Kerberos Deployment

##

Kerberos Installation CDP

##

Install kerberos KDC and Admin server

On Cm host install kdc and admin server

$ sudo apt-get install -y rng-tools

$ sudo apt install krb5-kdc krb5-admin-server

For realm give : HADOOP.COM

Kerberos server for your realm : <private-dns-of-cm>

$ sudo krb5_newrealm

Check the krb5.conf

nano /etc/krb5.conf

Check kdc.conf for kdc configurations

sudo nano /usr/share/doc/krb5-kdc/examples/kdc.conf

Uncomment - supported enryption type

sudo /etc/init.d/krb5-admin-server restart

$ sudo kadmin.local

addprinc cm/admin

quit

sudo nano /etc/krb5kdc/kadm5.acl
cm/admin@HADOOP.COM *

sudo /etc/init.d/krb5-admin-server restart

sudo kadmin.local
addprinc user1

Intall kerberos clients

sudo apt-get install krb5-user -y

Select aes256-cts as algorithm type

Create a principal for hdfs superuser

sudo kadmin.local
addprinc hdfs@HADOOP.com

Create principal for other users

addprinc usera
addprinc userb
addprinc user2
addprinc userc

Kerberos Commands

-> Adding principal
addprinc prinname

-> Deleting Principal
delprinc princname

-> Listing all principals
listprincs

-> Getting information about a particular principal
getprinc princname

-> Change password for particular principal
cpw princname

Creating and using keytab files

--* Create principal and its keytab *--

$ sudo kadmin.local

addprinc user2

xst -kt /tmp/user2.keytab user2@HADOOP.COM

--* Send keytab files to user *--

$ sudo chmod a+r /tmp/user2.keytab

$ scp -i key.pem /tmp/user2.keytab ubuntu@ip-172-31-87-98.ec2.internal:~

--* Authenticate using keytab *--

$ chmod 600 user2.keytab

$ kinit -kt user1.keytab user1

$ klist