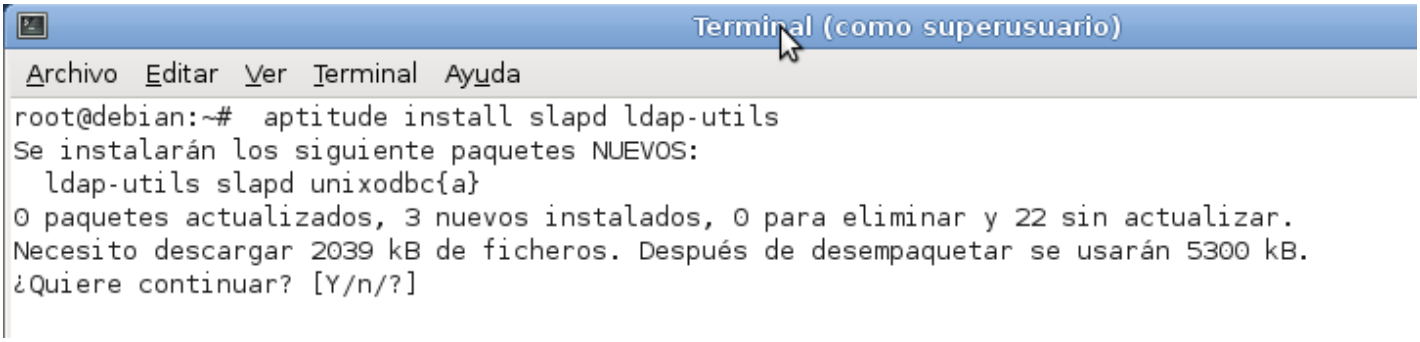
Servidor LDAP en Debian 6 Squeeze

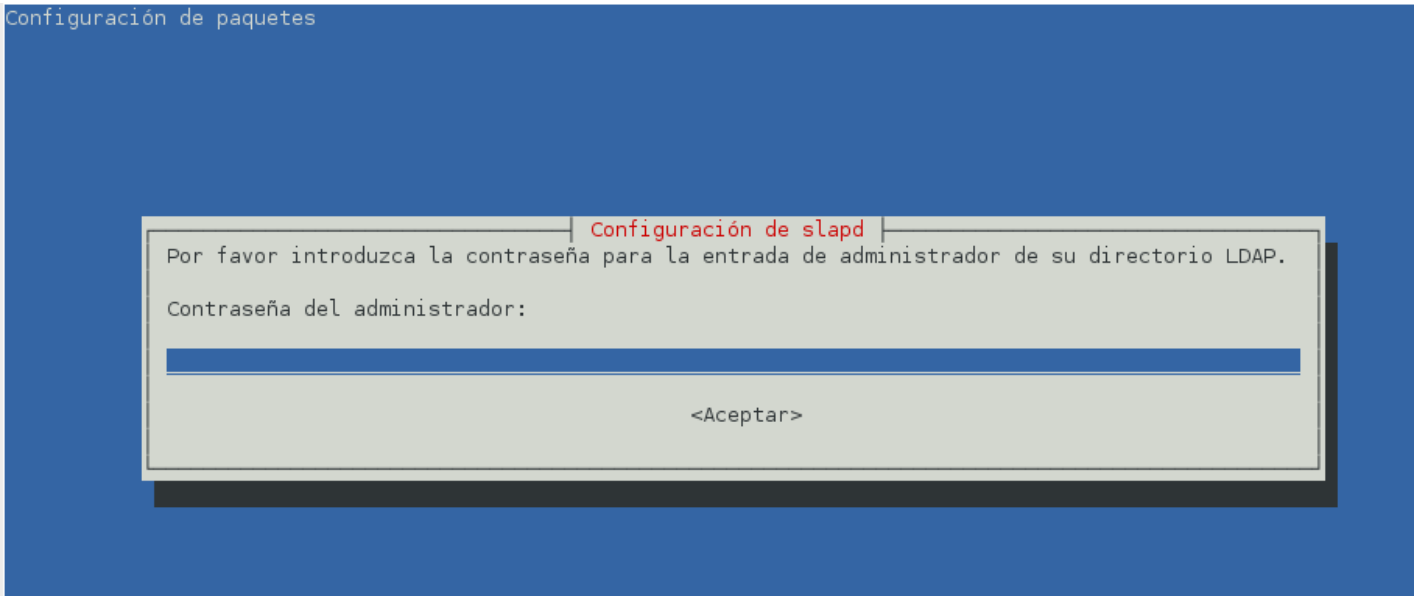
Vamos a explicar los pasos necesarios para configurar un servidor LDAP y un cliente que lo utilice para la identificación de usuarios

