

Architectures sécurisées d'entreprise

Evaluation du Sprint 1 rendue par Vincent LAGOGUE et Thomas PEUGNET.

Configuration

Création de l'utilisateur Pierre

```
root@tpnagios-1:~/openldap
@UBUNTU ~/openldap 7:30:49
$ adduser pierre
Adding user `pierre' ...
Adding new group `pierre' (1003) ...
Adding new user `pierre' (1002) with group `pierre' ...
Creating home directory `/home/pierre' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for pierre
Enter the new value, or press ENTER for the default
      Full Name []: Pierre
      Room Number []:
      Work Phone []:
      Home Phone []:
      Other []:
Is the information correct? [Y/n]
> @UBUNTU ~/openldap 7:31:31
$ sudo usermod -aG sudo pierre
> @UBUNTU ~/openldap 7:31:48
$
```

```
$ adduser pierre
$ usermod -aG sudo pierre

# Changement du hostname
$ hostnamectl hostname Efrei.fr
```

Installation

```
$ apt install slapd ldap-utils

# Création de la configuration de base
$ dpkg-reconfigure slapd
```

Durant cette étape, choisir les options suivantes :

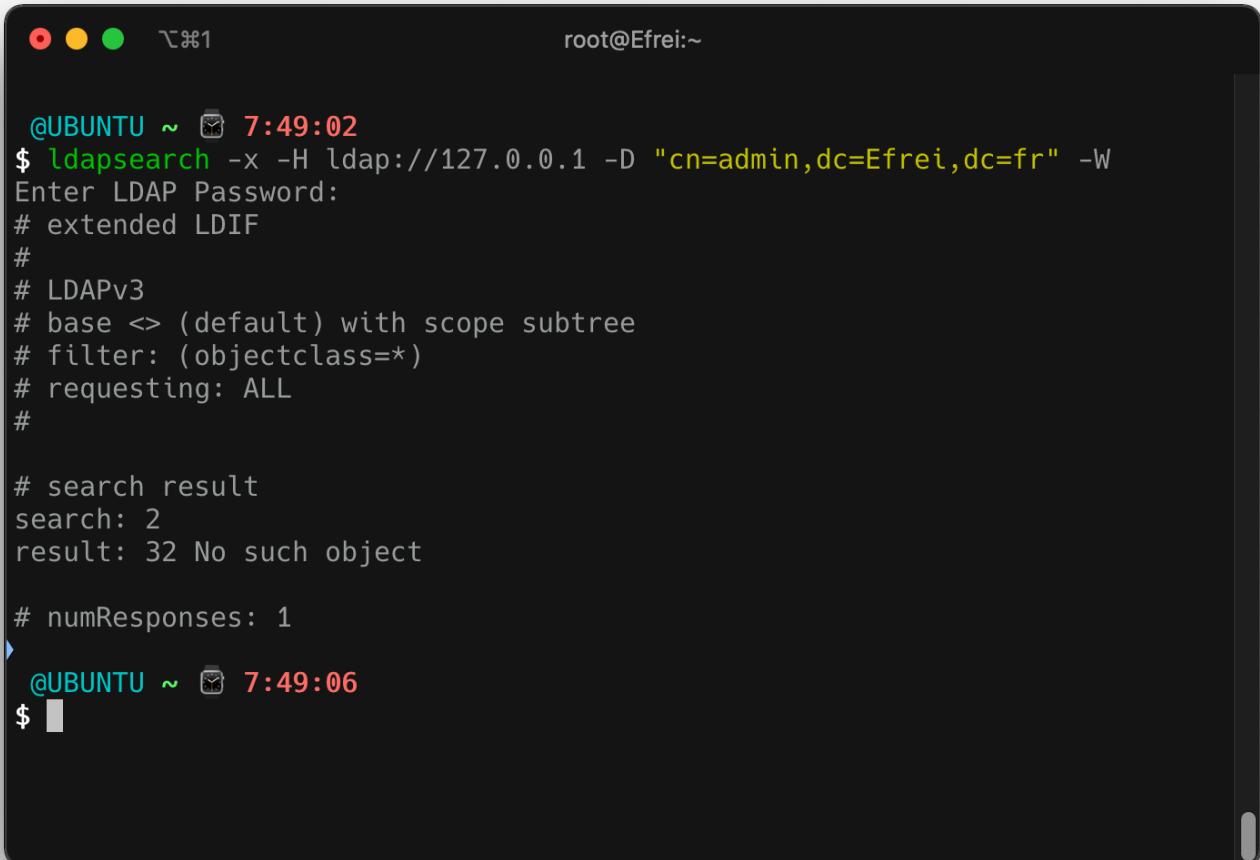
- Omit OpenLDAP server configuration ? No
- DNS Domain Name : Efrei.fr
- Org. Name: Efrei
- Do you want the database to be removed when `slapd` is purged ? : Yes

Vérifier que le service fonctionne correctement : `systemctl status slapd` doit posséder le statut `active`.

