

# SSL 证书

## 证书安装

### 产品文档



腾讯云

---

**【版权声明】**

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

**【商标声明】**

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

**【服务声明】**

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

## 文档目录

### 证书安装

#### SSL 证书安装部署至云服务

安装部署 SSL 证书到内容分发网络 (CDN) 指引

#### 国际标准 SSL 证书安装

Nginx 服务器 SSL 证书安装部署

Apache 服务器 SSL 证书安装部署 (Linux)

Apache 服务器 SSL 证书安装部署 (Windows)

Tomcat 服务器 SSL 证书安装部署 (JKS 格式) (Linux)

Tomcat 服务器 SSL 证书安装部署 (JKS 格式) (Windows)

Tomcat 服务器 SSL 证书安装部署 (PFX 格式)

GlassFish 服务器 SSL 证书安装部署

JBoss 服务器 SSL 证书安装部署

Jetty 服务器 SSL 证书安装部署

IIS 服务器 SSL 证书安装部署

Weblogic 服务器 SSL 证书安装部署

如何选择 SSL 证书安装部署类型？

# 证书安装

## SSL 证书安装部署至云服务

### 安装部署 SSL 证书到内容分发网络（CDN） 指引

最近更新时间：2024-03-06 17:38:42

## 概述

本文档指导您将 SSL 证书部署到 CDN 内容分发网络。

## 前提条件

已登录 [证书管理控制台](#)，成功申请获取证书。

## 操作步骤

### 注意：

域名需要已经接入 CDN，且状态为部署中或已启动，关闭状态的域名无法部署证书。具体操作请参考 [接入域名](#)。

COS 或 数据万象开启 CDN 加速后，默认的 `.file.myqcloud.com` 或 `.image.myqcloud.com` 域名无法配置证书。

SVN 托管源暂时无法配置

1. 单击**已签发**页签，选择您需要部署的证书，并单击**证书详情**。
2. 进入**证书详情**管理页面，单击**一键部署**。
3. 在弹出的**选择部署类型**窗口中，选择**CDN**，并单击**确定**。
4. 跳转到 [CDN 控制台](#)，进入**配置证书**详情页，已显示对应的域名、证书来源以及证书 ID。
5. 选择回源协议方式，您可以选择 CDN 节点回源站获取资源时的回源方式。

选择 **HTTP** 回源配置成功后，用户至 CDN 节点请求支持 HTTPS/HTTP，CDN 节点回源站请求均为 HTTP。

选择 **协议跟随** 回源配置，您的源站需要部署有效证书，否则将导致回源失败。配置成功后，用户至 CDN 节点请求为 HTTP 时，CDN 节点回源请求也为 HTTP。用户至 CDN 节点请求为 HTTPS 时，CDN 节点回源请求也为 HTTPS。

若域名源站修改 HTTPS 端口为非 443 端口，会导致配置失败。

COS 源或 FTP 源域名仅支持 HTTP 回源。

6. 配置成功后，您可以在**证书管理**页面看到已经配置成功的域名以及证书情况。

# 国际标准 SSL 证书安装

## Nginx 服务器 SSL 证书安装部署

最近更新时间：2024-03-06 17:38:41

### 操作场景

本文档指导您如何在 Nginx 服务器中安装 SSL 证书。

#### 说明：

本文档以证书名称 `cloud.tencent.com` 为例。

Nginx 版本以 `nginx/1.18.0` 为例。

当前服务器的操作系统为 CentOS 7，由于操作系统的版本不同，详细操作步骤略有区别。

安装 SSL 证书前，请您在 Nginx 服务器上开启 HTTPS 默认端口 `443`，避免证书安装后无法启用 HTTPS。具体可参考 [服务器如何开启443端口？](#)

SSL 证书文件上传至服务器方法可参考 [如何将本地文件拷贝到云服务器](#)。

### 前提条件

已准备文件远程拷贝软件，例如 WinSCP（建议从官方网站获取最新版本）。

若您需部署到腾讯云云服务器，建议使用云服务器的文件上传功能。

已准备远程登录工具，例如 PuTTY 或者 Xshell（建议从官方网站获取最新版本）。

已在当前服务器中安装配置含有 `http_ssl_module` 模块的 Nginx 服务。

安装 SSL 证书前需准备的数据如下：

名称	说明
服务器的 IP 地址	服务器的 IP 地址，用于 PC 连接到服务器。
用户名	登录服务器的用户名。
密码	登录服务器的密码。

#### 说明：

在腾讯云官网购买的云服务器，您可以登录 [云服务器控制台](#) 获取服务器 IP 地址、用户名及密码。

### 操作步骤

## 证书安装

1. 请在 [SSL 证书管理控制台](#) 中选择您需要安装的证书并单击**下载**。
2. 在弹出的“证书下载”窗口中，服务器类型选择 **Nginx**，单击**下载**并解压缩 `cloud.tencent.com` 证书文件包到本地目录。

解压缩后，可获得相关类型的证书文件。其中包含 `cloud.tencent.com_nginx` 文件夹：

文件夹名称：`cloud.tencent.com_nginx`

文件夹内容：

`cloud.tencent.com_bundle.crt` 证书文件  
`cloud.tencent.com_bundle.pem` 证书文件（可忽略该文件）  
`cloud.tencent.com.key` 私钥文件  
`cloud.tencent.com.csr` CSR 文件

说明：

CSR 文件是申请证书时由您上传或系统在线生成的，提供给 CA 机构。安装时可忽略该文件。

3. 使用“WinSCP”（即本地与远程计算机间的复制文件工具）登录 Nginx 服务器。

说明：

WinSCP 上传文件操作可参考 [通过 WinSCP 上传文件到 Linux 云服务器](#)。

若您需部署到腾讯云云服务器，建议使用云服务器的文件上传功能。

4. 将已获取到的 `cloud.tencent.com_bundle.crt` 证书文件和 `cloud.tencent.com.key` 私钥文件从本地目录拷贝到 Nginx 服务器的 `/etc/nginx` 目录（此处为 Nginx 默认安装目录，请根据实际情况操作）下。

5. 远程登录 Nginx 服务器。例如，使用“PuTTY”工具登录。

6. 编辑 Nginx 根目录下的 `nginx.conf` 文件。修改内容如下：

说明：

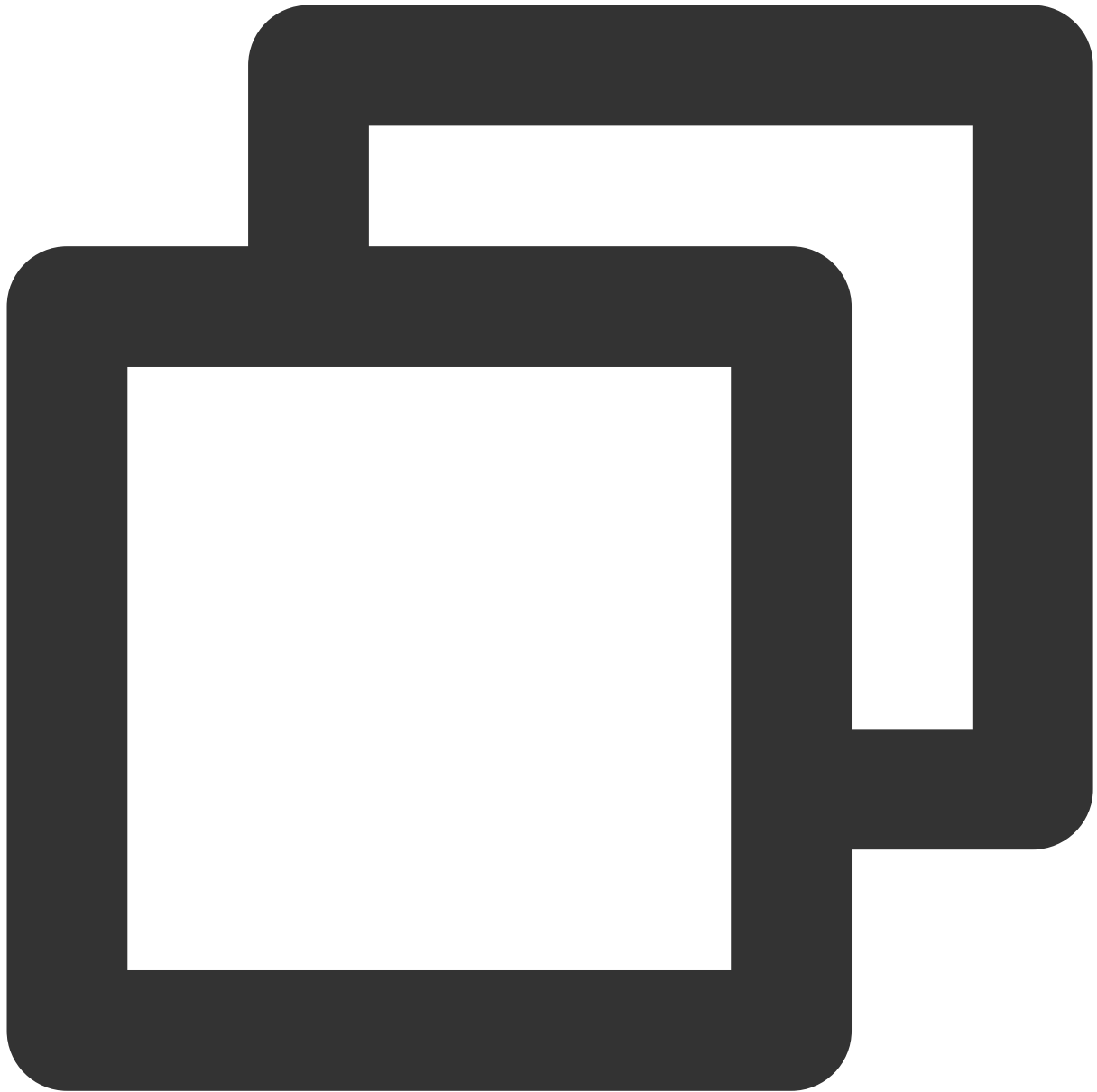
如找不到以下内容，可以手动添加。可执行命令 `nginx -t`，找到nginx的配置文件路径。

如下图示例：

```
# nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is
nginx: configuration file /etc/nginx/nginx.conf test is succe
#
```

此操作可通过执行 `vim /etc/nginx/nginx.conf` 命令行编辑该文件。

由于版本问题，配置文件可能存在不同的写法。例如：Nginx 版本为 `nginx/1.15.0` 以上请使用 `listen 443 ssl` 代替 `listen 443` 和 `ssl on`。



```
server {  
    #SSL 默认访问端口号为 443  
    listen 443 ssl;  
    #请填写绑定证书的域名  
    server_name cloud.tencent.com;  
    #请填写证书文件的相对路径或绝对路径  
    ssl_certificate cloud.tencent.com_bundle.crt;  
    #请填写私钥文件的相对路径或绝对路径  
    ssl_certificate_key cloud.tencent.com.key;  
    ssl_session_timeout 5m;  
    #请按照以下协议配置
```

```
ssl_protocols TLSv1.2 TLSv1.3;
#请按照以下套件配置，配置加密套件，写法遵循 openssl 标准。
ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:HIGH:!aNULL:!MD5:!RC4:!DHE;
ssl_prefer_server_ciphers on;
location / {
    #网站主页路径。此路径仅供参考，具体请您按照实际目录操作。
    #例如，您的网站主页在 Nginx 服务器的 /etc/www 目录下，则请修改 root 后面的 html 为
    root html;
    index index.html index.htm;
}
}
```

7. 通过执行以下命令验证配置文件问题。





```
nginx -t
```

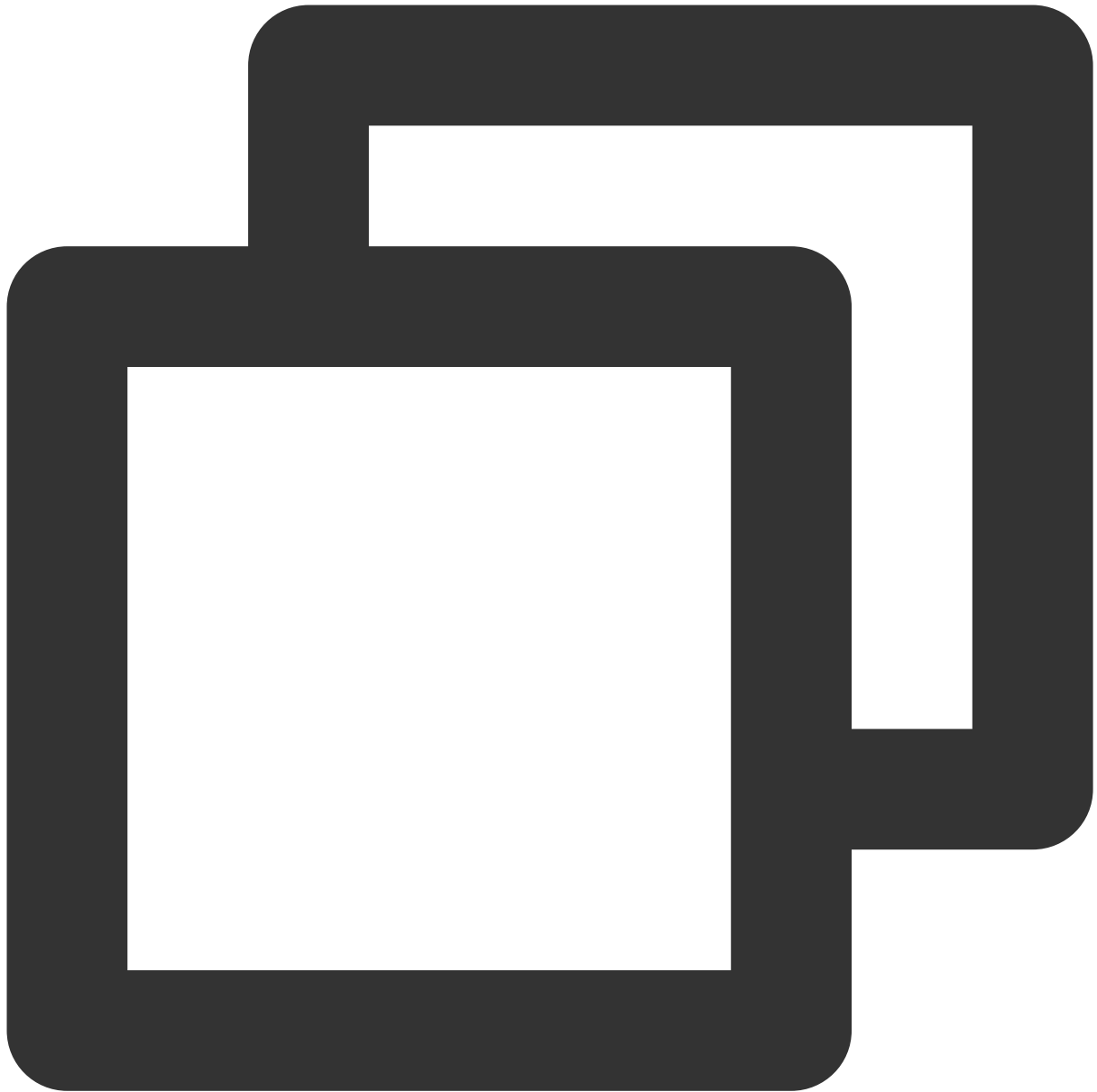
若存在，请您重新配置或者根据提示修改存在问题。

若不存在，请执行 [步骤8](#)。

## 8. 通

过执

行以下命令重载 Nginx。



```
nginx -s reload
```

9. 重载成功，即可使用 `https://cloud.tencent.com` 进行访问。

### HTTP 自动跳转 HTTPS 的安全配置（可选）

如果您需要将 HTTP 请求自动重定向到 HTTPS。您可以通过以下操作设置：

1. 根据实际需求，选择以下配置方式：

在页面中添加 JS 脚本。

在后端程序中添加重定向。

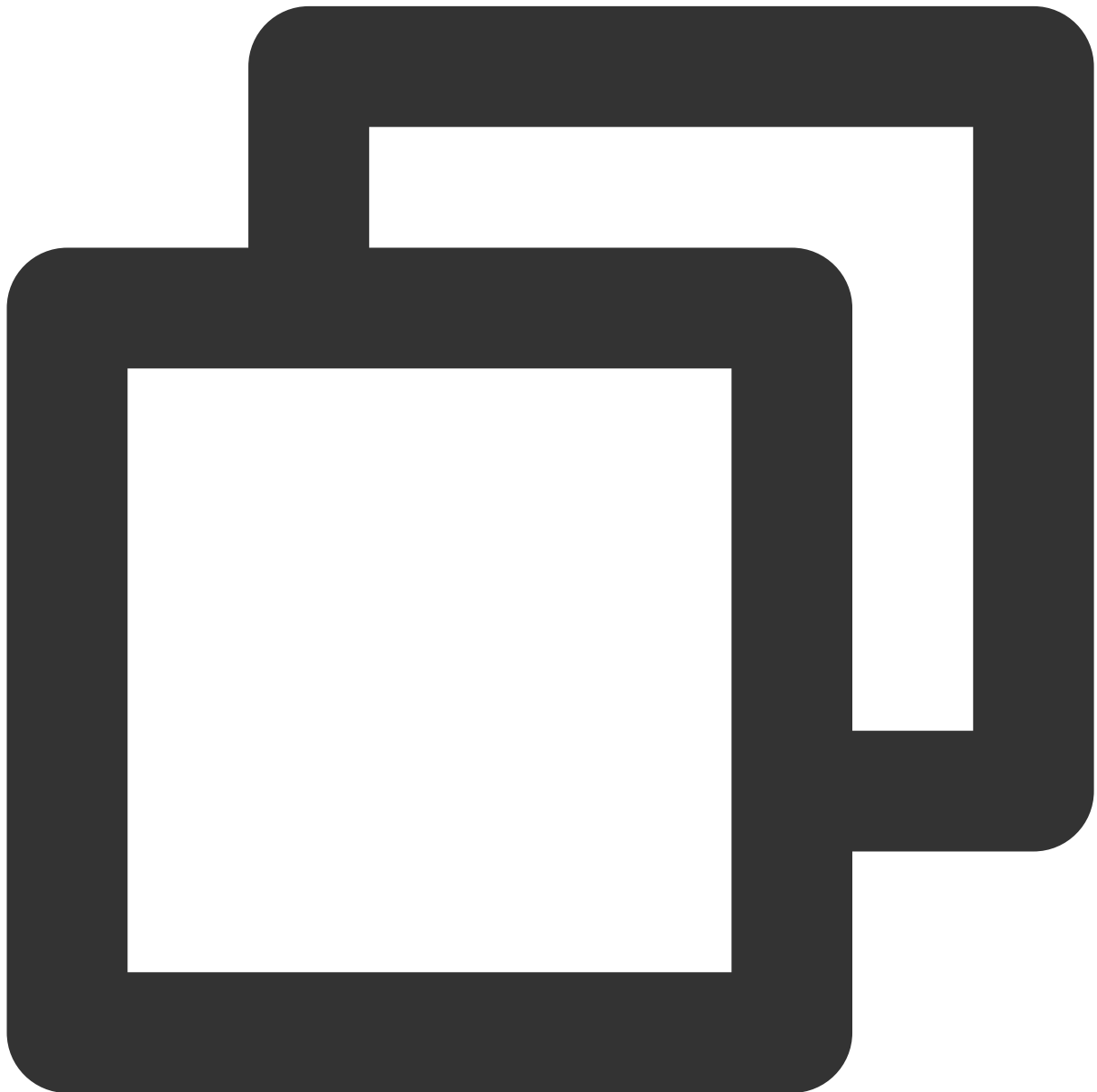
通过 Web 服务器实现跳转。

Nginx 支持 rewrite 功能。若您在编译时没有去掉 pcre，您可在 HTTP 的 server 中增加 `return 301 https://$host$request_uri;`，即可将默认80端口的请求重定向为 HTTPS。修改如下内容：

#### 说明：

未添加注释的配置语句，您按照下述配置即可。

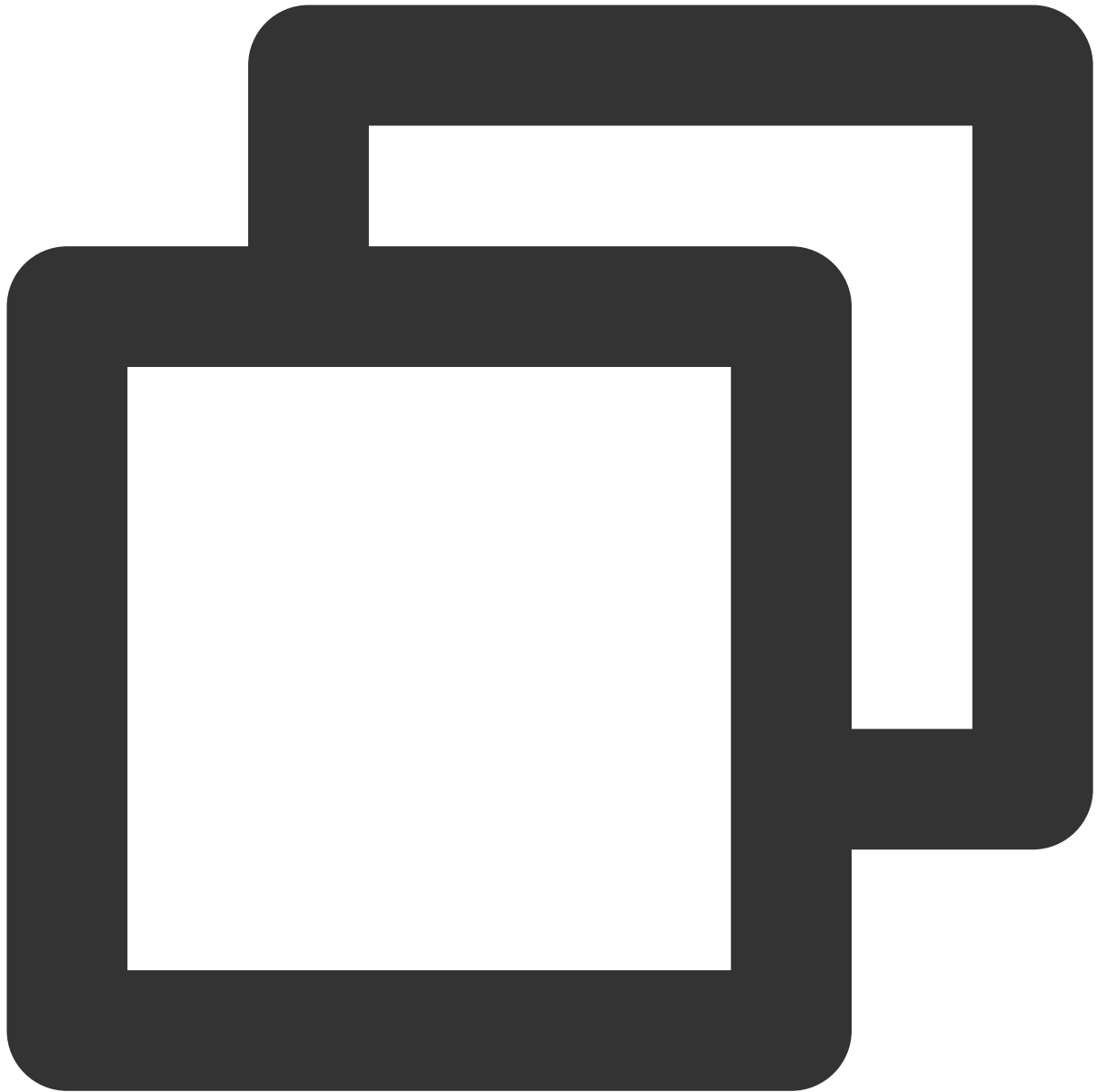
由于版本问题，配置文件可能存在不同的写法。例如：Nginx 版本为 `nginx/1.15.0` 以上请使用 `listen 443 ssl` 代替 `listen 443` 和 `ssl on`。



```
server {  
    #SSL 默认访问端口号为 443
```

```
listen 443 ssl;
#请填写绑定证书的域名
server_name cloud.tencent.com;
#请填写证书文件的相对路径或绝对路径
ssl_certificate cloud.tencent.com_bundle.crt;
#请填写私钥文件的相对路径或绝对路径
ssl_certificate_key cloud.tencent.com.key;
ssl_session_timeout 5m;
#请按照以下套件配置，配置加密套件，写法遵循 openssl 标准。
ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!MD5:!A
#请按照以下协议配置
ssl_protocols TLSv1.2 TLSv1.3;
ssl_prefer_server_ciphers on;
location / {
    #网站主页路径。此路径仅供参考，具体请您按照实际目录操作。
    #例如，您的网站主页在 Nginx 服务器的 /etc/www 目录下，则请修改 root 后面的 html 为 /etc
    root html;
    index index.html index.htm;
}
}
server {
    listen 80;
    #请填写绑定证书的域名
    server_name cloud.tencent.com;
    #把http的域名请求转成https
    return 301 https://$host$request_uri;
}
```

