Tomcat配置HTTPS访问

1、SSL证书获取

请用户向CA厂商获取证书。

获取证书后，参考以下的说明进行证书部署。

2、Tomcat服务器证书部署

①进入Tomcat部署目录conf子目录中，编辑 server.xml文件，修改里面的SSL设置，参考如下：

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
               maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS"
                keystoreFile="xx/xx/xx.keystore"
                keystorePass="xxxx"/>
```

⚠ 需要注意修改的端口号和证书路径，证书密码，端口是否开放。

②阿里云证书配置

进入Tomcat部署目录conf子目录中，编辑 server.xml文件，修改里面的SSL设置，参考如下：

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
          maxThreads="150"
          SSLEnabled="true"
          scheme="https"
          secure="true"
          clientAuth="false"
          keystoreFile="/xxx/xxx/xxx.pfx"
          keystoreType="PKCS12"
          keystorePass="xxx"
          SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
          ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA256"/>
```

⚠ 1、需要注意修改的端口号和证书路径，证书密码，端口是否开放。

2、Tomcat7及以下版本、Tomcat8及以上版本关于阿里云证书的配置方法不同，详情请参考 SSL证书安装指南 。