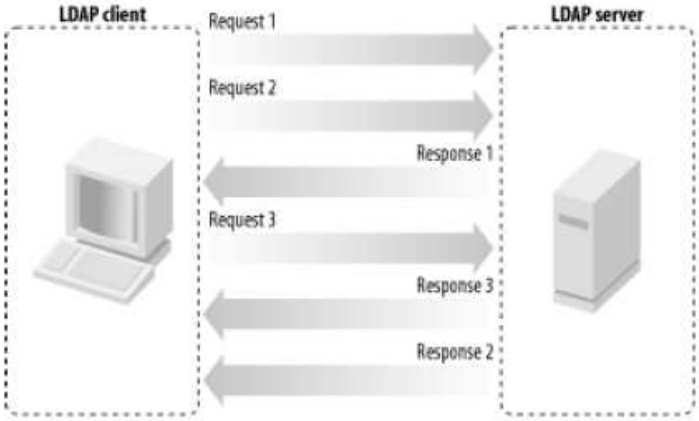
Índex de continguts

1 Què és el servei de directori?

Un **directori** és una base de dades altament optimitzada per realitzar operacions de lectura. Les operacions d'escriptura, en canvi, no són tan ràpides degut a que es realitzen amb molt poca freqüència. Un **servei de directori** és un procés que atén les peticions que fan els clients sobre el directori (lectura, escriptura...). Un exemple de servei de directori molt utilitzat és el DNS (Domain Name System), el qual emmagatzema adreces que s'organitzen de forma jeràrquica.

A continuació tractarem amb un tipus particular de servei de directori: aquells que utilitzen el **protocol LDAP** (*Lightweight Directory Access Protocol*) per comunicar-se amb els clients.

LDAP és un protocol de xarxa basat en el model client-servidor. El client genera peticions i el servidor les respòn de manera asíncrona.



El servei LDAP és un procés que s'executa en un servidor i respon a les peticions del client fent ús d'una base de dades que conté informació sobre el DIT. Aquesta BD pot estar en qualsevol format (fitxer de text, BD relacional, BD transaccional, etcètera), característica que és totalment transparent a l'usuari.

Una de les múltiples implementacions del servei LDAP per a Linux és l'**OpenLDAP**. La implementació de LDAP més utilitzada en Windows, i que ja coneixeu, és el servei

d'Active Directory.

2 Directori LDAP

Com s'organitza la informació dins d'un directori LDAP?

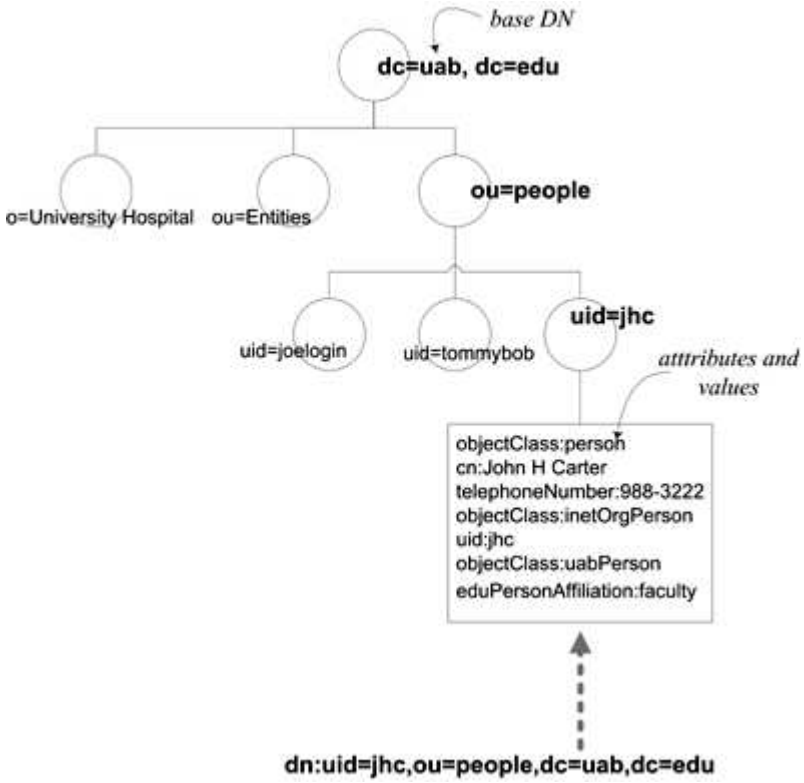
Les entrades del directori s'organitzen de forma jeràrquica o d'arbre. Tradicionalment, aquesta estructura reflexa limits geogràfics i/o organitzatius i es coneix com **DIT** (*Directory Information Tree*).

Quin tipus de dades hi ha dins d'un directori LDAP?

Tot i que es tendeix a pensar que la informació que hi ha en un directori és exclusivament relativa al domini d'una xarxa: usuaris, grups, hosts, etcètera, en realitat es pot utilitzar per emmagatzemar qualsevol tipus de dades.

Cada node contingut dins de l'arbre LDAP s'anomena **entrada**. Són exemples d'entrada un usuari, una unitat organitzativa, un grup, etcètera. Cada entrada conté una col·lecció d'**atributs** i **valors** (nom, cognoms, email de contacte...). Hi ha atributs opcionals i atributs obligatoris. El tipus d'entrada, així com els atributs que són opcionals i obligatoris estan definits en els **esquemes**.

Cada entrada es distingeix amb un nom únic conegut com a *Distinguished Name* (DN). En un directori mai hi haurà dues entrades amb el mateix DN.



Il·lustració 1: Exemple d'entrades en un directori

Com es construeix el DN?

Totes les entrades es referencien pel seu DN, que es construeix concatenant el nom de l'entrada (també anomenat *Relative Distinguished Name*) amb el RDN de tots els seus ancestres separats per comes.

La Il·lustració 1 mostra que el DN de l'entrada assenyalada és `uid=jhc,ou=people,dc=uab,dc=edu`. El RDN de l'entrada és `uid=jhc`. Observeu que fent la lectura del DN al revés podem determinar el camí a l'objecte partint del node arrel. Penseu que és similar a la ruta absoluta que té un fitxer dins de l'estructura de directoris.

Quin aspecte té una entrada en LDAP?

Les entrades contingudes en LDAP es presenten amb un format especial: el LDIF. A continuació es mostra un exemple:

```
dn: cn=pepe,ou=comptabilitat,dc=empresa,dc=com
cn: pepe
objectclass: person
sn: pérez
```

En aquest cas l'entrada conté informació d'una persona (`objectclass: person`). El nom de la persona (`cn`) és pepe i el cognom (`sn`) és pérez. Aquesta persona es pot trobar dins

del domini empresa.com dins de la unitat organitzativa comptabilitat (`dn: cn=pepe,ou=comptabilitat,dc=empresa,dc=com`).

En quines situacions s'utilitza LDAP?

En general, quan es necessita que les dades estigui centralitzades i accesibles a través de mètodes estàndards. Alguns exemples de situacions on es pot fer ús de LDAP són:

- Autenticació de màquines
- Autenticació d'usuaris
- Llibre d'adreces
- Llibre de nombres telefònics
- etc...

3 LDIF

LDIF (*LDAP Data Interchange Format*) és un format que s'utilitza per representar les entrades d'LDAP en format text. Els fitxers en LDIF s'utilitzen per importar dades al directori o bé modificar-les.

