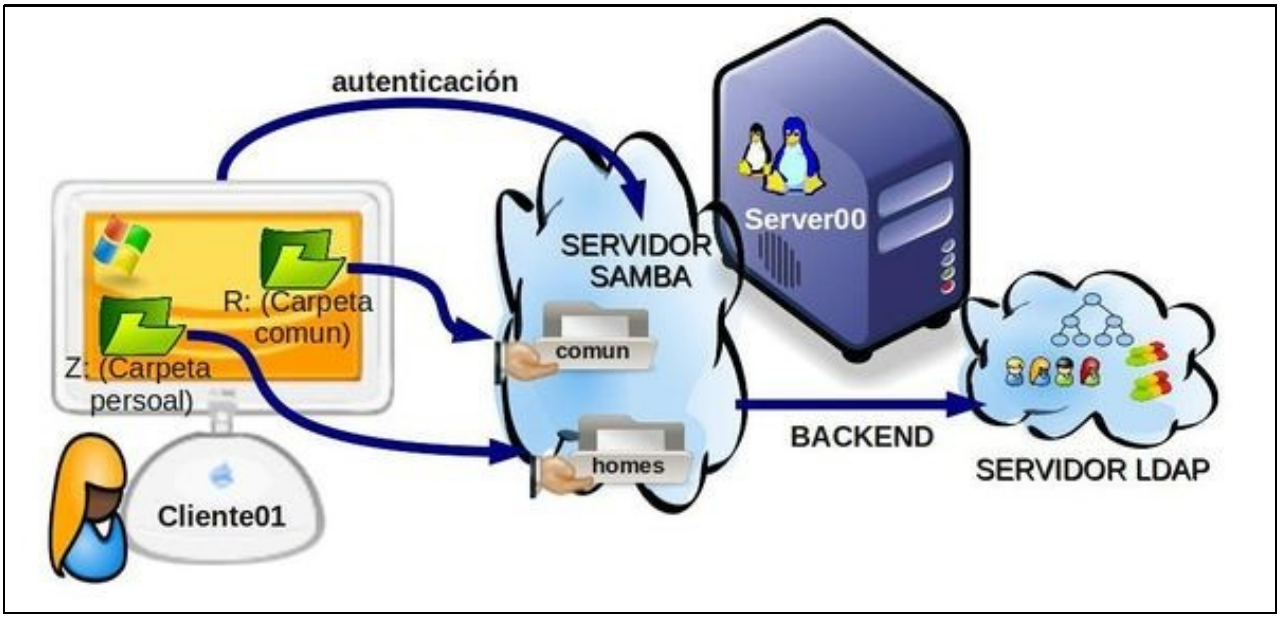
1 Instalación do servidor samba. Configuración LDAP

1.1 Sumario

1.2 Introdución

- Neste apartado abordaremos os pasos necesarios para instalar o servidor Samba e configuralo para que use como base de datos de usuarios o servidor LDAP.
- Pero en primeiro lugar, teremos que engadir no LDAP o esquema de samba, que define unha serie de atributos que o servidor samba precisará almacenar para as propiedades dos usuarios do dominio Windows.

- Imos configurar o servidor SAMBA para que use como backend o servizo LDAP.



1.3 Instalación do servidor Samba

- Imos instalar tres paquetes:
    - servidor samba,
    - a documentación
    - utilidades para xestionar os usuarios e grupos de samba no LDAP:

```
apt-get install samba smbldap-tools winbind smbclient samba-testsuite samba-common-bin samba-common registry-tools libsmbclient libp
```

- Podemos comprobar que a versión do paquete instalado é a 4.X, aínda que o usaremos en modo de compatibilidade de Samba3:

```
root@dserver00:~# samba --version
Version 4.X.X-Debian
```

1.4 Configurar o servidor LDAP para servir de base de datos de samba

1.4.1 Incluír o esquema de samba no servidor LDAP

- Para incluír o esquema no servizo LDAP, precisamos realizar unha serie de pasos:

1.4.1.1 Copiar o ficheiro samba.schema a /etc/ldap e estudo do mesmo

- O paquete **samba-doc** inclúe o esquema de samba para o LDAP en formato *schema*,
- Así que, descomprimirémolo a /etc/ldap/schema e converterémolo a formato LDIF para introducir o esquema no LDAP.

