P06- SERVIDOR LDAP

ANA OROZCO ASENSIO

2ºASIR
I.E.S. ANTONIO MACHADO
ASO

Contenido

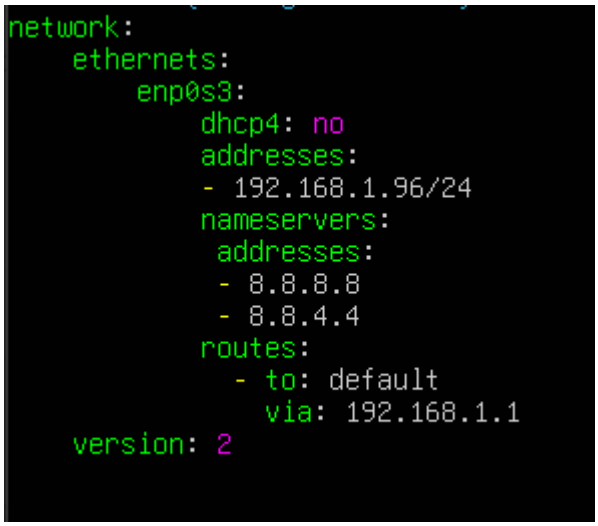
Introducción.

En esta práctica vamos a instalar servidor LDAP en una máquina Ubuntu Server y gestionarlo desde Webmin.

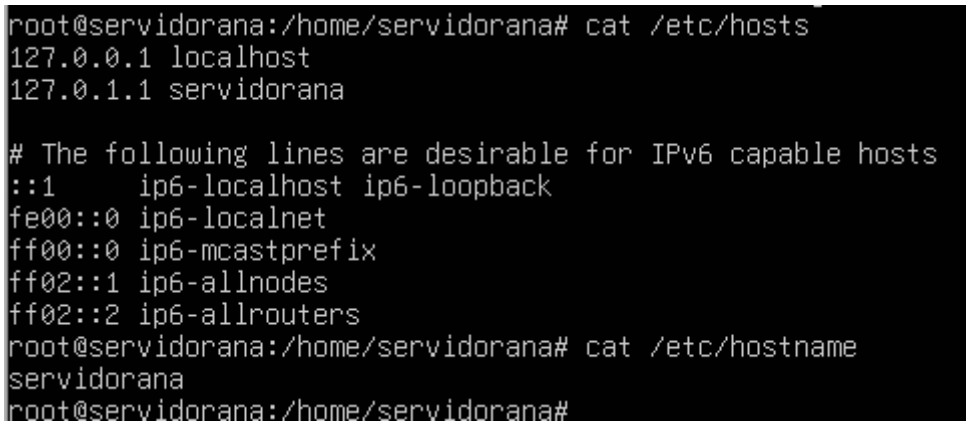
*NOTA: Al estar en mi casa tuve que usar la 192.168.1.0/24

1. Montar las máquinas virtuales. ¿Qué has tenido que modificar?

Primero que todo puse IP al servidor en /etc/netplan/*tabulación*



Y compruebo archivos /etc/hosts y /etc/hostname.



Miré la IP del cliente1:

```
ana@clienteana1:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.97  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::de7d:4e9d:b3a9:5eff  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:4c:87:50  txqueuelen 1000  (Ethernet)
        RX packets 6995  bytes 3653428 (3.6 MB)
        RX errors 0  dropped 30  overruns 0  frame 0
        TX packets 5235  bytes 840728 (840.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Bucle local)
        RX packets 1515  bytes 185722 (185.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1515  bytes 185722 (185.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ana@clienteana1:~$ cat /etc/hostname
clienteana1
```

Y la IP cliente2:

```
C:\Users\clienteana2>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::25f6:30c2:36ca:3a20%5
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.98
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.1.1
```

2. Instalar y configurar un servidor DNS que nos resuelva nuestras direcciones del dominio.

Instalaremos el servidor DNS, y antes actualizaremos

sudo apt-get update

apt-get install bind9 bind9utils

Iniciaré y lo activaré para que se inicie cada vez que se enciende:

```
root@servidorana:/home/servidorana# sudo systemctl start systemd-resolved
root@servidorana:/home/servidorana# sudo systemctl enable systemd-resolved
root@servidorana:/home/servidorana# sudo systemctl status systemd-resolved
● systemd-resolved.service - Network Name Resolution
     Loaded: loaded (/usr/lib/systemd/system/systemd-resolved.service; enabled; preset: enabled)
     Active: active (running) since Thu 2024-12-12 18:45:08 UTC; 6min ago
       Docs: man:systemd-resolved.service(8)
```

Configuraremos los archivos necesarios:

“/etc/bind/named.conf.local”

```
 GNU nano 7.2                                                  /etc/bind/named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "estaesmiclaseana.local" {
        type master;
        file "/var/cache/bind/estaesmiclaseana.local.db";
        };
zone "1.168.192.in-addr.arpa" {
        type master;
        file "/var/cache/bind/192.168.1.db";
        };
```

Y comprobaremos:

```
root@servidorana:/home/servidorana# named-checkconf /etc/bind/named.conf.local
root@servidorana:/home/servidorana#
```

Ahora vamos a crear la zona de configuración directa:

```
 GNU nano 7.2                                          /var/cache/bind/estaesmiclaseana.local.db
$TTL 604800
@ IN SOA        estaesmiclaseana.local. root.estaesmiclaseana.local. (
                                        2         ; Serial
                                        604800    ; Refresh
                                        86400     ; Retry
                                        2419200   ; Expire
                                        604800 ) ; Negative Cache TTL

@               IN      NS      servidorana.estaesmiclaseana.local.
servidorana     IN      A       192.168.1.96
clienteana1     IN      A       192.168.1.97
clienteana2     IN      A       192.168.1.98

dns             IN      CNAME servidorana
ldap            IN      CNAME servidorana
```

NOTA: a partir de aquí realicé la práctica con ssh.

Y la zona indirecta:

```
 GNU nano 7.2                                          /var/cache/bind/192.168.1.db
$TTL 604800
@ IN SOA         estaesmiclaseana.local. root.estaesmiclaseana.local. (
                                                      2         ; Serial
                                                      604800    ; Refresh
                                                      86400     ; Retry
                                                      2419200   ; Expire
                                                      604800 ) ; Default TTL
@       IN      NS      servidorana.estaesmiclaseana.local.
96      IN      PTR     servidorana.estaesmiclaseana.local.
97      IN      PTR     clienteana1.estaesmiclaseana.local.
98      IN      PTR     clienteana2.estaesmiclaseana.local.
```

Vamos a comprobarlo:

```
root@servidorana:/home/servidorana# named-checkzone estaesmiclaseana.local /var/cache/bind/estaesmiclaseana.local.db
zone estaesmiclaseana.local/IN: loaded serial 2
OK
root@servidorana:/home/servidorana# named-checkzone 1.168.192.in-addr.arpa /var/cache/bind/192.168.1.db
zone 1.168.192.in-addr.arpa/IN: loaded serial 2
OK
```

Vamos a modificar este archivo para que en caso de no tener alguna dirección, resuelva a otro servidor:

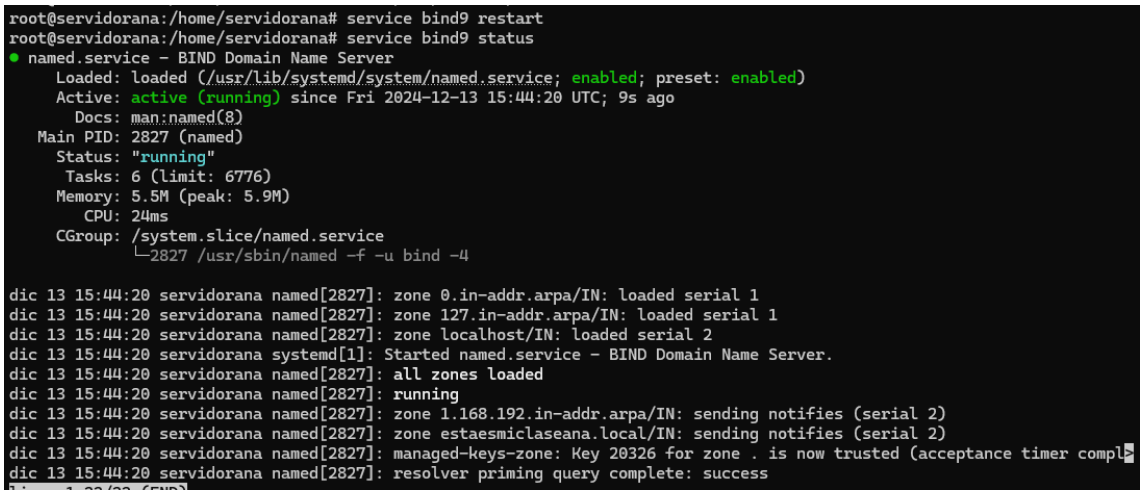
```
 GNU nano 7.2                                  /etc/bind/named.conf.options *
acl safeclients {
        localhost;
        localnets;
};

options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        allow-query { any; };
        allow-recursion { safeclients; };
        allow-query-cache {safeclients; };
         forwarders {
                8.8.8.8;
                8.8.4.4;
         };
```

```
        //========================
        dnssec-validation auto;

        listen-on-v6 { any; };
};
```

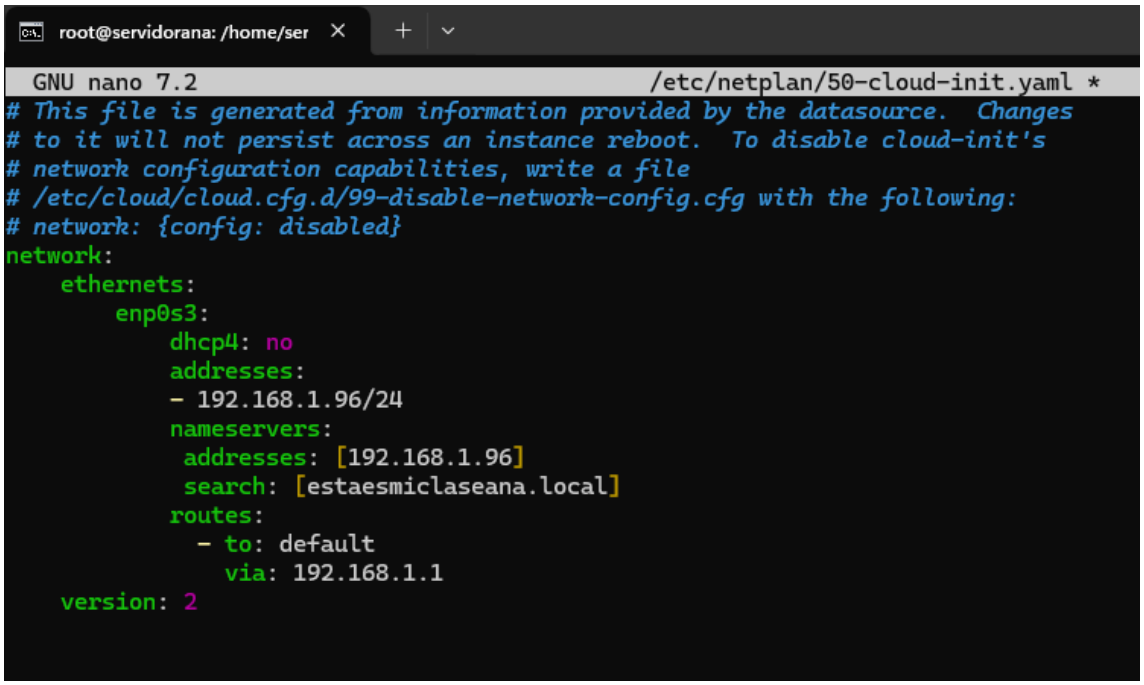
Por último, vamos a poner que use siempre IPv4 para evitar errores:

```
root@servidorana: /home/ser
 GNU nano 7.2                                  /etc/default/named
#
# run resolvconf?
RESOLVCONF=no

# startup options for the server
OPTIONS="-u bind -4"
```

Por último reiniciamos el servidor y lo activamos:



Ahora que funciona, vamos a cambiar el dns y hacer comprobaciones:



3. Realizar consultas dig/nslookup para comprobar el funcionamiento del servidor DNS.

```
root@servidorana:/home/servidorana# ls -l /etc/resolv.conf
lrwxrwxrwx 1 root root 39 ago 27 14:21 /etc/resolv.conf -> ../run/systemd/resolve/stub-resolv.conf
root@servidorana:/home/servidorana# ln -sf /run/systemd/resolve/resolv.conf /etc/resolv.conf
root@servidorana:/home/servidorana# cat /etc/resolv.conf
# This is /run/systemd/resolve/resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients directly to
# all known uplink DNS servers. This file lists all configured search domains.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 192.168.1.96
search estaesmiclaseana.local
root@servidorana:/home/servidorana#
```

```
root@servidorana:/home/servidorana# nslookup clienteana1
Server:         192.168.1.96
Address:        192.168.1.96#53

Name:   clienteana1.estaesmiclaseana.local
Address: 192.168.1.97

root@servidorana:/home/servidorana# nslookup clienteana2
Server:         192.168.1.96
Address:        192.168.1.96#53

Name:   clienteana2.estaesmiclaseana.local
Address: 192.168.1.98

root@servidorana:/home/servidorana# nslookup google.com
Server:         192.168.1.96
Address:        192.168.1.96#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.185.14
Name:   google.com
Address: 2a00:1450:4003:80c::200e
```

```
root@servidorana:/home/servidorana# nslookup 192.168.1.96
96.1.168.192.in-addr.arpa       name = servidorana.estaesmiclaseana.local.

root@servidorana:/home/servidorana# nslookup 192.168.1.97
97.1.168.192.in-addr.arpa       name = clienteana1.estaesmiclaseana.local.

root@servidorana:/home/servidorana# nslookup 192.168.1.98
98.1.168.192.in-addr.arpa       name = clienteana2.estaesmiclaseana.local.

root@servidorana:/home/servidorana# nslookup 8.8.8.8
8.8.8.8.in-addr.arpa    name = dns.google.

Authoritative answers can be found from:
```

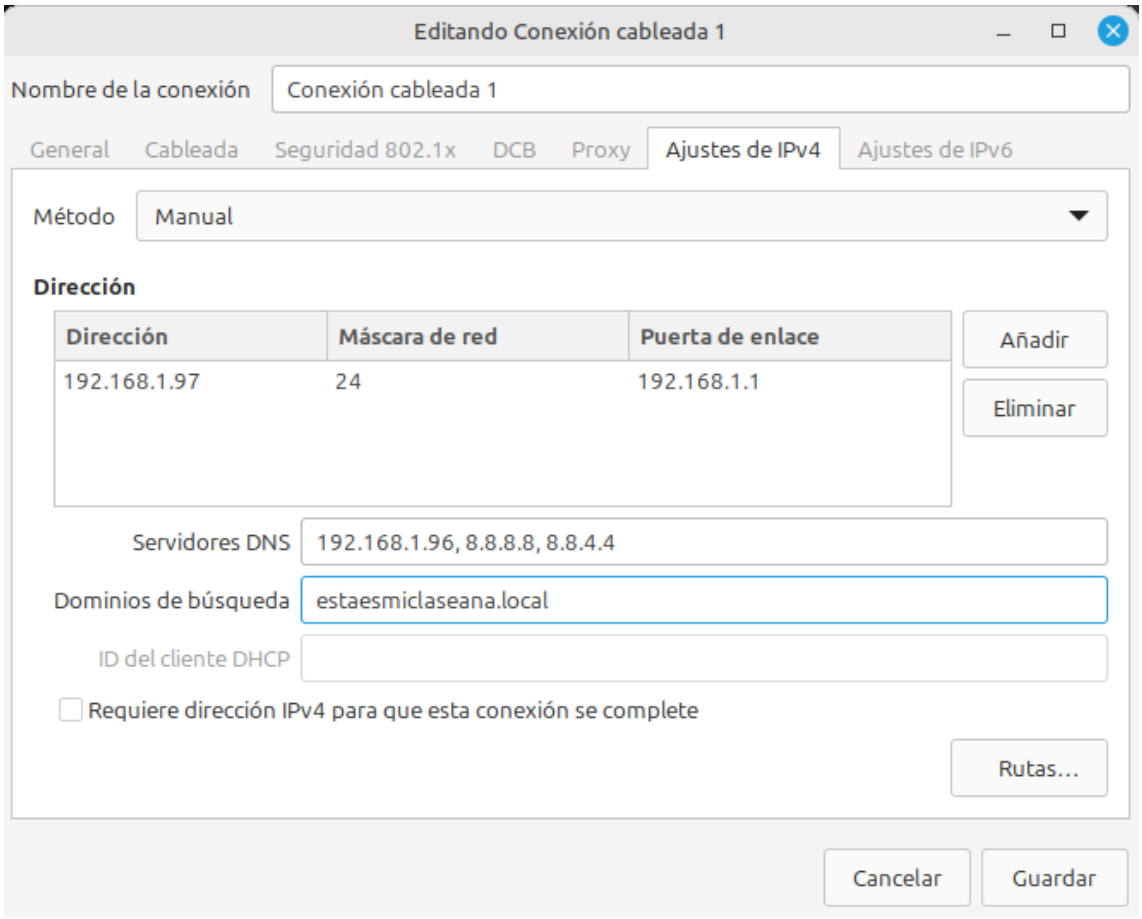
```
root@servidorana:/home/servidorana# dig ldap.estaesmiclaseana.local

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> ldap.estaesmiclaseana.local
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 6697
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: fbe64e8d404875500100000675c590c9f0bcab9f09e22b3 (good)
;; QUESTION SECTION:
;ldap.estaesmiclaseana.local.   IN      A

;; ANSWER SECTION:
ldap.estaesmiclaseana.local. 604800 IN  CNAME   servidorpm.estaesmiclaseana.local.

;; AUTHORITY SECTION:
estaesmiclaseana.local. 604800  IN      SOA     estaesmiclaseana.local. root.estaesmiclaseana.local. 2 604800 86400 2419
200 604800

;; Query time: 0 msec
;; SERVER: 192.168.1.96#53(192.168.1.96) (UDP)
;; WHEN: Fri Dec 13 15:55:56 UTC 2024
;; MSG SIZE  rcvd: 150
```

4. Instalar el Servidor LDAP, detallando los pasos seguidos.

Ahora voy a ir a los clientes y cambiaré los servidores dns preferidos:

Primero en clienteana1 y después en clienteana2.

