

PRÁCTICA 2.1. INSTALACIÓN Y CONFIGURACIÓN DE OpenLDAP.

Antes de comenzar a instalar, asegúrate la versión de los paquetes que debes usar según tu distribución <https://www.server-world.info>

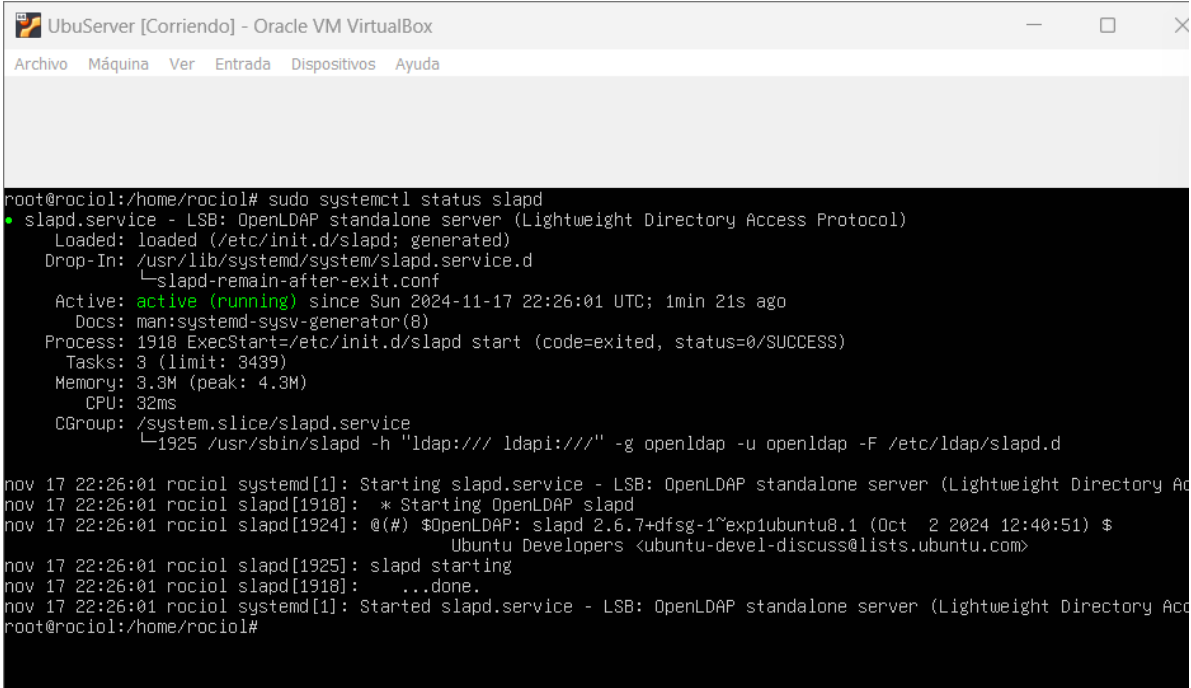
1) **Instala el servicio OpenLDAP según la documentación (*usa el mismo nombre de dominio que para ActiveDirectory*).**

- Durante la instalación, elige el motor de búsqueda recomendado en la propia instalación.
- Introduce el dominio y resto de configuración básica con
`# dpkg-reconfigure slapd`

Instalamos el servicio OpenLDAP: (Nos pedirá la contraseña del administrador

```
root@rociol:/var/lib/ldap# sudo apt install slapd ldap-utils
```

Probamos que esté funcionando:



```
UbuServer [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

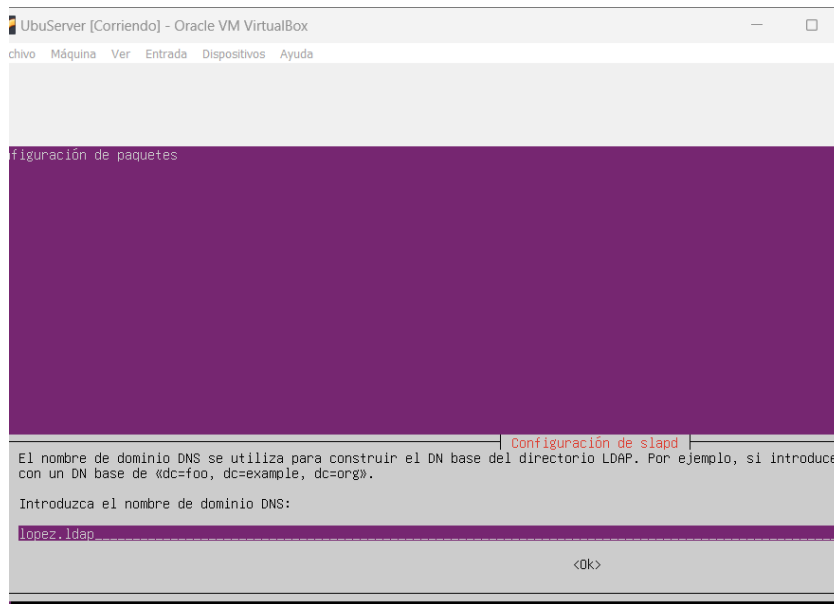
root@rociol:/home/rociol# sudo systemctl status slapd
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
   Loaded: loaded (/etc/init.d/slapd; generated)
   Drop-In: /usr/lib/systemd/system/slapd.service.d
            └─slapd-remain-after-exit.conf
   Active: active (running) since Sun 2024-11-17 22:26:01 UTC; 1min 21s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 1918 ExecStart=/etc/init.d/slapd start (code=exited, status=0/SUCCESS)
    Tasks: 3 (limit: 3439)
   Memory: 3.3M (peak: 4.3M)
      CPU: 32ms
   CGroup: /system.slice/slapd.service
           └─1925 /usr/sbin/slapd -h "ldap:/// ldapi:///" -g openldap -u openldap -F /etc/ldap/slapd.d

nov 17 22:26:01 rociol systemd[1]: Starting slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol):
nov 17 22:26:01 rociol slapd[1918]: * Starting OpenLDAP slapd
nov 17 22:26:01 rociol slapd[1924]: @(#) $OpenLDAP: slapd 2.6.7+dfsg-1~exp1ubuntu8.1 (Oct  2 2024 12:40:51) $
                        Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
nov 17 22:26:01 rociol slapd[1925]: slapd starting
nov 17 22:26:01 rociol slapd[1918]: ...done.
nov 17 22:26:01 rociol systemd[1]: Started slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol):
root@rociol:/home/rociol#
```

