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

ADMINISTRACIÓN DE SISTEMAS OPERATIVOS

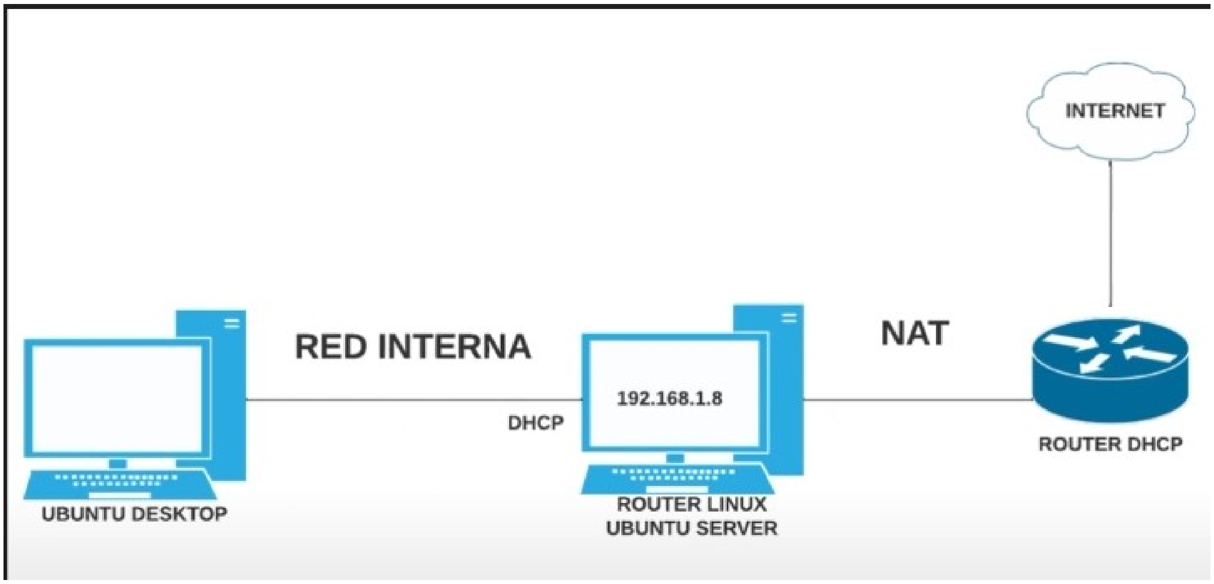
OpenLDAP

Nombre y apellidos:

- Diego Pastrana Monzón

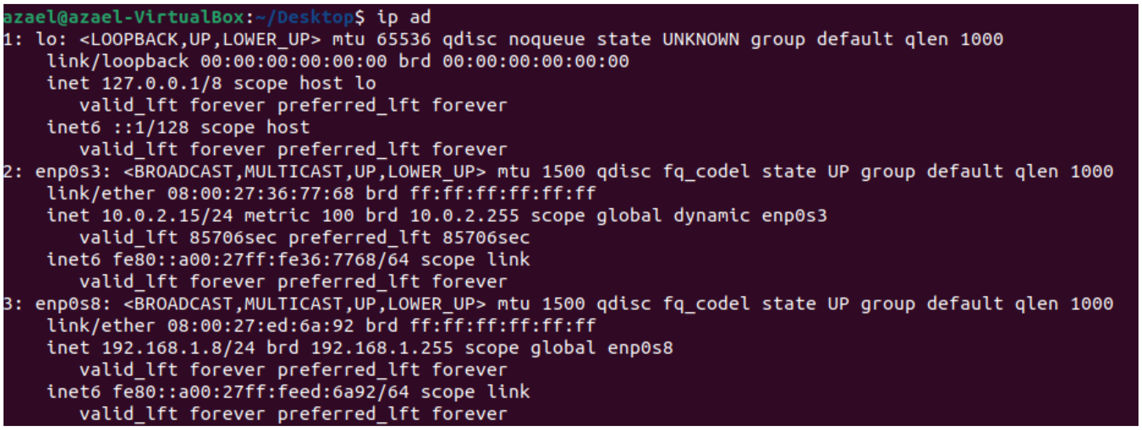
Preparación del entorno.

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



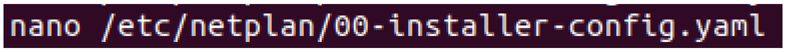
1. Creación y configuración del servidor como router dhcp.

   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”:

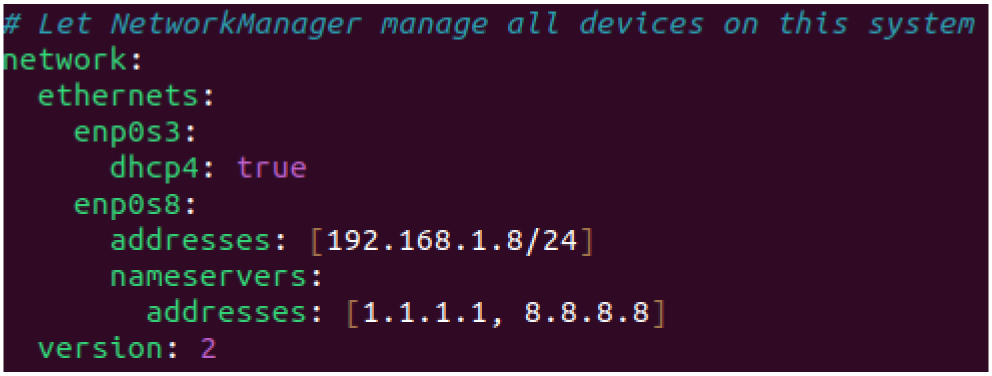


```
azael@azael-VirtualBox:~/Desktop$ ip ad
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       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
```

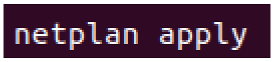
   a. Configuramos NetWorkManager de la siguiente forma:



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

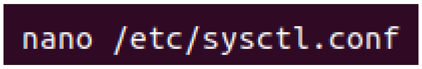


```
# Let NetworkManager manage all devices on this system
network:
  ethernets:
    enp0s3:
      dhcp4: true
    enp0s8:
      addresses: [192.168.1.8/24]
      nameservers:
        addresses: [1.1.1.1, 8.8.8.8]
  version: 2
```

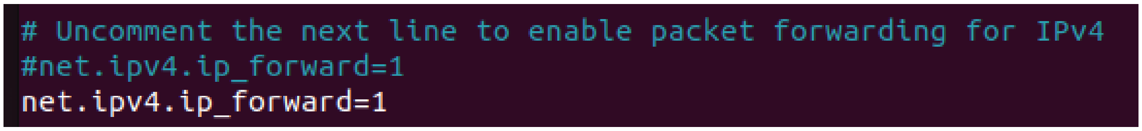


```
netplan apply
```

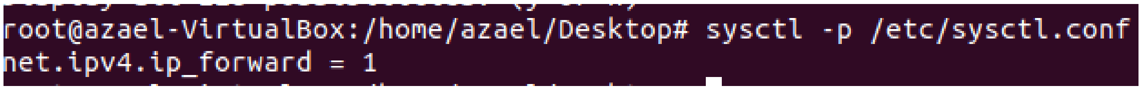
   b. Habilitamos la retransmisión de paquetes:



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

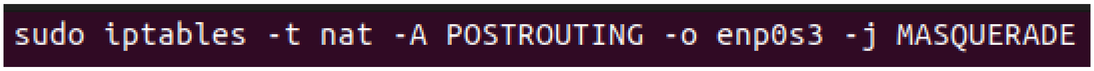


```
# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1
net.ipv4.ip_forward=1
```



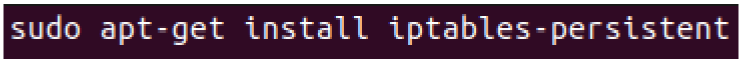
```
root@azael-VirtualBox:/home/azael/Desktop# sysctl -p /etc/sysctl.conf
net.ipv4.ip_forward = 1
```

c. Actualizamos el cortafuegos iptables con la siguiente configuración:

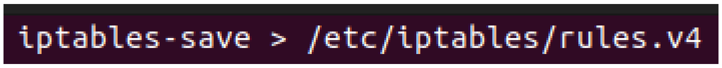


```
sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

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

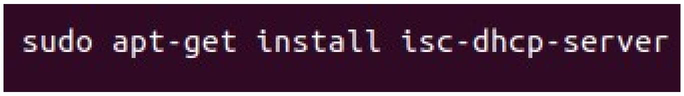


