yum -y install krb5-server krb5-libs krb5-workstation

yum -y install krb5-libs krb5-workstation (on client machines)

[root@ip-172-31-24-211 ~]# cat /etc/krb5.conf

[logging]

default = FILE:/var/log/krb5libs.log

kdc = FILE:/var/log/krb5kdc.log

admin\_server = FILE:/var/log/kadmind.log

[libdefaults]

default\_realm = VISA.COM

dns\_lookup\_realm = false

dns\_lookup\_kdc = false

ticket\_lifetime = 24h

renew\_lifetime = 7d

forwardable = true

[realms]

VISA.COM = {

kdc = ip-172-31-24-211.us-west-2.compute.internal

admin\_server = ip-172-31-24-211.us-west-2.compute.internal

}

[domain\_realm]

.visa.com = VISA.COM

visa.com = VISA.COM

:wq!

3-

[root@ip-172-31-24-211 ~]# kdb5\_util create s

Loading random data

Initializing database '/var/kerberos/krb5kdc/principal' for realm 'VISA.COM',

master key name 'K/M@VISA.COM'

You will be prompted for the database Master Password.

It is important that you NOT FORGET this password.

Enter KDC database master key: hadoop

Re-enter KDC database master key to verify: hadoop

[root@ip-172-31-24-211 ~]# ^C

[root@ip-172-31-24-211 ~]#

4-

[root@ip-172-31-24-211 ~]# service krb5kdc restart

Stopping Kerberos 5 KDC: [FAILED]

Starting Kerberos 5 KDC: [ OK ]

[root@ip-172-31-24-211 ~]# service kadmin restart

Stopping Kerberos 5 Admin Server: [FAILED]

Starting Kerberos 5 Admin Server: [ OK ]

[root@ip-172-31-24-211 ~]# service krb5kdc status

krb5kdc (pid 23051) is running...

[root@ip-172-31-24-211 ~]# service kadmin status

kadmind (pid 23104) is running...

5-

[root@ip-172-31-24-211 ~]# chkconfig krb5kdc on

[root@ip-172-31-24-211 ~]# chkconfig kadmin on

6-

[root@ip-172-31-24-211 ~]# kadmin.local -q "addprinc admin/admin"

Authenticating as principal root/admin@VISA.COM with password.

WARNING: no policy specified for admin/admin@VISA.COM; defaulting to no policy

Enter password for principal "admin/admin@VISA.COM": admin

Re-enter password for principal "admin/admin@VISA.COM": admin

Principal "admin/admin@VISA.COM" created.

7-

[root@ip-172-31-24-211 ~]# cat /var/kerberos/krb5kdc/kadm5.acl

\*/admin@VISA.COM

8-

[root@ip-172-31-24-211 ~]# service kadmin restart

Stopping Kerberos 5 Admin Server: [ OK ]

Starting Kerberos 5 Admin Server: [ OK ]

[root@ip-172-31-24-211 ~]# service krb5kdc restart

Stopping Kerberos 5 KDC: [ OK ]

Starting Kerberos 5 KDC: [ OK ]

9-

[root@ip-172-31-24-211 ~]# kadmin -p admin/admin@VISA.COM

Authenticating as principal admin/admin@VISA.COM with password.

Password for admin/admin@VISA.COM:

10-

kadmin: **listprincs**

K/M@VISA.COM

admin/admin@VISA.COM

kadmin/admin@VISA.COM

kadmin/changepw@VISA.COM

kadmin/ip-172-31-24-211.us-west-2.compute.internal@VISA.COM

[krbtgt/VISA.COM@VISA.COM](mailto:krbtgt/VISA.COM@VISA.COM)

11-

kadmin: **addprinc maalam**

WARNING: no policy specified for maalam@VISA.COM; defaulting to no policy

Enter password for principal "maalam@VISA.COM": maalam

Re-enter password for principal "maalam@VISA.COM":maalam

Principal "maalam@VISA.COM" created.

**NOW GO TO CM AND ENABLE THE KERBEROS**

**-----------------------------------------------For sentry------------------------------------------------------**

**[alam@ip-172-31-23-127 ~]$ kinit**

**Password for** [**alam@VISA.COM**](mailto:alam@VISA.COM)**:**

**[alam@ip-172-31-23-127 ~]$ beeline**

**Beeline version 1.1.0-cdh5.12.0 by Apache Hive**

**beeline> !connect jdbc:hive2://ip-172-31-23-127.us-west-2.compute.internal:10000/default;principal=hive/ip-172-31-23-127.us-west-2.compute.internal@VISA.COM**

