

TAREA LDAP Y DNS

23/24 DAW

Sumario

CONTEXTO.....	3
Apartado 1. Cuestionario sobre LDAP.....	4
Apartado 2. Cuestionario sobre DNS.....	5
Apartado 3. OpenLDAP.....	7
Apartado 4. Objetos de OpenLDAP.....	14
Apartado 5. Integración con Apache/FTP/aplicaciones (Opcional para un punto más de la nota)....	19

CONTEXTO

Aprenderemos sobre OpenLDAP y DNS

Documentar con explicaciones y las capturas necesarias que funciona cada uno de los puntos solicitados.

Apartado 1. Cuestionario sobre LDAP

1. ¿Qué es OpenLDAP?

- a) Un sistema operativo privativo
- b) Un servidor de bases de datos relacional
- c) Un software libre que implementa un servicio de directorio**
- d) Un servicio de correo electrónico

2. ¿Cuál es el puerto por defecto utilizado por OpenLDAP?

- a) 80
- b) 143
- c) 389**
- d) 8080

3. ¿Qué formato de datos utiliza OpenLDAP para almacenar la información de directorio?

- a) XML
- b) JSON
- c) LDIF**
- d) YAML

4. ¿Qué comando se utiliza comúnmente para agregar un nuevo registro en un directorio OpenLDAP?

- a) ldapsearch
- b) ldapdelete
- c) ldapadd**
- d) ldapmodify

Pistas:

[Teoría sobre o servizo de directorios - MediaWiki \(cifprodolfoucha.es\)](#)

[Práctica sobre o servizo de directorios - MediaWiki \(cifprodolfoucha.es\)](#)

Apartado 2. Cuestionario sobre DNS

1. ¿Qué significa DNS?

a) Digital Network Service

b) Domain Name System

c) Dynamic Naming Server

d) Data Network Security

2. ¿Cuál es el propósito principal del servicio DNS?

a) Enviar correos electrónicos

b) Traducir nombres de dominio a direcciones IP

c) Almacenar archivos en la nube

d) Encriptar conexiones de red

3. ¿Qué comando permite instalar un servicio DNS en Ubuntu?

a) apt install bind9 bind9util

b) apt install dns-service

c) dig dhcp

d) host nslookup

4. ¿Cuál es el puerto estándar utilizado por DNS para las consultas?

a) 80

b) 53

c) 443

d) 21

5. ¿Qué tipo de registro en DNS asocia un nombre de dominio a una dirección IPv4?

a) MX

b) CNAME

c) A

d) AAAA

6. ¿Cuál es el propósito del protocolo DNSSEC?

- a) Aumentar la velocidad de resolución de DNS
- b) Proteger contra ataques de envenenamiento de caché
- c) Encriptar las consultas DNS**
- d) Gestionar el tráfico de red

7. ¿Qué registro DNS se utiliza para identificar el servidor de correo electrónico de un dominio?

- a) A
- b) MX**
- c) NS
- d) TXT

8. ¿Qué comando se utiliza comúnmente para diagnosticar problemas de resolución DNS en sistemas Unix/Linux?

- a) ipconfig
- b) dig**
- c) ping
- d) traceroute

Pistas.

[Teoría sobre o Servizo de nomes de dominio - MediaWiki \(cifprodolfoucha.es\)](https://cifprodolfoucha.es/wiki/Teoría_sobre_o_Servizo_de_nomes_de_dominio)

[Prácticas sobre o servizo de resolución de nomes - MediaWiki \(cifprodolfoucha.es\)](https://cifprodolfoucha.es/wiki/Prácticas_sobre_o_servizo_de_resolución_de_nomes)

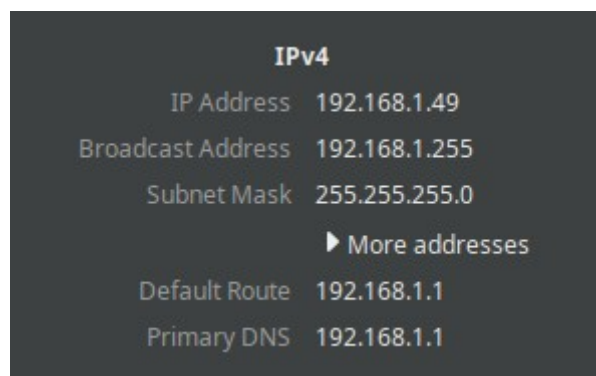
Apartado 3. OpenLDAP.

En este apartado, configuraremos un servicio de directorio con OpenLDAP en un entorno Ubuntu 22.04 (u otra distro de tu elección), Instalar un servidor Ubuntu 18.04 con OpenLDAP.

El nombre Dominio que vamos a utilizar será lbk.local.

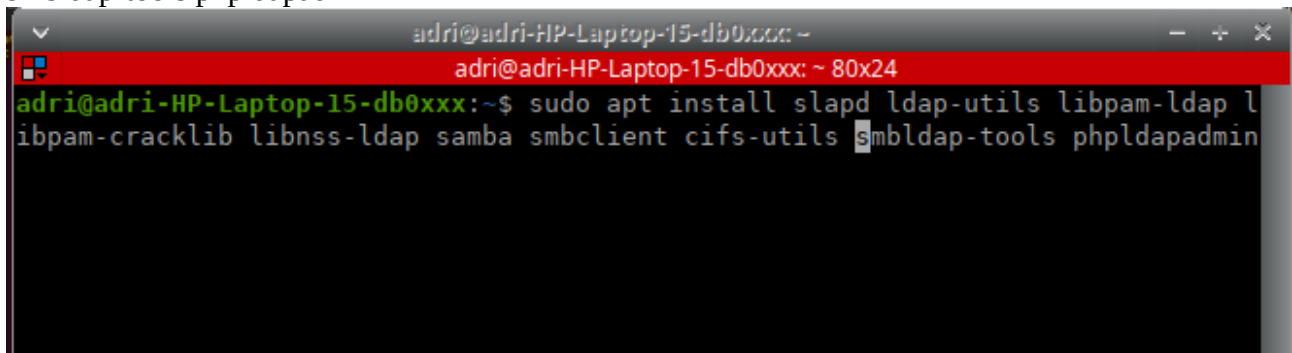
Instalaremos los servicios necesarios en el dominio GNU/Linux para que los equipos con sistema operativo Ubuntu se agreguen como clientes del dominio.

Estoy en un Xubuntu 22.04 y mi IP es la siguiente

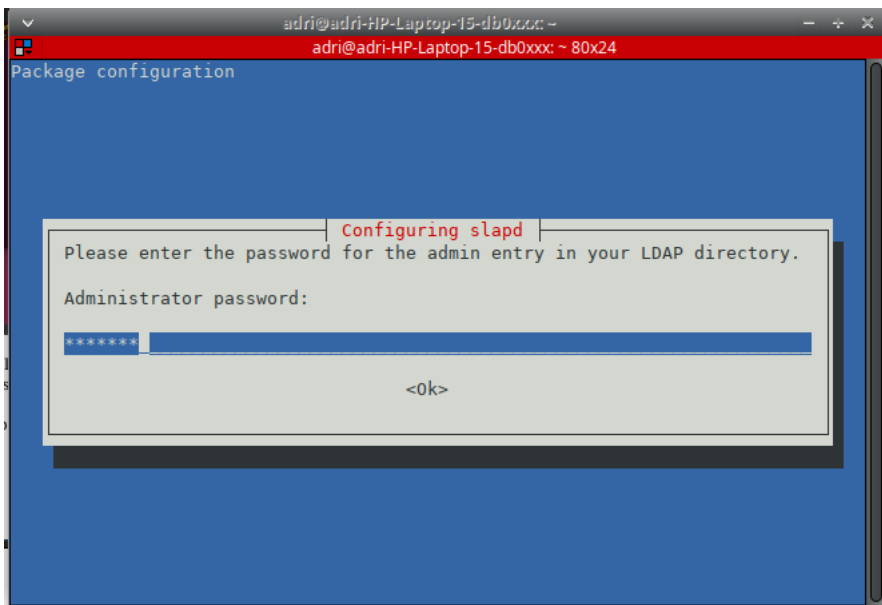


después de un *sudo apt update*,ejecuto el siguiente comando:

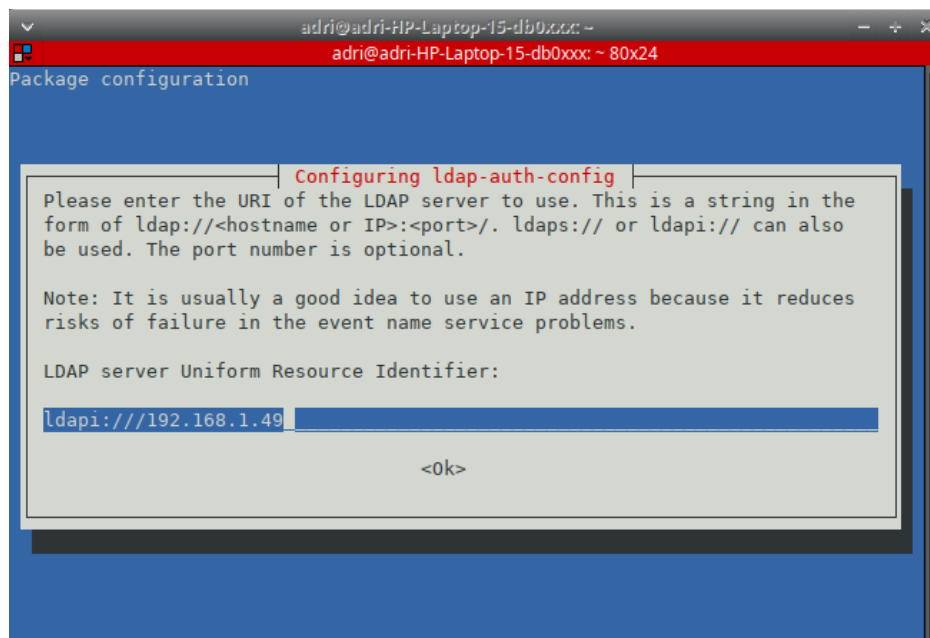
```
sudo apt install slapd ldap-utils libpam-ldap libpam-cracklib libnss-ldap samba smbclient cifs-utils  
smbldap-tools phpldapadmin
```



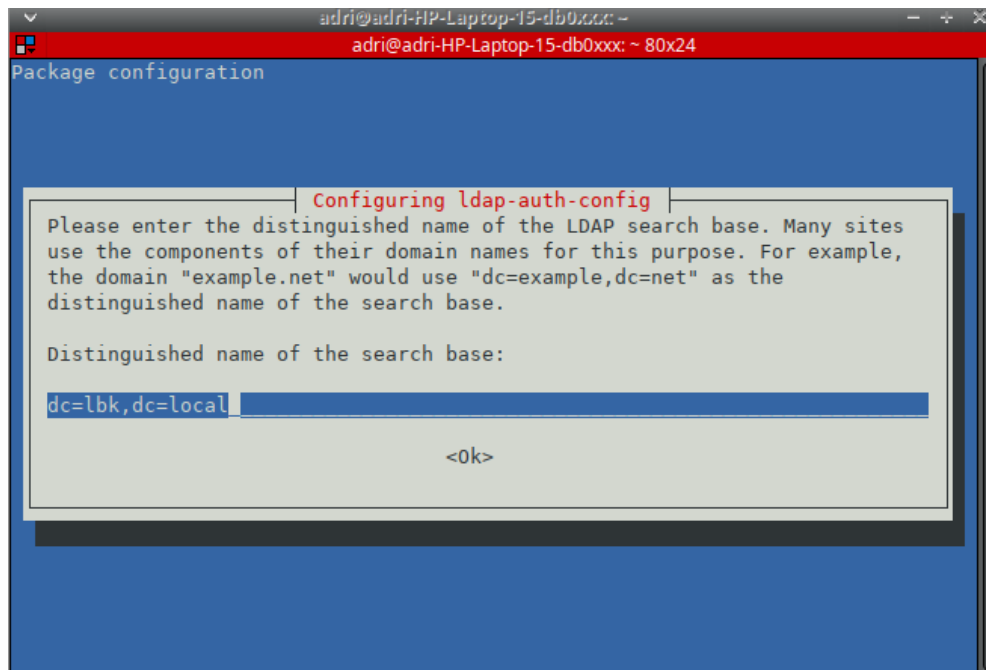
Inserto contraseña del administrador de ldap



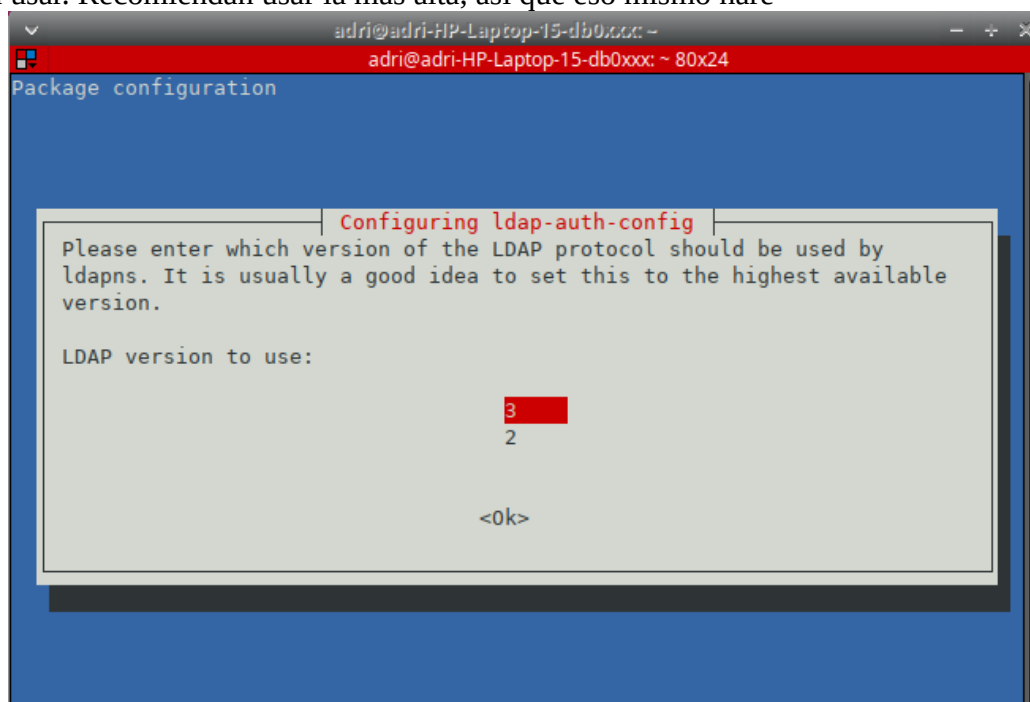
Ahora inserto la IP de mi equipo en el URI



