LDAP

~~ ## Conceptes generals de LDAP

Conceptes clau de configuració:

- El fitxer **slapd.conf** conté la configuració per generar la base de dades, però és un sistema deprecated.
- El directori **/etc/openldap/slapd.d** és on es desa la configuració en format d'estructura de directoris ldif. Es transforma en slaptest del fitxer de configuració al directori.
- El directori **/var/lib/ldap** és on es desa per defecte la informació, les dades de la base de dades. Si hi ha vàries bases de dades cal un directori diferent per a cada una.
- Es pot consultar (slapcat) i inserir dades massivament en offline (slapadd) amb el servei apagat.
- Per usar ordres LDAP client cal que el servei estigui engegat, i cal connectar al servidor **localhost** (a l'aula per defecte les ordres client consulten al servidor d'informàtica).

Conceptes claus de funcionament:

- Cal assdegurar-se que els permisos del directori /etc/openldap/slapd.d (i subarbre) i els de /var/lib/ldap (i subarbre) siguin propietat de l'usuari i grup ldap, és a dir **ldap.ldap**.
- Les dades es poden assignar a la base de dades amb ordres de servidor (slapadd) i amb ordres de client (ldapadd), que tenen característiques diferents.
- Sempre que es modifiqui la configuració del directori /etc/openldap/slapd.d o de les dades de /var/lib/ldap usant l'ordre slapadd cal tornar a assignar la propietat d'usuari i grup a ldap.ldap.
- La càrrega de dades intensiva (inicial per exemple) es fa accedint directament al backend (amb el servei offline) usant l'ordre slapadd.
- Amb el servei engegat es poden afegir dades a la base de dades amb l'ordre ldap client **ldapadd**. La comunicació és del client al servidor usant el protocol **LDAP**.
- Assegurar-se que les ordres client consulten al servidor LDAP apropiat, si no s'indica a les aules d'informàtica es consults al servidor d'informàtica (gandhi). Es recomana usar l'opció "**-h localhost:389**" per forçar l'ordre a consultar el propi servidor. ## Manual Creació bdd i inserció de dades.

1.**Creació container docker amb tot el necessari:**

```
[root@i14 ~]# docker run --name slapd01 -h slapd01 -it fedora:24 /bin/bash

Instal·lem els paquets que necessitarem durant tota la práctica:
```

```
[root@slapd01 /]# dnf -y install vim procps iputils iproute xinetd openldap openldap-servers

[root@slapd01 /]# mkdir /opt/docker
```

Al nostre pc:

```
[isx41536245@i14 ~]$ cd /home/groups/inf/hisx2/M06-ASO/01-ldap_basic/
[isx41536245@i14 01-ldap_basic]$ ll
total 28
-rw-r--r-- 1 ecanet hisx2  845 Oct 19  2016 DB_CONFIG
-rw-r--r-- 1 ecanet hisx2 5924 Dec 12 11:14 organitzacio-altres_edt.org.ldif
-rw-r--r-- 1 ecanet hisx2  492 Sep 23  2014 organitzacio_edt.org.ldif
-rw-r--r-- 1 ecanet hisx2 1361 Sep 20  2016 slapd-edt.org.conf
-rw-r--r-- 1 ecanet hisx2 2359 Sep 23  2014 usuaris_edt.org.ldif
-rw-r--r-- 1 ecanet hisx2 3704 Oct  2  2015 usuaris-mes_edt.org.ldif
```

Copiem aquests arxius al docker:

```
[root@i14 01-ldap_basic]# mkdir /var/tmp/docker
[root@i14 01-ldap_basic]# cp * /var/tmp/docker


[root@i14 01-ldap_basic]# docker cp . slapd01:/opt/docker
lstat /home/groups/inf/hisx2/M06-ASO: permission denied
[root@i14 01-ldap_basic]# cd /var/tmp/docker/

[root@i14 docker]# docker cp . slapd01:/opt/docker
```

2.**Verificació de carpetes i arxius:**

Esborrem les bases de dades existens al ldap (les que venen per defecte):

```
[root@slapd01 /]# rm -rf /etc/openldap/slapd.d/*
```

Copiem la configuració i estructura de la bbdd que crearem al directori corresponent:

```
[root@slapd01 /]# cp /opt/docker/DB_CONFIG /var/lib/ldap/.
```

Nota: recordar que cal tenir en compte que si anessim a crear més d'una bbdd cada una hauria d'anar a directoris diferents.

