

## SISTEMES OPERATIUS DE XARXA

U7: SERVEIS DE DIRECTORI. OpenLDAP

CFGM  
SMX  
DPT INF

# OpenLDAP a Ubuntu Server/Desktop 20.04 Instal·lació i configuració. ( Fitxers Idif i ordres ldap ) Part 3.

## UD3: Administració de serveis de directori: LDAP

EL SERVEI SLAPD.....	3
Comprovar la connexió amb el servidor LDAP.....	3
FITXERS Idif.....	4
Afegir objectes.....	4
Afegir un nou usuari.....	6
Modificar entrades existents a LDAP.....	7
Importar/Exportar fitxers LDIF.....	8
COMANDAMENTS ldap.....	9
Canvi de password: ladpasswd.....	9
Búsqueda d'objectes: ldapsearch.....	10
Esborrar entrades/usuarios a LDAP.....	11

## INTRODUCCIÓ.

Esta tercera part del OpenLDAP vorem una part del que és la gestió d'este des del Terminal ( mitjançant ordres ) , tant en l servidor com en una màquina client.

Per als exemples següents partim de:

Un Servidor en una IP fixa 192.168.10.1/24

Un administrador del servicis OpenLDAP «admin» amb password «tomas»

## EL SERVEI SLAPD

Si necessitem reiniciar el servei sense reiniciar la màquina podem fer

```
sudo /etc/init.d/slapd start  
sudo /etc/init.d/slapd stop  
sudo /etc/init.d/slapd restart
```

O si preferiu

```
sudo service slapd start  
sudo service slapd stop  
sudo service slapd restart
```

## Comprovar la connexió amb el servidor LDAP

En el servidor

```
tomas@linuxserver:~$ ldapwhoami -H ldap://localhost -D "cn=admin,dc=smx,dc=local" -W  
Enter LDAP Password:  
dn:cn=admin,dc=smx,dc=local
```

En un client.

```
ariadna@ariadnaUbuntu:~$ ldapwhoami -H ldap://linuxserver -D "cn=admin,dc=smx,dc=local" -W  
Enter LDAP Password:  
dn:cn=admin,dc=smx,dc=local
```

Ens retorna el DN si la connexió amb LDAP ha estat correcta.

## COMANDAMENTS AMB FITXERS ldif

Usarem la utilitat **slapadd** amb fitxers **ldif**

### Afegir objectes

La gestió del servici d'LDAP en mode consola es realitza al **servidor** fent ús de fitxers amb extensió ldif.

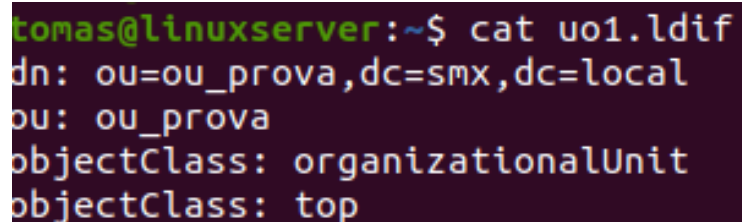
Creem un nou ou ldif:

```
nano ou1.ldif
```

L'emplenem amb el següent contingut:

```
dn: ou=ou_prova,dc=smx,dc=local
ou: ou_prova
objectClass: organizationalUnit
objectClass: top
```

Queda així:



```
tomas@linuxserver:~$ cat uo1.ldif
dn: ou=ou_prova,dc=smx,dc=local
ou: ou_prova
objectClass: organizationalUnit
objectClass: top
```

Per afegir l'uo al directori LDAP:

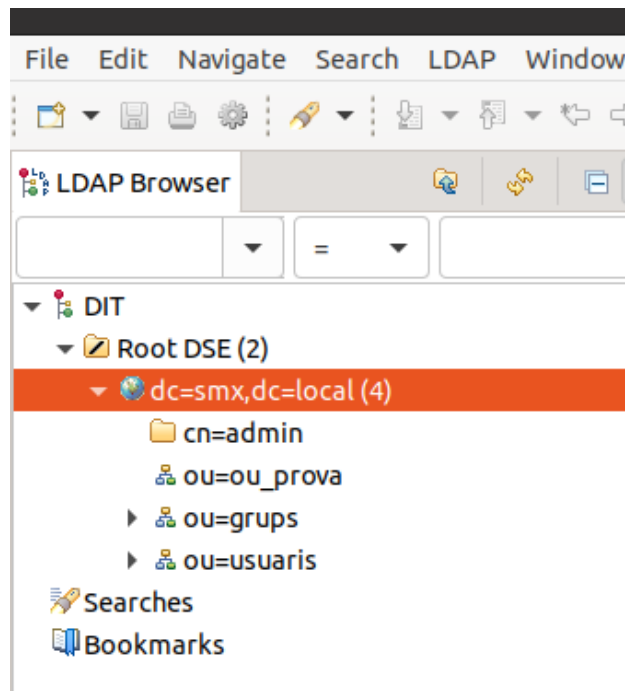
```
ldapadd -x -D 'cn=admin,dc=iesmariaenriquez,dc=es' -w tomas -f uo1.ldif
```

