# 李先生

在平凡中坚持前行，总有一天会遇到不一样的自己。

先写总结，再写正文，嘿嘿嘿。这还是第一次认真的写个文档，写个总结，哈哈。大概在一个月前，第一次听说这个东西，完全没有概念，刚开始的时候看理论的知识，看了几次之后就没看了，看不懂啊。太抽象了，真的太抽象了。然后就把它晾在一边了，又过了一段时间，想了想，既然知道了这个东西，还是得好好学学，好好了解一下。整个过程是在虚拟机上测试完成，期间遇到了太多太多的坑，一个问题就是好几天。这些只是基础的一些东西，还得好好的看看官方文档，嘿嘿嘿。

最大的收获就是整个学习过程中的解决问题的办法和思想，理论的知识看不懂，没关系，一定要一定要动手去做，有时候看书，觉得挺有理，但是不去动手做，永远都学不会，当你动手做的过程中就慢慢的理解了这个东西是干嘛的；还有一点就是不要怕难，就算一个东西再难，只要肯花时间，肯动手做，一定学的会；还有思考的方式，当你在一个问题是纠结一天了，几天的时候，不要陷进去了，换个方向想想，另一种解决办法马上就出来了。

文档信息
目　　的：搭建一套完整的OpenLDAP系统，实现账号的统一管理。
1：OpenLDAP服务端的搭建
2：PhpLDAPAdmin的搭建
3：OpenLDAP的打开日志信息
4：OpenLDAP与migrationtools实现导入系统账号的相关信息
6：OpenLDAP与SSH
7：OpenLDAP限制用户登录系统
8：OpenLDAP强制用户一登录系统更改密码
9：OpenLDAP与系统账号结合Samba
10：OpenLDAP的主从
11：OpenLDAP的双主

作　　者：李　乐
日　　期：2017-01-09
联系方式：836217653@qq.com

**系统环境信息**
操作系统：CentOS release 6.7

**基础的环境准备**：
**关闭防火墙**：/etc/init.d/iptables stop  && chkconfig iptables off
**关闭NetworkManager**：/etc/init.d/NetworkManager stop && chkconfig NetworkManager off
**SeLinux设为disabled**：getenforce 是否为Disabled，若不是，则修改：
1：临时的生效  setenforce 0，再getenforce的时候为permissive
2：修改配置文件，然后重启  vim /etc/sysconfig/selinux 把SELINUX=disabled
**yum源仓库的配置**：
1）mkdir /yum

2）vim /etc/yum.repos.d/ll.repo

```
[local]
name = local
baseurl = file:///yum
gpgcheck = 0
enabled = 1
```

3）挂载 mount /mnt/hgfs/软件/CentOS-6.7-x86_64-bin-DVD1to2/CentOS-6.7-x86_64-bin-DVD1.iso /yum -o loop

4）yum clean all 清除缓存

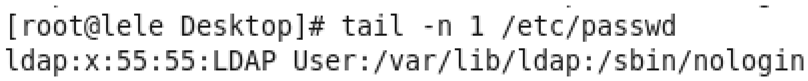
5）yum makecache 创建缓存

## 一：OpenLDAP服务器的搭建

1）安装OpenLDAP的相关

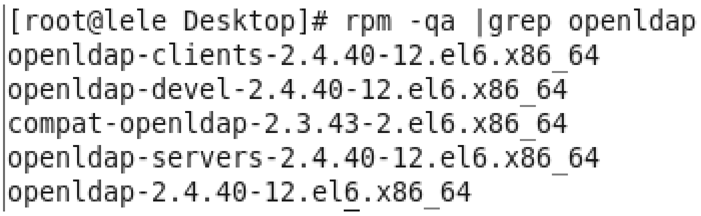
yum -y install openldap openldap-servers openldap-clients openldap-devel compat-openldap　其中compat-openldap这个包与主从有很大的关系

安装完后，可以看到自动创建了ldap用户：



```
[root@lele Desktop]# tail -n 1 /etc/passwd
ldap:x:55:55:LDAP User:/var/lib/ldap:/sbin/nologin
```

可以通过rpm -qa |grep openldap查看安装了哪些包：



```
[root@lele Desktop]# rpm -qa |grep openldap
openldap-clients-2.4.40-12.el6.x86_64
openldap-devel-2.4.40-12.el6.x86_64
compat-openldap-2.3.43-2.el6.x86_64
openldap-servers-2.4.40-12.el6.x86_64
openldap-2.4.40-12.el6.x86_64
```

2）OpenLDAP的相关配置文件信息

/etc/openldap/slapd.conf：OpenLDAP的主配置文件，记录根域信息，管理员名称，密码，日志，权限等

/etc/openldap/slapd.d/*：这下面是/etc/openldap/slapd.conf配置信息生成的文件，每修改一次配置信息，这里的东西就要重新生成

/etc/openldap/schema/*：OpenLDAP的schema存放的地方

/var/lib/ldap/*：OpenLDAP的数据文件

/usr/share/openldap-servers/slapd.conf.obsolete 模板配置文件

/usr/share/openldap-servers/DB_CONFIG.example 模板数据库配置文件

OpenLDAP监听的端口：

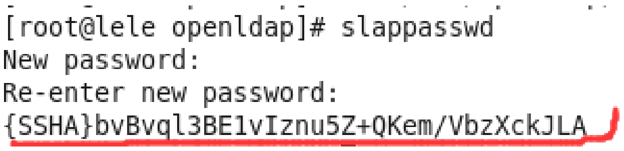
默认监听端口：389（明文数据传输）

加密监听端口：636（密文数据传输）

cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG cp /usr/share/openldap-servers/slapd.conf.obsolete /etc/openldap/slapd.conf

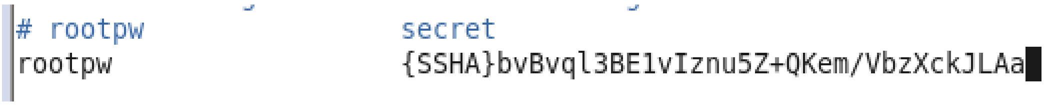
4）修改配置文件

首先，slappasswd生成密文密码123456，拷贝这个到/etc/openldap/slapd.conf里



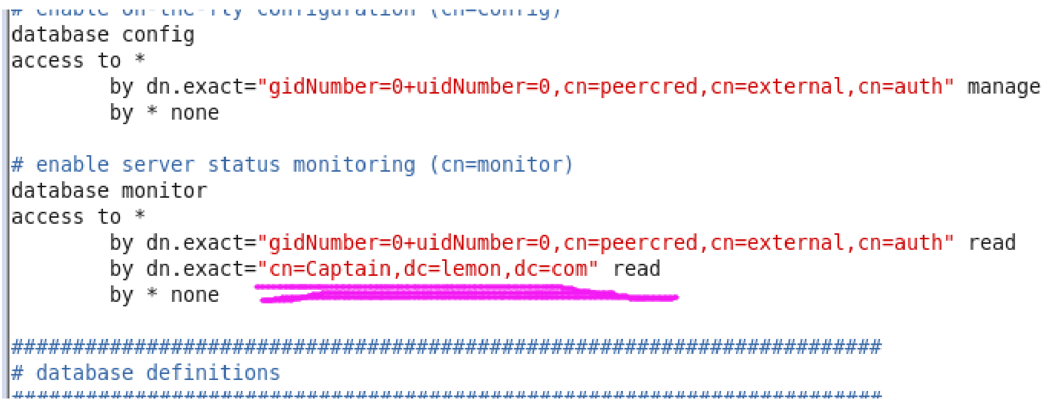
```
[root@lele openldap]# slappasswd
New password:
Re-enter new password:
{SSHA}bvBvql3BE1vIznu5Z+QKem/VbzXckJLA
```

这里的rootpw必须顶格写，而且与后面的密码文件用**Tab键**隔开

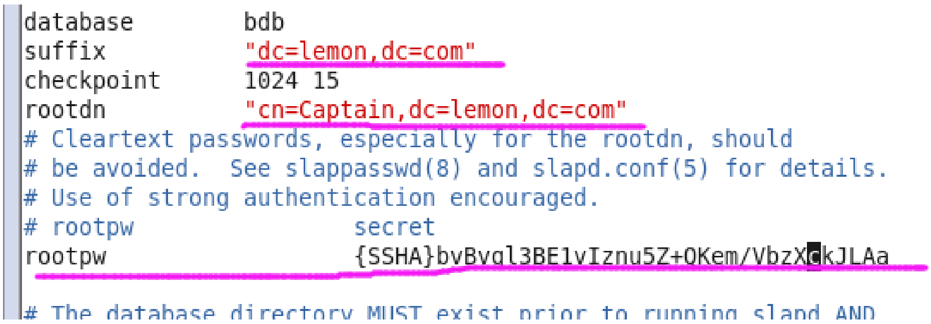


```
# rootpw                secret
rootpw                  {SSHA}bvBvql3BE1vIznu5Z+QKem/VbzXckJLAa
```

修改对应的



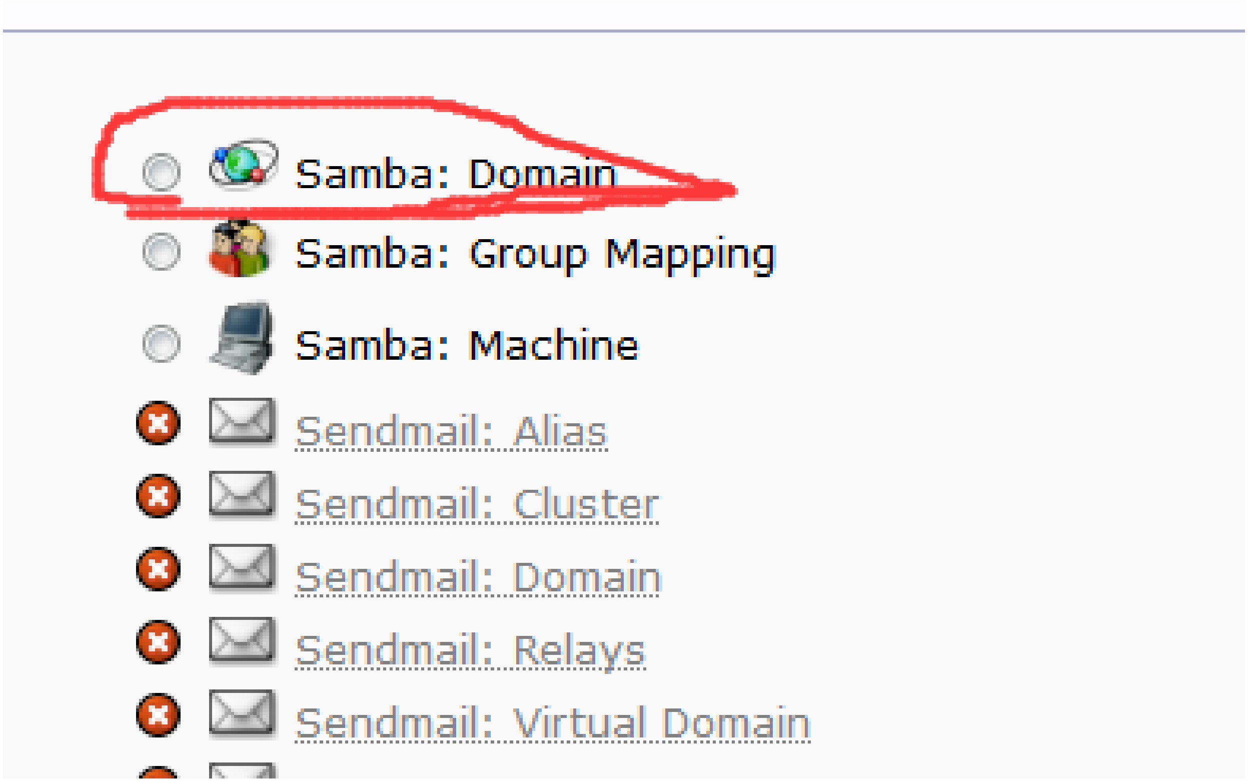
```
# enable on-the-fly configuration (cn=config)
database config
access to *
        by dn.exact="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage
        by * none

# enable server status monitoring (cn=monitor)
database monitor
access to *
        by dn.exact="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read
        by dn.exact="cn=Captain,dc=lemon,dc=com" read
        by * none

#######################################################################
# database definitions
#######################################################################
```



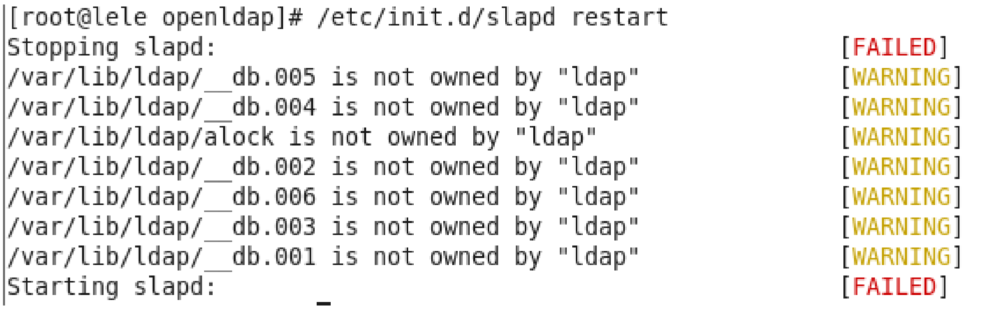
```
database        bdb
suffix          "dc=lemon,dc=com"
checkpoint      1024 15
rootdn          "cn=Captain,dc=lemon,dc=com"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
# rootpw                secret
rootpw                  {SSHA}bvBvql3BE1vIznu5Z+QKem/VbzXckJLAa

# The database directory MUST exist prior to running slapd AND
```

5）重新生成配置文件信息文件

先检测/etc/openldap/slapd.conf是否有错误：slaptest -f /etc/openldap/slapd.conf

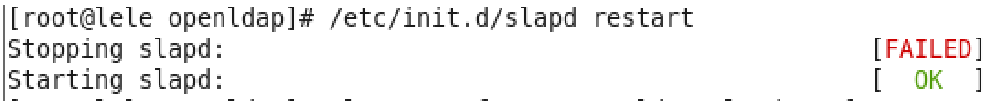


这里报错是因为在第三步后没有重新生成配置文件，启动slapd。而是直接修改配置文件去了。先启动slapd：/etc/init.d/slapd restart



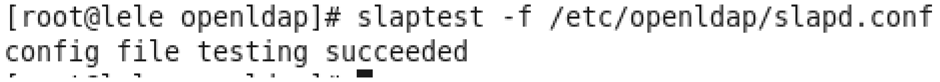
```
[root@lele openldap]# /etc/init.d/slapd restart
Stopping slapd:                                          [FAILED]
/var/lib/ldap/__db.005 is not owned by "ldap"            [WARNING]
/var/lib/ldap/__db.004 is not owned by "ldap"            [WARNING]
/var/lib/ldap/alock is not owned by "ldap"               [WARNING]
/var/lib/ldap/__db.002 is not owned by "ldap"            [WARNING]
/var/lib/ldap/__db.006 is not owned by "ldap"            [WARNING]
/var/lib/ldap/__db.003 is not owned by "ldap"            [WARNING]
/var/lib/ldap/__db.001 is not owned by "ldap"            [WARNING]
Starting slapd:                                          [FAILED]
```

这里又报错，这是因为没有给/var/lib/ldap授权，授权后chown -R ldap.ldap /var/lib/ldap/，再重启slapd，/etc/init.d/slapd restart，可以看到成功的



```
[root@lele openldap]# /etc/init.d/slapd restart
Stopping slapd:                                            [FAILED]
Starting slapd:                                            [  OK  ]
```

接着回到检测/etc/openldap/slapd.conf是否有错误：slaptest -f /etc/openldap/slapd.conf

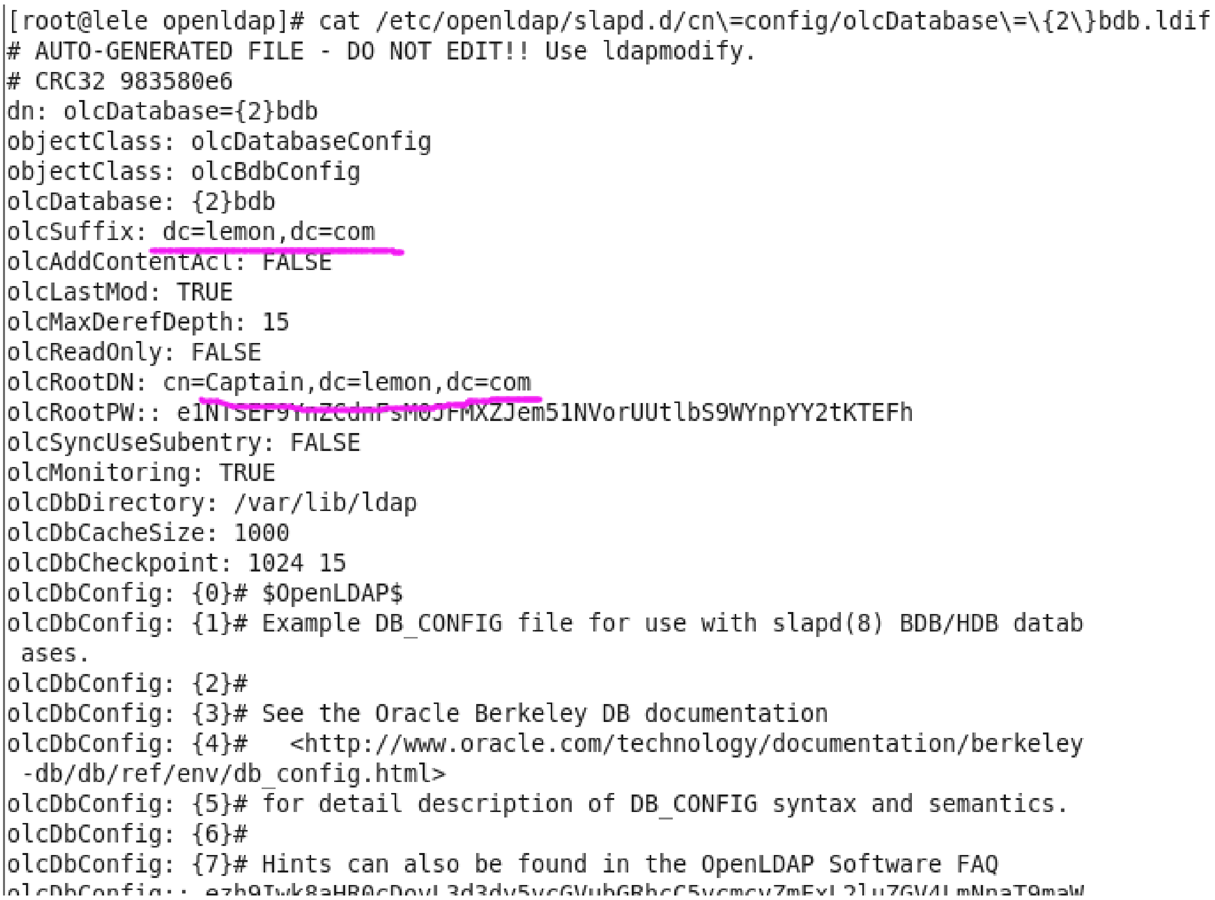


```
[root@lele openldap]# slaptest -f /etc/openldap/slapd.conf
config file testing succeeded
```

