***Práctica 5 – Servicio LDAP***

Contenido

[A) Tenemos este escenario inicial: 4](#_Toc85736075)

[a. Trabajaremos con un Ubuntu Server y Ubuntu Desktop, que por estar en una Red NAT se integran en un servicio DHCP de VirtualBox. 4](#_Toc85736076)

[b. Las dos VM están conectadas entre sí mediante una red nat, cada una con un IP fija establecida mediante VBoxManage en la práctica 4. 4](#_Toc85736077)

[B) En el Servidor. Preliminares: 4](#_Toc85736078)

[a. Instala un servicio LDAP mediante el paquete OpenLDAP: 4](#_Toc85736079)

[i. Instalación: sudo apt-get install slapd ldap-utils (te solicitará un password, pon “admin”) 4](#_Toc85736080)

[ii. Habilitando el servicio para que se ejecute al inicio: systemctl enable slapd 4](#_Toc85736081)

[iii. Para, reinicia y verifica el status del servicio con systemctl systemctl stop/restart/... slapd 4](#_Toc85736082)

[iv. Verifica que el puerto 389 está abierto con nmap: nmap 127.0.0.1, que ofrece los puertos abiertos en el servidor. 6](#_Toc85736083)

[b. Configuraremos el servicio con dpkg-reconfigure slapd 6](#_Toc85736084)

[i. Los valores por defecto respétalos 6](#_Toc85736085)

[ii. Introduce admin en la contraseña (sobreescribe a la primera) 6](#_Toc85736086)

[iii. Como dominio pon<nombreapellido> .local 7](#_Toc85736087)

[iv. Al finalizar ejecuta slaptcat, y te mostrará lo que hay actualmente configurado. 7](#_Toc85736088)

[C) En este punto, podemos empezar a crear el árbol del directorio. Nos convendrá instalar una interfaz gráfica que nos permitirá gestionarlo sin comandos de Shell. 8](#_Toc85736089)

[a. apt install ldap-account-manager 8](#_Toc85736090)

[b. reinicio del servicio de apache 8](#_Toc85736091)

[c. Acudiremos a localhost/lam y veremos el punto de entrada ó login de la aplicación web. 8](#_Toc85736092)

[d. Seleccionamos configuración LAM, en la parte superior derecha, y editar perfiles del servidor. 9](#_Toc85736093)

[e. Nos pedirá la contraseña maestra, es “lam” 9](#_Toc85736094)

[f. En la pestaña de configuración general: 9](#_Toc85736095)

[i. Preferencias del servidor: Sufijo del árbol ponemos nuestro dominio. Ej: dc=raulbonachia, dc=local 9](#_Toc85736096)

[ii. Configuración del idioma español 9](#_Toc85736097)

[iii. En preferencias del sistema (security settings) indicamos cn=admin, dc=,<nombreapellido> dc=local 9](#_Toc85736098)

[iv. En Profile password ponemos admin 10](#_Toc85736099)

[v. Le damos a Guardar 10](#_Toc85736100)

[g. En la pestaña de Tipos de Cuentas: 10](#_Toc85736101)

[i. Hay dos unidades organizativas, usuarios y grupos. 10](#_Toc85736102)

[ii. Para usuarios de sufijo: ou=usuarios,dc=,dc=local 10](#_Toc85736103)

[iii. Para grupos de sufijo: 10](#_Toc85736104)

[iv. ou=grupos,dc=,dc=local 10](#_Toc85736105)

[v. Agrega una nueva unidad organizativa para Equipos (Hosts) con sufijos: ou=equipos,dc=,dc=local 11](#_Toc85736106)

[vi. Le damos a Guardar 11](#_Toc85736107)

[h. En la pestaña de Módulos: 11](#_Toc85736108)

[i. Agregamos para Equipos el ítem Unix PosixAccount y el ítem Cuenta (Account) 11](#_Toc85736109)

[ii. Le damos a Guardar 11](#_Toc85736110)

[i. Nos lleva la aplicación al punto de entrada de login, con el usuario admin selecionado. Los autenticamos con la contraseña especificada y nos indicará si queremos crear las tres unidades organizativas configuradas: usuarios, grupos y equipos. Pulsamos que sí 11](#_Toc85736111)

[En este punto tendríamos que ver tantas pestañas como unidades organizativas 12](#_Toc85736112)

[D) Crearemos un nuevo grupo de nombre Profesores (GID number no se introduce) con descripción “Grupo de profesores”. Idem para el grupo Alumnos. 12](#_Toc85736113)

[E) Crea un nuevo usuario: Nombre:”Profesor”, apellidos “01”, en la pestaña personal. En la de Unix, username=”profesor01” y lo asociamos al grupo profesores. Le asociamos una contraseña (Set password) para dicho usuario. Guardamos 13](#_Toc85736114)

[F) Ahora tendremos que crear un cliente que haga uso del servidor LDAP. Usaremos un Ubuntu Desktop nuevo conectado a la red nat de nuestro servidor. 15](#_Toc85736115)

[a. apt install libnss-ldap libpam-ldap ldap-utils 15](#_Toc85736116)

[b. Nos pedirá el LDAP server URI: poner ldap://IPSERVIDOR 15](#_Toc85736117)

[c. Para la búsqueda base: dc=, dc=local, que es la raíz del árbol de nuestro directorio en el servidor. 3º DUAL Servicio LDAP 2021-2022 3 15](#_Toc85736118)

[d. Versión de LDAP, la 3 15](#_Toc85736119)

[e. En el resto de pantallas dejamos las opciones por defecto hasta llegar a la pantalla que nos pide LDAP account for root, que introduciremos: cn=admin, dc=, dc=local 16](#_Toc85736120)

[f. En la pantalla de acceso a LDAP root account password ponemos la contraseña (admin) y el proceso terminará de instalar todos los paquetes. 16](#_Toc85736121)

[G) Ahora, configuraremos el archivo /etc/nsswitch.conf, donde indicaremos dónde debe buscar para encontrar los nombres y password de los usuarios que se vayan a loguear, (querremos que use LDAP) quedando así 17](#_Toc85736122)

[H) Ahora, editaremos el archivo /etc/pam.d/common-password y, en la línea 26, eliminaremos la palabra use\_authtok, que nos impide usar varios métodos de autenticación en el caso de que el primero no salga bien. 18](#_Toc85736123)

[I)Ahora, editaremos el archivo /etc/pam.d/common-session, y añadiremos lo necesario para que cuando el usuario se autentique se genere un home dentro del equipo, con permisos para que el usuario pueda actuar sobre esos ficheros pero no los demás. Para ello añadiremos una línea al final del fichero: 18](#_Toc85736124)

[J) Ahora, comprobaremos que el cliente pueda autenticarse contra el servidor LDAP. Para ello, la manera más rápida es realizar una búsqueda contra el servidor LDAP, y si obtenemos una conexión será señal de que está todo bien. Para ello, no hace falta estar logueado: 19](#_Toc85736125)

[K) Ahora, nos autenticaremos vía terminal desde el cliente contra el servidor. Para ello reiniciaremos y cerraremos sesión en el cliente y cuando aparezca la pantalla de autenticación, pulsaremos ALT+CONTROL+F2 y nos autenticaremos con el usuario y contraseña a través de la Shell. Veremos que la autenticación es efectiva y podemos usar los comandos Shell habituales 21](#_Toc85736126)

