

# PRACTICA

## LDAP

### LDAP

LDAP, es un **protocolo** que ofrece el acceso a un **servicio de directorio** implementado sobre un entorno de red, con el objeto de **acceder** a una determinada **información**.

### Ejemplo de configuración práctico

Partimos como ejemplo de la Versión SO Ubuntu 20.04 LTS

```
fran@fran:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:   Ubuntu 22.04.1 LTS
Release:      22.04
Codename:     jammy
fran@fran:~$
```

Comprobar conexión a Internet, IP fija y repositorios actualizados

```
fran@fran:~$ sudo apt update
[sudo] password for fran:
```

### Procedimiento de instalación del servicio LDAP

Se instala el demonio del servicio, junto con sus utilidades:

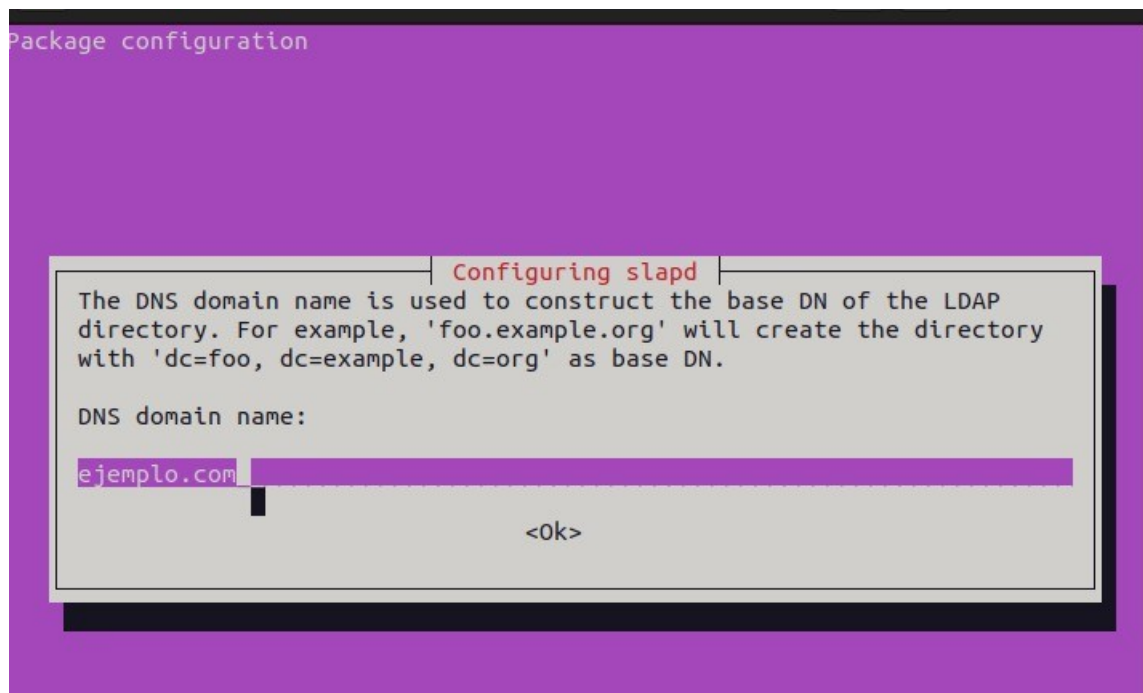
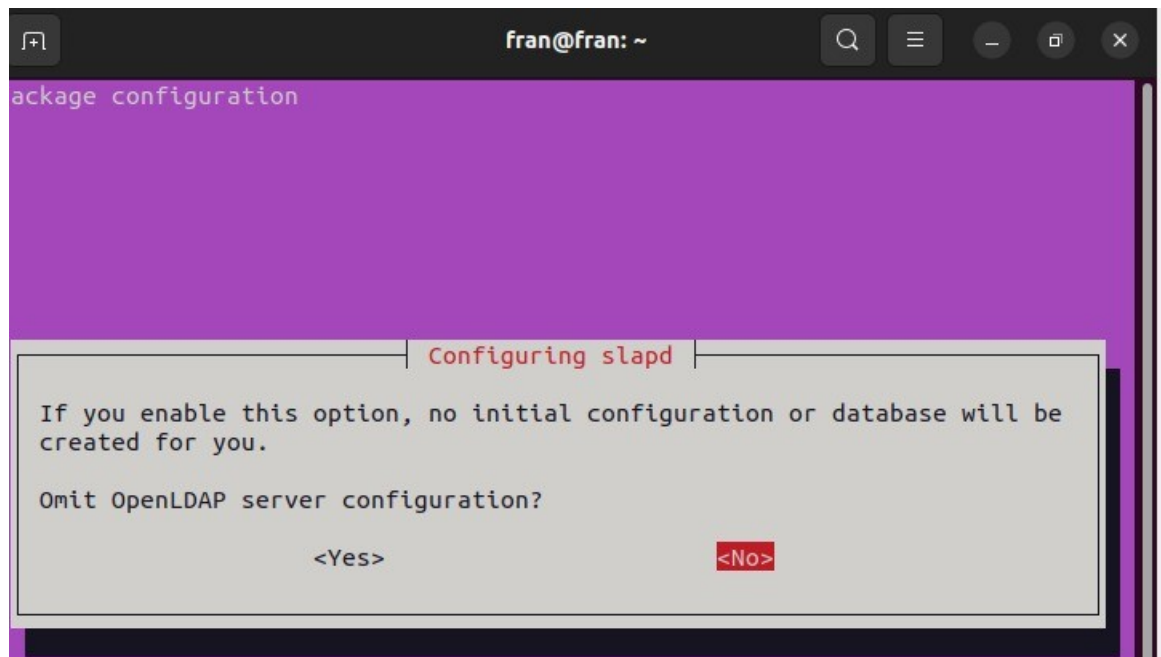
```
fran@fran:~$ sudo apt-get install slapd ldap-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required
 libflashrom1 libftdi1-2 libllvm13 linux-headers-5.15.0-43
 linux-headers-5.15.0-43-generic linux-headers-5.15.0-58
```

