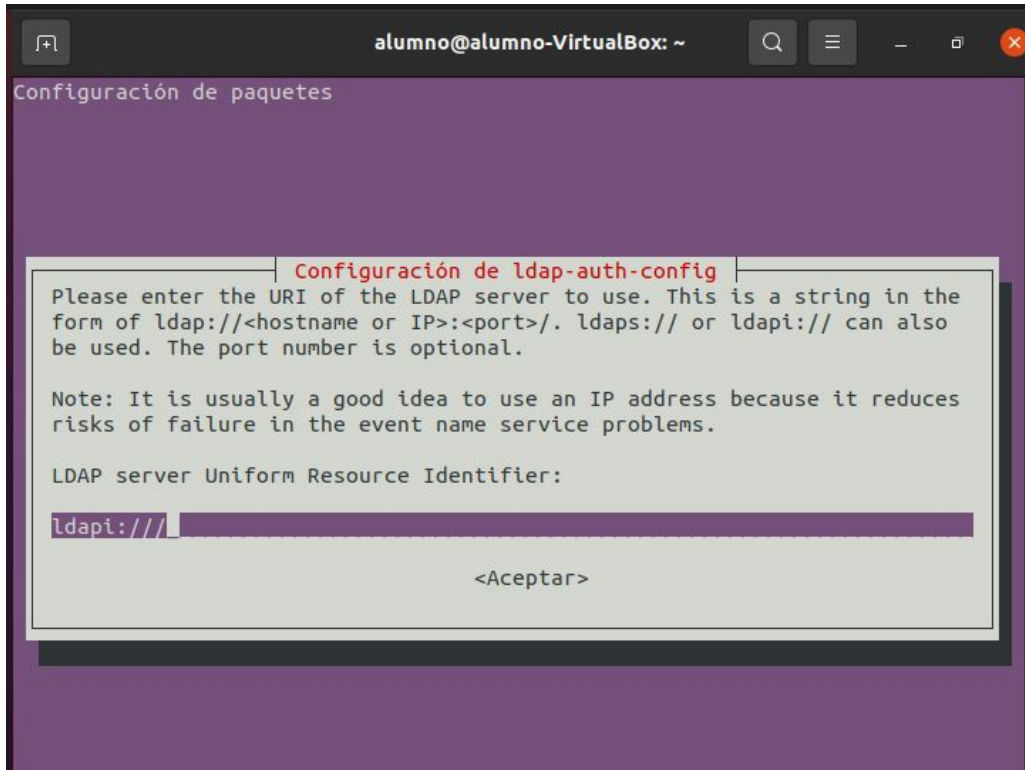


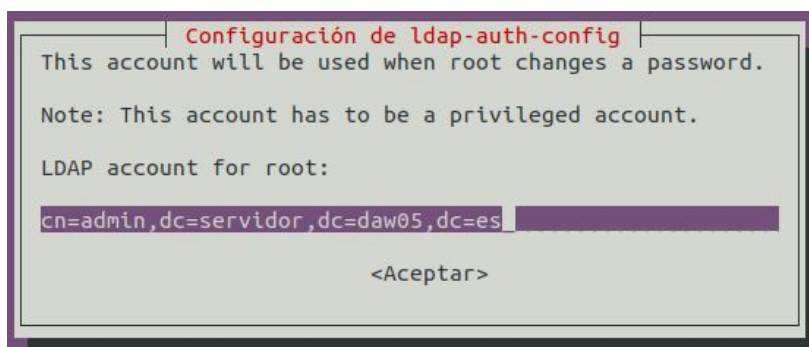
LDAP Cliente en Sistema operativo

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



Y comienza la configuración de la autenticación mediante LDAP.

