

Instalacion Inicial

Instalación Basica

1. Una vez obtenido el archivo *Tar* que contiene OpenLDAP, este debe ser descomprimido en un directorio temporal (`/tmp` por lo general) para poder iniciar la instalación.
2. Dentro del directorio temporal (`/tmp`) donde fue descomprimido OpenLDAP ejecute el comando: `./configure` , este comando configura los archivos de instalación de acuerdo a su sistema.
3. Posteriormente debe ejecutar `make depend` seguido de `make` , esto genera OpenLDAP dentro del *mismo directorio temporal*.
4. Debe ejecutar ciertas pruebas para garantizar que OpenLDAP funcione correctamente, colóquese dentro del directorio `tests` y ejecute `make`
5. Ahora si debe *instalar* OpenLDAP en el sistema, descienda del directorio `tests` y como raíz ejecute: `make install`
6. El comando anterior instala OpenLDAP bajo el directorio `/usr/local/etc/openldap` (si no cambio este parametro al tiempo de compilar OpenLDAP).
7. La instalación esta completa, ahora debe configurar los parametros basicos.

slapd.conf

El archivo `slapd.conf` ubicado dentro del directorio `/usr/local/etc/openldap/` contiene los parametros *globales* y *especificos por arbol* que serán utilizados por el servidor LDAP, éste es descrito a detalle en [Configuración y Ejecución de OpenLDAP](#)

Configuración y Ejecución

slapd.conf

Es el archivo principal de OpenLDAP y es aqui donde se configuran todos sus parametros, si realizó la instalación de acuerdo a esta guía, `slapd.conf` se encuentra dentro del directorio `/usr/local/etc/openldap`

Parametros Globales

Los parametros dentro de esta sección afectan el funcionamiento de todo el Servidor OpenLDAP, cualquier definición antes de un parametro `database` es considerado **global**, cabe mencionarse que los valores de parametros globales pueden ser contrarrestados al nivel de **bases de datos**, esto es, si se define el parametro `access` globalmente, es posible alterar el valor de este parametro en "X" base de datos y el resto de las bases de datos permanecerán con el valor **global**.

Los siguientes son parametros globales *basicos* para *slapd.conf* :

```
include          /usr/local/etc/openldap/slapd.at.conf
include          /usr/local/etc/openldap/slapd.oc.conf
schemacheck     off
#referral       ldap://root.openldap.org/
#access to *    by * write
pidfile         /usr/local/var/slapd.pid
argsfile        /usr/local/var/slapd.args
loglevel 0
```

- `include` : Este parametro indica otros archivos de configuración utilizados por el Servidor OpenLDAP, la declaración anterior carga los archivos `slapd.at.conf` y `slapd.oc.conf`, otros archivos de configuración ampliamente utilizados globalmente son denominados *schemas* .
- `schemacheck`: Es utilizado para la verificación de *schemas* , la utilización de *Schemas* es un tema muy amplio por ahora basta desactivarlo (`off`).
- `referral`: Indica un Servidor LDAP alternativo en dado caso de no poderse efectuar la búsqueda en el servidor LDAP actual.(Desactivado con comentario `#`).
- `access to ...`: Parametro utilizado para restringir acceso al servidor LDAP, la utilización de acceso también es un tema muy amplio descrito en otra sección de esta guía. (Desactivado con comentario `#`)
- `pidfile` : Contiene el numero de proceso asignado al servidor LDAP al arranque. (Vea: [Ejecución y Terminación del Servidor LDAP](#))
- `argsfile` : Contiene parametros utilizados en la linea de comandos al iniciar el servidor OpenLDAP (Vea: [Ejecución y Terminación del Servidor LDAP](#))
- `loglevel` : Indica el nivel de registros ("log") producidos por el servidor LDAP, posibles valores:

Level Description	Level Description
-1 enable all debugging	0 no debugging
1 trace function calls	2 debug packet handling
4 heavy trace debugging	8 connection management
16 print out packets sent and received	32 search filter processing
64 configuration file processing	access
256 stats log connections/operations/results	128 control list processing
1024 print communication with shell backends	512 stats log entries sent
	print entry
	2048 parsing debugging

Parametros por Base de Datos

Dentro de cada servidor LDAP se pueden encontrar *varias base de datos*, es dentro de estas *bases de datos* que residirá toda información del Servidor OpenLDAP.

