Práctica. Instalación y configuración de OpenLDAP en Ubuntu Server 25.04

Módulo: Despliegue de aplicaciones web (2ºDAW)

Profesora: Isabel Soriano

Objetivos de la práctica

1. Instalar y configurar un servidor OpenLDAP en Ubuntu Server.
2. Crear la estructura base del directorio (dominio, OU, grupos y usuarios).
3. Administrar usuarios/grupos.
4. Actualizar el servidor DNS.
5. Configurar el cliente.
6. Probar el funcionamiento de OpenLDAP.

Introducción

En esta práctica guiada vamos a **instalar y configurar OpenLDAP en Ubuntu Server**. El servidor deberá dar servicio al resto de equipos conectados en la misma red local.

Para esta práctica, debes usar las máquinas virtuales indicadas al inicio de curso. **La máquina donde se va a instalar OpenLDAP es la máquina 'server'**. Recuerda que deben tener el direccionamiento correcto. En concreto, para el servidor LDAP usaremos la **dirección 10.10.5.30/24 (máquina virtual 'server').**

Se recomienda guardar una copia de la máquina virtual una vez finalizada la práctica.

Parte 1. Instalar y configurar un servidor OpenLDAP en Ubuntu Server.

En esta parte de la práctica, solo debe estar encendida la máquina del servidor (llamada 'server').

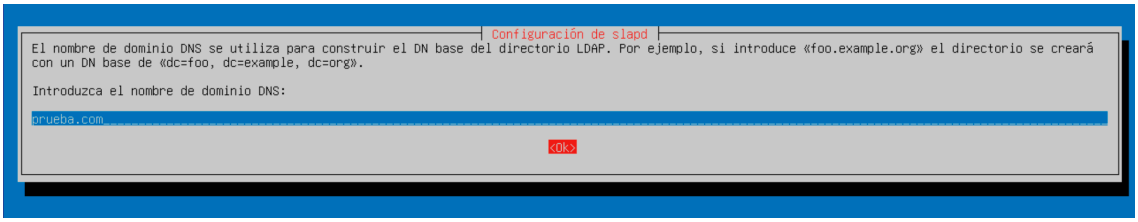
Pasos a seguir

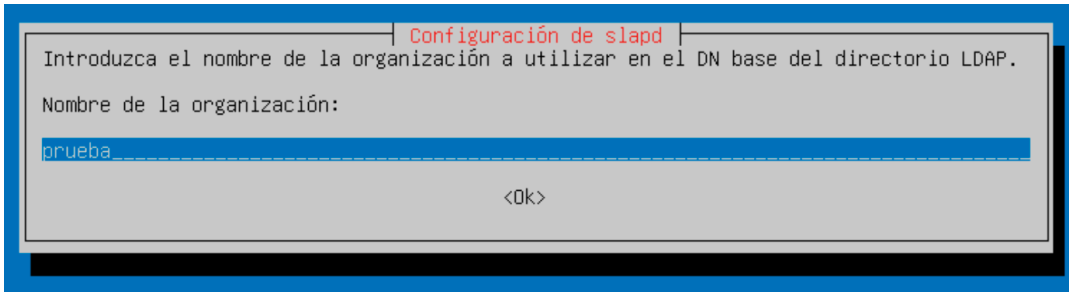
1. Actualiza el sistema: **sudo apt update**
2. Instala OpenLDAP: **sudo apt install slapd ldap-utils -y**
3. Configura slapd: **sudo dpkg-reconfigure slapd**

   Se abrirá una ventana donde tienes que ir indicando la siguiente información:

   - DNS domain name → prueba.com
   - Organization name → prueba
   - Admin password → prueba
   - Backend → MDB
   - Remove database → No
   - Move old database → Yes
   - Allow LDAPv2 → No

A continuación, se muestra un ejemplo de la ventana de configuración para configurar el dominio y el nombre de la organización:





*** Puede que alguna de las opciones anteriores no te las pregunte, no pasa nada. Lo más importante, que siempre te debe salir para configurar es, el nombre del dominio DNS y el nombre de la organización.*

4. Comprueba que el servicio está activo: **sudo systemctl status slapd**

Parte 2. Crear la estructura base del directorio LDAP.

