

Table des matières :

Table des matières :.....	1
1.Installation :.....	2
2.Configuration de base du serveur.....	2
3.Injection des données	4
Remarque : remise à zéro de la configuration (ne pas le faire, juste à titre d'information)	7
4.Installation d'un client graphique.....	7
5.Configuration du serveur LDAP	11

Avant-Propos

Compétences :

- A1.1.1 Analyse du cahier des charges d'un service à produire
- A1.2.4 Déterminer des tests nécessaires à la validation d'un service (3)
- A4.1.9 Rédaction d'une documentation technique

```
iface eth0 inet static
    address 192.168.1.144
    netmask 255.255.255.0
    gateway 192.168.1.254
```

LDAP (Lightweight Directory Access Protocoles) le protocole d'annuaire sur TCP/IP.

Définition d'un annuaire :

Un annuaire est un référentiel partagé de personne et de ressources, dont la vocation est de localiser à l'aide de fonctions élaborées de navigation et de recherche, et d'offrir des mécanismes de sécurité pour protéger ces informations et y accéder.

Objectif :

Dans cette procédure, nous allons montrer comment installer et configurer un annuaire LDAP sous Debian.

OS	Distribution	Version
Debian	Linux	8.5

1. Installation :

Commencer par faire le TP sur putty

Téléchargement d'openldap :

```
root@LDAP:~# wget ftp://ftp.openldap.org/pub/OpenLDAP/openldap-release/openldap-2.4.44.tgz
```

On installe les librairies :

```
root@LDAP:~# apt-get install libtool libltdl-dev libssl-dev libdb5.3-dev libsasl2-dev make_
```

On extrait le paquet télécharger :

```
root@LDAP:~# tar xzvf openldap-2.4.44.tgz
```

Puis on installe le paquet :

```
root@LDAP:~# cd openldap-2.4.44/  
root@LDAP:~/openldap-2.4.44# ./configure --enable-crypt=yes --enable-Impasswd=yes  
s --enable-spaswd=yes --enable-modules=yes --enable-overlays=yes_
```

Ensuite, on fait la relation entre les fichiers :

```
root@LDAP:~/openldap-2.4.44# make depend_
```

```
root@LDAP:~/openldap-2.4.44# make_
```

```
root@LDAP:~/openldap-2.4.44# make install_
```

Le binaire slapd se trouve /usr/local/libexec et les outils repartis entre /usr/local/bin et /usr/local/sbin. Pour éviter de faire tourner le serveur autrement qu'avec root, on crée un utilisateur openldap sans shell.

```
root@LDAP:~# useradd -s /bin/false -d /usr/local/var/openldap-data openldap_
```

2. Configuration de base du serveur

On va ensuite configurer le fichier slapd.conf :

```
root@LDAP:~# nano /usr/local/etc/openldap/slapd.conf_
```

```
GNU nano 2.2.6 Fichier : /usr/local/etc/openldap/slapd.conf
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
# Define global ACLs to disable default read access.
# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#referral      ldap://root.openldap.org
include        /usr/local/etc/openldap/schema/core.schema
include        /usr/local/etc/openldap/schema/cosine.schema
include        /usr/local/etc/openldap/schema/inetorgperson.schema
include        /usr/local/etc/openldap/schema/openldap.schema
include        /usr/local/etc/openldap/schema/nis.schema
pidfile        /usr/local/var/run/slapd.pid
argsfile       /usr/local/var/run/slapd.args
```

```
# Directives needed to implement policy:
access to dn.base="" by * read
access to dn.base="cn=Subschema" by * read
access to *
    by self write
    by users read
    by anonymous auth
# if no access controls are present, the default policy
```

```
#####
# MDB database definitions
#####
database config
rootdn      "cn=manager,cn=config"
rootpw      password

database    bdb
maxsize     1073741824
suffix      "dc=rezo,dc=com"
rootdn      "cn=admin,dc=rezo,dc=com"
# Cleartext passwords, especially for the rootdn, should
# be avoid. See slapasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw      password
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory   /usr/local/var/openldap-data
# Indices to maintain
index objectClass eq
index uid eq
index cn,gn,mail eq,sub
index ou eq
index default eq,sub
```

