OpenLDAP a Ubuntu

Server/Desktop 20.04

Instal·lació i configuració.

PART 1.

CFGS ASIX

Mòdul: Administració de Sistemes Operatius

UD3: Administració de serveis de directori: LDAP

[1 LDAP. Introducció 3](#__RefHeading___Toc1407_1745009031)

[1.1 Com funciona LDAP? 3](#__RefHeading___Toc1409_1745009031)

[1.2 Avantatges en l'ús de LDAP 3](#__RefHeading___Toc1411_1745009031)

[1.2.1 Usos pràctics de LDAP 4](#__RefHeading___Toc1413_1745009031)

[2 Estructura d’una base de dades/directori LDAP 5](#__RefHeading___Toc1415_1745009031)

[2.1 Entrades, objectes i atributs 5](#__RefHeading___Toc1417_1745009031)

[2.2 Estructura de l’atribut DN i una breu introducció històrica 6](#__RefHeading___Toc1419_1745009031)

[2.2.1 Introducció històrica 6](#__RefHeading___Toc1421_1745009031)

[2.2.2 Com organitzar les teues dades en el teu arbre de directori 7](#__RefHeading___Toc1423_1745009031)

[2.2.3 El DN d'una entrada LDAP 8](#__RefHeading___Toc1425_1745009031)

[3 Instal·lació i configuració de LDAP a Ubuntu 20.04 9](#__RefHeading___Toc1427_1745009031)

[3.1 Al servidor 9](#__RefHeading___Toc1429_1745009031)

[3.1.1 Configurar la targeta de xarxa 9](#__RefHeading___Toc1431_1745009031)

[3.1.2 Comprovem el nom de la màquina. 10](#__RefHeading___Toc1433_1745009031)

[3.1.3 Instal·lar els paquets d'OpenLDAP 11](#__RefHeading___Toc1435_1745009031)

[3.1.4 Parada i reinici del servei slapd 14](#__RefHeading___Toc1437_1745009031)

[3.2 Instal·lació d’eines de gestió de OpenLDAP 14](#__RefHeading___Toc1439_1745009031)

[3.2.1 Jxplorer 17](#__RefHeading___Toc1441_1745009031)

[3.2.1.1 Creació de les unitats organitzatives (ou) 19](#__RefHeading___Toc1443_1745009031)

[3.2.1.2 Afegir usuaris i grups 21](#__RefHeading___Toc1445_1745009031)

[4 Autenticació basada en LDAP 26](#__RefHeading___Toc1447_1745009031)

[4.1 Introducció 26](#__RefHeading___Toc1449_1745009031)

[4.2 Llibreries d'autenticació pam-ldap i nss-ldap 26](#__RefHeading___Toc1451_1745009031)

[4.3 Instal·lació i configuració de libpam-ldap i libnss-ldap 28](#__RefHeading___Toc1453_1745009031)

[4.3.1 Configuració de NSS 29](#__RefHeading___Toc1455_1745009031)

[4.3.2 Configuració de serveis PAM 31](#__RefHeading___Toc1457_1745009031)

[4.3.3 Creació automàtica directoris d’usuari (home) 31](#__RefHeading___Toc1459_1745009031)

[4.4 Comprovació de la configuració 33](#__RefHeading___Toc1461_1745009031)

[4.5 Configuració per iniciar sessió en entorn gràfic 34](#__RefHeading___Toc1463_1745009031)

[36](#__RefHeading___Toc1465_1745009031)

[5. Configuració dels perfils mòbils 38](#__RefHeading___Toc1467_1745009031)

[Enllaços d’interés 42](#__RefHeading___Toc1469_1745009031)

[5 Bibliografia 43](#__RefHeading___Toc1471_1745009031)

# LDAP. Introducció

LDAP significa Lightweight Directory Access Protocol. Com el seu nom indica, és un protocol lleuger en mode client-servidor per accedir als serveis de directori, específicament basats en els serveis de directori X.500. S'executa sobre TCP/IP o altres protocols orientats a connexió. LDAP es defineix a l'estàndard RFC2251. S'utilitza comunament per a emmagatzemar informació sobre organitzacions, usuaris, xarxes, etc.

Un directori (no confondre amb un directori del nostre disc dur, ja que és una estructura molt més àmplia) és similar a una base de dades, però tendeix a contenir més informació descriptiva, basada en atributs (recordem els atributs típics d'un arxiu en un directori local: només lectura, invisible, data de creació, etc...). En un directori, normalment, la informació es llegeix més que no pas s'escriu. **Els serveis de directori habitualment estan optimitzats per a donar una ràpida resposta en operacions de cerca o exploració**. També poden tenir la **capacitat de replicar (en diversos servidors físics) la informació continguda en un directori a fi i efecte de millorar la disponibilitat de les dades i la fiabilitat**. Com que la replicació de dades pot generar inconsistències, temporalment es sincronitzen les dades per a evitar-ho.

Hi ha moltes maneres diferents de proporcionar un servei de directori. Els diferents mètodes permeten que diferents tipus d'informació s'emmagatzemen en el directori, establir requisits diferents per a la forma en què la informació es pot referenciar, consultar i actualitzar, la manera com està protegida d'accessos no autoritzats, etc. Alguns serveis de directori són locals, proporcionant serveis a un context restringit (per exemple, el servei de finger en una única màquina). Altres serveis són globals, proporcionant serveis a un context molt més ampli.

## Com funciona LDAP?

El funcionament, com hem dit abans, està basat en un model client-servidor. Un client LDAP es connecta a un servidor LDAP i li fa una consulta. El servidor contesta amb la resposta, o amb un apuntador on el client pot obtenir més informació (típicament un altre servidor LDAP). Dèiem abans que poden haver molts servidors amb les dades replicades: per tant no és problema que un client es connecti amb un servidor o a un altre; el client veurà sempre la mateixa vista del directori. Aquesta és una característica molt important d'un servei global de directori com LDAP.

## Avantatges en l'ús de LDAP

Un directori LDAP destaca sobre els altres tipus de bases de dades per les següents característiques:

* És molt ràpid en la lectura de registres.
* Permet replicar el servidor de forma molt senzilla i econòmica.
* Moltes aplicacions de tot tipus tenen interfícies de connexió a LDAP i es poden integrar fàcilment.
* Disposa d'un model de noms globals que assegura que totes les entrades són úniques.
* Utilitza un sistema jeràrquic d'emmagatzematge d'informació.
* Permet múltiples directoris independents
* Funciona sobre TCP/IP i SSL
* La majoria de servidors LDAP són fàcils d'instal·lar, mantenir i optimitzar.

### Usos pràctics de LDAP

Donades les característiques de LDAP seus usos més comuns són:

* Directoris d'informació. Per exemple bases de dades d'empleats organitzats per departaments (seguint l'estructura organitzativa de l'empresa) o qualsevol tipus de pàgines grogues.
* Sistemes d'autenticació / autorització centralitzada. Grans sistemes on es guarda gran quantitat de registres i es requereix un ús constant dels mateixos. Per exemple: Active Directory Server de Microsoft, per gestionar tots els comptes d'accés a una xarxa corporativa i mantenir centralitzada la gestió de l'accés als recursos.
* Sistemes d'autenticació per a pàgines web, alguns dels gestors de continguts més coneguts disposen de sistemes d'autenticació a través de LDAP.
* Sistemes de control d'entrades a edificis, oficines ....
* Sistemes de correu electrònic. Grans sistemes formats per més d'un servidor que accedeixin a un repositori de dades comú.
* Sistemes d'allotjament de pàgines web i FTP, amb el repositori de dades d'usuari compartit.
* Grans sistemes d'autenticació basats en RADIUS, per al control d'accessos dels usuaris a una xarxa de connexió o ISP.
* Servidors de certificats públics i claus de seguretat.
* Autenticació única o "single sign-on" per a la personalització d'aplicacions.
* Perfils d'usuaris centralitzats, per permetre itinerància o "Roaming"
* Llibretes d'adreces compartides.

**Alguns exemples**

Sistema de correu electrònic

Cada usuari s'identifica per la seva adreça de correu electrònic, els atributs que es guarden de cada usuari són la seva contrasenya, el seu límit d'emmagatzematge (quota), la ruta del disc dur on s'emmagatzemen els missatges (bústia) i possiblement atributs addicionals per activar sistemes anti-spam o antivirus.

Com es pot veure aquest sistema LDAP rebrà centenars de consultes cada dia (una per cada correu electrònic rebut i una cada vegada que l'usuari es connecta mitjançant POP3 o webmail). No obstant el nombre de modificacions diàries és molt baix, ja que només es pot canviar la contrasenya o donar de baixa a l'usuari, operacions ambdues que no es realitzen de forma freqüent.

Sistema d'autenticació a una xarxa

Cada usuari s'identifica per un nom d'usuari i els atributs assignats són la contrasenya, els permisos d'accés, els grups de treball als quals pertany, la data de caducitat de la contrasenya, etc...

Aquest sistema rebrà una consulta cada vegada que l'usuari accedeixi a la xarxa i una més cada vegada que accedeixi als recursos del grup de treball (directoris compartits, impressores ...) per comprovar els permisos de l'usuari.

Enfront d'aquests centenars de consultes només unes poques vegades es canvia la contrasenya d'un usuari o se l'inclou en un nou grup de treball.

# Estructura d’una base de dades/directori LDAP

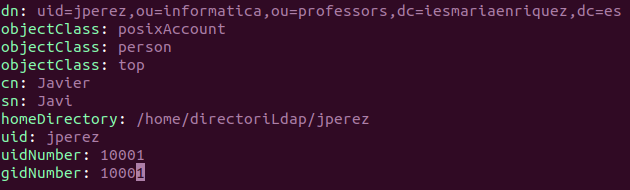
## Entrades, objectes i atributs

Com hem dit abans, una 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.**

Veiem primer, el punt i final del directori, que és **l’entrada o objecte**. El model d'informació de LDAP està basat en entrades. **Una entrada és una col·lecció d'atributs** que tenen un **Nom Distintiu o Distinguished Name** (identificat com **DN**) **únic i global**. El DN s'utilitza per referir-se a una entrada sense ambigüitats. Cada atribut d'una entrada té un tipus i un o més valors i son els que contenen la informació associada a l’objecte. Els tipus són normalment paraules mnemotècniques, com "**cn**" per **common name**, o "**mail**" per una adreça de **correu**.

En comparació amb una base de dades relacional, una entrada seria com un registre. L’atribut seria el camp.