Vérifier le port d'écoute du service : `netstat -laptun | grep slapd`

Première connexion

```
$ ldapsearch -x -H ldap://127.0.0.1 -D "cn=admin,dc=Efrei,dc=fr" -W
```



The screenshot shows a terminal window with a dark background and light-colored text. At the top, it displays the system tray icons (red, yellow, green circles) and the terminal prompt `root@Efrei:~`. The main area of the terminal shows the following command and its execution:

```
@UBUNTU ~ 7:49:02
$ ldapsearch -x -H ldap://127.0.0.1 -D "cn=admin,dc=Efrei,dc=fr" -W
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <> (default) with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# search result
search: 2
result: 32 No such object
#
# numResponses: 1
>
@UBUNTU ~ 7:49:06
$
```

Modification du fichier `/etc/hosts` :

Dans le fichier `/etc/ldap/ldap.conf`, modifier les lignes `BASE` et `URI` suivantes :

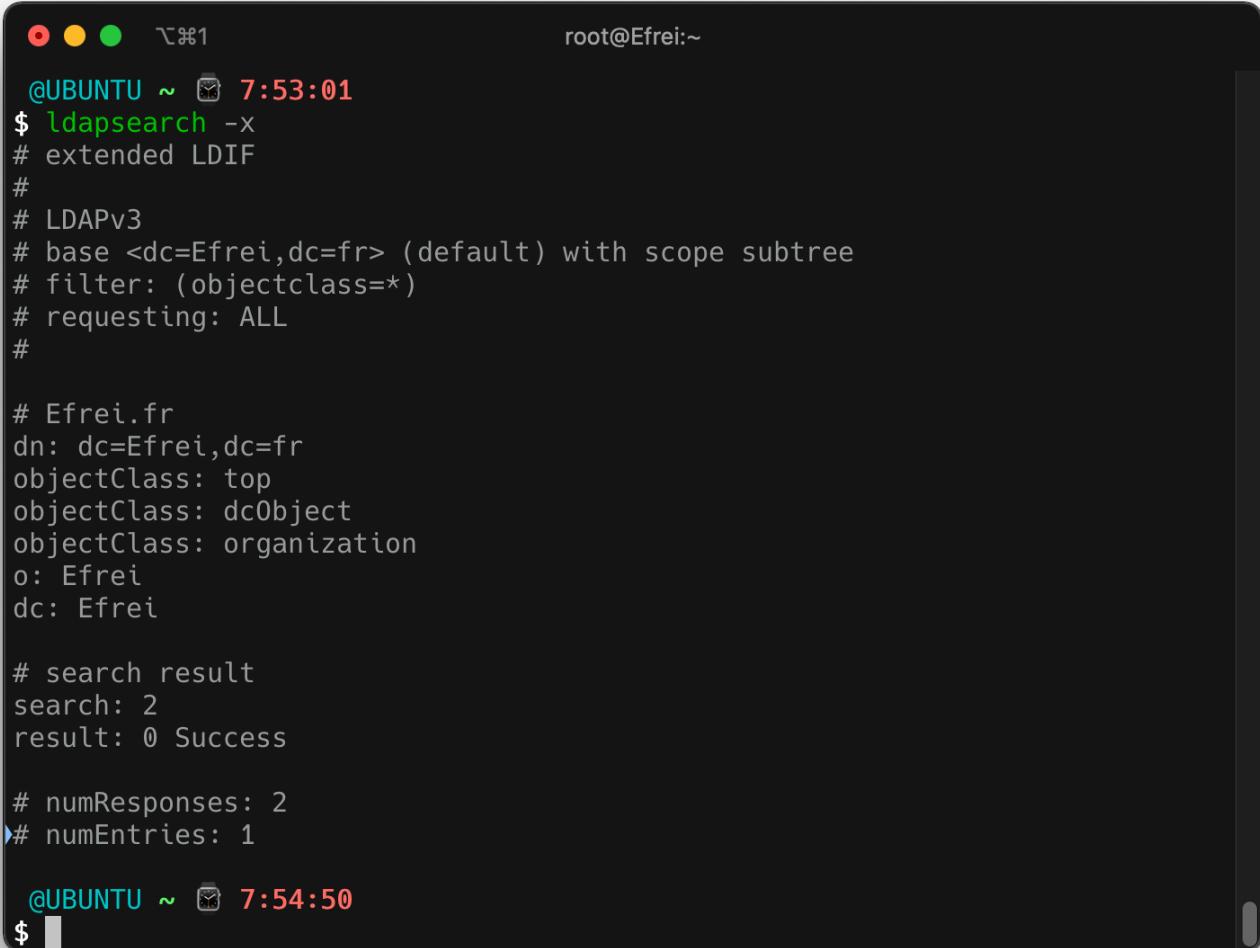
BASE dc=Efrei,dc=fr
URI ldap://Efrei.fr

Ce qui donne le fichier suivant :

```
#  
# LDAP Defaults  
#  
  
# See ldap.conf(5) for details  
# This file should be world readable but not world writable.  
  
BASE dc=Efrei,dc=fr  
URI ldap://Efrei.fr  
  
#SIZELIMIT 12  
#TIMELIMIT 15  
#DEREF never  
  
# TLS certificates (needed for GnuTLS)  
TLS_CACERT /etc/ssl/certs/ca-certificates.crt
```

