PRÁCTICA OPENLDAP

¿Que vamos a hacer ?

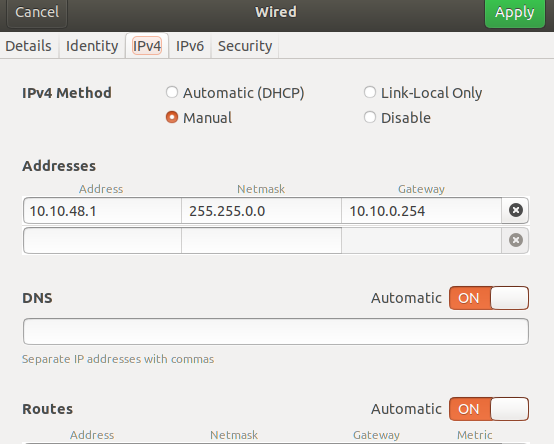
En esta práctica tenemos que crear un Dominio en Linux con openLDAP para integrar en el clientes windows y linux , pudiendo validar clientes Linux.

¿Que es OpenLDAP?

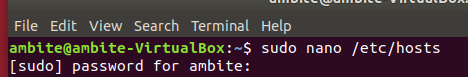
**OpenLDAP** es una implementación libre y de [código abierto](https://es.wikipedia.org/wiki/C%C3%B3digo_abierto) del protocolo Lightweight Directory Access Protocol ([LDAP](https://es.wikipedia.org/wiki/LDAP)) desarrollada por el proyecto OpenLDAP.

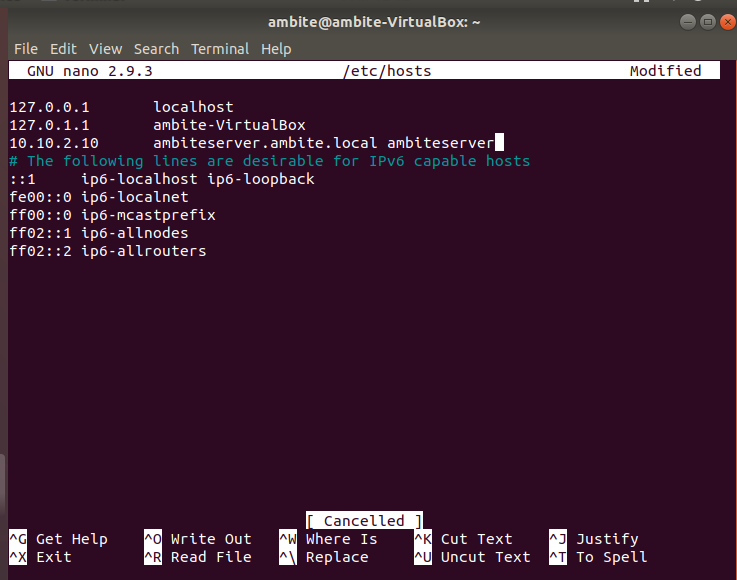
LDAP, es un protocolo que ofrece el acceso a un servicio de directorio implementado sobre un entorno de red, con el objeto de acceder a una determinada información. Puede ejecutarse sobre TCP/IP o sobre cualquier otro servicio de transferencia orientado a la conexión.

### CREAR MAQUINA LINUX, PONERLE IP FIJA



Tenemos que editar el fichero que tenemos en **/etc/hosts** aquí le ponemos la Ip que le daremos al servidor y el nombre .





Tenemos que añadir la ip de la máquina que va a funcionar como controlador de dominio, con el nombre que le vamos a dar al dominio .

En este fichero se ve la relación ip nombre de máquina , de esta form a el usuario no necesitará recordar las ips , solo los nombres de los hosts.

Normalmente se incluyen todos los de los equipos de la red local para que, el ordenador al comunicarse no tenga que recurrir a DNS para resolver los nombres de máquinas.

Lo siguiente será instalar la librería NSS para LDAP, que nos ofrece una interfaz para acceder y configurar las bases de datos utilizadas para almacenar cuentas de usuario.

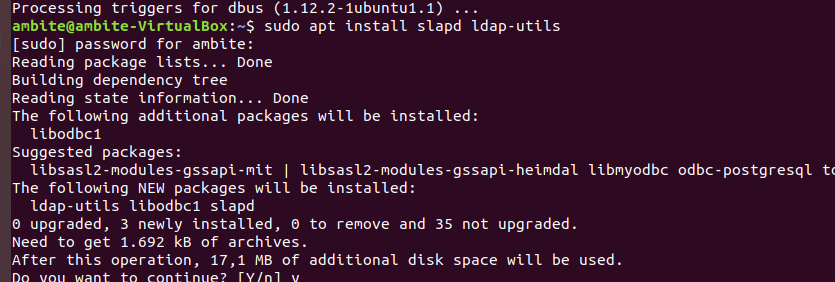
### INSTALAR SERVIDOR SLAPD

Para ello usaremos el siguiente comando.

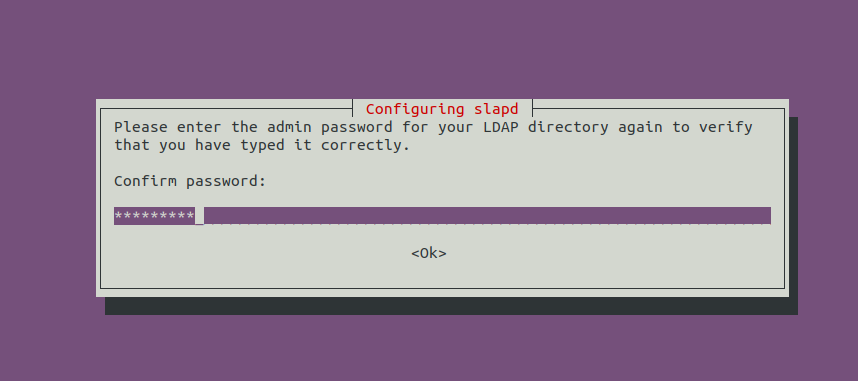
* **sudo apt install slapd ldap-utils -y**

He tenido problemas por no haber actualizado antes así que actualizamos con

* **sudo apt get update**
* **sudo apt get upgrade**

****

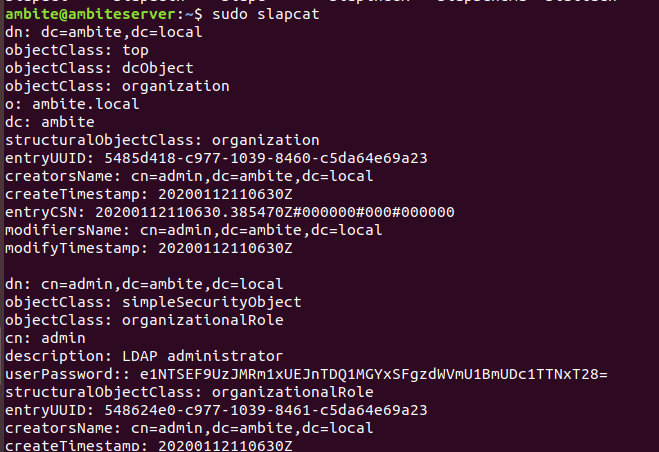
**Mientras se está instalando te pide que pongas la contraseña de administrador.**

****

**Para comprobar que esto está bien , podemos ejecutar el comando .**

* **sudo slapcat**

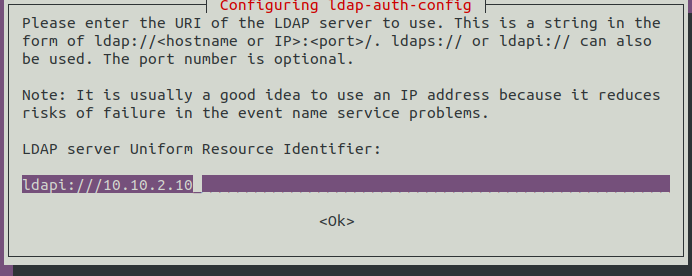
El objetivo de este comando consiste en obtener la información de la base de datos LDAP y su salida se produce en formato LDIF, lo que nos facilitará exportar la estructura del directorio LDAP o, sencillamente, obtener una copia de respaldo de su contenido, sólo con redirigir su salida a un archivo. Hablaremos de los archivos LDIF más adelante

****

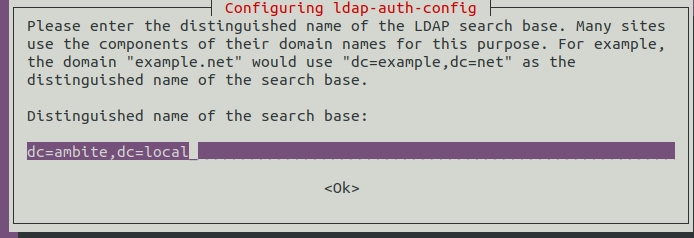
* **sudo apt install libnss-ldap -y**

Lo primero es configurar la dirección ip del servidor.

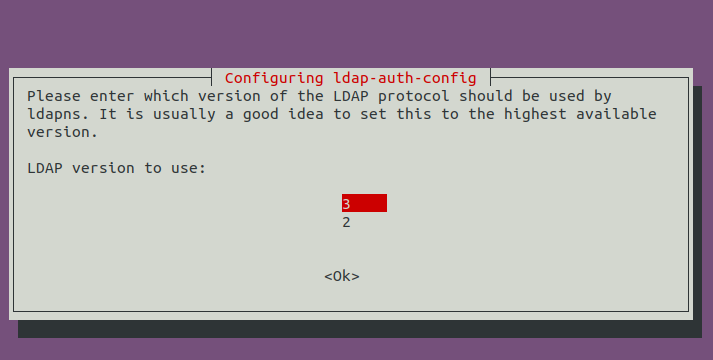
He tenido que cambiarla con respecto a la inicial porque en clase alguien la estaba usando y no tenia red asi que le he dado a la maquina y servidor la **ip 10.10.88.1, también la he cambiado en /etc/hosts .**

****

Después ponemos el nombre global único dc =álvaro, dc=local

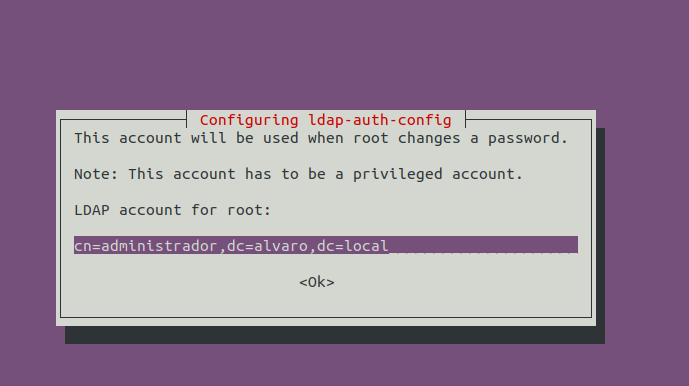


Versión de protocolo LDAP, vamos a usar el más nuevo .

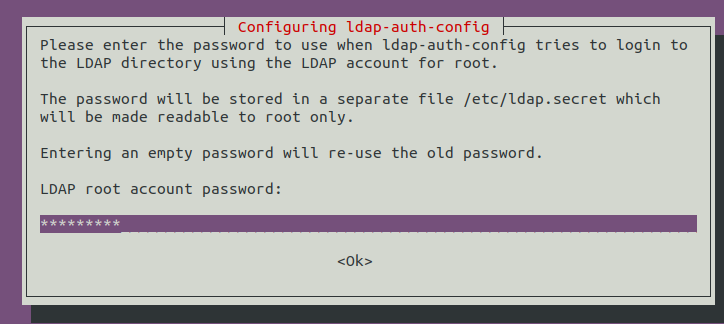


Lo siguiente es especificar si las utilidades que usen PAM, para guardar contraseñas tienes que usar superusuario par acceder a ellas .

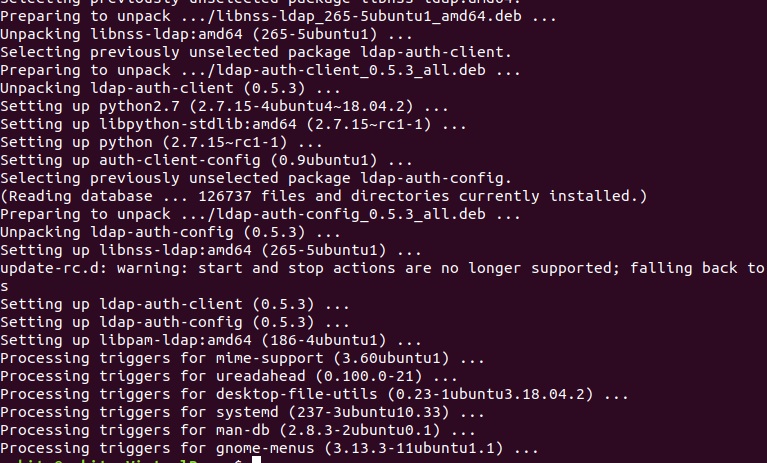
Ahora creamos la cuenta administradora para gestionar las contraseñas de LDAP. .



Por último le añadimos la contraseña , a la cuenta.



Vemos que todo se ha configurado sin errores .



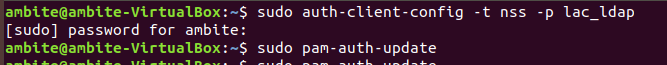
Si en un futuro hubiera que tocar algo de esta configuración tenemos el siguiente comando.

* **sudo dpkg-configure ldap-auth-config**

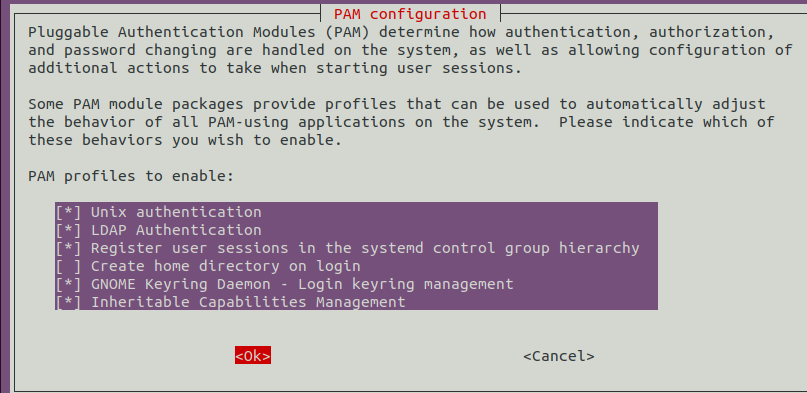
### CONFIGURAMOS AUTENTIFICACIÓN DE LOS CLIENTES

Lo primero que hacemos es utilizar auth-client-config, un script que ayuda a modificar los archivos PAM NSS.

* **sudo auth-client-config -t nss -p lac\_ldap**



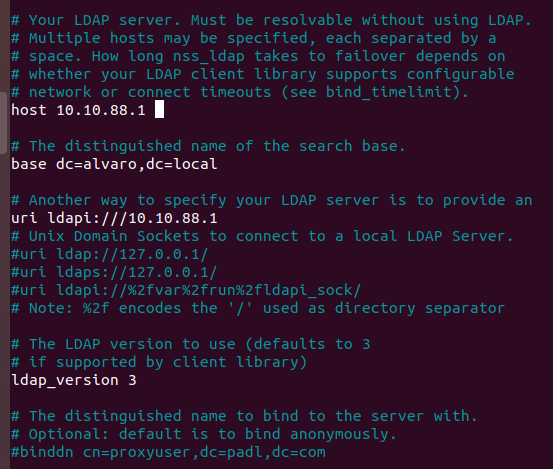
* sudo pam-auth-update

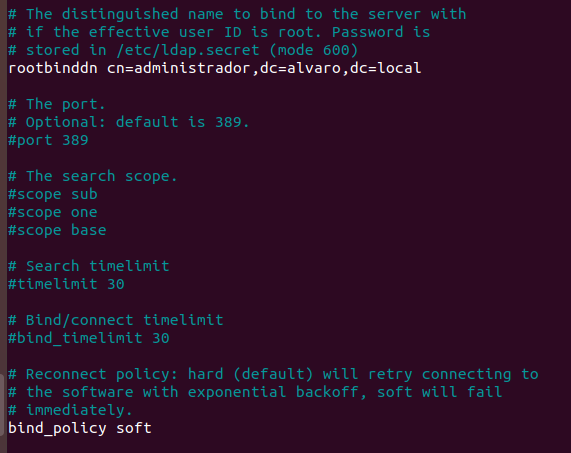


Después de esto vamos a configurar el archivo /etc/ldap.conf

Verificamos que todos los datos del servidor estén correctamente configurados .







Es importante que la configuración esté bien , ya que si no nos dará problemas al validar los usuarios .

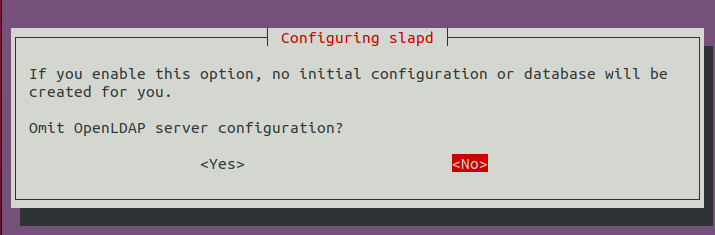
### CONFIGURACIÓN DE SLAPD

Para ello usaremos el siguiente comando como antes .

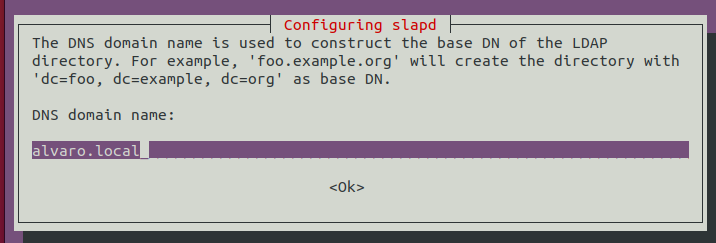
* **sudo dpkg-reconfigure slapd**

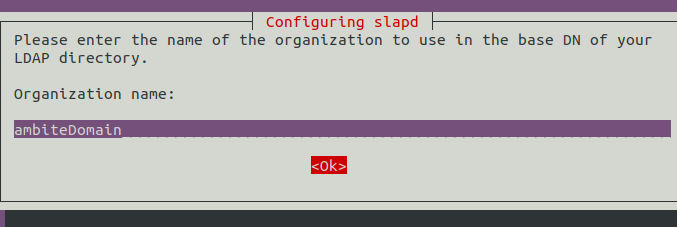


Primero te pide que le verifiques que quieres hacer camino y tienes que darles no.



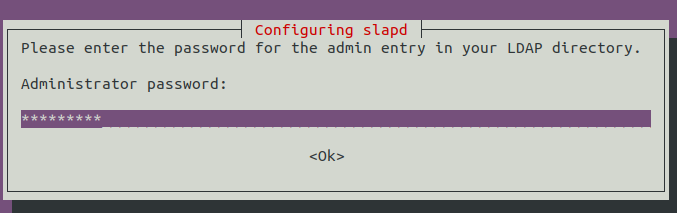
Nombre DNS para el DN base de LDAP



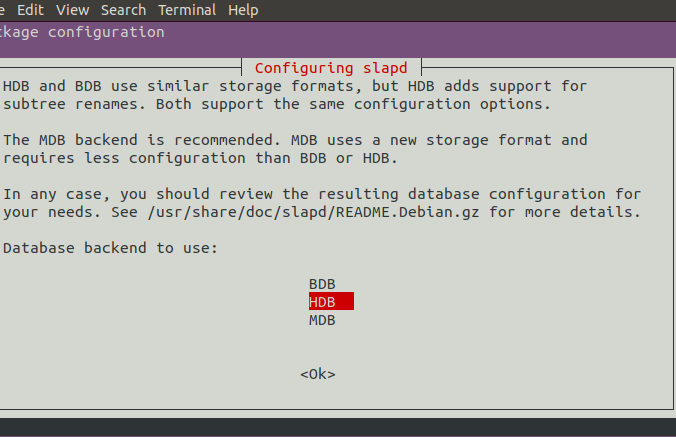


Nombre de la entidad en la que estamos instalando el directorio LDAP.

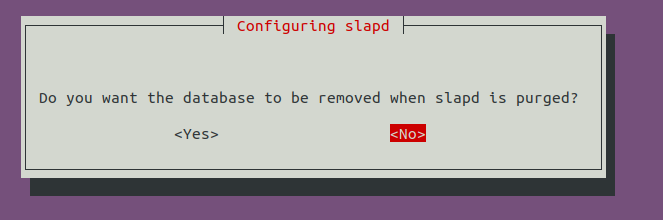
Escribimos la contraseña del administrador del directorio.



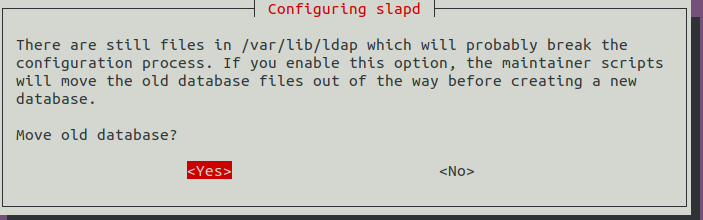
Lo siguiente es elegir el motor de base de datos elegimos HDB porque nos permite modificaciones futuras de los árboles a subárboles.



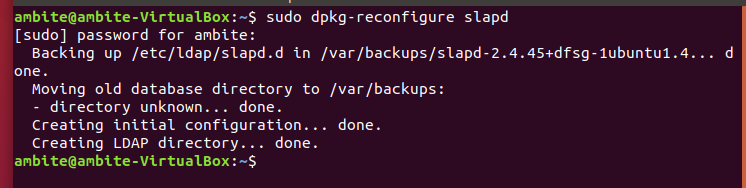
Si queremos borrar la base de datos anterior .



Ahora nos pregunta si queremos cambiarla de sitio.



Por último vemos que todo se realiza sin errores .



### CREAR UNA ESTRUCTURA DE DIRECTORIO.

Una vez configurado el servidor, deberemos configurar la estructura básica del directorio. Es decir, crearemos la estructura jerárquica del árbol (DIT – Directory Information Tree).

Una de las formas más sencillas de añadir información al directorio es utilizar archivos LDIF (LDAP Data Interchange Format). En realidad, se trata de archivos en texto plano, pero con un formato particular que debemos conocer poder construirlos correctamente

El formato básico de una entrada es así:

# comentario

dn: <nombre global único>

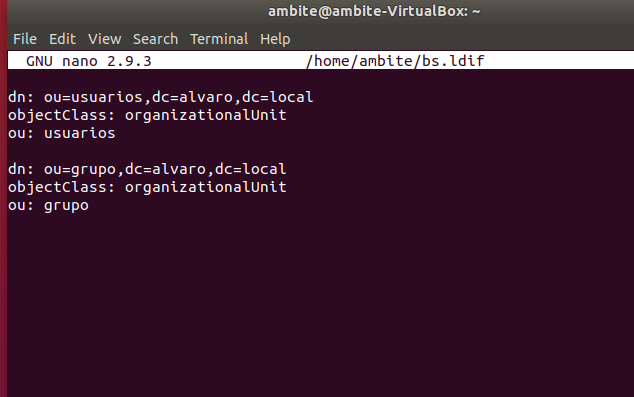
<atributo>: <valor>

<atributo>: <valor>

Con estas pautas ahora tenemos que crear el archivo .

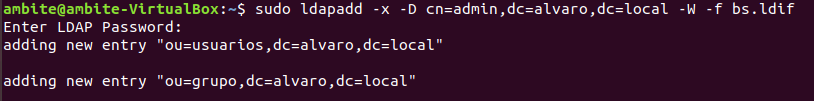
[**EN ESTOS ARCHIVOS HAY QUE TENER MUCHOS CUIDADO CON LOS ESPACIOS,LOS DOS PUNTOS SIEMPRE PEGADOS A CADA CLASE ME HAN DADO VARIOS PROBLEMAS]**

**Yo lo voy a llamar sudo nano ~/bs.ldif**

****

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

* **sudo ldapadd -x -D cn=admin,dc=alvaro,dc=local -W -f bs.ldif**

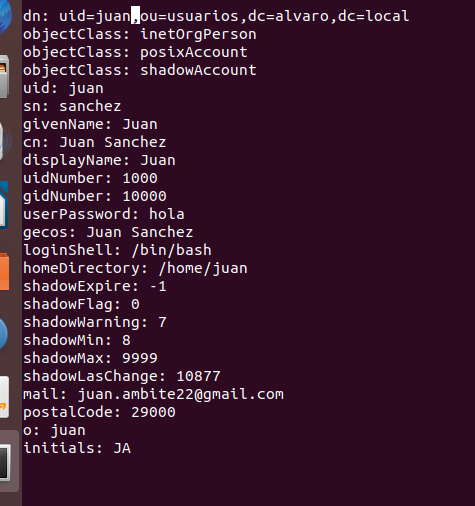
****

Por último tenemos que.

### AÑADIR USUARIO Y UN GRUPO .

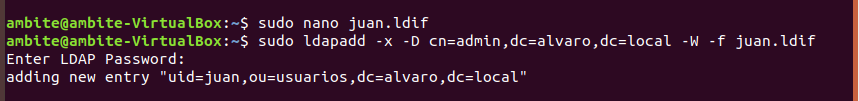
Para añadir un usuario tenemos que crear un archivo como antes , creamos un archivo .ldif y lo añadimos a la base de datos .

El archivo tiene que tener estos campos.

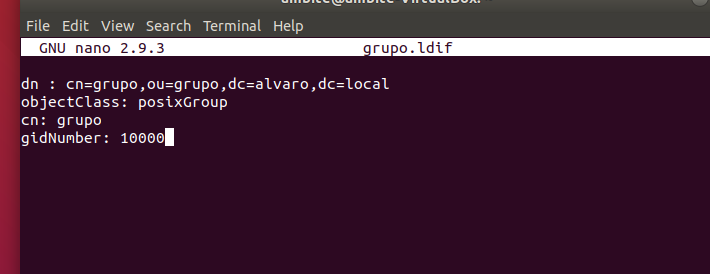


Después añadimos como antes la información a la base de datos con el siguiente comando.

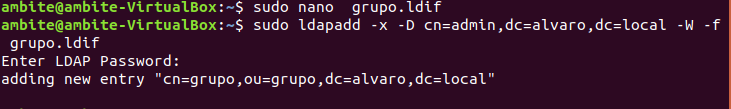
* **sudo ldapadd -x -D cn=admin,dc=alvaro,dc=local -W -f juan.ldif**



Ahora creamos un grupo nuevo , para añadirlos a la base de datos de la misma manera, creamos un archivo. ldif

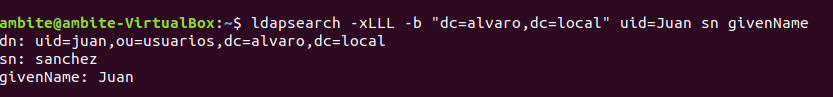


* **sudo ldapadd -x -D cn=admin,dc=alvaro,dc=local -W -f grupo.ldif**

****

Podemos comprobar que están bien creados con el siguiente comando .

* **ldapsearch -xLLL -b “dc=alvaro,dc=local” uid=juan sn givenName**

****

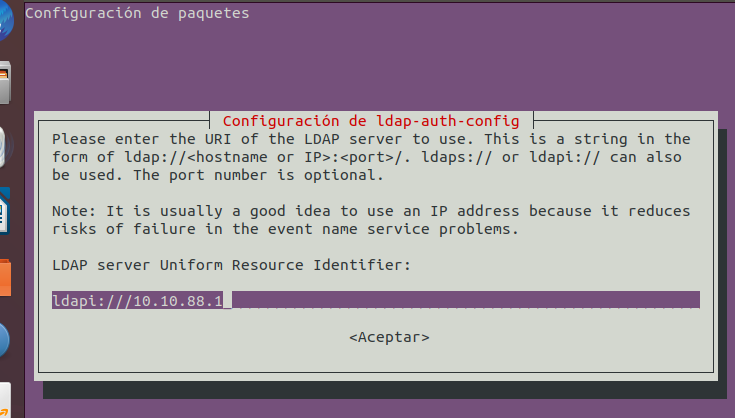
### AÑADIMOS UN CLIENTE QUE TENGA SO UBUNTU

Instalas el ubuntu y le ponemos una Ip, fija que queramos dentro del rango de la red del servidor .

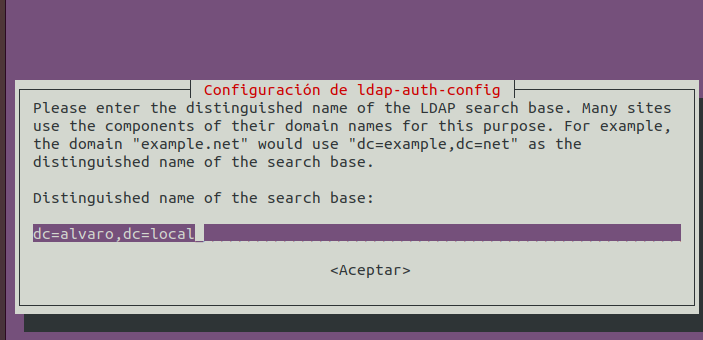
Después instalamos el cliente con el siguiente comando .

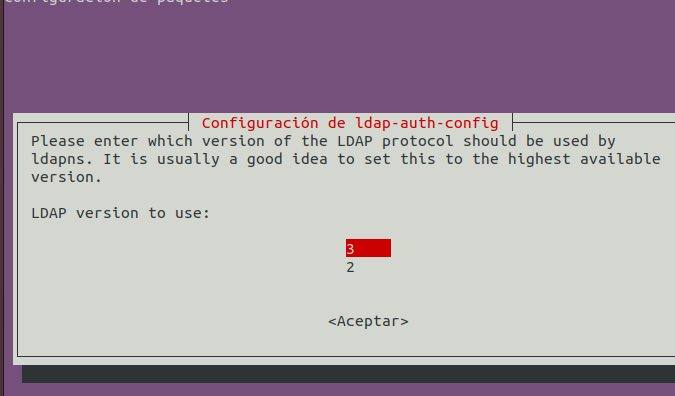
* **sudo apt-get install libpam-ldap libnss-ldap nss-updatedb libnss-db nscd ldap-utils -y**

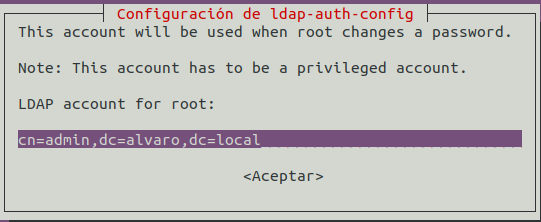
**Recordamos ponerle a continuación la ip que tengamos en el servidor puesta.**



Ponemos el dominio , que hemos configurado antes .



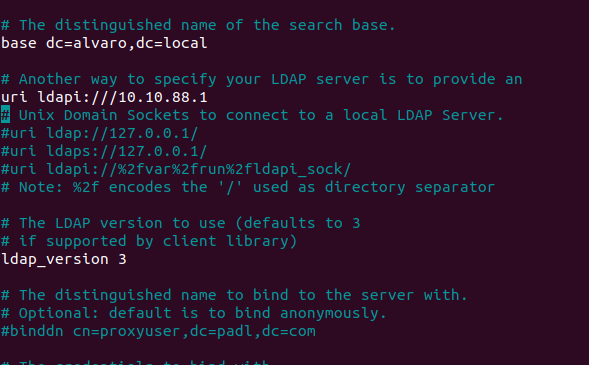


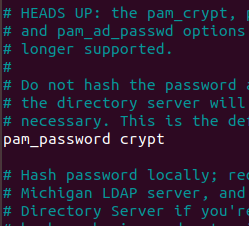


Una vez terminada la instalación, modificamos el **ldap.conf** como antes.

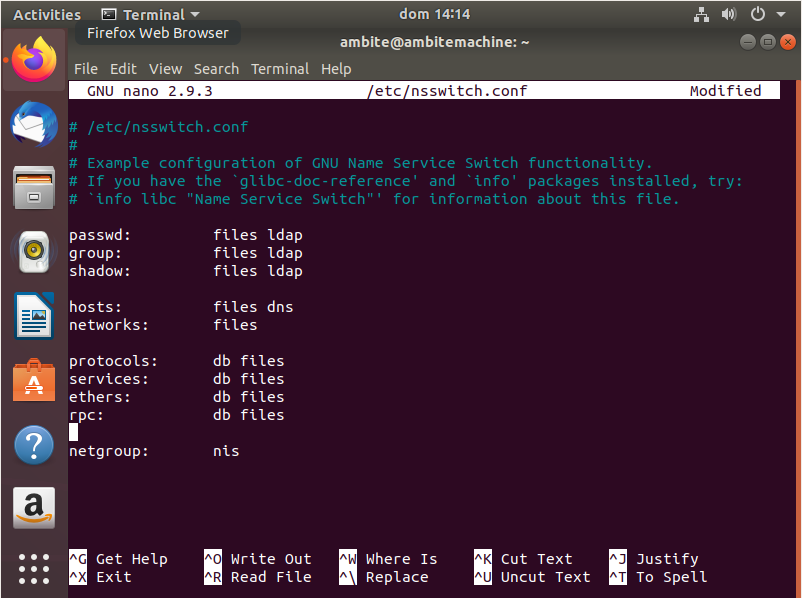
* **sudo nano /etc/ldap.conf**

**recordamos cambiar las opciones de antes como pam\_password crypt y bind\_policy soft**

****

****

Ahora modificamos el archivo **nsswitch.conf**,este es el fichero de configuración de las Bases de Datos del Sistema y el sistema de Conmutación de los Servicios de Nombres (Name Service Switch)

****

Ahora vamos a ejecutar el siguiente comando .

* **sudo nss updatedb ldap**

****

Tras muchos intentos no he podido conseguir que este error se me solucionaste y creo que es porque no consigue contactar con el servidor la verdad es que he probado muchas cosas, el ping funciona,el dns resuelve nombres no se me ocurren mas cosas que hacer, otras veces me salía un error con la clave, que no era capaz de verificarla o algo así todo lo que mire tenia que ver con el **pam\_password** y se supone que había que ponerlo en crypy cosas que hace mis compañeros con una configuraćion similar sí que consiguieron que se conectarse .

Aunque ahora no lo haya conseguido seguiré probando hasta que me funcione pero por ahora te mando esto un saludo.