

Servicio OpenLDAP

Protocolo LDAP

Entradas LDIF

Configuración y comprobación

Índice

LDAP.....	2
OpenLDAP.....	2
Instalación.....	2
Configuración.....	3
Configuración de datos del directorio LDAP.....	4
Unidades organizativas.....	4
Usuarios.....	4
Pepe.....	4
Manuel.....	5
Sofia.....	6
Añadir la configuración.....	7
Script de automatización.....	7
Comprobaciones.....	8
Fuentes.....	9
Complementarias.....	9
No disponibles al público.....	9

LDAP

LDAP (Protocolo Ligero de Acceso a Directorios. En inglés, *Lightweight Directory Access Protocol*) es un protocolo a nivel de aplicación para la **búsqueda de información en red**, prácticamente como una **base de datos**.¹

Nos permite **acceder** eficientemente a una **información concreta**, de carácter diverso. Un uso muy común suele ser la **autenticación**. Podemos guardar información acerca de usuarios, así como sus **credenciales de acceso**, y crear un sistema de autenticación.

OpenLDAP

OpenLDAP es un software de **código abierto** que implementa el protocolo LDAP.² Forma parte de la suite de aplicaciones y herramientas de desarrollo enfocado a este protocolo, el **proyecto OpenLDAP**.³

Instalación

- **Ubuntu / Debian**^{5 6}

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

- **CentOS8 / RHEL8 / Fedora**⁷

Por favor, visitar la referencia en [Cómo instalar el servidor OpenLDAP en CentOS 8/RHEL 8](#), que también aplica a Fedora.

- **FreeBSD**⁸

```
sudo pkg install openldap26-server
```

- **Alpine Linux**⁹

```
sudo apk add openldap openldap-back-mdb openldap-clients
```



Nótese que el servicio **OpenLDAP** no es soportado, de manera oficial, en plataformas basadas en **Windows**⁽ⁱ⁾ o **MacOS**⁽ⁱⁱ⁾.

- (i). Existen adaptaciones de este software creadas por terceros, disponibles en Internet. Por favor, tenga en cuenta que estas pueden suponer una grave brecha de seguridad. Considere utilizar WSL (Windows Subsystem for Linux) si Windows es su única opción.
- (ii). En el caso de MacOS, se realiza un soporte "Best-effort". Quiere decir que no es un objetivo principal, pero que en caso de errores significativos, se dará soporte.