On crée ensuite le fichier :

```
root@LDAP:~# mkdir /usr/local/etc/openldap/slapd.d
```

```
root@LDAP:~# cd /usr/local/etc/openldap/
```

```
root@LDAP:/usr/local/etc/openldap# slaptest -f slapd.conf -F slapd.d
57fb54f8 /usr/local/etc/openldap/schema/core.schema: line 78 attributetype: Duplicate attributeType: "2.5.4.2"
slaptest: bad configuration directory!
```

Ignorer la plainte de la commande slaptest

```
root@LDAP:/usr/local/etc/openldap# chown -R openldap.openldap /usr/local/etc/openldap/
```

On crée ensuite le fichier /usr/local/var/openldap-data/DB_CONFIG que slapd va utiliser pour gérer les bases de type BerkeleyDB. UN exemple est fourni.

```
root@LDAP:/usr/local/etc/openldap# mkdir /usr/local/var/openldap-data/DB_CONFIG
```

```
root@LDAP:/usr/local/etc/openldap# mv /usr/local/var/openldap-data/DB_CONFIG.example /usr/local/var/openldap-data/DB_CONFIG
```

```
root@LDAP:/usr/local/etc/openldap# chown -R openldap.openldap /usr/local/var/openldap-data/
```

```
root@LDAP:/usr/local/etc/openldap# /usr/local/libexec/slapd -u openldap -g openldap -h 'ldap:///'
```

Les options `-u` et `-g` indiquent sous quel utilisateur et groupe le serveur doit tourner et l'option `-h` indique le type de connexion supportée (ici connexion simple). Pour passer en mode debug et interdire au serveur de se mettre en arrière-plan :

```
root@LDAP:/usr/local/etc/openldap# /usr/local/libexec/slapd -d 3
```

La commande rend inutilisable putty, on doit donc passer sur la vm

```
root@LDAP:~# slapcat -s cn=config | less_
```

```
root@LDAP:~# ldapsearch -b cn=config -D "cn=manager,cn=config" -w password_
```

3. Injection des données

On crée ensuite le fichier init.ldif Les espaces sont importants !!

```
root@LDAP:~# nano init.ldif_
```

```
GNU nano 2.2.6      Fichier : init.ldif
dn:      dc=rezo,dc=com
objectclass:  dcObject
objectclass:  organization
o:      Linux
dc:      rezo

dn:      cn=admin,dc=rezo,dc=com
objectclass:  organizationalRole
cn:      admin
_
```

```
root@LDAP:~# ldapadd -x -D"cn=admin,dc=rezo,dc=com" -w password -f init.ldif
adding new entry "dc=rezo,dc=com"

adding new entry "cn=admin,dc=rezo,dc=com"
```

Les deux champs devraient s'insérer. Pour valider :

```
root@LDAP:~# ldapsearch -LLL -x -D "cn=admin,dc=rezo,dc=com" -w password -b 'dc=
rezo,dc=com' '(objectclass=*)'
dn: dc=rezo,dc=com
objectClass: dcObject
objectClass: organization
o: Linux
dc: rezo

dn: cn=admin,dc=rezo,dc=com
objectClass: organizationalRole
cn: admin
```

Même démarche pour les OU de base qui servent à créer les utilisateurs et les groupes (OU utilisateur : peopeople, OU groupes : groups) Le fichier s'appelle ou.ldif.

[OpenLDAP]

```
GNU nano 2.2.6 Fichier : ou.ldif
dn:      ou=people,dc=rezo,dc=com
objectclass:  organizationalUnit
ou:        people

dn:      ou=groups,dc=rezo,dc=com
objectclass:  organizationalUnit
ou:        groups
_
```

```
root@LDAP:~# ldapadd -x -D "cn=admin,dc=rezo,dc=com" -w password -f ou.ldif
adding new entry "ou=people,dc=rezo,dc=com"

adding new entry "ou=groups,dc=rezo,dc=com"
```

Pour créer un utilisateur sfonfec, le fichier users.ldif sera :

```
GNU nano 2.2.6 Fichier : users.ldif
dn:      cn=sfonfec,ou=people,dc=rezo,dc=com
objectclass:  top
objectclass:  account
objectclass:  posixAccount
objectclass:  shadowAccount
uid:        sfonfec
uidnumber:   1500
gidnumber:   10000
userpassword: password
gecos:      Sophie Fonfec
loginshell:  /bin/bash
homedirectory:  /home/sfonfec
shadowwarning:  7
shadowmin:    8
shadowmax:    9999
shadowlastchange:  10877
```

Les champs shadow sont définis par la FRC 2307.

