



RETO 4: OpenLDAP

Patricia Bastida Merino
Javier Díaz Expósito

INDICE

1 ENUNCIADO DEL RETO.....	2
2 CONFIGURACIÓN DEL SERVIDOR.....	3
3 CONFIGURACION DE MAQUINAS CLIENTE.....	14

1. ENUNCIADO DEL RETO

En el mismo servidor en el que hemos instalado el router y el servidor SSH queremos instalar y configurar un **servidor OpenLdap** sobre el dominio **xxxx.olimpo.god**, siendo xxxx el nombre correspondiente al dios de vuestro espacio de trabajo.

Los nombres de los dioses serán los siguientes: **Zeus | Atenea | Hera | Poseidón | Afrodita**

Por lo tanto, los dominios serán:

- (GRUPO 1) □ zeus.olimpo.god
- (GRUPO 2) □ atenea.olimpo.god
- (GRUPO 3) □ hera.olimpo.god
- (GRUPO 4) □ poseidon.olimpo.god

Máquinas conocidas:

- **router:** esta máquina es la que nos da salida al exterior
- **dns:** esta máquina es la misma que el router, pero nos ofrece resolución de nombres
- **ninfa:** es la máquina cliente dentro de vuestra red.
- **Oráculo:** máquina que tiene instalado el servicio FTP y donde instalaremos Apache.
- **Bastís:** Máquina donde instalaremos el Tomcat.

Teniendo en cuenta todo lo anterior, se te pide lo siguiente:

2. CONFIGURACIÓN DEL SERVIDOR

Instala y configura un servidor OpenLdap en Debian 10. El dominio será atenea.olimpo.god:

```
sudo nano /etc/hosts
```

Añadimos los siguientes datos:

```
127.0.0.1    localhost
127.0.1.1    router

10.106.5.1    router.atenea.olimpo.god    router
```

```
dw2@router: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 3.2 /etc/hosts

127.0.0.1    localhost
127.0.1.1    router

# The following lines are desirable for IPv6 capable hosts
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters

10.106.5.1    router.atenea.olimpo.god    router
```

```
sudo nano /etc/hostname
```

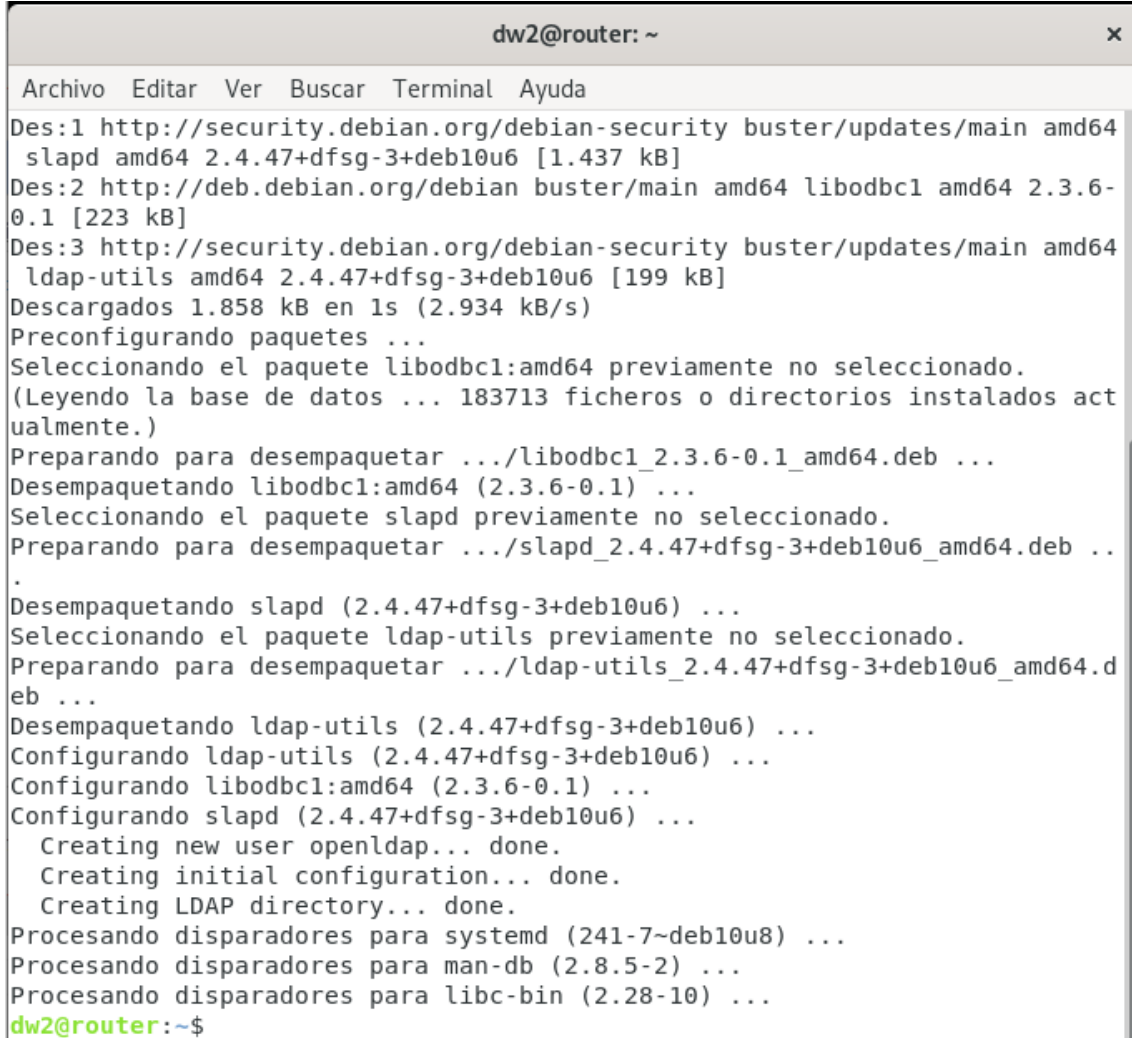
Añadimos en este archivo la palabra *router*. Es lo único que debe contener el archivo.

```
dw2@router: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 3.2 /etc/hostname

router
```