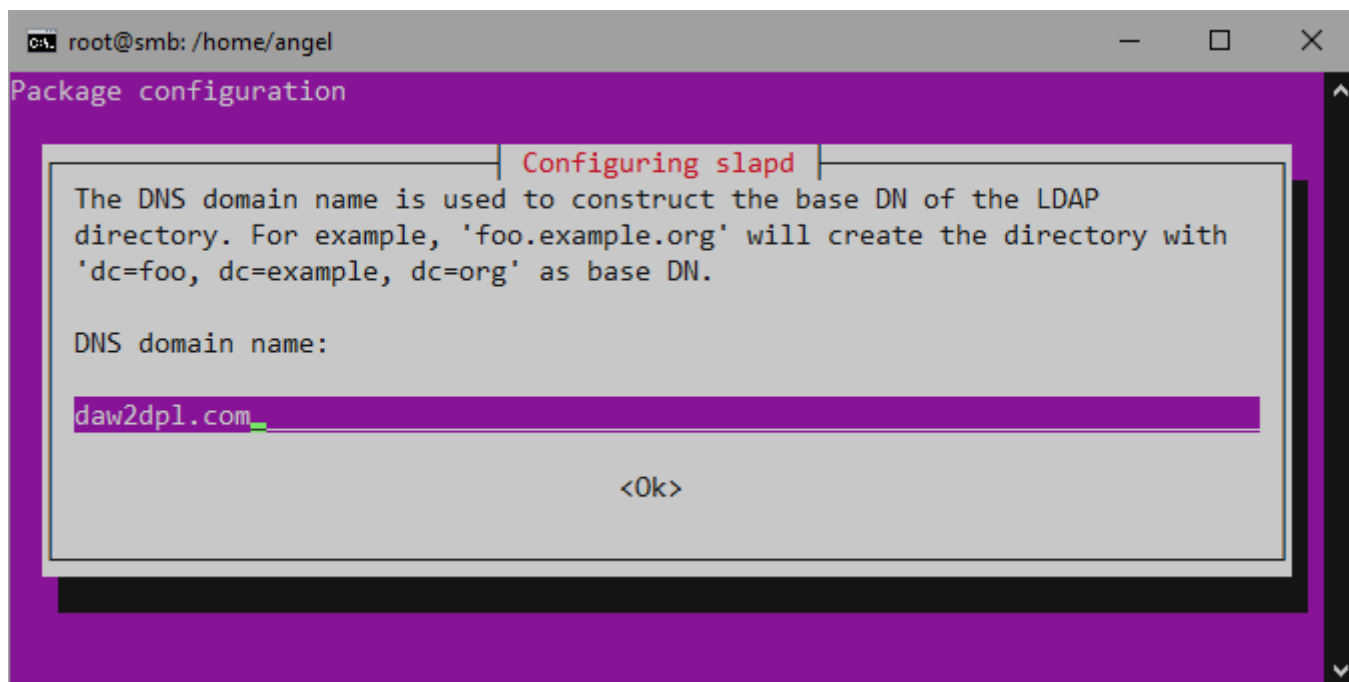
Esta práctica está elaborada bajo el sistema operativo **Ubuntu 22.04 LTS**. Por ello se asume que será responsabilidad del lector adaptar las utilidades y rutas empleadas al sistema propio.

Configuración

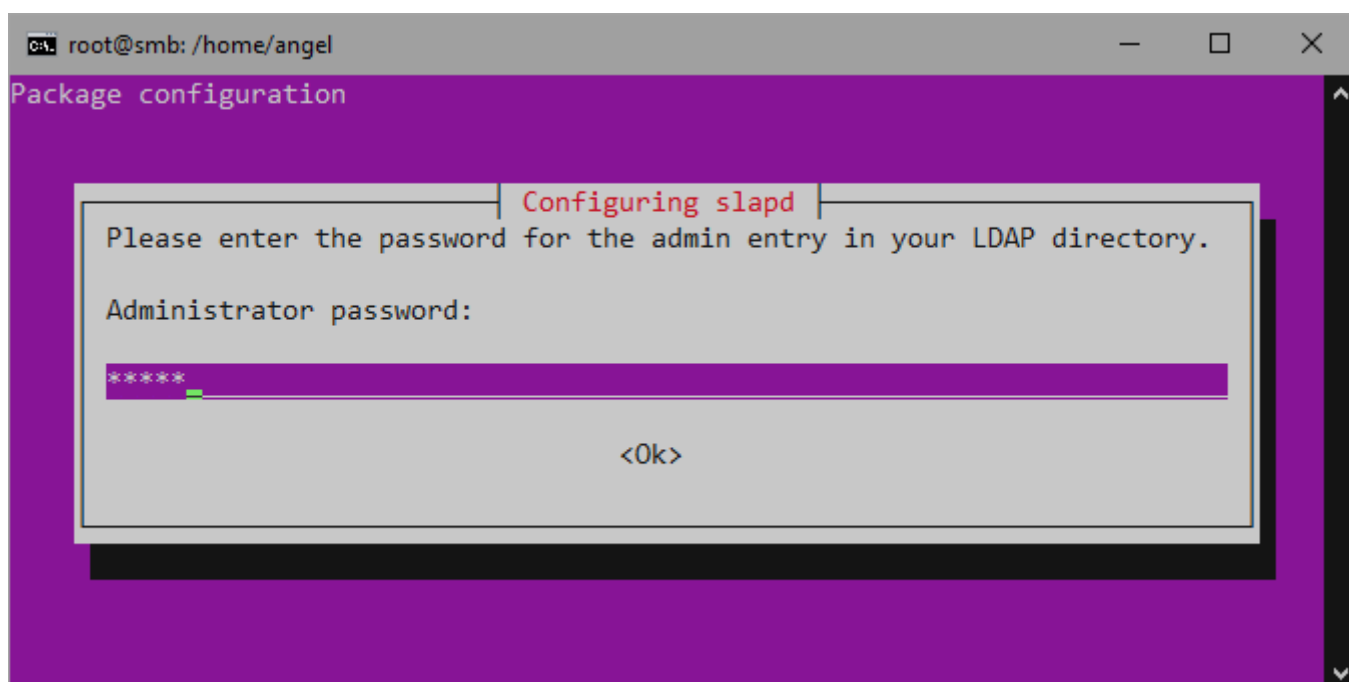
Una vez instalado, deberá aparecer el **configurador de paquetes**. Siguiendo los requerimientos de esta práctica, vamos a ingresar que nuestro directorio raíz sea daw2dpl.com.⁴

