



P06- SERVIDOR LDAP

ANA OROZCO ASENSIO



2ºASIR

I.E.S. ANTONIO MACHADO
ASO

Contenido

Contenido	2
Introducción.	3
1. Montar las máquinas virtuales. ¿Qué has tenido que modificar?.....	3
2. Instalar y configurar un servidor DNS que nos resuelva nuestras direcciones del dominio.....	5
3. Realizar consultas dig/nslookup para comprobar el funcionamiento del servidor DNS.....	9
4. Instalar el Servidor LDAP, detallando los pasos seguidos.	10
4. Crear el dominio estaesmiclaseana.local cuyo usuario administrador se llamará administrador.	16
6. Crear las unidades organizativas misgrupos y misusuarios, para grupos y usuarios, respectivamente.....	18
7. Crear los grupos jefes y subordinados en la unidad organizativa misgrupos. ...	20
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.....	22
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.	23
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?.....	26
11. Comprobar el acceso de los dos tipos de usuarios (perfiles móviles y locales) al dominio.....	29
12. Comprobar que el perfil móvil funciona correctamente.	36
13. Configurar el cliente de Windows 10 e incorporarlo al dominio y comprobar su correcto funcionamiento.	38
Incidencias	43
Valoración	44

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*

```
network:
  ethernets:
    enp0s3:
      dhcp4: no
      addresses:
        - 192.168.1.96/24
      nameservers:
        addresses:
          - 8.8.8.8
          - 8.8.4.4
      routes:
        - to: default
          via: 192.168.1.1
  version: 2
```

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

```
root@servidorana:/home/servidorana# cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 servidorana

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
root@servidorana:/home/servidorana# cat /etc/hostname
servidorana
root@servidorana:/home/servidorana#
```

Miré la IP del cliente1:

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

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  X + v
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:

```
root@servidorana:/home/servidorana# service bind9 restart
root@servidorana:/home/servidorana# service bind9 status
● named.service - BIND Domain Name Server
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Fri 2024-12-13 15:44:20 UTC; 9s ago
     Docs: man:named(8)
   Main PID: 2827 (named)
    Status: "running"
     Tasks: 6 (limit: 6776)
    Memory: 5.5M (peak: 5.9M)
       CPU: 24ms
    CGroup: /system.slice/named.service
            └─2827 /usr/sbin/named -f -u bind -4

dic 13 15:44:20 servidorana named[2827]: zone 0.in-addr.arpa/IN: loaded serial 1
dic 13 15:44:20 servidorana named[2827]: zone 127.in-addr.arpa/IN: loaded serial 1
dic 13 15:44:20 servidorana named[2827]: zone localhost/IN: loaded serial 2
dic 13 15:44:20 servidorana systemd[1]: Started named.service - BIND Domain Name Server.
dic 13 15:44:20 servidorana named[2827]: all zones loaded
dic 13 15:44:20 servidorana named[2827]: running
dic 13 15:44:20 servidorana named[2827]: zone 1.168.192.in-addr.arpa/IN: sending notifies (serial 2)
dic 13 15:44:20 servidorana named[2827]: zone estaesmiclaseana.local/IN: sending notifies (serial 2)
dic 13 15:44:20 servidorana named[2827]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
dic 13 15:44:20 servidorana named[2827]: resolver priming query complete: success
```

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

```
root@servidorana:/home/ser  X  +  v
GNU nano 7.2 /etc/netplan/50-cloud-init.yaml *
# This file is generated from information provided by the datasource. Changes
# to it will not persist across an instance reboot. To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  ethernets:
    enp0s3:
      dhcp4: no
      addresses:
        - 192.168.1.96/24
      nameservers:
        addresses: [192.168.1.96]
        search: [estaesmiclaseana.local]
      routes:
        - to: default
          via: 192.168.1.1
  version: 2
```


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: fbe64e8d4048755001000000675c590c9f0bcab9f09e22b3 (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.

Editar Conexión cableada 1

Nombre de la conexión:

General Cableada Seguridad 802.1x DCB Proxy **Ajustes de IPv4** Ajustes de IPv6

Método:

Dirección

Dirección	Máscara de red	Puerta de enlace
192.168.1.97	24	192.168.1.1

Servidores DNS:

Dominios de búsqueda:

ID del cliente DHCP:

☐ Requiere dirección IPv4 para que esta conexión se complete

```

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 time=17.3 ms
64 bytes from mad07s10-in-f4.1e100.net (172.217.168.164): icmp_seq=2 ttl=119 time=17.3 ms
64 bytes from mad07s10-in-f4.1e100.net (172.217.168.164): icmp_seq=3 ttl=119 time=15.4 ms
64 bytes from mad07s10-in-f4.1e100.net (172.217.168.164): icmp_seq=4 ttl=119 time=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

```

← Configuración

Red

Configuración de IP

Asignación de IP:	Manual
Dirección IPv4:	192.168.1.98
Longitud del prefijo de subred IPv4	24
Puerta de enlace de IPv4:	192.168.1.1
Servidores DNS IPv4:	192.168.1.96 8.8.8.8

Editar

```
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
```

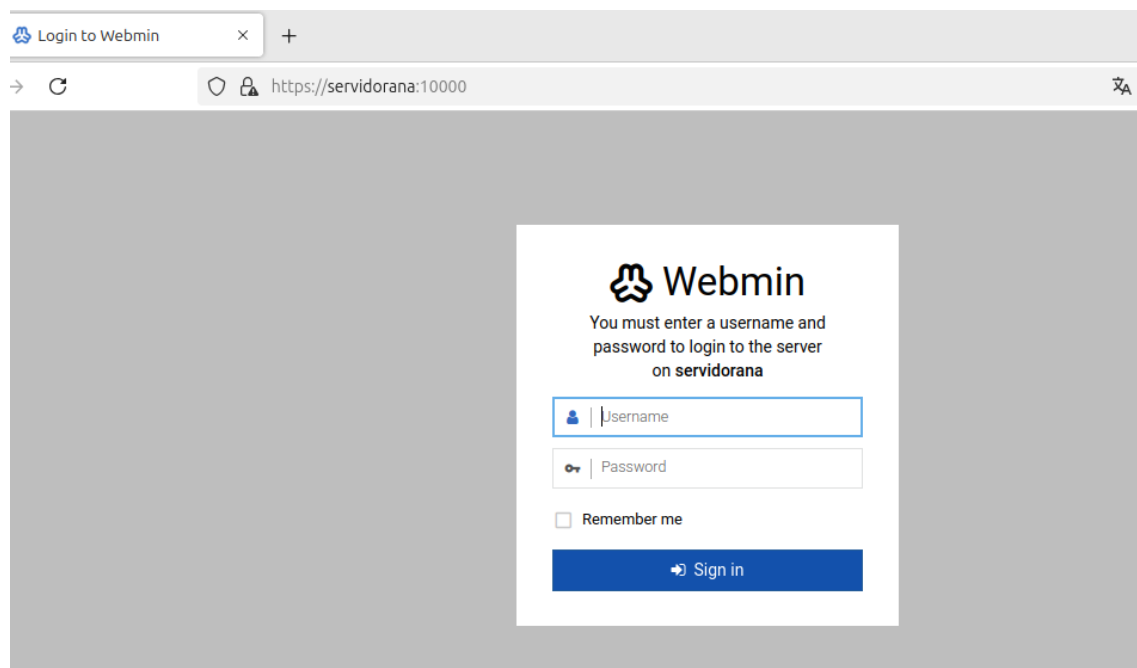
Ahora instalamos el Webmin a través de curl:

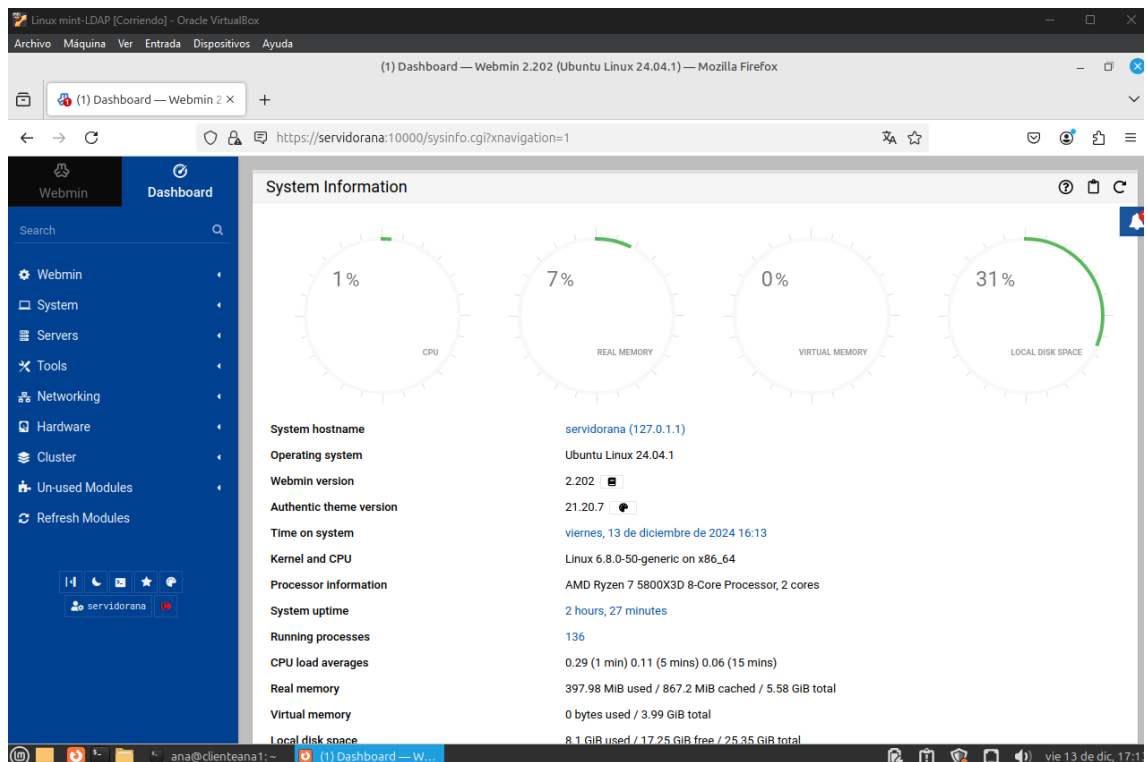
```
root@servidorana:/home/servidorana# curl -o webmin-setup-repos.sh https://raw.githubusercontent.com/webmin/webmin/master/webmin-setup-repos.sh
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 5286 100 5286    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:

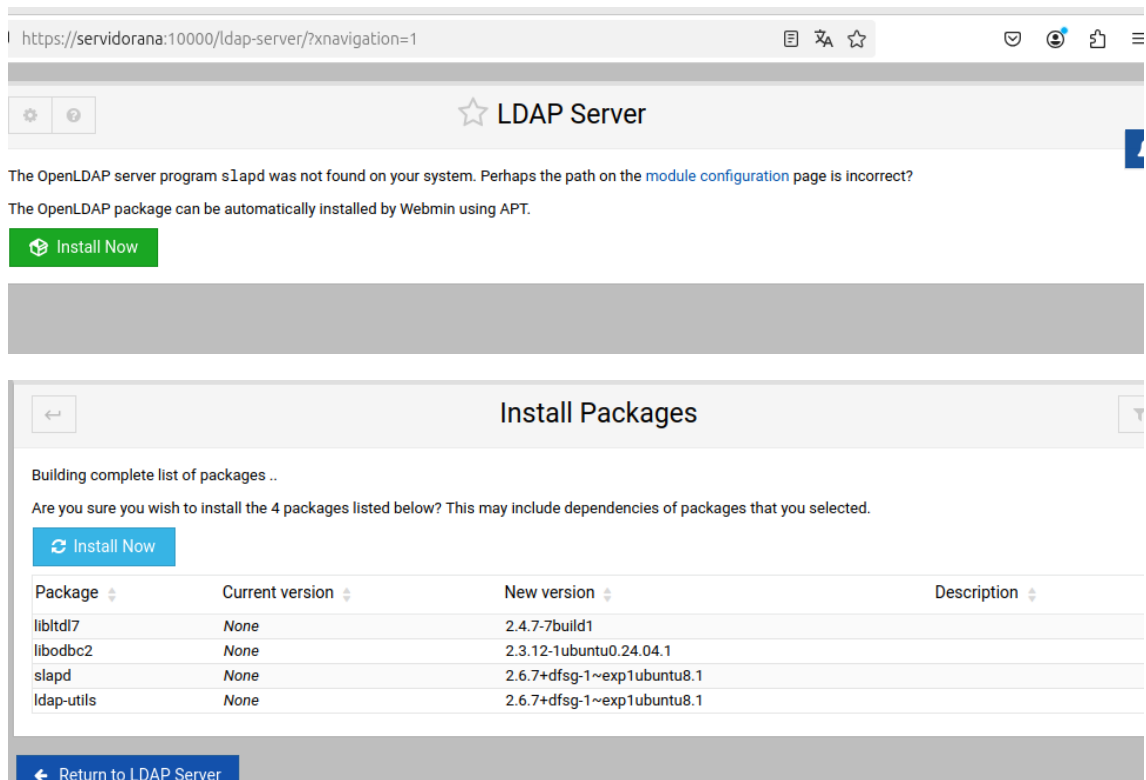
```
root@servidorana:/home/servidorana# apt-get update
Obj:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Obj:2 http://es.archive.ubuntu.com/ubuntu noble InRelease
Obj:3 http://es.archive.ubuntu.com/ubuntu noble-updates InRelease
Obj:4 http://es.archive.ubuntu.com/ubuntu noble-backports 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
```

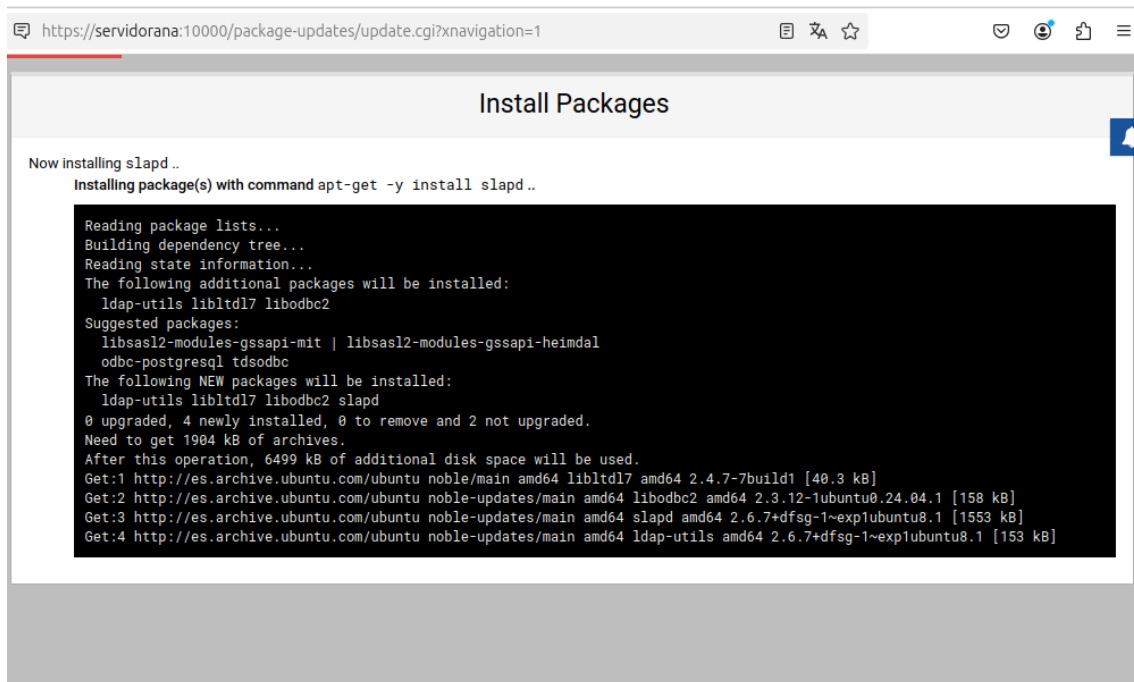
En clienteana1 iremos al webmin:



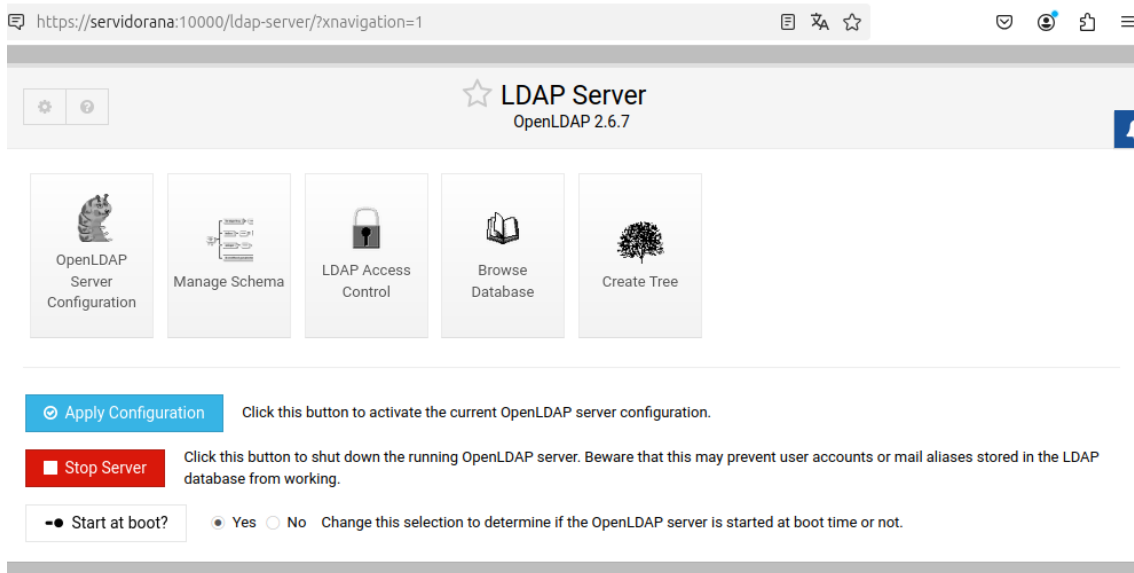


En el buscador ponemos LDAP Server y lo instalamos:





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:

The screenshot shows the 'OpenLDAP Server Configuration' web interface in a browser. The URL is `https://servidorana:10000/ldap-server/edit_ldif.cgi?xnavigation=1`. The page has a navigation bar with a star icon and the title 'OpenLDAP Server Configuration'. Below the bar, there's a section for 'Global LDAP server options'. It contains several fields: 'Root DN for LDAP database' with the value 'dc=estaesmiclaseana,dc=local', 'Administration login DN' with 'cn=administrador,dc=estaesmiclaseana,dc=local', and 'Administration password' with a long SSHA encrypted string. To the right, there are options for 'New administration password' (radio buttons for 'Don't change' and 'Set to' with a text input containing 'amazonas'), 'Database entries to cache' (radio buttons for 'Default' and an empty input), and 'Maximum number of search results to return' (radio buttons for 'Default (500)' and an empty input). Below these fields is an 'Encryption options' section. At the bottom left is a 'Save' button. At the bottom right is a 'Generate SSL Certificate' button with a descriptive text: 'To run your LDAP server in TLS mode, an SSL certificate and private key must first be generated. Click this button to create a self-signed certificate for your system.' A 'Return to module index' link is at the very bottom.

Crearemos un nuevo árbol:

The screenshot shows the 'Create Tree' web interface in a browser. The URL is `https://servidorana:10000/ldap-server/edit_create.cgi?xnavigation=1`. The page has a navigation bar with a star icon and the title 'Create Tree'. Below the bar, there's a section for 'New LDAP DN tree options'. It contains two radio buttons for 'Name for new DN': 'Based on domain name' (with a text input containing 'servidorana') and 'Distinguished name' (selected, with a text input containing 'dc=estaesmiclaseana,dc=local'). Below this is a section for 'Create example object under new DN?' with radio buttons for 'No' (selected), 'Unix user', 'Unix user with mail', 'Unix group', and 'Address mapping'. At the bottom is a 'Create' button.

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

←

Error

Failed to create new tree : The Perl module Net::LDAP needed to connect to the LDAP server is not installed. The full Perl error message is :

Can't locate Net/LDAP.pm in @INC (you may need to install the Net::LDAP module) (@INC entries checked: /usr/share/webmin/vendor_perl /usr/share/webmin /etc/perl /usr/local/lib/x86_64-linux-gnu/perl/5.38.2 /usr/local/share/perl/5.38.2 /usr/lib/x86_64-linux-gnu/perl5/5.38 /usr/share/perl5 /usr/lib/x86_64-linux-gnu/perl-base /usr/lib/x86_64-linux-gnu/perl/5.38 /usr/share/perl/5.38 /usr/local/lib/site_perl /usr/share/webmin/ . . .) at (eval 76) line 1. BEGIN failed--compilation aborted at (eval 76) line 1.

You can have the Net::LDAP Perl module [automatically installed](#) from CPAN.

Error details

Can't locate Net/LDAP.pm in @INC (you may need to install the Net::LDAP module) (@INC entries checked: /usr/share/webmin/vendor_perl /usr/share/webmin /etc/perl /usr/local/lib/x86_64-linux-gnu/perl/5.38.2 /usr/local/share/perl/5.38.2 /usr/lib/x86_64-linux-gnu/perl5/5.38 /usr/share/perl5 /usr/lib/x86_64-linux-gnu/perl-base /usr/lib/x86_64-linux-gnu/perl/5.38 /usr/share/perl/5.38 /usr/local/lib/site_perl /usr/share/webmin/ . . .) at (eval 76) line 1. BEGIN failed--compilation aborted at (eval 76) line 1. : ldap-server/create.cgi (line 9)

← Return to previous page

Y empezará la instalación:

https://servidorana:10000/cpan/download.cgi?source=3&cpan=Net::LDAP&cpan=Convert::ASN1&retur

Get:28 http://es.archive.ubuntu.com/ubuntu noble/main amd64 libnet-ldap-perl all 1:0.6800+dfsg-1 [361 kB]
Get:30 http://es.archive.ubuntu.com/ubuntu noble/main amd64 libauthen-sasl-perl all 2.1700-1 [42.9 kB]
Fetched 1688 kB in 1s (1570 kB/s)
Selecting previously unselected package libclone-perl:amd64.
(Reading database ...
(Reading database ... 5%
(Reading database ... 10%
(Reading database ... 15%
(Reading database ... 20%
(Reading database ... 25%
(Reading database ... 30%
(Reading database ... 35%
(Reading database ... 40%
(Reading database ... 45%
(Reading database ... 50%
(Reading database ... 55%
(Reading database ... 60%
(Reading database ... 65%
(Reading database ... 70%
(Reading database ... 75%
(Reading database ... 80%
(Reading database ... 85%
(Reading database ... 90%
(Reading database ... 95%
(Reading database ... 100%
(Reading database ... 116493 files and directories currently installed.)
Preparing to unpack .../00-libclone-perl_0.46-1build3_amd64.deb ...
Unpacking libclone-perl:amd64 (0.46-1build3) ...
Selecting previously unselected package libconvert-asn1-perl.
Preparing to unpack .../01-libconvert-asn1-perl_0.34-1_all.deb ...
Unpacking libconvert-asn1-perl (0.34-1) ...

Justo después probaremos de nuevo y esta vez sí funcionará:

https://servidorana:10000/ldap-server/create.cgi?xnavigation=1

←

Create Tree

Creating base DN dc=estaesmiclaseana,dc=local ..
.. done

← Return to module index

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”:

The screenshot shows a web browser window with the URL `https://servidorana:10000/ldap-server/edit_browser.cgi?xnavigation=1`. The page title is "Browse Database". Below the title, there is a "Browsing:" field containing the text `dc=estaesmiclaseana,dc=local`, a green "Show" button, and a "Browse Parent" button. Below this, there are two tabs: "Child objects" (selected) and "Object attributes". The "Child objects" tab shows the message "This object has no child objects." and an "Add new sub-object" button. At the bottom, there is a blue button labeled "Return to module index".

Creamos la unidad organizativa mis usuarios:

The screenshot shows a web browser window with the URL `https://servidorana:10000/ldap-server/add_form.cgi?base=dc%3Destaesmiclaseana%2Cdc%3Dlocal&x`. The page title is "Create Object". Below the title, there is a section titled "New LDAP object details". This section contains two main parts: "New object DN" and "Parent object DN". The "New object DN" part has a field with `ou` and a value field with `misusuarios`. The "Parent object DN" part has a field with `dc=estaesmiclaseana,dc=local`. Below these, there is a section titled "Object classes" with a list containing `organizationalUnit` and `top`. At the bottom, there is a section titled "Other attributes" which contains a table with two columns: "Attribute" and "Values". The table has two rows: the first row has `ou` in the "Attribute" column and `misusuarios` in the "Values" column; the second row is empty.

Attribute	Values
ou	misusuarios

Ahora copiaré esa unidad organizativa y le cambiaré los parámetros:

https://servidorana:10000/ldap-server/edit_browser.cgi?base=ou%3Dmisusuarios%2C%3Destaesmiclaseana,dc=local

☆ Browse Database

Browsing: 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
<input type="checkbox"/> objectClass	organizationalUnit, top
<input checked="" type="checkbox"/> ou	misusuarios

☒ Select all

☐ Invert selection

☐ Add attribute to object

Clone this object

Remove Selected Attributes

Return to module index

Y esta vez será mis grupos:

https://servidorana:10000/ldap-server/add_form.cgi?base=ou%3Dmisusuarios%2C%3Destaesmiclaseana,dc=local

☆ Create Object

New LDAP object details

New object DN

ou = misgrupos

Parent object DN

dc=estaesmiclaseana,dc=local

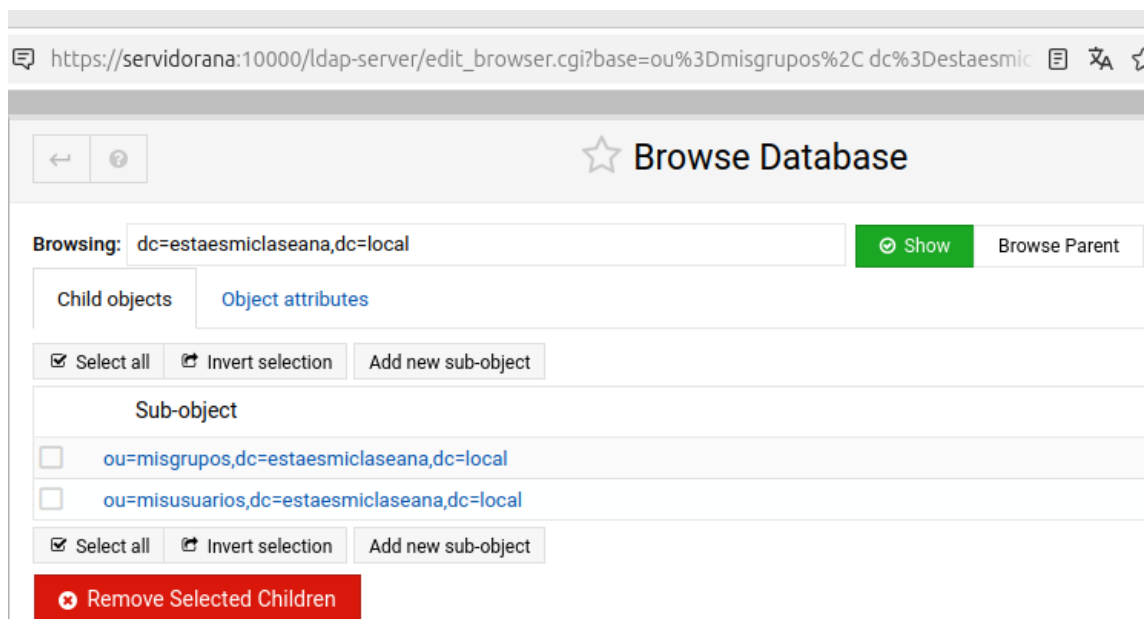
Object classes

organizationalUnit
top

Other attributes

Attribute	Values
ou	misgrupos

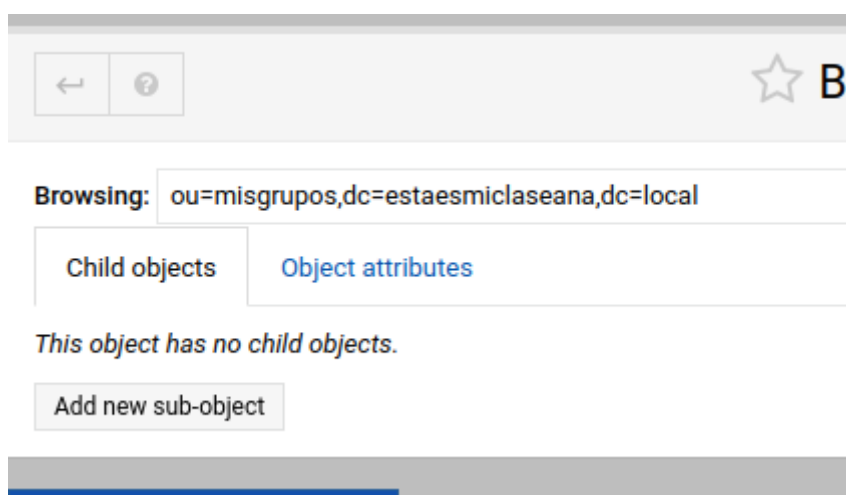
Create



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”:





☆ 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



☆ 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”:

https://servidorana:10000/ldap-server/edit_browser.cgi?base=ou%3Dmisusuarios%2Cdc%3Destaesmiclaseana,dc=local

Browse Database

Browsing: [Show](#) [Browse Parent](#)

[Child objects](#) [Object attributes](#)

This object has no child objects.

[Add new sub-object](#)

[Return to module index](#)

Juan:

https://servidorana:10000/ldap-server/edit_browser.cgi?base=uid%3Djuan%2Cou%3Dmisusuarios%2Cdc%3Destaesmiclaseana,dc=local

Browse Database

Browsing: [Show](#) [Browse Parent](#)

[Child objects](#) [Object attributes](#)

☒ Select all ☐ Invert selection

Attribute	Values	Actions
<input type="checkbox"/> cn	Juan Garcia	Edit
<input type="checkbox"/> gidNumber	2000	Edit
<input type="checkbox"/> givenName	Juan Garcia	Edit
<input type="checkbox"/> homeDirectory	/home/users/juan	Edit
<input type="checkbox"/> loginShell	/bin/bash	Edit
<input type="checkbox"/> objectClass	top, posixAccount, inetOrgPerson, person, shadowAccount	Edit
<input type="checkbox"/> shadowExpire	-1	Edit
<input type="checkbox"/> shadowFlag	7	Edit
<input type="checkbox"/> shadowMin	6	Edit
<input type="checkbox"/> sn	Garcia	Edit
<input type="checkbox"/> uid	juan	Edit
<input type="checkbox"/> uidNumber	3000	Edit
<input type="checkbox"/> userPassword	amazonas	Edit

☒ Select all ☐ Invert selection

[Remove Selected Attributes](#)

Rosa:

The screenshot shows a web-based LDAP browser interface. The address bar indicates the URL: `https://servidorana:10000/ldap-server/edit_browser.cgi?base=uid%3Drosa%2C ou%3Dmisusuarios%2C dc=estaesmiclaseana,dc=local`. The main heading is "Browse Database". Below the heading, the "Browsing:" field contains the LDAP entry path: `uid=rosa, ou=misusuarios, dc=estaesmiclaseana, dc=local`. There are "Show" and "Browse Parent" buttons. Below this, there are tabs for "Child objects" and "Object attributes". Under "Object attributes", there are buttons for "Select all", "Invert selection", "Add attribute to object", and "Clone this object". The main table displays the attributes of the user object:

Attribute	Values	Actions
<input type="checkbox"/> cn	Rosa Lopez	Edit
<input type="checkbox"/> gidNumber	2000	Edit
<input type="checkbox"/> givenName	Rosa Lopez	Edit
<input type="checkbox"/> homeDirectory	/home/users/rosa	Edit
<input type="checkbox"/> loginShell	/bin/bash	Edit
<input type="checkbox"/> objectClass	top, posixAccount, inetOrgPerson, person, shadowAccount	Edit
<input type="checkbox"/> shadowExpire	-1	Edit
<input type="checkbox"/> shadowFlag	7	Edit
<input type="checkbox"/> shadowMin	6	Edit
<input type="checkbox"/> sn	Lopez	Edit
<input type="checkbox"/> uid	rosa	Edit
<input type="checkbox"/> uidNumber	3001	Edit
<input type="checkbox"/> userPassword	amazonas	Edit

At the bottom of the table, there are buttons for "Select all", "Invert selection", "Add attribute to object", and "Clone this object". Below the table, there is a red button labeled "Remove Selected Attributes".

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
<input type="checkbox"/> cn	Luis Gutierrez	Edit
<input type="checkbox"/> gidNumber	2001	Edit
<input type="checkbox"/> givenName	Luis Gutierrez	Edit
<input type="checkbox"/> homeDirectory	/home/luis	Edit
<input type="checkbox"/> loginShell	/bin/bash	Edit
<input type="checkbox"/> objectClass	top, posixAccount, inetOrgPerson, person, shadowAccount	Edit
<input type="checkbox"/> shadowExpire	-1	Edit
<input type="checkbox"/> shadowFlag	7	Edit
<input type="checkbox"/> shadowMin	6	Edit
<input type="checkbox"/> sn	Gutierrez	Edit
<input type="checkbox"/> uid	luis	Edit
<input type="checkbox"/> uidNumber	3002	Edit
<input type="checkbox"/> 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
<input type="checkbox"/> cn	Ana Garcia	Edit
<input type="checkbox"/> gidNumber	2001	Edit
<input type="checkbox"/> givenName	Ana Garcia	Edit
<input type="checkbox"/> homeDirectory	/home/ana	Edit
<input type="checkbox"/> loginShell	/bin/bash	Edit
<input type="checkbox"/> objectClass	top, posixAccount, inetOrgPerson, person, shadowAccount	Edit
<input type="checkbox"/> shadowExpire	-1	Edit
<input type="checkbox"/> shadowFlag	7	Edit
<input type="checkbox"/> shadowMin	6	Edit
<input type="checkbox"/> sn	Garcia	Edit
<input type="checkbox"/> uid	ana	Edit
<input type="checkbox"/> uidNumber	3003	Edit
<input type="checkbox"/> userPassword	amazonas	Edit

Select all

Invert selection

Add attribute to object

Clone this object

Remove Selected Attributes

Antonio:

https://servidorana:10000/ldap-server/edit_browser.cgi?base=uid%3Dantonio%2C ou%3Dmisusuarios

🔍 ⚙️ ☆

📧 👤 📄 ☰

🔍 ⚙️ ☆

Browse Database

Browsing: uid=antonio, 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
<input type="checkbox"/> cn	Antonio Martinez	Edit
<input type="checkbox"/> gidNumber	2001	Edit
<input type="checkbox"/> givenName	Antonio Martinez	Edit
<input type="checkbox"/> homeDirectory	/home/antonio	Edit
<input type="checkbox"/> loginShell	/bin/bash	Edit
<input type="checkbox"/> objectClass	top, posixAccount, inetOrgPerson, person, shadowAccount	Edit
<input type="checkbox"/> shadowExpire	-1	Edit
<input type="checkbox"/> shadowFlag	7	Edit
<input type="checkbox"/> shadowMin	6	Edit
<input type="checkbox"/> sn	Martinez	Edit
<input type="checkbox"/> uid	antonio	Edit
<input type="checkbox"/> uidNumber	3004	Edit
<input type="checkbox"/> userPassword	amazonas	Edit

☒ Select all

☐ Invert selection

☐ Add attribute to object

☐ Clone this object

Patricia:

https://servidorana:10000/ldap-server/edit_browser.cgi?base=uid%3Dpatricia%2C ou%3Dmisusuarios

🔍 ⚙️ ☆

📧 👤 📄 ☰

🔍 ⚙️ ☆

Browse Database

Browsing: uid=patricia, 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
<input type="checkbox"/> cn	Patricia Torres	Edit
<input type="checkbox"/> gidNumber	2001	Edit
<input type="checkbox"/> givenName	Patricia Torres	Edit
<input type="checkbox"/> homeDirectory	/home/patricia	Edit
<input type="checkbox"/> loginShell	/bin/bash	Edit
<input type="checkbox"/> objectClass	top, posixAccount, inetOrgPerson, person, shadowAccount	Edit
<input type="checkbox"/> shadowExpire	-1	Edit
<input type="checkbox"/> shadowFlag	7	Edit
<input type="checkbox"/> shadowMin	6	Edit
<input type="checkbox"/> sn	Torres	Edit
<input type="checkbox"/> uid	patricia	Edit
<input type="checkbox"/> uidNumber	3005	Edit
<input type="checkbox"/> userPassword	amazonas	Edit

☒ Select all

☐ Invert selection

☐ Add attribute to object

☐ Clone this object

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?

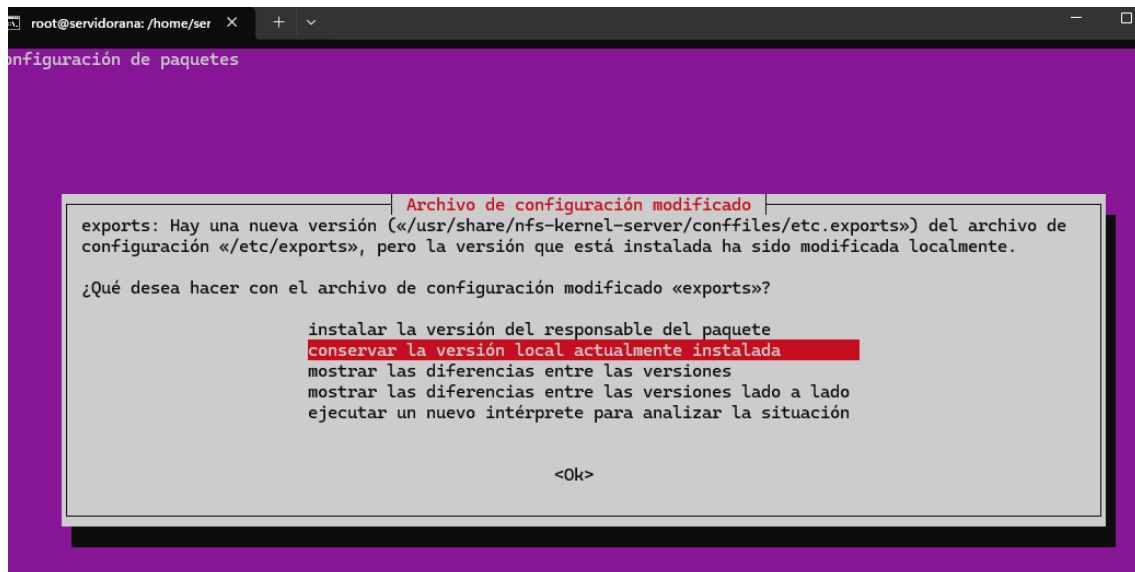
Los perfiles móviles permiten que esos usuarios accedan a datos y configuración desde cualquier dispositivo que se conecte desde la red porque se almacenan en el servidor.

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:

```
root@servidorana:/home/servidorana# apt-get install nfs-kernel-server nfs-common rpcbind
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  keyutils libnfsidmap1
Paquetes sugeridos:
  watchdog
Se instalarán los siguientes paquetes NUEVOS:
  keyutils libnfsidmap1 nfs-common nfs-kernel-server rpcbind
0 actualizados, 5 nuevos se instalarán, 0 para eliminar y 8 no actualizados.
Se necesita descargar 569 kB de archivos.
Se utilizarán 2.022 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://es.archive.ubuntu.com/ubuntu noble/main amd64 libnfsidmap1 amd64 1:2.6-4ubuntu5 [48.2 kB]
```



Y crearemos una carpeta donde se almacenarán:

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

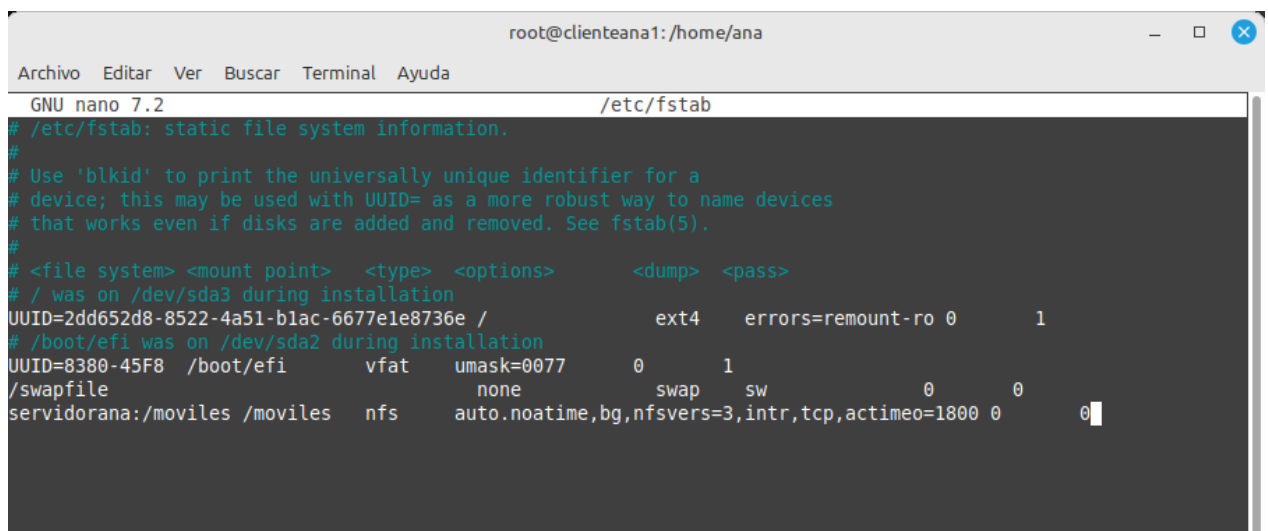
Reiniciaremos:

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

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:





The screenshot shows a terminal window titled 'root@clienteana1: /home/ana'. The window contains the GNU nano 7.2 editor editing the file /etc/fstab. The content of the file is as follows:

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/sda3 during installation
UUID=2dd652d8-8522-4a51-b1ac-6677e1e8736e / ext4 errors=remount-ro 0 1
# /boot/efi was on /dev/sda2 during installation
UUID=8380-45F8 /boot/efi vfat umask=0077 0 1
/swapfile none swap sw 0 0
servidorana:/moviles /moviles nfs auto,noatime,bg,nfsvers=3,intr,tcp,actimeo=1800 0 0
```

