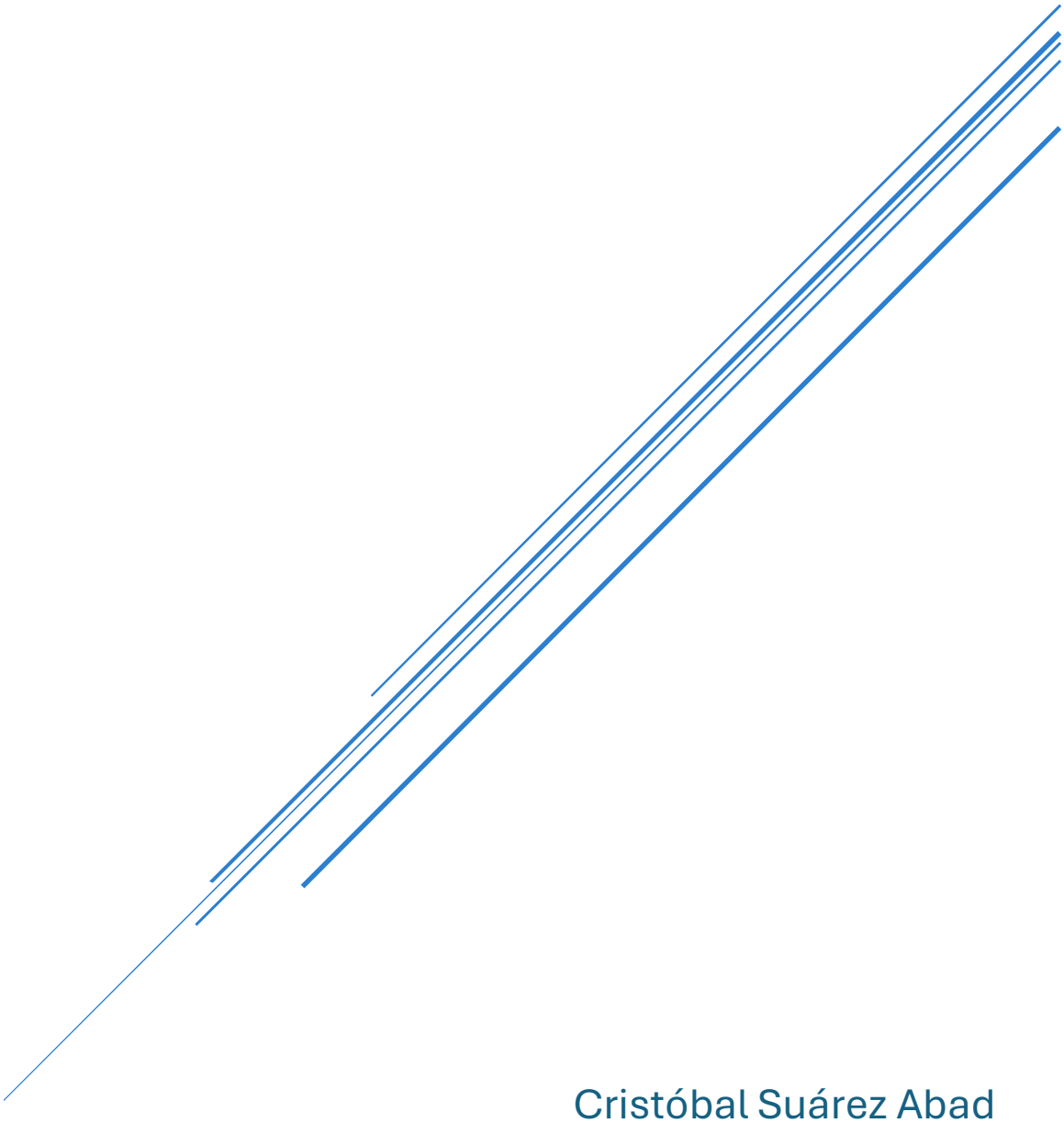
OPENLDAP (LINUX)



Cristóbal Suárez Abad

Administración de Sistemas Operativos – 2º ASIR

Índice:

0)Introducción:

1. Instalación y configuración del servidor y cliente LDAP.
2. Administración de usuarios, grupos y unidades organizativas.
3. Uso de herramientas gráficas como LDAP Account Manager y Apache Directory Studio.
4. Búsquedas y modificaciones dentro del árbol LDAP.
5. Operaciones avanzadas como gestión de atributos, eliminación, cambios de UID, etc.

1. Instalación del Servidor LDAP:

a) Instala en una máquina virtual Linux Server (con una distribución de tu elección) el servidor **OpenLDAP**. El dominio del directorio debe ser: APELLIDO1.apellido2, sin acentos ni eñes.

Lo primero que debemos hacer, como con todo servidor que vayamos a configurar es poner la IP estática.

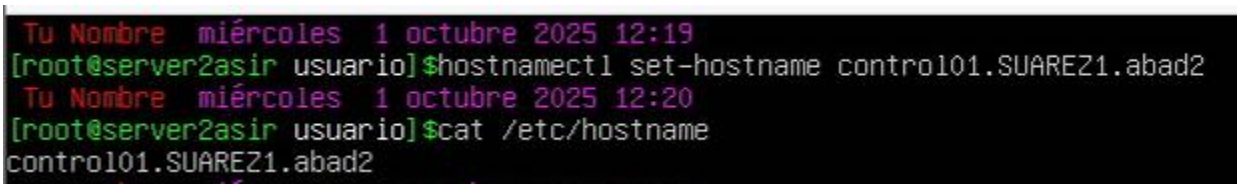
```
 Tu Nombre  miércoles  1 octubre 2025 12:14
[root@server2asir usuario]$nano /etc/netplan/00-installer-config.yaml _
```

```
  GNU nano 6.2
# This is the network config written by 'subiquity'
network:
  ethernets:
  version: 2
    ens18:
#       dhcp4: true
      addresses:
        - 10.2.17.10/24
      routes:
        - to: 0.0.0.0/0
          via: 10.2.17.1
      nameservers:
          search: [google]
          addresses: [8.8.8.8]
```

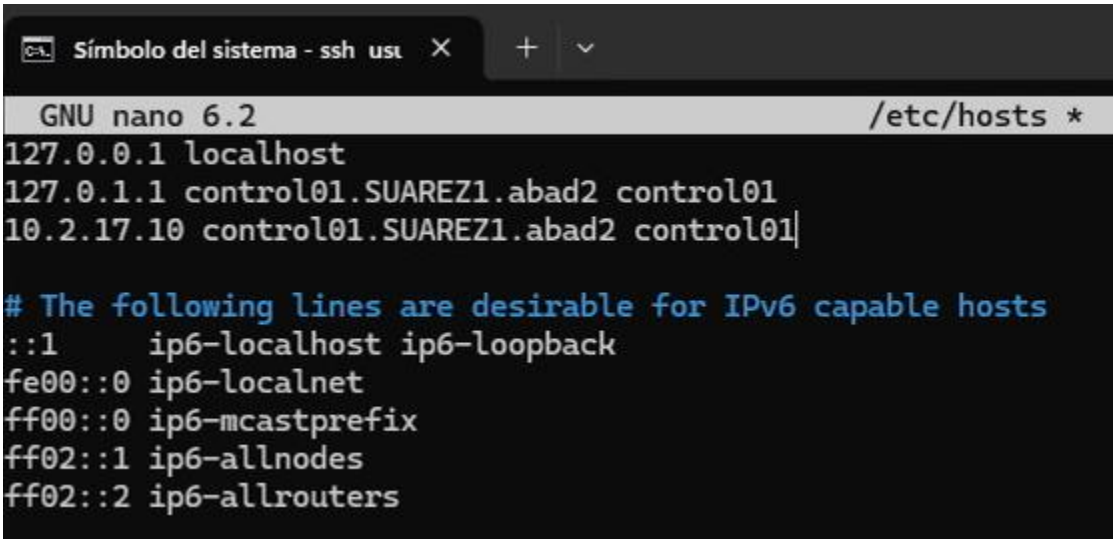
```
[root@server2asir usuario]$ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:1e:85:34 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 10.2.17.10/24 brd 10.2.17.255 scope global ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe1e:8534/64 scope link
       valid_lft forever preferred_lft forever
 Tu Nombre  miércoles  1 octubre 2025 12:18
```

Cambiamos el nombre del host:

Usamos **hostnamectl set-hostname “NombreEquipo.DOMINIO”**



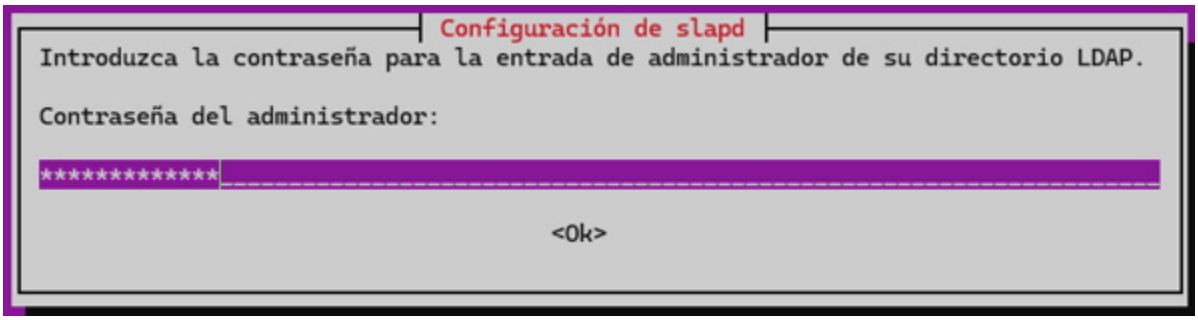
Ahora configuramos el archivo **hosts** para el DNS:

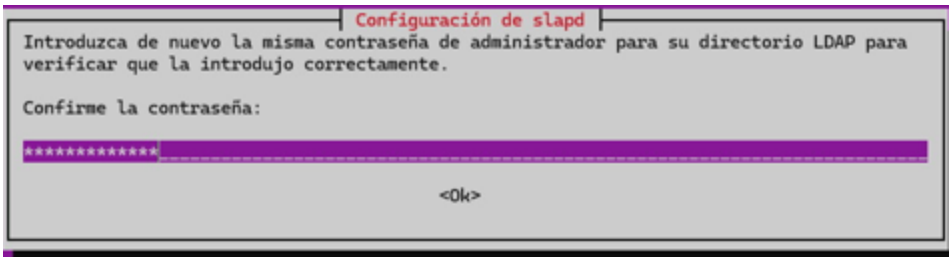


Ahora procedemos a instalar “lapd” en el equipo.

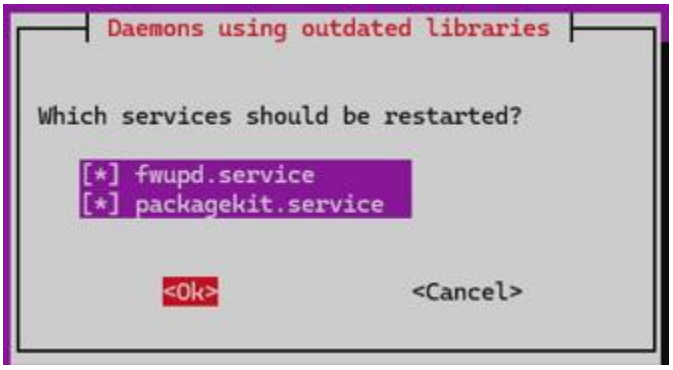
- “apt update”
- “sudo apt install slapd ldap-utils -y”

Introducimos contraseña y su confirmación.



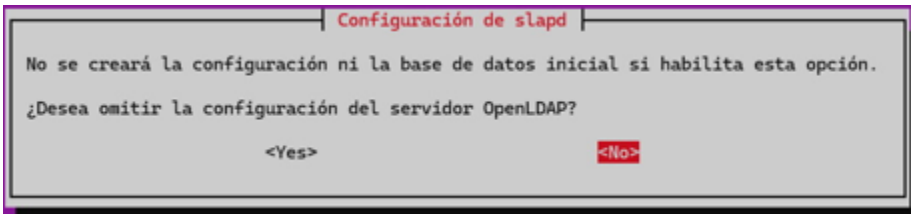


Nos pide reiniciar algunos servicios. Los reiniciamos todos.

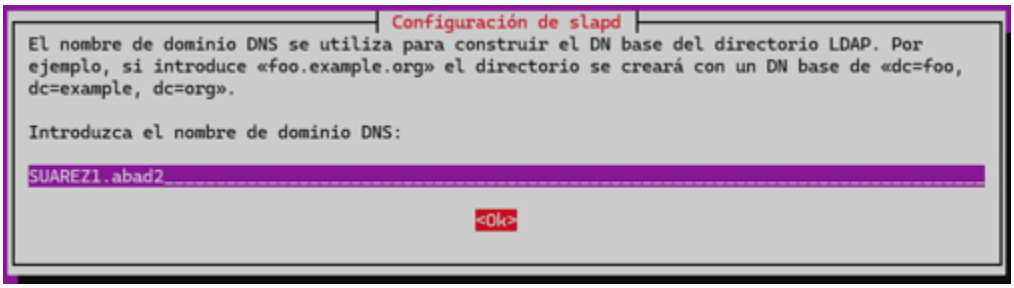


Una vez terminado, realizamos la configuración manual, la completa:

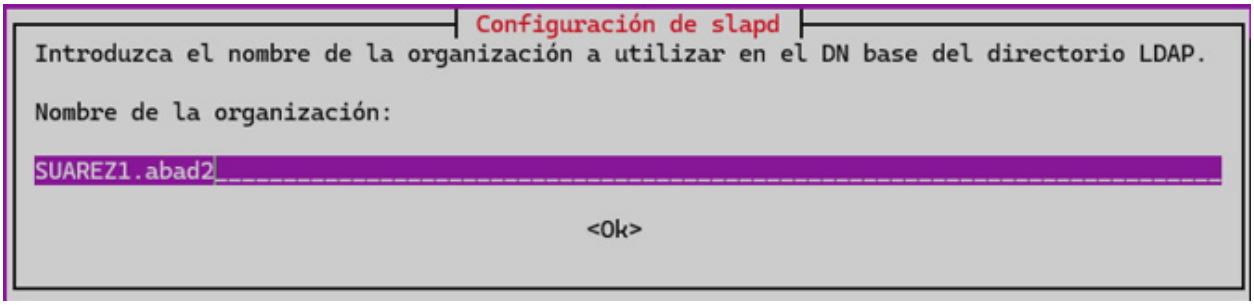
“**sudo dpkg-reconfigure slapd**”



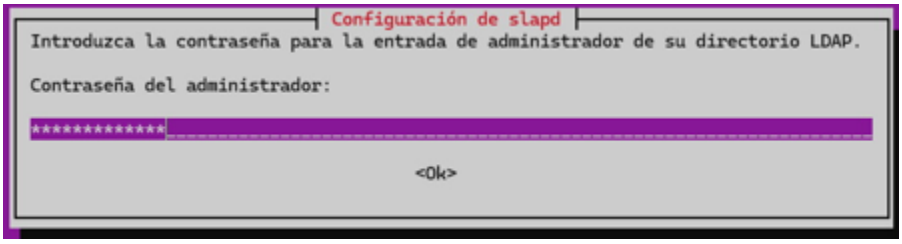
Establecemos el nombre del dominio.



