



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



SERVICIO DE
FORMACIÓN DEL
PROFESORADO

C/ TORRELAGUNA, 58
28027 - MADRID

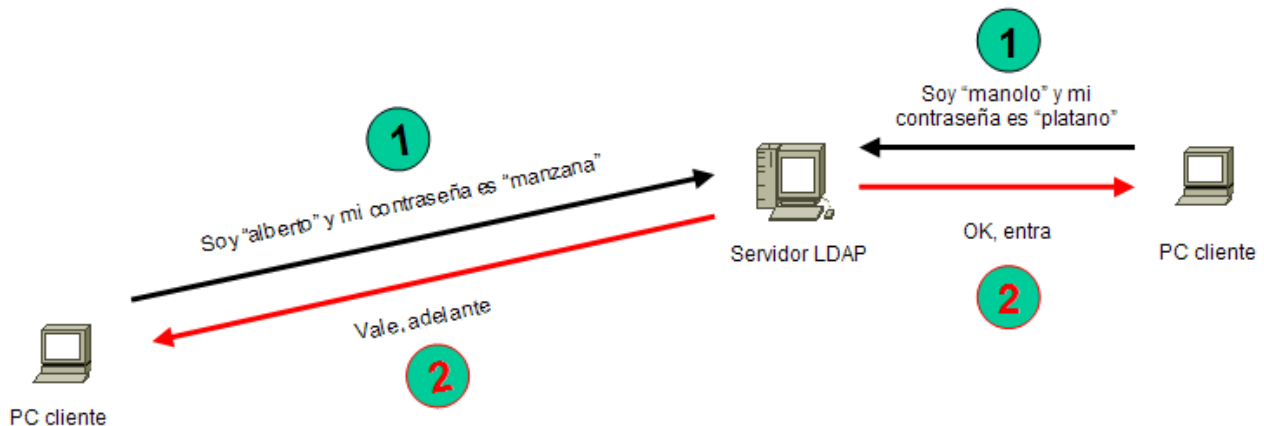
Índice de contenido

¿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	9
Arranque automático del servidor LDAP al iniciar el sistema	9
Administración de OpenLDAP	10
Introducción	10
Explorador de directorios LDAP	10
JXplorer - Explorador LDAP en java	11
Instalación de JXplorer	11
Conexión con el servidor LDAP	12
Organización del directorio LDAP	14
Creación de las unidades organizativas	14
Usuarios y grupos	16
Creación de grupos	16
Creación de usuarios	17
Autenticación basada en LDAP	19
Introducción	19
Librerías de autenticación pam-ldap y nss-ldap	19
Instalación y configuración de libpam-ldap	19
Instalación y configuración de libnss-ldap	20
Configuración de NSS	24
Configurar servicios PAM	25
Configuración archivo common-auth	26
Configuración archivo common-account	26
Configuración archivo common-session	26
Configuración archivo common-password	26
Configuración particular para cada servicio	26
Probar la autenticación	26
Autenticación segura con OpenLDAP	27
Justificación	27
LDAP seguro - ldaps	28
1.- Crear una nueva entidad certificadora	29
2.- Crear una petición de firma de certificado de servidor	30
3.- Firmar el certificado con la CA	31
4.- Copiar los certificados a la carpeta deseada, renombrar y proteger	35
5.- Configurar slapd para que utilice los certificados	36
6.- Modificar script de inicio de slapd para que utilice protocolo seguro ldaps	36
7.- Reiniciar servidor LDAP	36
Probando el acceso por ssl	36

¿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 **db4.2-util** que son un conjunto de utilidades para la base de datos dbd que es la que utilizaremos para nuestro servidor ldap y el paquete **ldap-utils** que contiene utilidades adicionales:

```
// Instalación del servidor LDAP
# apt-get install slapd db4.2-util ldap-utils
```

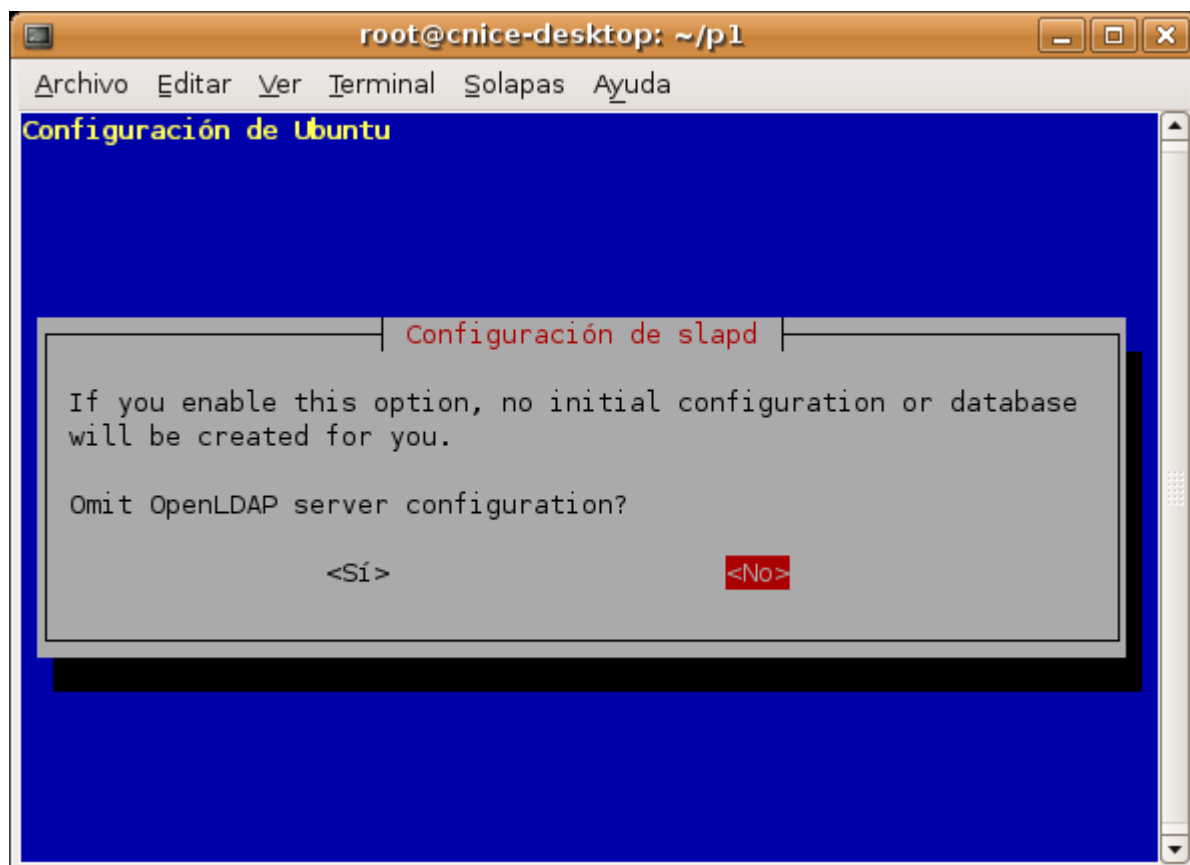
Durante la instalación, nos pedirá que introduzcamos la contraseña de administrador del servidor ldap. Podemos configurar cualquier contraseña, como por ejemplo 'ldadmin'