Además comprobaré si hacen ping.




```
ana@clienteana1:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.952 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.03 ms
^C
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 0.952/0.991/1.031/0.039 ms
ana@clienteana1:~$ ping www.google.com
PING www.google.com (172.217.168.164) 56(84) bytes of data.
64 bytes from mad07s10-in-f4.1e100.net (172.217.168.164): icmp_seq=1 ttl=119 tim
e=17.3 ms
64 bytes from mad07s10-in-f4.1e100.net (172.217.168.164): icmp_seq=2 ttl=119 tim
e=17.3 ms
64 bytes from mad07s10-in-f4.1e100.net (172.217.168.164): icmp_seq=3 ttl=119 tim
e=15.4 ms
64 bytes from mad07s10-in-f4.1e100.net (172.217.168.164): icmp_seq=4 ttl=119 tim
e=15.1 ms
^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3021ms
rtt min/avg/max/mdev = 15.092/16.272/17.345/1.045 ms
```


```
C:\Users\clienteana2>ping 192.168.1.1

Haciendo ping a 192.168.1.1 con 32 bytes de datos:
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=4ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 4ms, Media = 1ms

C:\Users\clienteana2>^X

C:\Users\clienteana2>ping 192.168.1.96

Haciendo ping a 192.168.1.96 con 32 bytes de datos:
Respuesta desde 192.168.1.96: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.96: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.96: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.1.96:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
^C
C:\Users\clienteana2>ping www.google.com

Haciendo ping a www.google.com [142.250.200.100] con 32 bytes de dato
Respuesta desde 142.250.200.100: bytes=32 tiempo=17ms TTL=119
Respuesta desde 142.250.200.100: bytes=32 tiempo=14ms TTL=119
Respuesta desde 142.250.200.100: bytes=32 tiempo=14ms TTL=119
Respuesta desde 142.250.200.100: bytes=32 tiempo=15ms TTL=119
```

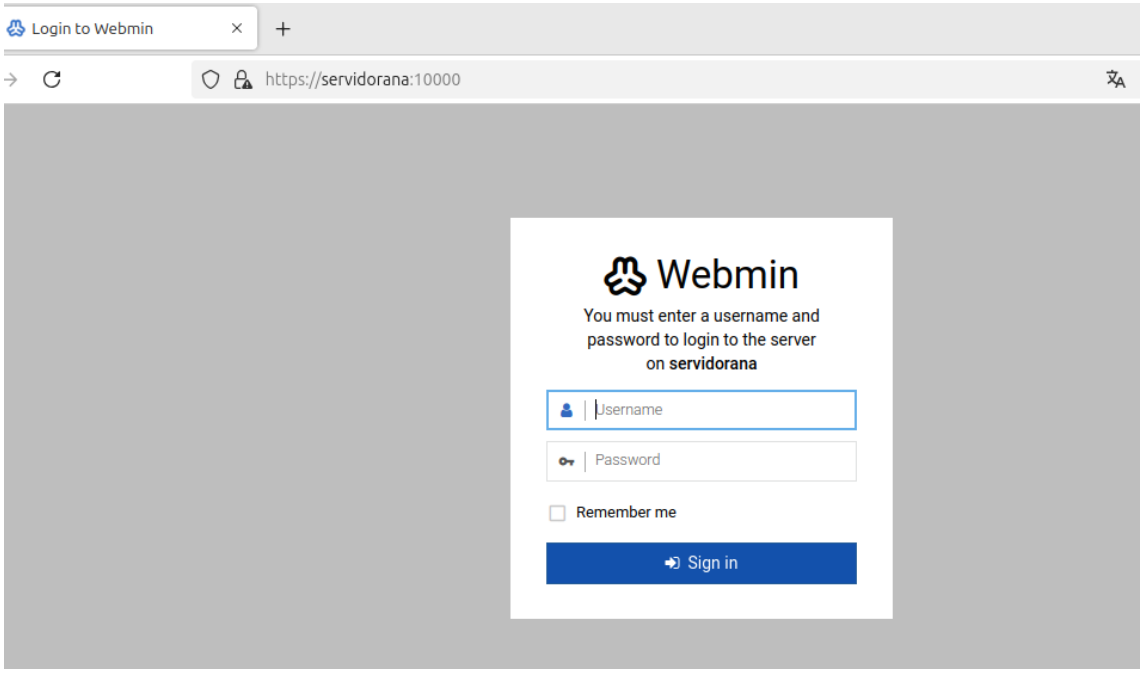
Ahora instalamos el Webmin a través de curl:

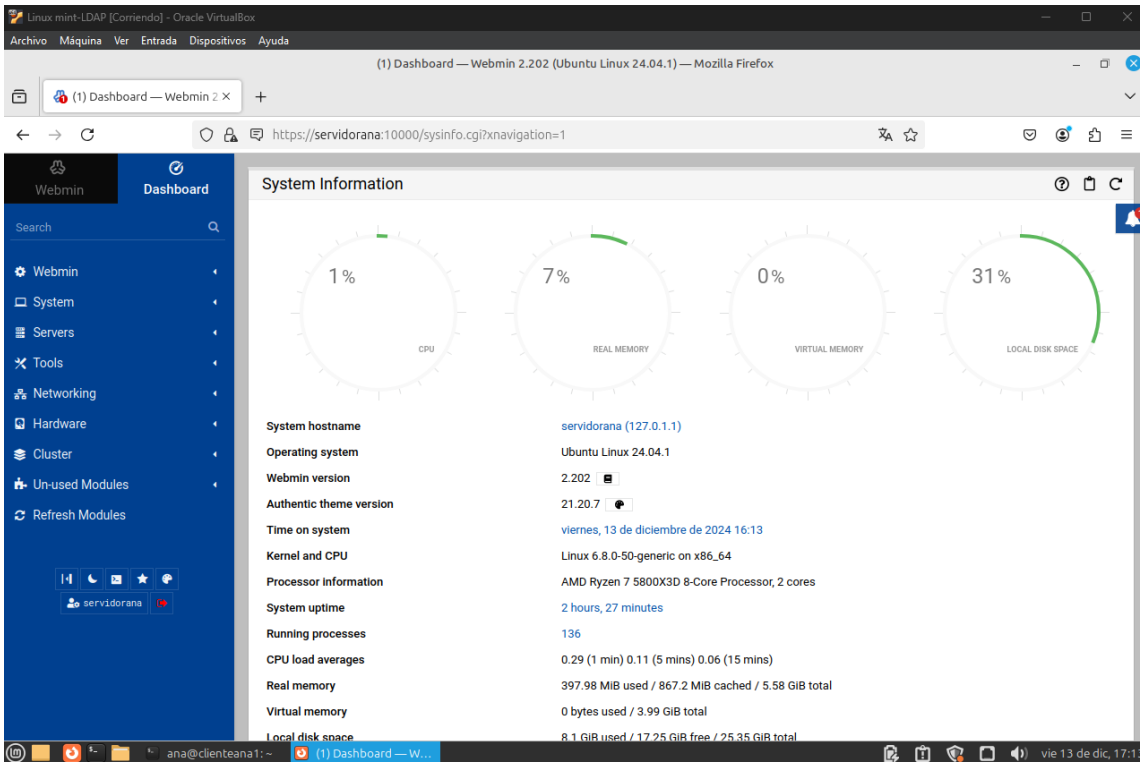
```
root@servidorana:/home/servidorana# curl -o webmin-setup-repos.sh https://raw.githubusercontent.com/webmin/webmin/master
/webmin-setup-repos.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  5286  100  5286    0     0  20611      0 --:--:-- --:--:-- --:--:-- 20568
root@servidorana:/home/servidorana# sh webmin-setup-repos.sh
Setup Webmin repository? (y/N) y
  Downloading Webmin key ..
  .. done
  Installing Webmin key ..
  .. done
  Setting up Webmin repository ..
  .. done
  Cleaning repository metadata ..
  .. done
  Downloading repository metadata ..
  .. done
Webmin package can now be installed using apt-get install --install-recommends webmin command.
```

Y actualizamos los paquetes:

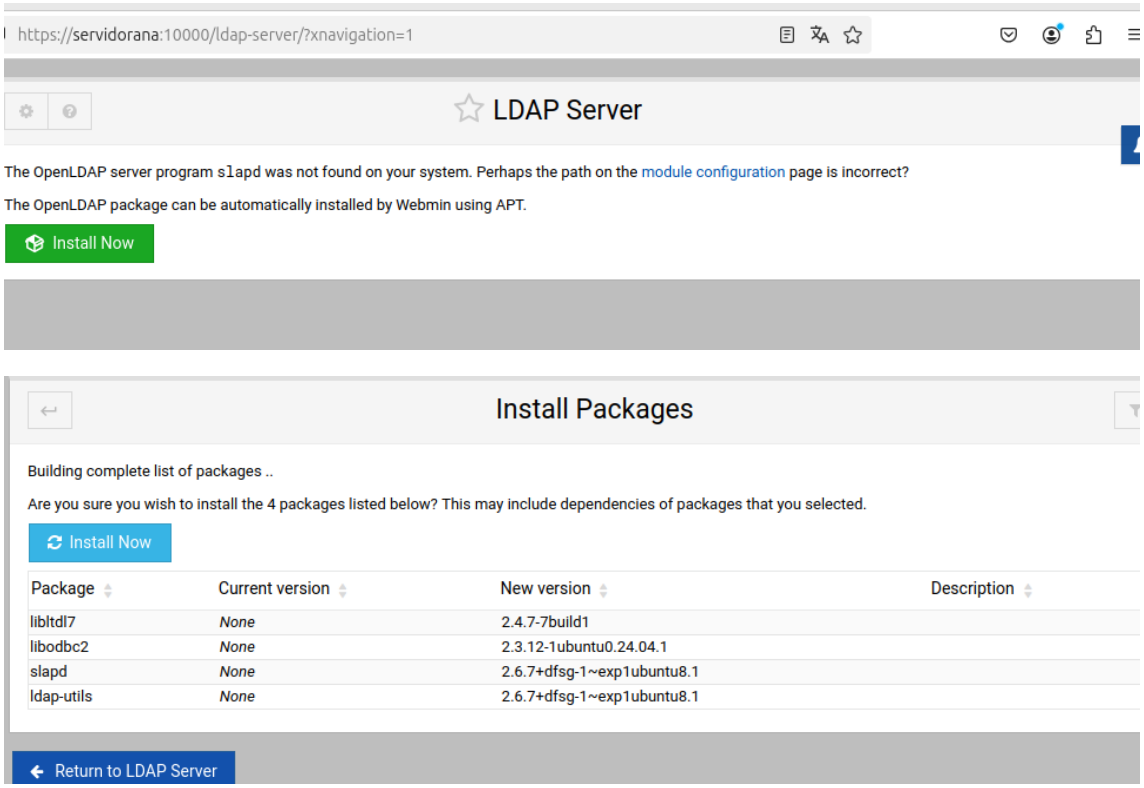
```
root@servidorana:/home/servidorana# apt-get update
Obj:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Obj:2 http://es.archive.ubuntu.com/ubuntu noble InRelease
Obj:3 http://es.archive.ubuntu.com/ubuntu noble-updates InRelease
Obj:4 http://es.archive.ubuntu.com/ubuntu noble-backports InRelease
Ign:5 https://download.webmin.com/download/newkey/repository stable InRelease
Obj:6 https://download.webmin.com/download/newkey/repository stable Release
Leyendo lista de paquetes... Hecho
root@servidorana:/home/servidorana# apt-get install webmin --install-recommends
```

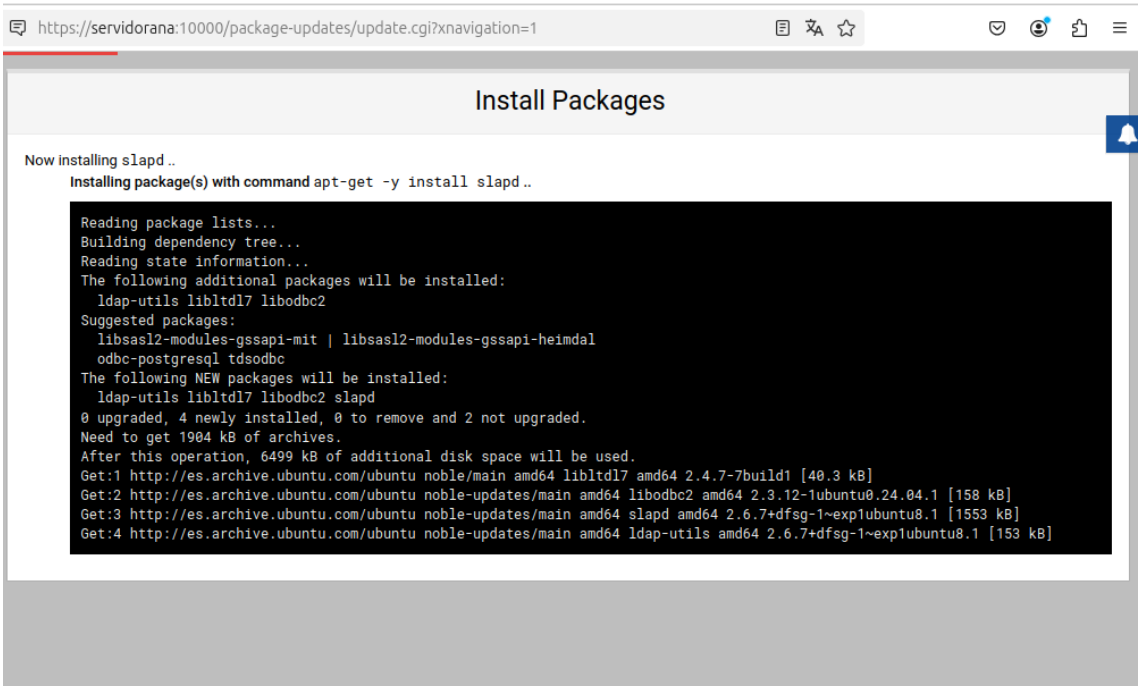
En clienteana1 iremos al webmin:



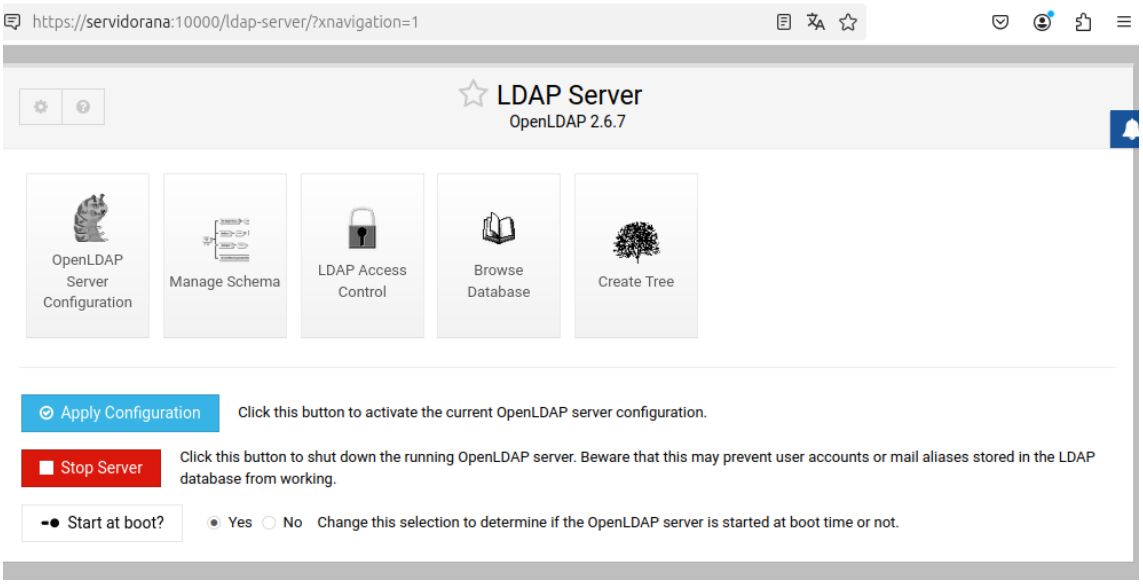


En el buscador ponemos LDAP Server y lo instalamos:



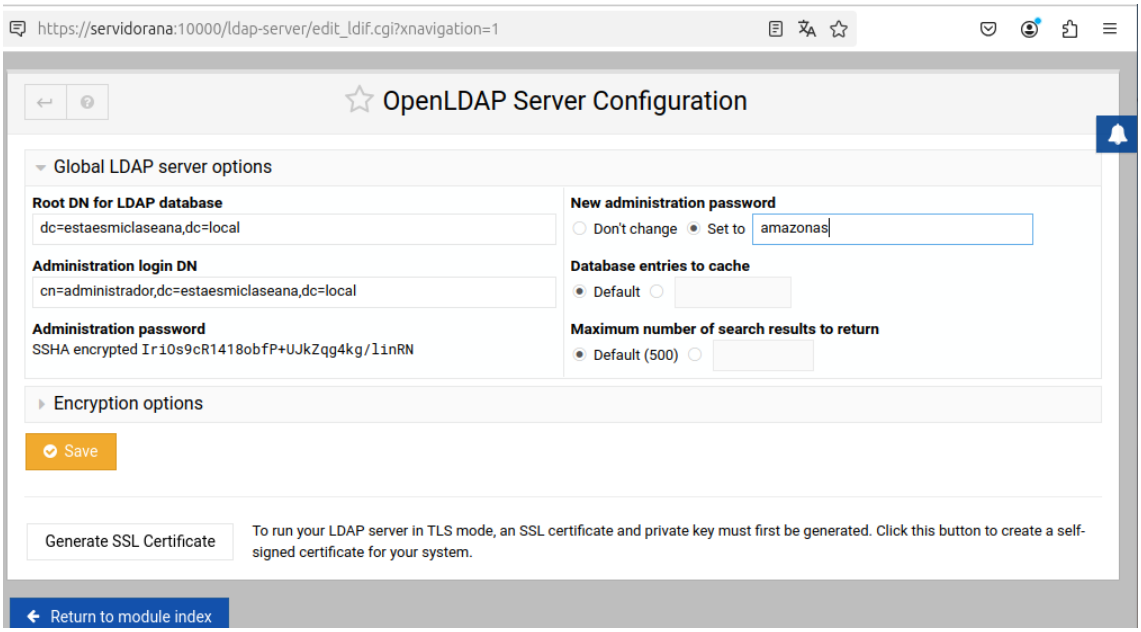


Y ya lo tendremos instalado:

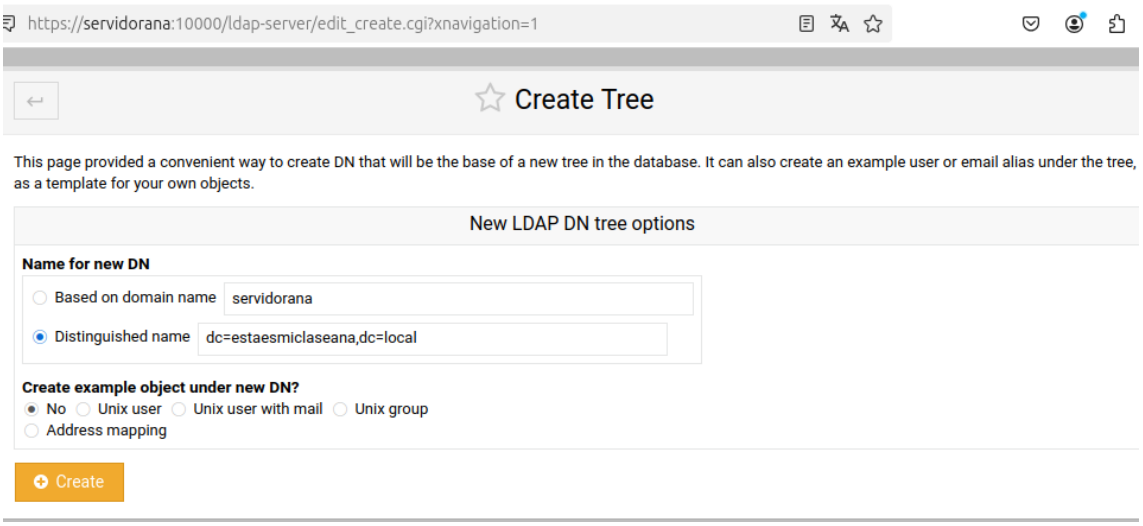


4. Crear el dominio estaesmiclaseana.local cuyo usuario administrador se llamará administrador.

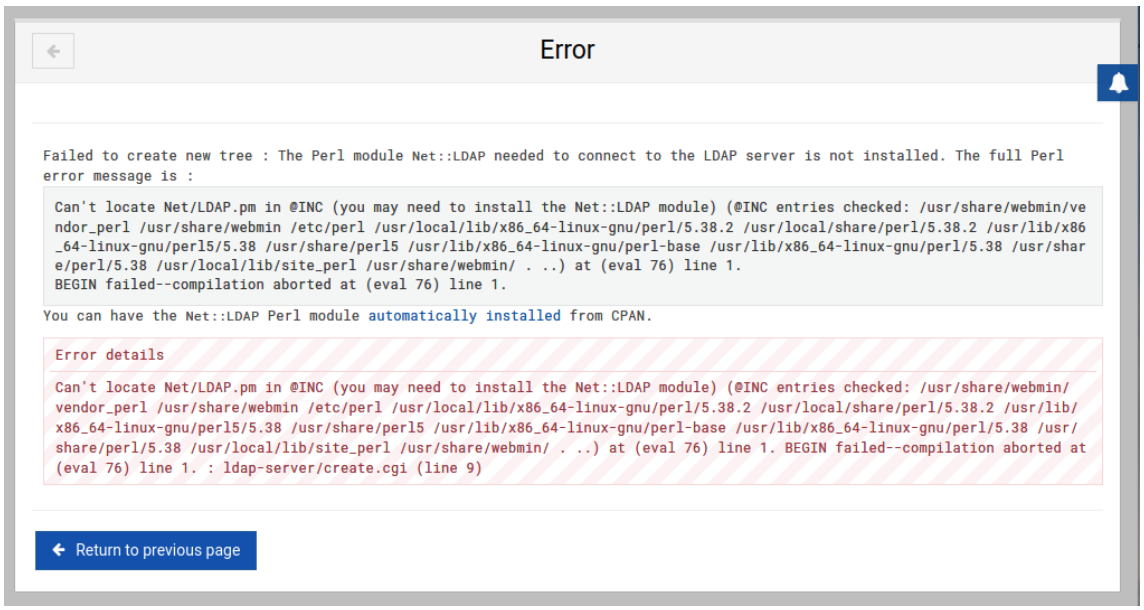
En la ventana anterior del Servidor LDAP le daremos a la configuración principal:



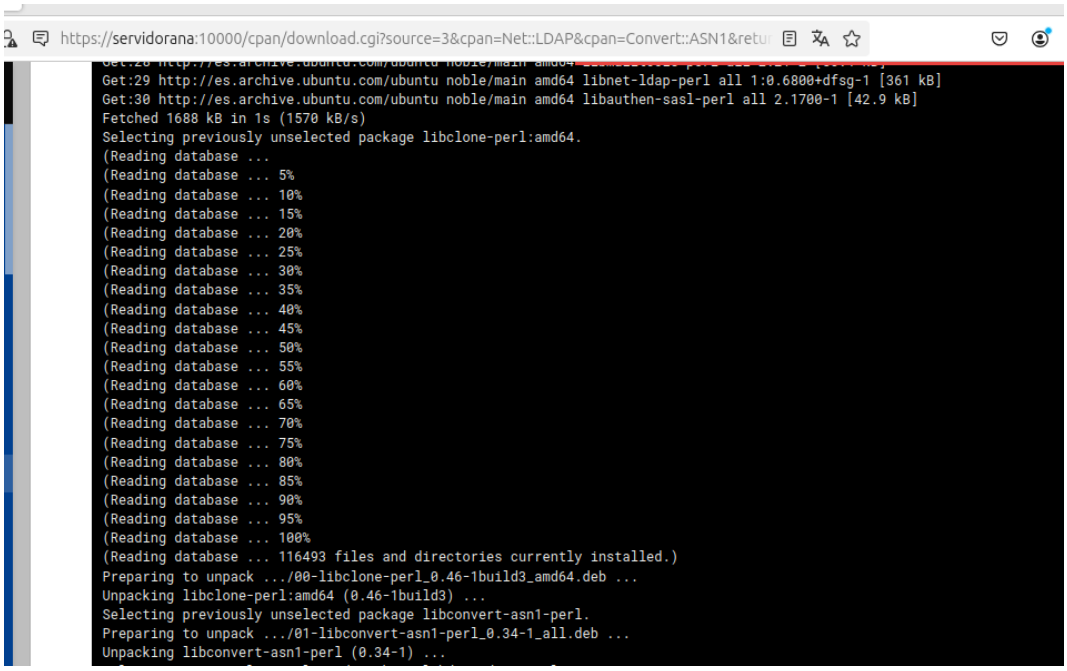
Crearemos un nuevo árbol:



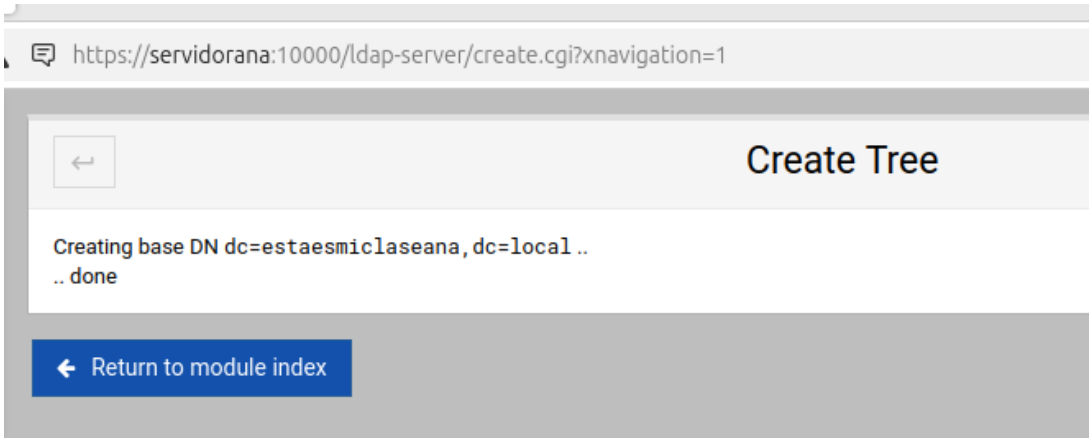
Dará este error y le haremos click “automatically installed” :



Y empezará la instalación:

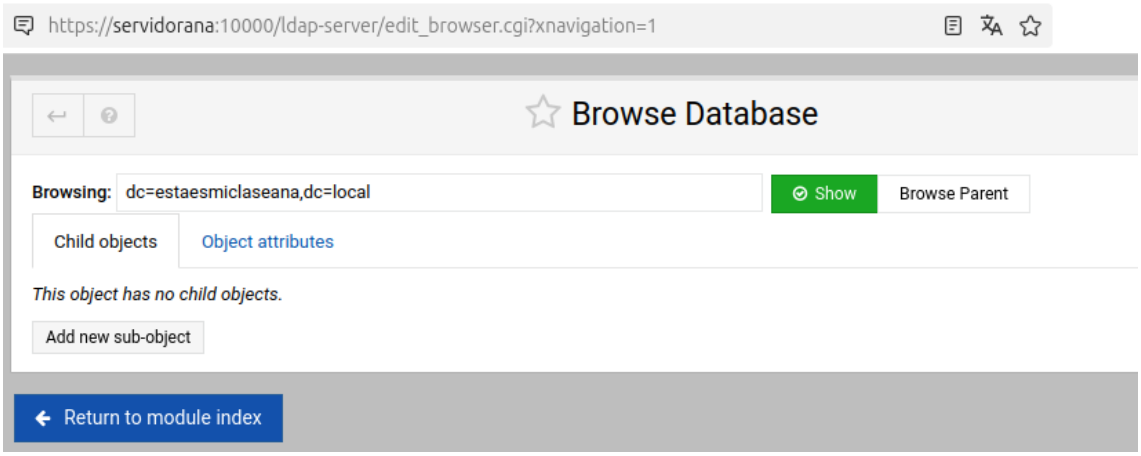


Justo después probaremos de nuevo y esta vez sí funcionará:

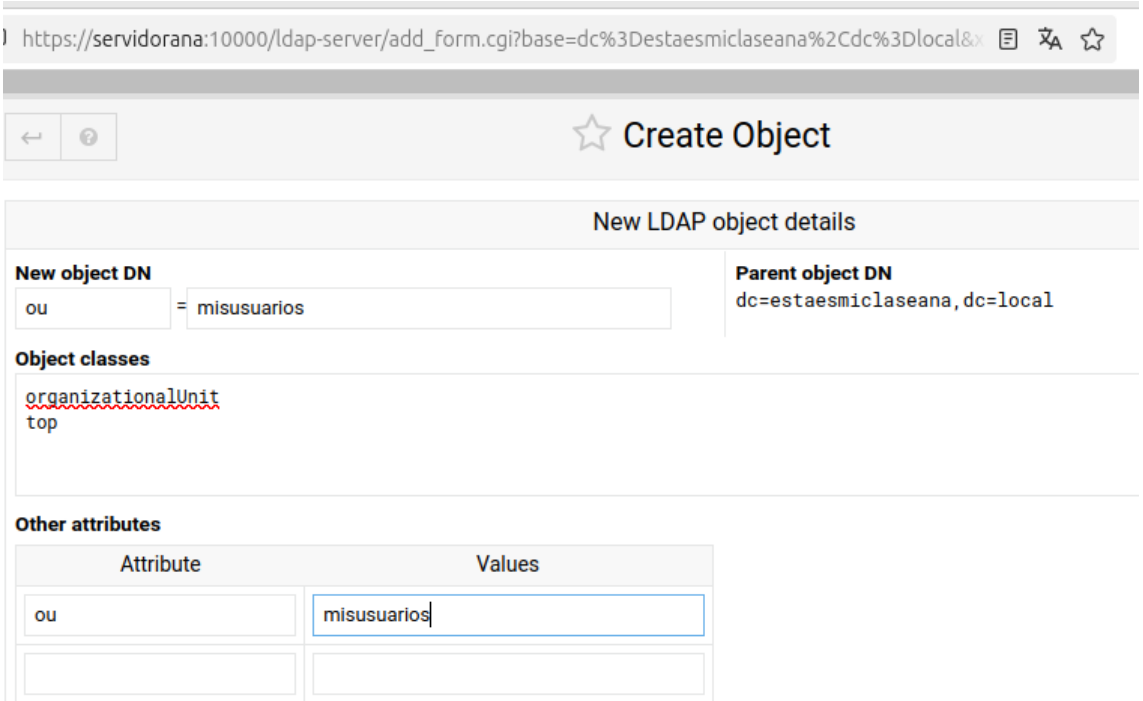


6. Crear las unidades organizativas misgrupos y misusuarios, para grupos y usuarios, respectivamente.

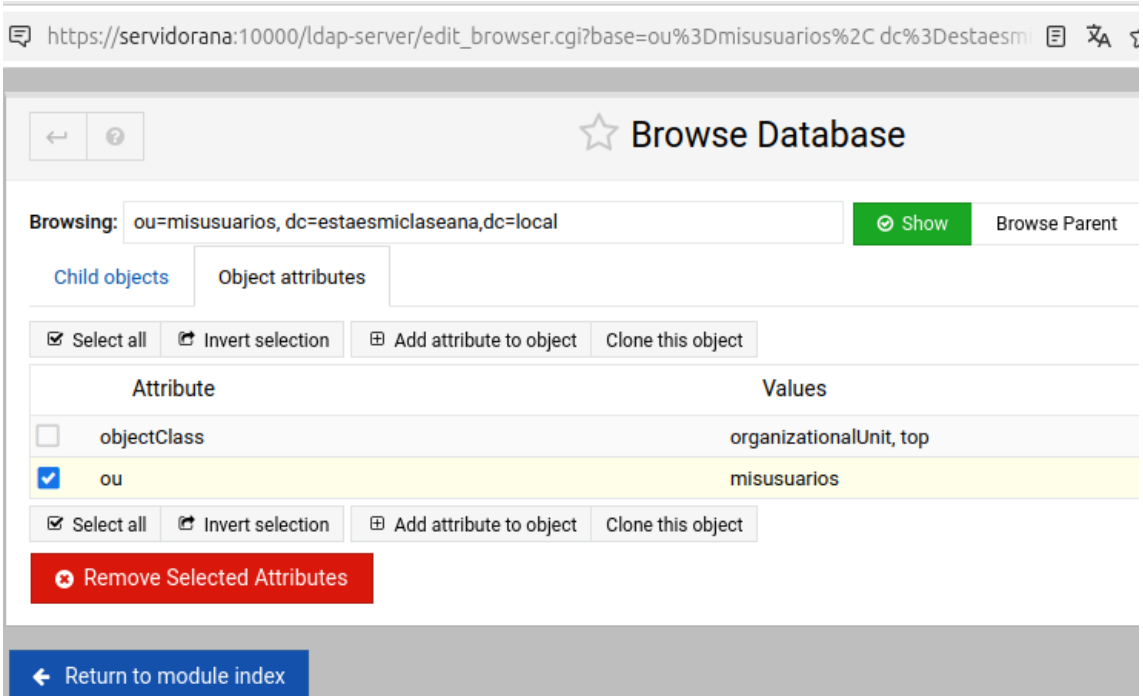
Ahora en el menú LDAP le damos a “Browse Database” y crearemos un nuevo “child object:



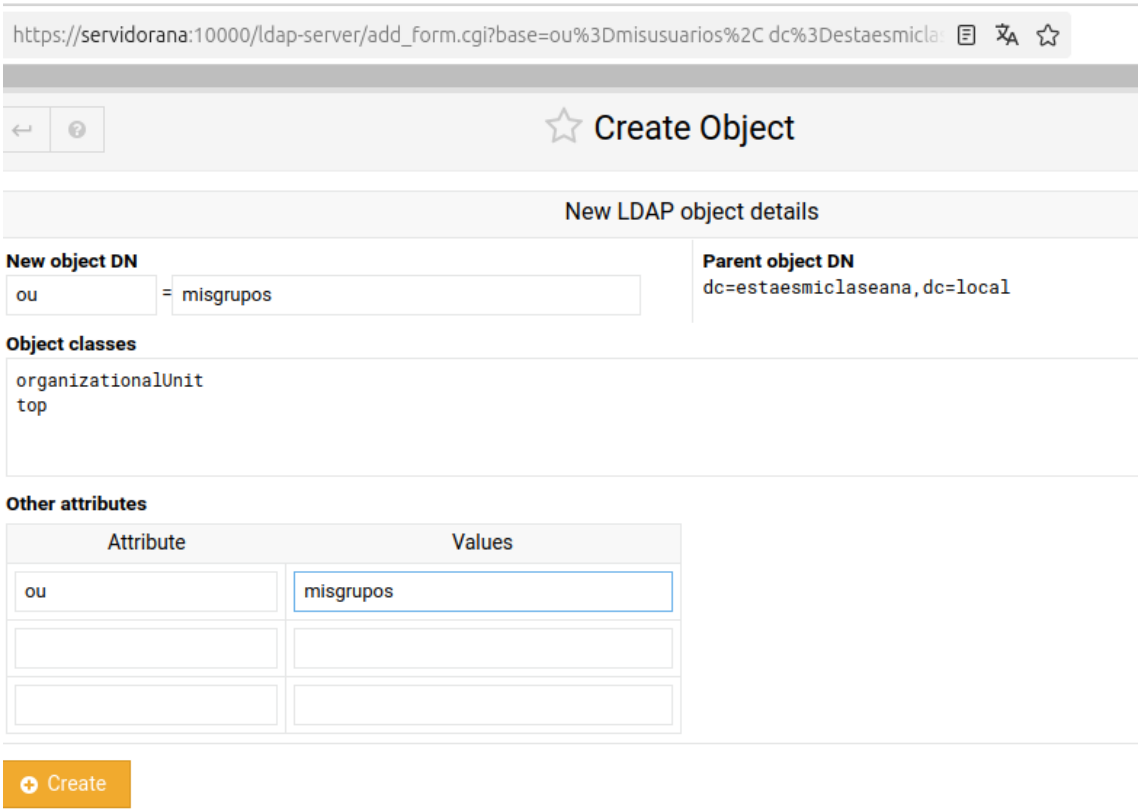
Creamos la unidad organizativa mis usuarios:

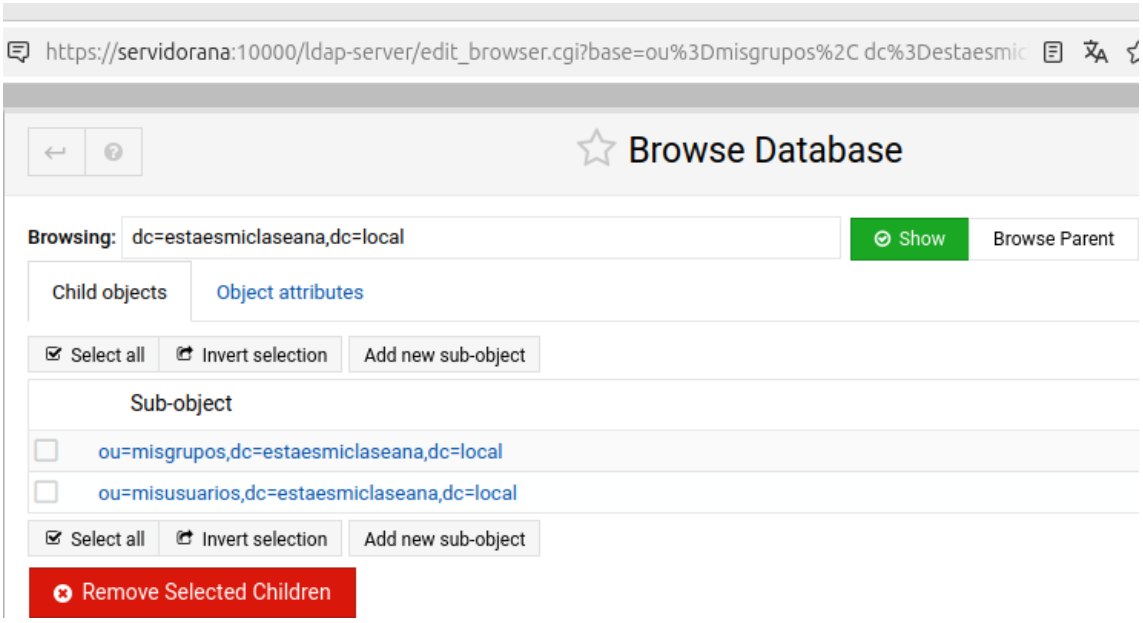


Ahora copiaré esa unidad organizativa y le cambiaré los parámetros:



Y esta vez será mis grupos:

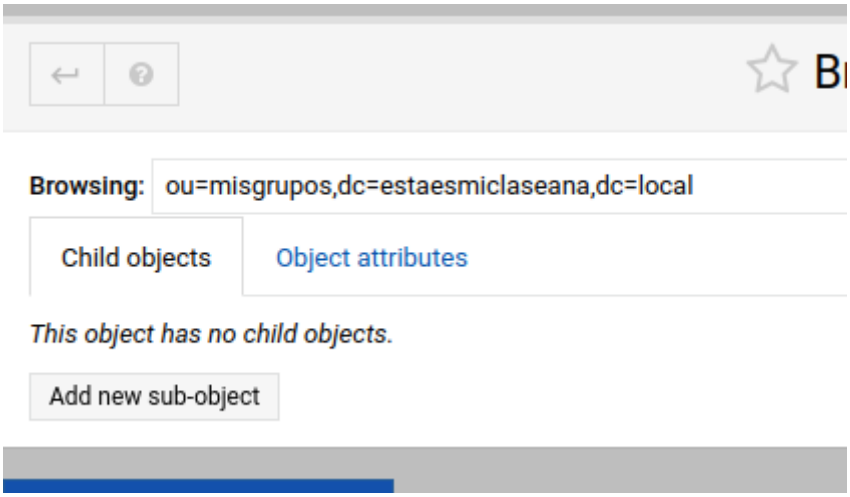


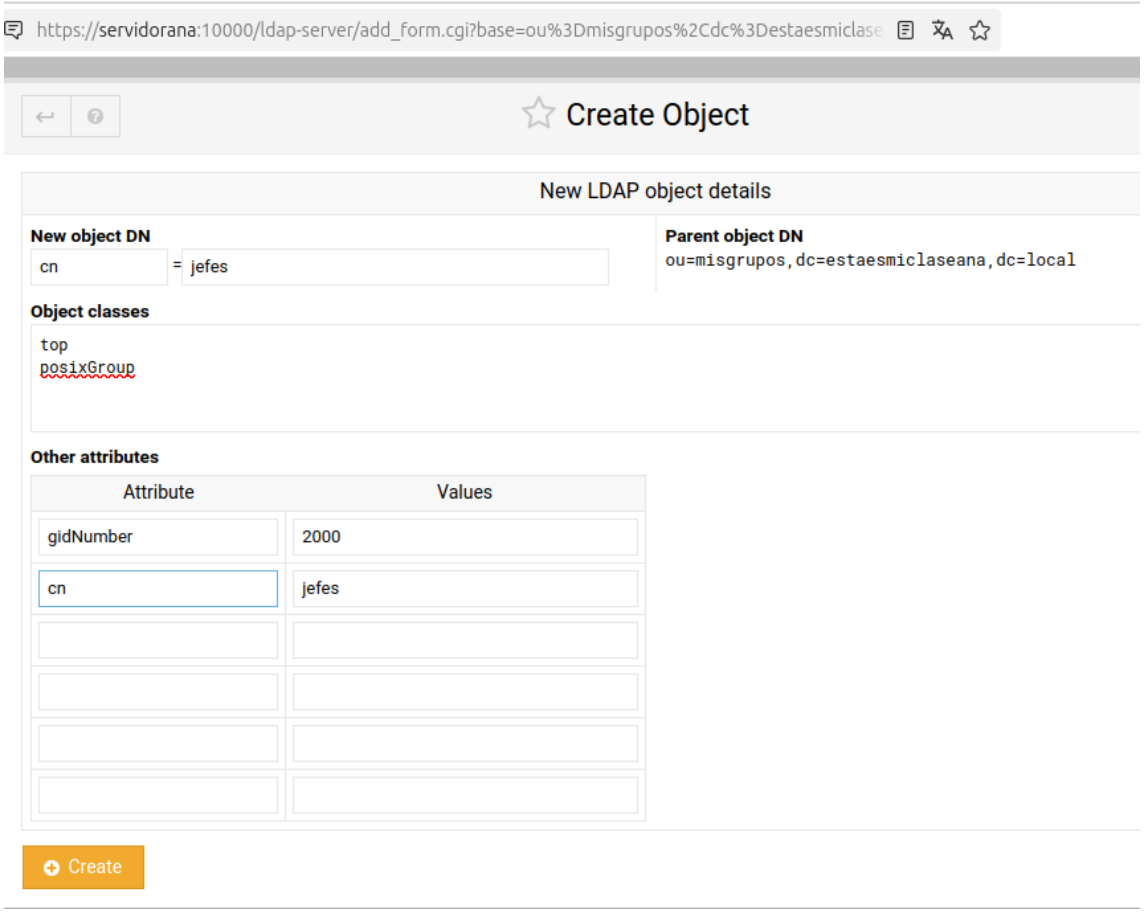


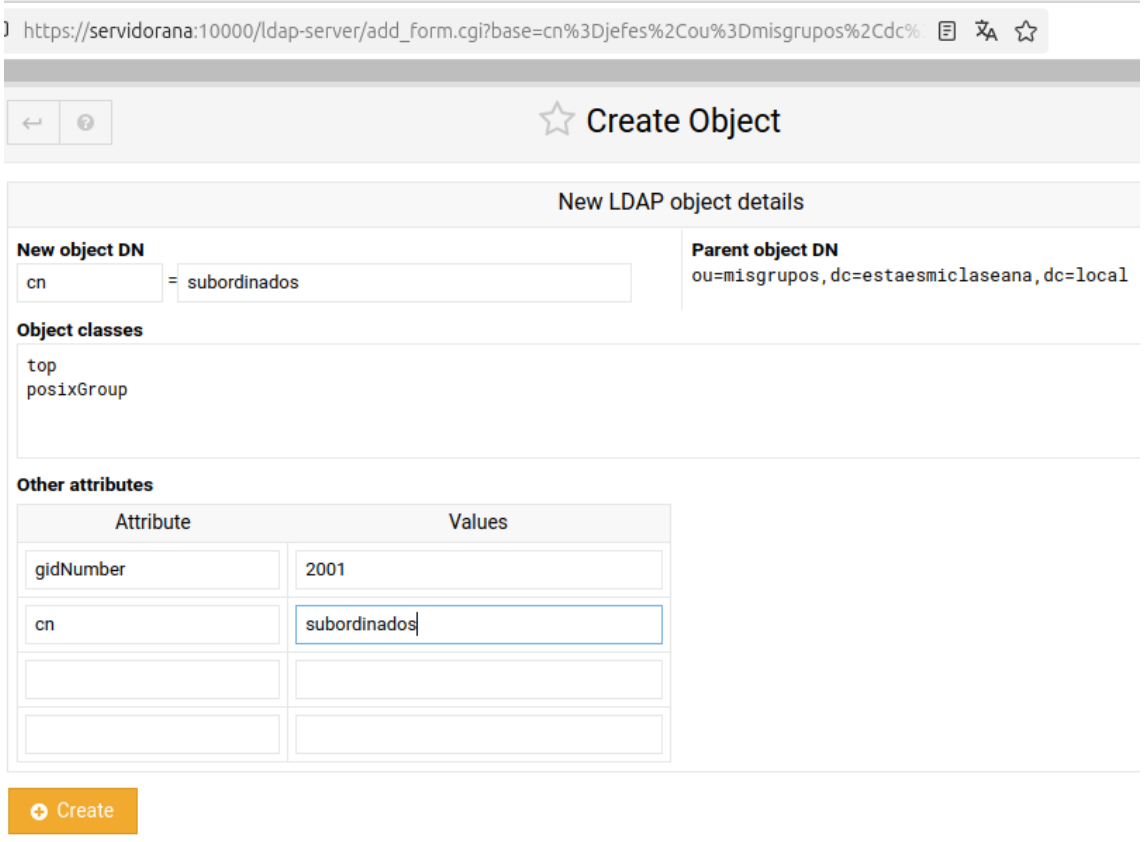
7. Crear los grupos jefes y subordinados en la unidad organizativa misgrupos.

