ASIX1 M06: administració de sistemes operatius			
UF1: administració avançada de sistemes operatius			
A05.06pi pràctica - Administració del servei de directori			
Revisió	**Data**	**Autor**	**Observacions**
0	01/02/2023	Josep Bassó	Document inicial
1	19/02/2023	Nil Massó	Document final

OBJECTIUS

1.1 Identifica la funció, els elements i les estructures lògiques del servei de directori.
1.2 Determina i crea l'esquema del servei de directori.
1.3 Realitza la instal·lació del servei de directori al servidor.
1.4 Realitza la configuració i personalització del servei de directori.
1.5 Integra el servei de directori amb altres serveis.
1.6 Aplica filtres de cerca en el servei de directori.
1.7 Utilitza el servei de directori com a mecanisme d'acreditació centralitzada dels usuaris en una xarxa.l'estructura i la implantació del servei de directori.
1.8 Realitza la configuració del client per a la seva integració en el servei de directori.
1.9 Utilitza eines gràfiques i comandaments per a l'administració del servei de directori.
1.10 Documenta l'estructura i la implantació del servei de directori.

INSTRUCCIONS

- Llegeix amb calma què s'ha de fer abans de començar.
- Lliura només un sol fitxer amb el nom: **A05_06pi_*cognom_nom***.
- El document ha de ser amb format **.docx** o **.pdf**.
- Escriu les respostes sota l'enunciat, sense esborrar-lo.
- Has de mostrar la instrucció, el resultat i la comprovació (si cal).
- L'incompliment d'un punt anterior pot provocar la no correcció.
- El professor pot demanar l'explicació del treball realitzat.
- En cas de còpia la nota serà un 1 a la UF per tots els implicats.

AVALUACIÓ

- Cada apartat et mostra la seva valoració màxima.

PRÀCTICA

Recordeu que teniu els enllaços oficials als exercicis. Us recordo aquests:

- http://somebooks.es/ldap-parte-1-instalar-openldap-en-ubuntu-20-04-lts/
- http://somebooks.es/ldap-parte2-iniciar-la-estructura-del-directorio/
- https://www.youtube.com/watch?v=kksS5daigg0
- https://docs.moodle.org/all/es/Autenticaci%C3%B3n_LDAP
- https://www.youtube.com/watch?v=DbfeA50OyyI

Apartat 1. Configuració de l'OpenLDAP. (1p)

- Instal·la l'openLDAP en un linux server.

sudo apt-get install slapd ldap-utils

- Configura'l amb el nom de domini: srvldap.{cognom}.com

```
root@us-nmc:~# dpkg-reconfigure slapd
debconf: unable to initialize frontend: Dialog
debconf: (No usable dialog-like program is installed, so the dialog based fronte
nd cannot be used. at /usr/share/perl5/Debconf/FrontEnd/Dialog.pm line 78.)
debconf: falling back to frontend: Readline
Configuring slapd
-----------------

If you enable this option, no initial configuration or database will be created
for you.

Omit OpenLDAP server configuration? [yes/no] no

The DNS domain name is used to construct the base DN of the LDAP directory. For
example, 'foo.example.org' will create the directory with 'dc=foo, dc=example,
dc=org' as base DN.

DNS domain name: srvldap.masso.com
```

- Realitza les verificacions i repassa la configuració.

```
root@us-nmc:~# slapcat
dn: dc=srvldap,dc=masso,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: sapa
dc: srvldap
structuralObjectClass: organization
entryUUID: 810118d0-44ef-103d-876a-51f2538a6346
creatorsName: cn=admin,dc=srvldap,dc=masso,dc=com
createTimestamp: 20230219222130Z
entryCSN: 20230219222130.655463Z#000000#000#000000
modifiersName: cn=admin,dc=srvldap,dc=masso,dc=com
modifyTimestamp: 20230219222130Z
```

- Si ja el tens instal·lat, modifica la instal·lació perquè quedi configurat així.
- Indica clarament els paràmetres de configuració que hagis fet servir.

