



MINISTERIO
DE EDUCACIÓN
Y CIENCIA

SECRETARÍA GENERAL
DE EDUCACIÓN
Y FORMACIÓN PROFESIONAL

DIRECCIÓN GENERAL
DE EDUCACIÓN,
FORMACIÓN PROFESIONAL
E INNOVACIÓN EDUCATIVA

CENTRO NACIONAL
DE INFORMACIÓN Y
COMUNICACIÓN EDUCATIVA

Redes de área local Aplicaciones y Servicios Linux

OpenLDAP (Ubuntu 10.04)



SERVICIO DE
FORMACIÓN DEL
PROFESORADO

C/ TORRELAGUNA, 58
28027 - MADRID

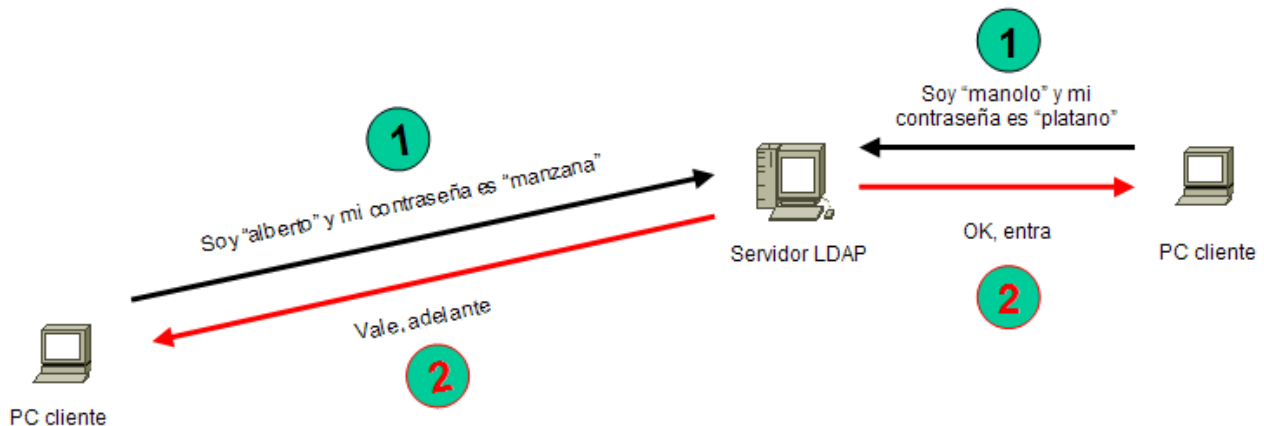
Índice de contenido

¿Qué es un servidor LDAP?	3
Instalación y configuración de OpenLDAP	3
Instalación de OpenLDAP	3
Configuración de OpenLDAP	4
Arranque y parada manual del servidor LDAP	7
Arranque automático del servidor LDAP al iniciar el sistema	7
Administración de OpenLDAP	7
Introducción	7
JXplorer - Explorador LDAP en java	7
Instalación de JXplorer	7
Conexión con el servidor LDAP	8
Organización del directorio LDAP	9
Creación de las unidades organizativas	9
Usuarios y grupos	10
Creación de grupos	10
Creación de usuarios	12
Autenticación basada en LDAP	13
Introducción	13
Librerías de autenticación pam-ldap y nss-ldap	13
Configuración de parámetros de librerías	17
Configurar servicios PAM	18
Configuración archivo common-auth	18
Configuración archivo common-account	19
Configuración archivo common-session	19
Configuración archivo common-password	19
Configuración particular para cada servicio	19
Probar la autenticación	19
Autenticación segura con OpenLDAP	20
Justificación	20
LDAP seguro - ldaps	21
1.- Crear una nueva entidad certificadora	21
2.- Crear una petición de firma de certificado de servidor	22
3.- Firmar el certificado con la CA	22
4.- Conceder permisos de lectura a los certificados	22
5.- Configurar slapd para que utilice los certificados	22
6.- Modificar script de inicio de slapd para que utilice protocolo seguro ldaps	23
7.- Reiniciar servidor LDAP	23
Probando el acceso por SSL	23

¿Qué es un servidor LDAP?

Un servidor LDAP es un servidor de datos optimizado para la realización rápida de consultas de lectura y orientado al almacenamiento de datos de usuarios a modo de directorio.

La principal utilidad de un directorio LDAP es como servidor de autenticación para los distintos servicios de un sistema informático como puedan ser: autenticación para entrar en un PC, para entrar en una aplicación web, para acceder a un servidor ftp, para acceder a servidores de correo entrante POP3 y saliente SMTP, etc...



Si en nuestra red disponemos de un servidor LDAP y configuramos todos los PCs y todos los servicios de la red para que se autentifiquen en él, bastará con crear las cuentas de usuario y grupos de usuarios en nuestro servidor LDAP para que los usuarios puedan hacer uso del sistema y de sus servicios desde cualquier puesto de la red. Es un sistema ideal para centralizar la administración de usuarios en un único lugar.

En el curso veremos cómo poner en marcha un servidor LDAP y cómo configurar el resto de PCs clientes de la red para que se autentifiquen en él. También utilizaremos OpenSSL para que durante el proceso de autenticación los datos viajen encriptados por la red, así ningún curioso podrá averiguar nuestras contraseñas. Además utilizaremos LDAP para que autentique el acceso al servidor ftp y el acceso a páginas restringidas en el servidor web.

Instalación y configuración de OpenLDAP

Para simplificar la administración de los usuarios del sistema es ideal utilizar una base de datos accesible mediante LDAP. Almacenar las cuentas de usuario de forma centralizada en un único repositorio facilitará la creación, modificación y eliminación de cuentas de usuario y grupos de usuarios. Será necesario configurar los PCs de la red para que utilicen el servidor LDAP como servidor de autenticación.

Instalación de OpenLDAP

El servidor OpenLDAP está disponible en el paquete **slapd** por tanto, lo instalaremos utilizando apt-get. También nos conviene instalar el paquete **ldap-utils** que contiene utilidades adicionales:

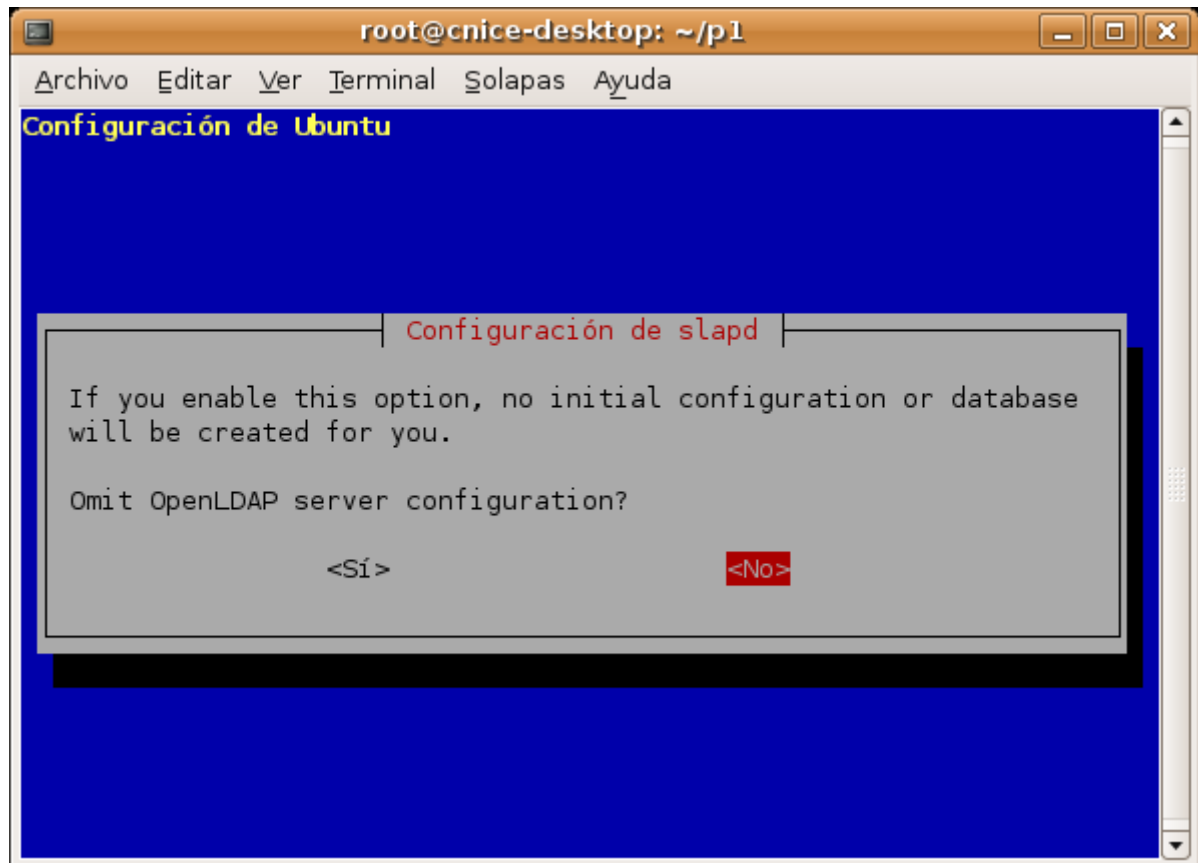
```
// Instalación del servidor LDAP
# apt-get install slapd ldap-utils
```

Configuración de OpenLDAP

La configuración del servidor LDAP se almacena en el archivo `/etc/ldap/slapd.conf`. Podemos editar manualmente dicho archivo, pero es mejor lanzar el asistente de configuración de slapd. Para ello debemos ejecutar el siguiente comando:

```
//Lanzar el asistente de configuración de slapd  
# dpkg-reconfigure slapd
```

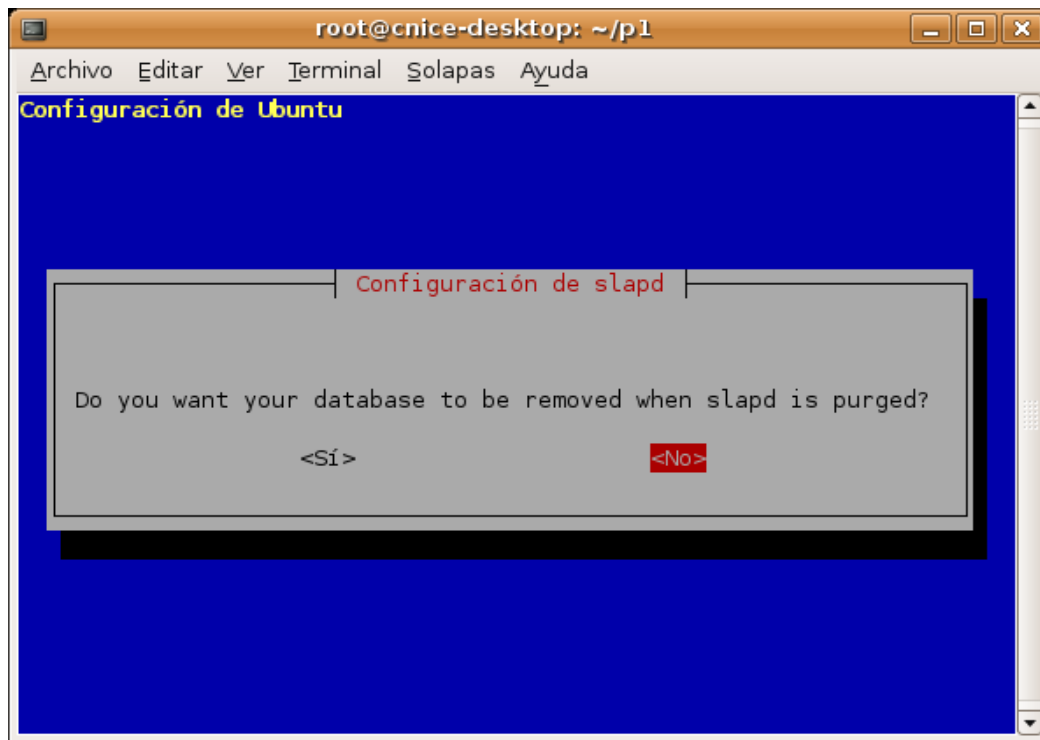
Lo primero que nos pregunta el asistente es si deseamos omitir la configuración del servidor LDAP:



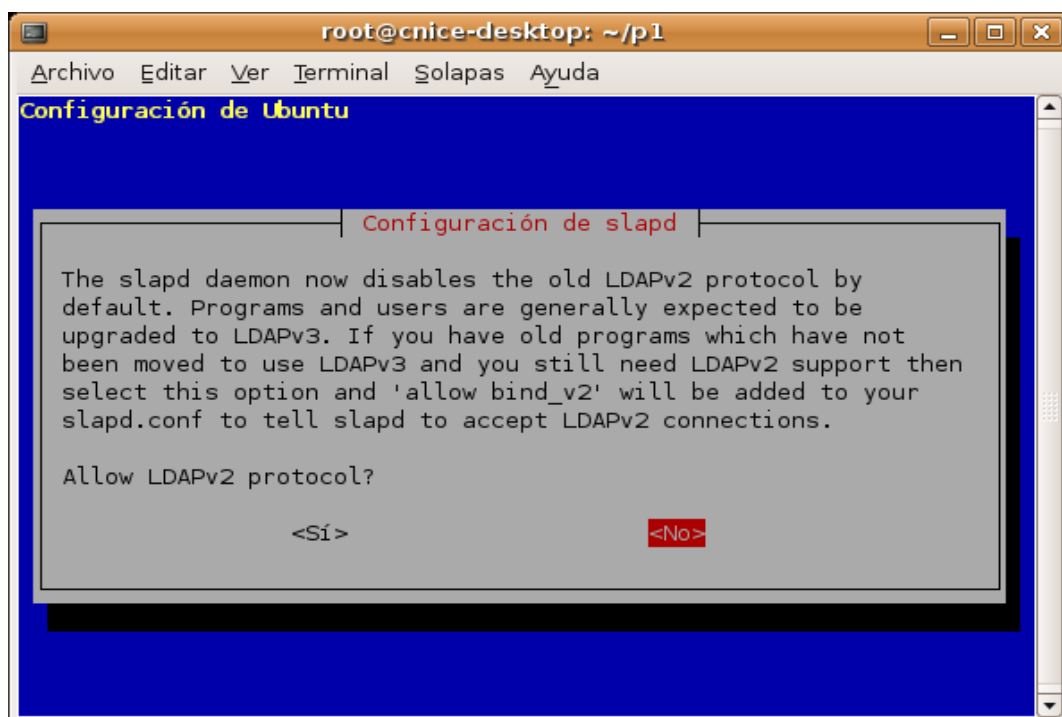
Obviamente responderemos que no, ya que precisamente lo que queremos es configurar el servidor LDAP.

La siguiente pregunta que nos hace el asistente es el nombre de nuestro dominio. Éste nombre lo utilizará para crear el nombre distinguido (DN) o dicho más claramente, nombre identificativo de la base de nuestro directorio LDAP.

Después nos preguntará si queremos que se elimine la base de datos cuando quitemos slapd. Por si acaso, lo mejor es responder que no:



Luego nos preguntará si deseamos utilizar LDAP versión 2, respondemos que no ya que apenas se utiliza.



A continuación, el administrador tiene que cargar los esquemas estandarizados que se usarán. Recuerda que en un directorio LDAP, un esquema es un paquete donde se incluyen definiciones de clases, atributos y reglas. Los esquemas disponible se encuentran en el directorio /etc/ldap/schema.

```
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/cosine.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/nis.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/inetorgperson.ldif
```

Nuestro directorio LDAP debe tener una base, a partir de la cual cuelgan el resto de elementos. Como nombre de la base, habitualmente se utiliza el nombre del dominio. Ejemplo, si nuestro dominio es aula209.ieszv.es, lo normal es que la base para nuestro directorio LDAP sea: dc=aula209,dc=ieszv,dc=es.

```
# Load dynamic backend modules
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulepath: /usr/lib/ldap
olcModuleload: back_hdb.la

# Database settings
dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcSuffix: dc=aula209,dc=ieszv,dc=es
olcDbDirectory: /var/lib/ldap
olcRootDN: cn=admin,dc=aula209,dc=ieszv,dc=es
olcRootPW: admin
olcDbConfig: set_cachesize 0 2097152 0
olcDbConfig: set_lik_max_objects 1500
olcDbConfig: set_lik_max_locks 1500
olcDbConfig: set_lik_max_lockers 1500
olcDbIndex: objectClass eq
olcLastMod: TRUE
olcDbCheckpoint: 512 30
olcAccess: to attrs=userPassword by dn="cn=admin,dc=aula209,dc=ieszv,dc=es"
write by anonymous auth by self write by * none
olcAccess: to attrs=shadowLastChange by self write by * read
olcAccess: to dn.base="" by * read
olcAccess: to * by dn="cn=admin,dc=aula209,dc=ieszv,dc=es" write by * read
```

Si guardamos la configuración anterior en un fichero llamado **base.ldif** y ejecutamos el comando que sigue a continuación, conseguiremos tener nuestro servidor LDAP listo para trabajar con él.

```
ldapadd -Y EXTERNAL -H ldapi:/// -f base.ldif
```

Por último introducimos dentro del esquema anterior un nodo raíz con el cual poder empezar a trabajar.

```
# Create top-level object in domain
dn: dc=aula209,dc=ieszv,dc=es
objectClass: top
objectClass: dcObject
objectClass: organization
o: aula209 Organization
dc: aula209
description: Ejemplo LDAP aula209

# Admin user.
dn: cn=admin,dc=aula209,dc=ieszv,dc=es
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword: admin
```

Guardamos la configuración anterior en un fichero llamado **raiz.ldif** y ejecutamos el siguiente comando para añadir la entrada.

```
ldapadd -x -D cn=admin,dc=aula209,dc=ieszv,dc=es -W -f raiz.ldif
```

-x: autentifica de forma simple, -D: dn indicado en el fichero de configuración
-w: solicita contraseña, -f: fichero de configuración

Arranque y parada manual del servidor LDAP

El servidor LDAP, al igual que todos los servicios en Debian, dispone de un script de arranque y parada en la carpeta /etc/init.d.

```
// Arrancar o reiniciar el servidor LDAP
root@cnice-desktop:~# /etc/init.d/slaped restart
```

```
// Parar el servidor LDAP
root@cnice-desktop:~# /etc/init.d/slaped stop
```

Arranque automático del servidor LDAP al iniciar el sistema.

Para un arranque automático del servicio al iniciar el servidor, debemos crear los enlaces simbólicos correspondientes tal y como se indica en el apartado [Arranque automático de servicios al iniciar el sistema](#).

Administración de OpenLDAP

Introducción

Una vez instalado y configurado el servidor LDAP, la siguiente tarea es la del diseño de la estructura y la introducción de datos en el directorio.

Puesto que la finalidad de nuestro servidor LDAP es que sirva de almacén de usuarios y grupos para autenticar sistemas linux y servicios como ftp y web, deberemos crear una estructura que parta de la base de nuestro directorio, para almacenar dicha información. Tal y como se explica más abajo, crearemos una unidad organizativa (ou) llamada **groups**, para almacenar los grupos de usuarios y crearemos otra unidad organizativa llamada **users** para almacenar a los usuarios.

JXplorer - Explorador LDAP en java.

Por su calidad superior, en este curso utilizaremos JXplorer para administrar el directorio LDAP.

Instalación de JXplorer

```
apt-get install jxplorer
```

Después, debemos abrir un terminal y lo ejecutamos con el siguiente comando:

```
# jxplorer &
```

Veremos la pantalla principal de JXplorer:



Conexión con el servidor LDAP

La conexión con el servidor LDAP podemos hacerla como usuario anónimo o como usuario administrador. Si conectamos de forma anónima solo podremos visualizar los elementos pero no podremos hacer cambios. Si conectamos como administrador, podremos crear, modificar y eliminar elementos de cualquier tipo.

Para conectar al servidor LDAP como administrador necesitamos la siguiente información:

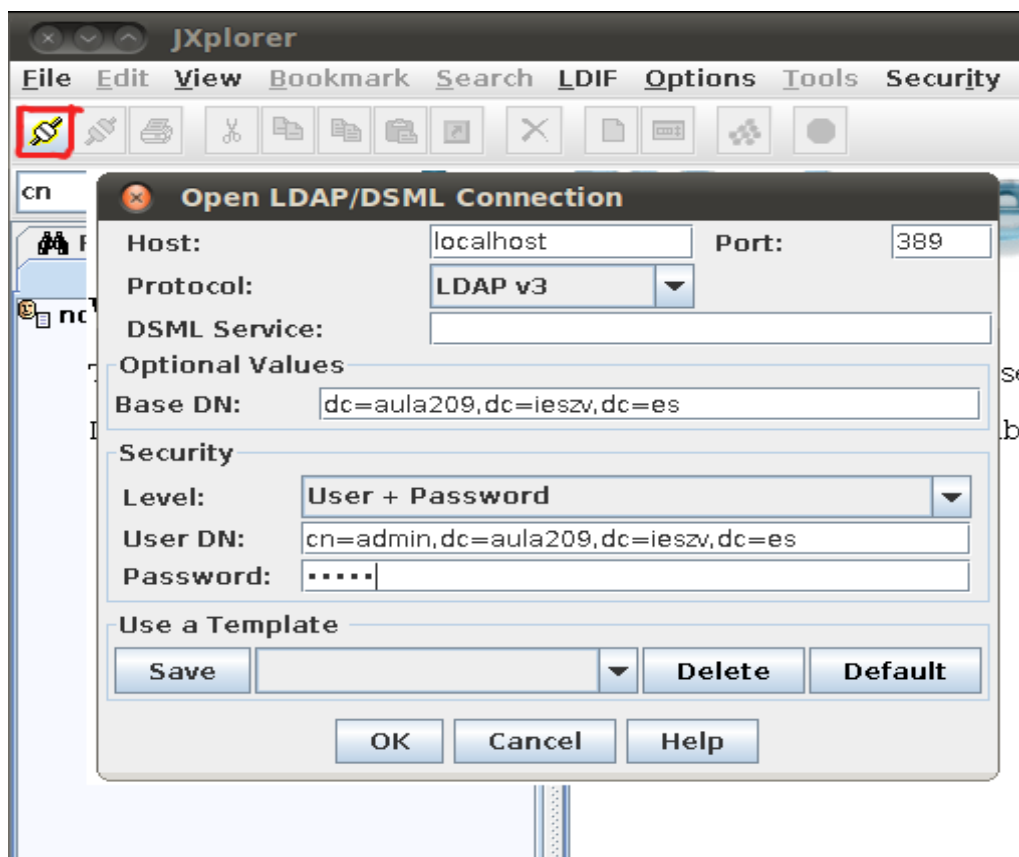
- Dirección IP del servidor LDAP
- Puerto 389
- Protocolo del servidor (LDAP v3 en nuestro caso)
- Base del directorio (dc=aula209,dc=ieszv,dc=es en nuestro caso)
- Nombre de usuario administrador (cn=admin,dc=aula209,dc=ieszv,dc=es en nuestro caso)
- Contraseña (admin en nuestro caso)

La base del directorio se suele denominar en inglés 'base DN' o 'Nombre Distinguido de la base del directorio'. Se corresponde con el parámetro 'suffix' del archivo de configuración del servidor LDAP /etc/ldap/slapd.conf.