Dentro de la unidad organizativa mis grupos crearemos jefe y subordinados.

Para ello haremos clic en misgrupos y seleccionamos “child objects” > “add new sub-object”:

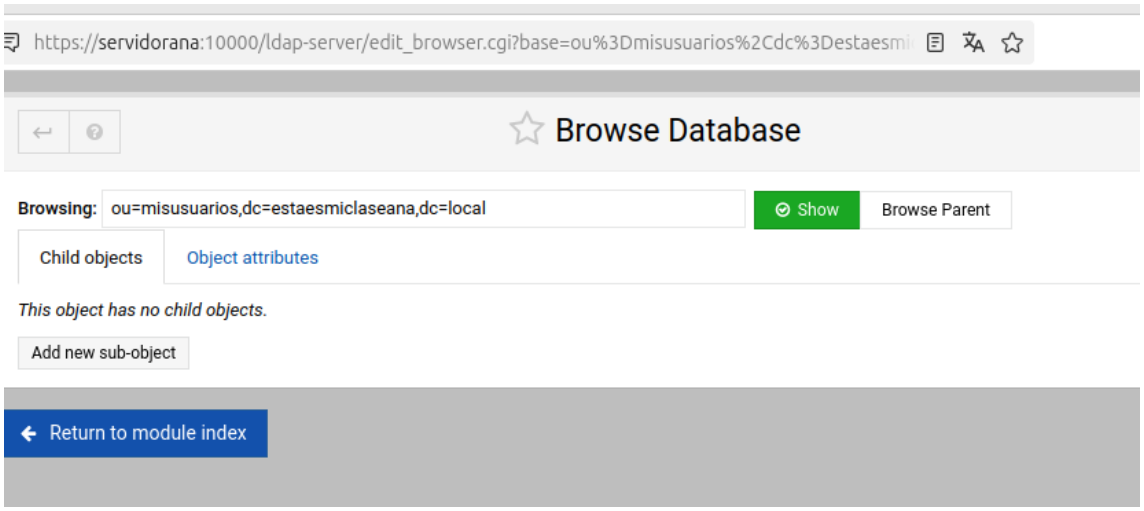



https://servidorana:10000/ldap-server/add_form.cgi?base=ou%3Dmisgrupos%2Cdc%3Destaesmiclase
Create Object
New LDAP object details
New object DN
cn = jefes
Parent object DN
ou=misgrupos,dc=estaesmiclaseana,dc=local
Object classes
top
posixGroup
Other attributes
Attribute
Values
gidNumber
2000
cn
jefes
Create

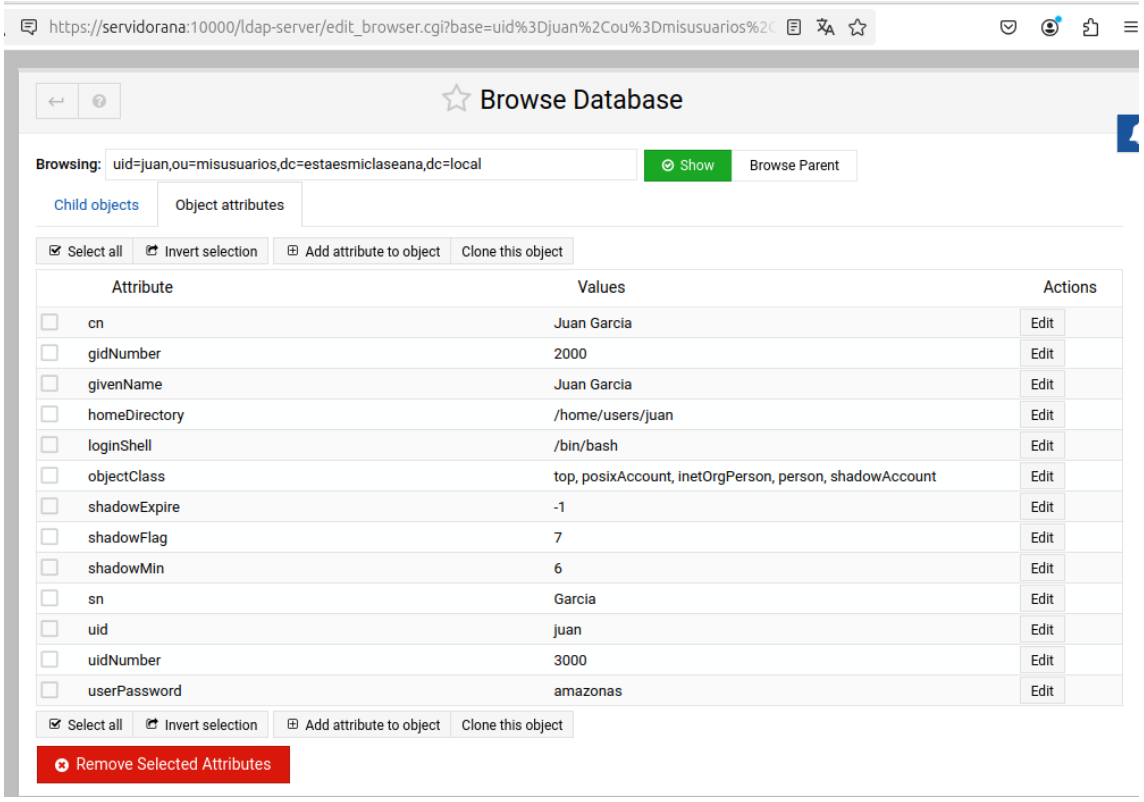

https://servidorana:10000/ldap-server/add_form.cgi?base=cn%3Djefes%2Cou%3Dmisgrupos%2Cdc%
Create Object
New LDAP object details
New object DN
cn = subordinados
Parent object DN
ou=misgrupos,dc=estaesmiclaseana,dc=local
Object classes
top
posixGroup
Other attributes
Attribute
Values
gidNumber
2001
cn
subordinados
Create

8. Crear los usuarios Juan García y Rosa López y hacerlos pertenecer al grupo Jefes. Estos usuarios contarán con perfiles móviles y sus directorios personales se crearán en /home/users.

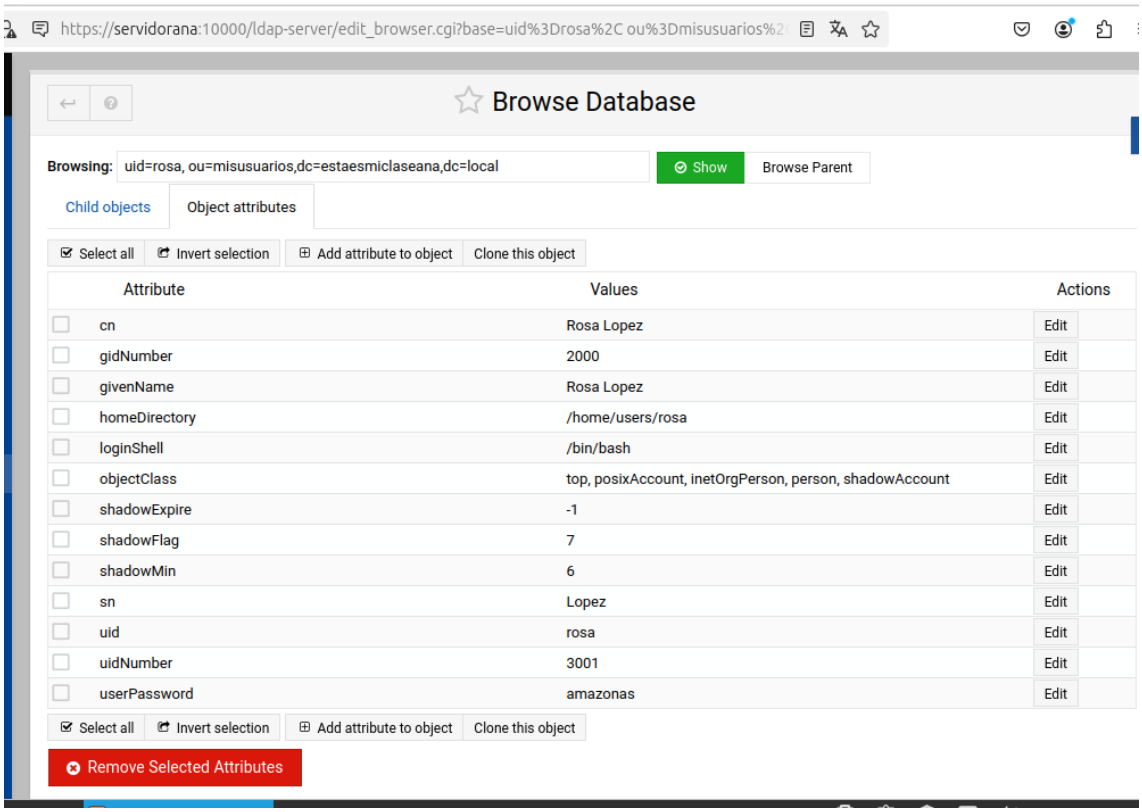
De la misma manera vamos a crear los usuarios “misusuarios”:



Juan:



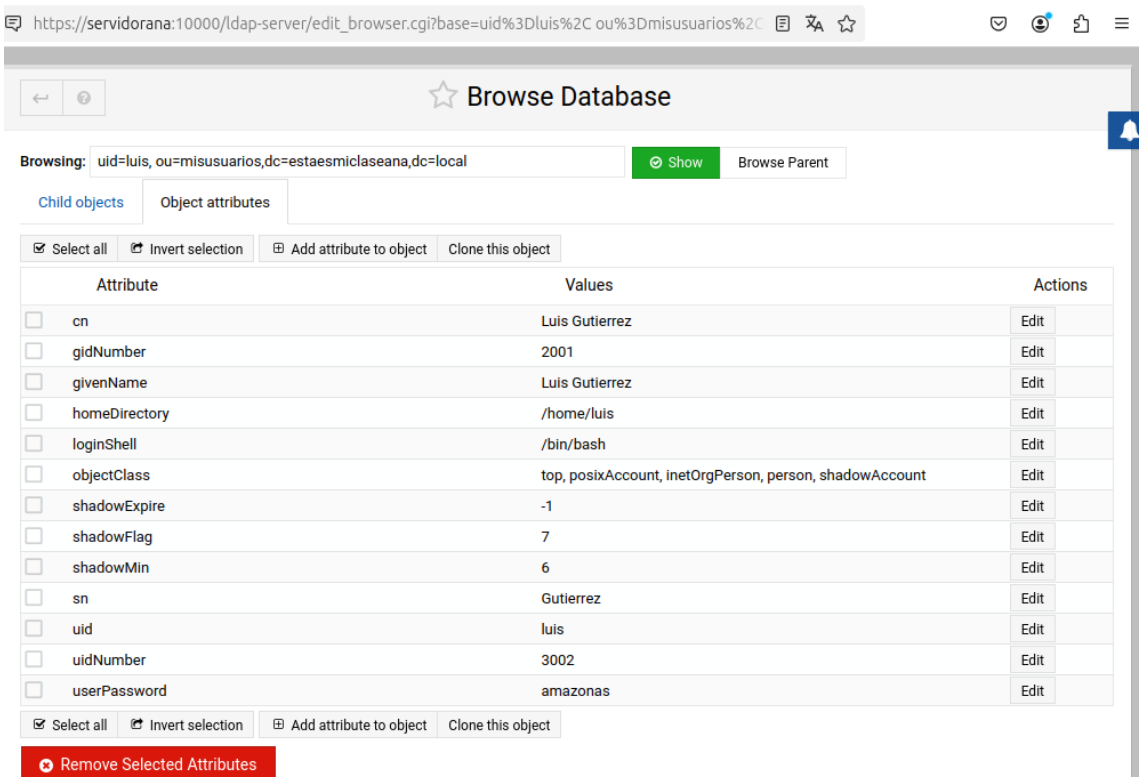
Rosa:



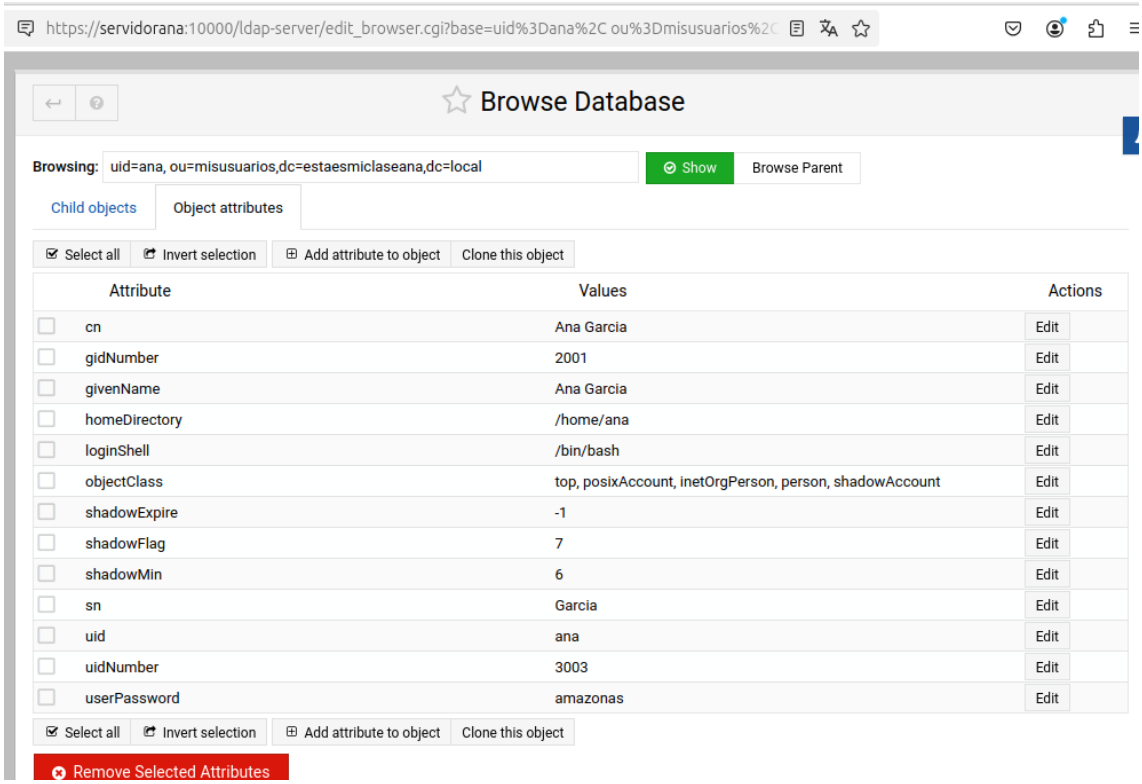
9. Crear también los usuarios Luis Gutiérrez, Ana García, Antonio Martínez y Patricia Torres pertenecientes al grupo subordinados. Estos usuarios tendrán perfiles locales y su directorio personal coincidirá con el login de usuario, directamente en el directorio /home.

Vamos a hacerlo de la misma forma:

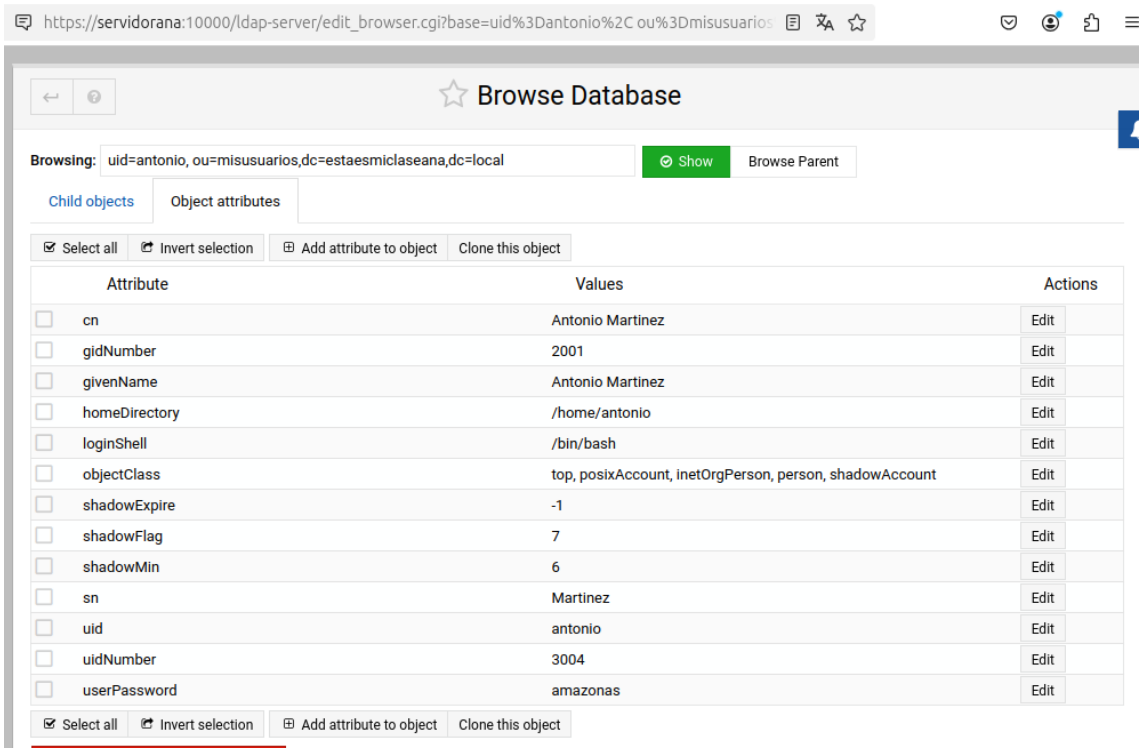
Luis:


https://servidorana:10000/ldap-server/edit_browser.cgi?base=uid%3Dluis%2C ou%3Dmisusuarios%2C
Browse Database
Browsing: uid=luis, ou=misusuarios,dc=estaesmiclaseana,dc=local
Show
Browse Parent
Child objects
Object attributes
Select all
Invert selection
Add attribute to object
Clone this object
Attribute
Values
Actions
cn
Luis Gutierrez
Edit
gidNumber
2001
Edit
givenName
Luis Gutierrez
Edit
homeDirectory
/home/luis
Edit
loginShell
/bin/bash
Edit
objectClass
top, posixAccount, inetOrgPerson, person, shadowAccount
Edit
shadowExpire
-1
Edit
shadowFlag
7
Edit
shadowMin
6
Edit
sn
Gutierrez
Edit
uid
luis
Edit
uidNumber
3002
Edit
userPassword
amazonas
Edit
Select all
Invert selection
Add attribute to object
Clone this object
Remove Selected Attributes