Vérification du fonctionnement avec la commande suivante :

```
$ ldapsearch -x
```



```
root@Efrei:~  
@UBUNTU ~ 7:53:01  
$ ldapsearch -x  
# extended LDIF  
#  
# LDAPv3  
# base <dc=Efrei,dc=fr> (default) with scope subtree  
# filter: (objectclass=*)  
# requesting: ALL  
#  
  
# Efrei.fr  
dn: dc=Efrei,dc=fr  
objectClass: top  
objectClass: dcObject  
objectClass: organization  
o: Efrei  
dc: Efrei  
  
# search result  
search: 2  
result: 0 Success  
  
# numResponses: 2  
# numEntries: 1  
  
@UBUNTU ~ 7:54:50  
$
```

Pour vérifier le bon fonctionnement du serveur LDAP, à tout moment utiliser :

```
$ slapcat
```

```
root@Efrei:~  
@UBUNTU ~ 7:54:50  
$ slapcat  
dn: dc=Efrei,dc=fr  
objectClass: top  
objectClass: dcObject  
objectClass: organization  
o: Efrei  
dc: Efrei  
structuralObjectClass: organization  
entryUUID: 9fd69654-7621-103e-902b-d3eadb1bce11  
creatorsName: cn=admin,dc=Efrei,dc=fr  
createTimestamp: 20240314073841Z  
entryCSN: 20240314073841.869902Z#000000#000#000000  
modifiersName: cn=admin,dc=Efrei,dc=fr  
modifyTimestamp: 20240314073841Z  
  
@UBUNTU ~ 7:55:53  
$
```

Remplissage de l'annuaire

Organization Units

Créer un fichier `org_unit.ldif` et le remplir avec le contenu suivant:

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

Appliquer le contenu présent dans ce fichier à notre serveur LDAP par la commande suivante :

```
$ ldapadd -W -D "cn=admin,dc=Efrei,dc=fr" -x -f org_unit.ldif
```

```
● ● ●  ↵ 1 root@Efrei:~/openldap

@UBUNTU ~/openldap 7:59:33
$ 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"

@UBUNTU ~/openldap 8:01:36
$
```

Groups

Créer un fichier `groups.ldif` et le remplir avec le contenu suivant:

```
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
```

Appliquer le contenu présent dans ce fichier à notre serveur LDAP par la commande suivante :

```
$ ldapadd -W -D "cn=admin,dc=Efrei,dc=fr" -x -f groups.ldif
```

```
@UBUNTU ~/openldap 8:04:52
$ ldapadd -W -D "cn=admin,dc=Efrei,dc=fr" -x -f groups.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"

@UBUNTU ~/openldap 8:06:09
$
```

Création de l'utilisateur Pierre et Souheib

Créer un fichier `pierre.ldif` et le remplir avec le contenu suivant:

```
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: posixGroup
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
```

Appliquer le contenu présent dans ce fichier à notre serveur LDAP par la commande suivante :

```
$ ldapadd -W -D "cn=admin,dc=Efrei,dc=fr" -x -f pierre.ldif
```

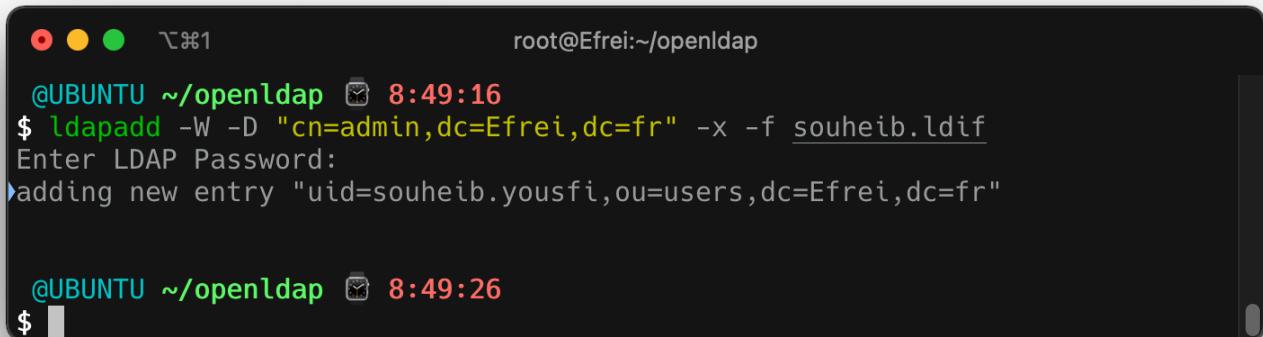
Créer un fichier `souheib.ldif` et le remplir avec le contenu suivant:

```
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
```