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
```

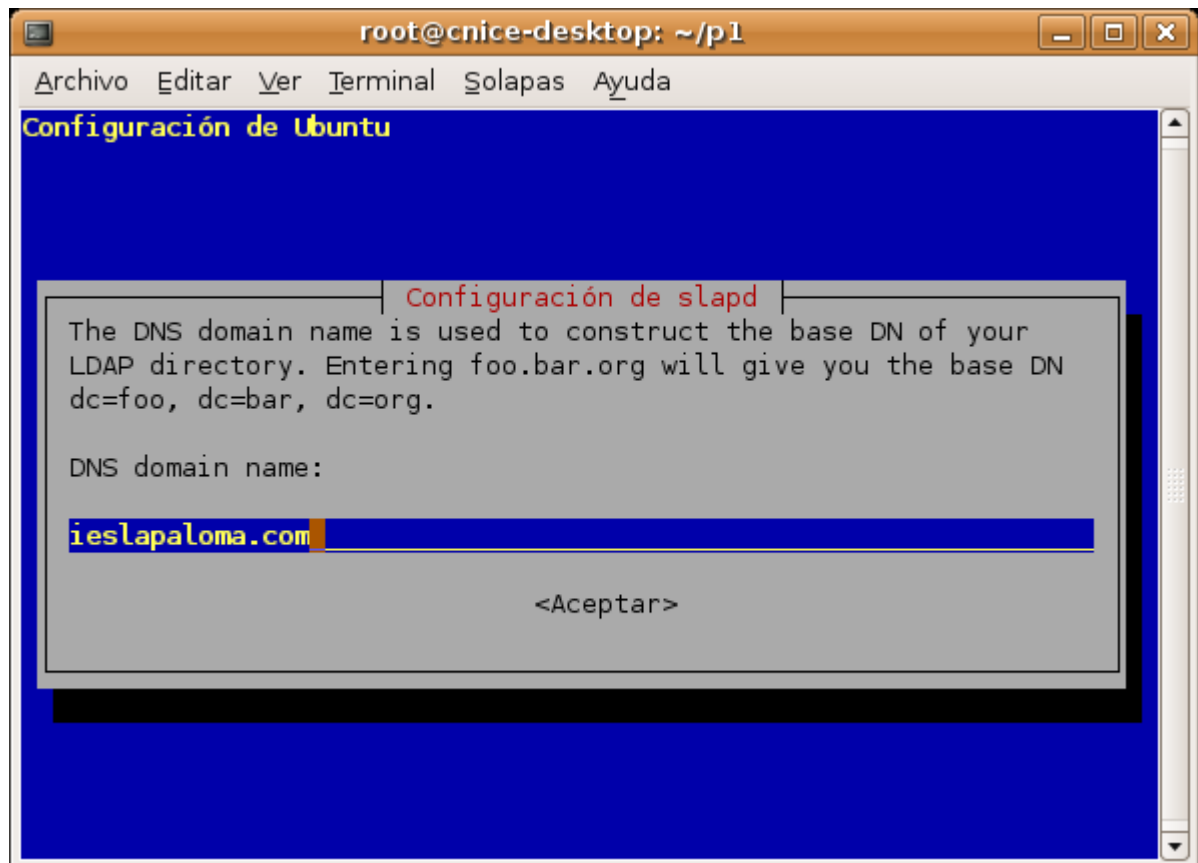
Lo primero que nos pregunta el asistente es si deseamos omitir la configuración del servidor LDAP:



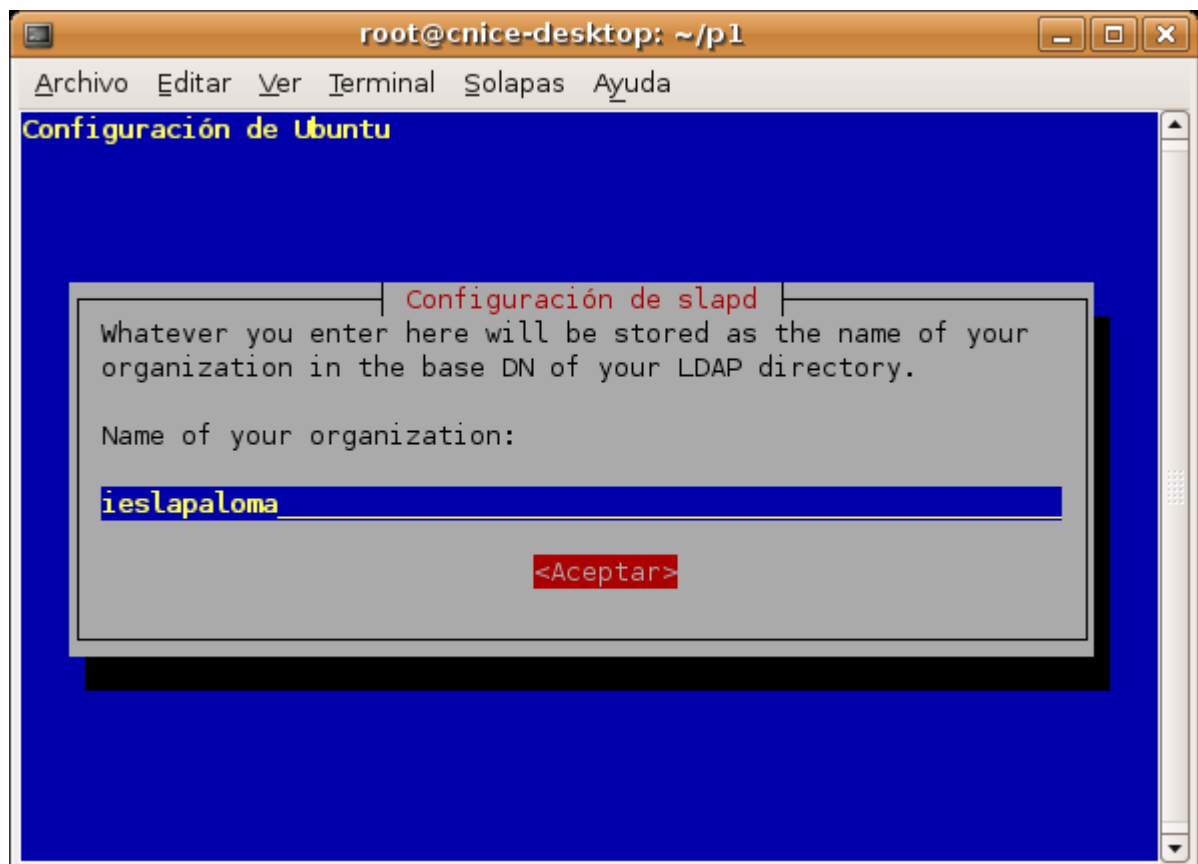
Obviamente responderemos que no, ya que precisamente lo que queremos es configurar el servidor LDAP.

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 `ieslapaloma.com`, lo normal es que la base para nuestro directorio LDAP sea: `dc=ieslapaloma,dc=com`.

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.

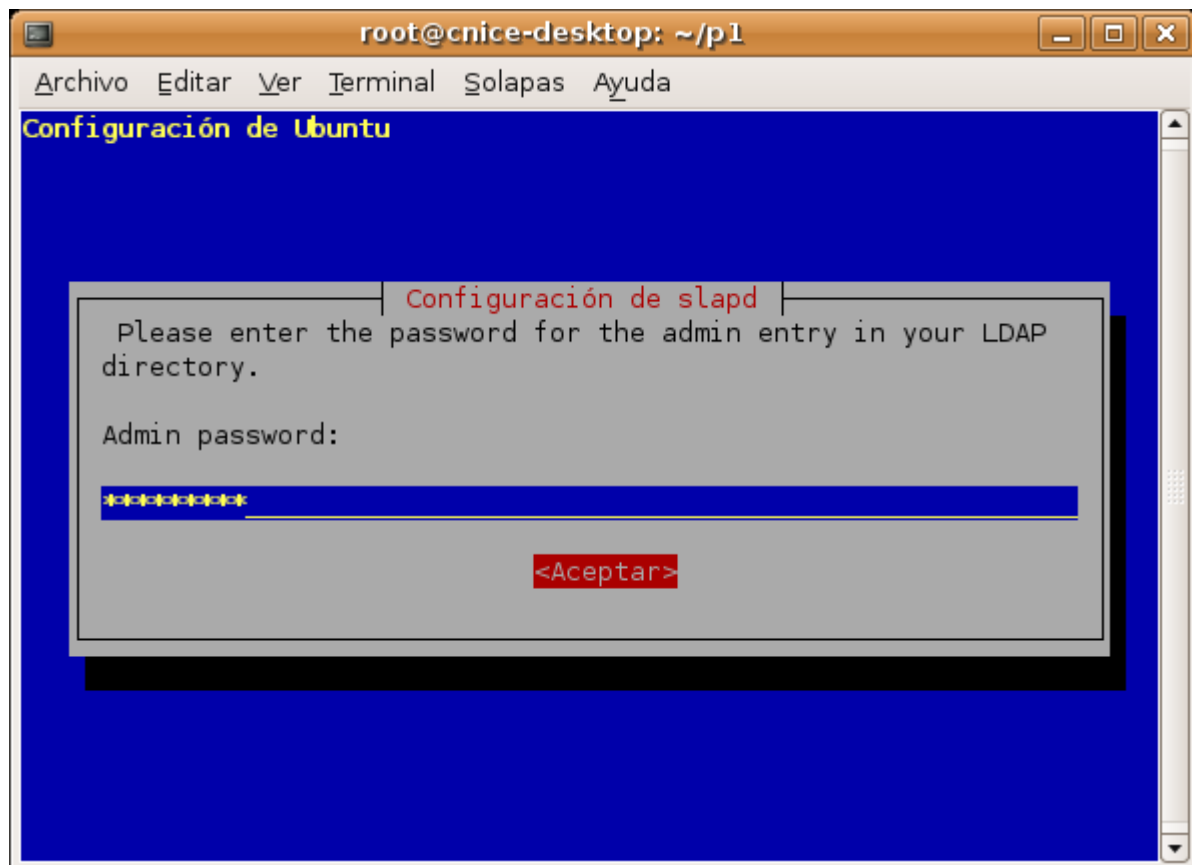


Posteriormente nos preguntará por el nombre de nuestra organización.

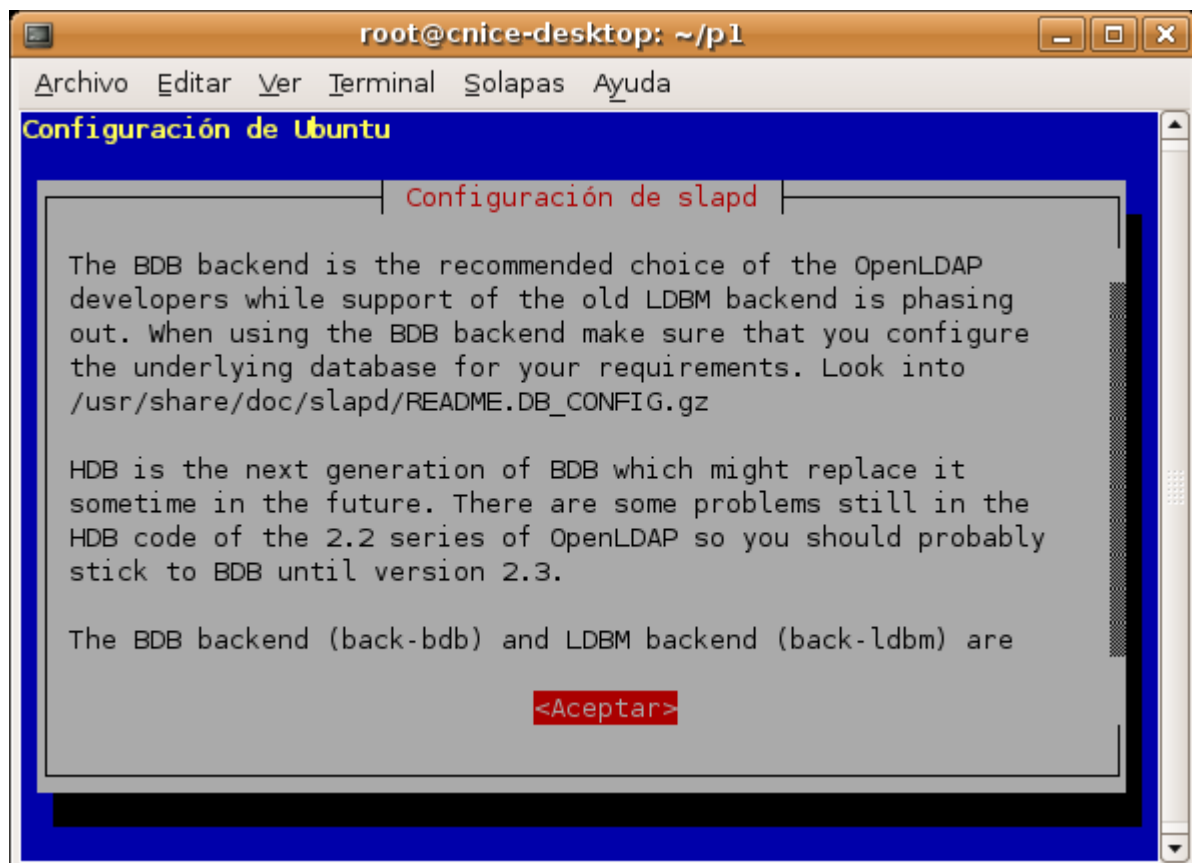


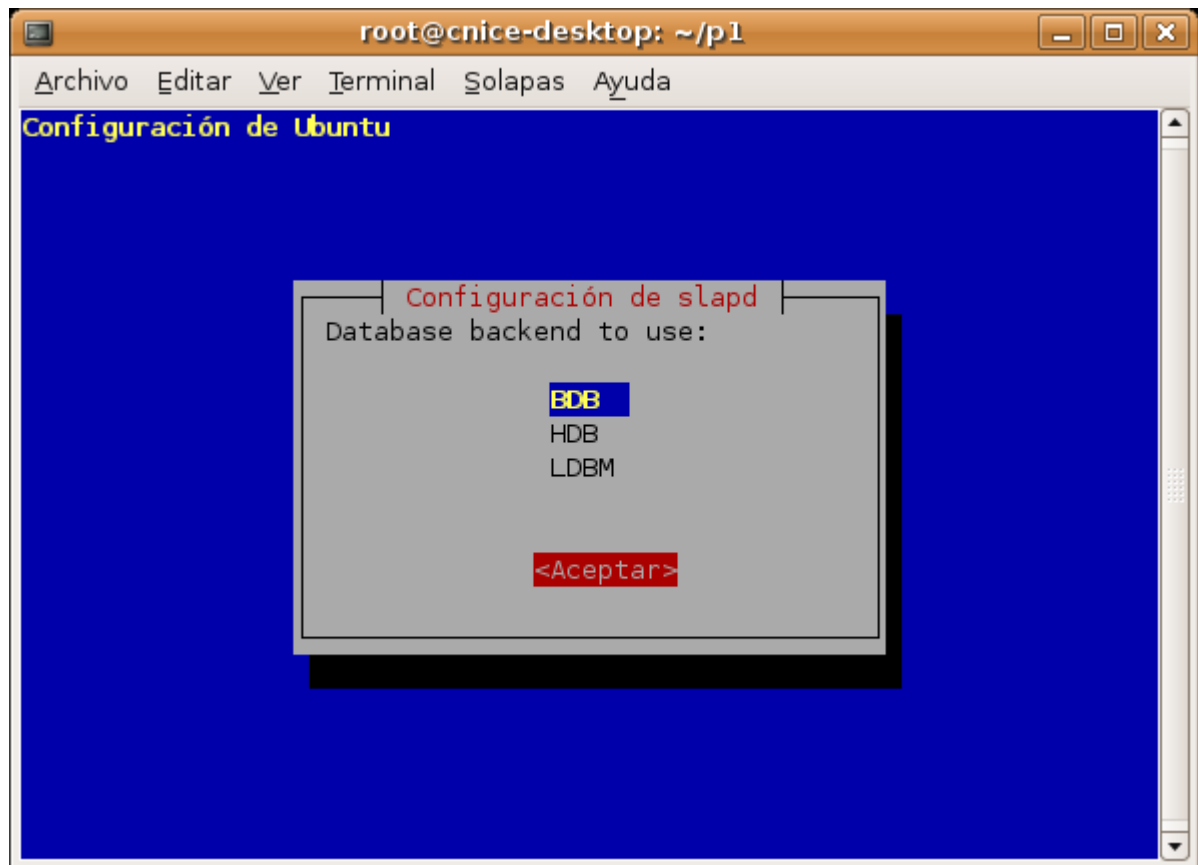
Después nos preguntará por la contraseña que deseamos poner al usuario admin (administrador) del servidor LDAP. Dicha contraseña nos la pedirá dos veces para evitar errores de tecleo. Podemos poner

cualquier contraseña, por ejemplo 'ldapadmin'.

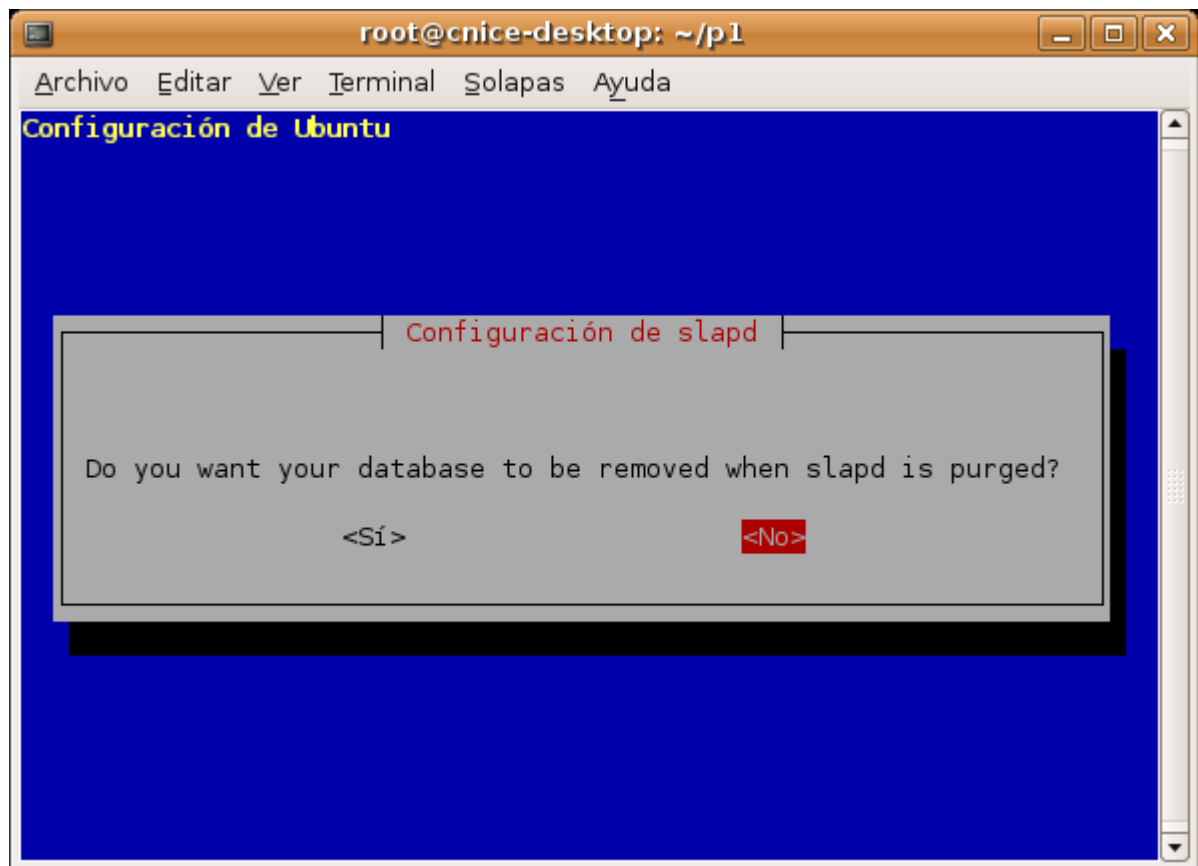


Acto seguido nos informará sobre los posibles gestores de datos para almacenar el directorio y en la siguiente ventana nos preguntará qué sistema utilizar. Lo recomendable es utilizar el sistema BDB.



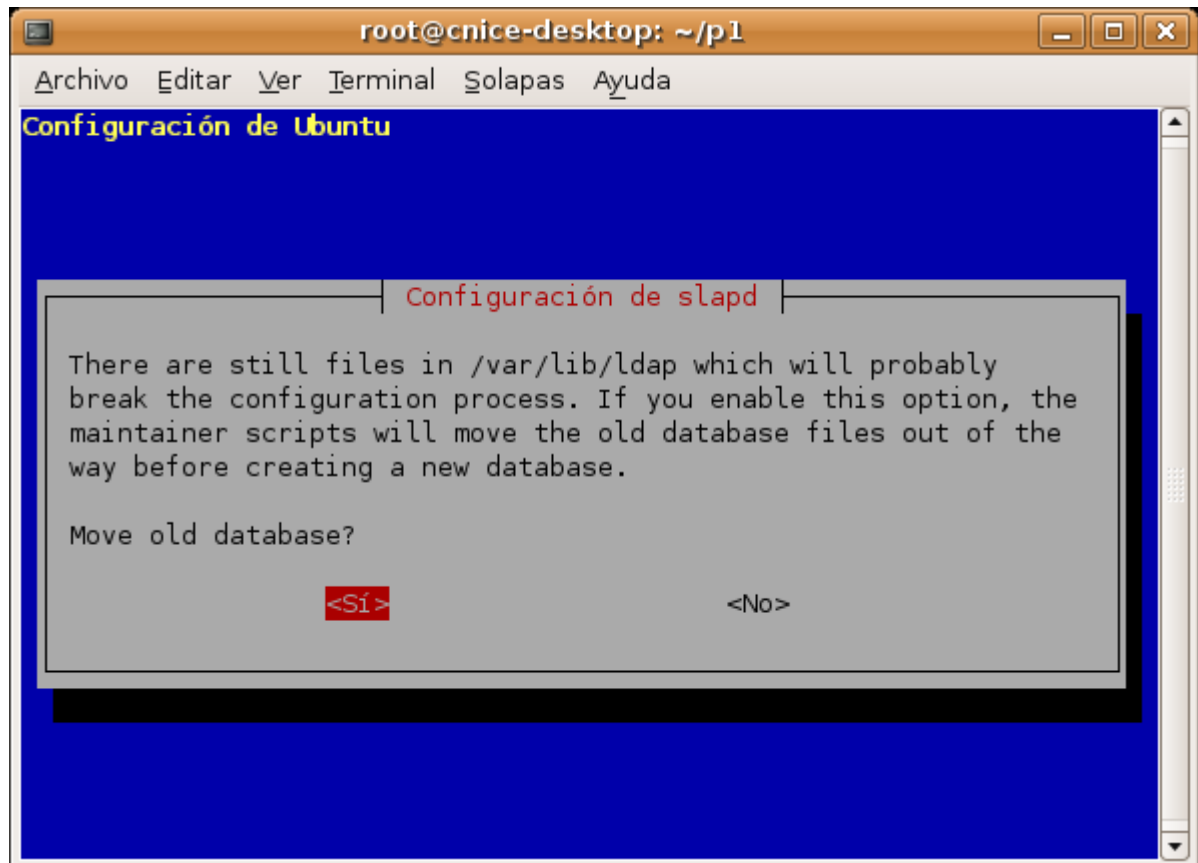


Después nos preguntará si queremos que se elimine la base de datos cuando quitemos slapd. Por si acaso, lo mejor es responder que no:

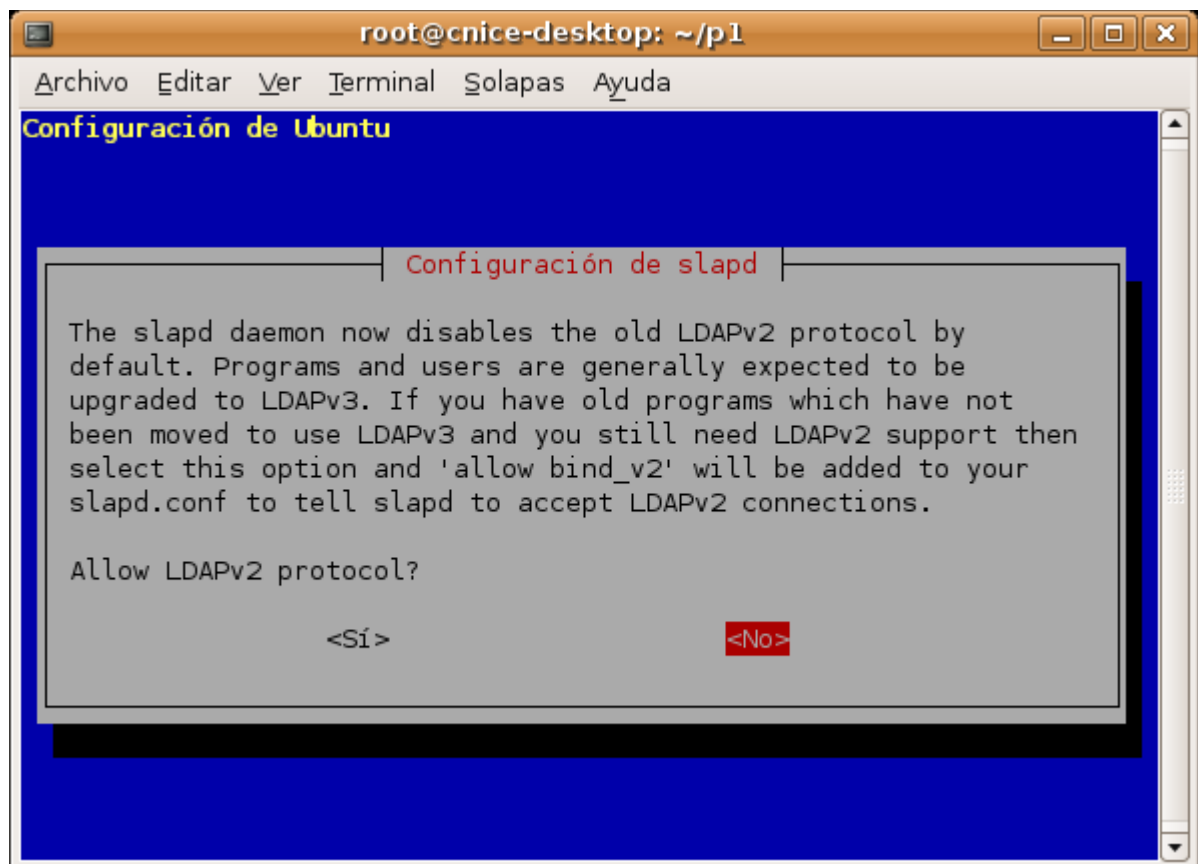


En el caso de que exista una base de datos LDAP previa, nos preguntará si deseamos moverla. Lo mejor es

responder Sí, para evitar que interfiera en la nueva base de datos:

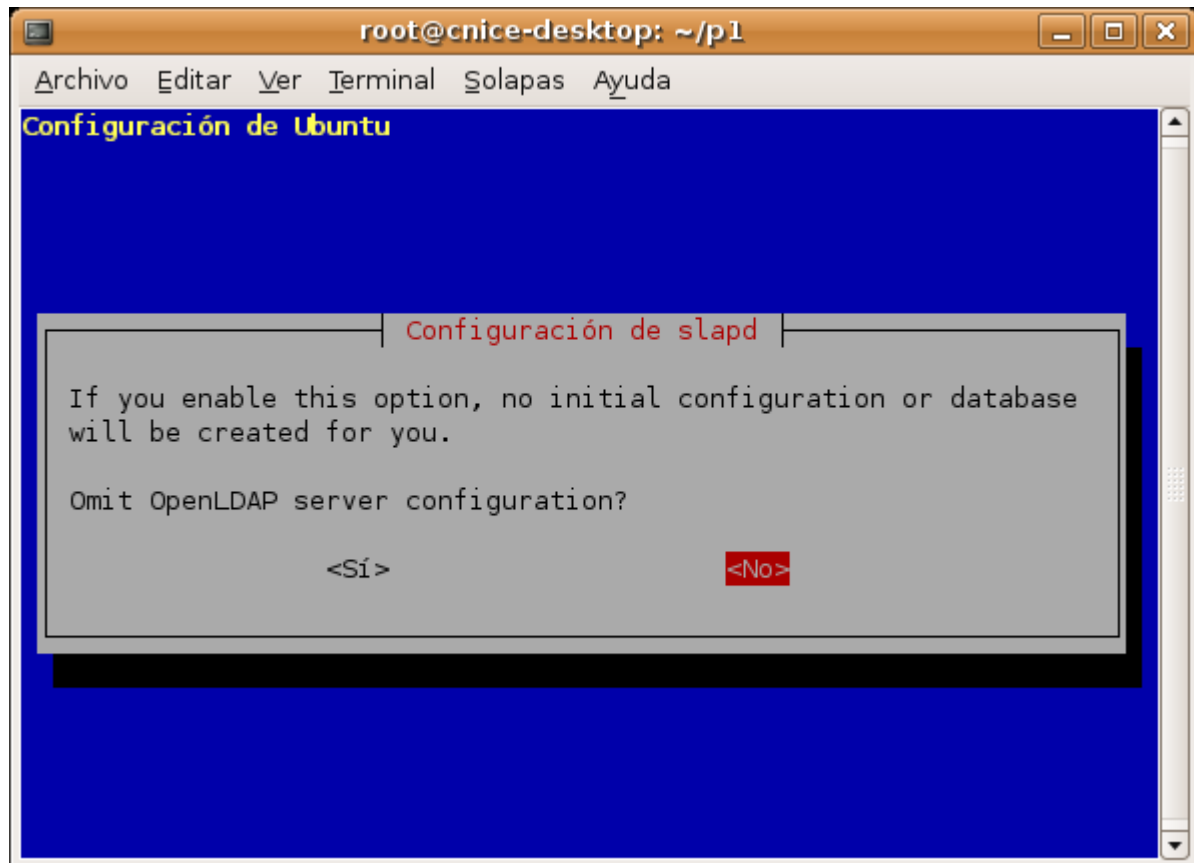


Luego nos preguntará si deseamos utilizar LDAP versión 2, respondemos que no ya que apenas se utiliza.



Finalmente nos da la oportunidad de omitir la configuración. Si respondemos que sí, será como que no

hemos ejecutado el asistente, por lo tanto si nuestra intención es configurar el servidor LDAP responderemos no:



Ya tendríamos nuestro servidor LDAP listo para trabajar con él.

