CICLO FORMATIVO DE GRADO SUPERIOR - TÉCNICO EN ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN REDES

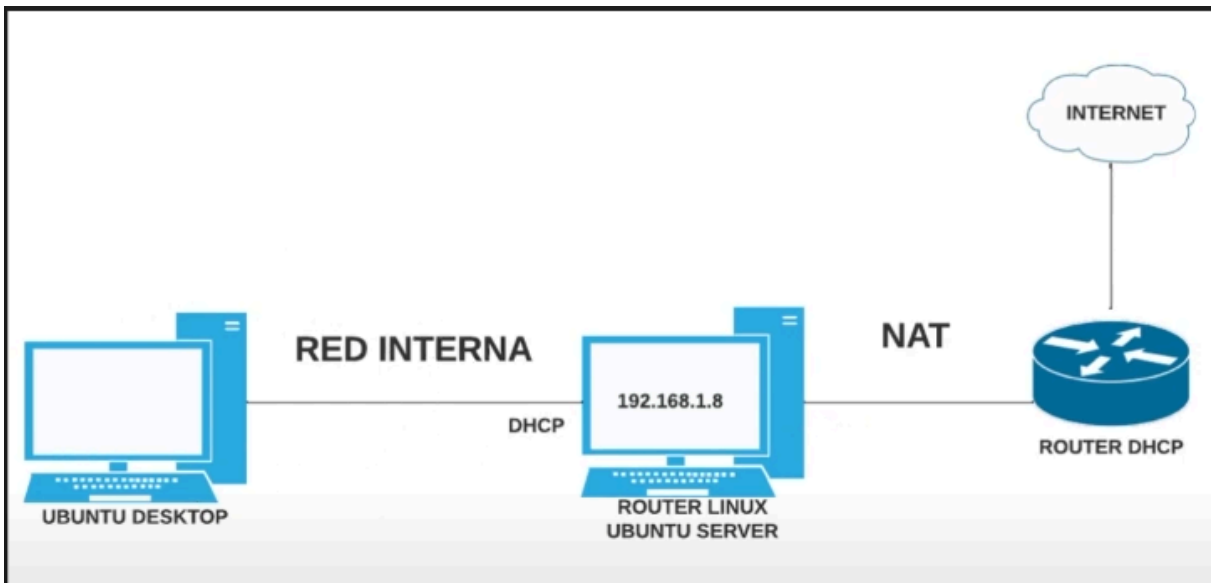
ADMINISTRACIÓN DE SISTEMAS OPERATIVOS

OpenLDAP

Nombre y apellidos:
-Wuke Zhang

Preparación del entorno.

Para esta práctica, vamos a necesitar usar **DOS** máquinas virtuales nuevas de Ubuntu 22.04 con la siguiente configuración de red:



1. Creación y configuración del servidor como router dhcp.

   Activamos dos interfaces de red en el Servidor, una en NAT y otra en red interna. Identificamos los nombres de cada conector con la instrucción “ip ad”:

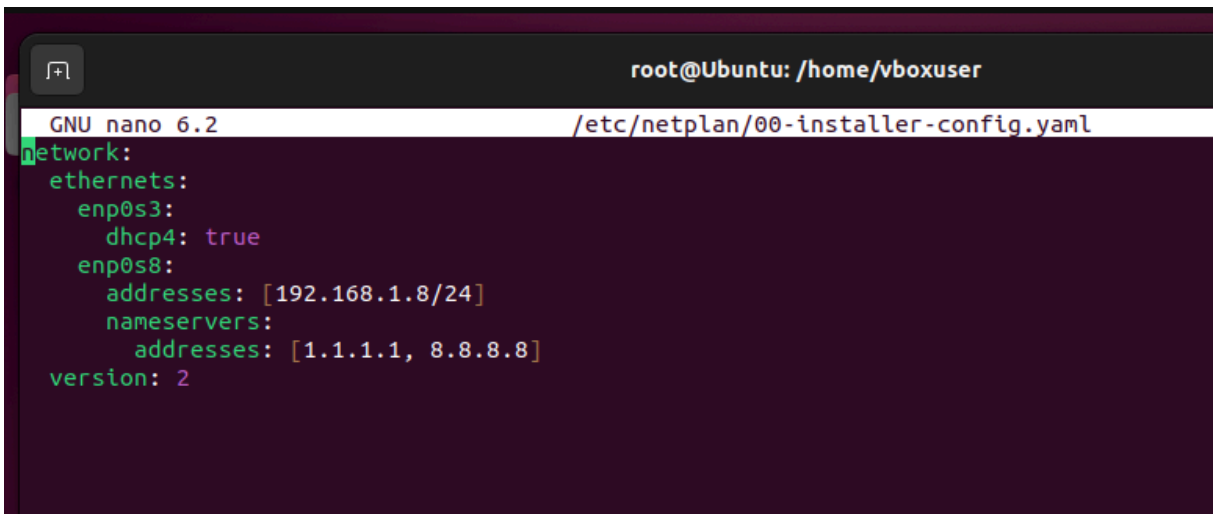
```
azael@azael-VirtualBox:~/Desktop$ ip ad
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:36:77:68 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 85706sec preferred_lft 85706sec
    inet6 fe80::a00:27ff:fe36:7768/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ed:6a:92 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.8/24 brd 192.168.1.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feed:6a92/64 scope link
       valid_lft forever preferred_lft forever
```

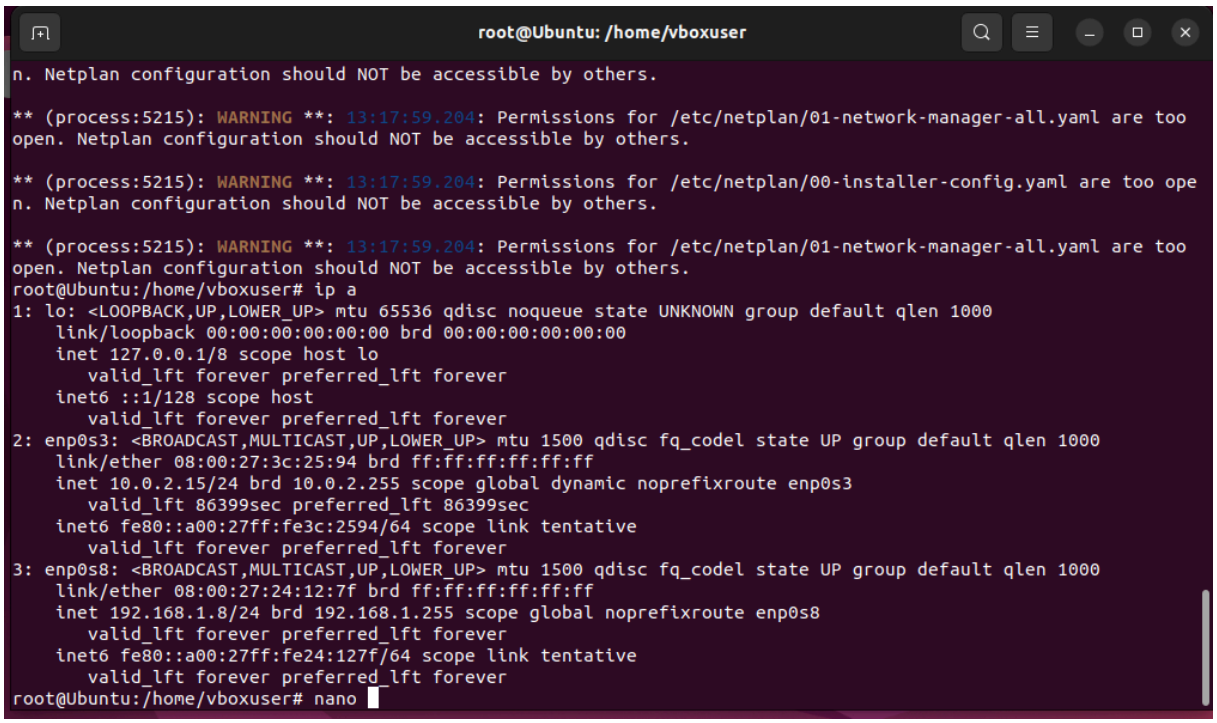
   a. Configuramos NetWorkManager de la siguiente forma:

```
nano /etc/netplan/00-installer-config.yaml
```

```
# Let NetworkManager manage all devices on this system
network:
  ethernets:
    enp0s3:
      dhcp4: true
    enp0s8:
      addresses: [192.168.1.8/24]
      nameservers:
        addresses: [1.1.1.1, 8.8.8.8]
  version: 2
```

```
netplan apply
```





b. Habilitamos la retransmisión de paquetes:

```
nano /etc/sysctl.conf
```

```
# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1
net.ipv4.ip_forward=1
```

```
root@azael-VirtualBox:/home/azael/Desktop# sysctl -p /etc/sysctl.conf
net.ipv4.ip_forward = 1
```

```
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
```