Création du fichier groups.ldif

```
GNU nano 2.2.6 Fichier : groups.ldif
dn:      cn=ldap,ou=groups,dc=rezo,dc=com
objectclass:  top
objectclass:  posixGroup
cn:          ldap
gidNumber:    1000_
```

On insère ensuite les deux fichiers users.ldif et groups.ldif

```
root@LDAP:~# ldapadd -x -D "cn=admin,dc=rezo,dc=com" -w password -f users.ldif
adding new entry "cn=sfonfec,ou=people,dc=rezo,dc=com"
```

```
root@LDAP:~# ldapadd -x -D "cn=admin,dc=rezo,dc=com" -w password -f groups.ldif
adding new entry "cn=ldap,ou=groups,dc=rezo,dc=com"
```

```
root@LDAP:~# ldapsearch -x -D 'cn=sfonfec,ou=people,dc=rezo,dc=com' -w password
-b 'ou=people,dc=rezo,dc=com' '(cn=sfonfec)' loginshell
# extended LDIF
#
# LDAPv3
# base <ou=people,dc=rezo,dc=com> with scope subtree
# filter: (cn=sfonfec)
# requesting: loginshell
#
# sfonfec, people, rezo.com
dn: cn=sfonfec,ou=people,dc=rezo,dc=com
loginShell: /bin/bash
# search result
search: 2
result: 0 Success
# numResponses: 2
# numEntries: 1
```

La commande permet de se connecter avec le compte de l'utilisateur sfonfec et récupérer correctement un paramètre de son compte.

Remarque : remise à zéro de la configuration (ne pas le faire, juste à titre d'information)

- Arrêter le serveur
- Supprimer la configuration de base # `rm -rf /usr/local/etc/openldap/slapd.d/*`
- Recrée la configuration au format LDIF et donner les droits
- Pour supprimer les données, purger la base bdb en sauvegardant le fichier DB_CONFIG
`rm -rf /usr/local/var/openldap-data/*`
- Et remettre le fichier DB_CONFIG à sa place et affecter le bon propriétaire.
- Redémarrer le serveur.

4. Installation d'un client graphique

phpLDAPadmin est une interface écrite en php qui permet de modifier facilement et via une interface conviviale un annuaire LDAP.

4.1. Installation :

Installer les paquets suivant :

Apache2, php5, phpldapadmin

```
root@LDAP:~# apt install apache2_
```

```
root@LDAP:~# apt install php5_
```

```
root@LDAP:~# apt install phpldapadmin
```

Après installation, on peut aller sur l'interface web :



L'application est déployée dans le répertoire `/usr/share/phpldapadmin`, et rendue visible sur le serveur Apache par la présence du lien `phpldapadmin`, dans le répertoire `/etc/apache2/conf.d`, pointant sur le fichier `/etc/phpldapadmin/apache.conf`

Pour des raisons des sécurités, les droits d'accès sont modifiés, ainsi que le propriétaire.

```
root@LDAP:~# chown -R www-data:www-data /etc/phpldapadmin
```

```
root@LDAP:~# chmod 640 /etc/phpldapadmin/config.php
```

```
root@LDAP:~# chown -R www-data:www-data /usr/share/phpldapadmin
```

4.2. Configuration :

La configuration de `phpLDAPADMIN` nécessite la modification du fichier `config.php`, situé dans le répertoire `/etc/phpldapadmin`

La première modification apportée concerne le nom du serveur LDAP qui sera affiché sur l'interface. Le nom affiché par défaut est `My LDAP server`. La modification consiste en la modification de la section suivante :

```
root@LDAP:/etc/phpldapadmin# nano config.php _
```

```
/* A convenient name that will appear in the tree viewer and throughout  
   phpLDAPAdmin to identify this LDAP server to users. */  
$servers->setValue('server', 'name', 'Mon serveur LDAP');
```

La second modification concerne la base de recherche, valeur souhaitée `dc=rezo,dc=com`, dans l'annuaire. Il faut modifier la section suivante :

```
/* Array of base DN's of your LDAP server. Leave this blank to have phpLDAPAdmin  
   auto-detect it for you. */  
$servers->setValue('server', 'base', array('dc=rezo,dc=com'));
```