```
sudo apt-get install iptables-persistent
```



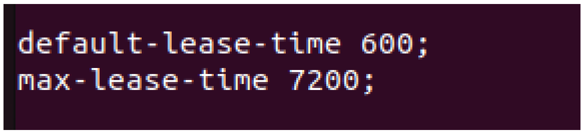
```
iptables-save > /etc/iptables/rules.v4
```

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



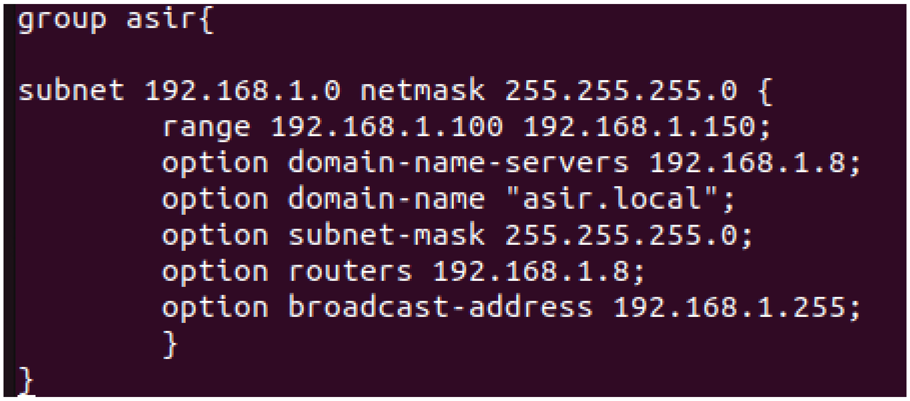
```
sudo apt-get install isc-dhcp-server
```

- Mantenemos los tiempos por defecto.



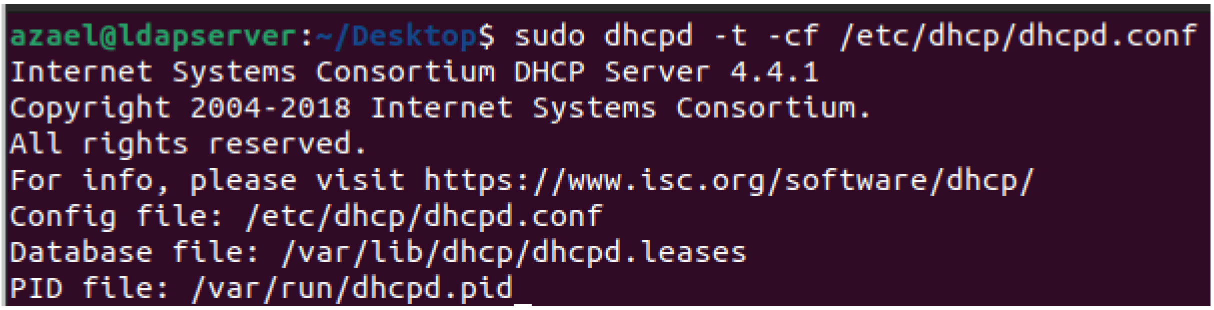
```
default-lease-time 600;
max-lease-time 7200;
```

- Creamos el grupo asir con la siguiente configuración dhcp.



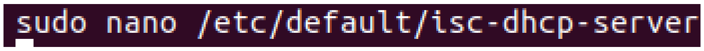
```
group asir{

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.

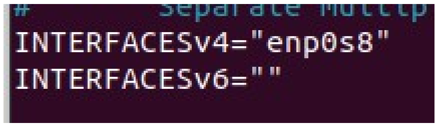


```
azael@ldapserver:~/Desktop$ sudo dhcpd -t -cf /etc/dhcp/dhcpd.conf
Internet Systems Consortium DHCP Server 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /etc/dhcp/dhcpd.conf
Database file: /var/lib/dhcp/dhcpd.leases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

- Habilitamos DHCP en el adaptador de red interna.



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



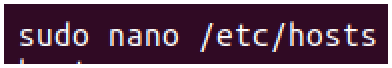
```
#         Separate multip
INTERFACESv4="enp0s8"
INTERFACESv6=""
```

- Reiniciamos el servicio.

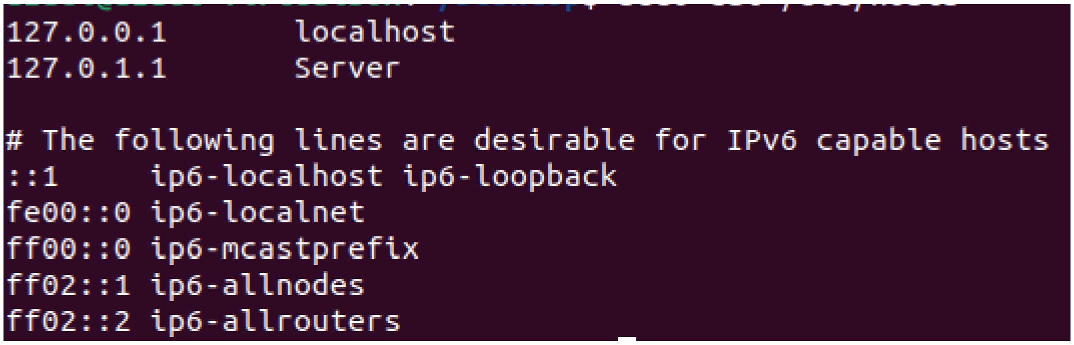
f. Crear una maquina virtual Ubuntu 22.04 denominada Cliente y conectarla a la red interna usando DHCP.

2. Configurar el servidor DNS en el Ubuntu Server.

a. Modificar el archivo host.

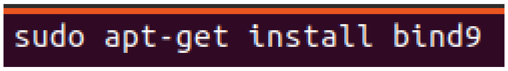


```
sudo nano /etc/hosts
```

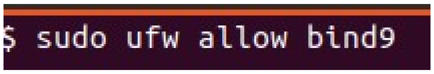


```
127.0.0.1       localhost
127.0.1.1       Server

# 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

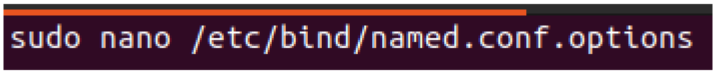


```
sudo apt-get install bind9
```

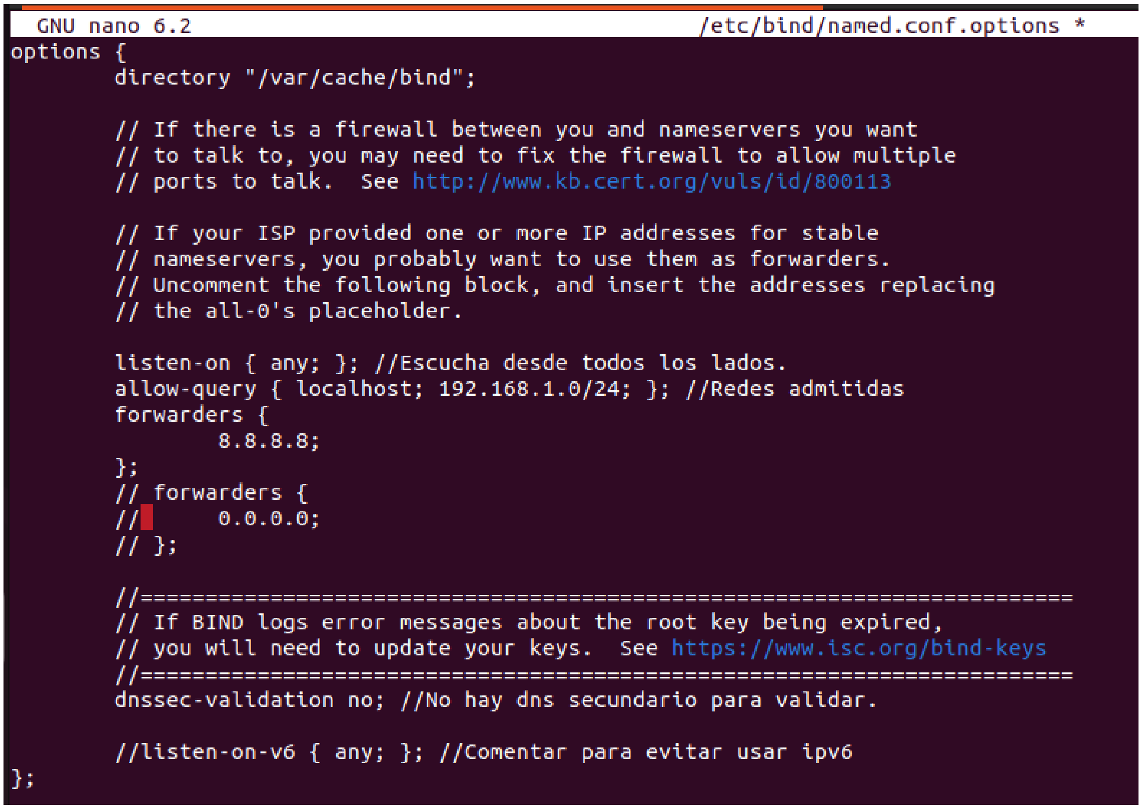


```
$ sudo ufw allow bind9
```

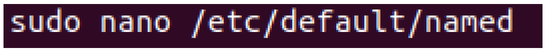
c. Configurar la red que va a usar el DNS:



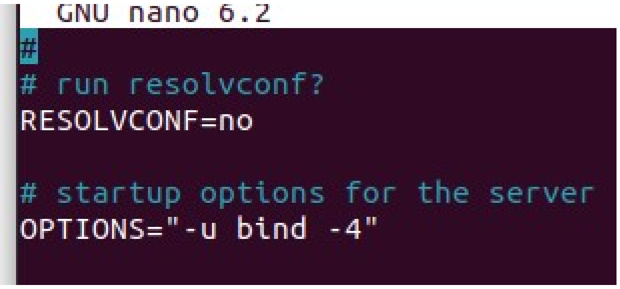
```
sudo nano /etc/bind/named.conf.options
```



```
  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
};
```

