

PRÁCTICA 2.2. INSTALACIÓN Y CONFIGURACIÓN SERVICIO LDAP

Duración: 2 horas + documentación (en casa)

Objetivo

Hasta ahora, nuestro sistema Linux autentificaba a los usuarios utilizando los clásicos archivos `/etc/passwd`, `/etc/group` y `/etc/shadow`. Queremos que nuestro cliente no use el sistema de autenticación local sino que autentifique los usuarios contra un servidor LDAP.

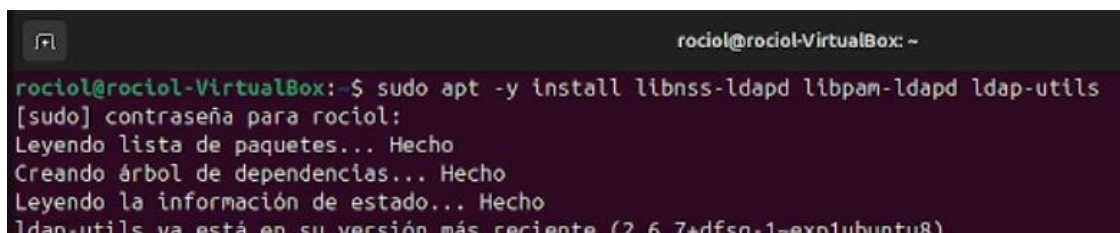
Realizarás la configuración necesaria para permitir la autenticación en el inicio de sesión conectando con el servidor LDAP.

Desarrollo:

PARTE I: Instalación y Configuración del Cliente para autenticación LDAP.

1. Instalación y configuración del Cliente LDAP

- a) **CAPTURA 1** Instala libnss-ldap y libpam-ldap:

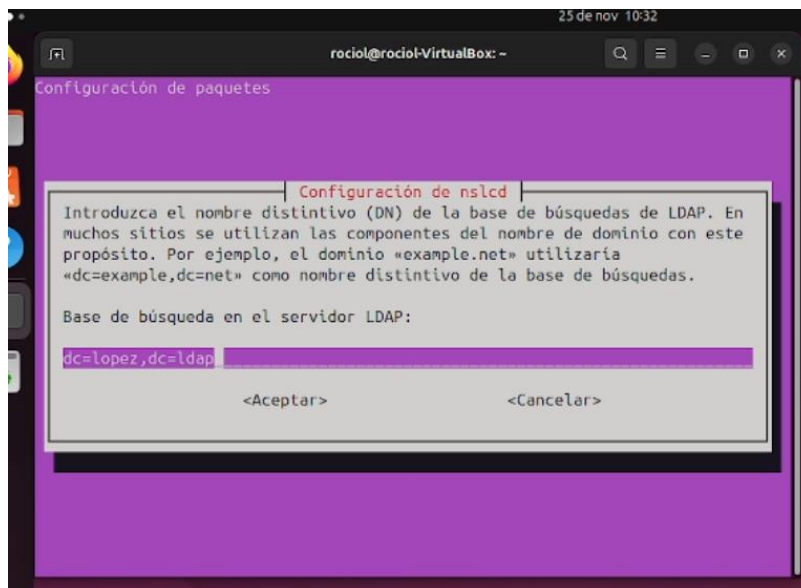
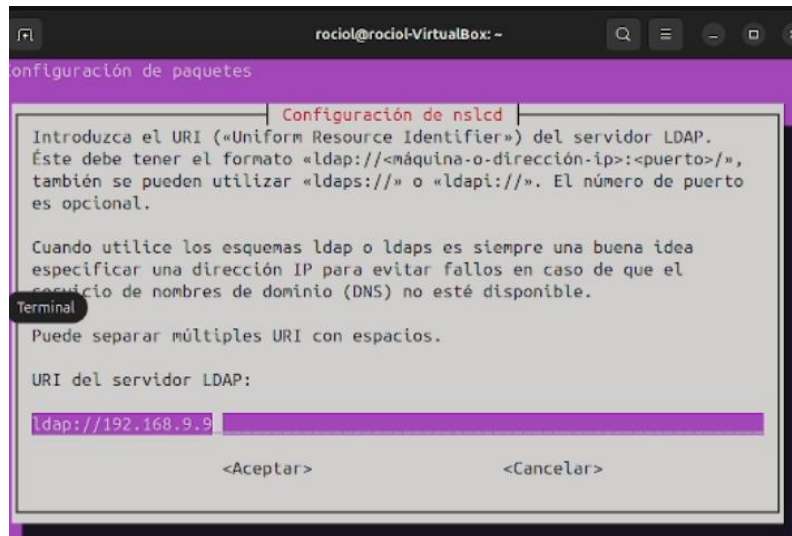


```
rociol@rociol-VirtualBox: ~  
rociol@rociol-VirtualBox:~$ sudo apt -y install libnss-ldapd libpam-ldapd ldap-utils  
[sudo] contraseña para rociol:  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
ldap-utils ya está en su versión más reciente (2.6.7-4dfsg-1-explubuntu8)
```

