Servidor LDAP

Índex

Cicle formatiu: CFGM Sistemes Microinformàtics i Xarxes (SMX) / CFGS Administració de Sistemes Informàtics en Xarxa (ASIX)

Mòdul: 0224 -- Sistemes operatius en xarxa / 0374 - Administració de sistemes operatius

Entorn: Ubuntu Server 26.04 LTS

1. Introducció

LDAP (*Lightweight Directory Access Protocol*) és un protocol de xarxa que permet accedir i mantenir serveis de directori distribuïts. S'utilitza habitualment per centralitzar l'autenticació d'usuaris en entorns corporatius i educatius.

OpenLDAP és la implementació lliure i de codi obert més estesa del protocol LDAP, i és la que s'instal·la en aquest document.

Figura 1: OpenLDAP Logo

Casos d'ús habituals

- Autenticació centralitzada d'usuaris en servidors Linux
- Integració amb Samba per a entorns Windows/Linux mixtos
- Directori d'adreces corporatiu
- Base d'autenticació per a serveis web (Apache, Nginx, aplicacions)
- Backend per a servidors de correu (Postfix, Dovecot)

Escenari del document

Rol	Hostname	IP	Sistema
Servidor LDAP	`ldapserver`	`192.168.1.10`	Ubuntu Server 26.04
Client LDAP	`ldapclient`	`192.168.1.20`	Ubuntu Desktop 26.04
Domini LDAP	`dc=thos,dc=local`	---	---
Administrador	`cn=admin,dc=thos,dc=local`	---	---

NOTA

Adapta les IP, el hostname i el domini al teu entorn real.

2. Conceptes previs

2.1. Terminologia LDAP

Terme	Significat
DN (*Distinguished Name*)	Identificador únic d'una entrada al directori. Ex: `cn=Joan,ou=Usuaris,dc=thos,dc=local`
RDN (*Relative Distinguished Name*)	Part del DN que identifica l'entrada dins del seu contenidor. Ex: `cn=Joan`
DC (*Domain Component*)	Component del domini. Ex: `dc=thos,dc=local`
CN (*Common Name*)	Nom comú d'un objecte. Ex: `cn=admin`
OU (*Organizational Unit*)	Unitat organitzativa (contenidor). Ex: `ou=Usuaris`
UID (*User ID*)	Identificador d'usuari. Ex: `uid=joan`
DIT (*Directory Information Tree*)	Arbre jeràrquic que conté totes les entrades del directori
Schema	Defineix els tipus d'objectes i atributs permesos al directori
objectClass	Atribut que defineix el tipus d'entrada (persona, grup, unitat org.)

2.2. Estructura jeràrquica (DIT)

```
dc=thos,dc=local                    ← Arrel (base DN)
├── cn=admin                        ← Administrador
├── ou=Usuaris                      ← Unitat organitzativa
│   ├── uid=joan
│   ├── uid=maria
│   └── uid=pere
├── ou=Grups                        ← Unitat organitzativa
│   ├── cn=professors
│   └── cn=alumnes
└── ou=Serveis                      ← Unitat organitzativa
    └── cn=mailserver
```

2.3. Format LDIF

LDIF (*LDAP Data Interchange Format*) és el format de fitxer estàndard per importar i exportar entrades LDAP.

```
# Exemple d'entrada LDIF per a un usuari
dn: uid=joan,ou=Usuaris,dc=thos,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: joan
cn: Joan Garcia
sn: Garcia
givenName: Joan
mail: joan@thos.local
uidNumber: 1001
gidNumber: 1001
```

```
homeDirectory: /home/joan
loginShell: /bin/bash
userPassword: {SSHA}...
```

3. Instal·lació d'OpenLDAP

3.1. Preparació del sistema

Actualitza la llista de paquets:

```
sudo apt update
```

Actualitza el sistema:

```
sudo apt upgrade
```

Configura el hostname:

```
sudo hostnamectl set-hostname ldapserver
```

Afegeix l'entrada al fitxer `/etc/hosts`:

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

Afegeix aquesta línia:

```
192.168.1.10    ldapserver.thos.local    ldapserver
```

Comprova:

```
hostname -f
```

Resposta esperada:

```
ldapserver.thos.local
```

3.2. Instal·lació dels paquets

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

Durant la instal·lació, el sistema demanarà la **contrasenya de l'administrador LDAP**. Introdueix-la i confirma-la.

Figura 2: Contrasenya d'administrador

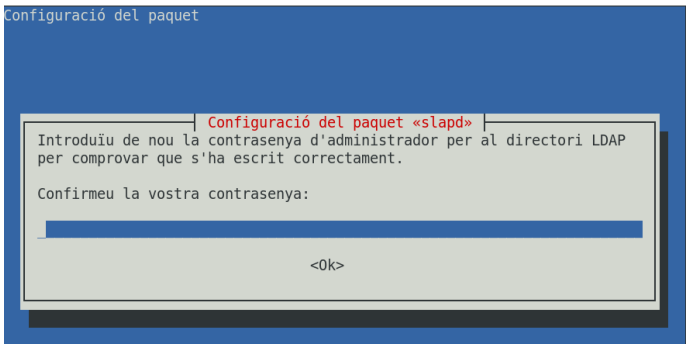


Figura 3: Confirma la contrasenya

IMPORTANT

Recorda aquesta contrasenya; és la de `cn=admin,dc=thos,dc=local`.

3.3. Reconfiguració interactiva

Si necessites reconfigurar el servei (canviar domini, contrasenya, etc.):

```
sudo dpkg-reconfigure slapd
```

El procés farà les preguntes següents:

Pregunta	Resposta recomanada
Ometre la configuració d'OpenLDAP?	**No**
Nom DNS del domini	`thos.local`
Nom de l'organització	`thos` (o el nom real)
Contrasenya de l'administrador	(la que triïs)
Motor de base de dades	**MDB** (recomanat)
Eliminar la base de dades en purgar slapd?	**No**
Moure la base de dades antiga?	**Sí**

3.4. Verificació de la instal·lació

Comprova que el servei està actiu:

```
sudo systemctl status slapd
```

Resposta esperada:

```
● slapd.service - OpenLDAP Server Daemon
     Loaded: loaded (/usr/lib/systemd/system/slapd.service; enabled;
 ↪  preset: enabled)
     Active: active (running) since Mon 2026-07-06 15:53:54 UTC; 28s
 ↪  ago
 Invocation: 57ac00e16e414f498cf382efec19c85f
       Docs: man:slapd
             man:slapd-config
             man:slapd-mdb
   Main PID: 17415 (slapd)
      Tasks: 3 (limit: 1885)
     Memory: 3M (peak: 3.4M)
        CPU: 15ms
     CGroup: /system.slice/slapd.service
             └─17415 /usr/sbin/slapd -d0 -h "ldap:/// ldapi:///" -u
 ↪  openldap -g openldap

de jul. 06 15:53:54 ldapserver systemd[1]: Starting slapd.service -
 ↪  OpenLDAP Server Daemon...
de jul. 06 15:53:54 ldapserver slapd[17415]: @(#) $OpenLDAP: slapd
 ↪  2.6.10+dfsg-1ubuntu5 (Nov 24 2025 11:17:55) $
```

```
                                                    Ubuntu Developers
 ↪  <ubuntu-devel-discuss@lists.ubuntu.com>
de jul. 06 15:53:54 ldapserver slapd[17415]: slapd starting
de jul. 06 15:53:54 ldapserver systemd[1]: Started slapd.service -
 ↪  OpenLDAP Server Daemon.
```

