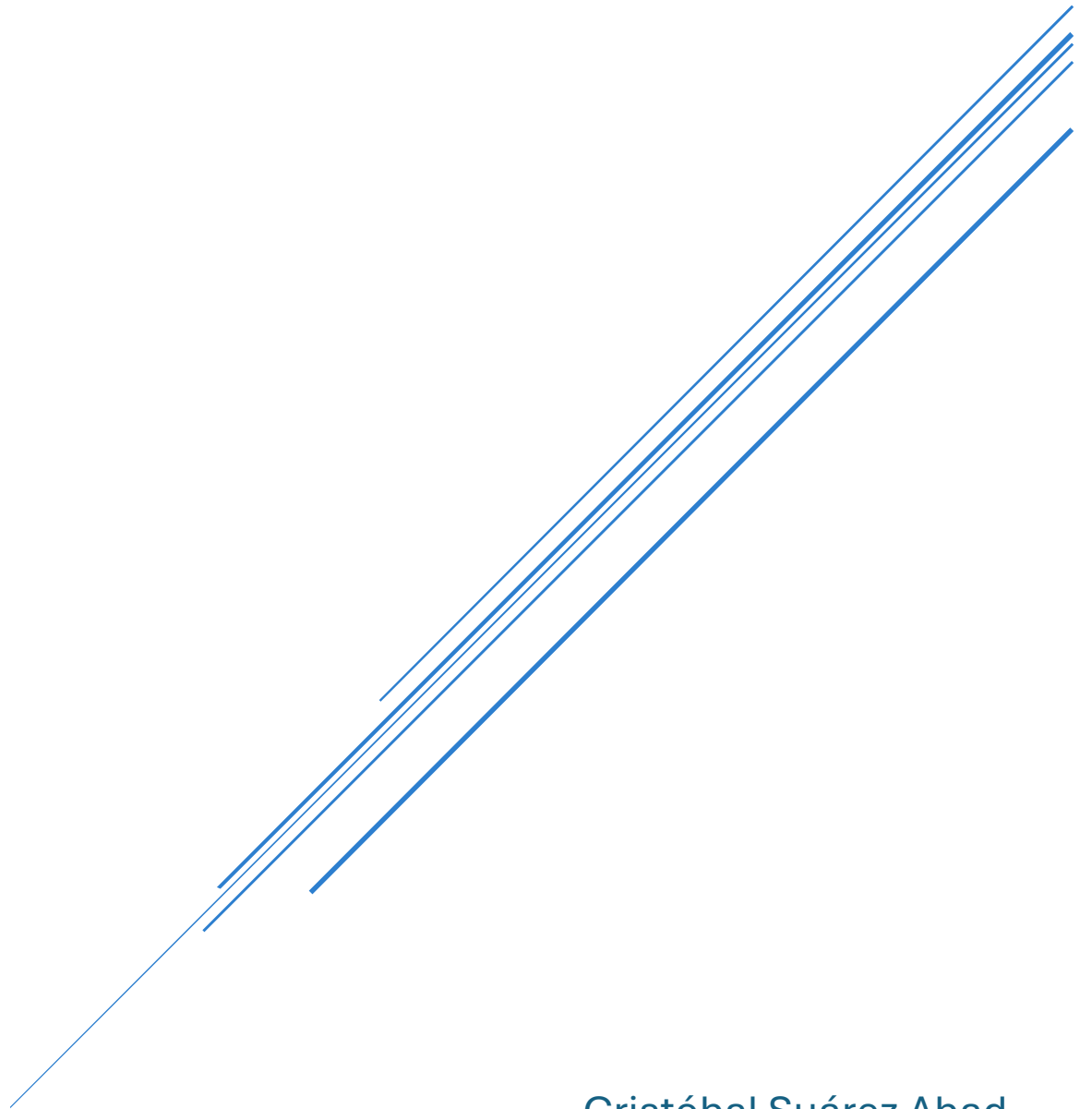


# OPENLDAP (LINUX)



Cristóbal Suárez Abad  
Administración de Sistemas Operativos – 2º ASIR

## Índice:

<b>0) Introducción:</b> .....	0
1. Instalación del Servidor LDAP: .....	1
a) Instala en una máquina virtual Linux Server (con una distribución de tu elección) el servidor <b>OpenLDAP</b> . El dominio del directorio debe ser: APELLIDO1.apellido2, sin acentos ni eñes. ....	1
b) Configura el servidor para que esté listo para aceptar conexiones LDAP. ....	5
2. Instalación de Herramienta de Administración Gráfica.....	0
a) Instala LDAP Account Manager (LAM) en el servidor.....	0
b) Configura LAM para conectarse correctamente al dominio recién creado.....	1
c) Instala y configura <b>Apache Directory Studio</b> ( <a href="https://sanchezcorbalan.es/administrar-ldap-con-apache-directory-studio/">https://sanchezcorbalan.es/administrar-ldap-con-apache-directory-studio/</a> ) .....	5
<b>3) Crea Unidades Organizativas.</b> .....	9
A) Utiliza ldapadd, LAM y Apache directory studio para crear las siguientes OU (una herramienta en cada caso):.....	9
4) Creación de Usuarios. ....	0
5) Creación de Grupos. ....	0
a) Crea los grupos: ASIR1 y ASIR2 dentro de ou=grupos. ....	0
b) Asigna los dos primeros usuarios al grupo 1, y los otros dos al grupo 2. ....	0
6) Realiza las siguientes modificaciones:.....	1
a) Añade al usuario con UID igual a tu <b>segundo apellido</b> la descripción: "Administrador de sistemas" y cámbiale el <b>uidNumber</b> a 1100. ....	1
b) Comprueba los cambios usando ldapsearch.....	1
Elimina la descripción del usuario anterior. ....	1
c) Cambia el nombre del usuario por su número de teléfono personal: 912345678. ....	2
d) Modifica su contraseña a 123456.....	2
7) Consultas Avanzadas. ....	3
a) Mostrar la información completa del grupo ASIR1. ....	3
b) Listar información de todos los usuarios. ....	3
c) Listar el homeDirectory de todos los usuarios.....	4
d) Mostrar el uidNumber del usuario de tus iniciales. ....	4

8) Gestión con LDAP Account Manager. ....	0
a) Eliminar el usuario de tus iniciales. ....	0
b) Cambiar el UID del usuario con UID igual a tu segundo apellido a <b>1111</b> , y establecer su homeDirectory como: /home/APELLIDO2 .....	1
c) Crear un grupo llamado administradores y añadir a tu usuario con nombre completo. 2	
d) Crear un nuevo usuario con UID igual a tus <b>iniciales + últimos 3 dígitos de tu DNI</b> ....	3
Debe pertenecer al grupo administradores.....	3
uidNumber y homeDirectory deben usarse los valores por defecto. ....	3
e) Añadirle al nuevo usuario una dirección de e-mail y teléfono de casa. ....	4
9) Gestión con Apache Directory Studio.....	0
a) Crear un grupo llamado Grupo3 y añadir a tu usuario con nombre completo. ....	0
b) Crear un nuevo usuario con llamado Apache: Debe pertenecer al grupo administradores. ....	1
10) Cliente LDAP. ....	0
a) Instala y configura un cliente Linux para conectarse al servidor LDAP. ....	0
b) Comprueba desde el cliente que: .....	4
- Se pueden ver los usuarios y grupos creados. ....	4
- Puedes iniciar sesión en el cliente con alguno de los usuarios creados .....	5

## 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”**

```
Tu Nombre miércoles 1 octubre 2025 12:19
[root@server2asir usuario]$hostnamectl set-hostname control01.SUAREZ1.abad2
Tu Nombre miércoles 1 octubre 2025 12:20
[root@server2asir usuario]$cat /etc/hostname
control01.SUAREZ1.abad2
```

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

```
Símbolo del sistema - ssh usu x + v
GNU nano 6.2 /etc/hosts *
127.0.0.1 localhost
127.0.1.1 control01.SUAREZ1.abad2 control01
10.2.17.10 control01.SUAREZ1.abad2 control01

# 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
```

Ahora procedemos a instalar “lapd” en el equipo.

