Kerberos 基本安装与配置

1 选择一台机器运行KDC，安装Kerberos相关服务

```
[root@cent-1 ~]# yum install -y krb5-server krb5-libs krb5-auth-dialog krb5-workstation
[root@cent-1 ~]# rpm -qa | grep krb5
krb5-workstation-1.10.3-57.el6.x86_64
krb5-libs-1.10.3-57.el6.x86_64
krb5-devel-1.10.3-57.el6.x86_64
krb5-server-1.10.3-57.el6.x86_64
krb5-auth-dialog-0.13-5.el6.x86_64
```

2 配置Kerberos，包括krb5.conf和kdc.conf，修改其中的realm，把默认的EXAMPLE.COM修改为自己要定义的值,详细参考https://github.com/WZQ1397/automatic-repo/salt下krb5的配置文件

```
[root@cent-1 ~]# cat /etc/krb5.conf
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = ESGYN.COM
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true

[realms]
```

```
 ESGYN.COM = {
  kdc = kerberos.esgyn.com
  admin_server = kerberos.esgyn.com
 }

[domain_realm]
 .esgyn.com = ESGYN.COM
 esgyn.com = ESGYN.COM

[root@cent-1 ~]# cat /var/kerberos/krb5kdc/kdc.conf
[kdcdefaults]
 kdc_ports = 88
 kdc_tcp_ports = 88

[realms]
 ESGYN.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 = aes128-cts:normal des3-hmac-sha1:normal arcfour-hmac:normal des-hmac-sha1:normal des-cbc-md5:norm
 }
```

3 创建Kerberos数据库，其中需要设置管理员密码，创建完成会在/var/kerberos/krb5kdc/下面生成一系列文件，若重建数据库则需先删除/var/kerberos/krb5kdc下面principal相关文件

```
[root@cent-1 ~]# /usr/sbin/kdb5_util create -s
Loading random data
Initializing database '/var/kerberos/krb5kdc/principal' for realm 'ESGYN.COM',
master key name 'K/M@ESGYN.COM'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
```

```
Enter KDC database master key:
Re-enter KDC database master key to verify:

[root@cent-1 ~]# ll /var/kerberos/krb5kdc/
total 24
-rw-------. 1 root root   22 Mar  9  2016 kadm5.acl
-rw-------. 1 root root  403 Jan 13 10:18 kdc.conf
-rw-------. 1 root root 8192 Jan 13 10:23 principal
-rw-------. 1 root root 8192 Jan 13 10:23 principal.kadm5
-rw-------. 1 root root    0 Jan 13 10:23 principal.kadm5.lock
-rw-------. 1 root root    0 Jan 13 10:24 principal.ok
```

4 添加数据库管理员，注意kadmin.local可以直接运行在KDC上，而无需通过Kerberos认证

```
[root@cent-1 ~]# /usr/sbin/kadmin.local -q "addprinc admin/admin"
Authenticating as principal centos/admin@ESGYN.COM with password.
WARNING: no policy specified for admin/admin@ESGYN.COM; defaulting to no policy
Enter password for principal "admin/admin@ESGYN.COM":
Re-enter password for principal "admin/admin@ESGYN.COM":
Principal "admin/admin@ESGYN.COM" created.
[root@cent-1 ~]# kadmin.local
Authenticating as principal centos/admin@ESGYN.COM with password.
kadmin.local:  listprinc
kadmin.local: Unknown request "listprinc".  Type "?" for a request list.
kadmin.local:  listprincs
K/M@ESGYN.COM
admin/admin@ESGYN.COM
kadmin/admin@ESGYN.COM
kadmin/cent-1.novalocal@ESGYN.COM
kadmin/changepw@ESGYN.COM
krbtgt/ESGYN.COM@ESGYN.COM
```

5 给数据库管理员添加ACL权限，修改kadm5.acl文件，*代表全部权限

```
[root@cent-1 ~]# cat /var/kerberos/krb5kdc/kadm5.acl
*/admin@ESGYN.COM    *
```

6 启动Kerberos进程并设置开机启动，通过/var/log/krb5kdc.log 和 /var/log/kadmind.log查看日志，通过kinit检查Kerberos正常运行

```
[root@cent-1 ~]# service krb5kdc start
Starting Kerberos 5 KDC:                                   [  OK  ]
[root@cent-1 ~]# service kadmin start
Starting Kerberos 5 Admin Server:                          [  OK  ]
[root@cent-1 ~]# service krb5kdc status
krb5kdc (pid  25980) is running...
[root@cent-1 ~]# service kadmin status
kadmind (pid  26017) is running...
[root@cent-1 ~]# chkconfig krb5kdc on
[root@cent-1 ~]# chkconfig kadmin on

[root@cent-1 krb5kdc]# kinit trafodion
Password for trafodion@ESGYN.COM:
[root@cent-1 krb5kdc]#
```

7 配置JCE，这是因为CentOS6.5及以上系统默认使用AES-256加密，因此需要所有节点安装并配置JCE，JCE下载路径: http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

```
[root@cent-1 UnlimitedJCEPolicyJDK8]# ll
total 16
-rw-rw-r--. 1 root root 3035 Dec 21  2013 local_policy.jar
-rw-r--r--. 1 root root 7323 Dec 21  2013 README.txt
-rw-rw-r--. 1 root root 3023 Dec 21  2013 US_export_policy.jar
```

```
[root@cent-1 security]# cp /home/centos/UnlimitedJCEPolicyJDK8/ /usr/java/jdk1.8.0_11/jre/lib/security/
local_policy.jar      README.txt            US_export_policy.jar
[root@cent-1 security]# cp /home/centos/UnlimitedJCEPolicyJDK8/US_export_policy.jar /usr/java/jdk1.8.0_11/jre/lib/securi
cp: overwrite `/usr/java/jdk1.8.0_11/jre/lib/security/US_export_policy.jar'? y
```

