ldap实现Linux登录账号统一管理

软件安装

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

配置openLDAP-client

```
cp /etc/nsswitch.conf /etc/nsswitch.conf.old
sed -i '/^passwd:.*$/s//&  ldap/g' /etc/nsswitch.conf
sed -i '/^shadow:.*$/s//&  ldap/g' /etc/nsswitch.conf

cp /etc/openldap/ldap.conf /etc/openldap/ldap.conf.old
cat >> /etc/openldap/ldap.conf <<EOF
host 10.0.19.49
BASE dc=baofoo,dc=com
URI ldap://10.0.19.49
ssl off
EOF
```

启用LDAP身份验证机制

```
cp /etc/sysconfig/authconfig /etc/sysconfig/authconfig.old

cat > /etc/sysconfig/authconfig <<EOF
IPADOMAINJOINED=no
USEMKHOMEDIR=no
```

```
USEPAMACCESS=no
CACHECREDENTIALS=yes
USESSSDAUTH=no
USESHADOW=yes
USEWINBIND=no
USEDB=no
USEFPRINTD=yes
FORCESMARTCARD=no
PASSWDALGORITHM=sha512
USELDAPAUTH=yes
USEPASSWDQC=no
IPAV2NONTP=no
USELOCAUTHORIZE=yes
USECRACKLIB=yes
USEIPAV2=no
USEWINBINDAUTH=no
USESMARTCARD=no
USELDAP=yes
USENIS=no
USEKERBEROS=no
USESYSNETAUTH=no
USESSSD=no
USEHESIOD=no
USEMD5=yes
FORCELEGACY=no
EOF
```

pam 认证

```
cp /etc/pam_ldap.conf /etc/pam_ldap.conf.old
```

```
sed -i 's/^host/#&/g' /etc/pam_ldap.conf
sed -i 's/^base/#&/g' /etc/pam_ldap.conf
cat >> /etc/pam_ldap.conf<<EOF
host=10.0.19.49
base dc=baofoo,dc=com
uri ldap://10.0.19.49
EOF
```

nslcd 服务

```
cat >> /etc/nslcd.conf <<EOF
uri ldap://10.0.19.49
base dc=baofoo,dc=com
EOF
```

编辑系统认证文件，保证使用LDAP来认证

```
cp /etc/pam.d/system-auth /etc/pam.d/system-auth.old
cat > /etc/pam.d/system-auth <<EOF
#%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_ldap.so use_first_pass
auth required pam_deny.so
```

```
account required pam_unix.so
account sufficient pam_localuser.so
account sufficient pam_succeed_if.so uid < 500 quiet
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 sha512 shadow nullok
try_first_pass 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_ldap.so
session required pam_mkhomedir.so skel=/etc/skel/ umask=0022
EOF
```

注意　我把它当做 登陆系统的开关。如果只做权限认证不让他登陆系统，这里就不用配置

vi /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                required            pam_faildelay.so
delay=2000000
auth                [default=1 ignore=ignore success=ok]
pam_succeed_if.so uid >= 1000 quiet
```

```
auth                [default=1 ignore=ignore success=ok]
pam_localuser.so
auth                sufficient        pam_unix.so nullok
try_first_pass
auth                requisite          pam_succeed_if.so uid >= 1000
quiet_success
auth                sufficient        pam_ldap.so forward_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 < 1000
quiet
account          [default=bad success=ok user_unknown=ignore]
pam_ldap.so
account          required            pam_permit.so
password        requisite          pam_pwquality.so try_first_pass
local_users_only retry=3 authtok_type=
password        sufficient        pam_unix.so md5 shadow nullok
try_first_pass 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_systemd.so
session          [success=1 default=ignore] pam_succeed_if.so
service in crond quiet use_uid
session          required            pam_unix.so
session          optional            pam_ldap.so
```

重启nslcd服务

```
systemctl restart  nslcd
systemctl enable  nslcd  //设置开机启动
systemctl list-unit-files  nslcd.service //查看开机启动状态
```