# Instalación y configuración del servicio LDAP con OpenLDAP

UT1: DNS y LDAP

DESPLIEGUE DE APLICACIONES WEB



## Introducción

**LDAP** es una implementación "ligera" del protocolo DAP (x.500), eliminando características poco usadas y complejas. Con este nombre también se hace referencia al servidor al que se accede, que provee una base de datos jerárquica muy usada especialmente para autenticación de usuarios, perfiles y AAA . OpenLDAP es una implementación libre y de código abierto del protocolo Lightweight Directory Access Protocol desarrollada por el proyecto OpenLDAP. Para instalarlo, podemos hacerlo con ***apt*** desde una consola de root:

```
// Instalación del servidor DNS bind
# apt install slapd ldap-utils
```

De esta forma instalaremos los programas necesarios para disponer de un completo servidor LDAP y sus utilidades de consulta. Tan solo será necesario configurarlo y ponerlo en marcha.

## Configuración del servidor LDAP

Esta vez los archivos de configuración se encuentran en /etc/ldap, pero en lugar de editarlos manualmente, usaremos un asistente:

```
# dpkg-reconfigure slapd
// Debemos responder No, Dar nombre de dominio (ej.
iespaloma.com) Sí para borrar la BD, para purgar BDs
// anteriores. Formato HDB.
```

## Arranque y parada manual del servidor LDAP

El arranque, parada y reinicio se realiza mediante el comando ***systemctl***, ***service*** o los habituales scripts de arranque de **/etc/init.d/**:

```
 # service slapd
Usage: /etc/init.d/slapd
{start|stop|reload|restart|force-reload|status}.
```

## Administración OpenLDAP

OpenLDAP ofrece una serie de comandos para la administración de datos en el directorio LDAP, contenidos en el paquete ldap-utils . Los cuatro comandos más importantes para añadir, modificar, buscar y eliminar son explicados a continuación.

Una vez instalado y configurado el servidor LDAP, la siguiente tarea es la del diseño de la estructura y la introducción de datos en el directorio.

Usaremos el servidor LDAP como almacén de usuarios y grupos para autenticar tanto a sistemas linux como servicios como ftp y web. Para ello, crearemos una estructura que parta de la base de nuestro directorio, para almacenar dicha información. Por tanto, crearemos una unidad organizativa ( ***ou*** ) llamada **groups** , para almacenar los grupos de usuarios y otra ***ou*** llamada **users** para almacenar a los usuarios.

Dado su uso tan habitual, existen plantillas para ello, e incluso suelen estar cargadas por defecto:

```
// Instalar plantillas para almacenamiento de usuarios unix
// Ya están cargadas en la versión actual. Habría que hacerlo
// en instalaciones antiguas
```

```
# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/cosine.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/nis.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/inetorgperson.ldif
```

## Creación esquema básico

A continuación, crearemos el esquema básico para nuestra organización (empresa), mediante un archivo ***ldif*** en el que indicaremos:

- **Base del directorio**: Se configura en el parámetro ***olcSuffix*** del archivo de configuración del esquema básico. En nuestro ejemplo usaremos: *dc=ieslapaloma,dc=com*
- **Nombre de usuario administrador**: Se configura en el parámetro ***olcRootDN*** del archivo de configuración del esquema básico. En nuestro ejemplo
  usaremos: *cn=admin,dc=ieslapaloma,dc=com*
- **Contraseña del administrador**: Se configura en el parámetro **olcRootPW** del archivo de configuración del esquema básico. En nuestro ejemplo usaremos: *ldapadmin*
- **Permiso de acceso a contraseñas**: Se configura en el parámetro ***olcAccess****: to attrs=userPassword* . Daremos al usuario administrador permiso de escritura y a cada usuario para cambiar su propia contraseña.
- **Permiso de acceso global al directorio**: Se configura en el parámetro ***olcAccess****: to* ***** . Daremos al usuario administrador permiso de escritura y a todos los usuarios, permisos de lectura.

```
# ---------- Archivo /tmp/ldapcurso-esquema-basico.ldif ----------
# Load dynamic backend modules
#dn: cn=module,cn=config
#objectClass: olcModuleList
#cn: module
#olcModulepath: /usr/lib/ldap
#olcModuleload: back_hdb

# Database settings
dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcSuffix: dc=ieslapaloma,dc=com
olcDbDirectory: /var/lib/ldap
olcRootDN: cn=admin,dc=ieslapaloma,dc=com
olcRootPW: ldapadmin
olcDbConfig: set_cachesize 0 2097152 0
olcDbConfig: set_lk_max_objects 1500
olcDbConfig: set_lk_max_locks 1500
olcDbConfig: set_lk_max_lockers 1500
olcDbIndex: objectClass eq
olcLastMod: TRUE
olcDbCheckpoint: 512 30
olcAccess: to attrs=userPassword by dn="cn=admin,dc=ieslapaloma,dc=com" write by auth by
self write by * none
olcAccess: to attrs=shadowLastChange by self write by * read
olcAccess: to dn.base="" by * read
olcAccess: to * by dn="cn=admin,dc=ieslapaloma,dc=com" write by * read
# ---------------------------------
```