[L) Ahora, querremos autenticarnos en modo gráfico. Para ello, nos autenticamos como administrador de la máquina cliente en modo gráfico, e instalamos el paquete que nos falta: 22](#_Toc85736127)

[a. apt install nslcd (al instalarlo después de los paquetes previos, como ldap-utils se aprovecha la configuración ya realizada y no habrá que volver a poner los datos del acceso a servidor y dominio, basta verificar en el instalador que está todo correcto). 22](#_Toc85736128)

[b. Reiniciamos y después cerramos sesión. 23](#_Toc85736129)

[c. Nos autenticamos con un usuario registrado en el directorio LDAP del servidor, que quedarán registrados como usuarios válidos en el login, posteriormente 23](#_Toc85736130)

# A) Tenemos este escenario inicial:

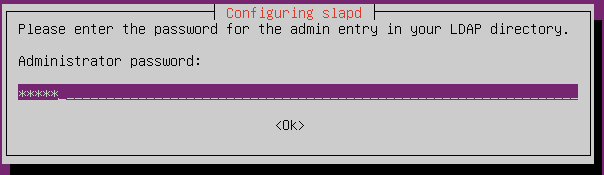
## a. Trabajaremos con un Ubuntu Server y Ubuntu Desktop, que por estar en una Red NAT se integran en un servicio DHCP de VirtualBox.

## b. Las dos VM están conectadas entre sí mediante una red nat, cada una con un IP fija establecida mediante VBoxManage en la práctica 4.

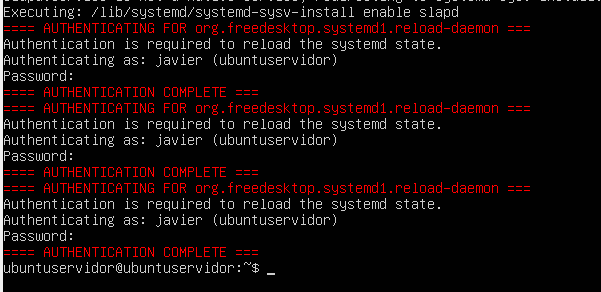
# B) En el Servidor. Preliminares:

## a. Instala un servicio LDAP mediante el paquete OpenLDAP:

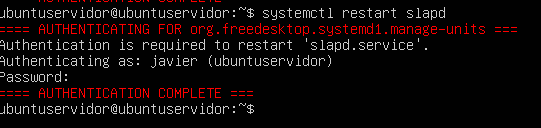
### i. Instalación: sudo apt-get install slapd ldap-utils (te solicitará un password, pon “admin”)

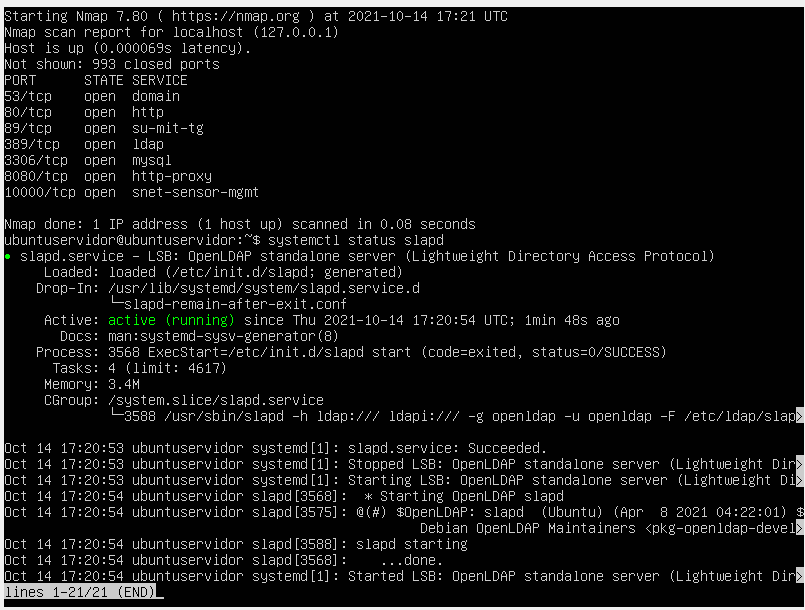


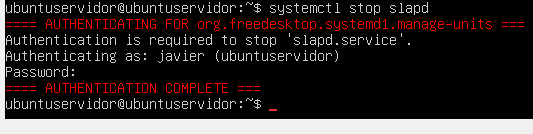
### ii. Habilitando el servicio para que se ejecute al inicio: systemctl enable slapd

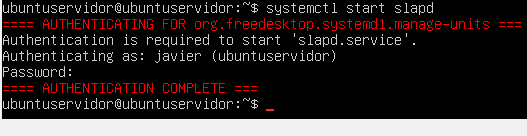


### iii. Para, reinicia y verifica el status del servicio con systemctl systemctl stop/restart/... slapd

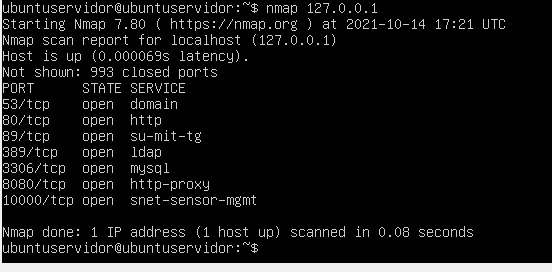








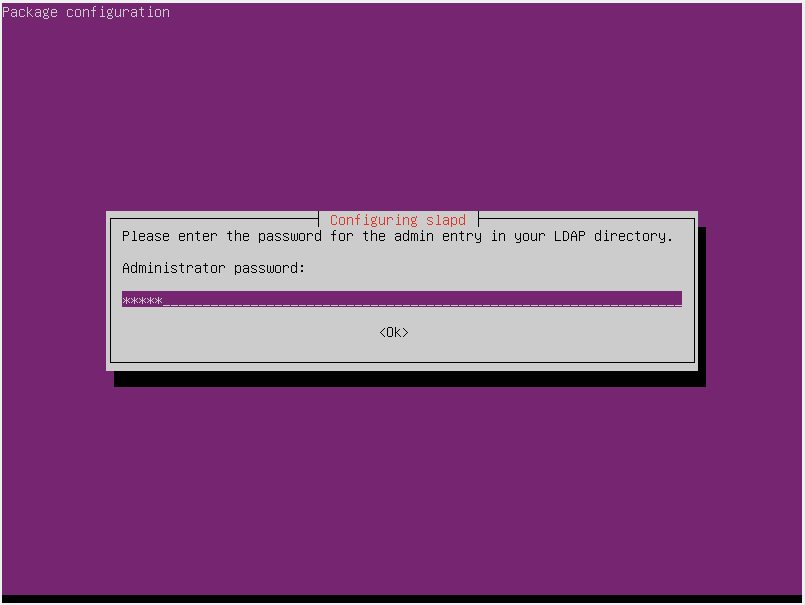
### iv. Verifica que el puerto 389 está abierto con nmap: nmap 127.0.0.1, que ofrece los puertos abiertos en el servidor.