Cambiamos a perfumes móviles:

https://servidorana:10000/ldap-server/edit_browser.cgi?base=uid%3Drosa%2Cou%3Dm



☆ Browse Database



Browsing: uid=rosa,ou=misusuarios,dc=estaesmiclaseana,dc=local Show Browse Pare

[Child objects](#) [Object attributes](#)

☒ Select all ☐ Invert selection ☐ Add attribute to object

Attribute	Values
<input type="checkbox"/> cn	Rosa Lopez
<input type="checkbox"/> gidNumber	2000
<input type="checkbox"/> givenName	Rosa Lopez
<input type="checkbox"/> homeDirectory	/moviles/rosa
<input type="checkbox"/> loginShell	/bin/bash
<input type="checkbox"/> objectClass	top, posixAccount, inetOrgPerson, person, shadowAc

https://servidorana:10000/ldap-server/edit_browser.cgi?base=uid%3Djuan%2Cou%3Dm



☆ Browse Database

Browsing: uid=juan,ou=misusuarios,dc=estaesmiclaseana,dc=local Show Browse Pare

[Child objects](#) [Object attributes](#)

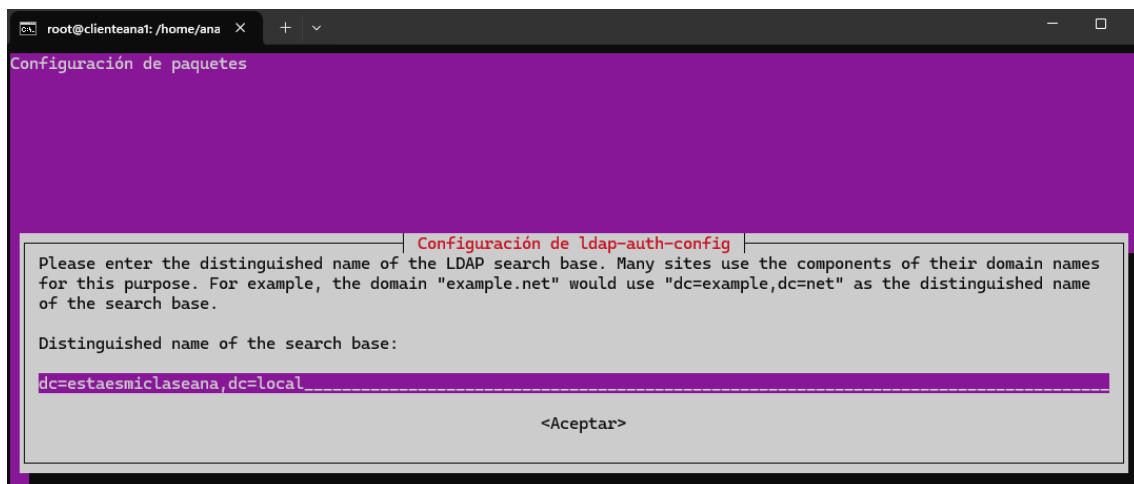
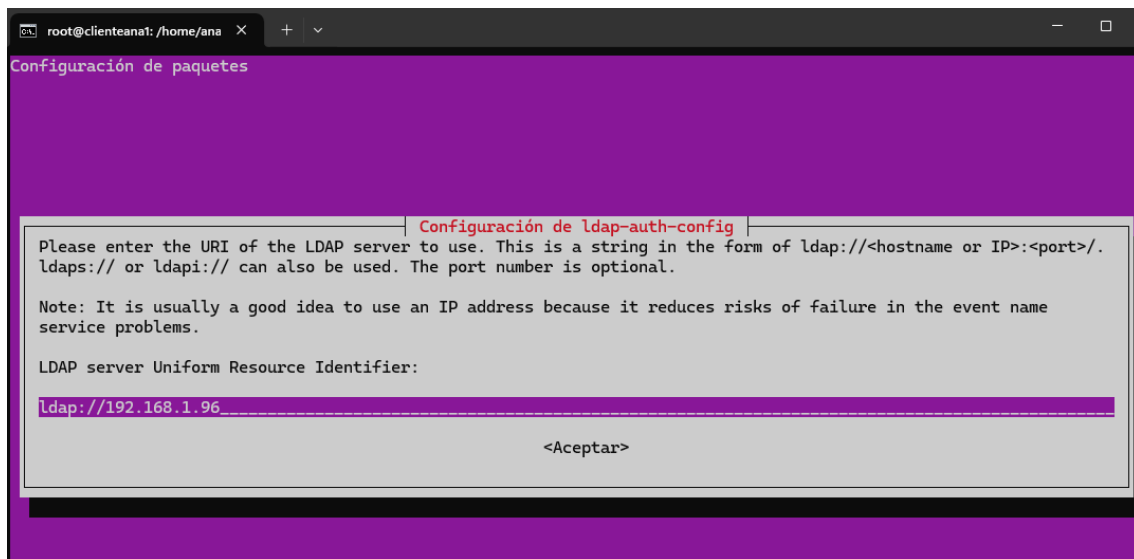
☒ Select all ☐ Invert selection ☐ Add attribute to object