Para cargar el esquema creado:

```
// Cargar en ldap el archivo ldapcurso-esquema-basico.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -f /tmp/ldapcurso-esquema-basico.ldif
```

## Creación de *OUs* para almacenar cuentas unix y creación de usuarios

Primero creamos la base del directorio: (*dn: dc=ieslapaloma,dc=com*), luego el administrador y después las OUs para grupos y usuarios de la cuentas Unix. A continuación se pueden crear los usuarios y finalmente asignarlos a grupos.

```
# ---------- Archivo /tmp/ldapcurso-usuarios.ldif ----------
dn: dc=ieslapaloma,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
dc: ieslapaloma
o: ieslapaloma

dn: cn=admin,dc=ieslapaloma,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e2NyeXB0fXdSVDNLMEpKSlQydmM=

dn: ou=users,dc=ieslapaloma,dc=com
objectClass: organizationalUnit
objectClass: top
ou: users

dn: ou=groups,dc=ieslapaloma,dc=com
objectClass: organizationalUnit
objectClass: top
ou: groups

dn: cn=Francisco Javier,ou=users,dc=ieslapaloma,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
objectClass: top
cn: Francisco Javier
gidNumber: 1001
homeDirectory: /home/javier
loginShell: /bin/bash
sn: Corcuera Ruiz
uid: javier
uidNumber: 1001

dn: cn=Joaquin,ou=users,dc=ieslapaloma,dc=com
objectClass: inetOrgPerson
```

```
objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
objectClass: top
cn: Joaquin
gidNumber: 1001
homeDirectory: /home/joaquin
loginShell: /bin/bash
sn:: R8OzbWV6
uid: joaquin
uidNumber: 1002

dn: cn=Miguel Angel,ou=users,dc=ieslapaloma,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
objectClass: top
cn: Miguel Angel
gidNumber: 1001
homeDirectory: /home/miguel
loginShell: /bin/bash
sn: Martinez
uid: miguel
uidNumber: 1003

dn: cn=Jessica,ou=users,dc=ieslapaloma,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
objectClass: top
cn: Jessica
gidNumber: 1002
homeDirectory: /home/jessica
loginShell: /bin/bash
sn: Perez
uid: jessica
uidNumber: 1004

dn: cn=Joel Javier,ou=users,dc=ieslapaloma,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: posixAccount
objectClass: top
cn: Joel Javier
gidNumber: 1002
homeDirectory: /home/joel
loginShell: /bin/bash
sn: Moreno
```

```
uid: joel
uidNumber: 1005

dn: cn=profesores,ou=groups,dc=ieslapaloma,dc=com
objectClass: posixGroup
objectClass: top
cn: profesores
gidNumber: 1001
memberUid: javier
memberUid: joaquin
memberUid: miguel

dn: cn=alumnos,ou=groups,dc=ieslapaloma,dc=com
objectClass: posixGroup
objectClass: top
cn: alumnos
gidNumber: 1002
memberUid: jessica
memberUid: joel
# ---------------------------------
```

## Inserción, Modificación, Búsqueda y Borrado

Cargamos los datos en el servidor con la orden:

```
// (contraseña: ldapadmin)
# ldapadd -c -x -D cn=admin,dc=ieslapaloma,dc=com -W -f /tmp/ldapcurso-usuarios.ldif
```

Añadir el atributo *userPassword*:

```
ldapmodify -x -D cn=admin,dc=ieslapaloma,dc=com -w ldapadmin
-f cambiar_usuario.ldif
```

```
// Fichero cambiar_usuario.ldif
dn: cn=Joel Javier,ou=users,dc=ieslapaloma,dc=com
changetype: modify
replace: userPassword
userPassword: 654321
```

Buscamos por nombre de usuario (*cn)*, desde otro cliente:

```
ldapsearch -x -b dc=ieslapaloma,dc=com "(cn=*el*)" -H
ldap://192.168.1.118
```

Borramos un usuario por *uid*:

```
ldapdelete -x -D cn=admin,dc=ieslapaloma,dc=com -W "cn=Joel
Javier,ou=users,dc=ieslapaloma,dc=com"
```