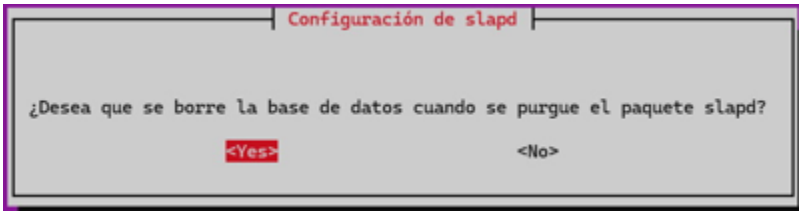
Nombre de la organización (lo mismo).



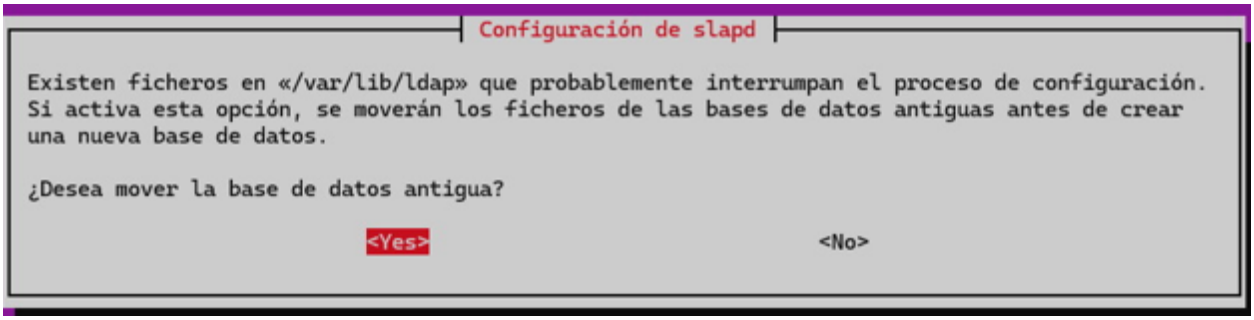
Contraseña del “admin” y luego otra vez se confirma.



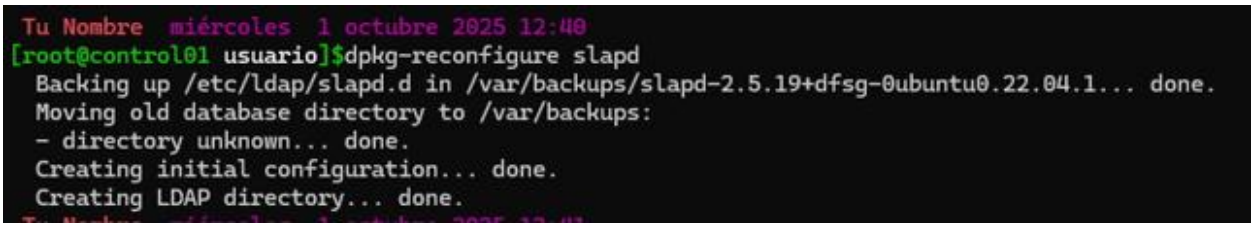
Borrar base de datos cuando se purgue el paquete slapd.



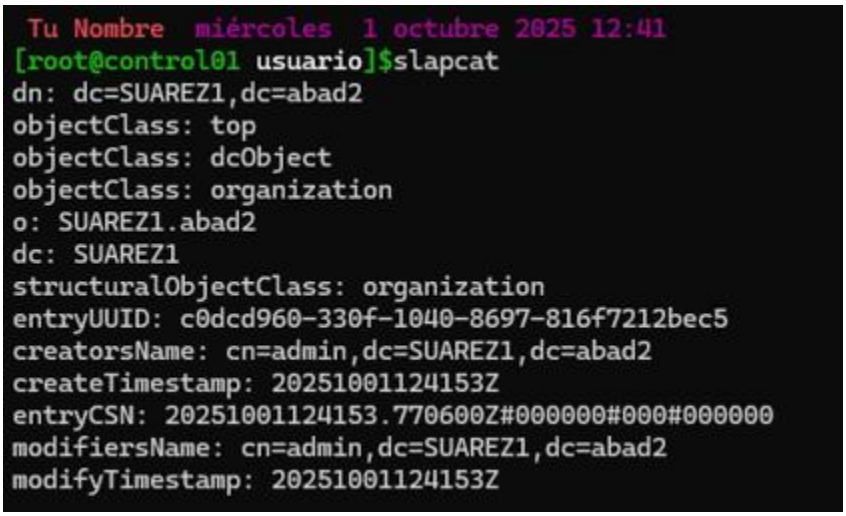
Mover base de datos antigua.



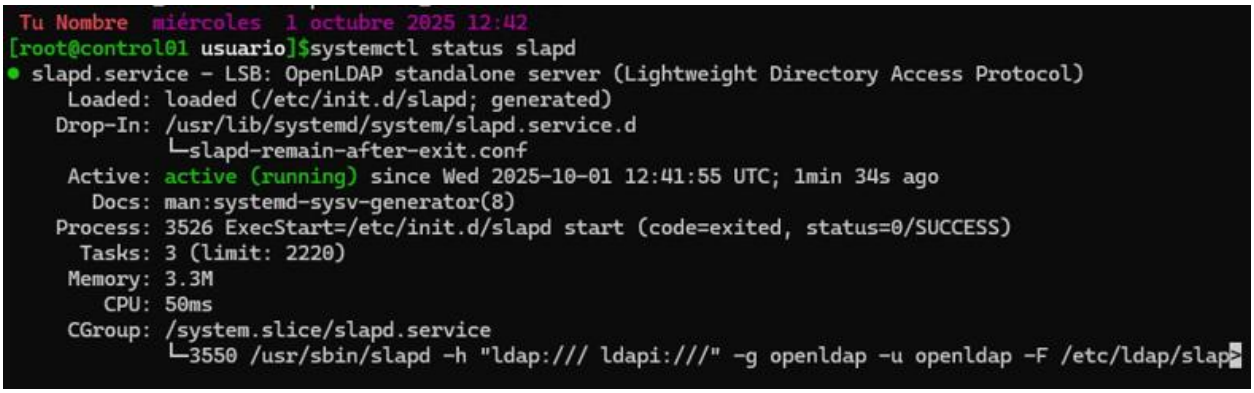
Todo bien.



Confirmación: “slapcat”.



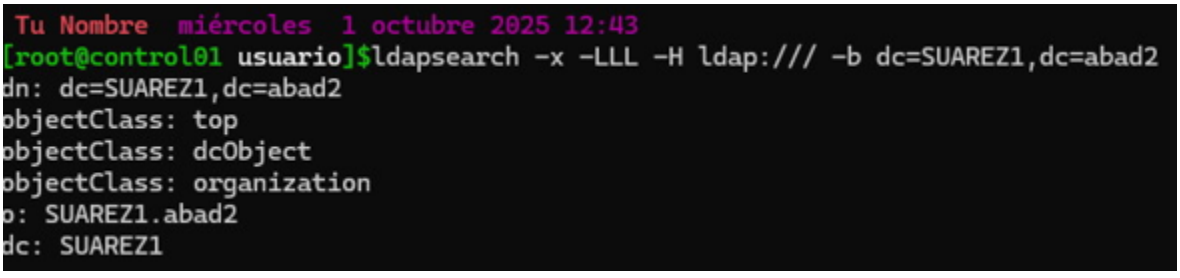
Otra confirmación: “systemctl status slapd”



b) Configura el servidor para que esté listo para aceptar conexiones LDAP.

Comandos de comprobación:

“**ldapsearch -x -LLL -H ldap:/// -b dc=SUAREZ1,dc=abad2**”



“ufw status”

“ufw allow 389/tcp”

“ss -tulpn | grep slapd”

2. Instalación de Herramienta de Administración Gráfica.

a) Instala LDAP Account Manager (LAM) en el servidor.

“apt update”

Primero hay que instalar Apache.

“sudo apt install apache2 php php-cgi libapache2-mod-php php-mbstring php-common php-pear -y”

```
 Tu Nombre  martes  7 octubre 2025 08:46
[usuario@control01 ~]$sudo apt install apache2 php php-cgi libapache2-mod-php php-mbstring php-common
php-pear -y
```

“sudo a2enconf php8.1-cgi”

“systemctl reload apache2”

```
usuario@control01 ~]$sudo a2enconf php8.1-cgi
nabling conf php8.1-cgi.
o activate the new configuration, you need to run:
 systemctl reload apache2
Tu Nombre  martes  7 octubre 2025 08:48
usuario@control01 ~]$systemctl reload apache2
=== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
uthentication is required to reload 'apache2.service'.
uthenticating as: usuario
assword:
=== AUTHENTICATION COMPLETE ===
Tu Nombre  martes  7 octubre 2025 08:48
usuario@control01 ~]$systemctl status apache2
 apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2025-10-07 08:47:41 UTC; 1min 31s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 13847 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Process: 14035 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=0/SUCCESS)
   Main PID: 13851 (apache2)
      Tasks: 6 (limit: 2220)
     Memory: 10.9M
        CPU: 359ms
```

Ahora instalamos **LDAP Account Manager.**

“sudo apt install ldap-account-manager -y”

```
 Tu Nombre  martes  7 octubre 2025 08:49
[usuario@control01 ~]$sudo apt install ldap-account-manager -y
```

Para restringir el acceso solo a los equipos de la red local debemos configurar un archivo:

sudo nano /etc/apache2/conf-enabled/ldap-account-manager.conf

En vez de “**Require all granted**”

Debemos poner “**Require ip 127.0.0.1 IP/CIDR**”

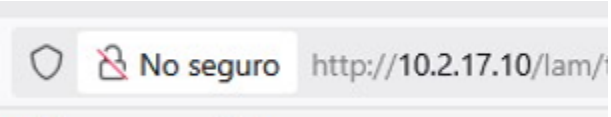
Ejemplo: “**Require ip 127.0.0.1 192.168.1.0/24**”

Para esta práctica se ha dejado como viene por defecto.

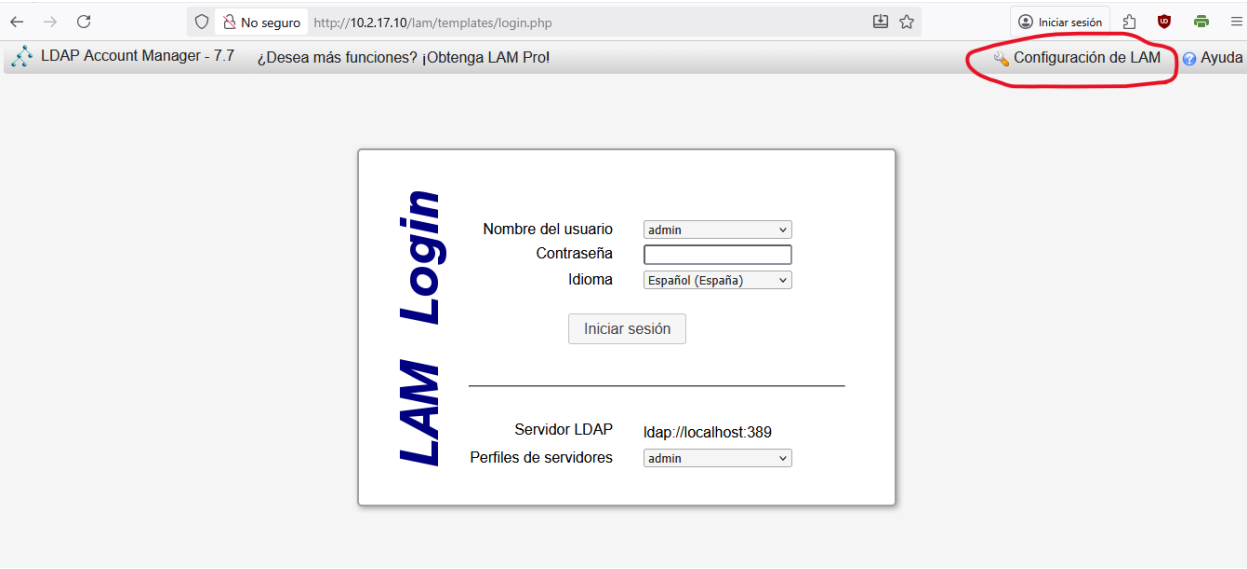
```
 GNU nano 6.2                /etc/apache2/conf-enabled/ldap-account-manager.conf

Alias /lam /usr/share/ldap-account-manager

<Directory /usr/share/ldap-account-manager>
  Options +FollowSymLinks
  AllowOverride All
  Require all granted
  DirectoryIndex index.html
</Directory>
```

b) Configura LAM para conectarse correctamente al dominio recién creado.

Ahora podemos acceder a LAM desde el navegador, para ello ponemos en la barra de búsqueda: “http://IP_SERVIDOR/lam”

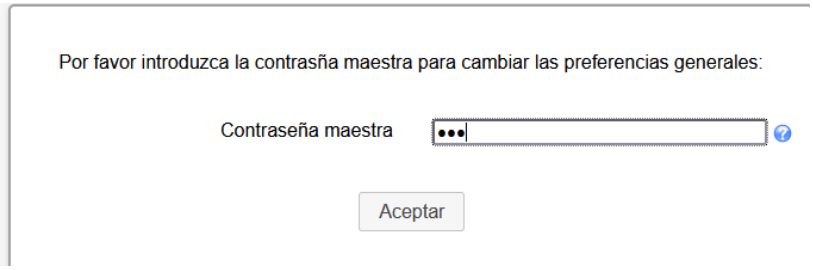


Ahora debemos ir a “Configuración LAM”



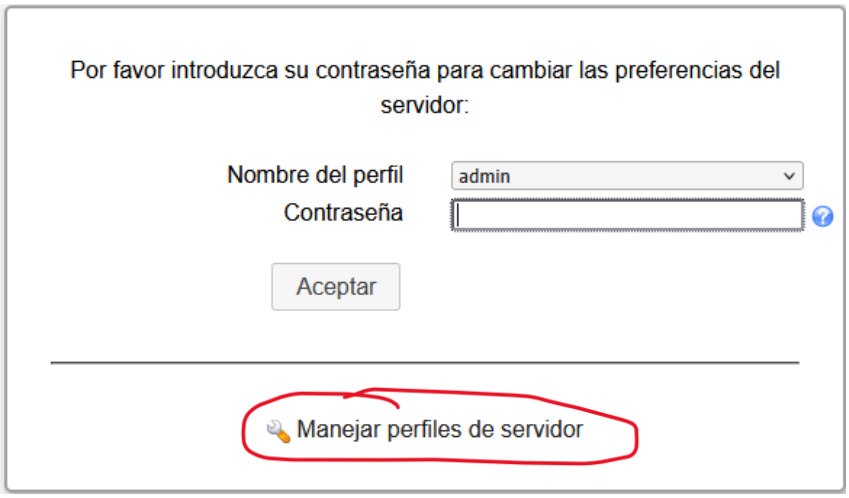
Elegimos “Editar los Ajustes Generales”

La contraseña maestra por defecto es “lam”, en el siguiente panel podremos modificarla.