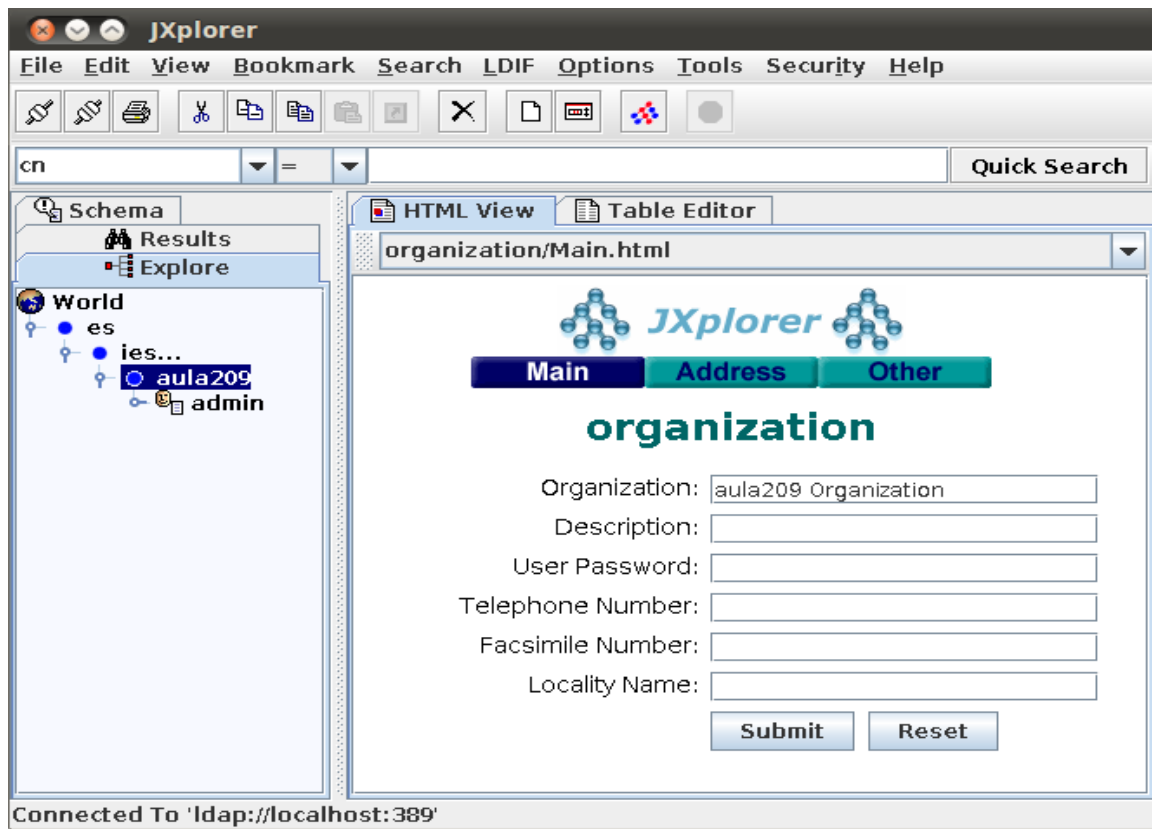
El nombre del usuario con el que nos conectamos se suele denominar en inglés 'user DN' o también 'bind DN'

El nombre de usuario administrador por defecto suele ser admin y a menudo hay que proporcionar nombre y base del directorio: cn=admin,dc=aula209,dc=ieszv,dc=es

Al hacer clic en el botón 'conectar' (marcado con círculo rojo en la figura) nos aparecerá el diálogo de conexión para que introduzcamos los datos de la conexión. Para no tener que introducir dicha información cada vez que conectemos, podemos grabar los datos pulsando 'Save'.



Si pulsamos OK, JXplorer conectará con el servidor LDAP y mostrará el directorio:



Vemos que en nuestro directorio directamente hay dos elementos: una organización llamada 'aula209' el usuario administrador llamado 'admin'.

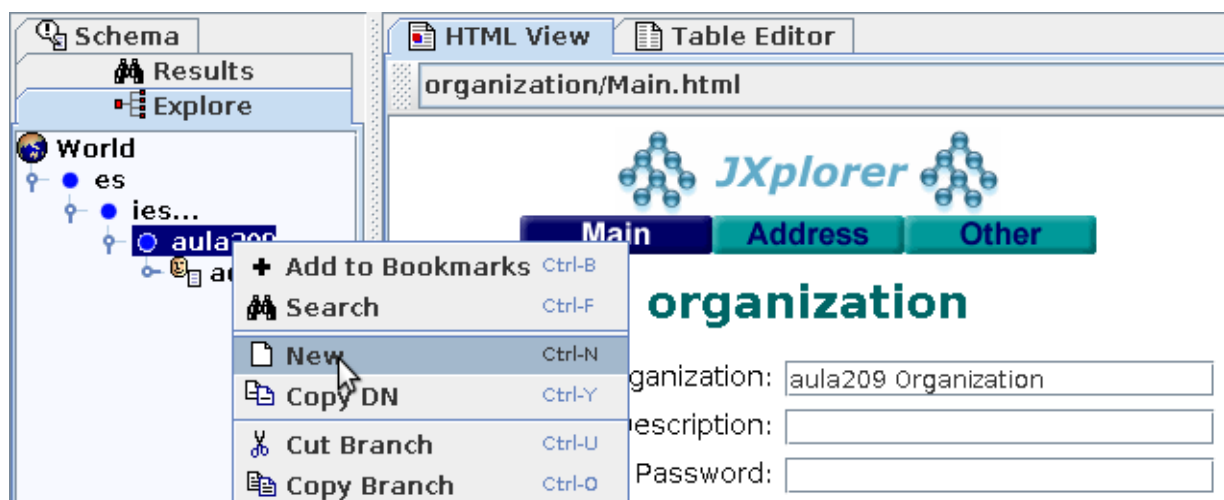
Organización del directorio LDAP

Creación de las unidades organizativas

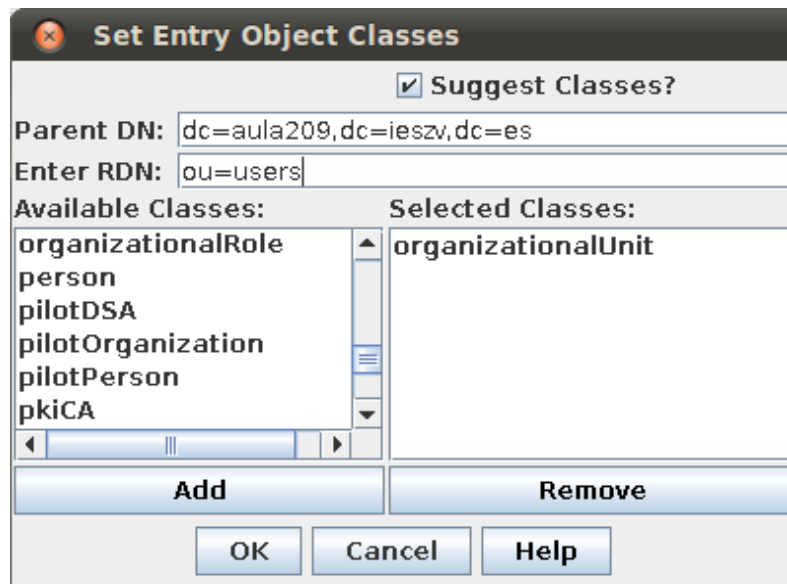
Puesto que nuestro directorio va a almacenar usuarios y grupos, vamos a crear sendas unidades organizativas (en inglés organizational unit - ou) llamadas 'users' y 'groups' que nos servirán para organizar los usuarios y los grupos por separado.

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 derecho sobre la organización 'aula209' y en el menú contextual elegiremos 'New'



Nos aparecerá la ventana 'Set Entry Object Classes' que podríamos traducir por 'Seleccione las clases objeto de la nueva entrada' o mejor, 'Seleccione las tipologías'. En ella podremos elegir los 'tipos' que tendrá nuestro nuevo elemento. Como se trata de una unidad organizativa (en inglés organizational unit - ou) debemos seleccionar el tipo organizationalUnit en la lista de la izquierda y pulsar el botón añadir (Add). Los otros dos tipos que aparecen por defecto (organizationalRole y simpleSecurityObject) no los necesitaremos, por lo tanto podemos seleccionarlos de la lista de la derecha y pulsar el botón quitar (remove). En la casilla 'Enter RDN' (introducir Nombre Distinguido Relativo) debemos poner el nombre de nuestro elemento. Escribiremos ou=users. Estaremos en la situación de la siguiente figura:



Tan solo debemos pulsar el botón OK y Submit y ya se habrá creado nuestra unidad organizativa 'users'. Repetiremos los pasos para crear otra unidad organizativa llamada 'groups'. El resultado que obtendremos será:



Usuarios y grupos

Ahora solamente nos queda crear los usuarios, crear los grupos y asignar los usuarios a sus grupos. Dentro de nuestra unidad organizativa 'groups' crearemos los siguientes grupos:

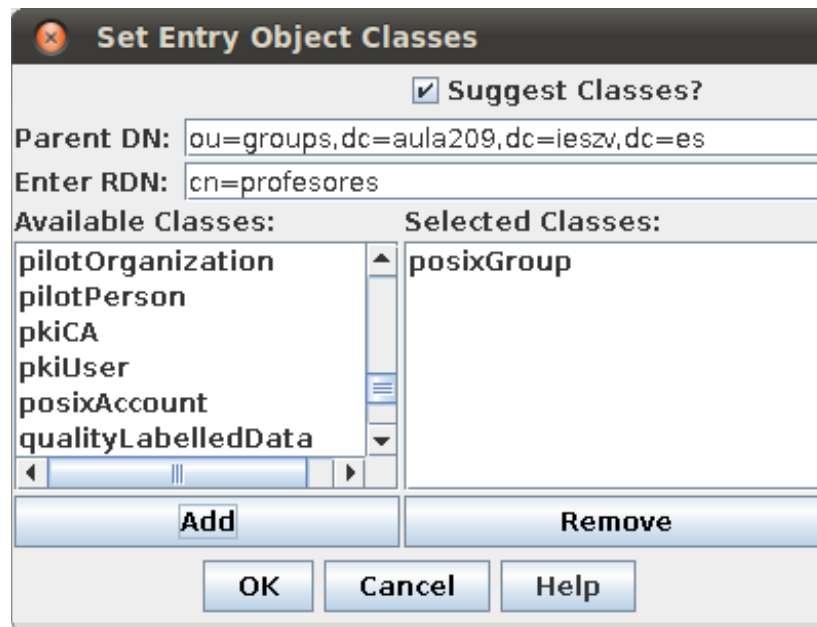
- profesores (gid=1001)
- alumnos (gid=1002)

Dentro de nuestra unidad organizativa 'users' crearemos los siguientes usuarios:

- javier (uid=1001, profesor)
- joaquin (uid=1002, profesor)
- miguel (uid=1003, profesor)
- jessica (uid=1004, alumno)
- joel (uid=1005, alumno)

Creación de grupos

Para crear los grupos, haremos clic con el derecho en la unidad organizativa 'groups' e igual que antes haremos clic en 'New'. Nuestro nuevo elemento será un nuevo grupo posix, por lo tanto debemos agregar el tipo 'posixGroup' de la lista de la izquierda. El nombre (RDN) será profesores, por tanto debemos escribir 'cn=profesores' (cn= Common Name - Nombre Común):



Set Entry Object Classes

☒ Suggest Classes?