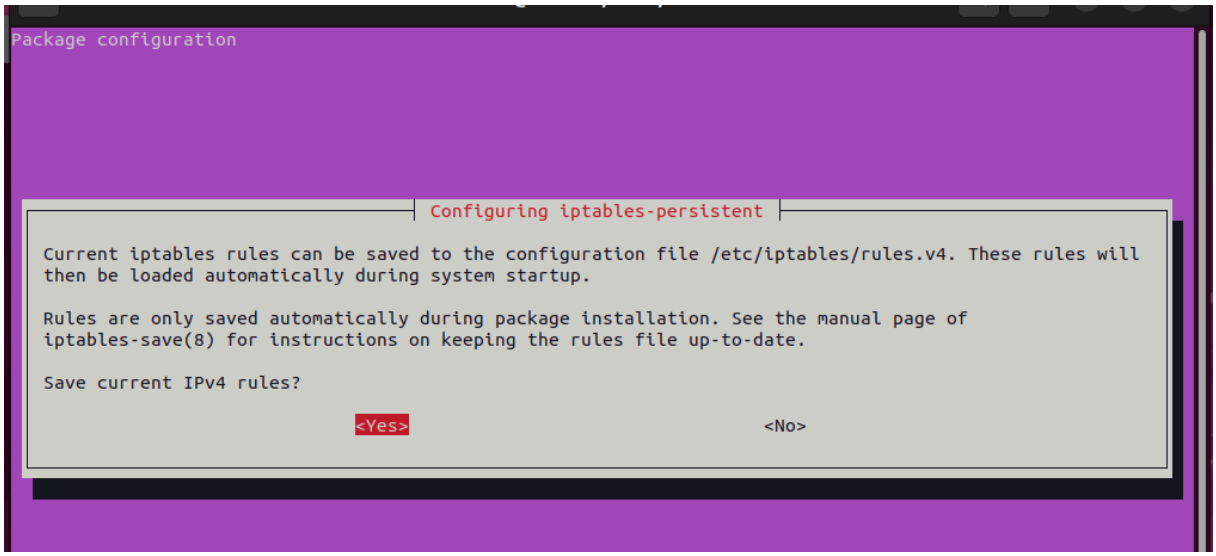
c. Actualizamos el cortafuegos iptables con la siguiente configuración:

```
sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

```
root@Ubuntu:/home/vboxuser# sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
root@Ubuntu:/home/vboxuser#
```

d. Añadimos persistencia al cortafuegos con el paquete “iptables-persistent”:

```
sudo apt-get install iptables-persistent
```




```
iptables-save > /etc/iptables/rules.v4
```

e. Instalamos “isc-dhcp-server” y lo configuramos de la siguiente forma:

```
sudo apt-get install isc-dhcp-server
```

- Mantenemos los tiempos por defecto.

```
default-lease-time 600;
max-lease-time 7200;
```

- Creamos el grupo asir con la siguiente configuración dhcp.

```
group asir{

subnet 192.168.1.0 netmask 255.255.255.0 {
        range 192.168.1.100 192.168.1.150;
        option domain-name-servers 192.168.1.8;
        option domain-name "asir.local";
        option subnet-mask 255.255.255.0;
        option routers 192.168.1.8;
        option broadcast-address 192.168.1.255;
        }
}
```

- Revisamos que la configuracion este correcta.