- Descomprimimos o ficheiro co esquema samba:

```
zcat /usr/share/doc/samba/examples/LDAP/samba.schema.gz > /etc/ldap/schema/samba.schema
```

- O contido do esquema pódese ver en: samba.schema

- Imos ver os **objectClass** que define:

```
cat /etc/ldap/schema/samba.schema | grep objectclass
 ## 1.3.6.1.4.1.7165.2.2.x - objectclasses
 ## 1.3.6.1.4.1.7165.2.3.2.x - objectclasses
 ## 1.3.6.1.4.1.7165.4.2.x - objectclasses
 ##   objectclass ( 1.3.6.1.4.1.7165.2.2.XX NAME ....
 ##    <attributetype|objectclass> ( 1.3.6.1.4.1.7165.2.XX.XX NAME ....
 ## The smbPasswordEntry objectclass has been depreciated in favor of the
 ## sambaAccount objectclass
 #objectclass ( 1.3.6.1.4.1.7165.2.2.1 NAME 'smbPasswordEntry' SUP top AUXILIARY
 #objectclass ( 1.3.6.1.4.1.7165.2.2.2 NAME 'sambaAccount' SUP top STRUCTURAL
 #objectclass ( 1.3.6.1.4.1.7165.2.2.3 NAME 'sambaAccount' SUP top AUXILIARY
 objectclass ( 1.3.6.1.4.1.7165.2.2.6 NAME 'sambaSamAccount' SUP top AUXILIARY
 objectclass ( 1.3.6.1.4.1.7165.2.2.4 NAME 'sambaGroupMapping' SUP top AUXILIARY
 objectclass ( 1.3.6.1.4.1.7165.2.2.14 NAME 'sambaTrustPassword' SUP top STRUCTURAL
 objectclass ( 1.3.6.1.4.1.7165.2.2.15 NAME 'sambaTrustedDomainPassword' SUP top STRUCTURAL
 objectclass ( 1.3.6.1.4.1.7165.2.2.5 NAME 'sambaDomain' SUP top STRUCTURAL
 objectclass ( 1.3.6.1.4.1.7165.2.2.7 NAME 'sambaUnixIdPool' SUP top AUXILIARY
 objectclass ( 1.3.6.1.4.1.7165.2.2.8 NAME 'sambaIdmapEntry' SUP top AUXILIARY
 objectclass ( 1.3.6.1.4.1.7165.2.2.9 NAME 'sambaSidEntry' SUP top STRUCTURAL
 objectclass ( 1.3.6.1.4.1.7165.2.2.10 NAME 'sambaConfig' SUP top AUXILIARY
 objectclass ( 1.3.6.1.4.1.7165.2.2.11 NAME 'sambaShare' SUP top STRUCTURAL
 objectclass ( 1.3.6.1.4.1.7165.2.2.12 NAME 'sambaConfigOption' SUP top STRUCTURAL
 ##objectclass ( 1.3.6.1.4.1.7165.2.2.13 NAME 'sambaPrivilege' SUP top AUXILIARY
 objectclass ( 1.3.6.1.4.1.7165.2.2.16 NAME 'sambaTrustedDomain' SUP top STRUCTURAL
```

- Observar que hai unhas cantas clases de obxectos comentadas, por evolución nas versións de samba.
- Por mencionar algunha clase de obxectos: sambaAccount, sambaDomain, sambaShare