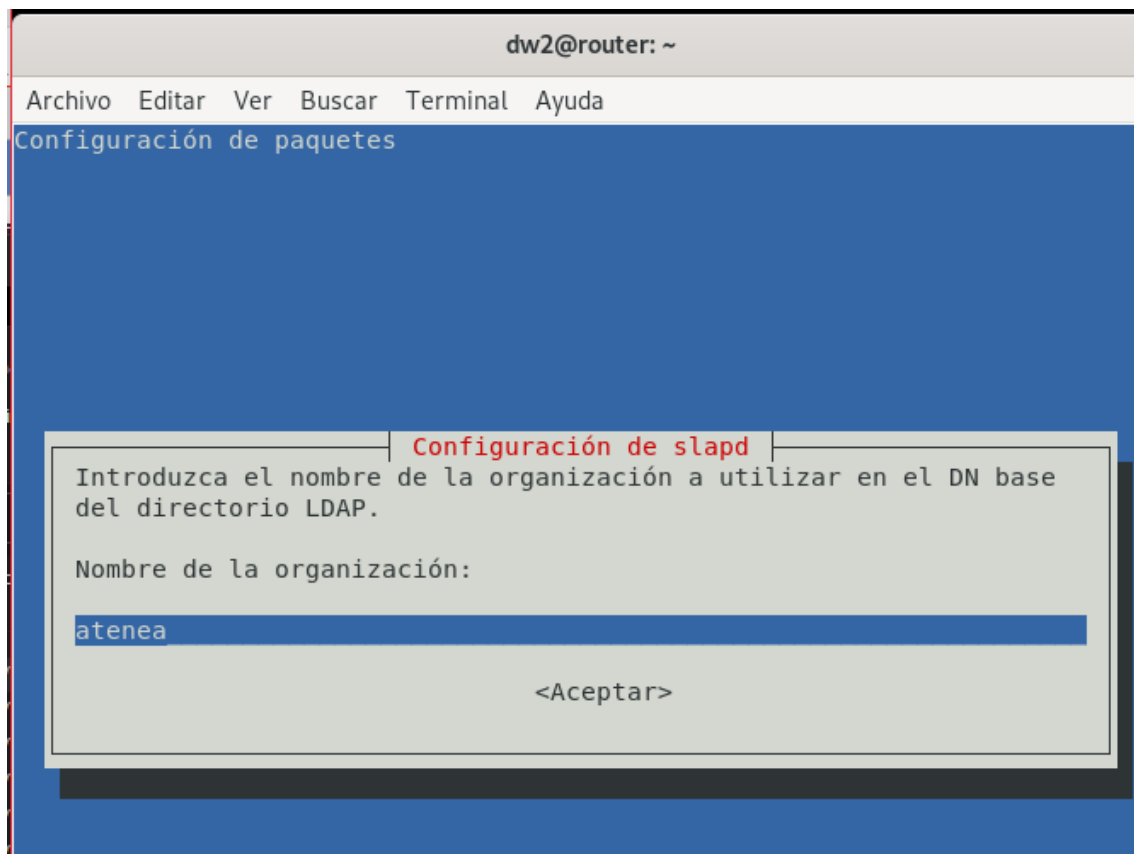
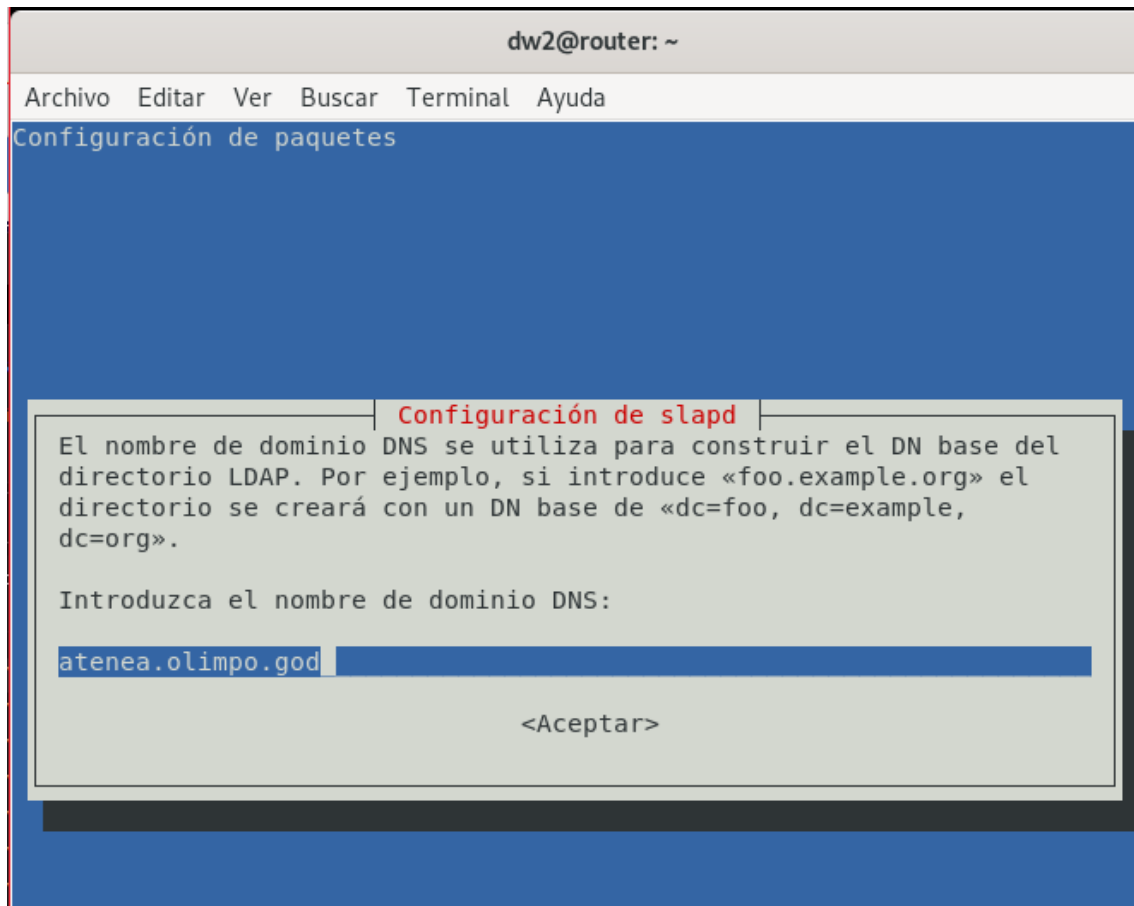
Ahora tenemos que instalar OpenLdap:

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



```
dw2@router: ~
Archivo Editar Ver Buscar Terminal Ayuda
Des:1 http://security.debian.org/debian-security buster/updates/main amd64
slapd amd64 2.4.47+dfsg-3+deb10u6 [1.437 kB]
Des:2 http://deb.debian.org/debian buster/main amd64 libodbc1 amd64 2.3.6-
0.1 [223 kB]
Des:3 http://security.debian.org/debian-security buster/updates/main amd64
ldap-utils amd64 2.4.47+dfsg-3+deb10u6 [199 kB]
Descargados 1.858 kB en 1s (2.934 kB/s)
Preconfigurando paquetes ...
Seleccionando el paquete libodbc1:amd64 previamente no seleccionado.
(Leyendo la base de datos ... 183713 ficheros o directorios instalados act
ualmente.)
Preparando para desempaquetar .../libodbc1_2.3.6-0.1_amd64.deb ...
Desempaquetando libodbc1:amd64 (2.3.6-0.1) ...
Seleccionando el paquete slapd previamente no seleccionado.
Preparando para desempaquetar .../slapd_2.4.47+dfsg-3+deb10u6_amd64.deb ..
.
Desempaquetando slapd (2.4.47+dfsg-3+deb10u6) ...
Seleccionando el paquete ldap-utils previamente no seleccionado.
Preparando para desempaquetar .../ldap-utils_2.4.47+dfsg-3+deb10u6_amd64.d
eb ...
Desempaquetando ldap-utils (2.4.47+dfsg-3+deb10u6) ...
Configurando ldap-utils (2.4.47+dfsg-3+deb10u6) ...
Configurando libodbc1:amd64 (2.3.6-0.1) ...
Configurando slapd (2.4.47+dfsg-3+deb10u6) ...
  Creating new user openldap... done.
  Creating initial configuration... done.
  Creating LDAP directory... done.
Procesando disparadores para systemd (241-7~deb10u8) ...
Procesando disparadores para man-db (2.8.5-2) ...
Procesando disparadores para libc-bin (2.28-10) ...
dw2@router:~$
```

```
dw2@router: ~  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
dw2@router:~$ sudo slapcat  
dn: dc=nodomain  
objectClass: top  
objectClass: dcObject  
objectClass: organization  
o: nodomain  
dc: nodomain  
structuralObjectClass: organization  
entryUUID: 02b5f738-ed71-103b-9101-db22147984aa  
creatorsName: cn=admin,dc=nodomain  
createTimestamp: 20211209192153Z  
entryCSN: 20211209192153.349527Z#000000#000#000000  
modifiersName: cn=admin,dc=nodomain  
modifyTimestamp: 20211209192153Z  
  
dn: cn=admin,dc=nodomain  
objectClass: simpleSecurityObject  
objectClass: organizationalRole  
cn: admin  
description: LDAP administrator  
userPassword:: e1NTSEF9RmdPUGFJK2RQKzLEWnNWL0k0cllaNWExbGpSNks2VTY=  
structuralObjectClass: organizationalRole  
entryUUID: 02b7354e-ed71-103b-9102-db22147984aa  
creatorsName: cn=admin,dc=nodomain  
createTimestamp: 20211209192153Z  
entryCSN: 20211209192153.357715Z#000000#000#000000  
modifiersName: cn=admin,dc=nodomain  
modifyTimestamp: 20211209192153Z  
  
dw2@router:~$ █
```



Mostrar que se ha creado correctamente el dominio.

sudo slapcat

```
dw2@router:~$ sudo slapcat
dn: dc=atenea,dc=olimpo,dc=god
objectClass: top
objectClass: dcObject
objectClass: organization
o: atenea
dc: atenea
structuralObjectClass: organization
entryUUID: 12747810-ed72-103b-91f4-15226842ee00
creatorsName: cn=admin,dc=atenea,dc=olimpo,dc=god
createTimestamp: 20211209192929Z
entryCSN: 20211209192929.260565Z#000000#000#000000
modifiersName: cn=admin,dc=atenea,dc=olimpo,dc=god
modifyTimestamp: 20211209192929Z

dn: cn=admin,dc=atenea,dc=olimpo,dc=god
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9YXNlY3F1c3RWTnMzK25uOTF1dHRlVidEdIdnhqZno=
structuralObjectClass: organizationalRole
entryUUID: 1275053c-ed72-103b-91f5-15226842ee00
creatorsName: cn=admin,dc=atenea,dc=olimpo,dc=god
createTimestamp: 20211209192929Z
entryCSN: 20211209192929.264225Z#000000#000#000000
modifiersName: cn=admin,dc=atenea,dc=olimpo,dc=god
modifyTimestamp: 20211209192929Z

dw2@router:~$ █
```

Crear un fichero “unidades_organizativas.ldif”. Habrá dos unidades organizativas: “profesores” y “alumnos”.

sudo nano unidades_organizativas.ldif

```
dn: ou=profesores,dc=atenea,dc=olimpo,dc=god
objectClass: organizationalUnit
ou: profesores

dn: ou=alumnos,dc=atenea,dc=olimpo,dc=god
objectClass: organizationalUnit
ou: alumnos
```

```
sudo ldapadd -x -D cn=admin,dc=atenea,dc=olimpo,dc=god -W -f
unidades_organizativas.ldif
```

Crear un fichero “usuarios.ldif”. Mediante este fichero vamos a crear el usuario “profe1” en la unidad organizativa “profesores”, y los usuarios “usu1” y “usu2” en la unidad organizativa “alumnos”. Añade todos los objectClass y atributos que consideres necesarios.

```
sudo nano usuarios.ldif
```

```
dn: uid=profe1,ou=profesores,dc=atenea,dc=olimpo,dc=god
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: profe1
sn: Lopez
givenName: Juan
cn: Juan Lopez
uidNumber: 2000
gidNumber: 10000
userPassword: dw2
homeDirectory: /home/profe1

dn: uid=usu1,ou=alumnos,dc=atenea,dc=olimpo,dc=god
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: usu1
sn: Gomez
givenName: Paco
cn: Paco Gomez
uidNumber: 2001
gidNumber: 20001
userPassword: dw2
homeDirectory: /home/usu1

dn: uid=usu2,ou=alumnos,dc=atenea,dc=olimpo,dc=god
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
```

```
uid: usu2
sn: Garcia
givenName: Sergio
cn: Sergio Garcia
uidNumber: 2002
gidNumber: 20001
userPassword: dw2
homeDirectory: /home/usu2
```

```
sudo ldapadd -x -D cn=admin,dc=atenea,dc=olimpodc=god -W -f
usuarios.ldif
```

Utilizando un comando “ldap” para mostrar todos los elementos del directorio que pertenecen a la unidad organizativa “alumnos”.

```
Ldapsearch -W -D “cn=admin,dc=atenea,dc=olimpodc=god” -b “ou=alumnos,
dc=atenea,dc=olimpodc=god” givenName dn
```

```
dw2@router:~$ ldapsearch -W -D "cn=admin,dc=atenea,dc=olimpodc=god" -b "ou=alumnos,dc=atenea,dc=olimpodc=god" givenName dn
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <ou=alumnos,dc=atenea,dc=olimpodc=god> with scope subtree
# filter: (objectclass=*)
# requesting: givenName dn
#
# alumnos, atenea.olimpodc=god
dn: ou=alumnos,dc=atenea,dc=olimpodc=god
# usu1, alumnos, atenea.olimpodc=god
dn: uid=usu1,ou=alumnos,dc=atenea,dc=olimpodc=god
givenName: Paco
# usu2, alumnos, atenea.olimpodc=god
dn: uid=usu2,ou=alumnos,dc=atenea,dc=olimpodc=god
givenName: Sergio
# search result
search: 2
result: 0 Success
# numResponses: 4
# numEntries: 3
dw2@router:~$ █
```

Investigar cómo utilizar el comando “ldapmodify” y cambia el apellido al usuario “usu1” de la unidad organizativa “alumnos” y añádele el número de teléfono.

```
sudo nano modificar.ldif -W -D "cn=admin,dc=atenea,dc=olimp,dc=god" -h router
```

```
dw2@router:~$ ldapmodify -W -D "cn=admin,dc=atenea,dc=olimp,dc=god" -h router
Enter LDAP Password:
dn:uid=usu1,ou=alumnos,dc=atenea,dc=olimp,dc=god
changetype:modify
replace:sn
sn:Almodobar
-
modifying entry "uid=usu1,ou=alumnos,dc=atenea,dc=olimp,dc=god"
```

```
dw2@router:~$ ldapmodify -W -D "cn=admin,dc=atenea,dc=olimp,dc=god" -h router
Enter LDAP Password:
dn:uid=usu1,ou=alumnos,dc=atenea,dc=olimp,dc=god
changetype:modify
add:mobile
mobile:123456789
modifying entry "uid=usu1,ou=alumnos,dc=atenea,dc=olimp,dc=god"
```

Busca información sobre los atributos que pueden tener entradas con los siguientes objectClass: organizationalUnit, inetOrgPerson, posixAccount y organizationalRole.

Señala los atributos que debe tener la entrada obligatoriamente para cada uno de ellos.

Crear un fichero “modificar.ldif”. Mediante este fichero modificarás un atributo del alumno “usu1” (cualquiera) y añadiras tres atributos que no tenía a la entrada de “usu2”.

```
sudo nano modificar.ldif
```

```
dn:uid=usu1,ou=alumnos,dc=atenea,dc=olimp,dc=god
changetype:modify
replace:sn
sn:Garcia

dn:uid=usu2,ou=alumnos,dc=atenea,dc=olimp,dc=god
```

```
changetype:modify
add:mobile
mobile: 123456789
-

add:homePhone
homePhone: 454364178
-

add: mail
mail: alumno2@olimpo.god
```

```
dw2@router:~$ ldapmodify -W -D "cn=admin,dc=atenea,dc=olimpo,dc=god" -h router -f modificar.ldif
Enter LDAP Password:
modifying entry "uid=usu1,ou=alumnos,dc=atenea,dc=olimpo,dc=god"

modifying entry "uid=usu2,ou=alumnos,dc=atenea,dc=olimpo,dc=god"

dw2@router:~$ █
```

```
dn: uid=usu1,ou=alumnos,dc=atenea,dc=olimpo,dc=god
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: usu1
givenName: Paco
cn: Paco Gomez
uidNumber: 2001
gidNumber: 20001
userPassword:: ZHcyIA==
homeDirectory: /home/usu1
structuralObjectClass: inetOrgPerson
entryUUID: 1eee9654-ed75-103b-83ab-db2f5391b0b3
creatorsName: cn=admin,dc=atenea,dc=olimpo,dc=god
createTimestamp: 20211209195118Z
mobile: 123456789
sn: Garcia
entryCSN: 20211212191524.029482Z#000000#000#000000
modifiersName: cn=admin,dc=atenea,dc=olimpo,dc=god
modifyTimestamp: 20211212191524Z
```

```
dn: uid=usu2,ou=alumnos,dc=atenea,dc=olimpo,dc=god
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: usu2
sn: Garcia
givenName: Sergio
cn: Sergio Garcia
uidNumber: 2002
gidNumber: 20001
userPassword:: ZHcyIA==
homeDirectory: /home/usu2
structuralObjectClass: inetOrgPerson
entryUUID: 1eef0d8c-ed75-103b-83ac-db2f5391b0b3
creatorsName: cn=admin,dc=atenea,dc=olimpo,dc=god
createTimestamp: 20211209195118Z
mobile: 123456789
homePhone: 454364178
mail: alumno2@olimpo.god
entryCSN: 20211212191524.033091Z#000000#000#000000
modifiersName: cn=admin,dc=atenea,dc=olimpo,dc=god
modifyTimestamp: 20211212191524Z
```

Crear un archivo ldif para añadir un nuevo profesor “profe2” y un alumno más a los existentes “usu3”.

```
sudo nano usuarios2.ldif
```

```
dn: uid=profe2,ou=profesores,dc=atenea,dc=olimpo,dc=god
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: profe2
sn: Gomez
givenName: Alfredo
cn: Alfredo Gomez
uidNumber: 2004
gidNumber: 10000
userPassword: dw2
homeDirectory: /home/profe2

dn: uid=usu3,ou=alumnos,dc=atenea,dc=olimpo,dc=god
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: usu3
```

```
sn: Sanchez
givenName: Pedro
cn: Pedro Sanchez
uidNumber: 2003
gidNumber: 20001
userPassword: dw2
homeDirectory: /home/usu3
```

```
sudo ldapadd -x -D cn=admin,dc=atenea,dc=olimpodc=god -W -f
usuarios2.ldif
```

Muestra de nuevo todos los elementos del directorio que pertenecen a la unidad organizativa “profesores” y “alumnos”.

```
dw2@router:~$ ldapsearch -W -D "cn=admin,dc=atenea,dc=olimpodc=god" -b "ou=alumnos,dc=atenea,dc=olimpodc=god" givenName dn
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <ou=alumnos,dc=atenea,dc=olimpodc=god> with scope subtree
# filter: (objectclass=*)
# requesting: givenName dn
#
# alumnos, atenea.olimpodc=god
dn: ou=alumnos,dc=atenea,dc=olimpodc=god

# usu1, alumnos, atenea.olimpodc=god
dn: uid=usu1,ou=alumnos,dc=atenea,dc=olimpodc=god
givenName: Paco

# usu2, alumnos, atenea.olimpodc=god
dn: uid=usu2,ou=alumnos,dc=atenea,dc=olimpodc=god
givenName: Sergio

# usu3, alumnos, atenea.olimpodc=god
dn: uid=usu3,ou=alumnos,dc=atenea,dc=olimpodc=god
givenName: Pedro

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4

dw2@router:~$ ldapsearch -W -D "cn=admin,dc=atenea,dc=olimpodc=god" -b "ou=profesores,dc=atenea,dc=olimpodc=god" givenName dn
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <ou=profesores,dc=atenea,dc=olimpodc=god> with scope subtree
# filter: (objectclass=*)
# requesting: givenName dn
#
# profesores, atenea.olimpodc=god
dn: ou=profesores,dc=atenea,dc=olimpodc=god

# profel1, profesores, atenea.olimpodc=god
dn: uid=profel1,ou=profesores,dc=atenea,dc=olimpodc=god
givenName: Juan

# profe2, profesores, atenea.olimpodc=god
dn: uid=profe2,ou=profesores,dc=atenea,dc=olimpodc=god
givenName: Alfredo

# search result
search: 2
result: 0 Success

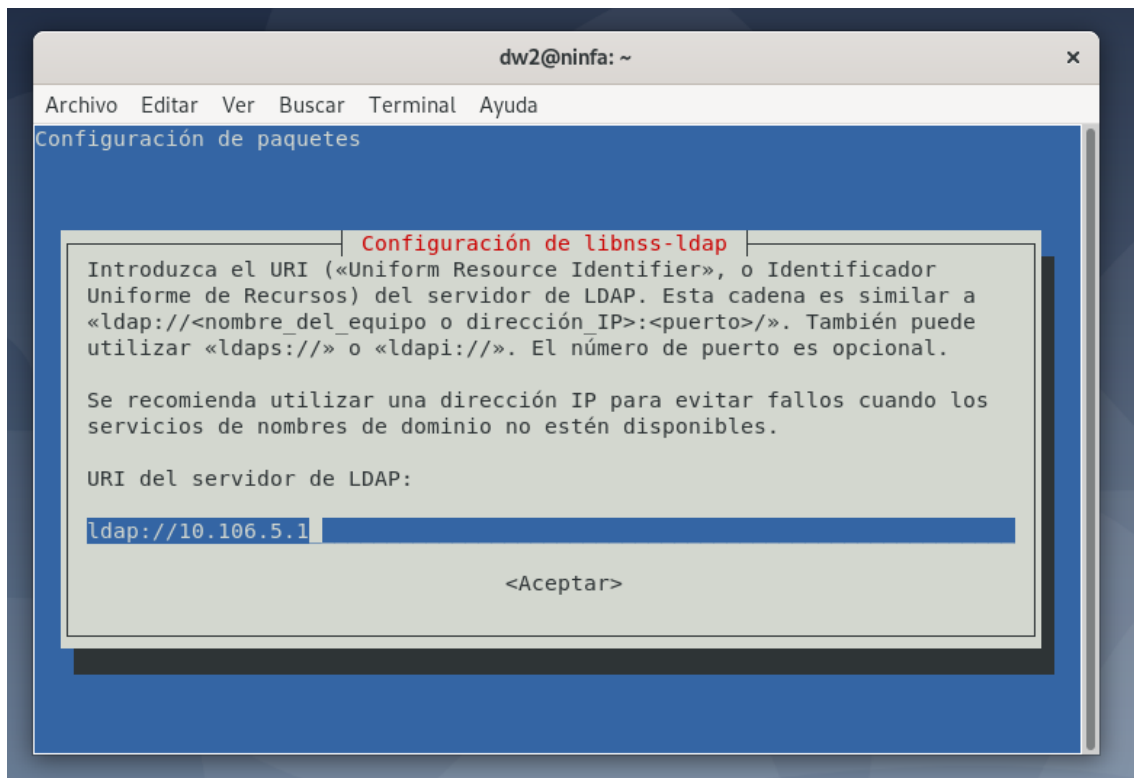
# numResponses: 4
# numEntries: 3
dw2@router:~$
```

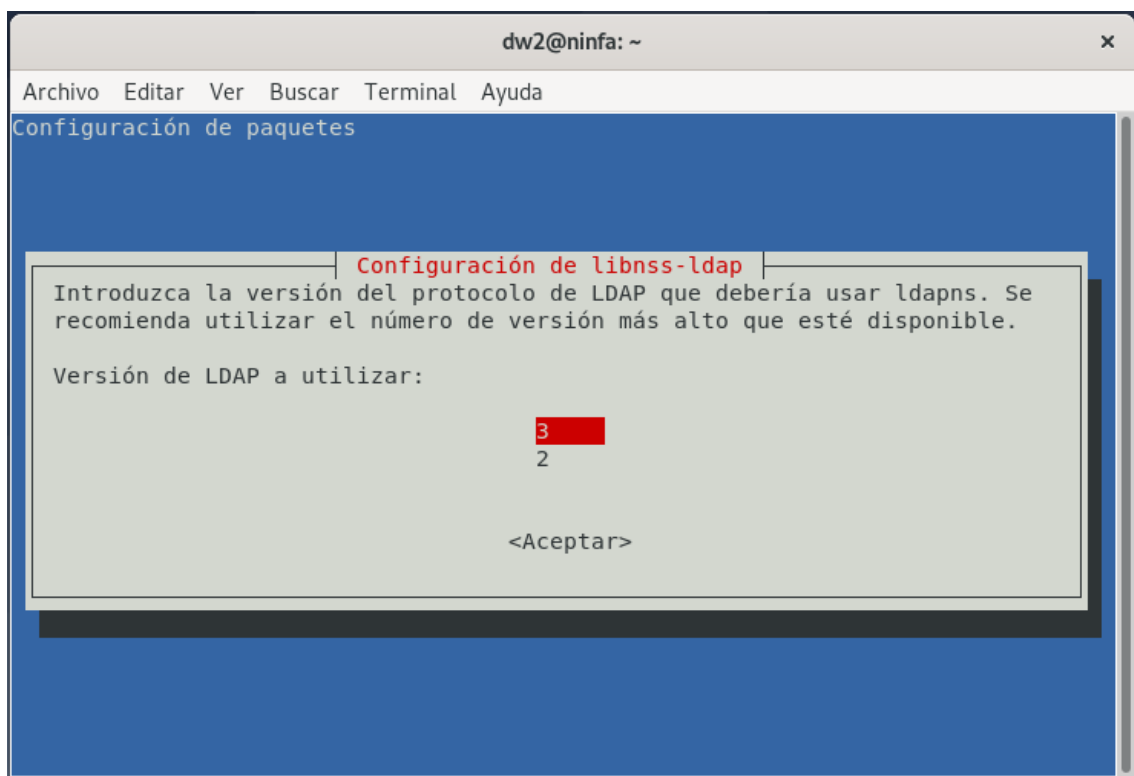
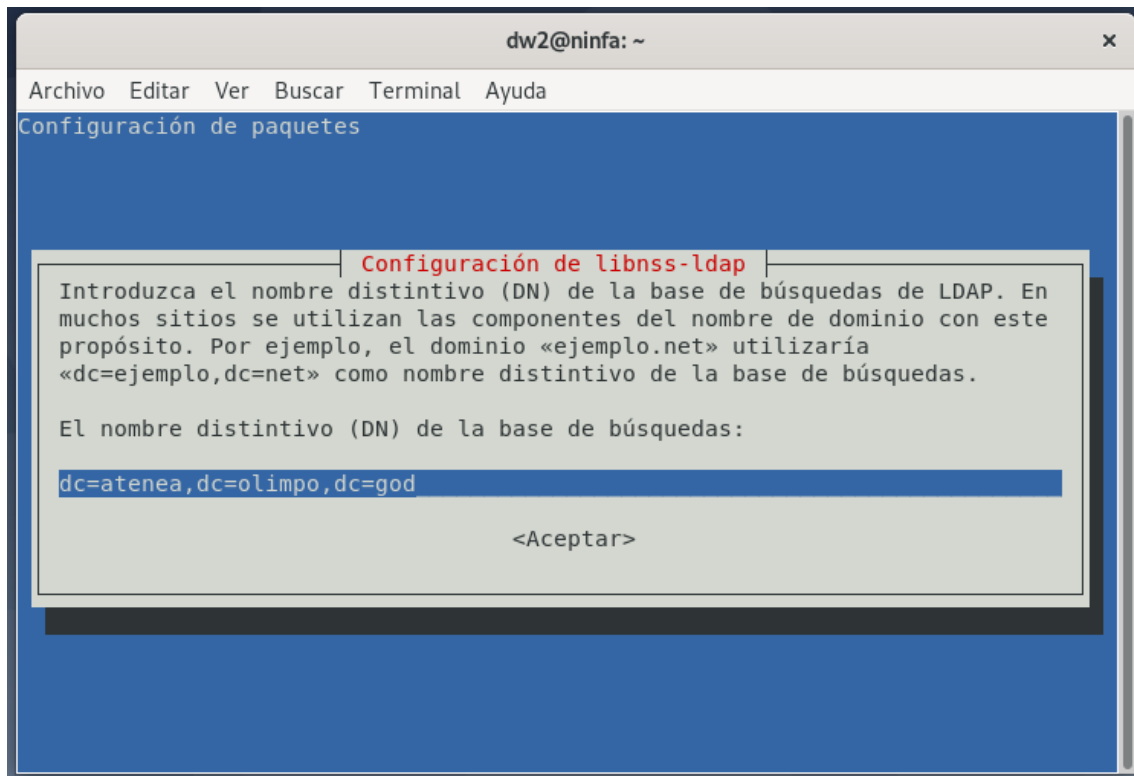
3. CONFIGURACION DE MAQUINAS CLIENTE

