**Kerberos原理和单机安装**

原创 2015年06月25日 10:36:29

# Kerberos原理

Kerberos 服务是单点登录系统，这意味着您对于每个会话只需向服务进行一次自我验证，即可自动保护该会话过程中所有后续事务的安全。服务对您进行验证后，即无需在每次使用基于 Kerberos 的服务时进行验证。因此，无需在每次使用这些服务时都在网络上发送口令（增强了安全性）。MIT写了一段故事型的对话，比较生动得表述了Kerberos协议的工作原理：  
Athena和欧里庇得斯关于地狱之门守护者的对话。简而言之，kerbores V5的工作原理如下：  
Kerbores中有三种角色：  
KDC：负责分发密钥的密钥分配中心  
Client：需要使用kerbores服务的客户端  
Service：提供具体服务的服务端  
其中，Client需要和KDC和Service都进行通信。协议授权流程分两个部分：

## 获取原始票据

首先，Client向KDC发送自己的身份信息，KDC从授予票据服务(Ticket Granting Service)得到可用的票据(ticket-granting ticket)，并用协议开始前KDC与Client之间的密钥将票据加密回复给client，client收到KDC回复的加密票据后利用与client先前协议的密钥将票据解密，从而获得票据，此步骤主要是允许client进行Kerberos的验证，是进行访问服务的先决条件。

## 获取服务票据以及访问服务

client利用之前获得的票据向KDC请求服务票据，从而通过服务的身份验证。获取服务票据以及访问服务总共有如下四步：

①. client将之前获得的票据和要请求的服务信息发送给KDC，KDC中的授予票据服务将client和service之间生成一个会话密钥(Session Key)用于服务器与client的身份验证。然后KDC将这个会话密钥和用户名，用户地址(IP)，服务名，有效期，时间戳一起包装成一个票据(这张票据用于service对client的身份验证)通过client转发给service。

②. 为了让票据对client保密，所以KDC用协议开始之前KDC与服务端之间的密钥将票据加密后再发给client，同时为了让client与service之间共享那个会话密钥，KDC用client与它之间的密钥将会话密钥加密返回给client

③. 为了完成票据的传递，client将刚才收到的票据转发到service，由于client不知道KDC与service的密钥，所以它无法修改票据的信息，同时client将收到的会话密钥解压出来，然后将自己的用户名，用户地址(IP)打包成验证包用会话密钥加密也发给service  
  
④. Service收到票据后利用它与KDC之间的密钥将票据中的信息解密出来，从而获得会话密钥和用户名，用户地址(IP)，服务名，有效期。然后再用会话密钥将验证包解密从而获得用户名，用户地址(IP)将其与之前票据中解密出来的用户名，用户地址(IP)做比较从而验证client的身份，如果service有返回结果，将其返回给client.

# 安装步骤：

## 下载krb5-1.9.5

http://web.mit.edu/kerberos/dist/krb5/1.9/krb5-1.9.5-signed.tar

## 解压

tar -xvf krb5-1.9.5-signed.tar  
生成krb5-1.9.5.tar.gz 和 krb5-1.9.5.tar.gz.asc  
继续解压tar zxvf krb5-1.9.5.tar.gz

## 编译

cd krb5-1.9.5/src  
./configure  
make && make install  
  
也可以直接用yum 安装,redhat默认自带的 yum 源需要注册,也可以使用centos的yum源.  
wget http://mirrors.163.com/.help/CentOS6-Base-163.repo  
KDC server 安装 yum -y krb5-server  
客户端安装: yum -y krb5-workstation

## 配置/etc/krb5.conf

这个是Kerberos最主要的配置文件，而且一定要放在/etc下

[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

forwardable = yes

[realms]

HADOOP.COM = {

kdc = kdc.hadoop.com:88

admin\_server = kdc.hadoop.com:749

default\_domain = HADOOP.COM

}

[domain\_realm]

.hadoop.com = HADOOP.COM

hadoop.com = HADOOP.COM

## 配置/usr/local/var/krb5kdc/kdc.conf

由于上面安装时没有选择安装目录，所以默认的安装位置在/usr/local/var/krb5kdc  
如果是yum安装,位置在/var/kerberos/krb5kdc

[kdcdefaults]

kdc\_ports = 88

kdc\_tcp\_ports = 88

[realms]

HADOOP.COM = {

max\_renewable\_life = 7d

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

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

}

配置acl文件

## 创建一个kerberos数据库

kdb5\_util create -r HADOOP.COM -s    
会要求创建数据库的密码。（123456）,创建principal保存数据库文件

## 登录kerberos

kadmin.local     
1）查看用户  
listprincs  
  
2）添加用户  
addprinc admin/admin@HADOOP.COM  
(password:123456)

## 启动服务

service krb5kdc start

Starting Kerberos 5 KDC: [ OK ]

service kadmin start

Starting Kerberos 5 Admin Server: [ OK ]

## 验证principle

在其他主机上需要有相同的krb5.conf配置。  
kinit [admin/admin@HADOOP.COM](mailto:admin/admin@HADOOP.COM)

以下面的3台机器做ssh+kerberos测试：从client1登陆client2

KDC服务器: kdc.hadoop.com

client1.hadoop.com

client2.hadoop.com

KDC服务器的kdc.conf文件如下:

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

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

}

3台机器的hosts文件改为如下

192.168.88.88 kdc.hadoop.com

192.168.88.89 client1.hadoop.com

192.168.88.90 client2.hadoop.com

3台机器的/etc/krb5.conf文件如下:

[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

forwardable = yes

[realms]

KRBTEST.COM = {

kdc = kdc.hadoop.com:88

admin\_server = kdc.hadoop.com:749

default\_domain = HADOOP.COM

}

[domain\_realm]

.hadoop.com = HADOOP.COM

hadoop.com = HADOOP.COM

[appdefaults]

pam = {

debug = false

ticket\_lifetime = 36000

renew\_lifetime = 36000

forwardable = true

krb4\_convert = false

}

在kdc.hadoop.com执行下面的命令

addprinc yorker/admin

（password:123456）

在client1.hadoop.com执行下面的命令

kinit yorker/admin

kadmin yorker/admin

addprinc -randkey host/client1.hadoop.com

ktadd -k /etc/krb5.keytab host/client1.hadoop.com

Update the following values in /etc/ssh/sshd\_config

GSSAPIAuthentication yes

GSSAPICleanupCredentials yes

在client2.hadoop.com执行下面的命令

kinit yorker/admin

kadmin yorker/admin

addprinc -randkey host/client1.hadoop.com

ktadd -k /etc/krb5.keytab host/client1.hadoop.com

Update the following values in /etc/ssh/sshd\_config

GSSAPIAuthentication yes

GSSAPICleanupCredentials yes

在client1.hadoop.com和client2.hadoop.com上重启sshd

service sshd restart

在client1.hadoop.com上 su - yorker

kinit yorker

再执行下面的命令不用输入密码就可以登录到client2.hadoop.com

ssh client2.hadoop.com

其它一些命令

klist

kdestroy

klist -k -t /etc/krb5.keytab

ssh -v

# 官方文档:

http://web.mit.edu/kerberos/krb5-current/doc/admin/install\_kdc.html#install-and-configure-the-master-kdc