- **Os atributos que define son:**

```
cat /etc/ldap/schema/samba.schema | grep attributetype
## 1.3.6.1.4.1.7165.2.1.x - attributetypes
## 1.3.6.1.4.1.7165.2.3.1.x - attributetypes
## 1.3.6.1.4.1.7165.4.1.x - attributetypes
##   attributetype ( 1.3.6.1.4.1.7165.2.1.XX NAME ....
##    <attributetype|objectclass> ( 1.3.6.1.4.1.7165.2.XX.XX NAME ....
#attributetype ( 1.3.6.1.4.1.7165.2.1.1 NAME 'lmPassword'
#attributetype ( 1.3.6.1.4.1.7165.2.1.2 NAME 'ntPassword'
#attributetype ( 1.3.6.1.4.1.7165.2.1.4 NAME 'acctFlags'
#attributetype ( 1.3.6.1.4.1.7165.2.1.3 NAME 'pwdLastSet'
#attributetype ( 1.3.6.1.4.1.7165.2.1.5 NAME 'logonTime'
#attributetype ( 1.3.6.1.4.1.7165.2.1.6 NAME 'logoffTime'
#attributetype ( 1.3.6.1.4.1.7165.2.1.7 NAME 'kickoffTime'
#attributetype ( 1.3.6.1.4.1.7165.2.1.8 NAME 'pwdCanChange'
#attributetype ( 1.3.6.1.4.1.7165.2.1.9 NAME 'pwdMustChange'
#attributetype ( 1.3.6.1.4.1.7165.2.1.10 NAME 'homeDrive'
```

```
#attributetype ( 1.3.6.1.4.1.7165.2.1.11 NAME 'scriptPath'
#attributetype ( 1.3.6.1.4.1.7165.2.1.12 NAME 'profilePath'
#attributetype ( 1.3.6.1.4.1.7165.2.1.13 NAME 'userWorkstations'
#attributetype ( 1.3.6.1.4.1.7165.2.1.17 NAME 'smbHome'
#attributetype ( 1.3.6.1.4.1.7165.2.1.18 NAME 'domain'
#attributetype ( 1.3.6.1.4.1.7165.2.1.14 NAME 'rid'
#attributetype ( 1.3.6.1.4.1.7165.2.1.15 NAME 'primaryGroupID'
attributetype ( 1.3.6.1.4.1.7165.2.1.24 NAME 'sambaLMPassword'
attributetype ( 1.3.6.1.4.1.7165.2.1.25 NAME 'sambaNTPassword'
attributetype ( 1.3.6.1.4.1.7165.2.1.26 NAME 'sambaAcctFlags'
attributetype ( 1.3.6.1.4.1.7165.2.1.27 NAME 'sambaPwdLastSet'
attributetype ( 1.3.6.1.4.1.7165.2.1.28 NAME 'sambaPwdCanChange'
attributetype ( 1.3.6.1.4.1.7165.2.1.29 NAME 'sambaPwdMustChange'
attributetype ( 1.3.6.1.4.1.7165.2.1.30 NAME 'sambaLogonTime'
attributetype ( 1.3.6.1.4.1.7165.2.1.31 NAME 'sambaLogoffTime'
attributetype ( 1.3.6.1.4.1.7165.2.1.32 NAME 'sambaKickoffTime'
attributetype ( 1.3.6.1.4.1.7165.2.1.48 NAME 'sambaBadPasswordCount'
attributetype ( 1.3.6.1.4.1.7165.2.1.49 NAME 'sambaBadPasswordTime'
attributetype ( 1.3.6.1.4.1.7165.2.1.55 NAME 'sambaLogonHours'
attributetype ( 1.3.6.1.4.1.7165.2.1.33 NAME 'sambaHomeDrive'
attributetype ( 1.3.6.1.4.1.7165.2.1.34 NAME 'sambaLogonScript'
attributetype ( 1.3.6.1.4.1.7165.2.1.35 NAME 'sambaProfilePath'
attributetype ( 1.3.6.1.4.1.7165.2.1.36 NAME 'sambaUserWorkstations'
attributetype ( 1.3.6.1.4.1.7165.2.1.37 NAME 'sambaHomePath'
attributetype ( 1.3.6.1.4.1.7165.2.1.38 NAME 'sambaDomainName'
attributetype ( 1.3.6.1.4.1.7165.2.1.47 NAME 'sambaMungedDial'