**-x**: empra autenticació simple

**-D 'cn=admin, dc=iesmariaenriquez,dc=es'** : especifica el DN per a autenticar-se (qui va a fer el canvi)

**-w pass** : password per a l'autenticació simple (si especifiquem -w, ens la demanarà a continuació i no cal escriure-la a la línia d'ordres).

**-f exemple.ldif**: indica el fitxer a importar.



Este format es repeteix a totes les ordres.

On la resposta obtinguda si tot és correcte és:

```
tomas@linuxserver:~$ sudo ldapadd -x -D "cn=admin,dc=smx,dc=local" -w tomas -f us1.ldif
adding new entry "uid=jFuster,ou=usuaris,dc=smx,dc=local"
ldap_add: Object class violation (65)
        additional info: object class 'posixAccount' requires attribute 'gidNumber'
tomas@linuxserver:~$
```

A este exemple podeu veure que he fet ús del paràmetre -W (en majúscula) i per això demana la contrasenya abans de fer cap addició.

Si volem introduir l'usuari **des de d'una màquina remota** ho faríem:

```
ldapadd -H ldap://192.168.10.1 -x -D 'cn=admin, dc=smx,dc=local' -w contrassadmin -f exemple.ldif
```

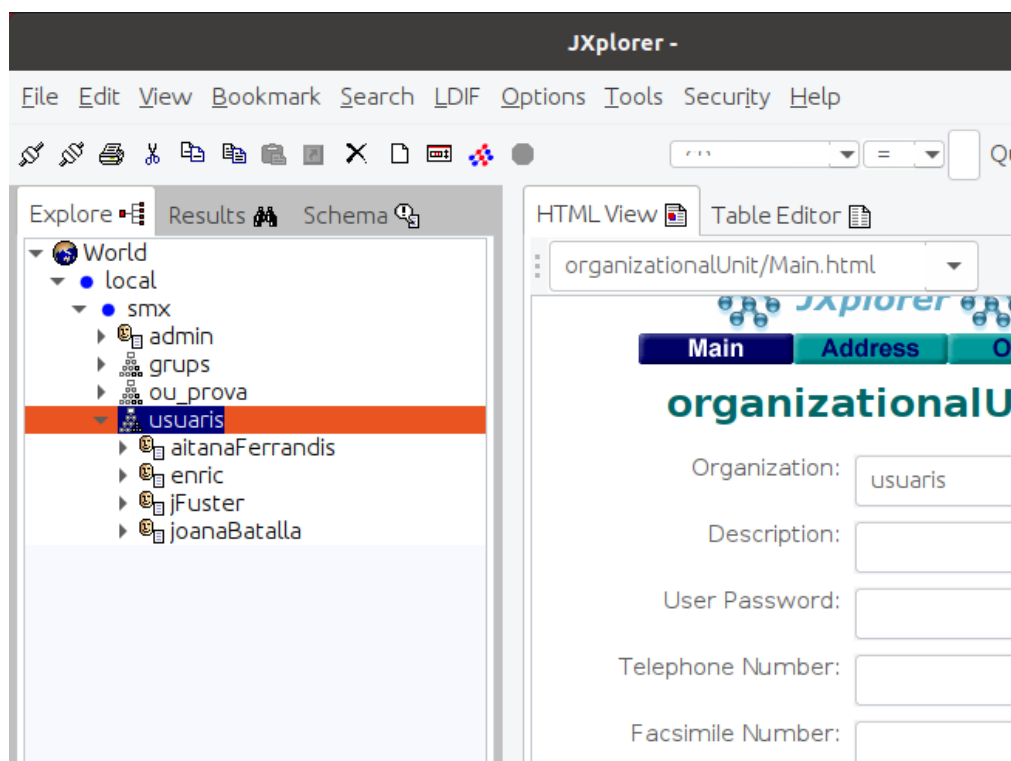
-H: especifiquem la URI (on està ubicat el servei ldap). Amb el nom ( si està a *etc/hosts* ) o la ip.  
Recorda que pots fer **sudo slapcat** per visualitzar el contingut del directori.