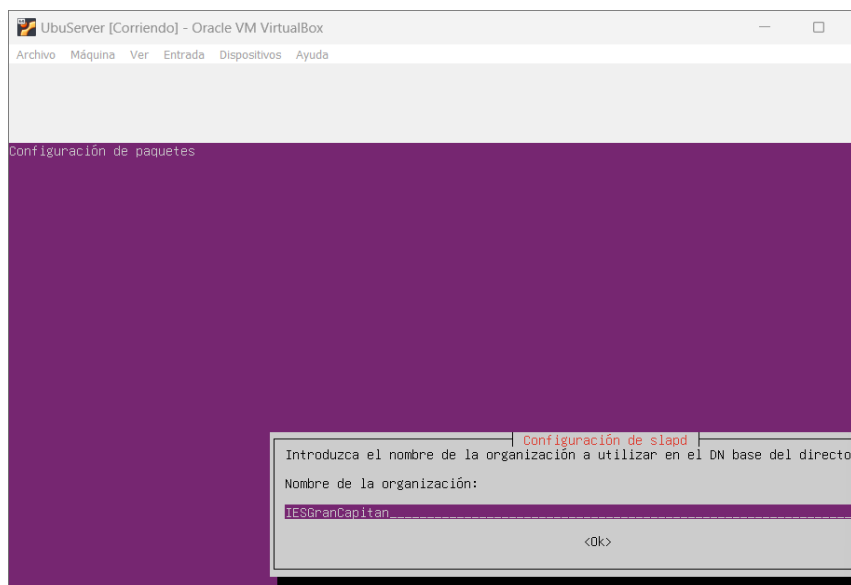
Introduce el dominio y resto de configuración básica con
dpkg-reconfigure slapd

```
rociol@rociol: ~  
rociol@rociol:~$ dpkg-reconfigure slapd
```

Primero configuraremos el nombre de dominio:



Luego ponemos el nombre de la organización:



Ahora nos pedirá la contraseña (Usuario123@):

Por último, nos dará dos opciones donde marcaremos primero no, y después yes.

- Que cuando se purge el paquete la base de datos no se elimine
- Que se muevan las antiguas base de datos a otro lado

- 2) **Comprueba con #slapcat que la estructura básica del árbol LDAP ya ha sido creada.**
Si has tenido algún problema o equivocación, haz de nuevo un `dpkg-reconfigure slapd`.

```
root@rociol: /home/rociol  X  +  v

root@rociol:/home/rociol# sudo slapcat
dn: dc=lopez,dc=ldap
objectClass: top
objectClass: dcObject
objectClass: organization
o: IESGranCapitan
dc: lopez
structuralObjectClass: organization
entryUUID: 873911d8-3b85-103f-91e4-ab627bd71dff
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120122009Z
entryCSN: 20241120122009.312333Z#000000#000#000000
modifiersName: cn=admin,dc=lopez,dc=ldap
modifyTimestamp: 20241120122009Z

root@rociol:/home/rociol# |
```

- 3) **Contesta a las siguientes preguntas:**

- a) ¿Qué puerto usa LDAP? Comprueba que está levantado mediante NMAP (instálalo si no lo tienes instalado).
- Como se muestra, LDAP utiliza el puerto 389 con el protocolo TCP.

```
root@rociol:/var/lib/ldap# nmap -v 192.168.9.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-20 17:22 UTC
Initiating Parallel DNS resolution of 1 host. at 17:22
Completed Parallel DNS resolution of 1 host. at 17:22, 0.04s elapsed
Initiating SYN Stealth Scan at 17:22
Scanning rociol (192.168.9.9) [1000 ports]
Discovered open port 22/tcp on 192.168.9.9
Discovered open port 80/tcp on 192.168.9.9
Discovered open port 389/tcp on 192.168.9.9
Completed SYN Stealth Scan at 17:22, 0.44s elapsed (1000 total ports)
Nmap scan report for rociol (192.168.9.9)
Host is up (0.000020s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
389/tcp    open  ldap

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds
Raw packets sent: 1000 (44.000KB) | Rcvd: 2003 (84.132KB)
root@rociol:/var/lib/ldap#
```

b) ¿Dónde se guarda la configuración de LDAP? Busca el fichero ldap.conf y observa si tienes que modificar algo.