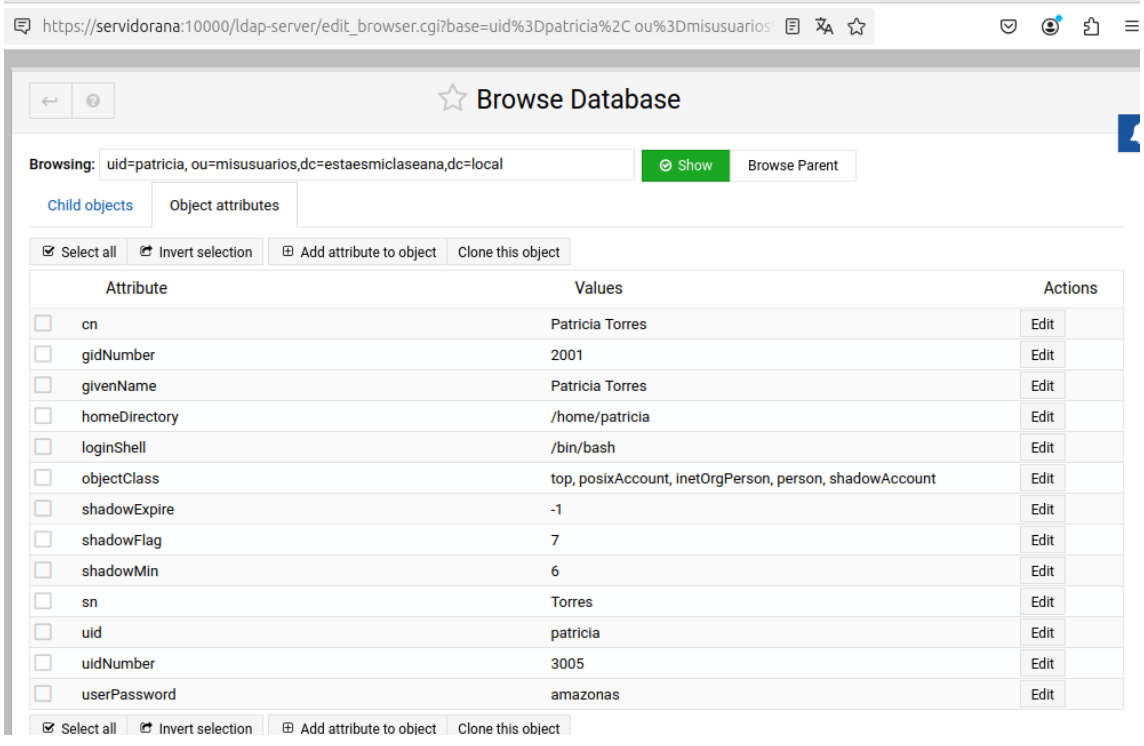
Ana:


https://servidorana:10000/ldap-server/edit_browser.cgi?base=uid%3Dana%2C ou%3Dmisusuarios%2C
Browse Database
Browsing: uid=ana, ou=misusuarios,dc=estaesmiclaseana,dc=local
Show
Browse Parent
Child objects
Object attributes
Select all
Invert selection
Add attribute to object
Clone this object
Attribute
Values
Actions
cn
Ana Garcia
Edit
gidNumber
2001
Edit
givenName
Ana Garcia
Edit
homeDirectory
/home/ana
Edit
loginShell
/bin/bash
Edit
objectClass
top, posixAccount, inetOrgPerson, person, shadowAccount
Edit
shadowExpire
-1
Edit
shadowFlag
7
Edit
shadowMin
6
Edit
sn
Garcia
Edit
uid
ana
Edit
uidNumber
3003
Edit
userPassword
amazonas
Edit
Select all
Invert selection
Add attribute to object
Clone this object
Remove Selected Attributes

Antonio:



Patricia:



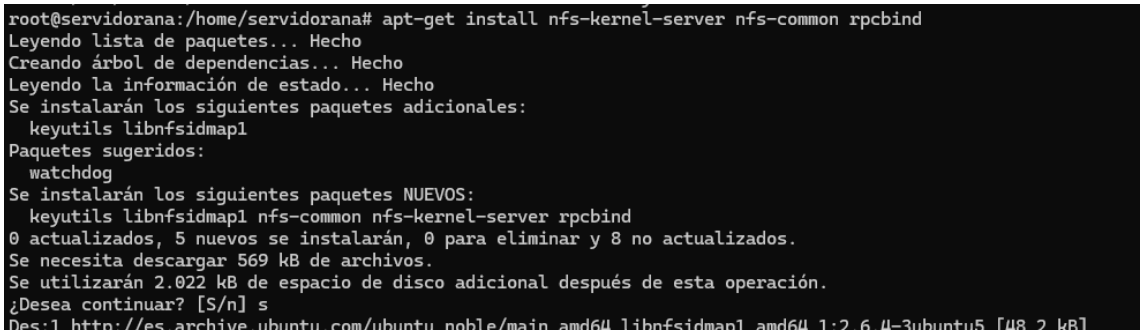
10. ¿En qué se diferencia la instalación de perfiles móviles de los perfiles locales? ¿Qué paquetes hay que instalar en el servidor? ¿Y en el cliente?

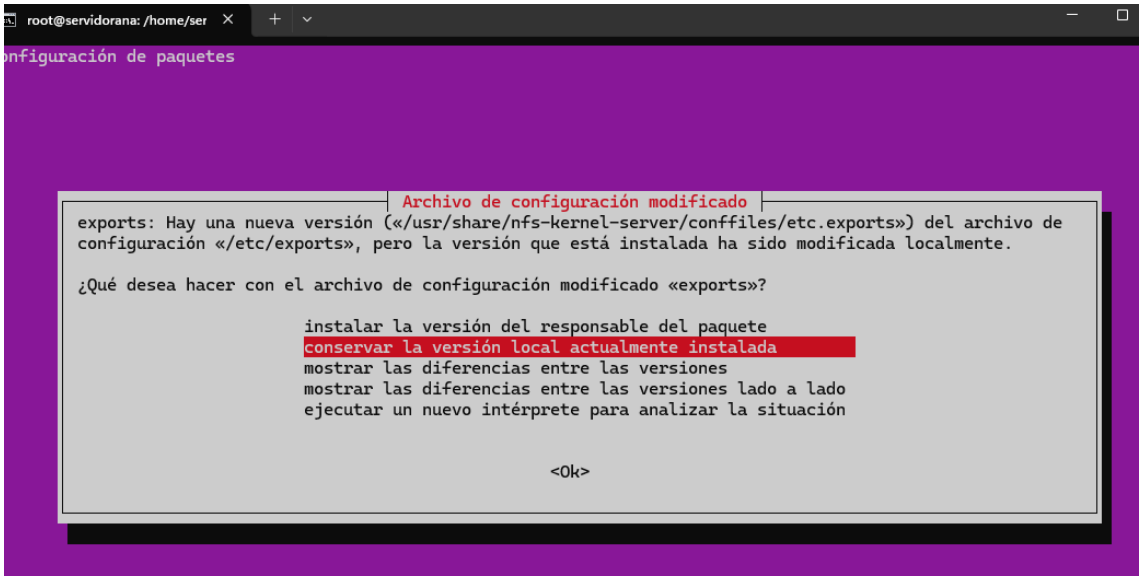
Los perfiles móviles permiten que esos usuarios accedan a datos y configuración desde cualquier dispositivo que se conecte desde la red porque se almacenan en el servidor.

Los perfiles locales, se almacenan en un dispositivo concreto por lo que no podremos acceder a datos y configuraciones desde otros dispositivos.

Servidor:

Para crear perfiles móviles instalaremos:





Y crearemos una carpeta donde se almacenarán:

```
root@servidorana:/home/servidorana# mkdir /moviles
root@servidorana:/home/servidorana# chown nobody:nogroup /moviles
```

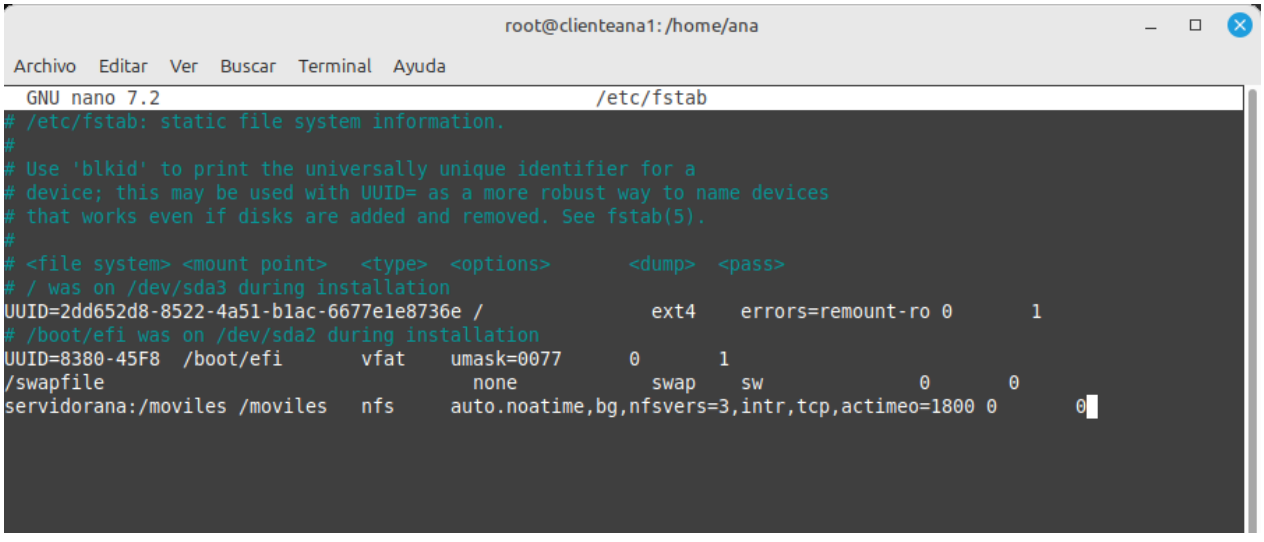
Reiniciaremos:

```
root@servidorana:/home/servidorana# /etc/init.d/nfs-kernel-server restart
Restarting nfs-kernel-server (via systemctl): nfs-kernel-server.service.
```

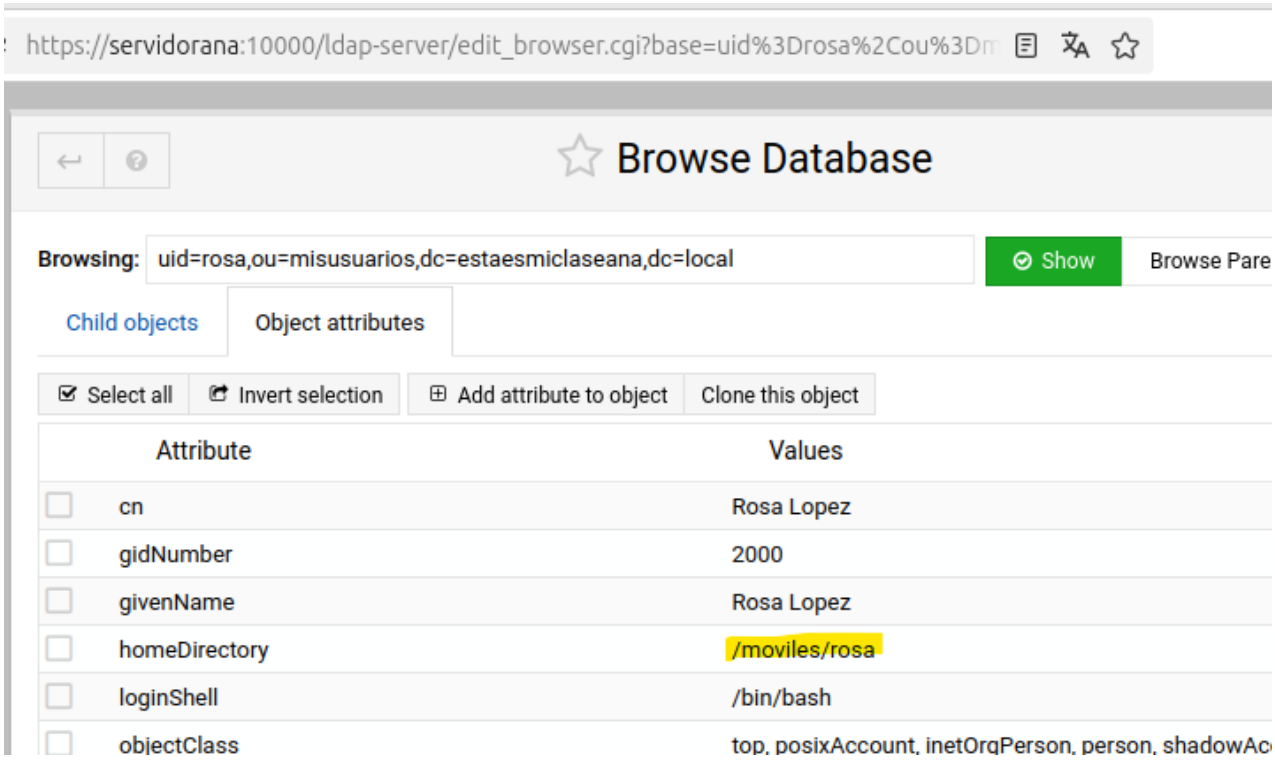
Clienteana1:

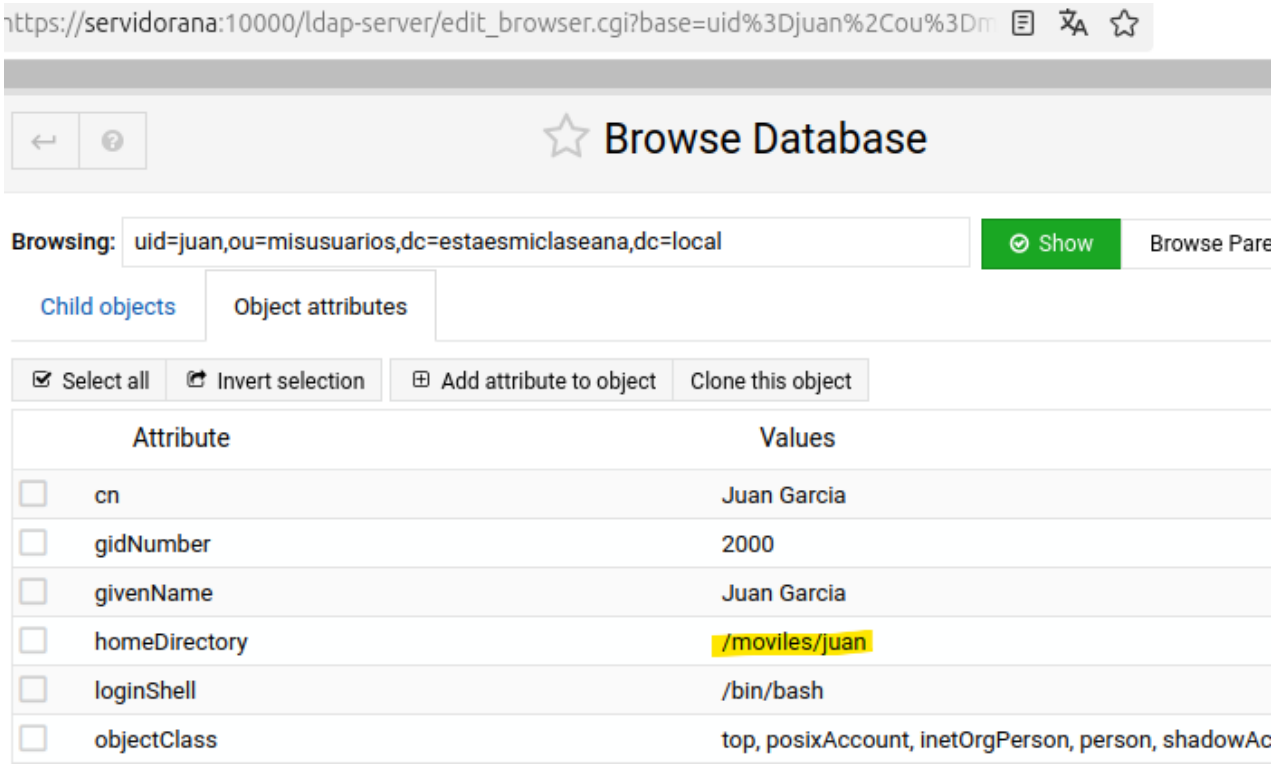
```
ana@clienteana1:~$ sudo apt-get install nfs-common rpcbind
[sudo] contraseña para ana:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libevent-core-2.1-7t64
Paquetes sugeridos:
```

Editaremos este archivo:



Cambiamos a perfumes móviles:

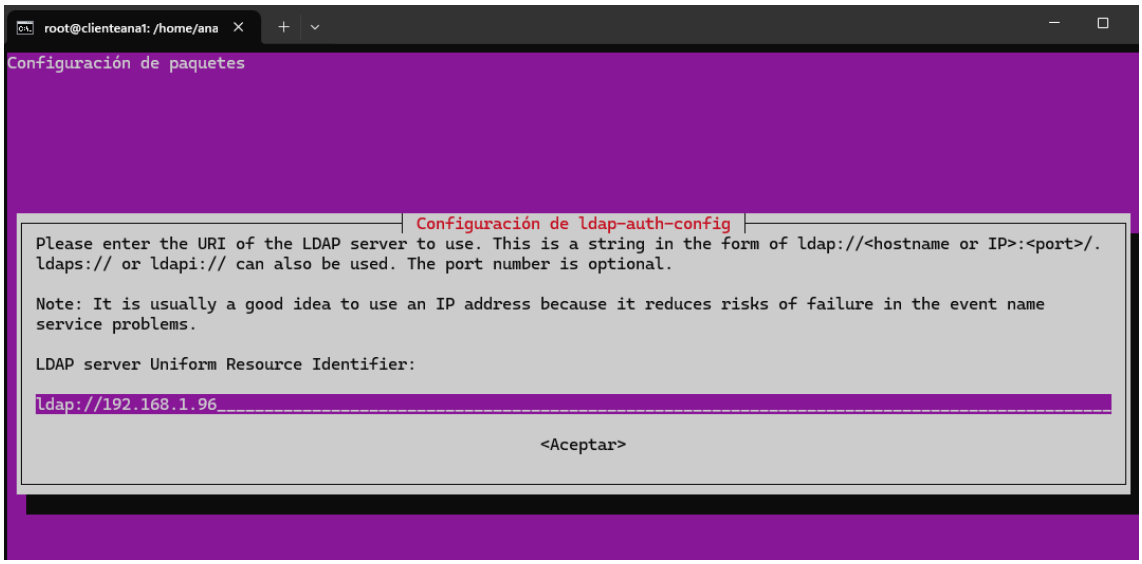


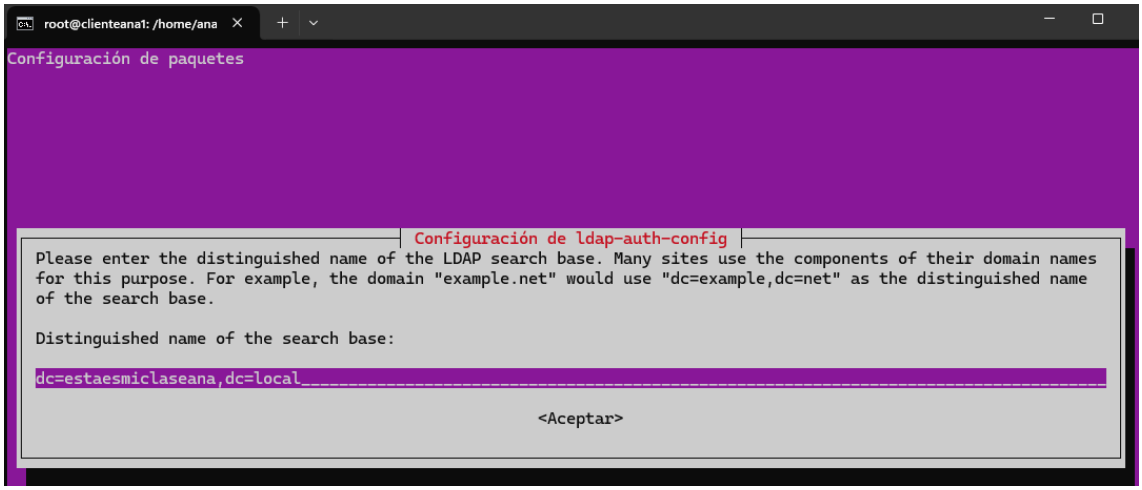


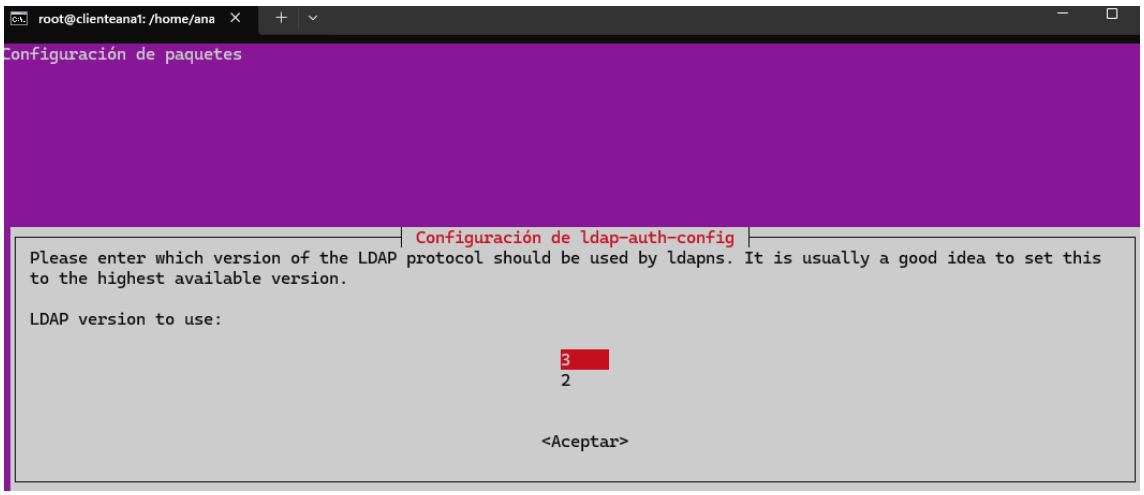
11. Comprobar el acceso de los dos tipos de usuarios (perfiles móviles y locales) al dominio.

