OpenLDAP en Ubuntu

Servidor/Escritorio 20.04

Instalación y configuración.

PARTE 1.

CFGS ASIX

Módulo: Administración de Sistemas Operativos

UD3: Administración de servicios de directorio: LDAP

[1 LDAP. Introducción 3](#__RefHeading___Toc1596_4213657510)

[1.1 ¿Cómo funciona LDAP? 3](#__RefHeading___Toc1598_4213657510)

[1.2 Ventajas en el uso de LDAP 3](#__RefHeading___Toc1600_4213657510)

[1.2.1 Usos prácticos de LDAP 4](#__RefHeading___Toc1602_4213657510)

[2 Estructura de una base de datos/directorio LDAP 5](#__RefHeading___Toc1604_4213657510)

[2.1 Entradas, objetos y atributos 5](#__RefHeading___Toc1606_4213657510)

[2.2 Estructura del atributo DN y una breve introducción histórica 6](#__RefHeading___Toc1608_4213657510)

[2.2.1 Introducción histórica 6](#__RefHeading___Toc1610_4213657510)

[2.2.2 Cómo organizar tus datos en tu árbol de directorio 7](#__RefHeading___Toc1612_4213657510)

[2.2.3 El DN d'una entrada LDAP 8](#__RefHeading___Toc1614_4213657510)

[3 Instalación y configuración de LDAP en Ubuntu 20.04 10](#__RefHeading___Toc1616_4213657510)

[3.1 Al servidor 10](#__RefHeading___Toc1618_4213657510)

[3.1.1 Configurar la tarjeta de red 10](#__RefHeading___Toc1620_4213657510)

[3.1.2 Comprobamos el nombre de la máquina. 11](#__RefHeading___Toc1622_4213657510)

[3.1.3 Instalar los paquetes de OpenLDAP 12](#__RefHeading___Toc1624_4213657510)

[3.1.4 Parada y reinicio del servicio slapd 15](#__RefHeading___Toc1626_4213657510)

[3.2 Instalación de herramientas de gestión de OpenLDAP 15](#__RefHeading___Toc1628_4213657510)

[3.2.1 Jxplorer 18](#__RefHeading___Toc1630_4213657510)

[3.2.1.1 Creación de las unidades organizativas (ou) 20](#__RefHeading___Toc1632_4213657510)

[3.2.1.2 Añadir usuarios y grupos 22](#__RefHeading___Toc1634_4213657510)

[4 Autenticación basada en LDAP 27](#__RefHeading___Toc1636_4213657510)

[4.1 Introducción 27](#__RefHeading___Toc1638_4213657510)

[4.2 Llibreries d'autenticació pam-ldap i nss-ldap 27](#__RefHeading___Toc1640_4213657510)

[4.3 Instalación y configuración de libpam-ldap y libnss-ldap 29](#__RefHeading___Toc1642_4213657510)

[4.3.1 Configuración de NSS 30](#__RefHeading___Toc1644_4213657510)

[4.3.2 Configuración de servicios PAM 32](#__RefHeading___Toc1646_4213657510)

[4.3.3 Creación automática directorios de usuario (home) 32](#__RefHeading___Toc1648_4213657510)

[4.4 Comprobación de la configuración 35](#__RefHeading___Toc1650_4213657510)

[4.5 Configuración para iniciar sesión en entorno gráfico 36](#__RefHeading___Toc1652_4213657510)

[38](#__RefHeading___Toc1654_4213657510)

[5. Configuración de los perfiles móviles 40](#__RefHeading___Toc1656_4213657510)

[Enlaces de interés 44](#__RefHeading___Toc1658_4213657510)

[5 Bibliografía 45](#__RefHeading___Toc1660_4213657510)

# LDAP. Introducción

LDAP significa Lightweight Directory Access Protocol. Como su nombre indica, es un protocolo ligero en modo cliente-servidor para acceder a los servicios de directorio, específicamente basados en los servicios de directorio X.500. Se ejecuta sobre TCP/IP u otros protocolos orientados a conexión. LDAP se define en el estándar RFC2251. Se utiliza comúnmente para almacenar información sobre organizaciones, usuarios, redes, etc.

Un directorio (no confundir con un directorio de nuestro disco duro, ya que es una estructura mucho más amplia) es similar a una base de datos, pero tiende a contener más información descriptiva, basada en atributos (recordemos los atributos típicos de un archivo en un directorio local: sólo lectura, invisible, fecha de creación, etc...). En un directorio, normalmente, la información se lee más que nada. **Los servicios de directorio habitualmente están optimizados para dar una rápida respuesta en operaciones de búsqueda o exploración**. También pueden tener la **capacidad de replicar (en varios servidores físicos) la información contenida en un directorio con el fin de mejorar la disponibilidad de los datos y la fiabilidad**. Como la replicación de datos puede generar inconsistencias, temporalmente se sincronizan los datos para evitarlo.

Hay muchas maneras diferentes de proporcionar un servicio de directorio. Los diferentes métodos permiten que diferentes tipos de información se almacenan en el directorio, establecer requisitos diferentes para la forma en que la información se puede referenciar, consultar y actualizar, la forma en que está protegida de accesos no autorizados, etc. Algunos servicios de directorio son locales, proporcionando servicios a un contexto restringido (por ejemplo, el servicio de finger en una única máquina). Otros servicios son globales, proporcionando servicios a un contexto mucho más amplio.

## ¿Cómo funciona LDAP?

El funcionamiento, como hemos dicho antes, está basado en un modelo cliente-servidor. Un cliente LDAP se conecta a un servidor LDAP y le hace una consulta. El servidor contesta con la respuesta, o con un apuntador donde el cliente puede obtener más información (típicamente otro servidor LDAP). Decíamos antes que pueden haber muchos servidores con los datos replicados: por lo tanto no es problema que un cliente se conecte con un servidor o a otro; el cliente verá siempre la misma vista del directorio. Esta es una característica muy importante de un servicio global de directorio como LDAP.

## Ventajas en el uso de LDAP

Un directorio LDAP destaca sobre los otros tipos de bases de datos por las siguientes características:

* Es muy rápido en la lectura de registros.
* Permite replicar el servidor de forma muy sencilla y económica.
* Muchas aplicaciones de todo tipo tienen interfaces de conexión a LDAP y se pueden integrar fácilmente.
* Dispone de un modelo de nombres globales que asegura que todas las entradas son únicas.
* Utiliza un sistema jerárquico de almacenamiento de información.
* Permite múltiples directorios independientes
* Funciona sobre TCP/IP i SSL
* La mayoría de servidores LDAP son fáciles de instalar, mantener y optimizar.

### 

### Usos prácticos de LDAP

Dadas las características de LDAP sus usos más comunes son:

* Directorios de información. Por ejemplo bases de datos de empleados organizados por departamentos (siguiendo la estructura organizativa de la empresa) o cualquier tipo de páginas amarillas.
* Sistemas de autenticación / autorización centralizada. Grandes sistemas donde se guarda gran cantidad de registros y se requiere un uso constante de los mismos. Por ejemplo: Active Directory Server de Microsoft, para gestionar todas las cuentas de acceso a una red corporativa y mantener centralizada la gestión del acceso a los recursos.
* Sistemas de autenticación para páginas web, algunos de los gestores de contenidos más conocidos disponen de sistemas de autenticación a través de LDAP.
* Sistemas de control de entradas a edificios, oficinas ....
* Sistemas de correo electrónico. Grandes sistemas formados por más de un servidor que accedan a un repositorio de datos común.
* Sistemas de alojamiento de páginas web y FTP, con el repositorio de datos de usuario compartido.
* Grandes sistemas de autenticación basados en RADIUS, para el control de accesos de los usuarios a una red de conexión o ISP.
* Servidores de certificados públicos y claves de seguridad.
* Autenticación única o "single sign-on" para la personalización de aplicaciones.
* Perfiles de usuarios centralizados, para permitir itinerancia o "Roaming"
* Libretas de direcciones compartidas.

**Algunos ejemplos**

Sistema de correo electrónico

Cada usuario se identifica por su dirección de correo electrónico, los atributos que se guardan de cada usuario son su contraseña, su límite de almacenamiento (cuota), la ruta del disco duro donde se almacenan los mensajes (buzón) y posiblemente atributos adicionales para activar sistemas anti-spam o antivirus.

Como se puede ver este sistema LDAP recibirá centenares de consultas cada día (una por cada correo electrónico recibido y una cada vez que el usuario se conecta mediante POP3 o webmail). No obstante el número de modificaciones diarias es muy bajo, ya que solo se puede cambiar la contraseña o dar de baja al usuario, operaciones ambas que no se realizan de forma frecuente.

Sistema de autenticación a una red

Cada usuario se identifica por un nombre de usuario y los atributos asignados son la contraseña, los permisos de acceso, los grupos de trabajo a los que pertenece, la fecha de caducidad de la contraseña, etc...

Este sistema recibirá una consulta cada vez que el usuario acceda a la red y una más cada vez que acceda a los recursos del grupo de trabajo (directorios compartidos, impresoras ...) para comprobar los permisos del usuario.

Frente a estos centenares de consultas solo unas pocas veces se cambia la contraseña de un usuario o se la incluye en un nuevo grupo de trabajo.

# Estructura de una base de datos/directorio LDAP

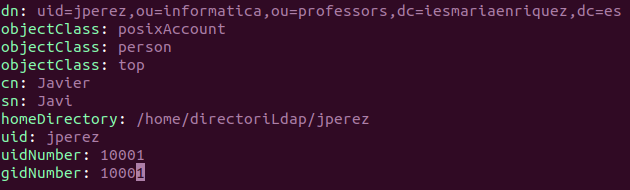
## Entradas, objetos y atributos

Como hemos dicho antes, una base de datos LDAP tiene una **estructura jerárquica**. Básicamente todos los datos se almacenan en alguna parte del directorio LDAP, y a similitud de los directorios de ficheros, este directorio se organiza en **árbol.**

Veamos primero, el punto y final del directorio, que es **la entrada u objeto**. El modelo de información de LDAP está basado en entradas. **Una entrada es una colección de atributos** que tienen un Nombre Distintivo o **Distinguished Name** (identificado como **DN**) único **y global**. El DN se utiliza para referirse a una entrada sin ambigüedades. Cada atributo de una entrada tiene un tipo y uno o más valores y son los que contienen la información asociada al objeto. Los tipos son normalmente palabras mnemotécnicas, como "**cn**" por **common name**, o "**mail**" por una dirección de **correo**.

En comparación con una base de datos relacional, una entrada sería como un registro. El atributo sería el campo.

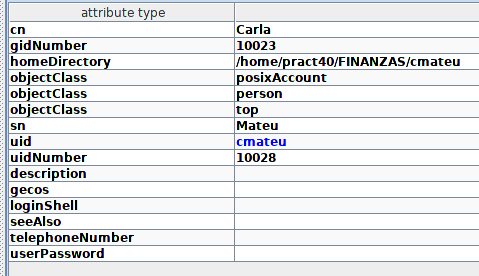
Una entrada, que no es más que un fichero de texto, tiene una estructura como la siguiente:



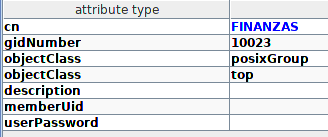
El **objetclass** indica qué atributos **podemos** y **debemos** utilizar para cada entrada. Si he programado con lenguajes orientados a objetos, el objeto es la clase que determina los elementos que componen un objeto. En la captura tenemos tres objectClass:

* posixAccount: Tiene como atributos obligatorios cn, uid, uidNumber, gidNumber, homeDirectory, y como opcionales description, userPassword, etc..
* person: Tiene como atributos obligatorios cn, sn y como opcionales description, userPassword, etc, telephone, etc.
* top: Este es el objetotClass raíz, todo el resto de clases cuelgan de esta

La siguiente captura corresponde a la entrada de un usuario. Con campo obligatorio el uid.



La siguiente captura corresponde a una entrada de un grupo. Sólo tenemos un atributo obligatorio, el cn.



## Estructura del atributo DN y una breve introducción histórica

### Introducción histórica

El nivel superior de un directorio LDAP es la base, conocido como el "DN base". Un DN base, generalmente, toma una de las tres formas listadas aquí. Suponemos que trabajas o estudias en el instituto Maria Enriquez de Gandia, el cual está en Internet en iesmariaenriquez.es.

**o = "IES Maria Enriquez", c = ES**

*(Base DN en formato X.500)*

En este ejemplo, **o = IES María Enriquez**  se refiere a la **organización**, que en este contexto debería ser tratada común sinónimo del nombre de la empresa. **c =ES** indica que la **localización general** de la empresa está en ES. Había una vez en que ese fue el método de especificar tu DN base. Los tiempos y las modas cambian, pero, estos días, la mayoría de las empresas están (o planean estar) en Internet. Y con la globalización de Internet, utilizar un código de país en la base DN probablemente haz las cosas más confusas al final. Con el tiempo, el formato X.500 ha evolucionado a otros formatos listados más abajo.

**o = iesmariaenriquez.es**

*(DN base derivado de la presencia en Internet de la empresa)*

Este formato es bastante sencillo, utilizando el nombre de dominio de la empresa como base. Unavez has pasado la porción o = (la cual viene de organization =), cualquiera en tu empresa debería saber de dónde viene el resto. Este fue, hasta hace poco, probablemente el más común de los formatos usados actualmente.

**dc=iesmariaenriquez, dc=ES**

*(DN base derivado de los componentes de dominio DNS de la empresa)*

Como el formato previo, éste utiliza el nombre de dominio DNS como su base. Pero donde el otro formato deja el nombre de dominio intacto (y así legible por las personas), este formato está separado en componentes de dominio: **iesmariaenriquez.es**  **se convierte en**  **dc = iesmariaenriquez, dc = es**. En teoría, esto puede ser levemente más versátil, aunque es un poco más duro de recordar para los usuarios finales.

**Este es el formato recomendable** para nuevas instalaciones. Si estás planeando utilizar Active Directory, Microsoft ya ha decidido por tú que este es el formato que necesitas .

### Cómo organizar tus datos en tu árbol de directorio

En un sistema de ficheros UNIX, el nivel más alto es la raíz (**/**). Por debajo de la raíz tienes muchos ficheros y directorios. Como se comentaba anteriormente los directorios LDAP están configurados en gran parte de la misma manera.

Bajo tu base de directorio, querrás crear contenedores que separen lógicamente tus datos. Por razones históricas (X.500), la mayoría de los directorios configuran estas separaciones lógicas como entradas OU. **OU** viene de "**Unidades organizacionales**" (**Organizational Units**, en inglés), que en X.500 eran utilizadas para indicar la organización funcional dentro de la empresa: ventas, finanzas, etc. Actualmente las implementaciones de LDAP han mantenido la convención del nombre ou =, pero separa las cosas por categorías amplias como ou = gente (ou = people), ou = grupos (ou = groups), ou = dispositivos (ou = devices), y otros.

Por ejemplo, un árbol de directorio LDAP (sin incluir entradas individuales) podría ser así:

dc = iesmariaenriquez, dc = es

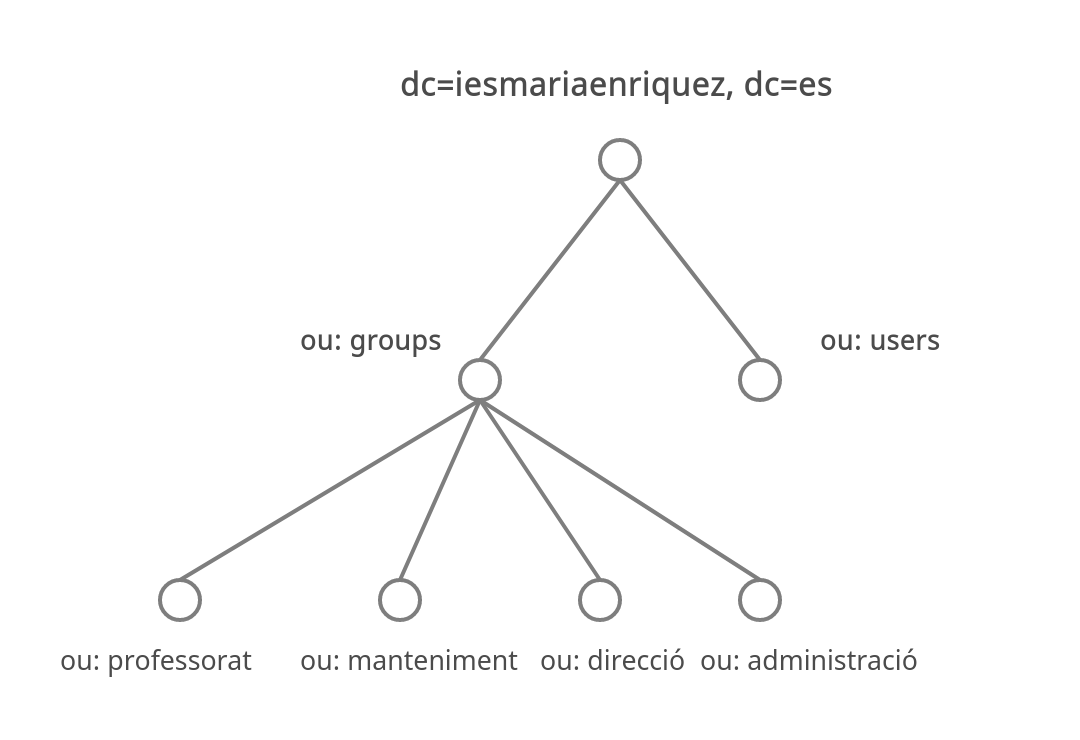
ou = grupos   
 ou = direccion

ou = administracion

ou = profesorado

ou=mantenimiento

ou = usuarios



### El DN d'una entrada LDAP

Todas las entradas almacenadas en un directorio LDAP tienen un único "**Distinguished Name**," o **DN**. El **DN** para cada entrada está compuesto de dos partes: el Nombre Relativo **Distinguido** (**RDN** por sus siglas en inglés, **Relative Distinguished Name**)y la **localización** dentro del directorio LDAP donde el registro reside.

El **RDN** es la porción de tu DN que no está relacionada con la estructura del árbol de directorio. La mayoría de los ítems que almacenamos en un directorio LDAP tendrá un nombre, y el nombre es almacenado frecuentemente en el atributo **cn** (**Common Name**). Ya que prácticamente todo tiene un nombre, la mayoría de los objetos que almacenará LDAP utilizan su valor **cn** como base para su RDN. Si estoy almacenando un registro por mi receta preferida de comida de avena, estaré utilizando cn=ComerdeCivadaDeluxe como el RDN de mi entrada.

* El **DN** base de mi directorio es *dc=iesmariaenriquez, dc=es*
* El **RDN** de un registro de un grupo *cn=alumnos*

Dado todo esto, ¿cuál es el DN completo del registro LDAP para este grupo? Recuerda, se lee en orden inverso, hacia atrás - como los nombres de máquina en los DNS.

**cn=alumnos, ou=groups, dc=iesmariaenriquez,**  dc=es

Ahora es el momento de abordar el DN de un miembro de nuestro instituto. Para **las cuentas de usuario,** típicamente verás un DN **basado en el cn o en el uid**  (ID del usuario). Por ejemplo, el DN del profesor Armand Mata (nombre de login: armandmata) puede parecerse a uno de estos dos formatos:

**uid = armandmata, ou = professorat, ou=personas, dc = iesmariaenriquez, dc = es**

(basado en el login)

LDAP (y X.500) utilizan uid para indicar "ID del usuario", **no debe confundirse con el número uid de UNIX.** La mayoría de las empresas intentan dar a cada uno un nombre de login, así esta aproximación hace que tengoa sentido almacenar información sobre los empleados. No te tienes que preocupar sobre qué harás cuando entre un nuevo profesor con el mismo nombre, o si el mismo profesor decide cambiarse el nombre. No tienes que cambiar el DN de la entrada LDAP.

**cn = ArmandMata, ou = professorat, ou=personas, dc = iesmariaenriquez, dc = es**

(basado en el nombre)

Aquí vemos la entrada **Nombre Común** o **CN (**por sussiglas en inglés, **common name**)utilizada. En el caso de un registro LDAP para una persona, **piensa en el nombre común como su nombre completo.** Uno puede ver fácilmente el efecto colateral de esta forma: si el nombre cambia, el registro LDAP debe "mover" de un **DN** a otro. Como se indica anteriormente, debes evitar cambiar en **DN** de una entrada siempre que sea posible.

# Instalación y configuración de LDAP en Ubuntu 20.04

## Al servidor

Nombre de la máquina virtual y del equipo: ombreDelServidoLDAP

Usuari principal: admin

Contraseña usuario principal: admin

Dos tarjetas de red

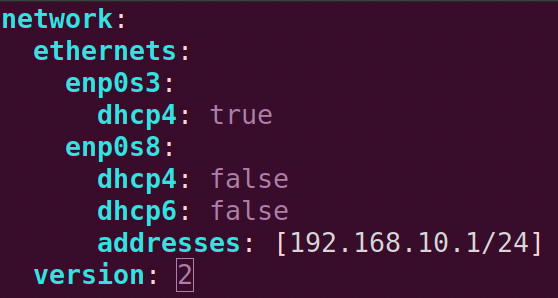
NAT --> DHCP

Red Interna, interfaz inet -> Manual

### Configurar la tarjeta de red

Editamos la configuración de la segunda tarjeta de red, la de red interna, y le ponemos una IP fija y la mascarilla. En mi caso utilizaré el IP 192.168.10.1. Esperamos unos segundos y comprobamos con ip a la configuración de las tarjetas.

*sudo nano /etc/netplan/00-installer-config.yaml*



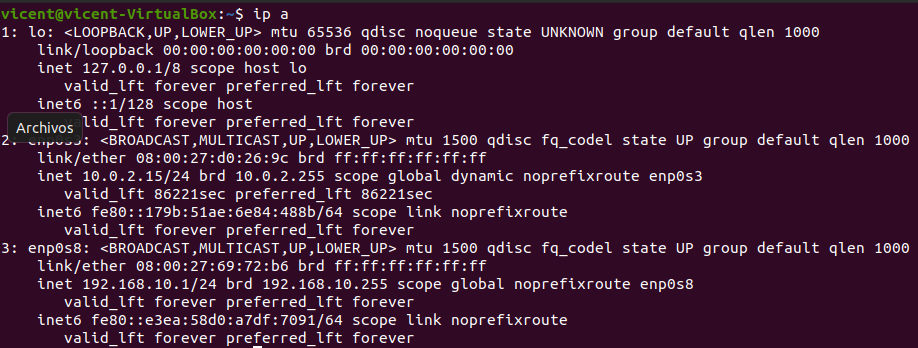
Y apelamos a los cambios.

*sudo netplan aplicar*

Hacemos ip a para comprobar los cambios

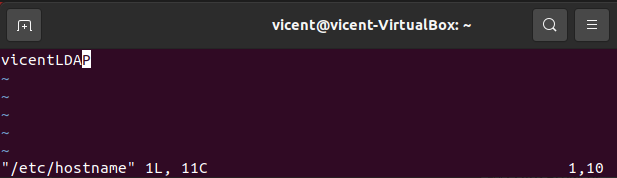
*IP A*

**(No hace falta hacer uso del netplan, podéis configurar la dirección en el entorno gráfico)**



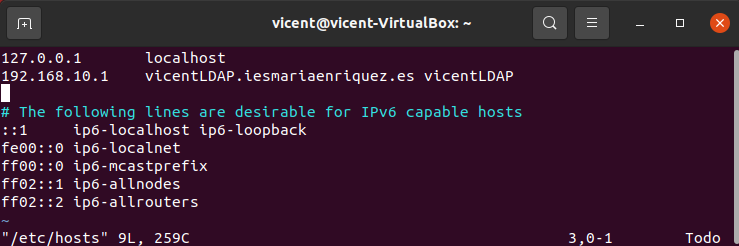
### Comprobamos el nombre de la máquina.

*sudo nano /etc/hostname*



*sudo nano /etc/hosts*

Debemos modificar un poco el fichero /etc/hosts para que nuestra IP estática esté asociada a nuestro dominio.



Hay que reiniciar la máquina para que los cambios sean efectivos.

*reinicio de sudo*

### Instalar los paquetes de OpenLDAP

Primero que nada actualizamos los repositorios de la máquina y aplicamos las últimas actualizaciones

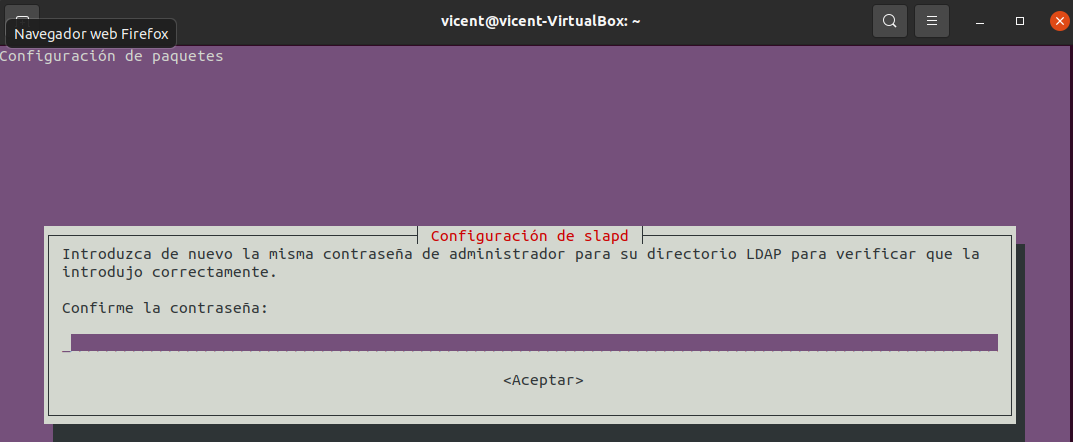
*sudo apt update*

*sudo apt upgrade*

Ahora sí, instalamos los paquetes de LDAP

*sudo apt install slapd ldap-utils -y*

Nos pide la contraseña que queremos utilizar, a las capturas utilizarem "test1"

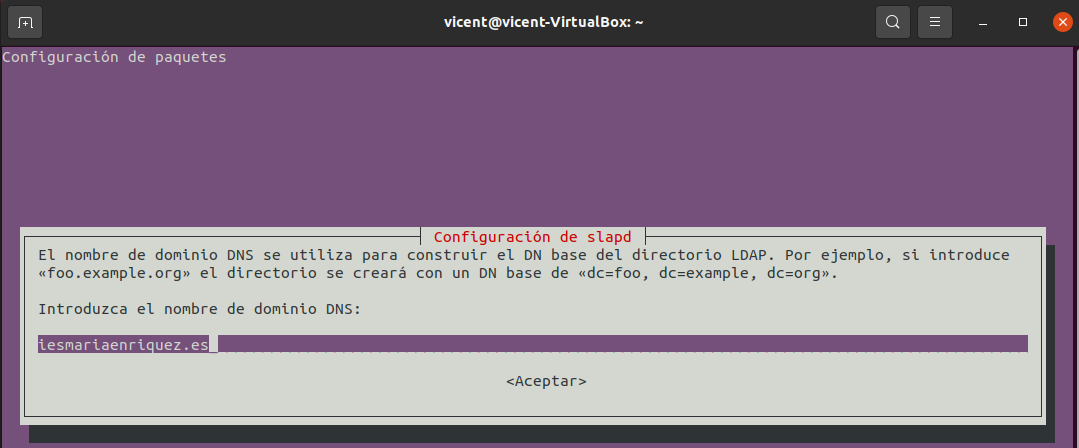


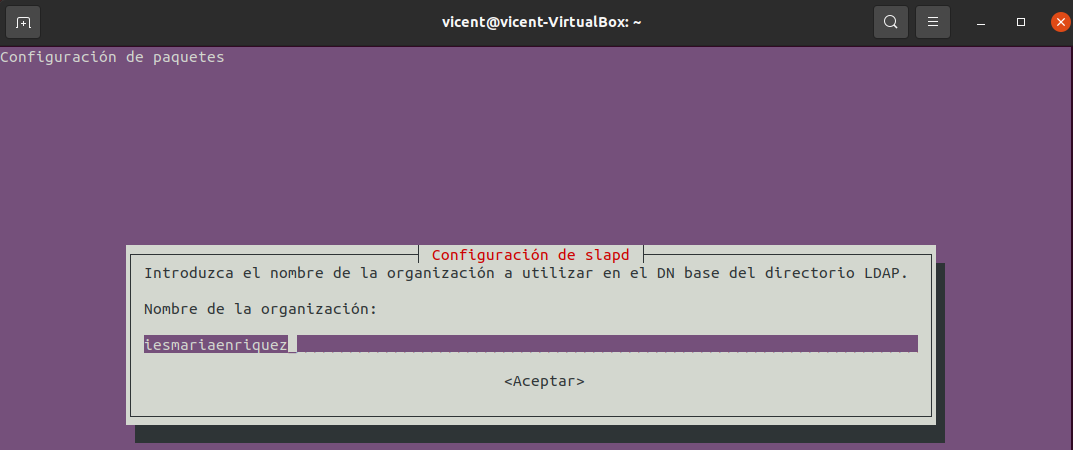
Si no se inicia el asistente de configuración podemos iniciarlo nosotros con:

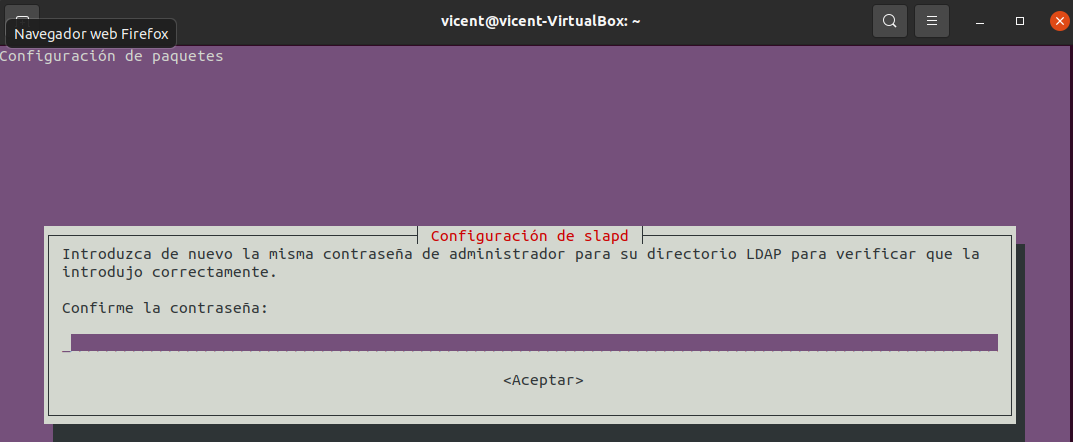
*sudo dpkg-reconfigure slapd*

* Nos pregunta si queremos omitir al asistente: Seleccionamos: **no**
* Nos pregunta la base de nuestro dominio: En mi caso: **iesmariaenriquez.** **se**
* Nos pregunta el nombre completo de nuestra empresa. En mi caso: **iesmariaenriquez**
* Nos pregunta la palabra de paso. En mi caso: **test1**
* En las siguientes preguntas podéis dejar la opción por defecto

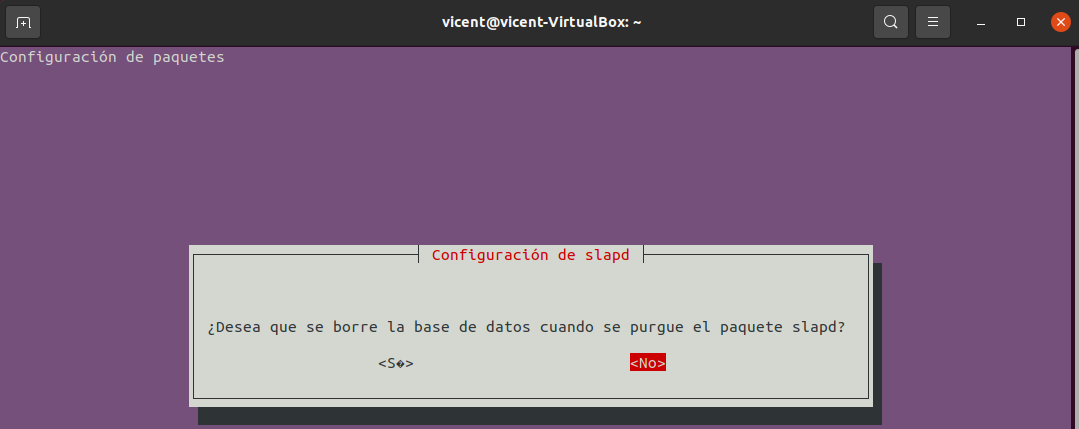








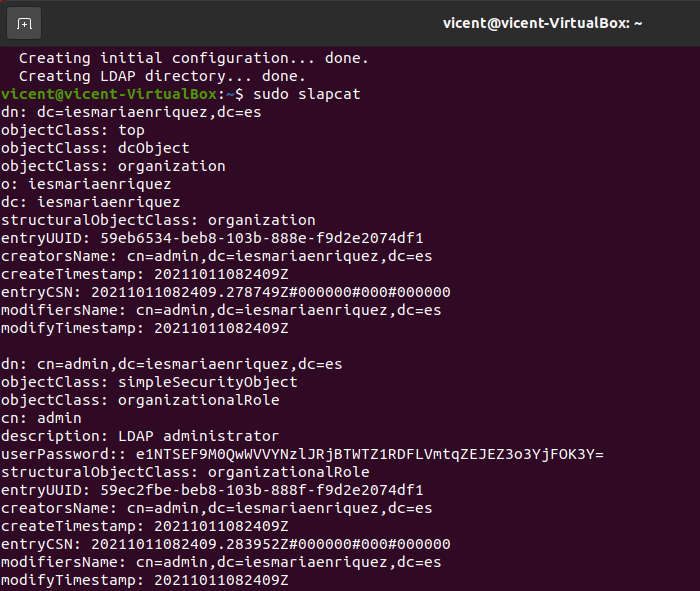
Por último, nos pide si queremos que se borre automáticamente la DDBB cuando hacemos un "purge" del paquete slapd. Todo depende de lo que tengamos, si somos responsables y tenemos copias de seguridad, podemos darle a "Sí", pero si únicamente tenemos el directorio a este equipo, nos interesa que no se borre.



Comprobamos si ha funcionado todo correcto con el orden

*slapcat sudo*

* Vemos que nuestra base de dominio es *dc=iesmariaenriquez,dc=es*
* Vemos que tenemos un objeto  ***admin***
  + DN*: cn=admin,dc=iesmariaenriquez,dc=es*
  + *RDN: cn=admin*



### Parada y reinicio del servicio slapd

Si necesitamos reiniciar el servicio sin reiniciar la máquina podemos hacer

*sudo /etc/init.d/slapd start*

*sudo /etc/init.d/slapd stop*

*sudo /etc/init.d/slapd reiniciar*

## Instalación de herramientas de gestión de OpenLDAP

Existen varias herramientas gráficas que podemos utilizar para gestionar OpenLDAP, las podemos usar a una máquina cliente como una máquina con rol de servidor. En estos apuntes la utilizaremos en un Ubuntu Desktop.

Antes de empezar vamos a revisar la configuración de la tarjeta de red al cliente.

**Cliente**

Nombre de la máquina virtual y del equipo: apellido\_clientLDAP

Usuario principal: cliente

Contraseña usuario principal: cliente

Dos tarjetas de red

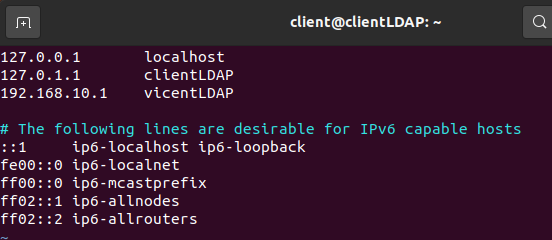
NAT --> DHCP

Interna interfície inet --manual de >

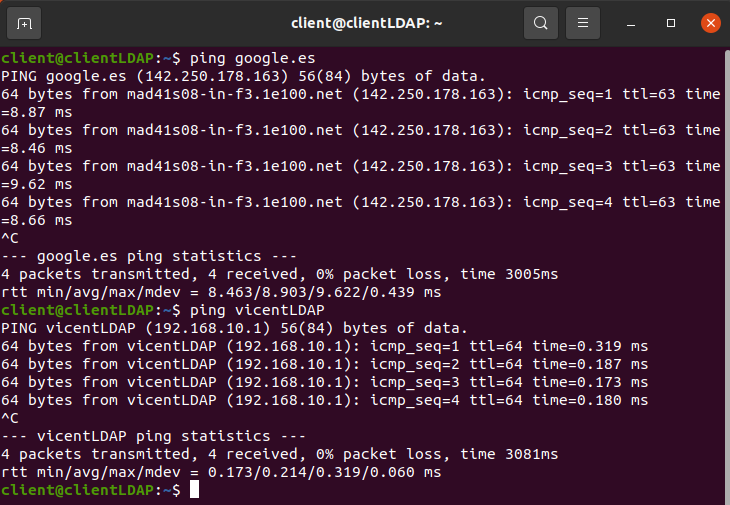
Editamos la configuración de la segunda tarjeta de red, la de red interna, y le ponemos una IP fija y la mascarilla. En mi caso utilizaré el IP 192.168.10.10.



Añadamos a "/etc/hosts" el nombre y la dirección de nuestro servidor LDAP, como es lógico, el nombre de vuestro servidor no será el mismo ni tampoco el del cliente.



Comprobamos que podemos hacer un ping en Google y en nuestro servidor. Para comunicarnos con el servidor podemos utilizar la IP o el nombre del servidor.



Ahora ya podemos empezar a trabajar.

Existen varias aplicaciones gráficas para facilitar la gestión de LDAP: **Jxplorer,** phpLDAPadmin, Apache Directory Studio.

La primera ofrece desde un entorno web la posibilidad de explorar la base de datos LDAP, los objetClass, sus atributos, etc. Importar/exportar elementos, etc.

El segundo y tercero es un entorno basado en Java, mucho más completo, pero también más lento. Veremos este segundo.

### 

### Jxplorer

Para utilizar el programa necesitamos tener el entorno de Java instalado. Revisemos si Java se ha instalado anteriormente:

*java -version*

Si no está instalado, lo instalamos

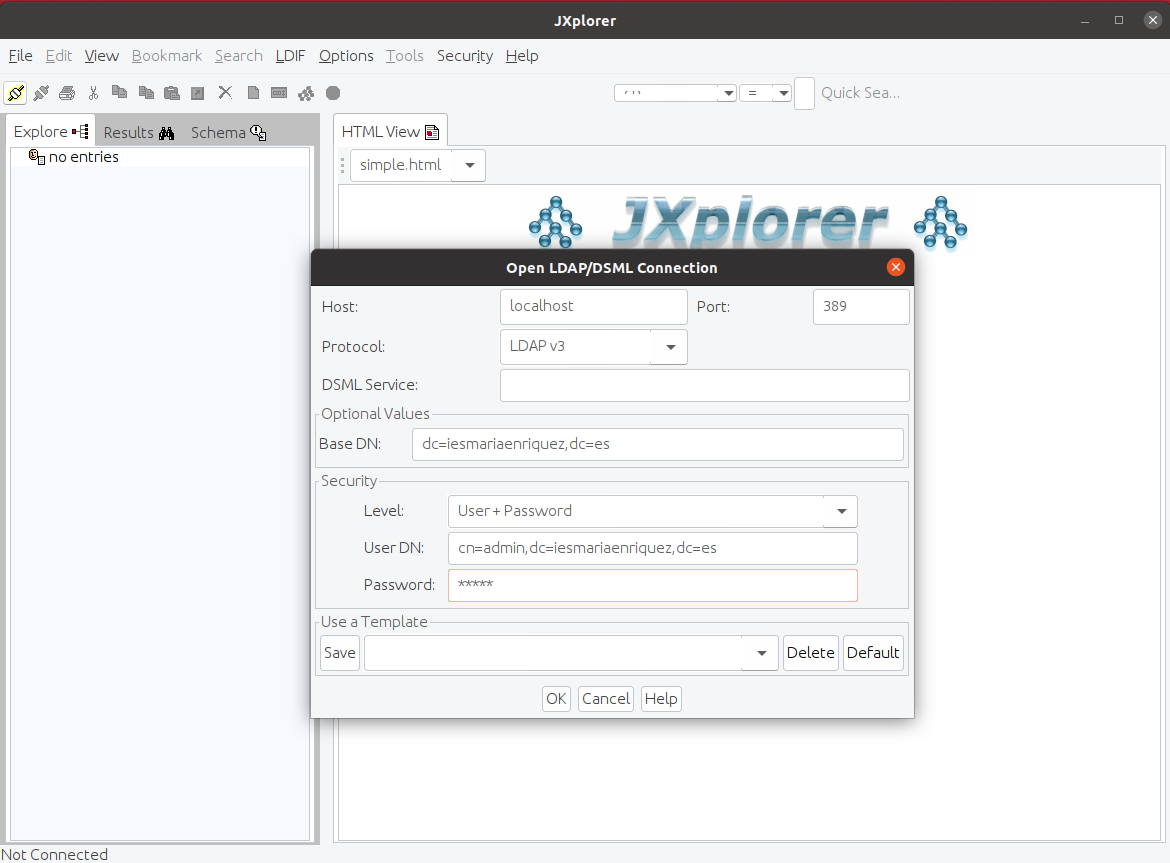
*sudo apt install openjdk-11-jdk*

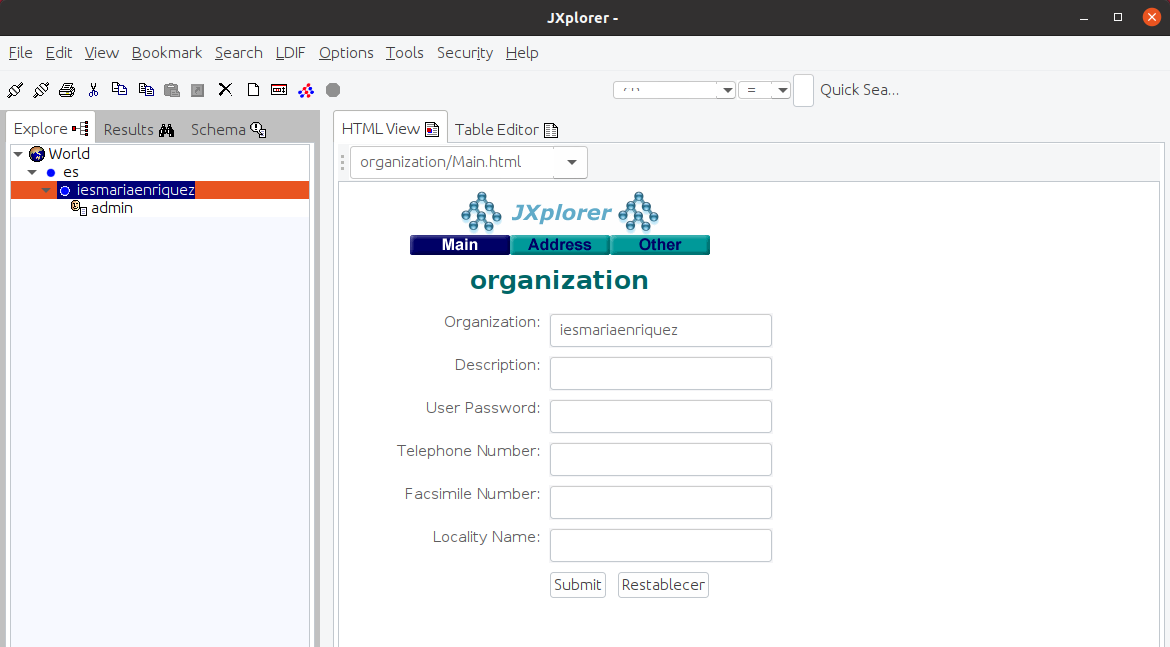
Ahora ya si podemos instalar el programa Jxplorer

*sudo apt install jxplorer*

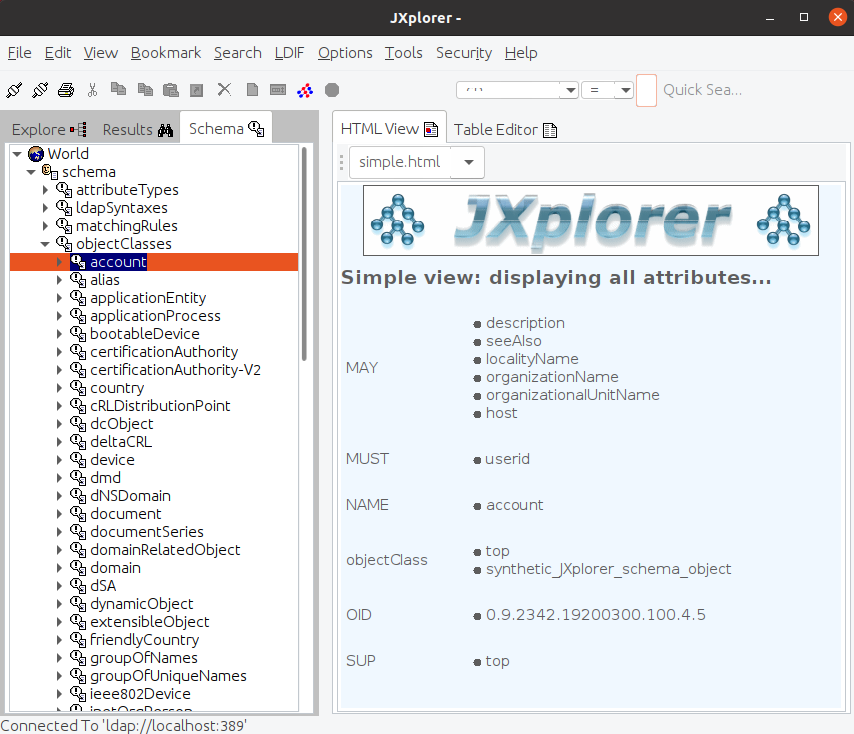
Iniciamos el programa. Unavez encés, el icono Conectar nos mostrará la siguiente pantalla donde configuraremos los parámetros de la conexión.

|  |
| --- |
| Importante: El cliente ejecutará jxplorer, pero deberá conectar con el servidor ldap. Si éste está en la misma máquina, la IP a especificar será 127.0.0.1 o local. Si el servidor se encuentra en otra máquina (habitual), habrá que indicar su IP o añadir el nombre al fichero /etc/hosts |





Si seleccionamos la pestaña ***schema*** podremos ver (e incluso editar, aunque no se recomienda) todos los objetos y atributos de nuestro directorio LDAP.



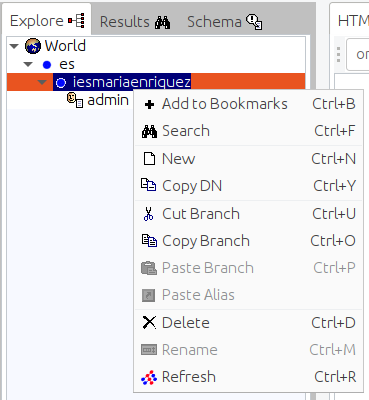
La pestaña ***Results*** servirá para hacer búsquedas. Inicialmente tenemos el directorio vacío, y por lo tanto no encontraremos nada.

#### Creación de las unidades organizativas (ou)

Ya que nuestro directorio, en prácticas posteriores, almacenará usuarios y grupos, vamos a crear **dos**  **unidades organizativas llamadas**  **"*users*"**  **y**  **"groups"** que nos servirán para organizar a los usuarios y grupos por separado.

Dentro de la unidad organizativa "*users*" crearemos todos los usuarios del sistema. Dentro de la unidad organizativa "*groups*" crearemos todos los grupos del sistema.

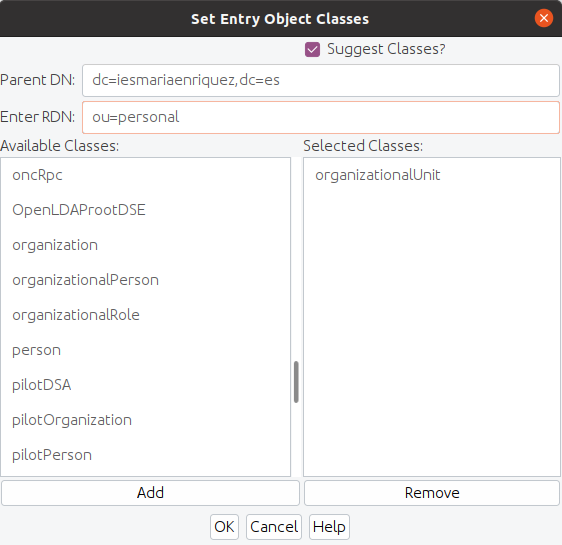
Para crear una unidad organizativa dentro de nuestra organización, haremos clic con el botón derecho sobre la organización "empresa" y en el menú contextual elegiremos 'New':



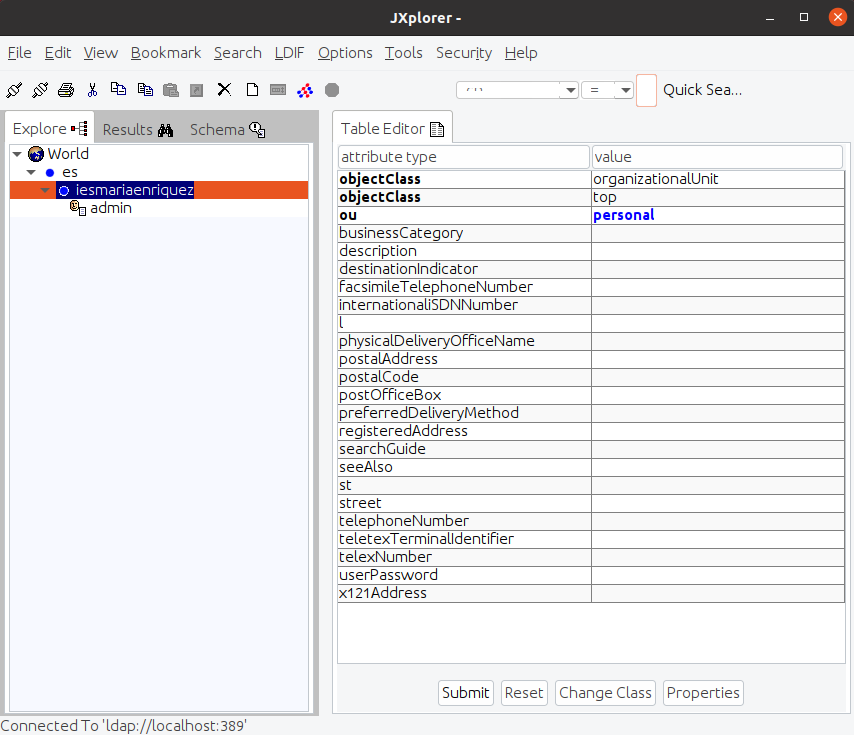
Nos aparecerá la ventana "Set Entry Object Classes". Podremos elegir los "tipus" que tendrá nuestro nuevo elemento. Como se trata de una unidad organizativa (**ou**) debemos seleccionar el tipo **organizationalUnit** en la lista de la izquierda y peer el botón añadir (Add).

Los otros dos tipos que aparecen por defecto (organizationalRole y simpleSecurityObjet) no los necesitaremos, por lo tanto podemos seleccionar de la lista de la derecha y pegarlo el botón quitar (remove).

En la casilla "Enter RDN" (introducir Nombre Distinguido Relativo) debemos poner el nombre de nuestro elemento. Escribimos **ou = users**.



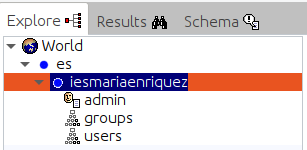
Estaremos en la situación de la siguiente figura:



En la parte de la derecha podremos terminar de llenar los atributos de nuestra nueva entrada y al finalizar pulsar **Submit**.

Hagamos lo mismo para "groups".

Y acabaremos con una estructura como la siguiente:



#### Añadir usuarios y grupos

Ahora sólo nos queda crear los usuarios y los grupos,cada uno dentro de su propia unidad organizativa.

Seguiremos un esquema como el siguiente:

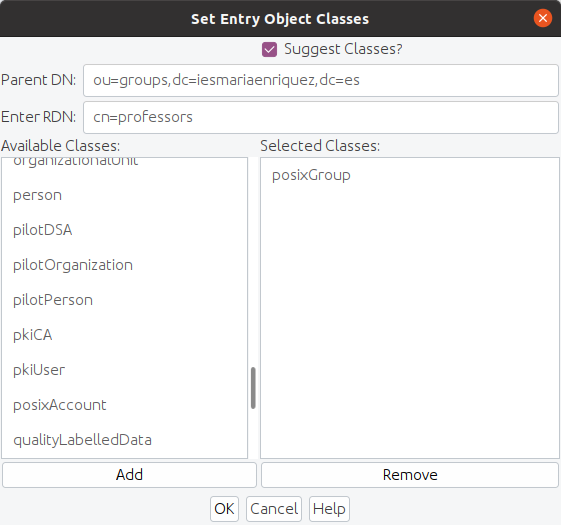
* profesorado (gidNumber=10001)
* alumnos (gidNumber=10002)

Dentro del **ou "users"** crearemos los siguientes usuarios:

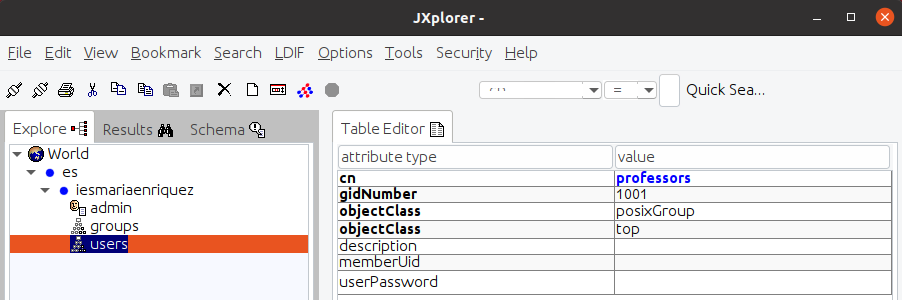
* **elteunom**(uidNumber=10001, profesor)
* carlosPerez (uidNumber=10002, profesor)
* josepPeiro(uidNumber=10003, profesor)
* cristinaDeArmas (uidNumber=10004, alumno)
* andreuMas (uidNumber=10005, alumno)

Para crear los grupos, haremos clic con el derecho a la unidad organizativa **"groups"** e igual que antes haremos clic en **"New"**. Nuestro nuevo elemento será un nuevo grupo **POSIX**, por lo tanto debemos añadir el tipo **"posixGroup"** de la lista de la izquierda.

El nombre (RDN) será **profesores**, por lo tanto debemos escribir 'cn = **profesores**' (cn = Common Name - Nombre Común):

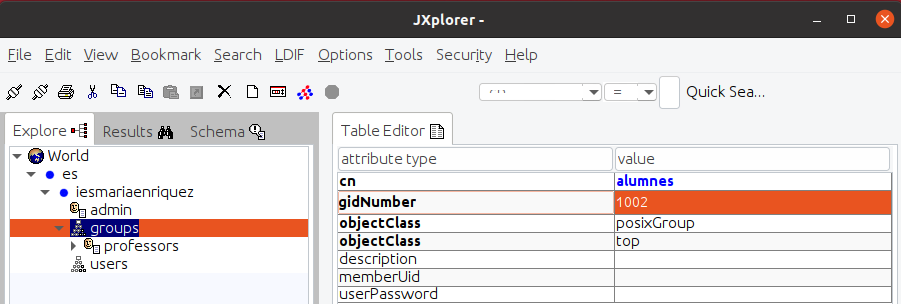


A continuación rellenamos el gid correspondiente a mano:



Premem presentar.

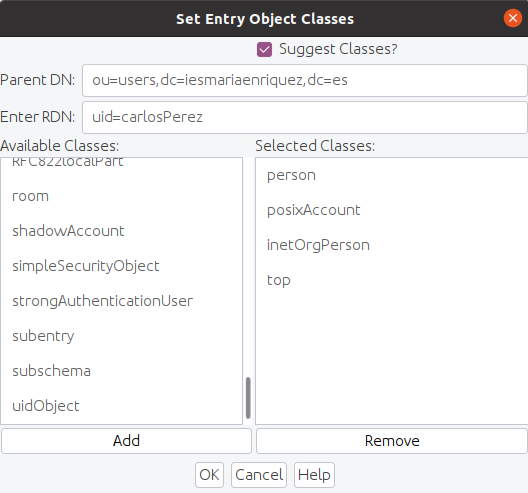
A continuación hacemos lo mismo para el grupo Alumnos.



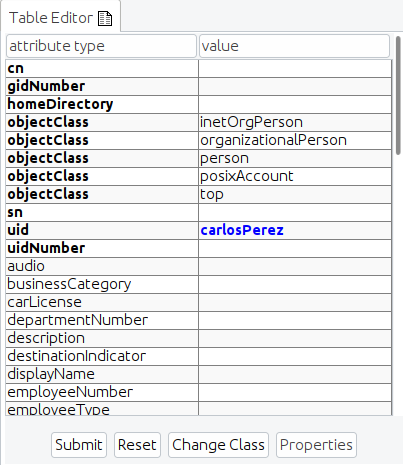
Para crear a los usuarios, haremos clic con el derecho a la unidad organizativa **"users"** e igual que antes haremos clic en **"New"**. Nuestro nuevo elemento será un nuevo usuario **POSIX**, por lo tanto debemos añadir el tipo "**posixAccount**" de la lista de la izquierda.

Pero nuestro usuario también será una persona, por eso nos interesa añadir el tipo **"person"** para disponer de los atributos de este tipo (nombre, apellidos, ...), además como será usuario de Internet nos interesa añadir también el tipo **"inetOrgPerson"**  para poder desar el e-mail y otros valores.

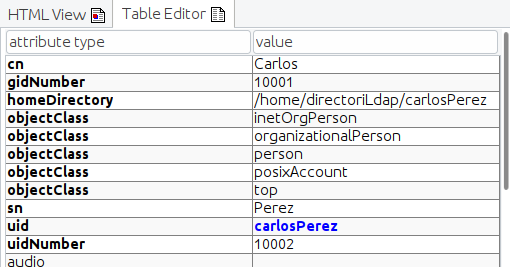
Como hemos dicho antes hay dos opciones, crear el usuario en base al uid (identificador o login) o con base el cn (Common Name). Recuerde que este valor debe ser único. Si su nombre es Paula Grau, podemos escribir en la casilla RDN 'uid= paulaGrau'.



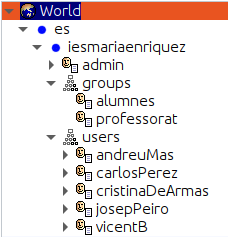
Aprendimos OK y a continuación llenamos los atributos que ves:



Observa que los objetClass que hemos indicado, nos indican **en negrita todos los atributos** que tiene el **uid=carlosPerez** como obligatorios , **además,** el gidNumber debe corresponder al grupo al que pertenece, y el uidNumber al que le corresponde también (no confundir con el uid, que llenamos con el nombre del login).



Finalmente nos queda una estructura similar a la siguiente:

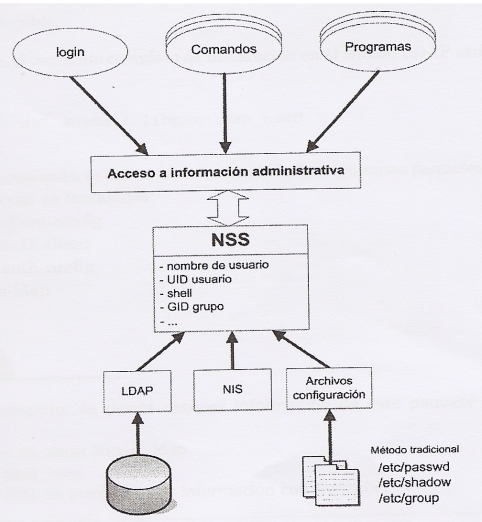


# Autenticación basada en LDAP

## Introducción

Entre las utilidades que habíamos comentado antes, una de las más utilizadas del servidor LDAP es **la autenticación**: para entrar en un sistema Unix/Linux., para acceder a servidores FTP, para páginas web privadas, etc.

En este apartado empezaremos a ver cómo hacer que un sistema Linux para que autentique a los usuarios en un servidor LDAP en lugar utilizar los clásicos ficheros /etc/passwd, /etc/group y /etc/shadow. Para hacerlo debemos instalar y configurar los paquetes ***libpam-ldap y libnss-ldap.***



## Llibreries d'autenticació pam-ldap i nss-ldap

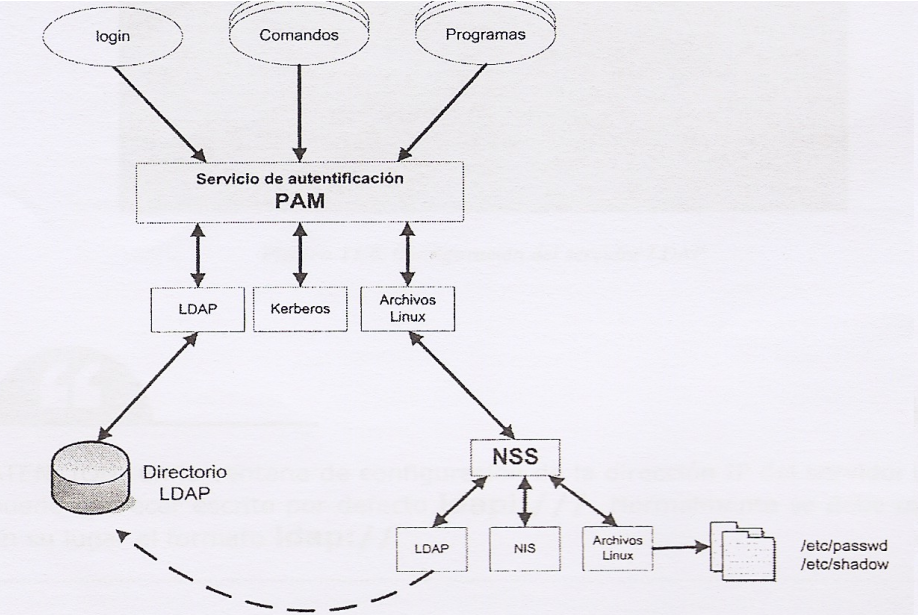
La librería **pam-ldap** permite que las aplicaciones que utilizan PAM **(Pluggable Authentication Modules)** para autenticar, puedan hacerlo mediante un servidor LDAP. Linux emplea este mecanismo para la validación local, por lo tanto debemos instalar esta librería.

El archivo de configuración de esta librería es **/etc/ldap.conf**. Hay otras aplicaciones o servicios que utilizan PAM para la autenticación y por lo tanto podrían, gracias a la librería **pam-ldap**, autenticarse ante un servidor LDAP.

Para especificar el modo de autenticación de cada servicio es necesario configurar los archivos que se encuentran en la carpeta ***/etc/pam.d/***. Al final de este apartado se indican los cambios necesarios en estos archivos.

La librería **nss-ldap** permite que un servidor LDAP suplante a los archivos /etc/passwd, /etc/group y /etc/shadow como bases de datos de nuestro sistema cliente. Su archivo de configuración se encuentra en ***/etc/ldap.conf*** (comparte archivo de configuración con la librería  **pam-ldap**).

Posteriormente deberemos configurar los archivos que son **/etc/nsswitch.conf** para que se utilice LDAP como base de datos del sistema en lugar de los archivos passwd, group y shadow.



## 

## Instalación y configuración de libpam-ldap y libnss-ldap

**Cliente**

Primero que nada actualizamos la máquina

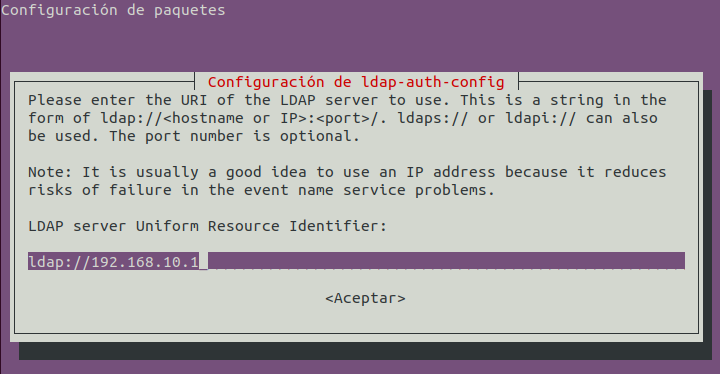
*$ sudo apt update*

*$ sudo apt upgrade*

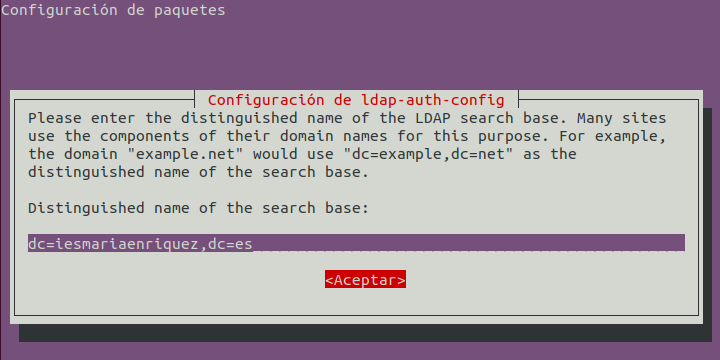
Ahora sí, instalamos los paquetes del cliente LDAP

*$ sudo apt install libnss-ldap libpam-ldap ldap-utils -y*

Comenzará el tutorial para la configuración:



**Fijémonos que NO**  **es ldapi:///, hemos levantado la**  **"y"** y **la tercera**  **"/",**  ***ldap://192.168.10.1***

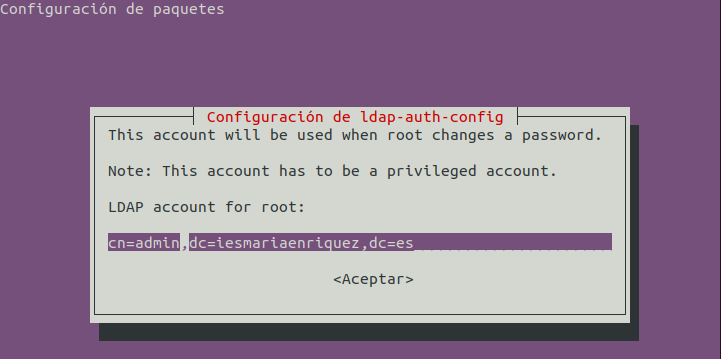


En las siguientes 3 pantallas dejaremos las opciones por defecto:

**Versión LDAP:** 3

**Hacer administrador de la base de datos raíz local:** Si

**¿La base de datos LDAP requiere inicio de sesión?**  No



Contraseña de la cuenta raíz LDAP: laContrasenya

La configuración que acabamos de hacer se almacena en el fichero **/etc/ldap.conf**  elcual podemos modificar manualmente**.** Este se utiliza tanto para el servicio de autenticación **PAM** como por el servicio de nombres **NSS (Name Service Switch).** Si posteriormente tuviésemos que cambiar esta configuración podemos editar el fichero o, más fácilmente, lo reconfiguraremos con el orden **dpkg-reconfigure ldap-auth-config.**

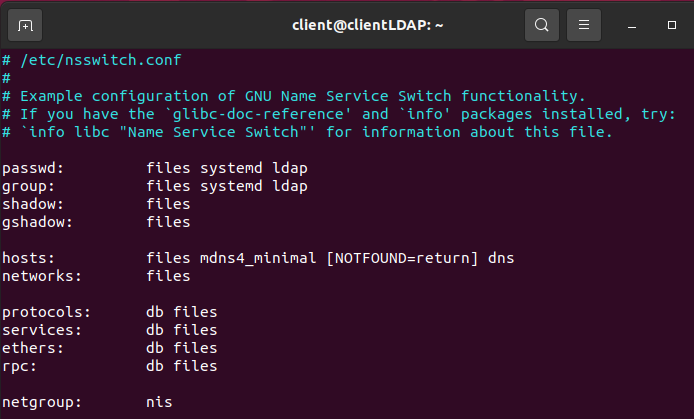
### Configuración de NSS

**Cliente**

Para que el servidor LDAP actue como si se tratara ahora de los archivos passwd, group y shadow, además de instalar las dos librerías anteriores, debemos indicar que se utiliza LDAP como alternativa para autenticar usuarios. Para ello modificamos el archivo /etc/nsswitch.conf:

*sudo nano /etc/nsswitch.conf*

Únicamente hay que añadir ldap (no hay que cambiar compat para file systemd). Según la versión del cliente en las líneas de passwd, group y shadow pondrá filas, compat o filas systemd. Los dos parámetros significan prácticamente lo mismo.



Lo que estamos configurando ací es que en primer lugar busque usuarios, grupos y contraseñas en los ficheros locales y si no los encuentra busque en LDAP. Respecto a las máquinas (hosts) primero las busca en el fichero local (/etc/hosts) y si no las encuentra pregunta en el DNS.

Cuenta ací con el detalle, si añadimos "ldap" como último elemento tanto de passwd y group, a la hora de montar las carpetas, tendrá más prioridad los elementos ya existentes a los usuarios (las carpetas locales de cada usuario del LDAP). Esto nos puede traer problemas en el punto **"Configuración de los perfiles móviles"**  cuando cambiamos la ruta del directorio de cada usuario.

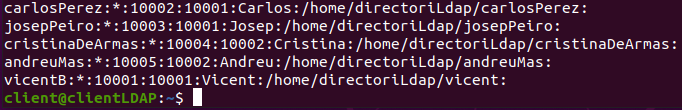
**Actualizamos los cambios reiniciando la máquina** o con el siguiente orden que habría que instalar. previamente:

*$ sudo nss\_updatedb ldap*

Podemos hacer una prueba de que NSS está funcionando con el orden ***getent:***

*$ getent passwd*

Esta orden mostrará por pantalla la información de usuarios contenida en el archivo */etc/passwd*. Si funciona NSS, además de la lista de usuarios locales, añadirá información de los usuarios creados en el directorio LDAP del servidor.



Podemos consultar los *logs* del sistema referentes a validación, */var/log/auth.log,* para comprobar y ver posibles problemas.

### Configuración de servicios PAM

**Cliente**

Ahora nuestro Linux ya estaría preparado para autenticar como LDAP. Editando los ficheros que hay en la carpeta ***/etc/pam.d*** podemos configurar la forma en que seautentica cada uno de los servicios que requieren autenticación.

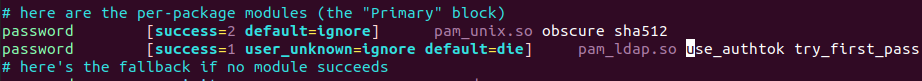
Para no tener que hacerlo individualmente, existen unos archivos cuyo nombre empieza por "common" y que en muchos de estos archivos hacen referencia a ellos mediante una línea @include

* /etc/pam.d/common-auth (por un autenticar-se)
* /etc/pam.d/common-account (para disponer de una cuenta)
* /etc/pam.d/common-session (para poder iniciar sesión)
* /etc/pam.d/common-password (para poder cambiar la palabra de paso)

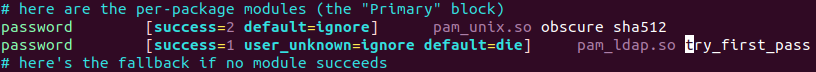
Estos archivos contienen una línea que hace referencia a la librería pam\_unix.so, que corresponde a la autenticación contra los archivos Linux (/etc/passwd, /etc/shadow,etc). Si nos fijamos en la línea señalada en la captura, vemos que nuestro sistema emplea primero las librerías [pam\_ldap.so](http://pam_ldap.so/) para autenticar a los usuarios, y después las de Unix. Así, si la autenticación falla probará con los archivos Linux. Esto nos irá muy bien ya que permitirá validarse con usuarios "locales" en máquinas que se pudovalidar en servicios LDAP remotos.

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

Vamos a la línea 26 y borramos ***use\_authtok:***



Y debe quedar así:



### Creación automática directorios de usuario (home)

**Cliente**

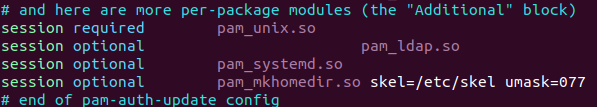
El módulo [pam\_mkhomedir.so](http://pam_mkhomedir.so/) es el que permite crear el directorio de usuario. Umask nos indica con qué permisos crearemos el directorio. Los permisos aplicados es el resultado del resto de 777 - 022 = 755, donde 022 es el valor especificado en umask; 755 corresponde a rwx r-x r-x

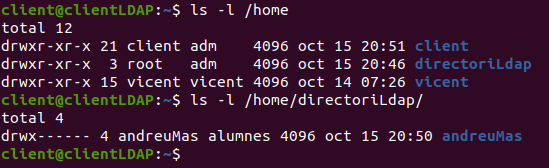
El parámetro skel nos indica un directorio, cuyo contenido, se copiará al nuevo directorio de usuario; puedes poner lo que quiero, todo se copiará en el nuevo directorio HOME creado.

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

Baix de ***session opcional pam\_system.so*** posem:

"sesión opcional pam\_mkhomedir.so skel=/etc/skel umask=077"



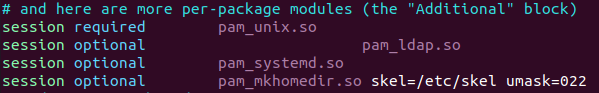


Es una buena práctica para introducir un fichero de información sobre los permisos, o que avise de que están utilizando el servicio LDAP, o lo que necesitamos.

Como hemos metido umask=077 los permisos que tendrán por defecto los directorios /home/usuario serán rwx --- --- .

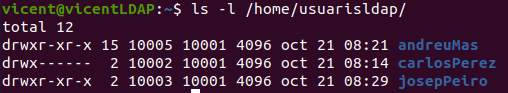
* client y vicent, son usuarios locales, la mascarilla por defecto es 022 (0022)
* andreuMas es un usuario LDAP, cuando vamos a iniciar sesión por primera vuelta la mascarilla era 077

Si queremos que los permisos por defecto de los nuevos directorios /hombre/usuario siga rwx r-x r-x (los permisos habituales para los nuevos usuarios en Linux), en el fichero deberíamos ficar umask=022. Por lo tanto, lo dejaremos así:



Porque los permisos quedan como es necesario, podemos cambiarlos manualmente con "chmod" o bien eliminar la carpeta del usuario (lo que causará que se borren todos sus datos).

Como podéis ver, los usuarios andreuMas y josepPeiro se han creado después de haber hecho el cambio del umask, en cambio, carlosPerez mantiene los permisos del umask antiguo, hay que cambiarlos para dejarlos como los de un usuario común.



Para finalizar la configuración y que se apliquen los cambios del cliente, reiniciamos la máquina:

*$ reiniciar*

Si queremos mostrar todos los usuarios de los sitios indicados en *nsswitch.conf*: "compat/files" y "ldap" haremos:

*$ getent passwd*

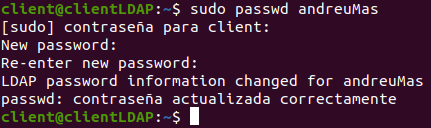
## Comprobación de la configuración

**Cliente**

Como parte final comprobaremos que todo nos funciona correctamente. No lo hará a la primera, ya que es fácil que nos dejemos o nos equivoquemos en algo.

Los usuarios que crecimos anteriormente aún no tienen contraseña. Por lo tanto ejecutaremos la orden "passwd usuari" para modificar su password:

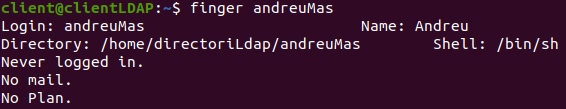
*$ sudo passwd cmateu*



Si este paso no da problemas ya vamos por el buen camino. Como nuestra máquina local no tiene el usuario "cmateu" en el archivo /etc/passwd, está claro que el usuario está interviniendo.

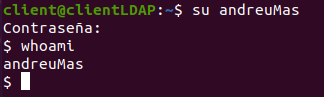
También podemos comprobar si el usuario existe con la orden ***finger*** que hay que instalar previamente:

*$ dedo cmateu*



Podemos probar a hacer laautenticación directamente sobre la consola con "su"

*$ su cmateu*



Cuenta, la autenticación solo funcionará mediante el terminal (u otro escritorio tty del S.O.), no con entorno gráfico, eso lo veremos más avante.

## Configuración para iniciar sesión en entorno gráfico

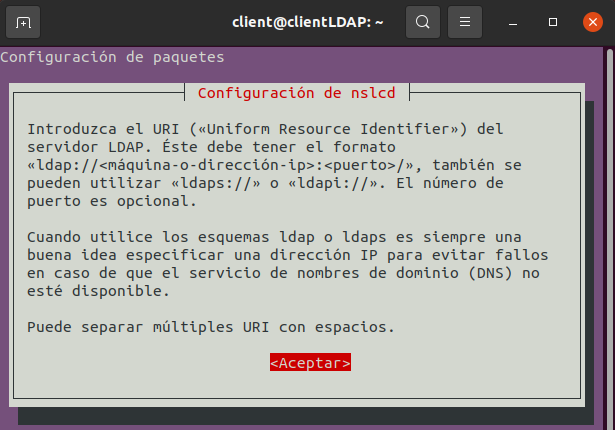
**Cliente**

Partiendo de que ya tenemos el servicio funcionando y que desde el cliente podemos iniciar sesión mediante el terminal, solamente nos queda configurar el inicio de sesión con GUI (entorno gráfico), este paso se hace al final de todo el procedimiento para que detecte automáticamente la configuración del servicio slapd.

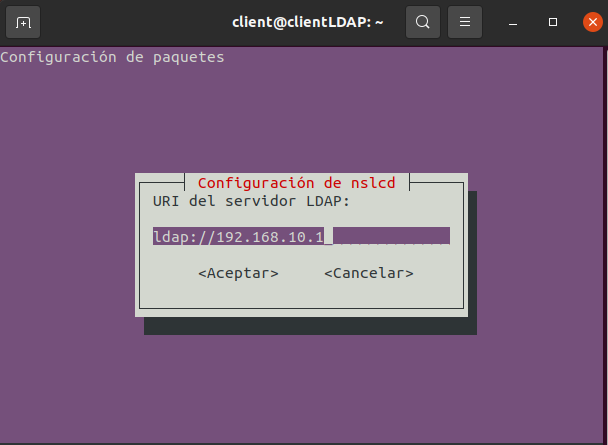
Nomas hay que instalar el paquete **nslcd**

*$ sudo apt install nslcd*

Este nos mostrará un asistente de instalación similar a los paquetes del punto 4.3 libpam-ldap y libnss-ldap, al que debemos seguir los pasos y automáticamente se activará el acceso mediante el entorno gráfico.



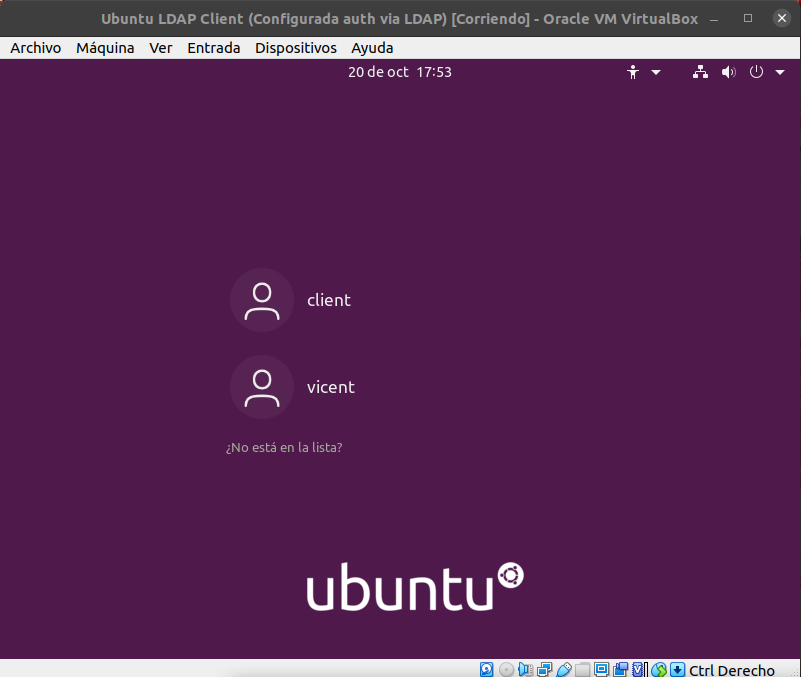
Si toda la configuración que hemos introducido en la configuración del cliente en los puntos anteriores es correcta, los campos nos aparecen autocompletados, solo hay que revisar que los datos son los correctos y seguir el asistente.



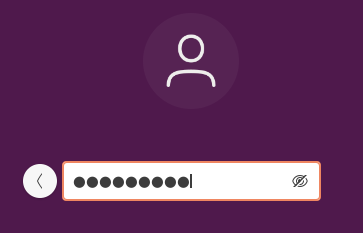
# 

Una vez instalado solo hay que reiniciar la máquina porque se aplican los cambios e intentar acceder desde el menú "login", mediante la opción "¿No está en la lista?":

CUENTA: Si nunca se ha hecho "login" al usuario que vamos a probar, reviso que aparece por pantalla el proceso de creación del directorio.



Introducimos los datos manualmente:



Esto hará el proceso de login y si todo está correcto nos mostrará el escritorio final del usuario mediante la autenticación por LDAP.

# 5. Configuración de los perfiles móviles

Ya tenemos configurado el directorio LDAP de manera que desde cualquier cliente puedo iniciar sesión con cualquier usuario del directorio. Sin embargo, su carpeta personal (que incluye su perfil y sus datos) se crea en cada máquina cliente, lo cual es un problema si el usuario no tiene un único ordenador cliente asignado (cosa que pasa normalmente en las aulas).

Lo que vamos a preparar se conoce como perfiles móviles, y lo que implica es que los usuarios tendrán todos sus ficheros estigmas en la máquina que estemos..

**Servidor**

Para hacer esto, el siguiente paso es hacer la configuración para que las carpetas personales de los usuarios móviles se alojen en el servidor directamente y se montan automáticamente en los clientes al iniciar sesión. Los pasos a hacer son:

* + Crear una carpeta en el servidor donde almacenar a los hombres de los usuarios móviles y compartirla con NFS (Network File System) con permisos de lectura y escritura para todos los clientes. Esta carpeta quizás el /hombre (pero estaremos exportando también las carpetas de los *usuarios locales* del servidor y eso no nos interesa) o cualquier otra, por ejemplo, **/home/usuariosldap**
  + Compartir el directorio que contiene los directorios personales de los clientes móviles, mediante el servicio NFS, para ello es necesario instalar el paquete NFS:

*$ sudo apt install nfs-kernel-server*

Una vez hecho esto, hay que añadir que se comparta en red el directorio "/home/usuarisldap" con el servicio NFS, por lo tanto, modificamos el fichero **/etc/exports**  y hay que añadir la siguiente línea:

*/home/usuarisldap \*(rw,sync,no\_root\_squash,no\_subtree\_check)*

La cual aplica los permisos de escritura y lectura, la sincronización de ficheros, que el usuario root del cliente pueda montar como root en el directorio compartido y desactiva que se revise los ficheros exportados desde la otra máquina (para evitar problemas a la sincronización).

Y reiniciamos la máquina del servidor, la parte del servidor ya la tenemos preparada.

**\* Si queréis más información sobre nfs y exports, reviséis los siguientes** [**NFS**](https://es.wikipedia.org/wiki/Network_File_System)  **y**  [**/etc/exports**](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/5/html/deployment_guide/s1-nfs-server-config-exports)

**Cliente**

Ahora vamos a trabajar con el cliente, hay que crear una carpeta que contendrá los contenidos que se guardan de cada usuario en el serverLDAP.

Para hacerlo fácil, vamos a crearla en la misma ubicación "/home/usuarisldap" y le damos permisos completos al directorio "chmod 777" lo que viene a ser "drwxrwxrwx".

Hecho esto, vamos a montar mediante el fichero "/etc/fstab", que la carpeta ubicada en el servidor se montará de forma automática en el arranque del sistema en nuestro directorio local.

Hay que **instalar el paquete "nfs-common"** para que el fstab monte correctamente el directorio alojado en el servidor, si no, voy como no funciona, accederé a /home/usuarisldap y dentro solo tenéis los documentos locales (no ninguno).

Por lo tanto, como tenemos el servidor con la IP: 192.168.10.1 y la carpeta está ubicada en /home/usuarisldap, vamos a añadir la siguiente línea al fichero /etc/fstab donde básicamente indicamos que la carpeta "/hombre/usuariosldap" del equipo remoto con IP 192.168.10.1, se montará en la carpeta local "/hombre/usuariosldap":

*192.168.10.1:/home/usuarisldap /home/usuarisldap nfs auto,noatime,nolock,bg,nfsvers=3, intr,tcp,actimeo=1800 0 0*

Quedaría así:



Y por último, es necesario que actualizamos a cada uno de los usuarios, la ruta de su propio directorio para que coincidiera con la carpeta móvil. Por ello, podemos hacerlo fácilmente con el entorno gráfico, pero es un proceso lento ir de uno en uno.

Tendríamos



Lo cambiamos e indicamos el nuevo directorio:



**CUESTIÓN:** Una mejora que podríamos implementar es preparar un script que mediante el orden "ladpmodify" vaya de uno en uno haciendo este cambio. Y también moga el contenido de cada uno de los directorios personales de los usuarios del antiguo directorio al sincronizado con el servidor.

**CUESTIÓN:** ¿Hay que crear manualmente la carpeta de cada usuario y hacer todo ese proceso o podríamos hacer que se cree automáticamente la primera vez que se loguee en un equipo cliente?

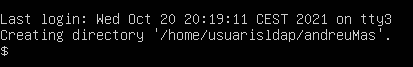
Si no creamos la carpeta manualmente, cuando iniciamos sesión esta se crea automáticamente, coge la configuración de permisos únicos para el usuario (755), los permisos basados en el "umask" que vamos a indicar en el fichero que hemos visto anteriormente (/etc/pam.d/common-session).

El propietario y grupo lo coge automáticamente de la configuración del usuario en el servidor LDAP. Como no estamos moviendo los datos de "/home/directoriLdap" (local) a "/home/usuarisldap" (NFS) todos los datos que tenía localmente ese usuario no le aparecerán. Hay que moverlas si queremos preservarlas. Igualmente, los ficheros ubicados en "/etc/skel" también se moverán cuando se crea el nuevo directorio de forma automática.

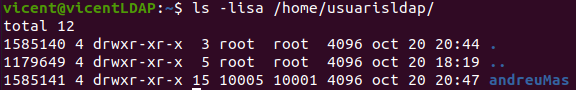
1. **Cuenta ací, cuando movemos toda la información existente localmente de los usuarios al nuevo directorio montado por NFS, hay que borrar el directorio local (/home/directoriLdap) para que LDAP funcione correctamente.**
2. **Esto se debe a que cuando el sistema detecta 2 "homeDirectory" por un mismo usuario, cogerá el directorio más antiguo (en este caso el local).**
3. **Otra posible solución para este problema, es modificar el fichero "nsswitch.conf" el orden en que "passwd" y "group" revisará las cuentas de usuario. Actualmente la orden es "files" -> "systemd" -> "ldap", habría que cambiarlo por "ldap" -> "filas" -> "ldap"**

**Por último, reiniciar la máquina para que coja los últimos datos actualizados del servidor LDAP.**

Finalmente, para verificar que todo está funcionando correctamente, deberíamos revisar haciendo "login" mediante un escritorio secundario de ubuntu ("tty3" por ejemplo) y revisando que cuando iniciamos sesión, crea automáticamente la carpeta que está en el servidor. Ejemplo de que no tenía ningún directorio antiguo:



Y si hacemos "login" y ejecutamos un "ls":



Desde este momento todo lo que creamos con ese usuario, realmente está guardándose en el servidor, y se conecte desde el cliente que se conecte tendrá exactamente lo mismo.

**CUENTA: Porque ahí funciona cuando el cliente arranque el servidor debe estar encerrado**  **si no, fallará el montaje del directorio NFS.**

# Enlaces de interés

* <http://www.yolinux.com/TUTORIALS/LinuxTutorialLDAP-DefineObjectsAndAttributes.html>
* [http://www.linuxquestions.org/questions/linux-server-73/how-to-add-a-new-schema-to-openldap-2-4-11-a-700452](http://www.linuxquestions.org/questions/linux-server-73/how-to-add-a-new-schema-to-openldap-2-4-11-a-700452/)
* <http://linuxgazette.net/130/peterson.html>
* <http://www.ite.educacion.es/formacion/materiales/85/cd/REDES_LINUX/openldap/Autentificacion_del_sistema_con_OpenLDAP.html>

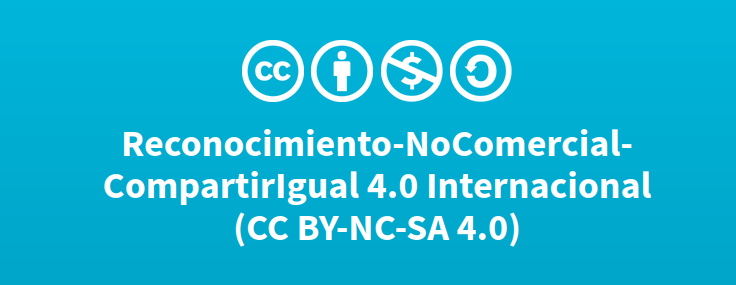
# Bibliografía

Temario original bajo licencia Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional:

Armand Mata (INS Joaquim Mir)

Javier Martínez (IES María Enríquez)

Vicent Benavent



Modificaciones por Vicent Benavent i Sentandreu:

-Actualizado el procedimiento de instalación en la última versión de Ubuntu 20.04-Actualizadas las capturas de pantalla de los procedimientos y el herraje Jxplorer.

-Adaptado y actualizado el módulo 4.6 (LDAP mediante el entorno gráfico) de la antigua versión en Ubuntu 20.04 con las nuevas herramientas y necesidades

- Añadido el módulo 4.7 (Perfiles móviles), para la última versión Ubuntu 20.04, junto con los paquetes necesarios para montar el sistema NFS tanto al cliente como al servidor