

# U7-OpenLDAP

## Introducció i instal·lació

Tomàs Ferrandis Moscardó

## 1. SERVICI DE DIRECTORI

Un servici de directori és una base de dades jeràrquica i centralitzada que s'utilitza per emmagatzemar i gestionar informació clau d'una organització. Aquesta informació pot incloure:

- Gestió d'usuaris i grups.
- Autenticació d'usuaris.
- Drets d'ús en la xarxa i les màquines.
- Configuracions relacionades amb sistemes i aplicacions.
- Autorització i assignació de permisos sobre el sistema de fitxers.
- Gestió centralitzada de recursos de la xarxa com impressores o equips.

## 2. LDAP

LDAP (Lightweight Directory Access Protocol) és un protocol estàndard i multiplataforma per accedir i gestionar serveis de directori. Entre les característiques principals de LDAP, destaquen:

- La seua independència del sistema operatiu.
- La capacitat de gestionar informació jeràrquica.
- La possibilitat d'autenticació centralitzada en grans xarxes.

Usos principals: - Autenticació d'usuaris. - Cerca i recuperació d'informació en bases de dades jeràrquiques.

**LDAP no està lligat a cap sistema operatiu** específic i és compatible amb diferents implementacions de serveis de directori com OpenLDAP, Active Directory, Novell eDirectory o Oracle Directory Server.

### 3. OpenLDAP

OpenLDAP és una implementació de codi obert del protocol LDAP. Es tracta d'una solució molt utilitzada en **entorns Linux** per implementar serveis de directori lleugers i altament configurables.

En un sistema Linux, OpenLDAP és sovint utilitzat com a nucli per proporcionar autenticació centralitzada i gestionar l'accés a recursos de la xarxa. Tot i això, no inclou funcions integrades com DNS o Kerberos, per la qual cosa sol integrar-se amb altres components per ampliar la funcionalitat.

Característiques destacades d'OpenLDAP:

- És una solució lleugera i modular.
- Suporta personalització avançada dels esquemes de dades.
- És altament compatible amb altres aplicacions i serveis que implementen LDAP.

A més, com hem dit, OpenLDAP pot integrar-se amb altres serveis com Kerberos o Samba per a ampliar les seues funcionalitats.

### 4. OpenLDAP vs ACTIVE DIRECTORY

#### Similituds

1. **Basats en el protocol LDAP:** Tant OpenLDAP com Active Directory utilitzen el protocol LDAP com a base per gestionar i accedir a la informació.
2. **Directorí jeràrquic:** Tots dos structuren la informació en forma d'arbre, amb nodes com dominis, unitats organitzatives (OUs), usuaris i grups.
3. **Autenticació centralitzada:** Ambdues solucions permeten autenticar usuaris i gestionar recursos de manera centralitzada en una xarxa.

4. **Multiplataforma:** Encara que Active Directory està més orientat a Windows, amb configuracions addicionals també pot treballar amb clients Linux, mentre que OpenLDAP és compatible amb diverses plataformes.

## Diferències

### 1. Funcionalitats integrades:

- Active Directory és un servei complet que inclou LDAP, Kerberos i DNS integrats, a més de funcions avançades com Group Policies (GPOs).
- OpenLDAP és una implementació lleugera del protocol LDAP que requereix integracions externes per proporcionar funcionalitats similars.

### 2. Entorn:

- Active Directory està optimitzat per a xarxes Windows.
- OpenLDAP és més flexible i està dissenyat principalment per entorns Linux/Unix.

### 3. Gestió:

- Active Directory ofereix eines gràfiques com l'Active Directory Users and Computers (ADUC) que simplifiquen la gestió però també cmdLets (PowerShell)
- OpenLDAP és configurat principalment a través de fitxers de configuració i eines de línia d'ordres però també té entorns gràfics com JXplorer.

## Punts de connexió

1. **Integració en entorns híbrids:** OpenLDAP es pot utilitzar com a complement o com a directori secundari en xarxes on Active Directory és el directori principal.
2. **Autenticació conjunta:** Mitjançant connectors com **Samba** (que estudiarem al curs) o **SSSD**, els sistemes Linux que utilitzen OpenLDAP poden autenticar-se en dominis d'Active Directory.

3. **Sincronització:** Es poden configurar sincronitzacions bidireccionals entre OpenLDAP i Active Directory per mantenir la coherència de dades entre els dos sistemes.

## Conclusions

OpenLDAP i Active Directory tenen objectius similars en la gestió centralitzada d'usuaris i recursos, però cada solució està optimitzada per a entorns diferents:

- **OpenLDAP:** És ideal per a entorns Linux que necessiten flexibilitat i personalització, especialment quan es prefereix una arquitectura modular amb components externs com Kerberos i DNS.
- **Active Directory:** És la solució preferida per a xarxes Windows gràcies a les seues funcionalitats integrades i eines d'administració simplifiades.

La integració entre ambdues eines permet aprofitar el millor de cada una en xarxes híbrides, oferint una gestió centralitzada i eficient en entorns complexos.

## 2 ESTRUCTURA DE LA BD/DIRECTORI LDAP

### 2.1 Entrades, objectes i atributs

La base de dades LDAP té una estructura jeràrquica. Bàsicament totes les dades s'emmagatzemen en alguna part del directori LDAP, i a similitud dels directoris de fitxers, aquest directori s'organitza en arbre.

El model d'informació de LDAP està basat en entrades. Cada **entrada és un objecte del directori** i conté una col·lecció d'atributs, alguns dels quals son definatoris o identificadors. El DN o Distinguished Name, per exemple és únic i global (identifica a tot el domini de forma única l'objecte).

Fent un símil amb la taula d'una base de dades relacional, **una entrada seria com un registre (fila de la taula) i un atribut seria com un camp (la columna de la taula).**

A partir d'un exemple ho vorem més clar.

## 2.2 Exemple.

L'alumnat de 2 SMXB, després de la visita al Programa Lanzadera ha decidit muntar una empresa. Al domini li han posat de nom *smx2b* amb l'extensió *.com*.

Aquí tens una taula amb els atributs i exemples corresponents:

Atribut	Definició	Exemple
<b>RDN</b>	Nom relatiu dins d'una entrada del directori LDAP.	<code>cn=comercials uid=Arantxa</code>
<b>DN</b>	Camí complet i únic que identifica una entrada al directori.	<code>cn=comercials,ou=DelegacioValencia,dc=smx2b,uid=Arantxa,ou=DelegacioValencia,dc=smx2b</code>
<b>cn</b>	Nom comú que identifica un grup o una persona.	<code>cn=comercials cn=Arantxa</code>
<b>uid</b>	Identificador únic d'un usuari.	<code>uid=Arantxa</code>
<b>gidNumber</b>	Identificador numèric d'un grup al qual pertany una entrada (especialment en sistemes UNIX).	<code>gidNumber: 10001</code>
<b>objectClass</b>	Classes que defineixen el tipus d'entrada i els atributs que pot tenir.	<code>objectClass: posixGroup, objectClass: inetOrgPerson, objectClass: top</code>
<b>homeDirectory</b>	Camí del directori personal d'un usuari (en sistemes UNIX).	<code>/home/smx2b/arantxa</code>

## 2.3 Atributs (RDN, DN, CN...)

Totes les entrades emmagatzemades en un directori LDAP tenen un únic “**Distinguished Name,**” o **DN**.

El DN per a cada entrada està compost de dos parts:

- el Nom Relatiu Distingit (**RDN** per les seves sigles en anglès, Relative Distinguished Name)
- la localització dins del directori LDAP on el registre resideix.

El RDN és la porció de la teva DN que no està relacionada amb l'estructura de l'arbre de directori.

La majoria dels objectes que emmagatzemes en un directori LDAP tindrà un nom, i el nom és emmagatzemat freqüentment en l'atribut `cn` (Common Name). Ja que pràcticament tot té un nom, la majoria dels objectes que emmagatzemarà LDAP utilitzen el seu valor `cn` com a base per a la seva RDN.

Exemple:

```
dn: cn=comercials,ou=DelegacioValencia,dc=smx2b,dc=com
cn: comercials
gidNumber: 10001
objectClass: posixGroup
objectClass: top
memberUid: 1001
```

- El DN base del meu directori `ou = DelegacioNord`, `dc = smx2b`, `dc = com`
- El RDN d'un registre d'un grup `cn=comercials`

Per als comptes d'usuari, típicament veuràs un DN basat en el `cn` o al `uid` (ID de l'usuari).

Per exemple, el DN del comercial de login: `arantxa` pot semblar-se a:

```
dn: uid=Arantxa,ou=DelegacioValencia,dc=smx2b,dc=com
cn: Arantxa
gidNumber: 10001
homeDirectory: /home/smx2b/arantxa
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: posixAccount
objectClass: person
objectClass: top
```

LDAP utilitzen `uid` per a indicar “ID de l'usuari”, no s'ha de confondre amb el número `uid` de UNIX. La majoria de les empreses intenten donar a cadascun un nom de login, així aquesta aproximació fa que tinga sentit emmagatzemar informació sobre els empleats.

