OpenLDAP 2.2.5

Nacho Díaz Asenjo
nacho@di.uc3m.es
Universidad Carlos III de Madrid

27 de febrero de 2004

1. Instalación de OpenLDAP 2.2.5 en Linux

En este documento intentaré explicar los pasos (de forma muy esquemática y breve) que hay que dar a la hora de instalar cualquier versión Openldap 2.1.x. No es mi intención escribir algo bien redactado, únicamente son unos ligeros apuntes que tomé mientras trabajaba en la instalación.

¿Qué vamos a utilizar para poner en marcha esta nueva versión de OpenLDAP?. Lo normal es utilizar la última versión a día de hoy.

- Berkeley DB 4.2.52
- Cyrus-SASL 2.1.17
- OpenSSL 0.9.6 (asumimos que está instalada por defecto en el sistema). En *apt-get install libssl0.9.6* instalará el paquete libssl0.9.6c-2woody.4.
- OpenLDAP 2.2.5

1.1. Compilando Berkeley DB

Obtenemos el paquete correspondiente a la versión 4.2.52 de la siguiente dirección *http://www.sleepycat.com/update/snapshot/db-4.2.52.tar.gz*. Además nos tenemos que descargar un nuevo parche aparecido recientemente
http://www.sleepycat.com/update/4.2.52/patch.4.2.52.html
y que será util siempre y cuando la versión que estés intentando instalar de OpenLDAP sea la 2.2.x

```
# tar xvzf db-4.2.52.tar.gz
# cd db-4.2.52
# patch -p0 < ../patch.4.2.52.1
# patch -p0 < ../patch.4.2.52.2
# cd build_unix
# ../dist/configure --prefix=/usr/local/BerkeleyDB-4.2.52/
# make
# make install
```

1.2. Compilando cyrus-sasl

El paquete de Cyrus lo obtuve de *ftp://ftp.andrew.cmu.edu/pub/cyrus-mail/cyrus-sasl-2.1.17.tar.gz*. Para compilar este paquete y asegurarte de que lo enlazas realmente con las nuevas BerkeleyDB 4.2, introduce en el fichero */etc/ld.so.conf* la línea correspondiente al path donde residen las librerías DB que acabas de compilar */usr/local/BerkeleyDB-4.2.52/lib*.

```
# cd cyrus-sasl-2.1.17
# ./configure --enable-krb4=no --with-bdb-libdir=/usr/local/BerkeleyDB-4.2.52/lib/ \
    --with-bdb-incdir=/usr/local/BerkeleyDB-4.2.52/include  \
    --prefix=/usr/local/Cyrus-SASL-2.1.17
# make
# make install
```

Tras la instalación es conveniente realizar un enlace simbólico de /usr/lib/sasl2 a este nuevo directorio

```
# ln -s /usr/local/Cyrus-SASL-2.1.17 /usr/lib/sasl2
```

Tampoco estaría mal poner los path de estas librerías dentro del fichero */etc/ld.so.conf*. Para lo que añadiremos estas 2 líneas:

```
/usr/local/BerkeleyDB-4.2.52/lib
/usr/local/Cyrus-SASL-2.1.17/lib
```

Y posteriormente ejecutaremos

```
#ldconfig -a
```

1.3. Compilando OpenLDAP 2.2.5

Respecto a OpenSSL, en mi caso no ha sido necesario compilarlo porque ya tenía instalado la versión 0.9.6c (en Woody *apt-get install libssl0.9.6 libssl-dev*).

Lo siguiente que debemos conseguir es la distribución de LDAP que deseamos instalar. En la siguiente URL *ftp://ftp.openldap.org/pub/OpenLDAP/openldap-release.tgz* se encuentra la última release de OpenLDAP (en la actualidad la versión 2.2.5).

```
# tar xvzf openldap-release.tgz
# cd openldap-2.2.5
```

A continuación tendrás que teclear la línea más importante.

```
# CPPFLAGS="-I/usr/local/BerkeleyDB-4.2.52/include \
            -I/usr/local/Cyrus-SASL-2.1.17/include/sasl/" \
  LDFLAGS="-L/usr/local/BerkeleyDB-4.2.52/lib \
           -L/usr/local/Cyrus-SASL-2.1.17/lib/sasl2 \
           -L/usr/local/Cyrus-SASL-2.1.17/lib" \
  ./configure --enable-threads --enable-tls --prefix=/usr/local/openldap-2.2.5 \
  --enable-ldbm --enable-bdb --enable-monitor --enable-crypt
```

Tal vez estés interesado en incluir más cosas como por ejemplo: *–enable-referrals o –enable-wrappers*. Ojo con el –enable-crypt ya que si no lo habilitas tu servidor será incapaz de hacer BIND con usuarios que tengan en el userPassword claves de este tipo. El –enable-ldbm se debe a que es el único backend que entiende *alias*.

Revisa la salida del configure para comprobar que no ha habido ningun error y que por lo menos encuentras estas líneas.

```
checking for Berkeley DB link (-ldb-4.2)... yes
checking for sasl_client_init in -lsasl2... yes
```

Finalmente ejecuta:

```
# make depend
# make
# make test <-- Si quieres hacer pruebas
# make install
```

Podemos verificar cuales son las librerías dinámicas de nuestro servidor LDAP.

```
# ldd /usr/local/openldap-2.2.5/libexec/slapd
  libsasl2.so.2 => /usr/local/Cyrus-SASL-2.1.17/lib/libsasl2.so.2 (0x40014000)
  libssl.so.0.9.6 => /usr/lib/libssl.so.0.9.6 (0x4002b000)
  libcrypto.so.0.9.6 => /usr/lib/libcrypto.so.0.9.6 (0x40059000)
  libresolv.so.2 => /lib/libresolv.so.2 (0x40119000)
  libdl.so.2 => /lib/libdl.so.2 (0x40129000)
  libpthread.so.0 => /lib/libpthread.so.0 (0x4012c000)
  libc.so.6 => /lib/libc.so.6 (0x40140000)
  /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000
```

1.3.1. Problemas

La ejecución del make me dio algunos problemillas debido a pequeñas cosas (librerías) de las que mi máquina carecía.

1. cannot find -lpam
   Solución: *apt-get install libpam0g-dev*

2. /usr/lib/libsasl.a db_berkeley: undefined reference to 'db_open'
   Solución: *Necesitaba tener instalada la versión adecuada de SASL.*

3. No me arranca el demonio con un fichero de configuración de OpenLDAP 2.0.x
   Solución: *Hay algunas directivas que han cambiado de nombre o no están soportadas. Asegúrate que la ejecución de ./libexec/slapd -t te devuelve que la sintaxis de fichero es correcta.*

4. Problema con los esquemas personales que utilizaba en OpenLDAP 2.0.x
   Solución: *Es posible que a la hora de cargar datos el directorio se queje porque tu esquema no es correcto, aunque sea el mismo que llevabas usando todas la vida. Por ejemplo, los objectos que crees necesitan tener SUP en el que indiques cual es la clase superior. Con la sintaxis de los atributos también puedes tener problemillas.*

5. Error con comillas dobles en DN (“)
   Solución: *Cargando un LDIF he tenido problemas con algunos DN's que tenían comillas dobles, cuando en mi antiguo directorio OpenLDAP 2.0.x, sí que me lo aceptaba.*

6. DBD no soporta aliasedObjectName
   Solución: *Quería sólo probar si lo que había leído era cierto. Pues sí lo es. Si tu directorio tiene alias deberas utilizar bases de datos ldbm.*

7. No me arranca y acabo de poner las opciones de TLS en mi fichero de configuracion
   Solución: *Comentar la línea TLSClientVerify porque la opción false ya no funciona y provoca que el servidor no arranque.*

8. Tengo un error con un schema que antes me funcionaba con OpenLDAP 2.0.x
   Solución: *Para los attributetype he cambiado las sintaxis de cadena terminada en .40 por .15, ya que la .40 ya no aceptaba EQUALITY caseIgnoreMatch.* Además para nuevos objectclass definidos en el schema antes los soportaba sin SUP y ahora en uc3mGrupo se debe añadir SUP organizationalUnit y en uc3mPersona SUP inetOrgPerson.

9. Fallo al realizar el bind's como un usuario
   Solución: Posiblemente el –enable-crypt está a no es necesario compilarlo con esta opción si deseamos utilizar el esquema Crypt. La opción por defecto en password-hash ahora es {SHA}.

10. Directiva dbcachesize desconocida
    Solución: Eliminar este directiva del fichero de configuración.

11. Permitir conexiones Versión 2. Solución: Por defecto la versión 2.1 de OpenLDAP ya no soporta conexiones V.2, si quieres añadir esta funcionalidad añade la siguiente opcion **allow bind_v2** en tu fichero de configuración.

1.4. Fichero /etc/syslog.conf

Añade una nueva línea al final del fichero de configuración de logs

```
LOCAL6.*            -/usr/local/openldap-2.2.5/var/log/openldap.log
```

y manda una señal -HUP al proceso syslogd

```
# ps -e | grep syslogd
  250 ?        00:13:31 syslogd
#kill -HUP 250
```

A partir de ese momento nuestro LDAP arrancado con la opción -l LOCAL6, enviará los log's del directorio a ese fichero.

1.5. Fichero de configuracion slapd.conf

Antes de arrancar el servidor es necesario que dispongas de un fichero slapd.conf bien configurado. Este fichero lo puedes encontrar en */usr/local/openldap-2.2.4/etc/openldap/slapd.conf*

```
# Aspectos globales de servidor
include de los schemas soportados
características generales (p.ej TLS)

# Especificación de cada Backend
  DBD
  ACL
```

Una de los puntos a configurar es el TLS para tener acceso a un puerto seguro. En la zona de características

```
## Información sobre TLS
## Juego de metodos de cifrado aceptados...
TLSCipherSuite HIGH:MEDIUM

## Path al certificado del servidor
TLSCertificateFile /usr/local/openldap-2.2.4/cert/ldap.pem

## Path al fichero con la clave privada.
## El contenido no puede estar cifrado, ojo con los permisos
TLSCertificateKeyFile /usr/local/openldap-2.2.4/cert/ldap_key.pem

## Path al fichero de con el certificado de la CA
TLSCACertificateFile    /usr/local/openldap-2.2.4/cert/CACerts
```

Luego comprueba que el servidor es capaz de ponerse a escuchar (omite la parte ldaps si no estás utilizando SSL). `./slapd -f ../etc/openldap/slapd.conf -h "ldap://:19389/ lda`

1.6. Configurando Replicación Segura

1.6.1. En el Maestro

En el fichero *slapd.conf*

```
replica host=maquinaesclava.uc3m.es:389
        suffix="o=Universidad Carlos III,c=es"
        binddn=<dn del Administrador>
        credentials=<clave del Administrador>
        bindmethod=simple
        tls=yes
        starttls=yes

replogfile /usr/local/openldap-2.2.5/var/openldap-slurp/slurp.log
```

En el fichero *ldap.conf*

```
TLS_CACERT      /usr/local/openldap-2.2.5/cert/CACerts
TLS_CERT        /usr/local/openldap-2.2.5/cert/ldap.pem
TLS_KEY         /usr/local/openldap-2.2.5/cert/ldap_key.pem

ssl     start_tls
```

1.6.2. En el Esclavo

```
updatedn        <dn del administrador>
updateref       ldaps://maquinamaestra.uc3m.es:636
```

1.7. Fichero /etc/init.d/openldap-2.2.5

Este es el script que utilizo para arrancar y parar el servicio.

```
#!/bin/bash

HOME=/usr/local/openldap-2.2.5
DAEMON=$HOME/libexec/slapd
SLURPD=$HOME/libexec/slurpd
CONFIG=$HOME/etc/openldap/slapd.conf


case "$1" in
'start')
        if [ -f /usr/local/openldap-2.2.5/etc/openldap/slapd.conf -a -f
```

```
           /usr/local/openldap-2.2.5/libexec/slapd ]; then
                echo "Arrancando Servicio de Directorio OPENLDAP."
                ulimit -n 4096
                /usr/local/openldap-2.2.5/libexec/slapd
                   -f /usr/local/openldap-2.2.5/etc/openldap/slapd.conf
                   -h "ldap://:389/ ldaps://:636/" -l LOCAL6
                echo "Arrancando Servicio de Replica  [slurpd]"
                replicas=`grep ^replica $CONFIG`
                test -z "$replicas" ||
  (echo -n " slurpd" && start-stop-daemon --start
                   --quiet --name slurpd --exec $SLURPD)
                echo "."

        fi
        ;;
'stop')
        [ ! -f /usr/local/openldap-2.2.5/var/slapd.pid ] && exit 0
        slapdpid=`cat /usr/local/openldap-2.2.5/var/slapd.pid`
        if [ "$slapdpid" -gt 0 ]; then
                echo "Parando Servicio de Directorio OPENLDAP."
                kill -SIGTERM  $slapdpid 2>&1 |
                  /bin/grep -v "no existe ese proceso."
        fi
        replicas=`grep ^replica $CONFIG`
        test -z "$replicas" ||
  (echo -n " slurpd" && killall slurpd > /dev/null 2>&1)
        ;;
*)
        echo "Usage: /etc/init.d/openldap-2.2.5 { start | stop }"
        ;;
esac
exit 0
```

1.8. Carga Masiva de Datos

Para realizar una carga masiva a este nuevo directorio instalado a partir de un fichero LDIF, el comando a ejecutar será el siguiente:

```
# /usr/local/openldap-2.2.5/sbin/slapadd
     -f /usr/local/openldap-2.2.5/etc/openldap/slapd.conf
     -b "o=Universidad Carlos III,c=es"
     -l <DatosIniciales>.ldif
```