En esta parte de la práctica, solo debe estar encendida la máquina del servidor (llamada 'server').

Pasos a seguir

1. Para darle estructura al directorio LDAP, crea un archivo LDIF llamado:
   sudo nano base.ldif
2. Dentro del fichero, añade la siguiente información:

```
dn: ou=usuarios,dc=prueba,dc=com
objectClass: organizationalUnit
ou: usuarios

dn: ou=grupos,dc=prueba,dc=com
objectClass: organizationalUnit
ou: grupos
```

El fichero 'base.ldif' contiene entradas iniciales para crear en LDAP dos unidades organizativas (OU): la de 'usuarios' y la de 'grupos'. Ambas cuelgan directamente del dominio prueba.com. Cada OU es un contenedor lógico para otras entradas (como dos carpetas del directorio). En la OU 'usuarios' se añadirán las cuentas de usuario y en la OU 'grupos', se incluirán los grupos POSIX (Portable Operating

System Interface for Unix, estándar que define cómo los sistemas tipo Unix manejan usuarios, grupos, permisos, etc.). La jerarquía sería la siguiente (DIT):

```
dc=prueba,dc=com
 ├── ou=usuarios   ← aquí irán las cuentas de usuarios POSIX
 └── ou=grupos     ← aquí irán los grupos POSIX
```

Un grupo POSIX en LDAP es un objeto del tipo posixGroup. Representa un grupo de usuarios de sistema UNIX/Linux, con un identificador numérico (gidNumber). Es el equivalente a los grupos que ya existen en /etc/group en un sistema Linux tradicional.

El contenido de este fichero no es siempre así, dependerá de las necesidades de tu servidor LDAP.

3. Importa en el servidor el contenido de 'base.ldif':

ldapadd -x -D "cn=admin,dc=prueba,dc=com" -W -f base.ldi

```
profesora@server:~$ ldapadd -x -D "cn=admin,dc=prueba,dc=com" -W -f base.ldif
Enter LDAP Password:
adding new entry "ou=usuarios,dc=prueba,dc=com"

adding new entry "ou=grupos,dc=prueba,dc=com"
```

***Ten en cuenta que, cn=admin es porque ese usuario se crea automáticamente cuando instalas y configuras el paquete slapd en Ubuntu.*

4. Verifica que se han añadido las entradas correctamente:

ldapsearch -x -LLL -b dc=prueba,dc=com dn

*** Muestra las 3 entradas creadas. El resultado de la búsqueda ha sido exitoso.*

```
profesora@server:~$ ldapsearch -x LLL -b dc=prueba,dc=com dn
# extended LDIF
#
# LDAPv3
# base <dc=prueba,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: LLL dn
#

# prueba.com
dn: dc=prueba,dc=com

# usuarios, prueba.com
dn: ou=usuarios,dc=prueba,dc=com

# grupos, prueba.com
dn: ou=grupos,dc=prueba,dc=com

# search result
search: 2
result: 0 Success

# numResponses: 4
# numEntries: 3
```

Parte 3. Administrar usuarios/grupos.

En esta parte de la práctica, solo debe estar encendida la máquina del servidor (llamada 'server').

Pasos a seguir

1. Necesitamos crear un grupo para los profesores del instituto. Crea el archivo LDIF:

   sudo nano profesores.ldif

   *** Ten en cuenta, que el nombre del archivo LDIF no tiene relación con ningún parámetro del archivo y no se va a ver reflejado en la jerarquía de LDAP. En este caso, le llamamos profesores.ldif, porque considero que es más intuitivo porque vamos a crear un grupo llamado 'profesores'. Este grupo estará dentro de la OU creada en base.ldif llamada 'grupos'.*

2. Dentro del fichero, añade la siguiente información:

```
dn: cn=profesores,ou=grupos,dc=prueba,dc=com
objectClass: posixGroup
cn: profesores
gidNumber: 10000
```