Pero podem usar el cn també.

Aquí veiem l'entrada Nom Comú o CN (per les seves sigles en anglès, common name) utilitzada. En el cas d'un registre LDAP per a una persona, pensa en el nom comú com els seu nom complet. Un pot veure fàcilment l'efecte col·lateral d'aquesta forma: si el nom canvia, el registre LDAP ha de "moure" d'un DN a un altre.

## 3 INSTAL·LACIÓ en el SERVIDOR

### 3.1 Preparar el servidor Ubuntu

Nom de la màquina virtual i de l'equip: ubuntu1server1 Usuari principal: admin  
Contrasenya usuari principal: Gandia2425

Dos targetes de xarxa (en Virtualització) NAT -> DHCP Xarxa Interna, interfície inet  
-> Manual

(al món real la NAT correspondria a una NIC connectada al router amb eixida a internet i la xarxa interna al switch de la LAN)

#### 3.1.1 Configurar la targeta de xarxa

Editem la configuració de la segona targeta de xarxa, la de xarxa interna, i li fiquem una IP fixa i la màscara. En el meu cas utilitzaré l'IP 192.168.1.1. Busque el fitxer i l'edite amb nano

```
sudo nano /etc/netplan/50-cloud-init.yaml
sudo netplan apply
ip a
```

```
tomas@ubuntuserver1: ~  
tomas@ubuntuserver1:~$ ls /etc/netplan/  
50-cloud-init-BACKUP.yaml 50-cloud-init.yaml  
tomas@ubuntuserver1:~$ sudo cat /etc/netplan/50-cloud-init.yaml  
# This file is generated from information provided by the datasource. Changes  
# to it will not persist across an instance reboot. To disable cloud-init's  
# network configuration capabilities, write a file  
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:  
# network: {config: disabled}  
network:  
  version: 2  
  ethernets:  
    enp0s3:  
      dhcp4: false  
      addresses:  
        - 192.168.1.1/24  
      nameservers:  
        addresses:  
          - 8.8.8.8  
          - 1.1.1.1  
    enp0s8:  
      dhcp4: true # DHCP i NAT ( pero tindre internet)
```

```
tomas@ubuntuserver1:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP  
group default qlen 1000  
    link/ether 08:00:27:72:14:ad brd ff:ff:ff:ff:ff:ff  
    inet 192.168.1.1/24 brd 192.168.1.255 scope global enp0s3  
        valid_lft forever preferred_lft forever  
    inet6 fe80::a00:27ff:fe72:14ad/64 scope link  
        valid_lft forever preferred_lft forever  
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP  
group default qlen 1000  
    link/ether 08:00:27:7e:0d:b8 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.3.15/24 metric 100 brd 10.0.3.255 scope global dynamic enp0s8  
        valid_lft 85212sec preferred_lft 85212sec  
    inet6 fe80::a00:27ff:fe7e:db8/64 scope link  
        valid_lft forever preferred_lft forever
```

### 3.1.2 Nom de màquina

- Consultem el nom del servidor

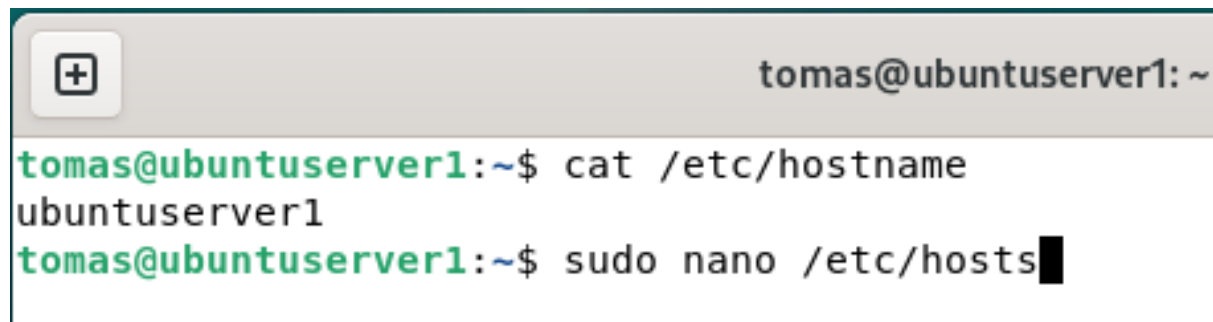


```
sudo cat /etc/hostname
```

(o echo \$HOSTNAME)

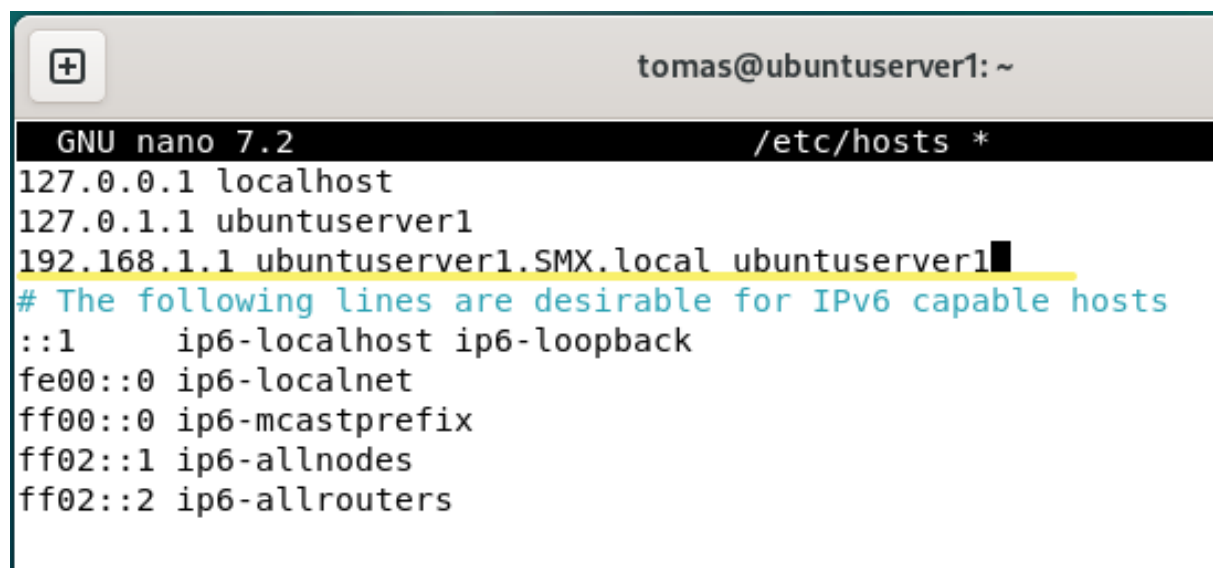
- Modifiquem el fitxer de noms

```
sudo nano /etc/hosts
```



A terminal window titled 'tomas@ubuntuserver1: ~'. The user runs 'cat /etc/hostname' and the output is 'ubuntuserver1'. Then, the user runs 'sudo nano /etc/hosts' and the terminal shows the start of the nano editor.

Afegim la tercera línia:



A terminal window titled 'tomas@ubuntuserver1: ~' showing the nano editor editing '/etc/hosts'. The file content is: '127.0.0.1 localhost', '127.0.1.1 ubuntuserver1', and '192.168.1.1 ubuntuserver1.SMX.local ubuntuserver1'. The third line is highlighted in yellow. Below it is a comment about IPv6 and several IPv6 addresses with their corresponding hostnames.

