Trabajo de investigación técnica: Implantación de dominios con OpenLDAP y gestión con Apache Directory Studio

Descripción general:

Vas a realizar un trabajo de investigación práctica centrado en la instalación, configuración y gestión de un dominio LDAP con OpenLDAP, así como su integración con NFS y herramientas gráficas. Este trabajo te permitirá entender cómo se centraliza la gestión de usuarios y grupos en entornos reales.

Objetivos del trabajo:

- Comprender cómo se instala y configura un servidor OpenLDAP.

- Investigar cómo se estructura un dominio LDAP con unidades organizativas, usuarios y grupos.

- Configurar un cliente para autenticación LDAP.

- Integrar el uso de NFS como sistema de directorios personales.

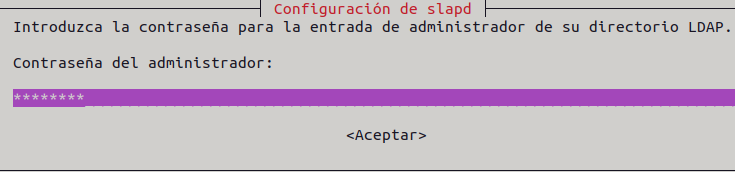
- Utilizar Apache Directory Studio para gestionar gráficamente el directorio LDAP.

Fases del trabajo:

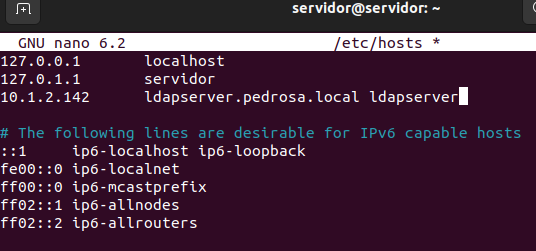
**1. Investigación sobre la instalación de OpenLDAP**

OpenLDAP es una implementación libre del protocolo LDAP. Se utiliza para almacenar información jerárquica de forma centralizada: usuarios, grupos, dispositivos, etc.

* **sudo apt update**
* **sudo apt install slapd ldap-utils**



Dentro del archivo /etc/hosts, añadimos una nueva línea que relacione la dirección IP estática del servidor con los nombres lógicos que tenemos previsto utilizar.

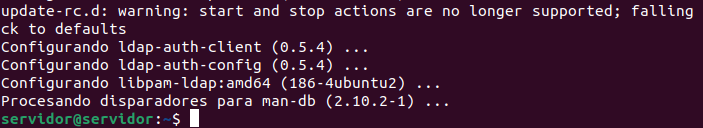


A continuación, instalaremos la librería NSS para LDAP.

* **sudo apt-get install libnss-ldap -y**

Durante la configuración:

1. Omitir configuración inicial: ❌ (seleccione **No**)
2. Nombre de dominio: pedrosa.local → se convierte en dc=pedrosa,dc=local
3. Organización: Pedrosa
4. Contraseña del administrador LDAP (admin): **elige una segura**
5. Base de datos a borrar: ✔ Sí
6. Mover antigua base de datos: ❌ No



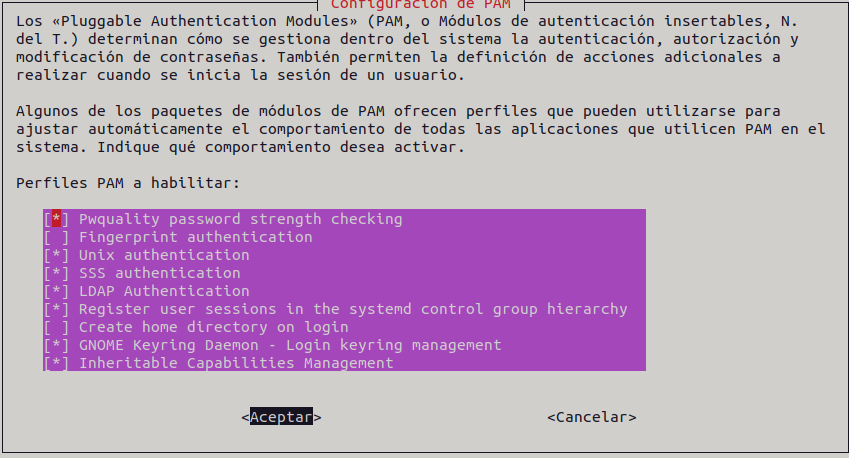
**Configurar la autenticación para los clientes**

* **sudo apt install libnss-ldap libpam-ldap ldap-utils nslcd**

La ejecución de este comando no debe ofrecer ningún tipo de error

A continuación, deberemos actualizar la configuración de las políticas de autenticación predeterminadas de PAM, lo que conseguimos con el siguiente comando:

* **sudo pam-auth-update**



Una vez acabada la configuración automática, podremos hacer algunos cambios complementarios editando el archivo /etc/ldap.conf.

Una vez que se abra el editor, podremos ajustar algunos de los valores del documento, pero, sobre todo, comprobaremos que son correctos los siguientes datos:

host 10.1.2.142 base

dc=pedrosa,dc=local

uri ldapi://10.1.2.142/

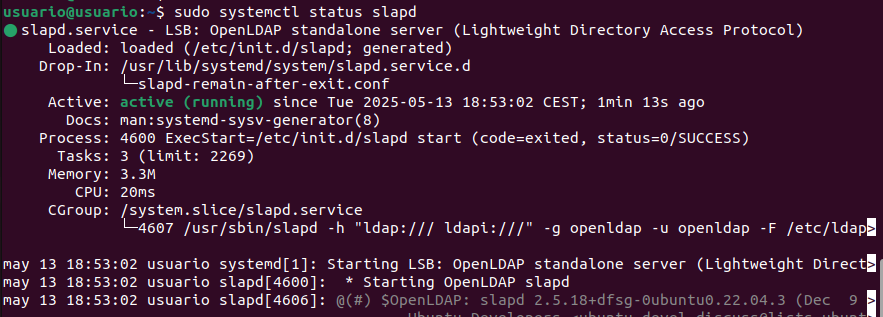
rootbinddn cn=admin,dc=pedrosa,dc=local

ldap\_version 3

bind\_policy soft

**2. Configuración básica del dominio**

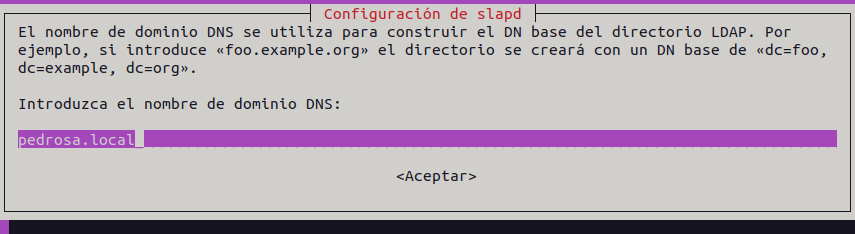
Verificar que OpenLDAP funciona:



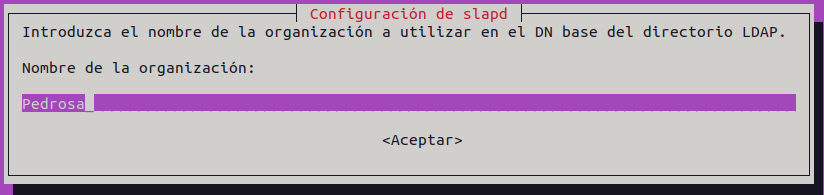
Como hemos dicho más arriba, el último paso en la configuración del servidor LDAP será establecer algunos parámetros en la configuración de este demonio

* **sudo dpkg-reconfigure slapd**

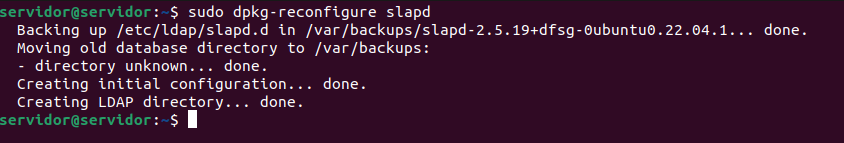
A continuación, deberemos escribir el nombre DNS que utilizamos para crear el DN base del directorio LDAP



Después, escribiremos el nombre de la entidad en la que estamos instalando el directorio LDAP.



