

1.- Choose your hardware platform

- **Processor:** Normally multiprocessors machines
- **Disks:** For OpenLDAP is better that you use one hard disk for the OS (with or without RAID) and other separate disk for the database (normally without RAID)
To choose one adequate disk you can go to <http://www.kegel.com/drives/>
This is the most important improve.
- **Choose memory size:** It depends of the load test and benchmarks. Normally between 2 and 5 GB

2.- Install Operative System

- Design one simple installation
- Update with the latest updates (i.e.: sunsolve.sun.com, redhat.com....)
- Choose one filesystem, normally:
 - o Ext3 for Linux
 - o UFS with LOGGING for SolarisIt's really important to choose 'logging' on UFS because increase performance dramatically.
Others: Veritas Filesystem
- Stops all innecessaries daemons
- Securize your machine
- Tune your operative system (there are diverse ways to do that)
- Tune your TCP stack

3.- Nomenclature

- Choose a directory nomenclature to all your work (you must think on updates)

One example is to use a directory like /opt/apps
/opt/source/openldap-2.0.25 directory with source code
/opt/apps/openldap-2.0.25 directory to your application
/opt/apps/openldap is a soft link to the previous
/opt/data/openldap is the directory for the database
/opt/backup is the dairy hard disk backup

With a nomenclature like this is easy make updates.

- Choose a nomenclature for all your users, LDAP users....

4.- Compiling OpenLDAP

- Choose if you want options like
 - o TLS/SSL support
 - o Ipv6 support (normally not needed)
 - o OpenLDAP in Chroot Jail (more secure)
 - o OpenLDAP running with another user (not with owner root)
- Always is a good idea keep a log with all changes:

Simply run the following command before installing the software:

```
[root@dep /root]# find /* > OpenLDAP1
```

And the following one after you install the software:

```
[root@dep /root]# find /* > OpenLDAP2
```

Then use the following command to get a list of what changed:

```
[root@dep /root]# diff OpenLDAP1 OpenLDAP2 > OpenLDAP-Installed
```

- Download latest stable OpenLDAP (today is 2.0.25) and verify the MD5 checksum of OpenLDAP, use the following command:

```
[root@dep tmp]# md5sum openldap-version.tgzstalled
```

Now check that this checksum is exactly the same as the one available into a file called "openldap-2.0.11.md5" on the OpenLDAP FTP site: 204.152.186.57

- Compiling:

Linux:

```
CC="egcs" \  
CFLAGS="-O9 -funroll-loops -ffast-math -malign-double -mcpu=pentiumpro -  
march=pentiumpro -fomitframe-  
pointer -fno-exceptions" \  
./configure \  
--disable-debug \  
--disable-ipv6 \  
--enable-crypt \  
--without-tls \  
--with-threads \  
--enable-shared \  
--with-gnu-ld
```

This tells OpenLDAP to set itself up for this particular hardware setup with:

- Build shared libraries.
- Assume the C compiler uses GNU ld.

Solaris:

```
./configure \  
--disable-debug \  
--disable-ipv6 \  
--enable-crypt \  
--without-tls \  
--with-threads
```

This tells OpenLDAP to set itself up for this particular configuration setup with:

- Disable debugging support to improve performance.
- Disable IPv6 support.
- Enable crypt passwords support.
- Disable and include TLS/SSL encryption support into the program.
 - Enable threads support for OpenLDAP on the system.

