Contenido

- 1 Instalar os paquetes necesarios
- 2 Agregar os esquemas básicos
- 3 Definir as directivas básicas de configuración do servidor LDAP
- 4 Agregar a información básica do directorio
- 5 Probar o servidor LDAP

Instalar os paquetes necesarios

En primeiro lugar, teremos que instalar no servidor os paquetes necesarios para a execución do servidor LDAP (*slapd*) e as utilidades básicas para manexar a súa información:

```
sudo apt-get install slapd ldap-utils
```

Agregar os esquemas básicos

Por defecto, o paquete *slapd* de Ubuntu Server só inclúe na configuración do LDAP o esquema básico *core.schema*. Co seguinte comando engadimos unha serie de esquemas básicos almacenados en ficheiros LDIF na carpeta */etc/ldap/schema*:

```
ls /etc/ldap/schema/*.ldif | xargs -I {} sudo ldapadd -Y EXTERNAL -H ldapi:/// -f {}
```

Se observamos a saída da execución do comando, veremos que se produce un erro ao intentar engadir o esquema *core*, debido a que xa está engadido:

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=core,cn=schema,cn=config"
ldap_add: Other (e.g., implementation specific) error (80)
        additional info: olcAttributeTypes: Duplicate attributeType: "2.5.4.2"
```

O resto dos esquemas serán engadidos con éxito, como se pode ver a continuación no caso do esquema *openldap*:

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=openldap,cn=schema,cn=config"
```

Definir as directivas básicas de configuración do servidor LDAP

Creamos un ficheiro LDIF coa información de configuración básica do LDAP, para crear a base de datos *cn=config* inicial. A continuación móstrase o contido deste ficheiro que crea o directorio base *dc=iescalquera,dc=local*:

```
# Carga dos modulos necesarios para o almacenamento da base de datos
dn: cn=module,cn=config
objectclass: olcModuleList
cn: module
olcModulepath: /usr/lib/ldap
olcModuleload: back_hdb

# Creacion do directorio da base de datos
dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
# Directorio do sistema onde se almacena a base de datos
olcDbDirectory: /var/lib/ldap
# Nome do dominio (por exemplo iescalquera.local)
olcSuffix: dc=iescalquera,dc=local
# Administrador do LDAP
olcRootDN: cn=admin,dc=iescalquera,dc=local
olcRootPW: admin
# Parametros para optimizar o rendemento
olcDbConfig: set_cachesize 0 2097152 0
olcDbConfig: set_lk_max_objects 1500
olcDbConfig: set_lk_max_locks 1500
olcDbConfig: set_lk_max_lockers 1500
olcLastMod: TRUE
olcDbCheckpoint: 512 30
# Indices na base de datos para optimizar as busquedas
olcDbIndex: uid pres,eq
olcDbIndex: cn,sn,mail pres,eq,approx,sub
olcDbIndex: objectClass eq
# Un usuario debe poder cambiar o seu contrasinal, calquera debe poder autentificarse contra ela
# O administrador debe poder cambiar o contrasinal de calquera usuario
olcAccess: to attrs=userPassword by self write by anonymous auth by dn="cn=admin,dc=iescalquera,dc=lc
olcAccess: to attrs=shadowLastChange by self write by dn="cn=admin,dc=iescalquera,dc=local" write by
# So o administrador pode modificar os datos dos usuarios ou o propio usuario
olcAccess: to * by self write by dn="cn=admin,dc=iescalquera,dc=local" write by * read
olcAccess: to dn.base="" by * read

# Modificacions necesarias para poder acceder ao LDAP para editar a rama cn=config
# Neste caso, ao usuario cn=admin,cn=config asignamoslle o contrasinal 1234
dn: olcDatabase={-1}frontend,cn=config
changetype: modify
delete: olcAccess

dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootDN
olcRootDN: cn=admin,cn=config

dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: 1234
```

```
dn: olcDatabase={0}config,cn=config
changetype: modify
delete: olcAccess
```

- **Nota**: Cos parámetros deste ficheiro imos almacenar os contrasinais de administración do LDAP en claro no propio directorio (neste caso se puxeron os contrasinais *abc123.* e *1234*). En lugar de poñer directamente os contrasinais en claro, poden poñerse tamén (e sería máis seguro) os *hashes* destes contrasinais, que se poden obter usando o comando *slappasswd* (Por exemplo, o comando *slappasswd -h {SHA}* devolveranos o hash que teriamos que introducir para o contrasinal que lle indiquemos usando o algoritmo SHA . O texto que nos devolva o comando, como por exemplo *{SHA}cRDtpNCeBiql5KOQsKVyrA0sAiA=* sería o que introduciríamos en lugar dos contrasinais en claro).

Supoñendo que o ficheiro está gardado co nome *db.ldif*, engadimos estes datos no directorio co seguinte comando:

```
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f db.ldif
```

Agregar a información básica do directorio

Imos inicializar o directorio coa rama principal *dc=iescalquera,dc=local* e dúas subramas para almacenar os usuarios (*ou=usuarios,dc=iescalquera,dc=local*) e os grupos (*ou=grupos,dc=iescalquera,dc=local*).

Engadiremos tamén no directorio un usuario (*alfredo*, con contrasinal *abc123.*) e un grupo (*profes*).

O contido do ficheiro LDIF será o seguinte:

```
# Creamos os obxecto raiz do dominio
dn: dc=iescalquera,dc=local
objectClass: top
objectClass: dcObject
objectclass: organization
o: iescalquera.local
dc: iescalquera
description:  Raiz de dominio

# Creamos a rama na que colocaremos os usuarios
dn: ou=usuarios,dc=iescalquera,dc=local
objectClass: organizationalUnit
ou: usuarios

# Creamos a rama na que colocaremos os grupos
dn: ou=grupos,dc=iescalquera,dc=local
objectClass: organizationalUnit
```

```
ou: grupos

# Creamos un usuario
dn: uid=alfredo,ou=usuarios,dc=iescalquera,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: alfredo
sn: perez
givenName: Alfredo
cn: Alfredo Perez
displayName: Alfredo Perez
uidNumber: 10000
gidNumber: 10000
userPassword: abc123.
gecos: Alfredo Perez
loginShell: /bin/bash
homeDirectory: /home/alfredo
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: alfredo.perez@iescalquera.local
initials: AP

# Creamos un grupo
dn: cn=profes,ou=grupos,dc=iescalquera,dc=local
objectClass: posixGroup
cn: profes
gidNumber: 10000
```

Almacenamos esta información no ficheiro *init.ldif* e imos introducila no LDAP conectándonos coas credencias do usuario administrador creado no ficheiro *db.ldif* (usuario *cn=admin,dc=iescalquera,dc=local*, contrasinal *admin*):

```
sudo ldapadd -x -D cn=admin,dc=iescalquera,dc=local -w admin -f init.ldif
```

Probar o servidor LDAP

Para comprobar o resultado, podemos realizar unha lectura do contido do directorio co seguinte comando:

```
ldapsearch -x -H ldap://localhost -b dc=iescalquera,dc=local
```

Este comando mostraranos pola pantalla todo contido do da rama *dc=iescalquera,dc=local*, que incluirá as ou de *usuarios* e *grupos* o usuario *alfredo* e o grupo *profes*. Móstrase a continuación un extracto da saída no que se visualiza a información no directorio do grupo *profes*:

```
# profes, grupos, iescalquera.local
dn: cn=profes,ou=grupos,dc=iescalquera,dc=local
objectClass: posixGroup
```

```
cn: profes
gidNumber: 10000
```

-- Antonio de Andrés Lema e Carlos Carrión Álvarez