

构建基于NFS文件系统的Openldap身份验证 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/467/2021_2022__E6_9E_84_E5_BB_BA_E5_9F_BA_E4_c67_467270.htm

一、说明LDAP（轻量级目录访问协议，Lightweight Directory Access Protocol）是实现提供被称为目录服务的信息服务。目录服务是一种特殊的数据库系统，其专门针对读取，浏览和搜索操作进行了特定的优化。二、下载软件

<ftp://ftp.openldap.org/pub/OpenLDAP/openldap-stable/openldap-stable-20070831.tgz> 三、解压安装 操作环境：RHEL AS4

```
#gunzip openldap-stable-20070831.tgz #tar xvf
```

```
openldap-stable-20070831.tar -C /tmp #cd /tmp #./configure
```

```
--prefix=/usr/local/openldap #make depend #make #make test
```

```
#make install 四、相关配置目录 LDAP后台程序slapd目录
```

：/usr/local/openldap/libexec 配置文件目录

：/usr/local/openldap/etc 运行数据库目录

：/usr/local/openldap/var/openldap-data OpenLDAP工具目录

：/usr/local/openldap/bin 五、修改配置文件 1) 更改配置文件

/usr/local/etc/openldap/slapd.conf 在include

/usr/local/etc/openldap/schema/core.schema这行后面加上下面的行，包括所有的方案。 include

```
/usr/local/etc/openldap/schema/corba.schema include
```

```
/usr/local/etc/openldap/schema/cosine.schema include
```

```
/usr/local/etc/openldap/schema/inetorgperson.schema include
```

```
/usr/local/etc/openldap/schema/java.schema include
```

```
/usr/local/etc/openldap/schema/krb5-kdc.schema include
```

```
/usr/local/etc/openldap/schema/misc.schema include
/usr/local/etc/openldap/schema/nadf.schema include
/usr/local/etc/openldap/schema/nis.schema include
/usr/local/etc/openldap/schema/openldap.schema
```

2) 在文件slapd.conf的"dbm database definitions"部分更改相应的suffix,rootdn行如下

```
database dbm suffix "dc=example,dc=com"
rootdn "cn=root,dc=example,dc=com" rootpw secret directory
/usr/local/openldap/var/openldap-data
```

rootdn的格式安装后默认为cn=Manager,这里改为root完全是自己的喜好,这样符合Unix/Linux中root具有最高权限的传统。

3) 现在可以启动slapd了,运行/usr/local/openldap/libexec/slapd 可以考虑把/usr/local/bin and /usr/local/libexec加到搜索路径中,即加到/etc/profile 中的PATH行:

```
PATH="$PATH:/usr/X11R6/bin:/usr/local/bin:/usr/local/openldap/libexec"
```

这样下次登录后只需键入slapd

4) 测试ldap server是否正常工作。运行下面的命令检查是否有相应的输出。

```
#ldapsearch -x -b "dc=example,dc=com" "(objectclass=*)"
```

5) 下载个migration脚本来创建.ldif文件, 链接地址:

```
http://www.padl.com/download/MigrationTools.tgz #gunzip MigrationTools.tgz.tar xvf MigrationTools.tar -C /usr/local/openldap #cd /usr/local/openldap/MigrationTools-47
```

先编辑migrate_common.ph 文件, 将其中两行改为下列形式

```
$DEFAULT_MAIL_DOMAIN = "example.com".
$DEFAULT_BASE = "dc=example,dc=com".
```

要注意修改的方法要和您/usr/local/openldap/etc/openldap/slapd.conf中的dc=example,dc=com 相对应 创建base.ldif文本文件 执行

```
#!/migrate_base.pl > /root/base.ldif #./migrate_group.pl /etc/group  
>> /root/base.ldif #./migrate_passwd.pl /etc/passwd >>
```

/root/base.ldif 用ldapadd添加记录进入LDAP数据库. 文件内容如下：
dn: dc=example,dc=com dc: example objectClass: top
objectClass: domain dn: ou=Hosts,dc=example,dc=com ou: Hosts
objectClass: top objectClass: organizationalUnit

...more..... 依次类推，添加每个人的记录进入该文件中 然后用下面的命令添加上面的.ldif文件进入LDAP数据库 #ldapadd -x -D

"cn=root,o=example,c=us" -w secret -f base.ldif 注：上面的文件的第一部分"dn: dc=example,dc=com"是必须的，否则不能添加数据。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com