La forma bàsica d'una entrada en format LDIF és:

```
# comentaris
dn: <distinguished name>
<atribut>: <valor>
<atribut>: <valor>
        ...
```

Característiques:

- Les línies que comencen amb # són comentaris.
- Cada **entrada** està separada de l'anterior per un salt de línia.
- El DN s'especifica a l'inici de l'entrada.
- A continuació del DN s'especifiquen els atributs i els seus valors.

Exemple. Fitxer LDIF.

```
# Barbara's Entry
dn: cn=Barbara J Jensen,dc=example,dc=com
cn: Barbara J Jensen
```

```
cn: Babs Jensen
objectClass: person
sn: Jensen

# Bjorn's Entry
dn: cn=Bjorn J Jensen,dc=example,dc=com
cn: Bjorn J Jensen
cn: Bjorn Jensen
objectClass: person
sn: Jensen
# Base64 encoded JPEG photo
jpegPhoto:: /9j/4AAQSkZJRgABAAAAAQABAAD/2wBDABALD
A4MChAODQ4SERATGCgaGBYWGDEjJR0oOjM9PDkzODdASFxOQ
ERXRTc4UG1RV19iZ2hnPk1xeXBkeFxlZ2P/2wBDARESEhgVG

# Jennifer's Entry
dn: cn=Jennifer J Jensen,dc=example,dc=com
cn: Jennifer J Jensen
cn: Jennifer Jensen
objectClass: person
sn: Jensen
# JPEG photo from file
jpegPhoto:< file:///path/to/file.jpeg
```

4 Backends

El backend és la base de dades encarregada d'emmagatzemar o de recuperar les dades que necessiti el servei LDAP. La informació pot emmagatzemar-se en un fitxer de text, en una base de dades relacional, en una base de dades transaccional, i en general en qualsevol sistema suportat. És necessari configurar el backend abans d'utilitzar el servei LDAP.

Alguns dels sistemes de backend suportats per OpenLdap són:

- Berkeley DB: és la BD que es recomana utilitzar. Fa servir bases de dades Oracle Berkeley DB (BDB), molt optimitzades per lectures indexades. Hi ha dos versions conegudes com **`bdb`** i **`hdb`**, aquesta última més optimitzada.
- LDAP: no és una base de dades. S'utilitza quan es volen redirigir les peticions rebudes cap a un altre servidor LDAP.
- LDIF: aquest backend emmagatzema tota la informació en fitxers de text tipus LDIF i utilitza una estructura de directoris per representar l'arbre. **En les darreres versions de OpenLDAP, la configuració es realitza a través d'un backend d'aquest estil**.
- SQL: backend que permet emmagatzemar les dades en una base de dades relacional.

Cal carregar els mòduls necessàris per utilitzar el tipus de backend que es vol.

5 Esquemes (Schema)

Una base de dades LDAP permet emmagatzemar informació molt variada, de fet, permet emmagatzemar entrades del que nosaltres volem. Tot i això, es necessita definir, en algun lloc, quines característiques tindran aquestes dades. De la mateixa manera que abans d'utilitzar bases de dades relacionals definim el contingut de les taules, quan treballem amb directoris cal definir quines característiques tindran les dades que emmagatzemarem.

En el moment de muntar la base de dades ens hem de plantejar:

- Quin tipus d'entrades (**`objectClasses`**) volem emmagatzemar? Persones?, usuaris?, grups?, provincies?, edificis?...
- Quins **atributs** tenen aquestes entrades? Els usuaris tindràn nom, cognoms, adreça de contacte. Els grups tindràn un nom...
- Quin tipus de dades emmagatzemen aquest atributs?
- Quins d'aquests atributs són obligatoris?, i quins són opcionals?
- Quina relació hi ha entre les entrades?
- ...

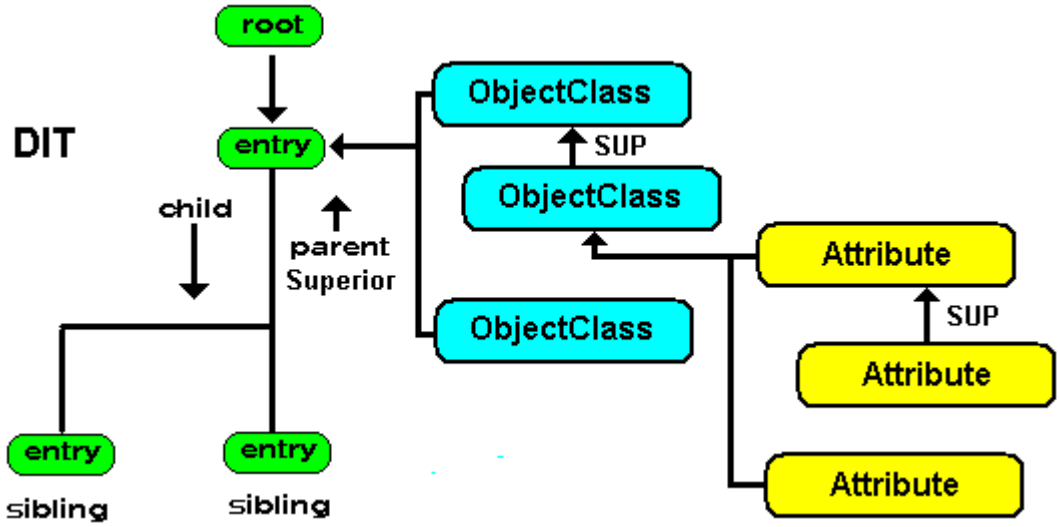
Totes aquestes regles que especifiquen com seran les dades del DIT s'han de definir en **esquemes**. En un esquema es defineixen **objectclasses** i **atributs**. Hi ha esquemes molt utilitzats i que normalment ja venen inclosos en els servidors de LDAP.

5.1 Regles

Un esquema ben format ha de seguir les següents regles:

1. Un **esquema** conté **objectclasses** i **atributs**.
    - Totes les **objectclasses** i els **atributs** han d'estar definits dins dels **esquemes** (exceptuant aquells inclosos per defecte en LDAP)
    - Un **atribut** contingut en un **esquema** pot ser utilitzat per un **objectclass** contingut en un altre esquema.
2. Un **objectclass** agrupa un conjunt d'**atributs**.
    - Les **objectclasses** es defineixen dins dels **esquemes**.
    - Les **objectclasses** es poden organitzar de manera jeràrquica, i en aquest cas s'hereten totes les propietats del seu parent (`SUP`) en el fitxer de configuració.
    - Les **objectclasses** ponden ser estructurals (`STRUCTURAL`), auxiliars (`AUXILIARY`) o abstractes (`ABSTRACT`). Les objectclasses estructurals defineixen una entrada, i les auxiliars es ponden afegir a una entrada. Les objectclasses abstractes no poden ser creades (un exemple és l'objectclass top, que defineix l'arrel de la jerarquia).
    - Les **objectclasses** defineixen quan un **atribut** és obligatori o opcional.
3. Els **atributs** contenen dades.
    - Cada **atribut** s'inclou en una o més **objectclasses**.
    - Un **atribut** pot contenir un valor únic (SINGLE-VALUE) o pot contenir més d'un valor (`MULTI-VALUE`). El valor per defecte és `MULTI-VALUE`.
    - Un **atribut** conté una definició del tipus que conté (`SYNTAX`), per exemple, un string o un enter.
    - Un **atribut** pot heretar les propietats d'un altre (`SUP`)
4. Cada **entrada** dins d'un DIT agrupa un conjunt d'**objectclasses**.
    - Cada **entrada** ha de contenir una i només una **objectclass** de tipus estructural (`STRUCTURAL`).

- Cada **entrada** pot contenir qualsevol nombre d'**objectclasses** auxiliars (AUXILIARY).