- Se guarda en el archivo /etc/ldap/ldap.conf.
- Modificamos el archivo con el nombre de nuestro dominio.

```
GNU nano 7.2 /etc/ldap/ldap.conf
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE    dc=lopez,dc=ldap
URI      ldap://192.168.9.9

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
TLS_CACERT      /etc/ssl/certs/ca-certificates.crt
```

- 4) **Crear para el dominio una estructura de unidades organizativas donde se puedan dar de alta los usuarios del CFGS ASIR (1º y 2º de ASIR) y CFGS DAW (en la organización iesgrancapitan.**

Condiciones:

- Como mínimo debe incluirse en el árbol al profesorado, alumnado, y los cursos.
- Añadir los grupos de 1º Y 2º de ASIR y DAW

- a) **Crea el archivo. ldif con la información de las Ous. Llama al fichero /var/lib/ldap/OUs.ldif**

Nota: recuerda parar el servicio para añadir los elementos y reiniciarlo al finalizar.

```
GNU nano 7.2 OUs.ldif
# Crear la unidad organizativa 'grupos'
dn: ou=grupos,dc=pozo,dc=ldap
objectClass: top
objectClass: organizationalUnit
ou: grupos

# Crear la unidad organizativa 'maquinas'
dn: ou=maquinas,dc=pozo,dc=ldap
objectClass: top
objectClass: organizationalUnit
ou: maquinas

# Crear la unidad organizativa 'aula01' dentro de 'maquinas'
dn: ou=aula01,ou=maquinas,dc=pozo,dc=ldap
objectClass: top
objectClass: organizationalUnit
ou: aula01

# Crear la unidad organizativa 'usuarios'
dn: ou=usuarios,dc=pozo,dc=ldap
objectClass: top
objectClass: organizationalUnit
ou: usuarios

# Crear la unidad organizativa 'alumnos' dentro de 'usuarios'
dn: ou=alumnos,ou=usuarios,dc=pozo,dc=ldap
objectClass: top
objectClass: organizationalUnit
ou: alumnos

# Crear la unidad organizativa 'profes' dentro de 'usuarios'
dn: ou=profes,ou=usuarios,dc=pozo,dc=ldap
objectClass: top
objectClass: organizationalUnit
ou: profes
```

- b) **Usa la orden ldapadd para añadirlo al árbol.**

```
root@rociol: /var/lib/ldap
root@rociol:/var/lib/ldap# sudo ldapadd -x -D "cn=admin,dc=lopez,dc=ldap" -W -f /var/lib/ldap/OUs.ldif
Enter LDAP Password:
adding new entry "ou=grupos,dc=lopez,dc=ldap"

adding new entry "ou=maquinas,dc=lopez,dc=ldap"

adding new entry "ou=aula01,ou=maquinas,dc=lopez,dc=ldap"

adding new entry "ou=usuarios,dc=lopez,dc=ldap"

adding new entry "ou=alumnos,ou=usuarios,dc=lopez,dc=ldap"

adding new entry "ou=profes,ou=usuarios,dc=lopez,dc=ldap"

root@rociol:/var/lib/ldap#
```

c) Muestra el resultado con slapcat

```
root@rociol: /var/lib/ldap
root@rociol:/var/lib/ldap# slapcat
dn: dc=lopez,dc=ldap
objectClass: top
objectClass: dcObject
objectClass: organization
o: IESGranCapitan
dc: lopez
structuralObjectClass: organization
entryUUID: c60047ea-3baf-103f-8d16-412c0c311c36
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120172233Z
entryCSN: 20241120172233.499309Z#000000#000#000000
modifiersName: cn=admin,dc=lopez,dc=ldap
modifyTimestamp: 20241120172233Z

dn: ou=grupos,dc=lopez,dc=ldap
objectClass: top
objectClass: organizationalUnit
ou: grupos
structuralObjectClass: organizationalUnit
entryUUID: feffa98-3bb0-103f-9167-81ae08300a61
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120173118Z
entryCSN: 20241120173118.618506Z#000000#000#000000
modifiersName: cn=admin,dc=lopez,dc=ldap
modifyTimestamp: 20241120173118Z

dn: ou=maquinas,dc=lopez,dc=ldap
objectClass: top
objectClass: organizationalUnit
ou: maquinas
structuralObjectClass: organizationalUnit
entryUUID: ff0c003c-3bb0-103f-9168-81ae08300a61
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120173118Z
entryCSN: 20241120173118.703065Z#000000#000#000000
modifiersName: cn=admin,dc=lopez,dc=ldap
modifyTimestamp: 20241120173118Z

dn: ou=aula01,ou=maquinas,dc=lopez,dc=ldap
objectClass: top
objectClass: organizationalUnit
ou: aula01
structuralObjectClass: organizationalUnit
entryUUID: ff103d3c-3bb0-103f-9169-81ae08300a61
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120173118Z
entryCSN: 20241120173118.730007Z#000000#000#000000
modifiersName: cn=admin,dc=lopez,dc=ldap
modifyTimestamp: 20241120173118Z

dn: ou=usuarios,dc=lopez,dc=ldap
objectClass: top
objectClass: organizationalUnit
ou: usuarios
structuralObjectClass: organizationalUnit
entryUUID: ff12c012-3bb0-103f-916a-81ae08300a61
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120173118Z
entryCSN: 20241120173118.747520Z#000000#000#000000
modifiersName: cn=admin,dc=lopez,dc=ldap
modifyTimestamp: 20241120173118Z

dn: ou=alumnos,ou=usuarios,dc=lopez,dc=ldap
objectClass: top
objectClass: organizationalUnit
ou: alumnos
structuralObjectClass: organizationalUnit
entryUUID: ff15211c-3bb0-103f-916b-81ae08300a61
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120173118Z
entryCSN: 20241120173118.762895Z#000000#000#000000
modifiersName: cn=admin,dc=lopez,dc=ldap
modifyTimestamp: 20241120173118Z

dn: ou=profes,ou=usuarios,dc=lopez,dc=ldap
objectClass: top
objectClass: organizationalUnit
ou: : wq8wcm9wZXN=
structuralObjectClass: organizationalUnit
entryUUID: ff17b742-3bb0-103f-916c-81ae08300a61
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120173118Z
entryCSN: 20241120173118.779836Z#000000#000#000000
modifiersName: cn=admin,dc=lopez,dc=ldap
modifyTimestamp: 20241120173118Z
root@rociol:/var/lib/ldap#
```

5) Crear una serie de usuarios y grupos en LDAP mediante las herramientas de consola.