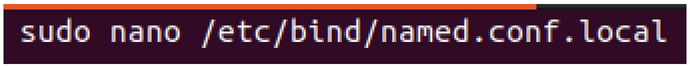


```
sudo nano /etc/default/named
```

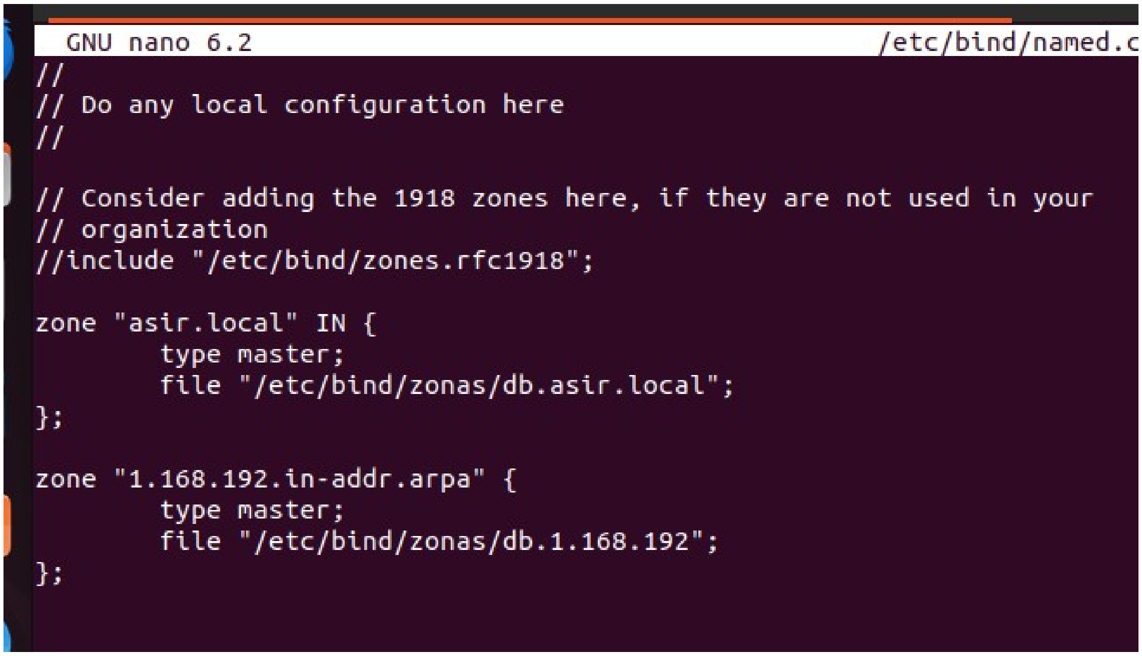


```
  GNU nano 6.2
#
# run resolvconf?
RESOLVCONF=no

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

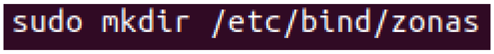
d. Configurar el siguiente dominio.



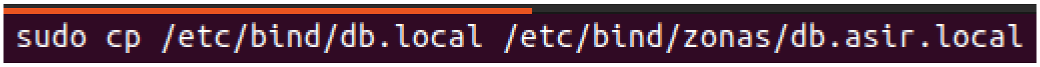
```
sudo nano /etc/bind/named.conf.local
```



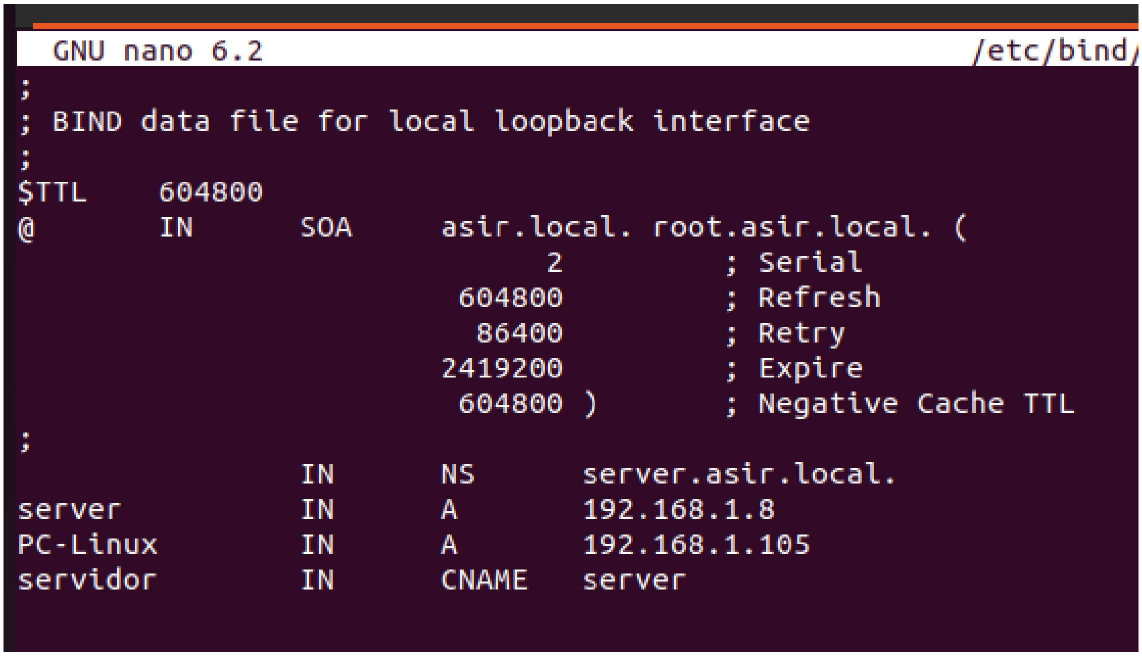
```
  GNU nano 6.2                                              /etc/bind/named.c
//
// Do any local configuration here
//

// 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";
};
```



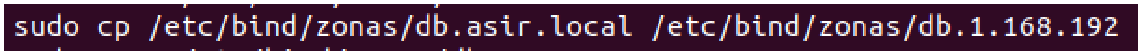
```
sudo mkdir /etc/bind/zonas
```



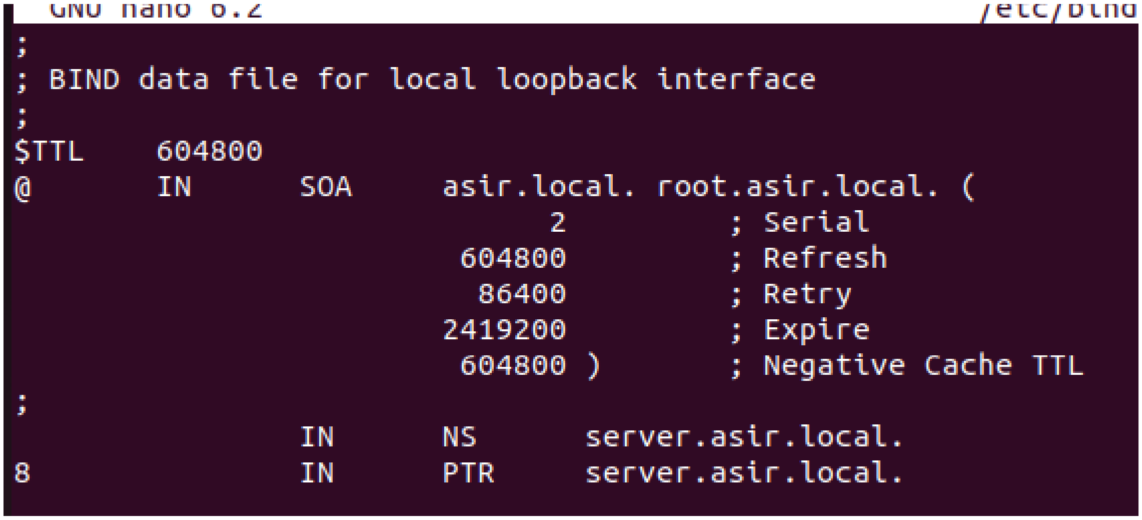
```
sudo cp /etc/bind/db.local /etc/bind/zonas/db.asir.local
```



```
  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
```

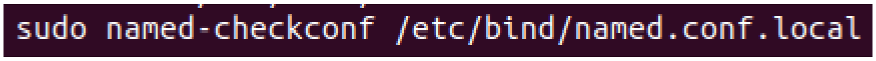


```
sudo cp /etc/bind/zonas/db.asir.local /etc/bind/zonas/db.1.168.192
```

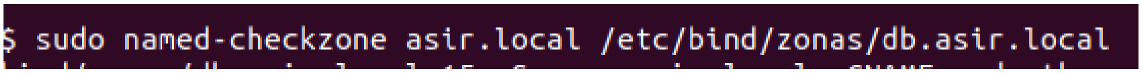


```
  GNU nano 6.2                                              /etc/bind
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     asir.local. root.asir.local. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
                IN      NS      server.asir.local.
8               IN      PTR     server.asir.local.
```

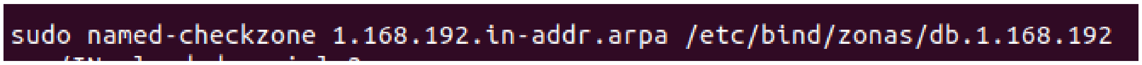
Comprobamos que la configuración esta correcta.



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

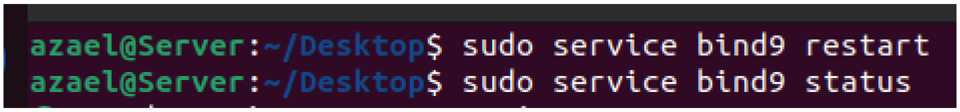