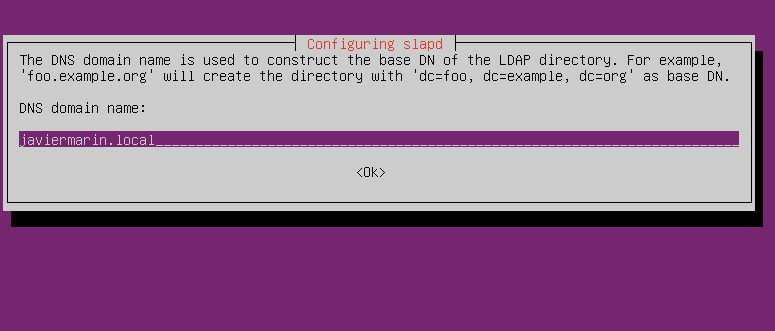
## b. Configuraremos el servicio con dpkg-reconfigure slapd

### i. Los valores por defecto respétalos

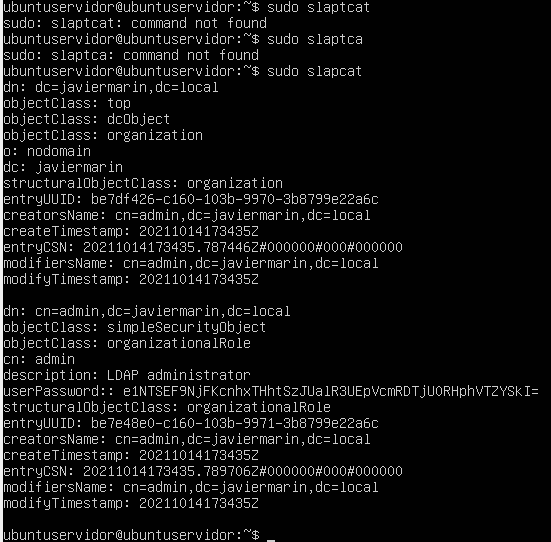
### ii. Introduce admin en la contraseña (sobreescribe a la primera)



### iii. Como dominio pon<nombreapellido> .local

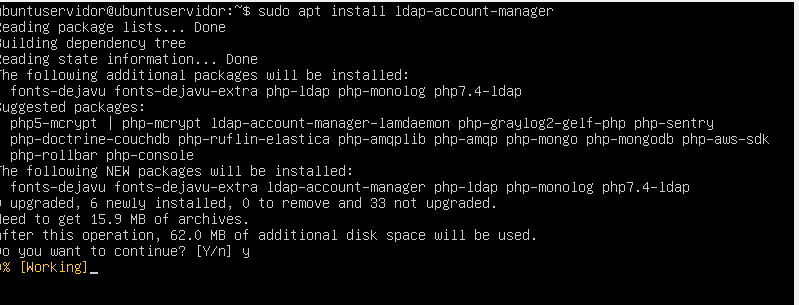


### iv. Al finalizar ejecuta slaptcat, y te mostrará lo que hay actualmente configurado.

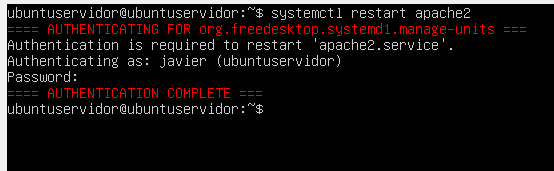


# C) En este punto, podemos empezar a crear el árbol del directorio. Nos convendrá instalar una interfaz gráfica que nos permitirá gestionarlo sin comandos de Shell.

