

EJERCICIOS DE LDAP II

1. Una vez instalado el servidor del ejercicio I, instala un nuevo cliente Ubuntu Desktop y sigue las instrucciones vistas en teoría para configurarlo atacando al servidor LDAP.

Ejecutaremos el siguiente comando:

```
fmol107@machine103:~$ sudo apt-get install libnss-ldap libpam-ldap ldap-utils -y
```

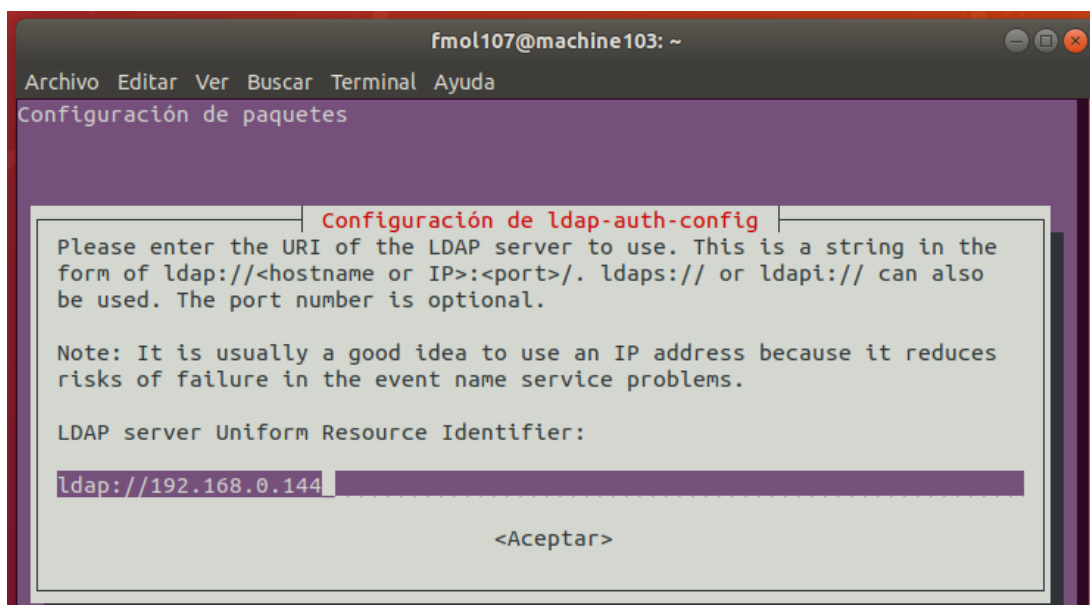
Empezaremos a configurar donde vamos a atacar para loguearnos.

libnss-ldap permitirá que NSS obtenga de LDAP información administrativa de los usuarios.

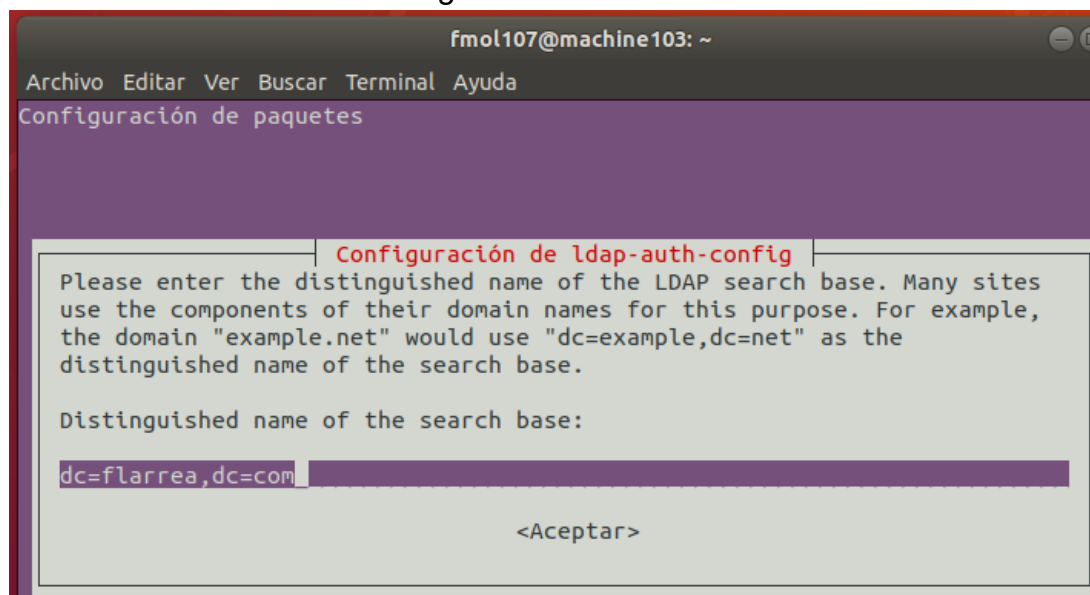
libpam-ldap facilitará la autenticación con LDAP a los usuarios que utilicen PAM.

Ldap-utils facilita la interacción con LDAP desde cualquier máquina de la red.