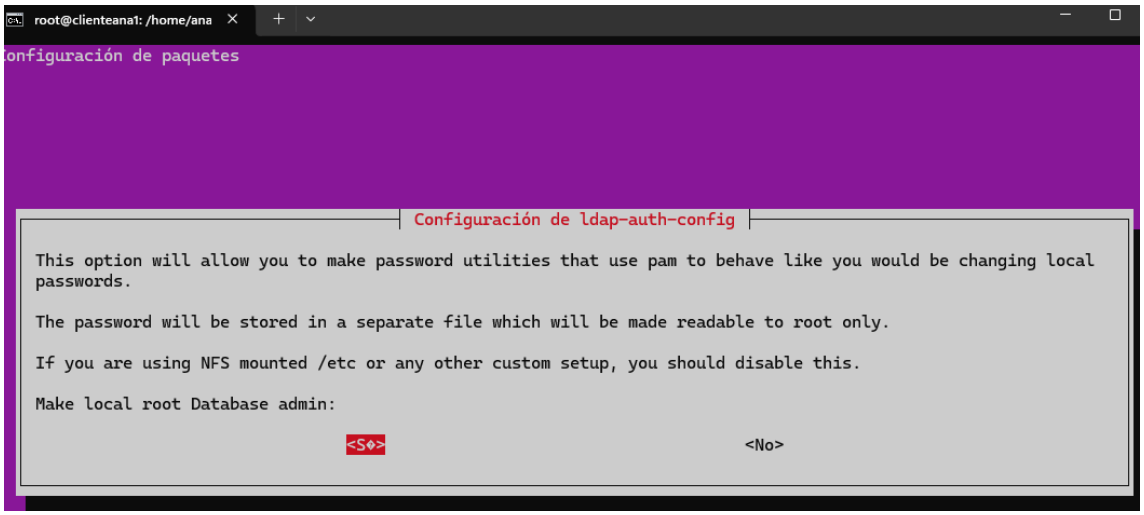
Ponemos este comando:

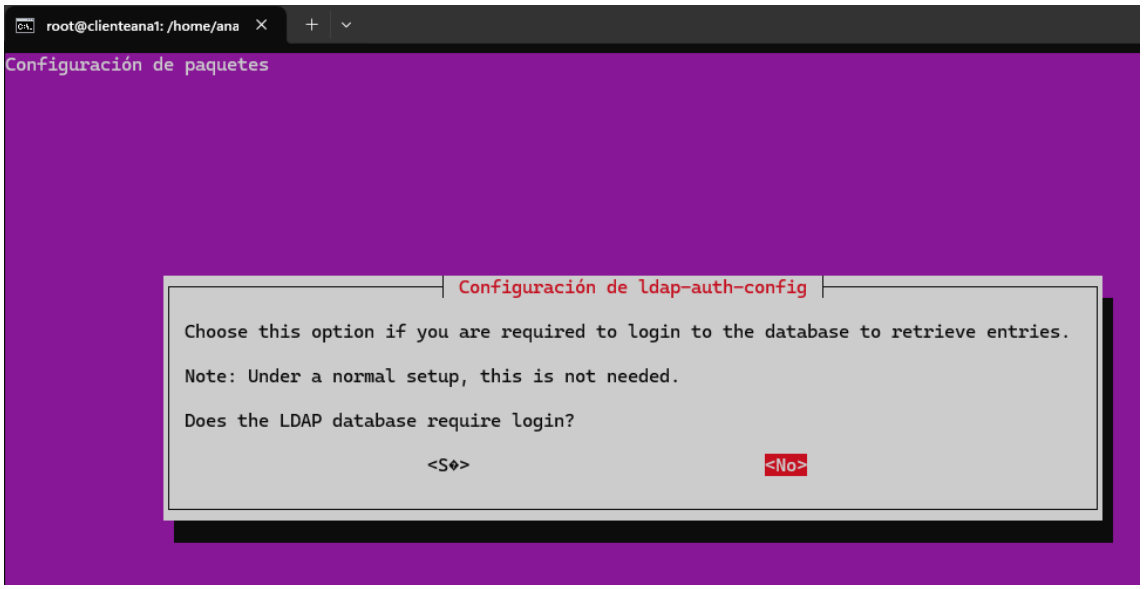
apt-get install libnss-ldap libpam-ldap ldap-utils -y

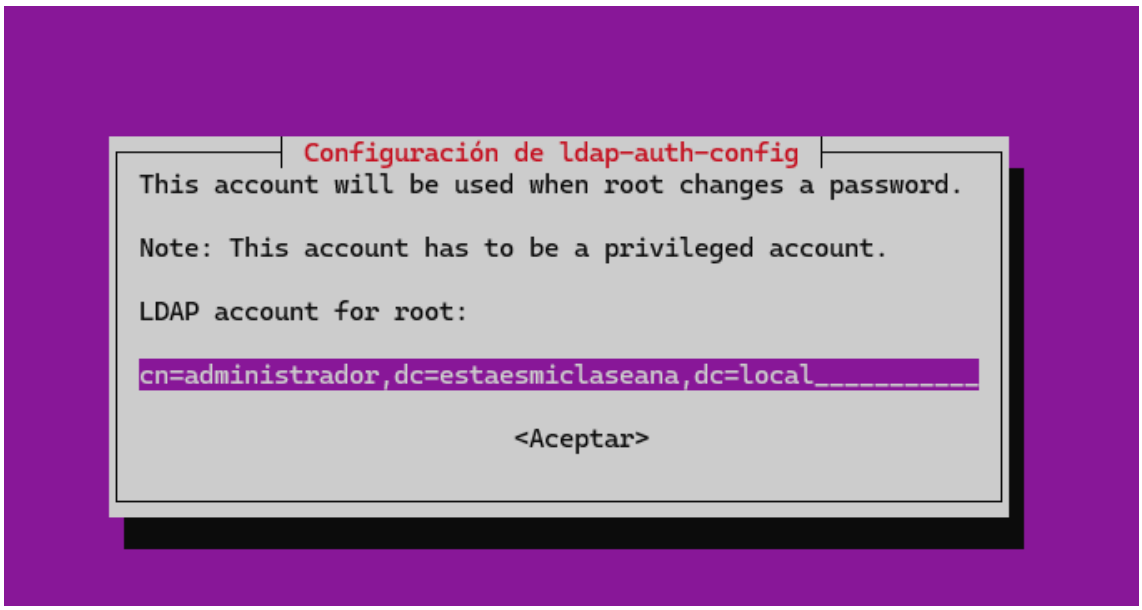


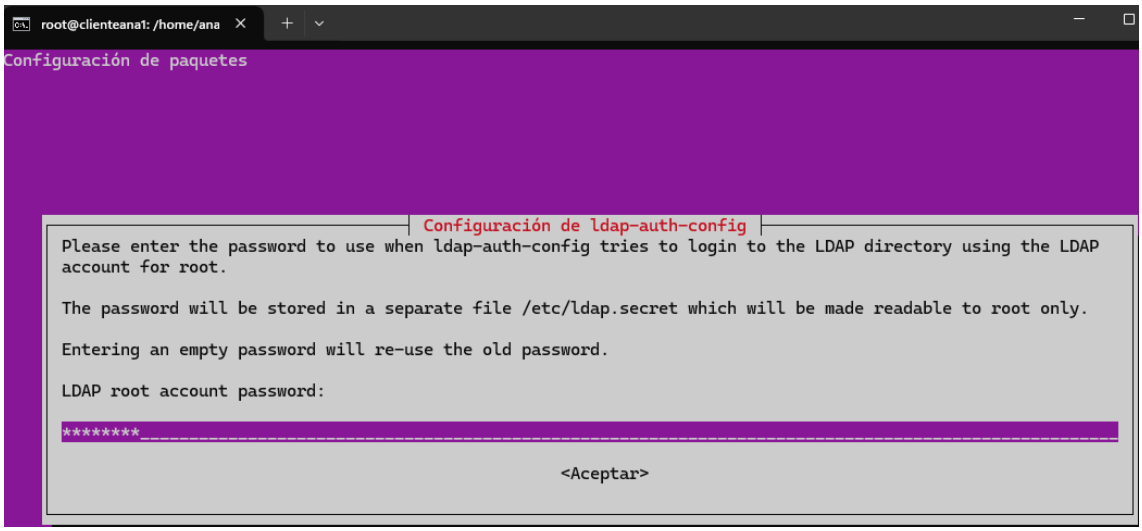


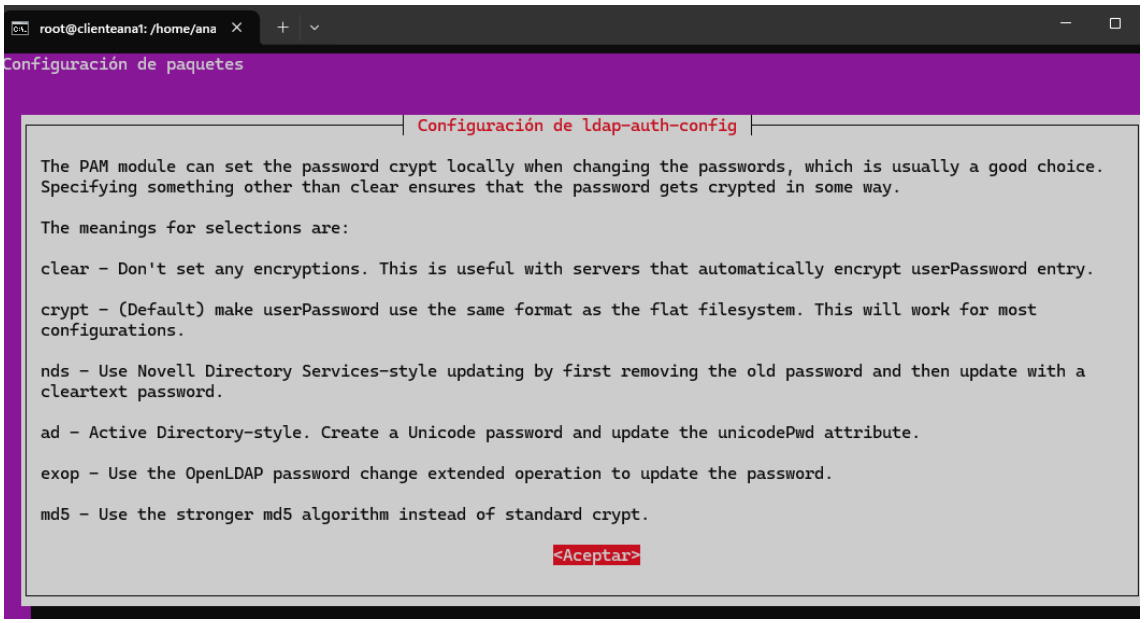

root@clienteana1: /home/ana
Configuración de paquetes
Configuración de ldap-auth-config
Please enter which version of the LDAP protocol should be used by ldapns. It is usually a good idea to set this to the highest available version.
LDAP version to use:
3
2
<Aceptar>


root@clienteana1: /home/ana
Configuración de paquetes
Configuración de ldap-auth-config
This option will allow you to make password utilities that use pam to behave like you would be changing local passwords.
The password will be stored in a separate file which will be made readable to root only.
If you are using NFS mounted /etc or any other custom setup, you should disable this.
Make local root Database admin:
<Sí>
<No>

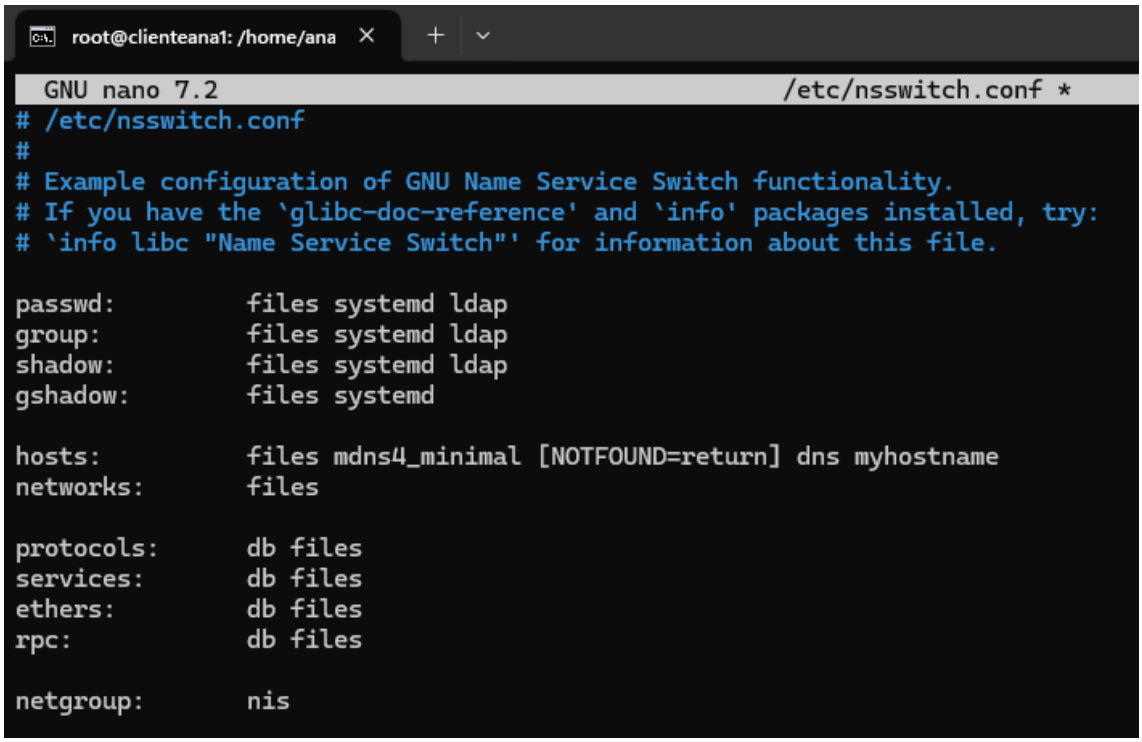

root@clienteana1: /home/ana
Configuración de paquetes
Configuración de ldap-auth-config
Choose this option if you are required to login to the database to retrieve entries.
Note: Under a normal setup, this is not needed.
Does the LDAP database require login?
<Sí>
<No>


Configuración de ldap-auth-config
This account will be used when root changes a password.
Note: This account has to be a privileged account.
LDAP account for root:
cn=administrador,dc=estaesmiclaseana,dc=local
<Aceptar>

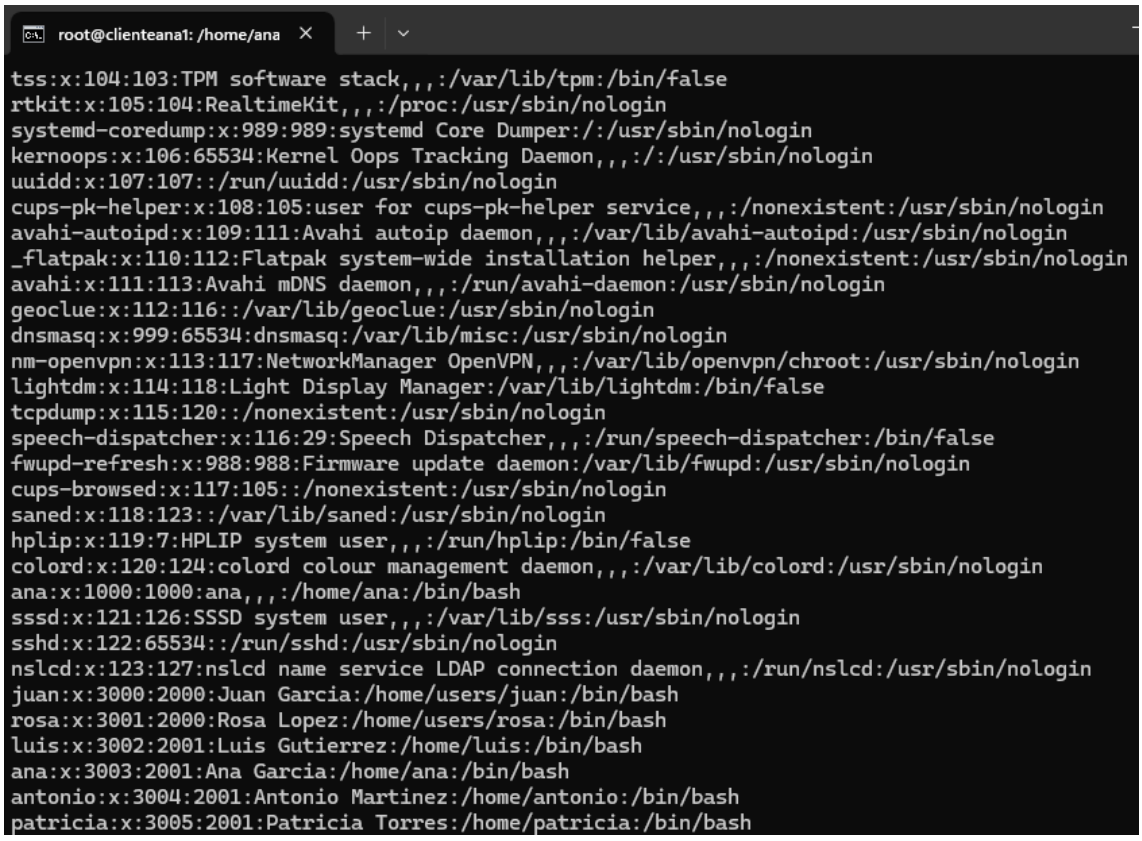

root@clienteana1: /home/ana
Configuración de paquetes
Configuración de ldap-auth-config
Please enter the password to use when ldap-auth-config tries to login to the LDAP directory using the LDAP account for root.
The password will be stored in a separate file /etc/ldap.secret which will be made readable to root only.
Entering an empty password will re-use the old password.
LDAP root account password:
****
<Aceptar>


root@clienteana1: /home/ana
Configuración de paquetes
Configuración de ldap-auth-config
The PAM module can set the password crypt locally when changing the passwords, which is usually a good choice. Specifying something other than clear ensures that the password gets crypted in some way.
The meanings for selections are:
clear - Don't set any encryptions. This is useful with servers that automatically encrypt userPassword entry.
crypt - (Default) make userPassword use the same format as the flat filesystem. This will work for most configurations.
nds - Use Novell Directory Services-style updating by first removing the old password and then update with a cleartext password.
ad - Active Directory-style. Create a Unicode password and update the unicodePwd attribute.
exop - Use the OpenLDAP password change extended operation to update the password.
md5 - Use the stronger md5 algorithm instead of standard crypt.
<Aceptar>

Vamos a cambiar este archivo, donde añadiremos ldap:



Haremos la comprobación con getent password: (esta captura es de antes de cambiar el directorio)



```
nscd:x:127:
jefes:*:2000:
subordinados:*:2001:
root@clienteana1:/home/ana#
```

Vamos al archivo /etc/pam.d/common-password y eliminamos use-authtok.

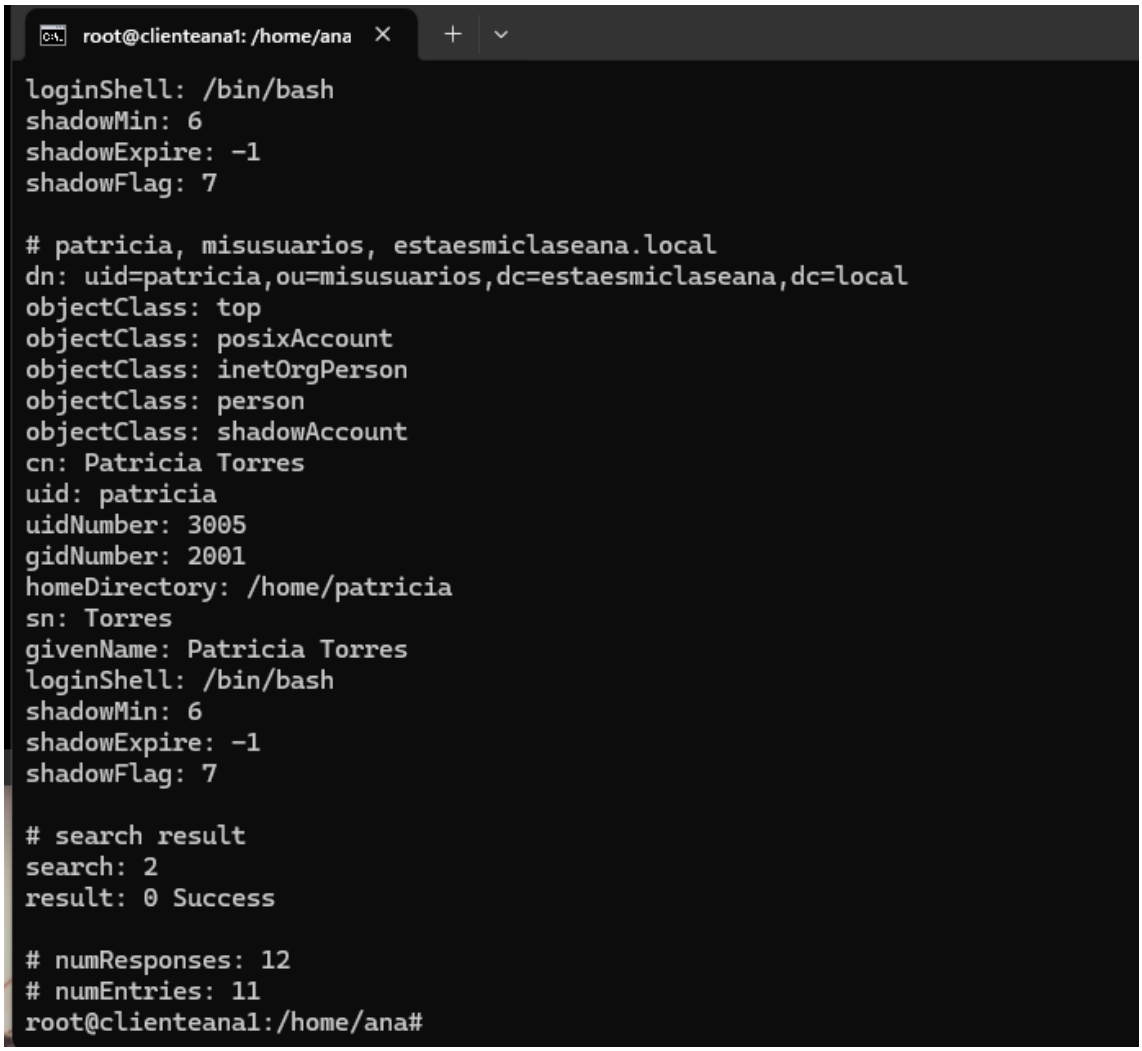
```
root@clienteana1: /home/ana
 GNU nano 7.2                                /etc/pam.d/common-password
#between Debian 11 and older releases replace "yescrypt" with "sha512"
#for compatibility .  The "obscure" option replaces the old
#`OBSCURE_CHECKS_ENAB' option in login.defs.  See the pam_unix manpage
#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 yescrypt
password        [success=1 user_unknown=ignore default=die]     pam_ldap.so 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
password        optional        pam_ecryptfs.so
# end of pam-auth-update config
```

También modificamos este archivo añadiendo al final este texto:

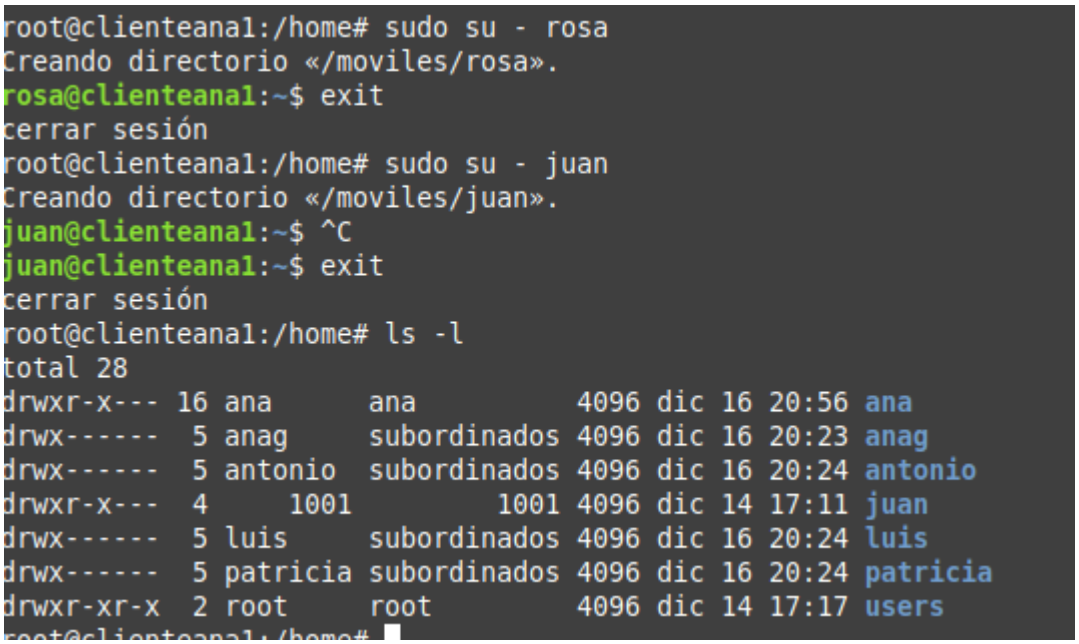
```
root@clienteana1: /home/ana
 GNU nano 7.2                                /etc/pam.d/common-session *
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default 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_ecryptfs.so unwrap
# end of pam-auth-update config
session optional        pam_mkhomed ir.so skel=/etc/skel umask=077
```

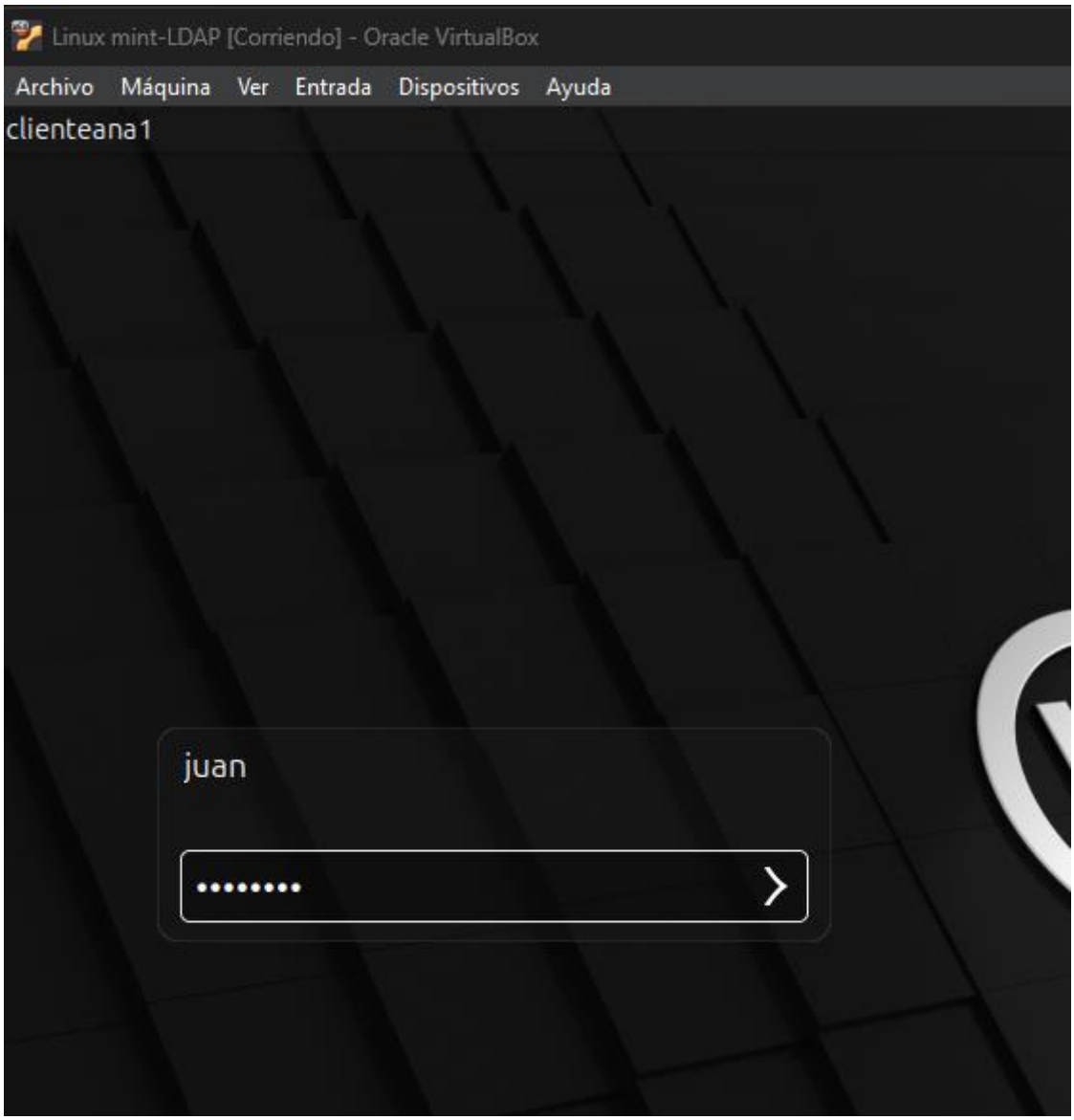
Vamos a comprobar que el fichero está bien usando este comando:

ldapsearch -x -H ldap://192.168.2.110 -b "dc=estaesmiclaseana,dc=local"



Iniciamos sesión con cada uno para que creen los directorios:



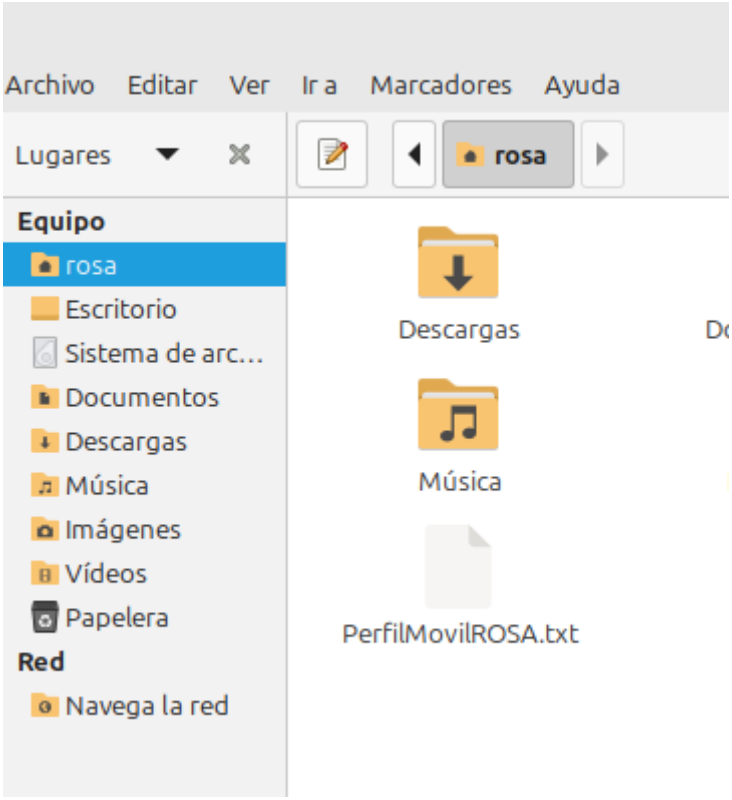


Comprobamos las carpetas del directorio

```
juan@clienteana1:~$ cd /home
juan@clienteana1:/home$ ls -l
total 28
drwxr-x--- 16 ana      ana          4096 dic 14 18:12 ana
drwx------  5 anag     subordinados 4096 dic 16 20:23 anag
drwx------  5 antonio  subordinados 4096 dic 16 20:24 antonio
drwxr-x---  4     1001         1001 4096 dic 14 17:11 juan
drwx------  5 luis     subordinados 4096 dic 16 20:24 luis
drwx------  5 patricia subordinados 4096 dic 16 20:24 patricia
drwxr-xr-x  2 root     root         4096 dic 14 17:17 users
juan@clienteana1:/home$
```

12. Comprobar que el perfil móvil funciona correctamente.

Voy a crear un archivo .txt para probar.




```
rosa@clienteana1:~$ ls -l
total 32
drwxr-xr-x 2 rosa jefes 4096 dic 16 20:27 Descargas
drwxr-xr-x 2 rosa jefes 4096 dic 16 20:27 Documentos
drwxr-xr-x 2 rosa jefes 4096 dic 16 20:27 Escritorio
drwxr-xr-x 2 rosa jefes 4096 dic 16 20:27 Imágenes
drwxr-xr-x 2 rosa jefes 4096 dic 16 20:27 Música
-rw-r--r-- 1 rosa jefes    0 dic 16 20:27 PerfilMovilROSA.txt
drwxr-xr-x 2 rosa jefes 4096 dic 16 20:27 Plantillas
drwxr-xr-x 2 rosa jefes 4096 dic 16 20:27 Público
drwxr-xr-x 2 rosa jefes 4096 dic 16 20:27 Vídeos
```

Compruebo en el servidor:

```
root@servidorana:/moviles/rosa# ls -l
total 32
drwxr-xr-x 2 3001 2000 4096 dic 16 20:02 Descargas
drwxr-xr-x 2 3001 2000 4096 dic 16 20:02 Documentos
drwxr-xr-x 2 3001 2000 4096 dic 16 20:02 Escritorio
drwxr-xr-x 2 3001 2000 4096 dic 16 20:02 Imágenes
drwxr-xr-x 2 3001 2000 4096 dic 16 20:02 Música
-rw-r--r-- 1 3001 2000    0 dic 16 20:02 PerfilMovilROSA.txt
drwxr-xr-x 2 3001 2000 4096 dic 16 20:02 Plantillas
drwxr-xr-x 2 3001 2000 4096 dic 16 20:02 Público
drwxr-xr-x 2 3001 2000 4096 dic 16 20:02 Vídeos
```

También lo haré con juan:

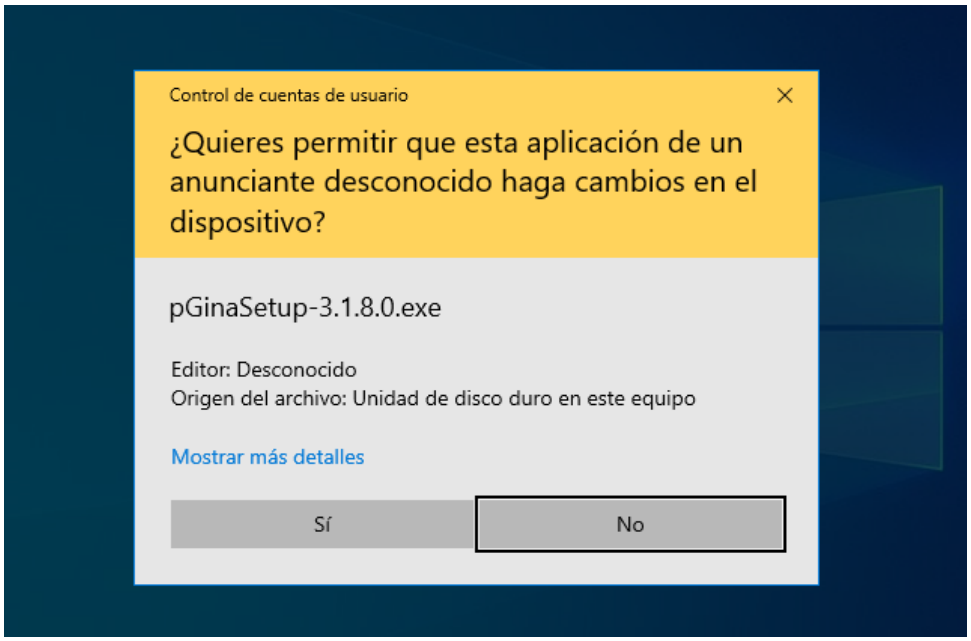
```
                                    juan@clienteana1: ~
 Archivo  Editar  Ver  Buscar  Terminal  Ayuda
juan@clienteana1:~$ ls -l
total 32
drwxr-xr-x 2 juan jefes 4096 dic 16 21:04 Descargas
drwxr-xr-x 2 juan jefes 4096 dic 16 21:04 Documentos
drwxr-xr-x 2 juan jefes 4096 dic 16 21:04 Escritorio
drwxr-xr-x 2 juan jefes 4096 dic 16 21:04 Imágenes
drwxr-xr-x 2 juan jefes 4096 dic 16 21:04 Música
-rw-r--r-- 1 juan jefes    0 dic 16 21:05 PerfilMovilJUAN.txt
drwxr-xr-x 2 juan jefes 4096 dic 16 21:04 Plantillas
drwxr-xr-x 2 juan jefes 4096 dic 16 21:04 Público
drwxr-xr-x 2 juan jefes 4096 dic 16 21:04 Vídeos
juan@clienteana1:~$
```

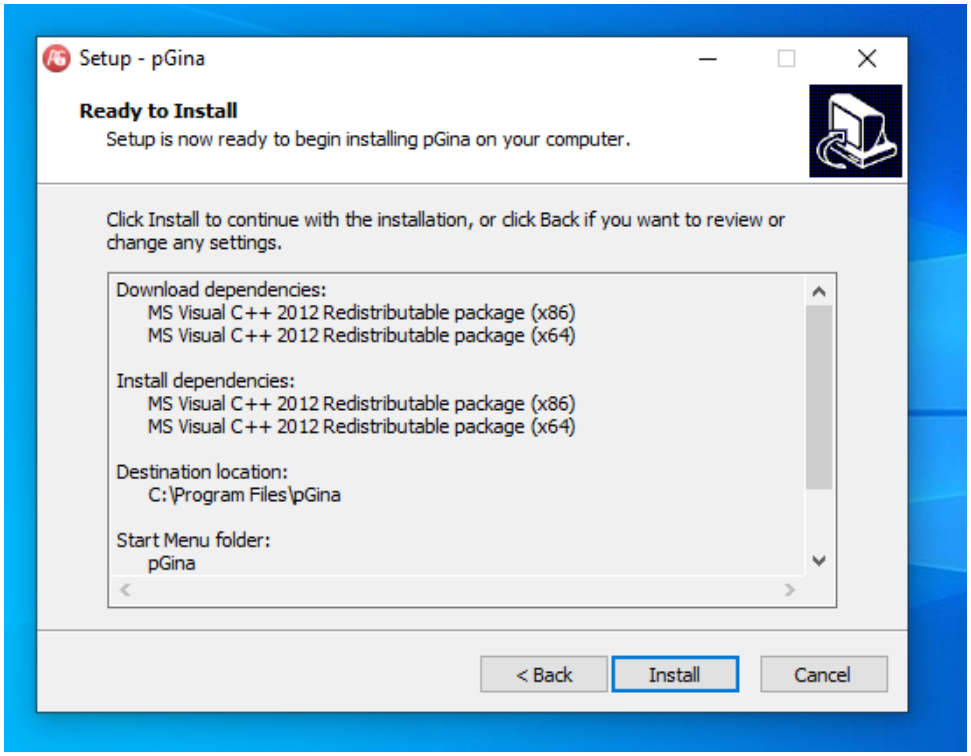
Y compruebo en el servidor:

```
root@servidorana:/moviles/rosa# cd /moviles/juan
root@servidorana:/moviles/juan# ls -l
total 32
drwxr-xr-x 2 3000 2000 4096 dic 16 20:04 Descargas
drwxr-xr-x 2 3000 2000 4096 dic 16 20:04 Documentos
drwxr-xr-x 2 3000 2000 4096 dic 16 20:04 Escritorio
drwxr-xr-x 2 3000 2000 4096 dic 16 20:04 Imágenes
drwxr-xr-x 2 3000 2000 4096 dic 16 20:04 Música
-rw-r--r-- 1 3000 2000    0 dic 16 20:05 PerfilMovilJUAN.txt
drwxr-xr-x 2 3000 2000 4096 dic 16 20:04 Plantillas
drwxr-xr-x 2 3000 2000 4096 dic 16 20:04 Público
drwxr-xr-x 2 3000 2000 4096 dic 16 20:04 Vídeos
```

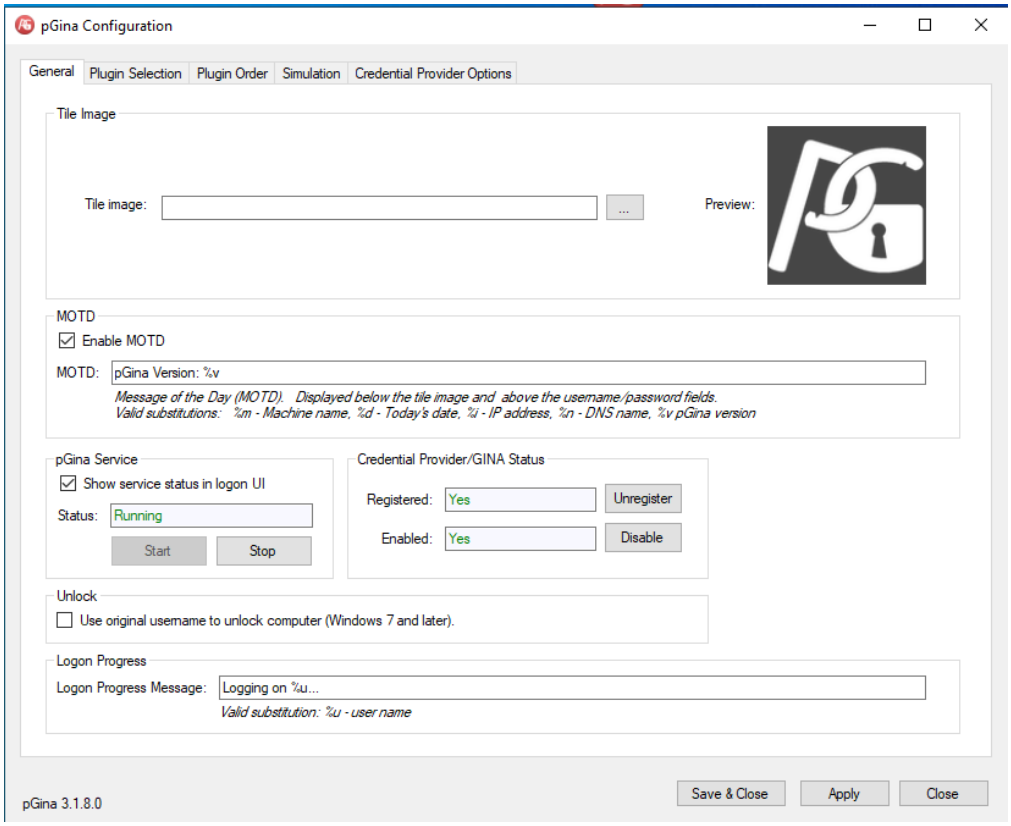
13. Configurar el cliente de Windows 10 e incorporarlo al dominio y comprobar su correcto funcionamiento.