**0: jdbc:hive2://ip-172-31-23-127.us-west-2.co> show databases;**

**>create database admindb;**

**>use admindb;**

**>create table admin\_users ( name string , dep string ) row format delimited fields terminated by ‘,’ ;**

**2nd**

**>create table admin2\_users ( name string , dep string ) row format delimited fields terminated by ',' ;**

**Alam$vi file1**

**John,finance**

**Admin,IT**

**>load data local inpath ‘/home/alam/file1’ overwrite into table admin\_users;**

**Or**

**jdbc:hive2://ip-172-31-23-127.us-west-2.co> load data local inpath '/tmp/test.txt' into table**

**admin\_users ;**

**2nd**

**>load data local inpath '/tmp/test2.txt' into table admin2\_users ;**

**>select \* from admin\_users; check**

**Note-if sentry is not enable means that impersonation is enable that’s means whatever databases is created it will show ownership of that user who are created like below- “alam” & “user1”**

**2nd thing every one have access on every db.**

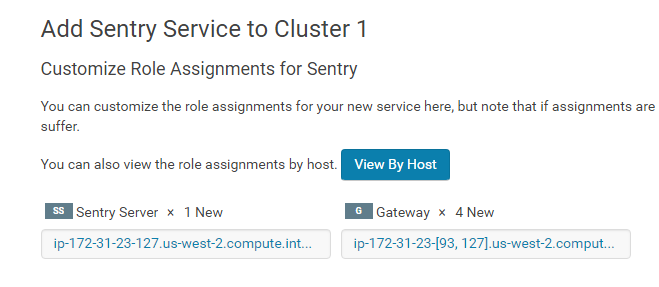
**[alam@ip-172-31-23-127 ~]$ hadoop fs -ls /user/hive/warehouse**

**Found 2 items**

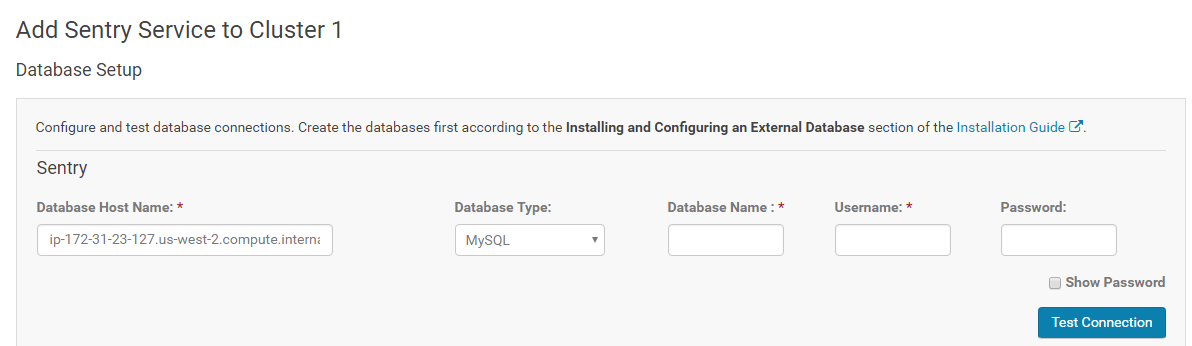
**drwxrwxrwt - alam hive 0 2018-10-24 10:22 /user/hive/warehouse/admindb.db**

**drwxrwxrwt - user1 hive 0 2018-10-25 06:24 /user/hive/warehouse/admindb2.db**

**Now go to cloudera manager and install sentry service-**



**Create sentry database-**



**]#yum -y install mysql-server mysql-connector-java**

**]#chkconfig mysqld on**

**]#service mysqld status**

**]#service mysqld start**

**change mysql paasword-**

**/usr/bin/mysql\_secure\_installation**

**(y,n,y,y)**

**mysql -u root -p**

**mysql> create database sentry;**

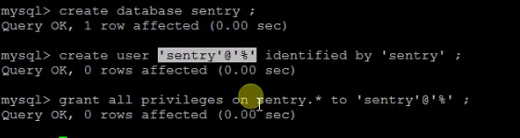
**Query OK, 1 row affected (0.00 sec)**

**mysql> create user 'sentry'@'%' identified by 'sentry' ;**

**Query OK, 0 rows affected (0.00 sec)**

**mysql> grant all privileges on sentry.\* to 'sentry'@'%';**

**Query OK, 0 rows affected (0.00 sec)**



**Restart stale service then**

**[alam@ip-172-31-23-127 ~]$ beeline**

**Beeline version 1.1.0-cdh5.12.0 by Apache Hive**

**beeline> !connect jdbc:hive2://ip-172-31-23-127.us-west-2.compute.internal:10000/default;principal=hive/ip-172-31-23-127.us-west-2.compute.internal@VISA.COM**