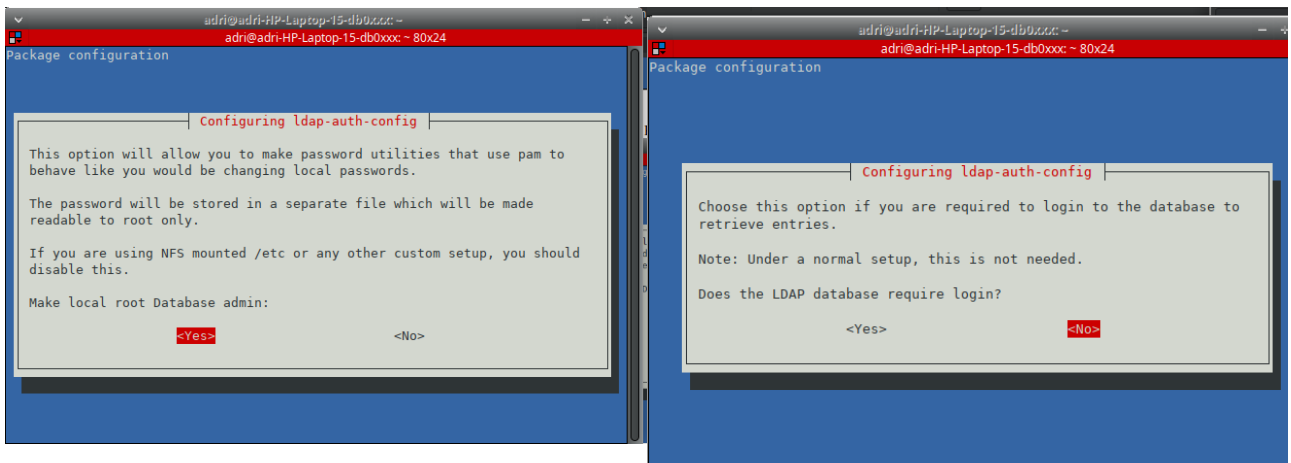
Como nuestro dominio tiene de nombre *lbk.local*, los inserto como nombres en los dc



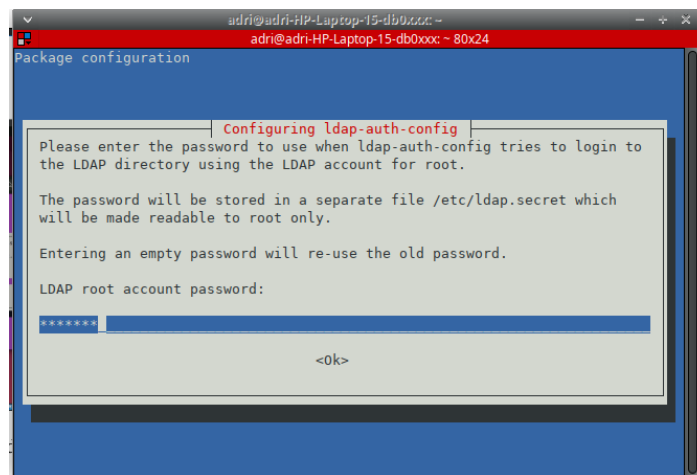
Versión a usar. Recomiendan usar la más alta, así que eso mismo haré



