## [Kerberos安装及使用](http://www.cnblogs.com/xiaodf/p/5968178.html)

转载请注明出处：<http://www.cnblogs.com/xiaodf/>

**2. 安装 Kerberos**  
**2.1. 环境配置**  
　　安装kerberos前，要确保主机名可以被解析。

　　主机名 内网IP 角色

Vmw201 172.16.18.201 Master KDC

Vmw202 172.16.18.202 Kerberos client

Vmw203 172.16.18.203 Kerberos client

**2.2 Configuring a Kerberos Server**  
**2.2.1 确保环境可用**  
　　确保所有的clients与servers之间的时间同步以及DNS正确解析

**2.2.2 选择一个主机来运行KDC，并在该主机上安装krb-5libs,krb5-server,已经krb5-workstation:**

|  |  |
| --- | --- |
| 1 | yum install krb5-server krb5-libs krb5-auth-dialog |

　　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vmw201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。

**2.2.3 配置kdc.conf**  
默认放在 /var/kerberos/krb5kdc/kdc.conf。或者通过覆盖KRB5\_KDC\_PROFILE环境变量修改配置文件位置。  
配置示例：

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13 | [kdcdefaults]  kdc\_ports = 88  kdc\_tcp\_ports = 88    [realms]  HADOOP.COM = {  #master\_key\_type = aes256-cts  acl\_file = /var/kerberos/krb5kdc/kadm5.acl  dict\_file = /usr/share/dict/words  admin\_keytab = /var/kerberos/krb5kdc/kadm5.keytab  max\_renewable\_life = 7d  supported\_enctypes = aes128-cts:normal des3-hmac-sha1:normal arcfour-hmac:normal des-hmac-sha1:normal des-cbc-md5:normal des-cbc-crc:normal  } |

说明：  
HADOOP.COM:是设定的realms。名字随意。Kerberos可以支持多个realms，会增加复杂度。本文不探讨。大小写敏感，一般为了识别使用全部大写。这个realms跟机器的host没有大关系。  
max\_renewable\_life = 7d 涉及到是否能进行ticket的renwe必须配置。  
master\_key\_type:和supported\_enctypes默认使用aes256-cts。由于，JAVA使用aes256-cts验证方式需要安装额外的jar包，更多参考2.2.9关于AES-256加密：。推荐不使用。  
acl\_file:标注了admin的用户权限。文件格式是   
Kerberos\_principal permissions [target\_principal] [restrictions]支持通配符等。  
admin\_keytab:KDC进行校验的keytab。后文会提及如何创建。  
supported\_enctypes:支持的校验方式。注意把aes256-cts去掉。

**2.2.4 配置krb5.conf**  
/etc/krb5.conf: 包含Kerberos的配置信息。例如，KDC的位置，Kerberos的admin的realms 等。需要所有使用的Kerberos的机器上的配置文件都同步。这里仅列举需要的基本配置。  
配置示例：

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23 | [logging]  default=FILE:/var/log/krb5libs.log  kdc = FILE:/var/log/krb5kdc.log  admin\_server = FILE:/var/log/kadmind.log    [libdefaults]  default\_realm = HADOOP.COM  dns\_lookup\_realm = false  dns\_lookup\_kdc = false  ticket\_lifetime = 24h  renew\_lifetime = 7d  forwardable = true  # udp\_preference\_limit = 1    [realms]  HADOOP.COM = {  kdc = vmw201  admin\_server = vmw201  }    [domain\_realm]  .hadoop.com = HADOOP.COM  hadoop.com = HADOOP.COM |

说明：  
[logging]：表示server端的日志的打印位置  
[libdefaults]：每种连接的默认配置，需要注意以下几个关键的小配置  
default\_realm = HADOOP.COM 默认的realm，必须跟要配置的realm的名称一致。  
udp\_preference\_limit = 1 禁止使用udp可以防止一个Hadoop中的错误  
oticket\_lifetime表明凭证生效的时限，一般为24小时。  
orenew\_lifetime表明凭证最长可以被延期的时限，一般为一个礼拜。当凭证过期之后，   
对安全认证的服务的后续访问则会失败。  
[realms]:列举使用的realm。  
kdc：代表要kdc的位置。格式是 机器:端口  
admin\_server:代表admin的位置。格式是机器:端口  
default\_domain：代表默认的域名  
[appdefaults]:可以设定一些针对特定应用的配置，覆盖默认配置。

**2.2.5 创建/初始化Kerberos database**  
初始化并启动：完成上面两个配置文件后，就可以进行初始化并启动了。

|  |  |
| --- | --- |
| 1 | [root@vmw201 ~]# /usr/sbin/kdb5\_util create -s -r HADOOP.COM |

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。

# 保存路径为/var/kerberos/krb5kdc 如果需要重建数据库，将该目录下的principal相关的文件删除即可

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  2  3  4  5  6 | kadm5.acl  kdc.conf  principal  principal.kadm5  principal.kadm5.lock  principal.ok |

**2.2.6 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：

|  |  |
| --- | --- |
| 1 | [root@vmw201 /]# /usr/sbin/kadmin.local -q "addprinc admin/admin" |

并为其设置密码

|  |  |
| --- | --- |
| 1 | kadmin.local |

可以直接运行在master KDC上，而不需要首先通过Kerberos的认证，实际上它只需要对本  
地文件的读写权限。

**2.2.7 为database administrator设置ACL权限**  
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。

我们现在为administrator设置权限：将文件/var/kerberos/krb5kdc/kadm5.acl的内容编辑为

|  |  |
| --- | --- |
| 1 | \*/admin@HADOOP.COM |

代表名称匹配\*/admin@HADOOP.COM 都认为是admin，权限是 \*。代表全部权限。

**2.2.8 在master KDC启动Kerberos daemons**  
手动启动：

|  |  |
| --- | --- |
| 1  2 | [root@vmw201 /]# service krb5kdc start  [root@vmw201 /]# service kadmin start |

设置开机自动启动：

|  |  |
| --- | --- |
| 1  2 | [root@vmw201 /]# chkconfig krb5kdc on  [root@vmw201 /]# chkconfig kadmin on |

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。

**2.2.9关于AES-256加密**  
对于使用 centos5. 6及以上的系统，默认使用 AES-256 来加密的。这就需要集群中的所有节点上安装 Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy File。  
下载的文件是一个 zip 包，解开后，将里面的两个文件放到下面的目录中：$JAVA\_HOME/jre/lib/security

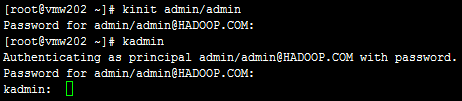
**2.3 Configuring Kerberos Clients**  
**2.3.1 Installing Kerberos Client(CentOS7可以省略此步骤)**  
在另外两台主机(vmw202,vmw203)上安装kerberos客户端。

|  |  |
| --- | --- |
| 1 | yum install krb5-workstation krb5-libs krb5-auth-dialog |

**2.3.2 配置krb5.conf**  
配置这些主机上的/etc/krb5.conf，这个文件的内容与KDC中的文件保持一致即可。

**3. kerberos的日常操作与常见问题**  
**3.1 管理员操作**  
**3.1.1 登录**  
登录到管理员账户: 如果在本机上，可以通过kadmin.local直接登录。其它机器的，先使用kinit进行验证。

IMG_256

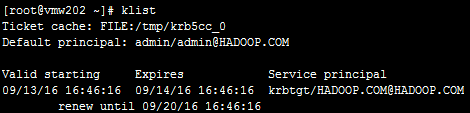


**3.1.2增删改查账户**  
在管理员的状态下使用addprinc,delprinc,modprinc,listprincs命令。使用?可以列出所有的命令。

|  |  |
| --- | --- |
| 1  2  3 | kadmin.local: addprinc test  kadmin.local: delprinc test  kadmin.local: listprincs |

**3.1.3生成keytab:使用xst命令或者ktadd命令**

|  |  |
| --- | --- |
| 1 | kadmin:xst -k /xxx/xxx/kerberos.keytab hdfs/hadoop1 |

**3.2 用户操作**  
**3.2.1 查看当前的认证用户**  


**3.2.3 认证用户**

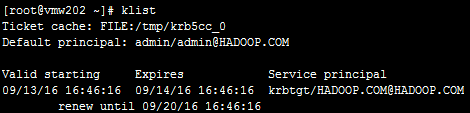
|  |  |
| --- | --- |
| 1 | kinit -kt /xx/xx/kerberos.keytab hdfs/hadoop1 |

**3.2.4 删除当前的认证的缓存**

|  |  |
| --- | --- |
| 1 | kdestroy |

3.3 常见问题  
**3.3.1 查看ticket是否是renewable**

通过klist命令来查看

  
如果Valid starting的值与renew until的值相同，则表示该principal的ticket 不是 renwable。

**3.3.2 ticket无法更新**  
如果过了Expires,可以通过命令kinit –R来更新ticket  
但如果ticket无法更新

|  |  |
| --- | --- |
| 1  2 | [root@vmw201 ~]$ kinit -R  kinit: Ticket expired while renewing credentials |

这是因为krbtgt/HADOOP.COM@ HADOOP.COM的[renewlife]被设置成了0，这一点可以通过[kadmin.local => getprinc krbtgt/ HADOOP.COM @ HADOOP.COM]看出来。

将krbtgt/HADOOP.COM@HADOOP.COM的[renewlife]修改为7days即可，方法

|  |  |
| --- | --- |
| 1 | kadmin.local: modprinc -maxrenewlife 1week krbtgt/HADOOP.COM@HADOOP.COM |