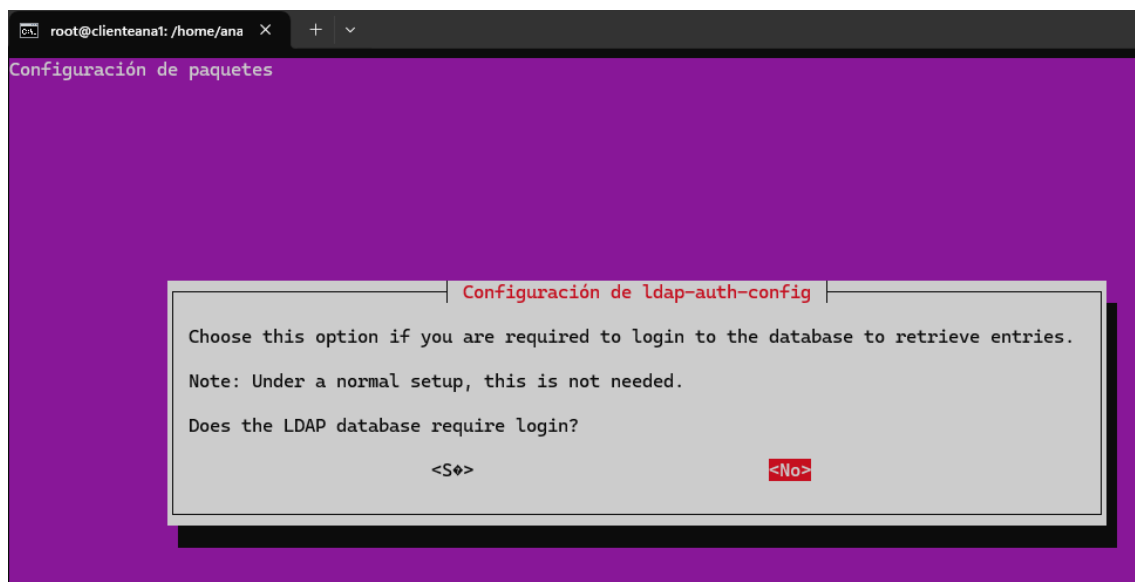
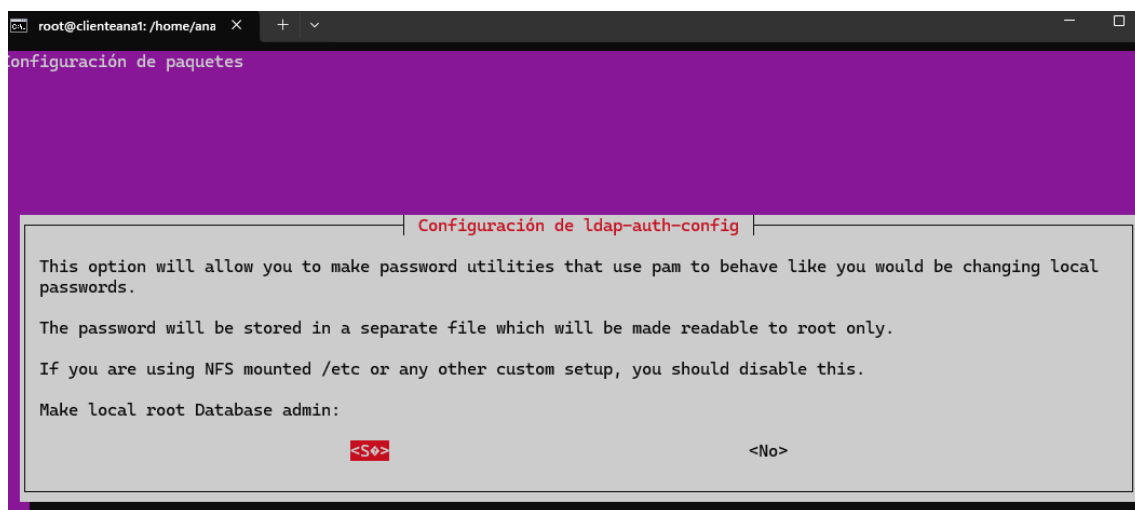
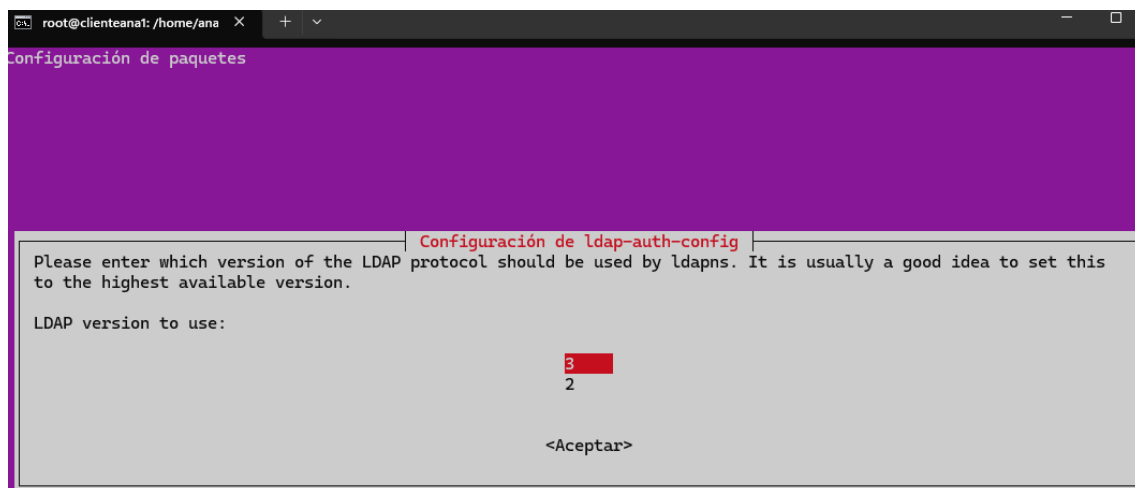
Attribute	Values
<input type="checkbox"/> cn	Juan Garcia
<input type="checkbox"/> gidNumber	2000
<input type="checkbox"/> givenName	Juan Garcia
<input type="checkbox"/> homeDirectory	/moviles/juan
<input type="checkbox"/> loginShell	/bin/bash
<input type="checkbox"/> objectClass	top, posixAccount, inetOrgPerson, person, shadowAc

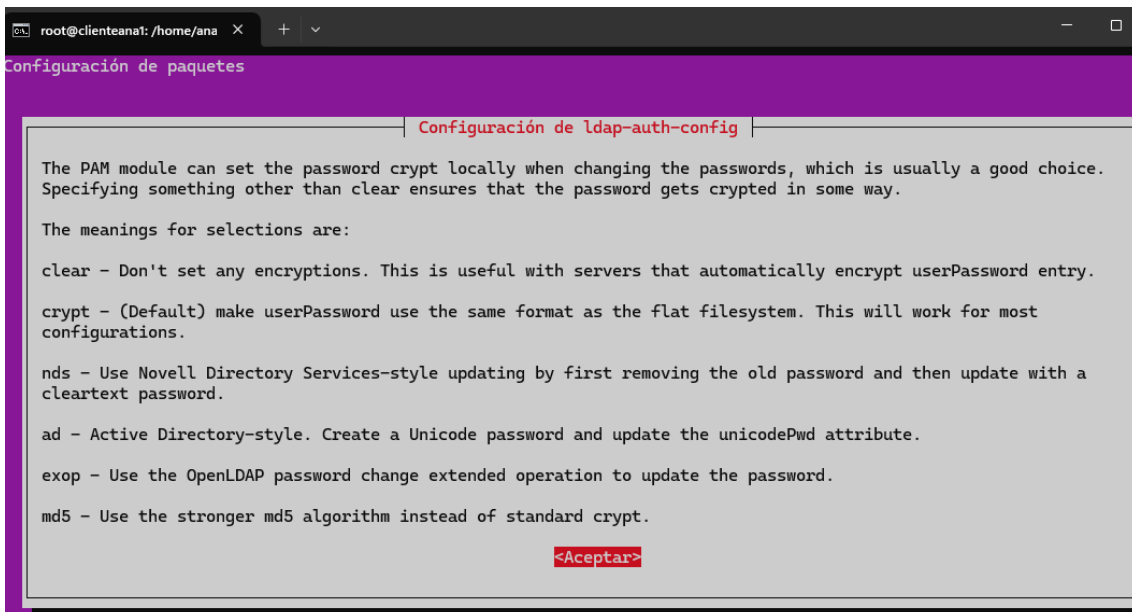
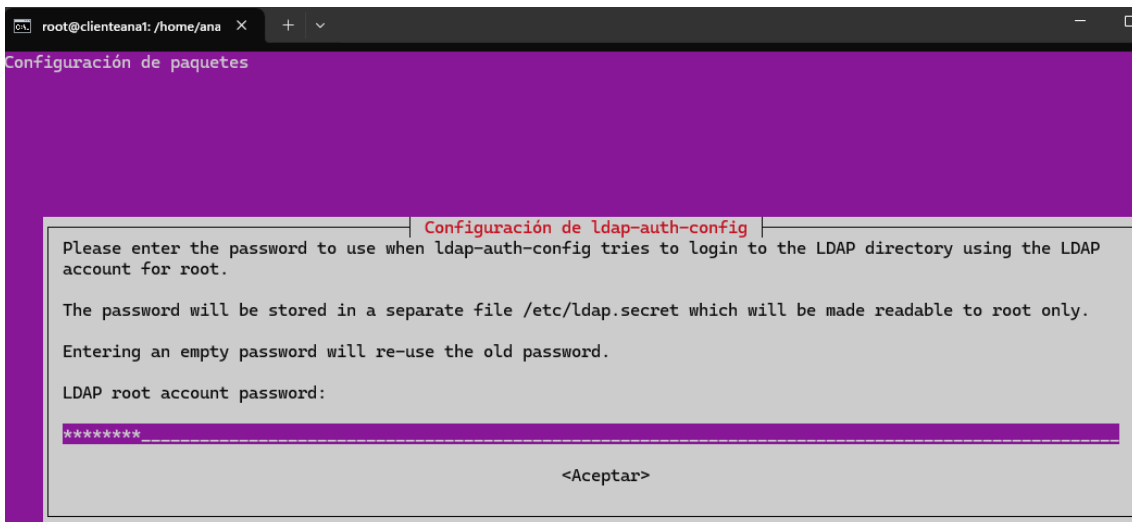
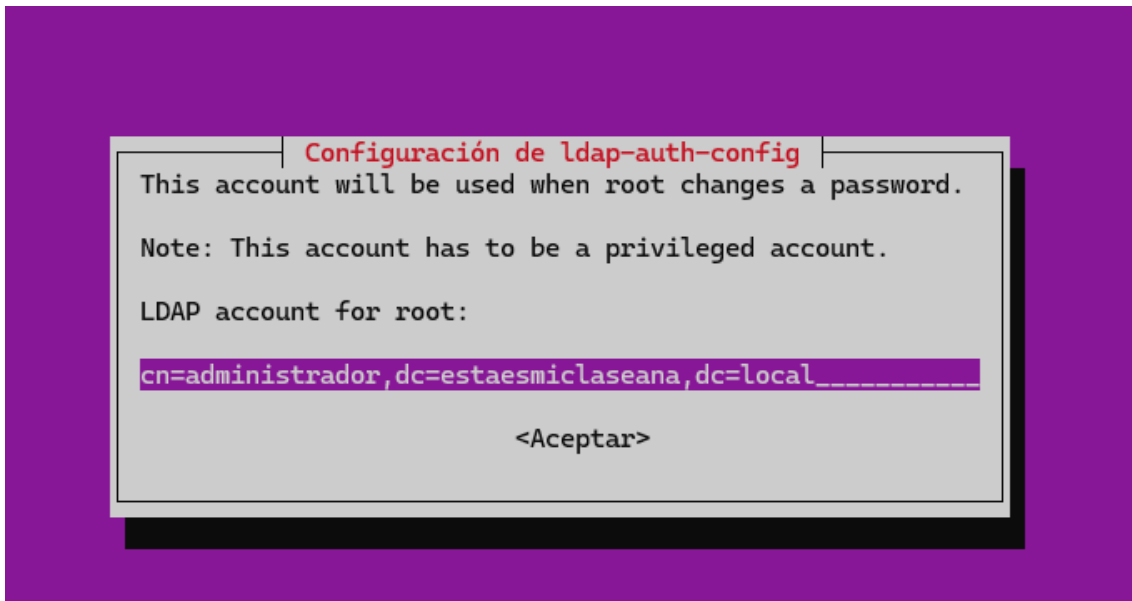
11. Comprobar el acceso de los dos tipos de usuarios (perfiles móviles y locales) al dominio.