Apartat 2. Comandes LDAP utils I. (1p -5*0,2-)

- Tenim aquests usuaris:
  - Manteniment: Tim Taylor, Al Borland i Heidi Keppert.
  - Expedicions: Han Solo, Chewbacca Wookiee i {tu} (usuari Sa Palomera sense punt, ex: jbasso).
  - Comercial: Lando Calrissian, Richard Shrewsbury, Edmond Blackadder, Baldrick Dogsbody.

a) Fes un esquema DIT per organitzar-ho.

dc=srvldap,dc=cognom,dc=com
├── ou=comercial
│ ├── cn=Richard Shrewsbury
│ ├── cn=Edmond Blackadder
│ ├── cn=Baldrick Dogsbody
│ └── cn=Lando Calrissan
├── ou=expedicions
│ ├── cn=Han Solo
│ ├── cn=Chewbacca Wookiee
│ └── cn={tu}
└── ou=manteniment
  ├── cn=Tim Taylor
  ├── cn=Al Borland
  └── cn=Heidi Keppert

b) Afegeix els 'grups' i els usuaris al servidor.

```
root@us-nmc:~# sudo ldapadd -x -D cn=admin,dc=srvldap,dc=masso,dc=com -W -f base.ldif
Enter LDAP Password:
adding new entry "ou=comercial,dc=srvldap,dc=masso,dc=com"

adding new entry "cn=Richard Shrewsbury,ou=comercial,dc=srvldap,dc=masso,dc=com"

adding new entry "cn=Edmond Blackadder,ou=comercial,dc=srvldap,dc=masso,dc=com"

adding new entry "cn=Baldrick Dogsbody,ou=comercial,dc=srvldap,dc=masso,dc=com"

adding new entry "cn=Lando Calrissian,ou=comercial,dc=srvldap,dc=masso,dc=com"

adding new entry "ou=expedicions,dc=srvldap,dc=masso,dc=com"

adding new entry "cn=Han Solo,ou=expedicions,dc=srvldap,dc=masso,dc=com"

adding new entry "cn=Chewbacca Wookiee,ou=expedicions,dc=srvldap,dc=masso,dc=com"

adding new entry "cn=Nil Masso,ou=expedicions,dc=srvldap,dc=masso,dc=com"

adding new entry "ou=manteniment,dc=srvldap,dc=masso,dc=com"

adding new entry "cn=Tim Taylor,ou=manteniment,dc=srvldap,dc=masso,dc=com"

adding new entry "cn=Al Borland,ou=manteniment,dc=srvldap,dc=masso,dc=com"

adding new entry "cn=Heidi Keppert,ou=manteniment,dc=srvldap,dc=masso,dc=com"
```

c) Fes una cerca de totes les persones que hi ha entrades i les seves dades.

```
root@us-nmc:~# ldapsearch -x -LLL -b dc=srvldap,dc=masso,dc=com "(objectClass=person)" *
dn: cn=Richard Shrewsbury,ou=comercial,dc=srvldap,dc=masso,dc=com

dn: cn=Edmond Blackadder,ou=comercial,dc=srvldap,dc=masso,dc=com

dn: cn=Baldrick Dogsbody,ou=comercial,dc=srvldap,dc=masso,dc=com

dn: cn=Lando Calrissian,ou=comercial,dc=srvldap,dc=masso,dc=com

dn: cn=Han Solo,ou=expedicions,dc=srvldap,dc=masso,dc=com

dn: cn=Chewbacca Wookiee,ou=expedicions,dc=srvldap,dc=masso,dc=com

dn: cn=Nil Masso,ou=expedicions,dc=srvldap,dc=masso,dc=com

dn: cn=Tim Taylor,ou=manteniment,dc=srvldap,dc=masso,dc=com

dn: cn=Al Borland,ou=manteniment,dc=srvldap,dc=masso,dc=com

dn: cn=Heidi Keppert,ou=manteniment,dc=srvldap,dc=masso,dc=com
```