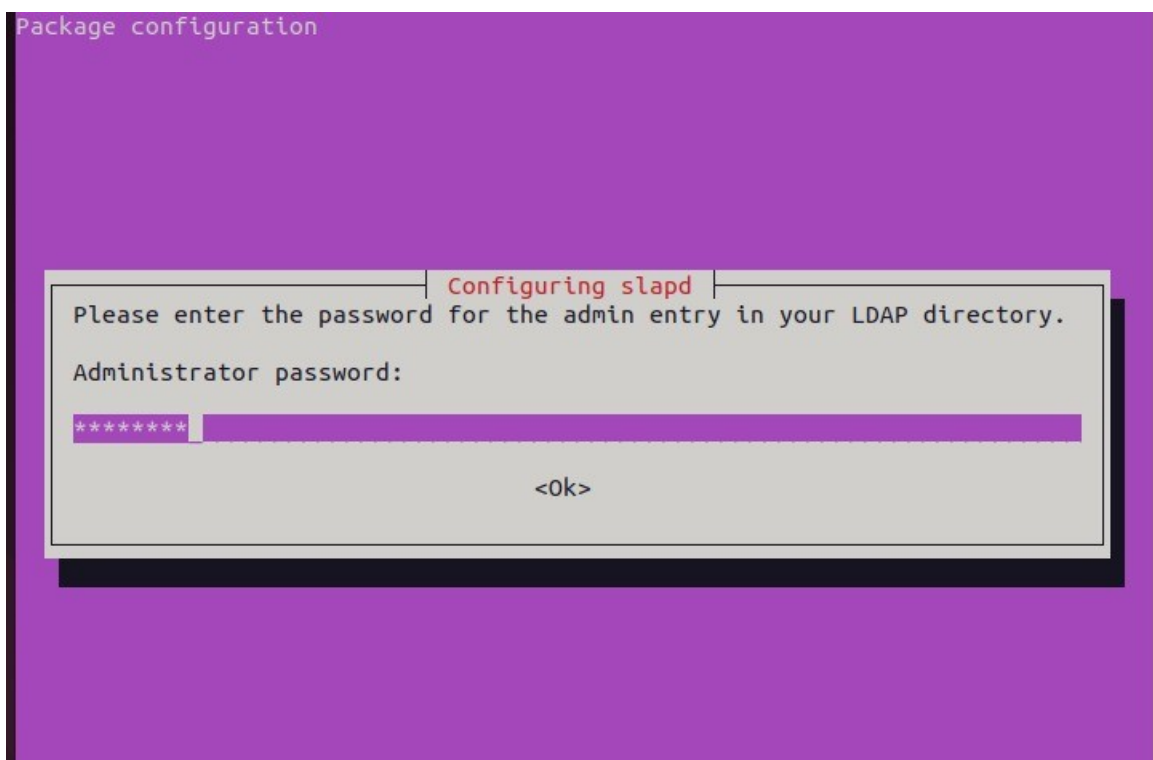
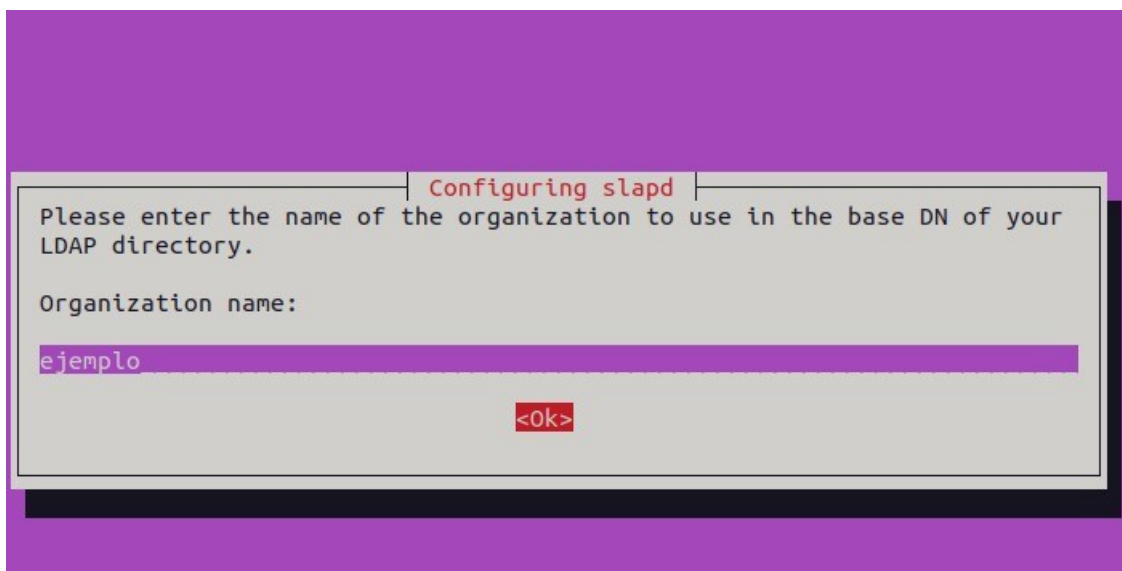
### Configurar slapd

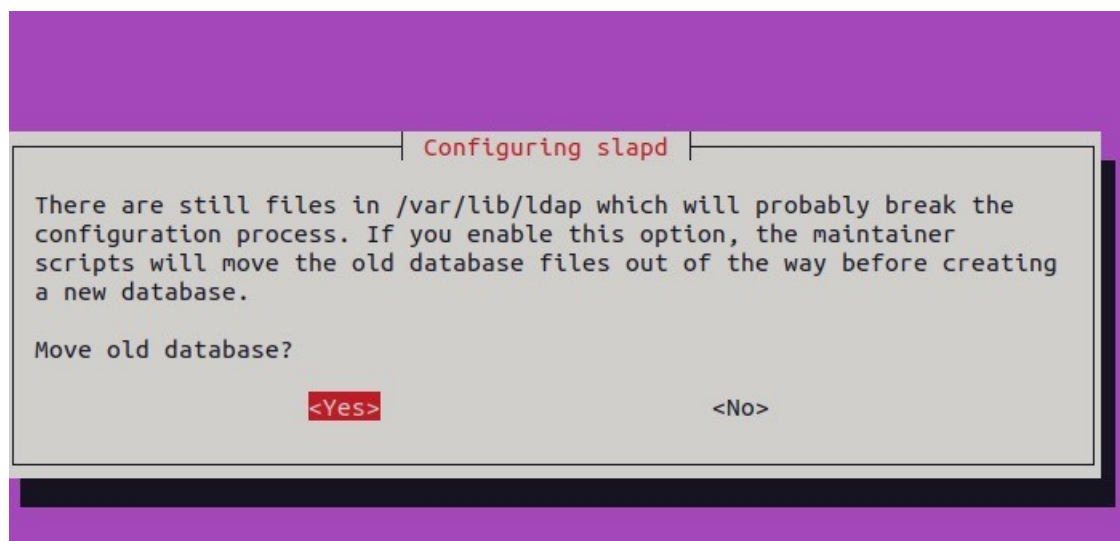
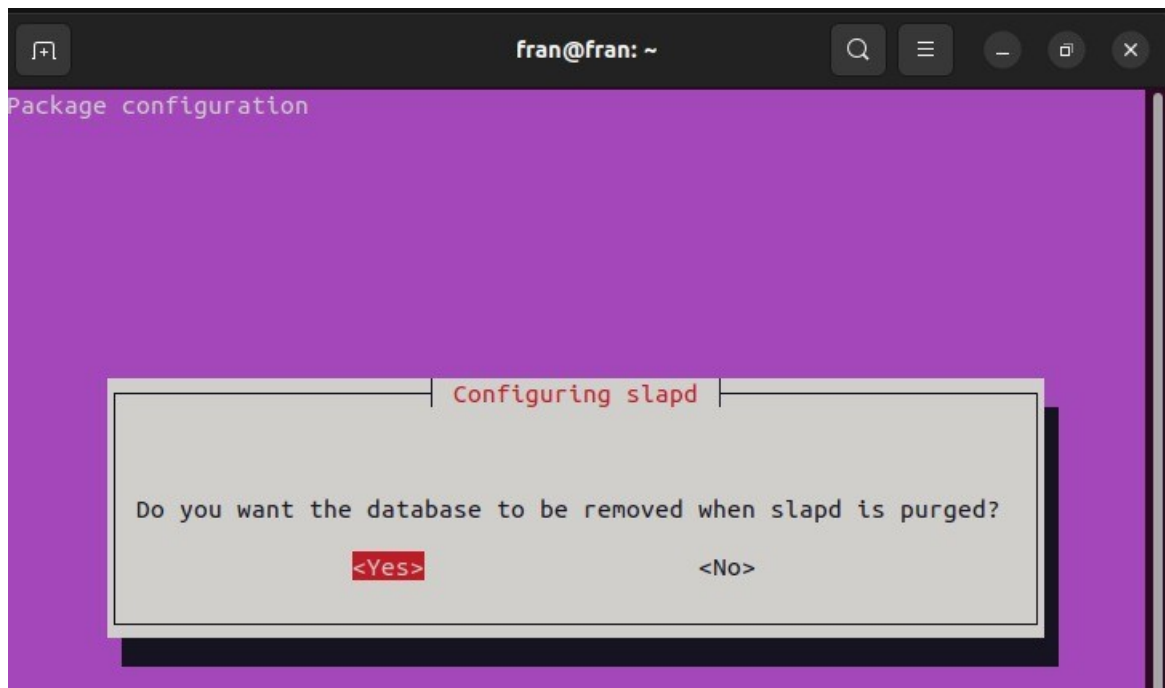
A la configuración se llama así:

```
fran@fran:~$ dpkg-reconfigure slapd
/usr/sbin/dpkg-reconfigure must be run as root
fran@fran:~$ sudo dpkg-reconfigure slapd
```

