

SSL 证书 证书安装



腾讯云

【版权声明】

©2013–2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【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。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。

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。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

证书安装

SSL 证书安装部署至云服务

- SSL 证书如何自动部署到腾讯云云资源
- 安装部署 SSL 证书到对象存储（COS）指引
- 安装部署 SSL 证书到负载均衡（CLB）指引
- 安装部署 SSL 证书到内容分发网络（CDN）指引
- 安装部署 SSL 证书到 Web 应用防火墙（WAF）指引
- 安装部署 SSL 证书到 DDoS 防护指引
- 安装部署 SSL 证书到云直播（CSS）指引
- 安装部署 SSL 证书到容器服务（Ingress）指引
- 安装部署 SSL 证书到轻量应用服务器（Lighthouse）指引
- 安装部署 SSL 证书到 API 网关指引

如何选择 SSL 证书安装部署类型？

国际标准 SSL 证书安装

- 腾讯云宝塔面板 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）
- Nginx 服务器 SSL 证书安装部署（Linux）
- Nginx 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
- Spring Boot 安装 SSL 证书
- IIS 服务器 SSL 证书安装部署
- WebLogic 服务器 SSL 证书安装部署
- Node.js 环境 SSL 证书安装部署
- SSL 根证书下载

国密标准（SM2）SSL 证书安装

Wotrus

- Apache 服务器国密 SSL 证书（Wotrus）安装部署
- Nginx For Linux 国密 SSL 证书（Wotrus）安装部署
- Nginx For Windows 国密 SSL 证书（Wotrus）安装部署

DNSPod

- Nginx For Linux 国密 SSL 证书安装（DNSPod）
- Apache 服务器国密 SSL 证书安装部署（DNSPod）

一键 HTTPS

常见问题

证书安装

SSL 证书安装部署至云服务

SSL 证书如何自动部署到腾讯云云资源

最近更新时间：2024-02-05 17:17:11

自动部署证书

如果您需要将证书部署在腾讯云的云资源上，如（CDN、负载均衡(CLB)、轻量应用服务器、对象存储（COS）、Web 应用防火墙等）可使用 SSL 证书控制台提供的自动部署功能，将证书自动部署到云资源。

云资源类型	是否支持自动部署	自动部署指南
负载均衡（CLB）	支持	安装部署 SSL 证书到负载均衡（CLB）指引
内容分发网络（CDN）	支持	安装部署 SSL 证书到内容分发网络（CDN）指引
Web应用防火墙（WAF）	支持	安装部署 SSL 证书到 Web 应用防火墙（WAF）指引
对象存储（COS）	支持	安装部署 SSL 证书到对象存储（COS）指引
容器服务（Ingress）	支持	安装部署 SSL 证书到容器服务 Ingress
轻量应用服务器	支持	安装部署 SSL 证书到轻量应用服务器（LightHouse）
DDos 防护	支持	安装部署 SSL 证书到 DDoS 防护指引
云直播	支持	安装部署 SSL 证书到云直播（CSS）指引
云点播	支持	敬请期待
API 网关	支持	安装部署 SSL 证书到 API 网关指引
EdgeOne	支持	敬请期待
网站建设	开发中	手动部署指南： 网站建设 > SSL 证书部署

安装部署 SSL 证书到对象存储（COS）指引

最近更新时间：2024-11-27 17:28:52

操作场景

本文档指导您将 SSL 证书部署到腾讯云对象存储（COS）。

前提条件

已成功申请并获取证书。

操作步骤

⚠ 注意：

操作之前，请确认您的 [COS 控制台](#) 是否有实例，若没有实例，请您先创建实例。

1. 登录 [SSL 证书控制台](#) > [我的证书](#)，选择您需要部署的证书，并单击部署。
2. 在弹出的窗口，根据页面提示，勾选跟证书域名匹配的 COS 实例，单击确定。

证书ID4b

证书类型DNSPod RSA DV

支持域名*.huixi.m

部署类型

☐ 负载均衡☐ 内容分发网络☐ 云直播☐ Web应用防火墙☐ DDoS防护☐ API 网关☐ EdgeOne☒ 容器服务☒ COS☐ 轻量应用服务器☐ 云点播☐ 服务器

资源实例

华东地区（南京）

选择域名

可输入域名进行搜索

☐ 域名

存储桶名称

状态

暂无匹配的域名，请前往[COS控制台](#)添加资源

已选择 (0)

域名	存储桶名称	状态
----	-------	----

确定

体验吐槽 & 遇到问题？[加入SSL证书交流群](#)

3. 在[任务部署](#)页面，等待部署完成即可。

证书部署到云资源后，还需等待云资源生效（不同云资源生效时间不同，CDN通常为5~10分钟），请您耐心等待。

刷新状态

一键重试

一键回退

域名	部署前绑定的证书	最后一次更新时间	资源部署状态	操作
tes		2023-04-24 17:13:49	等待部署	刷新部署状态

共 1 条

10 ▼ 条 / 页

1 / 1 页

注意：

若部署错误，您可通过**一键回退**功能将云资源回退到这次部署前的证书。

版权所有：腾讯云计算（北京）有限责任公司

第6 共115页

安装部署 SSL 证书到负载均衡（CLB）指引

最近更新时间：2024-08-16 21:21:42

操作场景

本文档指导您将 SSL 证书部署到负载均衡。

前提条件

已登录 [证书管理控制台](#)，且成功申请获取证书。

操作步骤

⚠ 注意

操作之前，请确认您的 [负载均衡控制台](#) 是否有实例，若没有实例，请您先创建实例。

1. 登录 [SSL 证书控制台](#) > [证书列表](#)，选择您需要部署的证书，并单击部署。

1. 【子账号用户必看】关于腾讯云SSL所有接口新增鉴权的通知 [查看详情](#)

2. 自2023年3月21日起，个人账号可申请50张免费证书，其中30张需使用腾讯云域名申请；企业可申请10张免费证书，均需使用腾讯云域名申请。 [查看详情](#)

申请中
2
待提交 1
待验证 1

已签发
24
即将过期 2

已过期
3

账号免费证书配额 ①

购买证书 批量操作

证书状态: 已签发 标签多个关键字用竖线"|"分隔，其它只能输入单个关键字

☐ 证书信息	绑定域名	到期时间 ①	域名解析 ①	关联资源 ①	自动续费	状态 ①	操作
☐ ID: 未命名 有效期: 共 1 年, 当前第 1 年	未命名	2024-04-21 07:59:59	未命名	未命名	☐	已签发	部署 下载 升级 更多
☐ ID: 上传证书 有效期: 共 1 年, 当前第 1 年 来源: 上传托管	上传证书	2024-04-12 07:59:59	--	未命名 1	☐	已签发	部署 下载 更多
☐ ID: 未命名 有效期: 共 1 年, 当前第 1 年	未命名	2024-04-12 07:59:59	未命名	未命名 100	☐	已签发	部署 下载 更多

2. 在 [证书部署](#) 页面，选择 [负载均衡](#)，根据项目和地域选择 [负载均衡实例](#)。如下图所示：

⚠ 注意

目前不支持华南地区-深圳金融。

证书ID

证书类型

支持域名

部署类型

资源实例

☒ 负载均衡

☐ 内容分发网络

☐ 云直播

☐ Web应用防火墙

☐ DDoS防护

☐ API 网关

☐ EdgeOne

☐ 容器服务

☐ COS

☐ 轻量应用服务器

☐ 云点播

☐ 服务器

暂无任何实例，[前往CLB新建](#)

为防止您误操作，只展示与证书域名相关的实例，也不支持部署到传统型负载均衡实例。如您需要部署传统型实例或查看所有实例，[请前往负载均衡控制台](#)。

选择监听器资源

监听器名称/域名	类型	SNI ⓘ	状态 ▾	已绑定证书
请先至少选择一项 CLB 资源。				

已选择 (0/1000)

监听器名称/域名	类型	SNI ⓘ	状态	已绑定证书
----------	----	-------	----	-------

确定

体验吐槽 & 遇到问题? [加入SSL证书交流群](#)

ⓘ 说明

- 此步骤只会显示与您当前证书域名匹配的监听器，如果您的负载均衡（CLB）资源未创建监听器资源，请参见 [负载均衡监听器概述](#) 并选择您需要的类型进行配置监听器。
- 在部署证书前，请您务必确保已正确配置监听器资源，否则无法加载监听器资源。如您配置监听器后仍无法显示，可能是因为监听器配置有误，请您前往 [负载均衡控制台](#) 核对配置是否有误。