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.

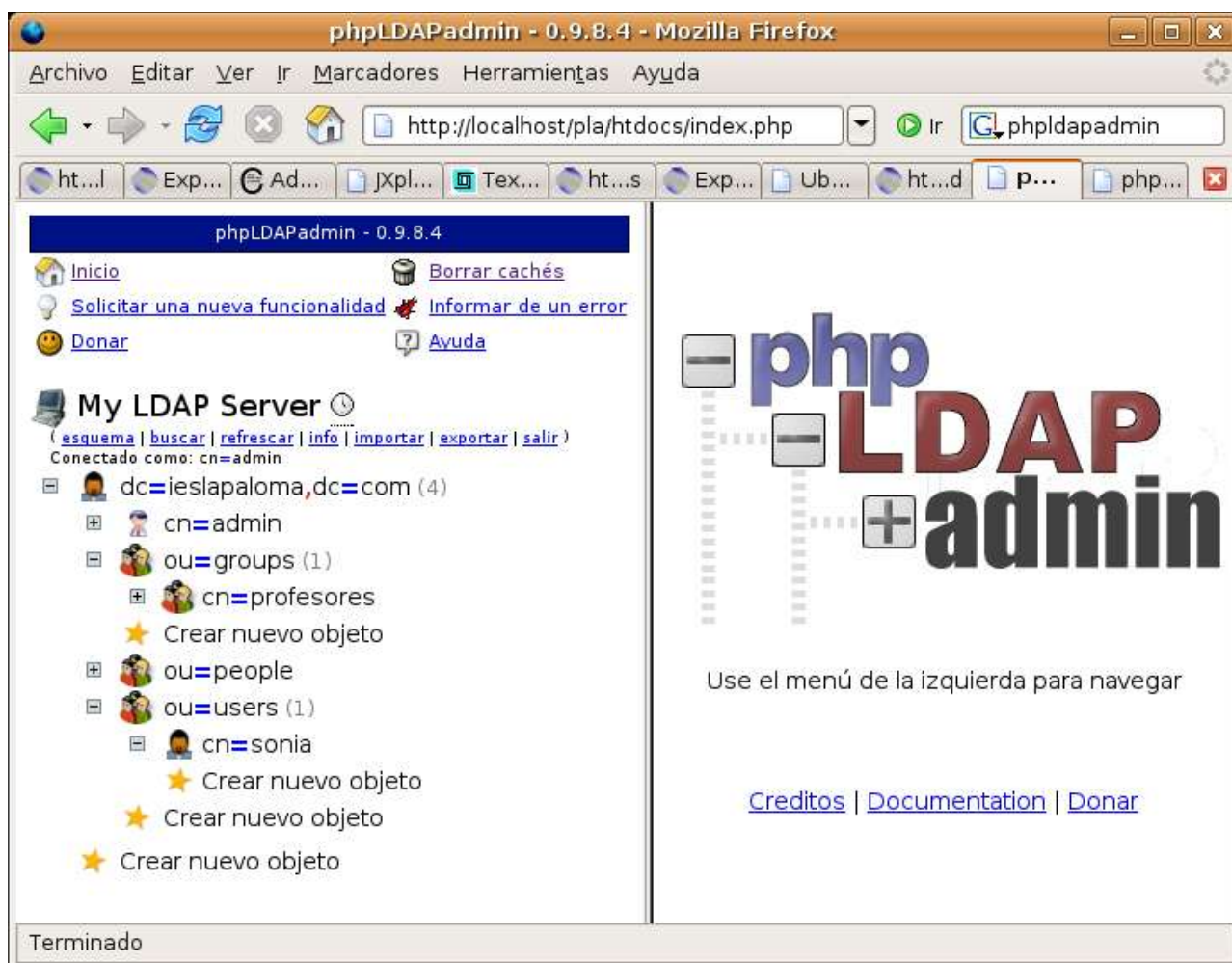
Puesto que la finalidad de nuestro servidor LDAP es que sirva de almacén de usuarios y grupos para autenticar sistemas linux y servicios como ftp y web, deberemos crear una estructura que parta de la base de nuestro directorio, para almacenar dicha información. Tal y como se explica más abajo, crearemos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

Explorador de directorios LDAP

Para acceder al directorio LDAP y poder crear y modificar elementos en dicho directorio, es necesario disponer de un explorador de directorios LDAP (LDAP browser). Existen muchos exploradores LDAP tanto de pago como libres. Entre las aplicaciones libres destacamos gq, phpldapadmin (aplicación web) y JXplorer.

Para instalar gq, podemos utilizar apt-get. Una vez instalada, para ejecutar gq tan solo debemos pulsar alt+f2 y escribir gq.

Para instalar phpldapadmin, al igual que otras aplicaciones web, deberemos descargarla desde <http://phpldapadmin.sourceforge.net/> y descomprimirla dentro del DocumentRoot de apache, es decir, dentro de la carpeta /var/www, por ejemplo en /var/www/phpldapadmin. Para ejecutarla, si la hemos descomprimido en la carpeta anterior, debemos ir a http://ip_del_servidor_web/phpldapadmin/ con el navegador y veremos la página principal de la aplicación:



JXplorer - Explorador LDAP en java.

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

Instalación de JXplorer

Previo a instalar jxplorer, es necesario instalar la máquina virtual java de Sun. Para ello debemos ir a <http://www.java.com/es/> y descargar la última versión del JRE (Java Runtime Environment). Puesto que no existe una versión específica para sistemas debian, debemos descargar la versión Linux (genérica), ejecutar el archivo 'bin' para que se descomprima el paquete y mover el directorio que se ha creado (ejemplo, jre1.6.0_02), a la carpeta /usr/lib. Posteriormente tendremos que editar el archivo /root/.bashrc y añadir las variables que permitan al shell encontrar el JRE:

```
// Añadir en /root/.bashrc (sustituir jre1.6.0_02 por la versión descargada)
# CLASSPATH=/usr/lib/jre1.6.0_02/bin/

JAVA_HOME=/usr/lib/jre1.6.0_02/bin/

PATH=/usr/lib/jre1.6.0_02/bin:/usr/lib/jre1.6.0_02/bin/java:/sbin:/bin
: /usr/sbin:/usr/bin:/usr/bin/X11:/usr/local/sbin:/usr/local/bin
```

Después, debemos abrir un terminal y ya estamos en condiciones de instalar JXplorer. JXplorer no está disponible en los repositorios de paquetes de debian, por ello debemos ir a <http://pegacat.com/jxplorer/downloads/users.html> y descargarnos la versión para linux. En el momento de escribir estas líneas, la última versión es la 3.1 y por tanto el archivo descargado se llama JXv3.1_install_linux.bin. Para instalar la aplicación debemos dar permisos de ejecución al archivo y ejecutar:

```
// Instalar JXplorer
# sh ./JXv3.1_install_linux.bin
```

Se iniciará un sencillo asistente de instalación que al finalizar habrá creado un enlace en nuestra carpeta home, por lo tanto para ejecutarlo debemos escribir:

```
// Ejecutar JXplorer
# ./JXplorer_LDAP_Browser
```

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:

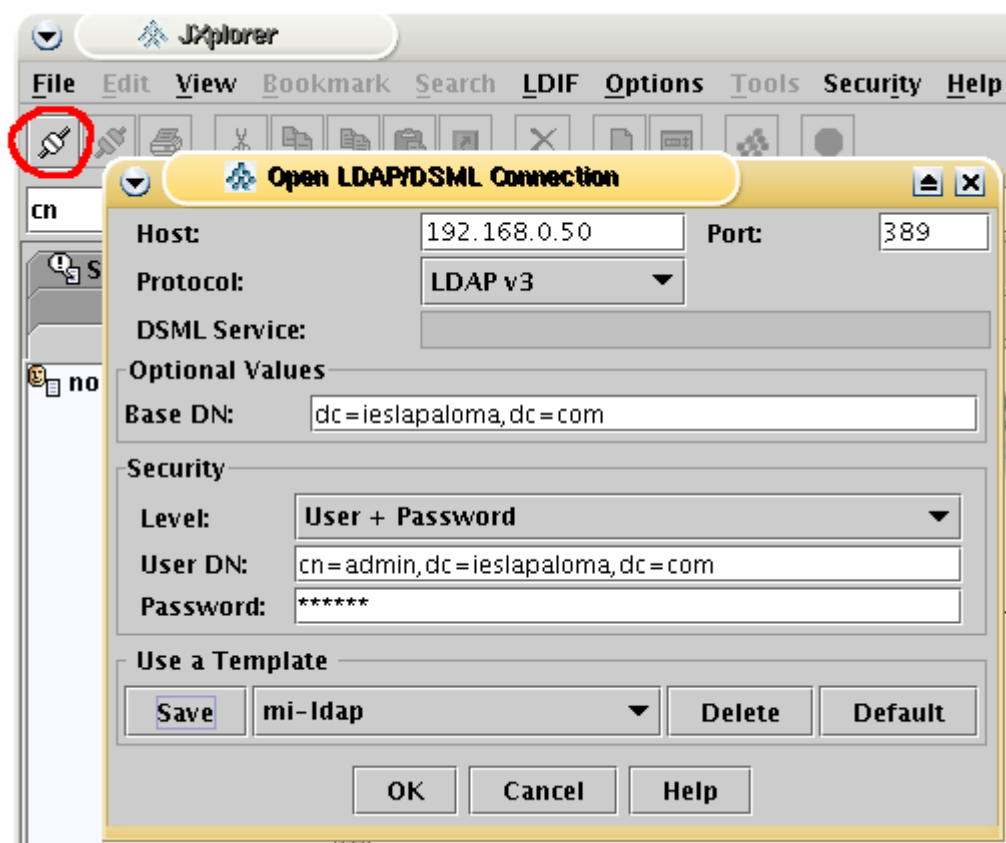
- Dirección IP del servidor LDAP
- Protocolo del servidor (LDAP v3 en nuestro caso)
- Base del directorio (dc=ieslapaloma,dc=com en nuestro caso)
- Nombre de usuario administrador (cn=admin,dc=ieslapaloma,dc=com en nuestro caso)
- Contraseña (ldadmin en nuestro caso)

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.

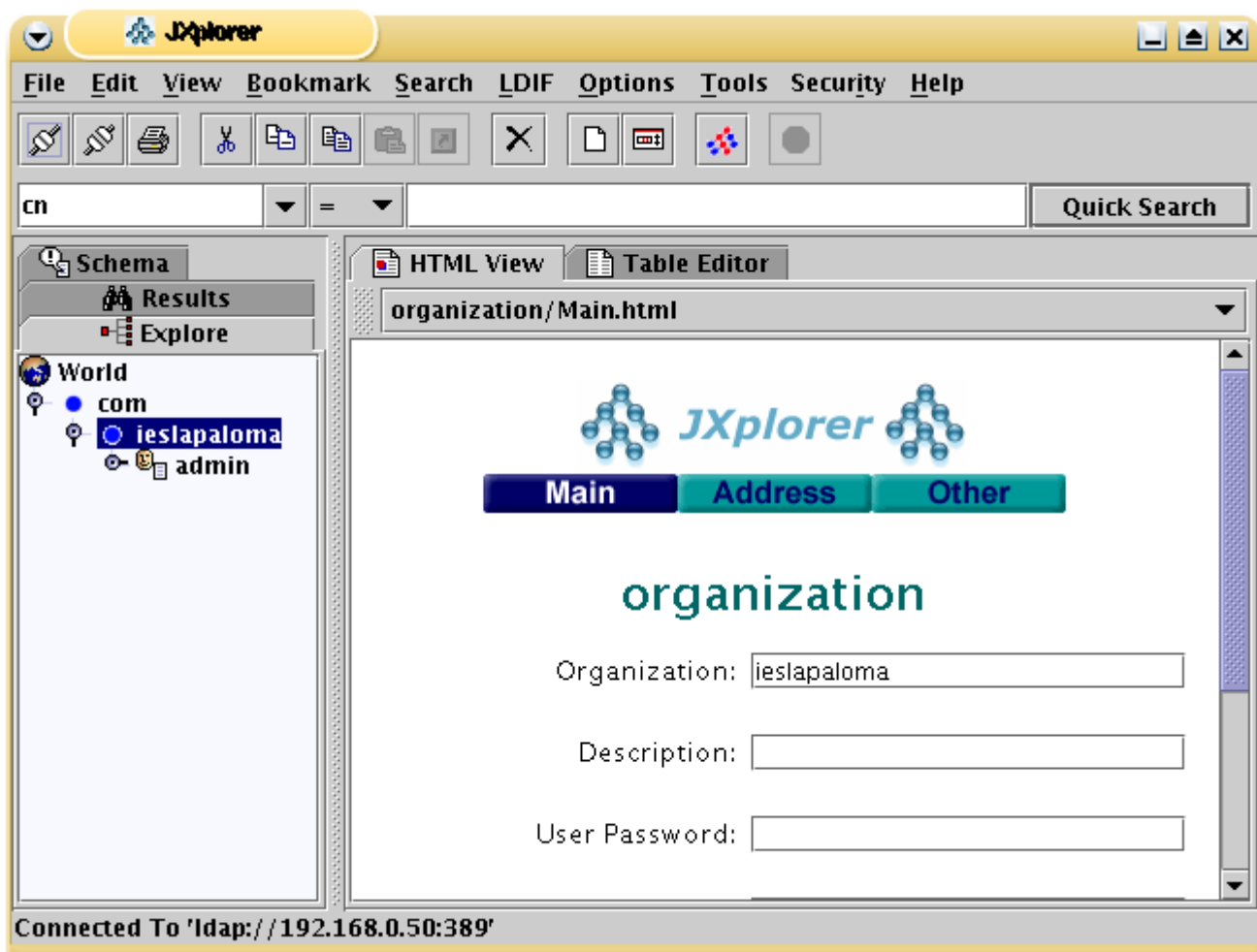
El nombre del usuario con el que nos conectamos se suele denominar en inglés 'user DN' o también 'bind DN'.

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

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 solamente hay dos elementos: una organización llamada 'ieslapaloma' y el usuario administrador llamado 'admin'.

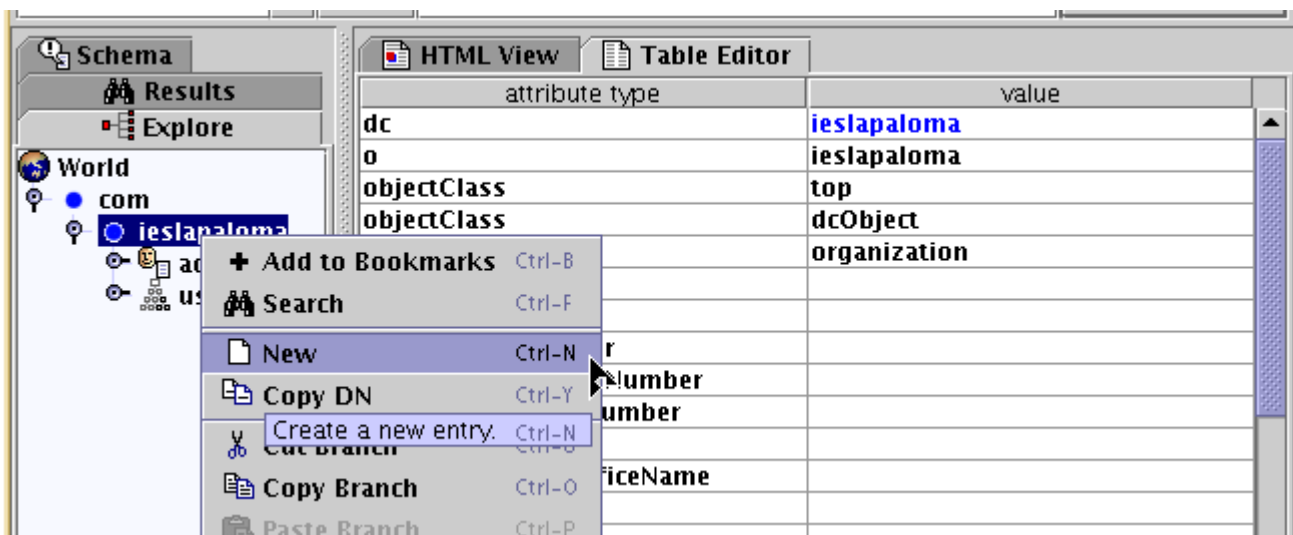
Organización del directorio LDAP

Creación de las unidades organizativas

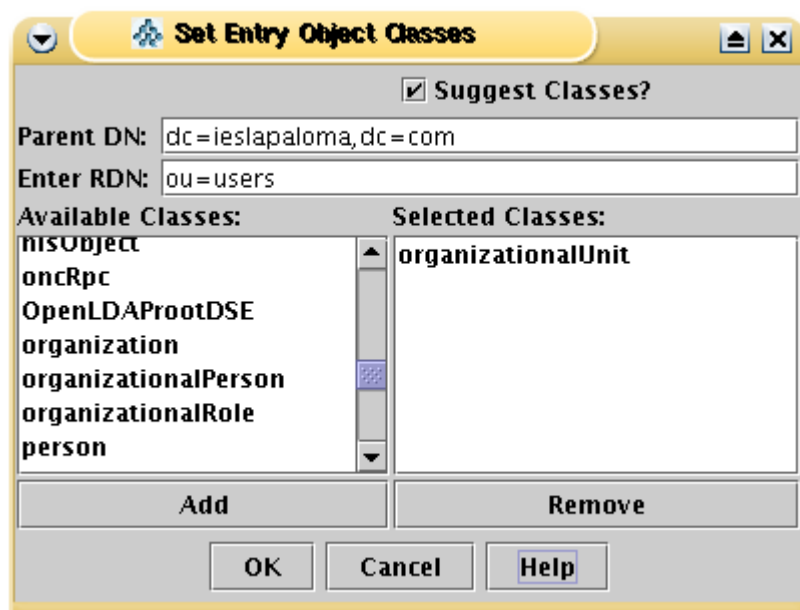
Puesto que nuestro directorio va a almacenar usuarios y grupos, vamos a crear sendas unidades organizativas (en inglés organizational unit - ou) llamadas 'users' y 'groups' que nos servirán para organizar los usuarios y los grupos por separado.

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 'ieslapaloma' 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 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:

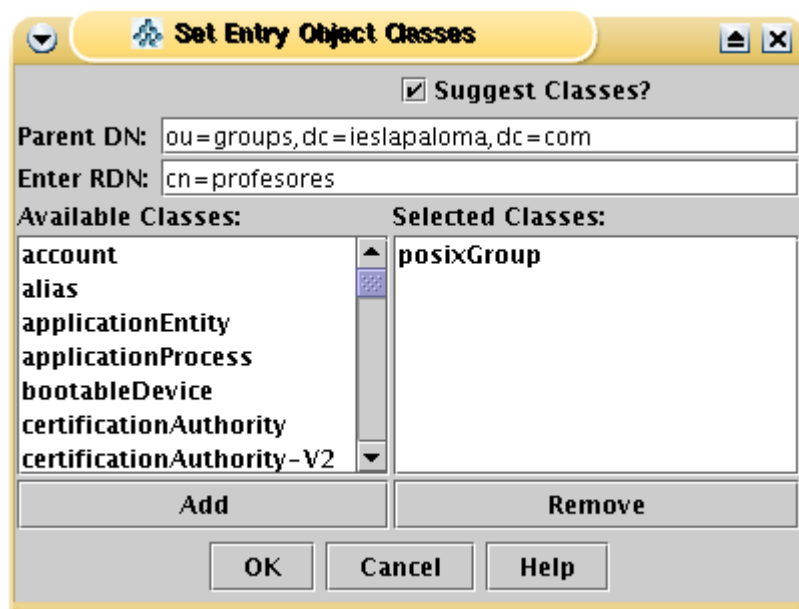
- profesores (gid=1001)
- alumnos (gid=1002)

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

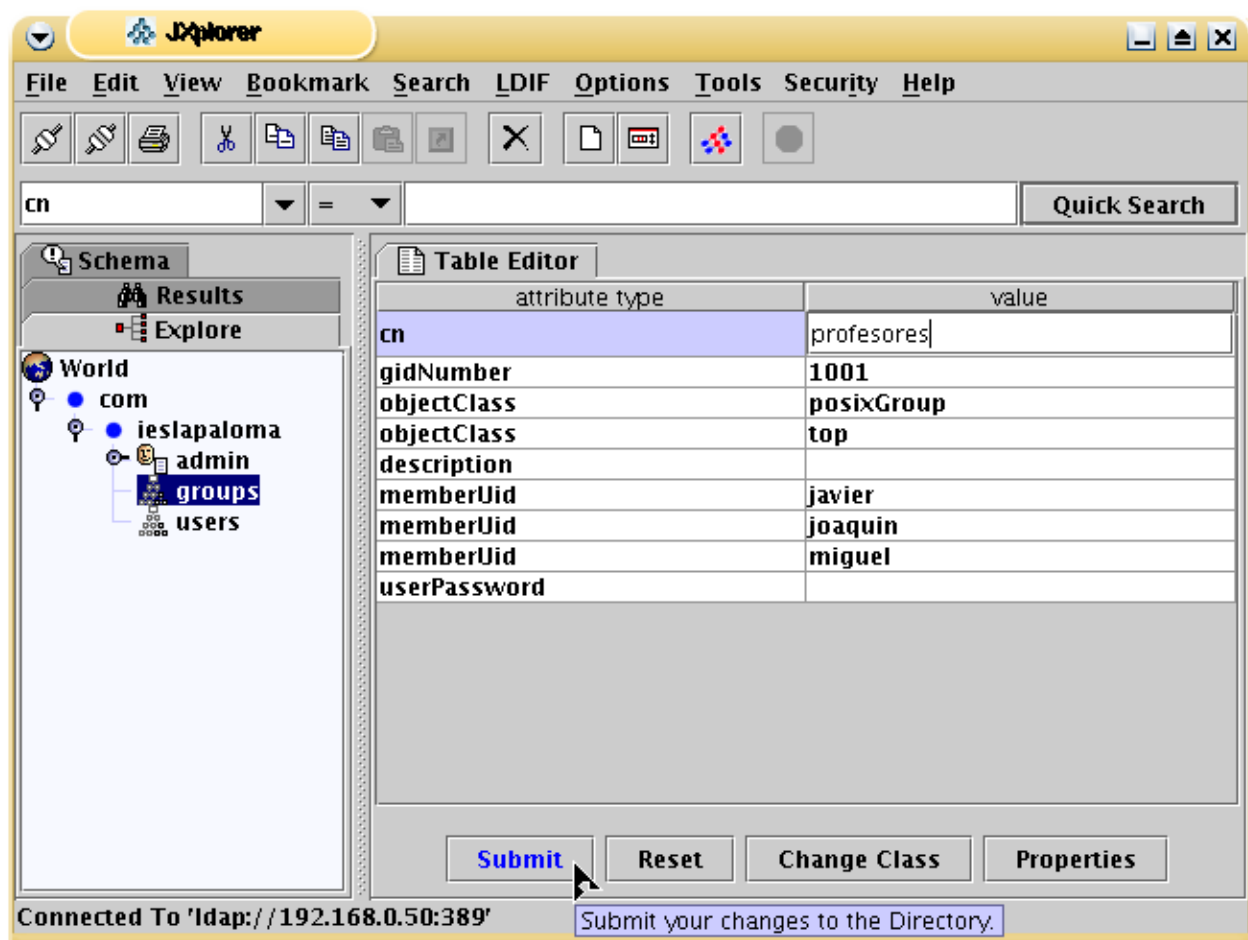
- javier (uid=1001, profesor)
- joaquin (uid=1002, profesor)
- miguel (uid=1003, profesor)
- jessica (uid=1004, alumno)
- joel (uid=1005, alumno)

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):

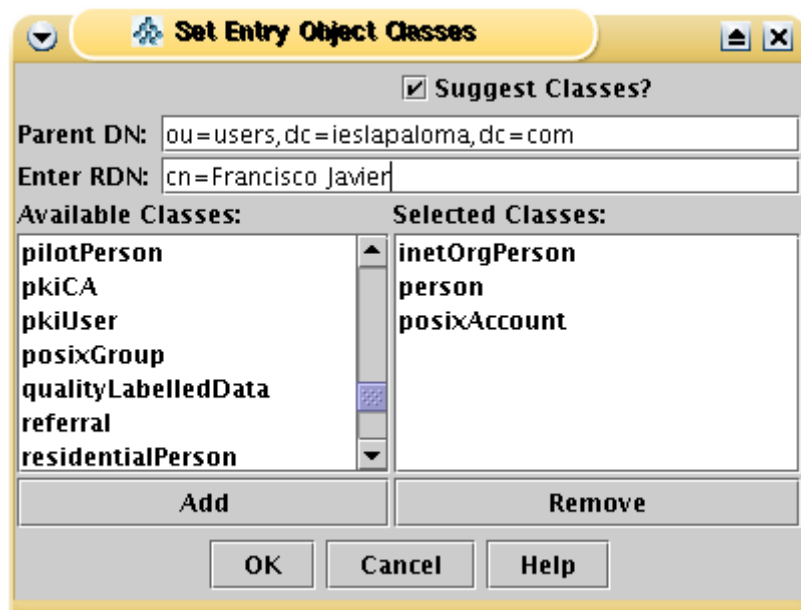


Al pulsar OK nos aparecerá la siguiente figura, en la cual observamos los atributos clásicos de un grupo posix. Debemos rellenar al menos el campo gidNumber. También podemos introducir miembros al grupo. En el parámetro memberUid añadimos javier. Luego, haciendo clic con el derecho en javier > Add another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

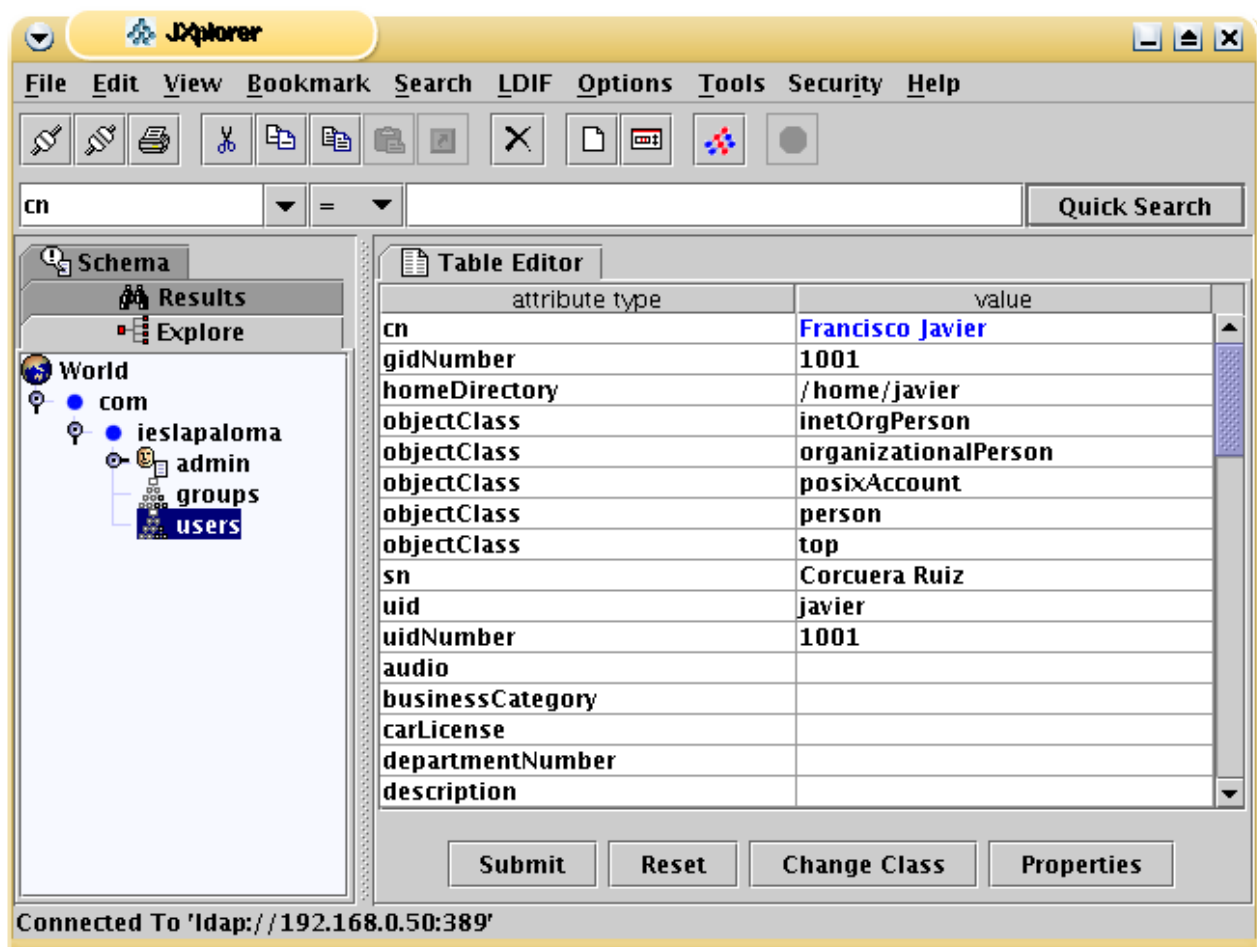


Creación de usuarios

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**.

Instalación y configuración de libpam-ldap

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

```
// Instalación de la librería libpam-ldap
# apt-get install libpam-ldap
```

El archivo de configuración de la librería es el archivo **/etc/pam_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/pam_ldap.conf
host 192.168.1.239 //nombre o IP del servidor LDAP

base dc=ieslapaloma,dc=com

ldap_version 3

rootbinddn cn=admin,dc=ieslapaloma,dc=com

nss_base_passwd ou=users,dc=ieslapaloma,dc=com?one

nss_base_shadow ou=users,dc=ieslapaloma,dc=com?one

nss_base_group ou=groups,dc=ieslapaloma,dc=com?one
```

Instalación y configuración de libnss-ldap

Para instalar la librería libnss-ldap debemos ejecutar el comando:

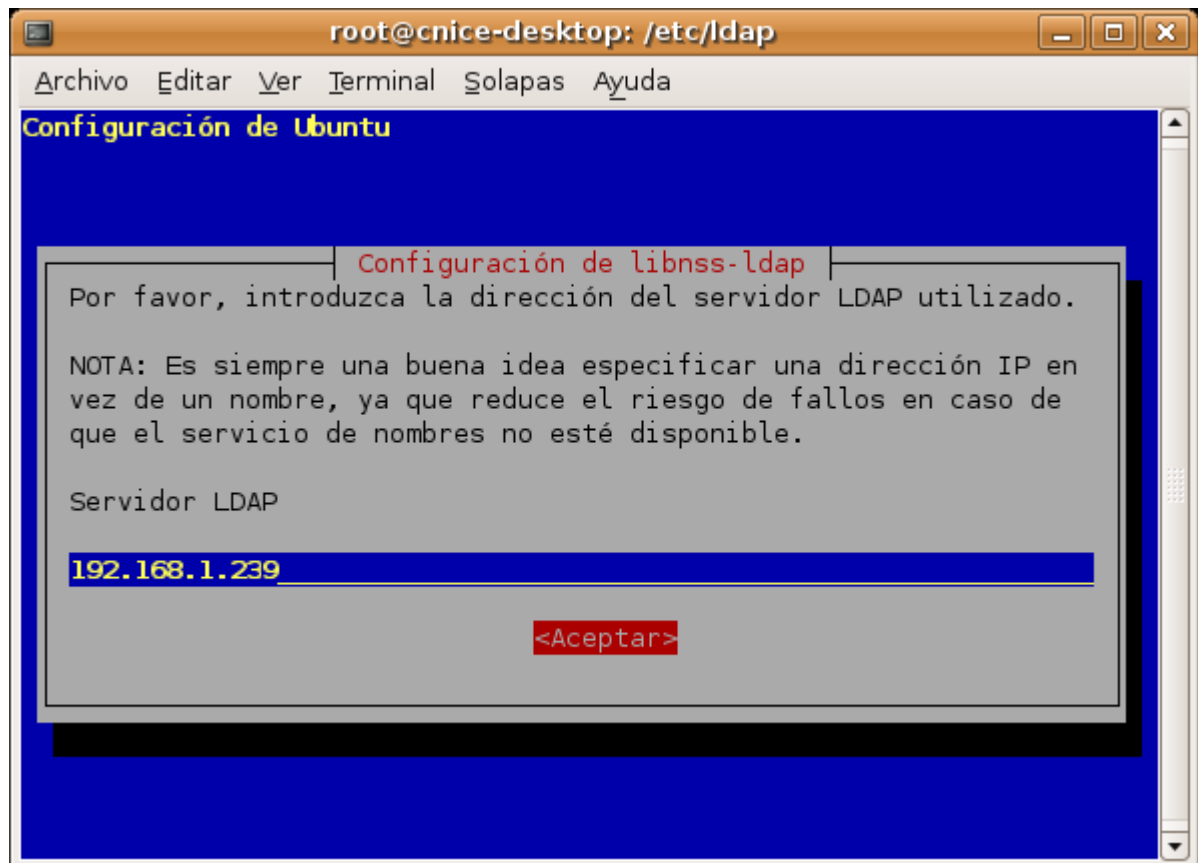
```
// Instalación de la librería libnss-ldap
# apt-get install libnss-ldap
```

Acto seguido se iniciará el asistente de configuración de dicha librería. Se puede lanzar dicho asistente más adelante mediante el comando:

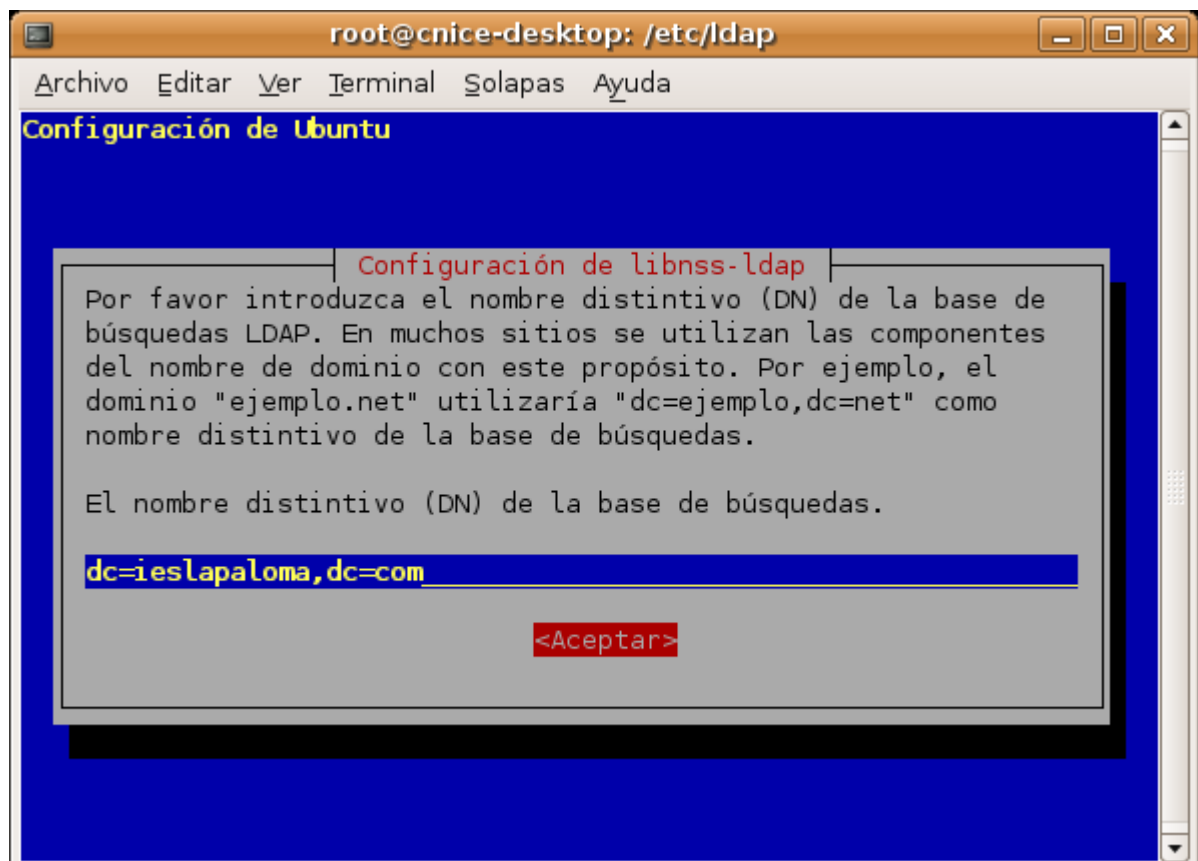
```
// Lanzar asistente de configuración de libnss-ldap
# dpkg-reconfigure libnss-ldap
```

Dicho asistente modificará el archivo **/etc/libnss-ldap.conf** que es donde se almacena la configuración de la librería. Posteriormente tendremos que editar dicho archivo manualmente para introducir algún cambio que no realiza el asistente.

La primera pregunta que nos hace el asistente es quién es el servidor LDAP. Podemos poner la IP o el nombre:



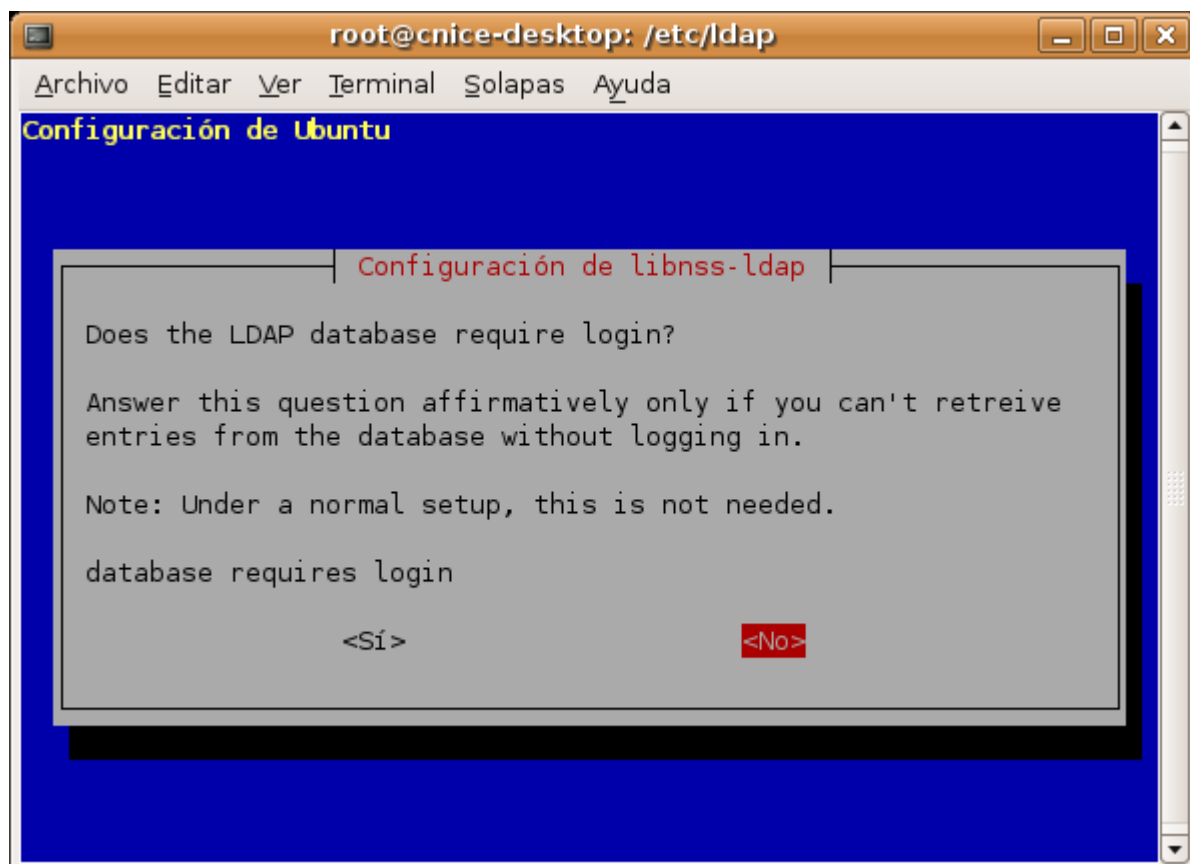
Luego nos preguntará por la base del directorio LDAP (base DN):



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

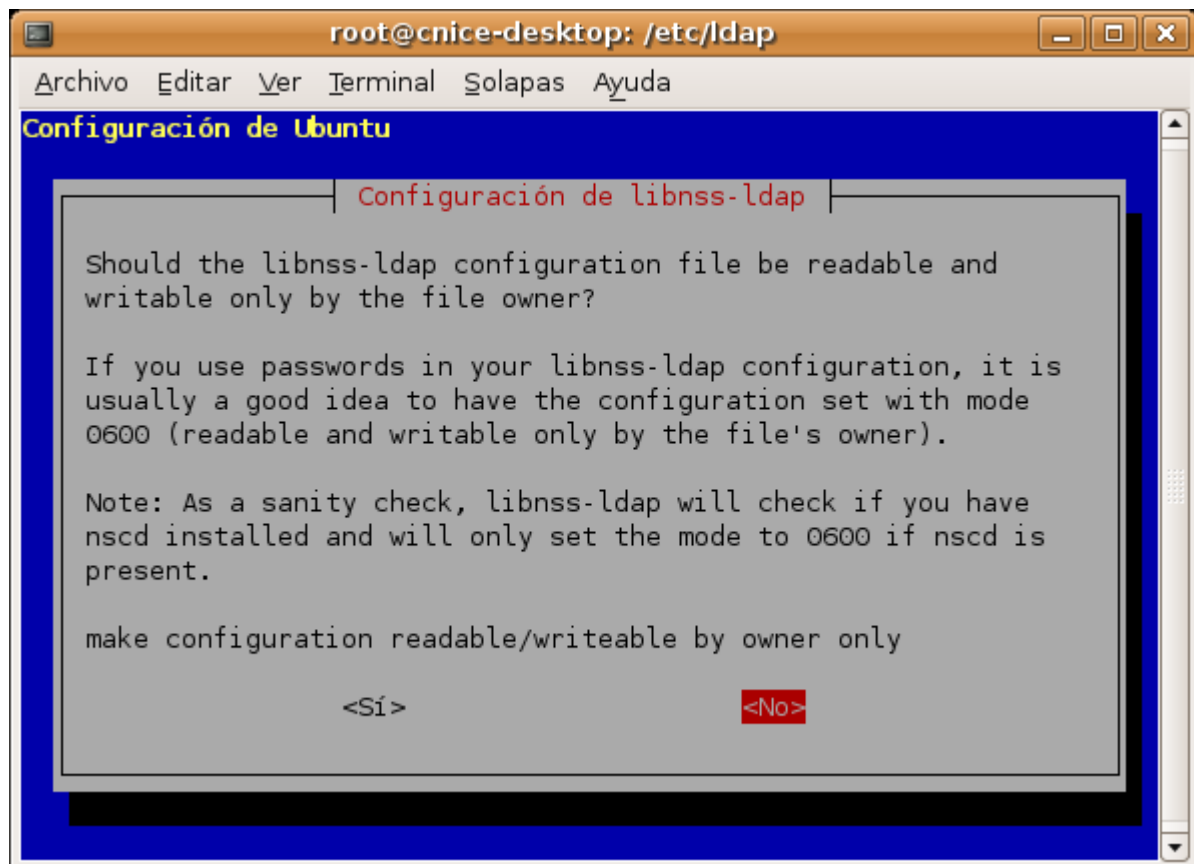


En el siguiente paso nos pregunta si necesitamos autenticarnos en el servidor LDAP o no. Como la librería únicamente va a realizar consultas, no es necesario autenticarse por lo tanto debemos responder 'No':

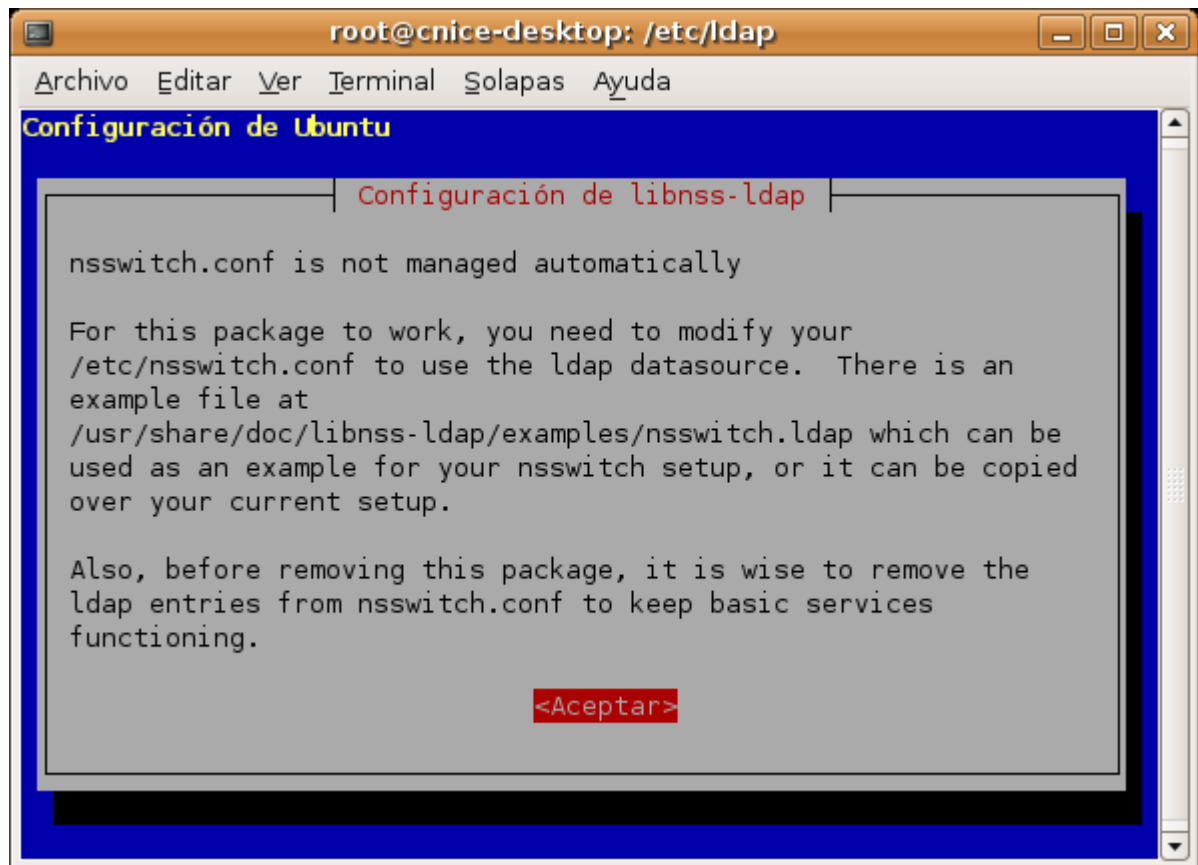


Posteriormente nos preguntará si el archivo **/etc/libnss-ldap** debe solamente tener permisos de lectura y

escritura para el usuario (root que es quién instala) o no. Como en el paso anterior hemos indicado que no necesitamos autenticación, no se almacenarán contraseñas en el archivo de configuración, por tanto podemos responder 'No':



Finalmente nos advierte que debemos modificar el archivo **/etc/nsswitch.conf** para que el sistema utilice el directorio LDAP como base de datos del sistema, al igual que hace con los archivos passwd, group y shadow:



Con el asistente se habrá configurado casi todo lo necesario aunque para que nuestro sistema se autentique por LDAP, aún hay que configurar dos parámetros más:

1. En qué unidad organizativa se encuentran los usuarios (sustituto de **/etc/passwd** - en nuestro caso ou=users)
2. En qué unidad organizativa se encuentran los grupos (sustituto de **/etc/group** - en nuestro caso ou=groups)

Para ello hay que modificar dos líneas en el archivo de configuración. Son las siguientes:

```
// Configurar en /etc/libnss-ldap.conf
nss_base_passwd ou=users,dc=ieslapaloma,dc=com

nss_base_group  ou=groups,dc=ieslapaloma,dc=com
```

Configuración de NSS

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 autentificar 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. Para que los servicios de nuestro sistema utilicen primero las librerías **pam_ldap.so** para autenticar al usuario, debemos añadir 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 añadir 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 añadir 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 añadir 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 añadir 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# ptest 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

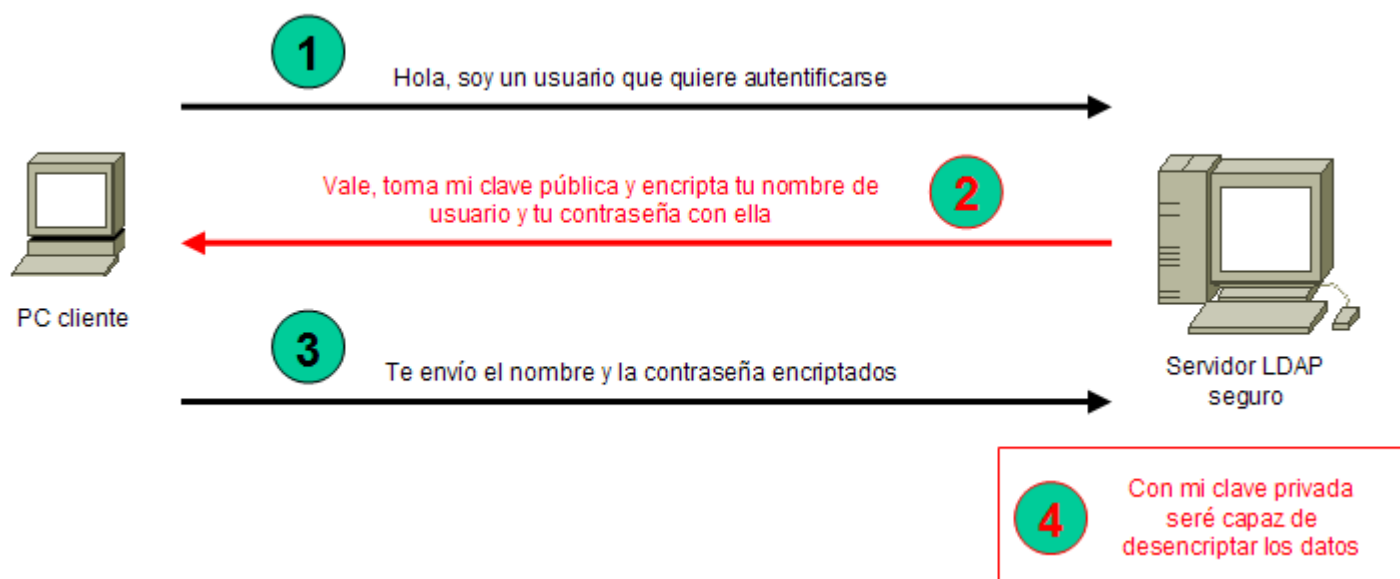
elementos caros para su aplicación. En entornos educativos y en pequeñas y medianas empresas, se sigue utilizando el mecanismo tradicional de autenticación del usuario mediante su nombre de usuario (login) y su contraseña (password).

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 cifrar (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.- Copiar los certificados a la carpeta deseada, renombrar y proteger
- 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,

```
// Crear nueva entidad certificadora
```

```
root@cnice-desktop:~# /usr/lib/ssl/misc/CA.pl -newca
```

```
CA certificate filename (or enter to create)Pulsamos enter para crear
```

```
Making CA certificate ...
```

```
Generating a 1024 bit RSA private key .....+++++
.....+++++
```

```
writing new private key to './demoCA/private/cakey.pem'
```

```
Enter PEM pass phrase: Ponemos contraseña
```

```
Verifying - Enter PEM pass phrase: Repetimos contraseña
```

```
-----
```

```
You are about to be asked to enter information that will be
incorporated
```

```
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or
a DN.
```

```
There are quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
```

```
If you enter '.', the field will be left blank.
```

```
-----
```

```
Country Name (2 letter code) [AU]:ES
```

```
State or Province Name (full name) [Some-State]:España
```

```
Locality Name (eg, city) []:Soria
```

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:I.E.S. La
Paloma
```

Organizational Unit Name (eg, section) []:**CertificadorIES**

Common Name (eg, YOUR name) []:**I.E.S. La Paloma**

Email Address []:**root@ieslapaloma.com**

Ya tendríamos creada nuestra nueva entidad certificadora bajo la carpeta demoCA 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 **newreq.pem**. Para crear la petición de firma debemos ejecutar el siguiente comando:

```
// Crear petición de firma de certificado de servidor
# openssl req -newkey rsa:1024 -nodes -keyout newreq.pem -out
newreq.pem

Generating a 1024 bit RSA private key
.....+++++ .....+++++

writing new private key to 'newreq.pem'

-----

You are about to be asked to enter information that will be
incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or
a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]:ES

State or Province Name (full name) [Some-State]:España

Locality Name (eg, city) []:Soria

Organization Name (eg, company) [Internet Widgits Pty Ltd]:I.E.S. La
Paloma

Organizational Unit Name (eg, section) []:Web IES La Paloma

Common Name (eg, YOUR name) []:I.E.S. La Paloma
```

Email Address []: **root@ieslapaloma.com**

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password !-[]: **Pulsamos enter**

An optional company name []: : **Pulsamos enter**

Ya tendríamos creado el archivo newreq.pem que contiene la petición de firma de certificado de servidor.

3.- Firmar el certificado con la CA

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

```
// Firmar la petición de firma de certificado del servidor
root@cnice-desktop:~# /usr/lib/ssl/misc/CA.sh -sign
```

Using configuration from /usr/lib/ssl/openssl.cnf

Enter pass phrase for ./demoCA/private/cakey.pem: **Contraseña de la CA**

Check that the request matches the signature

Signature ok

Certificate Details:

Serial Number:

a6:07:d5:91:ad:b3:8f:74

Validity

Not Before: Oct 10 18:46:12 2005 GMT

Not After : Oct 10 18:46:12 2006 GMT

Subject:

countryName = ES

stateOrProvinceName = Espa\Fla

localityName = Soria

organizationName = I.E.S. La Paloma

organizationalUnitName = Web IES La Paloma

commonName = I.E.S. La Paloma

emailAddress = root@ieslapaloma.com

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

Netscape Comment:

OpenSSL Generated Certificate

X509v3 Subject Key Identifier:

B1:DA:5C:4B:E8:9E:80:8B:9F:7D:51:B1:A5:E8:84:FF:6E:27:

1F:E6

X509v3 Authority Key Identifier:

keyid:D8:9A:35:45:0B:2F:BE:FC:CC:43:A6:0C:9F:27:08:93:

33:D0:D8:AA

DirName:/C=ES/ST=Espa\xFla/L=Soria/O=I.E.S. La Paloma

/OU=CertificadorIES/emailAddress=root@ieslapaloma.com

serial:A6:07:D5:91:AD:B3:8F:73

Certificate is to be certified until Oct 10 18:46:12 2006 GMT (365 days)

Sign the certificate? [y/n]: **y //** ¿Firmamos?

1 out of 1 certificate requests certified, commit? [y/n] **y //**
¿Proceder?

Write out database with 1 new entries

Data Base Updated

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

a6:07:d5:91:ad:b3:8f:74

Signature Algorithm: md5WithRSAEncryption

Issuer: C=ES, ST=Espa\xFla, L=Soria, O=I.E.S. La Paloma,
OU=CertificadorIES/emailAddress=root@ieslapaloma.com

Validity

Not Before: Oct 10 18:46:12 2005 GMT

Not After : Oct 10 18:46:12 2006 GMT

Subject: C=ES, ST=Espa\xFla, L=Soria, O=I.E.S. La Paloma,

OU=Web IES La Paloma, CN=I.E.S. La
Paloma/emailAddress=root@ieslapaloma.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:bc:10:87:92:cb:c8:dd:e1:9e:6a:15:a9:09:44:
7a:f9:bb:c7:1e:2e:66:23:92:56:ec:65:36:d3:15:
d6:62:56:e4:27:6a:a1:c1:36:7b:cc:c9:20:1e:9d:
8a:d8:cd:56:f1:60:d6:c7:6e:1f:6b:19:77:5f:6e:
ac:ec:4d:19:c8:bf:6e:6b:12:a2:b3:3f:56:84:c0:
c7:48:09:7a:52:d2:0c:6b:ca:0d:d8:37:90:48:2e:
58:16:b5:46:d8:6d:44:bf:2a:3b:07:12:51:d6:2e:
58:ed:46:0e:6f:d7:f5:f7:ce:3f:e8:93:98:62:d0:
8b:d1:9b:1f:08:58:09:30:d7

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

Netscape Comment:

OpenSSL Generated Certificate

X509v3 Subject Key Identifier:

B1:DA:5C:4B:E8:9E:80:8B:9F:7D:51:B1:A5:E8:84:FF:6E:27:
1F:E6

X509v3 Authority Key Identifier:

keyid:D8:9A:35:45:0B:2F:BE:FC:CC:43:A6:0C:9F:27:08:93:
33:D0:D8:AA

DirName:/C=ES/ST=Espa\xFla/L=Soria/O=I.E.S. La Paloma
/OU=CertificadorIES/emailAddress=root@ieslapaloma.com
serial:A6:07:D5:91:AD:B3:8F:73

Signature Algorithm: md5WithRSAEncryption

87:f1:0e:39:6d:02:48:ee:c2:2b:59:d4:e2:e5:ec:23:7e:7d:
f1:0d:bb:78:45:ad:04:f7:19:d0:a9:3d:3d:6b:e5:61:34:6b:
bc:fa:1b:d1:28:31:9a:aa:b4:93:f6:51:cf:36:83:cb:e1:29:
9b:7d:6c:a8:06:77:b6:80:f0:30:49:08:56:e9:f7:e0:24:1e:
8e:fa:d9:d6:f2:ad:f5:f8:f0:f2:c0:d1:92:c5:c5:17:3c:4c:
06:48:f5:c6:0c:4d:4f:39:fc:fb:f5:9f:2b:29:46:5a:fe:5d:
99:68:4d:73:02:4f:59:ab:e1:e2:5c:b1:86:b1:bb:85:c9:de:
fa:0b

-----BEGIN CERTIFICATE-----

MIIDyzCCAzSgAwIBAgIJAKYH1ZGts490MA0GCSqGSIb3DQEBAUAMIGIMQswCQYD
VQQGEwJFUzEPMA0GA1UECBQGRXNwYfFhMQ4wDAYDVQQHEwVTb3JpYTEZMBcGA1UE
ChMQSS5FLlMuIEExhIFBhbG9tYTEYMBYGA1UECxMPQ2VydGhmaWNhZG9ySUVTMSMw
IQYJKoZIhvcNAQkBFhRyb290QGllc2xhcGFsb21hLmNvbTAeFw0wNTEwMTAxODQ2
MTJaFw0wNjEwMTAxODQ2MTJaMIGlMQswCQYDVQQGEwJFUzEPMA0GA1UECBQGRXNw
YfFhMQ4wDAYDVQQHEwVTb3JpYTEZMBcGA1UEChMQSS5FLlMuIEExhIFBhbG9tYTEa
MBGGA1UECxMRV2ViIElFUyBMYSBQYWxvbWExGTAXBgNVBAMTEEkuRS5TLiBMYSBQ
YWxvbWExIzAhBgkqhkiG9w0BCQEFWFHJvb3RAaWVzbGFwYWxvbWEuY29tMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8EIEsy8jd4Z5qFakJRHR5u8ceLmYjklbs

```

ZTbTFdZiVuQnaqHBNnvMySAenYrYzVbxYNbHbh9rGXdfbqzsTRnIv25rEqKzPlaE
wMdICXpS0gxryg3YN5BILlgWtUbYbUS/KjsHElHWLljtRg5v1/X3zj/ok5hi0IvR
mx8IWAkw1wIDAQABo4IBHDCCARgwCQYDVR0TBAlwADAsBglghkgBhvhCAQ0EHxYd
T3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBByEFLHaXEvonocL
n3lRsaXohP9uJx/mMIG9BgNVHSMEgbUwgbKAFNiaNUULL778zEOmDJ8nCJMz0Niq
oYGOpIGLMIGIMQswCQYDVQQGEwJFUzEPMA0GA1UECBQGRXNwYfFhMQ4wDAYDVQQH
EwVTb3JpYTEZMBCGA1UEChMQSS5FLlMuIEExIFBhbG9tYTEYMBYGA1UECXPQ2Vy
dGlmaWNhZG9ySUVTMSMwIQYJKoZIhvcNAQkBFhRyb290QGllc2xhcGFsb21hLmNv
bYIJAKYH1ZGts49zMA0GCSqGSIb3DQEBAUAA4GBAIfxDjltAkjuwitZ1OL17CN+
ffENu3hFrQT3GdCpPT1r5WE0a7z6G9EoMZqqtJP2Uc82g8vhKZt9bKgGd7aA8DBJ
CFbp9+AkHo762dbyrfX48PLA0ZLFxRc8TAZI9cYMTU85/Pv1nyspRlr+XZloTXMC
Tlmr4eJcsYaxu4XJ3voL
-----END CERTIFICATE-----

Signed certificate is in newcert.pem

```

Este proceso nos habrá creado el archivo newcert.pem que contiene el certificado firmado.

4.- Copiar los certificados a la carpeta deseada, renombrar y proteger

Acto seguido debemos renombrar los archivos creados, moverlos a un lugar adecuado y proteger la clave privada del servidor. Un lugar adecuado para almacenar los certificados es dentro de la carpeta /etc/ldap que es donde se guardan los archivos de configuración del servidor LDAP, una carpeta llamada 'certs' que podemos crear manualmente. Luego copiaremos el certificado de la CA. Copiaremos el archivo newcert.pem con el nombre 'servercert.pem' ya que será el certificado de nuestro servidor. Copiaremos el archivo newreq.pem con el nombre 'serverkey.pem' ya que será la clave privada de nuestro servidor y finalmente pondremos permisos de solo lectura para el root ya que a la clave privada no tiene que tener acceso nadie, si no podrían descifrar la información cifrada dirigida al servidor.

```

// Copiar certificados a su destino
root@cnice-desktop:~# mkdir /etc/ldap/certs

root@cnice-desktop:~# cp demoCA/cacert.pem /etc/ldap/certs/cacert.pem

root@cnice-desktop:~# cp newcert.pem /etc/ldap/certs/servercert.pem

root@cnice-desktop:~# cp newreq.pem /etc/ldap/certs/serverkey.pem

root@cnice-desktop:~# chmod 400 /etc/ldap/certs/serverkey.pem

```

5.- Configurar slapd para que utilice los certificados

Para que el servidor LDAP utilice los certificados que acabamos de crear, es necesario indicarlo en el archivo de configuración.

```
// Configuración del servidor LDAP para que utilice ssl
// Añadir en /etc/ldap/slapd.conf

TLSCipherSuite HIGH:MEDIUM:+SSLv2

TLSCACertificateFile /etc/ldap/certs/cacert.pem

TLSCertificateFile /etc/ldap/certs/servercrt.pem

TLSCertificateKeyFile /etc/ldap/certs/serverkey.pem
```

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

Por defecto, cuando iniciamos el servidor LDAP con el comando '/etc/init.d/slapd start', arranca solamente en modo normal. Para que arranque también el modo seguro, es necesario realizar una modificación en el archivo '/etc/init.d/slapd' que es el script de inicio:

```
// Añadir en /etc/init.d/slapd
# Sección: Set default values

SLAPD_SERVICES="ldap:/// 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.

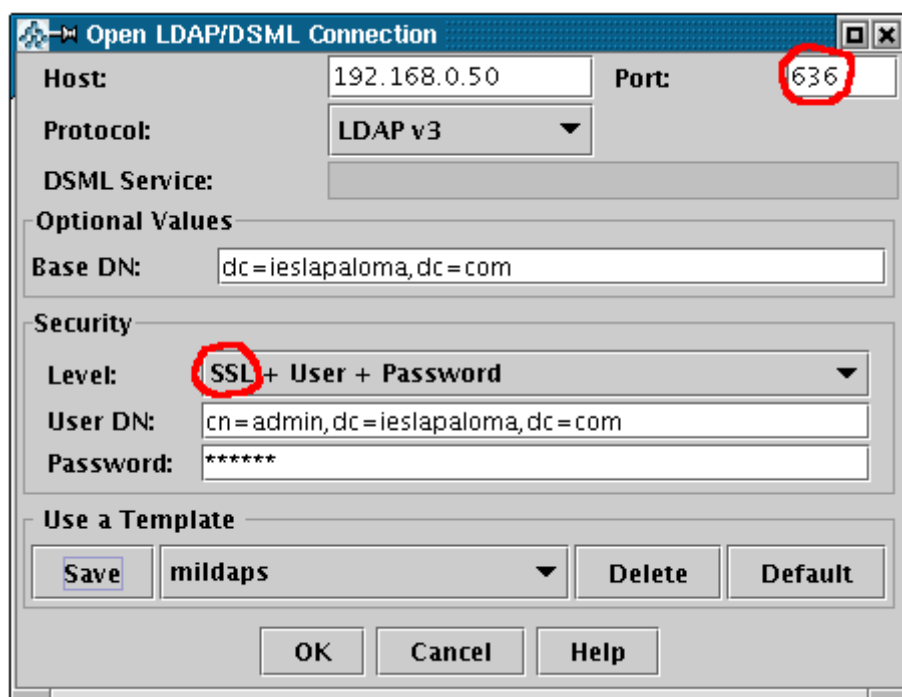
7.- Reiniciar servidor LDAP

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

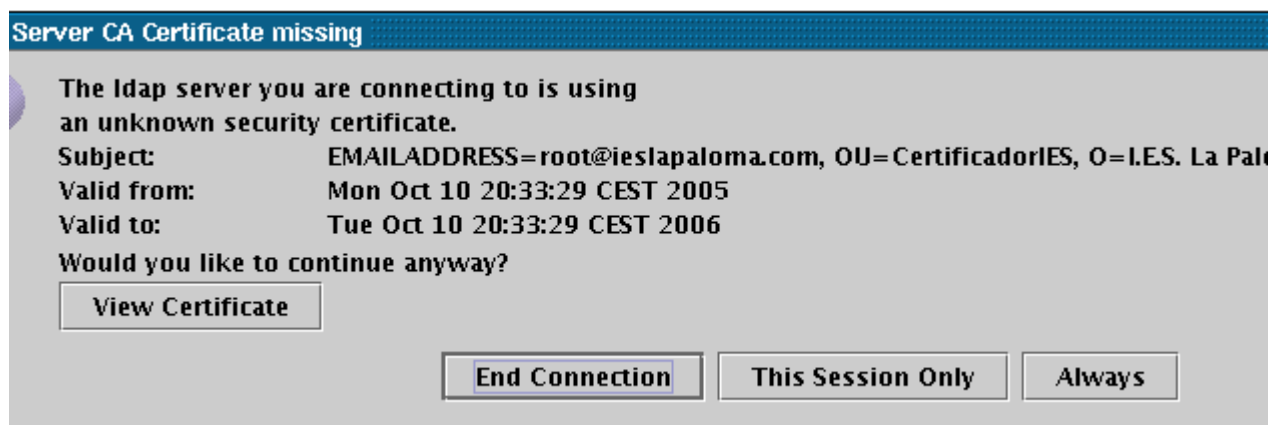
Si nuestro servidor LDAP está funcionando en modo seguro, estará escuchando en el puerto 636 ya que es el puerto utilizado por el protocolo ldaps. Para probarlo, iniciamos JXplorer pero la conexión la realizamos a dicho puerto y el nivel de seguridad seleccionamos SSL + User + Password ya que la autenticación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



The image shows a Windows-style dialog box titled "Open LDAP/DSML Connection". It contains several fields and sections:

- Host:** 192.168.0.50
- Port:** 636 (circled in red)
- Protocol:** LDAP v3 (dropdown menu)
- DSML Service:** (empty text field)
- Optional Values** section:
 - Base DN:** dc=ieslapaloma,dc=com
- Security** section:
 - Level:** SSL + User + Password (circled in red, dropdown menu)
 - User DN:** cn=admin,dc=ieslapaloma,dc=com
 - Password:** (masked with asterisks)
- Use a Template** section:
 - Save** button
 - mildaps** (dropdown menu)
 - Delete** button
 - Default** button
- At the bottom: **OK**, **Cancel**, and **Help** buttons.

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



The image shows a Windows-style dialog box titled "Server CA Certificate missing". It contains the following text and buttons:

The ldap server you are connecting to is using an unknown security certificate.

Subject: EMAILADDRESS=root@ieslapaloma.com, OU=CertificadorIES, O=I.E.S. La Paloma

Valid from: Mon Oct 10 20:33:29 CEST 2005

Valid to: Tue Oct 10 20:33:29 CEST 2006

Would you like to continue anyway?

View Certificate button

At the bottom: **End Connection**, **This Session Only**, and **Always** buttons.

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