attributetype ( 1.3.6.1.4.1.7165.2.1.54 NAME 'sambaPasswordHistory'
attributetype ( 1.3.6.1.4.1.7165.2.1.20 NAME 'sambaSID'
attributetype ( 1.3.6.1.4.1.7165.2.1.23 NAME 'sambaPrimaryGroupSID'
attributetype ( 1.3.6.1.4.1.7165.2.1.51 NAME 'sambaSIDList'
attributetype ( 1.3.6.1.4.1.7165.2.1.19 NAME 'sambaGroupType'
attributetype ( 1.3.6.1.4.1.7165.2.1.21 NAME 'sambaNextUserRid'
attributetype ( 1.3.6.1.4.1.7165.2.1.22 NAME 'sambaNextGroupRid'
attributetype ( 1.3.6.1.4.1.7165.2.1.39 NAME 'sambaNextRid'
attributetype ( 1.3.6.1.4.1.7165.2.1.40 NAME 'sambaAlgorithmicRidBase'
attributetype ( 1.3.6.1.4.1.7165.2.1.41 NAME 'sambaShareName'
attributetype ( 1.3.6.1.4.1.7165.2.1.42 NAME 'sambaOptionName'
attributetype ( 1.3.6.1.4.1.7165.2.1.43 NAME 'sambaBoolOption'
attributetype ( 1.3.6.1.4.1.7165.2.1.44 NAME 'sambaIntegerOption'
attributetype ( 1.3.6.1.4.1.7165.2.1.45 NAME 'sambaStringOption'
attributetype ( 1.3.6.1.4.1.7165.2.1.46 NAME 'sambaStringListOption'
##attributetype ( 1.3.6.1.4.1.7165.2.1.50 NAME 'sambaPrivName'
##attributetype ( 1.3.6.1.4.1.7165.2.1.52 NAME 'sambaPrivilegeList'
attributetype ( 1.3.6.1.4.1.7165.2.1.53 NAME 'sambaTrustFlags'
attributetype ( 1.3.6.1.4.1.7165.2.1.58 NAME 'sambaMinPwdLength'
attributetype ( 1.3.6.1.4.1.7165.2.1.59 NAME 'sambaPwdHistoryLength'
attributetype ( 1.3.6.1.4.1.7165.2.1.60 NAME 'sambaLogonToChgPwd'
attributetype ( 1.3.6.1.4.1.7165.2.1.61 NAME 'sambaMaxPwdAge'
attributetype ( 1.3.6.1.4.1.7165.2.1.62 NAME 'sambaMinPwdAge'
attributetype ( 1.3.6.1.4.1.7165.2.1.63 NAME 'sambaLockoutDuration'
attributetype ( 1.3.6.1.4.1.7165.2.1.64 NAME 'sambaLockoutObservationWindow'
attributetype ( 1.3.6.1.4.1.7165.2.1.65 NAME 'sambaLockoutThreshold'
attributetype ( 1.3.6.1.4.1.7165.2.1.66 NAME 'sambaForceLogoff'
attributetype ( 1.3.6.1.4.1.7165.2.1.67 NAME 'sambaRefuseMachinePwdChange'
attributetype ( 1.3.6.1.4.1.7165.2.1.68 NAME 'sambaClearTextPassword'
attributetype ( 1.3.6.1.4.1.7165.2.1.69 NAME 'sambaPreviousClearTextPassword'
attributetype ( 1.3.6.1.4.1.7165.2.1.70 NAME 'sambaTrustType'
attributetype ( 1.3.6.1.4.1.7165.2.1.71 NAME 'sambaTrustAttributes'
attributetype ( 1.3.6.1.4.1.7165.2.1.72 NAME 'sambaTrustDirection'
attributetype ( 1.3.6.1.4.1.7165.2.1.73 NAME 'sambaTrustPartner'
attributetype ( 1.3.6.1.4.1.7165.2.1.74 NAME 'sambaFlatName'
attributetype ( 1.3.6.1.4.1.7165.2.1.75 NAME 'sambaTrustAuthOutgoing'
attributetype ( 1.3.6.1.4.1.7165.2.1.76 NAME 'sambaTrustAuthIncoming'
attributetype ( 1.3.6.1.4.1.7165.2.1.77 NAME 'sambaSecurityIdentifier'
attributetype ( 1.3.6.1.4.1.7165.2.1.78 NAME 'sambaTrustForestTrustInfo'
```