```
azael@ldapserver:~/Desktop$ sudo dhcpd -t -cf /etc/dhcp/dhcpd.conf
Internet Systems Consortium DHCP Server 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /etc/dhcp/dhcpd.conf
Database file: /var/lib/dhcp/dhcpd.leases
PID file: /var/run/dhcpd.pid
```

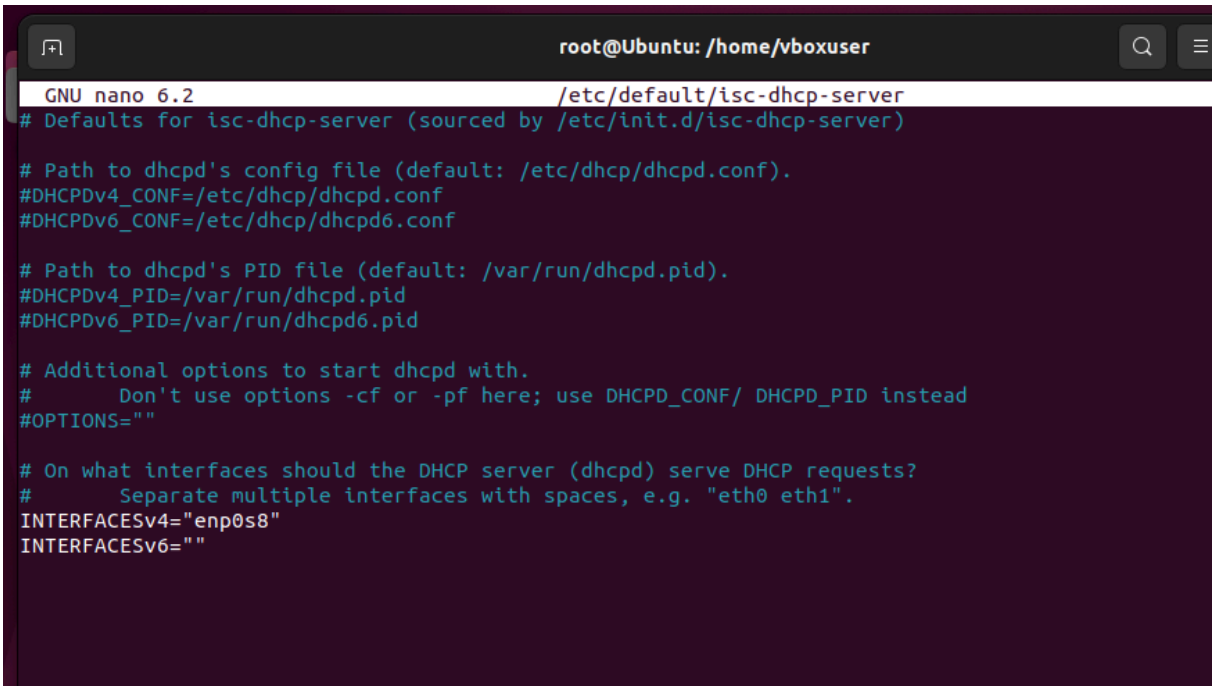
```
root@Ubuntu:/home/vboxuser# sudo dhcpd -t -cf /etc/dhcp/dhcpd.conf
Internet Systems Consortium DHCP Server 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /etc/dhcp/dhcpd.conf
Database file: /var/lib/dhcp/dhcpd.leases
PID file: /var/run/dhcpd.pid
```

- Habilitamos DHCP en el adaptador de red interna.

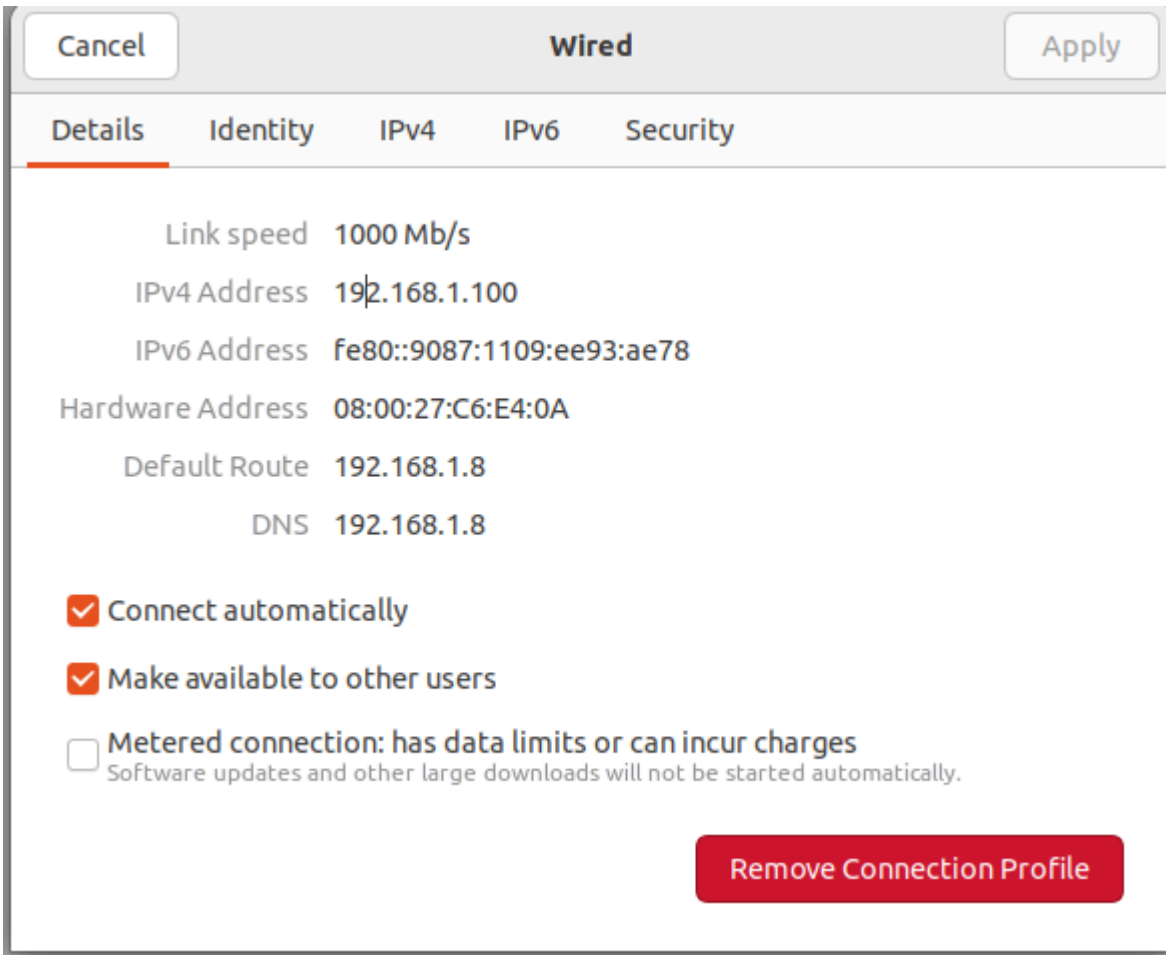
```
sudo nano /etc/default/isc-dhcp-server
```

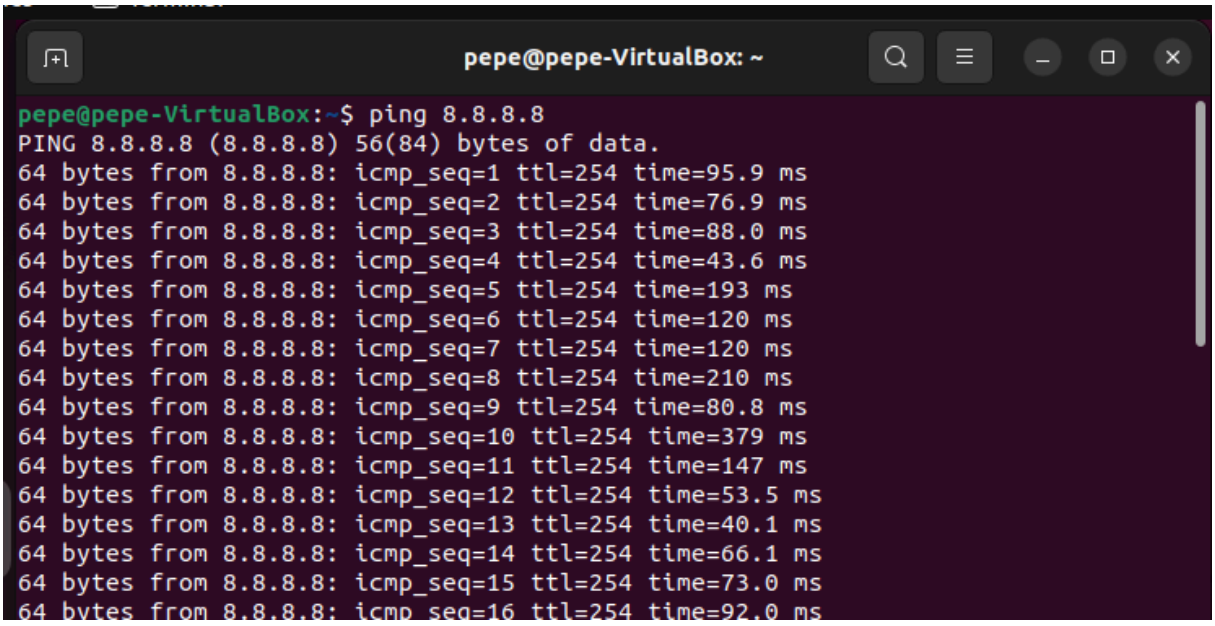
```
#       Separate multip
INTERFACESv4="enp0s8"
INTERFACESv6=""
```

- Reiniciamos el servicio.



f. Crear una maquina virtual Ubuntu 22.04 denominada Cliente y conectarla a la red interna usando DHCP.

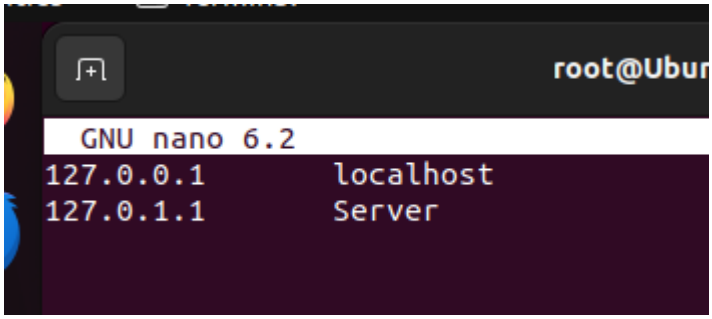




2. Configurar el servidor DNS en el Ubuntu Server.
    a. Modificar el archivo host.

```
sudo nano /etc/hosts
```

```
127.0.0.1       localhost
127.0.1.1       Server

# 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
```



b. Instalar y habilitar bind9

```
sudo apt-get install bind9
```

```
$ sudo ufw allow bind9
```

```
root@Ubuntu:/home/vboxuser# ufw allow bind9
Rule added
Rule added (v6)
root@Ubuntu:/home/vboxuser#
```

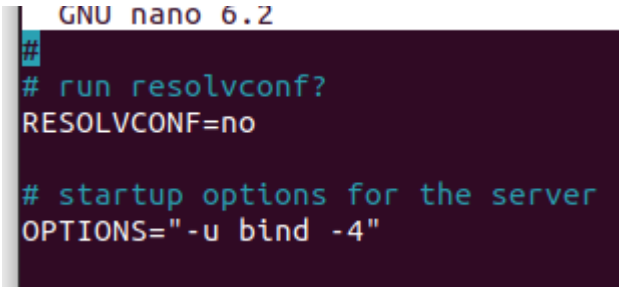
c. Configurar la red que va a usar el DNS:

```
sudo nano /etc/bind/named.conf.options
```

```
 GNU nano 6.2                                  /etc/bind/named.conf.options *
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.

        listen-on { any; }; //Escucha desde todos los lados.
        allow-query { localhost; 192.168.1.0/24; }; //Redes admitidas
        forwarders {
                8.8.8.8;
        };
        // forwarders {
        //      0.0.0.0;
        // };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation no; //No hay dns secundario para validar.