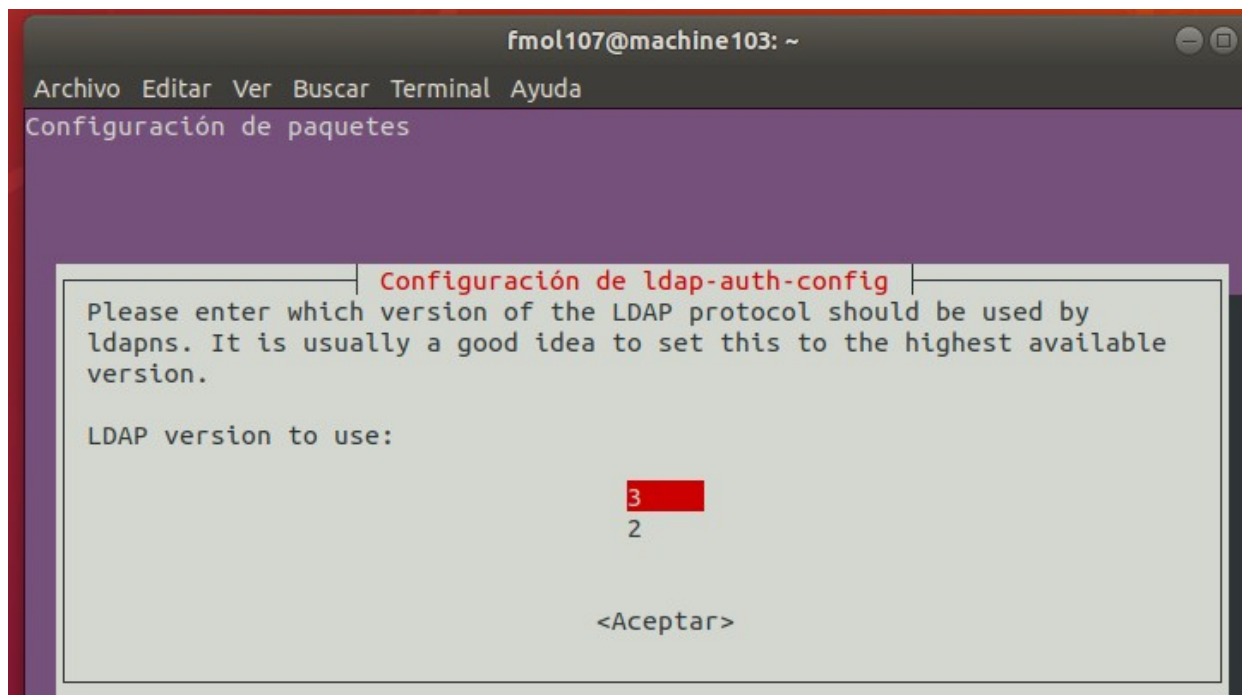
La sintaxis es > ldap://192.168.0.???



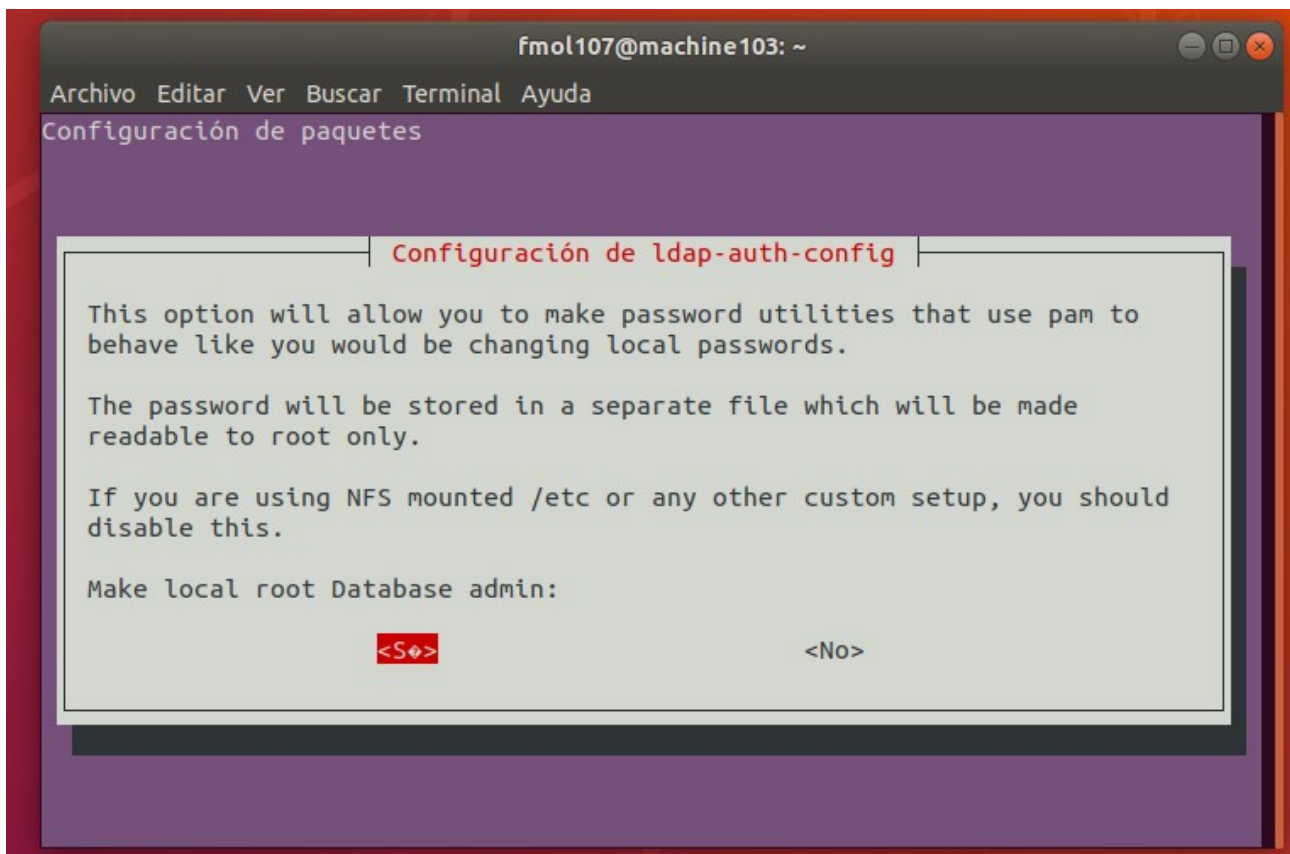
Deberemos indicar el nombre global único:



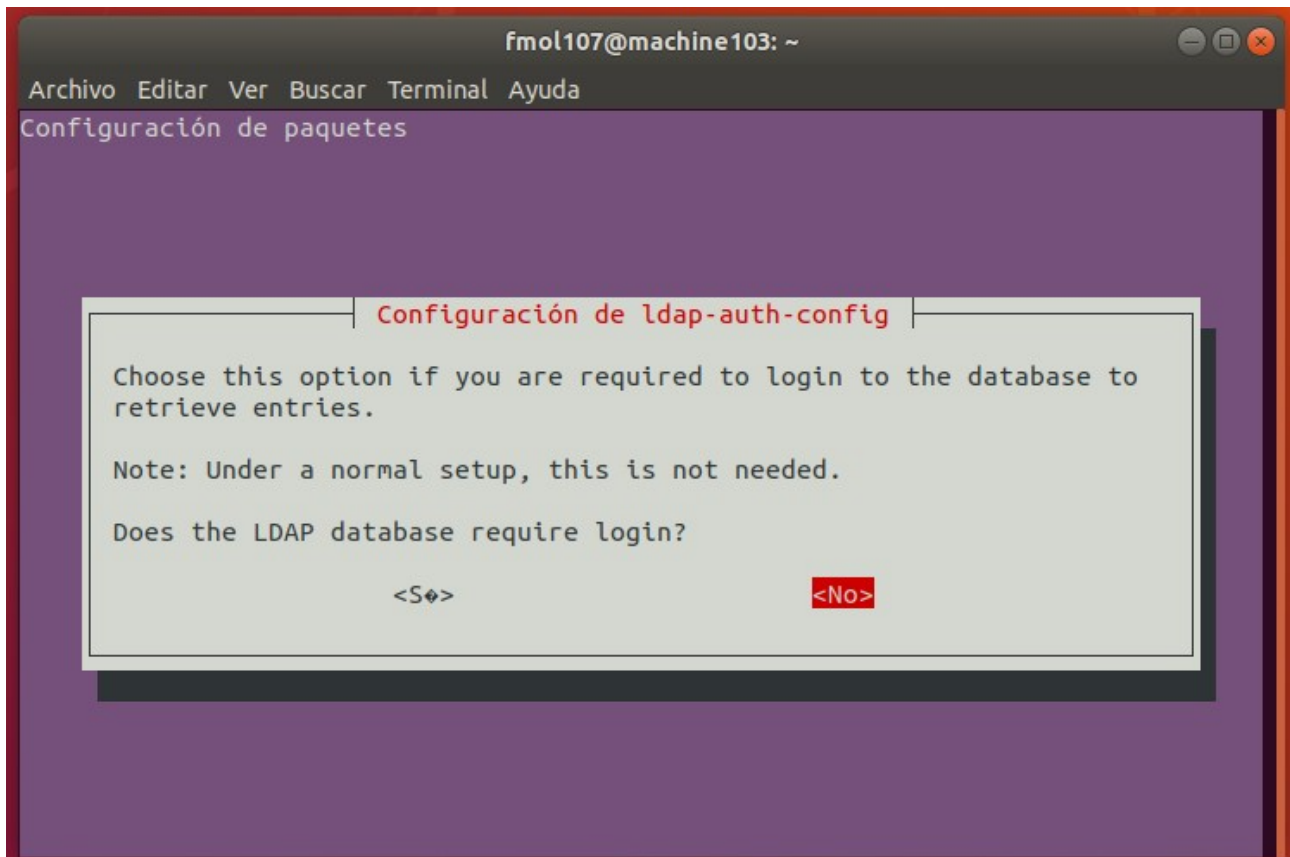
Usaremos LDAP versión 3.