El fitxer slapd-edt.org.conf conté les dades que ens disposem a carregar. Cal tenir present les línies següents:

```
database bdbz
suffix "dc=edt,dc=org" --> nom de la base de dades.
rootdn "cn=Manager,dc=edt,dc=org" --> Manager serà usuari administrador.
rootpw secret --> Password que definim a Manager.
directory /var/lib/lda --> directori on estarà la base de dades.
```

SLAPTEST

Eina de verificació de que el fitxer de configuració és correcte.

```
[root@slapd01 /]# slaptest -v -u -f /opt/docker/slapd-edt.org.conf

[root@slapd01 /]# slaptest -v -u -F /etc/openldap/slapd.d/
slaptest: bad configuration directory!

[root@slapd01 /]# slaptest -v -f /opt/docker/slapd-edt.org.conf -F /etc/openldap/slapd.d/
5a2fb360 bdb_db_open: database "dc=edt,dc=org": db_open(/var/lib/ldap/id2entry.bdb) failed:
5a2fb360 backend_startup_one (type=bdb, suffix="dc=edt,dc=org"): bi_db_open failed! (2)
slap_startup failed (test would succeed using the -u switch)
```

Opcions de slaptest:

- -v : verbose –> per veure els missatges.
- -u: engega el mode "dry-run". És a dir: no fallis si la base de dades no es pot obrir però la configuració és bona.
- -f: especifica un fitxer alternatiu al slapd.conf
- -F: especifica un directori de configuració. Si s'especifiquen amb -f i -F, el fitxer de configuració es llegirà i es convertirà al format del directori de configuració i s'escriurà al directori especificat. Si no s'especifica cap opció, slaptest intentarà llegir el directori de configuració predeterminat abans d'intentar utilitzar el fitxer de configuració predeterminat. Si existeix un directori de configuració vàlid, s'omet el fitxer de configuració predeterminat. Si el mode d'ús sec també s'especifica, no es produirà cap conversió. ***

3.**Càrrega de dades:**

```
[root@slapd01 /]# slapadd -v -F /etc/openldap/slapd.d -l /opt/docker/organitzacio_edt.org.lc
added: "dc=edt,dc=org" (00000001)
added: "ou=maquines,dc=edt,dc=org" (00000002)
added: "ou=clients,dc=edt,dc=org" (00000003)
added: "ou=productes,dc=edt,dc=org" (00000004)
_################### 100.00% eta   none elapsed            none fast!
Closing DB...
```

Ens ha carregat correctament les dades.

4.**Canvi de permisos:**

Recordem que s'han de canviar els permisos:

```
[root@slapd01 /]# chown -R ldap.ldap /var/lib/ldap/
[root@slapd01 /]# chown -R ldap.ldap /etc/openldap/slapd.d/
```

5.**Engegar el servei:**

Al docker no podem fer un systemctl start slapd.service. Llavors l'opció que tenim és:

```
[root@slapd01 /]# updatedb
[root@slapd01 /]# locate slapd.service
/usr/lib/systemd/system/slapd.service
[root@slapd01 /]# vim /usr/lib/systemd/system/slapd.service
```

Amb la línia de la variable ExecStart=/usr/sbin/slapd -u ldap -h "ldap:/// ldaps:/// ldapi:///" és com engegarem el servei.

```
[root@slapd01 /]# /usr/sbin/slapd -u ldap -h "ldap:/// ldaps:/// ldapi:///"
[root@slapd01 /]# ps ax
  PID TTY      STAT   TIME COMMAND
    1 ?        Ss     0:00 /bin/bash
  370 ?        Ssl    0:00 /usr/sbin/slapd -u ldap -h ldap:/// ldaps:/// ldapi:///
  372 ?        R+     0:00 ps ax
```

Consultar la base de dades (client).