Ponemos este comando:

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







Vamos a cambiar este archivo, donde añadiremos ldap:

```
root@clienteana1: /home/ana x + v
GNU nano 7.2 /etc/nsswitch.conf *
# /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 systemd ldap
group:        files systemd ldap
shadow:       files systemd ldap
gshadow:      files systemd

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

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

netgroup:     nis
```

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

```
root@clienteana1: /home/ana x + v
tss:x:104:103:TPM software stack,,,:/var/lib/tpm:/bin/false
rtkit:x:105:104:RealtimeKit,,,:/proc:/usr/sbin/nologin
systemd-coredump:x:989:989:systemd Core Dumper:/:/usr/sbin/nologin
kernoops:x:106:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
uuidd:x:107:107:/:/run/uuidd:/usr/sbin/nologin
cups-pk-helper:x:108:105:user for cups-pk-helper service,,,:/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:111:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
_flatpak:x:110:112:Flatpak system-wide installation helper,,,:/nonexistent:/usr/sbin/nologin
avahi:x:111:113:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
geoclue:x:112:116:/:/var/lib/geoclue:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
nm-openvpn:x:113:117:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
lightdm:x:114:118:Light Display Manager:/var/lib/lightdm:/bin/false
tcpdump:x:115:120:/:/nonexistent:/usr/sbin/nologin
speech-dispatcher:x:116:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
fwupd-refresh:x:988:988:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
cups-browsed:x:117:105:/:/nonexistent:/usr/sbin/nologin
saned:x:118:123:/:/var/lib/saned:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
colord:x:120:124:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
ana:x:1000:1000:ana,,,:/home/ana:/bin/bash
sssd:x:121:126:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
sshd:x:122:65534:/:/run/sshd:/usr/sbin/nologin
nslcd:x:123:127:nslcd name service LDAP connection daemon,,,:/run/nslcd:/usr/sbin/nologin
juan:x:3000:2000:Juan Garcia:/home/users/juan:/bin/bash
rosa:x:3001:2000:Rosa Lopez:/home/users/rosa:/bin/bash
luis:x:3002:2001:Luis Gutierrez:/home/luis:/bin/bash
ana:x:3003:2001:Ana Garcia:/home/ana:/bin/bash
antonio:x:3004:2001:Antonio Martinez:/home/antonio:/bin/bash
patricia:x:3005:2001:Patricia Torres:/home/patricia:/bin/bash
```



```
instcd: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
# 'OBSOLETE_CHECKS_ENAB' option in login.defs. See the pam_unix manpage
#for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password [success=2 default=ignore] pam_unix.so obscure 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"
```

```
root@clienteana1: /home/ana X + v
loginShell: /bin/bash
shadowMin: 6
shadowExpire: -1
shadowFlag: 7

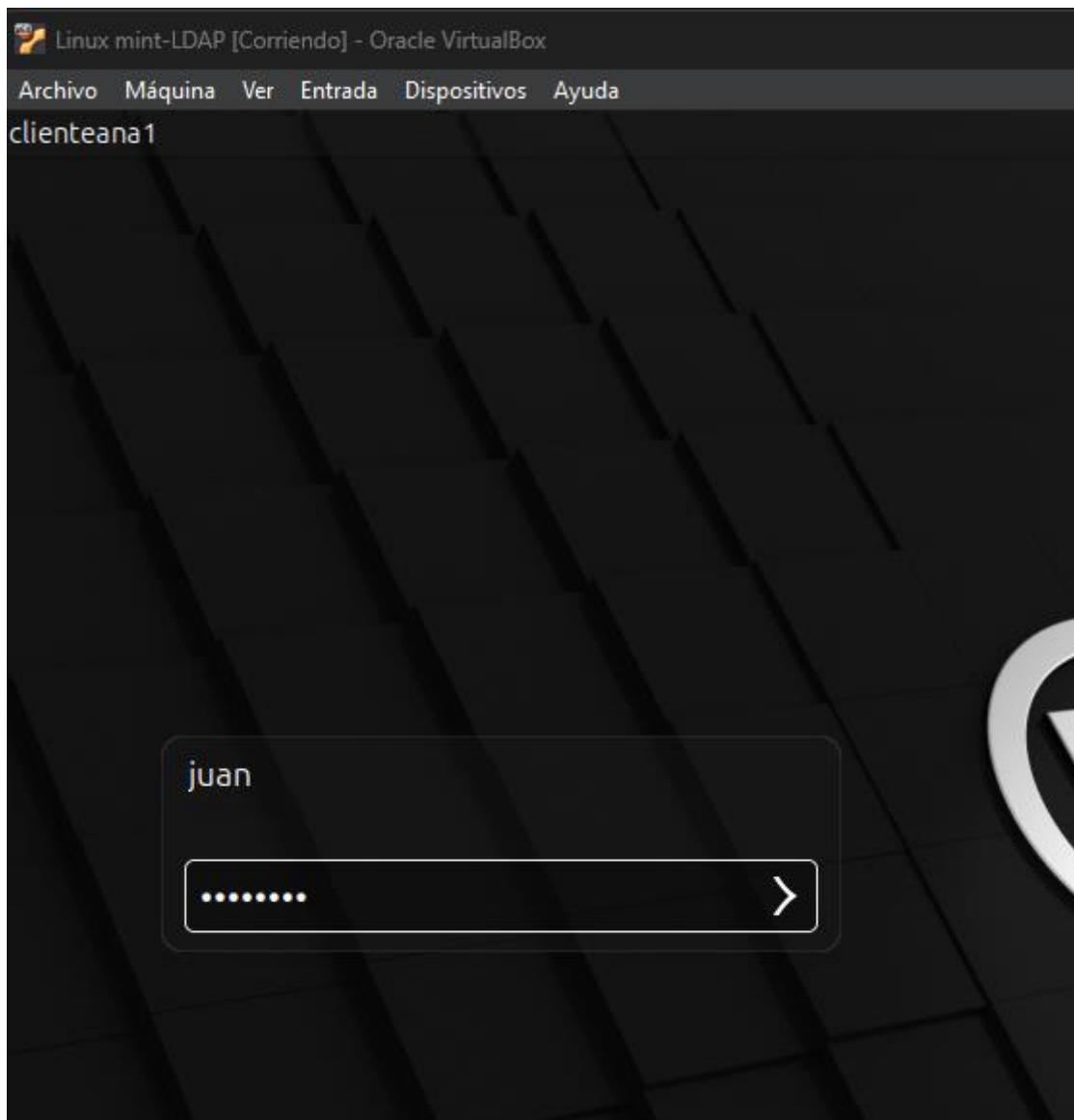
# patricia, misusuarios, estaesmiclaseana.local
dn: uid=patricia,ou=misusuarios,dc=estaesmiclaseana,dc=local
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
objectClass: shadowAccount
cn: Patricia Torres
uid: patricia
uidNumber: 3005
gidNumber: 2001
homeDirectory: /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#
```

Iniciamos sesión con cada uno para que creen los directorios:

```
root@clienteana1:/home# sudo su - rosa
Creando directorio «/moviles/rosa».
rosa@clienteana1:~$ exit
cerrar sesión
root@clienteana1:/home# sudo su - juan
Creando directorio «/moviles/juan».
juan@clienteana1:~$ ^C
juan@clienteana1:~$ exit
cerrar sesión
root@clienteana1:/home# ls -l
total 28
drwxr-x--- 16 ana      ana      4096 dic 16 20:56 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
root@clienteana1:/home#
```

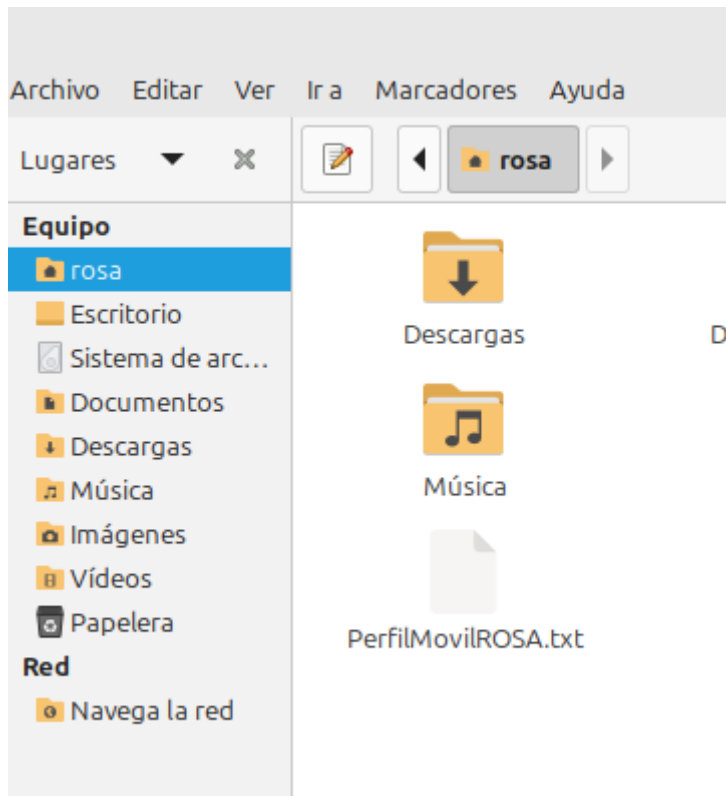


Comprobamos las carpetas del directorio

```
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@clienteanal:~$ 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
rosa@clienteanal:~$
```

