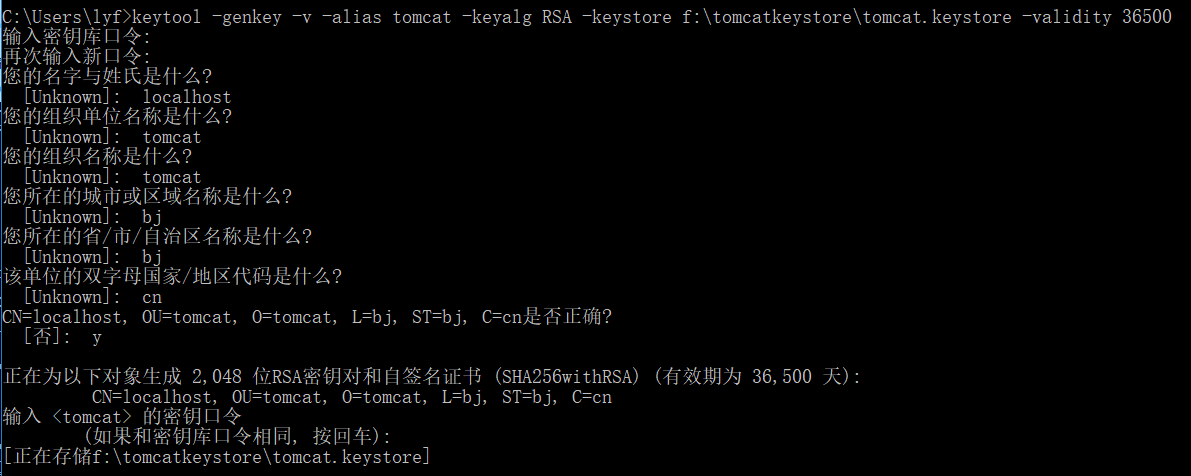
1. 双向认证
2. 一次性口令
3. 登录权限验证
4. 服务端密码加密存储
5. 建立会话机制

一、HTTPS协议的启用——双向认证

（1）启用HTTPS协议开启双向认证功能

1、生成服务器证书tomcat.keystore

keytool -genkey -v -alias tomcat -keyalg RSA -keystore f:\tomcatkeystore\tomcat.keystore -validity 36500



其中名字与姓氏必须为域名（localhost）

2、生成客户端client.p12

keytool -genkey -v -alias client1 -keyalg RSA -storetype PKCS12 -keysize 1024 -validity 365 -keystore "F:\tomcatkeystore\client1.p12"