**0: jdbc:hive2://ip-172-31-23-127.us-west-2.co> show databases;**

**(will display only default db.)**

**For testing-**

**Root#Groupadd sentryadmin**

**Root#usermod –g sentryadmin alam**

**beeline> !connect jdbc:hive2://ip-172-31-23-127.us-west-2.compute.internal:10000/default;principal=hive/ip-172-31-23-127.us-west-2.compute.internal@VISA.COM**

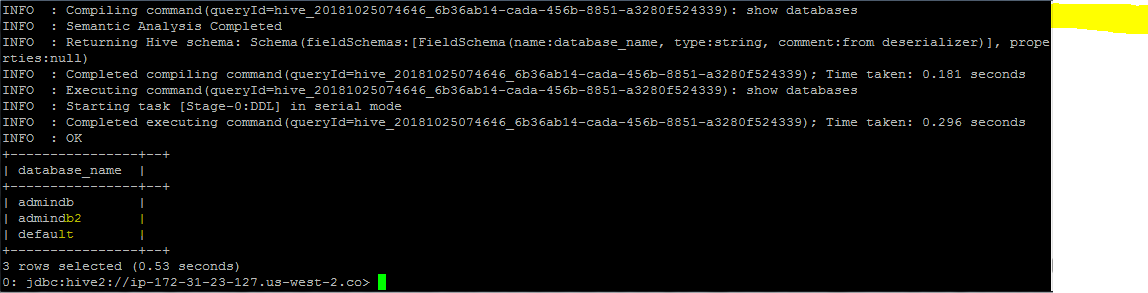
**jdbc:hive2://ip-172-31-23-127.us-west-2.co> create role admin\_role ;**

**>show roles;**

**> jdbc:hive2://ip-172-31-23-127.us-west-2.co> grant all on server server1 to role admin\_role ;**

**>jdbc:hive2://ip-172-31-23-127.us-west-2.co> grant role admin\_role to group sentryadmin;**

**>show databases;**



**And if u login with another user like user1 who is not part of sentryadmin team then he will not able to see the databases except default.**