En caso de que no aparezca, podemos ejecutar el comando `dpkg-reconfigure`.

```
sudo dpkg-reconfigure slapd
```



También pondremos como contraseña de administrador [admin](#).



Configuración de datos del directorio LDAP

Vamos a realizar las entradas LDIF necesarias para satisfacer los requisitos de esta práctica.¹⁰

Primero, creamos un directorio donde poder guardar los ficheros de entradas LDIF.

```
sudo mkdir ~/openldap_config && cd $_
```

Unidades organizativas

Primero vamos a crear la unidad organizativa llamada **alumnos**. Para ello, generemos un archivo con el nombre **unidad_alumnos.dif**, y escribimos esta estructura:



```
root@smb: ~/openldap_config
dn: ou=alumnos,dc=daw2dpl,dc=com
objectClass: organizationalUnit
ou: alumnos
-- INSERT --
```

Usuarios

Ahora, los usuarios de la unidad organizativa **alumnos**.

Los alumnos necesitarán tener **atributos** tales como **nombre**, **email**, **número de teléfono**, **directorío home** y **contraseña**. Para poder añadir estos, hay que usar o establecer el o los **esquemas apropiados**. Podríamos establecerlos, pero es más recomendable intentar utilizar los ya existentes.

En este caso, vamos a utilizar el esquema **inetOrgPerson**, puesto que nos permite añadir los **atributos básicos** que pueda tener una **persona** o trabajador. También, usaremos **posixAccount**, puesto que queremos añadir un **directorío home**. Este también requiere establecer la **terminal** del usuario, así como su **UID** y **GID**.^{11 12}

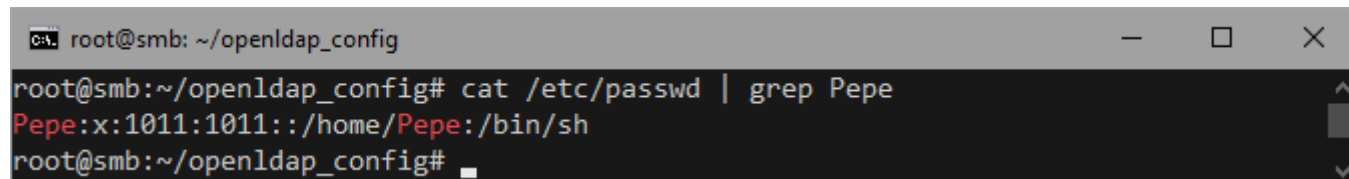
Pepe

Primero añadimos al alumno **Pepe**. Puesto que estamos usando el esquema **posixAccount**, deberemos **crear el usuario en el sistema**. Podemos hacerlo con el siguiente comando:

```
sudo useradd Pepe
```

Al crear el usuario, se han generado automáticamente algunos de los atributos que necesitamos. Podemos verlos con el comando siguiente:

```
sudo cat /etc/passwd | grep Pepe
```



```
root@smb: ~/openldap_config
root@smb:~/openldap_config# cat /etc/passwd | grep Pepe
Pepe:x:1011:1011:~/home/Pepe:/bin/sh
root@smb:~/openldap_config#
```

Se aprecia el UID y GID, directorío home y la terminal de usuario.

Ahora simplemente rellenamos el archivo. Puesto que el atributo **sn** es requerido por el esquema **inetOrgPerson**, debemos de configurarlo. Supongamos que Pepe se apellida **Perez**.

```
root@smb: ~/openldap_config
# usuario_pepe.ldif
dn: uid=Pepe,ou=alumnos,dc=daw2dpl,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
uid: Pepe
cn: Pepe
sn: Perez
mail: pepe@daw2dpl.com
telephoneNumber: 123456789
homeDirectory: /home/Pepe
uidNumber: 1011
gidNumber: 1011
loginShell: /bin/sh
-- INSERT --
```

Manuel

```
root@smb: ~/openldap_config
root@smb:~/openldap_config# useradd Manuel
root@smb:~/openldap_config# cat /etc/passwd | grep Manuel
Manuel:x:1012:1012:~/home/Manuel:/bin/sh
root@smb:~/openldap_config#
```

Nótese que, el usuario **Manuel**, tiene una **contraseña** representada por un **hash**. Para conseguir este hash, se utilizó la función **SSHA**¹³ (*Salted SHA*), que es la más recomendada, con el siguiente comando:

```
slappasswd -s P4ssw0rd
```

También hay que añadir dicha contraseña a la cuenta del usuario en el propio sistema:

```
slappasswd -s P4ssw0rd
```

```
root@smb: ~/openldap_config
root@smb:~/openldap_config# echo "Manuel:P4ssw0rd" | sudo chpasswd
root@smb:~/openldap_config#
```

Supongamos que Manuel se apellida **Martinez**.

```

root@smb: ~/openldap_config
# usuario_manuel.ldif
dn: uid=Manuel,ou=alumnos,dc=daw2dpl,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
uid: Manuel
cn: Manuel
sn: Martinez
userPassword: {SSHA}XPV RU82Ht8GGht3uTWguGFdVQRf5ecb
mail: manuel@daw2dpl.com
telephoneNumber: 912345678
homeDirectory: /home/Manuel
uidNumber: 1012
gidNumber: 1012
loginShell: /bin/sh
-- INSERT --

```

Sofia

```

root@smb: ~/openldap_config
root@smb:~/openldap_config# useradd Sofia
root@smb:~/openldap_config# cat /etc/passwd | grep Sofia
Sofia:x:1013:1013:./home/Sofia:/bin/sh
root@smb:~/openldap_config# echo "Sofia:p4SSW0RD" | sudo chpasswd
root@smb:~/openldap_config# slappasswd -s p4SSW0RD
{SSHA}C6tYHAu8x0xZ0cEq/0tyrm00uVrleLVZ
root@smb:~/openldap_config#

```

Para la última alumna, suponemos el apellido Ramirez.

```

root@smb: ~/openldap_config
# usuario_sofia.ldif
dn: uid=Sofia,ou=alumnos,dc=daw2dpl,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
uid: Sofia
cn: Sofia
sn: Ramirez
userPassword: {SSHA}C6tYHAu8x0xZ0cEq/0tyrm00uVrleLVZ
mail: sofia@daw2dpl.com
telephoneNumber: 891234567
homeDirectory: /home/Sofia
uidNumber: 1013
gidNumber: 1013
loginShell: /bin/sh
-- INSERT --

```

Añadir la configuración

Una vez creadas las entradas LDIF, deberemos añadirlas, mediante un comando, para que **OpenLDAP** pueda **reconocerlas**. Se realiza con el comando **ldapadd**.

Script de automatización

Normalmente, es común crear un **script** para automatizar el proceso de añadir las entradas LDIF. En nuestro caso, se llamará **script.sh** y tendrá el siguiente contenido:

```
root@smb: ~/openldap_config
#!/bin/bash

ldapadd -x -D "cn=admin,dc=daw2dpl,dc=com" -w admin -f unidad_alumnos.ldif
ldapadd -x -D "cn=admin,dc=daw2dpl,dc=com" -w admin -f usuario_pepe.ldif
ldapadd -x -D "cn=admin,dc=daw2dpl,dc=com" -w admin -f usuario_manuel.ldif
ldapadd -x -D "cn=admin,dc=daw2dpl,dc=com" -w admin -f usuario_sofia.ldif
-- INSERT --
```

Una vez hecho esto, necesitamos configurar los **permisos de ejecución** de dicho script y ejecutarlo. Podemos hacer esto mediante los siguientes comandos:

```
chmod +x script.sh
./script.sh
```

```
root@smb: ~/openldap_config
root@smb:~/openldap_config# ./script.sh
adding new entry "ou=alumnos,dc=daw2dpl,dc=com"

adding new entry "uid=Pepe,ou=alumnos,dc=daw2dpl,dc=com"

adding new entry "uid=Manuel,ou=alumnos,dc=daw2dpl,dc=com"

adding new entry "uid=Sofia,ou=alumnos,dc=daw2dpl,dc=com"

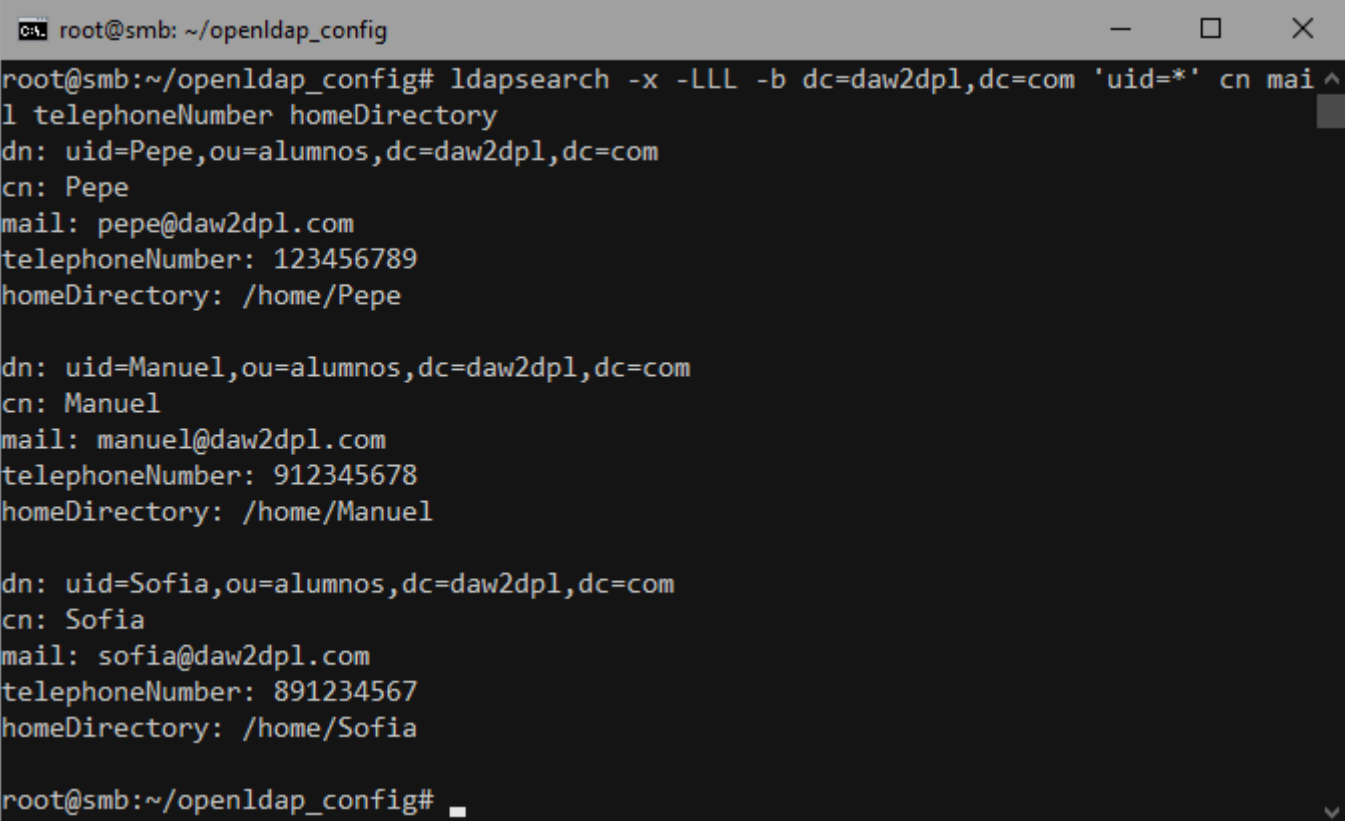
root@smb:~/openldap_config#
```

Comprobaciones

Ya tenemos el servicio funcionando. Ahora debemos comprobar que funciona correctamente. Para ello, podemos utilizar el comando `ldapsearch`.¹⁴ En nuestro caso vamos a usar:

```
ldapsearch -x -LLL -b dc=daw2dpl,dc=com 'uid=*' cn mail telephoneNumber homeDirectory
```

Así podemos ver las entradas coincidentes y bien configuradas. En cada alumno, podemos observar los atributos relevantes.



```
root@smb: ~/openldap_config
root@smb:~/openldap_config# ldapsearch -x -LLL -b dc=daw2dpl,dc=com 'uid=*' cn mail ^
l telephoneNumber homeDirectory
dn: uid=Pepe,ou=alumnos,dc=daw2dpl,dc=com
cn: Pepe
mail: pepe@daw2dpl.com
telephoneNumber: 123456789
homeDirectory: /home/Pepe

dn: uid=Manuel,ou=alumnos,dc=daw2dpl,dc=com
cn: Manuel
mail: manuel@daw2dpl.com
telephoneNumber: 912345678
homeDirectory: /home/Manuel

dn: uid=Sofia,ou=alumnos,dc=daw2dpl,dc=com
cn: Sofia
mail: sofia@daw2dpl.com
telephoneNumber: 891234567
homeDirectory: /home/Sofia

root@smb:~/openldap_config#
```


Fuentes

1. [LDAP Wikipedia](#). Información general.
2. [OpenLDAP](#) (en inglés). Página oficial de la aplicación OpenLDAP.
3. [Proyecto OpenLDAP](#) (en inglés). Página oficial del proyecto OpenLDAP.
4. [Guía oficial de OpenLDAP](#) (en inglés). Instalación y configuración, resumido.
5. [Instalación OpenLDAP en Ubuntu](#) (en inglés). Guía oficial.
6. [Instalación OpenLDAP en Debian](#) (en inglés). Guía oficial.
7. [Instalación OpenLDAP en CentOS8 / RHEL8 / Fedora](#) (en inglés). Para CentOS8 y RHEL8, siendo aplicable también en Fedora.
8. [Instalación OpenLDAP en FreeBSD](#) (en inglés). Guía oficial.
9. [Instalación OpenLDAP en Alpine](#) (en inglés). Guía oficial.
10. [Creación de ficheros Idif](#) (en inglés). Guía explicativa del proceso de crear y añadir ficheros Idif.
11. [Esquema inetOrgPerson](#) (en inglés). Referencia al esquema inetOrgPerson.
12. [Esquema posixAccount](#) (en inglés). Referencia al esquema posixAccount.
13. [SSHA en OpenLDAP](#) (en inglés).
14. [Comando ldapsearch](#) (en inglés). Referencia oficial al comando `ldapsearch`.

Complementarias

- [Función Hash Wikipedia](#). ¿Qué es hashear?

No disponibles al público

Fuentes no disponibles al público al momento de elaborar este documento.

- **UD_1_Servicios de red.odt**. Documento a modo de teoría adjuntado en el [campus](#). Hash del documento, utilizando “`sha256sum`”:
`7f390eae2edd658e53980eaa1e5b79107f4b63944b3b7a0f119ccb2171337df1`