Instalación del Servidor

Comenzaremos instalando en el servidor los paquetes slapd y ldap-utils

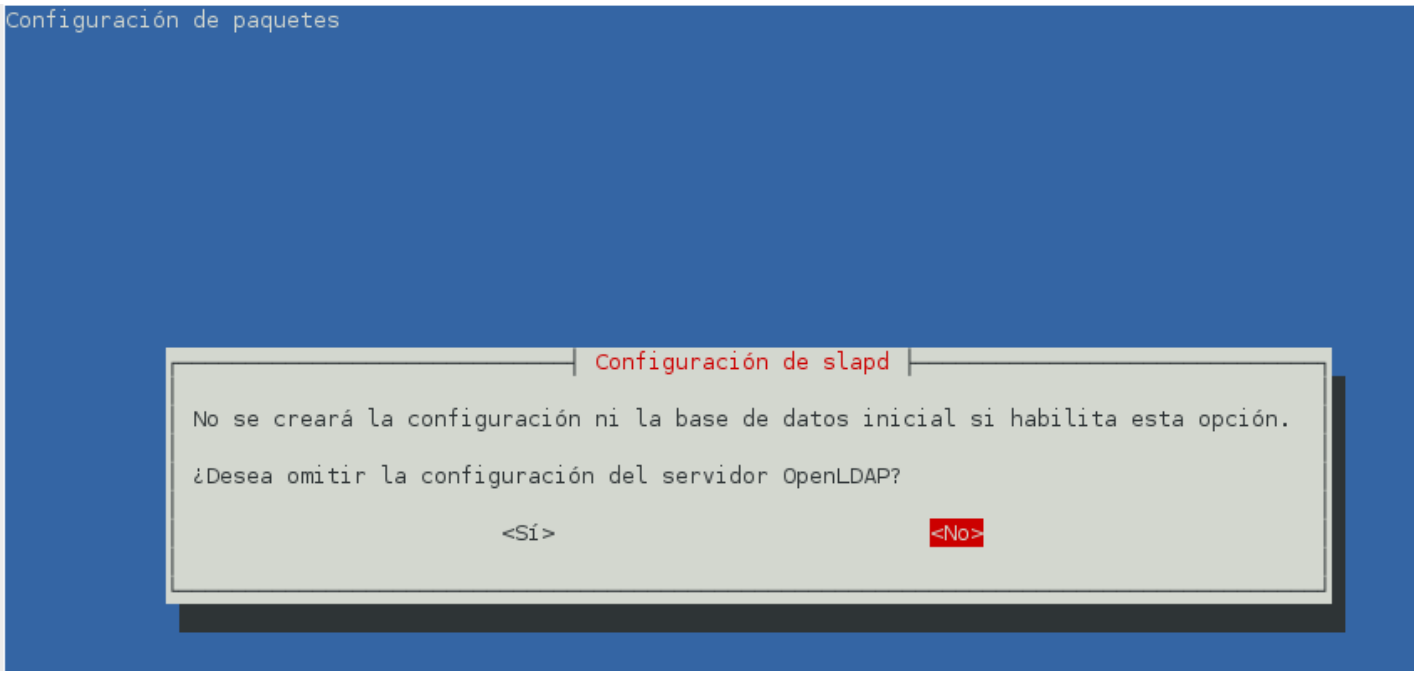


Durante la instalación nos pide la contraseña del administrador del servidor LDAP

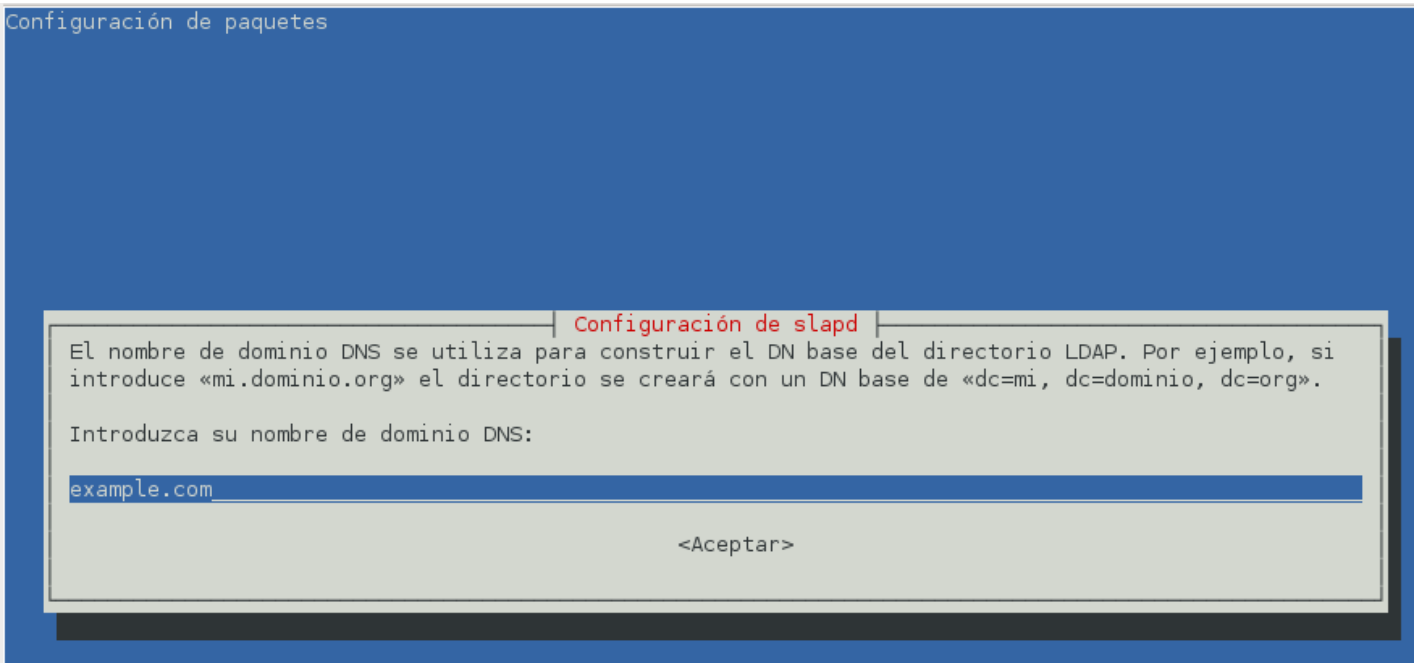


Introducimos una contraseña y en el siguiente paso nos la vuelve a pedir para verificarla.

Durante la instalación nos pedirá que configuremos el dominio que usará LDAP. Si no lo hace, podemos volver a configurarlo con *dpkg-reconfigure slapd* y aparecerán las siguientes ventanas