2. 通过执行以下命令验证配置文件问题。



```
nginx -t
```

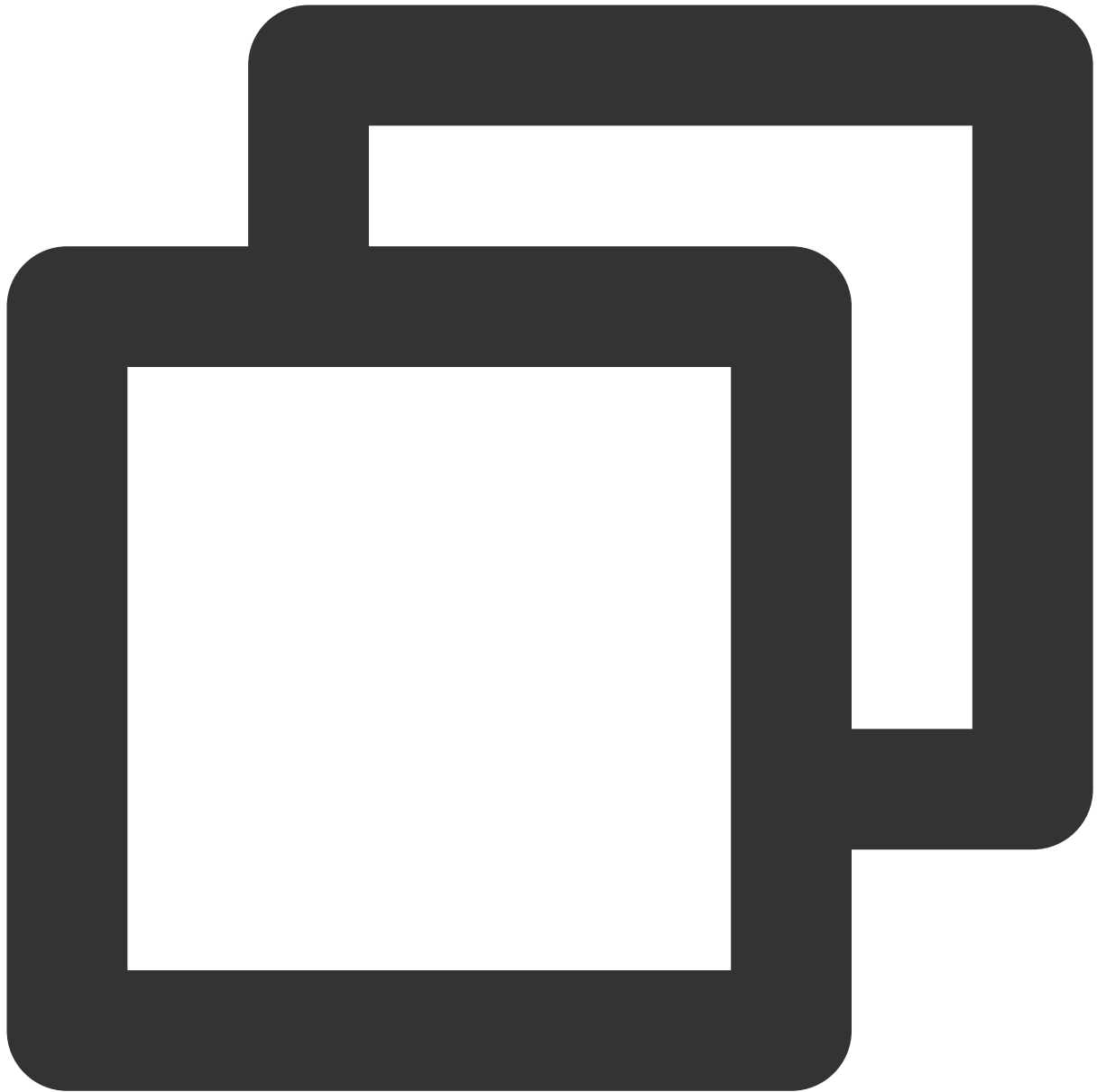
若存在，请您重新配置或者根据提示修改存在问题。

若不存在，请执行 [步骤3](#)。

### 3. 通

过执行

以下命令重载 Nginx。



```
nginx -s reload
```

4. 重载成功，即可使用 `https://cloud.tencent.com` 进行访问。

如果浏览器地址栏显示安全锁标识，则说明证书安装成功。

如果网站访问异常，可参考以下常见问题解决方案进行处理：

[无法使用 HTTPS 访问网站](#)

[部署 SSL 证书后，浏览器提示“网站连接不安全”](#)

[访问站点提示连接不安全？](#)

[在服务器上部署 SSL 证书后访问资源出现 404 报错](#)

---

**注意：**

操作过程如果出现问题，请您 [联系我们](#)。

# Apache 服务器 SSL 证书安装部署（Linux）

最近更新时间：2024-03-06 17:38:42

## 操作场景

本文档指导您如何在 Apache 服务器中安装 SSL 证书。

### 说明：

本文档以证书名称 `cloud.tencent.com` 为例。

Apache 版本以 `Apache/2.4.6` 为例。默认端口为 `80`。您可前往 [Apache 官网](#) 进行下载，若您需要采用其余版本，请您 [联系我们](#)。

当前服务器的操作系统为 CentOS 7，由于操作系统的版本不同，详细操作步骤略有区别。

安装 SSL 证书前，请您在 Apache 服务器上开启“443”端口，避免证书安装后无法启用 HTTPS。具体可参考 [服务器如何开启443端口？](#)

SSL 证书文件上传至服务器方法可参考 [如何将本地文件拷贝到云服务器](#)。

## 前提条件

已准备远程文件拷贝软件，例如 WinSCP（建议从官方网站获取最新版本）。

若您部署到腾讯云云服务器，建议使用云服务器的文件上传功能。

已准备远程登录工具，例如 PuTTY 或者 Xshell（建议从官方网站获取最新版本）。

已在当前服务器中安装配置 Apache 服务。

安装 SSL 证书前需准备的数据如下：

名称	说明
服务器的 IP 地址	服务器的 IP 地址，用于 PC 连接到服务器。
用户名	登录服务器的用户名。
密码	登录服务器的密码。

### 说明：

在腾讯云官网购买的云服务器，您可以登录 [云服务器控制台](#) 获取服务器 IP 地址、用户名及密码。

## 操作步骤



## 证书安装

1. 请在 [SSL 证书管理控制台](#) 中选择您需要安装的证书并单击**下载**。
2. 在弹出的“证书下载”窗口中，服务器类型选择 **Apache**，单击**下载**并解压缩 `cloud.tencent.com` 证书文件包到本地目录。

解压缩后，可获得相关类型的证书文件。其中包含 `cloud.tencent.com_apache` 文件夹：

**文件夹名称：** `cloud.tencent.com_apache`

**文件夹内容：**

`root_bundle.crt` 证书文件

`cloud.tencent.com.crt` 证书文件

`cloud.tencent.com.key` 私钥文件

**CSR 文件内容：** `cloud.tencent.com.csr` 文件

**说明：**

CSR 文件是申请证书时由您上传或系统在线生成的，提供给 CA 机构。安装时可忽略该文件。

3. 使用“WinSCP”（即本地与远程计算机间的复制文件工具）登录 Apache 服务器。

**说明：**

WinSCP 上传文件操作可参考 [通过 WinSCP 上传文件到 Linux 云服务器](#)。

若您需部署到腾讯云云服务器，建议使用云服务器的文件上传功能。

4. 将已获取到的 `root_bundle.crt` 证书文件、`cloud.tencent.com.crt` 证书文件以及 `cloud.tencent.com.key` 私钥文件从本地目录拷贝到 Apache 服务器的 `/etc/httpd/ssl` 目录下。

**说明：**

若无 `/etc/httpd/ssl` 目录，可通过 `mkdir /etc/httpd/ssl` 命令行创建。

5. 远程登录 Apache 服务器。例如，使用“PuTTY”工具登录。

**说明：**

首次安装的 Apache 服务器，`conf.d`、`conf`、`conf.modules.d` 等目录默认在 `/etc/httpd` 目录下。

6. 在 `/etc/httpd/conf` 目录下的 `httpd.conf` 配置文件找到 `Include conf.modules.d/*.conf`（用于加载配置 SSL 的配置目录）配置语句，并确认该配置语句未被注释。若已注释，请去掉首行的注释符号（`#`），保存配置文件。

7. 在 `/etc/httpd/conf.modules.d` 目录下的 `00-ssl.conf` 配置文件找到 `LoadModule ssl_module modules/mod_ssl.so`（用于加载 SSL 模块）配置语句，并确认该配置语句未被注释，若已注释，请去掉首行的注释符号（`#`），保存配置文件。

**注意：**

由于操作系统的版本不同，目录结构也不同，请根据实际操作系统版本进行查找。

若以上配置文件中均未找到 `LoadModule ssl_module modules/mod_ssl.so` 和 `Include conf.modules.d/*.conf` 配置语句，请确认是否已经安装 `mod_ssl.so` 模块。若未安装 `mod_ssl.so` 模块，您可通过执行 `yum install mod_ssl` 命令进行安装。

8. 编辑 `/etc/httpd/conf.d` 目录下的 `ssl.conf` 配置文件。修改如下内容：



```
<VirtualHost 0.0.0.0:443>
  DocumentRoot "/var/www/html"
  #填写证书名称
  ServerName cloud.tencent.com
  #启用 SSL 功能
  SSLEngine on
  #证书文件的路径
  SSLCertificateFile /etc/httpd/ssl/cloud.tencent.com.crt
  #私钥文件的路径
  SSLCertificateKeyFile /etc/httpd/ssl/cloud.tencent.com.key
  #证书链文件的路径
```

```
SSLCertificateChainFile /etc/httpd/ssl/root_bundle.crt
</VirtualHost>
```

9. 重新启动 Apache 服务器，即可使用 `https://cloud.tencent.com` 进行访问。

如果浏览器地址栏显示安全锁标识，则说明证书安装成功。

如果网站访问异常，可参考以下常见问题解决方案进行处理：

[无法使用 HTTPS 访问网站](#)

[部署 SSL 证书后，浏览器提示“网站连接不安全”](#)

[访问站点提示连接不安全？](#)

[在服务器上部署 SSL 证书后访问资源出现 404 报错](#)

## HTTP 自动跳转 HTTPS 的安全配置（可选）

如果您需要将 HTTP 请求自动重定向到 HTTPS。您可以通过以下操作设置：

1. 编辑 `/etc/httpd/conf` 目录下的 `httpd.conf` 配置文件。

### 注意：

Apache 的版本不同，目录结构也会有所区别。具体请您参阅 [Apache 官方 rewrite 的文档](#)。

`httpd.conf` 配置文件所在目录不唯一，您可以根据 `/etc/httpd/*` 逐一查找。

2. 请确认该配置文件是否存在 `LoadModule rewrite_module modules/mod_rewrite.so`。

若存在，请去掉 `LoadModule rewrite_module modules/mod_rewrite.so` 前面的注释符号（#）号。并执行 [步骤4](#)。

若不存在，请执行 [步骤3](#)。

3.

请您

在 `/etc/httpd/conf.modules.d` 中新建一个 `*.conf` 文件，例如 `00-rewrite.conf`。在新建文件中添加以下内容：



```
LoadModule rewrite_module modules/mod_rewrite.so
```

4. 在 `httpd.conf` 配置文件中添加如下内容：



```
<Directory "/var/www/html">  
# 新增  
RewriteEngine on  
RewriteCond %{SERVER_PORT} !^443$  
RewriteRule ^(.*)?$ https://%{SERVER_NAME}%{REQUEST_URI} [L,R]  
</Directory>
```

5. 重新启动 Apache 服务器，即可使用 `http://cloud.tencent.com` 进行访问。

**注意：**

操作过程如果出现问题，请您 [联系我们](#)。



# Apache 服务器 SSL 证书安装部署 (Windows)

最近更新时间：2024-03-06 17:38:42

## 操作场景

本文档指导您如何在 Apache 服务器中安装 SSL 证书。

### 说明：

本文档以证书名称 `cloud.tencent.com` 为例。

Apache 版本以 `Apache/2.4.53` 为例。默认端口为 `80`。您可前往 [Apache 官网](#) 进行下载，若您需要采用其余版本，请您 [联系我们](#)。

当前服务器的操作系统为 Windows Server 2012 R2，由于操作系统的版本不同，详细操作步骤略有区别。

安装 SSL 证书前，请您在 Apache 服务器上开启“443”端口，避免证书安装后无法启用 HTTPS。具体可参考 [服务器如何开启443端口？](#)

SSL 证书文件上传至服务器方法可参考 [如何将本地文件拷贝到云服务器](#)。

## 前提条件

已在当前服务器中安装配置 Apache 服务。

安装 SSL 证书前需准备的数据如下：

名称	说明
服务器的 IP 地址	服务器的 IP 地址，用于 PC 连接到服务器。
用户名	登录服务器的用户名。
密码	登录服务器的密码。

### 说明：

在腾讯云官网购买的云服务器，您可以登录 [云服务器控制台](#) 获取服务器 IP 地址、用户名及密码。

## 操作步骤

### 步骤1：上传证书文件

1. 请在 [SSL 证书管理控制台](#) 中选择您需要安装的证书并单击**下载**。
2. 在弹出的“证书下载”窗口中，服务器类型选择 **Apache**，单击**下载**并解压缩 `cloud.tencent.com` 证书文件包到本地目录。

解压缩后，可获得相关类型的证书文件。其中包含 `cloud.tencent.com_apache` 文件：

文件夹名称：`cloud.tencent.com_apache`

文件夹内容：

`root_bundle.crt` 证书文件  
`cloud.tencent.com.crt` 证书文件  
`cloud.tencent.com.key` 私钥文件  
`cloud.tencent.com.csr` CSR 文件

说明：

CSR 文件是申请证书时由您上传或系统在线生成的，提供给 CA 机构。安装时可忽略该文件。

3. 通过 RDP 登录 Apache 服务器。

说明：

通过 RDP 上传文件可参考 [通过 RDP 方式上传文件到云服务器](#)。

若您需部署到腾讯云云服务器，建议使用云服务器的文件上传功能。

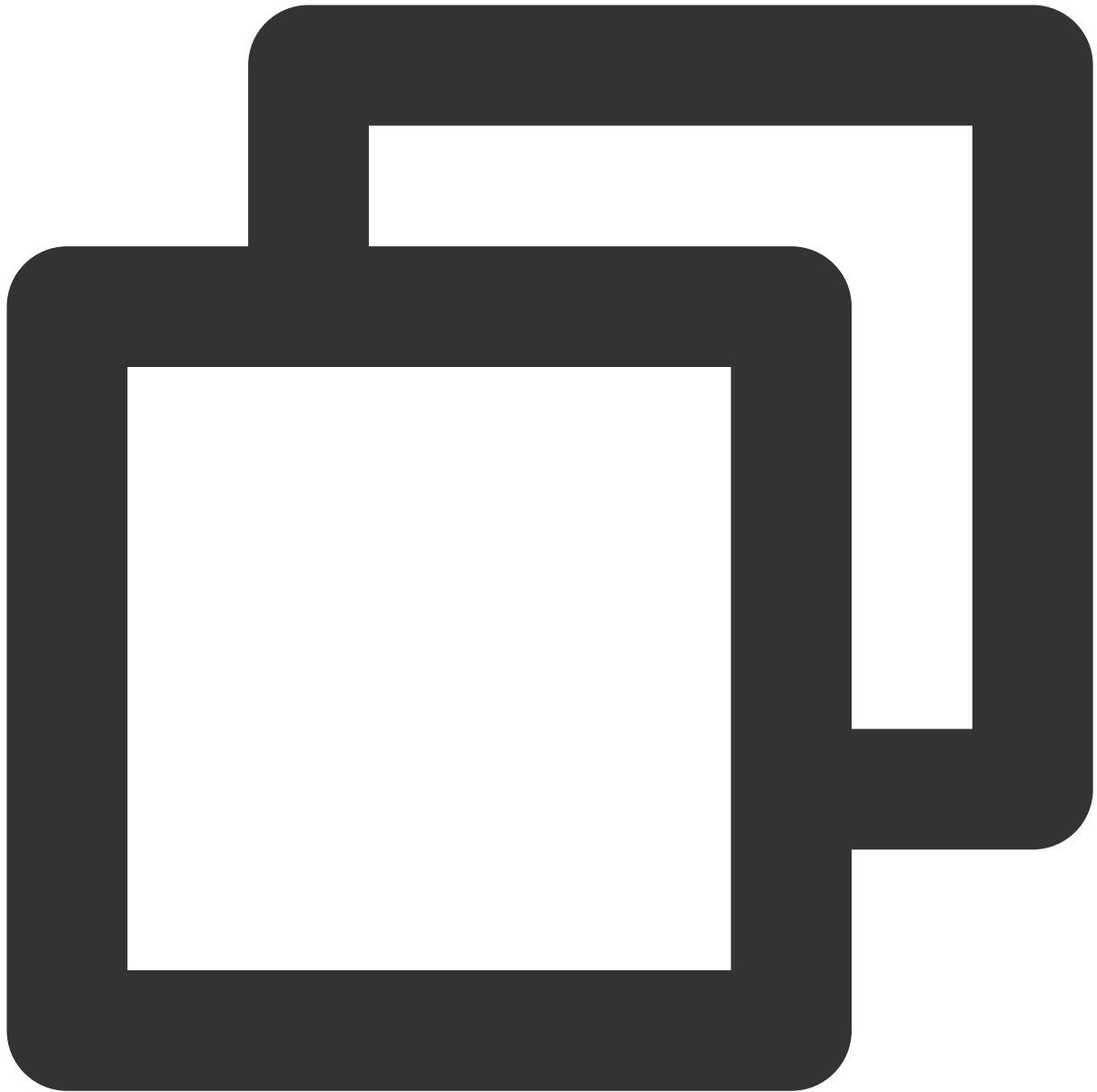
4. 将已获取到的 `root_bundle.crt` 证书文件、`cloud.tencent.com.crt` 证书文件以及 `cloud.tencent.com.key` 私钥文件从本地目录拷贝到 Apache 服务器目录的 `conf` 目录的下的 `ssl.crt` 与 `ssl.key` 文件夹。

SSL 证书文件	对应文件夹
<code>root_bundle.crt</code>	<code>ssl.crt</code>
<code>cloud.tencent.com.crt</code>	
<code>cloud.tencent.com.key</code>	<code>ssl.key</code>

## 步骤2：配置文件

1. 使用文本编辑器，打开 Apache 服务器 `conf` 目录下 `httpd.conf` 文件，并删除以下字段前 `#` 注释符。





```
#LoadModule ssl_module modules/mod_ssl.so
#Include conf/extra/httpd-ssl.conf
```

2. 使用文本编辑器，打开 Apache 服务器 `conf\extra` 目录下 `httpd-ssl.conf` 文件。
3. 修改 `httpd-ssl.conf` 文件，将以下字段参数设置为上传的证书文件路径，如下所示：



```
SSLCertificateFile "C:/apache/conf/ssl.crt/cloud.tencent.com.crt"  
SSLCertificateKeyFile "C:/apache/conf/ssl.key/cloud.tencent.com.key"  
SSLCACertificateFile "C:/apache/conf/ssl.crt/root_bundle.crt"
```

4. 重新启动 Apache 服务器，即可使用 `https://cloud.tencent.com` 进行访问。

如果浏览器地址栏显示安全锁标识，则说明证书安装成功。

如果网站访问异常，可参考以下常见问题解决方案进行处理：

[无法使用 HTTPS 访问网站](#)

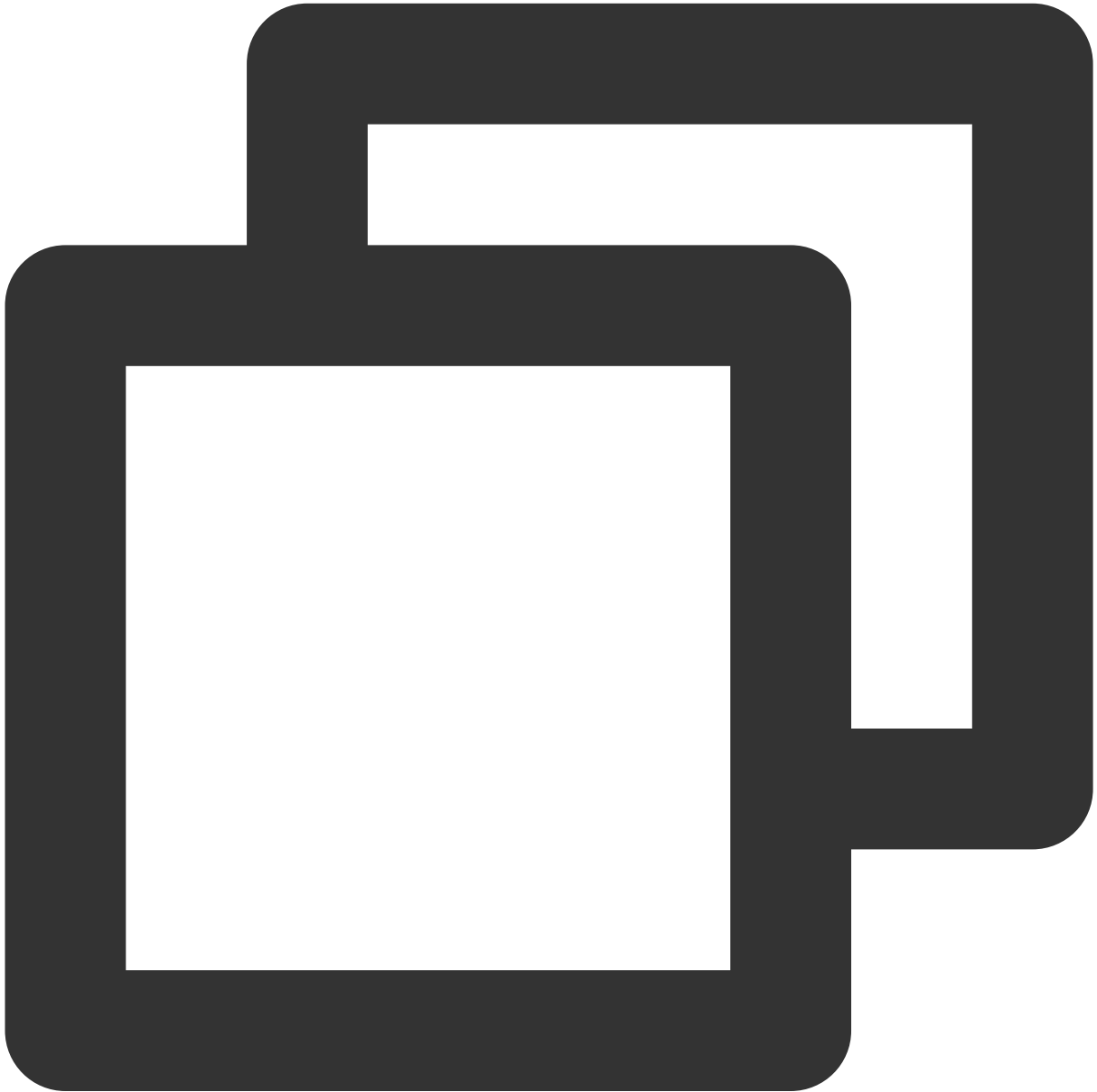
[部署 SSL 证书后，浏览器提示“网站连接不安全”](#)

[访问站点提示连接不安全？](#)

[在服务器上部署 SSL 证书后访问资源出现 404 报错](#)

## HTTP 自动跳转 HTTPS 的安全配置（可选）

1. 使用文本编辑器，打开 Apache 服务器 `conf` 目录下 `httpd.conf` 文件，并删除以下字段前 `#` 注释符。



```
#LoadModule rewrite_module modules/mod_rewrite.so
```

2. 并在网站运行目录配置字段。如： `<Directory "C:/xampp/htdocs">` 字段中添加如下内容：



```
<Directory "C:/xampp/htdocs">
RewriteEngine on
RewriteCond %{SERVER_PORT} !^443$
RewriteRule ^(.*)?$ https://%{SERVER_NAME}%{REQUEST_URI} [L,R]
</Directory>
```

3. 重新启动 Apache 服务器，即可使用 `https://intl.cloud.tencent.com/` 与 `https://intl.cloud.tencent.com/` 进行访问。访问后都将自动跳转到 `https://intl.cloud.tencent.com/`。

# Tomcat 服务器 SSL 证书安装部署（JKS 格式）（Linux）

最近更新时间：2024-03-06 17:42:37

## 操作场景

本文档指导您如何在 Tomcat 服务器中安装 JKS 格式的 SSL 证书。

### 说明：

本文档以证书名称 `cloud.tencent.com` 为例。

Tomcat 版本以 `tomcat-9.0.56` 为例。

当前服务器的操作系统为 CentOS 7 中文版，由于操作系统的版本不同，详细操作步骤略有区别。

安装 SSL 证书前，请您在 Tomcat 服务器上开启“443”端口，避免证书安装后无法启用 HTTPS。具体可参考 [服务器如何开启443端口？](#)

SSL 证书文件上传至服务器方法可参考 [如何将本地文件拷贝到云服务器](#)。

## 前提条件

已准备文件远程拷贝软件，例如 WinSCP（建议从官方网站获取最新版本）。

若您需部署到腾讯云云服务器，建议使用云服务器的文件上传功能。

已准备远程登录工具，例如 PuTTY 或者 Xshell（建议从官方网站获取最新版本）。

已在当前服务器中安装配置 Tomcat 服务。

安装 SSL 证书前需准备的数据如下：

名称	说明
服务器的 IP 地址	服务器的 IP 地址，用于 PC 连接到服务器。
用户名	登录服务器的用户名。
密码	登录服务器的密码。

### 注意：

在腾讯云官网购买的云服务器，您可以登录 [云服务器控制台](#) 获取服务器 IP 地址、用户名及密码。

当您申请 SSL 证书时选择“粘贴 CSR”方式，或购买的品牌证书为 Wotrus，则不提供 JKS 证书文件的下载，需要您通过手动转换格式的方式生成密钥库。其操作方法如下：

访问 [转换工具](#)。

将 Nginx 文件夹中的证书文件和私钥文件上传至转换工具中，并填写密钥库密码，单击提交，转换为 jks 格式证书。当前 Tomcat 服务默认安装在 /usr 目录下，例如，Tomcat 文件夹名称为 Tomcat-9.0.56，则其配置文件目录为：/usr/Tomcat-9.0.56/conf。

当您申请 SSL 证书时选择“粘贴 CSR”方式，或购买的品牌证书为 Wotrus，则不提供 JKS 证书文件的下载，需要您通过手动转换格式的方式生成密钥库。其操作方法如下：

访问 [转换工具](#)。

将 Nginx 文件夹中的证书文件和私钥文件上传至转换工具中，并填写密钥库密码，单击**提交**，转换为 jks 格式证书。当前 Tomcat 服务默认安装在 /usr 目录下，例如，Tomcat 文件夹名称为 Tomcat-9.0.56，则其配置文件目录为：`/usr/Tomcat-9.0.56/conf`。

## 操作步骤

### 证书安装

1. 请在 [SSL 证书管理控制台](#) 中选择您需要安装的证书并单击**下载**。
2. 在弹出的“证书下载”窗口中，服务器类型选择 **JKS**，单击**下载**并解压缩 `cloud.tencent.com` 证书文件包到本地目录。

解压缩后，可获得相关类型的证书文件。其中包含 `cloud.tencent.com_jks` 文件夹：

文件夹名称：`cloud.tencent.com_jks`

文件夹内容：

`cloud.tencent.com.jks` 密钥库

`keystorePass.txt` 密码文件（若已设置私钥密码，则无 `keystorePass.txt` 密码文件）

3. 使用 WinSCP（即本地与远程计算机间的复制文件工具）登录 Tomcat 服务器。将已获取到的 `cloud.tencent.com.jks` 密钥库文件从本地目录拷贝至 Tomcat 配置文件目录 `/usr/Tomcat-9.0.56/conf`。

说明：

WinSCP 上传文件操作可参考 [通过 WinSCP 上传文件到 Linux 云服务器](#)。

若您需部署到腾讯云云服务器，建议使用云服务器的文件上传功能。

4. 编辑在 `/usr/Tomcat-9.0.56/conf` 目录下的 `server.xml` 文件。添加如下内容：



```
<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"  
  maxThreads="150" scheme="https" secure="true"  
#证书保存的路径  
  keystoreFile="Tomcat 安装目录/conf/cloud.tencent.com.jks"  
#密钥库密码  
  keystorePass="*****"  
  clientAuth="false"/>
```

配置文件的主要参数说明如下：

**keystoreFile**：密钥库文件的存放位置，可以指定绝对路径，也可以指定相对于（Tomcat 安装目录）环境变量的相对路径。如果此项没有设定，默认情况下，Tomcat 将从当前操作系统用户的用户目录下读取名为“.keystore”的文件。

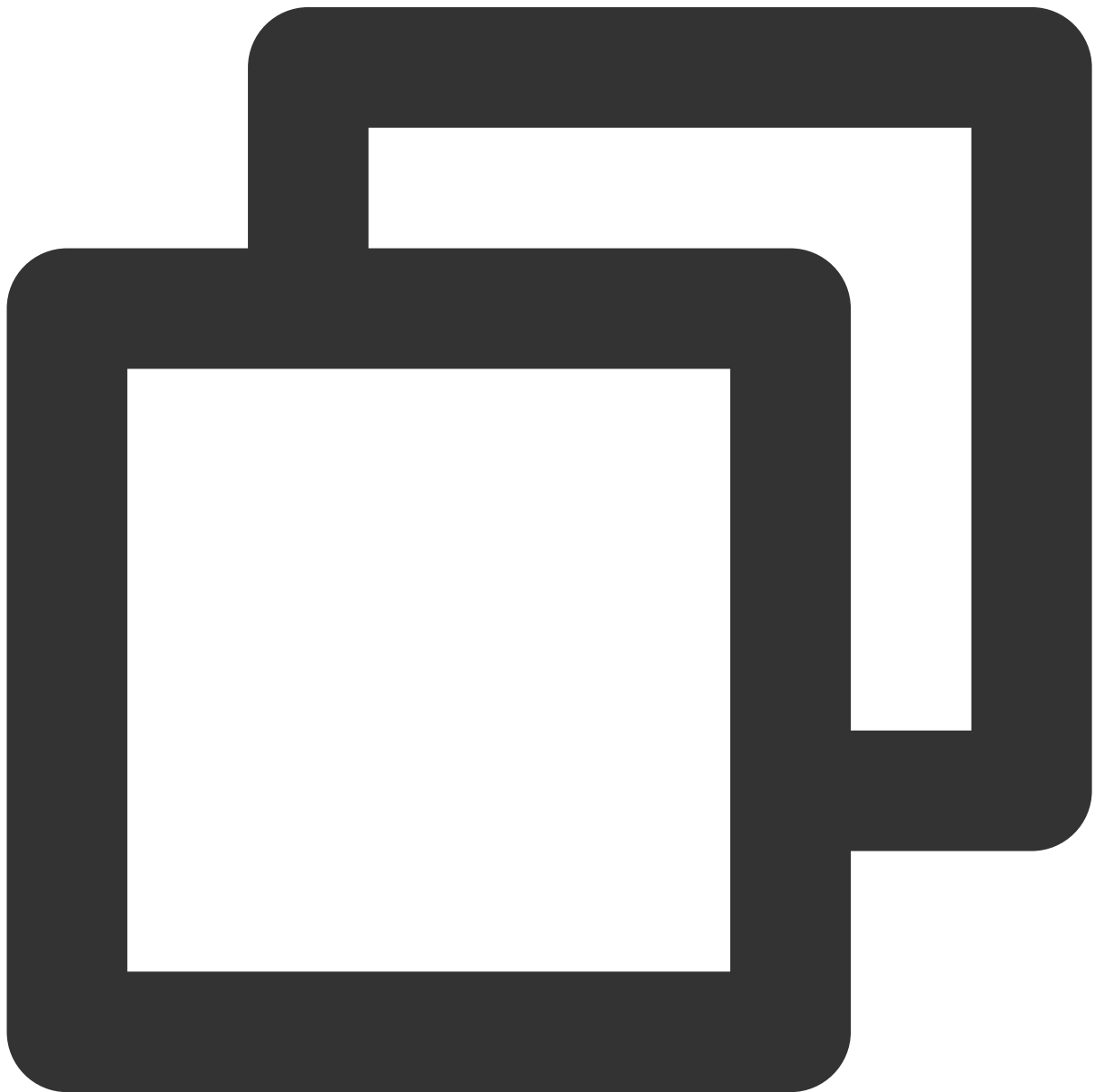
**keystorePass**：密钥库密码，指定 keystore 的密码。申请证书时若设置了私钥密码，请填写私钥密码；若申请证书时未设置私钥密码，请填写 Tomcat 文件夹中 keystorePass.txt 文件的密码。

**clientAuth**：如果设为 true，表示 Tomcat 要求所有的 SSL 客户出示安全证书，对 SSL 客户进行身份验证。

详细 `server.xml` 文件请参考如下内容：

**注意：**

不建议您直接复制 server.xml 文件内容，避免格式有误。





```
<?xml version="1.0" encoding="UTF-8"?>
<Server port="8005" shutdown="SHUTDOWN">
  <Listener className="org.apache.catalina.startup.VersionLoggerListener" />
  <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="
  <Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener"
  <Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListene
  <Listener className="org.apache.catalina.core.ThreadLocalLeakPreventionListener
<GlobalNamingResources>
  <Resource name="UserDatabase" auth="Container"
    type="org.apache.catalina.UserDatabase"
    description="User database that can be updated and saved"
    factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
    pathname="conf/tomcat-users.xml" />
</GlobalNamingResources>
  <Service name="Catalina">
    <Connector port="80" protocol="HTTP/1.1" connectionTimeout="20000" redirect
    <Connector port="443" protocol="HTTP/1.1"
      maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
      clientAuth="false"
      keystoreFile="Tomcat 安装目录/conf/cloud.tencent.com.jks"
      keystorePass="*****" />
    <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
  <Engine name="Catalina" defaultHost="cloud.tencent.com">
    <Realm className="org.apache.catalina.realm.LockOutRealm">
    <Realm className="org.apache.catalina.realm.UserDatabaseRealm"
      resourceName="UserDatabase"/>
    </Realm>
  <Host name="cloud.tencent.com" appBase="webapps"
    unpackWARs="true" autoDeploy="true" >
    <Context path="" docBase="Knews" />
    <Valve className="org.apache.catalina.valves.AccessLogValve" directory="log
      prefix="localhost_access_log" suffix=".txt"
      pattern="%h %l %u %t &quot;%r&quot; %s %b" />
    </Host>
  </Engine>
</Service>
</Server>
```

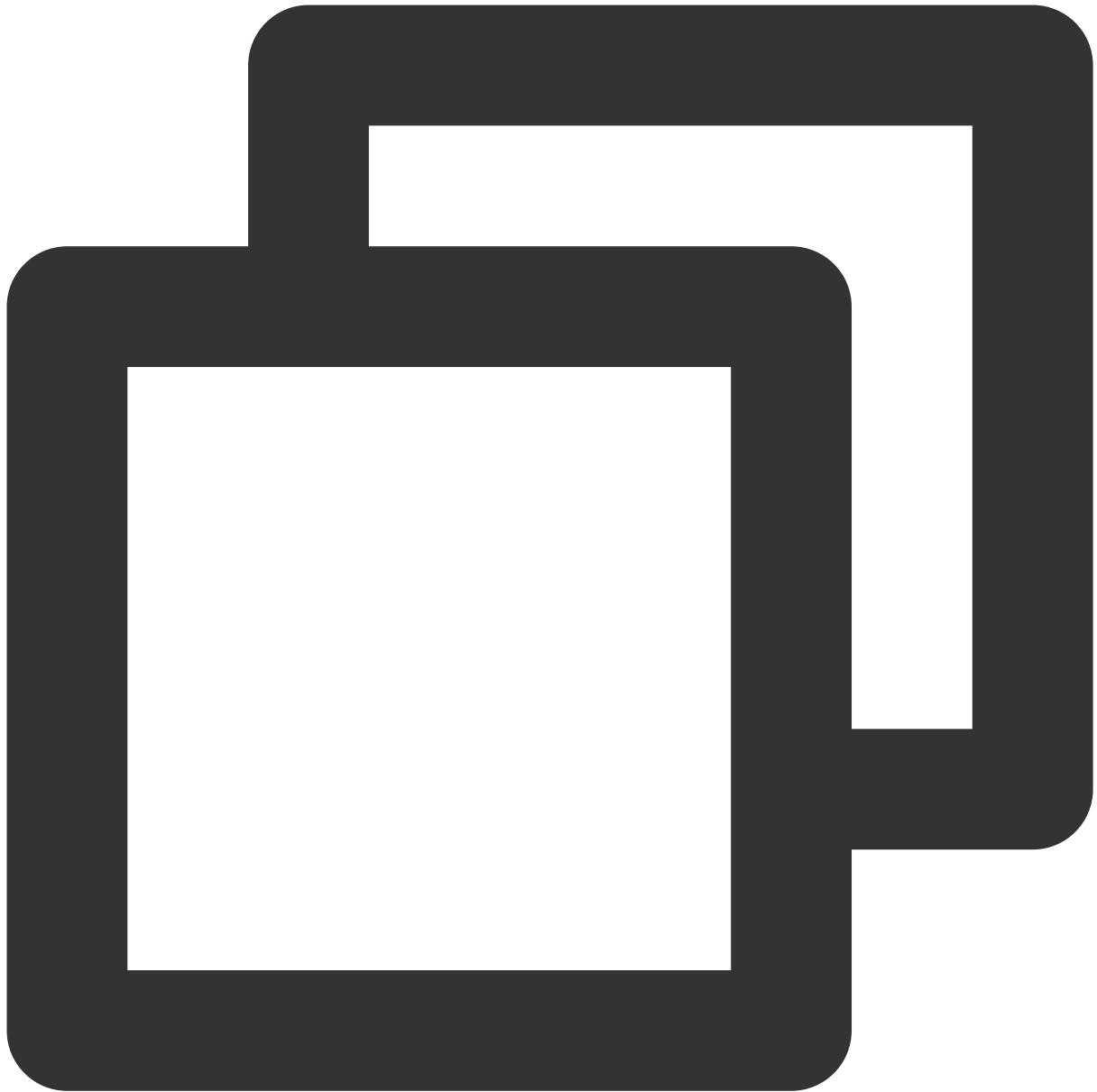
##### 5. 确认 Tomcat 服务器是否启动。

若已启动，您需要在 Tomcat 安装目录 `bin` 目录下（例如：`/usr/Tomcat-9.0.56/bin`）依次执行以下命令，关闭和重启 Tomcat 服务。



```
./shutdown.sh (关闭 Tomcat 服务)  
./startup.sh (启动 Tomcat 服务)
```

若未启动，您需要在 Tomcat 安装目录 `bin` 目录下（例如：`/usr/Tomcat-9.0.56/bin`）执行以下命令，启动 Tomcat 服务。



```
./startup.sh
```

6. 若启动成功，即可使用 `https://cloud.tencent.com` 进行访问。

如果浏览器地址栏显示安全锁标识，则说明证书安装成功。

如果网站访问异常，可参考以下常见问题解决方案进行处理：

[无法使用 HTTPS 访问网站](#)

[部署 SSL 证书后，浏览器提示“网站连接不安全”](#)

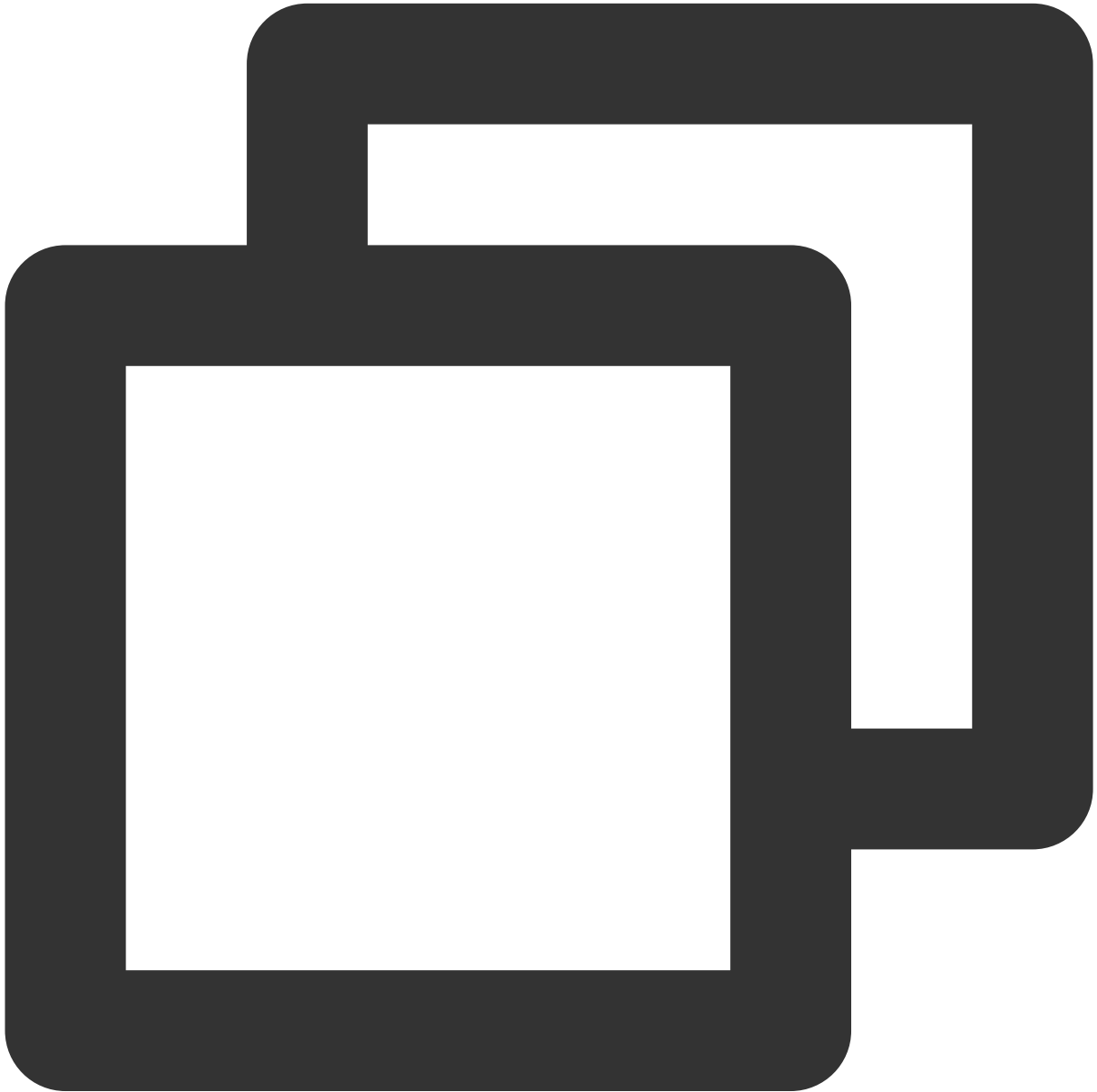
[访问站点提示连接不安全？](#)

[在服务器上部署 SSL 证书后访问资源出现 404 报错](#)

## HTTP 自动跳转 HTTPS 的安全配置（可选）

如果您需要将 HTTP 请求自动重定向到 HTTPS。您可以通过以下操作设置：

1. 编辑 Tomcat 安装目录 `conf` 目录下（例如：`/usr/Tomcat-9.0.56/conf`）的 `web.xml` 文件，并找到 `</welcome-file-list>` 标签。
2. 请在结束标签 `</welcome-file-list>` 后面换行，并添加以下内容：



```
<login-config>
  <!-- Authorization setting for SSL -->
  <auth-method>CLIENT-CERT</auth-method>
  <realm-name>Client Cert Users-only Area</realm-name>
```

```
</login-config>
<security-constraint>
<!-- Authorization setting for SSL -->
<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>
```

3. 编辑 Tomcat 安装目录 `conf` 目录下（例如：`/usr/Tomcat-9.0.56/conf`）的 `server.xml` 文件，将 `redirectPort` 参数修改为 SSL 的 `connector` 的端口，即443端口。如下所示：



```
<Connector port="80" protocol="HTTP/1.1"  
  connectionTimeout="20000"  
  redirectPort="443" />
```

**说明：**

此修改操作可将非 SSL 的 connector 跳转到 SSL 的 connector 中。

4. 在 Tomcat 安装目录 `/bin` 目录下（例如：`/usr/Tomcat-9.0.56/bin`）执行以下命令，关闭 Tomcat 服务。



```
./shutdown.sh
```

5. 执行以下命令，确认配置是否存在问题。



```
./configtest.sh
```

若存在，请您重新配置或者根据提示修改存在问题。

若不存在，请执行下一步。

6. 执行以下命令，启动 Tomcat 服务，即可使用 `http://cloud.tencent.com` 进行访问。





```
./startup.sh
```

# Tomcat 服务器 SSL 证书安装部署（JKS 格式）（Windows）

最近更新时间：2024-03-06 17:38:42

## 操作场景

本文档指导您如何在 Tomcat 服务器中安装 JKS 格式的 SSL 证书。

### 说明：

本文档以证书名称 `cloud.tencent.com` 为例。

Tomcat 版本以 `tomcat-9.0.56` 为例。

当前服务器的操作系统为 Windows Server 2016 中文版，由于操作系统的版本不同，详细操作步骤略有区别。

安装 SSL 证书前，请您在 Tomcat 服务器上开启“443”端口，避免证书安装后无法启用 HTTPS。具体可参考 [服务器如何开启443端口？](#)

SSL 证书文件上传至服务器方法可参考 [如何将本地文件拷贝到云服务器。](#)

## 前提条件

已在当前服务器中安装配置 Tomcat 服务。

安装 SSL 证书前需准备的数据如下：

名称	说明
服务器的 IP 地址	服务器的 IP 地址，用于 PC 连接到服务器。
用户名	登录服务器的用户名。
密码	登录服务器的密码。

### 注意：

在腾讯云官网购买的云服务器，您可以登录 [云服务器控制台](#) 获取服务器 IP 地址、用户名及密码。

当您申请 SSL 证书时选择“粘贴 CSR”方式，或购买的品牌证书为 Wotrus，则不提供 JKS 证书文件的下载，需要您通过手动转换格式的方式生成密钥库。其操作方法如下：

访问 [转换工具](#)。

将 Nginx 文件夹中的证书文件和私钥文件上传至转换工具中，并填写密钥库密码，单击**提交**，转换为 jks 格式证书。

## 操作步骤

### 证书安装

1. 请在 [SSL 证书管理控制台](#) 中选择您需要安装的证书并单击**下载**。
2. 在弹出的“证书下载”窗口中，服务器类型选择 **JKS**，单击**下载**并解压缩 `cloud.tencent.com` 证书文件包到本地目录。

解压缩后，可获得相关类型的证书文件。其中包含 `cloud.tencent.com_jks` 文件夹：

文件夹名称：`cloud.tencent.com_jks`

文件夹内容：

`cloud.tencent.com.jks` 密钥库

`keystorePass.txt` 密码文件（若已设置私钥密码，则无 `keystorePass.txt` 密码文件）

3. 将已获取到的 `cloud.tencent.com.jks` 密钥库文件拷贝至 Tomcat 安装目录 `conf` 目录下。
4. 编辑在 `conf` 目录下的 `server.xml` 文件。添加如下内容：

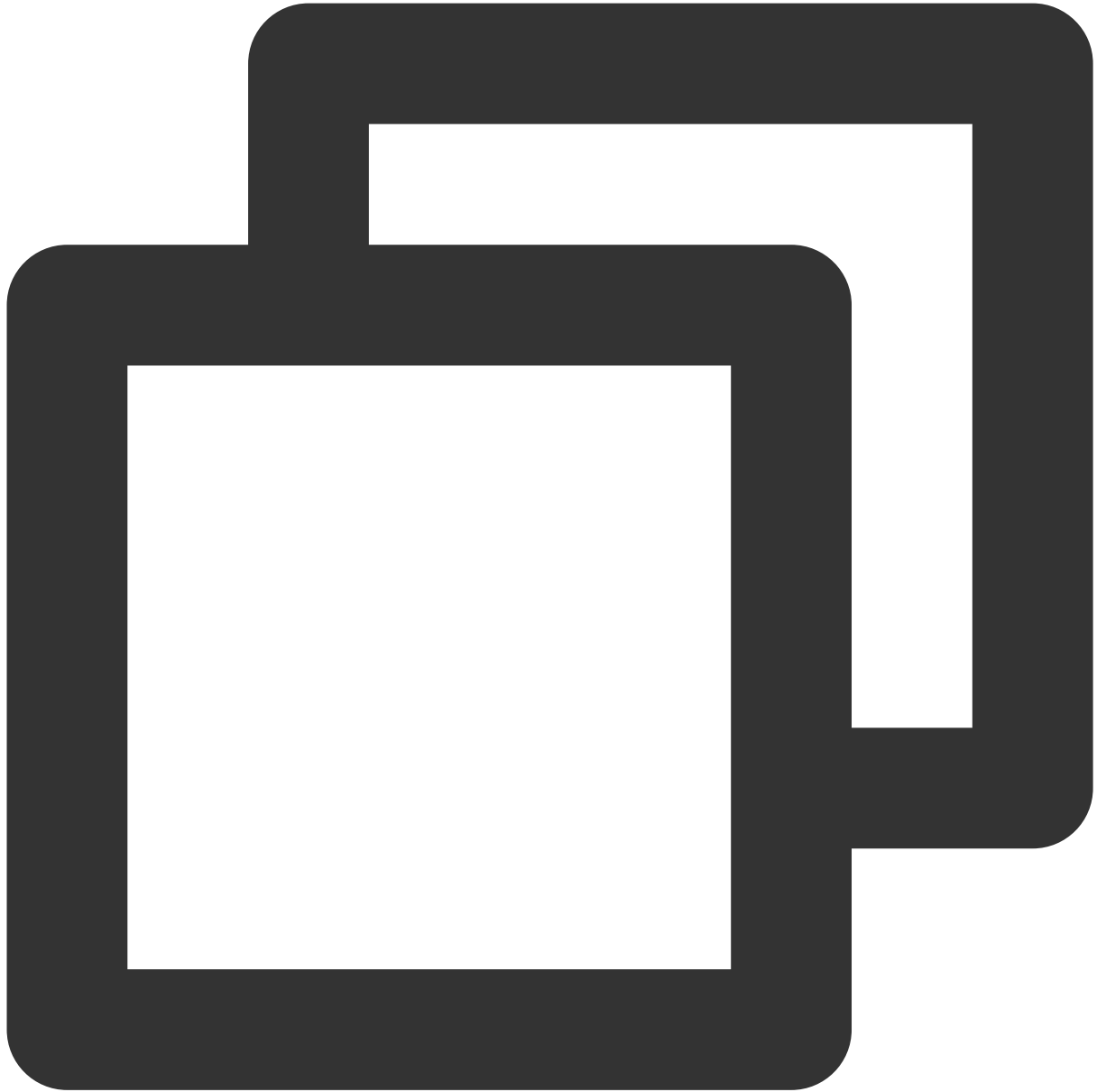


```
<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
  maxThreads="150" scheme="https" secure="true"
#证书保存的路径
  keystoreFile="Tomcat 安装目录/conf/cloud.tencent.com.jks"
#密钥库密码
  keystorePass="*****"
  clientAuth="false"/>
```

详细 `server.xml` 文件请参考如下内容：

**注意：**

不建议您直接复制 server.xml 文件内容，避免格式有误。



```
<?xml version="1.0" encoding="UTF-8"?>
<Server port="8005" shutdown="SHUTDOWN">
<Listener className="org.apache.catalina.startup.VersionLoggerListener" />
<Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
<Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener" />
<Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener" />
<Listener className="org.apache.catalina.core.ThreadLocalLeakPreventionListener" />
<GlobalNamingResources>
<Resource name="UserDatabase" auth="Container" />
</GlobalNamingResources>
</Server>
```

```
        type="org.apache.catalina.UserDatabase"
        description="User database that can be updated and saved"
        factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
        pathname="conf/tomcat-users.xml" />
</GlobalNamingResources>
<Service name="Catalina">
    <Connector port="80" protocol="HTTP/1.1" connectionTimeout="20000" redirectPo
    <Connector port="443" protocol="HTTP/1.1"
        maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
        clientAuth="false"
        keystoreFile="Tomcat 安装目录/conf/cloud.tencent.com.jks"
        keystorePass="*****" />
    <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
<Engine name="Catalina" defaultHost="cloud.tencent.com">
    <Realm className="org.apache.catalina.realm.LockOutRealm">
        <Realm className="org.apache.catalina.realm.UserDatabaseRealm"
            resourceName="UserDatabase"/>
    </Realm>
    <Host name="cloud.tencent.com" appBase="webapps"
        unpackWARs="true" autoDeploy="true" >
        <Context path="" docBase ="Knews" />
    <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
        prefix="localhost_access_log" suffix=".txt"
        pattern="%h %l %u %t &quot;%r&quot; %s %b" />
    </Host>
</Engine>
</Service>
</Server>
```

配置文件的主要参数说明如下：

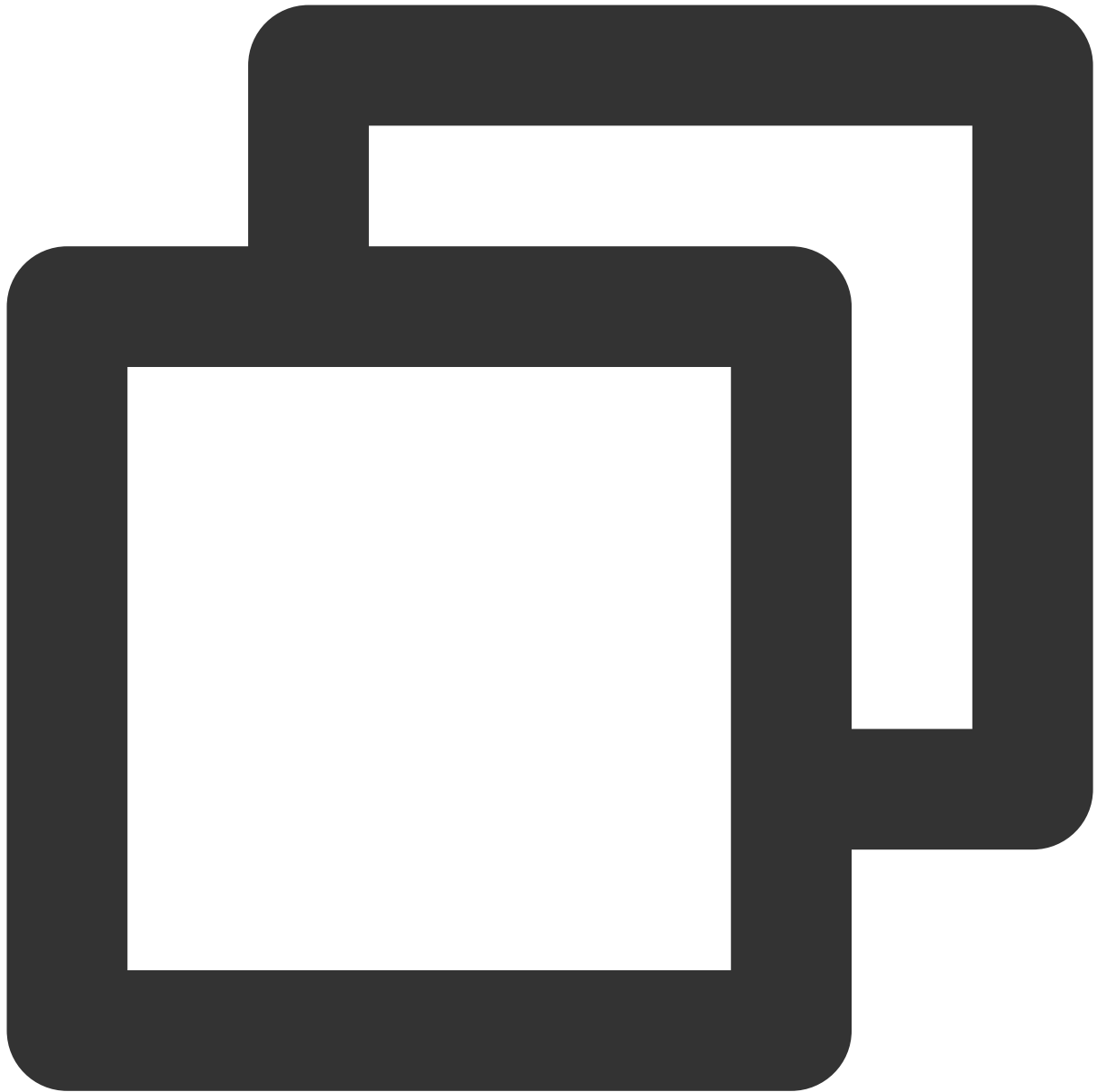
**keystoreFile**：密钥库文件的存放位置，可以指定绝对路径，也可以指定相对于 <CATALINA\_HOME>（Tomcat 安装目录）环境变量的相对路径。如果此项没有设定，默认情况下，Tomcat 将从当前操作系统用户的用户目录下读取名为“.keystore”的文件。

**keystorePass**：密钥库密码，指定 keystore 的密码。申请证书时若设置了私钥密码，请填写私钥密码；若申请证书时未设置私钥密码，请填写 Tomcat 文件夹中 keystorePass.txt 文件的密码。

**clientAuth**：如果设为 true，表示 Tomcat 要求所有的 SSL 客户出示安全证书，对 SSL 客户进行身份验证。

5. 确认 Tomcat 服务器是否启动。

若已启动，您需要在 Tomcat 安装目录 `bin` 目录下依次执行以下 bat 脚本，关闭和重启 Tomcat 服务。



```
shutdown.bat  (关闭 Tomcat 服务器)  
startup.bat  (启动 Tomcat 服务器)
```

若未启动，您需要在 Tomcat 安装目录 `bin` 目录下执行以下 bat 脚本，启动 Tomcat 服务。



```
startup.bat
```

6. 若启动成功，即可使用 `https://intl.cloud.tencent.com/` 进行访问。

如果浏览器地址栏显示安全锁标识，则说明证书安装成功。

如果网站访问异常，可参考以下常见问题解决方案进行处理：

[无法使用 HTTPS 访问网站](#)

[部署 SSL 证书后，浏览器提示“网站连接不安全”](#)

[访问站点提示连接不安全？](#)

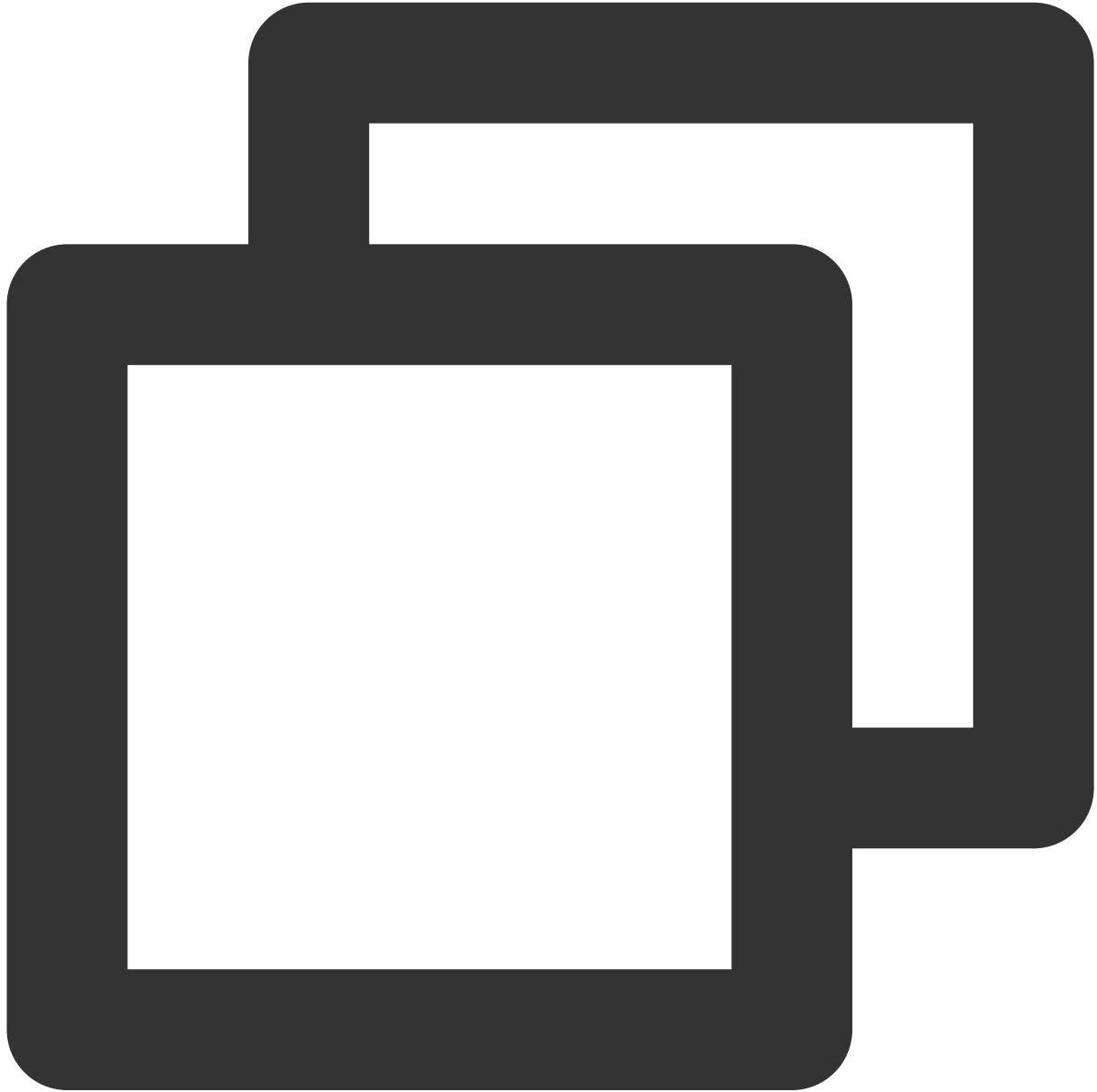
[在服务器上部署 SSL 证书后访问资源出现 404 报错](#)



## HTTP 自动跳转 HTTPS 的安全配置（可选）

如果您需要将 HTTP 请求自动重定向到 HTTPS。您可以通过以下操作设置：

1. 编辑 Tomcat 安装目录 `conf` 目录下的 `web.xml` 文件，并找到 `</welcome-file-list>` 标签。
2. 请在结束标签 `</welcome-file-list>` 后面换行，并添加以下内容：



```
<login-config>
  <!-- Authorization setting for SSL -->
  <auth-method>CLIENT-CERT</auth-method>
  <realm-name>Client Cert Users-only Area</realm-name>
</login-config>
```

```
<security-constraint>
<!-- Authorization setting for SSL -->
<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>
```

3. 编辑 Tomcat 安装目录下的 `server.xml` 文件，将 `redirectPort` 参数修改为 SSL 的 connector 的端口，即443 端口。如下所示：

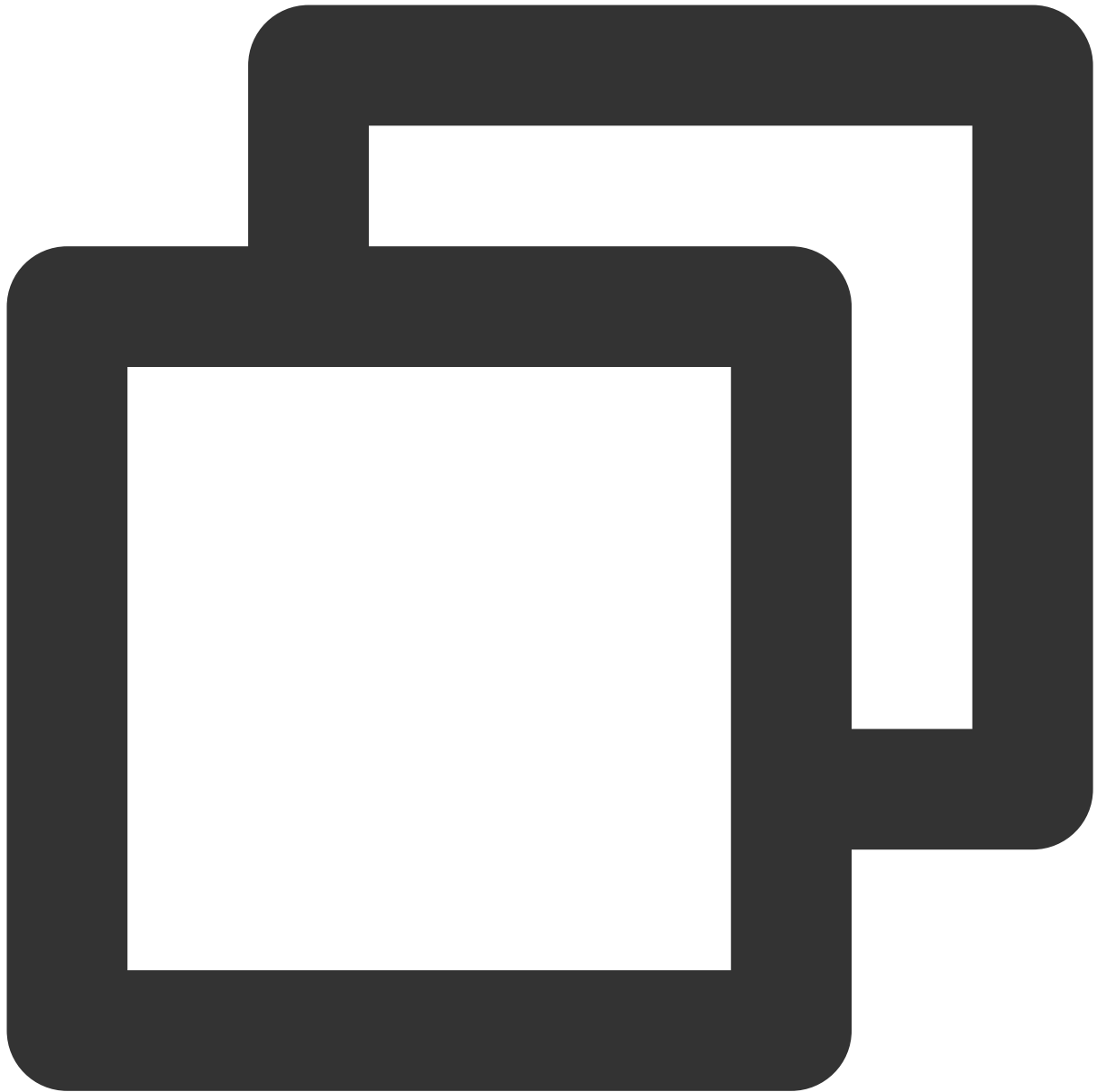


```
<Connector port="80" protocol="HTTP/1.1"  
  connectionTimeout="20000"  
  redirectPort="443" />
```

**说明：**

此修改操作可将非 SSL 的 connector 跳转到 SSL 的 connector 中。

4. 在 Tomcat 安装目录 `/bin` 目录下执行以下 bat 脚本，关闭 Tomcat 服务器。



```
shutdown.bat
```

5. 执行以下命令，确认配置是否存在问题。



```
configtest.bat
```

若存在，请您重新配置或者根据提示修改存在问题。

若不存在，请执行下一步。

6. 执行以下 bat 脚本，启动 Tomcat 服务器，即可使用 <https://intl.cloud.tencent.com/> 进行访问。



startup.bat

# Tomcat 服务器 SSL 证书安装部署（PFX 格式）

最近更新时间：2024-03-06 17:38:42

## 操作场景

本文档指导您如何在 Tomcat 服务器中安装 PFX 格式 SSL 证书。

### 说明：

文档以证书名称 `cloud.tencent.com` 为例。

Tomcat 版本以 `tomcat9.0.40` 为例。

当前服务器的操作系统为 CentOS 7，由于操作系统的版本不同，详细操作步骤略有区别。

若您需在 Tomcat 服务器中安装 JKS 格式 SSL 证书。具体可参考：[Tomcat 服务器 SSL 证书安装部署（JKS 格式）](#)。

安装 SSL 证书前，请您在 Tomcat 服务器上开启“443”端口，避免证书安装后无法启用 HTTPS。具体可参考：[服务器如何开启443端口？](#)