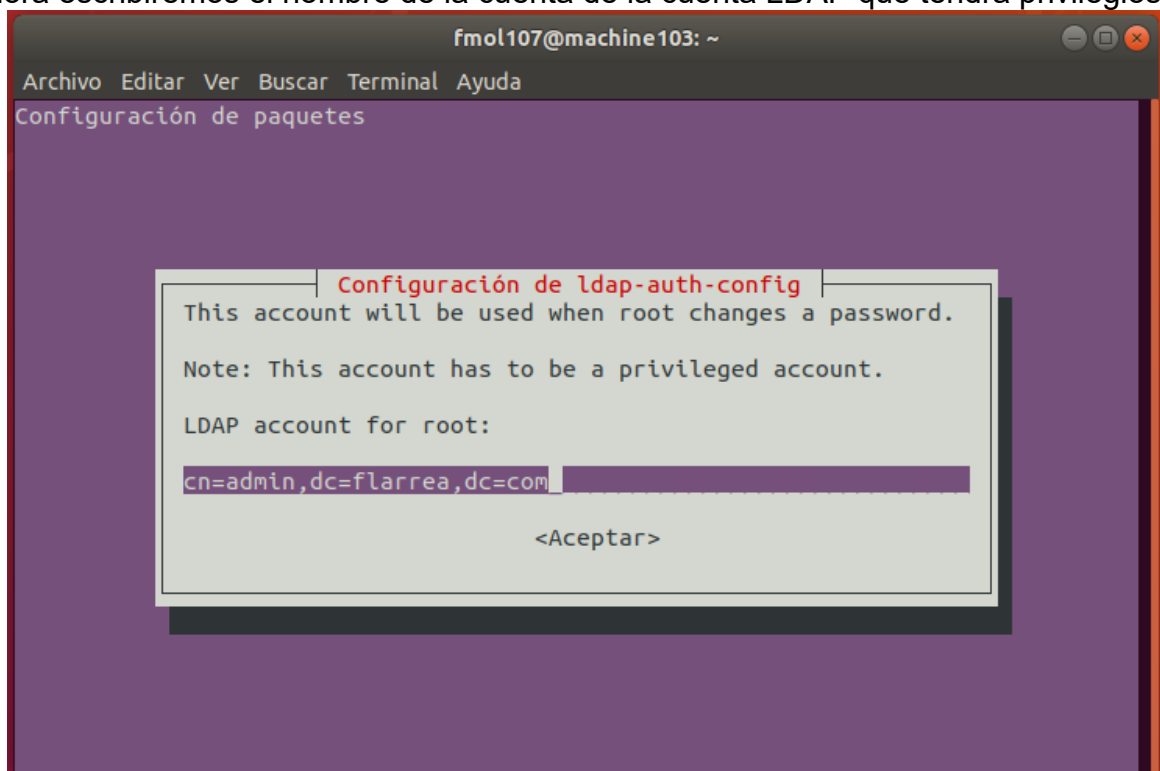
Elegimos la opción Sí y continuamos.



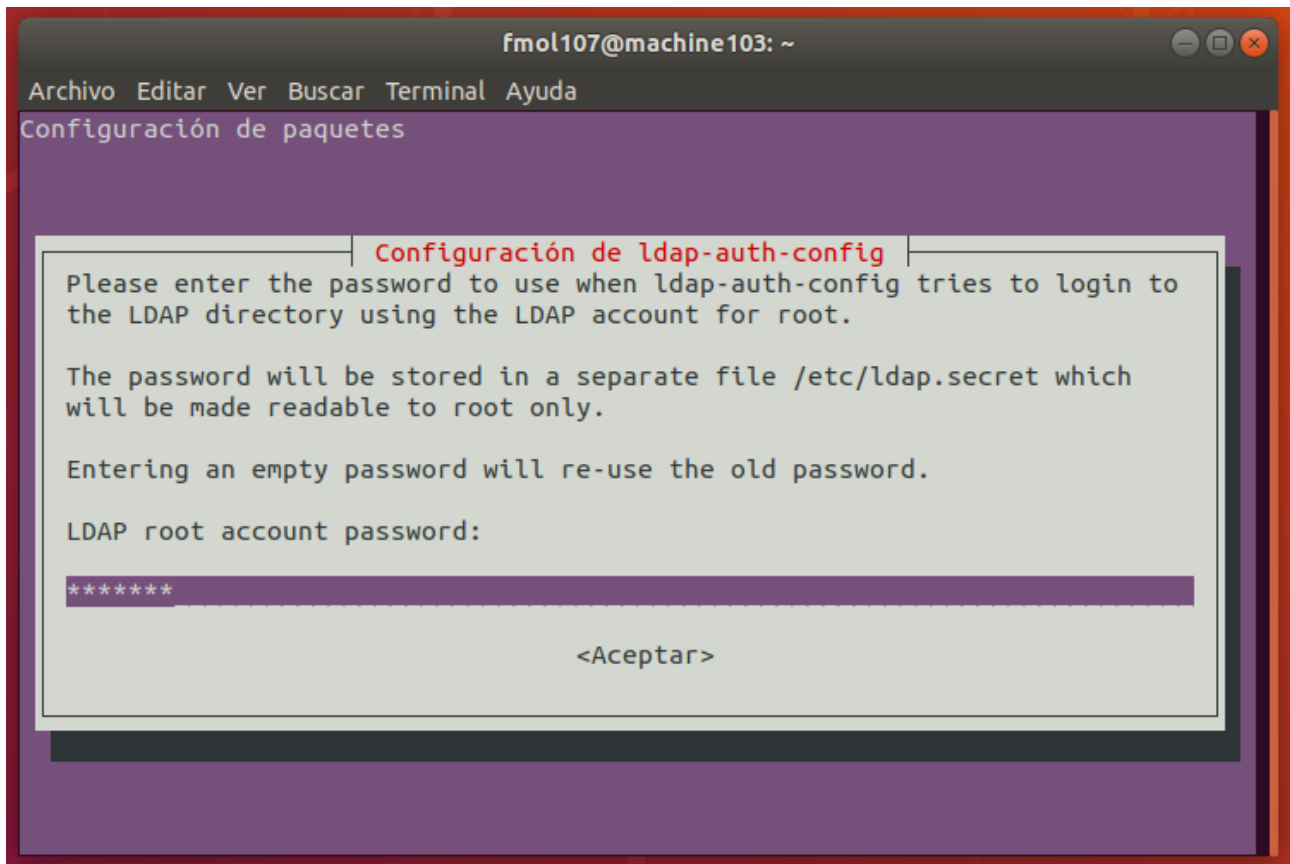
El sistema nos pregunta si queremos que sea necesario identificarse para realizar consultas en la base de datos de LDAP. Marcamos “No” y seguimos con la configuración.