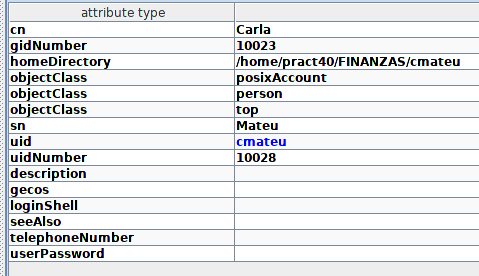
Una entrada, que no és més que un fitxer de text, té una estructura com la següent:



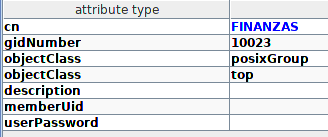
L’**objectclass** indica quins atributs **podem** i **hem** d’utilitzar per cada entrada. Si heu programat amb llenguatges orientats a objectes, l’objectclass és la classe que determina els elements que componen un objecte. A la captura tenim tres objectClass:

* posixAccount: Té com a atributs obligatoris cn, uid, uidNumber, gidNumber, homeDirectory, i com a opcionals description, userPassword, etc..
* person: Té com a atributs obligatoris cn, sn i com a opcionals description, userPassword, etc, telephone, etc.
* top: Aquest és l’objectClass arrel, tota la resta de classes pengen d’aquesta

La següent captura correspon a l’entrada d’un usuari. Amb camp obligatori el uid.



La següent captura correspon a una entrada d’un grup. Només tenim un atribut obligatori, el cn.



## Estructura de l’atribut DN i una breu introducció històrica

### Introducció històrica

El nivell superior d'un directori LDAP és la base, conegut com el "DN base". Un DN base, generalment, pren una de les tres formes llistades ací. Suposem que treballes o estudies a l’institut Maria Enriquez de Gandia, el qual està a Internet a iesmariaenriquez.es.

**o = "IES Maria Enriquez", c = ES**

*(DN base en format X.500)*

En aquest exemple, **o = IES Maria Enriquez** es refereix a l'**organització**, que en aquest context hauria de ser tractada com un sinònim del nom de l'empresa. **c = ES** indica que la **localització general** de l'empresa està a ES. Hi havia una vegada en què aquest va ser el mètode d'especificar la teva DN base. Els temps i les modes canvien, però, aquests dies, la majoria de les empreses estan (o planegen estar) a Internet. I amb la globalització d'Internet, utilitzar un codi de país a la base DN probablement faça les coses més confuses al final. Amb el temps, el format X.500 ha evolucionat a altres formats llistats més avall.

**o = iesmariaenriquez.es**

*(DN base derivat de la presència a Internet de l'empresa)*

Aquest format és bastant senzill, utilitzant el nom de domini de l'empresa com a base. Una vegada has passat la porció o = (la qual ve de organization =), qualsevol a la teva empresa hauria de saber d'on ve la resta. Aquest va ser, fins fa poc, probablement el més comú dels formats usats actualment.

**dc = iesmariaenriquez, dc = ES**

*(DN base derivat dels components de domini DNS de l'empresa)*

Com el format previ, aquest utilitza el nom de domini DNS com la seva base. Però on l'altre format deixa el nom de domini intacte (i així llegible per les persones), aquest format està separat en components de domini: **iesmariaenriquez.es esdevé dc = iesmariaenriquez, dc = es**. En teoria, això pot ser lleument més versàtil, encara que és una mica més dur de recordar per als usuaris finals.

**Aquest és el format recomanable** per a noves instal·lacions. Si estàs planejant utilitzar Active Directory, Microsoft ja ha decidit per tu que aquest és el format que necessites .

### Com organitzar les teues dades en el teu arbre de directori

En un sistema de fitxers UNIX, el nivell més alt és l'arrel (**/**). Per sota de l'arrel tens molts fitxers i directoris. Com es comentava anteriorment els directoris LDAP estan configurats en gran part de la mateixa manera.

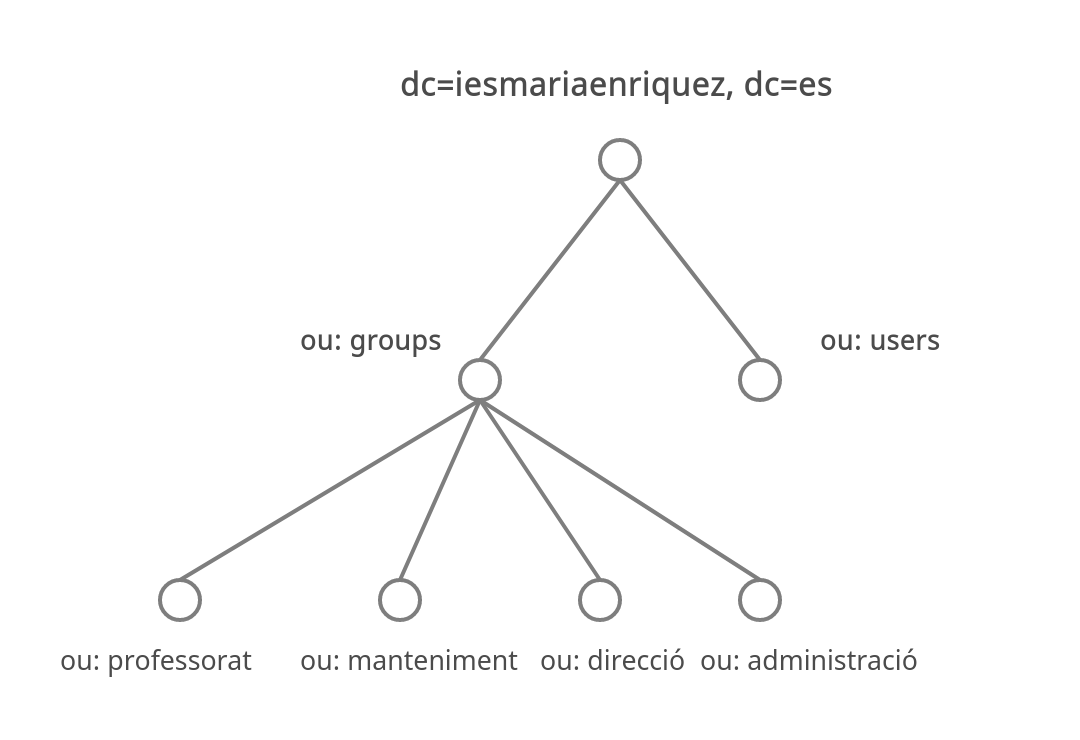
Sota la teva base de directori, voldràs crear contenidors que separin lògicament les teves dades. Per raons històriques (X.500), la majoria dels directoris configuren aquestes separacions lògiques com a entrades OU. **OU** ve de "**Unitats organitzacionals**" (**Organizational Units**, en anglès), que en X.500 eren utilitzades per indicar l'organització funcional dins de l'empresa: vendes, finances, etc. Actualment les implementacions de LDAP han mantingut la convenció del nom ou =, però separa les coses per categories àmplies com ou = gent (ou = people), ou = grups (ou = groups), ou = dispositius (ou = devices), i altres.

Per exemple, un arbre de directori LDAP (sense incloure entrades individuals) podria ser així:

dc = iesmariaenriquez, dc = es  
 ou = groups   
 ou = direccio  
 ou = administracio  
 ou = professorat

ou = manteniment

ou = users



### El DN d'una entrada LDAP

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**) i **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 ítems 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. Si estic emmagatzemant un registre per la meva recepta preferida de menjar de civada, estaré utilitzant cn=MenjardeCivadaDeluxe com el RDN de la meva entrada.

* El **DN** base del meu directori és *dc=iesmariaenriquez, dc=es*
* El **RDN** d’un registre d’un grup *cn=alumnes*

Atès tot això, quin és el DN complet del registre LDAP per a aquesta grup? Recorda, es llegeix en ordre invers, cap a enrere - com els noms de màquina en els DNS.

**cn = alumnes, ou = groups, dc = iesmariaenriquez, dc = es**

Ara és el moment d'abordar el DN d'un membre del nostre institut. 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 professor Armand Mata (nom de login: armandmata) pot semblar-se a un d'aquests dos formats:

**uid = armandmata, ou = professorat, ou=people, dc = iesmariaenriquez, dc = es**

(basat en el login)

LDAP (i X.500) 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. No t'has de preocupar sobre què faràs quan entre un nou professor amb el mateix nom, o si el mateix professor decideix canviar-se el nom. No has de canviar el DN de l'entrada LDAP.

**cn = ArmandMata, ou = professorat, ou=people, dc = iesmariaenriquez, dc = es**

(basat en el nom)

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. Com s'indica anteriorment, has d'evitar canviar en **DN** d'una entrada sempre que siga possible.

# Instal·lació i configuració de LDAP a Ubuntu 20.04

## Al servidor

Nom de la màquina virtual i de l'equip: elVostreNomLDAP

Usuari principal: admin

Contrasenya usuari principal: admin

Dos targetes de xarxa

NAT --> DHCP

Xarxa Interna, interfície inet -> Manual

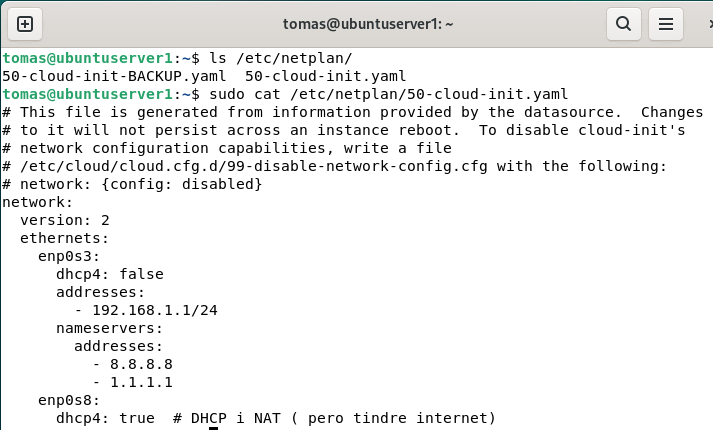
### Configurar la targeta de xarxa

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. Esperem uns segons i comprovem amb ip a la configuració de les targetes.