Descargo el programa pGina desde Classroom y voy a instalarlo:

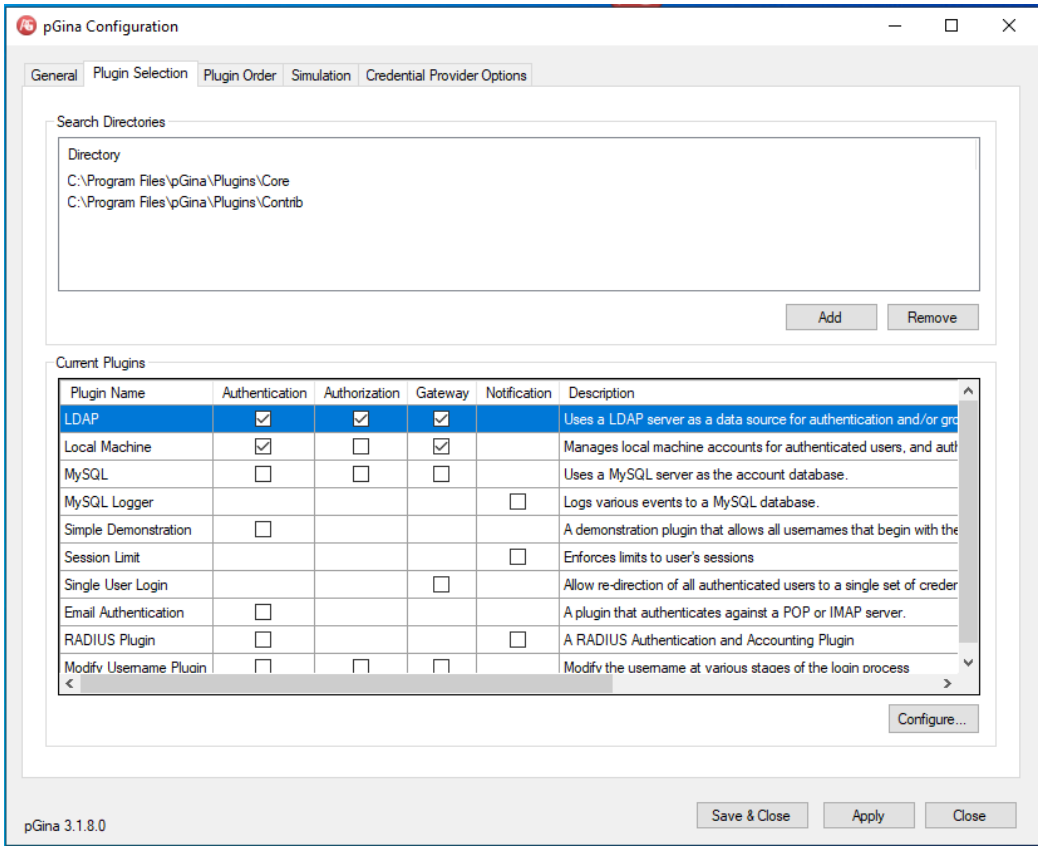




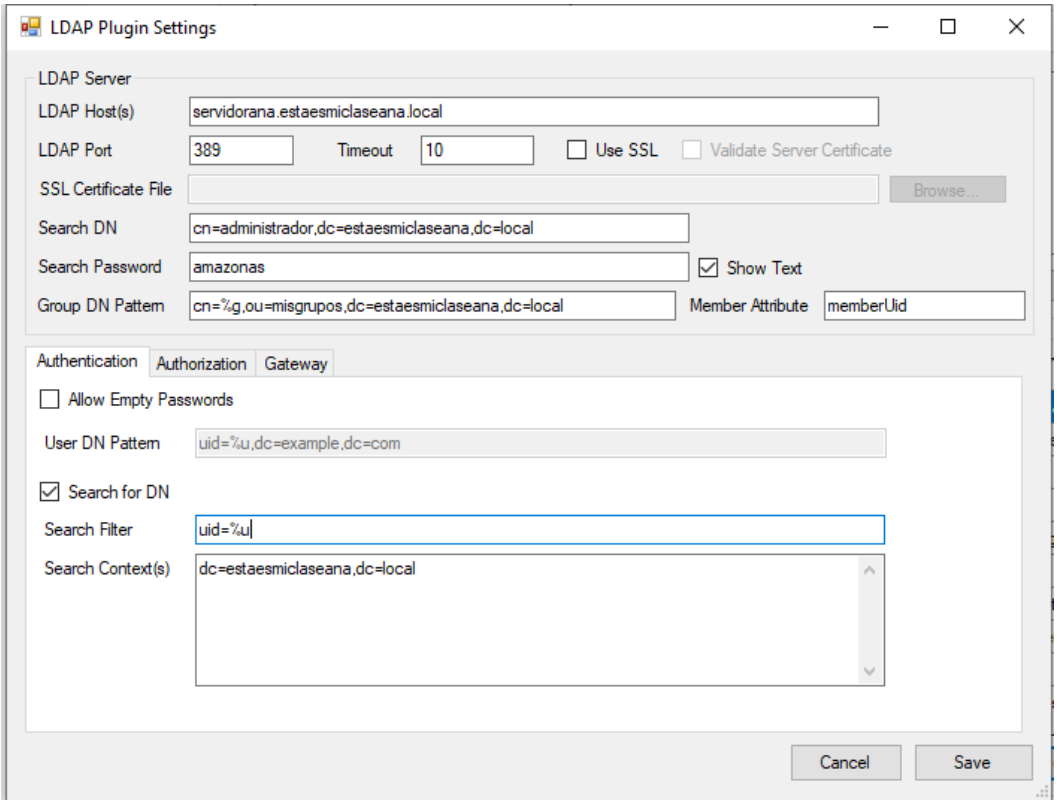
Ahora abriré el programa y nos iremos a Plugin selection:



Aquí haremos clic en todas las opciones de LDAP y aplicaremos:

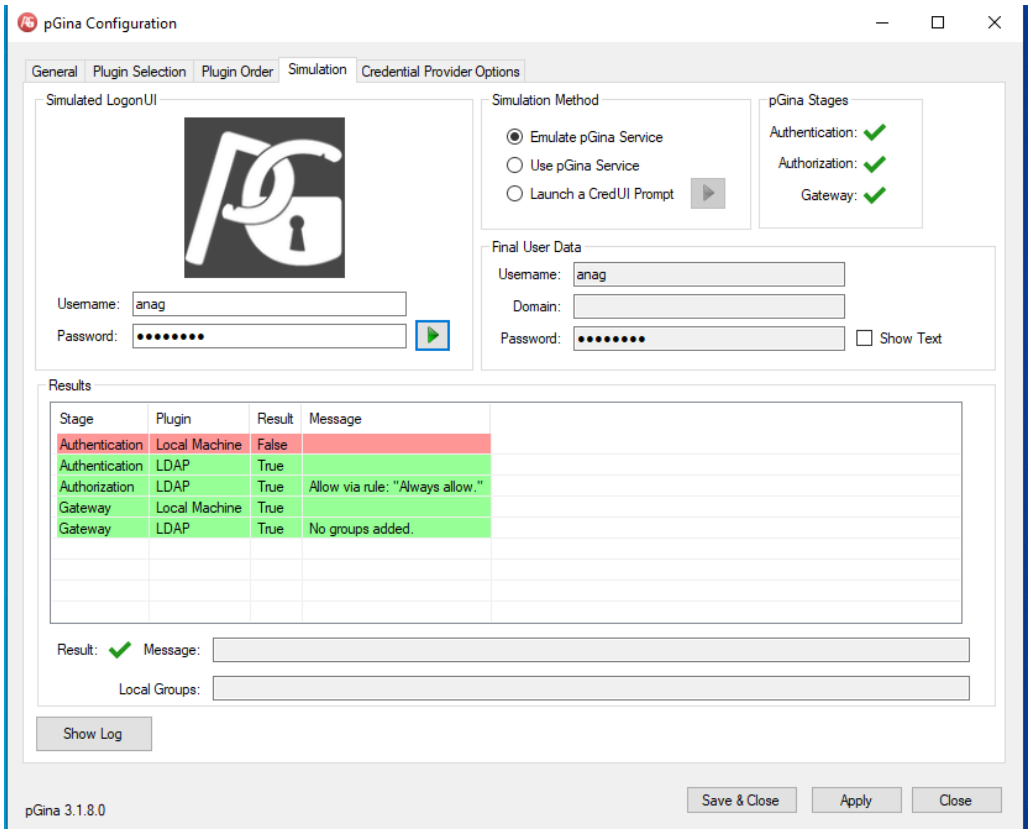


Para poder hacer la conexión le daremos a configure.. Y pondremos los datos de nuestro LDAP, el nombre, el administrador y en group dn pattern pondremos la ruta donde debe buscar los usuarios.

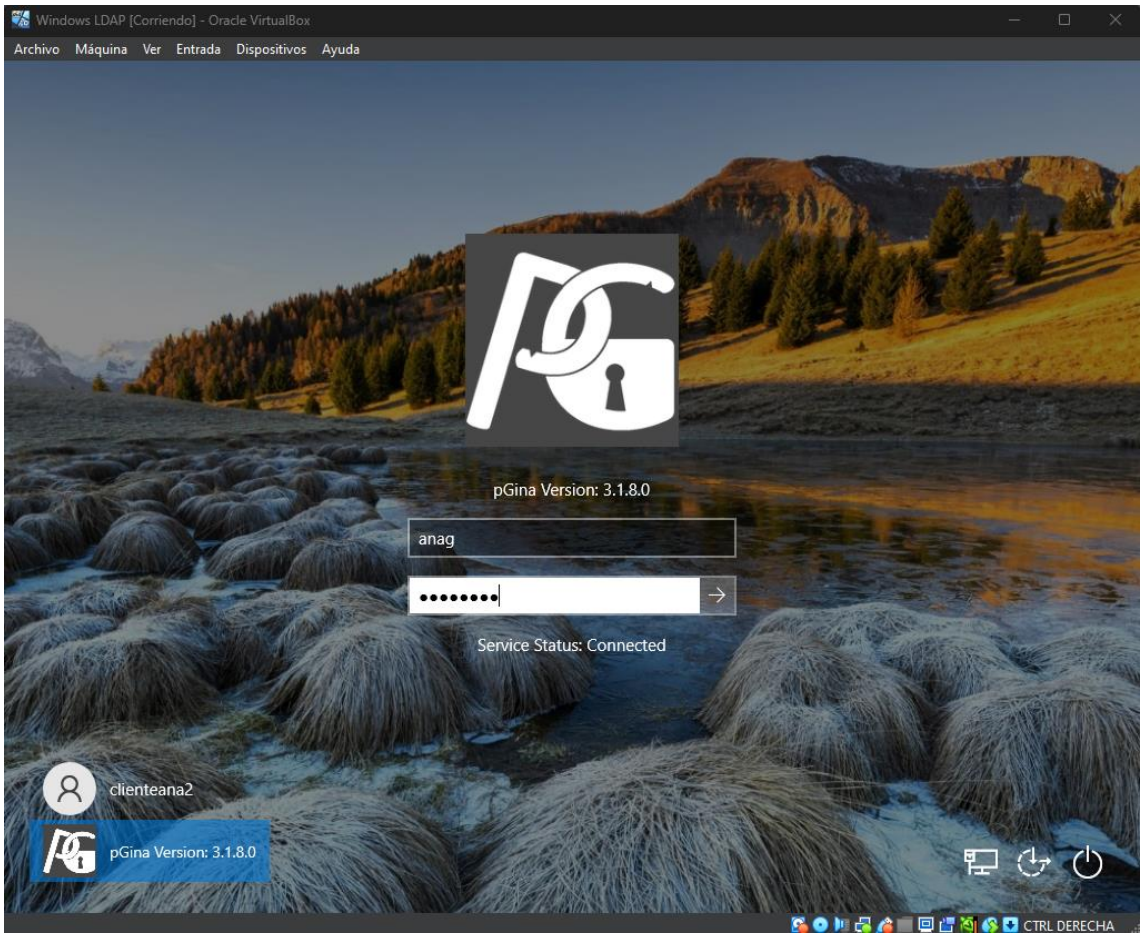


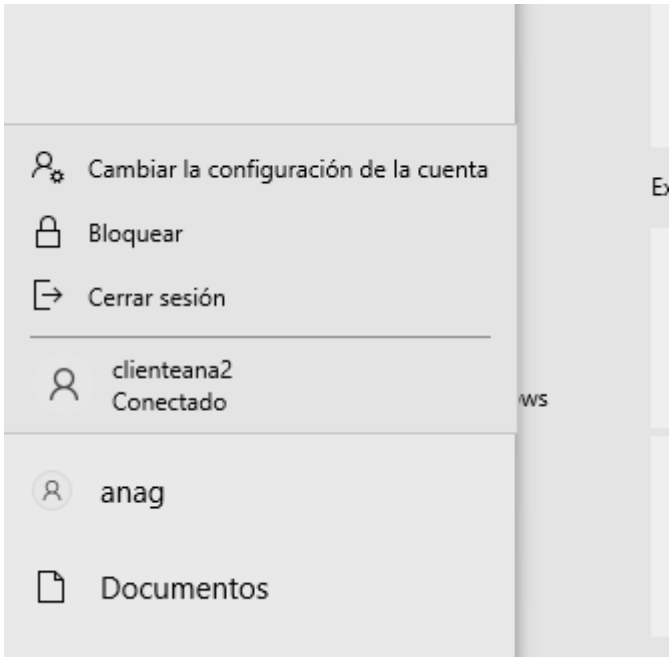
Comprobaremos en la simulación con el usuario anag.

El error que da es porque busca el usuario en el Windows que estamos usando.

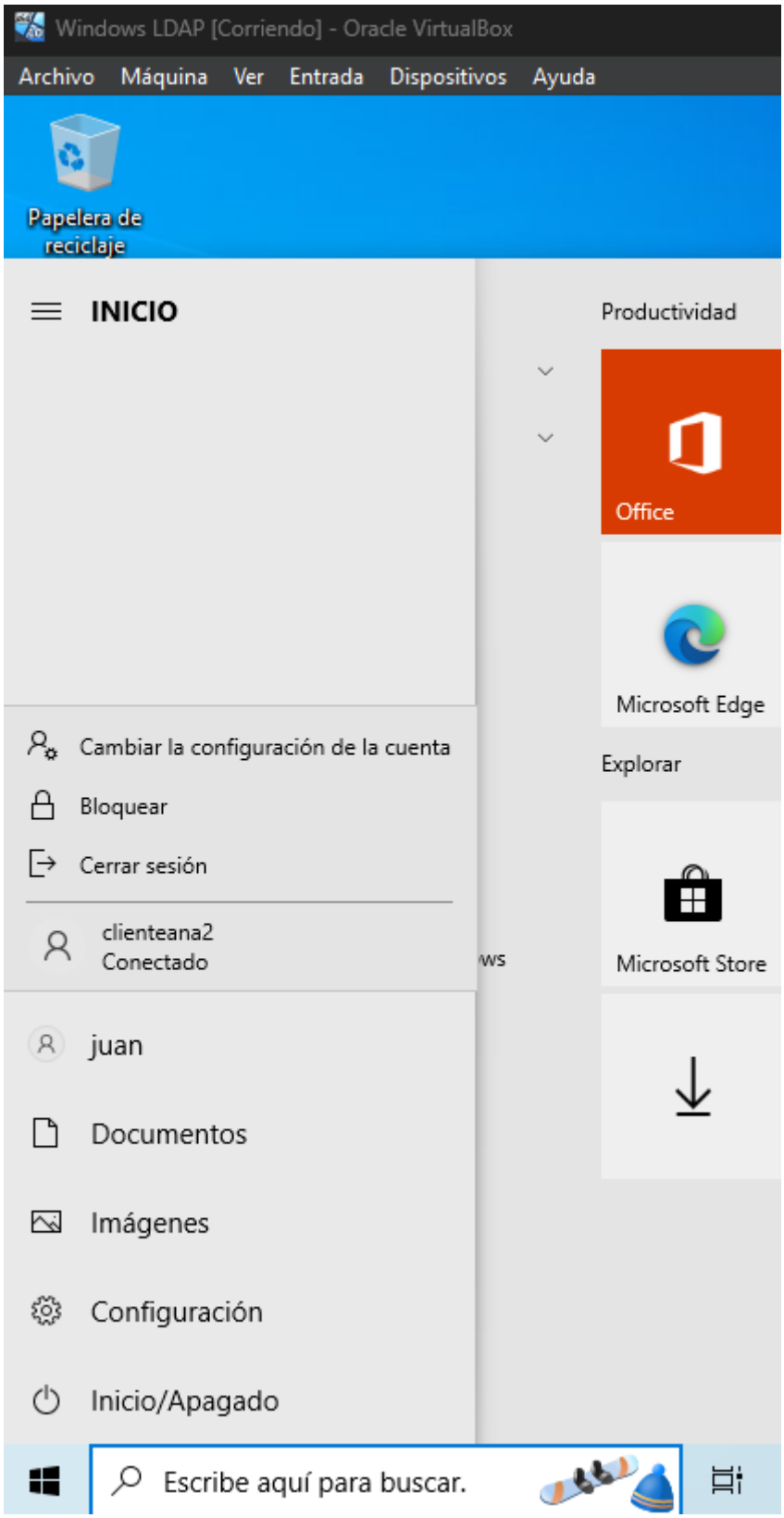


Ahora sí comprobaremos accediendo





Y también con juan

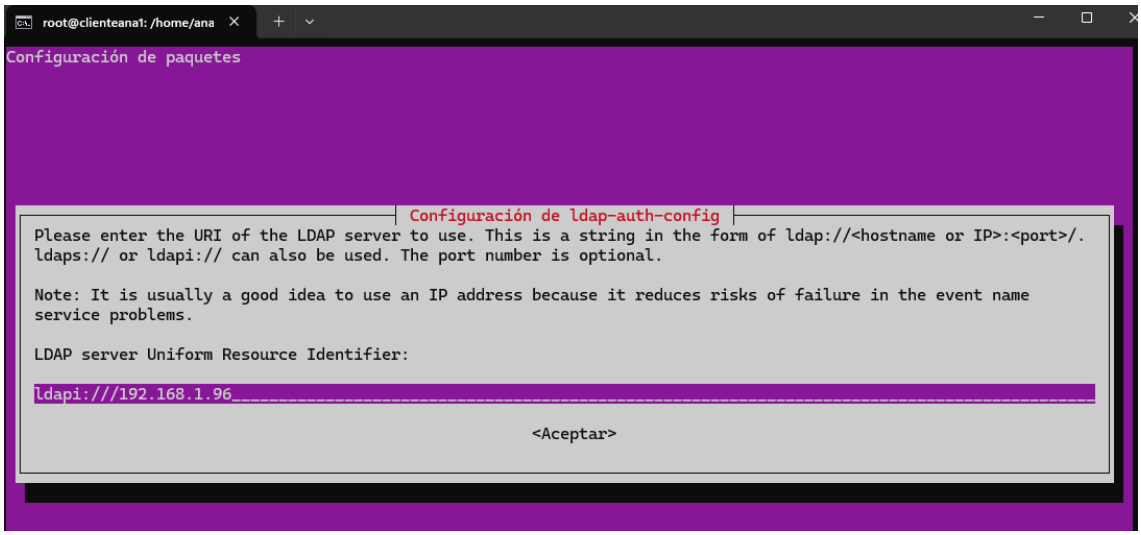


Incidencias

Tuve este fallo:

```
# patricia, misusuarios, estaesmiclaseana.local
dn: uid=patricia,ou=misusuarios,dc=estaesmiclaseana,dc=local
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
objectClass: shadowAccount
cn: Patricia Torres
uid: patricia
uidNumber: 3005
gidNumber: 2001
homeDirectory: /home/patricia
sn: Torres
givenName: Patricia Torres
loginShell: /bin/bash
shadowMin: 6
shadowExpire: -1
shadowFlag: 7

# search result
search: 2
result: 0 Success

# numResponses: 12
# numEntries: 11
root@clienteana1:/home/ana# sudo su - luis
su: user luis does not exist or the user entry does not contain all the required fields
root@clienteana1:/home/ana# sudo su - patricia
su: user patricia does not exist or the user entry does not contain all the required fields
```

Y fue porque al hacer apt-get install libnss-ldap libpam-ldap ldap-utils -y no eliminé los caracteres sobrantes:



También tengo un error con juan que me ha creado carpeta con nombre de uid.

Además, el usuario ana es el mío y anag es el usuario de ana García.

He tenido incidencias de tonterías como nombres o ips mal puestas.

Valoración

Esta práctica me ha resultado más complicada, es la práctica a la que más horas he echado de todo el curso y más incidencias he tenido aunque fueran tontas.

Pero también sé que LDAP es importante en muchas empresas así que será útil.