1. 설치 계정 : root
2. 2. Cluster 구성

dn01.cdh.exem

dn02.cdh.exem

dn02.cdh.exem

dn03.cdh.exem

manage.cdh.exem

nn01.cdh.exem

nr02.cdh.exem

rm01.cdh.exem

1. 위의 서버명을 servers.txt로 저장
2. 아래 스크립트(ssh\_all.sh)를 이용하여 ntpd 서비스가 설치되어 있는지 확인한다.

#!/bin/bash

while read line

do  
 echo $line

ssh -n $line $1

done < servers.txt

[root@manage ~]# **./ssh\_all.sh 'service ntpd status'**

dn01.cdh.exem

ntpd (pid 16533) is running...

dn02.cdh.exem

ntpd (pid 18849) is running...

dn02.cdh.exem

ntpd (pid 18849) is running...

dn03.cdh.exem

ntpd (pid 19257) is running...

manage.cdh.exem

ntpd (pid 26116) is running...

nn01.cdh.exem

ntpd (pid 32007) is running...

nr02.cdh.exem

ntpd (pid 15481) is running...

rm01.cdh.exem

ntpd (pid 18343) is running...

1. Java Cryptography Extension 모듈 설치(주의: 라이선스 동의 문제로 단순히 wget으로는   
   다운로드가 않 됨 아래의 옵션을 주고 수행해야 함.)

wget \

--no-cookies \

--no-check-certificate \

--header "Cookie: gpw\_e24=http%3A%2F%2Fwww.oracle.com%2F; oraclelicense=accept-securebackup-cookie" \

-O jce\_policy-8.zip \

http://download.oracle.com/otn-pub/java/jce/8/jce\_policy-8.zip

1. 아래 스크립트를 이용하여 모든 서버에 다운받은 파일을 전송해 준다.

./scp\_all.sh jce\_policy-8.zip /root/

#!/bin/bash

while read line

do  
 echo $line

scp $1 $line:$2

done < servers.txt

1. 전송한 파일을 ssh\_all.sh을 이용하여 압축을 풀어준다.  
   ./ssh\_all.sh 'jar xvf jce\_policy-8.zip'
2. 압축해제 한 파일을 복사해 준다.

./ssh\_all.sh 'cp -f /root/UnlimitedJCEPolicyJDK8/\*.jar /usr/lib/jvm/java-1.8.0/jre/lib/security'

1. /etc/krb5.conf 파일 수정

[logging]

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

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

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

[libdefaults]

default\_realm = EXEM.COM

dns\_lookup\_realm = false

dns\_lookup\_kdc = false

ticket\_lifetime = 24h

renew\_lifetime = 7d

forwardable = true

[realms]

EXAMPLE.COM = {

kdc = manage.cdh.exem

admin\_server = manage.cdh.exem

default\_domain= dn01.cdh.exem

}

[domain\_realm]

dn01.cdh.exem = EXEM.COM

dn02.cdh.exem = EXEM.COM

dn03.cdh.exem = EXEM.COM

manage.cdh.exem = EXEM.COM

nn01.cdh.exem = EXEM.COM

nr02.cdh.exem = EXEM.COM

rm01.cdh.exem = EXEM.COM

10. krb5.conf 전체 노드에 복사

./scp\_all.sh /etc/krb5.conf /etc/

vi /var/kerberos/krb5kdc/kadm5.acl 수정

\*/admin@EXEM.COM \*

cloudera-scm@EXEM.COM \* flume/\*@EXEM.COM

cloudera-scm@EXEM.COM \* hbase/\*@EXEM.COM

cloudera-scm@EXEM.COM \* hdfs/\*@EXEM.COM

cloudera-scm@EXEM.COM \* hive/\*@EXEM.COM

cloudera-scm@EXEM.COM \* httpfs/\*@EXEM.COM

cloudera-scm@EXEM.COM \* HTTP/\*@EXEM.COM

cloudera-scm@EXEM.COM \* hue/\*@EXEM.COM

cloudera-scm@EXEM.COM \* impala/\*@EXEM.COM

cloudera-scm@EXEM.COM \* mapred/\*@EXEM.COM

cloudera-scm@EXEM.COM \* oozie/\*@EXEM.COM

cloudera-scm@EXEM.COM \* solr/\*@EXEM.COM

cloudera-scm@EXEM.COM \* sqoop/\*@EXEM.COM

cloudera-scm@EXEM.COM \* yarn/\*@EXEM.COM

cloudera-scm@EXEM.COM \* zookeeper/\*@EXEM.COM

cloudera-scm@EXEM.COM \* kudu/\*@EXEM.COM

12. kdb5\_util을 이용해서 KDC가 티켓 발급 대상 데이터베이스 생성  
master key name은 'K/M@EXEM.COM'  
database Master Password(그냥 엔터)  
# /usr/sbin/kdb5\_util create -r EXEM.COM -s  
# ls /var/kerberos/krb5kdc/principal  
\*\* 참고 : 데이터베이스 삭제 명령  
 kdb5\_util destroy-f EXEM.COM

위 과정에서 패스워드는 그냥 엔터로 만듬.

Step 8) Principal을 데이터베이스발급한다.(패스워드는 exem)

# kadmin.local

kadmin.local: addprinc root/admin  
kadmin.local: addprinc cloudera-scm/admin  
kadmin.local: addprinc cloudera-scm/admin@EXEM.COM

13. kadmin 키탭파일 추가

# kadmin.local

kadmin.local : ktadd -k /var/kerberos/krb5kdc/kadm5.keytab kadmin/admin  
kadmin.local : ktadd -k /var/kerberos/krb5kdc/kadm5.keytab kadmin/changepw

14. 호스트 principals 등록

kadmin.local: addprinc -randkey host/dn01.cdh.exem

kadmin.local: addprinc -randkey host/dn02.cdh.exem

kadmin.local: addprinc -randkey host/dn03.cdh.exem

kadmin.local: addprinc -randkey host/manage.cdh.exem

Kadmin.local: addprinc -randkey host/nn01.cdh.exem

kadmin.local: addprinc -randkey host/nr02.cdh.exem

kadmin.local: addprinc -randkey host/rm01.cdh.exem

15. 호스트 keytab 등록

kadmin.local: ktadd -k /etc/krb5.keytab host/dn01.cdh.exem

kadmin.local: ktadd -k /etc/krb5.keytab host/dn02.cdh.exem

kadmin.local: ktadd -k /etc/krb5.keytab host/dn03.cdh.exem

kadmin.local: ktadd -k /etc/krb5.keytab host/manage.cdh.exem

kadmin.local: ktadd -k /etc/krb5.keytab host/nn01.cdh.exem

kadmin.local: ktadd -k /etc/krb5.keytab host/nr02.cdh.exem

kadmin.local: ktadd -k /etc/krb5.keytab host/rm01.cdh.exem

16. Kerboros 서비스를 시작한다.  
 #service krb5kdc start  
 #service kadmin start

서비스 프로세스를 확인한다.

netstat -nat | grep 88로 포트 Listen을 확인한다.

netstat -nat | grep 749로 포트 Listen을 확인한다.

17. keytab file 확인

# ktutil   
ktutil : rkt /var/kerberos/krb5kdc/kadm5.keytab   
ktutil : list

~~18. /etc/kdc5.conf 파일을 각 호스트에 (클라이언트)에 전송한다.~~

~~# scp /etc/krb5.conf root@name.localdomain:/etc/krb5.conf~~

CM에서 Kerberos 클라이언트 구성배포를 선택하면 자동배포

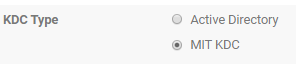
되므로 위 작업은 필요업음

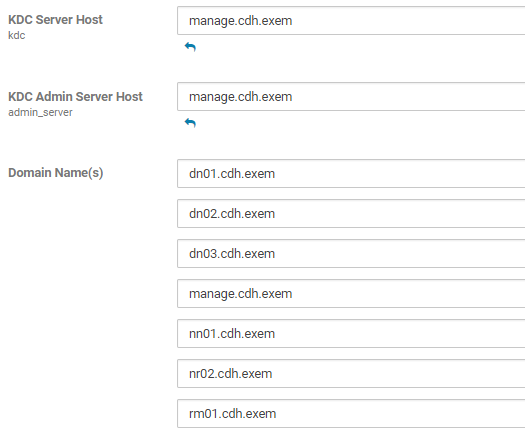
19. 각 커러로스 클라이언트 에서 커버로스 서버로 접속을 확인한다.

# kadmin -p root/admin

20. Cloudera Manger 시작  
 #service cloudera-scm-manager start

21 cm으로 로긴해서 커버로스 enable 프로세스를 진행한다.  
관리 > 보안 > kerberos 설정  
사전작업 진행여부 체크박스에 모두 체크하고 계속을 클릭한다.  
아래 화면을 참조하여 진행을 하면 된다.