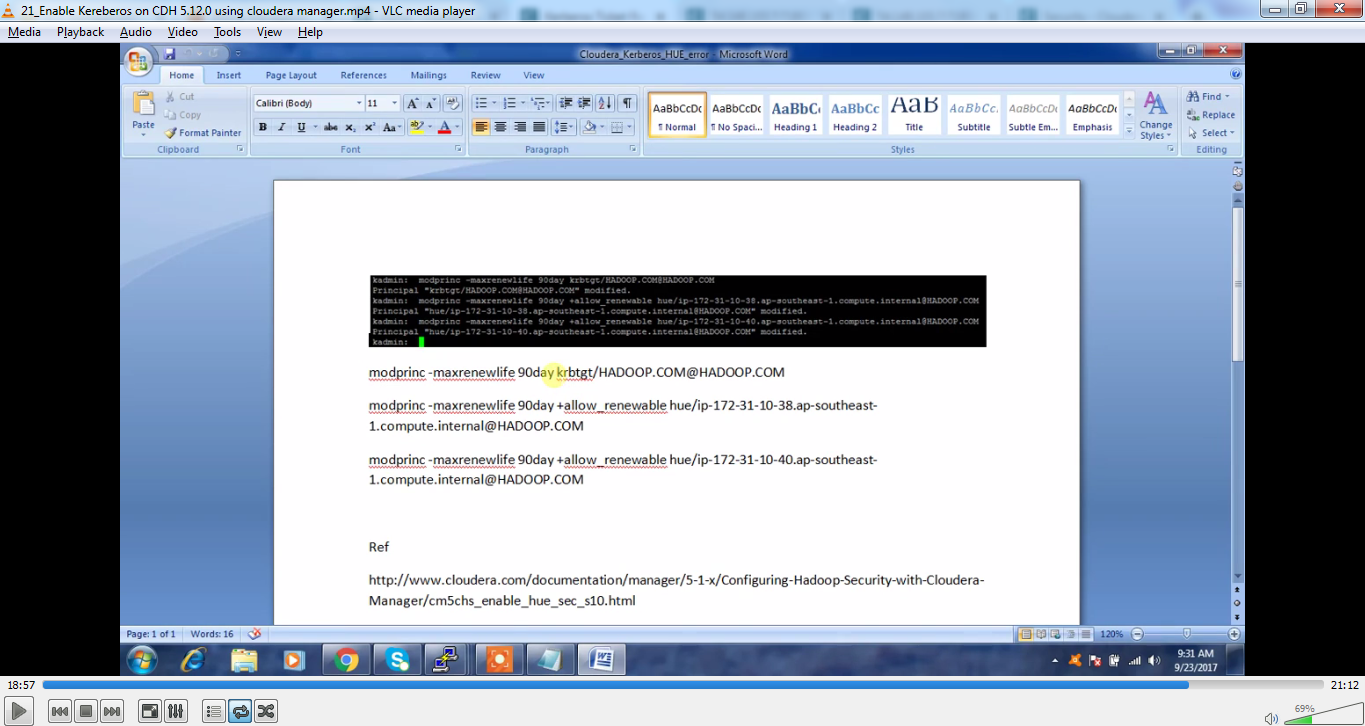
**Alam#**

**jdbc:hive2://ip-172-31-23-127.us-west-2.co> create role marketing\_role ;**

**jdbc:hive2://ip-172-31-23-127.us-west-2.co> grant all on database marketing to role marketing\_role ;**

**jdbc:hive2://ip-172-31-23-127.us-west-2.co> grant role marketing\_role to group marketing ;**

**================================Hue Max renewable===================**

 **kadmin.local: modprinc -maxrenewlife 90day** [**krbtgt/VISA.COM@VISA.COM**](mailto:krbtgt/VISA.COM@VISA.COM)

**kadmin.local: modprinc -maxrenewlife 90day +allow\_renewable hue/ip-172-31-23-127.us-west-2.compute.internal@VISA.COM**

**------------------------------------------------------------Open ldap----------------------------------------------------------------**

[root@ip-172-31-28-112 ~]# yum -y install epel-release

cp /usr/share/openldap-servers/DB\_CONFIG.example /var/lib/ldap/DB\_CONFIG

chown ldap. /var/lib/ldap/DB\_CONFIG

service slapd start

chkconfig slapd on

[root@ip-172-31-28-112 ~]# slappasswd

New password:hadoop

Re-enter new password:hadoop

{SSHA}Pq5idXMk0dKIF7joNw0fGViIrwPdqOgJ

[root@ip-172-31-28-112 ~]# mkdir ldap\_files

[root@ip-172-31-28-112 ~]# cd ldap\_files/

[root@ip-172-31-28-112 ldap\_files]# vi setrootpass.ldif

[root@ip-172-31-28-112 ldap\_files]# cat setrootpass.ldif

dn: olcDatabase={0}config,cn=config

changetype:modify

add:olcRootPW

olcRootPW:{SSHA}Pq5idXMk0dKIF7joNw0fGViIrwPdqOgJ

[root@ip-172-31-28-112 ldap\_files]# ldapadd -Y EXTERNAL -H ldapi:/// -f setrootpass.ldif

* Note-**There are some more commands and files entry after this-** - ----

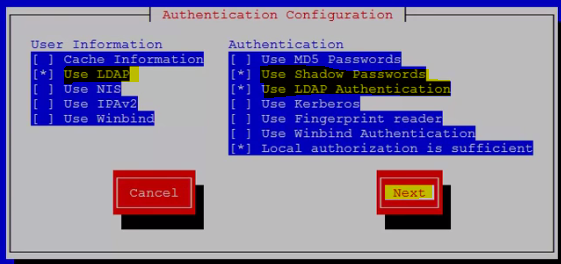
Login through web ui & u can create an OU, Groups, Users…..etc.

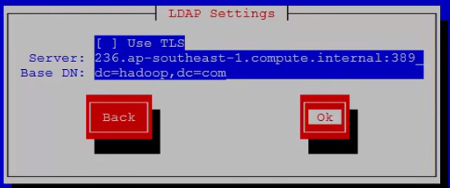
**On all Nodes->**

**#Yum –y install nss-pam-ldapd**

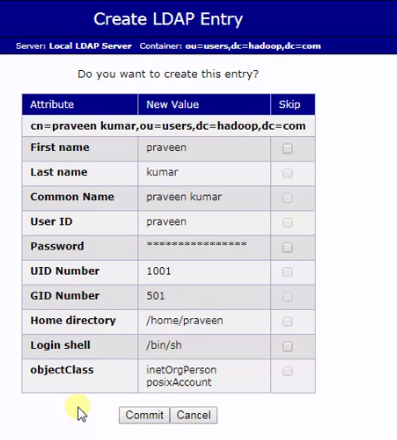
**#authoconfig –enableldap –enablemkhomedir –ldapserver=ldap://ip-172.31.24.236----internal:389 –ldapbasedn=”dc=hadoop,dc=com” –update**

**#authoconfig-tui**





**After these configuration on all the nodes. When u create a user on ldap server then those a/c will reflect on all the nodes. Like below-**





**Now u can integrate the Hue with open LDAP—using below changes in CM->HUE->configuration--**