5.2 Objectclass

La definició d'un objectclass es troba en la RFC 2252 i és la següent:

```
ObjectClassDescription = "(" whsp
 numericoid whsp      ; ObjectClass identifier
 [ "NAME" qdescrs ]
 [ "DESC" qdstring ]
 [ "OBSOLETE" whsp ]
 [ "SUP" oids ]       ; Superior ObjectClasses
 [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ]
                      ; default structural
 [ "MUST" oids ]      ; AttributeTypes
 [ "MAY" oids ]       ; AttributeTypes
  whsp ")"
```

on **whsp** és un espai en blanc. Veiem un exemple:

```
objectclass ( 2.5.6.2 NAME 'country' SUP top STRUCTURAL
        MUST c
        MAY ( searchGuide $ description ) )
```

- **`objectclass`** indica que a continuació hi ha una definició d'un objectclass.
- **2.5.6.2 NAME 'country'** defineix l'identificador únic per aquest objectclass. Té dues parts: **NAME 'country'** és el nom de l'objecte. El nombre **2.5.6.2** és l'OID (Object Identifier). Aquest valor ha de ser **UNIC** en tot els esquemes carregats en un servidor.
- **SUP top** indica que el objectclass hereta de **'top'**.
- **STRUCTURAL** indica que aquest objectclass pot formar una entrada en un DIT.

- **DESC 'descripció'**. L'exemple no en té, però es pot posar una descripció en forma de text.
- **MUST c**. Indica que els atributs de la llista següent són obligatoris. En aquest cas **c** (countryName) ha d'estar present en totes les entrades que continguin aquest objectclass.
- **MAY (searchguide $ description)**. MAY indica que els atributs en la llista que segueix són opcionals. Si posem més d'un atribut s'han de posar entre parèntesis.

5.3 Atributs

La definició dels atributs es troba en la RFC 2252 i és la següent:

```
AttributeTypeDescription = "(" whsp
   numericoid whsp     ; AttributeType identifier
 [ "NAME" qdescrs ]            ; name used in AttributeType
 [ "DESC" qdstring ]           ; description
 [ "OBSOLETE" whsp ]
 [ "SUP" woid ]                ; derived from this other
                               ; AttributeType
 [ "EQUALITY" woid             ; Matching Rule name
 [ "ORDERING" woid             ; Matching Rule name
 [ "SUBSTR" woid ]             ; Matching Rule name
 [ "SYNTAX" whsp noidlen whsp ] ; Syntax OID
 [ "SINGLE-VALUE" whsp ]       ; default multi-valued
 [ "COLLECTIVE" whsp ]         ; default not collective
 [ "NO-USER-MODIFICATION" whsp ]; default user modifiable
 [ "USAGE" whsp AttributeUsage ]; default userApplications
 whsp ")"
```

whsp és un espai en blanc. Veiem un exemple:

```
attributetype ( 2.5.4.3 NAME ( 'cn' 'commonName' ) SUP name )
```

- **attributetype** indica que l'entrada que hi ha a continuació és un atribut.
- **2.5.4.3 NAME ('cn' 'commonName')** defineix un identificador per aquest atribut. Té dues parts: **NAME ('cn' 'commonName')** permet referir-se a aquest atribut mitjançant text, són els alias (en aquest cas `cn` o `commonName`). En principi no hi ha limits en el nombre d'alies per un atribut. El nombre **2.5.4.3** és l'OID (objectidentifier) i ha de ser únic dins de tots els esquemes carregats en un servidor ldap.
- **SUP name** indica quin és l'atribut pare. En aquest cas name. L'atribut hereta les

propietats del pare, que veiem a continuació.

```
attributetype ( 2.5.4.41 NAME 'name'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )
```

- **EQUALITY caseIgnoreMatch** indica com es comportarà l'atribut (i tots els seus atributs fills) quan s'utilitzi un filtre de cerca. No cal entrar en detall.
- **SUBSTR caseIgnoreSubstringsMatch** idem que l'anterior.
- **SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768}** és un OID que defineix el tipus de dades i quines regles s'apliquen. Aquest OID és un string.

6 Eines client d'OpenLDAP (ldap tools)

OpenLDAP proporciona un paquet de software amb eines per gestionar el directori LDAP. Aquestes eines estan contingudes en el paquet de software `ldap-utils`.

`ldapadd` - afegeix entrades LDIF a un directori LDAP

`ldapdelete` - esborra entrades del directori LDAP

`ldapmodify` - modifica entrades del directori LDAP

`ldapmodrdn` - modifica el DN (*Distinguished Name*) d'una entrada del directori LDAP

`ldappasswd` - modifica el password d'una entrada del directori LDAP

`ldapsearch` - cerca dins del directori LDAP

`ldapwhoami` - pregunta qui ets dins del directori LDAP

6.1 ldapsearch

ldapsearch obre una connexió amb un servei LDAP, es vincula (bind) i fa una cerca utilitzant els paràmetres especificats. Es pot indicar un filtre de cerca, però si no s'indica es fa servir un per defecte `(objectClass=*)`, que retorna totes les entrades del directori.

Els resultats de ldapsearch es mostren en format LDIF.

Sintaxi:

```
ldapsearch  [-a never|always|search|find] [-A] [-b searchbase] [-c] [-d
debuglevel] [-D binddn] [-e [!]ext[=extparam]] [-E [!]ext[=extparam]] [-f
```

```
file] [-F prefix] [-h ldaphost] [-H ldapuri] [-I] [-l time] [-L[L[L]]] [-
M[M]] [-n] [-O security-properties] [-p ldapport] [-P 2|3] [-Q] [-R realm]
[-s base|one|sub|children] [-S attribute] [-t[t]] [-T path] [-u] [-U
authcid] [-v] [-w passwd] [-W] [-x] [-X authzid] [-y passwdfile] [-Y mech]
[-z sizelimit] [-Z[Z]] filter [attrs...]
```

Opcions:

opció	descripció:
-b baseUse	DN base a partir del qual efectuar la cerca
-D binddn	Fer servir el DN especificat per vincular-se al directori LDAP.
-H ldapuri	URI del servidor ldap. Si no es defineix fa servir per defecte la URI `ldap://localhost:389`. Per exemple: `-H ldap://ldap.example.com`
-L	Els resultats de la cerca es mostren en format LDIF en diferents versions. -L: LDIF v1, -LL: LDIF sense comentaris, -LLL: no imprimeix la versió de LDIF. Per defecte: -L.
-s [base|one|sub|children]	Especifica el nivell de profunditat de la cerca. `base`: només mostra l'element cercat, sense cap fill `one`: mostra el primer nivell de fills `sub`: mostra tots els descendents, inclosa l'entrada `children`: mostra tots els descendents, sense incloure l'entrada.
-x	Utilitzar autenticació simple en comptes de SASL.
-Y mecanisme	Especificar el mecanisme d'autenticació SASL.

Exemples:

```
# ldapsearch -x -H ldap://ldap.example.com -LL -b dc=example,dc=com
```

Cerca tota la informació de totes les entrades del servidor LDAP incloses dins de dc=example, dc=com.

```
# ldapsearch -x -H ldap://ldap.example.com -LL -b
ou=people,dc=example,dc=com "(mail=*smith*)" sn cn mail
```

Cerca en el servidor LDAP totes aquelles entrades que estiguin dins de la UO `ou=people,dc=example,dc=com` i que tinguin la paraula `smith` en l'atribut `mail`. Retorna només els atributs `cn`, `sc` i `mail`.

