

UBUNTU: SERVICIO DE DIRECTORIO LDAP



Juan Carlos Navidad García
Sistemas Operativos en Red

SERVICIO DE DIRECTORIO**1. Explica que es LDAP**

LDAP son las siglas de Lightweight Directory Access Protocol, un protocolo a nivel de aplicación que permite realizar consultas sobre un servicio de directorio para poder buscar información.

2. ¿Qué es un servicio de directorio y en qué modelo se basa?

Un servicio de directorio es una aplicación o un conjunto de aplicaciones, parecida a una base de datos, que almacena y organiza la información sobre los usuarios y recursos de una red de ordenadores.

Se basa en el modelo cliente-servidor.

3. Ejemplos de uso del servicio de directorio

Se puede usar como servidor de autenticación o como repositorio.

4. Ventajas e inconvenientes del servidor LDAP

Ventajas:

- Es muy rápido en lecturas y escrituras.
- Permite replicar el servidor de forma muy sencilla y económica.
- Dispone de un modelo de nombres globales que asegura que todas las entradas son únicas.
- Permite múltiples directorios independientes.
- Se pueden establecer medidas de seguridad a través de SSL.
- La mayoría de las aplicaciones disponen de soporte LDAP.

Desventajas:

- Es muy poco intuitivo y difícil de manejar, pero existen múltiples herramientas que facilitan su uso.

5. ¿Cómo se llaman las estructuras de datos que almacenan y organizan la información del directorio?

Entradas.

6. Estructura LDAP

- Clases: en ellas, se definen los objetos y sus características.
- Objetos: los objetos son entradas en el directorio. Los objetos son instancias creadas a partir de una clase o de varias, en función de los atributos necesarios para un objeto.
- Atributos: son los campos asociados a cada objeto creado y definen sus características.

7. ¿Qué es DN? En la estructura de directorio del ejemplo escribe el DD de profesores

Cada entrada del directorio describe un objeto. Cada entrada tiene un nombre llamado Distinguished Name (DN), el cual lo identifica unívocamente.

8. ¿Qué es DIT?

DIT son las entradas de directorio organizadas en forma de árbol que se basan en los DN.

9. ¿Qué es OpenLDAP?

OpenLDAP es una implementación libre y de código abierto del protocolo Lightweight Directory Access Protocol desarrollada por el proyecto OpenLDAP.

INSTALACION Y CONFIGURACION DE EL SERVIDOR OpenLDAP

10. Instala OpenLDAP

Instalamos con el comando **sudo apt-get install slapd ldap-utils**.

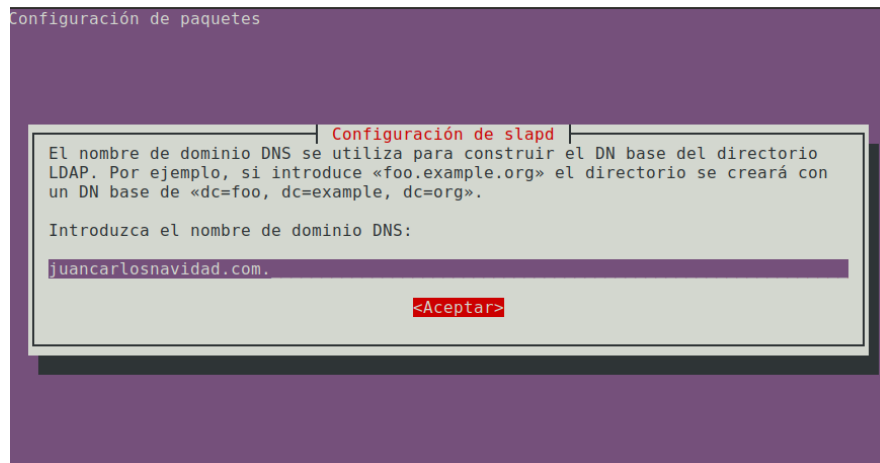
```
jnav@jnav2:~$ sudo apt-get install slapd ldap-utils
[sudo] contraseña para jnav:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
```

11. Archivos de configuración de OpenLDAP

El archivo de configuración de openldap se encuentra en
`/etc/openldap/ldap.conf`

12. Configura el servidor con

- a. El dominio tunombre.com



b. La organización 2SMR

Configuración de paquetes

Configuración de slapd

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

Nombre de la organización:

2SMR

<Aceptar>

c. El motor de la base de datos

Configuración de paquetes

Configuración de slapd

Los motores HDB y BDB utilizan formatos de almacenamiento semejantes, pero HDB permite realizar cambios de nombre de subárboles («subtree renames»). Los dos permiten las mismas opciones de configuración.