3. Ahora, tenemos que añadir información de los profesores. De momento, solo vamos a añadir información de un profesor llamado 'Juan'. Crea el archivo LDIF:

   sudo nano infoprof.ldif

4. Dentro del fichero, añade la siguiente información:

```
dn: uid=juan,ou=usuarios,dc=prueba,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Juan Perez
sn: Perez
uid: juan
uidNumber: 10001
gidNumber: 10000
homeDirectory: /home/juan
loginShell: /bin/bash
userPassword: {SSHA}HASH_AQUI
```

¡IMPORTANTE! Para poder completar el campo **userPassword** debes generar la password antes (*nuestra password va a ser 'prueba'*). Una vez generada la debes copiar y pegar en tu documento LDIF.

Para generarla ejecuta el siguiente comando: **slappasswd -s prueba**

La puedes generar y copiar directamente a tu fichero infoprof.ldif, de la siguiente manera:

```
profesora@server:~$ slappasswd | sudo tee -a infoprof.ldif
New password:
Re-enter new password:
{SSHA}2RS2D7wCioaTmzpEwHQmopeY/O3uGVlg
```

Cuando te pregunte el password, debes poner 'prueba'.

El hash generado es aleatorio, por tanto, el que te salga no será el mismo de esta captura.

Una vez hecho esto, edita el fichero infoprof.ldif y déjalo correctamente escrito:

```
dn: uid=juan,ou=usuarios,dc=prueba,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Juan Perez
sn: Perez
uid: juan
uidNumber: 10001
gidNumber: 10000
homeDirectory: /home/juan
loginShell: /bin/bash
userPassword: {SSHA}2RS2D7wCioaTmzpEwHQmopeY/O3uGVlg
```

Por otro lado, ten en cuenta que los objectClass significan lo siguiente:

- *inetOrgPerson → define atributos de persona (nombre, apellido, email, etc.).*
- *posixAccount → lo convierte en un usuario UNIX (uidNumber, gidNumber, homeDirectory, loginShell).*
- *shadowAccount → añade atributos relacionados con la contraseña y caducidad, como en /etc/shadow.*

Actualmente, la jerarquía sería la siguiente (DIT):

```
dc=prueba,dc=com
├── ou=usuarios
│   └── uid=juan
│       ├── objectClass: inetOrgPerson
│       ├── objectClass: posixAccount
│       ├── objectClass: shadowAccount
│       ├── cn: Juan Perez
│       ├── sn: Perez
│       ├── uid: juan
│       ├── uidNumber: 10001
│       ├── gidNumber: 10000          ← Grupo principal (apunta al grupo POSIX de abajo)
│       ├── homeDirectory: /home/juan
│       ├── loginShell: /bin/bash
│       └── userPassword: {SSHA}HASH_AQUI
│
└── ou=grupos
    └── cn=profesores
        ├── objectClass: posixGroup
        ├── cn: profesores
        └── gidNumber: 10000          ← Este gidNumber coincide con el gidNumber de juan
```

5. Importa en LDAP los ficheros LDIF creados:

   ldapadd -x -D "cn=admin,dc=prueba,dc=com" -W -f profesores.ldif

   ldapadd -x -D "cn=admin,dc=prueba,dc=com" -W -f infoprof.ldif

```
profesora@server:~$ sudo ldapadd -x -D "cn=admin,dc=prueba,dc=com" -W -f profesores.ldif
Enter LDAP Password:
adding new entry "cn=profesores,ou=grupos,dc=prueba,dc=com"

profesora@server:~$ sudo ldapadd -x -D "cn=admin,dc=prueba,dc=com" -W -f infoprof.ldif
Enter LDAP Password:
adding new entry "uid=juan,ou=usuarios,dc=prueba,dc=com"
```

6. Comprueba en el servidor LDAP que está la entrada creada para 'juan':

   ldapsearch -x -b "uid=juan,ou=usuarios,dc=prueba,dc=com"