Comprova que escolta al port 389:

```
sudo ss -tlnp | grep slapd
```

Resposta esperada:

```
LISTEN 0      2048         0.0.0.0:389       0.0.0.0:*
 ↪  users:(("slapd",pid=17415,fd=7))
LISTEN 0      2048            [::]:389          [::]:*
 ↪  users:(("slapd",pid=17415,fd=8))
```

Prova de connexió bàsica (sense autenticació):

```
ldapsearch -x -b "dc=thos,dc=local" -H ldap://localhost
```

Resposta esperada:

```
# extended LDIF
#
# LDAPv3
# base <dc=thos,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# thos.local
dn: dc=thos,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: thos.local
dc: thos

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Prova amb autenticació d'administrador:

```
ldapsearch -x -D "cn=admin,dc=thos,dc=local" -W -b "dc=thos,dc=local"
```

La resposta ha de mostrar l'entrada arrel del directori.

Resposta esperada:

```
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <dc=thos,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# thos.local
dn: dc=thos,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: thos.local
dc: thos

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

4. Configuració bàsica del servidor

OpenLDAP a Ubuntu 26.04 utilitza el sistema de configuració dinàmica **cn=config** (OLC --- *On-Line Configuration*), que substitueix el fitxer `slapd.conf` tradicional.

4.1. Consulta la configuració actual

Veure tota la configuració (requereix sudo):

```
sudo ldapsearch -Y EXTERNAL -H ldapi:/// -b "cn=config"
```

Veure els paràmetres del servidor:

```
sudo ldapsearch -Y EXTERNAL -H ldapi:/// -b "cn=config"
 ↪  "(objectClass=olcGlobal)"
```

Veure la base de dades configurada:

```
sudo ldapsearch -Y EXTERNAL -H ldapi:/// -b "cn=config"
 ↪  "(objectClass=olcDatabaseConfig)"
```

4.2. Activa el log del servidor

Crea el fitxer `log.ldif`:

```
sudo nano log.ldif
```

```
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: stats
```

Aplica'l:

```
sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f log.ldif
```

Nivells de log disponibles:

Nivell	Valor	Descripció
`none`	0	Sense log
`stats`	256	Estadístiques de connexions (recomanat en producció)
`filter`	32	Filtres de cerca
`acl`	128	Comprovacions ACL
`any`	-1	Tot (només per depurar)

Configura `rsyslog` per separar els logs de LDAP:

```
sudo nano /etc/rsyslog.d/10-slapd.conf
```

```
local4.*    /var/log/slapd.log
```

Reinicia syslog:

```
sudo systemctl restart rsyslog
```

Reinicia ldap:

```
sudo systemctl restart slapd
```

4.3. Afegeix índexs per millorar el rendiment

```
sudo nano index.ldif
```

```
# fitxer: index.ldif
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcDbIndex
olcDbIndex: objectClass eq
olcDbIndex: uid eq,pres,sub
olcDbIndex: cn eq,pres,sub
olcDbIndex: sn eq,pres,sub
olcDbIndex: mail eq,pres,sub
olcDbIndex: memberUid eq
```

```
sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f index.ldif
```

5. Estructura del directori (DIT)

5.1. Crea les unitats organitzatives bàsiques

Crea el fitxer `estructura.ldif`:

```
sudo nano estructura.ldif
```

```
# Unitat organitzativa: Usuaris
dn: ou=Usuaris,dc=thos,dc=local
objectClass: organizationalUnit
ou: Usuaris
description: Usuaris del sistema

# Unitat organitzativa: Grups
dn: ou=Grups,dc=thos,dc=local
objectClass: organizationalUnit
ou: Grups
description: Grups del sistema
```

Importa l'estructura:

```
ldapadd -x -D "cn=admin,dc=thos,dc=local" -W -f estructura.ldif
```

Resposta esperada:

```
Enter LDAP Password:
adding new entry "ou=Usuaris,dc=thos,dc=local"
```

```
adding new entry "ou=Grups,dc=thos,dc=local"
```

Verifica:

```
ldapsearch -x -b "dc=thos,dc=local" -H ldap://localhost
 ↪  "(objectClass=organizationalUnit)"
```

Resposta esperada:

```
# extended LDIF
#
# LDAPv3
# base <dc=thos,dc=local> with scope subtree
# filter: (objectClass=organizationalUnit)
# requesting: ALL
#

# Usuaris, thos.local
dn: ou=Usuaris,dc=thos,dc=local
objectClass: organizationalUnit
ou: Usuaris
description: Usuaris del sistema

# Grups, thos.local
dn: ou=Grups,dc=thos,dc=local
objectClass: organizationalUnit
ou: Grups
description: Grups del sistema

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

5.2. Crea usuaris

Primer, genera un hash de contrasenya:

```
slappasswd
# Introdueix la contrasenya i et retornarà el hash {SSHA}...
```

Resposta esperada:

```
New password:
Re-enter new password:
{SSHA}TBIdrK2UoZVHk6h9bORCURCYz/3DccH2
```

Crea el fitxer `usuaris.ldif`:

```
sudo nano usuaris.ldif
```

```
# Usuari: Joan Garcia
dn: uid=joan,ou=Usuaris,dc=thos,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: joan
cn: Joan Garcia
sn: Garcia
givenName: Joan
displayName: Joan Garcia
mail: joan@thos.local
uidNumber: 10001
gidNumber: 10001
homeDirectory: /home/joan
loginShell: /bin/bash
userPassword: {SSHA}XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

# Usuari: Maria Puig
dn: uid=maria,ou=Usuaris,dc=thos,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: maria
cn: Maria Puig
sn: Puig
givenName: Maria
displayName: Maria Puig
mail: maria@thos.local
uidNumber: 10002
gidNumber: 10001
homeDirectory: /home/maria
loginShell: /bin/bash
userPassword: {SSHA}XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

IMPORTANT

Substitueix `{SSHA}XXXXX...` pel hash generat amb `slappasswd`.

```
ldapadd -x -D "cn=admin,dc=thos,dc=local" -W -f usuaris.ldif
```

Resposta esperada:

```
Enter LDAP Password:
adding new entry "uid=joan,ou=Usuaris,dc=thos,dc=local"

adding new entry "uid=maria,ou=Usuaris,dc=thos,dc=local"
```

5.3. Crea grups

Crea el fitxer `grups.ldif`:

```
sudo nano grups.ldif
```

```
# Grup: professors
dn: cn=professors,ou=Grups,dc=thos,dc=local
objectClass: posixGroup
cn: professors
gidNumber: 10001
memberUid: joan
memberUid: maria

# Grup: alumnes
dn: cn=alumnes,ou=Grups,dc=thos,dc=local
objectClass: posixGroup
cn: alumnes
gidNumber: 10002
```

```
ldapadd -x -D "cn=admin,dc=thos,dc=local" -W -f grups.ldif
```

Resposta esperada:

```
Enter LDAP Password:
adding new entry "cn=professors,ou=Grups,dc=thos,dc=local"

adding new entry "cn=alumnes,ou=Grups,dc=thos,dc=local"
```

6. Gestió d'entrades amb ldapadd i ldapmodify

6.1. Eines de línia d'ordres

Ordre	Funció
`ldapsearch`	Cerca entrades al directori
`ldapadd`	Afegeix entrades noves
`ldapmodify`	Modifica entrades existents
`ldapdelete`	Elimina entrades
`ldappasswd`	Canvia contrasenyes
`slappasswd`	Genera hash de contrasenya

6.2. Cerques amb ldapsearch

Cerca tots els usuaris

```
ldapsearch -x -b "ou=Usuaris,dc=thos,dc=local"
 ↪  "(objectClass=posixAccount)"
```

Cerca un usuari per uid

```
ldapsearch -x -b "dc=thos,dc=local" "(uid=joan)"
```

Cerca per nom parcial (comodí)

```
ldapsearch -x -b "dc=thos,dc=local" "(cn=Joan*)"
```

Mostra només atributs específics

```
ldapsearch -x -b "dc=thos,dc=local" "(objectClass=posixAccount)" uid
 ↪  cn mail
```

Cerca tots els membres d'un grup

```
ldapsearch -x -b "ou=Grups,dc=thos,dc=local" "(cn=professors)"
 ↪  memberUid
```

Autenticació amb l'usuari administrador

```
ldapsearch -x -D "cn=admin,dc=thos,dc=local" -W -b "dc=thos,dc=local"
```

6.3. Modifica entrades amb ldapmodify

Per modificar atributs, crea un fitxer LDIF amb el tipus de canvi:

```
sudo nano canvis.ldif
```

```
# Canvia el correu d'un usuari (replace)
dn: uid=joan,ou=Usuaris,dc=thos,dc=local
changetype: modify
replace: mail
mail: joan.garcia@thos.local

# Afegeix un atribut nou (add)
dn: uid=joan,ou=Usuaris,dc=thos,dc=local
changetype: modify
add: telephoneNumber
telephoneNumber: +34 93 000 0001

# Elimina un atribut (delete)
dn: uid=joan,ou=Usuaris,dc=thos,dc=local
changetype: modify
delete: telephoneNumber
```

```
ldapmodify -x -D "cn=admin,dc=thos,dc=local" -W -f canvis.ldif
```

Resposta esperada:

```
Enter LDAP Password:
modifying entry "uid=joan,ou=Usuaris,dc=thos,dc=local"

modifying entry "uid=joan,ou=Usuaris,dc=thos,dc=local"

modifying entry "uid=joan,ou=Usuaris,dc=thos,dc=local"
```

6.4. Canvia contrasenyes

Canvia la contrasenya d'un usuari (com a administrador)

```
ldappasswd -x -D "cn=admin,dc=thos,dc=local" -W -s novacontrasenya \
  "uid=joan,ou=Usuaris,dc=thos,dc=local"
```

L'usuari canvia la seva pròpia contrasenya

```
ldappasswd -x -D "uid=joan,ou=Usuaris,dc=thos,dc=local" -W -s
 ↪  novacontrasenya
```

6.5. Elimina entrades

Elimina un usuari

```
ldapdelete -x -D "cn=admin,dc=thos,dc=local" -W \
  "uid=joan,ou=Usuaris,dc=thos,dc=local"
```

Elimina una OU (ha d'estar buida)

```
ldapdelete -x -D "cn=admin,dc=thos,dc=local" -W \
  "ou=Temporal,dc=thos,dc=local"
```

6.6. Exporta i importa el directori complet

Exporta tot el directori a LDIF

```
sudo slapcat -v -l backup_ldap.ldif
```

Importa (amb slapd aturat)

Atura

```
sudo systemctl stop slapd
```

Importa

```
sudo slapadd -v -l backup_ldap.ldif
```

Engega

```
sudo systemctl start slapd
```

7. Autenticació d'usuaris Linux via LDAP

Configura el **client LDAP** (`192.168.1.20`) perquè els usuaris LDAP puguin iniciar sessió al sistema.

7.1. Configuració del fitxer `/etc/hosts`

Edita el fitxer `/etc/hosts`. Afegeix el servidor LDAP:

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

```
192.168.1.10 ldapserver.thos.local ldapserver
```

Comprova connectivitat i que el servidor respon:

```
ldapsearch -x -H ldap://ldapserver.thos.local -b "dc=thos,dc=local"
 ↪  -s base
```

Resposta esperada:

```
# extended LDIF
#
# LDAPv3
# base <dc=thos,dc=local> with scope baseObject
# filter: (objectclass=*)
# requesting: ALL
#

# thos.local
dn: dc=thos,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: thos.local
dc: thos

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
ramon@client:~$
```

7.2. Configuració del fitxer `/etc/sssd/sssd.conf`

```
sudo nano /etc/sssd/sssd.conf
```

Contingut bàsic:

```
[sssd]
services = nss, pam
domains = thos.local

[domain/thos.local]
id_provider = ldap
auth_provider = ldap
ldap_uri = ldap://ldapserver.thos.local
ldap_search_base = dc=thos,dc=local
ldap_id_use_start_tls = false
ldap_auth_disable_tls_never_use_in_production = true
lookup_family_order = ipv4_first
```

Canvia el propietari

```
sudo chown root:root /etc/sssd/sssd.conf
```

Canvia els permisos (SSSD es nega a arrencar si no són correctes):

```
sudo chmod 600 /etc/sssd/sssd.conf
```

7.3. Configuració de PAM

Activa la creació automàtica del home directory

```
sudo pam-auth-update --enable mkhomedir
```

Això afegeix `pam_mkhomedir.so` a la pila PAM perquè es creï `/home/usuari` automàticament al primer login si l'usuari existeix a LDAP però no localment.

7.4. Reinicia el servei SSSD

Reinicia SSSD

```
sudo systemctl restart sssd
```

Habilita SSSD en l'inici

```
sudo systemctl enable sssd
```

7.5. Verifica l'inici de sessió amb un usuari

Prova que funciona

```
getent passwd joan
```

Resposta esperada:

```
joan:*:10001:10001:Joan Garcia:/home/joan:/bin/bash
```

```
id joan
```

Resposta esperada:

```
uid=10001(joan) gid=10001(professors) groups=10001(professors)
```

Si retorna informació de l'usuari LDAP, NSS ja el troba. Per provar l'autenticació completa:

```
su - joan
```

Resposta esperada:

```
Contrasenya:
Creant el directori '/home/joan'.
joan@client:~$
```

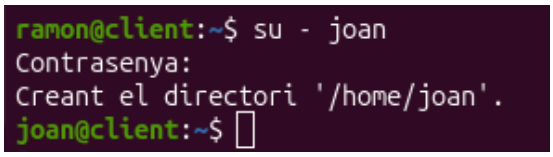


Figura 4: Inici de sessió

8. Seguretat: TLS/SSL

Per defecte, LDAP transmet les dades en text pla. És **imprescindible** activar TLS en entorns de producció.

8.1. Genera certificats autosignats

Crea el directori per als certificats

```
sudo mkdir -p /etc/ldap/certs
```

Mou-te al directori creat

```
cd /etc/ldap/certs
```

Genera la clau privada i el certificat de la CA

```
sudo openssl req -new -x509 -nodes -out ca.crt -keyout ca.key -days
 ↪  3650 \
  -subj "/C=ES/ST=Catalunya/L=Mataro/O=THOS/CN=CA-LDAP"
```

Genera la clau del servidor

```
sudo openssl genrsa -out ldapserver.key 4096
```

Genera la petició de certificat (CSR)

```
sudo openssl req -new -key ldapserver.key -out ldapserver.csr \
  -subj "/C=ES/ST=Catalunya/L=Mataro/O=THOS/CN=ldapserver.thos.local"
```

Signa el certificat amb la CA

```
sudo openssl x509 -req -in ldapserver.csr -CA ca.crt -CAkey ca.key \
  -CAcreateserial -out ldapserver.crt -days 3650
```

Canvia el propietari

```
sudo chown openldap:openldap /etc/ldap/certs/*.key
```

Ajusta permisos

```
sudo chmod 640 /etc/ldap/certs/*.key
```

Torna al teu home

```
cd
```

8.2. Configura TLS a OpenLDAP

Crea el fitxer `tls.ldif`:

```
sudo nano tls.ldif
```

```
dn: cn=config
changetype: modify
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ldap/certs/ca.crt
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ldap/certs/ldapserver.crt
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ldap/certs/ldapserver.key
-
add: olcTLSVerifyClient
olcTLSVerifyClient: never
```

```
sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f tls.ldif
```

Resposta esperada:

```
SASL/EXTERNAL authentication started
SASL username:
 ↪  gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"
```

8.3. Activa LDAPS (port 636)

Edita la configuració del servei:

```
sudo nano -l /etc/default/slapd
```

Modifica la variable `SLAPD_SERVICES` (línia 24):

```
SLAPD_SERVICES="ldap:/// ldapi:/// ldaps:///"
```

```
sudo systemctl restart slapd
```

Verifica que escolta al port 636

```
sudo ss -tlnp | grep slapd
```

Resposta esperada:

```
LISTEN 0      2048         0.0.0.0:636       0.0.0.0:*
 ↪  users:(("slapd",pid=3356,fd=10))
LISTEN 0      2048         0.0.0.0:389       0.0.0.0:*
 ↪  users:(("slapd",pid=3356,fd=7))
LISTEN 0      2048            [::]:636          [::]:*
 ↪  users:(("slapd",pid=3356,fd=11))
LISTEN 0      2048            [::]:389          [::]:*
 ↪  users:(("slapd",pid=3356,fd=8))
```

9. Autenticació d'usuaris Linux via LDAP amb TLS/SSL

Configura el **client LDAP** (`192.168.1.20`) perquè els usuaris LDAP puguin iniciar sessió al sistema.

9.1. Configuració del fitxer `/etc/hosts`

Edita el fitxer `/etc/hosts`. Afegeix el servidor LDAP:

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

```
192.168.1.10 ldapserver.thos.local ldapserver
```

Comprova connectivitat i que el servidor respon:

```
ldapsearch -x -H ldap://ldapserver.thos.local -b "dc=thos,dc=local"
 ↪  -s base
```

Resposta esperada:

```
# extended LDIF
#
# LDAPv3
# base <dc=thos,dc=local> with scope baseObject
# filter: (objectclass=*)
# requesting: ALL
#

# thos.local
dn: dc=thos,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: thos.local
dc: thos

# search result
```

```
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
ramon@client:~$
```

9.2. Copia el certificat de la CA al client

Crea una carpeta per al certificat

```
sudo mkdir -p /etc/ssl/certs/thos-ca
```

Copia el certificat de la CA al client:

```
sudo scp ramon@ldapserver:/etc/ldap/certs/ca.crt
 ↪  /etc/ssl/certs/thos-ca/ca.crt
```

Prova la negociació TLS

```
openssl s_client -connect ldapserver:389 -starttls ldap -CAfile
 ↪  /etc/ssl/certs/thos-ca/ca.crt
```

```
openssl s_client -connect ldapserver:636 -CAfile
 ↪  /etc/ssl/certs/thos-ca/ca.crt
```

9.3. Modifica `/etc/sssd/sssd.conf` per fer servir TLS

```
sudo nano /etc/sssd/sssd.conf
```

```
[sssd]
services = nss, pam
domains = thos.local

[domain/thos.local]
id_provider = ldap
auth_provider = ldap
ldap_uri = ldap://ldapserver.thos.local
ldap_search_base = dc=thos,dc=local
ldap_id_use_start_tls = true
ldap_tls_reqcert = demand
ldap_tls_cacert = /etc/ssl/certs/thos-ca/ca.crt
lookup_family_order = ipv4_first
```

Canvia el propietari

```
sudo chown root:root /etc/sssd/sssd.conf
```

Canvia els permisos (SSSD es nega a arrencar si no són correctes):

```
sudo chmod 600 /etc/sssd/sssd.conf
```

9.4. Configuració de PAM

Activa la creació automàtica del home directory

```
sudo pam-auth-update --enable mkhomedir
```

Això afegeix `pam_mkhomedir.so` a la pila PAM perquè es creï `/home/usuari` automàticament al primer login si l'usuari existeix a LDAP però no localment. Reinicia el servei:

9.5 Reinicia el servei SSSD

```
sudo systemctl restart sssd
```

Habilita SSSD en l'inici

```
sudo systemctl enable sssd
```

9.6 Verifica l'inici de sessió amb un usuari

Prova que funciona

```
getent passwd joan
```

Resposta esperada:

```
joan:*:10001:10001:Joan Garcia:/home/joan:/bin/bash
```

```
id joan
```

Resposta esperada:

```
uid=10001(joan) gid=10001(professors) groups=10001(professors)
```

Si retorna informació de l'usuari LDAP, NSS ja el troba. Per provar l'autenticació completa:

```
su - joan
```

Resposta esperada:

```
Contrasenya:
joan@client:~$
```

10. Eines de gestió

10.1. Apache Directory Studio

Apache Directory Studio és una eina gràfica (GUI) per gestionar servidors LDAP, basada en Eclipse RCP. S'instal·la en una màquina de la xarxa amb GUI, no al servidor.

Funcionalitats

- **Navegar per l'arbre LDAP (DIT)**: veure entrades, atributs i la seva jerarquia de forma visual, en lloc d'anar fent `ldapsearch` per terminal.
- **Editar entrades**: crear, modificar o eliminar usuaris, grups, unitats organitzatives, etc. amb formularis, sense escriure LDIF a mà.
- **Importar/exportar LDIF**: molt útil per fer càrregues massives o backups de la teva base LDAP.
- **Executar cerques LDAP** amb filtres, de forma similar a `ldapsearch` però amb interfície visual i historial de cerques.
- **Gestionar schemas**: veure i editar les *objectClasses* i *attributeTypes* disponibles al servidor.
- **Connexions múltiples**: pots tenir definides connexions a diversos servidors (útil si tens `ldapserver.thos.local` i potser altres entorns de prova).

Instal·lació

Descàrrega des de https://directory.apache.org/studio/ la versió per a Linux (tar.gz)

```
wget -c
 ↪  https://dlcdn.apache.org/directory/studio/2.0.0.v20210717-M17/Ap
 ↪  acheDirectoryStudio-2.0.0.v20210717-M17-linux.gtk.x86_64.tar.gz
```

Descomprimeix

```
tar -zxvf
 ↪  ApacheDirectoryStudio-2.0.0.v20210717-M17-linux.gtk.x86_64.tar.gz
```

Si no tens un entorn d'execució Java (JRE) instal·la:

```
sudo apt install default-jre
```

Executa

```
ApacheDirectoryStudio/ApacheDirectoryStudio
```

Crea una nova connexió:

- **Host:** `ldapserver.thos.local` o `192.168.1.10`
- **Port:** 389 (o 636 per LDAPS)
- **Bind DN:** `cn=admin,dc=thos,dc=local`
- **Base DN:** `dc=thos,dc=local`

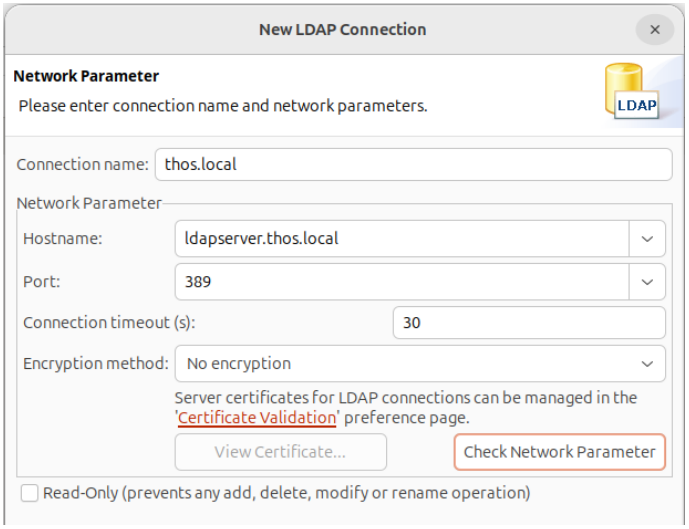


Figura 5: Paràmetres de xarxa

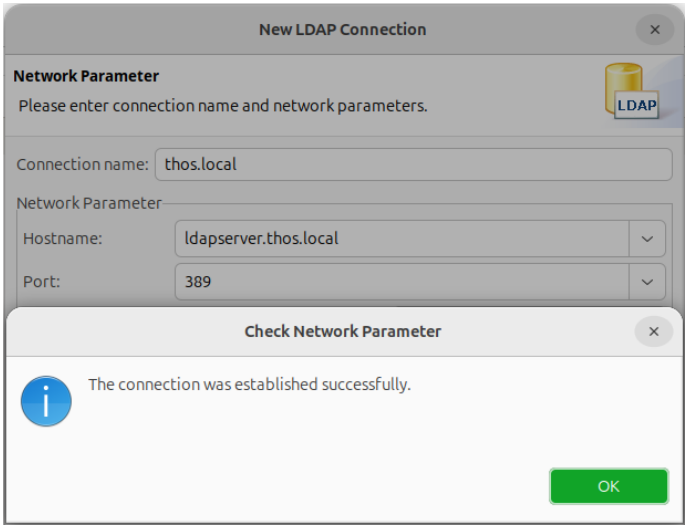


Figura 6: Comprova paràmetres de xarxa

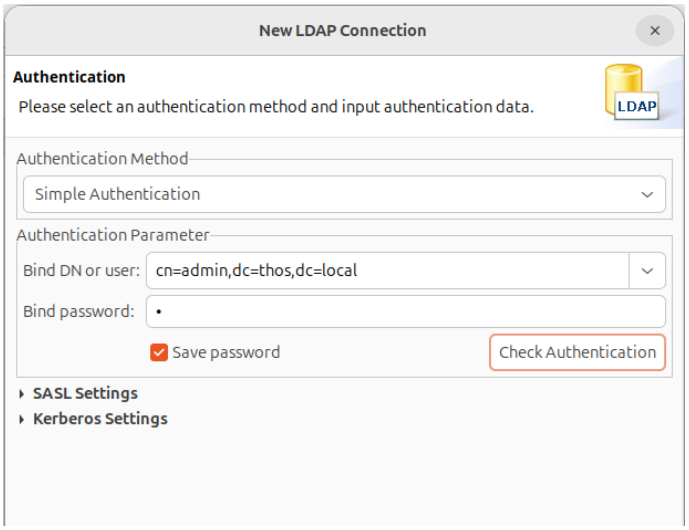


Figura 7: Autenticació

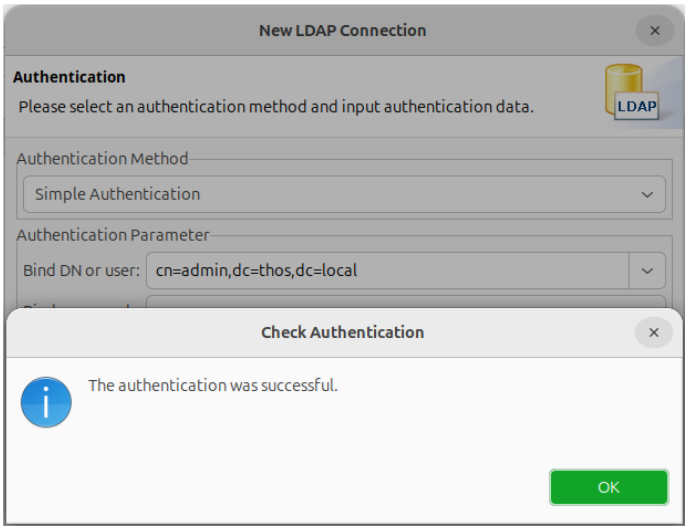


Figura 8: Base DN

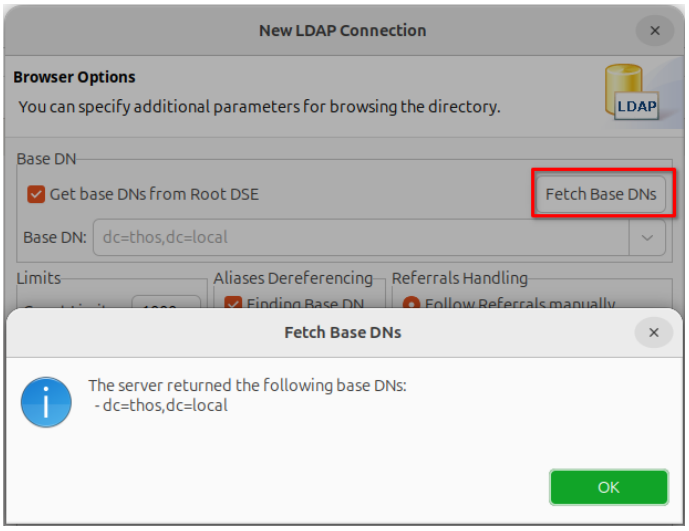


Figura 9: Recupera Base DN

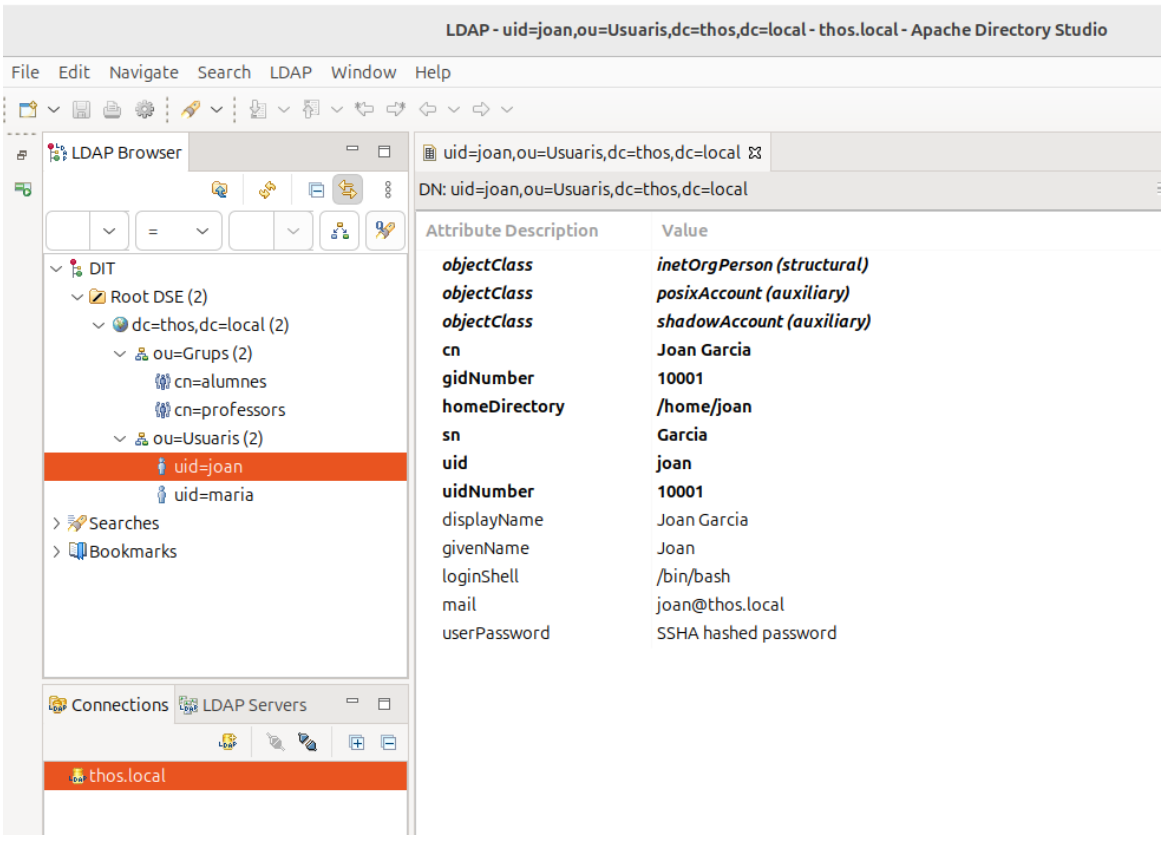


Figura 10: Interfície d'Apache Directory Studio

10.2. phpLDAPadmin (interfície web)

phpLDAPadmin és una eina web (PHP) per administrar servidors LDAP des del navegador, a diferència d'Apache Directory Studio que és una aplicació d'escriptori. S'instal·la al servidor.

Funcionalitats

- **Navegar i editar el DIT** des d'un navegador web, amb una interfície d'arbre similar a Directory Studio.
- **Crear/modificar/eliminar entrades** (usuaris, grups, OU) amb formularis HTML.
- **Importar/exportar LDIF** des de la interfície web.
- **Cercar** amb filtres LDAP predefinits o personalitzats.
- **Gestió d'esquemes**: consultar objectClasses i attributeTypes disponibles.

Comparativa amb Apache Directory Studio

	phpLDAPadmin	Apache Directory Studio
Tipus	Aplicació web (Apache+PHP)	Aplicació d'escriptori (Java)
Accés	Des de qualsevol navegador de la xarxa	Cal instal·lar-lo a cada màquina client
Manteniment	**Projecte pràcticament abandonat** des de fa anys	Actiu i mantingut per Apache
TLS/SSL	Suport limitat i configuració sovint problemàtica	Gestió de certificats més robusta

AVÍS

phpLDAPadmin **fa anys que no rep actualitzacions actives** (l'última versió estable és de 2015-2016, tot i que hi ha forks comunitaris com **ldapadmin** o **phpLDAPadmin** mantingut per algunes distribucions).

Instal·lació

```
sudo apt install phpldapadmin
