Unidad de comunicaciones-fmat

Ldap para directorio activo por Jorge Fuentes.

Tabla de contenido

[Instalación LDAP (Directorio Activo) sobre Linux 2](#_Toc460341799)

[Introducción. 2](#_Toc460341800)

[¿Qué es y cómo funcionan Ldap y OpenLdap? 2](#_Toc460341801)

[Manual de instalación. 4](#_Toc460341802)

[Parte 1: instalación del servicio. 4](#_Toc460341803)

[Parte 1.2 Realizar la configuración básica de openLDAP 5](#_Toc460341804)

[Parte 1.3 Configuración del demonio SLAPD. 10](#_Toc460341805)

[Referencias 12](#_Toc460341806)

Instalación LDAP (Directorio Activo) sobre Linux

# Introducción.

**¿Qué es Ldap?**

LDAP son las siglas de Lightweight Directory Access Protocol (en español Protocolo Ligero de Acceso a Directorios) que hacen referencia a un protocolo a nivel de aplicación el cual 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 directorio es un conjunto de objetos con atributos organizados en una manera lógica y jerárquica. El ejemplo más común es el directorio telefónico, que consiste en una serie de nombres (personas u organizaciones) que están ordenados alfabéticamente, con cada nombre teniendo una dirección y un número de teléfono adjuntos.

**¿Qué es openLdap?**

*OpenLDAP* es un desarrollo del protocolo *LDAP*, implementado con la filosofía del software libre y código abierto.

El proyecto *OpenLDAP* se inició en agosto de 1998 y está sustentado por una entidad sin ánimo de lucro llamada *OpenLDAP Foundation*, creada por el desarrollador estadounidense Kurt D. Zeilenga para coordinar las actividades del proyecto.

*OpenLDAP* está muy optimizado para ofrecer los mejores resultados en situaciones que requieran operaciones de lectura intensivas. De esta forma, un directorio *OpenLDAP* arrojará unos resultados muy superiores a los que ofrece una base de datos relacional optimizada, cuando realicemos operaciones de consulta intensivas sobre ambas.

# ¿Cómo funcionan Ldap y OpenLdap?

El modelo de información de LDAP se basa en entradas, entendiendo por entrada un conjunto de atributos identificados por un nombre global único (Distinguished Name – DN), que se utiliza para identificarla de forma específica. Las entradas se organizan de forma lógica y jerárquica mediante un esquema de directorio, que contiene la definición de los objetos que pueden formar parte del directorio.

Cada entrada del directorio representa un objeto, que puede ser abstracto o real: una persona, un mueble o una función en la estructura de una empresa, etc.

Cada atributo de una entrada tendrá un tipo y un valor con el formato atributo/valor que permite caracterizar un aspecto del objeto que define la entrada. Estos atributos tienen nombres que hacen referencia a su contenido y pueden ser de dos tipos:

* Atributos normales: Son los atributos que identifican al objeto (nombre, apellidos, etc.).
* Atributos operativos: Son los atributos que utiliza el servidor para administrar el directorio (fecha de creación, tamaño, etc.).

Las entradas se indexan mediante el nombre completo (dn), que facilita la identificación singular a cada elemento del árbol. 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.

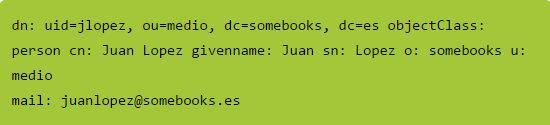
Para referirse al nombre completo suelen utilizarse las siglas RDN, que provienen del inglés Relative Distinguished Name.

Entre los atributos que suelen emplearse habitualmente, encontramos los siguientes, aunque puede haber muchos más:

* 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.
* (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.

Obviamente, los atributos anteriores hacen referencia a un tipo de objeto que representa a los miembros de una empresa. Para representar a otros tipos de objetos, necesitaríamos atributos diferentes.

Una entrada almacenada en el directorio LDAP podría tener el siguiente aspecto:



LDAP establece operaciones para consultar o actualizar el directorio. Estas nos permiten crear o eliminar entradas y modificar entradas existentes.

Este protocolo también se utiliza la mayor parte del tiempo para diversas consultas sobre la información que contiene, por lo que es común que la estructura de su base de datos se encuentre optimizada para la lectura en detrimentos de la escritura.

LDAP puede usarse para organizar de forma unificada el acceso a la información representativa de una red. Sin embargo, es muy frecuente que también almacene la información de autenticación para los usuarios y/o recursos. De esta forma, se facilita el control de acceso sobre los datos contenidos en el servidor.

Por último, LDAP incluye servicios de integridad y confidencialidad de los datos que almacene.

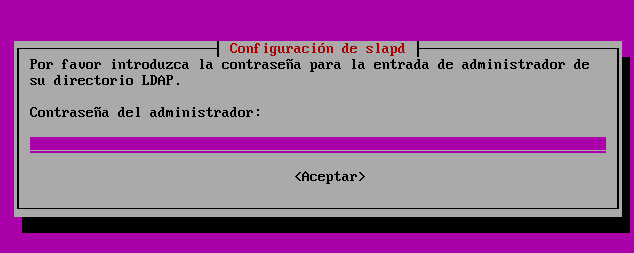
# Manual de instalación.

## Parte 1: instalación del servicio.

Con este comando instalaremos y habilitaremos el servicio de ldap en nuestro servidor

**Sudo apt-get install slapd ldap-utils migrationtools**

Nos preguntara cual será la clave del administrador, la ingresaremos y terminara con la instalación, luego continuaremos con el siguiente comando para configurar correctamente nuestros datos.

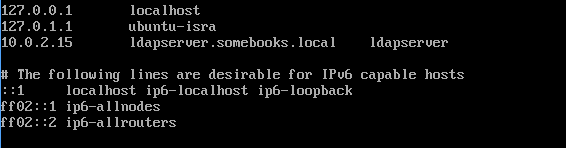


**Nota**\* De forma predeterminada, slapd se configura con las mínimas opciones necesarias para que el demonio funcione de forma correcta.

## Parte 1.2 Realizar la configuración básica de openLDAP

Podemos comenzar modificando el contenido del archivo de hosts en /etc/hosts. El objetivo es para hacer referencia a los nombres de ldapserver o ldapserver.somebooks.local, por ejemplo de nuestro sistema, que entienda que nos estamos refiriendo al servidor.

Dentro del archivo añadimos una nueva línea que relacione la dirección IP estática del servidor con los nombres lógicos que tenemos previsto usar.



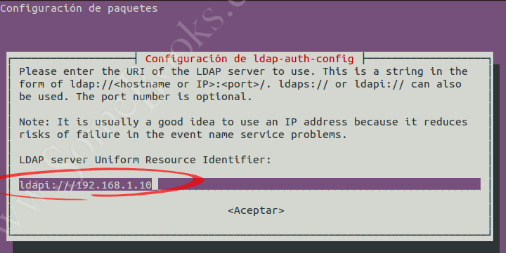
Luego de eso necesitamos instalar la librería NSS (Name Service Switch) para LDAP. Esta librería ofrece una interfaz para acceder y configurar distintas bases de datos utilizadas para almacenar cuentas de usuario (entre otras, /etc/passwd, /etc/group, etc/hosts, Ldap, etc).

El comando es este:

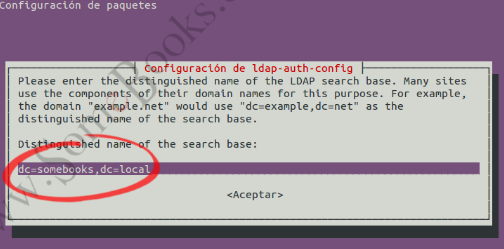
Sudo apt-get install libnss-ldap –y

Instalamos el paquete con privilegios de superusuario.

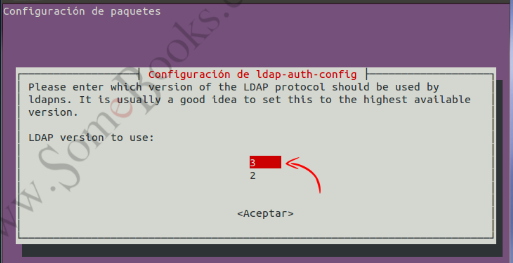
En el primer paso, nos solicita la dirección URI del servidor LDAP. Es importante dejar el principio tal y como lo encontramos (**ldapi:///**).



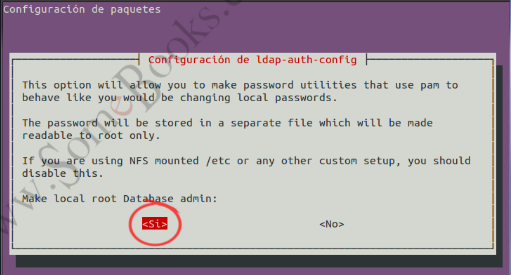
A continuación escribimos el nombre global único (Distinguished Name – DN) siguiendo las indicaciones del principio (dc = somebooks, dc= local)



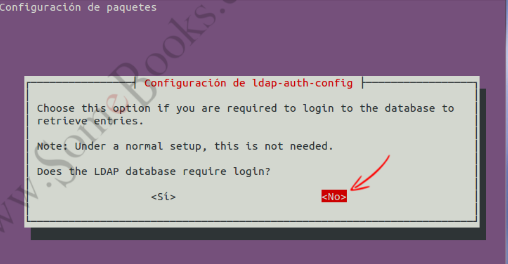
En el siguiente paso, indicaremos la versión del protocolo LDAP que vamo a usar. Salvo que dispongamos en nuestra red de clientes muy antiguos, lo normal será elegir el valor más alto.



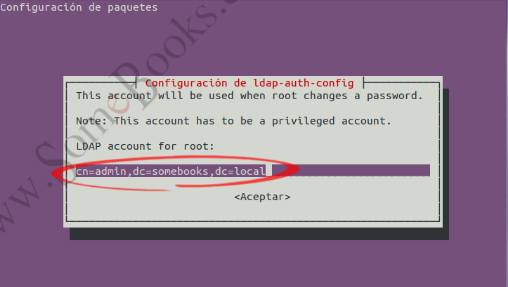
A continuación, indicaremos si las utilidades que utilicen PAM deberán comportarse del mismo modo que cuando cambiamos contraseñas locales. Esto hará que las contraseñas se guarden en un archivo independiente que sólo podrá ser leído por el superusuario.



A continuación, el sistema nos pregunta si queremos que sea necesario identificarse para realizar consultas en la base de datos de LDAP.



Ya sólo nos queda indicar 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) siguiendo las indicaciones que vimos al principio de este capítulo (**cn=admin, dc=somebooks, dc=local**)



En el último paso, el asistente nos solicita la contraseña que usará la cuenta anterior (como siempre, habrá que escribirla por duplicado para evitar errores tipográficos). Deberá coincidir con la que escribimos en el apartado *Instalar OpenLDAP en el servidor*.

Y con esto habremos terminado la configuración básica de LDAP.

Si más adelante observamos algún error o necesitamos efectuar alguna modificación, sólo tenemos que ejecutar el siguiente comando:

sudo dpkg-reconfigure ldap-auth-config

Parte 1.3 Configurar la autentificación para los clientes.

Lo primero que haremos será usar auth-client-config, un script que nos ayuda a modificar archivos de configuración de PAM y NSS. Para conseguirlo, ejecutamos el siguiente comando en la terminal:

sudo auth-client-config -t nss -p lac\_ldap

Explicando el comando, podemos ver que usamos dos atributos en la sentencia:

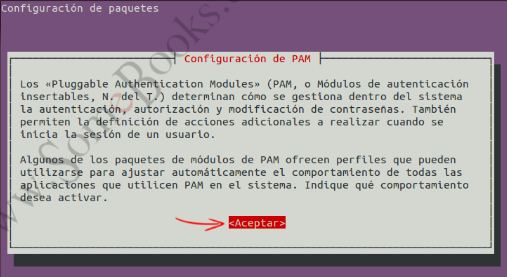
* -t nss, con el que indicamos que los archivos que vamos a configurar son los correspondientes a NSS
* -p lac\_ldap, con el que indicamos que los datos para la configuración debe tomarlos del archivo lac\_ldap. Este archivo se habrá generado durante la ejecución de ldap-auth-config en el punto anterior.

