链滴

centos7 安装 openldap

作者：cuijianzhe
原文链接：https://ld246.com/article/1620382031181
来源网站：链滴

一、 安装openldap

```
yum install -y openldap openldap-clients openldap-servers
cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
chown -R ldap. /var/lib/ldap/DB_CONFIG
```

当前版本：

```
[root@localhost ~]# slapd -V
@(#) $OpenLDAP: slapd 2.4.44 (Sep 30 2020 17:16:39) $
    mockbuild@x86-02.bsys.centos.org:/builddir/build/BUILD/openldap-2.4.44/openldap-2.4.4
/servers/slapd
```

修改配置

这里就是重点中的重点了，从openldap2.4.23版本开始，所有配置都保存在/etc/openldap/slapd.d录下的cn=config文件夹内，不再使用slapd.conf作为配置文件。配置文件的后缀为 ldif，且每个配文件都是通过命令自动生成的，任意打开一个配置文件，在开头都会有一行注释，说明此为自动生成文件，请勿编辑，使用ldapmodify命令进行修改

```
# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
```

安装openldap后，会有三个命令用于修改配置文件，分别为ldapadd, ldapmodify, ldapdelete，顾思义就是添加，修改和删除。而需要修改或增加配置时，则需要先写一个ldif后缀的配置文件，然后过命令将写的配置更新到slapd.d目录下的配置文件中去，完整的配置过程如下，跟着我做就可以了：

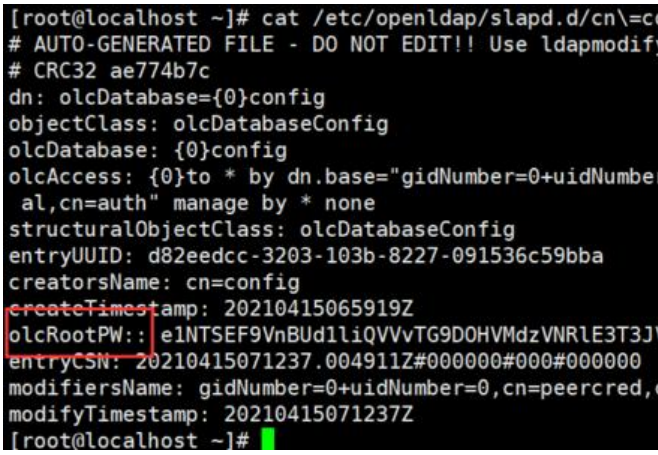
```
# 生成管理员密码,记录下这个密码，后面需要用到
[root@localhost slapd.d]# slappasswd -s 598941324
{SSHA}VpTwYbAUoLoC8uLw5MFQ7OrUc8KM/eda
# 新增修改密码文件,ldif为后缀，文件名随意，不要在/etc/openldap/slapd.d/目录下创建类似文件
# 生成的文件为需要通过命令去动态修改ldap现有配置，如下，我在家目录下，创建文件
```

```
[root@localhost ~]# cat modify.ldif
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}VpTwYbAUoLoC8uLw5MFQ7OrUc8KM/eda

# 这里解释一下这个文件的内容：
# 第一行执行配置文件，这里就表示指定为 cn=config/olcDatabase={0}config 文件。你到/etc/op
nldap/slapd.d/目录下就能找到此文件
# 第二行 changetype 指定类型为修改
# 第三行 add 表示添加 olcRootPW 配置项
# 第四行指定 olcRootPW 配置项的值
# 在执行下面的命令前，你可以先查看原本的olcDatabase={0}config文件，里面是没有olcRootPW
个项的，执行命令后，你再看就会新增了olcRootPW项，而且内容是我们文件中指定的值加密后的字
串

[root@localhost ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f modify.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={0}config,cn=config"
```

查看olcDatabase={0}config内容,新增了一个olcRootPW项。



然后继续配置：

```
# 我们需要向 LDAP 中导入一些基本的 Schema。这些 Schema 文件位于 /etc/openldap/schema/
目录中，schema控制着条目拥有哪些对象类和属性，可以自行选择需要的进行导入，
# 依次执行下面的命令，导入基础的一些配置,我这里将所有的都导入一下，其中core.ldif是默认已经
载了的，不用导入
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/collective.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/corba.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/duaconf.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/dyngroup.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/java.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/misc.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/openldap.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/pmi.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/ppolicy.ldif
```

修改域名，新增changedomain.ldif, 这里我自定义的域名为 wenyang.com，管理员用户账号为admin。
我们需要配置 LDAP 的顶级域（以 dc=wenyang,dc=com 为例）及其管理域：

```
[root@localhost ~]# cat changedomain.ldif
dn: olcDatabase={1}monitor,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to * by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read by dn.base="cn=admin,dc=wenyang,dc=com" read by * none

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=wenyang,dc=com

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=admin,dc=wenyang,dc=com

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootPW
olcRootPW: {SSHA}VpTwYbAUoLoC8uLw5MFQ7OrUc8KM/eda

dn: olcDatabase={2}hdb,cn=config
changetype: modify
add: olcAccess
olcAccess: {0}to attrs=userPassword,shadowLastChange by dn="cn=admin,dc=wenyang,dc=com" write by anonymous auth by self write by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by dn="cn=admin,dc=wenyang,dc=com" write by * read

#执行
[root@localhost ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f changedomain.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={1}monitor,cn=config"

modifying entry "olcDatabase={2}hdb,cn=config"

modifying entry "olcDatabase={2}hdb,cn=config"

modifying entry "olcDatabase={2}hdb,cn=config"

modifying entry "olcDatabase={2}hdb,cn=config"
```

错误集：

ldapmodify: wrong attributeType at line 5, entry "olcDatabase={1}monitor,cn=config"

需要在vim 文件视图下 ,把空格删除，用vim的大写O进行换行处理

● 在上述基础上，我们来创建一个叫做 wenyang.com 的组织，并在其下创建一个 Manager 的组角色（该角色内的用户具有管理整个 LDAP 的权限）和 People 和Group两个组织单元：

```
[root@localhost ~]# cat add-memberof.ldif
dn: cn=module{0},cn=config
cn: modulle{0}
objectClass: olcModuleList
objectclass: top
olcModuleload: memberof.la
olcModulePath: /usr/lib64/openldap

dn: olcOverlay={0}memberof,olcDatabase={2}hdb,cn=config
objectClass: olcConfig
objectClass: olcMemberOf
objectClass: olcOverlayConfig
objectClass: top
olcOverlay: memberof
olcMemberOfDangling: ignore
olcMemberOfRefInt: TRUE
olcMemberOfGroupOC: groupOfUniqueNames
olcMemberOfMemberAD: uniqueMember
olcMemberOfMemberOfAD: memberOf
[root@localhost ~]# cat refint1.ldif
dn: cn=module{0},cn=config
add: olcmoduleload
olcmoduleload: refint
[root@localhost ~]# cat refint2.ldif
dn: olcOverlay=refint,olcDatabase={2}hdb,cn=config
objectClass: olcConfig
objectClass: olcOverlayConfig
objectClass: olcRefintConfig
objectClass: top
olcOverlay: refint
olcRefintAttribute: memberof uniqueMember  manager owner
## 新建上述文件后执行如下命令
[root@localhost ~]# ldapadd -Q -Y EXTERNAL -H ldapi:/// -f add-memberof.ldif
adding new entry "cn=module{0},cn=config"

adding new entry "olcOverlay={0}memberof,olcDatabase={2}hdb,cn=config"

[root@localhost ~]# ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f refint1.ldif
modifying entry "cn=module{0},cn=config"

[root@localhost ~]#
[root@localhost ~]# ldapadd -Q -Y EXTERNAL -H ldapi:/// -f refint2.ldif
adding new entry "olcOverlay=refint,olcDatabase={2}hdb,cn=config"
```

到此，配置修改完了，在上述基础上，我们来创建一个叫做 wenyang.com 的组织，并在其下创建一 admin 的组织角色（该组织角色内的用户具有管理整个 LDAP 的权限）和 People 和 Group 两个组单元：

```
[root@localhost ~]# cat base
```

```
cat: base: No such file or directory
[root@localhost ~]# cat base.ldif
dn: dc=wenyang,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: wenyang Company
dc: wenyang

dn: cn=admin,dc=wenyang,dc=com
objectClass: organizationalRole
cn: admin

dn: ou=People,dc=wenyang,dc=com
objectClass: organizationalUnit
ou: People

dn: ou=Group,dc=wenyang,dc=com
objectClass: organizationalRole
cn: Group

[root@localhost ~]# ldapadd -x -D cn=admin,dc=wenyang,dc=com -W -f base.ldif
Enter LDAP Password:
adding new entry "dc=wenyang,dc=com"

adding new entry "cn=admin,dc=wenyang,dc=com"

adding new entry "ou=People,dc=wenyang,dc=com"

adding new entry "ou=Group,dc=wenyang,dc=com"
```

通过以上的所有步骤，我们就设置好了一个 LDAP 目录树：其中基准 dc=yuelvhui,dc=com 是该树根节点，其下有一个管理域 cn=admin,dc=wenyang,dc=com 和两个组织单元 ou=People,dc=wenang,dc=com 及 ou=Group,dc=wenyang,dc=com。

添加人员试试：

```
[root@localhost ~]# ldapadd -x -w 598941324 -D "cn=admin,dc=wenyang,dc=com" -f add.ldi

adding new entry "uid=cuijianzhe,ou=People,dc=wenyang,dc=com"
```

ok，大功告成