```

Configura la connexió

```
sudo nano -l /etc/phpldapadmin/config.php
```

Modifica les línies 324, 331 i 358:

```
$servers->setValue('server','host','192.168.1.10');
$servers->setValue('server','base',array('dc=thos,dc=local'));
$servers->setValue('login','bind_id','cn=admin,dc=thos,dc=local');
```

Accedeix des del navegador: `http://192.168.1.10/phpldapadmin`

Figura 11: Interfície de phpLDAPadmin

10.3. LDAP Account Manager (interfície web)

LDAP Account Manager

Manual d'LDAP Account Manager

LDAP Account Manager és una interfície web avançada per administrar comptes d'usuari, grups i altres objectes LDAP, pensada com a alternativa moderna i mantinguda a phpLDAPadmin. Destaca per la seva integració amb esquemes estàndard (`posixAccount`, `inetOrgPerson`, Samba, etc.) i per oferir funcions de gestió massiva d'usuaris. S'instal·la al servidor.

Funcionalitats

- **Gestió d'usuaris i grups** amb formularis pensats per a casos d'ús reals (POSIX accounts, Samba accounts, Kerberos, etc.), no només edició genèrica d'atributs com phpLDAPadmin.
- **Assistents (wizards)** per crear usuaris/grups amb tots els atributs necessaris ja predefinits (UID, GID, shell, home directory…), útil per no haver d'omplir manualment cada objectClass.
- **Suport per a múltiples esquemes:** Unix, Samba, Kolab, etc.

- **Perfils de configuració**: permet definir plantilles diferents segons el tipus d'entrada (professors, alumnes, equips…).
- **Importació/exportació massiva** en format LDIF o CSV
- **Gestió de contrasenyes** amb polítiques configurables
- **Auditoria** de canvis al directori
- **Perfils múltiples** per gestionar diversos servidors LDAP
- **LAM Pro** (versió de pagament, encara que hi ha versió gratuïta prou completa) afegeix autoservei per a usuaris, gestió de polítiques de contrasenyes, i més integracions.

Comparativa amb phpLDAPadmin

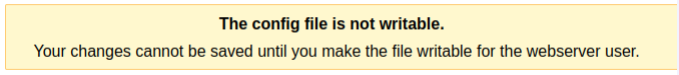
	LAM	phpLDAPadmin
Manteniment	Actiu (última release el 2025)	Abandonat des de ~2015
TLS/SSL modern	Suport complet TLS 1.2/1.3	Sovint problemàtic
Enfocament	Orientat a tasques (crear usuari, grup…)	Edició genèrica d'atributs bruts
PHP modern	Compatible amb PHP 8.x	Pot requerir pedaços per PHP recent

Instal·lació

```
sudo apt install ldap-account-manager
```

NOTA

Fins a la versió d'Ubuntu 24.04, això instal·la LAM i configura automàticament Apache per servir-lo a `/lam`, però a la versió 26.04 d'Ubuntu s'ha endurit el sandboxing.