Condiciones:

- Un alumno solo puede estar en 1º de Asir o en 2º Asir.
- Un profesor puede dar clase en los dos cursos

1. Grupos

- Son objetos tipo **objectClass: posixGroup**.

- Los grupos tendrán atributo gid y gidnumber. Hay que tener cuidado de no asignarle un valor ya usado por el sistema, así que usa un valor elevado para que no coincida con alguno ya existente en el sistema (Ej. 10000, 20000 y 30000)

2. Usuarios

- Son objetos tipo **posixAccount**, pero también **inetOrgPerson**, y **shadowAccount**

- Serán: asir1_1, asir1_2, asir1_3, asir2_1, asir2_2 y profe1, profe2, profe3

- Los usuarios tendrán atributo cn y uid.

- Los usuarios tendrán atributo uidNumber y gidNumber (según grupo al que queramos que pertenezcan). Dale un valor elevado para que no coincida con alguno ya existente en el sistema.

- Atributo userPassword: la contraseña debe estar encriptada.

Ejecuta **slappasswd** para generar una contraseña encriptada

Nota: ¡¡crear la misma contraseña “usuario” para todos!! Y copias y pegas en cada elemento del .ldif

- Atributo homeDirectory: los directorios de cada usuario se crearán en /home/usuariosldap/nombreuser (esto lo vamos a dejar así preparado para la siguiente práctica).

- a) **Prepara los archivos ldif. Los ficheros se llamarán /var/lib/ldap/grupos.ldif y usuarios.ldif.**

Empezaremos creando el archivo grupos.ldif

```
root@rociol: /var/lib/ldap
GNU nano 7.2                                grupos.ldif
# Crear el grupo 'asir1'
dn: cn=asir1,ou=grupos,dc=lopez,dc=ldap
objectClass: top
objectClass: posixGroup
cn: asir1
gidNumber: 10000
description: Grupo ASIR 1

# Crear el grupo 'asir2'
dn: cn=asir2,ou=grupos,dc=lopez,dc=ldap
objectClass: top
objectClass: posixGroup
cn: asir2
gidNumber: 10001
description: Grupo ASIR 2

# Crear el grupo 'profes'
dn: cn=profes,ou=grupos,dc=lopez,dc=ldap
objectClass: top
objectClass: posixGroup
cn: profes
gidNumber: 10002
description: Grupo de Profesores
```


Antes de hacer el archivo de usuarios, deberemos crear una contraseña encriptada (Usuario123@)

{SSHA}NvQp/GOXStP4z8ajrbz9K0inRx6sia+S

```
root@rociol: /home/rociol
root@rociol:/home/rociol# slappasswd
New password:
Re-enter new password:
{SSHA}NvQp/GOXStP4z8ajrbz9K0inRx6sia+S
root@rociol:/home/rociol#
```

Ahora crearemos el archivo usuarios.ldif, usaremos la contraseña encriptada para todos los usuarios:

```
root@rociol: /var/lib/ldap
GNU nano 7.2 usuarios.ldif
# Crear los usuarios (alumnos)

#asir11
dn: uid=asir1_1,ou=alumnos,ou=usuarios,dc=lopez,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: asir1_1
cn: Asir 1.1
sn: 1.1
uidNumber: 20000
gidNumber: 10000
homeDirectory: /home/usuariosldap/asir1_1
userPassword: {SSHA}NvQp/GOXStP4z8ajrbz9K0inRx6sia+S

#asir12
dn: uid=asir1_2,ou=alumnos,ou=usuarios,dc=lopez,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: asir1_2
cn: Asir 1.2
sn: 1.2
uidNumber: 20001
gidNumber: 10000
homeDirectory: /home/usuariosldap/asir1_2
userPassword: {SSHA}NvQp/GOXStP4z8ajrbz9K0inRx6sia+S

#asir13
dn: uid=asir1_3,ou=alumnos,ou=usuarios,dc=lopez,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: asir1_3
cn: Asir 1.3
sn: 1.3
uidNumber: 20002
gidNumber: 10000
homeDirectory: /home/usuariosldap/asir1_3
userPassword: {SSHA}NvQp/GOXStP4z8ajrbz9K0inRx6sia+S

#asir21
dn: uid=asir2_1,ou=alumnos,ou=usuarios,dc=lopez,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: asir2_1
cn: Asir 2.1
sn: 2.1
uidNumber: 20003
gidNumber: 10001
homeDirectory: /home/usuariosldap/asir2_1
userPassword: {SSHA}NvQp/GOXStP4z8ajrbz9K0inRx6sia+S

#asir22
dn: uid=asir2_2,ou=alumnos,ou=usuarios,dc=lopez,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: asir2_2
cn: Asir 2.2
sn: 2.2
uidNumber: 20004
gidNumber: 10001
homeDirectory: /home/usuariosldap/asir2_2
userPassword: {SSHA}NvQp/GOXStP4z8ajrbz9K0inRx6sia+S
```

```
# Crear los profesores

#profe1
dn: uid=profe1,ou=profes,ou=usuarios,dc=lopez,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: profe1
cn: Profe 1
sn: 1
uidNumber: 20005
gidNumber: 10002
homeDirectory: /home/usuariosldap/profe1
userPassword: {SSHA}NvQp/GOXStP4z8ajrbz9K0inRx6sia+S

#profe2
dn: uid=profe2,ou=profes,ou=usuarios,dc=lopez,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: profe2
cn: Profe 2
sn: 2
uidNumber: 20006
gidNumber: 10002
homeDirectory: /home/usuariosldap/profe2
userPassword: {SSHA}NvQp/GOXStP4z8ajrbz9K0inRx6sia+S

#profe3
dn: uid=profe3,ou=profes,ou=usuarios,dc=lopez,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: profe3
cn: Profe 3
sn: 3
uidNumber: 20007
gidNumber: 10002
homeDirectory: /home/usuariosldap/profe3
userPassword: {SSHA}NvQp/GOXStP4z8ajrbz9K0inRx6sia+S
```

b) Añádelos al árbol y muestra el nuevo árbol con slapcat

- Los añadimos:

```
root@rociol: /var/lib/ldap # sudo ldapadd -x -D "cn=admin,dc=lopez,dc=ldap" -W -f /var/lib/ldap/grupos.ldif
Enter LDAP Password:
adding new entry "cn=asir1,ou=grupos,dc=lopez,dc=ldap"

adding new entry "cn=asir2,ou=grupos,dc=lopez,dc=ldap"

adding new entry "cn=profes,ou=grupos,dc=lopez,dc=ldap"

root@rociol: /var/lib/ldap # |
```

```
root@rociol: /var/lib/ldap # sudo ldapadd -x -D "cn=admin,dc=lopez,dc=ldap" -W -f /var/lib/ldap/usuarios.ldif
Enter LDAP Password:
adding new entry "uid=asir1_1,ou=alumnos,ou=usuarios,dc=lopez,dc=ldap"

adding new entry "uid=asir1_2,ou=alumnos,ou=usuarios,dc=lopez,dc=ldap"

adding new entry "uid=asir1_3,ou=alumnos,ou=usuarios,dc=lopez,dc=ldap"

adding new entry "uid=asir2_1,ou=alumnos,ou=usuarios,dc=lopez,dc=ldap"

adding new entry "uid=asir2_2,ou=alumnos,ou=usuarios,dc=lopez,dc=ldap"

adding new entry "uid=profe1,ou=profes,ou=usuarios,dc=lopez,dc=ldap"

adding new entry "uid=profe2,ou=profes,ou=usuarios,dc=lopez,dc=ldap"

adding new entry "uid=profe3,ou=profes,ou=usuarios,dc=lopez,dc=ldap"

root@rociol: /var/lib/ldap # |
```

- ```
root@rociol:/var/lib/ldap# dn: cn=loper,dc=ldap
objectClass: top
objectClass: dcObject
objectClass: organization
o: IESGranCapitan
dc: lopez
structuralObjectClass: organization
entryUUID: 6d8ff80b-3b87-183f-83ef-c0000ff666da
creatorName: cn=admin,dc=loper,dc=ldap
createTimestamp: 202411201233802
entryCN: 20241120123380 76461322000000000000000000000000
modifiersName: cn=admin,dc=loper,dc=ldap
modifyTimestamp: 202411201233802

dn: ou=grupos,dc=loper,dc=ldap
objectClass: top
objectClass: organizationalUnit
ou: grupos
structuralObjectClass: organizationalUnit
entryUUID: d0e2cec2-3b87-183f-9c2a-955e727395c
creatorName: cn=admin,dc=loper,dc=ldap
createTimestamp: 202411201236382
entryCN: 20241120123638 66237020000000000000000000000000
modifiersName: cn=admin,dc=loper,dc=ldap
modifyTimestamp: 202411201236382

dn: ou=maquinas,dc=loper,dc=ldap
objectClass: top
objectClass: organizationalUnit
ou: maquinas
structuralObjectClass: organizationalUnit
entryUUID: d0e4ab1b-3b87-183f-9c2b-955e727395c
creatorName: cn=admin,dc=loper,dc=ldap
createTimestamp: 202411201236382
entryCN: 20241120123638 61506620000000000000000000000000
modifiersName: cn=admin,dc=loper,dc=ldap
modifyTimestamp: 202411201236382

dn: ou=aula01,ou=maquinas,dc=loper,dc=ldap
objectClass: top
objectClass: organizationalUnit
ou: aula01
structuralObjectClass: organizationalUnit
entryUUID: d0e80dae-3b87-183f-9c2c-955e727395c
creatorName: cn=admin,dc=loper,dc=ldap
createTimestamp: 202411201236382
entryCN: 20241120123638 67956700000000000000000000000000
modifiersName: cn=admin,dc=loper,dc=ldap
modifyTimestamp: 202411201236382

dn: ou=usuarios,dc=loper,dc=ldap
objectClass: top
objectClass: organizationalUnit
ou: usuarios
structuralObjectClass: organizationalUnit
entryUUID: d0e8cd3c-3b87-183f-9c2d-955e727395c
creatorName: cn=admin,dc=loper,dc=ldap
createTimestamp: 202411201236382
entryCN: 20241120123638 60211820000000000000000000000000
modifiersName: cn=admin,dc=loper,dc=ldap
modifyTimestamp: 202411201236382

dn: ou=alumnos,ou=usuarios,dc=loper,dc=ldap
objectClass: top
objectClass: organizationalUnit
ou: alumnos
structuralObjectClass: organizationalUnit
entryUUID: d0e9ccab-3b87-183f-9c2e-955e727395c
creatorName: cn=admin,dc=loper,dc=ldap
createTimestamp: 202411201236382
entryCN: 20241120123638 60470220000000000000000000000000
modifiersName: cn=admin,dc=loper,dc=ldap
modifyTimestamp: 202411201236382

dn: ou=profes,ou=usuarios,dc=loper,dc=ldap
objectClass: top
objectClass: organizationalUnit
ou: asBeca9a220e
structuralObjectClass: organizationalUnit
entryUUID: d0eac8dc-3b87-183f-9c2f-955e727395c
creatorName: cn=admin,dc=loper,dc=ldap
createTimestamp: 202411201236382
entryCN: 20241120123638 66323120000000000000000000000000
modifiersName: cn=admin,dc=loper,dc=ldap
modifyTimestamp: 202411201236382

dn: cn=asir1,ou=grupos,dc=loper,dc=ldap
objectClass: top
objectClass: posixGroup
cn: asir1
gidNumber: 10000
description: Grupo ASIR 1
structuralObjectClass: posixGroup
entryUUID: 581e671b-3b87-183f-9c30-955e727395c
creatorName: cn=admin,dc=loper,dc=ldap
createTimestamp: 202411201207282
entryCN: 20241120120728 27197820000000000000000000000000
modifiersName: cn=admin,dc=loper,dc=ldap
modifyTimestamp: 202411201207282
```

```
root@kali: /var/lib/ldap
```

```
dn: cn=asir2,ou=grupos,dc=lopez,dc=ldap
objectClass: top
objectClass: posixGroup
cn: asir2
gidNumber: 10001
description: Grupo ASIR 2
structuralObjectClass: posixGroup
entryUUID: 5821f7ee-3b09-103f-9c31-955e7275395c
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120124728Z
entryCSN: 20241120124728.2567928900000000000000000000000000
modifiersName: cn=admin,dc=lopez,dc=ldap