LDAPSEARCH

```
[root@slapd01 /]# ldapsearch -x -h localhost -LLL -b 'dc=edt,dc=org'
dn: dc=edt,dc=org
dc: edt
description: Escola del treball de Barcelona
objectClass: dcObject
objectClass: organization
o: edt.org

dn: ou=maquines,dc=edt,dc=org
ou: maquines
description: Container per a maquines linux
objectClass: organizationalunit
```

Opcions de ldapsearch:

- -x: autenticació simple en comptes de SASL.
- -h: ldaphost. Especifica un host alternatiu en el que s'estigui executant ldap server.
- -LLL: serveix per restringir la sortida a ldif v1 (-L), la segona -L deshabilita els comentaris. I la tercera -L deshabilita printar la versió de ldif.
- -b: Utilitzeu la base de cerca com a punt de partida de la cerca en comptes de la predeterminada.
- +: si afegim el + al final ens mostrarà també els atributs funcionals. ***

Si volem fer un ldapsearch des del nostre host:

```
[root@i14 docker]# ldapsearch -x -h 172.16.0.2 -LLL -b 'dc=edt,dc=org' dn
dn: dc=edt,dc=org
```

Més exemples:

```
[root@slapd01 /]# ldapsearch -x -h localhost -LLL -b 'dc=edt,dc=org' dn cn

[root@slapd01 /]# ldapsearch -x -h localhost -LLL -b 'dc=edt,dc=org' dn *

[root@slapd01 /]# ldapsearch -x -h localhost -LLL -b 'dc=edt,dc=org' +
```

Condicions de filtrat amb ldapsearch.

Filtrar pel common name (cn=Pau Pou):

```
[root@slapd01 /]# ldapsearch -x -h localhost -LLL -b 'dc=edt,dc=org' 'cn=Pau Pou'
dn: cn=Pau Pou,ou=usuaris,dc=edt,dc=org
```

Filtrar pel common name i mostrar el dn i la descripció de l'usuari:

```
[root@slapd01 /]# ldapsearch -x -h localhost -LLL -b 'dc=edt,dc=org' 'cn=Pau Pou' dn descrip
dn: cn=Pau Pou,ou=usuaris,dc=edt,dc=org
description: Watch out for this guy
```

Mostrar el home phone de tots els users

```
Tots els home phones:

[root@slapd01 /]# ldapsearch -x -h localhost -LLL -b 'dc=edt,dc=org' dn homePhone

Els que comencin per 555:

[root@slapd01 /]# ldapsearch -x -h localhost -LLL -b 'dc=edt,dc=org' dn homePhone 'homePhone
```

Mostrar el git number de tots els users:

```
[root@slapd01 /]# ldapsearch -x -h localhost -LLL -b 'dc=edt,dc=org' dn gidNumber
```

Buscar els users que tenen el gid 600 i el cognom Pou:

```
[root@slapd01 /]# ldapsearch -x -h localhost -LLL -b 'dc=edt,dc=org' '(&(cn=* Pou)(gidNumber
```

La mateixa que abans però amb OR i no amb AND:

```
[root@slapd01 /]# ldapsearch -x -h localhost -LLL -b 'dc=edt,dc=org' '(|(cn=* Pou)(gidNumber
```

Llistar els Pou i els Mas amb gid number 600:

```
[root@slapd01 /]# ldapsearch -x -h localhost -LLL -b 'dc=edt,dc=org' '(|(cn=* Pou)(cn=* Mas)
```

Llistar els gid diferents de 600:

```
[root@slapd01 /]# ldapsearch -x -h localhost -LLL -b 'dc=edt,dc=org' '(!(gidNumber=60))' dn
```

Modificació del base search:

- **Base**: s'aplica la consulta a una sola entitat, en aquest cas la base.

```
[root@slapd01 /]# ldapsearch -x -h localhost -LLL -s base -b 'ou=usuaris,dc=edt,dc=org'
dn: ou=usuaris,dc=edt,dc=org
```

- **One**: mostra el primer sub-nivell.

```
[root@slapd01 /]# ldapsearch -x -h localhost -LLL -s one -b 'ou=usuaris,dc=edt,dc=org'

[root@slapd01 /]# ldapsearch -x -h localhost -LLL -s one -b 'dc=edt,dc=org' dn
```

- **Sub**: és l'opció per defecte i ho llista tot a partir del . :

```
[root@slapd01 /]# ldapsearch -x -h localhost -LLL -s sub -b 'ou=usuaris,dc=edt,dc=org'

[root@slapd01 /]# ldapsearch -x -h localhost -LLL -s sub -b 'dc=edt,dc=org' dn
```

- **Children**: tots els descendents menys la base.

```
[root@slapd01 /]# ldapsearch -x -h localhost -LLL -s children -b 'ou=usuaris,dc=edt,dc=
```

Afegir més dades en calent (client).

LDAPADD

ldapmodify obre una connexió a un servidor LDAP, s'uneix i modifica o afegeix entrades. La informació d'entrada es llegeix des de l'entrada estàndard o des del fitxer mitjançant l'ús de l'opció -f.

```
[root@slapd01 /]# ldapadd -v -x -h localhost -D "cn=Manager,dc=edt,dc=org" -w secret -f /opt

[root@slapd01 /]# ldapadd -x -h localhost -D "cn=Manager,dc=edt,dc=org" -w secret -f /opt/do
adding new entry "ou=usuaris,dc=edt,dc=org"
ldap_add: Already exists (68)

[root@slapd01 /]# ldapsearch -x -h localhost -LLL -b 'dc=edt,dc=org' dn
dn: dc=edt,dc=org
```

Afegir un usuari concret:

Ens creem un altre fitxer i hi afegim les dades del Jordi Mas que ahir vam esborrar (està al fitxer usuaris_edt...).

Ara l'afegirem de nou:

```
[root@slapd01 docker]# ldapadd -x -h localhost -D 'cn=Manager,dc=edt,dc=org' -w secret -f da
adding new entry "cn=Jordi Mas,ou=usuaris,dc=edt,dc=org"
```

Opcions de ldapadd:

- -v: verbose.
- -x: autenticació simple en comptes de SASL.
- -h: ldaphost. Especifica un host alternatiu en el que s'estigui executant ldap server.
- -D: per especificar el distinguished name en la base de dades.
- -w passwd: seguit de la password de l'usuari amb el que ens autentiquem.
- -W: el prompt ens demanarà la password.
- -f file: llegirà la informació modificada del fitxer en lloc de passar-la per l'entrada estàndar. ***

Les comandes **ldapXXXXX** són utilitzades pel client per introduïr dades quan estem connectats. Des del servidor, i en mode **offline**, ho hem de fer amb les comandes **slapXXXX**.

Esborrar dades.

LDAPDELETE

Esborrar un usuari:

```
[root@slapd01 /]# ldapdelete -x -h localhost -D 'cn=Manager,dc=edt,dc=org' -W 'cn=Jordi Mas,
Enter LDAP Password:
```

Creem un altre fitxer dades02 i hi afegim els dn del Pau i Pere Pou

```
[root@slapd01 docker]# ldapdelete -x -h localhost -D 'cn=Manager,dc=edt,dc=org' -W -f dades0
```

```
cn=Pau Pou,ou=usuaris,dc=edt,dc=org
cn=Pere Pou,ou=usuaris,dc=edt,dc=org
```

```
[root@slapd01 docker]# ldapdelete -x -h localhost -D 'cn=Manager,dc=edt,dc=org' -W -f   dade
Enter LDAP Password:
```

També podem esborrar de cop dos usuaris passant-li per argument el dn de cada un d'aquests usuaris.

```
[root@slapd01 docker]# ldapdelete -x -h localhost -D 'cn=Manager,dc=edt,dc=org' -W  "cn=Anna
```

Modificar dades.

LDAPMODIFY

El primer pas sería crear-nos un arxiu de modificació:

```
[root@slapd01 docker]# vim dada01.ldif
```

Si volem introduir totes les dades d'un usuari:

```
dn: cn=Jordi Mas,ou=usuaris,dc=edt,dc=org
changetype: add
objectclass: posixAccount
objectclass: inetOrgPerson
cn: Jordi Mas
cn: Giorgios Mas
sn: Mas
homephone: 555-222-2224
mail: jordi@edt.org
description: Watch out for this girl
ou: Alumnes
ou: Profes
uid: jordi
uidNumber: 5004
gidNumber: 100
homeDirectory: /tmp/home/jordi
userPassword: {SSHA}T5jrMgpJwZZgu0azkLIVoYhiG08/KGUv
```

Esborrar un usuari:

```
dn: cn=user10,ou=usuaris,dc=edt,dc=org
changetype: delete
```

a) Modificar les dades de l'usuari 9 reemplaçant el seu mail per un de nou.

   dn: cn=user09,ou=usuaris,dc=edt,dc=org changetype: modify replace: mail mail: newmail@binladen.155

   •

b) Esborrar la description de l'user 9.