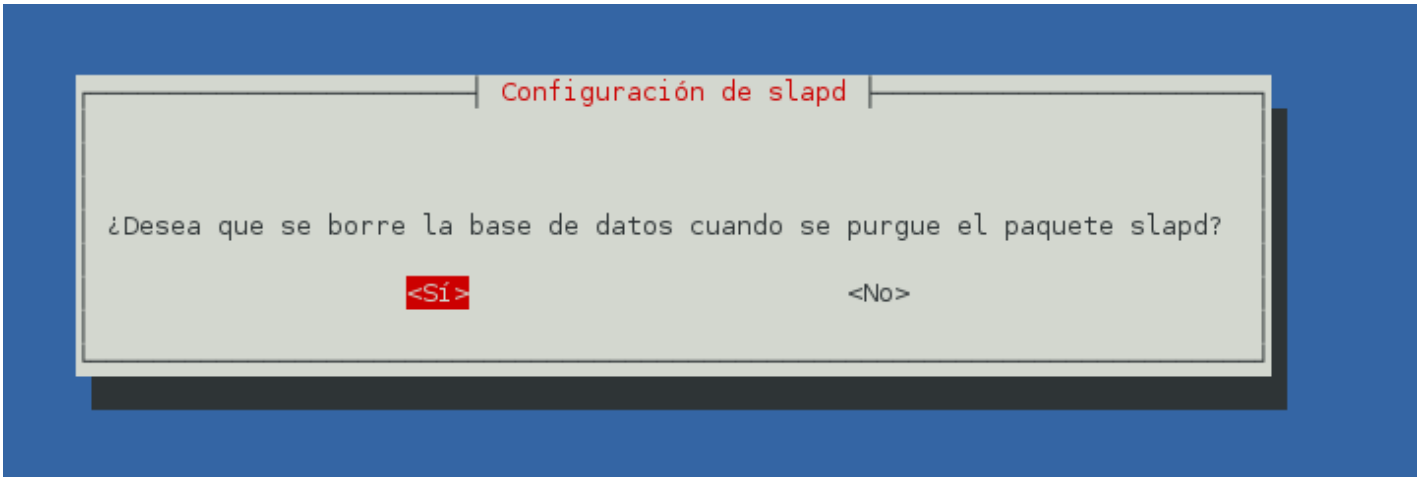


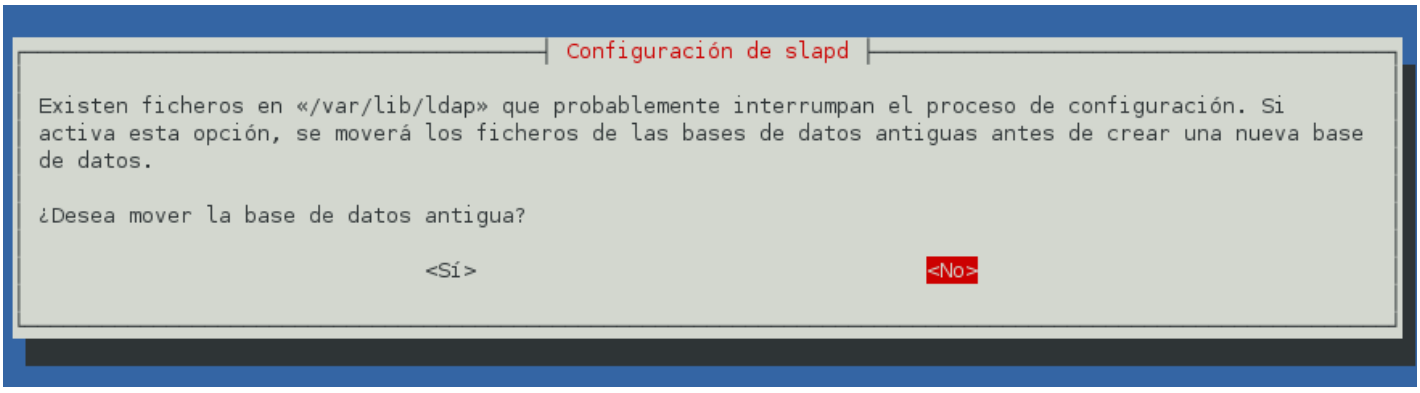
Pulsamos en NO, para que nos deje volver a configurar el servidor

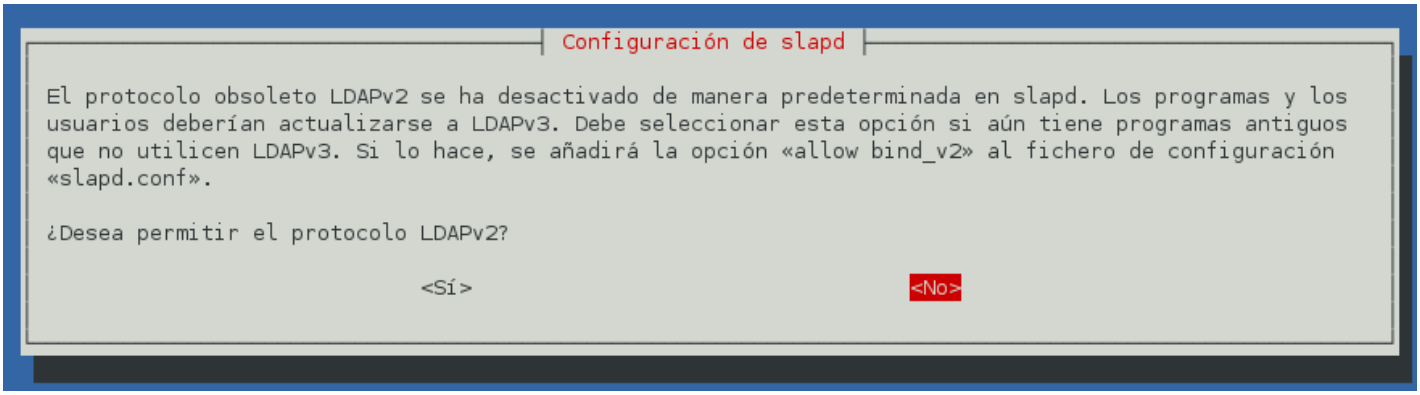


Introducimos el nombre del dominio que usará LDAP. También nos volverá a pedir la contraseña. El resto de opciones las configuramos como sigue (opción en rojo):


Configuración de paquetes
Configuración de slapd
Se recomienda el motor HDB. Los motores HDB y BDB utilizan formatos de almacenamiento semejantes, pero HDB permite realizar cambios de nombre de subárboles («subtree renames»). Ambos tienen las mismas opciones de configuración.
En cualquier caso, debe revisar la configuración de la base de datos. Vea en «/usr/share/doc/slapd/README.DB_CONFIG.gz» para más detalles.
Motor de base de datos a utilizar:
BDB
HDB
<Aceptar>


Configuración de slapd
¿Desea que se borre la base de datos cuando se purgue el paquete slapd?
<Sí>
<No>


Configuración de slapd
Existen ficheros en «/var/lib/ldap» que probablemente interrumpan el proceso de configuración. Si activa esta opción, se moverá los ficheros de las bases de datos antiguas antes de crear una nueva base de datos.
¿Desea mover la base de datos antigua?
<Sí>
<No>



Para ver los datos que tenemos insertados en nuestro servidor, podemos utilizar el comando *slapcat* y obtendremos algo como esto:

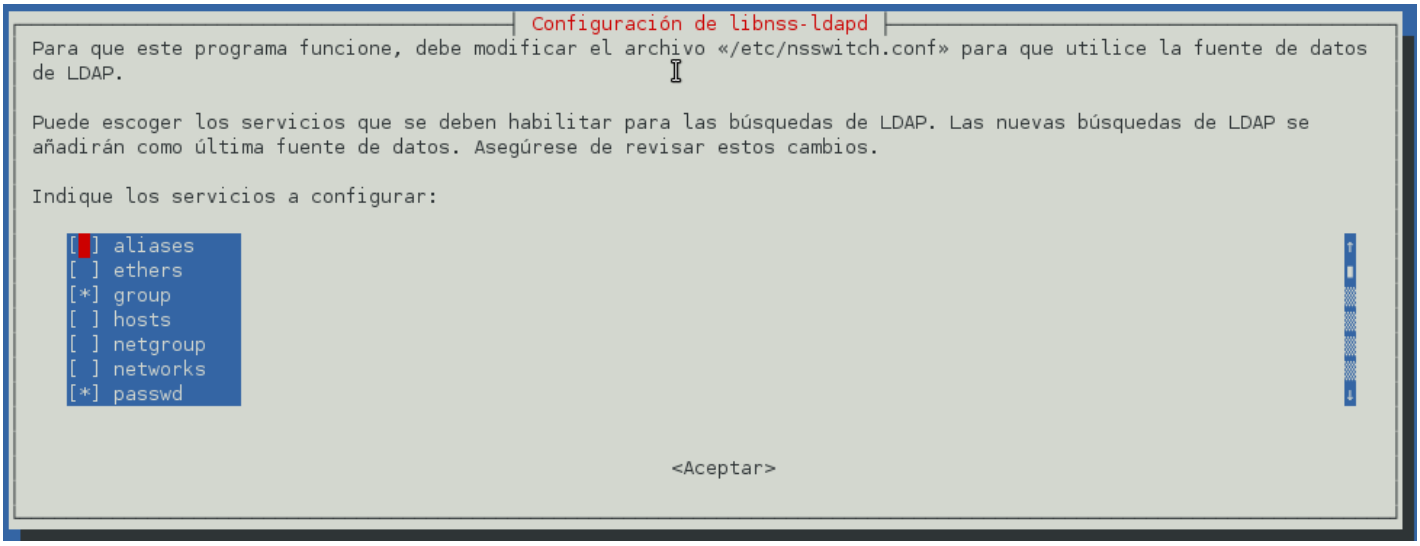
```
root@debian:~# slapcat
dn: dc=example,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: example.com
dc: example
structuralObjectClass: organization
entryUUID: e401c28c-7d5e-1030-829c-e9194ce08a19
creatorsName: cn=admin,dc=example,dc=com
createTimestamp: 20110927141526Z
entryCSN: 20110927141526.282973Z#000000#000#000000
modifiersName: cn=admin,dc=example,dc=com
modifyTimestamp: 20110927141526Z

dn: cn=admin,dc=example,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9b2E1SHBFTGJpeTJML2Rwc2VZamNSd1NGejFRZ2Q0Smk=
structuralObjectClass: organizationalRole
entryUUID: e40218a4-7d5e-1030-829d-e9194ce08a19
creatorsName: cn=admin,dc=example,dc=com
createTimestamp: 20110927141526Z
entryCSN: 20110927141526.285186Z#000000#000#000000
modifiersName: cn=admin,dc=example,dc=com
modifyTimestamp: 20110927141526Z
```

Para ver si tenemos el servidor LDAP a la escucha podemos usar *nmap -p 389 localhost* (si no está instalado se puede descargas de los repositorios con *aptitude install nmap*)

