# 1. DIRECTORI

Un directori és una base de dades especialitzada que emmagatzema informació sobre els recursos o les entitats que hi ha en una xarxa, com ara usuaris, ordinadors o impressores, i la posa a disposició dels usuaris de la xarxa. Un servei de directori és el programari que emmagatzema, organitza i facilita l'accés a la informació d'un directori.

Així doncs, el directori constitueix la base de dades en què s'emmagatzema la informació, mentre que el servei de directori és la infraestructura física i lògica que permet gestionar les dades del directori. L'arquitectura del servei de directori és client/servidor.

Per exemple, aquesta és una cerca que podríem fer a un directori: "Troba al directori de correus de la companyia, tota la gent que viu a Hospitalet que el seu nom sigui Xavi que tingui una adreça de correu electrònic. Retorna el seu nom complet, correu electrònic, i tipus de feina."

Els directoris compleixen aquestes característiques:

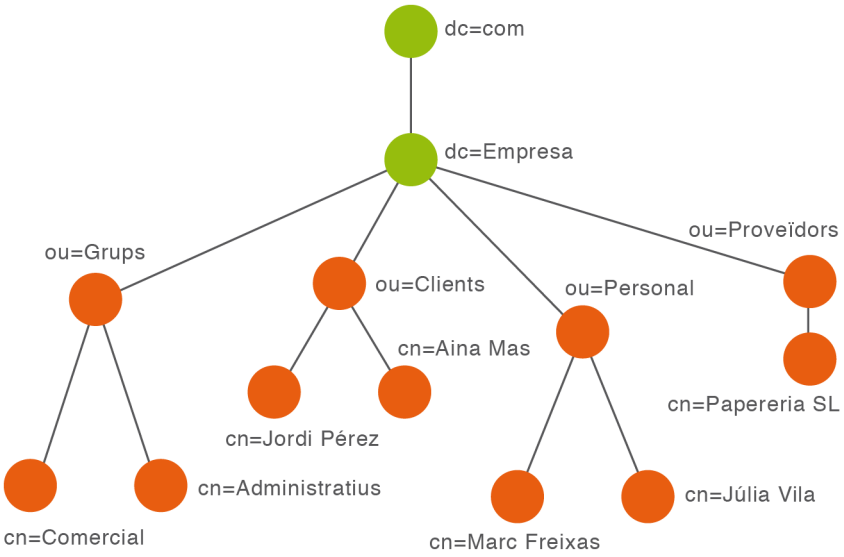
(1) La informació que contenen està basada en objectes (cada objecte és una entrada del directori) i en els atributs d'aquests objectes.

(2) Les actualitzacions i modificacions de les dades són simples i no gaire freqüents.

(3) Estan optimitzats per donar una resposta ràpida a operacions de cerca i revisió.

(4) Poden replicar la informació per augmentar-ne la disponibilitat i la fiabilitat alhora que disminueix el temps de resposta a les consultes.

(5) La informació que contenen té uns estructura jeràrquica, que fa complicat establir relacions entre diferents objectes.




exemple d'organització jeràrquica en arbre al directori

Els serveis de directori també es poden fer servir per autentificar usuaris, bé mitjançant contrasenya, bé mitjançant claus de xifratge.

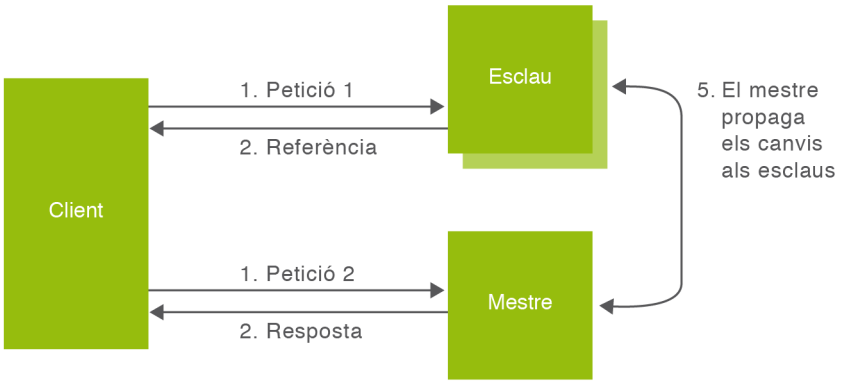
A més a més el servei de directori és el lloc natural per gestionar els certificats dels usuaris de manera còmoda.

Si totes les aplicacions susceptibles d'accedir l directori poden utilitzar-ho, la informació estarà centralitzada i sincronitzada, sense còpies per a cada aplicació, no hi haurà informació repetida ni inconsistències. Aplicacions que poden emprar el directori són, per exemple: gestors de continguts web per autentificar usuaris, sistemes de control d'entrada a oficines, serveis de correu i ftp, sistemes d'autentificació basats en RADIUS per accés a una xarxa, etc.