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:

```

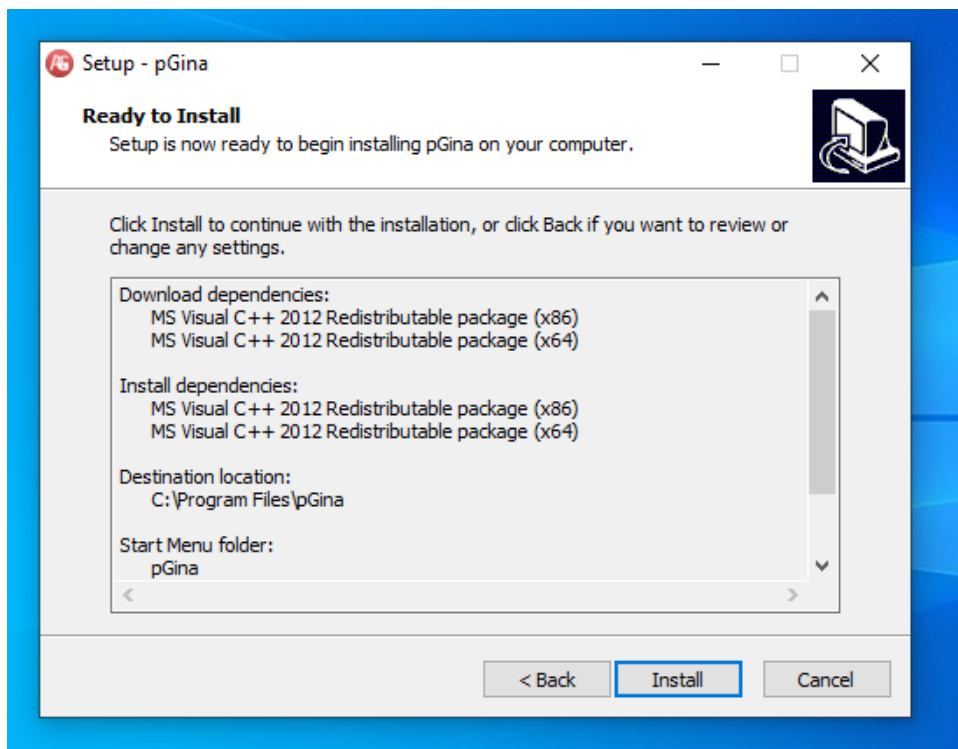
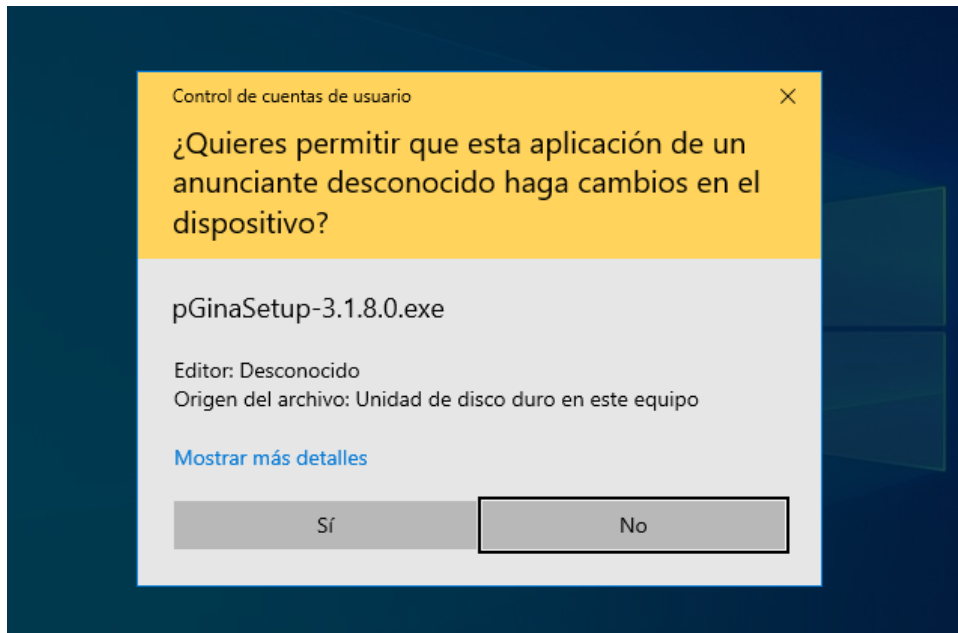
                                     juan@clienteana1: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
juan@clienteana1:~$ ls -l
total 32
drwxr-xr-x 2 juan jefes 4096 dic 16 21:04 Descargas
drwxr-xr-x 2 juan jefes 4096 dic 16 21:04 Documentos
drwxr-xr-x 2 juan jefes 4096 dic 16 21:04 Escritorio
drwxr-xr-x 2 juan jefes 4096 dic 16 21:04 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
root@servidorana:/moviles/juan#
```

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:

pGina Configuration

General Plugin Selection Plugin Order Simulation Credential Provider Options

Tile Image

Tile image: ... Preview: 

MOTD

☒ Enable MOTD

MOTD:
*Message of the Day (MOTD). Displayed below the tile image and above the username/password fields.
Valid substitutions: %m - Machine name, %d - Today's date, %i - IP address, %n - DNS name, %v pGina version*

pGina Service

☒ Show service status in logon UI

Status: Running

Credential Provider/GINA Status

Registered: Yes

Enabled: Yes

Unlock

☐ Use original username to unlock computer (Windows 7 and later).

Logon Progress

Logon Progress Message:
Valid substitution: %u - user name

pGina 3.1.8.0

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

pGina Configuration

General Plugin Selection Plugin Order Simulation Credential Provider Options

Search Directories

Directory

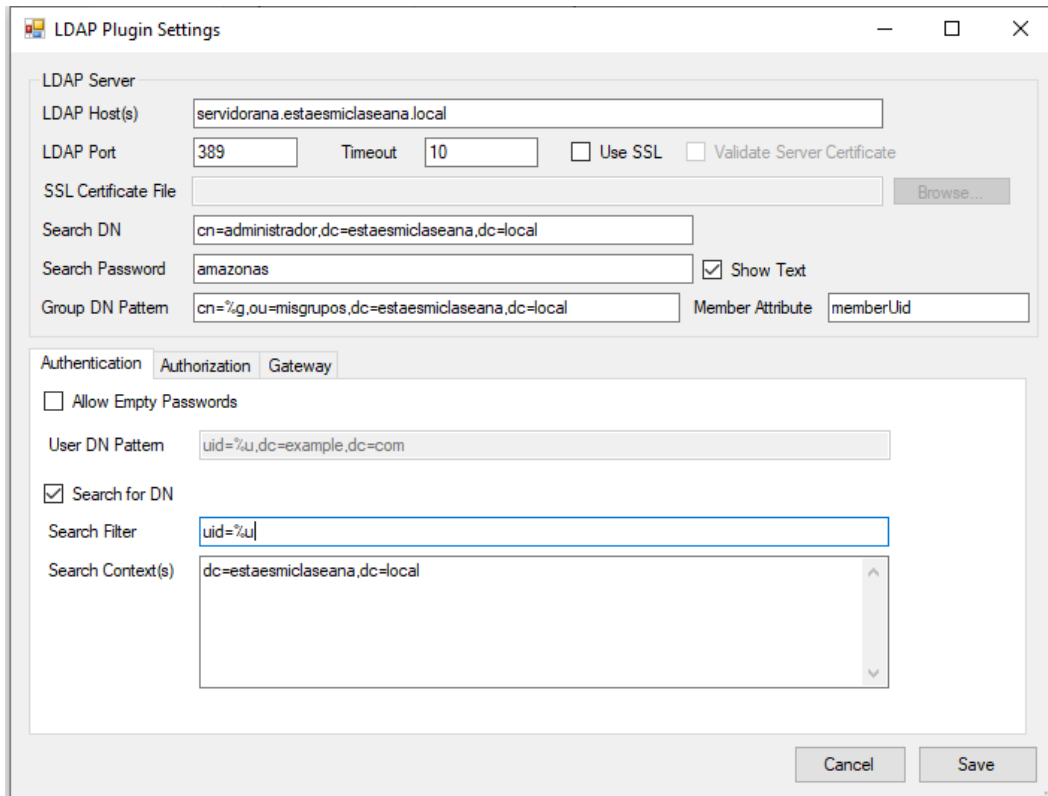
C:\Program Files\pGina\Plugins\Core
C:\Program Files\pGina\Plugins\Contrib

Current Plugins

Plugin Name	Authentication	Authorization	Gateway	Notification	Description
LDAP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Uses a LDAP server as a data source for authentication and/or group information.
Local Machine	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Manages local machine accounts for authenticated users, and authenticates users against the local machine.
MySQL	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Uses a MySQL server as the account database.
MySQL Logger	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Logs various events to a MySQL database.
Simple Demonstration	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A demonstration plugin that allows all usernames that begin with the letter 'd' to log on.
Session Limit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Enforces limits to user's sessions.
Single User Login	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Allow re-direction of all authenticated users to a single set of credentials.
Email Authentication	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A plugin that authenticates against a POP or IMAP server.
RADIUS Plugin	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A RADIUS Authentication and Accounting Plugin.
Modify Username Plugin	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Modify the username at various stages of the login process.

pGina 3.1.8.0

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.



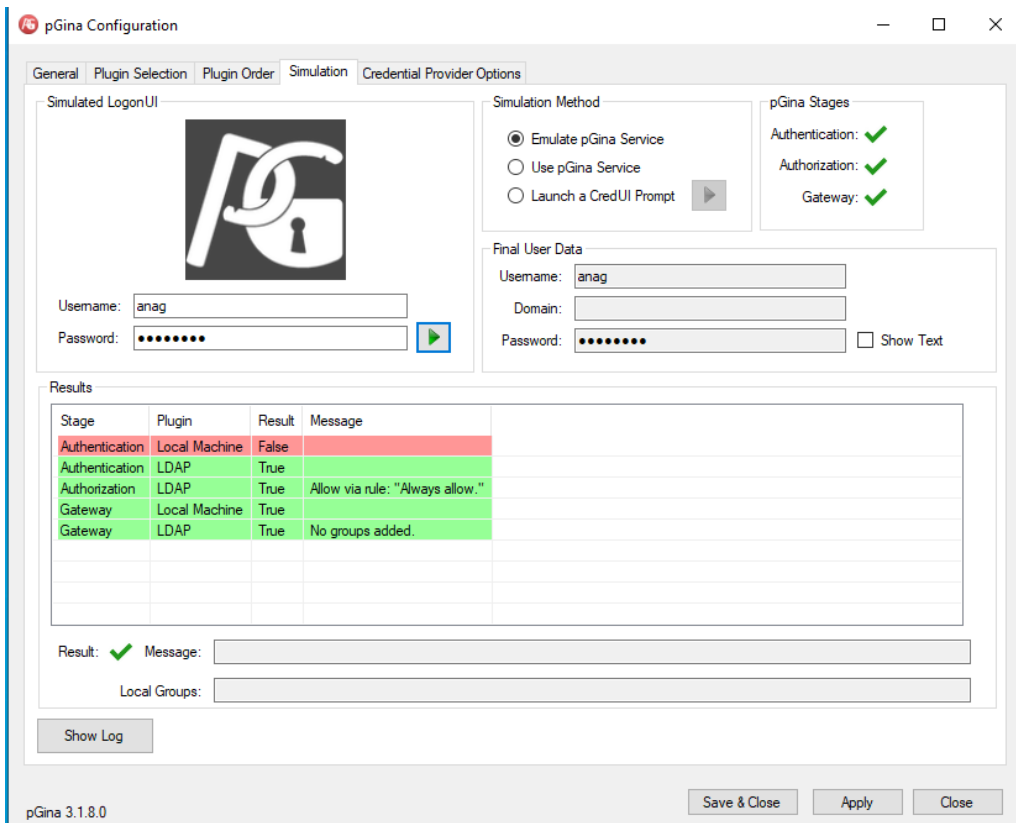
The LDAP Plugin Settings dialog box is shown with the following configuration:

- LDAP Server:**
 - LDAP Host(s): `servidorana.estaesmiclaseana.local`
 - LDAP Port: `389`
 - Timeout: `10`
 - ☐ Use SSL
 - ☐ Validate Server Certificate
 - SSL Certificate File: (empty) [Browse...]
- Search:**
 - Search DN: `cn=administrador,dc=estaesmiclaseana,dc=local`
 - Search Password: `amazonas` [Show Text]
 - Group DN Pattern: `cn=%g,ou=misgrupos,dc=estaesmiclaseana,dc=local`
 - Member Attribute: `memberUid`
- Authentication:**
 - ☐ Allow Empty Passwords
 - User DN Pattern: `uid=%u,dc=example,dc=com`
 - ☒ Search for DN
 - Search Filter: `uid=%u`
 - Search Context(s): `dc=estaesmiclaseana,dc=local`

Buttons: Cancel, Save

Comprobaremos en la simulación con el usuario anag.