        //listen-on-v6 { any; }; //Comentar para evitar usar ipv6
};
```

```
 GNU nano 6.2                                                named.conf.options
        // 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.

        listen-on { any; };
        allow-query { localhost; 192.168.1.0/24; };
        forwarders {
                8.8.8.8;
        };
        // forwarders {
        //      0.0.0.0;
        // };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation no;

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

```
sudo nano /etc/default/named
```


GNU nano 6.2
#
# run resolvconf?
RESOLVCONF=no
# startup options for the server
OPTIONS="-u bind -4"

d. Configurar el siguiente dominio.

```
sudo nano /etc/bind/named.conf.local
```

```
 GNU nano 6.2                                          /etc/bind/named.c
//
// 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 "asir.local" IN {
        type master;
        file "/etc/bind/zonas/db.asir.local";
};

zone "1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/zonas/db.1.168.192";
};
```

```
sudo mkdir /etc/bind/zonas
```

```
sudo cp /etc/bind/db.local /etc/bind/zonas/db.asir.local
```

```
 GNU nano 6.2                                                  /etc/bind/
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     asir.local. root.asir.local. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
                IN      NS      server.asir.local.
server          IN      A       192.168.1.8
PC-Linux        IN      A       192.168.1.105
servidor        IN      CNAME   server
```

```
sudo cp /etc/bind/zonas/db.asir.local /etc/bind/zonas/db.1.168.192
```

```
root@Ubuntu:/etc/bind# cat zonas/*
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     asir.local. root.asir.local. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
        IN      NS      server.asir.local.
8       IN      PTR     server.asir.local.
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     asir.local. root.asir.local. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
        IN      NS      server.asir.local.
server  IN      A       192.168.1.8
PC-Linux        IN      A       192.168.1.105
servidor        IN      CNAME server
root@Ubuntu:/etc/bind# nano /etc/dhcp/dhc
```

Comprobamos que la configuración esta correcta.

```
sudo named-checkconf /etc/bind/named.conf.local
```

```
$ sudo named-checkzone asir.local /etc/bind/zonas/db.asir.local
```

```
root@Ubuntu:/home/vboxuser# named-checkzone asir.local /etc/bind/zonas/db.asir.l
ocal
zone asir.local/IN: loaded serial 2
OK
```

```
sudo named-checkzone 1.168.192.in-addr.arpa /etc/bind/zonas/db.1.168.192
```

```
root@Ubuntu:/home/vboxuser# named-checkzone 1.168.192.in.addr.arpa /etc/bind/zon
as/db.1.168.192
zone 1.168.192.in.addr.arpa/IN: loaded serial 2
OK
root@Ubuntu:/home/vboxuser#
```

Iniciamos el servicio:

```
azael@Server:~/Desktop$ sudo service bind9 restart
azael@Server:~/Desktop$ sudo service bind9 status
```

```
pepe@PC-Linux:~/Desktop$ ping PC-Linux
PING PC-Linux (192.168.1.105) 56(84) bytes of data.
64 bytes from PC-Linux (192.168.1.105): icmp_seq=1 ttl=64 time=0.008 ms
64 bytes from PC-Linux (192.168.1.105): icmp_seq=2 ttl=64 time=0.022 ms
64 bytes from PC-Linux (192.168.1.105): icmp_seq=3 ttl=64 time=0.025 ms
64 bytes from PC-Linux (192.168.1.105): icmp_seq=4 ttl=64 time=0.025 ms
64 bytes from PC-Linux (192.168.1.105): icmp_seq=5 ttl=64 time=0.023 ms
64 bytes from PC-Linux (192.168.1.105): icmp_seq=6 ttl=64 time=0.022 ms
64 bytes from PC-Linux (192.168.1.105): icmp_seq=7 ttl=64 time=0.024 ms
^C
--- PC-Linux ping statistics ---
10 packets transmitted, 7 received, 30% packet loss, time 9087ms
rtt min/avg/max/mdev = 0.008/0.021/0.025/0.005 ms
```

3. Configuración de OpenLDAP
    a. Cambiamos el nombre del host

```
sudo hostnamectl set-hostname ldapserver.asir.local
```

```
$ sudo nano /etc/hosts
```

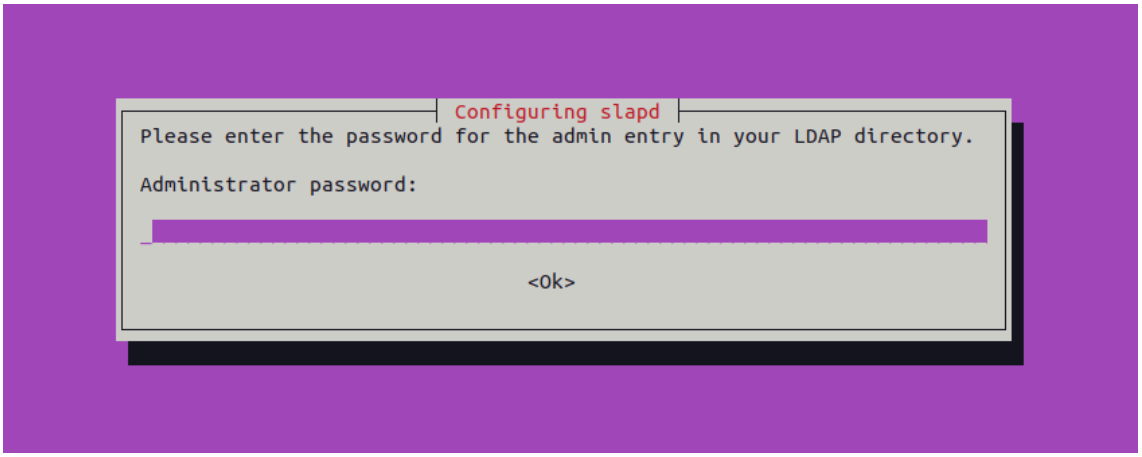
```
127.0.0.1       localhost
127.0.1.1       ldapserver.asir.local
192.168.1.8     ldapserver.asir.local
```

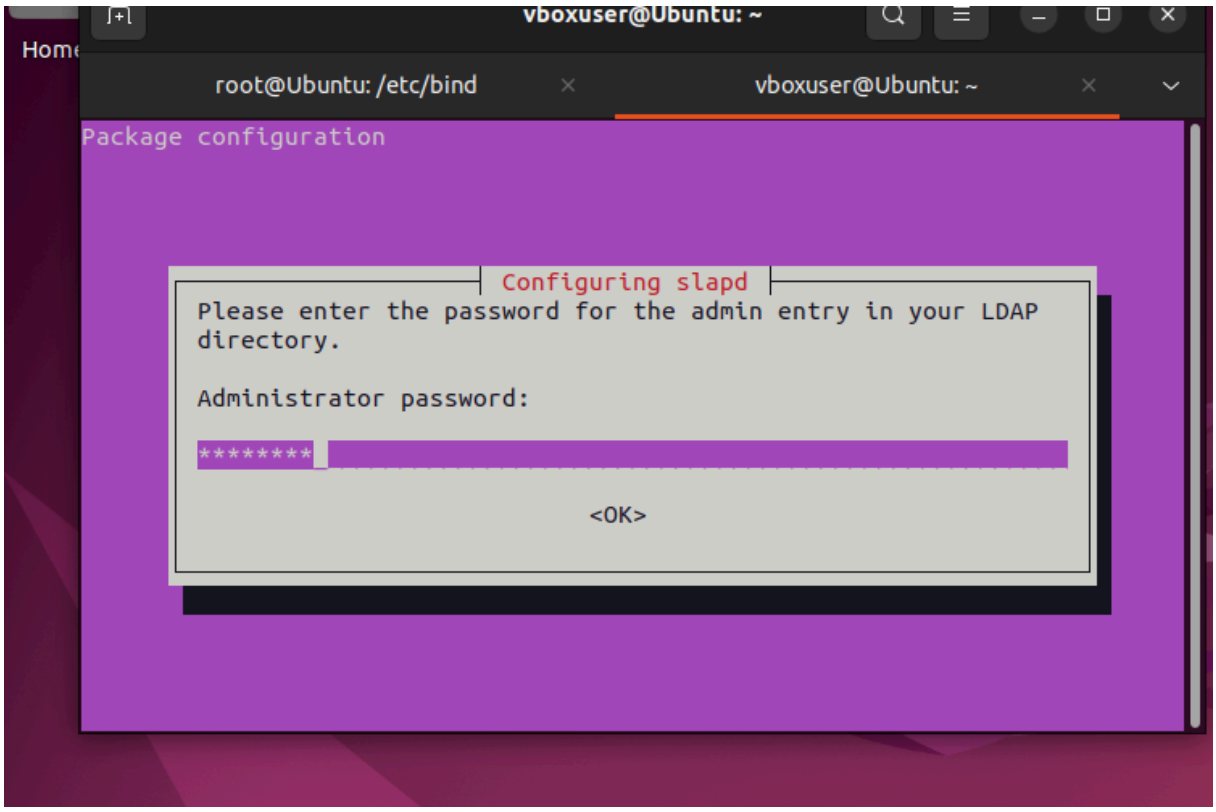
    b. Actualizar el Ubuntu Cliente en **segundo plano** mientras configuramos el resto.