Ahora escribiremos el nombre de la cuenta de la cuenta LDAP que tendrá privilegios.



Nos pedirá una contraseña que usará la cuenta con privilegios.



Después de esto habremos terminado la configuración básica del cliente LDAP.

Para terminar la configuración deberemos editar algunos parámetros en los archivos de configuración del cliente.

Debemos editar tres específicamente:

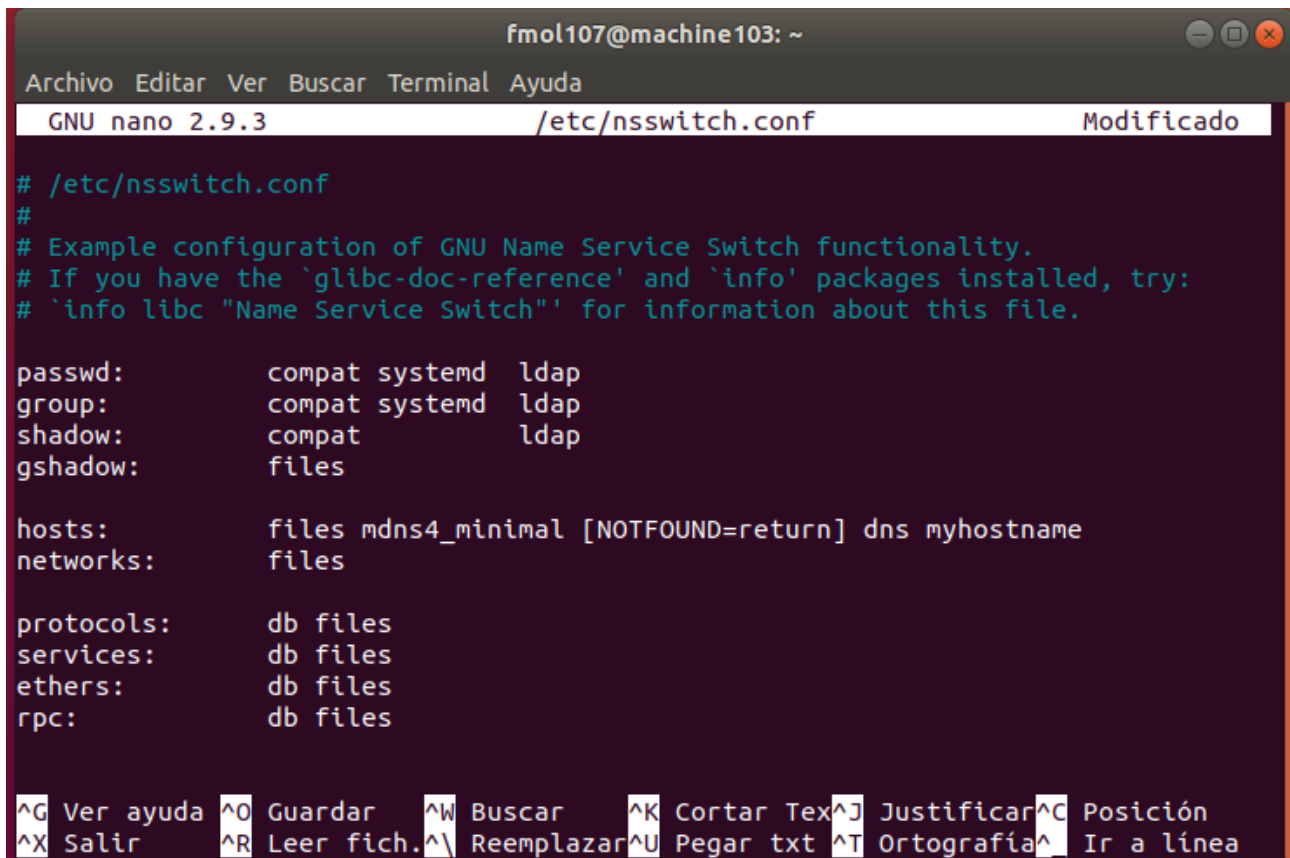
- /etc/nsswitch.conf
- /etc/pam.d/common-password
- /etc/pam.d/common-session