先删除最先的配置文件生成的信息：rm -rf /etc/openldap/slapd.d/*

重新生成：slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d/

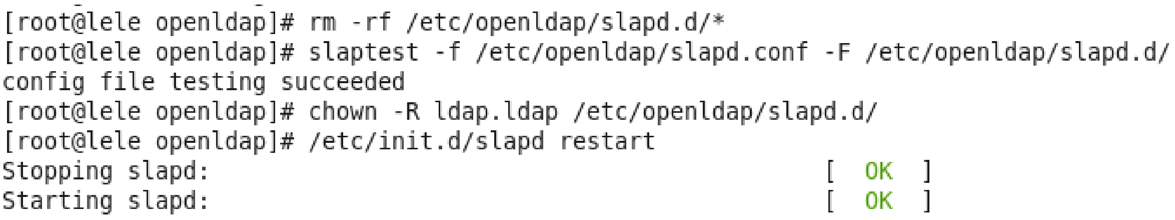
查看是否生成的是自己修改的配置文件信息：cat /etc/openldap/slapd.d/cn\=config/olcDatabase\=\{2\}bdb.ldif



```
[root@lele openldap]# cat /etc/openldap/slapd.d/cn\=config/olcDatabase\=\{2\}bdb.ldif
# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
# CRC32 983580e6
dn: olcDatabase={2}bdb
objectClass: olcDatabaseConfig
objectClass: olcBdbConfig
olcDatabase: {2}bdb
olcSuffix: dc=lemon,dc=com
olcAddContentAcl: FALSE
olcLastMod: TRUE
olcMaxDerefDepth: 15
olcReadOnly: FALSE
olcRootDN: cn=Captain,dc=lemon,dc=com
olcRootPW:: e1NTSEF9YnZCdnFsM0JFMXZJem51NVorUUtlbS9WYnpYY2tKTEFh
olcSyncUseSubentry: FALSE
olcMonitoring: TRUE
olcDbDirectory: /var/lib/ldap
olcDbCacheSize: 1000
olcDbCheckpoint: 1024 15
olcDbConfig: {0}# $OpenLDAP$
olcDbConfig: {1}# Example DB_CONFIG file for use with slapd(8) BDB/HDB datab
 ases.
olcDbConfig: {2}#
olcDbConfig: {3}# See the Oracle Berkeley DB documentation
olcDbConfig: {4}#   <http://www.oracle.com/technology/documentation/berkeley
 -db/db/ref/env/db_config.html>
olcDbConfig: {5}# for detail description of DB_CONFIG syntax and semantics.
olcDbConfig: {6}#
olcDbConfig: {7}# Hints can also be found in the OpenLDAP Software FAQ
olcDbConfig:: ezh9Iwk8aHR0cDovL3d3dy5vcGVubGRhcC5vcmcvZmFxL2luZGV4LmNnaT9maW
```

授权：chown -R ldap.ldap /etc/openldap/slapd.d/

重启：/etc/init.d/slapd restart



```
[root@lele openldap]# rm -rf /etc/openldap/slapd.d/*
[root@lele openldap]# slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d/
config file testing succeeded
[root@lele openldap]# chown -R ldap.ldap /etc/openldap/slapd.d/
[root@lele openldap]# /etc/init.d/slapd restart
Stopping slapd:                                            [  OK  ]
Starting slapd:                                            [  OK  ]
```

到这里为止，OpenLDAP服务端基本上完成了，我们可以通过PhpLDAPAdmin来登录看一下，那先得安装PhpLDAPAdmin

## 二：PhpLDAPAdmin的搭建

1）安装EPEL仓库，镜像里没有PhpLDAPAdmin这个的安装包，所以得安装EPEL仓库

rpm -ivh http://mirrors.ukfast.co.uk/sites/dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm

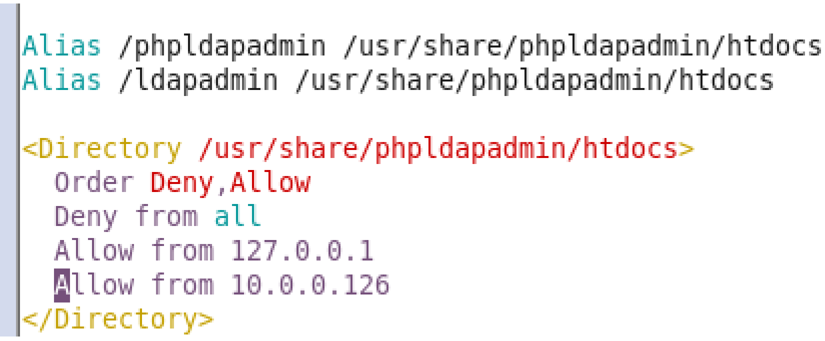
yum clean all

yum makecache

2）安装PhpLDAPAdmin

yum install -y phpldapadmin

3）修改phpldapadmin的配置文件，访问控制权限vim /etc/httpd/conf.d/phpldapadmin.conf，允许谁访问

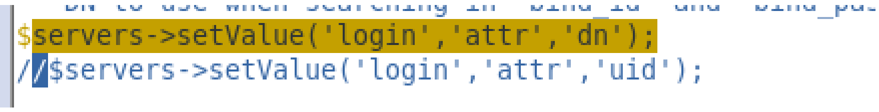


```
Alias /phpldapadmin /usr/share/phpldapadmin/htdocs
Alias /ldapadmin /usr/share/phpldapadmin/htdocs

<Directory /usr/share/phpldapadmin/htdocs>
  Order Deny,Allow
  Deny from all
  Allow from 127.0.0.1
  Allow from 10.0.0.126
</Directory>
```

4）修改配置文件：vim /etc/phpldapadmin/config.php

$servers->setValue('login','attr','dn');　这一行的注释去掉

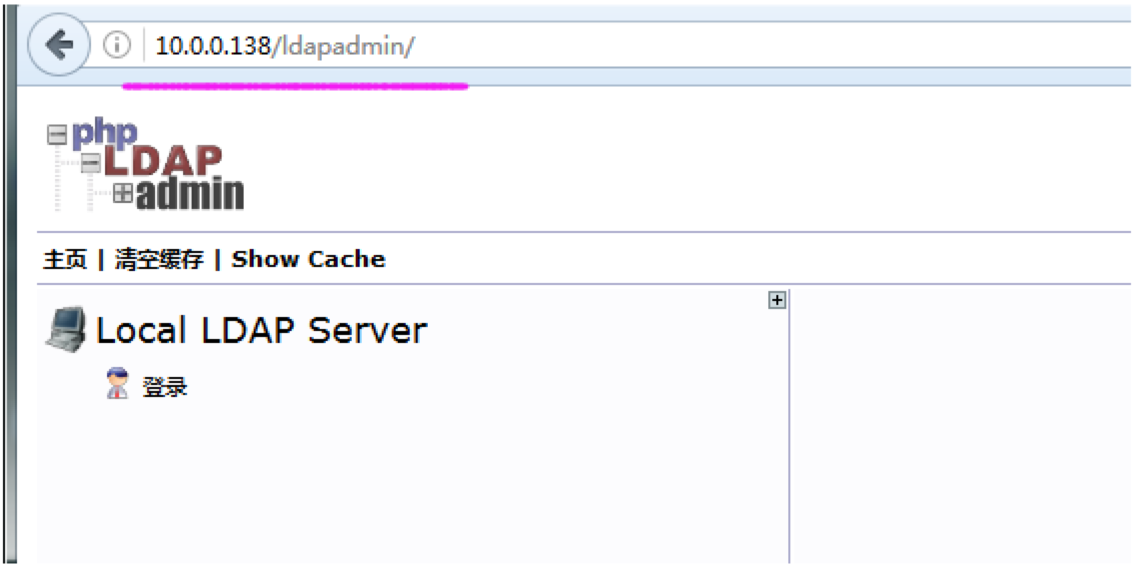
//$servers->setValue('login','attr','uid');　这一行注释掉



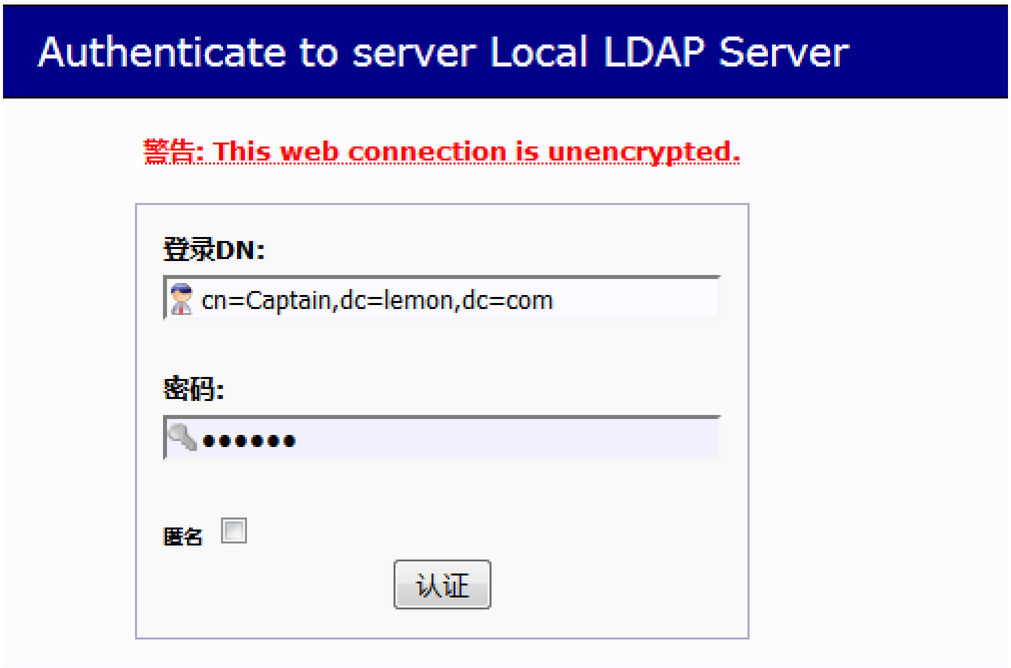
```
   DN to use when searching in  bind_id  and  bind_pa
$servers->setValue('login','attr','dn');
//$servers->setValue('login','attr','uid');
```

5）重启httpd服务/etc/init.d/httpd restart

6）在浏览器输入OpenLDAP服务端的IP　　10.0.0.138/ldapadmin



7）登录，输入管理员的DN，也就是配置文件里配置的



Authenticate to server Local LDAP Server

警告: This web connection is unencrypted.

登录DN:

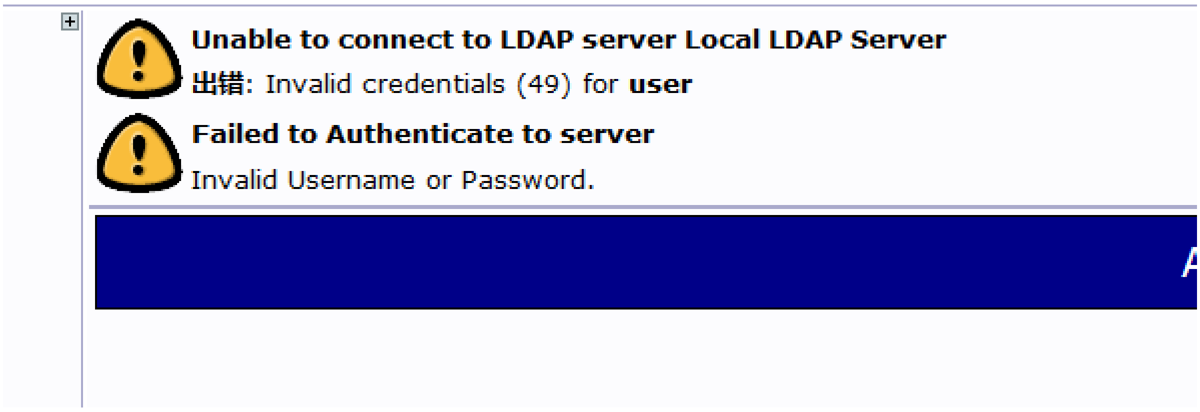
cn=Captain,dc=lemon,dc=com

密码:

●●●●●●

匿名 □

8）认证，报错



Unable to connect to LDAP server Local LDAP Server

出错: Invalid credentials (49) for **user**

Failed to Authenticate to server

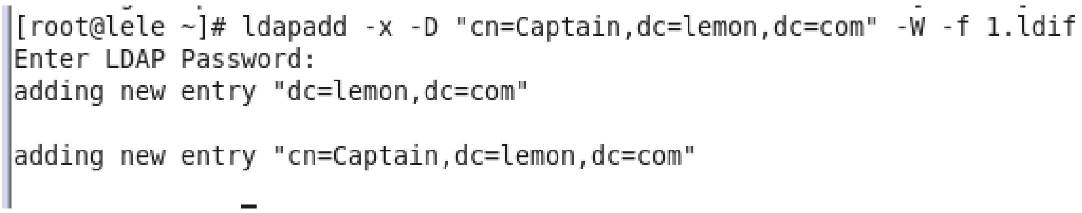
Invalid Username or Password.

这是因为在第一步搭建OpenLDAP服务端的时候，并没有把管理员的账号信息导入，编辑root.ldif，然后导入

```
dn: dc=lemon,dc=com
objectclass: dcObject
objectclass: organization
o: Yunzhi,Inc.
dc: lemon

dn: cn=Captain,dc=lemon,dc=com
objectclass: organizationalRole
cn: Captain
```

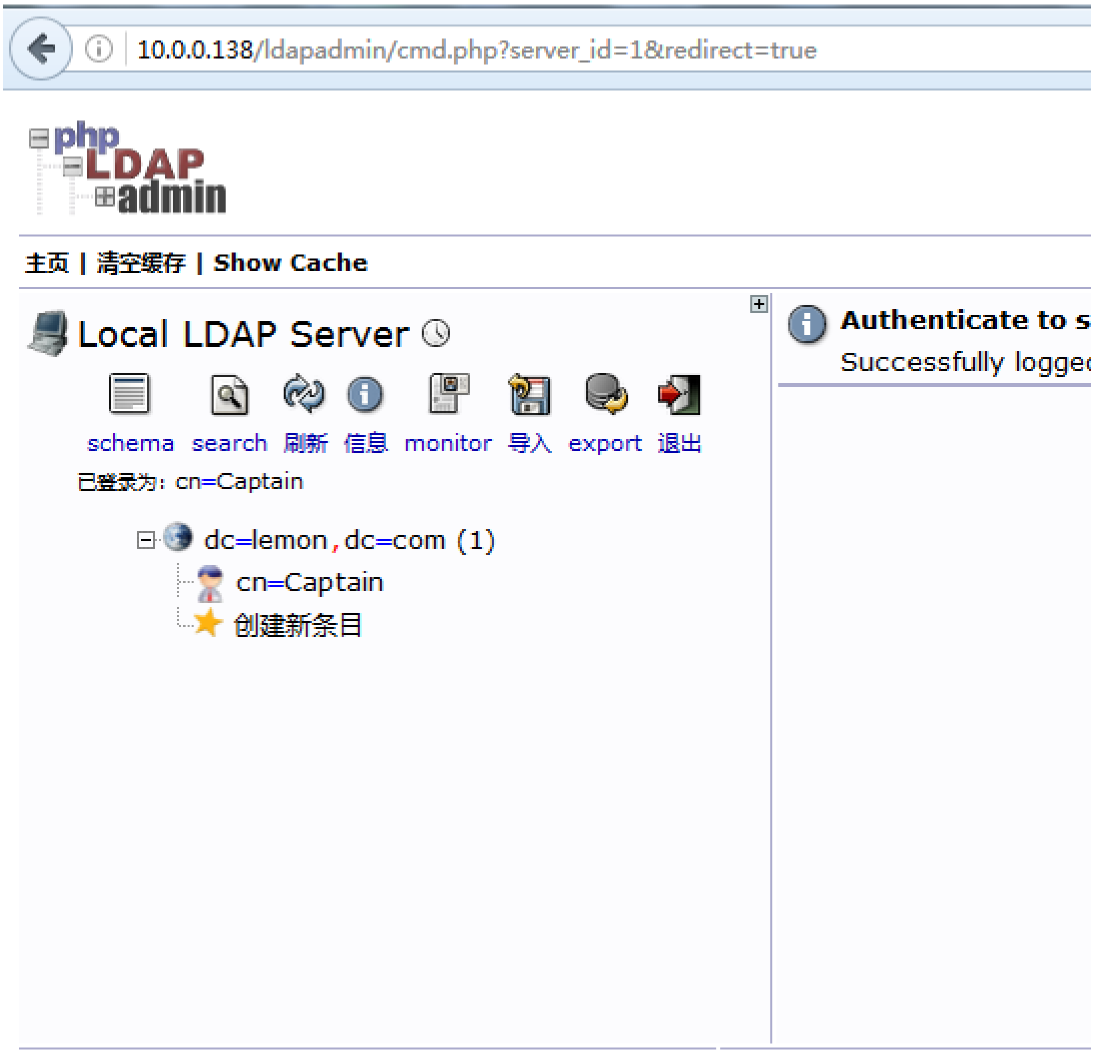
这里得注意每一个属性： **后必须有空格，但是值的后面不能有任何空格**

然后导入：ldapadd -x -D "cn=Captain,dc=lemon,dc=com" -W -f root.ldif



```
[root@lele ~]# ldapadd -x -D "cn=Captain,dc=lemon,dc=com" -W -f 1.ldif
Enter LDAP Password:
adding new entry "dc=lemon,dc=com"

adding new entry "cn=Captain,dc=lemon,dc=com"
```

然后再通过浏览器去访问的话：



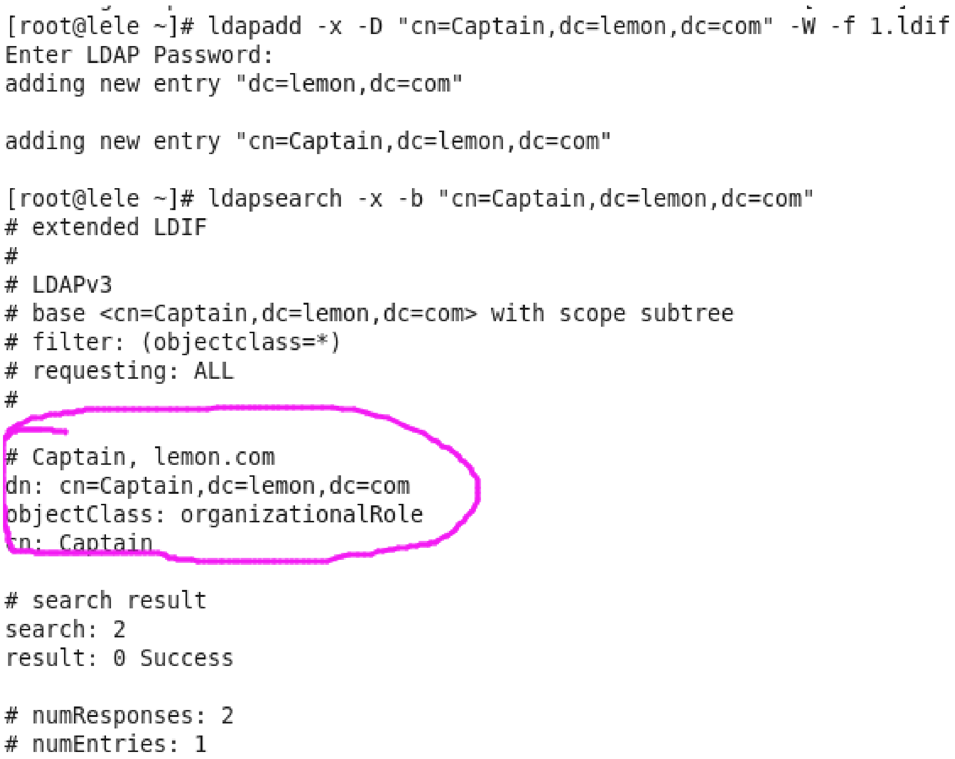
10.0.0.138/ldapadmin/cmd.php?server_id=1&redirect=true

