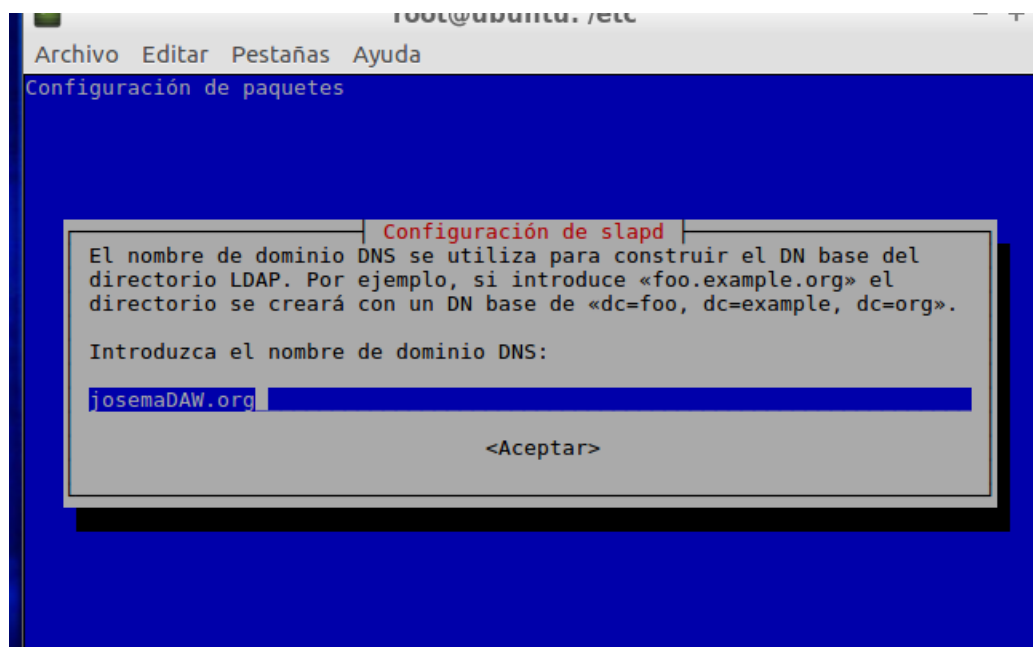
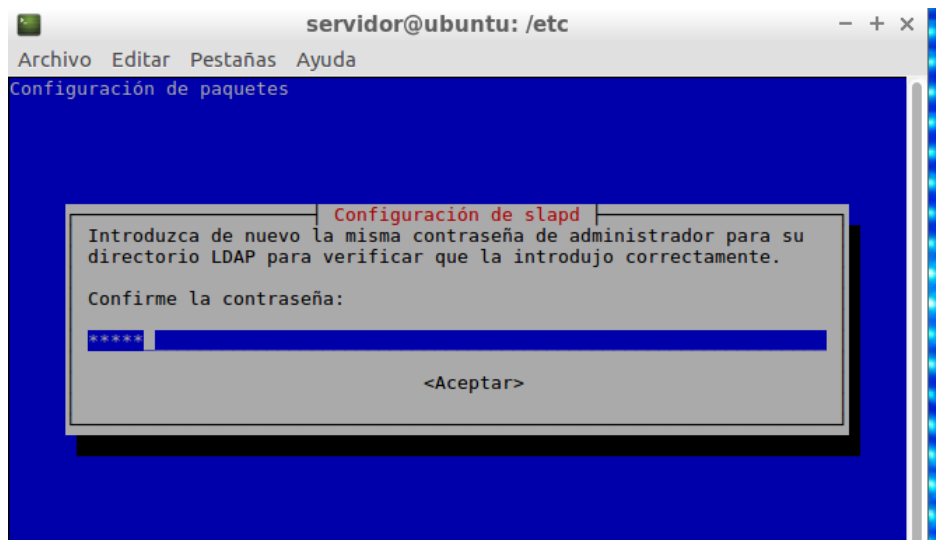


Alumno/a: José Manuel González Peña

PRÁCTICA 15. INSTALACIÓN Y CONFIGURACIÓN DE UN SERVICIO LDAP.

