****1.KDC服务安装及配置****

## 1.在Cloudera Manager服务器上安装KDC服务

yum -y install krb5-serverkrb5-libs krb5-auth-dialog krb5-workstation

## 2.修改/etc/krb5.conf配置

vi /etc/krb5.conf

# Configuration snippets may be placed in this directory as well

includedir /etc/krb5.conf.d/

[logging]

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

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

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

[libdefaults]

dns\_lookup\_realm = false

ticket\_lifetime = 24h

renew\_lifetime = 7d

forwardable = true

default\_tgs\_enctypes = aes256-cts-hmac-sha1-96

default\_tkt\_enctypes = aes256-cts-hmac-sha1-96

permitted\_enctypes = aes256-cts-hmac-sha1-96

rdns = false

pkinit\_anchors = /etc/pki/tls/certs/ca-bundle.crt

default\_realm = DTSTACK.COM

# default\_ccache\_name = KEYRING:persistent:%{uid}

[realms]

DTSTACK.COM = {

kdc = cdh01

admin\_server = cdh01

}

[domain\_realm]

.dtstack.com = DTSTACK.COM

dtstack.com = DTSTACK.COM

## 3.修改/var/kerberos/krb5kdc/kadm5.acl配置

vim /var/kerberos/krb5kdc/kadm5.acl

\*/admin@DTSTACK.COM \*

## 4.修改/var/kerberos/krb5kdc/kdc.conf配置

vim /var/kerberos/krb5kdc/kdc.conf

[kdcdefaults]

kdc\_ports = 88

kdc\_tcp\_ports = 88

[realms]

DTSTACK.COM = {

#master\_key\_type = aes256-cts

max\_renewable\_life = 10d

acl\_file = /var/kerberos/krb5kdc/kadm5.acl

dict\_file = /usr/share/dict/words

admin\_keytab = /var/kerberos/krb5kdc/kadm5.keytab

supported\_enctypes = aes256-cts:normal aes128-cts:normal des3-hmac-sha1:normal arcfour-hmac:normal camellia256-cts:normal camellia128-cts:normal des-hmac-sha1:normal des-cbc-md5:normal des-cbc-crc:normal

## 5.创建Kerberos数据库

kdb5\_util create –r DTSTACK.COM -s

Loading random data

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

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

You will be prompted for the database Master Password.

It is important that you NOT FORGET this password.

Enter KDC database master key:

Re-enter KDC database master key to verify:

## 6.创建Kerberos的管理账号

kadmin.local

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

kadmin.local: addprinc admin/admin@DTSTACK.COM

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

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

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

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

kadmin.local: exit

## 将Kerberos服务添加到自启动服务，并启动krb5kdc和kadmin服务

[root@cdh01]# chkconfig krb5kdc on

[root@cdh01]# chkconfig kadmin on

[root@cdh01]# service krb5kdc start

Starting Kerberos 5 KDC:                                   [  OK  ]

[root@cdh01]# service kadmin start

Starting Kerberos 5 Admin Server:                          [  OK  ]

## 8.测试Kerberos的管理员账号

[root@cdh01]# kinit admin/admin@DTSTACK.COM

Password for admin/admin@DTSTACK.COM:

[root@cdh01]# klist

Ticket cache: FILE:/tmp/krb5cc\_0

Default principal: admin/admin@DTSTACK.COM

Valid starting Expires Service principal

01/07/19 11:47:24 01/08/19 11:47:24 krbtgt/DTSTACK.COM@DTSTACK.COM

renew until 01/07/19 11:47:24

## 为集群安装所有Kerberos客户端，包括Cloudera Manager

yum -y install krb5-libs krb5-workstation

## 10.在Cloudera Manager Server服务器上安装额外的包

yum -y install openldap-clients

## 11.将KDC Server上的krb5.conf文件拷贝到所有Kerberos客户端

scp -r /etc/krb5.conf root@cdh02:/etc/

# CDH集群启用Kerberos

## 1.在KDC中给Cloudera Manager添加管理员账号

kadmin.local

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

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

WARNING: no policy specified for cloudera-scm/admin@DTSTACK.COM; defaulting to no policy

Enter password for principal "cloudera-scm/admin@DTSTACK.COM":

Re-enter password for principal "cloudera-scm/admin@DTSTACK.COM":

Principal "cloudera-scm/admin@DTSTACK.COM" created.