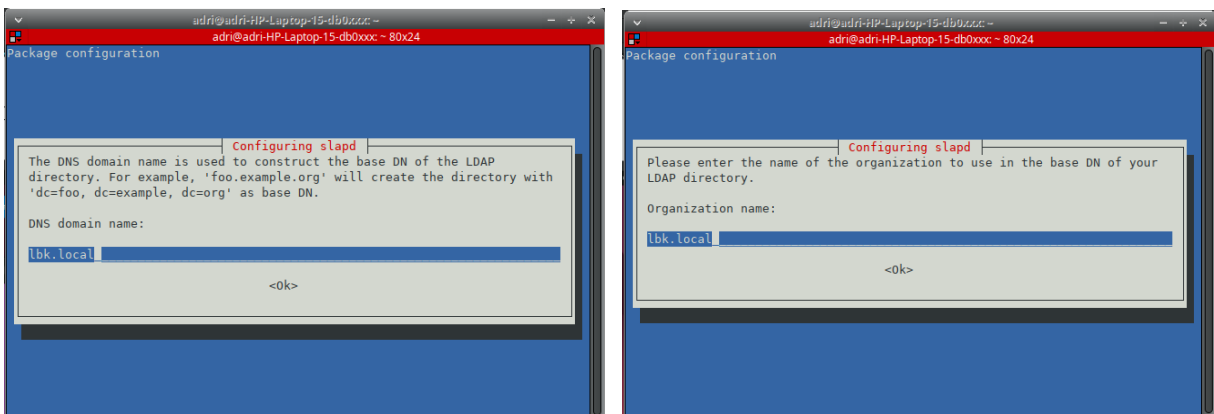
Configuración de contraseñas y login



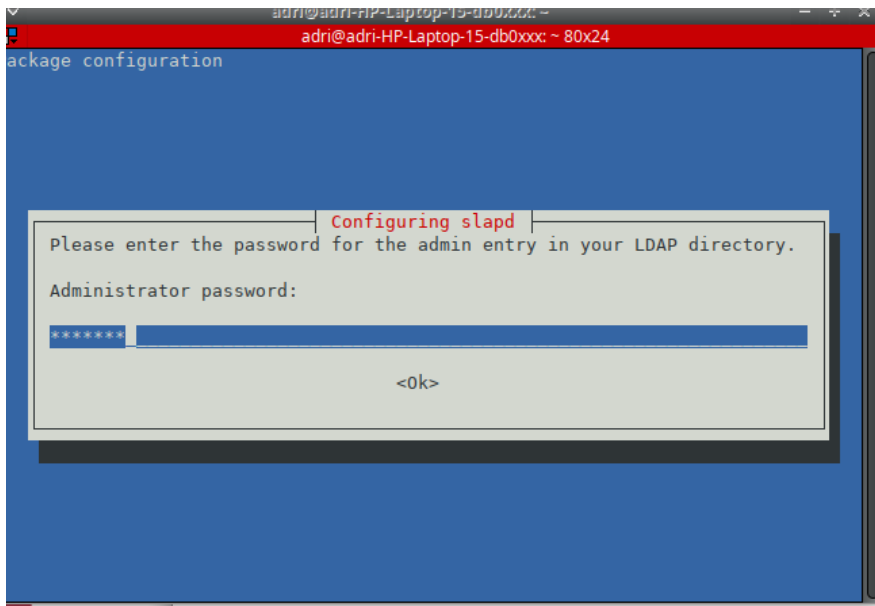
Cuenta root



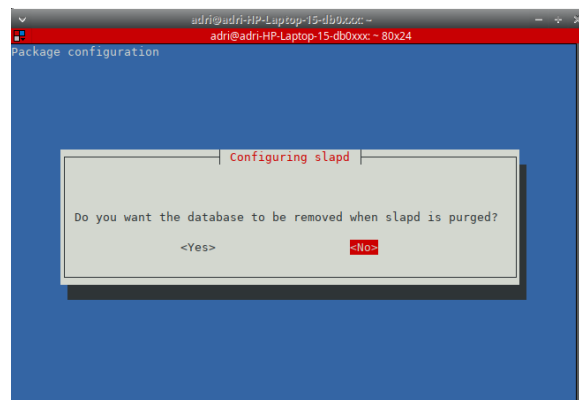
Luego, ejecutas el comando `sudo dpkg-reconfigure slapd`
Te preguntan si quieres saltar la configuración, presionas no



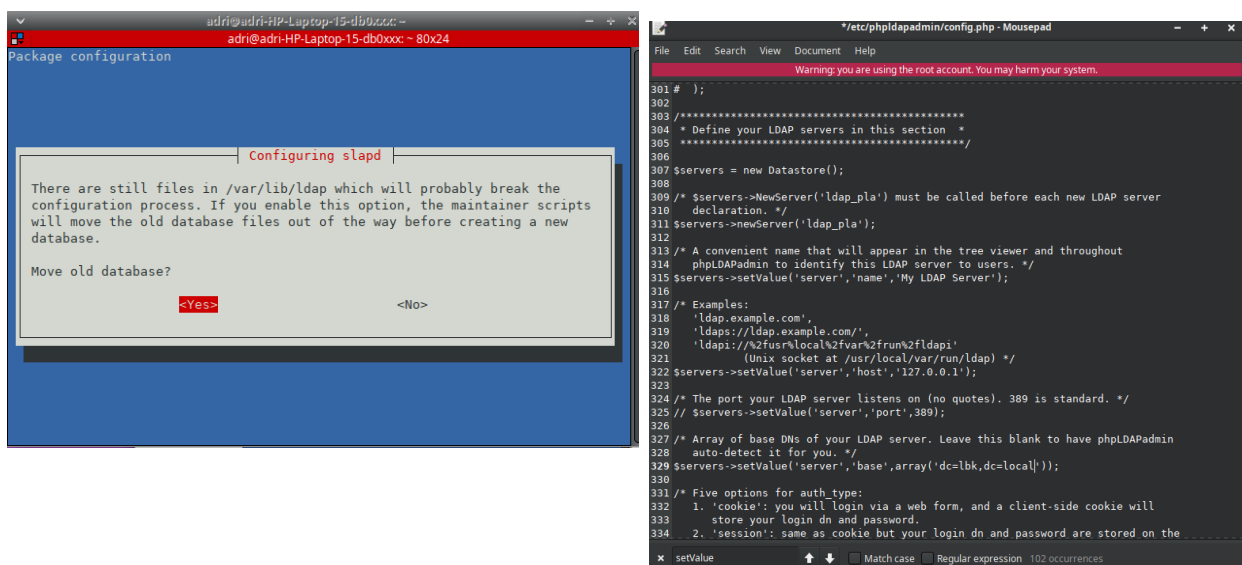
Contraseña de administrador (el usuario te lo piden antes, y escribí “cn=admin,dc=lbk,dc=local”)



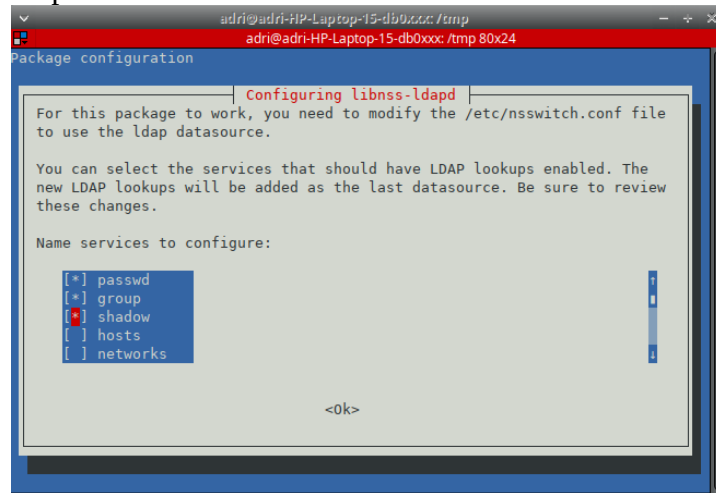
Borrar la BBDD si se borra el paquete slapd



Configuración de BBDD (el fichero de texto se cambia la línea 329)

