# openldap客户端配置

#### /etc/openldap/ldap.conf

BASE dc=jops,dc=cnT  
LS\_CACERTDIR /etc/openldap/cacerts  
TLS\_CACERT /etc/openldap/cacerts/ca.crt  
TLS\_REQCERT never  
URI ldap://192.168.100.151 ldap://192.168.100.152

#### /etc/pam\_ldap.conf

#host 127.0.0.1  
base dc=jops,dc=cn  
uri ldaps://ldap1.jops.cn ldaps://ldap2.jops.cn  
ssl start\_tls  
tls\_cacertdir /etc/openldap/cacerts  
tls\_cacertfile /etc/openldap/cacerts/root.crt  
tls\_reqcert never  
bind\_policy soft  
pam\_password md5

#### /etc/sysconfig/authconfig

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

#### /etc/nslcd.conf

uid nslcd  
gid ldap  
uri ldaps://ldap1.jops.cn ldaps://ldap2.jops.cn  
base dc=jops,dc=cn  
ssl start\_tls  
tls\_cacertdir /etc/openldap/cacerts  
tls\_cacertfile /etc/openldap/cacerts/root.crt  
tls\_reqcert never  
  
# getent passwd\shadow\group (查看是否可以显示AD信息，可以才算正常)

#### /etc/nsswitch.conf

passwd: files sss  
shadow: files sss  
group: files sss  
hosts: files dns  
bootparams: nisplus [NOTFOUND=return] files  
ethers: files  
netmasks: files  
networks: files  
protocols: files  
rpc: files  
services: files sss  
netgroup: files sss  
publickey: nisplus  
automount: files sss  
aliases: files nisplus  
sudoers: files ldap

#### /etc/sssd/sssd.conf

ldap\_uri = ldaps://master.local,ldaps://slave.local

[domain/default]  
  
autofs\_provider = ldap  
cache\_credentials = True  
ldap\_search\_base = dc=jops,dc=cn  
id\_provider = ldap  
auth\_provider = ldap  
chpass\_provider = ldap  
ldap\_uri = ldaps://ldap1.jops.cn,ldaps://ldap2.jops.cn  
ldap\_id\_use\_start\_tls = True  
ldap\_tls\_cacertdir = /etc/openldap/cacerts  
ldap\_default\_bind\_dn = cn=readuser,ou=readonly,ou=Manager,dc=jops,dc=cn  
ldap\_default\_authtok\_type = password  
ldap\_default\_authtok = 123456  
override\_homedir = /home/%u  
default\_shell = /bin/bash  
[sssd]  
services = nss, pam, autofs  
  
domains = default  
[nss]  
homedir\_substring = /home  
  
[pam]  
  
[sudo]  
  
[autofs]  
  
[ssh]  
  
[pac]  
  
[ifp]  
  
[secrets]  
  
[session\_recording]

ldap\_default\_bind\_dn = cn=readuser,ou=readonly,ou=Manager,dc=jops,dc=cn

ldap\_default\_authtok\_type = password

ldap\_default\_authtok = 123456

此用户为【OpenLDAP 完整部署(含高可用)-12.1.8 LDAP用户权限配置】创建或者

[基于SSSD同步LDAP账号](https://aws.amazon.com/cn/blogs/china/amazon-emr-authentication-scheme-based-on-openldap-and-kerberos-ii-synchronize-ldap-accounts-based-on-sssd/)

#### /etc/sudo-ldap.conf

tls\_cacertfile /etc/openldap/cacerts/root.crt  
binddn cn=readuser,ou=readonly,ou=Manager,dc=jops,dc=cn  
bindpw 123456  
sudoers\_base cn=sudo\_ops\_role,ou=SUDOers,dc=jops,dc=cn  
uri ldaps://ldap1.jops.cn ldaps://ldap2.jops.cn  
TLS\_CHECKPEER no

#### 参考文档

[OpenLDAP+SSL+SSSD 实现 Linux 登录集中认证](https://my.oschina.net/u/3021599/blog/3210170)

<https://wiki.shileizcc.com/confluence/pages/viewpage.action?pageId=40566794>

[LDAP客户端认证配置与应用接入](https://cloud.tencent.com/developer/article/2129545)