d) En Han Solo ha marxat de l'empresa i en Lando Calrissian deixarà el dptm comercial i passarà al d'expedicions. Aplica els canvis i repeteix la cerca.

```
root@us-nmc:~# sudo ldapdelete -x -D "cn=admin,dc=srvldap,dc=masso,dc=com" -W "cn=Han Solo,ou=expedicions,dc=srvldap,dc=masso,dc=com"
```

```
root@us-nmc:~# sudo ldapmodify -x -D "cn=admin,dc=srvldap,dc=masso,dc=com" -W << EOF
dn: cn=Lando Calrissian,ou=comercial,dc=srvldap,dc=masso,dc=com
changetype: modify
replace: ou
ou: expedicions
EOF
```

```
root@us-nmc:~# ldapsearch -x -LLL -b dc=srvldap,dc=masso,dc=com "(objectClass=perso
n)" *
dn: cn=Richard Shrewsbury,ou=comercial,dc=srvldap,dc=masso,dc=com

dn: cn=Edmond Blackadder,ou=comercial,dc=srvldap,dc=masso,dc=com

dn: cn=Baldrick Dogsbody,ou=comercial,dc=srvldap,dc=masso,dc=com

dn: cn=Lando Calrissian,ou=comercial,dc=srvldap,dc=masso,dc=com

dn: cn=Chewbacca Wookiee,ou=expedicions,dc=srvldap,dc=masso,dc=com

dn: cn=Nil Masso,ou=expedicions,dc=srvldap,dc=masso,dc=com

dn: cn=Tim Taylor,ou=manteniment,dc=srvldap,dc=masso,dc=com

dn: cn=Al Borland,ou=manteniment,dc=srvldap,dc=masso,dc=com

dn: cn=Heidi Keppert,ou=manteniment,dc=srvldap,dc=masso,dc=com
```

Fes una cerca dels usuaris que el seu nom (cn) contingui 'al' mostrant només el dn.

```
root@us-nmc:~# ldapsearch -x -LLL -b "dc=srvldap,dc=masso,dc=com" "(cn=*al*)" dn
dn: cn=Lando Calrissian,ou=comercial,dc=srvldap,dc=masso,dc=com

dn: cn=Baldrick Dogsbody,ou=comercial,dc=srvldap,dc=masso,dc=com

dn: cn=Al Borland,ou=manteniment,dc=srvldap,dc=masso,dc=com
```

Apartat 3. Comandes LDAP utils II. (2p -10*0,2-)

a) Fes una consulta de la configuració del servidor.

```
root@us-nmc:~# slapcat
dn: dc=srvldap,dc=masso,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: sapa
dc: srvldap
structuralObjectClass: organization
entryUUID: 9924550a-456f-103d-9464-c7c693ccf4a8
creatorsName: cn=admin,dc=srvldap,dc=masso,dc=com
createTimestamp: 20230220133826Z
entryCSN: 20230220133826.733071Z#000000#000#000000
modifiersName: cn=admin,dc=srvldap,dc=masso,dc=com
modifyTimestamp: 20230220133826Z
```

b) Importa els dos fitxers ldif del moodle (uo's i usuaris). Si has de fer-hi modificacions, indica-les i els motius.

```
dn: ou=profesapa,dc=srvldap,dc=masso,dc=com
objectClass: organizationalUnit
ou: profesapa

dn: ou=alusapa,dc=srvldap,dc=masso,dc=com
objectClass: organizationalUnit
ou: alusapa
```