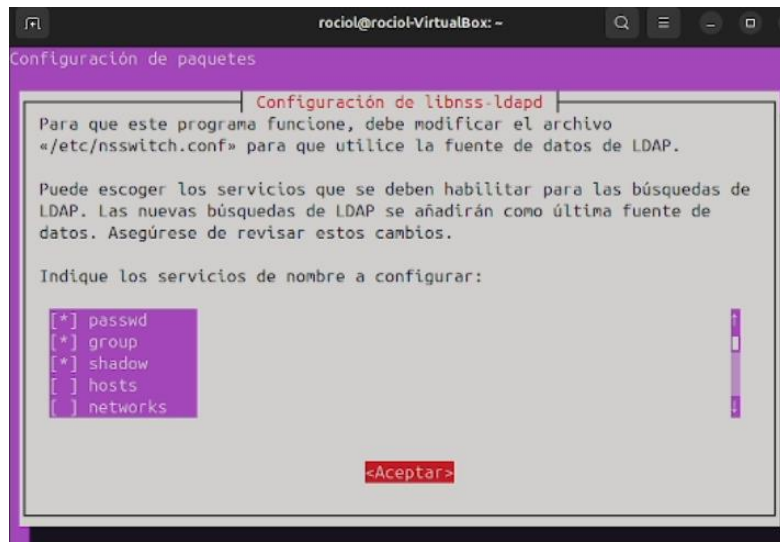
Ayuda: https://www.server-world.info/en/note?os=Ubuntu_20.04&p=openldap&f=3

En la instalación se ha instalado dependencias como **ldap-auth-config** y se configurará con el asistente: indica IP del servidor openldap, vuestro dominio (dc) y elegir versión 3 de LDAP. Resto de opciones: default.

CAPTURA 2: Captura del asistente indicando la IP del server LDAP



Para la configuración para libnss-ldapd y debes marcar lo siguiente:



- b) **CAPTURA 3** Comprueba que el archivo `/etc/nsswitch.conf` tiene la columna "ldap"
Nota: si esto ha sido configurado con el asistente, éste paso debería ya aparecer configurado.

```
rociol@rociol-VirtualBox: ~  
GNU nano 7.2 /etc/nsswitch.conf *  
# /etc/nsswitch.conf  
#  
# Example configuration of GNU Name Service Switch functionality.  
# If you have the 'glibc-doc-reference' and 'info' packages installed, try:  
# 'info libc "Name Service Switch"' for information about this file.  
  
passwd:      files systemd ldap  
group:       files systemd ldap  
shadow:      files ldap  
gshadow:     files  
  
hosts:       files mdns4_minimal [NOTFOUND=return] dns  
networks:    files  
  
protocols:   db files  
services:    db files  
ethers:       db files  
rpc:         db files  
  
netgroup:    nis
```

Saber más :

El valor que se indica en la columna corresponderá con un archivo en `/lib` que se llama `/lib/libnss_ldap.so.X` (también existe `libnss_compat.so.X` , `libnss_files.so.X` , etc)

Más información: <https://man7.org/linux/man-pages/man5/nsswitch.conf.5.html>

- c) **CAPTURA 4** Modifica la BASE y URI en `/etc/ldap.conf` y `/etc/ldap/ldap.conf`
Nota: recuerda para qué se usa cada uno (ver teoría y foro del tema).

```
rociol@rociol-VirtualBox: ~  
GNU nano 7.2 /etc/ldap/ldap.conf *  
#  
# LDAP Defaults  
#  
# See ldap.conf(5) for details  
# This file should be world readable but not world writable.  
  
BASE      dc=lopez,dc=ldap  
URI       ldap://192.168.9.9  
  
#SIZELIMIT      12  
#TIMELIMIT      15  
#DEREF          never  
  
# TLS certificates (needed for GnuTLS)  
TLS_CACERT      /etc/ssl/certs/ca-certificates.crt
```

d) **CAPTURA 5:** Comprobar con la orden **getent passwd** que se visualizan tanto los usuarios locales como los de LDAP.