6.1.1 filtres de cerca

Els filtres de cerca permeten afinar el resultat obtingut per `ldapsearch`. S'inclouen al final de la comanda i la seva sintaxi és la següent:

atribut operador valor

Exemples:

```
cn=pepe
uidNumber>500
```

L'atribut pot ser qualsevol atribut d'una entrada (objectclass, cn, uid, telephoneNumber...)

La llista d'operadors possibles és la següent:

Tipus	Operador	Descripció
Igualtat	=	Retorna totes les entrades que conten exàctament el valor proporcionat. pe: cn="pepe"
Substring	=string*	Retorna les entrades que contenen el substring especificat. L'asterisc es pot substituir per qualsevol string.
Major o igual a	>=	Retorna les entrades amb el valor major o igual al valor indicat.
Major	>	Retorna les entrades amb el valor major al valor indicat
Presencia	=*	Retorna les entrades amb un o més valors d'aquest atribut

Composició de filtres

Si volem filtrar per més d'un atribut, podem composar múltiples filtres. Ens pot interessar, per exemple, cercar aquelles entrades amb `gidNumber = 1000` i en el nom tinguin una lletra 'a' `cn=*a*`.

Llavors podem fer el següent:

```
(&(gidNumber=1000)(cn=*a*))
```

El símbol & vol dir que s'han de cumplir totes les condicions que venen després dels parèntesis.

En general, la sintaxi per composar filtres és la següent:

```
(operador-boolea(filtre)(filtre)(filtre)...)
```

Operador	Símbol	Descripció
AND	&	Tots els filtres han de ser certs
OR	|	Al menys un filtre ha de ser cert
NOT	!	El filtre ha de ser fals

6.2 ldapadd i ldapmodify

Les dues comandes fan servir els mateixos arguments. `ldamodify` és equivalent a ldapadd quan fa servir l'argument -a. Les dues comandes fan servir arxius ldif.

Sintaxi:

```
ldapmodify/ldapadd [-a] [-c] [-d debug_level] [-f file] [-D binddn] [-H ldapuri] [-h ldaphost] [-I] [-k] [-K] [-M[M]] [-n] [-O security-properties] [-p ldapport] [-P 2|3] [-Q] [-S file] [-R realm] [-U authcid] [-v] [-W] [-w password] [-x] [-X authzid] [-y passwdfile] [-Y mech] [-Z[Z]]
```

Opció	Descripció
-a	Afegir noves entrades. Per defecte, ldapadd sempre ho té activat.
-c	Continua encara que hi hagi errors. Per defecte, si hi ha un error en un fitxer ldif s'aturarà el procés.
-D binddn	Fer servir el DN especificat per vincular-se al directori LDAP.
-f arxiu	Carrega l'arxiu ldif.
-H ldapuri	URI del servidor ldap. Si no es defineix fa servir per defecte la URI `ldap://localhost:389`. Per exemple: `-H ldap://ldap.example.com`
-w passwd	Fes servir el password donat.
-W	Preguntarà pel password.
-x	Utilitzar autenticació simple en comptes de SASL.
-Y mecanisme	Especificar el mecanisme d'autenticació SASL.

6.3 ldapdelete

Obre una connexió amb un servidor LDAP, es vincula i esborra una o més entrades. Cal especificar el DN de les entrades que volem esborrar, que es poden indicar dins d'un fitxer (opció `-f`).

Nota: El fitxer cal que estigui en format LDIF. Simplement és un fitxer de text que conté, en cada línia, els DN que es volen esborrar:

```
cn=someone,ou=people,dc=example,dc=com
cn=someone else,ou=people,dc=example,dc=com
```

alternativament es pot utilitzar un fitxer LDIF:

```
dn: cn=someone,ou=people,dc=example,dc=com
changetype: delete

cn=someone else,ou=people,dc=example,dc=com
changetype: delete
```

Sintaxi:

```
ldapdelete [-c] [-d debuglevel] [-D binddn] [-f file] [-h ldaphost] [-H
ldapuri] [-I] [-k] [-K] [-M[M]] [-n] [-O security-properties] [-P 2|3] [-p
ldapport] [-Q] [-R realm] [-U authcid] [-v] [-W] [-w passwd] [-x] [-X
authzid] [-y passwdfile] [-Y mech] [-Z[Z]] [dn]...
```

Opció	Descripció
dn	Entrades a esborrar.
-c	Continua encara que hi hagi errors. Per defecte, si hi ha un error en un fitxer ldif s'aturarà el procés.
-D binddn	Fer servir el DN especificat per vincular-se al directori LDAP.
-f arxiu	Carrega l'arxiu ldif.
-H ldapuri	URI del servidor ldap. Si no es defineix fa servir per defecte la URI `ldap://localhost:389`. Per exemple: `-H ldap://ldap.example.com`
-w passwd	Fes servir el password donat.
-W	Preguntarà pel password.
-x	Utilitzar autenticació simple en comptes de SASL.
-Y mecanisme	Especificar el mecanisme d'autenticació SASL.

6.4 ldappasswd

Modifica el password d'un usuari que resideix al directori.

Sintaxi:

```
ldappasswd [-A] [-a oldpasswd] [-t oldpasswdfile] [-D binddn]
  [-d debuglevel] [-H ldapuri] [-h ldaphost]  [-n]  [-p ldapport]
  [-S]  [-s newpasswd]   [-T newpasswdfile]   [-v]  [-W]  [-w passwd]
  [-y passwdfile]  [-O props]  [-I]  [-Q]  [-U authcid]
  [-x]  [-X authzid] [-R realm] [-Y mech] [-Z[Z]] [user]
```

Opció	Descripció
user	L'usuari al qual aplicar l'acció. Exemple: `"cn=usuari,ou=people,dc=example,dc=com"`
-A	Preguntar pel password anterior.
-a passwd	El password actual és `passwd`.
-D binddn	Fer servir el DN especificat per vincular-se al directori LDAP.
-H ldapuri	URI del servidor ldap. Si no es defineix fa servir per defecte la URI `ldap://localhost:389`. Per exemple: `-H ldap://ldap.example.com`
-w passwd	Fes servir el password donat.

-W	Preguntarà pel password.
-x	Utilitzar autenticació simple en comptes de SASL.
-Y mecanisme	Especificar el mecanisme d'autenticació SASL.

Exemple:

```
# ldappasswd -H ldap://localhost -D cn=admin,dc=example,dc=com -W -A
```

Modifica el password per l'entrada cn=usuari,ou=people,dc=example,dc=com fent servir el compte d'administrador `cn=admin,dc=example,dc=com`.

7 Mètodes d'autenticació

Per realitzar qualsevol operació amb LDAP ens hem d'autenticar (afegir entrades, cercar dins del DIT, esborrar entrades...). Hi ha dos mètodes per autenticar-se:

- mètode simple
- per SASL (*Simple Authentication and Security Layer*)

7.1 Simple

El mètode d'autenticació simple té tres modes d'operació:

1. Anònim
2. No autenticat: només proporcionem l'usuari, no el password
3. Autenticat: proporcionem usuari/password

Quan no proporcionem ni usuarii ni password es farà servir l'autenticació anònima i per tant, durant la connexió tindrem els permisos que s'hagin assignat a l'usuari anònim.

En les eines de ldaptools, l'autenticació simple es realitza mitjançant l'opció `-x`.

```
# ldapsearch -x ...
# ldapadd -x ...
```

Exemple: cerca de tot l'arbre del domini dc=example,dc=com com un usuari anònim.

```
# ldapsearch -x -b "dc=example,dc=com"
```

Si ens volem vincular **utilitzant un usuari** de l'arbre hem de proporcionar el DN d'aquest usuari amb la opció `-D`. La opció -w o -W s'ha d'incloure si volem escriure

password.