Appliquer le contenu présent dans ce fichier à notre serveur LDAP par la commande suivante :

```
$ ldapadd -W -D "cn=admin,dc=Efrei,dc=fr" -x -f souheib.ldif
```



The screenshot shows a terminal window with a dark background and light-colored text. At the top, it says 'root@Efrei:~/openldap'. Below that, the command '\$ ldapadd -W -D "cn=admin,dc=Efrei,dc=fr" -x -f souheib.ldif' is entered. A prompt 'Enter LDAP Password:' follows. The response 'adding new entry "uid=souheib.yousfi,ou=users,dc=Efrei,dc=fr"' is shown. The timestamp '8:49:16' is visible above the password entry. The bottom of the terminal shows the prompt '\$'.

On met à jour le mot de passe à l'aide la commande suivante :

```
$ ldappasswd -H ldap://127.0.0.1 -x -D "cn=admin,dc=Efrei,dc=fr" -W -S
"uid=souheib.yousfi,ou=users,dc=Efrei,dc=fr"
```

Vérification et ajout d'un email

On effectue une requête pour vérifier l'utilisateur à l'aide de la commande suivante :

```
$ ldapsearch -x -b "dc=Efrei,dc=fr" -LLL uid=souheib.yousfi cn mail
```

```
● ○ ●  ↻ 1 root@Efrei:~/openldap

@UBUNTU ~/openldap 9:10:38
$ 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

@UBUNTU ~/openldap 9:12:17
$
```

On crée un nouvel email pour l'utilisateur au sein du fichier `add_email.ldif` :

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

On ajoute un email à l'utilisateur à l'aide de la commande suivante :

```
$ ldapmodify -D cn=admin,dc=Efrei,dc=fr -W -f add_email.ldif
```

```
● ○ ●  ↻ 1 root@Efrei:~/openldap

@UBUNTU ~/openldap 9:15:44
$ ldapmodify -D cn=admin,dc=Efrei,dc=fr -W -f add_email.ldif
Enter LDAP Password:
modifying entry "uid=souheib.yousfi,ou=users,dc=Efrei,dc=fr"
>

@UBUNTU ~/openldap 9:24:33
$
```

Création des certificats

Création d'un certificat à l'aide de la commande suivante :

```
$ mkdir /etc/ldap/ssl && cd /etc/ldap/ssl
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 3650 -nodes
```

(Photo non-contractuelle)

● ● ● ↵ 1

root@Efrei:~/openldap/Cert

```
@UBUNTU ~/openldap/Cert 9:48:37
$ openssl req -new -key server-key.pem -out server-csr.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:France
Locality Name (eg, city) []:Paris
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Efrei
Organizational Unit Name (eg, section) []:RS
Common Name (e.g. server FQDN or YOUR name) []:Efrei.fr
Email Address []:serveur@efrei.fr

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
>An optional company name []:
```

```
@UBUNTU ~/openldap/Cert 9:49:56
$
```

Changer l'appartenance et les permissions avec les commandes suivantes :

```
$ chown openldap:openldap /etc/ldap/ssl/cert.pem
$ chown openldap:openldap /etc/ldap/ssl/key.pem
```

Configuration du certificat avec slapd

Créer un fichier `cert.ldif` avec le contenu suivant :

```
dn: cn=config
changetype: modify
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ldap/ssl/cert.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ldap/ssl/cert.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ldap/ssl/key.pem
-
add: olcTLSVerifyClient
olcTLSVerifyClient: never
```