Nos aparece lo siguiente y configuramos tal y como aparecen en las imágenes







Tras lo cual debe finalizarse la configuración y volver sin errores al prompt inicial:

```
Creating LDAP directory... done.  
fran@fran:~$ sudo dpkg-reconfigure slapd  
Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.5.13+dfsg-0ubuntu0.22.04  
.1... done.  
Moving old database directory to /var/backups:  
- directory unknown... done.  
Creating initial configuration... done.  
Creating LDAP directory... done.
```

El estado del servicio se consulta: debe aparecer activo y sin errores en los mensajes de consola:

```
root@fran:/home/fran# /etc/init.d/slapd status
●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 Mon 2023-03-06 17:31:49 CET; 1min 2s ago
     Docs: man:systemd-sysv-generator(8)
   Process: 95901 ExecStart=/etc/init.d/slapd start (code=exited, status=0/SUC
CESS)
    Tasks: 3 (limit: 2288)
   Memory: 3.3M
      CPU: 22ms
   CGroup: /system.slice/slapd.service
            └─95908 /usr/sbin/slapd -h "ldap:/// ldapi:///" -g openldap -u op...

mar 06 17:31:49 fran systemd[1]: Starting LSB: OpenLDAP standalone server (...)...
mar 06 17:31:49 fran slapd[95901]: * Starting OpenLDAP slapd
mar 06 17:31:49 fran slapd[95907]: @(#) $OpenLDAP: slapd 2.5.13+dfsg-0ubun...2) $
                                Ubuntu Developers <ubuntu-devel...com>
mar 06 17:31:49 fran slapd[95908]: slapd starting
mar 06 17:31:49 fran slapd[95901]: ...done.
mar 06 17:31:49 fran systemd[1]: Started LSB: OpenLDAP standalone server (...ol).
Hint: Some lines were ellipsized, use -l to show in full.
```

Para comprobar que el servidor está iniciado y escuchando peticiones en el puerto se ejecuta el siguiente comando y se observa que está en estado escuchando (tanto para IPv4 como IPv6):

```
fran@fran:~$ ps -ef | grep slapd
openldap  95908      1  0 17:31 ?          00:00:00 /usr/sbin/slapd -h ldap://
ldapi:/// -g openldap -u openldap -F /etc/ldap/slapd.d
fran      96150    47085  0 17:41 pts/0    00:00:00 grep --color=auto slapd
fran@fran:~$ ps -ef | grep slapd | netstat -ltn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::389                   :::*                    LISTEN
tcp6       0      0 :::8080                  :::*                    LISTEN
tcp6       0      0 127.0.0.1:8005          :::*                    LISTEN
tcp6       0      0 :::1:631                 :::*                    LISTEN
```

## Configuración de los ficheros en la carpeta instalada:

Se observan los ficheros y directorios de configuración:

Con el comando `tree /etc/ldap`



```

/etc/ldap
├── ldap.conf
├── sasl2
├── schema
│   ├── collective.ldif
│   ├── collective.schema
│   ├── corba.ldif
│   ├── corba.schema
│   ├── core.ldif
│   ├── core.schema
│   ├── cosine.ldif
│   ├── cosine.schema
│   ├── dsee.ldif
│   ├── dsee.schema
│   ├── duaconf.ldif
│   ├── duaconf.schema
│   ├── dyngroup.ldif
│   ├── dyngroup.schema
│   ├── inetorgperson.ldif
│   ├── inetorgperson.schema
│   ├── java.ldif
│   ├── java.schema
│   ├── misc.ldif
│   ├── misc.schema
│   ├── msuser.ldif
│   ├── msuser.schema
│   ├── namedobject.ldif
│   ├── namedobject.schema
│   ├── nis.ldif
│   ├── nis.schema
│   ├── openldap.ldif
│   ├── openldap.schema
│   ├── pmi.ldif
│   ├── pmi.schema
│   └── README
└── slapd.d
    ├── cn=config [error opening dir]
    └── cn=config.ldif

4 directories, 33 files

```

Is `/etc/ldap/slapd.d` se almacena el DIT de configuración del servidor

```

fran@fran:~$ ls /etc/ldap/slapd.d
'cn=config' 'cn=config.ldif'

```

En árbol:

```

fran@fran:~$ tree /etc/ldap/slapd.d

/etc/ldap/slapd.d
├── cn=config [error opening dir]
└── cn=config.ldif

```

El directorio **/etc/ldap/schema** contiene esquemas en formato LDIF que incluye el servidor:

```
fran@fran:~$ ls /etc/ldap/schema
collective.ldif    dsee.ldif          java.ldif           nis.ldif
collective.schema dsee.schema         java.schema         nis.schema
corba.ldif        duaconf.ldif       misc.ldif           openldap.ldif
corba.schema      duaconf.schema     misc.schema         openldap.schema
core.ldif         dyngroup.ldif      msuser.ldif        pmi.ldif
core.schema       dyngroup.schema    msuser.schema      pmi.schema
cosine.ldif       inetorgperson.ldif namedobject.ldif    README
cosine.schema     inetorgperson.schema namedobject.schema
```