Se recomienda utilizar MDB. El motor MDB utiliza un nuevo formato de almacenamiento y requiere menos configuración que BDB o HDB.

En cualquier caso, debe revisar la configuración de la base de datos. Consulte «/usr/share/doc/slapd/README.Debian.gz» para más detalles.

Motor de base de datos a utilizar:

BDB
HDB
MDB

<Aceptar>

13. Comprueba que el servidor se ha instalado y su estado

```
jnav@jnav2:~$ sudo service slapd status
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
   Loaded: loaded (/etc/init.d/slapd; generated)
   Drop-In: /lib/systemd/system/slapd.service.d
            └─slapd-remain-after-exit.conf
   Active: active (running) since Fri 2021-12-10 11:06:08 CET; 29s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 4546 ExecStop=/etc/init.d/slapd stop (code=exited, status=0/SUCCESS)
 Process: 4552 ExecStart=/etc/init.d/slapd start (code=exited, status=0/SUCCESS)
    Tasks: 3 (limit: 4666)
   CGroup: /system.slice/slapd.service
            └─4559 /usr/sbin/slapd -h ldap:/// ldapi:/// -g openldap -u openldap -F /etc

dic 10 11:06:08 jnav2 systemd[1]: Starting LSB: OpenLDAP standalone server (Lightweight
dic 10 11:06:08 jnav2 slapd[4552]: * Starting OpenLDAP slapd
dic 10 11:06:08 jnav2 slapd[4558]: @(#) $OpenLDAP: slapd (Ubuntu) (Feb 18 2021 14:22:4
        Debian OpenLDAP Maintainers <pkg-openldap-de
dic 10 11:06:08 jnav2 slapd[4559]: slapd starting
dic 10 11:06:08 jnav2 slapd[4552]: ...done.
dic 10 11:06:08 jnav2 systemd[1]: Started LSB: OpenLDAP standalone server (Lightweight
lines 1-19/19 (END)
```

14. Indica los comandos para:

a. Arrancar el servidor

Sudo service slapd start

Systemctl stop slapd.service

b. Parar el servidor

Sudo service slapd stop

Systemctl stop slapd.service

c. Reiniciar el servidor

Sudo service slapd stop

Systemctl stop slapd.service

CREACION DE LA ESTRUCTURA DE DIRECTORIO

**1. ¿Como se puede crear la estructura jerárquica de directorio?
(información del directorio)**

La estructura deberá ser realizada en un archivo LDIF (LDAP Data Interchange Format), que es un archivo de texto plano con un formato y sintaxis especial.

2. ¿Qué formato tiene la estructura de directorio?

comentario

dn: <Nombre global único>

<atributo>: <valor>

<atributo>: <valor>

...

```
dn: dc=jcngsor,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
```

3. ¿Cuál es el comando para comprobar la configuración del directorio?

Slapcat es el comando que permite comprobar la configuración del directorio.

4. ¿Dónde se guarda la configuración del servidor LDAP?

La configuración del servidor LDAP se guarda en el fichero /etc/ldap/ldap.conf.

5. ¿Antes de crear las cuentas de usuarios y grupos que necesitaríamos crear?

Se debe crear el directorio raíz y el usuario administrador.

6. Comandos para:

a. Búsqueda de objetos

El comando es `ldapsearch`

b. Borrar objetos

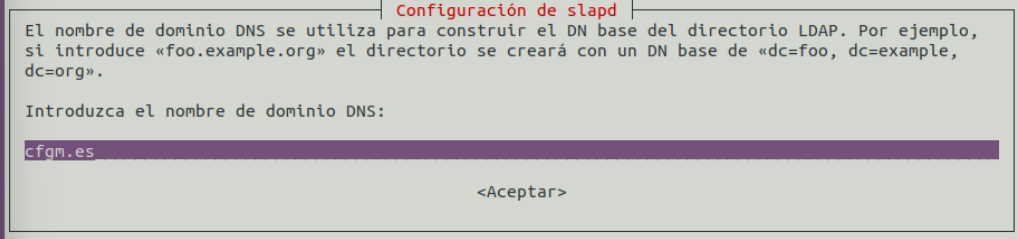
El comando para borrar objetos es `ldapdelete`

c. Modificar objetos

El comando para modificar objetos es `ldapmodify`, este tiene tres atributos: `add`, `replace` y `delete`.

