

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 8

Apartado 5. Integración con Apache/FTP/aplicaciones (Opcional para un punto más de la nota) 9

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

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

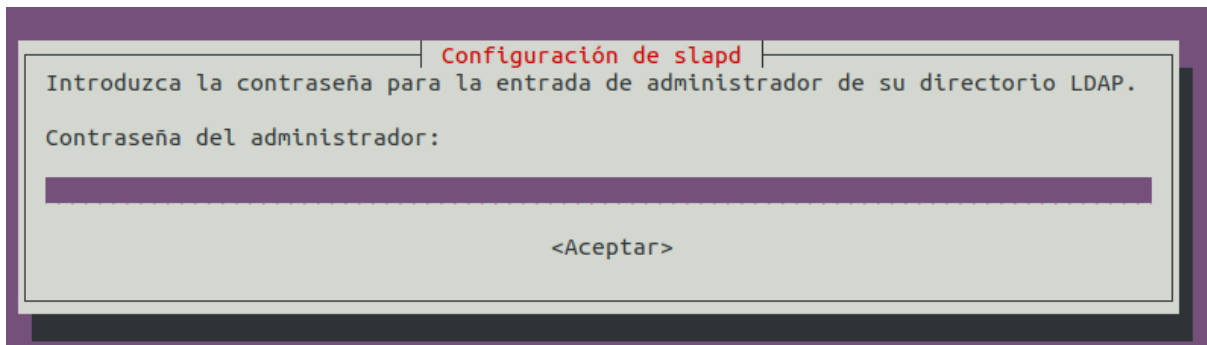
Apartado 3. OpenLDAP.

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.

El primer paso sería instalar LDAP:

```
patricia@patricia-VirtualBox:~$ sudo apt install slapd ldap-utils libpam-ldap libpam-cracklib l  
ibnss-ldap samba smbclient cifs-utils smbldap-tools phpldapadmin
```

Nos saltara esto en la instalación:



Configuración de slapd

Introduzca la contraseña para la entrada de administrador de su directorio LDAP.

Contraseña del administrador:

<Aceptar>

Luego tendremos que mirar nuestra ip:

Cancelar Cableada Aplicar

Detalles Identidad IPv4 IPv6 Seguridad

Velocidad de conexión 1000 Mb/s

Dirección IPv4 10.0.2.15

Dirección IPv6 fe80::4e4:2579:ef4a:e304

Dirección física 08:00:27:3E:23:7A

Ruta predeterminada 10.0.2.2

DNS 172.30.1.4

☒ Conectar automáticamente

☒ Hacer disponible para otros usuarios

☐ Restringir el uso de datos en segundo plano
Adecuado para conexiones que consumen o limitan los datos.

Eliminar perfil de conexión

La ponemos en esta opción:

Configuración de ldap-auth-config

Please enter the URI of the LDAP server to use. This is a string in the form of ldap://<hostname or IP>:<port>/. ldaps:// or ldapi:// can also be used. The port number is optional.

Note: It is usually a good idea to use an IP address because it reduces risks of failure in the event name service problems.

LDAP server Uniform Resource Identifier:

ldapi:///10.0.2.15

<Aceptar>

En la siguiente opción:

Configuración de ldap-auth-config

Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.

Distinguished name of the search base:

`dc=lbk,dc=local`

<Aceptar>

Elegimos la version:

Configuración de ldap-auth-config

Please enter which version of the LDAP protocol should be used by ldapns. It is usually a good idea to set this to the highest available version.

LDAP version to use:

`3`
2

<Aceptar>

Se establece la DB:

Configuración de ldap-auth-config

This option will allow you to make password utilities that use pam to behave like you would be changing local passwords.

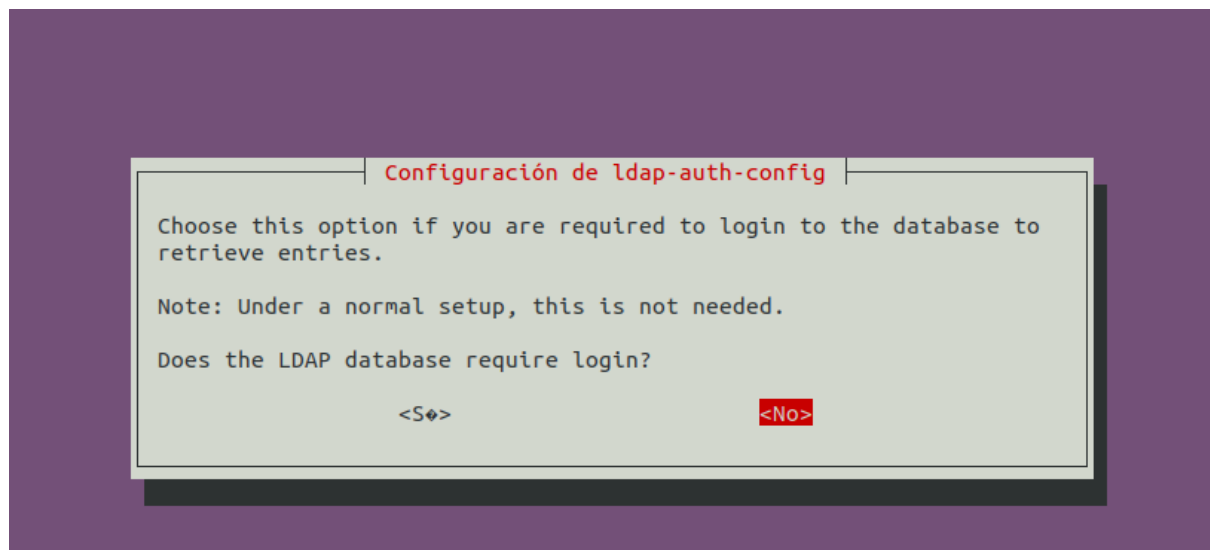
The password will be stored in a separate file which will be made readable to root only.

If you are using NFS mounted /etc or any other custom setup, you should disable this.

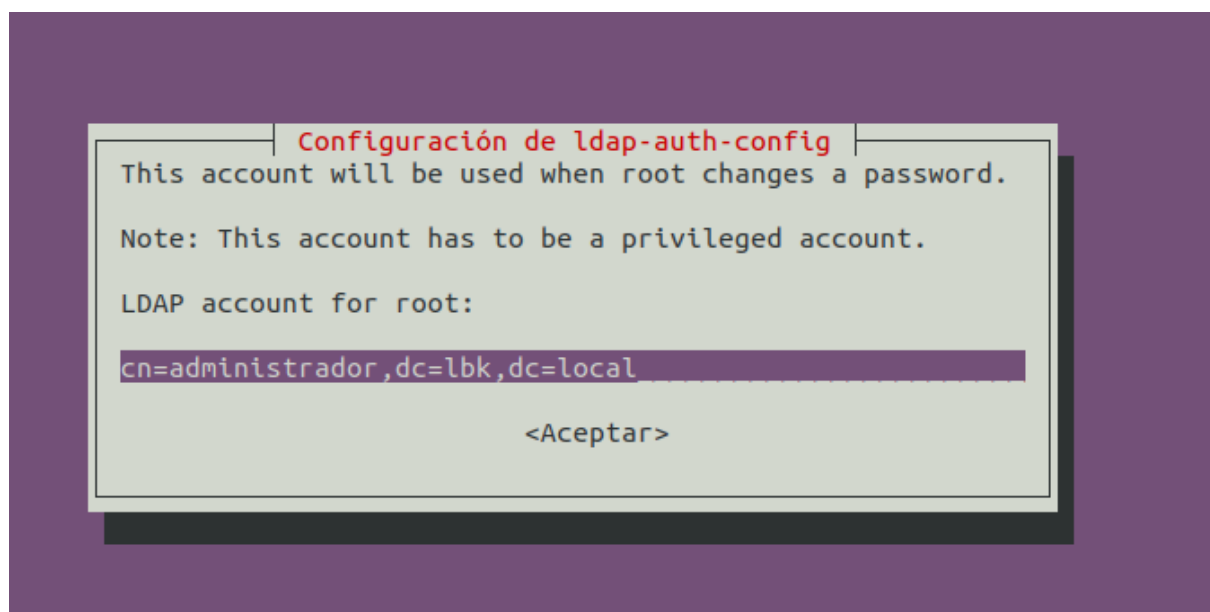
Make local root Database admin:

`<S>` <No>

Creamos la BBDD sin login y local:



Por último configurar administrador y contraseña del root de LDAP.



Luego nos pedirá poner la contraseña.

Después tendríamos que poner este comando:

```
patricia@patricia-VirtualBox:~$ sudo dpkg-reconfigure slapd
```

Entonces configuramos el dominio DNS:

Configuración de slapd

El nombre de dominio DNS se utiliza para construir el DN base del directorio LDAP. Por ejemplo, si introduce «foo.example.org» el directorio se creará con un DN base de «dc=foo, dc=example, dc=org».

Introduzca el nombre de dominio DNS:

lbk.local

<Aceptar>

Y la organización:

Configuración de slapd

Introduzca el nombre de la organización a utilizar en el DN base del directorio LDAP.

Nombre de la organización:

lbk.local

<Aceptar>

Nos pedirá la contraseña:

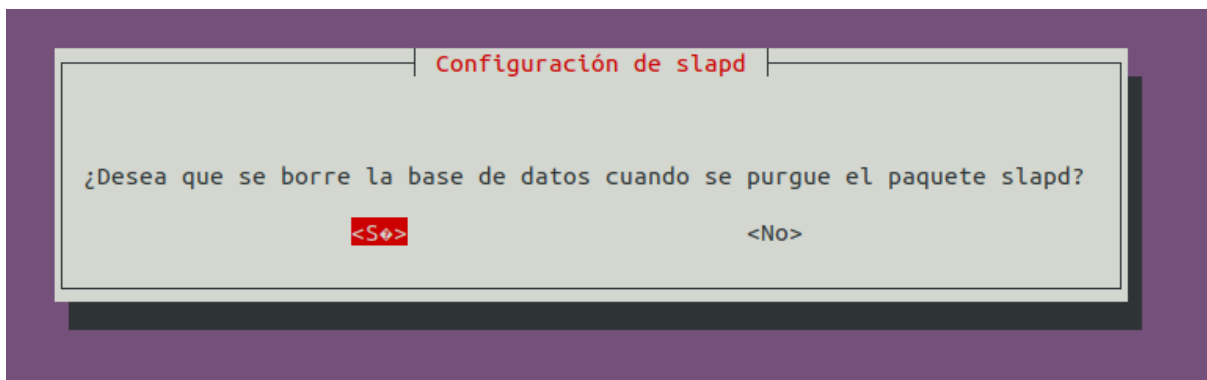
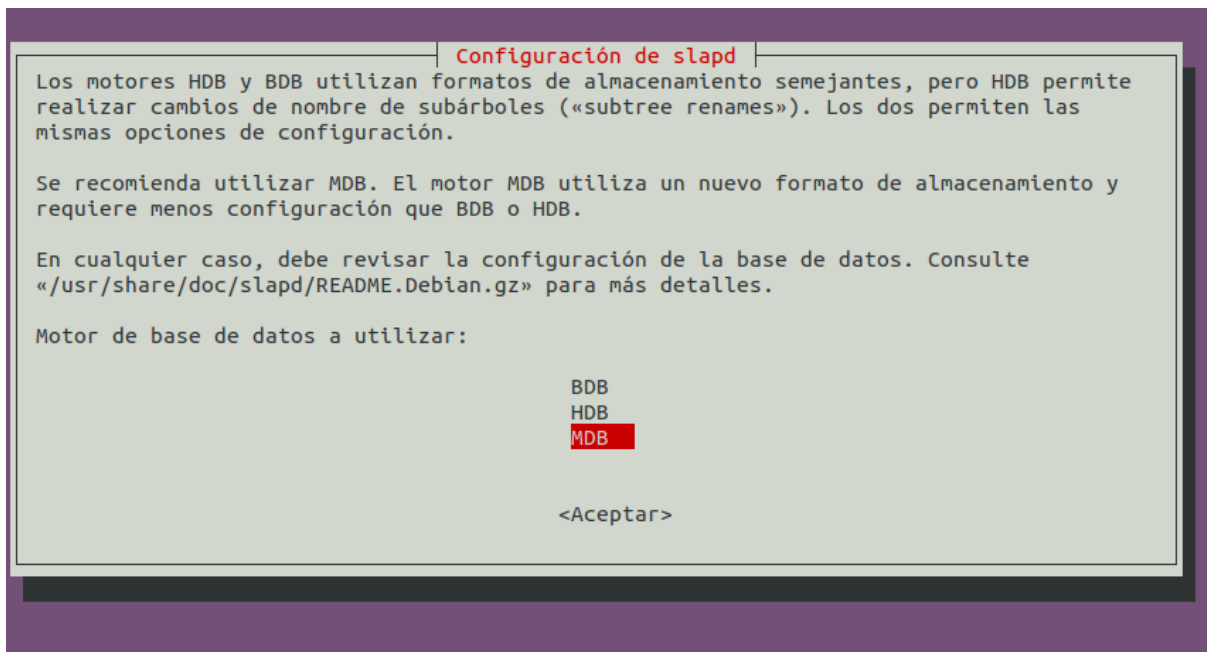
Configuración de slapd

Introduzca la contraseña para la entrada de administrador de su directorio LDAP.

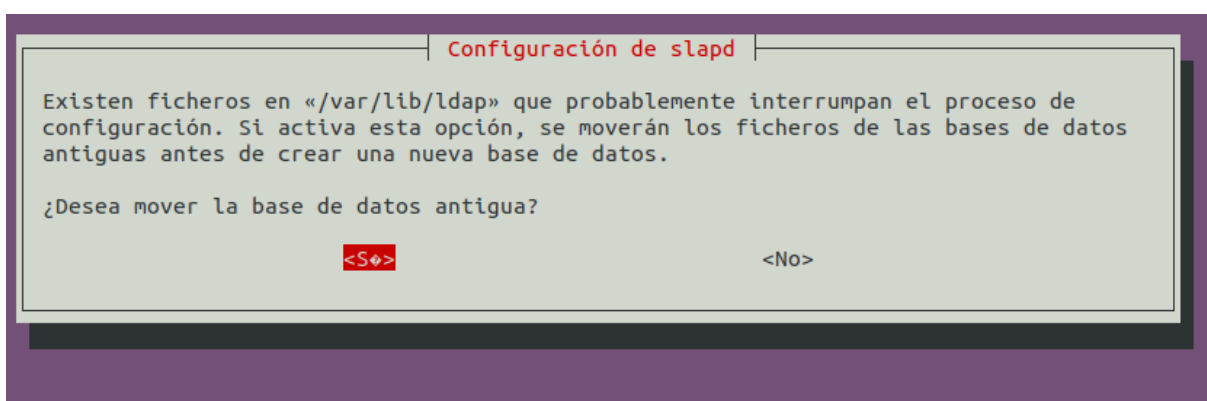
Contraseña del administrador:

<Aceptar>

Yo elegí esta opción:



Había una BBDD incorrecta que se mueve a otro sitio:



Se configura en este archivo:

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
GNU nano 2.9.3 /etc/phpldapadmin/config.php Modificado

# 'displayName',
# 'uid',
# 'uidNumber',
# 'gidNumber',
# 'homeDirectory',
# 'mail',
# 'userPassword'
# );

/*****
 * Define your LDAP servers in this section *
 *****/

$servers = new Datastore();

/* $servers->NewServer('ldap_pla') must be called before each new LDAP server
   declaration. */
$servers->newServer('ldap_pla');

/* A convenient name that will appear in the tree viewer and throughout
   phpLDAPadmin to identify this LDAP server to users. */
$servers->setValue('server','name','My LDAP Server');

/* Examples:
   'ldap.example.com',
   'ldaps://ldap.example.com/',
   'ldapi://%2fusr%2flocal%2fvar%2frun%2fldapi'
   (Unix socket at /usr/local/var/run/ldap) */
$servers->setValue('server','host','127.0.0.1');

/* The port your LDAP server listens on (no quotes). 389 is standard. */
// $servers->setValue('server','port',389);

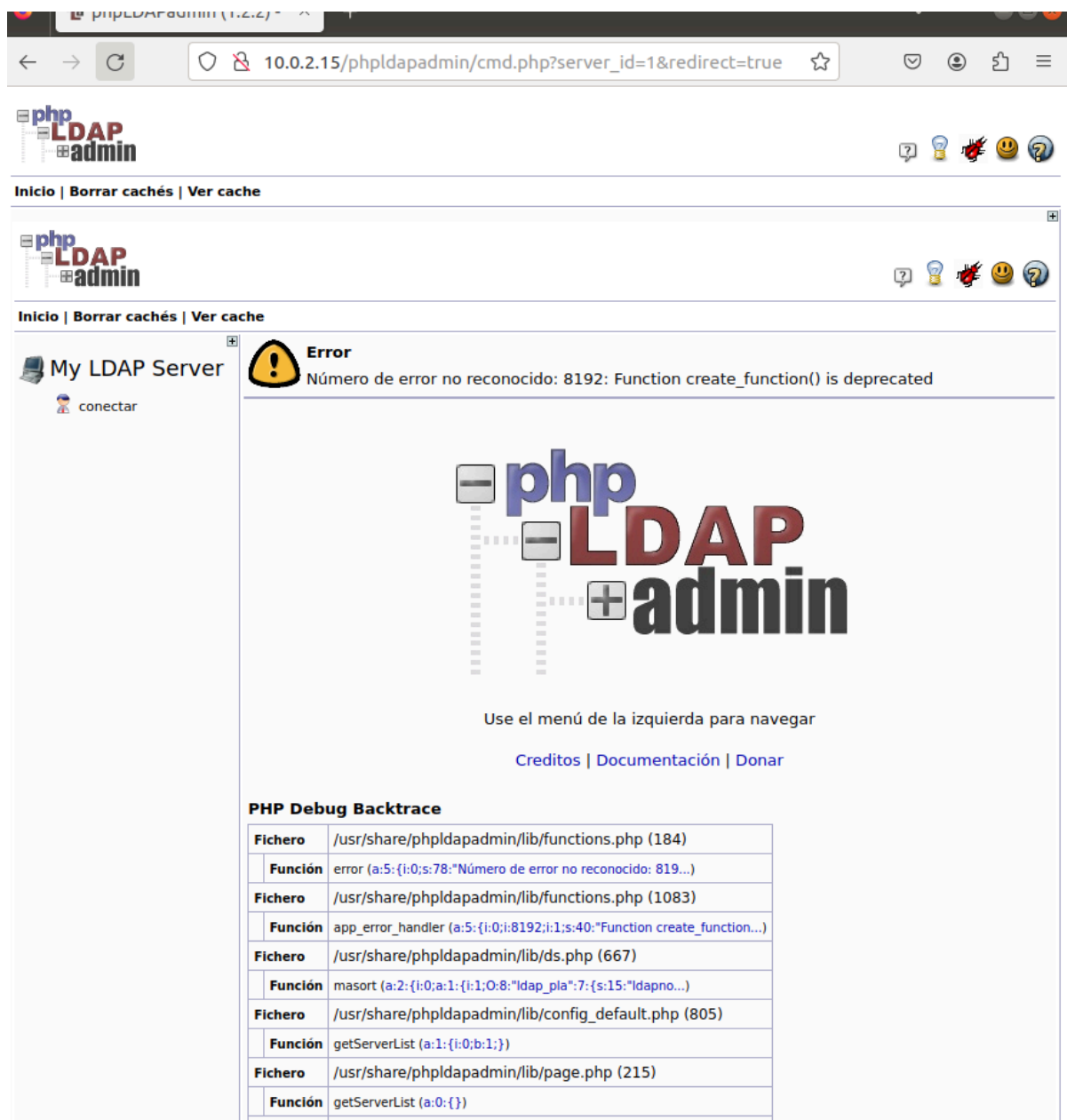
/* Array of base DN's of your LDAP server. Leave this blank to have phpLDAPadmin
   auto-detect it for you. */
$servers->setValue('server','base',array('dc=lbk,dc=local'));

/* Five options for auth_type:
   1. 'cookie': you will login via a web form, and a client-side cookie will
      store your login dn and password.
   2. 'session': same as cookie but your login dn and password are stored on the
      web server in a persistent session variable.
   3. 'http': same as session but your login dn and password are retrieved via
      HTTP authentication.

^G Ver ayuda    ^O Guardar     ^W Buscar      ^K Cortar Texto ^J Justificar   ^C Posición
^X Salir        ^R Leer fich.  ^\ Reemplazar  ^U Pegar txt    ^T Ortografía  ^_ Ir a línea
```

Tenemos que cambiar el array a nuestra BBDD.

Y tendremos nuestra página de admin: Esta en concreto da error por la versión que tenemos de php, que hace que algunas funciones estén deprecated.



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.

Creamos las unidades organizativas:

```
patricia@patricia-VirtualBox:~$ nano ou.ldif
```

Creamos las unidades organizativas:

```
dn: ou=ucha,dc=lbk,dc=local
objectClass: top
objectClass: organizationalUnit
ou: ucha

dn: ou=sanclemente,dc=lbk,dc=local
objectClass: top
objectClass: organizationalUnit
ou: sanclemente
```

La explicación de lo que está escrito:

top porque será un objeto que pende da raíz. Poderíamos por exemplo crear unha OU que fora xuntadegalicia, e que ucha e sanclemente penderan dela.

Luego con ldapadd añadiremos las entradas:

```
patricia@patricia-VirtualBox:~$ ldapadd -x -D cn=admin,dc=lbk,dc=local -W -f ou.ldif
Enter LDAP Password:
adding new entry "ou=ucha,dc=lbk,dc=local"

adding new entry "ou=sanclemente,dc=lbk,dc=local"

patricia@patricia-VirtualBox:~$
```

Ahora con este comando:

```
patricia@patricia-VirtualBox:~$ sudo slapcat
```

Comprobaremos que efectivamente fueron añadidas:

Lo siguiente sería crear las unidades organizativas, los grupos y los usuarios. Empezamos creando un archivo de texto vacío:

```
patricia@patricia-VirtualBox:~$ nano grupos-usuarios.ldif
```

Y después modificamos el archivo:

```
# Crear la Unidad Organizativa para el Departamento IT
dn: ou=IT,dc=lbk,dc=local
objectClass: organizationalUnit
ou: IT

# Crear la Unidad Organizativa para el Departamento FCT
dn: ou=FCT,dc=lbk,dc=local
objectClass: organizationalUnit
ou: FCT

# Crear el grupo para el Departamento IT
dn: cn=IT_Group,ou=IT,dc=lbk,dc=local
objectClass: groupOfNames
cn: IT_Group
member: uid=user1,ou=IT,dc=lbk,dc=local
member: uid=user2,ou=IT,dc=lbk,dc=local

# Crear usuarios para el Departamento IT
dn: uid=user1,ou=IT,dc=lbk,dc=local
objectClass: inetOrgPerson
cn: User One
sn: One
uid: user1
userPassword: {SSHA}EfQP4+ilUWm5JuHleA9mdWTpVm0GRBPx

dn: uid=user2,ou=IT,dc=lbk,dc=local
objectClass: inetOrgPerson
cn: User Two
sn: Two
uid: user2
userPassword: {SSHA}EfQP4+ilUWm5JuHleA9mdWTpVm0GRBPx

# Crear el grupo para el Departamento FCT
dn: cn=FCT_Group,ou=FCT,dc=lbk,dc=local
objectClass: groupOfNames
cn: FCT_Group
member: uid=user3,ou=FCT,dc=lbk,dc=local
member: uid=user4,ou=FCT,dc=lbk,dc=local

# Crear usuarios para el Departamento FCT
dn: uid=user3,ou=FCT,dc=lbk,dc=local
objectClass: inetOrgPerson
cn: User Three
sn: Three
```

```
dn: uid=user4,ou=FCT,dc=lbk,dc=local
objectClass: inetOrgPerson
cn: User Four
sn: Four
uid: user4
userPassword: {SSHA}EfQP4+ilUWm5JuHleA9mdWTpVm0GRBPx
```

Lo siguiente es añadirlos con el siguiente comando:

```
patricia@patricia-VirtualBox:~$ ldapadd -x -D "cn=admin,dc=lbk,dc=local" -W -f grupos-usuarios.ldif
Enter LDAP Password:
adding new entry "ou=IT,dc=lbk,dc=local"

adding new entry "ou=FCT,dc=lbk,dc=local"

adding new entry "cn=IT_Group,ou=IT,dc=lbk,dc=local"

adding new entry "uid=user1,ou=IT,dc=lbk,dc=local"

adding new entry "uid=user2,ou=IT,dc=lbk,dc=local"

adding new entry "cn=FCT_Group,ou=FCT,dc=lbk,dc=local"

adding new entry "uid=user3,ou=FCT,dc=lbk,dc=local"

adding new entry "uid=user4,ou=FCT,dc=lbk,dc=local"

patricia@patricia-VirtualBox:~$
```

Y con un slapcat como antes comprobamos que estén correctamente (aquí solo hay algunas de las añadidas):


```

objectClass: organizationalUnit
ou: IT
structuralObjectClass: organizationalUnit
entryUUID: 68f80758-6c53-103e-8c9f-e908c067e572
creatorsName: cn=admin,dc=lbk,dc=local
createTimestamp: 20240301200953Z
entryCSN: 20240301200953.023121Z#000000#000#000000
modifiersName: cn=admin,dc=lbk,dc=local
modifyTimestamp: 20240301200953Z

dn: ou=FCT,dc=lbk,dc=local
objectClass: organizationalUnit
ou: FCT
structuralObjectClass: organizationalUnit
entryUUID: 68f89916-6c53-103e-8ca0-e908c067e572
creatorsName: cn=admin,dc=lbk,dc=local
createTimestamp: 20240301200953Z
entryCSN: 20240301200953.026858Z#000000#000#000000
modifiersName: cn=admin,dc=lbk,dc=local
modifyTimestamp: 20240301200953Z

dn: cn=IT_Group,ou=IT,dc=lbk,dc=local
objectClass: groupOfNames
cn: IT_Group
member: uid=user1,ou=IT,dc=lbk,dc=local
member: uid=user2,ou=IT,dc=lbk,dc=local
structuralObjectClass: groupOfNames
entryUUID: 68f91382-6c53-103e-8ca1-e908c067e572
creatorsName: cn=admin,dc=lbk,dc=local
createTimestamp: 20240301200953Z
entryCSN: 20240301200953.029992Z#000000#000#000000
modifiersName: cn=admin,dc=lbk,dc=local
modifyTimestamp: 20240301200953Z

dn: uid=user1,ou=IT,dc=lbk,dc=local
objectClass: inetOrgPerson
cn: User One
sn: One
uid: user1
userPassword:: e1NTSEF9RWZxUDQraWx1V201SnVIbGVBOw1kV1RwVm0wR1JCUGg=
structuralObjectClass: inetOrgPerson
entryUUID: 68f9b72e-6c53-103e-8ca2-e908c067e572
creatorsName: cn=admin,dc=lbk,dc=local
createTimestamp: 20240301200953Z
entryCSN: 20240301200953.034182Z#000000#000#000000
modifiersName: cn=admin,dc=lbk,dc=local
modifyTimestamp: 20240301200953Z

```

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.

Primero instalamos apache:

```
sudo apt-get update
sudo apt-get install apache2 libapache2-mod-ldap-userdir libapache2-mod-authnz-ldap
```

Después configuramos con un sudo nano el archivo de apache con nuestras credenciales de LDAP:

```
GNU nano 2.9.3 /etc/apache2/sites-available/000-default.conf
<VirtualHost *:80>
  ServerAdmin webmaster@localhost
  DocumentRoot /var/www/html

  <Directory /var/www/html>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted

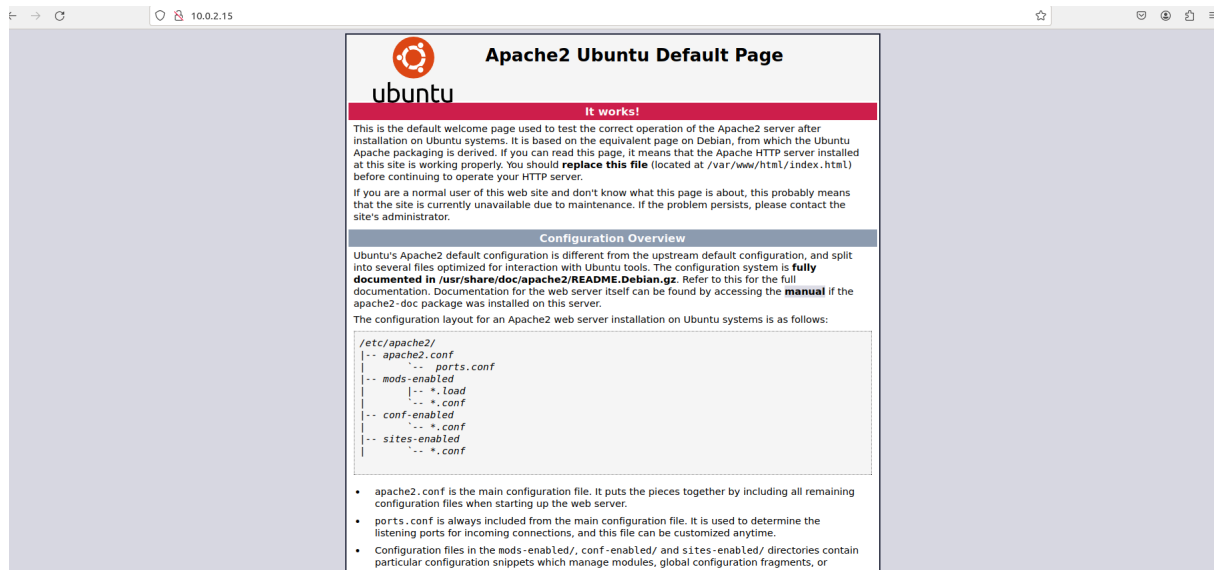
    AuthType Basic
    AuthName "LDAP Authentication"
    AuthBasicProvider ldap
    AuthLDAPURL "ldap://10.0.2.15/dc=lbk,dc=local?uid"
    AuthLDAPBindDN "cn=admin,dc=lbk,dc=local"
    AuthLDAPBindPassword "admin"
    Require valid-user
  </Directory>

  ErrorLog ${APACHE_LOG_DIR}/error.log
  CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Después lo habilitamos y reiniciamos el servicio:

```
patricia@patricia-VirtualBox:~$ sudo nano /etc/apache2/sites-available/000-default.conf
patricia@patricia-VirtualBox:~$ sudo a2enmod authnz_ldap
Considering dependency ldap for authnz_ldap:
Enabling module ldap.
Enabling module authnz_ldap.
To activate the new configuration, you need to run:
  systemctl restart apache2
patricia@patricia-VirtualBox:~$ sudo a2enmod ldap
Module ldap already enabled
patricia@patricia-VirtualBox:~$ sudo systemctl restart apache2
patricia@patricia-VirtualBox:~$
```

Finalmente al entrar en apache nos debería de pedir las credenciales:



En mi caso no lo hizo a pesar de seguir todos los pasos correctamente.