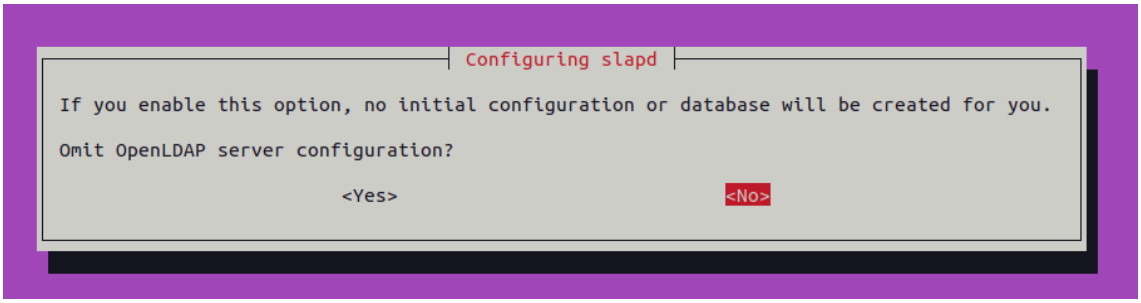
```
$ sudo apt update -y && sudo apt upgrade -y && sudo apt dist-upgrade -y
```

    c. Instalamos y configuramos de base OpenLDAP

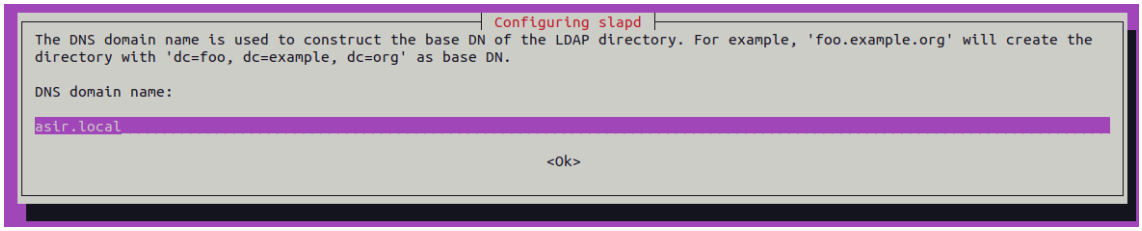
```
sudo apt install slapd ldap-utils -y
```

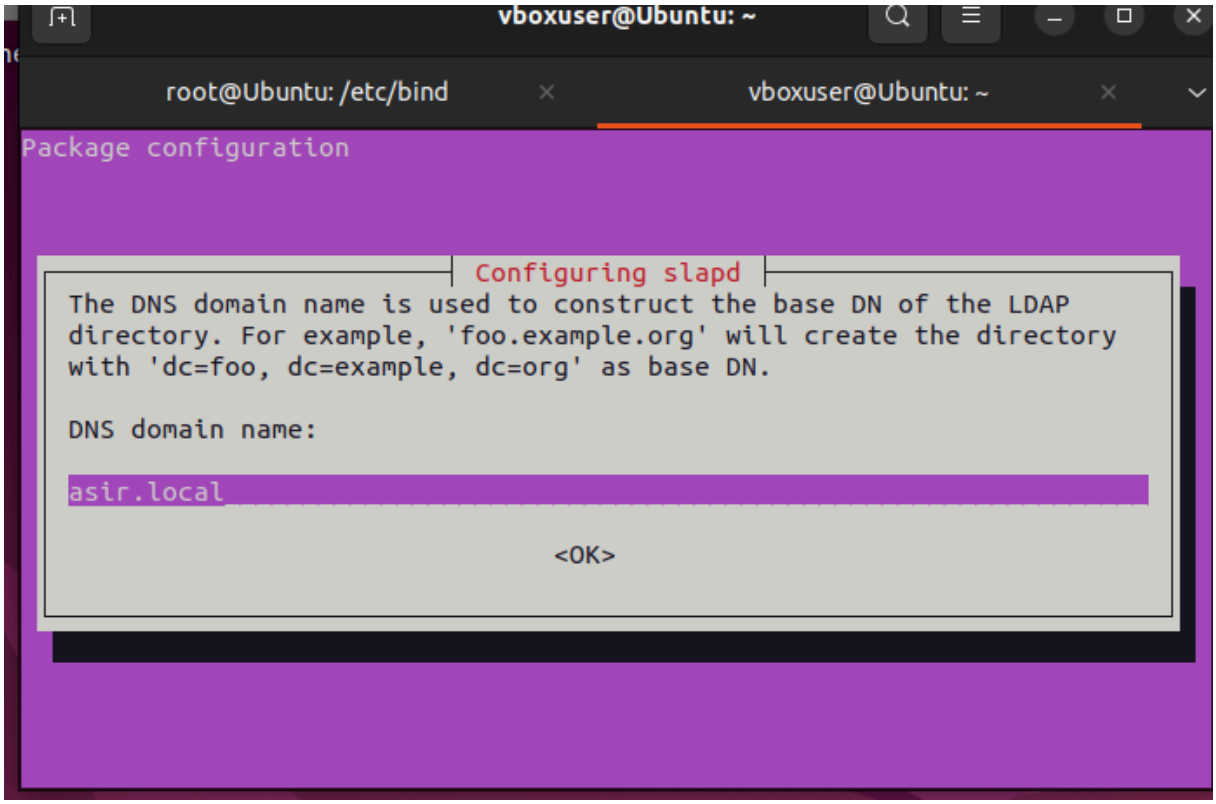


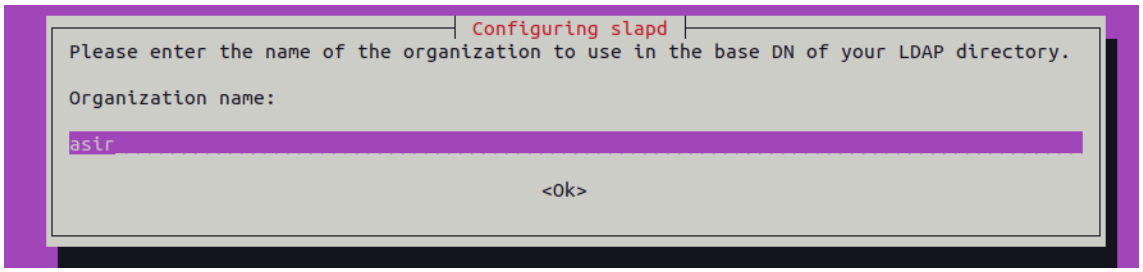

vboxuser@Ubuntu: ~
root@Ubuntu: /etc/bind
vboxuser@Ubuntu: ~
Package configuration
Configuring slapd
Please enter the password for the admin entry in your LDAP directory.
Administrator password:
****
<OK>

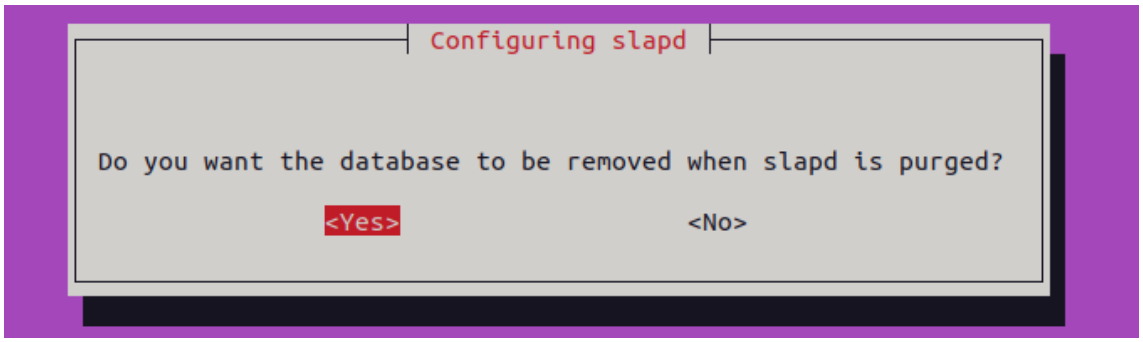

Configuring slapd
If you enable this option, no initial configuration or database will be created for you.
Omit OpenLDAP server configuration?
<Yes>
<No>