   ***Ese comando hace una búsqueda LDAP comenzando exactamente en la entrada uid=juan,... (como base DN), con el filtro por defecto "cualquier objeto", y te devuelve la ficha completa de juan (si tienes permiso para verla).*

```
profesora@server:~$ sudo ldapsearch -x -b "uid=juan,ou=usuarios,dc=prueba,dc=com"
# extended LDIF
#
# LDAPv3
# base <uid=juan,ou=usuarios,dc=prueba,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# juan, usuarios, prueba.com
dn: uid=juan,ou=usuarios,dc=prueba,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Juan Perez
sn: Perez
uid: juan
uidNumber: 10001
gidNumber: 10000
homeDirectory: /home/juan
loginShell: /bin/bash

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Parte 4. Actualización del servidor DNS.

En esta parte de la práctica, solo debe estar encendida la máquina del servidor (llamada 'server').

Este paso no es obligatorio para que funcione un servidor LDAP, pero sí recomendable si tenemos ya instalado un servidor DNS. La única modificación que debemos hacer es, respecto a nuestros 'archivos de zona'.

El archivo **'db.prueba.com**' debe quedar de la siguiente manera:

```
  GNU nano 8.3                                          /etc/bind/zonas/db.prueba.com
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     dns1.prueba.com. admin.prueba.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@           IN  NS      dns1.prueba.com.
dns1        IN  A       10.10.5.30
ldap        IN  A       10.10.5.30
_ldap._tcp  IN  SRV 0 5 389 ldap.prueba.com.
_ldaps._tcp IN  SRV 0 5 636 ldap.prueba.com.
```

El archivo **'db.5.10.10**' debe quedar de la siguiente manera:

```
  GNU nano 8.3                                                /etc/bind/zonas/db.5.10.10
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     dns1.prueba.com. admin.prueba.com. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
        IN      NS      dns1.prueba.com.
30      IN      PTR     dns1.prueba.com.
30      IN      PTR     ldap.prueba.com.
```

Parte 5. Configuración del cliente.

En esta parte de la práctica, debe estar encendida la máquina cliente (llamada 'desktop').

Pasos a seguir

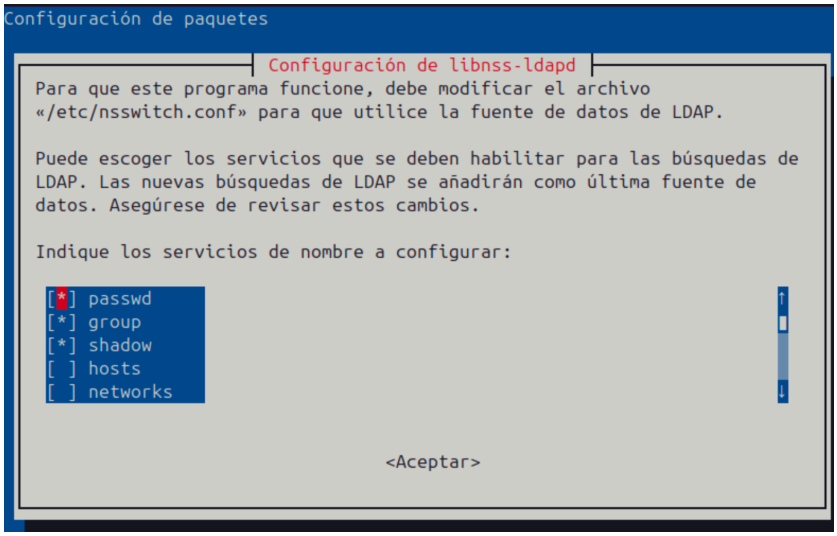
1. Actualiza el sistema: **sudo apt update**

2. Instala los paquetes correspondientes para LDAP:

sudo apt install libnss-ldapd libpam-ldapd nslcd ldap-utils -y

3. Configura LDAP: **sudo dpkg-reconfigure libnss-ldapd**

- Servicios → marcar passwd, group, shadow



4. Edita el fichero 'nsswitch.conf' y añade esta información (*solo deben estar estas líneas en el fichero, comenta con # el resto de líneas*): **sudo nano /etc/nsswitch.conf**

```
passwd: files systemd ldap
group: files systemd ldap
shadow: files ldap
```

5. Edita el fichero 'nslcd.conf ' y añade esta información (*solo deben estar estas líneas en el fichero, comenta con # el resto de líneas*): **sudo nano /etc/nslcd.conf**

