1、背景：

openLooKeng开启kerberos认证后，使用浏览器通过https访问openLooKeng，出现登录界面，提示输出用户名、密码，导致无法登录WEB UI。



2、原因分析：

常规认证方式如LDAP，采用的是用户名、密码认证，因此如果openLooKeng采用LDAP认证，在浏览器输出用户名、密码可完成认证并登录，但对于Kerberos认证，采用的是ticket的认证的方式，因此不管在浏览器输什么用户名、密码都无法认证通过。

3、解决方法：

配置浏览器使用ticker认证方式，不用传统的用户名、密码认证方式。

当前对于ticket认证方式支持比较好的是firefox浏览器，以下以firefox浏览器配置为例说明如何配置ticket认证，访问开启kerberos认证的openLooKeng服务。

1. 安装windows Kerberos客户端

Kerberos windows客户端叫KFW，下载地址：<http://web.mit.edu/kerberos/dist/index.html>，默认安装即可。默认情况会安装到C:\Program Files\MIT\Kerberos 路径，同时在C:\ProgramData\MIT\Kerberos5 路径下生成kerberos的配置文件krb5.ini 。

1. 配置kerberos客户端

配置环境变量：

KRB5\_CONFIG ------kerberos配置文件

KRB5CCNAME -------kerberos认证缓存文件路径



备注：重启系统，使配置生效

1. 配置浏览器

在浏览器输入about：config，搜索network.negotiate，配置如下图：

* network.negotiate-auth.delegation-uris、network.negotiate-auth.trusted-uris为coordinator的hostname
* network.negotiate-auth.gsslib 为KFW安装路径下gssapid的路径（根据浏览器是32位、64位选择对应文件）
* network.negotiate-auth.using-native-gsslib 修改为false
* network.negotiate-auth.allow-non-fqdn修改为true



搜索network.auth.use-sspi ，设置为false



1. 配置KFW

将KDC Server服务器上/ect/krb5.conf选中的内容，拷贝到krb5.ini文件中，生成KFW的配置文件



1. 完成认证

配置完成后，使用创建的用户认证（kerberos客户端或命令行）

使用Kerberos客户端：

 

使用命令行：



如果是机机用户，使用keytab认证



备注：

1. 在C:\Windows\System32\drivers\etc\hosts中增加KDC、coordinator节点hostname到IP的映射关系；
2. 使用KFW的kinit，不能使用java的kinit
3. 登录openLooKeng WEB UI

https://coordinator:9090 

备注：

1. 配置openLooKeng的config.properties中http.server.authentication.krb5.service-name 必须为HTTP；
2. 配置openLooKeng的config.properties中http.server.authentication.krb5.keytab的Principal为HTTP/HOSTNAME。（HOSTNAME为coordinator的主机hostname）