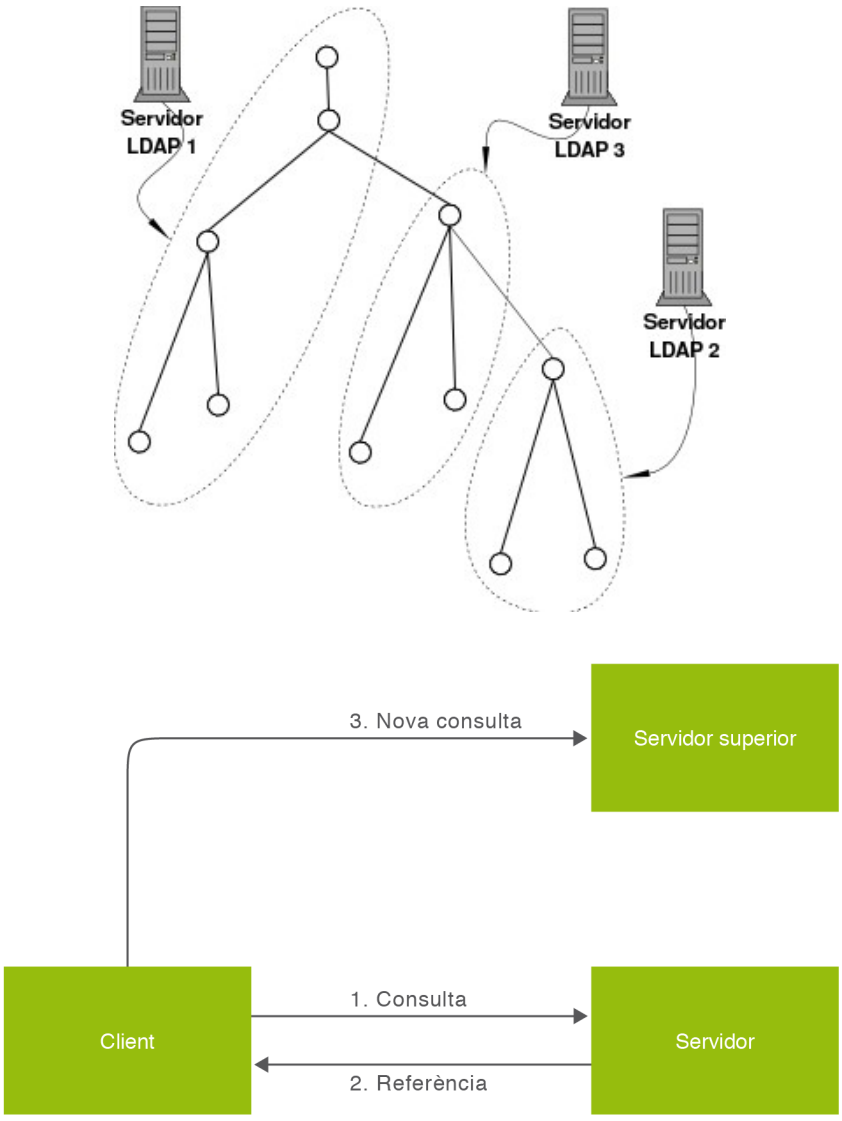
No volem que tots els usuaris consultin o modifiquin determinada informació del directori. Per això el directori tindrà les capacitats bàsiques per implementar una política de seguretat que defineix quin usuari té quin tipus d'accés sobre quina informació.

El servei de directori pot estar centralitzat o distribuït. En cas d'estar centralitzat, un únic servidor subministra tot el servei de directori i respon totes les consultes dels clients. Si el directori està distribuït, hi ha diversos servidors que proporcionen el servei de directori.

Quan el servei de directori està distribuït, les dades poden estar fraccionades o replicades. Quan la informació està fraccionada, cada servidor del servei de directori emmagatzema un subconjunt únic de la informació. És a dir, una entrada només s'emmagatzema en un servidor. Quan la informació està replicada, una entrada es pot emmagatzemar en diversos servidors. Generalment, quan el servei de directori està distribuït, una part de la informació està fraccionada i una altra part està replicada.




Servei de directori amb replicació




Servei de directori amb delegació

# 2. LDAP

El protocol LDAP (Lightweight Directory Access Protocol) és un protocol obert, estàndard i independent de venedor, per a accedir i mantenir serveis distribuïts de directori sobre xarxes IP. És un protocol binari. No especifica com guardar la informació.

Ports:

- LDAP : TCP/UDP 389
- SSL LDAP : TCP 636

La última especificació és la versió 3 (LDAPv3).

El directori LDAP destaca sobre els altres serveis de directori per les característiques següents:

- És molt ràpid en la lectura de registres.
- Permet replicar el servidor de manera molt senzilla i econòmica.
- Moltes aplicacions de tot tipus tenen interfícies de connexió amb LDAP i s'hi poden integrar fàcilment.
- Com que el protocol és independent de la plataforma, podem canviar la implementació de LDAP sense afectar la forma en que s'accedeix a les dades.
- Disposa d'un model de noms globals que assegura que totes les entrades són úniques.
- Permet múltiples directoris independents.
- Funciona sobre TCP/IP i SSL/TLS.
- La majoria de servidors LDAP són fàcils d'instal·lar, mantenir i optimitzar, encara que la configuració és una mica tediosa.

A LDAP la informació està estructurada en forma d'arbre. Aquesta estructura s'anomena directori i cada node s'anomena entrada. Per la seva part, cada entrada està formada per un conjunt d'atributs, cadascun dels quals és d'un tipus i conté un o més valors.

## 2.1 DEFINICIONS

Algunes definicions per entendre l'estructura de LDAP:

- Les **entrades** són les estructures de dades en què el directori emmagatzema i organitza la informació. La unitat bàsica d'informació emmagatzemada en el directori LDAP és l'entrada.

- Cada entrada del directori descriu un **objecte**, com ara una persona, un grup, una organització, una impressora, un servidor, etc. Per tant, els objectes són els elements del món real als quals representen les entrades del directori.