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



The pGina Configuration dialog box is shown with the following configuration:

- General:**
 - Simulated LogonUI: [Image]
 - Username: `anag`
 - Password: [Masked]
- Simulation Method:**
 - ☒ Emulate pGina Service
 - ☐ Use pGina Service
 - ☐ Launch a CredUI Prompt
- pGina Stages:**
 - Authentication: ☒
 - Authorization: ☒
 - Gateway: ☒
- Final User Data:**
 - Username: `anag`
 - Domain: (empty)
 - Password: [Masked] [Show Text]
- Results:**

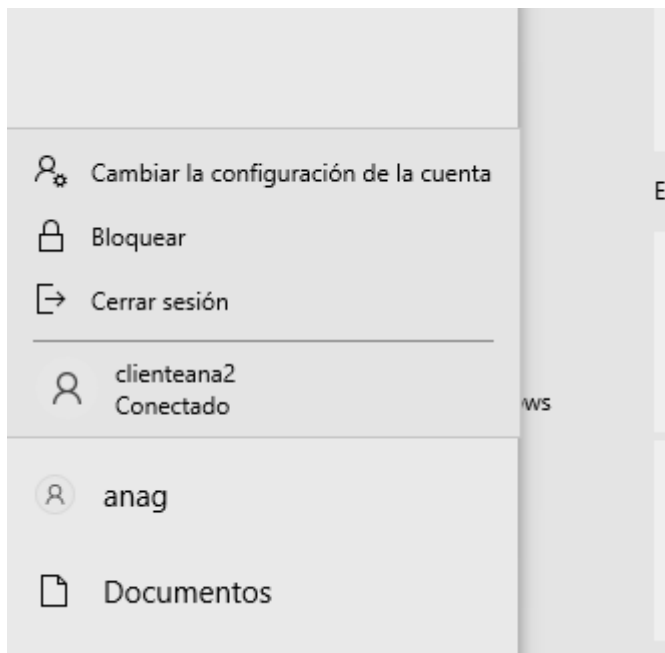
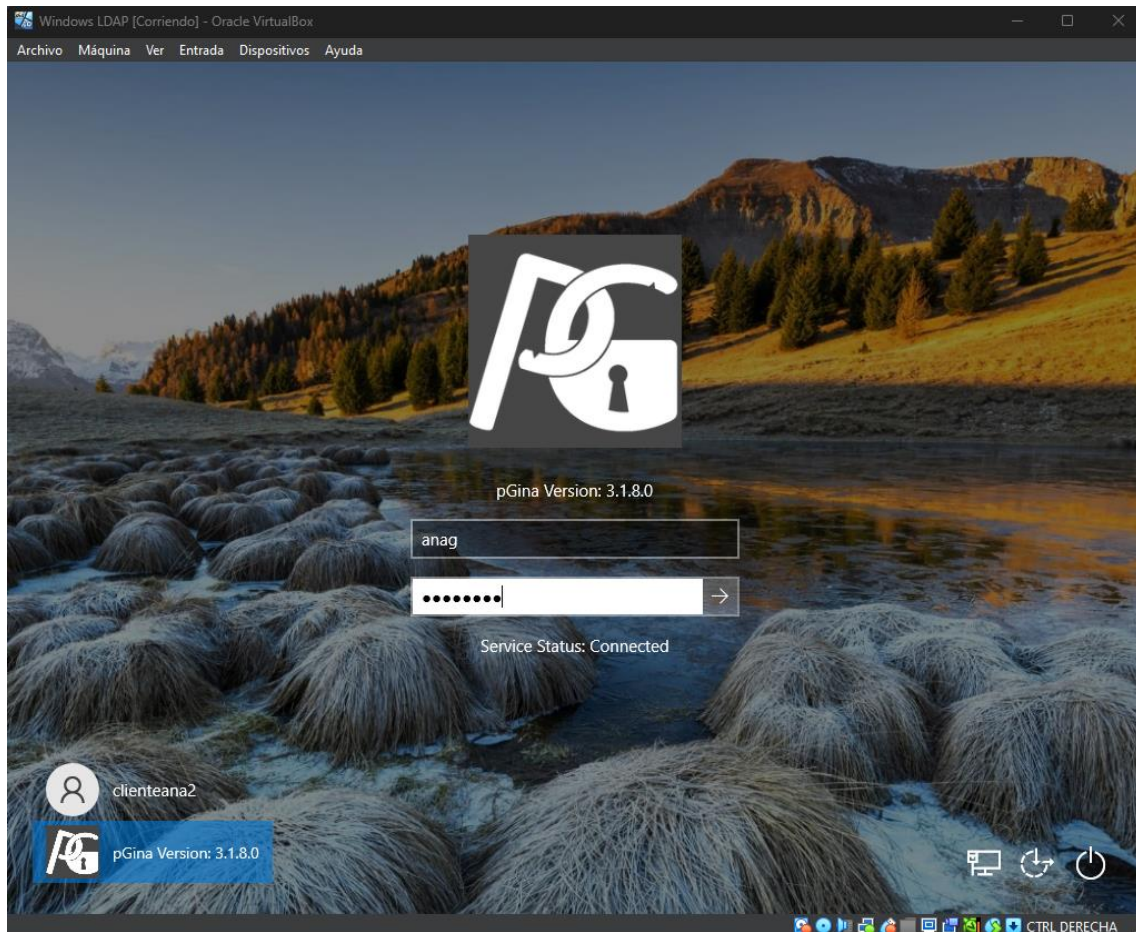
Stage	Plugin	Result	Message
Authentication	Local Machine	False	
Authentication	LDAP	True	
Authorization	LDAP	True	Allow via rule: "Always allow."
Gateway	Local Machine	True	
Gateway	LDAP	True	No groups added.

Result: ☒ Message: [Empty]
Local Groups: [Empty]

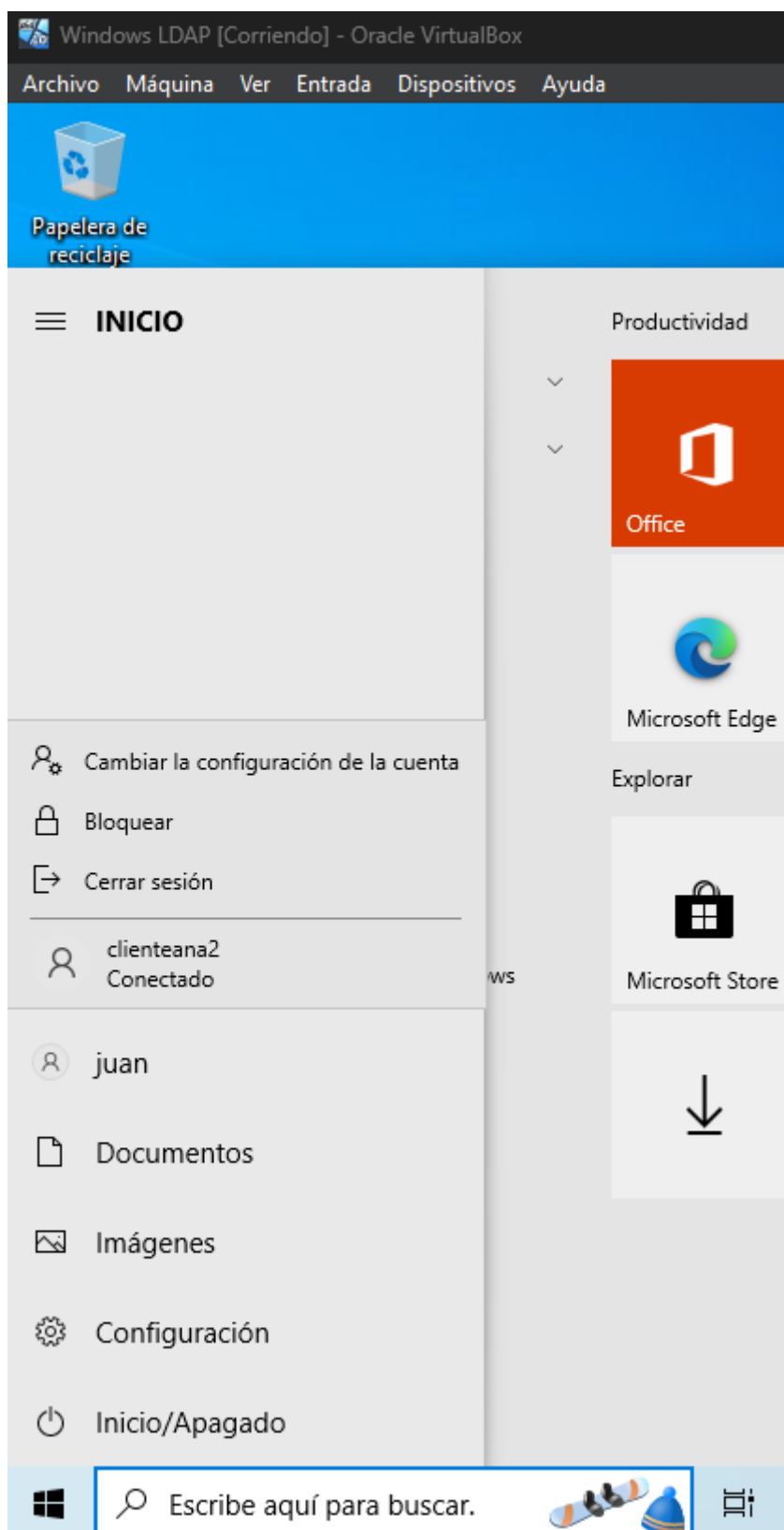
Buttons: Show Log, Save & Close, Apply, Close

pGina 3.1.8.0

Ahora sí comprobaremos accediendo



Y también con juan



Incidencias

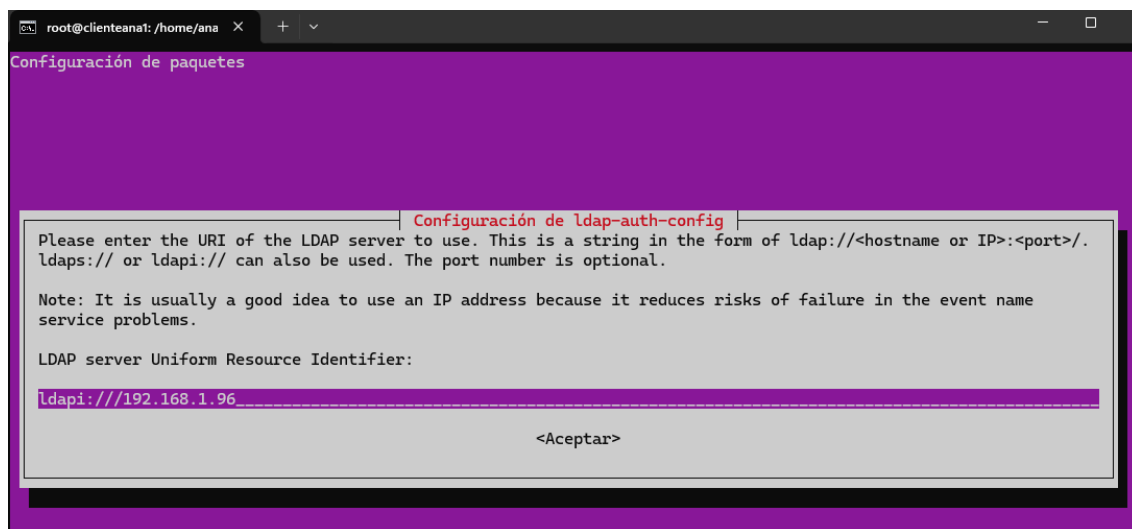
Tuve este fallo:

```
# 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@clienteanal:/home/ana# sudo su - luis
su: user luis does not exist or the user entry does not contain all the required fields
root@clienteanal:/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.