   ### delete: description

c) Afegir nous home phones a l'user 9:

   add: homePhone homePhone: 111-111-111 homePhone: 111-111-112

   •

d) Afegir nous common names a l'user 9:

   add: cn cn: lo puto crac cn: hola user cn: lo usuari de proves

Format dels fitxers de modificació:

Registres d'entrada:

Els registres d'entrada LDIF s'utilitzen per representar entrades de directori. La forma bàsica d'un registre d'entrada és:

```
dn: <distinguished name>
   <attrdesc>: <attrvalue>
   <attrdesc>: <attrvalue>
   <attrdesc>:: <base64-encoded-value>
   <attrdesc>:< <URL>
   ...
```

Es pot continuar amb una línia començant la següent línia amb un sol espai o una tabulació:

```
dn: cn=Barbara J Jensen,dc=exam
        ple,dc=com
```

Modificació de registres:

Els registres de canvi LDIF s'utilitzen per representar les sol·licituds de canvi de directori. Cada registre de canvis comença amb la línia que indica el nom distingit de l'entrada que es modifica:

```
dn: <distinguishedname>
changetype: <[modify|add|delete|modrdn]>
```

Finalment, es dóna la informació del canvi, el format del qual depèn de quin tipus de canvi s'ha especificat anteriorment. Per obtenir un tipus de canvi de modificació, el format és un o més dels següents:

```
add: <attributetype>
<attrdesc>: <value1>
<attrdesc>: <value2>
...
-
```

O, per a una modificació de substitució:

```
replace: <attributetype>
<attrdesc>: <value1>
<attrdesc>: <value2>
...
-
```

Si no es donen línies d'atributs per reemplaçar, l'atribut sencer s'ha de suprimir (si és present).

O bé, per a una modificació de supressió:

```
delete: <attributetype>
<attrdesc>: <value1>
<attrdesc>: <value2>
```

```
...
-
```

Si no es donen línies d'atributs per suprimir, s'haurà de suprimir tot l'atribut.

Per a un changetype de tipus add, el format és el següent:

```
<attrdesc1>: <value1>
<attrdesc1>: <value2>
...
<attrdescN>: <value1>
<attrdescN>: <value2>
```

Per obtenir un tipus de canvi modrdn o moddn, el format és:

```
newrdn: <newrdn>
deleteoldrdn: 0 | 1
newsuperior: <DN>
```

on un valor de 1 per deleteoldrdn significa eliminar els valors que formen el rdn antic de l'entrada i un valor de 0 significa deixar els valors com a atributs no distingits a l'entrada. La línia newsuperior és opcional i, si està present, especifica el nou superior per moure l'entrada.

Modificar el dn d'un usuari amb el changetype modrdn

```
vim dades02.ldif

dn: cn=user09,ou=usuaris,dc=edt,dc=org
changetype: modify
add: description
description: segona descripcio de l'usuari
-
replace: mail
mail: renou@email.cat
-
delete: homePhone

dn: cn=user09,ou=usuaris,dc=edt,dc=org
changetype: modrdn
newrdn: cn=superuser09
deleteoldrdn:0 --> si volem mantenir o no l'antic cn. Si el mantenim s'afegirà a l'antic
```

I tot seguit fem un ldapmodify:

```
[root@slapd01 docker]# ldapmodify -v -x -h localhost -D 'cn=Manager,dc=edt,dc=org' -W -f dad
```

Més exemples de modificació:

```
vim dades03.ldif
```

```
dn: cn=superuser09,ou=usuaris,dc=edt,dc=org
changetype: modify
add: mail
mail: mail2@edt.org
mail: mail3@edt.org
mail: mail4@edt.org

dn: cn=superuser09,ou=usuaris,dc=edt,dc=org
changetype: modrdn
newrdn: cn=louser09
deleteoldrdn:1 --> amb el valor 1 li diem que no mantingui l'anterior cn.

dn: cn=louser09,ou=usuaris,dc=edt,dc=org
changetype: modify
delete: mail
mail: mail3@edt.org
```

Per a un tipus de canvi de supressió, no es necessita informació addicional al registre.