L'example que es mostra a continuació fa una cerca de tot l'arbre del domini dc=example,dc=com com l'usuari pepe de la uo informàtica. El password s'ha d'introduir a continuació.

```
# ldapsearch -x -D "cn=pepe,ou=informàtica,dc=example,dc=com" -b "dc=example,dc=com" -W
```

També podem introduir el password per la línia de comandes amb la opció `-w`.

```
# ldapsearch -x -D "cn=pepe,ou=informàtica,dc=example,dc=com" -b "dc=example,dc=com" -w secret
```

7.2 SASL

Podem fer servir mecanismes d'autenticació SASL (*Simple Authentication and Security Layer*). Entre aquests s'inclouen:

- GSSAPI (Kerberos)
- DIGEST-MD5
- PLAIN
- EXTERNAL
- i més.

Amb la opció `-Y` podem indicar quin mecanisme utilitzar.

El mecanisme EXTERNAL fa servir mecanismes de inclosos en el protocol de baix nivell per a l'autenticació. Per exemple, podem utilitzar els usuaris linux si fem servir el protocol IPC (`ldapi:///`).

Exemples:

```
# ldapsearch -Y EXTERNAL -H ldapi:/// -b "dc=example,dc=com"
```

8 ACL

De vegades ens insteressa controlar l'accés a diferents parts del directori i restringir determinades accions a determinats usuaris. Per exemple, ens pot interessar que l'administrador del directori pugui modificar tot el contingut, mentre que un altre usuari només pugui modificar les seves dades.

L'accés a les entrades i atributs de LDAP estan controlades per atributs olcAccess, que determinen quins usuaris poden realitzar determinades accions. Aquest atributs tenen la següent estructura:

```
access to <què> by <qui> <nivell d'accés>
```

Un exemple:

```
access to attr=telephoneNumber                        - es defineix l'accés sobre l'atribut telephon.
       by dn="cn=pepe,dc=example,dc=com" write        - pepe pot modificar l'atribut de tots
       by self write                                  - cada usuari pot modificar el seu atribut
       by * read                                      - els altres només poden llegir
```

La taula següent resumeix què es pot posar en cadascun d'aquests camps (hi ha moltes més possibilitats).

access to	***què***	**by**	***qui***	***nivell d'accés***
access to	* (tot) dn=".*,o=*organization*" filter="sn=Ander*" attr=*atribut* attr=atribut*1*,*atribut2*.	by	* (tothom) anonymous users (Usuaris autenticats) self (Usuari associat amb l'entrada) dn= (Usuaris que tinguin aquest dn)	none auth read write

La sintaxi general d'un atribut olcAccess en LDIF és:

```
olcAccess: <access directive>
       <access directive> ::= to <what>
              [by <who> [<access>] [<control>] ]+
       <what> ::= * |
              [dn[.<basic-style>]=<regex> | dn.<scope-style>=<DN>]
              [filter=<ldapfilter>] [attrs=<attrlist>]
       <basic-style> ::= regex | exact
       <scope-style> ::= base | one | subtree | children
       <attrlist> ::= <attr> [val[.<basic-style>]=<regex>] | <attr> , <attrlist>
       <attr> ::= <attrname> | entry | children
       <who> ::= * | [anonymous | users | self
                     | dn[.<basic-style>]=<regex> | dn.<scope-style>=<DN>]
              [dnattr=<attrname>]
              [group[/<objectclass>[/<attrname>][.<basic-style>]]=<regex>]
              [peername[.<basic-style>]=<regex>]
              [sockname[.<basic-style>]=<regex>]
              [domain[.<basic-style>]=<regex>]
              [sockurl[.<basic-style>]=<regex>]
              [set=<setspec>]
              [aci=<attrname>]
       <access> ::= [self]{<level>|<priv>}
       <level> ::= none | disclose | auth | compare | search | read | write | manage
```

```
<priv> ::= {=|+|-}{m|w|r|s|c|x|d|0}+
<control> ::= [stop | continue | break]
```

9 LDIF en detall

Les dades en format LDIF s'utilitzen en els següents casos:

1. Per construir l'estructura incial del DIT
2. Per afegir (importar) dades al DIT.
3. Per restaurar (importar) dades d'un DIT.
4. Per arxivar (exportar) dades d'un DIT.
5. Per aplicar edicions massives en un DIT.

Per operar amb LDIF podem utilitzar les comandes que s'han vist en seccions anteriors. Cal tenir en compte que és un format molt delicat: la omisió d'espais en blanc o l'inclusió allà on no toca és particularment important.

9.1 Format LDIF

El LDIF consisteix en un nombre determinat de linies de text, cadascuna de les quals conté **directives**. Les linies de text s'agrupen en **seqüències** que defineixen **entrades** o **operadors**.

Una línia pot ser:

- **Una directiva**: una línia que comença (columna 1) amb qualsevol caràcter excepte un espai o un #.
- **Una continuació**: una línia que segueix a una directiva i comença (columna 1) amb un espai. Els caràcters que hi ha a continuació s'assumeixen com a continuació de la línia anterior.
- **Una línia en blanc**: no hi ha caràcters. S'utilitzen per separar entrades.
- **Un comentari**: línia que comença (columna 1) amb el caràcter #.
- **Una línia de separació**: línia que comença amb un – (guió). S'utilitzen per indicar el fi d'un operador.

Una seqüència de línies pot ser:

- **Una entrada**: grup de directives que, normalment, comencen amb dn:. Una entrada acaba amb una línia en blanc.
- **Un operador**: grup de directives que contenen la directiva changetype: modify.

Un operador acaba amb una línia en blanc o una línia de separació.

Exemple:

```
## DEFINE DIT ROOT/BASE/SUFFIX ####
## uses RFC 2377 format
## replace example and com as necessary below
## or for experimentation leave as is

## dcObject is an AUXILLIARY objectclass and MUST
## have a STRUCTURAL objectclass (organization in this case)
# this is an ENTRY sequence and is preceded by a BLANK line

dn: dc=example,dc=com
dc: example
description: My wonderful company as much text as you want to place
 in this line up to 32K continuation data for the line above must
 have <CR> or <CR><LF> i.e. ENTER works
 on both Windows and *nix system - new line MUST begin with ONE SPACE
objectClass: dcObject
objectClass: organization
o: Example, Inc.

## FIRST Level hierarchy - people
## uses mixed upper and lower case for objectclass
# this is an ENTRY sequence and is preceded by a BLANK line

dn: ou=people, dc=example,dc=com
ou: people
description: All people in organisation
objectclass: organizationalunit

## SECOND Level hierarchy
## ADD a single entry under FIRST (people) level
# this is an ENTRY sequence and is preceded by a BLANK line
# the ou: Human Resources is the department name

dn: cn=Robert Smith,ou=people,dc=example,dc=com
objectclass: inetOrgPerson
cn: Robert Smith
cn: Robert J Smith
cn: bob  smith
sn: smith
uid: rjsmith
userpassword: rJsmitH
carlicense: HISCAR 123
homephone: 555-111-2222
mail: r.smith@example.com
mail: rsmith@example.com
mail: bob.smith@example.com
description: swell guy
ou: Human Resources
```

9.2 Directives

9.2.1 add

Format:

```
add: attributename
```

La directiva `add` sempre segueix una directiva `changetype: modify` i defineix el nom de l'atribut que s'ha d'afegir a l'entrada existent.