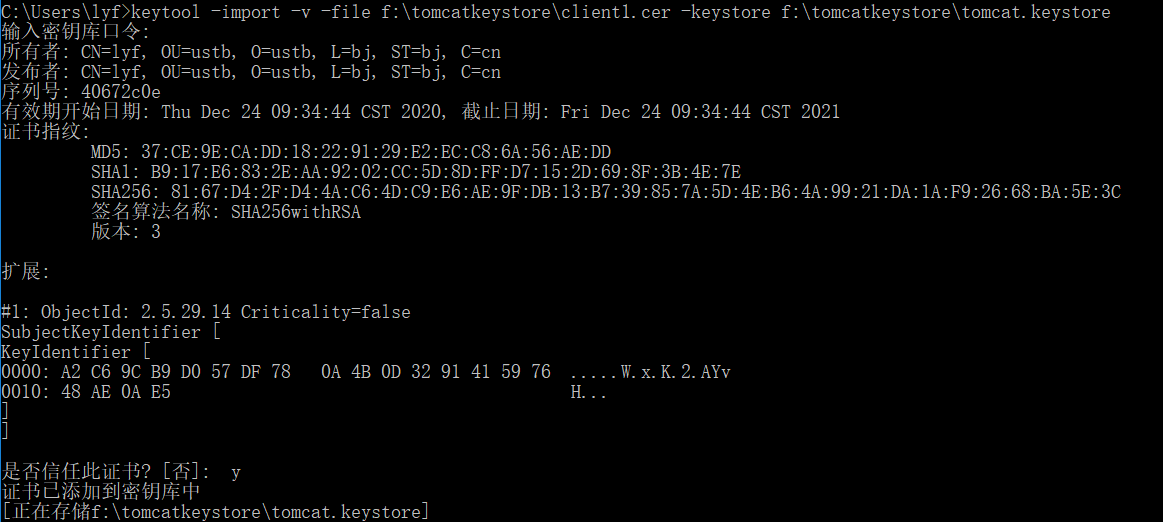


1. 将客户端p12证书格式导出成cer证书格式

keytool -export -alias client1 -storetype PKCS12 -keystore "F:\tomcatkeystore\client1.p12" -storepass tomcat -rfc -file "F:\tomcatkeystore\client1.cer"

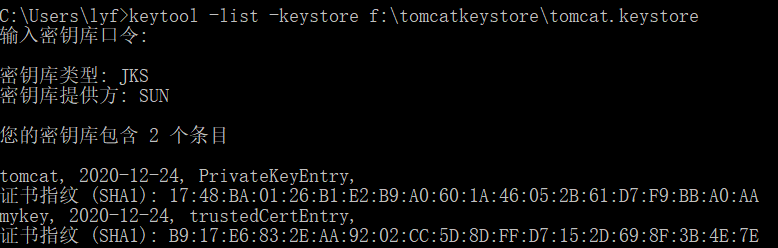
4、将客户端cer导入服务器证书库，添加为一个信任证书

keytool -import -v -file f:\tomcatkeystore\client1.cer -keystore f:\tomcatkeystore\tomcat.keystore



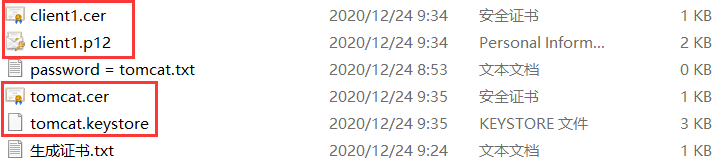
5、查看服务器的证书库，会发现有服务器和客户端两条证书条目

keytool -list -keystore f:\tomcatkeystore\tomcat.keystore

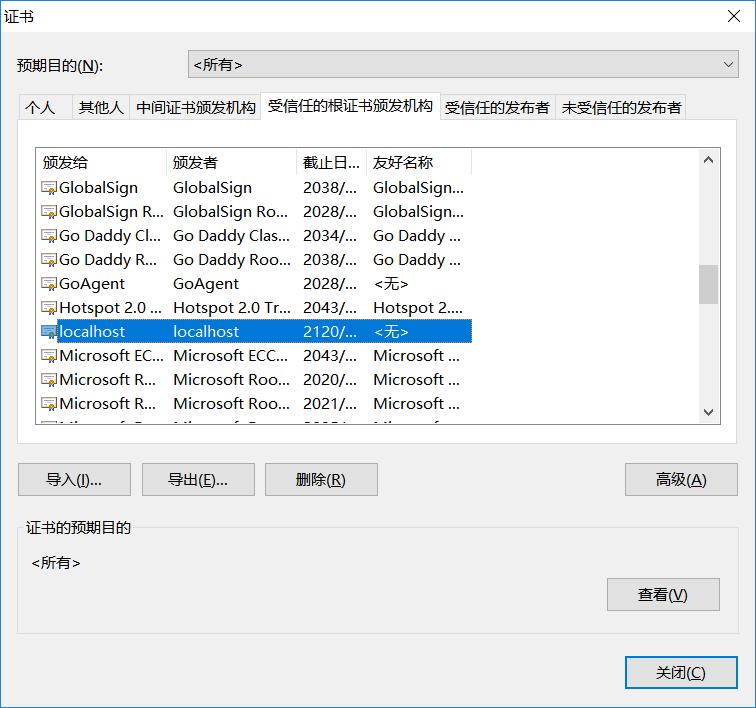
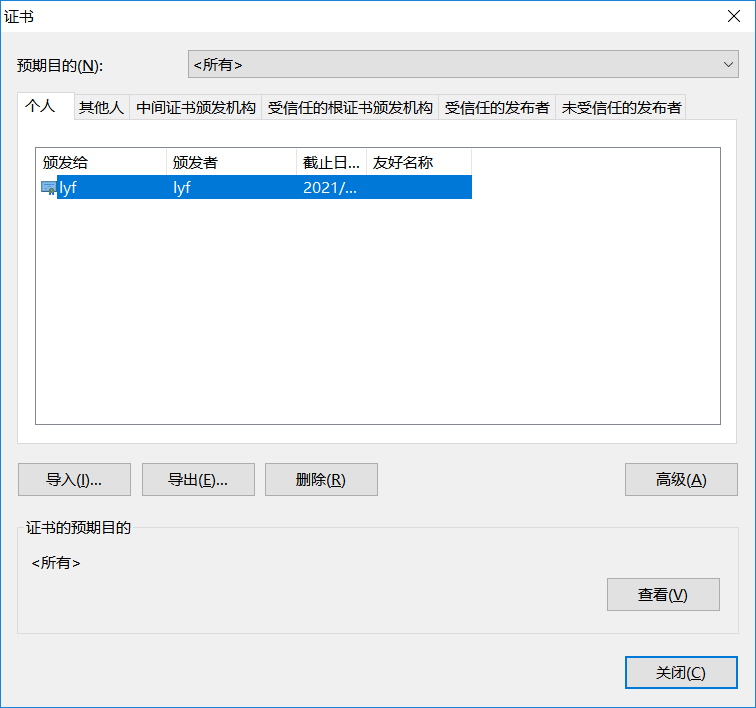


6、让客户端信任服务器证书导出服务器证书为cer

keytool -keystore f:\tomcatkeystore\tomcat.keystore -export -alias tomcat -file f:\tomcatkeystore\tomcat.cer