7. Ejercicio 5.8

a)



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:

cfgm.es

<Aceptar>

b)

Grupos:

```
dn: ou=grupos,dc=cfgm,dc=es
changetype: add
objectClass: organizationalUnit
objectClass: top
ou: grupos
```

```
jnav@jnav-vb:~$ nano grupos.ldif
jnav@jnav-vb:~$ ldapadd -W -D "cn=admin,dc=cfgm,dc=es" -f grupos.ldif
Enter LDAP Password:
adding new entry "ou=grupos,dc=cfgm,dc=es"

jnav@jnav-vb:~$
```

Usuarios:

```
dn: ou=usuarios,dc=cfgm,dc=es
changetype: add
objectClass: organizationalUnit
objectClass: top
ou: usuarios
```

```
jnav@jnav-vb:~$ nano usuarios.ldif
jnav@jnav-vb:~$ ldapadd -W -D "cn=admin,dc=cfgm,dc=es" -f usuarios.ldif
Enter LDAP Password:
adding new entry "ou=usuarios,dc=cfgm,dc=es"

jnav@jnav-vb:~$
```

PCs del aula:

```
dn: ou=aulapcs,dc=cfgm,dc=es
changetype: add
objectClass: organizationalUnit
objectClass: top
ou: aulapcs
```

```
jnav@jnav-vb:~$ nano aulapc.ldif
jnav@jnav-vb:~$ ldapadd -W -D "cn=admin,dc=cfgm,dc=es" -f aulapc.ldif
Enter LDAP Password:
adding new entry "ou=aulapcs,dc=cfgm,dc=es"

jnav@jnav-vb:~$
```

c)**1º Alumno:**

```
dn: uid=navidad,ou=usuarios,dc=cfgm,dc=es
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: navidad
sn: navidad
givenName: navidad
cn: navidad
uidNumber: 4000
gidNumber: 4000
userPassword: jnav987
loginShell: /bin/bash
homeDirectory: /home/navidad
```

```
jnav@jnav-vb:~$ nano navidad_user.ldif
jnav@jnav-vb:~$ ldapadd -x -W -D "cn=admin,dc=cfgm,dc=es" -f navidad_user.ldif
Enter LDAP Password:
adding new entry "uid=navidad,ou=usuarios,dc=cfgm,dc=es"

jnav@jnav-vb:~$
```

2º Alumno:

```
dn: uid=garcia,ou=usuarios,dc=cfgm,dc=es
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: garcia
sn: garcia
givenName: garcia
cn: garcia
uidNumber: 5000
gidNumber: 5000
userPassword: jnav987
loginShell: /bin/bash
homeDirectory: /home/garcia
```

```
jnav@jnav-vb:~$ nano garcia_user.ldif
jnav@jnav-vb:~$ ldapadd -x -W -D "cn=admin,dc=cfgm,dc=es" -f garcia_user.ldif
Enter LDAP Password:
adding new entry "uid=garcia,ou=usuarios,dc=cfgm,dc=es"

jnav@jnav-vb:~$
```

3º Alumno:

```
dn: uid=juan,ou=usuarios,dc=cfgm,dc=es
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: juan
sn: juan
givenName: juan
cn: juan
uidNumber: 6000
gidNumber: 6000
userPassword: jnav987
loginShell: /bin/bash
homeDirectory: /home/juan
```

```
jnav@jnav-vb:~$ nano juan_user.ldif
jnav@jnav-vb:~$ ldapadd -x -W -D "cn=admin,dc=cfgm,dc=es" -f juan_user.ldif
Enter LDAP Password:
adding new entry "uid=juan,ou=usuarios,dc=cfgm,dc=es"

jnav@jnav-vb:~$
```

4º Alumno:

```
dn: uid=jcng,ou=usuarios,dc=cfgm,dc=es
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: jcng
sn: jcng
givenName: jcng
cn: jcng
uidNumber: 7000
gidNumber: 7000
userPassword: jnav987
loginShell: /bin/bash
homeDirectory: /home/jcng
```

```
jnav@jnav-vb:~$ nano jcng_user.ldif
jnav@jnav-vb:~$ ldapadd -x -W -D "cn=admin,dc=cfgm,dc=es" -f jcng_user.ldif
Enter LDAP Password:
adding new entry "uid=jcng,ou=usuarios,dc=cfgm,dc=es"

jnav@jnav-vb:~$
```

d)**Primer grupo:**

```
dn: cn=smr1,ou=grupos,dc=cfgm,dc=es
objectClass: posixGroup
objectClass: top
cn: smr1
gidNumber: 4000
```

```
jnav@jnav-vb:~$ nano smr1_grupo.ldif
jnav@jnav-vb:~$ ldapadd -x -W -D "cn=admin,dc=cfgm,dc=es" -f smr1_grupo.ldif
Enter LDAP Password:
adding new entry "cn=smr1,ou=grupos,dc=cfgm,dc=es"

jnav@jnav-vb:~$
```

