple.
- **-W** : Demande le mot de passe de l'utilisateur.
- **-s** : Spécifie l'étendue de la recherche :
 - **base** : La recherche porte uniquement sur la base de la recherche.
 - **one** : La recherche porte uniquement sur les enfants de la base.
 - **sub** : La recherche porte sur le sous-arbre dont la racine est la base.
 - **children** : La recherche porte uniquement sur les descendants de la base.
- **-b** : Spécifie le DN de la base de la recherche.

Pour plus de détail, on procède comme suit (à chaque modification, utilisez cette commande pour vérifier votre annuaire) :

```
(kali㉿kali)-[~/Desktop]
└─$ sudo slapcat
```

- Remplissage de l'annuaire :

L'annuaire que nous utilisons, présente deux **OU**, deux **Utilisateurs** et deux **groupes**. Les données à ajouter peuvent être insérées dans un fichier de type **ldif**.

Nous commençons par la création du fichier org_unit.ldif :

```
(kali㉿kali)-[~/Desktop/TP_LDAP]
└─$ cat org_unit.ldif
dn: ou=users,dc=Efrei,dc=fr
objectClass: organizationalUnit

dn: ou=groups,dc=Efrei,dc=fr
objectClass: organizationalUnit
```

Par défaut, OpenLDAP accepte les requêtes anonymes. Ces requêtes permettent d'interroger l'annuaire, mais pas d'effectuer des changements dans la base de données. Si l'on ajoute, supprime ou modifie des objets, il est nécessaire d'authentifier un utilisateur en utilisant l'opération **bind** du protocole LDAP. Les commandes du paquet `ldap-utils` effectuent l'opération bind si l'option **-D** est renseignée avec le DN d'un utilisateur et que l'option **-x** (*simple authentication*) est présente. Le mot de passe peut être fourni sur la ligne de commande avec l'option **-w**, ou saisi comme spécifié dans la commande ci-dessous avec l'option **-W** :

```
(kali㉿kali)-[~/Desktop/TP_LDAP]
$ ldapadd -W -D "cn=admin,dc=efrei,dc=fr" -x -f org_unit.ldif
Enter LDAP Password:
adding new entry "ou=users,dc=efrei,dc=fr"

adding new entry "ou=groups,dc=efrei,dc=fr"
```

Ajoutons les utilisateurs et les groupes en s'appuyant sur le DIT de la page 2. Pour ce faire, créons un deuxième ldif qui illustre les groupes, que nous nommons `groupes.ldif`. Et puis, on l'ajoute à notre annuaire :

```
(kali㉿kali)-[~/Desktop/TP_LDAP]
$ cat groupes.ldif
dn: cn=teachers,ou=groups,dc=efrei,dc=fr
objectClass: posixGroup
objectClass: top
gidNumber: 6001
cn: teachers

dn: cn=students,ou=groups,dc=efrei,dc=fr
objectClass: posixGroup
objectClass: top
gidNumber: 6002
cn: students

(kali㉿kali)-[~/Desktop/TP_LDAP]
$ ldapadd -W -D "cn=admin,dc=efrei,dc=fr" -x -f groupes.ldif
Enter LDAP Password:
adding new entry "cn=teachers,ou=groups,dc=efrei,dc=fr"

adding new entry "cn=students,ou=groups,dc=efrei,dc=fr"
```

Créons un troisième ldif qui illustre les informations sur notre utilisateur pierre qui appartient au groupe students de notre annuaire, que nous nommons `pierre.ldif` :

```
(kali㉿kali)-[~/Desktop/TP_LDAP]
$ cat pierre.ldif
dn: cn=teachers,ou=groups,dc=efrei,dc=fr
objectClass: posixGroup
objectClass: top
gidNumber: 6001
cn: teachers

dn: uid=pierre.dupont,ou=users,dc=efrei,dc=fr
objectClass: person
objectClass: top
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
uidNumber: 6002
gidNumber: 6002
homeDirectory: /home/pierre
loginShell: /bin/bash
uid: pierre.dupont
sn: dupont
cn: pierre dupont
mail: pierre.dupont@efrei.fr
userPassword: pierre
```

```
(kali㉿kali)-[~/Desktop/TP_LDAP]
└─$ ldapadd -W -D "cn=admin,dc=Efrei,dc=fr" -x -f pierre.ldif
Enter LDAP Password:
adding new entry "uid=pierre.dupont,ou=users,dc=Efrei,dc=fr"
```

Créons un quatrième ldif qui illustre les informations sur l'utilisateur souheib qui appartient au groupe teachers de notre annuaire, que nous nommons souheib.ldif :

```
(kali㉿kali)-[~/Desktop/TP_LDAP]
└─$ cat souheib.ldif
dn: uid=souheib.yousfi,ou=users,dc=Efrei,dc=fr
objectClass: person
objectClass: top
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
uidNumber: 6001
gidNumber: 6001
homeDirectory: /home/souheib
loginShell: /bin/bash
uid: souheib.yousfi
sn: yousfi
cn: souheib yousfi
mail: souheib.yousfi@efrei.fr
userPassword: souheib

(kali㉿kali)-[~/Desktop/TP_LDAP]
└─$ ldapadd -W -D "cn=admin,dc=Efrei,dc=fr" -x -f souheib.ldif
Enter LDAP Password:
adding new entry "uid=souheib.yousfi,ou=users,dc=Efrei,dc=fr"
```

Nous remarquons lorsqu'on interroge **slapcat**, les mots de passe sont enregistrés encodés :

```
[userPassword:: c291aGVpYg=]
(kali㉿kali)-[~/Desktop/TP_LDAP]
└─$ echo 'c291aGVpYg=' | base64 -d
souheib
```

Nous devrions changer les mots de passe en les rendant mieux sécurisés. Pour ce faire, nous devons renseigner le Domaine racine (DN) de notre annuaire. Le DN représente le nom d'une entrée (l'utilisateur souheib), sous la forme d'un chemin d'accès à celle-ci, depuis le sommet de l'arborescence :

```
(kali㉿kali)-[~/Desktop/TP_LDAP]
└─$ ldappasswd -H ldap://192.168.56.20 -x -D "cn=admin,dc=Efrei,dc=fr" -W -S
"uid=souheib.yousfi,ou=users,dc=Efrei,dc=fr"
```

Une fois on vérifie notre annuaire on trouve que le nouveau mot de passe de souheib est bien encodé en base 64 et haché (faites le nécessaires pour tous vos utilisateurs).

```
(kali㉿kali)-[~/Desktop/TP_LDAP]
└─$ ldapsearch -x -D "cn=admin,dc=Efrei,dc=fr" -W -b "uid=souheib.yousfi,ou=users,dc=Efrei,dc=fr"

Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <uid=souheib.yousfi,ou=users,dc=Efrei,dc=fr> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# souheib.yousfi, users, Efrei.fr
dn: uid=souheib.yousfi,ou=users,dc=Efrei,dc=fr
objectClass: person
objectClass: top
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
uidNumber: 6001
gidNumber: 6001
homeDirectory: /home/souheib
loginShell: /bin/bash
uid: souheib.yousfi
sn: yousfi
cn: souheib yousfi
mail: souheib.yousfi@efrei.fr
userPassword:: e1NTSEF9WnFKbVhCNU9YSldSd0hvUzAzMU8wY2R5NHRad0t0MXo=


# search result
search: 2
result: 0 Success

# numResponses: 2
```

Interrogation et modification de l'annuaire :

Interrogation spécifique :

```
(kali㉿kali)-[~/Desktop/TP_LDAP]
└─$ ldapsearch -x -b "dc=Efrei,dc=fr" -LLL uid=souheib.yousfi cn mail

dn: uid=souheib.yousfi,ou=users,dc=Efrei,dc=fr
cn: souheib yousfi
mail: souheib.yousfi@efrei.fr
```

Ajout d'un email à un utilisateur :

```
(kali㉿kali)-[~/Desktop/TP_LDAP]
└─$ cat ajout_email.ldif
dn: uid=souheib.yousfi,ou=users,dc=Efrei,dc=fr
changetype:modify
add:mail
mail:souheib.yousfi@efrei.net

(kali㉿kali)-[~/Desktop/TP_LDAP]
└─$ ldapmodify -D cn=admin,dc=Efrei,dc=fr -W -f ajout_email.ldif
Enter LDAP Password:
modifying entry "uid=souheib.yousfi,ou=users,dc=Efrei,dc=fr"

(kali㉿kali)-[~/Desktop/TP_LDAP]
└─$ ldapsearch -x -b "dc=Efrei,dc=fr" -LLL uid=souheib.yousfi cn mail

dn: uid=souheib.yousfi,ou=users,dc=Efrei,dc=fr
cn: souheib yousfi
mail: souheib.yousfi@efrei.fr
mail: souheib.yousfi@efrei.net
```