SSL 证书文件上传至服务器方法可参考：[如何将本地文件拷贝到云服务器。](#)

## 前提条件

已准备文件远程拷贝软件，例如 WinSCP（建议从官方网站获取最新版本）。

已准备远程登录工具，例如 PuTTY 或者 Xshell（建议从官方网站获取最新版本）。

已在当前服务器中安装配置 Tomcat 服务。

安装 SSL 证书前需准备的数据如下：

名称	说明
服务器的 IP 地址	服务器的 IP 地址，用于 PC 连接到服务器。
用户名	登录服务器的用户名。
密码	登录服务器的密码。

### 注意：

在腾讯云官网购买的云服务器，您可以登录 [云服务器控制台](#) 获取服务器 IP 地址、用户名及密码。

当前 Tomcat 服务器安装在 `/usr` 目录下，例如，Tomcat 文件夹名称为 `tomcat9.0.40`。则 `/usr/*/conf` 实际为 `/usr/tomcat9.0.40/conf`。

## 操作步骤

### 证书安装

1. 请在 [SSL 证书管理控制台](#) 中选择您需要安装的证书并单击**下载**。
2. 在弹出的“证书下载”窗口中，服务器类型选择 **Tomcat**，单击**下载**并解压缩 `cloud.tencent.com` 证书文件包到本地目录。  
解压缩后，可获得相关类型的证书文件。其中包含 `cloud.tencent.com_tomcat` 文件夹：  
**文件夹名称：** `cloud.tencent.com_tomcat`  
**文件夹内容：**  
`cloud.tencent.com.pfx` 证书文件  
`keystorePass.txt` 密码文件（若已设置私钥密码，则无 `keystorePass.txt` 密码文件）
3. 使用“WinSCP”（即本地与远程计算机间的复制文件工具）登录 Tomcat 服务器。
4. 将已获取到的 `cloud.tencent.com.pfx` 证书文件从本地目录拷贝至 `/usr/*/conf` 目录下。
5. 远程登录 Tomcat 服务器。例如，使用“[PuTTY](#)”工具登录。
6. 编辑在 `/usr/*/conf` 目录下的 `server.xml` 文件。并根据实际需求从以下方式中选择一种进行操作：

#### 说明：

使用方式1配置时，Tomcat 将自动为您选择 SSL 的实现方式。如果您按照方式1无法完成后续配置，可能是因为您的环境不支持该实现方式。您可以根据环境属性，使用方式2手动选择 SSL 进行配置。

方式1：自动选择 SSL

方式2：手动选择 SSL

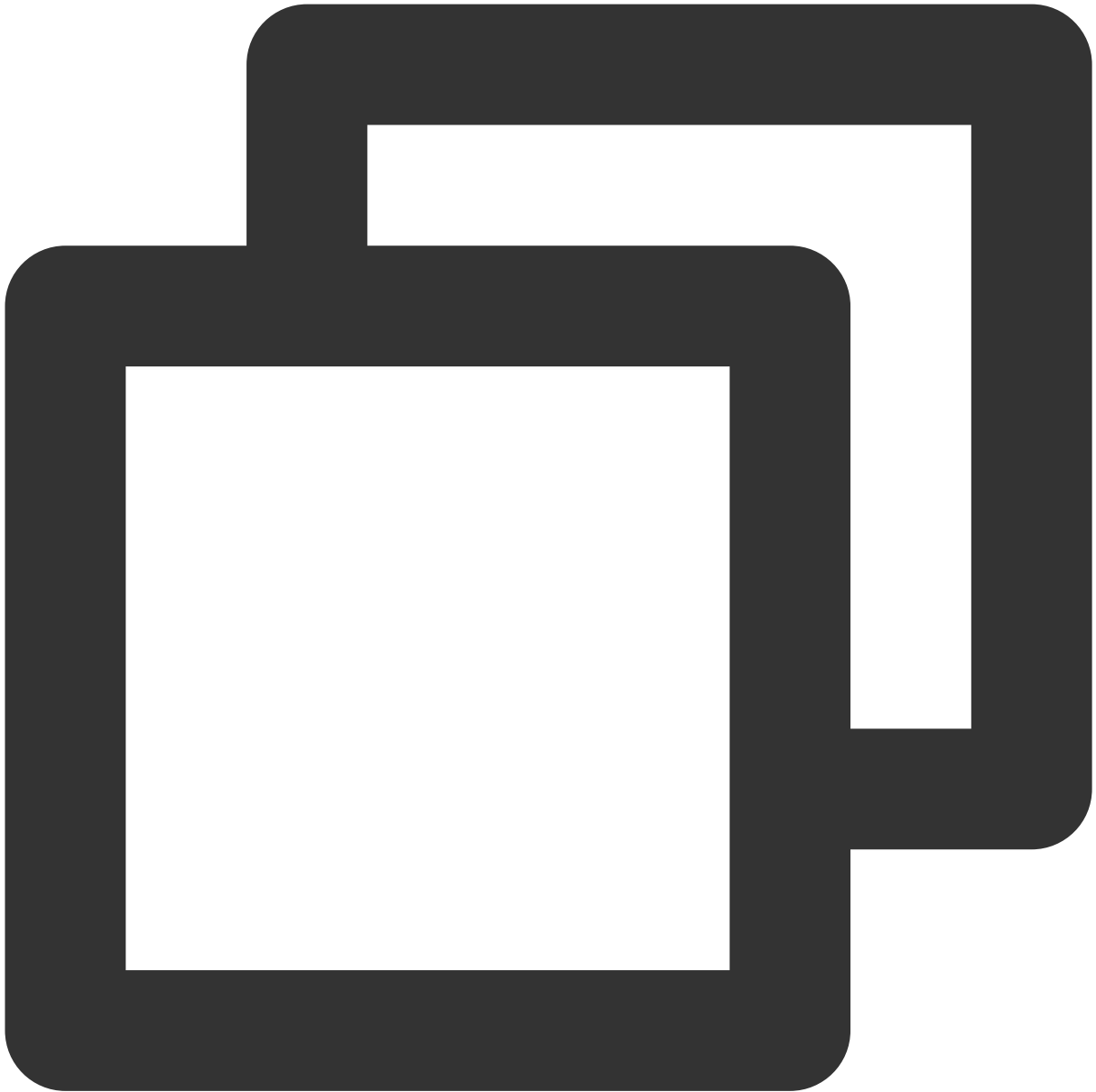
修改 `server.xml` 文件 `Connector` 的属性为以下内容：





```
<Connector port="443"  
protocol="HTTP/1.1"  
  SSLEnabled="true"  
  scheme="https"  
  secure="true"  
  keystoreFile="/usr/*/conf/cloud.tencent.com.pfx" #证书保存的路径  
  keystoreType="PKCS12"  
  keystorePass="证书密码" # 请替换为 keystorePass.txt 密码文件中的内容。  
  clientAuth="false"  
  SSLProtocol="TLSv1.1+TLSv1.2+TLSv1.3"  
  ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RS
```

修改 `server.xml` 文件 `Connector` 的属性为以下内容：



```
<Connector
  protocol="org.apache.coyote.http11.Http11NioProtocol"
  port="443" maxThreads="200"
  scheme="https" secure="true" SSLEnabled="true"
  keystoreFile="/usr/*/conf/cloud.tencent.com.pfx" keystorePass="证书密码" #pfx替换
  clientAuth="false" sslProtocol="TLS"/>
```

配置文件的主要参数说明如下：

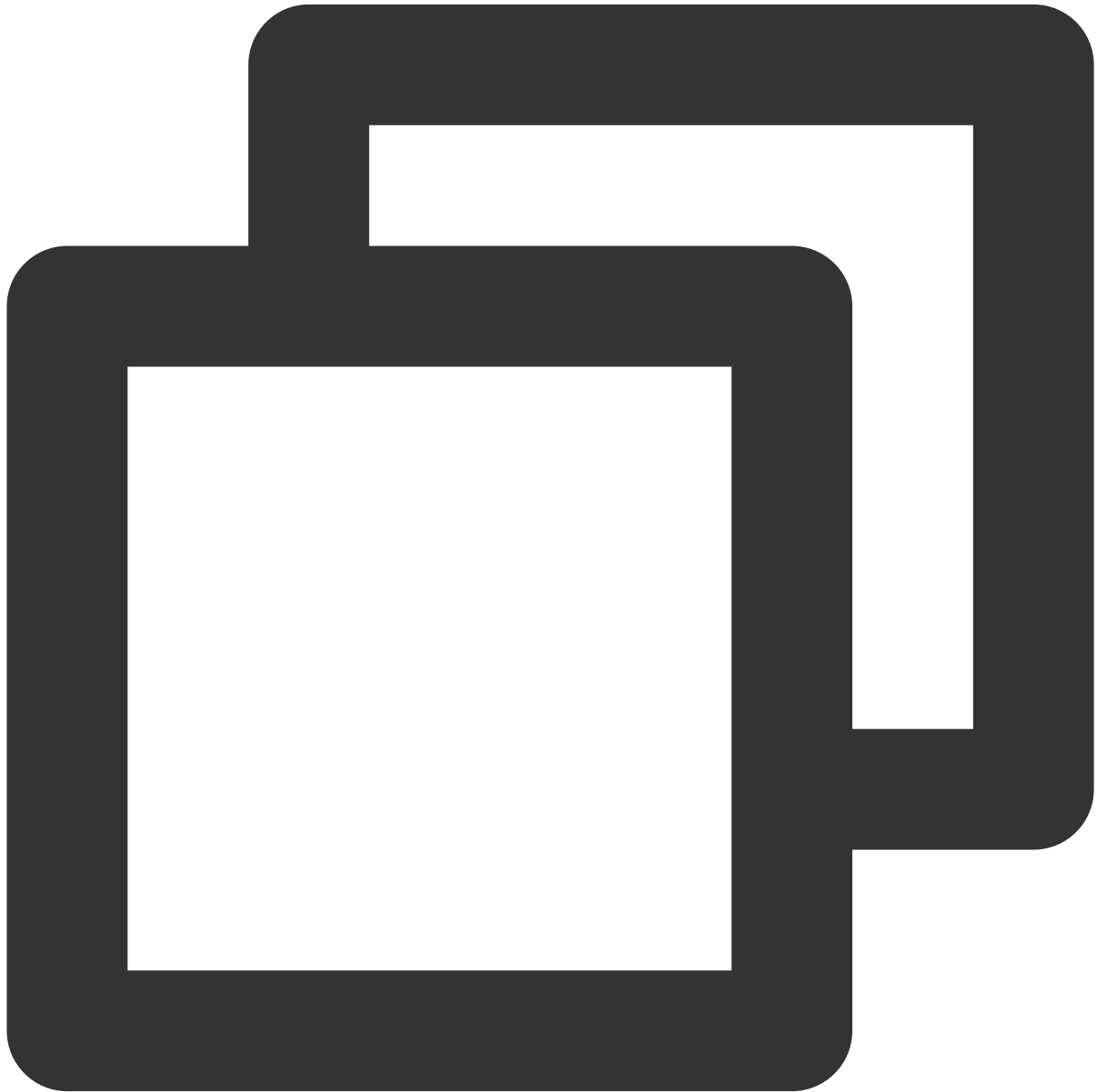
**keystoreFile**：证书文件的存放位置，可以指定绝对路径，也可以指定相对于 <CATALINA\_HOME>（Tomcat 安装目录）环境变量的相对路径。如果此项没有设定，默认情况下，Tomcat 将从当前操作系统用户的用户目录下读取名为“.keystore”的文件。

**keystorePass**：密码文件密码，指定 keystore 的密码。申请证书时若设置了私钥密码，请填写私钥密码；若申请证书时未设置私钥密码，请填写 `cloud.tencent.com_tomcat` 文件夹中 `keystorePass.txt` 文件内的密码。

**clientAuth**：如果设为 true，表示 Tomcat 要求所有的 SSL 客户出示安全证书，对 SSL 客户进行身份验证。

7. 确认 Tomcat 服务器是否启动。

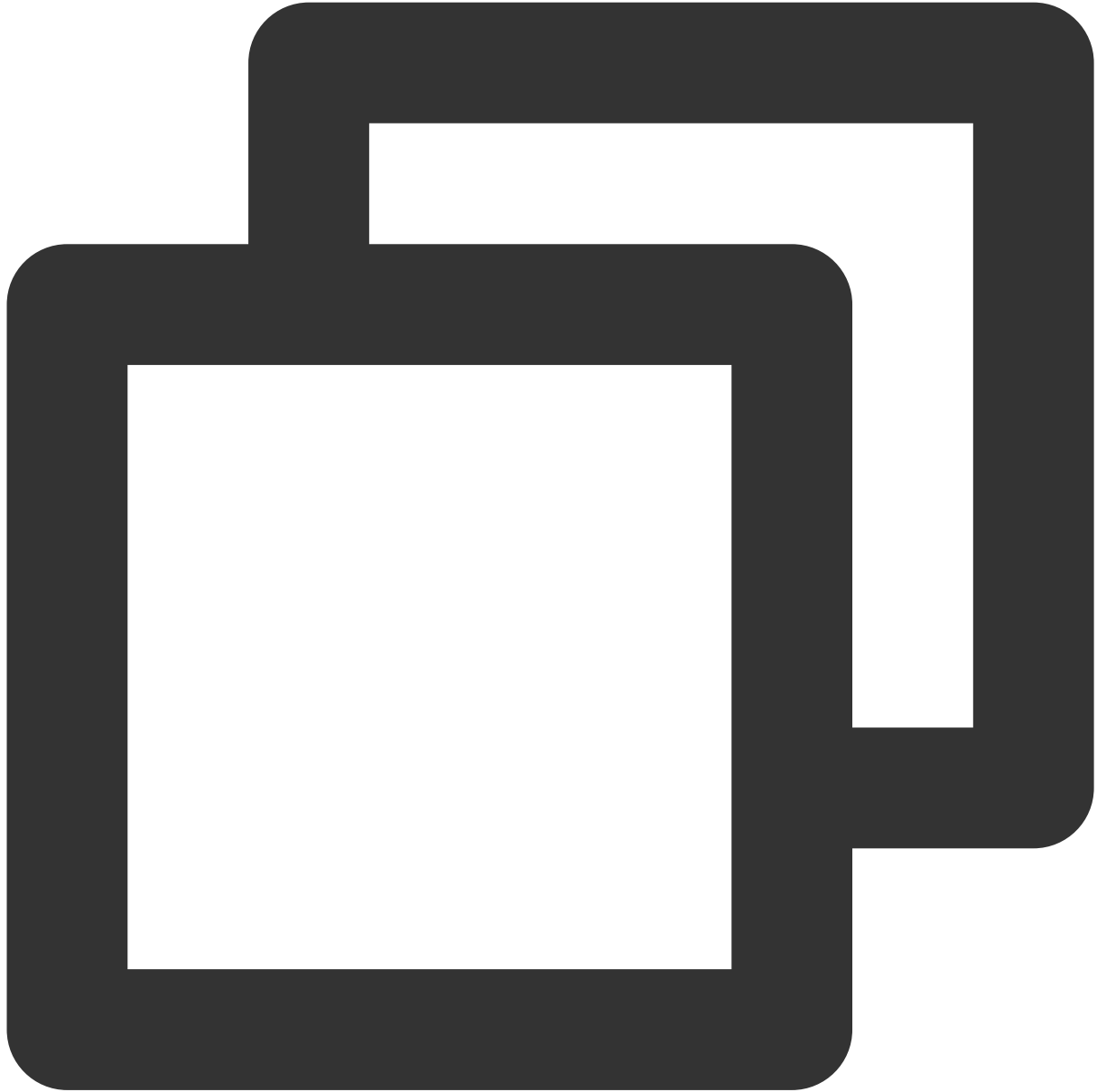
若已启动，您需要在 `/usr/*/bin` 目录下依次执行以下命令，关闭和重启 Tomcat 服务器。



```
./shutdown.sh （关闭 Tomcat 服务器）
```

```
./startup.sh (启动 Tomcat 服务器)
```

若未启动，您需要在 `/usr/*/bin` 目录下执行以下命令，启动 Tomcat 服务器。



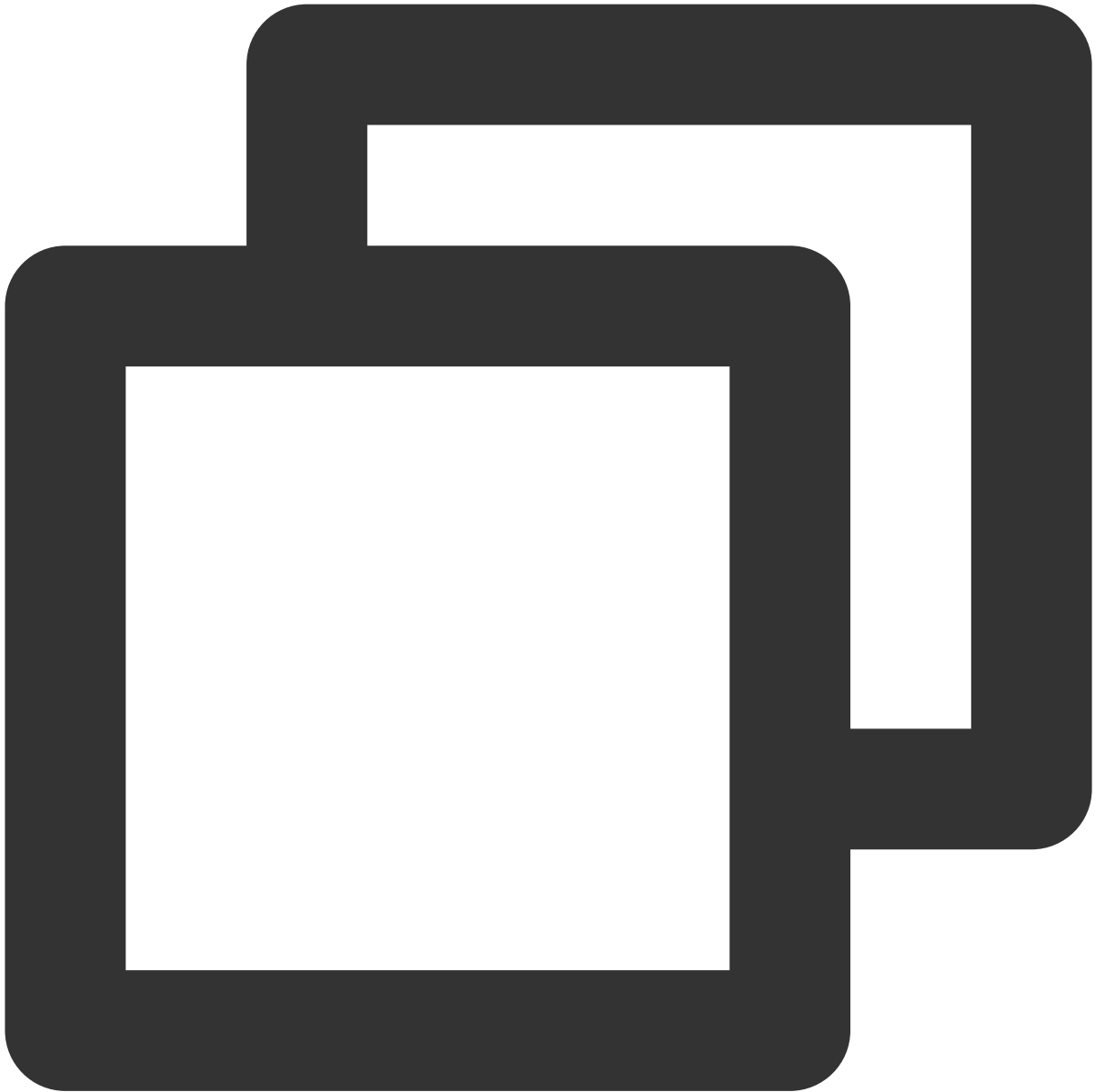
```
./startup.sh
```

8. 若启动成功，即可使用 `https://cloud.tencent.com` 进行访问。

### HTTP 自动跳转 HTTPS 的安全配置（可选）

如果您需要将 HTTP 请求自动重定向到 HTTPS。您可以通过以下操作设置：

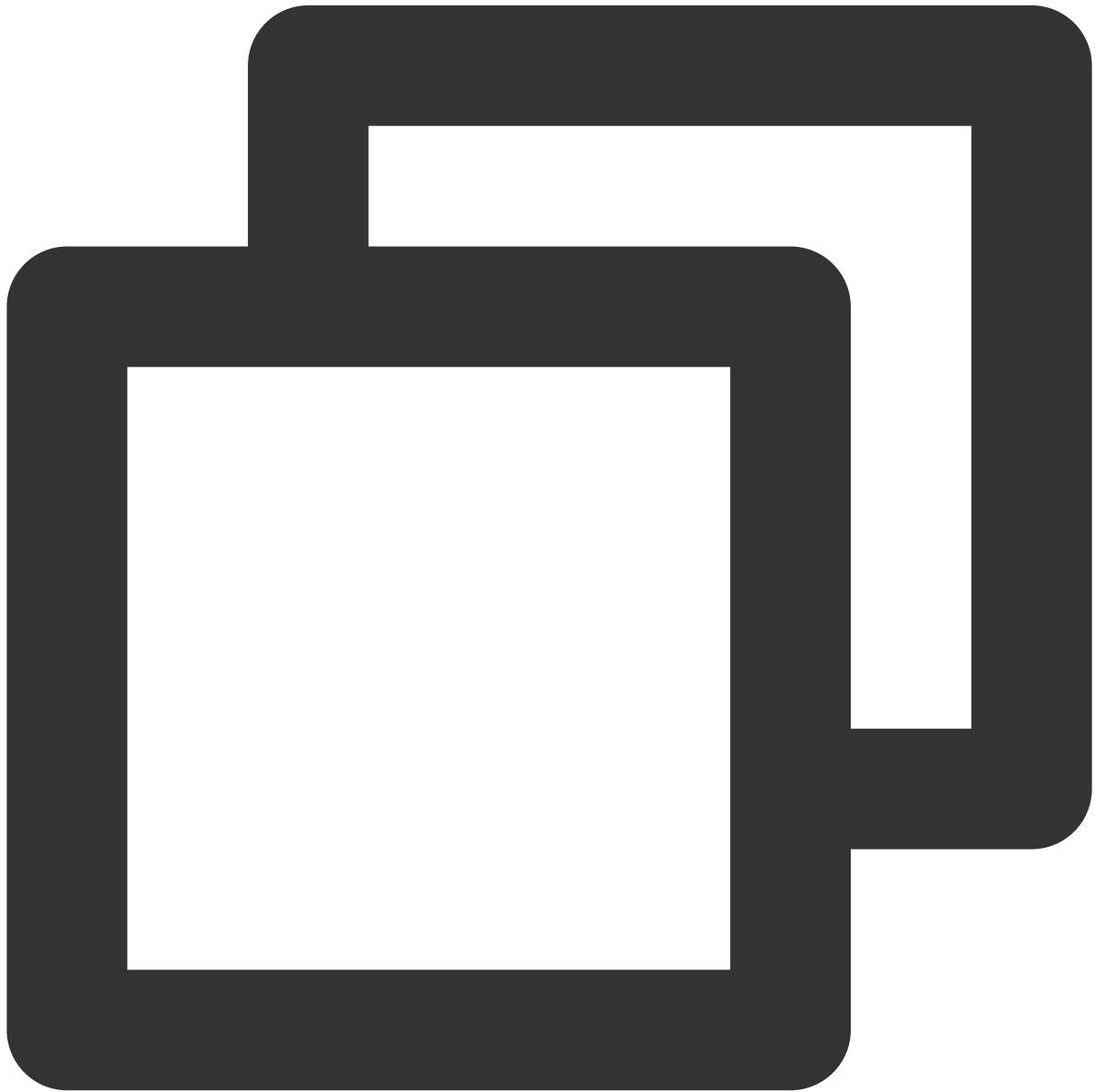
1. 编辑 `/usr/*/conf` 目录下的 `web.xml` 文件，找到 `</welcome-file-list>` 标签。
2. 请在结束标签 `</welcome-file-list>` 后面换行，并添加以下内容。



```
<login-config>
  <!-- Authorization setting for SSL -->
  <auth-method>CLIENT-CERT</auth-method>
  <realm-name>Client Cert Users-only Area</realm-name>
</login-config>
<security-constraint>
  <!-- Authorization setting for SSL -->
  <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>
```

3. 编辑 `/usr/*/conf` 目录下的 `server.xml` 文件，将 `redirectPort` 参数修改为 SSL 的 connector 的端口，即 443 端口。如下所示：

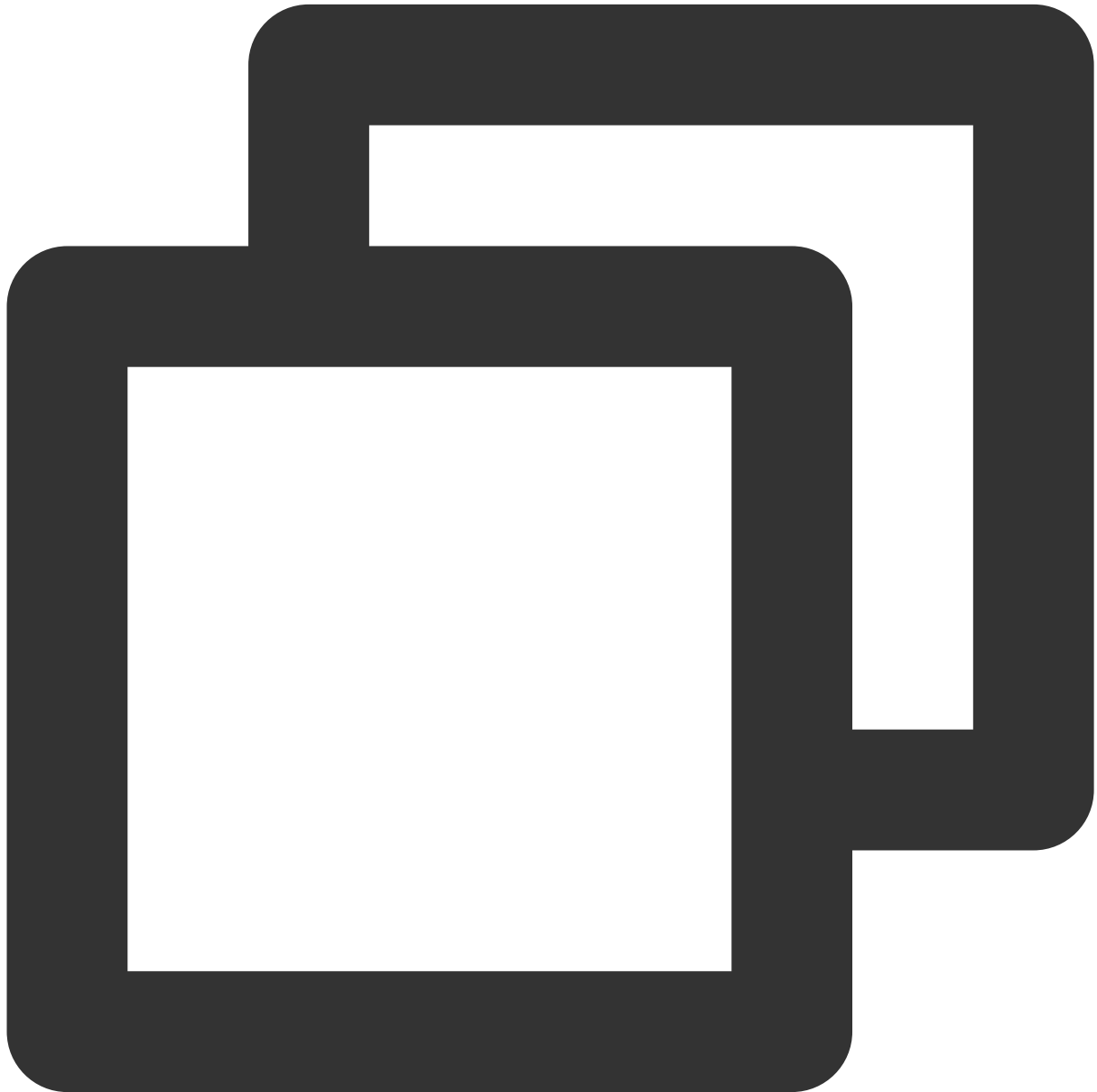


```
<Connector port="80" protocol="HTTP/1.1"  
  connectionTimeout="20000"  
  redirectPort="443" />
```

**说明：**

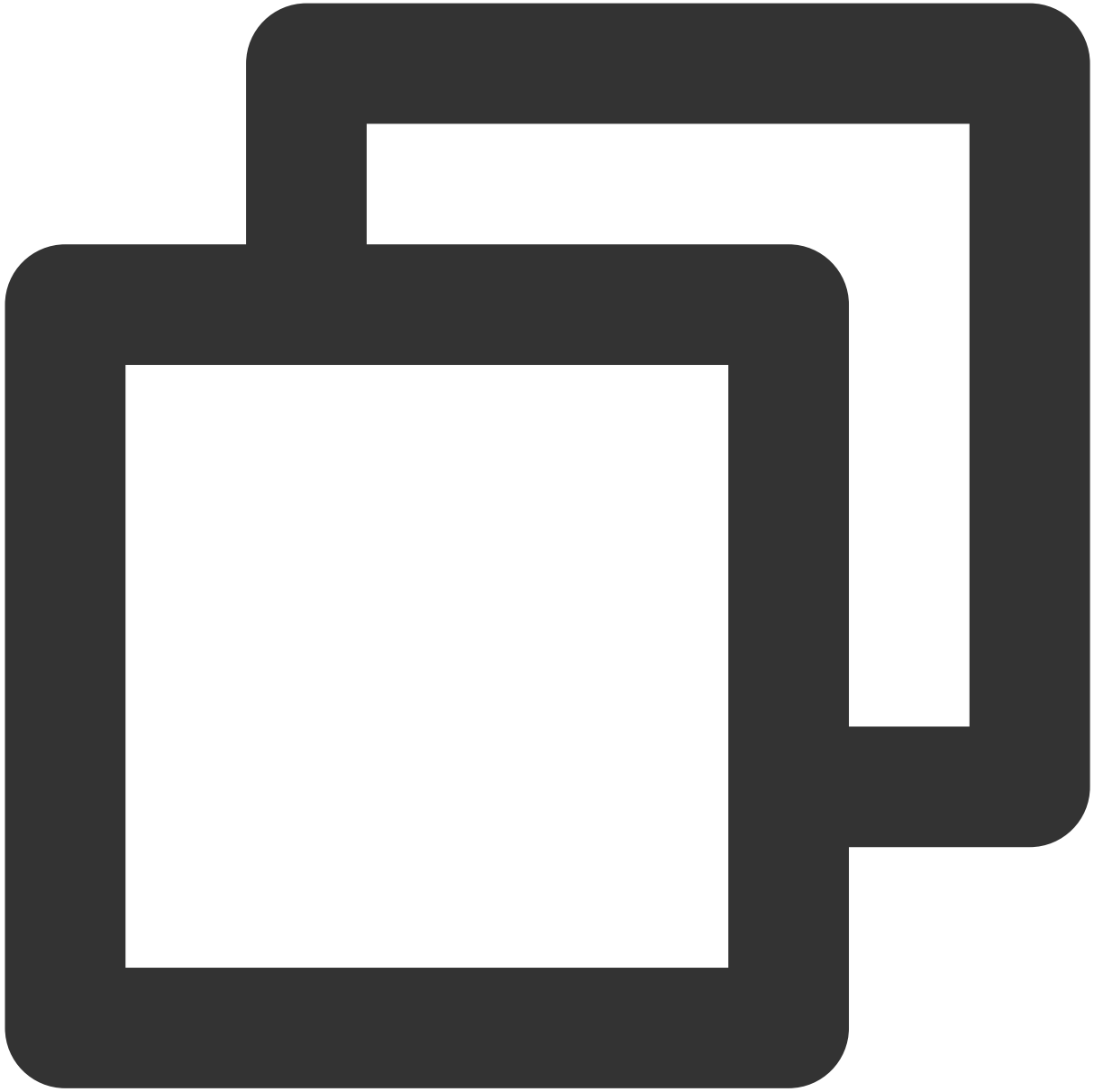
此修改操作可将非 SSL 的 connector 跳转到 SSL 的 connector 中。

4. 在 `/usr/*/bin` 目录下执行以下命令，关闭 Tomcat 服务器。



```
./shutdown.sh
```

5. 执行以下命令，确认配置是否存在问题。



```
./configtest.sh
```

若存在，请您重新配置或者根据提示修改存在问题。

若不存在，请执行下一步。

6. 执行以下命令，启动 Tomcat 服务器，即可使用 `http://cloud.tencent.com` 进行访问。





```
./startup.sh
```

# GlassFish 服务器 SSL 证书安装部署

最近更新时间：2024-03-06 17:38:42

## 操作场景

本文档指导您如何在 GlassFish 服务器中安装 SSL 证书。

### 说明

本文档以证书名称 `cloud.tencent.com` 为例。

GlassFish 版本以 `glassfish-4.0` 为例。

当前服务器的操作系统为 CentOS 7，由于操作系统的版本不同，详细操作步骤略有区别。

安装 SSL 证书前，请您在 GlassFish 服务器上开启“443”端口，避免证书安装后无法启用 HTTPS。具体可参考[服务器如何开启443端口？](#)

SSL 证书文件上传至服务器方法可参考[如何将本地文件拷贝到云服务器。](#)

## 前提条件

已准备文件远程拷贝软件，例如 WinSCP（建议从官方网站获取最新版本）。

若您需部署到腾讯云云服务器，建议使用云服务器的文件上传功能。

已准备远程登录工具，例如 PuTTY 或者 Xshell（建议从官方网站获取最新版本）。

已在当前服务器中安装配置 GlassFish 服务。

安装 SSL 证书前需准备的数据如下：

名称	说明
服务器的 IP 地址	服务器的 IP 地址，用于 PC 连接到服务器。
用户名	登录服务器的用户名。
密码	登录服务器的密码。

### 注意

在腾讯云官网购买的云服务器，您可以登录[云服务器控制台](#)获取服务器 IP 地址、用户名及密码。

当您申请 SSL 证书时选择“粘贴 CSR”方式，或购买的品牌证书为 Wotrus，则不提供 Tomcat 支持的证书文件格式（.pfx 和 .jks）的下载，需要您通过手动转换格式的方式生成密钥库。其操作方法如下：

访问[转换工具](#)。

将 Nginx 文件夹中的证书文件和私钥文件上传至转换工具中，并填写密钥库密码，单击**提交**，转换为 jks 格式证书。

当前 GlassFish 服务安装在 `/usr/share` 目录下。

## 操作步骤

1. 请在 [SSL 证书管理控制台](#) 中选择您需要安装的证书并单击**下载**。
2. 在弹出的“证书下载”窗口中，服务器类型选择 **Apache、JKS**，单击**下载**并解压缩 `cloud.tencent.com` 证书文件包到本地目录。

解压缩后，可获得相关类型的证书文件。其中包含 `cloud.tencent.com_apache` 文件夹、`cloud.tencent.com_jks` 文件夹：

**文件夹名称：** `cloud.tencent.com_apache`

`cloud.tencent.com.crt` 证书文件

`cloud.tencent.com.key` 私钥文件

**CSR 文件内容：** `cloud.tencent.com.csr` 文件

### 说明

CSR 文件是申请证书时由您上传或系统在线生成的，提供给 CA 机构。安装时可忽略该文件。

3. 远程登录 GlassFish 服务器。

4. 进入 `/usr/share/glassfish4/glassfish/bin` 目录下执行命令 `./asadmin` 后，需更换 domain 的管理密码，请执行命令 `change-master-password --savemasterpassword=true domain1`。如下图所示：

### 注意

`domain1` 安装默认路径为 `/usr/share/glassfish4/glassfish/domains`，`domain` 名称请根据实际情况填写。

默认密码为 `changeit`，请输入回车后再输入新密码，新密码请填写申请证书时设置的**私钥密码**。

若申请证书时未设置私钥密码，则填写 `cloud.tencent.com_jks` 文件夹中 `keystorePass.txt` 文件的密码。

5. 在 `/usr/share` 目录下执行命令 `mkdir temp` 创建 `temp` 文件夹。

6. 使用“WinSCP”（即本地与远程计算机间的复制文件工具）登录 GlassFish 服务器，将

`cloud.tencent.com.crt` 证书文件、`cloud.tencent.com.key` 私钥文件从本地目录拷贝至 `temp` 文件夹。

### 说明

WinSCP 上传文件操作可参考 [通过 WinSCP 上传文件到 Linux 云服务器](#)。

若您需部署到腾讯云云服务器，建议使用云服务器的文件上传功能。

7. 在 `temp` 目录执行以下命令生成 PKCS12 文件，并提示输入密码，请输入新设置的密码，即私钥密码。如下图所示：



```
openssl pkcs12 -export -in cloud.tencent.com.crt -inkey cloud.tencent.com.key -out
```

8. 在 `temp` 目录下执行命令 `ls -l` 确认 PKCS12 文件是否包含您申请的证书。

9. 生成 `keystore.jks` 文件，请在 `temp` 目录执行以下命令，则生成的 `keystore.jks` 文件显示在此目录下。如下所示：



```
keytool -importkeystore -destkeystore keystore.jks -srckeystore mycert.p12 -srcstor
```

10. 生成 `cacert.jks` 文件，请在 `temp` 目录执行以下命令，则生成的 `cacert.jks` 文件显示在此目录下。若提示输入密码，输入新设置的密码，即私钥密码。如下所示：



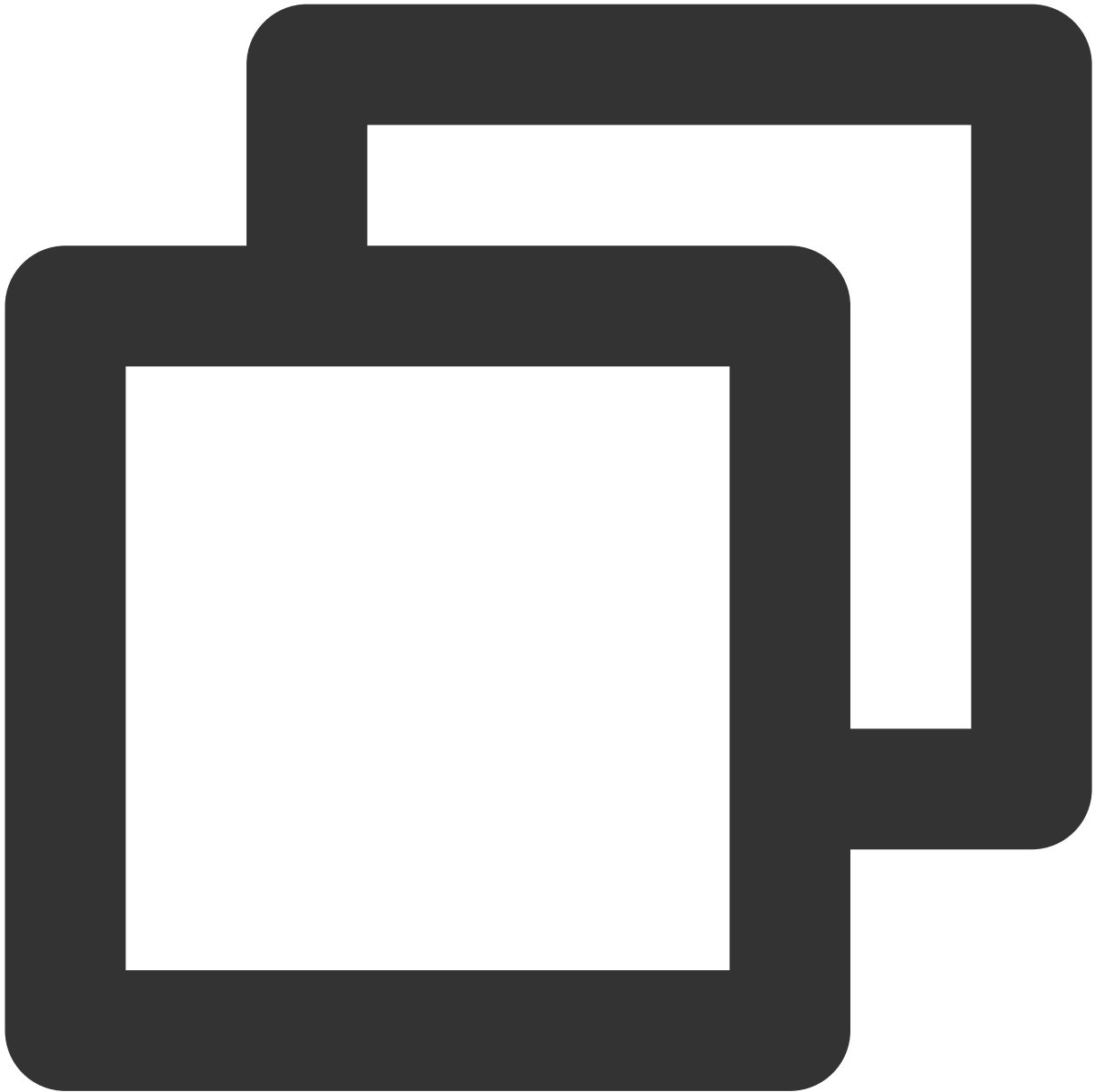
```
keytool -importcert -trustcacerts -destkeystore cacerts.jks -file cloud.tencent.com
```

执行命令后若提示是否信任此证书，请按图示进行操作。

```
Trust this certificate? [no]: yes
Certificate was added to keystore
[root@VM_4_2_centos Apache]# █
```

11. 将步骤8和步骤9生成的文件替换 `domain1/config` 目录下的 `keystore.jks` 和 `cacert.jks` 文件。

12. 编辑 `/usr/share/glassfish4/glassfish/domains/domain1/config` 目录下的 `domain.xml` 文件，修改端口号。如下所示：



```
<network-listeners>
  <network-listener port="80" protocol="http-listener-1" transport="tcp" name="
  <network-listener port="443" protocol="http-listener-2" transport="tcp" name=
  <network-listener port="4848" protocol="admin-listener" transport="tcp" name=
</network-listeners>
```

13. 启动 GlassFish 服务器，即可使用 `https://cloud.tencent.com` 进行访问。如下图所示：

```
[root@VM_4_2_centos ~]# cd /usr/share/glassfish4/glassfish/bin/  
[root@VM_4_2_centos bin]# ./asadmin  
Use "exit" to exit and "help" for online help.  
asadmin> start-domain domain1
```

如果浏览器地址栏显示安全锁标识，则说明证书安装成功。

如果网站访问异常，可参考以下常见问题解决方案进行处理：

[无法使用 HTTPS 访问网站](#)

[部署 SSL 证书后，浏览器提示“网站连接不安全”](#)

[访问站点提示连接不安全？](#)

[SSL 证书过期后重新申请部署依然提示 HTTPS 不安全？](#)

[在服务器上部署 SSL 证书后访问资源出现 404 报错](#)

### 注意

操作过程如果出现问题，请您 [联系我们](#)。



# JBoss 服务器 SSL 证书安装部署

最近更新时间：2024-03-06 17:38:42

## 操作场景

本文档指导您如何在 JBoss 服务器中安装 SSL 证书。

### 说明：

本文档以证书名称 `cloud.tencent.com` 为例。

JBoss 版本以 `jboss-7.1.1` 为例。

当前服务器的操作系统为 CentOS 7，由于操作系统的版本不同，详细操作步骤略有区别。

安装 SSL 证书前，请您在 JBoss 服务器上开启“443”端口，避免证书安装后无法启用 HTTPS。具体可参考 [服务器如何开启443端口？](#)

SSL 证书文件上传至服务器方法可参考 [如何将本地文件拷贝到云服务器。](#)

## 前提条件

已准备文件远程拷贝软件，例如 WinSCP（建议从官方网站获取最新版本）。

若您需部署到腾讯云云服务器，建议使用云服务器的文件上传功能。

已准备远程登录工具，例如 PuTTY 或者 Xshell（建议从官方网站获取最新版本）。

已在当前服务器中安装配置 JBoss 服务。

安装 SSL 证书前需准备的数据如下：

名称	说明
服务器的 IP 地址	服务器的 IP 地址，用于 PC 连接到服务器。
用户名	登录服务器的用户名。
密码	登录服务器的密码。

### 注意：

在腾讯云官网购买的云服务器，您可以登录 [云服务器控制台](#) 获取服务器 IP 地址、用户名及密码。

当您申请 SSL 证书时选择“粘贴 CSR”方式，或购买的品牌证书为 Wotrus，则不提供 JKS 证书文件的下载，需要您通过手动转换格式的方式生成密钥库。其操作方法如下：

访问 [转换工具](#)。

将 Nginx 文件夹中的证书文件和私钥文件上传至转换工具中，并填写密钥库密码，单击提交，转换为 jks 格式证书。

当前 JBoss 服务器安装在 `/usr/local` 目录下。

当您申请 SSL 证书时选择“粘贴 CSR”方式，或购买的品牌证书为 Wotrus，则不提供 JKS 证书文件的下载，需要您通过手动转换格式的方式生成密钥库。其操作方法如下：

访问 [转换工具](#)。

将 Nginx 文件夹中的证书文件和私钥文件上传至转换工具中，并填写密钥库密码，单击**提交**，转换为 jks 格式证书。

当前 JBoss 服务器安装在 `/usr/local` 目录下。

## 操作步骤

1. 请在 [SSL 证书管理控制台](#) 中选择您需要安装的证书并单击**下载**。
2. 在弹出的“证书下载”窗口中，服务器类型选择 **JKS**，单击**下载**并解压缩 `cloud.tencent.com` 证书文件包到本地目录。