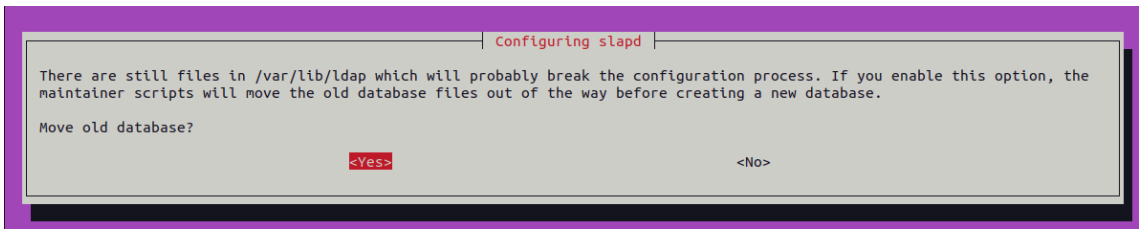
Usamos el DNS que hemos creado.












```
vboxuser@Ubuntu:~$ sudo dpkg-reconfigure slapd
  Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.5.18+dfsg-0ubuntu0.22
.04.2... done.
  Moving old database directory to /var/backups:
  - directory unknown... done.
  Creating initial configuration... done.
  Creating LDAP directory... done.
vboxuser@Ubuntu:~$
```

d. Por último, ejecutamos el comando slapcat para ver el contenido del Directorio base

```
azael@Server:~/Desktop$ sudo slapcat
dn: dc=asir,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: asir
dc: asir
structuralObjectClass: organization
entryUUID: 4a63af20-661a-103e-8d2e-c16ebd46e661
creatorsName: cn=admin,dc=asir,dc=local
createTimestamp: 202402222220553Z
entryCSN: 20240222220553.429013Z#000000#000#000000
modifiersName: cn=admin,dc=asir,dc=local
modifyTimestamp: 202402222220553Z
```

```
vboxuser@Ubuntu:~$ sudo slapcat
dn: dc=asir,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: asir
dc: asir
structuralObjectClass: organization
entryUUID: 2e2ed426-6d10-103f-8712-f9b9af987dcc
creatorsName: cn=admin,dc=asir,dc=local
createTimestamp: 202501221326062
entryCSN: 20250122132606.949608Z#000000#000#000000
modifiersName: cn=admin,dc=asir,dc=local
modifyTimestamp: 202501221326062
```

4. Añadir nodos.

   Para gestionar la información del directorio, tenemos que redactar un archivo de configuración con extensión .ldif.

a. Creación de una unidad organizacional.

```
sudo nano ou.ldif
```

```
dn: ou=informatica,dc=asir,dc=local
objectClass: top
objectClass: organizationalUnit
ou: informatica
```

```
sudo ldapadd -x -D cn=admin,dc=asir,dc=local -W -f ou.ldif
```

```
vboxuser@Ubuntu:~$ sudo ldapadd -x -D "cn=admin,dc=asir,dc=local" -W -f ou.l
dif
Enter LDAP Password:
adding new entry "ou=informatica,dc=asir,dc=local"
```

b. Creación de un grupo de usuarios.

```
cp ou.ldif grp.ldif
```

```
nano grp.ldif
```

```
  GNU nano 6.2                                grp.ldif
dn: cn=informatica,ou=informatica,dc=asir,dc=local
objectClass: top
objectClass: posixGroup
gidNumber: 10000
cn: informatica
```

```
root@ldapserver:/home/azael/Desktop# ldapadd -x -D cn=admin,dc=asir,dc=local -W -f grp.ldif
Enter LDAP Password:
adding new entry "cn=informatica,ou=informatica,dc=asir,dc=local"
```

```
vboxuser@Ubuntu:~$ sudo ldapadd -x -D "cn=admin,dc=asir,dc=local" -W -f ou.l
dif
Enter LDAP Password:
adding new entry "ou=informatica,dc=asir,dc=local"
ldap_add: Already exists (68)
```

c. Creación de un usuario.

```
cp grp.ldif usr.ldif
```

```
nano usr.ldif
```

```
  GNU nano 6.2
dn: uid=alumno,ou=informatica,dc=asir,dc=local
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: alumno
uid: alumno
ou: informatica
uidNumber: 2000
gidNumber: 10000
homeDirectory: /home/alumno
loginShell: /bin/bash
userPassword: temppassword
sn: student
mail: alumno@asir.local
givenName: alumno
```

```
root@ldapserver:/home/azael/Desktop# ldapadd -x -D cn=admin,dc=asir,dc=local -W -f usr.ldif
Enter LDAP Password:
adding new entry "uid=alumno,ou=informatica,dc=asir,dc=local"
```

```
vboxuser@Ubuntu:~$ sudo ldapadd -x -D "cn=admin,dc=asir,dc=local" -W -f usr.
ldif
Enter LDAP Password:
adding new entry "uid=alumno,ou=informatica,dc=asir,dc=local"

vboxuser@Ubuntu:~$
```

```
root@ldapserver:/home/azael/Desktop# cp usr.ldif newusr.ldif
root@ldapserver:/home/azael/Desktop#
```

```
dn: uid=invitado,ou=informatica,dc=asir,dc=local
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: invitado
uid: invitado
ou: informatica
uidNumber: 2000
gidNumber: 10000
homeDirectory: /home/alumno
loginShell: /bin/bash
userPassword: temppassword
sn: guest
mail: invitado@asir.local
givenName: invitado
```

```
ldapadd -x -D cn=admin,dc=asir,dc=local -W -f newusr.ldif
```

d. Búsqueda dentro del directorio

```
root@ldapserver:/home/azael/Desktop# ldapsearch -xLLL -b "dc=asir,dc=local" uid=alumno sn givenName cn
dn: uid=alumno,ou=informatica,dc=asir,dc=local
cn: alumno
sn: student
givenName: alumno
```

```
root@ldapserver:/home/azael/Desktop# ldapsearch -xLLL -b "dc=asir,dc=local" uid=* sn givenName cn
dn: uid=alumno,ou=informatica,dc=asir,dc=local
cn: alumno
sn: student
givenName: alumno

dn: uid=invitado,ou=informatica,dc=asir,dc=local
cn: invitado
sn: guest
givenName: invitado
```

```
vboxuser@Ubuntu:~$ ldapsearch -xLLL -b "dc=asir,dc=local" uid=* sn givenName
 cn
dn: uid=alumno,ou=informatica,dc=asir,dc=local
cn: alumno
sn: student
givenName: alumno
```

e. Modificación de atributos de una entrada.

```
 GNU nano 6.2
dn: uid=invitado,ou=informatica,dc=asir,dc=local
changetype: modify
replace: mail
mail:
```

```
ldapmodify -x -D cn=admin,dc=asir,dc=local -W -f modif.ldif
```

```
root@ldapserver:/home/vboxuser# ldapadd -x -D "cn=admin,dc=asir,dc=local" -W -f
newusr.ldif
Enter LDAP Password:
adding new entry "uid=alumno,ou=informatica,dc=asir,dc=local"
```

f. Eliminación de entradas del directorio.

```
root@ldapserver:/home/azael/Desktop# ldapdelete -x -W -D 'cn=admin,dc=asir,dc=local' "uid=invitado,ou=informatica,
dc=asir,dc=local"
```

Ya está eliminado, porque no aparece con slapcat y ya estaba creado.

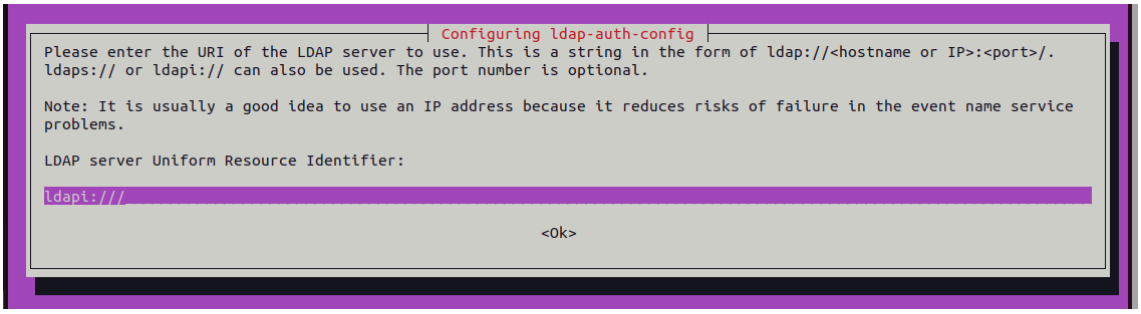
5. Cliente OpenLDAP

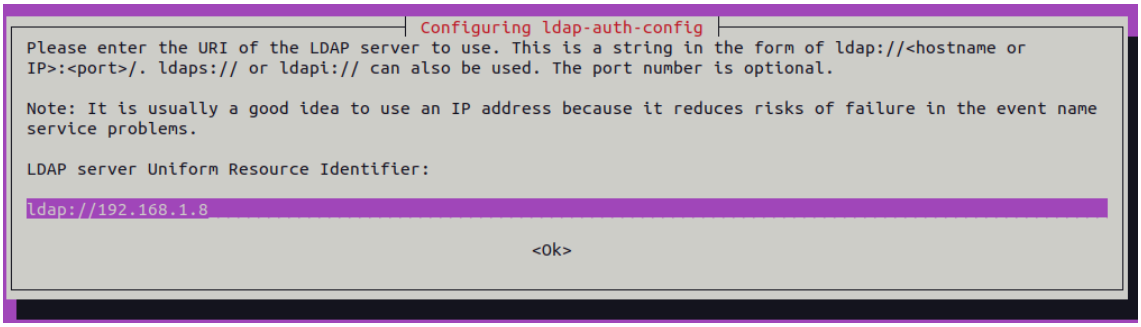
Ahora vamos a configurar el Ubuntu Cliente para que utilice el servidor como directorio de cuentas.

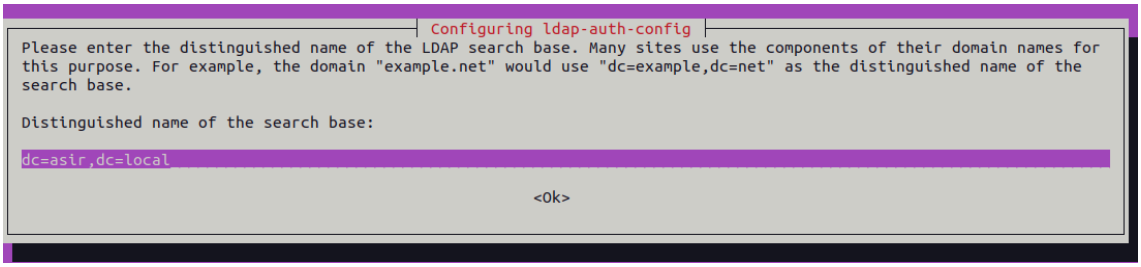
a. Instalación de base de nss pam y nscd.

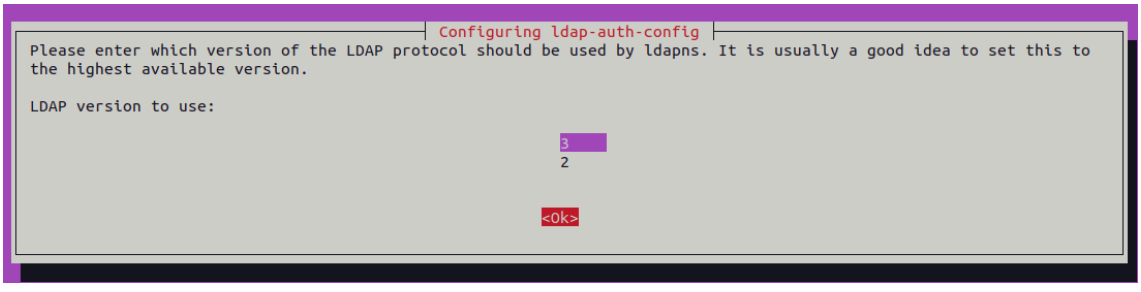
- NSS: Network Security Services, librería de soporte para aplicaciones cliente-servidor multiplataforma.
- PAM: Pluggable Authentication Modules.
- Nscd: es un demonio que proporciona una caché para la mayoría de peticiones comunes del servicio de nombres de red.

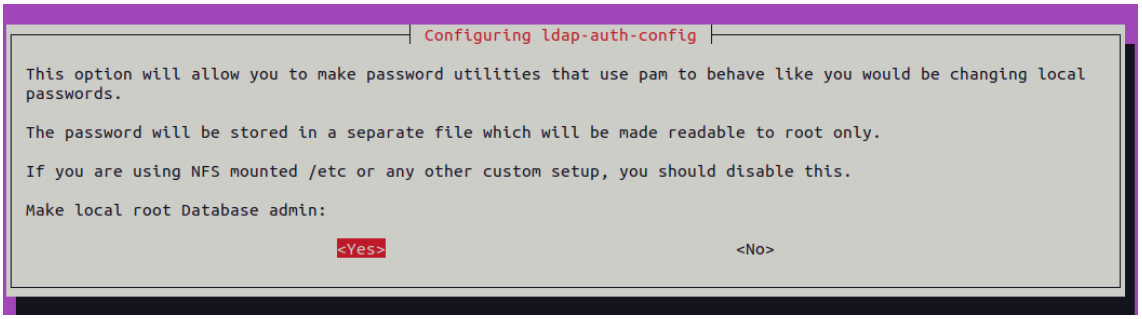
```
sudo apt-get install libnss-ldap libpam-ldap ldap-utils nscd -y
```

