这节比较简单。

前面第一篇说道了配置HTTPS访问需要三件事：

1、生成keystore，keystore的域（CN，如果不知道CN是哪个，请参看<http://www.cnblogs.com/flying607/p/7598248.html#keystore>）要和客户端的配置的过滤器中的各个服务端地址的域保持一致，且不能是IP。

2、配置Tomcat使用该keystore来支持https

3、客户端的jre的证书仓库（cacerts）要加上该keystore生成的证书

如果我们的客户端就是要使用IP来访问服务端，怎么办？

答案就是配置成HTTP访问，如果你之前配置了HTTPS，那么步骤如下：

1、服务端的Tomcat改回普通的http Connector访问，比如用原来的8080端口配置方式。  
2、建议从客户端jre的证书仓库中删掉之前为做HTTPS单点登录加的那个证书：

keytool -delete -alias cas -keystore C:/Java/jdk1.8.0\_91/jre/lib/security/cacerts

做完这两步还不够，你会发现每个客户端的访问虽然都需要登录服务端，但是彼此的登录状态是不互通的。所以还有第三步

3、在application.properties里加上这么一句：

cas.tgc.secure=false

如果登录状态还是不互通，请清空浏览器的cookie，重开浏览器试试。

参考：<https://apereo.github.io/cas/5.1.x/installation/Configuration-Properties.html#ticket-granting-cookie>

如果你之前没配置HTTPS，就是用的HTTP，那么你只需要上文的第三步，也就是加个配置：cas.tgc.secure=false