Exemple del man:

```
dn: cn=Babs Jensen,dc=example,dc=com
changetype: add
objectclass: person
objectclass: extensibleObject
cn: babs
cn: babs jensen
sn: jensen

dn: cn=Babs Jensen,dc=example,dc=com
changetype: modify
add: givenName
givenName: Barbara
givenName: babs
-
replace: description
description: the fabulous babs
-
delete: sn
sn: jensen
-

dn: cn=Babs Jensen,dc=example,dc=com
changetype: modrdn
newrdn: cn=Barbara J Jensen
```

```
deleteoldrdn: 0
newsuperior: ou=People,dc=example,dc=com

dn: cn=Barbara J Jensen,ou=People,dc=example,dc=com
changetype: delete
```

Comparació de registres:

LDAPCOMPARE

Li estem preguntant si louser09 té un email usr@edt.org. I ens contesta que no.

```
[root@slapd01 docker]# ldapcompare -x "cn=louser09,ou=usuaris,dc=edt,dc=org" mail:usr@edt.or
FALSE
```

```
[root@slapd01 docker]# ldapcompare -x "cn=louser09,ou=usuaris,dc=edt,dc=org" mail:mail2@edt.
TRUE

[root@slapd01 docker]# ldapcompare -x "cn=louser09,ou=usuaris,dc=edt,dc=org" "cn:lo puto cra
FALSE
```

LDAPWHOAMI

Al docker:

```
[root@slapd01 docker]# ldapwhoami -x
anonymous

[root@i14 docker]# ldapwhoami -x
anonymous
    Li acabem de preguntar a ghandi

[root@i14 docker]# ldapwhoami -x -h 172.17.0.2
anonymous
    Li acabem de preguntar al docker

[root@slapd01 docker]# ldapwhoami -x -h localhost -W -D "cn=louser09,ou=usuaris,dc=edt,dc=or

password = jupiter
```

Al nostre pc:

```
[root@i14 docker]# ldapwhoami -x -h 172.17.0.2 -W -D "cn=louser09,ou=usuaris,dc=edt,dc=org"
Enter LDAP Password:
dn:cn=louser09,ou=usuaris,dc=edt,dc=org
 password = jupiter
```

Al nostre compte d'usuari:

```
[isx41536245@i14 ~]$ ldapsearch -x -LLL dn
```

Amb això acabem de llistar tots els usuaris de gandhi!!!

El meu compte:

```
[isx41536245@i14 ~]$ ldapsearch -x -LLL -b "uid=isx41536245,ou=users,ou=inf,dc=escoladeltreb
dn: uid=isx41536245,ou=users,ou=inf,dc=escoladeltreball,dc=org
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: sambaSamAccount
cn: isx41536245
sn: Miquel Ferran Esteva Thomas
uid: isx41536245
mail: isx41536245@correu.escoladeltreball.org
uidNumber: 101080
gidNumber: 100096
homeDirectory: /home/users/inf/hisx2/isx41536245
loginShell: /bin/bash
gecos: isx41536245
description: User: isx41536245; Group: hisx2; Domain: inf
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaSID: S-1-5-21-1935048863-3121341026-513757114-203160
sambaPrimaryGroupSID: S-1-5-21-1935048863-3121341026-513757114-513
sambaHomeDrive: P:
sambaAcctFlags: [U          ]
displayName: Miquel Ferran Esteva Thomas
sambaLogonScript: hisx2.BAT
sambaPwdCanChange: 2147483647
sambaPwdMustChange: 2147483647
sambaPwdLastSet: 62701200

[isx41536245@i14 ~]$ getent passwd isx41536245
isx41536245:*:101080:100096:isx41536245:/home/users/inf/hisx2/isx41536245:/bin/bash
```

Això està al ldap de gandhi

```
[isx41536245@i14 ~]$ getent group inf
inf:*:100000:gmartinez,rbruballa,jandugar,jordinas,mramirez,sgarrido,jamoros,jmendez,llriera
[isx41536245@i14 ~]$ getent group hisx2
```

```
hisx2:*:100096:isx26067826,isx39441584,isx41536245,isx41745190,isx45128227,isx47408534,isx47
```

LDAPPASSWD

Utilitzarem per modificar la password d'un usuari (sempre i quan tinguem permisos).

```
[root@slapd01 docker]# ldappasswd -v -x -D 'cn=Manager,dc=edt,dc=org' -W "cn=Jordi Mas,ou=us
```

Per canviar el password utilitzarem -S. Sense -S li establirá un password aleatori.
-s minúscula introduïras tu la password a la línia de comandes.

```
[root@slapd01 docker]# ldappasswd -v -x -D "cn=Manager,dc=edt,dc=org" -w secret -S "cn=Jordi
New password:
Re-enter new password:
ldap_initialize( <DEFAULT> )
Result: Success (0)
```

(li hem posat com a passwd jordi).

Anem a comprovar que hem canviat la passwd:

```
[root@slapd01 docker]# ldapwhoami -x -v -h localhost -D "cn=Jordi Mas,ou=usuaris,dc=edt,dc=o
ldap_initialize( ldap://localhost )
Enter LDAP Password:
dn:cn=Jordi Mas,ou=usuaris,dc=edt,dc=org
Result: Success (0)
```

Com a manager no ens ha demanat la passwd anterior que tenia Jordi Mas. Ara anem a canviar la passwd com a Jordi Mas

```
[root@slapd01 docker]# ldappasswd -v -x -D "cn=Jordi Mas,ou=usuaris,dc=edt,dc=org" -W -s kak
ldap_initialize( <DEFAULT> )
Enter LDAP Password:
Result: Success (0)

[root@slapd01 docker]# ldappasswd -v -x -D "cn=Jordi Mas,ou=usuaris,dc=edt,dc=org" -W -s kak
```

Amb el -s li indiquem la nova passwd.

```
[root@slapd01 docker]# ldapwhoami -x -v -h localhost -D "cn=Jordi Mas,ou=usuaris,dc=edt,dc=o
ldap_initialize( ldap://localhost )
Enter LDAP Password:
ldap_bind: Invalid credentials (49)
[root@slapd01 docker]# ldapwhoami -x -v -h localhost -D "cn=Jordi Mas,ou=usuaris,dc=edt,dc=o
ldap_initialize( ldap://localhost )
Enter LDAP Password:
dn:cn=Jordi Mas,ou=usuaris,dc=edt,dc=org
Result: Success (0)

[root@slapd01 docker]# ldappasswd -v -x -D "cn=Jordi Mas,ou=usuaris,dc=edt,dc=org" -W -s jor
ldap_initialize( <DEFAULT> )
```

```
Enter LDAP Password:
Result: Success (0)
```

Provem ara a canviar la passwd d'un altre usuari amb el compte del jordi mas:

```
root@slapd01 docker]# ldappasswd -v -x -D "cn=Jordi Mas,ou=usuaris,dc=edt,dc=org" -W -s joro
ldap_initialize( <DEFAULT> )
Enter LDAP Password:
Result: Insufficient access (50)
```

Introducció de dades en calent (server):

SLAPADD

Slapadd s'utilitza per afegir entrades especificades en el Format d'intercanvi de directoris LDAP (LDIF) a una base de dades slapd (8). Obre la base de dades determinada pel número o sufix de la base de dades i afegeix les entrades corresponents al LDIF proporcionat a la base de dades. Les bases de dades configurades com subordinades d'aquesta també s'actualitzen, tret que s'especifiqui -g. L'entrada LDIF es llegeix des de l'entrada estàndard o el fitxer especificat.

```
[root@slapd01 /]# slapadd -v -F /etc/openldap/slapd.d/ -l /opt/docker/usuaris-mes_edt.org.ld
5a2fbcbf bdb_db_open: database "dc=edt,dc=org": unclean shutdown detected; attempting recove
added: "cn=user01,ou=usuaris,dc=edt,dc=org" (0000000c)
added: "cn=user02,ou=usuaris,dc=edt,dc=org" (0000000d)
added: "cn=user03,ou=usuaris,dc=edt,dc=org" (0000000e)
added: "cn=user04,ou=usuaris,dc=edt,dc=org" (0000000f)
added: "cn=user05,ou=usuaris,dc=edt,dc=org" (00000010)
added: "cn=user06,ou=usuaris,dc=edt,dc=org" (00000011)
added: "cn=user07,ou=usuaris,dc=edt,dc=org" (00000012)
added: "cn=user08,ou=usuaris,dc=edt,dc=org" (00000013)
added: "cn=user09,ou=usuaris,dc=edt,dc=org" (00000014)
added: "cn=user10,ou=usuaris,dc=edt,dc=org" (00000015)
_################### 100.00% eta   none elapsed            none fast!
Closing DB...
```