modifyTimestamp: 20241120124728Z

dn: cn=profes,ou=grupos,dc=lopez,dc=ldap
objectClass: top
objectClass: posixGroup
cn: profes
gidNumber: 10002
description: R3J1cG/CodRwgBQcw9wZXIvcvVz
structuralObjectClass: posixGroup
entryUUID: 582d0809-3b09-103f-9c31-955e7275395c
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120124728Z
entryCSN: 20241120124728.3137182f00000000000000000000000000
modifiersName: cn=admin,dc=lopez,dc=ldap
modifyTimestamp: 20241120124728Z

dn: uid=asirl_1,ou=alumnos,ou=usuarios,dc=lopez,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: asirl_1
cn: Asir 1.1
sn: 1.1
uidNumber: 20000
gidNumber: 10000
homeDirectory: /home/usuarios/ldap/asirl_1
userPassword:: e1kTSEF9tnZ8rc9Wt1htGFABejhanJieJlLT2Luwngc2clhkM1=
structuralObjectClass: inetOrgPerson
entryUUID: 619cf8fa-3b09-103f-9c31-955e7275395c
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120124740Z
entryCSN: 20241120124740.1730862f00000000000000000000000000
modifiersName: cn=admin,dc=lopez,dc=ldap
modifyTimestamp: 20241120124740Z

dn: uid=asirl_2,ou=alumnos,ou=usuarios,dc=lopez,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: asirl_2
cn: Asir 1.2
sn: 1.2
uidNumber: 20001
gidNumber: 10000
homeDirectory: /home/usuarios/ldap/asirl_2
userPassword:: e1kTSEF9tnZ8rc9Wt1htGFABejhanJieJlLT2Luwngc2clhkM1=
structuralObjectClass: inetOrgPerson
entryUUID: 619fd0ae-3b09-103f-9c31-955e7275395c
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120124740Z
entryCSN: 20241120124740.1963642f00000000000000000000000000
modifiersName: cn=admin,dc=lopez,dc=ldap
modifyTimestamp: 20241120124740Z

dn: uid=asirl_3,ou=alumnos,ou=usuarios,dc=lopez,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: asirl_3
cn: Asir 1.3
sn: 1.3
uidNumber: 20002
gidNumber: 10000
homeDirectory: /home/usuarios/ldap/asirl_3
userPassword:: e1kTSEF9tnZ8rc9Wt1htGFABejhanJieJlLT2Luwngc2clhkM1=
structuralObjectClass: inetOrgPerson
entryUUID: 619f5eca-3b09-103f-9c31-955e7275395c
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120124740Z
entryCSN: 20241120124740.2166482f00000000000000000000000000
modifiersName: cn=admin,dc=lopez,dc=ldap
modifyTimestamp: 20241120124740Z

dn: uid=asir2_1,ou=alumnos,ou=usuarios,dc=lopez,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: asir2_1
cn: Asir 2.1
sn: 2.1
uidNumber: 20003
gidNumber: 10001
homeDirectory: /home/usuarios/ldap/asir2_1
userPassword:: e1kTSEF9tnZ8rc9Wt1htGFABejhanJieJlLT2Luwngc2clhkM1=
structuralObjectClass: inetOrgPerson
entryUUID: 61a28aan-3b09-103f-9c31-955e7275395c
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120124740Z
```

```
root@rociol: /var/lib/ldap

dn: uid=asir2_2,ou=alumnos,ou=usuarios,dc=lopez,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: asir2_2
cn: Asir 2.2
sn: 2.2
uidNumber: 20004
gidNumber: 10001
homeDirectory: /home/usuariosldap/asir2_2
userPassword:: e1NTSEF9TnZRcC9HT1hTdFA0ejhhanJiejLLT2luUng2c2lhK1M=
structuralObjectClass: inetOrgPerson
entryUUID: 1d71a248-3bb1-103f-9174-81ae08300a61
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120173209Z
entryCSN: 20241120173209.700782Z#000000#000#000000
modifiersName: cn=admin,dc=lopez,dc=ldap
modifyTimestamp: 20241120173209Z

dn: uid=profe1,ou=profes,ou=usuarios,dc=lopez,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: profe1
cn: Profe 1
sn: 1
uidNumber: 20005
gidNumber: 10002
homeDirectory: /home/usuariosldap/profe1
userPassword:: e1NTSEF9TnZRcC9HT1hTdFA0ejhhanJiejLLT2luUng2c2lhK1M=
structuralObjectClass: inetOrgPerson
entryUUID: 1d77b836-3bb1-103f-9175-81ae08300a61
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120173209Z
entryCSN: 20241120173209.740666Z#000000#000#000000
modifiersName: cn=admin,dc=lopez,dc=ldap
modifyTimestamp: 20241120173209Z

dn: uid=profe2,ou=profes,ou=usuarios,dc=lopez,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: profe2
cn: Profe 2
sn: 2
uidNumber: 20006
gidNumber: 10002
homeDirectory: /home/usuariosldap/profe2
userPassword:: e1NTSEF9TnZRcC9HT1hTdFA0ejhhanJiejLLT2luUng2c2lhK1M=
structuralObjectClass: inetOrgPerson
entryUUID: 1d7a9d44-3bb1-103f-9176-81ae08300a61
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120173209Z
entryCSN: 20241120173209.750617Z#000000#000#000000
modifiersName: cn=admin,dc=lopez,dc=ldap
modifyTimestamp: 20241120173209Z

dn: uid=profe3,ou=profes,ou=usuarios,dc=lopez,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: profe3
cn: Profe 3
sn: 3
uidNumber: 20007
gidNumber: 10002
homeDirectory: /home/usuariosldap/profe3
userPassword:: e1NTSEF9TnZRcC9HT1hTdFA0ejhhanJiejLLT2luUng2c2lhK1M=
structuralObjectClass: inetOrgPerson
entryUUID: 1d7ce022-3bb1-103f-9177-81ae08300a61
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120173209Z
entryCSN: 20241120173209.774453Z#000000#000#000000
modifiersName: cn=admin,dc=lopez,dc=ldap
modifyTimestamp: 20241120173209Z
```

- 6) **Utilidades:** usa la orden de consola *ldapsearch* para encontrar un usuario y comprobar que se han creado adecuadamente.

Ayuda: [UTILIDADES](#) de ldap

```
root@rociol: /var/lib/ldap × + v
root@rociol:/var/lib/ldap# ldapsearch -x -D "cn=admin,dc=lopez,dc=ldap" -W -b "dc=lopez,dc=ldap" "(uid=asir1_3)"
Enter LDAP Password:
extended LDIF
#
LDAPv3
base <dc=lopez,dc=ldap> with scope subtree
filter: (uid=asir1_3)
requesting: ALL
#
asir1_3, alumnos, usuarios, lopez.ldap
dn: uid=asir1_3,ou=alumnos,ou=usuarios,dc=lopez,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: asir1_3
cn: Asir 1.3
sn: 1.3
uidNumber: 20002
gidNumber: 10000
homeDirectory: /home/usuariosldap/asir1_3
userPassword:: e1NTSEF9TnZRcC9HT1hTdFA0ejhhanJiej\LT2luUng2c2lhK1M=

search result
search: 2
result: 0 Success

numResponses: 2
numEntries: 1
root@rociol:/var/lib/ldap# |
```

- 7) Instalar una herramienta gráfica (phpldapadmin o LAM-ldap account manager) en alguna máquina de la red y comprobar mediante un navegador la configuración realizada desde consola.

a) Instalar LAM-ldap

```
root@rociol: /home/rociol × + v
root@rociol:/home/rociol# sudo apt install ldap-account-manager
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
```

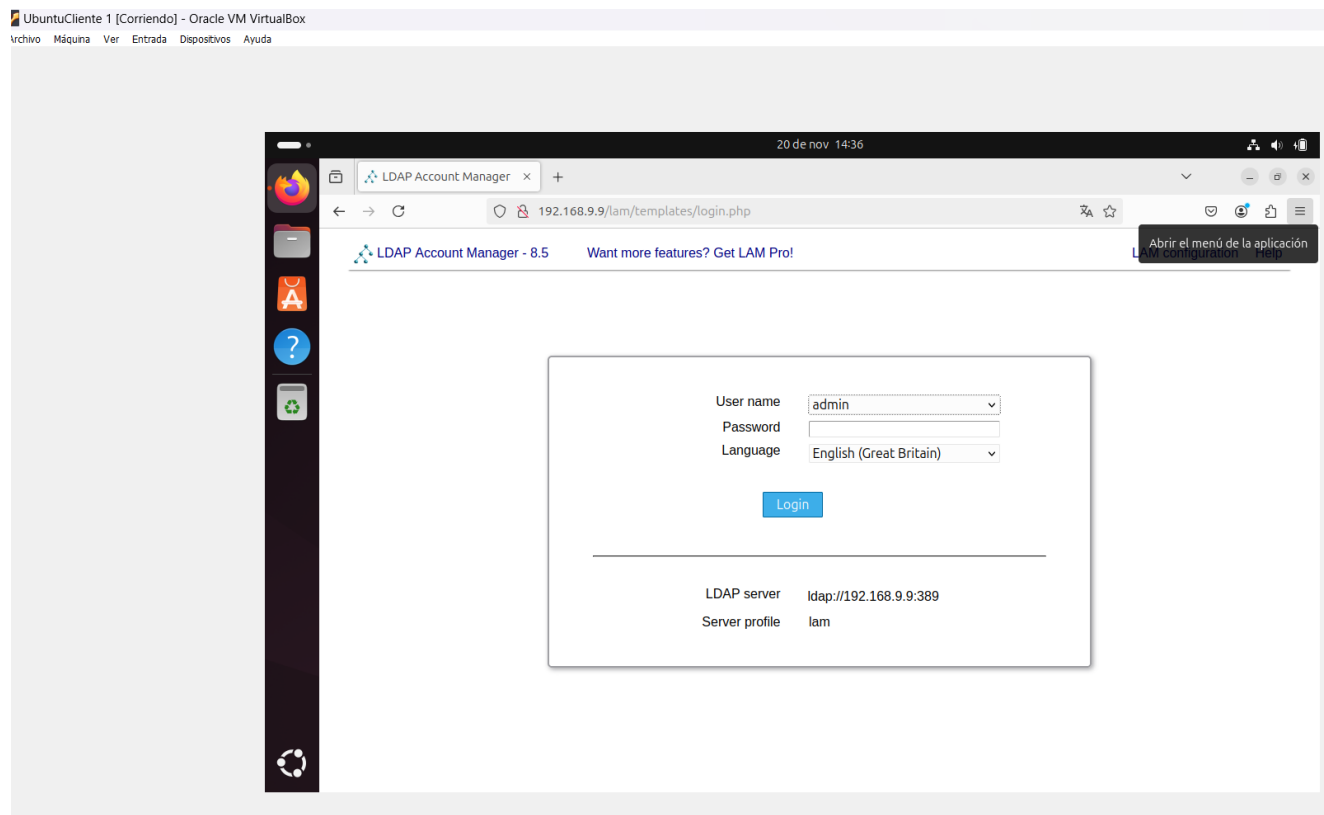
b) Configurar correctamente la herramienta: por defecto trae configurado como servidor example.com así que hay que sustituirlo por nuestros "dc" y al administrador por el nombre que le dimos