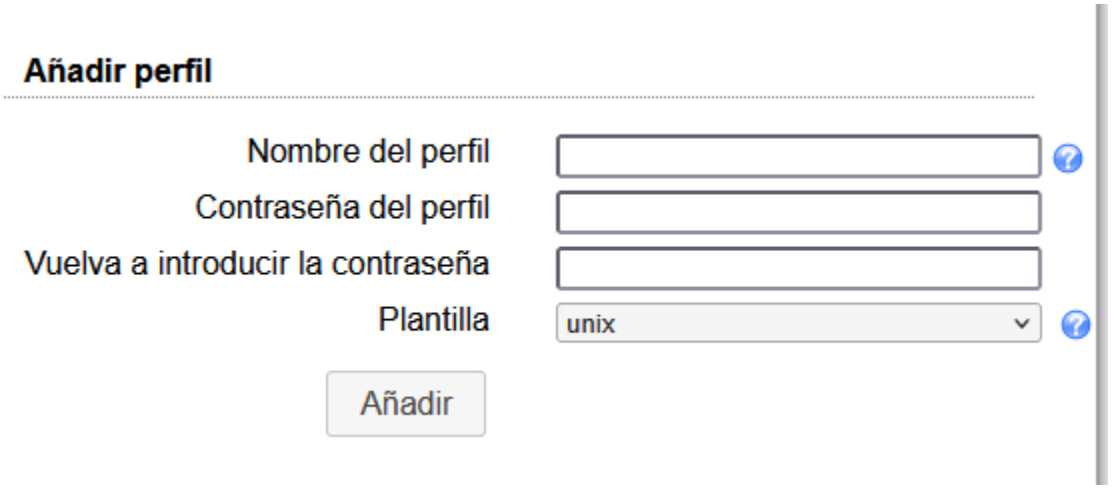


En la siguiente ventana tenemos opciones de Seguridad (limitar IPs de los equipos que se pueden conectar, pedir certificados de SSL, etc), Políticas de Contraseñas, de Inicios de Sesión y también podemos modificar la contraseña que hemos mencionado antes.

Volvemos al panel precio y vamos a “Editar perfiles del servidor”. Y aquí debemos pulsar en “Manejar perfiles de servidor”.

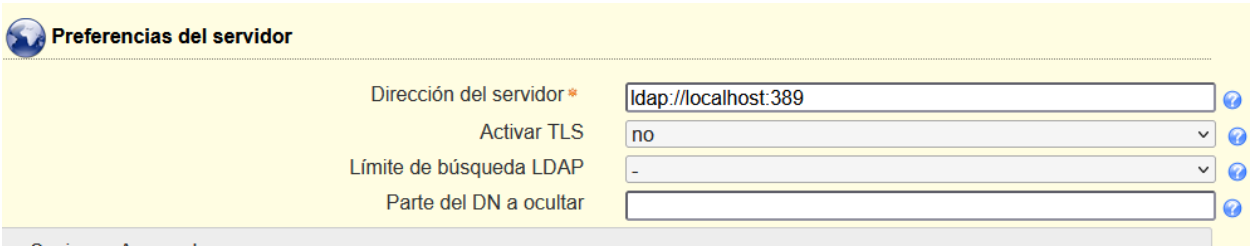


Aquí debemos añadir un perfil, en nuestro caso “admin” y la contraseña la que queramos. Una vez creado. En el panel previo entramos con el perfil recién creado.



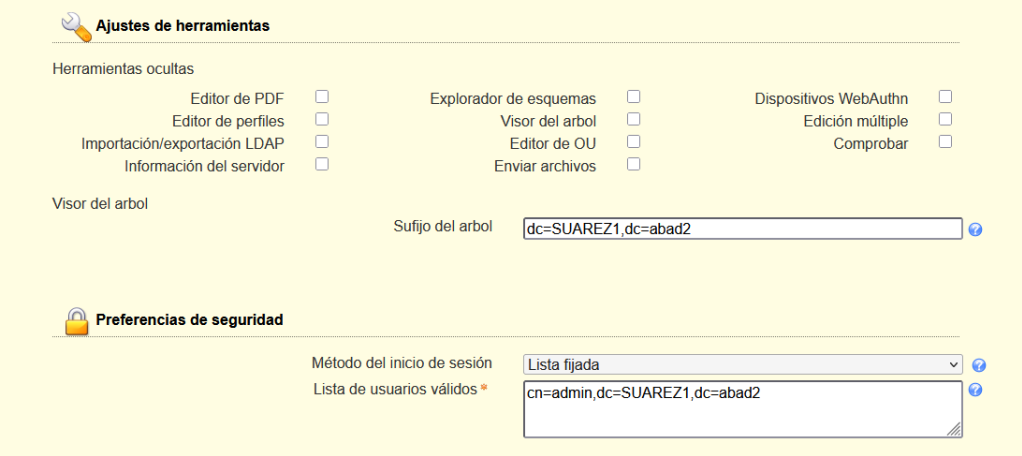
Las principales configuraciones que debemos hacer en “Ajustes Generales:

Dirección del servidor. Como “LAM” está instalado en el mismo servidor, pues se pone “localhost” más el puerto 389.

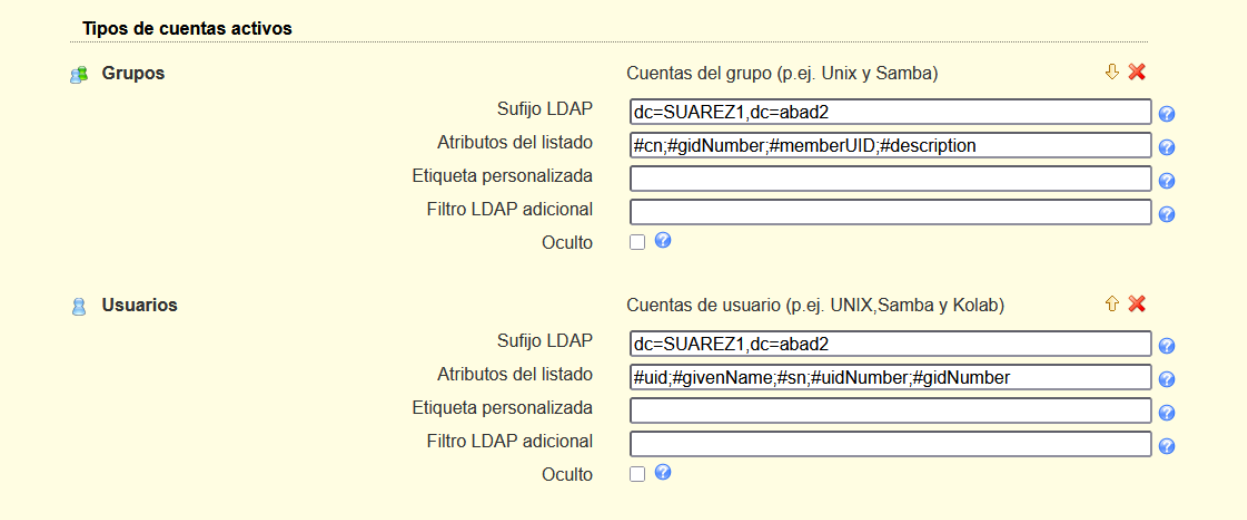


En “Ajustes de Herramientas” → Visor del árbol. Debemos de indicar el dominio.

En “Preferencias de Seguridad” → Lista de usuarios válidos. Debemos, como mínimo poner al “admin”.

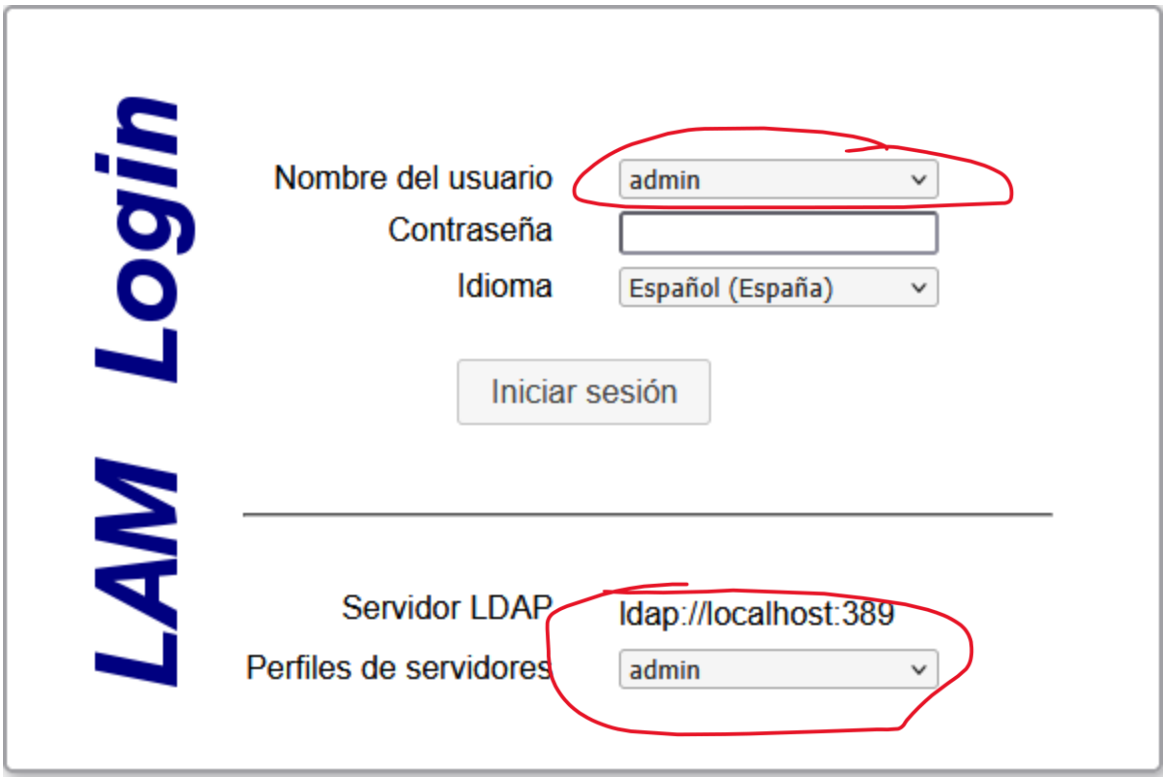


En la pestaña “Tipos de Cuentas”, podemos seleccionar el tipo de cuentas que queremos administrar. En nuestro caso administraremos de Grupos y Usuarios. Aquí debemos especificar el dominio en “Sufijo LDAP” y un listado de atributos (estos últimos salen por defecto).

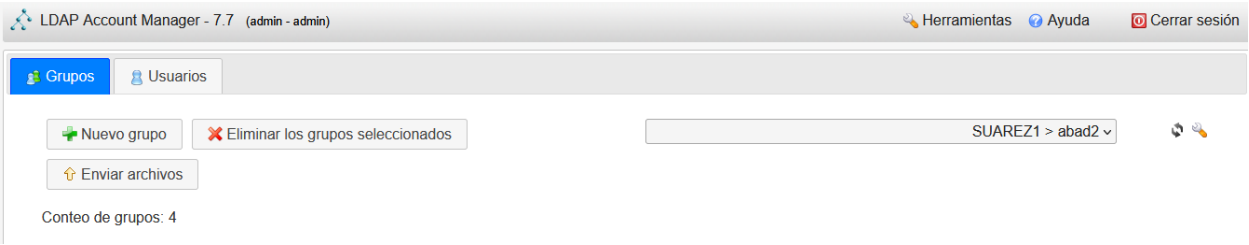


En las pestañas “Módulos” y “Preferencias del Módulo” no hemos modificado nada.

Una vez que hemos terminado volvemos a la ventana principal y seleccionamos a “admin” tanto en “Nombres de usuario” como en “Perfiles de Servidor”.



Entonces nos aparecerá una ventana así. Estaremos conectados al servidor

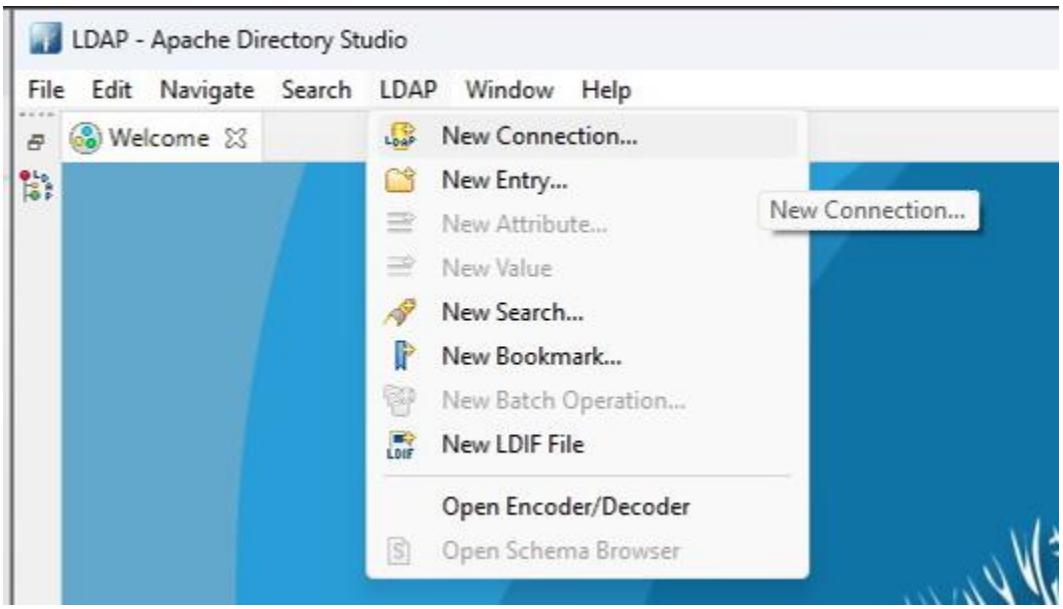


C) Instala y configura **Apache Directory Studio** (https://sanchezcorbalan.es/administrar-ldap-con-apache-directory-studio/)

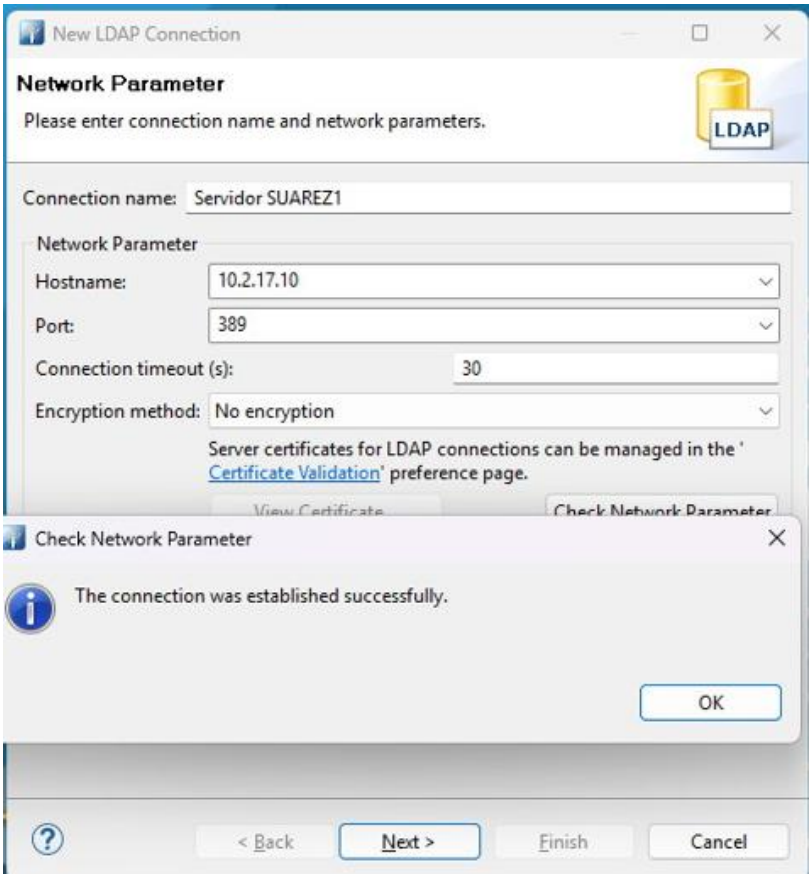
En Windows nos descargamos el instalador de la página oficial: https://directory.apache.org/studio/downloads.html

El asistente de instalación es muy claro y simple.