- Botarlle un ollo aos distintos atributos, seguro que moitos son familiares.

1.4.1.2 Transformar o ficheiro samba.schema en formato LDIF

- Imos agora **transformar samba.schema en formato LDIF** para poder engadilo no LDAP

- Creamos o ficheiro **schema_convert.conf** co seguinte contido:

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/samba.schema
```

- Creamos un directorio temporal para almacenar o ficheiros LDIF:

```
mkdir /tmp/ldif
```

- Usamos o comando **slaptest** para converter o ficheiro de esquema a LDIF:

```
slaptest -f schema_convert.conf -F /tmp/ldif
```

- Podemos ver no directorio temporal todo o que se creou, e entre outros, o ficheiro **cn={4}samba.ldif** que é o que cargaremos no LDAP.

```
tree /tmp/ldif
/tmp/ldif
??? cn=config
?   ??? cn=schema
?   ?   ??? cn={0}core.ldif
?   ?   ??? cn={1}cosine.ldif
?   ?   ??? cn={2}inetorgperson.ldif
?   ?   ??? cn={3}nis.ldif
?   ?   ??? cn={4}samba.ldif
?   ??? cn=schema.ldif
?   ??? olcDatabase={0}config.ldif
?   ??? olcDatabase={-1}frontend.ldif
??? cn=config.ldif
```

1.4.1.3 Cargar o ficheiro LDIF no ldap

- Temos dúas opcións:
    - Usando o comando **ldapadd**, precisamos facer uns cambios no ficheiro, pero non hai que reiniciar o servizo.
    - Copiando o ficheiro ldif a **/etc/ldap/slapd.d/cn=config/cn=schema**, pero hai que reiniciar o servizo ldap.
- En calquera caso imos facer unha copia do ficheiro ldif a */etc/ldap/schema* que é onde tiñamos os outros esquemas e os seus ficheiros ldif asociados, e así témolos todos xuntos.

```
ls /etc/ldap/schema/
collective.ldif    duaconf.ldif          misc.ldif        ppolicy.ldif
collective.schema  duaconf.schema        misc.schema      ppolicy.schema
corba.ldif         dyngroup.ldif         nis.ldif         README
corba.schema       dyngroup.schema       nis.schema       samba.schema
core.ldif          inetorgperson.ldif    openldap.ldif
core.schema        inetorgperson.schema  openldap.schema
cosine.ldif        java.ldif             pmi.ldif
cosine.schema      java.schema           pmi.schema
```

- Copiamos o ficheiro ao directorio anterior

```
cp "/tmp/ldif/cn=config/cn=schema/cn={4}samba.ldif" "/etc/ldap/schema/samba.ldif"
```

- O ficheiro copiado (/etc/ldap/schema/samba.ldif) precisa que realicemos nel as seguintes modificacións, cambiando estes dous atributos:

```
dn: cn=samba,cn=schema,cn=config
...
cn: samba
```

- e borrando as seguintes liñas que se atopan ao final do ficheiro:

```
structuralObjectClass: olcSchemaConfig
entryUUID: b53b75ca-083f-102d-9fff-2f64fd123c95
creatorsName: cn=config
createTimestamp: 20080827045234Z
entryCSN: 20080827045234.341425Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20080827045234Z
```

- Antes de cargar o LDIF no servizo LDAP imos ver que esquemas están cargados:

```
tree /etc/ldap
/etc/ldap
??? ldap.conf
??? sasl2
??? schema
?   ??? collective.ldif
...
?   ??? core.ldif
?   ??? core.schema
?   ??? cosine.ldif
?   ??? cosine.schema
...
?   ??? inetorgperson.ldif
?   ??? inetorgperson.schema
...
?   ??? nis.ldif
?   ??? nis.schema
...
?   ??? samba.ldif
?   ??? samba.schema
??? slapd.d
    ??? cn=config
    ?   ??? cn=module{0}.ldif
    ?   ??? cn=schema
    ?   ?   ??? cn={0}core.ldif
    ?   ?   ??? cn={1}cosine.ldif
    ?   ?   ??? cn={2}nis.ldif
    ?   ?   ??? cn={3}inetorgperson.ldif
    ?   ??? cn=schema.ldif
    ?   ??? olcBackend={0}mdb.ldif
    ?   ??? olcDatabase={0}config.ldif
    ?   ??? olcDatabase={-1}frontend.ldif
    ?   ??? olcDatabase={1}mdb.ldif
    ??? cn=config.ldif
```

- Vemos que en **/etc/ldap/slap.d/cn=config/cn=schema** están os esquemas que actualmente están cargados no ldap.

- Tamén o podemos ver consultado o directorio ldap.