## Herramientas del servidor LDAP

Mostrar la información de la que se dispone con el comando **# slapcat**

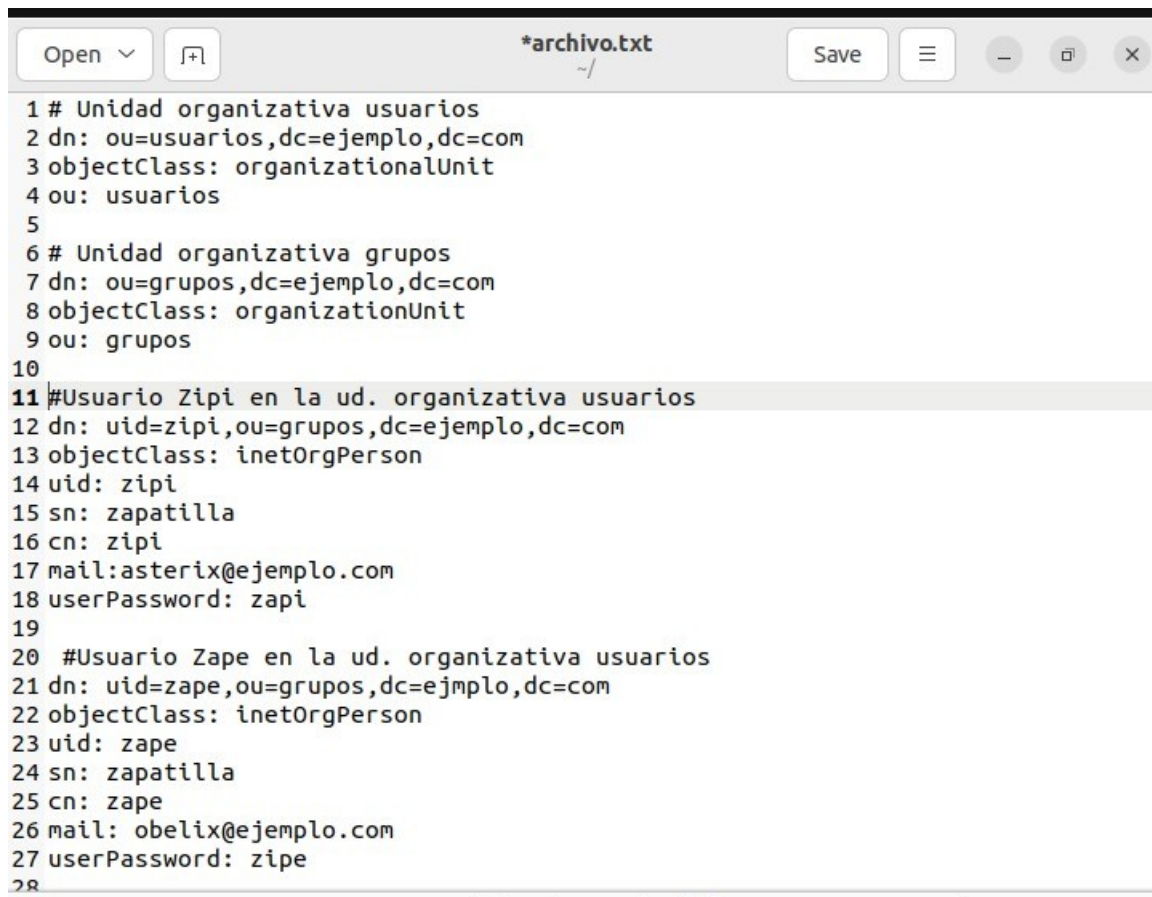
```
fran@fran:~$ sudo slapcat
dn: dc=ejemplo,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: ejemplo
dc: ejemplo
structuralObjectClass: organization
entryUUID: 22f050a4-5088-103d-9d14-734b89400d6e
creatorsName: cn=admin,dc=ejemplo,dc=com
createTimestamp: 20230306163148Z
entryCSN: 20230306163148.629776Z#000000#000#000000
modifiersName: cn=admin,dc=ejemplo,dc=com
modifyTimestamp: 20230306163148Z
```

## Operaciones sobre LDAP

**Comandos para agregar información al servicio de directorio LDAP**, desde el punto de vista del cliente:

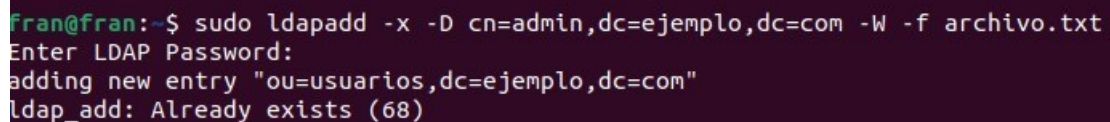
### Añadir entidades

**Idapadd** : añadir entradas como objetos al DIT de nuestro servicio de directorio. Puede hacerse de forma individual una entrada por comando, o varias que se pasan como argumento en un fichero



```
Open  [icon] *archivo.txt  Save  [icon]  [icon]  [icon]
1 # Unidad organizativa usuarios
2 dn: ou=usuarios,dc=ejemplo,dc=com
3 objectClass: organizationalUnit
4 ou: usuarios
5
6 # Unidad organizativa grupos
7 dn: ou=grupos,dc=ejemplo,dc=com
8 objectClass: organizationUnit
9 ou: grupos
10
11 #Usuario Zipi en la ud. organizativa usuarios
12 dn: uid=zipi,ou=grupos,dc=ejemplo,dc=com
13 objectClass: inetOrgPerson
14 uid: zipi
15 sn: zapatilla
16 cn: zipi
17 mail:asterix@ejemplo.com
18 userPassword: zapi
19
20 #Usuario Zape en la ud. organizativa usuarios
21 dn: uid=zape,ou=grupos,dc=ejemplo,dc=com
22 objectClass: inetOrgPerson
23 uid: zape
24 sn: zapatilla
25 cn: zape
26 mail: obelix@ejemplo.com
27 userPassword: zipe
28
```

Con dicho fichero creado, se repite el comando de añadir entidades:

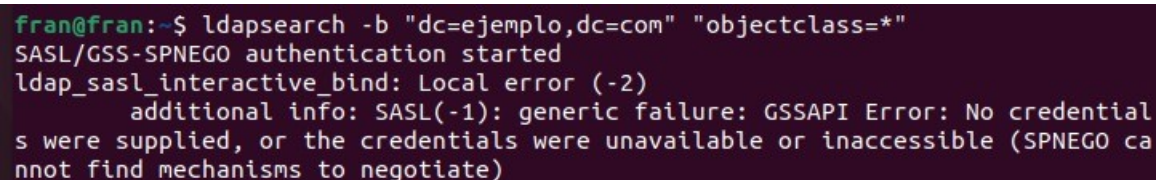


```
fran@fran:~$ sudo ldapadd -x -D cn=admin,dc=ejemplo,dc=com -W -f archivo.txt
Enter LDAP Password:
adding new entry "ou=usuarios,dc=ejemplo,dc=com"
ldap_add: Already exists (68)
```