Cal reiniciar el servidor

```
reboot
```

## 3.2 Instal·lar el OpenLDAP

- Actualitzem repositori i software prèviament

```
sudo apt update && sudo apt upgrade
```

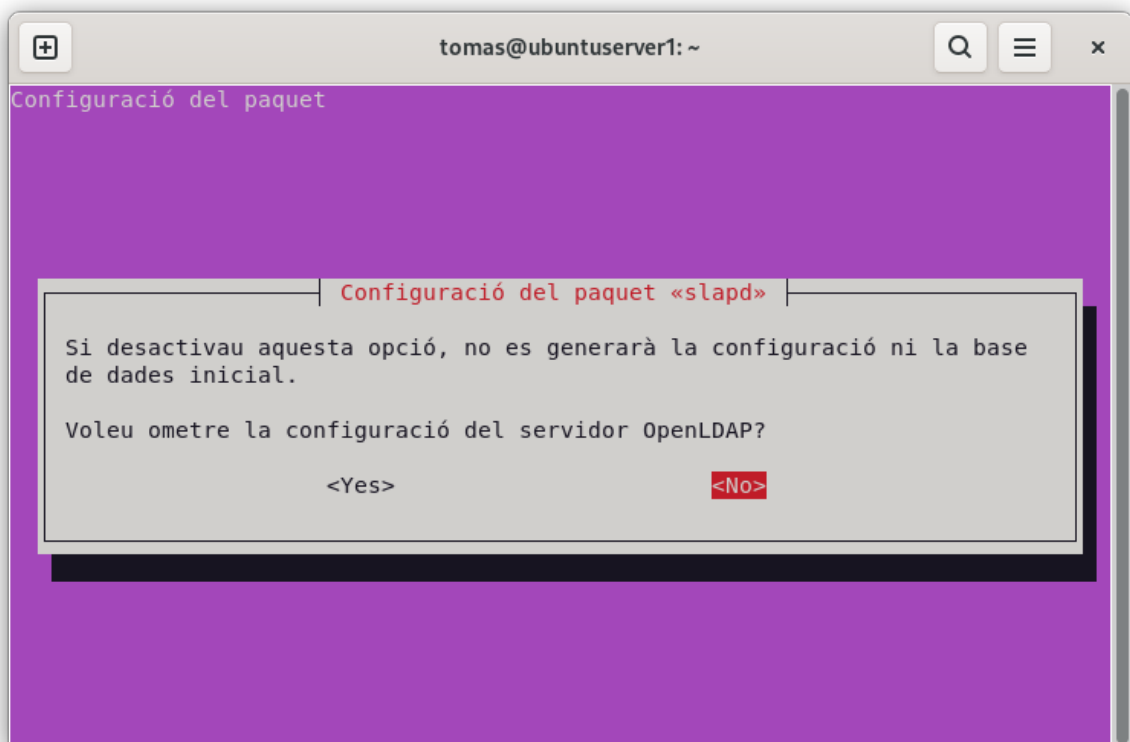
- Instal·lem

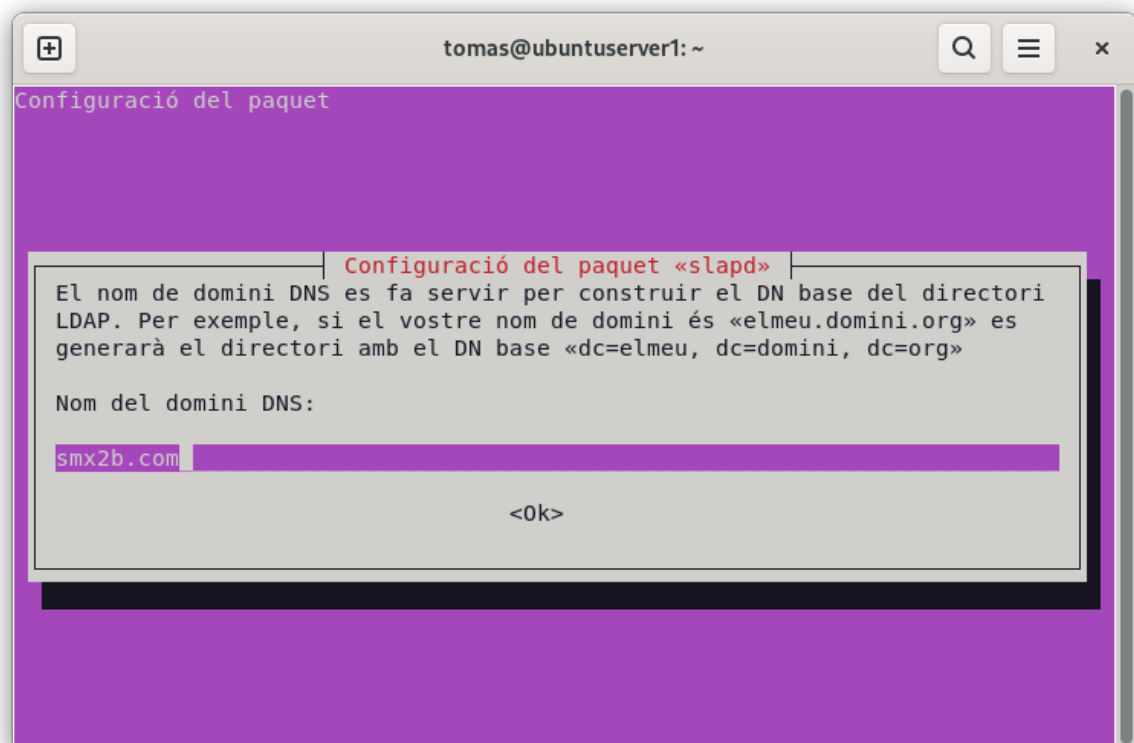
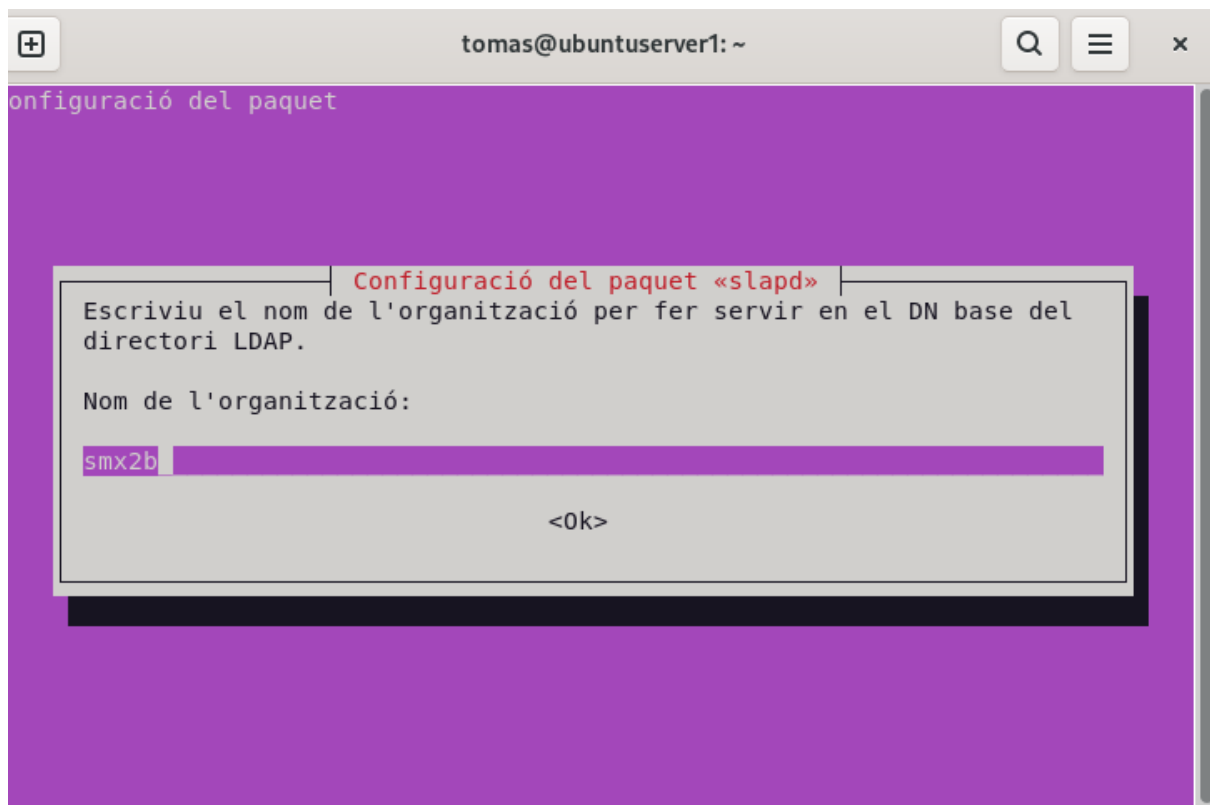
```
sudo apt install slapd ldap-utils -y
```