Exemple:

```
# adding single attribute
# current attribute values unchanged

dn: cn=Robert Smith,ou=people,dc=example,dc=com
changetype: modify
add: telephonenumber
telephonenumber: 123-111

# adding multiple attributes
# current attribute values unchanged

dn: cn=Robert Smith,ou=people,dc=example,dc=com
changetype: modify
add: telephonenumber
telephonenumber: 555-123-1111
telephonenumber: 111
```

9.2.2 changetype

Format:

```
changetype: type
```

Una directiva `changetype` sempre ha d'anar a continuació d'una directiva `dn:` i defineix la operació que es farà a l'entrada.

`type` pot ser un d'aquest valors:

- **`add`**: indica que les següents directives crearan l'entrada. Si l'entrada ja existeix, s'ha d'utilitzar changetype: modify. Si no hi ha directiva changetype, s'assumeix `changetype: add`.

Exemple:

```
dn: cn=Robert Smith,ou=people,dc=example,dc=com
# adds entry of dn above
changetype: add
objectclass: inetorgperson
cn: Robert Smith
...
```

- **`delete`**: l'entrada especificada en la directiva dn s'esborrarà.

Exemple:

```
dn: cn=Robert Smith,ou=people,dc=example,dc=com

# delete entry pointed to by dn above

changetype: delete
```

- **`modify`**: Les directives que venen a continuació modificaràn l'entrada. A continuació, els atributs es poden afegir, canviar o eliminar.

Exemple:

```
dn: cn=Robert Smith,ou=people,dc=example,dc=com
# modifies entry pointed to by dn above
changetype: modify
# single operation
add: telephonenumber
telephonenumber: 555

dn: cn=Robert Smith,ou=people,dc=example,dc=com
# modifies entry pointed to by dn above
changetype: modify
# multiple operations
add: telephonenumber
telephonenumber: 555
# following line is a SEPARATOR line
-
replace: mail
mail: bob.smith@example.com
-
delete: secretary

# to ADD a new AUXILIARY object class
# to an existing entry
```

```
dn: cn=Robert Smith,ou=people,dc=example,dc=com
# modifies entry pointed to by dn above
changetype: modify
# this objectclass is used for binding
objectclass: inetorgperson
# AUXILIARY objectclass being added
objectclass: posixaccount
# following attributes include MUST attributes
# of new objectclass
uidnumber: 200
gidnumber: 207
homedirectory: /home/rsmith
...
```

- **`modrdn`** o **`moddn`**: s'utilitza per canviar el RDN de l'entrada. A continuació ha d'haver-hi una directiva **`newrdn:`** i pot seguir-ne una directiva **`deleteoldrdn:`** i una directiva **`newsuperior:`**.

  NO és pot renombrar una entrada quan aquesta té un o més fills.

Exemple:

```
dn: cn=Robert Ssmith,ou=people,dc=example,dc=com
# following sequence renames the above DN to
# cn=Robert Smith,ou=people.dc=example,dc=com
# and deletes the entry
# cn=Robert Ssmith,ou=people,dc=example,dc=com
changetype: modrdn
newrdn: cn=Robert Smith
deleteoldrdn: 1
```

9.2.3 delete

Format:

```
delete: attributename
```

La directiva delete va seguida de la directiva `changetype: modify` i defineix el nom de l'atribut que cal esborrar. Per esborrar una entrada cal utilitzar `changetype: delete`.

La directiva delete pot anar seguida d'una o més directives que especifiquin quin atribut esborrar. Si no va seguida de res (línia en blanc o separador) llavors tots els atributs s'eliminen.

Exemple:

```
# deleting single attribute value

dn: cn=Robert Ssmith,ou=people,dc=example,dc=com
changetype: modify
# deletes only the attributes with value 123-111 and 111
# all other telephonenumber attributes are unchanged
delete: telephonenumber
telephonenumber: 123-111
telephonenumber: 111

# deleting multiple attributes
dn: cn=Robert Ssmith,ou=people,dc=example,dc=com
changetype: modify
# deletes all telephonenumber attributes
delete: telephonenumber
```

9.2.4 deleteoldrdn

Format:

```
deleteoldrdn: acció
```

La directiva deleteoldrdn defineix l'acció que cal dur a terme amb el DN original després d'haver inclòs la directiva `changetype: modrdn`. Aquesta directiva pot prendre el valor 0 (fals), en el cas de no voler esborrar l'entrada original, o d'1 (cert) en el cas de voler esborrar l'entrada original.

Exemple:

```
# fixes error in entry DN and
# deletes current entry


dn: cn=Robert Ssmith,ou=people,dc=example,dc=com
changetype: modrdn
# create the new name (RDN)
newrdn: cn=Robert Smith
# delete current (Robert Ssmith) entry
deleteoldrdn: 1
```

9.2.5 dn

Format:

```
dn: DN
```

La directiva dn defineix el Distinguished Name (DN). Ha d'anar precedida per una línia en blanc.

9.2.6 newrdn

Format:

```
newrdn: RDN
```

La directiva `newrdn` va precedida de `changetype: modrdn`. Crea una còpia de l'entrada especificada en la directiva `dn`. Normalment es combina amb `deleteoldrdn`.

Si es combina amb la directiva `newsuperior` es pot utilitzar per copiar o moure una entrada dins del DIT.

Exemple:

```
# use when correcting an error

dn: cn=Robert Ssmith,ou=people,dc=example,dc=com
changetype: modrdn
# corrected entry
newrdn: cn=Robert Smith
# deletes old entry
deleteoldrdn: 1
```

9.2.7 newsuperior

Format:

```
newsuperior: DN
```

La directiva newsuperior permet moure una entrada dins del DIT. Aquesta directiva s'utilitza amb changetype: `modrdn`, `newrdn` i `deleteoldrdn`.

Exemple:

```
# moves the entry from people to expeople

dn: cn=Robert Smith,ou=people,dc=example,dc=com
```

```
changetype: modrdn
# rdn unchanged
newrdn: cn=Robert Smith
# deletes old entry
deleteoldrdn: 1
# adds to expeople hierarchy
newsuperior: ou=expeople,dc=example,dc=com

# makes a copy of the entry in expeople

dn: cn=Robert Smith,ou=people,dc=example,dc=com
changetype: modrdn
# rdn unchanged
newrdn: cn=Robert Smith
# keeps current entry
deleteoldrdn: 0
# adds to expeople hierarchy
newsuperior: ou=expeople,dc=example,dc=com
```

9.2.8 objectclass

Format:

objectclass: nomobjectclass

Configura l'atribut objectclass. És imprescindible que hi hagi, al menys, un `objectclass` de tipus estructural. Poden haver-hi múltiples `objectclass` de tipus auxiliar.

Exemple:

```
# adding objectclasses to a new entry

dn: cn=Robert Smith,ou=people,dc=example,dc=com
changetype: add
# inetorgperson is lowest level in hierarchy
objectclass: inetorgperson
cn: Robert smith
cn: Robert J Smith
cn: Bob Smith
telephonenumber: 123-111
...
```

```
# adding objectclasses to a new entry

dn: cn=Robert Smith,ou=people,dc=example,dc=com
changetype: add
# inetorgperson is lowest level in hierarchy
objectclass: inetorgperson
# both objectclasses must be present here
# because posixaccount is an AUXILIARY
objectclass: posixaccount
cn: Robert smith
cn: Robert J Smith
cn: Bob Smith
telephonenumber: 123-111
...

# to ADD a new AUXILIARY object class
# to an existing entry

dn: cn=Robert Smith,ou=people,dc=example,dc=com
# modifies entry pointed to by dn above
changetype: modify
# this objectclass is used for binding
objectclass: inetorgperson
# AUXILIARY objectclass being added
objectclass: posixaccount
# following attributes include MUST attributes
# of new objectclass
uidnumber: 200
gidnumber: 207
homedirectory: /home/rsmith
```

9.2.9 replace

Format:

```
replace: attributename
```

La directiva replace va seguida de `changetype: modify` i defineix el nom de l'atribut que serà reemplaçat. Si l'atribut és multi-valor, es reemplaçen TOTS els valors amb el nou valor. Si només es vol canviar un, cal esborrar (**`delete`**) l'atribut i després afegir-lo (**`add`**).