1. Configuración del Servidor: instala y define el dominio para el servicio OpenLDAP

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



- Indica *el mismo nombre de dominio que en práctica anterior.*
- Comprueba con `#sldapcat` que la estructura básica del árbol LDAP ya ha sido creada y no tienes que hacerlo mediante un fichero `.ldif` (saltar por tanto paso indicado en documentación ITE)

```

servidor@ubuntu:/$ sudo slapcat
58fd9f52 ldif_read_file: checksum error on "/etc/ldap/slapd.d/cn=config.ldif"
dn: dc=josemaDAW,dc=org
objectClass: top
objectClass: dcObject
objectClass: organization
o: josemaDAW.org
dc: josemaDAW
structuralObjectClass: organization
entryUUID: d102c0b8-b936-1036-9090-e92f80642fe6
creatorsName: cn=admin,dc=josemaDAW,dc=org
createTimestamp: 20170419102930Z
entryCSN: 20170419102930.336435Z#000000#000#000000
modifiersName: cn=admin,dc=josemaDAW,dc=org
modifyTimestamp: 20170419102930Z

dn: cn=admin,dc=josemaDAW,dc=org
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9M2ZlamxseTVuZGpMQk1q0VRibE9VZnhvTCsrUWZDS0Y=
structuralObjectClass: organizationalRole
entryUUID: d1043e98-b936-1036-9091-e92f80642fe6
creatorsName: cn=admin,dc=josemaDAW,dc=org
createTimestamp: 20170419102930Z
entryCSN: 20170419102930.346417Z#000000#000#000000
modifiersName: cn=admin,dc=josemaDAW,dc=org
modifyTimestamp: 20170419102930Z

```

- ¿Qué puerto usa LDAP? Comprueba que está levantado mediante NMAP (si no lo tienes instalado instálalo).

```

servidor@ubuntu:/etc$ nmap 192.168.1.152

Starting Nmap 7.01 ( https://nmap.org ) at 2017-04-26 12:24 CEST
Nmap scan report for www.josemagonzalez.es (192.168.1.152)
Host is up (0.000040s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
389/tcp   open  ldap
443/tcp   open  https
8080/tcp   open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
servidor@ubuntu:/etc$

```

389

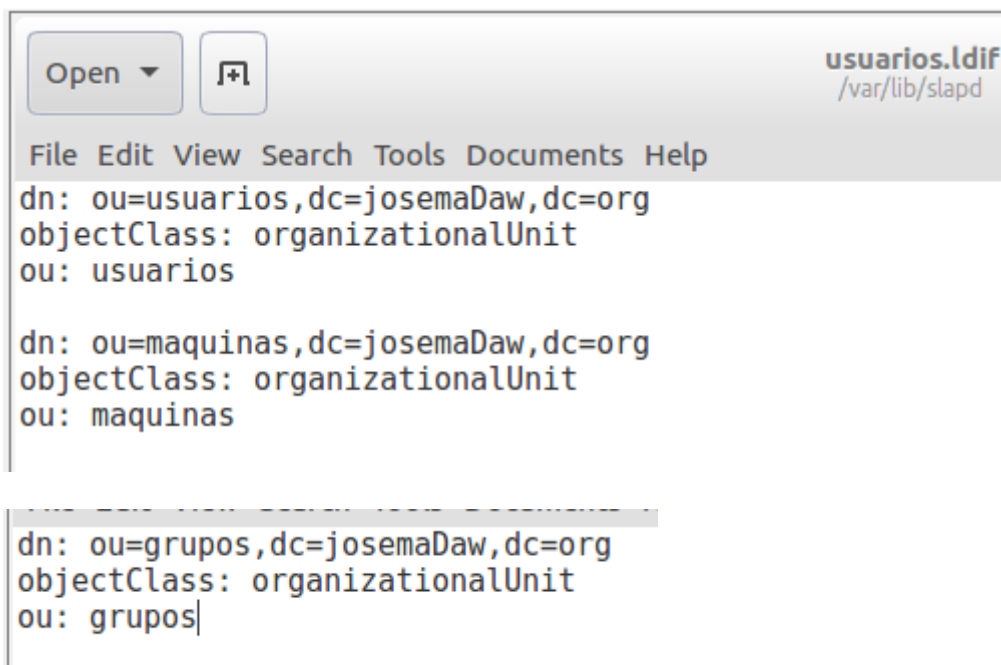
- ¿Dónde se guarda la configuración de LDAP? Busca el fichero ldap.conf y observa si tienes que modificar algo.

```

servidor@ubuntu:/etc/ldap$ cat ldap.conf
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
#BASE    dc=example,dc=com
#URI      ldap://ldap.example.com ldap://ldap-master.example.com:666
#
#SIZELIMIT    12
#TIMELIMIT    15
#DEREF        never
#
# TLS certificates (needed for GnuTLS)
#TLS_CACERT    /etc/ssl/certs/ca-certificates.crt

```

2. Crear para el dominio una estructura de unidades organizativas donde se puedan dar de alta los usuarios del sistema (*OUalumnos*, *OUprofesores*) y otra *OU* para *maquinasWXP* (*OUxp*).



```

dn: ou=usuarios,dc=josemaDaw,dc=org
objectClass: organizationalUnit
ou: usuarios

dn: ou=maquinas,dc=josemaDaw,dc=org
objectClass: organizationalUnit
ou: maquinas

```

```

dn: ou=grupos,dc=josemaDaw,dc=org
objectClass: organizationalUnit
ou: grupos

```

```

root@ubuntu:/var/lib/slapd# slapadd -v -l usuarios.ldif
59007950 ldif_read_file: checksum error on "/etc/ldap/slapd.d/cn=config.ldif"
added: "ou=usuarios,dc=josemaDaw,dc=org" (00000003)
added: "ou=maquinas,dc=josemaDaw,dc=org" (00000004)
##### 100.00% eta    none elapsed          none fast!
Closing DB...
root@ubuntu:/var/lib/slapd# /etc/init.d/slapd start
[ ok ] Starting slapd (via systemctl): slapd.service.

```

3. Crear una serie de usuarios y grupos en LDAP mediante las herramientas de consola (fichero .ldif en /var/lib/ldap) o mediante la herramienta PHPLAPADMIN y comprobar mediante un navegador la configuración realizada desde consola.

Usuarios: alumno y profesor

Grupos: grupoalumnos y grupoprofesores

```
Open [icon] grupos.ldif /var/lib/slapd
File Edit View Search Tools Documents Help
dn: cn=grupoAlumnos,ou=grupos,dc=josemaDaw,dc=org
objectClass: posixGroup
gidNumber: 11000

dn: cn=grupoProfesores,ou=grupos,dc=josemaDaw,dc=org
objectClass: posixGroup
gidNumber: 11001|
```

```
Open [icon] cuentas.ldif /var/lib/slapd
File Edit View Search Tools Documents Help
dn: cn=alumno,ou=usuarios,dc=josemaDaw,dc=org
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: ShadowAccount
uid: alumno
cn: alumno
givenName: alumno
sn: alumno
uidNumber: 1000|
gidNumber: 11000
userPassword: alumno
loginShell: /bin/bash
homeDirectory: /home/nfs/alumno
mail: alumno@alumno.com

dn: cn=profesor,ou=usuarios,dc=josemaDaw,dc=org
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: ShadowAccount
uid: profesor
cn: profesor
givenName: profesor
sn: profesor
uidNumber: 1001
gidNumber: 11001
userPassword: profesor
loginShell: /bin/bash
homeDirectory: /home/nfs/profesor
mail: profesor@profesor.com|
```

```

root@ubuntu:/var/lib/slapd# slapadd -v -l grupos.ldif
59007dc4 ldif_read_file: checksum error on "/etc/ldap/slapd.d/cn=config.ldif"
added: "cn=grupoAlumnos,ou=grupos,dc=josemaDaw,dc=org" (000000006)
added: "cn=grupoProfesores,ou=grupos,dc=josemaDaw,dc=org" (000000007)
##### 100.00% eta none elapsed none fast!
Closing DB...Error, entries missing!
entry 5: ou=grupos,dc=josemadaw,dc=org

root@ubuntu:/var/lib/slapd# slapadd -v -l cuentas.ldif
59007dce ldif_read_file: checksum error on "/etc/ldap/slapd.d/cn=config.ldif"
added: "cn=alumno,ou=usuarios,dc=josemaDaw,dc=org" (000000008)
added: "cn=profesor,ou=usuarios,dc=josemaDaw,dc=org" (000000009)
##### 100.00% eta none elapsed none fast!
Closing DB...
root@ubuntu:/var/lib/slapd#

```

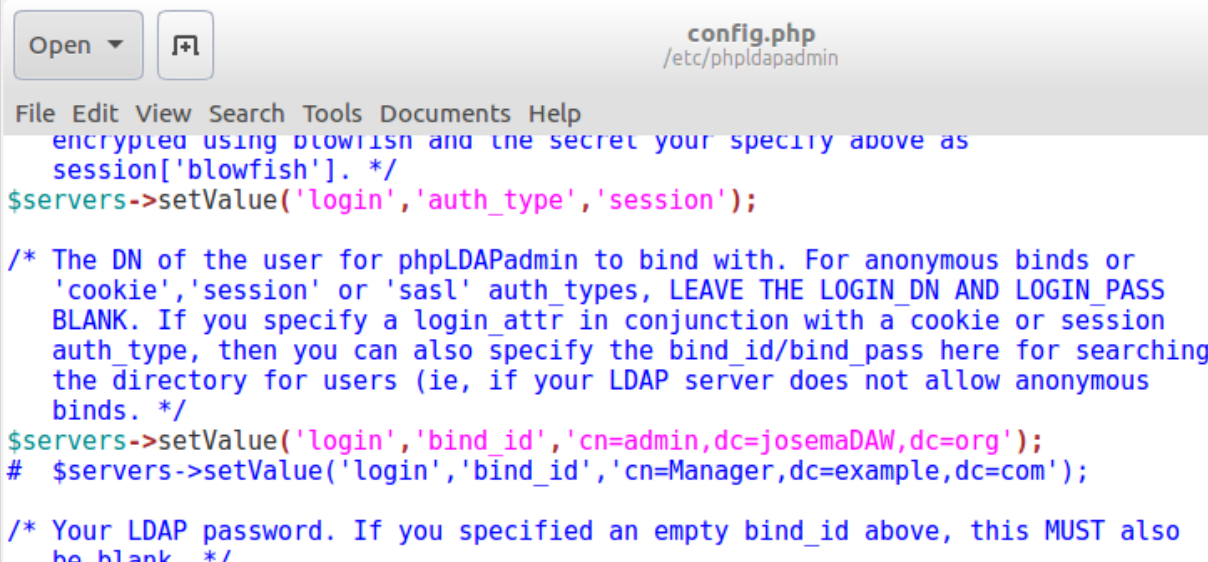
4. Comprobar mediante la orden de consola *ldapsearch* (y/o mediante el navegador usando PHPLDAPADMIN) la configuración realizada : grupos , usuarios, etc que se han creado adecuadamente.

```

root@ubuntu:/home/nfs# apt-get install phpldapadmin -y

```

Editamos el fichero de configuración para que lo detecte bien la db



```

config.php
/etc/phpldapadmin

File Edit View Search Tools Documents Help
encrypted using blowfish and the secret you specify above as
session['blowfish']. */
$servers->setValue('login','auth_type','session');

/* The DN of the user for phpLDAPAdmin to bind with. For anonymous binds or
'cookie','session' or 'sasl' auth_types, LEAVE THE LOGIN_DN AND LOGIN_PASS
BLANK. If you specify a login_attr in conjunction with a cookie or session
auth_type, then you can also specify the bind_id/bind_pass here for searching
the directory for users (ie, if your LDAP server does not allow anonymous
binds. */
$servers->setValue('login','bind_id','cn=admin,dc=josemaDAW,dc=org');
# $servers->setValue('login','bind_id','cn=Manager,dc=example,dc=com');

/* Your LDAP password. If you specified an empty bind_id above, this MUST also
be blank. */