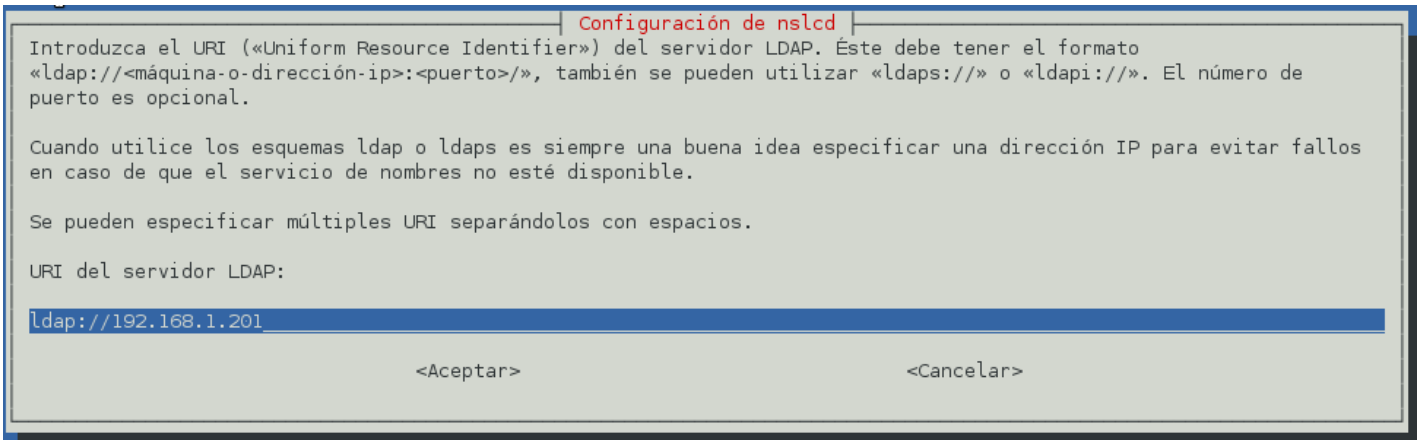
```
root@debian:~# nmap -p 389 localhost

Starting Nmap 5.00 ( http://nmap.org ) at 2011-09-27 18:38 CEST
Interesting ports on localhost (127.0.0.1):
PORT    STATE SERVICE
389/tcp open  ldap

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

Instalación del Cliente

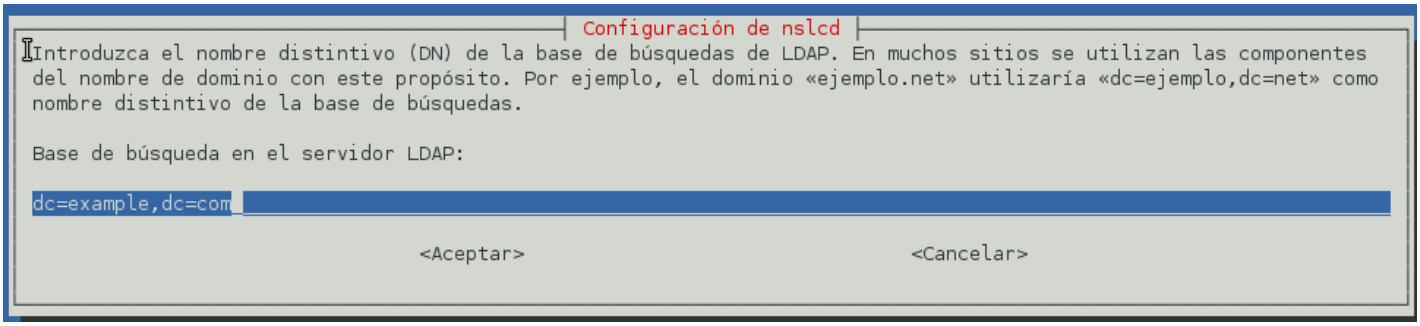
Instalamos los siguiente paquetes: libnss-ldapd libpam-ldapd nscd nslcd

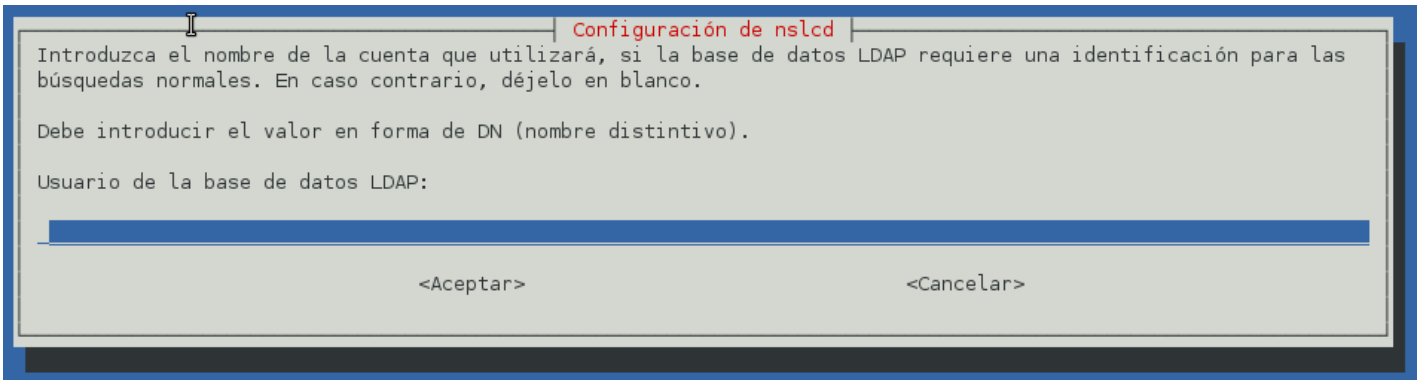


En la configuración de libnss-ldapd marcamos (con el espacio) *group, passwd y shadow*

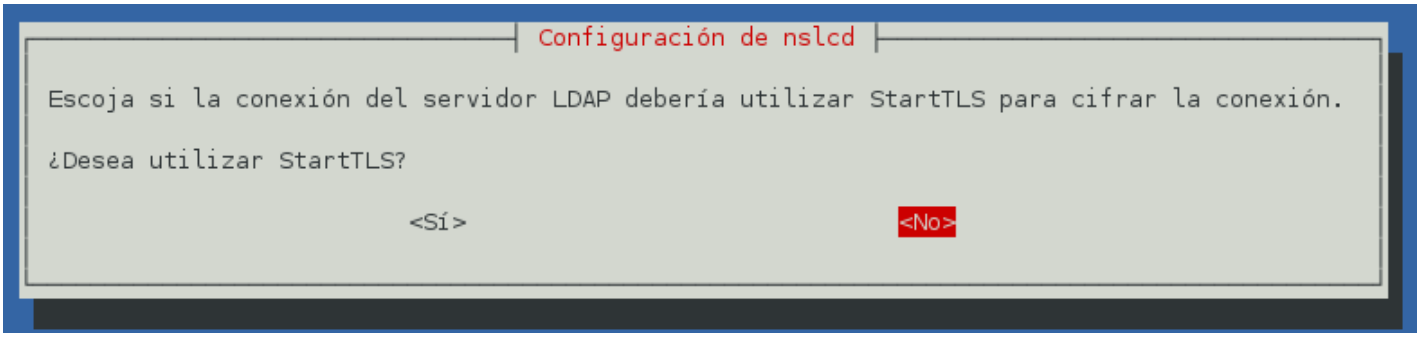


En la configuración de nslcd pondremos los parámetros del servidor LDAP. Si no aparece en la instalación ejecutaremos *dpkg-reconfigure nslcd*





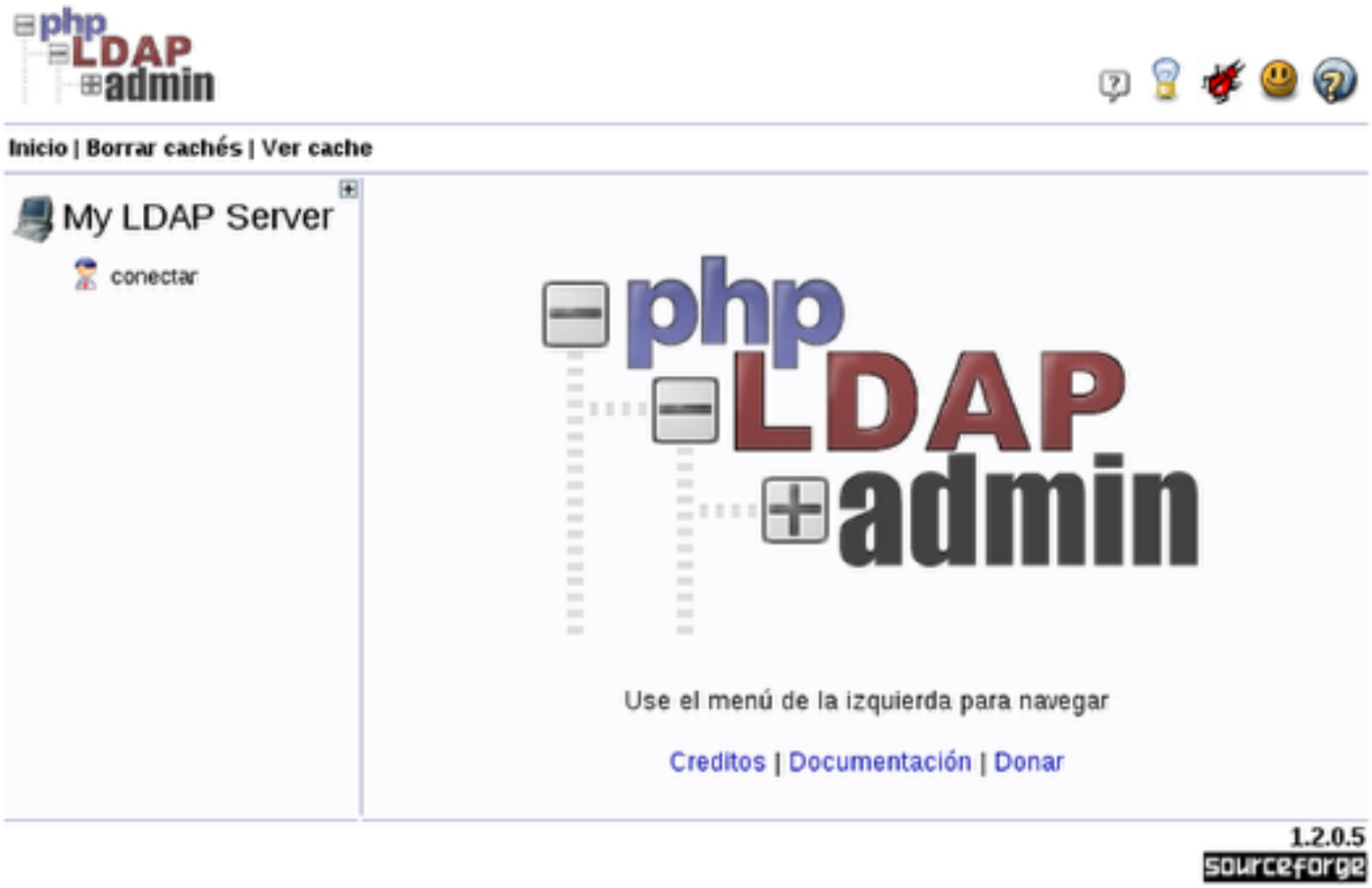
Como en nuestro caso no necesitamos ningún usuario especial para consultar el servidor LDAP, no ponemos nada



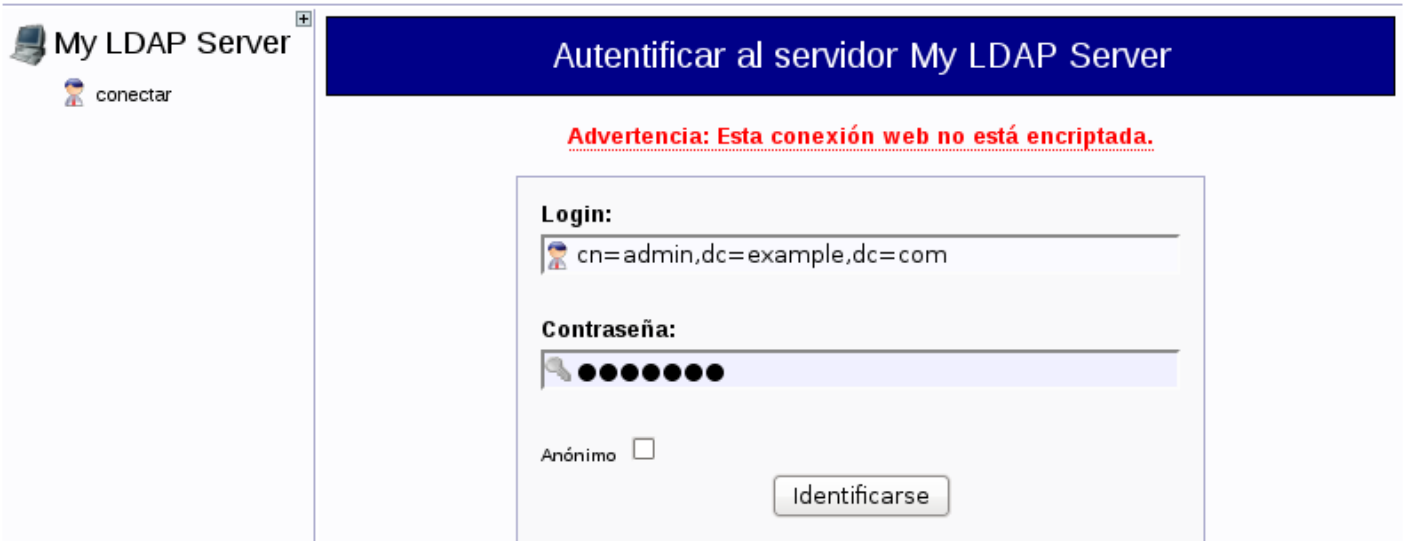
En nuestro caso no tenemos configurada una conexión segura (que sería lo recomendable), por eso ponemos que no use StartTLS

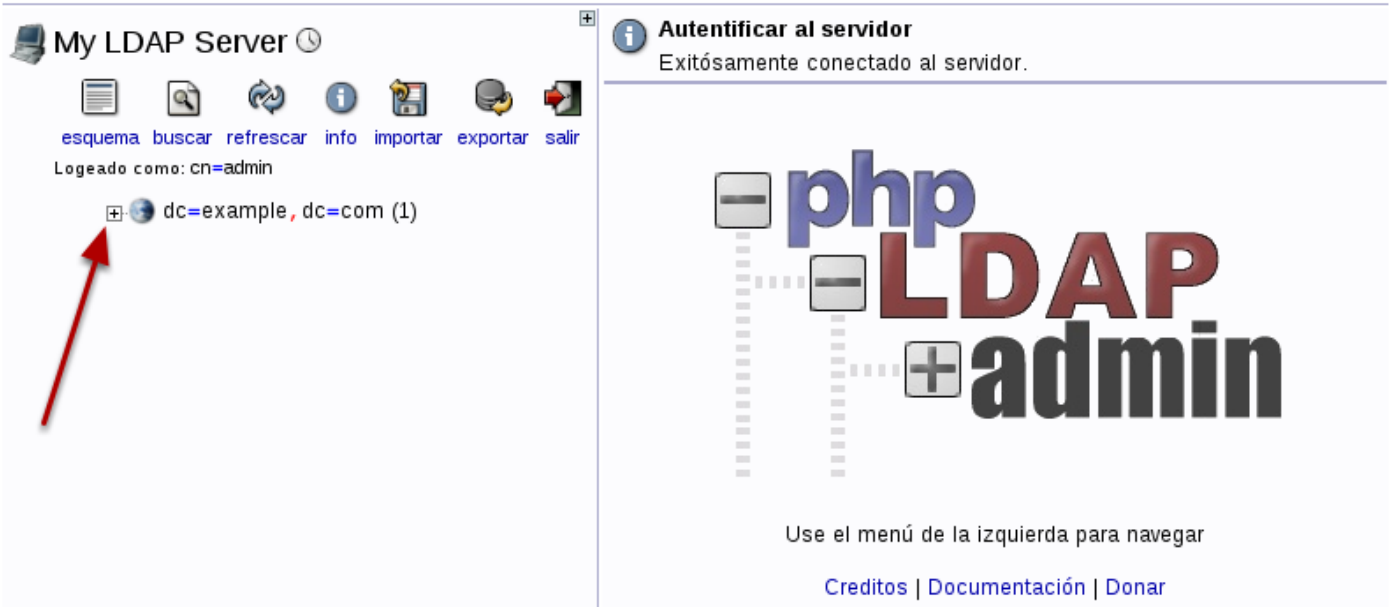