## a. apt install ldap-account-manager

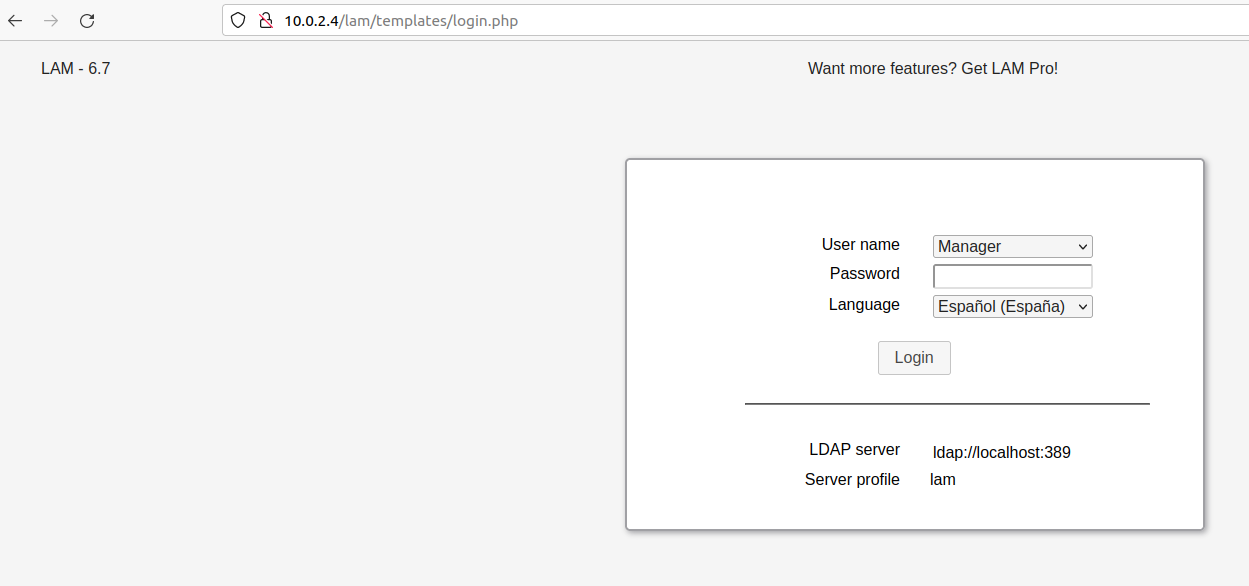


## b. reinicio del servicio de apache



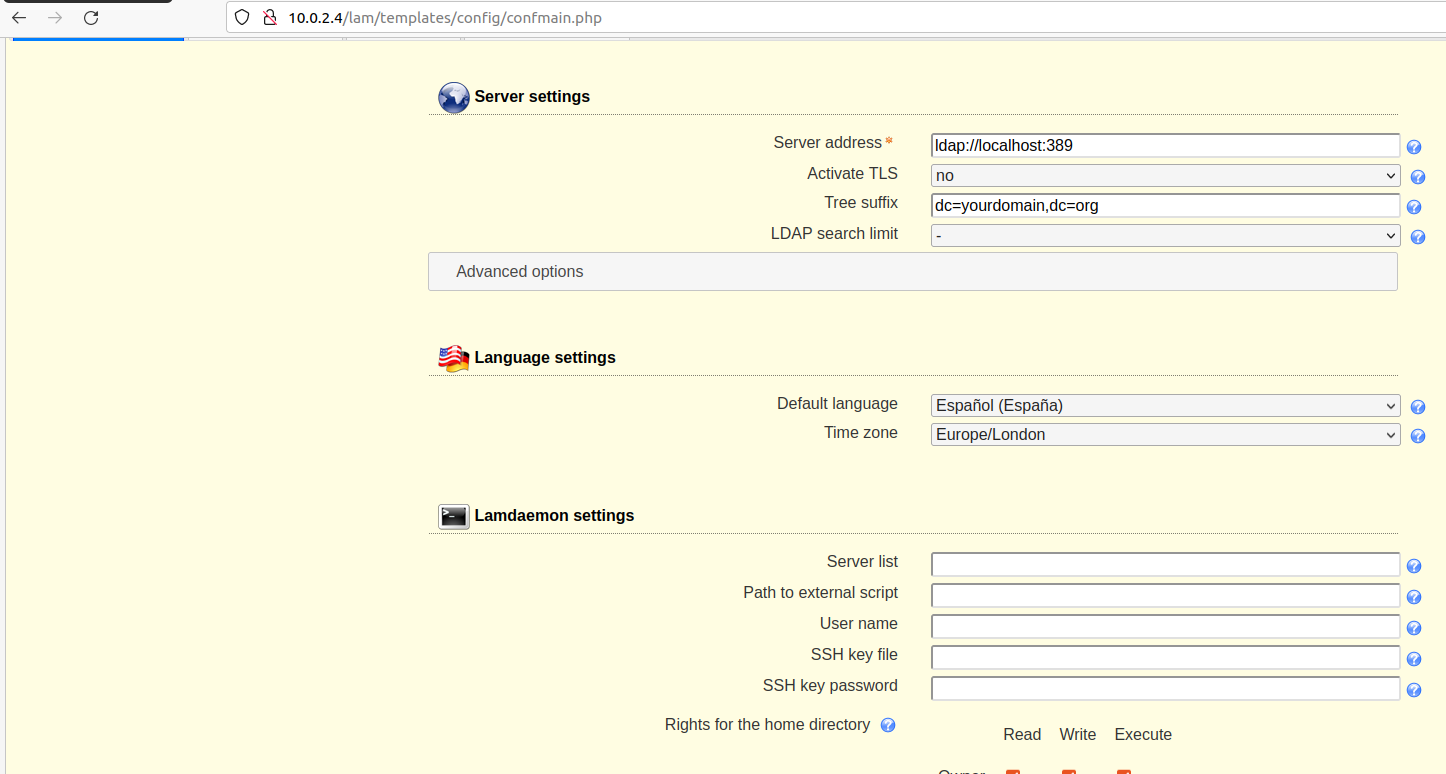
## c. Acudiremos a localhost/lam y veremos el punto de entrada ó login de la aplicación web.

DESDE EL CLIENTE:



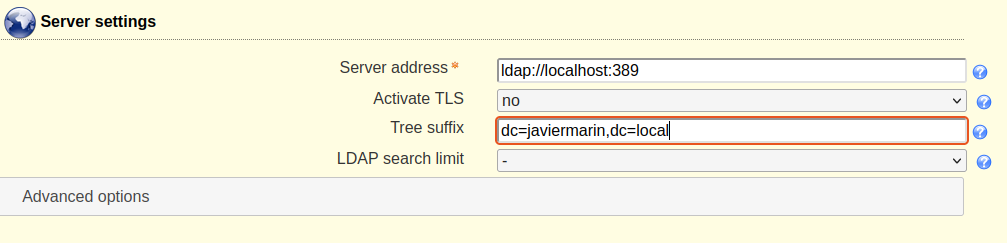
## d. Seleccionamos configuración LAM, en la parte superior derecha, y editar perfiles del servidor.

## e. Nos pedirá la contraseña maestra, es “lam”

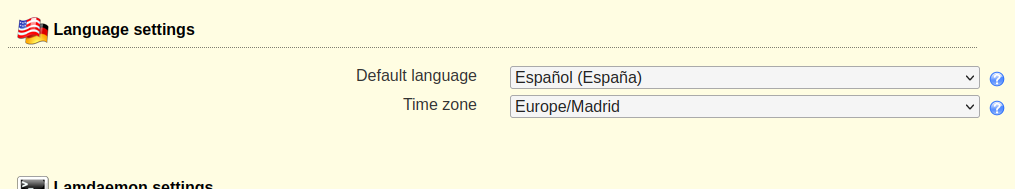


## f. En la pestaña de configuración general:

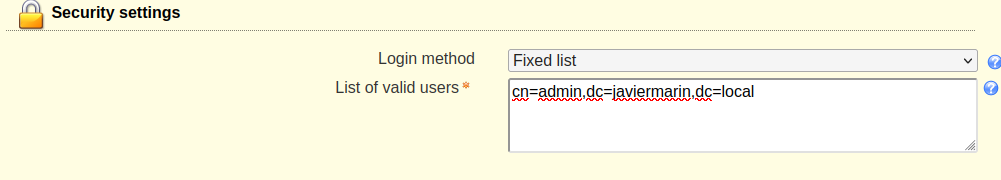
### i. Preferencias del servidor: Sufijo del árbol ponemos nuestro dominio. Ej: dc=raulbonachia, dc=local



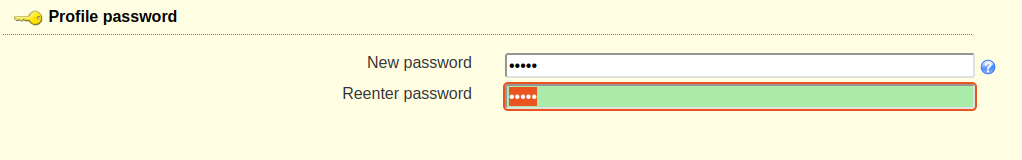
### ii. Configuración del idioma español



### iii. En preferencias del sistema (security settings) indicamos cn=admin, dc=,<nombreapellido> dc=local



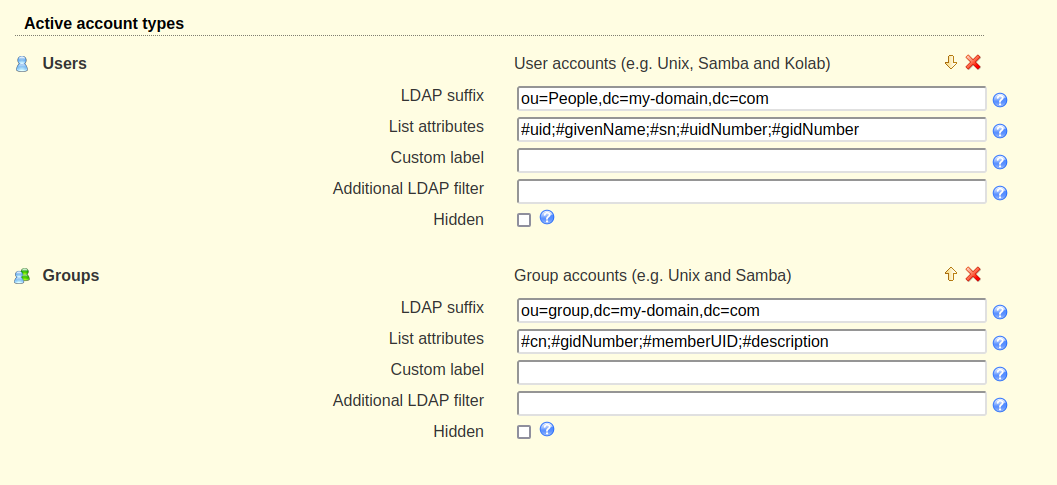
### iv. En Profile password ponemos admin



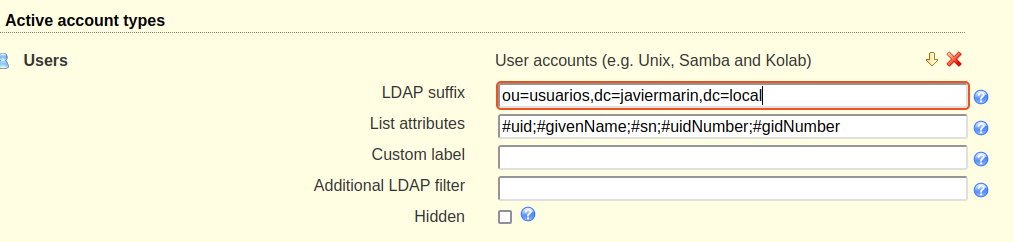
### v. Le damos a Guardar

## g. En la pestaña de Tipos de Cuentas:

### i. Hay dos unidades organizativas, usuarios y grupos.

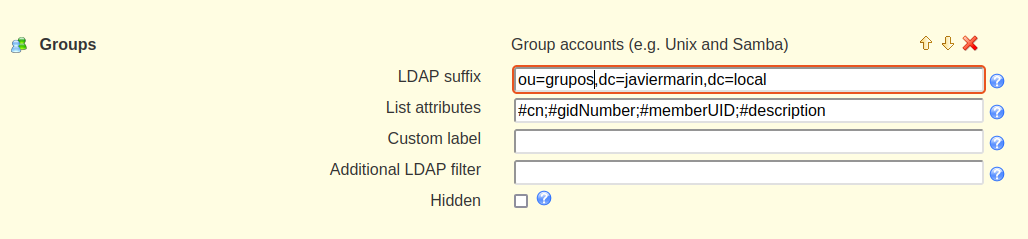


### ii. Para usuarios de sufijo: ou=usuarios,dc=,dc=local



### iii. Para grupos de sufijo:

### iv. ou=grupos,dc=,dc=local

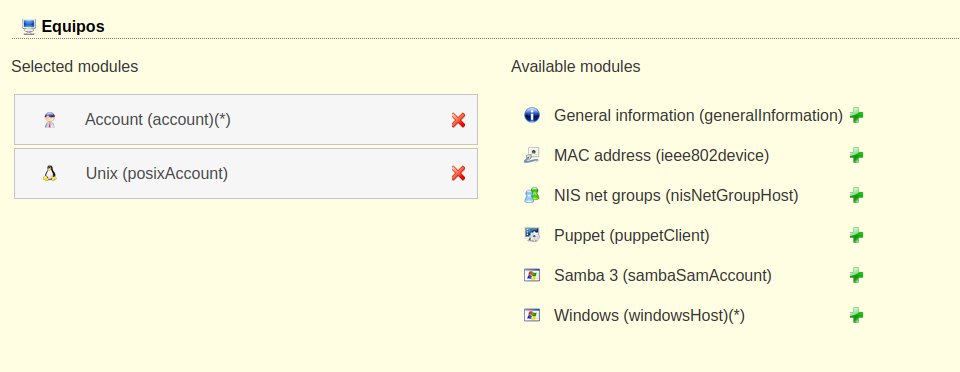


### v. Agrega una nueva unidad organizativa para Equipos (Hosts) con sufijos: ou=equipos,dc=,dc=local

### vi. Le damos a Guardar

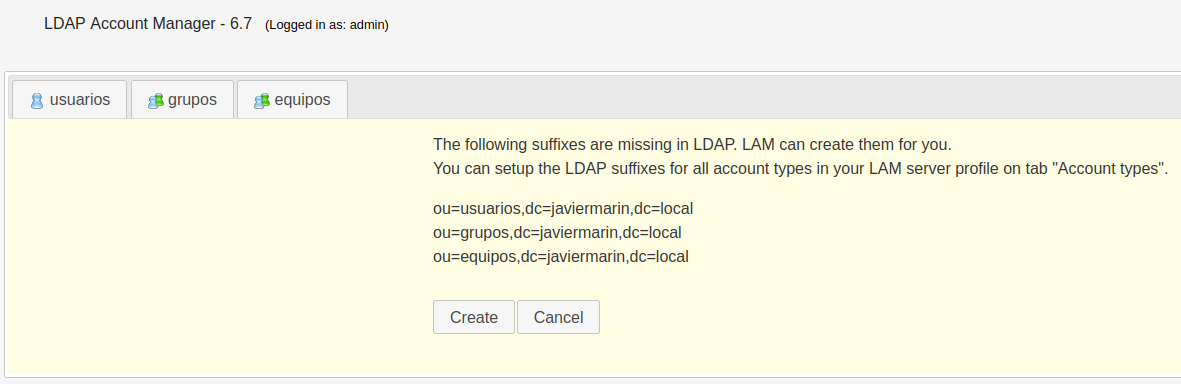
## h. En la pestaña de Módulos:

### i. Agregamos para Equipos el ítem Unix PosixAccount y el ítem Cuenta (Account)

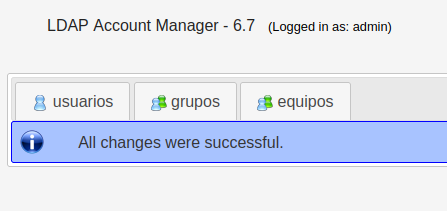


### ii. Le damos a Guardar

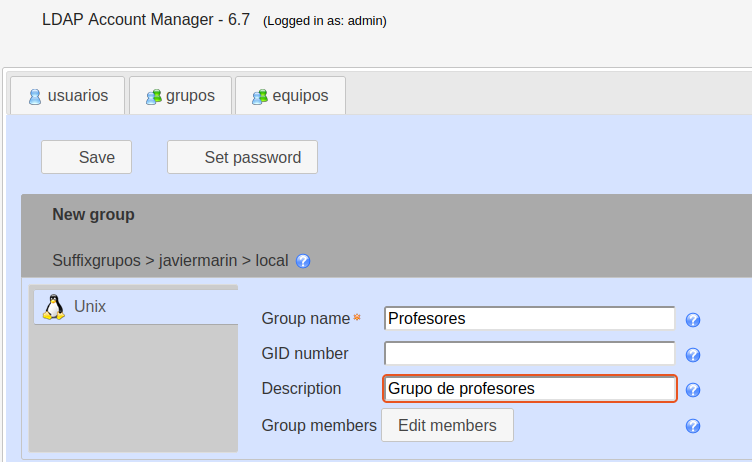
## Nos lleva la aplicación al punto de entrada de login, con el usuario admin selecionado. Los autenticamos con la contraseña especificada y nos indicará si queremos crear las tres unidades organizativas configuradas: usuarios, grupos y equipos. Pulsamos que sí



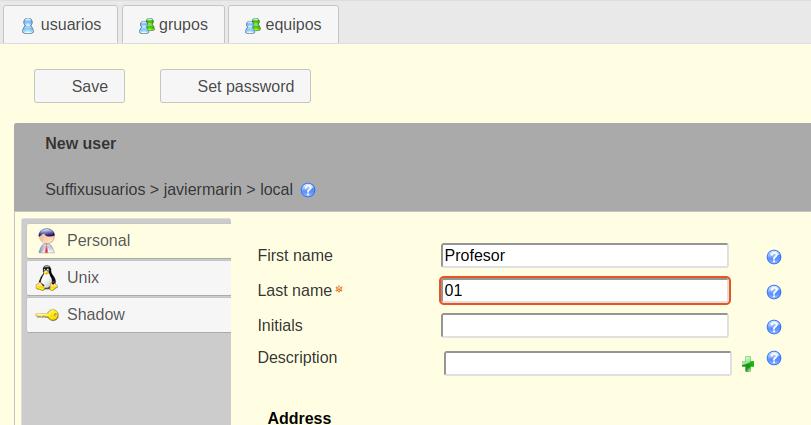
## En este punto tendríamos que ver tantas pestañas como unidades organizativas

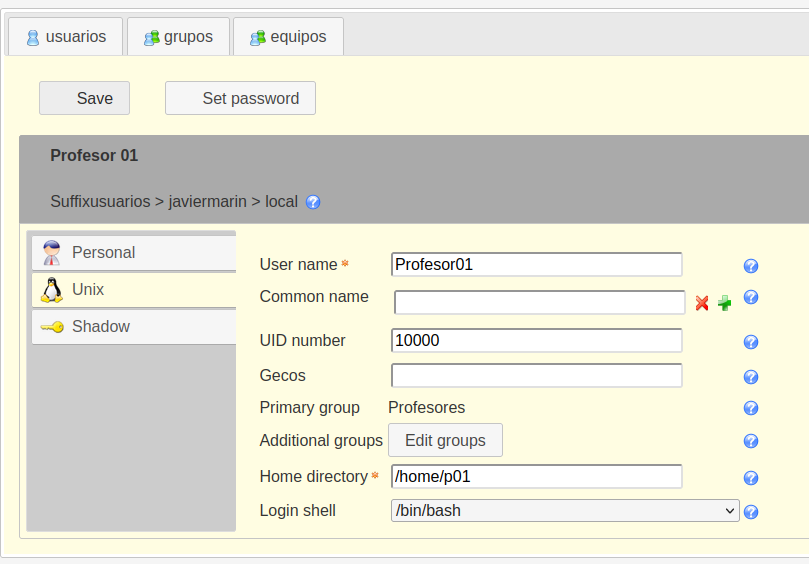


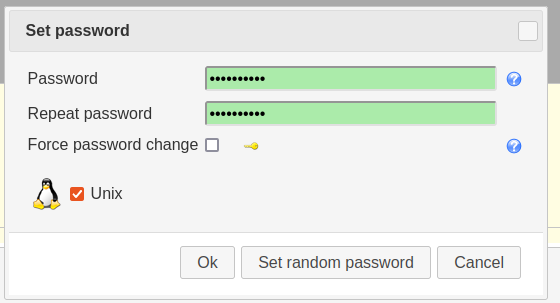
# D) Crearemos un nuevo grupo de nombre Profesores (GID number no se introduce) con descripción “Grupo de profesores”. Idem para el grupo Alumnos.

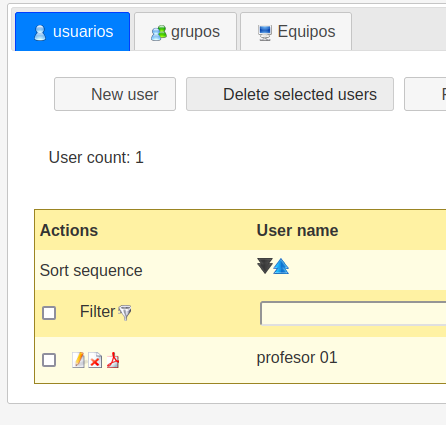


# E) Crea un nuevo usuario: Nombre:”Profesor”, apellidos “01”, en la pestaña personal. En la de Unix, username=”profesor01” y lo asociamos al grupo profesores. Le asociamos una contraseña (Set password) para dicho usuario. Guardamos



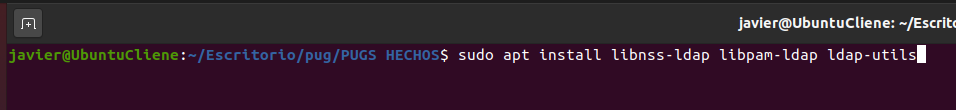




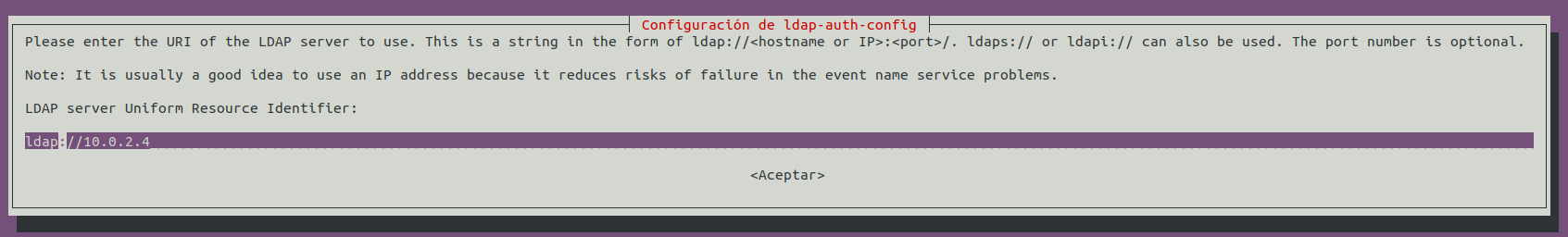


# F) Ahora tendremos que crear un cliente que haga uso del servidor LDAP. Usaremos un Ubuntu Desktop nuevo conectado a la red nat de nuestro servidor.

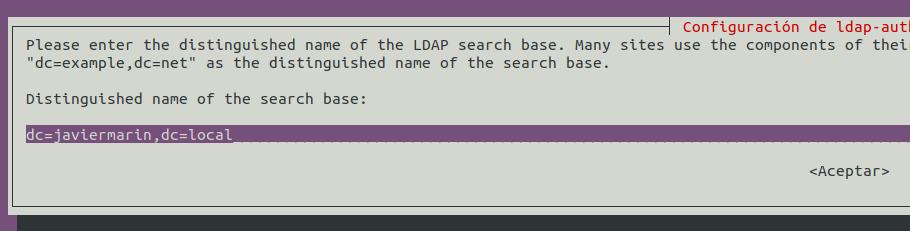
## a. apt install libnss-ldap libpam-ldap ldap-utils



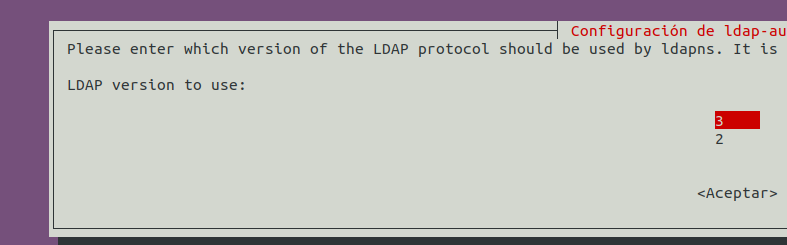
## b. Nos pedirá el LDAP server URI: poner ldap://IPSERVIDOR



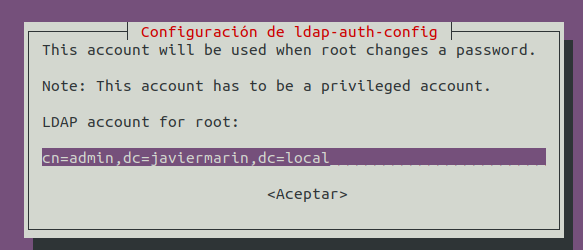
## c. Para la búsqueda base: dc=, dc=local, que es la raíz del árbol de nuestro directorio en el servidor. 3º DUAL Servicio LDAP 2021-2022 3



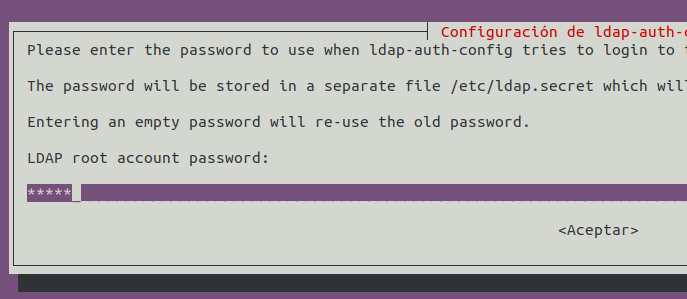
## d. Versión de LDAP, la 3



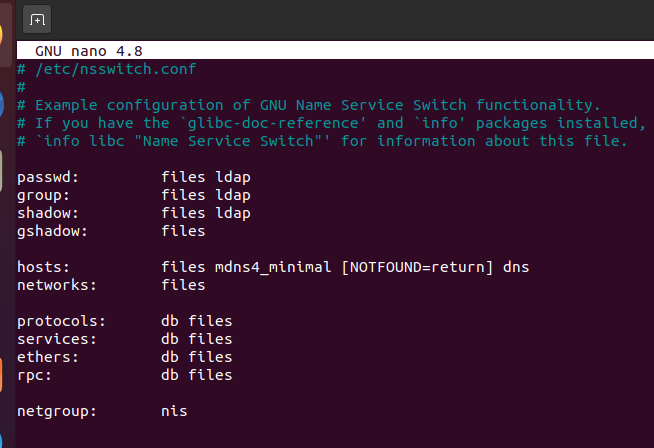
## e. En el resto de pantallas dejamos las opciones por defecto hasta llegar a la pantalla que nos pide LDAP account for root, que introduciremos: cn=admin, dc=, dc=local



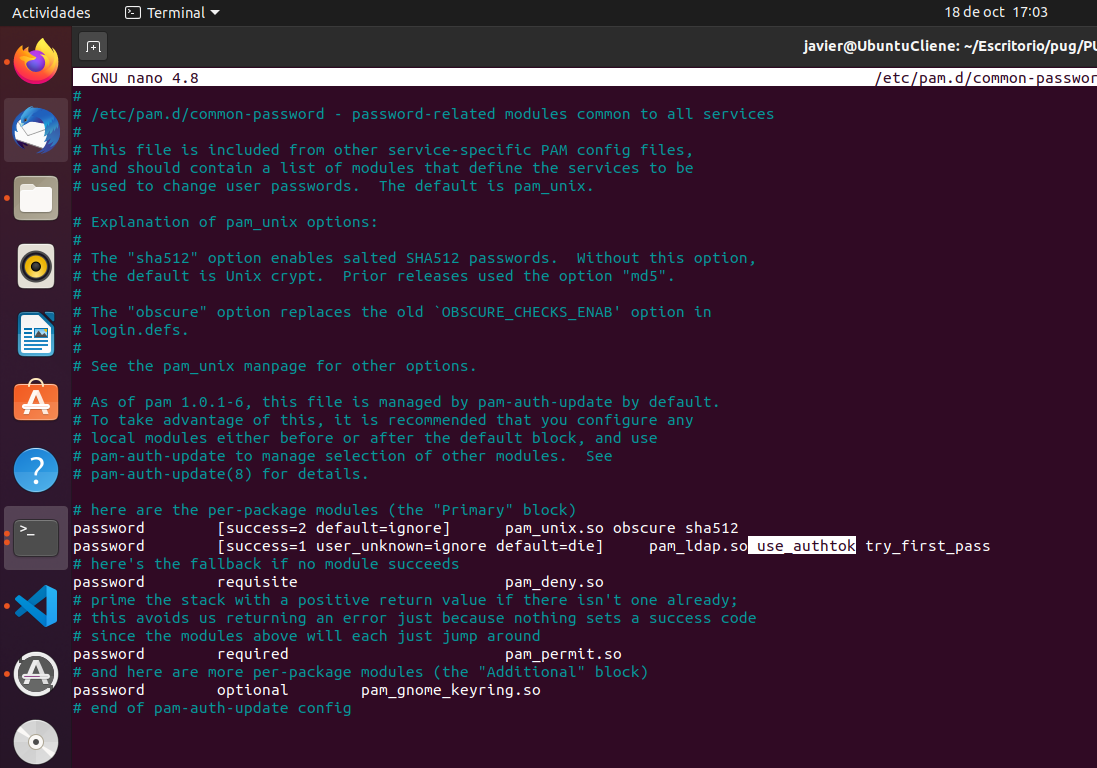
## f. En la pantalla de acceso a LDAP root account password ponemos la contraseña (admin) y el proceso terminará de instalar todos los paquetes.



# G) Ahora, configuraremos el archivo /etc/nsswitch.conf, donde indicaremos dónde debe buscar para encontrar los nombres y password de los usuarios que se vayan a loguear, (querremos que use LDAP) quedando así

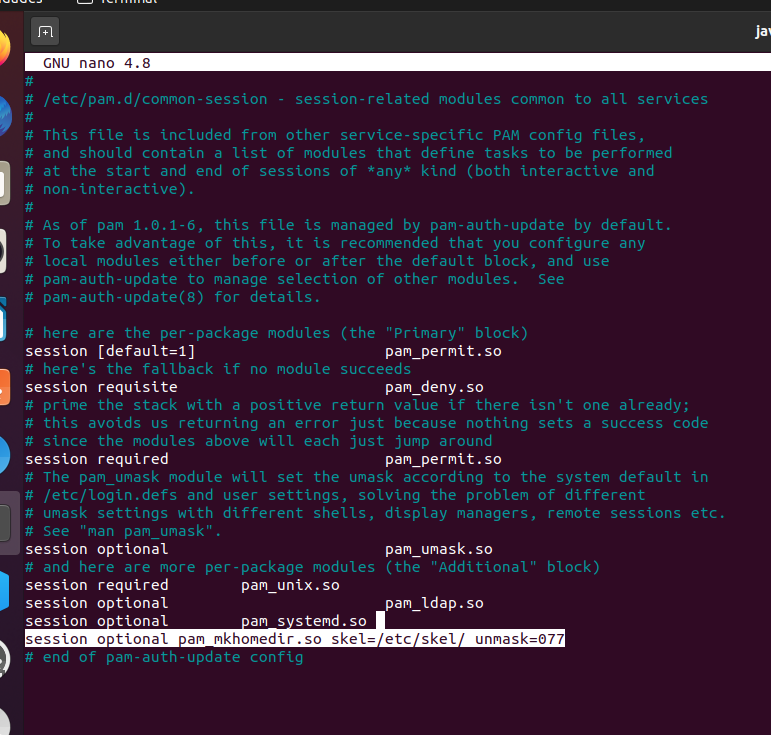


# H) Ahora, editaremos el archivo /etc/pam.d/common-password y, en la línea 26, eliminaremos la palabra use\_authtok, que nos impide usar varios métodos de autenticación en el caso de que el primero no salga bien.



# I)Ahora, editaremos el archivo /etc/pam.d/common-session, y añadiremos lo necesario para que cuando el usuario se autentique se genere un home dentro del equipo, con permisos para que el usuario pueda actuar sobre esos ficheros pero no los demás. Para ello añadiremos una línea al final del fichero:

session optional pam\_mkhomedir.so skel=/etc/skel/ unmask=077



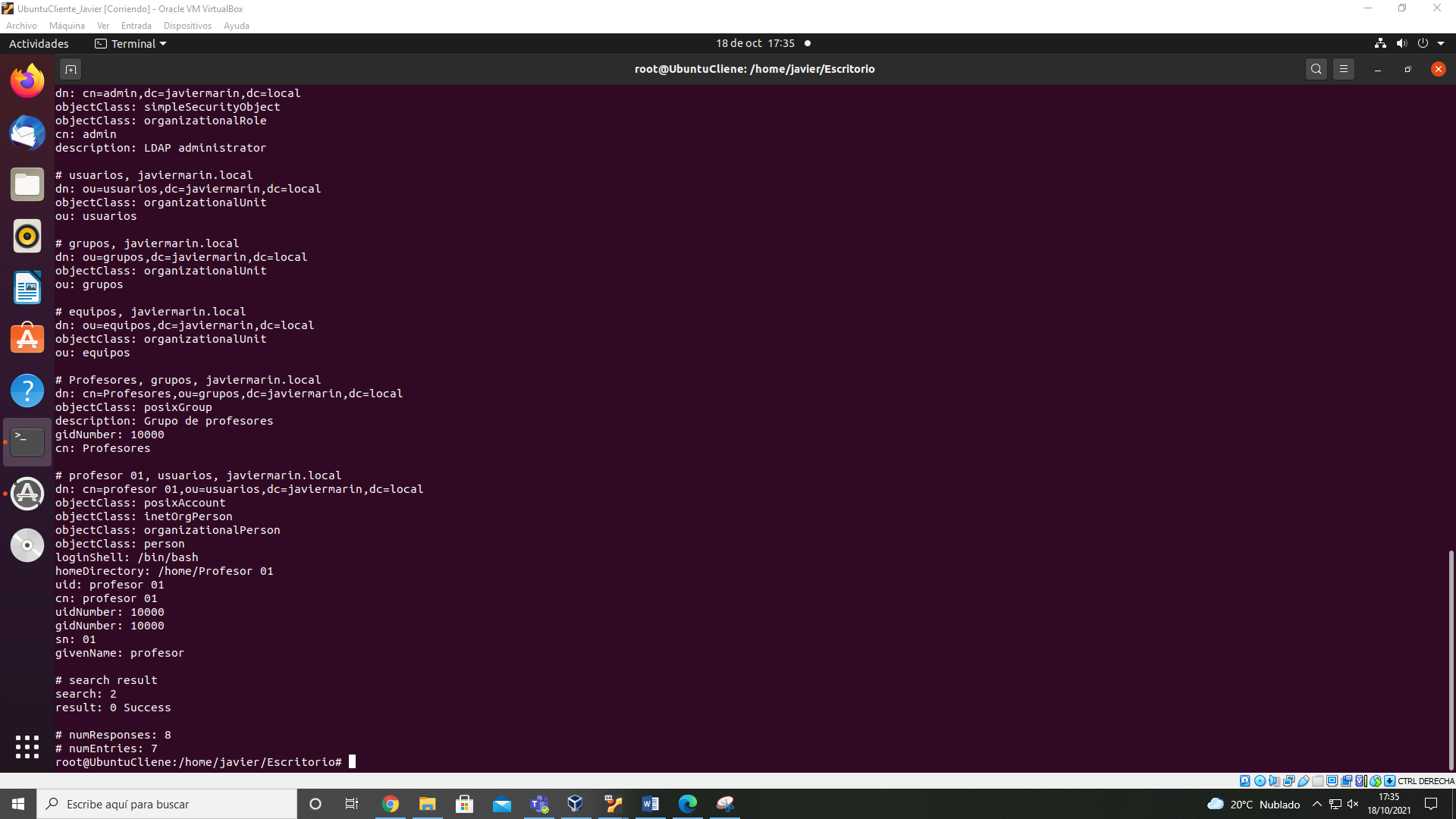
# J) Ahora, comprobaremos que el cliente pueda autenticarse contra el servidor LDAP. Para ello, la manera más rápida es realizar una búsqueda contra el servidor LDAP, y si obtenemos una conexión será señal de que está todo bien. Para ello, no hace falta estar logueado:

ldapsearch -x -H ldap://IPSERVIDOR -b “dc=, dc=local” -s sub

x: indica que no se va usar ningún usuario

H: indica el servidor

B: indica qué elemento se va a buscar y obtendremos un resultado como el siguiente

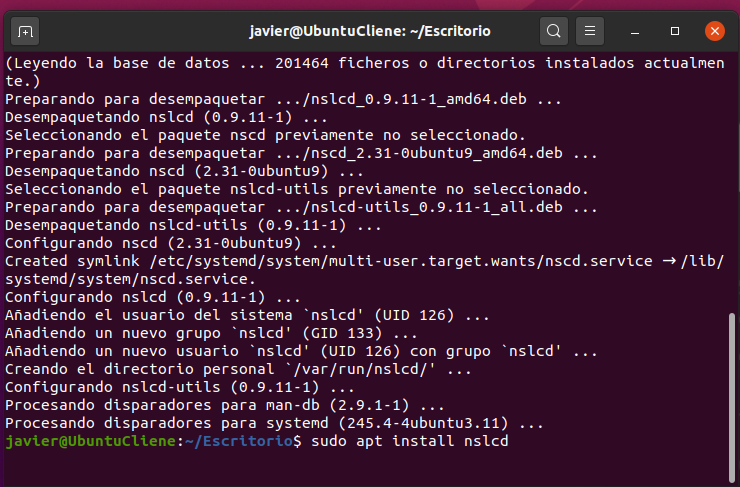


# K) Ahora, nos autenticaremos vía terminal desde el cliente contra el servidor. Para ello reiniciaremos y cerraremos sesión en el cliente y cuando aparezca la pantalla de autenticación, pulsaremos ALT+CONTROL+F2 y nos autenticaremos con el usuario y contraseña a través de la Shell. Veremos que la autenticación es efectiva y podemos usar los comandos Shell habituales



# L) Ahora, querremos autenticarnos en modo gráfico. Para ello, nos autenticamos como administrador de la máquina cliente en modo gráfico, e instalamos el paquete que nos falta:

## a. apt install nslcd (al instalarlo después de los paquetes previos, como ldap-utils se aprovecha la configuración ya realizada y no habrá que volver a poner los datos del acceso a servidor y dominio, basta verificar en el instalador que está todo correcto).



## b. Reiniciamos y después cerramos sesión.

## c. Nos autenticamos con un usuario registrado en el directorio LDAP del servidor, que quedarán registrados como usuarios válidos en el login, posteriormente