Has de donar permisos d'escriptura a dos directoris:

```
sudo systemctl edit apache2
```

```
[Service]
ReadWritePaths=/etc/ldap-account-manager
 ↪  /var/lib/ldap-account-manager
```

Rellegeix els **`unit files`** (`.service`, `.socket`, `.timer`, etc.)

```
sudo systemctl daemon-reload
```

Reinicia Apache

```
sudo systemctl restart apache2
```

Configuració inicial

Accedeix a la interfície de configuració:

```
http://ldapserver.thos.local/lam
```

IMPORTANT

La contrasenya de configuració per defecte és **`lam`**. Canvia-la immediatament a *LAM configuration → General settings → Master password*.

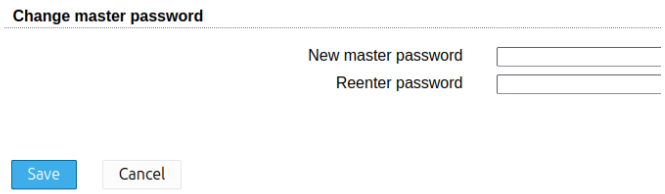


Figura 12: Canvia la contrasenya

Crear un perfil de servidor

Ves a **LAM configuration → Edit server profiles** i configura:

Paràmetre	Valor
Server address	`ldap://192.168.1.10:389`
Tree suffix	`dc=thos,dc=local`
List of valid users	`cn=admin,dc=thos,dc=local`
Login method	Fixed list

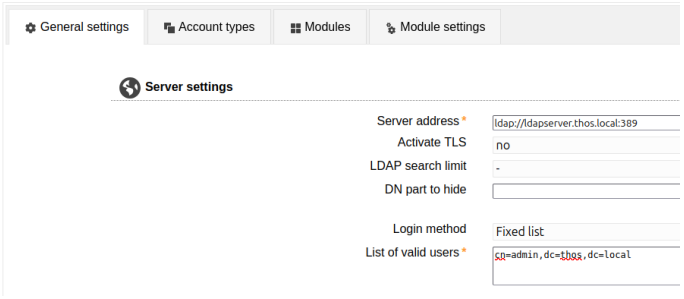


Figura 13: Configuració del servidor

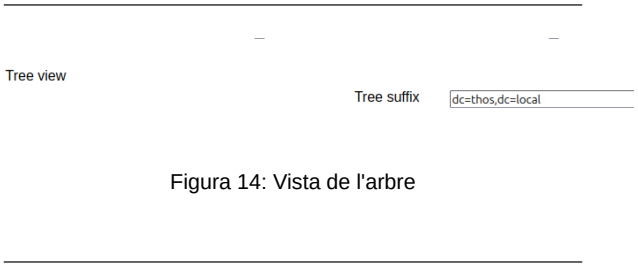


Figura 14: Vista de l'arbre

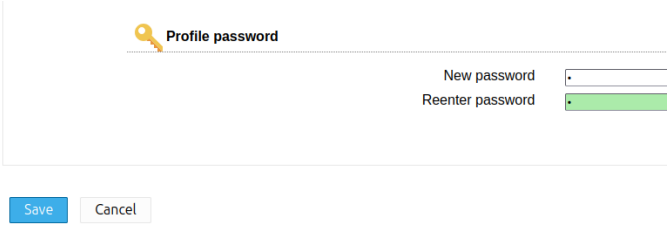


Figura 15: Contrasenya de l'administrador d'LDAP

A la pestanya **Account types**, defineix on es guarden els usuaris i grups:

Tipus	Suffix LDAP
Users	`ou=Usuaris,dc=thos,dc=local`
Groups	`ou=Grups,dc=thos,dc=local`

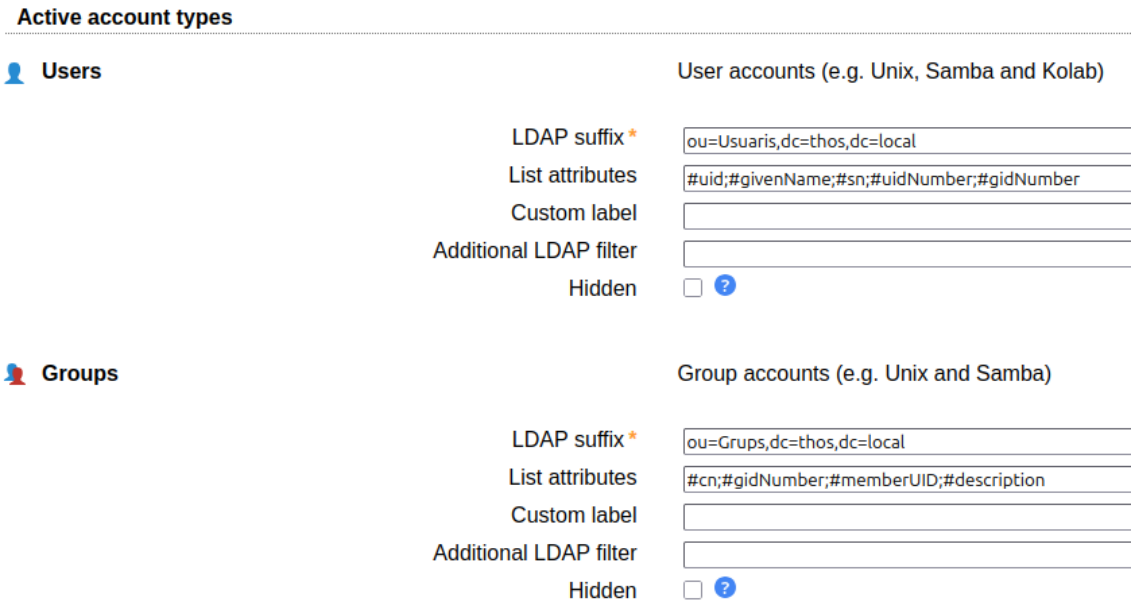


Figura 16: Tipus de comptes

Desa el perfil i accedeix al panell principal:

```
http://192.168.1.10/lam
```

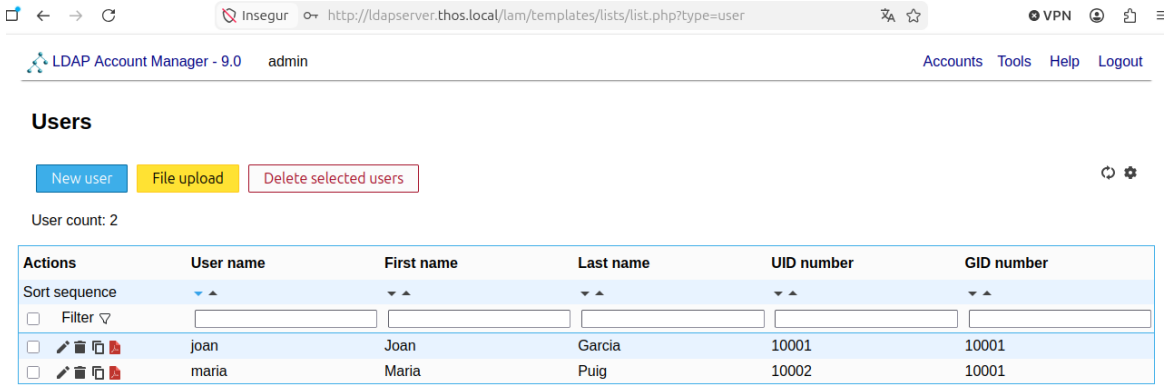


Figura 17: Usuaris d'LDAP

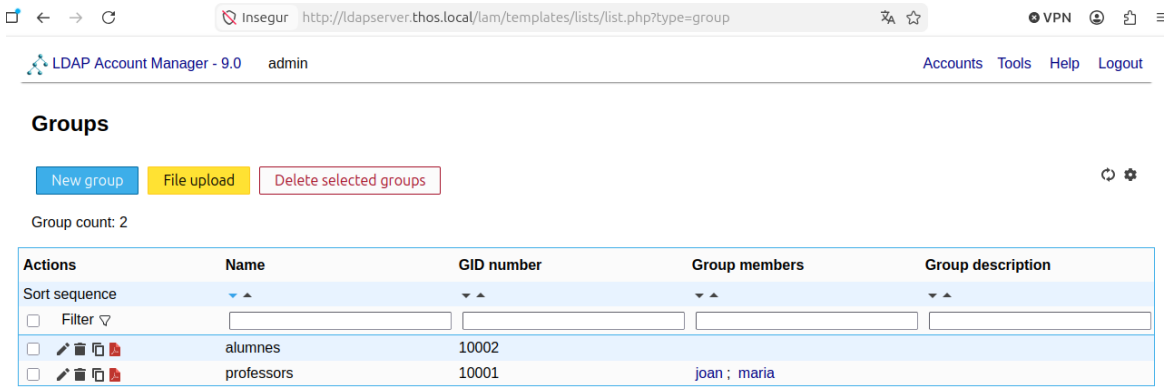


Figura 18: Grups d'LDAP

Accés per LDAPS

Per connectar via LDAPS, edita el perfil i canvia l'adreça del servidor:

```
ldaps://192.168.1.10:636
```

Si el certificat és autosignat, cal afegir la CA al sistema:

```
sudo cp /etc/ldap/certs/ca.crt
 ↪  /usr/local/share/ca-certificates/ldap-ca.crt
sudo update-ca-certificates
sudo systemctl restart apache2
```

10.4. ldapscripts --- gestió d'usuaris simplificada

```
sudo apt install ldapscripts

sudo nano /etc/ldapscripts/ldapscripts.conf
```

Paràmetres clau:

```
SERVER="ldap://localhost"
BINDDN="cn=admin,dc=thos,dc=local"
BINDPWDFILE="/etc/ldapscripts/ldapscripts.passwd"
SUFFIX="dc=thos,dc=local"
USUFFIX="ou=Usuaris"
GSUFFIX="ou=Grups"
UIDSTART=10000
GIDSTART=10000
```

```
# Desa la contrasenya de l'administrador
echo -n "contrasenya_admin" | sudo tee
 ↪  /etc/ldapscripts/ldapscripts.passwd
sudo chmod 400 /etc/ldapscripts/ldapscripts.passwd

# Afegir usuari
sudo ldapadduser pere professors

# Eliminar usuari
sudo ldapdeleteuser pere

# Afegir grup
sudo ldapaddgroup devops

# Afegir usuari a grup
sudo ldapaddusertogroup joan devops
```

11. Resolució de problemes

11.1. Diagnosi general

```
# Estat del servei
sudo systemctl status slapd

# Logs en temps real
sudo journalctl -u slapd -f

# Logs de rsyslog (si configurat)
sudo tail -f /var/log/slapd.log

# Comprovar la sintaxi de la configuració
sudo slaptest -v

# Comprovar la integritat de la base de dades
sudo slapd -T test -f /etc/ldap/slapd.conf
```

11.2. Errors freqüents

Error: `Can't contact LDAP server`

```
# Comprova que slapd està en marxa
sudo systemctl start slapd

# Comprova el port
sudo ss -tlnp | grep 389

# Comprova el tallafoc
sudo ufw status
sudo ufw allow 389/tcp
sudo ufw allow 636/tcp
```

Error: `Invalid credentials (49)`

```
# El DN o la contrasenya són incorrectes. Verifica:
ldapwhoami -x -D "cn=admin,dc=thos,dc=local" -W

# Reseteja la contrasenya de l'admin
sudo ldappasswd -Y EXTERNAL -H ldapi:/// \
  -s nova_contrasenya \
  "cn=admin,dc=thos,dc=local"
```

Error: `No such object (32)` en cercar

```
# La base de cerca no existeix. Verifica la base DN:
sudo ldapsearch -Y EXTERNAL -H ldapi:/// -b "cn=config" \
  "(olcSuffix=*)" olcSuffix
```

Error: `TLS: can't connect`

```
# Comprova els certificats
openssl verify -CAfile /etc/ldap/certs/ca.crt
 ↪  /etc/ldap/certs/ldapserver.crt

# Comprova la data de caducitat
openssl x509 -in /etc/ldap/certs/ldapserver.crt -noout -dates

# Desactiva temporalment la verificació TLS per depurar
LDAPTLS_REQCERT=never ldapsearch -x -ZZ -b "dc=thos,dc=local" \
  -H ldap://ldapserver.thos.local
```

Problema: usuaris LDAP no apareixen amb `getent passwd`

```
# Comprova nsswitch.conf
grep passwd /etc/nsswitch.conf

# Comprova la connexió des del client
ldapsearch -x -b "ou=Usuaris,dc=thos,dc=local" -H ldap://192.168.1.10

# Reinicia nscd
sudo systemctl restart nscd

# Neteja la caché de nscd
sudo nscd -i passwd
sudo nscd -i group
```

11.3. Eines de diagnosi avançada

```
# Activar log detallat temporalment
sudo ldapmodify -Y EXTERNAL -H ldapi:/// << EOF
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: -1
EOF

# Tornar al nivell normal quan hagis acabat
sudo ldapmodify -Y EXTERNAL -H ldapi:/// << EOF
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: stats
EOF
```

12. Resum de ports i serveis

Port	Protocol	Servei	Descripció
389	TCP	LDAP	Connexió LDAP estàndard (text pla o STARTTLS)
636	TCP	LDAPS	LDAP sobre SSL/TLS
3268	TCP	GC	Global Catalog (Active Directory)
3269	TCP	GC over SSL	Global Catalog sobre SSL

Ordres de referència ràpida

```
# Iniciar / aturar / reiniciar / comprovar l'estat
sudo systemctl start|stop|restart|status slapd

# Cercar tots els objectes
ldapsearch -x -b "dc=thos,dc=local" -H ldap://localhost

# Afegir entrades des de fitxer LDIF
ldapadd -x -D "cn=admin,dc=thos,dc=local" -W -f fitxer.ldif

# Modificar entrades des de fitxer LDIF
ldapmodify -x -D "cn=admin,dc=thos,dc=local" -W -f canvis.ldif

# Eliminar una entrada
ldapdelete -x -D "cn=admin,dc=thos,dc=local" -W
 ↪  "uid=joan,ou=Usuaris,dc=thos,dc=local"

# Exportar el directori complet
sudo slapcat -v -l backup.ldif

# Importar (slapd ha d'estar aturat)
sudo systemctl stop slapd
sudo slapadd -v -l backup.ldif
sudo systemctl start slapd
```

Referències

- Documentació oficial d'OpenLDAP
- Ubuntu Server Guide --- OpenLDAP
- RFC 4511 --- Lightweight Directory Access Protocol (LDAP)

Versions d'aquest document

- HTML - ldap.html
- PDF - ldap.pdf
- ODT - ldap.odt
- MD - ldap.md