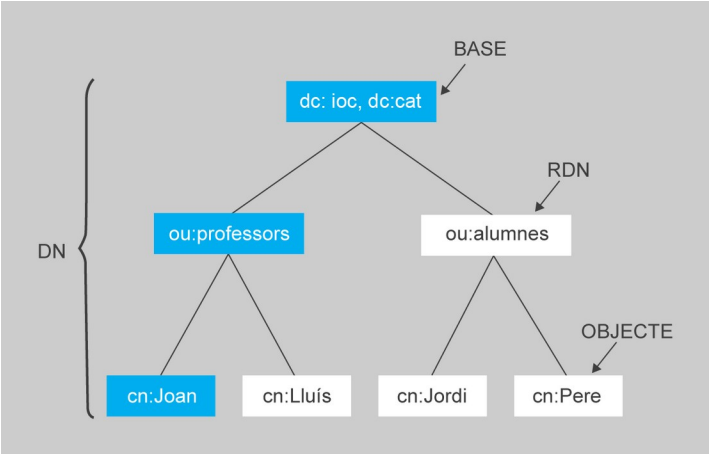
- Cadascun dels objectes o entrades té un conjunt d'**atributs**, opcionals o obligatoris, identificats amb un nom, són d'un cert tipus i poden tenir un o diversos valors associats. El tipus defineix la classe d'informació que els atributs emmagatzemen i els valors són la informació en si. Els atributs que conté una entrada estan condicionats per les classes d'objecte a les quals pertany.

- La definició dels possibles tipus d'objectes i dels atributs que els componen (incloent-hi el nom, el tipus, el valor o valors admesos i les restriccions, i com es comparen), que el directori d'un servidor LDAP pot utilitzar, la fa el servidor mateix mitjançant el denominat **esquema** (schema) del directori. Per tant, l'esquema conté les definicions dels objectes que es poden donar d'alta en el directori. El administrador del directori pot modificar esquemes i crear-ne de nous.

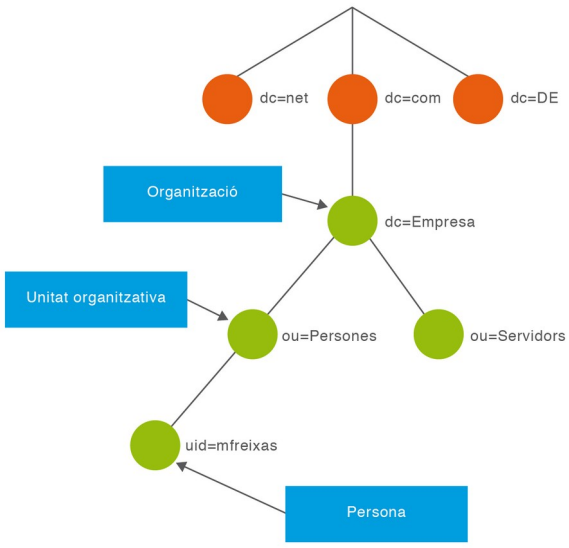
- Cada entrada té un atribut especial anomenat **distinguished name** o nom distingit (DN), que la identifica unívocament en la base de dades del directori. Aquest nom distingit pot incorporar múltiples atributs de l'objecte, com per exemple el nom i cognom de la persona, o el NIF.

- Els noms distingits relatius o **relatives distinguished names** (RDN) són les seqüències més petites que componen un nom distingit (DN). Fent metàfora amb un sistema de fitxers, el DN és el camí absolut al fitxer i el RDN és el camí relatiu.

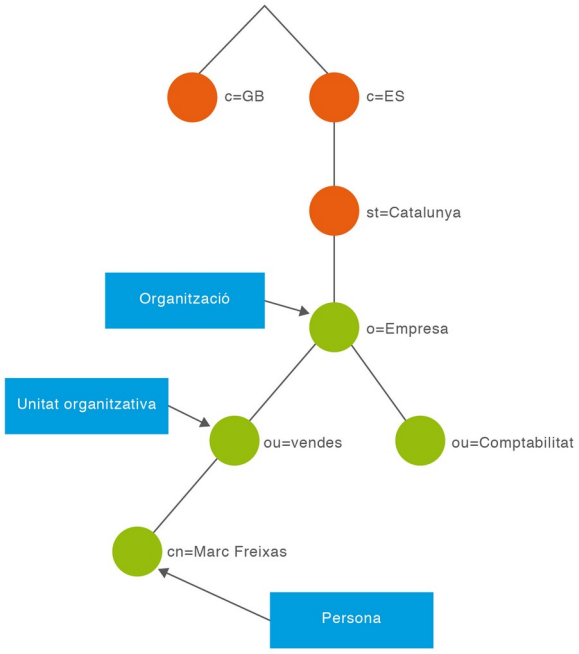
- Les entrades estan organitzades en forma d'arbre basant-se en els DN. L'arbre d'entrades de directori es coneix com a **directory information tree** o arbre d'informació del directori (DIT). Cada directori posseeix com a arrel o base la ubicació de l'organització. A partir d'aquesta base, l'arbre se subdivideix en els nodes i subnodes necessaris per tal d'estructurar de manera adequada els objectes de l'organització, objectes que se situen finalment com les fulles de l'arbre.




A l'estructura tradicional de LDAP la base està formada pel país, estat i nom de l'organització. Per exemple: o=iam, st=catalunya, c=cat . Però actualment es fa servir més l'estructura basada en DNS, on la base és el domini de l'organització. Per exemple: dc=iam, dc=cat




Organització de la base formada per DNS




Organització de la base tradicional

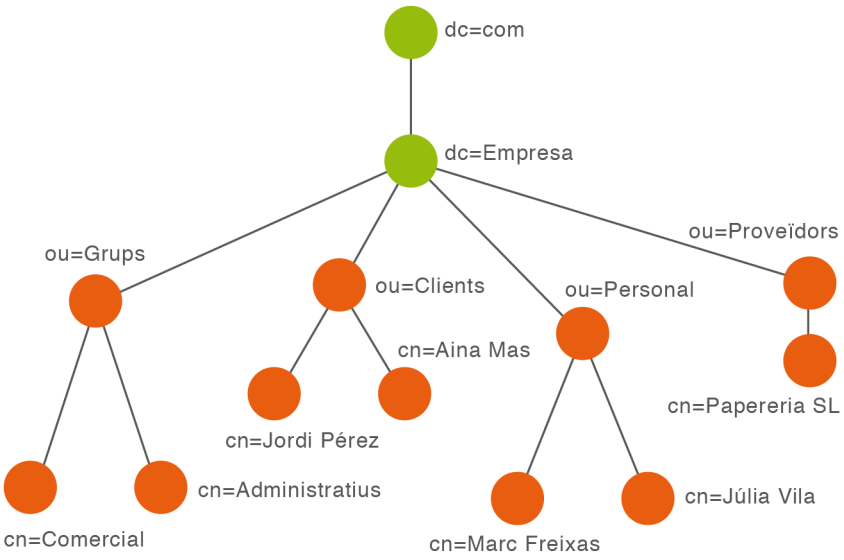
Un servidor gestiona el subarbre que comença a una entrada específica, per exemple "dc=iam,dc=cat", i els seus descendents. Els servidors també poden gestionar referències a altres servidors, de tal manera que un intent d'accedir a "ou=informatica,dc=iam,dc=cat" podria retornar una referència a un servidor que gestiona aquesta part de l'arbre de directori. D'aquesta manera el client pot llavors contactar amb aquest altre servidor. Alguns servidors també són capaços de contactar ells mateixos amb l'altre servidor per proporcionar la informació al client.

- Cal tenir en compte que una entrada pot canviar de posició dins de l'arbre i modificar el seu DN. Per això tots els objectes tenen un **universally unique identifier** (UUID) que els identifica de manera única.

- El format **LDIF** (LDAP data tnterchange format) és l'estàndard per representar les entrades del directori LDAP en format text. Cada entrada té dues parts: el DN a la primera línia, i els atributs de l'entrada. Cada atribut es compon d'un nom d'atribut, seguit del caràcter dos punts i el valor de l'atribut. Si hi ha atributs multivalorats, han de posar-se seguits. Per exemple:

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

A aquest exemple "dn" és el nom distingit de l'entrada, i no és ni un atribut ni forma part de l'entrada. "cn=John Doe" és el nom relatiu distingit de l'entrada, i "dc=example,dc=com" és el nom distingt de l'entrada pare, on "dc" significa Component del Domini. Les altres línies mostres els atributs de l'entrada. Attribute names are typically mnemonic strings, like "cn" for canonical name, "dc" for domain component, "mail" for e-mail address, and "sn" for surname.



- A LDAP es pot accedir mitjançant adreça URI (uniform resource identifier):

ldap://host:port/DN?attributes?scope?filter?extensions

Per exemple, "ldap://ldap.example.com/cn=Alex%20Castan,dc=iam,dc=cat"

## 2.2 OPERACIONS

Un client pot consultar, afegir, esborrar, modificar i reanomenar entrades del directori, així com identificar-se en el directori i controlar certs aspectes de la sessió.

Les operacions que pot sol·licitar un client al servidor LDAP són:

- Search : permet buscar en el directori les entrades que compleixen una determinada condició. Cal especificar el punt d'inici de la cerca (DN), la profunditat de la cerca (base, one o subtree), els valors que han de tenir determinats atributs, i els atributs que es retornaran.

- Compare : és similar a l'operació de cerca però si una entrada compleix la condició i no té l'atribut que es vol retornar, el directori retorna un valor especial.

- Add : permet afegir entrades noves en el directori. Com a paràmetres, rep el DN de l'entrada que cal crear i també els atributs i els valors que hi estan associats. Per poder fer aquesta operació, s'han de complir les condicions següents: (1) El node pare de l'entrada ha de ser en el directori; (2) No hi ha d'haver cap altra entrada amb el mateix DN; (3) L'entrada ha de complir els requisits especificats en l'esquema; i (4) El control d'accessos ha de permetre aquesta operació.

- Delete : permet eliminar entrades del directori. Com a paràmetres, rep el DN de l'entrada a esborrar. Per poder fer aquesta operació, s'han de complir les condicions següents: (1) L'entrada a esborrar ha de ser en el directori; (2) Aquesta entrada no pot tenir cap fill; i (3) El control d'accessos ha de permetre aquesta operació.

- Modify : permet modificar els atributs d'una entrada. Per poder executar aquesta operació, s'han de complir les condicions següents: (1) L'entrada a modificar ha d'existir; (2) L'entrada resultant s'ha d'ajustar a l'esquema; i (3) El control d'accessos ha de permetre l'actualització. Si alguna de les modificacions falla, tota l'operació d'actualització falla.

- Rename : permet modificar el DN d’una entrada. Per poder reanomenar una entrada, s’han de complir les condicions següents: (1) L’entrada a reanomenar ha d’existir; (2) No hi pot haver una entrada amb el DN nou; i (3) El control d’accessos ha de permetre aquesta operació.

- Bind : permet autenticar el client en el directori. Trobem sessions anònimes (solament tenen sentit per a operacions de cerca), sessions autenticades (amb dn d’usuari i contrasenya, en clar). i sessions xifrades (amb dn d’usuari, mètode d’autentificació i credencials).

- Unbind : tanca la connexió amb el servidor LDAP.

- Abandon : indica al servidor LDAP que el client abandona l’operació en curs.

# 3. OpenLDAP

L'OpenLDAP és una implementació de codi obert i gratuïta de l'estàndard LDAP desenvolupada pel projecte OpenLDAP ( http://www.openldap.org/ ). Altres implementacions conegudes són Oracle Directory Server, Red Hat Directory Server, Apache Directory, Microsoft Active Directory, OpenDJ i 389 Directory Server.

OpenLDAP posseeix tres components principals:

- slapd: Format pel servidor LDAP i algunes eines de gestió com slapauth, slapadd, slaptest, slapcat, etc.

- ldap-utils: Paquet que agrupa alguns programes client, com ldapsearch, ldapadd, ldapdelete o ldapmodify, entre d'altres.

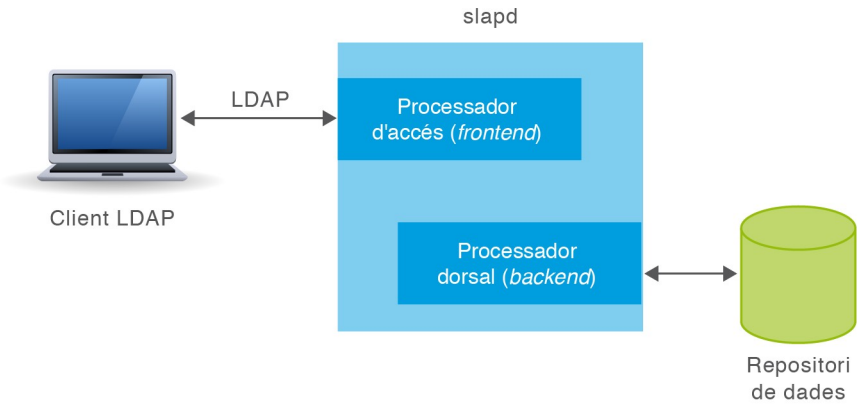
- Biblioteques que implementen el protocol LDAP, com liblber i libldap.

Historically the OpenLDAP server (slapd) architecture was split between a frontend which handles network access and protocol processing, and a backend which deals strictly with data storage. The architecture is modular and many different backends are now available for interfacing to other technologies, not just traditional databases.

Ordinarily an LDAP request is received by the frontend, decoded, and then passed to a backend for processing. When the backend completes a request, it returns a result to the frontend, which then sends the result to the LDAP client. An overlay is a piece of code that can be inserted between the

frontend and the backend. It is thus able to intercept requests and trigger other actions on them before the backend receives them, and it can also likewise act on the backend's results before they reach the frontend. Overlays have complete access to the slapd internal APIs, and so can invoke anything the frontend or other backends could perform. Multiple overlays can be used at once, forming a stack of modules between the frontend and the backend.

Overlays provide a simple means to augment the functionality of a database without requiring that an entirely new backend be written, and allow new functionalities to be added in compact, easily debuggable and maintainable modules.




Arquitectura de OpenLDAP

## 3.1 INSTAL·LACIÓ I GESTIÓ

Actualitzar les llistes de programari disponible:

```
sudo apt update
```

Instal·lar OpenLDAP:

```
sudo apt install slapd ldap-utils
```

Configurar OpenLDAP:

```
sudo dpkg-reconfigure slapd
```

Les respostes a les preguntes de configuració:

- Omit OpenLDAP server configuration? **No**
- DNS domain name? **mired.org**

- Organization name? **Ausias**
- Administrator password? **iesam38**
- Database backend? **MDB**
- Database removed when slapd is purged? **Yes** (estem fent probes i experiments)
- Move old database? **Yes**
- Allow LDAPv2 protocol? **No**

Tot i que trobaràs una carpeta amb configuració de LDAP a /etc/ldap , la configuració del servidor no està a un fitxer de configuració típic, sino que es troba a un directori dels que serveix (cn=config) i la informació es "mapeja" a fitxers LDIF dins de /etc/ldap/slapd.d/

Comprovar que funciona:

```
sudo ps -ef | grep slapd
sudo systemctl status slapd
sudo ss -tunlp | grep slapd
sudo ldapsearch -Q -Y EXTERNAL -LLL -H ldapi:// -b "cn=config" dn
sudo ldapsearch -x -LLL -H ldap:// -b "dc=mired,dc=org"
```

Instal.lar PHPLDAPAdmin per gestionar el directori des d'un navegador web remot (també instal.larà un servidor web de pàgines dinàmiques amb Apache2 i PHP):

```
sudo apt install phpldapadmin
```

Configurar PHPLDAPAdmin:

```
sudo nano /etc/phpldapadmin/config.php
```

```
  $servers->setValue('server','name','Nom que volguem');
  $servers->setValue('server','host','127.0.0.1');
  $servers->setValue('server','port',389);
  $servers->setValue('server','base',array('dc=mired,dc=org'));
  $servers->setValue('login','bind_id','cn=admin,dc=mired,dc=org');
```

En cas que volguem restringir l'accés amb PHPLDAPAdmin a algunes IPs:

```
sudo nano /etc/apache2/conf-enabled/phpldapadmin.conf
```

```
  # Order allow,deny
  # Allow from all
  Order deny,allow
  Deny from all
  Allow from 127.0.0.1 10.0.0.0/24
```

```
sudo systemctl restart apache2
```

Si has redireccionat ports a virtualbox, a la targeta de xarxa en mode NAT, per exemple del port 8000 de la màquina real al port 80 de la màquina virtual, ara pots accedir a PHPLDAPAdmin amb un navegador des de la màquina real. Prova a navegar la URL http://localhost:8000/phpldapadmin/

## 3.2 APROFUNDINT EN LA INSTAL·LACIÓ

El fitxer de configuració es troba al fitxer /usr/share/slapd/slapd.conf , però en realitat actualment gran part de la configuració es guarda dins el mateix servidor OpenLDAP i es troba «mapejada» al directori /etc/ldap/slapd.d/ en format ldif recreant un arbre de directori.

Dins d'aquest fitxer /usr/share/slapd/slapd.conf temps abans hom podia trobar la configuració d'accés administratiu al directori:

```
database    mdb
suffix      "dc=mired,dc=org"
rootdn      "cn=admin,dc=mired,dc=org"
rootpw
secret
```

També es podien trobar les llistes de control d'accés (ACL) que controlen quins usuaris poden accedir a quina informació i amb quins permisos.

Exemple 1: Permite a usuarios autentificados cambiar contraseña, a los no autentificados autentificarse, y no muestra la contraseña a ningún usuario

```
access to attr=userPassword
       by self                 write
       by anonymous            auth
       by *
```

Exemple 2: Permite a usuarios autentificados cambiar sus datos, a los no autentificados o a los que se conectan de la IP 10.0.0.* leer los datos de todos los usuarios, y nada al resto

```
access to *
       by self                 write
       by users                read
       by peername=10.0.0.*    read
       by *                    none
```

També a aquest fitxer es pot configurar la replicació amb un servidor mestre i un o més esclaus. Cal, però, instal·lar el dimoni slurpd que s'encarrega de les replicacions. En cas de configurar el mestre, al fitxer escriuríem per a cada esclau unes línies com aquestes:

```
replogfile /opt/openldap/var/openldap-slurp/replica/slurpd.replog
replica host=nom_esclau.mired.org
        bindmethod=simple
```

```
          binddn="cn=admin,dc=mired,dc=org"
          credentials=secret
```

Mentre que si estem a l'esclau, al fitxer de configuració escriuríem unes línies com aquestes:

```
  updateref ldap://nom_mestre.mired.org:389
  updatedn "cn=admin,dc=mired,dc=org"
```

## 3.3 BACKUPS I RECUPERACIÓ

No se realizan backups "en caliente" del servidor OpenLDAP. El método de backup más común es programar un script que a determinada hora:

* Para el servidor de LDAP (slapd y slurpd).

* Hace una copia de la base de datos y la configuración.

* Comprime la copia y la deja en un punto accesible por nuestro programa de backup.

* Arranca el servidor y comprueba que todo funciona correctamente.

Para recuperar un servidor basta con:

* Instalar la misma versión de OpenLDAP que el servidor que ha fallado

* Copiar la base de datos y el archivo de configuración

* Arrancar el servidor

## 3.4 EXERCICIS

Exercici 1: Crear l'organització

```
 nano ldif1.ldif
```

```
  dn: dc=setec,dc=com
  objectclass: dcObject
  objectclass: organization
  o: Setec Astronomy
  dc: setec
```

```
  dn: cn=root,dc=setec,dc=com
  objectclass: organizationalRole
  cn: root
```

```
 ldapadd -x -D "cn=root,dc=setec,dc=com" -W -f ldif1.ldif
```

```
ldapsearch -x -b 'dc=setec,dc=com' '(objectclass=*)'
```

Exercici 2: Crear les seus

```
nano ldif2.ldif
```

```
dn: ou=es,dc=setec,dc=com
ou: es
description: Sede en Espana
objectclass: organizationalunit

dn: ou=pt,dc=setec,dc=com
ou: pt
description: Sede en Portugal
objectclass: organizationalunit

dn: ou=us,dc=setec,dc=com
ou: us
description: Sede en USA
objectclass: organizationalunit

dn: ou=mad,ou=es,dc=setec,dc=com
ou: mad
description: Sede en Madrid (Spain)
objectclass: organizationalunit

dn: ou=bcn,ou=es,dc=setec,dc=com
ou: bcn
description: Sede en Barcelona (Spain)
objectclass: organizationalunit

dn: ou=lis,ou=pt,dc=setec,dc=com
ou: lis
description: Sede en Lisboa (Portugal)
objectclass: organizationalunit

dn: ou=ny,ou=us,dc=setec,dc=com
ou: ny
description: Sede en New York (USA)
objectclass: organizationalunit

dn: ou=sfo,ou=us,dc=setec,dc=com
ou: sfo
description: Sede en San Francisco (USA)
objectclass: organizationalunit

dn: ou=bos,ou=us,dc=setec,dc=com
ou: bos
description: Sede en Boston (USA)
objectclass: organizationalunit
```

```
ldapadd -x -D "cn=root,dc=setec,dc=com" -W -f ldif2.ldif
ldapsearch -x -b 'dc=setec,dc=com' '(objectclass=*)'
```

Exercici 3: Crear les persones

```
nano ldif3.ldif
```

```
dn: uid=jmsuarez,ou=mad,ou=es,dc=setec,dc=com
uid: jmsuarez
cn: Jose Manuel
sn: Manuel
objectclass: top
objectclass: person
objectclass: posixaccount
loginshell: /bin/bash
uidnumber: 99
gidnumber: 99
homedirectory: /home/jmsuarez
userpassword: secret1
```

```
dn: uid=msilva,ou=lis,ou=pt,dc=setec,dc=com
uid: msilva
cn: Mauro
sn: Silva
objectclass: top
objectclass: person
objectclass: posixaccount
loginshell: /bin/bash
uidnumber: 100
gidnumber: 100
homedirectory: /home/msilva
userpassword: secret2
```

```
dn: uid=jsmith,ou=ny,ou=us,dc=setec,dc=com
uid: jsmith
cn: John
sn: Smith
objectclass: top
objectclass: person
objectclass: posixaccount
loginshell: /bin/bash
uidnumber: 102
gidnumber: 102
homedirectory: /home/jsmith
userpassword: secret3
```

```
ldapadd -x -D "cn=root,dc=setec,dc=com" -W -f ldif3.ldif
ldapsearch -x -b 'dc=setec,dc=com' uid=jmsuarez
ldapsearch -x -b 'dc=setec,dc=com' uid=msilva
ldapsearch -x -b 'dc=setec,dc=com' uid=jsmith
```

Exercici 4: SETEC ha abierto una nueva sucursal en Londres, añádela al directorio.

Exercici 5: A partir del directorio creado para la empresa SETEC crea un nuevo usuario ficticio en la sede de Lisboa.

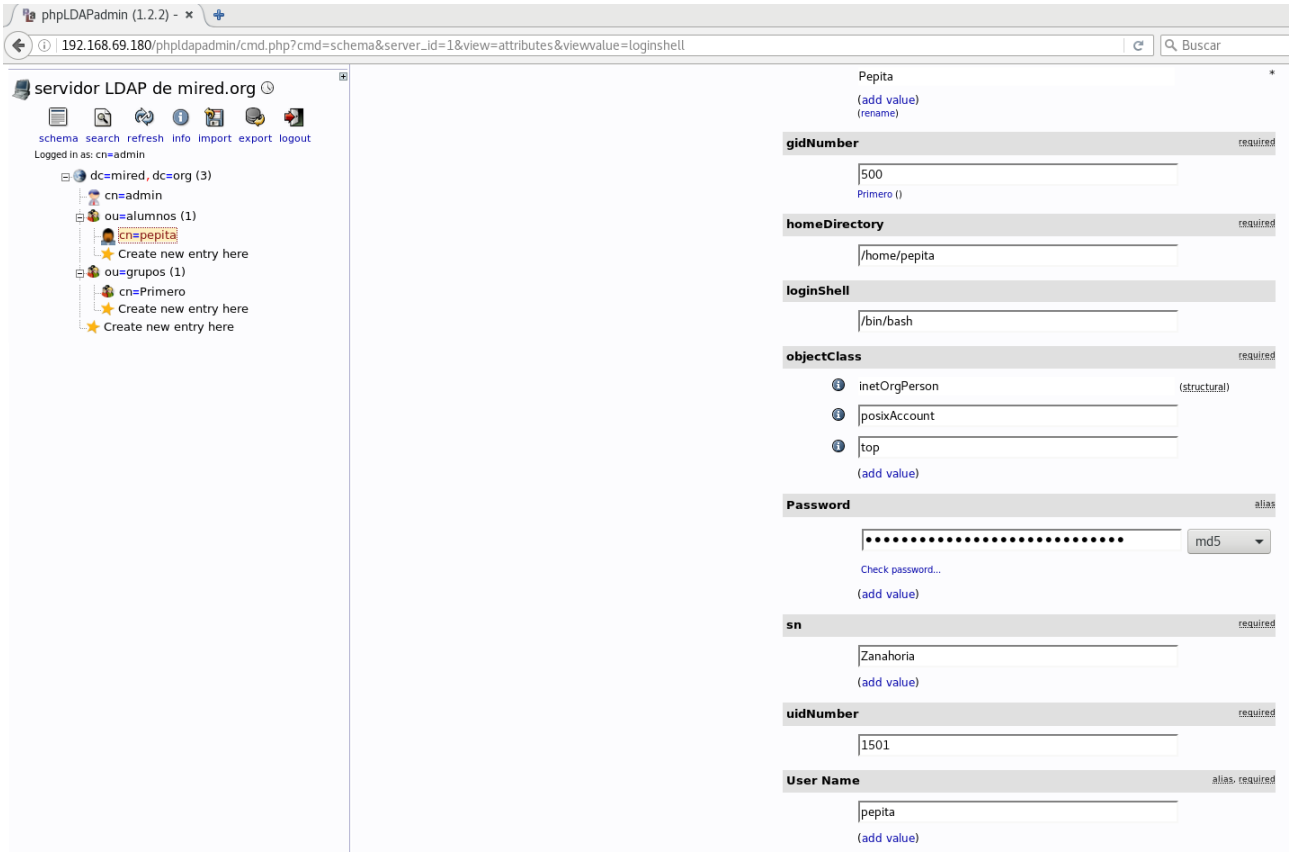
Exercici 6: Al usuario que acabas de crear modifícale el apellido (campo sn).

Exercici 7: Borra el campo apellido del usuario que acabas de crear.

Exercici 8: Borra del directorio al usuario que acabas de crear.

## 3.5 AUTENTIFICACIÓ CONTRA LDAP

Creem un grup («posix group») i un usuari («posix account») en el servidor LDAP. En aquesta pantalla d'exemple, he creat una unitat organitzativa pels grups i una unitat organitzativa pels usuaris. Primer, a la unitat organitzativa de grups he afegit el grup «primero» amb gid 500, i després a la unitat organitzativa de persones he afegit l'usuari «pepita» amb uid 1501 i gid 500.




Incís: En cas que calgués importar els usuaris del sistema a LDAP ho podem fer amb les eines del paquet *migrationtools*. Caldrà editar el fitxer resultat per deixar només els usuaris que ens interessin.

```
sudo apt install migrationtools
```

```
cp /etc/passwd ~/passwd2
nano ~/passwd2
/usr/share/migrationtools/migrate_passwd.pl ~/passwd2 ~/usuaris.ldif
nano ~/usuaris.ldif
```

I a continuació importem aquest fitxer ldif al servidor mitjançant phpLDAPadmin.

A continuació cal configurar el Name Service Switch (NSS), que permet especificar com ens autentificarem al sistema, mitjançant el fitxer /etc/nsswitch.conf. Això es configura **als clients**.

Primer cal instal·lar als clients el paquet que permet a NSS treballar amb LDAP

```
sudo apt install libnss-ldap libpam-ldap
```

Les respostes a les preguntes de configuració:

- servidor OpenLDAP que emprem? **ldap://*IP_del_servidor_LDAP***
- DN de la base del directori? **dc=mired,dc=org**
- Versió de LDAP a emprar? **versió 3**
- Aplicacions que canvien claus mitjançant PAM es comportaran de manera local? **sí**
- Autentificar-se per accedir al directori? **no**
- Administrador del servidor LDAP? **cn=admin,dc=mired,dc=org**
- Contrasenya de l'administrador del servidor LDAP? i**esam38**

Aneu amb compte perquè aquesta contrasenya s'emmagatzema en clar en el client al fitxer /etc/ldap.secret , que és només de lectura per root.

- Mode de xifrat de les contrasenyes? **Exop o crypt, però no md5 (opció per defecte)**
- Perfils PAM a habilitar? **Unix** i **LDAP**

Si volem fer canvis a aquestes dades que hem introduït, o per verificar les respostes, podem modificar el fitxer /etc/ldap.conf , o podem executar:

```
sudo dpkg-reconfigure ldap-auth-config
```

En el nostre cas **segurament ho haurem de fer**, ja que si no ens ha preguntat el mode per xifrar les contrasenyes, el mode escollit per defecte (md5) no ens permetrà autenticar els usuaris de LDAP.

Ara cal modificar el fitxer /etc/nsswitch.conf per afegir l'autentificació amb LDAP:

```
sudo nano /etc/nsswitch.conf
```

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

El que hem escrit especifica que el client faci l'autentificació local i, si no troba l'usuari, que provi l'autentificació contra el servidor LDAP. Ara cal provar que funciona. Per això escrivim la següent comanda per a llistar tots els usuaris del sistema, tant els locals com els de LDAP:

```
sudo getent passwd
```

```
   ...
   ausias:×:1000:1000:Institut Ausias March,,,:/home/ausias:/bin/bash
   pepita:*:1501:500:Pepita:/home/pepita:
```

```
sudo getent group
```

```
   ...
   Primero:*:500:
```

En el meu cas, mirant el resultat comprovo que:

* Al meu usuari Pepita li falta la línia de comandes /bin/bash. Això no li deixarà iniciar sessió. Amb *phpLDAPadmin* puc afegir a l'objecte un atribut *loginShell*.

* L'usuari Pepita no té una carpeta «home» creada. Això no li deixarà iniciar sessió. Podem afegir una línia al fitxer /etc/pam.d/common-session que crei automàticament la carpeta quan un usuari inici sessió per primer cop i no en tingui «home»:

```
sudo nano /etc/pam.d/common-session
```

```
   session required pam_mkhomedir.so skel=/etc/skel umask=0022
```

* Si combino autentificació local amb autentificació remota, per si de cas intentaré que els usuaris i grups que crei a LDAP no tinguin ni noms ni identificadors numèrics similars als locals.

Fem els canvis pertinents i tornem a repetir les proves:

```
sudo getent passwd
```

```
   ...
   ausias:×:1000:1000:Institut Ausias March,,,:/home/ausias:/bin/bash
   pepita:*:1501:500:Pepita:/home/pepita:/bin/bash
```

```
sudo getent group
```

```
   ...
   Primero:*:500:
```

```
id
```

```
id pepita
```

```
su pepita
```

```
passwd
```

Si tot ha anat bé ens ha deixat iniciar sessió, però no ens ha deixat canviar la contrasenya. Per solucionar-ho al fitxer /etc/pam.d/common-passwd a la línia que parla de l'autentificació LDAP traiem la paraula «use_authtok»:

```
sudo nano /etc/pam.d/common-passwd
```

```
   password   [...el que hi hagi...]   pam_ldap.so try_first_pass
```

Comproveu que podeu tancar la sessió d'escriptori i obrir una sessió d'escriptori amb l'usuari creat a LDAP i amb la contrasenya canviada. Si alguna cosa falla pot ser útil consultar els logs al client:

```
sudo cat /var/log/auth.log
```

```
sudo cat /var/log/syslog
```

Heu de saber algunes coses addicionals:

(1) A més de configurar NSS ha quedat configurat PAM, que és el conjunt de llibreries que indiquen a les aplicacions com autentificar usuaris i accedir a la seva informació. Aplicacions com *ssh* i *ftp*, comandes com *su* i *passwd*, etc. necessiten accedir a la informació dels usuaris. Els fitxers de configuració de PAM estan a /etc/pam.d/ i hi ha alguns fitxers que hauríem de conèixer i **comprovar que ara utilitzen LDAP**:

/etc/pam.d/common-auth : utilitzat per les aplicacions i serveis per autenticar usuaris.

/etc/pam.d/common-account : utilitzat per poder accedir a les dades d'un compte, però també per permetre o restringir l'accés d'un usuari donats determinats criteris.

/etc/pam.d/common-password : utilitzat per canviar la contrasenya de l'usuari.

/etc/pam.d/common-session : utilitzat per poder iniciar o tancar una sessió.

/etc/pam.d/... : la resta de fitxers són per a cada aplicació o servei específic.

(2) Ara també podem configurar qualsevol servei (ftp, correu electrònic) i qualsevol gestor de contingut (Moodle, Joomla, Wordpress, ...) per a que faci l'autentificació dels seus usuaris a través del nostre servidor OpenLDAP.

(3) En cas que volem especificar que només una part del directori conté la informació de configuració, podem especificar al fitxer /etc/libnss-ldap.conf a quines unitats organitzatives es troben els usuaris i els grups afegint un parell de línies:

```
sudo nano /etc/libnss-ldap.conf
```

```
nss_base_password    ou=alumnos,dc=mired,dc=org
nss_base_group       ou=grupos,dc=mired,dc=org
```

(4) Tocant fitxers de configuració es poden afegir restriccions a l'accés d'usuaris, però queda fora de temari.

(5) Podeu agilitzar l'accés al directori i augmentar el rendiment instal·lant el «Name Service Cache Daemon» (paquet «ncsd») , però queda fora de temari.