US-RS7G
Sécurité des réseaux
Le Rebours Paris XIII

Découverte & Compréhension de l'annuaire OpenLDAP sous Debian
Durée : **2 heures**
TP du **20 octobre 2025**

Introduction

OpenLDAP est un outil puissant pour la gestion d'annuaires et d'informations. Il s'agit d'un système d'annuaire libre et open-source basé sur le protocole X.500 LDAP (Lightweight Directory Access Protocol). Il est utilisé pour développer un service d'annuaire centralisé afin de stocker des informations pertinentes sur les utilisateurs, les groupes, les applications et d'autres ressources. Dans ce TP, nous allons explorer comment installer, configurer et utiliser OpenLDAP sur Debian. Ce TP sera également l'occasion de découvrir deux logiciels couramment utilisés à savoir Apache Directory Studio et FusionDirectory.

Objectifs

- Installer et configurer OpenLDAP
- Créer une structure de base pour l'organisation 'lerebours' ayant pour racine 'lerebours.fr'
- Ajouter les branches 'people' et 'dsa'
- Créer des comptes dans chaque branche
- Modifier le mot de passe des comptes
- Supprimer des comptes
- Modifier les attributs des comptes
- Exporter et restaurer les données de l'annuaire
- Découvrir l'interface d'administration LDAP Apache Directory Studio[1]
- Découvrir le logiciel de gestion des identités FusionDirectory[2]

→ Merci de lire le TP *en entier* au moins une fois avant de commencer ! De plus, il faut *absolument éviter* de copier-coller du texte ou des commandes depuis le sujet vers un terminal.

1. https://directory.apache.org/studio/
2. https://www.fusiondirectory.org/

1. [5 points] Installation et configuration initiale du serveur LDAP
   (a) Mettez à jour votre système `Debian` :

```
sudo apt update && sudo apt upgrade
```

   (b) Installez les paquets nécessaires :

```
sudo apt install slapd ldap-utils terminator net-tools
```

   (c) Lors de l'installation, il faut définir le mot de passe administrateur pour le serveur LDAP. Pour ce TP, nous utiliserons 'admin'.
   (d) Configurez votre serveur LDAP :

```
sudo dpkg-reconfigure slapd
```

   Suivez les instructions et définissez le *nom de domaine* (la racine) de votre serveur LDAP et l'*organisation*. Pour ce TP, nous utiliserons les informations suivantes : 'lerebours.fr' et 'lerebours'. Faut-il déplacer et purger la BDD ? → *OUI*.
   (e) Vérifiez que votre serveur LDAP soit bien installé, démarré et qu'il fonctionne correctement avec les commandes suivantes :

```
sudo systemctl status slapd
sudo netstat -ntlp | grep 389
sudo slapcat
```

2. [10 points] Création des branches et des comptes
   (a) Créez un répertoire 'ldif' et déplacez-vous à l'intérieur :

```
cd && sudo mkdir ldif && cd ldif
```

   (b) Créez un fichier 'base.ldif' pour définir les branches 'people' et 'dsa' :

```
### /!\ La syntaxe doit être très rigoureuse /!\ ###
dn: ou=people,dc=lerebours,dc=fr            # dn: ou=students,ou=people,dc=lerebours,dc=fr
objectClass: top                            # objectClass: top
objectClass: organizationalUnit             # objectClass: organizationalUnit
ou: people                                  # ou: students
description: Branche des personnes          # description: Sous-branche OPTIONNELLE

dn: ou=dsa,dc=lerebours,dc=fr
objectClass: top
objectClass: organizationalUnit
ou: dsa
description: Branche des comptes de service d'annuaire (DSA)
```

   DIT de l'annuaire 'lerebours' pour ce TP :

```
                dc=fr
                  |
                  |
              dc=lerebours  <-- Organization (lerebours)
             /        \
            /          \
        ou=people     ou=dsa
```

   (c) Importez la structure de base précédente dans votre serveur LDAP en utilisant le compte 'admin' et le mot de passe correspondant :

```
ldapadd -x -D cn=admin,dc=lerebours,dc=fr -W -f base.ldif
```

   (d) Comptez le nombre de branches créées dans votre annuaire (si OK → *2*) :

```
ldapsearch -x -LLL -b dc=lerebours,dc=fr -D cn=admin,dc=lerebours,dc=fr -W | egrep '^ou' |
    ↪ wc -l
```

(e) Créez un fichier ‘comptes.ldif‘ pour définir six comptes - trois dans la branche ’people’ et trois dans la branche ’dsa’ :

```
# Entrées pour les comptes dans la branche "people"
dn: uid=foo.bar,ou=people,dc=lerebours,dc=fr
objectClass: top
objectClass: account
objectClass: posixAccount
uid: foo.bar
#cn: Foo Bar
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/foo
userPassword: password

dn: uid=alice.wonderland,ou=people,dc=lerebours,dc=fr
objectClass: top
objectClass: person
objectClass: posixAccount
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: alice.wonderland
cn: Alice Wonderland
mail: alice.wonderland@lerebours.fr
sn: Wonderland
givenName: Alice
uidNumber: 1001
gidNumber: 1001
homeDirectory: /home/alice
userPassword: password123

dn: uid=john.doe,ou=people,dc=lerebours,dc=fr
objectClass: top
objectClass: person
objectClass: posixAccount
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: john.doe
cn: John Doe
mail: john.doe@lerebours.fr
sn: Doe
givenName: John
uidNumber: 1002
gidNumber: 1002
homeDirectory: /home/john
userPassword: password123

# Entrées pour les comptes dans la branche "dsa"
### Utilisez ’slappasswd’ pour hacher & saler LES MdP des comptes applicatifs ###
dn: uid=service-desk,ou=dsa,dc=lerebours,dc=fr
objectClass: top
objectClass: account
objectClass: simpleSecurityObject
uid: service-desk
description: Compte utilisé par Service-Desk
userPassword: # Remplacer par le {SSHA} de ’servicedesk’

dn: uid=lemonldap,ou=dsa,dc=lerebours,dc=fr
objectClass: top
objectClass: account
objectClass: simpleSecurityObject
uid: lemonldap
description: Compte utilisé par LemonLDAP::NG
userPassword: # Remplacer par le {SSHA} de ’lemonldap’

dn: uid=syncrepl,ou=dsa,dc=lerebours,dc=fr
objectClass: top
objectClass: account
objectClass: simpleSecurityObject
uid: syncrepl
description: Compte utilisé pour la réplication
userPassword: # Remplacer par le {SSHA} de ’secret’
```

Astuce : Vous pouvez utiliser la commande suivante pour générer le SSHA (salted SHA1) et rediriger la sortie de ‘slappasswd‘ à la fin de votre fichier ‘comptes.ldif‘ :

```
# Commande à exécuter 3 fois !
slappasswd >> comptes.ldif
# puis
vi comptes.ldif # Demandez à votre enseignant si besoin ;-)
```

(f) Importez les comptes dans votre serveur LDAP :

```
# ‘-c‘ permet de continuer meme en cas d'erreur
ldapadd -x -D cn=admin,dc=lerebours,dc=fr -W -c -f comptes.ldif
```

(g) Expliquez et *justifiez* l'erreur levée par `OpenLDAP` avec la documentation officielle. Corrigez la et exécutez à nouveau la commande.

(h) Comptez le nombre de comptes créés dans votre annuaire (si OK → *6*) :

```
ldapsearch -x -LLL -b dc=lerebours,dc=fr -D cn=admin,dc=lerebours,dc=fr -W uid|egrep '^uid'
    ↪ |wc -l
```

3. [5 points] Stockage des informations des comptes

(a) Affichez le DIT de votre annuaire :

```
sudo slapcat | less
```

(b) La description des comptes 'lemonldap' et 'syncrepl' a été encodée en *base64* par `OpenLDAP` à cause des caractères spéciaux. Décodez les à l'aide d'une commande `Linux`.

(c) Calculez l'empreinte `sha1` de 'secret' à l'aide d'une commande `Linux`.

(d) Expliquez le principe du « salage » mis en œuvre par `OpenLDAP` et son utilité pour le stockage des mots de passe dans l'annuaire.

(e) Expliquez le principe du « poivrage ».

4. [3 points] Modification du mot de passe d'un compte

(a) Créez un fichier ‘modify-pwd.ldif‘ :

```
dn: uid=john.doe,ou=people,dc=lerebours,dc=fr
changetype: modify
replace: userPassword
userPassword: NewPasswd456
```

(b) Modifiez le mot de passe et testez la connexion (bind) avec le nouveau MdP :

```
ldapmodify -x -D cn=admin,dc=lerebours,dc=fr -W -f modify-pwd.ldif
ldapwhoami -D 'uid=john.doe,ou=people,dc=lerebours,dc=fr' -W
```

5. [3 points] Suppression d'un compte

(a) Créez un fichier ‘del-user.ldif‘ :

```
dn: uid=foo.bar,ou=people,dc=lerebours,dc=fr
changetype: delete
```

(b) Supprimez le compte :

```
ldapmodify -x -D cn=admin,dc=lerebours,dc=fr -W -f del-user.ldif
```

6. [3 points] Modification des attributs d'un compte

(a) Supposons que nous voulons changer le nom complet (‘cn‘) de l'utilisateur *John Doe* à *Jonathan Doe*. Créez un fichier ‘modify-att.ldif‘ :

```
dn: uid=john.doe,ou=people,dc=lerebours,dc=fr
changetype: modify
replace: cn
cn: Jonathan Doe
```

(b) Utilisez 'ldapmodify' pour modifier l'attribut :

```
ldapmodify -x -D cn=admin,dc=lerebours,dc=fr -W -f modify-att.ldif
```

(c) Installez et utilisez 'ldapvi' pour modifier les descriptions (un utilitaire *indispensable*!!!) :

```
sudo apt install ldapvi
ldapvi -h 127.0.0.1 -D cn=admin,dc=lerebours,dc=fr -b ou=people,dc=lerebours,dc=fr # Choix
    ↪ '2' pour définir 'vi' comme éditeur par défaut
```

7. [2 points] Vérifications

(a) Utilisez 'ldapsearch' pour rechercher des comptes dans votre annuaire et vérifiez les modifications effectuées précédemment :

```
ldapsearch -x -b dc=lerebours,dc=fr -D cn=admin,dc=lerebours,dc=fr -W
ldapsearch -x -LLL -b ou=people,dc=lerebours,dc=fr -D cn=admin,dc=lerebours,dc=fr -W mail=*
    ↪ lerebours.fr uid + # le symbole '+' permet d'afficher les attributs techniques
```

(b) Utilisez 'slapcat' pour exporter toute la structure et les données de votre annuaire :

```
sudo slapcat > /tmp/myldap.ldif
```

8. [5 points] Insertion des schémas **EduPerson & SupAnn**.

Pour pouvoir insérer les schémas **EduPerson & SupAnn** dans l'annuaire, nous allons utiliser l'outil **Debian schema2ldif** afin de les convertir au format LDIF.

(a) Téléchargement & insertion des schémas **EduPerson & SupAnn** :

```
# Installation de l'utilitaire de conversion
sudo -s
apt install schema2ldif

# Téléchargement des schémas
cd /tmp
wget https://files.marwan.ma/eduPerson.schema
wget https://services.renater.fr/_export/code/documentation/supann/supann2021/
    ↪ recommandations/tables_references/schematechnique_openldap?codeblock=0 -O supAnn.
    ↪ schema

# Conversion des schémas en fichers .ldif afin de pouvoir les importer
schema2ldif /tmp/eduPerson.schema > eduperson.ldif
schema2ldif /tmp/supAnn.schema > supann.ldif

# Insertion des schémas
ldapadd -Y EXTERNAL -H ldapi:/// -f /tmp/eduperson.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /tmp/supann.ldif
```

(b) Recherchez les attributs **SupAnn** ajoutés au schéma de l'annuaire :

```
sudo ldapvi -Y EXTERNAL -h ldapi:/// -b cn=schema,cn=config
# /supann puis 'n'
```

(c) Quel est l'OID de l'attribut "identifiant cible de personne FranceConnect" ?

(d) Modifiez la configuration pour permettre l'accès à la branche 'cn=config' depuis l'extérieur de la VM :

```
sudo ldapvi -Y EXTERNAL -h ldapi:/// -b cn=config
# Allez à la fin de la config avec 'G'
# Ajoutez un MdP au compte cn=admin,cn=config ('olcRootPW') en copiant celui de 'admin'
    ↪ puis testez l'accès
sudo ldapvi -h ldap://127.0.0.1 -b cn=config -D cn=admin,cn=config
```

(e) Ajoutez des attributs **SupAnn** aux comptes 'alice.wonderland' et 'john.doe' à l'aide de la commnade 'ldapvi'.

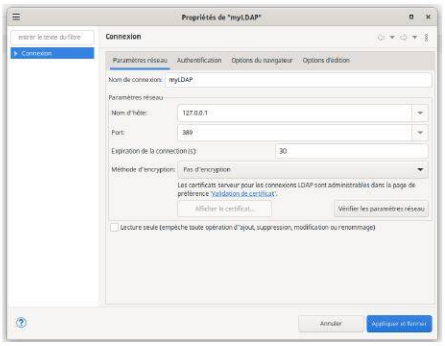
9. [5 points (bonus)] Administration ide l'annuaire avec `Apache Directory Studio` depuis une machine disposant d'une interface graphique (GUI)
   (a) Installez la machine `Java` et vérifiez sa version :

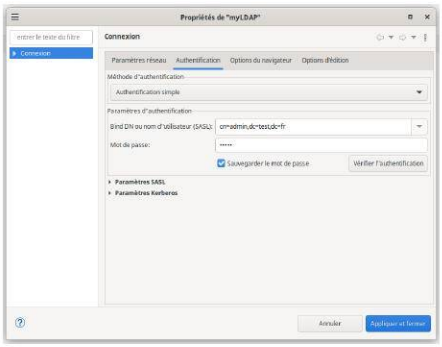
```
apt install default-jre
java -version
```

   (b) Téléchargez la dernière version d'ADS[3], décompressez l'archive et exécutez `Apache Directory Studio` :

```
cd /tmp # Vérifiez la version disponible
wget https://dlcdn.apache.org/directory/studio/2.0.0.v20210717-M17/ApacheDirectoryStudio
    ↪ -2.0.0.v20210717-M17-linux.gtk.x86_64.tar.gz
tar xvzf ApacheDirectoryStudio-2.0.0.v20210717-M17-linux.gtk.x86_64.tar.gz
cd ApacheDirectoryStudio && ./ApacheDirectoryStudio
```

   (c) Configurez `Apache Directory Studio` pour vous connecter à votre annuaire et visualiser l'ensemble du DIT.





   (d) Fournissez une capture d'écran de la structure de votre anuuaire.
   (e) Désinstallez et purgez votre annuaire. Supprimez dans votre fichier '/tmp/myldap.ldif' *tous les attributs techniques* créés par `OpenLDAP` (quels sont-ils ?) puis réinstallez l'annuaire et restaurez votre DIT :

```
apt purge slapd
vi /tmp/myldap.ldif # Supprimez les attributs techniques
ldapadd -x -D cn=admin,dc=lerebours,dc=fr -W -f /tmp/myldap.ldif
```

10. [4 points] Discussion
   (a) Pourquoi certains attributs sont suivis de ' : :' ?
   (b) Quelle est l'importance des identifiants uniques (uid) pour les comptes LDAP ?
   (c) Comment pourriez-vous améliorer la disponibilité de votre annuaire `OpenLDAP` ?
   (d) Comment pourriez-vous sécuriser davantage votre annuaire `OpenLDAP` ?

Conclusion

Vous avez maintenant une compréhension de base du fonctionnement d'`OpenLDAP` sous `Debian`, de la création de la structure de base et de l'ajout de comptes. Vous savez comment gérer les comptes, notamment comment ajouter, modifier le mot de passe, supprimer des comptes et changer leurs attributs. Ces compétences sont essentielles pour administrer efficacement un annuaire LDAP. Il y a encore beaucoup à apprendre sur `OpenLDAP`, y compris la sécurisation (LDAPS), l'optimisation (réplication) et la gestion des schémas (OIDs) ou des droits (ACLs).

3. `https://directory.apache.org/studio/download/download-linux.html`

Question:	1	2	3	4	5	6	7	8	9	10	Total
Points:	5	10	5	3	3	3	2	5	0	4	40
Score:											