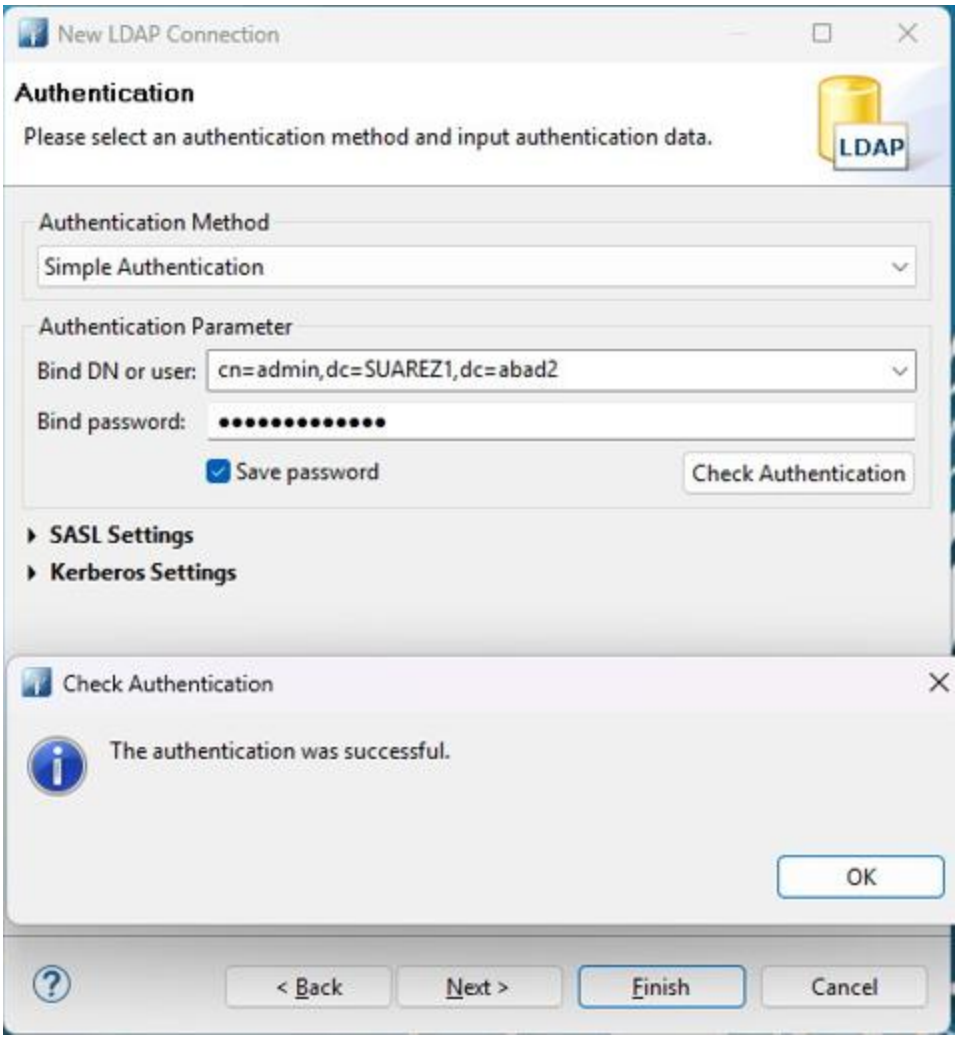
Una vez instalador, lo abrimos y vamos "LDAP" → "Nueva Conexión".



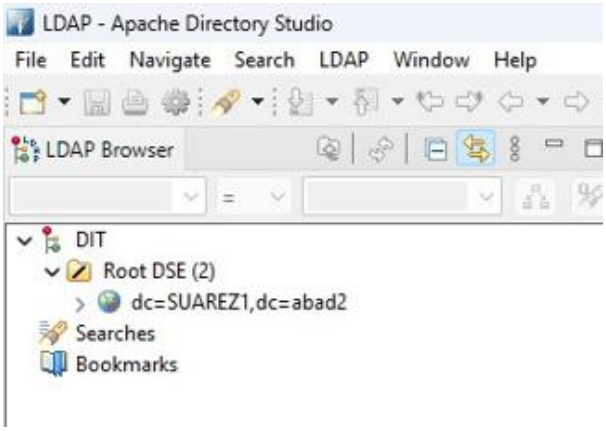
En la nueva ventana especificamos un nombre para la conexión (cualquiera), ponemos la IP del servidor, el puerto viene por defecto (389). Le damos a probar conexión.



En la siguiente ventana elegimos “Simple Authentication”. Ponemos como “user” al “admin” e introducimos su contraseña. Probamos la autentificación.



Si todo está bien, le damos a “Finalizar” y veremos en la parte izquierda como hemos hecho conexión con el servidor.



3) Crea Unidades Organizativas.

A) Utiliza ldapadd, LAM y Apache directory studio para crear las siguientes OU (una herramienta en cada caso):

- ldapadd: ou=usuarios

Usamos la plantilla para OU. Creamos con nano un archivo ".ldif" y escribimos esto:

```
 GNU nano 6.2
dn: ou=usuarios,dc=SUAREZ1,dc=abad2
objectClass: organizationalUnit
ou: usuarios
```

Lo guardamos y ejecutamos el siguiente comando.

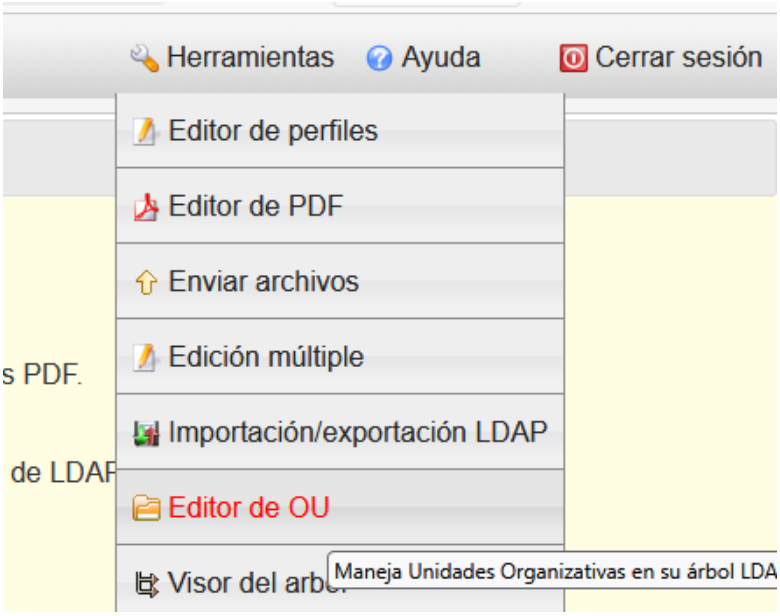
sudo ldapadd -x -D cn=admin,dc=SUAREZ1,dc=abad2 -W -f ARCHIVO.ldif

Nos pedirá meter la contraseña del "admin" y luego se llevará a cabo la acción.

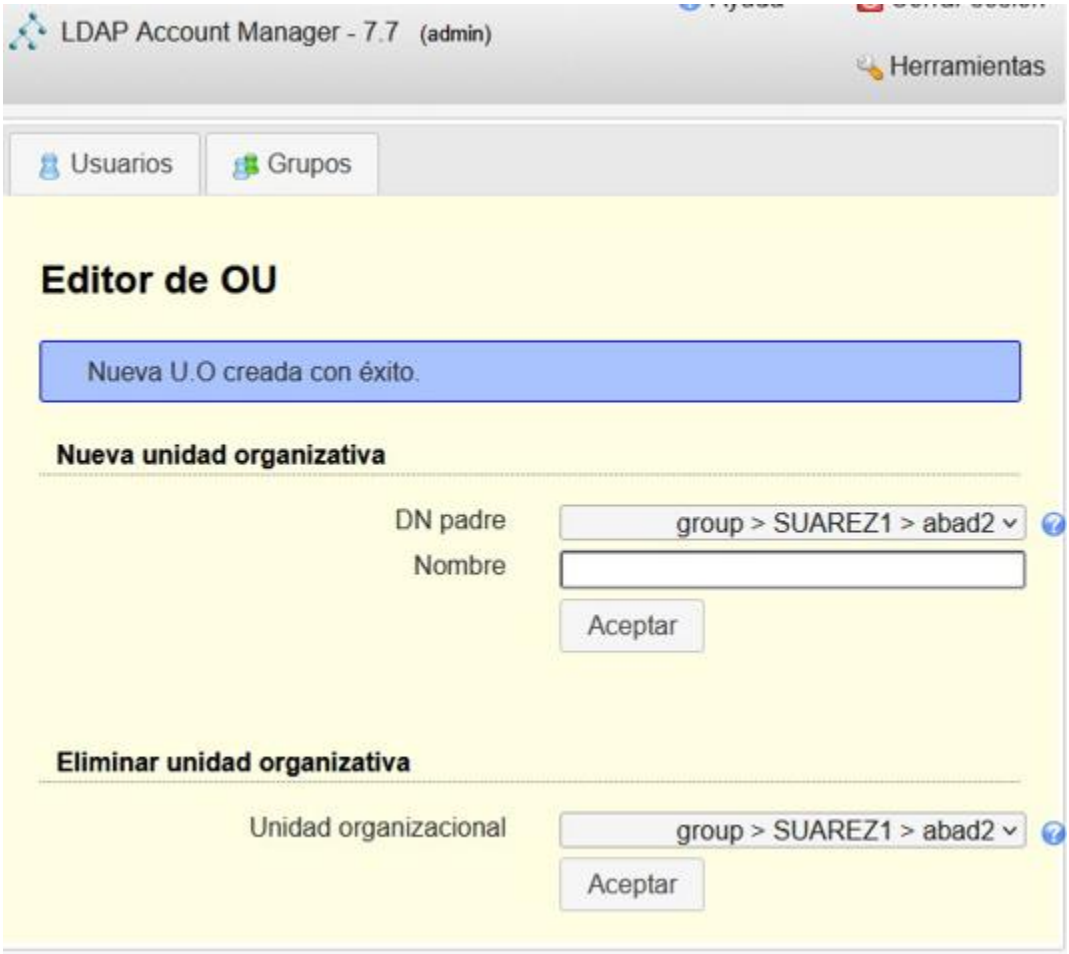
```
[root@control01 usuario]$sudo ldapadd -x -D cn=admin,dc=SUAREZ1,dc=abad2 -W -f grp.ldif
Enter LDAP Password:
adding new entry "ou=usuarios,dc=SUAREZ1,dc=abad2"
```

- LAM: ou=grupos

Vamos a "Herramientas" → "Editor de OU".

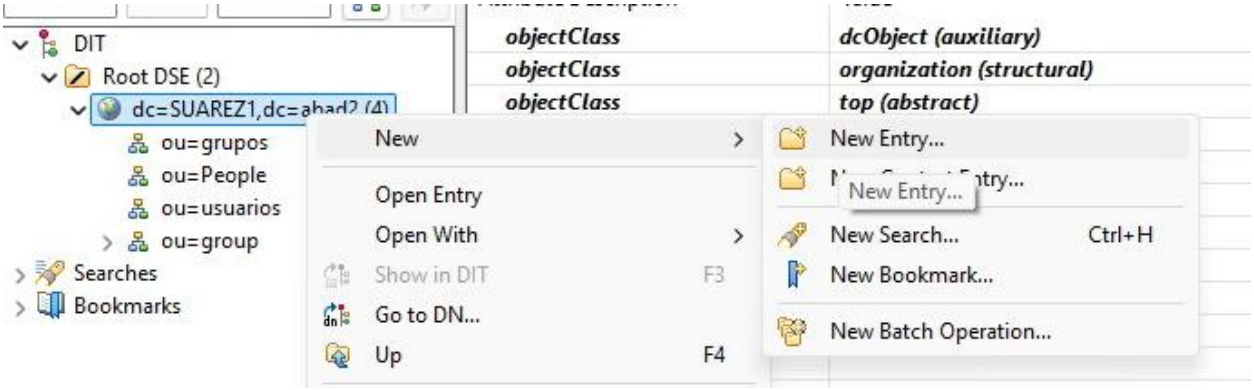


Y ahí podemos crear y eliminar OUs y enmarcarlas dentro de otras OUs.

