

# **Práctica UD5:**

## **Servicio de directorio**

### **OpenLDAP**

Desenvolvemento de aplicacións web

**MP0614. Despregamento de aplicacións web**

## Sumario

Instrucciones .....	3
Ejercicio 1: Teoría de servicio de directorio .....	4
Ejercicio 2. Instalación de OpenLDAP e integración con Apache Web Server.....	5
Ejercicio 3. Instalación de OpenLDAP e integración con Apache Web Server mediante containers de docker .....	8
ANEXO. Información de apoyo. ....	12
Sobre los ejercicios .....	13

## Instrucciones

- Las capturas de las máquinas virtuales deben mostrar el nombre de la máquina.
- En el nombre de la máquina virtual debe contener la inicial y el apellido del alumno/a que entrega la práctica.
  - Por ejemplo, si creo una máquina virtual llamada "LDAP Server", debo nombrarla "jlopez LDAP Server".
- Las capturas deben de tener una calidad suficiente para que su contenido pueda ser legible.
- La entrega será en la tarea de la plataforma moodle mediante un fichero pdf practica\_x\_tu\_nombre.pdf (x es número de practica y tu\_nombre es tu nombre) en el que se puedan ver en las diferentes secciones lo solicitado.

## Ejercicio 1: Teoría de servicio de directorio

a) ¿Qué es un servicio de directorio? ¿De qué se encarga? ¿Para qué se utiliza en un entorno informático?

Un servicio de directorio, es una aplicación que nos permite gestionar, usuarios, equipos y recursos en red de nuestro entorno.

El ejemplo mas común de uso lo podemos ver en prácticamente cualquier entorno informático de una empresa, donde por necesidades obvias, necesitamos gestionar de manera interna nuestros usuarios, ordenadores y recursos en red, como pueden ser el acceso a determinados archivos o la aplicación de políticas sobre los equipos para evitar o forzar cierto tipo de comportamientos, por ejemplo, que un usuario no administrador no pueda ejecutar “Regedit.exe”

Pistas.

¿Qué es un servicio de directorio LDAP?

Teoría sobre o servizo de directorios - MediaWiki

b) ¿Qué es un DN (Distinguished Name) en LDAP?

El Distinguished Name hace referencia al nombre unico que identifica un recurso en LDAP, por ejemplo, tengo el usuario “david.rod” que dentro de LDAP pertenece a la unidad organizativa “Alumnos”, este es un usuario del dominio “davidrl.local”, pues su DN seria algo asi:

uid=david.rod ,ou=Alumnos,dc=davidrl,dc=local

Pistas

Cómo configurar el servidor OpenLDAP y autenticar la estación de trabajo del cliente

LDAP Explained: From Distinguished Names to User Authentication

c) ¿Qué herramienta se usa comúnmente para realizar búsquedas en un directorio LDAP? Pon algún ejemplo.

La herramienta que se suele usar es ldapsearch, es una herramienta por linea de comandos que nos permite buscar recursos dentro de nuestro LDAP.

Pongamonos en el caso que queremos buscar un host que tiene asignada de manera estatica la ip 192.168.0.10 y pertenece al domino “davidrl.local”

pongamonos en el caso de que en el servidor permita la autentificacion anonima (con lo que no necesitaríamos una cuenta de administrador)

En ese caso usariamos ldapsearch con los siguientes paramentos:

```
ldapsearch -x -b "dc=devconnected,dc=com" -H ldap://192.168.178.29
```

Los parametros hacen lo siguiente:

- x : indicamos que estamos usando la autentificacion basica
- b : indicamos sobre el dominio sobre el que hacemos la busqueda
- H : indicamos el nombre o IP del host que queremos buscar

Pista.

Cómo Buscar LDAP usando ldapsearch (Con Ejemplos) – devconnected | Adam Faliq

The ldapsearch Command-Line Tool

## Ejercicio 2. Instalación de OpenLDAP e integración con Apache Web Server

Instala y configura un servidor OpenLDAP en un entorno Linux.

Comprueba su integración configurando un servidor Apache Web Server para autenticarse contra el directorio LDAP.

### Requisitos previos

- Una distribución Linux (te sugiero Ubuntu/Debian).
- Acceso con privilegios al sistema.
- Instalación de Apache Web Server (puedes instalarlo si no está disponible).

Obviamente todo esto puede ser realizado en una máquina virtual de tu elección.

### 1. Instalación de OpenLDAP

#### 1.1 Instala el paquete OpenLDAP y las herramientas de cliente necesarias.

Instalamos Apache2 :

```
apt-get install apache2
```

Instalamos OpenLDAP:

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

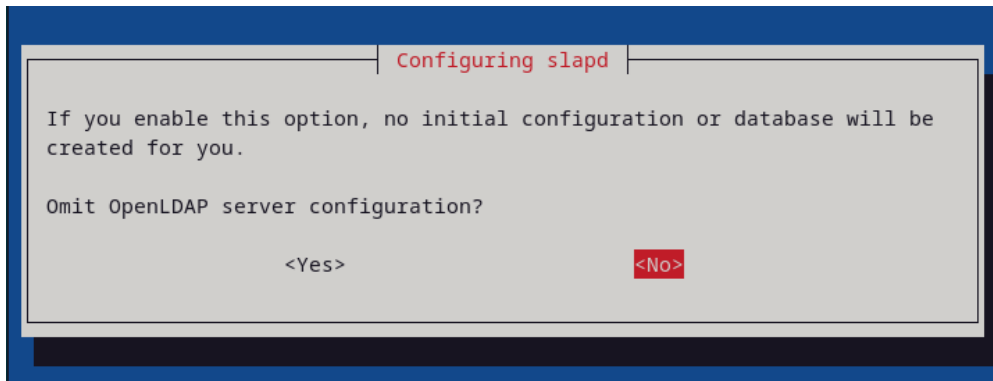
```
root@examenDespliegues:/home/davidrl# sudo apt-get install slapd ldap-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libodbc2
Suggested packages:
  libsasl2-modules-gssapi-mit | libsasl2-modules-gssapi-heimdal
  odbc-postgresql tdsodbc
The following NEW packages will be installed:
  ldap-utils libodbc2 slapd
0 upgraded, 3 newly installed, 0 to remove and 98 not upgraded.
Need to get 1,730 kB of archives.
After this operation, 5,950 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://deb.debian.org/debian bookworm/main amd64 libodbc2 amd64 2.3.11-2+deb12u1 [150 kB]
Get:2 http://deb.debian.org/debian bookworm/main amd64 slapd amd64 2.5.13+dfsg-5 [1,435 kB]
59% [2 slapd 983 kB/1,435 kB 68%] 32.0 kB/s 18s
```

#### 1.2 Configura OpenLDAP con un dominio base, por ejemplo, dc=miempresa,dc=com.

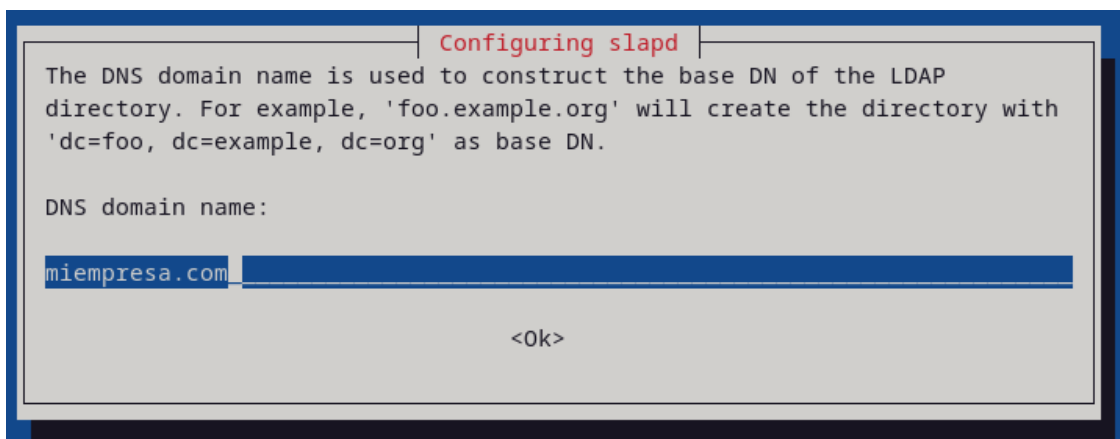
Reconfiguramos el LDAP usando el siguiente comando:

```
dpkg-reconfigure slapd
```

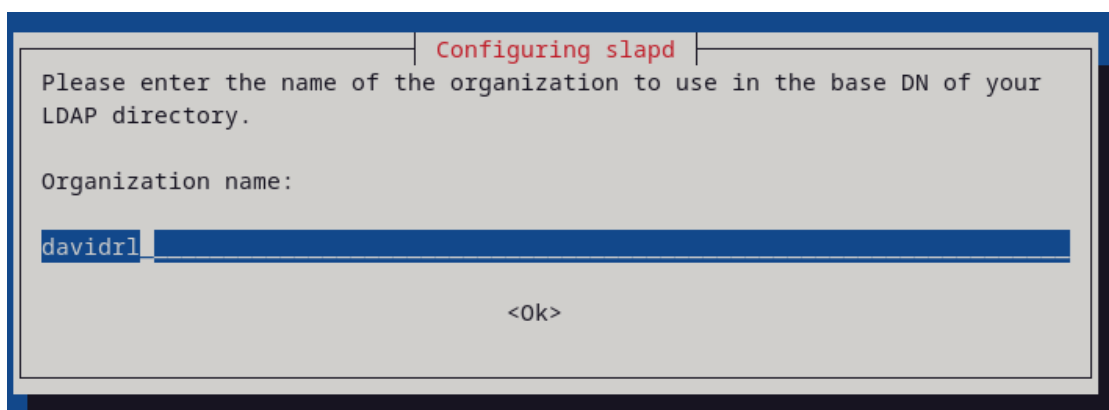
Nos llevara al asistente grafico, en la primera pantalla decimos que no:



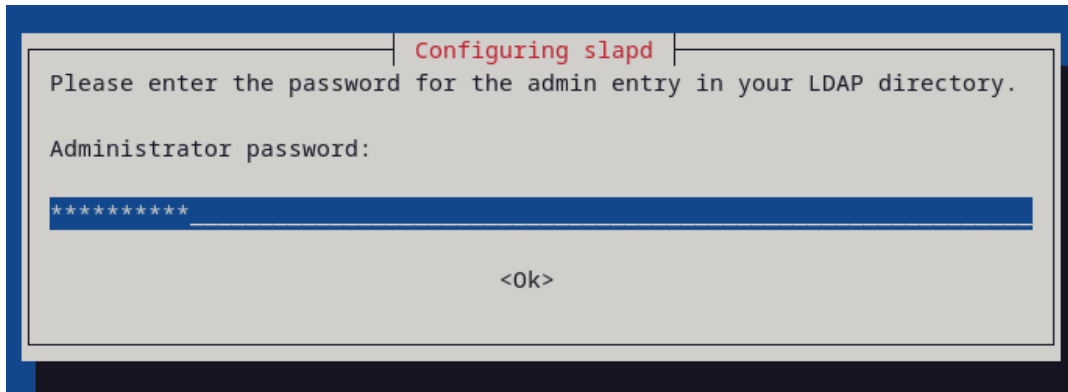
Como queremos que nuestro dominio base se llame dc=miempresa,dc=com , en esta segunda pantalla deberemos poner el nombre del dc como enseño a continuacion:



Por ultimo indicamos el nombre de la organización, como no se ha especificado un nombre, le llamare davidrl:



Nos pedira la contraseña del dominio:



Y las siguientes pantallas deberemos responder YES.

Una vez hecho comprobamos que se han efectuado los cambios con el siguiente comando:

slapcat

```
entryCSN: 20250117195038.842701Z#000000#000#000000
modifiersName: cn=admin,dc=myguest,dc=virtualbox,dc=org
modifyTimestamp: 20250117195038Z

dn: dc=miempresa,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: davidrl
dc: miempresa
structuralObjectClass: organization
entryUUID: 41f7dda0-6959-103f-831f-0fb3152c605c
creatorsName: cn=admin,dc=miempresa,dc=com
createTimestamp: 20250117195908Z
entryCSN: 20250117195908.753995Z#000000#000#000000
modifiersName: cn=admin,dc=miempresa,dc=com
modifyTimestamp: 20250117195908Z

root@examenDespliegues:/home/davidrl#
```

Tambien podemos usar lo siguiente:

ldapwhoami -H ldap:// -x

```
root@examenDespliegues:/home/davidrl# ldapwhoami -H ldap:// -x
anonymous
root@examenDespliegues:/home/davidrl#
```



### 1.3 Crea al menos dos usuarios dentro del directorio LDAP utilizando herramientas como ldapadd.

Ahora voy a crear dos usuarios, pepe y ana dentro de nuestro LDAP, para ello vamos a crear primero una Unidad Organizativa(OU) que los contenga y un Grupo dentro de la misma al que perteneceran dichos usuarios.

Para crear la OU hacemos lo siguiente:

-Vamos a la carpeta /home y creamos un nuevo fichero “ou.ldif”:

```
cd /home
```

```
nano ou.ldif
```

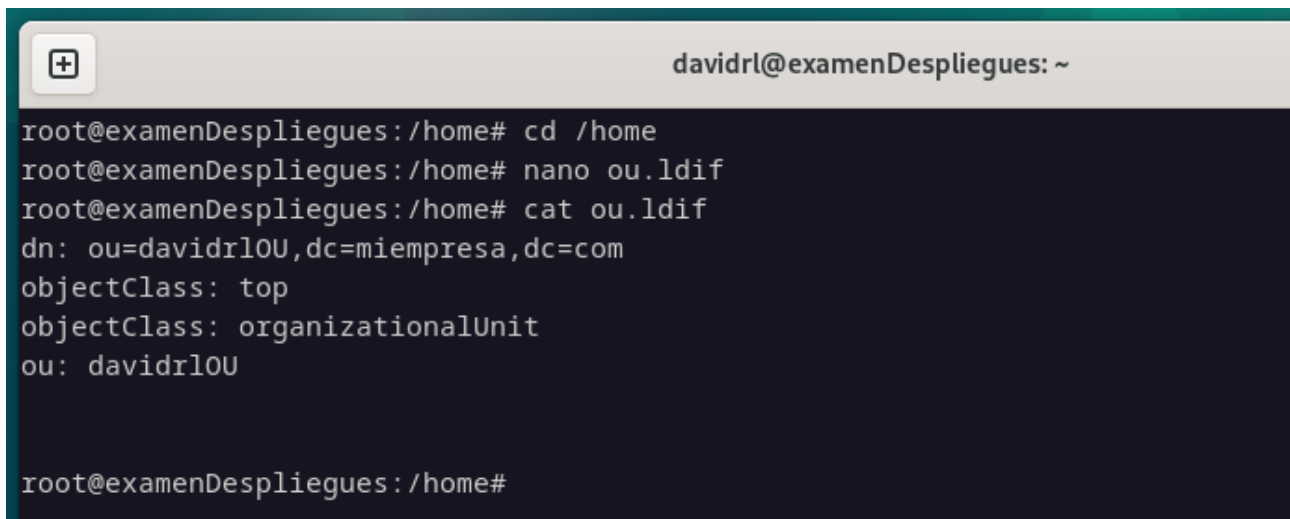
-Dentro de este “ou.ldif”: ponemos lo siguiente:

```
dn: ou=<nombreOU>,dc=<nombredominio>,dc=<nombredominio2>
```

```
objectClass: top
```

```
objectClass: organizationalUnit
```

```
ou: <nombreOU>
```

A terminal window titled 'davidrl@examenDespliegues: ~' showing a series of commands and their outputs. The user navigates to the /home directory, creates a file named ou.ldif using nano, and then displays its contents with cat. The file contains LDAP entry details for an organizational unit named 'davidrlOU' under the domain 'miempresa.com'.

