Cliente-Servidor Openldap

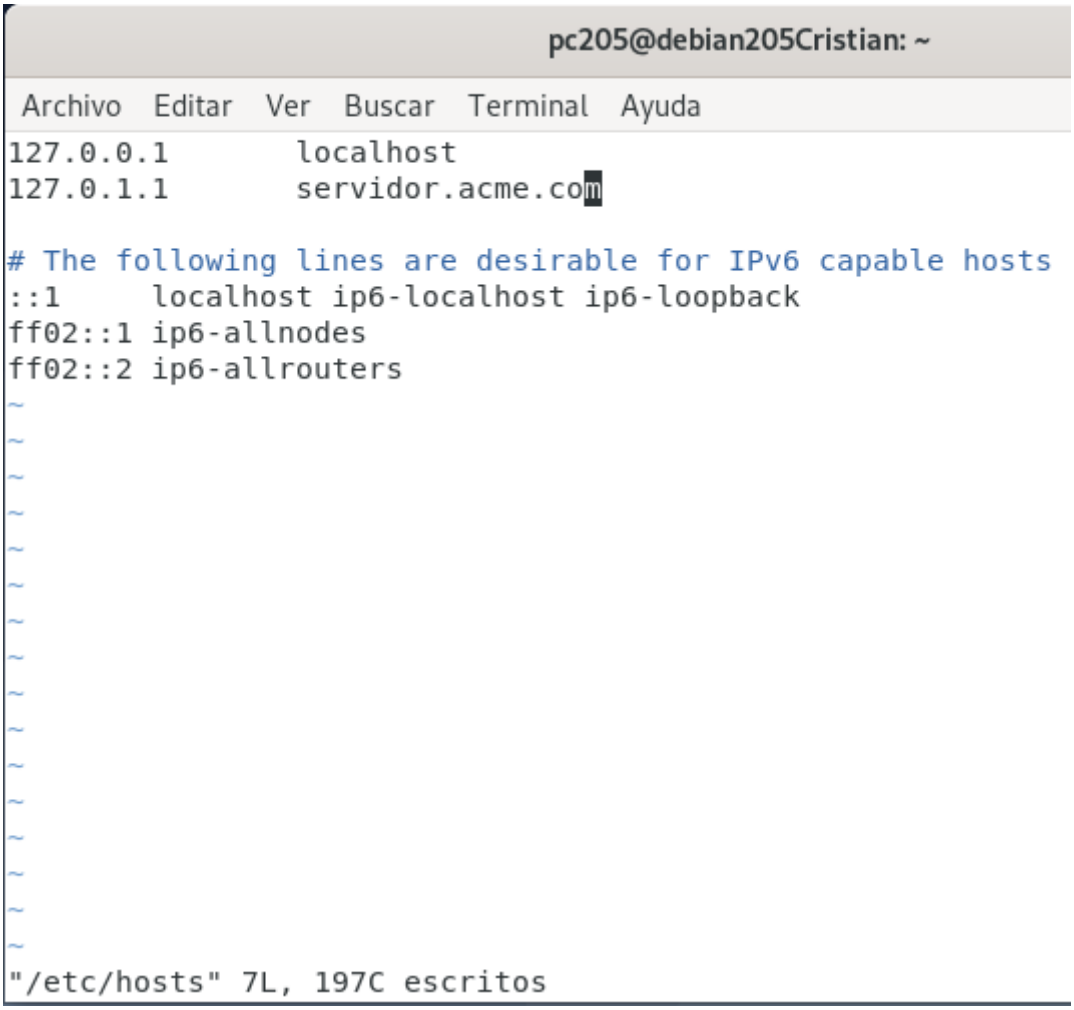
SERVIDOR

1. **Que se hagan ping entre ellos**
2. **Archivo /etc/resolv.conf**

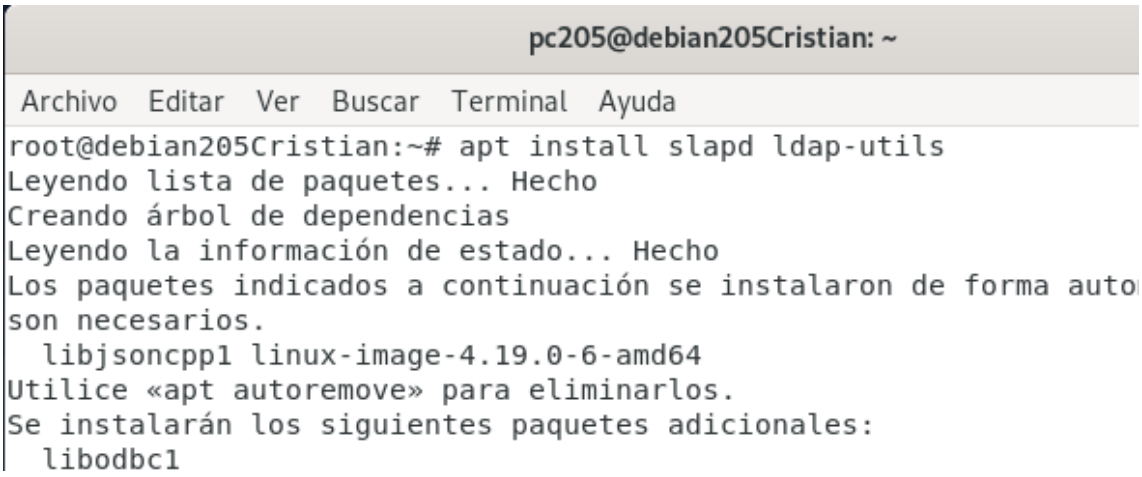
3. **Archvio /etc/hostname**

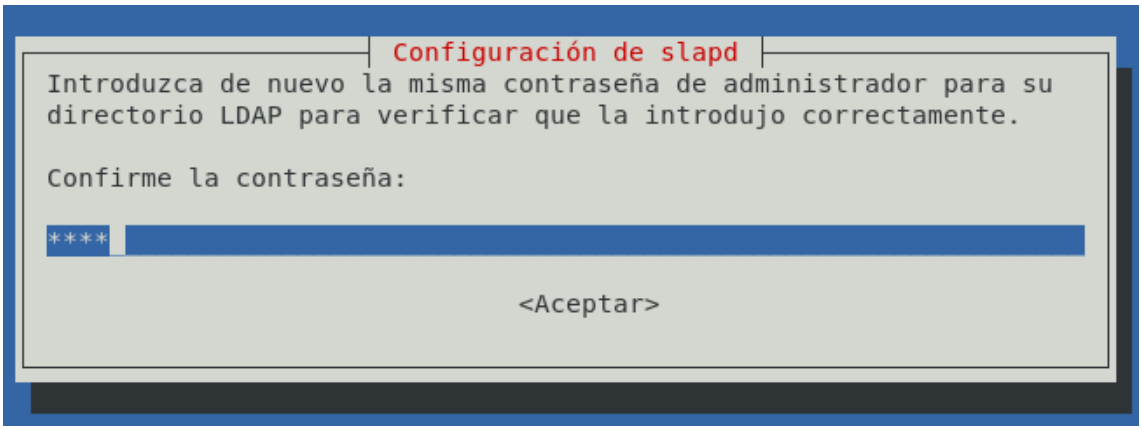

pc205@debian205Cristian: ~
Archivo Editar Ver Buscar Terminal Ayuda
servidor.acme.com
"/etc/hostname" 1L, 18C

4. **Archivo /etc/hosts**



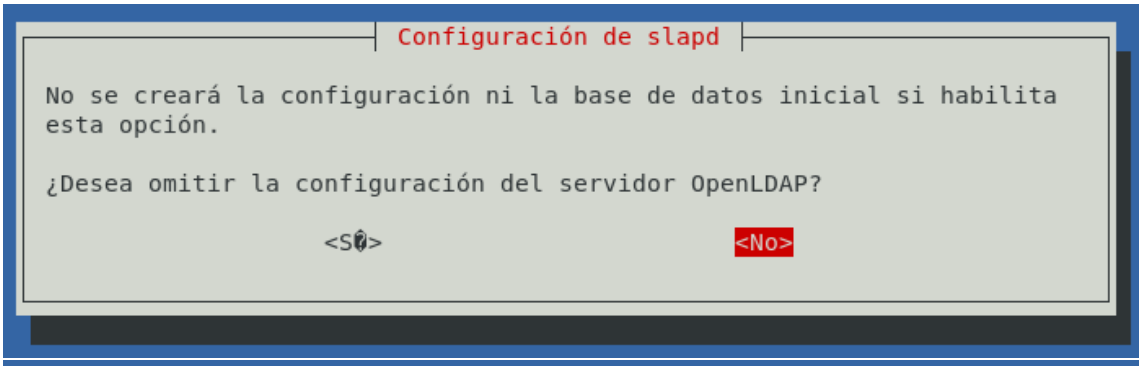
5. **Instalar LDAP**

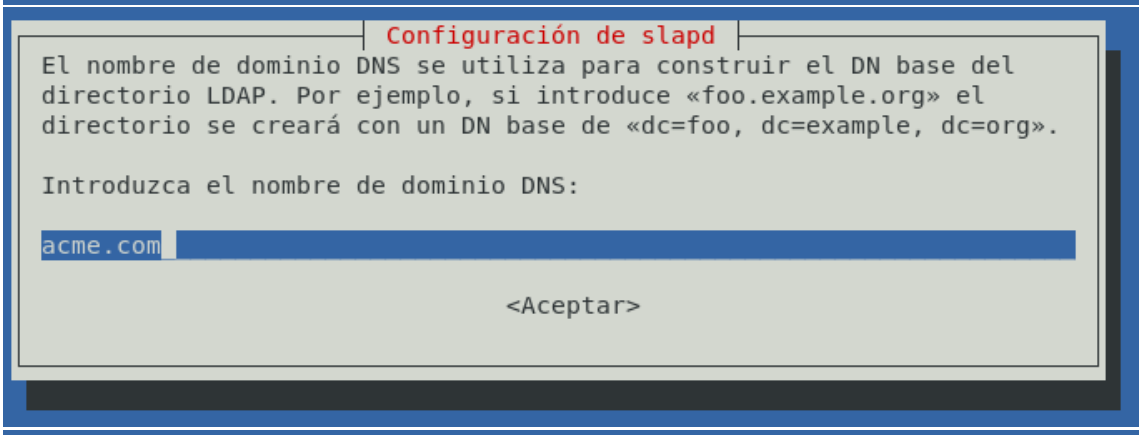


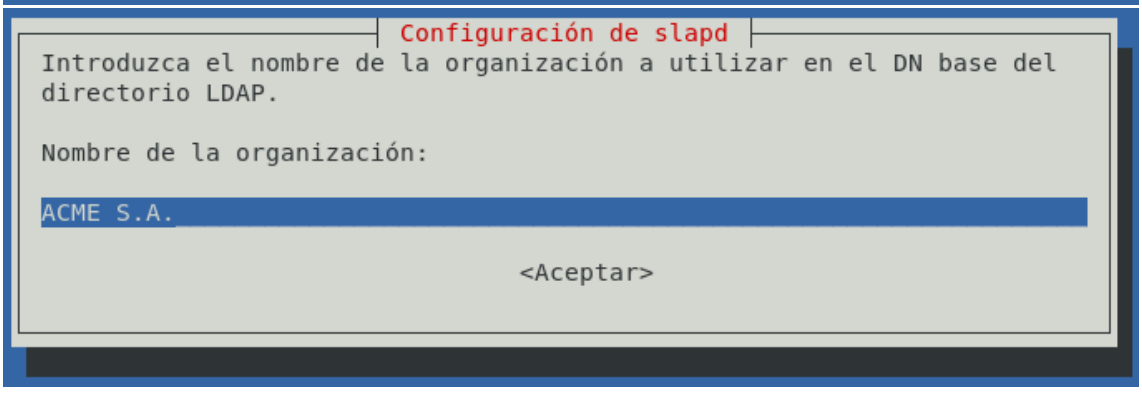


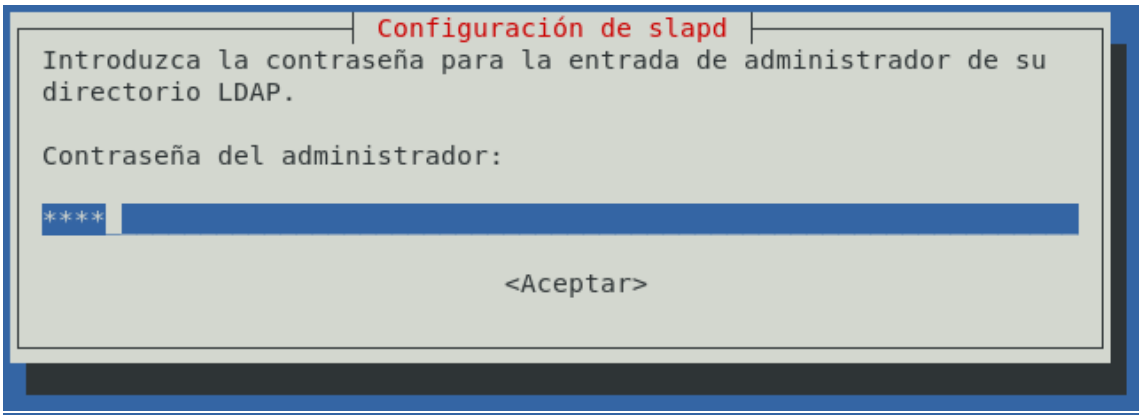
Contraseña root

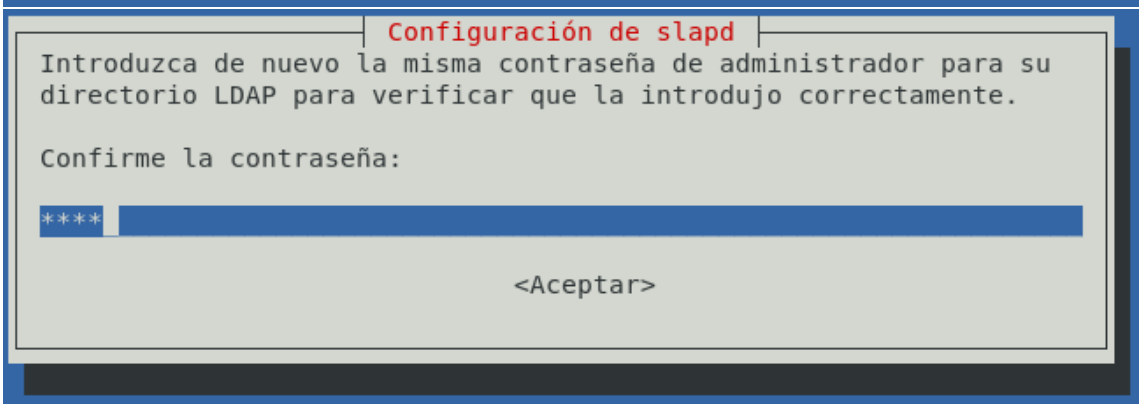
Dpkg-reconfigure slapd

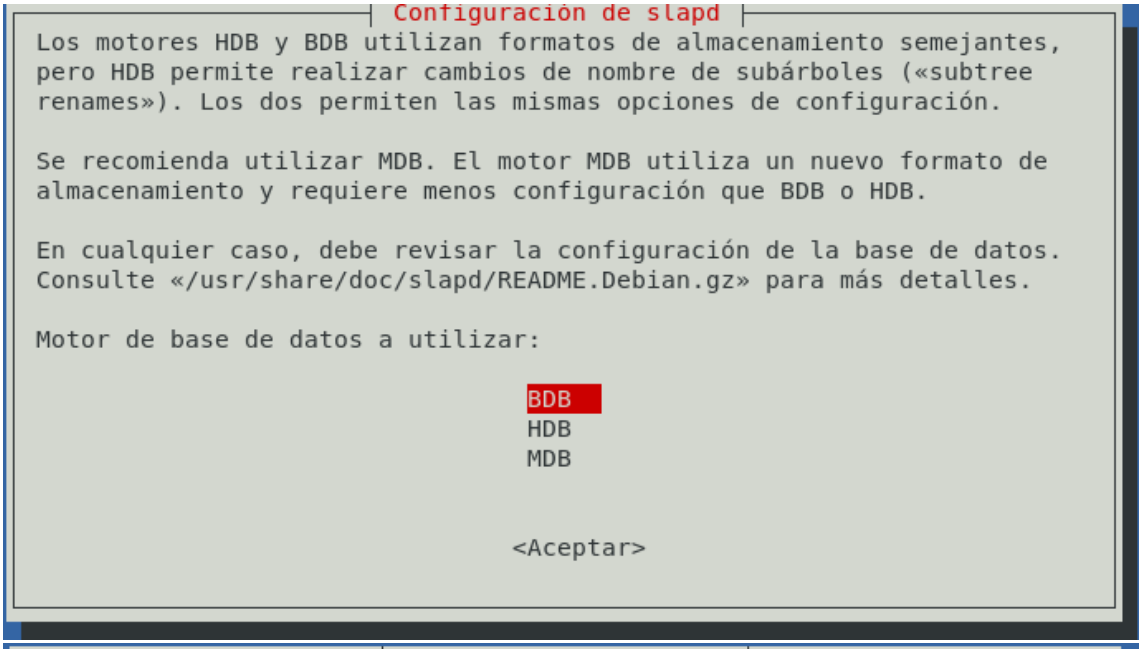


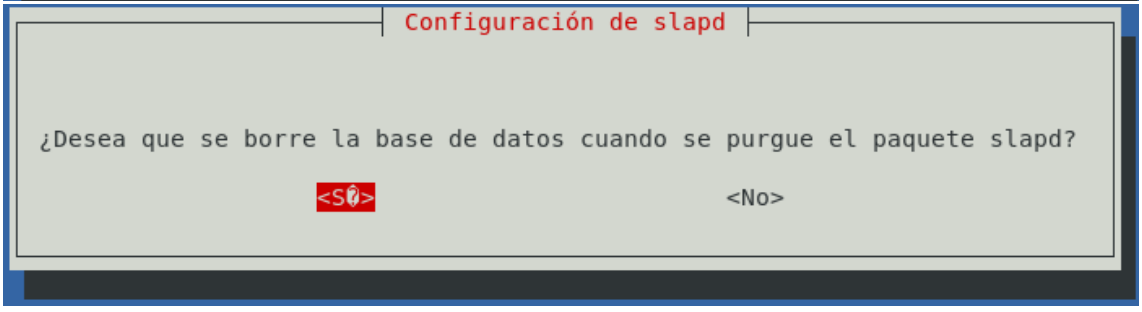


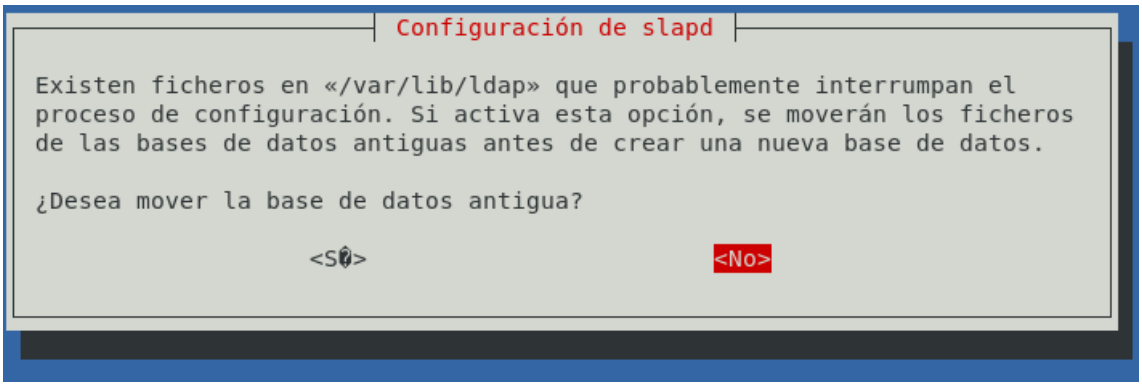



Configuración de slapd
Introduzca la contraseña para la entrada de administrador de su directorio LDAP.
Contraseña del administrador:
****
<Aceptar>

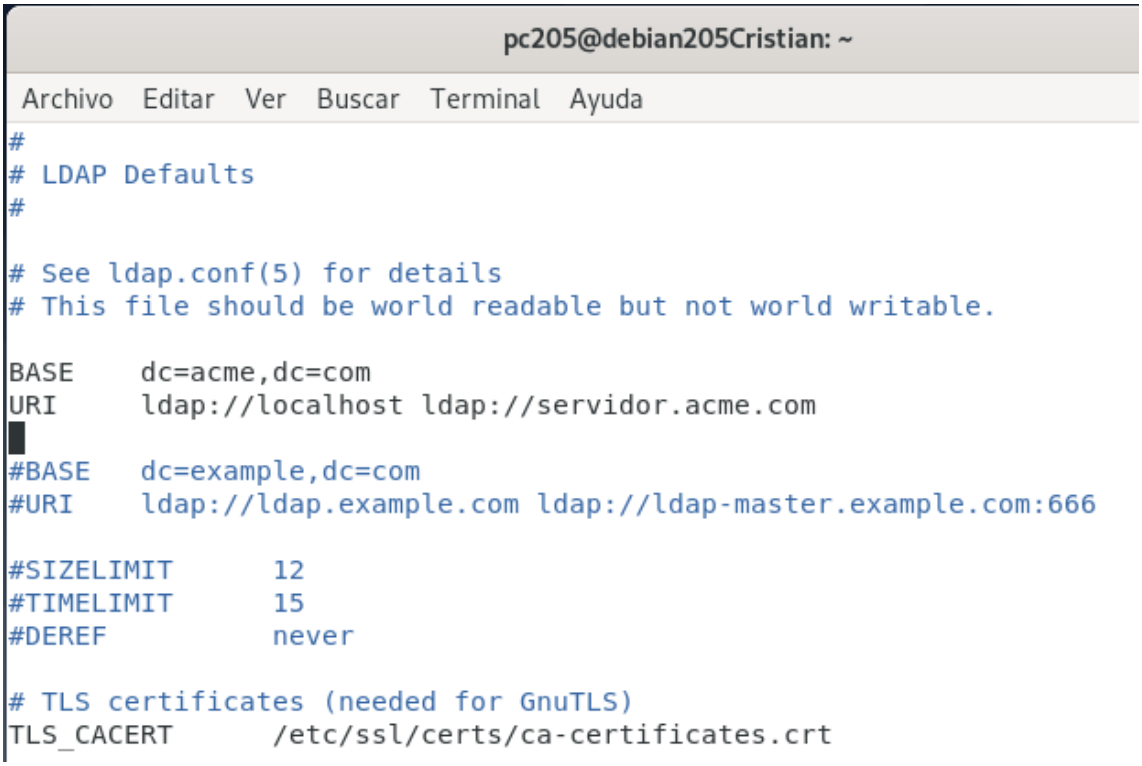

Configuración de slapd
Introduzca de nuevo la misma contraseña de administrador para su directorio LDAP para verificar que la introdujo correctamente.
Confirme la contraseña:
****
<Aceptar>


Configuración de slapd
Los motores HDB y BDB utilizan formatos de almacenamiento semejantes, pero HDB permite realizar cambios de nombre de subárboles («subtree renames»). Los dos permiten las mismas opciones de configuración.
Se recomienda utilizar MDB. El motor MDB utiliza un nuevo formato de almacenamiento y requiere menos configuración que BDB o HDB.
En cualquier caso, debe revisar la configuración de la base de datos. Consulte «/usr/share/doc/slapd/README.Debian.gz» para más detalles.
Motor de base de datos a utilizar:
BDB
HDB
MDB
<Aceptar>


Configuración de slapd
¿Desea que se borre la base de datos cuando se purgue el paquete slapd?
<Sí>
<No>



6. **Archivo /etc/ldap/ldap.conf**



7. **Slapcat**

```
root@debian205Cristian:~# slapcat
dn: dc=acme,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: ACME S.A.
dc: acme
```

8. **Ficheros ldif para cargar el esquema.**

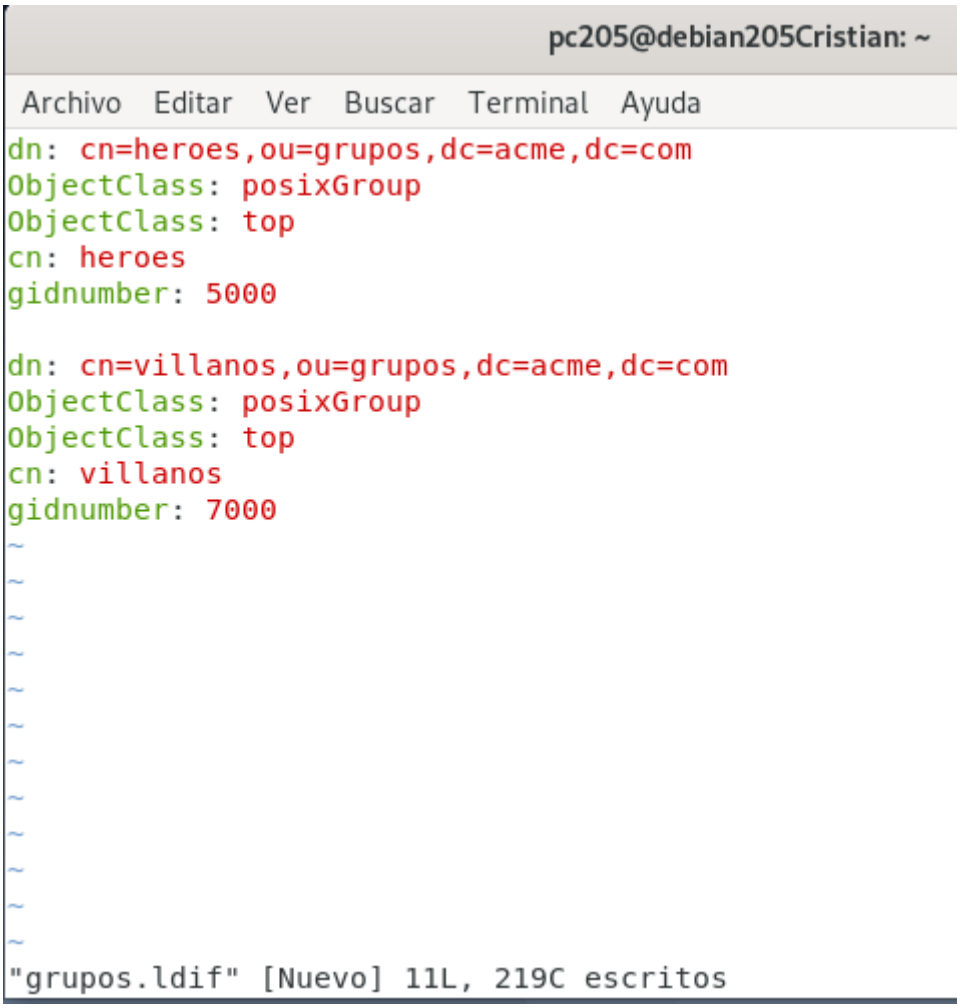
   ARCHIVO base.ldif

pc205@debian205Cristian: ~

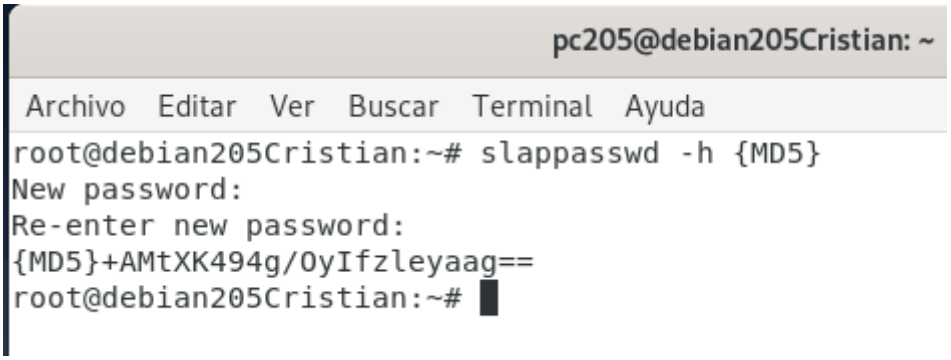
Archivo Editar Ver Buscar Terminal Ayuda

```
dn: ou=usuarios,dc=acme,dc=com
ou: usuarios
ObjectClass: top
ObjectClass: organizationalUnit

dn: ou=grupos,dc=acme,dc=com
ou: grupos
ObjectClass: top
ObjectClass: organizationalUnit
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"base.ldif" [Nuevo] 9L, 183C escritos
```

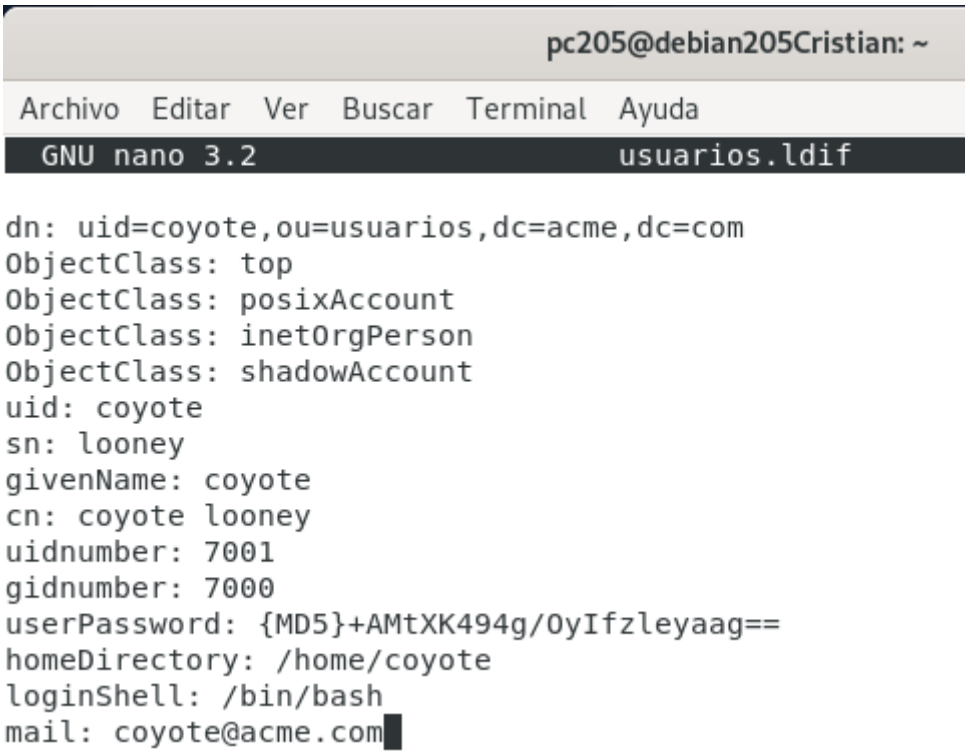
ARCHIVO grupos.ldif



CREO UNA CONSTRASEÑA PARA LOS USUARIOS. Contraseña usuario



ARCHIVO usuarios.ldif



9. **Añado los datos introducidos en dichos ficheros.**

Archivo base.ldif

```
root@debian205Cristian:~# ldapadd -x -W -D cn=admin,dc=acme,dc=com -f base.ldif
Enter LDAP Password:
adding new entry "ou=usuarios,dc=acme,dc=com"

adding new entry "ou=grupos,dc=acme,dc=com"
```

Archivo grupos.ldif

```
root@debian205Cristian:~# ldapadd -x -W -D cn=admin,dc=acme,dc=com -f grupos.ldi
f
Enter LDAP Password:
adding new entry "cn=heroes,ou=grupos,dc=acme,dc=com"

adding new entry "cn=villanos,ou=grupos,dc=acme,dc=com"
```

Archivo usuarios.ldif

```
root@debian205Cristian:~# ldapadd -x -W -D cn=admin,dc=acme,dc=com -f usuarios.l
dif
Enter LDAP Password:
adding new entry "uid=coyote,ou=usuarios,dc=acme,dc=com"
```

PARA BORRAR UN USUARIO

Ldapdelete -W -D cn=admin,dc=acme,dc=com

“uid=nombreusuario,ou=grupo,dc=acme,dc=com”

PARA COMPROBARLO

Ldapsearch -LL -x -b “uid=nombreusuario,ou=grupo,dc=acmé,dc=com”

PARA CAMBIAR ALGUN DATO (Ejemplo borrar mail)

CREAR UN ARCHIVO DE MODIFICACION

```
pc205@debian205Cristian: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
dn: uid=coyote,ou=usuarios,dc=acme,dc=com
changetype: modify
delete: mail
~
```

```
root@debian205Cristian:~# ldapmodify -x -W -D cn=admin,dc=acme,dc=com -f modific
acion.ldif
Enter LDAP Password:
modifying entry "uid=coyote,ou=usuarios,dc=acme,dc=com"
```

SLAPCAT

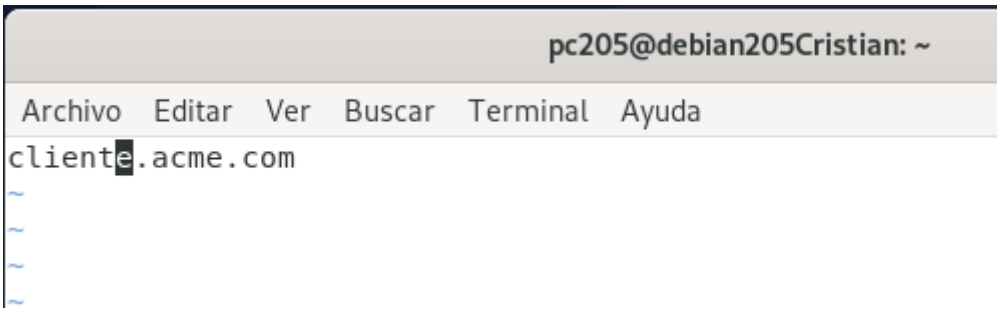
```
dn: uid=coyote,ou=usuarios,dc=acme,dc=com
objectClass: top
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: coyote
sn: looney
givenName: coyote
cn: coyote looney
uidNumber: 7001
gidNumber: 7000
userPassword:: e01ENX0rQU10WEs0OTRnL095SWZ6bGV5YWFnPT0=
homeDirectory: /home/coyote
loginShell: /bin/bash
structuralObjectClass: inetOrgPerson
entryUUID: 55984e46-d342-103a-80e4-fbcc5e1f5887
creatorsName: cn=admin,dc=acme,dc=com
createTimestamp: 20201215165718Z
entryCSN: 20201215170417.038071Z#000000#000#000000
modifiersName: cn=admin,dc=acme,dc=com
modifyTimestamp: 20201215170417Z

root@debian205Cristian:~#
```

CONFIGURACIÓN PARA ACCEDER DESDE OTRA MÁQUINA

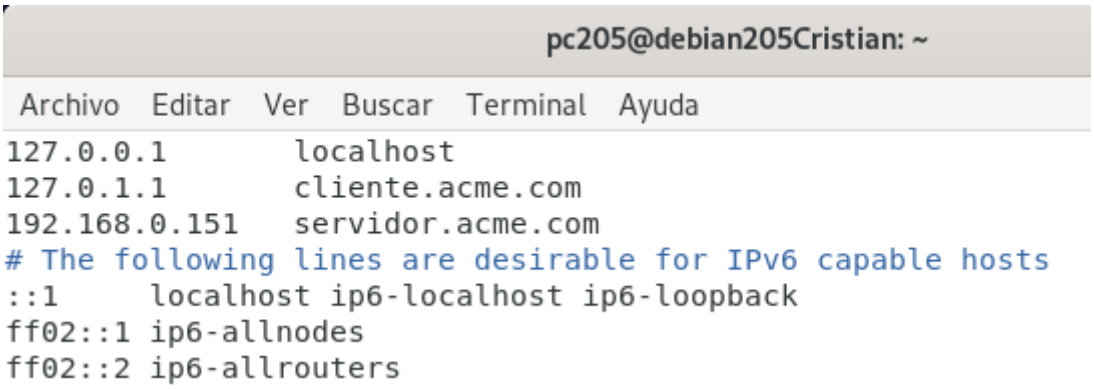
```
pc205@debian205Cristian: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@debian205Cristian:/home# ls
lost+found  pc205
root@debian205Cristian:/home# mkdir coyote
root@debian205Cristian:/home# cp /etc/skel/.* /home/coyote
cp: -r not specified; omitting directory '/etc/skel/.'
cp: -r not specified; omitting directory '/etc/skel/..'
root@debian205Cristian:/home# chown -R 7001:7000 /home/coyote
```

CLIENTE

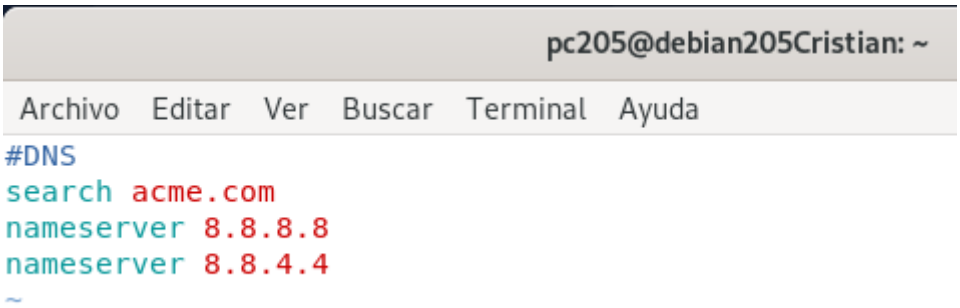
/etc/hostname



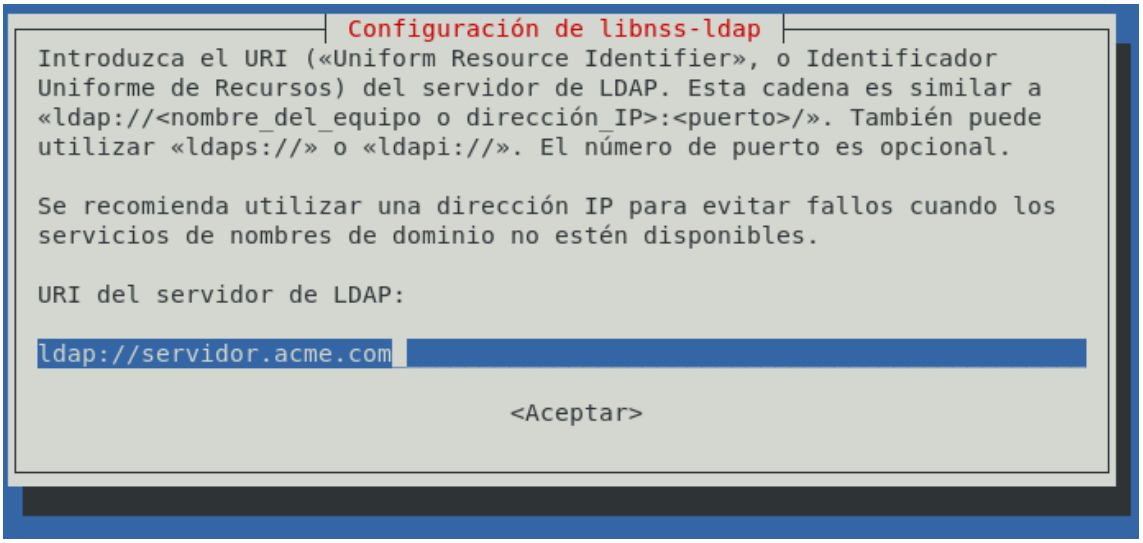
/etc/hosts

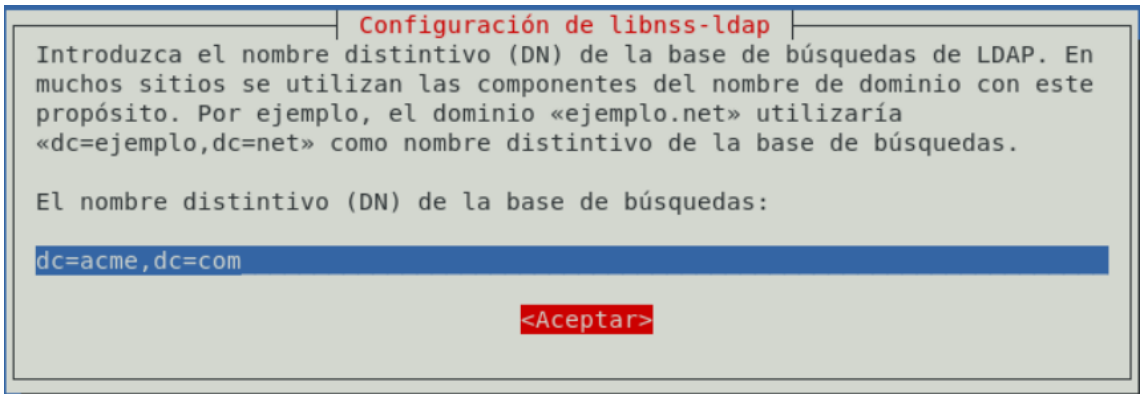


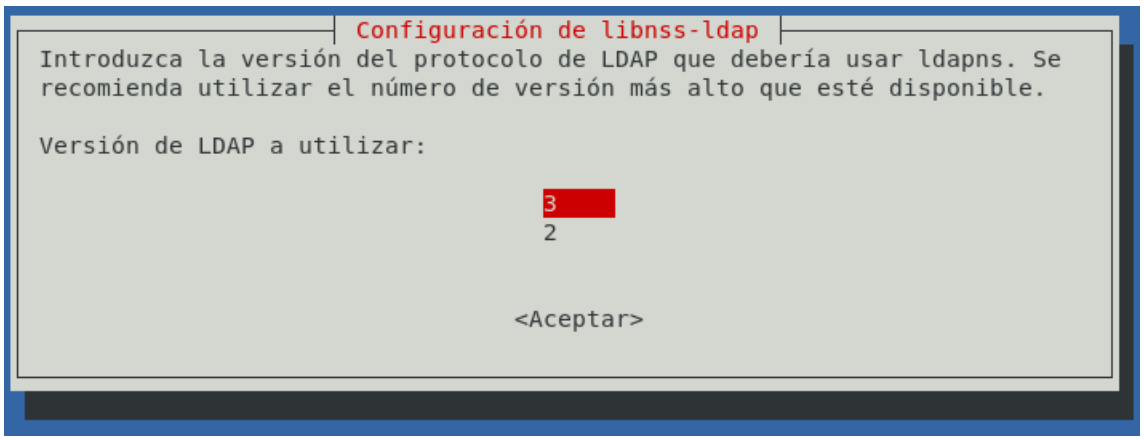
/etc/resolv.conf

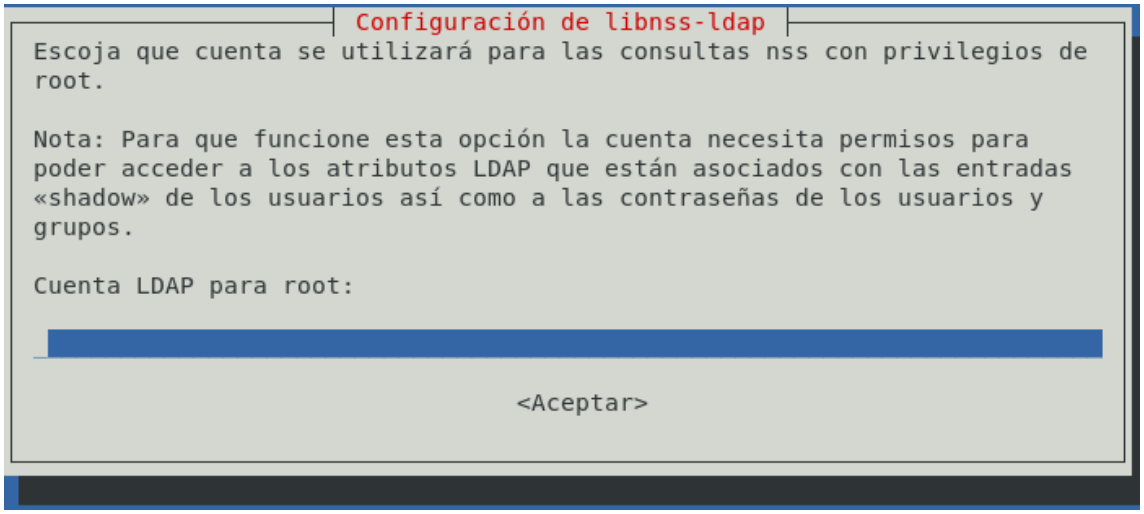


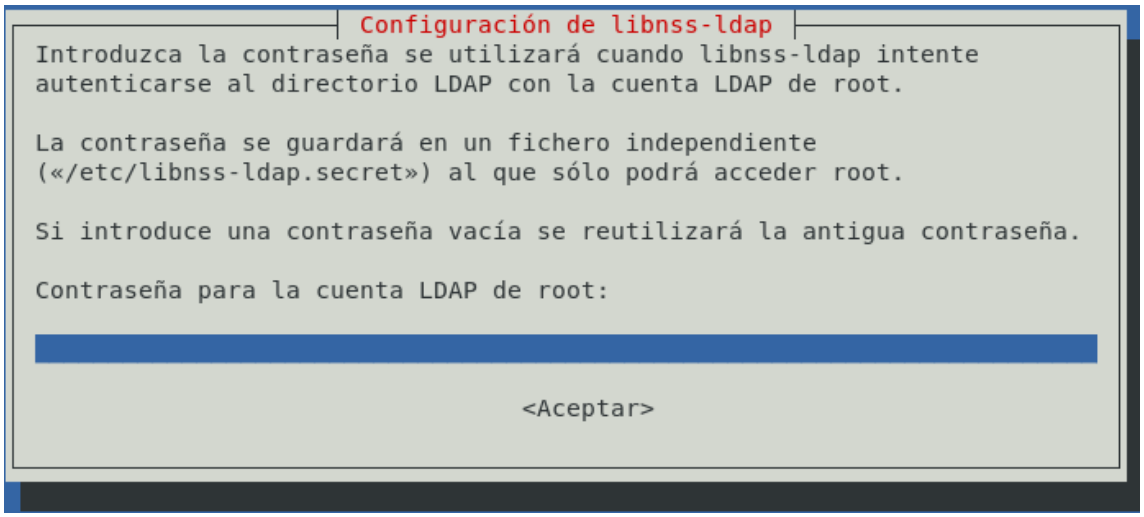

```
apt-get install libnss-ldap libpam-ldap nscd
```

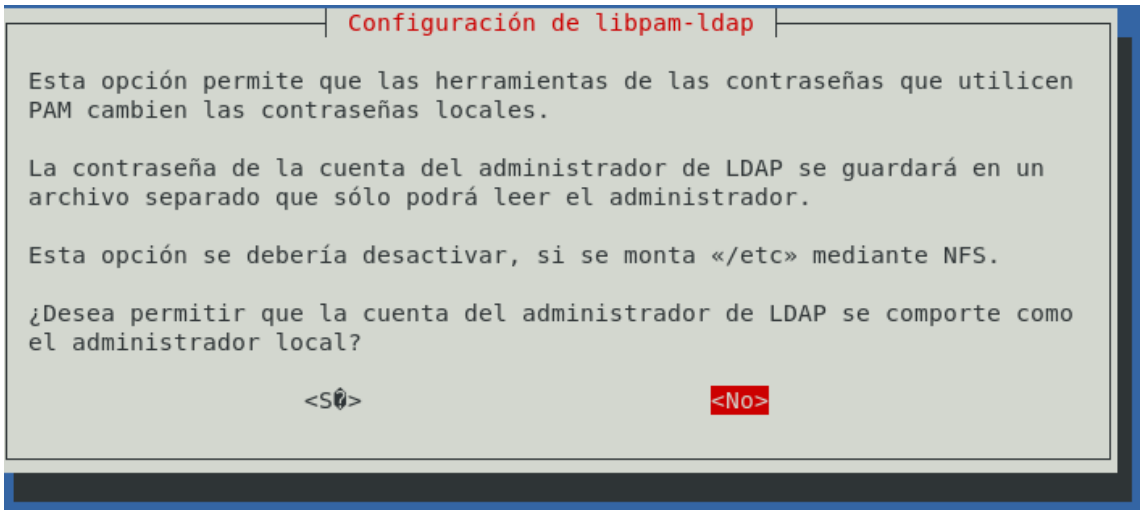


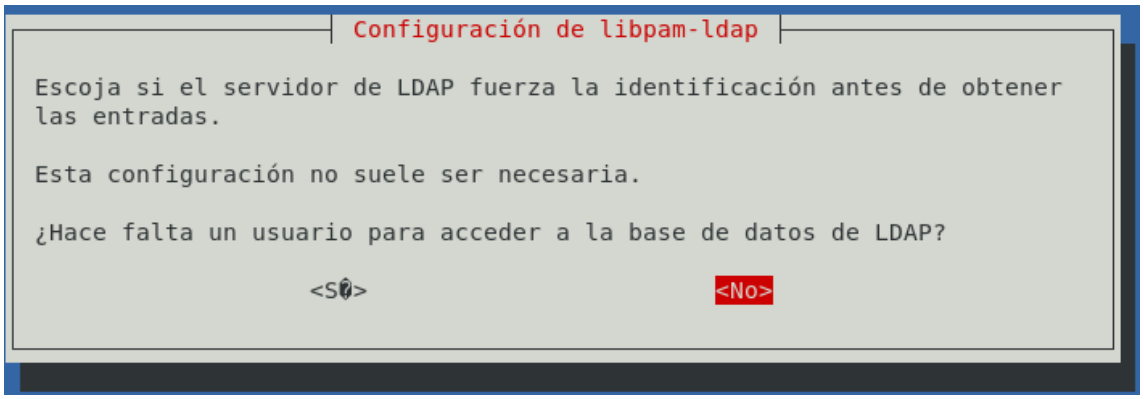

Configuración de libnss-ldap
Introduzca el nombre distintivo (DN) de la base de búsquedas de LDAP. En muchos sitios se utilizan las componentes del nombre de dominio con este propósito. Por ejemplo, el dominio «ejemplo.net» utilizaría «dc=ejemplo,dc=net» como nombre distintivo de la base de búsquedas.
El nombre distintivo (DN) de la base de búsquedas:
dc=acme,dc=com
<Aceptar>


Configuración de libnss-ldap
Introduzca la versión del protocolo de LDAP que debería usar ldapns. Se recomienda utilizar el número de versión más alto que esté disponible.
Versión de LDAP a utilizar:
3
2
<Aceptar>

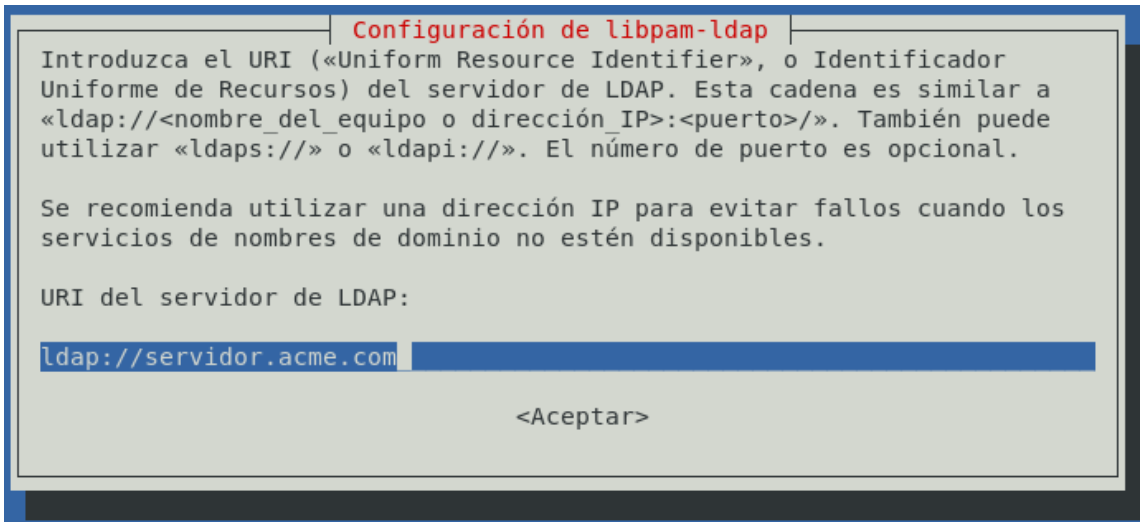

Configuración de libnss-ldap
Escoja que cuenta se utilizará para las consultas nss con privilegios de root.
Nota: Para que funcione esta opción la cuenta necesita permisos para poder acceder a los atributos LDAP que están asociados con las entradas «shadow» de los usuarios así como a las contraseñas de los usuarios y grupos.
Cuenta LDAP para root:
<Aceptar>

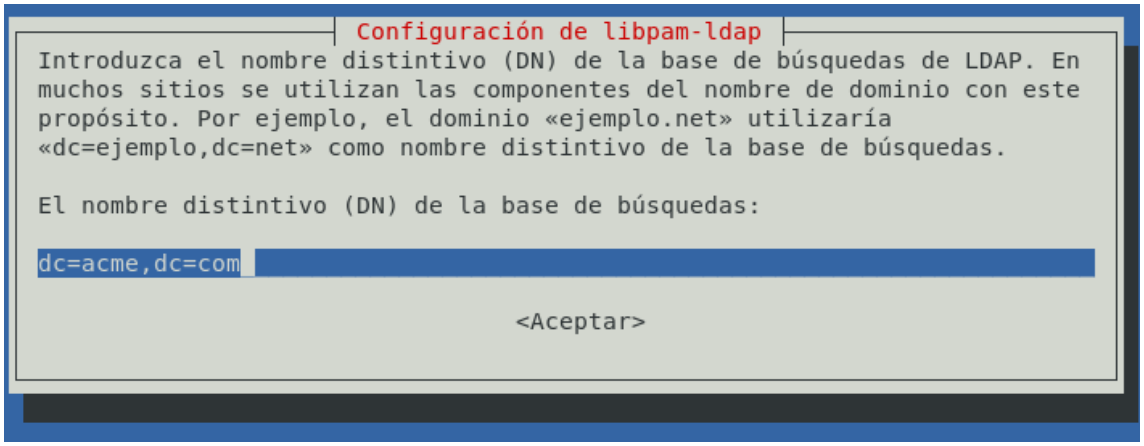


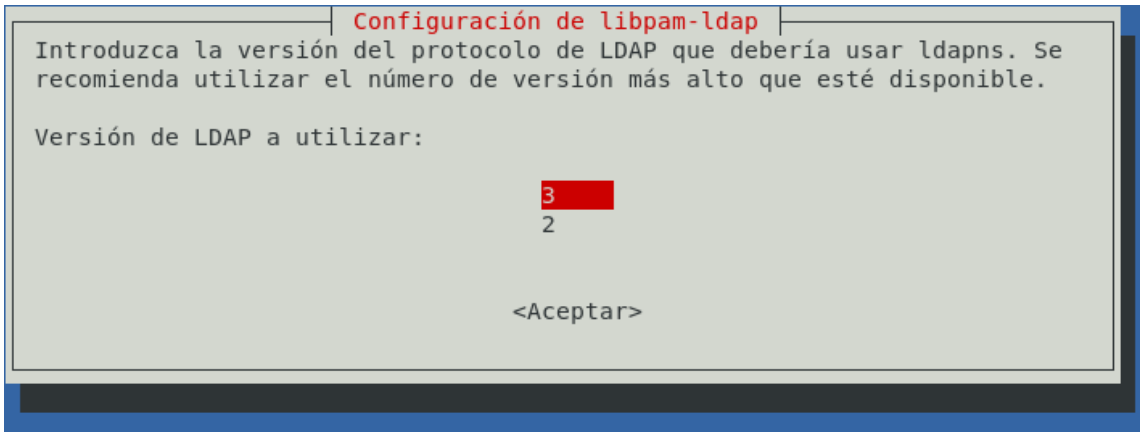


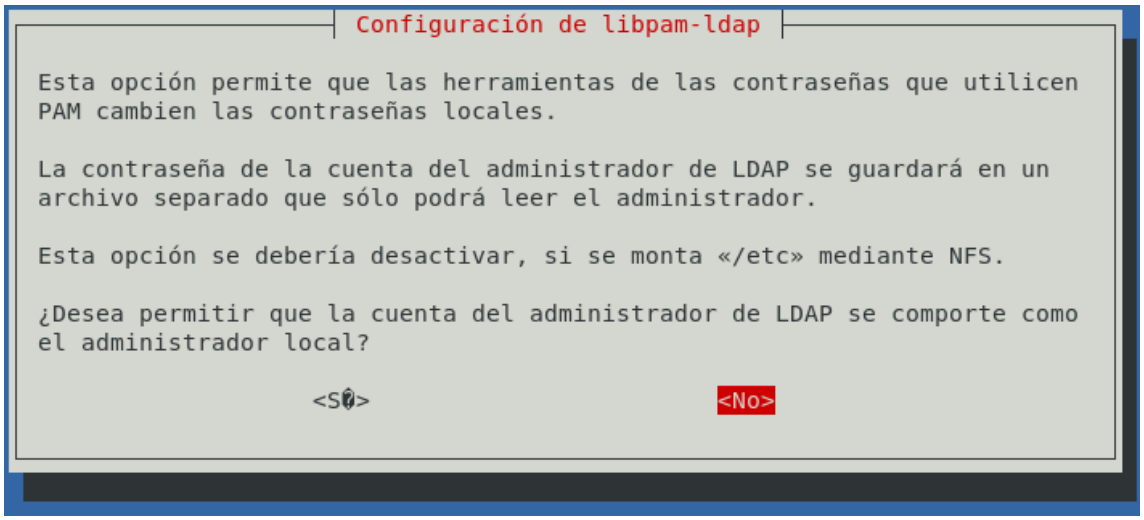


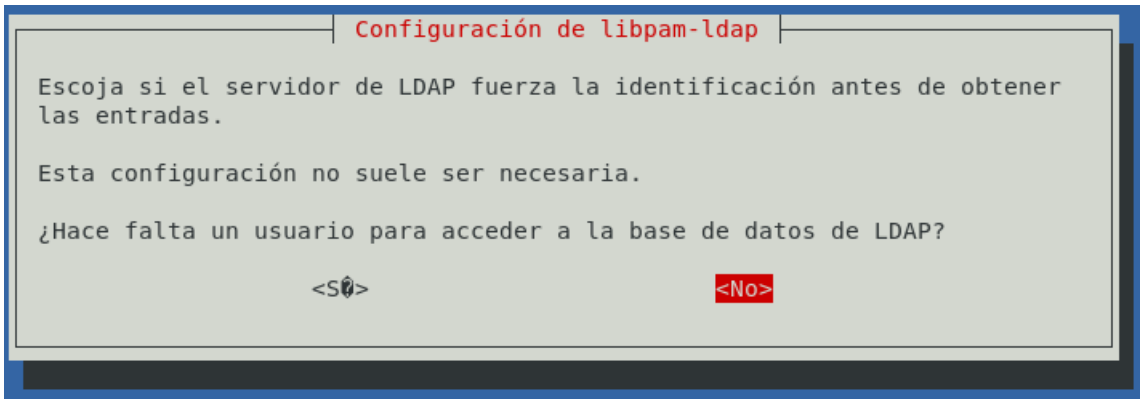
Dpkg-reconfigure libpam-ldap

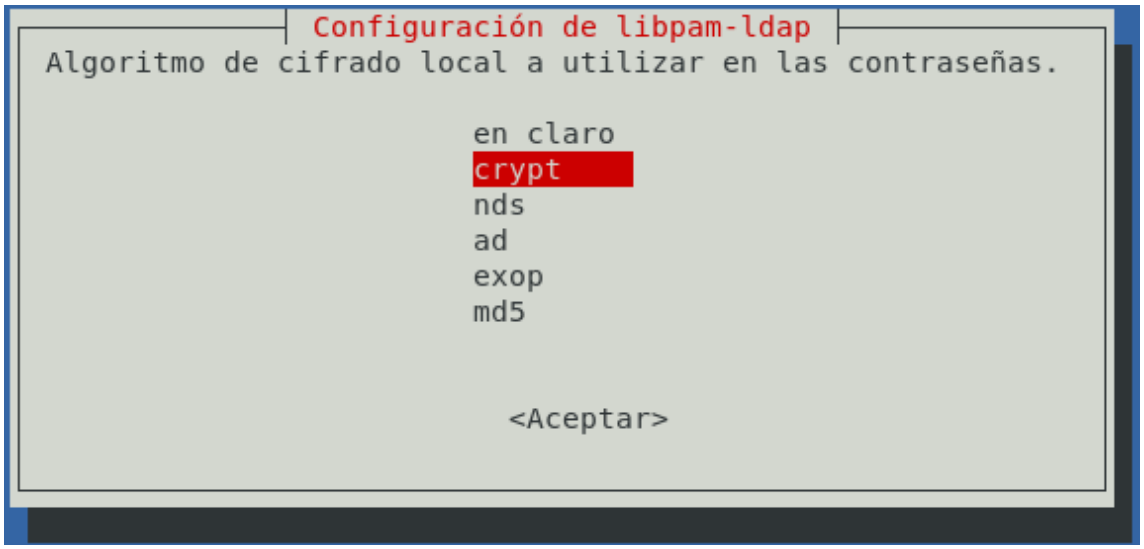

Configuración de libpam-ldap
Introduzca el URI («Uniform Resource Identifier», o Identificador Uniforme de Recursos) del servidor de LDAP. Esta cadena es similar a «ldap://<nombre_del_equipo o dirección_IP>:<puerto>/». También puede utilizar «ldaps://» o «ldapi://». El número de puerto es opcional.
Se recomienda utilizar una dirección IP para evitar fallos cuando los servicios de nombres de dominio no estén disponibles.
URI del servidor de LDAP:
ldap://servidor.acme.com
<Aceptar>

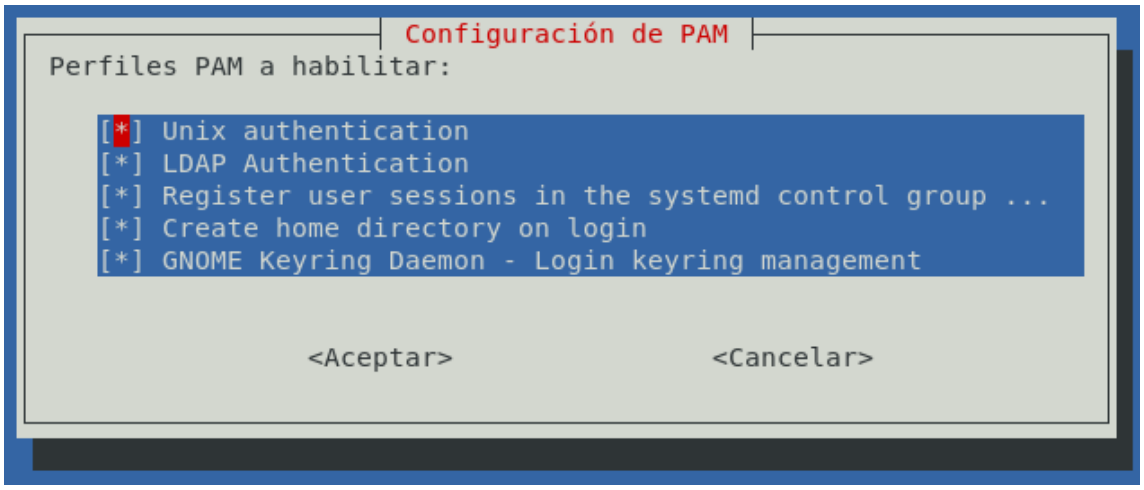

Configuración de libpam-ldap
Introduzca el nombre distintivo (DN) de la base de búsquedas de LDAP. En muchos sitios se utilizan las componentes del nombre de dominio con este propósito. Por ejemplo, el dominio «ejemplo.net» utilizaría «dc=ejemplo,dc=net» como nombre distintivo de la base de búsquedas.
El nombre distintivo (DN) de la base de búsquedas:
dc=acme,dc=com
<Aceptar>


Configuración de libpam-ldap
Introduzca la versión del protocolo de LDAP que debería usar ldapns. Se recomienda utilizar el número de versión más alto que esté disponible.
Versión de LDAP a utilizar:
3
2
<Aceptar>


Configuración de libpam-ldap
Esta opción permite que las herramientas de las contraseñas que utilicen PAM cambien las contraseñas locales.
La contraseña de la cuenta del administrador de LDAP se guardará en un archivo separado que sólo podrá leer el administrador.
Esta opción se debería desactivar, si se monta «/etc» mediante NFS.
¿Desea permitir que la cuenta del administrador de LDAP se comporte como el administrador local?
<S>
<No>


Configuración de libpam-ldap
Escoja si el servidor de LDAP fuerza la identificación antes de obtener las entradas.
Esta configuración no suele ser necesaria.
¿Hace falta un usuario para acceder a la base de datos de LDAP?
<S>
<No>


Configuración de libpam-ldap
Algoritmo de cifrado local a utilizar en las contraseñas.
en claro
crypt
nds
ad
exop
md5
<Aceptar>



/etc/ldap/ldap.conf

```
pc205@debian205Cristian: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE   dc=example,dc=com
#URI    ldap://ldap.example.com ldap://ldap-master.example.c

BASE    dc=acme,dc=com
URI     ldap://servidor.acme.com

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
TLS_CACERT      /etc/ssl/certs/ca-certificates.crt

~
~
~
"/etc/ldap/ldap.conf" 20L, 382C escritos
```

/etc/nsswitch.conf

```
pc205@debian205Cristian: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages insta
# `info libc "Name Service Switch"' for information about this fi

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

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

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

netgroup:       nis
~
~
~
"/etc/nsswitch.conf" 20L, 559C escritos                       13,
```

```
root@debian205Cristian:~# systemctl restart nscd
root@debian205Cristian:~# systemctl status nscd
● nscd.service - Name Service Cache Daemon
   Loaded: loaded (/lib/systemd/system/nscd.service; enabled; vendor preset: ena
   Active: active (running) since Tue 2020-12-15 19:24:26 CET; 4s ago
  Process: 2915 ExecStart=/usr/sbin/nscd (code=exited, status=0/SUCCESS)
 Main PID: 2916 (nscd)
    Tasks: 11 (limit: 9494)
   Memory: 1.7M
   CGroup: /system.slice/nscd.service
           └─2916 /usr/sbin/nscd
```

REINICIAR CLIENTE

PARA AÑADIR UN CLIENTE

```
root@servidor:~# ldapadd -x -W -D cn=admin,dc=acme,dc=com -f bugs.ldif
Enter LDAP Password:
adding new entry "uid=bugs,ou=usuarios,dc=acme,dc=com"
```