

1 · Introducció a ldap-utils

El paquet ldap-utils proporciona un conjunt d'eines de línia de comandes per interactuar amb un servidor LDAP (Lightweight Directory Access Protocol). Permet realitzar consultes, afegir, modificar i eliminar entrades del directori sense necessitat d'una interfície gràfica.

Instal·lació del paquet:

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

Les eines principals incloses al paquet son:

Eina	Acció principal
ldapsearch	Cercar i consultar entrades del directori
ldapadd	Afegir noves entrades a partir d'un fitxer LDIF
ldapmodify	Modificar atributs d'entrades existents
ldapdelete	Eliminar entrades del directori
ldappasswd	Canviar la contrasenya d'un usuari LDAP
ldapwhoami	Mostrar la identitat autenticada a la sessió actual
ldapmodrdn	Canviar el RDN (nom relatiu) d'una entrada
slapcat	Exportar la base de dades LDAP a format LDIF (servidor)
slapadd	Importar entrades LDIF directament a la BD (servidor)

2 · Opcions comunes a totes les eines

La majoria d'eines de ldap-utils comparteixen les opcions següents:

Opció	Descripció	Exemple
-x	Autenticació simple (sense SASL)	-x
-H uri	URI del servidor LDAP	-H ldap://192.168.1.2
-D "dn"	DN de l'usuari per autenticar-se (Bind DN)	-D "cn=admin,dc=clotfje,dc=net"
-W	Demana la contrasenya de forma interactiva	-W
-w "pass"	Contrasenya en text pla (per a scripts)	-w fjeclot
-b "base"	Base de cerca del directori	-b "dc=clotfje,dc=net"
-f fitxer	Fitxer LDIF d'entrada	-f usuaris.ldif
-v	Mode verbose (mes informació de sortida)	-v
-Z	Inicia connexió TLS (StartTLS)	-Z
-p port	Port del servidor (per defecte 389)	-p 389

NOTA: Utilitza -W (majúscula) per introduir la contrasenya de forma interactiva i segura. Evita -w en entorns de producció perquè la contrasenya quedaria visible a la història de comandes.

3 · ldapsearch · Cercar entrades al directori

ldapsearch permet fer consultes al servidor LDAP i mostrar els resultats en format LDIF. Es l'eina mes utilitzada per comprovar el contingut del directori.

3.1 · Sintaxi general

```
ldapsearch [opcions] [filtre] [atributs...]
```

3.2 · Opcions especificques de ldapsearch

Opció	Descripció
-L	Format de sortida LDIF (una -L = LDIF v1, -LL sense comentaris, -LLL mínim)
-s	Abast de la cerca: base, one, sub (per defecte sub = recursiu)
-z N	Limita el nombre màxim de resultats a N entrades
-l N	Temps màxim d'espera (en segons) per la resposta
-a	Com gestionar les referències (never, always, search, find)
-A	Nomes mostra els noms dels atributs, sense els valors
-T	Desa els valors binaris en fitxers temporals

3.3 · Filtres de cerca LDAP

Els filtres segueixen la sintaxi X.500 amb parèntesis. Es poden combinar amb operadors lògics:

Filtre	Significat	Exemple
(atribut=valor)	Igualtat exacta	(uid=alop)
(atribut=*)	L'atribut existeix (qualsevol valor)	(mail=*)
(atribut=val*)	Comença per "val"	(cn=jor*)
(atribut>=valor)	Major o igual que	(uidNumber>=3000)
(atribut<=valor)	Menor o igual que	(uidNumber<=3999)
(&(f1)(f2))	I logic (AND): f1 i f2 han de ser certs	(&(uid=alop) (objectClass=person))
((f1)(f2))	O logic (OR): f1 o f2 han de ser certs	((uid=alop)(uid=jgim))
(!(filtre))	Negació (NOT)	(!(objectClass=posixAccount))

3.4 · Exemples de ldapsearch

Llistar totes les entrades del domini

```
ldapsearch -x -b "dc=clotfje,dc=net" "(objectClass=*)" "
```

Llistar tots els usuaris (posixAccount)

```
ldapsearch -x -b "dc=clotfje,dc=net" "(objectClass=posixAccount) "
```

Buscar un usuari concret per uid

```
ldapsearch -x -b "dc=clotfje,dc=net" "(uid=alop) "
```

Mostrar noms atributs concrets d'un usuari

```
ldapsearch -x -b "dc=clotfje,dc=net" "(uid=alop)" uid cn sn uidNumber gidNumber  
homeDirectory loginShell
```

Llistar tots els grups del domini

```
ldapsearch -x -b "dc=clotfje,dc=net" "(objectClass=posixGroup) "
```

