Gestión de LDAP en Debian

Índice de contenido

Realizado por: Sagrario Pedraza Labrador
Módulo: Implantación de Sistemas Operativos (ISO)
Curso: 2011/2012

1. LDAP

LDAP (***L**ightweight **D**irectory **A**ccess **P**rotocol*) es un servicio de directorio optimizado para la realización rápida de operaciones de lectura y búsqueda de información.

LDAP se usa principalmente como servidor de autentificación para controlar el acceso de los usuarios a un sistema, aunque por lo que me han comentado, la tendencia hoy en día es que todos los servicios de una organización usen los datos almacenados en el servidor ldap.

Los institutos de Extremadura almacenan en LDAP además de la información de usuarios y grupos, toda la información de dns y dhcp. El control de acceso inalámbrico del IES Valle del Jerte se hace mediante un servidor que obtiene los datos de usuarios y grupos de un servidor ldap.

LDAP se puede usar también para controlar el acceso de usuarios a aplicaciones web, a servidores ftp, servidores de correo, servidores de mensajería, etc...

La ventaja de tener un servidor LDAP es que podemos tener centralizada toda la información en un único lugar. Además, un servidor LDAP se puede replicar de forma que tengamos un servidor de reserva por si el servidor principal cae.

En el sistema de autentificación con LDAP un usuario que quiere acceder al sistema envía su usuario y su contraseña al servidor y éste le concede o deniega el acceso.

Para realizar el trabajo he instalado:

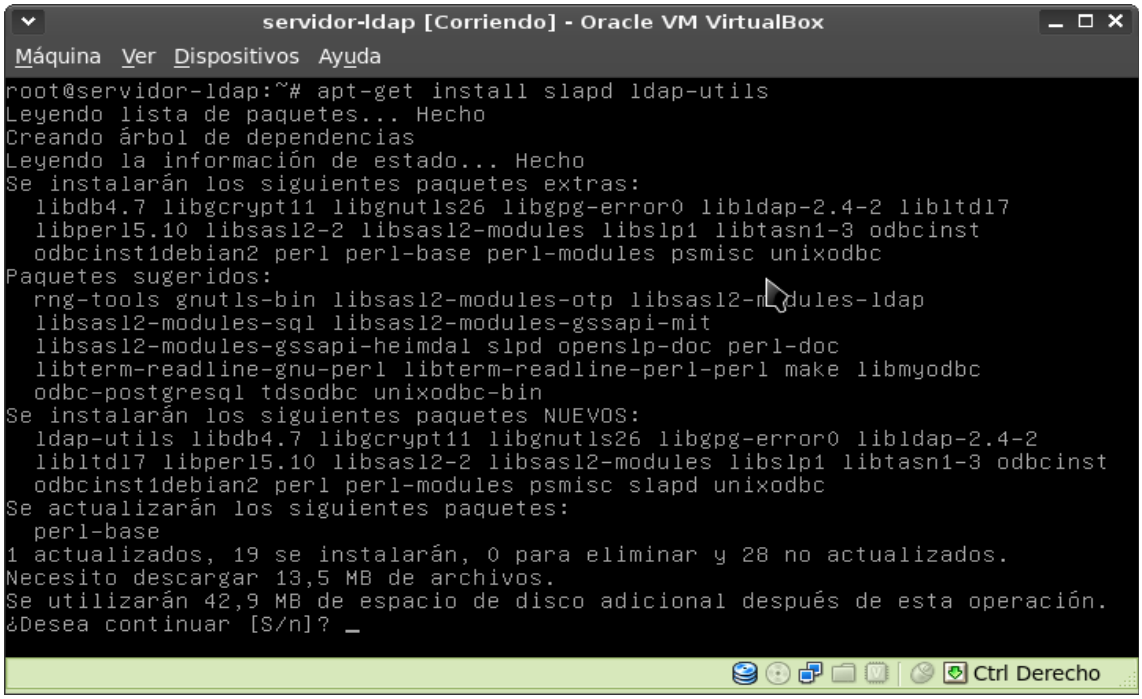
- Un servidor LDAP en una máquina virtual con Debian Squeeze.
- Un cliente LDAP en una máquina virtual con Debian Squeeze.

2. Instalación de un servidor LDAP.

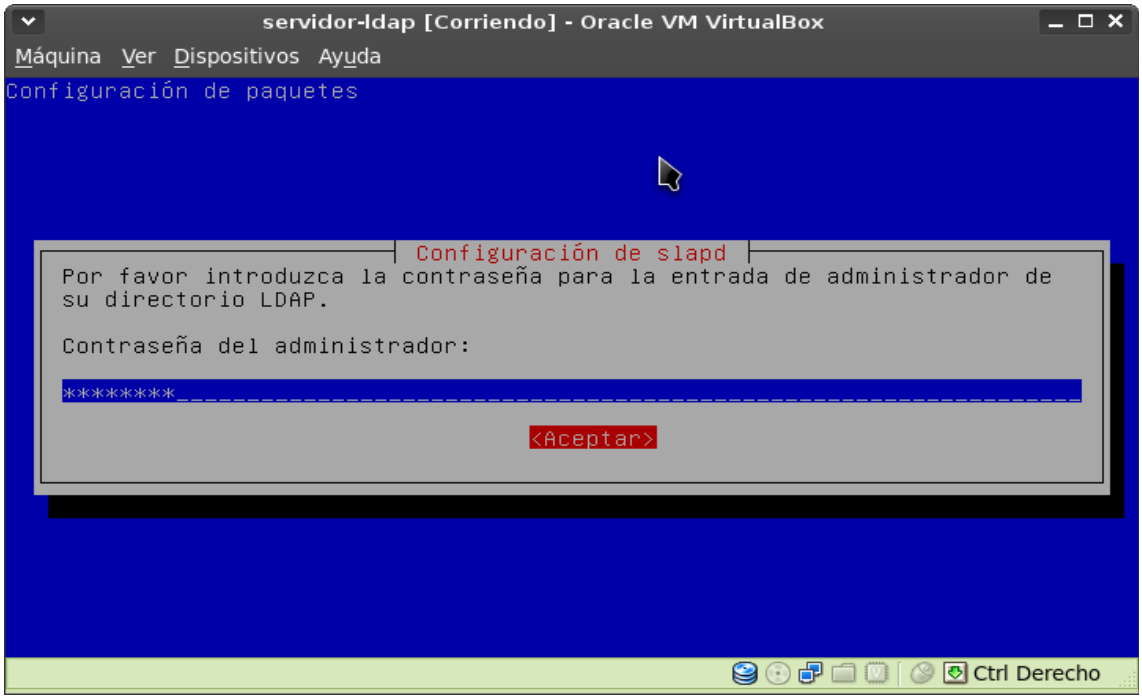
2.1 Instalación del servicio LDAP.

Instalar el servidor LDAP en Debian es muy sencillo. Tan sólo tenemos que instalar el paquete **slapd**. Además instalaremos también el paquete **ldap-utils** que nos va a proporcionar utilidades adicionales para realizar consultas y modificaciones del servidor ldap desde la línea de comandos.

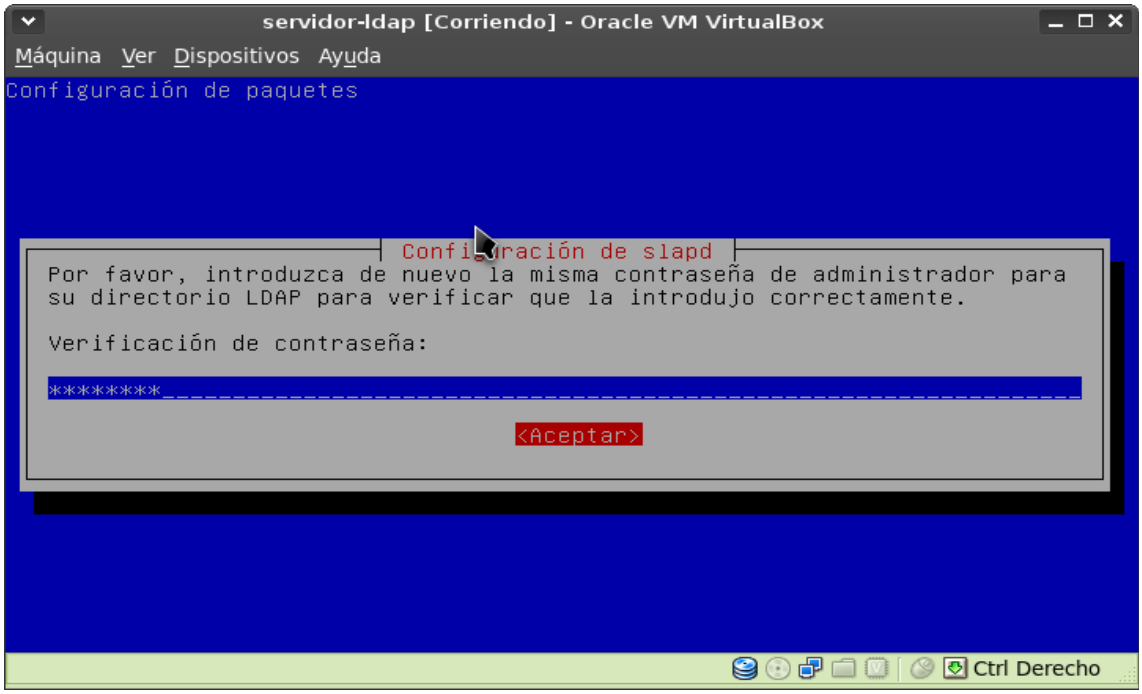
```
# apt-get install slapd ldap-utils
```



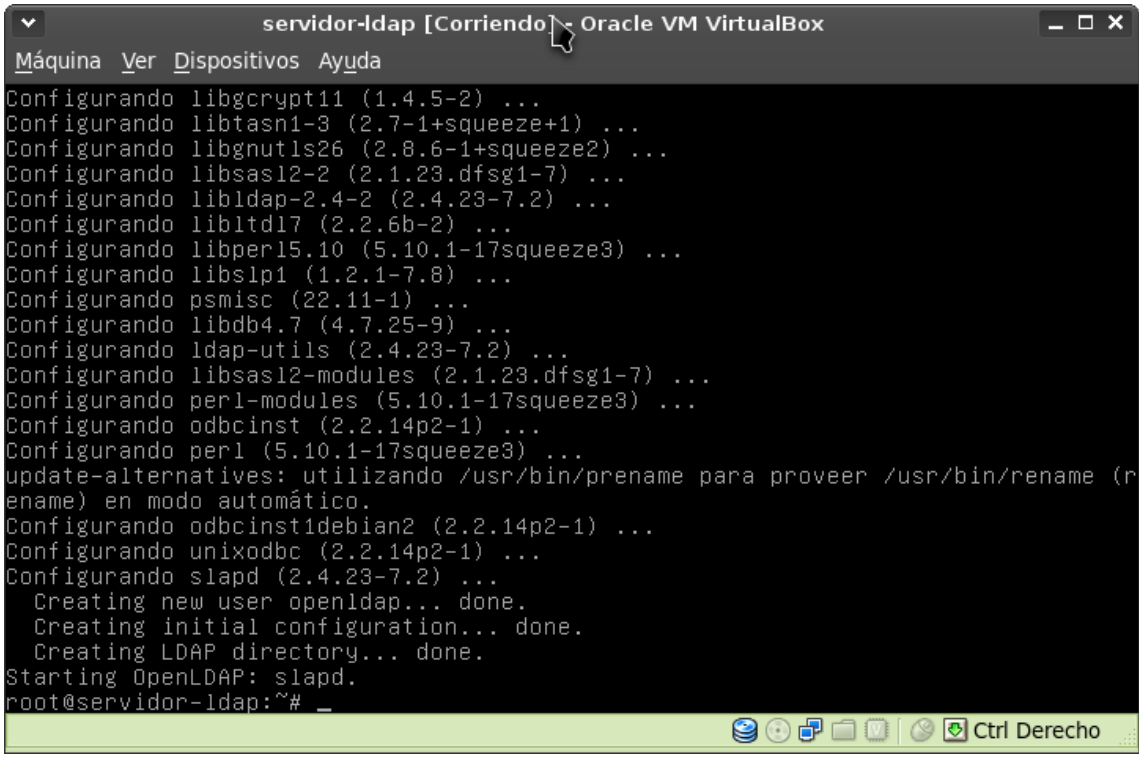
Nos pide confirmación. Pulsamos Enter para confirmar que queremos realizar la instalación. A continuación nos pedirá que introduzcamos una contraseña para el administrador de ldap:



Nos pedirá que volvamos a introducir la contraseña para asegurar que la introducimos bien:

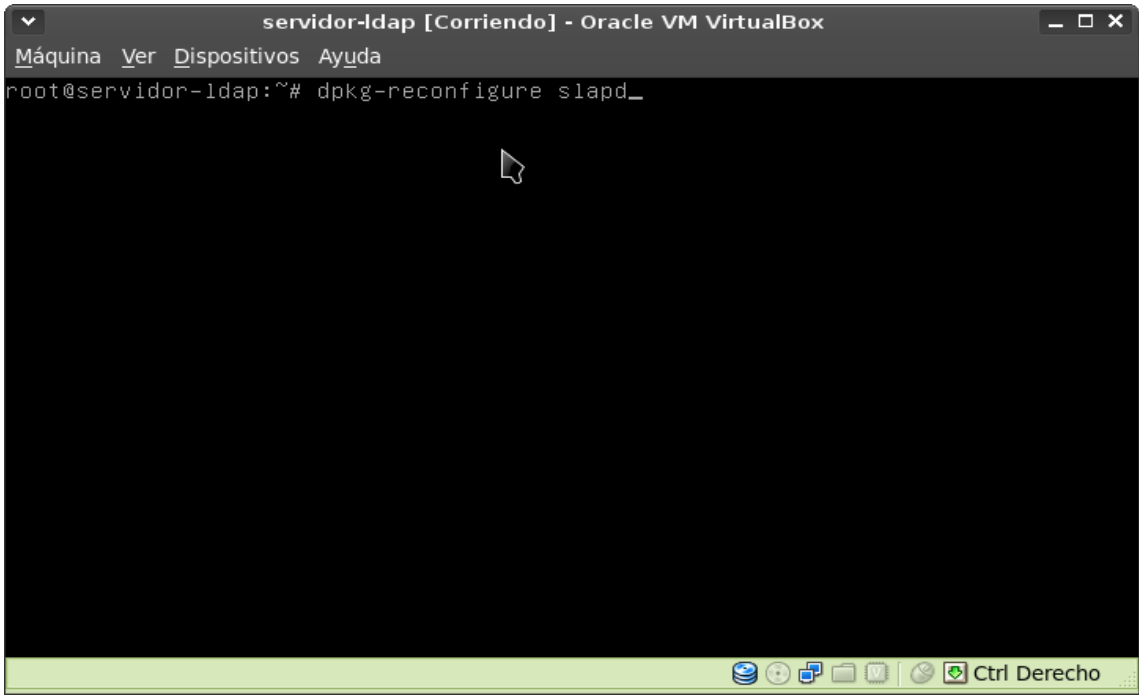


Una vez introducida, comenzará el proceso de instalación y configuración:

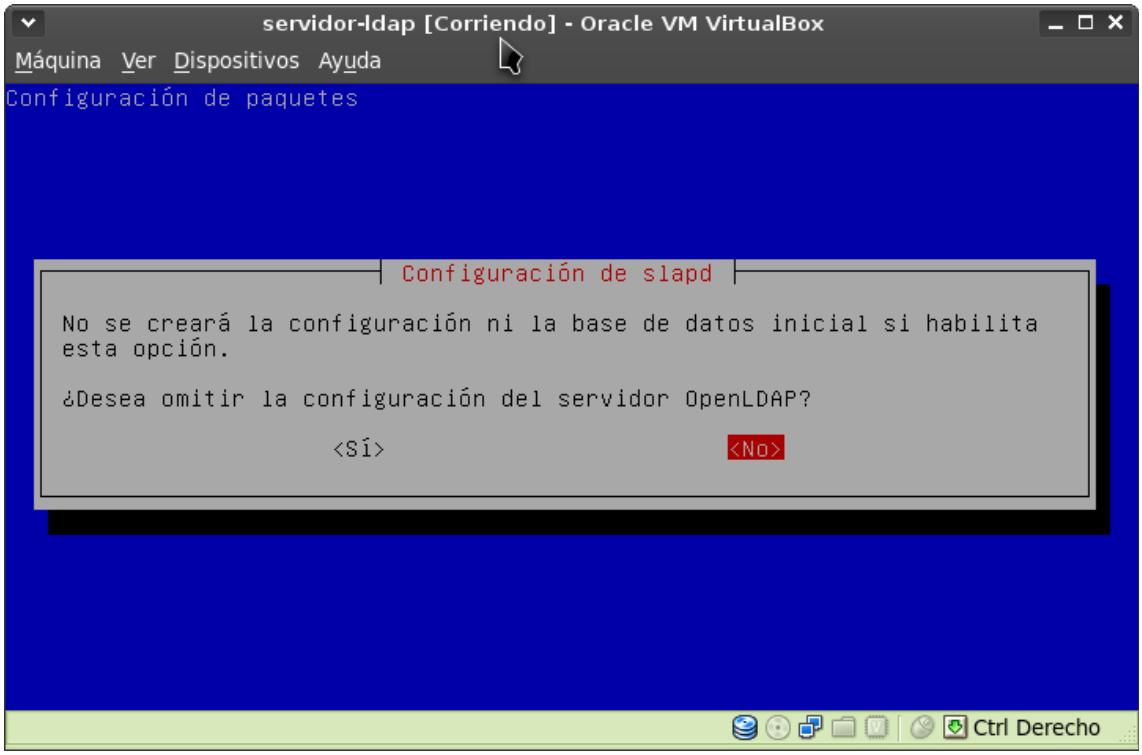


2.2 Configuración del servicio LDAP.

Bien, pues ahora que ya tenemos instalado el servidor LDAP, ahora vamos a configurarlo:



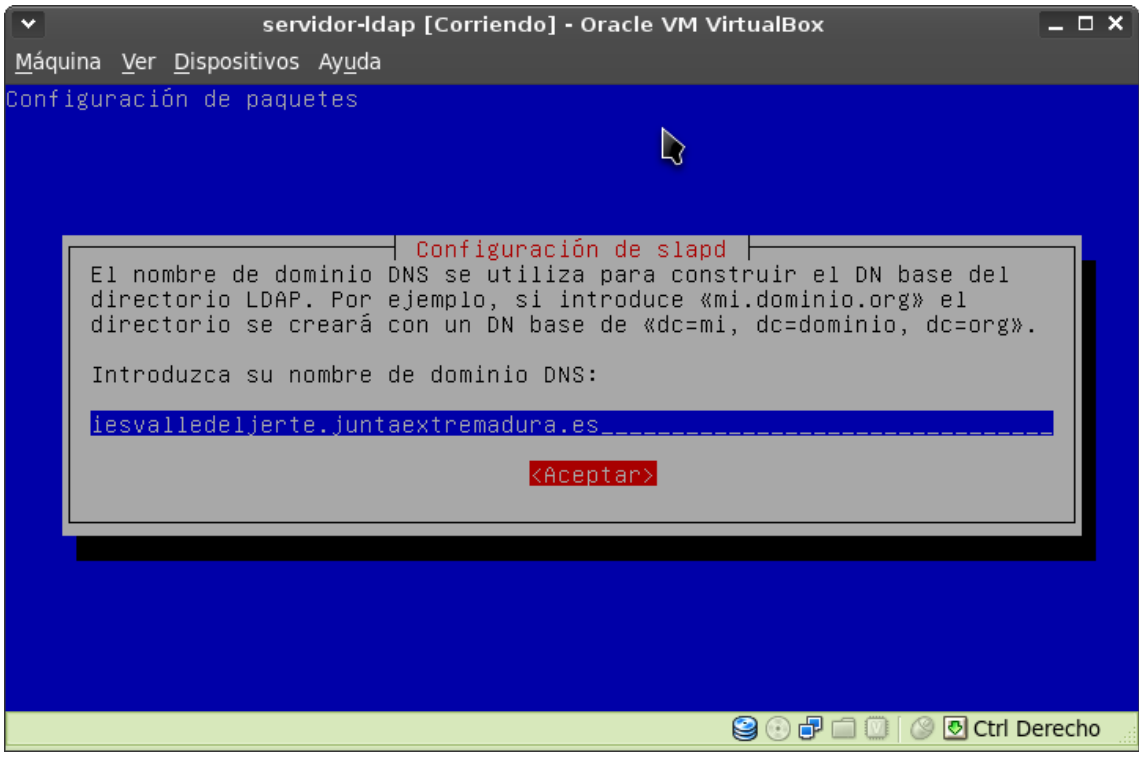
Pulsamos **enter** y se iniciará un asistente que nos irá pidiendo los datos para configurar el servicio LDAP. Lo primero que nos pregunta es si deseamos omitir la configuración de LDAP:



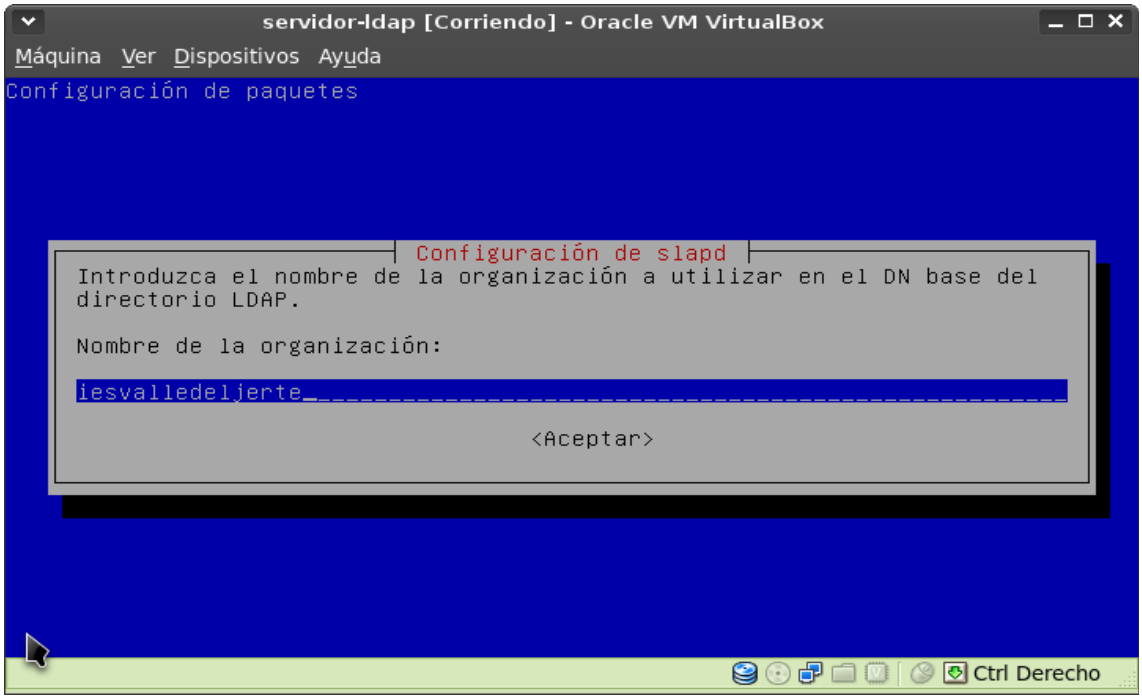
Le respondemos **“No”** porque precisamente lo que queremos es configurarlo.

Nos preguntará qué nombre de dominio queremos darle a la base de nuestro directorio LDAP. Esta base es el elemento raiz del que cuelgan todos los demás. En LDAP se almacenan los datos de forma jerárquica en forma de árbol. Para la práctica, como nombre de dominio he elegido:

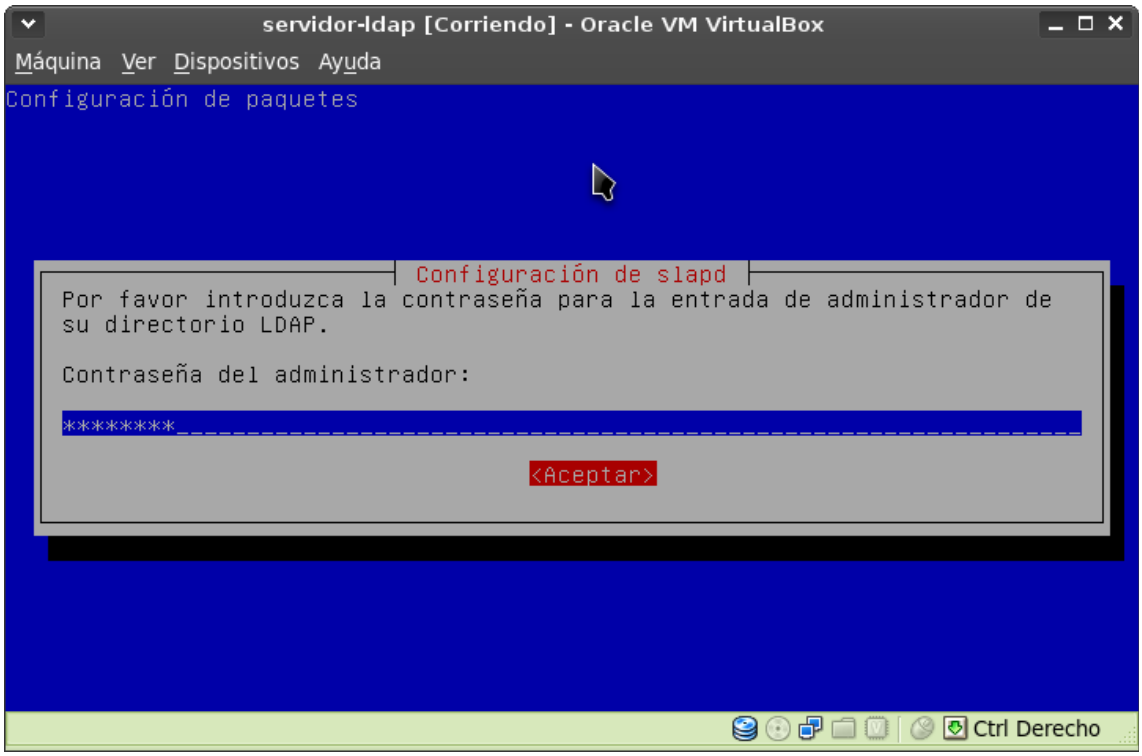
iesvalledeljerte.juntaextremadura.es



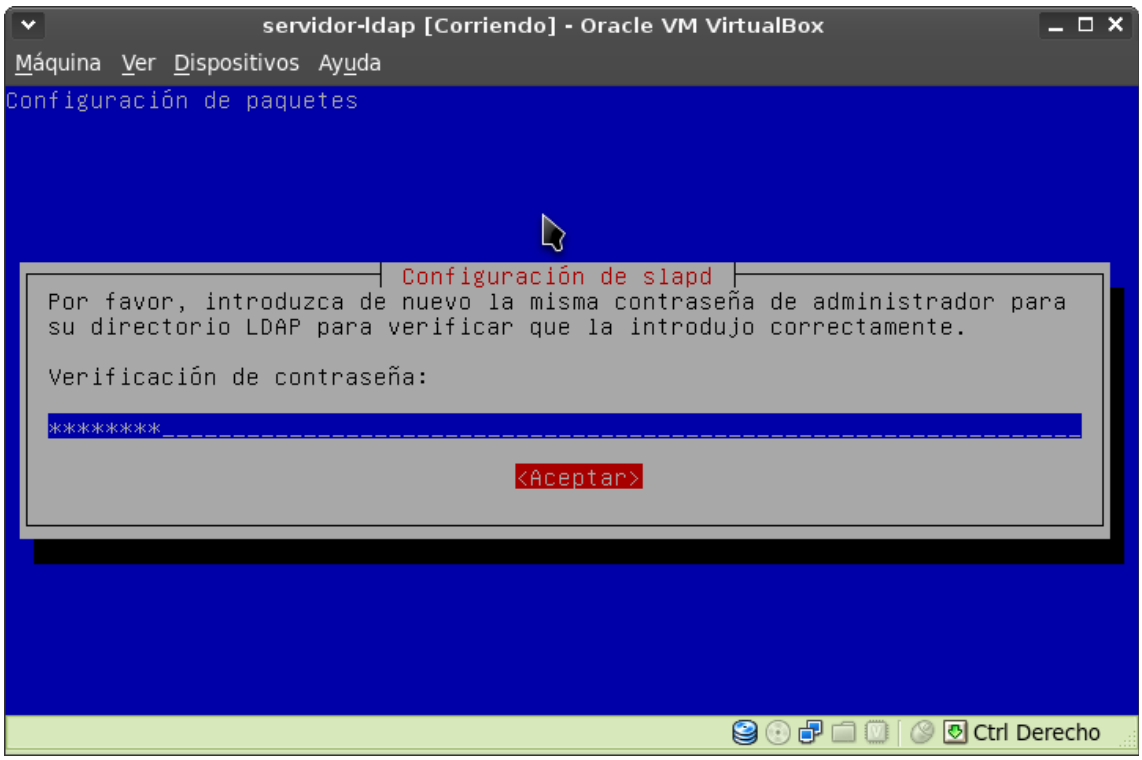
A continuación nos pedirá que introduzcamos el nombre de nuestra organización:



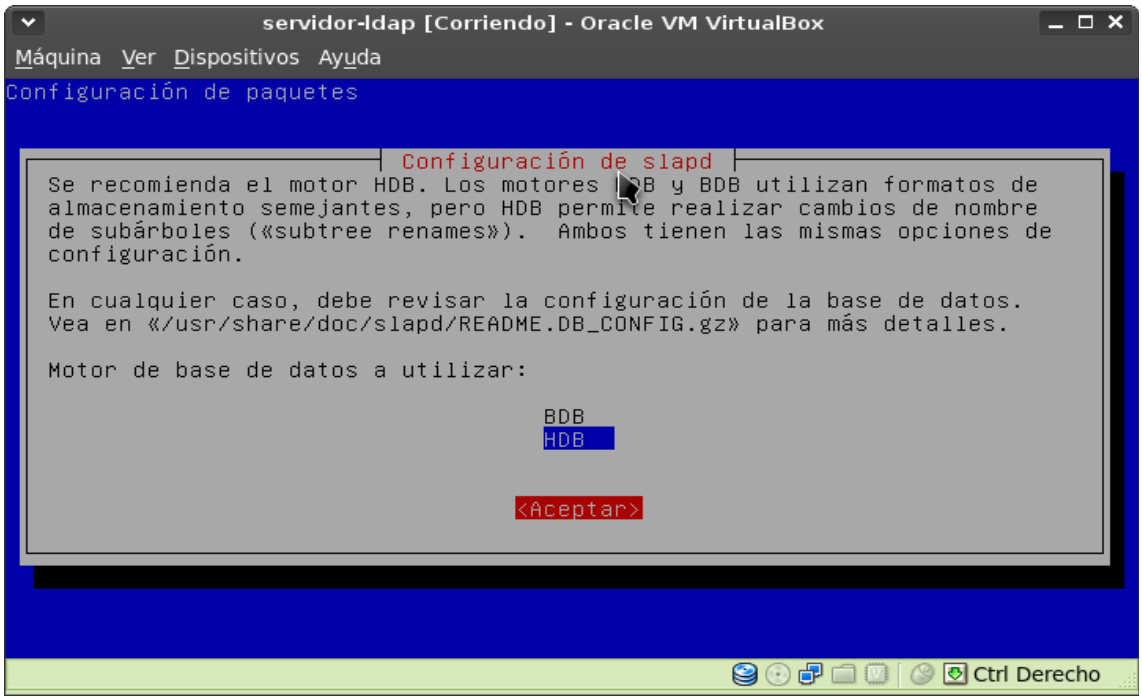
Una vez especificado, nos pedirá que introduzcamos la contraseña del administrador LDAP. La introducimos y pulsamos <**Aceptar**>:



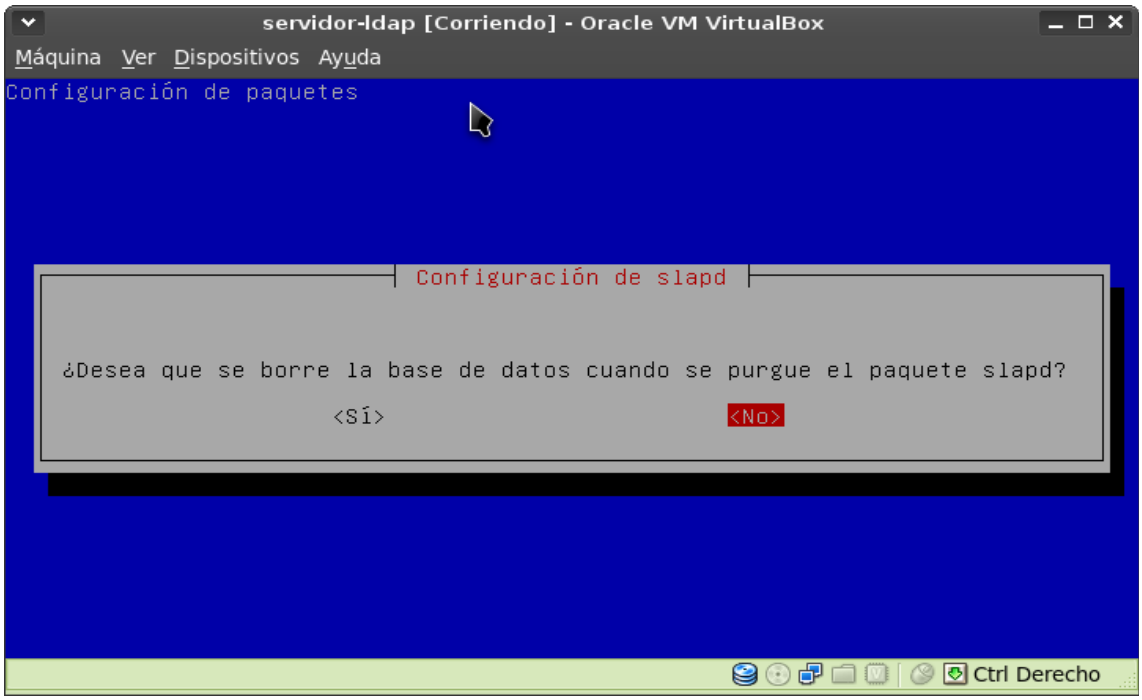
Nos pedirá que volvamos a introducirla de nuevo para confirmar:



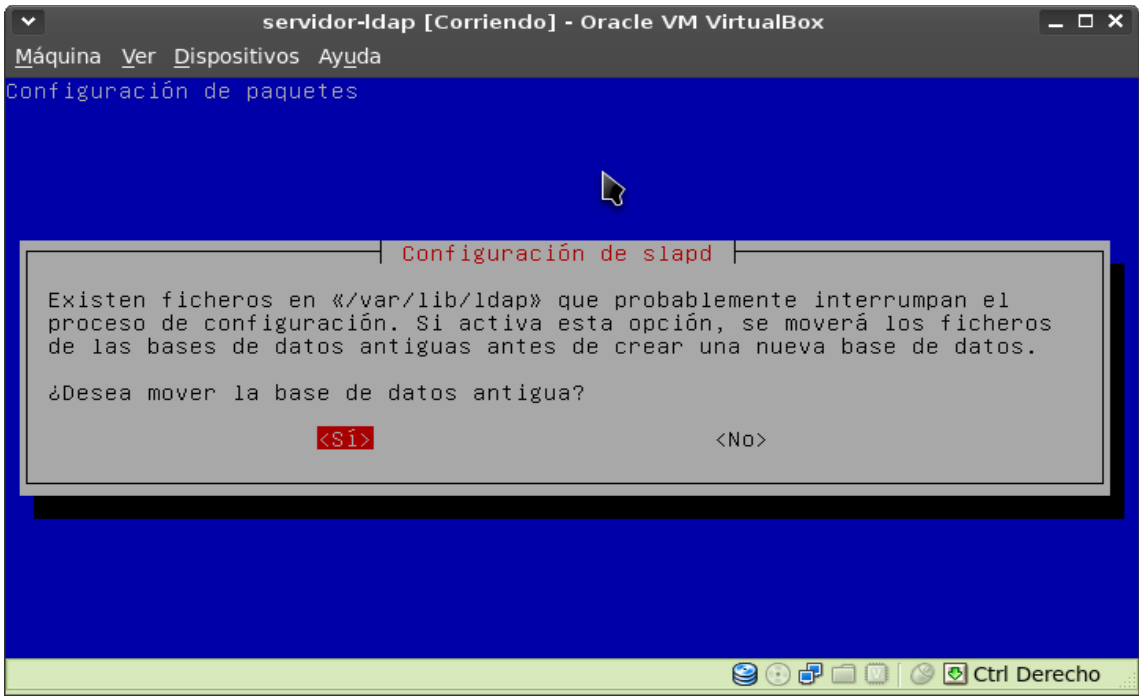
A continuación nos pedirá que elijamos qué motor de almacenamiento de datos queremos usar. El motor HDB es más nuevo. Lo seleccionamos:



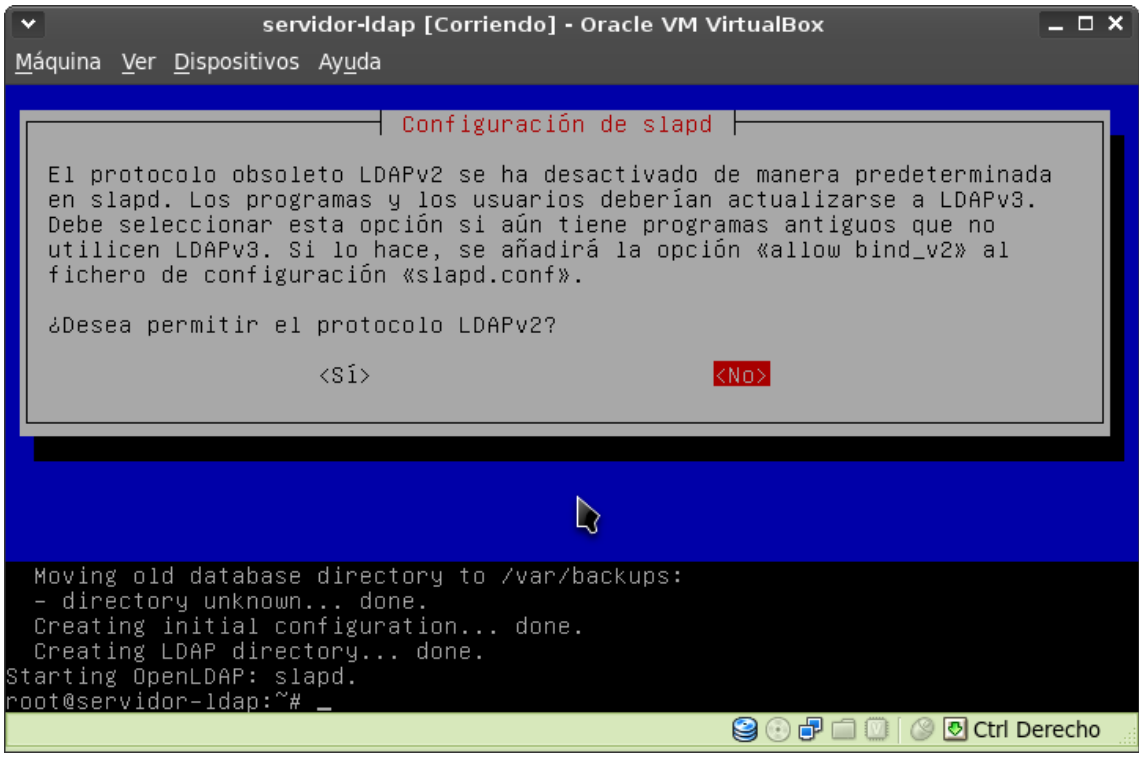
Nos preguntará si queremos que se elimine la base de datos cuando elijamos desinstalar ldap y borrar sus archivos de configuración. Le respondemos que no:



Si hemos configurado anteriormente el servicio LDAP, tendremos los ficheros de la base de datos almacenados en el directorio /var/lib/ldap. Nos pregunta si queremos moverlos a un directorio de backup (concretamente a /var/backups) por si fuera necesario recuperarlos. Le decimos que si:



A continuación nos preguntará si queremos permitir usar el protocolo LDAPv2. Por lo que he leído actualmente se usa el protocolo LDAPv3. Tan sólo tendríamos que permitir usar LDAPv2 si tuviéramos programas antiguos que no utilizan LDAPv3.Una vez hecho ésto ya tendremos configurado el servicio LDAP.


servidor-ldap [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
Configuración de slapd
El protocolo obsoleto LDAPv2 se ha desactivado de manera predeterminada en slapd. Los programas y los usuarios deberían actualizarse a LDAPv3. Debe seleccionar esta opción si aún tiene programas antiguos que no utilicen LDAPv3. Si lo hace, se añadirá la opción «allow bind_v2» al fichero de configuración «slapd.conf».
¿Desea permitir el protocolo LDAPv2?
<Sí>
<No>
Moving old database directory to /var/backups:
- directory unknown... done.
Creating initial configuration... done.
Creating LDAP directory... done.
Starting OpenLDAP: slapd.
root@servidor-ldap:~# _
Ctrl Derecho

2.3 Creación del directorio LDAP

Una vez instalado y configurado el servicio LDAP nuestra siguiente tarea será crear la estructura de nuestra base de datos LDAP e introducir los datos.

Como elegí como nombre de dominio **iesvalledeljerte.juntaextremadura.es**, la base de mi directorio es: **dc=iesvalledeljerte, dc=juntaextremadura, dc=es**. De esta base colgarán las diferentes unidades organizativas (**ou**).

Como en esta práctica sólo vamos a usar LDAP como servidor de autentificación para sistemas Linux, crearemos dos unidades organizativas:

- **users**: donde almacenaremos los datos de nuestros usuarios.
- **groups**: donde almacenaremos los datos de los grupos.

Puesto que al principio instalamos un paquete de herramientas (ldap-utils) podemos acceder al directorio LDAP mediante la línea de comandos, pero para facilitarnos la tarea de administración del mismo, recomendamos instalar dos herramientas en el equipo del administrador:

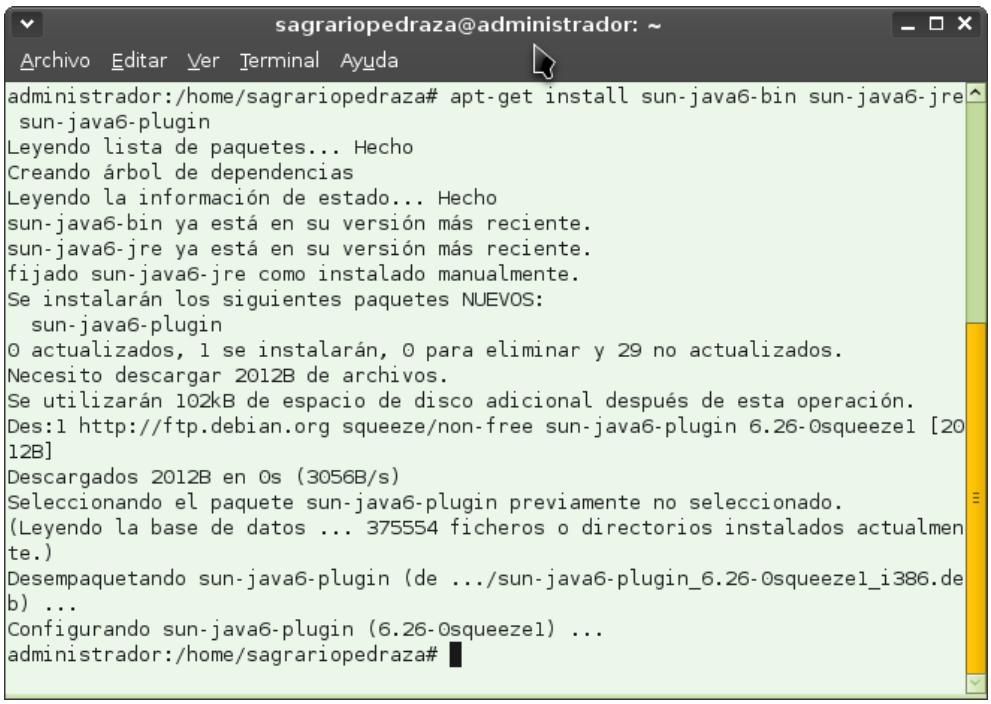
- **Phpldapadmin**: Es una aplicación web que se usa en los IES de Extremadura.
- **JXplorer**: Una aplicación java para admnistrar el directorio LDAP.

Como el el servidor LDAP no tiene entorno gráfico, administraremos LDAP desde nuestro equipo de administrador, instalando estas herramientas.

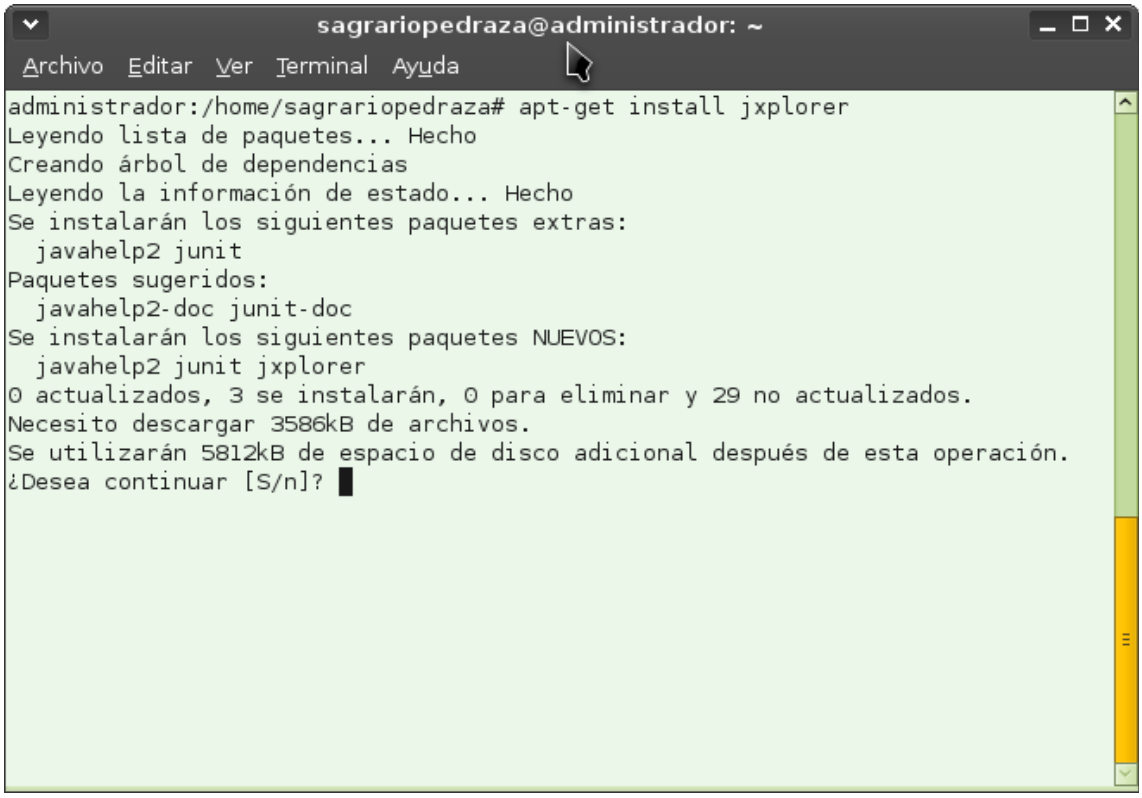
A continuación vamos a crear la estructura de nuestro directorio con Jxplorer, por lo tanto lo primero que haremos será instalarlo.

Instalar Jxplorer.

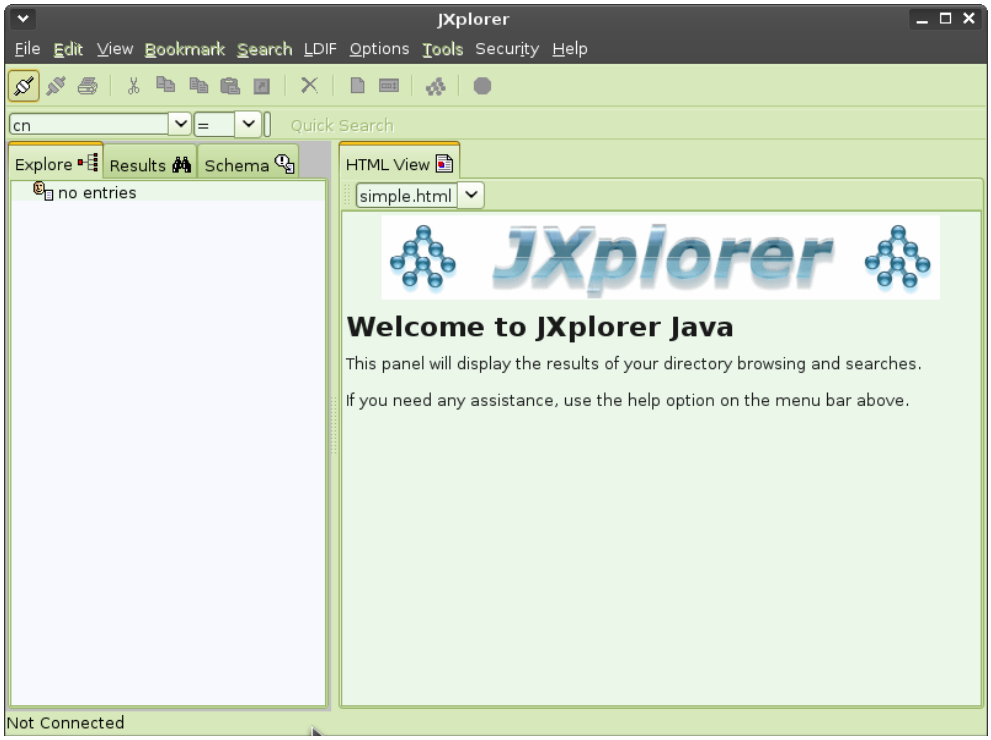
Como es una aplicación java, primero instalamos java en el equipo del administrador:



A continuación instalamos **Jxplorer**:



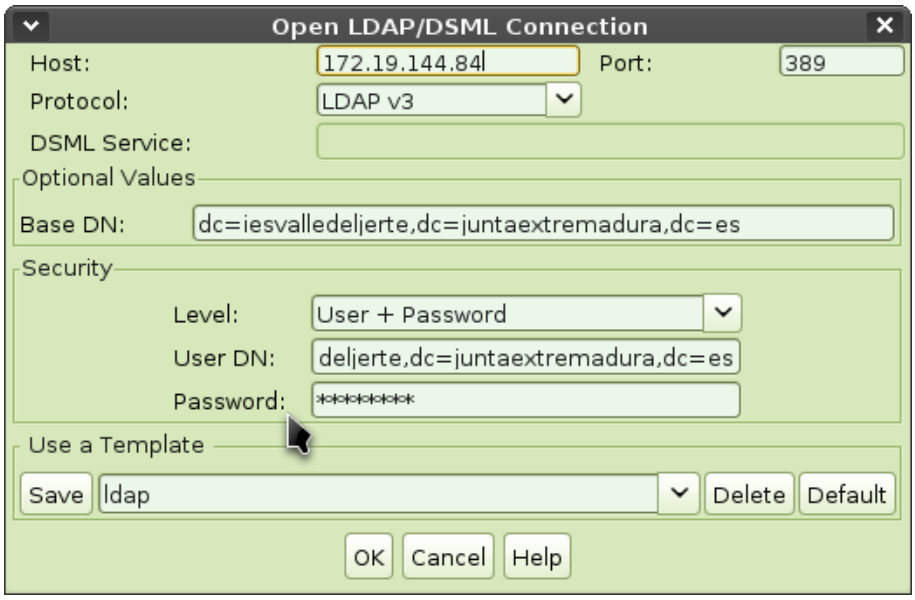
Una vez que termine el proceso de instalación, ya podemos abrir Jxplorer desde el menú o desde un terminal. Veremos la pantalla principal:



Conectar al servidor LDAP

Accederemos al servidor LDAP como administrador para crear la estructura de nuestro directorio. Para lograrlo, tendremos que pulsar el botón de conectar que aparece en la barra de herramientas de Jxplorer:

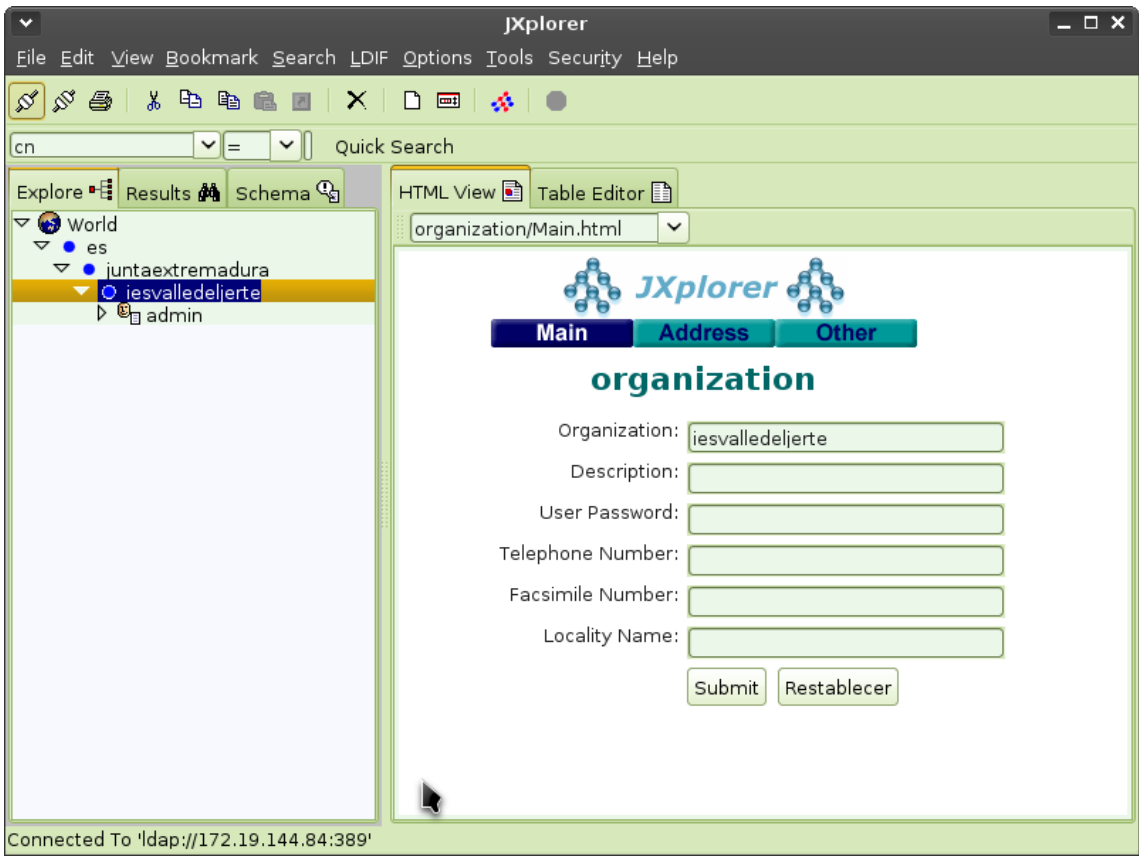
Se nos abrirá un cuadro de diálogo donde introduciremos los datos de acceso:



Resumiendo:

- Dirección IP del servidor de LDAP En mi práctica: 172.19.144.84.
- Protocolo del servidor: El que elegimos al instalarlo: LDAPv3.
- Base del directorio: iesvalledeljerte.juntaextremadura.es
- Nombre usuario administrador: cn=admin,dc=iesvalledeljerte,dc=juntaextremadura,dc=es
- Contraseña: La del usuario administrador.

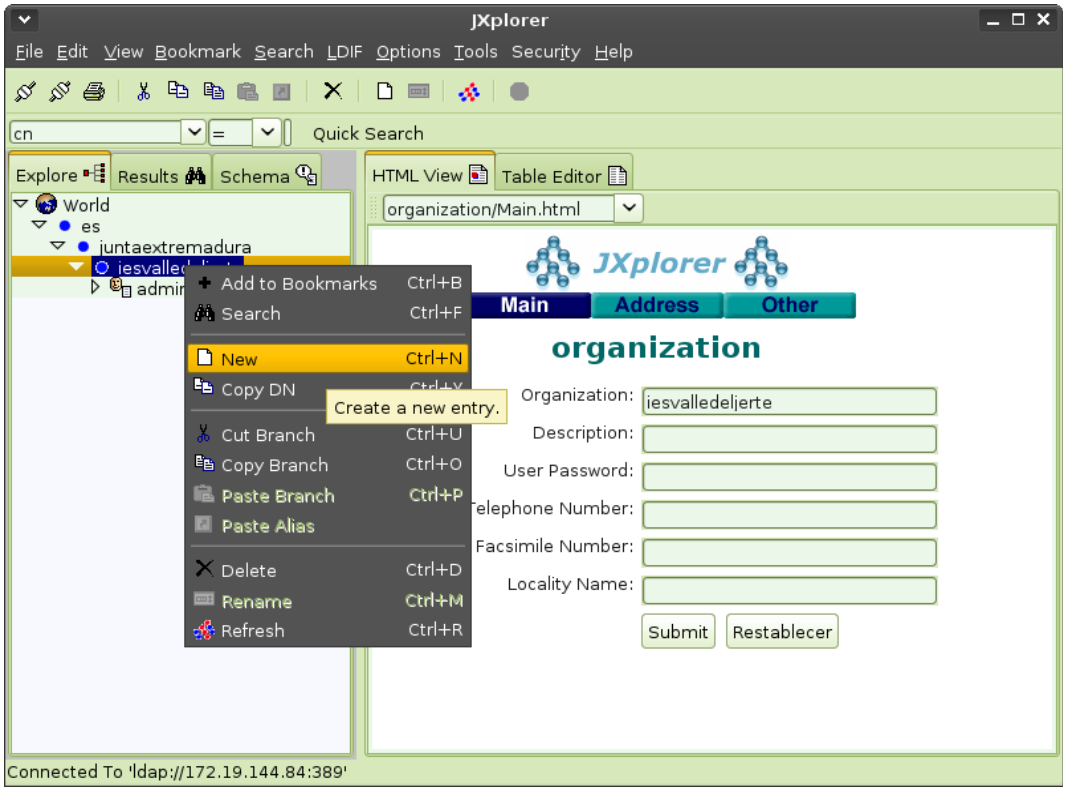
Pulsamos el botón OK. JXplorer conectará con el servidor LDAP y nos mostrará el directorio:



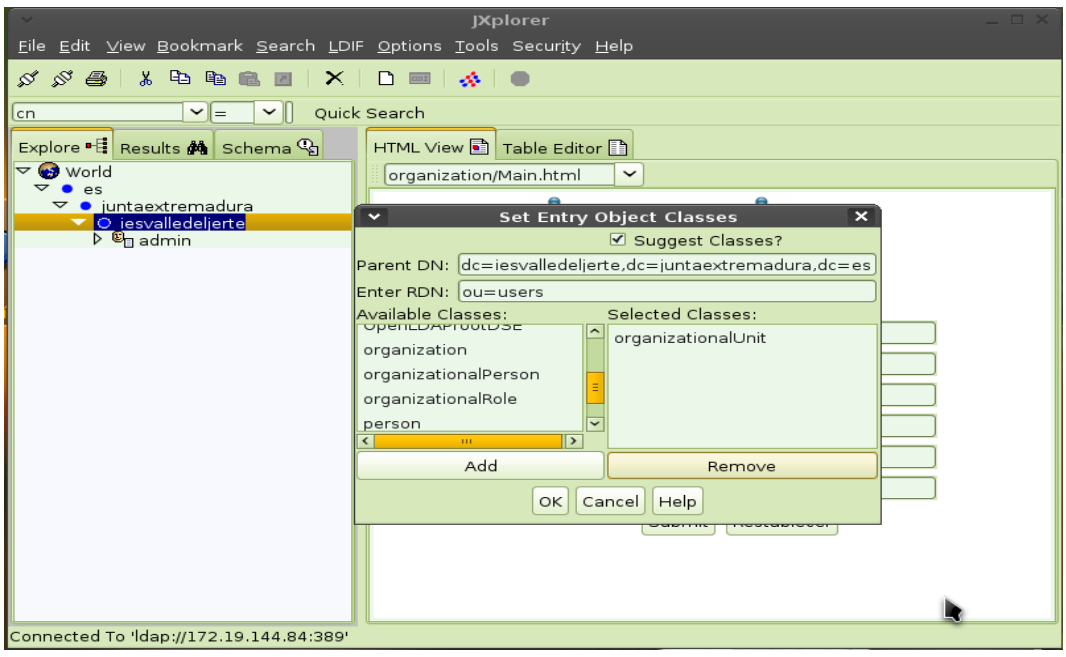
Como podemos ver en la imagen anterior, tan sólo tenemos creado el directorio base del que cuelga el usuario administrador: **admin**.

Creación de las unidades organizativas

Primero crearemos la unidad organizativa **users**, para lo que haremos clic con el botón derecho del ratón sobre **iesvalledeljerte**. Se nos abre un menú de contexto donde elegimos "**New**":

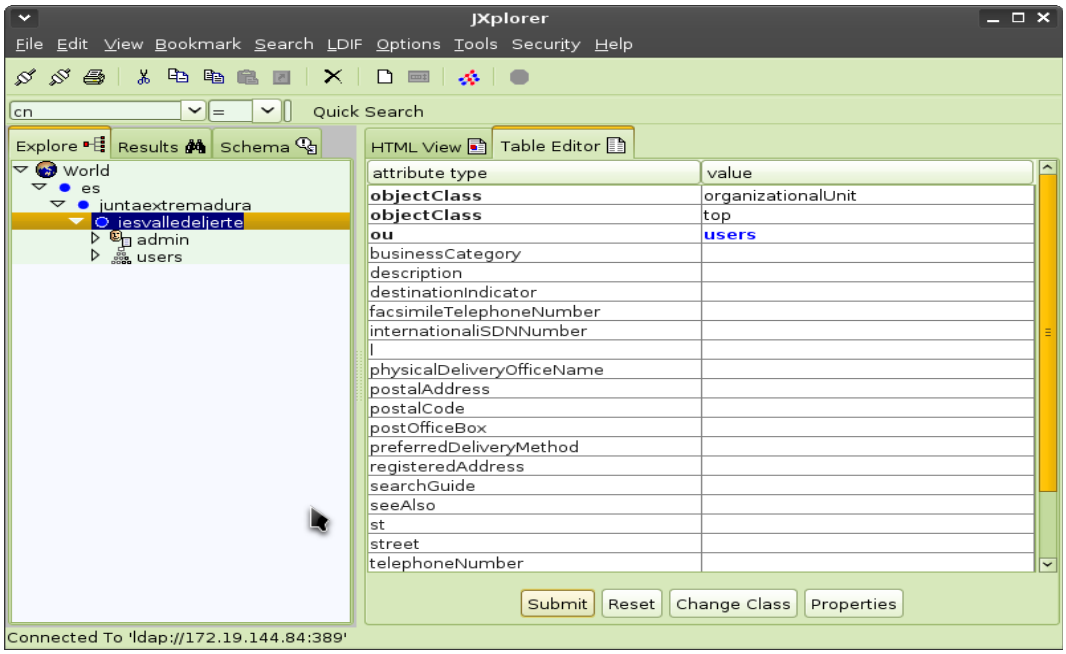


Introducimos los datos para crear la unidad organizativa users:

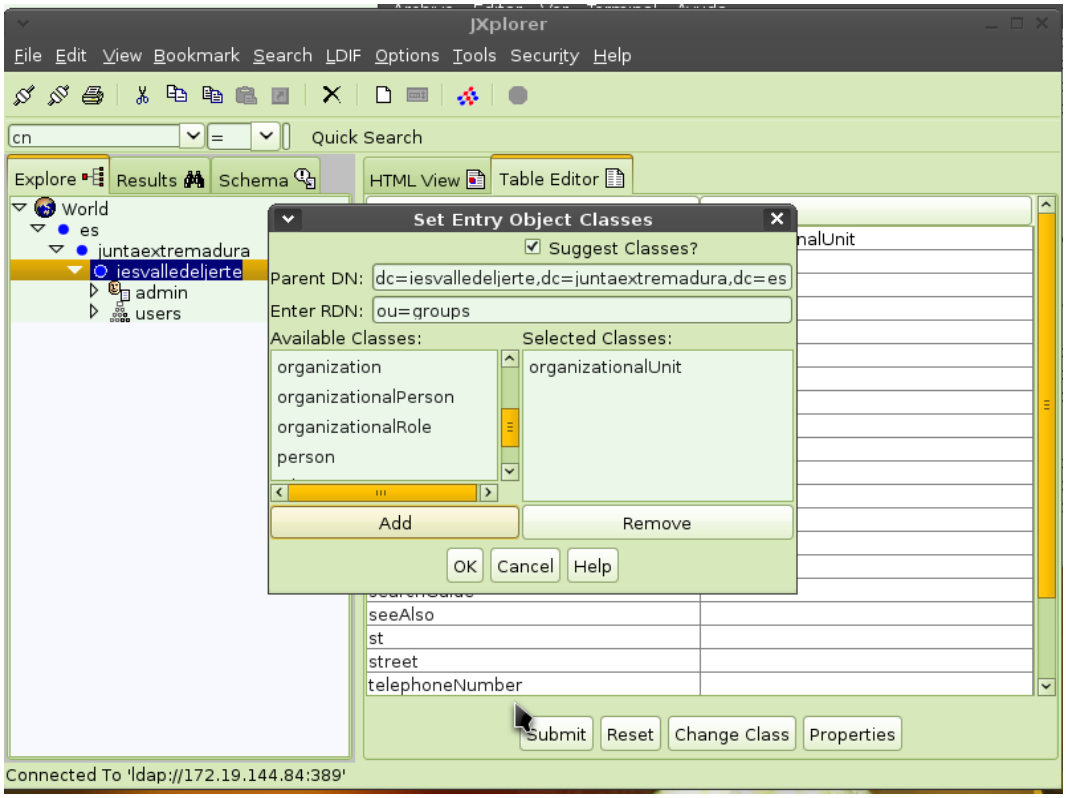


En el cuadro de texto RDN introducimos: **ou=users**. Como lo que estamos creando es una unidad organizacional (**organizationalUnit**), en “Available Classes” seleccionamos “organizationalUnit” y pulsamos el botón “Add”. Las otras dos clases que aparecen por defecto (organizationalRole y simpleSecurityObject) las quitamos seleccionándolas y pulsando el botón “Remove” porque no las necesitamos.

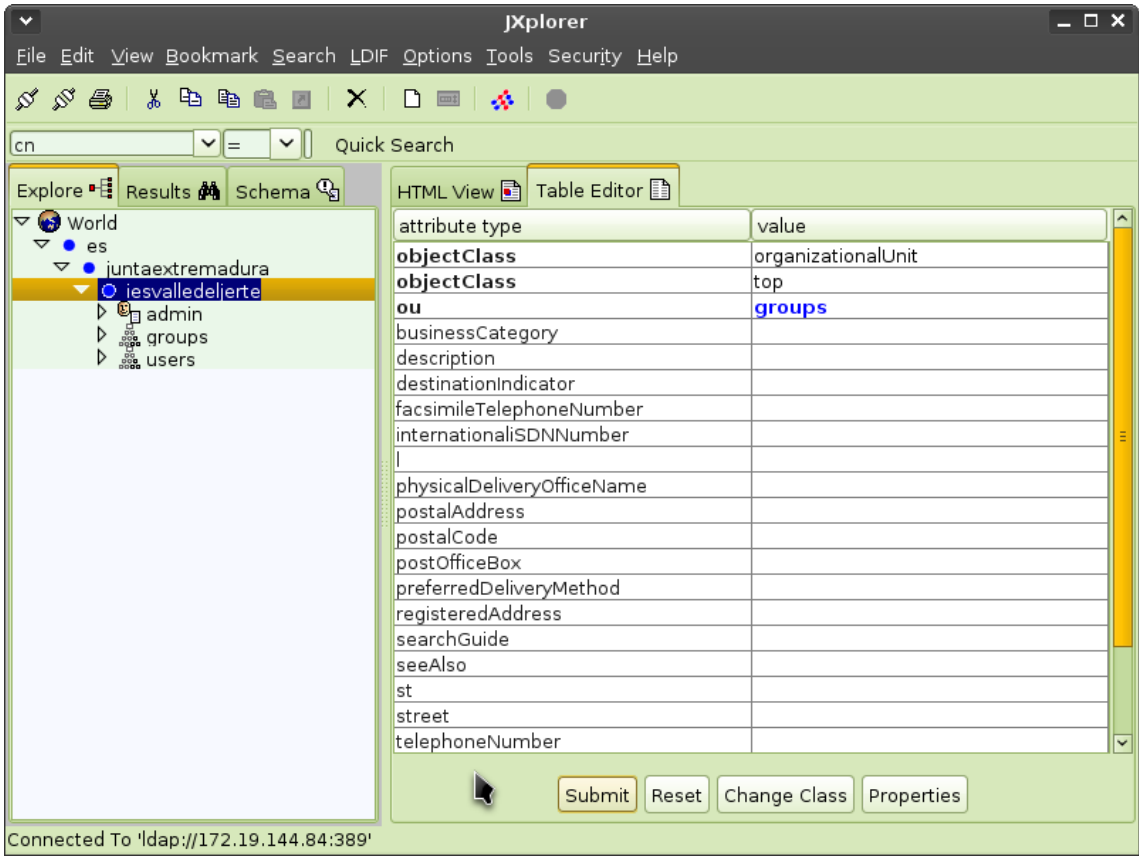
Una vez hecho ésto, pulsamos el botón OK y veremos que la unidad organizacional users se ha creado:



Del mismo modo, creamos la unidad organizacional **groups**:



Comprobamos que se ha creado:

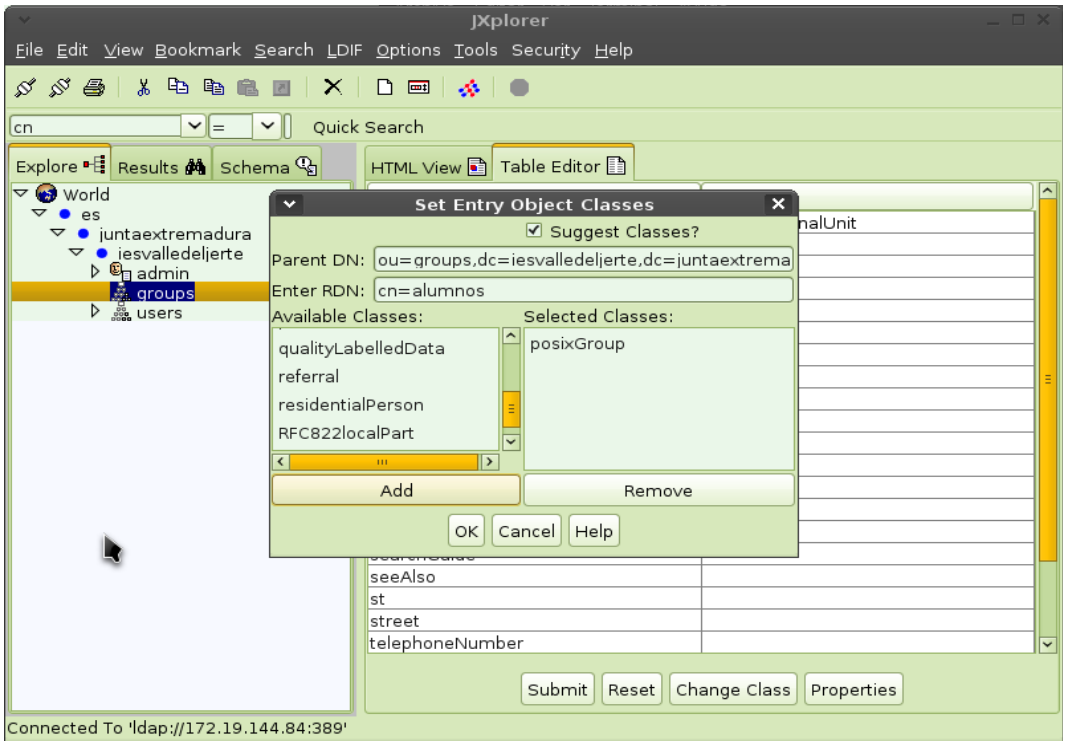


Creación de usuarios y grupos

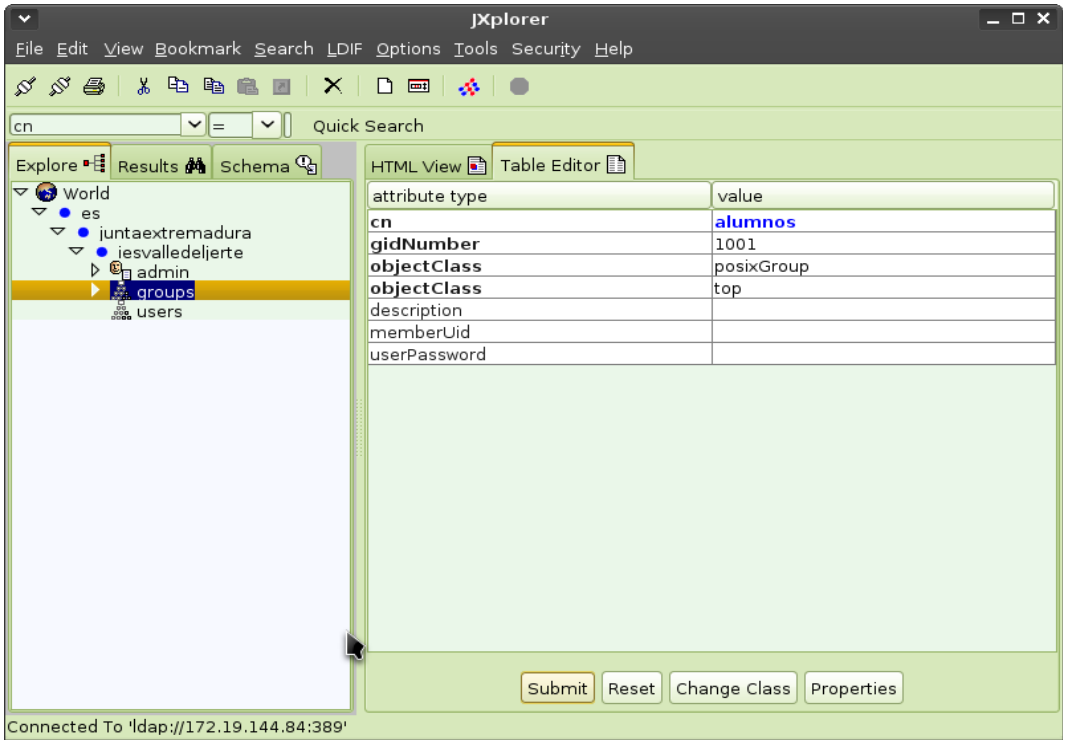
A continuación vamos a crear los usuarios, los grupos y asignamos los usuarios a sus grupos.

Primero creamos los grupos: • alumnos (gid=1001). • Profesores (gid=1002).	Después creamos los usuarios: • sagrario (uid=1001) • adrian (uid=1002) • natalia (uid=1003) • esteban (uid=1004)

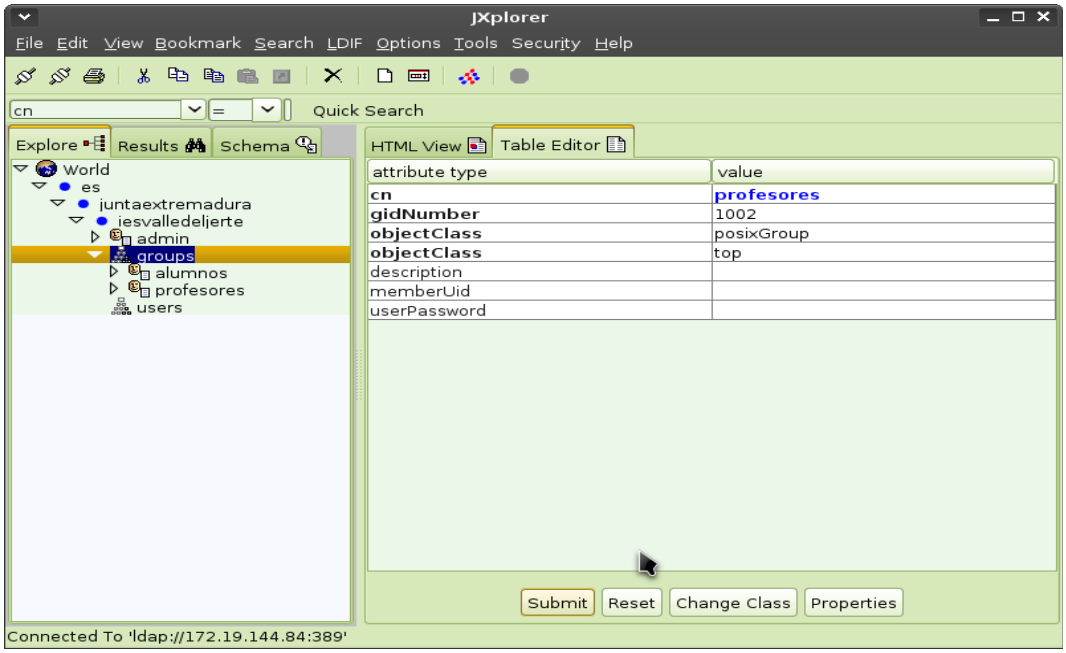
Pulsamos con el botón derecho del ratón sobre la entrada groups y en la casillla **RDN** escribimos "**cn=alumnos**" para crear el grupo de alumnos. Seleccionamos sólo la clase **posixGroup** en "Available Classes" y pulsamos el botón "Add" para añadirla. A continuación pulsamos el botón **OK**.



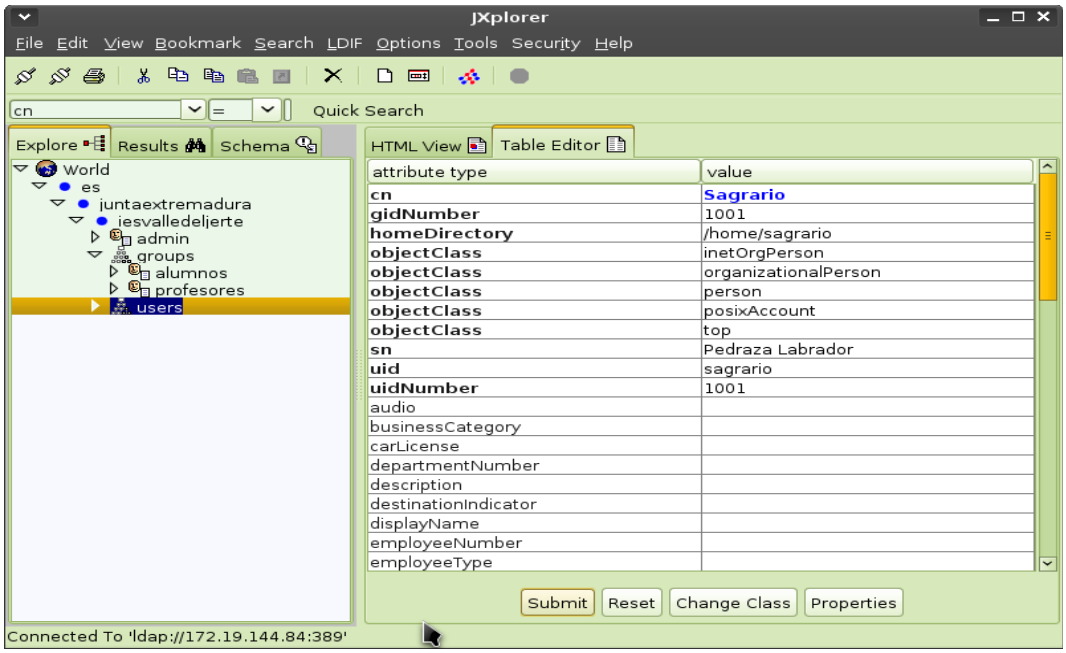
Pulsamos el botón "Submit" y comprobamos que el grupo se ha creado.



Del mismo modo, creamos el grupo de profesores:



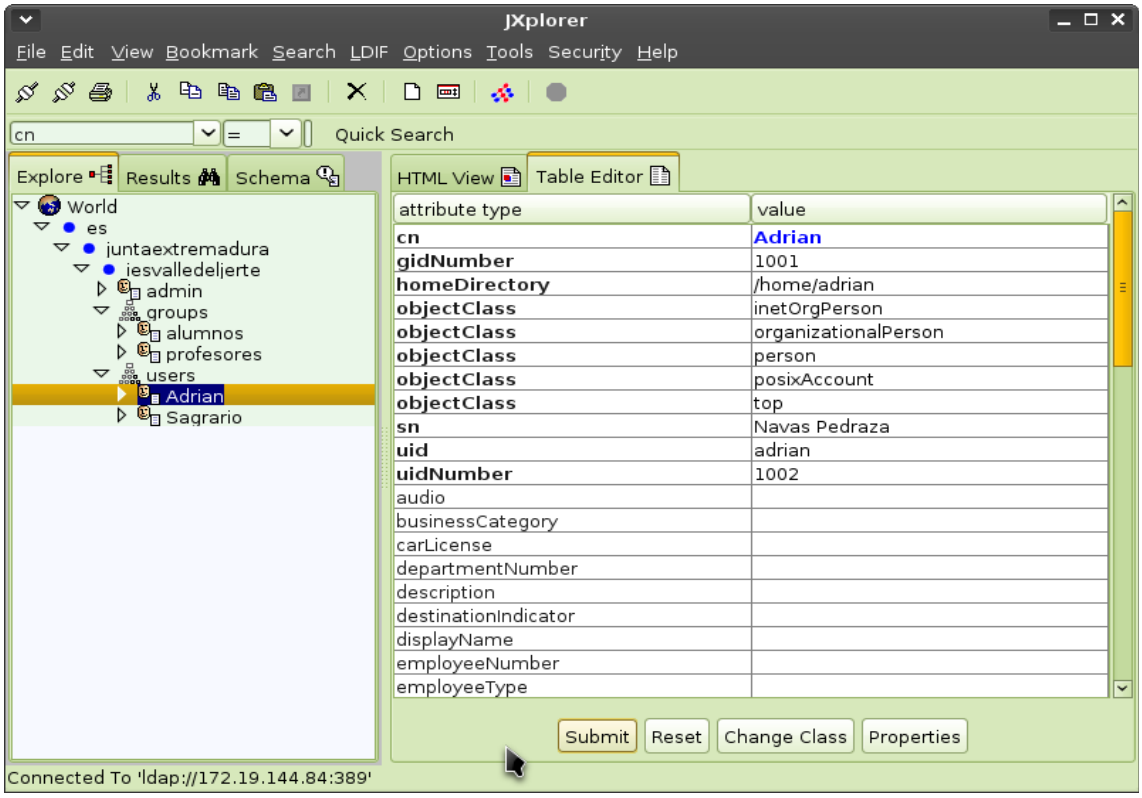
Una vez creados los grupos, pasamos a crear los usuarios. Para ello, hacemos clic con el botón derecho sobre la unidad organizativa **users** e igual que antes, hacemos clic en "New". En "Available Classes" seleccionamos los tipos "posixAccount", "person" e "inetOrgPerson" para disponer de los campos de datos que nos ofrece cada uno de los tipos:

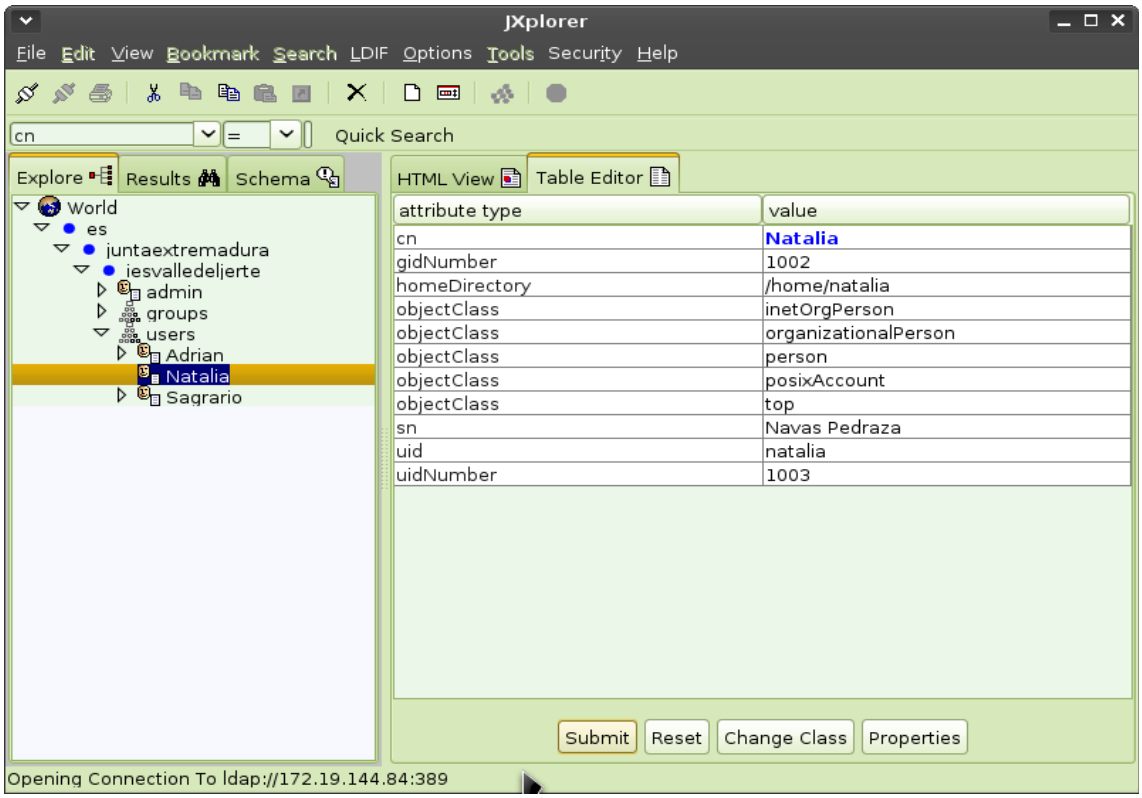


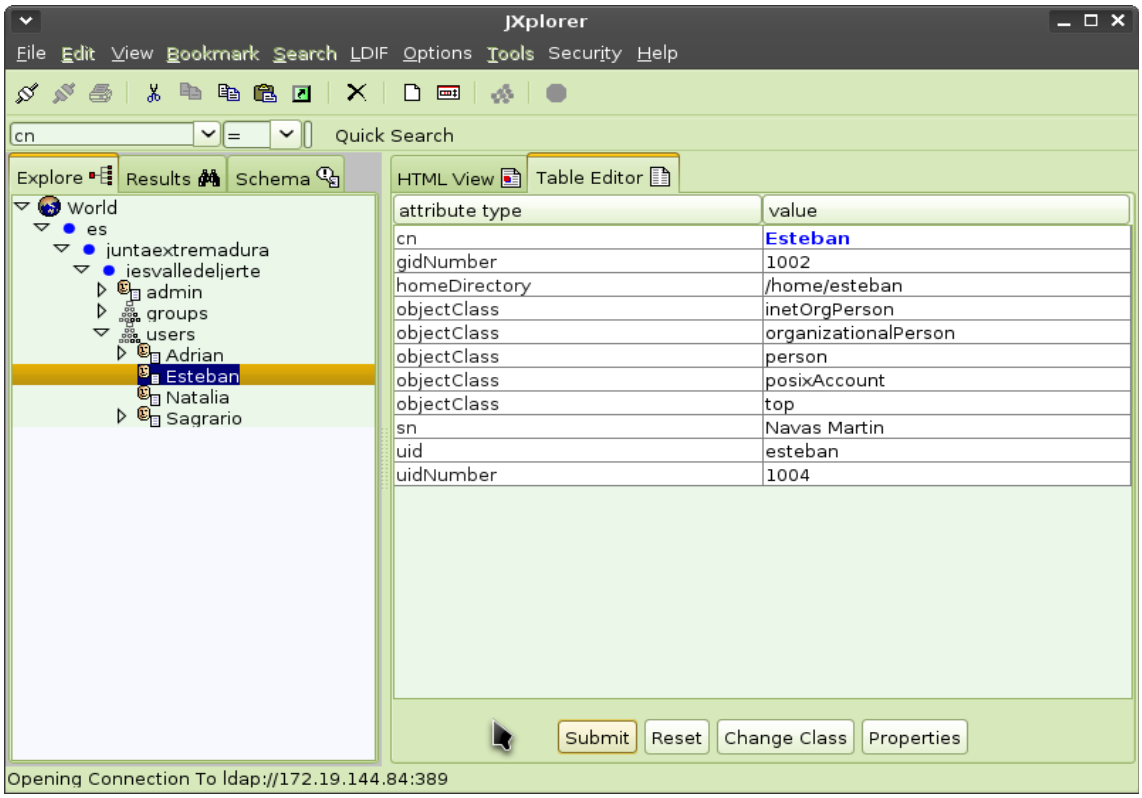
Al seleccionar el tipo "person" disponemos de campos como el nombre, apellidos, etc...

Al seleccionar el tipo "inetOrgPerson" dispondremos de campos como el e-mail, etc...

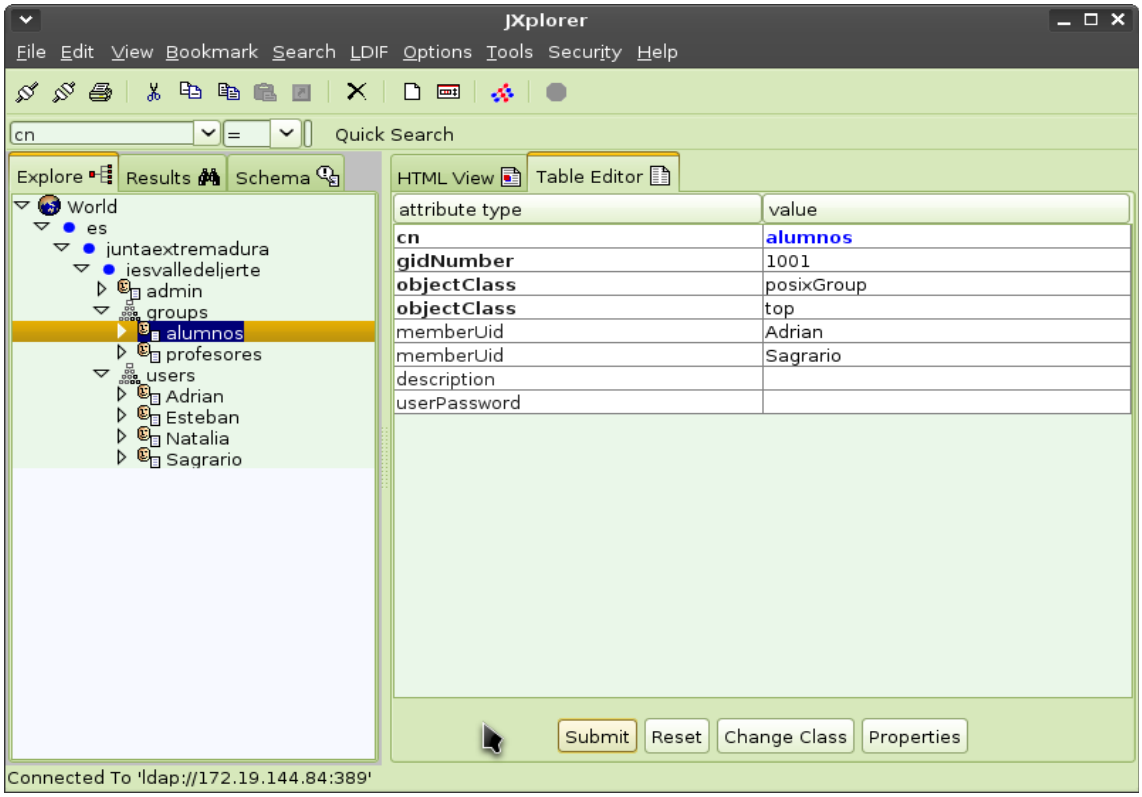
Del mismo modo añadimos más usuarios:



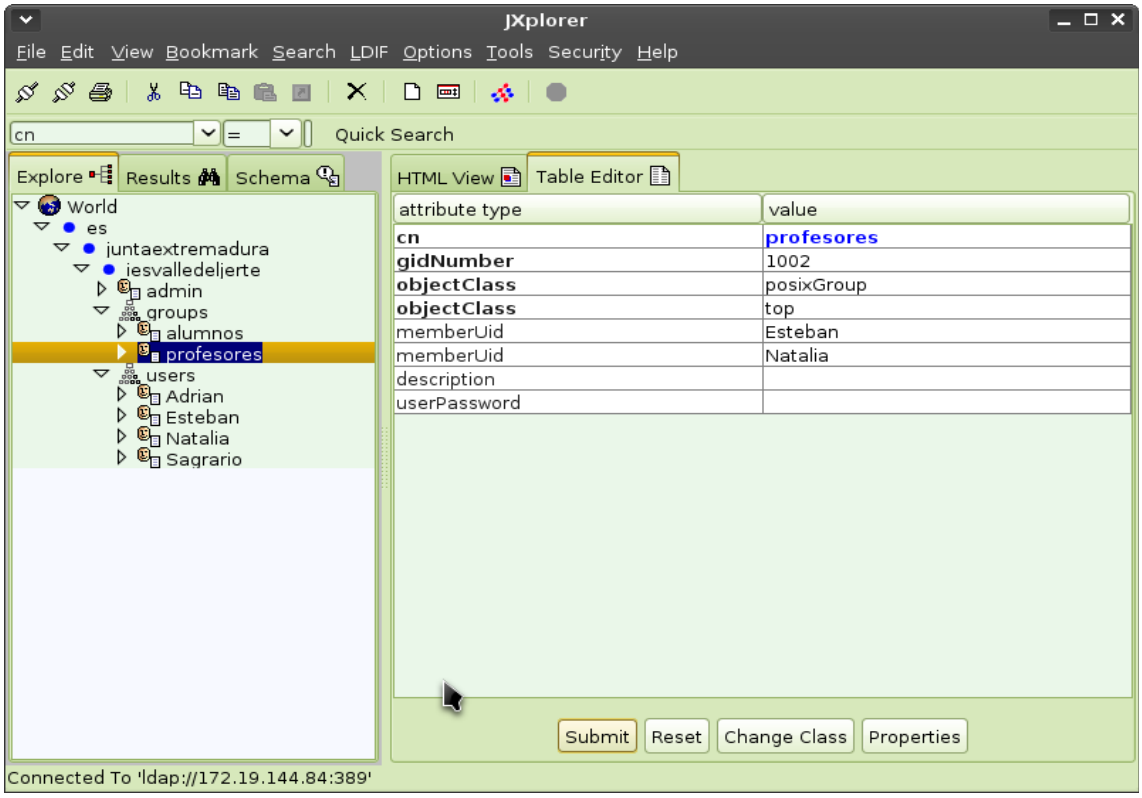




A continuación asignamos los usuarios Adrian y Sagrario al grupo de alumnos editando la unidad organizacional “alumnos” y en la pestaña “Table Editor” especificando sus nombres de usuario en “memberUid”. Habrá un campo “memberUid” por cada usuario del grupo:

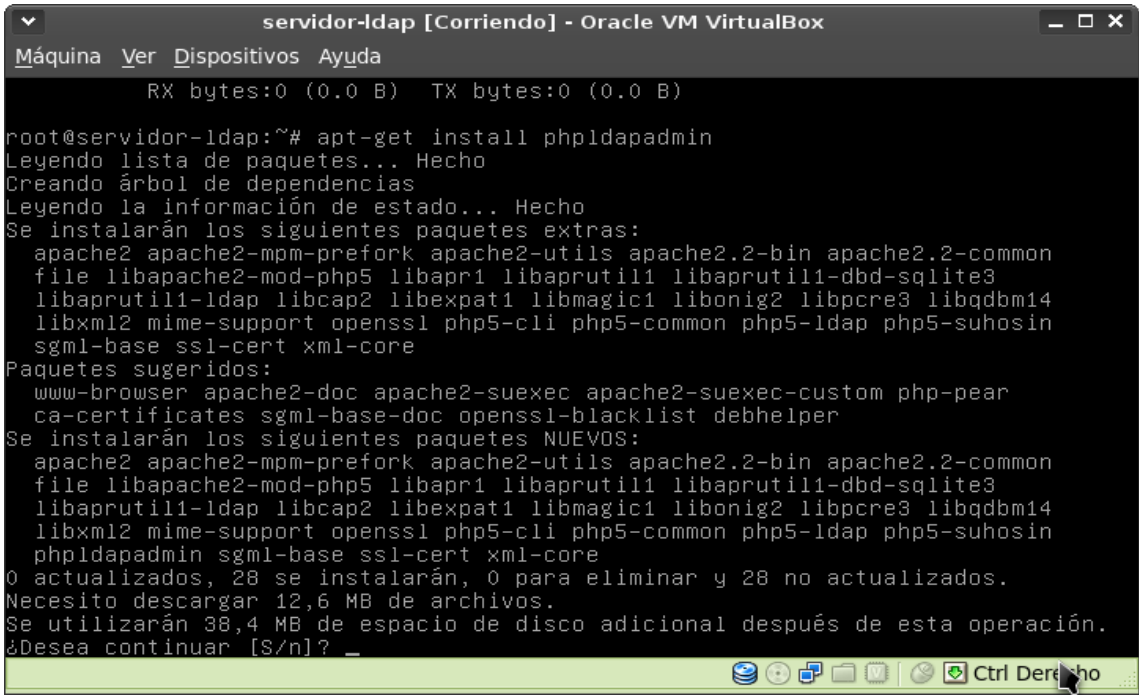


Del mismo modo, asignamos los usuarios Natalia y Esteban al grupo profesores:



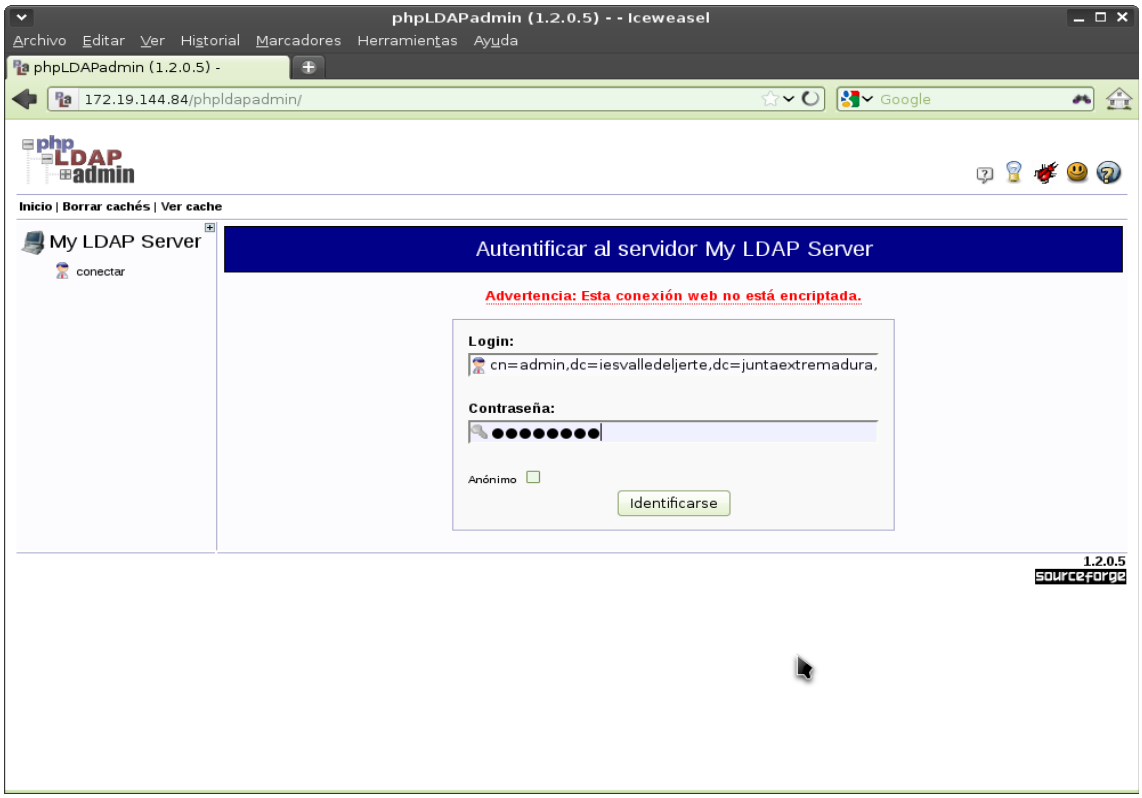
Instalación de phpldapadmin

Hemos visto cómo modificar el directorio ldap con Jxplorer. Si quisiéramos usar phpldapadmin, tan sólo tendríamos que instalarlo:



El archivo de configuración de ldap es /etc/phpldapadmin.conf.

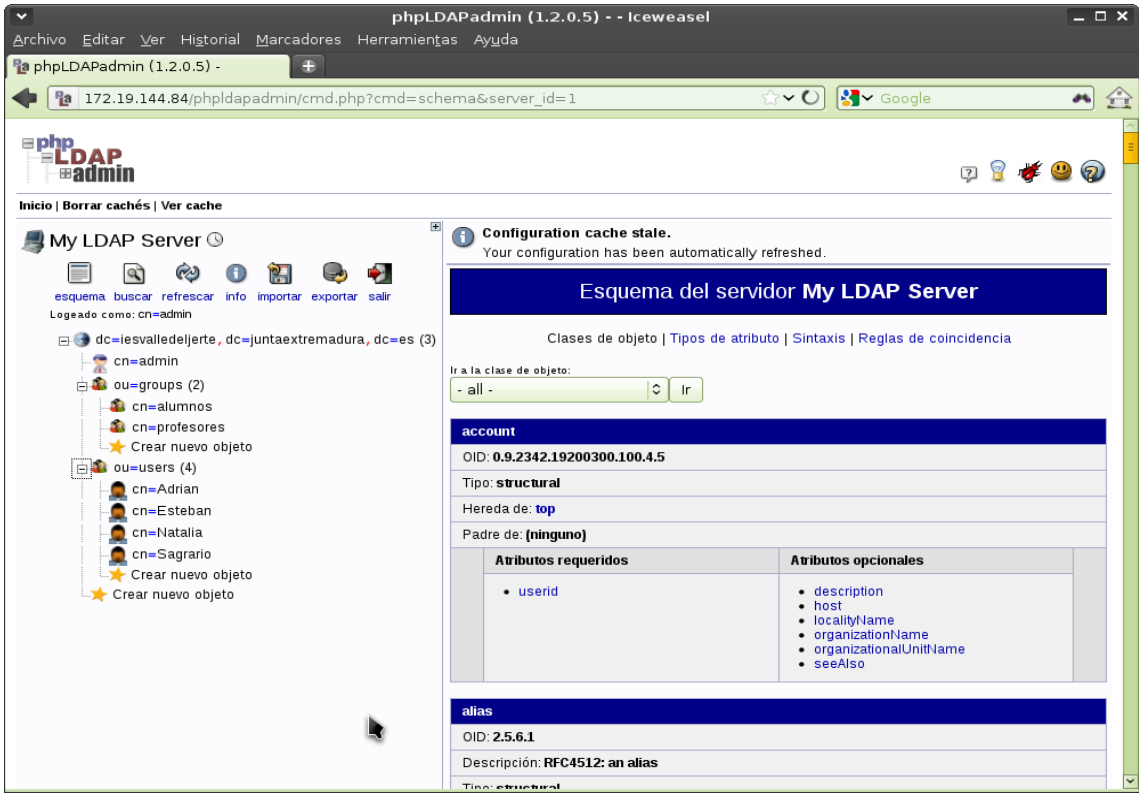
Ésta es la pantalla de acceso de phpldapadmin:



Para entrar tendremos que introducir el usuario administrador y su contraseña:

Login: **cn=admin,dc=iesvalledeljerte,dc=juntaextremadura,dc=es**

Una vez dentro, veremos la estructura de nuestro directorio ldap del mismo modo que la veíamos con JXplorer:



3. Instalación de un cliente LDAP.

En un sistema Linux, los usuarios se autentifican con los datos almacenados en los ficheros:

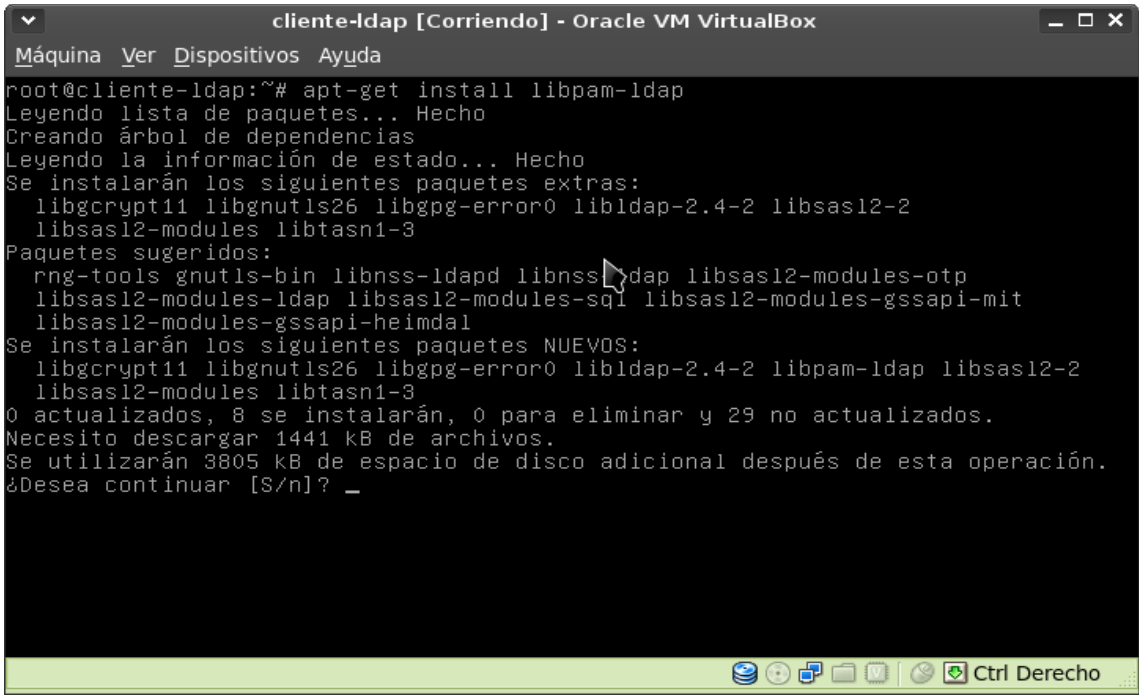
- /etc/passwd
- /etc/group
- /etc/shadow

Si queremos que los usuarios de un equipo cliente puedan acceder con los datos almacenados en un servidor ldap, básicamente habrá que hacer lo siguiente:

- Instalar y configurar la librería libpam-ldap.
- Instalar y configurar la librería libnss-ldap.
- Configurar nsswitch.conf.

3.1 Instalar y configurar la librería libpam-ldap

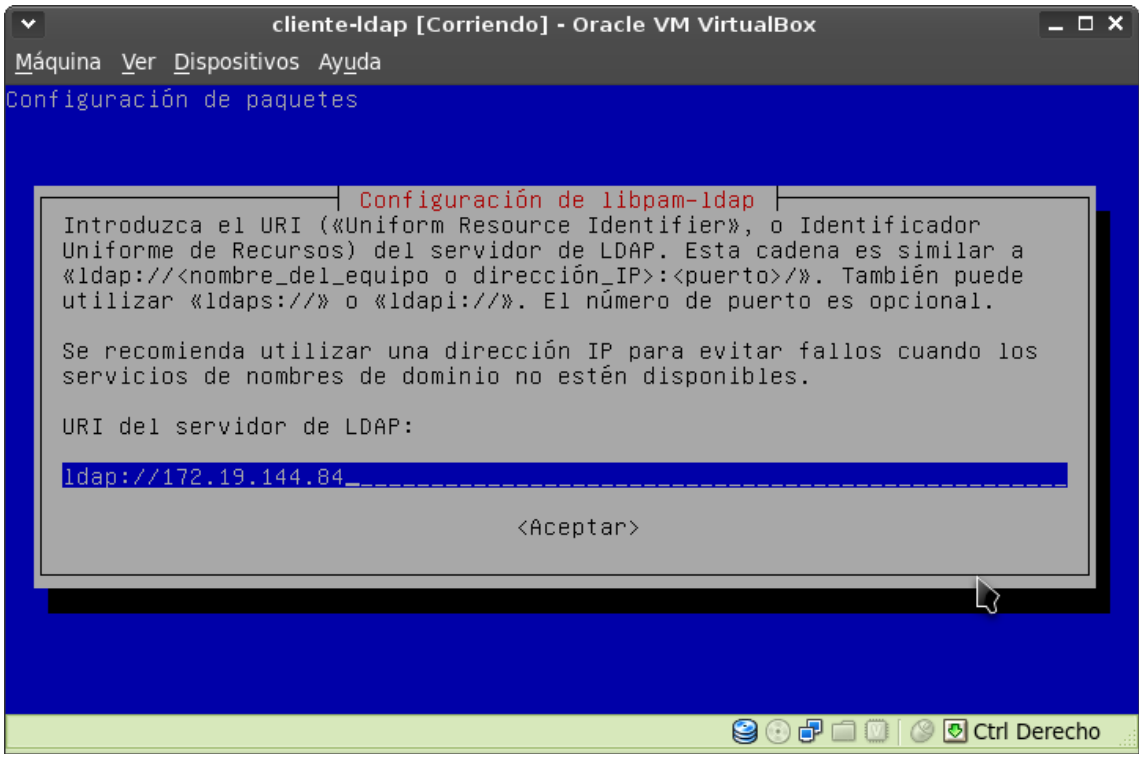
En Debian es sencillo instalar esta librería:



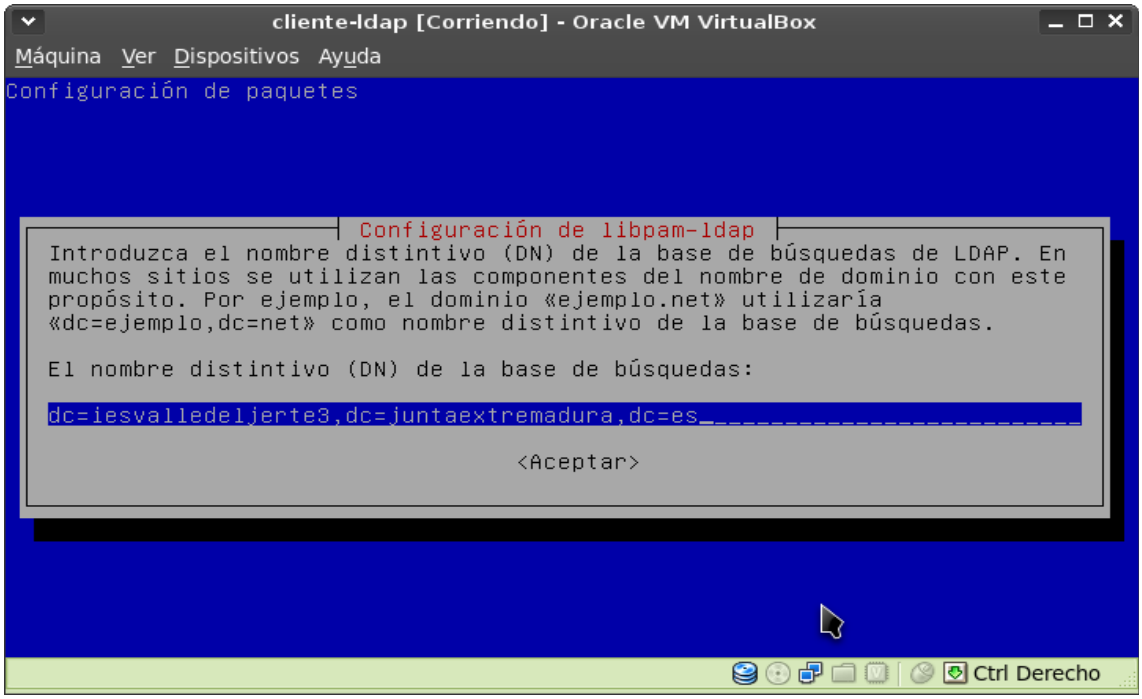
Pulsamos Enter para que comience la instalación. Una vez instalado, se inicia automáticamente un asistente de configuración que nos irá haciendo preguntas para configurarla.

En cualquier momento podemos reconfigurar libpam-ldap con tan sólo ejecutar: dpkg-reconfigure libpam-ldap.

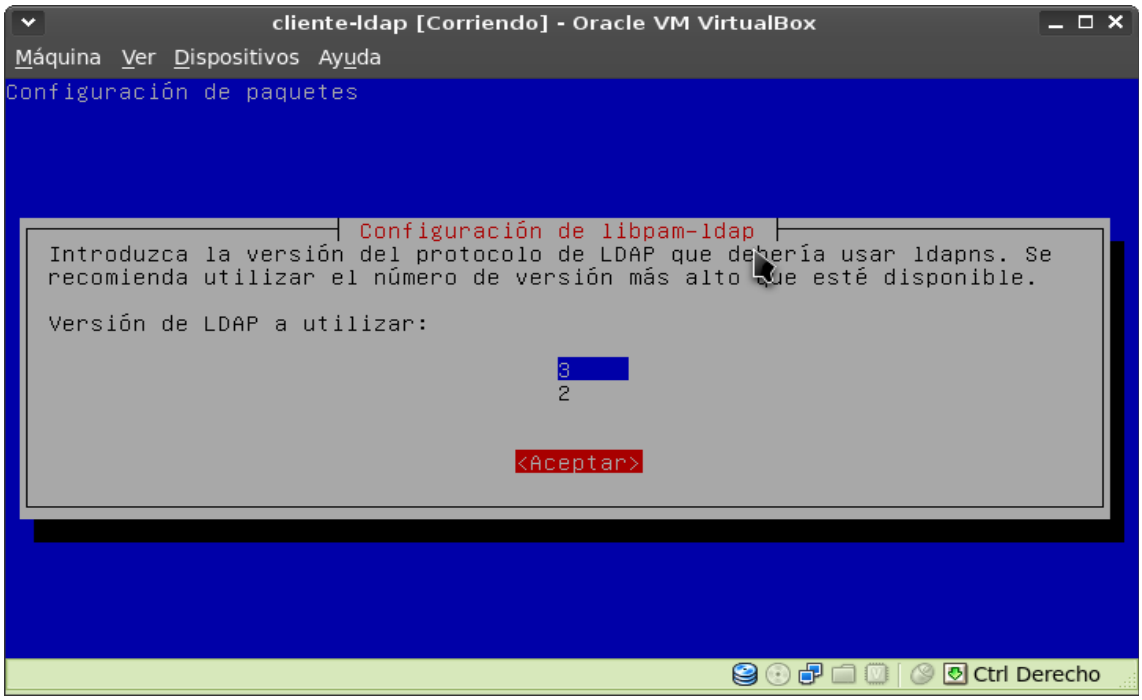
Lo primero que nos preguntará es el URI del servidor ldap. Introduciremos la IP de nuestro servidor ldap de la siguiente manera: **ldap://172.19.144.84**:



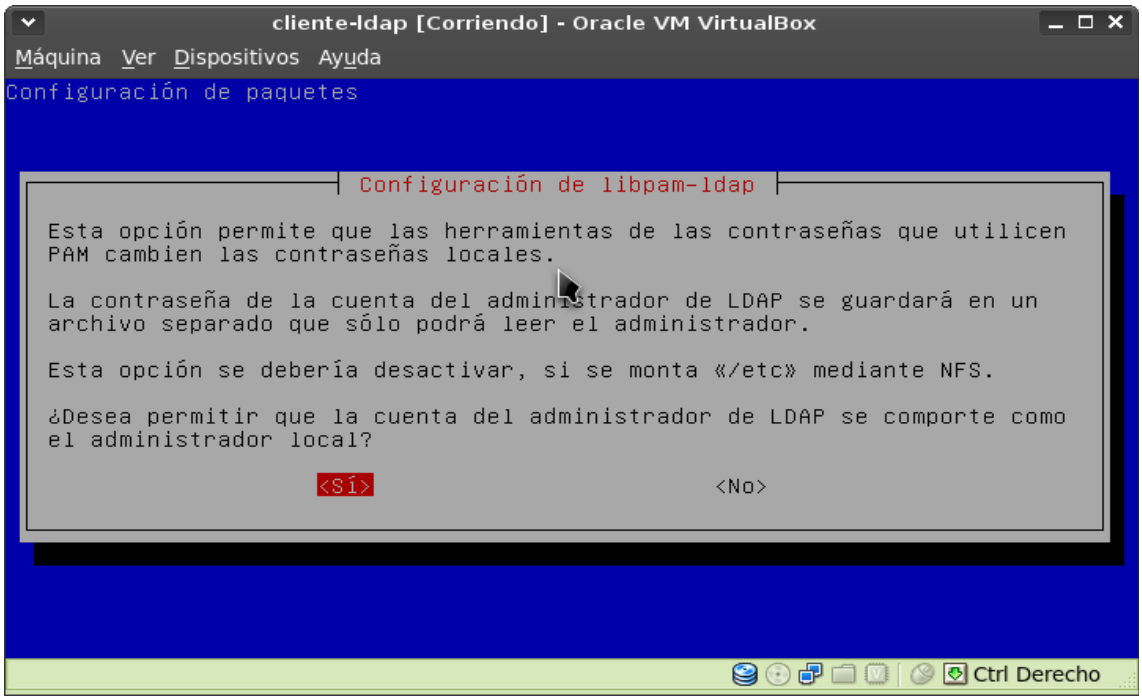
A continuación nos pedirá que introduzcamos el nombre de nuestro dominio base. Introducimos el nombre que elegimos cuando instalamos el servidor ldap:



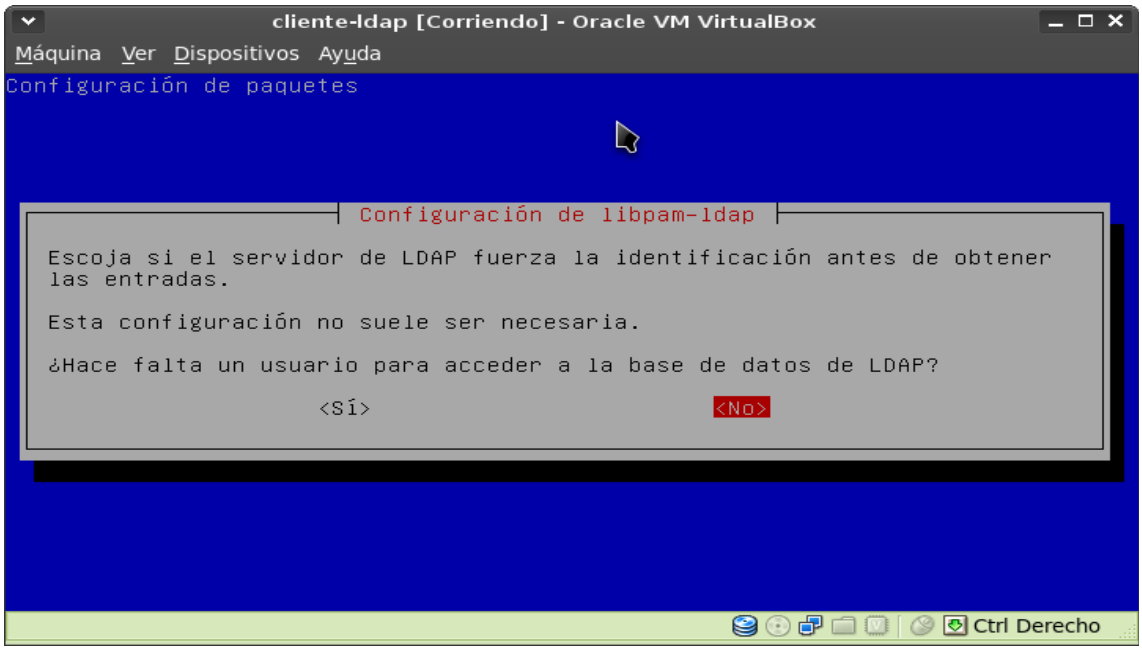
Ahora nos preguntará qué versión de LDAP vamos a utilizar. Recordemos que elegimos usar LDAPv3 en el servidor:



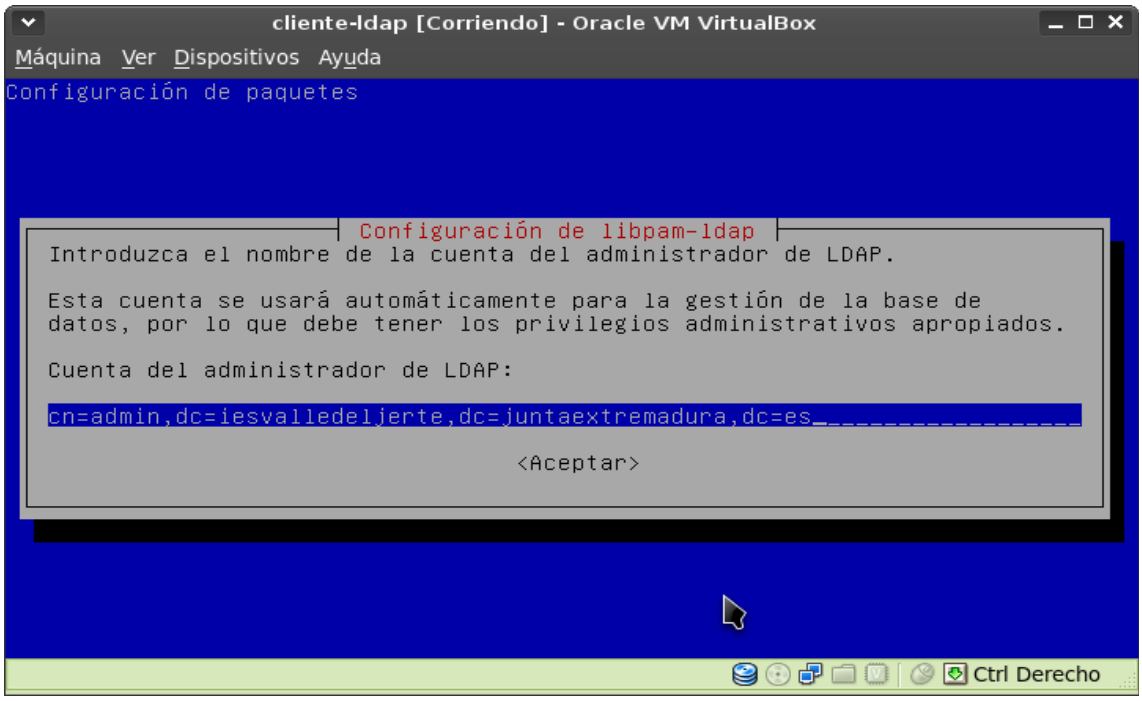
En el siguiente paso nos pregunta si necesitamos permitimos que la cuenta del admnistrador de LDAP se comporte como el administrador local. Le decimos que sí.



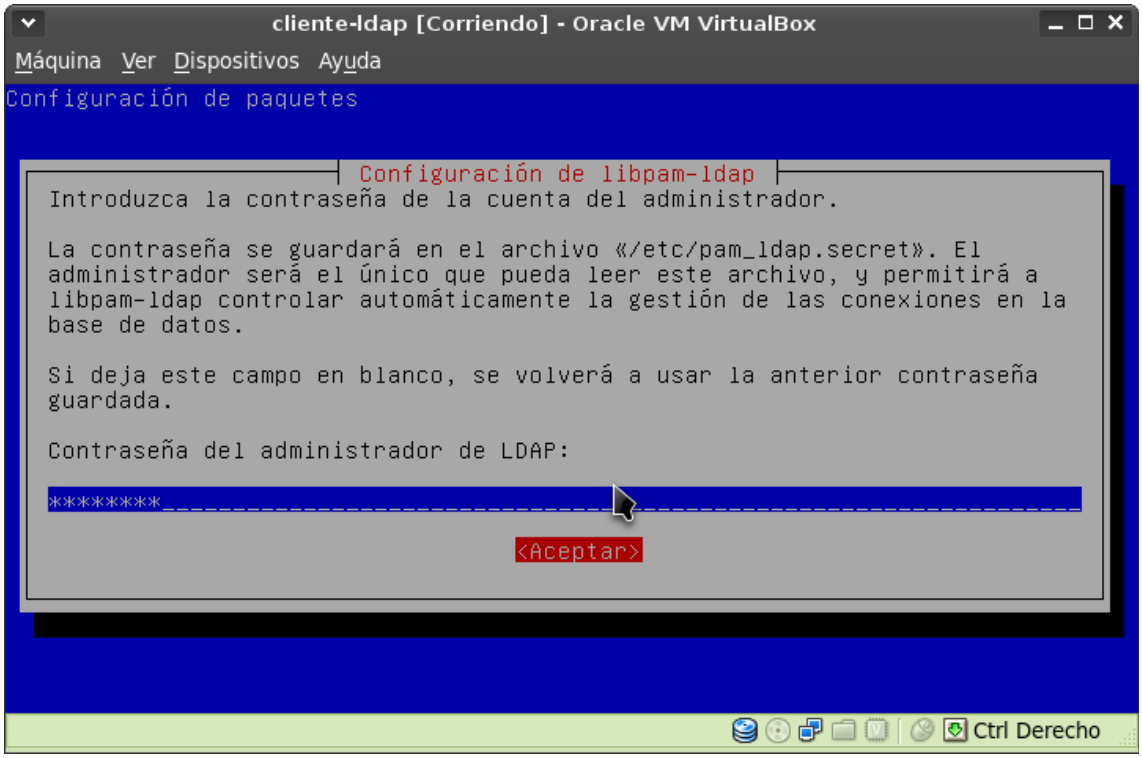
En la siguiente ventana respondemos que no se necesita usuario para acceder a la base de datos de ldap.



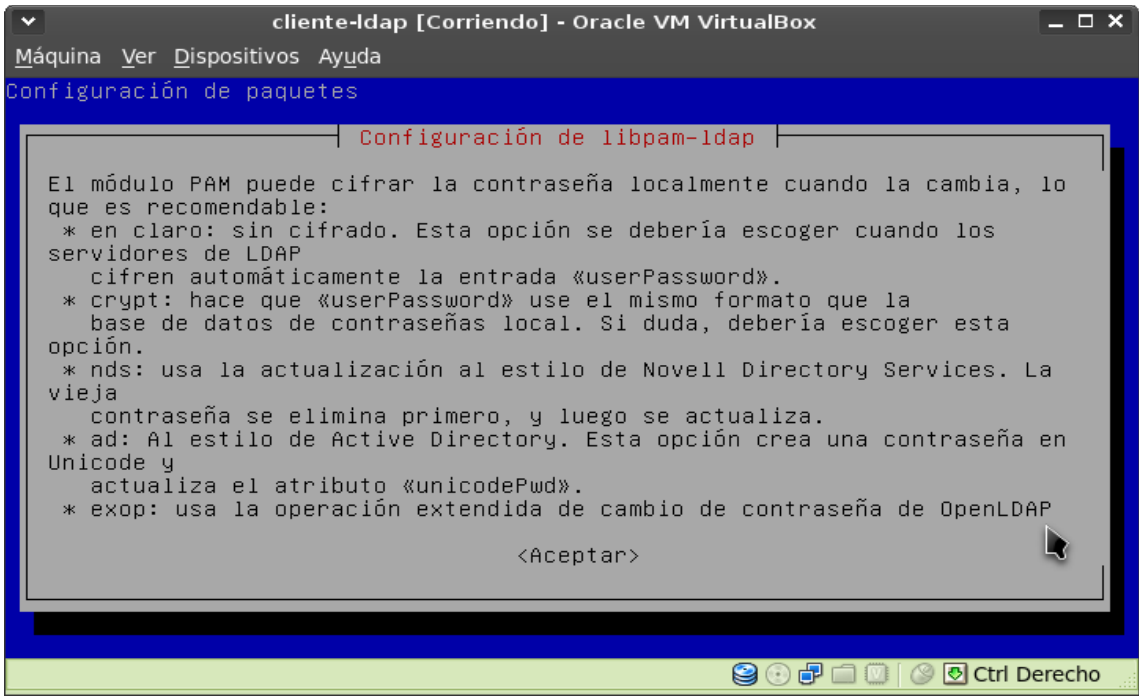
Nos pedirá que introduzcamos la cuenta del administrador de ldap. Introduciremos la que creamos en el servidor de ldap: **cn=admin,dc=iesvalledeljerte,dc=instituto,dc=extremadura,dc=es**



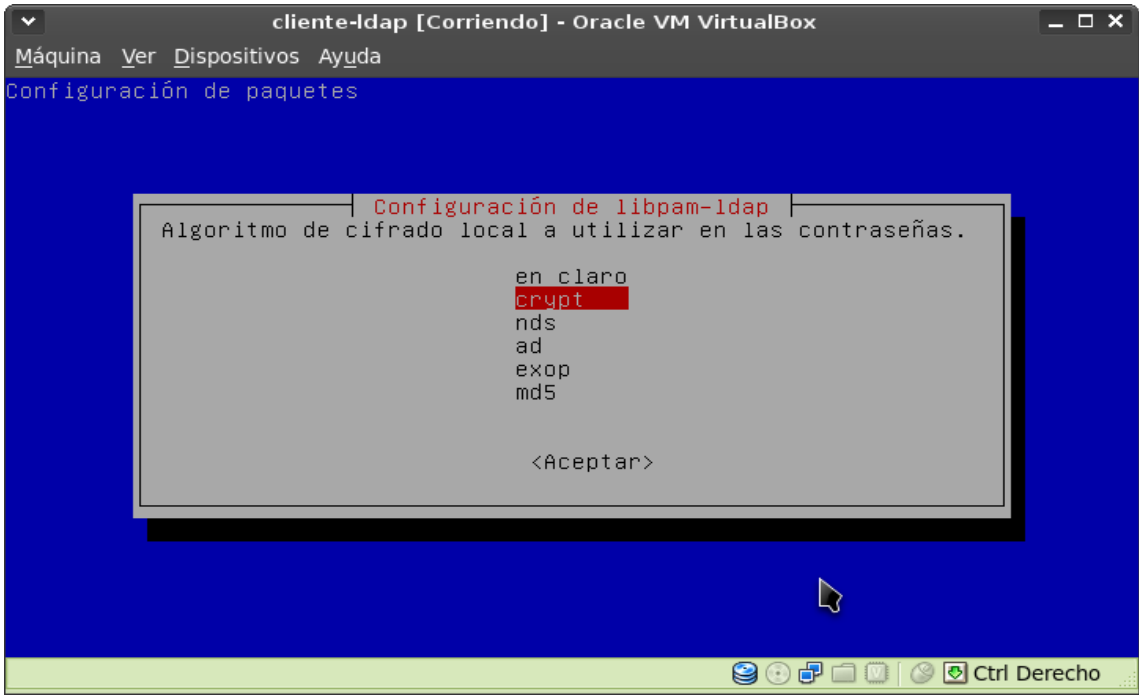
Nos pedirá que introduzcamos la contraseña del administrador de ldap. La introducimos:



En la siguiente ventana nos informa de los posibles modos para cifrar la contraseña:

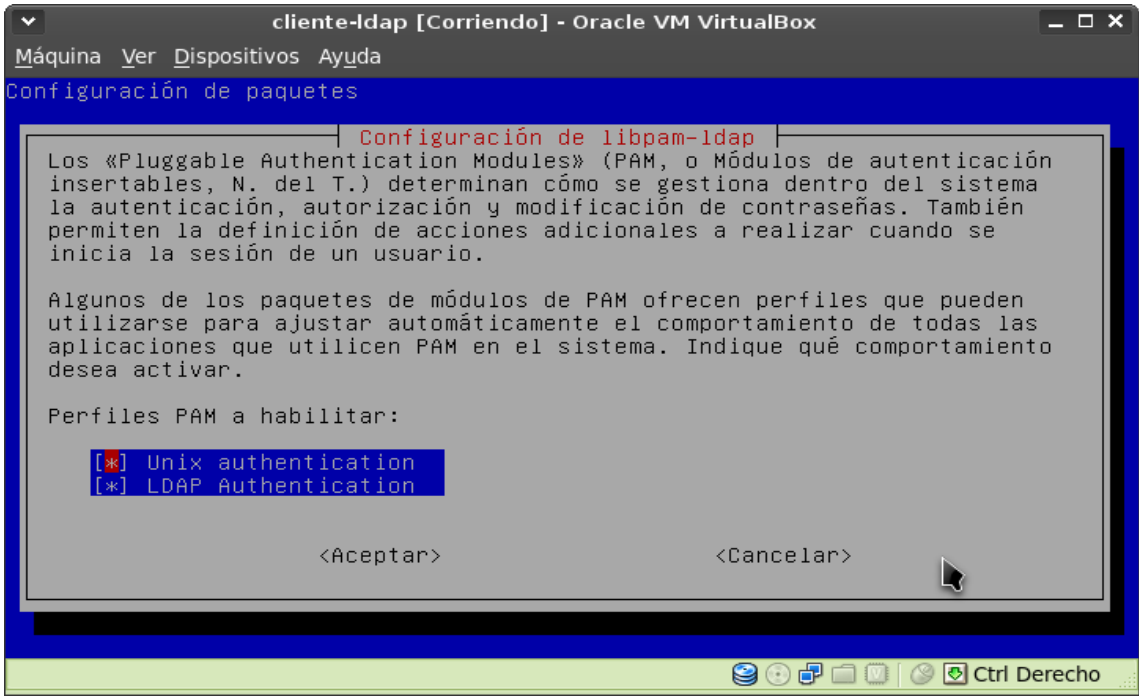


Elegimos crypt:



Los módulos PAM nos permiten configurar cómo se va a realizar la autentficación en el sistema. Como queremos permitir tanto la autentificación de los usuarios almacenados localmente en el equipo, como por ejemplo root, como la autentificación de los usuarios almacenados en ldap, marcaremos ambas opciones:

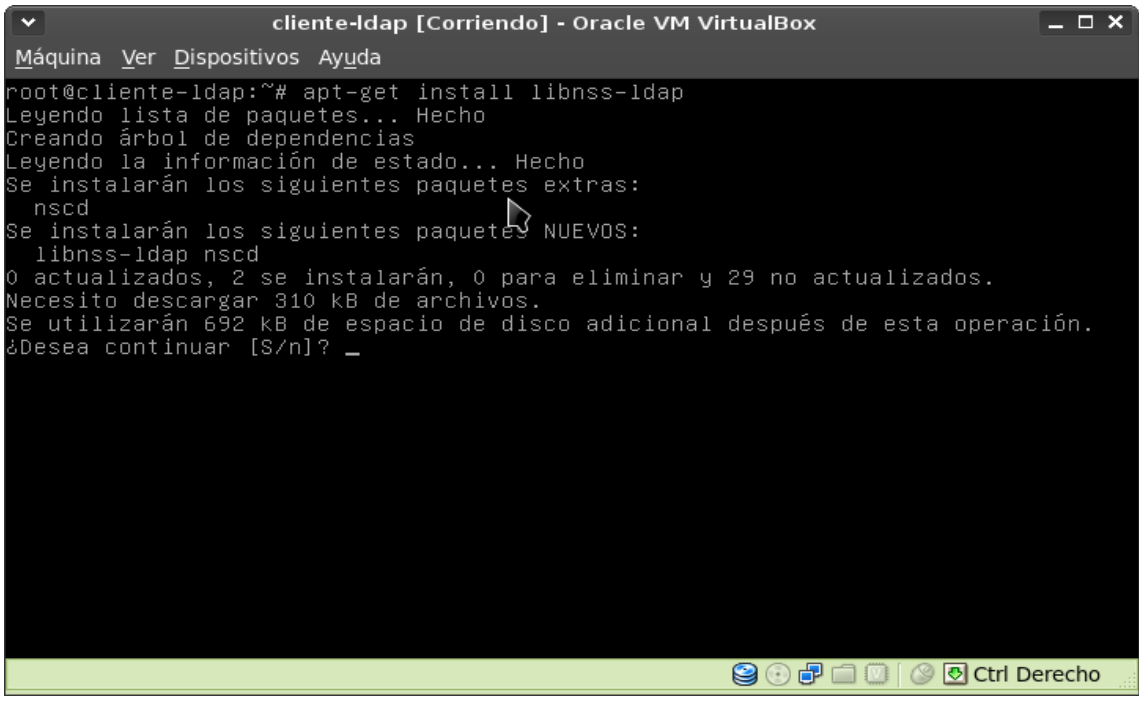
- Unix Authentication.
- LDAP Auhentication.



De este modo, se configurará automáticamente PAM para permitir ambos sistemas de autentificación. Pulsamos “Aceptar” y habremos terminado de configurar libpam-ldap.

3.2 Instalar y configurar la librería libnss-ldap

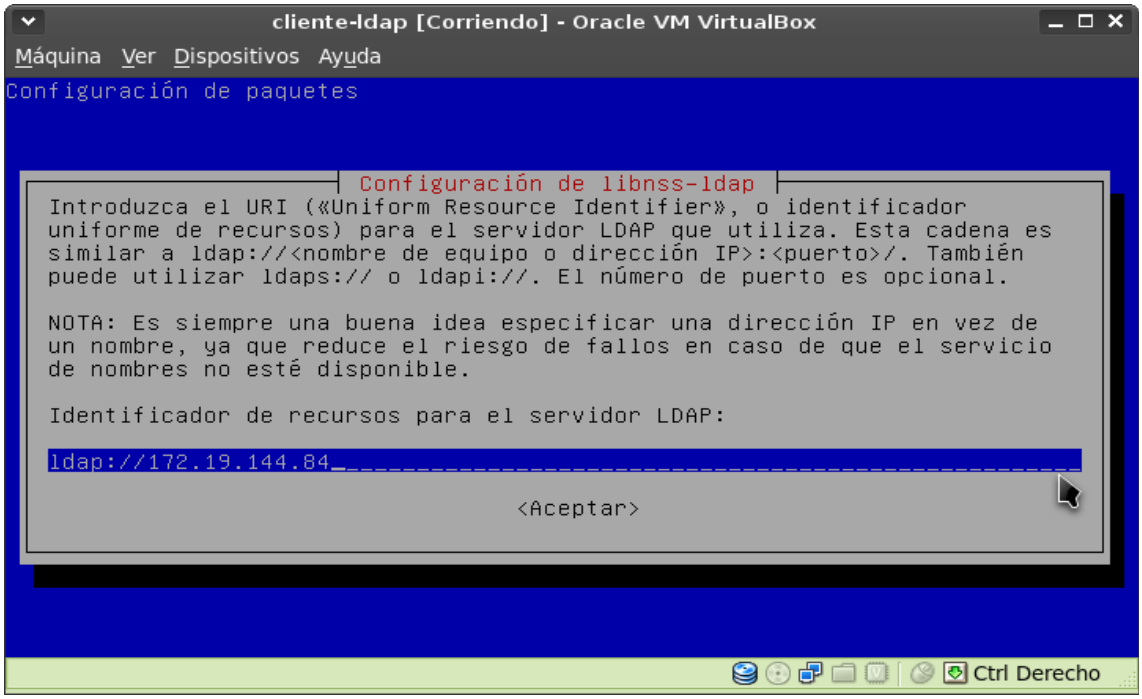
Instalar libnss-ldap es sencillo:



Pulsamos Enter para que comience la instalación. Se inicia automáticamente un asistente de configuración que nos irá haciendo preguntas para configurarla.

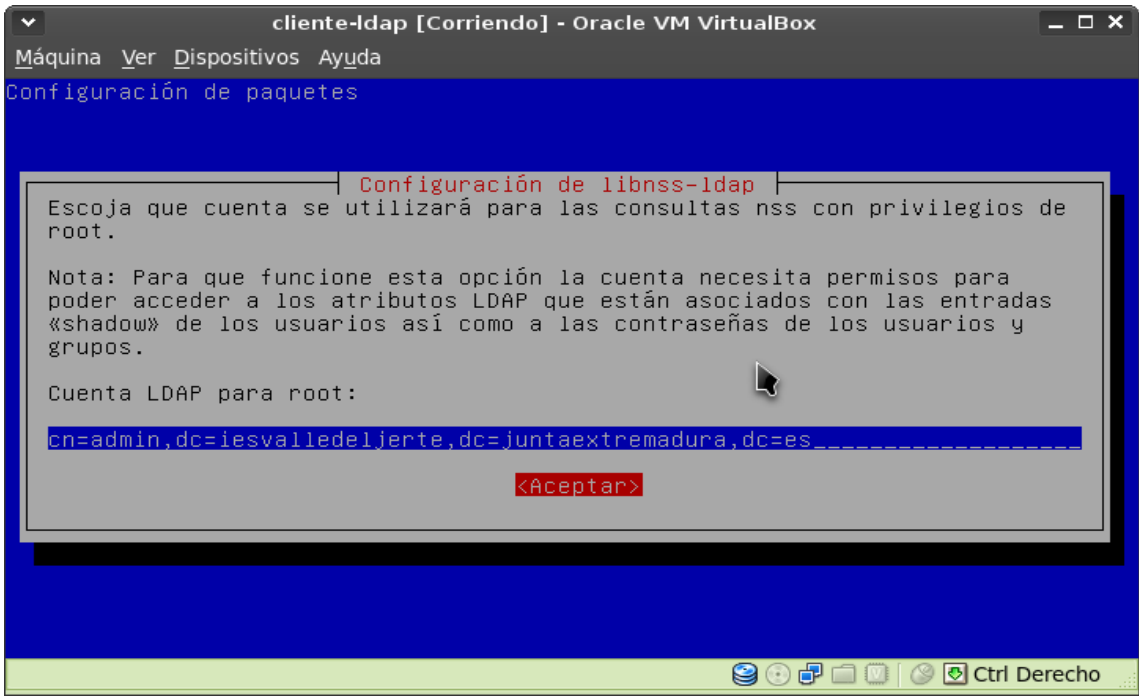
Una vez instalado, en cualquier momento podemos configurar libnss-ldap con tan sólo ejecutar: dpkg-reconfigure libnss-ldap.

Lo primero que nos pedirá el asistente será el URI del servidor ldap. Introduciremos: la IP del servidor ldap de la siguiente manera: http://172.19.144.84:

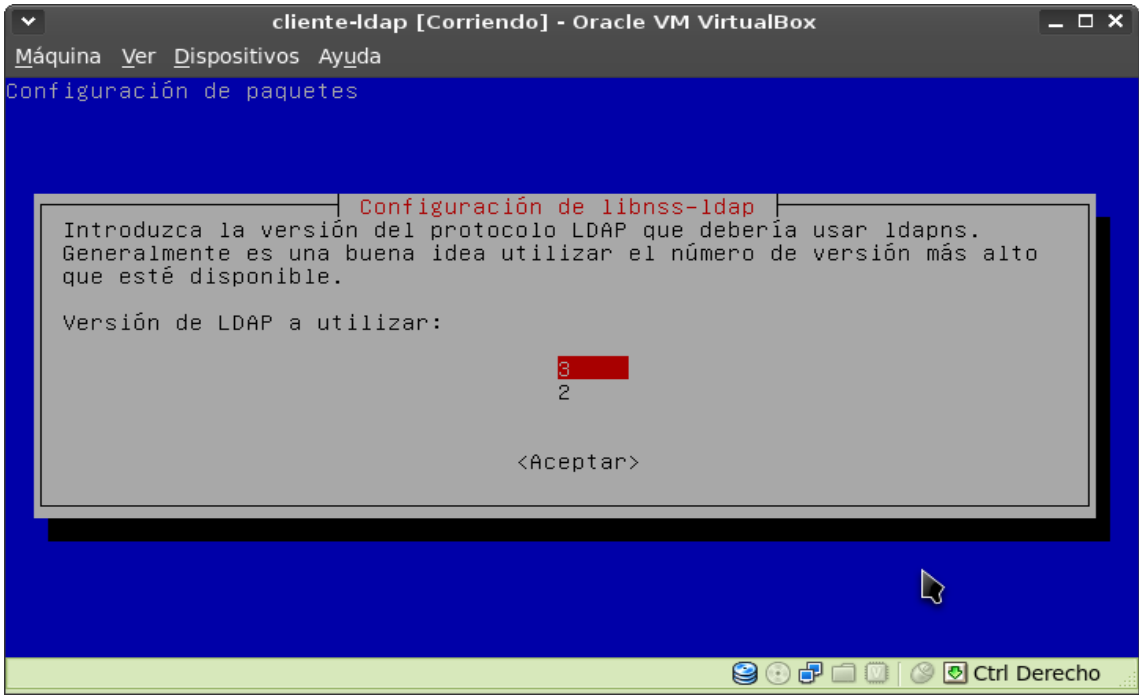


A continuación nos preguntará el nombre del administrador ldap:

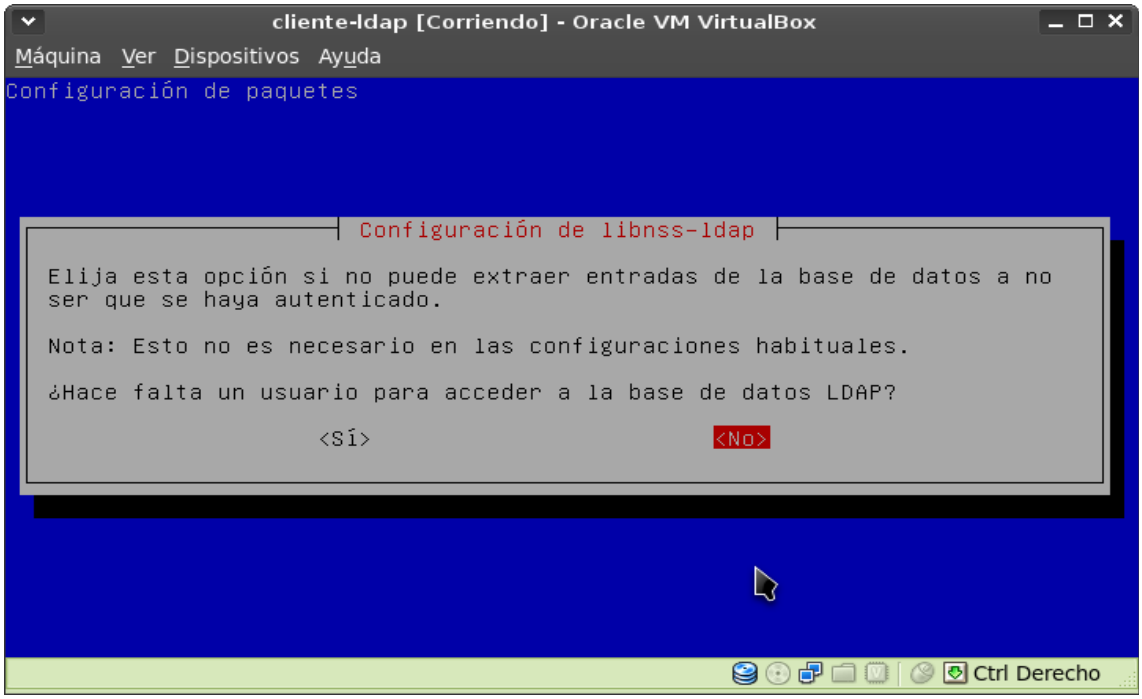
cn=admin,dc=iesvalledeljerte,dc=juntaextremadura,dc=es



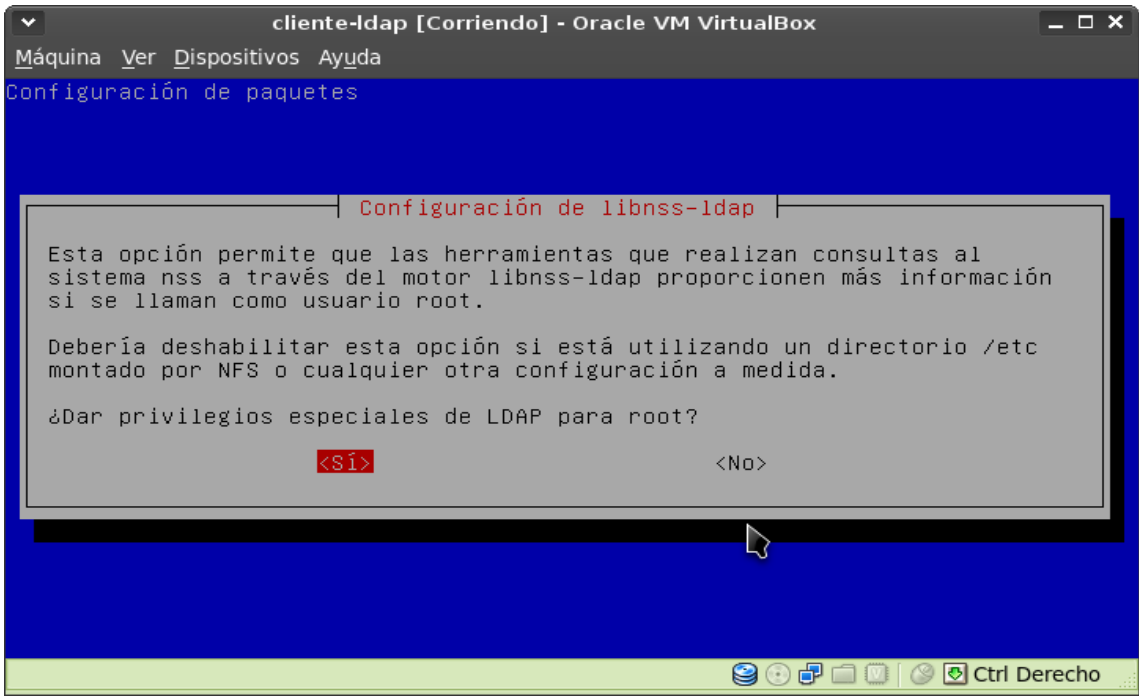
Nos preguntará la versión de LDAP. Elegimos LDAPv3:



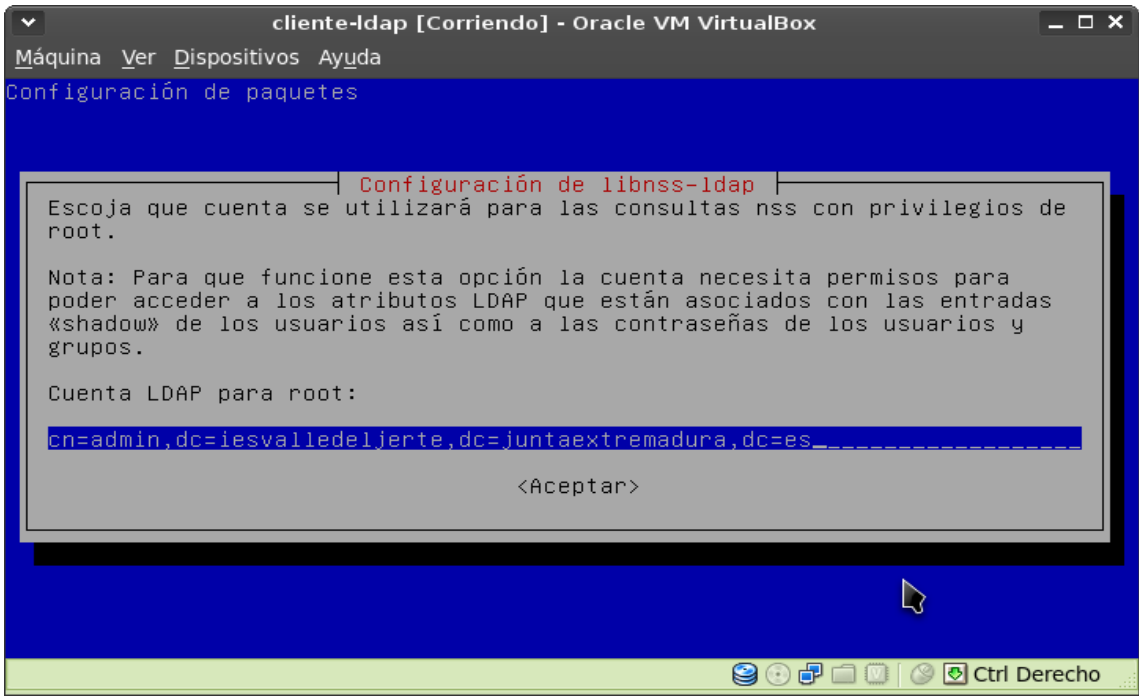
Nos preguntará si hace falta un usuario para acceder a la base de datos LDAP. Le decimos que no:



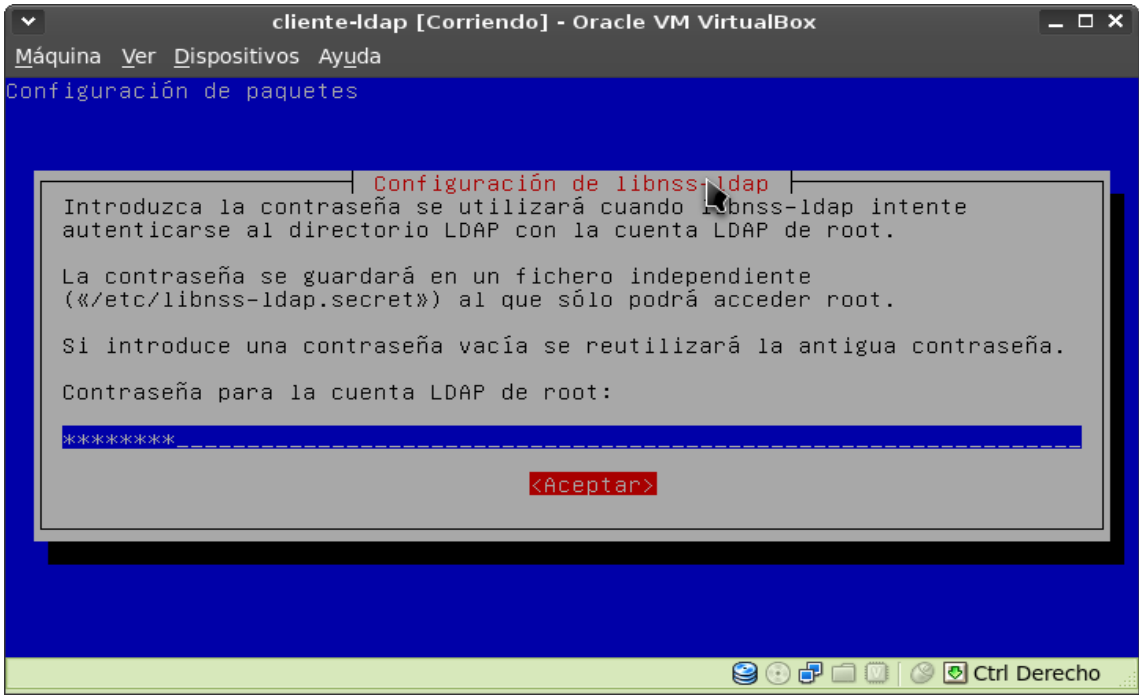
Nos preguntará si queremos dar privilegios especiales de LDAP para root. Le decimos que sí:



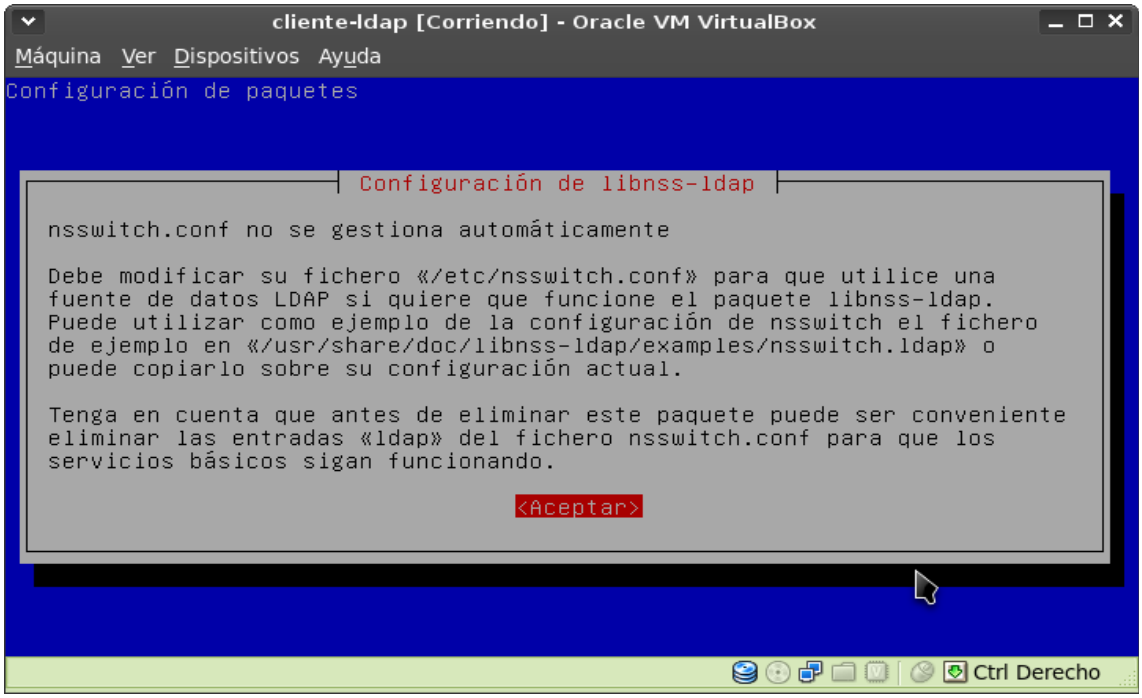
Nos pedirá que indiquemos una cuenta para las consultas nss con privilegios de root. Indicamos la del administrador:



Nos preguntará por la contraseña del usuario root. La introducimos:



Nos informa de que **nsswitch.conf** no se gestiona automáticamente. Esto quiere decir que tendremos que modificar el fichero /etc/nsswitch.conf para que nuestro sistema se autentifique con ldap:



El asistente terminará y con ello habremos configurado casi todo.

Para terminar la configuración de libnss-ldap vamos a modificar el fichero /etc/libnss-ldap.conf anñadiendo las líneas que le indican en qué unidades organizativas se encuentran los usuarios y los grupos:

nss_base_passwd	**ou=users,dc=iesvalledeljerte,dc=juntaextremadura,dc=es**
nss_base_group	**ou=group,dc=iesvalledeljerte,dc=juntaextremadura,dc=es**

3.3 Configurar nsswitch.conf

Por último, editamos el fichero /etc/nsswitch.conf y añadimos la palabra ldap detrás de la palabra compat en las líneas passwd, group y shadow. De este modo, estamos indicando que se utilice LDAP como alternativa para autentificar los usuarios:

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' 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
```

4. Probar la autentificación

Para comprobar si funciona la autentificación arranco la máquina virtual servidora de ldap y la máquina virtual cliente de ldap.

A continuación, inicio sesión en la máquina cliente, y ejecuto el comando:

```
# getent passwd
```

Este comando me muestra todos los usuarios que hay en el sistema, tanto los locales como los que están almacenados en ldap. Si no se mostraran los de ldap es porque habría algún error en la configuración.

Para asegurarnos de que se realiza la autentificación, instalamos el paquete libpam-dotfile:

```
# apt-get install libpam-dotfile
```

Una vez instalado, ejecutamos el comando pamtest passwd usuariodeldap. Por ejemplo:

```
# pamtest passwd sagrario
```

Nos pedirá la contraseña. Si todo está bien configurado, veremos un mensaje que dice:

```
Authentication successful.
```

También podríamos ejecutar el comando **su** (switch user) desde una consola de root a un usuario almacenado en ldap. Si nos permite cambiar de usuario y no nos pide contraseña es porque la autentificación con ldap está funcionando correctamente.

5. Crear home del usuario al vuelo

Tal y como está configurado el sistema, tenemos nuestros usuarios creados en el servidor ldap y éste nos va a permitir autentificarnos en un cliente con ellos, pero si no tenemos un directorio home creado en la máquina cliente nos advertirá de ello.

Podemos hacer que se cree el directorio home de un usuario al vuelo cuando éste inicie sesión por primera vez añadiendo la siguiente línea al fichero de configuración **/etc/pam.d/common-session**:

```
session                 required        pam_mkhomedir.so  skel=/etc/skel umask=0022
```