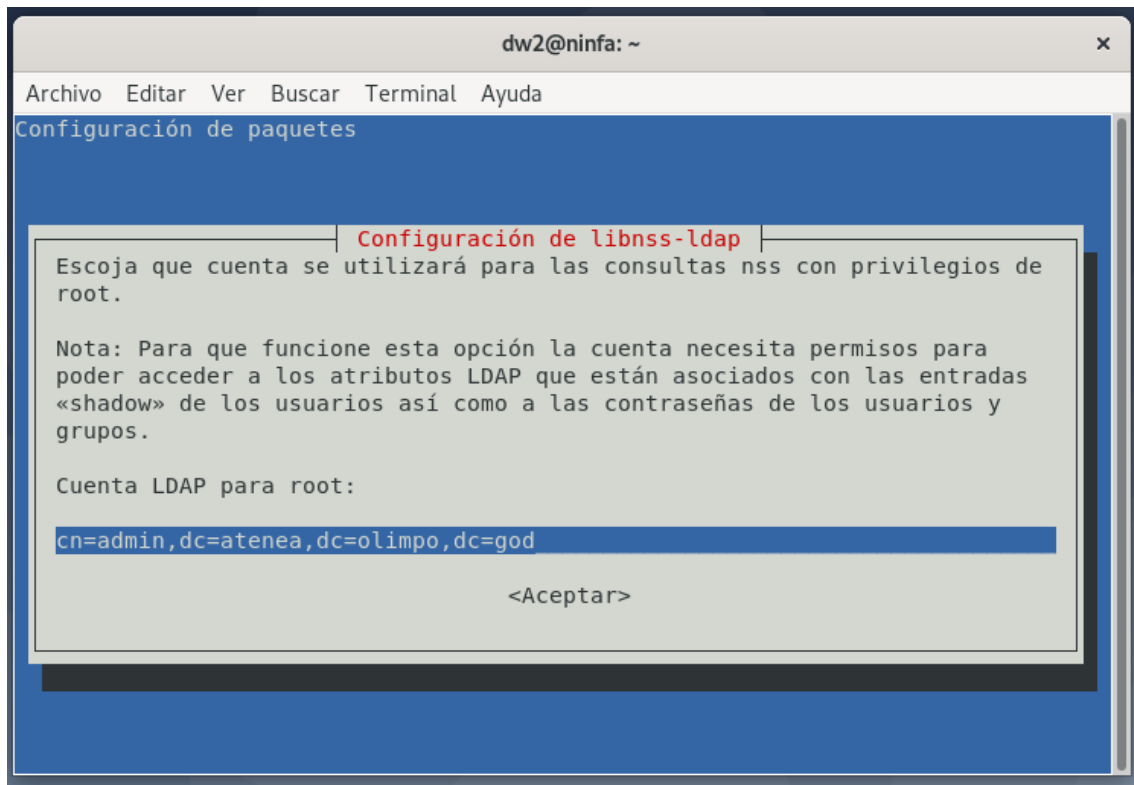
Configura los diferentes clientes/máquinas de la red para que puedan autenticarse contra el servidor OpenLdap.

*Instalación de paquetes necesarios:

```
sudo apt-get install libnss-ldap libpam-ldap ldap-utils -y
```