La troisième modification concerne le compte d'authentification par défaut est `cn=admin,dc=example,dc=com`. Il parait utile de modifier cette valeur pour être le « vrai » compte administrateur de l'annuaire accédé.

```
$servers->setValue('login', 'bind_id', 'cn=admin,dc=rezo,dc=com');  
# _$servers->setValue('login', 'bind_id', 'cn=Manager,dc=example,dc=com');
```

On peut vérifier le bon fonctionnement en vous connectant sur la page d'accueil.

DN de connexion:
cn=admin,dc=rezo,dc=com

Mot de passe:
.....

Connexion anonyme

S'authentifier

mdp : password

Ajouter un nouvel utilisateur dans l'OU people.

Mon serveur LDAP

schéma rechercher rafraîchir info importer exporter se déconnecter

Connecté en tant que :: cn=admin

dc=rezo,dc=com (3)

- cn=admin
- ou=groups (1)
- ou=people (1)
- cn=sfonfec

Créer une nouvelle entrée ici

Créer une nouvelle entrée ici

Créer un objet

Serveur: Mon serveur LDAP Conteneur: ou=people,dc=rezo,dc=com

Sélectionner un modèle pour le processus de création

Modèles:

- E-Mail : Compte
- E-Mail : Alias
- Générique : Entrée Carnet d'Adresse
- Générique : Entrée DNS
- Générique : LDAP Alias
- Générique : Rôle Organisationnel
- Générique : Unité Organisationnelle
- Générique : Groupe Posix
- Generic: Simple Security Object
- Générique : Compte Utilisateur
- Samba: Account
- Samba: Domain
- Samba: Group Mapping
- Samba: Machine
- Sendmail: Alias
- Sendmail: Cluster
- Sendmail: Domain
- Sendmail: Relays
- Sendmail: Virtual Domain
- Sendmail: Virtual Users
- Thunderbird: Address Book Entry
- Valeur par défaut

Créer un objet

Serveur: **Mon serveur LDAP** Conteneur: **ou=people,dc=rezo,dc=com**
Modèle: **Generic: User Account (posixAccount)**

Nouveau compte utilisateur (Étape 1 sur 1)

Nom Commun

alias, requis, rdn

*

Prénom

alias



GID

alias, requis, astuce

*

Répertoire personnel

alias, requis

*

Nom de famille

alias, requis

*

Login shell

alias

Mot de passe

alias, astuce



md5

(confirmer)

[Vérifier le mot de passe...](#)

UID

alias, requis, astuce, ro



ID utilisateur

alias, requis

*

On doit maintenant vérifier la présence de l'utilisateur à l'aide de la commande `ldapsearch`.

```
root@LDAP:/etc/php/ldapadmin# ldapsearch -LLL -x -D "cn=admin,dc=rezo,dc=com" -w
password -b 'dc=rezo,dc=com' '(objectclass=*)'_
```

```
dn: cn=arthur bigorno,ou=people,dc=rezo,dc=com
cn: arthur bigorno
givenName: arthur
gidNumber: 1000
homeDirectory: /home/users/abigorno
sn: bigorno
loginShell: /bin/sh
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
userPassword:: e01ENX12Nm53Nm51NwdGQjVhM1N1aFVnWVJRPT0=
uidNumber: 1000
uid: abigorno
```

5. Configuration du serveur LDAP

```
root@LDAP:~# apt install tree_
```

Cela permettra de faire une arborescence.

```
root@LDAP:~# tree /usr/local/etc/openldap/slapd.d
/usr/local/etc/openldap/slapd.d
├── cn=config
│   ├── cn=schema
│   │   ├── cn={0}core.ldif
│   │   ├── cn={1}cosine.ldif
│   │   ├── cn={2}inetorgperson.ldif
│   │   ├── cn={3}openldap.ldif
│   │   └── cn={4}nis.ldif
│   ├── cn=schema.ldif
│   ├── olcDatabase={0}config.ldif
│   ├── olcDatabase={1}bdb.ldif
│   └── olcDatabase={-1}frontend.ldif
└── cn=config.ldif

2 directories, 10 files
```