Implementar LDAP: Moodle, clientes escritorio, radius WIFI, OpenVPN, Openstack

Grado Superior en administración de sistemas informáticos en red

2015

Nabil Salhi Mohamed

I.E.S Leopoldo Queipo

03/06/2015

# Índice

# Conceptos básicos:

**¿Qué es openstack?**

* OpenStack es un proyecto de [computación en la nube](http://es.m.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube) para proporcionar una [infraestructura como servicio](http://es.m.wikipedia.org/wiki/Infraestructura_como_servicio), es un software libre y de código abierto distribuido bajo los términos de la licencia Apache.

**¿Qué es LDAP?**

* Permite el acceso a un [servicio de directorio](http://es.wikipedia.org/wiki/Servicio_de_directorio) ordenado y distribuido para buscar diversa información en un entorno de red, LDAP también se considera una [base de datos](http://es.wikipedia.org/wiki/Base_de_datos) a la que pueden realizarse consultas. Habitualmente, almacena la información de [autenticación](http://es.wikipedia.org/wiki/Autenticaci%C3%B3n) (usuario y [contraseña](http://es.wikipedia.org/wiki/Contrase%C3%B1a)) 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](http://es.wikipedia.org/wiki/Certificado_digital), etc). LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.
  + **¿Qué es NSS?**

NSS es un servicio 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, en nuestro caso LDAP (Lightweight Directory Access Protocol)

* + **¿Qué es PAM?**

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.

**¿Qué es 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.

# 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.

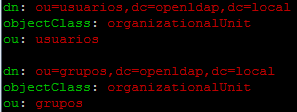
Para configurarlo utilizaremos el comando “dpkg-reconfigure slapd” y seguiremos los pasos del asistente, no pedirá el nombre de dominio, de la organización y una contraseña, elegiremos el motor de la base de datos que será “HDB” y acabaremos con esta configuración.

**Creación de la estructura del directorio**

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

Nuestro servidor utilizará archivos en texto plano con extensión LDIF, en un primer momento se quería montar con mysql pero investigando encontré con que no hay nada oficial relacionado con mysql y LDAP, encontré un plugin pero que está en desarrollo.

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



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

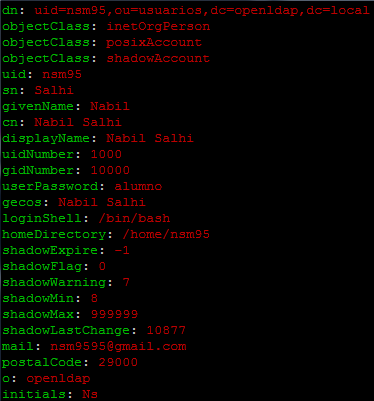
* ldapadd -x -D “cn=admin,dc=openldap,dc=local” -W -f base.ldif

**Añadir usuarios y grupos**

Se realzará 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.

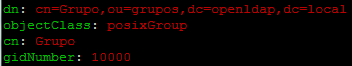


Una vez configurado el fichero ”usuario.ldif” añadiremos esta información a la base de datos OpenLDAP de esta forma:

* 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.

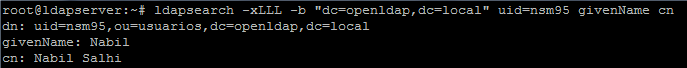
****

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:



# 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 traves 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:

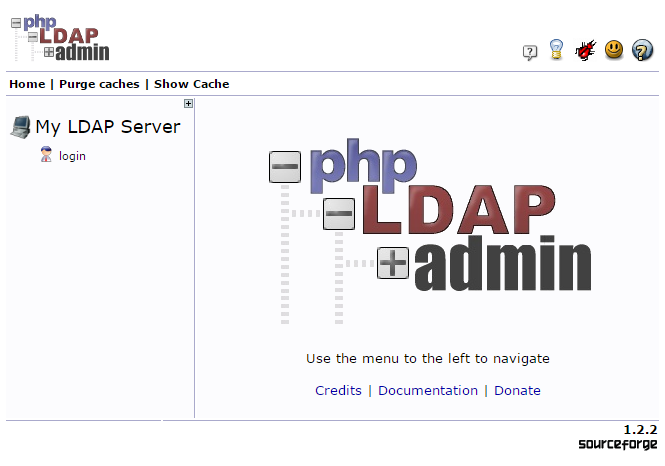
* apt-get install phpldapadmin –y

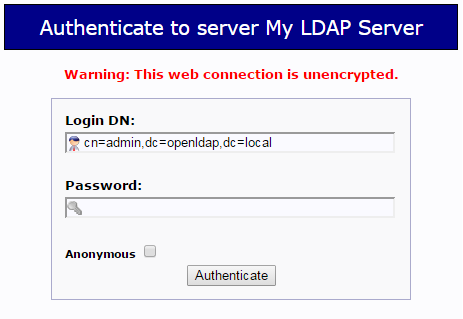
**Acceso al servidor a través de phpLDAPadmin**

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

C:\Users\NsM95\Desktop\direccion phpLDAPadmin.PNG

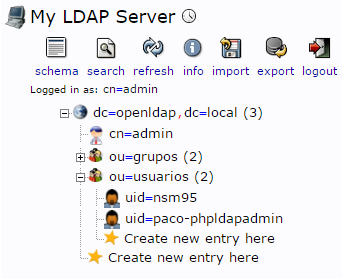
Si todo ha ido correctamente nos aparecerá la pantalla principal de phpLDAPadmin:



Nada comenzar a usar phpLDAPadmin nos encontramos con un inicio de sesión algo raro ya que iniciamos sesión con el nombre de dominio: 

**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”.

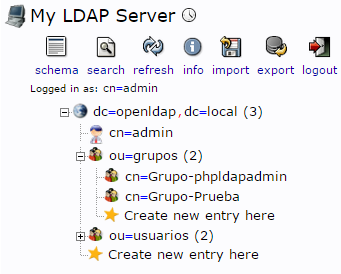
De nuevo cambiará el panel derecho y llegamos a la parte donde rellenar los datos de usuario, al crear por primera vez un usuario no me aparecía el botón de crear objeto que se sitúa al final de la página con lo cual no me dejaba crear ningún usuario, buscando en internet encontré el siguiente error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