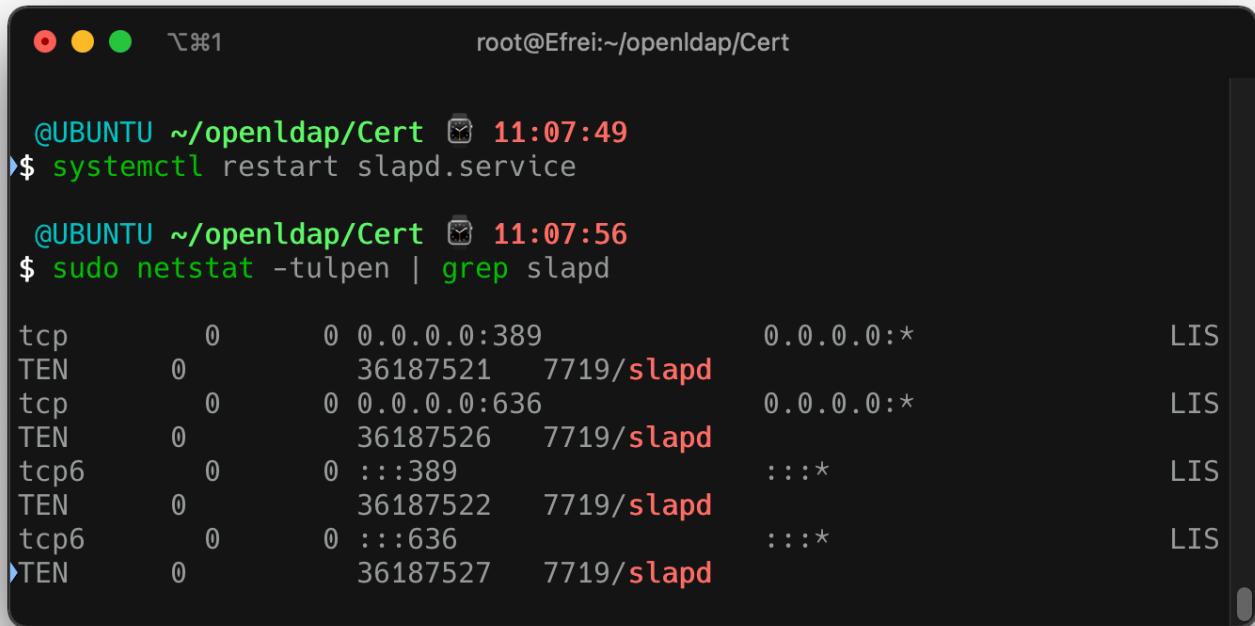
On applique ce fichier à l'aide de la commande suivante :

```
$ ldapmodify -QY EXTERNAL -H ldapi:/// -f cert.ldif
```

On modifie le fichier de configuration `/etc/default/slapd` pour ajouter le service `ldaps` en ajoutant à `ldaps://` à la suite de la ligne `SLAPD_SERVICES`.

Redémarrer le service et vérifier que le port `636` est bien sur écoute.

```
$ systemctl restart slapd.service
$ sudo netstat -tulpen | grep slapd
```



```
@UBUNTU ~/openldap/Cert 11:07:49
$ systemctl restart slapd.service

@UBUNTU ~/openldap/Cert 11:07:56
$ sudo netstat -tulpen | grep slapd

tcp      0      0 0.0.0.0:389          0.0.0.0:*          LIS
TEN      0      36187521  7719/slapd
tcp      0      0 0.0.0.0:636          0.0.0.0:*          LIS
TEN      0      36187526  7719/slapd
tcp6     0      0 :::389              ::::*             LIS
TEN      0      36187522  7719/slapd
tcp6     0      0 :::636              ::::*             LIS
TEN      0      36187527  7719/slapd
```

Création des utilisateurs (DIT Personnel)

Créer 3 fichiers correspondant aux informations des 3 utilisateurs, ayant respectivement chacun le contenu suivant :

`thomas.ldif`:

```
dn: uid=thomas.peugnet,ou=users,dc=Efrei,dc=fr
objectClass: person
objectClass: top
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
uidNumber: 6001
gidNumber: 6001
homeDirectory: /home/thomas
loginShell: /bin/bash
uid: thomas.peugnet
```

```
sn: peugnet
cn: thomas peugnet
mail: thomas.peugnet@efrei.fr
userPassword: thomas
```

tom.ldif:

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

alexis.ldif:

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

Nous les appliquons au serveur LDAP à l'aides des 3 commandes suivantes :

```
$ ldapadd -W -D "cn=admin,dc=Efrei,dc=fr" -x -f thomas.ldif
$ ldapadd -W -D "cn=admin,dc=Efrei,dc=fr" -x -f tom.ldif
$ ldapadd -W -D "cn=admin,dc=Efrei,dc=fr" -x -f alexis.ldif
```

```
● ● ●  ~@Efrei:~/openldap
@UBUNTU ~/openldap 12:20:54
$ ldapadd -W -D "cn=admin,dc=Efrei,dc=fr" -x -f thomas.ldif
Enter LDAP Password:
>adding new entry "uid=thomas.peugnet,ou=users,dc=Efrei,dc=fr"

@UBUNTU ~/openldap 12:21:04
$ ldapadd -W -D "cn=admin,dc=Efrei,dc=fr" -x -f tom.ldif
Enter LDAP Password:
>adding new entry "uid=tom.thioulouse,ou=users,dc=Efrei,dc=fr"

@UBUNTU ~/openldap 12:21:16
$ ldapadd -W -D "cn=admin,dc=Efrei,dc=fr" -x -f alexis.ldif
Enter LDAP Password:
>adding new entry "uid=alexis.plessias,ou=users,dc=Efrei,dc=fr"

@UBUNTU ~/openldap 12:21:31
$
```