## Afegir un nou usuari

Fitxer ldif=usuaris,

```
tomas@linuxserver:~$ cat us1.ldif
dn: uid=jFuster,ou=usuaris,dc=smx,dc=local
cn: Joan
sn: Fuster
objectClass: person
objectClass: posixAccount
objectClass: top
uid: jFuster
uidNumber: 30001
gidNumber: 10002
homeDirectory: /home/usuaris/jFuster
```

```
tomas@linuxserver:~$ sudo ldapadd -x -D "cn=admin,dc=smx,dc=local" -w tomas -f us1.ldif
adding new entry "uid=jFuster,ou=usuaris,dc=smx,dc=local"
```



## Modificar entrades existents a LDAP

Cal crear un fitxer ldif, com els següents (compte amb la sintaxi):

Modifica el sn:

Ordre:

```
tomas@linuxserver:~$ ldapadd -x -D "cn=admin,dc=smx,dc=local" -w tomas -f enricpardoSN.ldif
modifying entry "cn=enric,ou=usuaris,dc=smx,dc=local"
```

```
ldapmodify -x -D 'cn=admin,dc=smx,dc=local' -w tomas -f enricpardoSN.ldif
```

I com podem revisar, si comprovem amb "slapcat", l'última línia és la de l'últim usuari que hem afegit, i revisem el 'sn':

```
entryUUID: 587ddf3a-0c86-103c-869e-57df0c21f20b
creatorsName: cn=admin,dc=smx,dc=local
createTimestamp: 20220118084242Z
userPassword:: e1NTSEF9d2ZNQ2VNUk16VE9uSkxobVJEUhdGb2JrMVlJem
entryCSN: 20220119220355.937831Z#000000#000#000000
modifiersName: cn=admin,dc=smx,dc=local
modifyTimestamp: 20220119220355Z
```

```
tomas@linuxserver:~$ cat enricpardoSN.ldif
dn:cn=enric,ou=usuaris,dc=smx,dc=local
changetype: modify
replace: sn
sn: Enric Pardo
```

Afegir un sn:

```
dn:uid=jFuster,ou=usuaris,dc=smx,dc=local
changetype: modify
add: sn
sn: Enric Ferrandis
```

En aquest punt tindrem dos atributs sn.

Intenta esborrar tots els atributs sn: (donarà error ja que sn és OBLIGATORI a la classe person i per tant obligatori):

```
dn:uid=jFuster,ou=usuaris,dc=smx,dc=local
changetype: modify
delete: sn
```

Esborrar només un dels atribut sn (així evitem l'error):

```
dn:uid=jFuster,ou=usuaris,dc=smx,dc=local
changetype: modify
delete: sn
sn: Fuster Combustible
```

Si per exemple volem afegir una fotografia a qualsevol dels usuaris:

```
dn:uid=jFuster,ou=usuaris,dc=smx,dc=local
changetype: modify
add: jpegPhoto
jpegPhoto: /tmp/foto.jpg
```

foto.jpg ha de ser una foto en format jpg i ha d'estar al directori que especifiquem. No el podem visualitzar amb Jxplorer.



## **Importar/Exportar fitxers LDIF**

Si volem exportar una part del nostre arbre una forma de fer-ho seria

```
ldapsearch -x -b 'ou=usuaris,dc=smx,dc=local' > usuaris.ldif
```

Un altra forma d'exportar seria emprant l'ordre slapcat.

```
slapcat -l users.ldif -s "ou=usuaris,dc=smx,dc=local"
```

**Aquesta ordre també inclou més informació de l'objecte**, com per exemple createTimeStamp, per la qual cosa si vulguerem importar el fitxer anterior (sense modificar) ens donaria un error de sintaxis.

Per importar objectes al nostre arbre ho faríem amb l'ordre ldapadd, com hem vist anteriorment.

## COMANDAMENTS ldap

- **ldappasswd**
- **ldapsearch**
- **ldapdelete**

### Opcions comuns:

- D indica el DN amb el qual va a identificar-se en el servidor
- w especifica la seua contrasenya
- W ens la demanarà posteriorment interactivament, ara no cal indicar-la
- H indica el nom del servidor ldap ( -h es obsoleta ).
- x força el mecanisme d'autenticació simple en compte de SASL.
- p port TCP ( 389 per defecte )

### Canvi de password: *ldappasswd*.

#### Des del servidor

Exemple de canvi de password a dos usuaris amb «uid» i amb «cn» identificant-se com l'usuari que es modifica.

```
tomas@linuxserver:~$ ldappasswd -D "uid=jFuster,ou=usuaris,dc=smx,dc=local" -w jfuster2022 -s jfuster2023 "uid=jFuster,ou=usuaris,dc=smx,dc=local"
```

```
tomas@linuxserver:~$ ldappasswd -D "cn=enric,ou=usuaris,dc=smx,dc=local" -w enric2022 -s enric2023 "cn=enric,ou=usuaris,dc=smx,dc=local"
```

Exemple de canvi de password a dos usuaris amb «uid» i amb «cn» identificant-se com l'usuari admin

```
tomas@linuxserver:~$ ldappasswd -D "cn=admin,dc=smx,dc=local" -w tomas -s enric2023 "cn=enric,ou=usuaris,dc=smx,dc=local"
```

```
tomas@linuxserver:~$ ldappasswd -D "cn=admin,dc=smx,dc=local" -w tomas -s jfuster2023 "uid=jFuster,ou=usuaris,dc=smx,dc=local"
```

#### Des d'un client ( -H ldap://nomservidor )

```
ariadna@ariadnaUbuntu:~$ ldappasswd -H ldap://linuxserver -D "cn=admin,dc=smx,dc=local" -w tomas -s enric2022 "cn=enric,ou=usuaris,dc=smx,dc=local"
```

```
ariadna@ariadnaUbuntu:~$ sudo ldappasswd -H ldap://192.168.10.1 -D "cn=enric,ou=usuaris,dc=smx,dc=local" -w enric2022 "cn=enric,ou=usuaris,dc=smx,dc=local"
New password: id.NPvQc
```

## Búsqueda d'objectes: ldapsearch

Des d'un client filtrant per objectclass

```
ariadna@ariadnaUbuntu:~$ ldapsearch -x -H ldap://linuxserver -D "cn=admin,dc=smx,dc=local" -w tomas -b "dc=smx,dc=local" "(objectclass=posixAccount)" | grep uid:
uid: enricPardo
uid: joanaBatalla
uid: aitanaFerrandis
uid: jFuster
```

Des del mateix servidor filtrant per uid

```
tomas@linuxserver:~$ ldapsearch -D "cn=admin,dc=smx,dc=local" -w tomas -b "dc=smx,dc=local" "(uid=*)" | grep uid:
uid: enricPardo
uid: joanaBatalla
uid: aitanaFerrandis
uid: jFuster
```

### Més detall

Ordre:

```
ldapsearch -x -b 'dc=smx,dc=local' -LLL '(uid=enricPardo)'
```

Cerca l'usuari amb uid=cristina

-LLL mostra la informació en format LDIF v1, sense comentaris i sense indicar la versió de LDIF

'(uid=cristina)': el que busquem

Ordre:

```
ldapsearch -x -b 'dc=smx,dc=local' -LLL '(uid=enricPardo)' cn sn
```

Mostrarà només el cn i el sn de l'uid "cristina"

## Buscar amb variable

```
ldapsearch -x -b 'dc=smx,dc=local' -LLL "(&(cn=$departament))"
```

Altres exemples de cerca:

- (mail=\*) Totes les entrades que tinguin mail
- (mail=\*@\*) Totes les entrades que tinguin mail vàlid
- (sn=smith) Cerca per cognom
- (sn=s\*) Entrades amb cognom començant per s o S
- (cn=\*a\*i\*) Entrades amb una a o una i en qualsevol lloc
- (telephonenumber=\*555)
- (objectclass=person) Buscar objectes person

A l'adreça <http://www.zytrax.com/books/ldap/apa/search.html> (anglès) hi ha exemples més complexos

## Esborrar entrades/usuaris a LDAP

Ordre:

Data última modificació:12/01/2021

Pàgina 11 de 12

```
ldapdelete -x -D 'cn=admin,dc=smx,dc=local' -w tomas 'uid=jFuster,ou=usuaris, dc=smx,dc=local'
```