1. **Installation et configuration Openldap :**
2. Les packages à installer :

* openldap
* openldap-servers
* openldap-clients
* openldap-devel

1. le fichier de configuration d’un serveur openldap :

/etc/openldap/slapd.conf

1. **Configuration d’un serveur ldap :**
2. Modification du fichier slapd.conf :

Une fois les packages sont installés, vous commencez par la modification du fichier de configuration qui se trouve :

# **vi /etc/openldap/slapd.conf**

* définir la base de données et son type : database bdb
* définir le nom du domaine : suffix ‘’dc=exemple, dc=ma’’
* définir le mot de passe de l’administrateur : rootdn ‘’cn=admin,dc=exemple,dc=ma’’
* définir le mot de passe de la BD d’annuaire : rootpw secret

Dans ce que il suffit de taper la commande suivante pour obtenir le mot de passe encrypté, dans ce cas il s’agit de password mais vous pouvez choisir un autre :

**# slappasswd –s password –h {MD5}**

Puis coller le mot de passe généré dans le fichier de configuration.

Pour tester la syntaxe du fichier slapd.conf, vous tapez la commande suivante :

**# slaptest**

Et maintenant vous pouvez redémarrer le service ldap :

**# service ldap restart**

1. Insertion des enregistrements dans la base de données d’annuaire :
2. Définition de l’organisation

Dans un premier lieu, on commence par la création de l’organisation dans notre cas est : **exemple.ma** donc : dc=exemple,dc=ma

On nomme le fichier par exemple : **entree1.ldif :**

**# vi entree1.ldif**

Le contenu du fichier entree1.ldif

dn : dc=exemple,dc=ma

objectClass : dcobject

objectClass : organization

dc : exemple

o: exemple

La commande afin d’ajouter l’entrée créée précédemment :

**# ldapadd –x -D ‘’cn=admin,dc=exemple,dc=ma’’ –W –f entree1.ldif**

L’option :

-x : pour ne spécifier que le mot de passe

-D : indique le DN de l’administrateur de l’annuaire

-w : le mot de passe sera demandé

-f : le nom du fichier .ldif à insérer

1. Définition des unités d’organisation comptes et groupes :

Dans un premier temps, vous créez un nouveau fichier dont le nom par exemple : **entree2.ldif** et sera rempli comme suit :

dn: ou=comptes, dc=exemple,dc=ma

objectClass : organizationalUnit

ou : comptes

dn : ou=groupes, dc=exemple,dc=ma

objectClass : organizationalUnit

ou : groupes

1. Définition d’un utilisateur possédant un compte :

De la même manière, vous créez un fichier, vous le nommez par exemple **entree3.ldif** dont le contenu est le suivant :

dn : uid=user1,ou=comptes,dc=exemple,dc=ma

objectClass: account

objectClass : posixAccount

cn : user1

uid: user1

uidNumber: 1000

gidNumber: 1000

homeDirectory: /home/user1

loginShell: /sbin/bash

userPassword: P@ssword

1. Définition du groupe principal de l’utilisateur user1:

Pour définir un groupe à l’utilisateur user1, vous procédez de la même manière, vous créez un fichier dont le nom **entree4.ldif** cette fois puis vous saisissez les lignes suivantes :

dn : cn=user1,ou=groupes,dc=exemple,dc=ma

objectClass : posixGroup

gidNumber : 1000

1. Afficher le contenu de l’annuaire :

**# ldapsearch –x –b ‘’dc=exemple,dc=ma’’**

1. N’afficher que les données du compte user1 :

**# ldapsearch –x –b dc=exemple,dc=ma uid=user1**

1. Supprimer le compte user1 :

**# ldapdelete –x –D ‘’cn=admin,dc=exemple,dc=ma’’ –W uid=user1,ou=compte,dc=exemple,dc=ma**

1. Ajouter un attribut à en enregistrement :

Pour ajouter un attribut, il suffit de créer un fichier :

**# vi modify.ldif**

Dont le contenu est :

dn : uid=user1,ou=comptes,dc=exemple,dc=ma

add : userPasswd

userPasswd : Password

Puis vous tapez la commande suivante :

# ldapmodify –x –D ‘’cn=admin,dc=exemple,dc=ma’’ –W –f modify.ldif

1. Modifier un attribut :

De la même manière, vous créez un fichier dont le nom est par exemple modify2.ldif

Dont le contenu est :

dn : uid=user1,ou=comptes,dc=exemple,dc=ma

changetype : modify

replace : userPasswd

userPasswd : user1

Finalement vous tapez la commande suivante :

# ldapmodify –x –D ‘’cn=admin,dc=exemple,dc=ma’’ –W -f modify2.ldif

Résumé : le DIT réalisé

dc=exemple,dc=ma

ou=comptes ou=groupes

cn=user1

1. **Configuration d’un poste client ldap:**

On souhaite ouvrir une session utilisateur en s’authentifiant sur le serveur ldap

Premièrement, Vérifiez que le package nss\_ldap est installé : **# rpm –q nss\_ldap**

1. Après vous passez à la modification du fichier /etc/ldap.conf, ce dernier permet de définir le serveur ldap : **# vi /etc/ldap.conf**

Ajoutez les lignes suivantes :

Base dc=exemple,dc=ma

Host 192.168.0.1

1. Le fichier /etc/nsswitch.conf permet de préciser quelles sont les sources d’information utlisées pour s’authentifier, modifier les lignes suivantes **: # vi /etc/nsswitch.conf**

Modifiez les lignes suivantes :

passwd : files ldap

shadow : files ldap

group : files ldap

1. Le fichier /etc/pam.d/system-auth permet de gérer l’authentification au niveau de l’ouverture de session, du mot de passe : **# vi /etc/pam.d/system-auth**

Ajoutez les lignes suivantes :

* **Auth sufficient pam\_ldap.so user\_first\_pass**

Authentifie l’utilisateur sur une base ldap par une demande de mot de passe

* **Account [default=bad success=ok user\_unkhnow=ignore] pam\_ldap.so**

L’accès de l’utilisateur aux ressources sur des critères: Expiration du compte, heure de restriction

* **Password sufficient pam\_ldap.so use\_authtok**

Gérer la modification de mot de passé

* **Session optional pam\_ldap.so**

Gérer l’ouverture et la fermeture de sessuion

1. Test :

* Vérifier la possibilité de se connecter à l’annuaire ldap : **# getent passwd**
* Ouvrir une session avec l’utilisateur : user1 **: # su – user1**
* créer un répertoire personnel pour l’utilisateur user1 :

**# mkdir /home/user1**

**# chown –R user1 :user1 /home/user1**

**# cp –R /etc/skel /home/user1**