Segundo grupo:

```
dn: cn=smr2,ou=grupos,dc=cfgm,dc=es
objectClass: posixGroup
objectClass: top
cn: smr2
gidNumber: 5000
```

```
jnav@jnav-vb:~$ nano smr2_grupo.ldif
jnav@jnav-vb:~$ ldapadd -x -W -D "cn=admin,dc=cfgm,dc=es" -f smr2_grupo.ldif
Enter LDAP Password:
adding new entry "cn=smr2,ou=grupos,dc=cfgm,dc=es"

jnav@jnav-vb:~$
```

e)

```
dn: uid=garcia,ou=usuarios,dc=cfgm,dc=es
changetype: modify
replace: uidNumber
uidNumber: 1100
-
add: description
description: admin
```

```
jnav@jnav-vb:~$ nano mod_garcia.ldif
jnav@jnav-vb:~$ ldapmodify -x -W -D "cn=admin,dc=cfgm,dc=es" -f mod_garcia.ldif
Enter LDAP Password:
modifying entry "uid=garcia,ou=usuarios,dc=cfgm,dc=es"
ldap_modify: Type or value exists (20)
    additional info: modify/add: description: value #0 already exists
```

f)

```
jnav@jnav-vb:~$ ldapsearch -xLLL -b dc=cfgm,dc=es uid=garcia
dn: uid=garcia,ou=usuarios,dc=cfgm,dc=es
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: garcia
sn: garcia
givenName: garcia
cn: garcia
gidNumber: 5000
loginShell: /bin/bash
homeDirectory: /home/garcia
uidNumber: 1100
description: admin

jnav@jnav-vb:~$
```

g)

```
dn: uid=garcia,ou=usuarios,dc=cfgm,dc=es
changetype: modify
delete: description
```

```
jnav@jnav-vb:~$ nano mod_garcia.ldif
jnav@jnav-vb:~$ ldapmodify -x -W -D "cn=admin,dc=cfgm,dc=es" -f mod_garcia.ldif
Enter LDAP Password:
modifying entry "uid=garcia,ou=usuarios,dc=cfgm,dc=es"

jnav@jnav-vb:~$ ldapsearch -xLLL -b dc=cfgm,dc=es uid=garcia
dn: uid=garcia,ou=usuarios,dc=cfgm,dc=es
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: garcia
sn: garcia
givenName: garcia
cn: garcia
gidNumber: 5000
loginShell: /bin/bash
homeDirectory: /home/garcia
uidNumber: 1100
jnav@jnav-vb:~$
```

h)

```
dn: uid=juan,ou=usuarios,dc=cfgm,dc=es
changetype: modify
replace: userPassword
userPassword: 123456
-
add: homephone
homephone: 912345678
```

```
jnav@jnav-vb:~$ nano mod_juan.ldif
jnav@jnav-vb:~$ ldapmodify -x -W -D "cn=admin,dc=cfgm,dc=es" -f mod_juan.ldif
Enter LDAP Password:
modifying entry "uid=juan,ou=usuarios,dc=cfgm,dc=es"

jnav@jnav-vb:~$ ldapsearch -xLLL -b dc=cfgm,dc=es uid=juan
dn: uid=juan,ou=usuarios,dc=cfgm,dc=es
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: juan
sn: juan
givenName: juan
cn: juan
uidNumber: 6000
gidNumber: 6000
loginShell: /bin/bash
homeDirectory: /home/juan
homePhone: 912345678
jnav@jnav-vb:~$
```

i)

```
jnav@jnav-vb:~$ ldapsearch -xLLL -b dc=cfgm,dc=es cn=smr1
dn: cn=smr1,ou=grupos,dc=cfgm,dc=es
objectClass: posixGroup
objectClass: top
cn: smr1
gidNumber: 4000

jnav@jnav-vb:~$
```

j)

```
jnav@jnav-vb:~$ ldapsearch -xLLL -b dc=cfgm,dc=es uid=*
dn: uid=navidad,ou=usuarios,dc=cfgm,dc=es
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: navidad
sn: navidad
givenName: navidad
cn: navidad
uidNumber: 4000
gidNumber: 4000
loginShell: /bin/bash
homeDirectory: /home/navidad

dn: uid=garcia,ou=usuarios,dc=cfgm,dc=es
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: garcia
sn: garcia
givenName: garcia
cn: garcia
gidNumber: 5000
loginShell: /bin/bash
homeDirectory: /home/garcia
uidNumber: 1100

dn: uid=juan,ou=usuarios,dc=cfgm,dc=es
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: juan
sn: juan
givenName: juan
cn: juan
uidNumber: 6000
gidNumber: 6000
loginShell: /bin/bash
homeDirectory: /home/juan
homePhone: 912345678

dn: uid=jcng,ou=usuarios,dc=cfgm,dc=es
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: jcng
```

k)

```
jnav@jnav-vb:~$ ldapsearch -xLLL -b dc=cfgm,dc=es uid=* | grep "homeDirectory"
homeDirectory: /home/navidad
homeDirectory: /home/garcia
homeDirectory: /home/juan
homeDirectory: /home/jcng
jnav@jnav-vb:~$
```


I)

```
jnav@jnav-vb:~$ ldapsearch -xLLL -b dc=cfgm,dc=es uid=jcng | grep "gidNumber"
gidNumber: 7000
jnav@jnav-vb:~$
```

8. Indica una herramienta grafica de administración de openldap

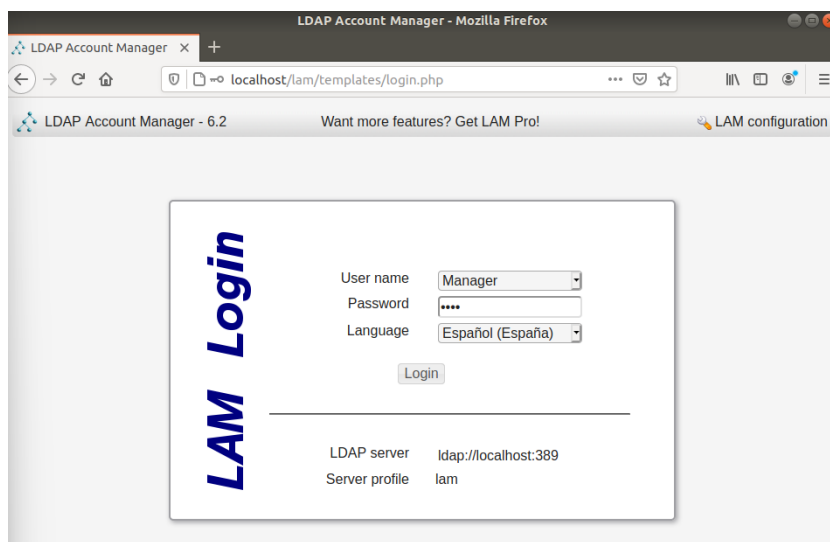
Por ejemplo, una herramienta bastante común, sería **phpldapadmin**.

9. Instalación de LAM

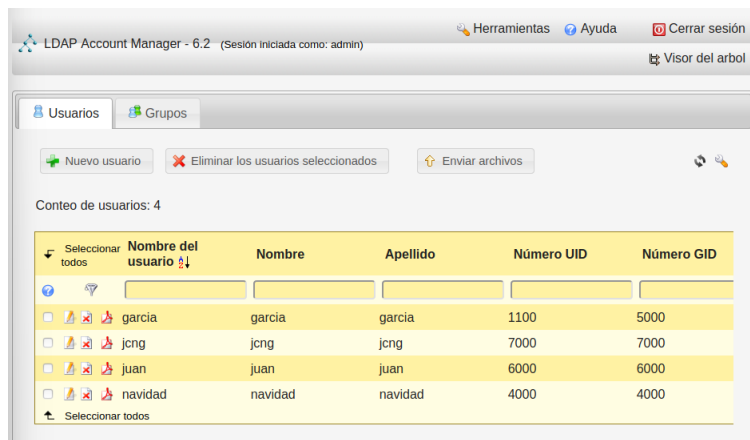
Para instalar LAM, utilizaremos el comando `sudo apt install ldap-account-manager`:

```
jnav@jnav-vb:~$ sudo apt install ldap-account-manager
[sudo] contraseña para jnav:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```

Una vez se haya instalado, comprobaremos que funciona. Nos iremos al navegador y escribiremos: <http://localhost/lam>

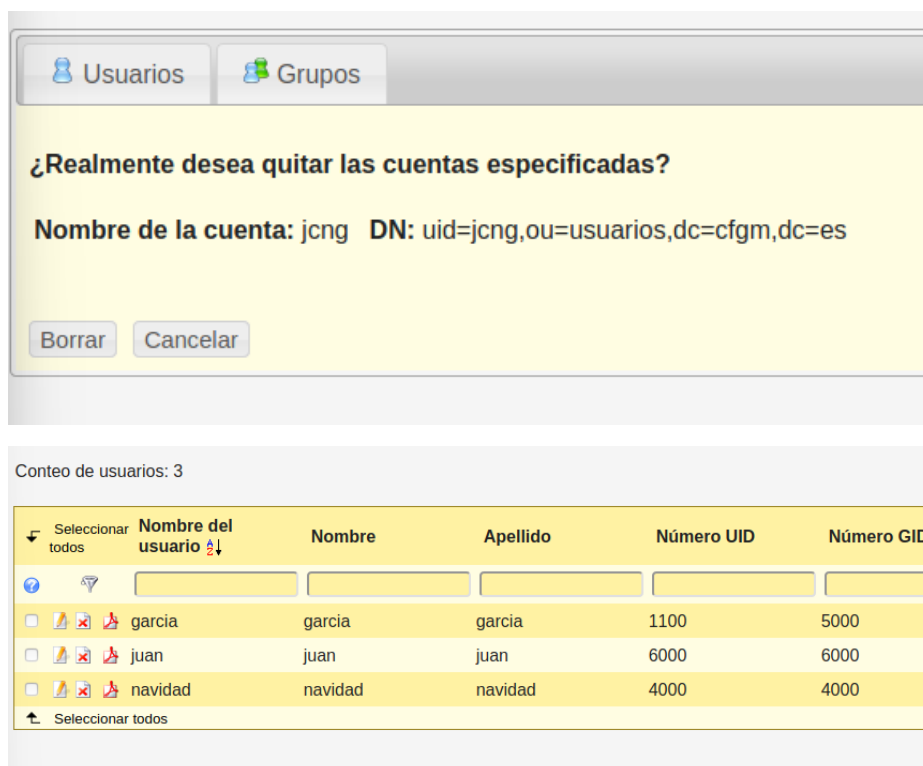


Haciendo unos cuantos ajustes previos, accederemos como admin y con la contraseña configurada anteriormente al instalar openLDAP:



10. Ejercicio 5.9

a)



b)

Usuarios Grupos

Guardar Restablecer cambios. Establecer contraseña default Cargar perfil

garcia garcia Sufijo usuarios > cfgm > es Identificador RDN uid

Personal Unix Sombra

Nombre del usuario * garcia

Nombre común garcia

Número UID 1111

Gecos

Grupo primario smr2

Grupos adicionales Editar grupos

Directorio inicial * /home/garcia

Intérprete del inicio de sesión /bin/bash

Contraseña Bloquear contraseña Quitar contraseña

Seleccionar todos Nombre del usuario Nombre Apellido Número UID Número GID

garcia	garcia	garcia	11111	5000
--------	--------	--------	-------	------

c)

Usuarios Grupos

Guardar Establecer contraseña default Cargar perfil

administradores Sufijo grupos > cfgm > es Identificador RDN cn

Unix

Nombre del grupo * administradores

Número GID 10002

Descripción

Miembros del grupo Editar miembros

juan (juan)

Conteo de grupos: 3

Seleccionar todos Nombre del grupo Número GID Miembros del grupo Descripción del grupo

administradores	10002	juan	
smr1	4000		
smr2	5000		

Seleccionar todos

d)

Nuevo usuario Sufijo usuarios > cfgm > es Identificador RDN

Personal
 Unix
 Sombra

Nombre del usuario *

Nombre común

Número UID

Gecos

Grupo primario

Grupos adicionales

Directorio inicial *

Intérprete del inicio de sesión

Seleccionar todos	Nombre del usuario	Nombre	Apellido	Número UID	Número GID
<input type="checkbox"/>		garcia	garcia	11111	5000
<input type="checkbox"/>		jcng341	jcng341	26529	10002
<input type="checkbox"/>		juan	juan	6000	6000
<input type="checkbox"/>		navidad	navidad	4000	4000
Seleccionar todos					

e)

Datos de contacto

Número de teléfono

Número de teléfono del hogar

Numero de móvil

Número de fax

Dirección de correo electrónico

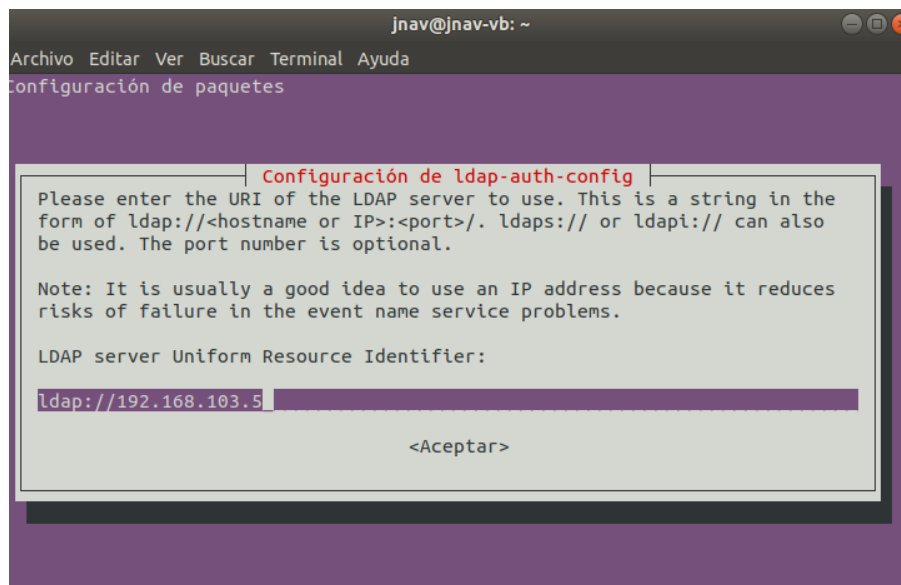
Sitio Web

CONEXIÓN DESDE UN CLIENTE LINUX AL SERVIDOR LDAP

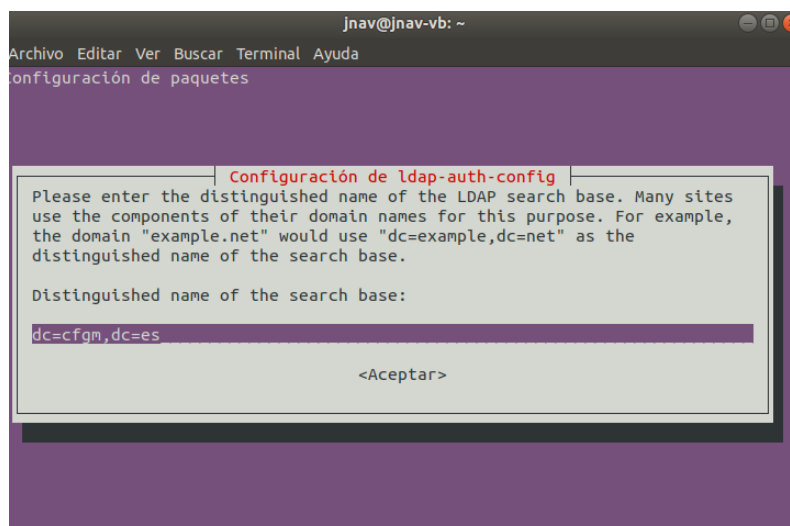
1. Crea una máquina virtual de Ubuntu e instala y configura el cliente LDAP

Para instalar el cliente ldap tenemos que utilizar el siguiente comando:
Sudo apt install libnss-ldap libpam-ldap nscd

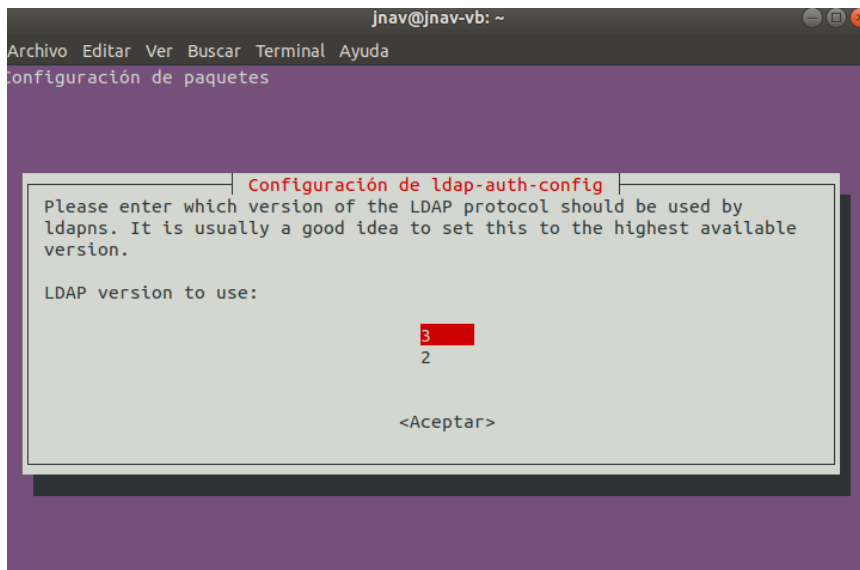
Nos saldrá la siguiente pantalla de configuración en la que tendremos que poner la dirección por la que se podrá acceder:



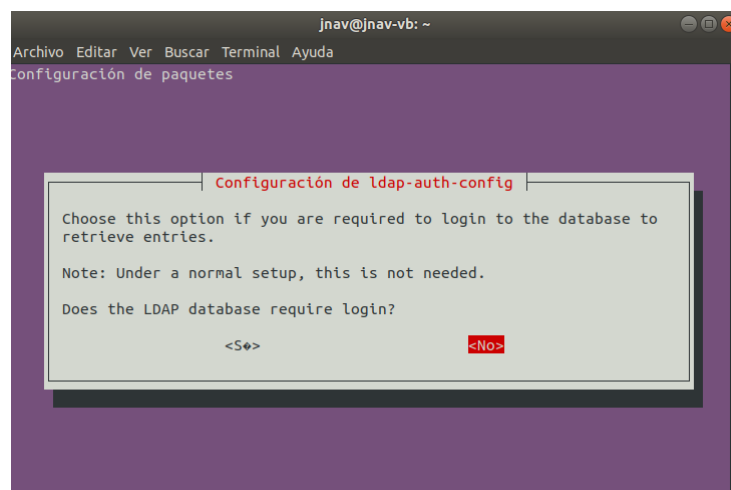
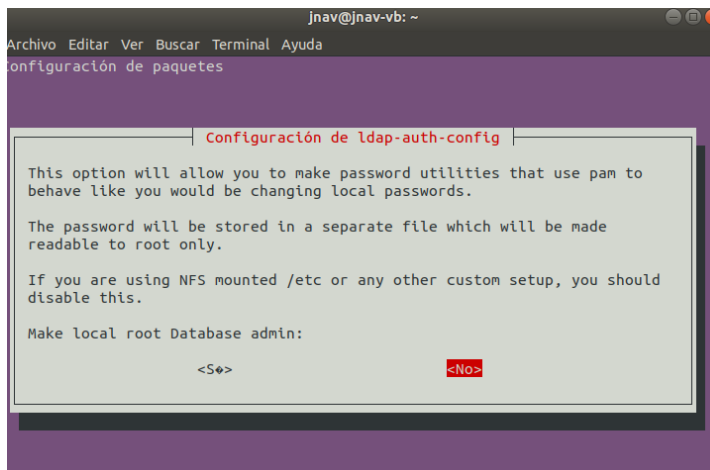
Posteriormente, nos pedirá el dominio que le queremos poner, como anteriormente en OpenLDAP hemos utilizado cfgm.es, en este caso utilizaré el mismo.



Después, elegiremos la versión de LDAP, se recomienda utilizar la última versión.



Esta dos últimas pantallas, es recomendable marcarlas como no.



2. Prueba la conexión del cliente con el servidor LDAP con un usuario

Si utilizamos el comando `getent passwd` podremos comprobar la conexión con el servidor LDAP, este nos devolverá los usuarios que hay, los últimos serán los que pertenecen al servidor:

```
navidad:x:4000:4000:navidad:/home/navidad:/bin/bash
garcia:x:11111:5000:garcia:/home/garcia:/bin/bash
juan:x:6000:6000:juan:/home/juan:/bin/bash
jcng341:*:26529:10002:jcng341:/home/jcng341:/bin/bash
jnav@jnav-vb:~$
```

Si probamos a iniciar sesión con el comando `su <usuario>`, podemos observar cómo inicia sesión:

Para que no quepan dudas de que el usuario pueda estar creado en la máquina directamente, he hecho un `ls` de `/home` y se puede comprobar que solamente está mi usuario.

```
jnav@jnav-vb:~$ ls /home
jnav
jnav@jnav-vb:~$ su jcng341
Contraseña:
Creando directorio «/home/jcng341».
jcng341@jnav-vb:/home/jnav$
```