NOTA: En el sentido más estricto de la palabra OpenLDAP no utiliza una [base de datos](#) , la "base de datos" utilizada en OpenLDAP es un tipo de "Flat File" generalmente `ldbm` .

Una definición para base de datos seria la siguiente:

```
database        ldbm
suffix          "dc=osmosislatina, dc=com"
```

```
#suffix          "o=Osmosislatina, c=MX"
rootdn          "cn=Admin, dc=osmosislatina, dc=com"
#rootdn         "cn=Admin, o=Osmosislatina, c=MX"
rootpw         daniel
directory      /usr/local/var/openldap-ldbm
```

- `database`: Indica el tipo de "base de datos" a utilizarse, generalmente del tipo `ldbm` (Otras alternativas: `shell,passwd`), además indica el inicio de "base de datos", esto es, cada declaración de `database` se considera una "base de datos" por separado, esto será descrito a mayor detalle en [Insertar datos en OpenLDAP](#).
- `suffix`: Este parametro indica el *nodo raiz* de la base de datos, esto es, el nodo sobre el cual será derivada toda la información, en este caso `dc=osmosislatina, dc=com` (Notese que este también pudo ser `o=Osmosislatina, c=MX`). Lo anterior indica que toda información dentro de esta "base de datos" LDAP descenderá de la jerarquía `dc=osmosislatina, dc=com` (Esta jerarquía fue ilustrada en [LDAP](#)). Lo anterior será descrito a mayor detalle en [Insertar datos en OpenLDAP](#)
- `rootdn` : Establece el nodo ("usuario") que tiene privilegios globales para modificar la "base de datos" LDAP, en este caso `cn=Admin`, notese que *desciende* del nodo raiz (`suffix`) `dc=osmosislatina, dc=com` .
- `rootpw` : Indica la contraseña para el usuario `rootdn`.
- `directory` : Define el directorio donde residirá la base de datos, este directorio debe existir antes iniciar el Servidor LDAP.

Ejecución y Terminación del Servidor LDAP

Ejecución

Para iniciar OpenLDAP se ejecuta el comando `slapd`, ubicado en `/usr/local/libexec/`, esto inicia el Daemon LDAP bajo el **puerto TCP 389** por default. Al momento de ejecutar `slapd` también es posible indicar ciertos parametros de arranque como el (los) puerto(s) TCP: `slapd -h "ldaps:// ldap://127.0.0.1:978"`, lo anterior inicia el servidor LDAP bajo SSL (Secure Socket Layer) bajo el puerto default 636 y bajo el puerto TCP 978 (en vez del default 389).

El indicar estos parametros en la linea de comandos *cada ocasión* puede ser tedioso, por lo que se recomienda agregar estos parametros al archivo `slapd.args` ubicado generalmente en `/usr/local/var/` (ambos modificables de `slapd.conf`).

Para cerciorarse que el servidor LDAP esta operativo realice un `telnet` al puerto TCP en cuestion: `telnet localhost 389`, si la conexión no es aceptada verifique los registros ("logs") de OpenLDAP.

Terminación

Para terminar el Daemon LDAP se debe ejecutar: `kill -INT `cat /usr/local/var/slapd.pid``, lo anterior asume que el parametro `pidfile` en `slapd.conf` se encuentra definido como: `pidfile /usr/local/var/slapd.pid`.

Registros ("Logs")

En el archivo `slapd.conf` se indico un nivel de registro ("logs") mediante el parametro `loglevel`, pero a que archivo ("logfile") es enviada esta información ?

