Kerberos简介

# 一、简介

Kerberos协议主要用于计算机网络的身份鉴别，其特点是用户只需要输入一次身份验证信息就可以凭借此验证获得票据（ticket-granting ticket）访问多个服务，即SSO（single sign on）。由于在每个Client和Service之间建立了共享密钥，使得该协议具有相当的安全性。使用Kerberos后，任意机器的任意用户都必须在Kerberos的KDC中有记录，才允许和集群中其他的模块进行通信。

使用Kerberos时，一个客户端需要经过三个步骤来获取服务：

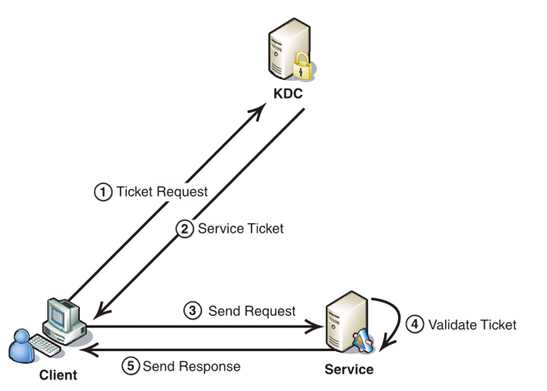
1）认证，客户端向认证服务器发送一条报文，并获取一个含时间戳的Ticket-Granting Ticket（TGT）

2）授权，客户端使用TGT向Ticket-Granting Server（TGS）请求一个服务Ticket。

3）服务请求，客户端向服务器出示服务Ticket，以证实自己的合法性

为此，Kerberos需要The Key Distributed Centers（KDC）来认证。KDC只是一个Master，可以带多个Slave机器。Slave机器仅进行普通验证，Master上的修改需要自动同步到Slaves。

Client首先向KDC发送自己的身份信息，KDC从Ticket Granting Service得到TGT，并用协议开始前Client与KDC之间的密钥将TGT加密回复给Client。此时只要真正的Client才能利用它与KDC之间的密钥将加密后的TGT解密，从而获得TGT。Client利用之前获得的TGT向KDC请求其他Service的Ticket，从而通过其他Service的身份鉴别：



1. Client将之前获得TGT和要请求的服务信息（服务名等）发送给KDC，KDC中的Ticket Granting Service将为Client和Service之间生成一个Session Key用于Service对Client的身份鉴别。然后KDC将这个Session key和（用户名，IP，服务名，有效期和时间戳）包装成一个Ticket发送给Service。不过Kerberos协议并没有直接将Ticket发送给Services，而是通过Client转发给Services
2. 此时KDC将刚才的Ticket转发给Client。由于这个Ticket是要给service的，不能Client看到，所以KDC用协议开始前KDC与sevice之间的密钥将Ticket加密后发送给Client。同时为了让Client和Service之间共享，KDC用Client与它之间的密钥将Session key加密随加密的Ticket一起返回给Client。
3. 为了完成Ticket的传递，Client将刚才收到的Ticket转发给Service，由于Client不知道KDC与Service之间的密钥，所有它无法篡改Ticket中的信息。同时Client将收到的Session key解密处理，然后将自己的用户名，用户地址打包成Authenticator用Session key加密也发送给Service。
4. Service收到Ticket后利用它与KDC之间的密钥将Ticket中的信息解密处理，从而获得Session key和用户名,IP,服务名,有效期。然后再用Session Key将Authenticator解密从而或得用户名将之前Ticket中解密的用户名,IP做比较从而验证Client的身份
5. 如果Service有返回结果，将其返回给Client。

Kerberos实现的是机器级别的安全认证，也就是服务到服务的认证，事先对集群中确定的集群由管理员手动添加到kerberos数据库中，在KDC上分别产生主机与各个节点的keytab（包含了host和对应节点的名字，还有他们之间的密钥），并将这些Keytab分发到对应的节点上。通过这些keytab文件，节点可以从KDC上获得与目标相同通信的密钥，进而被目标节点所认证，提供相应的服务，防止被冒充的可能性。当前Kerberos可以解决服务器到服务器，Client到服务的认证。

# 二、基本概念

KDC（key distributed center）: 负责分发密钥的密钥分配中心，提供ticket和临时会话密钥

AS（Authentication Server）:认证服务器

TSG（Ticket Granting Server）:许可证服务器

principal：安全个体，被认证的个体，有一个名字和口令

Ticket：一个记录，客户用它来向服务器证明自己的身份，包括客户标识、会话密钥、时间戳

# 三、Kerberos安装

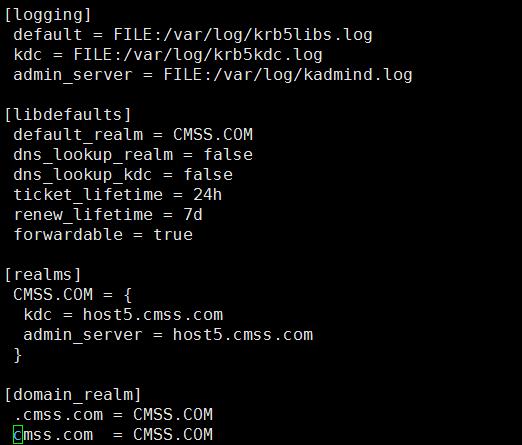
/etc/krb5.conf说明：

|  |  |  |
| --- | --- | --- |
| 参数域 | 参数 | 含义 |
| logging |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

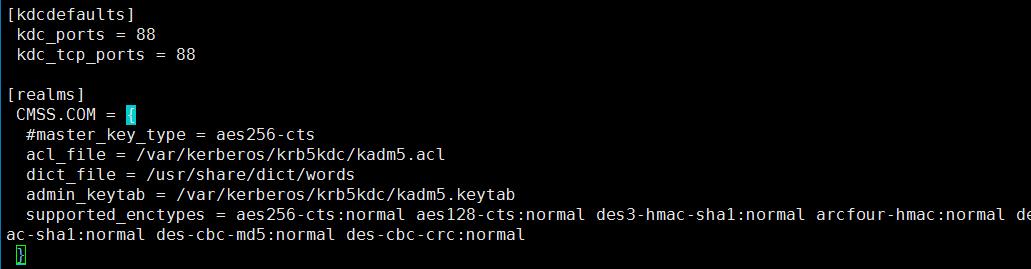
krb-server的安装：

yum -y install krb5-server krb5-workstation krb5-libs

配置/etc/krb5.conf及/var/kerberos/krb5kdb/kdc.conf，将EXAMPLE.COM修改成CMSS.COM，如下所示：krb5.conf



/var/kerberos/krb5kdb/kdc.conf



创建Kerberos realm数据库  
 kdb\_util create -s

在目录/var/kerberos/krb5kdc下生成5个文件：

principal principal.kadm5 principal.kadm5.lock principal.ok

配置/var/kerberos/krb5kdc/kadm5.acl，用于Kadmin命令确定哪些principlas拥有Kerberos数据库访问权，可以配置如下：

\*/admin@CMSS.COM \*

kerberos的启动：

service krb5kdc start

service kadmin start

检查KDC是否分发票据ticket，

通过命令：

/usr/sbin/kadmin.local

进入kerberos管理客户端，在kadmin中添加一条principal

进入客户端命令：

$kadmin

kadmin.local > addprinc {username} //添加一条principal，名字为{username}，密码：{enter}

通过

通过kinit命令，获取凭证：

kinit {principal} //默认是root@CMSS.COM，用户名@CMSS.COM

通过klist命令，查看缓存的principal

klist

结果如下：

Ticket cache: FILE:/tmp/krb5cc\_0

Default principal: root@CMSS.COM

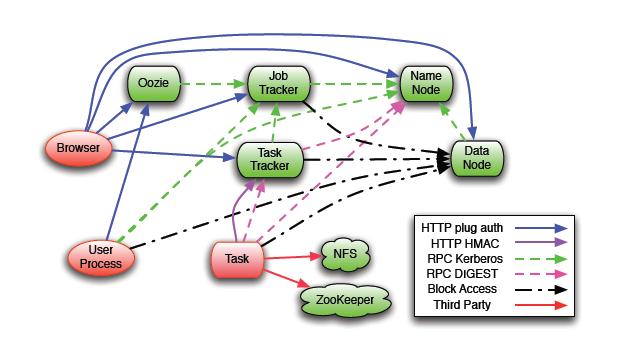
Valid starting Expires Service principal

06/07/15 15:10:07 06/08/15 15:10:01 krbtgt/CMSS.COM@CMSS.COM

renew until 06/07/15 15:10:07

# 四、Hadoop Kerberos配置及使用

hadoop集群内部使用Kerberos进行认证



具体执行过程可以举例如下：

