Directory-Kerby

Apache Kerby是基于Java的KDC实现，对Kerberos协议做了一些集成绑定

*Apache Kerby, as an Apache Directory sub project, is a Java Kerberos binding*

其关键特性包括：

* 继承Kerberos、PKI以及OAuth2 Token
* 与KDC服务器交互的Client API(包括应用可感知的获取TGT或Service Ticket接口)
* 基于Java实现一个可嵌入或者独立的KDC Server(Hadoop 3.0的MiniKDC应用该方案)
* 提供对JAAS、GSS-API和SASL框架的支持
* 可通过插件支持第三方身份认证服务

从上述特性可以看出，Java应用基于Kerby可以与KDC之间做更丰富的一些交互，例如在没有Kerby之前，TGT与Service Ticket的获取对应用都是透明无感知的，同时能够更好的支持第三方的身份认证服务。

# 安装和使用

1. 下载源代码并编译

*git clone https://github.com/apache/directory-kerby.git*

*cd directory-kerby*

*mvn clean package -Pdist -DskipTests*

在kerby-dist目录下生成kdc-dist,tool-dist及has-dist安装目录。kdc-dist的目录结构如下：

├── *bin //启动目录*

├── *conf //配置目录*

├── *lib //依赖jar包*

├── *log4j.propertie*s

├── *logs*

└── *README.txt*

1. 启动Simple KDC Server

*$bin/kdcinit.sh conf conf/ //第一次启动要进行初始化*

*$bin/start-kdc.sh conf/ data*

启动进程信息如下：

*# jps*

*28425 KerbyKdcServer*

*# netstat -anp|grep 28425*

*tcp6 0 0 :::88 :::\* LISTEN 28425/java*

1. 管理命令kadmin，命令执行如下：

*$bin/kadmin.sh conf/ -k conf/admin.keytab*

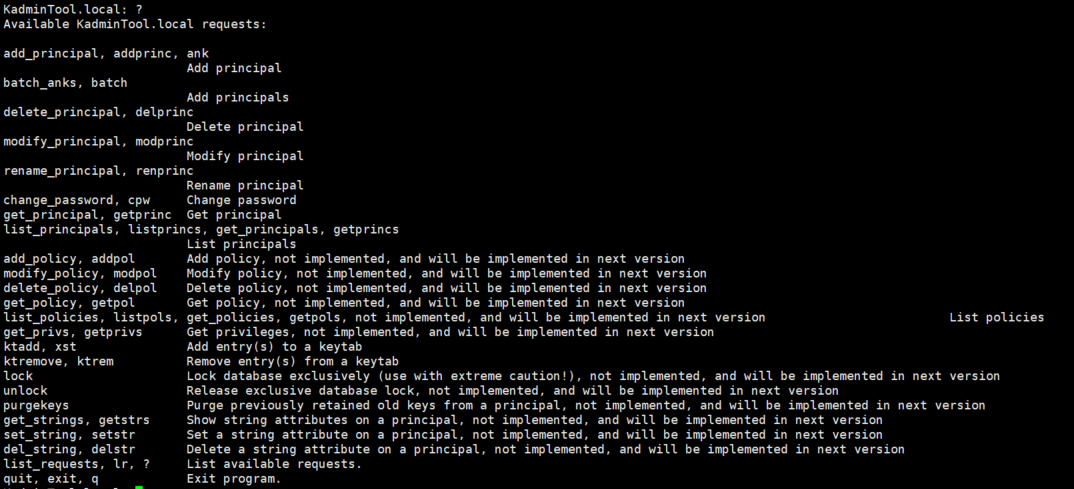
*principal is kadmin/EXAMPLE.COM@EXAMPLE.COM*

*Will use keytab*

*Commit Succeeded*

*KadminTool.local:*

kadmin支持krb5所有命令，如下所示：



* 添加principal

*KadminTool.local: addprinc kerby@EXAMPLE.COM*

*Enter password for principal "kerby@EXAMPLE.COM":*

*Re-enter password for principal "kerby@EXAMPLE.COM":*

*Principal "kerby@EXAMPLE.COM" created.*

*KadminTool.local: list\_principals*

*Principals are listed:*

*adminprotocol/localhost@EXAMPLE.COM*

*kadmin/EXAMPLE.COM@EXAMPLE.COM*

*kerby@EXAMPLE.COM*

*krbtgt/EXAMPLE.COM@EXAMPLE.COM*

*test@EXAMPLE.COM*

* 生成keytab文件

*KadminTool.local: xst -k /root/kerby.keytab kerby@EXAMPLE.COM*

*Export Keytab to /root/kerby.keytab*

在/root目录下回生成kerby.keytab文件

1. 创建keytab文件后，可以通过kinit命令获取许可票据，执行如下：

*cd tool-list*

*# bin/kinit.sh -conf conf/ kerby@EXAMPLE.COM*

*Password for kerby@EXAMPLE.COM:*

*Successfully requested and stored ticket in /tmp/krb5cc\_0*

查看TGT，信息如下：

*# bin/klist.sh*

*Ticket cache: /tmp/krb5cc\_0*

*Default principal: kerby@EXAMPLE.COM*

*Valid starting Expires Service principal*

*1969-12-31 16:00:00 2018-09-11 10:38:20 krbtgt/EXAMPLE.COM@EXAMPLE.COM*

*renew until 2018-09-13 09:38:20*

1. 数据存储目录，在backend.conf中配置了数据的存储，示例如下：

*kdc\_identity\_backend = org.apache.kerby.kerberos.kdc.identitybackend.JsonIdentityBackend*

*backend.json.dir = /tmp/kerby/jsonbackend*

数据使用JsonIdentityBackEnd，目录为/tmp/kerby/jsonbackend，打开目录包含文件：

*json-backend.json*

用于存储principal，文件内容如下（创建keyby principal的基本数据）：

*"kerby@EXAMPLE.COM": {*

*"principal": "kerby@EXAMPLE.COM",*

*"keyVersion": 1,*

*"kdcFlags": 0,*

*"disabled": false,*

*"locked": false,*

*"expireTime": "253402300799900",*

*"createdTime": "1536683036579",*

*"keys": {*

*"AES128\_CTS\_HMAC\_SHA1\_96": {*

*"kvno": 1,*

*"key": "3019A003020111A112041006CA8E59AE5EF0E4AD7B7B51FFBF3865"*

*},*

*"DES3\_CBC\_SHA1": {*

*"kvno": 1,*

*"key": "3021A003020110A11A0418C2896E4FF445FBBC1FE9A1EC7F61ADF1572AC75B94CD4C3B"*

*}*

*}*

*}*

# 执行流程分析

****

Ticket的描述类图如下所示：



https://blog.csdn.net/fjssharpsword/article/details/60571711

http://www.nosqlnotes.com/technotes/hadoop-kerby-has/

http://directory.apache.org/kerby/user-guide/1-how-to-begin.html

http://directory.apache.org/kerby/

<https://github.com/apache/directory-kerby>

<http://directory.apache.org/kerby/user-guide/2.1-krbclient-apis.html>

NettyKdcServerImpl

#NettyKdcHandler

#KdcHandler

#handleMessage

KdcContext

IdentityService

TgsRequest

AsRequest

TicketIssuer

TgtTicketIssuer

ServiceTicketIssuer

#default\_tgs\_enctypes = aes des3-cbc-sha1 rc4 des-cbc-md5

#default\_tkt\_enctypes = aes des3-cbc-sha1 rc4 des-cbc-md5