Busque el fitxer i l'edite amb nano

*sudo nano /etc/netplan/50-cloud-inityaml*

EL resultat és:



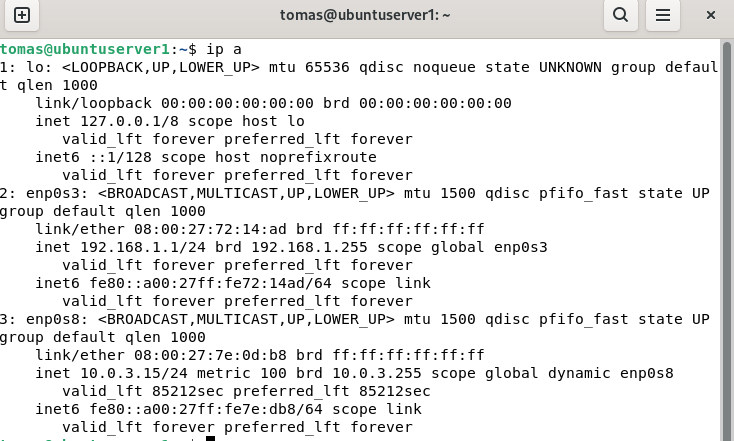
I apliquem els canvis

*sudo netplan apply*

Fem ip a per comprovar els canvis

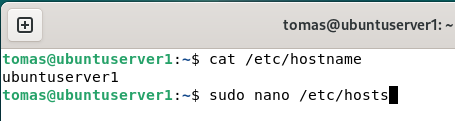
*ip a*

**(No fa falta fer ús del netplan, podeu configurar la direcció a l’entorn gràfic)**



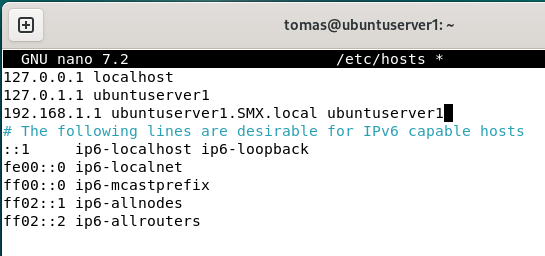
### Comprovem el nom de la màquina.

*sudo cat /etc/hostname*



*sudo nano /etc/hosts*

Hem de modificar el fitxer /etc/hosts per a que la nostra IP estàtica estiga associada al nostre domini.



Cal reiniciar la màquina per a que els canvis siguen efectius

*sudo reboot*

### Instal·lar els paquets d'OpenLDAP

Primer que res actualitzem els repositoris de la màquina i apliquem les últimes actualitzacions

*sudo apt update*

*sudo apt upgrade*

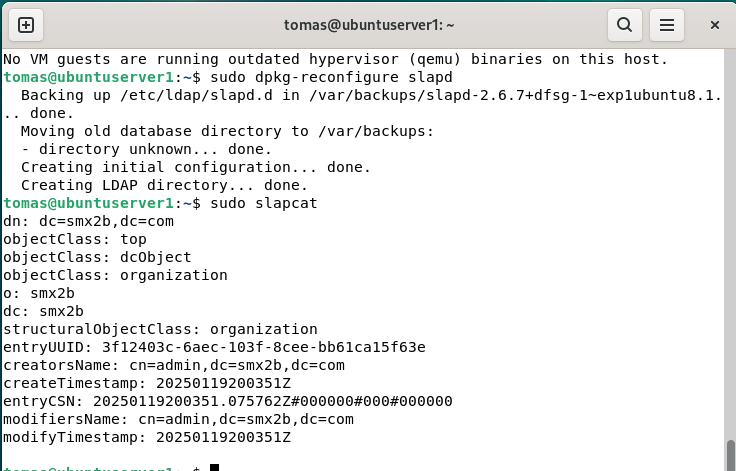
Ara sí, instal·lem els paquets de LDAP

*sudo apt install slapd ldap-utils -y*

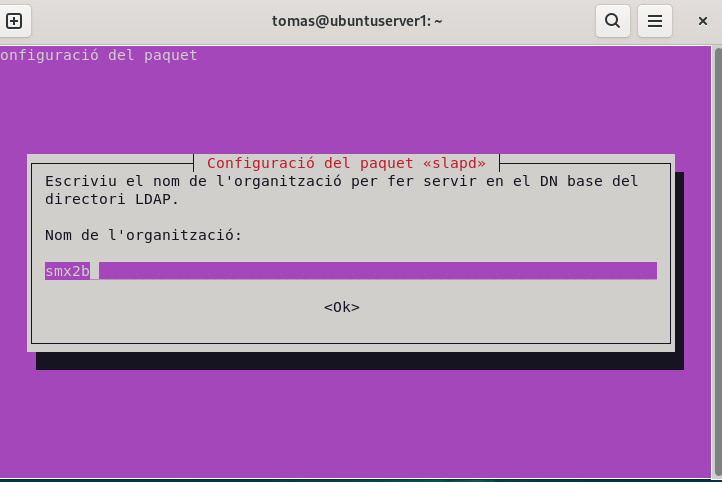
Ens demana la contrasenya que volem utilitzar

Si no s’inicia l’assistent de configuració podem iniciar-ho nosaltres amb:

*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.
* A les següents preguntes podeu deixar l’opció per defecte.



Per últim, ens demana si volem que s’esborre automàticament la DDBB quan fem un “purge” del paquet slapd. Tot depén del que tingam, si som responsables i tenim còpies de seguretat, podem donar-li a “Sí”, però si únicament tenim el directori a este equip, ens interessa que no s’esborre.

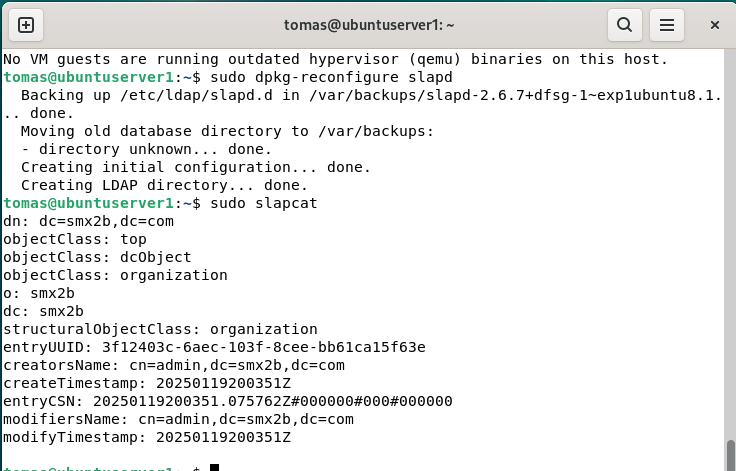
Comprovem si ha funcionat tot correcte amb l'ordre

*sudo slapcat*

### Parada i reinici del servei slapd

Si necessitem reiniciar el servei sense reiniciar la màquina podem fer

*sudo systemctl start/restart/status/stop*



## Instal·lació d’eines de gestió de OpenLDAP

Hi ha diverses eines gràfiques que podem utilitzar per gestionar OpenLDAP, les podem fer servir a una màquina client com a una màquina amb rol de servidor. En aquests apunts la farem servir a un Ubuntu Desktop.

Abans de començar anem a revisar la configuració de la targeta de xarxa al client.

**Client**

Nom de la màquina virtual i de l'equip: cognom\_clientLDAP

Usuari principal: client

Contrasenya usuari principal: client

Dos targetes de xarxa

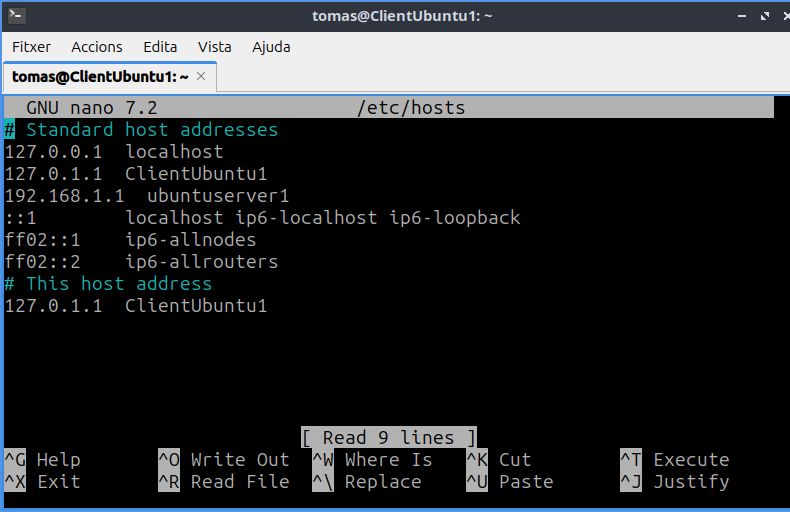
NAT --> DHCP

Interna interfície inet --> Manual

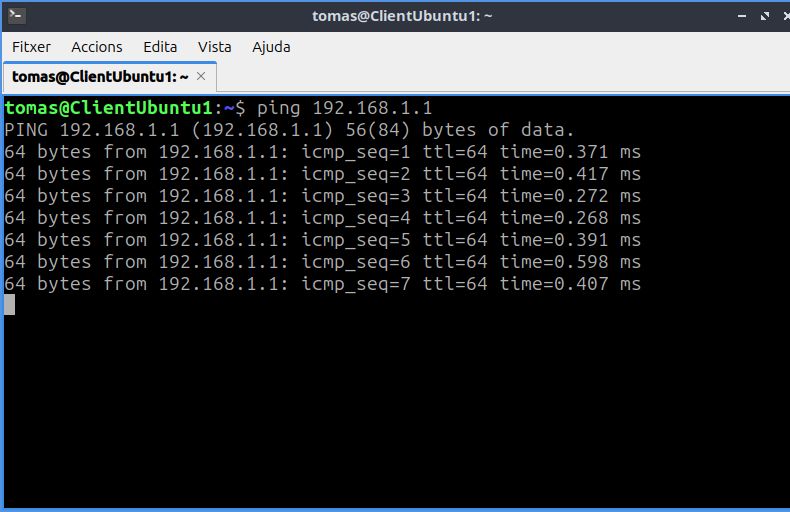
Editem la configuració de la segona targeta de xarxa, la de xarxa interna, i li fiquem una IP fixa i la màscara. En el meu cas utilitzaré l'IP 192.168.1.10/24

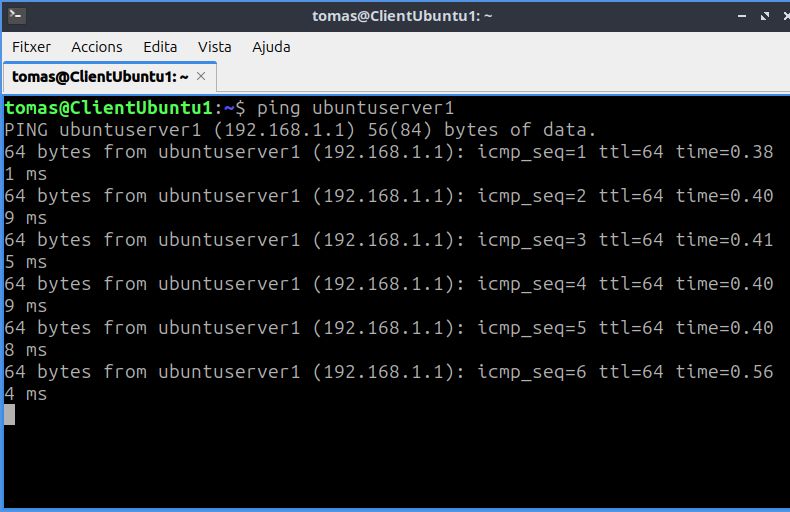


Afegim a “/etc/hosts” el nom i la direcció del nostre servidor LDAP, com és lògic, el nom del vostre servidor no serà el mateix ni tampoc el del client.



Comprovem que podem fer un ping a Google i al nostre servidor. Per comunicar-nos amb el servidor podem utilitzar la IP o el nom del servidor.





Ara ja podem començar a treballar.

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

La primera ofereix des d’un entorn web la possibilitat d’explorar la base de dades LDAP, els objectClass, els seus atributs, etc. Importar/exportar elements, etc.

El segon i tercer és un entorn basat en Java, molt més complet, però també més lent. Veurem aquest segon.

### 

### Jxplorer

Per utilitzar el programa necessitem tindre l'entorn de Java instal·lat. Revisem si Java s'ha instal·lat anteriorment:

*java -version*

Si no està instal·lat, l'instal·lem

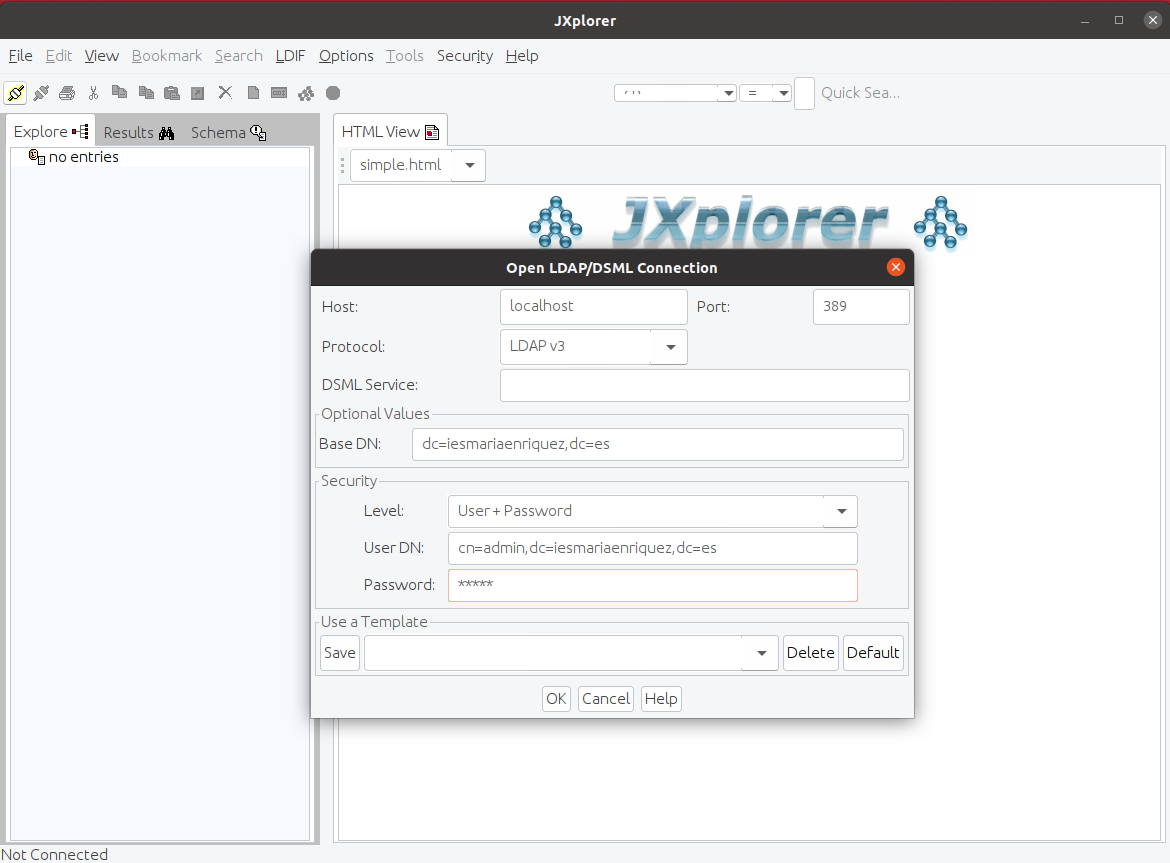
*sudo apt install openjdk-11-jdk*

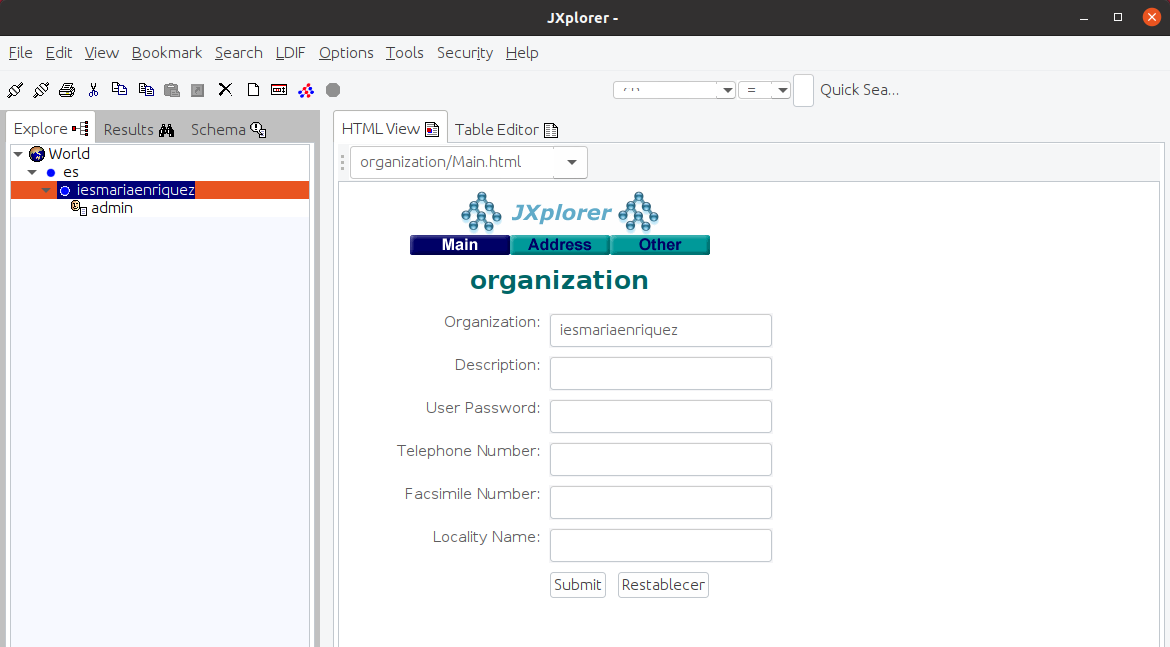
Ara ja si podem instal·lar el programa Jxplorer

*sudo apt install jxplorer*

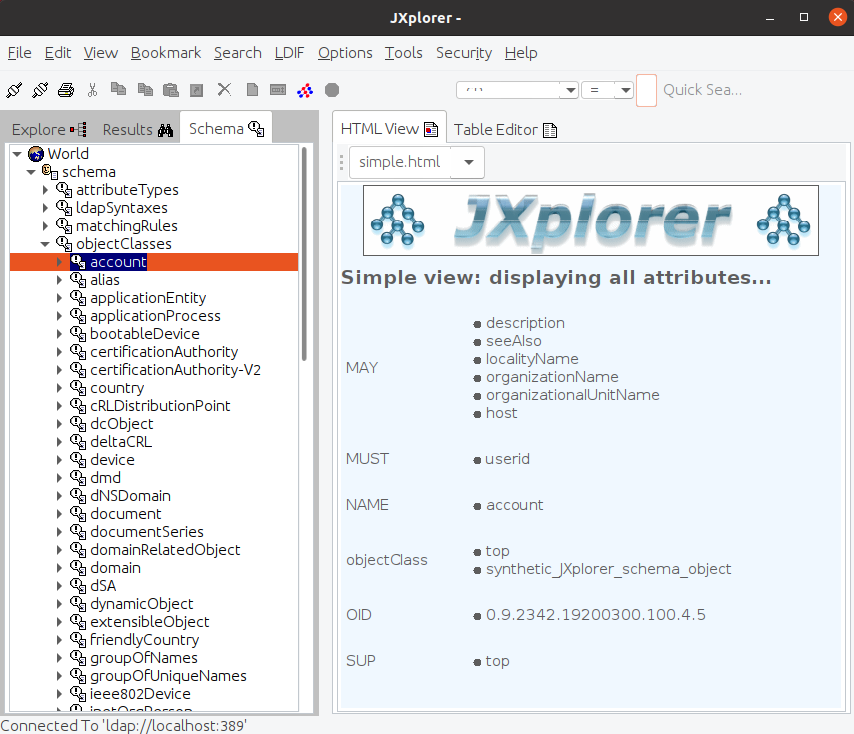
Iniciem el programa. Una vegada encés, la icona Connectar ens mostrarà la següent pantalla on configurarem els paràmetres de la connexió.

|  |
| --- |
| Important: El client executarà jxplorer, però haurà de connectar amb el servidor ldap. Si aquest és a la mateixa màquina, la IP a especificar serà 127.0.0.1 o localhost. Si el servidor es troba en una altra màquina (habitual), caldrà indicar la seva IP o afegir el nom al fitxer /etc/hosts |





Si seleccionem la pestanya ***schema*** podrem veure (i fins i tot editar, tot i que no es recomana) tots els objectes i atributs del nostre directori LDAP.



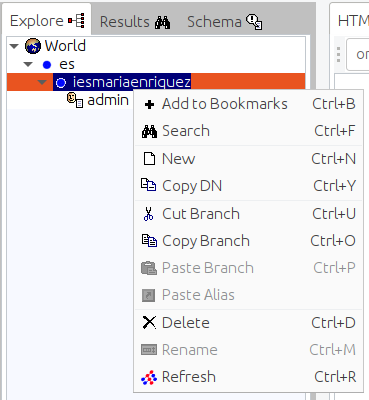
La pestanya ***Results*** servirà per a fer recerques. Inicialment tenim el directori buit, i per tant no trobarem res.

#### Creació de les unitats organitzatives (ou)

Ja que el nostre directori, en pràctiques posteriors, emmagatzemarà usuaris i grups, anem a crear **dos unitats organitzatives anomenades "*users*" i "groups"** que ens serviran per a organitzar els usuaris i grups per separat.

Dins de la unitat organitzativa “*users*” crearem tots els usuaris del sistema. Dins de la unitat organitzativa “*groups*” crearem tots els grups del sistema.