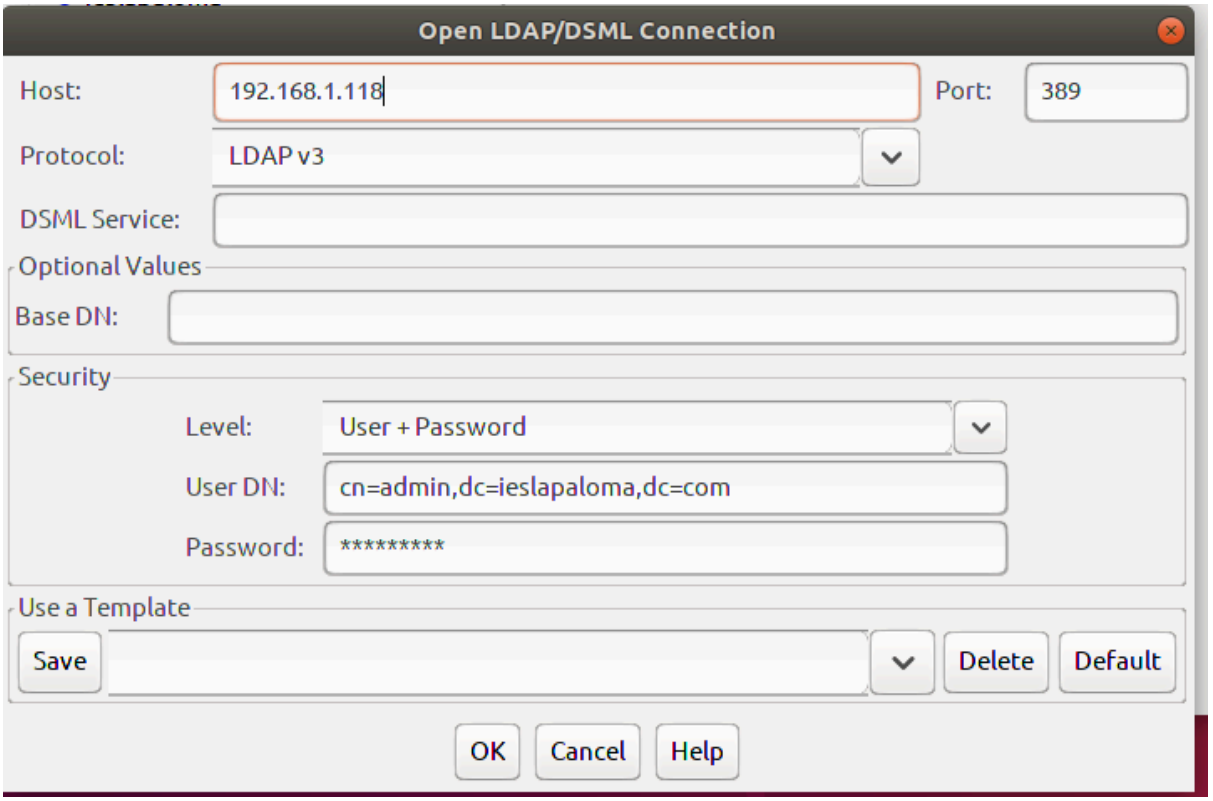
## Configuración de los clientes. Interacción gráfica con el servidor.

Para simplificar la interacción con el servidor, suelen usarse **GUIs** como **phpLDAPadmin** y **JXplorer,** aunque para cargas masivas de datos lo mejor es utilizar archivos ldif.

Por ejemplo para utilizar JXplorer:

```
# apt install jxplorer
```

Conectamos con:




## Configuración de los clientes. Instalación de librerías de autenticación.

Los servidor LDAP se usan principalmente como servidores de autenticación. A continuación veremos cómo configurar los clientes para que además de los usuarios locales (/etc/passwd), se puedan autentican los usuarios de LDAP.

Los pasos a seguir son:

1. Instalación de librerías:
   ```
   apt install libnss-ldap libpam-ldap nscd
   ```

   Aparecerá un asistente, elegir::
   1. `LDAP server Uniform Resource Identifier:`
      **`ldap://192.168.114.X`**

2. Distinguished name of the search base:**dc=ieslapaloma,dc=com**
3. LDAP version to use: **3**
4. Make local root Database admin: **Yes**
5. Does the LDAP database require login? **No**
6. LDAP account for root: **cn=admin,dc=ieslapaloma,dc=com**
7. LDAP root account password: **ldapadmin**

2. Modifica el archivo **/etc/nsswitch.conf** que indica donde "buscar" a los usuarios, añadiendo al final de las filas de *passwd, shadow y group* la palabra clave ***ldap***

```
passwd:         compat systemd ldap
group:          compat systemd ldap
shadow:         compat ldap
```

3. Modifica el archivo **/etc/nscd.conf** y descomenta la línea logfile, esto hará que el servicio nscd guarde sus logs aparte.

```
        logfile                 /var/log/nscd.log
```

4. Edita */etc/pam.d/common-password* y en la línea 26 borra [*use_authtok*] de manera que quede:
   **password [success=1 user_unknown=ignore default=die] pam_ldap.so try_first_pass**

5. Reinicia el servicio ***nscd,*** encargado de la conexión con LDAP para autenticar usuarios, de manera que se apliquen los cambios anteriores.
   **# service nscd restart**

6. Revisa mediante el comando ***pam-auth-update*** que los servicios *Unix authentication* y *LDAP authentication* están marcados. Añade que se creen los directorios ***home*** al iniciar sesión.

7. Finalmente, comprueba que los usuarios LDAP son accesibles desde el cliente con:
   **# getent passwd | grep bash**

8. Inicia una consola de texto (shell) con un usuario de LDAP, p.e:
   **$ su - joel**

## Probar la autenticación con *pamtester*

**# apt install pamtester**

**# pamtester {passwd | ssh | ftp} <usuario> authenticate**

Ejemplos: