openldap设置用户修改密码权限 密码过期

hiveServer2 连接ldap报下面错误：

javax.security.sasl.SaslException: Error validating the login [Caused by javax.security.sasl.AuthenticationException: LDAP Authentication failed for user [Caused by javax.naming.AuthenticationException: [LDAP: error code 49 - Invalid Credentials]]]

解决方法修改ldap：

sldap.conf

```
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
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
# Allow LDAPv2 client connections.  This is NOT the default.
```

```
allow bind_v2
# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#referral       ldap://root.openldap.org
pidfile               /var/run/openldap/slapd.pid
argsfile       /var/run/openldap/slapd.args
# Load dynamic backend modules
# - modulepath is architecture dependent value (32/64-bit system)
# - back_sql.la overlay requires openldap-server-sql package
# - dyngroup.la and dynlist.la cannot be used at the same time
# modulepath /usr/lib/openldap
modulepath /usr/lib64/openldap
# moduleload accesslog.la
# moduleload auditlog.la
# moduleload back_sql.la
# moduleload chain.la
# moduleload collect.la
# moduleload constraint.la
# moduleload dds.la
# moduleload deref.la
# moduleload dyngroup.la
# moduleload dynlist.la
# moduleload memberof.la
# moduleload pbind.la
# moduleload pcache.la
moduleload ppolicy.la
# moduleload refint.la
# moduleload retcode.la
# moduleload rwm.la
# moduleload seqmod.la
# moduleload smbk5pwd.la
# moduleload sssvlv.la
# moduleload syncprov.la
# moduleload translucent.la
# moduleload unique.la
# moduleload valsort.la
# The next three lines allow use of TLS for encrypting connections
using a
# dummy test certificate which you can generate by running
# /usr/libexec/openldap/generate-server-cert.sh. Your client software
may balk
# at self-signed certificates, however.
TLSCACertificatePath /etc/openldap/certs
TLSCertificateFile "\"OpenLDAP Server\""
TLSCertificateKeyFile /etc/openldap/certs/password
# Sample security restrictions
#       Require integrity protection (prevent hijacking)
#       Require 112-bit (3DES or better) encryption for updates
#       Require 63-bit encryption for simple bind
# security ssf=1 update_ssf=112 simple_bind=64
# Sample access control policy:
#       Root DSE: allow anyone to read it
#       Subschema (sub)entry DSE: allow anyone to read it
#       Other DSEs:
#               Allow self write access
#               Allow authenticated users read access
#               Allow anonymous users to authenticate
#       Directives needed to implement policy:
# access to dn.base="" by * read
# access to dn.base="cn=Subschema" by * read
#access to   attrs=userPassword
#       by dn="cn=Manager,dc=qlbigdata,dc=com" write
#       by self write
#       by anonymous auth
#       by * read
# 这里特别注意，不这样设置 HiveServer2 会报错
access to *
       by self write
       by users read
       by anonymous auth
#
# if no access controls are present, the default policy
# allows anyone and everyone to read anything but restricts
# updates to rootdn.   (e.g., "access to * by * read")
#
# rootdn can always read and write EVERYTHING!
# 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=Manager,dc=qlbigdata,dc=com" read
               by * none
#######################################################################
# database definitions
#######################################################################
database       bdb
suffix                 "dc=qlbigdata,dc=com"
```

```
checkpoint       1024 15
rootdn               ″cn=Manager,dc=qlbigdata,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}tgAwb0e3T9hwV7x/2oKZCJnJshjc7cuf
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory       /var/lib/ldap
# 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
# Replicas of this database
#replogfile /var/lib/ldap/openldap-master-replog
#replica host=ldap-1.example.com:389 starttls=critical
#         bindmethod=sasl saslmech=GSSAPI
#         authcId=host/ldap-master.example.com@EXAMPLE.COM
overlay   ppolicy
ppolicy_default ″cn=Captain,ou=pwpolicies,dc=qlbigdata,dc=com″
#ppolicy_use_lockout
#ppolicy_hash_text
loglevel 256
```

ppolicy.ldif

```
# Default Policies
dn: cn=Captain,ou=pwpolicies,dc=qlbigdata,dc=com
#sn: pwp
cn: Captain
objectClass: top
objectClass: device
objectClass: pwdPolicy
pwdAllowUserChange: TRUE
pwdAttribute: userPassword
#通过pwdCheckModule检查密码质量, 0为不控制，由SSO的认证模块自己控制
pwdCheckQuality: 0
#密码失效提前7天警告
pwdExpireWarning: 300
#密码失败次数复位时间，1天
pwdFailureCountInterval: 0
#密码过期不允许登录
pwdGraceAuthNLimit: 0
#保存密码历史3次，新密码不能与之相同
pwdInHistory: 3
#超过最多失败次数账号被锁定
pwdLockout: TRUE
#锁定后不能自动解锁，必须由管理员解锁
pwdLockoutDuration: 0
#密码有效期3个月
pwdMaxAge: 60
#密码最大失败次数，超过后被账号锁定
pwdMaxFailure: 10
pwdMinAge: 0
#密码最小长度
pwdMinLength: 8
pwdMustChange: FALSE
pwdSafeModify: FALSE
```

```
pwdChangedTime: last-password-change-time
#密码必须由管理员重置
pwdReset: FALSE
```

ldap中增加一个新的组

```
dn: ou=pwpolicies,dc=qlbigdata,dc=com
ou: pwpolicies
objectClass: top
objectClass: organizationalUnit
description: policy
```

参考： http://luvjennifer-tw-blog.logdown.com/posts/2015/03/31/ldap-password-control-ppolicy-overlay