openldap安装，hue、hive、impala集成ldap

参考：

https://www.cnblogs.com/bugsbunny/p/6862906.html

、概要

1.1 环境信息

- hadoop：cdh5.10
- os：centos6.7
- user：root
- hive、impala已集成sentry

1.2 访问控制权限

这里通过使用openldap来控制hive、impala的访问权限，即通过用户名、密码来进行访问。而hive、impala内部则已集成了sentry来控制更为细粒度的权限访问。

2、openldap

2.1 安装

```
# yum install -y openldap-*
```

2.2 配置

- 拷贝ldap配置文件到ldap目录

```
# cp /usr/share/openldap-servers/slapd.conf.obsolete
# /etc/openldap/slapd.conf
```

- 创建ldap管理员密码

```
# slappasswd
New password:
Re-enter new password:
{SSHA}k8dOPcF3Y1VcI/ixMiss8e5ZmIkFC8dl
```

输入保存管理员密码，返回的是加密后的一串密文

- 编辑配置文件

注：这里组织的域为 qlbigdata.com

```
# vim /etc/openldap/slapd.conf 修改对应如下内容
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      {SSHA}k8dOPcF3Y1VcI/ixMiss8e5ZmIkFC8dl #加密后的管理员密码
#rootpw     {SSHA}k8dOPcF3Y1VcI/ixMiss8e5ZmIkFC8dl
```

- 拷贝DB_CONFIG文件到指定目录

```
cp /usr/share/openldap-servers/DB_CONFIG.example  /var/lib/ldap/DB_CONFIG
```

- 删除默认/etc/openldap/slapd.d下面的所有内容

```
rm -rf /etc/openldap/slapd.d/*
```

- 赋予配置目录相应权限

```
# chown -R ldap:ldap /var/lib/ldap
# chown -R ldap:ldap /etc/openldap/
# service slapd start
```

- 生成配置文件并赋值

```
# slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d
config file testing succeeded
# chown -R ldap:ldap /etc/openldap/slapd.d/*
# service slapd restart
```

2.3 migrationtools

- 安装migrationtools

```
# yum install -y migrationtools
```

- 修改migrate_common.ph文件

```
# vim /usr/share/migrationtools/migrate_common.ph
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = "qlbigdata.com";

# Default base
$DEFAULT_BASE = "dc=qlbigdata,dc=com";
```

- 利用pl脚本将/etc/passwd 和/etc/group生成LDAP能读懂的文件格式

```
# 这里导入一个etl用户来测试
# cat /etc/passwd | grep etl > /tmp/passwd
# cat /etc/group | grep etl > /tmp/group

# /usr/share/migrationtools/migrate_base.pl > /tmp/base.ldif
# /usr/share/migrationtools/migrate_passwd.pl  /tmp/passwd > /tmp/passwd.ldif
# /usr/share/migrationtools/migrate_group.pl  /tmp/group > /tmp/group.ldif
```

- 将文件导入到LDAP

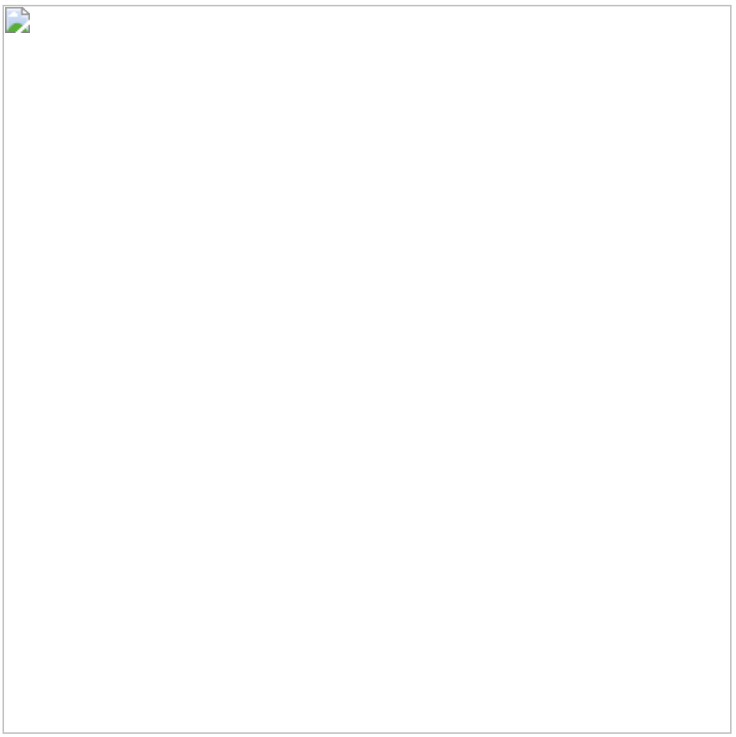
```
# ldapadd -x -D "cn=Manager,dc=qlbigdata,dc=com" -W -f /tmp/base.ldif
# ldapadd -x -D "cn=Manager,dc=qlbigdata,dc=com" -W -f /tmp/passwd.ldif
# ldapadd -x -D "cn=Manager,dc=qlbigdata,dc=com" -W -f /tmp/group.ldif
```

2.4 ldapadmin

ldapadmin，它提供一个简单的、支持多语言多环境的LDAP管理功能。

下载地址：http://www.ldapadmin.org/download/index.html

下载exe文件就可以了



可以看到刚刚测试导入的用户etl。

3、hive集成ldap

3.1 修改配置

在/etc/hive/conf/hive-site.xml中添加

```
    <property>
        <name>hive.server2.authentication</name>
        <value>LDAP</value>
    </property>

    <property>
        <name>hive.server2.authentication.ldap.url</name>
        <value>ldap://ip</value>
    </property>

    <property>
        <name>hive.server2.authentication.ldap.baseDN</name>
        <value>ou=People,dc=qlbigdata,dc=com</value>
    </property>
```

添加完后重启hive-server2.

3.2 验证

此时通过beeline连接，需要ldap中对应的用户名密码才能连接成功。

4、impala集成ldap

4.1 修改配置

修改/etc/default/impala文件，在IMPALA_SERVER_ARGS中添加：

-enable_ldap_auth=true

-ldap_tls=false

-ldap_passwords_in_clear_ok=true

-ldap_uri=ldap://idap_ip

-ldap_baseDN=ou=People,dc=qlbigdata,dc=com

添加完后重启impala。

4.2 验证

验证命令：

impala-shell -i impalad-server -u etl -l --auth_creds_ok_in_clear

-i 集群中任意一台impalad服务器都可以

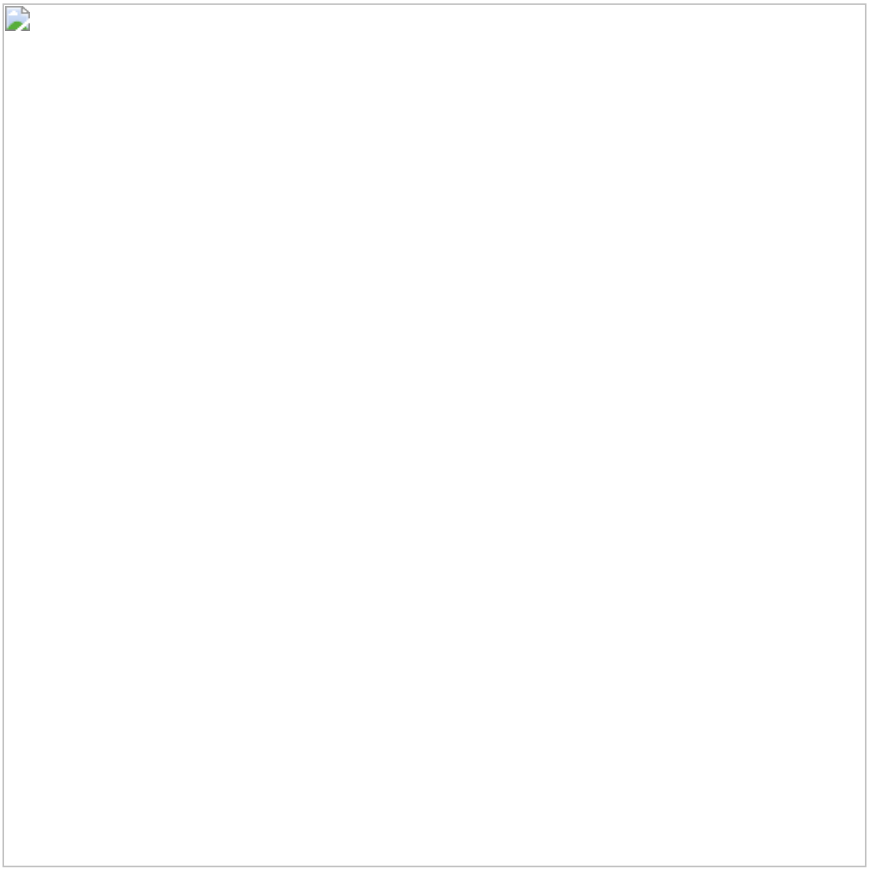
-u 登录用户

-l 使用ldap

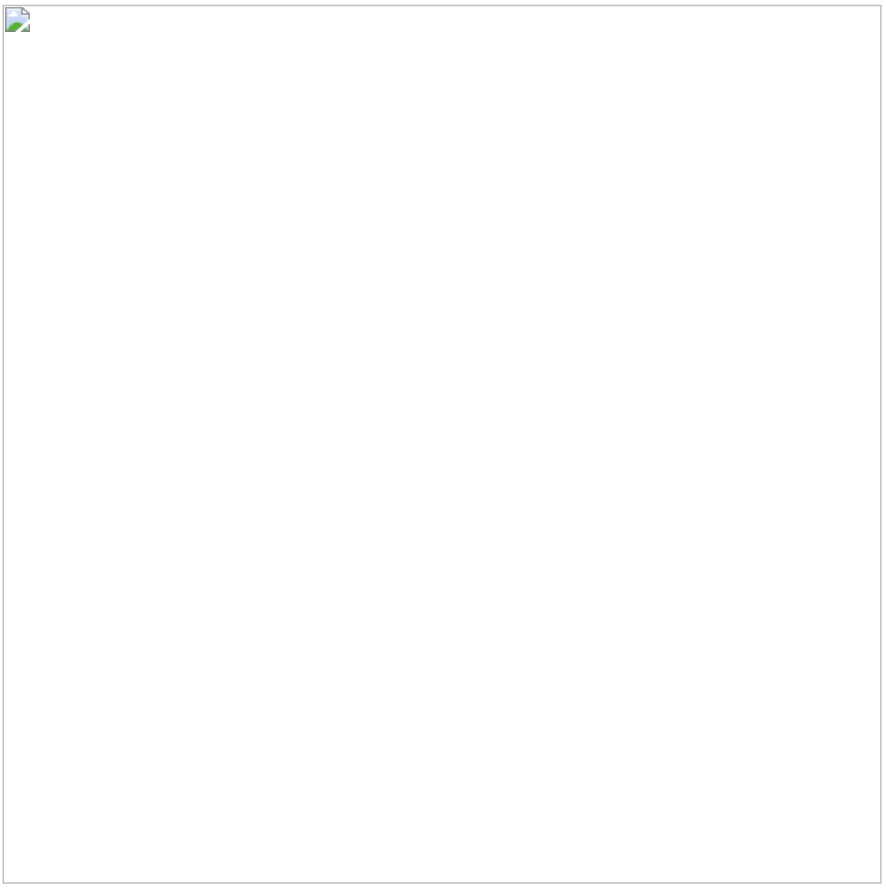
--auth_creds_ok_in_clear 由于没有使用ssl，需要添加该参数。

5、hue集成ldap

5.1 修改配置



下面是同步组的设置：



注意：设置不对不能同步组

参考官

网：　　https://www.cloudera.com/documentation/enterprise/latest/topics/hue_sec_ldap_auth.html