Hem de tenir en compte que en afegir dades en calent estem modificant directament la carpeta on es troba la base de dades /etc/openldap/slapd.d). Llavors, si tot seguit intentem engegar no ens deixarà ja que s'han canviat els permisos. Així, haurem de tornar a canviarlos.

```
[root@slapd01 /]# chown -R ldap.ldap /var/lib/ldap/
```

Ara ja sí ens deixa engegar el servei. *** Opcions de slapadd:

- -v: verbose
- -F confdir: especifica el directori de configuració.

- -l ldif-file: llegeix el ldif de l'arxiu especificat en lloc de l'entrada estàndar. ***

Ordres del servidor.

SLAPCAT

```
[root@slapd01 docker]# slapcat -n0
```

Això mostra la base de dades "motor" del servidor ldap. Conté tota la informació per a la correcta "construcció" de les bases de dades. És a dir, conté tota la configuració del dimoni de l'slapd.

```
dn: olcDatabase={1}bdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcBdbConfig
olcDatabase: {1}bdb
olcSuffix: dc=edt,dc=org
olcAccess: {0}to *  by self write  by * read
```

Aquesta sería la bbdd que nosaltres hem creat.

```
olcRootDN: cn=Manager,dc=edt,dc=org
olcRootPW:: c2VjcmV0
```

I aquí hem definit qui será el "puto amo"

```
olcDbDirectory: /var/lib/ldap
```

Directori de configuració.

```
olcDbIndex: objectClass pres,eq
olcDbLinearIndex: FALSE
```

Aquí definirem els índex de la bbdd.

SLAPPASSWD

```
[root@slapd01 docker]# slappasswd -h {md5}
New password:
Re-enter new password:
{MD5}J6UUjqD73a4i2QK+qaGVMQ==
```

Ordre que genera un passwd encriptat segons el format que li indiquem {md5} *** Tipus d'encriptacions:

-h "scheme" If -h is specified, one of the following RFC 2307 schemes may be specified: {CRYPT}, {MD5}, {SMD5}, {SSHA}, and {SHA}. The default is {SSHA}. Note that scheme names may need to be protected, due to { and }, from expansion by the user's command interpreter.

{SHA} and {SSHA} use the SHA-1 algorithm (FIPS 160-1), the latter with a seed.

{MD5} and {SMD5} use the MD5 algorithm (RFC 1321), the latter with a seed.

{CRYPT} uses the crypt(3).

{CLEARTEXT} indicates that the new password should be added to userPassword as clear text. Unless {CLEARTEXT} is used, this flag is incompatible with option -g. ***

Configuració dinàmica del servidor

```
[root@slapd01 docker]# vim slapd-cn=config-edt.org.conf
```

Afegim al fitxer slapd-edt.org-conf les tres línies:

```
database config
rootdn "cn=Sysadmin,cn=config"
rootpw syskey

[root@slapd01 docker]# rm -rf /etc/openldap/slapd.d/*

[root@slapd01 docker]# slaptest -f slapd-config-edt.org.conf -F /etc/openldap/slapd.d/

[root@slapd01 docker]# chown -R ldap.ldap /var/lib/ldap/
[root@slapd01 docker]# chown -R ldap.ldap /etc/openldap/slapd.d/


[root@slapd01 docker]# ldapsearch -x -h localhost -LLL -D 'cn=Sysadmin,cn=config' -w syskey
```

Configuració múltibles bases de dades.

Practicar creant múltiples bbdd amb els fitxers de configuració corresponents.