Exemple:

```
# replace single attribute value

dn: cn=Robert Ssmith,ou=people,dc=example,dc=com
changetype: modify
replace: uid
uid: bill



# replace multi attribute value

dn: cn=Robert Smith,ou=people,dc=example,dc=com
changetype: modify
# replaces ALL telephonenumber attributes
# with 555-111-1212
replace: telephonenumber
telephonenumber: 555-111-1212

# replace a single value of a multi attribute value
# delete then add
# example replaces 555-111-1212 with 555

dn: cn=Robert Smith,ou=people,dc=example,dc=com
changetype: modify
# first delete the required attribute
delete: telephonenumber
telephonenumber: 555-111-1212
# SEPARATOR line essential
-
# add new value
add: telephonenumber
telephonenumber: 555
```

10 Instal·lació del servei OpenLDAP (Ubuntu 10.10)

10.1 Instal·lacció de paquets

El paquet slapd conté el servidor ldap. ldap-utils són les eines client que utilitzarem per fer proves.

```
# apt-get install slapd ldap-utils
```

Per saber quines aplicacions venen en cada paquet podem utilitzar l'eina `dpkg`.

```
# dpkg -L slapd  | grep bin
/usr/sbin
/usr/sbin/slapd: dimoni servei ldap
/usr/sbin/slapacl
/usr/sbin/slapadd
/usr/sbin/slapauth
/usr/sbin/slapcat
/usr/sbin/slapdn
/usr/sbin/slapindex
/usr/sbin/slappasswd
/usr/sbin/slaptest
/etc/apparmor.d/usr.sbin.slapd
```

```
# dpkg -L ldap-utils  | grep bin
/usr/bin
/usr/bin/ldapdelete
/usr/bin/ldapmodrdn
/usr/bin/ldapsearch
/usr/bin/ldapcompare
/usr/bin/ldapmodify
/usr/bin/ldappasswd
/usr/bin/ldapwhoami
/usr/bin/ldapexop
/usr/bin/ldapurl
/usr/bin/ldapadd
```

10.2 Afegir els esquemes bàsics

Farem servir els esquemes preinstalats `cosine.ldif`, `nis.ldif` i `inetorgperson.ldif`.

```
# sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/cosine.ldif
# sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/nis.ldif
# sudo ldapadd -Y EXTERNAL -H ldapi:/// -f
/etc/ldap/schema/inetorgperson.ldif
```

10.3 Afegir la configuració del backend.

Cal configurar un backend, la base de dades per emmagatzemar el directori. A continuació es mostra un exemple de fitxer LDIF per configurar un backend i que podem adaptar a les nostres necessitats.

```
# Load dynamic backend modules
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulepath: /usr/lib/ldap
olcModuleload: back_hdb

# Database settings
dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcSuffix: dc=example,dc=com
olcDbDirectory: /var/lib/ldap
olcRootDN: cn=admin,dc=example,dc=com
olcRootPW: secret
olcDbConfig: set_cachesize 0 2097152 0
olcDbConfig: set_lk_max_objects 1500
olcDbConfig: set_lk_max_locks 1500
olcDbConfig: set_lk_max_lockers 1500
olcDbIndex: objectClass eq
olcLastMod: TRUE
olcDbCheckpoint: 512 30
olcAccess: to attrs=userPassword by dn="cn=admin,dc=example,dc=com" write by
anonymous auth by self write by * none
olcAccess: to attrs=shadowLastChange by self write by * read
olcAccess: to dn.base="" by * read
olcAccess: to * by dn="cn=admin,dc=example,dc=com" write by * read
```

L'atribut **olcRootPW**: secret conté el password. Cal canviar-lo per el

`password que volem.`

Alguns comentaris:

olcSuffix conté el domini que administrarem.

olcRootDN conté l'usuari que serà administrador (root) del directori. En aquest cas l'usuari admin dins del domini dc=example,dc=com.

olcRootPW conté el password de root. Caldria modificar-lo al nostre gust.

Carregar-lo:

```
# sudo ldapadd -Y EXTERNAL -H ldapi:/// -f fitxer_backend.ldif
```

On `fitxer_backend.ldif` és el fitxer amb el contigut anterior.

10.4 Poblar l'arbre

Cal crear un arxiu ldif per poblar l'arbre i carregar-lo. Aquí teniu un exemple (modifiqueu-lo per adaptar-lo a les vostres necessitats).

```
# Create top-level object in domain
dn: dc=example,dc=com
objectClass: top
objectClass: dcObject
objectclass: organization
o: Example Organization
dc: Example
description: LDAP Example

# Admin user.
dn: cn=admin,dc=example,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword: secret

dn: ou=people,dc=example,dc=com
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=example,dc=com
objectClass: organizationalUnit
ou: groups

dn: uid=john,ou=people,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: john
sn: Doe
givenName: John
cn: John Doe
```

```
displayName: John Doe
uidNumber: 1000
gidNumber: 10000
userPassword: password
gecos: John Doe
loginShell: /bin/bash
homeDirectory: /home/john
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: john.doe@example.com
postalCode: 31000
l: Toulouse
o: Example
mobile: +33 (0)6 xx xx xx xx
homePhone: +33 (0)5 xx xx xx xx
title: System Administrator
postalAddress:
initials: JD

dn: cn=example,ou=groups,dc=example,dc=com
objectClass: posixGroup
cn: example
gidNumber: 10000
```

I afegir-ho:

```
# sudo ldapadd -x -D cn=admin,dc=example,dc=com -W -f fitxer_arbre.ldif
```

On fitxer_arbre.ldif és el fitxer amb el contingut ldif.

10.5 phpldapadmin

Aplicació web per configurar ldap

```
# apt-get install phpldapadmin
```

Podem accedir utilitzant un navegador (firefox) i introduint la següent URL: http://localhost/phpldapadmin/

10.6 Ubuntu LDAP Administration tool

Aplicaciones\Centro de software ubuntu

Afegir: ldap administration tool.

11 Autenticació d'un client amb LDAP en Ubuntu 10.10

11.1 Eines bàsiques (ldap-client)

```
# apt-get install ldap-utils
```

es configura `/etc/ldap.conf` (no confondre amb `/etc/ldap.conf`)

`ldapsearch`: permet cercar dins del directori

11.2 Configurar una màquina Linux per autenticar-se amb LDAP

11.2.1 NSSwitch

Name Service Switch (NSS) permet reemplaçar fitxers bàsics de configuració de Unix (com per exemple: `/etc/passwd`, `/etc/group`, `/etc/hosts`) per bases de dades centralitzades.