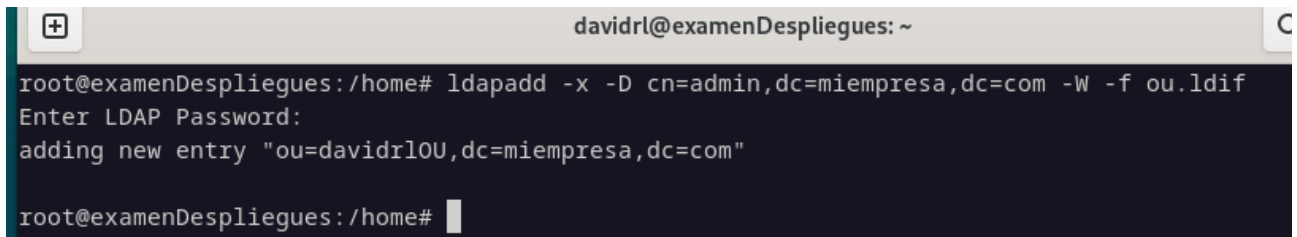
```
root@examenDespliegues:/home# cd /home
root@examenDespliegues:/home# nano ou.ldif
root@examenDespliegues:/home# cat ou.ldif
dn: ou=davidrlOU,dc=miempresa,dc=com
objectClass: top
objectClass: organizationalUnit
ou: davidrlOU

root@examenDespliegues:/home#
```

Ahora cargamos el archivo en nuestro ldap usando el siguiente comando para crear la OU:

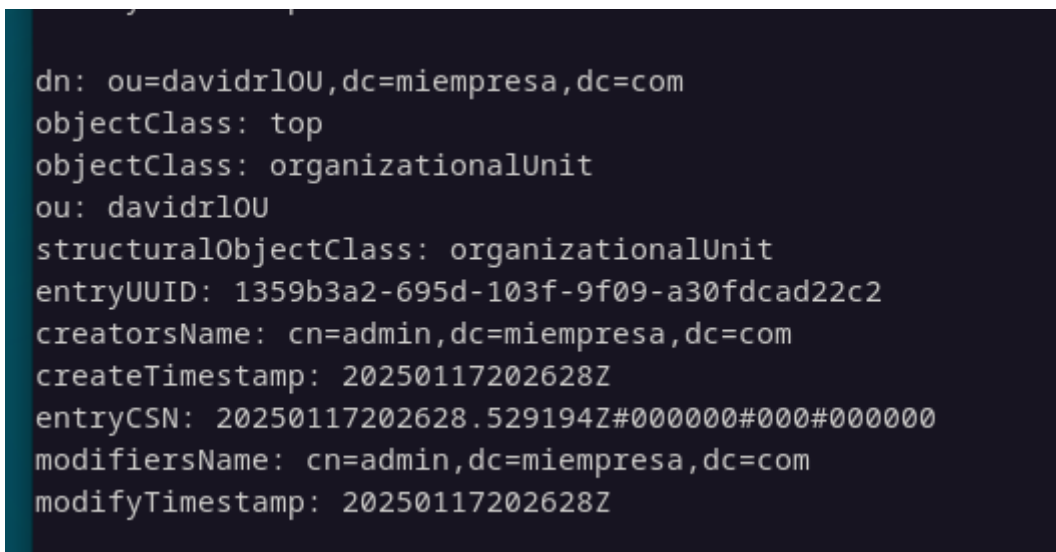
`ldapadd -x -D cn=admin,dc=<nombreDominio1>,dc=<nombreDominio2> -W -f ou.ldif`

Veremos algo así:



```
davidrl@examenDespliegues: ~  
root@examenDespliegues:/home# ldapadd -x -D cn=admin,dc=miempresa,dc=com -W -f ou.ldif  
Enter LDAP Password:  
adding new entry "ou=davidrlOU,dc=miempresa,dc=com"  
root@examenDespliegues:/home#
```

Podemos comprobar que esta usando de nuevo slapcat:



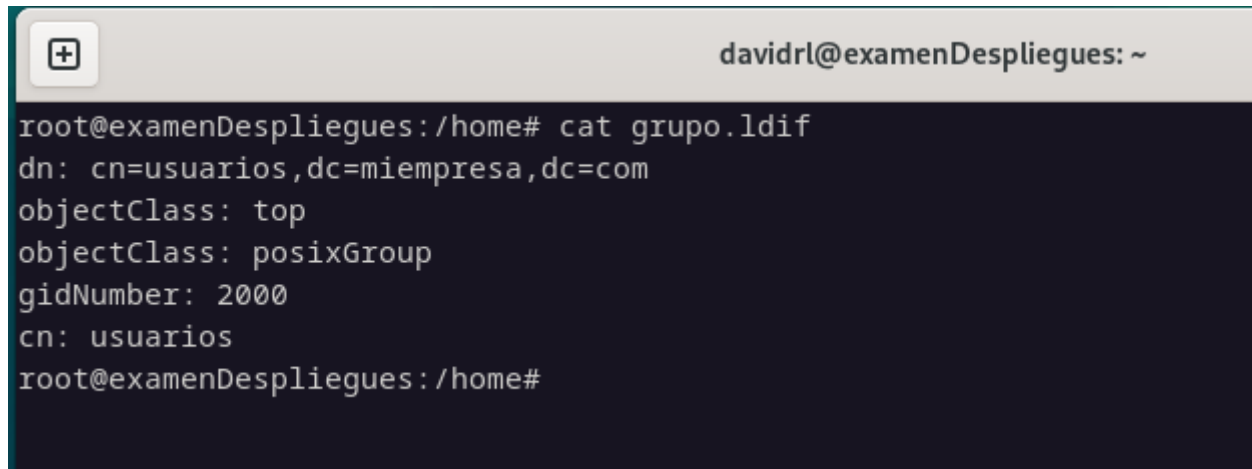
```
dn: ou=davidrlOU,dc=miempresa,dc=com  
objectClass: top  
objectClass: organizationalUnit  
ou: davidrlOU  
structuralObjectClass: organizationalUnit  
entryUUID: 1359b3a2-695d-103f-9f09-a30fdcad22c2  
creatorsName: cn=admin,dc=miempresa,dc=com  
createTimestamp: 20250117202628Z  
entryCSN: 20250117202628.529194Z#000000#000#000000  
modifiersName: cn=admin,dc=miempresa,dc=com  
modifyTimestamp: 20250117202628Z
```