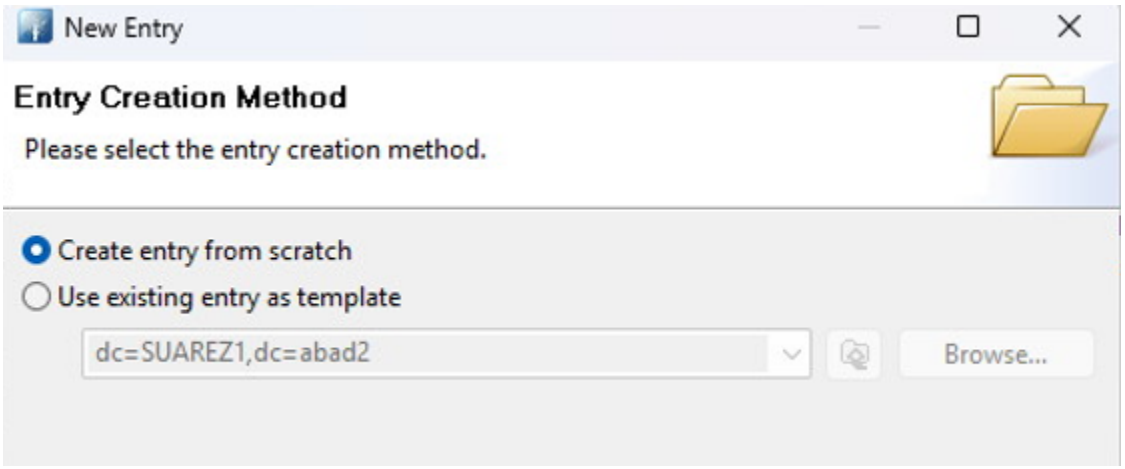


- Apache Directory: ou=equipos

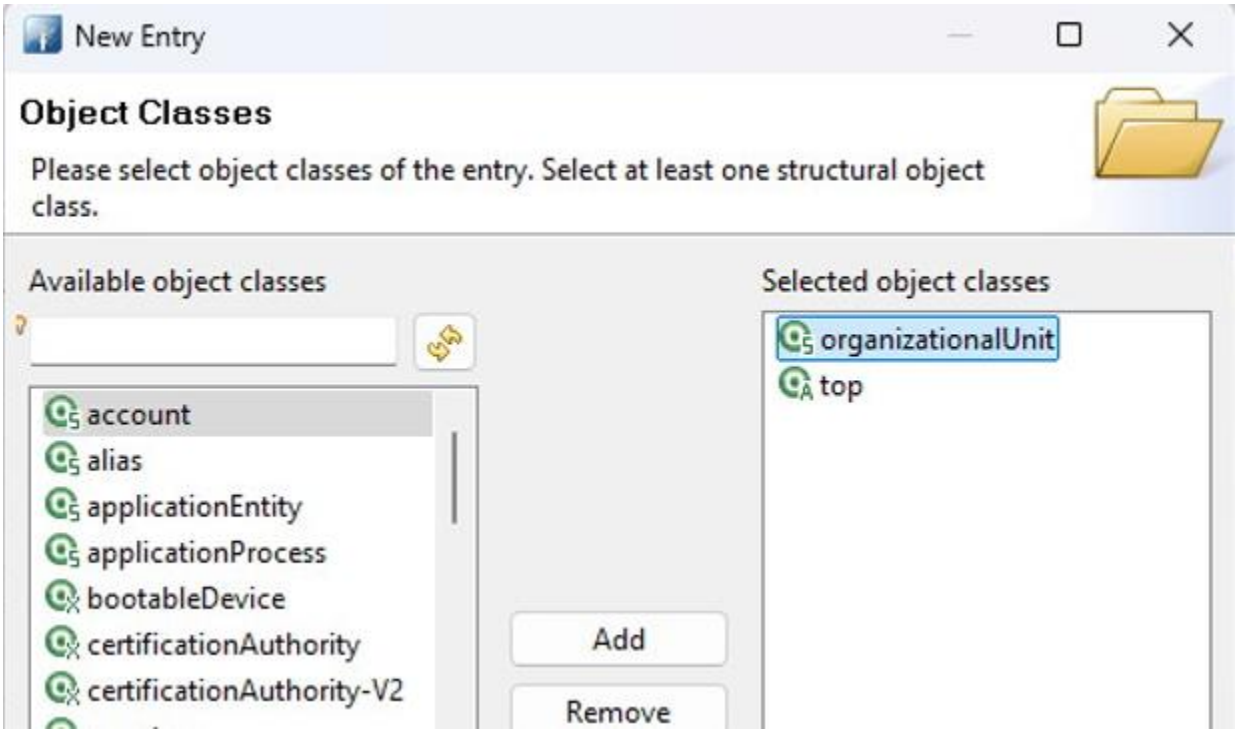
Pinchamos en el dominio u OU donde queremos que se cree y le damos a “Nuevo” → “Nueva entrada”.



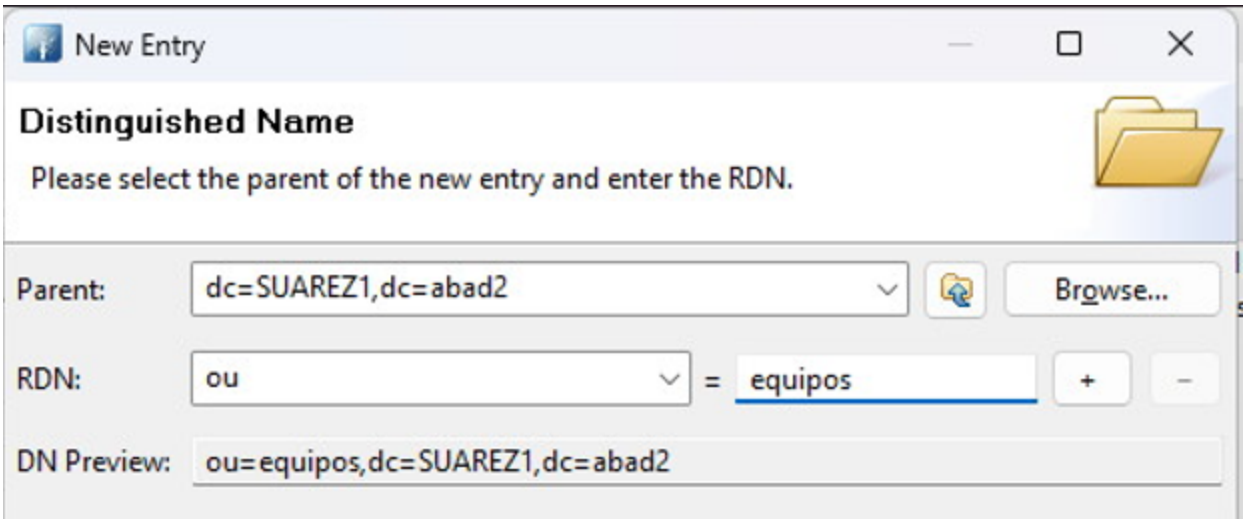
Crear desde cero.



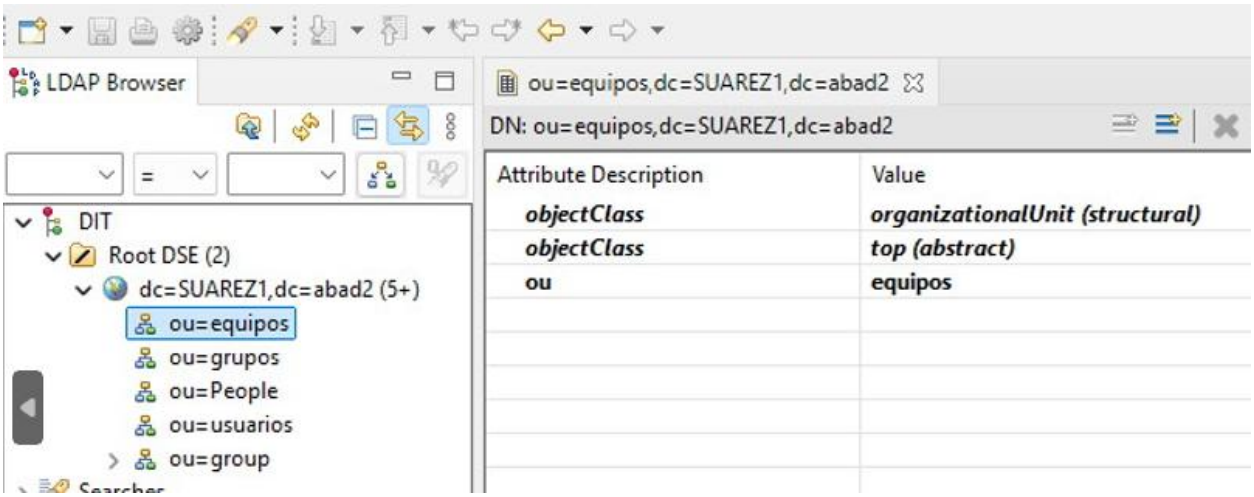
En “ObjectClasses” debemos elegir “organizationalUnit”.



Y después su nombre:


New Entry
Distinguished Name
Please select the parent of the new entry and enter the RDN.
Parent:
dc=SUAREZ1,dc=abad2
Browse...
RDN:
ou
=
equipos
+
DN Preview:
ou=equipos,dc=SUAREZ1,dc=abad2

OU creada:


LDAP Browser
ou=equipos,dc=SUAREZ1,dc=abad2
DN: ou=equipos,dc=SUAREZ1,dc=abad2
DIT
Root DSE (2)
dc=SUAREZ1,dc=abad2 (5+)
ou=equipos
ou=grupos
ou=People
ou=usuarios
ou=group
Attribute Description
Value
objectClass
organizationalUnit (structural)
objectClass
top (abstract)
ou
equipos

4) Creación de Usuarios.

Crea 4 usuarios con las siguientes características: (Usando ficheros .ldif)

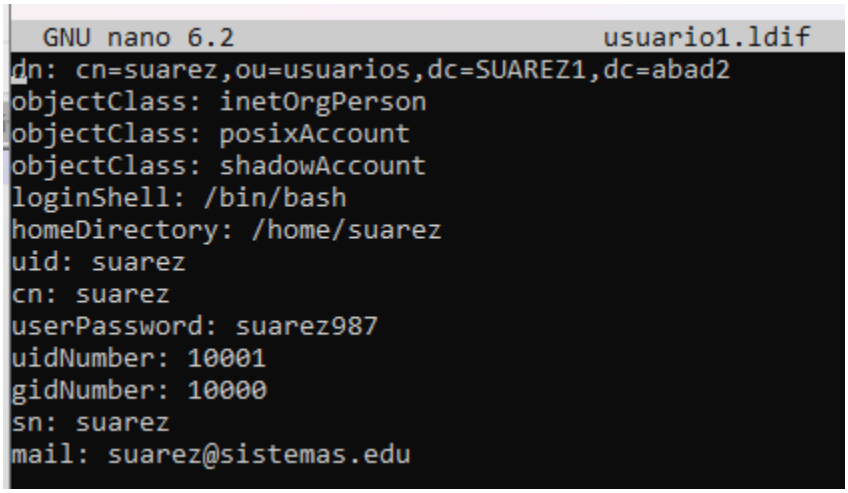
Usuario	UID	Contraseña	Ubicación
Alumno 1	Primer apellido	apellido987	ou=usuarios
Alumno 2	Segundo apellido	apellido987	ou=usuarios
Alumno 3	Nombre	nombre987	ou=usuarios
Alumno 4	Iniciales	iniciales987	ou=usuarios

La contraseña es el nombre de usuario seguido de 987.

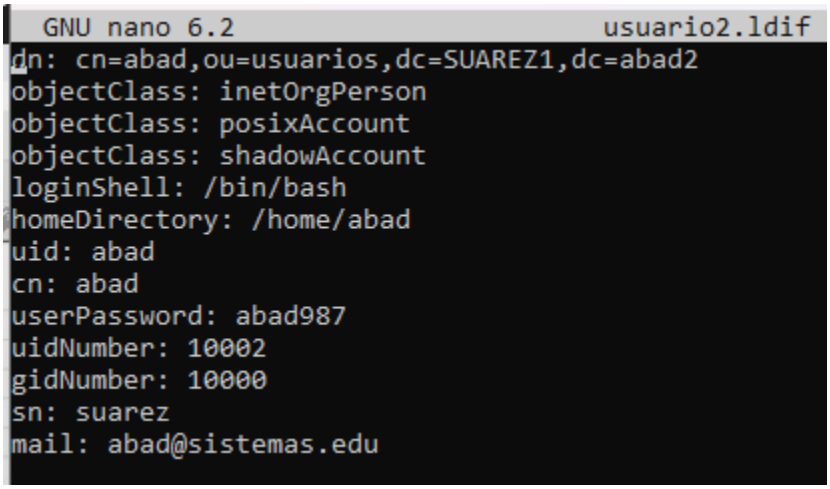
Para ejecutar los ficheros "-ldif" usaremos este comando:

ldapadd -x -D cn=admin,dc=SUAREZ1,dc=abad2 -W -f usuario.ldif

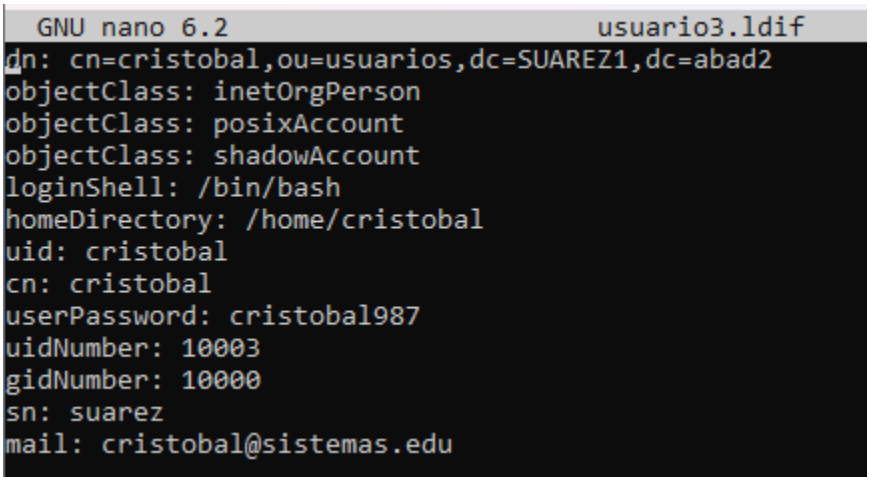
- Alumno 1 Primer apellido apellido987 ou=usuarios



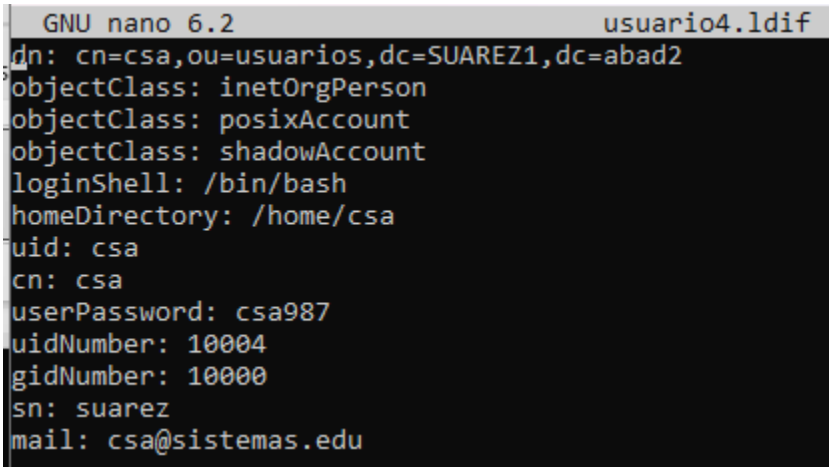
- Alumno 2 Segundo apellido apellido987 ou=usuarios



- Alumno 3 Nombre nombre987 ou=usuarios



- Alumno 4 Iniciales iniciales987 ou=usuarios



5) Creación de Grupos.

a) Crea los grupos: ASIR1 y ASIR2 dentro de ou=grupos.

```
 GNU nano 6.2                                ASIR1.ldif
dn: cn=ASIR1,ou=grupos,dc=SUAREZ1,dc=abad2
objectClass: posixGroup
gidNumber: 10002
cn: ASIR1
```

```
 GNU nano 6.2                                ASIR2.ldif
dn: cn=ASIR2,ou=grupos,dc=SUAREZ1,dc=abad2
objectClass: posixGroup
gidNumber: 10003
cn: ASIR2
```

Y usamos el comando:

ldapadd -x -D cn=admin,dc=sistemas,dc=edu -W -f unidades_organizativas.ldif

b) Asigna los dos primeros usuarios al grupo 1, y los otros dos al grupo 2.

```
 GNU nano 6.2                              unirASIR1.ldif
dn: cn=ASIR1,ou=grupos,dc=SUAREZ1,dc=abad2
changetype: modify
add: memberUid
memberUid: suarez
memberUid: 912345678
```

```
 GNU nano 6.2                              unirASIR2.ldif
dn: cn=ASIR2,ou=grupos,dc=SUAREZ1,dc=abad2
changetype: modify
add: memberUid
memberUid: cristobal
memberUid: csa
```

Y usamos el comando:

ldapmodify -x -D cn=admin,dc=sistemas,dc=edu -W -f modificacion.ldif

Para buscar: **ldapsearch -xLLL -b dc=SUAREZ1,dc=abad2 cn=ASIR1**

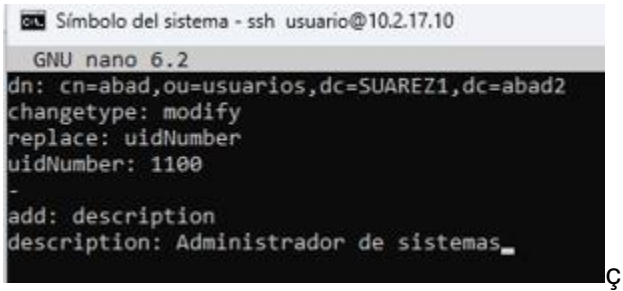
Para ver a que grupo pertenece un usuario:

ldapsearch -x -b “ou=grupos,dc=SUAREZ1,dc=abad2” “(memberUid=csa)” cn

Cuidado, que al copiarlo al terminal desaparecen las comillas.

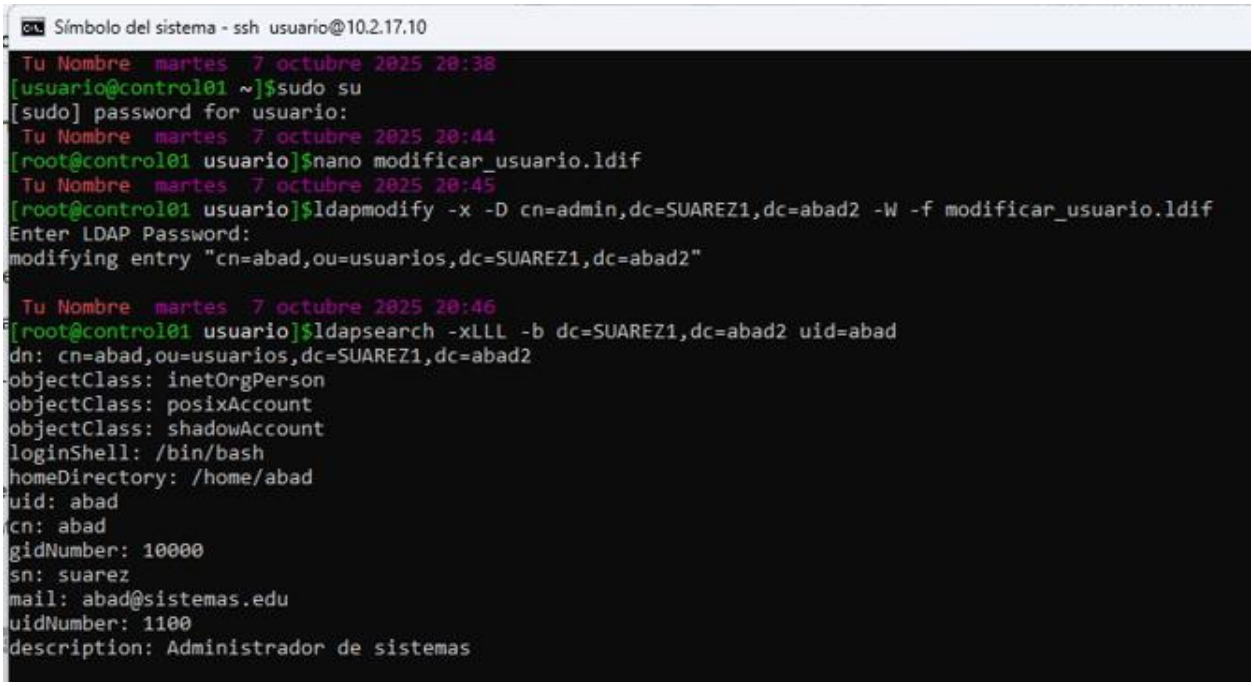
6) Realiza las siguientes modificaciones:

a) Añade al usuario con UID igual a tu **segundo apellido** la descripción: "Administrador de sistemas" y cámbiale el **uidNumber** a 1100.

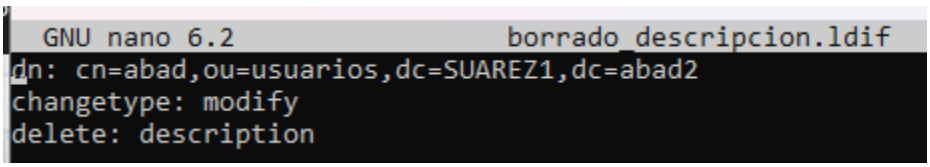


ç

b) Comprueba los cambios usando ldapsearch.



Elimina la descripción del usuario anterior.



c) Cambia el nombre del usuario por su número de teléfono personal: 912345678.

```
  GNU nano 6.2                        modificar_nombre.ldif
dn: cn=abad,ou=usuarios,dc=SUAREZ1,dc=abad2
changetype: modrdn
newrdn: cn=912345678
deleteoldrdn: 1
```

```
[root@control01 usuario]$ldapmodify -x -D cn=admin,dc=SUAREZ1,dc=abad2 -W -f modificar_nombre.ldif
Enter LDAP Password:
modifying rdn of entry "cn=abad,ou=usuarios,dc=SUAREZ1,dc=abad2"
```

```
[root@control01 usuario]$ldapsearch -xLLL -b dc=SUAREZ1,dc=abad2 cn=912345678
dn: cn=912345678,ou=usuarios,dc=SUAREZ1,dc=abad2
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash
homeDirectory: /home/abad
uid: abad
gidNumber: 10000
sn: suarez
mail: abad@sistemas.edu
uidNumber: 1100
cn: 912345678
```

d) Modifica su contraseña a 123456.

```
  GNU nano 6.2                          cambiar_pass.ldif
dn: cn=912345678,ou=usuarios,dc=SUAREZ1,dc=abad2
changetype: modify
replace: userPassword
userPassword: 123456
```

```
[root@control01 usuario]$ldapmodify -x -D cn=admin,dc=SUAREZ1,dc=abad2 -W -f cambiar_pass.ldif
Enter LDAP Password:
modifying entry "cn=912345678,ou=usuarios,dc=SUAREZ1,dc=abad2"
```

7) Consultas Avanzadas.

Utiliza ldapsearch para realizar las siguientes búsquedas:

a) Mostrar la información completa del grupo ASIR1.

```
[root@control01 usuario]$ldapsearch -xLLL -b dc=SUAREZ1,dc=abad2 cn=ASIR1
dn: cn=ASIR1,ou=grupos,dc=SUAREZ1,dc=abad2
objectClass: posixGroup
gidNumber: 10002
cn: ASIR1
memberUid: cn=suarez,ou=usuarios,dc=SUAREZ1,dc=abad2
memberUid: cn=abad,ou=usuarios,dc=SUAREZ1,dc=abad2
```

b) Listar información de todos los usuarios.

Usamos: **ldapsearch -xLLL -b dc=SUAREZ1,dc=abad2 '(objectClass=posixAccount)'**

```
[root@control01 usuario]$ldapsearch -xLLL -b dc=SUAREZ1,dc=abad2 '(objectClass=posixAccount)'
dn: cn=suarez,ou=usuarios,dc=SUAREZ1,dc=abad2
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash
homeDirectory: /home/suarez
uid: suarez
cn: suarez
uidNumber: 10001
gidNumber: 10000
sn: suarez
mail: suarez@sistemas.edu

dn: cn=912345678,ou=usuarios,dc=SUAREZ1,dc=abad2
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash
uid: abad
sn: suarez
mail: abad@sistemas.edu
cn: 912345678
gidNumber: 10002
homeDirectory: /home/abad2
uidNumber: 1111

dn: cn=cristobal,ou=usuarios,dc=SUAREZ1,dc=abad2
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash
homeDirectory: /home/cristobal
uid: cristobal
cn: cristobal
uidNumber: 10003
sn: suarez
mail: cristobal@sistemas.edu
gidNumber: 10021
shadowLastChange: 20372
```

c) Listar el homeDirectory de todos los usuarios.

```
Tu Nombre  martes  7 octubre 2025 22:16
[root@control01 usuario]$ldapsearch -xLLL -b dc=SUAREZ1,dc=abad2 '(objectClass=posixAccount)' homeDirectory
dn: cn=suarez,ou=usuarios,dc=SUAREZ1,dc=abad2
homeDirectory: /home/suarez

dn: cn=912345678,ou=usuarios,dc=SUAREZ1,dc=abad2
homeDirectory: /home/abad

dn: cn=cristobal,ou=usuarios,dc=SUAREZ1,dc=abad2
homeDirectory: /home/cristobal

dn: cn=csa,ou=usuarios,dc=SUAREZ1,dc=abad2
homeDirectory: /home/csa
```

d) Mostrar el uidNumber del usuario de tus iniciales.

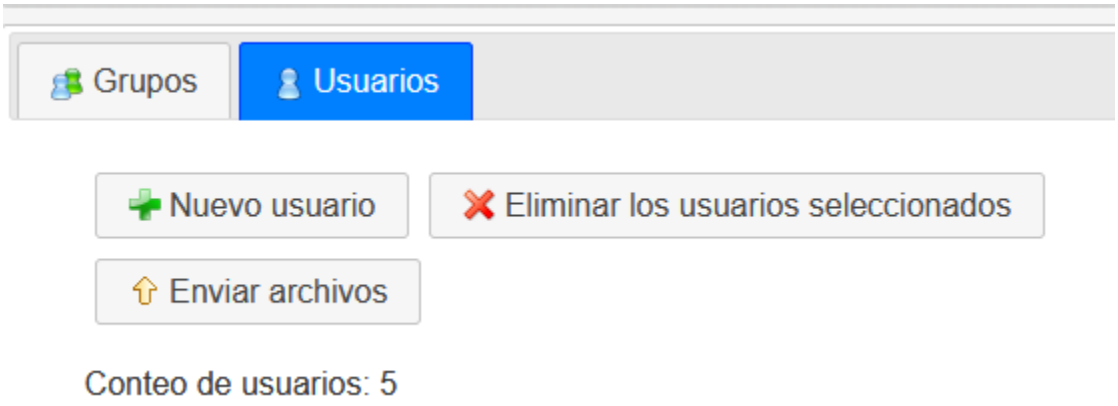
```
[root@control01 usuario]$ldapsearch -xLLL -b dc=SUAREZ1,dc=abad2 uid=csa uidNumber
dn: cn=csa,ou=usuarios,dc=SUAREZ1,dc=abad2
uidNumber: 10004
```

8) Gestión con LDAP Account Manager.

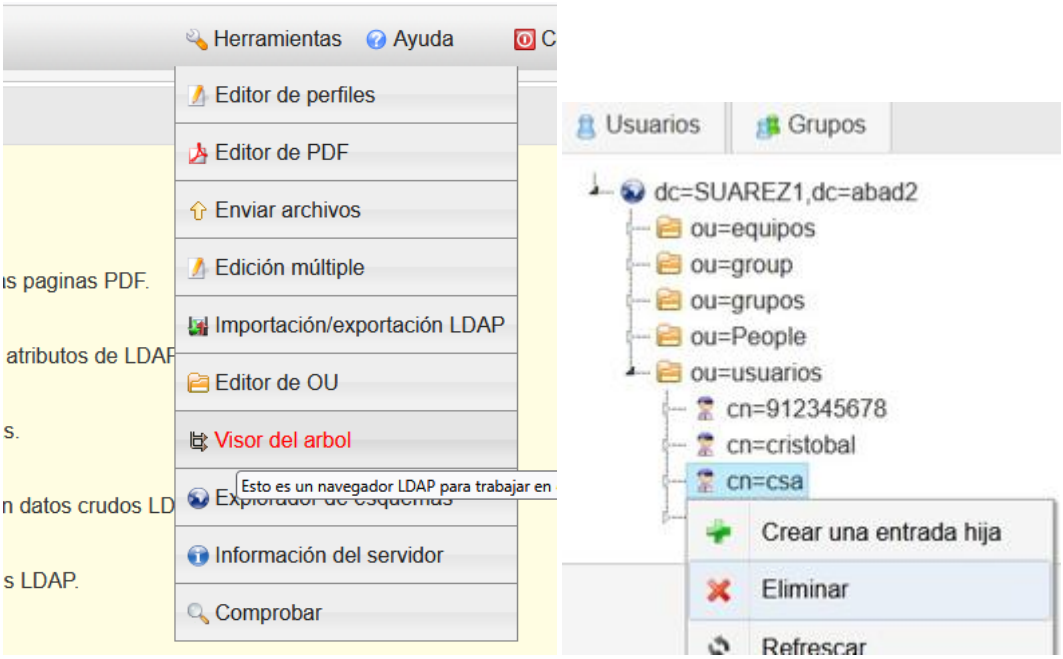
Usa **LDAP Account Manager** para:

a) Eliminar el usuario de tus iniciales.

Hay diferentes maneras. Podemos ir a Usuarios, seleccionarlo y luego Eliminar.