```



5. Las carpetas personales de cada usuario se crearán en /home/nfs/

Instalamos los paquetes necesarios de nfs

```
root@ubuntu:/var/lib/ldap# apt-get install nfs-common nfs-kernel-server
```



```

Open [icon] exports
/etc

File Edit View Search Tools Documents Help
# /etc/exports: the access control list for filesystems which
#           to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes          hostname1(rw,sync,no_subtree_check) hostname1
#
# Example for NFSv4:
# /srv/nfs4           gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes     gss/krb5i(rw,sync,no_subtree_check)
#
/home/nfs             192.168.1.0/255.255.255.0(rw)|

```

```

root@ubuntu:/home# ls
gopejo invitado servidor
root@ubuntu:/home# mkdir nfs
root@ubuntu:/home# chmod 775 nfs/
root@ubuntu:/home# ls -l
total 16
drwxr-xr-x  4 gopejo   root    4096 mar 28 17:17 gopejo
drwxr-xr-x  3 invitado root    4096 mar 29 12:08 invitado
drwxrwxr-x  2 root     root    4096 abr 26 13:35 nfs
drwxr-xr-x 20 servidor servidor 4096 abr  5 12:15 servidor
root@ubuntu:/home# cd nfs
root@ubuntu:/home/nfs# mkdir alumno
root@ubuntu:/home/nfs# mkdir profesor
root@ubuntu:/home/nfs# ls
alumno profesor

```

```

cliente@cliente-VirtualBox: ~
Archivo Editar Pestañas Ayuda
GNU nano 2.5.3 Archivo: /etc/fstab

# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options>          <dump> <pass>
# / was on /dev/sda1 during installation
UUID=8da033a1-53fa-450d-a9b6-de340343ec04 /          ext4      errors=remount-ro 0      1
# swap was on /dev/sda5 during installation
UUID=08f94234-765d-428a-a9bc-f7aea5366363 none        swap      sw        0      0

192.168.1.152:/home/nfs/alumno /home/nfs/alumno nfs rw 0 0

```

6. Configuración del Cliente

Instalamos los siguientes paquetes:

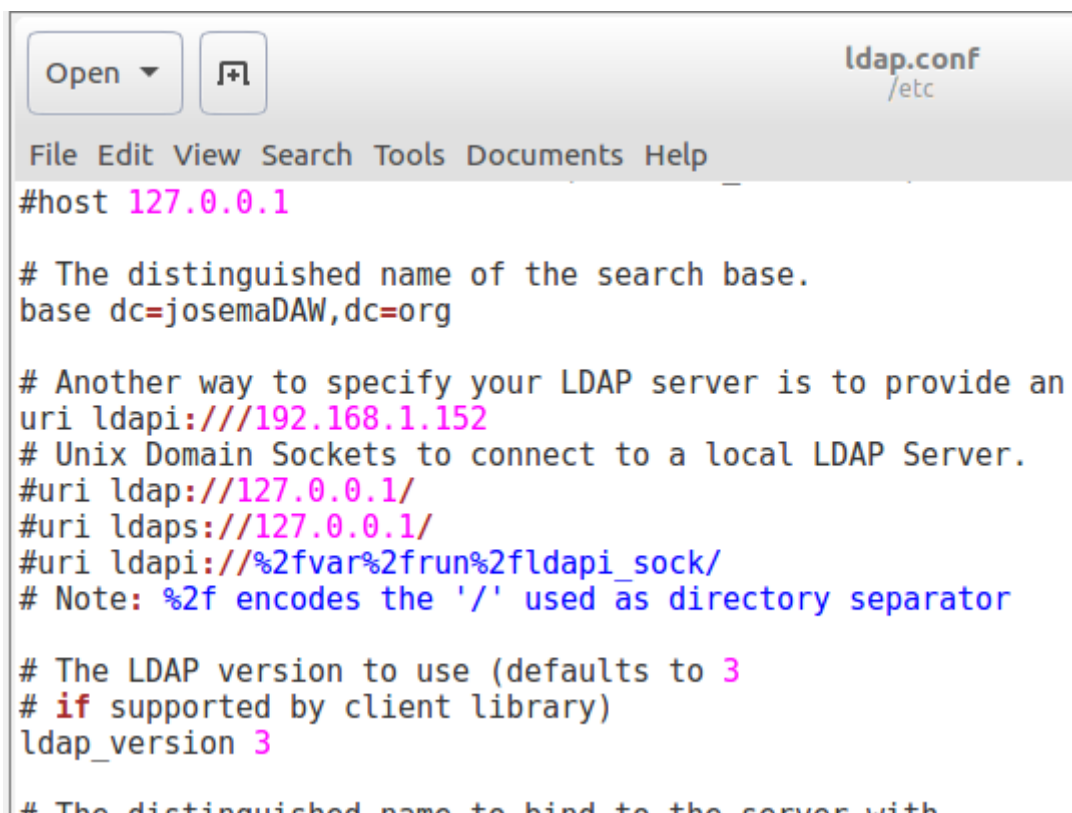
```
root@ubuntu:/home/nfs# sudo apt-get install ldap-auth-client nscd
```

```
Se instalarán los siguientes paquetes adicionales:  
auth-client-config ldap-auth-config libnss-ldap libpam-ldap  
Paquetes sugeridos:  
libpam-cracklib  
Se instalarán los siguientes paquetes NUEVOS:  
auth-client-config ldap-auth-client ldap-auth-config libnss-ldap libpam-ldap  
nscd
```

Configuramos con esta orden:

```
root@ubuntu:/home/nfs# auth-client-config -t nss -p lac_ldap
```

Al instalar los paquetes se configura el ldap, que lo refleja en este fichero:



```
Open [icon] ldap.conf /etc  
File Edit View Search Tools Documents Help  
#host 127.0.0.1  
  
# The distinguished name of the search base.  
base dc=josemaDAW,dc=org  
  
# Another way to specify your LDAP server is to provide an  
uri ldapi:///192.168.1.152  
# Unix Domain Sockets to connect to a local LDAP Server.  
#uri ldap://127.0.0.1/  
#uri ldaps://127.0.0.1/  
#uri ldapi://%2fvar%2frun%2fldapi_sock/  
# Note: %2f encodes the '/' used as directory separator  
  
# The LDAP version to use (defaults to 3  
# if supported by client library)  
ldap_version 3  
  
# The distinguished name to bind to the server with
```

Y en este fichero hay que indicar donde está nuestro servidor activo:


```
Open [icon] ldap.conf /etc/ldap
File Edit View Search Tools Documents Help
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
BASE      DC=josemaDAW,dc=org
URI        ldapi:///192.168.1.152
#BASE      dc=example,dc=com
#URI       ldan://ldan.example.com ldan://ldan-master.example.c
```

Comprobamos que tenemos los usuarios:

```
root@ubuntu:/# getent passwd alumno
alumno:x:1000:11000:alumno:/home/nfs/alumno:/bin/bash
root@ubuntu:/# getent passwd profesor
profesor:x:1001:11001:profesor:/home/nfs/profesor:/bin/bash
```

Y nos logueamos para comprobarlo:

```
root@ubuntu:/# sudo login alumno
Contraseña:
Último inicio de sesión: mié sep 21 14:35:15 CEST 2016 en tty1
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-57-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Pueden actualizarse 44 paquetes.
0 actualizaciones son de seguridad.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

alumno@ubuntu:~$ exit
logout
```

```
root@ubuntu:/# sudo login profesor
Contraseña:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-57-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Pueden actualizarse 44 paquetes.
0 actualizaciones son de seguridad.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

profesor@ubuntu:~$ exit
logout
```