

PRÁCTICA 2.2. INSTALACIÓN Y CONFIGURACIÓN SERVICIO LDAP

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

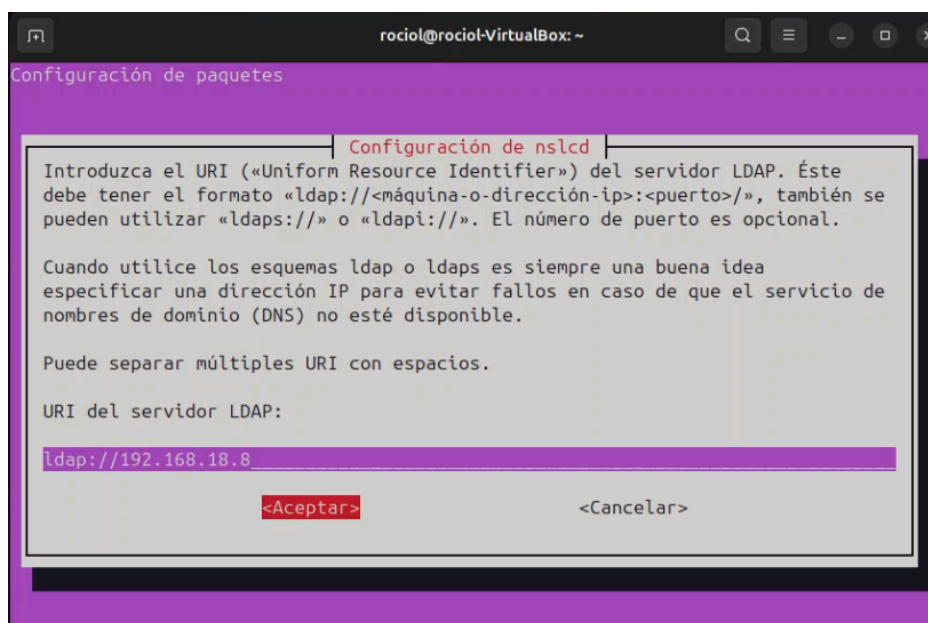
a) **CAPTURA 1** Instala `libnss-ldap` y `libpam-ldap`:

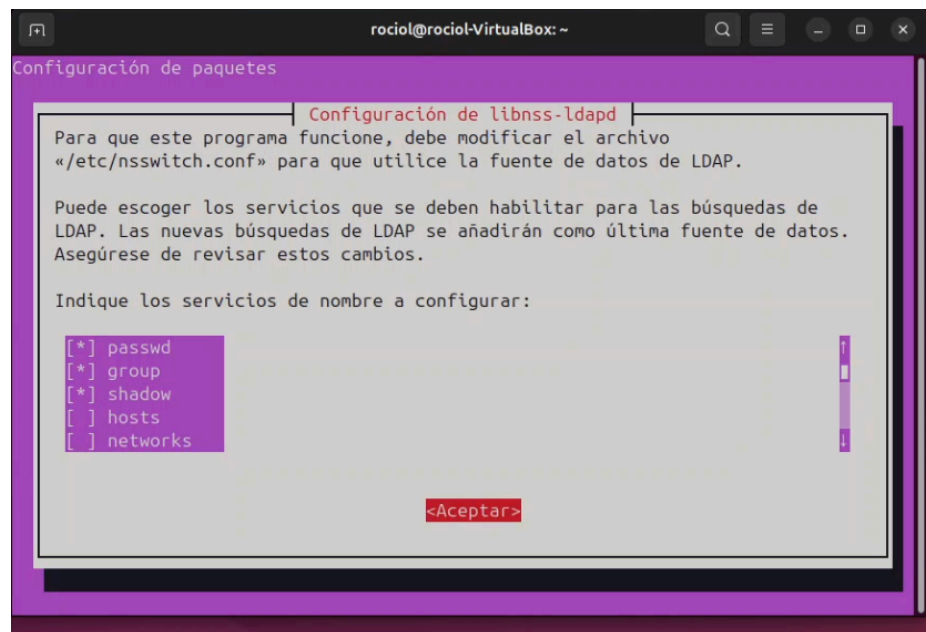
```
rociol@rociol-VirtualBox:~$ sudo apt -y install libnss-ldapd libpam-ldapd ldap-utils
[sudo] contraseña para rociol:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... 50%
```