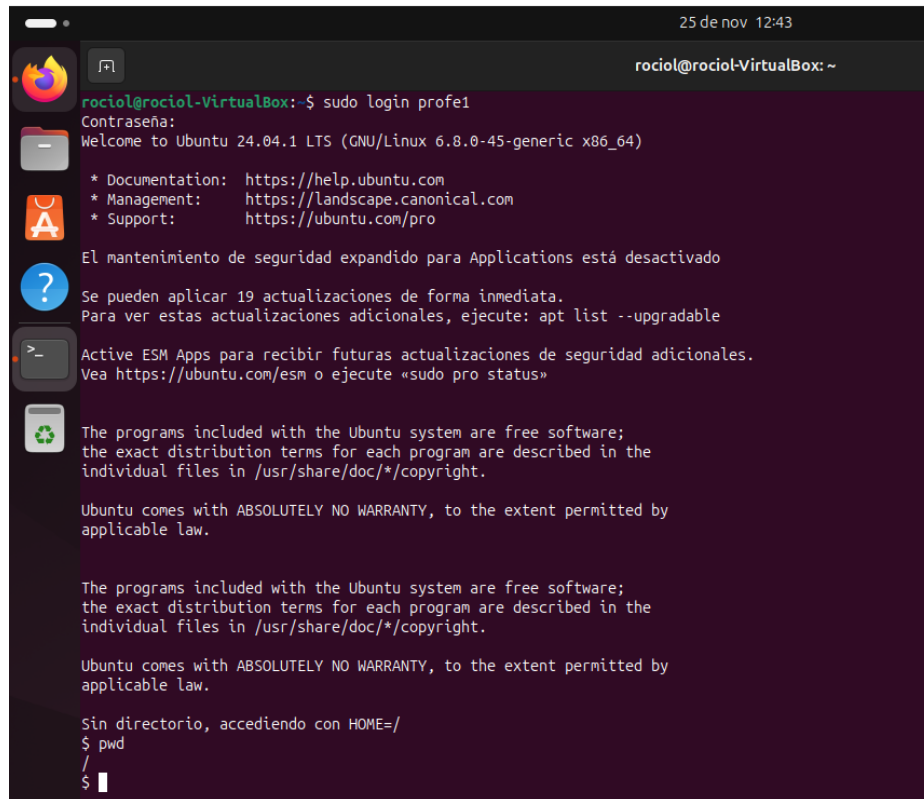
```
rociol@rociol-VirtualBox:~$ getent passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/usr/sbin/nologin
systemd-timesync:x:996:996:systemd Time Synchronization:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:181:181::/nonexistent:/usr/sbin/nologin
syslog:x:102:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:991:991:systemd Resolver:/usr/sbin/nologin
uiddd:x:103:103::/run/uiddd:/usr/sbin/nologin
usbmux:x:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
tss:x:105:105:TPM software stack,,,:/var/lib/tpm:/bin/false
systemd-oom:x:990:990:systemd Userspace OOM Killer:/usr/sbin/nologin
kernoops:x:106:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
whoopsie:x:107:109::/nonexistent:/bin/false
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
avahi:x:108:111:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
tcpdump:x:109:112::/nonexistent:/usr/sbin/nologin
sssd:x:110:113:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
cups-pk-helper:x:112:114:user for cups-pk-helper service,,,:/nonexistent:/usr/sbin/nologin
fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
saned:x:113:116::/var/lib/saned:/usr/sbin/nologin
geoclue:x:114:117::/var/lib/geoclue:/usr/sbin/nologin
cups-browsed:x:115:114::/nonexistent:/usr/sbin/nologin
hplip:x:116:7:HPLIP system user,,,:/run/hplip:/bin/false
gnome-remote-desktop:x:988:988:GNOME Remote Desktop:/var/lib/gnome-remote-desktop:/usr/sbin/nologin
polkitd:x:987:987:User for polkitd:/usr/sbin/nologin
rtkit:x:117:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:118:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup:/bin/false
gdm:x:120:121:Gnome Display Manager:/var/lib/gdm3:/bin/false
nm-openvpn:x:121:122:NetworkManager OpenVPN,,,:/var/lib/openvpn/chronot:/usr/sbin/nologin
rociol:x:1000:1000:rociol:/home/rociol:/bin/bash
nslcd:x:122:124:nslcd name service LDAP connection daemon,,,:/run/nslcd:/usr/sbin/nologin
asir1_1:x:20000:10000:Asir 1.1:/home/usuariosldap/asir1_1:
asir1_2:x:20001:10000:Asir 1.2:/home/usuariosldap/asir1_2:
asir1_3:x:20002:10000:Asir 1.3:/home/usuariosldap/asir1_3:
asir2_1:x:20003:10001:Asir 2.1:/home/usuariosldap/asir2_1:
asir2_2:x:20004:10001:Asir 2.2:/home/usuariosldap/asir2_2:
profe1:x:20005:10002:Profe 1:/home/usuariosldap/profe1:
profe2:x:20006:10002:Profe 2:/home/usuariosldap/profe2:
profe3:x:20007:10002:Profe 3:/home/usuariosldap/profe3:
rociol@rociol-VirtualBox:~$
```

CAPTURA 6: Demuestra con **\$cat /etc/passwd** que son distintos usuarios los del sistema y los de LDAP

```
rociol@rociol-VirtualBox:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/usr/sbin/nologin
systemd-timesync:x:996:996:systemd Time Synchronization:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:181:181::/nonexistent:/usr/sbin/nologin
syslog:x:102:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:991:991:systemd Resolver:/usr/sbin/nologin
uiddd:x:103:103::/run/uiddd:/usr/sbin/nologin
usbmux:x:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
tss:x:105:105:TPM software stack,,,:/var/lib/tpm:/bin/false
systemd-oom:x:990:990:systemd Userspace OOM Killer:/usr/sbin/nologin
kernoops:x:106:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
whoopsie:x:107:109::/nonexistent:/bin/false
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
avahi:x:108:111:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
tcpdump:x:109:112::/nonexistent:/usr/sbin/nologin
sssd:x:110:113:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
cups-pk-helper:x:112:114:user for cups-pk-helper service,,,:/nonexistent:/usr/sbin/nologin
fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
saned:x:113:116::/var/lib/saned:/usr/sbin/nologin
geoclue:x:114:117::/var/lib/geoclue:/usr/sbin/nologin
cups-browsed:x:115:114::/nonexistent:/usr/sbin/nologin
hplip:x:116:7:HPLIP system user,,,:/run/hplip:/bin/false
gnome-remote-desktop:x:988:988:GNOME Remote Desktop:/var/lib/gnome-remote-desktop:/usr/sbin/nologin
polkitd:x:987:987:User for polkitd:/usr/sbin/nologin
rtkit:x:117:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:118:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup:/bin/false
gdm:x:120:121:Gnome Display Manager:/var/lib/gdm3:/bin/false
nm-openvpn:x:121:122:NetworkManager OpenVPN,,,:/var/lib/openvpn/chronot:/usr/sbin/nologin
rociol:x:1000:1000:rociol:/home/rociol:/bin/bash
nslcd:x:122:124:nslcd name service LDAP connection daemon,,,:/run/nslcd:/usr/sbin/nologin
rociol@rociol-VirtualBox:~$
```

e) **CAPTURA 7**: Comprobar que se autentican los usuarios creados en LDAP. El usuario no debe existir en el sistema. Hay varias formas de probar:

- `$ sudo login usuarioldap.`



```
rociol@rociol-VirtualBox:~$ sudo login profe1
Contraseña:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-45-generic x86_64)

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

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 19 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

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.

Sin directorio, accediendo con HOME=/
$ pwd
/
$
```

f) Muestra al profesorado que funciona

Nota IMPORTANTE: por ahora solo probamos que autentica, pero su \$HOME no se va a crear pues no lo hemos preparado aún. Lo haremos en la siguiente parte (Parte II).

- Está arriba la captura

PARTE II: Directorio home de los usuarios. Compartición mediante NFS.

2. Server: instalación de NFS en el server.

a) Lee la documentación en moodle del Anexo del tema 2 sobre NFS. Instala la paquetería necesaria en el servidor : **nfs-common** y **nfs-kernel-server**

- Vamos a /etc/pam.d/common-session (Configuramos para crear el home de los usuarios al loguearse)

```
session optional      pam_mkhomedir.so skel=/etc/skel umask=077
```

- Realizamos Práctica Básica

b) Crea la carpeta compartida **para los homes de los users (tal y como indicaste en el atributo "homeDirectory" de los .ldif)** . Asigne propietarios **nobody:nogroup** y **permisos 750**.
CAPTURA 8: Muestra con slapcat/slapsearch el valor del atributo homeDirectory de los usuarios creados Y muestra también un ls -ld de la carpeta compartida en el servidor (ver permisos y propietarios).

```
dn: uid=profe2,ou=profes,ou=usuarios,dc=lopez,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: profe2
cn: Profe 2
sn: 2
uidNumber: 20006
gidNumber: 10002
homeDirectory: /home/usuariosldap/profe2
userPassword:: e1NTSEF91nZRC9HT1hTdfA0ejhhanJiejllT2luUng2c2lhK1M=
structuralObjectClass: inetOrgPerson
entryUUID: 1d7a9d44-3bb1-103f-9176-81ae08300a61
creatorsName: cn=admin,dc=lopez,dc=ldap
createTimestamp: 20241120173209Z
entryCSN: 20241120173209.759617Z#000000#000#000000
modifiersName: cn=admin,dc=lopez,dc=ldap
modifyTimestamp: 20241120173209Z
```

```
rociol@rociol:/home/usuariosldap$ ls -ld
drwxr-xr-x 2 nobody nogroup 4096 nov 25 12:56
rociol@rociol:/home/usuariosldap$ _
```

c) **CAPTURA 9:** Configuración para exportar la carpeta en el fichero adecuado y con las opciones de lectura y escritura,etc y para que todos accedan como nobody. EXPLICA las opciones seleccionadas.

```
root@rociol:~# sudo exportfs -v
/mnt/nfs_share 192.168.9.0/24(sync,wdelay,hide,no_subtree_check,sec=sys,rw,secure,root_squash,no_all_squash)
/home/usuariosldap
192.168.9.0/24(sync,wdelay,hide,no_subtree_check,sec=sys,rw,secure,root_squash,no_all_squash)
root@rociol:~#
```

- /mnt/nfs_share: Ruta del directorio a compartir.
- 192.168.1.0/24: Subred que tendrá acceso (ajusta según tu red).
- rw: Permite lectura y escritura.
- sync: Garantiza que los cambios se escriban inmediatamente en disco.
- no_subtree_check: Mejora el rendimiento al no verificar el árbol completo del directorio.
- root_squash: **Cuando un cliente accede a un recurso compartido en el servidor NFS como el usuario root, la opción root_squash hace que las solicitudes de este usuario no tengan privilegios de administrador (mapea las acciones del usuario root en el cliente al usuario nobody en el servidor) mejorando la seguridad.**

3. Cliente NFS : Instalación y Configuración de la paquetería NFS para acceder al futuro %HOME remoto.

Nota: Si faltase este atributo homeDirectory debes añadirlo al árbol ldap bien a través de phpldapadmin/lam o mediante la orden ldapmodify

a) **Instala la paquetería NFS en el cliente y configura siguiendo las indicaciones de:**

- Lo instalamos en la Práctica Básica

✓ https://www.server-world.info/en/note?os=Ubuntu_20.04&p=nfs&f=2

✓ [y la documentación sobre NFS del tema2 de moodle.](#)

Rellena esta tabla indicando la paquetería total (LDAP y NFS) instalada en el cliente:

Paquete instalado en cliente	Versión	Descripción
Libnss-ldap	ÚLTIMA	Paquetería para clientes NFS que permite acceder a recursos NFS.
Libpam-ldap	ÚLTIMA	Herramientas para gestionar y consultar servidores LDAP
Ldap-utils	ÚLTIMA	Integración de NSS con autenticación LDAP.
Nfs-common	ÚLTIMA	Integración de PAM para autenticación con LDAP.

b) **Prueba a acceder y crear archivos desde un usuario del cliente al recurso compartido.**
CAPTURA10 y explica los propietarios de los nuevos archivos.

c) **Prueba a acceder desde un usuario root del cliente.**
CAPTURA11 y explica los propietarios de los nuevos archivos

d) ¿Podrías cambiar la configuración del /etc/export y usar "anongid" para que funcione según la configuración de UIDs y GUIDs que has preparado en los .ldif? Explica claramente cómo lo harías. Haz una prueba .

4. Cliente LDAP: Instalación y configuración de LDAP para permitir la creación de un home remoto (en el server) y acceso al mismo al iniciar sesión.

a) Configurar para que se cree el home del usuario cuando autentique contra LDAP:
/etc/pam.d/common-session:

```
session optional      pam_mkhomedir.so skel=/etc/skel umask=077
```

Explica lo que significa cada directiva de la línea anterior.

b) Crea el directorio de montaje en el cliente donde se montará el directorio /home/nfs del servidor en /home/usuariosldap del cliente.

CAPTURA 12: Muestra propietarios y permisos del punto de montaje.

c) Móntalo mano (con mount) para probar que hay acceso.

CAPTURA 13: Muestra propietarios y permisos una vez montado.

d) **CAPTURA 14** Una vez comprobado, móntalo automáticamente en el arranque del sistema (fstab)

e) **CAPTURA 15** Comprobar que se crea el home del usuario logueado.

f) **CAPTURA 16** Comprobar que el usuario (ej. Profe1ESO) puede escribir en su home pero no en el de otro (alumno1ESO).

g) Si tienes más de un cliente, comprobar que se puede acceder al mismo usuario desde distintas máquinas.