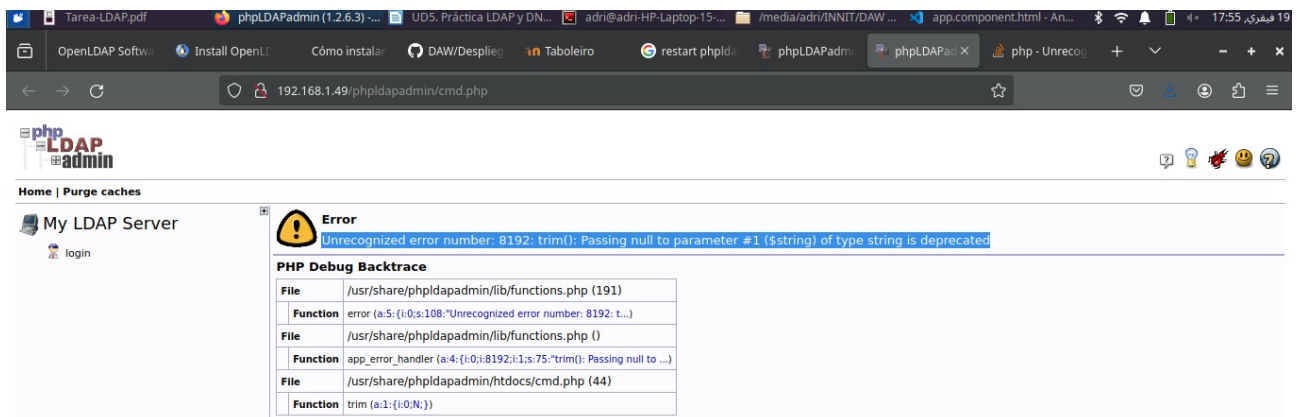


sudo apt install libnss-ldapd

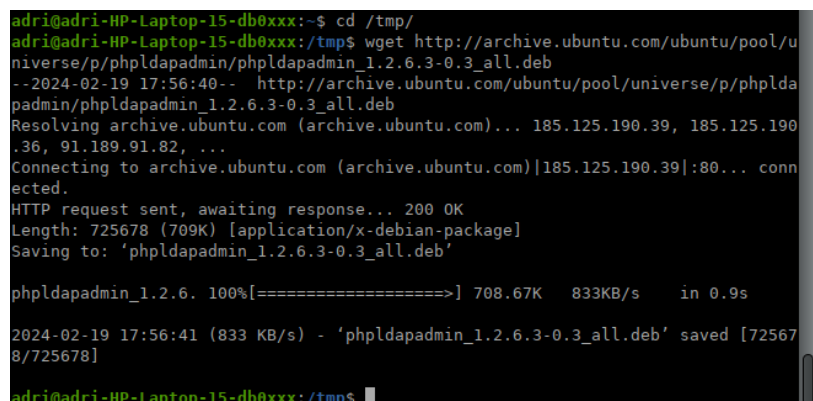


sudo service apache2 restart

Al intentar acceder a “<http://192.168.1.49/phpldapadmin>” me salta este error. Hay que actualizar la versión



```
cd /tmp/  
wget http://archive.ubuntu.com/ubuntu/pool/universe/p/phpldapadmin/phpldapadmin_1.2.6.3-0.3_all.deb  
dpkg -i phpldapadmin_1.2.6.3-0.3_all.deb  
sudo dpkg -i phpldapadmin_1.2.6.3-0.3_all.deb  
sudo apt-get -f install
```

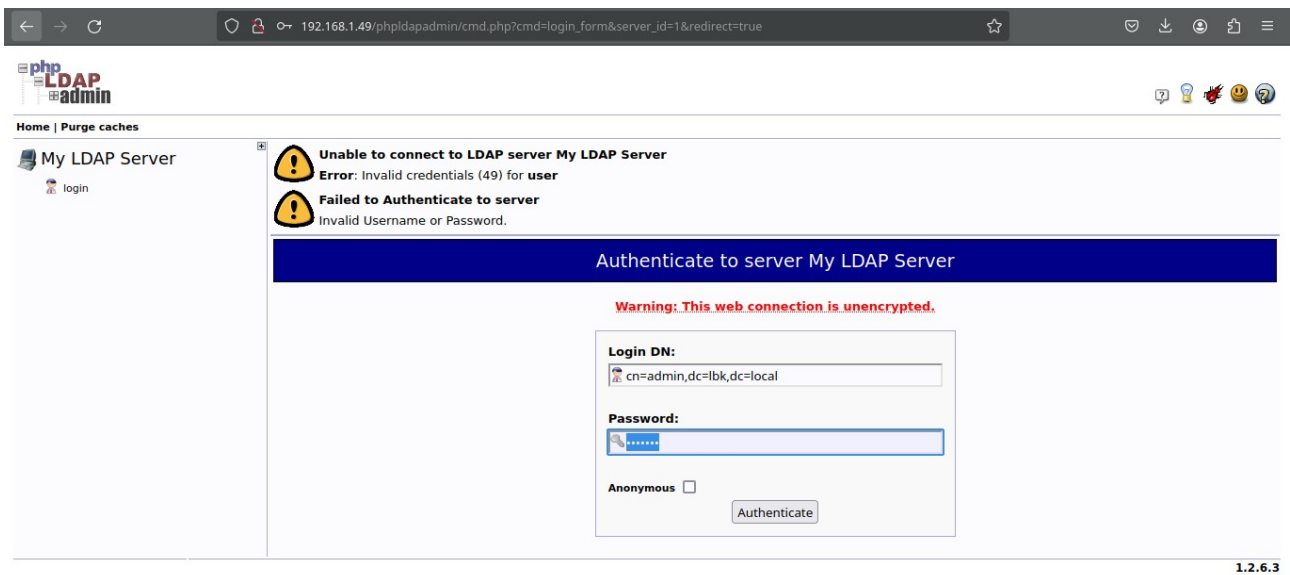


```

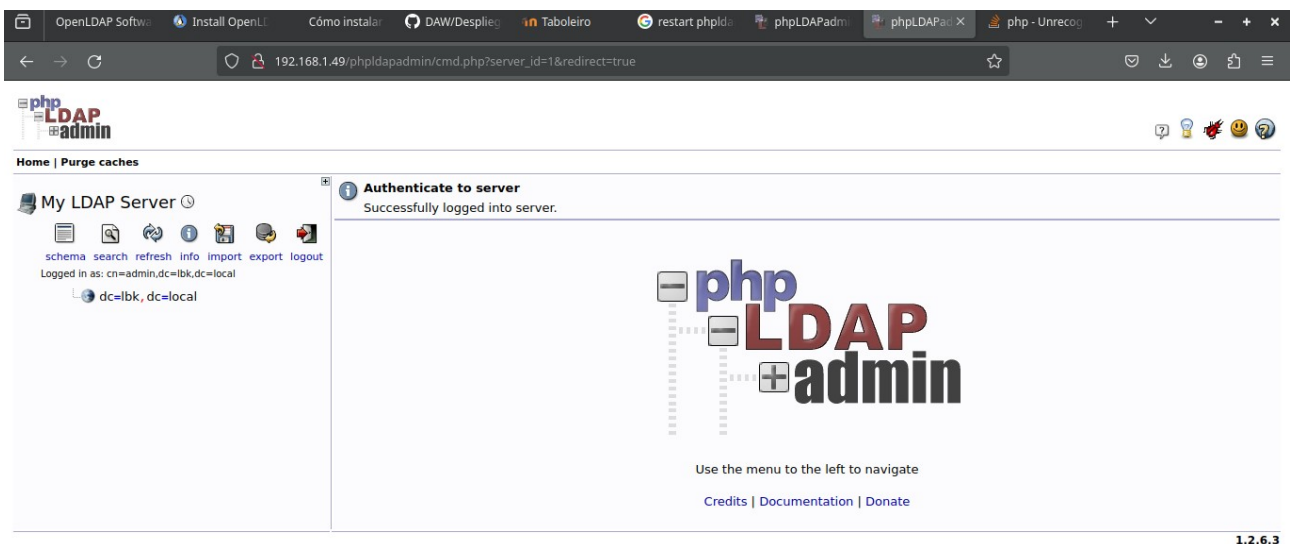
adri@adri-HP-Laptop-15-db0xxx:/tmp$ sudo dpkg -i phpldapadmin_1.2.6.3-0.3_all.de
b
(Reading database ... 227472 files and directories currently installed.)
Preparing to unpack phpldapadmin_1.2.6.3-0.3_all.deb ...
Unpacking phpldapadmin (1.2.6.3-0.3) over (1.2.6.3-0.2) ...
Setting up phpldapadmin (1.2.6.3-0.3) ...
adri@adri-HP-Laptop-15-db0xxx:/tmp$ sudo apt-get -f install
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 26 not upgraded.
adri@adri-HP-Laptop-15-db0xxx:/tmp$

```

Ahora ya funciona. Procedo a iniciar sesión



A la izquierda se ve el nombre del servidor



Apartado 4. Objetos de OpenLDAP

Generar unidades organizativas, grupos y usuarios, así como recursos en el propio sistema para comprobar su funcionamiento.