Luego de aplicar la contraseña del administrador y dejar las siguientes opciones por defecto, en último paso se cierra el asistente y volvemos a la consola.

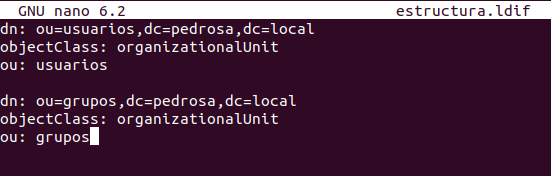


Con esto habremos terminado la configuración del servidor LDAP. Ahora está listo para autenticar usuarios.

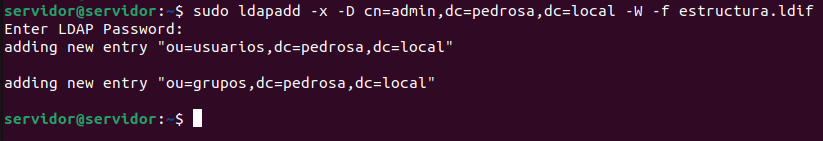
**3. Creación de la estructura organizativa**

Una vez configurado el servidor, deberemos configurar la estructura básica del directorio. Es decir, crearemos la estructura jerárquica del árbol

* Creamos un archivo LDIF (estructura.ldif):

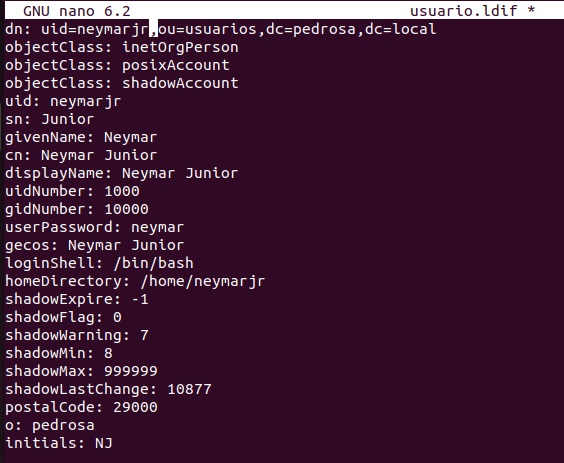


A continuación, deberemos añadir la información a la base de datos OpenLDAP. Como sabemos, esto se hace con el comando ldapadd:

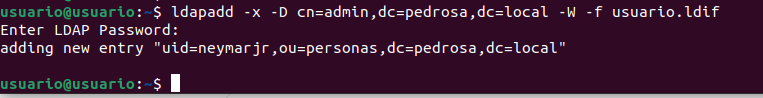


**4. Creación de usuarios**

* Archivo usuario.ldif:



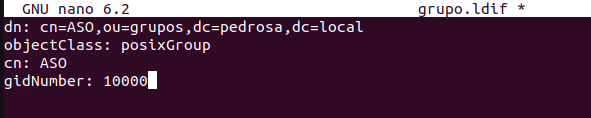
* Añadir usuario:



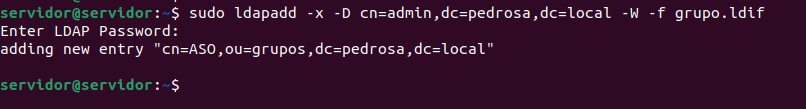
**Añadir un grupo**

Para añadir el grupo, repetimos de nuevo el proceso anterior:

* Archivo grupo.ldif:



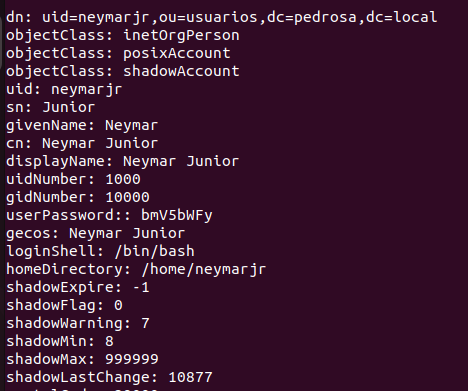
* Añadir grupo:



Con esto, ya tendremos en la base de datos un nuevo usuario y un nuevo grupo.

Ahora podemos comprobar que el contenido anterior se ha añadido correctamente. Para lograrlo podemos utilizar, por ejemplo, el comando ldapsearch , que nos permite hacer una búsqueda en el directorio:

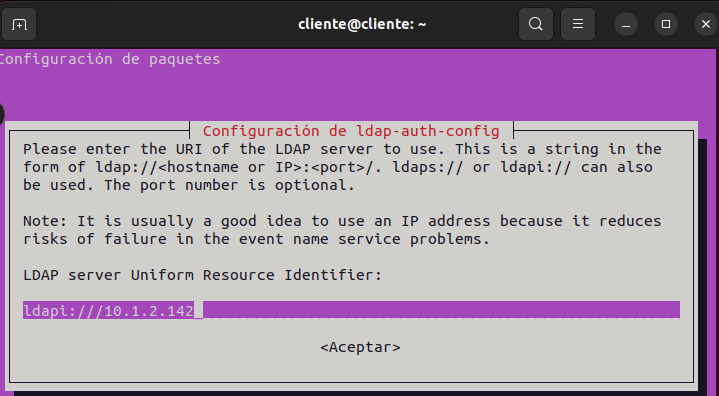
* **sudo slapcat**



**5. Unión de clientes al dominio LDAP**

1. Instalar paquetes necesarios
   * **sudo apt-get install libpam-ldap libnss-ldap nss-updatedb libnss-db nscd ldap-utils -y**
2. Configuración

* URI del servidor: ldap://IP-del-servidor



* DN base: dc=pedrosa,dc=local
* Versión LDAP: 3
* Administrador: cn=admin,dc=pedrosa,dc=local
* Contraseña: la que configuraste

1. Editar el archivo /etc/ldap.conf

uri ldap://10.1.2.142/

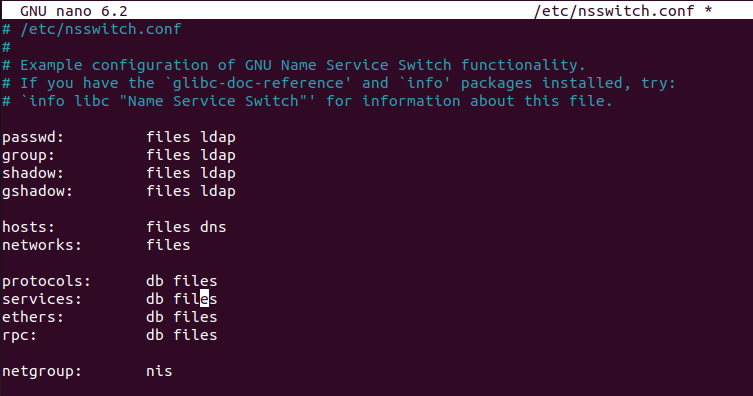
pam\_password crypt

bind\_policy soft

1. Editar el archivo /etc/ldap/ldap.conf



1. Editar el archivo /etc/nsswitch.conf

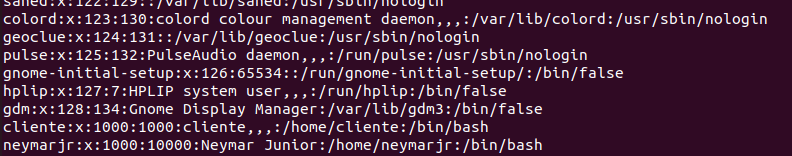


Una vez guardados los archivos, actualizaremos pam mediante el siguiente comando:

* **sudo nss\_updatedb ldap**

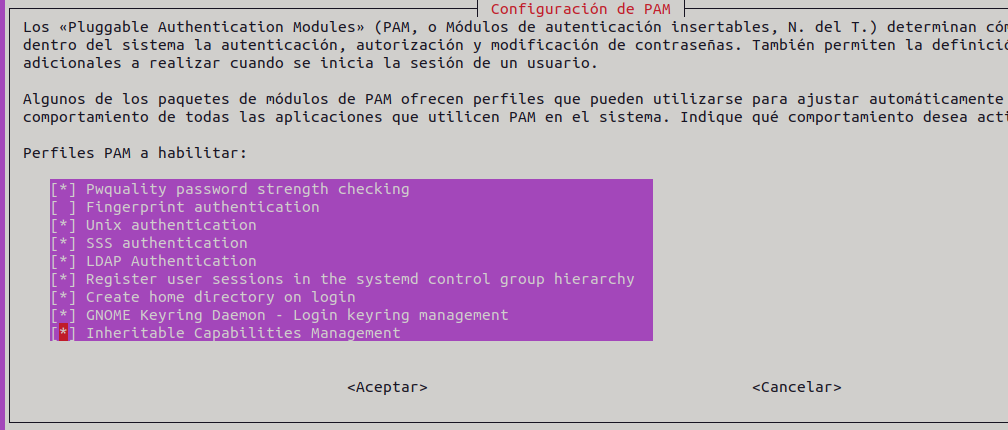
Si todo ha ido bien, podemos utilizar el comando getent, que nos permite obtener entradas de varios archivos de texto del sistema

* **getent passwd**



Lo siguiente será actualizar la configuración de las políticas de autenticación predeterminadas de PAM, lo que conseguimos con el siguiente comando:

* **sudo pam-auth-update**

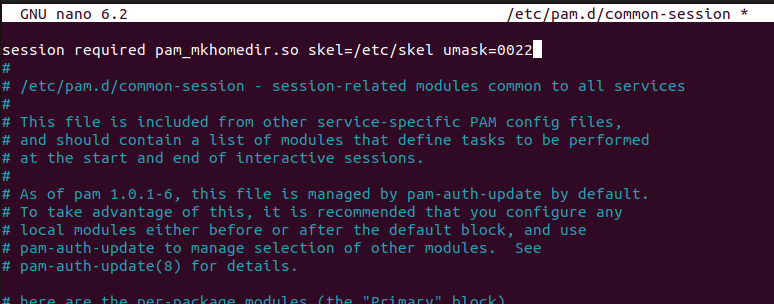


1. Habilitar autenticación LDAP:

Si queremos que la carpeta se cree automáticamente cuando el usuario inicie sesión por primera vez en un equipo, deberemos hacer uso de un módulo PAM llamado pam\_mkhomedir. Esto lo conseguimos haciendo una pequeña modificación en el archivo /etc/pam.d/common-session del cliente.

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

Cuando se abra el editor, añadiremos una nueva línea al principio del archivo con este contenido:



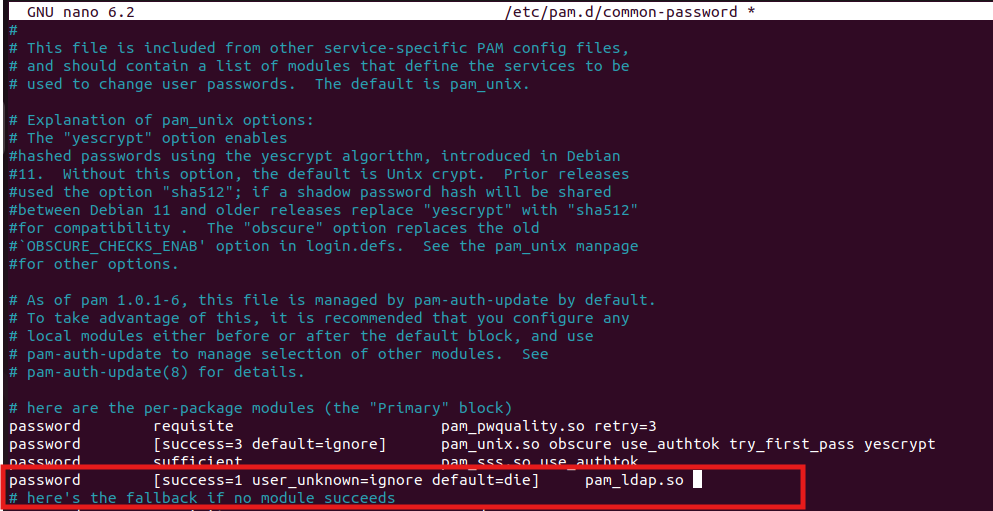
Otro inconveniente que tiene la configuración actual es que los usuarios LDAP no podrán cambiar sus propias contraseñas.

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

Cuando veamos el contenido del archivo, buscaremos una línea en concreto:

password [success=1 user\_unknown=ignore default=die] pam\_ldap.so use\_authtok try\_first\_pass

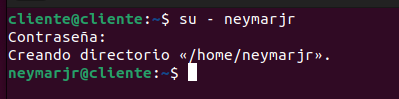
y eliminamos su parte final, de modo que quede así:



La forma más sencilla de comprobar que podemos iniciar sesión en el servidor usando el siguiente comando:

* **su - neymarjr**

Aplicamos el comando y nos pedirá la contraseña del usuario, en mi caso “neymar”



Aquí podemos comprobar que:

* durante el inicio de sesión se crea el directorio /home para la cuenta
* nos encontramos en el equipo cliente.
* estamos iniciando sesión con un usuario LDAP
* el inicio de sesión se produce satisfactoriamente

**6. Integración con NFS**

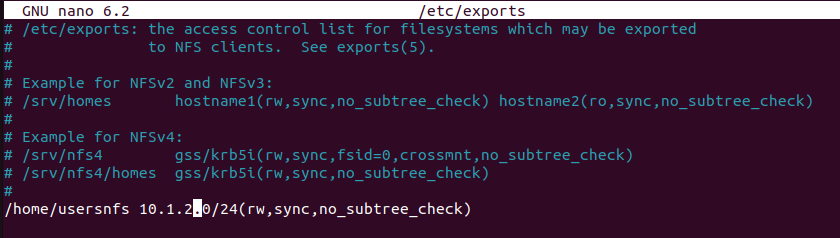
Comenzaremos instalando el siguiente paquete NFS

* **sudo apt install nfs-kernel-server -y**

A continuación vamos a crear el directorio para los usuarios LDAP, este lo llamaremos usersnfs.

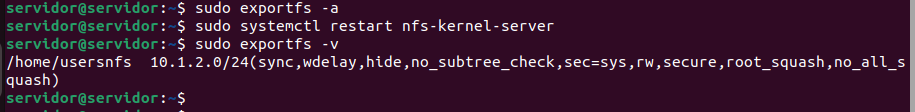


Editamos el fichero /etc/exports y añadimos la siguiente línea:



Esto permite a los clientes de la red 10.1.2.0/24 acceder al directorio con permisos de lectura/escritura

A continuación exportamos los directorios compartidos



Una vez configurado el servidor accedemos a la máquina cliente para ejecutar los siguientes comandos:

* **sudo apt update**
* **sudo apt install nfs-common -y**

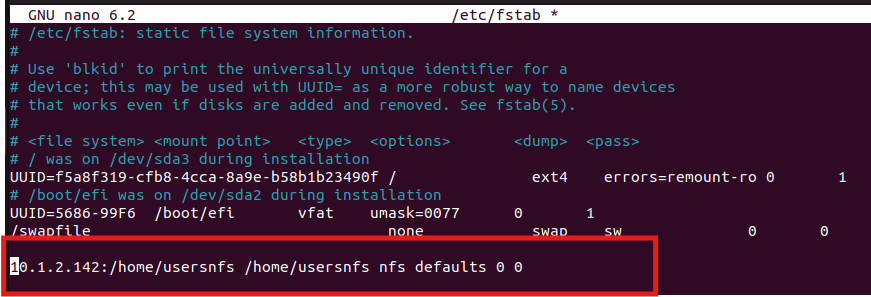
A continuación, crearemos el punto de montaje con el siguiente comando:

* **sudo mkdir -p /home/usersnfs**

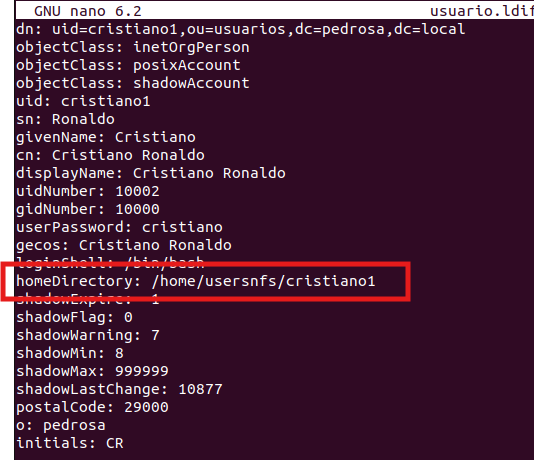
Ahora prueba a montarlo manualmente



Una vez montado, editaremos el archivo de configuración /etc/fstab, en el agregaremos al final del archivo la siguiente línea:



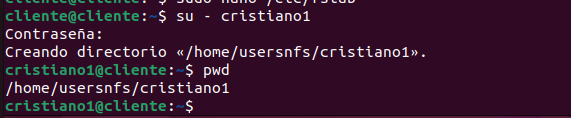
Para esta conexión debemos tener en cuenta que debemos modificar homeDirectory, por ello yo he decidido crear un nuevo usuario llamado cristiano1 con el siguiente directorio:



Guardamos el archivo , creamos el usuario y ejecutamos los siguientes comandos:

* **sudo exportfs -rav**
* **sudo systemctl restart nfs-kernel-server**

Una vez configurado todo, solo nos queda la conexión y comprobación de este usuario, desde la máquina cliente usaremos el comando visto anteriormente para conectarnos a el servidor. Si todo va bien deberemos ver la siguiente secuencia



Además podemos comprobar esto creando un archivo de prueba y, desde el servidor, ver el resultado



Servidor:



**7. Administración gráfica con Apache Directory Studio**

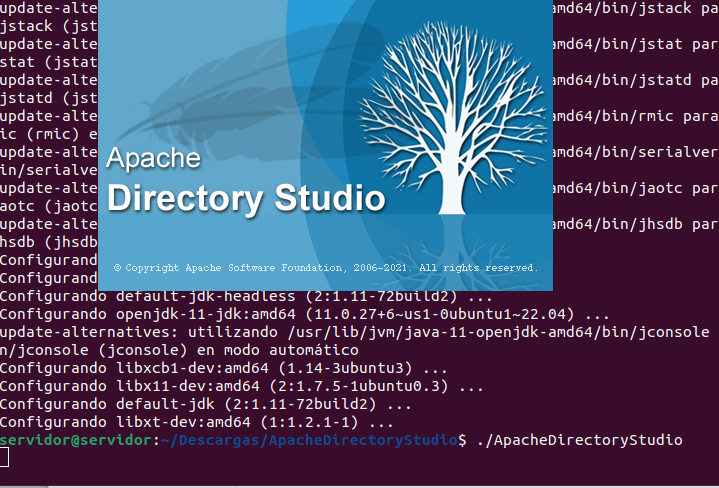
Para este último apartado comenzaremos instalando Apache Directory Studio manualmente, para ello entraremos en el siguiente enlace:

* <https://directory.apache.org/studio/download/>

Elige la versión para tu sistema operativo e instala java con el siguiente comando:

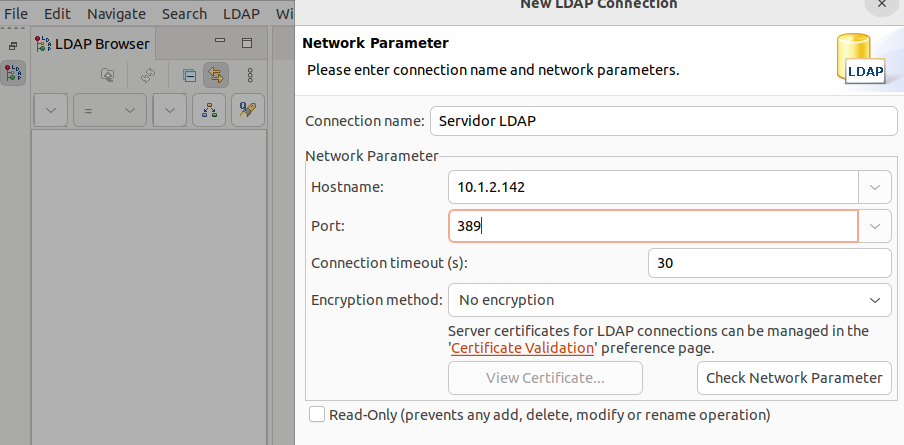
* **sudo apt install default-jdk**

Inicia la aplicación

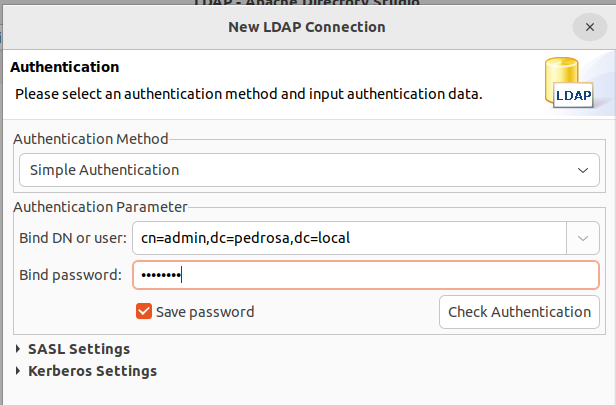


1. **Abre Apache Directory Studio**
2. Ve a **File → New → LDAP Connection**
3. Se abre un asistente. Rellénalo así:

* **Connection name**: Servidor LDAP
* **Hostname**: la IP del servidor LDAP
* **Port**: normalmente 389 (sin cifrado) o 636 (con LDAPS)

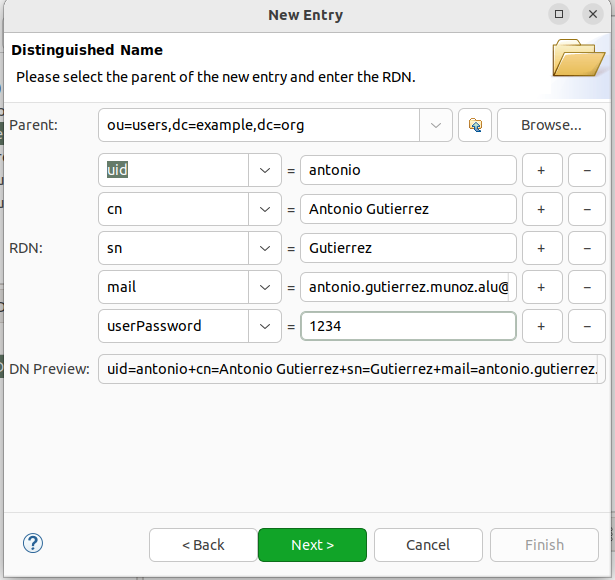


En la siguiente pantalla:



Para **crear un usuario**:

1. Clic derecho en ou=usuarios → **New → New Entry**
2. Elige plantilla inetOrgPerson
3. Rellena los campos (uid, sn, cn, etc.)
4. Acepta y guarda



Para **crear un grupo:**

* + Haz clic derecho en ou=users y selecciona New Entry.
  + Selecciona Create entry from scratch y usa groupOfNames como objectClass.
  + Define cn como el nombre del grupo (superusers, bloggers, readers).
  + Agrega member para vincular usuarios al grupo