OpenLDAP por "default" envia su información de registro ("log") al Daemon `syslogd` (`syslogd`) bajo el canal `LOCAL4`, sin entrar en los detalles de `syslogd` se deben realizar los siguientes pasos:

- Modificar el archivo [syslog.conf](#), agregando una linea como la siguiente:

```
local4.*                                /var/log/openldap
```

Lo anterior indica enviar todo mensaje del canal `LOCAL4` al archivo `/var/log/openldap`

- Reiniciar el daemon `syslogd` con el comando: `killall -HUP syslogd`

Busquedas e Insercion de Datos

El insertar información en un servidor LDAP es uno de los primeros pasos a seguir después de su instalación, pero antes de insertar información es conveniente saber cual es su estructura dentro de las bases de datos (LDBM) utilizadas por LDAP .

Todo nodo o fragmento en un servidor LDAP es un **DN Distinguished Name**

Es dentro de cada **Distinguished Name** que son definidos distintos *atributos* los cuales contienen información relevante como: Contraseñas, Apellidos, Fotografías, Nodos IP, o cualquier otro fragmento de información imaginable.

Distinguished Name Raiz (suffix)

Cuando son definidos [parametros para base de datos](#) siempre se indica un **DN (Distinguished Name) raiz**, éste debe ser representativo de la estructura jerarquica que se intenta captar.

DISTINGUISHED NAME Raiz

mexico	mexico	brasil	brasil	venezuela	venezuela
drubio	garaiza	lsantos	ffontes	kpiment	agarcia
3ffw12eg	2emndfs	we334faf	tert232	4fhlzpq	dfvn24f
(52)-(6)-3422321	(52)-(5)-2353312	(55)-(11)-8696446	(55)-(21)-7453242	(58)-(2)-4943421	(58)-(61)-6543231

La jerarquia anterior representa una organización , por lo que el **Distinguished Name Raiz** puede ser:

"dc=osmosislatina, dc=com"

o

"o=Osmosislatina, c=MX"

La composición de cada **distinguished name** puede variar, en este caso se utilizaron los vocablos `dc` de "Domain Component", `c` de "Country", `o` de "Object", sin embargo también hubiera sido posible utilizar `p` de "Pais", `cd` de "Componente Dominio". Los vocablos son *solo descriptivos* y su única restricción (si existiese) es llevada acabo en la *definicion de Schemas* .

Distinguished Name Administrativo (rootdn)

Además del *DN distinguished name raiz*, previa inserción de datos también existe un *DN* el cual posee acceso global sobre la base de datos (LDBM) en cuestión. Este *DN* es derivado del *DN raiz*, por lo que puede ser: "cn=Admin, dc=osmosislatina, dc=com", donde se utiliza `cn` como vocablo y `Admin` como valor, sin embargo, al igual que el *DN raiz*, este vocablo y valor pueden variar.

Para acceder la base de datos (LDBM) utilizando el *DN administrativo* se emplea la contraseña también definida en `slapd.conf` mediante el parametro `rootpw`.

Archivos LDIF

Estas estructuras o **DN distinguished names** generalmente se definen en archivos denominados LDIF. El siguiente archivo LDIF contiene los *DN's* mencionados anteriormente (*raiz* y *administrativo*):

```
dn: dc=osmosislatina,dc=com
objectClass: dcObject
objectClass: organization
o: Osmosislatina
description: Desarrollos Open-Soruce en Español

# Rol para administrador de la Red

dn: cn=Admin,dc=osmosislatina,dc=com
objectClass: organizationalRole
cn: Admin
description: Administrador del Servidor LDAP
```

El primer elemento de cada estructura es casi obvio *dn* de *distinguished name*. Los **elementos en azul** `objectclass` estan directamente relacionados con *Schemas* y definen el tipo de objeto para el *DN*, esto es: cuales y cuantos atributos puede contener.

Posteriormente se definen los **Atributos** para cada *DN*:

- `o` y `description` para el primer *DN*
- `cn` y `description` para el segundo *DN*

Notese que no necesariamente existe correlación *directa* entre el *DN* y sus atributos, y como fue mencionado anteriormente la única restricción para atributos (si existiese) es llevada a cabo mediante *Schemas*

Insertar *DN's* *raiz* y *administrativo*

Aunque los *DN's* *raiz* y *administrativos* se encuentran *definidos* para una base de datos (LDBM) es necesario *insertarlos* antes de realizar cualquier tipo de operación, el siguiente ejemplo asume que los [parametros para base de datos](#) definidos en la seccion de configuracion serán utilizados.

