

Sistemes Informàtics

UD13. Part 2. GNU_Linux. Ubuntu. Instal·lació i configuració d'OpenLDAP.



ÍNDEX

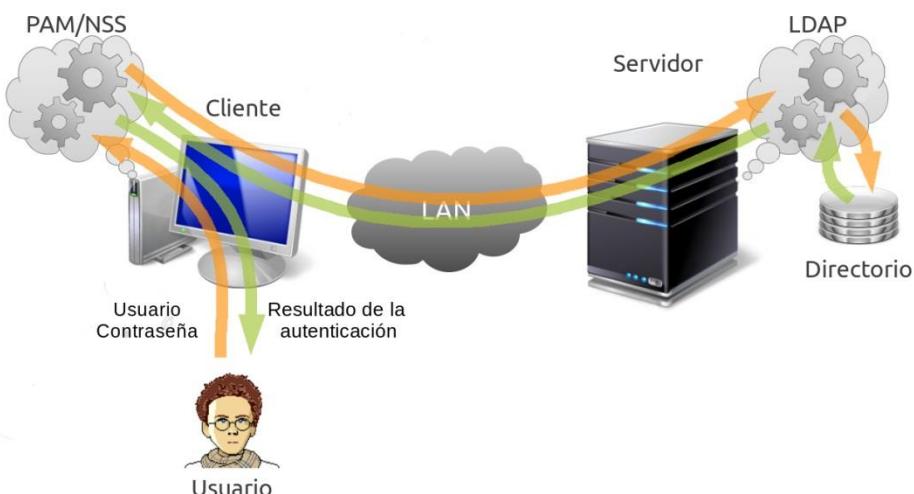
1.	Introducció.....	3
2.	Què és NSS?.....	3
3.	Què és PAM?	4
4.	Què és LDAP?.....	4
5.	Què és OpenLDAP?.....	5
6.	Com funcionen LDAP I OPENLDAP?.....	5
7.	Instal·lar OPENLDAP en EL SERVIDOR Ubuntu	7
7.1.	Configuracions prèvies.....	7
7.2.	Instal·lar el programari necessari	8
8.	Crear l'estructura del directori	9
9.	Afegir usuaris i grups de manera manual.....	11
9.1.	Afegir un usuari.....	11
9.2.	Afegir un grup	12
9.3.	Comprovar que tot és correcte.....	13
10.	Buscar, modificar i eliminar elements del directori	14
10.1.	Buscar elements del directori	14
10.2.	Modificar entrades del directori	15
10.3.	Esborrar entrades del directori.....	16
11.	Importar els usuaris i grups locals en el servidor OpenLDAP.....	17
11.1.	Importar usuaris locals al directori OpenLDAP	17
11.2.	Importar grups locals al directori OpenLDAP	21
12.	Configurar un equip client amb Ubuntu per a autenticar-s'en el servidor OpenLDAP	24
12.1.	Instal·lar els paquets necessaris	24
12.2.	Realitzar ajustos en els arxius de configuració	27
12.3.	Comprovar que funciona l'inici de sessió	30
13.	Iniciar sessió gràfica en l'equip client amb un usuari LDAP	31
14.	Instal·lar i configurar la interfície web LDAP Account Manager per a administrar OpenLDAP	32
14.1.	Instal·lació de LDAP Account Manager	32
14.2.	Realitzar ajustos previs	33
15.	Usar LDAP Account Manager per a gestionar usuaris i grups en el servidor OpenLDAP	41
15.1.	Comptes d'usuari	41
15.2.	Comptes de grups	43
16.	Perfils mòbils d'usuari usant NFS i LDAP	45
16.1.	Crear una carpeta per a guardar els perfils mòbils en el servidor.....	45
16.2.	Exportar el contingut de la carpeta que tindrà els perfils mòbils	45
16.3.	Crear una carpeta per a guardar els perfils mòbils en cada client	47
16.4.	Modificar l'arxiu /etc/fstab en cada client per a muntar la carpeta en l'arrancada	47
16.5.	Indicar en l'usuari LDAP la carpeta on tindrà el seu perfil en el client	47
16.6.	Comprovar que la configuració funciona correctament	48
17.	Errors tipicos en instal·lar openldap	50

1. INTRODUCCIÓ

Existeixen diferents maneres d'autenticar **clients en una xarxa GNU/Linux**, però una dels més usades és la combinació de tres eines diferents: **PAM, NSS i LDAP**.

La idea consisteix a disposar d'un **servidor** que facilite l'autenticació **dels clients**, de manera que aquests recorreguen al servidor cada vegada que un client necessite identificar-se. D'aquesta manera, el **compte d'usuari** no és específic d'un equip client, sinó que serà **vàlid en qualsevol equip de la xarxa** que haja sigut degudament configurat.

De fet, aquest és el mètode que sol utilitzar-se en *GNU/Linux* per a obtindre una gestió d'usuaris globals similar a la que ofereixen els *Servidors Windows* a través d'una estructura de dominis.



En aquest tema aprendrem la funció de cadascun dels components, tant de manera individual com combinat amb els altres. Després, veurem com realitzar la instal·lació i configuració de l'estructura que hem il·lustrat en la imatge anterior.

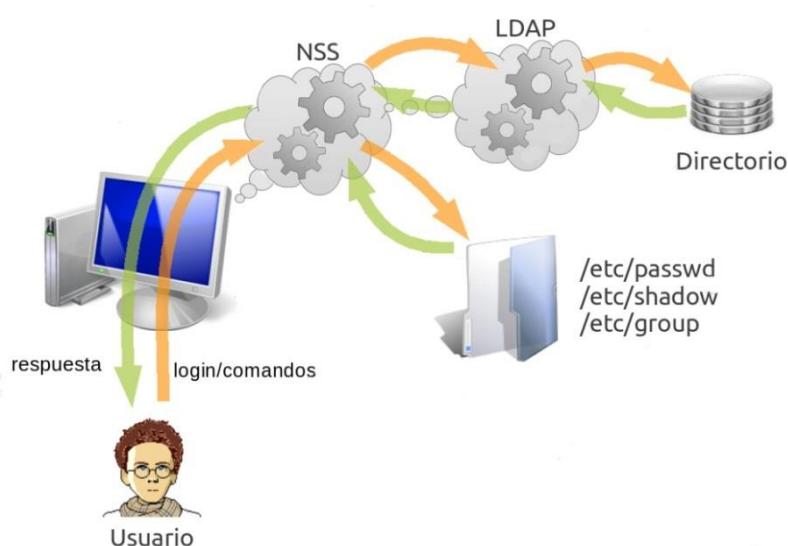
A manera de resum, **LDAP** ho instal·larem en el **serveidor**, mentre que **NSS i PAM** s'instal·laran en els equips **client**. **LDAP** ofereix l'accés al servei de directori, **NSS** s'encarrega de **buscar i obtindre de LDAP la informació administrativa dels usuaris** (Informació dels comptes d'usuari, dels grups, informació de la màquina...) i **PAM** s'encarrega de l'autenticació amb **LDAP**, l'inici de sessió i la seu configuració.

2. QUÈ ÉS NSS?

NSS (Nestime Service Switch) és un **servei que permet la resolució de noms d'usuari i contrasenyes** (o grups) mitjançant l'accés a **diferents orígens d'informació**. En condicions normals, aquesta informació és troba en els arxius locals del sistema operatiu, en concret en */etc/passwd*, */etc/shadow* i */etc/group*, però pot procedir d'altres fonts, com *DNS (Domain Name System)*, *NIS (Network Information Service)*, *LDAP (Lightweight Directory Access Protocol)* o *WINS (Windows Internet Name Service)*.

Sun Microsystems va ser el primer a desenvolupar *NSS* d'una forma molt semblant a com ho coneixem en l'actualitat. Per tant, el primer sistema operatiu que va incorporar *NSS* va ser *Solaris*. Poc després, es va portar a diferents sistemes operatius, com *AIX*, *NetBSD*, *FreeBSD* o *GNU/Linux*.

L'objectiu de **NSS** és que els **programes** o els **comandos** del sistema operatiu puguen **manejjar informació administrativa relacionada amb els usuaris, els contrasenyes i els grups** (inclosos aspectes com la caducitat d'una contrasenya o el seu nivell de complexitat) **sense haver de conéixer el lloc on és troben emmagatzemats**.



3. QUÈ ÉS PAM?

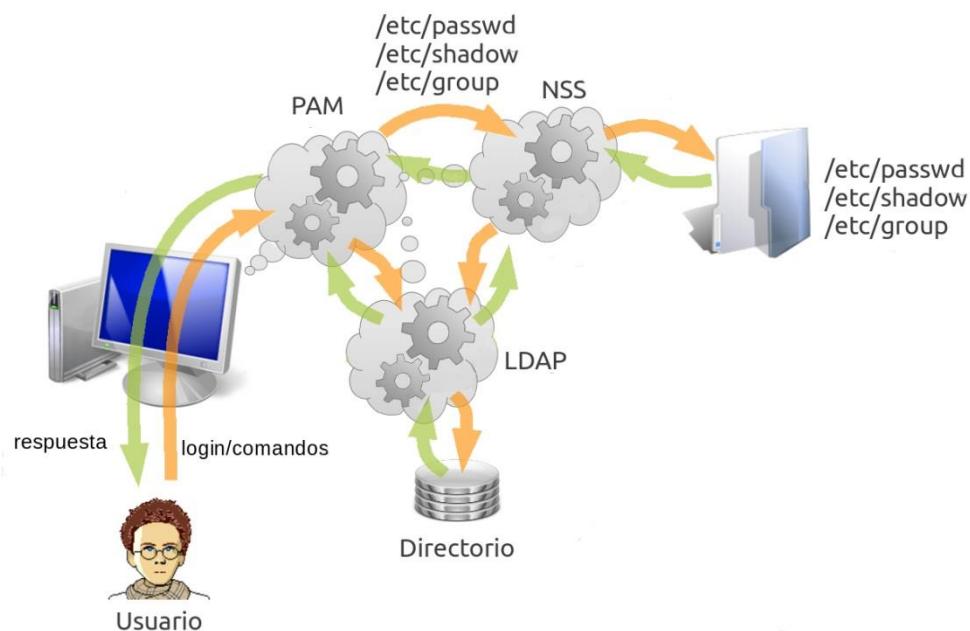
PAM (*Pluggable Authentication Modules*) estableix una **interfície entre els programes d'usuari i diferents mètodes d'autenticació**. D'aquesta manera, el mètode d'autenticació és fa **transparent per als programes**.

Com va ocórrer amb NSS, PAM va sorgir en *Sun Microsystems*, encara que, en aquest cas, com una proposta a Open Programari Foundation. Va ser Red Hat qui ho va desenvolupar com una eina de Programari lliure i ho va incorporar per primera vegada a la versió 3.0.4 del seu sistema operatiu en 1996.

La idea és basa en la creació de mòduls d'autenticació reemplaçables, de manera que seguísca transparent per al sistema l'ús de diferents mètodes d'autenticació. Això fa que, sense realitzar modificacions en el sistema, puguem utilitzar mètodes que vagen dones de l'ús típic d'un nom d'usuari i una contrasenya, fins a dispositius que faciliten la identificació biomètrica dels usuaris (lectors de petjades, de veu, d'imatge, etc.). Fins i tot incorpora opcions per a acceptar contrasenyes d'un sol ús, restringir l'accés a determinats horaris o establir polítiques d'autenticació específiques per a cada usuari o grups d'usuaris.

Bàsicament, **PAM complementa en alguns aspectes el funcionament de NSS** ja que mentre aquest se centra en la cerca i mapatge dels usuaris, PAM controla l'autenticació, l'inici de sessió i la seu configuració.

En l'actualitat, PAM és el mètode que utilitzen la majoria dels aplicacions i eines de GNU/Linux que necessiten relacionar-se, d'alguna manera, amb l'autenticació dels usuaris.



4. QUÈ ÉS LDAP?

LDAP és un **protocol** que ofereix l'accés a **un servei de directori** implementat sobre un entorn de xarxa, a fi d'accedir a una determinada informació. Pot executar-se sobre TCP/IP o sobre qualsevol altre servei de transferència orientat a la connexió.

LDAP són els sigles en anglès de Lightweight Directory Access Protocol (*Protocol Lleuger d'Accés a Directoris*) i podem considerar-ho com un **sistema d'emmagatzematge de xarxa** (normalment construït com una **base de dades**) al qual **és poden realitzar consultes**.

El protocol LDAP és va crear originalment en la Universitat de Michigan, que va publicar un primer desenvolupament en 1993. Més tard, Tim Howes i Steve Killela, dues dels dissenyadors originals del projecte comencen a treballar en una nova versió sota els auspícis de IETF (*Internet Engineering Task Force*) completant el desenvolupament original. La nova versió (*LDAPv3*) és va publicar en 1997 i integrava mecanismes d'autenticació senzilla i capa de seguretat. Després d'això, la IETF ha afegit nombroses extensions i especificacions pròpies que li han anat incorporant noves capacitats.

5. QUÈ ÉS OPENLDAP?

La resposta és molt senzilla: **OpenLDAP** és un **desenvolupament del protocol LDAP**, implementat amb la filosofia del **programari lliure i codi obert**.

El projecte *OpenLDAP* és va iniciar a l'agost de 1998 i està sustentat per una entitat sense ànim de lucre anomenada *OpenLDAP Foundation*, creada pel desenvolupador estatunidenc Kurt D. Zeilenga per a coordinar els activitats del projecte.

OpenLDAP és publica sota la seuva pròpia llicència *OpenLDAP Public License* (<http://www.openldap.org/software/release/license.html>)



Com ocorria en el cas de *LDAP*, *OpenLDAP* està molt **optimitzat** per a oferir els millors resultats en situacions que requerisquen **operacions de lectura intensives**. D'aquesta manera, un directori *OpenLDAP* llançarà uns resultats molt superiors als que ofereix una base de dades relacional optimitzada, quan realitzem operacions de consulta intensives sobre ambdues. Per contra, si utilitzarem un directori *OpenLDAP* per a guardar dades que segueixen actualitzats de manera freqüent, els resultats obtinguts serien molt inferiors als oferits per una base de dades relacional.

No sols podem trobar *OpenLDAP* en la majoria dels distribucions Linux, sinó que també ho trobem per a Microsoft Windows, Apple OSX, Solaris, HP-UX, BSD, etc.

6. COMO FUNCIONEN LDAP I OPENLDAP?

El model d'informació de *LDAP* és basa en **entrades**, entenent per entrada un **conjunt d'atributs** identificats per un **nom global únic** (Distinguished Name – **DN**), que s'utilitza per a **identificar-la de manera específica**. Els entrades s'**organitzen de manera lògica i jeràrquica** mitjançant un **esquema de directori**, que vaig comptar la **definició dels objectes que poden formar part del directori**.

Cada entrada del directori representa un **objecte**, que pot ser abstracte o real: una persona, un moble o una funció en l'estruccura d'una empresa, etc.

Cada atribut d'una entrada tindrà un **tipus** i un **valor** amb el format *atribut/valor* que permet caracteritzar un aspecte de l'objecte que defineix l'entrada. Aquests atributs tenen noms que fan referència al seu contingut i poden ser de dues tipus:

- **Atributs normals:** Són els atributs que identifiquen a l'objecte (nom, cognoms, etc.).
- **Atributs operatius:** Són els atributs que utilitza el servidor per a administrar el directori (data de creació, grandària, etc.).

Els **entrades** s'indexen mitjançant el **nom complet (dn)**, que facilita la identificació singular a cada element de l'arbre. El nom complet és formarà amb una sèrie de parells *atribut/valor*, separats per menges, que reflecteixen la ruta inversa dones de la posició lògica de l'objecte fins a l'arrel de l'arbre.

Per a referir-se al nom complet solem utilitzar-se's sigles RDN, que provenen de l'anglés *Relative Distinguished Name*.

Entre els atributs que solem emprar-se habitualment, trobem els següents, encara que pot haver-hi molts més:

- **uid** (user aneu): Identificació única de l'entrada en l'arbre.
- **objectClass**: Indica el tipus d'objecte al qual pertany l'entrada.
- **cn (common name)**: Nom de la persona representada en l'objecte.
- **givenname**: Nom de pila.
- **sn (surname)**: Cognom de la persona.
- **o (organization)**: Entitat a la qual pertany la persona.
- **o (organizational unit)**: El departament en el qual treballa la persona.
- **mail**: adreça de correu electrònic de la persona.

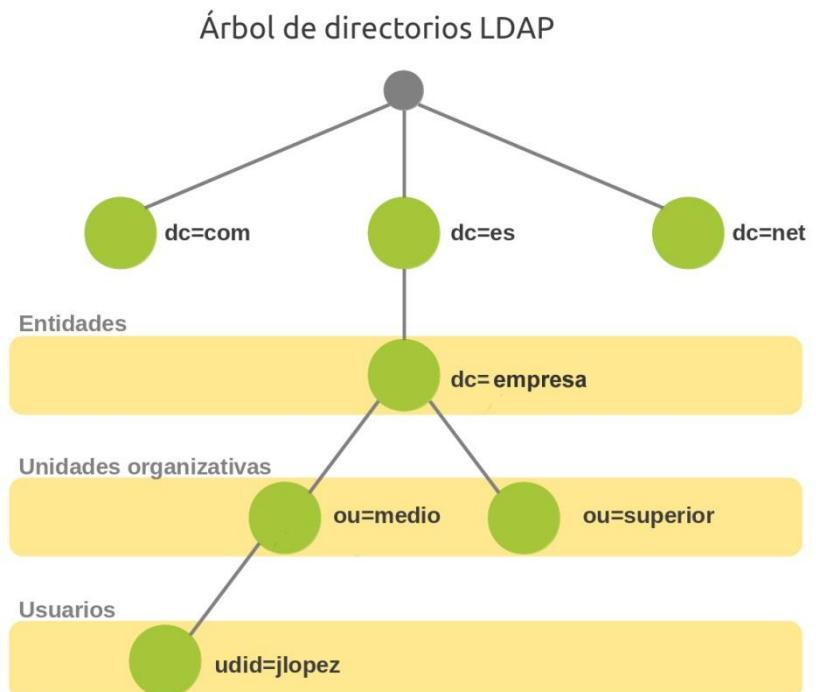
Obviament, els atributs anteriors fan referència a una mena d'objecte que representa als membres d'una empresa. Per a representar a altres tipus d'objectes, necessitaríem atributs diferents.

D'aquesta manera, una entrada emmagatzemada en el directori LDAP podria tindre el següent aspecte:

```
dn: uid=jlopez, ou=medio, dc=empresa, dc=com
objectClass: person
cn: Juan Lopez
givenname: Juan
sn: Lopez
o: empresa
ou: mitjà
mail: juanlopez@empresa.com
```

Com hem dit abans, els diferents entrades s'organitzen a manera d'arbre jeràrquic que, normalment, representa una estructura organitzativa o geogràfica en particular. Així, per exemple, els entrades que representen comunitats autònombes apareixeran en la part superior de l'arbre, davall estaran els que representen províncies, després els ciutats, els departaments, els usuaris, etc.

En l'actualitat, les **implementacions de LDAP** solen utilitzar **DNS (Domain Name Service)** per a l'estructura dels nivells superiors de l'arbre. En els nivells inferiors, no obstant això, les entrades representen un altre tipus d'unitats organitzatives, usuaris o recursos.



D'altra banda, gràcies a l'ús d'un atribut especial anomenat **objectClass**, podem controlar **quins atributs són vàlids i quins imprescindibles** en una entrada. Els **valors** d'objectClass estableixen els **regles** que ha de seguir el valor d'una entrada.

Lògicament, **LDAP** estableix **operacions** per a **consultar o actualitzar el directori**. Aquestes ens permeten **crear o eliminar entrades i modificar entrades existents**.

La major part del temps, **LDAP** s'utilitza per a diverses **consultes** sobre la informació que vaig comptar, per la qual cosa és comuna que l'estructura de la seu base de dades és trobe **optimitzada per a la lectura** en detriment de l'escriptura.

Com veiem, **LDAP** pot utilitzar-se per a organitzar de forma unificada l'accés a la informació representativa d'una xarxa. No obstant això, és molt freqüent que també emmagatzeme la **informació d'autenticació per als usuaris i/o recursos**. D'aquesta manera, és **facilita el control d'accés** sobre els dades contingudes en el servidor.

Encara que ja hem vist al principi un esquema de funcionament molt més detallat, podríem representar el funcionament de **LDAP** d'una forma més abstracta amb el següent esquema:



Finalment, **LDAP** inclou serveis d'integritat i **confidencialitat** dels dades que vaig comptar.

7. INSTAL·LAR OPENLDAP EN EL SERVIDOR UBUNTU

En aquest apartat veurem com s'instal·la OpenLDAP en un equip amb el sistema operatiu *Ubuntu LTS*. Al final del tema, també suposarem que el sistema disposa del sistema d'arxius NFS degudament instal·lat i configurat per a exportar la carpeta /home. Tanmateix, això només serà necessari quan necessitem crear perfils mòbils d'usuari en Ubuntu usant NFS i LDAP.

7.1. CONFIGURACIONS PRÈVIES

7.1.1. Configurar una IP estàtica

El primer serà assegurar-nos que el **sistema** te assignada una **adreça IP estàtica**. En el nostre cas, la IP serà la 192.168.1.200

Recorda que per a això has de modificar el fitxer /etc/netplan/01-network-manager-all.yaml

```
GNU nano 2.9.3      /etc/netplan/01-network-manager-all.yaml

# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      addresses: [192.168.1.200/24]
      gateway4: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
```

7.1.2. Configurar un nom adequat per al servidor

També canviarem el nom al servidor a "ldapserver" modificant els arxius **/etc/hostname** i **/etc/hosts**.

En el cas de **/etc/hostname**:

```
GNU nano 2.9.3      /etc/hostname

ldapserver
```

En el cas de **/etc/hosts** haurà d'incloure una línia que relate l'adreça IP estàtica del servidor amb els noms lògics que tenim previst utilitzar. L'objectiu és que, quan fem referència als noms *ldapserver* o *ldapserver.empresa.local*, el nostre sistema entenga que ens estem referint al servidor.

D'aquesta manera, modifiquem la segona línia del fitxer i escrivim:

192.168.1.200 ldapserver.empresa.local ldapserver

```
GNU nano 2.9.3      /etc/hosts

127.0.0.1      localhost
192.168.1.200  ldapserver.empresa.local  ldapserver

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

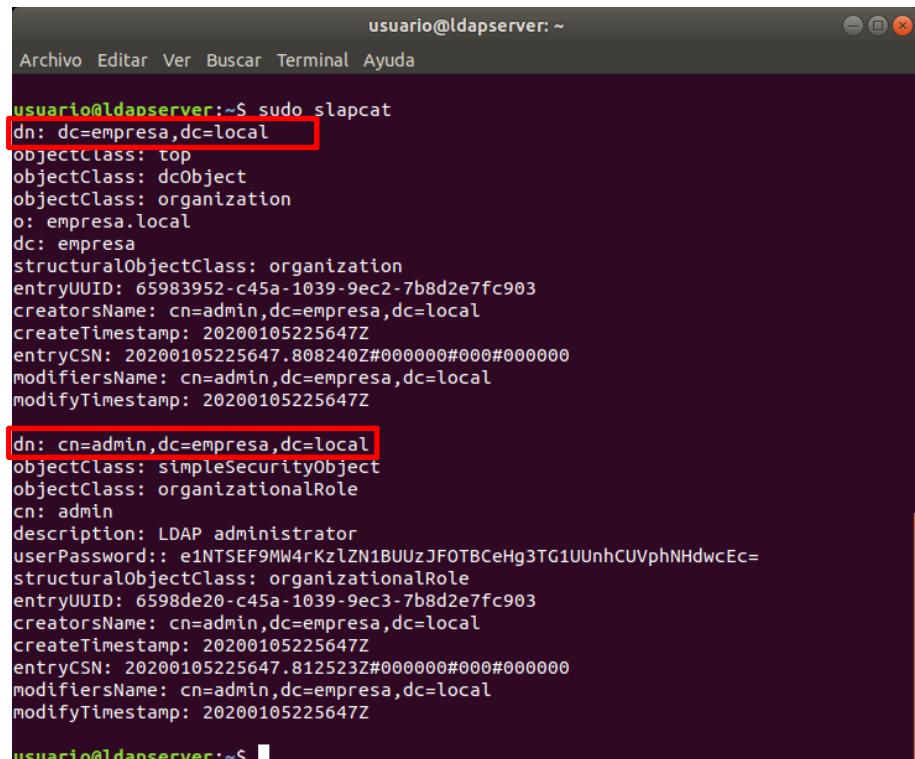
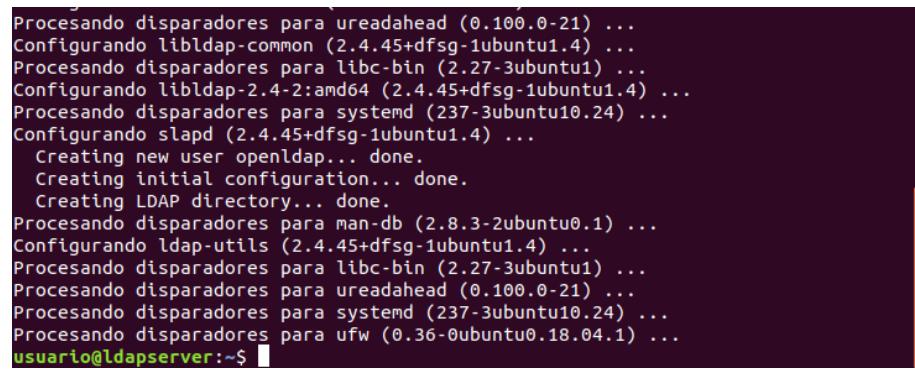
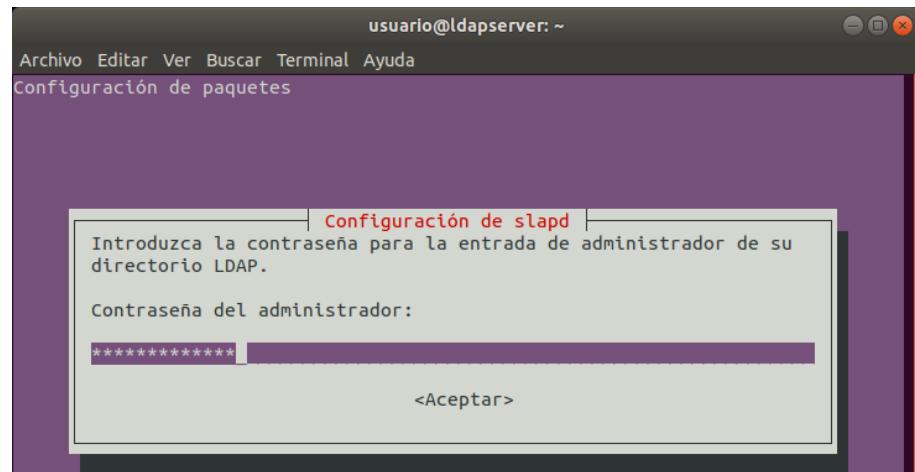
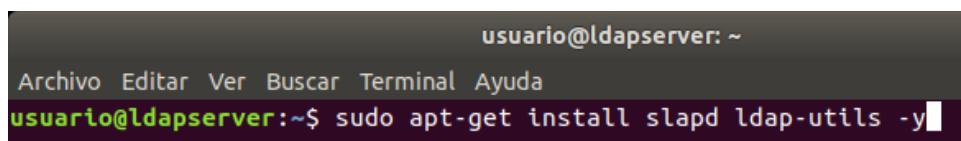
I després d'això reiniciem.

7.2. INSTAL·LAR EL PROGRAMARI NECESSARI

El procés d'instal·lació és realment senzill. Només hem d'instal·lar el paquet *slapd* i el paquet amb les utilitats d'administració de LDAP *ldap-utils*.

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

(Nota: Acabem el comando amb *-y* perquè instal·le les dependències sense preguntar-nos)



Durant la instal·lació, apareix en la consola un **missatge** que ens sol·licita la **contrasenya d'administració per a LDAP**. Com sempre, ha ser una contrasenya segura. Si consideres que la contrasenya local compleix els requisits, no hi ha cap inconvenient per a tornar a usar-la, encara que seràs la teua qui haja d'avaluar aquest aspecte en funció dels requisits de seguretat del teu entorn.

Després de tornar a escriure la contrasenya triada, tornarem a l'aspecte normal de la terminal i comprovarrem que la instal·lació segueix el seu curs.

De manera predeterminada, *slapd* és configura amb els mínimes opcions necessàries perquè el dimoni funcione de manera correcta.

Una vegada conclosa la instal·lació, podem comprovar que tot és correcte usant el comando **slapcat**. L'objectiu d'aquest comando consisteix a obtindre la informació de la base de dades LDAP i la seua eixida és produïx en format LDIF, la qual cosa ens facilitarà exportar l'estruatura del directori LDAP o, senzillament, obtindre una còpia de seguretat del seu contingut, només amb redirigir la seua eixida a un arxiu. Parlarem dels arxius LDIF més endavant.

8. CREAR L'ESTRUCTURA DEL DIRECTORI

Una vegada configurat el servidor, haurem de configurar l'estructura bàsica del directori. És a dir, crearem l'estructura jeràrquica de l'arbre (*DIT – Directory Information Tree*).

Una de les formes més senzilles d'afegir **informació al directori** és utilitzar **arxius LDIF** (LDAP Data Interchange Format). En realitat, és tracta d'arxius en text pla, però amb un format particular que hem de conéixer.

El **format bàsic** d'una **entrada** és així:

```
# comentari
dn: <nom global únic>
<atribut>: <valor>
<atribut>: <valor>
...Administració de directives de grup
```

Els línies que comencen amb un caràcter # són comentaris.

<atribut> pot ser un tipus d'atribut com *cn* o *objectClass*, o pot incloure opcions com *cn;lang_en_US* o *userCertificate;binary*.

Entre dues entrades consecutives ha d'existir sempre una línia en blanc.

Si una línia és massa llarga, podem repartir el seu contingut entre diverses, sempre que els línies de continuació comencen amb un caràcter de tabulació o un espai en blanc.

Per exemple, els següents línies són equivalents:

```
dn: uid=jlopez, ou=mitjà, dc=empresa, dc=local
      i
dn: uid=jlopez, ou=mitjà,
dc=empresa, dc=local
```

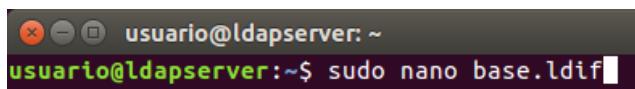
També podem assignar diversos valors a un mateix atribut utilitzant diverses línies:

```
cn: Juan Jose Lopez
cn: Juan Lopez
```

Amb aquesta informació en ment, crearem un arxiu que continga els tipus d'objecte bàsics del directori. Començarem per obrir un editor de textos, per exemple *nano*, indicant-li el nom del nostre arxiu.

Concretament, en aquest cas, l'hem anomenat *base.ldif*, però, lògicament, podràs cridar-ho com et resulte més apropiat.

```
sudo nano base.ldif
```



Una vegada obert l'editor, escriurem un contingut com aquest:

```
dn: ou=usuari,dc=empresa,dc=local
objectClass: organizationalUnit
ou: usuari

dn: ou=grups,dc=empresa,dc=local
objectClass: organizationalUnit
ou: grups
```

Lògicament, en cada lloc on apareixen els valors **dc=empresa,dc=local** haurem de substituir-los pels valors correctes en cada implementació

The screenshot shows a terminal window titled "usuario@ldapserver: ~". The title bar also displays "GNU nano 2.9.3", "base.ldif", and "Modificado". The main area of the terminal contains the following LDIF data:

```
dn: ou=usuarios,dc=empresa,dc=local
objectClass: organizationalUnit
ou: usuarios

dn: ou=grupos,dc=empresa,dc=local
objectClass: organizationalUnit
ou: grupos
```

Quan hagem acabat d'escriure-ho, només ens quedarà guardar els canvis efectuats i tancar.

A continuació, haurem d'afegir la informació a la base de dades *OpenLDAP*. Com sabem, això és fa amb el comando *ldapadd*:

```
sudo ldapadd -x -D cn=admin,dc=empresa,dc=local -W -f base.ldif
```

Per a executar el comando, haurem d'escriure la contrasenya d'administració de LDAP.

The screenshot shows a terminal window titled "usuario@ldapserver: ~". The title bar also displays "usuario@ldapserver:~\$". The main area of the terminal shows the command being run and its output:

```
usuario@ldapserver:~$ sudo ldapadd -x -D cn=admin,dc=empresa,dc=local -W -f base.ldif
Enter LDAP Password:
adding new entry "ou=usuarios,dc=empresa,dc=local"
adding new entry "ou=grupos,dc=empresa,dc=local"

usuario@ldapserver:~$
```

Després, podrem comprovar que els nous objectes s'han afegit correctament fent un slapcat:

The screenshot shows a terminal window displaying the output of the slapcat command, which lists the entries added from the base.ldif file:

```
dn: ou=usuarios,dc=empresa,dc=local
objectClass: organizationalUnit
ou: usuarios
structuralObjectClass: organizationalUnit
entryUUID: 251e0c9c-c45c-1039-9a3e-fd557943ac84
creatorsName: cn=admin,dc=empresa,dc=local
createTimestamp: 20200105230918Z
entryCSN: 20200105230918.626884Z#000000#000#000000
modifiersName: cn=admin,dc=empresa,dc=local
modifyTimestamp: 20200105230918Z

dn: ou=grupos,dc=empresa,dc=local
objectClass: organizationalUnit
ou: grupos
structuralObjectClass: organizationalUnit
entryUUID: 251ea3aa-c45c-1039-9a3f-fd557943ac84
creatorsName: cn=admin,dc=empresa,dc=local
createTimestamp: 20200105230918Z
entryCSN: 20200105230918.6307627#000000#000#000000
```

9. AFEGIR USUARIS I GRUPS DE MANERA MANUAL

El mètode per a afegir nous usuaris i grups a l'arbre és molt similar al vist en el punt anterior, ja que consisteix a crear un nou arxiu *ldif* i, a continuació, integrar-l'en la base de dades amb *ldapadd*.

9.1. AFEGIR UN USUARI

Per a afegir un nou usuari, recorrem, com fins llaura, a l'editor *nano*:

```
sudo nano usuari.ldif
```

```
usuario@ldapserver: ~
Archivo Editar Ver Buscar Terminal Ayuda
usuario@ldapserver:~$ sudo nano usuari.ldif
```

Per descomptat, pots canviar el nom *usuari.ldif* pel qual et resulte més adequat en el teu cas.

En l'àrea de treball de l'editor, escriurem un contingut com aquest:

```
dn: uid=jlopez,ou=usuarios,dc=empresa,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: jlopez
sn: Lopez
givenName: Juan
cn: Juan Lopez
displayName: Juan Lopez
uidNumber: 2000
gidNumber: 10000
userPassword: el meu_password
gecos: Juan Lopez
loginShell: /bin/bash
homeDirectory: /home/jlopez
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: juan.lopez@empresa.com
postalCode: 29000
o: empresa
initials: JL
```

```
usuario@ldapserver: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.9.3
usuario@ldapserver: ~
dn: uid=jlopez,ou=usuarios,dc=empresa,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: jlopez
sn: Lopez
givenName: Juan
cn: Juan Lopez
displayName: Juan Lopez
uidNumber: 2000
gidNumber: 10000
userPassword: mi_password
gecos: Juan Lopez
loginShell: /bin/bash
homeDirectory: /home/jlopez
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: juan.lopez@empresa.com
postalCode: 29000
o: empresa
initials: JL
```

Quan hagem acabat d'escriure-ho, només ens quedarà guardar els canvis i tancar la finestra de l'editor.

Nota: En l'exemple, hem seguit la convenció de començar els UID dels usuaris a partir del valor 2000 (uidNumber: 2000). Així, els següents usuaris que creem de manera manual, rebran els valors 2001, 2002, etc.

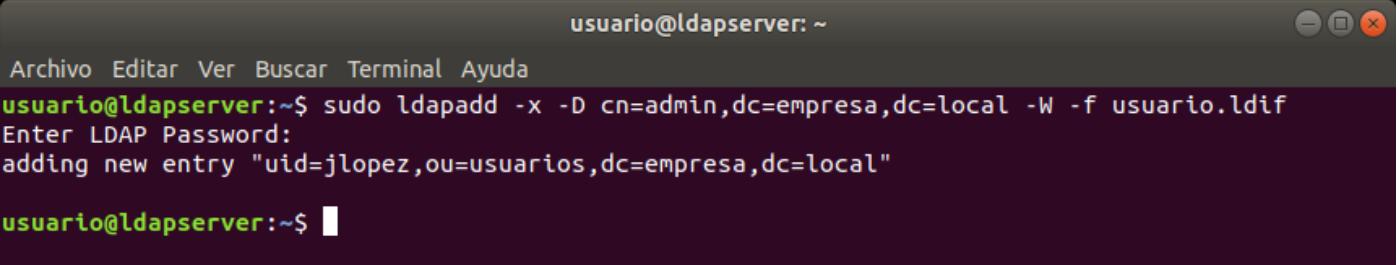
D'aquesta manera, evitem solapar-se amb els UID que assigna el sistema de manera automàtica, ja que aquests comencen de manera predeterminada en 1000.

Suposem que aqueix és un marge suficient però, en el teu cas, pots partir d'un valor diferent per a ampliar o disminuir l'interval.

Amb això ja estem llestos per a carregar el nou usuari en el directori. Només hem d'escriure el següent comando:

```
sudo ldapadd -x -D cn=admin,dc=empresa,dc=local -W -f usuari.ldif
```

Després d'escriure la contrasenya d'administració de LDAP, podrem comprovar que l'usuari s'ha afegit correctament.



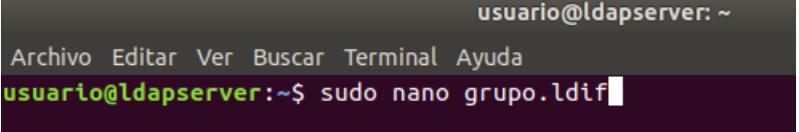
```
usuario@ldapserver:~$ sudo ldapadd -x -D cn=admin,dc=empresa,dc=local -W -f usuario.ldif
Enter LDAP Password:
adding new entry "uid=jlopez,ou=usuarios,dc=empresa,dc=local"

usuario@ldapserver:~$
```

9.2. AFEGIR UN GRUP

Per a afegir el grup, repetim de nou el procés anterior:

```
sudo nano grup.ldif
```



```
usuario@ldapserver:~$ sudo nano grupo.ldif
```

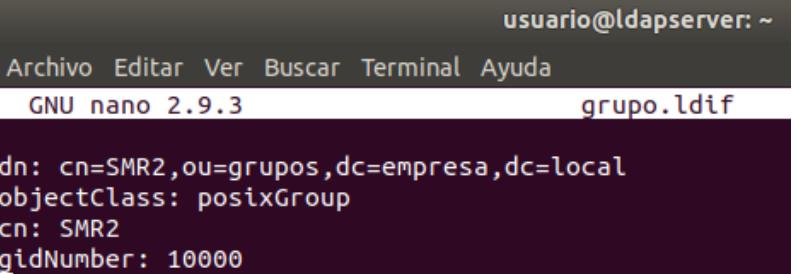
Una vegada obert l'editor, escriurem aquest contingut per a crear el grup SMR2:

```
dn: cn=SMR2,ou=grups,dc=empresa,dc=local
objectClass: posixGroup
cn: SMR2
gidNumber: 10000
```

Quan estiga llest, guardem els canvis i tanquem la finestra de l'editor.

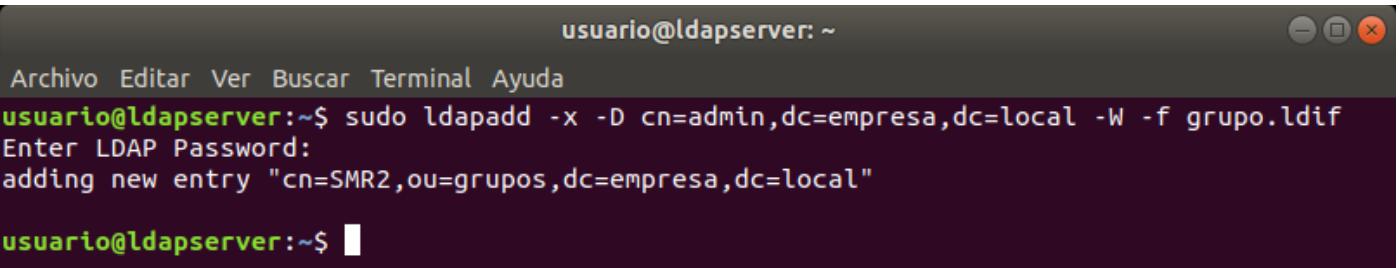
De tornada en la terminal, usem de nou el comando *ldapadd*:

```
sudo ldapadd -x -D cn=admin,dc=empresa,dc=local -W -f grup.ldif
```



```
usuario@ldapserver:~$ sudo ldapadd -x -D cn=admin,dc=empresa,dc=local -W -f grupo.ldif
Enter LDAP Password:
adding new entry "cn=SMR2,ou=grupos,dc=empresa,dc=local"
```

Després d'escriure la contrasenya d'administració de LDAP, podrem comprovar que el grup s'ha afegit correctament.



```
usuario@ldapserver:~$ sudo ldapadd -x -D cn=admin,dc=empresa,dc=local -W -f grupo.ldif
Enter LDAP Password:
adding new entry "cn=SMR2,ou=grupos,dc=empresa,dc=local"

usuario@ldapserver:~$
```

Amb això, ja tindrem en la base de dades un nou usuari i un nou grup.

IMPORTANT:

Quan afiges nous usuaris, recorda que els valors per als atributs **uidNumber** i **homeDirectory** han de ser diferents per a cada usuari. També caldrà substituir el text **el meu_password** per la contrasenya adequada per a l'usuari. El mateix ocorre amb l'atribut **gidNumber** dels grups.

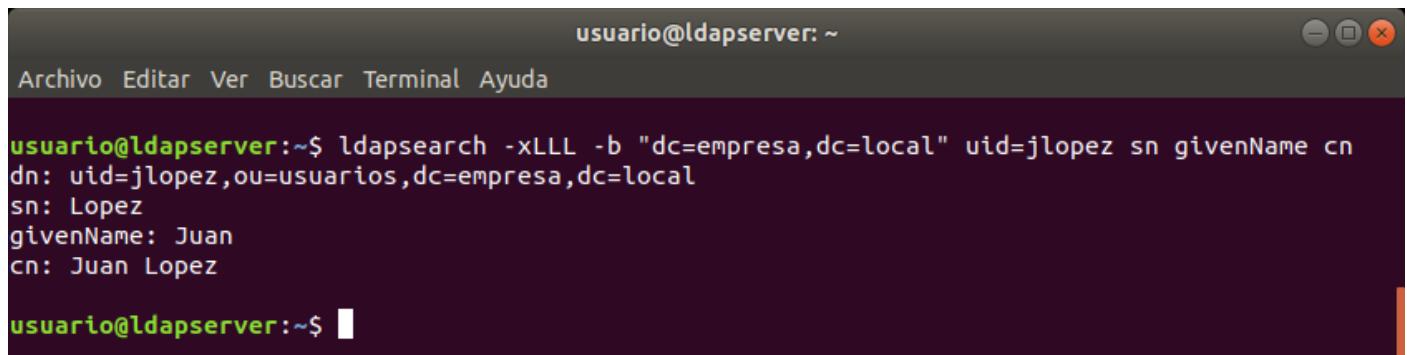
A més, els valors dels camps **uidNumber** i **gidNumber** no han de coincidir amb l'UID i GID de cap usuari i grup local.

9.3. COMPROVAR QUE TOT ÉS CORRECTE

Llaura podem comprovar que el contingut anterior s'ha afegit correctament. Per a aconseguir-ho podem utilitzar, per exemple, el comando *ldapsearch*, que ens permet fer una a prop en el directori:

```
ldapsearch -xLLL -b "dc=empresa,dc=local" uid=jlopez sn givenName cn
```

En aquest exemple busquem un usuari amb **uid=jlopez** i demanem que ens mostre el contingut dels atributs **sn**, **givenName** i **cn**.



```
usuario@ldapserver:~$ ldapsearch -xLLL -b "dc=empresa,dc=local" uid=jlopez sn givenName cn
dn: uid=jlopez,ou=usuarios,dc=empresa,dc=local
sn: Lopez
givenName: Juan
cn: Juan Lopez

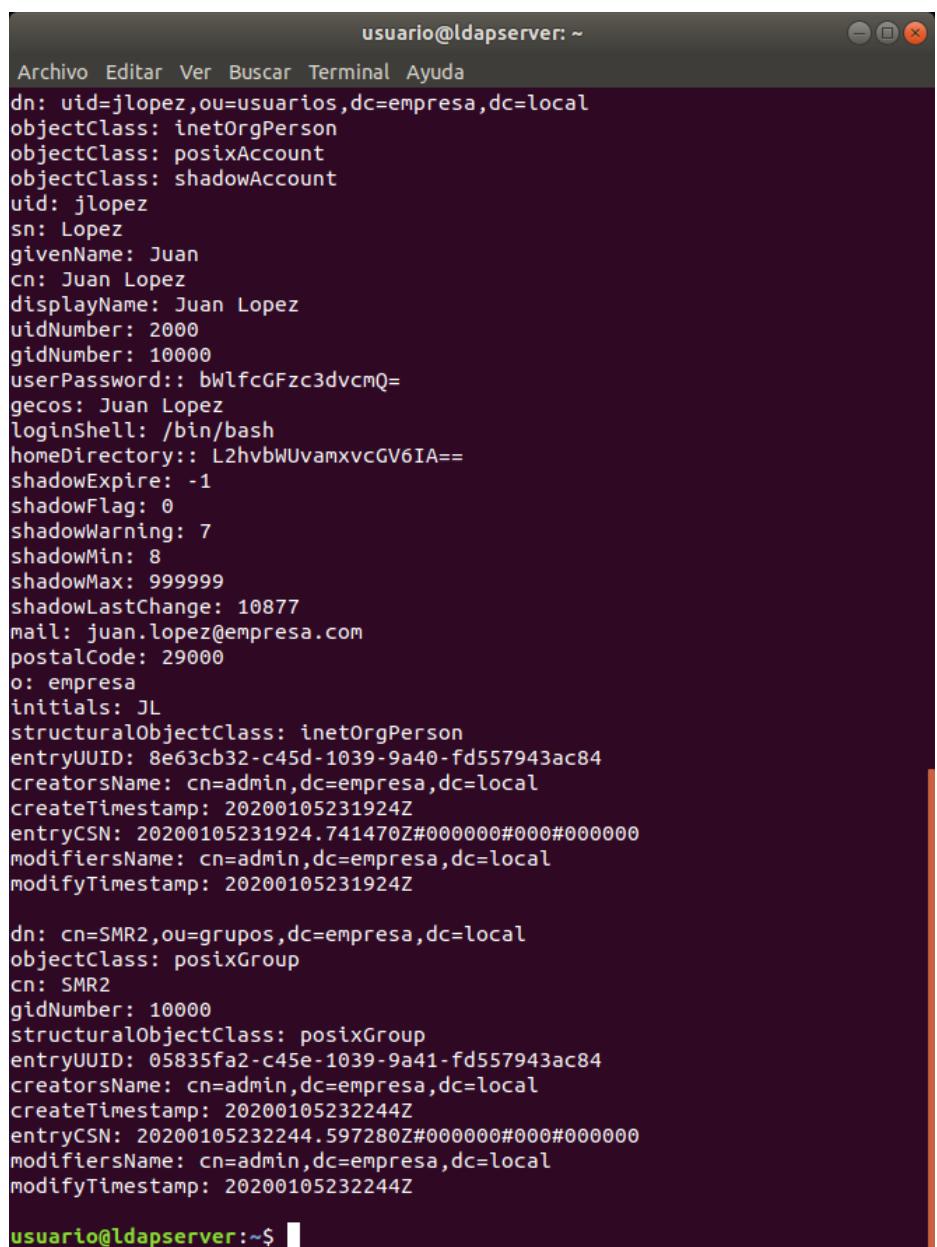
usuario@ldapserver:~$
```

Una altra opció interessant per a comprovar el contingut del directori és utilitzar el comando *slapcat*. Recorda que la seua comesa és mostrar el contingut complet del directori LDAP. A més, aquesta informació s'obté en format LDIF, la qual cosa ens permetrà bolcar-la a un fitxer i exportar la base de dades d'una manera molt senzilla.

En el nostre cas, ens limitarem a obtindre l'eixida en la pantalla:

```
sudo slapcat
```

Que ens mostrarà tota la informació de manera similar a aquesta captura:



```
usuario@ldapserver:~$ sudo slapcat
dn: uid=jlopez,ou=usuarios,dc=empresa,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: jlopez
sn: Lopez
givenName: Juan
cn: Juan Lopez
displayName: Juan Lopez
uidNumber: 2000
gidNumber: 10000
userPassword:: bWlfcGFzc3dvcmQ=
gecos: Juan Lopez
loginShell: /bin/bash
homeDirectory:: L2hvbwUvamxvcGV6IA==
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: juan.lopez@empresa.com
postalCode: 29000
o: empresa
initials: JL
structuralObjectClass: inetOrgPerson
entryUUID: 8e63cb32-c45d-1039-9a40-fd557943ac84
creatorsName: cn=admin,dc=empresa,dc=local
createTimestamp: 20200105231924Z
entryCSN: 20200105231924.741470Z#000000#000#000000
modifiersName: cn=admin,dc=empresa,dc=local
modifyTimestamp: 20200105231924Z

dn: cn=SMR2,ou=grupos,dc=empresa,dc=local
objectClass: posixGroup
cn: SMR2
gidNumber: 10000
structuralObjectClass: posixGroup
entryUUID: 05835fa2-c45e-1039-9a41-fd557943ac84
creatorsName: cn=admin,dc=empresa,dc=local
createTimestamp: 20200105232244Z
entryCSN: 20200105232244.597280Z#000000#000#000000
modifiersName: cn=admin,dc=empresa,dc=local
modifyTimestamp: 20200105232244Z

usuario@ldapserver:~$
```

10. BUSCAR, MODIFICAR I ELIMINAR ELEMENTS DEL DIRECTORI

Una vegada que hem aprés a afegir elements al directori LDAP, aprendrem a localitzar els elements que ja existeixen, a realitzar modificacions sobre ells i a poder eliminar-los si ho considerem necessari. Anem a pams:

10.1. BUSCAR ELEMENTS DEL DIRECTORI

Com hem vist més amunt, la utilitat de línia de comandos que permet realitzar voltes en el directori LDAP és **ldapsearch**. És tracta d'una utilitat amb multitud d'opcions, però ací farem un ús bàsic d'ella.

Per exemple, podríem buscar tots els usuaris usant la següent sintaxi:

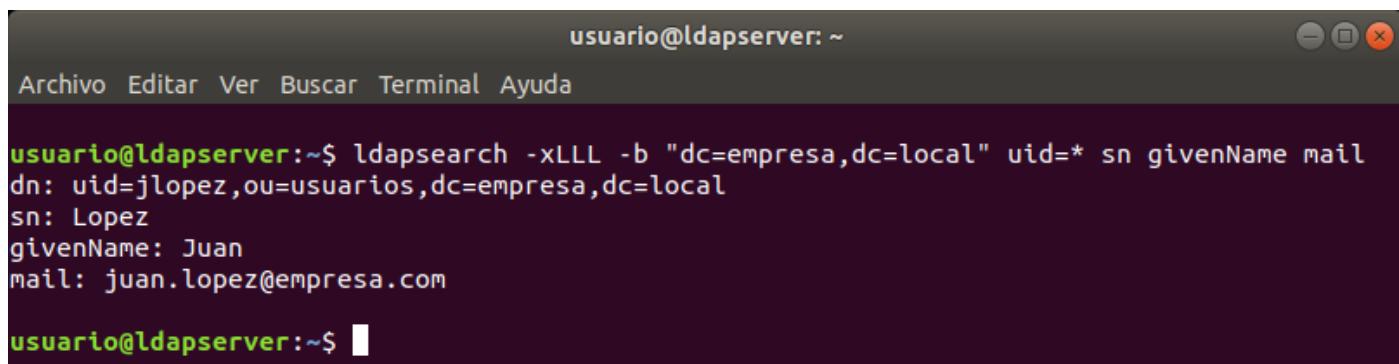
```
ldapsearch -xLLL -b "dc=empresa,dc=local" uid=* sn givenName mail
```

(Observa que és la mateixa ordre que escrivim en l'apartat anterior, però llaura hem utilitzat un asterisc com a valor d'uid).

Encara que no entrarem en molts detalls, almenys explicarem els arguments que estem usant per a aquest exemple:

- -x indica que usarem autenticació simple.
- -LLL serveix perquè l'eixida seguís del tipus LDAPv1.
- -b va seguida del punt de l'arbre on ha de començar l'a prop. En aquest cas, dc=empresa,dc=local.
- Després s'inclou la condició que hauran de complir els objectes buscats. En l'exemple, qualsevol valor (*) per a l'atribut **uid**.
- Finalment, s'inclou el nom dels atributs que volem obtindre en el resultat de la consulta.

Com pots veure en la imatge següent, el resultat de la consulta s'obté en format LDIF, la qual cosa facilitarà redirigir-ho a un arxiu i usar-ho com a còpia de seguretat o fins i tot com a mètode d'exportació de dades a una altra implementació d'OpenLDAP.



The screenshot shows a terminal window titled "usuario@ldapserver: ~". The window has standard OS X-style window controls (minimize, maximize, close) at the top right. The menu bar includes "Archivo", "Editar", "Ver", "Buscar", "Terminal", and "Ayuda". The main terminal area displays the following text:

```
usuario@ldapserver:~$ ldapsearch -xLLL -b "dc=empresa,dc=local" uid=* sn givenName mail
dn: uid=jlopez,ou=usuarios,dc=empresa,dc=local
sn: Lopez
givenName: Juan
mail: juan.lopez@empresa.com

usuario@ldapserver:~$
```

10.2. MODIFICAR ENTRADES DEL DIRECTORI

Si et fixes en l'eixida de la consulta anterior, existeix un error: el valor del correu electrònic dels dos últims usuaris és el mateix.

Aquesta situació ens ofereix l'excusa perfecta per a comprovar com podem canviar el valor de l'atribut **mail** per a l'usuari **lgomez**.

El comando que usarem en aquest cas és **ldapmodify**, que permet canviar el contingut de qualsevol atribut, afegir atributs nous, eliminar-los, etc.

Atés que la sintaxi és més complexa ens recolzarem en un arxiu LDIF que especifique els canvis que necessitem realitzar. En el nostre cas, l'arxiu tindrà el següent aspecte:

```
dn: uid=jlopez,ou=usuarios,dc=empresa,dc=local
changetype: modify
replace: mail
mail: juan.lopez@empresa.es
```

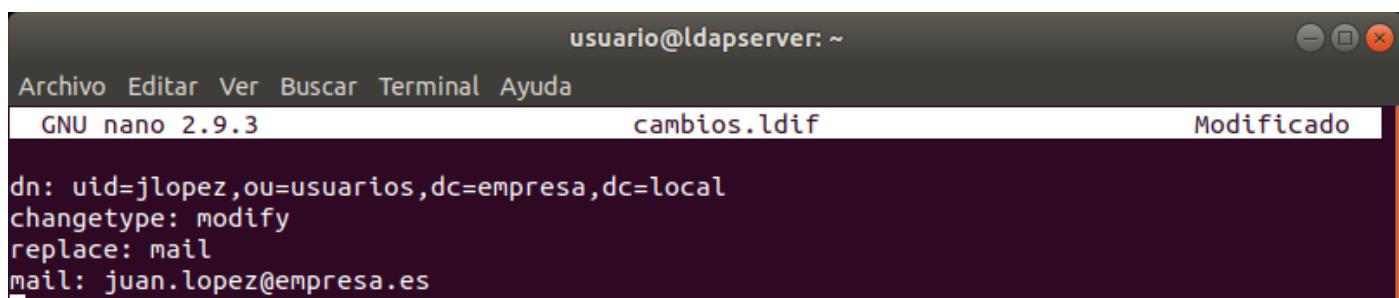
Com pots suposar, la primera línia identifica el compte en la qual farem el canvi. La segona indica el tipus d'operació a realitzar, la tercera identifica l'atribut i, finalment, la quarta inclou el nou valor que ha d'assignar-li.

Usarem l'editor nano per a crear l'arxiu, que per a aquest exemple direm canvis.ldif.

```
sudo nano canvis.ldif
```

```
usuario@ldapserver:~$ sudo nano cambios.ldif
```

Una vegada obert l'editor, escrivim el text de l'exemple.

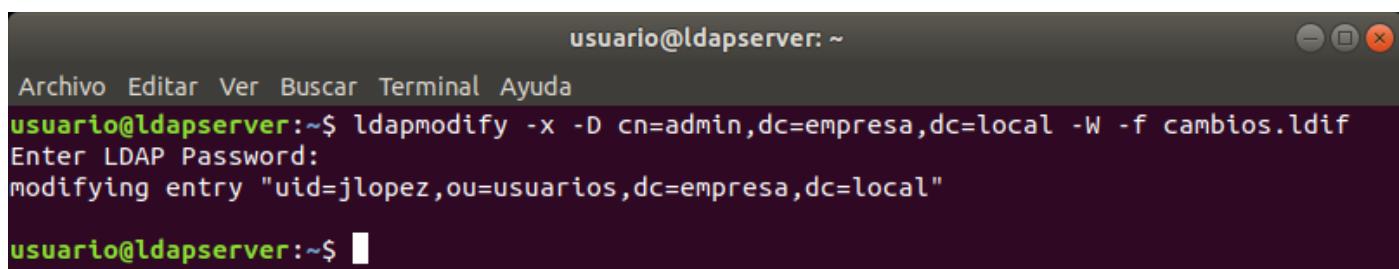


```
usuario@ldapserver: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.9.3           cambios.ldif          Modificado
dn: uid=jlopez,ou=usuarios,dc=empresa,dc=local
changetype: modify
replace: mail
mail: juan.lopez@empresa.es
```

Finalment, executem la utilitat **ldapmodify**, indicant-li el nom de l'arxiu on és troben els dades:

```
ldapmodify -x -D cn=admin,dc=empresa,dc=local -W -f canvis.ldif
```

Després d'escriure la contrasenya, el comando ens respon amb els dades de l'entrada que ha sigut modificada.

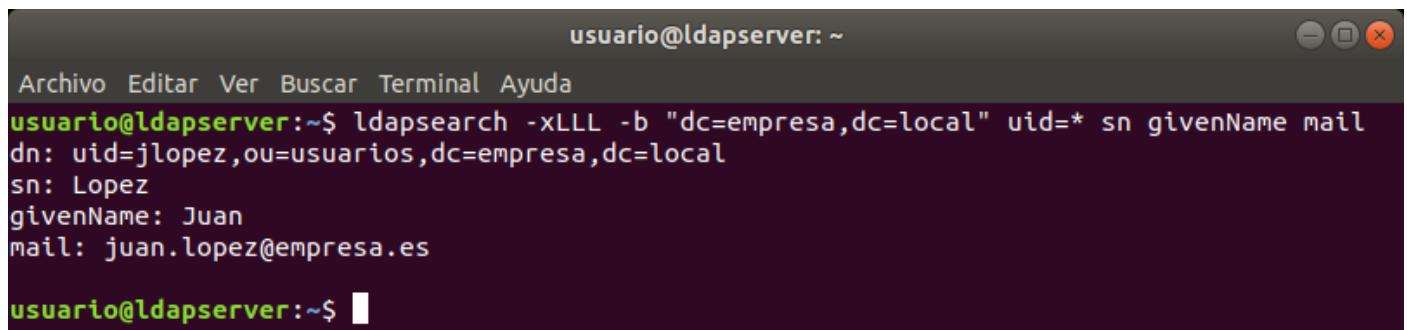


```
usuario@ldapserver: ~
Archivo Editar Ver Buscar Terminal Ayuda
usuario@ldapserver:~$ ldapmodify -x -D cn=admin,dc=empresa,dc=local -W -f cambios.ldif
Enter LDAP Password:
modifying entry "uid=jlopez,ou=usuarios,dc=empresa,dc=local"

usuario@ldapserver:~$
```

Si vols comprovar que els canvis s'han efectuat correctament, n'hi ha prou amb tornar a utilitzar la utilitat **ldapsearch**, tal i com vam fer en el punt anterior:

```
ldapsearch -xLLL -b "dc=empresa,dc=local" uid=* sn givenName mail
```



A terminal window titled "usuario@ldapserver: ~". The window has a dark background with white text. The title bar says "usuario@ldapserver: ~". The menu bar includes "Archivo", "Editar", "Ver", "Buscar", "Terminal", and "Ayuda". The command entered is "ldapsearch -xLLL -b \"dc=empresa,dc=local\" uid=* sn givenName mail". The output shows a single user entry:

```
usuario@ldapserver:~$ ldapsearch -xLLL -b "dc=empresa,dc=local" uid=* sn givenName mail
dn: uid=jlopez,ou=usuarios,dc=empresa,dc=local
sn: Lopez
givenName: Juan
mail: juan.lopez@empresa.es
```

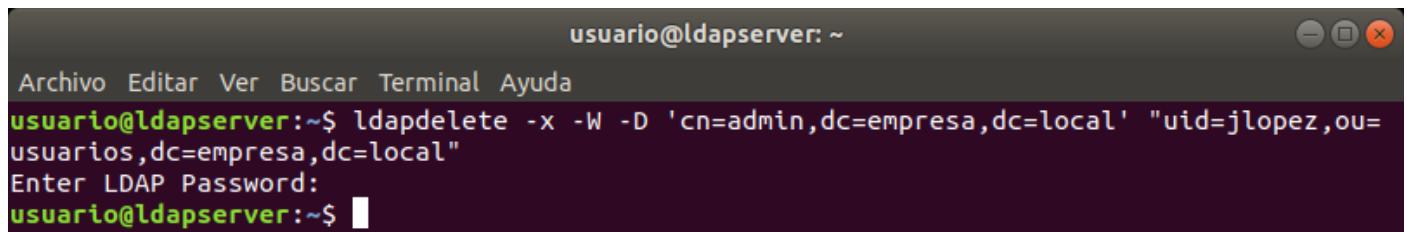
The prompt "usuario@ldapserver:~\$" is visible at the bottom.

10.3. ESBORRAR ENTRADES DEL DIRECTORI

La utilitat que permet eliminar entrades del directori és diu **ldapdelete**. Per a utilitzar-la, només hem d'aportar els dades de l'objecte a esborrar i els dades del compte administrador que ha de permetre-ho. La sintaxi serà com segueix:

```
ldapdelete -x -W -D 'cn=admin,dc=empresa,dc=local' "uid=jlopez,ou=usuarios,dc=empresa,dc=local"
```

Després d'escriure la contrasenya, semblarà que no ha ocorregut cap de bestiar. No obstant això, l'objecte haurà sigut eliminat.

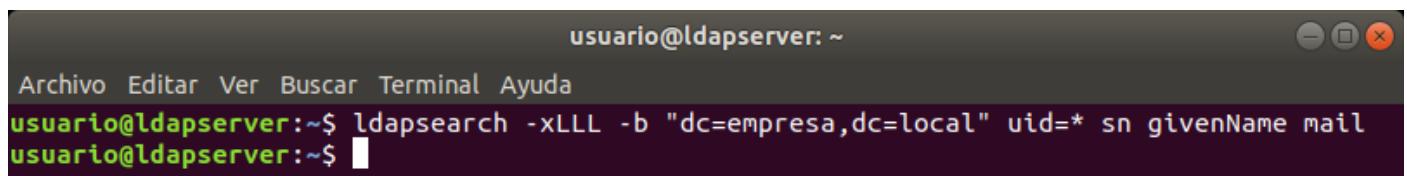


A terminal window titled "usuario@ldapserver: ~". The window has a dark background with white text. The title bar says "usuario@ldapserver: ~". The menu bar includes "Archivo", "Editar", "Ver", "Buscar", "Terminal", and "Ayuda". The command entered is "ldapdelete -x -W -D 'cn=admin,dc=empresa,dc=local' "uid=jlopez,ou=usuarios,dc=empresa,dc=local"". A password prompt "Enter LDAP Password:" appears. The prompt "usuario@ldapserver:~\$" is visible at the bottom.

```
usuario@ldapserver:~$ ldapdelete -x -W -D 'cn=admin,dc=empresa,dc=local' "uid=jlopez,ou=usuarios,dc=empresa,dc=local"
Enter LDAP Password:
usuario@ldapserver:~$
```

Per a comprovar que l'eliminació ha sigut efectiva, podem tornar a utilitzar la utilitat **ldapsearch**.

```
ldapsearch -xLLL -b "dc=empresa,dc=local" uid=* sn givenName mail
```



A terminal window titled "usuario@ldapserver: ~". The window has a dark background with white text. The title bar says "usuario@ldapserver: ~". The menu bar includes "Archivo", "Editar", "Ver", "Buscar", "Terminal", and "Ayuda". The command entered is "ldapsearch -xLLL -b \"dc=empresa,dc=local\" uid=* sn givenName mail". The output is empty, indicating the user has been deleted.

```
usuario@ldapserver:~$ ldapsearch -xLLL -b "dc=empresa,dc=local" uid=* sn givenName mail
usuario@ldapserver:~$
```

11. IMPORTAR ELS USUARIS I GRUPS LOCALS EN EL SERVIDOR OPENLDAP

Utilitzant el mecanisme que hem aprés en l'apartat anterior, podríem crear tants usuaris com necessitarem. Fins i tot podem crear un nou compte en el servidor OpenLDAP per a cadascun dels usuaris i grups locals que ja tinguem en l'equip que actua com a servidor.

No obstant això, en aquest últim cas, potser és més recomanable escriure un xicotet script que obtinga la informació que necessite i cree els nous comptes de manera automàtica. Sobretot quan el nom d'usuaris seguisca elevat.

11.1. IMPORTAR USUARIS LOCALS AL DIRECTORI OPENLDAP

Per a dur a terme aquesta taverna, és important saber que GNU/LINUX, de manera predeterminada, guarda la informació sobre els usuaris locals dins de l'arxiu /etc/passwd. Per tant, l'objectiu general del script serà obtindre aquestes dades i crear amb ells un arxiu ldif com el que hem escrit nosaltres en l'apartat anterior. Després, executarà el comando ldapadd per a afegir-los.

Nota: L'arxiu /etc/passwd vaig comptar tant usuaris normals com usuaris especials del sistema. Per a diferenciar-los, els primers tenen un UID amb un valor 1000 o superior.

```
Archivo Editar Ver Buscar Terminal Ayuda
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uidd:x:105:111::/run/uidd:/usr/sbin/nologin
avahi-autoipd:x:106:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
cups-pk-helper:x:110:116:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
whoopsie:x:112:117::/nonexistent:/bin/false
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
saned:x:114:119::/var/lib/saned:/usr/sbin/nologin
pulse:x:115:120:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
avahi:x:116:122:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:117:123:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:118:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:119:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:120:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
administrador:x:1000:1000:administrador,,,:/home/administrador:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
usuario:x:1001:1001:usuario,,,:/home/usuario:/bin/bash
openldap:x:122:127:OpenLDAP Server Account,,,:/var/lib/ldap:/bin/false
usuario@ldapserver:~$
```

En termes generals, observem que els diferents dades de cada compte van separats per dos punts (:); i, en particular, els dades contingudes són els següents:

- El nom del compte (també conegut com login).
- La contrasenya, encara que apareix una x perquè en realitat és troba en l'arxiu /etc/shadow (aquest camp és manté per compatibilitat amb l'estructura original de l'arxiu).
- L'UID d'usuari que ha de ser un identificador únic en el sistema.
- El GID del grup primari al qual pertany l'usuari. En Ubuntu, de manera predeterminada, quan creuem un usuari es crea un grup amb el mateix nom, que actua com el seu grup primari.
- Informació sobre l'usuari, separada per menges. La primera donada sol ser el seu nom complet.
- El directori home de l'usuari, que sol ser una carpeta amb el nom del compte, dins de la carpeta /home.

- La shell que utilitzarà l'usuari de manera predeterminada. Sol ser /bin/bash/.

A partir d'ací, ens posaríem a la feina per a escriure el script. Probablement, cada programador li donaria a aquest problema una solució diferent. Nosaltres hem inclòs un possible resultat, on hem prevalgut la claredat a l'eficàcia (per evidents motius pedagògics), encara que compleix perfectament amb la seua comesa:

```
#!/bin/bash

#Obtindre usuaris amb uidNumber >= 1000

grep "x:[1-9][0-9][0-9][0-9]:" /etc/passwd > tmp.txt

#Crear o reiniciar arxiu ldif
>tmp.ldif

#Recórrer l'arxiu tmp.txt amb la llista d'usuaris
while read línia
do
    #Mostrar la línia que processarem
    echo "$línia"

    #Obtindre dades
    uid=$(echo $línia | cut -d: -f1) # El primer camp, separant amb :
    nomComp=$(echo $línia | cut -d: -f5 | cut -d, -f1) # El que hi ha abans de la 1a
    menge del 5é camp
    nomArray=($nomComp) #Converteix el nom en un array de paraules
    nom=${nomArray[0]}
    if [ "$nom" == "" ]
    then
        nom=$uid
    fi
    ape=${nomArray[1]}
    if [ "$ape" == "" ]
    then
        ape=$uid
    fi
    inic=$(echo $nom | cut -c 1)$(echo $ape | cut -c 1)
    uidNum=$(echo $línia | cut -d: -f3)
    usrPass=$(grep $uid: /etc/shadow | cut -d: -f2)
    shell=$(echo $línia | cut -d: -f7)
    homedir=$(echo $línia | cut -d: -f6)

    #Bolcar dades a l'arxiu ldif
    echo "dn: uid=$uid,ou=usuaris,dc=empresa,dc=local" >> tmp.ldif
    echo "objectClass: inetOrgPerson" >> tmp.ldif
    echo "objectClass: posixAccount" >> tmp.ldif
    echo "objectClass: shadowAccount" >> tmp.ldif
    echo "uid: $uid" >> tmp.ldif
    echo "sn: $ape" >> tmp.ldif
    echo "givenName: $nom" >> tmp.ldif
    echo "cn: $nomComp" >> tmp.ldif
    echo "displayName: $nomComp" >> tmp.ldif
    echo "uidNumber: $uidNum" >> tmp.ldif
    echo "gidNumber: 10000" >> tmp.ldif
    echo "userPassword: $usrPass" >> tmp.ldif
    echo "gecos: $nomComp" >> tmp.ldif
    echo "loginShell: $shell" >> tmp.ldif
    echo "homeDirectory: $homedir" >> tmp.ldif
    echo "shadowExpire: -1" >> tmp.ldif
```

```

echo "shadowFlag: 0" >> tmp.ldif
echo "shadowWarning: 7" >> tmp.ldif
echo "shadowMin: 8" >> tmdddp.ldif
echo "shadowMax: 999999" >> tmp.ldif
echo "shadowLastChange: 10877" >> tmp.ldif
echo "mail: ${nom[0]}.${nom[1]}@empresa.com" >> tmp.ldif
echo "postalCode: 29000" >> tmp.ldif
echo "o: empresa" >> tmp.ldif
echo "initials: $inic" >> tmp.ldif
echo >> tmp.ldif
done < tmp.txt

#Afegim els nous usuaris a LDAP
ldapadd -x -D cn=admin,dc=empresa,dc=local -W -f tmp.ldif
rm tmp.txt
rm tmp.ldif

```

Encara que no realitzarem una explicació detallada del funcionament del script, a continuació s'inclouen uneixes pautes amb la finalitat de facilitar la seu interpretació:

1. En la línia 5, comencem per buscar totes els línies de l'arxiu /etc/passwd que incloguen, a continuació del text 'x:', un número de 4 xifres. Aquestes línies es copien a un arxiu anomenat tmp.txt.
2. En la línia 8, creem un arxiu amb el nom tmp.ldif, que serà el que continga la definició dels usuaris per a OpenLDAP. Farà la funció de l'arxiu usuari.ldif de l'apartat anterior. Si l'arxiu ja existeix, perdrà tot el seu contingut anterior. Si no, senzillament es crea.
3. Entre la línia 11 i la 63, fem un bucle que obté, en cada iteració, una línia de l'arxiu tmp.txt, dins d'una variable anomenada línia.
4. Una vegada obtinguda una línia, la vam mostrar, en la línia 14, perquè puguem comprovar que l'usuari que s'està processant és l'adequat.
5. Després, entre els línies 17 i 34, anem partint la informació obtinguda de l'arxiu per a obtindre cadascun dels seus camps per separat:
 - a) En la línia 17, dividim el text en camps usant com a separador el caràcter de dos punts (:) i ens quedem amb el primer d'aquests camps (cut -d: -f1). Això és el nom del compte d'usuari.
 - b) En la línia 18 obtenim el nom complet de l'usuari. Primer el cinqué camp, usant com a separador els dos punts (:) i, dins d'ell, el primer usant com a separador la coma (,).
 - c) En la línia 19 convertim el nom complet en un array, de manera que puguem separar el nom dels cognoms (línies 20 i 25).
 - d) En cas que el nom estiga buit, usem el nom del compte (línies 21 a 24). I fem el mateix amb el cognom (línies 26 a 29).
 - e) En la línia 30, obtenim la primera lletra del nom i del cognom per a crear els inicials.
 - f) En la línia 32, busquem la línia que vaig comptar el nom del compte en l'arxiu /etc/shadow i ens quedem amb el segon camp, que és la contrasenya xifrada per a aqueix usuari.
 - g) Finalment, en els línies 31, 33 i 34 apliquem el mateix procediment de la línia 17, per a obtindre l'UID, la shell i el directori home del compte.
6. A continuació, entre els línies 37 i 62 componem el contingut de l'arxiu tmp.ldif per a l'usuari que ens ocupa. Cada línia és limitada a realitzar un echo amb el format adequat per a l'arxiu, usant els dades obtingudes en els línies 17 a 34. L'eixida s'afegirà (>>) al contingut de l'arxiu tmp.ldif.
7. Una vegada acabat el recorregut de l'arxiu tmp.txt, només quedarà executar el comando ldapadd que ja coneixem, i eliminar els arxius temporals que hem creat durant el procés (tmp.txt i tmp.ldif).

Nota: Observa que, en afegir els usuaris al directori OpenLDAP, no hem mantingut el seu grup original, sinó que els hem assignats al grup usuaris que havíem creat en l'apartat anterior. D'aquesta manera, podem evitar la creació d'un grup diferent per a cada usuari importat.

L'avantatge que te usar l'editor gedit és que te la capacitat d'acolorir la sintaxi, la qual cosa simplifica l'escriptura del codi:

```
sudo gedit importar.sh
```

```
#!/bin/bash
#Obtener usuarios con uidNumber >= 1000
grep "x:[1-9][0-9][0-9]:" /etc/passwd > tmp.txt
#Crear o reiniciar archivo ldif
>tmp.ldif
#Recorrer el archivo tmp.txt con la lista de usuarios
while read linea
do
    #Mostrar la linea que vamos a procesar
    echo "$linea"

    #Obtener datos
    uid=$(echo $linea | cut -d: -f1) # El primer campo, separando con :
    nomComp=$(echo $linea | cut -d: -f5 | cut -d. -f1) # Lo que hay antes de la 1º coma del 5º campo
    nomArray=($nomComp) #Convierte el nombre en un array de palabras
    nom=${nomArray[0]}
    if [ "$nom" == "" ]
    then
        nom=$uid
    fi
    ape=${nomArray[1]}
    if [ "$ape" == "" ]
    then
        ape=$uid
    fi
    inic=$(echo $nom | cut -c 1)$(echo $ape | cut -c 1)
    uidNum=$(echo $linea | cut -d: -f3)
    usrPass=$(grep $uid: /etc/shadow | cut -d: -f2)
    shell=$(echo $linea | cut -d: -f7)
    homedir=$(echo $linea | cut -d: -f6)

    #Volcar datos al archivo ldif
    echo "dn: uid=$uid,ou=usuarios,dc=empresa,dc=local" >> tmp.ldif
    echo "objectClass: inetOrgPerson" >> tmp.ldif
    echo "objectClass: posixAccount" >> tmp.ldif
    echo "objectClass: shadowAccount" >> tmp.ldif
    echo "uid: $uid" >> tmp.ldif
    echo "sn: $ape" >> tmp.ldif
    echo "givenName: $nom" >> tmp.ldif
    echo "cn: $nomComp" >> tmp.ldif
    echo "displayName: $nomComp" >> tmp.ldif
    echo "uidNumber: $uidNum" >> tmp.ldif
    echo "gidNumber: 10000" >> tmp.ldif
sh ▾ Anchura del tabulador: 8 ▾ Ln 69, Col 1 ▾ INS
```

A continuació, hem d'atorgar-li al script permisos d'execució. Per a aconseguir-ho, haurem d'assegurar-ens que el nostre directori de treball és on tenim l'arxiu (recorda que l'hem anomenat importar.sh i és troba en la carpeta personal de l'usuari amb el qual estem treballant).

Una vegada en ací, només hem d'executar el següent comando:

```
sudo chmod +x importar.sh
```

```
usuario@ldapserver: ~
Archivo Editar Ver Buscar Terminal Ayuda
usuario@ldapserver:~$ sudo chmod +x importar.sh
```

Com és lòtic, el següent pas consistirà a executar el script, encara que hem de recordar fer-ho amb privilegis d'administració:

```
sudo ./importar.sh
```

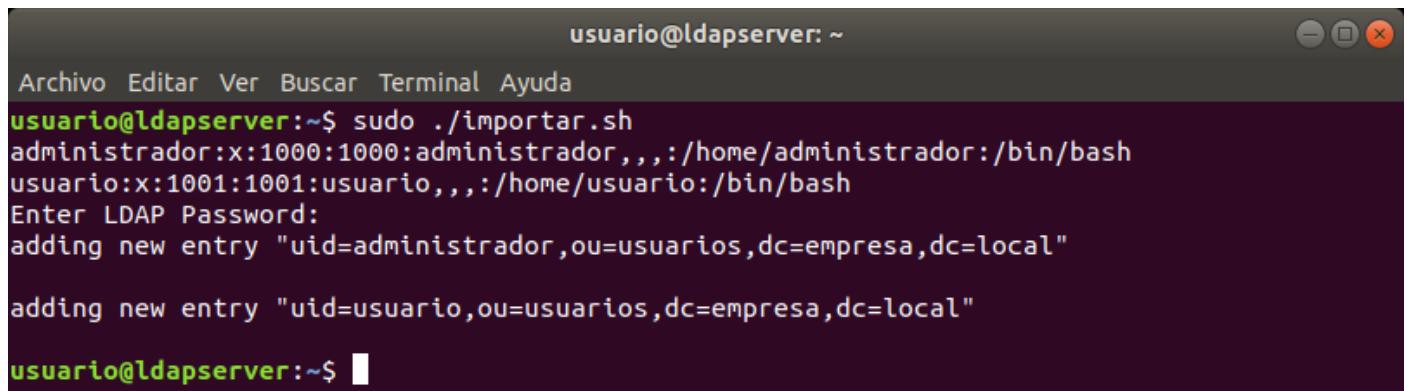
```
usuario@ldapserver: ~
Archivo Editar Ver Buscar Terminal Ayuda
usuario@ldapserver:~$ sudo ./importar.sh
```

Com veiem en la imatge de baix, el primer que fa el script és mostrar-nos la llista dels usuaris que seran importats (encara que, en aquest cas, només hi ha un). Encara que te el format de l'arxiu /etc/passwd, en realitat el que estem veient és el contingut de l'arxiu ./tmp.txt.

Després, encara que no vegem cap de bestiar, s'haurà produït la creació de l'arxiu ./tmp.ldif.

Finalment, s'executarà el comando ldapadd que, per a completar el seu treball, necessitarà que ens autentiquem com a administradors del directori OpenLDAP. D'aquí es veu que se'n demane la contrasenya.

Finalment, l'eixida del comando ldapadd ens confirmarà que la taverna s'ha completat amb èxit.



```
usuario@ldapserver: ~
Archivo Editar Ver Buscar Terminal Ayuda
usuario@ldapserver:~$ sudo ./importar.sh
administrador:x:1000:1000:administrador,,,:/home/administrador:/bin/bash
usuario:x:1001:1001:usuario,,,:/home/usuario:/bin/bash
Enter LDAP Password:
adding new entry "uid=administrador,ou=usuarios,dc=empresa,dc=local"

adding new entry "uid=usuario,ou=usuarios,dc=empresa,dc=local"

usuario@ldapserver:~$
```

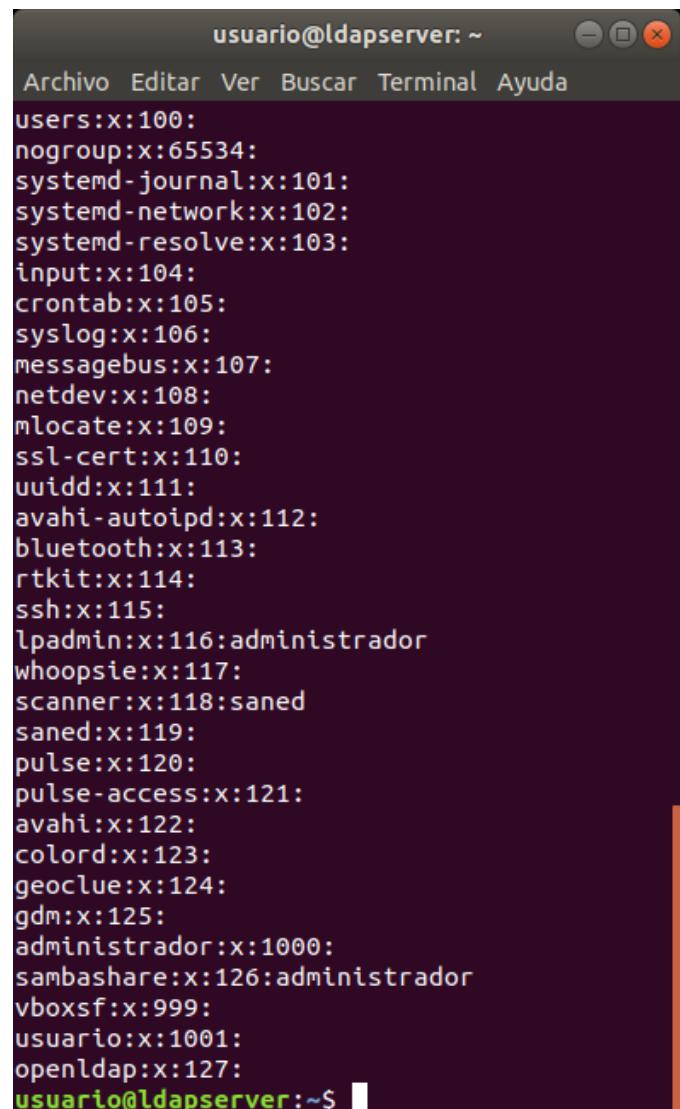
Nota: Com abans, podem tornar a usar el comando slapcat per a mostrar el contingut complet del directori, tal com vam veure més amunt.

11.2. IMPORTAR GRUPS LOCALS AL DIRECTORI OPENLDAP

La manera d'importar els grups locals és bastant semblant a la qual hem aplicat per a importar els usuaris, per la qual cosa, aquesta vegada ho explicarem de forma menys detallada.

Per a començar, hem de saber que, de manera predeterminada, GNU/Linux, guarda la informació sobre els grups locals en l'arxiu /etc/group. Com abans, l'objectiu general del script serà obtindre aquestes dades i crear amb ells un nou arxiu ldif. A continuació, tornarà a executar el comando ldapadd per a afegir-los.

Per a fer-ne una idea del treball a realitzar, hem d'estudiar l'aspecte general de l'arxiu /etc/group.



```
usuario@ldapserver: ~
Archivo Editar Ver Buscar Terminal Ayuda
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-network:x:102:
systemd-resolve:x:103:
input:x:104:
crontab:x:105:
syslog:x:106:
messagebus:x:107:
netdev:x:108:
mlocate:x:109:
ssl-cert:x:110:
uuidd:x:111:
avahi-autoipd:x:112:
bluetooth:x:113:
rtkit:x:114:
ssh:x:115:
lpadmin:x:116:administrador
whoopsie:x:117:
scanner:x:118:saned
saned:x:119:
pulse:x:120:
pulse-access:x:121:
avahi:x:122:
colord:x:123:
geoclue:x:124:
gdm:x:125:
administrador:x:1000:
sambashare:x:126:administrador
vboxsf:x:999:
usuario:x:1001:
openldap:x:127:
usuario@ldapserver:~$
```

Com hem dit, ací seguirem, aproximadament, els passos donats per a crear el script anterior:

- Copiarem totes les línies de l'arxiu /etc/group que incloguen el text 'x:', seguit d'un número de 4 xifres, en un nou arxiu anomenat tmp.txt.
- Crearem un nou arxiu anomenat tmp.ldif on després guardarem la definició dels grups per a OpenLDAP.
- Incloureml un bucle que recórrega l'arxiu tmp.txt línia a línia. La vam mostrar en pantalla i la descomponem en els seus diferents elements, bolcant-los a l'arxiu tmp.ldif.
- Una vegada acabat el recorregut de l'arxiu tmp.txt, només quedarà executar el comando ldapadd, i eliminar els arxius temporals que hem creat durant el procés (tmp.txt i tmp.ldif).

Finalment, el resultat haurà de semblar-se a aquest:

```
#!/bin/bash

#Obtindre grups amb uidNumber >= 1000
grep "x:[1-9][0-9][0-9][0-9]:" /etc/group > tmp.txt

#Crear o reiniciar arxiu ldif
>tmp.ldif

#Recórrer l'arxiu tmp.txt amb la llista de grups
while read línia
do
    #Mostrar la línia que processarem
    echo "$línia"

    #Obtindre dades
    cn=$(echo $línia | cut -d: -f1) # El primer camp, separant amb :
    gid=$(echo $línia | cut -d: -f3)
    usuaris=$(echo $línia | cut -d: -f4 | set "s/,/ /g")

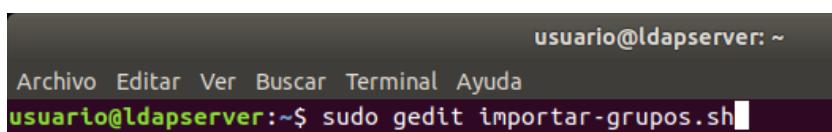
    #Bolcar dades a l'arxiu ldif
    echo "dn: cn=$cn,ou=grups,dc=empresa,dc=local" >> tmp.ldif
    echo "objectClass: posixGroup" >> tmp.ldif
    echo "cn: $cn" >> tmp.ldif
    echo "gidNumber: $gid" >> tmp.ldif
    echo >> tmp.ldif

    #afegir usuaris
    for usuari in ${usuaris} ; do
        echo "memberUid: ${usuari}" >> tmp.ldif
    done
done < tmp.txt

#Afegim els nous grups a LDAP
ldapadd -x -D cn=admin,dc=empresa,dc=local -W -f tmp.ldif
rm tmp.txt
rm tmp.ldif
```

Com abans, tornem a usar gedit, que te la capacitat afegida d'acolorir la sintaxi, la qual cosa simplifica l'escriptura del codi:

```
sudo gedit importar-grupos.sh
```



The screenshot shows a terminal window with a dark background. At the top, it says 'usuario@ldapserver: ~'. Below that is a menu bar with options: Archivo, Editar, Ver, Buscar, Terminal, Ayuda. The main area of the terminal is a light grey color. A green cursor is visible at the bottom of the screen. The text 'usuario@ldapserver:~\$ sudo gedit importar-grupos.sh' is written in white, indicating the command being entered.

Una vegada escrit, o copiat, el codi del script, ja podem guardar el seu contingut.



```
*importar-grupos.sh
#!/bin/bash

#Obtener grupos con uidNumber >= 1000
grep "x:[1-9][0-9][0-9][0-9]:" /etc/group > tmp.txt

#Crear o reiniciar archivo ldif
>tmp.ldif

#Recorrer el archivo tmp.txt con la lista de grupos
while read linea
do
    #Mostrar la linea que vamos a procesar
    echo "$linea"

    #Obtener datos
    cn=$(echo $linea | cut -d: -f1) # El primer campo, separando con :
    gid=$(echo $linea | cut -d: -f3)
    usuarios=$(echo $linea | cut -d: -f4 | sed "s/,/ /g")

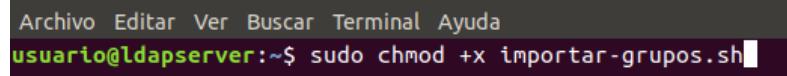
    #Volcar datos al archivo ldif
    echo "dn: cn=$cn,ou=grupos,dc=empresa,dc=local" >> tmp.ldif
    echo "objectClass: posixGroup" >> tmp.ldif
    echo "cn: $cn" >> tmp.ldif
    echo "gidNumber: $gid" >> tmp.ldif
    echo >> tmp.ldif

    #añadir usuarios
    for usuario in ${usuarios} ; do
        echo "memberUid: ${usuario}" >> tmp.ldif
    done
done < tmp.txt

#Añadimos los nuevos grupos a LDAP
ldapadd -x -D cn=admin,dc=empresa,dc=local -W -f tmp.ldif
rm tmp.txt
rm tmp.ldif
```

Iugal que en el cas anterior, el següent serà atorgar al script permisos d'execució. Tornem a assegurar-nos que el nostre directori de treball és el que vaig comptar a l'arxiu (recorda que l'hem anomenat importar-grupos.sh i és troba en la carpeta personal de l'usuari amb el qual estem treballant). Una vegada en ací, només hem d'executar el següent comando:

```
sudo chmod +x importar-grupos.sh
```



```
usuario@ldapserver: ~
Archivo Editar Ver Buscar Terminal Ayuda
usuario@ldapserver:~$ sudo chmod +x importar-grupos.sh
```

A continuació, executem el script mitjançant el comando:

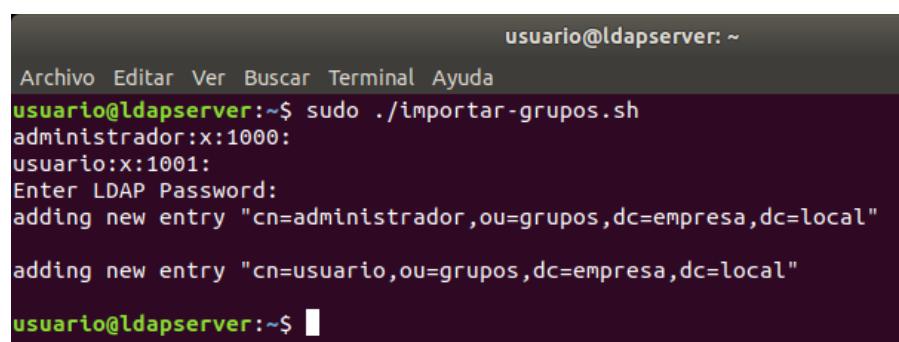
```
sudo ./importar-grups.sh
```

Com veiem en la imatge de baix, el primer que fa el script és mostrar-nos la llista dels grups que seran importats (encara que, en aquest cas, torna a haver-hi només un). Encara que te el format de l'arxiu /etc/group, en realitat el que estem veient és el contingut de l'arxiu ./tmp.txt.

Després, encara que no vegem cap de bestiar, s'haurà produït la creació de l'arxiu ./tmp.ldif.

Finalment, s'executarà el comando ldapadd que, per a completar el seu treball, necessitarà que ens autentiquem com a administradors del directori OpenLDAP. D'ací es veu que se'n demane la contrasenya.

Com abans, l'eixida del comando ldapadd ens confirmarà que la taverna s'ha completat amb èxit.



```
usuario@ldapserver: ~
Archivo Editar Ver Buscar Terminal Ayuda
usuario@ldapserver:~$ sudo ./importar-grupos.sh
administrador:x:1000:
usuario:x:1001:
Enter LDAP Password:
adding new entry "cn=administrador,ou=grupos,dc=empresa,dc=local"
adding new entry "cn=usuario,ou=grupos,dc=empresa,dc=local"
usuario@ldapserver:~$
```

Nota: Recorda que pots tornar a usar el comando slapcat per a assegurar-te que el contingut complet del directori és correcte.

12. CONFIGURAR UN EQUIP CLIENT AMB UBUNTU PER A AUTENTICAR-SE AL SERVIDOR OPENLDAP

En els apartats anteriors hem configurat el servidor OpenLDAP perquè seguisca capaç d'autenticar clients en la xarxa. Llaura a dalt la segona part de la taverna: Configurar els clients.

En aquest apartat ens centrarem en la configuració d'un client que està executant un sistema Ubuntu Desktop. Més endavant veurem com resoldre la taverna amb clients Windows.

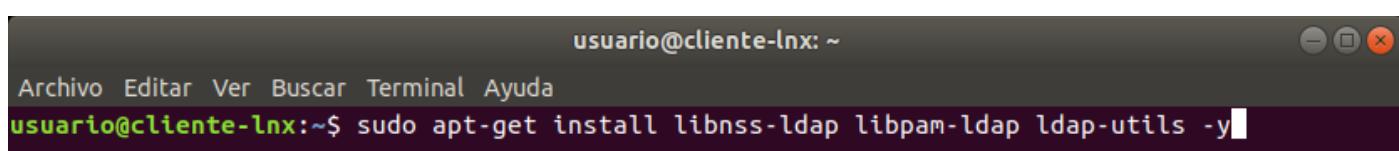
12.1. INSTAL·LAR ELS PAQUETS NECESSARIS

En Ubuntu, necessitarem ajustar el comportament dels serveis **NSS** i **PAM** en **cada client** que hagem de configurar. Comencem per instal·lar els següents paquets:

- **libnss-ldap**: Permetrà que NSS obtinga de LDAP informació administrativa dels usuaris (Informació dels comptes, dels grups, informació de la màquina, els àlies, etc.)
- **libpam-ldap**: Que facilitarà l'autenticació amb LDAP als usuaris que utilitzen PAM.
- **ldap-utils**: Facilita la interacció con LDAP dones de qualsevol màquina de la xarxa.

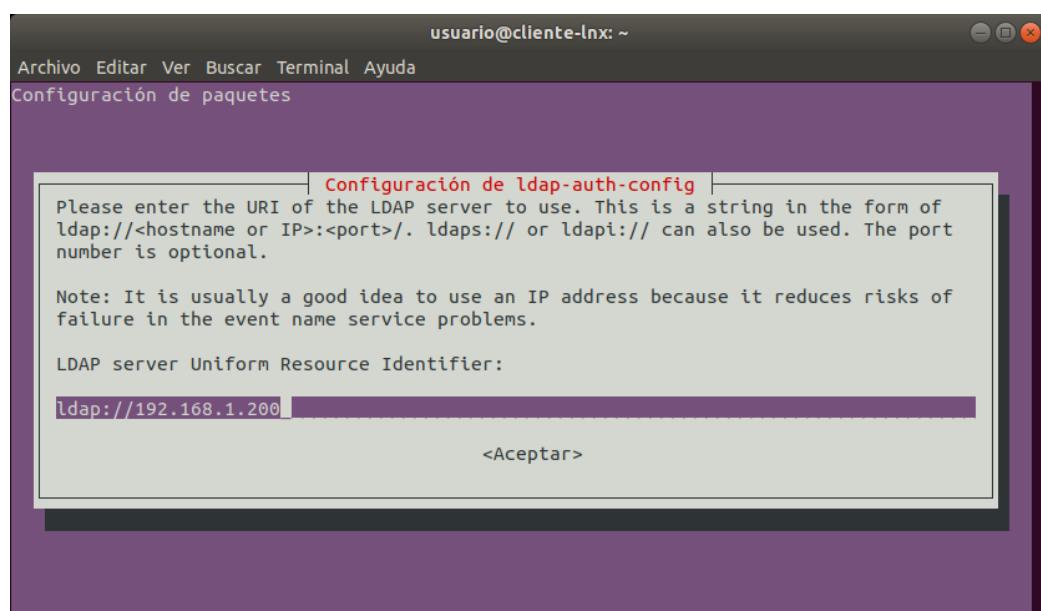
Per a instal·lar-los tots en una sola ordre, hem d'escriure el següent:

```
sudo apt-get install libnss-ldap libpam-ldap ldap-utils -y
```



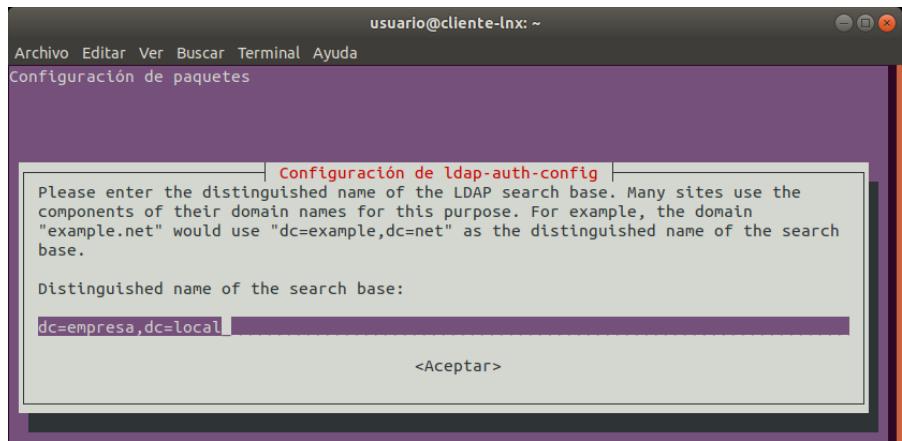
Nota: Acabem el comando amb **-y** perquè instal·le les dependències sense preguntar-nos.

Una dels dependències del paquet *libnss-ldap* és el paquet de configuració de l'autenticació de *LDAP* (*ldap-auth-config*). Durant la seu instal·lació s'iniciarà un assistent que ens anirà sol·licitant la informació que necessita per a la seu correcta configuració.

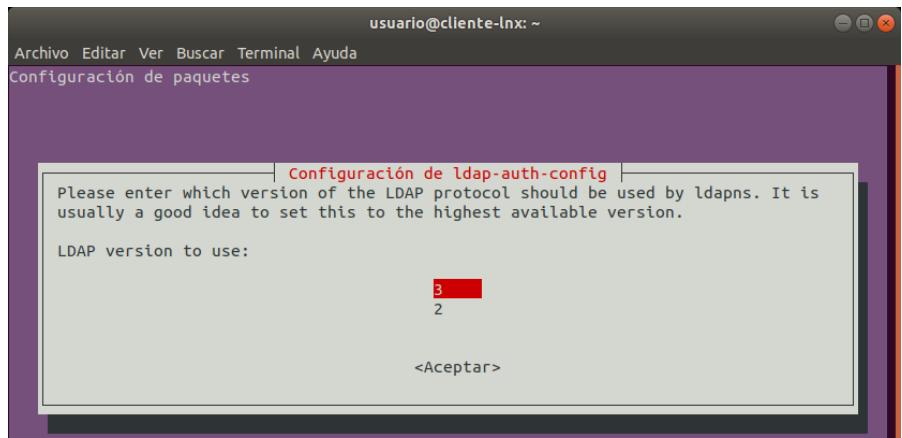


En el primer pas, ens sol·licita la direcció URI del servidor LDAP. En el nostre cas, escriurem l'adreça IP del servidor (en el nostre cas 192.168.1.200) i substituirem el protocol *ldapi:///* per *ldap://*.

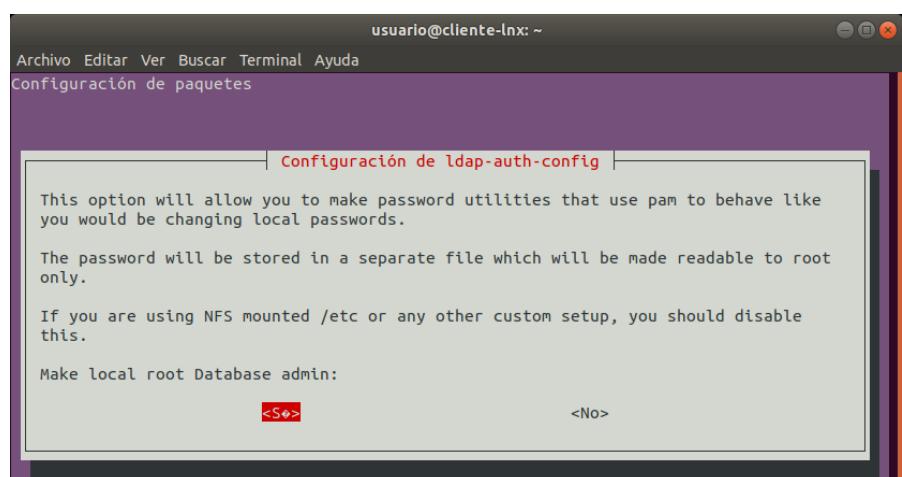
En el següent pas, cal indicar el nom global únic (Distinguished Name – DN). Inicialment apareix en valor dc=example,dc=net però nosaltres ho substituirem per dc=empresa,dc=local.



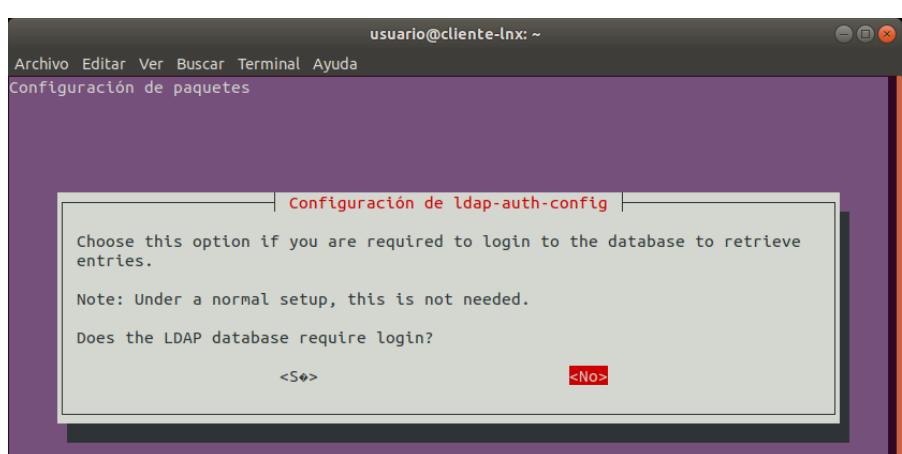
A continuació, l'assistent ens demana el número de versió del protocol LDAP que estem utilitzant. De manera predeterminada apareix seleccionada la versió 3. Ens limitem a prémer de nou la tecla Intro.



A continuació, indicarem si els utilitats que utilitzen PAM hauran de comportar-se de la mateixa manera que quan canviem contrasenyes locals. Això farà que els contrasenyes és guarden en un arxiu independent que només podrà ser llegit pel superusuari. Triem l'opció Si i premem la tecla Intro.



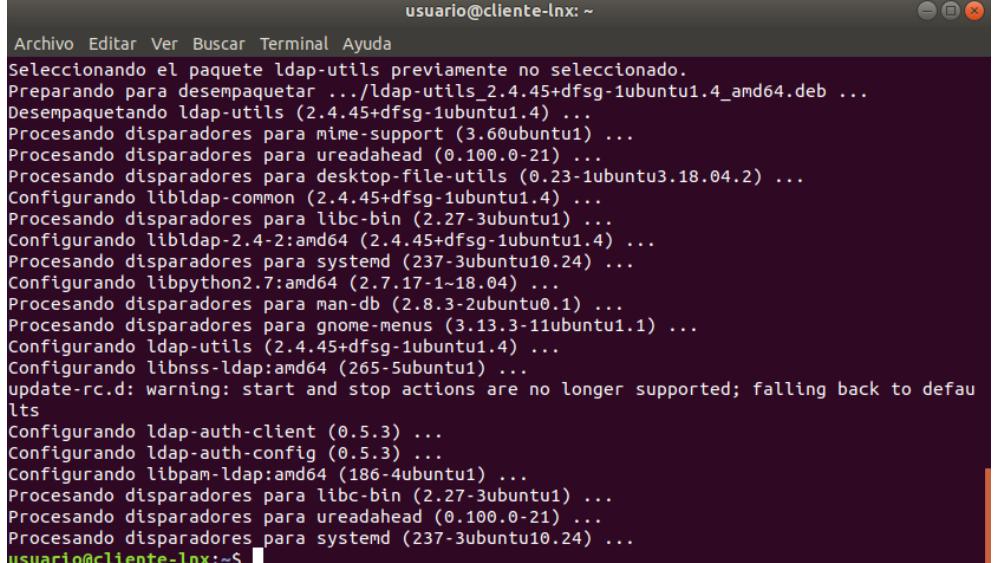
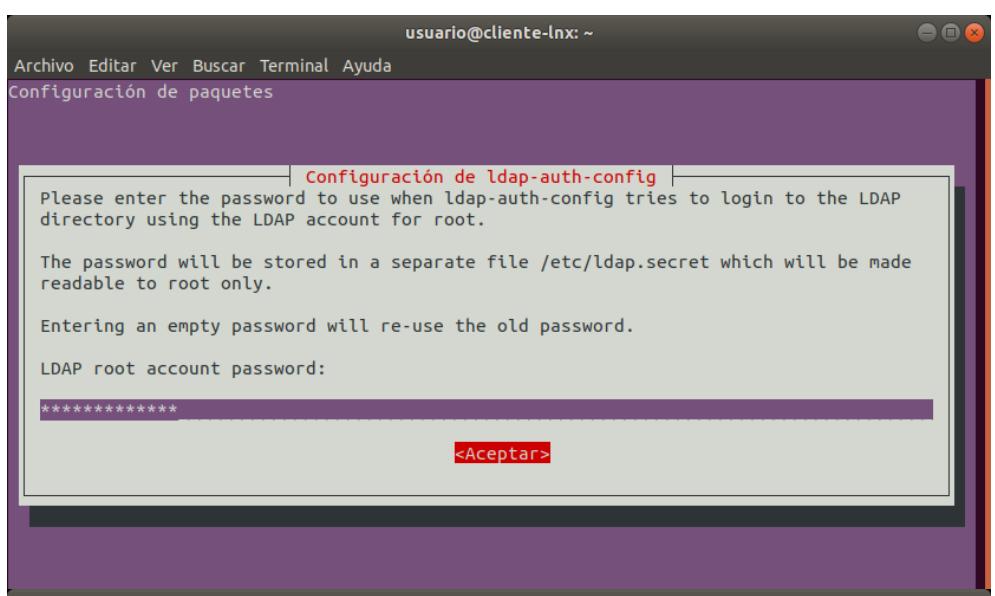
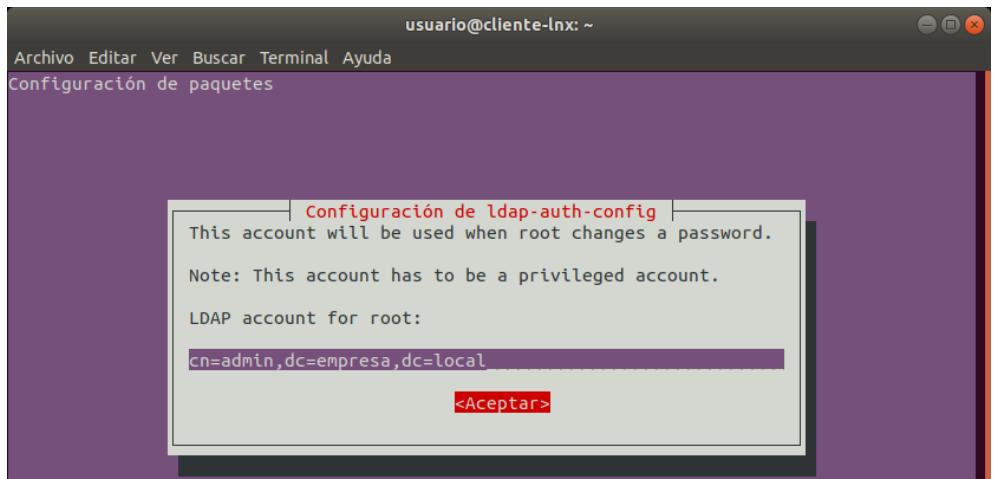
Després, el sistema ens pregunta si volem que siga necessari identificar-se per a realitzar consultes en la base de dades de LDAP. Triem l'opció No i tornem a prémer la tecla Intro.



Ja només ens queda indicar el nom del compte LDAP que tindrà privilegis per a fer canvis en els contrasenyes. Com abans, haurem d'escriure un nom global únic (Distinguished Name – DN), substituint el valor predeterminat que ens ofereix (cn=manager,dc=example,dc=net) perquè usem en la configuració del servidor (cn=admin,dc=empresa,dc=local). Després d'escriure el nom correcte, premem la tecla Intro.

En l'últim pas, l'assistent ens sol·licita la contrasenya que usará el compte anterior (com sempre, caldrà escriure-la per duplicat per a evitar errors tipogràfics). Haurà de coincidir amb la que escrivim en l'apartat Instal·lar OpenLDAP en el servidor. Quan acabem d'escriure la contrasenya, premerem la tecla Intro.

De tornada en la pantalla de la terminal, podrem comprovar que no s'han produït errors durant el procés. Amb això haurem acabat la configuració bàsica del client LDAP.



Com ocorria amb el servidor, si més endavant observem algun error o necessitem efectuar alguna modificació, només hem d'executar el següent comando:

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

12.2. REALITZAR AJUSTOS EN ELS ARXIUS DE CONFIGURACIÓ

Per a completar la taverna, haurem de canviar alguns paràmetres en els arxius de configuració del client. En concret, haurem d'editar /etc/nsswitch.conf, /etc/pam.d/common-password i /etc/pam.d/common-session. Així és que, per a no demorar-se'n més, comencem...

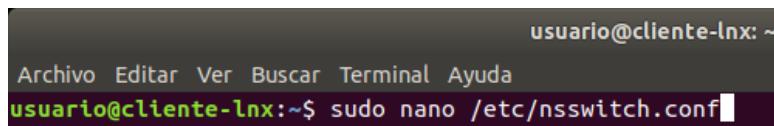
12.2.1. Editar l'arxiu /etc/nsswitch.conf

En l'arxiu /etc/nsswitch.conf s'inclouen els fonts dones dels quals s'obté la informació del servei de noms en diferents categories i en quina ordre. Cada categoria d'informació s'identifica sota un nom.

Com és habitual, l'arxiu està format per text pla. En ell trobarem columnes separades per espais o caràcters de tabulació. La primera columna indica l'emmagatzematge i, els restants, l'ordre dels orígens a consultar i un conjunt limitat d'accions a realitzar com a resultat de la consulta.

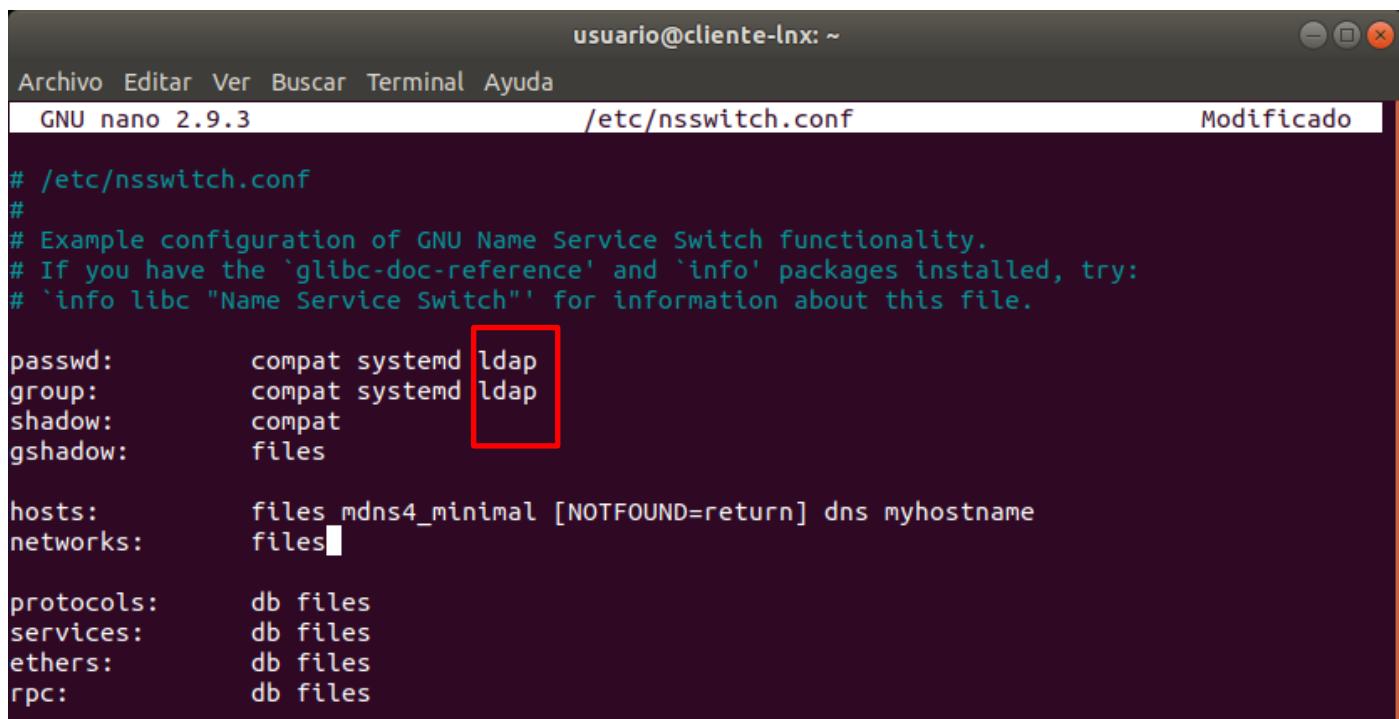
Per a editar l'arxiu, n'hi ha prou amb fer ús d'un editor de textos amb privilegis d'administració:

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



```
usuario@cliente-lnx: ~
Archivo Editar Ver Buscar Terminal Ayuda
usuario@cliente-lnx:~$ sudo nano /etc/nsswitch.conf
```

A continuació, localitzem els línies que comencen per passwd i group i els afegim el text ldap, per a indicar el nou origen per a autenticar els comptes. L'aspecte final de l'arxiu serà com en la imatge:



```
usuario@cliente-lnx: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.9.3          /etc/nsswitch.conf      Modificado
# /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 systemd ldap
group:       compat systemd ldap
shadow:      compat
gshadow:     files

hosts:        files mdns4_minimal [NOTFOUND=return] dns myhostname
networks:    files

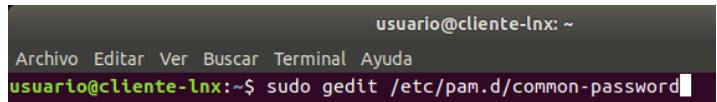
protocols:   db files
services:    db files
ethers:      db files
rpc:         db files
```

12.2.2. Editar l'arxiu /etc/pam.d/common-password

L'arxiu /etc/pam.d/common-password proporciona un conjunt comú de regles PAM per a la comprovació de contrasenyes. En particular, la línia 26 vaig comptar l'opció use_authok, que impedeix utilitzar un segon mètode d'autenticació quan ja ha sigut aplicat un altre anterior, encara que aquest haja sigut insatisfactori.

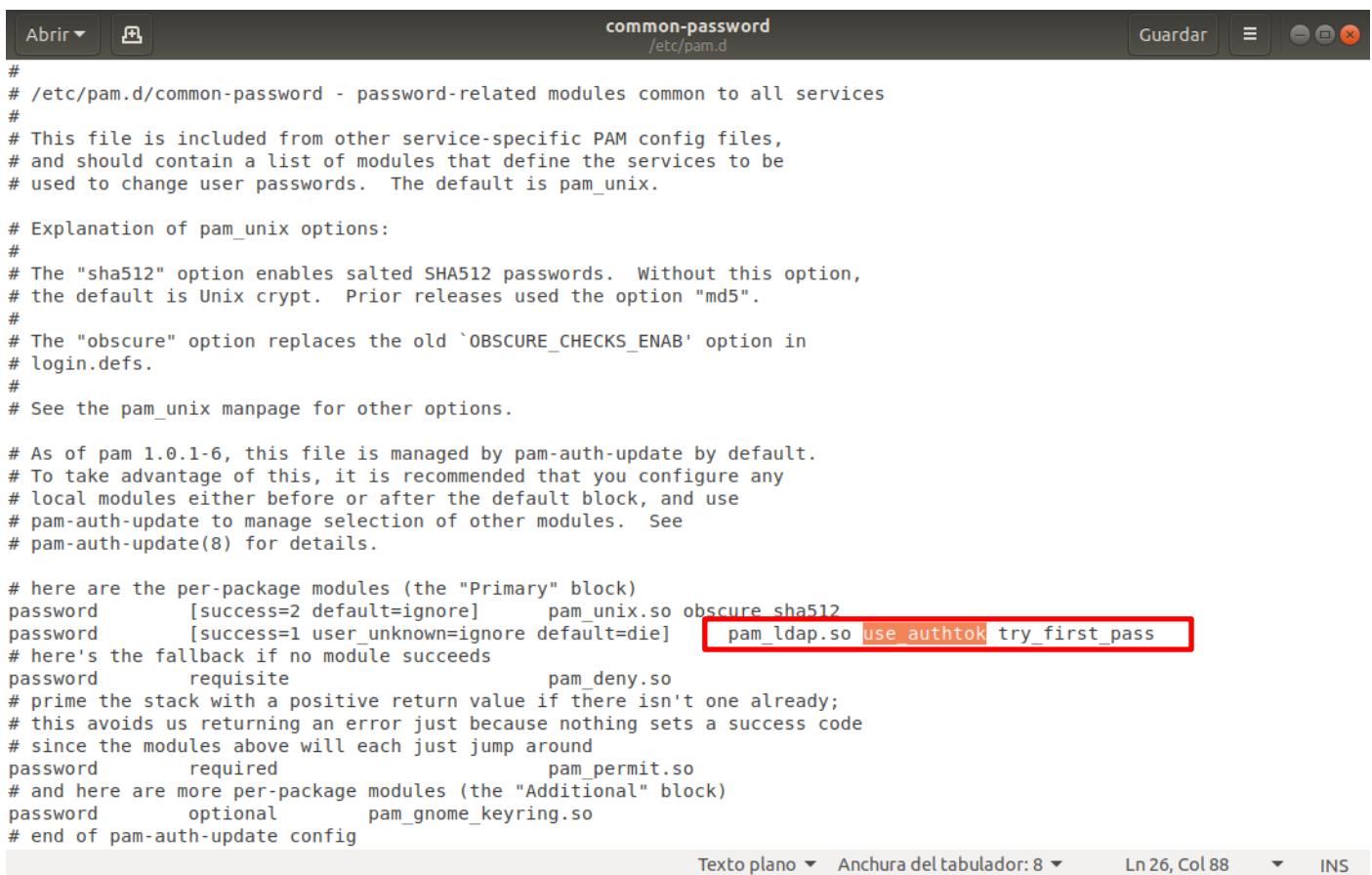
Per a evitar aquest comportament, haurem d'eliminar l'opció use_authok de la citada línia 26 de l'arxiu. Atés que en aquest cas l'arxiu també està construït amb text pla, tornarem a fer ús d'un editor de textos amb privilegis d'administració:

```
sudo gedit /etc/pam.d/common-password
```



```
usuario@cliente-lnx: ~
Archivo Editar Ver Buscar Terminal Ayuda
usuario@cliente-lnx:~$ sudo gedit /etc/pam.d/common-password
```

En la finestra de l'editor, localitzem la línia 26 i comprovem que vaig comptar l'argument **use_authok**.



```
common-password
/etc/pam.d

#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.

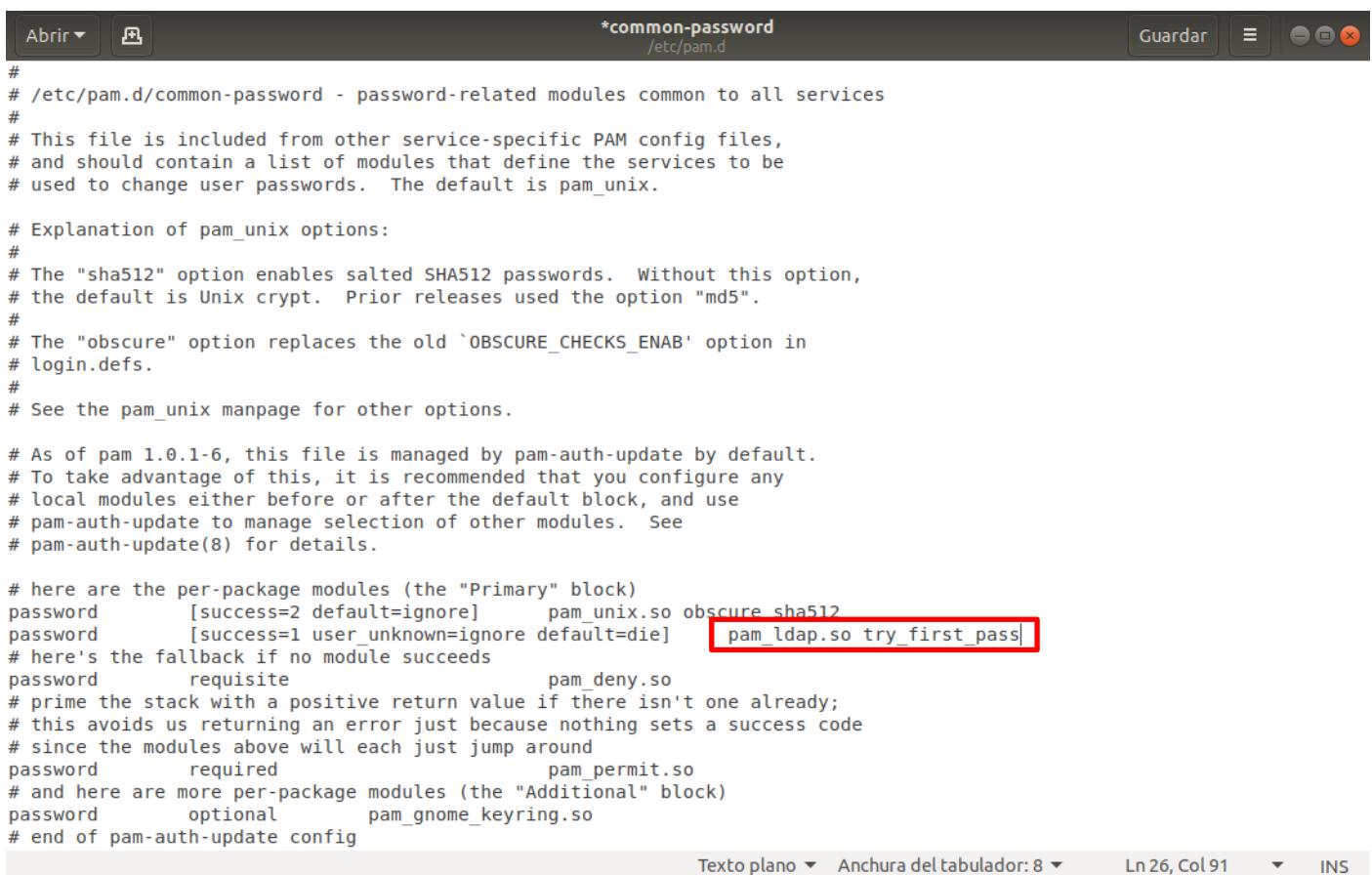
# Explanation of pam_unix options:
#
# The "sha512" option enables salted SHA512 passwords. Without this option,
# the default is Unix crypt. Prior releases used the option "md5".
#
# The "obscure" option replaces the old `OBSCURE_CHECKS_ENAB` option in
# login.defs.
#
# See the pam_unix manpage for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password      [success=2 default=ignore]      pam_unix.so obscure sha512
password      [success=1 user_unknown=ignore default=die]    pam_ldap.so use_authok try_first_pass
# here's the fallback if no module succeeds
password      requisite          pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password      required          pam_permit.so
# and here are more per-package modules (the "Additional" block)
password      optional          pam_gnome_keyring.so
# end of pam-auth-update config
```

Texto plano ▾ Anchura del tabulador: 8 ▾ Ln 26, Col 88 ▾ INS

Després d'eliminar-ho, ens assegurem de guardar els canvis.



```
*common-password
/etc/pam.d

#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.

# Explanation of pam_unix options:
#
# The "sha512" option enables salted SHA512 passwords. Without this option,
# the default is Unix crypt. Prior releases used the option "md5".
#
# The "obscure" option replaces the old `OBSCURE_CHECKS_ENAB` option in
# login.defs.
#
# See the pam_unix manpage for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password      [success=2 default=ignore]      pam_unix.so obscure sha512
password      [success=1 user_unknown=ignore default=die]    pam_ldap.so try_first_pass
# here's the fallback if no module succeeds
password      requisite          pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password      required          pam_permit.so
# and here are more per-package modules (the "Additional" block)
password      optional          pam_gnome_keyring.so
# end of pam-auth-update config
```

Texto plano ▾ Anchura del tabulador: 8 ▾ Ln 26, Col 91 ▾ INS

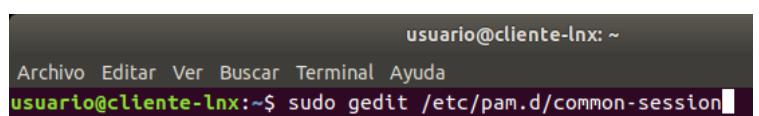
12.2.3. Editar l'arxiu /etc/pam.d/common-session

L'arxiu /etc/pam.d/common-session ofereix un conjunt de regles PAM per a l'inici de sessió, tant si aquest és interactiu com si és no interactiu. Ací serà on indiquem que s'ha de crear un directori home durant el primer inici de sessió, també per als usuaris autenticats mitjançant LDAP. Aquest comportament l'aconseguirem afegint al final de l'arxiu la següent línia:

```
session optional pam_mkhomedir.so skel=/etc/skel umask=077
```

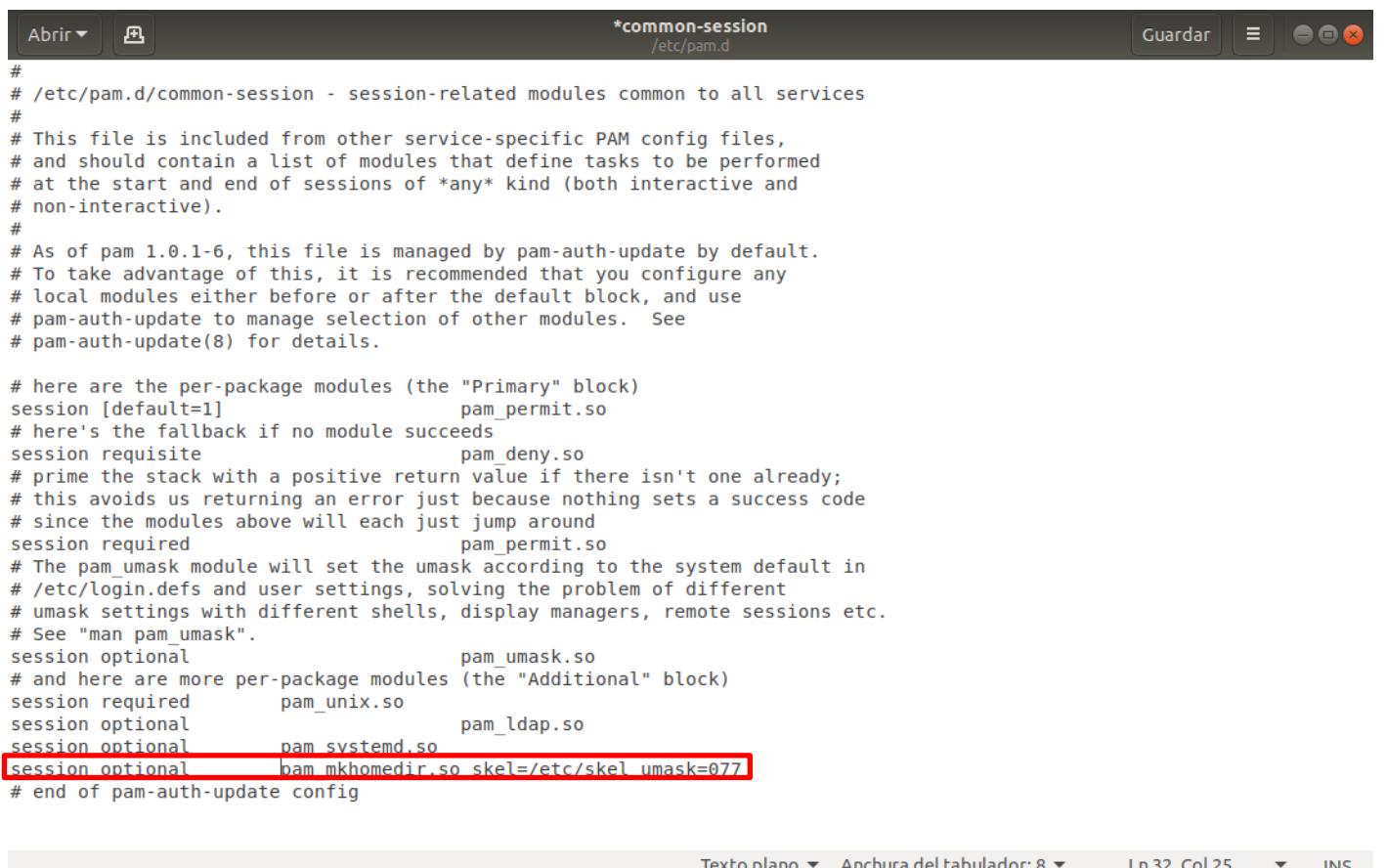
Com en els ocasions anteriors, usarem gedit amb privilegis d'administrador per a fer el canvi:

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



```
usuario@cliente-lnx: ~
Archivo Editar Ver Buscar Terminal Ayuda
usuario@cliente-lnx:~$ sudo gedit /etc/pam.d/common-session
```

Una vegada escrita, o copiada, la línia anterior al final de l'arxiu, guardem els canvis



```
*common-session
/etc/pam.d
#
# /etc/pam.d/common-session - session-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be performed
# at the start and end of sessions of *any* kind (both interactive and
# non-interactive).
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
session [default=1]          pam_permit.so
# here's the fallback if no module succeeds
session requisite           pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
session required             pam_permit.so
# The pam_umask module will set the umask according to the system default in
# /etc/login.defs and user settings, solving the problem of different
# umask settings with different shells, display managers, remote sessions etc.
# See "man pam_umask".
session optional             pam_umask.so
# and here are more per-package modules (the "Additional" block)
session required             pam_unix.so
session optional             pam_ldap.so
session optional             pam_systemd.so
session optional             pam_mkhomedir.so skel=/etc/skel umask=077
# end of pam-auth-update config
```

Texto plano ▾ Anchura del tabulador: 8 ▾ Ln 32, Col 25 ▾ INS

Una vegada completats tots els canvis, només queda **reiniciar l'equip**.

12.3. COMPROVAR QUE FUNCIONA L'INICI DE SESSIÓ

La forma més senzilla de comprovar que podem iniciar sessió en el servidor usant LDAP consisteix a arrancar el sistema en manera text (o arrancar-ho en manera gràfica i usar la combinació de tecles alt + ctrl + f1/f2/f3/f4/f5/f6 per a anar a una consola de text) i escriure els credencials d'un usuari LDAP.

Important: si la contrasenya de l'usuari té algun número, no has d'escriure aquests números amb el teclat numèric, és a dir, fes-ho amb els números que hi ha damunt dels lletres. Si no, et donarà error a validar l'usuari.

En aquesta imatge podem comprovar diverses cuses:

- Que ens trobem en l'equip client.
- Que estem iniciant sessió amb un usuari LDAP.
- Que durant l'inici de sessió és creat el directori /home per al compte.
- Que l'inici de sessió és produeix satisfactoriament.

```
Ubuntu 18.04.3 LTS cliente-lnx tty3
cliente-lnx login: jlopez
Password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 5.0.0-23-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

Pueden actualizarse 238 paquetes.
139 actualizaciones son de seguridad.

Your Hardware Enablement Stack (HWE) is supported until April 2023.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Creating directory '/home/jlopez '.
jlopez@cliente-lnx:~$ _
```

13. INICIAR SESSIÓ GRÀFICA EN L'EQUIP CLIENT AMB UN USUARI LDAP

En primer lloc, instal·larem el paquet nscd, que és un paquet de noms i accelerarà totes els operacions d'autenticació.

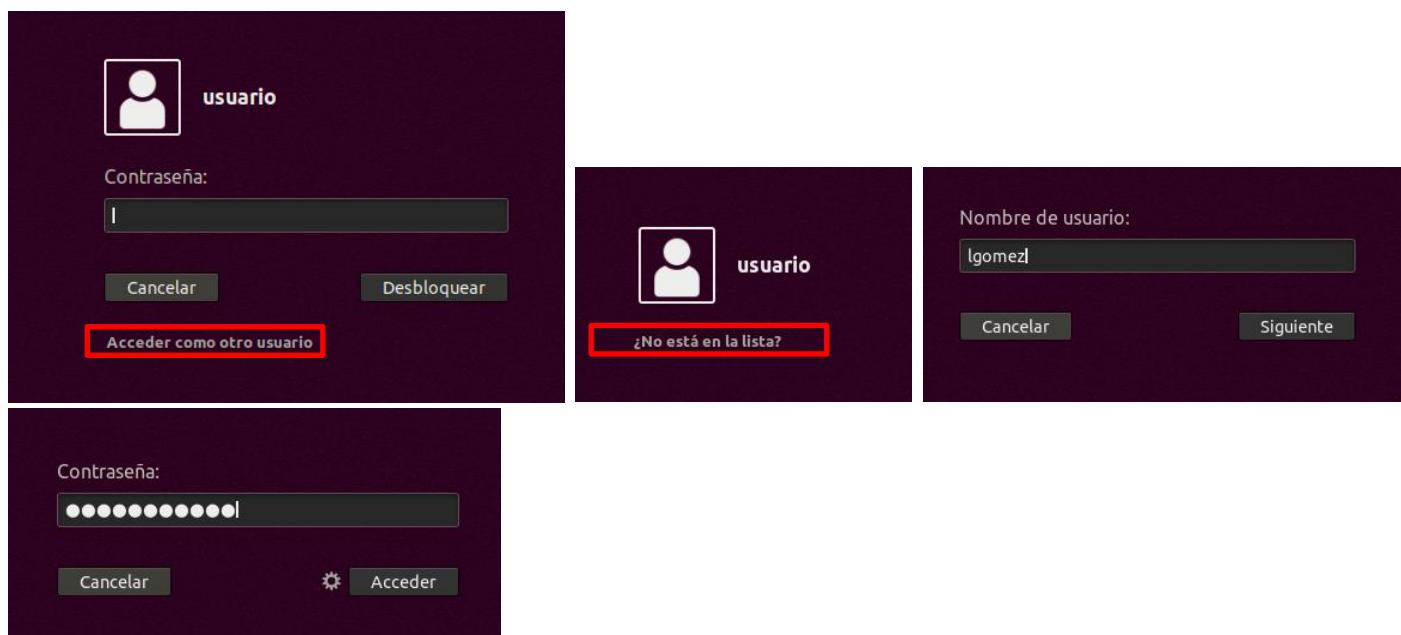
```
sudo apt-get install nscd
```

Reiniciem el servei nscd:

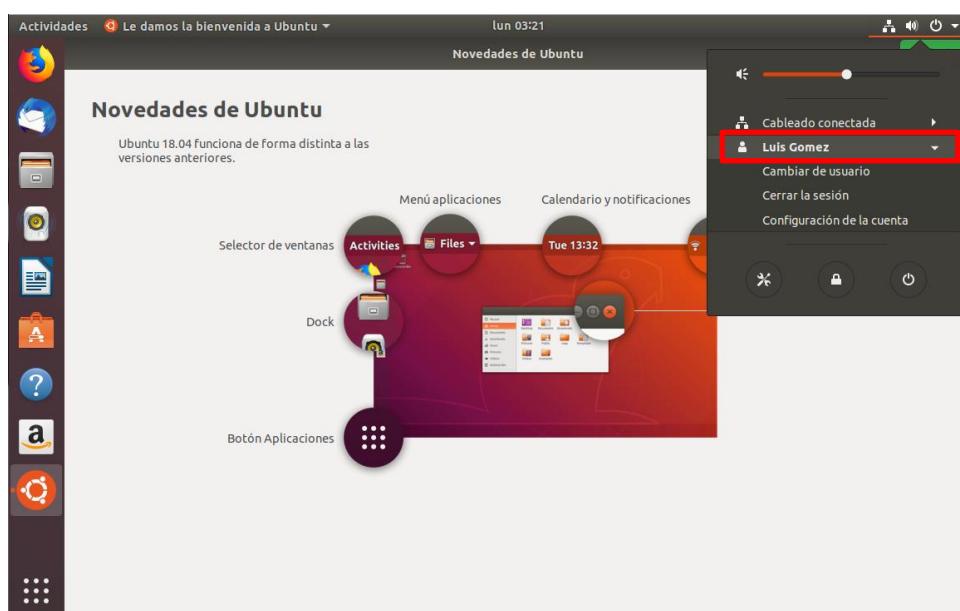
```
sudo /etc/init.d/nscd restart
```

I reiniciem l'equip.

A continuació, per a poder iniciar sessió amb els usuaris LDAP en la sessió gràfica, farem clic a “Accedir com un altre usuari” i seguidament en “No està en la llista?”. Escriurem el nom d'usuari (login) i la seu contrasenya.



Després d'uns segons veiem un missatge de creació del directori Home de l'usuari i s'accedeix al sistema.



A partir d'ara, cada vegada que iniciem sessió en el client, se'n oferirà el compte anterior entre el grup dels seus comptes coneguts, encara que podem tornar a triar un compte diferent, si és necessari.

14. INSTAL·LAR I CONFIGURAR LA INTERFÍCIE WEB LDAP ACCOUNT MANAGER PER A ADMINISTRAR OPENLDAP

Existeix un **client per a LDAP**, basat en una **interfície web**, que permet **administrar d'una forma senzilla un servidor LDAP** dones de qualsevol lloc, a través d'un senzill **navegador** d'Internet. Aquest client és **LDAP Account Manager**, encara que també és coneix de forma abreujada com **LAM**.

El projecte va ser creat en 2003 per Michael Dürchner, Roland Gruber, Til-Ler Lutz i Leonhard Walchshäusl amb l'objectiu d'administrar comptes d'usuaris, equips i grups sota els protocols POSIX i SAMBA. El resultat va ser LDAP Account Manager, un programari escrit en PHP que és va oferir a la comunitat informàtica sota llicència GPL.

Els avantatges que aporta són:

- Pot funcionar sobre qualsevol servidor web que suport PHP a partir de la versió 4.
- És compatible amb qualsevol navegador web en el costat client que suport CSS.
- Pot utilitzar-se amb OpenLDAP a partir de la versió 2.0.
- Pot utilitzar connexions sense xifrar o xifrades amb SSL.
- Pot exportar la informació dels comptes en format PDF.
- Pot crear nous comptes a partir d'arxius de text.

A més dels característiques anteriors, podem destacar els següents:

- Edició d'entrades a partir de plantilles.
- Còpies d'entrades d'un lloc a un altre, fins i tot entre diferents servidors.
- És capaç de copiar arbres complets de forma recursiva.
- Esborra entrades individuals i arbres complets.
- Voltes senzilles i avançades en el directori.
- etc.

Com és tracta d'una aplicació web, funciona perfectament en diferents plataformes, permetent-nos administrar el servidor LDAP dones de qualsevol lloc i dones de qualsevol sistema.

Nota: Pots obtindre més informació sobre LDAP Account Manager en la seua pàgina oficial (<http://sourceforge.net/projects/lam>) o en la Wikipedia (http://en.wikipedia.org/wiki/Ldap_account_manager).

14.1. INSTAL·LACIÓ DE LDAP ACCOUNT MANAGER

LDAP Account Manager és troba de manera predeterminada en els repositoris oficials d'Ubuntu LTS, per la qual cosa serà molt senzill instal·lar-ho.

L'única circumstància a tindre en compte són els dependències. Com és tracta d'una aplicació escrita en PHP, per a funcionar correctament necessita disposar d'un servidor LAMP instal·lat i actiu en el servidor.

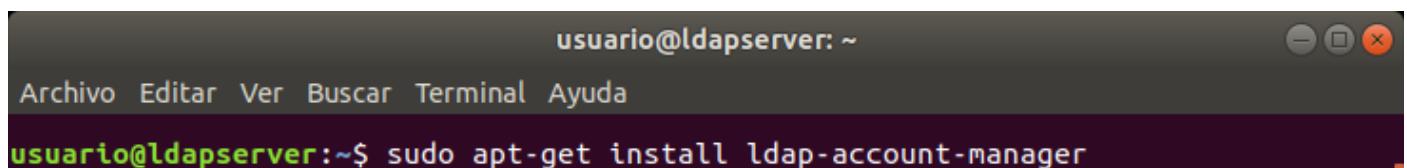
Nota: L'acrònim LAMP és refereix a una infraestructura web basada en els següents eines:

- *El sistema operatiu LINUX.*
- *El servidor web Apache.*
- *El gestor de bases de dades MySQL*
- *El llenguatge de programació PHP*

No obstant això, el procés d'instal·lació ens oferirà incloure'l's de manera automàtica, per la qual cosa el problema quedarà resolt implícitament. Fins i tot podem afegir l'opció -y a l'ordre d'instal·lació per a evitar fins i tot que ens pregunte.

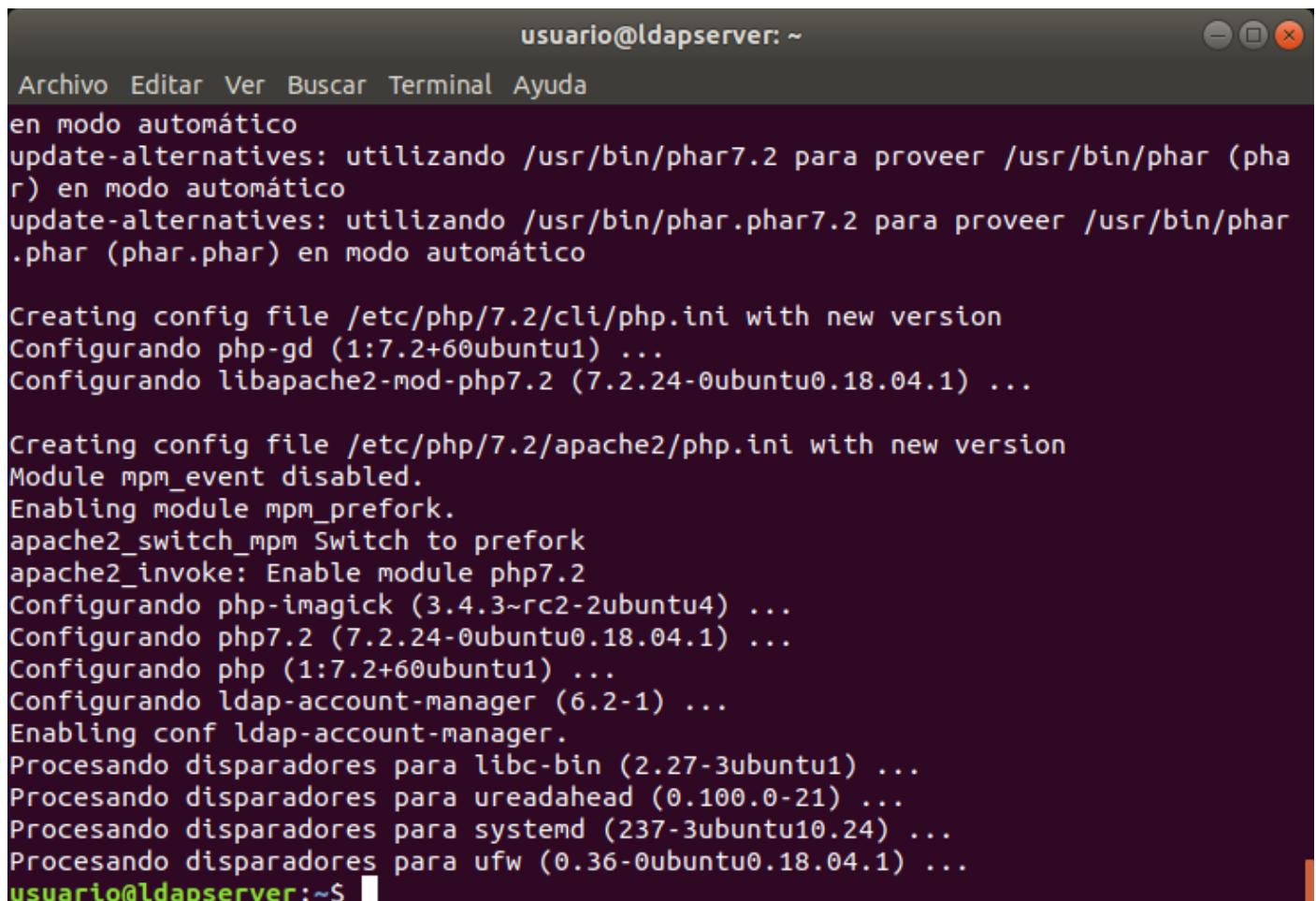
Per tant, obrirem la terminal i executarem el següent comand:

```
sudo apt-get install ldap-account-manager
```



A screenshot of a terminal window titled "usuario@ldapserver: ~". The window has a dark theme with white text. The menu bar includes "Archivo", "Editar", "Ver", "Buscar", "Terminal", and "Ayuda". The command "sudo apt-get install ldap-account-manager" is typed into the terminal and is highlighted in green.

Poc després, el programa estarà instal·lat.



A screenshot of a terminal window titled "usuario@ldapserver: ~". The window has a dark theme with white text. The terminal displays the output of the package installation process, which includes several configuration steps for PHP and Apache, and the successful installation of the "ldap-account-manager" package. The command "sudo apt-get install ldap-account-manager" is visible at the bottom.

```
usuario@ldapserver:~$ sudo apt-get install ldap-account-manager
...
Creating config file /etc/php/7.2/cli/php.ini with new version
Configurando php-gd (1:7.2+60ubuntu1) ...
Configurando libapache2-mod-php7.2 (7.2.24-0ubuntu0.18.04.1) ...

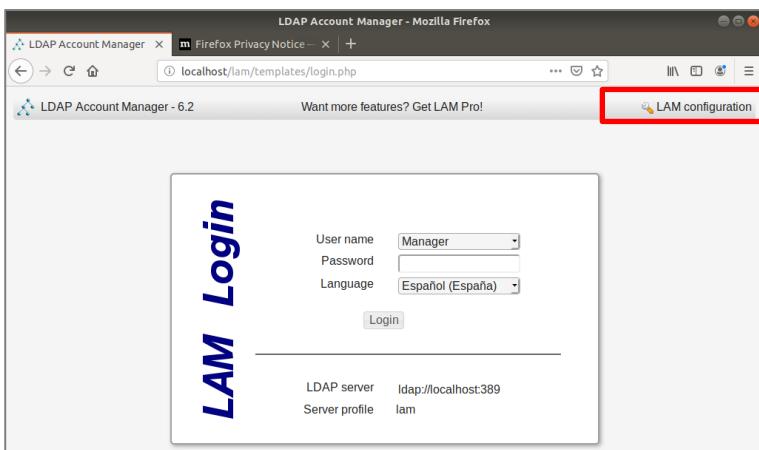
Creating config file /etc/php/7.2/apache2/php.ini with new version
Module mpm_event disabled.
Enabling module mpm_prefork.
apache2_switch_mpm Switch to prefork
apache2_invoke: Enable module php7.2
Configurando php-imagine (3.4.3~rc2-2ubuntu4) ...
Configurando php7.2 (7.2.24-0ubuntu0.18.04.1) ...
Configurando php (1:7.2+60ubuntu1) ...
Configurando ldap-account-manager (6.2-1) ...
Enabling conf ldap-account-manager.
Procesando disparadores para libc-bin (2.27-3ubuntu1) ...
Procesando disparadores para ureadahead (0.100.0-21) ...
Procesando disparadores para systemd (237-3ubuntu10.24) ...
Procesando disparadores para ufw (0.36-0ubuntu0.18.04.1) ...
usuario@ldapserver:~$
```

14.2. REALITZAR AJUSTOS PREVIS

Per a realitzar la configuració prèvia de LDAP Account Manager no és necessari editar cap arxiu de configuració. N'hi ha prou amb obrir el navegador i escriure en la barra d'adreses el següent:

```
http://localhost/lam
```

Això ens portarà a la pàgina inicial de LDAP Account Manager. Per a iniciar la configuració, n'hi ha prou amb fer clic sobre l'enllaç "LAM configuration".



Si prefereixes realitzar tot el procés en espanyol, has de fer clic sobre l'enllaç “LAM configuration” → “Edit server profiles” → escriure contrasenya per defecte: “lam” → pestanya “General settings”→ “Language settings”→ “Default language”: espanyol → clic en va botar “Save”.

The screenshot illustrates the configuration steps for the LDAP Account Manager (LAM) in Spanish. It shows the LAM login interface, the configuration overview, and the detailed configuration for the 'lam' server profile, specifically focusing on language settings.

Una vegada amb l'idioma adequat, tornarem a fer clic en “Configuració de LAM” i analitzarem els options disponibles:

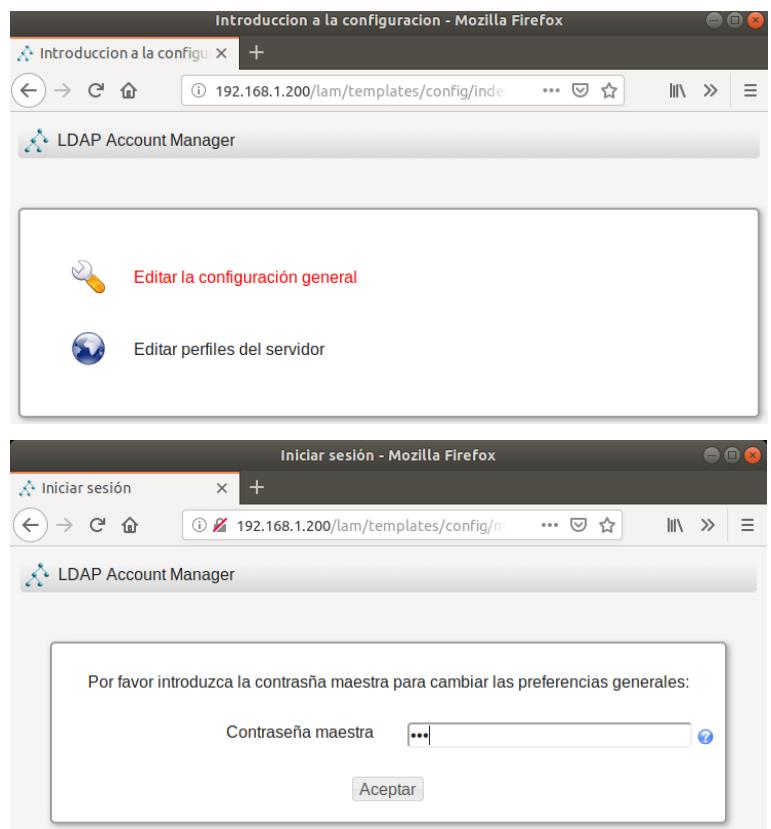
- Editar la configuració general.
- Editar perfils del servidor.

14.2.1. Editar la configuració general.

Començarem per “Editar la configuració general” per a establir el perfil del servidor.

Abans d'entrar en l'opció triada, LDAP Account Manager ens demana la contrasenya mestra. Aquesta contrasenya no està relacionada amb la que escrivim per a l'administració del directori OpenLDAP, sinó que és pròpia de LDAP Account Manager.

De manera predeterminada, el seu valor és lam, encara que haurem de canviar-la el més prompte possible.

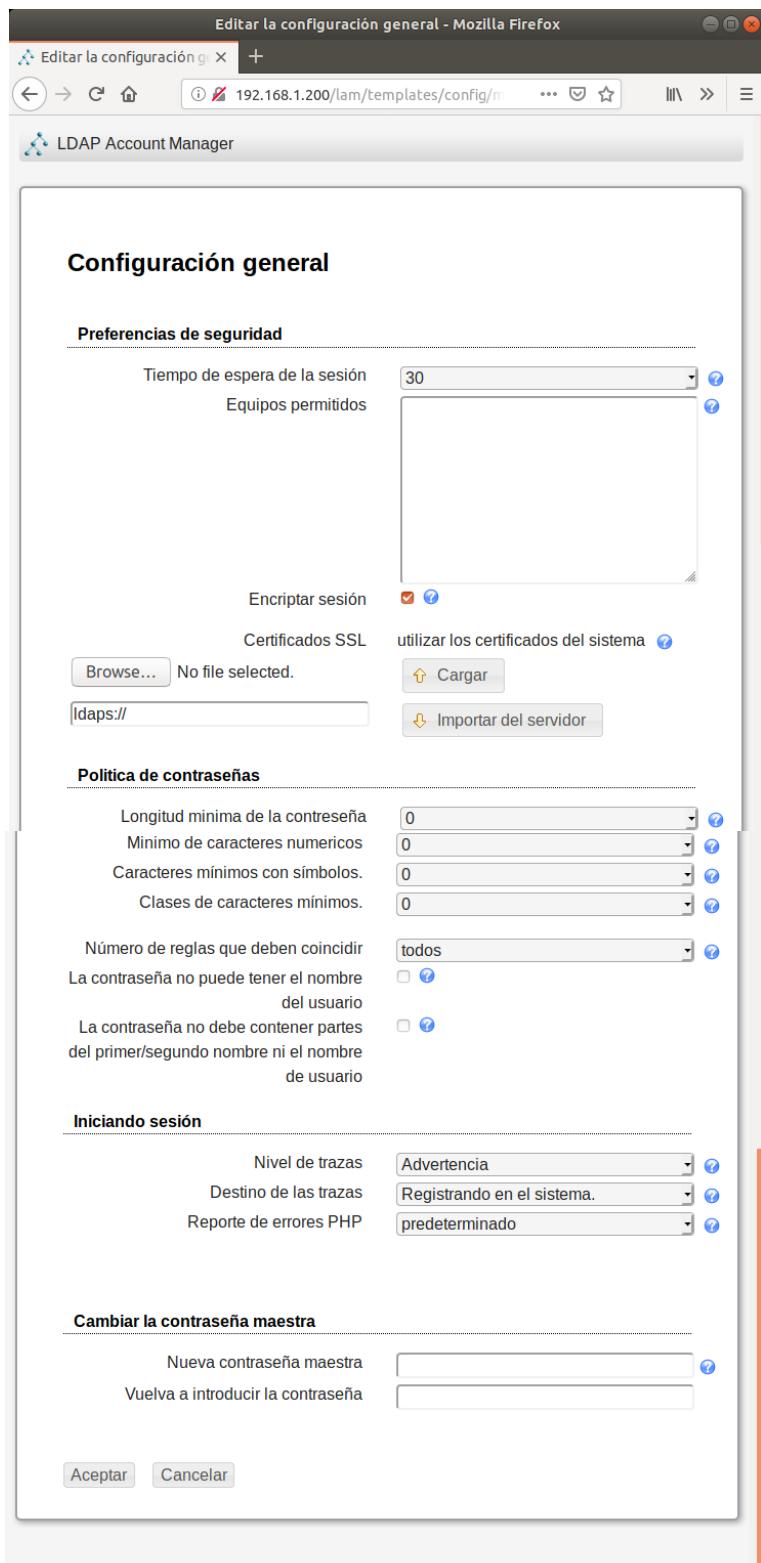


Així arribem a la pàgina Configuració general, que és divideix, al seu torn en quatre apartats diferents:

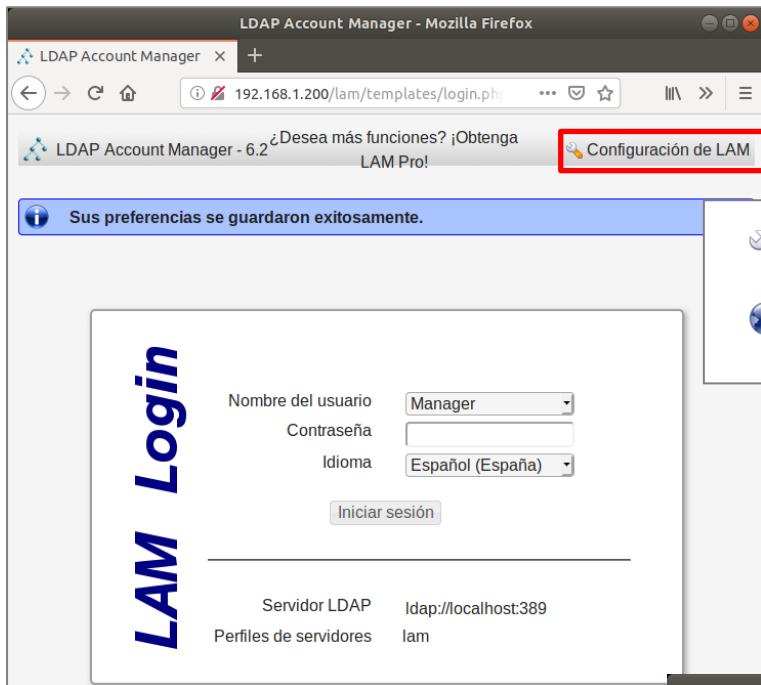
- “Preferències de seguretat”, on podem establir els següents valors:
 - Un límit de temps en el qual una sessió pot estar inactiva. Després d'aqueix període, és tancarà automàticament. Com pots veure, de manera predeterminada, el límit és de 30 minuts.
 - Una llista d'adreses IP dones dels quals és pot accedir a LDAP Account Manager. És poden establir rangs de valors usant el caràcter asterisc (*). Per exemple, 192.168.1.*.
 - Els certificats SSL que usarem, encara que de manera predeterminada s'utilitzen els certificats que tinguem preinstal·lats en el sistema.
- “Política de contrasenyes”, on podem indicar una política centralitzada per a els contrasenyes en LDAP Account Manager. Aquesta política serà vàlida en tots els camps de contrasenya dins de l'administrador LDAP Account Manager, excepte els contrasenyes de configuració.
- “Iniciant sessió”, que permet el seguiment d'esdeveniments de forma integrada amb el sistema (syslog en GNU/Linux o el Visor d'esdeveniments en Windows) o en un arxiu separat. Hem d'anar amb compte amb els arxius d'esdeveniments de LAM, perquè en el nivell d'Advertiment poden contindre informació sensible (com a contrasenyes). Per això, en un sistema en producció, hem de canviar el Nivell de traces a un valor diferent. Quant als errors que puga produir PHP, LDAP Account Manager els ignora de manera predeterminada i, en la majoria dels casos, aquesta serà l'opció apropiada.
- “Canviar la contrasenya mestra”, és l'opció que ens permet canviar la contrasenya mestra. No hem de deixar el valor predeterminat (lam), perquè és àmpliament conegut.

De moment, deixarem tots els valors predeterminats, excepte la contrasenya mestra. Pel que ens dirigim a la part inferior de la pàgina i l'escrivim (per duplicat, com és habitual, per a evitar els errors tipogràfics). Després, podem fer clic sobre el va botar Acceptar.

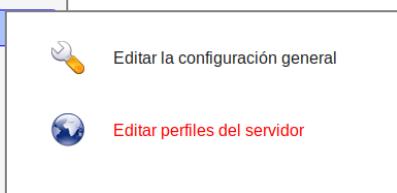
En fer-ho, tornarem a la pantalla principal.



14.2.2. Editar perfils del servidor.



Una vegada de tornada en la pantalla principal, el següent pas serà editar els perfils del servidor. Per a aconseguir-ho, haurem de tornar a la pàgina "Configuració de LAM".

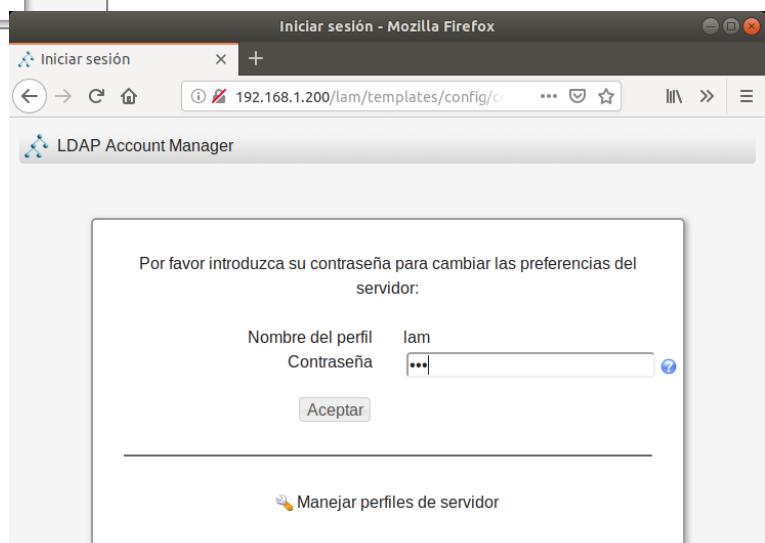


Com calç esperar, llaura farem clic sobre la segona opció: "Editar perfils del servidor". Els perfils

del servidor emmagatzemen informació sobre el servidor OpenLDAP i els característiques dels seus comptes. D'altra banda, no hi ha límit en el nom de perfils de servidor, encara que, com veurem, nosaltres ens centrarem en els valors predeterminats.

Com abans, per a entrar en l'opció triada, LDAP Account Manager ens demana la contrasenya mestra. Has de tindre en compte que el canvi de contrasenya que hem fet més amunt te efecte quan iniciem sessió la pròxima vegada pel que, si has seguit els passos que indiquem ací de manera consecutiva, hauràs de continuar usant la contrasenya predeterminada (lam), encara que la pròxima vegada que entres, ja hauràs d'usar la nova.

Escrivim la contrasenya i fem clic sobre el va botar Acceptar.



Així arribem a la pàgina Configuració dels perfils. Com pots veure, la pàgina és divideix en quatre solapes:

- “Configuració general”, que vaig comptar la informació global del servidor LDAP, com el nom de l’host o els característiques de seguretat.
- “Tipus de comptes”, on s’indiquen els diferents classes de comptes que administrarem, com a usuaris, grups o equips.
- “Mòduls”, que vaig comptar la llista de mòduls que defineixen els característiques dels comptes que administrarem (si són comptes Unix, Samba, Koalab, etc).
- “Preferències del mòdul”, que vaig comptar aspectes específics del mòdul que hagèm seleccionat en la pestanya anterior.

Ací ens centrarem només en els dues primeres.

Pestanya “Configuració general”

La pestanya Configuració general és divideix en els següents àrees:

- Preferències del servidor
- Configuració de l’idioma
- Preferències de lamdaemon
- Configuració d’eines
- Preferències de seguretat

Anirem explicant el contingut de cadascuna d’elles dobles segons anem avançant.

Contingut complet de la pestanya Configuració general:

En l'apartat “Preferències del servidor” haurem de completar els següents dades:

- Direcció del servidor: Com el servidor OpenLDAP és troba en el mateix equip que LDAP Account Manager, ens limitarem a deixar el valor predeterminat (`ldap://localhost:389`).
- Activar TLS: TLS són els sigles de Transport Layer Security (Seguretat de la capa de transport). Com llaura com llaura no utilitzarem connexions xifrades, mantenim el valor predeterminat (no).
- Sufix de l'arbre: LDAP Account Manager inclou un navegador per a LDAP. Si volem fer modificacions de manera directa en ell, haurem d'incloure **ací el sufíx que use el nostre arbre**. Per al nostre exemple, serà aquest: `dc=empresa,dc=local`.
- Límit de prop LDAP: Permet reduir els resultats d'una a prop quan tenim un directori molt extens. En el nostre cas, el deixarem desactivat.

En l'apartat “Configuració de l'idioma”, triem l'idioma per a aquest perfil de servidor. En el nostre cas triem, lògicament, l'idioma “Español”.

Completem els dades i continuem avançant per la pàgina.

LDAP Account Manager només pot manejar carpetes personals (home) i quotes mitjançant scripts externs. L'apartat “Preferències de lamdaemon” ens permet indicar qui és el servidor per als carpetes personals i on és troba el script que administra els quotes. També permet establir els permisos predeterminats per als carpetes personals dels nous usuaris.

L'apartat “Configuració d'eines” ens permet indicar si utilitzarem algunes dels eines que és relacionen:

- Editor de PDF (PDF editor): Si ho habilitem, podrem exportar la informació dels comptes en arxius PDF. A més, podrem editar els perfils PDF per a indicar l'estructura de la pàgina i la informació inclosa.
- Editor d'OU (OU editor): És tracta d'un senzill editor que ens permetrà afegir o portar Unitats Organitzatives del nostre arbre LDAP.
- Informació del servidor (Server information): Ens mostrarà informació i estadístiques relacionades amb el servidor LDAP.

- Comprovar (Tests): Permet verificar si l'esquema LDAP que estem usant és compatible amb LDAP Account Manager, indicant els possibles problemes.
- Explorador d'esquemes (Schema browser): permet examinar l'esquema del servidor LDAP, obtenint els tipus de classes, atributs, sintaxi i regles que hi ha disponibles.
- Editor de perfils (Profile editor): Vaig comptar plantilles per als comptes. Amb ell, és podran indicar valors predeterminats que s'utilitzaran durant la creació de comptes.
- Multi edit: Facilita la modificació per lots d'un gran nomene d'entrades LDAP, afegint o llevant atributs o assignant-los valors específics.
- Enviar arxius (File upload): Ens permet crear els comptes mitjançant un senzill editor de textos, usant format CVS, i després incloure'ls totes alhora en l'arbre LDAP pujant l'arxiu

Encara que pot ser molt interessant habilitar algunes d'aquestes opcions, de moment ho deixarem tot en blanc.

En l'apartat “Preferències de seguretat”, disposarem de dos mètodes d'inici de sessió: Llista fixada i A prop LDAP.

- Si triem Llista fixada, haurem d'especificar un o diversos usuaris (un en cada línia). Per cadascun d'ells, escriurem el seu nom global únic (Distinguished Name – DN) seguint els indicacions que vam veure al principi d'aquest tema (per exemple, cn=admin,dc=empresa,dc=local).
- Per part seua, triant A prop LDAP farem que LDAP Account Manager busque un DN en el directori a partir d'un nom d'usuari.

En el nostre cas, triarem la primera opció.

Finalment, també podrem canviar la contrasenya d'aquest perfil de servidor, escrivint-la per duplicat en els dues últims camps d'aquesta pàgina.

Llaura, podem fer clic sobre el va botar “Guardar” o continuar configurant la pestanya “Tipus de comptes”.

Pestanya “Tipus de comptes”

LDAP Account Manager admet diferents tipus d'entrades LDAP i, en aquesta pestanya, tenim l'oportunitat d'indicar necessitem administrar nosaltres en particular. La pestanya “Tipus de comptes” és divideix només en dues àrees:

- Tipus de comptes disponibles
- Tipus de comptes actius

Contingut complet de la pestanya “Tipus de comptes”:

A continuació veurem el contingut d'ambdues:

- La secció “Tipus de comptes disponibles” mostra una llista dels possibles tipus de comptes. Podem activar qualsevol d'ells fent clic en el signe més que hi ha al costat de cadascun d'ells.
- La secció “Tipus de comptes actius” vaig comptar els tipus de comptes que és troben vigents en el nostre sistema. En cadascun d'ells, podrem configurar diferents opcions, encara que nosaltres ens limitarem als bàsiques:
 - Sufix LDAP: Com calç esperar, ha de contindre el sufíx LDAP per a cada entrada d'aquest tipus
 - Atributs del llistat: Representa la llista d'atributs que és mostraren en el llistat de comptes.

En particular, per a aquest exemple, podem limitar-nos a escriure el sufíx per a cadascun dels tipus de comptes que manejarem. En el nostre cas seran els següents:

- Per a la mena de compte Usuaris, escriurem el sufíx ou=usuari,dc=empresa,dc=local
- Per a la mena de compte Grups, escriurem el sufíx ou=grups,dc= empresa,dc=local

Com pots suposar, els valors concrets dependran de l'estructura del directori que hem creat en la primera part d'aquest capítol.

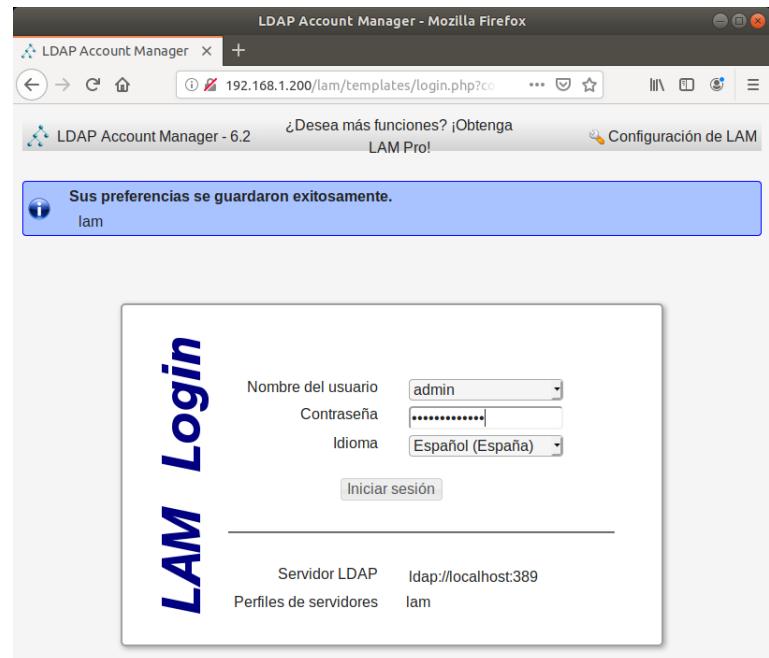
Quan hagèm conclòs, fem clic sobre el va botar Guardar que trobem al final de la pàgina. En fer-ho, tornarem a la pantalla principal.

The screenshot shows the configuration interface for LDAP Account Manager. The 'Tipos de cuentas' tab is active. In the 'Tipos de cuentas disponibles' section, various account types are listed with green plus icons. In the 'Tipos de cuentas activos' section, two specific configurations are shown for 'Usuarios' and 'Grupos'. Each configuration includes fields for 'Sufijo LDAP' (highlighted with a red box), 'Atributos del listado', 'Etiqueta personalizada', 'Filtro LDAP adicional', and an 'Oculto' checkbox. The 'Guarda' button is visible at the bottom.

15. USAR LDAP ACCOUNT MANAGER PER A GESTIONAR USUARIS I GRUPS EN EL SERVIDOR OPENLDAP

Una vegada que hagim completat els preferències de l'apartat anterior, tindrem LDAP Account Manager llest per a començar a usar-lo. Lògicament, el primer que haurem de fer en la pàgina principal serà autenticar-se'n. Observa que, de manera predeterminada, el nom d'usuari serà el que hagim definit com a administrador en el nostre directori LDAP.

Només hem d'escriure la contrasenya i fer clic sobre el va botar Iniciar sessió.



En fer-ho, obtenim una pàgina on s'observen diverses solapes, una per cada categoria de la relació Tipus de comptes actius que configurem en l'apartat anterior.

15.1. COMPTES D'USUARI

Per a administrar els comptes d'usuari en LDAP Account Manager, només hem de tindre activa la pestanya “Usuaris”.

En la pestanya “Usuaris” és mostra una relació amb els diferents comptes d'usuari disponibles en el directori. Dones d'aquesta pantalla podem realitzar diferents accions i, encara que no els expliquem totes, sí que esmentarem els més importants:

- El va botar “Nou usuari” ens permet crear nous comptes d'usuari en el directori LDAP. Veurem com funciona més a baix.
- El va botar “Eliminar els usuaris seleccionats”, com pot suposar-se, esborra del directori LDAP els comptes que indiquem. Per a seleccionar un compte, n'hi ha prou amb activar la casella de verificació que hi ha al principi de cada línia. També tenim una opció al final de la llista que permet Selecció tots alhora.
- Davall de cada títol de columna trobem un quadre de text que ens permet escriure una part del contingut d'aquesta columna. D'aquesta manera creem un filtre en el qual només és mostraren els elements que continguin el text escrit. Una cosa molt útil quan el nom de comptes que estem administrant és molt elevat.
- Finalment, al principi de cada línia disposem d'una icona que ens permet editar (modificar) el compte corresponent () o fins i tot esborrar-la ().

Contingut de la pestanya “Usuaris”:

Nombre del usuario	Nombre	Apellido	Número UID
administrador	administrador	administrador	1000
jbaeza	Juanjo	Baeza	10000
jlopez	Juan	Lopez	2000
lgomez	Luis	Gomez	2001
msoler	Mar	Soler	2002
usuario	usuario	usuario	1001

Si fem clic en el va botar “Nou usuari” accedim a la pàgina on podem ingressar els dades per a un nou compte. Ací veurem que els dades és diferencien en diferents categories que podem veure classificades a l'esquerra: Personal, Unix i Ombra (shadow).

Per al nostre exemple, només caldrà centrar-nos en els dues primeres:

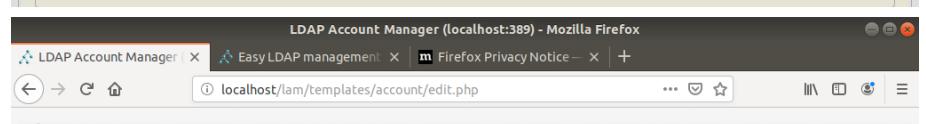
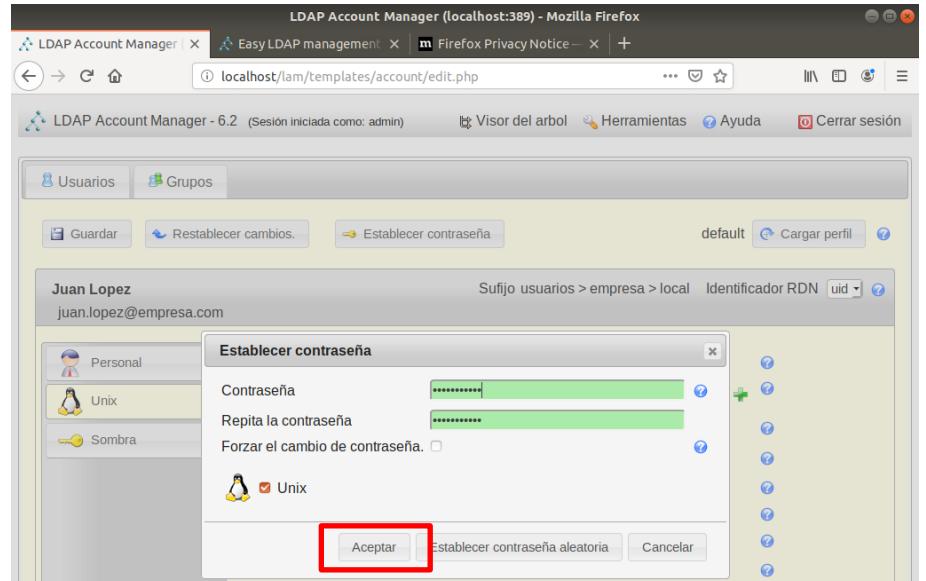
- En la categoria “Personal” introduirem els dades generals que defineixen el compte: El seu nom complet, els seus cognoms, els seus inicials, la seua adreça física, i moltes altres dades. És important tindre clar que només hem d'emplenar els que ens resulten imprescindibles. Introduïm els noves dades en la categoria “Personal”:
- En la categoria “Unix” inclourem els dades específiques del compte, com el seu UID, la seua carpeta home, l'intèrpret de comandos que usrà, etc. Escrivim els dades específiques del compte.

Nombre del usuario*	jlopez
Nombre común	Juan Lopez
Número UID	2000
Gecos	Juan Lopez
Grupo primario	SMR2
Grupos adicionales	Editar grupos
Directorio inicial*	/home/jlopez
Intérprete del inicio de sesión	/bin/bash
Contraseña	Bloquear contraseña Quitar contraseña

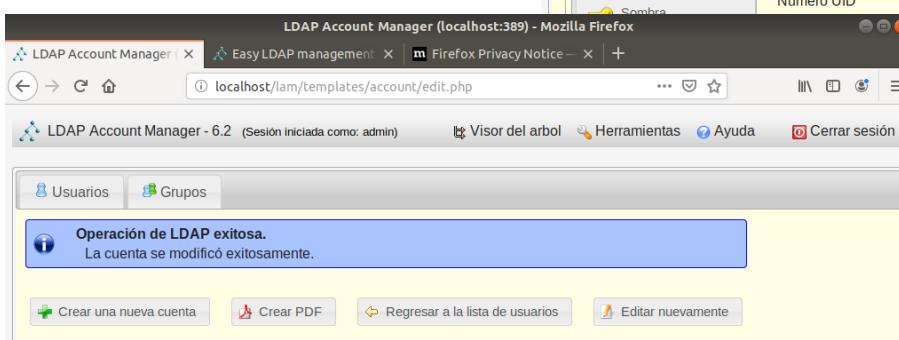
A més, disposem del va botar “Establir contrasenya” que ens permetrà fixar el valor inicial que tindrà la contrasenya per al compte d’usuari que estem creant. També podem establir que seguisca obligatori canviar la contrasenya en el primer inici de sessió i si la contrasenya serà vàlida per als diferents perfils de compte que tinguem definits (en aquest cas, Unix).

Nota: Encara que en l'exemple hem escrit el contingut per a UID, podem deixar-l'en blanc perquè LDAP Account Manager li assigne el primer valor disponible.

Escrivim la contrasenya i fem clic sobre el va botar Acceptar.



Quan hagem establit el valor de la contrasenya, estarem llestos per a acabar la creació del compte. Fem clic sobre el va botar “Guardar”.



Si més endavant necessitem fer algun canvi sobre els dades que acabem d'introduir, bastarà amb fer clic sobre el seu va botar “Editar” en la pestanya “Usuaris” i tornarem a obtindre una pàgina similar a la que usem per a crear els comptes, només que amb valors inicials.

15.2. COMPTES DE GRUPS

La pestanya Grups ens ofereix un aspecte molt semblant al d'Usuaris i vaig comptar pràcticament els mateixos components, per la qual cosa el seu ús és pràcticament idèntic a l'estudiat més amunt

Aspecte de la pestanya “Grups”:

LDAP Account Manager (localhost:389) - Mozilla Firefox

LDAP Account Manager | Easy LDAP management | Firefox Privacy Notice | +

localhost/lam/templates/lists/list.php?type=group

LDAP Account Manager - 6.2 (Sesión iniciada como: admin) Visor del arbol Herramientas Ayuda Cerrar sesión

Usuarios Grupos

Nuevo grupo Eliminar los grupos seleccionados Enviar archivos grupos > empresa > local

Conteo de grupos: 3

Seleccionar todos	Nombre del grupo	Número GID	Miembros del grupo	Descripción del grupo
<input type="checkbox"/>				
<input type="checkbox"/>	administrador	1000		
<input type="checkbox"/>	SMR2	10000		
<input type="checkbox"/>	usuario	1001		
↑ Seleccionar todos				

Per exemple, si fem clic sobre el va botar “Nou grup”, obtindrem una pàgina com la de la següent imatge, on, a més del panell principal, tornem a disposar a l'esquerra d'una àrea que mostra els categories (Unix, Samba 3...).

En el nostre cas, només tenim un, per la qual cosa únicament emplenarem els dades de la categoria “Unix”.

LDAP Account Manager (localhost:389) - Mozilla Firefox

LDAP Account Manager | Easy LDAP management | Firefox Privacy Notice | +

localhost/lam/templates/account/edit.php?type=group&suffix=ou=grupos>empresa>local

Visor del arbol Herramientas Ayuda Cerrar sesión

Usuarios Grupos

Guardar Establecer contraseña default Cargar perfil

Nuevo grupo Sufijo grupos > empresa > local Identificador RDN cn

Unix	Nombre del grupo *		?
	Número GID		?
	Descripción		?
	Miembros del grupo	Editar miembros	?

Quan hagem acabat d'escriure els dades, només hem de fer clic sobre el va botar “Guardar”.

Nota: Com en el cas anterior, podrem deixar en blanc el valor per al GID i LDAP Account Manager l'assignarà de manera automàtica.

16. PERFILS MÒBILS D'USUARI USANT NFS I LDAP

En molts contextos de xarxa, l'apartat anterior pot plantejar més dubtes que solucions, ja que un usuari que vaja itinerant entre diversos equips client acabarà tenint una carpeta per al seu perfil en cadascun dels equips i el seu contingut no se sincronitza! És a dir, si crea un arxiu en el client A, no el trobarà en la seua carpeta quan inicie sessió dones del client B. El motiu és que LDAP només s'encarrega d'autenticar als usuaris.

No obstant això, en el tema anterior vam aprendre a compartir dades entre el servidor i els clients a través de NFS.

En aquest apartat, aprendrem a unir els possibilitats d'autenticació **centralitzada en el servidor que ofereix LDAP amb la capacitat d'emmagatzematge centralitzat que aporta NFS**. El resultat seran els **perfils mòbils** d'usuari. És a dir, un usuari trobarà la seua carpeta personal (l'equivalent a /home/usuari) en tots els equips client on inicie sessió.

Els tasques que haurem de completar per a resoldre-ho són aquestes:

1. Crear una carpeta en el servidor per a guardar la carpeta /home dels usuaris mòbils (l'equivalent a /home/usuari de cada usuari en el servidor). En aquest exemple, en lloc de la carpeta /home crearem una específicament per a perfils mòbils a la qual anomenarem /moviles.
2. Modificar l'arxiu /etc/exports per a compartir el directori anterior amb permisos de lectura/escriptura per a tots els usuaris.
3. Crear una carpeta en els equips client per a muntar els perfils mòbils (l'equivalent a /home/usuari de cada usuari en cada client). Per a aquest exemple, la carpeta dels clients també és dirà /moviles, encara que no és necessari que el seu nom coincidís amb el de la carpeta que crearem per al punt q.
4. Modificar l'arxiu /etc/fstab de cada client perquè munte la carpeta que hem creat en el pas 1 en el punt de muntatge establert en el pas 3 i reiniciar l'equip.
5. Modificar els comptes d'usuari LDAP per a indicar que la carpeta on han de tindre el seu perfil és troba dins de la carpeta creada en el pas 3 (la que muntem en el client).

Bé, ara que ja tenim clars els passos que hem de donar, comencem...

16.1. CREAR UNA CARPETA PER A GUARDAR ELS PERFILS MÒBILS EN EL SERVIDOR

En realitat, ja hem vist com fer aquesta taverna dins de l'apartat “Configurar el servidor NFS” del tema anterior (Instal·lar i configurar NFS en Ubuntu). Per tant, només hem de seguir els indicacions del punt “Crear els carpetes a compartir” i “crear una nova carpeta”.

Ací, crearem una nova carpeta anomenada /moviles:

```
sudo mkdir /moviles  
sudo chown nobody:nogroup /moviles
```

Creem la carpeta i canviem el seu propietari i grup.

```
usuario@ldapserver:~$ sudo mkdir /moviles  
[sudo] password for usuario:  
usuario@ldapserver:~$ sudo chown nobody:nogroup /moviles  
usuario@ldapserver:~$ █
```

16.2. EXPORTAR EL CONTINGUT DE LA CARPETA QUE TINDRÀ ELS PERFILS MÒBILS

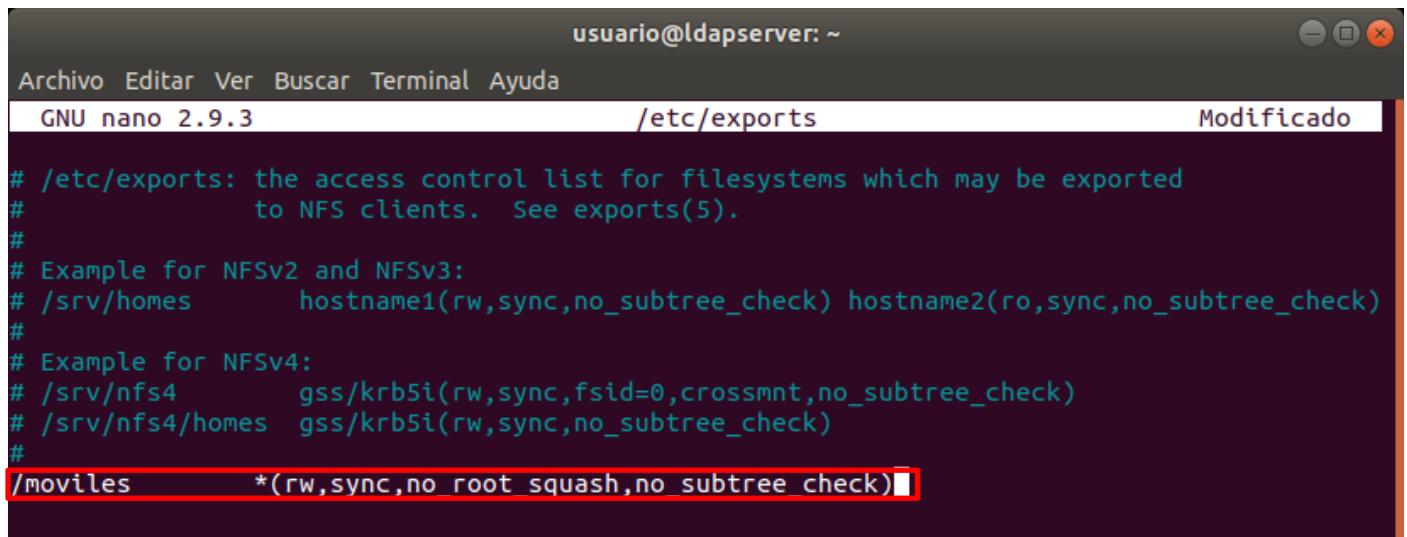
Llaura hem d'aconseguir que NFS compartisca la carpeta amb tots els usuaris de la xarxa. De nou, pots obtindre més detalls en el tema “Instal·lar i configurar NFS en Ubuntu”, concretament en l'apartat “Configurar el servidor NFS”.

Com podràs recordar, la idea bàsica consisteix a editar l'arxiu /etc/exports i crear una línia com aquesta:

```
/moviles *(rw,sync,no_root_squash,no_subtree_check)
```

Usem l'editor nano amb privilegis de superusuari:

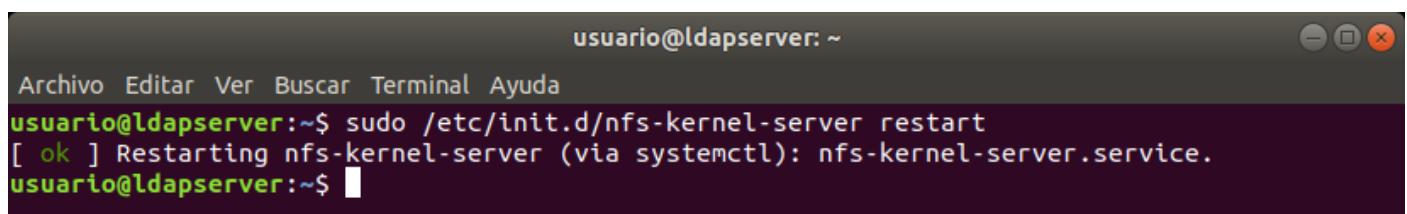
```
sudo nano /etc/exports
```



```
usuario@ldapserver: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.9.3           /etc/exports          Modificado
#
# /etc/exports: the access control list for filesystems which may be exported
#                 to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
#
/movies      *(rw,sync,no_root_squash,no_subtree_check)
```

Quan fas canvis en l'arxiu /etc/exports, recorda que has de reiniciar el servei NFS perquè segueixen efectius. Per a aconseguir-ho, només has d'escriure la següent ordre en la finestra de terminal:

```
sudo /etc/init.d/nfs-kernel-server restart ó (sudo systemctl restart nfs-kernel-server)
```



```
usuario@ldapserver: ~
Archivo Editar Ver Buscar Terminal Ayuda
usuario@ldapserver:~$ sudo /etc/init.d/nfs-kernel-server restart
[ ok ] Restarting nfs-kernel-server (via systemctl): nfs-kernel-server.service.
usuario@ldapserver:~$
```

16.3. CREAR UNA CARPETA PER A GUARDAR ELS PERFILS MÒBILS EN CADA CLIENT

Llaura, en cada equip client dones del qual els usuaris vagen a iniciar sessió, haurem de repetir el mateix procés, que consisteix a **crear la carpeta que usarem després com a punt de muntatge per a la carpeta compartida amb el servidor**. Recorda que tens més detalls en l'apartat “Accedir a la carpeta compartida amb NFS dunes d'un client amb Ubuntu” del tema anterior.

Comptat i debatut, la idea és crear una nova carpeta i permetre que puga accedir a ella qualsevol usuari:

```
sudo mkdir /moviles  
sudo chmod 777 /moviles
```

```
usuario@clientelinux:~$ sudo mkdir /moviles  
[sudo] password for usuario:  
usuario@clientelinux:~$ sudo chmod 777 /moviles  
usuario@clientelinux:~$ █
```

Recorda: Per a aquest exemple, hem fet coincidir el nom de la carpeta en el servidor i en el client, però això no és en absolut necessari.

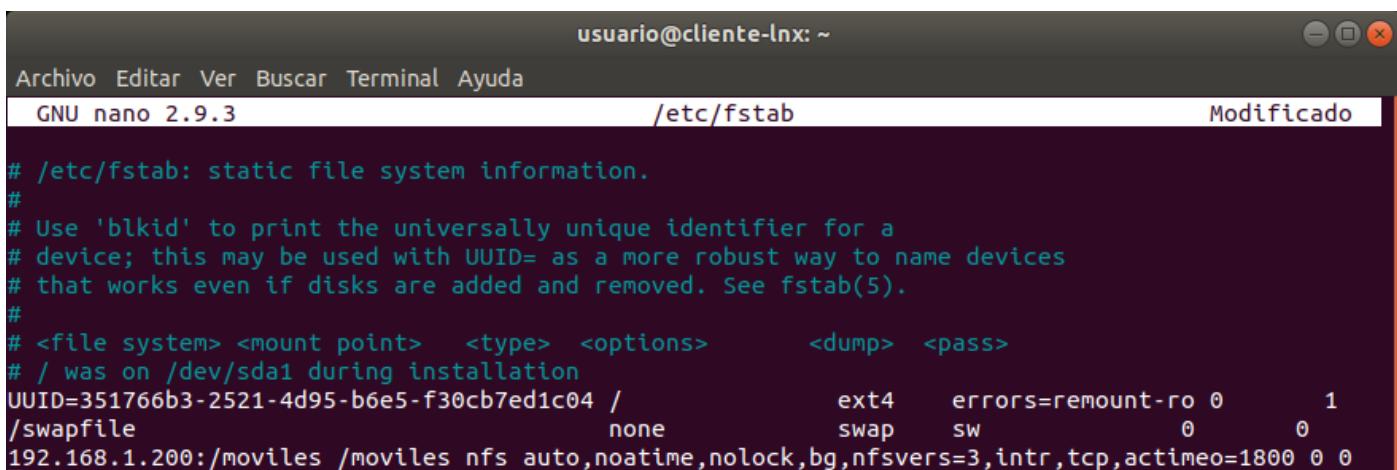
16.4. MODIFICAR L'ARXIU /ETC/FSTAB EN CADA CLIENT PER A MUNTAR LA CARPETA EN L'ARRANCADA

Com ja expliquem en el tema anterior, també dins de l'apartat “Accedir a la carpeta compartida amb NFS dunes d'un client amb Ubuntu”, l'arxiu /etc/fstab guarda la informació dels volums que han de muntar-se durant l'arrancada del sistema operatiu. Com necessitarem que la carpeta del servidor és munte de manera local en l'equip client abans que l'usuari inicie sessió, haurem d'afegir la següent línia a l'arxiu /etc/fstab:

```
192.168.1.200:/moviles /moviles nfs acte,noatime,nolock,bg,nfsvers=3,intr,tcp,actimeo=1800 0 0
```

De nou, usem l'editor nano amb privilegis de superusuari:

```
sudo nano /etc/fstab
```



```
usuario@cliente-lnx: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
GNU nano 2.9.3 /etc/fstab Modificado  
# /etc/fstab: static file system information.  
#  
# Use 'blkid' to print the universally unique identifier for a  
# device; this may be used with UUID= as a more robust way to name devices  
# that works even if disks are added and removed. See fstab(5).  
#  
# <file system> <mount point> <type> <options> <dump> <pass>  
# / was on /dev/sda1 during installation  
UUID=351766b3-2521-4d95-b6e5-f30cb7ed1c04 / ext4 errors=remount-ro 0 1  
/swapfile none swap sw 0 0  
192.168.1.200:/moviles /moviles nfs auto,noatime,nolock,bg,nfsvers=3,intr,tcp,actimeo=1800 0 0
```

Important: Una vegada fets els canvis, haurem de **reiniciar** l'equip perquè aquests segueixin aplicats.

16.5. INDICAR EN L'USUARI LDAP LA CARPETA ON TINDRÀ EL SEU PERFILEN EL CLIENT

L'últim pas consistirà a modificar els usuari existents, o crear altres nous, indicant que el seu atribut homeDirectory és una subcarpeta de la carpeta que hem creat en els passos anteriors.

Per a completar aquesta taverna pots seguir qualsevol dels mètodes que hem explicat en aquest tema.

En el nostre cas, hem creat un nou usuari anomenat “amartinez” usant l'eina LDAP Account Manager (on l'atribut homeDirectory rep el nom “Directori inicial”).

The screenshot shows the LDAP Account Manager web interface. At the top, it says "LDAP Account Manager (localhost:389) - Mozilla Firefox". Below the address bar, it shows "LDAP Account Manager - 6.2 (Sesión iniciada como: admin)" and "Visor del arbol", "Herramientas", "Ayuda", and "Cerrar sesión". The main area has tabs for "Usuarios" and "Grupos", with "Guardar" and "Establecer contraseña" buttons. The user "Antonio Martinez" is selected. The configuration form includes fields for "Nombre del usuario*" (amartinez), "Nombre común" (Antonio Martinez), "Número UID" (10001), "Gecos" (empty), "Grupo primario" (SMR2), "Grupos adicionales" (Editar grupos), "Directorio inicial*" (highlighted with a red box and set to /moviles/amartinez), and "Intérprete del inicio de sesión" (/bin/bash). A sidebar on the left shows icons for Personal, Unix, and Sombra.

Com pot veure's en la imatge, hem indicat que la carpeta home de l'usuari és trobarà en /moviles/amartinez.

16.6. COMPROVAR QUE LA CONFIGURACIÓ FUNCIONA CORRECTAMENT

Sols caldrà iniciar el client i indicar el nom del compte LDAP i la seu contrasenya.

Basta amb iniciar sessió la primera vegada en manera text, perquè és creu el perfil de l'usuari en el client. D'aquesta manera, a iniciar sessió en manera text, observem com és crea el directori local per a guardar els dades del client.

```
Ubuntu 18.04.3 LTS cliente-lnx tty4
cliente-lnx login: amartinez
Password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 5.0.0-37-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

Pueden actualizarse 113 paquetes.
0 actualizaciones son de seguridad.

Your Hardware Enablement Stack (HWE) is supported until April 2023.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

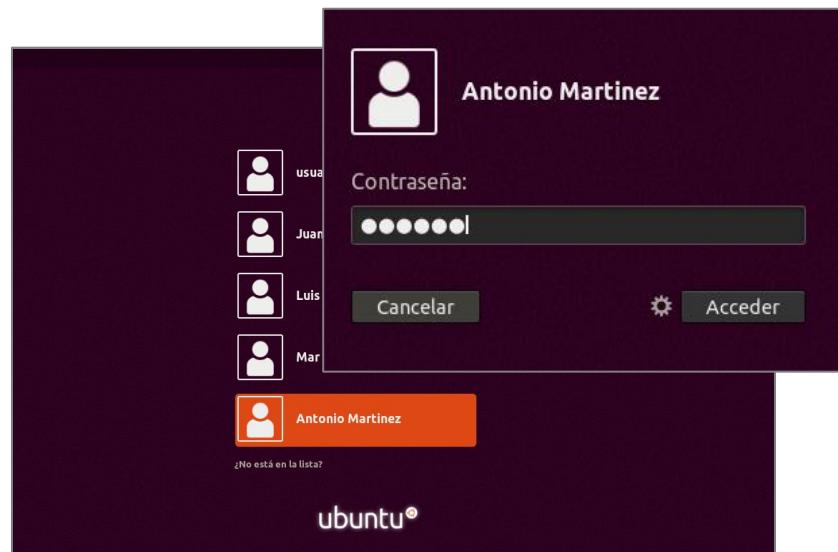
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Creating directory '/moviles/amartinez'.
amartinez@cliente-lnx:$
```

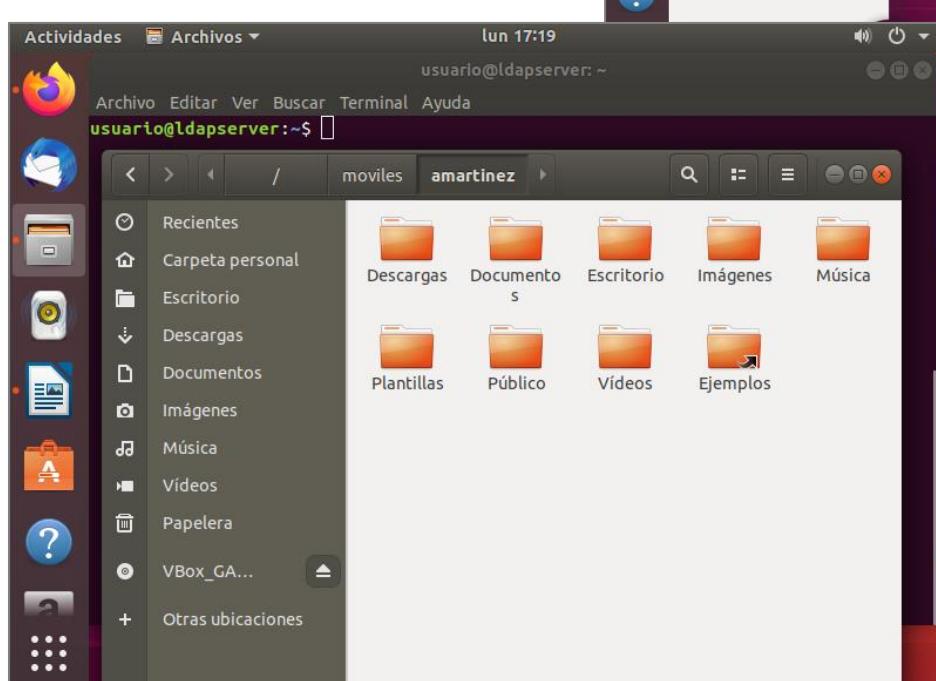
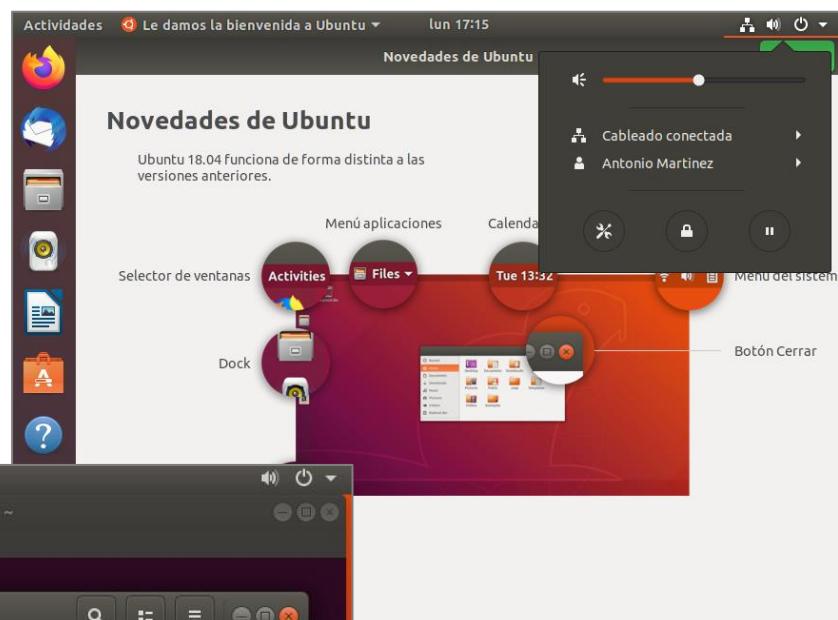
En aquest punt hem de fer algunes apreciacions:

- L'inici de sessió ha creat el directori home local per a l'usuari, però l'ha fet en una carpeta compartida pel servidor, per la qual cosa, en realitat, la carpeta s'està creant en el servidor.
- Perquè això funcione així, haurem hagut de modificar l'arxiu `/etc/pam.d/common-session` dels clients on iniciarà sessió l'usuari, tal com explicàvem en l'apartat “Configurar un equip client amb Ubuntu per a autenticar-se'sns el servidor OpenLDAP” d'aquest mateix tema. Si no has modificat aquest arxiu, sempre pots crear amb antelació la carpeta a mà.

A partir d'ací, la pròxima vegada que inicies sessió en el client, ja trobaràs el nou usuari en la pantalla d'autenticació. Només caldrà seleccionar-ho i escriure la contrasenya per a començar a treballar.



Com veuràs, la sessió s'inicia igual que amb qualsevol un altre usuari:



Podem obtindre la comprovació definitiva si accedim en el servidor a la carpeta que està compartint. Podrem comprovar que s'ha creat la carpeta “amartinez” i que vaig comptar els dades del perfil de l'usuari.

17. ERRORS TÍPICS EN INSTAL·LAR OPENLDAP

Error típic 1: /etc/hosts mal configurat

Cap de bestiar més instal·lar OpenLDAP el primer que heu de fer és mirar si s'ha creat bé el domini mitjançant **slapcat**. Ací heu de veure el domini, (en aquest exemple, empresa.local) i l'usuari administrador admin de l domini.

```
usuario@ldapserver:~$ sudo slapcat
dn: dc=empresa,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: empresa.local
dc: empresa
structuralObjectClass: organization
entryUUID: 201a16ea-3a65-1034-8489-55c26ad15d50
creatorsName: cn=admin,dc=empresa,dc=local
createTimestamp: 20150127114106Z
entryCSN: 20150127114106.864273Z#000001#000#000000
modifiersName: cn=admin,dc=empresa,dc=local
modifyTimestamp: 20150127114106Z

dn: cn=admin,dc=empresa,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9dDJyWlMvRkJONzRhWTRBYUMvWm9BUHlwSzdVazdIbWM=
structuralObjectClass: organizationalRole
entryUUID: 201ab33e-3a65-1034-848a-55c26ad15d50
creatorsName: cn=admin,dc=empresa,dc=local
createTimestamp: 20150127114106Z
entryCSN: 20150127114106.868275Z#000000#000#000000
modifiersName: cn=admin,dc=empresa,dc=local
modifyTimestamp: 20150127114106Z

usuario@ldapserver:~$
```

Si no ix així (us posa **nodomain**), probablement no heu configurat bé el **/etc/hosts**. Recordeu que ha de configurar-se així:

```
usuario@linuxserver: ~
GNU nano 2.2.6          Archivo: /etc/hosts          Modificado
127.0.0.1      localhost
192.168.0.200  ldapserver.empresa.local      ldapserver

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

IPServidor      NombreServidor.domini      NombreServidor
```

Error típic 2: no afeg unitats organitzatives, ni usuaris, ni grups

```
sudo ldapadd -x -D cn=admin,dc=empresa,dc=local -W -f fitxer.ldif
```

Assegura't que el domini és el que toca i que has posat bé la ruta del fitxer!

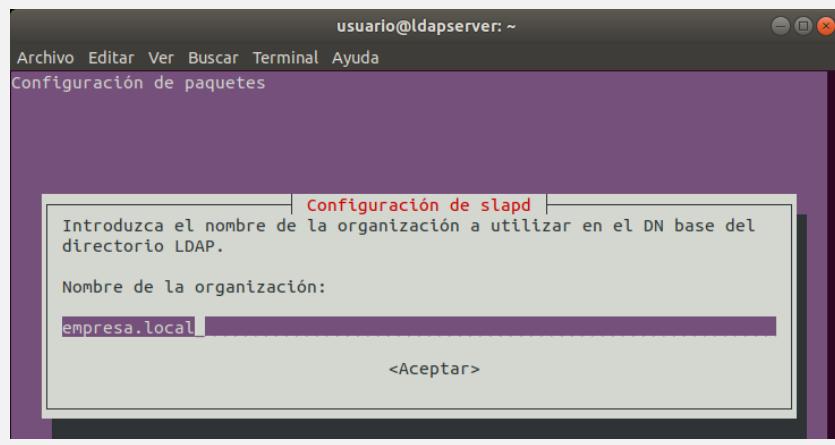
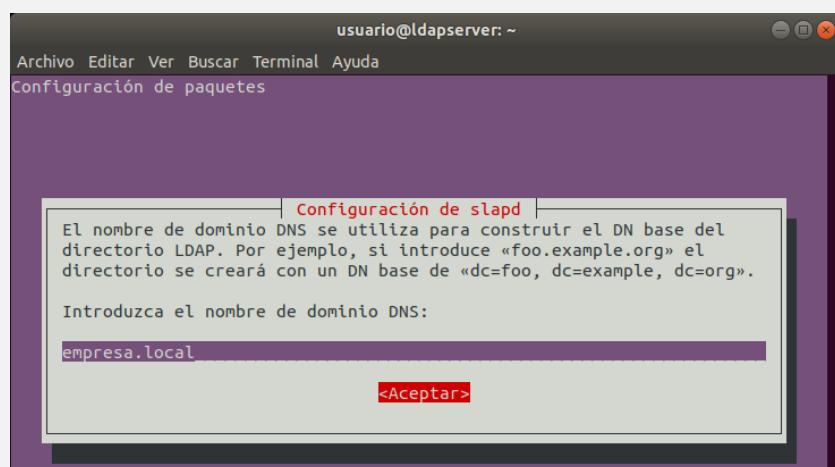
Error típic 3: no us recordeu o no us funciona la contrasenya que heu posat en instal·lar OpenLDAP

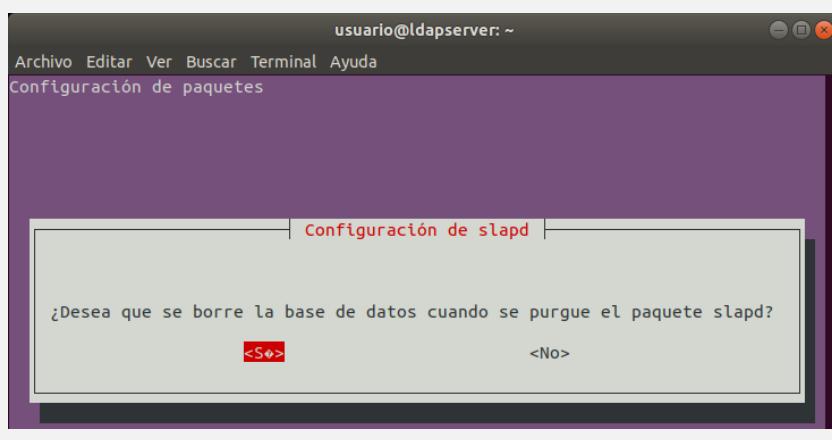
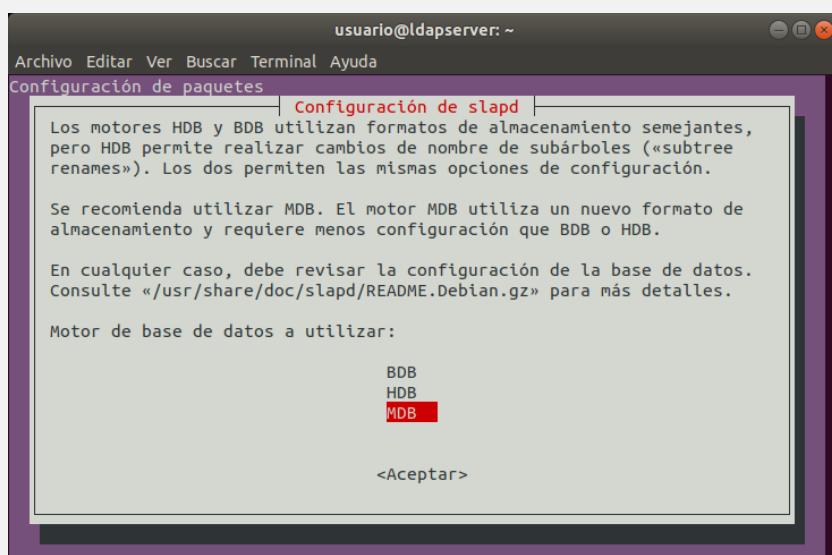
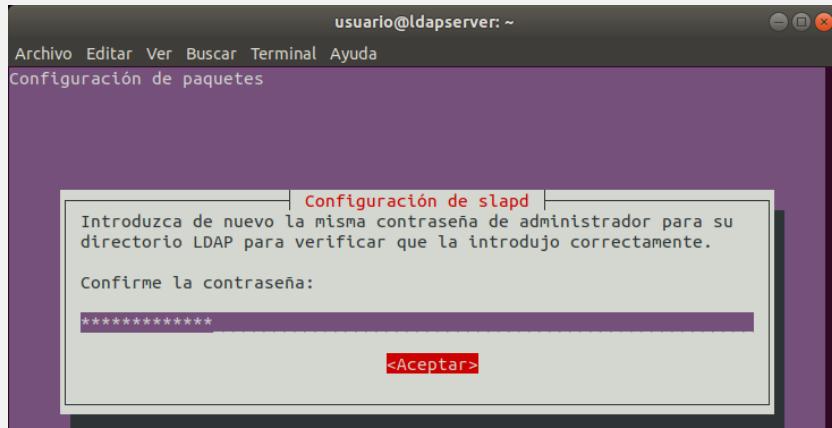
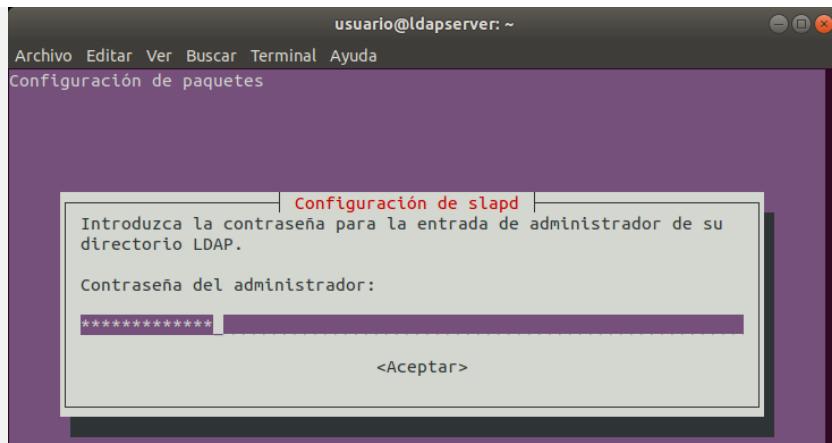
Si no us funciona la contrasenya en afegir un usuari o un grup, podeu reconfigurar OpenLDAP mitjançant:

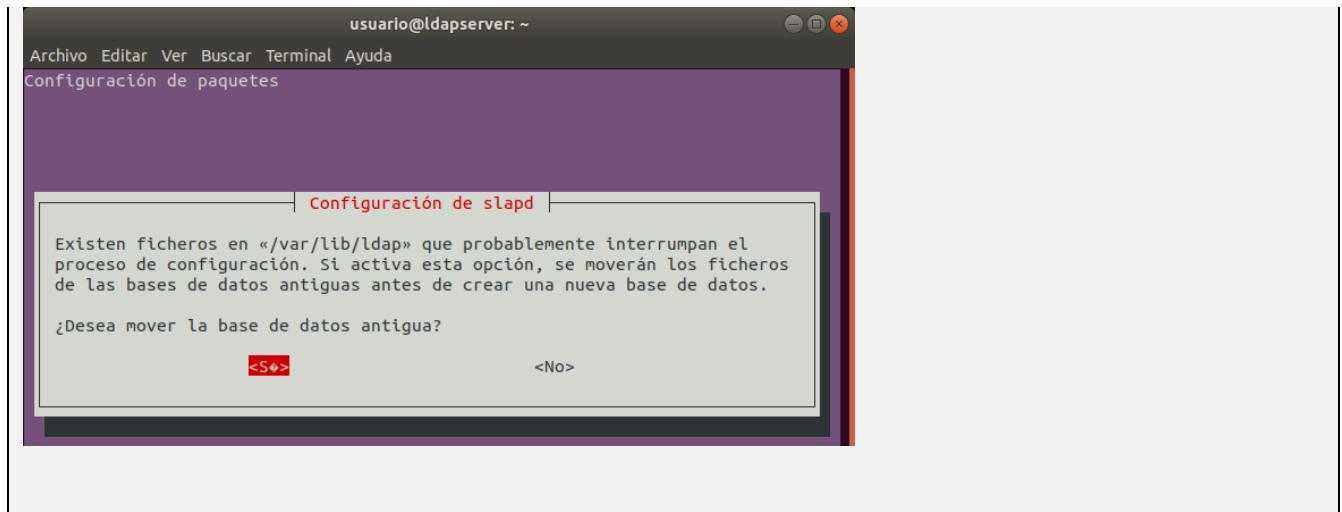
Si no està ben configurat llavors executarem el comando:

```
sudo dpkg-reconfigure slapd
```

I anirem seguint els següents captures:







També podeu desinstal·lar tot i tornar-ho a instal·lar mitjançant apt-get purge o apt-get remove:

- *apt-get remove paquet*: desinstal·la paquets
- *apt-get purge paquet*: elimina el paquet i els seus arxius de configuració