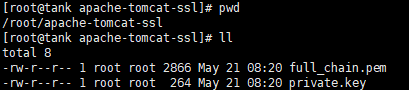
分析云配置https访问

1. **总览流程**



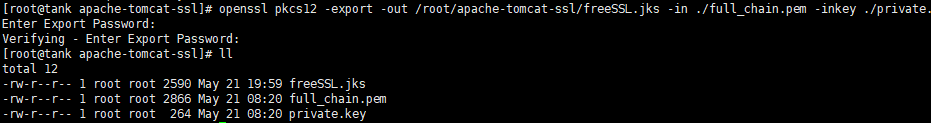
1. **pem转化为jks**

由于Tomcat证书不支持直接使用pem + 私钥的方式，因此，需要多一步使用Openssl将full\_chain.pem+private.key转换为jks的步骤，首先将full\_chain.pem和private.key放到一个任何目录，我存放的目录是：/root/apache-tomcat-ssl，如下图：



随后使用如下命令，在当前目录下生成一个名为freeSSL.jks的文件，如果使用不了如下命令，尝试考虑升级Openssl到最新版本：

openssl pkcs12 -export -out /root/apache-tomcat-ssl/freeSSL.jks -in ./full\_chain.pem -inkey ./private.key



命令过程中会要求输入keystore密码，两次确保一致，并记住该密码。

1. **自己生成jks**
   1. 使用jdk的keytool工具生成.keystore文件。

这一步可以在任意安装了jdk的机器上完成，打开命令行窗口，然后进入到jdk安装目录下的bin目录中，输入以下命令（需要按需修改）：

|  |
| --- |
| keytool -genkey -alias "10.2.108.37" -keypass "yonyou@1" -keyalg RSA -keysize 1024 -validity 365 -keystore "c:\10.2.108.37.keystore" |

* -alias "10.2.108.37"：指定别名，这里指定的是分析云服务的ip(10.2.108.37)。
* -keypass "yonyou@1"：自定义一个密钥密码，这里指定的是yonyou@1。
* -keyalg RSA：指定签名算法为RSA。
* -keysize 1024：指定密钥长度1024。
* -validity 365：指定有效期为365天。
* -keystore "c:\10.2.108.37.keystore"：指定生成的keystore文件的位置。

输入完成之后按回车，命令行会需要你指定密钥库密码，这个与上面命令中指定的密钥密码保持一致比较好，即yonyou@1。



完成之后会在c盘下生成10.2.108.37.keystore文件。

* 1. 导出crt证书。

继续在上一步的命令行窗口执行执行以下命令：

|  |
| --- |
| keytool -export -alias "10.2.108.37" -keystore "c:\10.2.108.37.keystore" -file "c:\10.2.108.37.crt" -storepass "yonyou@1" |

* + -alias "10.2.108.37"：别名部分要与上一步保持一致。
  + -keystore "c:\10.2.108.37.keystore"：指定上一步生成的keystore文件的位置。
  + -file "c:\10.2.108.37.crt"：指定要导出的证书文件位置。
  + -storepass "yonyou@1"：上一步操作中指定的密钥库密码。

输入完成后按回车，会在c盘下生成10.2.108.37.crt文件。

1. **在分析云部署服务器中配置**

首先将keystore文件上传到分析云服务器。

然后在分析云服务器上，找到分析云”conf/server.xml”，打开server.xml，在已有的<Connector>元素后再加如下一个<Connector>元素：

|  |
| --- |
| <Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"  maxThreads="200" SSLEnabled="true" scheme="https" secure="true"  clientAuth="false" sslProtocol="TLS"  keystoreFile="c:\10.2.108.37.keystore"  keystorePass="yonyou@1" /> |

注意：端口指定为443，keystoreFile指定该keystore文件路径（上传到的路径），keystorePass指定密钥密码（第1步设置的)。

另外此文件中其它几个<Connector>元素使用了8443端口的地方，都要将8443改为443。

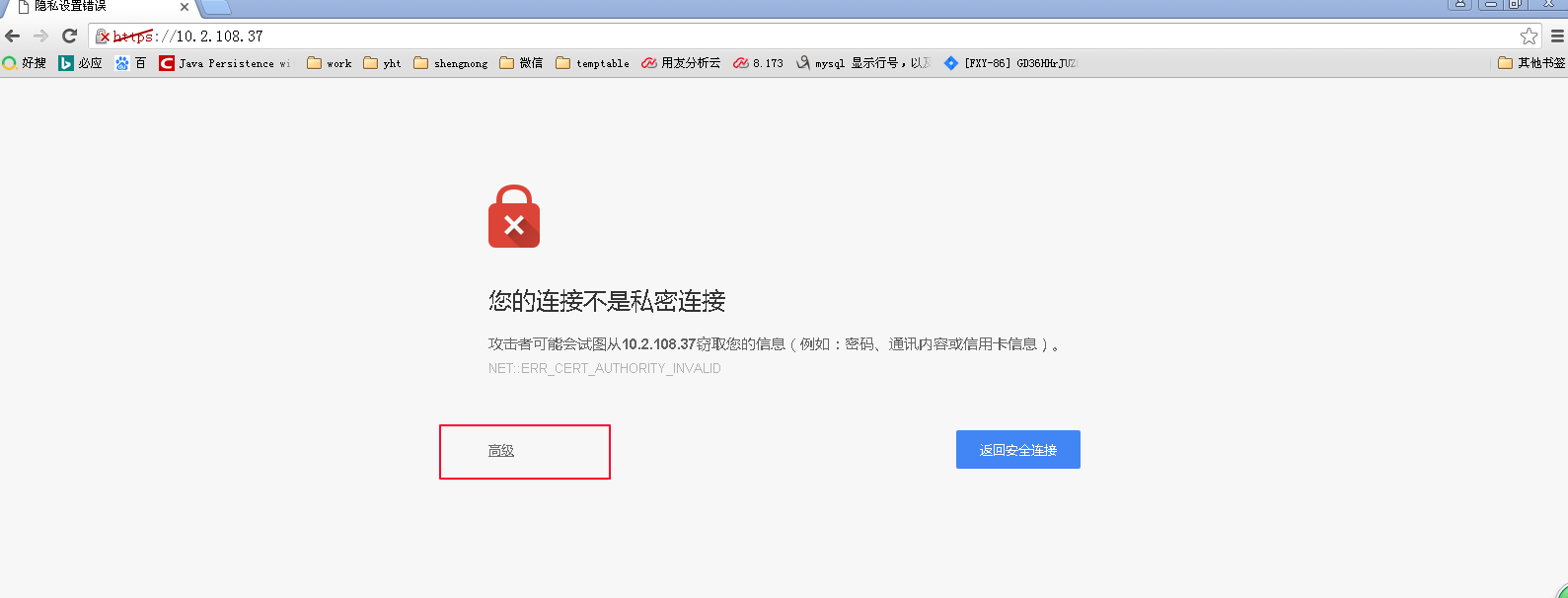
如果希望http自动转为https：编辑分析云下的/conf/web.xml文件，在其中添加如下代码：

|  |
| --- |
| <!-- 增加所有网址自动跳转https -->   <security-constraint>    <web-resource-collection>      <web-resource-name >SSL</web-resource-name>       <url-pattern>/\*</url-pattern>      </web-resource-collection>     <user-data-constraint>      <transport-guarantee>CONFIDENTIAL</transport-guarantee>     </user-data-constraint>  </security-constraint> |

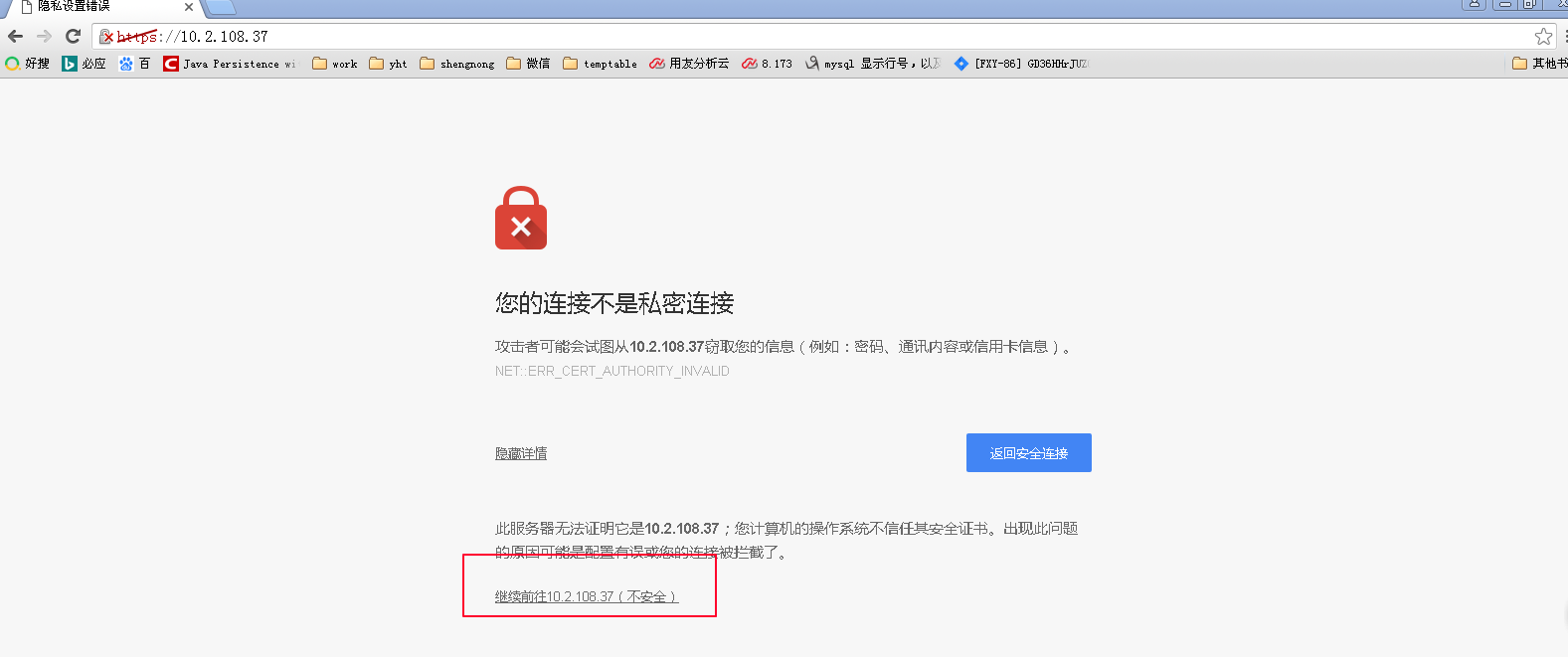
最后重启分析云服务。

1. **在客户端访问**

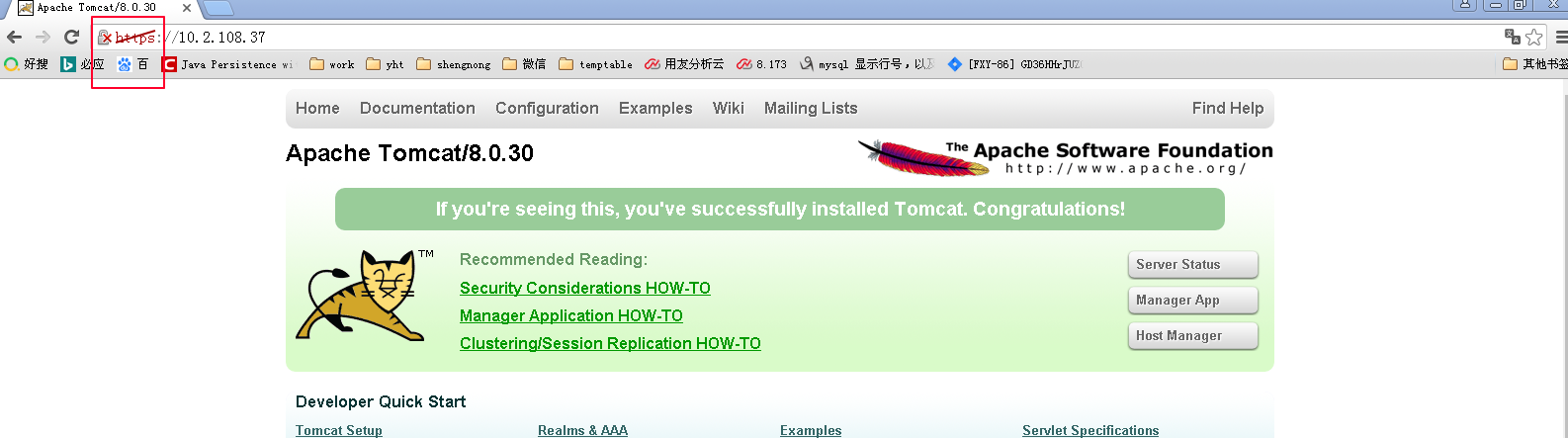
现在就可以用https访问分析云服务了。



这里可以点击，高级，选择继续访问：



点击继续前往过后，就访问到分析云的服务了:



1. **客户端浏览器导入crt证书**

上一步虽是能够通过https访问分析云了，但是由于证书不受信任，网址栏的https上是有错误标识的，主要原因是自己制作的证书浏览器和操作系统还不信任，如果是认证机构申请的证书，则没有问题。下面介绍通过导入crt来解决红色警告。证书我们是在第二步生成的，由相关人员发送给用户。

谷歌浏览器导入crt证书的步骤如下：

设置 >> 高级 >> HTTPS/SSL >> 管理证书

>> 导入 >> 下一步 >> 浏览框选中crt文件 >> 下一步

>> 选择将证书存储到”受信任的根证书颁发机构”

>> 下一步 >> 完成。

完成之后重启浏览器，再访问分析云时就没有错误标识了。

这一步的一些截图参考如下：