Parent DN: ou=groups,dc=aula209,dc=ieszv,dc=es

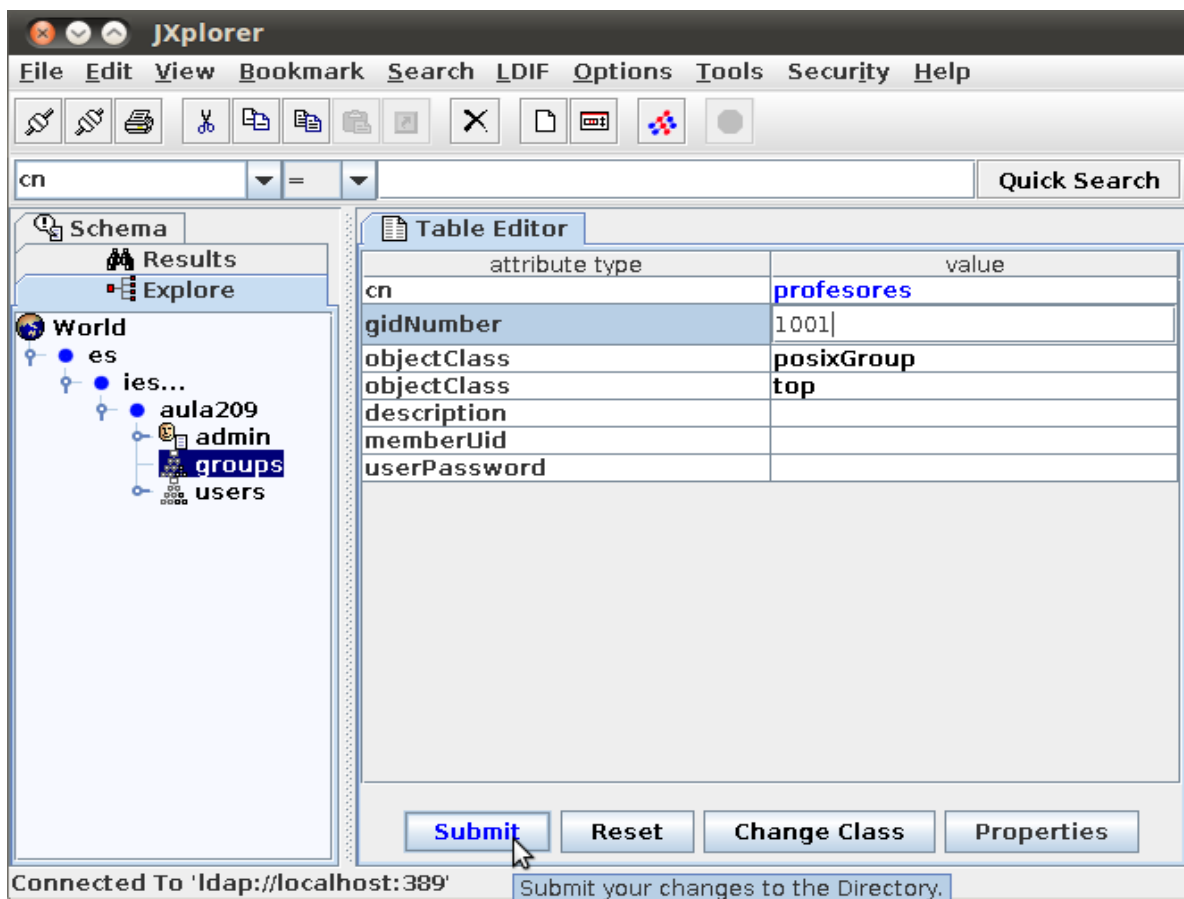
Enter RDN: cn=profesores

Available Classes:	Selected Classes:
pilotOrganization	posixGroup
pilotPerson	
pkiCA	
pkiUser	
posixAccount	
qualityLabelledData	

Add **Remove**

OK **Cancel** **Help**

Al pulsar OK nos aparecerá la siguiente figura, en la cual observamos los atributos clásicos de un grupo posix. Debemos rellenar al menos el campo gidNumber. También podemos introducir miembros al grupo. En el parámetro memberUid añadimos javier. Luego, haciendo clic con el derecho en javier > Add another value, podemos añadir otro valor: joaquin. De igual manera añadiremos a miguel. No importa que todavía no hayamos creado a dichos usuarios:



JXplorer

File Edit View Bookmark Search LDIF Options Tools Security Help

cn = Quick Search

Schema

- Results
- Explore
- World
 - es
 - ies...
 - aula209
 - admin
 - groups**
 - users

Table Editor

attribute type	value
cn	profesores
gidNumber	1001
objectClass	posixGroup
objectClass	top
description	
memberUid	
userPassword	

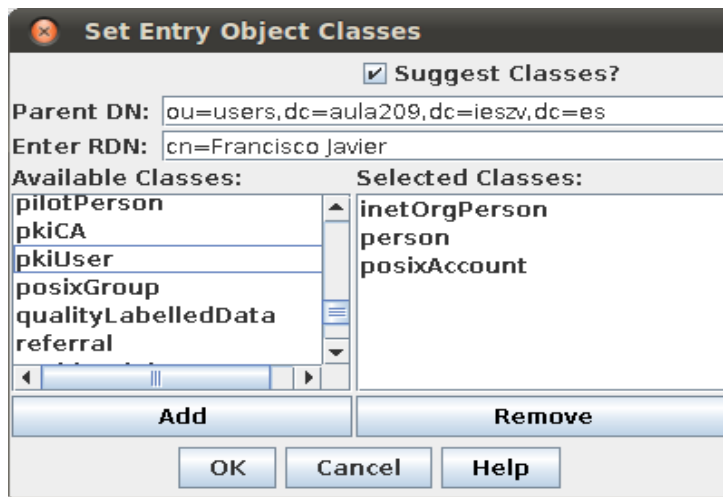
Submit **Reset** **Change Class** **Properties**

Connected To 'ldap://localhost:389'

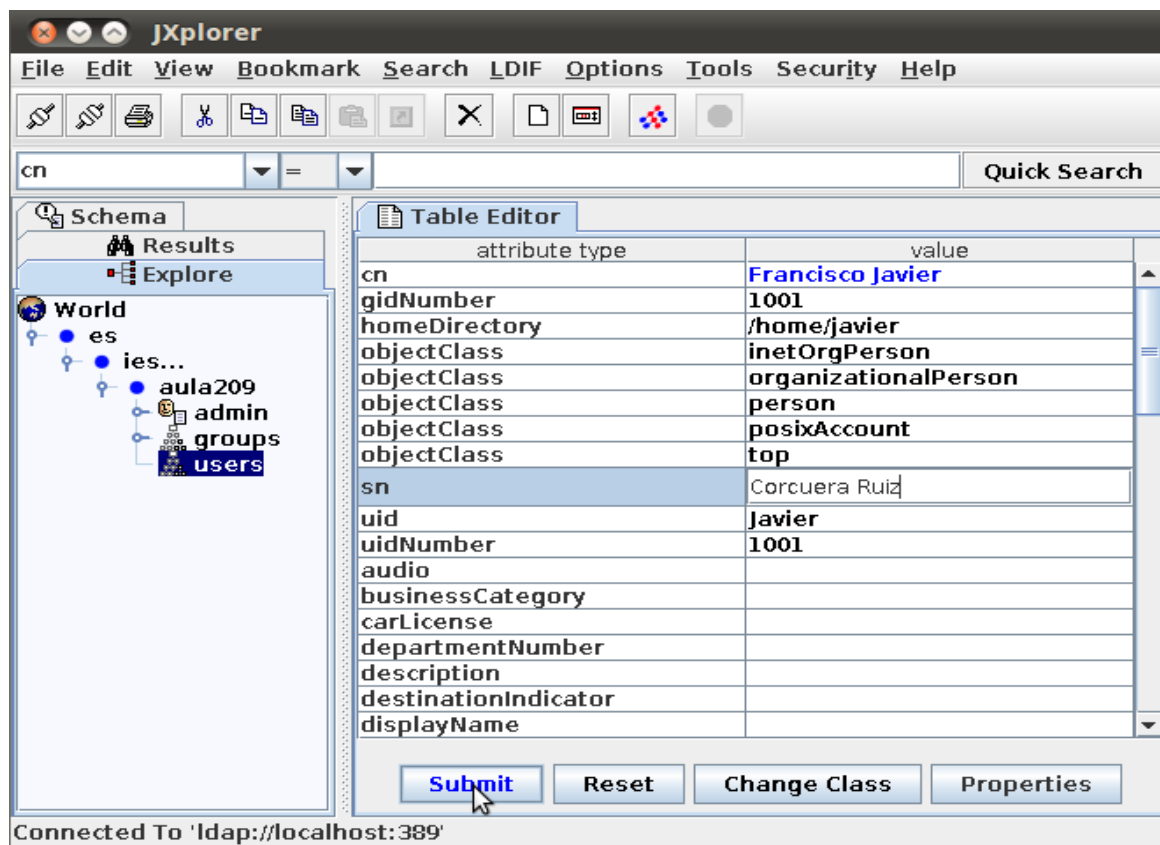
Submit your changes to the Directory.