Abriremos el fichero /etc/nsswitch.conf con derechos de superusuario.

- sudo nano /etc/nsswitch.conf

Y añadiremos "ldap" a las líneas que empiezan por "passwd", "group" y "shadow".

Debería quedar algo así:



```
fmol107@machine103: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.9.3 /etc/nsswitch.conf Modificado

# /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:      compat systemd ldap
group:       compat systemd ldap
shadow:      compat      ldap
gshadow:     files

hosts:       files mdns4_minimal [NOTFOUND=return] dns myhostname
networks:    files

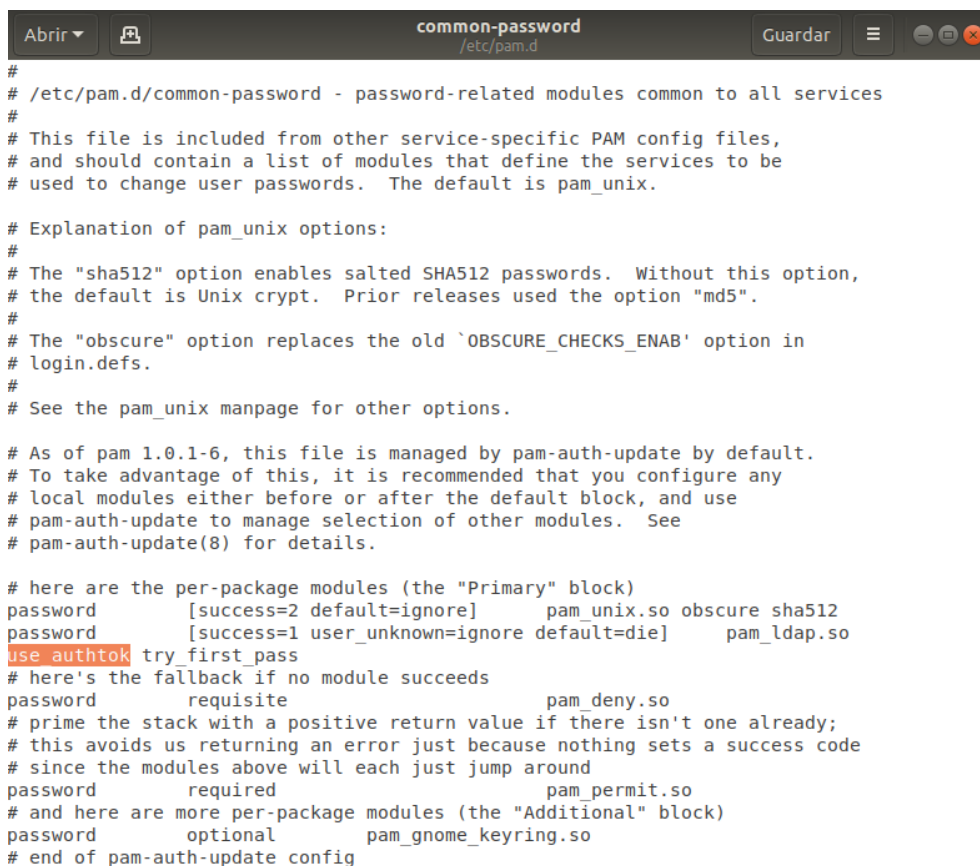
protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Text ^J Justificar ^C Posición
^X Salir    ^R Leer fich. ^L Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea
```

Ahora editaremos el siguiente archivo.

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

Eliminaremos de la línea 26 la opción “use_authtok”



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

#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.

# Explanation of pam_unix options:
#
# The "sha512" option enables salted SHA512 passwords. Without this option,
# 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.

