OpenLDAP 安装说明

目 录

一、 环境说明

1.1 网络及硬件环境

CPU: 4U 内存：8G 硬盘：60G

1.2 软件环境

Red Hat Linux 6.4 64 位

1.3 文档

二、 安装准备

2.1 在安装 OpenLDAP 前应确保下列的系统软件已经安装

软件名称	软件描述
gcc-4.4.7	编程语言编译器
Berkeley DB-6.0.30	Berkeley 数据库
Cyrus SASL-2.1.26	提供简单认证及安全层协议
OpenSSL-1.0.1h	提供加密相关的管理工具和库
libtool-2.4.2	提供脚本支持的通用库
autoconf-2.69	生成 shell 脚本的扩展包，用于自动配置源代码包
automake-1.11.1	自动创建 Makefiles 的 GNU 工具

2.2 创建 ldap 用户

1) 创建 ldap 组：

```
groupadd -g 83 ldap
```

2) 创建 ldap 用户：

```
useradd -c "OpenLDAP Daemon Owner" -u 83 -g ldap ldap
```

3) 修改 ldap 密码：

```
passwd ldap
```

2.3 准备安装目录

1) 创建 OpenLDAP 安装目录：

```
chmod -R 757 src
```

```
mkdir /usr/local/openldap2.4.39
```

```
chown ldap:ldap /usr/local/openldap2.4.39
```

2) 创建 OpenLDAP 数据存储目录：

```
mkdir /data/ldap
```

```
chown ldap:ldap /data/ldap
```

3) 创建 OpenLDAP 运行期工作目录：

```
mkdir /var/run/openldap
```

chown ldap:ldap /var/run/openldap

4) 通过 ldap 用户创建配置和数据及日志目录：

以 ldap 登录系统 或 su - ldap

cd /usr/local/openldap2.4.39

mkdir conf

cd /data/ldap

mkdir ldap1-m1-data

mkdir ldap1-m1-log

5) 增加 ldap 用户的环境变量

vi ~/.bash_profile

增加 export LDAP_HOME=/usr/local/openldap2.4.39

source ~/.bash_profile

6) 上传 OpenLDAP 的安装文件到/usr/local/src 目录，包括补丁，见下面列表：

openldap-2.4.39-blfs_paths-1.patch

openldap-2.4.39-symbol_versions-1.patch

openldap-2.4.39.tgz

三、 安装 OpenLDAP

下面的安装步骤需要使用 ldap 用户来执行。

1) 为了编译时能够找到需要的头文件和库，设置环境变量：

export CPPFLAGS="-I/usr/local/libtool/include -I/usr/local/sasl/include/sasl"

export LDFLAGS="-L/usr/local/libtool/lib -L/usr/local/sasl/lib"

2) 解压缩安装包：

cd /usr/local/src

tar -xzvf openldap-2.4.39.tgz

3) 安装 OpenlDAP 的补丁：

cd openldap-2.4.39

patch -Np1 -i ../openldap-2.4.39-blfs_paths-1.patch

patch -Np1 -i ../openldap-2.4.39-symbol_versions-1.patch

4) 自动配置源代码包

```
autoconf
```

5) 配置编译参数：

```
./configure --prefix=$LDAP_HOME                \
            --sysconfdir=$LDAP_HOME/conf \
            --disable-static          \
            --enable-debug            \
            --enable-dynamic          \
            --enable-crypt            \
            --enable-spasswd          \
            --enable-modules          \
            --enable-rlookups         \
            --enable-backends=mod \
            --enable-overlays=mod \
            --disable-ndb             \
            --disable-sql
```

备注：

--sysconfdir: 配置 OpenLDAP 的配置文件目录。

--disable-static: 禁止库的静态版本的安装。

--enable-debug: 打开 DEBUG 模式，便于在运行出错时分析错误原因。

--enable-dynamic: 强迫 OpenLDAP 库动态链接到可执行程序。

--enable-crypt: 打开密码的加密支持。

--enable-spasswd: 打开 SASL 密码验证。

--enable-modules: 打开动态模块支持。

--enable-rlookups: 打开对 client 主机名的反向搜索。

--enable-backends: 打开所有可支持的后端（backend）。

--enable-overlays: 打开所有可支持的 overlay。

--disable-ndb: 关闭 MySQL NDB Cluster 的后端支持，当使用 MySQL 会造成配置失败。

--disable-sql: 关闭 SQL server 后端支持。

6) 执行 make 安装：

```
make depend

make

make install
```

7) 设置 OpenLDAP 目录的访问权限：

```
chmod -v 700 /data/ldap
chmod -v 640 $LDAP_HOME/conf/openldap/{slapd.{conf,ldif},DB_CONFIG.example}
```

install -v -dm700 -o ldap -g ldap $LDAP_HOME/conf/openldap/slapd.d

8) 拷贝 OpenLDAP 的文档：

install -v -dm755 $LDAP_HOME/doc

cp -vfr doc/drafts $LDAP_HOME/doc &&

cp -vfr doc/rfc $LDAP_HOME/doc &&

cp -vfr doc/guide $LDAP_HOME/doc

四、 启动

4.1 安装启动脚本

使用 root 用户 copy 启动脚本 slapd 到/etc/rc.d/init.d/。

设置所有用户对脚本的执行权限：

chmod +x /etc/rc.d/init.d/slapd

下面的安装步骤需要使用 ldap 用户来执行。

4.2 设置 ldap 的执行环境变量

vi ~/.bash_profile

增加$LDAP_HOME/sbin 到 PATH，内容见下：

```
# OpenLDAP 的 HOME
export LDAP_HOME=/usr/local/openldap2.4.39
PATH=$PATH:$HOME/bin:$LDAP_HOME/sbin
export PATH
# OpenLDAP 执行的服务
export SLAPD_SERVICE=ldap:< hostname or ip >:12389
```

source ~/.bash_profile

注意：< hostname or ip >为实际安装 OpenLDAP 的主机名或 ip 地址。OpenLDAP 的默认端口是 389，因为 OpenLDAP 部署在内网，为了不占用系统的预留端口，使用端口号 12389。启动参数 –h ldap://< hostname or ip>:12389。

4.3 启动 OpenLDAP

/etc/rc.d/init.d/slapd start

通过/etc/rc.d/init.d/slapd status 查看是否启动成功：

```
[ldap@cas ~]$ /etc/rc.d/init.d/slapd status
slapd (pid 29185) 正在运行...
```

如上信息，说明已经正常启动。

```
[ldap@cas ~]$ /etc/rc.d/init.d/slapd status
slapd 已停
```

如上信息，说明 OpenLDAP 已经停止。

4.4 停止 OpenLDAP

/etc/rc.d/init.d/slapd stop

4.5 调试启动

如果启动失败，要跟踪详细的调试详细，以-d 参数启动：

slapd -h ldap:// < hostname or ip >:12389 –d 1

备注：

1) -d 1:表示调试状态，会输出更详细日志，实际启动时不要加该参数

2) 启动时如果报错：

unable to open pid file "/var/run/openldap/slapd.pid": 2(No such file or directory),则按照 2.3 中 3）的内容，创建对应的目录。

3) 启动时如果提示警告：

bdb_db_open：warning -no DB_CONFIG file found in directory /data/ldap/ldap1-m1-data: (2),则执行下面的命令创建这个配置文件：

cp $LDAP_HOME/etc/openldap/DB_CONFIG.example /data/ldap/ldap1-m1-data /DB_CONFIG/