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

Introducimos contraseña y su confirmación.

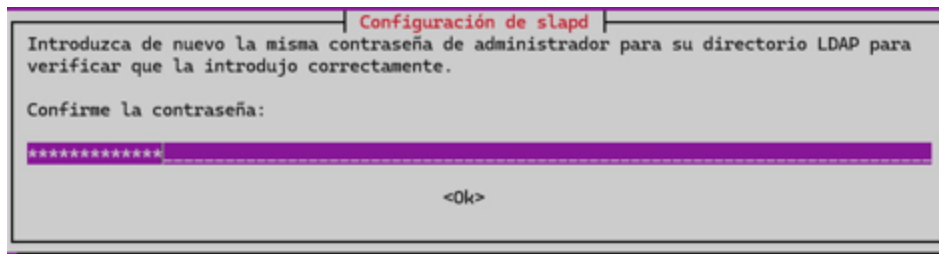
Configuración de slapd

Introduzca la contraseña para la entrada de administrador de su directorio LDAP.

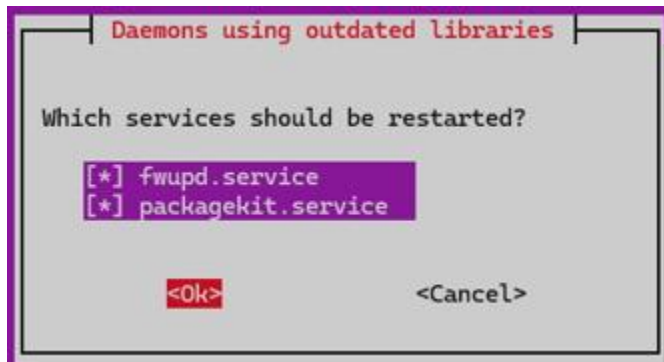
Contraseña del administrador:

\*\*\*\*\*

<Ok>

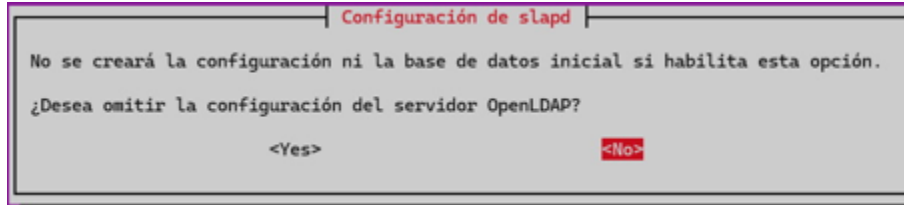


Nos pide reiniciar algunos servicios. Los reiniciamos todos.

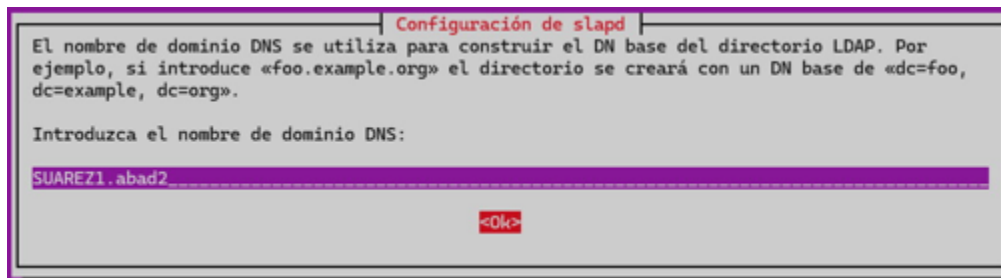


Una vez terminado, realizamos la configuración manual, la completa:

**“sudo dpkg-reconfigure slapd”**



Establecemos el nombre del dominio.



Nombre de la organización (lo mismo).

**Configuración de slapd**

Introduzca el nombre de la organización a utilizar en el DN base del directorio LDAP.

Nombre de la organización:

SUAREZ1.abad2

<Ok>

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

**Configuración de slapd**

Introduzca la contraseña para la entrada de administrador de su directorio LDAP.

Contraseña del administrador:

\*\*\*\*\*

<Ok>

Borrar base de datos cuando se purgue el paquete slapd.

**Configuración de slapd**

¿Desea que se borre la base de datos cuando se purgue el paquete slapd?

<Yes> <No>

Mover base de datos antigua.

**Configuración de slapd**

Existen ficheros en «/var/lib/ldap» que probablemente interrumpen el proceso de configuración. Si activa esta opción, se moverán los ficheros de las bases de datos antiguas antes de crear una nueva base de datos.

¿Desea mover la base de datos antigua?

<Yes> <No>

Todo bien.

```
Tu Nombre miércoles 1 octubre 2025 12:40
[root@control01 usuario]$dpkg-reconfigure slapd
Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.5.19+dfsg-0ubuntu0.22.04.1... done.
Moving old database directory to /var/backups:
- directory unknown... done.
Creating initial configuration... done.
Creating LDAP directory... done.
```



Confirmación: “slapcat”.

```
Tu Nombre miércoles 1 octubre 2025 12:41
[root@control01 usuario]$slapcat
dn: dc=SUAREZ1,dc=abad2
objectClass: top
objectClass: dcObject
objectClass: organization
o: SUAREZ1.abad2
dc: SUAREZ1
structuralObjectClass: organization
entryUUID: c0dcd960-330f-1040-8697-816f7212bec5
creatorsName: cn=admin,dc=SUAREZ1,dc=abad2
createTimestamp: 20251001124153Z
entryCSN: 20251001124153.770600Z#000000#000#000000
modifiersName: cn=admin,dc=SUAREZ1,dc=abad2
modifyTimestamp: 20251001124153Z
```

Otra confirmación: “systemctl status slapd”

```
Tu Nombre miércoles 1 octubre 2025 12:42
[root@control01 usuario]$systemctl status slapd
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
   Loaded: loaded (/etc/init.d/slapd; generated)
   Drop-In: /usr/lib/systemd/system/slapd.service.d
            └─slapd-remain-after-exit.conf
   Active: active (running) since Wed 2025-10-01 12:41:55 UTC; 1min 34s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 3526 ExecStart=/etc/init.d/slapd start (code=exited, status=0/SUCCESS)
    Tasks: 3 (limit: 2220)
   Memory: 3.3M
      CPU: 50ms
   CGroup: /system.slice/slapd.service
            └─3550 /usr/sbin/slapd -h "ldap:/// ldapi:///" -g openldap -u openldap -F /etc/ldap/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”

```
Tu Nombre miércoles 1 octubre 2025 12:43
[root@control01 usuario]$ldapsearch -x -LLL -H ldap:/// -b dc=SUAREZ1,dc=abad2
dn: dc=SUAREZ1,dc=abad2
objectClass: top
objectClass: dcObject
objectClass: organization
o: SUAREZ1.abad2
dc: SUAREZ1
```

“ufw status”

“ufw allow 389/tcp”

“ss -tulpn | grep slapd”

```
upc ansible-tee-0003
Tu Nombre miércoles 1 octubre 2025 12:46
[root@control01 usuario]$ ss -tulpn | grep slapd
tcp  LISTEN 0      2048      0.0.0.0:389      0.0.0.0:*      users:(("slapd",pid=3550,fd=8))
tcp  LISTEN 0      2048      [::]:389        [::]:*        users:(("slapd",pid=3550,fd=9))
```

## 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”

```
Tu Nombre martes 7 octubre 2025 08:46
usuario@control01 ~]$sudo a2enconf php8.1-cgi
enabling conf php8.1-cgi.
To activate the new configuration, you need to run:
  systemctl reload apache2
Tu Nombre martes 7 octubre 2025 08:48
usuario@control01 ~]$systemctl reload apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to reload 'apache2.service'.
Authenticating as: usuario
Password:
==== 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.

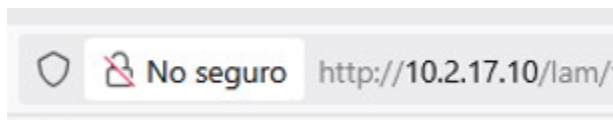
```
GNU nano 6.2 /etc/apache2/conf-enabled/ldap-account-manager.conf

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

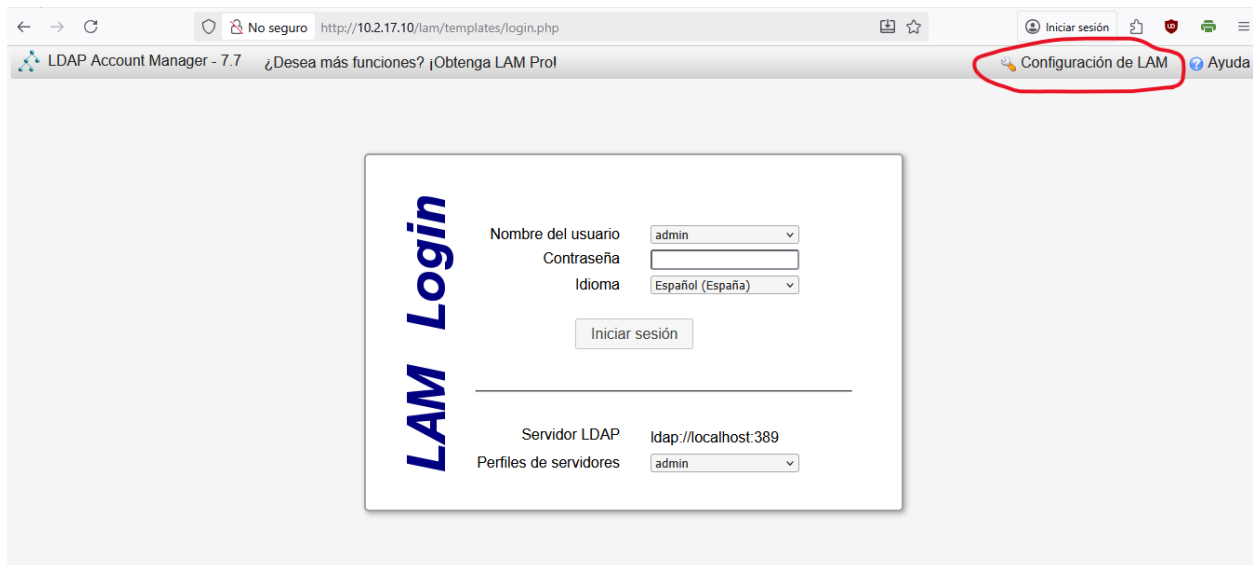
<Directory /usr/share/ldap-account-manager>
  Options +FollowSymLinks
  AllowOverride All
  Require all granted
  DirectoryIndex index.html
</Directory>
```

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

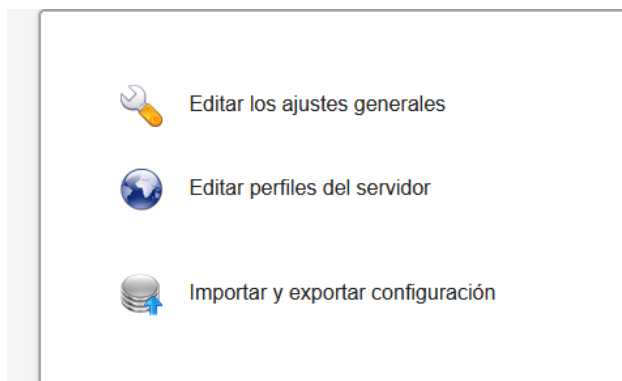
Ahora podemos acceder a LAM desde el navegador, para ello ponemos en la barra de búsqueda: “http://IP\_SERVIDOR/lam”



Ahora debemos ir a “Configuración LAM”



Elegimos “Editar los Ajustes Generales”



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

Por favor introduzca la contraseña maestra para cambiar las preferencias generales:

Contraseña maestra  ?

Aceptar

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”.


Por favor introduzca su contraseña para cambiar las preferencias del servidor:

Nombre del perfil  ▼

Contraseña  ?

Aceptar

---

 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.

### Añadir perfil

Nombre del perfil	<input type="text"/>	?
Contraseña del perfil	<input type="password"/>	
Vuelva a introducir la contraseña	<input type="password"/>	
Plantilla	unix	?

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.

### Preferencias del servidor

Dirección del servidor *	ldap://localhost:389	?
Activar TLS	no	?
Límite de búsqueda LDAP	-	?
Parte del DN a ocultar		?

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”.

**Ajustes de herramientas**

Herramientas ocultas

<input type="checkbox"/> Editor de PDF	<input type="checkbox"/> Explorador de esquemas	<input type="checkbox"/> Dispositivos WebAuthn
<input type="checkbox"/> Editor de perfiles	<input type="checkbox"/> Visor del arbol	<input type="checkbox"/> Edición múltiple
<input type="checkbox"/> Importación/exportación LDAP	<input type="checkbox"/> Editor de OU	<input type="checkbox"/> Comprobar
<input type="checkbox"/> Información del servidor	<input type="checkbox"/> Enviar archivos	

Visor del arbol

Sufijo del arbol

**Preferencias de seguridad**

Método del inicio de sesión

Lista de usuarios válidos

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).

**Tipos de cuentas activos**

**Grupos**

Cuentas del grupo (p.ej. Unix y Samba)

Sufijo LDAP

Atributos del listado

Etiqueta personalizada

Filtro LDAP adicional

Oculto ☐

**Usuarios**

Cuentas de usuario (p.ej. UNIX,Samba y Kolab)

Sufijo LDAP

Atributos del listado

Etiqueta personalizada

Filtro LDAP adicional

Oculto ☐

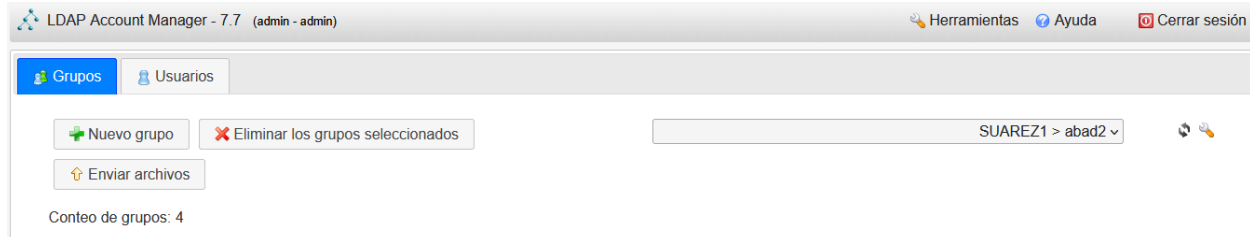
En las pestañas “Módulos” y “Preferencias del Módulo” no hemos modificado nada.

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



The image shows the LAM Login interface. On the left, the text "LAM Login" is written vertically in a large, bold, blue font. To the right, there is a login form with the following fields: "Nombre del usuario" (Username) with a dropdown menu showing "admin", "Contraseña" (Password) with an empty text box, and "Idioma" (Language) with a dropdown menu showing "Español (España)". Below these fields is a button labeled "Iniciar sesión". A horizontal line separates the login section from the LDAP configuration section. In the LDAP section, there is a label "Servidor LDAP" and a text box containing "ldap://localhost:389". Below this is a label "Perfiles de servidores" and a dropdown menu showing "admin". Red circles highlight the "admin" dropdown in the username field and the "ldap://localhost:389" text box and "admin" dropdown in the LDAP section.

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>

#### Windows 64 bit installer

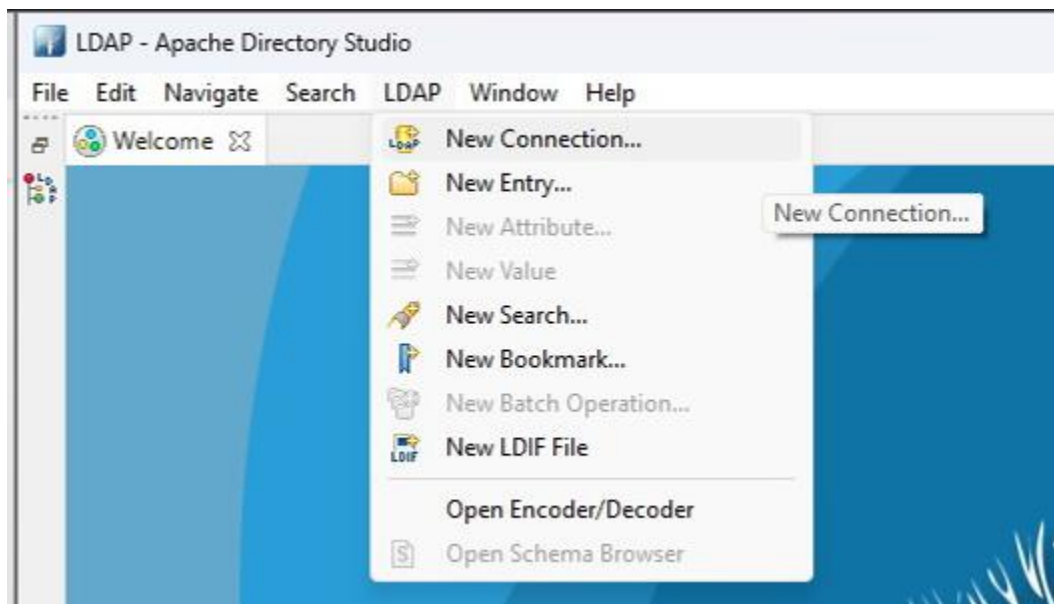




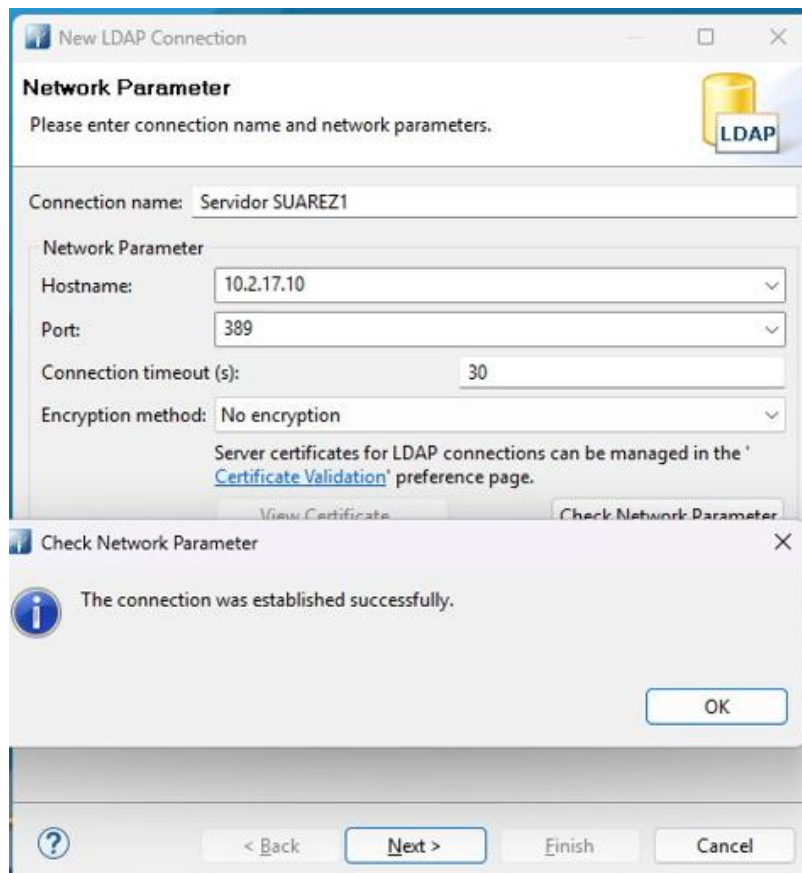
El asistente de instalación es muy claro y simple.



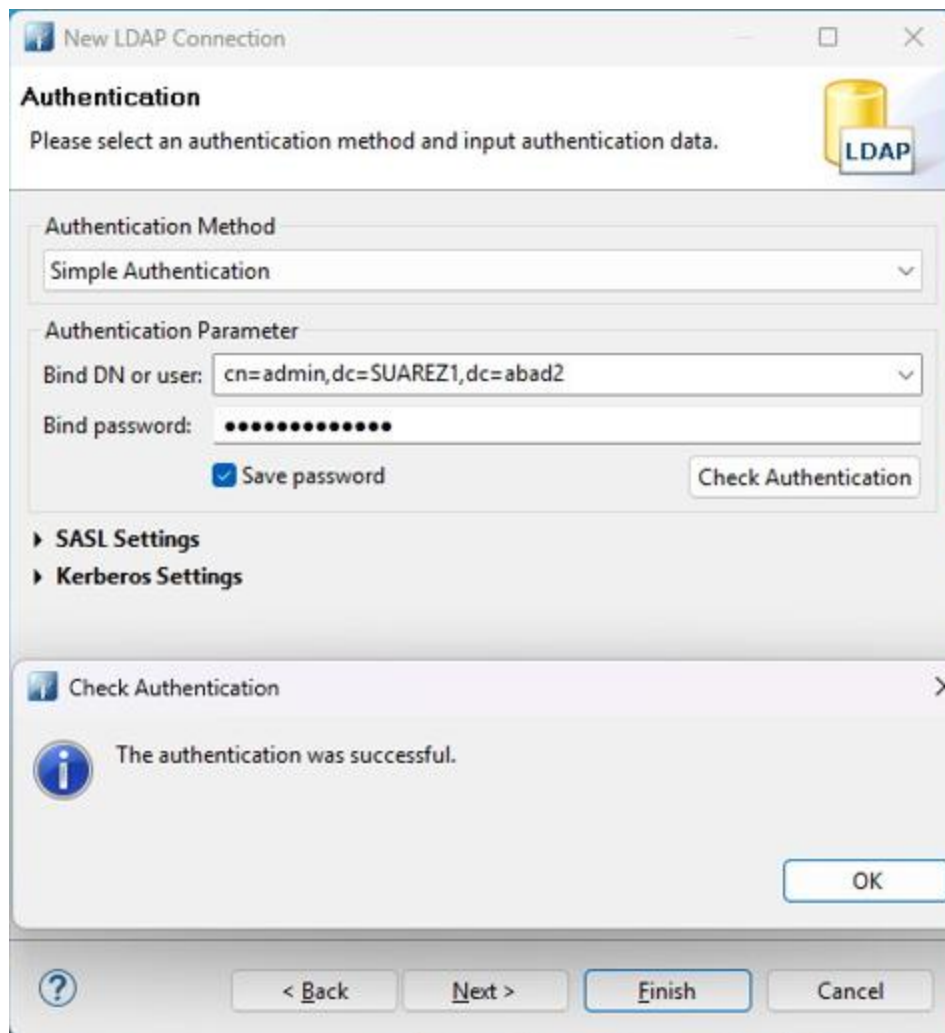
Una vez instalador, lo abrimos y vamos “LDAP” → “Nueva Conexión”.



