OpenLDAP a Ubuntu

Server/Desktop 20.04

Instal·lació i configuració.

( Fitxers ldif i ordres ldap )

Part 3.



Administració de serveis de directori: LDAP

[EL SERVEI SLAPD 3](#__RefHeading___Toc3419_2310447174)

[Comprovar la connexió amb el servidor LDAP 3](#__RefHeading___Toc3439_2310447174)

[FITXERS ldif 4](#__RefHeading___Toc1464_1411336733)

[Afegir objectes 4](#__RefHeading___Toc3427_2310447174)

[Afegir un nou usuari 6](#__RefHeading___Toc1466_1411336733)

[Modificar entrades existents a LDAP 7](#__RefHeading___Toc1430_1411336733)

[Importar/Exportar fitxers LDIF 8](#__RefHeading___Toc3437_2310447174)

[COMANDAMENTS ldap 9](#__RefHeading___Toc3429_2310447174)

[Canvi de password: ladppasswd. 9](#__RefHeading___Toc1426_1411336733)

[Búsqueda d’objectes: ldapsearch 10](#__RefHeading___Toc1428_1411336733)

[Esborrar entrades/usuaris a LDAP 11](#__RefHeading___Toc3431_2310447174)

# 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 adminsitrador ddel servicis OpenLDAP «admin» amb password «tomas»

Les ordres que veiem indiquem la base de dades d'objectes del directori on accedim amb el paràmetre -b.

Si configurem el fitxer ldap.conf podem omitir este paràmetre

# EL SERVEI SLAPD

Si necessitem reiniciar el servei sense reiniciar la màquina podem fer

*sudo systemctl start slapd*

*sudo systemctl restart slapd*

*udo systemctl stop slapd*

*udo systemctl status slapd*

## Comprovar la connexió amb el servidor LDAP

En el servidor



En un client.



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

# COMANDAMENTS AMB FITXERS ldif

Usarem la utilitst **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:

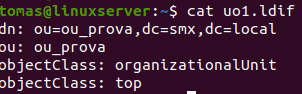
dn: ou=ou\_prova,dc=smx,dc=local

ou: ou\_prova

objectClass: organizationalUnit

objectClass: top

Queda així:



Per afegir l'uo al directori LDAP:

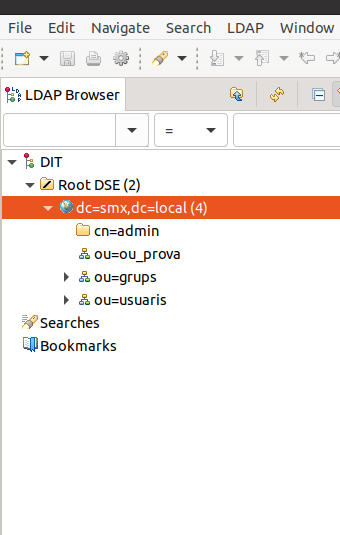
*ldapadd -x -D 'cn=admin,dc=smx,dc=local' -w tomas -f uo1.ldif*

**-x**: empra autenticació simple

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

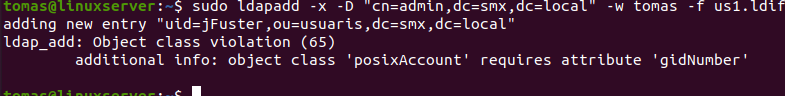
**-w pass** : password per a l’autenticació simple (si especifiquem -w, ens la demanarà a continuació i no cal escriure-la a la línia d’ordres).

**-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:



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:

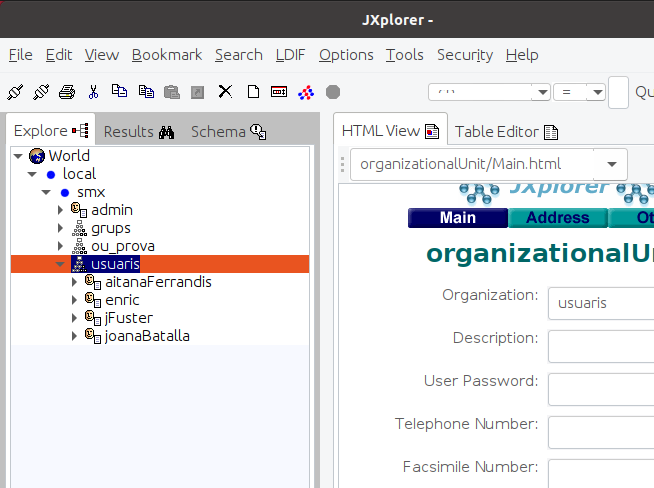
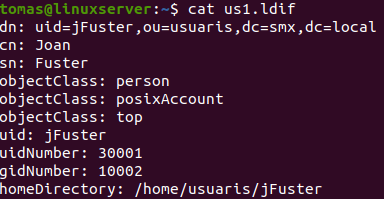
*ldapadd* -H ldap://192.168.10.1 *-x -D 'cn=admin, dc=smx,dc=local' -w contrassadmin -f exemple.ldif*

**-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,



## Modificar entrades existents a LDAP

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

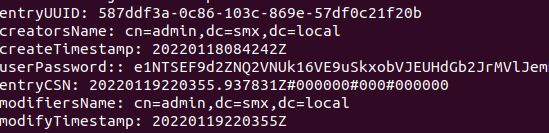
Modifica el sn:

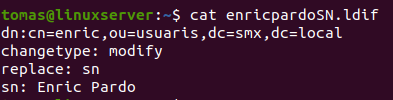
Ordre:



*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’:





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 especifiques. 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 slapacat.

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

**Aquesta ordre també inclou més informació de l’objecte**, com per exemple createTimeStampt, 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**
* **ldapdeletete**

**Opcions comuns:**

-D indica el DN amb el qual va a indetificar-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 lddap ( -h es obsoleta ).

-x força el mecanisme d’autenticació simple en compte de SASL.

-p port TCP ( 389 per defecte )

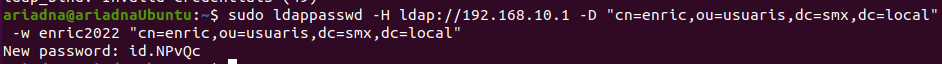
## Canvi de password: ladppasswd.

**Des del servidor**

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

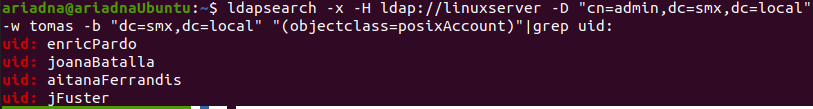
Exemple de canvi de password a dos usuaris amb «uid» i amb «cn» identificant-se com l’usuari admin

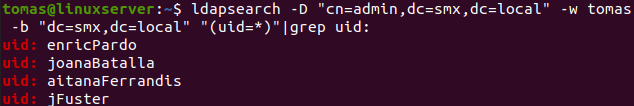
**Des d’un client** ( -H ldpap://nomservidor )



## Búsqueda d’objectes: ldapsearch

**Des d’un client** filtrant per objectclass

 **Des del mateix servidor** filtrant per uid

**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:

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