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

En la instalación se han 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





- 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.

```
GNU nano 7.2 /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
```

- 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=pozo,dc=ldap
URI      ldap://192.168.18.8

#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.

```

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/chroot:/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
_rpc:x:123:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:124:65534::/var/lib/nfs:/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:~$ getent passwd

```

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

```
GNU nano 7.2 /etc/passwd
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/chroot:/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
_rpc:x:123:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:124:65534::/var/lib/nfs:/usr/sbin/nologin
```

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:

- `$ pamtest login userdeldap` (Nota: quizás necesites instalar paquetería para esta utilidad)
- `$ sudo login usuarioldap`.
- Abrir nuevas terminales (`Ctrl+Alt+Fx`) y loguear allí.
- `$ finger usuarioldap`

```
rociol@rociol-VirtualBox:~$ sudo login asir1_1
Contraseña: 
```

```
rociol@rociol-VirtualBox: ~
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
/
$
```

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

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.

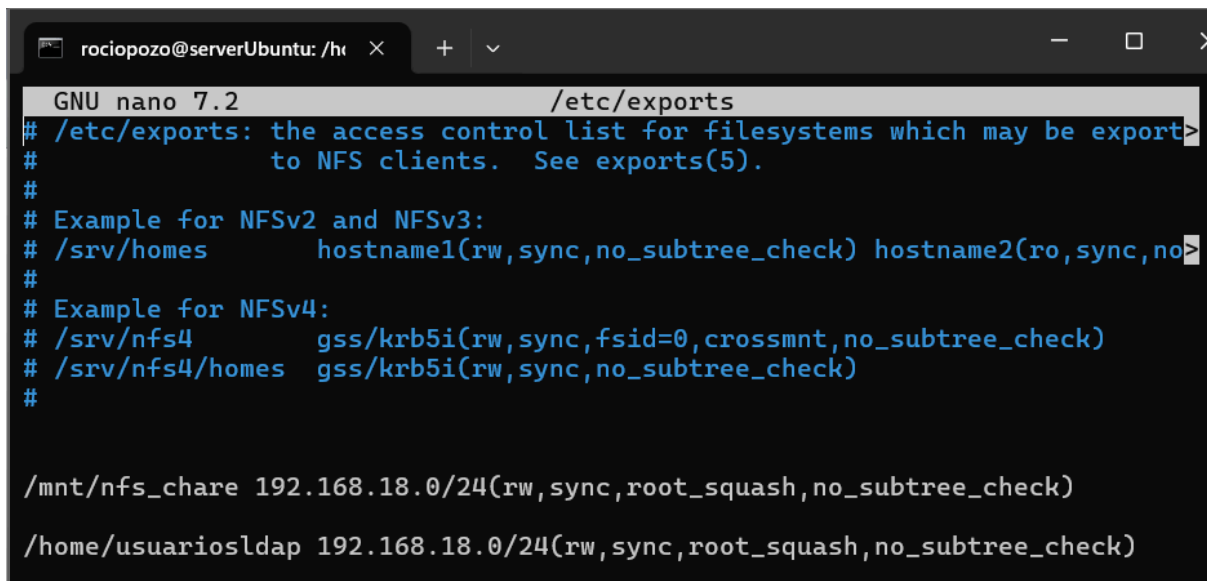
CAPTURA 8: Muestra con slapcat/slapsearch el valor del atributo homeDirectory de los usuarios creados Y muestra también un ls -ld de la carpeta compartida en el servidor (ver permisos y propietarios).

```
dn: uid=asir1_1,ou=alumnos,ou=usuarios,dc=pozo,dc=ldap
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: asir1_1
cn: Asir 1.1
sn: 1.1
uidNumber: 20000
gidNumber: 10000
homeDirectory: /home/usuariosldap/asir1_1
userPassword:: e1NTSEF9WGdoMzhRYWNBU2xudUJVdXRddjJWcHl3N1QyeEJxVy8=
structuralObjectClass: inetOrgPerson
entryUUID: 645bb8c8-34d7-103f-904a-51c9ad0a625d
creatorsName: cn=admin,dc=pozo,dc=ldap
createTimestamp: 20241112001831Z
entryCSN: 20241112001831.411692Z#000000#000#000000
modifiersName: cn=admin,dc=pozo,dc=ldap
modifyTimestamp: 20241112001831Z
```

```
rociopozo@serverUbuntu:/home$ sudo slapcat | grep homeDirectory
homeDirectory: /home/usuariosldap/asir1_1
homeDirectory: /home/usuariosldap/asir1_2
homeDirectory: /home/usuariosldap/asir1_3
homeDirectory: /home/usuariosldap/asir2_1
homeDirectory: /home/usuariosldap/asir2_2
homeDirectory: /home/usuariosldap/profe1
homeDirectory: /home/usuariosldap/profe2
homeDirectory: /home/usuariosldap/profe3
rociopozo@serverUbuntu:/home$ ls -ld /home/usuariosldap
```

```
rociopozo@serverUbuntu:/home$ ls -ld /home/usuariosldap
drwxr-x--- 3 nobody nogroup 4096 nov 25 13:32 /home/usuariosldap
rociopozo@serverUbuntu:/home$
```