Ahora voy a crear el grupo, el proceso es similar, creare un nuevo archivo llamado grupo.ldif y le pondre lo siguiente:

```
dn: cn=<nombreGrupo>,dc=<nombreDominio1>,dc=<nombreDominio2>  
objectClass: top  
objectClass: posixGroup
```

gidNumber: 2000

cn: <nombreGrupo>

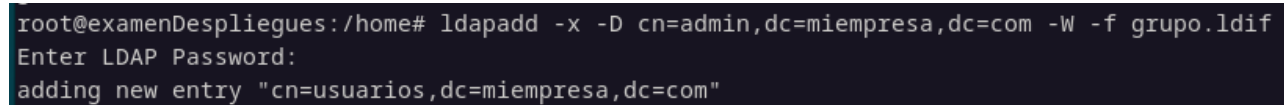
A terminal window with a title bar showing a plus icon and the user 'davidrl@examenDespliegues: ~'. The terminal content shows the command 'cat grupo.ldif' being executed, displaying the LDAP entry for a group named 'usuarios' with gidNumber 2000.

```
root@examenDespliegues:/home# cat grupo.ldif
dn: cn=usuarios,dc=miempresa,dc=com
objectClass: top
objectClass: posixGroup
gidNumber: 2000
cn: usuarios
root@examenDespliegues:/home#
```

**\*\*Es importante resaltar que el gidNumber en cada grupo debe ser distinto y que dicho parametro a partir de 1000 se usa en usuarios locales**

Usamos el siguiente comando para agregar el grupo a LDAP:

`ldapadd -x -D cn=admin,dc=<nombreDominio1>,dc=<nombreDominio2> -W -f ou.ldif`

A terminal window showing the execution of the 'ldapadd' command. It prompts for the LDAP password and then confirms the addition of a new entry for the 'usuarios' group.

```
root@examenDespliegues:/home# ldapadd -x -D cn=admin,dc=miempresa,dc=com -W -f grupo.ldif
Enter LDAP Password:
adding new entry "cn=usuarios,dc=miempresa,dc=com"
```

Finalmente vamos a agregar los usuarios, el proceso es similar, creo un nuevo archivo usuarios.ldif ,la estructura para cada usuario es la siguiente:

dn: uid=<nombreUsuario>,dc=<nombreDominio1>,dc=<nombreDominio2>

objectClass: top

objectClass: posixAccount

objectClass: inetOrgPerson

objectClass: person

cn: <nombreUsuario>

uid: <nombreUsuario>

uidNumber: 2000

gidNumber: 2000

homeDirectory: /home/<nombreUsuario>

loginShell: /bin/bash

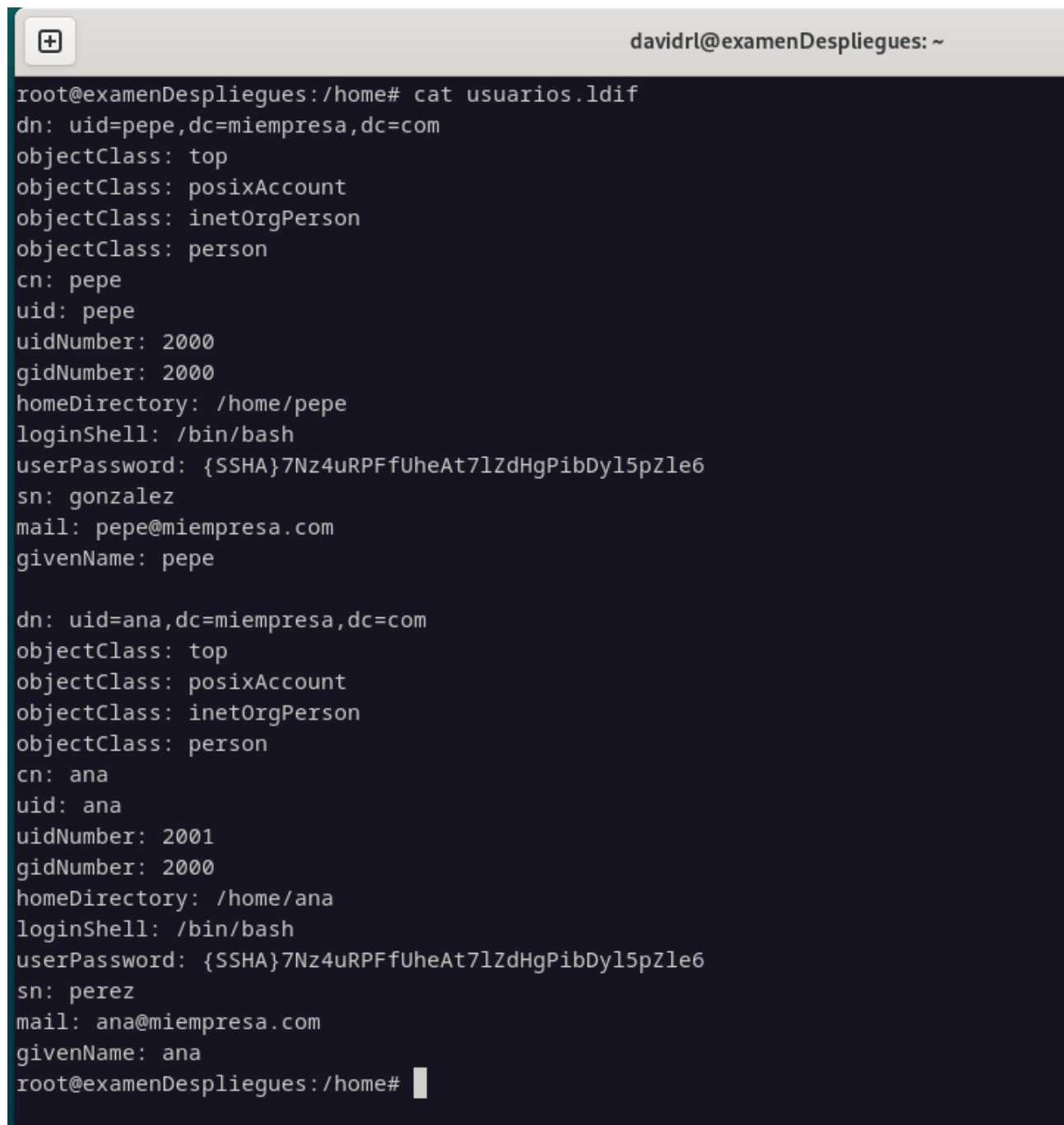
userPassword: {SSHA}7Nz4uRPFfUheAt7lZdHgPibDyl5pZle6

sn: <apellido>

mail: <correoUsuario>

givenName: <nombreUsuario>

Quedaria asi:

A terminal window titled 'davidrl@examenDespliegues: ~' showing the output of the command 'cat usuarios.ldif'. The output displays two LDAP entries. The first entry is for 'pepe' with uid=pepe, cn=pepe, uidNumber=2000, gidNumber=2000, homeDirectory=/home/pepe, loginShell=/bin/bash, userPassword={SSHA}7Nz4uRPFfUheAt7lZdHgPibDyl5pZle6, sn=gonzalez, mail=pepe@miempresa.com, and givenName=pepe. The second entry is for 'ana' with uid=ana, cn=ana, uidNumber=2001, gidNumber=2000, homeDirectory=/home/ana, loginShell=/bin/bash, userPassword={SSHA}7Nz4uRPFfUheAt7lZdHgPibDyl5pZle6, sn=perez, mail=ana@miempresa.com, and givenName=ana. The terminal prompt is root@examenDespliegues:/home#.

```
root@examenDespliegues:/home# cat usuarios.ldif
dn: uid=pepe,dc=miempresa,dc=com
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: pepe
uid: pepe
uidNumber: 2000
gidNumber: 2000
homeDirectory: /home/pepe
loginShell: /bin/bash
userPassword: {SSHA}7Nz4uRPFfUheAt7lZdHgPibDyl5pZle6
sn: gonzalez
mail: pepe@miempresa.com
givenName: pepe

dn: uid=ana,dc=miempresa,dc=com
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: ana
uid: ana
uidNumber: 2001
gidNumber: 2000
homeDirectory: /home/ana
loginShell: /bin/bash
userPassword: {SSHA}7Nz4uRPFfUheAt7lZdHgPibDyl5pZle6
sn: perez
mail: ana@miempresa.com
givenName: ana
root@examenDespliegues:/home#
```

El uidNumber tiene que ser unico para cada usuario y el gidNumber es el numero del grupo asignado.

Para generar las contraseña usare el comando:

slappasswd

```
root@examenDespliegues:/home# slappasswd
New password:
Re-enter new password:
{SSHA}0IJ07KRBWFTx3gLj1KoRaphlYTifX70
root@examenDespliegues:/home#
```

Copiamos el texto generado al campo Userpassword de cada usuario.