And then:

```
[root@dep openldap-2.0.25]# make depend  
[root@dep openldap-2.0.25]# make  
[root@dep openldap-2.0.25]# cd tests/  
[root@dep tests]# make test  
[root@dep tests]# cd  
[root@dep /root]# find /* > OpenLDAP1  
[root@dep /root]# cd /var/tmp/openldap-2.0.25/  
[root@dep openldap-2.0.25]# make install  
[root@dep openldap-2.0.25]# install -d -m 700 /var/lib/ldap  
[root@dep openldap-2.0.25]# rm -rf /var/run/openldap-ldbm  
[root@dep openldap-2.0.25]# rm -f /etc/openldap/*.default  
[root@dep openldap-2.0.25]# rm -f /etc/openldap/schema/*.default  
[root@dep openldap-2.0.25]# strip /usr/lib/liblber.a (Linux)  
[root@dep openldap-2.0.25]# strip /usr/lib/liblber.so.2.0.5 (Linux)  
[root@dep openldap-2.0.25]# strip /usr/lib/libldap.a (Linux)  
[root@dep openldap-2.0.25]# strip /usr/lib/libldap.so.2.0.5 (Linux)  
[root@dep openldap-2.0.25]# strip /usr/lib/libldap_r.a (Linux)  
[root@dep openldap-2.0.25]# strip /usr/lib/libldap_r.so.2.0.5 (Linux)  
[root@dep openldap-2.0.25]# /sbin/ldconfig (Linux)  
[root@dep openldap-2.0.25]# cd  
[root@dep /root]# find /* > OpenLDAP2  
[root@dep /root]# diff OpenLDAP1 OpenLDAP2 > OpenLDAP-Installed
```

The strip command will discard all symbols from the object files. This means that our library files will be smaller in size and will improve the performance hit to the program since there will be fewer lines to be read by the system when it uses the libraries.

5.- Configuring OpenLDAP

- First design one tree
- Create administrative users
- Create ACL's for this users. Something like:

```
defaultaccess read
access to attr=userpassword
by self write
by dn="cn=admin,ou=users, ou=administrative,o=business" write
by * compare
```

- Configure slapd.conf
- Immunize important configuration files
[root@dep /]# chown root:root /etc/openldap/slapd.conf
[root@dep /]# chmod 600 /etc/openldap/slapd.conf
[root@dep /]# chattr +i /etc/openldap/slapd.conf
- Make an initialization file and install it on /etc/rc.d

6.- Tune OpenLDAP

- **Use index attributes you frequently search for.** But each index requires time to maintain and uses additional memory.
- On a heavily loaded LDAP server, you'll want to add the following to your slapd.conf config file:

```
loglevel 0
```

This will prevent slapd from using up extra CPU via syslogd. Because syslog uses both a userland process (syslogd) and system calls syslog, the performance gained by disabling syslog completely is very noticeable but you lose control above application

- You can improve logging performance on some systems by configuring syslog not to sync the file system with every write-- see your man pages for syslogd/syslog.conf. In Linux, you can prepend the log file name with a "-" in syslog.conf. For example, if you are using the default LOCAL4 logging you could try:

```
# LDAP logs
LOCAL4.*                -/var/log/ldap
```

- You may want to tune the cache using `cachesize` and `dbcachesize` `slapd.conf` configuration directives.

```
cachesize 1000000
dbcachesize 100000000
```

will allow the entry cache to hold 1,000,000 entries and allow 100MB for each open index file

- `slapd`, by default, synchronizes the underlying DB after each modification. This is safe, but slow. In situations where you do not need this protection (such as on a slave server), you can disable write sync by specifying the database configuration directive

```
dbcacheNoWsync
```

- On Solaris systems, it is critical important to enable "priority paging". See Sun's paper on (http://www.sun.com/sun-on-net/performance/priority_paging.html)

Note that the priority paging algorithm should only be enabled for pre-Solaris 8 systems. "Solaris 8 separates file system data from other data so that the file cache will no longer compete with programs for physical memory." This algorithm is known as the cyclical page cache. Therefore it is unnecessary to turn priority paging on.

7.- Choose your backup strategy

Make a script that:

- o Stops OpenLDAP server
- o Copy the database directory
- o Starts OpenLDAP
- o Checks the integrity of the operation

8.- Choose your monitoring strategy

All you need is check:

- o Daemon `slapd` (and `slurpd` on master) is running
- o Queries are inside the respond level
- o Queries are correct

-