**Buscar** objetos en el directorio:

**ldapsearch:** para seleccionar los objetos de un directorio a partir de cierta raíz del árbol de directorio.

Ejemplo de sentencia: para buscar todos los objetos dentro del dominio ejemplo.com



```
fran@fran:~$ ldapsearch -b "dc=ejemplo,dc=com" "objectclass=*"
SASL/GSS-SPNEGO authentication started
ldap_sasl_interactive_bind: Local error (-2)
    additional info: SASL(-1): generic failure: GSSAPI Error: No credential
s were supplied, or the credentials were unavailable or inaccessible (SPNEGO ca
nnot find mechanisms to negotiate)
```



Con una variante del comando se obtendría la consulta de todo el DIT:

```
fran@fran:~$ sudo ldapsearch -x -LLL -H ldap://localhost -b "dc=ejemplo, dc=com" "objectClass=*"
[sudo] password for fran:
dn: dc=ejemplo,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: ejemplo
dc: ejemplo

dn: ou=usuarios,dc=ejemplo,dc=com
objectClass: organizationalUnit
ou: usuarios
```

Ejemplo 2): para mostrar todos los atributos de todos los tipos de entidades

```
fran@fran:~$ sudo ldapsearch -x -b "dc=ejemplo, dc=com" "objectClass=*"
# extended LDIF
#
# LDAPv3
# base <dc=ejemplo, dc=com> with scope subtree
# filter: objectClass=*
# requesting: ALL
#
# ejemplo.com
dn: dc=ejemplo,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: ejemplo
dc: ejemplo

# usuarios, ejemplo.com
dn: ou=usuarios,dc=ejemplo,dc=com
objectClass: organizationalUnit
ou: usuarios

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
fran@fran:~$
```

Ejemplo3):

```
fran@fran:~$ ldapsearch -x -b "dc=ejemplo, dc=com" "objectClass=organizationalUnit"
# extended LDIF
#
# LDAPv3
# base <dc=ejemplo, dc=com> with scope subtree
# filter: objectClass=organizationalUnit
# requesting: ALL
#
# usuarios, ejemplo.com
dn: ou=usuarios,dc=ejemplo,dc=com
objectClass: organizationalUnit
ou: usuarios

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
fran@fran:~$
```

Ejemplo 4) :

```
fran@fran:~$ ldapsearch -x -b "dc=ejemplo, dc=com" "objectClass=inetOrgPerson"
# extended LDIF
#
# LDAPv3
# base <dc=ejemplo, dc=com> with scope subtree
# filter: objectClass=inetOrgPerson
# requesting: ALL
#
# search result
search: 2
result: 0 Success

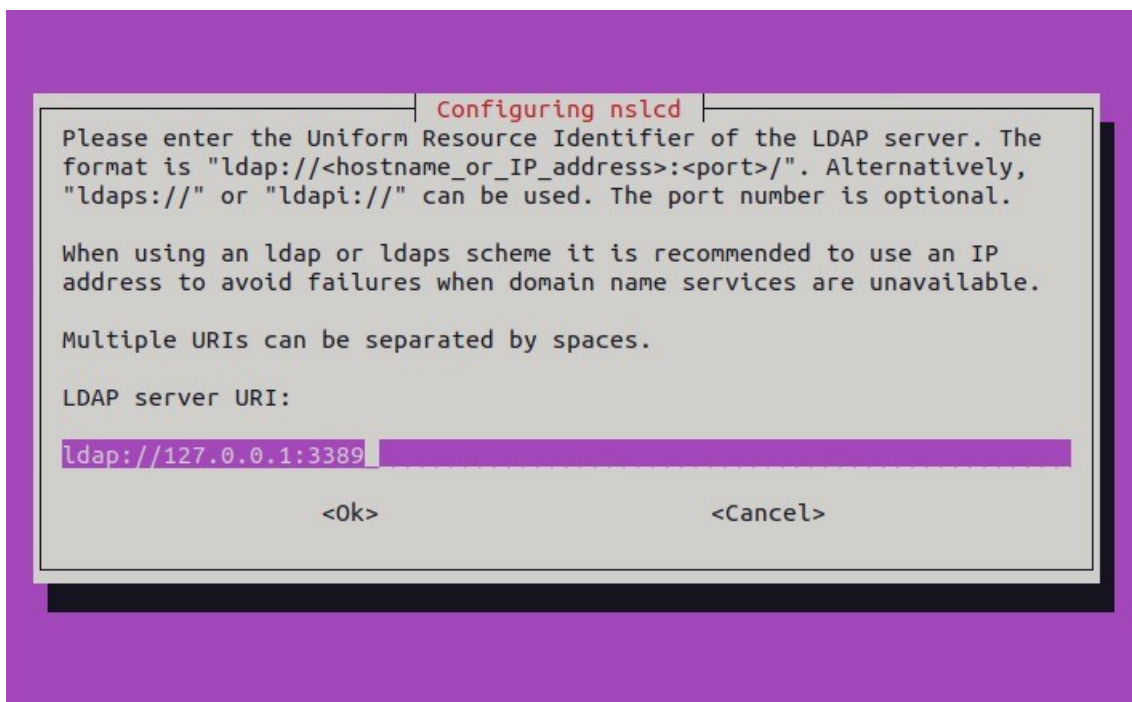
# numResponses: 1
```

Se pueden crear todos los **usuarios que queramos e introducirlos en el directorio LDAP**, para permitir así la validación. Para ello:

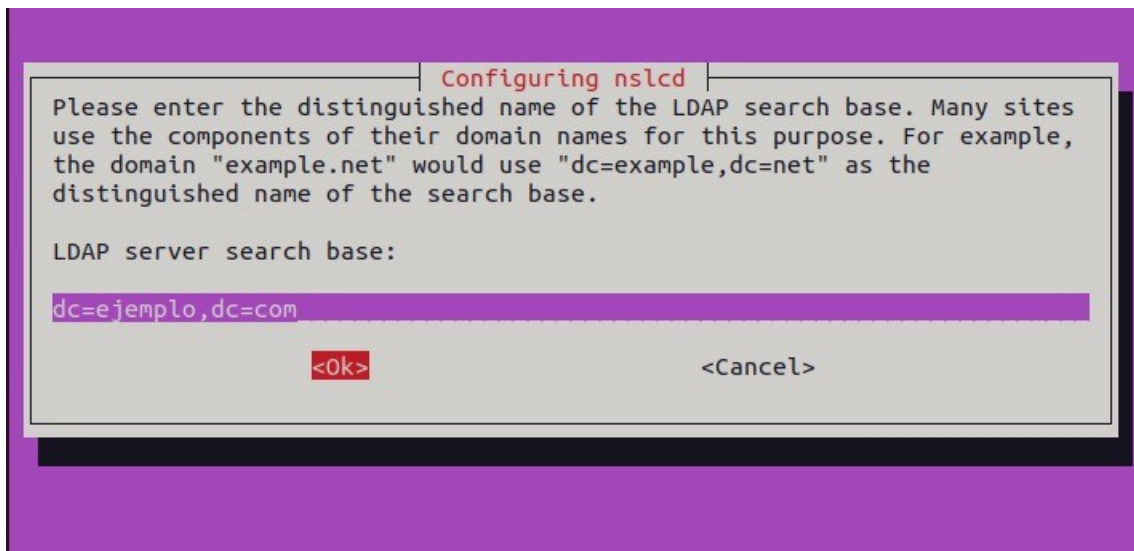
- Instalar y configurar los paquetes libnss-ldapd y libpam-ldapd:

```
fran@fran:~$ sudo apt-get install libpam-ldapd libnss-ldapd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2 liblvm13 linux-headers-5.15.0-43
  linux-headers-5.15.0-43-generic linux-headers-5.15.0-58
  linux-headers-5.15.0-58-generic linux-image-5.15.0-43-generic
  linux-image-5.15.0-58-generic linux-modules-5.15.0-43-generic
  linux-modules-5.15.0-58-generic linux-modules-extra-5.15.0-43-generic
  linux-modules-extra-5.15.0-58-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  nscd nslcd nslcd-utils
Suggested packages:
  kstart
The following NEW packages will be installed:
  libnss-ldapd libpam-ldapd nscd nslcd nslcd-utils
0 upgraded, 5 newly installed, 0 to remove and 8 not upgraded.
Need to get 304 kB of archives.
After this operation, 1.223 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Completar en la pantalla que aparece, el campo de LDAP con la IP del servidor de LDAP (en local 127.0.0.1 y puerto 389).

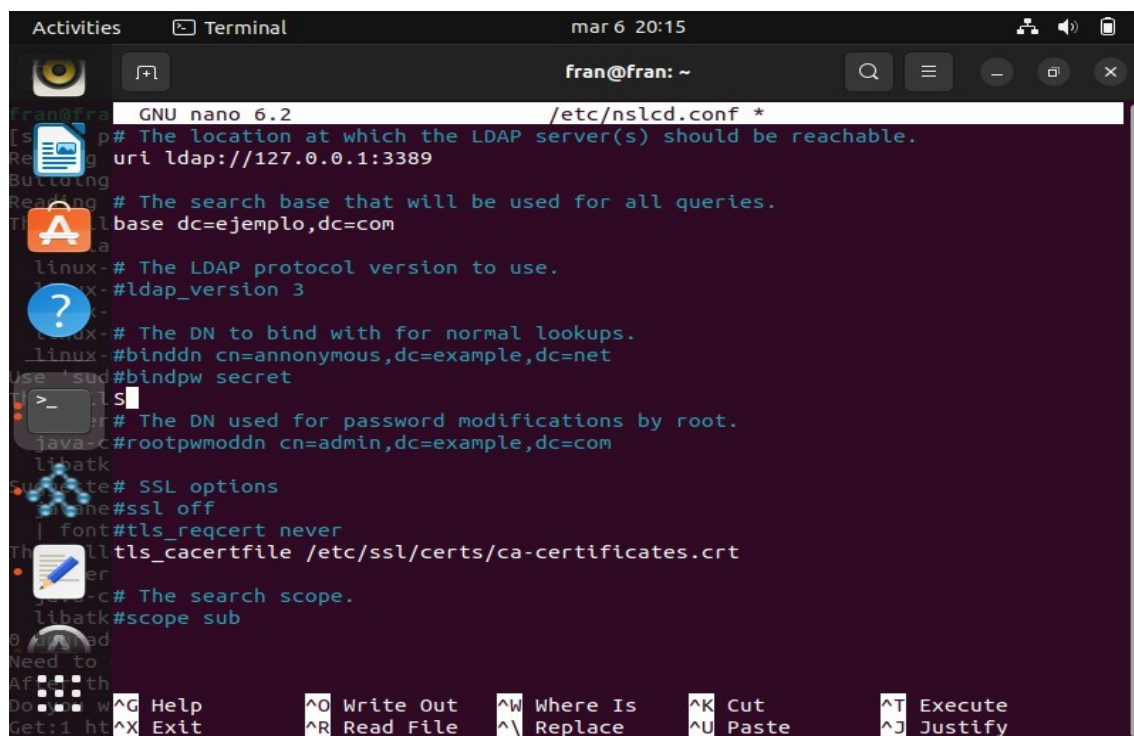


Completar el dominio con el que accedemos al servicio de directorio.

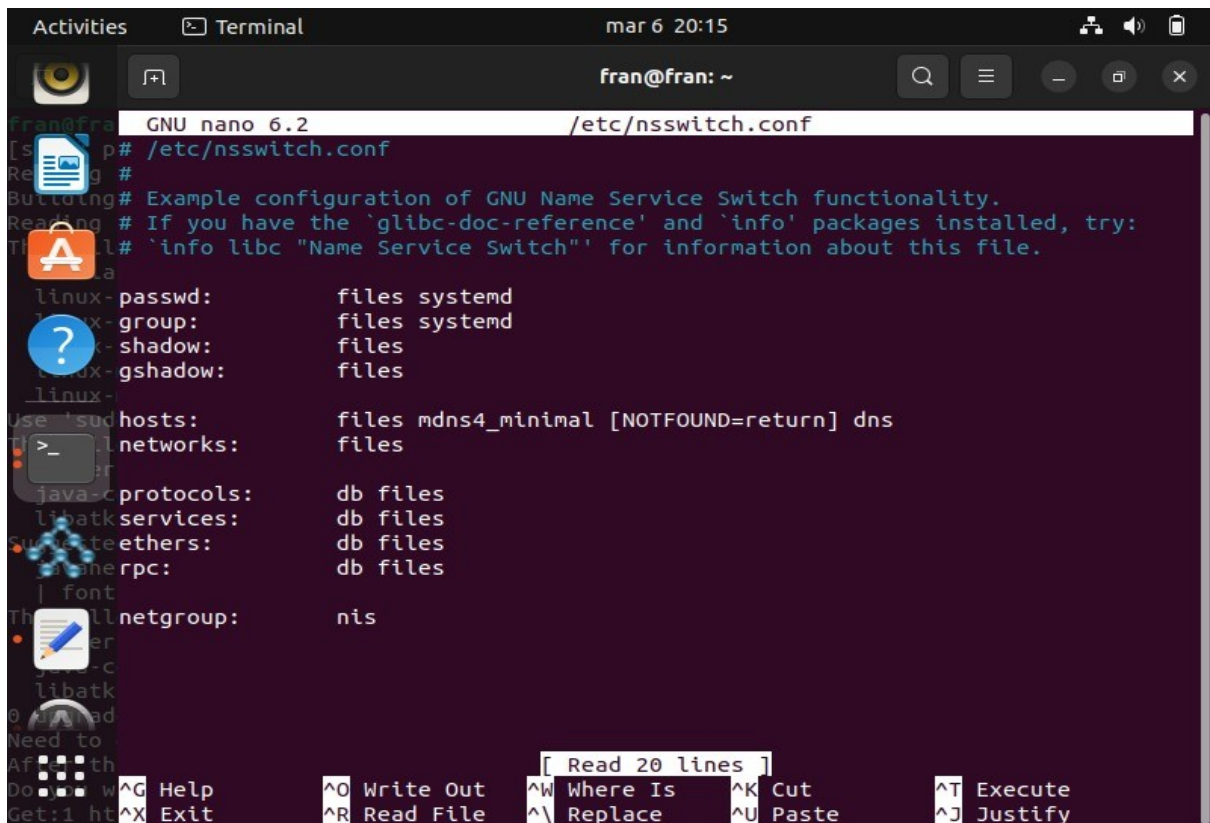


Elegir los servicios que se van a usar para la conexión: **password y group**.

Ficheros de configuración:

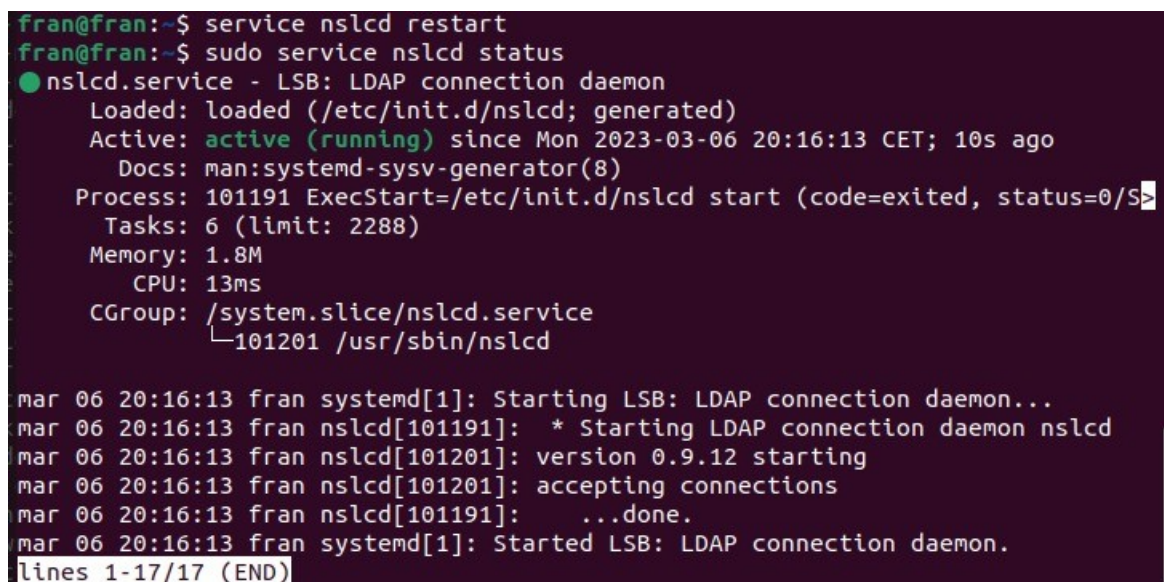