```
uri ldap://10.10.5.30/
base dc=prueba,dc=com
ldap_version 3
```

6. Instala el módulo PAM (*Pluggable Authentication Modules*) correspondiente:

sudo apt install libpam-mkhomedir -y

***PAM, es un sistema que permite a Linux gestionar la autenticación de usuarios de manera modular y flexible. En lugar de tener un único método fijo para validar usuarios, PAM usa módulos (pequeños archivos o librerías) que se pueden añadir o quitar según el tipo de autenticación que quieras usar: local, LDAP, Kerberos, Active Directory, etc.*

7. Edita el archivo PAM: **sudo nano /etc/pam.d/common-session**

8. Añade esta línea al final del archivo:

session required pam_mkhomedir.so skel=/etc/skel/ umask=077

6. Reinicia el servicio y comprueba su estado:

sudo systemctl restart nslcd
sudo systemctl status nslcd

Parte 6. Pruebas de funcionamiento.

En esta parte de la práctica, debe estar encendida la máquina del servidor (llamada 'server') y la máquina cliente (llamada 'desktop').

Pasos a seguir

1. Comprueba la conectividad con el servidor desde la máquina cliente: **ping 10.10.5.30**

2. Comprueba que conectas con el servidor LDAP y te devuelve la entrada del usuario 'juan' desde la máquina cliente:

   ldapsearch -x -H ldap://10.10.5.30 -b "uid=juan,ou=usuarios,dc=prueba,dc=com"

```
profesora@profesora-Clienteprivado:~$ sudo ldapsearch -x -H ldap://10.10.5.30 -b"uid=juan,ou=usuarios,dc=prueba,dc=com"

# extended LDIF
#
# LDAPv3
# base <uid=juan,ou=usuarios,dc=prueba,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# juan, usuarios, prueba.com
dn: uid=juan,ou=usuarios,dc=prueba,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Juan Perez
sn: Perez
uid: juan
uidNumber: 10001
gidNumber: 10000
homeDirectory: /home/juan
loginShell: /bin/bash

# search result
search: 2
result: 0 Success

# numResponses: 2
```

3. Comprueba los usuarios LDAP desde la máquina cliente:

   id juan
   getent passwd juan

```
profesora@profesora-Clienteprivado:~$ id juan
uid=10001(juan) gid=10000(profesores) grupos=10000(profesores)
profesora@profesora-Clienteprivado:~$ getent passwd juan
juan:x:10001:10000:Juan Perez:/home/juan:/bin/bash
```

*** Estos comandos permiten verificar que el cliente está consultando correctamente el directorio LDAP. El comando **id** muestra la información de identidad del usuario juan tal como la ve el sistema*

operativo. El comando ***getent*** *consulta las fuentes de datos del sistema definidas en el fichero /etc/nsswitch.conf. La 'x' que aparece en el resultado representa la contraseña la cual no se muestra.*

4. Prueba el login con 'juan' desde la máquina cliente: **su - juan**

```
profesora@profesora-Clienteprivado:~$ su - juan
Contraseña:
Creando directorio «/home/juan».
juan@profesora-Clienteprivado:~$
```

Para salir del home del usuario 'juan' debes poner exit.

Ejercicios propuestos

1. Crea otros dos usuarios (APELLIDO1 y APELLIDO2) con diferentes uidNumber, siguiendo la jerarquía realizada durante la práctica.
2. Añade el usuario APELLIDO1 al grupo de 'profesores'.
3. Crea un grupo adicional llamado 'alumnos'. Añade al usuario APELLIDO2 a este nuevo grupo.
4. ¿Cómo sería el DIT tras los ejercicios anteriores?
5. Haz las pruebas de funcionamiento (*Parte 6 de la práctica*) para los nuevos usuarios.

Aunque no haya que entregar la práctica, se recomienda crear un documento con capturas de pantalla y explicaciones de los pasos realizados, tanto de la parte guiada como de los ejercicios propuestos. Esto os ayudará para tener vuestros propios apuntes de cara al examen.