**CM cluster configuration**

Cloudera is designed to be configured through the cloudera web interface. Unless you disable the CM, it will overwrite any changes to the XML files that you make.

Cloudera has a restful API which is documented at http://cdh-master1.staging.hq.YourCompanyDomain.com:7180/static/apidocs/tutorial.html

http://cdh-master2.prod.hq.YourCompanyDomain.com:7180/cmf/home

### FreeIPA + Kerberos - Architecture

We are using FreeIPA to control access to the boxes but we cannot set up realms with freeIPA. We are setting up Kerberos per-cluster to manage authentication within the cluster. Kerberos will build trust with FreeIPA.

### Step 1: Setting up Kerberos on a cluster

yum install krb5-server

* edit /var/kerberos/krb5kdc/kdc.conf
  + ADD REALM
  + RD1.HQ.YourCompanyDomain.COM = {
  + max\_life = 1d 0h 0m 0s
  + max\_renewable\_life = 7d 0h 0m 0s
  + remove **aes256-cts:normal** if we don’t use JCE patch
* edit **/var/kerberos/krb5kdc/kadm5.acl** (access control list)   
  \*/admin@<ENV>.HQ.YourCompanyDomain.COM \*
* edit /etc/krb5.conf
  + add realm and if neeeded add user specific params
    - update **default\_realm**
  + add
    - [logging]
    - default = FILE:/var/log/krb5libs.log
    - kdc = FILE:/var/log/krb5kdc.log
    - admin\_server = FILE:/var/log/kadmind.log
    - See Diff and file at bottom
* create DB
  + /usr/sbin/kdb5\_util create -s
  + see password in personal files
  + WILL FAIL IF IT CANNOT RESOLVE HOSTS
* Create admin principals
  + /usr/sbin/kadmin.local -q "addprinc root/admin"
  + /usr/sbin/kadmin.local -q "addprinc cmadm/admin"
    - for CM to do it
* start krb5kdc and kadmin
  + systemctl enable krb5kdc
  + systemctl start krb5kdc
  + systemctl enable kadmin
  + systemctl start kadmin
* TEST IF IT WORKED with admin user (requires PW)
  + kinit root/admin
* Automate generating keytab
  + Copy /etc/krb5.conf to every host in the cluster
  + from admin server run to generate a keytab (for automation)  
    **kadmin.local -q "xst -k /etc/krb5kdc.keytab root/admin"**
  + test it (OPTIONAL)  
    **kinit -kt /etc/krb5kdc.keytab root/admin  
    klist**
  + NOTE Test The **/etc/krb5kdc.keytab** can be moved to other machines to give the keypair  
     always 600
* Activate Kerberos in WebApp - See pics “kerberos\_admin\*” PORT 8080 in ambari
  + click DROPDOWN MENU on top, NOT Side-menu. *administration > security*
  + select *Enable kerberos* and accept checkboxes
  + pg.2 g Dump encryption types with **klist -ket /etc/krb5kdc.keytab** and add lines to **Kerberose Encryption Types**
  + Manage krb5.conf through Cloudera Manager -- **NO**
  + **Configured ports - select “yes I am ready to restart”**
* **Setting up TLS - fixing config issues**
  + see pic TLS\_config\_issue
  + Skippable for now
* restart the manage and cluster
* krb5cc - ticket cache file problems
  + you may have problems if you use keyring instead of a file on file system. comment out **default\_ccache\_name = KEYRING:persistent:%{uid}** if this is an issue
* Make sure kerberos is working
  + change user to HDFS  
    sudo -u hdfs /bin/bash
  + hadoop fs -ls /
  + kinit <name/type> e.g. cmadm/admin
    - klist -- see principals

### Step 2: Trust Between Kerberos and FreeIPA

go to admin server running free IPA and use MIT kerberos commands to create TGT principal. This works around the fact that freeIPA does not have realms by dropping down to the MIT commands.

* kadmin.local -q 'addprinc -pw <pw> <princ name>/<MIT/hadoop realm>@<FreeIPA realm>' -x ipa-setup-override-restrictions  
  e.g.   
  kadmin.local -q 'addprinc -e "aes128-cts:normal" -pw xxxxx krbtgt/RD1.HQ.YourCompanyDomain.COM@YourCompanyDomain.COM' -x ipa-setup-override-restrictions
  + Test it  
    kinit cmadm/admin
  + export KRB5CCNAME=/tmp/ccache\_$UID
  + kdestroy
  + kinit cmadm/admin
  + klist

[root@bos-rd1-cdh-master1 ~]# cat /etc/krb5.conf

#File modified by ipa-client-install

includedir /var/lib/sss/pubconf/krb5.include.d/

[logging]

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

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

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

[libdefaults]

default\_realm = RD1.HQ.YourCompanyDomain.COM

dns\_lookup\_realm = false

dns\_lookup\_kdc = false

rdns = false

ticket\_lifetime = 24h

renew\_lifetime = 7d

forwardable = yes

udp\_preference\_limit = 0

default\_ccache\_name = FILE:/tmp/krb5\_ccache\_uid

[realms]

RD1.HQ.YourCompanyDomain.COM = {

kdc = bos-rd1-cdh-master1.rd1.hq.YourCompanyDomain.com

admin\_server = bos-rd1-cdh-master1.rd1.hq.YourCompanyDomain.com

}

YourCompanyDomain.COM = {

kdc = bos-admin1.hq.YourCompanyDomain.com:88

master\_kdc = bos-admin1.hq.YourCompanyDomain.com:88

admin\_server = bos-admin1.hq.YourCompanyDomain.com:749

default\_domain = rd1.hq.YourCompanyDomain.com

pkinit\_anchors = FILE:/etc/ipa/ca.crt

}

[domain\_realm]

.rd1.hq.YourCompanyDomain.com = RD1.HQ.YourCompanyDomain.COM

rd1.hq.YourCompanyDomain.com = RD1.HQ.YourCompanyDomain.COM

.YourCompanyDomain.com = YourCompanyDomain.COM

YourCompanyDomain.com = YourCompanyDomain.COM