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 en /etc/exports



```
rociopozo@serverUbuntu: /h...
GNU nano 7.2 /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no
#
# 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)
#
/mnt/nfs_chare 192.168.18.0/24(rw,sync,root_squash,no_subtree_check)
/home/usuariosldap 192.168.18.0/24(rw,sync,root_squash,no_subtree_check)
```

- **192.168.18.0/24**
Esto indica que el acceso al recurso está permitido para todas las máquinas dentro de nuestra subred.
- **rw**
Permite que los clientes monten el recurso en modo de lectura y escritura.
- **sync**
Garantiza que los cambios realizados por el cliente se escriban inmediatamente en el disco del servidor.
- **root_squash**
Mapea al usuario root en el cliente al usuario anónimo (nobody) en el servidor.
- **no_subtree_check**
Desactiva la verificación de subárbol. Es útil si los clientes acceden frecuentemente a grandes directorios.

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:

- ✓ 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	0.9.12	Cliente NSS para autenticación LDAP.
libpam-ldap	0.9.12	Autenticación PAM para LDAP.
ldap-utils	2.6.7	Herramientas de línea de comandos LDAP.
nfs-common	1:2.6.4	Cliente NFS para montajes remotos.

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) OPCIONAL ¿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. Éste servirá para montar el directorio /home/usuariosldap del servidor. Dale permisos y propietarios adecuado.

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) DESDE EL CLIENTE, hacer login con un usuario ldap. Comprobar que se crea el home del usuario logueado. **CAPTURA 14** debe incluir, como se muestra en la imagen :

- Ejecutar pwd Captura en el cliente una vez logueado mostrando pwd.
- Captura mostrando el directorio en el servidor (ls -ld /home/usuariosldap/XXXX) en la que se vea que el propietario de la carpeta es el propio usuario (ver uidnumber)

```
mctr@ubuntu22:/home/usuariosldap$ sudo ls -l
total 8
drwx----- 2 1051 1051 4096 Nov 25 14:12 daw1_1
drwx----- 2 1100 1100 4096 Nov 25 14:13 profe_mctr
-rw-r--r-- 1 root root   0 Nov 25 08:42 prueba.txt
```

Individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.
Last login: lun nov 25 14:13:00 UTC 2024 on tty1
Creating directory '/home/usuariosldap/profe_mctr'.
\$ pwd
/home/usuariosldap/profe_mctr
\$

e) **CAPTURA 15** Una vez comprobado, móntalo automáticamente en el arranque del sistema (/etc/fstab) . Vuelve a comprobar que se crea el home del usuario logueado.

192.168.1.X:/mnt/nfs_share /mnt/nfs_client nfs defaults 0 0

Nota 1: para coger los cambios en el archivo, ejecutar:

mount -a

Nota 2: no olvides desmontarlo antes

umount PUNTO-MONTAJE)

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.