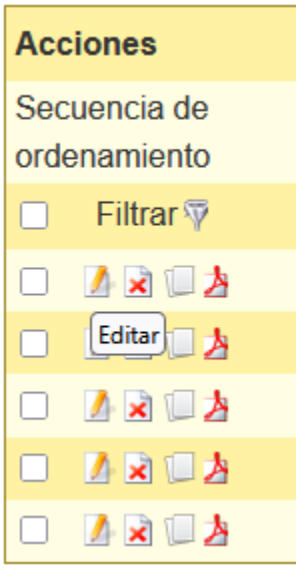


También podemos ir a Herramientas → Visor del Arbol y eliminarlo desde allí.

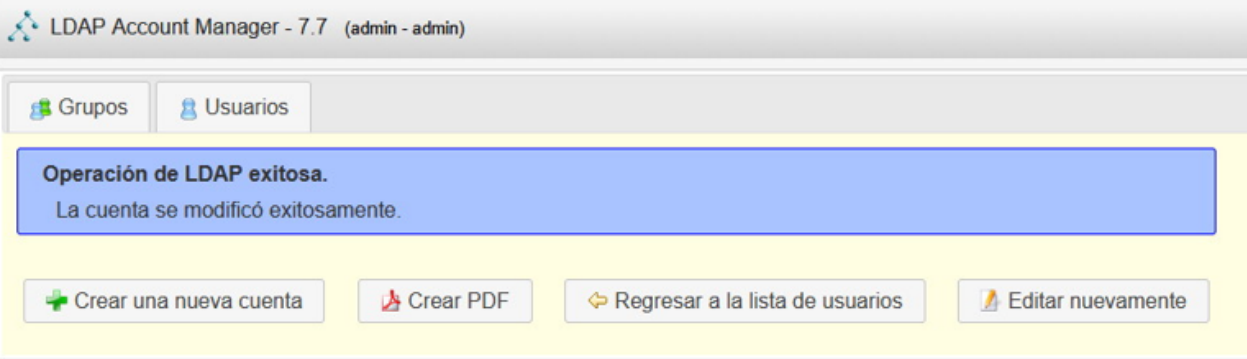


b) Cambiar el UID del usuario con UID igual a tu segundo apellido a **1111**, y establecer su homeDirectory como: /home/APELLIDO2

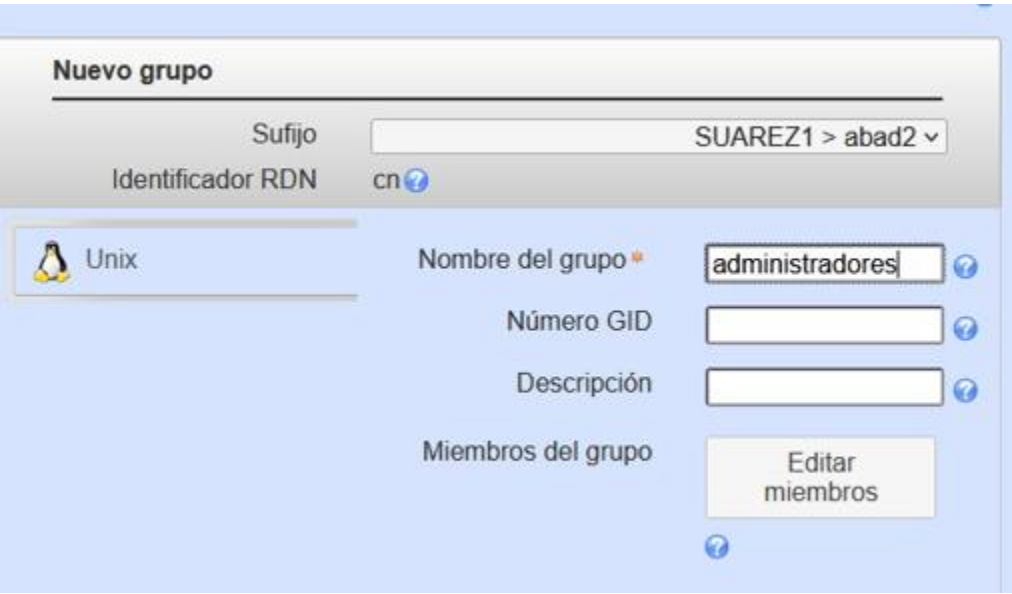
Nos vamos a la pestaña de Usuarios y le damos a Editar.

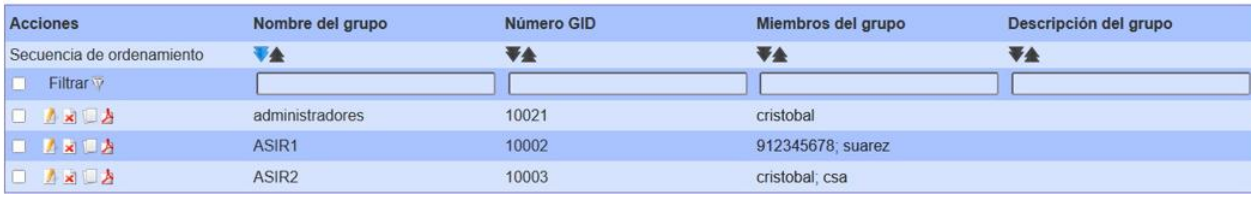


En esta ocasión nos vamos a la pestaña Unix y allí introducimos las modificaciones.



c) Crear un grupo llamado administradores y añadir a tu usuario con nombre completo.



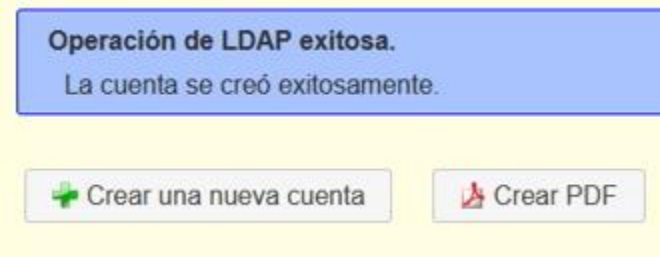


Acciones	Nombre del grupo	Número GID	Miembros del grupo	Descripción del grupo
Secuencia de ordenamiento				
Filtrar				
	administradores	10021	cristobal	
	ASIR1	10002	912345678; suarez	
	ASIR2	10003	cristobal; csa	

d) Crear un nuevo usuario con UID igual a tus **iniciales + últimos 3 dígitos de tu DNI**.

Debe pertenecer al grupo administradores.

uidNumber y homeDirectory deben usarse los valores por defecto.

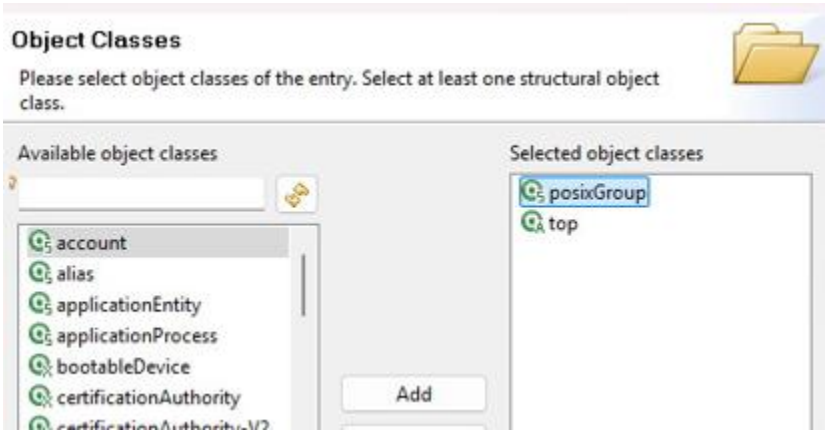


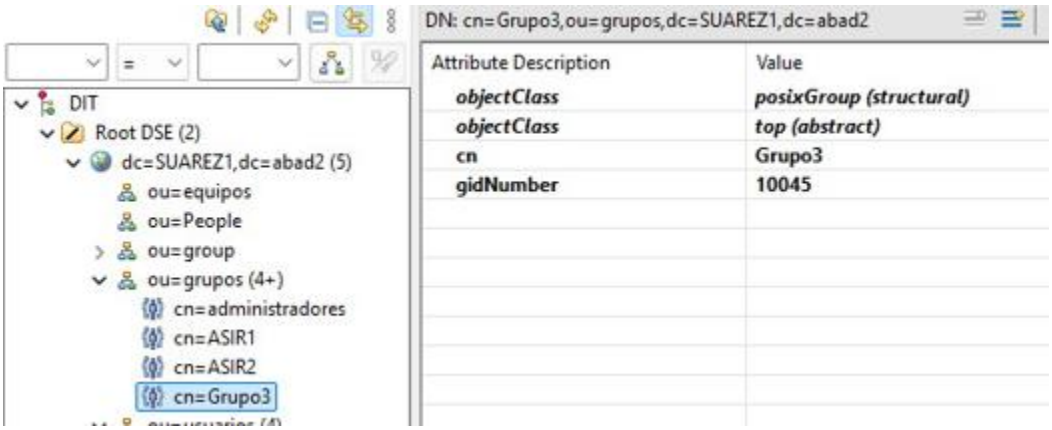
e) Añadirle al nuevo usuario una dirección de e-mail y teléfono de casa.

En “Editar” → “Personal”

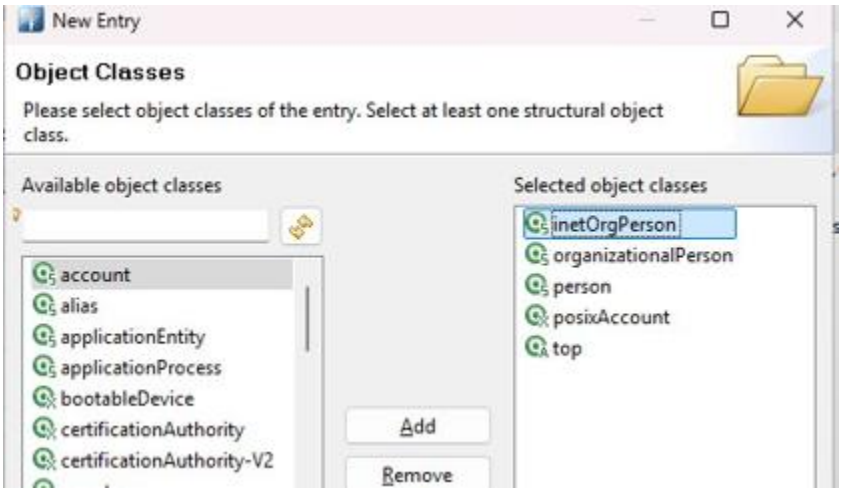
9) Gestión con Apache Directory Studio.

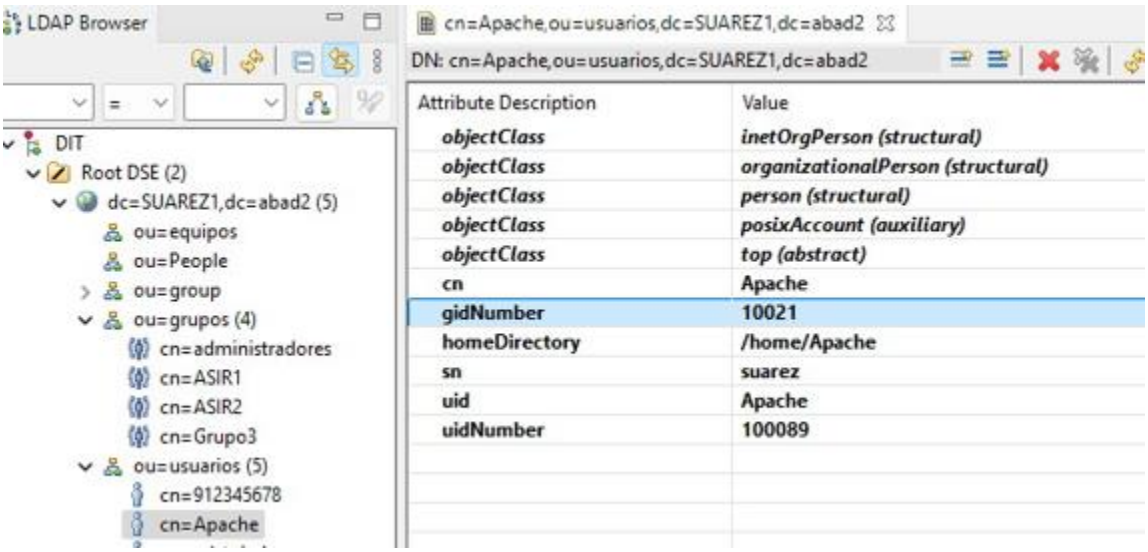
a) Crear un grupo llamado Grupo3 y añadir a tu usuario con nombre completo.





b) Crear un nuevo usuario con llamado Apache: Debe pertenecer al grupo administradores.





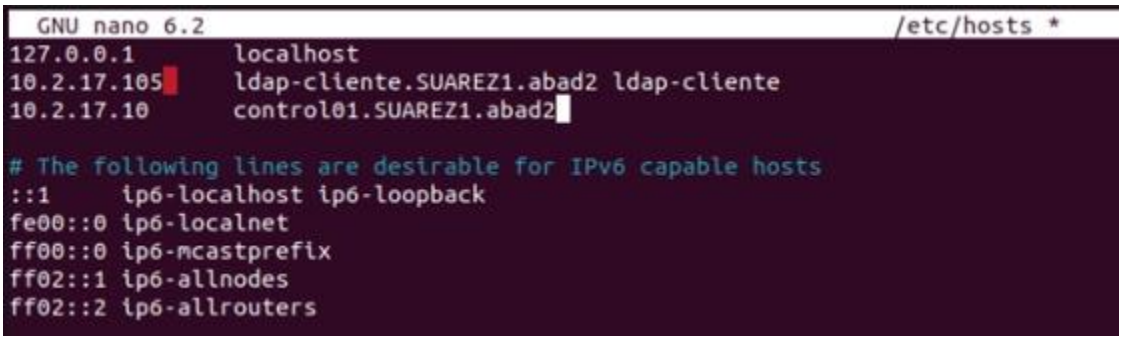
10) Cliente LDAP.

Antes de nada, hay que hacer ciertas configuraciones en el archivo “hosts”.

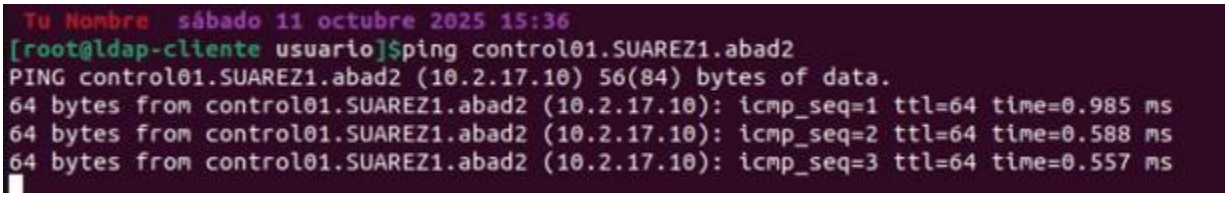
Primero debemos cambiarle el nombre al cliente para además de darle un nombre personalizado, unirlo al dominio:

sudo hostnamectl set-hostname ldap-cliente.SUAREZ1.abad2

Ahora, en **/etc/hosts** debemos indicar la ip de nuestro equipo y la del servidor, poniendo el nombre completo de ambos.