- Lo primero es decirle dónde está el servidor LDAP.
 - Nosotrosle decimos que en nuestro ordenador: 127.0.0.1
- Nodo raíz:
 - dc=servidor,dc=daw05,dc=es
- Versión: 3
- Make local root database admin: Sí
- Does the LDAP database require login? No
- Cuenta del administrador LDAP:
 - cn=admin,dc=servidor,dc=daw05,dc=es



- Contraseña

Esto ha preparado el sistema operativo para enlazar con la autenticación de LDAP. Pero hay que añadir más cosas.

Editar el archivo `/etc/nsswitch.conf`

`sudo gedit /etc/nsswitch.conf`

Este es un archivo donde se indica donde nos vamos a poder autenticar. Añadimos ldap para passwd, group y shadow:



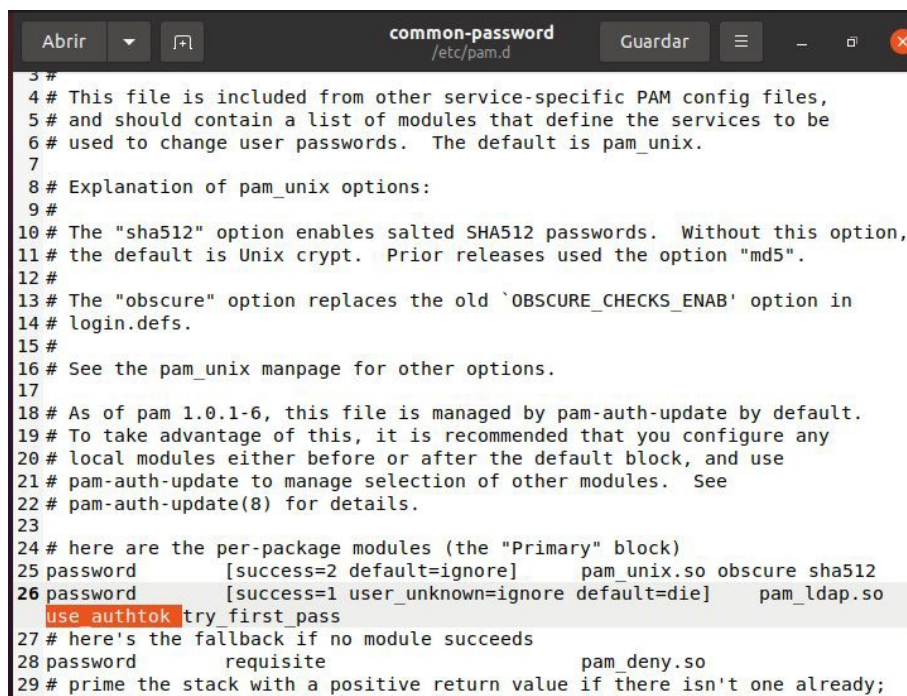
```
1 # /etc/nsswitch.conf
2 #
3 # Example configuration of GNU Name Service Switch functionality.
4 # If you have the 'glibc-doc-reference' and 'info' packages installed, try:
5 # 'info libc "Name Service Switch"' for information about this file.
6
7 passwd:    files systemd ldap
8 group:     files systemd ldap
9 shadow:    files ldap
10 gshadow:   files
11
12 hosts:     files mdns4_minimal [NOTFOUND=return] dns
13 networks:  files
14
15 protocols: db files
16 services: db files
17 ethers:    db files
18 rpc:       db files
19
20 netgroup:  nis
```

Editar el archivo `/etc/pam.d/common-password`

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

Vamos a decirle con esto qué aplicaciones pueden autenticarse mediante los métodos que tiene el sistema operativo de autenticación.