```
$ sudo named-checkzone asir.local /etc/bind/zonas/db.asir.local
```



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

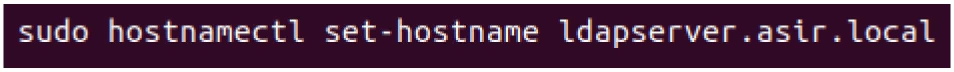
Iniciamos el servicio:



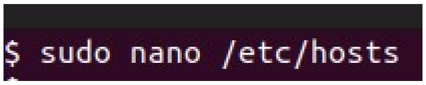
```
azael@Server:~/Desktop$ sudo service bind9 restart
azael@Server:~/Desktop$ sudo service bind9 status
```

3. Configuración de OpenLDAP

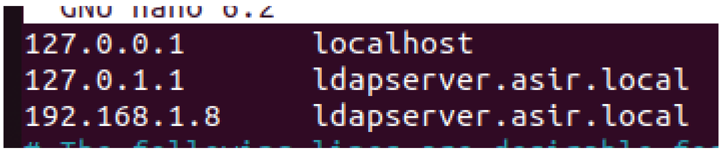
a. Cambiamos el nombre del host



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

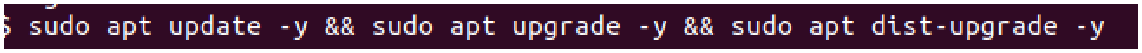


```
$ sudo nano /etc/hosts
```



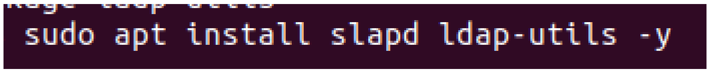
```
  GNU nano 6.2
127.0.0.1       localhost
127.0.1.1       ldapserver.asir.local
192.168.1.8     ldapserver.asir.local
# The following lines are desirable for
```

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

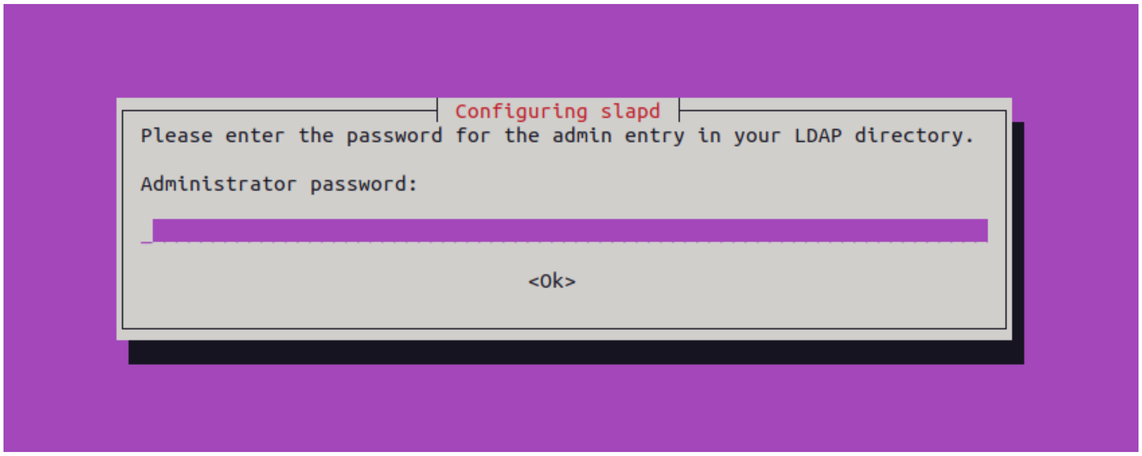


```
$ sudo apt update -y && sudo apt upgrade -y && sudo apt dist-upgrade -y
```

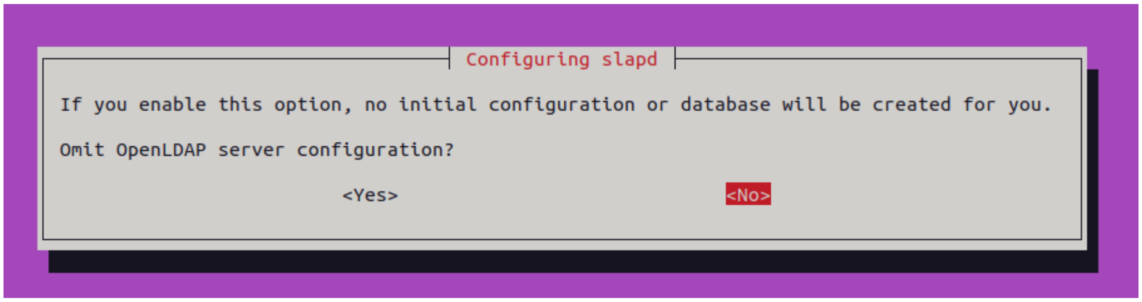
c. Instalamos y configuramos de base OpenLDAP



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

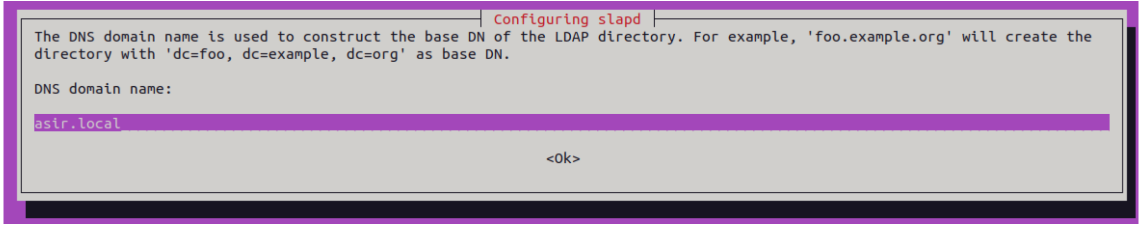


```
Configuring slapd
Please enter the password for the admin entry in your LDAP directory.

Administrator password:

_

<Ok>
```

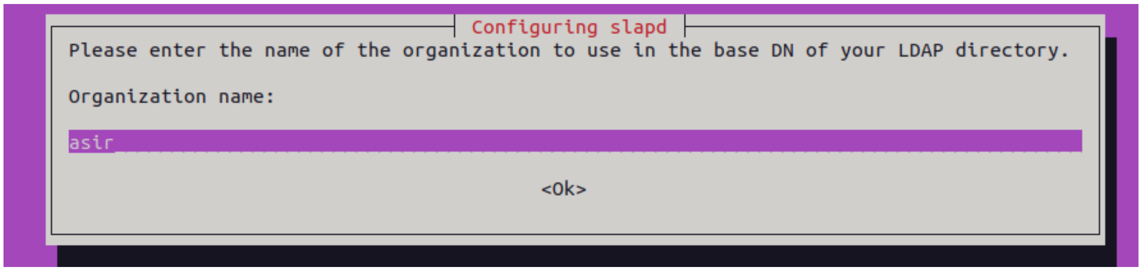


```
Configuring slapd
If you enable this option, no initial configuration or database will be created for you.

Omit OpenLDAP server configuration?

        <Yes>                    <No>
```

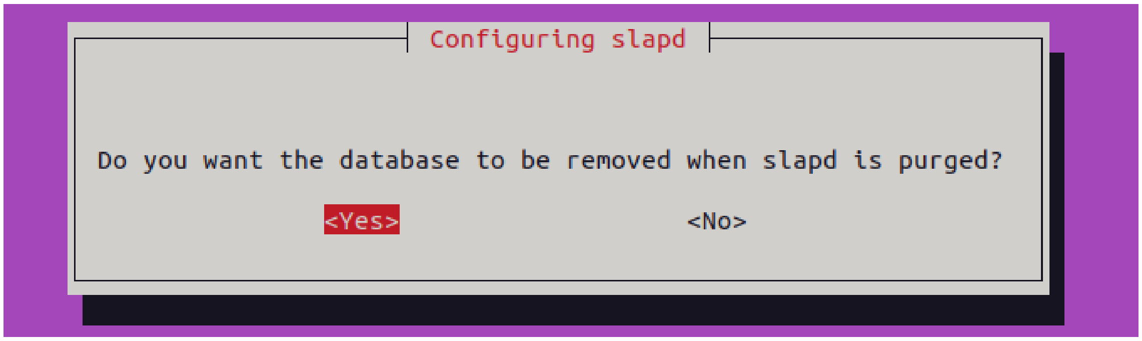
Usamos el DNS que hemos creado.



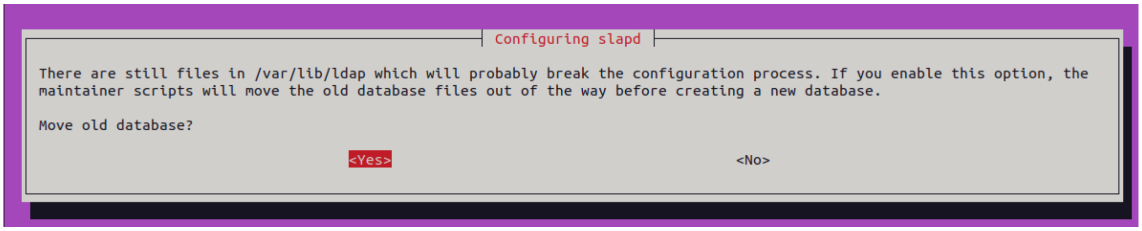
```
Configuring slapd
The DNS domain name is used to construct the base DN of the LDAP directory. For example, 'foo.example.org' will create the
directory with 'dc=foo, dc=example, dc=org' as base DN.

DNS domain name:

asir.local

                                                    <Ok>
```



```
Configuring slapd
Please enter the name of the organization to use in the base DN of your LDAP directory.

Organization name:

asir

                                <Ok>
```

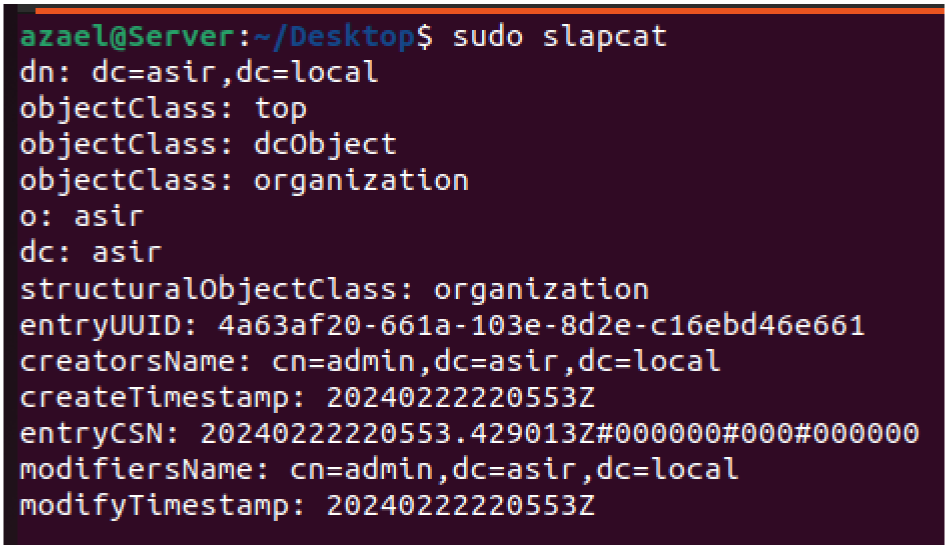


```
Configuring slapd

Do you want the database to be removed when slapd is purged?

          <Yes>                        <No>
```



```
Configuring slapd
There are still files in /var/lib/ldap which will probably break the configuration process. If you enable this option, the
maintainer scripts will move the old database files out of the way before creating a new database.

Move old database?

                          <Yes>                                            <No>
```

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

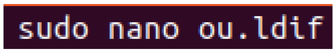


```
azael@Server:~/Desktop$ sudo slapcat
dn: dc=asir,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: asir
dc: asir
structuralObjectClass: organization
entryUUID: 4a63af20-661a-103e-8d2e-c16ebd46e661
creatorsName: cn=admin,dc=asir,dc=local
createTimestamp: 20240222220553Z
entryCSN: 20240222220553.429013Z#000000#000#000000
modifiersName: cn=admin,dc=asir,dc=local
modifyTimestamp: 20240222220553Z
```

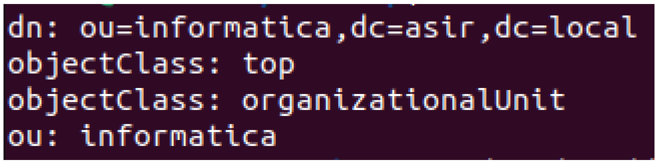
4. Añadir nodos.

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

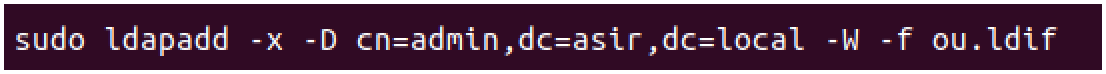
a. Creación de una unidad organizacional.



```
sudo nano ou.ldif
```

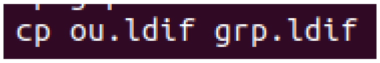


```
dn: ou=informatica,dc=asir,dc=local
objectClass: top
objectClass: organizationalUnit
ou: informatica
```

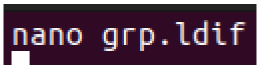


```
sudo ldapadd -x -D cn=admin,dc=asir,dc=local -W -f ou.ldif
```

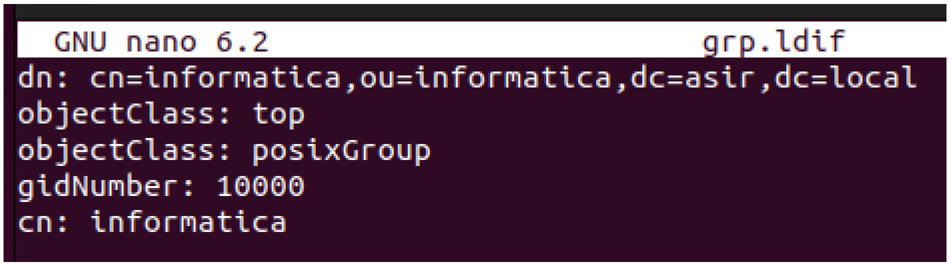
b. Creación de un grupo de usuarios.



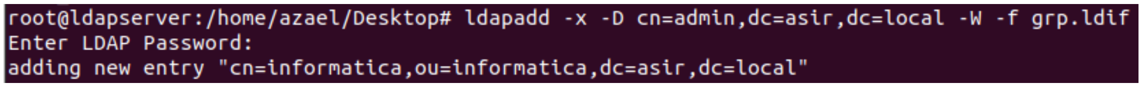
```
cp ou.ldif grp.ldif
```



```
nano grp.ldif
```

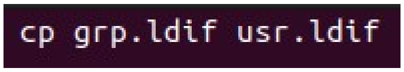


```
  GNU nano 6.2                              grp.ldif
dn: cn=informatica,ou=informatica,dc=asir,dc=local
objectClass: top
objectClass: posixGroup
gidNumber: 10000
cn: informatica
```

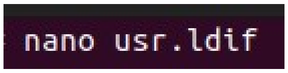


```
root@ldapserver:/home/azael/Desktop# ldapadd -x -D cn=admin,dc=asir,dc=local -W -f grp.ldif
Enter LDAP Password:
adding new entry "cn=informatica,ou=informatica,dc=asir,dc=local"
```

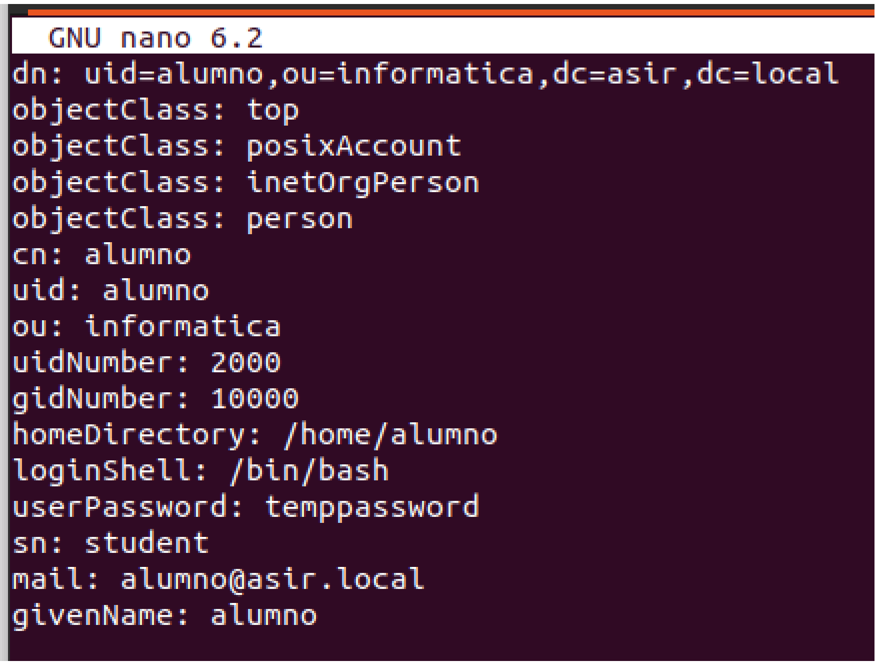
c. Creación de un usuario.



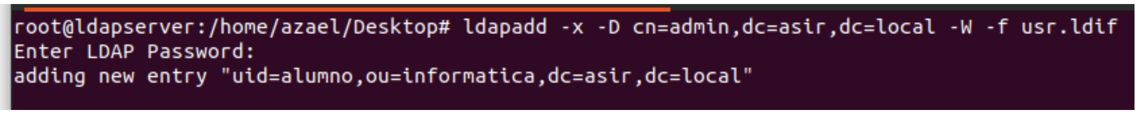
```
cp grp.ldif usr.ldif
```



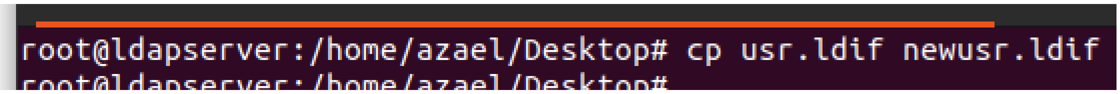
```
nano usr.ldif
```



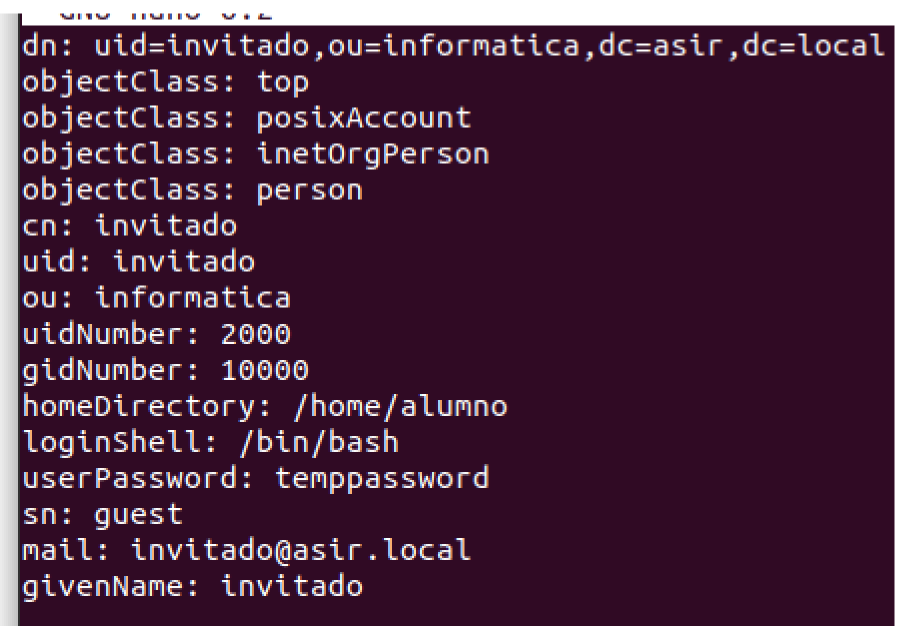
```
  GNU nano 6.2
dn: uid=alumno,ou=informatica,dc=asir,dc=local
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: alumno
uid: alumno
ou: informatica
uidNumber: 2000
gidNumber: 10000
homeDirectory: /home/alumno
loginShell: /bin/bash
userPassword: temppassword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



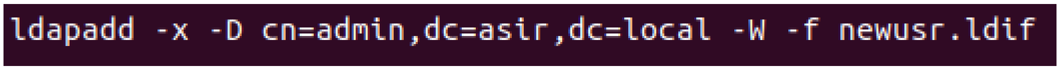
```
root@ldapserver:/home/azael/Desktop# ldapadd -x -D cn=admin,dc=asir,dc=local -W -f usr.ldif
Enter LDAP Password:
adding new entry "uid=alumno,ou=informatica,dc=asir,dc=local"
```



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

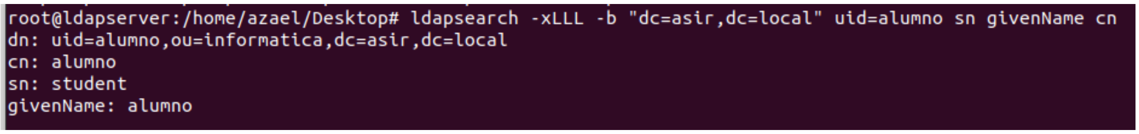


```
  GNU nano 6.2
dn: uid=invitado,ou=informatica,dc=asir,dc=local
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: person
cn: invitado
uid: invitado
ou: informatica
uidNumber: 2000
gidNumber: 10000
homeDirectory: /home/alumno
loginShell: /bin/bash
userPassword: temppassword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

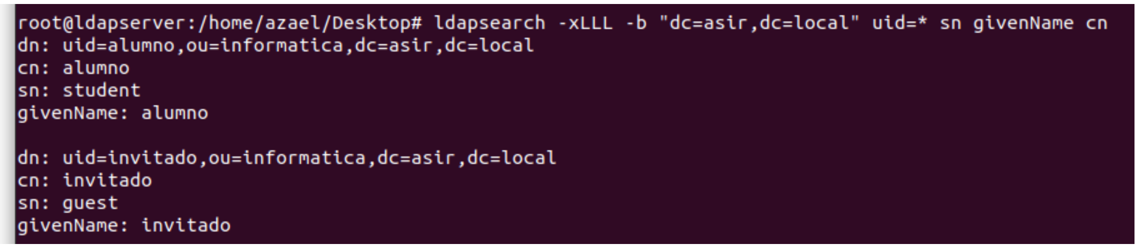


```
ldapadd -x -D cn=admin,dc=asir,dc=local -W -f newusr.ldif
```

d. Búsqueda dentro del directorio

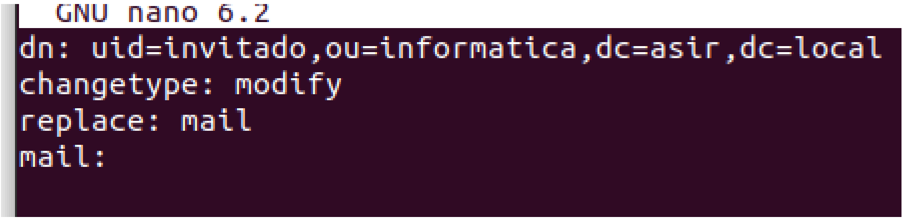


```
root@ldapserver:/home/azael/Desktop# ldapsearch -xLLL -b "dc=asir,dc=local" uid=alumno sn givenName cn
dn: uid=alumno,ou=informatica,dc=asir,dc=local
cn: alumno
sn: student
givenName: alumno
```

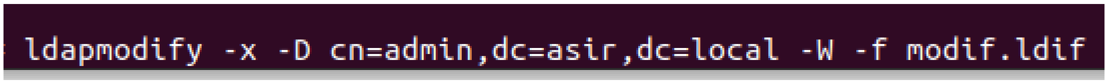


```
root@ldapserver:/home/azael/Desktop# ldapsearch -xLLL -b "dc=asir,dc=local" uid=* sn givenName cn
dn: uid=alumno,ou=informatica,dc=asir,dc=local
cn: alumno
sn: student
givenName: alumno

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

e. Modificación de atributos de una entrada.

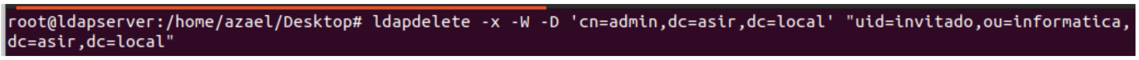


```
  GNU nano 6.2
dn: uid=invitado,ou=informatica,dc=asir,dc=local
changetype: modify
replace: mail
mail:
```



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

f. Eliminación de entradas del directorio.



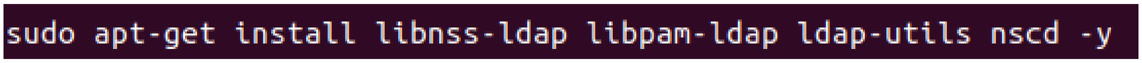
```
root@ldapserver:/home/azael/Desktop# ldapdelete -x -W -D 'cn=admin,dc=asir,dc=local' "uid=invitado,ou=informatica,
dc=asir,dc=local"
```

5. Cliente OpenLDAP

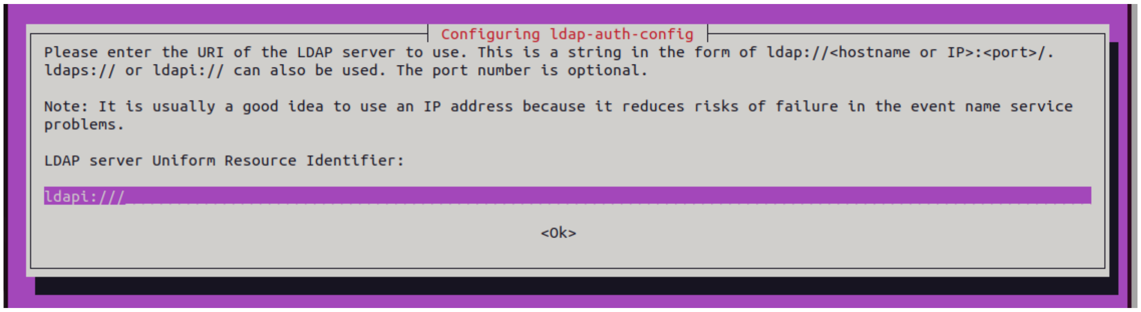
Ahora vamos a configurar el Ubuntu Cliente para que utilice el servidor como directorio de cuentas.

a. Instalación de base de nss pam y nscd.

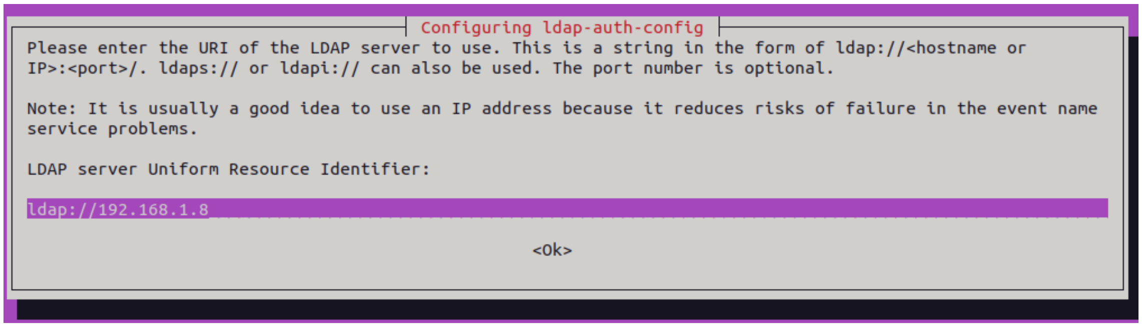
- NSS: Network Security Services, librería de soporte para aplicaciones cliente-servidor multiplataforma.
- PAM: Pluggable Authentication Modules.
- Nscd: es un demonio que proporciona una caché para la mayoría de peticiones comunes del servicio de nombres de red.



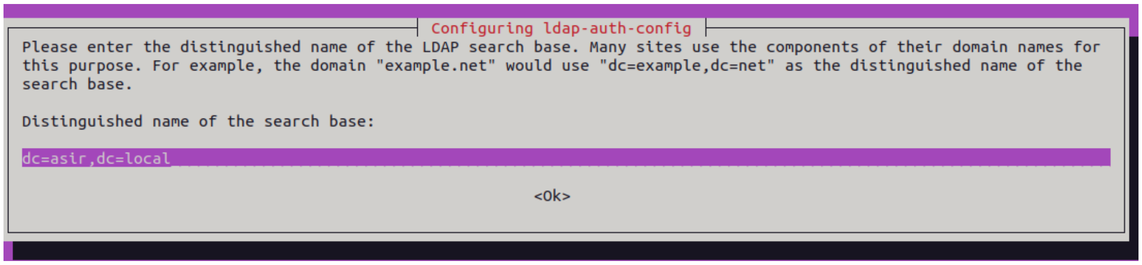
```
sudo apt-get install libnss-ldap libpam-ldap ldap-utils nscd -y
```



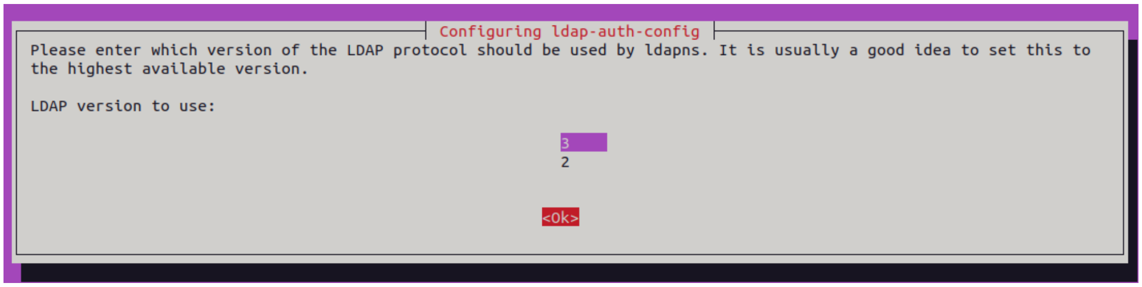
```
Configuring ldap-auth-config
Please enter the URI of the LDAP server to use. This is a string in the form of ldap://<hostname or IP>:<port>/.
ldaps:// or ldapi:// can also be used. The port number is optional.

Note: It is usually a good idea to use an IP address because it reduces risks of failure in the event name service
problems.

LDAP server Uniform Resource Identifier:

ldapi:///

<Ok>
```



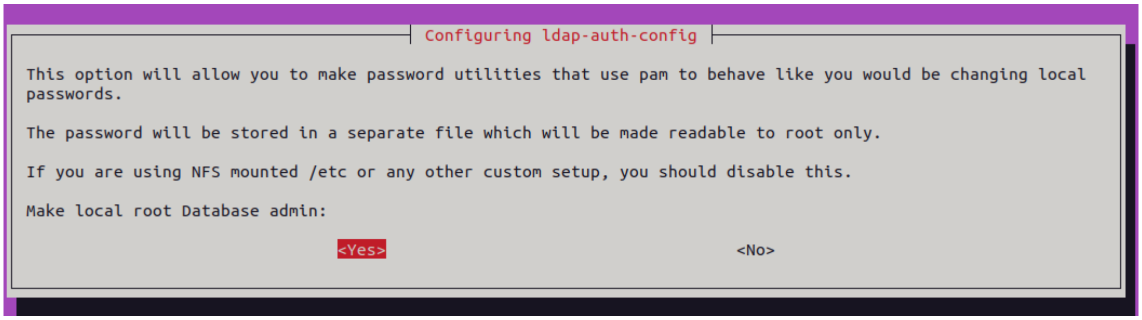
```
Configuring ldap-auth-config
Please enter the URI of the LDAP server to use. This is a string in the form of ldap://<hostname or
IP>:<port>/. ldaps:// or ldapi:// can also be used. The port number is optional.

Note: It is usually a good idea to use an IP address because it reduces risks of failure in the event name
service problems.

LDAP server Uniform Resource Identifier:

ldap://192.168.1.8

<Ok>
```



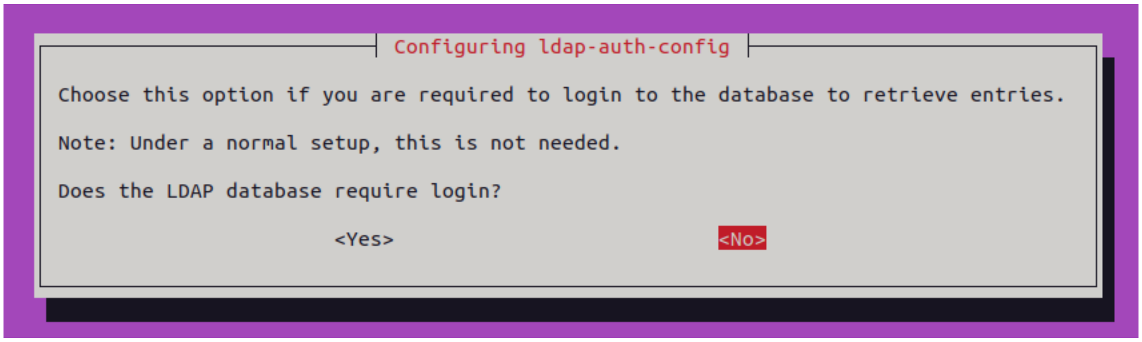
```
Configuring ldap-auth-config
Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for
this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the
search base.

Distinguished name of the search base:

dc=asir,dc=local

<Ok>
```



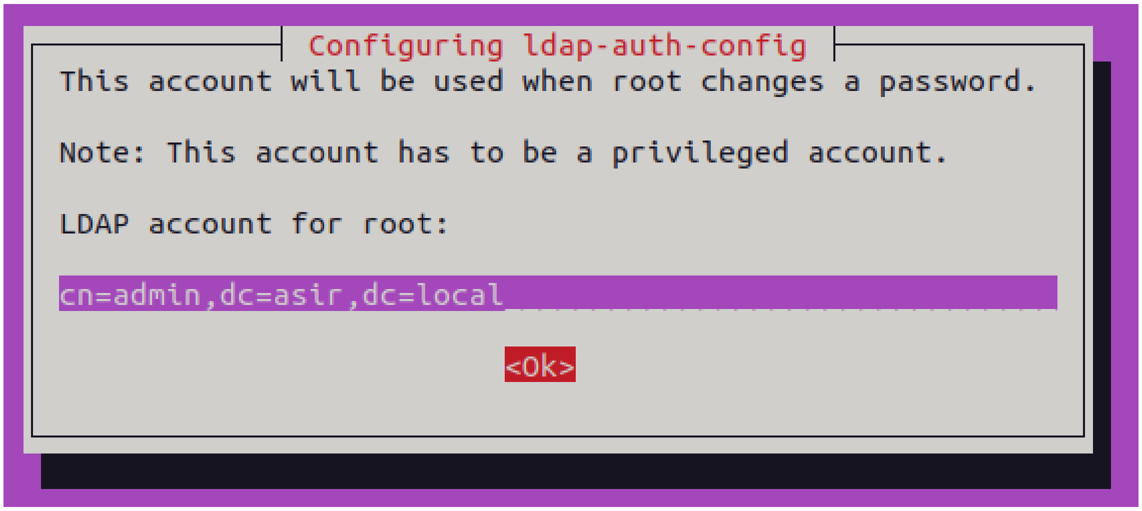
```
Configuring ldap-auth-config
Please enter which version of the LDAP protocol should be used by ldapns. It is usually a good idea to set this to
the highest available version.

LDAP version to use:

                                             3
                                             2

                                            <Ok>
```



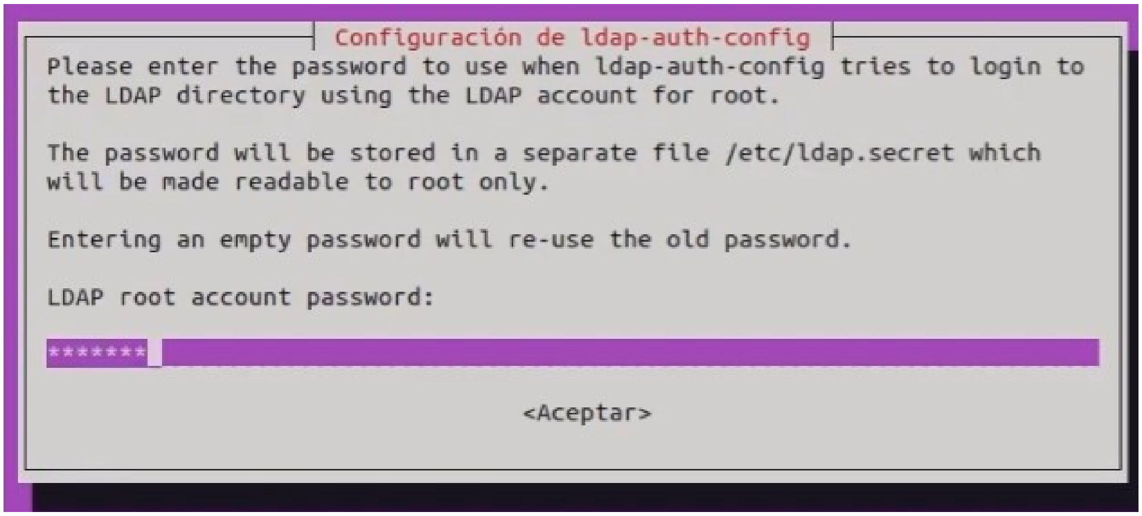
```
Configuring ldap-auth-config

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:
```



```
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?
```