Comprobamos haciendo PING al servidor:

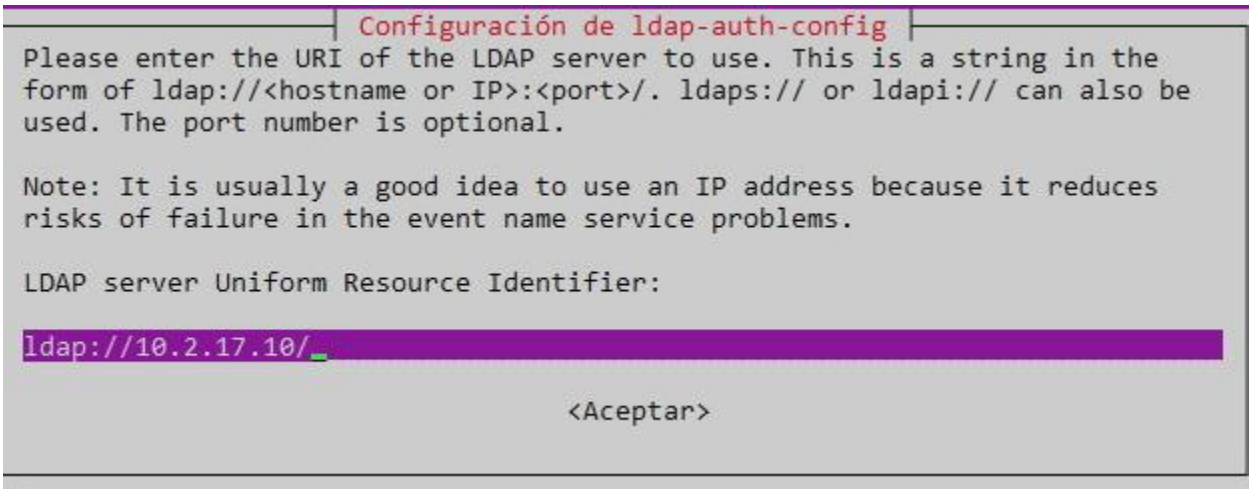


a) Instala y configura un cliente Linux para conectarse al servidor LDAP.

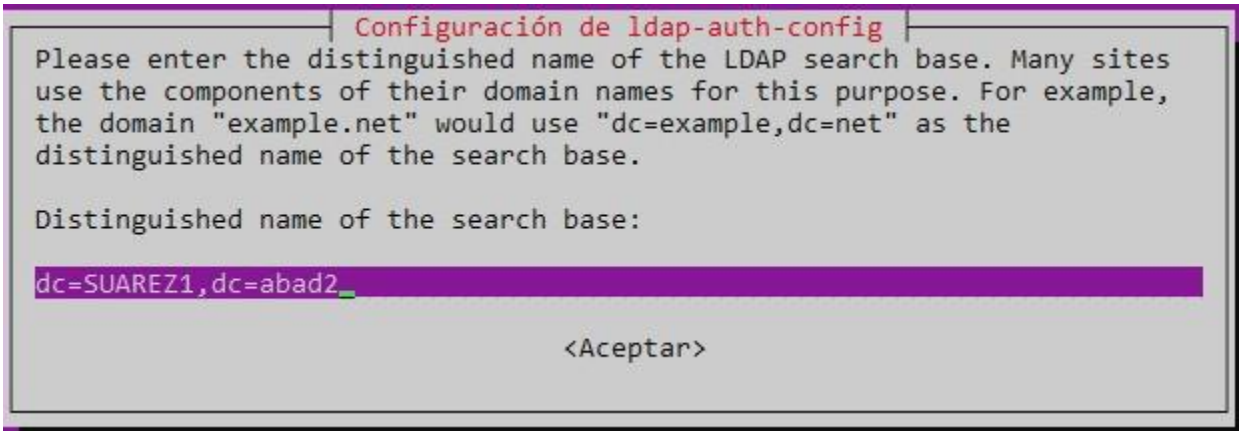
Ahora hacemos un “**apt update**”.

Luego: **sudo apt-get install libnss-ldap libpam-ldap ldap-utils -y**

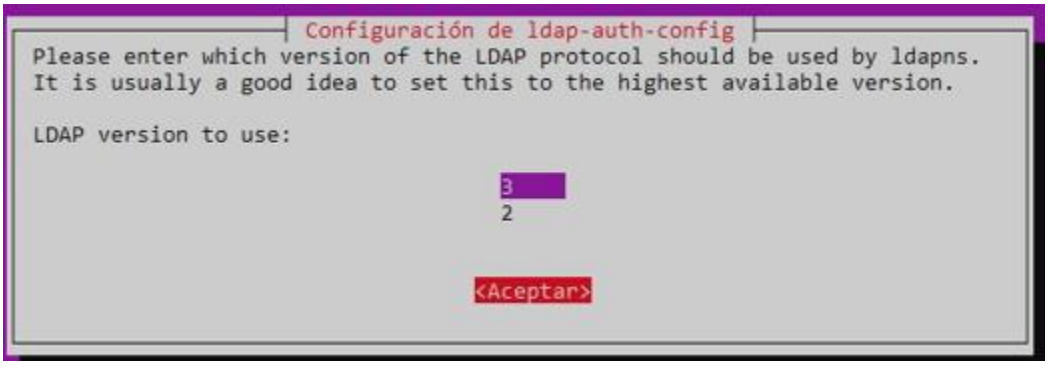
Indicamos la IP del servidor. Recuerda quitar **ldapi** y poner solo **ldap.**

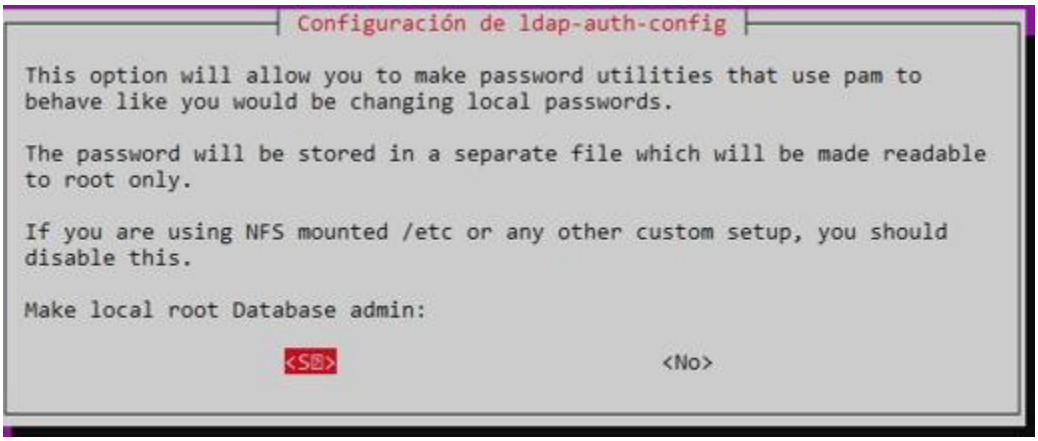


Nombre dominio.

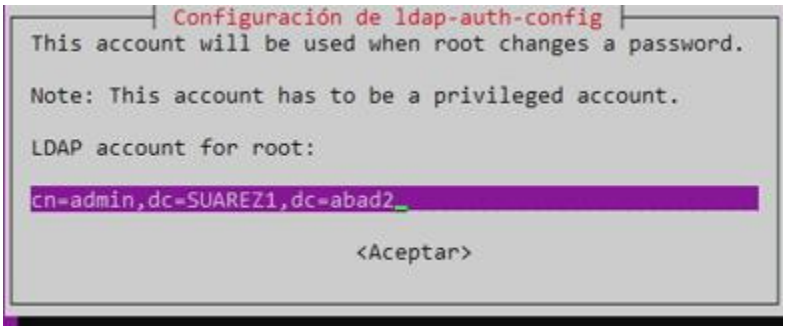


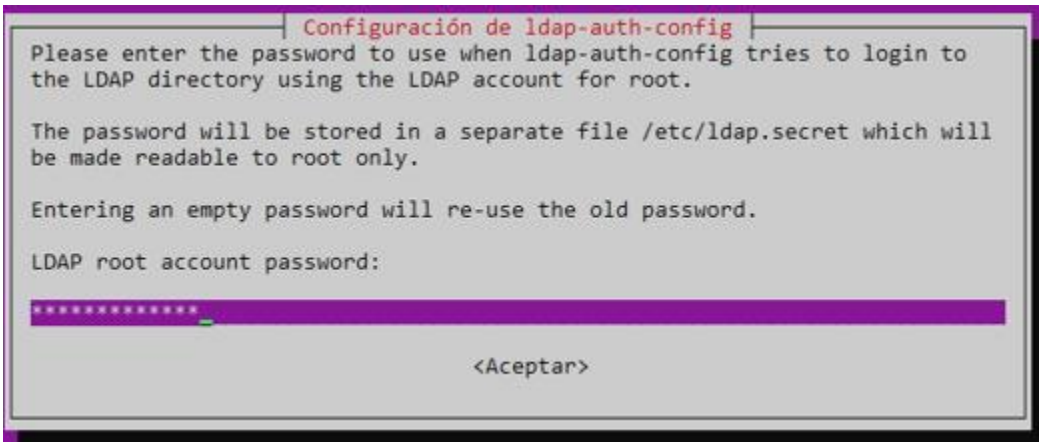
Protocolo 3



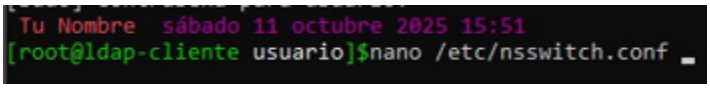


Cuenta con privilegios:

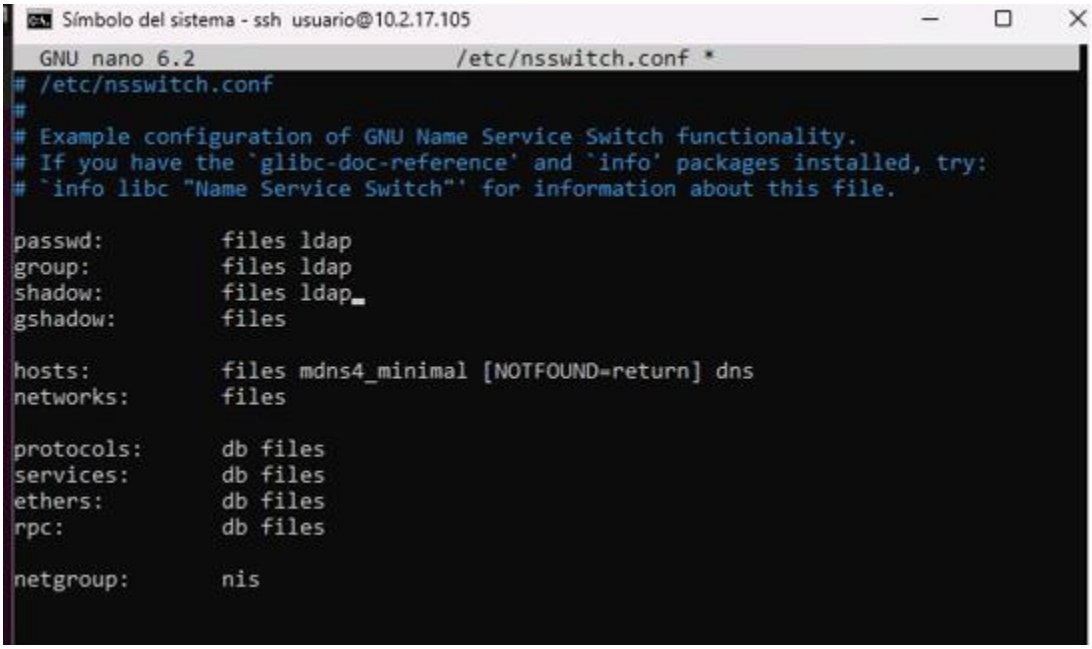




Ahora debemos configurar el archivo “**nsswitch.conf**”.



En passwd, group y shadow debemos poner lo siguiente.

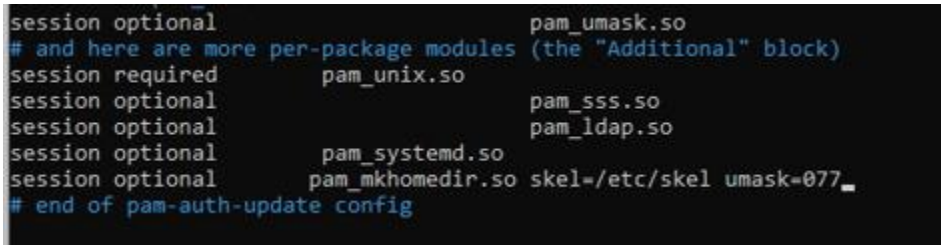


Para comprobar que está bien, usamos: **sudo getent passwd**

Nos debe mostrar los usuarios del ldap.

Otro archivo: **/etc/pam.d/common-session**

En la última fila ponemos: “**session optional pam_mkhomedir.so skel=/etc/skel umask=077**”



b) Comprueba desde el cliente que:

- Se pueden ver los usuarios y grupos creados.

Usamos el comando:

ldapsearch -x -H ldap://192.168.1.10 -b "dc=somebooks,dc=local"

```
[root@ldap-cliente usuario]$ldapsearch -x -H ldap://10.2.17.10 -b "dc=SUAREZ1,dc=abad2"
# extended LDIF
#
# LDAPv3
# base <dc=SUAREZ1,dc=abad2> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# SUAREZ1.abad2
dn: dc=SUAREZ1,dc=abad2
objectClass: top
objectClass: dcObject
objectClass: organization
o: SUAREZ1.abad2
dc: SUAREZ1

# group, SUAREZ1.abad2
dn: ou=group,dc=SUAREZ1,dc=abad2
objectClass: organizationalUnit
ou: group

# grupos, SUAREZ1.abad2
dn: ou=grupos,dc=SUAREZ1,dc=abad2
objectClass: organizationalUnit
ou: grupos

# People, SUAREZ1.abad2
dn: ou=People,dc=SUAREZ1,dc=abad2
objectClass: organizationalUnit
ou: People

# equipos, SUAREZ1.abad2
dn: ou=equipos,dc=SUAREZ1,dc=abad2
ou: equipos
objectClass: organizationalUnit
objectClass: top
```

- Puedes iniciar sesión en el cliente con alguno de los usuarios creados