Creación de usuarios

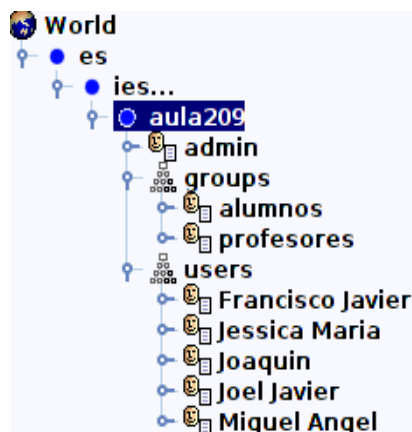
Para crear los usuarios, haremos clic con el derecho en la unidad organizativa 'users' e igual que antes haremos clic en 'New'. Nuestro nuevo elemento será un nuevo usuario posix, por lo tanto debemos agregar el tipo 'posixAccount' de la lista de la izquierda. Pero nuestro usuario también será una persona, por eso nos interesará agregar el tipo 'person' para disponer de los atributos de dicho tipo (nombre, apellidos, ...), además como será usuario de Internet nos interesará agregar también el tipo 'inetOrgPerson' para poder almacenar el e-mail y otros valores. Si su nombre es Francisco Javier, podemos escribir en la casilla RDN 'cn=Francisco Javier' (cn= Common Name - Nombre Común):



Al pulsar OK nos aparecerá la siguiente figura, en la cual observamos los atributos de las tres tipologías de nuestro elemento: persona, usuario de internet y cuenta posix. Debemos rellenar al menos los campos gidNumber (grupo primario que será el 1001), homeDirectory, uid (identificador), uidNumber, loginShell y sn (surname - apellidos). También añadiremos el e-mail aunque en la figura no se vea ya que está más abajo:



Lo mismo haremos con el resto hasta que tengamos creados los cinco usuarios. Al final nuestro servidor LDAP tendrá la siguiente información:



Ya tendríamos creada la estructura, los grupos y los usuarios que necesitamos para nuestro sistema.

Autenticación basada en LDAP

Introducción

Como ya hemos comentado anteriormente, una de las utilidades más importantes de un servidor LDAP es como servidor de autenticación. Autenticarse es necesario para entrar en un sistema linux. También para acceder a algunos servicios como un servidor FTP o a páginas privadas en un servidor web. En otros apartados veremos como utilizar un servidor LDAP para permitir el acceso a páginas web privadas y para autenticar a usuarios del servidor de ftp Proftpd. Aquí veremos las modificaciones que hay que realizar en un sistema Linux para que autentique a los usuarios en un servidor LDAP en lugar de utilizar los clásicos archivos **/etc/passwd**, **/etc/group** y **/etc/shadow**. Para ello es necesario instalar y configurar los paquetes **libpam-ldap** y **libnss-ldap**.

Librerías de autenticación pam-ldap y nss-ldap

La librería **pam-ldap** permite que las aplicaciones que utilizan PAM para autenticarse, puedan hacerlo mediante un servidor LDAP. Para que el sistema linux se autentique mediante un servidor LDAP es necesario instalar esta librería ya que utiliza PAM. El archivo de configuración de ésta librería es **/etc/pam_ldap.conf**. Hay otras aplicaciones o servicios que utilizan PAM para la autenticación y por 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 documento se indican los cambios necesarios en éstos 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 del sistema. Su archivo de configuración se encuentra en **/etc/libnss-ldap.conf**. Posteriormente deberemos configurar el archivo **/etc/nsswitch.conf** para que se utilice LDAP como base de datos del sistema en lugar de los archivos **passwd**, **group** y **shadow**.

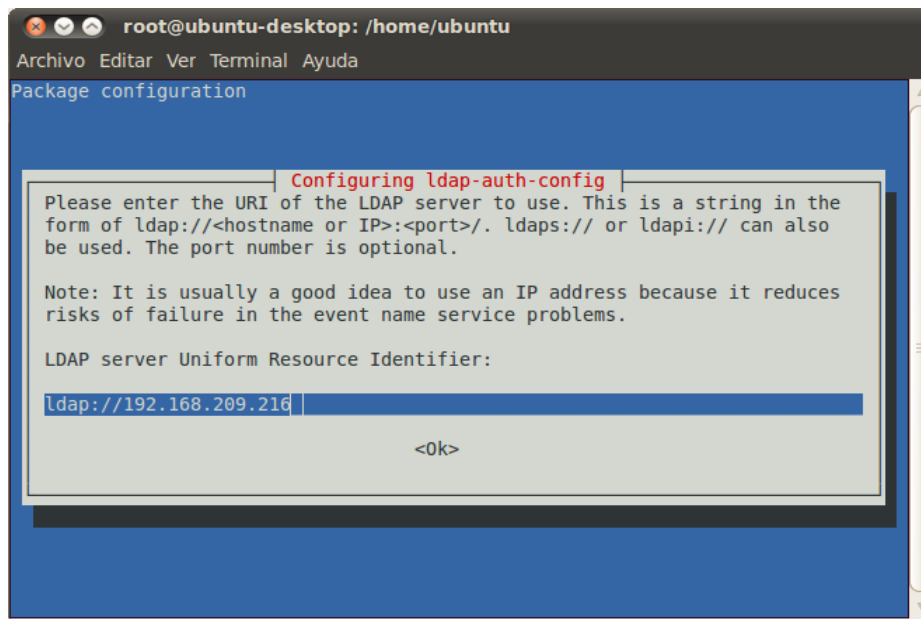
La instalación de ambas librerías se puede realizar mediante **apt-get**.

La instalación de la librería **libpam-ldap** se puede realizar ejecutando el comando:

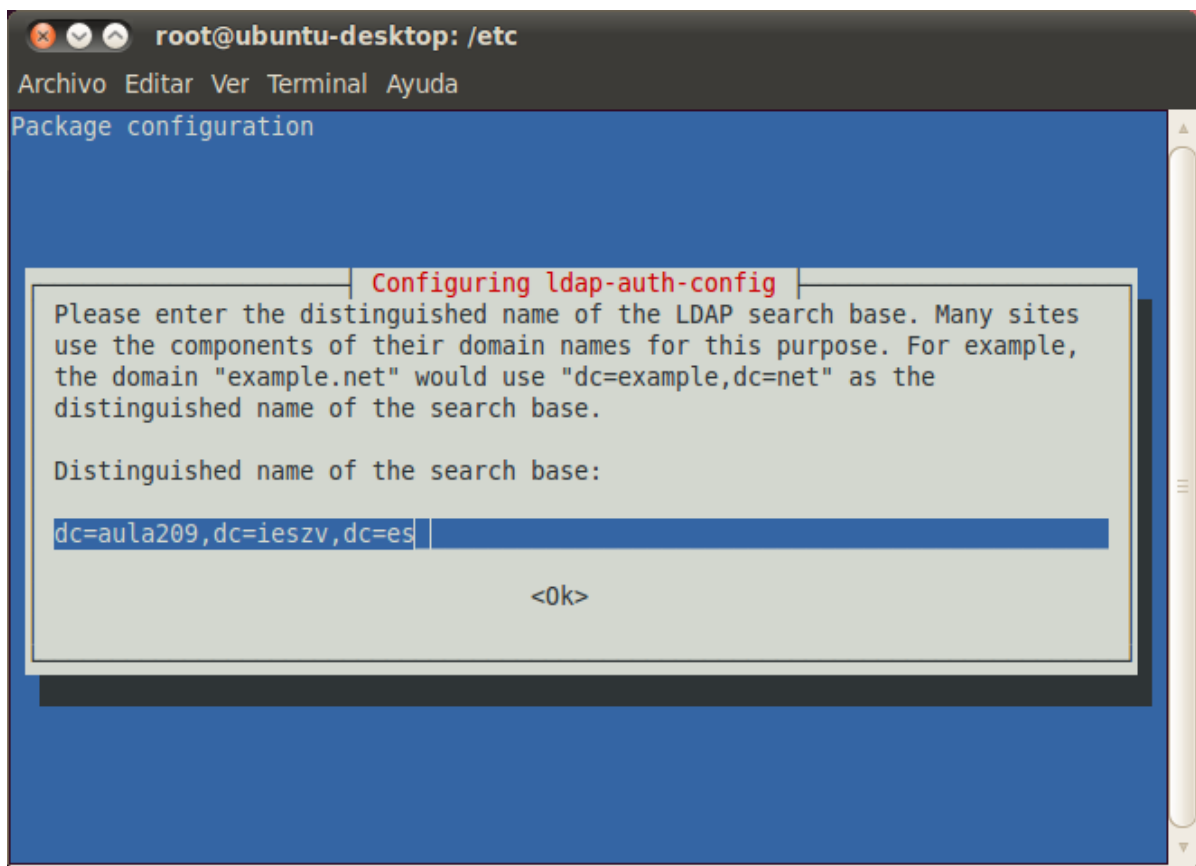
```
# apt-get install libpam-ldap
```

A continuación se iniciará el proceso de instalación de dicha librería junto con todas las dependencias de la misma como son: **libnss-ldap** y **ldap-auth-config** entre las más importantes.

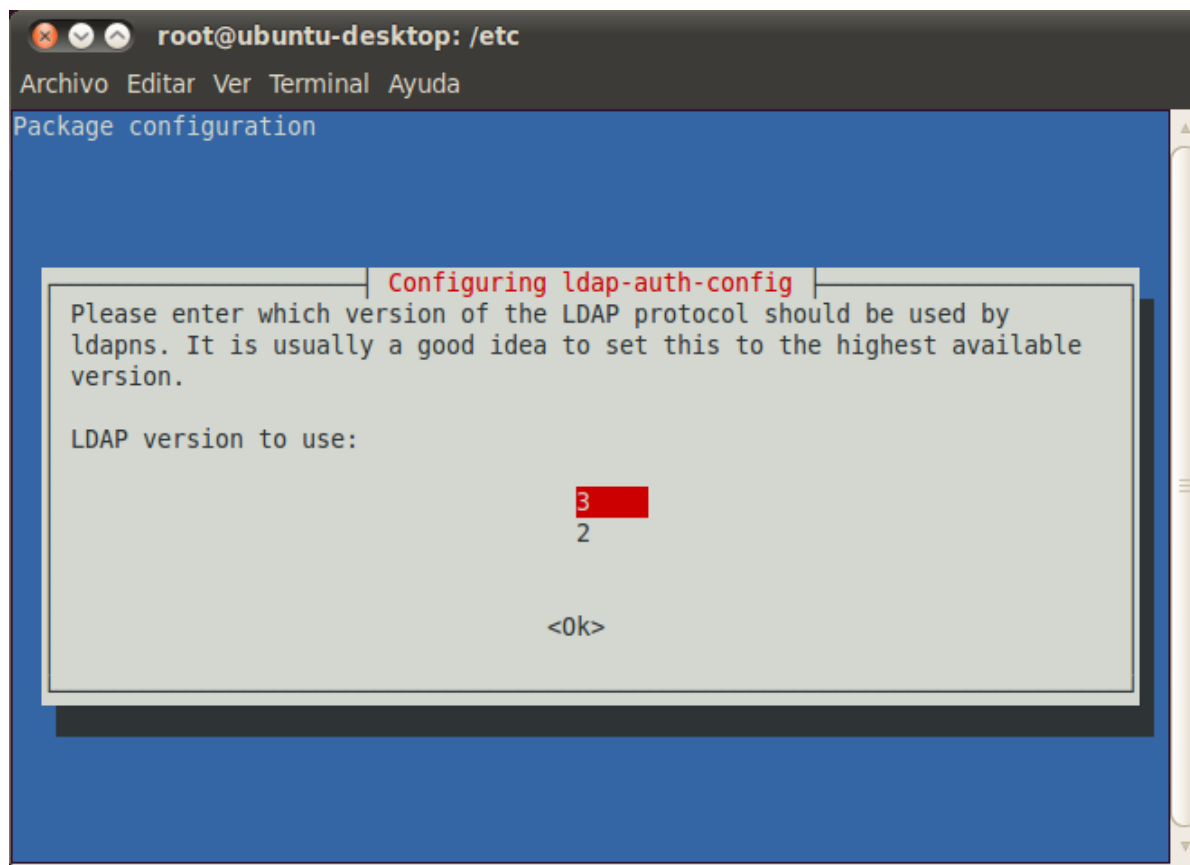
Acto seguido se iniciará el asistente de configuración de las librerías. La primera pregunta que nos hace el asistente es quién es el servidor LDAP. Podemos poner la IP o el nombre:



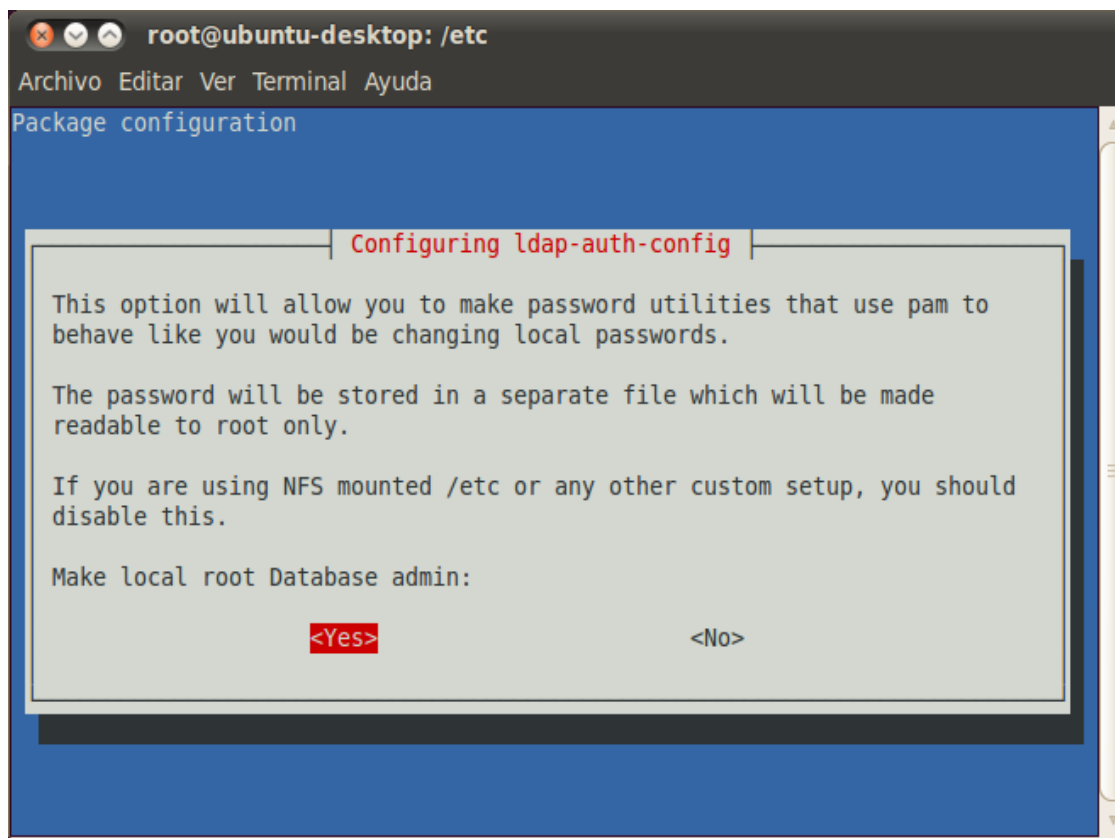
Luego nos preguntará por la base del directorio LDAP (base DN):



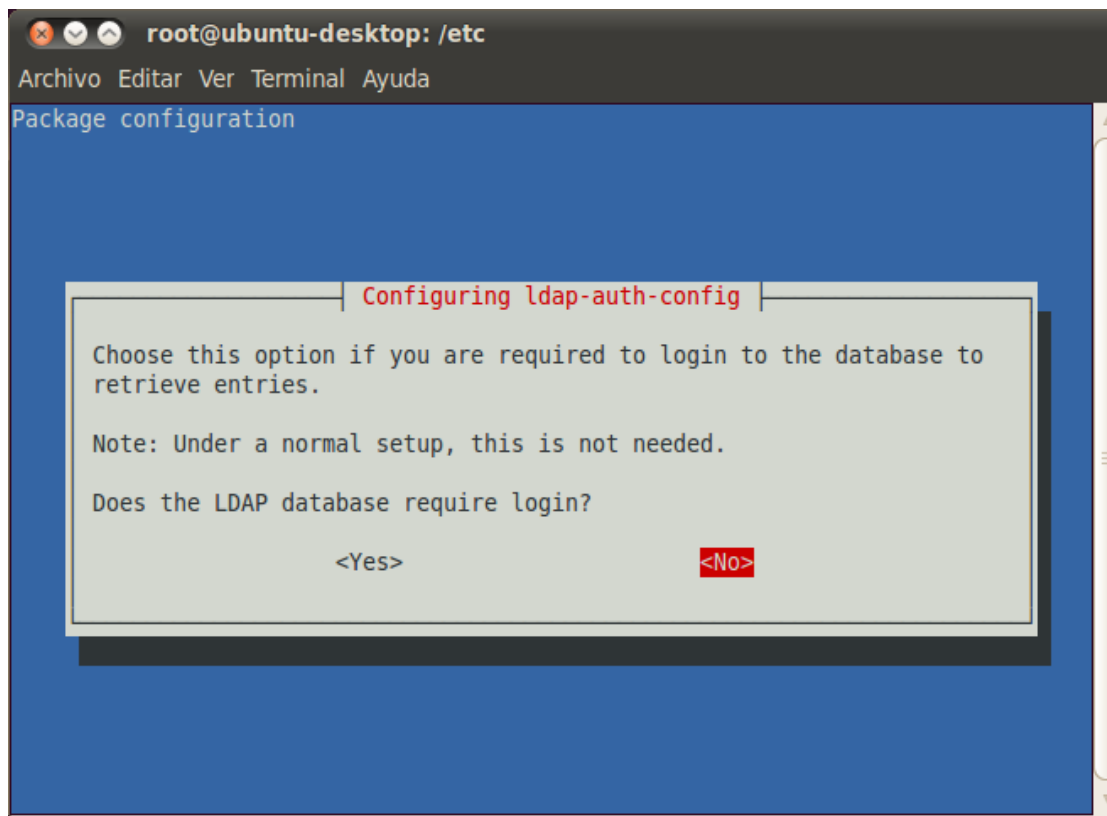
Acto seguido tendremos que indicar la versión de LDAP a utilizar:



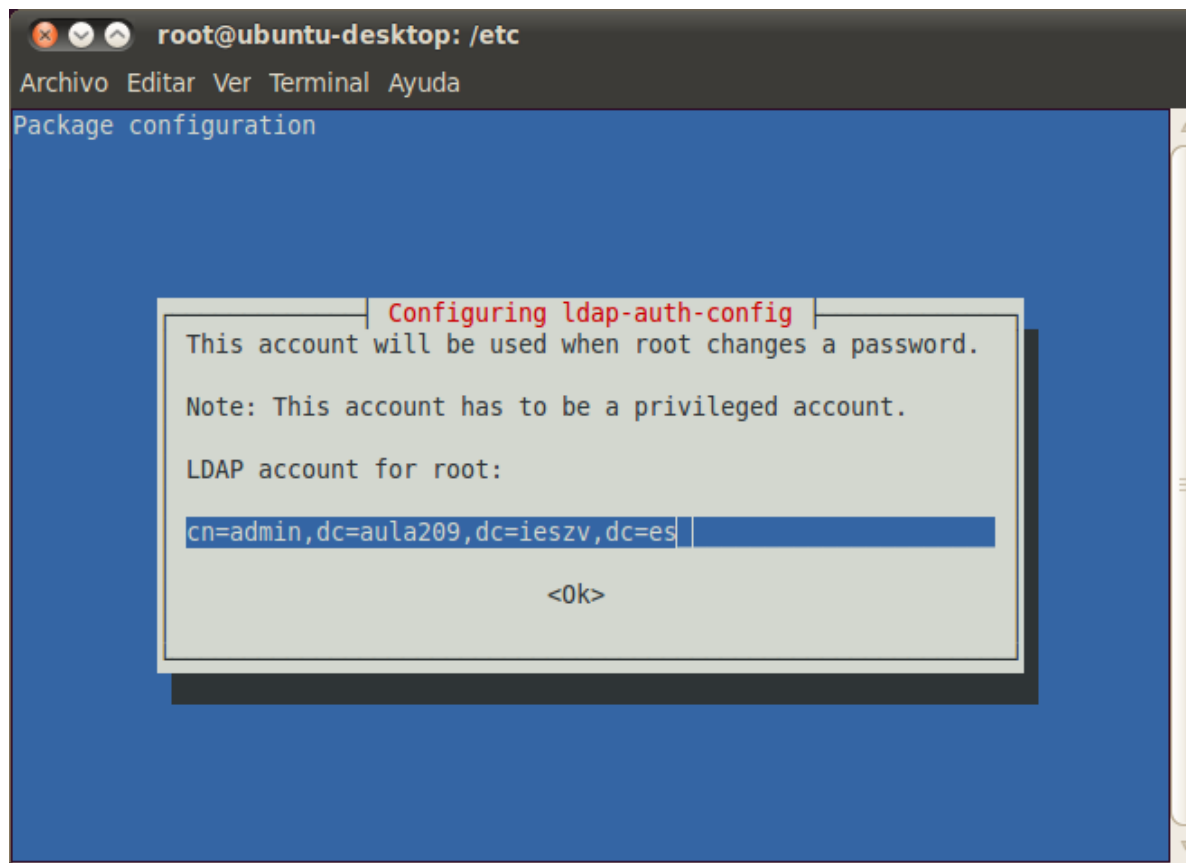
En este paso nos pregunta si queremos hacer que las herramientas de manejo de contraseñas que usa pam se comporten como si se tratase de contraseñas locales. Por defecto viene que sí, aceptamos.



