

2015

# Autenticación LDAP

Grado Superior en administración de sistemas informáticos en red



## Índice

<b>Índice</b>	<b>1</b>
<b>Introducción y Justificación</b>	<b>2</b>
<b>Objetivos</b>	<b>3</b>
<b>Conclusión y valoración personal</b>	<b>5</b>
<b>Administración del servidor</b>	<b>6</b>
<b>Instalación y configuración OpenLDAP en servidor Ubuntu</b>	<b>6</b>
Pasos a seguir	6
<b>Uso de interfaz web para gestionar usuarios y grupos en el servidor OpenLDAP</b>	<b>11</b>
Pasos a seguir	11
<b>Administración del cliente</b>	<b>15</b>
<b>Configuración de un equipo cliente basado en Linux</b>	<b>15</b>
<b>Iniciar sesión gráfica con un usuario LDAP</b>	<b>19</b>
<b>Instalación y configuración del servidor Moodle</b>	<b>20</b>
<b>Bibliografía y fuentes de consulta</b>	<b>22</b>

## Introducción y Justificación

La idea básica a desarrollar partirá de un concepto sencillo: se pretendió unificar los usuarios de la plataforma moodle y de un sistema linux (Ubuntu) teniendo así un usuario para identificarse en los dos lugares y esto es lo que se ha conseguido.

## Objetivos

- Configurar Servidor LDAP.
- Configurar Servidor Moodle.
- Configurar clientes.
- Implementar “radius WIFI” que es un protocolo que nos permitirá poder identificarnos a través de la red wifi, pero esto no ha sido conseguido.
- implementar una base de datos mysql con todos los usuarios reales de modle y así poder trabajar con ellos, pero lo investigado por mí ha sido que existe un plugin para moodle, no oficial, pero que está en desarrollo, pero realmente si se puede realizar ya que mysql es compatible con ldap, este objetivo tampoco ha sido conseguido.

## Análisis del contexto

Para la realización de este proyecto los materiales usados son:

- OpenStack, es un proyecto de computación en la nube para proporcionar una infraestructura como servicio.  
Dentro de openstack tenemos 2 Instancias creadas, un servidor LDAP: “Permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red” y un servidor Moodle “Moodle es una plataforma de aprendizaje diseñada para proporcionarle a educadores, administradores y estudiantes un sistema integrado único, robusto y seguro para crear ambientes de aprendizaje personalizados”
- OpenVPN client, aplicación para realizar una conexión vpn al instituto ya que openstack se encuentra dentro de la red del instituto
- Virtual Box, donde tenemos instalado y configurado el cliente Ubuntu para realizar la comprobación de la autenticación de los usuarios.

## Conclusión y valoración personal

En mi opinión respecto a la elaboración del proyecto Autenticación LDAP logré aprender cómo unificar una cuenta de usuario para dos sistemas totalmente diferentes como es Moodle y un cliente Ubuntu.

Al principio no me gustaba la idea de estar creando nuevos servidores y estar aprendiendo a utilizarlos, pero a medida que estaba trabando con ellos me gustaba más y más lo que hacía y lo que llegaba a conseguir, una pena que no haya podido aprovechar el tiempo para llegar más lejos en el proyecto y así poder completarlo del todo.

El proyecto a primera vista parece otro trabajo del famoso “copia y pega” pero en parte no es así ya que más o menos esta todo explicado con mis palabras, está claro que habrá pasos que serán iguales al del manual que he seguido para realizar este proyecto, eso no se puede remediar, ya que gracias a ese manual he podido lograr lo que tengo.

## Administración del servidor

### Instalación y configuración OpenLDAP en servidor Ubuntu

#### Pasos a seguir:

- Instalación de los paquetes necesarios
- Configuración básica OpenLDAP
- Configuración de la Autenticación de los clientes
- Configuración del demonio SLAPD
- Creación de la estructura del directorio
- Añadir usuarios y grupos
- Comprobación

#### Instalación de los paquetes necesarios:

El proceso de instalación es sencillo, instalaremos dos paquetes, `slapd` y `slapd-utils`, durante la instalación de este paquete lo único importante la contraseña que le pondremos para la administración de LDAP.

