
Resin SSL 证书部署指南



沃通电子认证服务有限公司

WoSignCA Limited

目 录

一、 安装 SSL 服务器证书	3
1.1 获取 SSI 证书	3
1.2 2018 年之前签发获取 SSI 证书.....	3
1.3 服务器安装 SSL 证书环境	3
1.4 配置部署 SSL 证书	7
1.4.1 启动 SSL 端口	7
1.4.2 配置证书路径	8
二、 SSL 证书的备份	9
三、 SSL 证书的恢复	9

技术支持联系方式

技术支持邮箱: support@wosign.com
技术支持热线电话: 0755-26027828
技术支持网页: <https://bbs.wosign.com>
公司官网地址: <https://www.wosign.com>

声明

此文档仅做参考使用，相应的配置需根据当前的配置进行调整。

一、 安装 SSL 服务器证书

1.1 获取 SSI 证书

最终沃通数字证书系统将会给您颁发证书文件（.zip）压缩格式，当中有包含四种证书

格式如：for Apache、for IIS、for Nginx、for Other Server；Resin 应用服务器上需要 for Nginx 里面的 crt 证书文件，然后用工具合成 jks 格式：

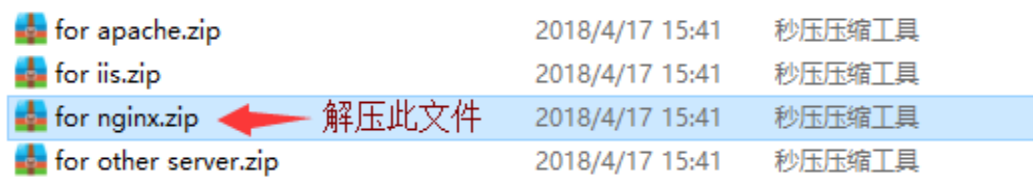


图 1

打开 for Nginx 文件可以看到公钥，如图 2

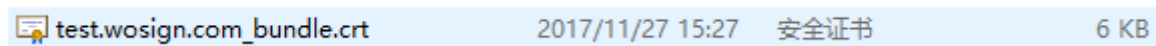


图 2

私钥 key 文件，需要找到生成 CSR 一起生成出的两个文件，如图 3，其中一个为 .key 文件，若生成出来的是 .com 文件，修改一下后缀即可。

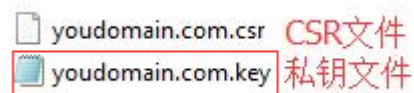


图 3

合成工具下载地址：<https://download.wosign.com/wosign/wosigncode.exe>

合成方式：先把 key 文件放到 for nginx 里，再双击下载的工具，选择证书项，操作选项，选择证书格式转换，源格式选择 PEM，目标格式选择 JKS。

证书文件：点击后面的选择按钮，找到 for nginx 目录，选择 yourdomain.com_bundle.crt，点击确定。

私钥文件：点击后面的选择按钮，找到 for nginx 目录，选择 yourdomain.com.key，点击确定。

私钥密码：为空，不用填写（因为生成私钥的时候没有填写，如果之前有填写过私钥密码，这里也填写相同的私钥密码）

JKS 密码：任意填写一个密码（合成 JKS 格式证书后的密码，之后在 Resin 上安装证书的时候需要使用到）



填写完毕后，点击转换，选择保存证书文件的位置，填写证书名称，推荐使用 yourdomain.com.jks，点击保存。



最后，得到 jks 格式证书。

ssl.key	2018/4/17 17:37	KEY 文件
test.wosign.com.jks	2018/4/17 17:38	JKS 文件
test.wosign.com_bundle.crt	2017/11/27 15:27	安全证书

1.2 2018 年之前签发获取 SSL 证书

颁发证书文件（.zip）压缩格式，当中有包含五种证书

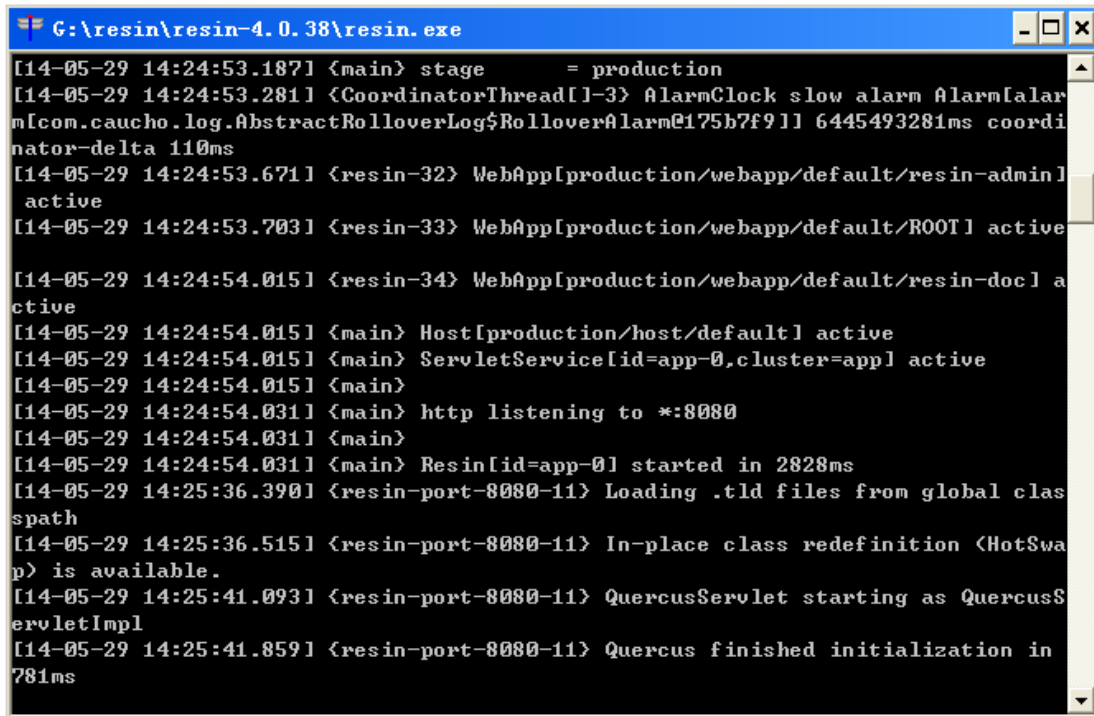
格式如：for Apache、for IIS、for Ngnix、for Tomcat、for Other Server；Tomcat 应用服务器上只需要 for Tomcat 里面的 JKS 证书文件即可。

for Apache.zip	2014/8/20 14:00	WinRAR ZIP 压缩...
for IIS.zip	2014/8/20 14:00	WinRAR ZIP 压缩...
for Ngnix.zip	2014/8/20 14:00	WinRAR ZIP 压缩...
for Other Server.zip	2014/8/20 14:00	WinRAR ZIP 压缩...
for Tomcat.zip	2014/8/20 14:00	WinRAR ZIP 压缩... 解压此文件

1.3 服务器安装 SSL 证书环境

首先访问 Resin 官网 (<http://www.caucho.com>) 当前可根据您的系统下载不同的应用程序包，我们以 Windows 系统为例。所以下载 Windows 版本的 Resin-4.0.38 版本。

下载 Resin 解压到其中一个盘符下后，进入 Resin-4.0.38 根目录下找到 resin.exe 文件，运行期间将出现如图 1 所示的命令提示符窗口。



```
G:\resin\resin-4.0.38\resin.exe
[14-05-29 14:24:53.187] <main> stage = production
[14-05-29 14:24:53.281] <CoordinatorThread[1-3] AlarmClock slow alarm Alarm[alarm[com.caucho.log.AbstractRolloverLog$RolloverAlarm@175b7f91]] 6445493281ms coordinator-delta 110ms
[14-05-29 14:24:53.671] <resin-32> WebApp[production/webapp/default/resin-admin] active
[14-05-29 14:24:53.703] <resin-33> WebApp[production/webapp/default/ROOT] active
[14-05-29 14:24:54.015] <resin-34> WebApp[production/webapp/default/resin-doc] active
[14-05-29 14:24:54.015] <main> Host[production/host/default] active
[14-05-29 14:24:54.015] <main> ServletService[id=app-0,cluster=appl] active
[14-05-29 14:24:54.015] <main>
[14-05-29 14:24:54.031] <main> http listening to *:8080
[14-05-29 14:24:54.031] <main>
[14-05-29 14:24:54.031] <main> Resin[id=app-0] started in 2828ms
[14-05-29 14:25:36.390] <resin-port-8080-11> Loading .tld files from global classpath
[14-05-29 14:25:36.515] <resin-port-8080-11> In-place class redefinition (HotSwap) is available.
[14-05-29 14:25:41.093] <resin-port-8080-11> QuercusServlet starting as QuercusServletImpl
[14-05-29 14:25:41.859] <resin-port-8080-11> Quercus finished initialization in 781ms
```

图 2

启动执行文件后，我们将输入 Resin 应用服务默认的地址如：<http://127.0.0.1:8080>
点击/resin-admin 图 2 图 3



图 3

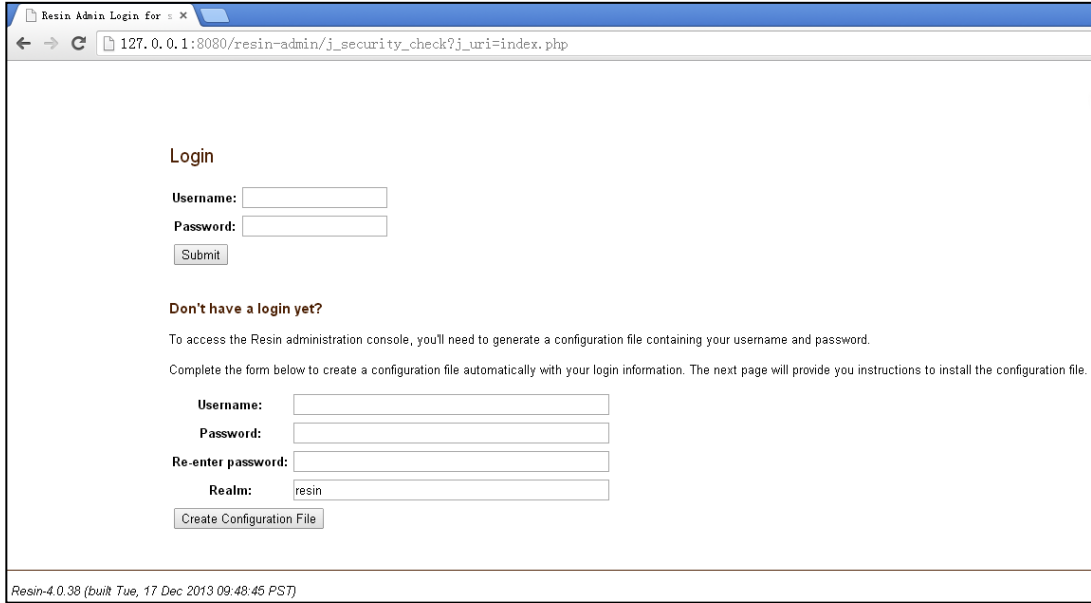


图 4

1.4 配置部署 SSL 证书

1.4.1 启动 SSL 端口

首先找到安装 Resin 目录下该配置文件“Resin.properties”，一般默认路径都是在 Conf 文件夹中。然后用文本编辑器打开该文件，接着找到如下所示 图 4

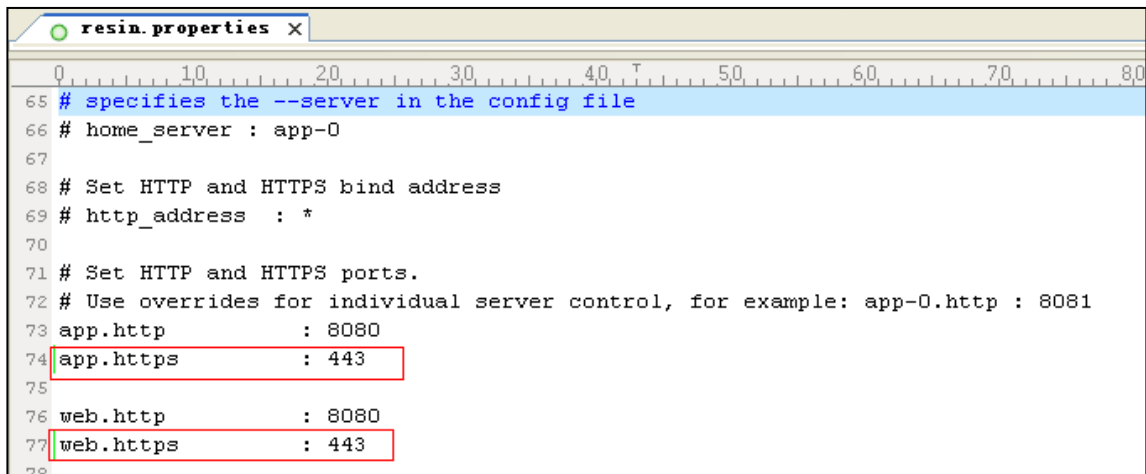


图 5

默认情况下 app.https 和 web.https : 8443 是用“#”注释掉的。所以我们可以去掉“#”然后把 8443 修改为：443。

注释：（因为版本繁多没能一一去下载来检查，只能通过在此说明。根据不同的版本寻找不同的配置文件如“Resin.properties”或是“resin.xml”文件进行配置。）

1.4.2 配置证书路径

其次同一个文件中在找到如图 5

```
# JSSE certificate configuration
# Keys are typically stored in the resin configuration directory.
jsse_keystore_type : jks
jsse_keystore_file : keys/jks.jks
jsse_keystore_password : XXXXXXXXXX
```

图 6

默认情况下：Jsse_keystore_tye:jks 证书类型；

Jsse_keystore_file:keys/xx.jks 证书存放路径；

Jsse_keystore_password:changeme 证书密码；

三行都是“#”注释状态，所以我们可以去掉“#”，最后只要改成您的证书路径(例如：**keys/SSL.jks**)、证书密码(您申请证书时所设置密码)。最后保存重启 Resin 应用服务就 OK。测试访问效果图 6



图 7

二、 SSL 证书的备份

请保存好收到的证书压缩包文件及密码，以防丢失

三、 SSL 证书的恢复

重复第 1.4 步操作即