En la línea 26 quitamos **`use_authok`**



```
3 #
4 # This file is included from other service-specific PAM config files,
5 # and should contain a list of modules that define the services to be
6 # used to change user passwords. The default is pam_unix.
7
8 # Explanation of pam_unix options:
9 #
10 # The "sha512" option enables salted SHA512 passwords. Without this option,
11 # the default is Unix crypt. Prior releases used the option "md5".
12 #
13 # The "obscure" option replaces the old 'OBSCURE_CHECKS_ENAB' option in
14 # login.defs.
15 #
16 # See the pam_unix manpage for other options.
17
18 # As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
19 # To take advantage of this, it is recommended that you configure any
20 # local modules either before or after the default block, and use
21 # pam-auth-update to manage selection of other modules. See
22 # pam-auth-update(8) for details.
23
24 # here are the per-package modules (the "Primary" block)
25 password [success=2 default=ignore] pam_unix.so obscure sha512
26 password [success=1 user_unknown=ignore default=die] pam_ldap.so
27 use authtok try_first_pass
28 # here's the fallback if no module succeeds
28 password requisite pam_deny.so
29 # prime the stack with a positive return value if there isn't one already;
```

Editar el archive /etc/pam.d/common-session

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

Y añadimos al final la línea:

```
session optional pam_mkhomedir.so skel=/etc/skel umask=022
```

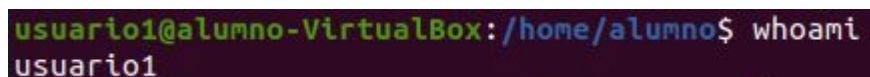
Y ya lo tenemos hecho. Vamos a comprobar que podemos autenticarnos mediante los usuarios del OpenLDAP.

```
su usuario1
```

me pide contraseña. Si pruebo a poner otro nombre, no funciona.

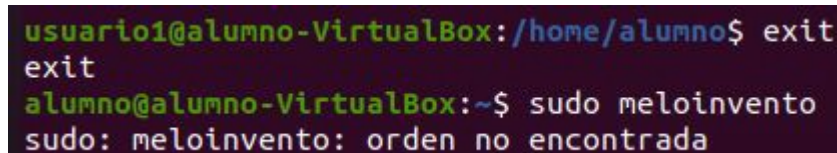
Para ver el usuario con el que estamos autenticados en este momento es:

```
whoami
```



```
usuario1@alumno-VirtualBox:/home/alumno$ whoami
usuario1
```

salgo con exit y repito whoami, dice que soy el usuario.



```
usuario1@alumno-VirtualBox:/home/alumno$ exit
exit
alumno@alumno-VirtualBox:~$ sudo meloinvento
sudo: meloinvento: orden no encontrada
alumno@alumno-VirtualBox:~$
```

Probamos con el otro usuario: **su usuario2** y contraseña. whoami. No lleva al directorio del usuario, pero si lo crea. Con **ls -la** en

/home que ha creado las carpetas de home de los usuarios ldap.

```
usuario2@alumno-VirtualBox:/home$ ls -l
total 16
drwxr-xr-x 17 alumno      alumno      4096 feb 18 07:56 alumno
drwxr-xr-x  2 ejemploftp ejemploftp  4096 ene 18 17:51 ejemploftp
drwxr-xr-x  2 usuario1    ejemploftp  4096 feb 18 08:12 usuario1
drwxr-xr-x  2 usuario2    ejemploftp  4096 feb 18 08:13 usuario2
usuario2@alumno-VirtualBox:/home$
```

