kerberos认证协议

Kerberos是一种网络认证协议，其设计目标是通过密钥系统为客户机 / 服务器应用程序提供强大的认证服务。

简介
使用Kerberos时，一个客户端需要经过三个步骤来获取服务:

- 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）。
- 授权：客户端使用TGT向Ticket-Granting Server（TGS）请求一个服务Ticket。
- 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。该服务器提供客户端所需服务，在Hadoop应用中，服务器可以是namenode或jobtracker。

为此，Kerberos需要The Key Distribution Centers（KDC）来进行认证。KDC只有一个Master，可以带多个slaves机器。slaves机器仅进行普通验证。Mater上做的修改需要自动同步到slaves。

另外，KDC需要一个admin，来进行日常的管理操作。这个admin可以通过远程或者本地方式登录。

搭建Kerberos

环境说明：3台服务器，vrv145、vrv147、vrv148

主机	组件
vrv145	slave
vrv147	slave
vrv148	master slave

- vrv148 上执行
  `yum install krb5-libs krb5-server krb5-workstation`
- vrv145 及 vrv147 上执行
  `yum install krb5-libs krb5-workstation`

服务配置

修改/etc/krb5.conf文件

设置default_realm

```
    default_realm = me
```

添加realms

```
    me = {
      kdc = 192.168.118.148:88
      admin_server = 192.168.118.148:88
    }
```

修改/var/kerberos/krb5kdc/kdc.conf

设置realms，域对应为krb5.conf中default_realm的配置

```
    me = {
     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 = 10d
     supported_enctypes = aes128-cts:normal des3-hmac-sha1:normal arcfour-hmac:normal camellia256-cts:normal camellia128-cts:norma
    }
```

修改/var/kerberos/krb5kdc/kadm5.acl

添加kadmin账号,*me*为krb5.conf中配置的defaul_realm

```
    */admin@me    *
```

创建kerberos数据库

在master服务器上执行以下命令

```
    kdb5_util create -r me -s
```

执行完毕后会在/var/kerberos/krb5kdc下生成几个principal文件

创建管理员账号

在master服务器上执行以下命令

```
    kadmin.local -q "addprinc root/admin@me"
```

测试kerberos服务

启动kerberos服务

```
    systemctl krb5kdc start
    systemctl kadmin start
```

用户登录

```
    kinit root/admin
```

验证登录

```
    [root@vrv148 ~]# klist
    Ticket cache: KEYRING:persistent:0:0
    Default principal: root/admin@me

    Valid starting       Expires              Service principal
    09/13/2017 15:19:27  09/14/2017 15:19:27  krbtgt/me@me
```

添加账号

```
    [root@vrv148 ~]# kadmin -q "addprinc test2"
    Authenticating as principal root/admin@me with password.
    Password for root/admin@me:
    kadmin:  addprinc test2
    WARNING: no policy specified for test2@me; defaulting to no policy
    Enter password for principal "test2@me":
    Re-enter password for principal "test2@me":
    Principal "test2@me" created.
```

新建测试账号登录

```
    [root@vrv148 ~]# kinit test2
    Password for test2@me:
    [root@vrv148 ~]# klist
    Ticket cache: KEYRING:persistent:0:krb_ccache_pSsVgHm
    Default principal: test2@me

    Valid starting       Expires              Service principal
    09/13/2017 15:24:33  09/14/2017 15:24:33  krbtgt/me@me
```

导出票据文件

```
kadmin:  xst -k /home/vrv/test.keytab test
Entry for principal test with kvno 5, encryption type aes128-cts-hmac-sha1-96 added to keytab WRFILE:/home/vrv/test.keytab.
...
Entry for principal test with kvno 5, encryption type des-cbc-md5 added to keytab WRFILE:/home/vrv/test.keytab.or principal te
```

使用票据免秘钥登录

- 查看票据信息

```
[root@vrv148 ~]# ktutil
ktutil:  rkt /home/vrv/test.keytab
ktutil:  list
slot KVNO Principal
---- ---- ---------------------------------------------------------------------
   1    5                                 test@me
   2    5                                 test@me
   3    5                                 test@me
   4    5                                 test@me
   5    5                                 test@me
   6    5                                 test@me
   7    5                                 test@me
```

- 使用票据登录

```
[root@vrv148 ~]# kinit -kt /home/vrv/test.keytab test@me
[root@vrv148 ~]# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_PFm0472
Default principal: test@me

Valid starting       Expires              Service principal
09/13/2017 15:31:30  09/14/2017 15:31:30  krbtgt/me@me
```

---

hadoop集群添加kerberos认证

以下均为为CDH版本配置说明

CDH配置

进入 管理->安全->kerberos凭据

- 开启kerberos认证
- 选择导入kerberos account manager凭据
  - 填写kadmin的管理员账号及密码
- 选择生成丢失kerberos凭据

hdfs开启kerberos

进入hdfs配置页面

- 修改hadoop.security.authentication为kerberos
- 修改hadoop.security.authorization为true
- 修改dfs.datanode.address为1004
- 修改dfs.datanode.http.address为1006

hbase开启kerberos

进入hbase配置页面

- 修改hbase.security.authentication为kerberos
- 修改hbase.security.authorization为true

zookeeper开启kerberos

进入zookeeper配置页面

- 修改 enableSecurity为true