**설치 테스트 1)**

cm 재시작, agent 재시작, 서비스 재시작

**트러블 슈팅 1)**

Cloudera-scm-server 시작 시 아래와 같은 에러가 발생할 경우

/usr/share/java/postgresql-connector-java.jar 파일을 삭제하고 시작을 해보면

postgresql-42.2.5.jre7.jar 파일이 자동생성되면서 시작이 된다.

java.lang.UnsupportedClassVersionError: org/postgresql/Driver : Unsupported major.minor version 52.0

트러블 슈팅 2)  
Hue ticket\_renewer를 시작 할때 아래 에러가 나는 경우 아래명령어를 수행해 준다.

Couldn't renew kerberos ticket in order to work around Kerberos 1.8.1 issue. Please check that the ticket for 'hue/ngs-poc2.tcshydnextgen.com@TCSHYDNEXTGEN.COM' is still renewable:

kadmin.local: modprinc -maxrenewlife 90day krbtgt/YOUR\_REALM.COM  
kadmin.local: modprinc -maxrenewlife 90day +allow\_renewable hue/ manage.cdh.exem@EXEM.COM

**설치 테스트 2)**

Manage 서버에서 유저아이디를 생성하고 키탭파일을 생성하여 Hdfs 커맨드 실행

모든 서버에서 아래명령 실행  
$>adduser jhkang  
  
커버로스 서버에서 아래명령 수행

Kadmin.local : addprinc jhkang@EXEM.COM

kadmin.local : ktadd -k /opt/Cloudera/keytabs/jhkang.keytab jhkang@EXEM.COM

Problem 1)

SIMPLE authentication is not enabled. Available:[TOKEN, KERBEROS]

위와 같은 에러가 발생하는 경우는 CORE-SITE.XML 파일에 아래와 같은 내용이 변경되지 않아서 이다. CM에 재로그인 하여 오래된 구성을 재배포 해준다.

다른 서버에서는 모두 잘되는데 특정서버만 안되는 경우는 게이트웨이가 설치가 않되서 그런 경우가 있으니 게이트웨이 서버는 모두 설치해줘야 한다.

manage배포가 안되는 경우는 수동으로 해준다.( /etc/hadoop/conf.cloudera.hdfs/core-site.xml)

수동으로 수정을 해줘도 않된는 경우는 gateway가 없는 서버에는 cm이 client configuration을 배포하지 않는다.

<property>

<name>hadoop.security.authentication</name>

<value>kerberos</value> <!-- A value of "simple" would disable security. -->

</property>

<property>

<name>hadoop.security.authorization</name>

<value>true</value>

</property>

설치 테스트 3)

1. 키탭파일 생성을 통한 hdfs 테스트

사용자 TIP KEYTAB파일 저장 폴더를 생성해준다.

해당폴더는 모든유저가 접근 가능해야 하고 키탭파일 자체는 본인만 읽을 수 있어야 해서 600 퍼미션 이여야 한다.

./ssh\_all.sh ‘mkdir -p /opt/Cloudera/keytabs’

1. 사용자 키탭추가와 프린시펄 추가

Kadmin.local : ktadd -k /opt/Cloudera/keytabs/jhkang.keytab jhkang@EXEM.COM

addprinc [jhkang@EXEM.COM](mailto:jhkang@EXEM.COM)

1. 키탭파일 오너 변경

chmod jhkang:jhkang /opt/Cloudera/keytab/jhkang.keytab

1. 키탭파일 모든 서버에 복사

./scp\_all.sh /opt/Cloudera/keytabs/jhkang.keytab /opt/Cloudera/keytabs/

1. 키탭을 이용한 커버로스 티켓 발급테스트  
   $>su - jhkang

$>kinit -kt /opt/Cloudera/keytabs/jhkang.keytab [jhkang@EXEM.COM](mailto:jhkang@EXEM.COM)

1. Klist

[jhkang@manage ~]$ klist

Ticket cache: FILE:/tmp/krb5cc\_505

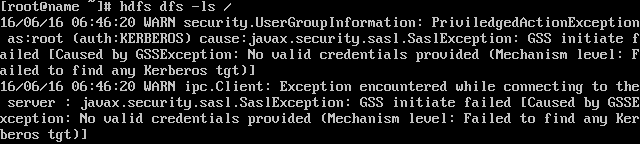
Default principal: jhkang@EXEM.COM

Valid starting Expires Service principal

10/10/18 20:40:37 10/11/18 20:40:37 krbtgt/EXEM.COM@EXEM.COM

renew until 10/10/18 20:40:37

1. Hdfs 명령어가 잘되는 지 테스트

아래와 같은 에러가 발생하지 않으면 성공  


1. 키탭을 이용한 hive 접속 테스트

beeline -u "jdbc:hive2://nr02.cdh.exem:10000/default;principal=hive/nr02.cdh.exem@EXEM.COM"