Modifiquem l'altre arxiu amb:

```
:%s/dc=b/dc=srvldap,dc=m/g
```

Els importem:

```
root@us-nmc:~# ldapadd -x -D cn=admin,dc=srvldap,dc=masso,dc=com -W -f ous.ldif
Enter LDAP Password:
adding new entry "ou=profesapa,dc=srvldap,dc=masso,dc=com"

adding new entry "ou=alusapa,dc=srvldap,dc=masso,dc=com"

root@us-nmc:~# ldapadd -x -D cn=admin,dc=srvldap,dc=masso,dc=com -W -f usuaris.ldif
Enter LDAP Password:
adding new entry "uid=jbasso,ou=profesapa,dc=srvldap,dc=masso,dc=com"

adding new entry "uid=jcata,ou=profesapa,dc=srvldap,dc=masso,dc=com"

adding new entry "uid=jpou,ou=profesapa,dc=srvldap,dc=masso,dc=com"

adding new entry "uid=mhamilton,ou=profesapa,dc=srvldap,dc=masso,dc=com"

adding new entry "uid=asotes,ou=alusapa,dc=srvldap,dc=masso,dc=com"

adding new entry "uid=jsola,ou=alusapa,dc=srvldap,dc=masso,dc=com"
```

c) Consulta només les unitats organitzatives que has importat.

```
root@us-nmc:~# slapcat | grep ou:
ou: comercial
ou: expedicions
ou: expedicions
ou: manteniment
ou: profesapa
ou: alusapa
```

d) Consulta l'uid dels alumnes. Fes-ho de dues formes, acotant amb el paràmetre –b i sense acotar-ho.

```
root@us-nmc:~# ldapsearch -x -b "ou=alusapa,dc=srvldap,dc=masso,dc=co
m" "(objectClass=posixAccount)" uid
# extended LDIF
#
# LDAPv3
# base <ou=alusapa,dc=srvldap,dc=masso,dc=com> with scope subtree
# filter: (objectClass=posixAccount)
# requesting: uid
#

# jsola, alusapa, srvldap.masso.com
dn: uid=jsola,ou=alusapa,dc=srvldap,dc=masso,dc=com
uid: jsola

# asotes, alusapa, srvldap.masso.com
dn: uid=asotes,ou=alusapa,dc=srvldap,dc=masso,dc=com
uid: asotes

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

Sense -b no mostra res:

```
root@us-nmc:~# ldapsearch -x "ou=alusapa,dc=srvldap,dc=masso,dc=com"
"(objectClass=posixAccount)" uid
# extended LDIF
#
# LDAPv3
# base <dc=srvldap,dc=masso,dc=com> (default) with scope subtree
# filter: ou=alusapa,dc=srvldap,dc=masso,dc=com
# requesting: (objectClass=posixAccount) uid
#

# search result
search: 2
result: 0 Success

# numResponses: 1
```

e) Consulta l'uid dels alumnes que el nom (givenName) comenci per 'A' i el cognom (sn) comenci per 'So'.

```
root@us-nmc:~# ldapsearch -x -LLL -b "dc=srvldap,dc=masso,dc=com" "(&(givenName=a*)(sn=So*))" uid
dn: uid=asotes,ou=alusapa,dc=srvldap,dc=masso,dc=com
uid: asotes
```

f) Consulta el nom dels professors que es diguin Josep (givenName). Tingues en compte que també cal mostrar-los si el nom és compost (p.ex. Josep Maria).

```
root@us-nmc:~# ldapsearch -x -LLL -b "ou=profesapa,dc=srvldap,dc=masso,dc=com"
(givenName=Josep*)" cn
dn: uid=jcata,ou=profesapa,dc=srvldap,dc=masso,dc=com
cn: Josep Cata

dn: uid=jbasso,ou=profesapa,dc=srvldap,dc=masso,dc=com
cn: Josep Basso
```

g) Consulta el dn de només els usuaris que contenen una 'j' al nom (givenName).