- Si usas ldap account manager: /usr/share/ldap-account-manager/config/lam.conf (cambiar manager por admin)

```
GNU nano 7.2 /usr/share/ldap-account-manager/config/lam.conf
LDAP Account Manager configuration
#
Please do not modify this file manually. The configuration can be done completely by the LAM GUI.
#
#####
server address (e.g. ldap://localhost:389 or ldaps://localhost:636)
ServerURL: ldap://192.168.9.9:389
list of users who are allowed to use LDAP Account Manager
names have to be separated by semicolons
e.g. admins: cn=admin,dc=yourdomain,dc=org;cn=root,dc=yourdomain,dc=org
Admins: cn=admin,dc=lopez,dc=ldap
password to change these preferences via webfrontend (default: lam)
Passwd: Usuario123@
suffix of tree view
e.g. dc=yourdomain,dc=org
tools: treeViewSuffix: dc=lopez,dc=ldap
```

```
types: suffix_user: dc=lopez,dc=ldap
types: attr_user: #uid;#givenName;#sn;#uidNumber;#gidNumber
types: modules_user: inetOrgPerson, posixAccount, shadowAccount
types: suffix_group: dc=lopez,dc=ldap
types: attr_group: #cn;#gidNumber;#memberUID;#description
types: modules_group: posixGroup
```

c) Desde un navegador, acceder a la herramienta:  
- http://IP/lam



LDAP Account Manager - 8.5 admin Accounts Tools Help Logout

### Users

[New user](#) [File upload](#) [Delete selected users](#) lopez > ldap

User count: 8

| Actions                         | User name | First name | Last name | UID number | GID number |
|---------------------------------|-----------|------------|-----------|------------|------------|
| Sort sequence                   |           |            |           |            |            |
| <input type="checkbox"/> Filter |           |            |           |            |            |
| <input type="checkbox"/>        | asir1_1   | 1.1        |           | 20000      | 10000      |
| <input type="checkbox"/>        | asir1_2   | 1.2        |           | 20001      | 10000      |
| <input type="checkbox"/>        | asir1_3   | 1.3        |           | 20002      | 10000      |
| <input type="checkbox"/>        | asir2_1   | 2.1        |           | 20003      | 10001      |
| <input type="checkbox"/>        | asir2_2   | 2.2        |           | 20004      | 10001      |
| <input type="checkbox"/>        | profe1    | 1          |           | 20005      | 10002      |
| <input type="checkbox"/>        | profe2    | 2          |           | 20006      | 10002      |
| <input type="checkbox"/>        | profe3    | 3          |           | 20007      | 10002      |



## 8) CONCLUSIÓN

a) *Haz una tabla indicando la paquetería instalada en el servidor y su utilidad. Esta tabla debes ir rellenándola durante el desarrollo de la práctica.*

| Paquete instalado en server | Versión        | Descripción                                                                                                                   |
|-----------------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------|
| Slapd                       | Última versión | LDAP gestiona y almacena información jerárquica de directorios, como usuarios y grupos.                                       |
| Ldap-utils                  | Última versión | Conjunto de herramientas de línea de comandos para interactuar con servidores LDAP, como buscar, agregar o eliminar entradas. |
| Nmap                        | Última versión | Herramienta de análisis de redes que permite descubrir hosts, puertos abiertos y servicios activos en una red.                |
| Ldap-account-manager        | Última versión | Interfaz web para gestionar usuarios, grupos y recursos en servidores LDAP de manera más fácil y visual.                      |

b) *Haz otra tabla indicando los ficheros de configuración que has tenido que modificar.*

| Fichero modificado | Path                                            | Modificación                                        |
|--------------------|-------------------------------------------------|-----------------------------------------------------|
| Ldap.conf          | /etc/ldap/ldap.conf                             | Cambiar configuración con nuestro dominio e ip      |
| Ous.ldif           | /var/lib/ldap/ous.ldif                          | Crear todas las OUs                                 |
| grupos.ldif        | /var/lib/ldap/grupos.ldif                       | Crear grupos                                        |
| usuarios.ldif      | /var/lib/ldap/usuarios.ldif                     | Crear usuarios                                      |
| Lam.conf           | /usr/share/ldap-account-manager/config/lam.conf | Modificar líneas para que funcione el ldap-manager. |