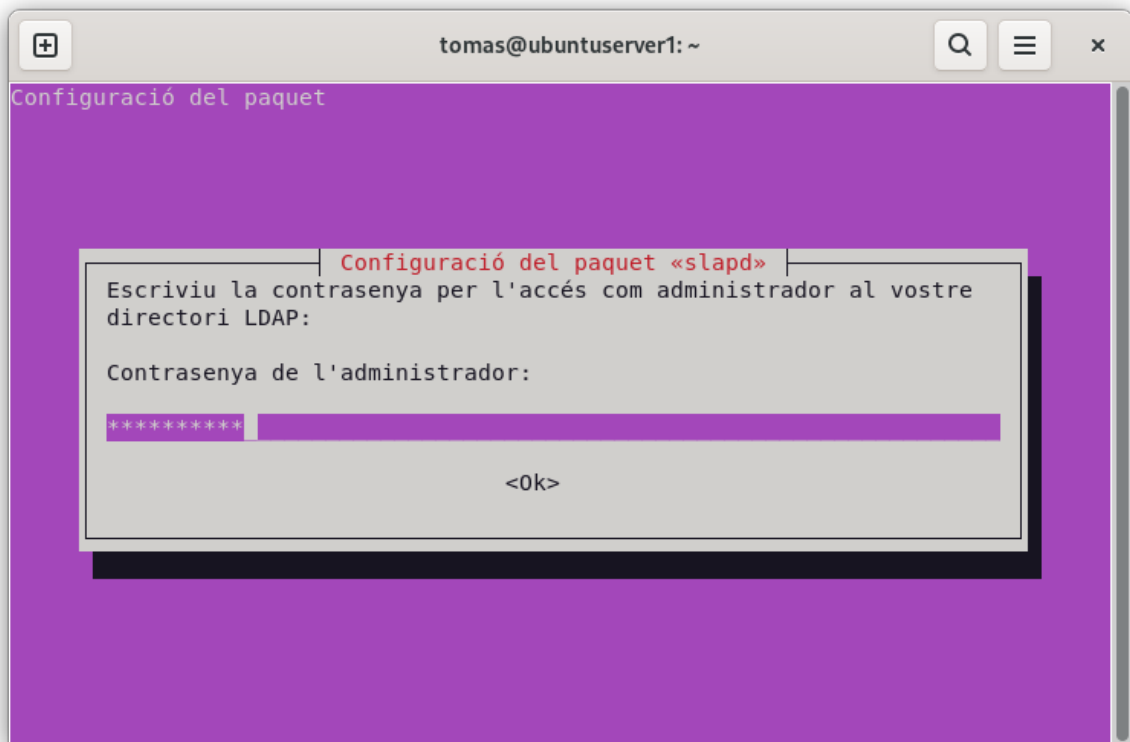
Si no s'inicia l'assistent, executa...

```
sudo dpkg-reconfigure slapd
```

- Ens pregunta si volem ometre l'assistent: Seleccionem: no
- Ens pregunta la base del nostre **domini DNS**: En el meu cas: **smx2b.com**
- Ens pregunta el nom complet de l'**organització**: En el meu cas: **smx2b**
- Ens pregunta la paraula de pas. És la que usarem amb *admin* més avant per connectar-nos.
- A les següents preguntes podeu deixar l'opció per defecte.

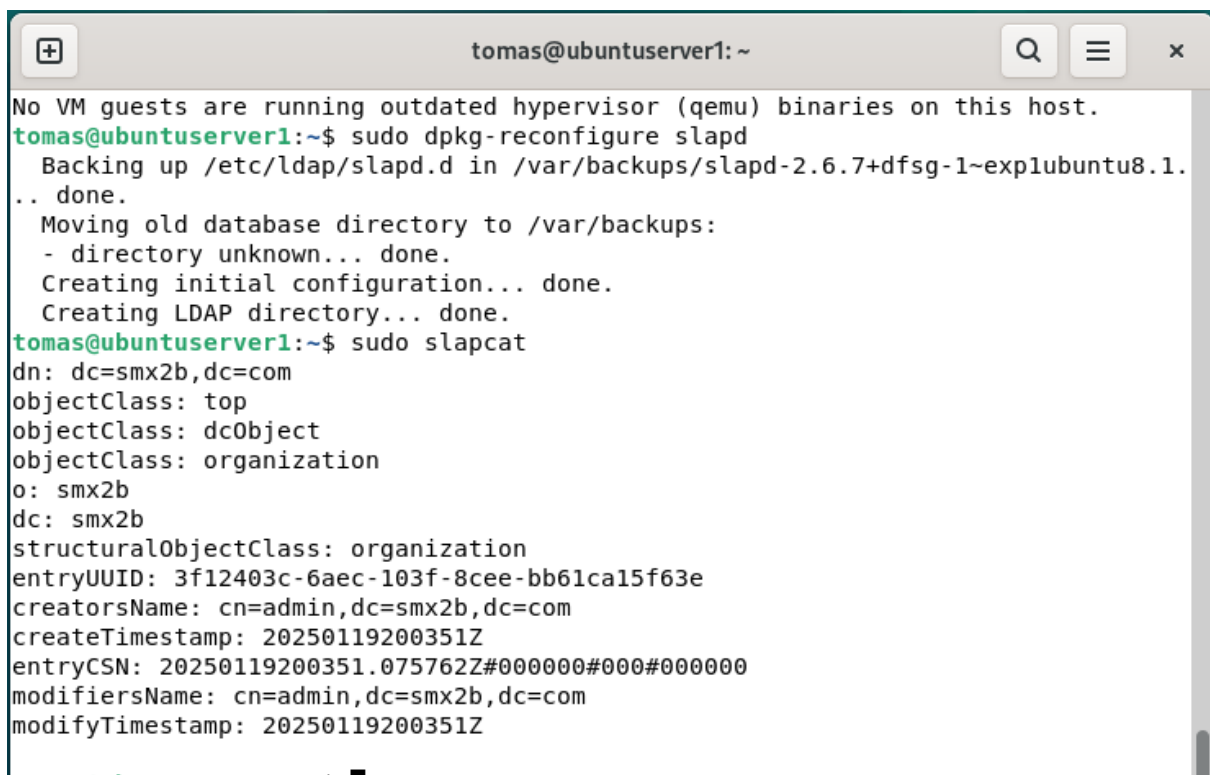






Comprovar el resultat

```
sudo slapcat
```



Reiniciar el servici

```
sudo systemctl restart slapd
```

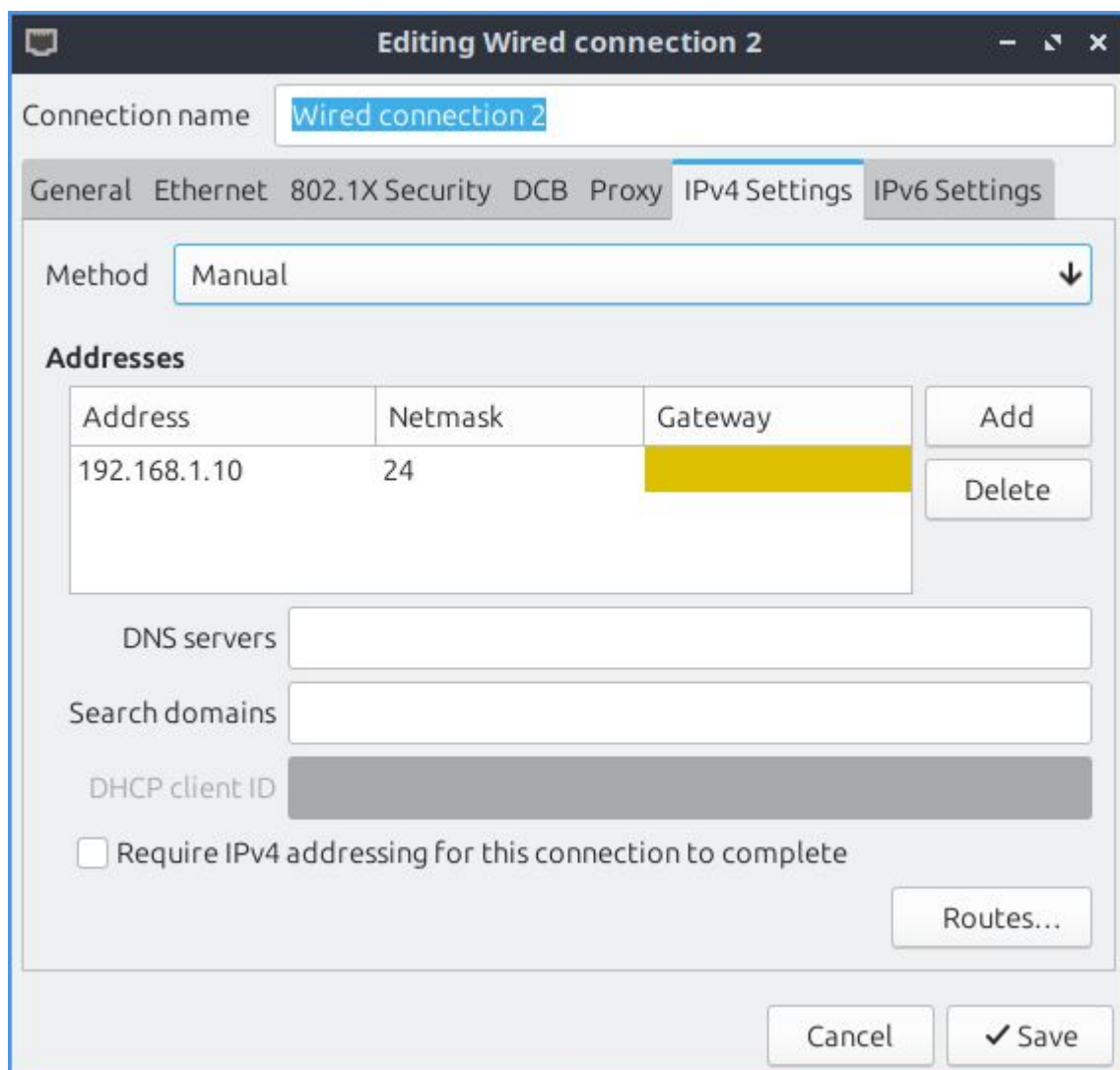
Amb *status* podem comprovar si està “running”.

## 4. INSTAL·LACIÓ en el CLIENT UBUNTU

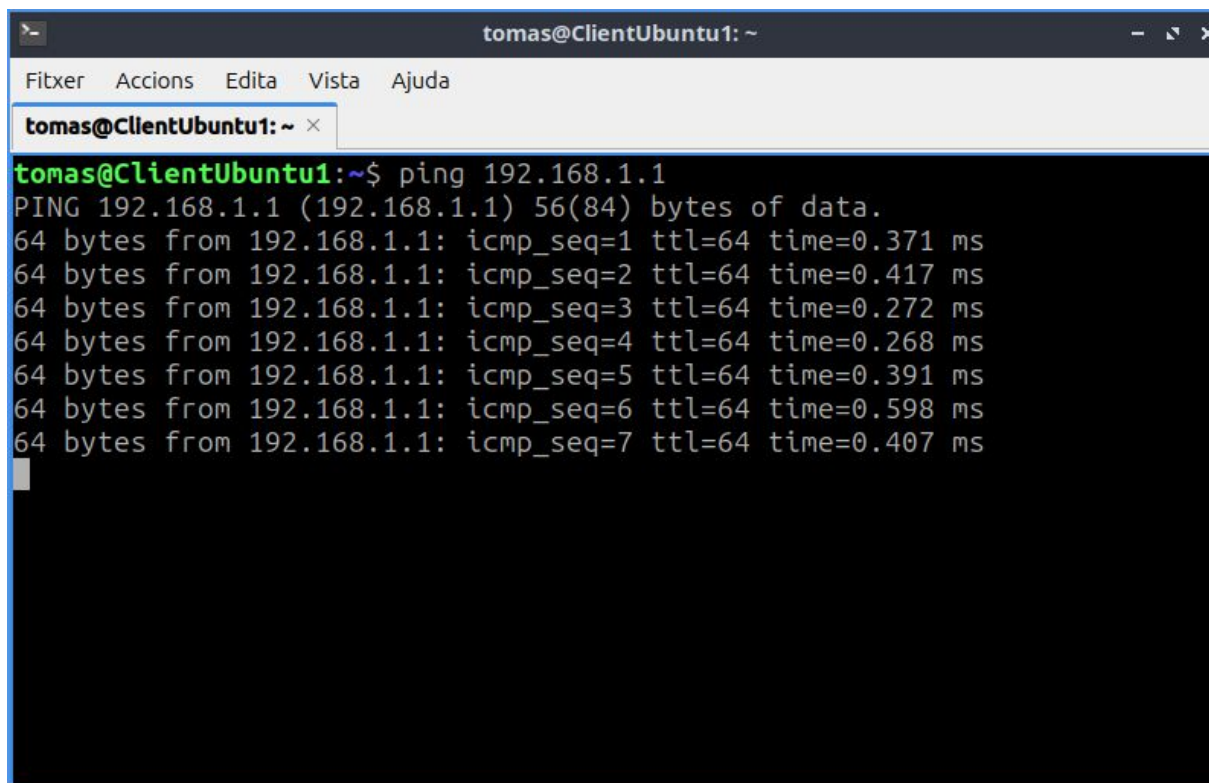
### 4.1 Configuració de la NIC

Xarxa interna -> Manual

Podem optar per modificar el netplan com hem fet en el servidor o gràficament. Alguns Entorns d'Escriptori com el LXQt de Lubuntu ho failiten prou:



Comprovem la connectivitat entre Servidor i Client



The screenshot shows a terminal window titled 'tomas@ClientUbuntu1: ~'. The window has a menu bar with 'Fitxer', 'Accions', 'Edita', 'Vista', and 'Ajuda'. Below the menu bar is a tab labeled 'tomas@ClientUbuntu1: ~'. The terminal content shows a user prompt 'tomas@ClientUbuntu1:~\$' followed by the command 'ping 192.168.1.1'. The output of the command is as follows:

```
tomas@ClientUbuntu1:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.371 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.417 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.272 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.268 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.391 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=0.598 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=0.407 ms
```

## 4.2 Configurar la resolució de noms.

Associació del nom del servidor a la seua IP en el `/etc/hosts`

```
sudo nano /etc/hosts
```

```
tomas@ClientUbuntu1: ~  
Fitxer Accions Edita Vista Ajuda  
tomas@ClientUbuntu1: ~ x  
GNU nano 7.2 /etc/hosts  
# Standard host addresses  
127.0.0.1 localhost  
127.0.1.1 ClientUbuntu1  
192.168.1.1 ubuntuserver1  
::1 localhost ip6-localhost ip6-loopback  
ff02::1 ip6-allnodes  
ff02::2 ip6-allrouters  
# This host address  
127.0.1.1 ClientUbuntu1  
[ Read 9 lines ]  
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify
```

Comprovem que funciona la resolució de noms

```
tomas@ClientUbuntu1: ~  
Fitxer Accions Edita Vista Ajuda  
tomas@ClientUbuntu1: ~ x  
tomas@ClientUbuntu1:~$ ping ubuntuserver1  
PING ubuntuserver1 (192.168.1.1) 56(84) bytes of data.  
64 bytes from ubuntuserver1 (192.168.1.1): icmp_seq=1 ttl=64 time=0.38  
1 ms  
64 bytes from ubuntuserver1 (192.168.1.1): icmp_seq=2 ttl=64 time=0.40  
9 ms  
64 bytes from ubuntuserver1 (192.168.1.1): icmp_seq=3 ttl=64 time=0.41  
5 ms  
64 bytes from ubuntuserver1 (192.168.1.1): icmp_seq=4 ttl=64 time=0.40  
9 ms  
64 bytes from ubuntuserver1 (192.168.1.1): icmp_seq=5 ttl=64 time=0.40  
8 ms  
64 bytes from ubuntuserver1 (192.168.1.1): icmp_seq=6 ttl=64 time=0.56  
4 ms  
■
```

## 5 JXPLOER

Existeixen varies aplicacions gràfiques per a facilitar la gestió d'LDAP: Jxplorer, phpLDAPadmin i Apache Directory Studio.

Anem a provar el JXPLOER instal·lada en el client. Pot instal·lar-se en el servidor però la majoria de servidors Linux no tindran entorn gràfic.

### 5.1 Instal·lació del JXplorer en el client

Instal·lem requisits previs

```
sudo apt install openjdk-11-jdk
```

Ara ja si podem instal·lar el programa Jxplorer

```
sudo apt install jxplorer
```

Un vegada l'engeguem des de l'icona, hem de **connectar amb el servidor**.

Important: El client executarà jxplorer, però haurà de connectar amb el servidor ldap.

- Si estiguérem al servidor indicariem *127.0.0.1 o localhost*. Al nostre cas (instal·lació en el client) caldrà indicar la IP del servidor.
- Hem de triar l'opció de **Usuari + Password** que és la que hem configurat en instal·lar el servici i...
- indicar el password que també hem introduït en la configuració

## 6 Els objectes principals

Anem a crear i modificar Unitats Organitzatives, grups d'usuaris i usuaris del domini. I amb la creació des del *jXplorer* podrem introduir uns conceptes bàsics de teoria sobre el LDAP perquè ens cladrà conèixer les **propietats mínimes** fan falta en cada objecte.



## 6.1 Propietats: classes i atributs

Les propietats que veiem quan donem d'alta una Unitat Organitzativa, un usuari o un grup poden ser:

- **Classes:** Esquemes que defineixen què pot o ha de tenir un objecte.
- **Atributs:** Dades concretes d'un objecte definides per les classes.

Característica	Classes (objectClass)	Atributs
<b>Funció</b>	Defineixen el tipus d'objecte i els seus atributs	Contenen dades específiques de l'objecte
<b>Tipus</b>	Estructural, auxiliar o abstracte	Obligatori ( <b>must</b> ) o opcional ( <b>may</b> )
<b>Exemple</b>	<code>inetOrgPerson</code> , <code>posixAccount</code> , <code>top</code>	<code>cn</code> , <code>uid</code> , <code>mail</code> , <code>gidNumber</code> , <code>sn</code>
<b>Obligatorietat</b>	Cada entrada LDAP ha de tenir almenys una classe	Només els atributs marcats com a <b>must</b> són obligatoris
<b>Herència</b>	Pot heretar atributs d'altres classes	No hereten, són definits per les classes

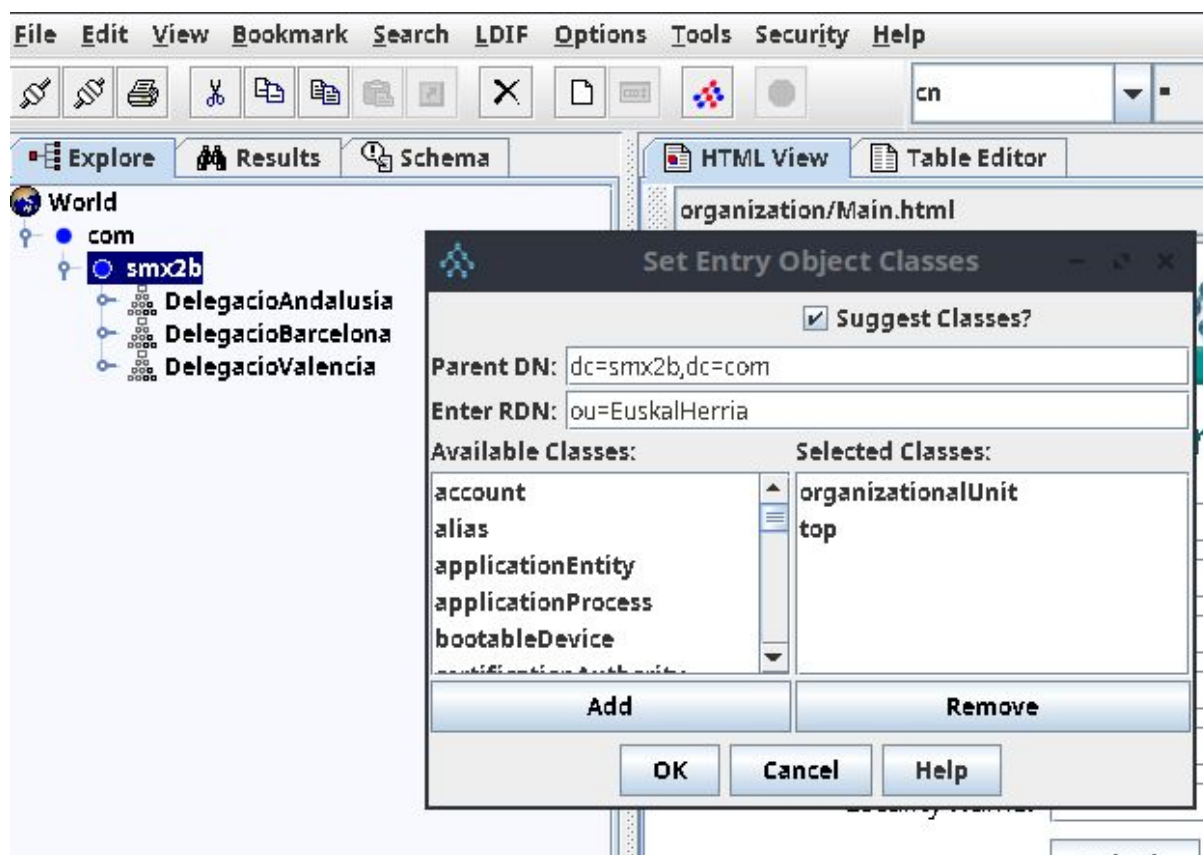
## 6.2 Principals objectes

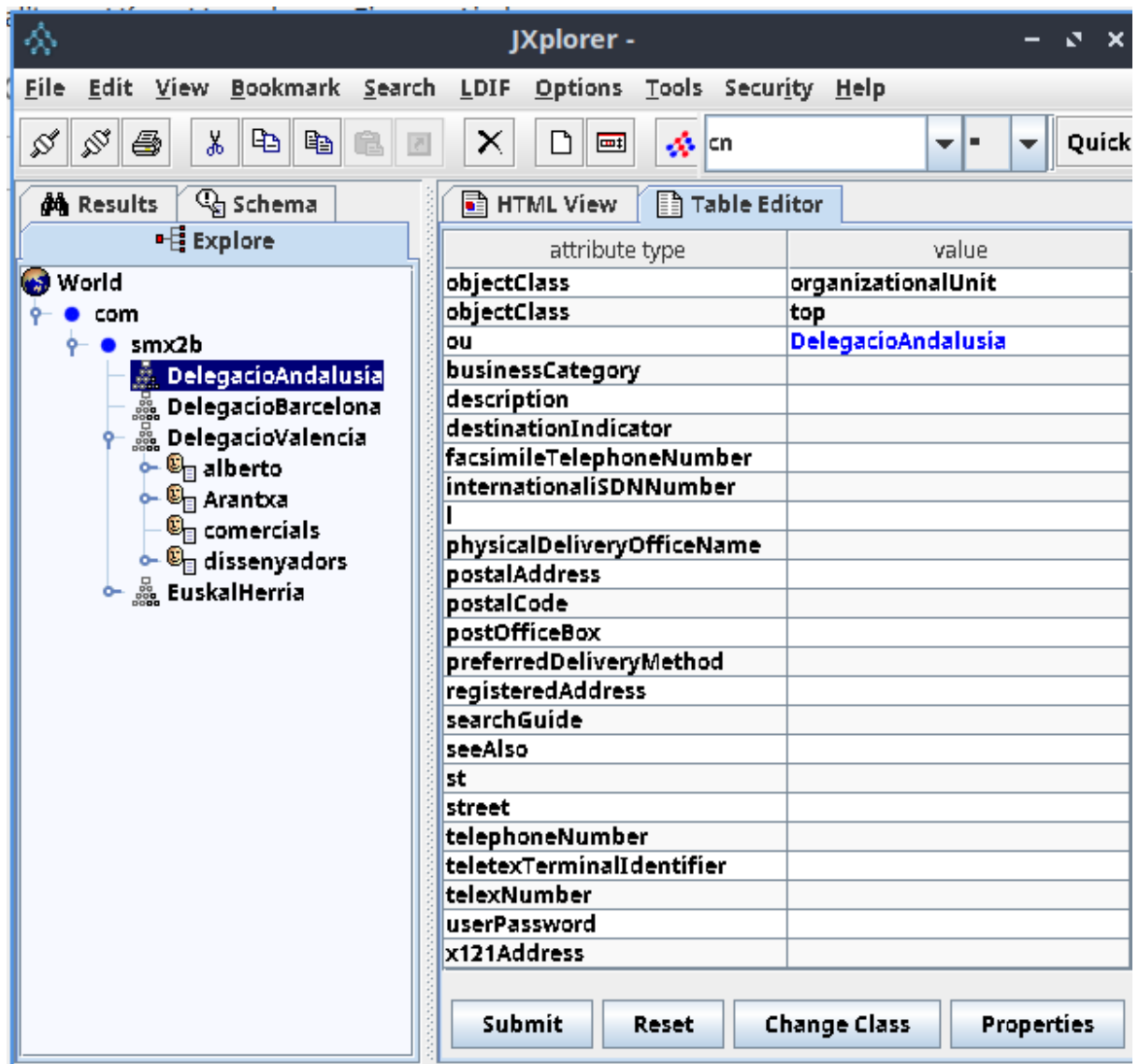
### Unitat Organitzativa (OU)

Com ja sabeu, una **unitat organitzativa** serveix com a contenidor lògic per organitzar altres objectes com usuaris, grups o altres OU dins del directori LDAP.

- **Classes d'objecte necessàries:**
  - `top`
  - `organizationalUnit`
- **Atributs obligatoris:**

- ou (Organizational Unit Name): El nom de la unitat organitzativa.





## Usuari del domini

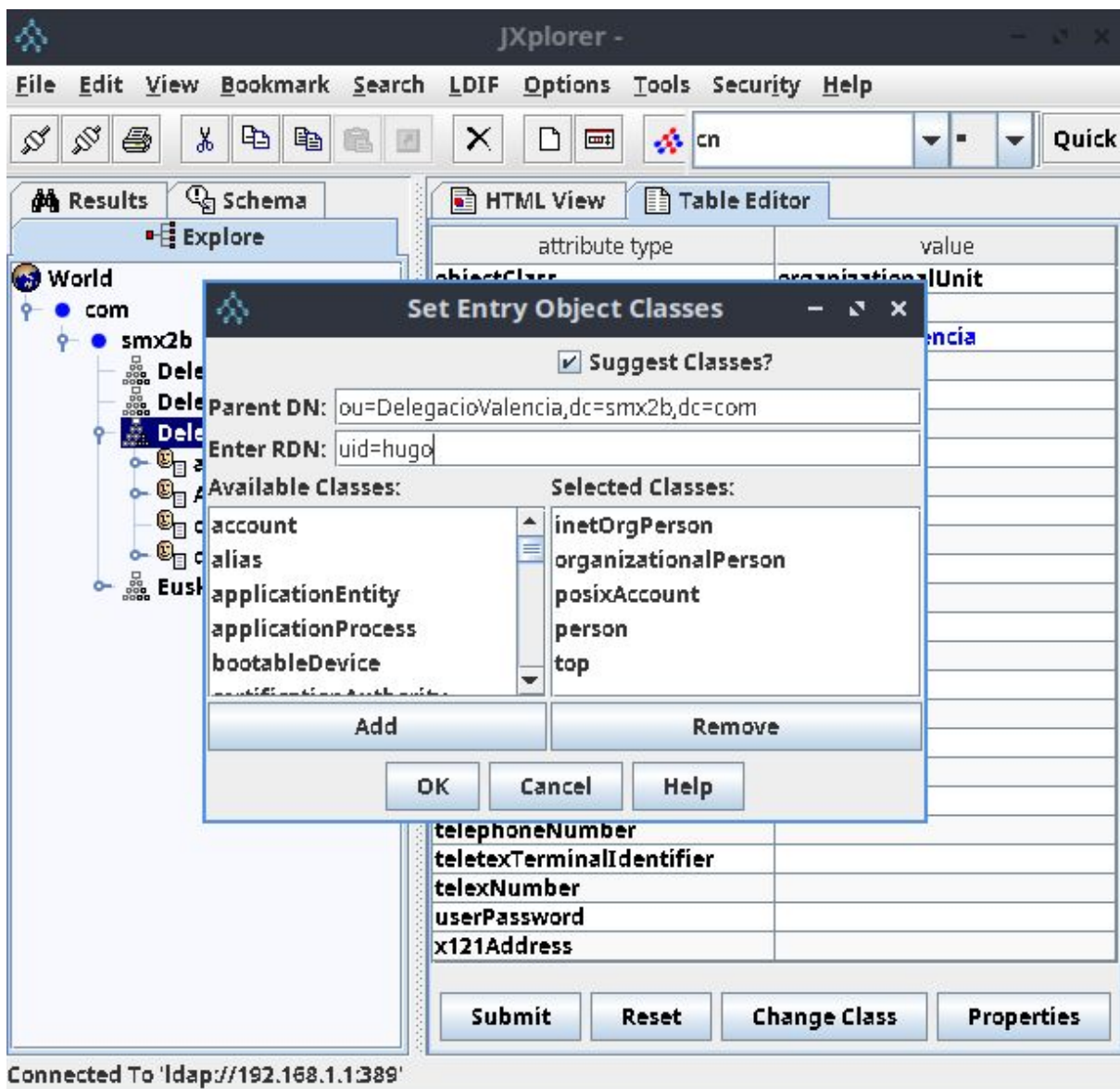
Un **usuari** ha de tenir atributs mínims per ser compatible amb Linux, especialment per poder iniciar sessió i interactuar amb el sistema.

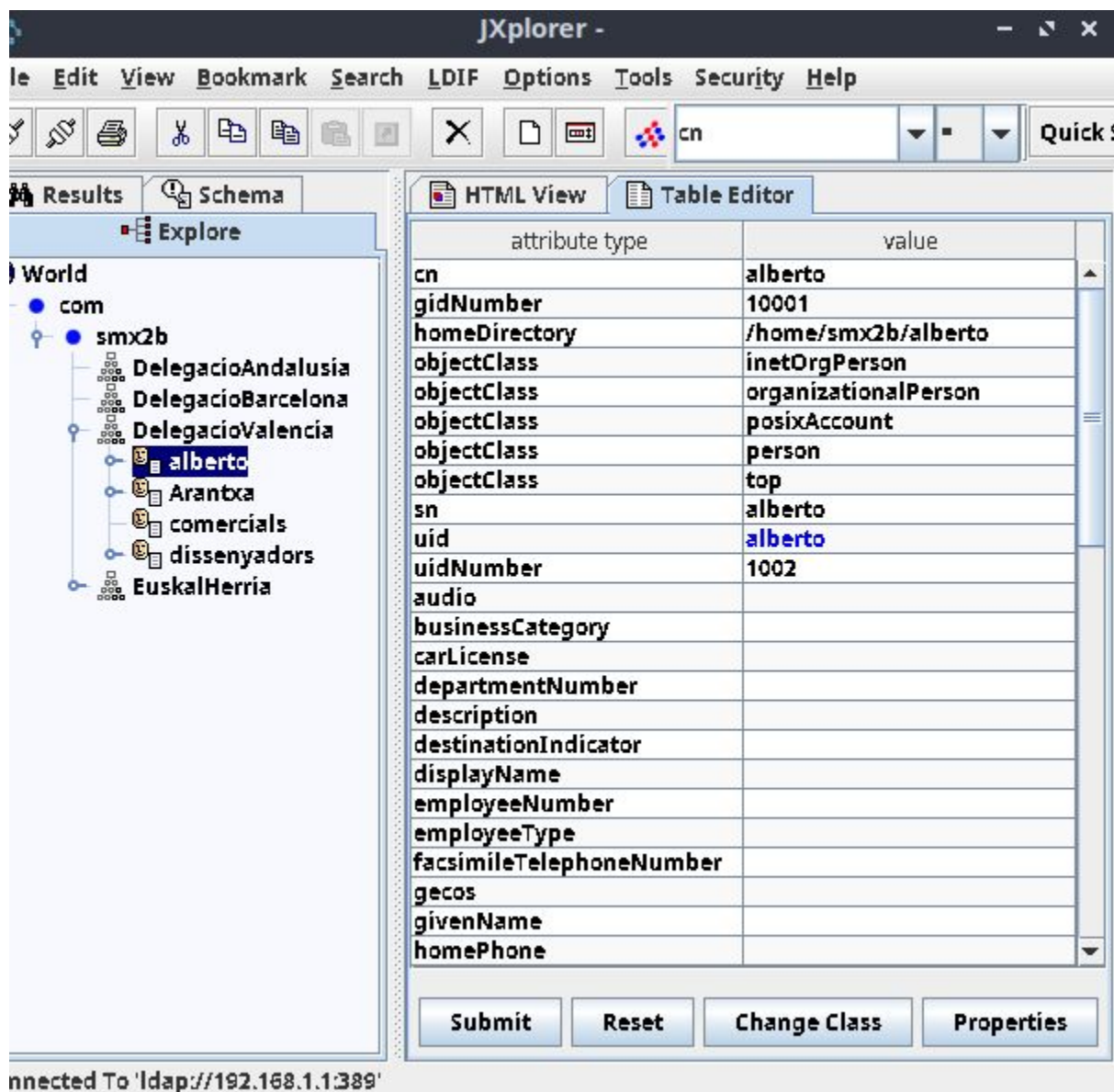
- **Classes d'objecte necessàries:**

- top
- posixAccount (indispensable per a compatibilitat amb Linux)
- inetOrgPerson (opcional, però útil per informació addicional de l'usuari)

- Atributs obligatoris per Linux (posixAccount):

- cn (Common Name): Nom complet de l'usuari.
- uid (User ID): Identificador únic de l'usuari.
- uidNumber: Número d'usuari (ha de ser únic).
- gidNumber: Número de grup principal associat a l'usuari.
- homeDirectory: Ruta del directori personal de l'usuari.
- loginShell: Shell de connexió (exemple: /bin/bash).





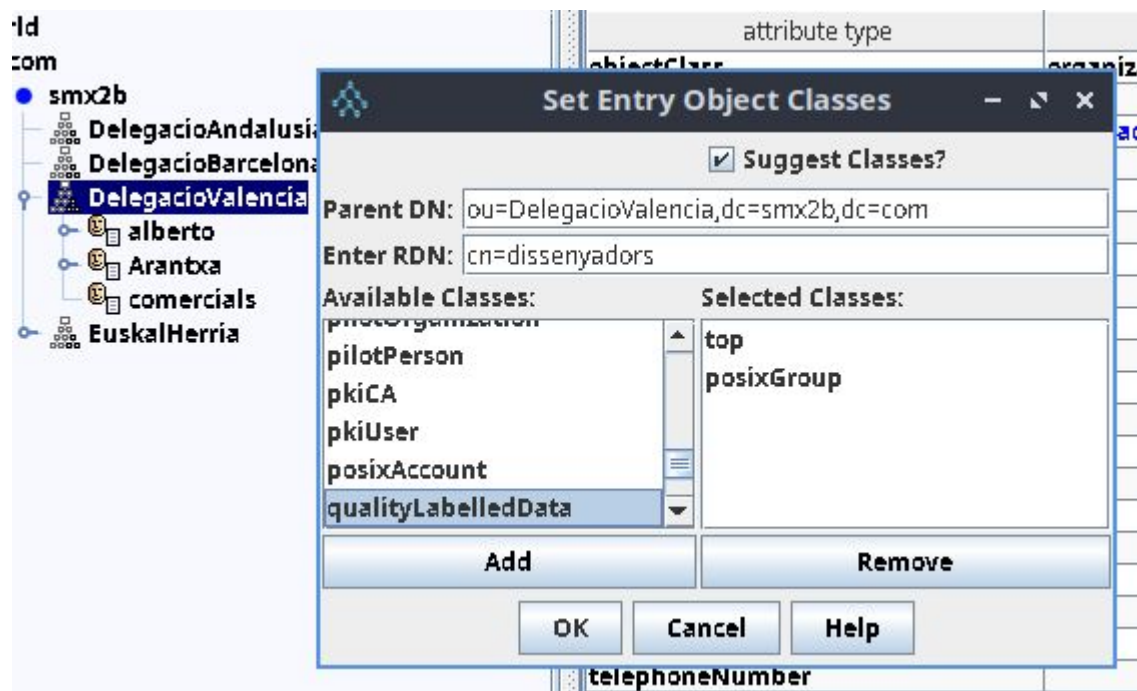
## Grup d'usuaris del domini

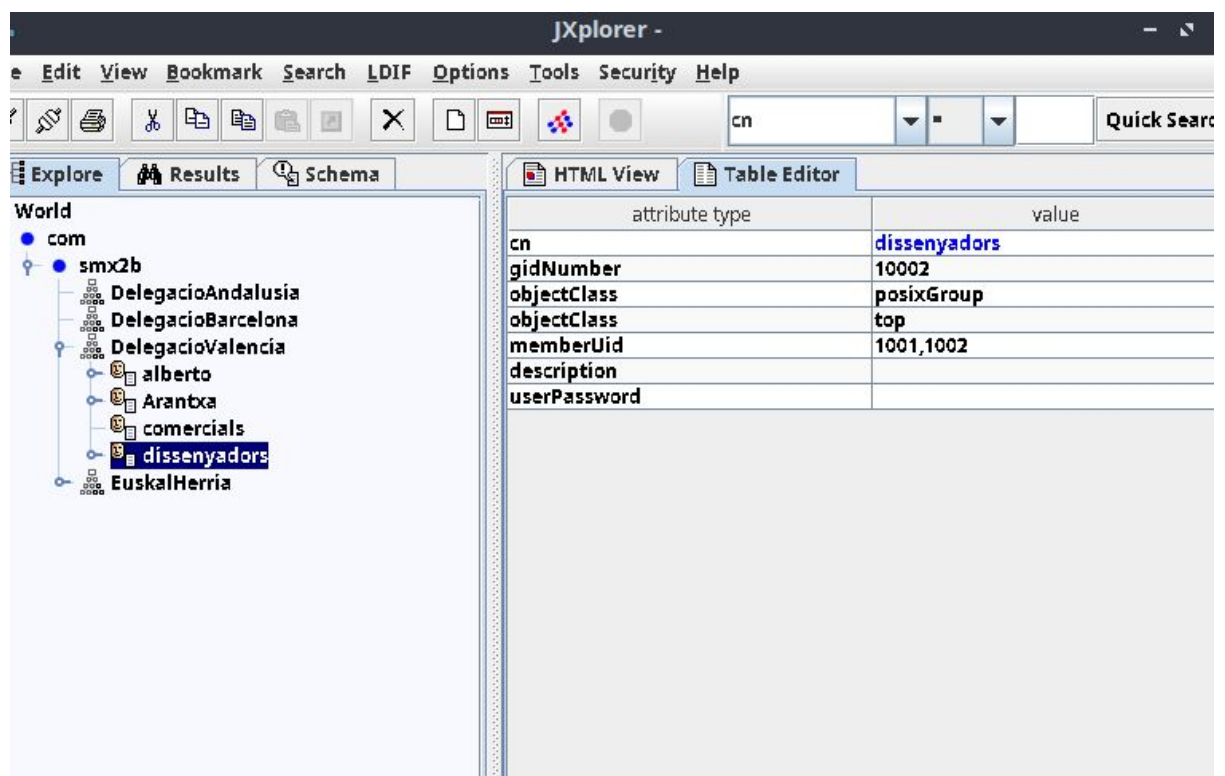
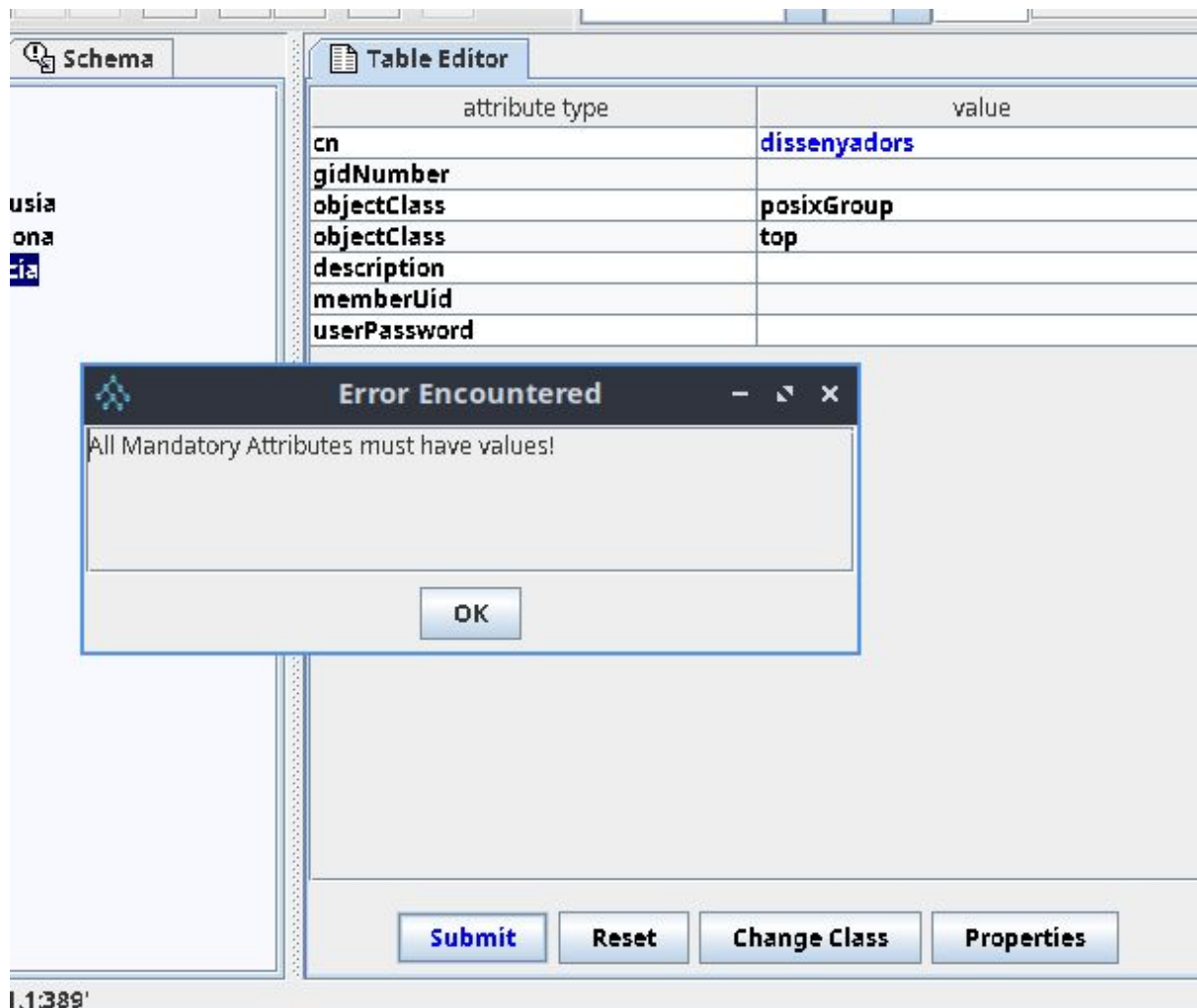
Un **grup** ha de tenir atributs mínims per ser reconegut pel sistema Linux i associar-se amb usuaris.

- Classes d'objecte necessàries:
  - top
  - posixGroup
- Atributs obligatoris per Linux (posixGroup):

- cn (Common Name): Nom del grup.
- gidNumber: Número de grup (ha de ser únic).
- memberUid (opcional, però recomanat): Identificadors dels usuaris que pertanyen al grup.

Veiem què passa si falten propietats requerides:





---

Tipus	Classes d'Objecte	Atributs Mínims Necessaris
Unitat	top,	ou
Organitzativa	organizationalUnit	
Usuari	top, posixAccount	cn, uid, uidNumber, gidNumber, homeDirectory, loginShell
Grup	top, posixGroup	cn, gidNumber, (memberUid opcional però recomanat)

---