Llistar les unitats organitzatives

```
ldapsearch -x -b "dc=clotfje,dc=net" "(objectClass=organizationalUnit) "
```

Buscar usuaris amb UID entre 3000 i 3999

```
ldapsearch -x -b "dc=clotfje,dc=net" "(&(objectClass=posixAccount)  
(uidNumber>=3000)(uidNumber<=3999)) "
```

Buscar usuaris pertanyents a un grup GID concret

```
ldapsearch -x -b "dc=clotfje,dc=net" "(&(objectClass=posixAccount)  
(gidNumber=1001)) "
```

Buscar usuaris amb el cognom que comença per "g"

```
ldapsearch -x -b "dc=clotfje,dc=net" "(&(objectClass=person)(sn=g*)) "
```

Cercar amb autenticació d'administrador

```
ldapsearch -x -D "cn=admin,dc=clotfje,dc=net" -W -b "dc=clotfje,dc=net"  
"(objectClass=*)" "
```

Sortida mínima LDIF (noms DN i atributs, sense comentaris)

```
ldapsearch -x -LLL -b "dc=clotfje,dc=net" "(objectClass=posixAccount)" uid  
uidNumber
```

Limitar la cerca a la unitat organitzativa ouUsuaris

```
ldapsearch -x -b "ou=ouUsuaris,dc=clotfje,dc=net" "(objectClass=posixAccount) "
```

Cercar en un servidor remot especificant la URI

```
ldapsearch -x -H ldap://192.168.1.2 -b "dc=clotfje,dc=net" "(uid=jpons) "
```

CONSELL: Afegiu -LLL a ldapsearch per obtenir la sortida més neta possible, sense comentaris ni número de versió LDIF. Molt útil per processar la sortida amb scripts Bash.

4 · ldapadd · Afegir entrades al directori

ldapadd llegeix un fitxer LDIF i afegiu les entrades que conte al directori LDAP. És equivalent a executar ldapmodify -a (mode d'afegir).

4.1 · Sintaxi general

```
ldapadd [opcions] -f fitxer.ldif
```

4.2 · Estructura d'un fitxer LDIF

Un fitxer LDIF (LDAP Data Interchange Format) conté una o més entrades separades per una línia en blanc:

```
# Comentari: línia ignorada pel parser
dn: uid=mgarcia,ou=ouUsuaris,dc=clotfje,dc=net
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: person
uid: mgarcia
cn: marc
sn: garcia
uidNumber: 3010
gidNumber: 1001
homeDirectory: /home/mgarcia
loginShell: /bin/bash
userPassword: Asix2Clot25!

# Segona entrada (separada per línia en blanc)
dn: uid=lmorales,ou=ouUsuaris,dc=clotfje,dc=net
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: person
uid: lmorales
cn: laura
sn: morales
uidNumber: 3011
gidNumber: 1001
homeDirectory: /home/lmorales
loginShell: /bin/bash
userPassword: Asix2Clot25@
```

4.3 · Exemples de ldapadd

Afegir entrades des d'un fitxer LDIF (amb contrasenya interactiva)

```
ldapadd -x -D "cn=admin,dc=clotfje,dc=net" -W -f usuarios.ldif
```

Afegir entrades amb contrasenya en text pla (per a scripts)

```
ldapadd -x -D "cn=admin,dc=clotfje,dc=net" -w fjeclot -f usuarios.ldif
```

Afegir una entrada des de la línia de comandes (sense fitxer)

```
ldapadd -x -D "cn=admin,dc=clotfje,dc=net" -W << EOF
dn: uid=psol,ou=ouUsuaris,dc=clotfje,dc=net
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: person
uid: psol
cn: pau
sn: soler
uidNumber: 3012
gidNumber: 1001
homeDirectory: /home/psol
loginShell: /bin/bash
userPassword: Asix2Clot25#
EOF
```

Afegir una unitat organitzativa

```
ldapadd -x -D "cn=admin,dc=clotfje,dc=net" -W << EOF
dn: ou=ouProfessors,dc=clotfje,dc=net
objectClass: top
objectClass: organizationalUnit
ou: ouProfessors
EOF
```

Afegir un grup posixGroup

```
ldapadd -x -D "cn=admin,dc=clotfje,dc=net" -W << EOF
dn: cn=gProfessors,ou=ouGrups,dc=clotfje,dc=net
objectClass: top
objectClass: posixGroup
cn: gProfessors
gidNumber: 1003
EOF
```

Afegir entrades des d'un servidor remot

```
ldapadd -x -H ldap://192.168.1.2 -D "cn=admin,dc=clotfje,dc=net" -W -f
nous_usuaris.ldif
```

ATENCIÓ: Si una entrada ja existeix al directori, ldapadd retornara un error "Already exists".
Utilitza ldapmodify per modificar entrades existents.

5 · ldapmodify · Modificar entrades existents

ldapmodify permet modificar atributs d'entrades existents al directori. El fitxer LDIF ha d'especificar el tipus de canvi amb el camp changetype.

5.1 · Sintaxi general

```
ldapmodify [opcions] -f canvis.ldif
```

5.2 · Tipus de changetype

changetype	Acció
modify	Modifica atributs d'una entrada existent
add	Afegeix una nova entrada (equivalent a ldapadd)
delete	Elimina una entrada (equivalent a ldapdelete)
modrdn	Canvia el RDN d'una entrada

5.3 · Operacions dins de changetype: modify

Operació	Acció
replace: atribut	Substitueix el valor actual per un de nou
add: atribut	Afegeix un nou valor a l'atribut (si admet múltiples)
delete: atribut	Elimina l'atribut de l'entrada

5.4 · Exemples de ldapmodify

Canviar el shell d'un usuari

```
# Fitxer canvi_shell.ldif:
dn: uid=alop,ou=ouUsuaris,dc=clotfje,dc=net
changetype: modify
replace: loginShell
loginShell: /bin/zsh

ldapmodify -x -D "cn=admin,dc=clotfje,dc=net" -W -f canvi_shell.ldif
```

Afegir un atribut nou (adreça de correu)

```
# Fitxer afegir_mail.ldif:
dn: uid=alop,ou=ouUsuaris,dc=clotfje,dc=net
changetype: modify
add: mail
mail: alop@clotfje.net

ldapmodify -x -D "cn=admin,dc=clotfje,dc=net" -W -f afegir_mail.ldif
```

Eliminar un atribut d'una entrada

```
# Fitxer eliminar_mail.ldif:
dn: uid=alop,ou=ouUsuaris,dc=clotfje,dc=net
changetype: modify
delete: mail

ldapmodify -x -D "cn=admin,dc=clotfje,dc=net" -W -f eliminar_mail.ldif
```

Modificar múltiples atributs en una sola operació (separats per -)

```
# Fitxer canvis_multiples.ldif:
dn: uid=alop,ou=ouUsuaris,dc=clotfje,dc=net
changetype: modify
replace: loginShell
loginShell: /bin/bash
-
replace: cn
cn: arnau lopez
-
add: mail
mail: alop@clotfje.net

ldapmodify -x -D "cn=admin,dc=clotfje,dc=net" -W -f canvis_multiples.ldif
```

Canviar el gidNumber d'un usuari

```
ldapmodify -x -D "cn=admin,dc=clotfje,dc=net" -w fjeclot << EOF
dn: uid=alop,ou=ouUsuaris,dc=clotfje,dc=net
changetype: modify
replace: gidNumber
gidNumber: 1002
EOF
```

Afegir un membre a un grup posixGroup

```
ldapmodify -x -D "cn=admin,dc=clotfje,dc=net" -W << EOF
dn: cn=gAdmins,ou=ouGrups,dc=clotfje,dc=net
changetype: modify
add: memberUid
memberUid: alop
EOF
```

Eliminar un membre d'un grup posixGroup

```
ldapmodify -x -D "cn=admin,dc=clotfje,dc=net" -W << EOF
dn: cn=gAdmins,ou=ouGrups,dc=clotfje,dc=net
changetype: modify
delete: memberUid
memberUid: alop
EOF
```

6 · ldapdelete · Eliminar entrades del directori

ldapdelete elimina una o mes entrades del directori LDAP a partir dels seus DN (Distinguished Names).

6.1 · Sintaxi general

```
ldapdelete [opcions] "dn_de_l_entrada"
```

6.2 · Opcions específiques de ldapdelete

Opció	Descripció
-r	Elimina l'entrada i tots els seus fills (recursiu)
-f fitxer	Llegeix la llista de DN a eliminar d'un fitxer de text

6.3 · Exemples de ldapdelete

Eliminar un usuari concret

```
ldapdelete -x -D "cn=admin,dc=clotfje,dc=net" -W \
"uid=alop,ou=ouUsuaris,dc=clotfje,dc=net"
```

Eliminar un grup

```
ldapdelete -x -D "cn=admin,dc=clotfje,dc=net" -W \
"cn=gUsuaris,ou=ouGrups,dc=clotfje,dc=net"
```

Eliminar múltiples entrades en una sola comanda

```
ldapdelete -x -D "cn=admin,dc=clotfje,dc=net" -W \
"uid=alop,ou=ouUsuaris,dc=clotfje,dc=net" \
"uid=jpons,ou=ouUsuaris,dc=clotfje,dc=net" \
"uid=jgim,ou=ouUsuaris,dc=clotfje,dc=net"
```

Eliminar entrades des d'un fitxer de DN's

```
# Crea el fitxer eliminar.txt amb un DN per línia:
cat > /tmp/eliminar.txt << EOF
uid=alop,ou=ouUsuaris,dc=clotfje,dc=net
uid=jpons,ou=ouUsuaris,dc=clotfje,dc=net
EOF

ldapdelete -x -D "cn=admin,dc=clotfje,dc=net" -W -f /tmp/eliminar.txt
```

Eliminar una unitat organitzativa i tot el seu contingut (recursiu)

```
ldapdelete -x -D "cn=admin,dc=clotfje,dc=net" -W -r \
"ou=ouUsuaris,dc=clotfje,dc=net"
```

ATENCIÓ: ldapdelete amb -r elimina totes les entrades filles sense demanar confirmació. Comprova sempre primer amb ldapsearch quines entrades seran afectades.

7 · Idappasswd · Canviar contrasenyes

Idappasswd permet canviar la contrasenya d'un usuari LDAP de forma segura, sense haver d'editar manualment l'atribut userPassword.

7.1 · Sintaxi general

```
ldappasswd [opcions] [dn_usuari]
```

7.2 · Opcions específiques de Idappasswd

Opció	Descripció
-s nova_pass	Especifica la nova contrasenya en text pla
-S	Demana la nova contrasenya de forma interactiva (mes segur)
-a pass_antiga	Especifica la contrasenya actual de l'usuari
-A	Demana la contrasenya actual de forma interactiva

7.3 · Exemples de Idappasswd

Canviar la contrasenya d'un usuari (admin la canvia)

```
ldappasswd -x -D "cn=admin,dc=clotfje,dc=net" -W \  
-s "NovaContrasenya25!" \  
"uid=alop,ou=ouUsuaris,dc=clotfje,dc=net"
```

Canviar contrasenya de forma interactiva (el propi usuari)

```
ldappasswd -x -D "uid=alop,ou=ouUsuaris,dc=clotfje,dc=net" \  
-W -S \  
"uid=alop,ou=ouUsuaris,dc=clotfje,dc=net" \  
# -W demana la contrasenya actual \  
# -S demana la nova contrasenya (dos cops per confirmar)
```

Canviar la contrasenya de l'administrador LDAP

```
ldappasswd -x -D "cn=admin,dc=clotfje,dc=net" -W \  
-s "NovaPassAdmin25!" \  
"cn=admin,dc=clotfje,dc=net"
```

Canviar contrasenyes de múltiples usuaris amb un script Bash

```
#!/bin/bash
# Canvia la contrasenya de tots els usuaris d'una llista
LDAP_ADMIN="cn=admin,dc=clotfje,dc=net"
LDAP_PASS="fjeclot"
LDAP_BASE="dc=clotfje,dc=net"

while IFS=',' read -r UID_NOM NOVA_PASS; do
  ldappasswd -x -D "$LDAP_ADMIN" -w "$LDAP_PASS" \
    -s "$NOVA_PASS" \
    "uid=${UID_NOM},ou=ouUsuaris,${LDAP_BASE}"
  echo "Contrasenya canviada: $UID_NOM"
done < canvi_contrasenyes.csv
# Format CSV: uid,nova_contrasenya
```

8 · ldapwhoami · Identificar la sessió activa

ldapwhoami retorna la identitat amb la qual s'ha autenticat al servidor LDAP. Es molt útil per verificar que les credencials son correctes.

8.1 · Exemples de ldapwhoami

Comprova la identitat de l'administrador

```
ldapwhoami -x -D "cn=admin,dc=clotfje,dc=net" -W
```

Sortida esperada: dn:cn=admin,dc=clotfje,dc=net

Comprova la identitat d'un usuari del domini

```
ldapwhoami -x -D "uid=alop,ou=ouUsuaris,dc=clotfje,dc=net" -W
```

Connexió anònima (sense autenticació)

```
ldapwhoami -x
```

Sortida esperada: dn:

9 · ldapmodrdn · Canviar el nom d'una entrada

ldapmodrdn permet reanomenar una entrada del directori canviant el seu RDN (Relative Distinguished Name), i opcionalment moure-la a una altra part de l'arbre.

9.1 · Sintaxi general

```
ldapmodrdn [opcions] "dn_actual" "nou_rdn"
```

9.2 · Opcions específiques de ldapmodrdn

Opció	Descripció
-r	Elimina l'antic valor del RDN de l'entrada
-s nou_pare	Mou l'entrada a un nou node pare (nova ubicació a l'arbre)

9.3 · Exemples de ldapmodrdn

Canviar el uid d'un usuari (reanomenar)

```
ldapmodrdn -x -D "cn=admin,dc=clotfje,dc=net" -W -r \  
"uid=alop,ou=ouUsuaris,dc=clotfje,dc=net" \  
"uid=arnaulopez"
```

Moure un usuari d'una OU a una altra

```
ldapmodrdn -x -D "cn=admin,dc=clotfje,dc=net" -W -r \  
-s "ou=ouAdmins,dc=clotfje,dc=net" \  
"uid=alop,ou=ouUsuaris,dc=clotfje,dc=net" \  
"uid=alop"
```

10 · slapcat i slapadd · Exportar i importar la base de dades

Aquestes eines actuen directament sobre la base de dades del servidor LDAP (slapd) sense passar pel protocol LDAP. S'executen al servidor i normalment requereixen que el servei slapd estigui aturat.

10.1 · slapcat · Exportar la base de dades

slapcat exporta totes les entrades de la base de dades LDAP en format LDIF. Es la millor eina per fer còpies de seguretat del directori.

Exportar tota la base de dades a la sortida estàndard

```
sudo slapcat
```

Exportar a un fitxer LDIF (backup)

```
sudo slapcat -l /tmp/backup_ldap_$(date +%Y%m%d).ldif
```

Exportar només la configuració del servidor (cn=config)

```
sudo slapcat -n 0 -l /tmp/backup_config.ldif
```

Exportar la base de dades de dades (índex 1)

```
sudo slapcat -n 1 -l /tmp/backup_dades.ldif
```

10.2 · slapadd · Importar entrades a la base de dades

slapadd importa entrades en format LDIF directament a la base de dades. Requereix que el servei slapd estigui ATURAT.

Importar un fitxer LDIF a la base de dades (slapd ha d'estar aturat)

```
sudo systemctl stop slapd
sudo slapadd -l /tmp/backup_ldap.ldif
sudo systemctl start slapd
```

Importar amb verificació i mode verbose

```
sudo systemctl stop slapd
sudo slapadd -v -l /tmp/backup_ldap.ldif
sudo systemctl start slapd
```

Script complet de backup diari amb slapcat

```
#!/bin/bash
# backup-ldap.sh - Backup diari de la base de dades LDAP
BACKUP_DIR="/mnt/copSeg/ldap"
DATA=$(date +%Y%m%d_%H%M%S)
FITXER="${BACKUP_DIR}/ldap_backup_${DATA}.ldif"

mkdir -p "$BACKUP_DIR"
sudo slapcat -l "$FITXER"

if [ $? -eq 0 ]; then
    echo "[$(date)] Backup LDAP creat: $FITXER ($(du -h $FITXER | cut -f1))"
    # Conserva noms els 7 backups mes recents
    ls -T ${BACKUP_DIR}/ldap_backup_*.ldif | tail -n +8 | xargs -r rm
else
    echo "[$(date)] ERROR en el backup LDAP" >&2
fi
```

ATENCIÓ: Quan s'usa slapadd per restaurar, el servei slapd HA D'ESTAR ATURAT. Si s'importa amb slapd en marxa, la base de dades pot corrompre's.

11 · Taula resum de totes les eines

Eina	Acció	Exemple ràpid
ldapsearch	Cercar entrades	ldapsearch -x -b "dc=..." "(uid=alop)"
ldapadd	Afegir entrades des de LDIF	ldapadd -x -D "cn=admin,..." -W -f fitxer.ldif
ldapmodify	Modificar atributs existents	ldapmodify -x -D "cn=admin,..." -W -f canvis.ldif
ldapdelete	Eliminar entrades	ldapdelete -x -D "cn=admin,..." -W "uid=alop,..."
ldappasswd	Canviar contrasenya d'usuari	ldappasswd -x -D "cn=admin,..." -W -s "Nova!" "uid=alop,..."
ldapwhoami	Verificar identitat autenticada	ldapwhoami -x -D "cn=admin,..." -W
ldapmodrdn	Canviar nom o moure entrada	ldapmodrdn -x -D "cn=admin,..." -W -r "uid=alop,..." "uid=nou"
slapcat	Exportar BD a LDIF (servidor)	sudo slapcat -l backup.ldif
slapadd	Importar LDIF a BD (servidor)	sudo slapadd -l backup.ldif