

Lightweight Directory Access Protocol (LDAP) es un protocolo que permite el acceso a un directorio con información diversa como recursos, servicios, ordenadores, usuarios, etc. LDAP es una norma implementada en Linux con OpenLDAP. Aunque OpenLDAP puede gestionar mucha información, actualmente se utiliza principalmente para autenticación de usuarios y como guía de direcciones de correo y teléfonos. OpenLDAP está muy lejos de otros servicios de directorio más avanzados como [NDS de Novell](#).

LDAP es un sistema cliente-servidor. Un cliente LDAP se conecta a un servidor LDAP y solicita información o proporciona los datos necesarios para acceder a un directorio. El servidor responde a la solicitud, envía la consulta a otro servidor o acepta la información para incorporarla al directorio.

Voy a utilizar openLDAP para crear un directorio de direcciones de correo y teléfonos del personal de la empresa, que podrá ser consultado por clientes LDAP como Netscape, Outlook o via web con la utilidad [web500gw](#).

Instalo los paquetes openldap-1.2.9-5 y openldap-devel-1.2.9-5. Los ficheros de configuración están en `/etc/openldap` donde se encuentra `ldap.conf` y `slapd.conf`

```
file:/etc/openldap/ldap.conf
```

```
-----  
BASE o=miempresa.es  
# IP del host donde está el server LDAP  
HOST 192.168.8.1
```

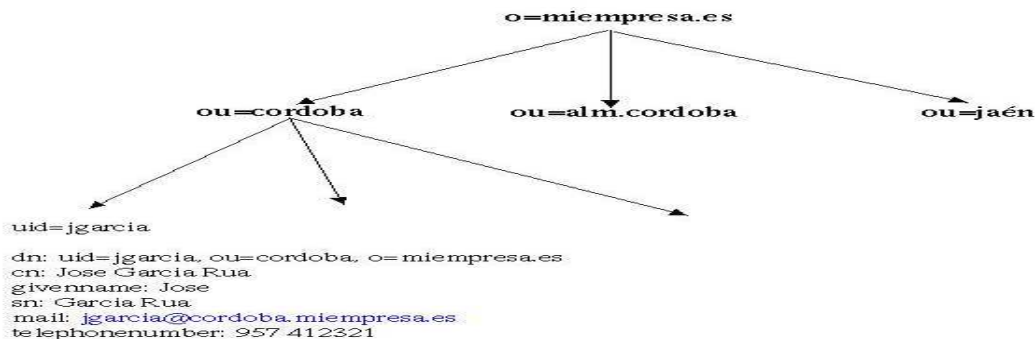
```
file:/etc/openldap/slapd.conf
```

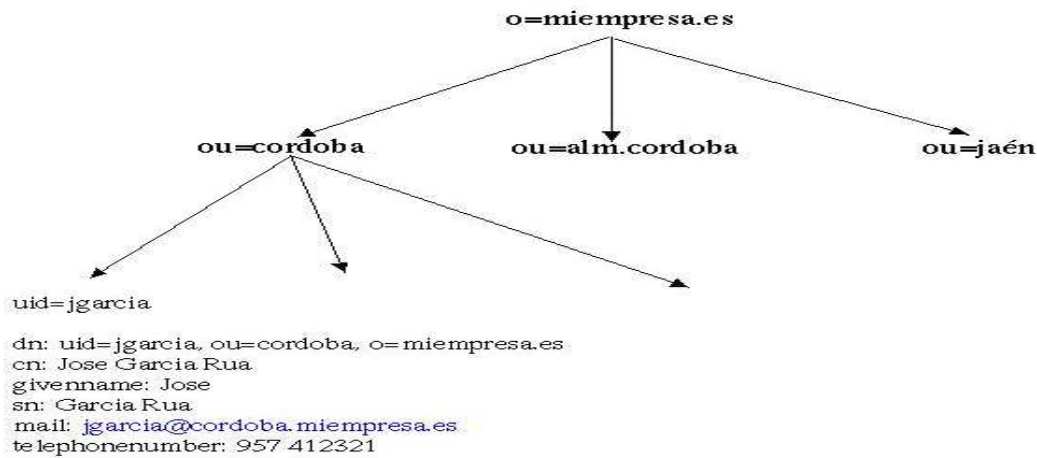
```
-----  
include /etc/openldap/slapd.at.conf  
include /etc/openldap/slapd.oc.conf  
schemacheck off
```

```
pidfile /var/run/slapd.pid  
argsfile /var/run/slapd.args
```

```
#####  
# ldbm database definitions  
#####  
# tipo de base de datos  
database ldbm  
# raiz del directorio  
suffix "o=miempresa.es"  
# nombre distintivo del directorio  
rootdn "cn=master, o=miempresa.es"  
# password  
rootpw horka.8  
# directorio donde se crean las bases de datos  
directory /var/lib/ldap
```

Las bases de datos en LDAP tienen una estructura arborescente, el siguiente diagrama muestra la estructura del directorio en el que se basan las explicaciones de este documento:





Donde "ou" lo he utilizado para especificar el nombre de host, el "dn" es el Distinguished Name, es un nombre unico en el directorio, el resto son los atributos de las entradas del directorio que están predefinidas en `slapd.oc.conf` y `slapd.at.conf`.

Ejecuto el servidor ldap, en RedHat: `/etc/rc.d/init.d/ldap start`

Para añadir entradas en el directorio creo el fichero `miempres.es.ldif` con un formato llamado LDIF:

```
file:miempres.es.ldif
```

```
-----
dn: o=miempres.es
o: miempres.es
object class: top
objectclass: organization

```

```
dn: ou=cordoba, o=miempres.es
ou: cordoba
description: Sede Central Cordoba
streetAddress: C/ Marruecos, 1
l: Cordoba
postalCode: 14023
telephoneNumber: 957 22 33 44
objectclass: organizationalUnit

```

```
dn: ou=alm.cordoba, o=miempres.es
ou: alm.cordoba
description: Almacen
streetAddress: C/ Marruecos, 3
l: Cordoba
postalCode: 14023
telephoneNumber: 957 22 33 55
objectclass: organizationalUnit

```

```
dn: ou=sevilla, o=miempres.es
ou: sevilla
description: Sede Central Sevilla
streetAddress: C/ Arco, 25
l: Sevilla
postalCode: 41023
telephoneNumber: 957 11 22 33
objectclass: organizationalUnit

```

```
dn: uid=jgarcia, ou=cordoba, o=miempres.es
description: Jefe Informatica
uid: jgarcia
cn: Jose Garcia Rua
givenname: Jose
sn: Garcia Rua

```

mail: jgarcia@cordoba.miempresa.es  
telephoneNumber: 957 42 32 34  
l: Cordoba  
ou: cordoba  
objectclass: person

dn: uid=lhuertas, ou=alm.cordoba, o=miempresa.es  
description: Responsable Almacen  
uid: lhuertas  
cn: Lolo Huertas Perez  
givenname: Lolo  
sn: Huertas Perez  
mail: lhuertas@alm.cordoba.miempresa.es  
telephoneNumber: 957 42 32 33  
l: Cordoba  
ou: cordoba  
objectclass: person

dn: uid=smontero, ou=sevilla, o=miempresa.es  
description: Jefe Informatica  
uid: smontero  
cn: Santiago Montero Garcia  
givenname: Santiago  
sn: Montero Garcia  
mail: smontero@sevilla.miempresa.es  
telephoneNumber: 951 23 62 35  
l: Sevilla  
ou: sevilla  
objectclass: person

En el primer párrafo creo la raíz del directorio, con el segundo, tercer y cuarto párrafo creo el segundo nivel en el directorio, y el resto son los "registros". Ejecuto el comando

```
# ldapadd -D "cn=master, o=miempresa.es" -W < miempresa.es.ldif
```

y se crea el directorio.

Para buscar datos se utiliza *ldapsearch*:

```
# ldapsearch uid="jgarcia"
```

Para borrar y modificar datos del directorio, el paquete OpenLDAP incluye los comandos *ldapdelete* y *ldapmodify*.

Configuración de clientes LDAP:

- Para acceder al directorio LDAP desde Netscape, en Preferencias añado un nuevo Directorio con los siguientes datos:

*Descripción: Servidor LDAP MiEmpresa*  
*Servidor LDAP: pinero*  
*Buscar en raíz: o=miempresa.es*  
*Número de puerto: 389*

En el Libro de Direcciones selecciono el Directorio "*Servidor LDAP MiEmpresa*" y ya puedo realizar búsquedas en el directorio por los campos Nombre, email, teléfono, etc.

- Con Outlook 98, supongo que en otras versiones será parecido, en el menú *Herramientas/Cuentas*, en la pestaña *Servicio de Directorio*, hago click en el botón *Agregar/Servicio de Directorio*, y se inicia el asistente, en:

*Servidor de Directorio de internet LDAP: pinero*  
*Nombre del servicio de Directorio: Servidor LDAP MiEmpresa*

y click en botón *Finalizar*, click en botón *propiedades*, otro click en la pestaña *Avanzado* y en el cuadro de texto *Base de búsqueda: o=miempresa.es*

Para buscar entradas en el Directorio ejecutar Inicio/Buscar/Personas o en la Libreta de Direcciones en Edición/Buscar.

- [web500gw](http://web500gw) es otro cliente LDAP, una vez instalado se configura mediante el fichero *web500gw.conf*, cuyos parámetros más

importantes son:

```
file://web500gw.conf
-----
# Nombre del servidor LDAP
ldapserv pinero

# Nombre Directorio
homedn: o=miempresa.es
```

Ejecuto el demonio web500gw y en el navegador escribo: <http://pinero:8888> y ya puedo realizar consultas en el Directorio de forma muy cómoda.

El resultado es que tengo una guía telefónica y direcciones emails del personal de la empresa, fácil de mantener y consultar.

Más información en <http://www.openldap.org>, en <http://www.tu-chemnitz.de/web500gw/>, en el The SLAPD and SLURPD Administrators Guide y en [LDAP-Linux-Como](#).

---

GarZa, garzalin@worldonline.es

Sobre el Copyright: todos los documentos publicados en el sitio web LinuxGarZa, están bajo los derechos de copyright de GarZa o de sus autores, y pueden ser distribuidos total o parcialmente, en cualquier medio físico o electrónico incluyendo esta nota de derechos en todas las copias. Todas las traducciones, trabajos derivados o adicionales que incorporen alguno de nuestros documentos o parte de su contenido deben ser cubiertos bajo esta nota de derechos y de cualquier trabajo derivado de éste documento no se pueden imponer restricciones a su distribución gratuita.