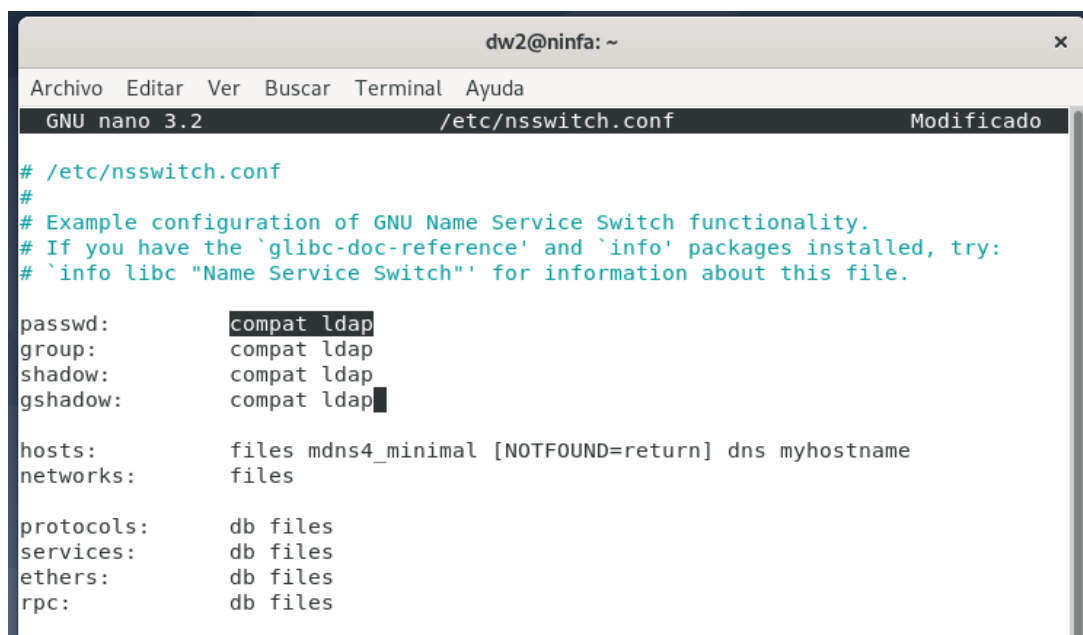






Introducimos el siguiente comando y cambiamos el valor de passwd, group, shadow y de gshadow por compat ldap en todas ellas.

```
sudo nano /etc/nsswitch.conf
```



```
sudo nano /etc/pam.d/common-password
```

```
dw2@ninfa: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
GNU nano 3.2 /etc/pam.d/common-password

# the default is Unix crypt. Prior releases used the option "md5".
#
# The "obscure" option replaces the old `OBSOLETE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password      [success=2 default=ignore]      pam_unix.so obscure sha512
password      [success=1 user_unknown=ignore default=die]      pam_ldap.so use_authok try_first$
# here's the fallback if no module succeeds
password      requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
```

Hay que eliminar use_authok:

```
dw2@ninfa: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
GNU nano 3.2 /etc/pam.d/common-password Modificado

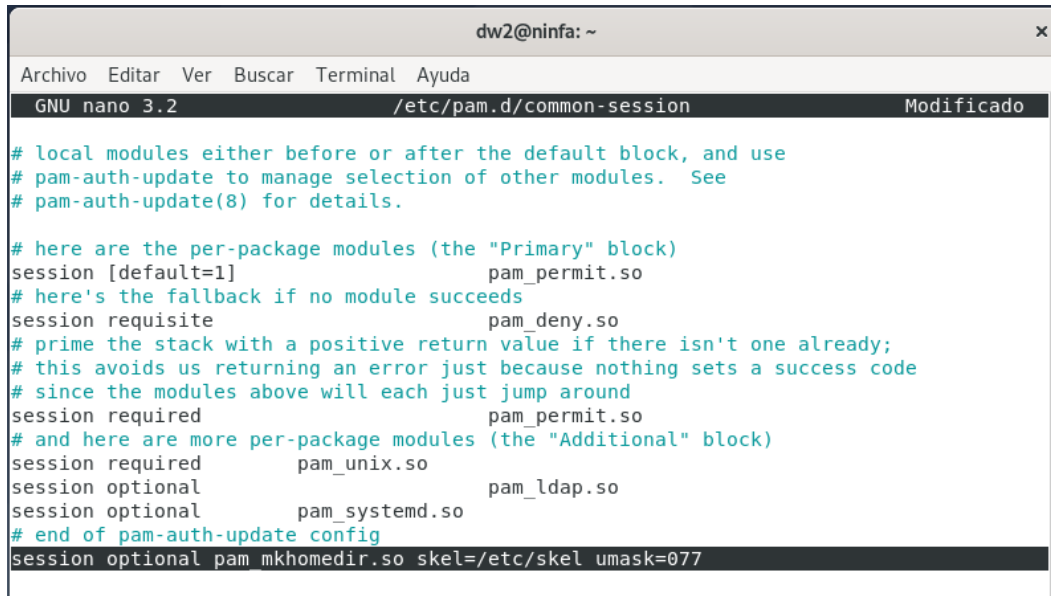
# the default is Unix crypt. Prior releases used the option "md5".
#
# The "obscure" option replaces the old `OBSOLETE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password      [success=2 default=ignore]      pam_unix.so obscure sha512
password      [success=1 user_unknown=ignore default=die]      pam_ldap.so try_first_pass
# here's the fallback if no module succeeds
password      requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
```

```
sudo nano /etc/pam.d/common-session
```

Añadimos en la última línea del archivo lo seleccionado en la siguiente captura:



```
dw2@ninja: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
GNU nano 3.2 /etc/pam.d/common-session Modificado  
# local modules either before or after the default block, and use  
# pam-auth-update to manage selection of other modules. See  
# pam-auth-update(8) for details.  
  
# here are the per-package modules (the "Primary" block)  
session [default=1] pam_permit.so  
# here's the fallback if no module succeeds  
session requisite pam_deny.so  
# prime the stack with a positive return value if there isn't one already;  
# this avoids us returning an error just because nothing sets a success code  
# since the modules above will each just jump around  
session required pam_permit.so  
# and here are more per-package modules (the "Additional" block)  
session required pam_unix.so  
session optional pam_ldap.so  
session optional pam_systemd.so  
# end of pam-auth-update config  
session optional pam mkhomedir.so skel=/etc/skel umask=077
```

Instalamos el programa sysv-rc-conf con el siguiente comando:

```
sudo apt-get install sysv-rc-conf
```

Y ahora lo activamos libnss-ldap con el siguiente comando:

```
sudo sysv-conf libnss-ldap on
```

Reiniciamos la máquina cliente y comprobamos que logea:



```
Debian GNU/Linux 10 bastis tty3  
bastis login: usu3  
Password:  
Linux bastis 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Creating directory '/home/usu3'.  
$ _
```