Podem afegir diferents moduls per suportar diferents tipus de bases de dades. Per exemple, per suportar ldap cal instal·lar el paquet `libnss-ldap`. **A l'instal·lar aquest paquet també s'afegeix el paquet libpam-ldap.**

```
$ cat /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         compat
group:          compat
shadow:         compat
```

```
hosts:          files mdns4_minimal [NOTFOUND=return] dns mdns4
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

Primera columna: base de dades.

Segona columa: llista el lloc a on es buscarà aquesta base de dades, en ordre.

Bases de dades

`passwd`: paraules de pas dels usuaris.

`group`: grups d'usuaris

`shadow`: paraules de pas shadow del usuaris

`hosts`: noms de màquina i números

`networks`: noms i números de xarxes

`aliases`: Mail aliases

`ethers`: números Ethernet numbers,

... i més

Llocs a on buscar les bases de dades:

files: buscarà a

`/etc/hosts`
`/etc/netgroup`
`/etc/networks`
`/etc/protocols`
`/etc/rpc`
`/etc/services`

compat: buscarà a

`/etc/passwd`

`/etc/group`

`/etc/shadow`

ldap: buscarà a ldap. Cal isntal·lar el paquet `libnss-ldap`. (es configura a `/etc/ldap.conf` o fent `dpkg-reconfigure libnss-ldap`, no confondre amb `/etc/ldap/ldap.conf` del paquet ldap-utils)

Podem utilitzar la comanda `getent` per llegir alguna base de dades des del client.

```
# getent passwd
```

actualitzar els serveis de nsswitch

```
# nss_updatedb ldap
```

11.2.2 PAM ldap

PAM: **Pluggable Authentication Modules**

Permet que les aplicacions utilitzin altres sistemes d'autenticació que no només el típic sistema de /etc/passwd.

Per defecte s'instal·la amb el paquet libnss-ldap.

```
# apt-get install libpam-ldap
```

Llista d'aplicacions configurades per utilitzar pam

```
# ls /etc/pam.d/
atd       chpasswd     common-account     common-password     common-session-
noninteractive  cups  gdm-autologin      login      other    polkit-1  samba
sudo   chfn      chsh   common-auth              common-session        cron
gdm   gnome-screensaver  newusers  passwd  ppp       su
```

NOTES:

login: es el programa de login des de la consola

gdm (gnome display manager): programa de login de gnome.

11.2.3 Configurar el client ubuntu

```
# sudo apt-get install libpam-ldap libnss-ldap nss-updatedb libnss-db nfs-
common nscd ldap-utils
```

la instal·lació del paquet libnss-ldap preguntarà per:

LDAP server Uniform Resource Identifier: ldap://ldap.example.com

Distinguished name of the search base: dc=example,dc=com

ldap://ldap.example.com 3

Make local root Database admin: Yes

Does the LDAP database require login? No

LDAP account for root: cn=admin,dc=example,dc=com

LDAP root password: password

per tornar-hi: **sudo dpkg-reconfigure ldap-auth-config**

Editar l'arxiu /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

SIZELIMIT       0
TIMELIMIT       0
DEREF           never
```

Actualitzem el NSSwiitch.

```
# sudo nss_updatedb ldap
```

Podem provar el funcionament amb la comanda `# getent passwd`. Si aparèixen els usuaris donats d'alta en el servidor LDAP podem executar la comanda login des d'un terminal i entrar fent servir un usuari de LDAP.

12 Annex: Atributs i objectclasses més freqüents

Abbrev.	Name	objectClass	Schema
c	countryName	country	core.schema
cn	commonName	person organizationalPerson organizationalRole groupOfNames applicationProcess applicationEntity posixAccount device	core.schema
dc	domainComponent	dcObject	core.schema
co	friendlyCountryName	friendlyCountry	cosine.schema
gn	givenName	inetOrgPerson	core.schema
l	localityName	locality organizationalPerson	core.schema
mail	rfc822Mailbox	inetOrgPerson	core.schema
mobile	mobileTelephoneNumber	inetOrgPerson	cosine.schema
o	organizationName	organization	core.schema
ou	organisationalUnitName	organizationUnit	core.schema
sn	surname	person	core.schema
st	stateOrProvinceName	organizationalPerson	core.schema
street	streetAddress	organizationalPerson	core.schema
userPassword	userPassword	organization organizationalUnit person dmd simpleSecurityObject domain posixAccount	core.schema
uid	userid	account inetOrgPerson posixAccount	core.schema

Name	MUST	MAY	Schema
account	userid	description $ seeAlso $ localityName $ organizationName $ organizationalUnitName $ host	cosine.schema
country	c	searchGuide $ description	core.schema
dcObject	dc	-	core.schema
device	cn	serialNumber $ seeAlso $ owner $ ou $ o $ l $ description	core.schema
friendlyCountry [->country]	friendlyCountyName	-	cosine.schema
groupOfNames	member $ cn	businessCategory $ seeAlso $ owner $ ou $ o $ description	core.schema
groupOfUniqueNames	uniqueMember $ cn	businessCategory $ seeAlso $ owner $ ou $ o $ description	core.schema
inetOrgPerson [->person]	-	audio $ businessCategory $ carLicense $ departmentNumber $ displayName $ employeeNumber $ employeeType $ givenName $ homePhone $ homePostalAddress $ initials $ jpegPhoto $ labeledURI $ mail $ manager $ mobile $ o $ pager $ photo $ roomNumber $ secretary $ uid $ userCertificate $ x500uniqueIdentifier $ preferredLanguage $ userSMIMECertificate $ userPKCS12	inetorgperson.schema
organizationalPerson [->person]	-	title $ x121Address $ registeredAddress $ destinationIndicator $ preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $ telephoneNumber $ internationaliSDNNumber $ facsimileTelephoneNumber $ street $ postOfficeBox $ postalCode $ postalAddress $ physicalDeliveryOfficeName $ ou $ st $ l	core.schema
organization	o	userPassword $ searchGuide $ seeAlso $ businessCategory $ x121Address $ registeredAddress $ destinationIndicator $	core.schema

		preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $ telephoneNumber $ internationaliSDNNumber $ facsimileTelephoneNumber $ street $ postOfficeBox $ postalCode $ postalAddress $ physicalDeliveryOfficeName $ st $ l $ description	
organizationalRole	cn	x121Address $ registeredAddress $ destinationIndicator $ preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $ telephoneNumber $ internationaliSDNNumber $ facsimileTelephoneNumber $ seeAlso $ roleOccupant $ preferredDeliveryMethod $ street $ postOfficeBox $ postalCode $ postalAddress $ physicalDeliveryOfficeName $ ou $ st $ l $ description	core.schema
organizationalUnit	ou	userPassword $ searchGuide $ seeAlso $ businessCategory $ x121Address $ registeredAddress $ destinationIndicator $ preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $ telephoneNumber $ internationaliSDNNumber $ facsimileTelephoneNumber $ street $ postOfficeBox $ postalCode $ postalAddress $ physicalDeliveryOfficeName $ st $ l $ description	core.schema
person	sn $ cn	userPassword $ telephoneNumber $ seeAlso $ description	core.schema
posixAccount	cn $ uid $ uidNumber $ gidNumber $ homeDirectory	userPassword $ loginShell $ gecos $ description	nis.schema

13 Annex: Servidor DNS en ubuntu 10.10

```
# apt-get install bind9


# vi /etc/bind/named.conf.local
zone "example.com" {
      type master;
      file "/etc/bind/db.example.com";
};
# vi /etc/bind/db.example.com
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns.example.com. root.example.com. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.example.com.
ns      IN      A       192.168.0.1
ldap  IN    A     192.168.0.1

# /etc/init.d/bind9 restart
```

14 Recursos

http://tuxnetworks.blogspot.com/2010/04/ldap-client-lucid-lynx.html

http://tuxnetworks.blogspot.com/2010/06/howto-ldap-server-on-1004-lucid-lynx.html

http://www.zytrax.com/books/ldap

http://www.centos.org/docs/5/html/CDS/ag/8.0/Finding_Directory_Entries-LDAP_Search_Filters.html