**在CDH 5.x中部署Kerberos**

**整理编写者：于康**

1. **前提：**

已经安装好CDH 并且能正常运行。配置好ntp时间同步（这个对于部署Kerberos很重要，具体可以看下Kerberos简介）。用到hfs此工具，修改yum配置（借鉴CDH5 安装文档.docx 十一、安装配置mysql 下的 1.安装mysql前的准备工作）。

1. **环境配置：**

|  |  |  |
| --- | --- | --- |
| **主机名** | **内网IP** | **角色** |
| **n1** | **172.16.71.237** | **Master KDC** |
| **n2** | **172.16.71.238** | **Kerberos client** |
| **n3** | **172.16.71.239** | **Kerberos client** |

1. **安装Kerberos安装包：**

**主节点n1上执行：**

yum install krb5-server krb5-libs krb5-auth-dialog

**所有子节点上执行：**

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

**当跳出[y/n]输入y继续。**

## 安装JCE Policy File

如果你的操作系统是CentOS/Red Hat 5.5或更高版本（这些OS默认使用AES-256来加密tickets），则你就必须在所有的集群节点以及Hadoop使用者的主机上安装 [Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy File](http://www.oracle.com/technetwork/java/javase/downloads/index.html" \t "https://www.zybuluo.com/xtccc/note/_blank) 。本文中使用的是jdk1.7，下载的jce也是1.7的版本。

将这两个文件放到

{JAVA\_HOME}/jre/lib/security/directory

这个文件下，所有节点都要执行次操作

1. **配置Master KDC 服务端：**
2. 确保所有的clients与servers之间的时间同步以及DNS正确解析。
3. 选择一个主机来运行KDC，确保已经在主节点（本文是n1）执行yum安装Kerberos包。

KDC的主机必须非常自身安全，一般该主机只运行KDC程序。   
 本文中我们选择 n1 作为运行KDC的主机。

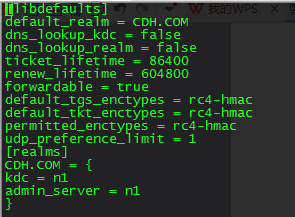
在安装完上述的软件之后，会在KDC主机上生成配置文件/etc/krb5.conf和 /var/kerberos/krb5kdc/kdc.conf，它们分别反映了realm name 以及 domain-to-realm mappings。

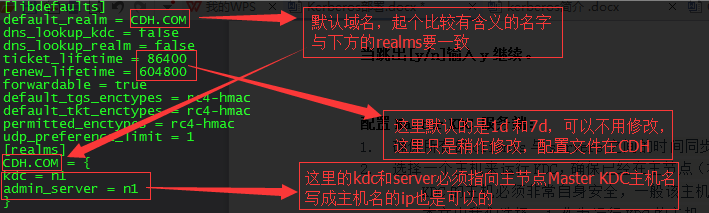
1. 配置 *krb5.conf* 与 *kdc.conf*

我们对这两个模板文件稍加修改即可。

**vi /etc/krb5.conf**

例图：



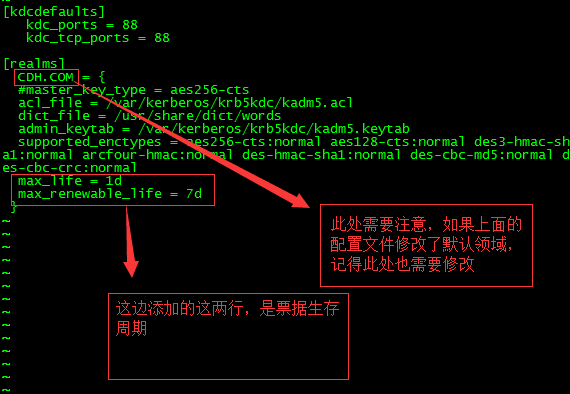
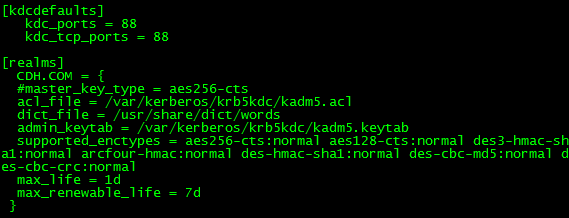


以上这个配置文件，配好之后scp到其他子节点上面

scp /etc/krb5.conf root@n2:/etc/

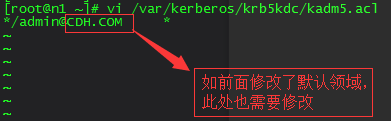
scp /etc/krb5.conf root@n2:/etc/

**vi /var/kerberos/krb5kdc/kdc.conf**



在KDC上我们需要编辑acl文件来设置权限，该acl文件的默认路径是 /var/kerberos/krb5kdc/kadm5.acl（也可以在文件kdc.conf中修改）。Kerberos的*kadmind* daemon会使用该文件来管理对Kerberos database的访问权限。对于那些可能会对pincipal产生影响的操作，acl文件也能控制哪些principal能操作哪些其他pricipals。

**vi /var/kerberos/krb5kdc/kadm5.acl**



1. 创建/初始化Kerberos database

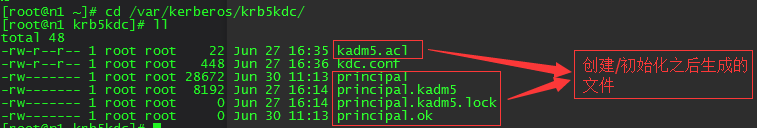
/usr/sbin/kdb5\_util create -s



其中，『-s』表示生成stash file，并在其中存储master server key（krb5kdc）；还可以用『-r』来指定一个realm name —— 当krb5.conf中定义了多个realm时才是必要的。

在此过程中，我们会输入database的管理密码。这里设置的密码一定要记住，如果忘记了，就无法管理Kerberos server。

当Kerberos database创建好后，可以看到目录 */var/kerberos/krb5kdc* 下生成了几个文件：



1. 添加database administrator

我们需要为Kerberos database添加administrative principals (即能够管理database的principals) —— 至少要添加1个principal来使得Kerberos的管理进程kadmind能够在网络上与程序kadmin进行通讯。

在maste KDC上执行：

/usr/sbin/kadmin.local -q "addprinc admin/admin"

提示输入密码，同样的这里的密码要牢记。

在master KDC上启动Kerberos daemons

在KDC server上必须运行的daemons是krb5kdc 和kadmin，它们可以被设置为自动启动：

[root@n1 ~]# /sbin/chkconfig krb5kdc on

[root@n1 ~]# /sbin/chkconfig kadmin on

也可以手动启动：

[root@n1 ~]# /etc/rc.d/init.d/krb5kdc start

[root@n1 ~]# /etc/rc.d/init.d/kamdin start

显示[OK]，启动成功，现在KDC已经在工作了。这两个daemons将会在后台运行，可以查看它们的日志文件（/var/log/krb5kdc.log 和 /var/log/kadmind.log）。

可以通过命令kinit来检查这两个daemons是否正常工作。

[root@n1 ~]# kinit admin/admin

Password for admin/admin@CDH.COM:

[root@n1 ~]# klist

Ticket cache: FILE:/tmp/krb5cc\_0

Default principal: admin/admin@CDH.COM

Valid starting Expires Service principal

07/01/16 14:23:59 07/02/16 14:23:59 krbtgt/CDH.COM@CDH.COM

renew until 07/01/16 14:23:59

[root@n1 ~]# kdestroy

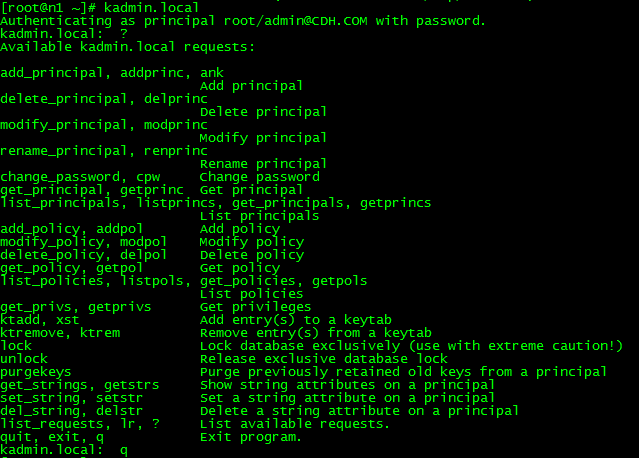
[root@n1 ~]# klist

klist: No credentials cache found (ticket cache FILE:/tmp/krb5cc\_0)

[root@n1 ~]#

到这一步，linux上面的Kerberos已经部署好了，下面就是在CDH 5.x上面启用Kerberos

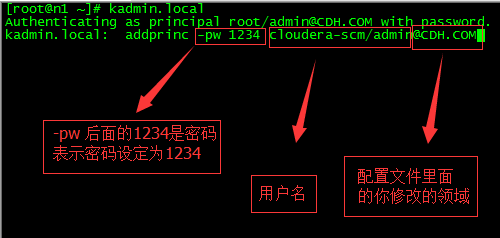
在本机kdc上输入kadmin.local 可以进入kadmin.local命令



1. **创建Cloudera Manager Principal**

为了能在集群中创建和部署host principals和keytabs，Cloudera Manager Server必须有一个Kerberos principal来创建其他的账户。如果一个principal的名字的第二部分是admin（例如， username/admin@CDH.COM ），那么该principal就拥有administrative privileges。

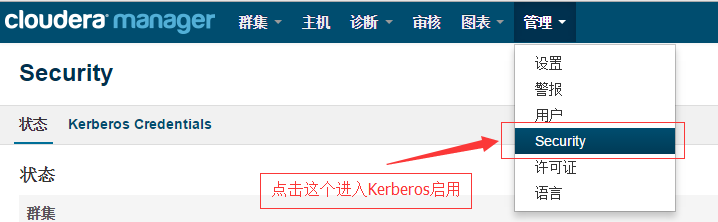
在KDC server主机上，创建一个名为『cloudera-scm』的principal，并将其密码设为『1234』(这里设置的密码简单，不建议设置简单的密码，这里仅是测试，写的简单密码容易遭到密码猜测攻击，相关缺点见Kerberos简介文档)。执行命令：

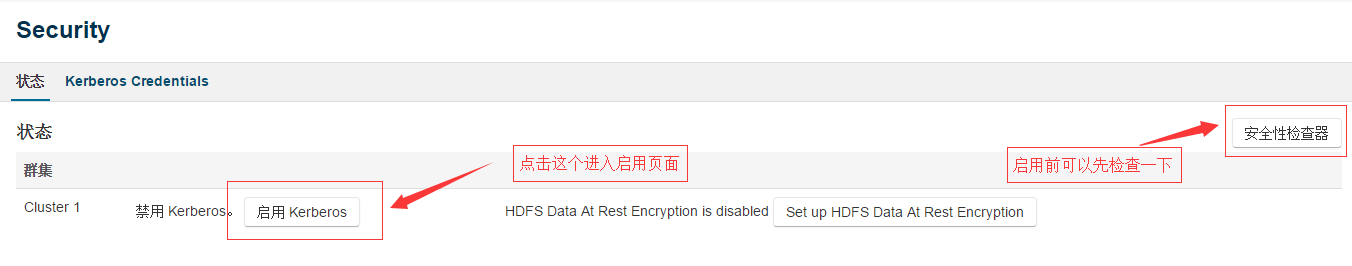


看到 Principal "cloudera-scm/admin@CDH.COM" created. 表示创建成功

输入 listprincs 可以看到已经创建的用户

1. **通过CDH 来启用Kerberos**













后面基本上继续，这样CDH启用Kerberos就成功了！