```
root@us-nmc:~# ldapsearch -x -LLL -b "ou=alusapa,dc=srvldap,dc=masso,dc=com" "(g
ivenName=*j*)" dn
dn: uid=jsola,ou=alusapa,dc=srvldap,dc=masso,dc=com
```

h) Consulta el dn dels professors que tenen una 'o' o una 'a' al nom (givenName)

```
root@us-nmc:~# ldapsearch -x -LLL -b "ou=profesapa,dc=srvldap,dc=masso,dc=com" "
(|(givenName=*o*)(givenName=*a*))" dn
dn: uid=jpou,ou=profesapa,dc=srvldap,dc=masso,dc=com

dn: uid=jcata,ou=profesapa,dc=srvldap,dc=masso,dc=com

dn: uid=jbasso,ou=profesapa,dc=srvldap,dc=masso,dc=com

dn: uid=mhamilton,ou=profesapa,dc=srvldap,dc=masso,dc=com
```

i) Canvia el homeDirectory de l'usuari jpou per /home/jpou. Consulta el resultat.

```
root@us-nmc:~# ldapmodify -x -D "cn=admin,dc=srvldap,dc=masso,dc=com" -W << EOF
dn: uid=jpou,ou=profesapa,dc=srvldap,dc=masso,dc=com
changetype: modify
replace: homeDirectory
homeDirectory: /home/jpou
EOF
Enter LDAP Password:
modifying entry "uid=jpou,ou=profesapa,dc=srvldap,dc=masso,dc=com"

root@us-nmc:~# ldapsearch -x -LLL -b "ou=profesapa,dc=srvldap,dc=masso,dc=com" "uid=jpou" homeDirectory
dn: uid=jpou,ou=profesapa,dc=srvldap,dc=masso,dc=com
homeDirectory: /home/jpou
```

j) Esborra la professora Margaret Hamilton. Consulta per veure el resultat.

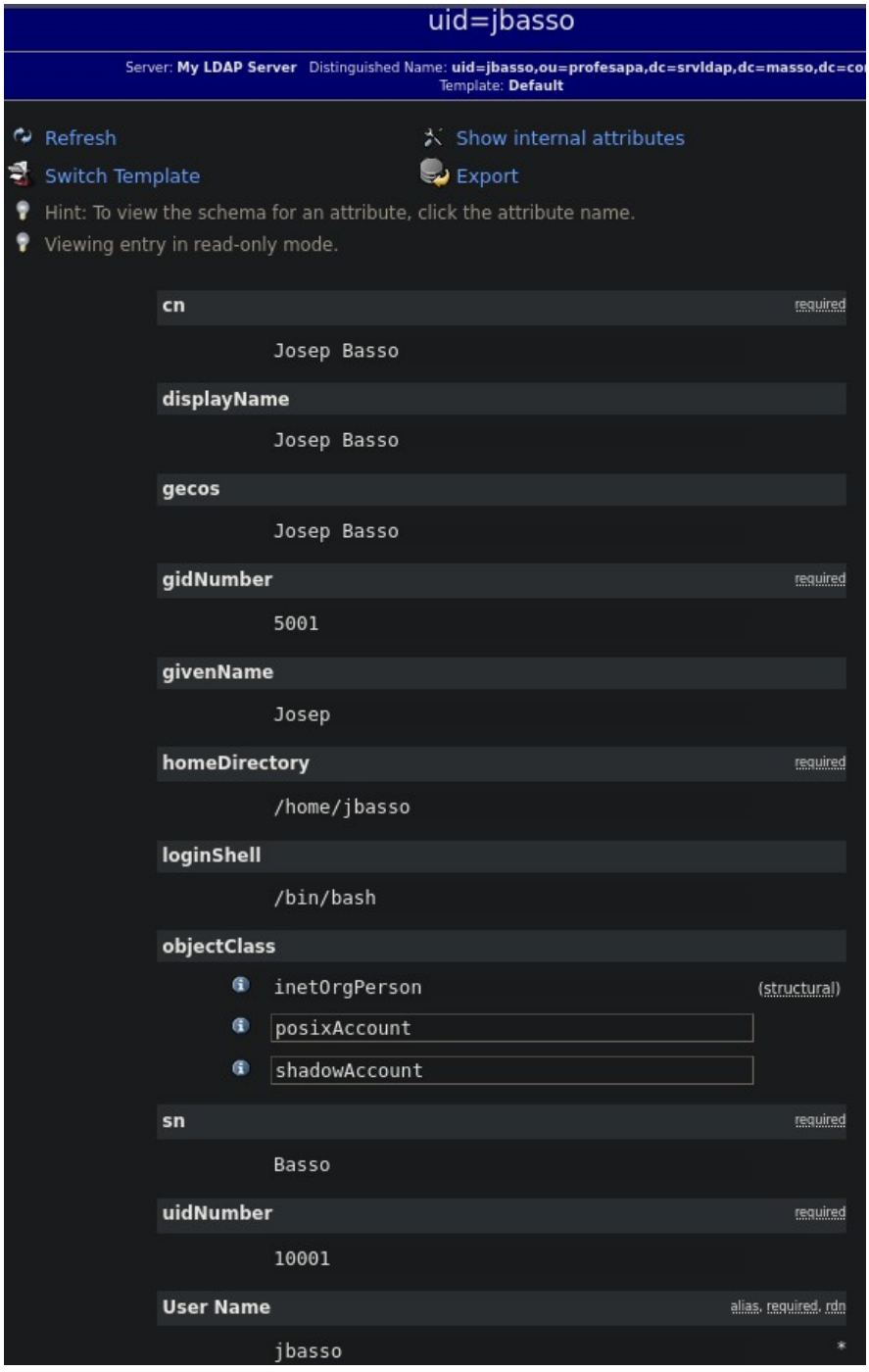
```
root@us-nmc:~# ldapdelete -x -D "cn=admin,dc=srvldap,dc=masso,dc=com" -W "uid=mhamilton,ou=profesapa,dc=s
rvldap,dc=masso,dc=com"
Enter LDAP Password:
root@us-nmc:~# ldapsearch -x -LLL -b "dc=srvldap,dc=masso,dc=com" "uid=mhamilton,ou=profesapa,dc=srvldap,
dc=masso,dc=com"
root@us-nmc:~#
```

Apartat 4. Configuració d'una eina gràfica. (1p)

- Instal·la una eina gràfica i fes-ne la configuració.

He instal·lat phpldapadmin, per saltarme els errors de compatibilitat, previ a intsalar el paquet :
apt purge php*
rm -r /etc/php8*
Ara fem apt install phpldapadmin però **NO** li donem a si, mirem quines dependències de php te
Les instalem però posant 7.4 al darrere de tots els php
Recordem tmb instalar les llibreries de comunicacio de php amb apache si no shan instalat, recordem posar 7.4 tmambe
Un cop fet entrariem al navegador a IP/phpldapadmin i posariem la nostra config de domini

- Mostra la pantalla d'un usuari.



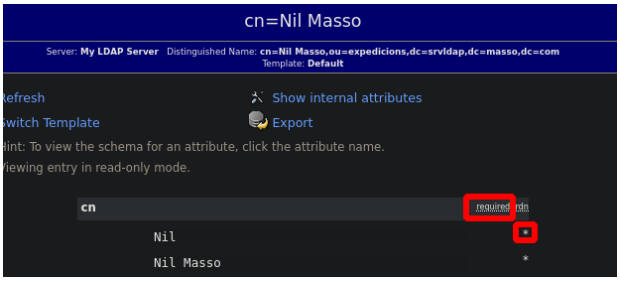
- Realitza la cerca de tots els usuaris d'expedicions (apartat 2).

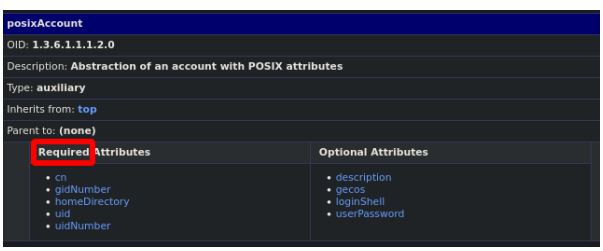
Apartat 5. Esquemes. (1p -4*0,25-)

a) Als fitxers ldif fets servir a l'apartat 2, a partir de quines línies sabrem quins atributs han de tenir els usuaris?