#### Configuración básica OpenLDAP:

Lo primero que debemos de tener en cuenta es el nombre de la máquina virtual para que cuando hagamos referencia al nombre del servidor, que en este caso es `"ldapserver.openldap.local ldapserver"` entienda que nos estamos refiriendo a él, añadimos el nombre en el archivo `"/etc/hosts"`. A continuación de esto instalaremos una librería NSS, que ofrece una interfaz para acceder y configurar distintas bases de datos usadas para almacenar cuentas de usuario, lo instalamos a través del paquete `libnss-ldap`. Una vez ejecutada la instalación nos pedirá una serie de pasos, entre ellos está el más importante donde indicaremos la dirección IP del servidor LDAP `"192.168.88.11"`. Entre estos pasos encontraremos cual será el nombre global único `"dc=openldap,dc=local"`, el nombre de la cuenta LDAP que tendrá privilegios `"cn=admin,dc=openldap,dc=local"` y la contraseña de la misma cuenta.

### Configuración de la autenticación de los clientes

Lo primero en realizar es ejecutar un script que nos ayudará a modificar los archivos de configuración de PAM y NSS, para ello ejecutamos el siguiente comando en el terminal:

```
- Auth-client-config -t nss -p lac_ldap
```

Los atributos utilizados en este comando son `-t nss`, en el que indicamos los archivos que vamos a modificar son los correspondientes a NSS y `-p lac_ldap` en el que indicamos que los datos para la configuración debe tomarlos del archivo `lac_ldap`. Cuando ejecutemos este script no debe de ofrecer ningún tipo de error.

A continuación actualizaremos la configuración de las políticas de autenticación de PAM con el siguiente comando:

```
- Pam-auth-update
```

Lo que hacemos con esto es instalar los módulos que queremos usar en nuestro servidor, en nuestro caso instalaremos todos los módulos.

Una vez acabada la configuración en el archivo `/etc/ldap.conf` podremos realizar cambios y comprobar si están bien los datos insertados.

### Configuración del demonio SLAPD

SLAPD es un programa multiplataforma, que se ejecuta en segundo plano, atendiendo las solicitudes de autenticación LDAP que se reciban en el servidor.

Para configurarlo utilizaremos el comando `"dpkg-reconfigure slapd"` y seguiremos los pasos del asistente, no pedirá el nombre de dominio, de la organización y una contraseña, elegiremos el motor de la base de datos que será "HDB" y acabaremos con esta configuración.



### Creación de la estructura del directorio

Una vez configurado el servidor pasaremos a crear la estructura básica, crearemos la estructura jerárquica.

A continuación crearemos un archivo llamado "base.ldif" que contenga los tipos de objeto básicos del directorio, quedará de esta forma:

```
dn: ou=usuarios,dc=openldap,dc=local
objectClass: organizationalUnit
ou: usuarios

dn: ou=grupos,dc=openldap,dc=local
objectClass: organizationalUnit
ou: grupos
```

Una vez configurado el fichero "base.ldif" añadiremos esta información a la base de datos OpenLDAP de esta forma:

```
- ldapadd -x -D "cn=admin,dc=openldap,dc=local" -W -f
  base.ldif
```

## Añadir usuarios y grupos

Se realizará de la misma manera que el paso anterior, esta vez creando un archivo para los usuarios y otro para los grupos, de esta manera:

### Usuarios:

Crearemos el archivo "usuario.ldif" y añadimos la siguiente información, esa información se les añadirá para cada usuario.

```
dn: uid=nsm95,ou=usuarios,dc=openldap,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: nsm95
sn: Salhi
givenName: Nabil
cn: Nabil Salhi
displayName: Nabil Salhi
uidNumber: 1000
gidNumber: 10000
userPassword: alumno
gecos: Nabil Salhi
loginShell: /bin/bash
homeDirectory: /home/nsm95
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: nsm9595@gmail.com
postalCode: 29000
o: openldap
initials: Ns
```

Una vez configurado el fichero "usuario.ldif" añadiremos esta información a la base de datos OpenLDAP de esta forma:

- ldapadd -x -D "cn=admin,dc=openldap,dc=local" -W -f usuario.ldif

### Grupos:

Crearemos el archivo "grupo.ldif" y añadimos la siguiente información, esa información se les añadirá para cada usuario.

```
dn: cn=Grupo,ou=grupos,dc=openldap,dc=local
objectClass: posixGroup
cn: Grupo
gidNumber: 10000
```

Una vez configurado el fichero "grupo.ldif" añadiremos esta información a la base de datos OpenLDAP de esta forma:

```
- ldapadd -x -D "cn=admin,dc=openldap,dc=local" -W -f
  grupo.ldif
```

### Comprobación:

Para saber si todo es bien redactado y que el contenido anterior se ha añadido correctamente realizamos una búsqueda del usuario creado con el siguiente comando y nos tendrá que mostrar los detalles del usuario:

```
root@ldapservers:~# ldapsearch -xLLL -b "dc=openldap,dc=local" uid=nsm95 givenName cn
dn: uid=nsm95,ou=usuarios,dc=openldap,dc=local
givenName: Nabil
cn: Nabil Salhi
```

## Uso de interfaz web para gestionar usuarios y grupos en el servidor OpenLDAP

### Pasos a seguir:

- Instalación
- Acceso al servidor a través de phpLDAPAdmin
- Añadir usuarios con phpLDAPAdmin
- Añadir grupos con phpLDAPAdmin

Existe 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 web. Este cliente es phpLDAPAdmin.

phpLDAPAdmin dispone de una vista con forma de árbol jerárquico que permite recorrer toda la estructura del directorio. Además, incorpora funciones de búsqueda avanzadas que lo convierten en una herramienta intuitiva para consultar y administrar el directorio LDAP.

### Instalación

Instalamos el paquete a través del terminal con el siguiente comando:

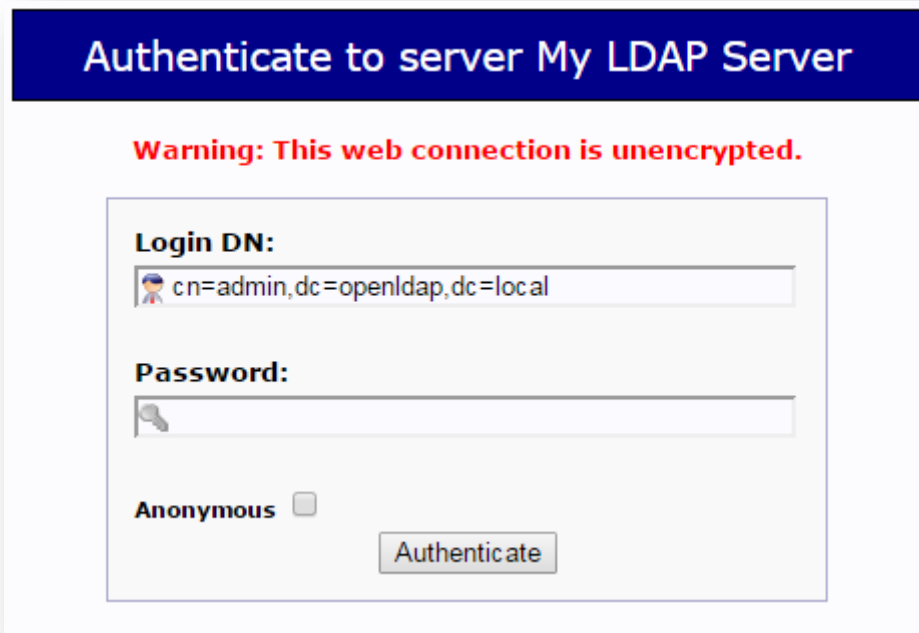
- `apt-get install phpldapadmin -y`

### Acceso al servidor a través de phpLDAPAdmin

Accederemos a phpLDAPAdmin a través de nuestro navegador de esta forma:



Si todo ha ido correctamente nos aparecerá la pantalla principal de phpLDAPadmin. Nada más comenzar a usar phpLDAPadmin nos encontramos con un inicio de sesión algo raro ya que iniciamos sesión con el nombre global único de nuestro servidor:



**Authenticate to server My LDAP Server**

**Warning: This web connection is unencrypted.**

**Login DN:**  
cn=admin,dc=openldap,dc=local

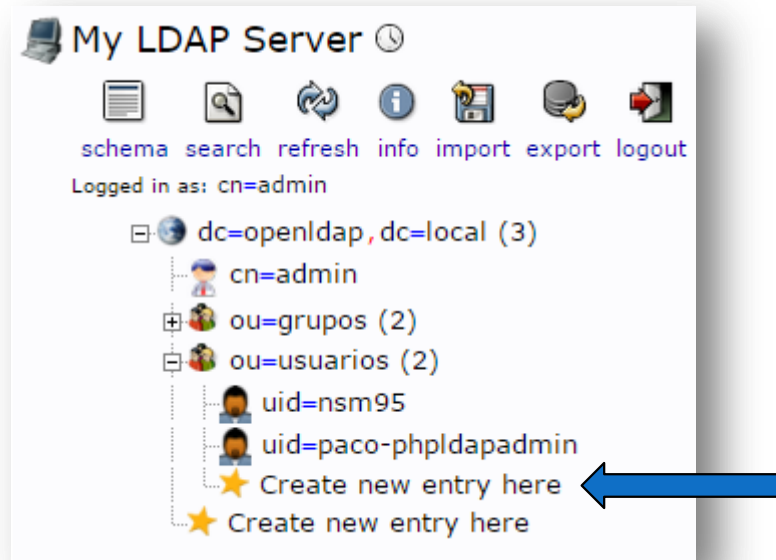
**Password:**

**Anonymous** ☐

**Authenticate**

## Añadir usuarios con phpLDAPAdmin

Después de identificarnos, accedemos al menú que tenemos a la izquierda, entramos en la sección usuarios y dentro crear nueva entrada:



Una vez hecho esto nos cambiará el panel de la derecha y escogeremos la opción “predeterminado”, a continuación nos aparecerá un desplegable para escoger los tipos de objetos a los que pertenecerá el usuario, seleccionamos “account” y “posiAccount”.

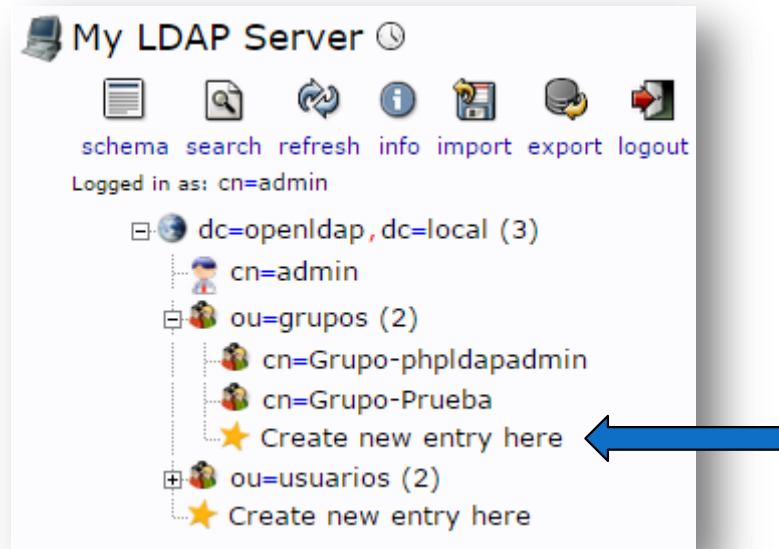
De nuevo cambiará el panel derecho y llegamos a la parte donde rellenar los datos de usuario, al crear por primera vez un usuario no me aparecía el botón de crear objeto que se sitúa al final de la página con lo cual no me dejaba crear ningún usuario, buscando en internet encontré el siguiente error a solucionar:

- En phpLDAPAdmin a la hora de crear un usuario no te deja crear el objeto, investigando he encontrado que en el archivo `/usr/share/phpldapadmin/lib/TemplateRender.php` en la línea 2470 cambiar `password_hash` por `password_hash_custom` y de esta manera funcionará.

Por último aparecerá un resumen del usuario verificando si lo que hemos escrito sobre él es correcto y así crear el usuario dándole al botón “cometer”.

### Añadir grupos con phpLDAPAdmin

Lo pasos son más o menos parecidos como los de crear un usuario, en vez de dirigirnos a la pestaña de usuarios vamos a la de grupos:



Nos cambiará el panel de la derecha y escogeremos la opción “predeterminado”, a continuación nos aparecerá un desplegable para escoger los tipos de objetos a los que pertenecerá el grupo, seleccionamos “posixGroup” y rellenamos los campos requeridos para la creación del grupo.

Esta herramienta solo nos vale para archivos con extensión lidif ya que solo nos permite importar bases de datos con ese tipo de extensión.

## Administración del cliente

### Configuración de un equipo cliente basado en Linux

#### Pasos a seguir:

- **Instalación de los paquete**
- **Ajustes en los archivo de configuración**
- **Actualizar NSS y configurar PAM**
- **Un último ajuste**

#### Instalación de los paquetes:

Lo que haremos en este apartado será explicar cómo configuraremos un equipo Ubuntu para poder autenticarse a través del servidor LDAP, utilizamos una máquina virtual creada en Virtual box ya que en OpenStack surgían fallos a medidas que iba trabajando en ella.

Para comenzar tendremos que instalar una serie de paquetes que necesitará el cliente para poder conectarse y facilitar la autenticación, todo esto se hará través de un asistente:

El primer paso será indicar la dirección ip de nuestro servidor de esta forma:

- `"ldapi:///192.168.5.128"`

Segundo paso será indicar el nombre global único:

- `"dc=openldap,dc=local"`

Tercer paso, elegir la versión del protocolo LDAP, seleccionaremos la versión 3

Cuarto paso deberemos indicar el nombre del administrador, el nombre global único y la contraseña:

- `"cn=admin,dc=openldap,dc=local"`

Con esto tenemos la configuración básica del cliente LDAP.



### Ajustes en los archivo de configuración:

Para completar la instalación deberemos editar 3 ficheros en nuestro cliente, estos ficheros son:

- /etc/ldap.conf
- /etc/ldap/ldap.conf
- /etc/nsswitch.conf

Comencemos por editar el fichero /etc/ldap.conf:

En el fichero tendremos que realizar una serie de búsquedas y esas búsquedas editarlas.

La primera búsqueda será la línea `"#bind_policy hard"` y sustituirla por `"bind_policy soft"` (Si en algún momento nos encontramos con alguna línea comentada a como en este caso la des comentamos para que la configuración realizada tenga efecto).

La segunda búsqueda será `"pam_password md5"` y la sustituimos por `"pam_password crypt"`.

Tercera y última búsqueda, buscaremos una línea que comience por `"uri ldapi:///192.168.5.128"` y la sustituimos por `"uri ldap:///192.168.5.128"`.

Ahora editaremos el fichero /etc/ldap/ldap.conf:

Este fichero tiene que quedar configurado de esta forma:

```
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE      dc=openldap,dc=local
URI       ldap:///ldap.openldap.local

SIZELIMIT      0
TIMELIMIT      0
DEREF          never

# TLS certificates (needed for GnuTLS)
TLS_CACERT     /etc/ssl/certs/ca-certificates.crt
```

Y por último configuraremos el archivo “/etc/nsswitch.conf”

Accederemos al fichero y tendrá que quedar de esta forma:

```
# /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:      files ldap
group:       files ldap
shadow:      files ldap

hosts:       files dns
networks:    files

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

netgroup:    nis
```

### Actualizar NSS y configurar PAM

Una vez realizada toda la configuración para saber si está conectado el cliente con el servidor realizamos este comando que lo que haces es actualizar la base de datos con usuarios y grupos que contiene en LDAP, de esta manera sabemos que estamos accediendo al servidor:

```
root@localhost:~# nss_updatedb ldap
passwd... done.
group... done.
root@localhost:~# clear
```

Una vez echa esta comprobación para estar seguro de ello lo que hacemos es ejecutar el comando “getent passwd” y veremos los usuarios creados en el servidor:

```
alumno:x:1000:1000:alumno,,,:/home/alumno:/bin/bash
sshd:x:116:65534::/var/run/sshd:/usr/sbin/nologin
xrdp:x:117:125::/var/run/xrdp:/bin/false
nsm95:x:1000:10000:Nabil Salhi:/home/nsm95:/bin/bash
paco-phpldapadmin:*:1001:10001:paco:/home/paco:/bin/bash
root@localhost:~#
```

**Un último ajuste:**

El cliente ya está listo para autenticarnos con una cuenta del servidor LDAP, pero si lo hacemos con un usuario creado en el servidor nos dará un error ya que no encontrará la carpeta en /home/, podemos crear la carpeta a mano, pero lo tendríamos que realizar con todos los usuarios creados, por eso haremos que se cree automáticamente cuando iniciemos sesión con un nuevo usuario, lo conseguiremos de la siguiente manera:

Nos dirigimos al archivo `/etc/pam.d/common-session` del cliente y lo editamos, añadiremos una nueva línea al principio de archivo con este contenido:

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

De esta manera estaría resuelto este problema.

Otra configuración que debemos realizar es permitir que los usuarios LDAP puedan cambiar sus propias contraseñas, para ello deberemos modificar el archivo

`/etc/pam.d/common-password` y retocar una línea:

- Sustituir esta línea:  

```
"password [success=1 user_unknown=ignore
  default=die]pam_ldap.so use_auth tok try_first_pass"
```
- Por esta otra:  

```
"password [success=1 user_unknown=ignore default=die]
  pam_ldap.so"
```

Y ya habremos acabado de configurar el cliente para su conexión con el servidor, con lo que he realizado podemos iniciar sesión a través del terminal, pero no buscamos eso.

## Iniciar sesión gráfica con un usuario LDAP

Lo primero que haremos será cambiar el modo de inicio de sesión de un Ubuntu desktop haciendo que nos pida el nombre de usuario y contraseña, no que escojamos un usuario ya creado en el sistema.

Para ello editamos el fichero `"/etc/lightdm/lightdm.conf"` dentro de ese fichero encontraremos lo siguiente:

```
[SeatDefaults]

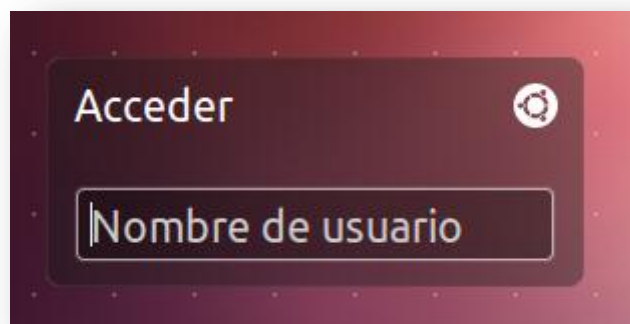
greeter-session=unity-greeter

user-session=Ubuntu
```

Lo que tenemos que hacer es añadir dos nuevas líneas al final del fichero y que quede de esta manera:

```
[SeatDefaults]
greeter-session=unity-greeter
user-session=ubuntu
allow-guest=false ←
greeter-hide-users=true ←
```

Reiniciamos la máquina y ahora cambiará la forma de logearnos, ahora nos pedirá que escribamos el nombre de usuario:

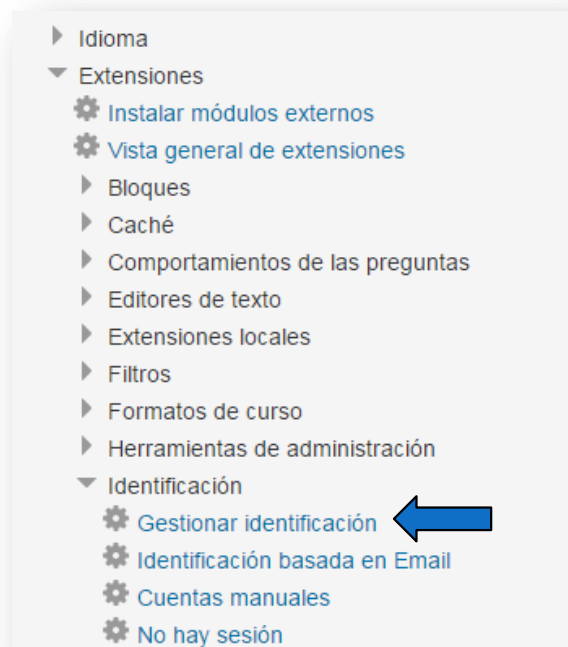


## Instalación y configuración del servidor Moodle:

La instalación de Moodle la realizamos a través del repositorio GIT, recomendado para desarrolladores y aparte hace que las actualizaciones sean más simple y rápidas.

Una vez instalado moodle, accederemos a él a través del navegador y realizaremos la configuración básica como por ejemplo como se llamará el moodle.

Pasamos a la configuración para la unión de moodle con LDAP. Para la configuración nos dirigimos a la siguiente dirección:



Dentro nos aparecerán todos los plugins de identificación disponibles, buscamos “Usar un servidor ldap” y lo habilitamos, el siguiente paso será configurarlo, pero no nos dejará hasta que la instancia del servidor moodle no tengamos php instalado.



Una vez que tengamos instalado php en nuestra instancia podremos configurar la unión de los dos servidores, mi configuración quedará de esta forma:

The screenshot shows the 'Openldap' configuration page in Moodle. The left sidebar contains a navigation menu with options like 'Administración del sitio', 'Notificaciones', 'Registro', 'Características avanzadas', 'Usuarios', 'Cursos', 'Calificaciones', 'Insignias', 'Ubicación', 'Idioma', 'Extensiones', 'Instalar módulos externos', 'Vista general de extensiones', 'Bloques', 'Caché', 'Comportamientos de las preguntas', 'Editores de texto', 'Extensiones locales', 'Filtros', 'Formatos de curso', 'Herramientas de administración', 'Identificación', and 'Gestionar identificación'. The main content area is titled 'Ajustes de servidor LDAP' and includes fields for 'URL del host' (ldap://192.168.88.11), 'Versión' (3), 'Usar TLS' (No), 'Codificación LDAP' (utf-8), and 'Tamaño de página' (250). Below this is the 'Fijar ajustes' section with 'No cachear contraseñas' (No), 'Nombre distinguido' (cn=admin,dc=openldap,dc=local), and a password field. On the right, there is explanatory text about LDAP URLs, protocols, and security.

Cuando accedamos por primera vez con un usuario creado en el servidor ldap nos aparecerá de esta forma, teniendo que rellenar los datos para dar de alta al usuario en moodle:

The screenshot shows the Moodle user registration form for 'Nabil Salhi Mohamed'. The top section displays the user's name and a navigation bar with links to 'Área personal', 'Preferencias', 'User account', and 'Editar perfil'. Below this is a 'NAVEGACIÓN' sidebar with links to 'Área personal', 'Inicio del sitio', 'Páginas del sitio', and 'Cursos'. The main form area is titled 'Nabil Salhi Mohamed' and includes a 'General' section with fields for 'Nombre' (Nabil), 'Apellido(s)' (Salhi Mohamed), 'Dirección de correo' (Cambio pendiente. Abra el enlace enviado en nsm9595@hotmail.com. Cancelar cambio de email), 'Mostrar correo' (Mostrar mi dirección de correo sólo a mis compañeros de curso), 'Ciudad' (Melilla), and 'Seleccione su país' (España).

## Bibliografía y fuentes de consulta

Libro usado para la realización del proyecto:

- <http://somebooks.es/?p=3356>

Documentación de Moodle:

- [https://docs.moodle.org/29/en/Main\\_page](https://docs.moodle.org/29/en/Main_page)