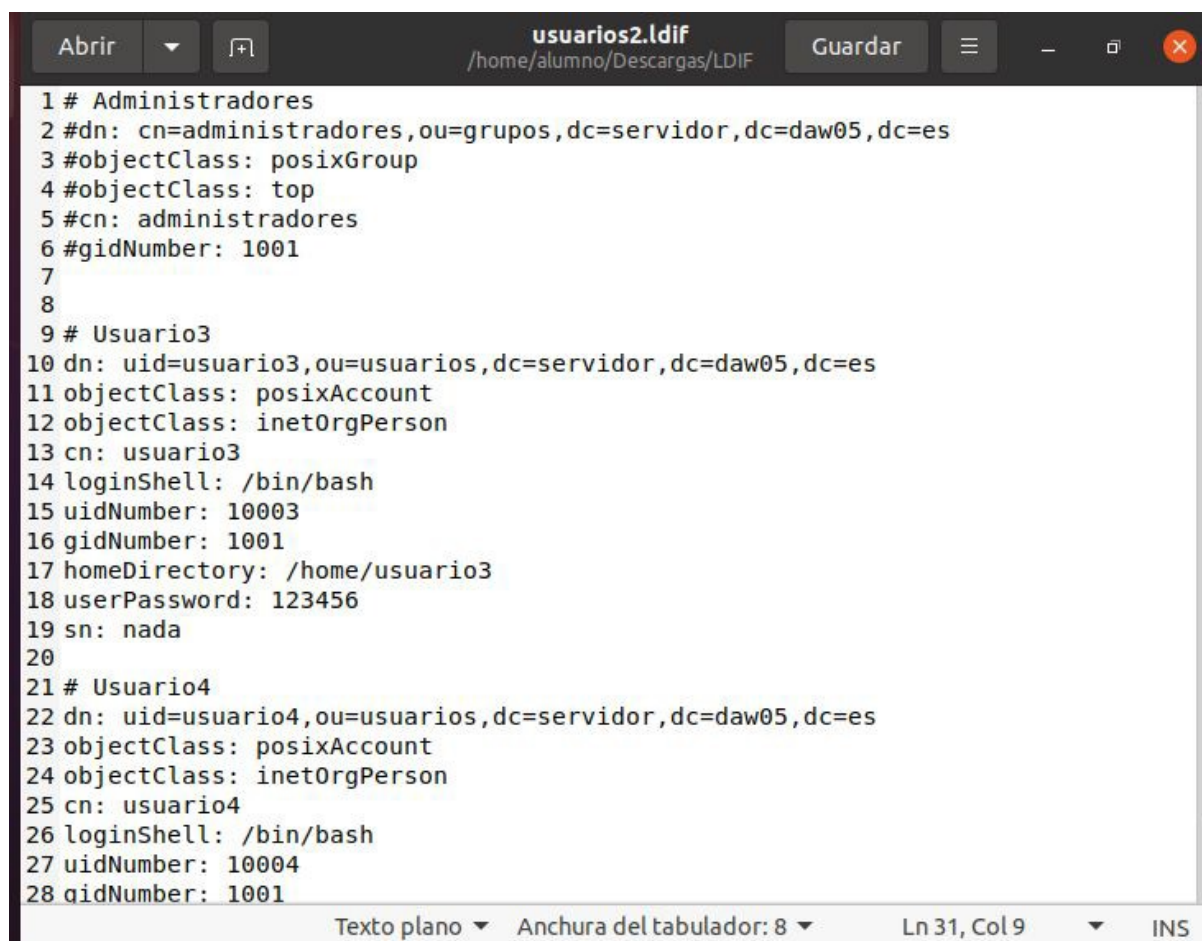
MÁS USUARIOS

Si queremos cargar más usuarios, nos vamos al directorio donde tenemos los archivos ldif. Si tratamos de ejecutar otra vez el `ldapadd` con `usuarios.ldif` daría error porque dice que esa entrada ya existe.

Creemos otro archivo: **`cp usuarios.ldif usuarios2.ldif`**

Y lo editamos para crear usuarios 3 y 4, con `uidNumber`, `cn` y `homeDirectory` para cada uno. Quitar (o comentar) el objeto que define el grupo de usuarios, porque ya existe y solo queremos objetos de tipo Usuario. Así no dará error al hacer de nuevo el **`ldapadd`**.

Entramos en `usuarios2.ldif` y comentamos la parte del grupo administradores.

