Manual de OpenLDAP

Nombre: Alejandro
Apellidos: Román Caballero
Curso: 2ASIR

ÍNDICE

Introducción **3**

SERVIDOR **4**

CLIENTE **6**

Introducción

OpenLDAP : Directorio activo de linux
Que mediante esto desde una máquina linux puedas iniciar sesion en otra máquina linux.

Necesario antes de empezar: bind9 configurado y instalado en la máquina servidor y la cliente tiene que tener de dns la máquina del servidor.

Instalarlo siguiendo documentación:
Los errores mirarlos aquí:

https://ldap.com/ldap-result-code-reference/

Pagina para documentarse:

https://www.youtube.com/watch?v=2yjhxGNbDjo

https://franbellido.wordpress.com/2010/11/30/creacion-de-usuarios-y-grupos-en-ldap/

SERVIDOR

Instalar servidor openldap con el siguiente comando:

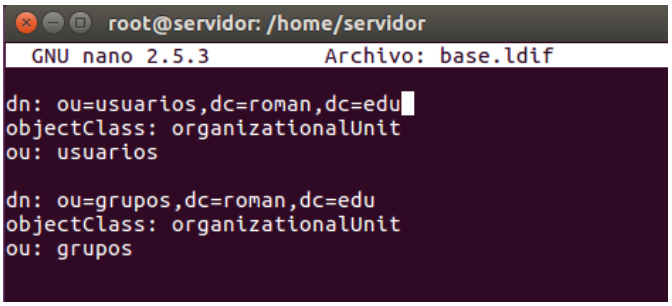
sudo apt-get install slapd ldap-utils -y

Una vez instalado pasaremos a crear los tres archivos de configuración para la creación de la unidad organizativa , los grupos y los usuarios de openldap.

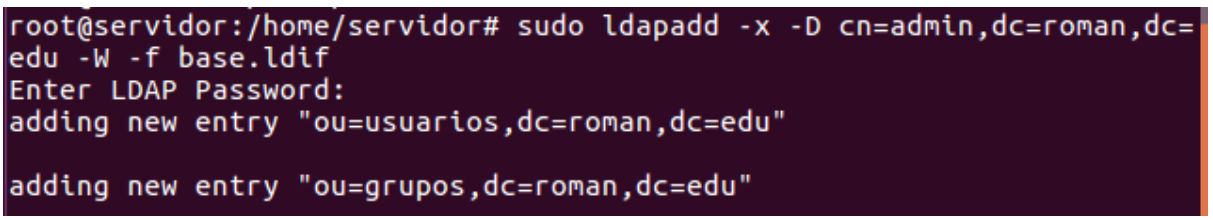
Creando las unidades organizativas
sudo nano base.ldif //Cuidado de no tener espacios al final de cada línea

dn: ou=usuarios,**dc=roman,dc=edu**
objectClass: organizationalUnit
ou: usuarios

dn: ou=grupos,**dc=roman,dc=edu**
objectClass: organizationalUnit
ou: grupos



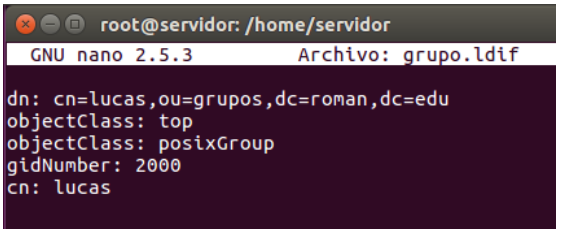
sudo ldapadd -x -D cn=admin,**dc=roman,dc=edu** -W -f base.ldif



Creación de los grupos del openldap

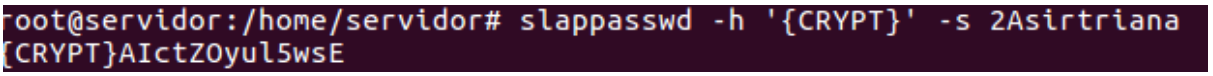
nano grupo.ldif

dn: **cn=lucas**,ou=grupos,**dc=roman,dc=edu**
objectClass: top
objectClass: posixGroup
gidNumber: 2000
cn: lucas



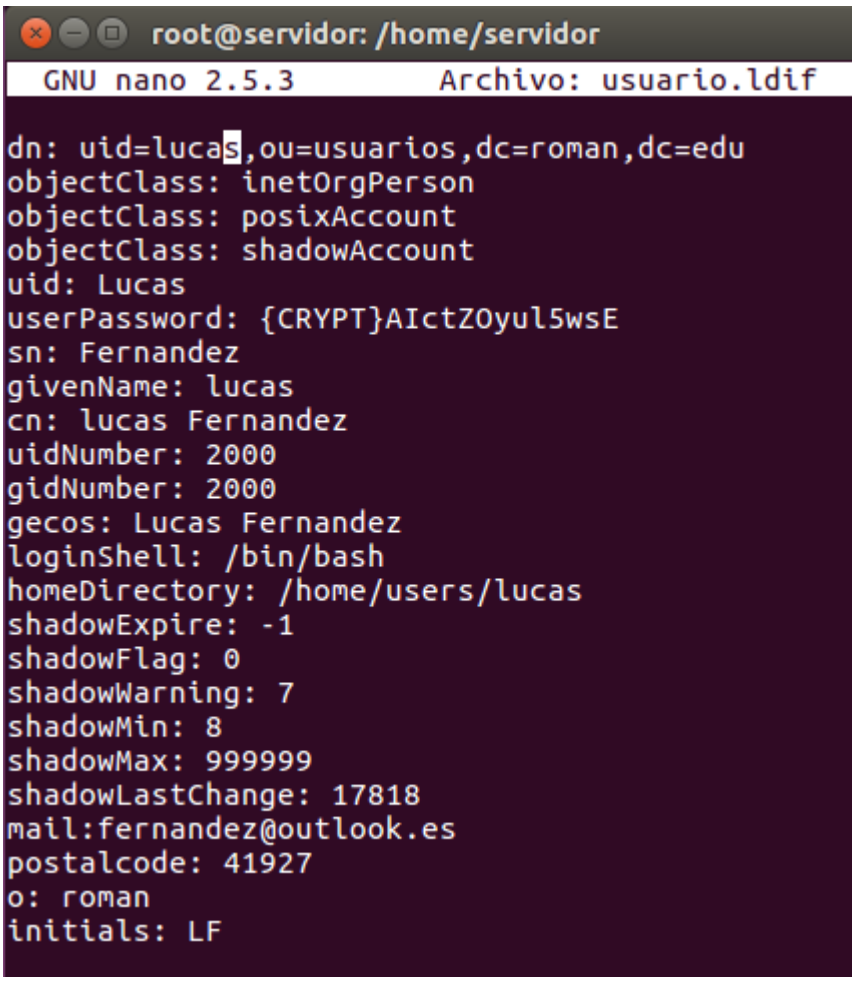
ldapadd -x -D cn=admin,**dc=roman,dc=edu** -W -f grupo.ldif

Para poner el userPassword: crear la contraseña con :
slappasswd -h '{CRYPT}' -s contraseña_que_queremos_crear
Ejemplo slappasswd -h '{CRYPT}' -s 2Asirtriana
{CRYPT}AIctZOyul5wsE

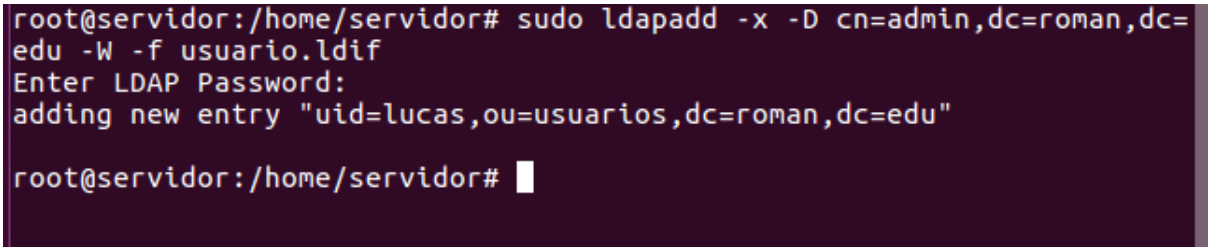


sudo nano usuario.ldif

dn: **uid=lucas**,ou=usuarios,**dc=roman,dc=edu**
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: Lucas
userPassword: **{CRYPT}AIctZOyul5wsE**
sn: Fernandez
givenName: lucas
cn: lucas Fernandez
uidNumber: **2000**
gidNumber: **2000**
gecos: Lucas Fernandez
loginShell: /bin/bash
homeDirectory: /home/users/lucas
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 17818
mail:**fernandez@outlook.es**
postalcode: **41927**
o: **roman**
initials: **LF**



sudo ldapadd -x -D cn=admin,**dc=roman,dc=edu** -W -f usuario.ldif



CLIENTE

En el cliente hacer lo siguiente:
sudo update
sudo apt-get install libnss-ldap libpam-ldap ldap-utils -y

primera imagen: **ldap://ip_del_servidor openldap**
segunda imagen: **dc=roman,dc=edu**
tercera imagen: **3**
cuarta imagen: **si**
quinta imagen: **no**
sexta imagen: **cn=admin,dc=roman,dc=edu**
séptima: contraseña: **contraseña del servidor openldap**

sudo nano /etc/nsswitch.conf

```
passwd:         compat ldap
group:          compat ldap
shadow:         compat ldap
```

sudo nano /etc/pam.d/common-password
En la línea 26 del fichero dejar linea asi(borrando el user_authtok):
password [success=1 **user_unknown**=ignore default=die] pam_ldap.so try_first_pass

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

añadir esta linea al final del fichero:

session optional pam_mkhomedir.so skel=/etc/skel umask=007

```
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_mkhomedir.so skel=/etc/skel umask=007
# end of pam-auth-update config
```

sudo apt install sysv-rc-conf
sudo sysv-rc-conf libnss-ldap on

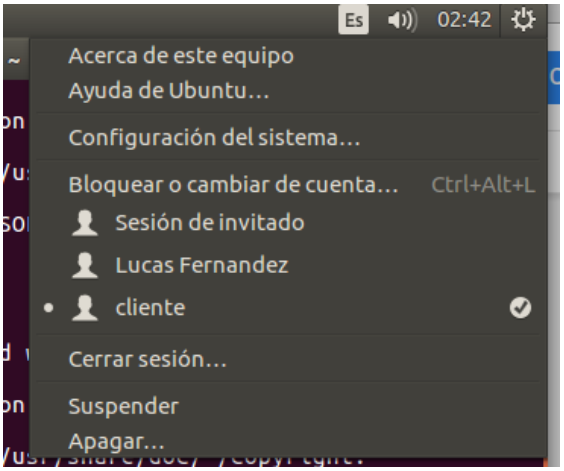
Por último un **init 6**

Y hacemos la prueba de que funciona haciendo login en el cliente en un directorio activo del servidor openldap.

```
The programs included with the Ubuntu system are free softw
are;
the exact distribution terms for each program are described
 in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent per
mitted by
applicable law.

Creando directorio «/home/users/lucas».
Lucas@cliente:~$
```



##login remoto , que los cambios de la máquina cliente se refleja en la máquina real ubuntu