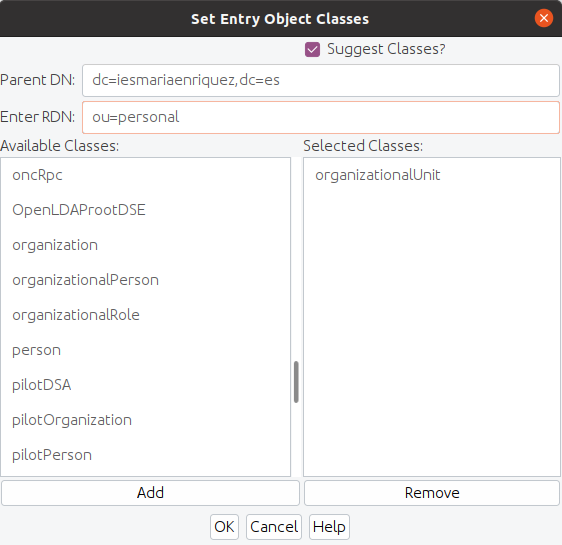
Per a crear una unitat organitzativa dins la nostra organització, farem clic amb el botó dret sobre l'organització “empresa” i al menú contextual elegirem 'New':



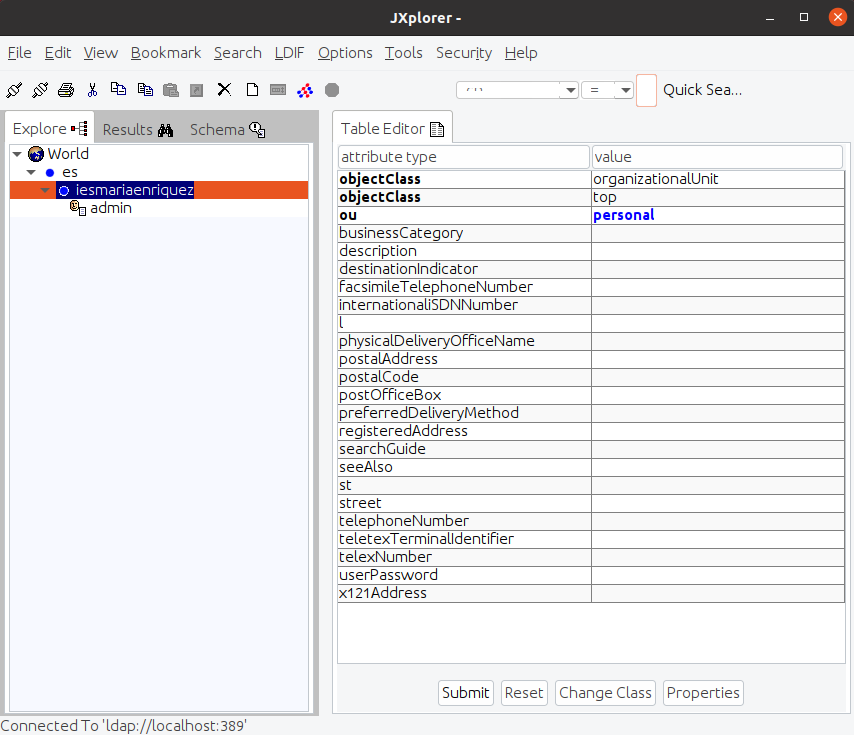
Ens apareixerà la finestra “Set Entry Object Classes”. Hi podrem triar els “tipus” que tindrà el nostre nou element. Com es tracta d'una unitat organitzativa (**ou**) hem de seleccionar el tipus **organizationalUnit** a la llista de l'esquerra i prémer el botó afegir (Add).

Els altres dos tipus que apareixen per defecte (organizationalRole i simpleSecurityObjet) no els necessitarem, per tant podem seleccionar de la llista de la dreta i prémer el botó treure (remove).

A la casella “Enter RDN” (introduir Nom Distingit Relatiu) hem de posar el nom del nostre element. Escriurem **ou = users**.



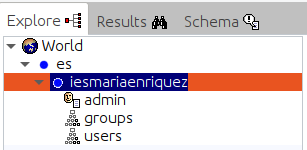
Estarem en la situació de la següent figura:



A la part de la dreta podrem acabar d’emplenar els atributs de la nostra nova entrada i al finalitzar prémer **Submit**.

Fem el mateix per a “groups”.

I acabarem amb una estructura com la següent:



#### Afegir usuaris i grups

Ara només ens queda crear els usuaris i els grups,cadascun dintre de la seva pròpia unitat organitzativa.

Seguirem un esquema com el següent:

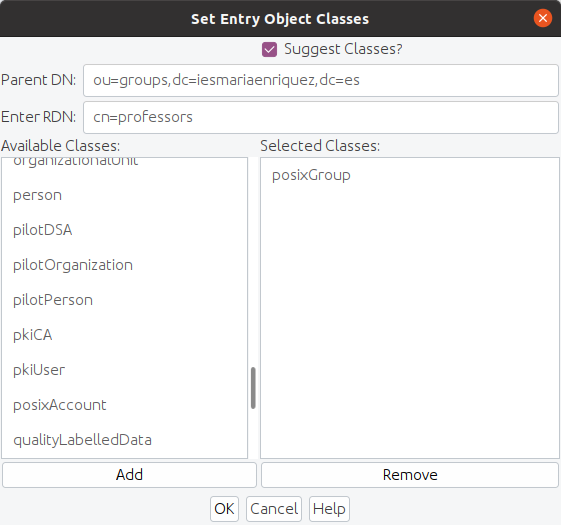
* professorat (gidNumber=10001)
* alumnes (gidNumber=10002)

Dintre de la **ou “users”** crearem els següents usuaris:

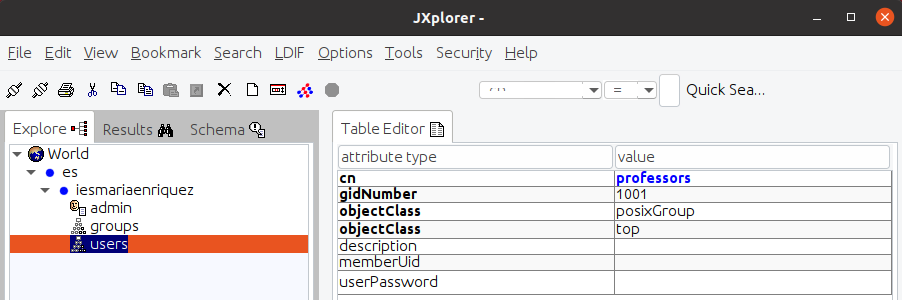
* **elteunom**(uidNumber=10001, professor)
* carlosPerez (uidNumber=10002, professor)
* josepPeiro(uidNumber=10003, professor)
* cristinaDeArmas (uidNumber=10004, alumne)
* andreuMas (uidNumber=10005, alumne)

Per a crear els grups, farem clic amb el dret a la unitat organitzativa **“groups”** i igual que abans farem clic a **“New”**. El nostre nou element serà un nou **grup POSIX**, per tant hem d'afegir el tipus **“posixGroup”** de la llista de l'esquerra.

El nom (RDN) serà **professors**, per tant hem d'escriure 'cn = **professors**' (cn = Common Name - Nom Comú):

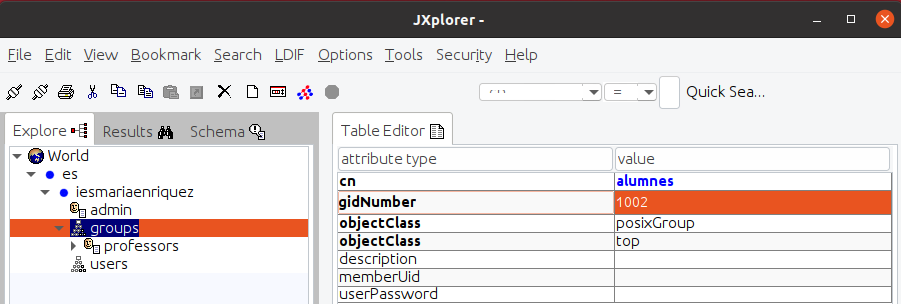


A continuació emplenem el gid corresponent a mà:



Premem submit.

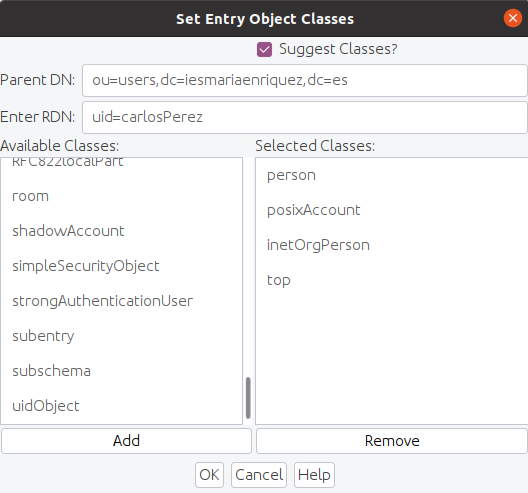
A continuació fem el mateix per al grup Alumnes.



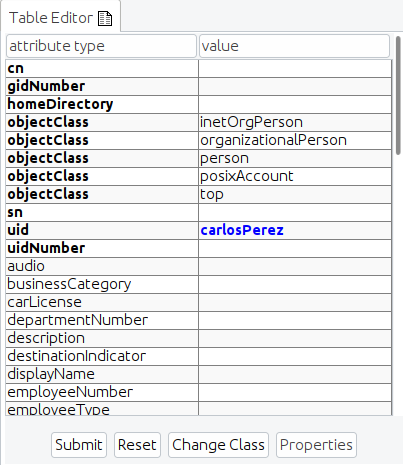
Per a crear els usuaris, farem clic amb el dret a la unitat organitzativa **“users”** i igual que abans farem clic a **“New”**. El nostre nou element serà un nou **usuari POSIX**, per tant hem d'afegir el tipus “**posixAccount**” de la llista de l'esquerra.

Però el nostre usuari també serà una persona, per això ens interessa afegir el tipus **“person”** per disposar dels atributs d'aquest tipus (nom, cognoms, ...), a més com serà usuari d'Internet ens interessa afegir també el tipus **“inetOrgPerson”** per poder desar l'e​-mail i altres valors.

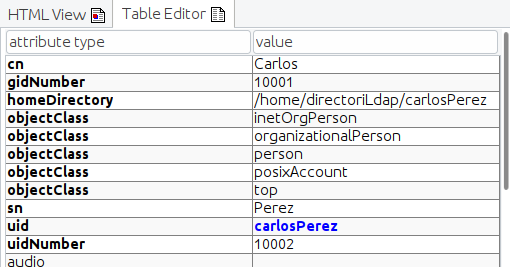
Com hem dit abans hi ha dos opcions, crear l’usuari en base a l’uid (identificador o login) o amb base el cn (Common Name). Recordeu que aquest valor ha de ser únic. Si el seu nom és Tomàs Ferrandis, podem escriure a la casella RDN 'uid= tomasFerrandis'.



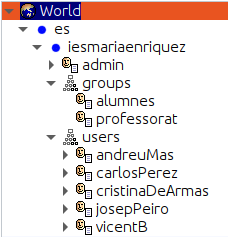
Premem OK i a continuació emplenem els atributs que veus:



Observa que els objectClass que hem indicat, ens indiquen **en negreta tots els atributs** que té el **uid=carlosPerez** com **obligatoris**, a més, el gidNumber ha de correspondre al grup al qual pertany, i el uidNumber al que li correspon també (no confondre amb el uid, que omplim amb el nom del login).



Finalment ens queda una estructura similar a la següent:

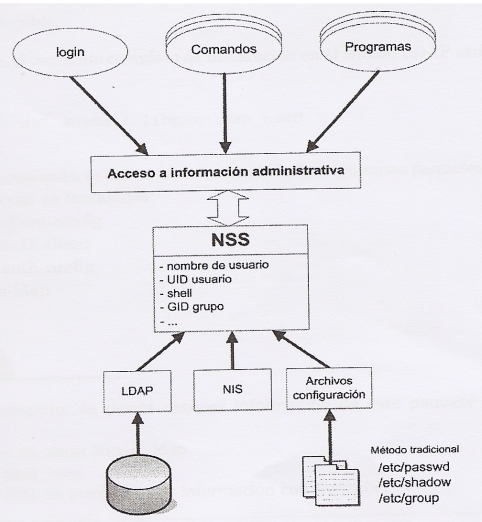


# Autenticació basada en LDAP

## Introducció

Entre les utilitats que havíem comentat abans, una de les més utilitzades del servidor LDAP és **l’autenticació**: per a entrar en un sistema Unix/Linux., per accedir a servidors FTP, per a pàgines web privades, etc.

En aquest apartat començarem a veure com fer que un sistema Linux per a que autentique als usuaris en un servidor LDAP enlloc utilitzar els clàssics fitxers /etc/passwd, /etc/group i /etc/shadow. Per fer-ho hem d’instal·lar i configurar els paquets ***libpam-ldap i libnss-ldap.***



## Llibreries d'autenticació pam-ldap i nss-ldap

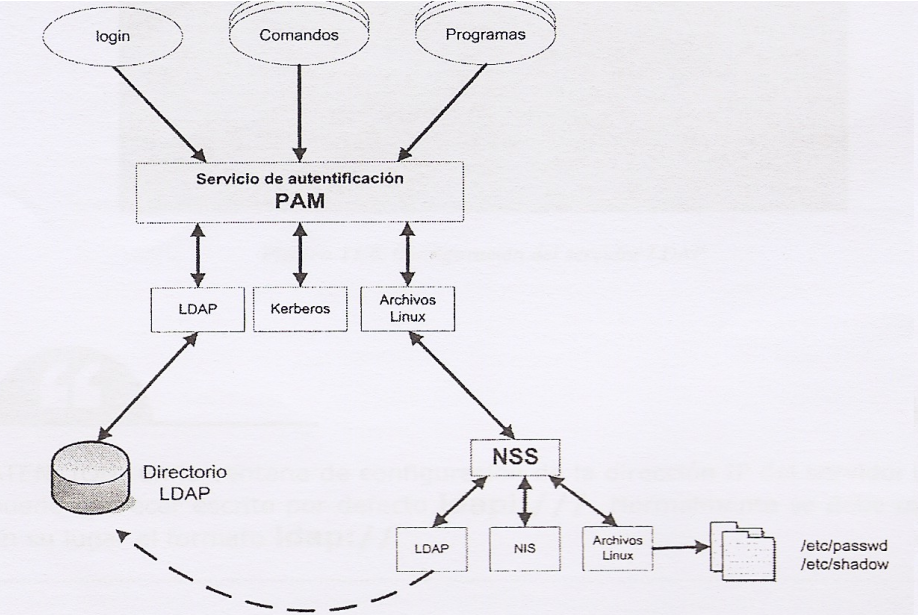
La llibreria **pam-ldap** permet que les aplicacions que utilitzen **PAM (Pluggable Authentication Modules)** per autenticar, puguen fer-ho mitjançant un servidor LDAP. Linux empra aquest mecanisme per a la validació local, per tant ens cal instal·lar aquesta llibreria.

L'arxiu de configuració d'aquesta llibreria és **/etc/ldap.conf**. Hi ha altres aplicacions o serveis que utilitzen PAM per l'autenticació i per tant podrien, gràcies a la llibreria **pam-ldap**, autenticar-se davant un servidor LDAP.

Per especificar el mode d'autenticació de cada servei és necessari configurar els arxius que es troben a la carpeta ***/etc/pam.d/***. Al final d'aquest apartat s'indiquen els canvis necessaris en aquests arxius.

La llibreria **nss-ldap** permet que un servidor LDAP suplanti als arxius /etc/passwd, /etc/group i /etc/shadow com a bases de dades del nostre sistema client. El seu arxiu de configuració es troba a ***/etc/ldap.conf*** (comparteix arxiu de configuració amb la llibreria **pam-ldap**).

Posteriorment haurem de configurar el arxius que són **/etc/nsswitch.conf** per a que s'utilitze LDAP com a base de dades del sistema en lloc dels arxius passwd, group i shadow.



## 

## Instal·lació i configuració de libpam-ldap i libnss-ldap

**Client**

Primer que res actualitzem la màquina

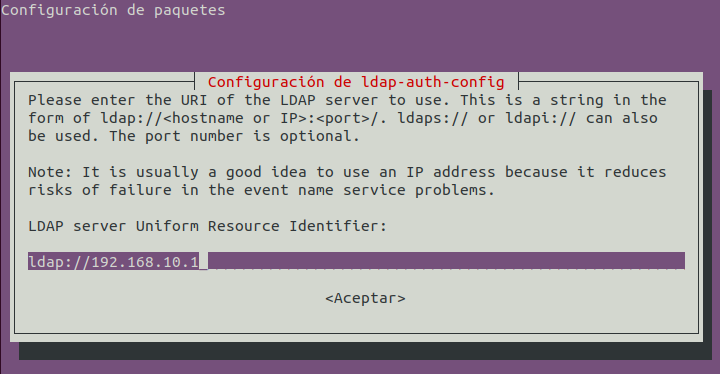
*$ sudo apt update*

*$ sudo apt upgrade*

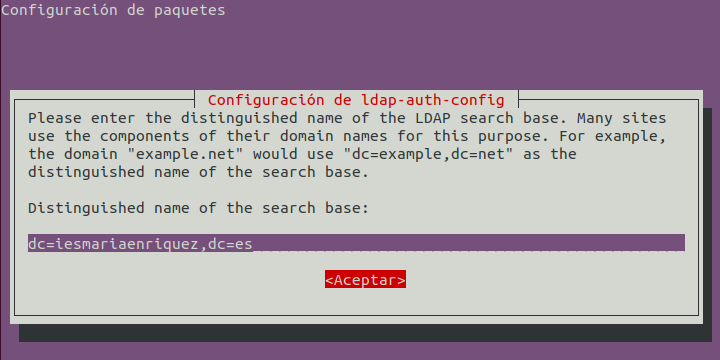
Ara sí, instal·lem els paquets del client LDAP

*$ sudo apt install libnss-ldap libpam-ldap ldap-utils -y*

Començarà el tutorial per a la configuració:



**Fixeu-vos que NO és ldapi:///, hem llevat la “i” i la tercera “/”, *ldap://192.168.10.1***

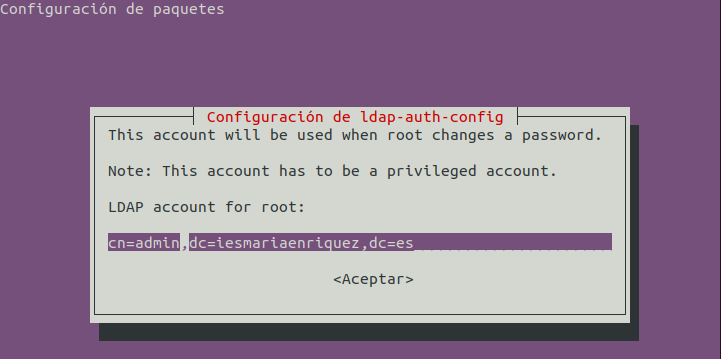


A les següent 3 pantalles deixarem les opcions per defecte:

**LDAP version:** 3

**Make local root Database admin:** Si

**Does the LDAP database require login?** No



LDAP root account password: laContrasenya

La configuració que acabem de fer s'emmagatzema en el fitxer **/etc/ldap.conf** el qual podem modificar manualment**.** Aquest s'utilitza tant pel servei d'autenticació **PAM** com pel servei de noms **NSS (Name Service Switch).** Si posteriorment tinguem que canviar aquesta configuració podem editar el fitxer o, més fàcilment, el reconfigurarem amb l’ordre **dpkg-reconfigure ldap-auth-config.**

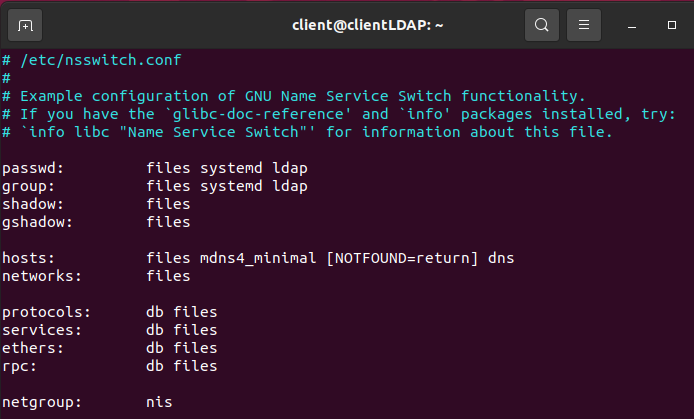
### Configuració de NSS

**Client**

Per a que el servidor LDAP actue com si es tractara dels arxius passwd, group i shadow, a més d’instal·lar les dos llibreries anteriors, hem d'indicar que s'utilitze LDAP com alternativa per a autenticar usuaris. Per a això modifiquem l'arxiu /etc/nsswitch.conf:

*sudo nano /etc/nsswitch.conf*

Únicament cal afegir ldap (no cal canviar compat per file systemd). Segons la versió del client en les línies de passwd, group i shadow posarà files, compat o files systemd. Els dos paràmetres signifiquen pràcticament el mateix.



El que estem configurant ací és que en primer lloc busque usuaris, grups i contrasenyes en els fitxers locals i si no els troba busque en LDAP. Respecte a les màquines (hosts) primer les busca en el fitxer local (/etc/hosts) i si no les troba pregunta al DNS.

Compte ací amb el detall, si afegim “ldap” com últim element tant de passwd i group, a l’hora de montar les carpetes, tindrà més prioritat els elements ja existents als usuaris (les carpetes locals de cada usuari del LDAP). Això ens pot portar problemes en el punt **“4.7 Configuració dels perfils mòbils”** quan canviem la ruta del directori de cada usuari.

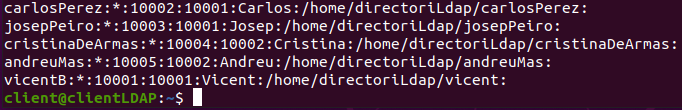
**Actualitzem els canvis reiniciant la màquina** o amb la següent ordre que caldria instal·lar prèviament:

*$ sudo nss\_updatedb ldap*

Podem fer una prova de que NSS està funcionant amb l'ordre ***getent:***

*$ getent passwd*

Aquesta ordre mostrarà per pantalla la informació d'usuaris continguda en l'arxiu */etc/passwd*. Si funciona NSS, a més de la llista d'usuaris locals, afegirà informació dels usuaris creats en el directori LDAP del servidor.



Podem consultar el *logs* del sistema referents a validació, */var/log/auth.log,* per comprovar i veure possibles problemes.

### Configuració de serveis PAM

**Client**

Ara el nostre Linux ja estaria preparat per a autenticar-se com a LDAP. Editant els fitxers que hi ha a la carpeta ***/etc/pam.d*** podem configurar la forma en que s’autentica cadascun dels serveis que requereixen autenticació.

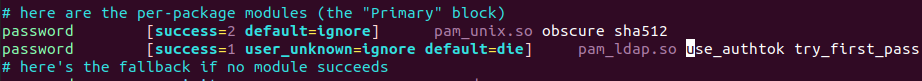
Per a no haver de fer-ho individualment, existeixen uns arxius el nom dels quals comença per “common” i que en molts d’aquests arxius hi fan referència mitjançant una línia @include

* /etc/pam.d/common-auth (per a autenticar-se)
* /etc/pam.d/common-account (per a disposar d’un compte)
* /etc/pam.d/common-session (per a poder iniciar sessió)
* /etc/pam.d/common-password (per a poder canviar la paraula de pas)

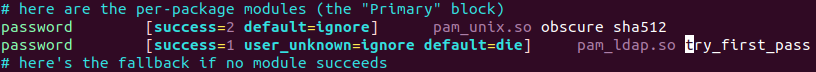
Aquest arxius contenen una línia que fa referència a la llibreria pam\_unix.so, que correspon a l’autenticació contra els arxius Linux (/etc/passwd, /etc/shadow,etc). Si ens fixem en la línia assenyalada en la captura, veiem que el nostre sistema empra primer les llibreries [pam\_ldap.so](http://pam_ldap.so/) per a autenticar els usuaris, i desprès les de Unix. Així, si la autenticació falla provarà amb els arxius Linux. Això ens anirà molt bé ja que permetrà validar-se amb usuaris “locals” en màquines que es puguen validar en serveis LDAP remots.

*$ sudo nano /etc/pam.d/common-password*

Anem a la línia 26 i esborrem***use\_authtok:***



I deu quedar així:



### Creació automàtica directoris d’usuari (home)

**Client**

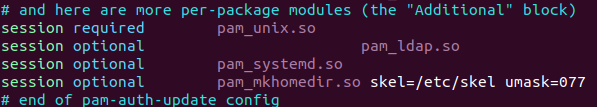
El mòdul [pam\_mkhomedir.so](http://pam_mkhomedir.so/) és el que permet crear el directori d’usuari. Umask ens indica amb quins permisos crearem el directori. Els permisos aplicats és el resultat de la resta de 777 - 022 = 755, on 022 és el valor especificat a umask; 755 correspon a rwx r-x r-x

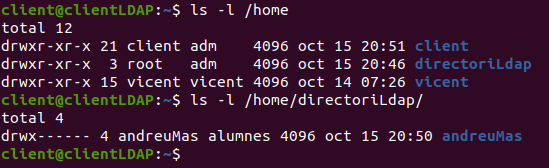
El paràmetre skel ens indica un directori, el contingut del qual, es copiarà al nou directori d’usuari; pots posar-hi el que vullgues, tot es copiarà al nou directori HOME creat.

*$ sudo nano /etc/pam.d/common-session*

Baix de ***session optional pam\_system.so*** posem:

“session optional pam\_mkhomedir.so skel=/etc/skel umask=077”



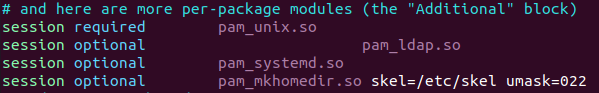


És una bona pràctica per introduir un fitxer de informació sobre els permisos, o que avise que estan utilitzant el servei LDAP, o el que necessitem.

Com hem ficat umask=077 els permisos que tindran per defecte els directoris /home/usuari seran rwx --- --- .

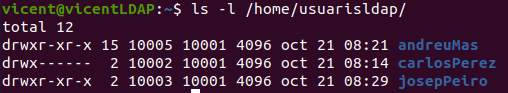
* client i vicent, son usuaris locals, la màscara per defecte és 022 (0022)
* andreuMas és un usuari LDAP, quan vam iniciar sessió per primera volta la màscara era 077

Si volem que els permisos per defecte dels nous directoris /home/usuari siga rwx r-x r-x (els permisos habituals per als nous usuaris a Linux), al fitxer hauríem de ficar umask=022. Per tant, ho deixarem així:



Perquè els permisos queden com cal, podem canviar-los manualment amb “chmod” o bé eliminar la carpeta de l’usuari (cosa que causarà que s’esborren totes les seues dades).

Com podeu vore, els usuaris andreuMas i josepPeiro s’han creat després d’haver fet el canvi del umask, en canvi, carlosPerez manté els permisos del umask antic, cal canviar-los per deixar-los com els d’un usuari comú.



Per finalitza la configuració i que s’apliquen els canvis del client, reiniciem la màquina:

*$ reboot*

Si volem mostrar tots els usuaris dels llocs indicats a *nsswitch.conf*: "compat/files" i "ldap" farem:

*$ getent passwd*

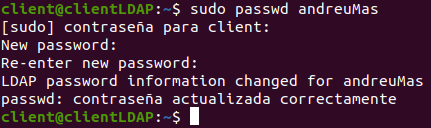
## Comprovació de la configuració

**Client**

Com a part final comprovarem que tot ens funciona correctament. No ho farà a la primera, ja que és fàcil que ens deixem o ens equivoquem en alguna cosa.

Els usuaris que vàrem crear anteriorment encara no tenen contrasenya. Per tant executarem l’ordre “passwd usuari” per a modificar el seu password:

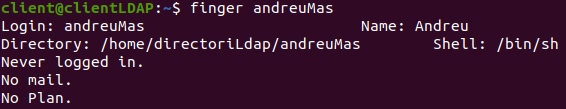
*$ sudo passwd cmateu*



Si aquest pas no dona problemes ja anem pel bon camí. Com que la nostra màquina local no té l’usuari “cmateu” a l’arxiu /etc/passwd, està clar que ldap està intervenint.

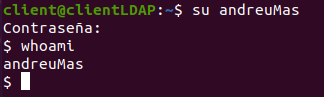
També podem comprovar si l’usuari existeix amb l’ordre ***finger*** que caldria instal·lar prèviament:

*$ finger cmateu*



Podem provar a fer l’autenticació directament sobre la consola amb “su”

*$ su cmateu*



Compte, l’autenticació solament funcionarà mitjançant el terminal (o un altre escriptori tty del S.O.), no amb entorn gràfic, això ho veurem més avant.

## Configuració per iniciar sessió en entorn gràfic

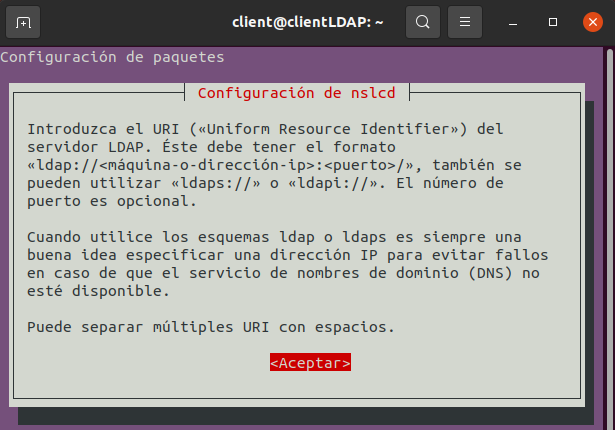
**Client**

Partint que ja tenim el servei funcionant i que des del client podem iniciar sessió mitjançant el terminal, solament ens queda configurar l’inici de sessió amb GUI (entorn gràfic), aquest pas es fa al final de tot el procediment perquè detecte automàticament la configuració del servei slapd.

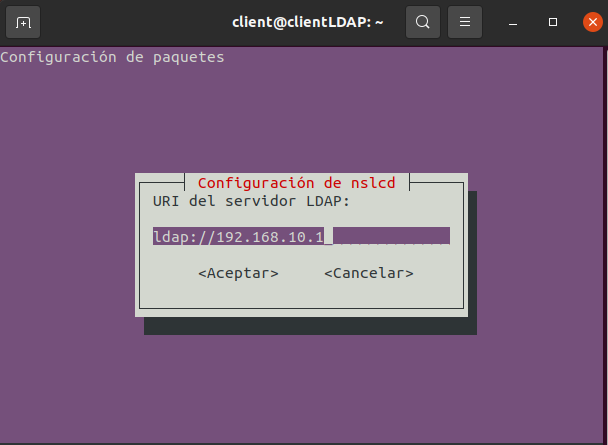
Nomes cal instal·lar el paquet **nslcd**

*$ sudo apt install nslcd*

Este ens mostrarà un assistent d'instal·lació similar als paquets del punt 4.3 libpam-ldap i libnss-ldap, al qual hem de seguir els passos i automàticament s’activarà l’accés mitjançant l’entorn gràfic.



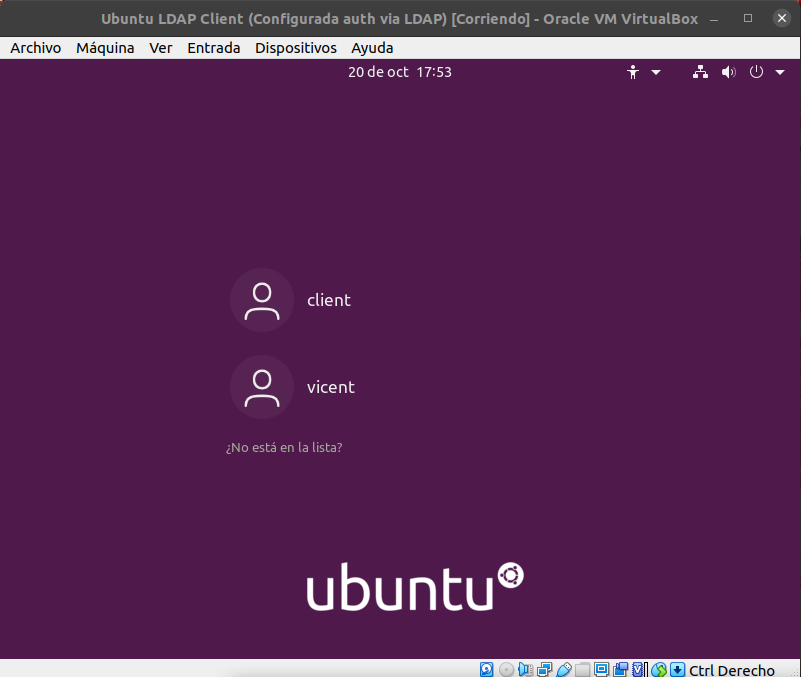
Si tota la configuració que hem introduït a la configuració del client als punts anteriors és correcta, els camps ens apareixen autocompletats, només cal revisar que les dades siguen les correctes i seguir el assistent.



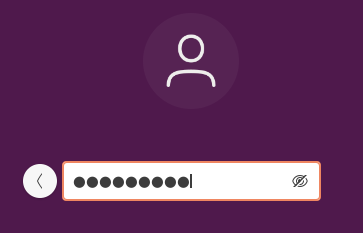
# 

Una vegada instal·lat només cal reiniciar la màquina perquè s’apliquen els canvis i intentar accedir des del menú “log in”, mitjançant l’opció “No està a la llista?”:

COMPTE: Si mai s’ha fet “login” a l’usuari que aneu a provar, reviseu que apareix per pantalla el procés de creació del directori.



Introduïm les dades manualment:



Això farà el procés de login i si tot està correcte ens mostrarà l’escriptori final de l’usuari mitjançant l'autenticació per LDAP.

# 5. Configuració dels perfils mòbils

Ja tenim configurat el directori LDAP de manera que des de qualsevol client puc iniciar sessió amb qualsevol usuari del directori. Però, la seua carpeta personal (que inclou el seu perfil i les seues dades) es crea en cada màquina client, la qual cosa és un problema si l'usuari no té un únic ordinador client assignat (cosa que passa normalment a les aules).

El que anem a preparar és coneix com perfils mòbils, i el que implica és que els usuaris tindran tots els seus fitxers estiguen a la màquina que estiguen.

**Servidor**

Per fer això, el següent pas és fer la configuració perquè les carpetes personals dels usuaris mòbils s'allotgen en el servidor directament i es munten automàticament en els clients al iniciar sessió. Els passos a fer són:

* + Crear una carpeta en el servidor on emmagatzemar els homes dels usuaris mòbils i compartir-la amb NFS (Network File System) amb permisos de lectura i escriptura per a tots els clients. Aquesta carpeta potser el /home (però estarem exportant també les carpetes dels *usuaris locals* del servidor i això no ens interessa) o qualsevol altra, per exemple, **/home/usuarisldap**
  + Compartir el directori que conté els directoris personals dels clients mòbils, mitjançant el servei NFS, per això cal instal·lar el paquet NFS:

*$ sudo apt install nfs-kernel-server*

Una vegada fet això, cal afegir que es compartisca en xarxa el directori “/home/usuarisldap” amb el servei NFS, per tant, modifiquem el fitxer **/etc/exports** i cal afegir la següent línia:

*/home/usuarisldap \*(rw,sync,no\_root\_squash,no\_subtree\_check)*

La qual aplica els permisos de escritura i lectura, la sincronització de fitxers, que l’usuari root del client puga muntar com a root en el directori compartit i desactiva que es revise els fitxers exportats des de l’altra màquina (per evitar problemes a la sincronització).

I reiniciem la màquina del servidor, la part del servidor ja la tenim preparada.

**\* Si voleu més informació sobre nfs i exports:**

**https://www.digitalocean.com/community/tutorials/how-to-set-up-an-nfs-mount-on-ubuntu-20-04-es**

**( No obstant el NFS el vorem més avant )**

**Client**

Ara anem a treballar amb el client, cal crear una carpeta que contindrà els continguts que es guarden de cada usuari al serverLDAP.

Per fer-ho fàcil, anem a crearla a la mateixa ubicació “/home/usuarisldap” i li donem permisos complets al directori “chmod 777” el que ve a ser “drwxrwxrwx”.

Fet això, anem a montar mitjançant el fitxer “/etc/fstab”, que la carpeta ubicada al servidor es muntarà de forma automàtica en el arranc del sistema al nostre directori local.

Cal **instal·lar el paquet “nfs-common”** perquè el fstab monte correctament el directori allotjat al servidor, si no, voreu com no funciona, accedireu a /home/usuarisldap i dins sols tindreu els documents locals (no cap).

Per tant, com que tenim el servidor amb la IP: 192.168.10.1 i la carpeta està ubicada a /home/usuarisldap, anem a afegir la següent línia al fitxer /etc/fstab on bàsicament indiquem que la carpeta “/home/usuarisldap” de l’equip remot amb IP 192.168.10.1, es muntarà a la carpeta local “/home/usuarisldap”:

*192.168.10.1:/home/usuarisldap /home/usuarisldap nfs auto,noatime,nolock,bg,nfsvers=3, intr,tcp,actimeo=1800 0 0*

Quedaria així:



I per últim, cal que actualitzem a cadascun dels usuaris, la ruta del seu propi directori perquè coincidisca amb la carpeta mòbil. Per això, podem fer-ho fàcilment amb l’entorn gràfic, però és un procés lent anar d’un en un.

On tindriem:



Ho canviem i indiquem el nou directori:



**QÜESTIÓ:** Una millora que podriem implementar és preparar un script que mitjançant l’ordre “ladpmodify” vaja d’un en un fent aquest canvi. I també moga el contingut de cadascun del directoris personals dels usuaris de l’antic directori al sincronitzat amb el servidor.

**QÜESTIÓ:** Cal crear manualment la carpeta de cada usuari i fer tot eixe procés o podríem fer que es cree automàticament la primera vegada que es logeja en un equip client?

Si no creem la carpeta manualment, quan iniciem sessió esta es crea automàticament, agafa la configuració de permisos únics per l’usuari (755), els permisos basats en el “umask” que vam indicar en el fitxer que hem vist anteriorment (/etc/pam.d/common-session).

El propietari i grup l’agafa automàticament de la configuració de l’usuari al servidor LDAP. Com que no estem movent les dades de “/home/directoriLdap” (local) a “/home/usuarisldap” (NFS) totes les dades que tenia localment eixe usuari no li apareixeran. Cal moure-les si volem preservar-les. Igualment, els fitxers ubicats a “/etc/skel” també es mouran quan es crea el nou directori de forma automàtica.

**Quan el sistema detecta 2 “homeDirectory” per a un mateix usuari, agafarà el directori més antic ( que és el local ).**

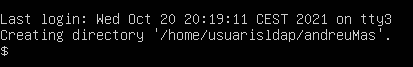
**Dos solucions:**

1. **Modificar en el fitxer “nsswitch.conf” l’ordre en que “passwd” i “group” revisarà els comptes d’usuari. Actualment l’ordre és “files” -> “systemd” -> “ldap”, caldria canviar-lo per “ldap” -> “files” -> “systemd”**

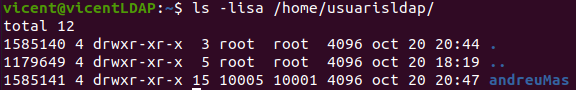
**Reiniciar la màquina perquè agafe les últimes dades actualitzades del servidor LDAP.**

1. **Eliminar el directori local (/home/directoriLdap) perquè LDAP funcione correctament.**

Finalment, per verificar que tot està funcionant correctament, deuríem de revisar fent “login” mitjançant un escriptori secundari de ubuntu (“tty3” per exemple) i revisant que quan iniciem sessió, crea automàticament la carpeta que està al servidor. Exemple de andreuMas que no tenia cap directori antic:



I si fem “login” i executem un “ls”:



Des d’este moment tot el que creem amb eixe usuari, realment està guardant-se al servidor, i es connecte des del client que es connecte tindrà exactament el mateix.

**COMPTE: Perquè açò funcione quan el client arranque el servidor deu estar encés si no, fallarà el muntatge del directori NFS.**

Enllaços d’interés

* <http://www.yolinux.com/TUTORIALS/LinuxTutorialLDAP-DefineObjectsAndAttributes.html>
* [http://www.linuxquestions.org/questions/linux-server-73/how-to-add-a-new-schema-to-openldap-2-4-11-a-700452](http://www.linuxquestions.org/questions/linux-server-73/how-to-add-a-new-schema-to-openldap-2-4-11-a-700452/)
* <http://linuxgazette.net/130/peterson.html>
* <http://www.ite.educacion.es/formacion/materiales/85/cd/REDES_LINUX/openldap/Autentificacion_del_sistema_con_OpenLDAP.html>

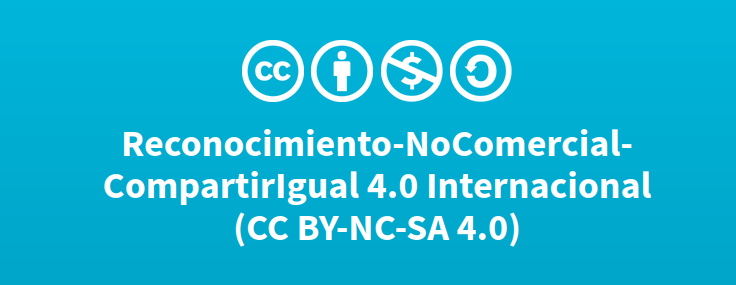
# Bibliografia

Temari original baix llicència Creative Commons Reconeixement-NoComercial-CompartirIgual 4.0 Internacional:

Armand Mata (INS Joaquim Mir)

Javier Martínez (IES María Enríquez)

Vicent Benavent



Modificacions per Vicent Benavent i Sentandreu:

-Actualitzat el procediment d’instal·lació a l’última versió d’Ubuntu 20.04  
-Actualitzades les captures de pantalla dels procediments i la ferramenta JXplorer  
-Adaptat i actualitzat el mòdul 4.6 (LDAP mitjançant l’entorn gràfic) de l’antiga versió a Ubuntu 20.04 amb les noves ferramentes i necessitats

- Afegit el mòdul 4.7 (Perfils mòbils), per a l’última versió Ubuntu 20.04, junt amb els paquets necessaris per a muntar el sistema NFS tant al client com al servidor