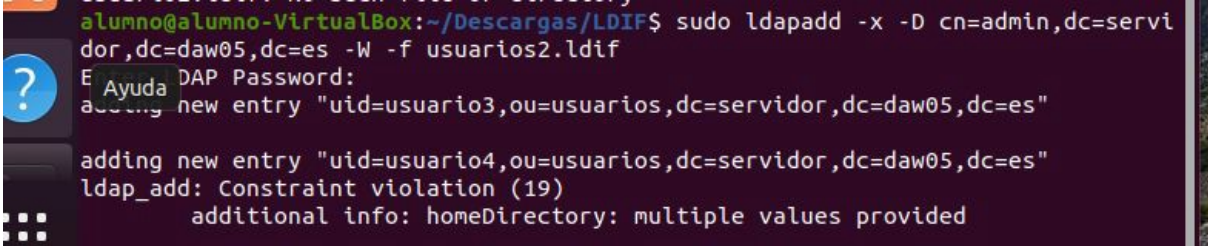


```
Abrir usuarios2.ldif Guardar
/home/alumno/Descargas/LDIF

1 # Administradores
2 #dn: cn=administradores,ou=grupos,dc=servidor,dc=daw05,dc=es
3 #objectClass: posixGroup
4 #objectClass: top
5 #cn: administradores
6 #gidNumber: 1001
7
8
9 # Usuario3
10 dn: uid=usuario3,ou=usuarios,dc=servidor,dc=daw05,dc=es
11 objectClass: posixAccount
12 objectClass: inetOrgPerson
13 cn: usuario3
14 loginShell: /bin/bash
15 uidNumber: 10003
16 gidNumber: 1001
17 homeDirectory: /home/usuario3
18 userPassword: 123456
19 sn: nada
20
21 # Usuario4
22 dn: uid=usuario4,ou=usuarios,dc=servidor,dc=daw05,dc=es
23 objectClass: posixAccount
24 objectClass: inetOrgPerson
25 cn: usuario4
26 loginShell: /bin/bash
27 uidNumber: 10004
28 gidNumber: 1001

Texto plano Anchura del tabulador: 8 Ln 31, Col 9 INS
```

```
sudo ldapadd -x -D cn=admin,dc=servidor,dc=daw05,dc=es -W -f usuarios2.ldif
```

A terminal window with a dark background. The prompt is 'alumno@alumno-VirtualBox:~/Descargas/LDIF\$'. The command 'sudo ldapadd -x -D cn=admin,dc=servidor,dc=daw05,dc=es -W -f usuarios2.ldif' is entered. The output shows 'E Ayuda DAP Password:' followed by 'adding new entry "uid=usuario3,ou=usuarios,dc=servidor,dc=daw05,dc=es"'. Then, another entry is added: 'adding new entry "uid=usuario4,ou=usuarios,dc=servidor,dc=daw05,dc=es"'. Finally, an error message is displayed: 'ldap_add: Constraint violation (19)' followed by 'additional info: homeDirectory: multiple values provided'.

```
alumno@alumno-VirtualBox:~/Descargas/LDIF$ sudo ldapadd -x -D cn=admin,dc=servidor,dc=daw05,dc=es -W -f usuarios2.ldif
E Ayuda DAP Password:
adding new entry "uid=usuario3,ou=usuarios,dc=servidor,dc=daw05,dc=es"
adding new entry "uid=usuario4,ou=usuarios,dc=servidor,dc=daw05,dc=es"
ldap_add: Constraint violation (19)
additional info: homeDirectory: multiple values provided
```

su usuario3

Y entro como usuario3. Lo compruebo con whoami. Al hacer cd me lleva al directorio del usuario.


```
pwd: /home/usuario3
```

Aunque al autenticarnos no nos introduce en el directorio home, si tiene identificado el directorio home de forma correcta.

```
alumno@alumno-VirtualBox:~/Descargas/LDIF$ su usuario3
Contraseña:
usuario3@alumno-VirtualBox:/home/alumno/Descargas/LDIF$ whoami
usuario3
usuario3@alumno-VirtualBox:/home/alumno/Descargas/LDIF$ cd
usuario3@alumno-VirtualBox:~$ ls
usuario3@alumno-VirtualBox:~$ pwd
/home/usuario3
usuario3@alumno-VirtualBox:~$
```