- Una vez definido un archivo LDIF con los *DN's* *raiz* y *administrativos*. (Como el [definido anteriormente](#))
- Ejecute el comando:

```
ldapadd -f osmo.ldif -D "cn=Admin,dc=osmosislatina,dc=com" -w daniel
```

Donde `osmo.ldif` es el archivo LDIF.

- Si aparece `adding new entry dc=smosislatina,dc=com` fue exitosa la inserción, de otra manera deberá revisar [Registros \("logs"\) de OpenLDAP](#) para observar el error ocurrido.

DN's Generales

Una vez definidos los *DN's* *raiz* y *administrativo* es posible insertar otros *DN's* que conformarán parte de la jerarquia. A continuación tres *DN's* estructurados como un archivo LDIF:

```
dn: cn=Daniel Rubio,dc=osmosislatina,dc=com
cn: Daniel Rubio
p=Mexico
mail: daniel@osmosislatina.com
telefono: (52)-(6)-3422321

dn: cn=Fernanda Fontes,dc=osmosislatina,dc=com
cn: Fernanda Fontes
p=Brazil
mail: fontes@yahoo.com
telefono: (55)-(11)-8696446

dn: cn=Luis Arano,dc=osmosislatina,dc=com
cn: Luis Arano
p=Argentina
mail: larano@slb.com
telefono: (58)-(2)-4943421
```

Para agregar estos *DN's* a la base de datos (LDBM) se debe ejecutar:

```
ldapadd -f personal.ldif -D "cn=Admin,dc=osmosislatina,dc=com" -w daniel
```

Donde `personal.ldif` es el archivo LDIF definido en la parte superior.

Mas DN's

Los *DN's* y sus atributos declarados anteriormente son *solo basicos*, ya que es posible definir una extensa jerarquia asi como atributos; *DN's* por paises, oficinas, hardware....., asi como atributos relacionados con: [nodos IP](#), contraseñas, fotografías [JPEG o GIF](#)

Busquedas

Con los *DN's* que ya han sido insertados en la base de datos (LDBM) del servidor LDAP, ya es posible realizar busquedas de información:

- `ldapsearch -bdc=osmosislatina,dc=com telefono=*52*` : Busca los *DN's* bajo el *DN* raiz `dc=osmosislatina,dc=com` que contengan el atributo `telefono` con las cifras 52
- `ldapsearch -bdc=osmosislatina,dc=com mail=*` : Busca los *DN's* bajo el *DN* raiz `dc=osmosislatina,dc=com` que contengan el atributo `email`.

La instalación del servidor OpenLDAP que ha sido llevada acabo permite que cualquier tipo de búsqueda sea llevada acabo, sin embargo, en un ambiente de producción es un hecho que deben ser agregados diversos filtros y restricciones en base al usuario que este realizando la búsqueda.

Otras Herrmientas para Insertar y Buscar Información en un Servidor LDAP

Los ejemplos anteriores utilizaron las herramientas `ldapadd` y `ldapsearch` ofrecidas por OpenLDAP, sin embargo, cabe mencionar que existen otras herramientas para realizar busquedas e insertar información en *cualquier* directorio LDAP:

- [Clientes LDAP](#) : Lista de Diversos Clientes LDAP para ambientes Windows y Unix.
- [LDAP Browser/Editor 2.8.2](#) : Cliente LDAP escrito en Java.
- [Writing LDAP Clients](#) : Instrucciones para escribir un cliente LDAP en C.

-
- **Actualizado** : 2002/06/11 23:12
 - **Autor**: Daniel Rubio (daniel@osmosislatina.com)

[Enviar esta pagina a un Amigo](#) | [Agregarse a la lista de Correo](#) | [Mapa OsmosisLatina](#)
[Administración de Información](#) | [Aplicaciones](#) | [Conectividad](#) | [Guías Rapidas](#) | [Mercadotecnia](#)
[Noticias](#) | [Que Hacemos](#) | [Servicios](#) | [Soporte de Sistemas](#) | [XML y Java](#)