kadmin.local: exit

## 2.进入Cloudera Manager的“管理”-> “安全”界面

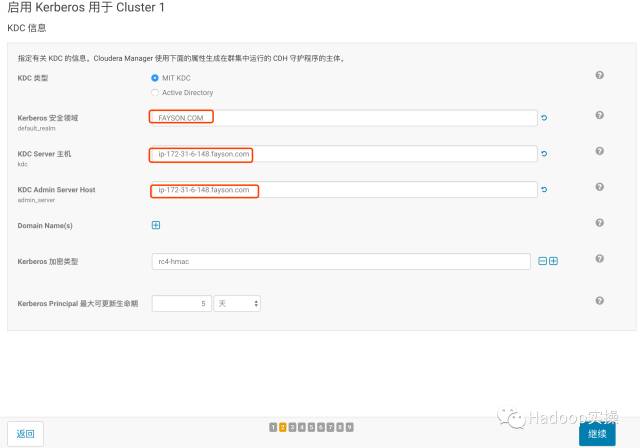


## 3.选择“启用Kerberos”，进入如下界面

确保如下列出的所有检查项都已完成



## 4.点击“继续”，配置相关的KDC信息，包括类型、KDC服务器、KDC Realm、加密类型以及待创建的Service Principal（hdfs，yarn,，hbase，hive等）的更新生命期等



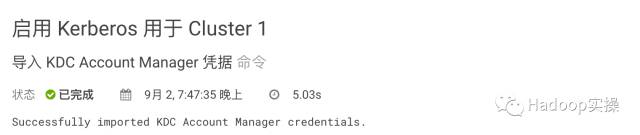
## 5.点击“继续”



## 6.不建议让Cloudera Manager来管理krb5.conf, 点击“继续”



## 7.输入Cloudera Manager的Kerbers管理员账号，必须和之前创建的账号一致，点击“继续”



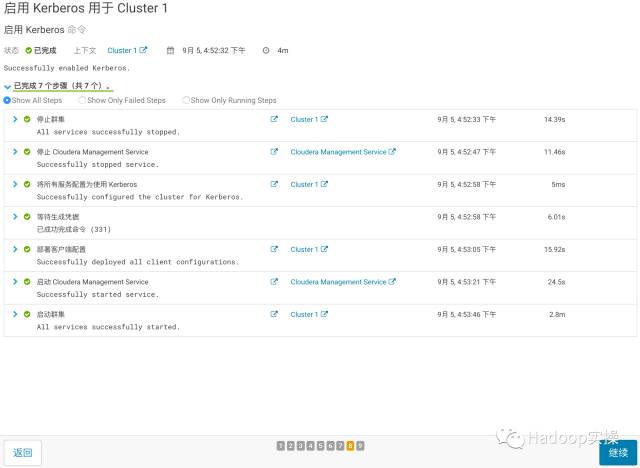
## 8.等待启用Kerberos完成，点击“继续”



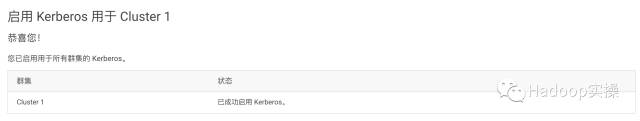
## 9.点击“继续”



## 10.勾选重启集群，点击“继续”

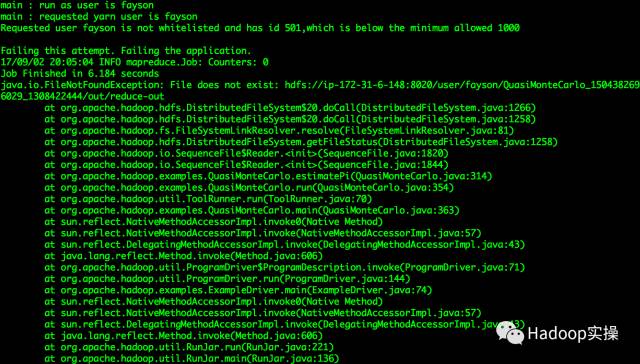


## 11.等待集群重启成功，点击“继续”



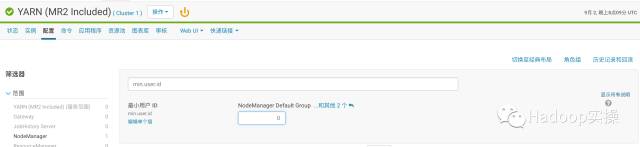
至此已成功启用Kerberos。

# 常见问题

1.Yarn限制了用户id小于10000的用户提交作业

问题原因：是由于Yarn限制了用户id小于10000的用户提交作业；

解决方法：修改Yarn的min.user.id来解决



## container启动失败

问题原因：认证的用户不允许运行container

解决方法：修改yarn的配置项，添加认证用户到allowed.system.users