```
fran@fran: ~  
GNU nano 6.2 /etc/nsswitch.conf  
[s]p# /etc/nsswitch.conf  
Re[ ]g#  
Building# Example configuration of GNU Name Service Switch functionality.  
Reading# If you have the 'glibc-doc-reference' and 'info' packages installed, try:  
T[ ]ll# `info libc "Name Service Switch"' for information about this file.  
la  
linux- passwd:      files systemd  
linux- group:       files systemd  
linux- shadow:      files  
linux- gshadow:     files  
linux-  
Use 'su[ ]d hosts:      files mdns4_minimal [NOTFOUND=return] dns  
> _l networks:      files  
java-c protocols:   db files  
libatk services:    db files  
Su[ ]te ethers:     db files  
merpc:              db files  
| font  
Th[ ]ll netgroup:    nis  
er  
-c  
libatk  
0[ ] had  
Need to  
Aff[ ] th  
Do[ ] w  
Get:1 ht  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute  
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Iniciar el servicio nslcd para poner en funcionamiento la validación de LDAP mediante el comando:



```
fran@fran:~$ service nslcd restart  
fran@fran:~$ sudo service nslcd status  
● nslcd.service - LSB: LDAP connection daemon  
   Loaded: loaded (/etc/init.d/nslcd; generated)  
   Active: active (running) since Mon 2023-03-06 20:16:13 CET; 10s ago  
     Docs: man:systemd-sysv-generator(8)  
  Process: 101191 ExecStart=/etc/init.d/nslcd start (code=exited, status=0/S>  
    Tasks: 6 (limit: 2288)  
   Memory: 1.8M  
      CPU: 13ms  
   CGroup: /system.slice/nslcd.service  
           └─101201 /usr/sbin/nslcd  
  
mar 06 20:16:13 fran systemd[1]: Starting LSB: LDAP connection daemon...  
mar 06 20:16:13 fran nslcd[101191]: * Starting LDAP connection daemon nslcd  
mar 06 20:16:13 fran nslcd[101201]: version 0.9.12 starting  
mar 06 20:16:13 fran nslcd[101201]: accepting connections  
mar 06 20:16:13 fran nslcd[101191]: ...done.  
mar 06 20:16:13 fran systemd[1]: Started LSB: LDAP connection daemon.  
lines 1-17/17 (END)
```

Comprobar que se ha configurado correctamente la validación, mediante el comando login, donde debería validarse al usuario de la instalación.



```
fran@fran:~$ sudo login
fran login: fran
Password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-56-generic x86_64)

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

* Introducing Expanded Security Maintenance for Applications.
  Receive updates to over 25,000 software packages with your
  Ubuntu Pro subscription. Free for personal use.

https://ubuntu.com/pro
```

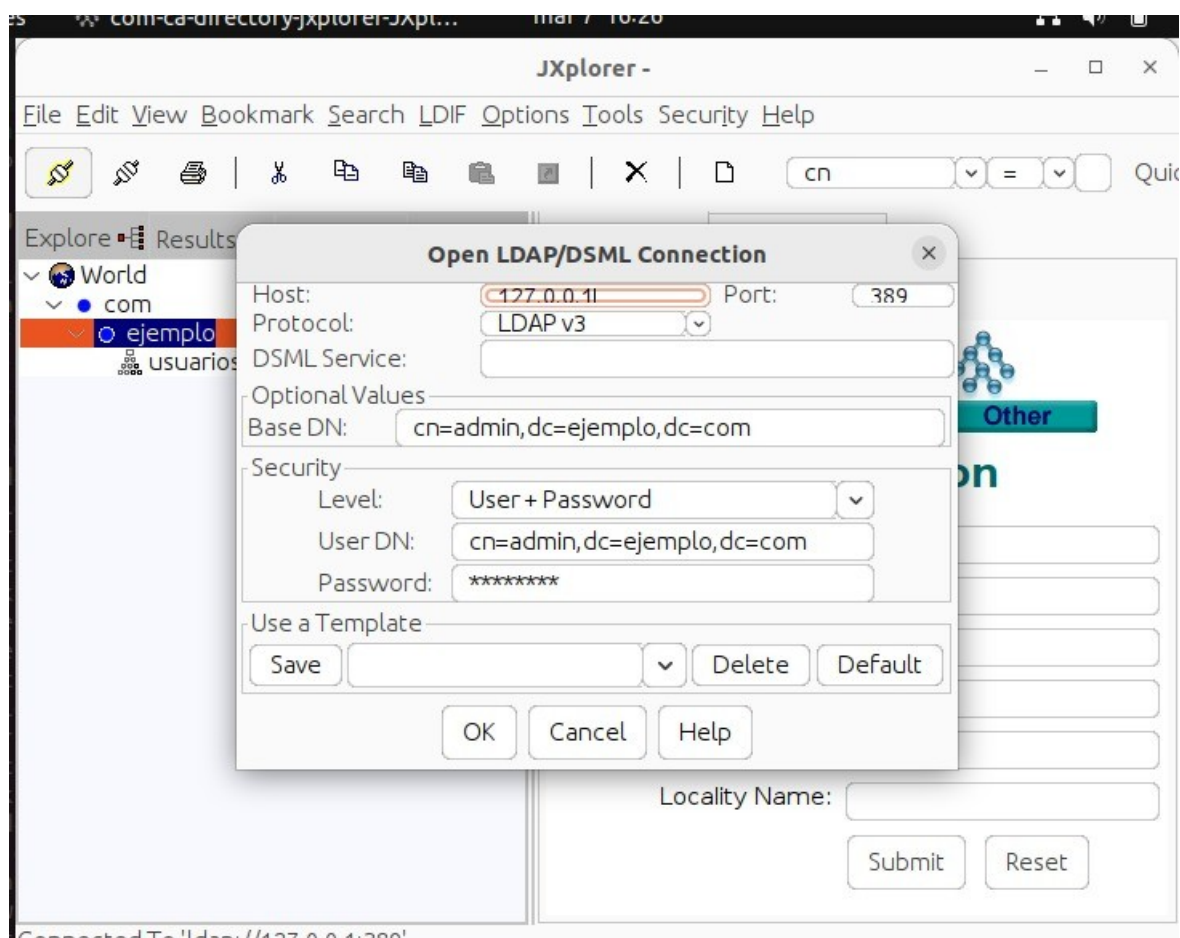
## Ejemplo con JXplorer

Instalar en el sistema operativo host para pruebas locales. Verificar prerequisites de instalación

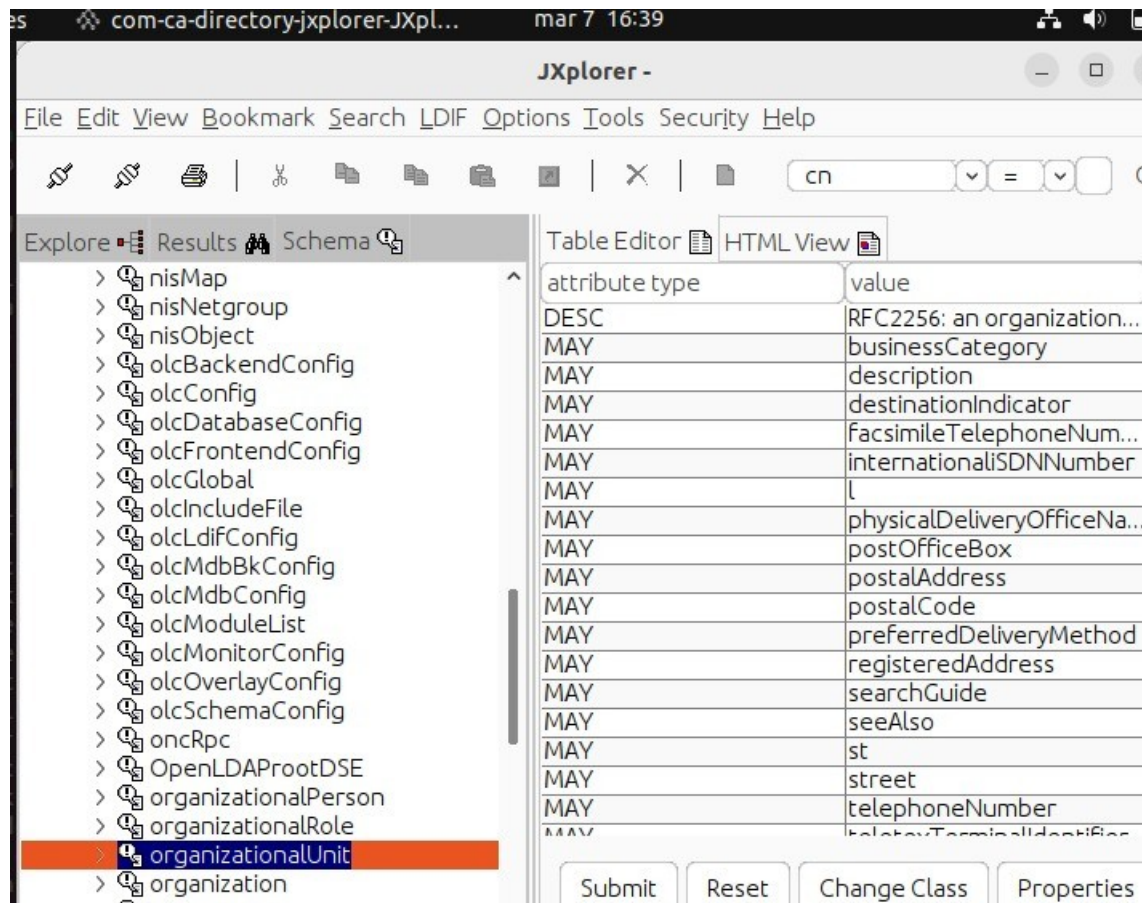
### Uso de JXplorer

Lo primero es conectar al servicio de directorio

Hay que asegurarse de que los parámetros de configuración son válidos, ver:



Pueden añadirse nuevos nodos y modificar los atributos. Para conocer los que hay disponibles (son muchos los tipos de nodos LDIF), se puede consultar en la pestaña de **Schema** y navegar por los que aparecen



Desde la vista del explorador, se podrán añadir las entradas adicionales que se consideren:

