



UNIVERSIDAD LUTERANA SALVADOREÑA
FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA
LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

CATEDRA:

REDES II

TEMA:

Diseñar e implementar un prototipo de protocolo LDAP para la centralización de los usuarios y claves el servicio de entorno de aprendizaje virtual (EVA) que ofrece la Universidad Luterana Salvadoreña.

TÍTULO:

SERVIDOR LDAP

AUTORES:

CARNET	NOMBRE	AUTO-EVALUACIÓN
MM012255	MANUEL ANTONIO MAZANA	10
CP02110469	LUIS MIGUEL CRUZ PEÑATE	10
MM02110895	MANUEL ANTONIO MOLINA MARTINEZ	10

CATEDRÁTICO:

ING. MANUEL FLORES VILLATORO

SAN SALVADOR, 8 NOVIEMBRE DE 2014

Índice de contenido

1. INTRODUCCIÓN.....	1
2. OBJETIVOS.....	2
2.1 General:.....	2
2.2 Específicos:.....	2
3. MARCO TEÓRICO.....	3
3.1 ¿En que consiste un Servidor LDAP?.....	3
3.1.1 Definición de LDAP.....	3
3.2 Open LDAP.....	3
3.2.1 Componentes.....	4
3.3 Moodle.....	4
3.3.1 Características generales de Moodle.....	5
3.3.2 VENTAJAS.....	5
3.3.4 DESVENTAJAS.....	5
3.4 PHPLDAPADMIN.....	6
3.4.1 CARACTERÍSTICAS.....	6
3.5 LAM.....	7
3.5.1 LAM requisitos :.....	7
3.6 JXPLOER.....	8
3.6.1 CARACTERÍSTICAS FUNDAMENTALES.....	8
4. DIAGRAMA DE RED.....	9
5. DESCRIPCIÓN DEL PROYECTO.....	10
6. CRONOGRAMA DE ACTIVIDADES.....	11
7. VIABILIDAD.....	12
7.1 Viabilidad Técnica.....	12
7.2 Viabilidad Económica-Financiera.....	12
8. INSTALACIÓN DE OPEN LDAP.....	13
8.1 configurar paquete slapd.....	13
8.2 Comprobación de la instalación.....	15
9. ADMINISTRACIÓN DEL OPENLDAP.....	16
9.1 Requerimientos previos para instalación de LAM.....	16
9.2 Instalación de LAM (Ldap Accoun Manager).....	17
9.3 Configuración de LAM.....	17
9.4 Crear grupos de usuario.....	22
9.5 Crear usuarios.....	23
10. CONFIGURACIÓN DE MOODLE 2.7.2+.....	26
10.1 Conexión a LDAP.....	26
10.2 Validar usuario de ldap en moodle.....	29
11. BUENAS PRACTICAS.....	31
12. CONCLUSIÓN.....	32
13. BIBLIOGRAFIA.....	33

1. INTRODUCCIÓN

El presente proyecto se desarrollará utilizando OpenLdap, el cual es un software de implementación del protocolo LDAP (Lightweight Directory Acces Protocol) (traducido, Protocolo Ligero de Acceso a Directorios). LDAP hace referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado distribuido para buscar diversa información en un entorno de red. Ldap también se considera una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que puedan dar consultas.

También se utilizarán herramientas para la administración del servidor ldap, phpldapadmin y lam basadas en interfaz web, jxplorer navegador basado en java. Para las pruebas del funcionamiento del servicio será mediante el cms moodle, el cual es utilizado como entorno de aprendizaje virtual para los estudiantes de la Universidad Luterana Salvadoreña.

Así mismo se elaborará la guía de instalación y configuración de las herramientas de software a emplear en el servicio.

2. OBJETIVOS

2.1 General:

- Implementar un prototipo de servidor con protocolo LDAP en un equipo con sistema operativo GNU/LINUX.

2.2 Específicos:

- Investigar las tecnologías que componen un servidor LDAP.
- Implementar y configurar herramientas de administración del servicio LDAP.
- Implementar y configurar moodle para autenticar usuarios por medio del servicio LDAP.
- Desarrollar los procedimientos para la configuración de las herramientas aplicadas.
- Mostrar los recursos a utilizados en la instalación, configuración e implementación del proyecto.

3. MARCO TEÓRICO

3.1 ¿En que consiste un Servidor LDAP?

Si en nuestra red disponemos de un servidor LDAP y configuramos todos los PCs y todos los servicios de la red para que se autentifiquen en él, bastará con crear las cuentas de usuario y grupos de usuarios en nuestro servidor LDAP para que los usuarios puedan hacer uso del sistema y de sus servicios desde cualquier posición de la red. Es un sistema ideal para centralizar la administración de usuarios en un único lugar.

3.1.1 Definición de LDAP

LDAP (Lightweight Directory Access Protocol, Protocolo Ligero de Acceso a Directorios) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

Un servidor LDAP no es más que un gestor de bases de datos jerárquico al contrario que MySQL que es un gestor de bases de datos relacional, pero además su diseño está optimizado para realizar cientos de consultas simultáneas de forma eficiente ya que es la operación más común.

Un árbol de directorio LDAP a veces refleja varios límites políticos, geográficos u organizacionales, dependiendo del modelo elegido. Los despliegues actuales de LDAP tienden a usar nombres de Sistema de Nombres de Dominio (DNS por sus siglas en inglés) para estructurar los niveles más altos de la jerarquía. Conforme se desciende en el directorio pueden aparecer entradas que representan personas, unidades organizacionales, impresoras, documentos, grupos de personas o cualquier cosa que representa una entrada dada en el árbol (o múltiples entradas).

Habitualmente, almacena la información de identificación (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc). A manera de síntesis, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.

3.2 Open LDAP

OpenLDAP es una implementación libre y de código abierto del protocolo Lightweight Directory Access Protocol (**LDAP**) desarrollada por el proyecto OpenLDAP.

Está liberada bajo su propia licencia [OpenLDAP Public License](#). LDAP es un protocolo de comunicación independiente de la plataforma.

Muchas distribuciones GNU/Linux incluyen el software OpenLDAP para el soporte **LDAP**. Este software también corre en plataformas BSD, AIX, HP-UX, Mac OS X, Solaris, Microsoft Windows

(NT y derivados, incluyendo 2000, XP, Vista), y z/OS.

3.2.1 Componentes

Básicamente, OpenLDAP posee tres componentes principales:

- slapd -Dominio de servidor y herramientas
- Bibliotecas que implementan el protocolo LDAP
- Programas cliente: ldapsearch, ldapadd, ldapdelete, entre otros

Adicionalmente, el proyecto OpenLDAP es anfitrión de los subproyectos:

- JLDAP - biblioteca de clases LDAP para Java
- JDBC-LDAP - controlador Java JDBC - LDAP
- ldapc++ - biblioteca de clases LDAP para C++

3.3 Moodle

Moodle es una aplicación web de tipo [Ambiente Educativo Virtual](#), un sistema de gestión de cursos, de [distribución libre](#), que ayuda a los educadores a crear comunidades de [aprendizaje en línea](#). Este tipo de plataformas tecnológicas también se conoce como [LCMS \(Learning Content Management System\)](#). La versión más reciente es la 2.7

Moodle fue creado por Martin Dougiamas, quien fue administrador de WebCT en la [Universidad Tecnológica de Curtin](#). Basó su diseño en las ideas del constructivismo en pedagogía que afirman que el conocimiento se construye en la mente del estudiante en lugar de ser transmitido sin cambios a partir de libros o enseñanzas, y en el [aprendizaje colaborativo](#). Un profesor que opera desde este punto de vista crea un ambiente centrado en el estudiante que le ayuda a construir ese conocimiento con base en sus habilidades y conocimientos propios en lugar de simplemente publicar y transmitir la información que se considera que los estudiantes deben conocer.

La primera versión de la herramienta apareció el 20 de agosto de 2002, a partir de allí han aparecido nuevas versiones de forma regular. Hasta julio de 2008, la base de usuarios registrados incluye más de 21 millones, distribuidos en 46.000 sitios en todo el mundo y está traducido a alrededor de 91 idiomas.¹

Estas herramientas son de gran utilidad en el ámbito educativo, ya que permiten a los profesores la gestión de cursos virtuales para sus alumnos ([educación a distancia](#), [educación en línea](#) o [e-learning](#)), o la utilización de un espacio en línea que dé apoyo a la presencialidad ([aprendizaje semipresencial](#), blended learning o b-learning).

Una de las ventajas es que respaldan la interacción grupal, al mismo tiempo que permite la conversación privada entre los estudiantes. Este medio es ideal para llevar a cabo evaluaciones del curso; en este caso el docente prepara una serie de preguntas y las plantea durante la realización del

encuentro con sus estudiantes. Todos los participantes responden y, al mismo tiempo, pueden hacer observaciones sobre los comentarios expresados por los demás compañeros. Todos los participantes pueden contribuir simultáneamente mientras el sistema los identifica automáticamente y al finalizar aparece una transcripción del encuentro. No obstante, es necesario resaltar que estas herramientas sólo pueden ser utilizadas con el uso del internet.

3.3.1 Características generales de Moodle

Promueve una manera constructiva social (colaboración, actividades, reflexión crítica, etc.). Su arquitectura y herramientas fueron diseñadas para clases en línea, así como también para complementar el aprendizaje presencial.

La instalación requiere una plataforma que soporte PHP y la disponibilidad de una base de datos. Moodle tiene una capa de abstracción de bases de datos por lo que soporta los principales sistemas gestores de bases de datos.

Se ha puesto énfasis en una seguridad sólida en toda la plataforma. Todos los formularios son revisados, las cookies cifradas, etc. La mayoría de las áreas de introducción de texto (materiales, mensajes de los foros, entradas de los diarios, etc.) pueden ser editadas usando el editor HTML, tan sencillo como cualquier editor de texto.

3.3.2 VENTAJAS

Una de las características más atractivas de Moodle, que también aparece en otros gestores de contenido educativo, es la posibilidad de que los alumnos participen en la creación de glosarios, y en todas las lecciones se generan automáticamente enlaces a las palabras incluidas en estos.

Además, las Universidades podrán poner su Moodle local y así poder crear sus plataformas para cursos específicos en la misma universidad y dando la dirección respecto a Moodle, se moverá en su mismo idioma y podrán abrirse los cursos a los alumnos que se encuentren en cualquier parte del planeta: <http://moodle.org/>.

3.3.4 DESVENTAJAS

- Algunas actividades pueden ser un poco mecánicas, dependiendo mucho del diseño instruccional. Por estar basado en tecnología PHP, la configuración de un servidor con muchos usuarios debe ser cuidadosa para obtener el mejor desempeño. Falta mejorar su interfaz de una manera más sencilla. Hay desventajas asociadas a la seguridad, dependiendo en dónde se esté alojando la instalación de Moodle y cuáles sean las políticas de seguridad y la infraestructura tecnológica con la cual se cuente durante la instalación.
- La plataforma puede no ser relativamente fácil para muchos usuarios.
- Un fallo en los servidores o caída del servicio de internet, puede dejar al usuario inhabilitado para realizar sus actividades.

3.4 PHPLDAPADMIN

phpLDAPadmin (también conocido como PLA) es un cliente de LDAP basada en web. Proporciona fácil, en cualquier lugar accesible, la administración multi-idioma para el servidor LDAP.

Su árbol-espectador y la funcionalidad de búsqueda avanzada jerárquica hacen que sea intuitiva para navegar y administrar su directorio LDAP. Dado que es una aplicación web, este navegador LDAP funciona en muchas plataformas, por lo que su servidor LDAP fácilmente manejable desde cualquier ubicación.

phpLDAPadmin es el navegador LDAP perfecto para el profesional y novatos por igual LDAP. Su base de usuarios está compuesta principalmente por profesionales de la administración de LDAP.

3.4.1 CARACTERISTICAS

Navegador del árbol LDAP (ver capturas de pantalla)

- Edición de entrada basada en plantillas
- Copiar entradas LDAP (incluso copiar entre diferentes servidores)
- Copiar recursivamente árboles enteros
- Eliminar entradas LDAP
- Borrar recursivamente árboles enteros
- Ver y editar atributos de imagen (como jpegPhoto)
- Navegador esquema LDAP avanzada
- Creación de entrada basada en plantillas
- Búsquedas LDAP (simples y avanzados)
- LDIF y DSML exportación
- Importación de LDIF
- Cambiar el nombre de las entradas LDAP
- Administrar los hashes de contraseñas de usuario (soporta sha, cripta, md5, pez globo, md5crypt)
- Examine la información RootDSE LDAP
- Determinar automáticamente raíz de su servidor LDAP DN
- Autenticación configurable (anónimo, web de inicio de sesión, o estática)
- Traducción friendly atributo (es decir, la pantalla "Fax" en lugar de "facsimileTelephoneNumber")
- Apoyo atributo binario
- Soporte configurable para los alias y referencias
- Incrementar automáticamente los números UID
- Los hipervínculos para mailto y valores de atributo href.
- Sólo lectura configurable y leer modos / escritura.
- Soporte i18n robusta
- Disponible en 10 idiomas

3.5 LAM

El administrador de cuentas LDAP (LAM) es una suite de aplicaciones para la gestión de cuentas de POSIX, así como las cuentas de Samba SAM para usuarios, grupos y máquinas Microsoft Windows. LAM se puede utilizar con cualquier servidor Web que tiene soporte PHP4. Se conecta al servidor LDAP utilizando cualquiera de las conexiones no cifradas o SSL.

LAM está escrito en PHP y está disponible en la página principal de LAM, sourceforge.net/projects/lam, bajo la GNU GPL. La contraseña por defecto es lam. Usted debe utilizar sólo una conexión SSL con el servidor Web para todas las operaciones remotas que involucran LAM. Si quieres conexiones seguras, debe configurar el servidor Web Apache para permitir conexiones a LAM utilizando sólo SSL.

3.5.1 LAM requisitos :

- Un servidor Web que funciona con PHP4.
- PHP4 (disponibles en la página principal de PHP, www.php.net).
- OpenLDAP 2.0 o posterior.
- Un navegador Web que soporte CSS.
- Perl.
- El paquete gettext.
- mcrypt + mhash.
- Soporte SSL no es necesario, pero es bueno tener.

Las instrucciones de instalación se proporcionan en el paquete de archivos de distribución y son fáciles de seguir. Cuando haya instalado el MELA, iniciar el servidor Web y, a continuación, utilizando su navegador Web, conectarse a la URL LAM. Haga clic en el enlace Configuración de inicio de sesión y luego en el enlace Asistente de configuración para comenzar a ejecutar el perfil predeterminado. El servidor LDAP debe estar en ejecución en el momento LAM está configurado. Esto le permite validar las operaciones correctas.

3.6 JXPLOER

Jxplorer es una, libre de código abierto cliente de navegación Lightweight Directory Access Protocol (LDAP) y servidores LDAP Data Interchange Format (LDIF). Es liberado bajo una licencia Apache-equivalente. JXplorer está escrito en Java y es independiente de la plataforma, configurable, y ha sido traducida a varios idiomas. Los principales autores y mantenedores son Chris Betts y Trudi Ersvaer, originalmente tanto trabajo en la CA (entonces Computer Associates) Directorio de eTrust (ahora CA Directory) laboratorio de software en Melbourne, Australia .

Varios comunes de Linux distribuciones incluyen JXplorer Software para la administración del servidor LDAP. El software también funciona en BSD -variants, AIX , HP-UX , Mac OS X , Solaris , de Microsoft Windows (2000, XP) y z / OS .

3.6.1 CARACTERÍSTICAS FUNDAMENTALES

- SSL, SASL y GSSAPI;
- DSML;
- LDIF;
- I18n (actualmente alemán, francés, japonés, chino tradicional, chino simplificado, húngaro);
- opcional interfaz gráfica de usuario de LDAP constructor de filtro; arquitectura extensible.

Versión 3.3, el '10th Anniversary Edition' fue lanzado en julio de 2012. En general, el programa ha sido descargado más de un millón de veces desde SourceForge y se incluye con varias distribuciones de Linux.

4. DIAGRAMA DE RED

Diagrama de red a implementar en el proyecto.

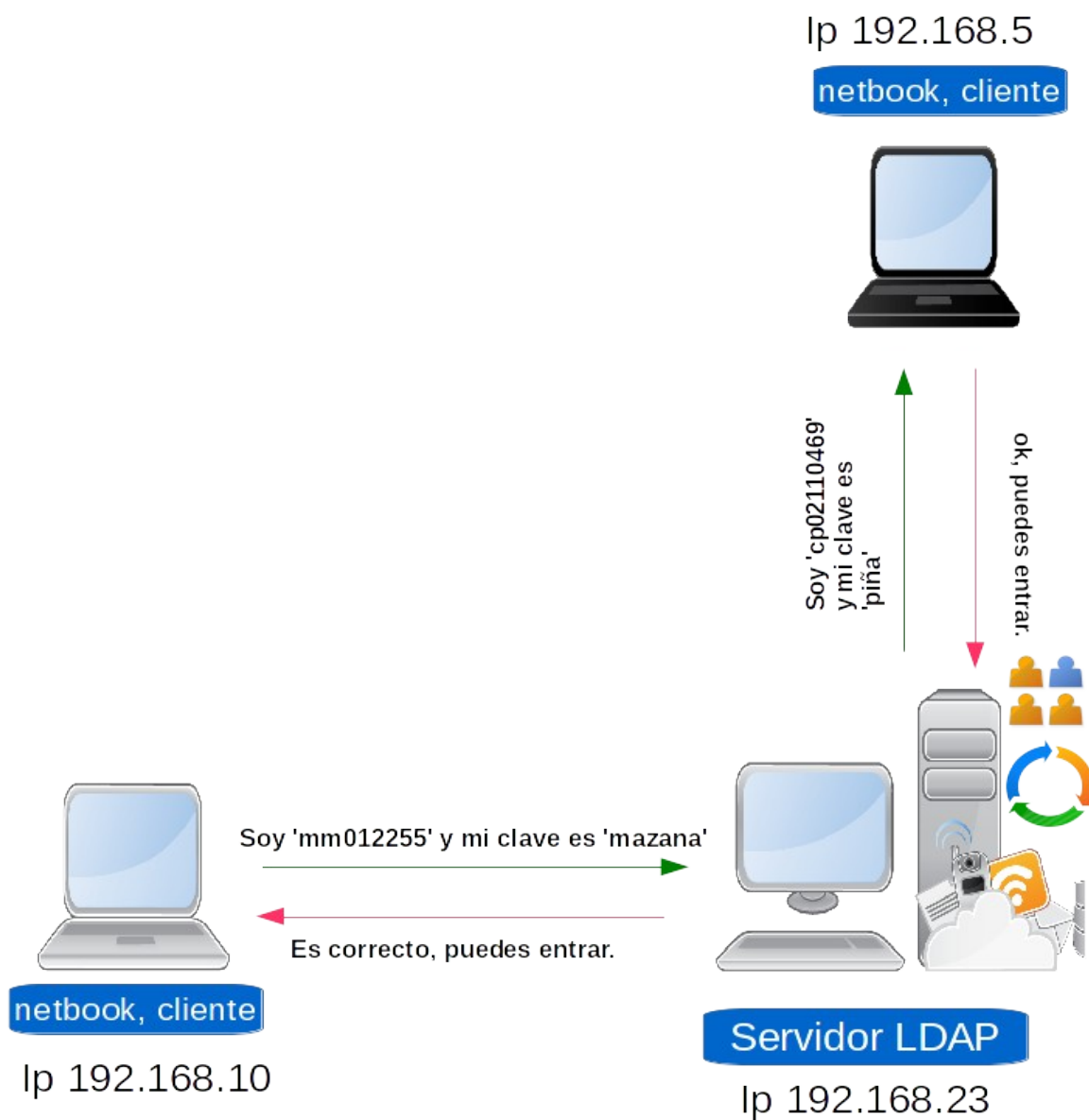


Ilustración 1: diagrama de red a utilizar

5. DESCRIPCIÓN DEL PROYECTO

El proyecto a realizar consiste una guía de instalación, configuración y uso del protocolo LDAP, el nombre del software a utilizar es OpenLDAP. Este protocolo servirá para centralizar la gestión de autenticación de usuarios en las peticiones para acceder a cierto servicio, facilitando el acceso simultaneo. La guía ilustrará un prototipo a implementar, que constara de dos servicios disponibles en un equipo servidor, el cual se comprobará el proceso para acceder a estos servicios con uno o dos equipos clientes.

El prototipo del proyecto a elaborar servirá para guiar en la implementación de este protocolo de servicio en la Universidad Luterana Salvadoreña.

La Universidad Luterana Salvadoreña ofrece a su comunidad estudiantil y docentes una serie de servicios tecnológicos en línea, esencialmente el entorno virtual de aprendizaje (EVA) y Sistema de Gestión Educativa. Cada servicio cuenta con su propia base de datos, pero los datos de validación para acceder son distintos en cada servicio, el cual puede atraer procesos engorrosos como la edición y actualización de claves para un usuario en cada servicio, inserción de un nuevo usuario en los tres servicios. Los resultados a esperar son la optimización de consultas simultaneas en línea y optimización de gestión de cuenta de usuarios.

6. CRONOGRAMA DE ACTIVIDADES

Tareas	agosto			septiembre				octubre				noviembre				diciembre				
	semana			semana				semana				semana				semana				
	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	
1. Selección del tema	x																			
2. Levantamiento de requerimientos		x																		
3. Elaboración de perfil			x																	
Entrega de perfil			x																	
4. primer avance																				
4.1. Instalación de software				x	x															
4.2. Configuraciones				x	x	x														
Entrega primer avance							x													
5. Segundo Avance																				
5.1 Pruebas de ejecución								x	x	x	x	x								
5.2 Elaboración de guía								x	x	x	x									
Entrega segundo avance												x								
6. Defensa y documento Final																				
6.1 Elaboración de documento final												x	x	x						
6.2 Defensa clase														x						
6.3 Defensa FESOL (sujeto a confirmación)															x					

7. VIABILIDAD

Para realizar nuestro proyecto nos enfocaremos en hacer lo mas favorable para la resolución del proyecto.

7.1 Viabilidad Técnica

definición

Condición que hace posible el funcionamiento del sistema, proyecto o idea al que se refiere, atendiendo a sus características tecnológicas.

Para nuestro proyecto ocuparemos lo siguiente :

- computadora mini-laptop con sistema operativo GNU/Linux.
- Openldap.

son los recursos mínimos para obtener el directorio LDAP en tu computadora

requisitos mínimos generales del hardware para implementación de prototipo LDAP.

- 1GB en RAM y 8 GB de espacio en disco.
- Procesador de 1.60 GHz
- conexión a internet

Estos solo los requisitos mínimos para la implementación de nuestro proyecto

7.2 Viabilidad Económica-Financiera

NOMBRE	COSTO UNITARIO	CON ACCESO	SIN ACCESO	CANTIDAD	COSTO TOAL
Computadora para la instalación de LDAP	\$500.00			1	\$500.00
switch	\$50.00	x		1	\$50.00
Acceso a internet	\$20.00	x		3	\$60.00
Computadora cliente	\$500.00	x		2	\$1,000.00
Impresión de documentaciones	\$60.00	x		4	\$10.00
Sueldo del personal	\$500.00		x	3	\$1,500.00
Refrigerios	\$15.00	x		3	\$45.00
Total	\$1,645.00				\$2,250.00

8. INSTALACIÓN DE OPEN LDAP

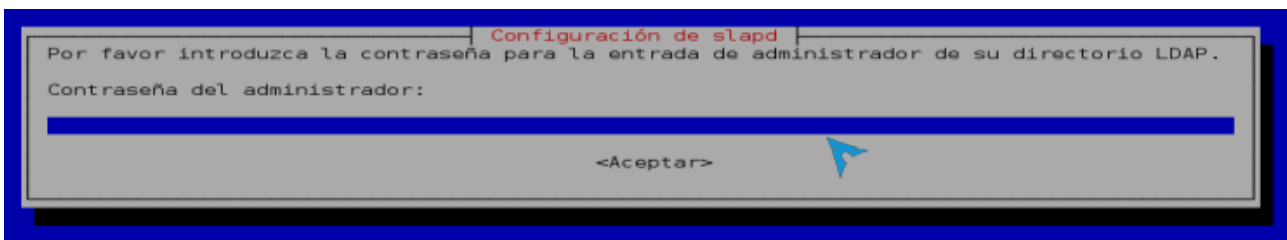
A continuación se presenta los pasos para la instalación del software que permitirá usar el protocolo LDAP. Se instalará en Debian Wheezy 7.1.

En una terminal como usuario root tecleamos lo siguiente.

```
# aptitude install slapd ldap-utils
```

Presionamos *enter* e inicia instalación.

En algún momento, cuando se este instalando slapd nos saldrá el siguiente asistente:



- introducimos la contraseña para el administrador del servidor LDAP.
- Luego nos solicitara confirmación de la contraseña.

8.1 configurar paquete slapd

Detenemos el servicio:

```
# /etc/init.d/slapd stop
```

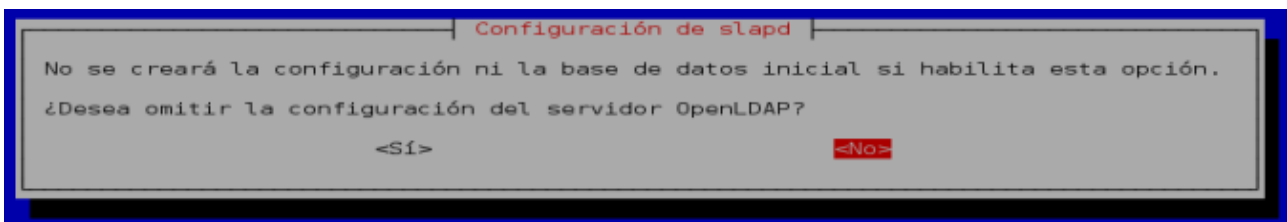
Eliminamos la base de datos creada DURANTE LA INSTALACIÓN:

```
# rm -rf /var/lib/ldap/*
```

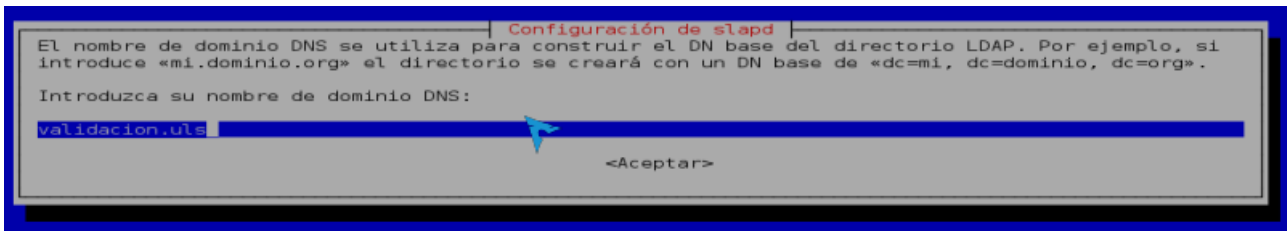
Configurar slapd, jecutar el siguiente comando:

```
# dpkg-reconfigure slapd
```

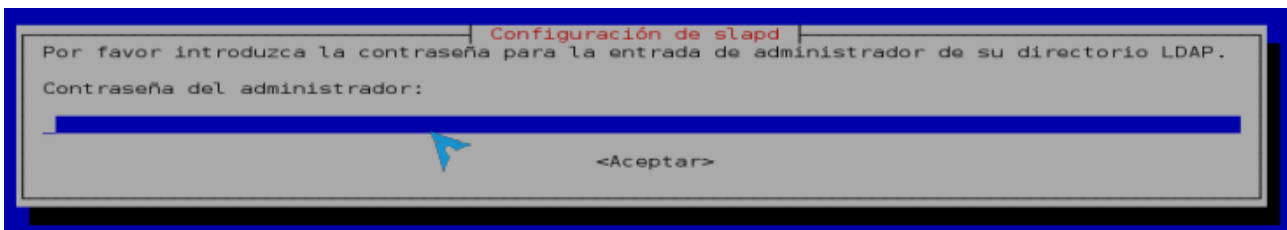
Entraremos al siguiente asistente:



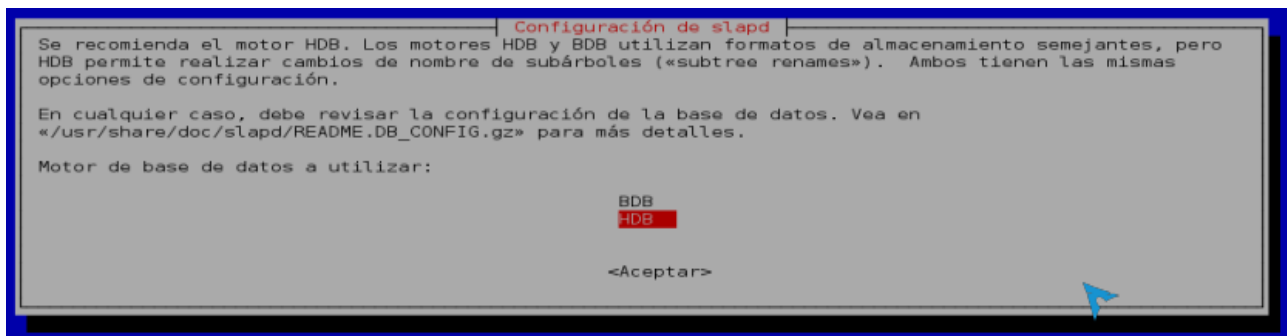
- no omitiremos la configuración.



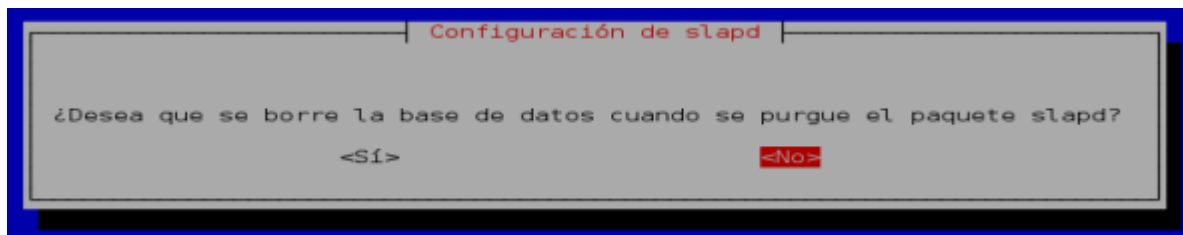
- Introducir el dn (componente de dominio), como ejemplo introduciremos *validacion.uls* ó *dc=validacion,dc=uls*, ambas formas son válidas.
- Luego ingresamos el nombre de la organización, generalmente se utiliza el mismo del dn.



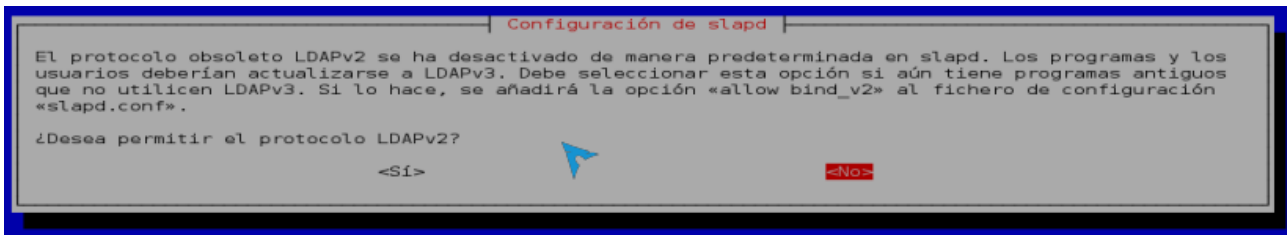
- Aquí introduciremos la contraseña del administrador del directorio a crear.
- Después no pedirá la confirmación de la contraseña.



- Escogeremos el motor de base de datos HDB (aparece por defecto), en comparación al de BDB son similares, BDB fue el primer motor creado.



- Se recomienda por situaciones de seguridad elegir que no, por si algún motivo purgamos slapd (aptitude purge slapd), la base de datos del directorio quedará intacta para poderlo recuperar, si desearíamos borrar la base de datos, lo podemos hacer de forma manual como lo hicimos al principio de la configuración.



- Seleccionamos que no, ya que la versión 2 esta obsoleta.

Con esto estaremos terminando la configuración de slapd.

8.2 Comprobación de la instalación

Verificaremos si esta escuchando por el puerto correspondiente:

|| → # netstat -tpua | more

El resultado sería el siguiente:

```
levi@kamehouse:~$ netstat -tpua | more
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 *:sunrpc                *:*                     LISTEN      -
tcp        0      0 *:ssh                   *:*                     LISTEN      -
tcp        0      0 localhost:postgresql    *:*                     LISTEN      -
tcp        0      0 *:52792                  *:*                     LISTEN      -
tcp        0      0 localhost:smtp          *:*                     LISTEN      -
tcp        0      0 *:ldap                   *:*                     LISTEN      -
tcp        0      0 192.168.1.9:50488       yk-in-f188.1e100.n:5228 ESTABLISHED 5610/chrome
tcp6       0      0 [::]:sunrpc             [::]:*                  LISTEN      -
tcp6       0      0 [::]:http                [::]:*                  LISTEN      -
tcp6       0      0 [::]:ssh                 [::]:*                  LISTEN      -
tcp6       0      0 localhost:postgresql    [::]:*                  LISTEN      -
tcp6       0      0 localhost:smtp          [::]:*                  LISTEN      -
tcp6       0      0 [::]:ldap                [::]:*                  LISTEN      -
tcp6       0      0 [::]:34923               [::]:*                  LISTEN      -
--More--
```

9. ADMINISTRACIÓN DEL OPENLDAP

Una vez instalado el servidor LDAP, la siguiente tarea es la del diseño de la estructura y la introducción de datos al directorio.

Mencionaremos las opciones más conocidas para la administración del servicio, en el marco teórico de este documento podemos conocer un poco sobre cada uno:

- **phpldapadmin:** (también conocido como PLA) es un cliente de LDAP basada en web, con soporte para PHP4.
- **Lam login:** LAM se puede utilizar con cualquier servidor Web que tiene soporte PHP4.
- **Jxplorer:** JXplorer está escrito en Java y es independiente de la plataforma, configurable.

También se puede administrar desde la consola (TUI), utilizando sentencias de comando y archivos ldif (LDAP Data Interchange Format), en este proyecto nos basaremos ocupando una de las tres herramientas (GUI) ya mencionadas.

En la siguiente parte veremos la instalación y configuración de LAM login

9.1 Requerimientos previos para instalación de LAM

Tener instalado:

- Servidor web apache
- PHP 5
- navegador
- OpenLdap

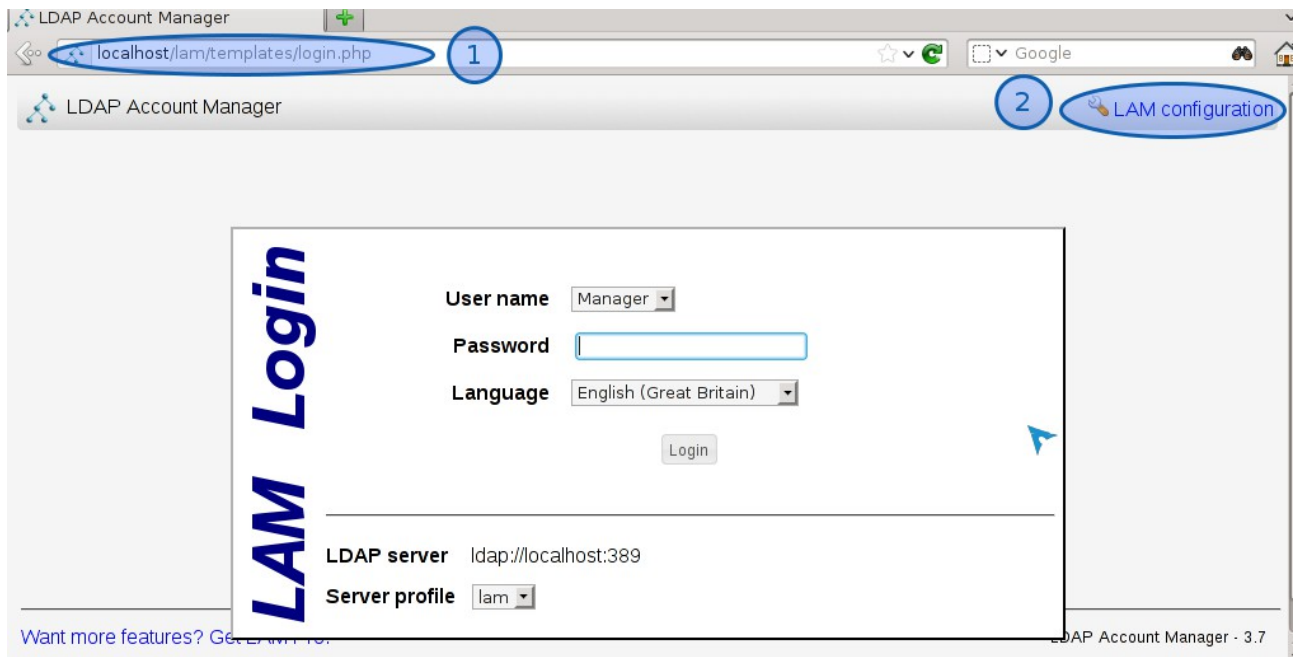
9.2 Instalación de LAM (Ldap Account Manager)

Tipeando el siguiente comando:

```
➡ # apt-get install ldap-account-manager
```

9.3 Configuración de LAM

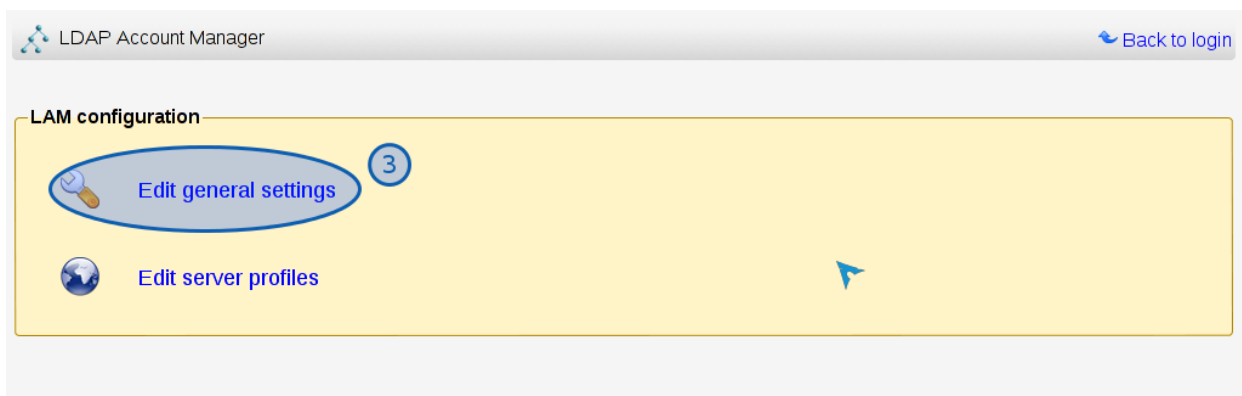
Al terminar la instalación, abrir un navegador.



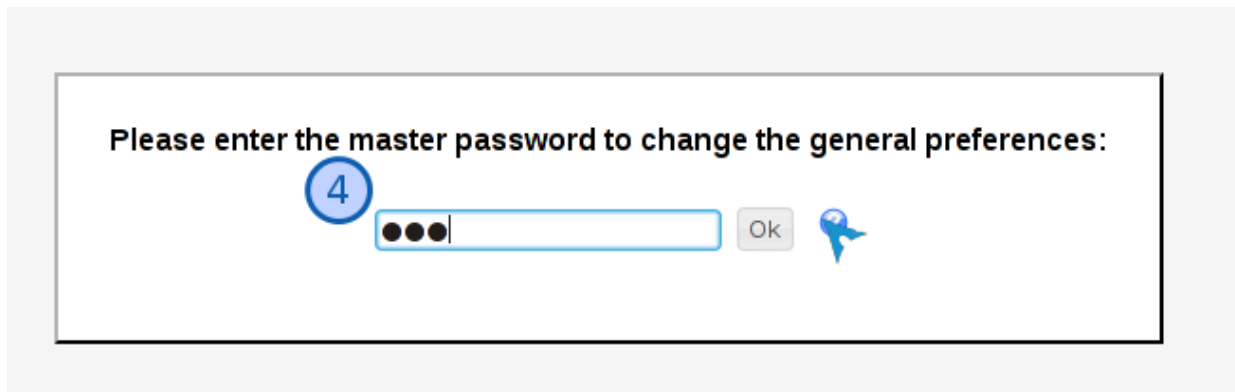
1. En la barra de direcciones introducir *localhost/lam*, luego presionar *enter*, veremos el portal de LAM.

No podremos acceder aun, ya que el nombre de usuario administrador está por defecto como Manager, debemos configurarlo.

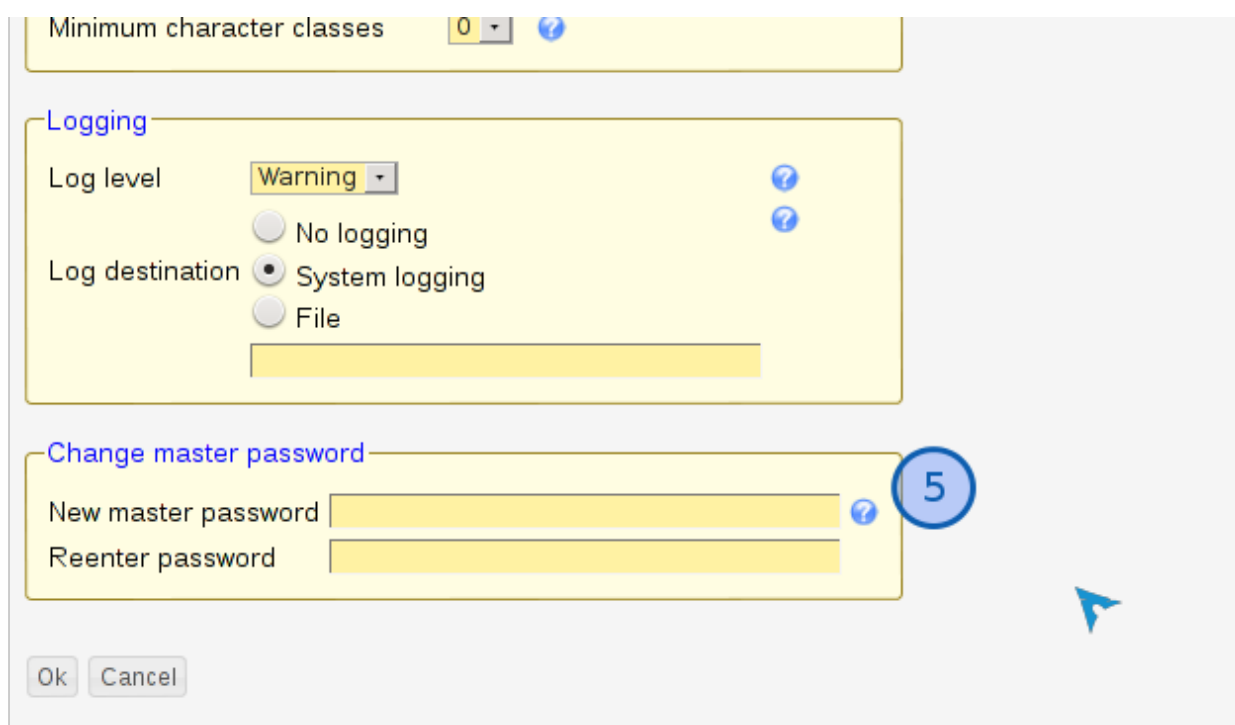
2. Seleccionar LAM configuration.



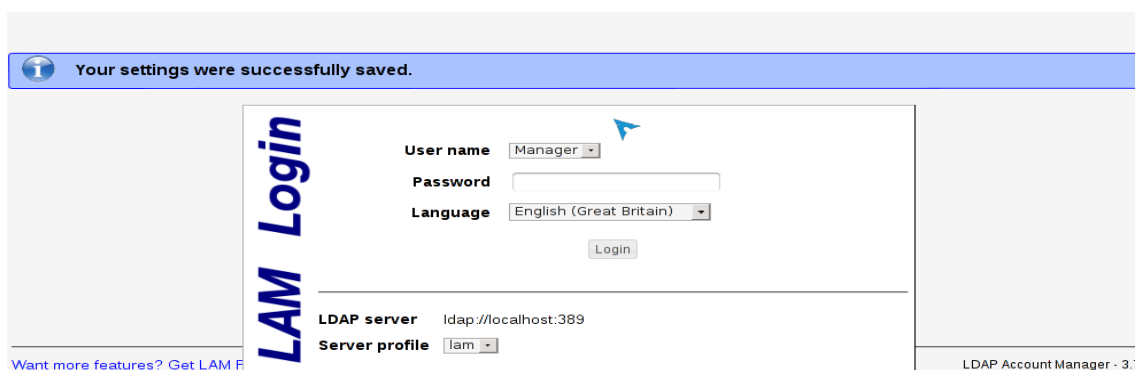
3. En LAM configuration seleccionaremos Edit general settings.



4. Lo que haremos son configuraciones de LAM, nos pide una contraseña, el cual es por defecto **lam**, esta contraseña la editaremos.

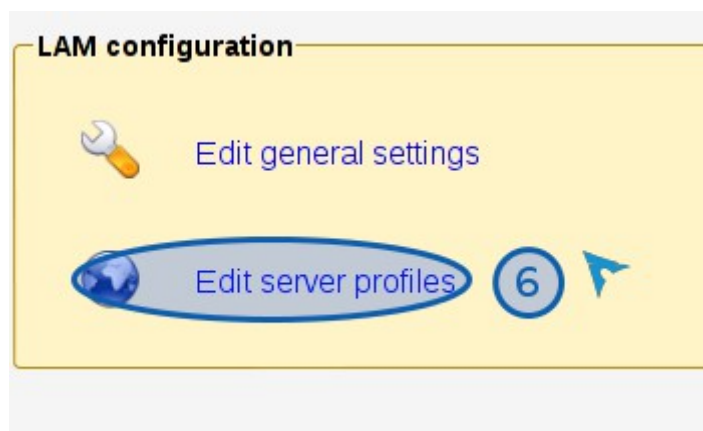


5. En el navegador nos desplazamos hasta el final para encontrar *Change master password* , introducimos la nueva contraseña a utilizar, luego pulsamos en el botón **ok** para guardar la configuración.



Nos enviara al inicio, confirmando con un mensaje que la configuración se guardo.

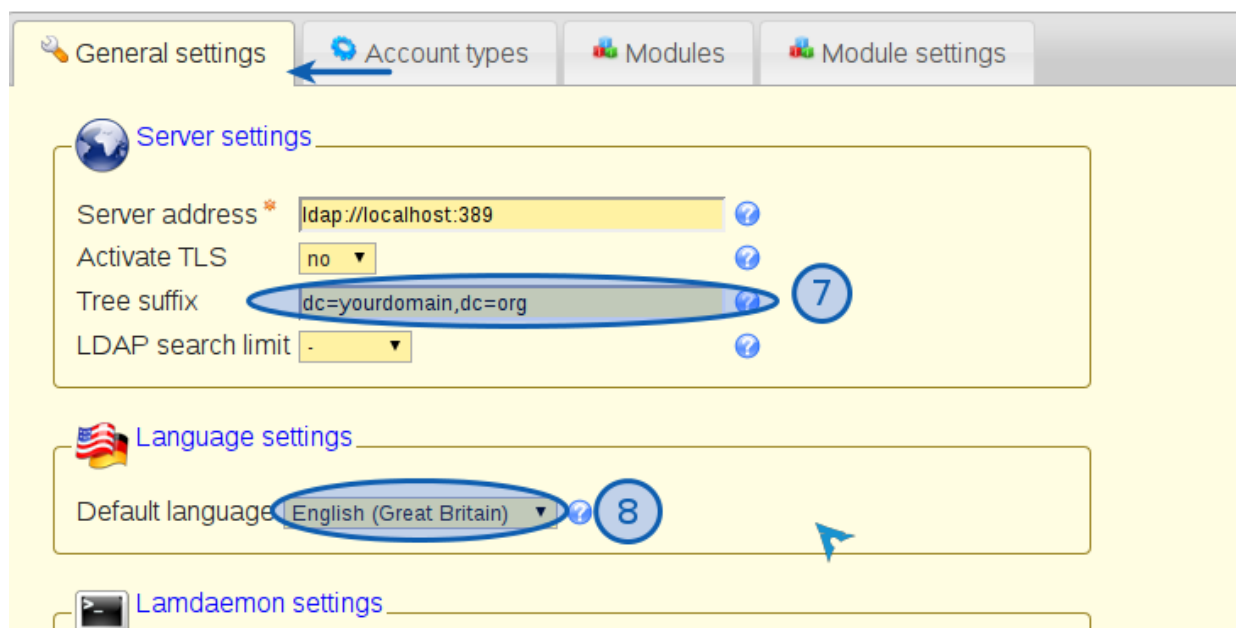
Seguimos con las configuraciones, Estando en el inicio pulsamos de nuevo en *LAM configuration*.



6. Esta vez pulsaremos en Edit server profiles.

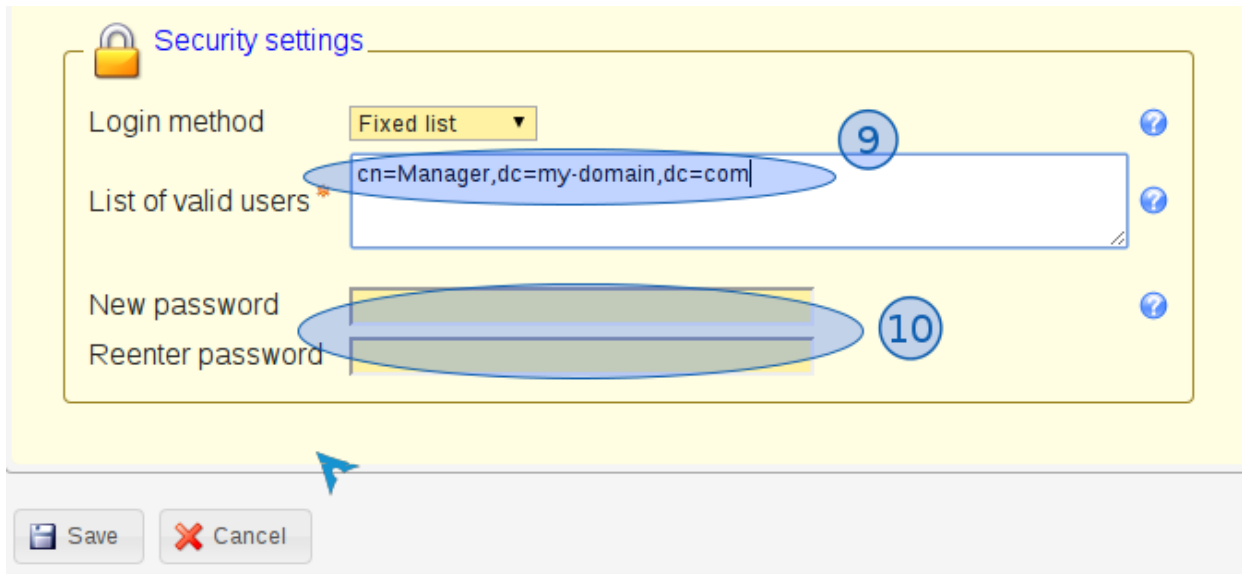
- nos solicitará contraseña para permitir realizar las configuraciones de LAM, recuerden ahora introducir la nueva clave.

Al ingresar veremos la siguiente pantalla:



Estaremos en la opción *General settings* del menú.

7. En *Server settings* editamos el **Tree suffix** (sufijo de árbol), sustituimos **yourdomain** por *validacion* y **org** por *uls*, recuerden que *validacion.uls* es el dominio con el que estamos trabajando.
8. Luego en *Language settings* buscamos y seleccionamos el idioma español.



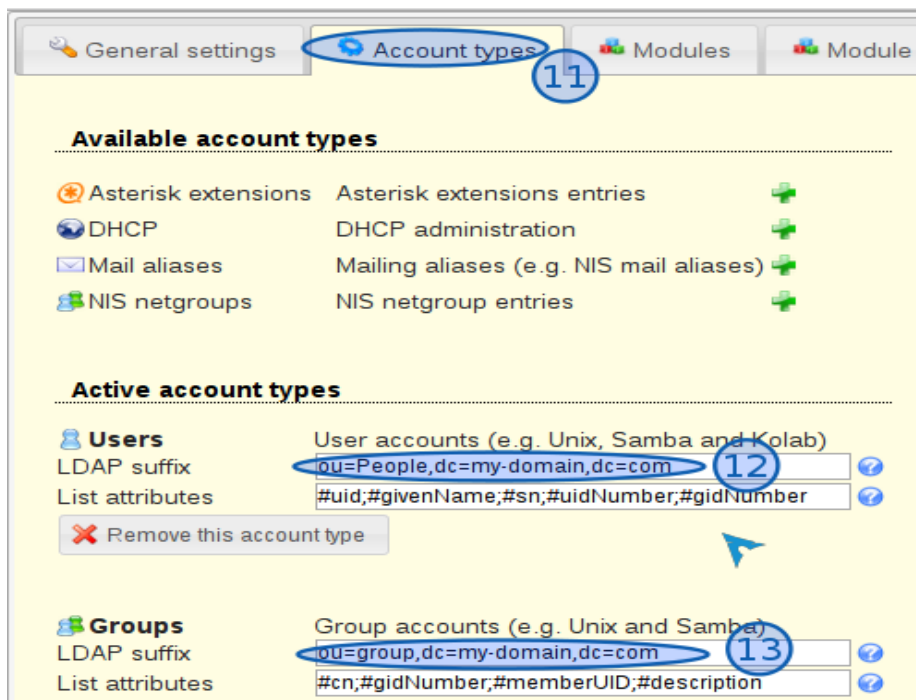
Más abajo en Security settings es donde crearemos a los usuarios que podrán ingresar al administrador de LAM, en este ejemplo solo crearemos a un administrador, lo nombraremos admin.

9. Entonces sustituir **Manager** por **admin**, **my-domain** por **validacion** y **org** por **uls**.

10. Ingresar y confirmar la clave del usuario admin.

- Por ultimo pulsamos en save para guardar.

- Nos enviará al inicio, debemos seguir con las configuraciones, de nuevo ir a LAM configuration y luego de nuevo a Edit Server profile, introducimos la contraseña.



11. Seleccionar Account Types

12. Veremos la interfaz que aparece en la imagen anterior, en la seccion Active account types editaremos el LDAP suffix de **Users**, sustituimos People por Usuarios, y el resto conformando el dominio validacion.uls .

13. En **groups**, editamos group por tipos_usuarios, y el resto conformando el dominio validacion.uls .

- Mencionar que mas a bajo aparecen otras opciones para crear mas organizaciones, las removemos y solo ocuparemos **users** y **groups**.

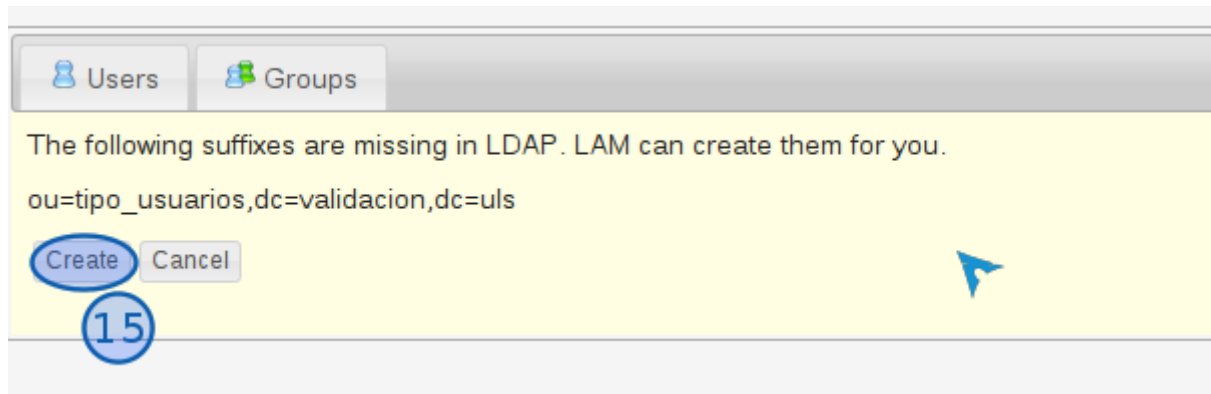
- Ahora guardamos pulsando en save.



- Nos redireccionará al inicio confirmando que los ajustes se han guardado.

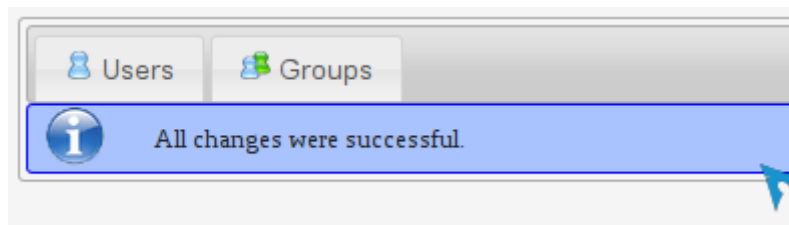
- observar que el usuario por defecto ya no es Manager, ahora es admin.

14. Ahora entraremos a la administración de LAM ingresar la clave que le asignamos al usuario admin y pulsamos en Login.



Al ingresar nos mostrara que debemos crear el grupo tipo_usuarios.

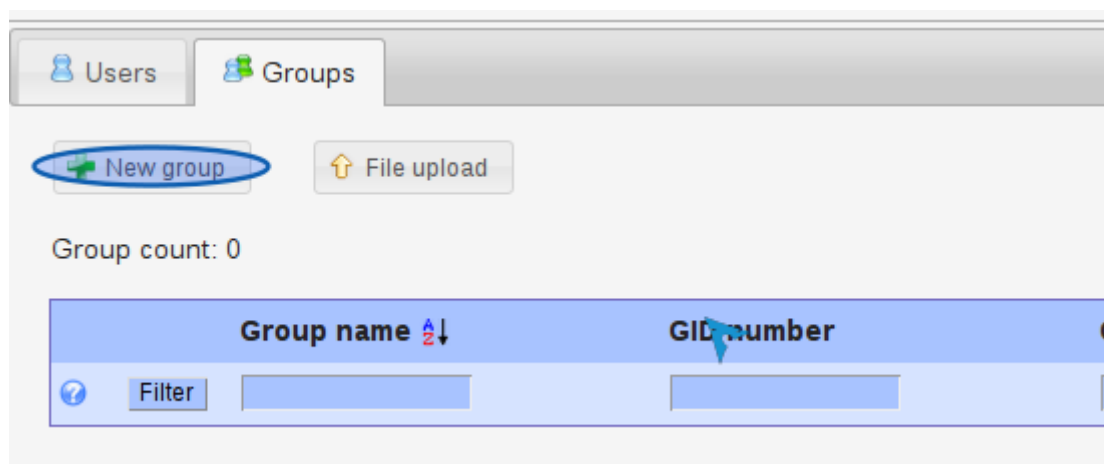
15. Seleccionar create.



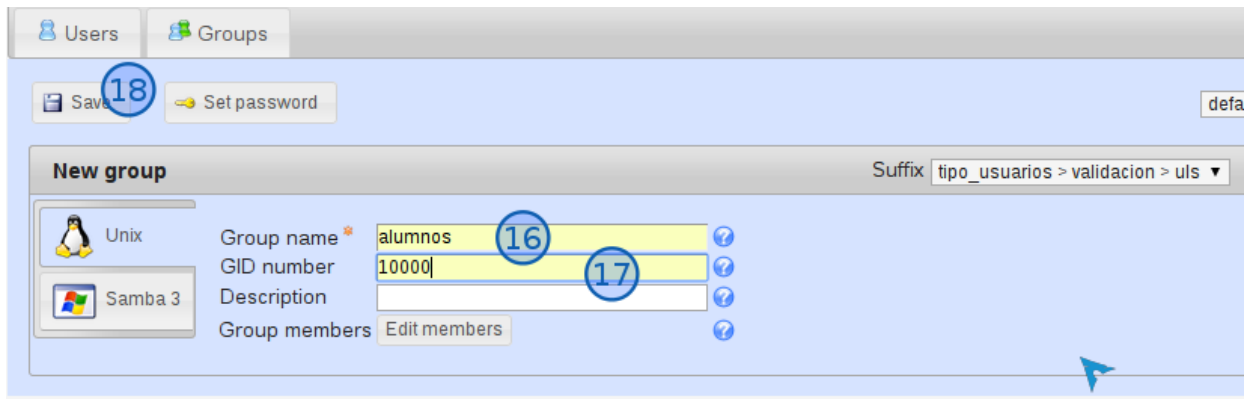
- Mostrará la confirmación del cambio.

- Seleccionar groups.

9.4 Crear grupos de usuario



-Estando en groups, seleccionar new group ya que no tenemos creado grupos dentro de tipo_grupos.



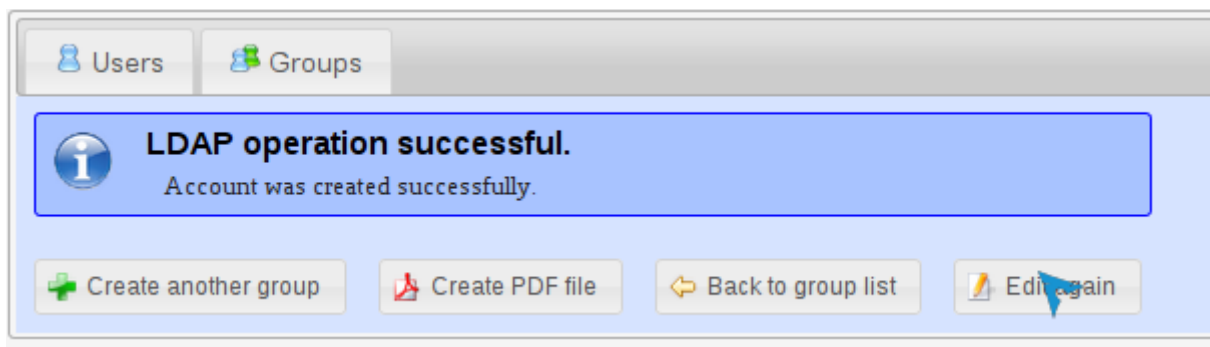
16. Ingresar un nombre de grupo, en este caso crearemos el de alumnos.

17. Asignar un ID para el grupo.

- la descripción es opcional

- la opción set password, es para asignar una clave cuando deseemos ingresar al grupo alumno, es opcional.

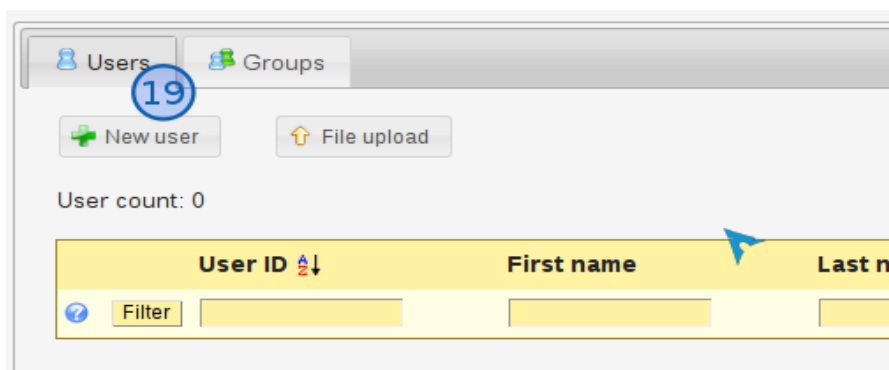
18. Presionar en save para guardar.



Mensaje de confirmación de la creación del grupo.

Repetir el procedimiento del paso 15 al 18 para crear el grupo para los usuarios docentes.

9.5 Crear usuarios



19. Vamos con los usuarios, Iniciaremos con un usuario alumno, para eso presionar sobre en

users luego en new users.

20. Ingresar nombres.

21. Ingresar apellidos.

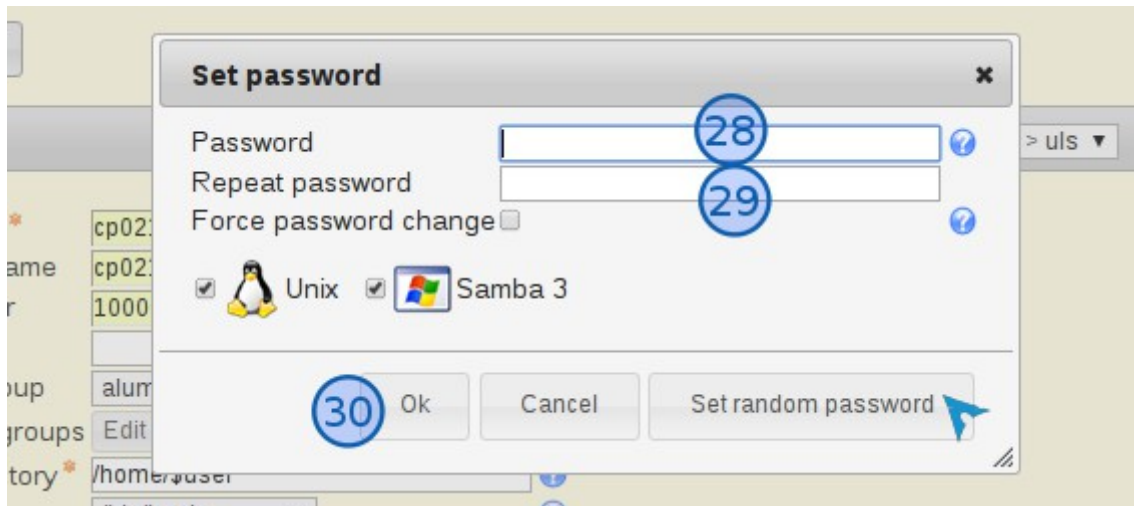
- desplazándose hacia abajo hay una serie de datos personales que pueden registrarse, en esta ocasión solo ingresaremos estos dos nombre y apellidos. Luego

22. Pulsar sobre Unix para otros registros importantes para definir y crear el usuario.

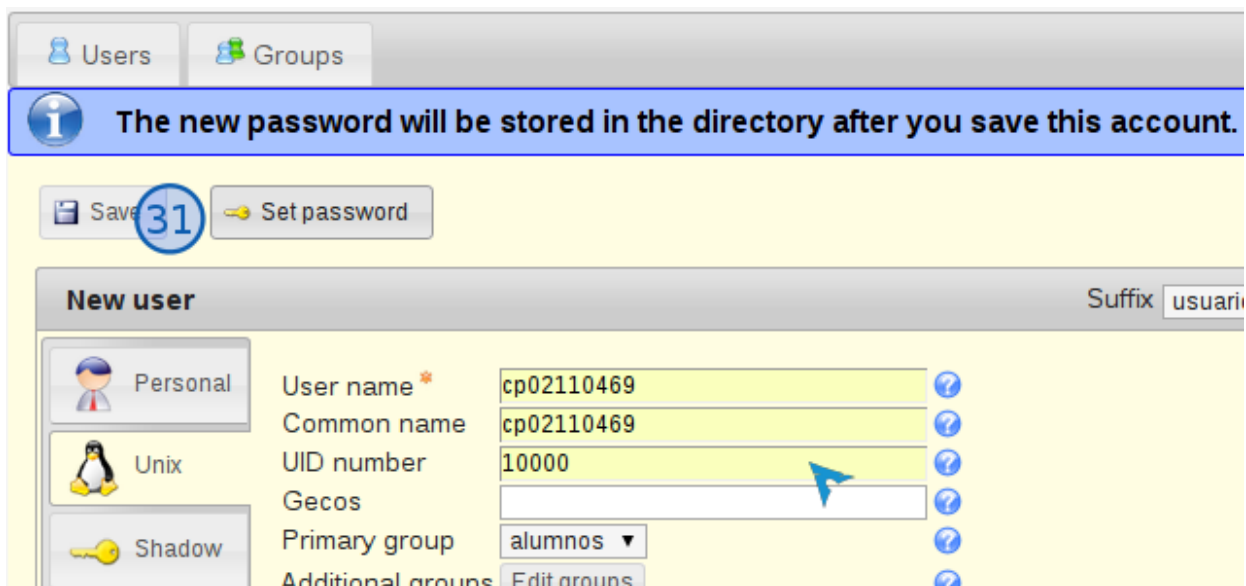
ATENCIÓN a lo siguiente, al seleccionar sobre unix, automáticamente nos rellena los campos de User name y Common name (cn), vamos a editarlos, nos interesa que el cn sea registrado con el número de carnet del estudiante, ya que este dato utilizará el usuario para ingresar al moodle, también podríamos dejar el User name con el numero de carnet, este nombre de usuario es como un alias.

23. En user name Ingresar numero de carnet del estudiante.

24. Common name Ingresamos el número de carnet del estudiante.
25. En Uid number Ingresar un id para el usuario.
26. Primary group Seleccionar a que grupo pertenecerá el usuario.
27. Vamos a generar la contraseña del usuario, pulsar sobre Set password.

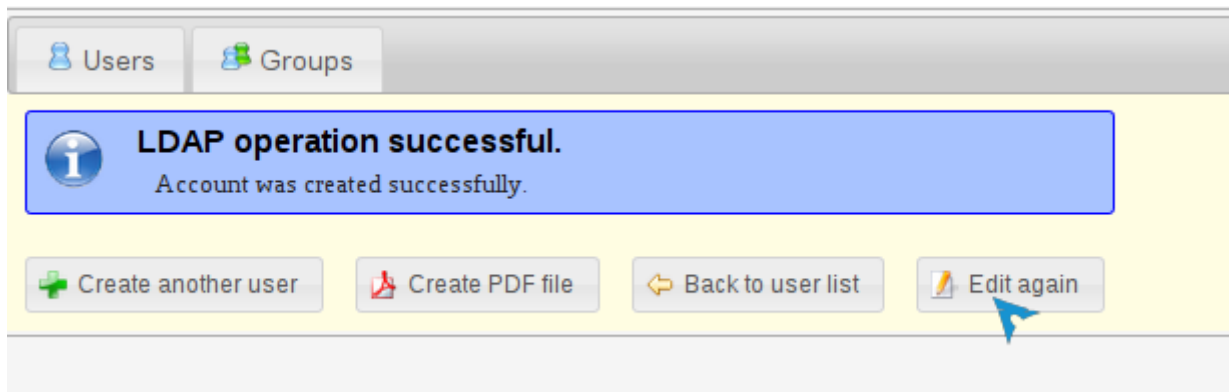


28. Insertar la clave a asignar para el usuario.
29. Re confirmar clave.
30. Presionar sobre ok para guardar.



- confirma la asignacion de una clave al usuario.

31. Presionar sobre save para guardar, con esto estaremos creando a un usuario para el grupo alumno.



Este mensaje sera la confirmación del usuario creado. Si después vamos a users veremos el registro.

Será el mismo procedimiento para crear los usuarios para le grupo de docentes, solamente estar atento en la indicacion26.

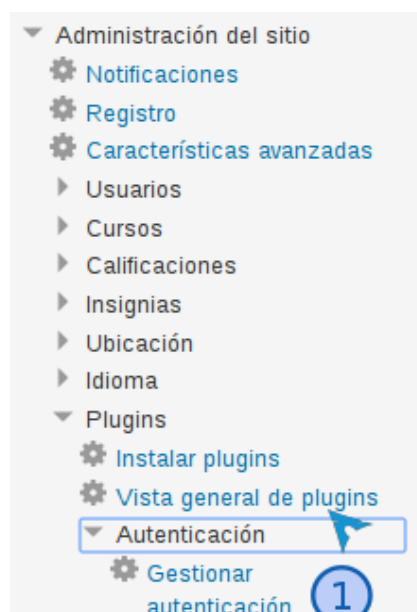
10. CONFIGURACIÓN DE MOODLE 2.7.2+

A continuación se mostrará las configuraciones básicas para la conexión y autenticación en moodle con el servicio LDAP.

10.1 Conexión a LDAP

- Vamos a ir a nuestro moodle e ingresar con el usuario administrador.

- ya logueados en el menú de administración nos dirigimos a: Administración de sitio>> plugins>> autenticación>> Gestionar autenticación.



1. En la imagen anterior se observa Gestionar autenticación, seleccionar.

Gestionar autenticación

Plugins de autenticación disponibles

Nombre	Usuarios	Habilitar	Arriba/Abajo	Configuración	Configuraciones de prueba	Desinstalar
Cuentas manuales	2			Configuración		
Sin ingreso al sistema	0			Configuración		
Usar un servidor LDAP	0			Configuración	Configuraciones de prueba	
Usar un servidor CAS (SSO)	0			Configuración		Desinstalar
Usar una base de datos	0			Configuración	Configuraciones de prueba	Desinstalar

Veremos esta interfaz, tomar en cuenta dos cosas, uno es cierto que ya tenemos un usuario creado en el servidor ldap, pero este usuario debe intentar loguearse en moodle para que quede registrado en la base de datos de moodle, por eso observamos que moodle nos dice que no tenemos usuario usando servidor ldap. Dos asegurarse que este habilitado, es el icono de un ojo, presionar sobre este icono en caso de que este inabilitado.

2. Pinchamos en configuración.

Ajustes de servidor LDAP


3 URL del host

Versión

Usar TLS

Codificación LDAP

Tamaño de página



3. Estamos en los ajuste de servidor LDAP, introduce la ip a la que responde el servidor LDAP.

Fijar ajustes

Ocultar contraseñas 4

Nombre distinguido

Contraseña

Desenmascarar

4. En fijar ajustes, solo verificaremos que la opción ocultar contraseñas tenga el valor si, lo que evitara que la contraseña se guarde en la base de datos de moodle.

Ajustes de búsqueda de usuario

Tipo de usuario 5

Contextos

Buscar subcontextos

Des-referenciar alias

Atributo de usuario

Atributo de miembro

En ajustes de búsqueda de usuario verificar que tenga la opción de *por defecto* y

5. en contextos, es donde ingresamos aquellos DN (nombre global distinguido) en donde están localizados los usuarios, cada DN separarlo por ';'. Ejemplo:
ou=docentes,dc=validacion,dc=uls;ou=alumnos=validacion,dc=uls.

Creador de curso

Creadores



En creador de curso, por consecuente permitiremos a los usuarios docentes crear cursos en moodle.

Estas son las configuraciones básicas para que moodle busque en el servidor ldap a los usuarios. Existen más opciones de configuraciones opcionales o dependiendo de la necesidad para el uso.



6. Desplazar hasta el final y buscar el botón Guardar cambios.

10.2 Validar usuario de ldap en moodle

Ahora intentar loguear el usuario que creamos en ldap, cerramos sesión de administrador de moodle y buscar el formulario de login.

Ingresar

Nombre_de_usuario

Contraseña

Recordar nombre_de_usuario

[Olvidó su nombre de usuario o contraseña](#)

El nombre de usuario sería el cn (nombre común) en el cual lo registramos en ldap, lo insertamos y luego la clave que le asignamos. Presionamos ingresar.

[e\)](#) > [Ajustes de mi perfil](#) > [Editar perfil](#)

[e\)](#)
[sonal\)](#)

[os](#)

[vados](#)

[il](#)

General

Nombre*

Apellido(s)*

Dirección de correo*

Mostrar correo

Mostrar mi dirección de correo sólo a mis compañeros de curso

moodle encontro el usuario en el servicio de ldap y lo dejo accesar, por defecto moodle le muestra un formulario para identificarse con algunos datos personales.

Plugins de autenticación disponibles

Nombre	Usuarios	Habilitar	Arriba/Abajo	Configuración	Configuraciones de prueba	Desinstalar
Cuentas manuales	2			Configuración		
Sin ingreso al sistema	0			Configuración		
Usar un servidor LDAP	1	<input checked="" type="checkbox"/>		Configuración		
Usar un servidor CAS (SSO)	0	<input type="checkbox"/>		Configuración		Desinstalar

Si esta vez verificamos en Administración de sitio>> plugins>> autenticación>> Gestionar autenticación. Notaremos que ahora si nos aparece el usuario utilizando servidor LDAP.

11. BUENAS PRACTICAS

- La versión de moodle 2.7.2+ tiene soporte en php 5.5, si deseas administrar el servidor LDAP con PHPLDAPADMIN este no tendrá el funcionamiento adecuado, PHPLDAPADMIN tiene soporte hasta php 5.4.
- si deseas administrar el servidor LDAP con LAM podrás realizar las operaciones esenciales en la administración, el inconveniente será cuando quieras realizar la vista en forma de árbol, existen errores de funciones de php obsoletas, esto cuando estés utilizando php5.5, LAM tiene soporte hasta php 5.4.
- Con respecto a los dos puntos anteriores, en internet existe propuestas de soluciones, la mayoría relata sobre cambiar las funciones php obsoletas a las nuevas, esto no soluciona en su totalidad los errores, debido a que las nuevas funciones esta conformadas con otra estructura. Existe un [parche](#) que configura el archivo /usr/share/phpldapadmin/lib/functions.php. Con conocimiento de como aplicar esto, es muy probable que solucione los errores ya sea en PHPLDAPADMIN ó LAM.
Fuente: https://bugzilla.redhat.com/show_bug.cgi?id=974928

12. CONCLUSIÓN

La principal utilidad de un directorio LDAP es como servidor de autenticación para los distintos servicios de un sistema informático como puedan ser: autenticación para entrar en un PC, para entrar en una aplicación web, para acceder a un servidor ftp, para acceder a servidores de correo entrante POP3 y saliente SMTP, etc.

Existen configuraciones para emplear en el área de seguridad. Ya que se trata de la transmisión de información, estas están expensas de ser capturadas en el trafico de la red, la opción a utilizar es el cifrado que ofrece OpenSSL. Para elaborar el prototipo de nuestro proyecto nos limitaremos de estas configuraciones, por la complejidad de esta configuración y la disposición del tiempo para presentar el proyecto finalizado.

13. BIBLIOGRAFIA

- Sitio: <http://es.wikipedia.org>
url: <http://es.wikipedia.org/wiki/LDAP>
Tema: LDAP
fecha consultada: 23-08-2014
- Sitio: <http://es.wikipedia.org>
url: <http://es.wikipedia.org/wiki/OpenLDAP>
Tema: OpenLDAP
fecha consultada: 23-08-2014
- Sitio: <http://modle.org>
url: <https://moodle.org/mod/forum/discuss.php?d=74752>
Tema: problemas generales con ldap
fecha consultada: 5-11-2014
- Sitio: <http://modle.org>
url: <https://moodle.org/mod/forum/discuss.php?d=66276>
Tema: problemas generales con ldap
fecha consultada: 5-11-2014
- Sitio: <http://www.josedomingo.org>
url: <http://www.josedomingo.org/web/mod/page/view.php?id=1953>
Tema: autentificacion mediante ldap con moodle
fecha consultada: 4-11-2014
- Sitio: <http://docs.moodle.org>
url: https://docs.moodle.org/19/en/LDAP_authentication
Tema: configuración de la autenticación en moodle
fecha consultada: 4-11-2014