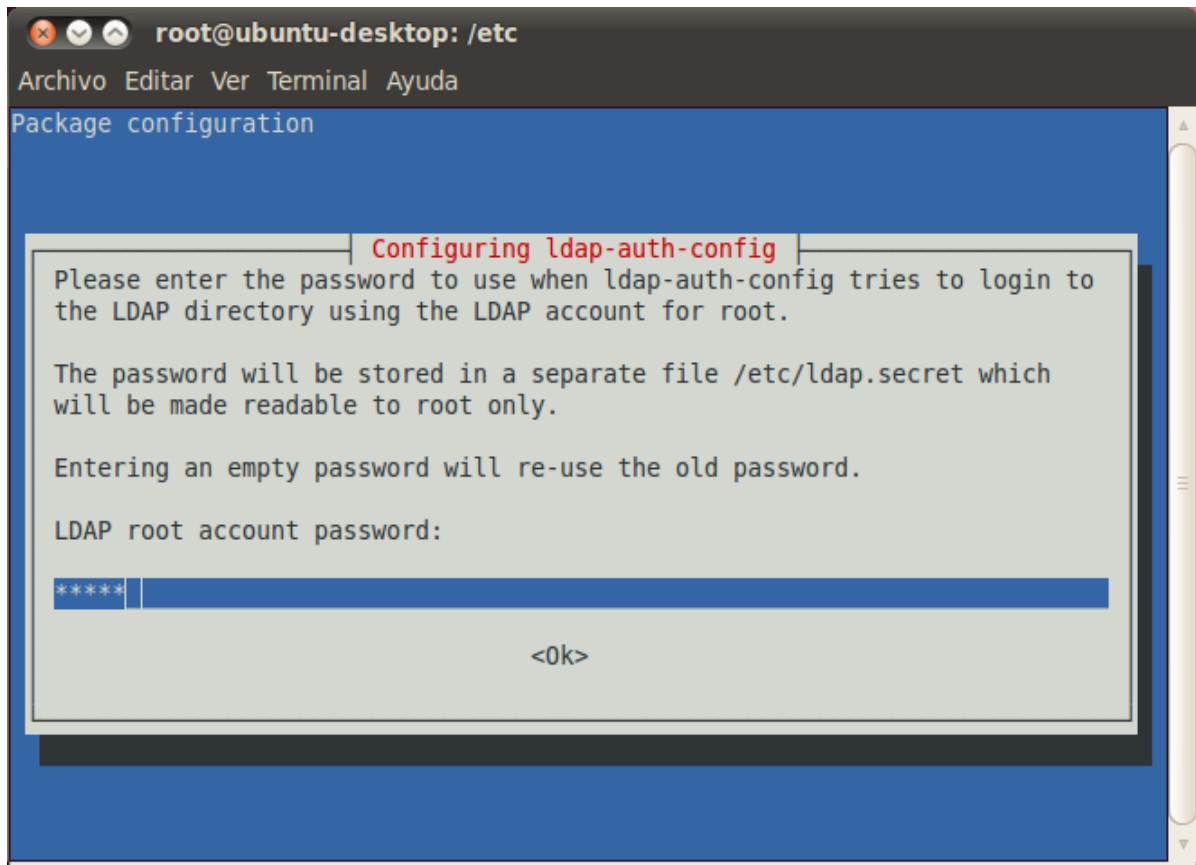
En el siguiente paso nos pregunta si necesitamos autenticarnos en el servidor LDAP o no. Como la librería únicamente va a realizar consultas, no es necesario autenticarse por lo tanto debemos responder 'No':



En el siguiente paso se nos pregunta por la cuenta del administrador de LDAP, introducimos la información adecuada como se muestra en la imagen.



Por último introducimos la contraseña del administrador (la misma que se usa en el servicio de LDAP)



Si nos equivocamos en algo, se puede lanzar dicho asistente de nuevo mediante el comando

```
// Lanzar asistente de configuración de ldap-auth-config
# dpkg-reconfigure ldap-auth-config
```

Configuración de parámetros de librerías

El archivo de configuración de la librería es el archivo **/etc/ldap.conf**. Únicamente hay que configurar los siguientes parámetros:

1. Quién es el servidor LDAP (nombre o IP)
- 2.Cuál es la base de nuestro directorio LDAP (base DN)
- 3.Cuál es la versión de LDAP a utilizar
4. Quién es el administrador del directorio
5. En qué unidad organizativa se encuentran los usuarios (sustituto de **/etc/passwd**)
6. En qué unidad organizativa se encuentran las contraseñas (sustituto de **/etc/shadow**)
7. En qué unidad organizativa se encuentran los grupos (sustituto de **/etc/group**)

Para ello las líneas que hay que modificar en el archivo de configuración son las siguientes (el valor de los parámetros es un ejemplo):

```
// Configurar en /etc/ldap.conf
host 192.168.209.216 //nombre o IP del servidor LDAP
uri ldap://192.168.209.216
base dc=aula209,dc=ieszv,dc=es
ldap_version 3
rootbinddn cn=admin,dc=aula209,dc=ieszv,dc=es
nss_base_passwd ou=users,dc=aula209,dc=ieszv,dc=es?one
nss_base_shadow ou=users,dc=aula209,dc=ieszv,dc=es?one
nss_base_group ou=groups,dc=aula209,dc=ieszv,dc=es?one
```

Para que el servidor LDAP actúe como si se tratara de los archivos passwd, group y shadow, además de

instalar las dos librerías anteriores, debemos indicar que se utilice LDAP como alternativa para autenticar usuarios. Para ello hay que añadir en las líneas que hacen referencia a passwd, group y shadow en el archivo `/etc/nsswitch.conf`, la palabra 'ldap' tras la palabra 'compat' quedando el archivo `/etc/nsswitch.conf` así:

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

passwd:          compat ldap
group:           compat ldap
shadow:          compat ldap

hosts:           files dns
networks:         files

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

netgroup:         nis
```

Configurar servicios PAM

Nuestro sistema ya estaría preparado para autenticarse por LDAP. Editando los archivos que hay en la carpeta `/etc/pam.d`, podemos configurar la forma en la que se autentifica cada uno de los servicios que requieren autenticación.

Para no tener que configurar de cada uno de los servicios, existen unos archivos comunes cuyo nombre empieza por **common** que afectan a la mayoría de ellos y sus archivos de configuración los referencian mediante una línea `@include` a los archivos comunes causando el mismo el efecto que si el contenido de los archivos comunes estuviera copiado en el lugar de la línea `@include`. Los archivos comunes son:

- `/etc/pam.d/common-auth` (para autenticarse)
- `/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 password)

Estos archivos contienen una línea que hace referencia a la librería `pam_unix.so` que corresponde a la autenticación contra los archivos UNIX. En Ubuntu 10.04 vienen configurados por defecto. Para que los servicios de nuestro sistema utilicen primero las librerías `pam_ldap.so` para autenticar al usuario, debemos comprobar que existe la línea correspondiente a `pam_ldap.so` por encima de la línea correspondiente a la librería `pam_unix.so` en los archivos `common`. Así, autenticará primero contra el servidor LDAP, y si la autenticación falla, probará después con los archivos UNIX.

Configuración archivo common-auth

Para que los servicios de nuestro sistema utilicen las librerías `pam-ldap` para autenticar al usuario, debemos comprobar en el archivo `/etc/pam.d/common-auth` la siguiente línea:

```
// Añadir en /etc/pam.d/common-auth encima de la línea pam_unix.so
auth      sufficient      pam_ldap.so
```

Configuración archivo common-account

Para permitir que los servicios de nuestro sistema comprueben la cuenta del usuario mediante las librerías pam-ldap, debemos comprobar en el archivo **/etc/pam.d/common-account** la siguiente línea:

```
// Añadir en /etc/pam.d/common-account encima de la línea pam_unix.so
account      sufficient      pam_ldap.so
```

Configuración archivo common-session

Para permitir que los servicios de nuestro sistema obtengan los parámetros de la sesión de usuario mediante las librerías pam-ldap, debemos comprobar en el archivo **/etc/pam.d/common-session** la siguiente línea:

```
// Añadir en /etc/pam.d/common-session encima de la línea pam_unix.so
session      sufficient      pam_ldap.so
```

Configuración archivo common-password

Para permitir que los servicios de nuestro sistema puedan modificar la contraseña del usuario mediante las librerías pam-ldap, debemos comprobar en el archivo **/etc/pam.d/common-password** la siguiente línea:

```
// Añadir en /etc/pam.d/common-password encima de la línea pam_unix.so
password     sufficient      pam_ldap.so
```

Configuración particular para cada servicio

Si deseamos que algún servicio se autentique de forma diferente, podemos editar el archivo del servicio (ej: **/etc/pam.d/su**, **/etc/pam.d/ssh**, **/etc/pam.d/ftp**, etc...), eliminar la línea que comienza por **@include** e introducir la configuración particular que deseemos.

Probar la autenticación

Nuestro servidor LDAP ya debería autenticar correctamente . Podemos probar la autenticación de los servicios mediante el comando **pamtest** que se encuentra en el paquete **libpam-dotfile**, por lo tanto debemos instalarlo:

```
// Instalación del comando pamtest
# apt-get install libpam-dotfile
```

Si deseamos probar que funciona el servicio **passwd** (cambiar contraseña) sobre un usuario del directorio LDAP (ejemplo **jessica**) , podemos ejecutar:

```
// Probando el cambio de contraseña
root@cnice-desktop:/etc/pam.d# pamtest passwd jessica
Trying to authenticate for service .
Password:                // Introducimos el password de jessica
Authentication successful. // La autenticación ha sido satisfactoria
```

También podemos utilizar el comando **finger** sobre usuarios que estén solamente en el directorio LDAP, por ejemplo **joel**:

```
// Probando finger
root@cnice-desktop:/etc/pam.d# finger joel
Login: joel                      Name: Joel Javier
Directory: /home/www/alumnos     Shell: /bin/sh
Last login Tue Sep 27 18:02 (CEST) on pts/3 from 192.168.0.213
No mail.
No Plan.
```

Podemos por ejemplo, desde una consola de root, cambiar mediante el comando 'su' (su=Switch User - cambiar de usuario) a un usuario que esté en el directorio LDAP, para lo cual no nos pedirá contraseña ya que root tiene permiso para cambiar a cualquier usuario. Si posteriormente cambiamos a otro usuario del directorio, ahora sí que nos pedirá contraseña. Debemos introducir la contraseña que esté almacenada en el directorio LDAP para dicho usuario:

```
// Cambiando de usuario
root@cnice-desktop:/etc/pam.d# su joel          // Somos root y cambiamos a joel
joel@cnice-desktop:                          // No nos pide password
joel@cnice-desktop:/etc/pam.d$ su jessica      // Somos joel, y cambiamos a jessica
Password:                                     // Nos pide password, le introducimos
jessica@cnice-desktop:/etc/pam.d$            // Ha cambiado correctamente
```

Las opciones de configuración de PAM son muy variadas. Para obtener más información se puede instalar el paquete libpam-doc que instala bastante documentación al respecto bajo la carpeta /usr/share/doc/libpam-doc/

Autenticación segura con OpenLDAP

Justificación

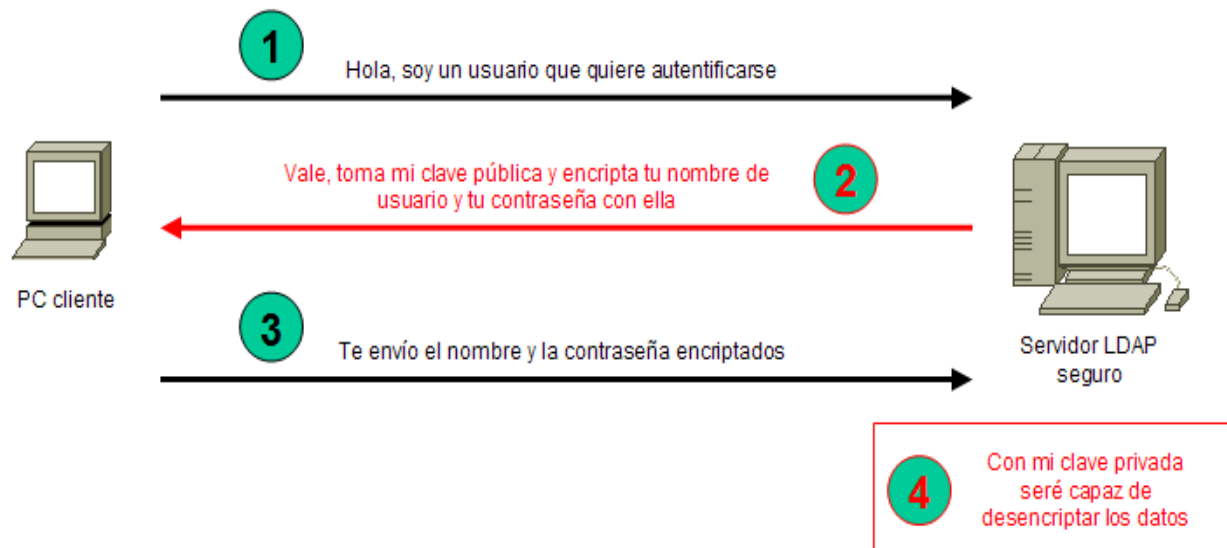
Los permisos que los usuarios tienen sobre los sistemas se basan en la autenticación del usuario. Aunque ya se han desarrollado sofisticados métodos de autenticación como sistemas de tarjeta electrónica (DNI electrónico) o sistemas biológicos como la huella dactilar o el iris del ojo, la realidad es que requieren de elementos caros para su aplicación. En entornos educativos y en pequeñas y medianas empresas, se sigue utilizando el mecanismo tradicional de autenticación del usuario mediante su nombre de usuario (login) y su contraseña (password).

Desde que el usuario introduce su contraseña hasta que ésta llega al servidor para comprobar la autenticación, el paquete de datos que contiene la contraseña viaja por los cables de red atravesando concentradores (hubs), conmutadores (switches) y enrutadores (routers) hasta llegar al servidor. Durante el trayecto, cualquier persona con los conocimientos necesarios podría quedarse con una copia del paquete de datos para, posteriormente analizarlo y tratar de descubrir el nombre y la contraseña del usuario sin que éste se percatase.

Con la finalidad de dificultar que alguien trate de descubrir contraseñas analizando los datos que las contienen, existe la posibilidad de cifrar los paquetes de datos en el PC antes de enviarlos por la red, de manera que lleguen al servidor cifrados. De esta forma, aunque un usuario malintencionado capture un paquete de datos con la información del usuario y la contraseña, será muy difícil, por no decir imposible, que sea capaz de descifrarlos ya que se utiliza cifrado asimétrico.

El cifrado asimétrico permite la generación de una pareja de claves comunmente denominadas clave pública y clave privada en el servidor. La pareja de claves es tal que, todo lo cifrado con una, solo se puede descifrar con la otra.

El servidor tiene guardada en un lugar seguro la clave privada. Cuando un cliente intenta autenticarse, el servidor le trasfiere la clave pública para que cifre los datos con dicha clave antes de enviarlos. El cliente utiliza la clave pública del servidor para cifrar los datos, así al llegar el paquete al servidor, éste podrá descifrarlo porque dispone de la clave privada. Si un usuario malintencionado intercepta el paquete de datos cifrado con la clave pública, no podrá hacer nada porque no dispone de la clave privada. Si el usuario malintencionado intercepta el primer paquete que envía el servidor con la clave pública, no le servirá para nada ya que no le permitirá descifrar los datos emitidos por el PC que se va autenticar.



Fundamentos de la autenticación segura

LDAP seguro - ldaps

Al igual que el servidor web apache utiliza el puerto 80 para transmitir información sin encifrar (protocolo http) y el puerto 443 para transmitir información cifrada (protocolo https), openLDAP también se puede configurar para que utilice las prestaciones de cifrado que ofrece OpenSSL.

Normalmente las consultas al servidor LDAP se realizan por el puerto 389 (protocolo ldap) pero dichas consultas se transmiten sin cifrar. Para realizar consultas seguras cifrando los datos con SSL, es necesario utilizar el puerto 636 (protocolo ldaps o protocolo ldap seguro). Para ello, el servidor deberá disponer de un certificado firmado por una entidad certificadora (CA) y habrá que configurar **slapd** para que utilice los certificados. Se deberán realizar los siguientes pasos:

- 1.- Crear una nueva entidad certificadora
- 2.- Crear una petición de firma de certificado del servidor
- 3.- Firmar el certificado con la CA
- 4.- Conceder permisos de lectura a los certificados
- 5.- Configurar slapd para que utilice los certificados
- 6.- Modificar script de inicio de slapd para que utilice protocolo seguro ldaps
- 7.- Reiniciar slapd

1.- Crear una nueva entidad certificadora

Como tenemos instalado el paquete openssl,

```
# apt-get install gnutls-bin
```

```
# certtool --generate-privkey > /etc/ssl/private/ieszv-ca.key
```

Creamos el fichero **/etc/ssl/ieszv-ca.info** que contiene los detalles de la entidad certificadora, con el siguiente contenido:

```
cn = IES Zaidin Vergeles
ca
cert_signing_key
```

A continuación ejecutamos el comando:

```
# certtool --generate-self-signed --load-privkey /etc/ssl/private/ieszv-ca.key
--template /etc/ssl/ieszv-ca.info --outfile /etc/ssl/certs/ieszv-ca.cert
```

Ya tendríamos creada nuestra nueva entidad certificadora bajo la carpeta **/etc/ssl** con sus certificados correspondientes.

2.- Crear una petición de firma de certificado de servidor

El siguiente paso es crear una petición de firma de certificado del servidor para, posteriormente, firmarlo con la CA que acabamos de crear y así disponer de un certificado firmado. Nuestra petición de firma se almacenará en un nuevo archivo que se llamará **ldap.key**. Para crear la petición de firma debemos ejecutar el siguiente comando:

```
// Crear petición de firma de certificado de servidor
# certtool --generate-privkey > /etc/ssl/private/ldap.key
```

Ya tendríamos creado el archivo **ldap.key** que contiene la petición de firma de certificado de servidor.

3.- Firmar el certificado con la CA

Creamos el fichero **/etc/ssl/ldap.info** que contiene los detalles de la entidad certificadora, con el siguiente contenido:

```
organization = IES Zaidin Vergeles
cn = aula209.ieszv.es
tls_www_server
encryption_key
signing_key
```

El paso siguiente sería firmar la petición, para ello debemos ejecutar el comando:

```
// Firmar la petición de firma de certificado del servidor
# certtool --generate-certificate --load-privkey /etc/ssl/private/ldap.key
--load-ca-certificate /etc/ssl/certs/ieszv-ca.cert --load-ca-privkey
/etc/ssl/private/ieszv-ca.key --template /etc/ssl/ldap.info --outfile
/etc/ssl/certs/ldap.cert
```

Este proceso nos habrá creado el archivo **ldap.cert** que contiene el certificado firmado.

4.- Conceder permisos de lectura a los certificados

Acto seguido debemos ejecutar los comandos necesarios para permitir que el servicio de directorio pueda leer los certificados

```
# adduser openldap ssl-cert
# chgrp ssl-cert /etc/ssl/certs/ieszv-ca.cert
# chgrp ssl-cert /etc/ssl/certs/ldap.cert
# chgrp ssl-cert /etc/ssl/private/ldap.key
```

5.- Configurar slapd para que utilice los certificados

Para que el servidor LDAP utilice los certificados que acabamos de crear, es necesario generar la configuración en un archivo LDIF. El fichero se llamará **ssl.ldif** y su contenido es el siguiente:

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/ieszv-ca.cert
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/ldap.cert
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/ldap.key
```

A continuación procedemos a cargar la configuración de la siguiente forma

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f ssl.ldif -v
```

6.- Modificar script de inicio de slapd para que utilice protocolo seguro ldaps

Por defecto, el servidor LDAP se inicia con la configuración que indica el fichero 'etc/default/slapd', arranca solamente en modo normal. Para que arranque también el modo seguro, es necesario realizar una modificación en el archivo 'etc/default/slapd' que es el fichero de configuración:

```
SLAPD_SERVICES="ldap:/// ldapi:/// ldaps:///"
```

Aquí podríamos poner únicamente SLAPD_SERVICES="ldaps:///" con lo cual solamente se iniciaría en modo seguro. Ello requerirá que todos los servicios que utilicen LDAP consulten al servidor obligatoriamente en modo seguro. Si deseamos que el login del sistema sea seguro, habría que modificar la configuración de las librerías pam_ldap y libnss-ldap para que utilicen ssl.

7.- Reiniciar servidor LDAP

Para que los cambios que hemos realizado tengan efecto, debemos reiniciar el servidor LDAP. Para ello, debemos ejecutar el siguiente comando:

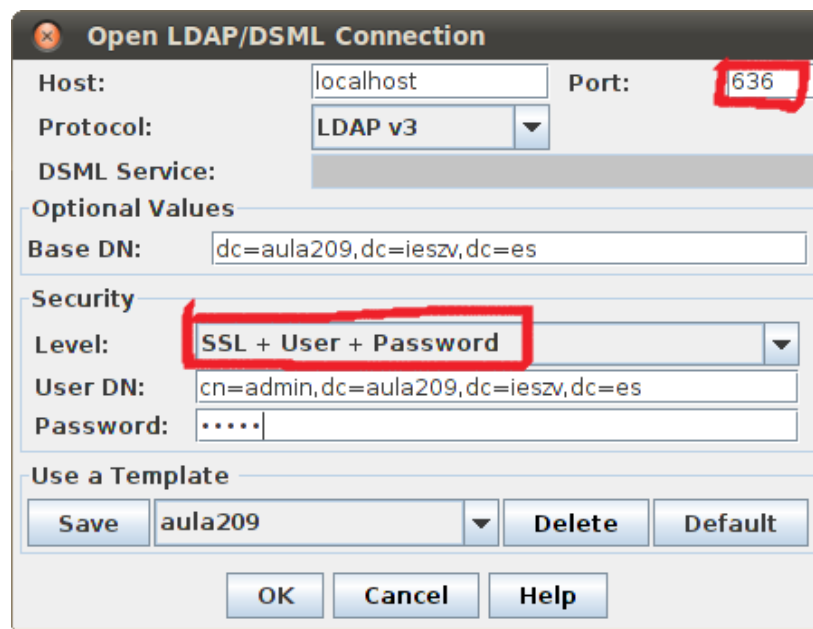
```
// Reiniciar slapd
# /etc/init.d/slapd restart
```

Probando el acceso por SSL

El acceso por SSL se puede probar desde consola con el siguiente comando:

```
ldapsearch -d 9 -D "cn=admin,dc=aula209,dc=ieszv,dc=es" -b
"dc=aula209,dc=ieszv,dc=es" -H "ldaps://localhost" "objectClass=*" -W
```

Si nuestro servidor LDAP está funcionando en modo seguro, estará escuchando en el puerto 636 ya que es el puerto utilizado por el protocolo ldaps. Para probarlo, iniciamos JXplorer pero la conexión la realizamos a dicho puerto y el nivel de seguridad seleccionamos SSL + User + Password ya que la autenticación va a ser por usuario y contraseña pero utilizando SSL:



Al intentar conectar, nos aparecerá la información del certificado. Podremos aceptar el certificado para esta sesión (This session only) o para siempre (Always):

Una vez que hemos conectado, podemos apreciar en la parte inferior que la conexión se ha realizado al puerto 636:

JXplorer

File Edit View Bookmark Search LDIF Options Tools Security Help

cn Quick Search

Results Schema HTML View Table Editor

organization/Main.html

World

- es
 - ies...
 - aula209
 - admin
 - proxyuser

organization

Main Address Other

Organization:

Description:

User Password:

Telephone Number:

Facsimile Number:

Locality Name:

Submit Reset

LDAPS

Connected To 'ldap://localhost:636'