```
ldapsearch -LLLQY EXTERNAL -H ldapi:/// -b cn=schema,cn=config "(objectClass=olcSchemaConfig)" dn
dn: cn=schema,cn=config

dn: cn={0}core,cn=schema,cn=config

dn: cn={1}cosine,cn=schema,cn=config

dn: cn={2}nis,cn=schema,cn=config

dn: cn={3}inetorgperson,cn=schema,cn=config
```

- **Opción A: cargar o esquema sen reiniciar o servizo: ldapadd**

- Cargamos o ficheiro samba.ldif modificado anteriormente

```
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/samba.ldif
  adding new entry "cn=samba,cn=schema,cn=config"
```

- Comprobación do realizado.

```
ldapsearch -LLLQY EXTERNAL -H ldapi:/// -b cn=schema,cn=config "(objectClass=olcSchemaConfig)" dn

dn: cn=schema,cn=config

dn: cn={0}core,cn=schema,cn=config

dn: cn={1}cosine,cn=schema,cn=config

dn: cn={2}nis,cn=schema,cn=config

dn: cn={3}inetorgperson,cn=schema,cn=config

dn: cn={4}samba,cn=schema,cn=config
```

- Vemos que en **/etc/ldap/slap.d/cn=config/cn=schema** está cargado o novo esquema.

```
tree /etc/ldap
/etc/ldap
??? ldap.conf
??? sasl2
??? schema
?   ??? collective.ldif
...
?   ??? core.ldif
?   ??? core.schema
?   ??? cosine.ldif
?   ??? cosine.schema
...
?   ??? inetorgperson.ldif
?   ??? inetorgperson.schema
...
?   ??? nis.ldif
?   ??? nis.schema
...
?   ??? samba.ldif
?   ??? samba.schema
??? slapd.d
    ??? cn=config
    ?   ??? cn=module{0}.ldif
    ?   ??? cn=schema
    ?   ?   ??? cn={0}core.ldif
    ?   ?   ??? cn={1}cosine.ldif
    ?   ?   ??? cn={2}nis.ldif
    ?   ?   ??? cn={3}inetorgperson.ldif
    ?   ?   ??? cn={4}samba.ldif
    ?   ??? cn=schema.ldif
    ?   ??? olcBackend={0}mdb.ldif
    ?   ??? olcDatabase={0}config.ldif
    ?   ??? olcDatabase={-1}frontend.ldif
    ?   ??? olcDatabase={1}mdb.ldif
    ??? cn=config.ldif
```

OPCIÓN B: reiniciando o servidor pero sen modificar o ficheiro:

```
cp "/tmp/ldif/cn=config/cn=schema/cn={4}samba.ldif" "/etc/ldap/slapd.d/cn=config/cn=schema"
chown openldap: '/etc/ldap/slapd.d/cn=config/cn=schema/cn={4}samba.ldif'
service slapd restart
```

1.4.2 Engadir os índices necesarios para as buscas de samba

- Neste caso imos engadir un conxunto de campos bastante grande que van ser índices no LDAP, así que os introduciremos nun ficheiro. Introducimos o seguinte contido no ficheiro **samba_indices_1.ldif**:

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: loginShell eq
olcDbIndex: uniqueMember eq,pres
olcDbIndex: sambaSID eq
olcDbIndex: sambaPrimaryGroupSID eq
olcDbIndex: sambaGroupType eq
olcDbIndex: sambaSIDList eq
olcDbIndex: sambaDomainName eq
olcDbIndex: default sub
```

- E cargamos os índices no LDAP con **ldapadd**:

```
ldapadd -Y EXTERNAL -H ldapi:/// -f samba_indices_1.ldif
 modifying entry "olcDatabase={1}mdb,cn=config"
```

- Reemplazamos índices que xa existen. Creamos o ficheiro: samba_indices_2.ldif

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcDbIndex
olcDbIndex: uidNumber eq
olcDbIndex: gidNumber eq
olcDbIndex: memberUid eq,pres,sub
```

- Aplicamos os cambios no LDAP con **ldapadd**:

```
ldapadd -Y EXTERNAL -H ldapi:/// -f samba_indices_2.ldif
 modifying entry "olcDatabase={1}mdb,cn=config"
```

-- Antonio de Andrés Lema e Carlos Carrión Álvarez