```
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
```

b) Mostra en l'entorn gràfic com es veu quins atributs són obligatoris i quins opcionals.





c) Indica en quins fitxers, ruta i nom, trobaries aquestes configuracions.

```
root@us-nmc:~# ls /etc/ldap/schema/
README              core.schema     duaconf.schema        java.schema       namedobject.schema  pmi.schema
collective.ldif     cosine.ldif     dyngroup.ldif         misc.ldif         nis.ldif            sapa.ldif
collective.schema   cosine.schema   dyngroup.schema       misc.schema       nis.schema
corba.ldif          dsee.ldif       inetorgperson.ldif    msuser.ldif       openldap.ldif
corba.schema        dsee.schema     inetorgperson.schema  msuser.schema     openldap.schema
core.ldif           duaconf.ldif    java.ldif             namedobject.ldif  pmi.ldif
```

d) Mostra la captura de pantalla de les parts corresponents.

Podem veure els must o required i els opcionals

```
  GNU nano 6.2                                /etc/ldap/schema/nis.schema
# Object Class Definitions

objectclass ( 1.3.6.1.1.1.2.0 NAME 'posixAccount'
        DESC 'Abstraction of an account with POSIX attributes'
        SUP top AUXILIARY
        MUST ( cn $ uid $ uidNumber $ gidNumber $ homeDirectory )
        MAY ( userPassword $ loginShell $ gecos $ description ) )
```

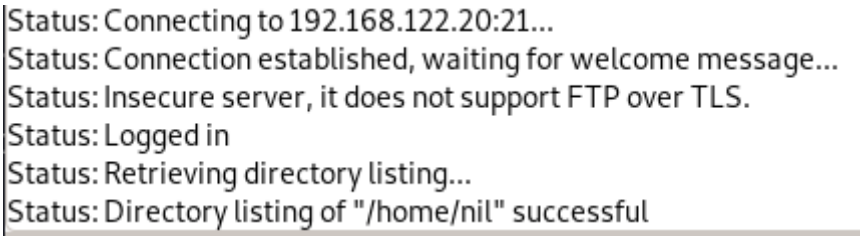
Apartat 6. Instal·lació en el client. (3,5p -0,5-1,5-1,5-)

a) Instal·la pure-ftpd en el servidor i, si és el cas, en el client. Configura'l perquè autentiqui al servidor LDAP i realitza les proves de funcionament.

```
root@us-nmc:~# ftp localhost
Connected to localhost.
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 23:15. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (localhost:nil): nil
331 User nil OK. Password required
Password:
230 OK. Current directory is /home/nil
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
  GNU nano 6.2                    /etc/pure-ftpd/auth/ldap.conf
LDAPServer ldap://localhost
LDAPDN "cn=admin,dc=srvldap,dc=masso,dc=com"
LDAPPW Aa12345678
LDAPBaseDN "dc=srvldap,dc=masso,dc=com"
LDAPFilter "(uid=\L)"
LDAPUIDAttribute uid
LDAPGIDAttribute gidNumber
LDAPHomeDirAttribute homeDirectory
LDAPLoginShellAttribute loginShell
```

b) Instal·la LDAP en un client, indica què instal·les i les passes que segueixes . I fes login amb un usuari del servidor LDAP.



c) Instal·la un moodle en un altre linux. Fes que faci l'autenticació al servidor LDAP.

Apartat 7. Documentació. (0,5p)

- Realitza la documentació de tots els passos. Cal fer-ho de forma ordenada i poder veure clarament quin punt s'està resolent.
- Es valorarà la senzillesa de la solució. El temps és limitat, la complicació excessiva penalitza.