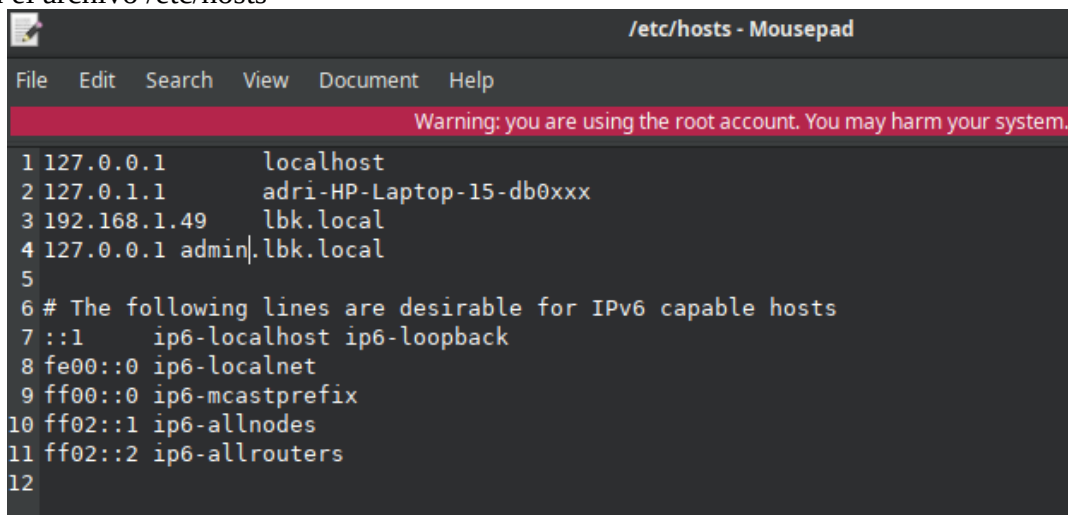
Hay que generar al menos dos unidades organizativas distintas (Departamento IT y FCT), cada una de ellas con varios usuarios.

Pistas. PDF adjuntado.

[Configure LDAP Client on Ubuntu 22.04|20.04|18.04|16.04 | ComputingForGeeks](#)

[Cómo instalar y configurar OpenLDAP y phpLDAPAdmin en Ubuntu 20.04 - HowtoForge](#)

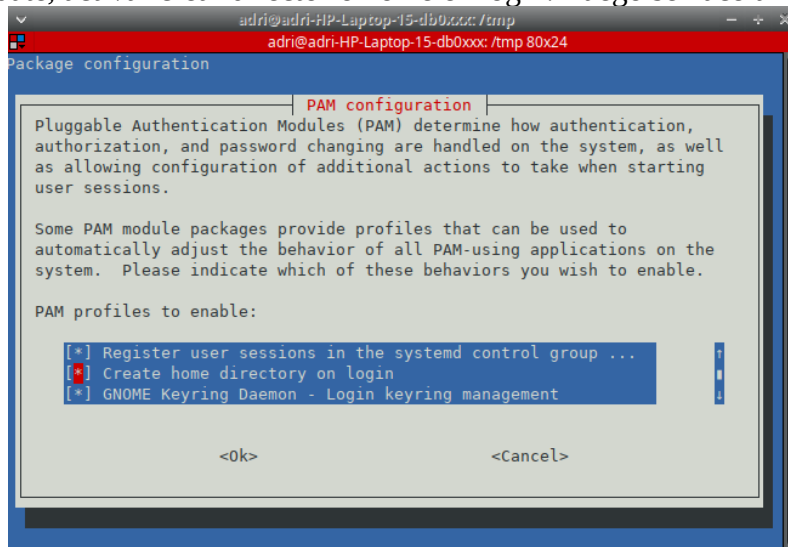
Se edita el archivo /etc/hosts



```
Warning: you are using the root account. You may harm your system.

1 127.0.0.1    localhost
2 127.0.1.1    adri-HP-Laptop-15-db0xxx
3 192.168.1.49 lbk.local
4 127.0.0.1 admin.lbk.local
5
6 # The following lines are desirable for IPv6 capable hosts
7 ::1          ip6-localhost ip6-loopback
8 fe00::0      ip6-localnet
9 ff00::0      ip6-mcastprefix
10 ff02::1      ip6-allnodes
11 ff02::2      ip6-allrouters
12
```

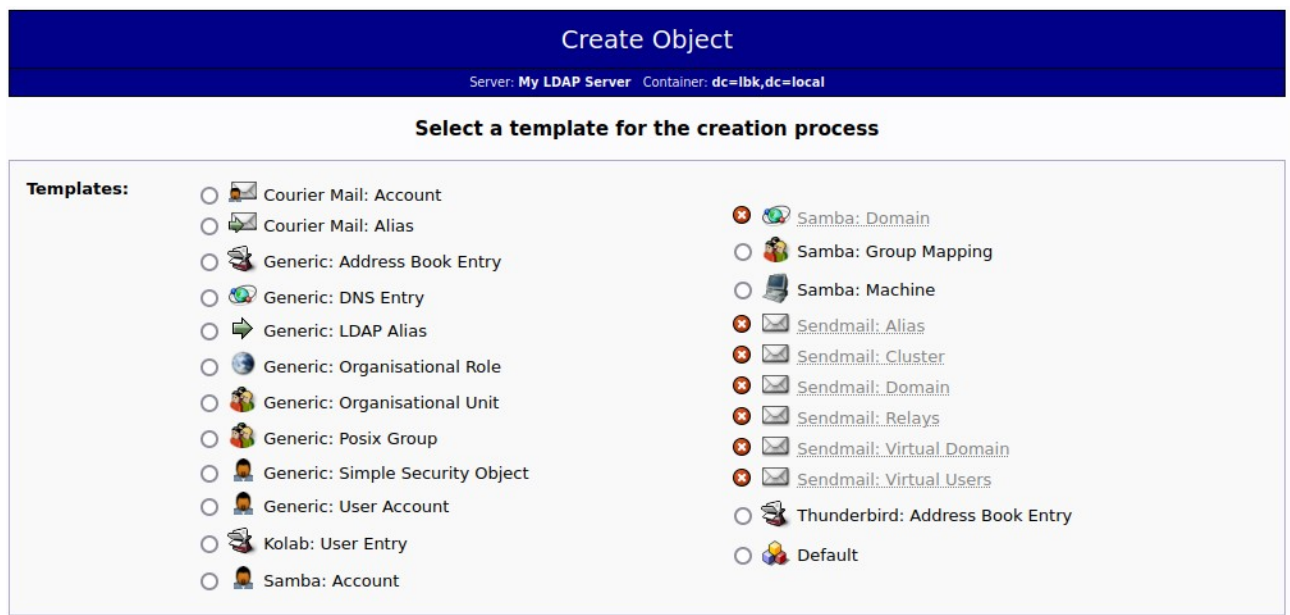
sudo pam-auth-update, activar crear directorio home en login. Luego se hace un reboot



Para crear una unidad organizativa, hay que autenticarse como administrador, darle al dominio y presionar en “Create a child entry”.

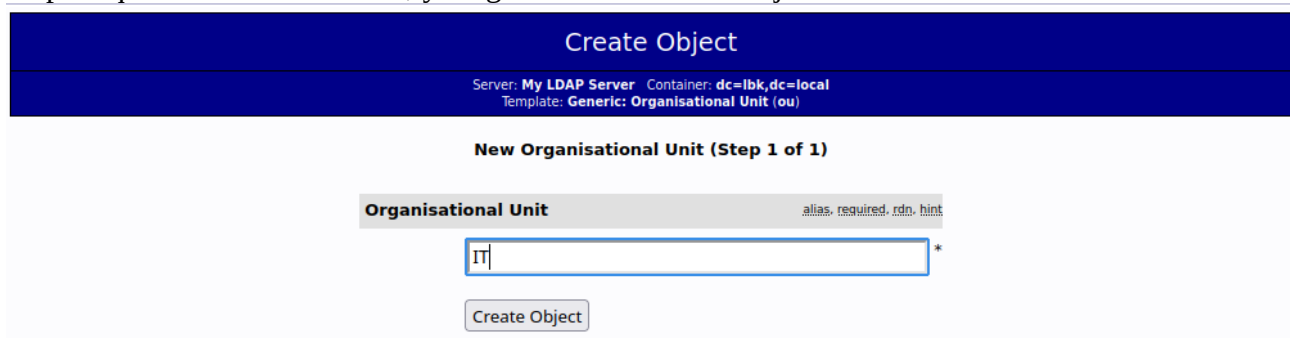


Aquí saldrán un montón de opciones de la cual seleccionamos “Generic: Organisational Unit”



1.2.6.3

Te pide que insertes un nombre, y luego le das a “Create Object”



Te pregunta si quieres crear la entrada, a lo cual presionas “Commit”. Repetí el mismo proceso para “FCT”

Attribute	New Value	Skip
ou=IT,dc=lbk,dc=local		
Organisational Unit	IT	<input type="checkbox"/>
objectClass	organizationalUnit	<input type="checkbox"/>

Commit Cancel

1.2.6.3

Para crear grupos vamos dentro de una ou, presionamos en “Create a child entry”, y luego en “Generic: Posix Group”

Select a template for the creation process

Templates:

- ☐ Courier Mail: Account
- ☐ Courier Mail: Alias
- ☐ Generic: Address Book Entry
- ☐ Generic: DNS Entry
- ☐ Generic: LDAP Alias
- ☐ Generic: Organisational Role
- ☐ Generic: Organisational Unit
- ☐ Generic: Posix Group
- ☐ Generic: Simple Security Object
- ☐ Generic: User Account
- ☐ Kolab: User Entry
- ☐ Samba: Account
- ☒ Samba: Domain
- ☐ Samba: Group Mapping
- ☐ Samba: Machine
- ☒ Sendmail: Alias
- ☒ Sendmail: Cluster
- ☒ Sendmail: Domain
- ☒ Sendmail: Relays
- ☒ Sendmail: Virtual Domain
- ☒ Sendmail: Virtual Users
- ☐ Thunderbird: Address Book Entry
- ☐ Default

1.2.6.3

Te pedirá que insertes un nombre del grupo y te generará un GID. Clic en el botón “Create Object” y te lo crea

New Posix Group (Step 1 of 1)

Group alias, required, rdn

DAW *

GID Number alias, required, hint, rd

500

Users alias, hint

Create Object

1.2.6.3

A continuación salta una previsualización de los cambios añadidos. Para aceptarlos se presiona el botón “Commit”.

Create LDAP Entry

Server: My LDAP Server Container: ou=FCT,dc=lbk,dc=local

Do you want to create this entry?

Attribute	New Value	Skip
cn=DAW,ou=FCT,dc=lbk,dc=local		
Group	DAW	<input type="checkbox"/>
GID Number	500	<input type="checkbox"/>
objectClass	posixGroup	<input type="checkbox"/>

Commit

Cancel

Y para crear usuarios precionas en el grupo que quieras que tenga usuarios (en mi caso voy a crar usuarios dentro del grupo “DAW”), haces click en el, “Create a child entry”, “Generic: User Account”

phpLDAPadmin

Home | Purge caches

My LDAP Server

schema search refresh info import export logout

Logged in as: cn=admin,dc=lbk,dc=local

dc=lbk, dc=local (2)

ou=FCT (1+)

cn=DAW

ou=IT

Create new entry here

Create Object

Server: My LDAP Server Container: cn=DAW,ou=FCT,dc=lbk,dc=local

Select a template for the creation process

Templates:

☐ Courier Mail: Account

☐ Courier Mail: Alias

☐ Generic: Address Book Entry

☐ Generic: DNS Entry

☐ Generic: LDAP Alias

☐ Generic: Organisational Role

☐ Generic: Organisational Unit

☐ Generic: Posix Group

☐ Generic: Simple Security Object

☐ Generic: User Account

☐ Kolab: User Entry

☐ Samba: Account

☒ Samba: Domain

☐ Samba: Group Mapping

☐ Samba: Machine

☒ Sendmail: Alias

☒ Sendmail: Cluster

☒ Sendmail: Domain

☒ Sendmail: Relays

☒ Sendmail: Virtual Domain

☒ Sendmail: Virtual Users

☐ Thunderbird: Address Book Entry

☐ Default

1.2.6.3

Te saldrá todo este menú, pero la mayoría se autocompleta si presionas Tabulador después del First y Last Name; después tienes que cubrir la contraseña, el tipo de cifrado de la misma, el GID al que va a pertenecer y su shell. Yo además le cambié la ruta del “Home Directory” por preferencia personal.

Al acabar, presionas “Create object”

Create Object

Server: My LDAP Server Container: cn=DAW,ou=FCT,dc=lbk,dc=local
Template: Generic: User Account (posixAccount)

New User Account (Step 1 of 1)

First name alias
Pablo

Last name alias, required
Fuentes *

Common Name alias, required, rdn
Pablo Fuentes *

User ID alias, required
pfuentes *

Password alias, hint
md5 (confirm)
Check password...

UID Number alias, required, hint, ro
1000

GID Number alias, required, hint
DAW *

Home directory alias, required
/home/pfuentes *

Login shell alias
Bash

Create Object

Te saldrán los cambios a aplicar. Presionas en “Commit” y te saldrá creado a la derecha. Repites el proceso para el resto de grupos y usuarios

Create LDAP Entry

Server: My LDAP Server Container: cn=DAW,ou=FCT,dc=lbk,dc=local

Do you want to create this entry?

Attribute	New Value	Stop
cn=Pablo Fuentes,cn=DAW,ou=FCT,dc=lbk,dc=local		<input type="checkbox"/>
First name	Pablo	<input type="checkbox"/>
Last name	Fuentes	<input type="checkbox"/>
Common Name	Pablo Fuentes	<input type="checkbox"/>
User ID	pfuentes	<input type="checkbox"/>
Password	*****	<input type="checkbox"/>
UID Number	1000	<input type="checkbox"/>
GID Number	500	<input type="checkbox"/>
Home directory	/home/pfuentes	<input type="checkbox"/>
Login shell	/bin/bash	<input type="checkbox"/>
objectClass	inetOrgPerson, posixAccount	<input type="checkbox"/>

Commit Cancel



Apartado 5. Integración con Apache/FTP/aplicaciones (Opcional para un punto más de la nota)

Configura alguna de estas alternativas:

- Apache Web Server
- un servidor FTP
- cualquier otro servicio
- o una aplicación desarrollada por ti

Para que se autentique contra el servidor LDAP que has instalado.

Pistas.

[Secure Apache Web Pages with LDAP Authentication | ComputingForGeeks](#)

[Servidor proFTPD con LDAP](#)

[Autenticando usuarios con LDAP programáticamente - MediaWiki \(cifprodolfoucha.es\)](#)
[LDAP Authentication Using Pure Java | Baeldung](#)

Yo he incorporado Apache con LDAP

Para eso, hay que instalar el módulo con `sudo a2enmod ldap authnz_ldap` y reiniciar el servicio

```
adri@adri-HP-Laptop-15-db0xxx:~$ sudo a2enmod ldap authnz_ldap
Module ldap already enabled
Considering dependency ldap for authnz_ldap:
Module ldap already enabled
Module authnz_ldap already enabled
adri@adri-HP-Laptop-15-db0xxx:~$ sudo service apache2 restart
adri@adri-HP-Laptop-15-db0xxx:~$
```

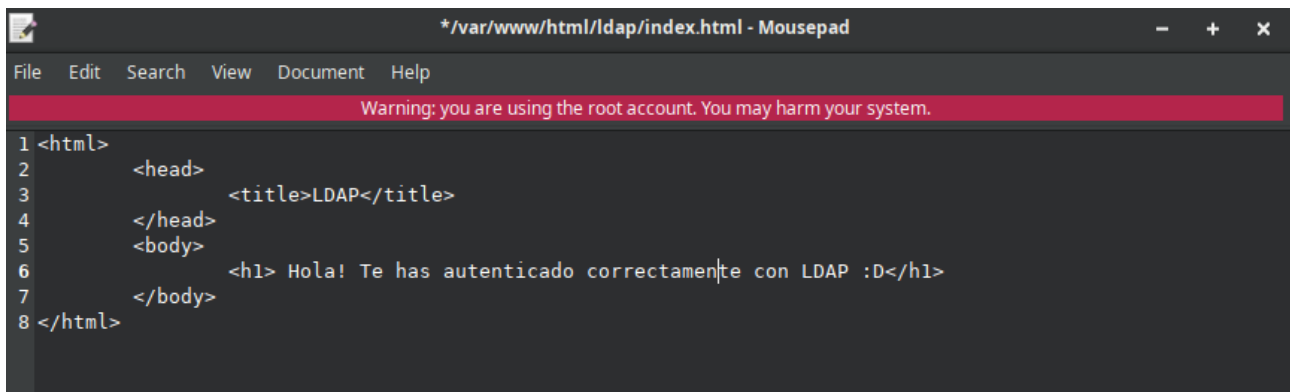
Después, hay que crear el archivo de configuración `/etc/apache2/sites-available/ldap.conf` con este contenido

```
<Directory /var/www/html/ldap>
    AuthName "LDAP Authentication"
    AuthType Basic
    AuthBasicProvider ldap
    AuthLDAPURL ldap://192.168.1.49/dc=lbk,dc=local?uid?sub?(objectClass=*)
    Require ldap-filter objectClass=posixAccount
</Directory>
```

La IP es la del servidor LDAP, y los dc son los nombres de tu servidor.

Después hay que crear la carpeta con `mkdir` y crear el archivo `index.html` dentro de este con este contenido

```
adri@adri-HP-Laptop-15-db0xxx:~$ sudo mousepad /etc/apache2/sites-available/ldap.conf
adri@adri-HP-Laptop-15-db0xxx:~$ sudo mkdir /var/www/html/ldap
adri@adri-HP-Laptop-15-db0xxx:~$ sudo mousepad /var/www/html/ldap/index.html
```



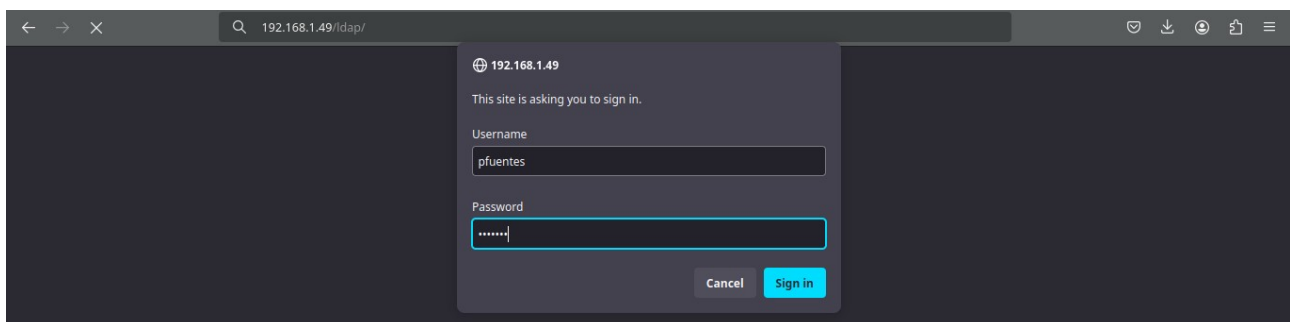
The screenshot shows a window titled `*/var/www/html/ldap/index.html - Mousepad`. A red warning bar at the top states: "Warning: you are using the root account. You may harm your system." The editor contains the following HTML code:

```
1 <html>
2   <head>
3     <title>LDAP</title>
4   </head>
5   <body>
6     <h1> Hola! Te has autenticado correctamente con LDAP :D</h1>
7   </body>
8 </html>
```

Le aplicamos permisos con el comando `sudo chown -R www-data:www-data /var/www/html/ldap` y reiniciamos el servicio.

```
adri@adri-HP-Laptop-15-db0xxx:~$ sudo chown -R www-data:www-data /var/www/html/ldap
adri@adri-HP-Laptop-15-db0xxx:~$ sudo systemctl restart apache
apache2.service                                apache-htcacheclean.service
adri@adri-HP-Laptop-15-db0xxx:~$ sudo systemctl restart apache2.service
```

Y al hacer <http://192.168.1.49/ldap/> te pide iniciar sesión con una cuenta de LDAP



Esto es lo que sale al iniciar sesión