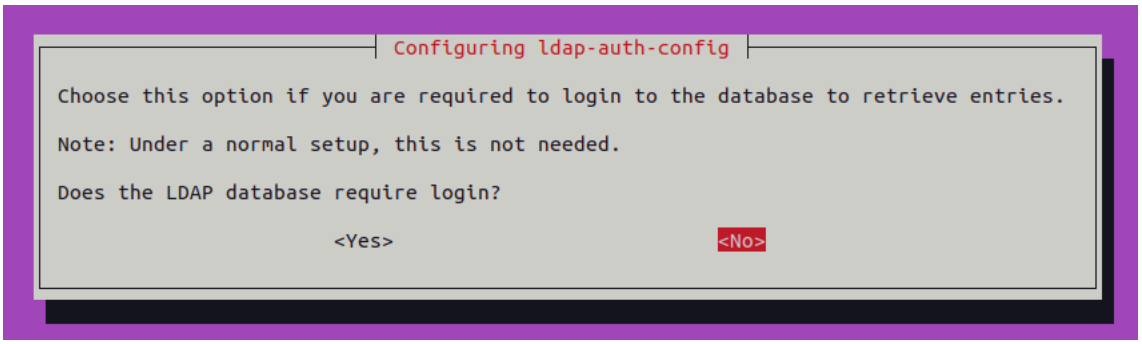


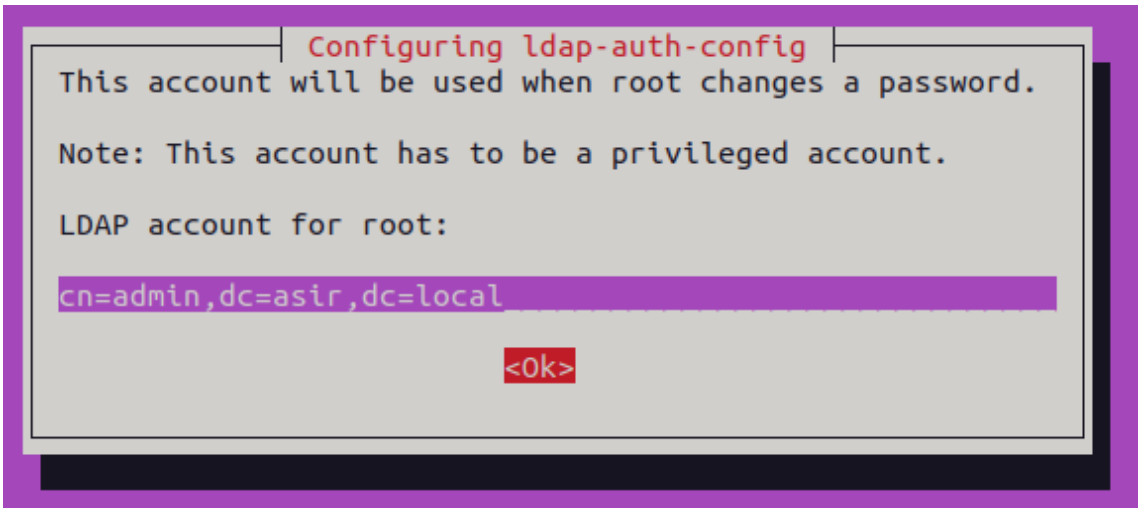


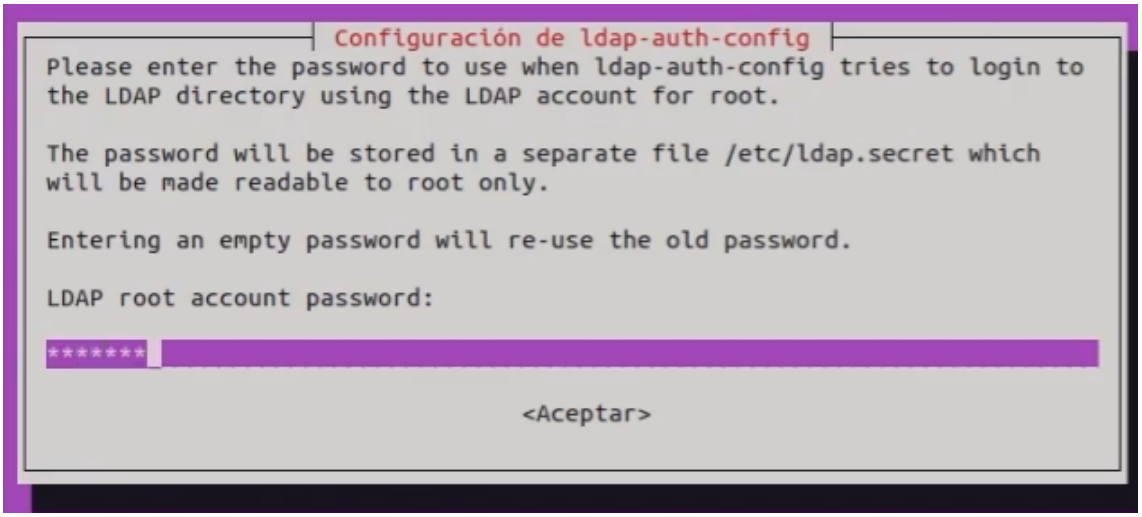





Configuring ldap-auth-config
This option will allow you to make password utilities that use pam to behave like you would be changing local passwords.
The password will be stored in a separate file which will be made readable to root only.
If you are using NFS mounted /etc or any other custom setup, you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


Configuring 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?
<Yes>
<No>


Configuring 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=admin,dc=asir,dc=local
<Ok>


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>

contraseña: changeme

*En caso de que algun dato de la configuracion este mal, ejecutar un dpkg-reconfigure:

```
sudo dpkg-reconfigure ldap-auth-config
```

```
root@ldapserver:/home/pepe/Desktop# dpkg-reconfigure ldap-auth-config
root@ldapserver:/home/pepe/Desktop# nano /etc/nsswitch.conf
root@ldapserver:/home/pepe/Desktop# getent passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:102:105::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
```

b. Configuración de las librerías para habilitar la autenticación remota:

- Modificamos las siguientes entradas así:

```
sudo nano /etc/nsswitch.conf
```

```
passwd:         compat systemd ldap
group:          compat systemd ldap
shadow:         compat
gshadow:        files
```

- Comprobamos si ya se recibe información del servidor.

```
sudo getent passwd
```

```
root@ldapserver:/home/pepe/Desktop# getent passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

```
aza:x:1000:1000:aza,,,:/home/aza:/bin/bash
alumno:*:2000:10000:alumno:/home/alumno:/bin/bash
aza@PC-Linux:~/Desktop$
```

- Ejecutamos una búsqueda contra el servidor y comprobamos si ya tenemos conexión.

```
aza@PC-Linux:~/Desktop$ ldapsearch -x -H ldap://192.168.1.8 -b "dc=asir,dc=local"
```

* Opción -H: permite indicar el host del directorio

- Modificamos PAM para que cree automáticamente directorios de usuarios.

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

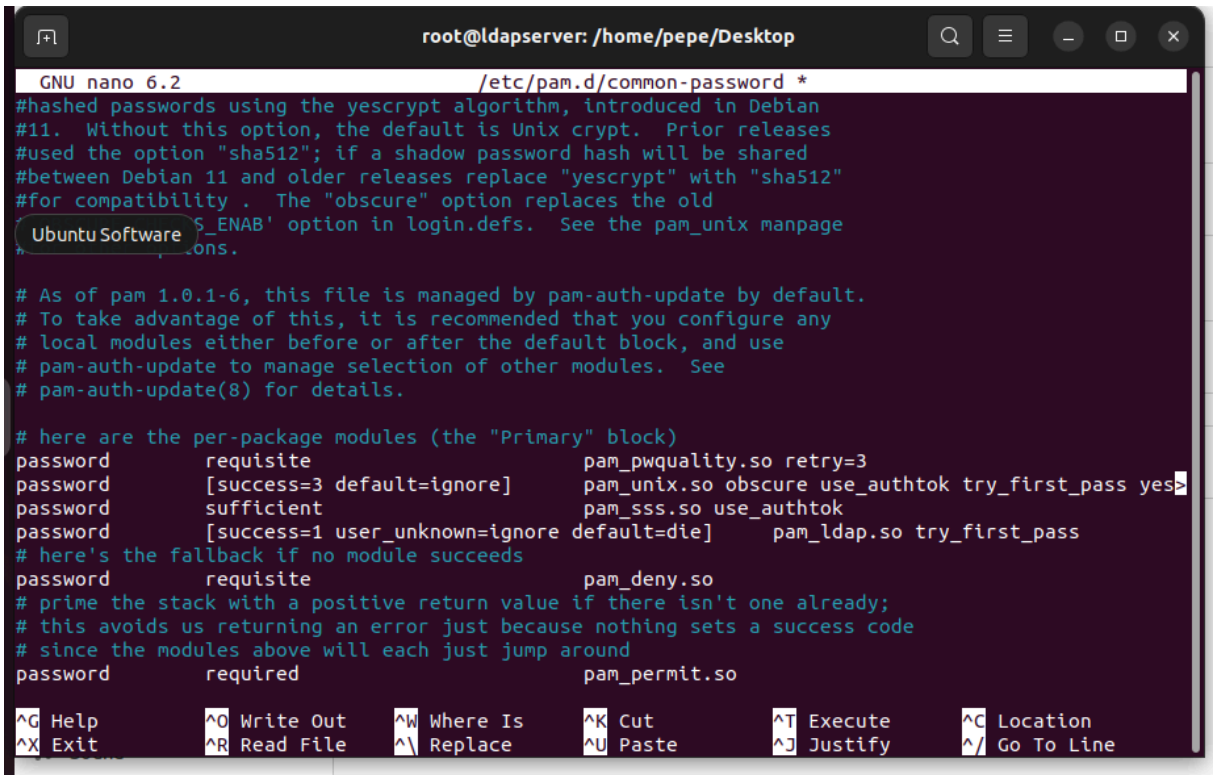
```
# and here are more per-package modules (the "Additional" block)
session required        pam_unix.so
session optional                        pam_sss.so
session optional                        pam_ldap.so
session optional        pam_systemd.so
session optional        pam_mkhomedir.so skel=/etc/skel umask=077
# end of pam-auth-update config
```

```
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_sss.so
session optional                        pam_ldap.so
session optional        pam_systemd.so
session optional        pam_mkhomedir.so skel=/etc/skel umask=077
# end of pam-auth-update config
File Name to Write: /etc/pam.d/common-session
^G Help                 M-D DOS Format          M-A Append              M-B Backup File
^C Cancel               M-M Mac Format          M-P Prepend             ^T Browse
```

- Modificamos PAM para que permita la autenticación remota simple, eliminando la palabra use_authtok.

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

```
  GNU nano 6.2                                  /etc/pam.d/common-password
#used the option "sha512"; if a shadow password hash will be shared
#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        requisite                       pam_pwquality.so retry=3
password        [success=3 default=ignore]      pam_unix.so obscure use_authtok try_first_pass yescrypt
password        sufficient                      pam_sss.so use_authtok
password        [success=1 user_unknown=ignore default=die]     pam_ldap.so use_authtok 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
# end of pam-auth-update config
```



c. Reiniciamos el equipo y comprobamos que el servicio funciona: