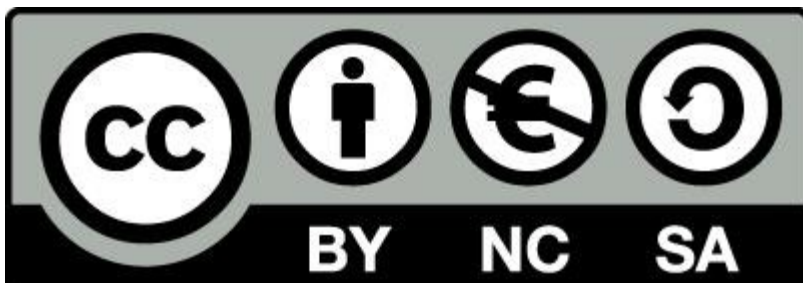


SISTEMAS OPERATIVOS EN RED

UT 3 – Gestión de usuarios. NFS y LDAP.

Mario García Alcázar

Esta obra esta sujeta a la Licencia Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons. Para ver una copia de esta licencia, visite <http://creativecommons.org/licenses/by-nc-nd/3.0/es/> o envíe una carta Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.



Última revisión Julio de 2020.

Índice de contenido

1. Introducción.....	4
2. Servicio LDAP (Lightweight Directory Access Protocol).....	5
3. Instalación de Open LDAP.....	8
3.1 Instalación del servidor LDAP.....	9
3.2 Instalación del cliente LDAP en sistemas Linux.....	25
3.3 Instalación del cliente LDAP en sistemas Windows.....	33
4. Configurar perfiles móviles con LDAP y NFS.....	37
4.1 Instalación de NFS.....	38
4.2 Configuración de perfiles móviles.....	41

1. Introducción.

A lo largo de este curso, hemos tratado la instalación de sistemas Debian, ya sea con una configuración básica o con particionado RAID y LVM. También repasamos los comandos básicos del sistema y programación en Shell Script.

Una vez dominados esos conceptos, en este tema estudiaremos uno de los protocolos más importantes que podemos configurar para mejorar la gestión de los usuarios en una red con un servidor Linux Debian.

Concretamente el servicio **LDAP (Lightweight Directory Access Protocol)**.

Este protocolo permite a los usuarios validarse en el sistema utilizando cuentas globales almacenadas en el servidor central, y no en equipos locales.

Además mantiene una base de datos con un **directorio de objetos** similar al Active Directory de Windows Server, el cual almacena información de múltiples tipos de objetos, como dominios, subdominios, usuarios, grupos, equipos, cuentas Samba, etc.

2. Servicio LDAP (Lightweight Directory Access Protocol).

Una parte fundamental del funcionamiento de un sistema operativo en red Linux consiste en permitir que las personas que utilizan dicho sistema puedan autenticarse por medio de usuarios globales ubicados en un servidor central, y no solamente con usuarios creados en sus propios equipos.

Esto mejora en gran manera la seguridad de los accesos al sistema, ya que la información de autenticación de dichos usuarios se almacena en un servidor central, al cual solo deberían tener acceso físico los administradores informáticos.

Para conseguir que el sistema funcione de esta forma utilizaremos un protocolo llamado **LDAP** (Lightweight Directory Access Protocol) y más concretamente su implementación de software libre **Open LDAP**.



LDAP y Open LDAP permiten implementar un dominio similar al **Active Directory** de los equipos que tienen instalado Windows Server. En este punto trataremos los conceptos teóricos referentes a los dominios que ofrece LDAP.

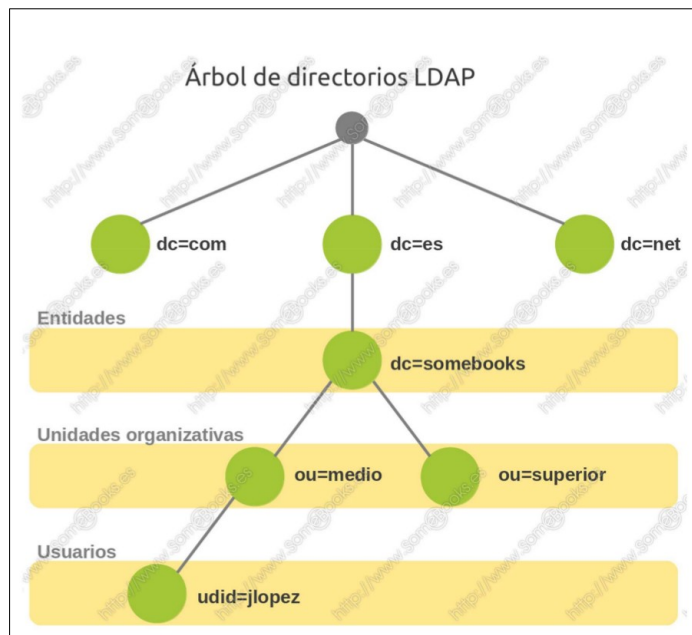
LDAP mantiene una base de datos que almacena una **estructura en forma de árbol o DIT (Directory Information Tree)**, donde cada nodo puede almacenar información sobre diferentes elementos, los principales son:

- **Dominio.**- Es una colección de objetos dentro del directorio **DIT**. Pueden existir diferentes dominios dentro del **DIT**, cada uno de ellos con su propia colección de objetos y unidades organizativas.

El **nombre de dicho dominio** está formado por la secuencia de entidades del árbol, en orden inverso (es decir desde abajo hasta la raíz). En la imagen de ejemplo el dominio sería somebooks.es

- **Entidades (dc).**- Son elementos que nos sirven para crear subdominios dentro de un dominio. Esto puede usarse por ejemplo en empresas u organizaciones muy grandes o distribuidas geográficamente.
- **Unidades organizativas (uo).**- Son unidades lógicas en las que podemos dividir un dominio, por ejemplo, si tenemos un servidor LDAP para gestionar a los usuarios de una empresa, las unidades organizativas podrían ser los departamentos de dicha empresa (informática, administración, dirección, etc)
- **Grupos de usuarios.**
- **Usuarios.**
- **Equipos.**

Lógicamente, el árbol establece una **estructura jerárquica** entre sus elementos, por ejemplo si tenemos un nodo con información de una unidad organizativa, todos los nodos que cuelguen de él pertenecerán a dicha unidad.



Por otra parte, el formato básico de cada nodo es el siguiente:

```
# comentario  
dn: <nombre global único>  
<atributo>: <valor>  
<atributo>: <valor>
```

Los nodos se identifican unívocamente usando el **nombre completo (dn)**. El nombre completo se formará con una serie de pares atributo/valor, separados por comas, que reflejan la ruta inversa desde la posición lógica del objeto hasta la raíz del árbol.

Entre los atributos que suelen emplearse habitualmente, encontramos los siguientes, aunque puede haber muchos más y variar en función del tipo de objeto que se esté almacenando:

- uid (user id): Identificación única de la entrada en el árbol.
- objectClass: Indica el tipo de objeto al que pertenece la entrada.
- cn (common name): Nombre de la persona representada en el objeto.
- givenname: Nombre de pila.
- sn (surname): Apellido de la persona.
- o (organization): Entidad a la que pertenece la persona.
- u (organizational unit): El departamento en el que trabaja la persona.
- mail: dirección de correo electrónico de la persona.

De esta forma, un nodo en el directorio LDAP con información sobre un usuario podría tener el siguiente aspecto:

```
dn: uid=lgomez, ou=medio, dc=somebooks, dc=es  
objectClass: person  
cn: Luis Gomez  
givenname: Luis  
sn: Gomez  
o: somebooks  
u: medio  
mail: luisgomez@somebooks.es
```

3. Instalación de Open LDAP.

Para realizar la instalación de **OpenLDAP**, hemos de completar diferentes tareas tanto en el servidor central como en los equipos clientes. Estas tareas van desde la instalación de los paquetes de LDAP a la configuración del dominio y creación de usuarios globales.

Por otra parte, hay que indicar que dichas tareas pueden realizarse en modo gráfico o en modo texto, no obstante, debido a la complejidad de los comandos de configuración en modo texto, en este curso, nos centraremos (siempre que sea posible) en la configuración gráfica del servicio.

3.1 Instalación del servidor LDAP.

A continuación, trataremos las acciones a realizar en el servidor para instalar LDAP y configurar el dominio:

1. Primero abriremos una consola como administrador e instalaremos LDAP, para lo cual ejecutaremos el comando:
apt-get install slapd ldap-utils php7.3-xml php7.3-zip

Durante la instalación el sistema solicitará que introduzcamos la contraseña del administrador de LDAP. Esta contraseña será necesaria para poder realizar las operaciones de configuración o creación de usuarios de LDAP.

2. Instalamos el cliente LDAP account manager. Podemos descargar el paquete desde la WEB de dicho proyecto:
<https://www.ldap-account-manager.org/lamcms/releases>
3. Seguidamente hemos de crear la base de datos de LDAP con el comando:
dpkg-reconfigure slapd

Durante este proceso deberemos de indicar el nombre del dominio LDAP y la clave del usuario administrador (admin).

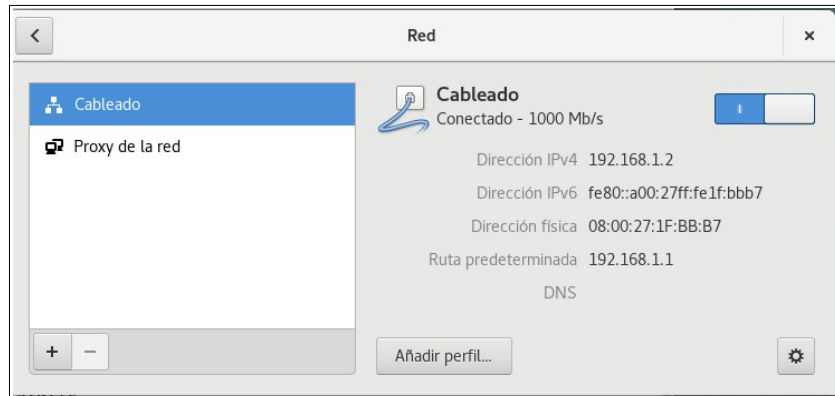
Una vez instalado podemos comprobar el resultado con el comando **slapcat**.

```
mario@debian: ~$ slapcat
dn: dc=clase,dc=es
objectClass: top
objectClass: dcObject
objectClass: organization
o: clase.es
dc: clase
structuralObjectClass: organization
entryUUID: 4d7193f6-056b-1037-8329-c1ef713ac3a7
creatorsName: cn=admin,dc=clase,dc=es
createTimestamp: 20170725095641Z
entryCN: 20170725095641.301425Z#000000#000#000000
modifiersName: cn=admin,dc=clase,dc=es
modifyTimestamp: 20170725095641Z

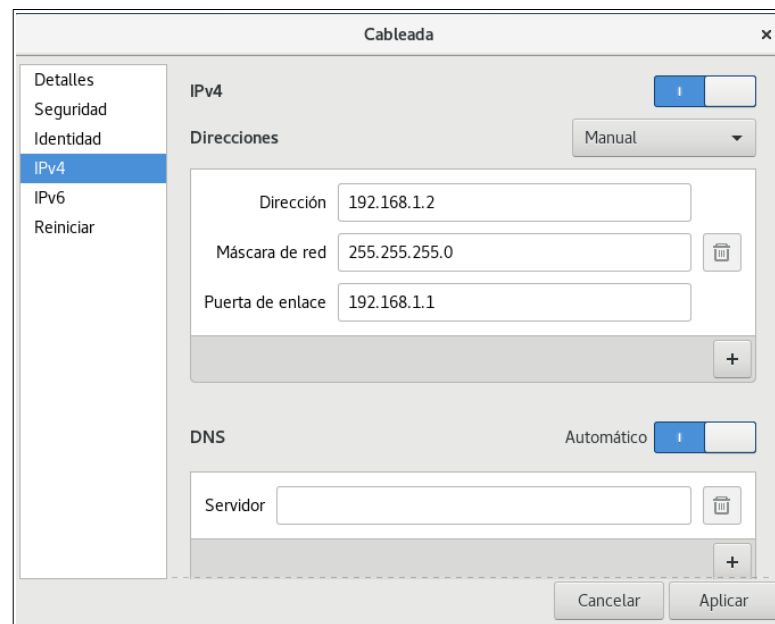
dn: cn=admin,dc=clase,dc=es
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: eINTSEF9b2IDY2ZDL285T38lVnpphUJpNwdPeXRLaGZ4eStoUk4=
structuralObjectClass: organizationalRole
entryUUID: 4d71b666-056b-1037-8329-c1ef713ac3a7
creatorsName: cn=admin,dc=clase,dc=es
createTimestamp: 20170725095641Z
entryCN: 20170725095641.30239Z#000000#000#000000
modifiersName: cn=admin,dc=clase,dc=es
modifyTimestamp: 20170725095641Z

root@debian:/home/mario#
```

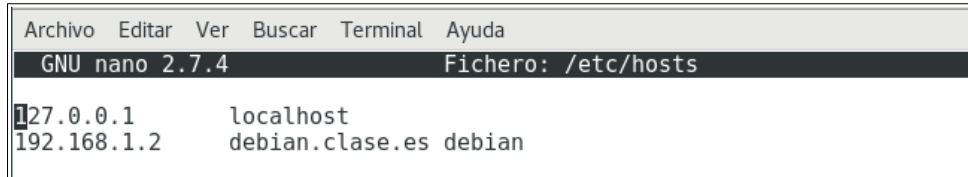
4. Para que el sistema funcione correctamente hemos de realizar algunas tareas previas:
- El servidor debe tener una IP fija. Para ello se la asignaremos desde la configuración de red del entorno gráfico.



En esta pantalla seleccionaremos el interfaz cableado y pulsamos en el botón de la esquina inferior derecha.

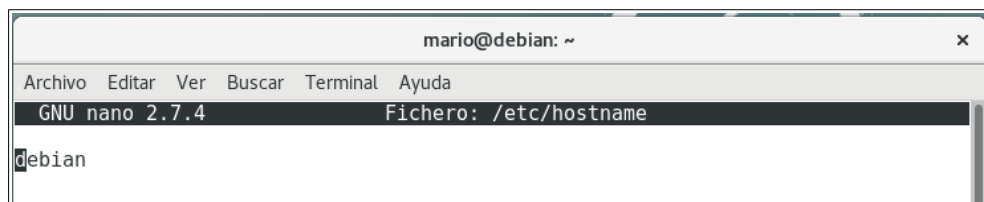


- En el fichero **/etc/hosts** debemos enlazar el nombre de nuestro equipo, el dominio LDAP y la dirección IP estática del servidor.

A screenshot of the GNU nano 2.7.4 text editor. The title bar shows 'GNU nano 2.7.4' and 'Fichero: /etc/hosts'. The editor content shows two lines: '127.0.0.1 localhost' and '192.168.1.2 debian.clase.es debian'. The cursor is at the end of the second line.

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
GNU nano 2.7.4                                Fichero: /etc/hosts
127.0.0.1      localhost
192.168.1.2    debian.clase.es  debian
```

- En el fichero **/etc/hostname** solo necesitamos tener una línea con el nombre del equipo servidor.

A screenshot of the GNU nano 2.7.4 text editor. The title bar shows 'GNU nano 2.7.4' and 'Fichero: /etc/hostname'. The editor content shows a single line: 'debian'. The cursor is at the end of the line.

```
mario@debian: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
GNU nano 2.7.4                                Fichero: /etc/hostname
debian
```

5. Ahora configuraremos el dominio y sus usuarios para lo cual utilizaremos la herramienta gráfica **LDAP Account Manager**.

LDAP Account Manager (LAM) es un cliente para LDAP, basado en una interfaz web, que permite administrar de una forma sencilla un servidor LDAP desde cualquier lugar, a través de un sencillo navegador de Internet.

El proyecto fue creado en 2003 por Michael Dürchner, Roland Gruber, Tilo Lutz y Leonhard Walchshäusl con el objetivo de administrar cuentas de usuarios, equipos y grupos bajo los protocolos POSIX y SAMBA. El resultado fue LDAP Account Manager, un software escrito en PHP que se ofreció a la comunidad informática bajo licencia GPL.

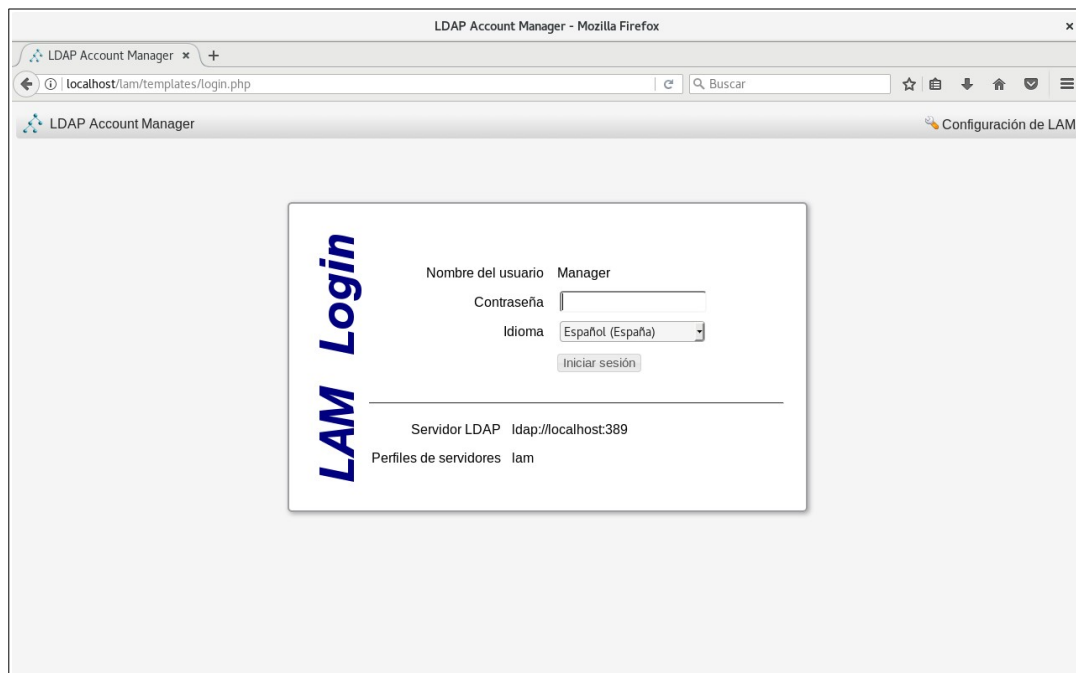
Las ventajas que aporta son:

- Puede funcionar sobre cualquier servidor web que soporte PHP a partir de la versión 4.
- Es compatible con cualquier navegador web en el lado cliente que soporte CSS.

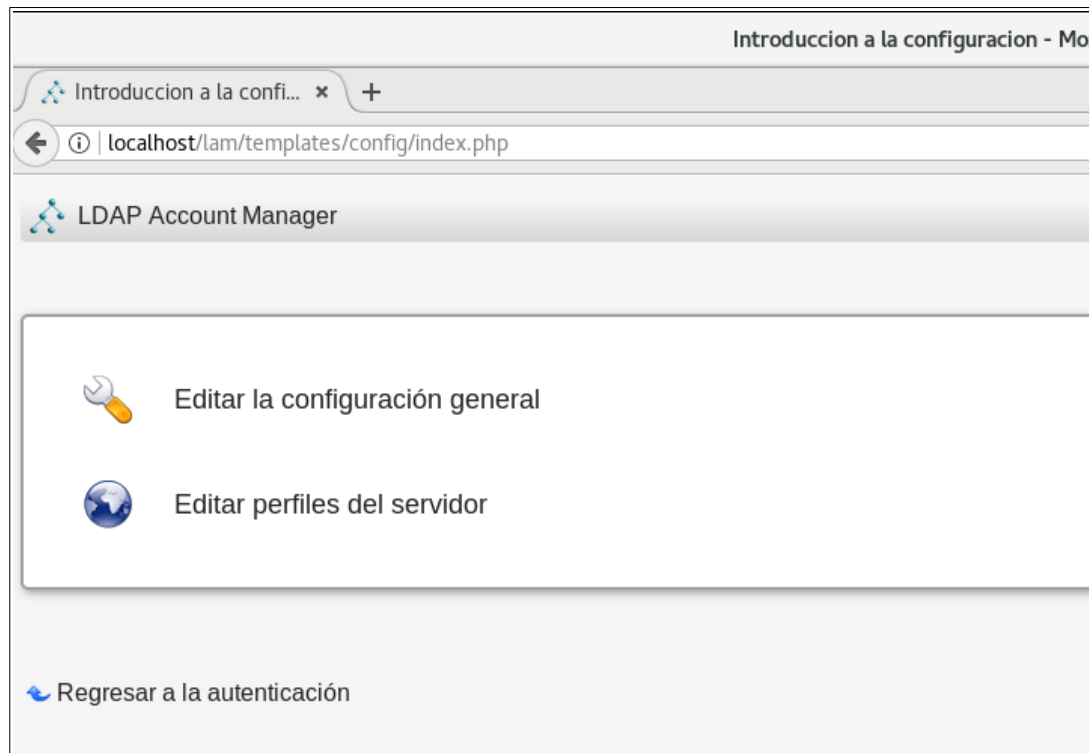
Sistemas Operativos en Red
UT 3 – Gestión de usuarios. NFS y LDAP.

- Puede utilizarse con OpenLDAP a partir de la versión 2.0.
- Puede utilizar conexiones sin cifrar o cifradas con SSL.
- Puede exportar la información de las cuentas en formato PDF.
- Puede crear nuevas cuentas a partir de archivos de texto.

Para ejecutar LAM, solo tenemos que abrir un navegador en el servidor y acceder a la siguiente dirección: **http://localhost/lam**



6. Primero de todo hemos de definir el funcionamiento de LAM, para lo cual, pulsaremos en el botón **“Configuración de LAM”** y seguidamente **“Editar la configuración general”**



La contraseña para acceder sera inicialmente **lam**.

Entre las opciones de configuración que se muestran está:

- El tiempo que permanecerá la sesión abierta en caso de inactividad del usuario.
- Las características que deben cumplir las contraseñas de los usuarios (longitud mínima, caracteres en mayúsculas, símbolos, etc).
- Cambio de contraseña para el acceso a la configuración. Este cambio no estará activo hasta que no reiniciemos el ordenador.

Configuración general

Preferencias de seguridad

Tiempo de espera de la sesión ?

Equipos permitidos ?

Encriptar sesión ☒ ?

Certificados SSL utilizar los certificados del sistema ?

No se ha seleccionado ningún archivo.

ldaps://

Política de contraseñas

Longitud mínima de la contraseña ?

Caracteres mínimos con minúscula. ?

Caracteres mínimos con mayúsculas. ?

Mínimo de caracteres numéricos ?

Caracteres mínimos con símbolos. ?

Clases de caracteres mínimos. ?

Número de reglas que deben coincidir ?

La contraseña no puede tener el nombre del usuario ☐ ?

La contraseña no debe contener partes del primer/segundo nombre ni el nombre de usuario ☐ ?

Iniciando sesión

Nivel de trazas ?

Destino de las trazas ☐ No iniciar sesión ?
☒ Registrando en el sistema.
☐ Archivo

Reporte de errores PHP ?

Cambiar la contraseña maestra

Nueva contraseña maestra ?

Vuelva a introducir la contraseña

7. El siguiente paso será acceder a “**Configuración de LAM**” y seguidamente a “**Editar perfiles del servidor**”.

En este punto definiremos las **características del dominio LDAP** que vamos a utilizar. Como puedes ver, la página se divide en cuatro pestañas:

- **Configuración general**, que contiene la información global del servidor LDAP, como el nombre del host o las características de seguridad.
- **Tipos de cuentas**, donde se indican las diferentes clases de cuentas que administraremos, como usuarios, grupos o equipos.
- **Módulos**, que contiene la lista de módulos que definen las características de las cuentas que vamos a administrar (si son cuentas Unix, Samba, Koalab, etc).
- **Preferencias del módulo**, que contiene aspectos específicos del módulo que hayamos seleccionado en la solapa anterior.

En este curso sólo trataremos las funcionalidades de las dos primeras pestañas, ya que es más que suficiente para realizar la configuración básica LDAP.

- Pestaña de **Configuración general**:

Configuración general | Tipos de cuentas | Módulos | Preferencias del módulo

Preferencias del servidor

Dirección del servidor ldap://localhost:389

Activar TLS no

Sufijo del arbol dc=clase,dc=es

Límite de búsqueda LDAP -

Opciones Avanzadas

Configuración del idioma

Idioma por defecto Español (España)

Zona horaria Europe/Madrid

Preferencias de lamdaemon

Lista de servidores

Path a script externo

Nombre del usuario

SSH key file

SSH key password

	Lectura	Escribir	Ejectuar	
Propietario	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Grupo	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Otro	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

The screenshot shows the 'Ajustes de herramientas' (Tools Settings) and 'Preferencias de seguridad' (Security Preferences) sections of the LDAP Account Manager configuration window. The 'Ajustes de herramientas' section contains a group of checkboxes for 'Herramientas ocultas' (Hidden Tools), including 'Edición múltiple' (Multiple editing), 'Editor de PDF' (PDF editor), 'Explorador de esquemas' (Schema explorer), 'Editor de OU' (OU editor), 'Comprobar' (Check), 'Enviar archivos' (Send files), 'Información del servidor' (Server information), and 'Editor de perfiles' (Profile editor). The 'Preferencias de seguridad' section contains fields for 'Método del inicio de sesión' (Login method) set to 'Lista fijada' (Fixed list), 'Lista de usuarios válidos' (Valid users list) containing 'cn=Manager,dc=my-domain,dc=com', 'Nueva contraseña' (New password), and 'Vuelva a introducir la contraseña' (Re-enter password).

Aquí hemos de configurar diversas opciones:

En el apartado **preferencias del servidor** deberemos completar los siguientes datos:

- Dirección del servidor: Como el servidor OpenLDAP se encuentra en el mismo equipo que LDAP Account Manager, nos limitaremos a dejar el valor predeterminado (<ldap://localhost:389>).
- Activar TLS: TLS son las siglas de Transport Layer Security (Seguridad de la capa de transporte). Como por ahora no vamos a utilizar conexiones cifradas, mantenemos el valor predeterminado (no).
- Sufijo del árbol: Es el nombre del dominio que queremos que use el directorio LDAP. Para nuestro ejemplo será: dc=clase,dc=es.
- Límite de búsqueda LDAP: Permite reducir los resultados de una búsqueda cuando tenemos un directorio muy extenso. En nuestro caso, lo dejaremos desactivado.

En el apartado **Configuración de idioma**, seleccionaremos **Español**.

Seguidamente, en el apartado **Preferencias de lamdaemon** podemos indicar cuál es el servidor para las carpetas personales y dónde se encuentra el script que administra las cuotas (cantidad de espacio que puede usar cada usuario). También permite establecer los permisos predeterminados para las carpetas personales de los nuevos usuarios.

En principio no tocaremos ninguna de estas opciones.

El apartado Ajustes **de herramientas** nos permite indicar si utilizaremos algunas de las herramientas que se relacionan:

- Editor de PDF (PDF editor): Si lo habilitamos, podremos exportar la información de las cuentas en archivos PDF. Además, podremos editar los perfiles PDF para indicar la estructura de la página y la información incluida.
- Editor de OU (OU editor): Se trata de un sencillo editor que nos permitirá añadir o quitar Unidades Organizativas de nuestro árbol LDAP.
- Información del servidor (Server information): Nos mostrará información y estadísticas relacionadas con el servidor LDAP.
- Comprobar (Tests): Permite verificar si el esquema LDAP que estamos usando es compatible con LDAP Account Manager, indicando los posibles problemas.
- Explorador de esquemas (Schema browser): permite examinar el esquema del servidor LDAP, obteniendo los tipos de clases, atributos, sintaxis y reglas que hay disponibles.
- Editor de perfiles (Profile editor): Contiene plantillas para las cuentas. Con él, se podrán indicar valores predeterminados que se utilizarán durante la creación de cuentas.
- Multi edit: Facilita la modificación por lotes de un gran número de entradas LDAP, añadiendo o quitando atributos o asignándoles valores específicos.
- Enviar archivos (File upload): Nos permite crear las cuentas mediante un sencillo editor de textos, usando formato CVS, y

después incluirlas todas a la vez en el árbol LDAP subiendo el archivo.

Nosotros en este curso activaremos la opción de **Editor OU** ya que nos va a interesar crear unidades organizativas.

Por último, en el apartado de **Preferencias de seguridad**, indicaremos de qué usuarios del directorio pueden entrar en la aplicación LDAP Account Manager. Hay dos métodos **lista fijada** o **búsqueda LDAP**.

Si elegimos **lista fijada**, deberemos especificar uno o varios usuarios (uno en cada línea). Por cada uno de ellos, escribiremos su nombre global único (Distinguished Name – DN) siguiendo las indicaciones que vimos al principio de este capítulo (por ejemplo, **cn=admin,dc=clase,dc=es**).

Por su parte, eligiendo **Búsqueda LDAP** haremos que LDAP Account Manager busque un DN en el directorio a partir de un nombre de usuario.

En nuestro caso, elegiremos la opción Lista fijada.

Hay que indicar que en la parte inferior de la pantalla se permite cambiar la contraseña de acceso de los usuarios a la aplicación LDAP Account Manager. Deberemos introducir una contraseña y reiniciar el equipo.

- Pestaña de **Tipos de cuentas**.

Tipos de cuentas disponibles

Alias de email	Alias de correo (p.ej. alias de correo NIS)	+
Códigos de facturación	Códigos de facturación PyKota	+
DHCP	Administración DHCP	+
Domínios de Samba	Entradas de al dominio de Samba 3	+
Equipos	Cuentas de equipos (p.ej. Samba)	+
Extensiones de Asterisk	Entradas de extensiones de Asterisk	+
Impresoras	Impresoras PyKota	+
NIS grupos de red	NIS entradas de grupo de red	+
Recursos compartidos Kolab	Recursos compartidos Kolab (p. ej. Carpetas de correo)	+

Tipos de cuentas activos

Usuarios Cuentas de usuario (p.ej. UNIX,Samba y Kolab) ✖

Sufijo LDAP Atributos del listado

Opciones Avanzadas

Grupos Cuentas del grupo (p.ej. Unix y Samba) ✖

Sufijo LDAP Atributos del listado

Opciones Avanzadas

Aquí podemos indicar los tipos de cuenta que administrará LDAP.

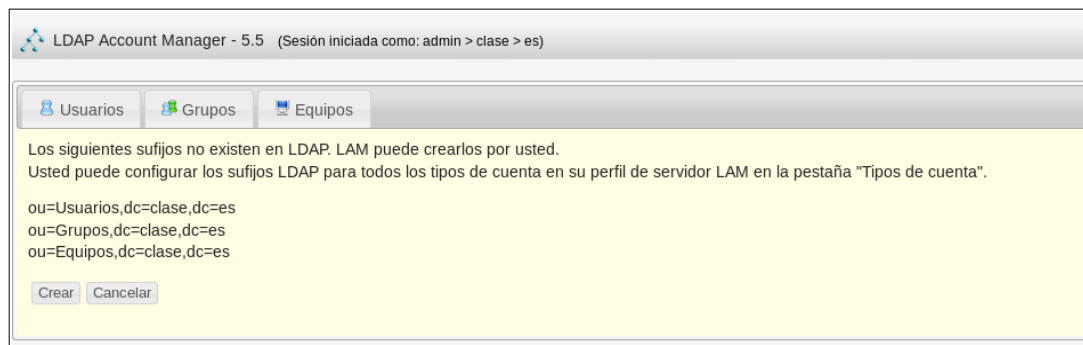
Como podemos ver, hay muchos tipos de cuentas disponibles, no obstante, en este curso solo trataremos las cuentas de usuarios y grupos.

Para cada tipo de cuenta, especificaremos:

- Sufijo LDAP: Nombre de dominio y unidad/es organizativas donde está la cuenta.

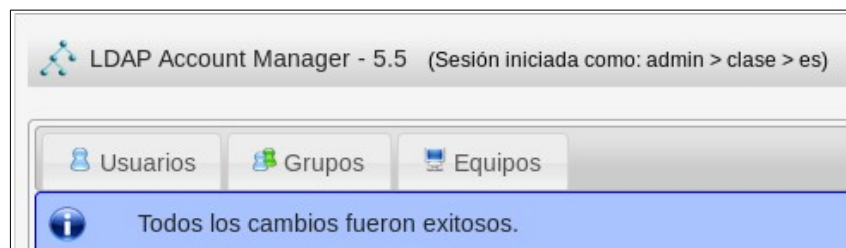
En nuestro ejemplo, para el tipo de cuenta de **Usuarios** usaremos el sufijo **ou=usuarios,dc=clase,dc=es** y para los grupos **ou=grupos,dc=clase,dc=es**

- Atributos del listado: Representa la lista de atributos que se mostrarán en el listado de cuentas. En principio dejaremos los valores por defecto.
8. El último paso que trataremos en la aplicación LAM, será la **creación y gestión de cuentas de usuarios y grupos**, para lo cual, en la pantalla de inicio de LAM, introduciremos la contraseña de usuario Manager y pulsaremos el botón de “**iniciar sesión**”.



Como podemos observar, esta pantalla tiene **una pestaña por cada tipo de cuenta que hemos configurado**. Además os indica que hay sufijos que no existen (esto es porque todavía no hemos creado las unidades organizativas usuarios, grupos y equipos).

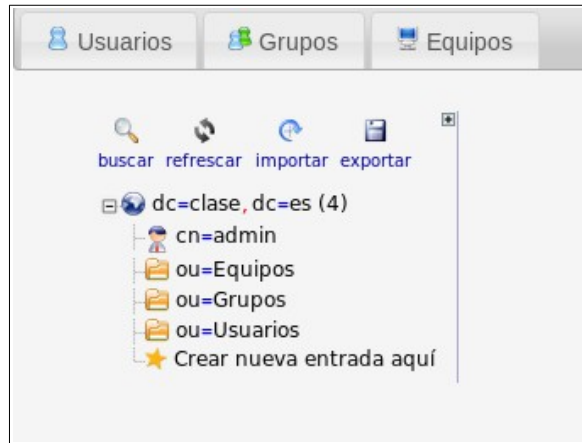
Para subsanar este problema solo hemos de pulsar en el botón “**crear**”.



Sistemas Operativos en Red

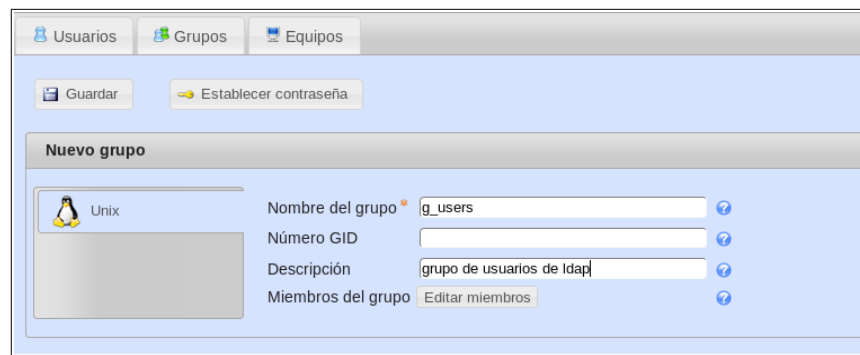
UT 3 – Gestión de usuarios. NFS y LDAP.

Por otra parte, en la parte de derecha de la pantalla hay un botón llamado Vista en Árbol”, el cual es muy interesante ya que nos permite visualizar el árbol de objetos del directorio LDAP.



A continuación trataremos como buscar crear y eliminar, usuarios, grupos y equipos.

Antes de poder crear usuarios hemos de tener al menos un grupo en LDAP, para ello accederemos a la **pestaña de Grupos** y pulsaremos el botón “nuevo grupo”.

A screenshot of the 'Nuevo grupo' (New group) form in the LDAP management interface. The form has a header with 'Usuarios', 'Grupos', and 'Equipos' tabs. Below the tabs, there are two buttons: 'Guardar' (Save) and 'Establecer contraseña' (Set password). The main form area is titled 'Nuevo grupo'. It contains a section for group details with the following fields: 'Nombre del grupo' (Group name) with the value 'g_users', 'Número GID' (GID number) which is empty, 'Descripción' (Description) with the value 'grupo de usuarios de ldap', and 'Miembros del grupo' (Group members) with a button 'Editar miembros' (Edit members). There is also a small icon of a penguin labeled 'Unix' on the left side of the form.

Hay que indicar que no es necesario indicar un número de GID, el sistema creará el grupo y asignará uno automáticamente.

Seleccionar todos	Nombre del grupo	Número GID	Miembros del grupo
<input type="checkbox"/>	g_admin	10001	
<input type="checkbox"/>	g_users	10000	
Seleccionar todos			

Una vez hecho esto, podremos **crear usuarios**. Para ello accederemos a la **pestaña de usuarios** y veremos una pantalla con un **buscador de usuarios** y un botón para “**crear nuevo usuario**”.

Una vez creado el o los usuarios que queremos incluir en el directorio pulsaremos en el botón “**Nuevo usuario**” e introduciremos sus datos personales en la pestaña **Personal**.

Nuevo usuario

Personal

Unix

Sombra

Nombre

Apellido

Iniciales

Descripción

Dirección

Calle

Oficina de correos

Código postal

Ubicación

Estado

Dirección postal

Dirección registrada

Añadir foto

LAM nos informará en todo momento si cometemos algún error o faltan datos obligatorios.

De la misma forma introduciremos los datos de su cuenta del servidor en la pestaña **Unix**.

Sistemas Operativos en Red

UT 3 – Gestión de usuarios. NFS y LDAP.

The screenshot shows a user configuration window for 'Luis Garcia' with email 'lgarcia@calse.es' and phone number '666666666'. The window is divided into three tabs: 'Personal', 'Unix', and 'Sombra'. The 'Personal' tab is active, showing fields for 'Nombre del usuario' (lgarcia), 'Nombre común' (Luis Garcia), 'Número UID' (empty), 'Gecos' (empty), 'Grupo primario' (g_users), 'Grupos adicionales' (Editar grupos), 'Directorio inicial' (/home/\$user), and 'Intérprete del inicio de sesión' (/bin/bash). Each field has a help icon (?) to its right. There are also red 'X' and green '+' icons next to the 'Nombre común' field.

Como en el caso de los grupos, no es necesario introducir un número de UID, ya que el sistema asignará uno automáticamente.

Hay que indicar que en la parte superior izquierda hay un botón llamado **“Establecer contraseña”**, que permite asignar una contraseña inicial para ese usuario. También puede forzarse al usuario a cambiarla la primera vez que inicie sesión.

The screenshot shows a dialog box titled 'Establecer contraseña'. It contains three input fields: 'Contraseña' (masked with dots), 'Repita la contraseña', and 'Forzar el cambio de contraseña.' (with an unchecked checkbox). Each field has a help icon (?) to its right. At the bottom left, there is a penguin icon and a checked checkbox labeled 'Unix'. At the bottom right, there are three buttons: 'Aceptar', 'Establecer contraseña aleatoria', and 'Cancelar'.

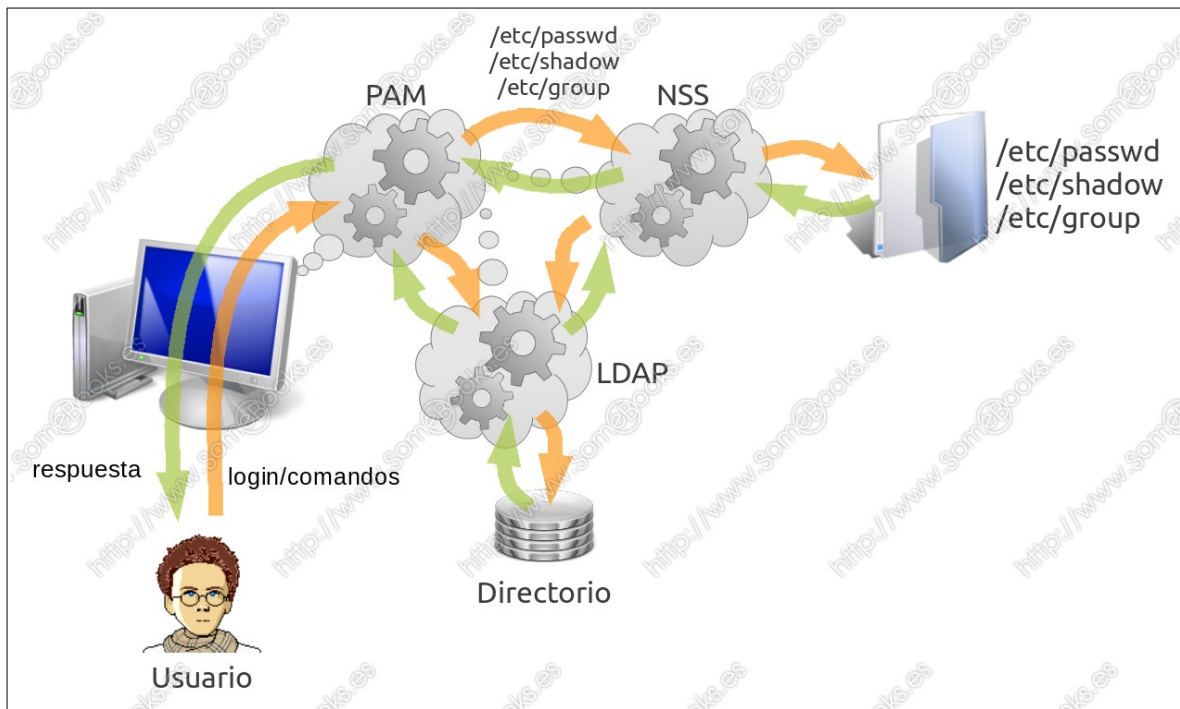
3.2 Instalación del cliente LDAP en sistemas Linux.

Una vez hemos instalado el servidor y creado el directorio con sus unidades organizativas y usuarios, nos queda configurar un equipo cliente para acceder mediante un usuario del dicho directorio.

En este tema realizaremos el proceso usando un equipo cliente con el sistema operativo Ubuntu, aunque podríamos haber usado cualquier otro sistema Linux.

Para comenzar, hemos de instalar una serie de paquetes:

- **libnss-ldap**: Permitirá que NSS obtenga de LDAP información administrativa de los usuarios (Información de las cuentas, de los grupos, información de la máquina, los alias, etc.).
NSS (Name Service Switch) es un protocolo que permite la resolución de nombres de usuario y contraseñas (o grupos) mediante el acceso a diferentes orígenes de información.
En condiciones normales, esta información se encuentra en los archivos locales del sistema operativo, en concreto en /etc/passwd, /etc/shadow y /etc/group, pero puede proceder de otras fuentes, como DNS (Domain Name System), NIS (Network Information Service), LDAP (Lightweight Directory Access Protocol) o WINS (Windows Internet Name Service).
- **libpam-ldap**: Que facilitará la autenticación con LDAP a los usuarios que utilicen PAM.
PAM (Pluggable Authentication Modules) es un protocolo que establece una interfaz entre los programas de usuario y distintos métodos de autenticación. De esta forma, el método de autenticación se hace transparente para los programas.
- **ldap-utils**: Facilita la interacción con LDAP desde cualquier máquina de la red.

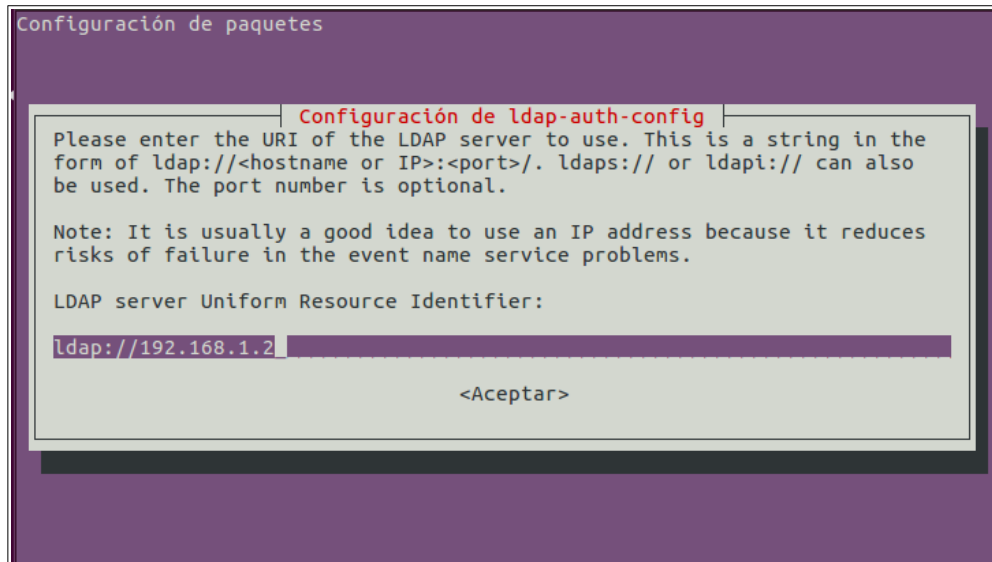


Para instalarlos todos en una sola orden, abrimos una consola y ejecutamos el siguiente comando:

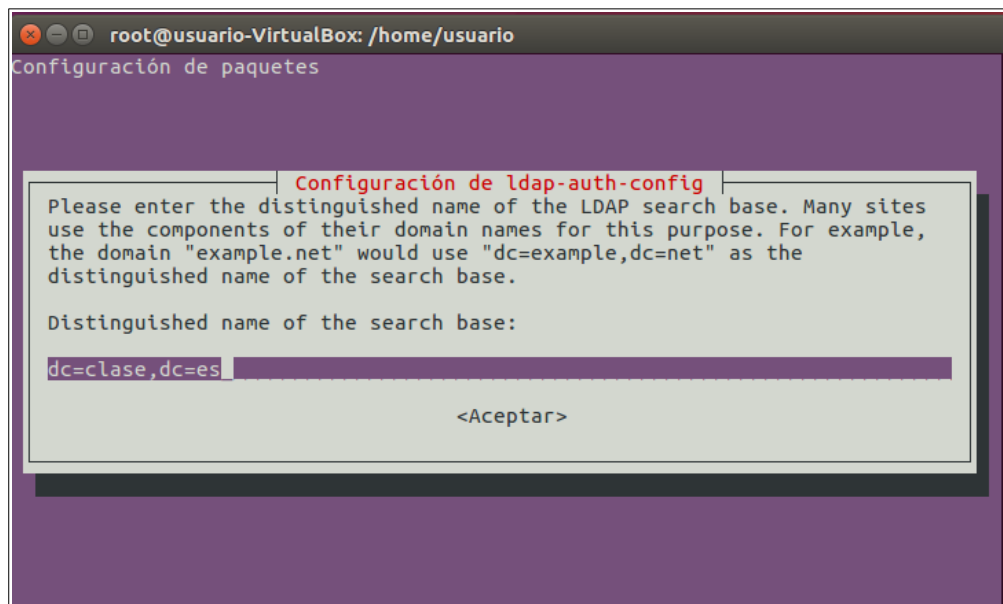
```
sudo apt-get install libnss-ldap libpam-ldap ldap-utils nscd nfs-common
```

El sistema solicitará una serie de datos de configuración:

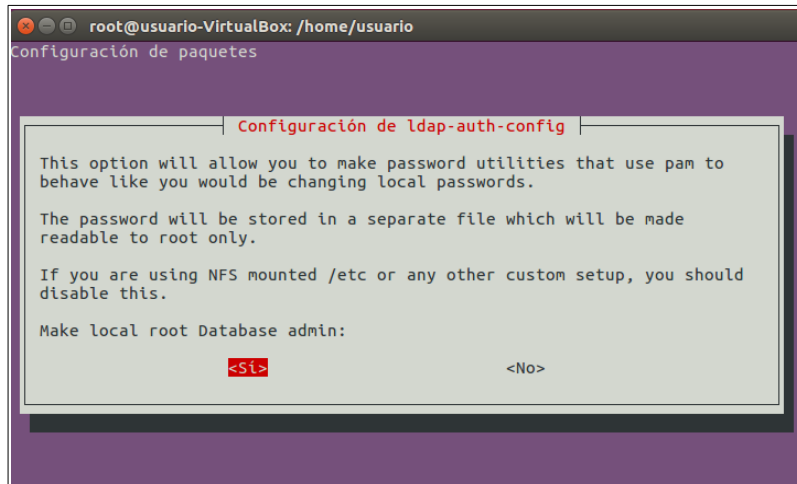
- **La dirección IP del servidor LDAP.** En este apartado hemos de cambiar el protocolo por defecto ldapi por ldap. Además hemos de asegurarnos de quitar una de las tres '/' que el sistema pone en la dirección.



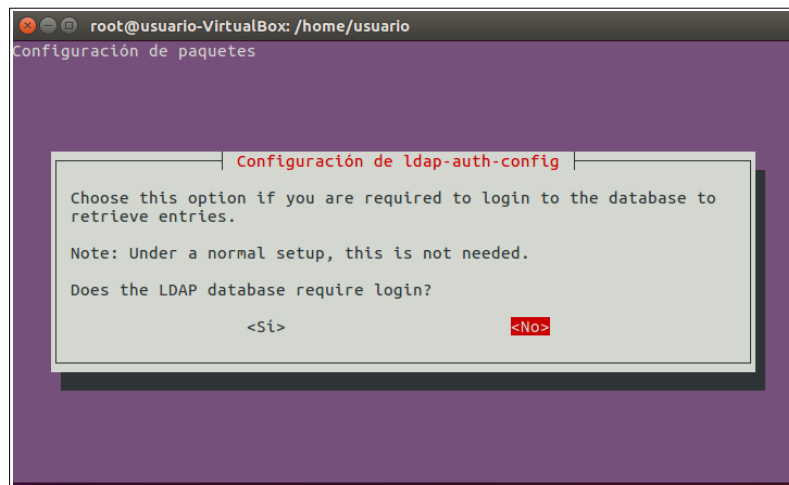
- **El nombre del dominio (*Distinguished Name – DN*).**



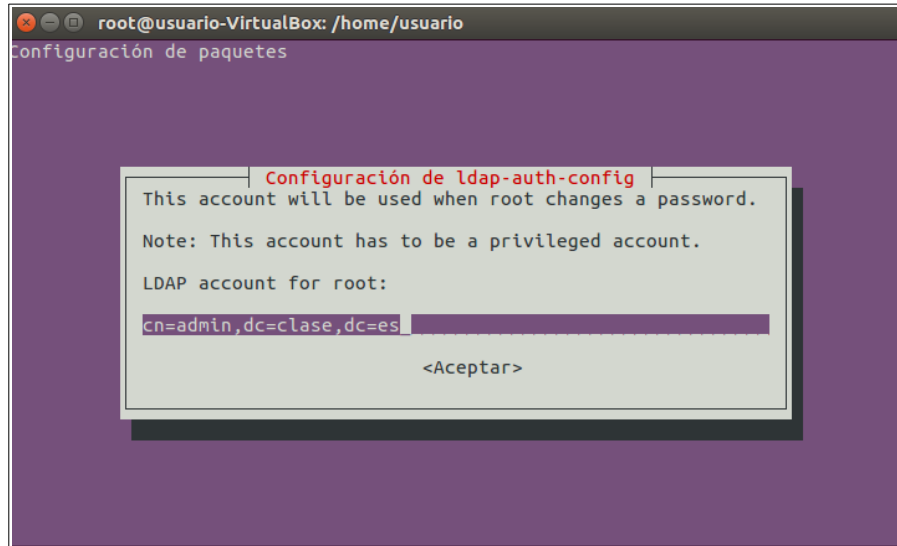
- **La versión del protocolo LDAP** (elegiremos versión 3).
- **Si las utilidades que utilicen PAM deberán comportarse del mismo modo que cuando cambiamos contraseñas locales.**
Esto hará que las contraseñas se guarden en un archivo independiente que sólo podrá ser leído por el superusuario. Elegiremos **Si**.



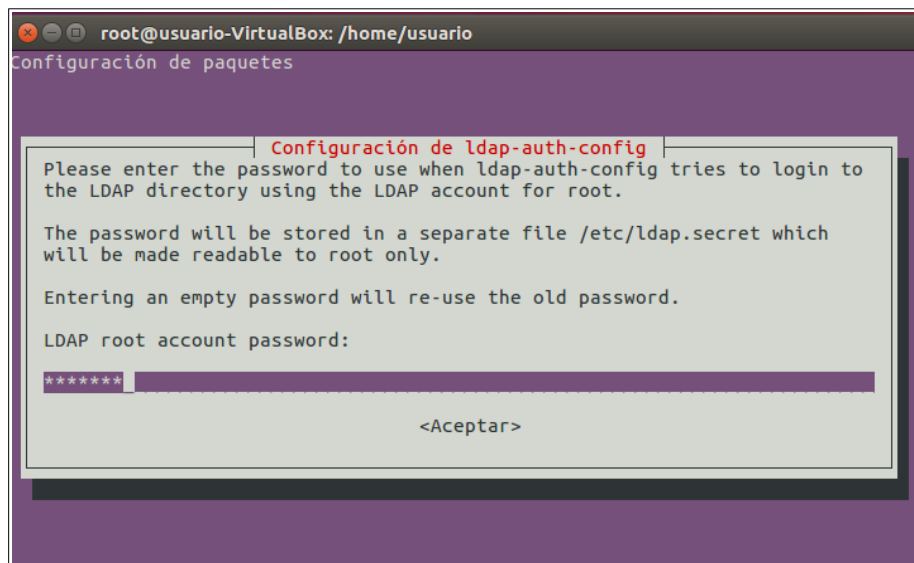
- **Si queremos que sea necesario identificarse para realizar consultas en la base de datos de LDAP.** Elegiremos **No**.



- **El nombre de la cuenta LDAP que tendrá privilegios para realizar cambios en las contraseñas.** Como antes, deberemos escribir un nombre global único (Distinguished Name – DN), sustituyendo el valor predeterminado que nos ofrece (cn=manager,dc=example,dc=net) por que usamos en la configuración del servidor (**cn=admin,dc=clase,dc=es**)



- **La contraseña del administrador del servidor LDAP.** Debe de coincidir con la que usa el administrador LDAP del servidor.



Una vez introducida esta información, habremos acabado la instalación del cliente LDAP, no obstante, en caso de error, **podemos volver a introducir dichos datos ejecutando** el comando: **sudo dpkg-reconfigure ldap-auth-config**

Seguidamente es conveniente asegurarnos de que tanto el cliente como el servidor está en la misma subred y pueden comunicarse. En caso de usar máquinas virtuales, pondremos ambas con una IP fija y en configuración de tipo “red interna”.

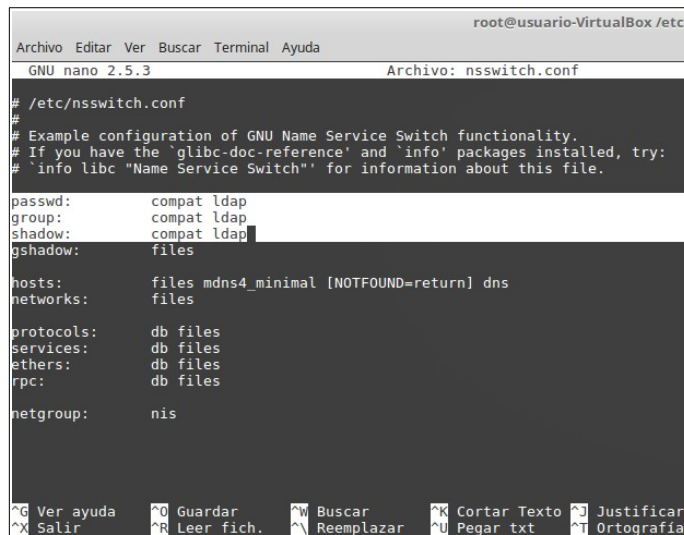
Utilizaremos el comando **ping** para verificar la conexión.

Por último, para que el sistema LDAP funcione correctamente **hemos de modificar algunos de los ficheros de configuración del sistema:**

- **Fichero /etc/nsswitch.conf**

En el archivo **/etc/nsswitch.conf** se incluyen las fuentes desde las que se obtiene la información del servicio de nombres en diferentes categorías y en qué orden. Cada categoría de información se identifica bajo un nombre.

Hemos de editar el archivo, **localizar las líneas que comienzan por passwd, group y shadow y escribir ldap al final de cada una de ellas.** Con esto indicamos el nuevo origen para autenticar las cuentas.



```
root@usuario-VirtualBox /etc
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.5.3 Archivo: nsswitch.conf
# /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
gshadow: files

hosts: files mdns4_minimal [NOTFOUND=return] dns
networks: files

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

netgroup: nis

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Texto ^J Justificar
^X Salir ^R Leer fich. ^N Reemplazar ^U Pegar txt ^I Ortografía
```

- **Fichero `/etc/pam.d/common-password`**

El archivo **`/etc/pam.d/common-password`** proporciona un conjunto común de reglas PAM para la comprobación de contraseñas. En particular, la línea 23 contiene la opción **`use_authok`**, que impide utilizar un segundo método de autenticación cuando ya ha sido aplicado otro anterior, aunque éste haya sido insatisfactorio.

Para evitar este comportamiento, deberemos eliminar la opción `use_authok` de la citada línea 23 del archivo.

```
# here are the per-package modules (the "Primary" block)
password      [success=2 default=ignore]      pam_unix.so obscure sha512
password      [success=1 user_unknown=ignore default=die]      pam_ldap.so use_authok try_first_pass
# here's the fallback if no module succeeds
password      requisite                        pam_deny.so
```

- **Fichero `/etc/pam.d/common-session`**

El archivo **`/etc/pam.d/common-session`** ofrece un conjunto de reglas PAM para el inicio de sesión, tanto si éste es interactivo como si es no interactivo. Aquí será donde indiquemos que **se debe crear un directorio home durante el primer inicio de sesión**, también para los usuarios autenticados mediante LDAP.

Este comportamiento lo conseguiremos añadiendo al final del archivo la siguiente línea:

`session required pam_mkhomedir.so skel=/etc/skel umask=077`

```
session optional      pam_systemd.so
session required      pam_mkhomedir.so skel=/etc/skel umask=077
# end of pam-auth-update config
```

Por último, solo queda reiniciar el equipo y comprobar que todo funciona correctamente. Para ello entraremos en una consola modo texto, pulsando CTRL + ALT + F1 o CTRL derecho + F1 (si estamos usando una máquina virtual) y probaremos a validarnos con un usuario del directorio LDAP.

```
cliente1 login: pperez
Password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Pueden actualizarse 311 paquetes.
146 actualizaciones son de seguridad.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Creating directory '/home/pperez'.
pperez@cliente1:~$ _
```

En esta imagen podemos comprobar varias cosas:

- Que nos encontramos en el equipo cliente.
- Que estamos iniciando sesión con un usuario LDAP.
- Que durante el inicio de sesión se crea el directorio /home para la cuenta.
- Que el inicio de sesión se produce satisfactoriamente.

Podemos acceder también como este usuario usando el modo gráfico, pero debido al funcionamiento del entorno gráfico de sesiones de Ubuntu, hemos de acceder la primera vez usando una consola en modo texto. En caso contrario no nos aparece el usuario en la lista de usuarios en la pantalla de login.

3.3 Instalación del cliente LDAP en sistemas Windows.

Hasta este punto hemos visto como instalar un servidor Debian con OpenLDAP y a configurar un cliente Linux para que realice la autenticación de usuarios por medio de dicho servidor. No obstante, OpenLDAP permite la conexión también desde clientes Windows.

Para permitir este método de autenticación, no es necesario realizar ninguna tarea en el servidor, simplemente realizaremos las siguientes tareas en los equipos Windows cliente:

1. **Instalar el software pGina.**

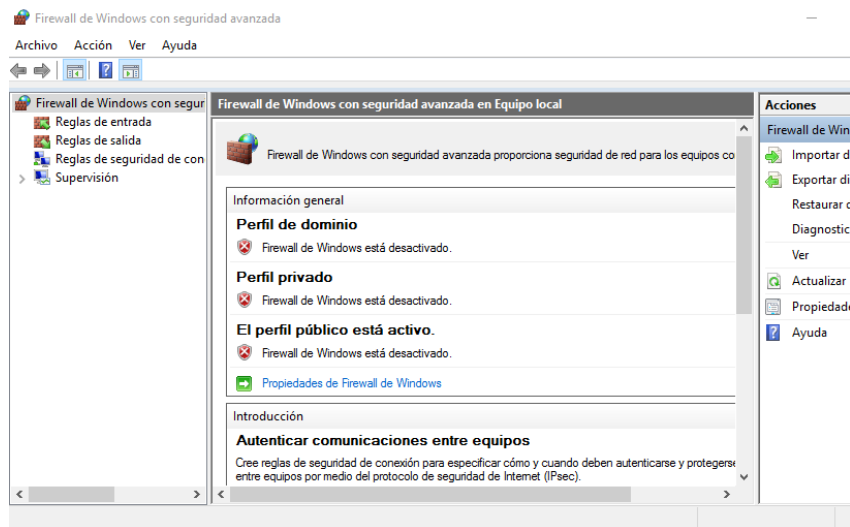
Pgina es un demonio de autenticación que permite realizar la validación de usuarios mediante múltiples protocolos. En nuestro caso lo usaremos para permitir la conexión con un servidor OpenLDAP.

Podemos descargar este programa desde <http://pgina.org/download.html>

2. **Configurar el equipo Windows de forma que tenga conexión con el servidor Linux de OpenLDAP.**

En este punto es conveniente **deshabilitar el Firewall de Windows**.

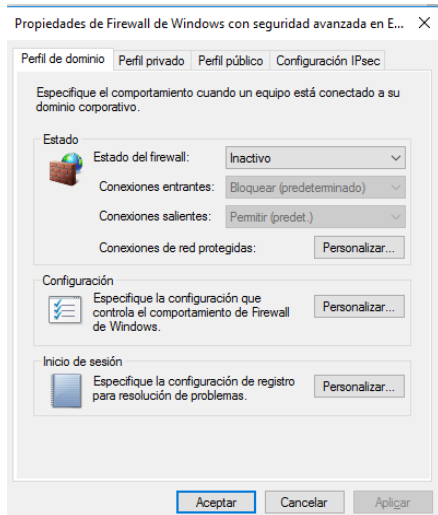
Para ello accederemos a las propiedades del Firewall de Windows y pulsaremos e link “**Propiedades de Firewall de Windows**”



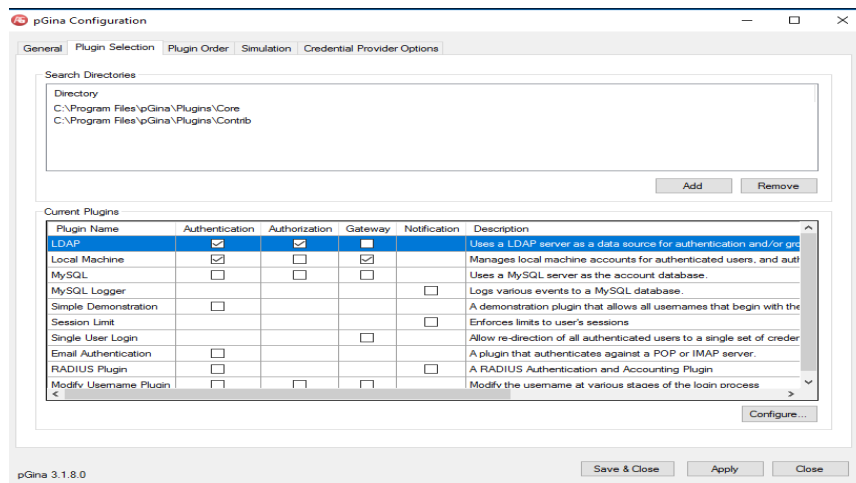
Sistemas Operativos en Red

UT 3 – Gestión de usuarios. NFS y LDAP.

Una vez hecho esto lo inactivaremos en las pestañas de “Perfil de dominio”, “Perfil privado” y “Perfil publico”.



3. **Configurar el demonio pGina.** Para ello ejecutaremos dicho programa y accederemos a la pestaña “Plugin selection”



Aquí pulsaremos en las opciones “**Authentication**” y “**Authorization**” del protocolo LDAP y seguidamente en el botón “**Configure**”.

4. En esta pantalla hemos de rellenar los siguientes campos:

- **LDAP Hosts.-** Pondremos la IP del servidor LDAP.
- **Group DN Pattern.-** Indicaremos el formato del DN de los grupos en el servidor LDAP. En nuestro ejemplo: `cn=%g,ou=grupos,dc=clase,dc=es`
- **User DN Pattern.-** Indicaremos el formato del DN de los usuarios en el servidor LDAP. En nuestro ejemplo: `cn=%u,ou=usuarios,dc=clase,dc=es`

LDAP Plugin Settings

LDAP Server

LDAP Host(s) 192.168.0.5

LDAP Port 389 Timeout 10 ☐ Use SSL ☐ Validate Server Certificate

SSL Certificate File

Search DN

Search Password ☐ Show Text

Group DN Pattern cn=%g,ou=grupos,dc=clase,dc=es Member Attribute memberUid

Authentication Authorization Gateway

☐ Allow Empty Passwords

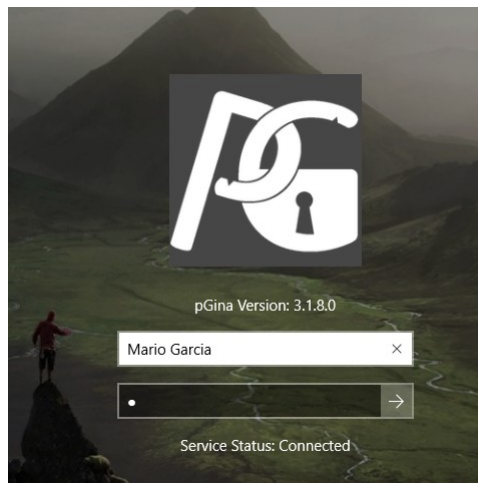
User DN Pattern cn=%u,ou=usuarios,dc=clase,dc=es

☐ Search for DN

Search Filter

Search Context(s)

5. Una vez hecho esto, podremos validarnos usando LDAP, con el nombre común (cn) de nuestros usuarios LDAP.



4. Configurar perfiles móviles con LDAP y NFS.

En muchas empresas u organizaciones, los apartados anteriores pueden plantear más dudas que soluciones, ya que un usuario que vaya cambiando entre varios equipos cliente acabará teniendo una carpeta para su perfil en cada uno de los equipos y su contenido no se sincroniza. Es decir, si crea un archivo en el cliente A, no lo encontrará en su carpeta cuando inicie sesión desde el cliente B. El motivo es que LDAP sólo se encarga de autenticar a los usuarios.

Para solucionar esto usaremos una solución que combine **LDAP** con un servidor de almacenamiento **NFS (Network File System)**.

El resultado serán los perfiles móviles de usuario. Es decir, los datos de la carpeta personal de los usuarios se almacenarán en el servidor central por medio de NFS y serán accesibles en los equipos cliente cuando un usuario entre en alguno de ellos.

4.1 Instalación de NFS.

NFS (Network File System) es un protocolo que El **Network File System** (*Sistema de archivos de red*), o **NFS**, es un protocolo de nivel de aplicación, según el modelo OSI. Es utilizado para sistemas de archivos distribuidos en un entorno de red de computadoras de área local. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratara de locales.

Hay que indicar, que la instalación y configuración de NFS no es un tema que trataremos en este módulo, no obstante, estudiaremos los conceptos básicos que necesitamos para realizar las tarea que nos interesa.

Para llevar a cabo la instalación de NFS seguiremos los siguientes pasos:

1. **Instalar los paquetes de nfs en el servidor**

Para ello ejecutaremos el comando:

```
sudo apt-get install nfs-common nfs-kernel-server
```

2. **Configurar NFS.**

Antes de arrancar el servicio NFS, es necesario indicar qué carpetas deseamos compartir y si queremos que los usuarios accedan con **permisos de solo lectura o de lectura y escritura**. También existe la posibilidad de establecer desde qué ordenadores es posible conectarse. Estas opciones se configuran en el archivo `/etc/exports`

En cada línea del archivo de configuración del servidor NFS `/etc/exports`, se puede especificar:

- La carpeta que se quiere compartir.
- El modo en que se comparte. Las principales opciones son:
 - ro → solo lectura. Opción por defecto.
 - rw → lectura y escritura.

- secure → Esta señal insiste en requerir que se haga desde un puerto origen reservado, por ejemplo, uno que sea menor que 1.024. Esta señal está puesta por omisión.
- insecure → Esta señal revierte el efecto de la señal *secure*.
- root_squash → Esta característica de seguridad deniega a los superusuarios en los hosts especificados cualquier derecho de acceso especial. Este uid debe ser asociado con el usuario nobody.
- no_root_squash → Esta opción está habilitada por omisión, así los superusuarios tienen acceso de supervisor a los directorios exportados de su sistema.
- link_relative → Esta opción convierte los enlaces simbólicos absolutos (donde el contenido del enlace comienza con un slash) en enlaces relativos. Esta opción sólo tiene sentido cuando está montado el sistema de ficheros entero de un anfitrión; por otra parte, algunos de los enlaces podrían apuntar a ninguna parte, o peor aún, a ficheros que nunca debieran apuntar. Esta opción está habilitada de forma predeterminada.
- link_absolute → Esta opción deja todos los enlaces simbólicos como son (la conducta normal para los servidores de NFS suministrados por Sun).
- map_identity → Esta opción le indica al servidor asumir que el cliente usa el mismo uid y gid que el servidor. Esta opción está habilitada por omisión.
- map_daemon → Esta opción indica al servidor de NFS asumir que el cliente y el servidor no comparten el mismo espacio uid/gid. **rpc.nfsd** entonces construye una lista que mapea los IDs entre cliente y servidor preguntando al demonio **rpc.ugidd** del cliente.
- anonuid y anongid → Estas opciones le permiten especificar el uid y el gid de la cuenta anónima. Esto es útil si tiene un volumen exportado para montajes públicos.

- subtree_check y no subtree_check → con subtree_check, si se exporta un subdirectorio (no un filesystem completo) el servidor comprueba que el fichero solicitado por el cliente esté en el subdirectorio exportado; con no_subtree_check (opción por defecto) se deshabilita ese chequeo.
- sync y async → Con sync (modo síncrono) se requiere que todas las escrituras se completen antes de continuar; es opción por defecto. En el caso de async (modo asíncrono). No requiere que todas las escrituras se completen. Es un sistema más rápido, pero puede provocar pérdida de datos en una caída del ordenador.
- Desde qué PC o PCs se permite el acceso (nombre o IP del PC o rango de direcciones IP).

A continuación se adjunta un ejemplo del archivo `/etc/exports` para configurar algunas carpetas compartidas

// Ejemplo de archivo `/etc/exports` de configuración del servidor NFS:

```
# Compartir la carpeta home del servidor
# en modo lectura y escritura y accesible desde la red 192.168.0.0/24
/home 192.168.0.0/255.255.255.0(rw)

# Compartir carpeta tmp a todos como 'solo-lectura'
/tmp *(ro)

# Compartir carpeta /var/log a un PC como 'solo-lectura'
/var/log 192.168.0.211(ro)
```


4.2 Configuración de perfiles móviles.

Por último, en este apartado, trataremos el proceso necesario para integrar la validación LDAP con el almacenamiento remoto de ficheros que ofrece NFS, para implementar los perfiles móviles en los usuarios LDAP.

Los pasos a seguir son los siguientes:

- 1. Instalar los paquetes de NFS en el servidor.**

Como vimos anteriormente, ejecutaremos el comando:

```
# apt-get install nfs-common nfs-kernel-server
```

- 2. En caso de usar una máquina virtual, configuramos el cliente con IP fija y red interna.** Nos aseguraremos que se conecta con el servidor LDAP por medio del comando **ping**.

- 3. Crear una carpeta para guardar los perfiles en el servidor.**

Además hemos de poner como propietario al usuario nobody y al grupo nogroup.

```
# mkdir /moviles  
# chown nobody:nogroup /moviles
```

- 4. Configurar NFS en el servidor para que la carpeta /moviles se comparta a todos los equipos de la red.**

Para ello añadiremos al fichero **/etc/exports** la línea:

```
/moviles *(rw,sync,no_root_squash,no_subtree_check)
```

Y reiniciamos el servicio nfs:

```
# service nfs-kernel-server restart
```

- 5. Ya en el equipo cliente, creamos una carpeta para almacenar los perfiles móviles.**

Para ello ejecutamos los comandos:

```
sudo mkdir /moviles  
sudo chmod a+rwX /moviles
```

6. Instalamos en el cliente los paquetes de nfs.

Concretamente ejecutaremos el comando:

```
# apt-get install nfs-common
```

7. Se modifica el sistema cliente para montar en el arranque, la carpeta / moviles del servidor en la carpeta local /moviles.

Para hacer esto modificamos el fichero /etc/fstab del cliente. En nuestro ejemplo, hemos de añadir:

```
192.168.1.2:/moviles    /moviles    nfs  
auto,noatime,nolock,bg,nfsvers=3,intr,tcp,actimeo=1800 0 0
```

Una vez hecho esto deberemos reiniciar el cliente.

8. Por último, en el servidor debemos indicar en el usuario LDAP la carpeta donde tendrá su perfil en el cliente.

Para ello usaremos la herramienta **LDAP Account Manager**. Solo hemos de acceder a la propiedad “**Directorio inicial**” de cada usuario e indicar que el home de ese usuario debe estar dentro de la carpeta /movies.

The screenshot shows the LDAP Account Manager web interface for user 'Mario Garcia' (mgarcia@calse.es). The interface is divided into a left sidebar with 'Personal', 'Unix', and 'Sombra' tabs, and a main configuration area. The 'Personal' tab is active, showing fields for 'Nombre del usuario' (mgarcia), 'Nombre común' (Mario Garcia), 'Número UID' (10000), 'Gecos', 'Grupo primario' (gusers), 'Grupos adicionales' (with an 'Editar grupos' button), 'Directorio inicial' (/moviles/mgarcia), 'Intérprete del inicio de sesión' (/bin/bash), and 'Contraseña' (with 'Bloquear contraseña' and 'Quitar contraseña' buttons). Each field has a help icon (question mark) to its right.

Si hemos seguido todos los pasos correctamente, el usuario tendrá configurado un perfil móvil, con lo que podrá acceder a sus archivos de su carpeta home, desde cualquier equipo conectado al servidor LDAP.