Interface Graphique LDAP Account Manager

Installation

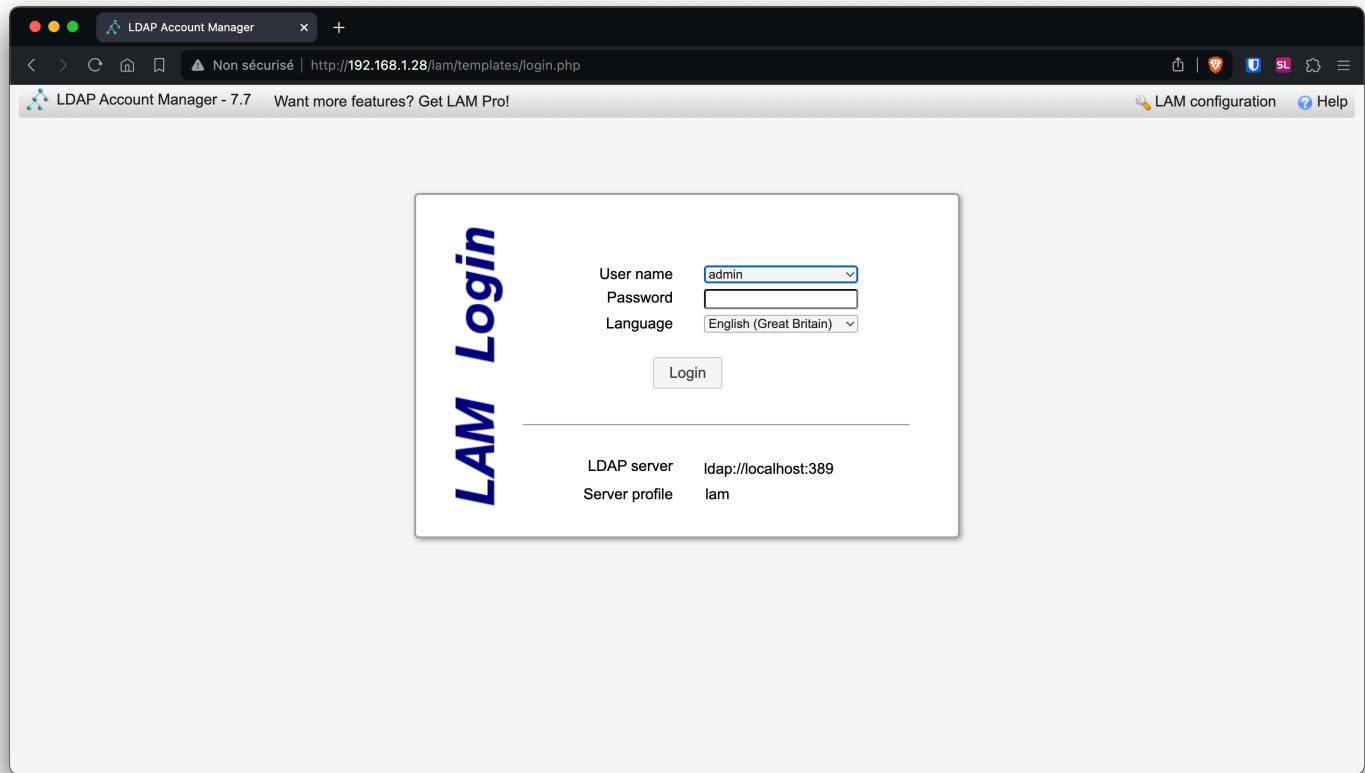
Utiliser la commande suivante pour installer toutes les dépendances et `ldap-account-manager` :

```
$ sudo apt install apache2 php php-cgi libapache2-mod-php php-mbstring php-common php-pear
ldap-account-manager -y

# Activer php-cgi
$ sudo a2enconf php8.1-cgi

# Restart apache2
$ systemctl restart apache2
```

Ensuite, se connecter sur `http://192.168.1.28/lam/templates/login.php`.



Puis, se rendre dans `LAM configuration`, utiliser le mot de passe `lam` et modifier les paramètres de domaine dans la page `General Settings` :

Enfin, modifier également les informations de domaine dans la partie `Account Types` :

LDAP Account Manager Config

Non sécurisé | http://192.168.1.28/lam/templates/config/conftypes.php

Printers	PyKota printers	
Samba domains	Samba 3 domain entries	
Users	User accounts (e.g. Unix, Samba and Kolab)	

Active account types

Users

User accounts (e.g. Unix, Samba and Kolab)

LDAP suffix: ou=users,dc=Efrei,dc=fr

List attributes: #uid;#givenName;#sn;#uidNumber;#gidNumber

Custom label:

Additional LDAP filter:

Hidden:

Groups

Group accounts (e.g. Unix and Samba)

LDAP suffix: ou=groups,dc=Efrei,dc=fr

List attributes: #cn;#gidNumber;#memberUID;#description

Custom label:

Additional LDAP filter:

Hidden:

Buttons: Save Cancel

Après avoir sauvegardé cette configuration, se reconnecter avec l'utilisateur `admin`

Nous pouvons constater le résultat suivant :

LDAP Account Manager (local)

Non sécurisé | http://192.168.1.28/lam/templates/lists/list.php?type=user

LDAP Account Manager - 7.7 (admin)