Añadir grupos y usuarios

Para administrar el servidor LDAP de manera más sencilla vamos a instalar una aplicación web llamada phpldapadmin. Está en los repositorios, por lo que sólo tendremos que usar apt-get o aptitude para instalarla: *aptitude install phpldapadmin.*
Una vez hecho esto, para acceder, entraremos a un navegador web y pondremos en la dirección *http://localhost/phpldapadmin/* y nos aparecerá una pantalla como esta:



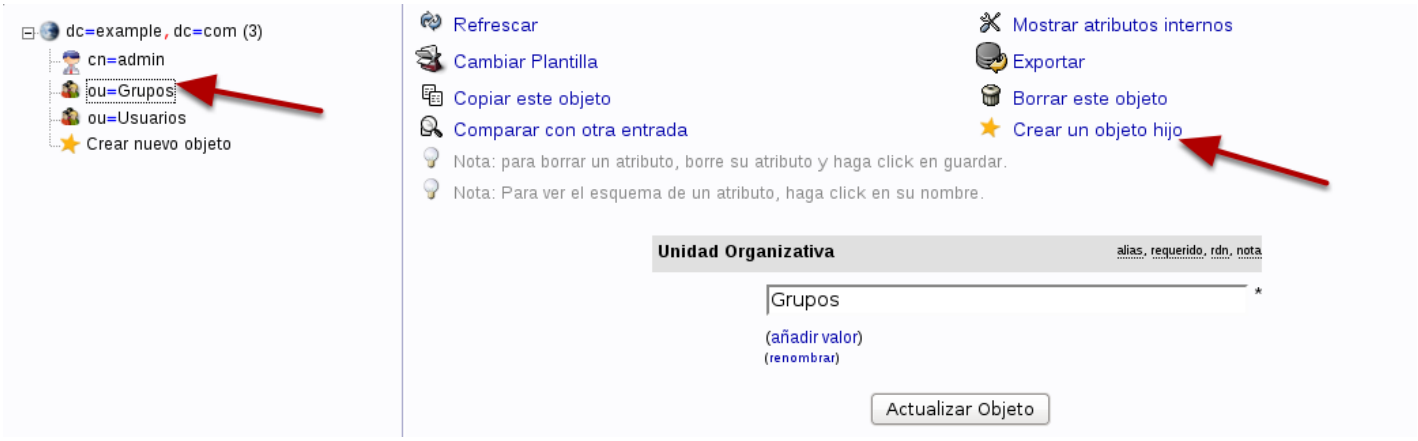
Para comenzar a administrar los elementos del LDAP pulsamos arriba a la izquierda donde pone "Conectar", luego ponemos el usuario administrador (cn=admin,dc=example,dc=com) y su contraseña.





Una vez dentro pulsamos en el signo + que hay a la izquierda del dominio para poder desplegar las opciones y veremos que sólo tenemos un elemento, el administrador. También veremos un icono para permitirnos crear más elementos. Pulsamos en crear nuevo objeto:

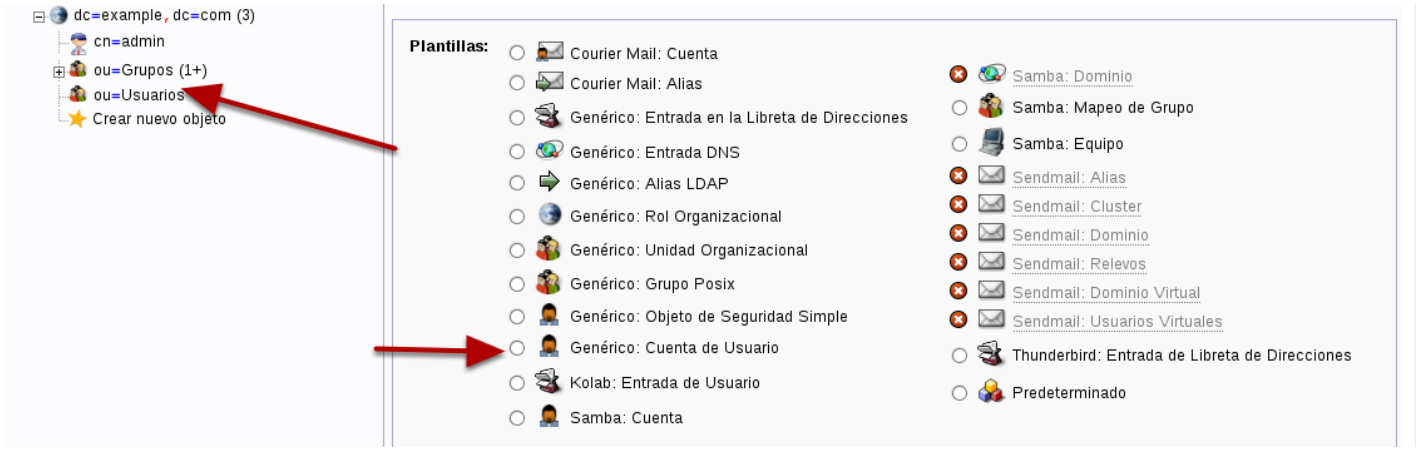
Una vez aquí, vamos a crear dos Unidades Organizativas, una para los grupos y otra para los usuarios



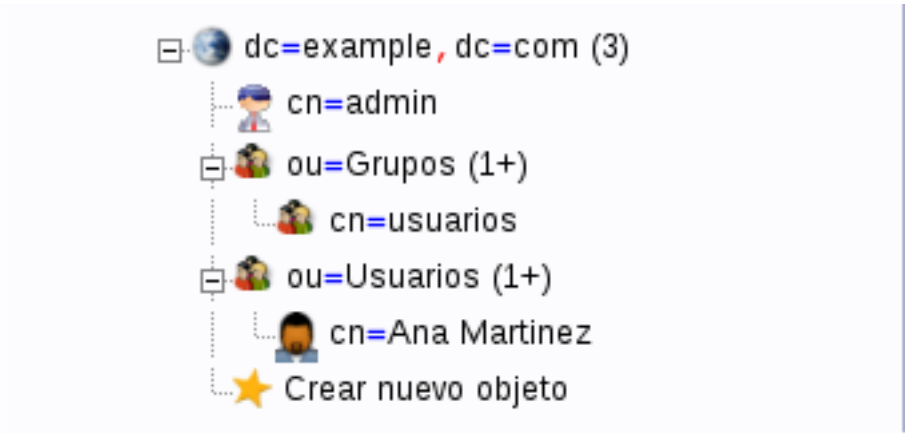
Ahora creamos los grupos como objeto hijo de la unidad organizativa "Grupos". En la plantilla elegimos Grupo Posix

Asiganos un nombre para el grupo y aceptamo el GID que nos sugiere. Si queremos poner uno nosotros y la casilla está desactivada tendríamos que editar la plantilla.
Vamos al fichero */etc/phpldapadmin/templates/creation/posixGroup.xml* y eliminamos la linea que pone *<readonly>1</readonly>*

Ahora vamos a crear los usuarios, pulsamos en ou=Usuarios y creamos un hijo del tipo Generico: Cuenta de Usuarios.



En el formulario que nos aparece rellenamos todas las opciones del usuarios. Con el UID nos pasará igual que con el GID explicado en el punto anterior. Si necesitamos insertar un número de nuestra preferencia editamos el fichero *posixAccount.xml* en el mismo directorio mencionado anteriormente.



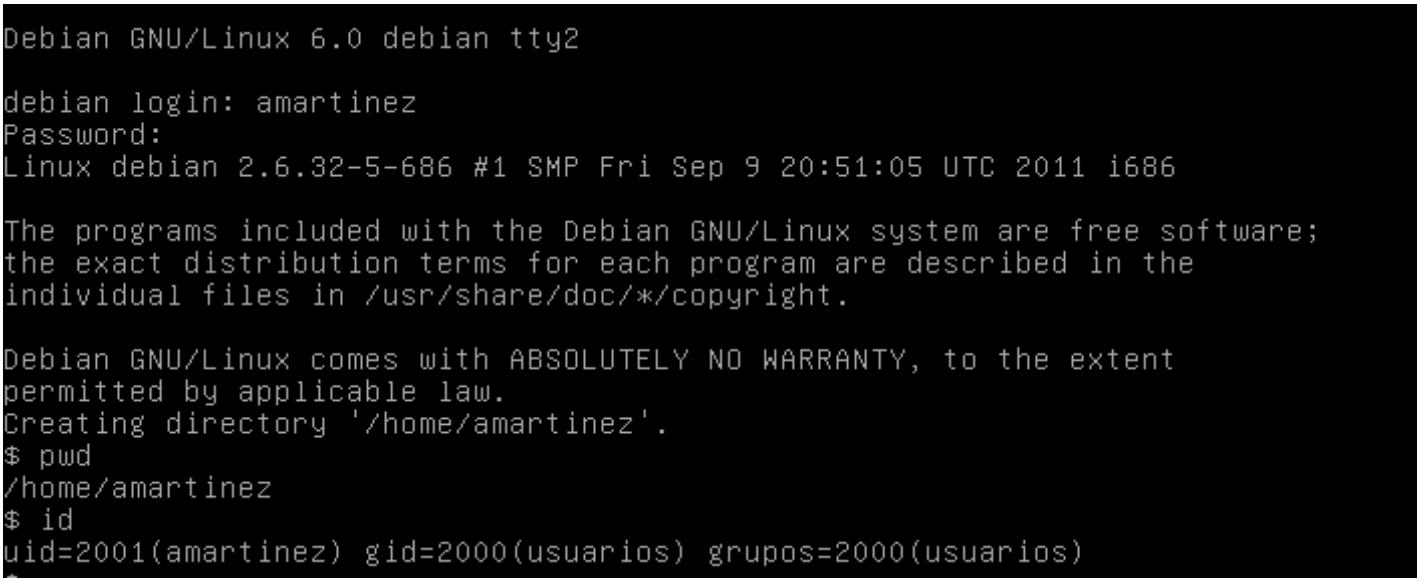
Este será el resultado final una vez creado el grupo y el usuario.

Comprobación y uso desde el cliente

Para comprobar que todo está correctos podemos ejecutar en el cliente la siguiente instrucción: *getent passwd*

```
saned:x:107:116::/home/saned:/bin/false
hplip:x:108:7:HPLIP system user,,,:/var/run/hplip:/bin/false
usuario:x:1000:1000:usuario,,,:/home/usuario:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
sshd:x:109:65534::/var/run/sshd:/usr/sbin/nologin
nslcd:x:110:117:nslcd name service LDAP connection daemon,,,:/var/run/nslcd/:/bin/false
amartinez:*:2001:2000:Ana Martinez:/home/amartinez:/bin/sh
root@debian:~#
```

Aquí podemos ver que aparecen los usuarios del sistema y también los que están creados en el LDAP, en este caso "amartinez". Lo mismo podríamos hacer para los grupos con *getent group*



Ahora podemos identificarnos en el sistema como "amartinez" y utilizar el sistema según los permisos configurados en él. Como podemos ver, si el directorio home del usuario no existe, lo crea automáticamente, eso lo realiza si existe la linea
session optional pam_mkhomedir.so skel=/etc/skel umask=0022
en el fichero */etc/pam.d/common-session* del cliente.

Enlaces relacionados

http://www.debian-administration.org/article/585/OpenLDAP_installation_on_Debian
http://www.saruman.biz/wiki/index.php/OpenLDAP
http://www.modlost.net/home/article/debian-gnulinux-open-ldap.html
http://www.debian.org/releases/stable/sparc/release-notes/ch-information.es.html#ldap-gnutls

Antonio Sánchez Corbalán, Septiembre 2011
http://antonio.sanchezcorbalan.es
@antosaco