Una vez hecho, podemos usar el comando usado anteriormente para añadir los usuarios:

```
root@examenDespliegues:/home# ldapadd -x -D cn=admin,dc=miempresa,dc=com -W -f usuarios.ldif
Enter LDAP Password:
adding new entry "uid=pepe,dc=miempresa,dc=com"

adding new entry "uid=ana,dc=miempresa,dc=com"

root@examenDespliegues:/home#
```

## 2. Configuración de Apache con módulo LDAP

### 2.2 Configura un directorio o recurso protegido en Apache para que requiera autenticación mediante LDAP.

### 2.3 Proporciona las credenciales necesarias para que Apache pueda conectarse al servidor LDAP.

Primero vamos al archivo de configuración del sitio en `/etc/apache2/sites-available/davidrl.conf`

Y añadimos la siguiente entrada:

```
<Directory /var/www/html/<nombreDirectorio> >

    AuthType Basic

    AuthName "LDAP Authentication"

    AuthBasicProvider ldap

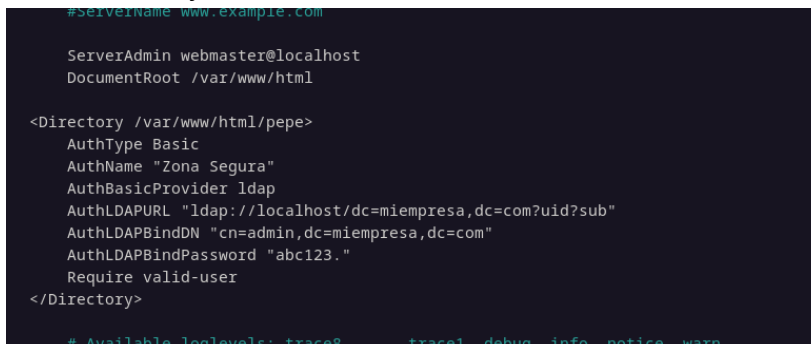
    AuthLDAPURL "ldap://<LDAP_SERVER_IP>/dc=example,dc=com?uid?sub"

    AuthLDAPBindDN "cn=<nombreUsuarioAdmin>,dc=ejemplo,dc=com"

    AuthLDAPBindPassword "contraseñaAdmin"

    Require valid-user

</Directory>
```



```
#ServerName www.example.com

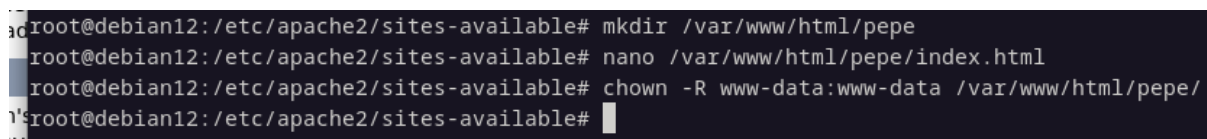
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html

<Directory /var/www/html/pepe>
    AuthType Basic
    AuthName "Zona Segura"
    AuthBasicProvider ldap
    AuthLDAPURL "ldap://localhost/dc=miempresa,dc=com?uid?sub"
    AuthLDAPBindDN "cn=admin,dc=miempresa,dc=com"
    AuthLDAPBindPassword "abc123."
    Require valid-user
</Directory>

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
```

creamos el directorio `/pepe` y un archivo `index.html` y le damos permisos a `www-data` de manera recursiva sobre el directorio de `pepe`:

```
chown -R www-data:www-data /var/www/html/pepe/
```



```
root@debian12:/etc/apache2/sites-available# mkdir /var/www/html/pepe
root@debian12:/etc/apache2/sites-available# nano /var/www/html/pepe/index.html
root@debian12:/etc/apache2/sites-available# chown -R www-data:www-data /var/www/html/pepe/
root@debian12:/etc/apache2/sites-available#
```

### 2.1 Asegúrate de que Apache tenga habilitado el módulo `mod_authnz_ldap`.

Ahora habilitamos el modulo de apache2 `authnz_ldap`

a2enmod authnz\_ldap

```
davidrl@debian12: ~  
  
root@debian12:/home/davidrl# a2enmod authnz_ldap  
Considering dependency ldap for authnz_ldap:  
Module ldap already enabled  
Module authnz_ldap already enabled  
root@debian12:/home/davidrl#
```