Tools Help Logout

Users **Groups**

New user Delete selected users File upload

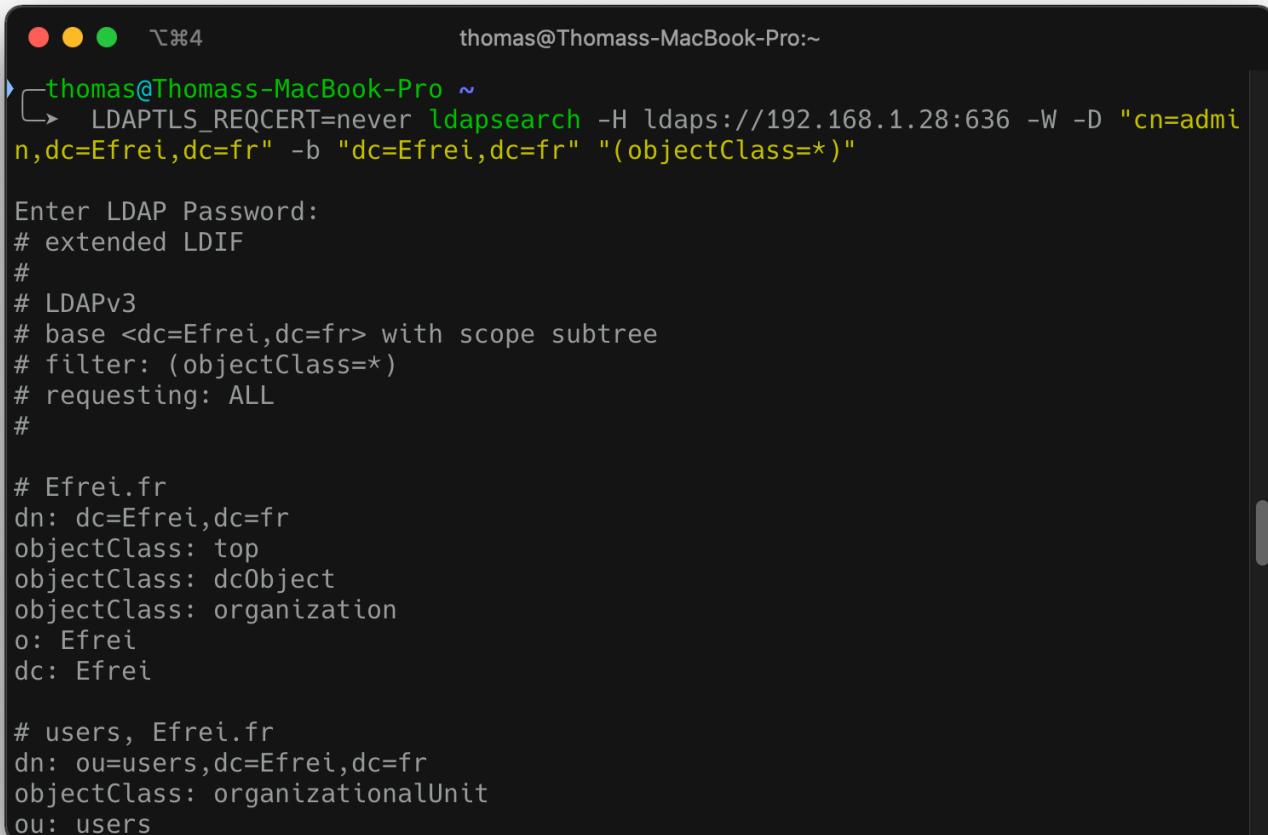
User count: 4

Actions	User name	First name	Last name	UID number	GID number
Sort sequence					
<input type="checkbox"/> Filter	<input type="text"/>				
<input type="checkbox"/>	alexis.plessias		plessias	6001	6001
<input type="checkbox"/>	souheib.yousfi		yousfi	6001	6001
<input type="checkbox"/>	thomas.peugnet		peugnet	6001	6001
<input type="checkbox"/>	tom.thioulouse		thioulouse	6001	6001

Connexion au serveur

Utiliser la commande suivante pour vérifier qu'il est bien possible de se connecter au serveur :

```
$ LDAPTLS_REQCERT=never ldapsearch -H ldaps://192.168.1.28:636 -W -D "cn=admin,dc=Efrei,dc=fr" -b "dc=Efrei,dc=fr" "(objectClass=*)"
```