La ejecución de este comando no debe ofrecer ningún tipo de error. De lo contrario, deberíamos repasar la configuración ejecutando de nuevo ldap-auth-config.

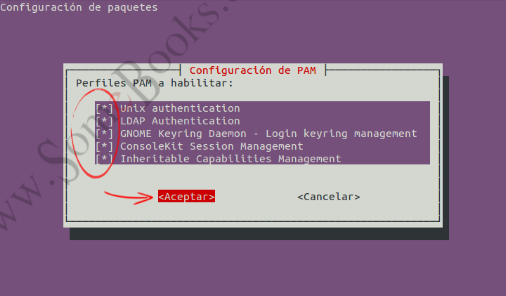
A continuación, deberemos actualizar la configuración de las políticas de autenticación predeterminadas de PAM, lo que conseguimos con el siguiente comando:

Sudo pam-auth-update

Al ejecutarlo, aparecerá un asistente, que nos muestra una primera pantalla informativa sobre la función de los módulos PAM.



En la siguiente pantalla, elegiremos cuáles de los módulos disponibles queremos habilitar. De forma predeterminada aparecen todos marcados…



Una vez acabada la configuración automática, podremos hacer algunos cambios complementarios editando el archivo**/etc/ldap.conf**. Para lograrlo, recurriremos, como siempre, al editor nano:

Sudo nano /etc/ldap.conf

Una vez que se abra el editor, podremos ajustar algunos de los valores del documento, pero, sobre todo, comprobaremos que son correctos los siguientes datos:

host 192.168.1.10 base

dc=somebooks,dc=local

uri ldapi://192.168.1.10/

rootbinddn cn=admin,dc=somebooks,dc=local

ldap\_version 3

bind\_policy soft

Solo nos queda guardar y con esto terminamos la configuración del servidor Ldap. Ahora está listo para autentificar usuarios. Sin embargo, aún queda por establecer el comportamiento del demonio Slapd.

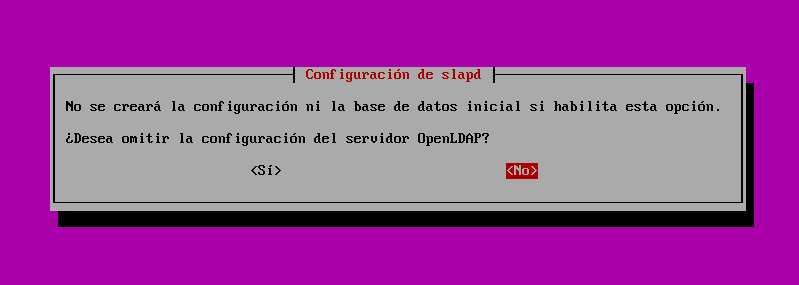
## Parte 1.3 Configuración del demonio SLAPD.

SLAPD (Standalone LDAP Daemon) es un programa multiplataforma, que se ejecuta en segundo plano, atendiendo las solicitudes de autentificación LDAP que se reciban en el servidor.

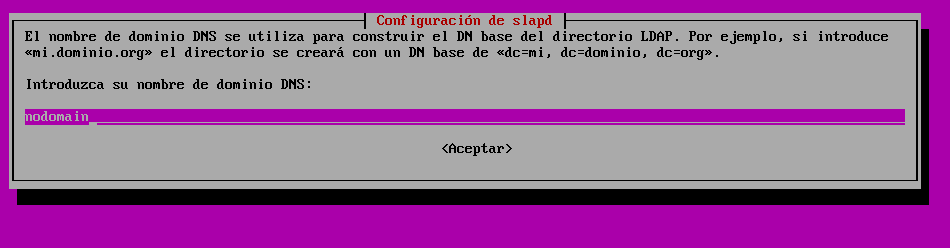
Estableceremos algunos parámetros para la configuración de este demonio. Para conseguirlo, ejecutaremos el siguiente comando:

Sudo dpkg-reconfigure slapd

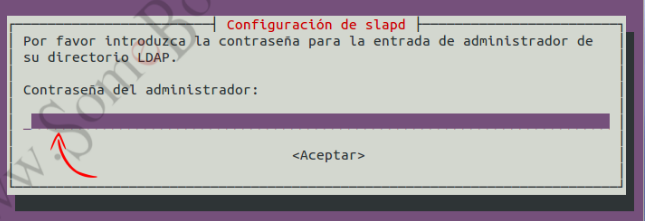
La primera pantalla que muestra es para asegurarnos de que realmente queremos realizar cambios en nuestra configuración. Diremos que no.



Luego nos pide un nombre para nuestro dominio o Distinguised Name base para nuestro directorio. Aquí colocare como DNS: gitlab.local

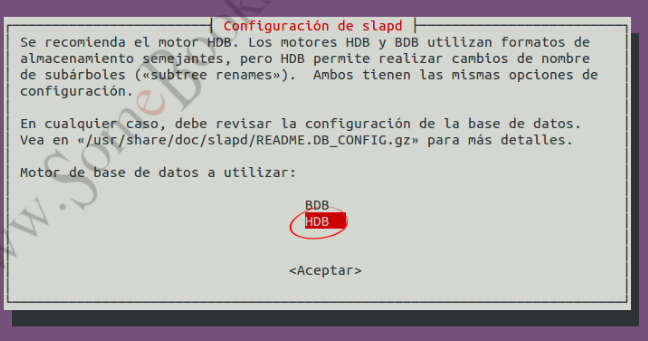


El siguiente paso es nombrar la organización como ejemplo use UC-servidores-Fmat y la contraseña para el administrador de LDAP. La contraseña debe coincidir con la que escribimos en el apartado *Instalar* OpenLDAP en el servidor.

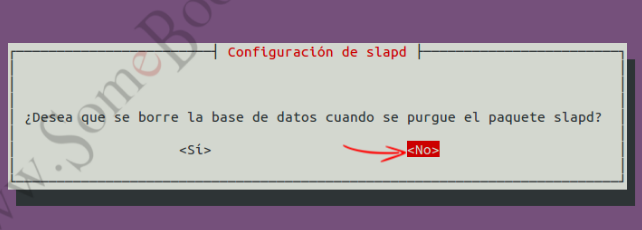


A continuación, elegiremos el motor de la base de datos que usaremos para el directorio. Se recomienda HDB porque nos permitirá, en el futuro, cambiar los nombres de los subárboles si fuese necesario.

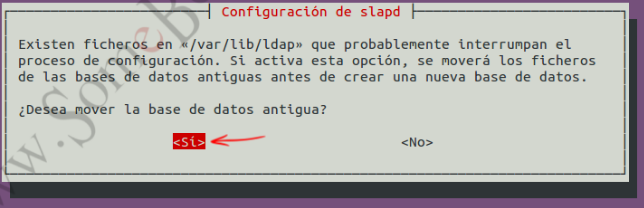
Si HDB no aparece elegida de forma predeterminada, usaremos la tecla *<tabulador>* para desplazarnos.



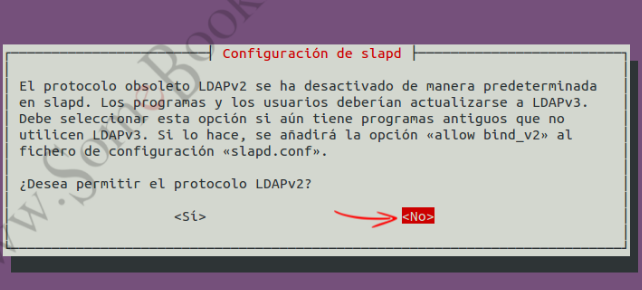
Lo siguiente que nos pregunta el asistente es si queremos que se borre la base de datos anterior del directorio cuando terminemos la configuración de *slapd*. Elegiremos la opción No.



A continuación, como hemos decidido no borrar la base de datos antigua, el asistente nos pregunta si queremos cambiarla de sitio.



En algunas redes, con clientes muy antiguos, puede ser necesario mantener la versión 2 del protocolo*LDAP*. Por ese motivo, antes de terminar, el asistente nos pregunta queremos permitir el protocolo LDAPv2.



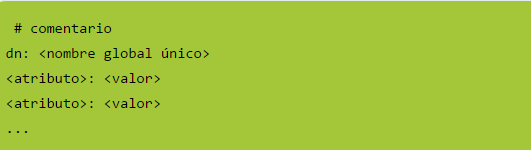
Después de este último paso, se cierra el asistente y volvemos a la consola. Con esto terminamos la configuración del LDAP. Ahora veremos cómo autentificar usuarios.

## Parte 2. Creación de la estructura del directorio.

Una vez configurado el servidor, deberemos configurar la estructura básica del directorio. Es decir, crearemos la estructura jerárquica del árbol (*DIT* – Directory Information Tree).

Una de las formas más sencillas de añadir información al directorio es utilizar archivos LDIF (LDAP Data Interchange Format). En realidad, se trata de archivos en texto plano, pero con un formato particular que debemos conocer poder construirlos correctamente

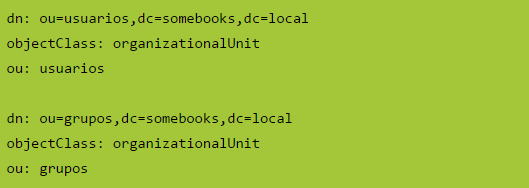
Un formato básico de entrada se vería así:



Con esta información en mente, crearemos un archivo que contenga los tipos de objeto básicos del directorio. Comenzaremos por abrir un editor de textos, por ejemplo *nano*, indicándole el nombre de nuestro archivo:

Sudo nano ~/base.ldif

Una vez creado el archivo, escribimos en el:

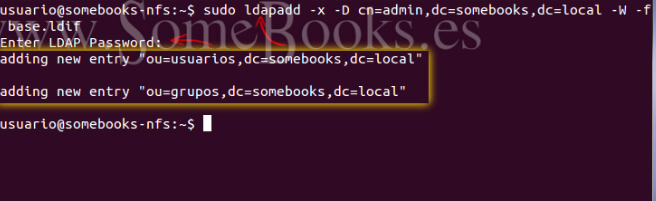


En dc=somebooks, dc=local seria reemplazado con mi dominio gitlab.local y quedaría de esta forma para todos valores correspondientes.

dn: ou=usuarios,dc=gitlab,dc=local

A continuación, deberemos añadir la información a la base de datos *OpenLDAP*. Como sabemos, esto se hace con el comando *ldapadd*:

sudo ldapadd -x -D cn=admin,dc=somebooks,dc=local -W -f base.ldif



Podemos comprobar que los usuarios fueron añadidos.

## Parte 3. Añadir un usuario

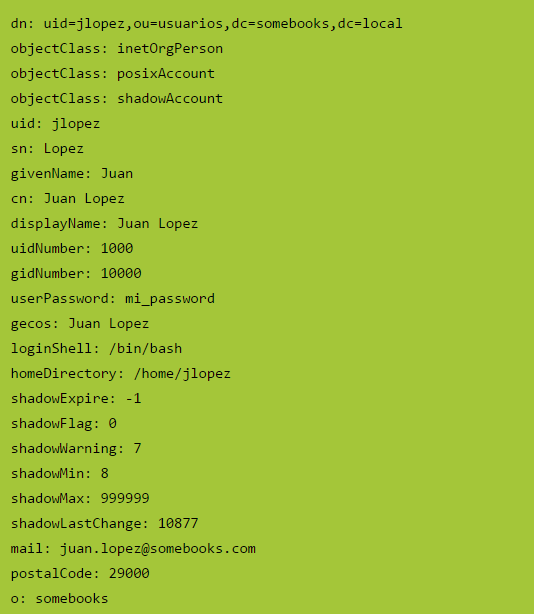
Crearemos un archivo para almacenar nuestros usuarios:

Sudo nano ~/usuarios.ldif

En el escribiremos algo como lo siguiente:

**Nota\*** Recordemos que en la primera línea debemos colocar correctamente el nombre de nuestro dominio, no debemos olvidar para cada user que creemos, por ejemplo en mi caso mi dominio es gitlab.local entonces en la primera línea de código iria esto:

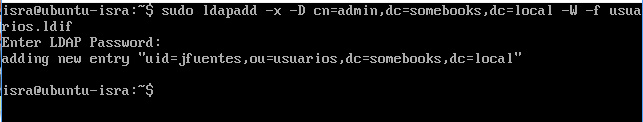
dn: ou= usuarios, dc=gitlab,dc=local



Luego salvamos el archivo con Ctrl- o y luego sali de ahí con Ctrl- x

Después añadimos el usuario al directorio activo con el siguiente comando:

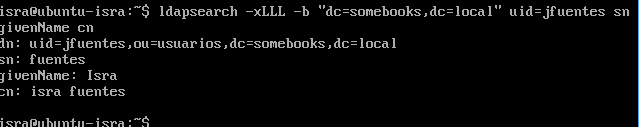
Sudo ldapadd –x –D cn=admin,dc=gitlab,dc=local –W –f usuarios.ldif



## Parte 4. Verificar que existen usuarios en el directorio

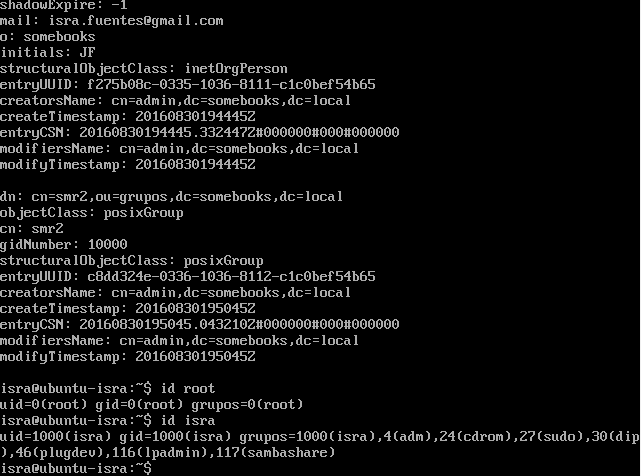
Para realizar esto necesitamos del comando “ldapsearch” para una búsqueda con parámetros específicos, o con el comando “slapcat” que nos despliega todo el contenido de nuestro directorio activo.

Explicando el comando de ejemplo en la captura.



Para este caso debemos indicar el DN (en mi ejemplo somebooks.local) en donde buscara por el directorio a los usuarios con los parámetros de búsqueda “uid” en mi ejemplo busco por el usuario jFuentes y luego le pido que me despliegue sus datos de “sn”, “givenName” y el “cn”.

**Captura del comando “slapcat”.**



También podemos ver información solo preguntando por medio del comando “id” luego escribiendo algún nombre que pertenezca al directorio como se observa en la captura de arriba con el ejemplo id root.

# Referencias

Ruiz, P. (11 de agosto de 2012). *SomeBooks*. Obtenido de Instalar y configurar OpenLDAP en el servidor Ubuntu: http://somebooks.es/

Zelaya, F. A. (14 de 09 de 2012). *Taringa*. Obtenido de http://www.taringa.net/post/linux/15577207/Instalacion-LDAP-Directorio-Activo-sobre-Ubuntu-Server.html