解压缩后，可获得相关类型的证书文件。其中包含 `cloud.tencent.com_jks` 文件夹：

**文件夹名称：** `cloud.tencent.com_jks`

**文件夹内容：**

`cloud.tencent.com.jks` 密钥库

`keystorePass.txt` 密码文件（若已设置私钥密码，则无 `keystorePass.txt` 密码文件）

3. 远程登录 JBoss 服务器。例如，使用“[PuTTY](#)”工具登录。
4. 进入部署证书步骤，在 `/usr/local/jboss-7.1.1/standalone/configuration` 目录下执行命令 `mkdir cert` 创建 `cert` 文件夹。
5. 使用“WinSCP”（即本地与远程计算机间的复制文件工具）登录 JBoss 服务器，将已获取到的 `cloud.tencent.com.jks` 密钥库文件从本地目录拷贝至 `cert` 文件夹。

**说明：**

WinSCP 上传文件操作可参考 [通过 WinSCP 上传文件到 Linux 云服务器](#)。

若您需部署到腾讯云云服务器，建议使用云服务器的文件上传功能。

6. 编辑在 `/usr/local/jboss-7.1.1/standalone/configuration` 目录下的 `standalone.xml` 文件。修改端口配置，如下所示：

第一部分：



```
<interfaces>
  <interface name="management">
    <inet-address value="{jboss.bind.address.management:127.0.0.1}"/>
  </interface>
  <!--开启远程访问-->
  <interface name="public">
    <inet-address value="{jboss.bind.address:0.0.0.0}"/>
  </interface>
  <interface name="unsecure">
    <inet-address value="{jboss.bind.address.unsecure:127.0.0.1}"/>
  </interface>
</interfaces>
```

```
</interfaces>
<socket-binding-group name="standard-sockets" default-interface="public" port-offs
  <socket-binding name="management-native" interface="management" port="${jboss.
  <socket-binding name="management-http" interface="management" port="${jboss.ma
  <socket-binding name="management-https" interface="management" port="${jboss.m
  <socket-binding name="ajp" port="8009"/>
    <!--修改http端口-->
  <socket-binding name="http" port="80"/>
    <!--修改https端口-->
  <socket-binding name="https" port="443"/>
  <socket-binding name="osgi-http" interface="management" port="8090"/>
  <socket-binding name="remoting" port="4447"/>
  <socket-binding name="txn-recovery-environment" port="4712"/>
  <socket-binding name="txn-status-manager" port="4713"/>
  <outbound-socket-binding name="mail-smtp">
    <remote-destination host="localhost" port="25"/>
  </outbound-socket-binding>
</socket-binding-group>
```

配置文件的主要调整说明如下：

**开启远程访问：**将 `${jboss.bind.address:127.0.0.1}` 调整为

`${jboss.bind.address:0.0.0.0}`。

**修改 http 端口：**将8080端口调整为80。

**修改 https 端口：**将8443端口调整为443。

第二部分：添加证书相关配置。



```
<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-host" n
  <connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="h
  <connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding=
    <ssl name="https" password="*****" certificate-key-file="../standalon
  </connector>
  <virtual-server name="default-host" enable-welcome-root="true">
    <alias name="localhost"/>
    <alias name="example.com"/>
  </virtual-server>
</subsystem>
```

7. 进入 `/usr/local/jboss-7.1.1/bin` 目录下，执行启动命令 `./standalone.sh`，确保正常启动。如下图所示：

```
[root@VM_4_2_centos ~]# cd /usr/local/jboss-7.1.1/bin
[root@VM_4_2_centos bin]# ./standalone.sh
```

8. 证书已部署完成，即可使用 `https://cloud.tencent.com` 进行访问。

如果浏览器地址栏显示安全锁标识，则说明证书安装成功。

如果网站访问异常，可参考以下常见问题解决方案进行处理：

[无法使用 HTTPS 访问网站](#)

[部署 SSL 证书后，浏览器提示“网站连接不安全”](#)

[访问站点提示连接不安全？](#)

[在服务器上部署 SSL 证书后访问资源出现 404 报错](#)

**注意：**

操作过程如果出现问题，请您 [联系我们](#)。

# Jetty 服务器 SSL 证书安装部署

最近更新时间：2024-03-06 17:38:42

## 操作场景

本文档指导您如何在 Jetty 服务器中安装 SSL 证书。

### 说明：

本文档以证书名称 `cloud.tencent.com` 为例。

Jetty 版本以 `jetty-distribution-9.4.28.v20200408` 为例。

当前服务器的操作系统为 CentOS 7，由于操作系统的版本不同，详细操作步骤略有区别。

安装 SSL 证书前，请您在 Jetty 服务器上开启“443”端口，避免证书安装后无法启用 HTTPS。具体可参考 [服务器如何开启443端口？](#)

SSL 证书文件上传至服务器方法可参考 [如何将本地文件拷贝到云服务器](#)。

## 前提条件

已准备文件远程拷贝软件，例如 WinSCP（建议从官方网站获取最新版本）。

若您需部署到腾讯云云服务器，建议使用云服务器的文件上传功能。

已准备远程登录工具，例如 PuTTY 或者 Xshell（建议从官方网站获取最新版本）。

已在当前服务器中安装配置 Jetty 服务。

安装 SSL 证书前需准备的数据如下：

名称	说明
服务器的 IP 地址	服务器的 IP 地址，用于 PC 连接到服务器。
用户名	登录服务器的用户名。
密码	登录服务器的密码。

### 注意：

在腾讯云官网购买的云服务器，您可以登录 [云服务器控制台](#) 获取服务器 IP 地址、用户名及密码。

当您申请 SSL 证书时选择“粘贴 CSR”方式，或购买的品牌证书为 Wotrus，则不提供 JKS 证书文件的下载，需要您通过手动转换格式的方式生成密钥库。其操作方法如下：

访问 [转换工具](#)。

将 Nginx 文件夹中的证书文件和私钥文件上传至转换工具中，并填写密钥库密码，单击**提交**，转换为 jks 格式证书。

当前 Jetty 服务器安装在 `/usr/local/jetty` 目录下。

## 操作步骤

1. 请在 [SSL 证书管理控制台](#) 中选择您需要安装的证书并单击**下载**。
2. 在弹出的“证书下载”窗口中，服务器类型选择 **JKS**，单击**下载**并解压缩 `cloud.tencent.com` 证书文件包到本地目录。

解压缩后，可获得相关类型的证书文件。其中包含 `cloud.tencent.com_jks` 文件夹：

**文件夹名称：** `cloud.tencent.com_jks`

**文件夹内容：**

`cloud.tencent.com.jks` 密钥库

`keystorePass.txt` 密码文件（若已设置私钥密码，则无 `keystorePass.txt` 密码文件）

3. 远程登录 Jetty 服务器。例如，使用“[PuTTY](#)”工具登录。
4. 进入部署证书步骤，在 `/usr/local/jetty/jetty-distribution-9.4.28.v20200408/etc` 目录下执行命令 `mkdir cert` 创建 `cert` 文件夹。
5. 使用“WinSCP”（即本地与远程计算机间的复制文件工具）登录 Jetty 服务器，将已获取到的 `cloud.tencent.com.jks` 密钥库文件从本地目录拷贝至 `cert` 文件夹。

**说明：**

WinSCP 上传文件操作可参考 [通过 WinSCP 上传文件到 Linux 云服务器](#)。

若您需部署到腾讯云云服务器，建议使用云服务器的文件上传功能。

6. 编辑 `/usr/local/jetty/jetty-distribution-9.4.28.v20200408/etc` 目录下的 `jetty-ssl-context.xml` 文件，如下所示：

**说明：**

**KeyStorePath**：默认值 `default` 请填写证书存放的路径。

**KeyStorePassword**：默认值 `default` 请填写密钥库密码，指定 `keystore` 的密码。申请证书时若设置了私钥密码，请填写私钥密码；若申请证书时未设置私钥密码，请填写 `cloud.tencent.com_jks` 文件夹中 `keystorePass.txt` 文件的密码。

**KeyManagerPassword**：请填写 `cloud.tencent.com_jks` 文件夹中 `keystorePass.txt` 文件的密码。

**TrustStorePath**：默认值 `default` 请填写证书存放的路径。

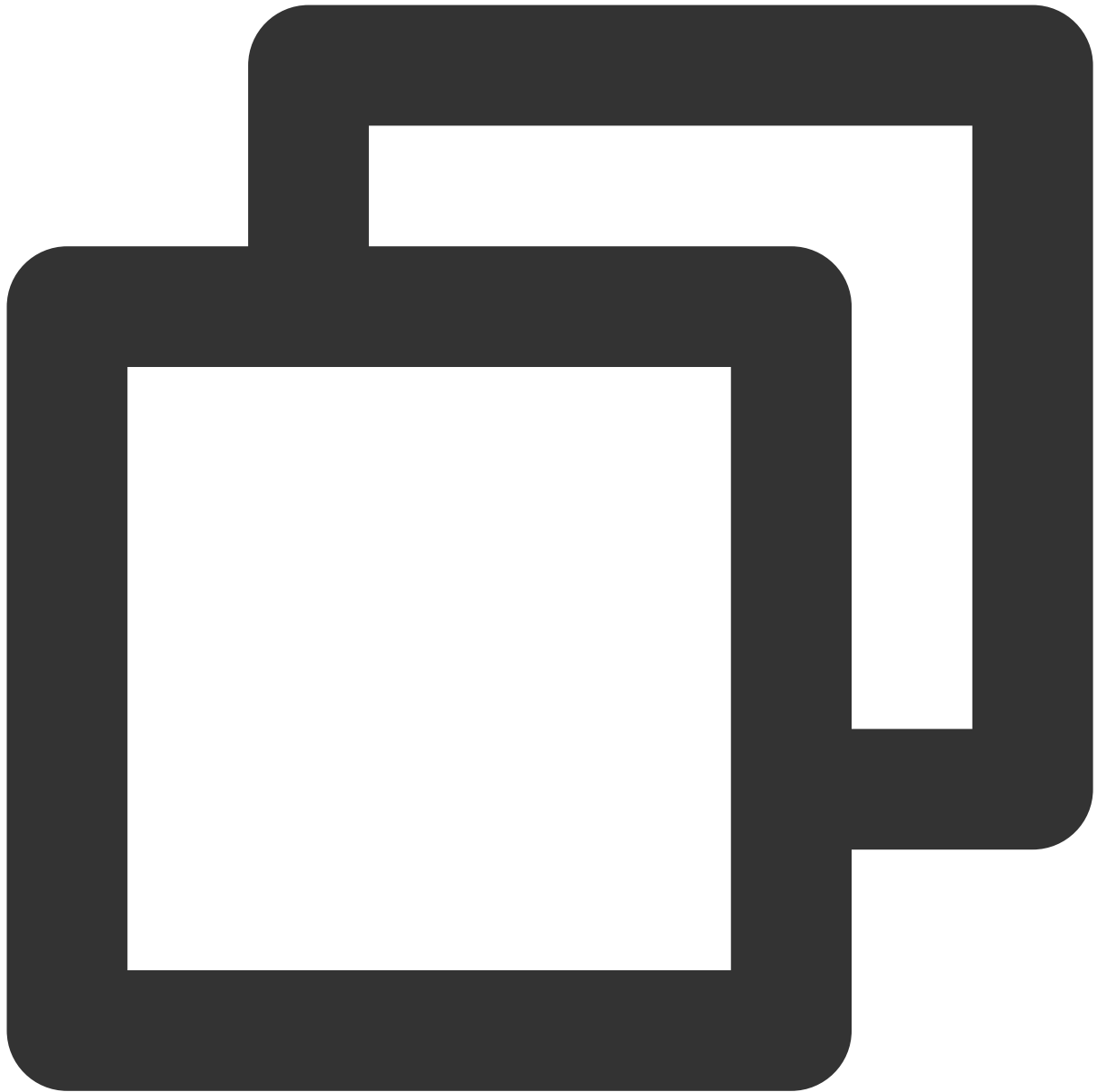




```
<?xml version="1.0"?><!DOCTYPE Configure PUBLIC "-//Jetty//Configure//EN" "http://w
<!-- ===== --><!-- SSL Cont
<!--
  To configure Includes / Excludes for Cipher Suites or Protocols see tweak-ssl.xml
  https://www.eclipse.org/jetty/documentation/current/configuring-ssl.html#configur
-->
<Configure id="sslContextFactory" class="org.eclipse.jetty.util.ssl.SslContextFacto
  <Set name="Provider"><Property name="jetty.sslContext.provider"/></Set>
  <Set name="KeyStorePath"><Property name="jetty.base" default="." /></Property nam
  <Set name="KeyStorePassword"><Property name="jetty.sslContext.keyStorePassword" d
  <Set name="KeyStoreType"><Property name="jetty.sslContext.keyStoreType" default="
```

```
<Set name="KeyStoreProvider"><Property name="jetty.sslContext.keyStoreProvider"/>
<Set name="KeyManagerPassword"><Property name="jetty.sslContext.keyManagerPasswor
<Set name="TrustStorePath"><Property name="jetty.base" default="." /></Property n
<Set name="TrustStorePassword"><Property name="jetty.sslContext.trustStorePasswor
<Set name="TrustStoreType"><Property name="jetty.sslContext.trustStoreType"/></Se
<Set name="TrustStoreProvider"><Property name="jetty.sslContext.trustStoreProvide
<Set name="EndpointIdentificationAlgorithm"><Property name="jetty.sslContext.endp
<Set name="NeedClientAuth"><Property name="jetty.sslContext.needClientAuth" depre
<Set name="WantClientAuth"><Property name="jetty.sslContext.wantClientAuth" depre
<Set name="useCipherSuitesOrder"><Property name="jetty.sslContext.useCipherSuites
<Set name="sslSessionCacheSize"><Property name="jetty.sslContext.sslSessionCacheS
<Set name="sslSessionTimeout"><Property name="jetty.sslContext.sslSessionTimeout"
<Set name="RenegotiationAllowed"><Property name="jetty.sslContext.renegotiationAl
<Set name="RenegotiationLimit"><Property name="jetty.sslContext.renegotiationLimi
<Set name="SniRequired"><Property name="jetty.sslContext.sniRequired" default="fa
<!-- Example of how to configure a PKIX Certificate Path revocation Checker
<Call id="pkixPreferCrls" class="java.security.cert.PKIXRevocationChecker$Option"
<Call id="pkixSoftFail" class="java.security.cert.PKIXRevocationChecker$Option" n
<Call id="pkixNoFallback" class="java.security.cert.PKIXRevocationChecker$Option"
<Call class="java.security.cert.CertPathBuilder" name="getInstance">
<Arg>PKIX</Arg>
<Call id="pkixRevocationChecker" name="getRevocationChecker">
  <Call name="setOptions">
    <Arg>
      <Call class="java.util.EnumSet" name="of">
        <Arg><Ref refid="pkixPreferCrls"/></Arg>
        <Arg><Ref refid="pkixSoftFail"/></Arg>
        <Arg><Ref refid="pkixNoFallback"/></Arg>
      </Call>
    </Arg>
  </Call>
</Call>
</Call>
</Call>
<Set name="PkixCertPathChecker"><Ref refid="pkixRevocationChecker"/></Set>
-->
</Configure>
```

7. 编辑 `/usr/local/jetty/jetty-distribution-9.4.28.v20200408/etc` 目录下的 `jetty-ssl.xml` 文件，修改端口为443。如下所示：



```
<Call name="addConnector">
<Arg>
  <New id="sslConnector" class="org.eclipse.jetty.server.ServerConnector">
    <Arg name="server"><Ref refid="Server" /></Arg>
    <Arg name="acceptors" type="int"><Property name="jetty.ssl.acceptors" deprecate="true" /></Arg>
    <Arg name="selectors" type="int"><Property name="jetty.ssl.selectors" deprecate="true" /></Arg>
    <Arg name="factories">
      <Array type="org.eclipse.jetty.server.ConnectionFactory">
        <!-- uncomment to support proxy protocol
        <Item>
          <New class="org.eclipse.jetty.server.ProxyConnectionFactory"/>
        </Item>
      </Array>
    </Arg>
  </New>
</Arg>
</Call>
```

```
        </Item>-->
    </Array>
</Arg>
<Set name="host"><Property name="jetty.ssl.host" deprecated="jetty.host" /></S
<Set name="port"><Property name="jetty.ssl.port" deprecated="ssl.port" default
<Set name="idleTimeout"><Property name="jetty.ssl.idleTimeout" deprecated="ssl
<Set name="acceptorPriorityDelta"><Property name="jetty.ssl.acceptorPriorityDe
<Set name="acceptQueueSize"><Property name="jetty.ssl.acceptQueueSize" depreca
<Get name="SelectorManager">
    <Set name="connectTimeout"><Property name="jetty.ssl.connectTimeout" default
</Get>
</New>
</Arg>
</Call>
```

8. 编辑 `/usr/local/jetty/jetty-distribution-9.4.28.v20200408` 目录下的 `start.ini` 文件，添加如下内容：



```
etc/jetty-ssl.xml  
etc/jetty-ssl-context.xml  
etc/jetty-https.xml
```

9. 证书已部署完成，在 **jetty** 根目录下，执行启动命令 `java -jar start.jar`，即可使用 `https://cloud.tencent.com` 访问。

如果浏览器地址栏显示安全锁标识，则说明证书安装成功。

如果网站访问异常，可参考以下常见问题解决方案进行处理：

[无法使用 HTTPS 访问网站](#)

部署 SSL 证书后，浏览器提示“网站连接不安全”

访问站点提示连接不安全？

在服务器上部署 SSL 证书后访问资源出现 404 报错

## 注意事项

证书部署成功后，使用 `https://cloud.tencent.com` 访问若显示如下：

### Error 404 - Not Found.

No context on this server matched or handled this request.

Contexts known to this server are:

Context Path	Display Name	Status	LifeCycle
--------------	--------------	--------	-----------

 [Powered by Eclipse Jetty:// Server](#)

解决方案：您可以将 `/usr/local/jetty/jetty-distribution-9.4.28.v20200408/demo-base/webapps` 目录下的 ROOT 文件复制到 `/usr/local/jetty/jetty-distribution-9.4.28.v20200408/webapps` 目录下，重启 jetty，即可访问成功。

**注意：**

操作过程如果出现问题，请您 [联系我们](#)。

# IIS 服务器 SSL 证书安装部署

最近更新时间：2024-03-06 17:38:42

## 操作场景

本文档指导您如何在 IIS 中安装 SSL 证书。

### 说明：

本文档以证书名称 `cloud.tencent.com` 为例，实际名称请以您申请的证书为准。

本文档以操作系统 Windows Server 2012 R2 为例。由于操作系统的版本不同，详细操作步骤略有区别。

安装 SSL 证书前，请您在 IIS 服务器上开启“443”端口，避免证书安装后无法启用 HTTPS。具体可参考 [服务器如何开启443端口？](#)

SSL 证书文件上传至服务器方法可参考 [如何将本地文件拷贝到云服务器。](#)

## 操作步骤

### 证书安装

1. 请在 [SSL 证书管理控制台](#) 中选择您需要安装的证书并单击**下载**。
2. 在弹出的**证书下载**窗口中，服务器类型选择 **IIS**，单击**下载**并解压缩 `cloud.tencent.com` 证书文件包到本地目录。

解压缩后，可获得相关类型的证书文件。其中包含 `cloud.tencent.com.iis` 文件夹：

文件夹名称：`cloud.tencent.com.iis`

文件夹内容：

`cloud.tencent.com.pfx` 证书文件

`keystorePass.txt` 密码文件（若已设置私钥密码，则无 `keystorePass.txt` 密码文件）

3. 打开 IIS 服务管理器，选择计算机名称，双击打开**服务器证书**。
4. 在服务器证书窗口的右侧**操作**栏中，单击**导入**。
5. 在弹出的**导入证书**窗口中，选择证书文件存放路径，输入密码，单击**确定**。如下图所示：

### 说明：

申请证书时若设置了私钥密码，输入密码时，请输入私钥密码。若申请证书时未设置私钥密码，输入密码时，请输入 `cloud.tencent.com.iis` 文件夹中 `keystorePass.txt` 文件的密码。

如果私钥密码不慎遗忘，请 [工单联系](#) 腾讯云工程师删除该证书，然后重新申请该域名证书。

6. 选择网站下的站点名称，并单击右侧**操作**栏的**绑定**。
7. 在弹出的**网站绑定**窗口中，单击**添加**。
8. 在**添加网站绑定**的窗口中，将网站类型设置为 `https`，IP 地址设置为全部未分配，端口设置为 `443`，主机名请填写您当前申请证书的域名，并指定对应的 SSL 证书，单击**确定**。

9. 添加完成后，即可在“网站绑定”窗口中查看到新添加的内容。

10. 请使用 `https://cloud.tencent.com` 进行访问。

如果浏览器地址栏显示安全锁标识，则说明证书安装成功。

如果网站访问异常，可参考以下常见问题解决方案进行处理：

[无法使用 HTTPS 访问网站](#)

[部署 SSL 证书后，浏览器提示“网站连接不安全”](#)

[访问站点提示连接不安全？](#)

[在服务器上部署 SSL 证书后访问资源出现 404 报错](#)

## HTTP 自动跳转 HTTPS 的安全配置（可选）

### 说明：

正常跳转可按照下列编辑规则。若您有其他需求可以自己设置。

HTTP 跳转 HTTPS 过程中，如果您的网站元素中存在外部链接或者使用的 HTTP 协议，导致整个页面不完全是 HTTPS 协议。部分浏览器会因为这些因素报不安全的提示，例如链接不安全。您可以单击不安全页面中的“详细信息”查看报错原因。

1. 打开 IIS 服务管理器。
2. 选择网站下的站点名称，双击打开 **URL 重写**。

### 注意：

执行该步骤前请下载安装 [rewrite 模块](#)。

3. 进入 **URL 重写** 页面，并单击右侧**操作**栏的**添加规则**。
4. 在弹出的**添加规则**窗口中，选择**空白规则**，单击**确定**。
5. 进入**编辑入站规则**页面。

名称：填写强制 HTTPS。

匹配URL：在**模式**中手动输入 `(.*)`。

条件：展开



单击**添加**，弹出**添加条件**窗口。

条件输入：`{HTTPS}`。

检查输入字符串是否：默认选择与模式匹配。

模式：手动输入 `^OFF$`。

操作：填写以下参数。

操作类型：选择**重定向**。

重定向 URL：`https://{HTTP_HOST}/{R:1}`。

重定向类型：选择**参阅其他（303）**。

6. 单击**操作**栏的**应用保存**。

7. 返回网站首页，单击右侧**管理网站**栏的**重新启动**。即可使用 `http://cloud.tencent.com` 进行访问。



**注意：**

操作过程如果出现问题，请您 [联系我们](#)。

# Weblogic 服务器 SSL 证书安装部署

最近更新时间：2024-03-06 17:38:42

## 操作场景

本文档指导您如何在 Weblogic 中安装 SSL 证书。

### 说明：

本文档以证书名称 `cloud.tencent.com` 为例，实际名称请以您申请的证书为准。

Weblogic 版本以 Weblogic/14.1.1 为例。

本文档以操作系统 Windows Server 2012 R2 为例。由于操作系统的版本不同，详细操作步骤略有区别。

安装 SSL 证书前，请您在 Weblogic 服务器上开启“443”端口，避免证书安装后无法启用 HTTPS。具体可参考 [服务器如何开启443端口？](#)

SSL 证书文件上传至服务器方法可参考 [如何将本地文件拷贝到云服务器。](#)

## 操作步骤

### 说明：

下述步骤中的目录皆是测试环境的目录，具体路径请根据您的实际环境与需求进行确定。

1. 已在 [SSL 证书管理控制台](#) 中下载并解压缩 `cloud.tencent.com` 证书文件包到本地目录。

解压缩后，可获得相关类型的证书文件。其中包含 Tomcat 文件夹和 CSR 文件：

文件夹名称：Tomcat

文件夹内容：

`cloud.tencent.com.jks` 证书文件

`keystorePass.txt` 密码文件（若已设置私钥密码，则无 `keystorePass.txt` 密码文件）

CSR 文件内容：`cloud.tencent.com.csr` 文件

### 说明：

CSR 文件是申请证书时由您上传或系统在线生成的，提供给 CA 机构。安装时可忽略该文件。

当您申请 SSL 证书时选择了“粘贴 CSR”方式，或者购买的品牌证书为 Wotrus，则不提供 Tomcat 证书文件的下载，需要您通过手动转换格式的方式生成密钥库。操作方法如下：访问 [转换工具](#)。

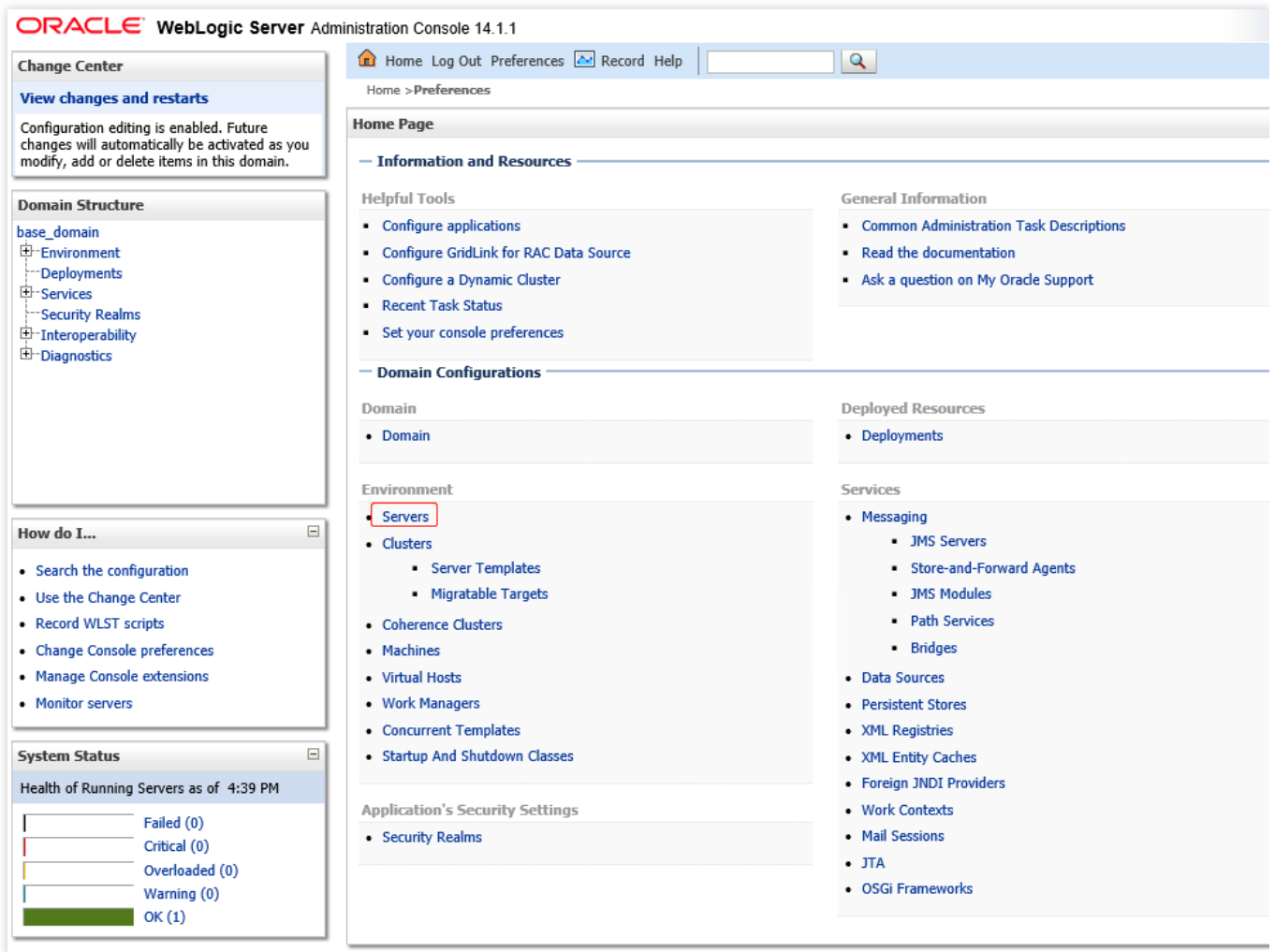
未提供 Tomcat 证书文件的情况下，您可以将 Nginx 文件夹中的证书文件和私钥文件上传至“转换工具”中，并填写密钥库密码，单击【提交】，即可转换为 jks 格式证书。

2. 请登录服务器，请在 C 盘中创建新的文件夹，以 `temp` 为例。

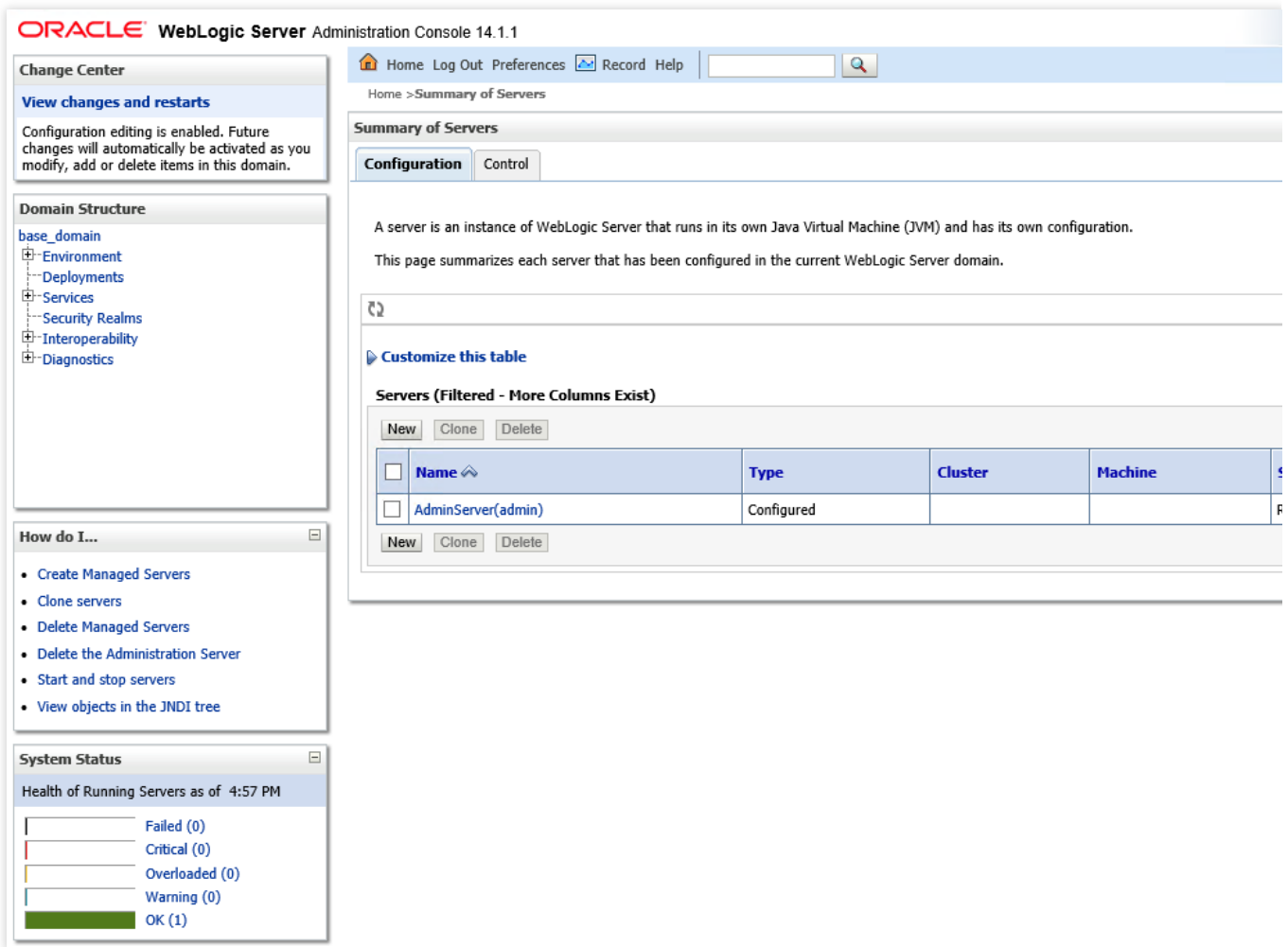
3. 将本地解压缩后的证书文件与密码文件上传至 `temp` 文件夹中。

4. 请登录 Weblogic 服务管理后台（默认地址：`http://localhost:7001/console`），输入您的用户名及密码，即可进入 WebLogic Server 管理控制台。

5. 单击域配置 > 服务器。进入服务器概要管理页面。如下图所示：



6. 选择您要配置的服务器名称，以 AdminiServer 为例。如下图所示：



**ORACLE WebLogic Server Administration Console 14.1.1**

Home > Summary of Servers

**Summary of Servers**

**Configuration** Control

A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration. This page summarizes each server that has been configured in the current WebLogic Server domain.

**Customize this table**

**Servers (Filtered - More Columns Exist)**

New Clone Delete

<input type="checkbox"/>	Name	Type	Cluster	Machine
<input type="checkbox"/>	AdminServer(admin)	Configured		

New Clone Delete

**Change Center**

**View changes and restarts**

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

**Domain Structure**

- base\_domain
  - Environment
  - Deployments
  - Services
  - Security Realms
  - Interoperability
  - Diagnostics

**How do I...**

- Create Managed Servers
- Clone servers
- Delete Managed Servers
- Delete the Administration Server
- Start and stop servers
- View objects in the JNDI tree

**System Status**

Health of Running Servers as of 4:57 PM

- Failed (0)
- Critical (0)
- Overloaded (0)
- Warning (0)
- OK (1)

7. 进入 `AdminServer` 的管理设置页面，勾选**启用 SSL 监听端口**并填写 SSL 监听端口为 `443`，单击**保存**。如下图所示：

ORACLE WebLogic Server Administration Console 14.1.1

Home Log Out Preferences Record Help

Home > Summary of Servers > AdminServer

**Settings for AdminServer**

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores SSL Federation Services Deployment Migration Tuning Overload Concurrency

Save

Use this page to configure general features of this server such as default network communications.

[View JNDI Tree](#)

**Name:** AdminServer

**Template:** (No value specified) [Change](#)

**Machine:** (None)

**Cluster:** (Stand-Alone)

**Listen Address:** [ ]

**Listen Port Enabled**

**Listen Port:** 7001

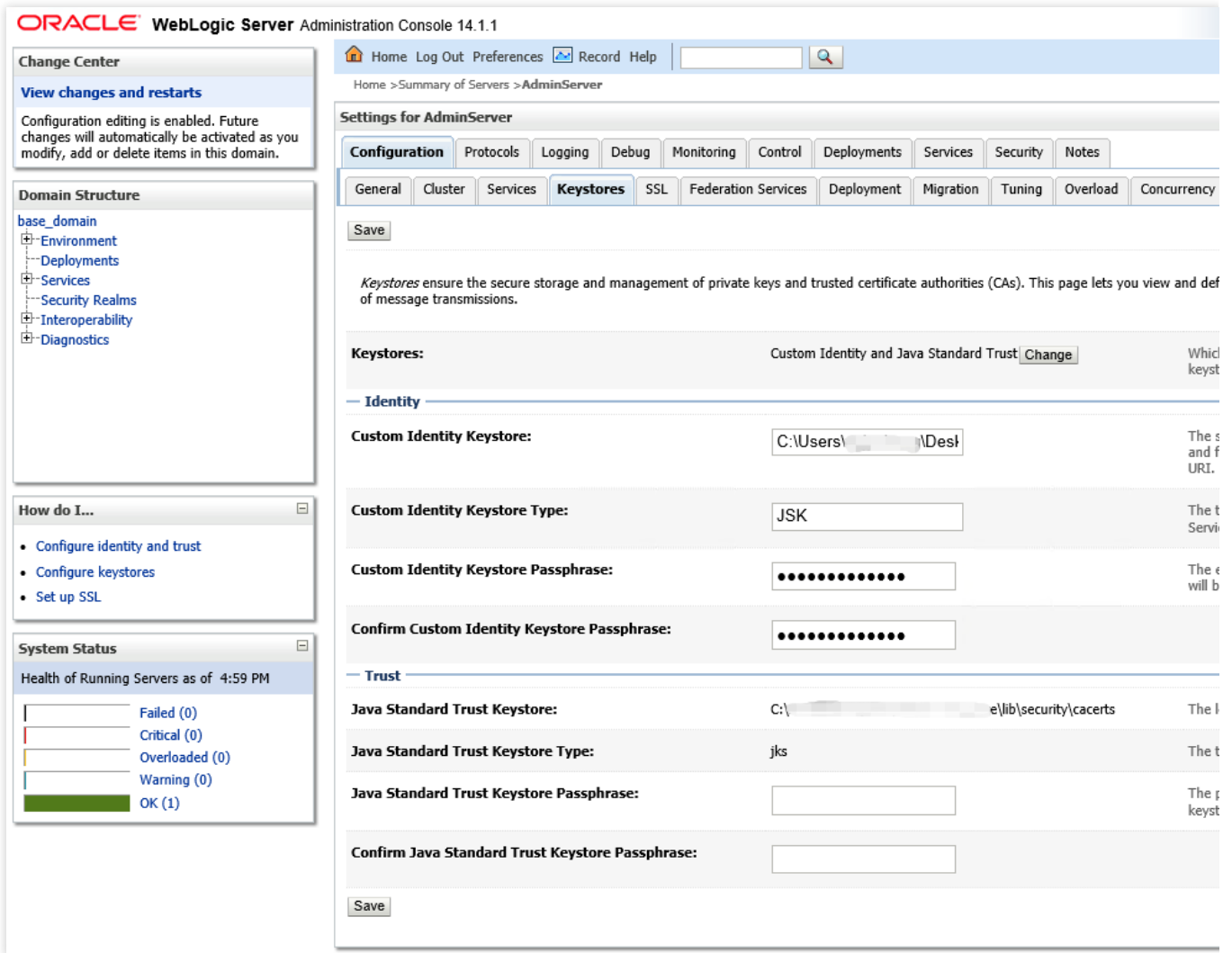
**SSL Listen Port Enabled**

**SSL Listen Port:** 443

**Client Cert Proxy Enabled**

**Java Compiler:** javac

8. 在 AdminServer 的管理设置页面，单击**密钥库**，设置完成后并单击**保存**。如下图所示：



设置如下信息：

**密钥库：**选择“定制身份和 JAVA 标准信任”。

**定制身份密钥库：**请填写您的 JKS 证书文件路径，例如：`C:\temp\cloud.tencent.com.jks`。

**定制身份密钥库类型：**请填写 JKS。

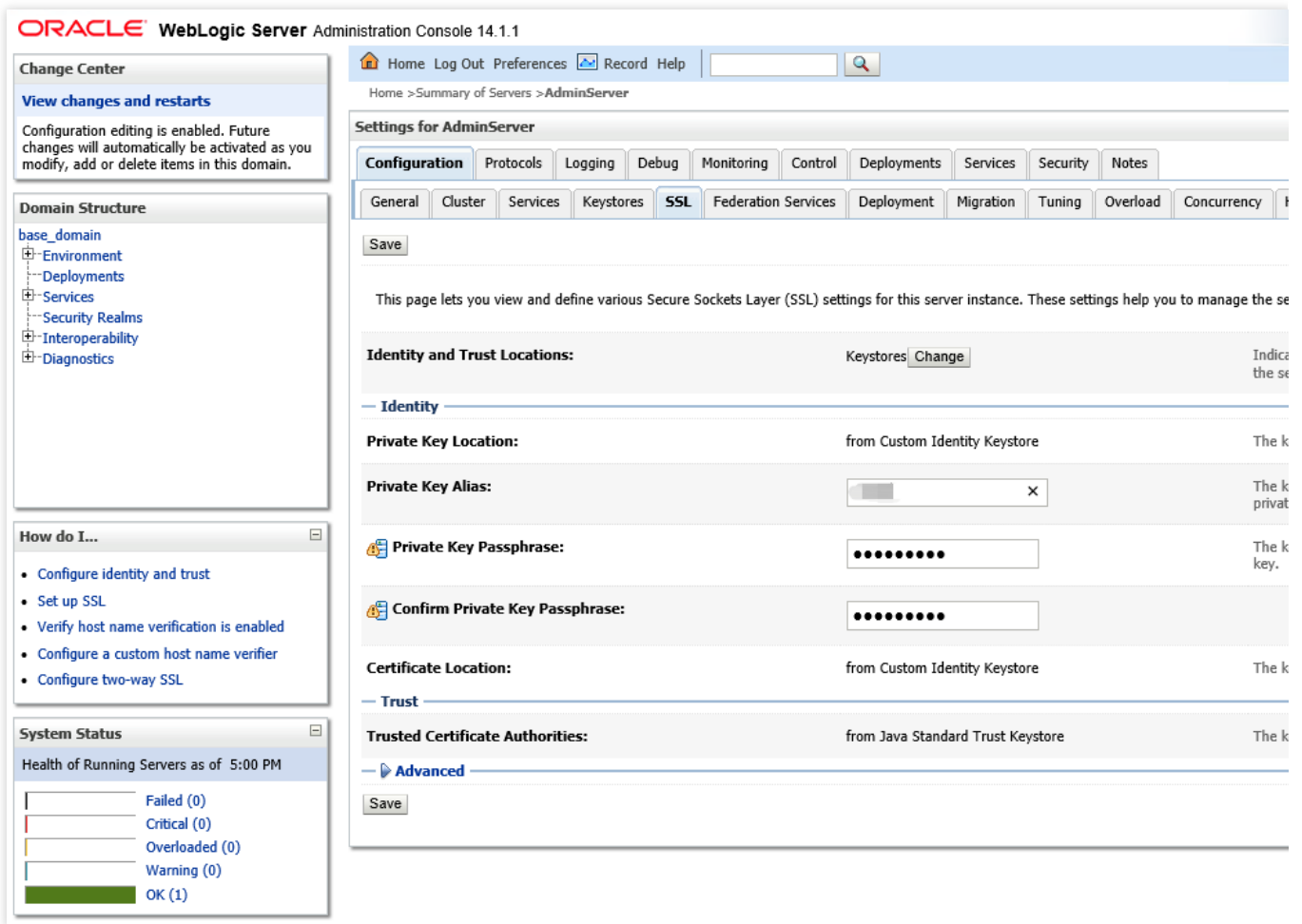
**定制身份密钥库密码短语：**请输入您的 JKS 密码。

**确认定制身份密钥库密码短语：**请再次输入您的密码。

**说明：**

**定制身份密钥库密码短语**与**确认定制身份密钥库密码短语**默认密码为空。此处密码可以和自己的 JKS 密码一致，也可以不做任何改动，此处设置不影响证书正常使用。

9. 在 `AdminiServer` 的管理设置页面，单击 **SSL**，设置完成后并单击**保存**。如下图所示：



设置如下信息：

**身份和信任位置：**请更改为**密钥库**。

**私有密钥别名：**请填写 JKS 的别名。

**私有密钥密码短语：**请输入您申请时设置的私有密码，如未设置可不填写。

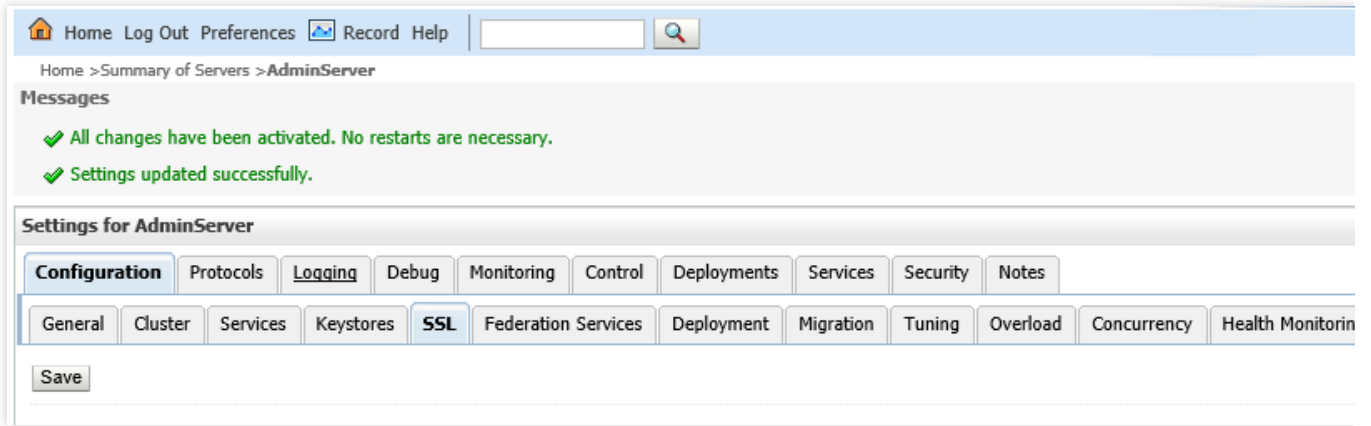
**确认私有密钥密码短语：**请再次输入私有密码。

**说明：**

如果您的 Weblogic 版本在 10.3.6-12C 之间，请在 **SSL** 设置页面，高级选项中勾选 JSSE。

Weblogic 版本在10.3.6 以下不支持 SHA2 算法证书，请升级后再试。

10. 修改内容后，单击**保存**，即可自动激活，不需要进行重启。如下图所示：



11. 请使用 `https://cloud.tencent.com` 进行访问。



# 如何选择 SSL 证书安装部署类型？

最近更新时间：2024-03-06 17:38:42

## 手动安装证书

证书安装目前有下列15种方式，您可以根据您购买的证书加密标准类型和搭建的服务器类型进行证书安装。

### 说明：

使用一键 HTTPS 功能，您无需进行繁琐的 SSL 证书部署操作，即可帮助您实现从 HTTP 到 HTTPS 的能力升级。

目前仅提供以下15种安装证书的方式。

证书类型	服务器系统	证书安装方式
国际标准证书 (RSA/ECC)	Linux 系统	<a href="#">Apache 服务器证书安装</a>
		<a href="#">Nginx 服务器证书安装</a>
		<a href="#">Tomcat 服务器 SSL 证书安装部署 (JKS 格式)</a>
		<a href="#">Tomcat 服务器 SSL 证书安装部署 (PFX 格式)</a>
		<a href="#">GlassFish 服务器证书安装</a>
		<a href="#">JBoss 服务器证书安装</a>
		<a href="#">Jetty 服务器证书安装</a>
	Windows 系统	<a href="#">IIS 服务器证书安装</a>
		<a href="#">Weblogic 服务器证书安装</a>
		<a href="#">Apache 服务器 SSL 证书安装部署 (Windows)</a>
		<a href="#">Tomcat 服务器 SSL 证书安装部署 (JKS 格式) (Windows)</a>