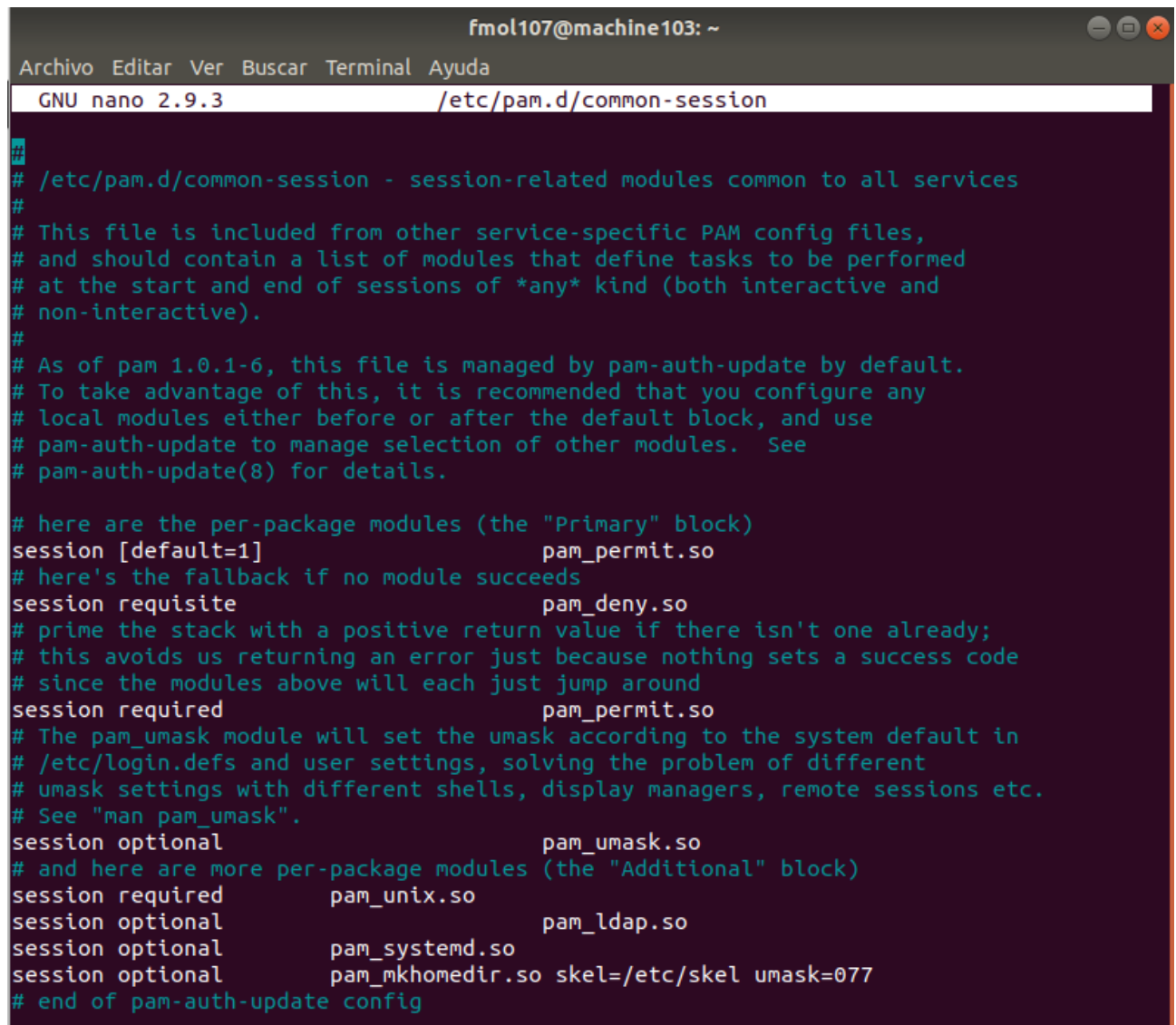
# here are the per-package modules (the "Primary" block)
password      [success=2 default=ignore]      pam_unix.so obscure sha512
password      [success=1 user_unknown=ignore default=die]      pam_ldap.so
use_authtok try_first_pass
# here's the fallback if no module succeeds
password      requisite                        pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password      required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
password      optional                        pam_gnome_keyring.so
# end of pam-auth-update config
```

Por ultimo modificaremos el archivo `/etc/pam.d/common-session`.

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

Añadiremos al final del archivo la siguiente linea:

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



```
fmol107@machine103: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.9.3 /etc/pam.d/common-session
##
# /etc/pam.d/common-session - session-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be performed
# at the start and end of sessions of *any* kind (both interactive and
# non-interactive).
#
# 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)
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
# The pam_umask module will set the umask according to the system default in
# /etc/login.defs and user settings, solving the problem of different
# umask settings with different shells, display managers, remote sessions etc.
# See "man pam_umask".
session optional pam_umask.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
session optional pam_mkhomedir.so skel=/etc/skel umask=077
# end of pam-auth-update config
```

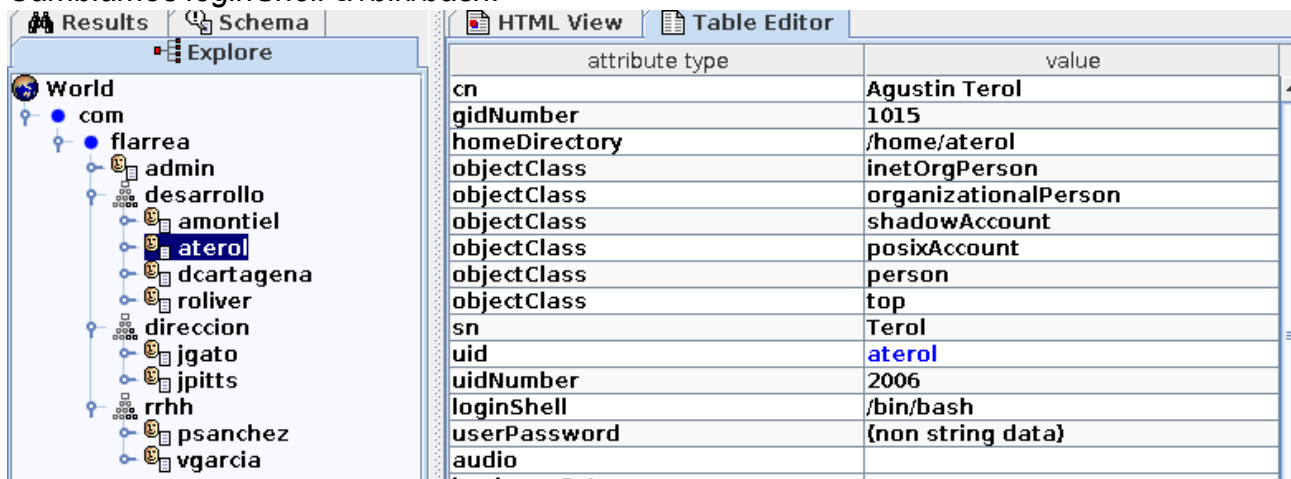
2. Realiza login en la máquina cliente instalada con alguno de los usuarios creados en el servidor LDAP y confirma que puedes entrar y que se crea la carpeta `/home/<login>`.

Al realizar login se crea el directorio `/home/aterol` para el usuario *aterol*.

```
fmo1107@machine103:~$ su - aterol
Contraseña:
Creando directorio «/home/aterol».
$
```

3. Cambia el shell con el que esos usuarios iniciarán la sesión. Para ello, debes configurarlo para cada usuario en el servidor LDAP, estableciendo la propiedad `loginShell` del usuario a `/bin/bash`. Recuerda que tras realizar los cambios, debes salir de Jxplorer y reiniciar el servidor con el comando que vimos en teoría.

Cambiamos loginShell a /bin/bash.



attribute type	value
cn	Agustin Terol
gidNumber	1015
homeDirectory	/home/aterol
objectClass	inetOrgPerson
objectClass	organizationalPerson
objectClass	shadowAccount
objectClass	posixAccount
objectClass	person
objectClass	top
sn	Terol
uid	aterol
uidNumber	2006
loginShell	/bin/bash
userPassword	{non string data}
audio	

Salimos del jxplorer y reiniciamos el servidor con el comando:

- `sudo jxplorer restart`


```
fmo1@machine103:~$ sudo jxplorer restart
oct. 31, 2019 1:53:43 P. M. com.ca.directory.jxplorer.JXplorer printTime
INFORMACIÓN: main start
TIME: Thu Oct 31 13:53:43 CET 2019 (673)

oct. 31, 2019 1:53:43 P. M. com.ca.directory.jxplorer.JXplorer checkJavaEnvironm
ent
INFORMACIÓN: running java from: /usr/lib/jvm/java-11-openjdk-amd64
oct. 31, 2019 1:53:43 P. M. com.ca.directory.jxplorer.JXplorer checkJavaEnvironm
ent
INFORMACIÓN: running java version 11.0.4
BATCH MODE USAGE
Currently only the -report option is supported for JXWorkBench batch reporting.
(For more information try -report -help
oct. 31, 2019 1:53:43 P. M. com.ca.directory.jxplorer.JXplorer printTime
INFORMACIÓN: main end
TIME: Thu Oct 31 13:53:43 CET 2019 (730)
```

4. Comprueba que al hacer login con los usuarios modificados, ya accedes con el shell correcto. Si te aparece algún error (como errores con el grupo del usuario, por ejemplo), intenta corregirlo realizando las acciones que consideres pertinentes en el servidor.

Cuando hago login, sale el shell que hemos configurado, pero da error.

```
fmo107@machine103:~$ su - aterol
Contraseña:
groups: no se puede encontrar el nombre para el grupo con ID 1015
aterol@machine103:~$ pwd
/home/aterol
aterol@machine103:~$
```

Para solucionarlo creamos un grupo desde el jxplorer con el GID del usuario *aterol*.

The screenshot shows the JXplorer - admin web interface. On the left, a tree view under 'World' shows a hierarchy: 'com' -> 'flarrea' -> 'admin' -> 'desarrollo' -> 'desarrollogroup' (highlighted). The main panel shows a 'Table Editor' with a table of LDAP attributes and their values.

attribute type	value
cn	desarrollogroup
gidNumber	1015
objectClass	posixGroup
objectClass	top
description	
memberUid	
userPassword	

Después de guardar los cambios y reiniciar el servidor se eliminó el error.


```
fmol107@machine103:~$ su - aterol
Contraseña:
aterol@machine103:~$ ls
examples.desktop
aterol@machine103:~$ pwd
/home/aterol
aterol@machine103:~$ █
```

Documenta los pasos realizados indicando los comandos utilizados y capturando las pantallas que consideres oportunas.