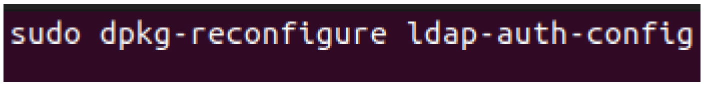


```
Configuring ldap-auth-config
This account will be used when root changes a password.

Note: This account has to be a privileged account.

LDAP account for root:

cn=admin,dc=asir,dc=local
```



```
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:

*******
```

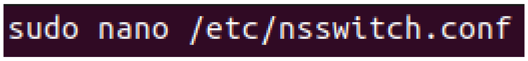
*En caso de que algun dato de la configuracion este mal, ejecutar un dpkg-reconfigure:



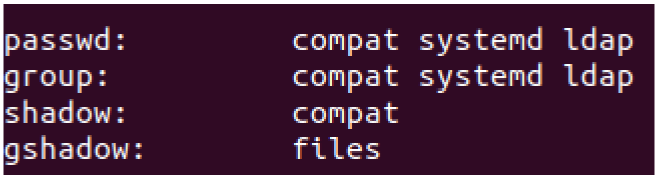
```
sudo dpkg-reconfigure ldap-auth-config
```

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

- Modificamos las siguientes entradas así:

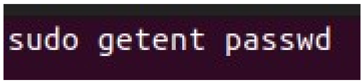


```
sudo nano /etc/nsswitch.conf
```

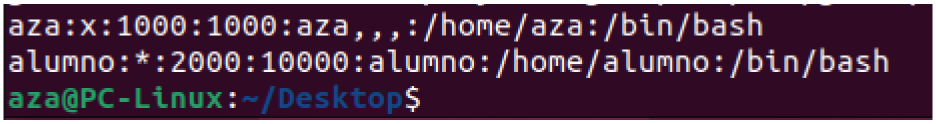


```
passwd:         compat systemd ldap
group:          compat systemd ldap
shadow:         compat
gshadow:        files
```

- Comprobamos si ya se recibe información del servidor.

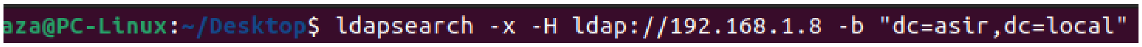


```
sudo getent passwd
```



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

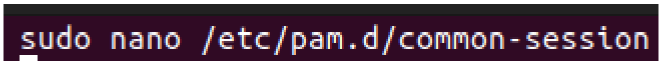
- Ejecutamos una búsqueda contra el servidor y comprobamos si ya tenemos conexión.



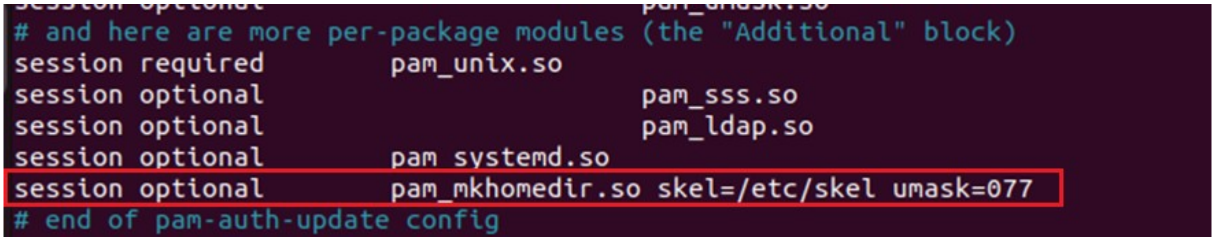
```
aza@PC-Linux:~/Desktop$ ldapsearch -x -H ldap://192.168.1.8 -b "dc=asir,dc=local"
```

* Opción -H: permite indicar el host del directorio

- Modificamos PAM para que cree automáticamente directorios de usuarios.

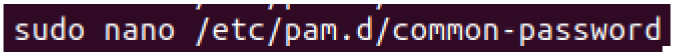


```
sudo nano /etc/pam.d/common-session
```

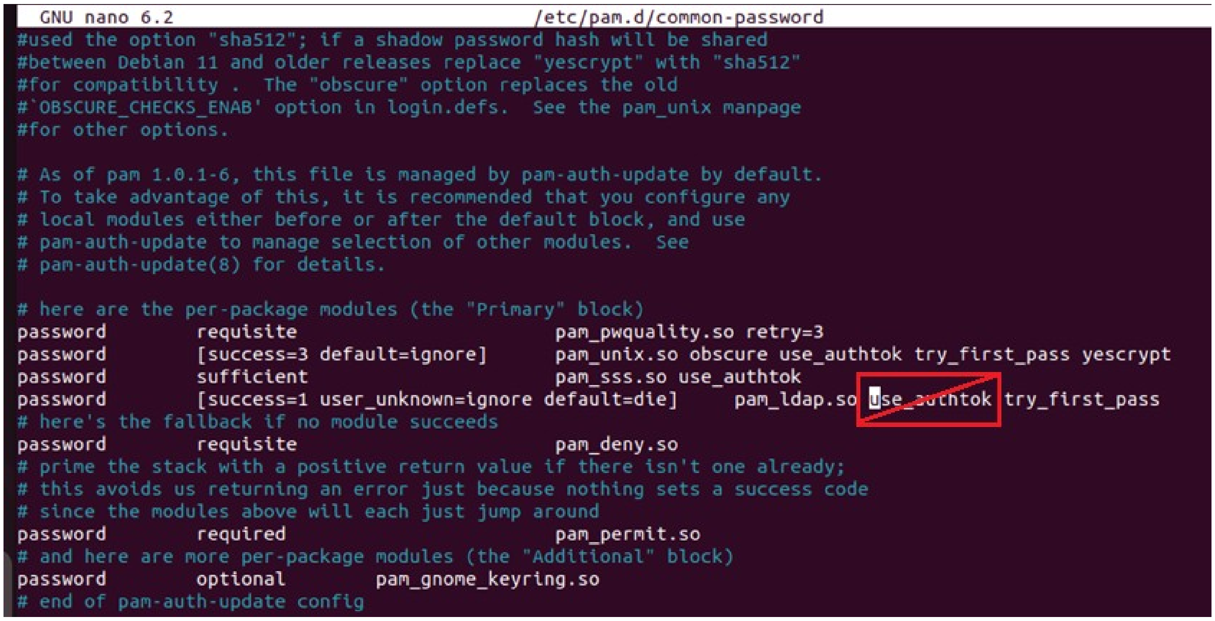


```
session optional                        pam_umask.so
# and here are more per-package modules (the "Additional" block)
session required        pam_unix.so
session optional                        pam_sss.so
session optional                        pam_ldap.so
session optional        pam systemd.so
session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

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

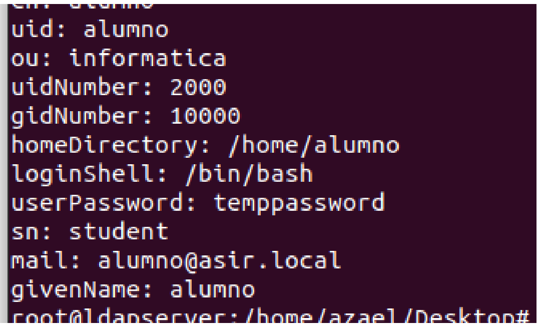


```
sudo nano /etc/pam.d/common-password
```

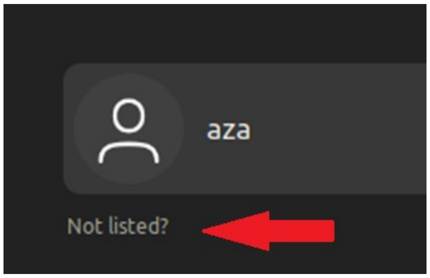


```
  GNU nano 6.2                                  /etc/pam.d/common-password
#used the option "sha512"; if a shadow password hash will be shared
#between Debian 11 and older releases replace "yescrypt" with "sha512"
#for compatibility .  The "obscure" option replaces the old
#`OBSCURE_CHECKS_ENAB' 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
```

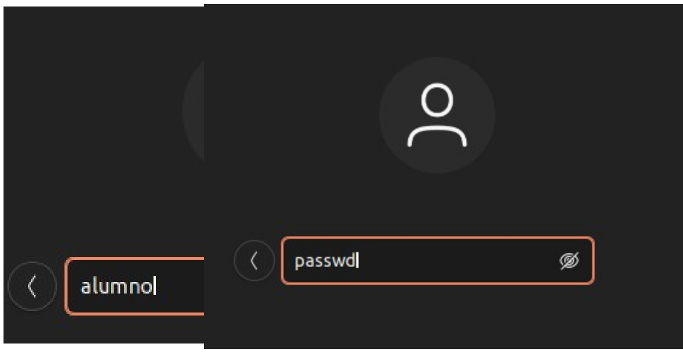
c. Reiniciamos el equipo y comprobamos que el servicio funciona:



```
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#
```



aza
Not listed?



alumno
passwd