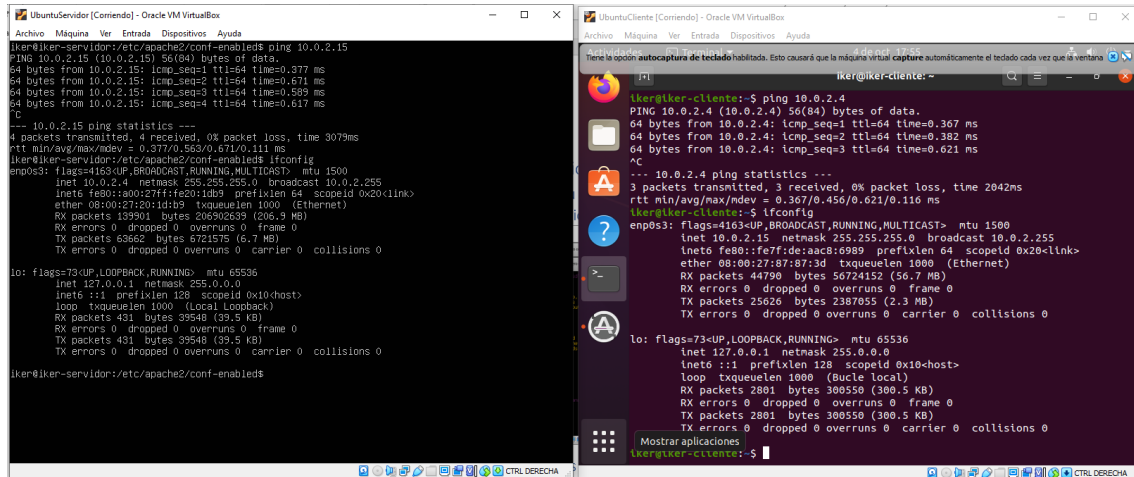


A) Tenemos este escenario inicial:

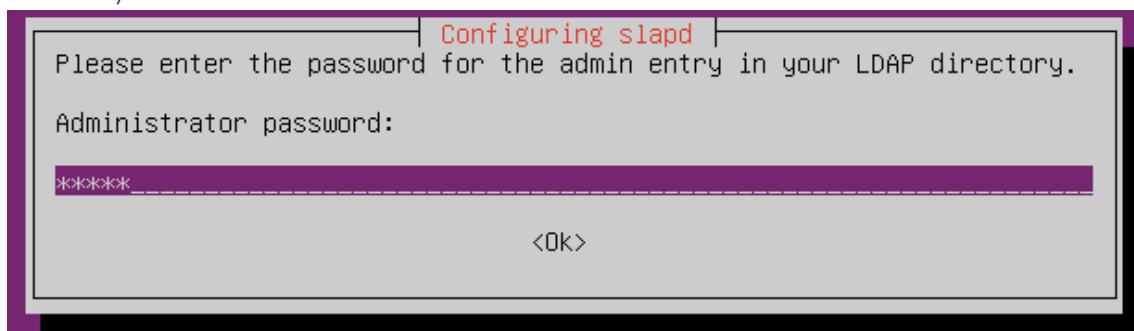
- Trabajaremos con un Ubuntu Server y Ubuntu Desktop, que por estar en una Red NAT se integran en un servicio DHCP de VirtualBox.
- Las dos VM están conectadas entre sí mediante una red nat, cada una con un IP fija establecida mediante VBoxManage en la práctica 4.



The image shows two terminal windows from Oracle VM VirtualBox. The left window is titled 'UbuntuServer [Coniende] - Oracle VM VirtualBox' and shows the output of a ping command from the server to the client (10.0.2.15). The output shows 4 packets transmitted, 4 received, 0% packet loss, and a time of 307ms. Below the ping output, the 'ifconfig' command is run, showing the network configuration for the 'eno333' interface, including IP address, netmask, broadcast, and MTU. The right window is titled 'UbuntuCliente [Coniende] - Oracle VM VirtualBox' and shows the output of a ping command from the client to the server (10.0.2.4). The output shows 3 packets transmitted, 3 received, 0% packet loss, and a time of 204ms. Below the ping output, the 'ifconfig' command is run, showing the network configuration for the 'eno333' interface, including IP address, netmask, broadcast, and MTU.

B) En el Servidor. Preliminares:

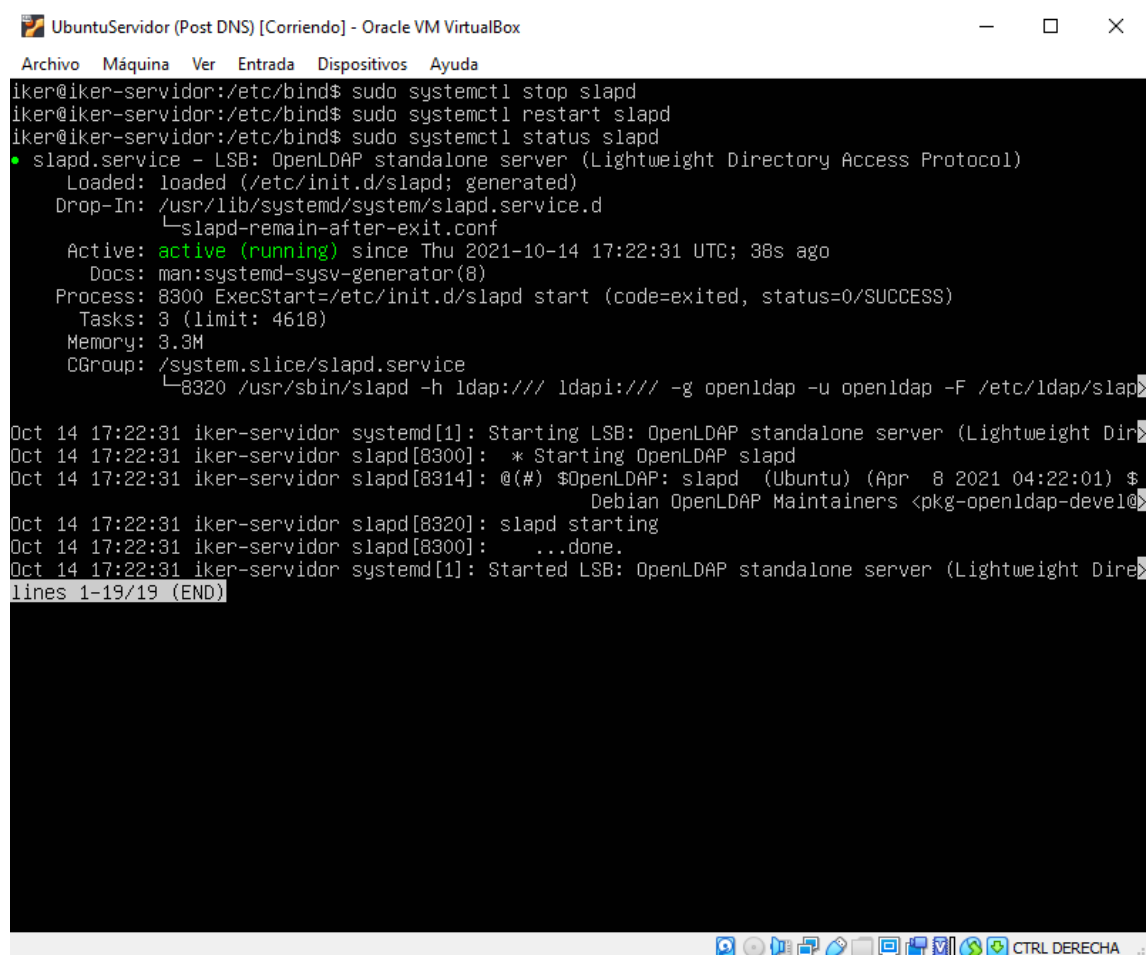
- Instala un servicio LDAP mediante el paquete OpenLDAP:
 - Instalación: `sudo apt-get install slapd ldap-utils` (te solicitará un password, pon "admin")



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

```
iker@iker-servidor:/etc/bind$ systemctl enable slapd
slapd.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable slapd
==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ====
Authentication is required to reload the systemd state.
Authenticating as: iker
Password:
==== AUTHENTICATION COMPLETE ====
==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ====
Authentication is required to reload the systemd state.
Authenticating as: iker
Password:
==== AUTHENTICATION COMPLETE ====
==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ====
Authentication is required to reload the systemd state.
Authenticating as: iker
Password:
==== AUTHENTICATION COMPLETE ====
iker@iker-servidor:/etc/bind$ _
```

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



```
UbuntuServidor (Post DNS) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
iker@iker-servidor:/etc/bind$ sudo systemctl stop slapd
iker@iker-servidor:/etc/bind$ sudo systemctl restart slapd
iker@iker-servidor:/etc/bind$ sudo systemctl status slapd
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
   Loaded: loaded (/etc/init.d/slapd; generated)
   Drop-In: /usr/lib/systemd/system/slapd.service.d
            └─slapd-remain-after-exit.conf
   Active: active (running) since Thu 2021-10-14 17:22:31 UTC; 38s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 8300 ExecStart=/etc/init.d/slapd start (code=exited, status=0/SUCCESS)
    Tasks: 3 (limit: 4618)
   Memory: 3.3M
    CGroup: /system.slice/slapd.service
            └─8320 /usr/sbin/slapd -h ldap:/// ldapi:/// -g openldap -u openldap -F /etc/ldap/slapd

Oct 14 17:22:31 iker-servidor systemd[1]: Starting LSB: OpenLDAP standalone server (Lightweight Dir
Oct 14 17:22:31 iker-servidor slapd[8300]: * Starting OpenLDAP slapd
Oct 14 17:22:31 iker-servidor slapd[8314]: @(#) $OpenLDAP: slapd (Ubuntu) (Apr  8 2021 04:22:01) $
                                Debian OpenLDAP Maintainers <pkg-openldap-devel@
Oct 14 17:22:31 iker-servidor slapd[8320]: slapd starting
Oct 14 17:22:31 iker-servidor slapd[8300]: ...done.
Oct 14 17:22:31 iker-servidor systemd[1]: Started LSB: OpenLDAP standalone server (Lightweight Dire
lines 1-19/19 (END)
```

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

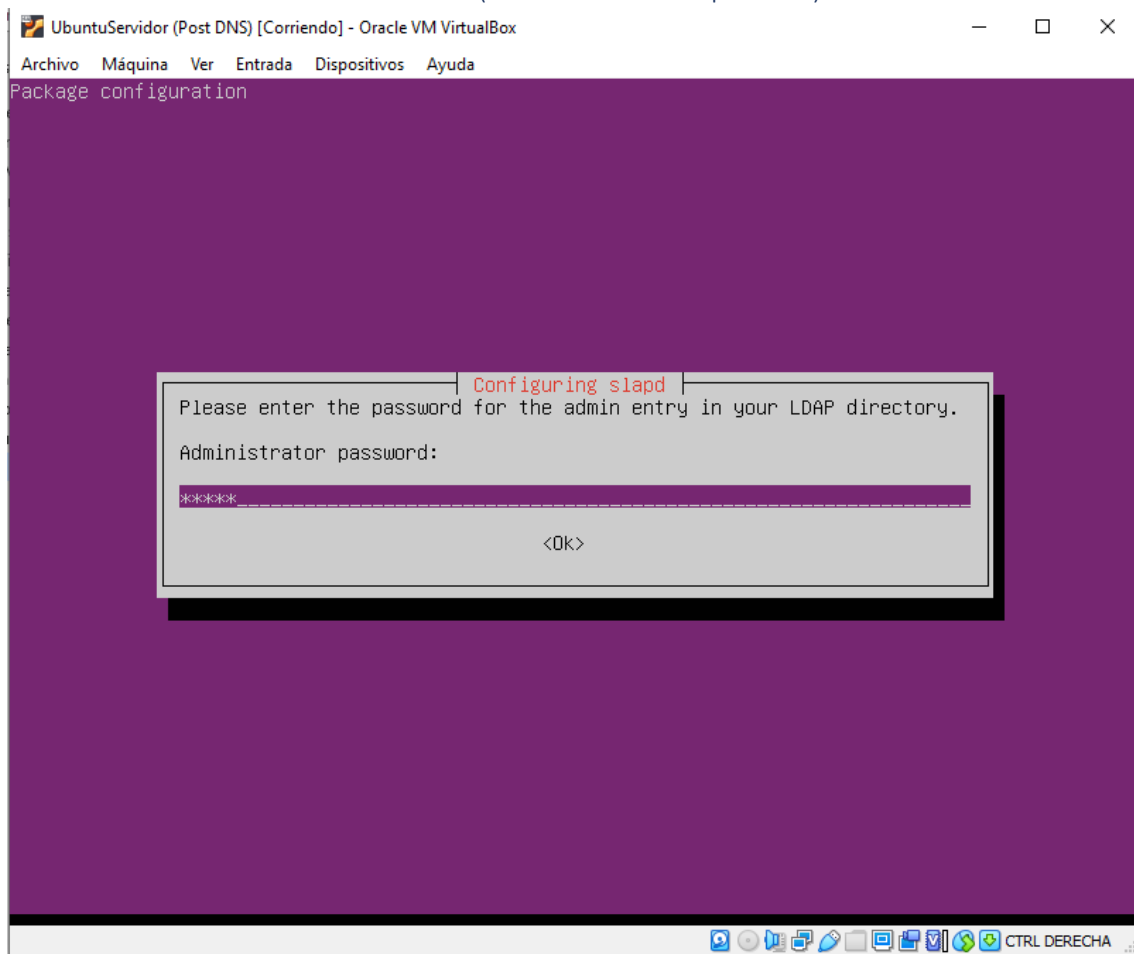
```
iker@iker-servidor:/etc/bind$ nmap 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-14 17:25 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000070s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
82/tcp    open  xfer
389/tcp    open  ldap
3306/tcp   open  mysql
8080/tcp   open  http-proxy
10000/tcp  open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
iker@iker-servidor:/etc/bind$ _
```

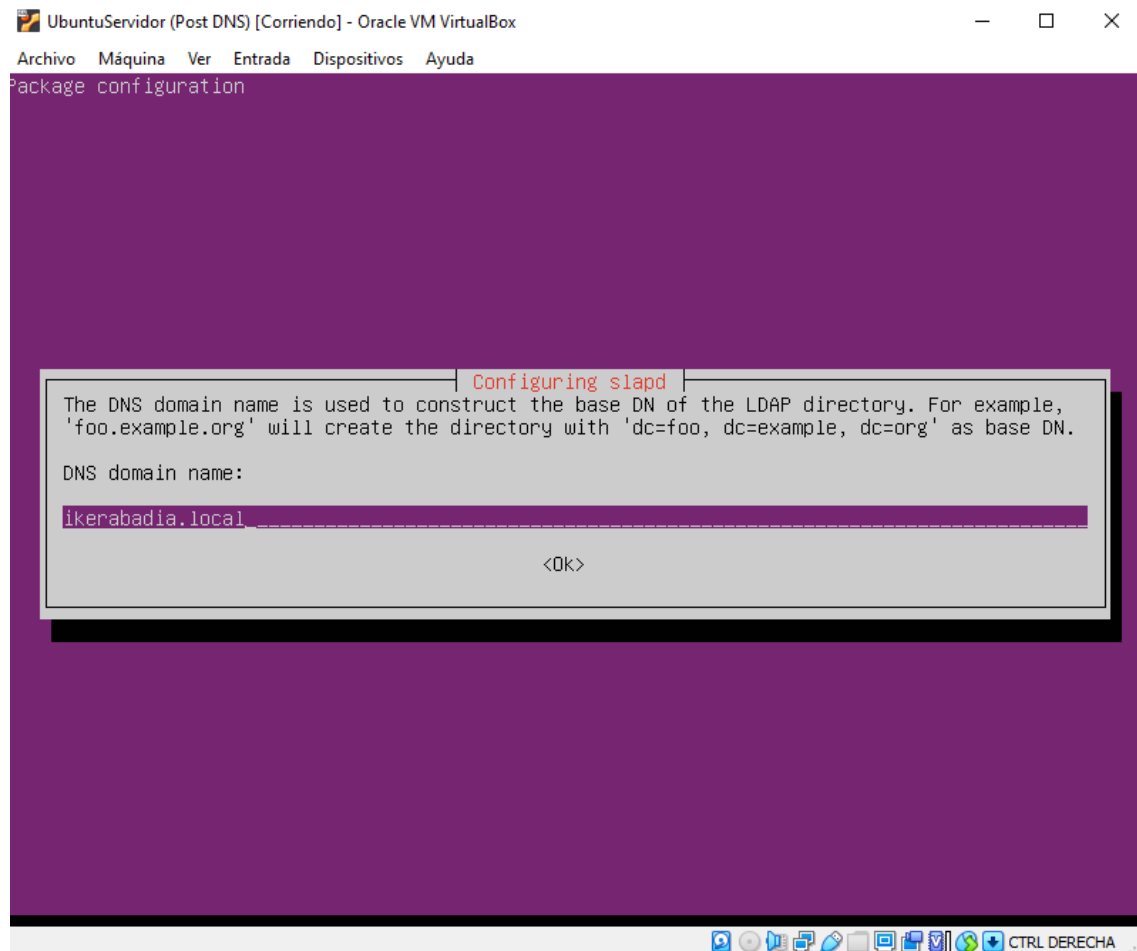
b. Configuraremos el servicio con dpkg-reconfigure slapd

i. Los valores por defecto respétalos

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



iii. Como dominio pon ikerabadia.local



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

```
iker@iker-servidor:/etc/bind$ sudo slapcat
dn: dc=ikerabadia,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: nodomain
dc: ikerabadia
structuralObjectClass: organization
entryUUID: b9ee7854-c160-103b-8025-63aa2804bfb4
creatorsName: cn=admin,dc=ikerabadia,dc=local
createTimestamp: 20211014173428Z
entryCSN: 20211014173428.1362782#000000#000#000000
modifiersName: cn=admin,dc=ikerabadia,dc=local
modifyTimestamp: 20211014173428Z

dn: cn=admin,dc=ikerabadia,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9K2JNzkFuc11GbnFYbXBuZ05wZ1JFSStnakV0ajJV0FM=
structuralObjectClass: organizationalRole
entryUUID: b9eec502-c160-103b-8026-63aa2804bfb4
creatorsName: cn=admin,dc=ikerabadia,dc=local
createTimestamp: 20211014173428Z
entryCSN: 20211014173428.1382812#000000#000#000000
modifiersName: cn=admin,dc=ikerabadia,dc=local
modifyTimestamp: 20211014173428Z

iker@iker-servidor:/etc/bind$
```

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

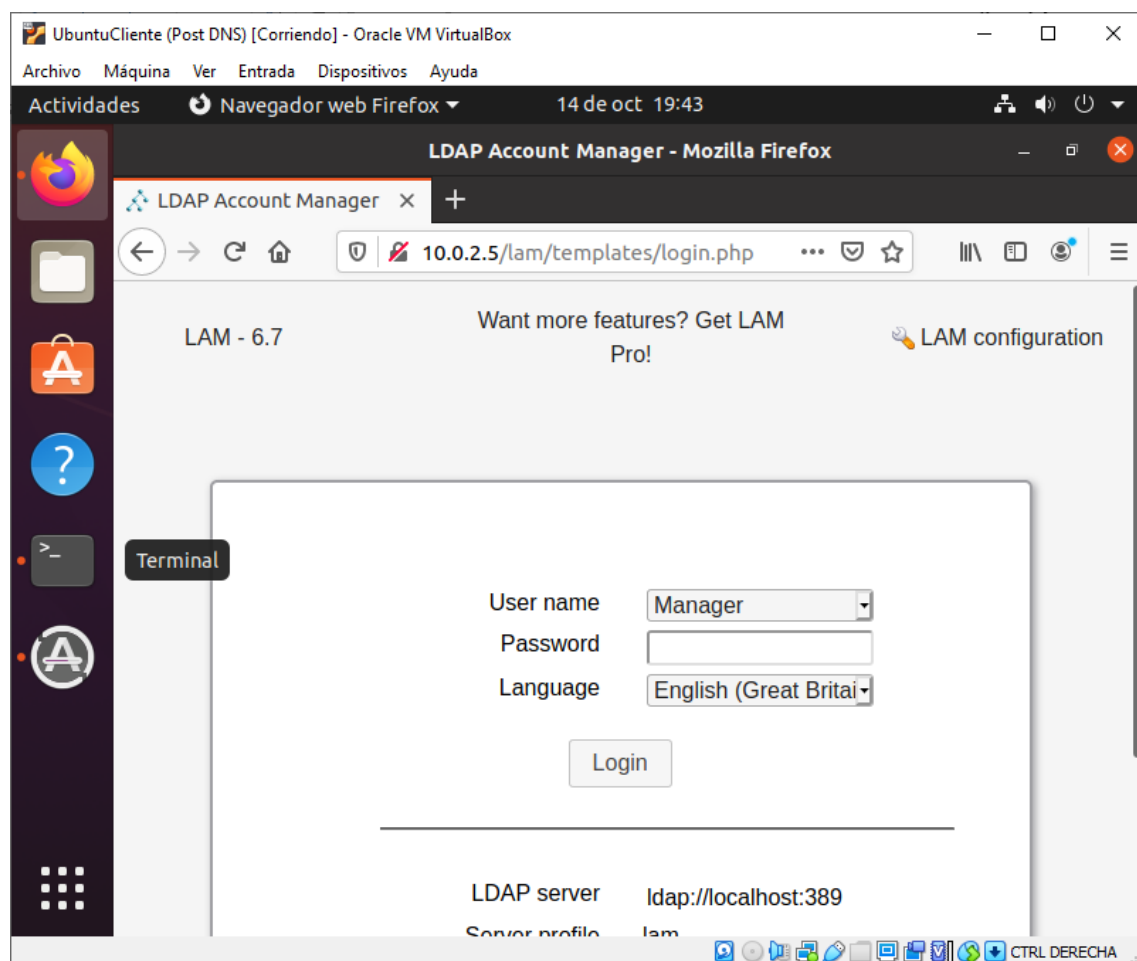
```
Enabling conf ldap-account-manager.  
Setting up php-ldap (2:7.4+75) ...  
Processing triggers for fontconfig (2.13.1-2ubuntu3) ...  
Processing triggers for libapache2-mod-php7.4 (7.4.3-4ubuntu2.6) ...  
Processing triggers for php7.4-cli (7.4.3-4ubuntu2.6) ...  
iker@iker-servidor:/etc/bind$ sudo apt install ldap-account-manager_
```

b. reinicio del servicio de apache

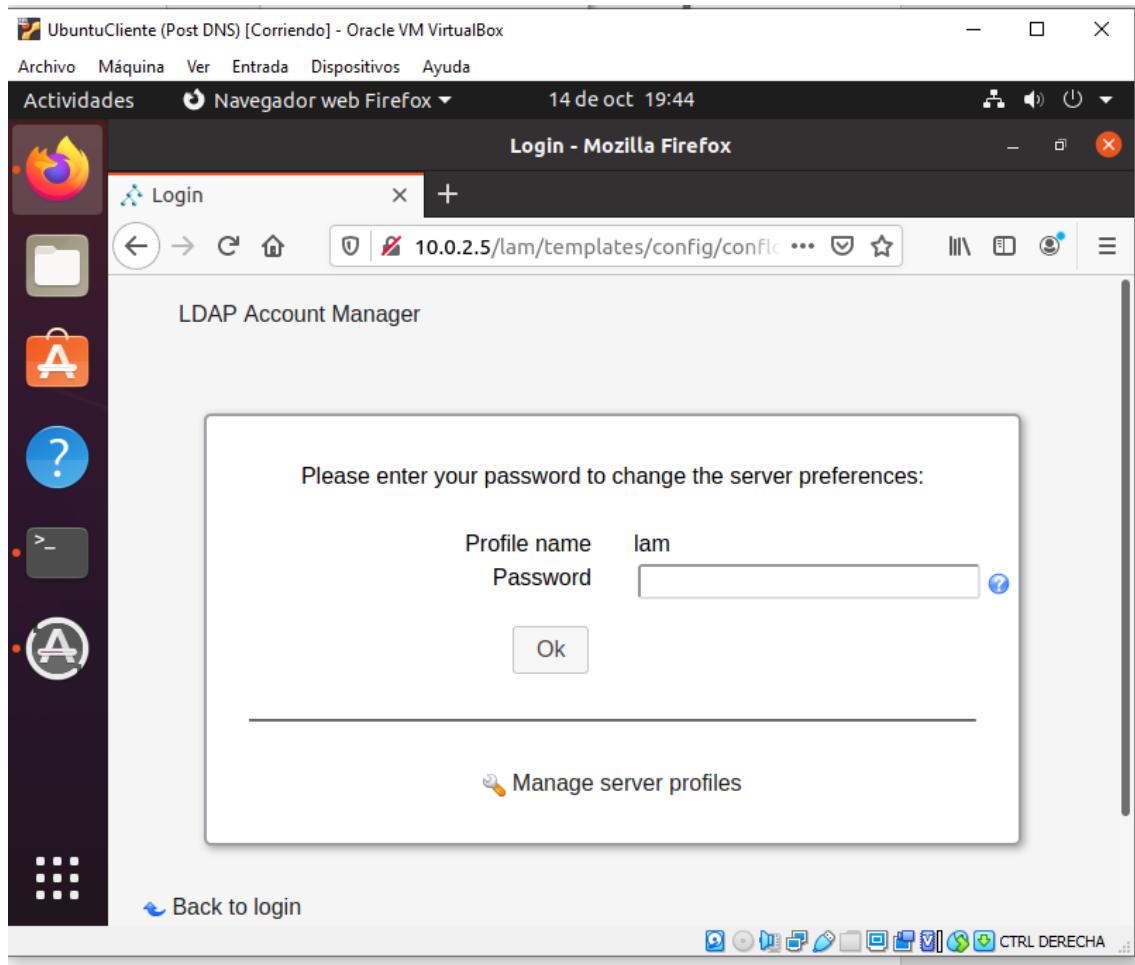
```
iker@iker-servidor:/etc/bind$ systemctl restart apache2  
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====  
Authentication is required to restart 'apache2.service'.  
Authenticating as: iker  
Password:  
==== AUTHENTICATION COMPLETE ====  
iker@iker-servidor:/etc/bind$
```

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

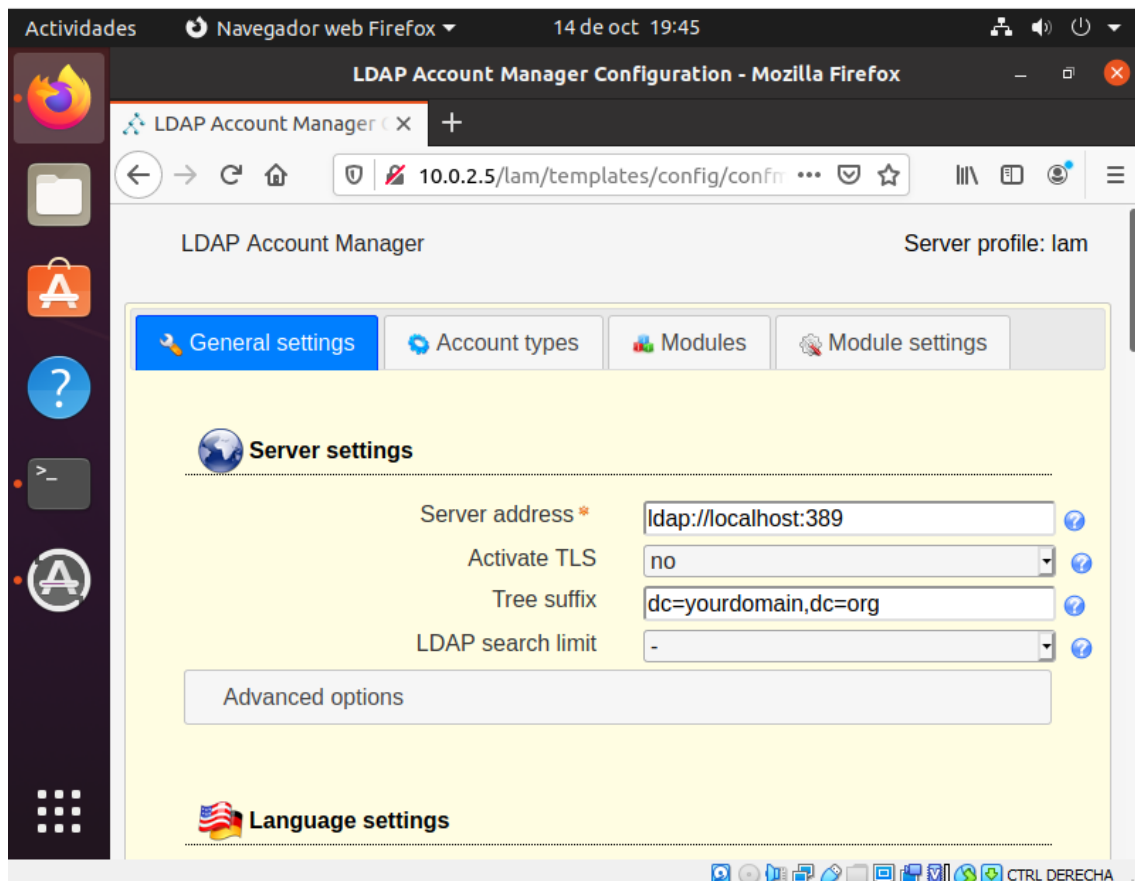
Hay que hacerlo desde el cliente poniendo ipservidor/lam



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

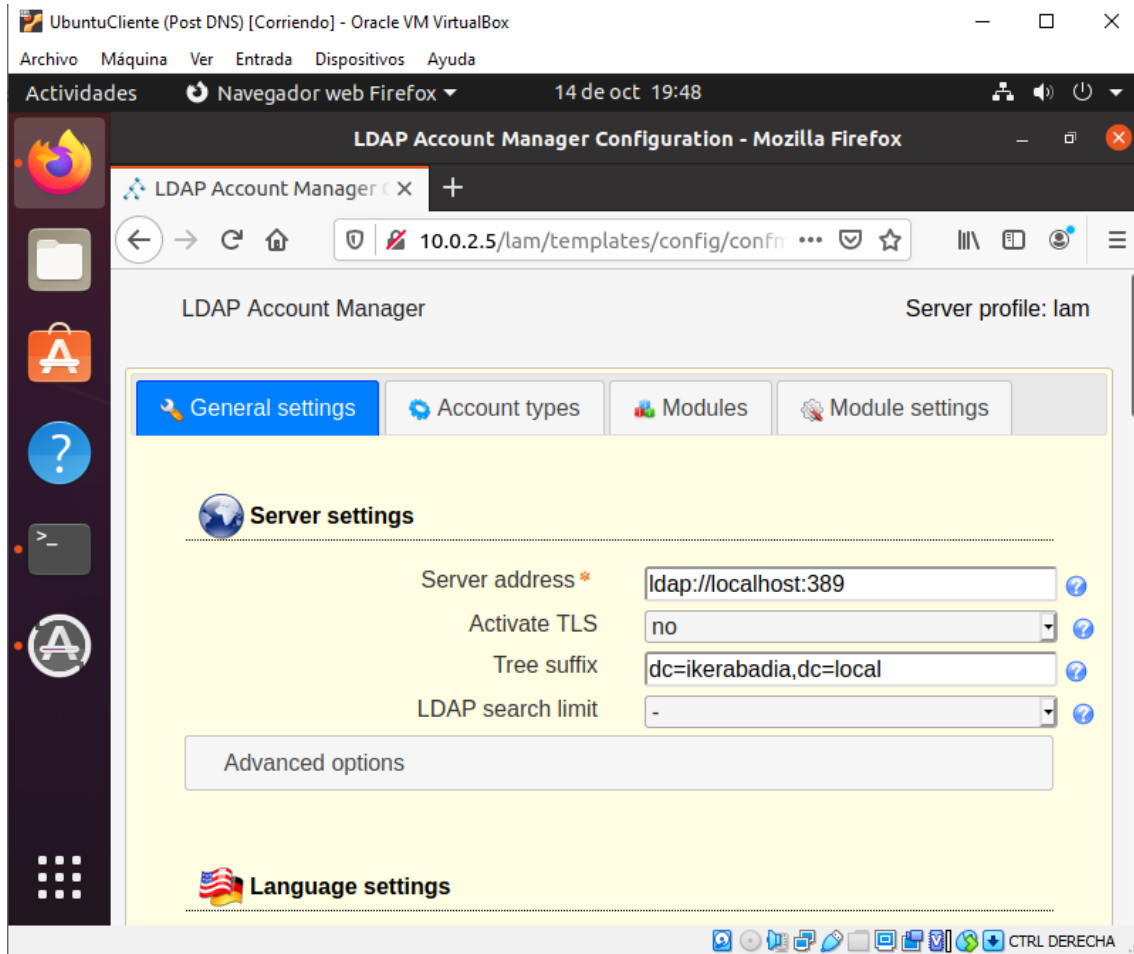


e. Nos pedirá la contraseña maestra, es “lam”



f. En la pestaña de configuración general:

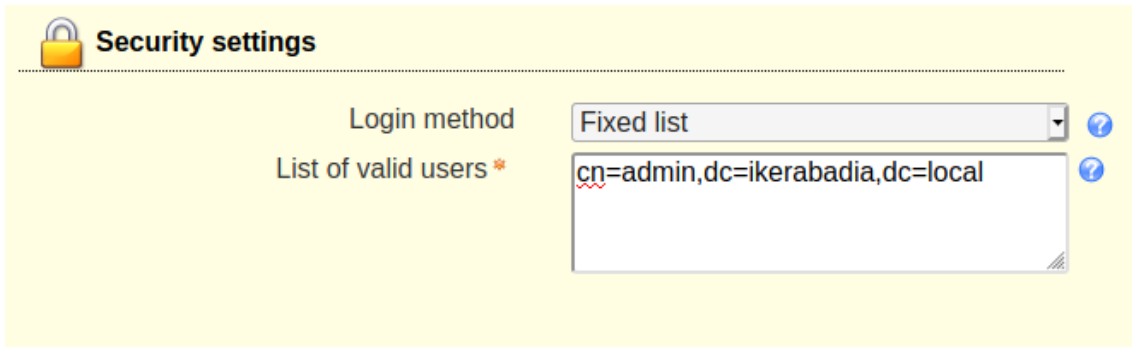
i. Preferencias del servidor: Sufijo del árbol ponemos nuestro dominio. Ej: dc=raulbonachia, dc=local



ii. Configuración del idioma español



iii. En preferencias del sistema (security settings) indicamos cn=admin, dc=ikerabadia, dc=local

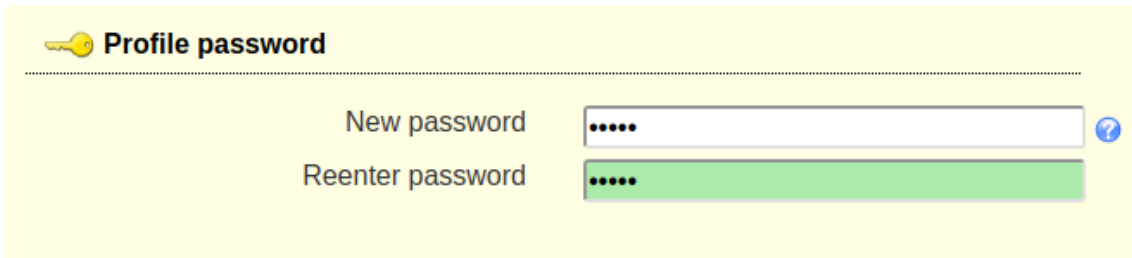


Security settings

Login method: Fixed list

List of valid users: cn=admin,dc=ikerabadia,dc=local

iv. En Profile password ponemos admin



Profile password

New password:

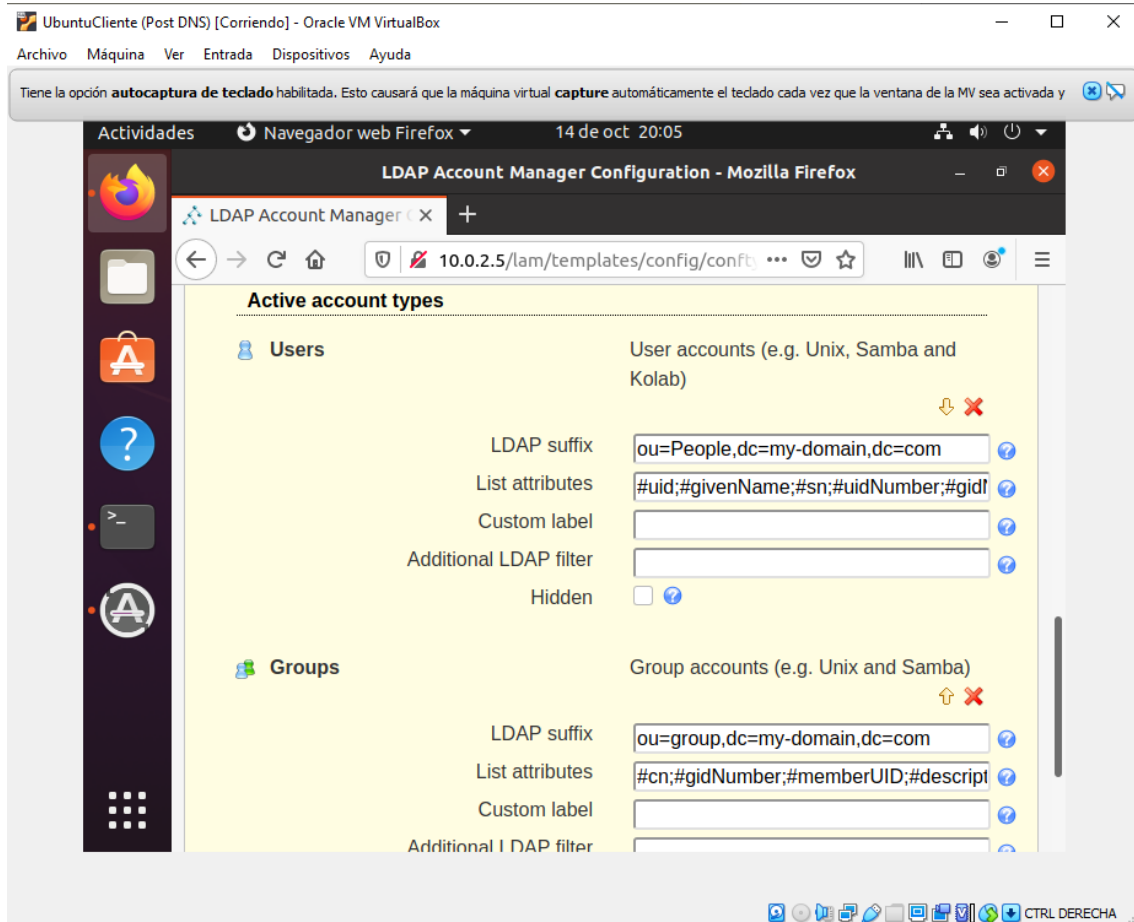
Reenter password:

v. Le damos a Guardar

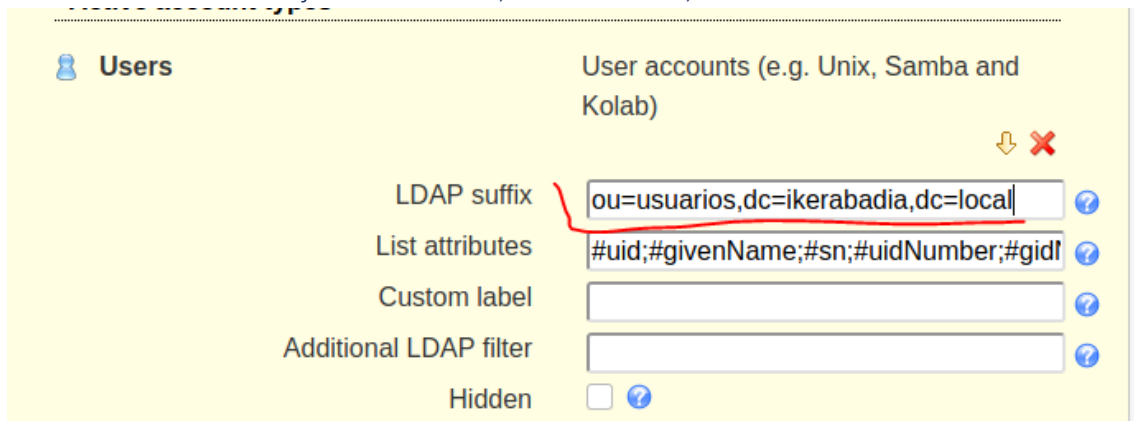
g. En la pestaña de Tipos de Cuentas:

Para ir a ella desde el login: LAM configuration -> Edit server profiles -> Account types

i. Hay dos unidades organizativas, usuarios y grupos



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



iii. Para grupos de sufijo:

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

The screenshot shows the 'Groups' configuration page. On the left, there is a sidebar with a 'Groups' icon and label. The main area is titled 'Group accounts (e.g. Unix and Samba)' and contains several input fields: 'LDAP suffix' with the value 'ou=grupos,dc=ikerabadia,dc=local' (highlighted with a red line), 'List attributes' with the value '#cn;#gidNumber;#memberUID;#descript', 'Custom label' (empty), 'Additional LDAP filter' (empty), and a 'Hidden' checkbox which is unchecked. There are up and down arrows and a red 'X' icon at the top right of the main area.

v. Agrega una nueva unidad organizativa para Equipos (Hosts) con sufijos:

ou=equipos,dc=,dc=local

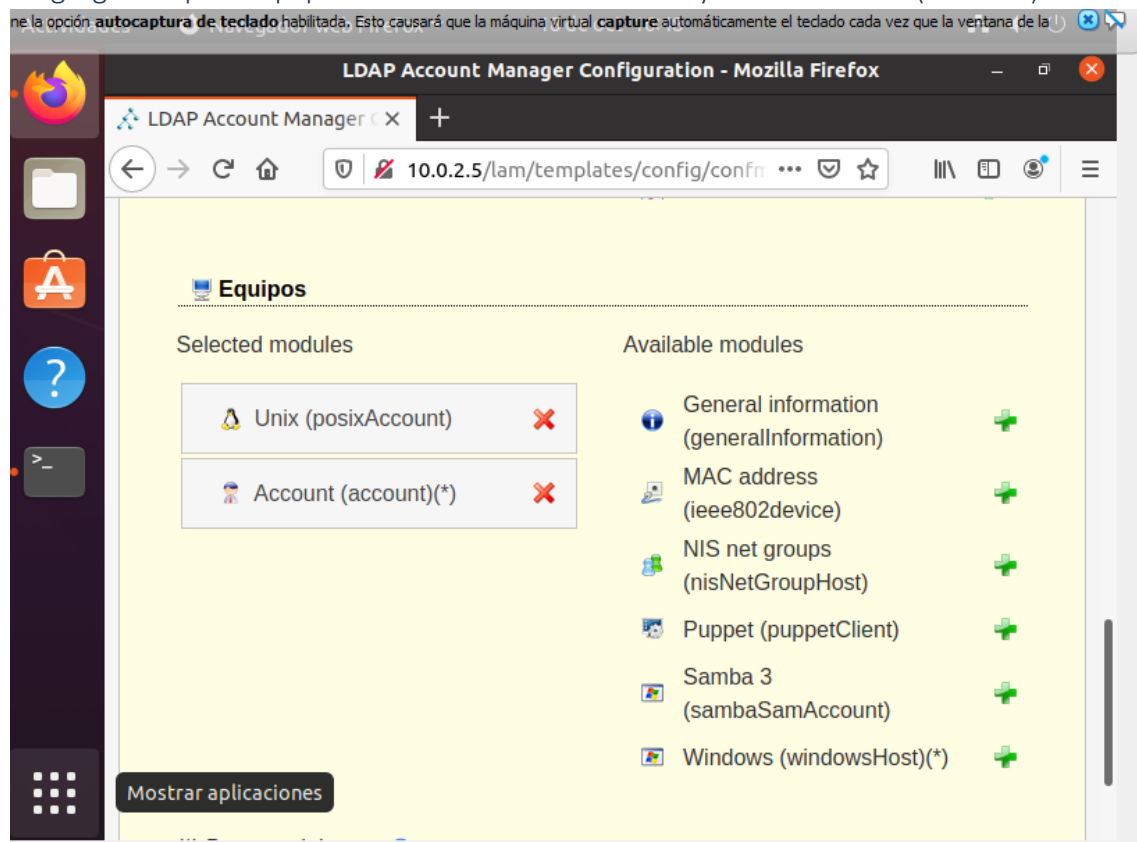
The screenshot shows the 'Hosts' configuration page. On the left, there is a sidebar with a 'Hosts' icon and label. The main area is titled 'Host accounts (e.g. Samba)' and contains several input fields: 'LDAP suffix' with the value 'ou=equipos,dc=ikerabadia,dc=local', 'List attributes' with the value '#cn;#description;#uidNumber;#gidNumb', 'Custom label' with the value 'Equipos', 'Additional LDAP filter' (empty), and a 'Hidden' checkbox which is unchecked. There are up and down arrows and a red 'X' icon at the top right of the main area.

vi. Le damos a Guardar

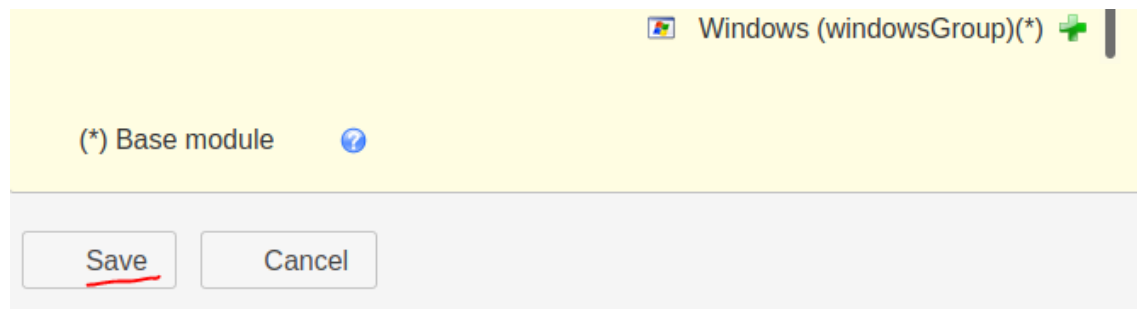
The screenshot shows the 'usuarios' module settings page. At the top, there is a navigation bar with four tabs: 'General settings', 'Account types', 'Modules' (which is active and highlighted in blue), and 'Module settings'. Below the navigation bar, the page is titled 'usuarios'. It is divided into two main sections: 'Selected modules' and 'Available modules'. The 'Selected modules' section contains three items: 'Personal (inetOrgPerson)(*)', 'Unix (posixAccount)', and 'Shadow (shadowAccount)', each with a red 'X' icon to its right. The 'Available modules' section contains a list of modules with a green plus icon to its right: 'Account (account)(*)', 'Asterisk (asteriskAccount)', 'Asterisk voicemail (asteriskVoicemail)', 'Authorized Services (authorizedServiceObject)', 'Courier (courierMailAccount)', and 'EDU person (eduPerson)'.

h. En la pestaña de Módulos:

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



ii. Le damos a Guardar



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

Your settings were successfully saved.
lam

User name

admin

Password

.....

Language

Español (España)

Login

LDAP Account Manager - 6.7 (Logged in as: admin)

Tools Help Logout

Tree view

usuarios

grupos

Equipos

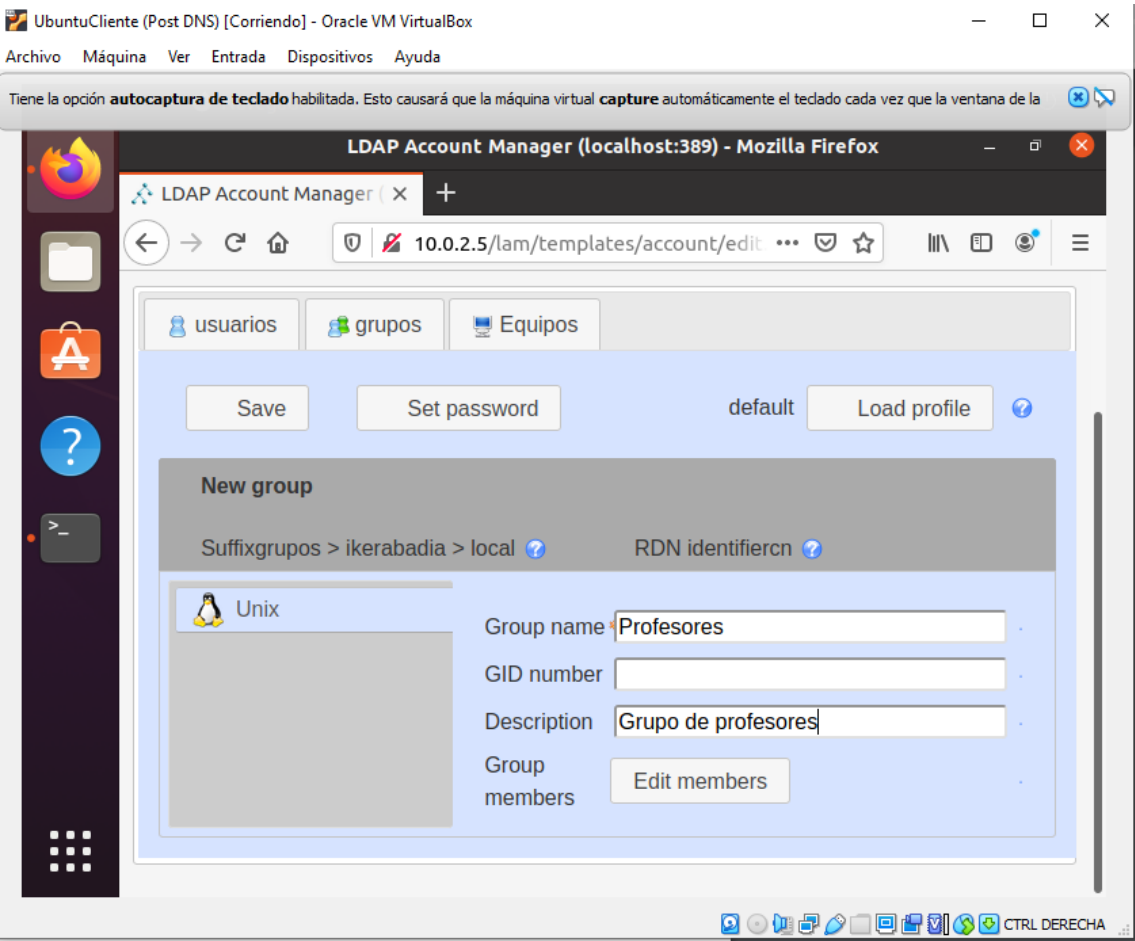
New user

File upload





User count: 0

Actions	User name	First name	Last name	UID number	GID number
Sort sequence					


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





Group count: 2


Actions	Group name	GID number	Group members	Group description
Sort sequence	▼▲	▼▲	▼▲	▼▲
<input type="checkbox"/> Filtre	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>  	Alumnos	10001		Grupo de alumnos
<input type="checkbox"/>  	Profesores	10000		Grupo de profesores


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.


 The new password will be stored in the directory after you save this account.

Profesor 01

Suffixusuarios > ikerabadia > local  RDN identifier **cn** 

 Personal

 Unix

 Shadow

First name

Profesor

Last name *

01

Initials




Description



Address


ene la opción **autocaptura de teclado** habilitada. Esto causará que la máquina virtual **capture** automáticamente el teclado cada vez que la ventana de la


LDAP Account Manager (localhost:389) - Mozilla Firefox


LDAP Account Manager | X +

10.0.2.5/lam/templates/account/edit ...   

Suffixusuarios > ikerabadia > local  RDN identifier **cn** 

 Personal

 Unix

 Shadow


Invalid configuration detected. Please edit your server profile (module settings) and fill all required fields.

User name *

profesor01

Common name

Profesor 01



UID number

10000

Gecos

Primary group



Profesores

Additional groups

Edit groups

Home directory *

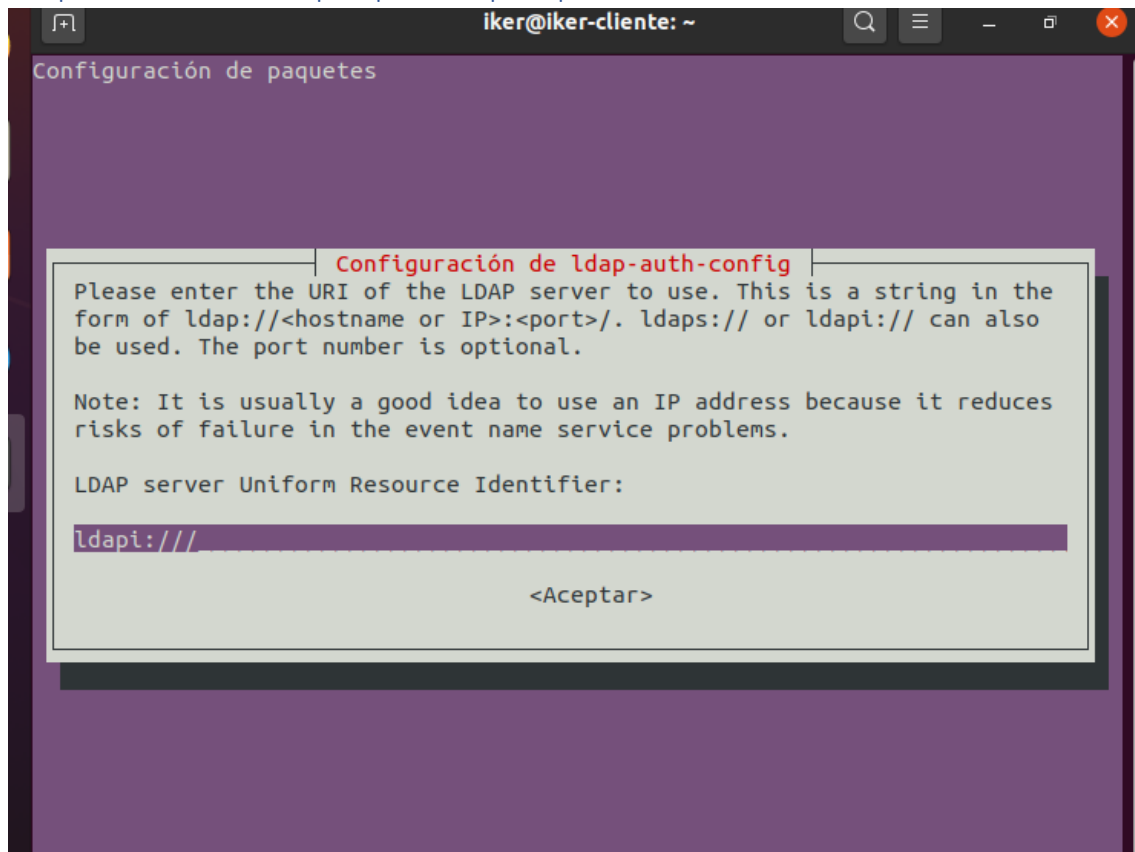
/home/profesor01

<input type="checkbox"/>	 	profesor01	Profesor	01	10000	10000
--------------------------	---	------------	----------	----	-------	-------

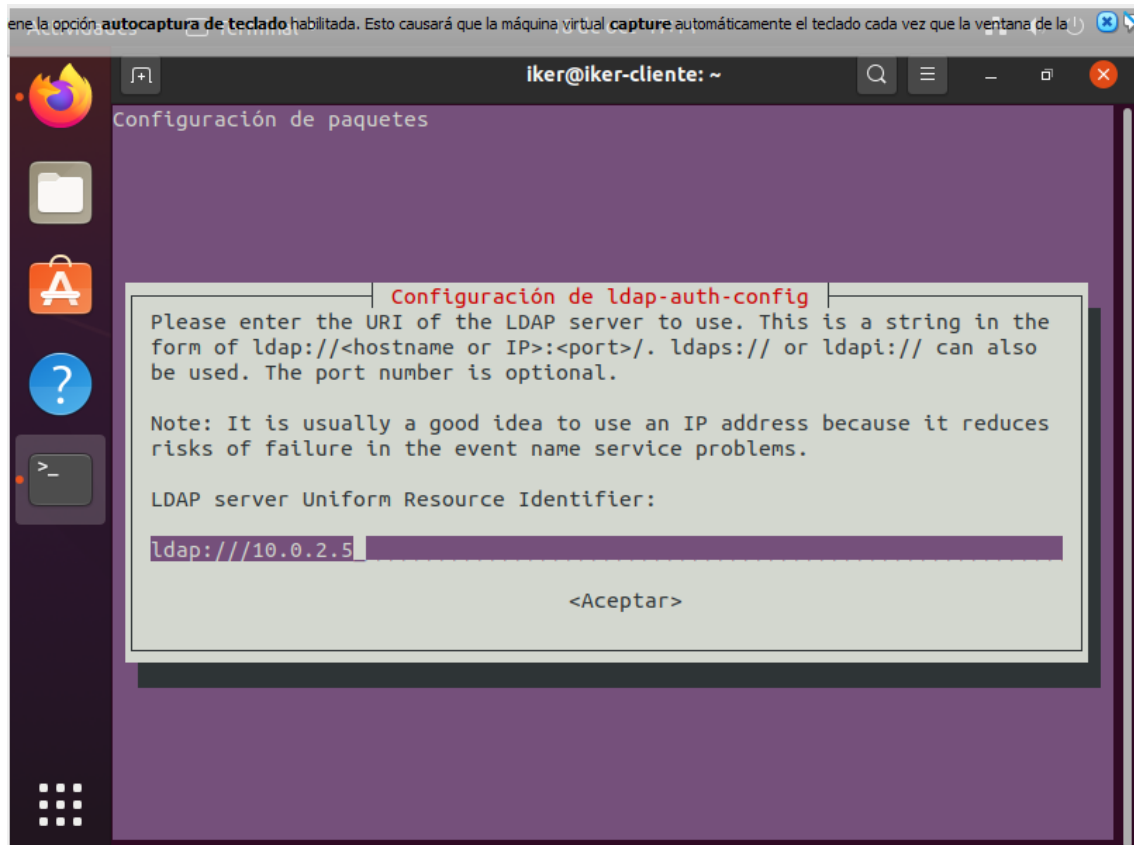
F) Ahora tendremos que crear un cliente que haga uso del servidor LDAP. Usaremos un Ubuntu Desktop nuevo conectado a la red nat de nuestro servidor.

Voy a usar el que he usado hasta ahora

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

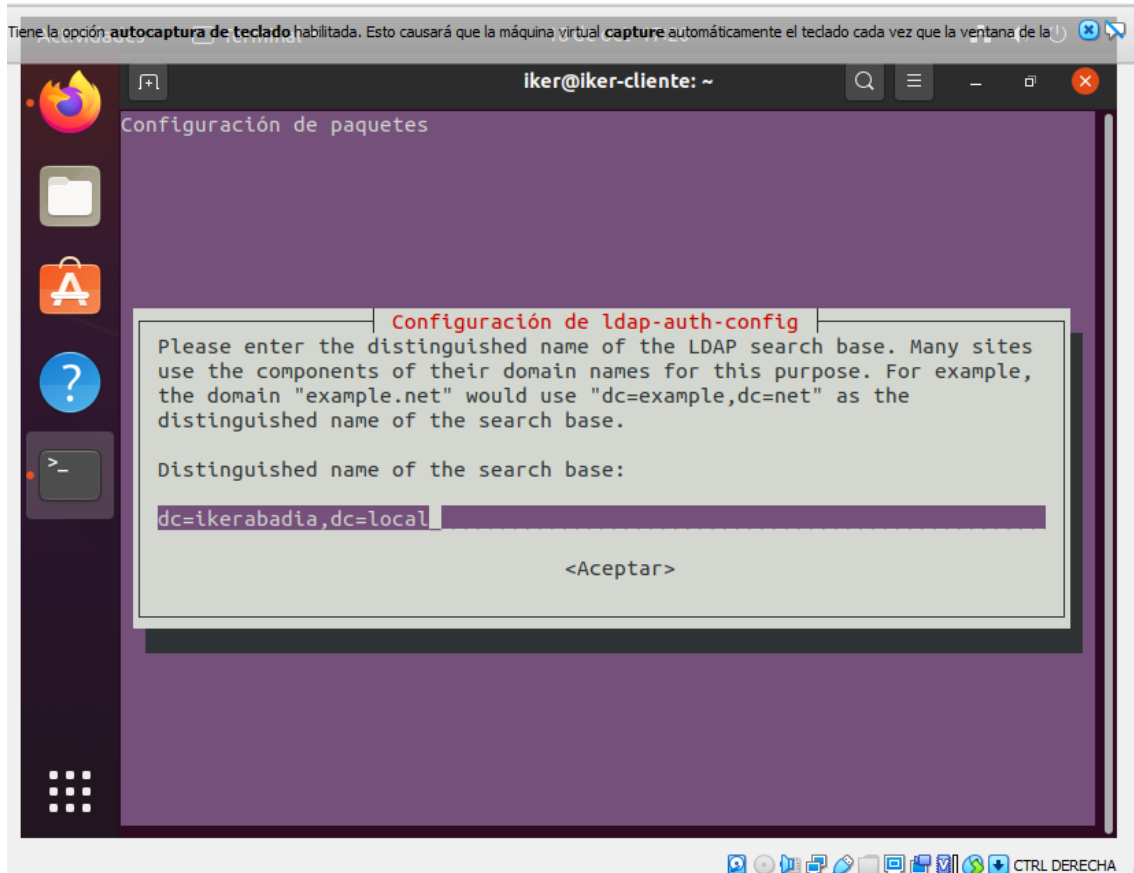


b. Nos pedirá el LDAP server URI: poner ldap://IPSERVERIDOR

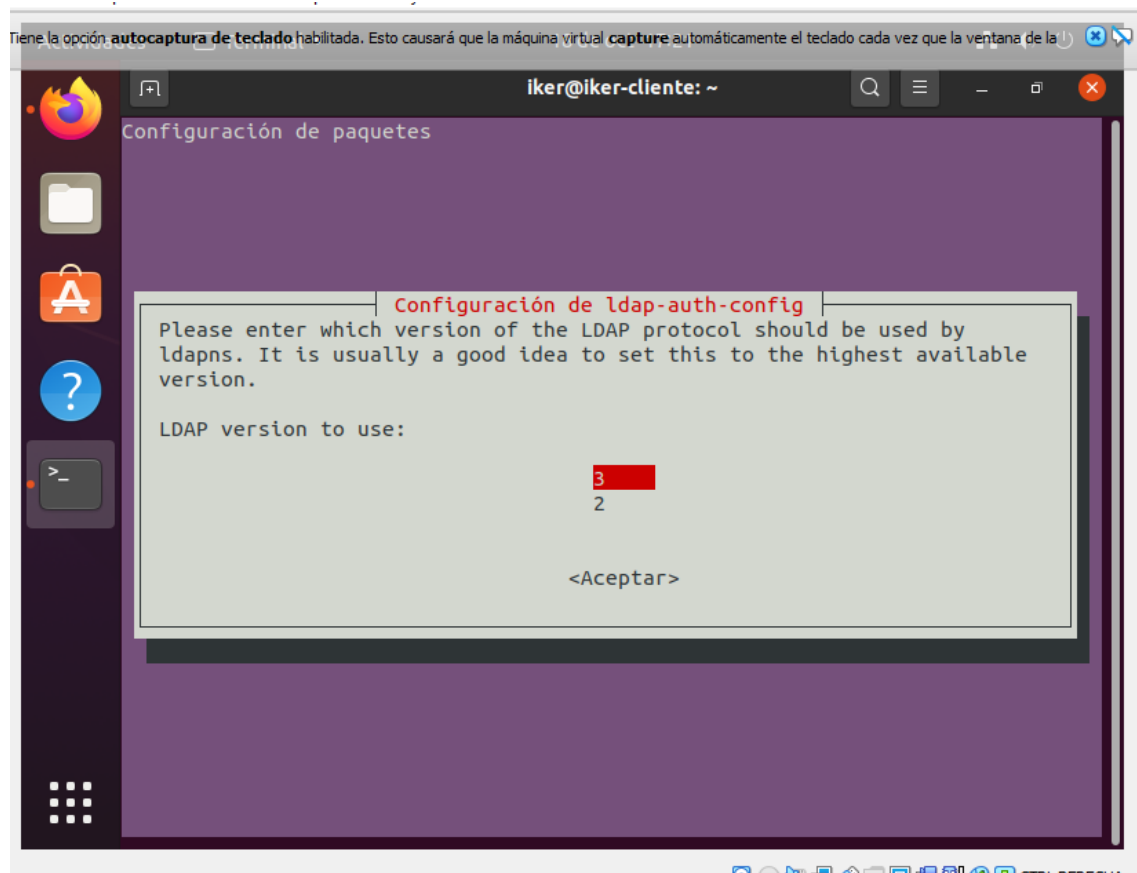


**IMPORTANTE PONER SOLO DOS BARRAS “//”
NO TRES COMO PONE EN LA CAPTURA.**

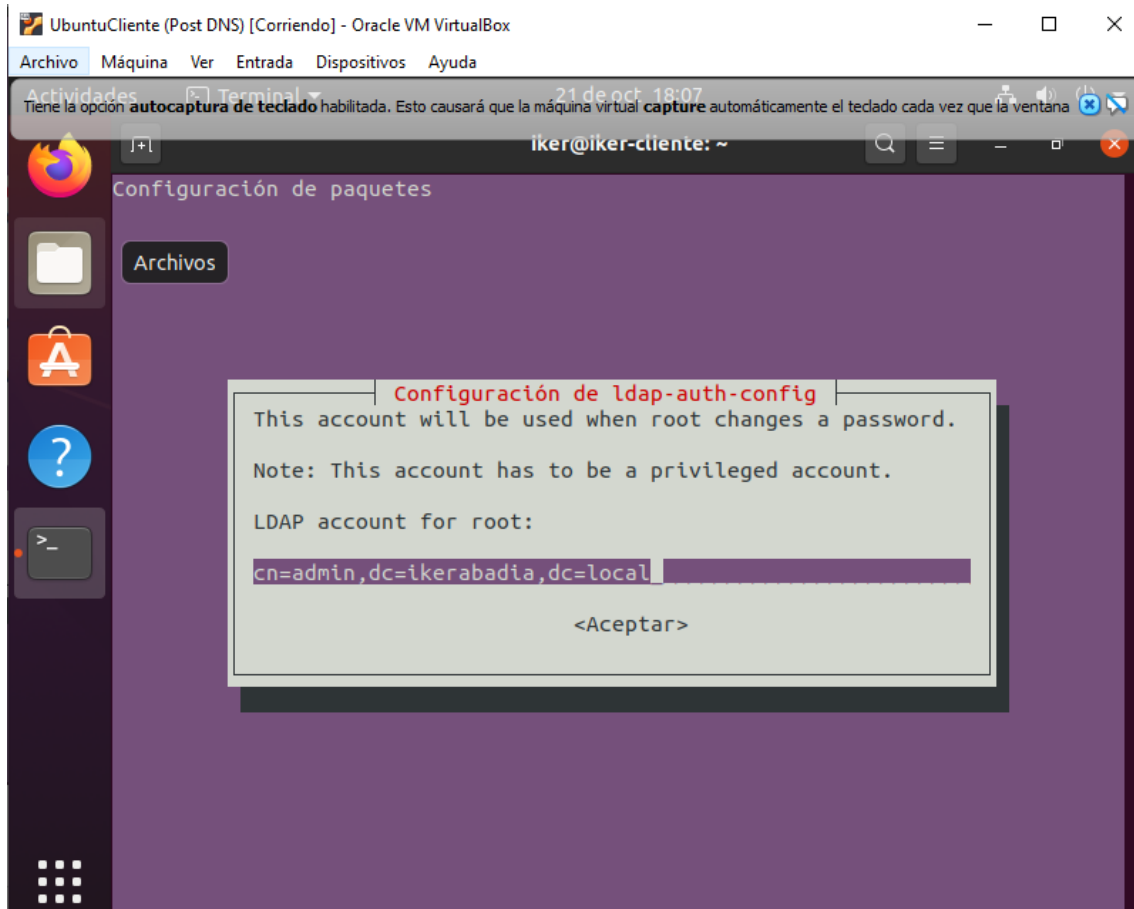
c. Para la búsqueda base: dc=ikerabadia, dc=local, que es la raíz del árbol de nuestro directorio en el servidor



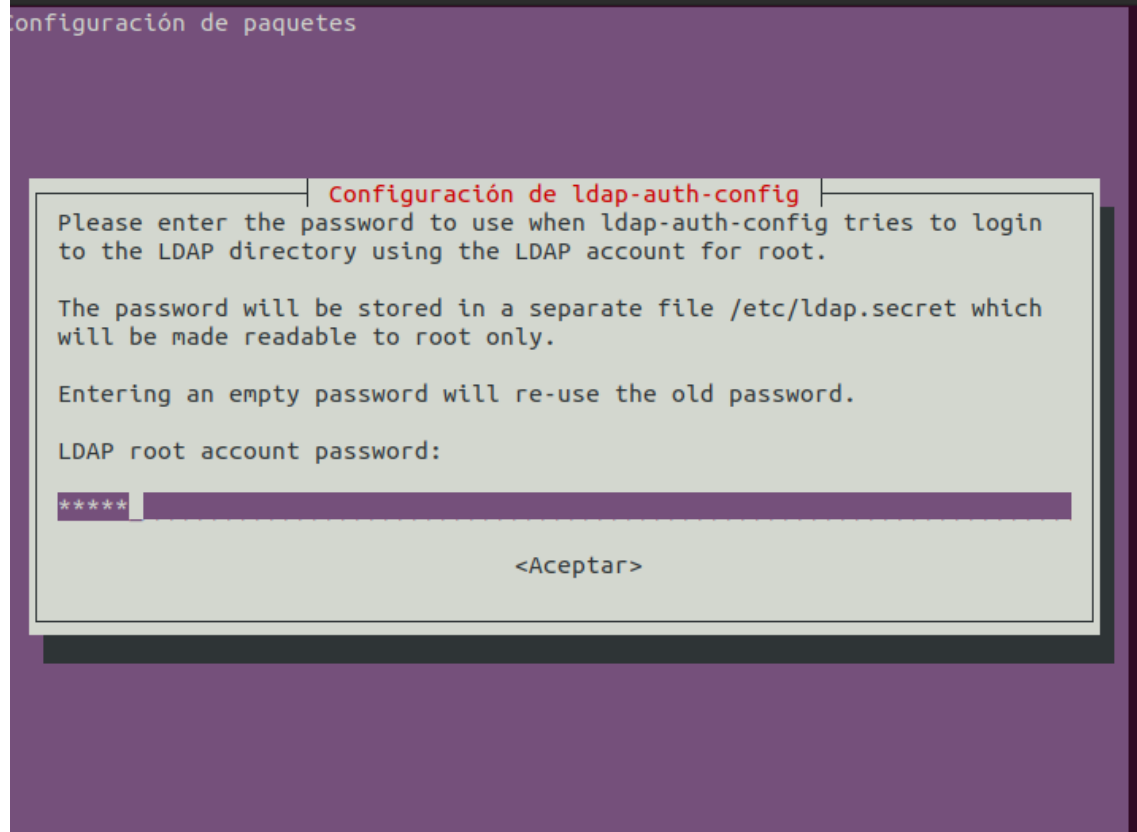
d. Versión de LDAP, la 3



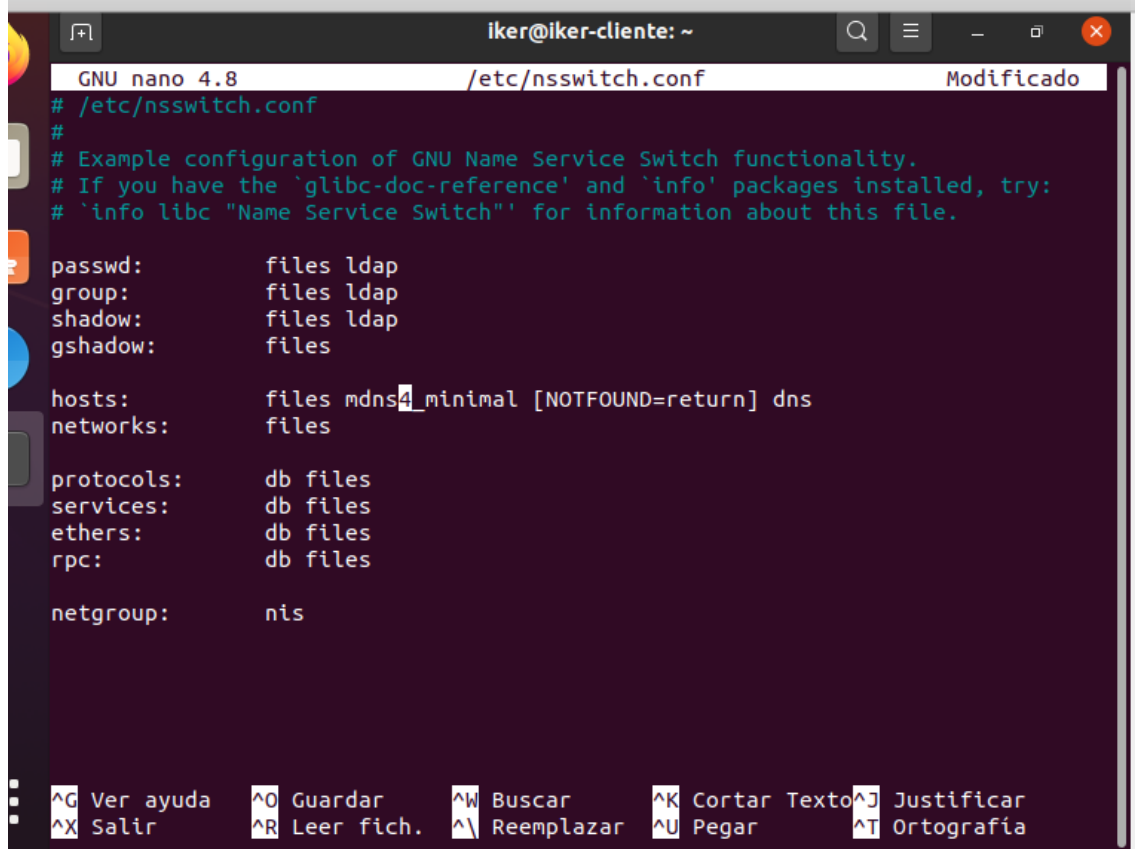
e. En el resto de pantallas dejamos las opciones por defecto hasta llegar a la pantalla que nos pide LDAP account for root, que introduciremos: cn=admin, dc=ikerabadia, dc=local



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 logear, (querremos que use LDAP) quedando así:



```
GNU nano 4.8 /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:      files ldap
group:       files ldap
shadow:      files ldap
gshadow:     files

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

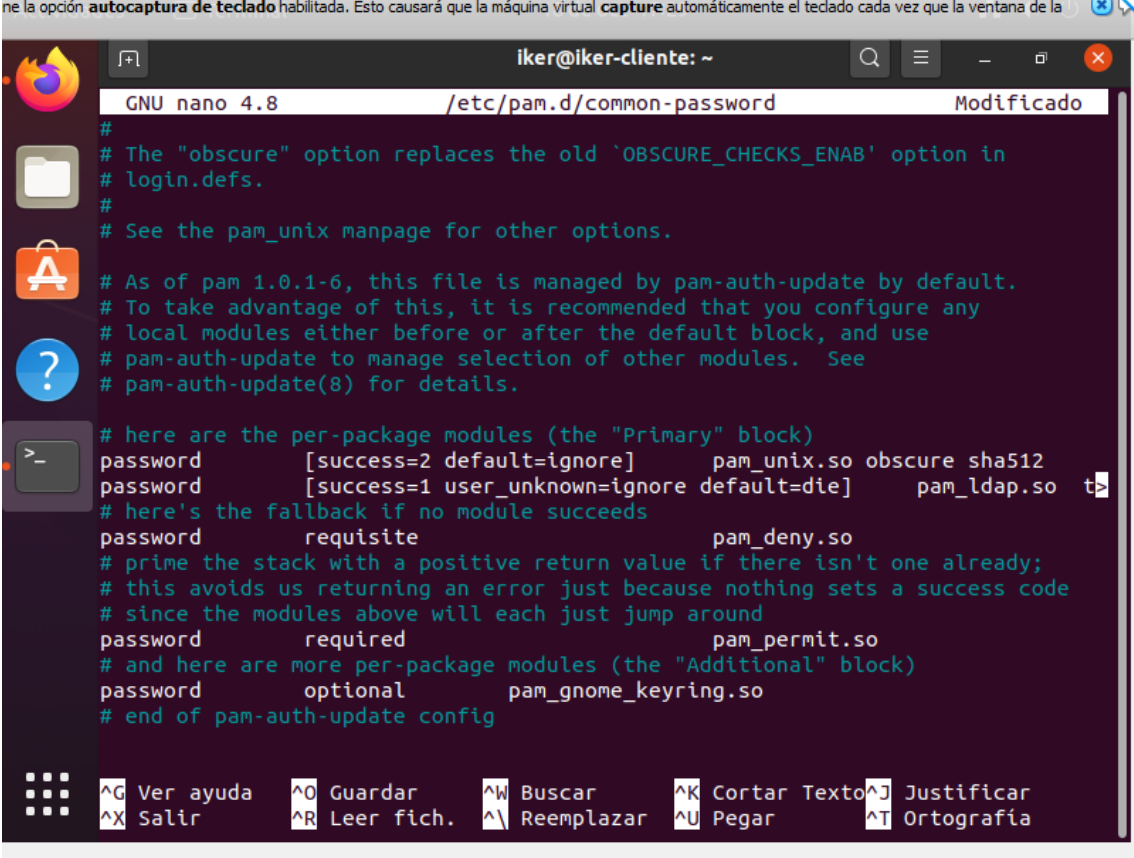
protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis

^G Ver ayuda  ^O Guardar   ^W Buscar    ^K Cortar Texto ^J Justificar
^X Salir      ^R Leer fich.^_ Reemplazar ^U Pegar      ^T Ortografía
```

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

ne la opción **autocaptura de teclado** habilitada. Esto causará que la máquina virtual **capture** automáticamente el teclado cada vez que la ventana de la



```
iker@iker-cliente: ~
GNU nano 4.8 /etc/pam.d/common-password Modificado
#
# The "obscure" option replaces the old 'OBSCURE_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
# 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

^G Ver ayuda  ^O Guardar   ^W Buscar    ^K Cortar Texto ^J Justificar
^X Salir      ^R Leer fich.^_ Reemplazar ^U Pegar       ^T Ortografia
```

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_mkhome.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=ikerabadia, 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:


```

+
iker@iker-cliente:~$ ldapsearch -x -H ldap://10.0.2.5 -b "dc=ikerabadia, dc=local" -s sub
# extended LDIF
#
# LDAPv3
# base <dc=ikerabadia, dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# ikerabadia.local
dn: dc=ikerabadia,dc=local
objectClass: top
objectClass: dcObject

```

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.

```

Ubuntu 20.04.1 LTS iker-cliente tty2
iker-cliente login: profesor01
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.11.0-34-generic x86_64)

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

443 updates can be installed immediately.
214 of these updates are security updates.
Para ver estas actualizaciones adicionales ejecute: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.

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.

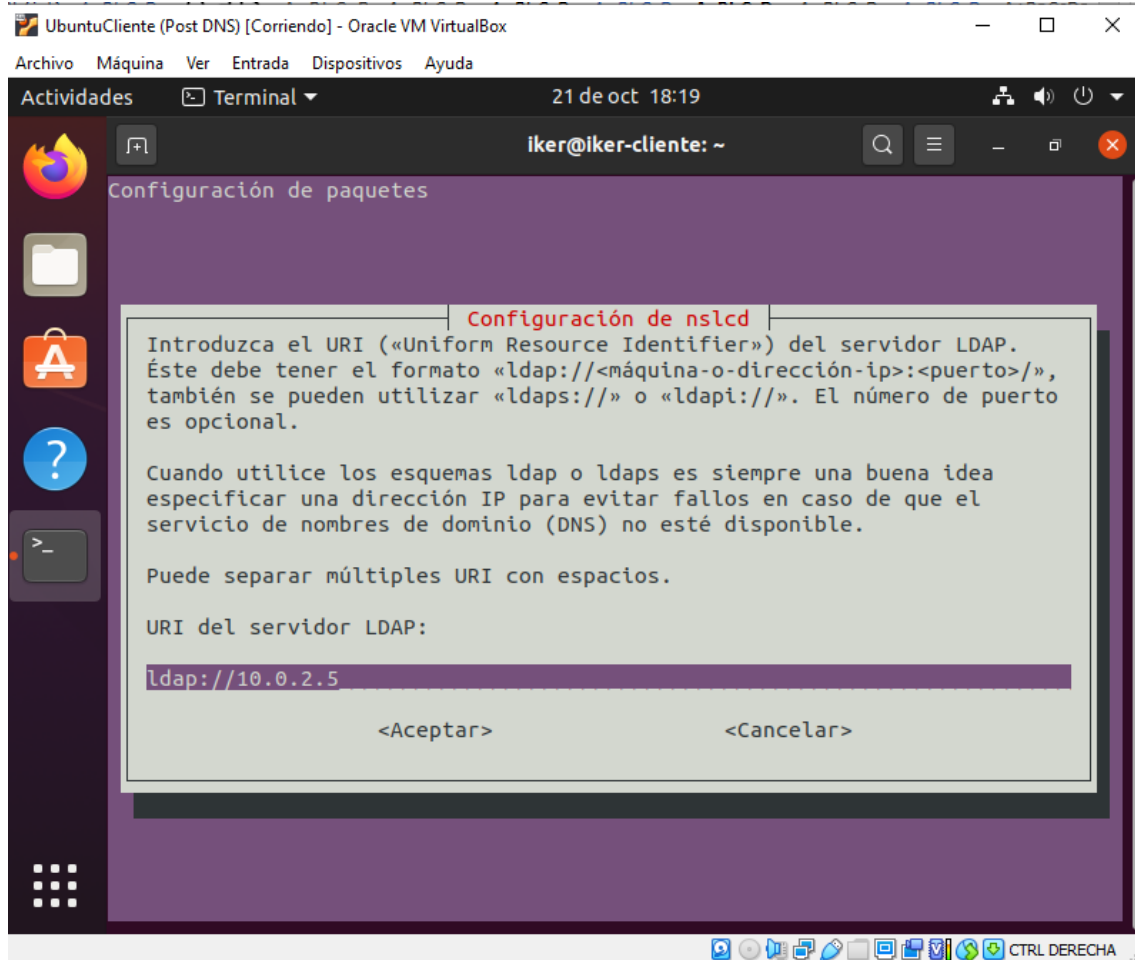
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Creating directory '/home/profesor01'.
profesor01@iker-cliente:~$ _

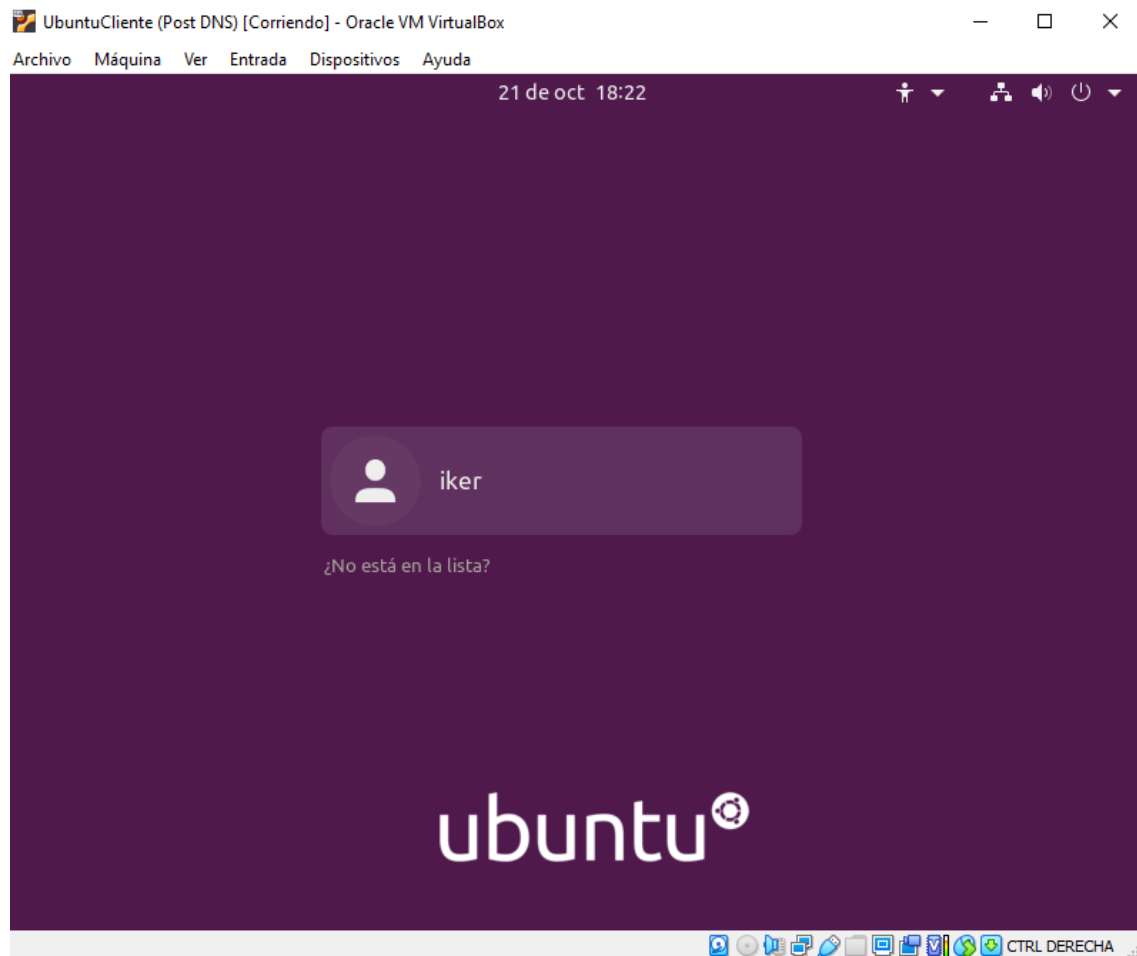
```

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.

