环境

OS:　　centos-7.5

Openldap version: openldap-2.4.44-21.el7-6.x86_64

OpenLDAP server 安装

用yum源安装：

yum -y install openldap compat-openldap openldap-clients openldap-servers openldap-servers-sql openldap-devel

```
启停命令：
systemctl start slapd
systemctl stop slapd
查看状态：
systemctl status slapd
开机启动：
systemctl enable slapd
```

配置server：

- DB、 monitor配置

```
slappasswd
New password:
Re-enter new password:
{SSHA}8nA/4N8p1ZMnJ3iHALZmM3kfPcP+tUWQ
db配置：
vim db.ldif
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=loreal,dc=com
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=ldpadm,dc=loreal,dc=com
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootPW
olcRootPW: {SSHA}8nA/4N8p1ZMnJ3iHALZmM3kfPcP+tUWQ
执行：
ldapmodify -Y EXTERNAL  -H ldapi:/// -f db.ldif
```

```
vim monitor.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=ldpadm,dc=loreal,dc=com" read by * none
执行：
ldapmodify -Y EXTERNAL  -H ldapi:/// -f monitor.ldif
```

- 设置LDAP数据库，BASE 信息

```
将示例数据库配置文件复制到/var/lib/ldap并更新文件权限。
cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
chown ldap:ldap /var/lib/ldap/*
添加cosine和nis LDAP模式。
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
base.ldif为您的域生成文件。
vim base.ldif
使用以下信息。您可以根据自己的要求进行修改。
dn: dc=loreal,dc=com
dc: loreal
objectClass: top
objectClass: domain
dn: cn=ldpadm ,dc=loreal,dc=com
objectClass: organizationalRole
cn: ldpadm
description: LDAP Manager
dn: ou=People,dc=loreal,dc=com
objectClass: organizationalUnit
ou: People
dn: ou=Group,dc=loreal,dc=com
objectClass: organizationalUnit
ou: Group
构建目录结构。
ldapadd -x -W -D "cn=ldpadm,dc=loreal,dc=com" -f base.ldif
```

- 启用LDAP日志记录

```
配置Rsyslog以将LDAP事件记录到日志文件/var/log/ldap.log。
vim /etc/rsyslog.conf
将以下行添加到/etc/rsyslog.conf文件中。
local4.* /var/log/ldap.log
重新启动rsyslog服务。
systemctl restart rsyslog
```

OpenLDAP 启动TLS

启动TLS需要配置CA证书，有三种类型的证书

自签名证书

CA证书 分内部CA 和公共CA (收费，不仅加密和给你证明身份)

测试可以用自签名，环境里已经有一套loreal的证书，采用那套来做TLS.

导入证书到配置文件

```
vim certs.ldif
# 按照此顺序（报错时切换顺序尝试）
dn: cn=config
changetype: modify
replace: olcTLSCertificateFile
olcTLSCertificateFile: /etc/openldap/certs/loreal.crt
dn: cn=config
changetype: modify
replace: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/openldap/certs/ca.pem
dn: cn=config
changetype: modify
replace: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/openldap/certs/loreal.key
```

导入配置

```
ldapmodify -Y EXTERNAL  -H ldapi:/// -f certs.ldif
```

验证服务

```
slapcat -b "cn=config" | egrep "olcTLS"
systemctl restart slapd
tailf /var/log/ldap.log
可以看到STARTTLS 日志内容。
执行ldapsearch -x -ZZ后，查看日志，内容有  TLS established tls_ssf=256 ssf=256, 服务端配置正常
#StartTLS 继续使用389端口
netstat -nlp -t |grep :389
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN
12483/slapd
tcp6       0      0 :::389                  :::*                    LISTEN
12483/slapd
```

- 配置slapd启用监听ldaps

```
vi  /etc/sysconfig/slapd
SLAPD_URLS="ldapi:///  ldap:///  ldaps:///"
重启openldap服务：
service slapd restart
这时开启了389 和 636 端口
```

OpenLDAP 启动主主同步

- 配置双主复制功能 在主1和主2上执行下面的步骤

```
ldap双主复制功能的实现依赖于syncprov模块，这个模块位于/usr/lib64/openldap目录下
vim mod_syncprov.ldif
# create new
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulePath: /usr/lib64/openldap
olcModuleLoad: syncprov.la
执行添加主主同步配置
```

```
ldapadd -Y EXTERNAL -H ldapi:/// -f mod_syncprov.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=module,cn=config"
```

```
vim syncprov.ldif
# create new
dn: olcOverlay=syncprov,olcDatabase={2}hdb,cn=config

objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpSessionLog: 100
```

执行 主主同步模式：

```
ldapadd -Y EXTERNAL -H ldapi:/// -f syncprov.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "olcOverlay=syncprov,olcDatabase={2}hdb,cn=config"
```

在主1和主2上执行下面的步骤，只需要替换olcServerID ， provider的值 和 rid的值

```
vim master01.ldif
# create new
dn: cn=config
changetype: modify
replace: olcServerID
# specify uniq ID number on each server
olcServerID: 2            #唯一值，主2上替换为1
dn: olcDatabase={2}hdb,cn=config
changetype: modify
add: olcSyncRepl
olcSyncRepl: rid=002        #001  此处与 olcServerID 对应； 1对应 001； 2 对应002
；  3 对应003；
  provider=ldap://10.162.66.135:389/   #此处为主2服务器地址，主2此处相应地上替换为主
1服务器地址192.168.255.124:389
  bindmethod=simple
  binddn="cn=ldpadm,dc=loreal,dc=com"
  credentials=Ab123456
  searchbase="dc=loreal,dc=com"
  scope=sub
  schemachecking=on
  type=refreshAndPersist
  retry="30 5 300 3"
  interval=00:00:05:00
-
add: olcMirrorMode
olcMirrorMode: TRUE
dn: olcOverlay=syncprov,olcDatabase={2}hdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
```

导入配置

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f master01.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"
modifying entry "olcDatabase={2}hdb,cn=config"
adding new entry "olcOverlay=syncprov,olcDatabase={2}hdb,cn=config"
```

至此双主配置完成。

验证

```
ldapsearch -x -b "dc=loreal,dc=com" -H ldap://10.162.66.135|grep uid=beihua_l
ldapsearch -x -b "dc=loreal,dc=com" -H ldap://10.162.66.145|grep uid=beihua_l
```

OpenLDAP client 安装

用yum源安装：

yum install -y openldap-clients nss-pam-ldapd

配置ldap client信息：主主模式

```
authconfig --enableldap --enableldapauth --enableldaptls --ldapserver=sta-
auth01.loreal.com,sta-auth02.loreal.com --ldapbasedn='dc=loreal,dc=com' --
enablemkhomedir --update
```

分发证书

```
scp /etc/openldap/cacerts/ca.pem
```

配置TLS

```
cat >> /etc/openldap/ldap.conf  << EOF
TLS_CACERTDIR /etc/openldap/cacerts
TLS_CACERT /etc/openldap/cacerts/ca.pem
TLS_REQCERT demand
EOF
cat >> /etc/nslcd.conf << EOF
# StartTLS
ssl start_tls
tls_cacertdir /etc/openldap/cacerts
tls_cacertfile /etc/openldap/cacerts/ca.pem
TLS_REQCERT demand
EOF
```

```
解释
TLS_REQCERT [never、allow、try、demand | hard]
设置是否在TLS会话中检查server证书。
Never：不检查任何证书。
Allow：检查server证书，没有证书或证书错误，都允许连接。
Try：检查server证书，没有证书（允许连接），证书错误（终止连接）。
demand | hard：检查server证书，没有证书或证书错误都将立即终止连接。（默认）
```

重启client服务

```
systemctl restart nslcd
systemctl enable nslcd
```

验证用户：

```
id  beihua_zhou
```

```
getent passwd beihua_zhou
ldapsearch -x -b "dc=loreal,dc=com" -H ldap://10.162.66.135|grep uid=beihua_1
ldapsearch -x -b "dc=loreal,dc=com" -H ldap://10.162.66.145|grep uid=beihua_1
```

添加用户

创建LDAP用户

```
vim beihua_zhou.ldif
dn: uid=beihua_zhou,ou=People,dc=loreal,dc=com
objectClass: account
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
cn: beihua_zhou
uid: beihua_zhou
uidNumber: 2000
gidNumber: 2000
homeDirectory: /home/beihua_zhou
loginShell: /bin/bash
userPassword: {SSHA}QM2y6m17g13FZLCvHwM9bruXj+k5UkRlbFQxL1JxcEU=
使用带有上述文件的ldapadd命令在OpenLDAP目录中创建名为“ beihua_zhou ” 的新用户。
ldapadd -x -W -D "cn=ldpadm,dc=loreal,dc=com" -f beihua_zhou.ldif
为用户分配密码。
ldappasswd -s 1@3456 -W -D "cn=ldpadm,dc=loreal,dc=com" -x
"uid=beihua_zhou,ou=People,dc=loreal,dc=com"
验证：
ldapsearch -x cn=beihua_zhou -b dc=loreal,dc=com
从LDAP中删除条目（可选）
ldapdelete -W -D "cn=ldpadm,dc=loreal,dc=com"
"uid=beihua_zhou,ou=People,dc=loreal,dc=com"
```

创建LDAP用户组

```
创建组：
vim g_beihua_zhou.ldif
dn: cn=g_beihua_zhou,ou=Group,dc=loreal,dc=com
cn: g_beihua_zhou
objectClass: posixGroup
objectClass: top
userPassword: {crypt}x
gidNumber: 2000
导入
ldapadd -x -W -D "cn=ldpadm,dc=loreal,dc=com" -f g_beihua_zhou.ldif
```

LDAPADMIN 添加用户，模板

LDAPAdmin管理工具

下载LDAPAdmin工具

添加新连接

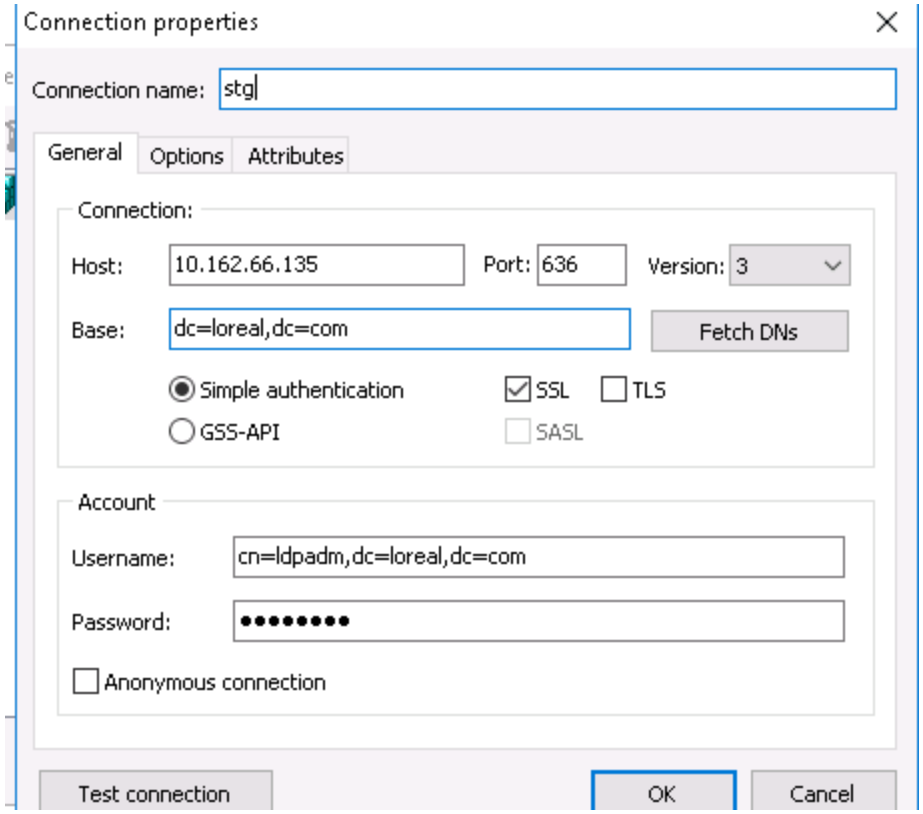
Stg：

```
connect name : stg_openldap_1
```

```
host :          10.162.66.135 或者 10.162.66.145

base:           dc=loreal,dc=com
选择sample authentication 和 SSL
用户名：cn=ldpadm,dc=loreal,dc=com
密码：Ab123456
```

测试连接，提示证书不能校验成功，不用管，点 Yes 完成。



导入系统用户和组

- 8.1安装migrationtools

  yum -y install migrationtools

- 8.2修改migrationtools的配置文件

，在/usr/share/migrationtools/这个目录下有很多migrationtools的文件

vim /usr/share/migrationtools/migrate_common.ph

修改以下的两个地方

```
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = "loreal.com";
# Default base
$DEFAULT_BASE = "dc=loreal,dc=com";
```

- 8.3生成基础的数据文件，可以自己修改这个生成的base.ldif文件，把不需要的去掉 （保留 People Group 就可以了。）

  /usr/share/migrationtools/migrate_base.pl > base.ldif

- 8.4 把base.ldif导入OpenLDAP

  ldapadd -x -D "cn=Captain,dc=lemon,dc=com" -W -f base.ldif

- 8.5 把系统的用户生成ldif文件

/usr/share/migrationtools/migrate_passwd.pl /etc/passwd passwd.ldif

/usr/share/migrationtools/migrate_group.pl /etc/group group.ldif

保留用户：hive livemap ldl-dwh ldl-workflow g2m-df omsview crmview presto kylin hypersuser livy

- 8.6 导入用户和组

把用户导入进去

ldapadd -x -D "cn=ldpadm,dc=loreal,dc=com" -W -f passwd.ldif

把组导进去：

ldapadd -x -D "cn=ldpadm,dc=loreal,dc=com" -W -f group.ldif

- 8.7检查用户

  ldapsearch -x -b "dc=loreal,dc=com" -H ldap://10.162.66.135 |grep uid=kylin

  或者到ldapadmin查看。