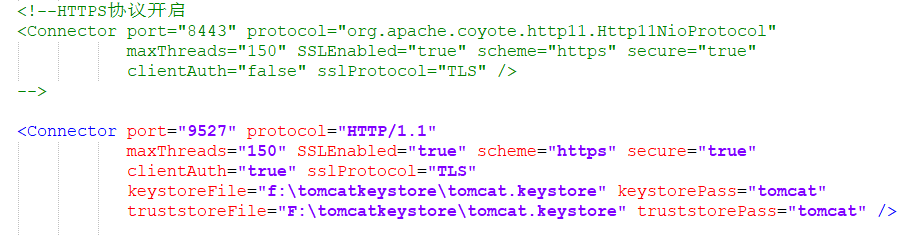


1. 安装client.p12到个人，tomcat.cer到受信任的根证书颁发机构，如下图所示。（左是客户端证书，右是服务端证书）

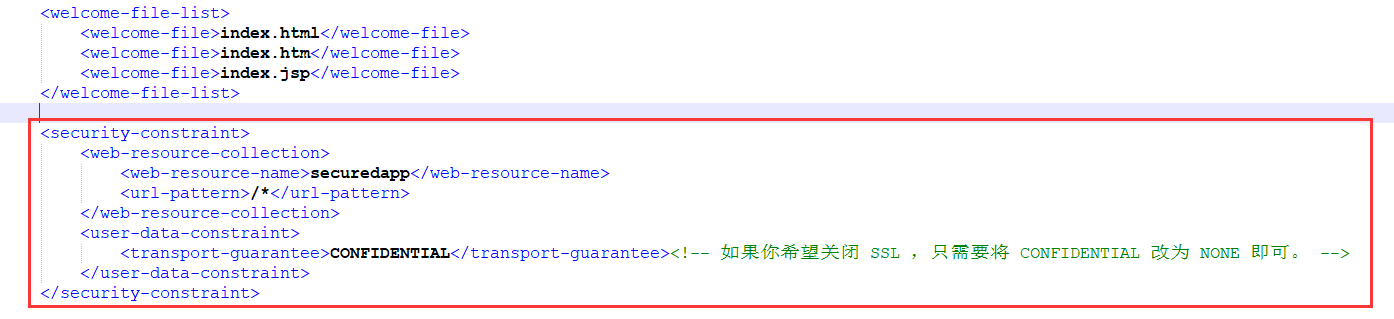


1. 配置tomcat

在tomcat目录下的conf/server.xml中开启HTTPS协议，将clientAuth设置为true，即开启双向认证，启用的是9527端口，添加服务器和客户端信任的证书，由于已经将客户端证书导入到了服务端中，所以一起只需用服务端证书一个即可。



配置conf/web.xml，添加如下内容，开启SSL。

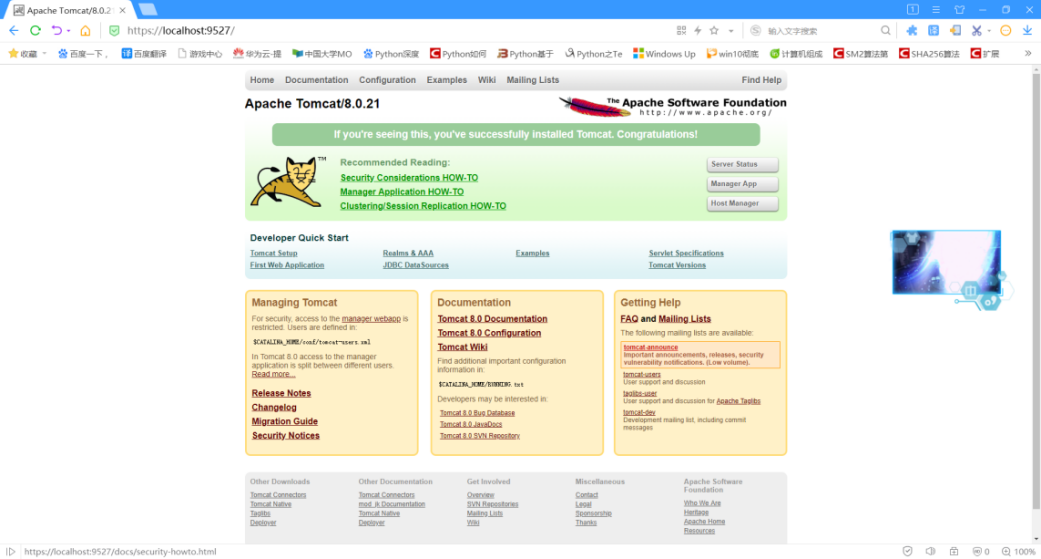


配置完成后，如果访问http://localhost:9527会拒绝连接。

访问https://localhost:9527，结果如下，会提示确认客户端证书。



点击确定后，进入tomcat主页面，此时就完成了双向认证。



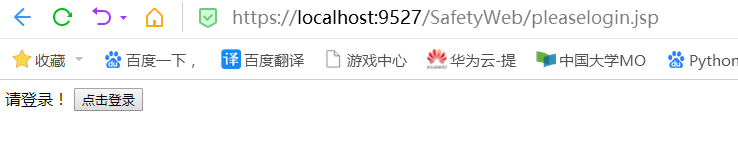
二、一次性口令

登录界面采用二维码验证功能。

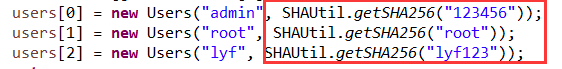


三、登录权限认证

未登录情况下直接访问users目录下的loginSuccess.jsp页面时会拦截提示登录。



四、服务器端用户密码加密存储



密码采用SHA256加密存储。

五、建立会话机制

登录成功后将用户信息保存到会话当中。



退出登录则清除会话中的用户信息。