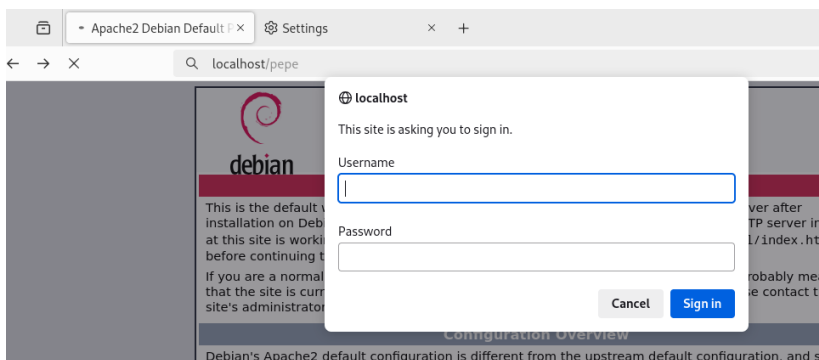
y levantamos el sitio davidrl.conf

a2ensite davidrl.conf

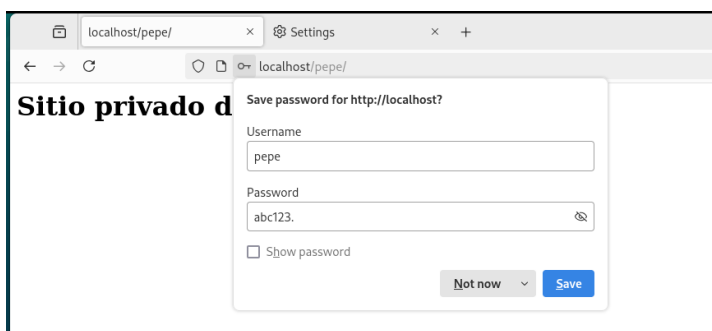
y reiniciamos el servicio de apache2

### 3. Pruebas de integración

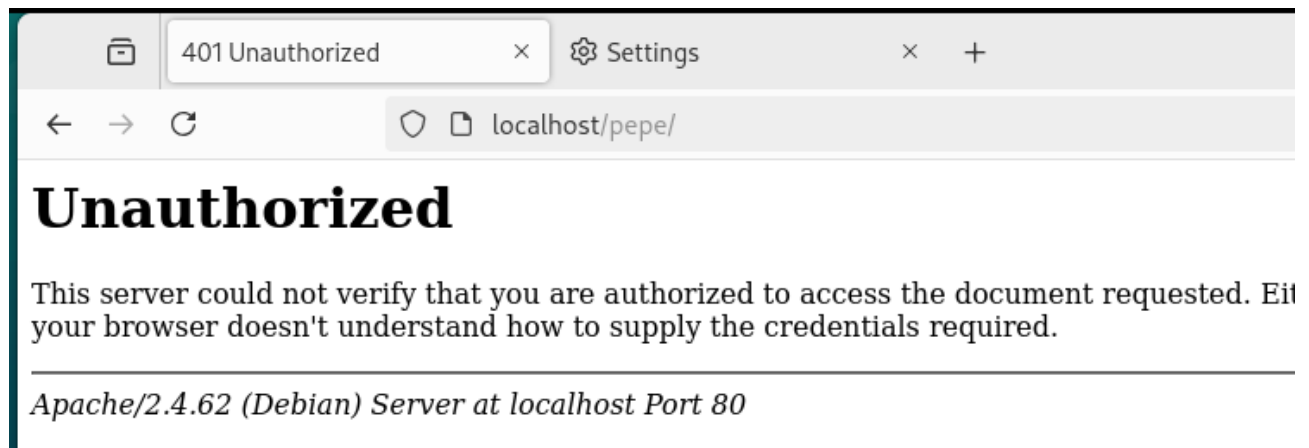
**3.1 Comprueba que los usuarios creados en OpenLDAP puedan autenticarse correctamente al acceder al recurso protegido en Apache.**



Accedemos con pepe:



**3.2 Realiza pruebas con credenciales incorrectas para validar que el sistema rechaza accesos no autorizados.**





## **Ejercicio 3. Instalación de OpenLDAP e integración con Apache Web Server mediante containers de docker**

Implementa un servidor OpenLDAP y un servidor Apache Web Server utilizando contenedores Docker.

Configurarás ambos servicios para que Apache utilice OpenLDAP como servidor de autenticación.

Requisitos previos:

- Una distribución Linux (te sugiero Ubuntu/Debian).
- Acceso con privilegios al sistema.
- Instalación de docker

Obviamente todo esto puede ser realizado en una máquina virtual de tu elección.

### **1. Preparar el entorno**

**1.1 Crea un directorio de trabajo para el proyecto (por ejemplo, openldap-docker).**

**1.2 Diseña un archivo docker-compose.yml que incluya servicios para OpenLDAP y Apache Web Server**

### **2. Configura el servidor OpenLDAP**

**2.1 Define un volumen para almacenar los datos persistentes del directorio LDAP.**

**2.2 Configura un dominio base, por ejemplo, dc=miempresa,dc=com, y un usuario administrador.**

**2.3 Carga una configuración inicial creando dos usuarios LDAP.**

### **3. Configurar el servidor Apache Web Server**

**3.1 Usa una imagen oficial de Apache con soporte para mod\_authnz\_ldap.**

**3.2 Configura un recurso protegido que requiera autenticación mediante OpenLDAP.**

#### **4. Comprueba la correcta integración**

**4.1 Verifica que puedes acceder al recurso protegido en Apache utilizando las credenciales almacenadas en OpenLDAP.**

**4.2 Asegúrate de que los accesos no autorizados son bloqueados correctamente.**

## **ANEXO. Información de apoyo.**

Estos enlaces te pueden servir de apoyo y guía para la realización de las tareas.

En general, para todas las tareas de este módulo, una muy buena referencia es esta:

<https://www.server-world.info/en/>

Y en concreto para OpenLDAP:

Ubuntu 22.04 LTS : OpenLDAP : Configure LDAP Server : Server World

Ubuntu 22.04 LTS : OpenLDAP : Add User Accounts : Server World

Ubuntu 22.04 LTS : OpenLDAP : LDAP Account Manager : Server World

Otras referencias útiles:

Práctica sobre o servizo de directorios - MediaWiki

Install and configure LDAP - Ubuntu Server documentation

How to set up LDAP users and groups - Ubuntu Server documentation

## Sobre los ejercicios

El ejercicio 1 es una introducción teórica al servicio de directorio y a sus posibilidades. Puedes usar ChatGPT u otras inteligencias para aprender y resolver la tarea... pero asegúrate de comprender lo que se pregunta y no hacer un mero “copia y pega”.

El ejercicio 2 es el centro de la tarea... instalar el servidor OpenLDAP, crear algunos usuarios, integrarlo con un Apache Web Server, y comprobar el funcionamiento

El ejercicio 3 es lo mismo... ¡pero con containers de docker!

En el examen se pedirá lo mismo que en el ejercicio 2 y 3, dando la alternativa para que lo resolváis de una manera u otra.

En esta práctica, os permito que alternativamente escojais una de las dos formas de resolverla. Y si la resolvéis de las dos, os daré 0,25 puntos optativos extra para esta segunda evaluación.