8 到此，Kerberos服务端已搭好，现在选择另外一台机器安装客户端，包括安装及配置/etc/krb5.conf与KDC相同

```
[root@cent-2 ~]# yum install -y krb5-workstation krb5-libs krb5-auth-dialog
```

9 kadmin生成keytab，如果是KDC上面直接运行kadmin.local,如果是在客户端先kinit再kadmin

(1)KDC

```
[root@cent-1 ~]# kadmin.local
Authenticating as principal trafodion/admin@ESGYN.COM with password.
kadmin.local:  listprincs
K/M@ESGYN.COM
kadmin/admin@ESGYN.COM
kadmin/cent-1.novalocal@ESGYN.COM
kadmin/changepw@ESGYN.COM
krbtgt/ESGYN.COM@ESGYN.COM
trafodion@ESGYN.COM
kadmin.local:  xst -k /opt/trafodion.keytab trafodion
Entry for principal trafodion with kvno 2, encryption type aes128-cts-hmac-sha1-96 added to keytab WRFILE:/opt/trafodior
Entry for principal trafodion with kvno 2, encryption type des3-cbc-sha1 added to keytab WRFILE:/opt/trafodion.keytab.
Entry for principal trafodion with kvno 2, encryption type arcfour-hmac added to keytab WRFILE:/opt/trafodion.keytab.
Entry for principal trafodion with kvno 2, encryption type des-hmac-sha1 added to keytab WRFILE:/opt/trafodion.keytab.
Entry for principal trafodion with kvno 2, encryption type des-cbc-md5 added to keytab WRFILE:/opt/trafodion.keytab.

[root@cent-1 opt]# ll /opt/trafodion.keytab
-rw-------. 1 root root 279 Jan 13 13:05 /opt/trafodion.keytab
```

(2)Client(需先kinit)

```
[root@cent-2 ~]# kinit kadmin/admin
Password for kadmin/admin@ESGYN.COM:
[root@cent-2 ~]# kadmin
Authenticating as principal kadmin/admin@ESGYN.COM with password.
Password for kadmin/admin@ESGYN.COM:
kadmin:  addprinc centos
WARNING: no policy specified for centos@ESGYN.COM; defaulting to no policy
Enter password for principal "centos@ESGYN.COM":
Re-enter password for principal "centos@ESGYN.COM":
Principal "centos@ESGYN.COM" created.
kadmin:  listprincs
K/M@ESGYN.COM
centos@ESGYN.COM
kadmin/admin@ESGYN.COM
kadmin/cent-1.novalocal@ESGYN.COM
kadmin/changepw@ESGYN.COM
krbtgt/ESGYN.COM@ESGYN.COM
trafodion@ESGYN.COM
```

10 kinit -kt认证用户，klist查看当前认证用户

```
[root@cent-2 ~]# kinit -kt /opt/trafodion.keytab trafodion
[root@cent-2 ~]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: trafodion@ESGYN.COM

Valid starting     Expires            Service principal
01/13/17 13:35:41  01/14/17 13:35:41  krbtgt/ESGYN.COM@ESGYN.COM
        renew until 01/13/17 13:35:41
```

1.默认安装路径为 /etc/krb5kdc
etc/krb5.conf
 |
  -- etc/krb5kdc/kdc.conf

etc/krb5.conf
[kdc] kdc位置
[logging]日志位置
[libdefaults]默认域
[realms]　kerberos域，表示KDC所管辖的范围；

2.etc/krb5kdc/kadm5.acl 若没有此文件则自己创建

> */admin@LOCAL.DOMAIN　*

3.创建 kerberos 数据库
$ /usr/sbin/kdb5_util create -r LOCAL.DOMAIN -s

创建数据库到/etc/krb5kdc/principal

Principal 是由三个部分组成：名字（name），实例（instance），REALM（域）。比如一个标准的 Kerberos 的用户是：name/instance@REALM

4.登录 kerberos
`$ /usr/sbin/kadmin.local`

查看用户
`kadmin.local　：　listprincs`
添加用户
`kadmin.local　：　addprinc kadmin/admin@LOCAL.DOMAIN`
删除用户
`kadmin.local　：　delprinc kadmin/admin@LOCAL.DOMAIN`
创建keytable文件　生成 kadmin/admin kadmin/changepw 两个用户的 keytab 文件到 krb5kdc 目录
kadmin.local ：ktadd -k /etc/krb5kdc/kadm5.keytab kadmin/admin kadmin/changepw
注意：keytab 得与配置文件kdc.conf里面配置一致

5、重启krb5kdc和kadmind进程

```
/usr/sbin/kadmind
/usr/sbin/krb5kdc
```

6、运行kerberos

```
$ sudo /usr/sbin/krb5kdc
$ sudo /usr/sbin/kadmind
```

7、在KDC服务器上测试申请票据，测试票据请求

```
$ /usr/sbin/kadmin.local
$ kadmin.local: addprinc linlin@LOCAL.DOMAIN
提示创建密码，然后退出
$ su linlin
$ kinit  linlin@LOCAL.DOMAIN
$ klist
$ /usr/sbin/kadmin.local
$ kadmin.local: addprinc -randkey hdfs/LL-167@LOCAL.DOMAIN
ktadd -norandkey -k hdfs.keytab hdfs/LL-167
```

查看自己申请的票据