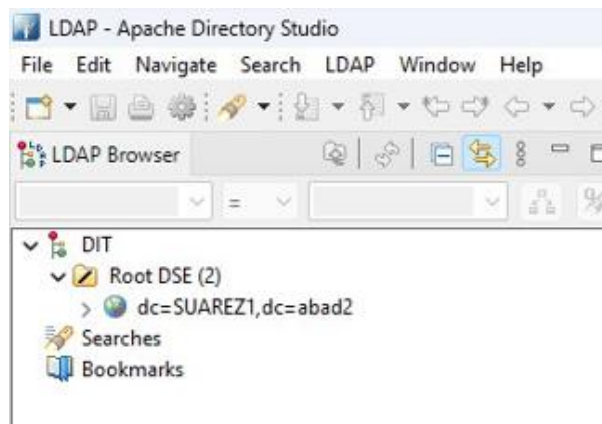
En la nueva ventana especificamos un nombre para la conexión (cualquiera), ponemos la IP del servidor, el puerto viene por defecto (389). Le damos a probar conexión.



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



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.

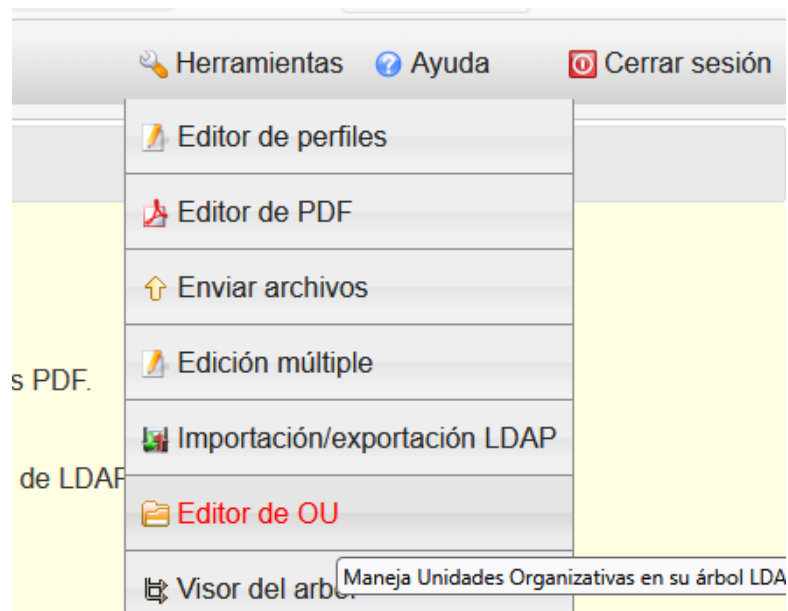
**sudo ldapadd -x -D cn=admin,dc=SUAREZ1,dc=abad2 -W -f ARCHIVO.ldif**

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.

LDAP Account Manager - 7.7 (admin) Herramientas

Usuarios Grupos

### Editor de OU

Nueva U.O creada con éxito.

#### Nueva unidad organizativa

DN padre: group > SUAREZ1 > abad2

Nombre:

Aceptar

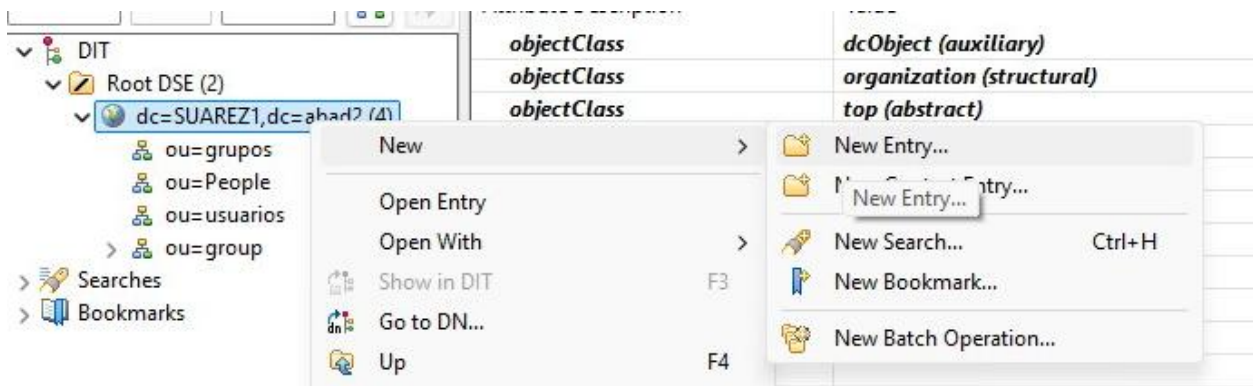
#### Eliminar unidad organizativa

Unidad organizativa: group > SUAREZ1 > abad2

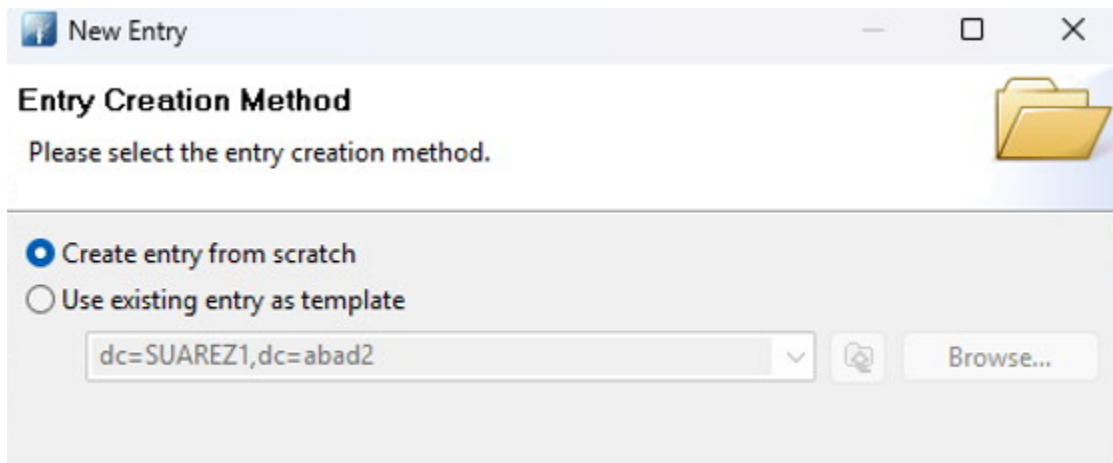
Aceptar

- Apache Directory: ou=equipos

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

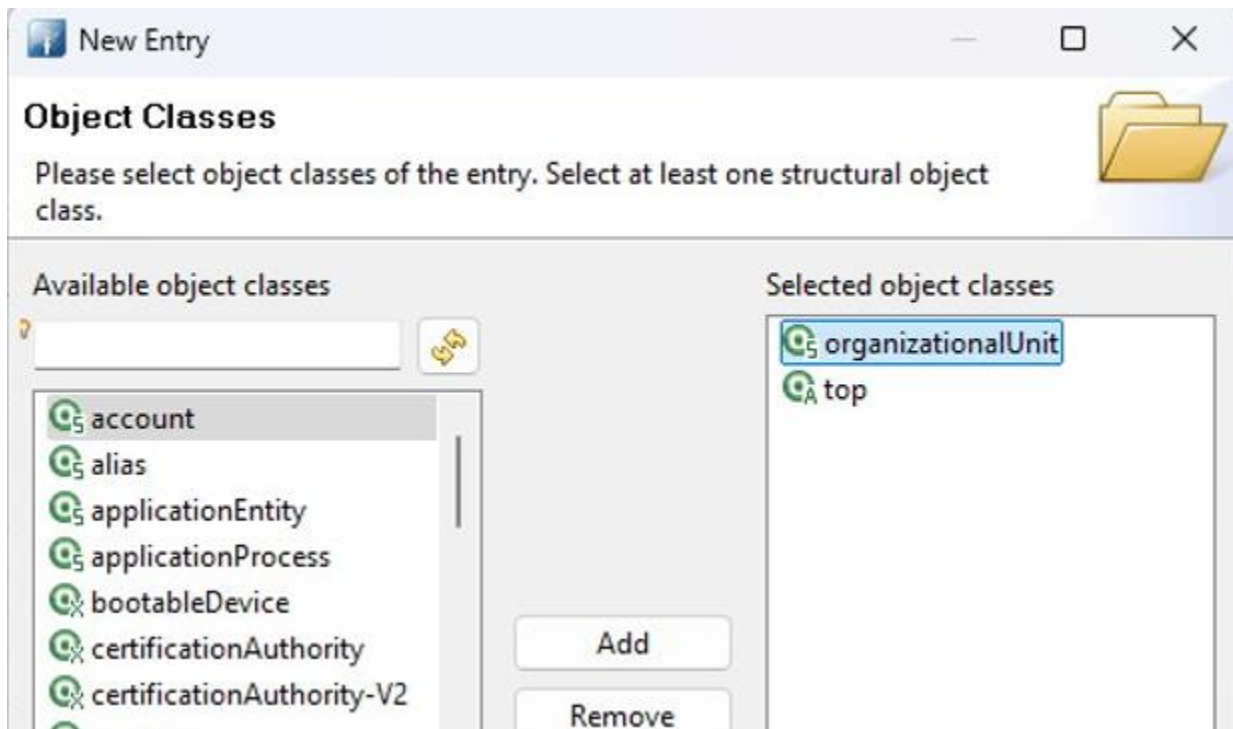


Crear desde cero.



The screenshot shows the 'New Entry' dialog box with the 'Entry Creation Method' tab selected. The title bar reads 'New Entry'. Below the title bar, the tab is labeled 'Entry Creation Method'. The instruction 'Please select the entry creation method.' is displayed. There are two radio buttons: 'Create entry from scratch' (selected) and 'Use existing entry as template'. Below the radio buttons, there is a text box containing 'dc=SUAREZ1,dc=abad2' and a 'Browse...' button. A folder icon is visible in the top right corner.

En “ObjectClasses” debemos elegir “organizationalUnit”.




The screenshot shows the 'New Entry' dialog box with the 'Object Classes' tab selected. The title bar reads 'New Entry'. Below the title bar, the tab is labeled 'Object Classes'. The instruction 'Please select object classes of the entry. Select at least one structural object class.' is displayed. There are two panels: 'Available object classes' on the left and 'Selected object classes' on the right. The 'Available object classes' panel contains a list of object classes: 'account', 'alias', 'applicationEntity', 'applicationProcess', 'bootableDevice', 'certificationAuthority', and 'certificationAuthority-V2'. The 'Selected object classes' panel contains 'organizationalUnit' and 'top'. There are 'Add' and 'Remove' buttons between the panels. A folder icon is visible in the top right corner.

Y después su nombre:

**New Entry**

**Distinguished Name**

Please select the parent of the new entry and enter the RDN.

Parent:  

RDN:  =

DN Preview:

OU creada:

LDAP Browser

ou=equipos,dc=SUAREZ1,dc=abad2

DN: ou=equipos,dc=SUAREZ1,dc=abad2

Attribute Description	Value
<b>objectClass</b>	<b>organizationalUnit (structural)</b>
<b>objectClass</b>	<b>top (abstract)</b>
<b>ou</b>	<b>equipos</b>

DIT

- Root DSE (2)
  - dc=SUAREZ1,dc=abad2 (5+)
    - ou=equipos**
    - ou=grupos
    - ou=People
    - ou=usuarios
    - ou=group

## 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

```
GNU nano 6.2          usuario1.ldif
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
userPassword: suarez987
uidNumber: 10001
gidNumber: 10000
sn: suarez
mail: suarez@sistemas.edu
```



- Alumno 2 Segundo apellido apellido987 ou=usuarios

```
GNU nano 6.2          usuario2.ldif
dn: cn=abad,ou=usuarios,dc=SUAREZ1,dc=abad2
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash
homeDirectory: /home/abad
uid: abad
cn: abad
userPassword: abad987
uidNumber: 10002
gidNumber: 10000
sn: suarez
mail: abad@sistemas.edu
```

- Alumno 3 Nombre nombre987 ou=usuarios

```
GNU nano 6.2          usuario3.ldif
dn: cn=crisobal,ou=usuarios,dc=SUAREZ1,dc=abad2
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash
homeDirectory: /home/crisobal
uid: crisobal
cn: crisobal
userPassword: crisobal987
uidNumber: 10003
gidNumber: 10000
sn: suarez
mail: crisobal@sistemas.edu
```

- Alumno 4 Iniciales iniciales987 ou=usuarios

```
GNU nano 6.2          usuario4.ldif
dn: cn=csa,ou=usuarios,dc=SUAREZ1,dc=abad2
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash
homeDirectory: /home/csa
uid: csa
cn: csa
userPassword: csa987
uidNumber: 10004
gidNumber: 10000
sn: suarez
mail: csa@sistemas.edu
```

## 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.

```
Símbolo del sistema - ssh usuario@10.2.17.10
GNU nano 6.2
dn: cn=abad,ou=usuarios,dc=SUAREZ1,dc=abad2
changetype: modify
replace: uidNumber
uidNumber: 1100
-
add: description
description: Administrador de sistemas_
```

b) Comprueba los cambios usando ldapsearch.

```
Símbolo del sistema - ssh usuario@10.2.17.10
Tu Nombre martes 7 octubre 2025 20:38
[usuario@control01 ~]$sudo su
[sudo] password for usuario:
Tu Nombre martes 7 octubre 2025 20:44
[root@control01 usuario]$nano modificar_usuario.ldif
Tu Nombre martes 7 octubre 2025 20:45
[root@control01 usuario]$ldapmodify -x -D cn=admin,dc=SUAREZ1,dc=abad2 -W -f modificar_usuario.ldif
Enter LDAP Password:
modifying entry "cn=abad,ou=usuarios,dc=SUAREZ1,dc=abad2"

Tu Nombre martes 7 octubre 2025 20:46
[root@control01 usuario]$ldapsearch -xLLL -b dc=SUAREZ1,dc=abad2 uid=abad
dn: cn=abad,ou=usuarios,dc=SUAREZ1,dc=abad2
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash
homeDirectory: /home/abad
uid: abad
cn: abad
gidNumber: 10000
sn: suarez
mail: abad@sistemas.edu
uidNumber: 1100
description: Administrador de sistemas
```

Elimina la descripción del usuario anterior.

```
GNU nano 6.2 borrado_descripcion.ldif
dn: cn=abad,ou=usuarios,dc=SUAREZ1,dc=abad2
changetype: modify
delete: description

Tu Nombre martes 7 octubre 2025 20:46
[root@control01 usuario]$ldapmodify -x -D cn=admin,dc=SUAREZ1,dc=abad2 -W -f borrado_descripcion.ldif
```

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.

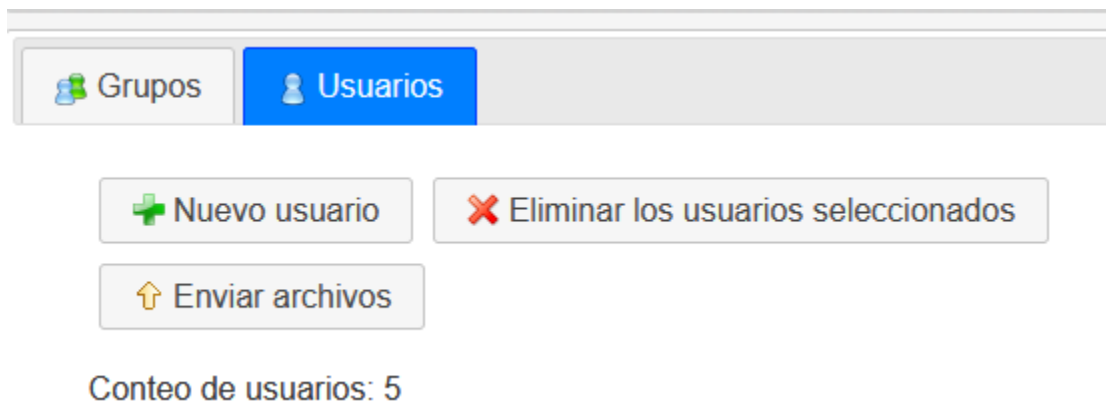
```
[root@control01 usuario]$ldapsearch -xLLL -b dc=SUAREZ1,dc=abad2 uid=csa uidNumber
dn: cn=csa,ou=usuarios,dc=SUAREZ1,dc=abad2
uidNumber: 10004
```

## 8) Gestión con LDAP Account Manager.

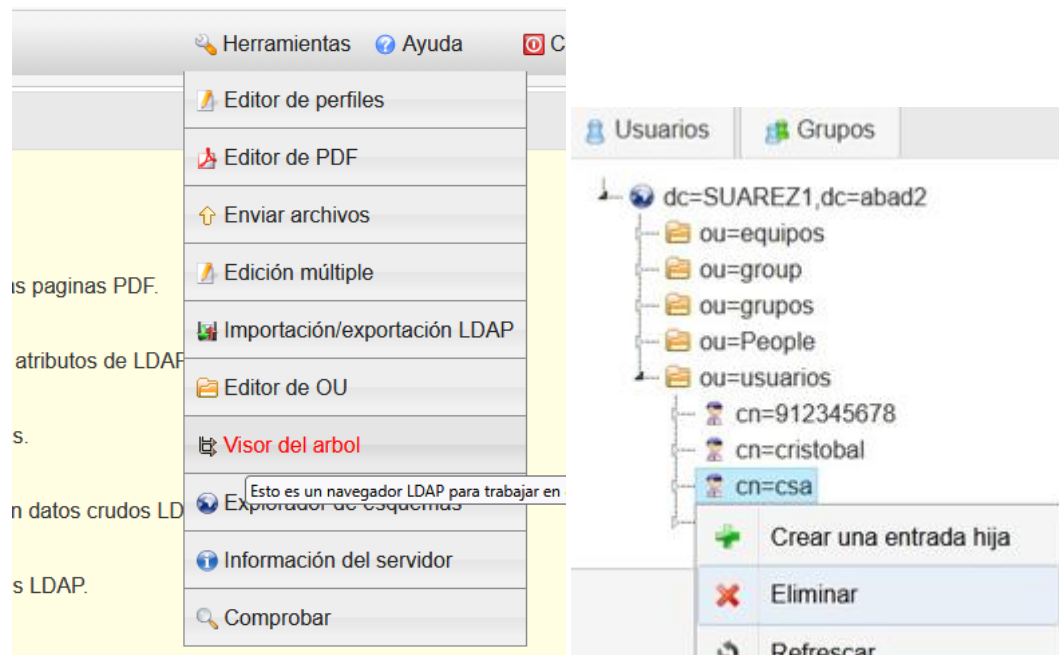
Usa **LDAP Account Manager** para:

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.

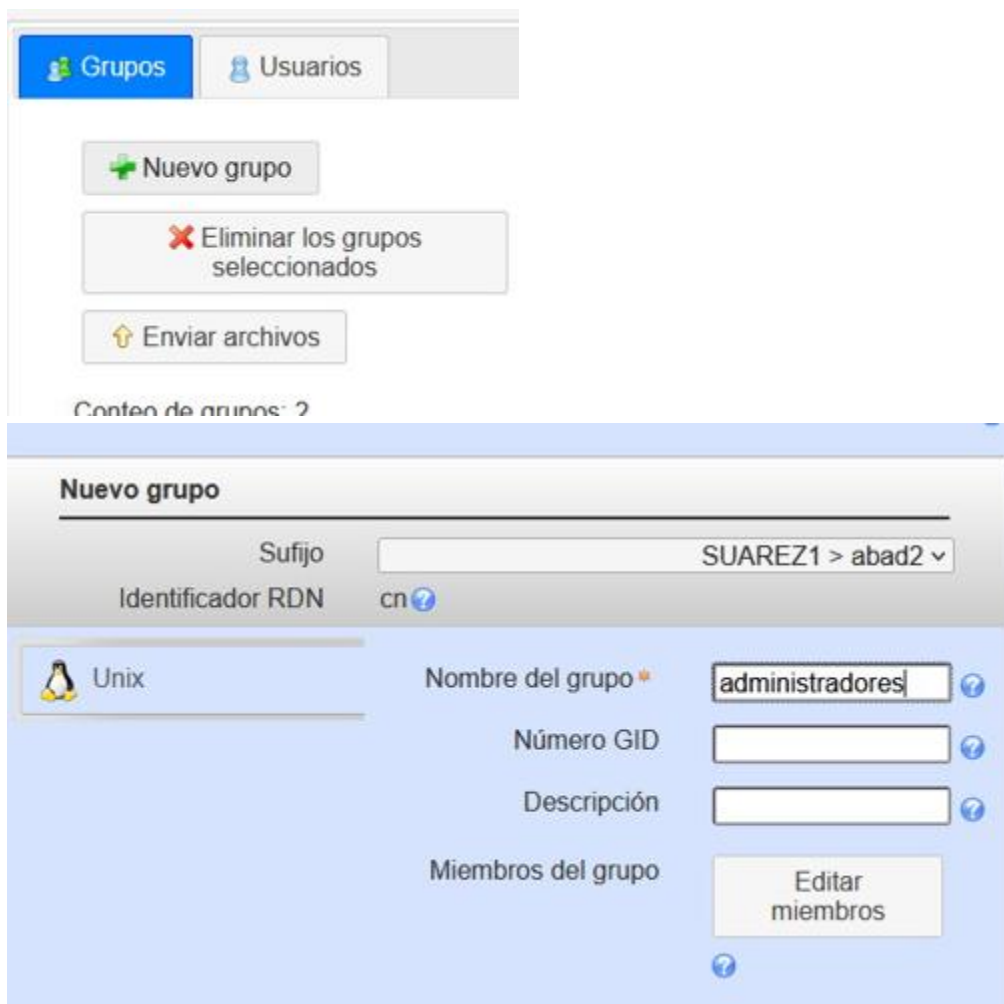
Acciones	
Secuencia de ordenamiento	
<input type="checkbox"/>	Filtrar
<input type="checkbox"/>	
<input type="checkbox"/>	Editar
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	

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

Nombre del usuario *	<input type="text" value="abad"/>	
Nombre común	<input type="text" value="912345678"/>	
Número UID	<input type="text" value="1111"/>	
Gecos	<input type="text"/>	
Grupo primario	<input type="text" value="ASIR1"/>	
Grupos adicionales	<input type="button" value="Editar grupos"/>	
Directorio inicial *	<input type="text" value="/home/abad2"/>	
Intérprete del inicio de sesión	<input type="text" value="/bin/bash"/>	
Contraseña	<input type="button" value="Bloquear contraseña"/> <input type="button" value="Quitar contraseña"/>	



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



### Miembros del grupo

Usuarios seleccionados		Usuarios disponibles
cristobal (cristobal)	←	abad (912345678)
	→	suarez (suarez)

### administradores

Sufijo: SUAREZ1 > abad2

Identificador RDN: cn

Nombre del grupo:













Número GID:

Descripción:

Miembros del grupo:

Grupos Usuarios

**Operación de LDAP exitosa.**  
La cuenta se creó exitosamente.

Acciones	Nombre del grupo	Número GID	Miembros del grupo	Descripción del grupo
Secuencia de ordenamiento	▼▲	▼▲	▼▲	▼▲
<input type="checkbox"/> Filtrar	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>    	administradores	10021	cristobal	
<input type="checkbox"/>    	ASIR1	10002	912345678; suarez	
<input type="checkbox"/>    	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.

Nombre del usuario *	<input type="text" value="csa818"/>	
Nombre común	<input type="text" value="csa818"/>	
Número UID	<input type="text"/>	
Gecos	<input type="text"/>	
Grupo primario	<input type="text" value="administradores"/>	
	<input type="button" value="Crear grupo con mismo nombre"/>	
Grupos adicionales	<input type="button" value="Editar grupos"/>	
Directorio inicial *	<input type="text" value="/home/\$user"/>	
Intérprete del inicio de sesión	<input type="text" value="/bin/bash"/>	

**Operación de LDAP exitosa.**

La cuenta se creó exitosamente.

[Crear una nueva cuenta](#)

[Crear PDF](#)

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

En “Editar” → “Personal”

Datos de contacto		
Número de teléfono	<input type="text" value="959123456"/>	
Número de teléfono del hogar	<input type="text"/>	
Numero de móvil	<input type="text"/>	
Número de fax	<input type="text"/>	
Dirección de correo electrónico	<input type="text" value="csa818@org.com"/>	
Sitio Web	<input type="text"/>	



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

The image shows two screenshots from the Active Directory console. The top screenshot is the 'New Entry' dialog box, which is used to create a new user. It has two panes: 'Available object classes' on the left and 'Selected object classes' on the right. The 'Available object classes' pane lists various classes like 'account', 'alias', 'applicationEntity', etc. The 'Selected object classes' pane shows the classes selected for the new entry: 'inetOrgPerson', 'organizationalPerson', 'person', 'posixAccount', and 'top'. The bottom screenshot is the 'LDAP Browser' window, which displays the directory structure on the left and the details of the selected entry on the right. The directory structure shows a hierarchy starting from 'DIT' down to 'ou=usuarios (5)', where the entry 'cn=Apache' is selected. The details pane on the right shows the entry's DN as 'cn=Apache,ou=usuarios,dc=SUAREZ1,dc=abad2' and lists its attributes and values.

**New Entry Dialog:**

Object Classes

Please select object classes of the entry. Select at least one structural object class.

Available object classes

- account
- alias
- applicationEntity
- applicationProcess
- bootableDevice
- certificationAuthority
- certificationAuthority-V2

Selected object classes

- inetOrgPerson
- organizationalPerson
- person
- posixAccount
- top

**LDAP Browser:**

DN: cn=Apache,ou=usuarios,dc=SUAREZ1,dc=abad2

Attribute Description	Value
objectClass	inetOrgPerson (structural)
objectClass	organizationalPerson (structural)
objectClass	person (structural)
objectClass	posixAccount (auxiliary)
objectClass	top (abstract)
cn	Apache
gidNumber	10021
homeDirectory	/home/Apache
sn	suarez
uid	Apache
uidNumber	100089

## 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.

```
GNU nano 6.2 /etc/hosts *
127.0.0.1    localhost
10.2.17.105  ldap-cliente.SUAREZ1.abad2 ldap-cliente
10.2.17.10   control01.SUAREZ1.abad2

# 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
```

Comprobamos haciendo PING al servidor:

```
Tu Nombre  sábado 11 octubre 2025 15:36
[root@ldap-cliente usuario]$ping control01.SUAREZ1.abad2
PING control01.SUAREZ1.abad2 (10.2.17.10) 56(84) bytes of data.
64 bytes from control01.SUAREZ1.abad2 (10.2.17.10): icmp_seq=1 ttl=64 time=0.985 ms
64 bytes from control01.SUAREZ1.abad2 (10.2.17.10): icmp_seq=2 ttl=64 time=0.588 ms
64 bytes from control01.SUAREZ1.abad2 (10.2.17.10): icmp_seq=3 ttl=64 time=0.557 ms
```

### 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**.



Configuración de 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://10.2.17.10/

<Aceptar>

Nombre dominio.

Configuración de 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=SUAREZ1,dc=abad2

<Aceptar>

Protocolo 3

Configuración de 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

<Aceptar>



Configuración de ldap-auth-config

This option will allow you to make password utilities that use pam to behave like you would be changing local passwords.

The password will be stored in a separate file which will be made readable to root only.

If you are using NFS mounted /etc or any other custom setup, you should disable this.

Make local root Database admin:

☒ <Yes> ☐ <No>

Configuración de ldap-auth-config

Choose this option if you are required to login to the database to retrieve entries.

Note: Under a normal setup, this is not needed.

Does the LDAP database require login?

☐ <Yes> ☒ <No>

Cuenta con privilegios:

Configuración de 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:

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:

```
Tu Nombre sábado 11 octubre 2025 15:51
[root@ldap-cliente usuario]$ nano /etc/nsswitch.conf
```

```

GNU nano 6.2 /etc/nsswitch.conf *
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.
#

passwd:      files ldap
group:       files ldap
shadow:      files ldap_
gshadow:     files

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

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

netgroup:    nis

```

Nos debe mostrar los usuarios del ldap.

```
suarez:x:10001:10000:suarez:/home/suarez:/bin/bash
abad:x:1111:10002:912345678:/home/abad2:/bin/bash
cristobal:x:10003:10021:cristobal:/home/cristobal:/bin/bash
csa818:*:10023:10021:csa818:/home/csa818:/bin/bash
Apache:*:100089:10021:Apache:/home/Apache:
```

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

```
session optional                                pam_umask.so
# and here are more per-package modules (the "Additional" block)
session required                                pam_unix.so
session optional                                pam_555.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
```

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

```
cristobal@ldap-cliente: ~  
Tu Nombre: sábado 11 octubre 2025 15:59  
[root@ldap-cliente usuario]$sudo su - cristobal  
Creando directorio «/home/cristobal».  
cristobal@ldap-cliente:~$
```