已登录为：cn=Captain

dc=lemon,dc=com (1)
cn=Captain
创建新条目

Authenticate to s
Successfully logge

也可以通过命令行查询：**ldapsearch -x -b "cn=Captain,dc=lemon,dc=com"**

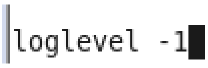


```
[root@lele ~]# ldapadd -x -D "cn=Captain,dc=lemon,dc=com" -W -f 1.ldif
Enter LDAP Password:
adding new entry "dc=lemon,dc=com"

adding new entry "cn=Captain,dc=lemon,dc=com"

[root@lele ~]# ldapsearch -x -b "cn=Captain,dc=lemon,dc=com"
# extended LDIF
#
# LDAPv3
# base <cn=Captain,dc=lemon,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# Captain, lemon.com
dn: cn=Captain,dc=lemon,dc=com
objectClass: organizationalRole
cn: Captain

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

到这里，PhpLDAPAdmin搭建完了，接下来，咱们得把**日志**打开，这样的话好排错，嘿嘿嘿

## 三：OpenLDAP的打开日志信息

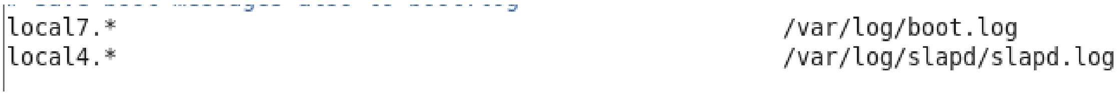
1：现在配置文件里加上日志行 ，这里的日志级别有很多种，-1的话会记录很多日志信息
vim /etc/openldap/slapd.conf 加上**loglevel -1**



```
loglevel -1
```

这里修改了配置文件，所有得重新生成配置文件的信息
rm -rf /etc/openldap/slapd.d/*
slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d/
chown -R ldap.ldap /etc/openldap/slapd.d/

2：在 vim /etc/rsyslog.conf加上
local4.*                                             /var/log/slapd/slapd.log



```
local7.*                                                /var/log/boot.log
local4.*                                                /var/log/slapd/slapd.log
```

然后重启/etc/init.d/rsyslog restart

3：创建日志文件目录，授权
mkdir /var/log/slapd
chmod 755 /var/log/slapd/
chown ldap.ldap /var/log/slapd/

4：重启slapd服务，/etc/init.d/slapd restart

5：就可以看到日志信息了cat /var/log/slapd/slapd.log

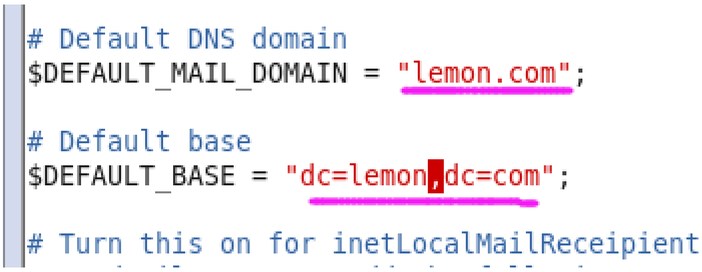
## 四：OpenLDAP与migrationtools实现导入系统账号的相关信息

1：安装migrationtools

  yum -y install migrationtools

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

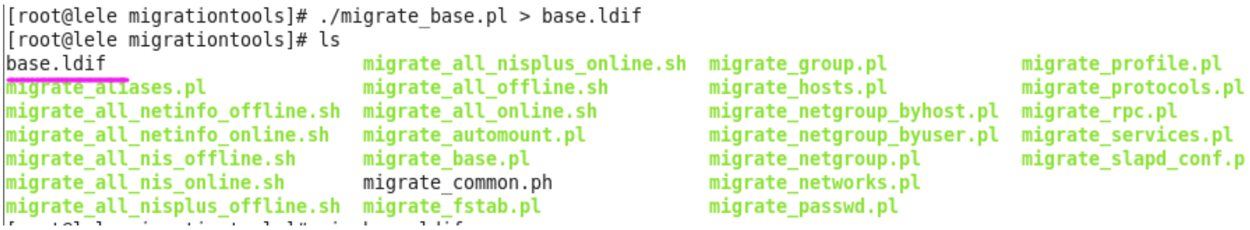
  vim /usr/share/migrationtools/migrate_common.ph 修改以下的两个地方



```
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = "lemon.com";

# Default base
$DEFAULT_BASE = "dc=lemon,dc=com";

# Turn this on for inetLocalMailReceipient
```

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

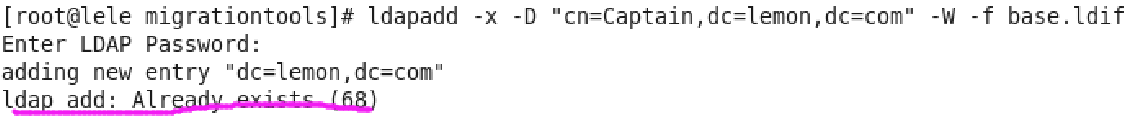
  /usr/share/migrationtools/migrate_base.pl > base.ldif



```
[root@lele migrationtools]# ./migrate_base.pl > base.ldif
[root@lele migrationtools]# ls
base.ldif                        migrate_all_nisplus_online.sh  migrate_group.pl             migrate_profile.pl
migrate_aliases.pl               migrate_all_offline.sh         migrate_hosts.pl             migrate_protocols.pl
migrate_all_netinfo_offline.sh   migrate_all_online.sh          migrate_netgroup_byhost.pl   migrate_rpc.pl
migrate_all_netinfo_online.sh    migrate_automount.pl           migrate_netgroup_byuser.pl   migrate_services.pl
migrate_all_nis_offline.sh       migrate_base.pl                migrate_netgroup.pl          migrate_slapd_conf.p
migrate_all_nis_online.sh        migrate_common.ph              migrate_networks.pl
migrate_all_nisplus_offline.sh   migrate_fstab.pl               migrate_passwd.pl
```

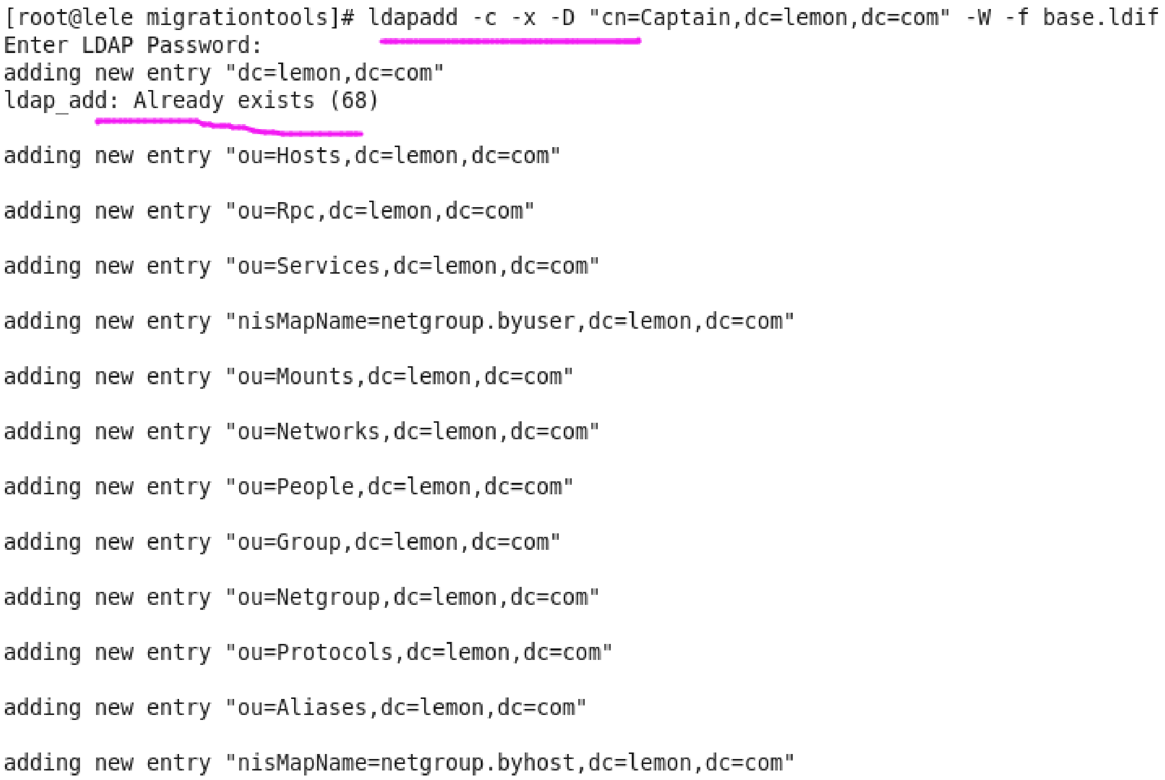
4：把base.ldif导入OpenLDAP

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



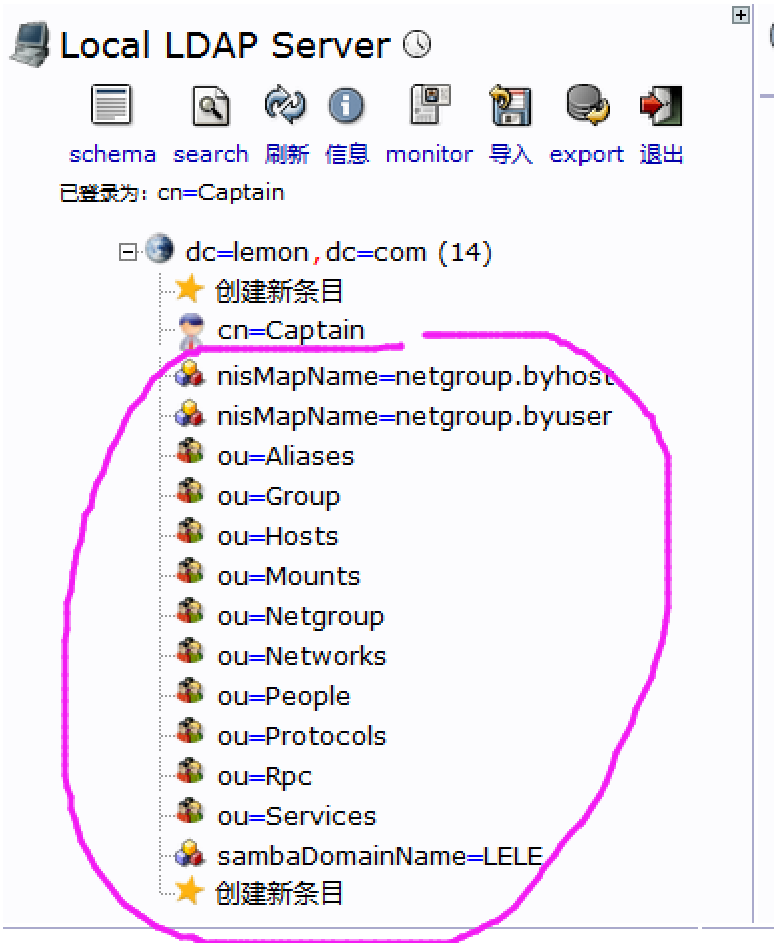
```
[root@lele migrationtools]# ldapadd -x -D "cn=Captain,dc=lemon,dc=com" -W -f base.ldif
Enter LDAP Password:
adding new entry "dc=lemon,dc=com"
ldap_add: Already exists (68)
```

  这里会报错，我们**可以通过-c参数强制加入**



```
[root@lele migrationtools]# ldapadd -c -x -D "cn=Captain,dc=lemon,dc=com" -W -f base.ldif
Enter LDAP Password:
adding new entry "dc=lemon,dc=com"
ldap_add: Already exists (68)

adding new entry "ou=Hosts,dc=lemon,dc=com"

adding new entry "ou=Rpc,dc=lemon,dc=com"

adding new entry "ou=Services,dc=lemon,dc=com"

adding new entry "nisMapName=netgroup.byuser,dc=lemon,dc=com"

adding new entry "ou=Mounts,dc=lemon,dc=com"

adding new entry "ou=Networks,dc=lemon,dc=com"

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

adding new entry "ou=Group,dc=lemon,dc=com"

adding new entry "ou=Netgroup,dc=lemon,dc=com"

adding new entry "ou=Protocols,dc=lemon,dc=com"

adding new entry "ou=Aliases,dc=lemon,dc=com"

adding new entry "nisMapName=netgroup.byhost,dc=lemon,dc=com"
```

导入之后，通过PhpLdapAdmin可以看到已经导入进来了：

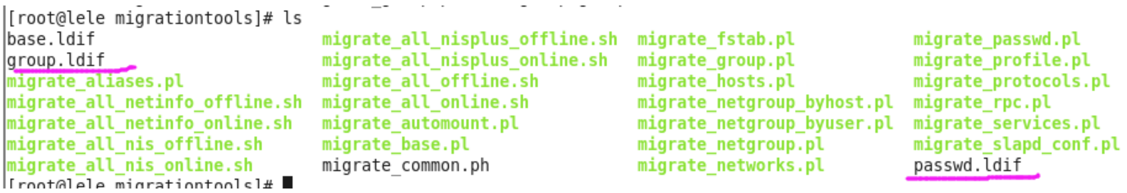


已登录为：cn=Captain

```
dc=lemon,dc=com (14)
  创建新条目
  cn=Captain
  nisMapName=netgroup.byhost
  nisMapName=netgroup.byuser
  ou=Aliases
  ou=Group
  ou=Hosts
  ou=Mounts
  ou=Netgroup
  ou=Networks
  ou=People
  ou=Protocols
  ou=Rpc
  ou=Services
  sambaDomainName=LELE
  创建新条目
```

5：把系统的用户生成ldif文件

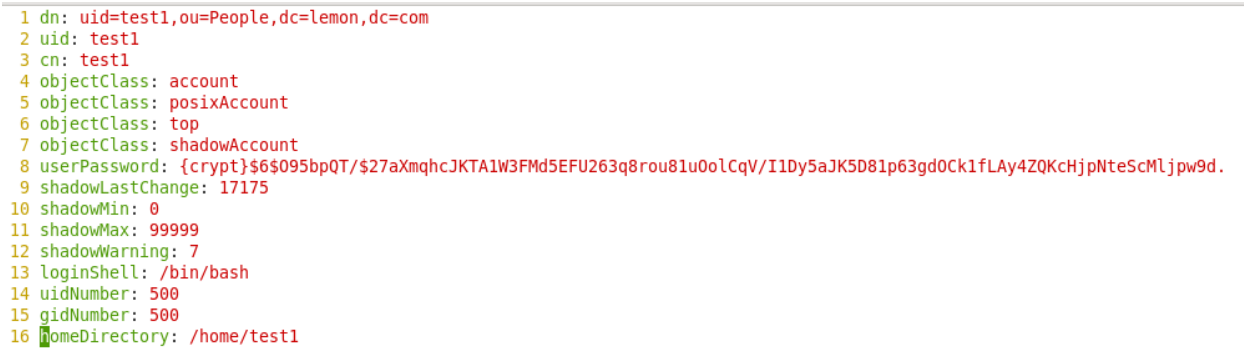
```
cd  /usr/share/migrationtools
./migrate_passwd.pl /etc/passwd passwd.ldif
./migrate_group.pl /etc/group group.ldif
```



```
[root@lele migrationtools]# ls
base.ldif                       migrate_all_nisplus_offline.sh  migrate_fstab.pl             migrate_passwd.pl
group.ldif                      migrate_all_nisplus_online.sh   migrate_group.pl             migrate_profile.pl
migrate_aliases.pl              migrate_all_offline.sh          migrate_hosts.pl             migrate_protocols.pl
migrate_all_netinfo_offline.sh  migrate_all_online.sh           migrate_netgroup_byhost.pl   migrate_rpc.pl
migrate_all_netinfo_online.sh   migrate_automount.pl            migrate_netgroup_byuser.pl   migrate_services.pl
migrate_all_nis_offline.sh      migrate_base.pl                 migrate_netgroup.pl          migrate_slapd_conf.pl
migrate_all_nis_online.sh       migrate_common.ph               migrate_networks.pl          passwd.ldif
[root@lele migrationtools]# 
```

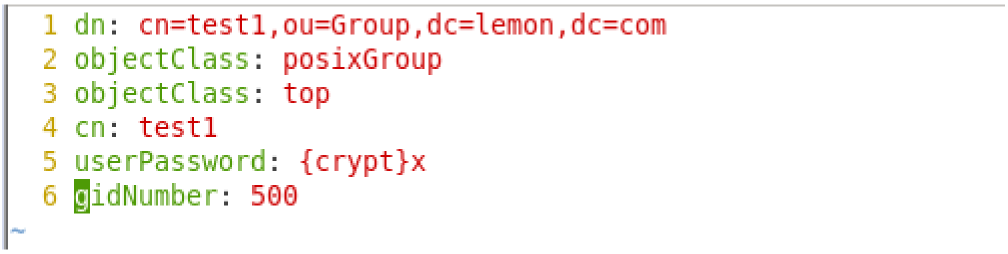
可以看到生成的文件，然后根据自己需要修改这两个ldif文件：

passwd.ldif只留一个test1测试用户：



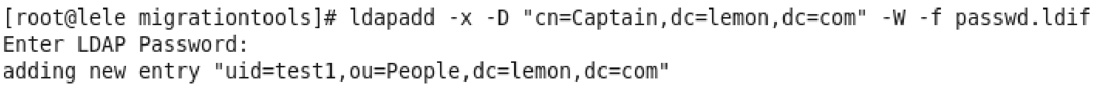
```
dn: uid=test1,ou=People,dc=lemon,dc=com
uid: test1
cn: test1
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {crypt}$6$095bpQT/$27aXmqhcJKTA1W3FMd5EFU263q8rou81uOolCqV/I1Dy5aJK5D81p63gdOCk1fLAy4ZQKcHjpNteScMljpw9d.
shadowLastChange: 17175
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 500
gidNumber: 500
homeDirectory: /home/test1
```

group.ldif留对应的test1：



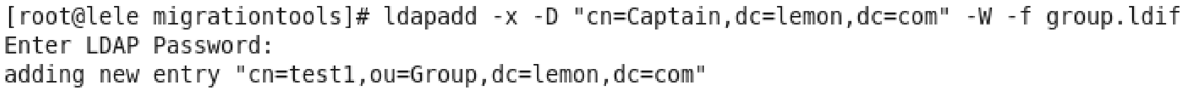
```
dn: cn=test1,ou=Group,dc=lemon,dc=com
objectClass: posixGroup
objectClass: top
cn: test1
userPassword: {crypt}x
gidNumber: 500
~
```

把用户导入进去：**ldapadd -x -D "cn=Captain,dc=lemon,dc=com" -W -f passwd.ldif**



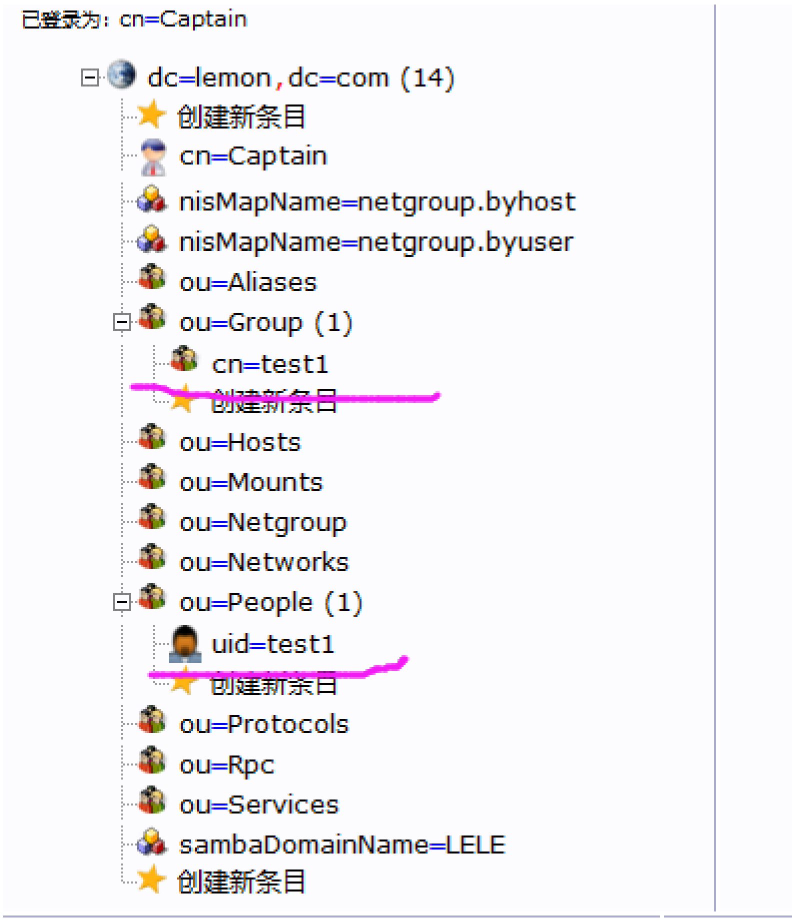
```
[root@lele migrationtools]# ldapadd -x -D "cn=Captain,dc=lemon,dc=com" -W -f passwd.ldif
Enter LDAP Password:
adding new entry "uid=test1,ou=People,dc=lemon,dc=com"
```

把组导进去：**ldapadd -x -D "cn=Captain,dc=lemon,dc=com" -W -f group.ldif**



```
[root@lele migrationtools]# ldapadd -x -D "cn=Captain,dc=lemon,dc=com" -W -f group.ldif
Enter LDAP Password:
adding new entry "cn=test1,ou=Group,dc=lemon,dc=com"
```

然后就可以看到：



```
已登录为：cn=Captain
⊟ dc=lemon,dc=com (14)
    创建新条目
    cn=Captain
    nisMapName=netgroup.byhost
    nisMapName=netgroup.byuser
    ou=Aliases
  ⊟ ou=Group (1)
      cn=test1
      创建新条目
    ou=Hosts
    ou=Mounts
    ou=Netgroup
    ou=Networks
  ⊟ ou=People (1)
      uid=test1
      创建新条目
    ou=Protocols
    ou=Rpc
    ou=Services
    sambaDomainName=LELE
    创建新条目
```

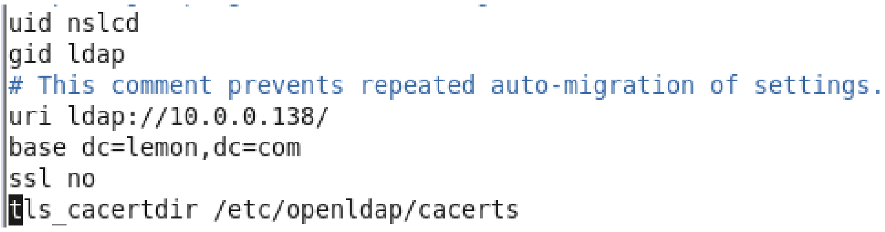
在这里就已经完成把系统的账号属性导入了OpenLDAP，然后就通过添加OpenLDAP用户，来进行验证，所以得先做好客户端的设置

## 五：OpenLDAP客户端的配置

1：停掉sssd服务  service sssd stop && chkconfig sssd off

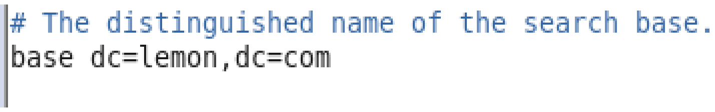
2：安装nslcd服务  yum install nss-pam-ldapd

3：修改vim /etc/nslcd.conf这个配置文件

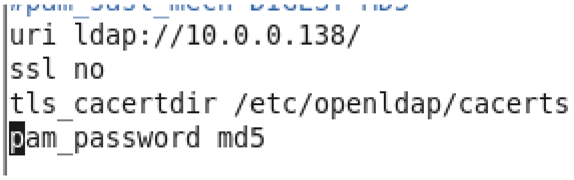


```
uid nslcd
gid ldap
# This comment prevents repeated auto-migration of settings.
uri ldap://10.0.0.138/
base dc=lemon,dc=com
ssl no
tls_cacertdir /etc/openldap/cacerts
```

4：修改vim /etc/pam_ldap.conf

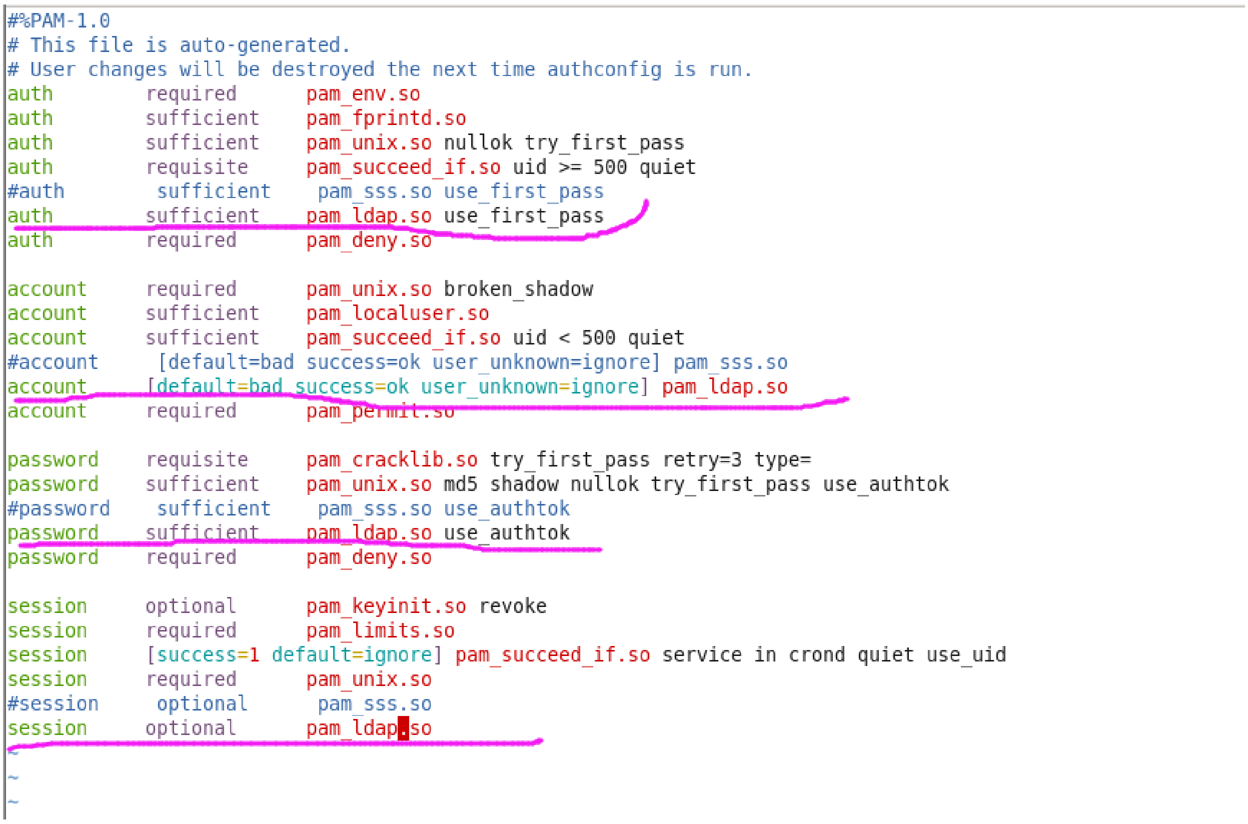


```
# The distinguished name of the search base.
base dc=lemon,dc=com
```



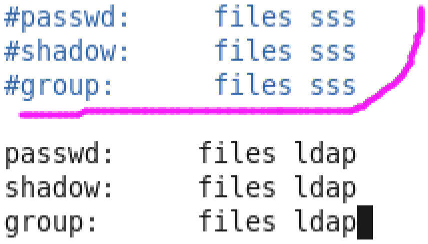
```
#pam_sasl_mech DIGEST-MD5
uri ldap://10.0.0.138/
ssl no
tls_cacertdir /etc/openldap/cacerts
pam_password md5
```

5： vim /etc/pam.d/system-auth 修改，把sss行的注释掉，改成ldap的



```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_fprintd.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
#auth        sufficient    pam_sss.so use_first_pass
auth        sufficient    pam_ldap.so use_first_pass
auth        required      pam_deny.so

account     required      pam_unix.so broken_shadow
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
#account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     [default=bad success=ok user_unknown=ignore] pam_ldap.so
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3 type=
password    sufficient    pam_unix.so md5 shadow nullok try_first_pass use_authtok
#password    sufficient    pam_sss.so use_authtok
password    sufficient    pam_ldap.so use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
#session     optional      pam_sss.so
session     optional      pam_ldap.so
~
~
```

6：vim /etc/nsswitch.conf 修改nsswitch.conf配置文件，修改后，默认登录的用户通过本地配置文件进行查找并匹配。当匹配不到用户信息时，会通过后端配置的LDAP认证服务进行匹配



```
#passwd:     files sss
#shadow:     files sss
#group:      files sss

passwd:     files ldap
shadow:     files ldap
group:      files ldap
```

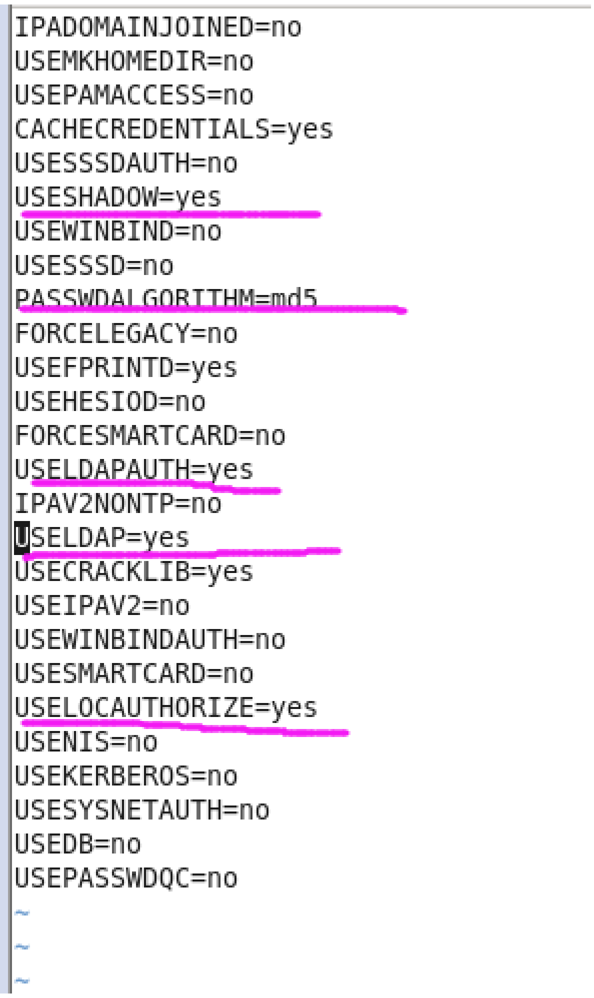
7：vim /etc/sysconfig/authconfig 确保标记的已打开为yes

USESHADOW=yes 启用密码验证

USELDAPAUTH=yes 启用OpenLDAP验证

USELOCAUTHORIZE=yes 启用本地验证

USELDAP=yes 启用LDAP认证协议

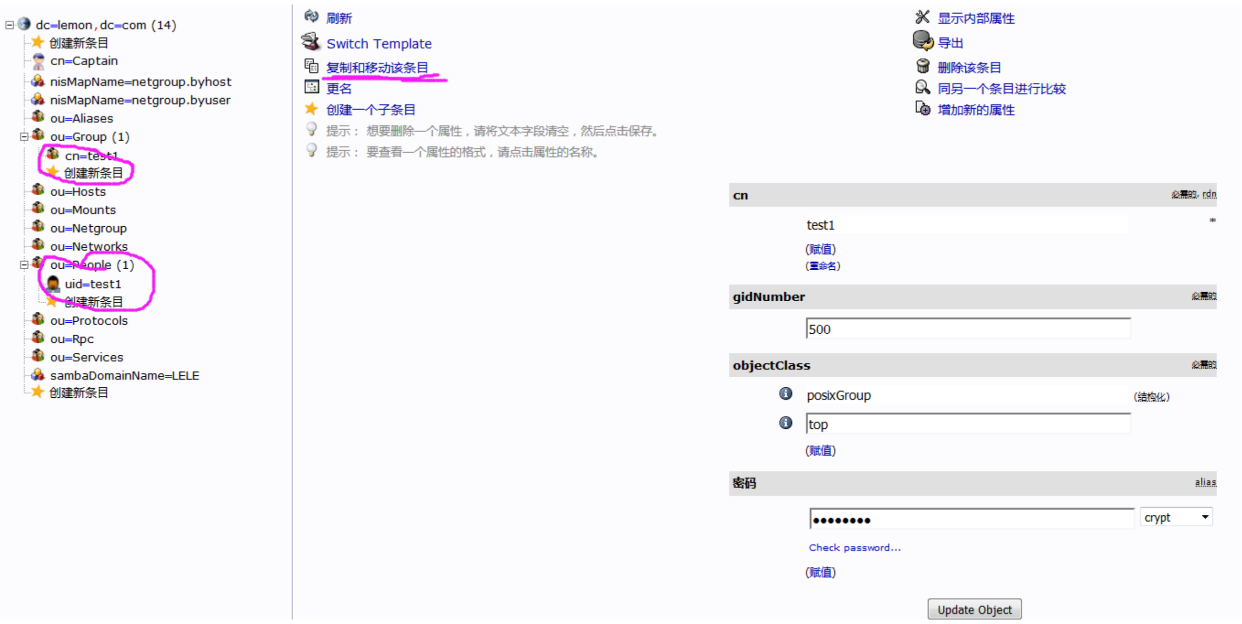


```
IPADOMAINJOINED=no
USEMKHOMEDIR=no
USEPAMACCESS=no
CACHECREDENTIALS=yes
USESSSDAUTH=no
USESHADOW=yes
USEWINBIND=no
USESSSD=no
PASSWDALGORITHM=md5
FORCELEGACY=no
USEFPRINTD=yes
USEHESIOD=no
FORCESMARTCARD=no
USELDAPAUTH=yes
IPAV2NONTP=no
USELDAP=yes
USECRACKLIB=yes
USEIPAV2=no
USEWINBINDAUTH=no
USESMARTCARD=no
USELOCAUTHORIZE=yes
USENIS=no
USEKERBEROS=no
USESYSNETAUTH=no
USEDB=no
USEPASSWDQC=no
~
~
~
```

8：重启nslcd服务

/etc/init.d/nslcd restart

9：验证，先通过OpenLDAP增加一个用户，在test1的基础上，复制一个test2的条目



```
dc=lemon,dc=com (14)
    创建新条目
    cn=Captain
    nisMapName=netgroup.byhost
    nisMapName=netgroup.byuser
    ou=Aliases
    ou=Group (1)
        cn=test1
        创建新条目
    ou=Hosts
    ou=Mounts
    ou=Netgroup
    ou=Networks
    ou=People (1)
        uid=test1
        创建新条目
    ou=Protocols
    ou=Rpc
    ou=Services
    sambaDomainName=LELE
    创建新条目
```

提示： 想要删除一个属性，请将文本字段清空，然后点击保存。

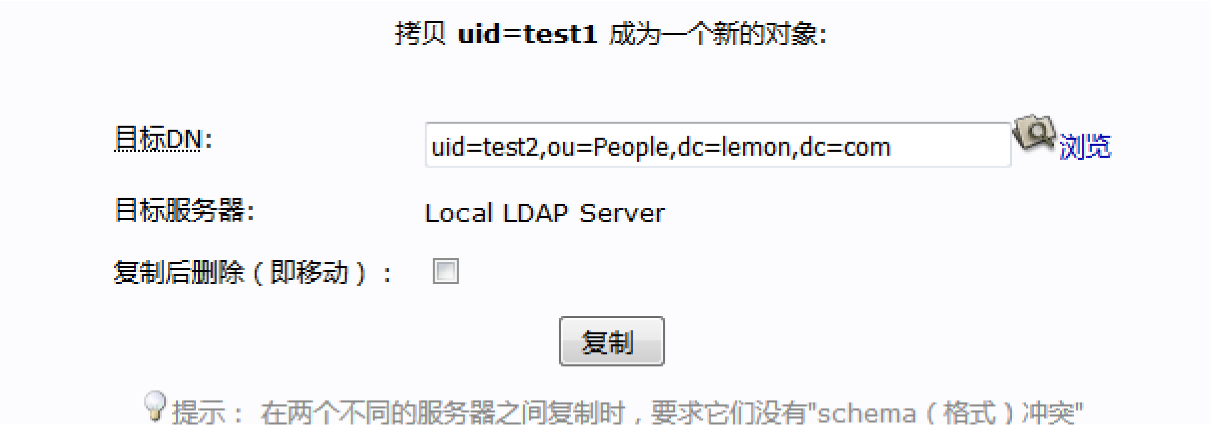
提示： 要查看一个属性的格式，请点击属性的名称。

cn 必需的, rdn: test1

gidNumber 必需的: 500

objectClass 必需的: posixGroup (结构化), top

密码 alias: •••••••• crypt



拷贝 **uid=test1** 成为一个新的对象:

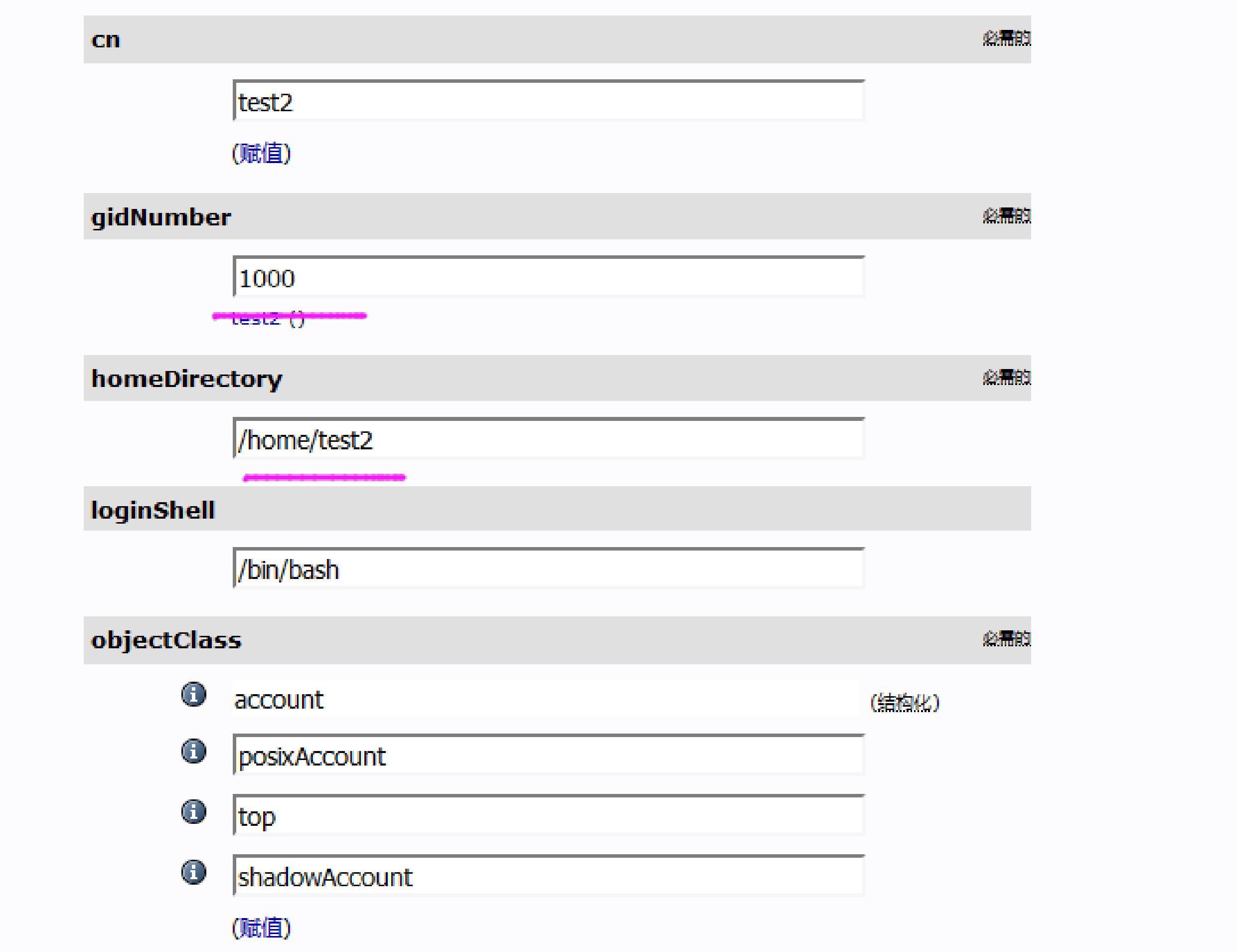
目标DN: uid=test2,ou=People,dc=lemon,dc=com

目标服务器: Local LDAP Server

复制后删除（即移动）： □

提示： 在两个不同的服务器之间复制时，要求它们没有"schema（格式）冲突"

后面的根据自己的修改



**cn** 必需的

test2

(赋值)

**gidNumber** 必需的

1000

~~test2 ()~~

**homeDirectory** 必需的

/home/test2

**loginShell**

/bin/bash

**objectClass** 必需的

account (结构化)

posixAccount

top

shadowAccount

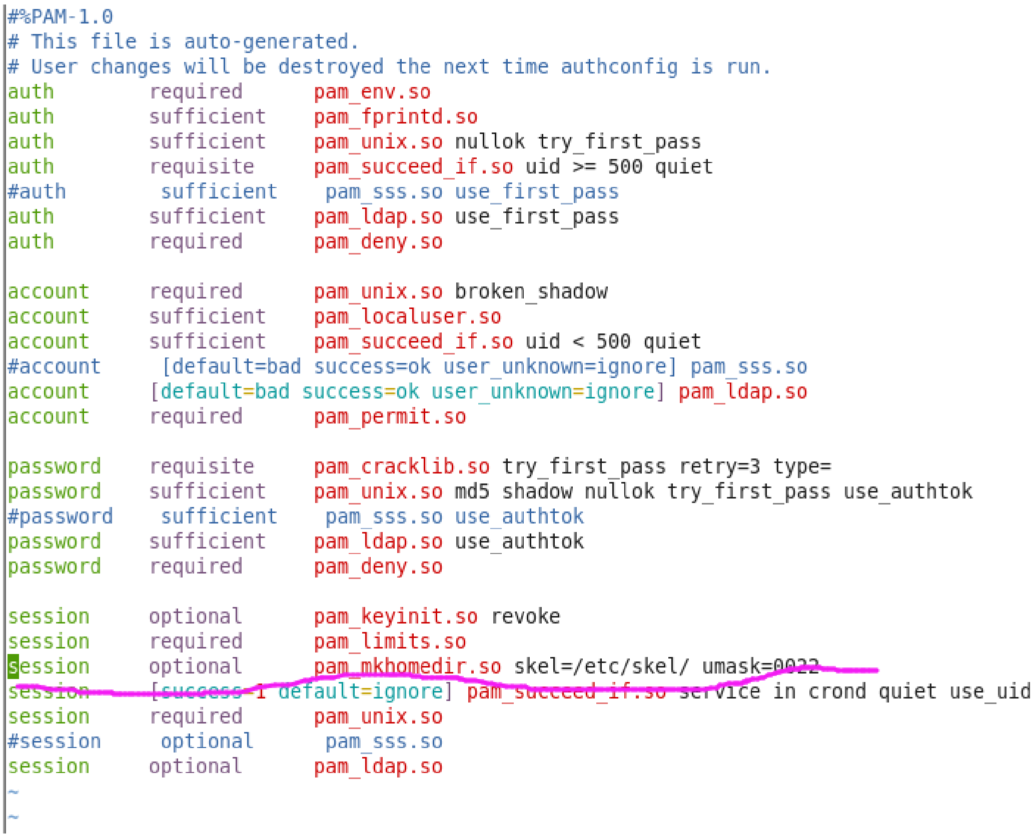
(赋值)

可以看到已经成功的添加了test2的用户，这是OpenLDAP添加的，在本地是没有的，用cat /etc/passwd 看是没有test2用户的

**测试：su - test2**

```
[root@lele migrationtools]# su - test2
su: warning: cannot change directory to /home/test2: No such file or directory
-bash-4.1$ exit
logout
```

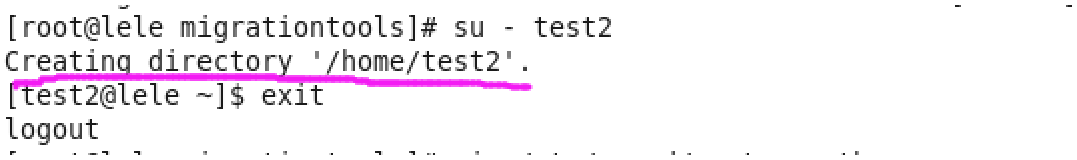
在/etc/pam.d/system-auth配置文件里添加这一行：**session optional pam_mkhomedir.so skel=/etc/skel/ umask=0022**



```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_fprintd.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
#auth        sufficient    pam_sss.so use_first_pass
auth        sufficient    pam_ldap.so use_first_pass
auth        required      pam_deny.so

account     required      pam_unix.so broken_shadow
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
#account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     [default=bad success=ok user_unknown=ignore] pam_ldap.so
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3 type=
password    sufficient    pam_unix.so md5 shadow nullok try_first_pass use_authtok
#password    sufficient    pam_sss.so use_authtok
password    sufficient    pam_ldap.so use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     optional      pam_mkhomedir.so skel=/etc/skel/ umask=0022
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
#session     optional      pam_sss.so
session     optional      pam_ldap.so
~
~
```

重启 /etc/init.d/nslcd restart

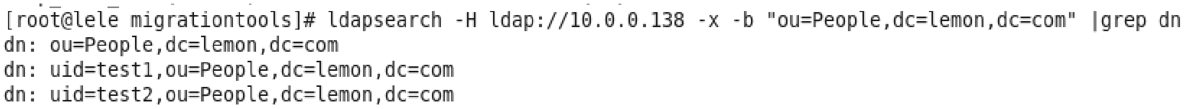
在进行测试：就可以了



```
[root@lele migrationtools]# su - test2
Creating directory '/home/test2'.
[test2@lele ~]$ exit
logout
```

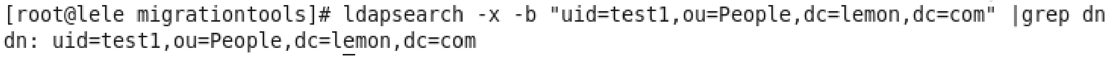
查看系统用户列表：

服务端查询：**ldapsearch -x -b "ou=People,dc=lemon,dc=com" |grep dn**



```
[root@lele migrationtools]# ldapsearch -H ldap://10.0.0.138 -x -b "ou=People,dc=lemon,dc=com" |grep dn
dn: ou=People,dc=lemon,dc=com
dn: uid=test1,ou=People,dc=lemon,dc=com
dn: uid=test2,ou=People,dc=lemon,dc=com
```

查询单个用户：**ldapsearch -x -b "uid=test1,ou=People,dc=lemon,dc=com" |grep dn**

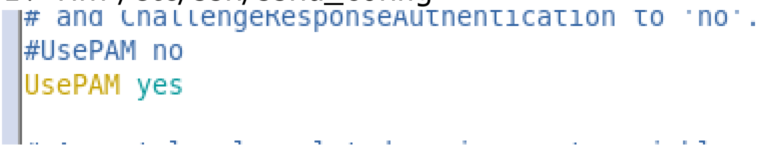


```
[root@lele migrationtools]# ldapsearch -x -b "uid=test1,ou=People,dc=lemon,dc=com" |grep dn
dn: uid=test1,ou=People,dc=lemon,dc=com
```

客户端的配置到这里ok啦。有账号肯定要能通过ssh登录系统

## 六：OpenLDAP与SSH

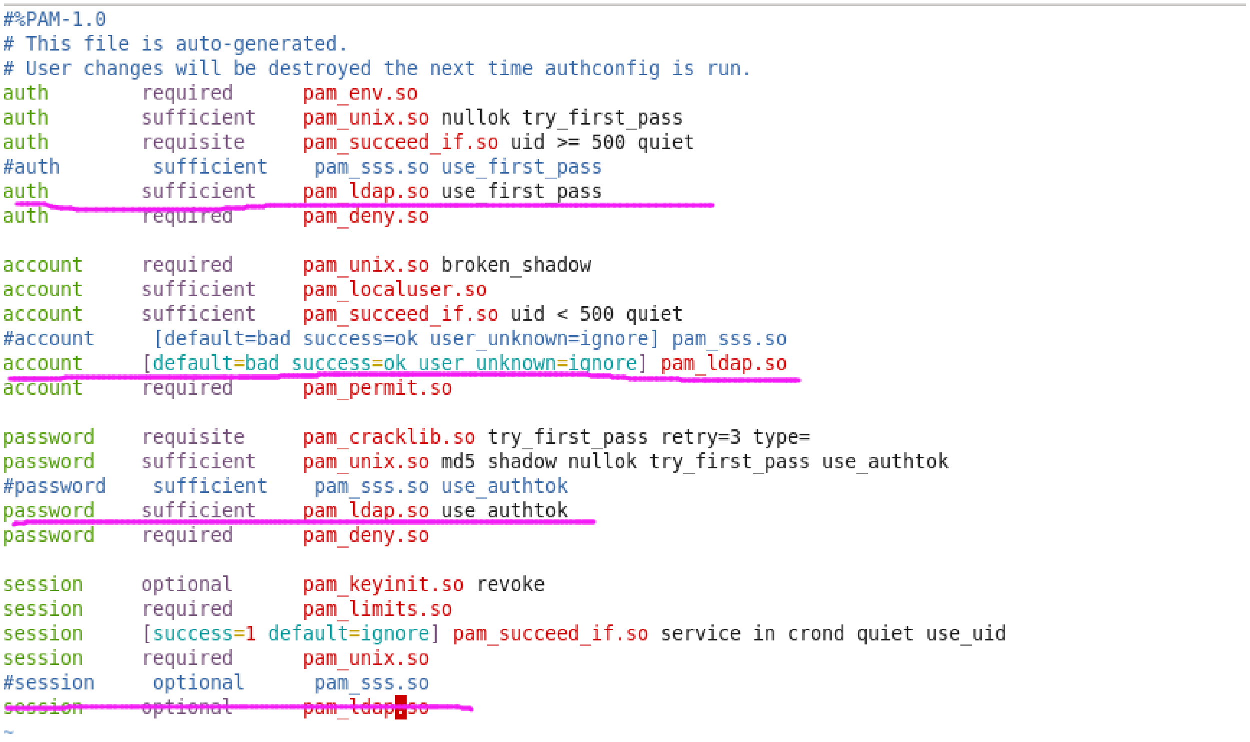
1：vim /etc/ssh/sshd_config



```
# and ChallengeResponseAuthentication to 'no'.
#UsePAM no
UsePAM yes
```

2：vim /etc/pam.d/sshd  用于第一次登陆的账户自动创建家目录

3：vim /etc/pam.d/password-auth



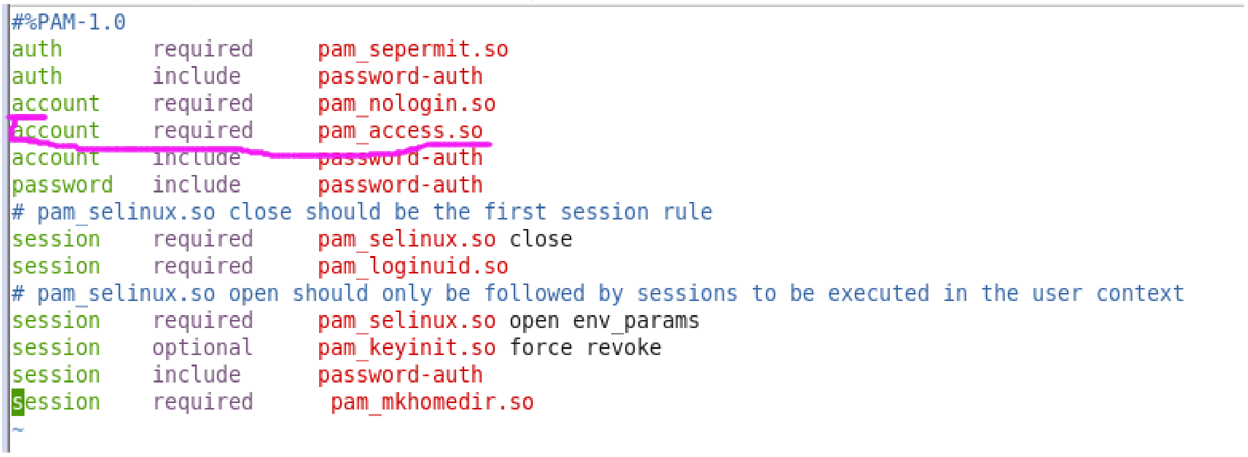
```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
#auth        sufficient    pam_sss.so use_first_pass
auth        sufficient    pam_ldap.so use_first_pass
auth        required      pam_deny.so

account     required      pam_unix.so broken_shadow
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
#account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     [default=bad success=ok user_unknown=ignore] pam_ldap.so
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3 type=
password    sufficient    pam_unix.so md5 shadow nullok try_first_pass use_authtok
#password    sufficient    pam_sss.so use_authtok
password    sufficient    pam_ldap.so use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
#session     optional      pam_sss.so
session     optional      pam_ldap.so
~
```

4：重启sshd

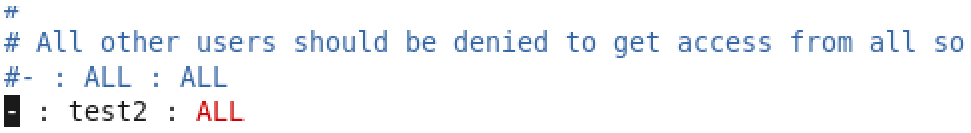
## 七：OpenLDAP限制用户登录系统

在账号中，不能让每个用户都能登录系统，所以要限制用户登录

1：vim /etc/pam.d/sshd 在这里加上pam_access.so模块

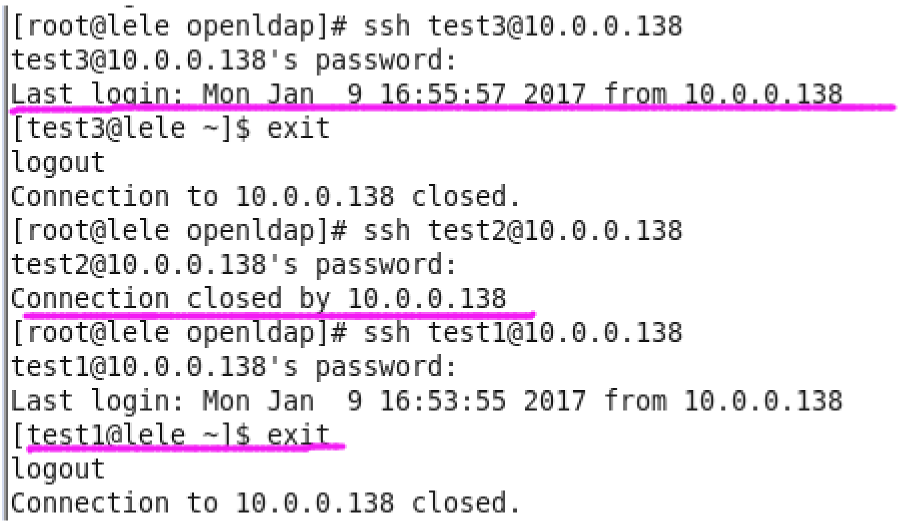


```
#%PAM-1.0
auth       required     pam_sepermit.so
auth       include      password-auth
account    required     pam_nologin.so
account    required     pam_access.so
account    include      password-auth
password   include      password-auth
# pam_selinux.so close should be the first session rule
session    required     pam_selinux.so close
session    required     pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session    required     pam_selinux.so open env_params
session    optional     pam_keyinit.so force revoke
session    include      password-auth
session    required      pam_mkhomedir.so
~
```



```
#
# All other users should be denied to get access from all so
#- : ALL : ALL
- : test2 : ALL
```

测试：可以看到就只有test2登录不上



```
[root@lele openldap]# ssh test3@10.0.0.138
test3@10.0.0.138's password:
Last login: Mon Jan  9 16:55:57 2017 from 10.0.0.138
[test3@lele ~]$ exit
logout
Connection to 10.0.0.138 closed.
[root@lele openldap]# ssh test2@10.0.0.138
test2@10.0.0.138's password:
Connection closed by 10.0.0.138
[root@lele openldap]# ssh test1@10.0.0.138
test1@10.0.0.138's password:
Last login: Mon Jan  9 16:53:55 2017 from 10.0.0.138
[test1@lele ~]$ exit
logout
Connection to 10.0.0.138 closed.
```

## 八：OpenLDAP强制用户一登录系统更改密码

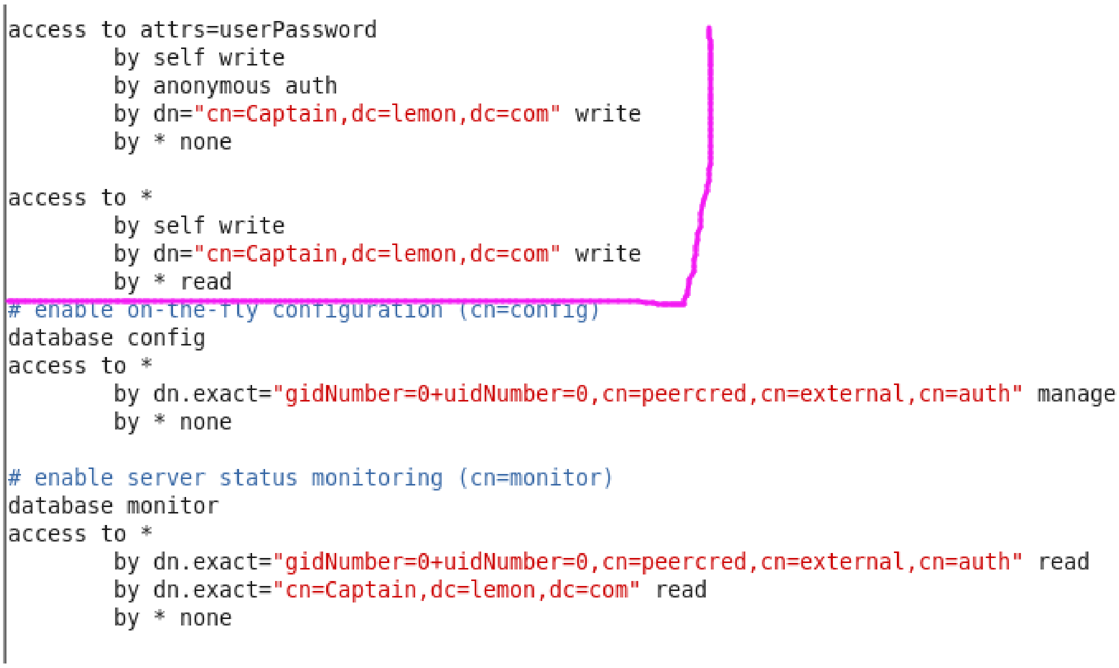
1：修改配置文件

在前面打开注释

```
moduleload ppolicy.la
modulepath /usr/lib/openldap
modulepath /usr/lib64/openldap
```

还要在database config前面加上这两段

```
access to attrs=userPassword
    by self write
    by anonymous auth
    by dn="cn=Captain,dc=lemon,dc=com" write
    by * none

access to *
    by self write
    by dn="cn=Captain,dc=lemon,dc=com" write
    by * read
```

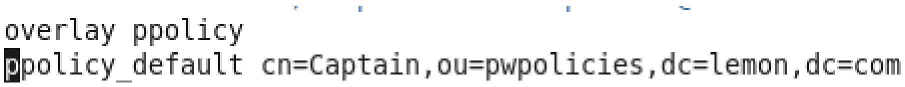


```
access to attrs=userPassword
        by self write
        by anonymous auth
        by dn="cn=Captain,dc=lemon,dc=com" write
        by * none

access to *
        by self write
        by dn="cn=Captain,dc=lemon,dc=com" write
        by * read
# enable on-the-fly configuration (cn=config)
database config
access to *
        by dn.exact="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage
        by * none

# enable server status monitoring (cn=monitor)
database monitor
access to *
        by dn.exact="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read
        by dn.exact="cn=Captain,dc=lemon,dc=com" read
        by * none
```

在文件的末尾添加:

**overlay ppolicy**

**ppolicy_default cn=Captain,ou=pwpolicies,dc=lemon,dc=com**



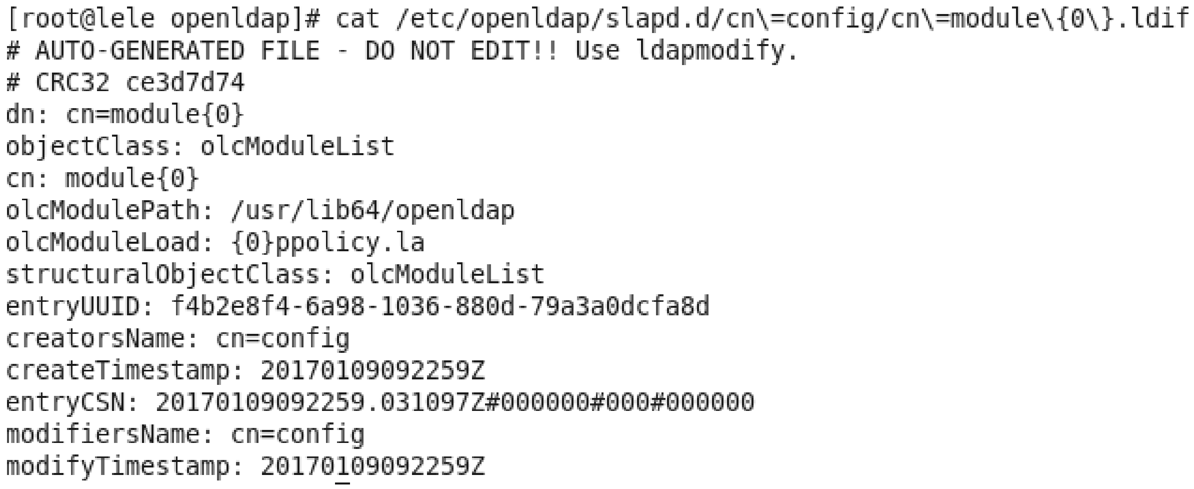
```
overlay ppolicy
ppolicy_default cn=Captain,ou=pwpolicies,dc=lemon,dc=com
```

2：重新生成配置文件数据库:

```
[root@lele openldap]# vim /etc/openldap/slapd.conf
[root@lele openldap]# rm -rf /etc/openldap/slapd.d/*
[root@lele openldap]#  slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d
config file testing succeeded
[root@lele openldap]# chown -R ldap.ldap /etc/openldap/slapd.d/
[root@lele openldap]# /etc/init.d/slapd restart
Stopping slapd:                                            [  OK  ]
Starting slapd:                                            [  OK  ]
```

可以通过配置文件的数据信息看到ppolicy模块已经加进来了

**cat /etc/openldap/slapd.d/cn\=config/cn\=module\{0\}.ldif**



```
[root@lele openldap]# cat /etc/openldap/slapd.d/cn\=config/cn\=module\{0\}.ldif
# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
# CRC32 ce3d7d74
dn: cn=module{0}
objectClass: olcModuleList
cn: module{0}
olcModulePath: /usr/lib64/openldap
olcModuleLoad: {0}ppolicy.la
structuralObjectClass: olcModuleList
entryUUID: f4b2e8f4-6a98-1036-880d-79a3a0dcfa8d
creatorsName: cn=config
createTimestamp: 20170109092259Z
entryCSN: 20170109092259.031097Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20170109092259Z
```

3：编辑

cat 1.ldif

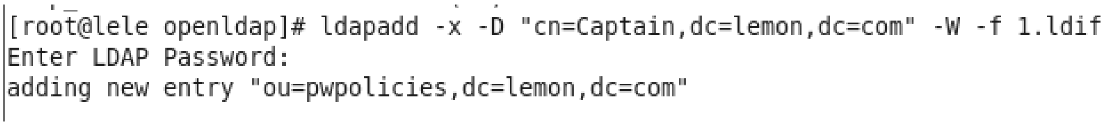
dn: ou=pwpolicies,dc=lemon,dc=com

objectClass: organizationalUnit

ou: pwpolicies

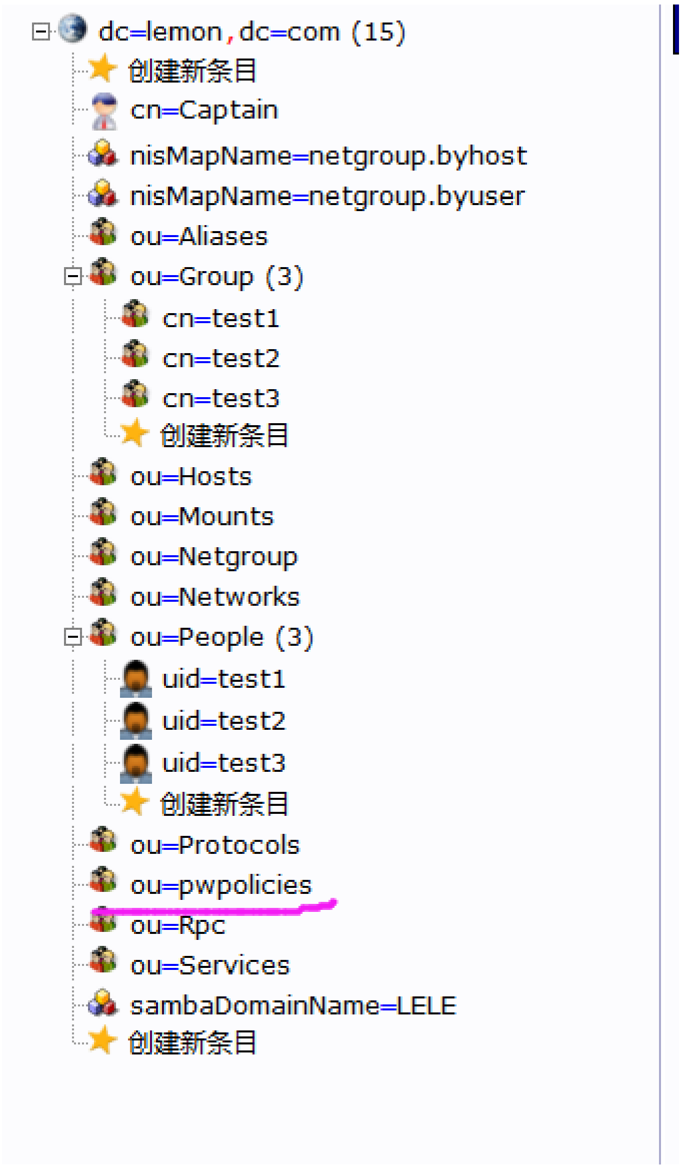
4：ldapadd -x -D "cn=Captain,dc=lemon,dc=com" -W -f 1.ldif

添加进去



```
[root@lele openldap]# ldapadd -x -D "cn=Captain,dc=lemon,dc=com" -W -f 1.ldif
Enter LDAP Password:
adding new entry "ou=pwpolicies,dc=lemon,dc=com"
```

可以在PhpLdapAdmin上看到:



```
dc=lemon,dc=com (15)
    创建新条目
    cn=Captain
    nisMapName=netgroup.byhost
    nisMapName=netgroup.byuser
    ou=Aliases
    ou=Group (3)
        cn=test1
        cn=test2
        cn=test3
        创建新条目
    ou=Hosts
    ou=Mounts
    ou=Netgroup
    ou=Networks
    ou=People (3)
        uid=test1
        uid=test2
        uid=test3
        创建新条目
    ou=Protocols
    ou=pwpolicies
    ou=Rpc
    ou=Services
    sambaDomainName=LELE
    创建新条目
```

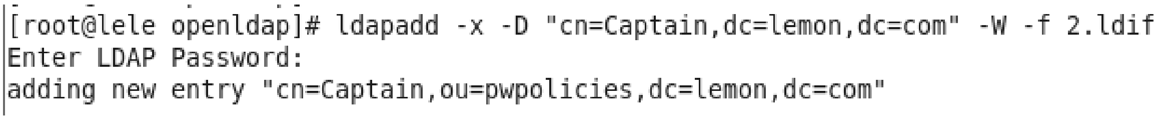
5：**添加cn=Captain,ou=pwpolicies,dc=lemon,dc=com这个的一些属性值**

[root@ll ~]# cat 2.ldif

```
dn: cn=Captain,ou=pwpolicies,dc=lemon,dc=com
cn: Captain
objectClass: pwdPolicy
objectClass: person
pwdAllowUserChange: TRUE
pwdAttribute: userPassword
pwdExpireWarning: 259200
pwdFailureCountInterval: 0
pwdGraceAuthNLimit: 5
pwdInHistory: 5
pwdLockout: TRUE
pwdLockoutDuration: 300
pwdMaxAge: 2592000
pwdMaxFailure: 5
pwdMinAge: 0
pwdMinLength: 8
```

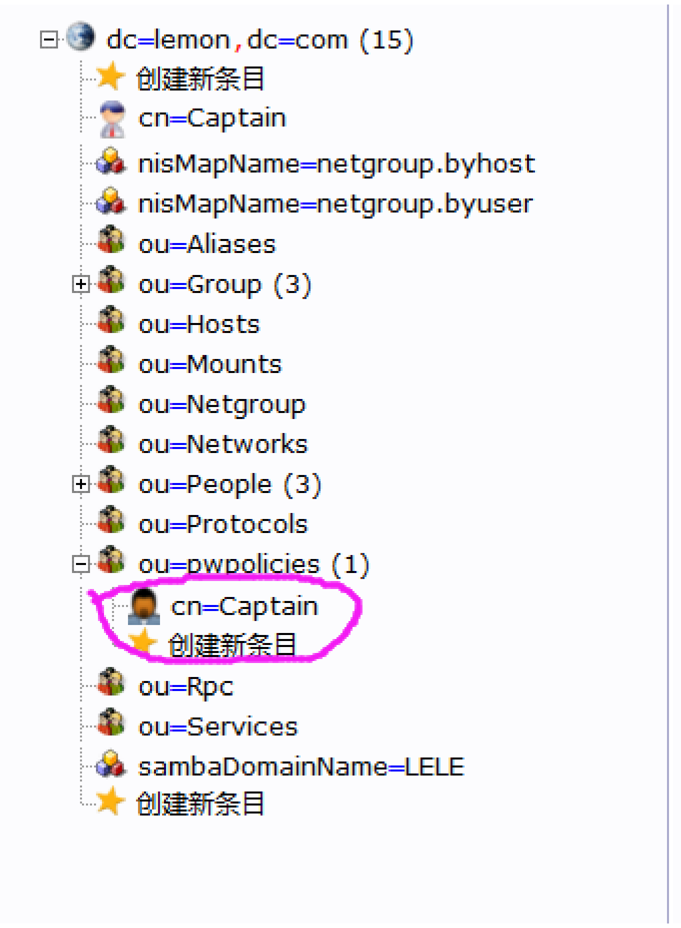
```
pwdMustChange: TRUE
pwdSafeModify: TRUE
sn: dummy value
```

把属性值添加进去



```
[root@lele openldap]# ldapadd -x -D "cn=Captain,dc=lemon,dc=com" -W -f 2.ldif
Enter LDAP Password:
adding new entry "cn=Captain,ou=pwpolicies,dc=lemon,dc=com"
```

在PhpLdapAdmin可以看到:



```
dc=lemon,dc=com (15)
    创建新条目
    cn=Captain
    nisMapName=netgroup.byhost
    nisMapName=netgroup.byuser
    ou=Aliases
  ⊞ ou=Group (3)
    ou=Hosts
    ou=Mounts
    ou=Netgroup
    ou=Networks
  ⊞ ou=People (3)
    ou=Protocols
  ⊟ ou=pwpolicies (1)
        cn=Captain
        创建新条目
    ou=Rpc
    ou=Services
    sambaDomainName=LELE
    创建新条目
```

6：在vim /etc/pam_ldap.conf中的末尾添加：使得客户端能识别服务端的密码策略

```
pam_password md5
bind_policy soft
pam_lookup_policy yes
pam_password clear_remove_old
```

7：重启nslcd

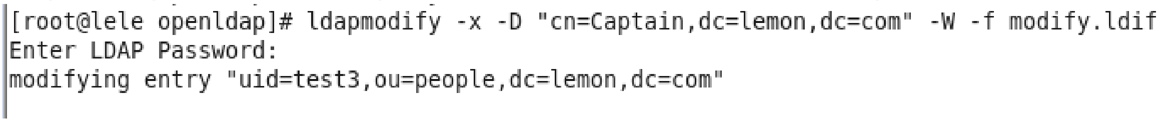
```
/etc/init.d/nslcd restart
```

8：测试

修改用户的属性，用test3做测试

```
[root@ll ~]# cat modify.ldif
dn: uid=test3,ou=people,dc=lemon,dc=com
changetype: modify
replace: pwdReset
pwdReset: TRUE
```

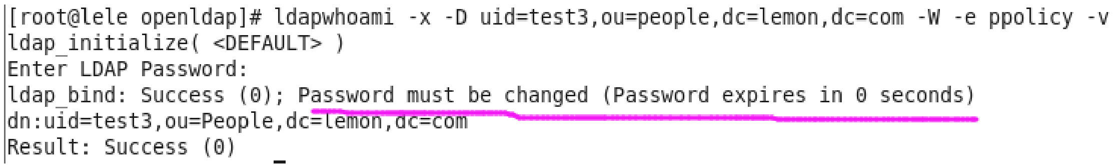
ldapmodify -x -D "cn=Captain,dc=le,dc=com" -W -f modify.ldif  导入



```
[root@lele openldap]# ldapmodify -x -D "cn=Captain,dc=lemon,dc=com" -W -f modify.ldif
Enter LDAP Password:
modifying entry "uid=test3,ou=people,dc=lemon,dc=com"
```

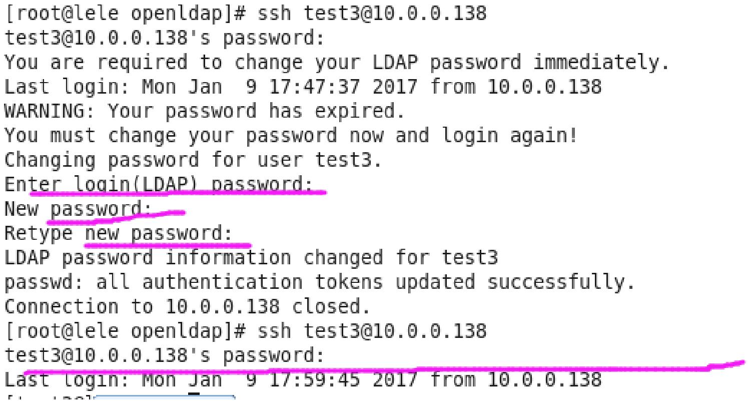
**ldapwhoami -x -D uid=test3,ou=people,dc=lemon,dc=com -W -e ppolicy -v**

查看test3用户的策略信息



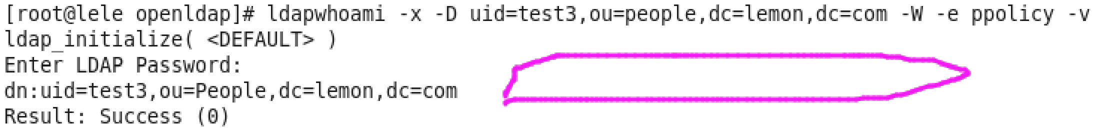
```
[root@lele openldap]# ldapwhoami -x -D uid=test3,ou=people,dc=lemon,dc=com -W -e ppolicy -v
ldap_initialize( <DEFAULT> )
Enter LDAP Password:
ldap_bind: Success (0); Password must be changed (Password expires in 0 seconds)
dn:uid=test3,ou=People,dc=lemon,dc=com
Result: Success (0)
```

这里显示输入test3 的原始密码，然后输入新修改的密码



```
[root@lele openldap]# ssh test3@10.0.0.138
test3@10.0.0.138's password:
You are required to change your LDAP password immediately.
Last login: Mon Jan  9 17:47:37 2017 from 10.0.0.138
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user test3.
Enter login(LDAP) password:
New password:
Retype new password:
LDAP password information changed for test3
passwd: all authentication tokens updated successfully.
Connection to 10.0.0.138 closed.
[root@lele openldap]# ssh test3@10.0.0.138
test3@10.0.0.138's password:
Last login: Mon Jan  9 17:59:45 2017 from 10.0.0.138
```

当修改完后，就没有必须改变密码的那一句话了



```
[root@lele openldap]# ldapwhoami -x -D uid=test3,ou=people,dc=lemon,dc=com -W -e ppolicy -v
ldap_initialize( <DEFAULT> )
Enter LDAP Password:
dn:uid=test3,ou=People,dc=lemon,dc=com
Result: Success (0)
```

这里可以啦

## 九：OpenLDAP与系统账号结合Samba

默认的Samba服务器支持本地系统用户（smbpasswd添加后）访问Samba资源，不支持OpenLDAP服务器账号访问Samba共享资源，配置完后，OpenLDAP每新增一个用户，就自动支持Samba，就可以用这个账号直接访问Samba，不需要存在于本地用户，不用smbpasswd用户

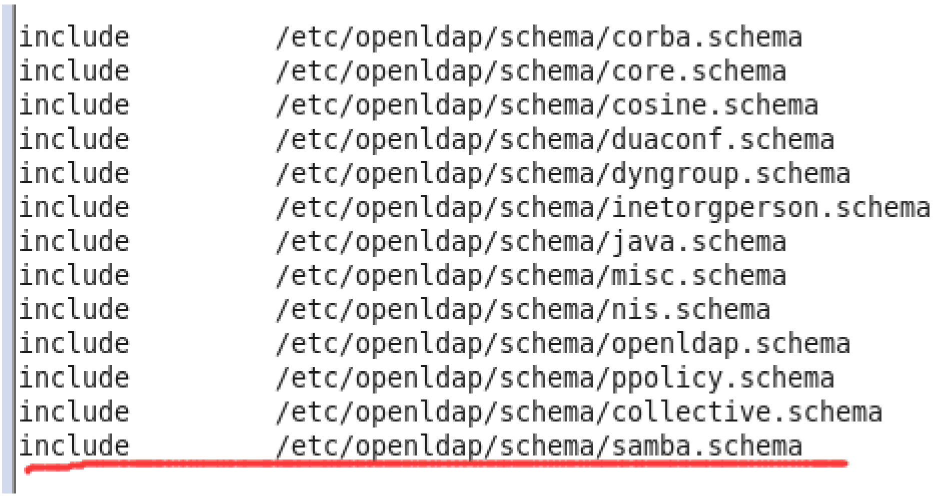
1：安装samba

```
yum -y install samba
```

2：把Samba.schema文件拷贝到LDAP的schema目录下，把原来的覆盖掉

3：修改配置文件vim /etc/openldap/slapd.conf

在include的地方，加上Samba的schema



```
include         /etc/openldap/schema/corba.schema
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/duaconf.schema
include         /etc/openldap/schema/dyngroup.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/java.schema
include         /etc/openldap/schema/misc.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/openldap.schema
include         /etc/openldap/schema/ppolicy.schema
include         /etc/openldap/schema/collective.schema
include         /etc/openldap/schema/samba.schema
```

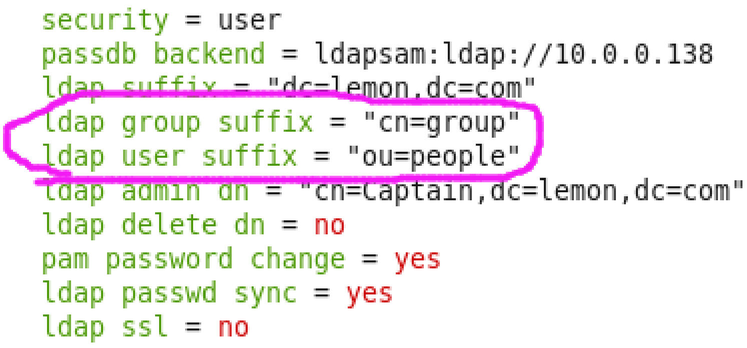
3：修改了配置文件，就有重新生成配置文件数据

```
rm -rf /etc/openldap/slapd.d/*
slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d/
config file testing succeeded
chown -R ldap.ldap /etc/openldap/slapd.d/
/etc/init.d/slapd restart
```

4：修改Samba的配置文件

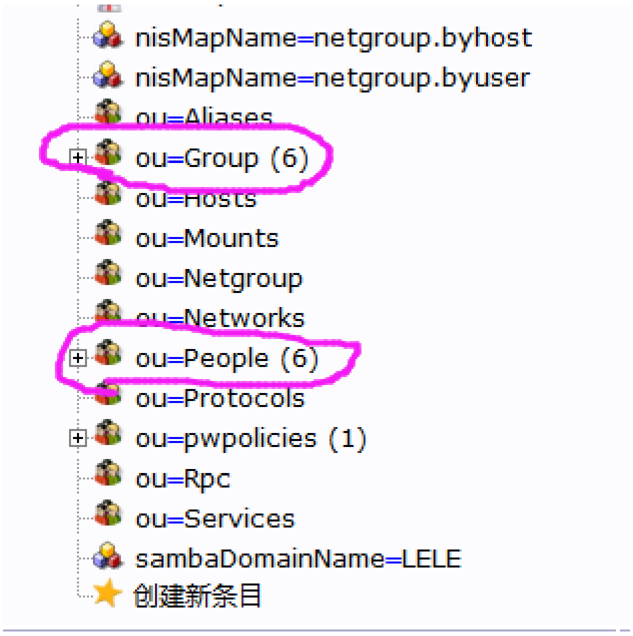
添加：

```
security = user
  passdb backend = ldapsam:ldap://10.0.0.138
  ldap suffix = "dc=lemon,dc=com"
  ldap group suffix = "cn=group"
  ldap user suffix = "ou=people"
  ldap admin dn = "cn=Captain,dc=lemon,dc=com"
  ldap delete dn = no
  pam password change = yes
  ldap passwd sync = yes
  ldap ssl = no
```



```
security = user
passdb backend = ldapsam:ldap://10.0.0.138
ldap suffix = "dc=lemon,dc=com"
ldap group suffix = "cn=group"
ldap user suffix = "ou=people"
ldap admin dn = "cn=Captain,dc=lemon,dc=com"
ldap delete dn = no
pam password change = yes
ldap passwd sync = yes
ldap ssl = no
```

对应这里的



nisMapName=netgroup.byhost
nisMapName=netgroup.byuser
ou=Aliases
ou=Group (6)
ou=Hosts
ou=Mounts
ou=Netgroup
ou=Networks
ou=People (6)
ou=Protocols
ou=pwpolicies (1)
ou=Rpc
ou=Services
sambaDomainName=LELE
创建新条目

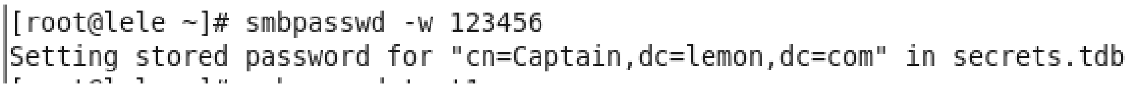
在最后的时候添加共享的文件：

```
[public]
comment = Public Stuff
path = /tmp/lile
public = yes
writable = yes
printable = no
```

5：创建共享文件夹，并且授权

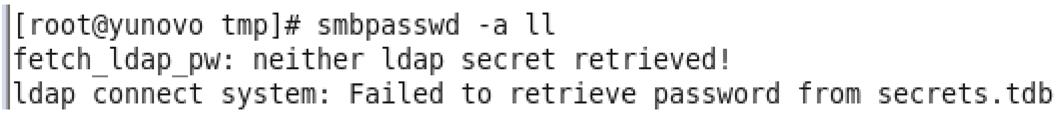
```
mkdir /tmp/lile
chmod 777 /tmp/lile/
```

6：把OpenLDAP的密码传给Samba，**smbpasswd -w 123456  这里的密码是OpenLDAP的管理员密码**



```
[root@lele ~]# smbpasswd -w 123456
Setting stored password for "cn=Captain,dc=lemon,dc=com" in secrets.tdb
```

若不加，会报错：

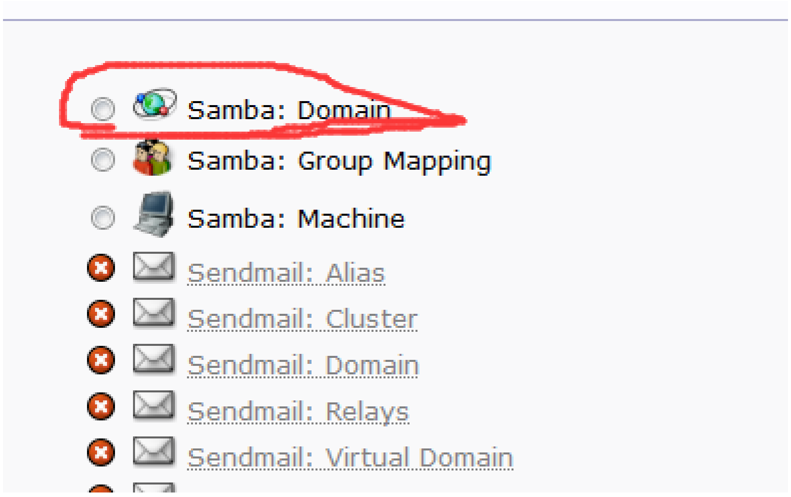


```
[root@yunovo tmp]# smbpasswd -a ll
fetch_ldap_pw: neither ldap secret retrieved!
ldap connect system: Failed to retrieve password from secrets.tdb
```

7：重启smb

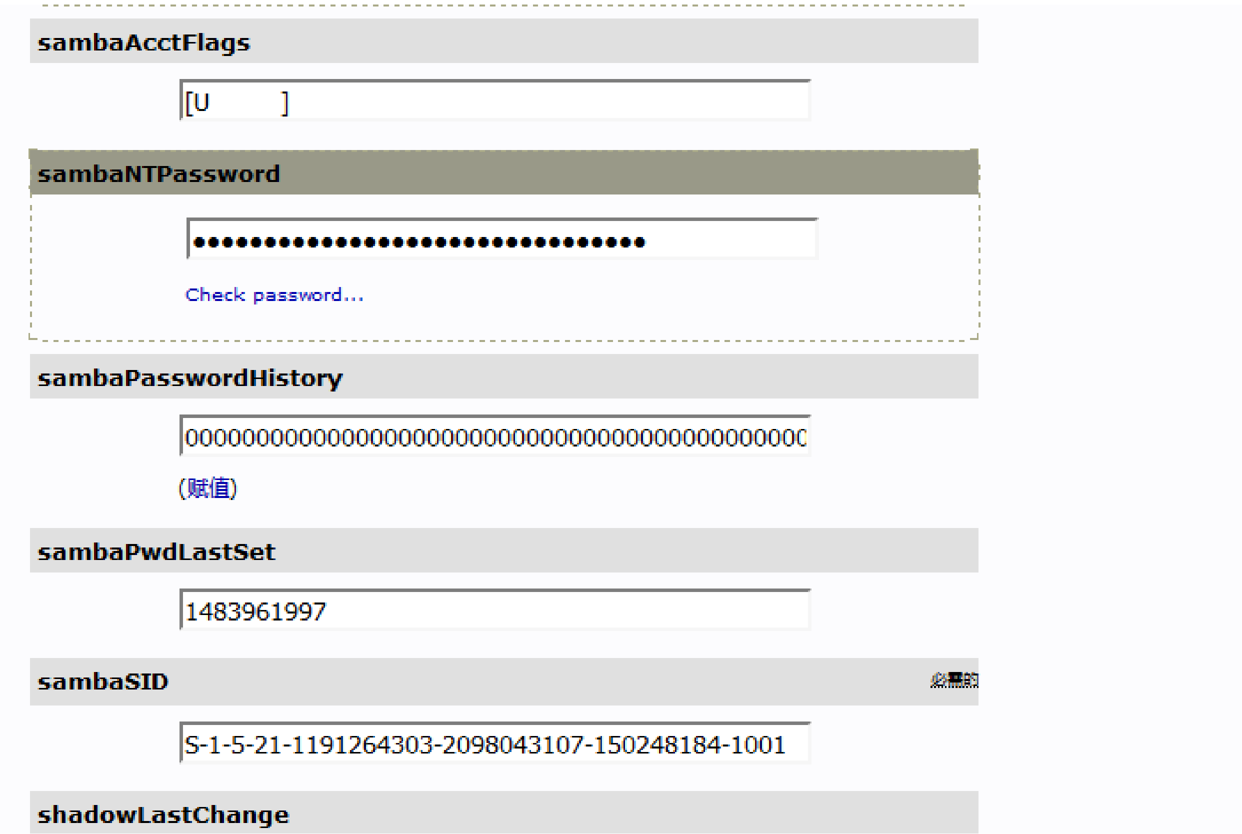
```
/etc/init.d/nmb restart
```

8： Samba开通之后，可以看到这里的开关也打开了



○ Samba: Domain
○ Samba: Group Mapping
○ Samba: Machine
⊗ Sendmail: Alias
⊗ Sendmail: Cluster
⊗ Sendmail: Domain
⊗ Sendmail: Relays
⊗ Sendmail: Virtual Domain

9：测试
先把系统用户test1用smbpasswd -a test1 加到Samba的用户下，就可以看到：
test1用户下多了Samba的特性，原来是没有的



**sambaAcctFlags**

[U          ]

**sambaNTPassword**

●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

Check password...

**sambaPasswordHistory**

0000000000000000000000000000000000000000000

(赋值)

**sambaPwdLastSet**

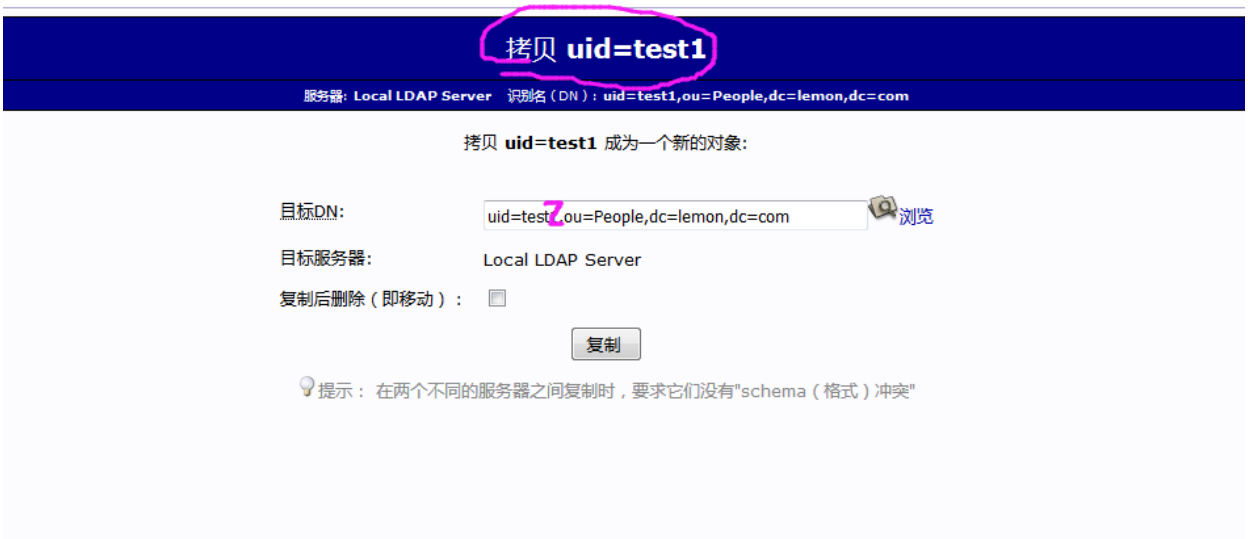
1483961997

**sambaSID** 必需的

S-1-5-21-1191264303-2098043107-150248184-1001

**shadowLastChange**

然后基于test1，在PhpLdapAdmin添加test2用户，不用smbpasswd，就只是OpenLDAP用户，复制的时候一定要重新改一下这里的密码，要不然登不进，



拷贝 uid=test1

服务器: Local LDAP Server　识别名（DN）: uid=test1,ou=People,dc=lemon,dc=com

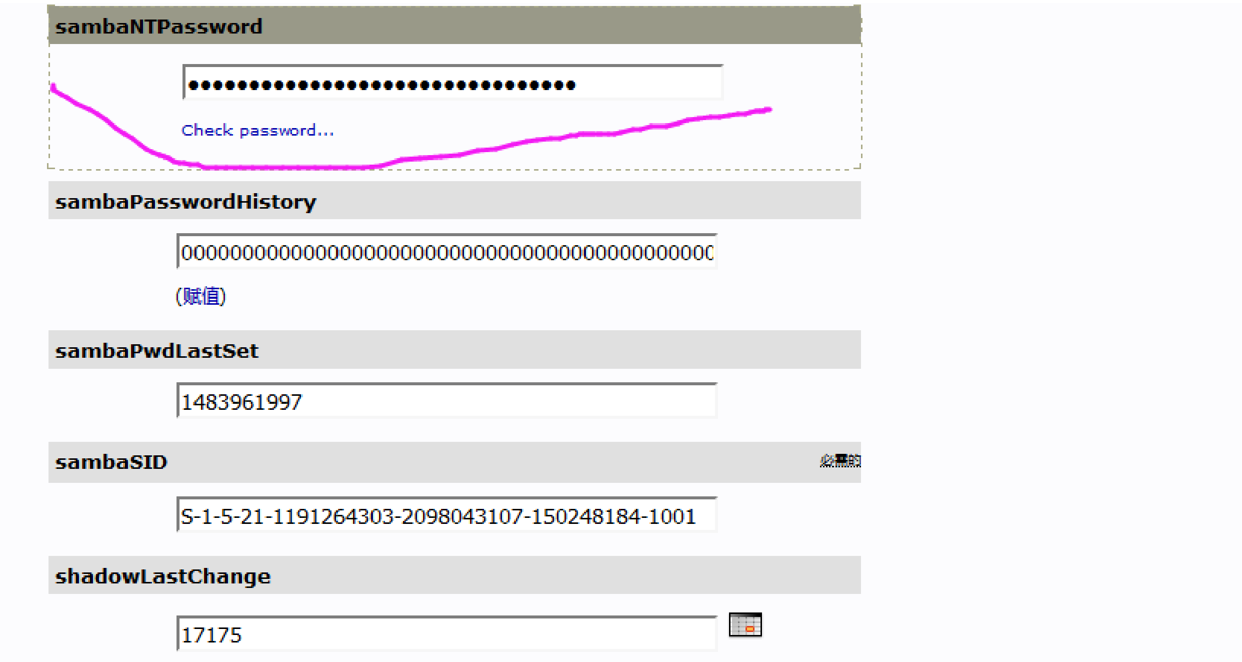
拷贝 uid=test1 成为一个新的对象:

目标DN: uid=testZ,ou=People,dc=lemon,dc=com

目标服务器: Local LDAP Server

复制后删除（即移动）: □

提示： 在两个不同的服务器之间复制时，要求它们没有"schema（格式）冲突"



sambaNTPassword

••••••••••••••••••••••••••••••••

sambaPasswordHistory

0000000000000000000000000000000000000000000

sambaPwdLastSet

1483961997

sambaSID 必要的

S-1-5-21-1191264303-2098043107-150248184-1001

shadowLastChange

17175

然后，就可以用windos去访问了，这里有一个概念就是**OpenLDAP添加了的用户，不要再用smbpasswd去添加了，可以直接登录Samba**

## 十：OpenLDAP的主从

1：做主从和双主的时候，一定要确认安装了 **compat-openldap这个包**

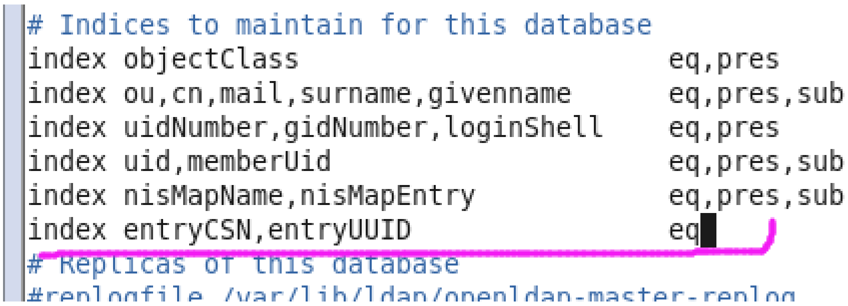
2：**在主上的配置文件　10.0.0.138**：

备份原来的配置文件：cp /etc/openldap/slapd.conf /etc/openldap/slapd.bak

先停掉服务 /etc/init.d/slapd stop

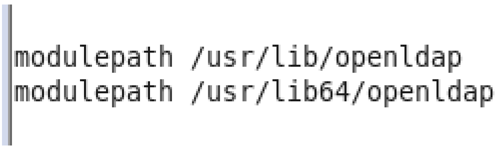
vim /etc/openldap/slapd.conf 修改配置文件

添加　　index entryCSN,entryUUID　　　　eq

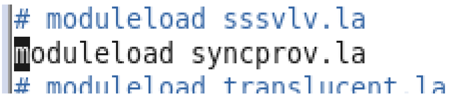


```
# Indices to maintain for this database
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub
index entryCSN,entryUUID                eq
# Replicas of this database
#replogfile /var/lib/ldap/openldap-master-replog
```

这里的注释去掉：



```
modulepath /usr/lib/openldap
modulepath /usr/lib64/openldap
```



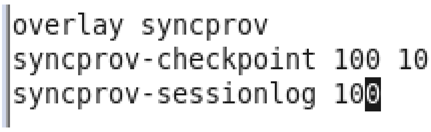
```
# moduleload sssvlv.la
moduleload syncprov.la
# moduleload translucent.la
```

在文件的最后添加：

**overlay syncprov**　　　　　　**后端工作再overlay模式**

**syncprov-checkpoint 100 10**　**当满足修改100个条目或者10分钟的条件时主动以推的方式执行**

**syncprov-sessionlog 100**　　　**会话日志条目的最大数量**



```
overlay syncprov
syncprov-checkpoint 100 10
syncprov-sessionlog 100
```

然后重新生成配置文件的数据文件：

```
rm -rf /etc/openldap/slapd.d/*
slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d/
chown -R ldap.ldap /etc/openldap/slapd.conf
chown -R ldap.ldap /etc/openldap/slapd.d
/etc/init.d/slapd restart
```

3：**导出主的数据文件 ldapsearch -x -b 'dc=lemon,dc=com' > root.ldif，拷贝到从上scp　scp root.ldif 10.0.0.140:~/**

4：**把主的配置文件slapd.conf 拷贝到从10.0.0.140上 用scp /etc/openldap/slapd.conf 10.0.0.140:~/**

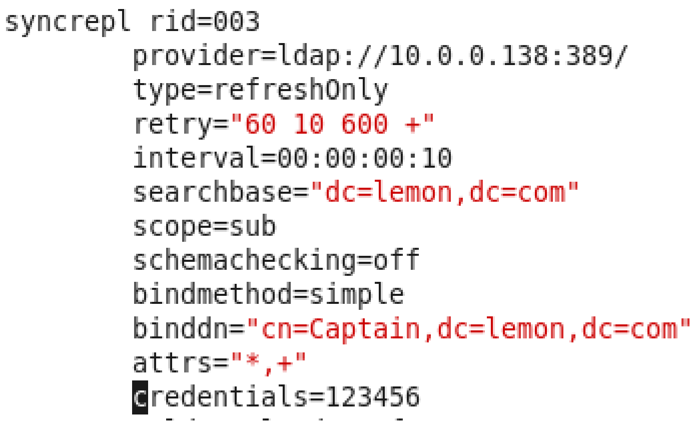
5：从上从主上拷贝了配置文件，

**去掉**：

overlay syncprov
syncprov-checkpoint 100 10

syncprov-sessionlog 100

**然后再加上**



```
syncrepl rid=003
        provider=ldap://10.0.0.138:389/
        type=refreshOnly
        retry="60 10 600 +"
        interval=00:00:00:10
        searchbase="dc=lemon,dc=com"
        scope=sub
        schemachecking=off
        bindmethod=simple
        binddn="cn=Captain,dc=lemon,dc=com"
        attrs="*,+"
        credentials=123456
```

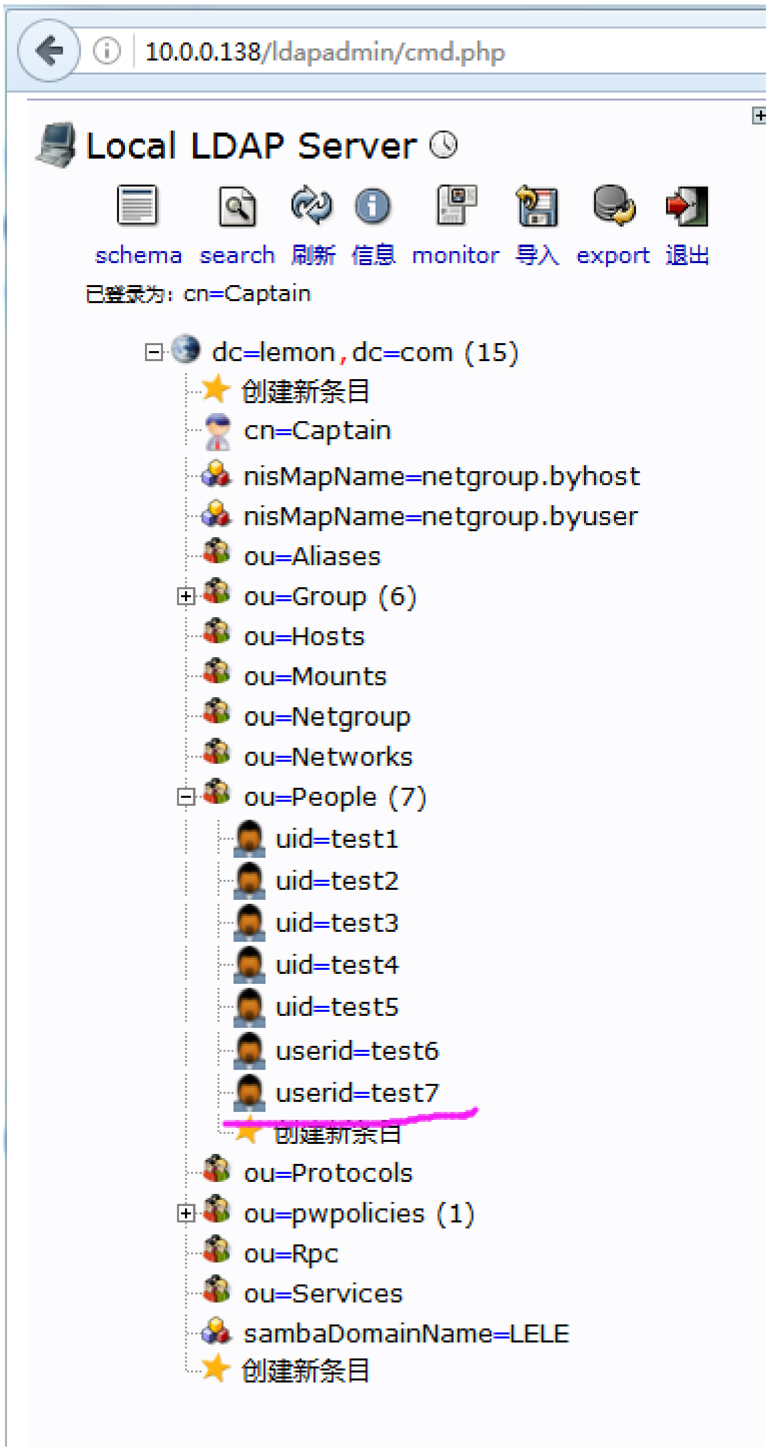
**syncrepl rid=003**
**provider=ldap://10.0.0.138:389/**
**type=refreshOnly**
**retry="60 10 600 +"**　　　**尝试时间**
**interval=00:00:00:10**　　　**设置同步更新时间（日：时：分：秒）**
**searchbase="dc=lemon,dc=com"**
**scope=sub**　　　**匹配根域所有条目**
**bindmethod=simple**　　　**同步验证模式为简单模式（即明文）**
**binddn="cn=Captain,dc=lemon,dc=com"**　　　**使用Captain用户读取目录树信息**
**attrs="*,+"**　　　**同步所有属性信息**
**credentials=123456**　　　**管理员密码**

重新生成数据配置文件

```
rm -rf /etc/openldap/slapd.d/*
slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d/
chown -R ldap.ldap /etc/openldap/slapd.conf
chown -R ldap.ldap /etc/openldap/slapd.d
/etc/init.d/slapd restart
```

6：测试

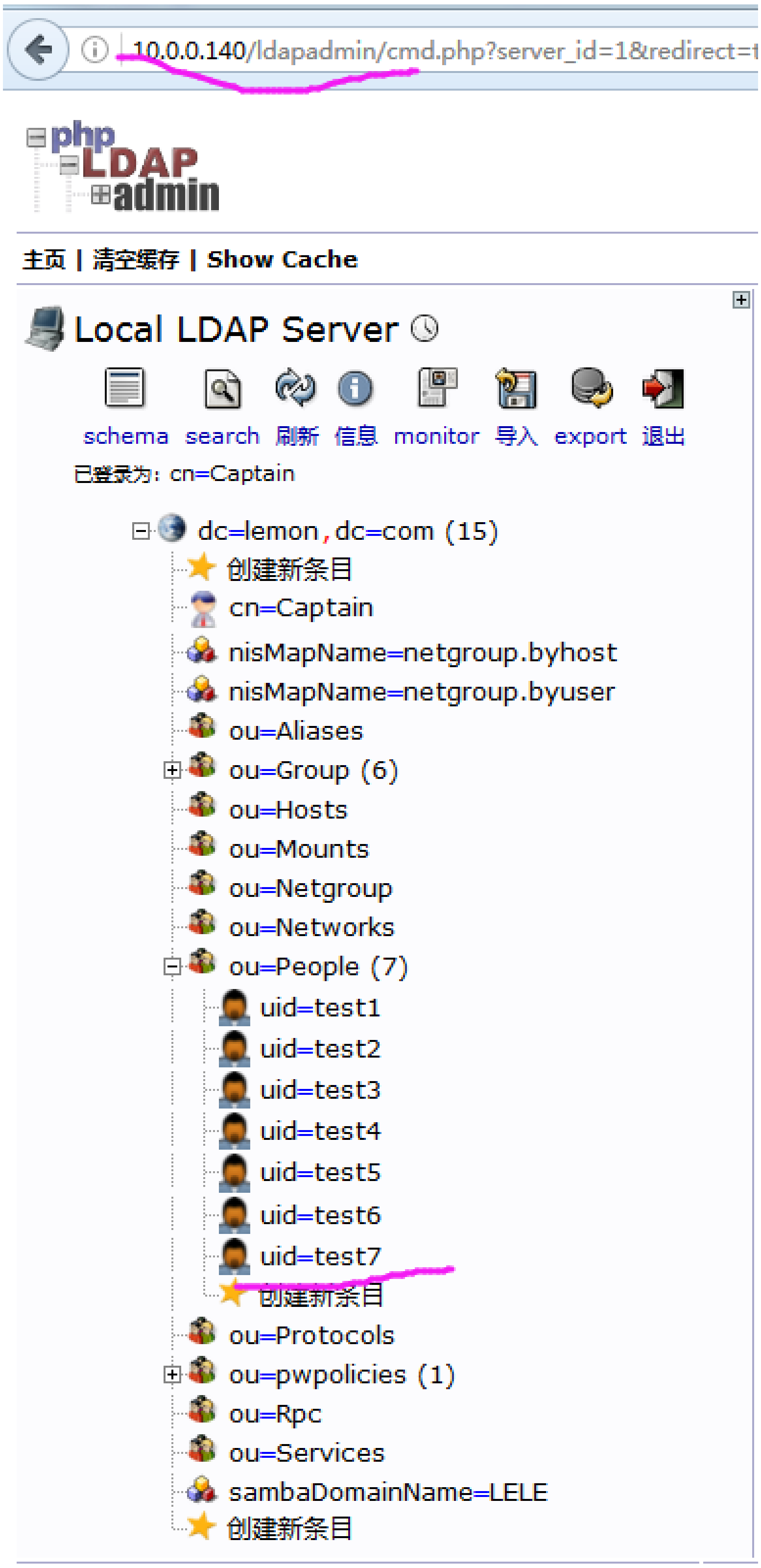
在主的10.0.0.138上添加一个test7的用户，在从上刷新一下，是同步到的



Local LDAP Server

已登录为：cn=Captain

```
dc=lemon,dc=com (15)
    创建新条目
    cn=Captain
    nisMapName=netgroup.byhost
    nisMapName=netgroup.byuser
    ou=Aliases
    ou=Group (6)
    ou=Hosts
    ou=Mounts
    ou=Netgroup
    ou=Networks
    ou=People (7)
        uid=test1
        uid=test2
        uid=test3
        uid=test4
        uid=test5
        userid=test6
        userid=test7
        创建新条目
    ou=Protocols
    ou=pwpolicies (1)
    ou=Rpc
    ou=Services
    sambaDomainName=LELE
    创建新条目
```



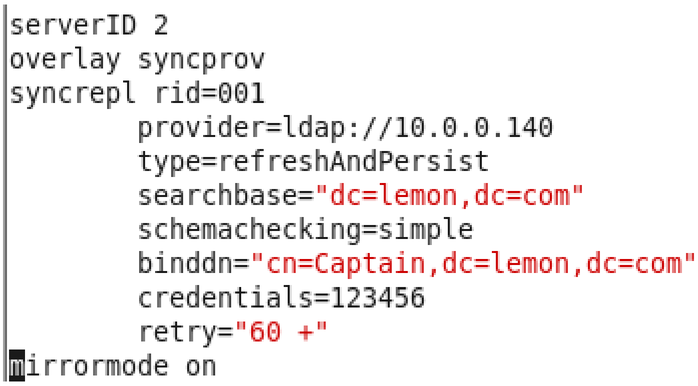
10.0.0.140/ldapadmin/cmd.php?server_id=1&redirect=t

已登录为：cn=Captain

```
dc=lemon,dc=com (15)
  创建新条目
  cn=Captain
  nisMapName=netgroup.byhost
  nisMapName=netgroup.byuser
  ou=Aliases
  ou=Group (6)
  ou=Hosts
  ou=Mounts
  ou=Netgroup
  ou=Networks
  ou=People (7)
    uid=test1
    uid=test2
    uid=test3
    uid=test4
    uid=test5
    uid=test6
    uid=test7
    创建新条目
  ou=Protocols
  ou=pwpolicies (1)
  ou=Rpc
  ou=Services
  sambaDomainName=LELE
  创建新条目
```

## 十一：OpenLDAP的双主

在主从的基础上，修改配置，**这是主的**

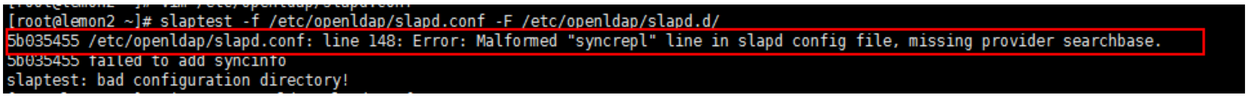


```
serverID 2
overlay syncprov
syncrepl rid=001
        provider=ldap://10.0.0.140
        type=refreshAndPersist
        searchbase="dc=lemon,dc=com"
        schemachecking=simple
        binddn="cn=Captain,dc=lemon,dc=com"
        credentials=123456
        retry="60 +"
mirrormode on
```

```
serverID 2
overlay syncprov
syncrepl rid=001
```

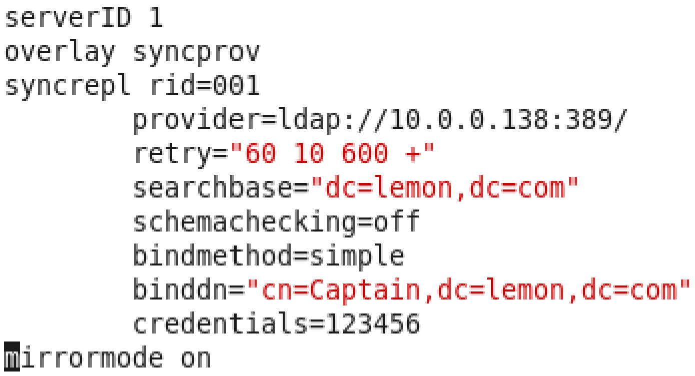
**（这里的格式一定要注意，中间这一段要用Tab键Tab一下，如果不的话会报错如下）**

```
    provider=ldap://10.0.0.140
    type=refreshAndPersist
    searchbase="dc=lemon,dc=com"
    schemachecking=simple
    binddn="cn=Captain,dc=lemon,dc=com"
    credentials=123456
    retry="60 +"
mirrormode on
```



```
[root@lemon2 ~]# vim /etc/openldap/slapd.conf
[root@lemon2 ~]# slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d/
5b035455 /etc/openldap/slapd.conf: line 148: Error: Malformed "syncrepl" line in slapd config file, missing provider searchbase.
5b035455 failed to add syncinfo
slaptest: bad configuration directory!
```

**这是从的**：



```
serverID 1
overlay syncprov
syncrepl rid=001
        provider=ldap://10.0.0.138:389/
        retry="60 10 600 +"
        searchbase="dc=lemon,dc=com"
        schemachecking=off
        bindmethod=simple
        binddn="cn=Captain,dc=lemon,dc=com"
        credentials=123456
mirrormode on
```

```
serverID 1
overlay syncprov
syncrepl rid=001
```

**（这里的格式一定要注意，中间这一段要用Tab键Tab一下）**

```
    provider=ldap://10.0.0.138:389/
    retry="60 10 600 +"
    searchbase="dc=lemon,dc=com"
    schemachecking=off
    bindmethod=simple
    binddn="cn=Captain,dc=lemon,dc=com"
    credentials=123456
mirrormode on
```

**测试**：在两台机上分别新建一个用户，看是否在对方能刷新到，主从与双主都只是备份的关系，若一台挂了，立即切换到另一台，则需做高可用和负载均衡

« 上一篇：OpenLDAP—登录系统就修改密码
» 下一篇：记录第一次服务器出现问题的过程以及心情

posted on 2017-01-09 23:19 Captain_Li 阅读(38089) 评论(9) 编辑 收藏

## 评论

**#1楼 2018-05-09 22:05 艾小小雨**

博主你好，我使用Centos7配置

1.OpenLDAP服务器的搭建中的徘徊

一直在slapd.conf配置文件中出错，有正常slapd.conf文件吗?

Job for slapd.service failed because the control process exited with error code. See "systemctl status slapd.service" and "journalctl -xe" for details.

支持(1)反对(0)

**#2楼[楼主] 2018-05-24 15:02 Captain_Li**

@ 艾小小雨

你好，根据安装好的配置文件，然后根据博文配置就行，报什么错可以贴出来看看

支持(0)反对(0)

**#3楼 2018-06-26 16:50 活蹦乱跳的鱼**

楼主您好， 我这没有slapd.conf.obsolete文件

支持(0)反对(0)

**#4楼[楼主] 2018-06-26 17:29 Captain_Li**

@ 活蹦乱跳的鱼

你的是怎么安装的

支持(0)反对(0)

**#5楼 2018-07-05 10:12 LittleLawson**

同上啊，哪有/etc/openldap/slapd.conf这个文件啊。安装一个ldap简直是够了。凸(艹皿艹 )

支持(0)反对(0)

**#6楼 2018-07-05 14:44 LittleLawson**

@ 艾小小雨

我今天也是用centos 7装，结果报错。一直无法启动。还有那个slap.conf文件，根本没有！简直是气死人啊

支持(0)反对(0)

**#7楼[楼主] 2018-07-05 21:22 Captain_Li**

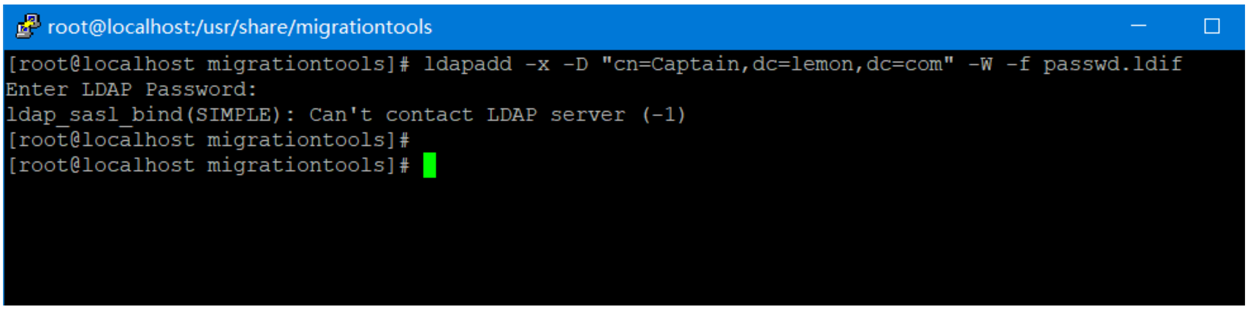
@ LittleLawson

淡定 淡定 淡定 有一种办法叫在centos6 上安装，然后把配置文件拷贝过去

支持(0)反对(0)

**#8楼 2018-07-31 16:04 唐筱蕊**

你好楼主 那个想问下为什么在导入用户的时候老是出现下面的错误啊，小白很头疼



```
[root@localhost migrationtools]# ldapadd -x -D "cn=Captain,dc=lemon,dc=com" -W -f passwd.ldif
Enter LDAP Password:
ldap_sasl_bind(SIMPLE): Can't contact LDAP server (-1)
[root@localhost migrationtools]#
[root@localhost migrationtools]#
```

支持(0)反对(0)

**#9楼 2018-11-15 16:05 lareen~**

博主你好，我在搭建的时候遇到一个很奇怪的问题。

为了让用户可以自己修改密码，在slapd.conf里面，database config上面写入

by self write

by anonymous auth

by dn.base="cn=Manager,dc=test,dc=com" write

by * none

access to *

by self write

by dn.base="cn=Manager,dc=test,dc=com" write

重建数据库后，用户无法SSH登录，提示Permission denied, please try again

把增加的配置注释掉，又可以登录了。。请教这是什么原因?