链滴

如何配置在 nginx 和 cas 上配置 ssl?

作者：turbidsoul

原文链接：https://ld246.com/article/1367996363724

来源网站：链滴

公司准备对登录服务采用 https，而登录服务采用的是 cas，前段的是用 nginx 代理， 所以就有之后的几个问题。 ### 主要碰到了下面 3 个问题： > 1. nginx 中配置 ssl > 2. cas 中开启 ssl gt; 3. java 中导入证书 其实我主要卡在了第三点上，这个问题会在之后有详细的说明。 ---------- ---------- 首先是生成我们的证书，我使用的是 openssl： 1. 首先是生成私钥： <code>openssl genrsa -out server.key</code> 2. 接下来要生成 CSR 文件： <code>openssl req -new -key server.key -out server.csr</code> 3. 最后就是生成证书文件： <code>openssl x509 -req days 365 -in server.csr -signkey server.key -out server.crt</code> 这里有我一个笔记是 openssl 的简单教程：openssl 简单教程 ---------- ---------- 生成证书后，就可以配置 nginx 了，打开 nginx.conf，加入以下几行: liste 443 ssl; ssl on; ssl_certificate login.cert; ssl_certificate_key login.key; 加入这几行配置后，重载 nginx， nginx 上 ssl 就可以生效了，这时用普通的 http 访问会无法访问， 必须使用 https 访问，第一访问 firefox 会提示证书不信任。 ---------- 接下来是在 cas 中启 ssl 的支持，虽然这一步很简单，但是具体我也不甚了解，因为 cas 是其他同事负责的， 我只是按他说的去做，所以我说的文件路径或者文件名和 cas 的原生项目会有不通。接下来我简单说以下如何置： 先找到 <code>WEB-INFO/spring-configuration</code> 下的配置文件, <code>ticketGrantngTicketCookieGenerator.xml</code> 和 <code>warnCookieGenerator.xml</code> 打开文件 <code>ticketGrantingTicketCookieGenerator.xml</code> Defines the cookie that stores th TicketGrantingTicket. You most likely should never modify these (especially the "secure" proerty). You can change the name if you want to make it harder for people to guess. 修改 <coe>p:cookieSecure="false"</code> 的值为 true 打开 <code>warnCookiGenerator.xml</code>: This Spring Configuration file describes the cookie used to store the WARN parameter so that a user is warned whenever the CAS service is used. You would modiy this if you wanted to change the cookie path or the name. 修改 <code>p:cookieSecure="false"</code> 的值为 true。 修改这两个之后就可以把 cas 的包放入 tomcat 中启动 tomcat。 经过上面两部其实按正常情况下已经可以访问了，但是在登录的时候， 进入 cas 的录页面进行登录，登录成功后返回的时候会抛出异常，对于这个异常我不甚理解， 但是我在 google 所有得到的结果是这时 java 的一个 bug，不过已经给出了解决方法. 下载下面的代码： InstallCert.java 编译之后使用使用下面命令执行以下： <code>java InstallCert cas.xxxxx.com</code> <code>https://login.xxxx.com</code> 是你配置了sl 的服务的那个域名 执行完后会在当前目录下生成 <code>jssecacerts</code> 的文件，把文件 coy 到 <code>jdk1.7.0_10\jre\lib\security</code> 目录下 重新启动服务即可。或者在 java 的启动数中加入 <code>-Djavax.net.ssl.trustStore=F:/work/Java/jssecacerts</code>, 重新启动也是可的，我使用的后面这个方法，前面的那个我没有测试，不过应该不会有问题。 到这里就算是把 ssl 配完成了，其实并没有什么复杂的东西，就是最后 java 这个问题让我找了很常时间。 最后在 java 的社中找到解决办法，可以这个类的源码文件的下载链接还失效了，在 google 中找了半天才找到个完整。