A screenshot of a macOS terminal window titled 'thomas@Thomass-MacBook-Pro ~'. The window contains the command: 'LDAPTLS_REQCERT=never ldapsearch -H ldaps://192.168.1.28:636 -W -D "cn=admin,dc=Efrei,dc=fr" -b "dc=Efrei,dc=fr" "(objectClass=*)"' followed by the output of the search. The output shows the structure of the LDAP directory, including the root 'dc=Efrei,dc=fr' and a 'users' organizational unit.

```
thomas@Thomass-MacBook-Pro ~
LDAPTLS_REQCERT=never ldapsearch -H ldaps://192.168.1.28:636 -W -D "cn=admin,dc=Efrei,dc=fr" -b "dc=Efrei,dc=fr" "(objectClass=*)"

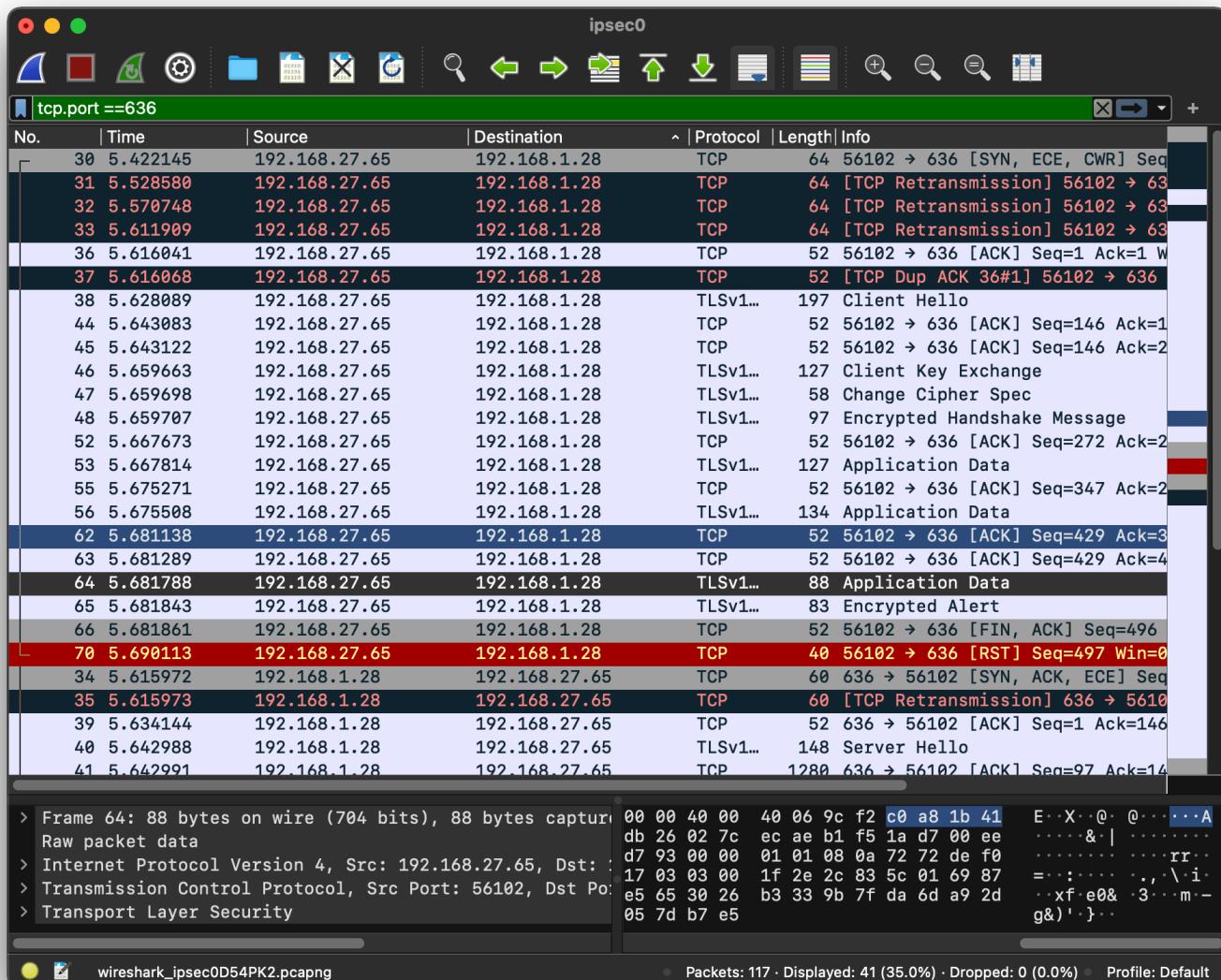
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <dc=Efrei,dc=fr> with scope subtree
# filter: (objectClass=*)
# requesting: ALL
#
# Ef frei.fr
dn: dc=Efrei,dc=fr
objectClass: top
objectClass: dcObject
objectClass: organization
o: Ef frei
dc: Ef frei

# users, Ef frei.fr
dn: ou=users,dc=Efrei,dc=fr
objectClass: organizationalUnit
ou: users
```

Il est nécessaire d'ignorer temporairement la vérification du certificat, d'où la variable `LDAPTLS_REQCERT=never`.

Wireshark

Après avoir lancé la capture Wireshark, et effectué une requête au serveur LDAP, on obtient le résultat suivant :



Etant donné que nous utilisons un protocole de chiffrement, il n'est pas étonnant de voir que nous ne pouvons pas déchiffrer directement dans Wireshark les informations du LDAP. Le traffic ne circule pas en clair sur le réseau.