安装部署 SSL 证书到内容分发网络（CDN）指引

最近更新时间：2024-10-22 17:13:32

操作场景

本文档指导您将 SSL 证书部署到 CDN 内容分发网络。

前提条件

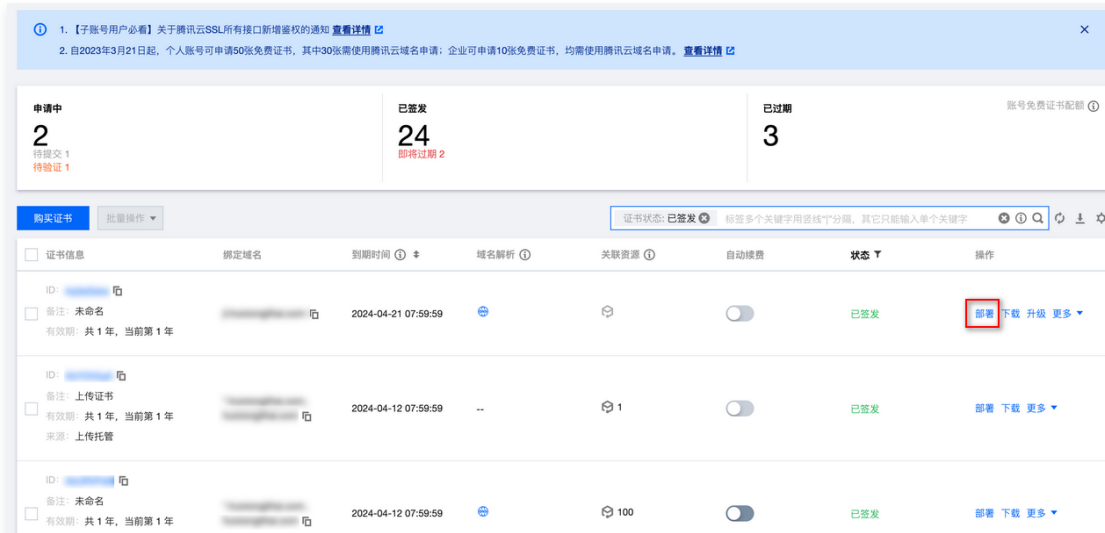
已在腾讯云申请 SSL 证书并成功颁发。

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。具体操作请参见 [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. 登录 [SSL 证书控制台](#) > [证书列表](#)，选择您需要部署的证书，并单击部署。



2. 在证书部署页面，选择内容分发网络，按需选择 CDN 资源。如下图所示：

证书ID

证书类型

支持域名

部署类型

资源实例

☐ 负载均衡
 ☒ 内容分发网络
 ☐ 云直播
 ☐ Web应用防火墙
 ☐ DDoS防护
 ☐ API 网关
 ☐ EdgeOne
 ☐ 容器服务
 ☐ COS
 ☐ 轻量应用服务器
 ☐ 云点播
 ☐ 服务器

☒ 隐藏未绑定SSL证书的域名

选择域名

可输入域名进行搜索

域名

已绑定证书

服务状态

暂无匹配的域名，请先前往[内容分发网络](#)控制台添加资源

共 0 条 10 条 / 页

已选择 (0)

域名

已绑定证书

服务状态

确定

体验吐槽 & 遇到问题? [加入SSL证书交流群](#)

3. 单击**确定**，等待部署即可，如下图所示：

证书部署到云资源后，还需等待云资源生效（不同云资源生效时间不同，CDN通常为5~10分钟），请您耐心等待。

刷新状态

一键重试

一键回退

域名	部署前绑定的证书	最后一次更新时间	资源部署状态	操作
test		2023-04-24 17:13:49	等待部署	刷新部署状态

共 1 条 10 条 / 页

如何在 CDN 开启 HTTPS

注意：

SSL证书部署完成以后，请务必前往 [CDN 控制台](#) 开启 **HTTPS 服务** 才可实现 **HTTPS**，详情请参见 [HTTPS 配置须知](#)。

安装部署 SSL 证书到 Web 应用防火墙（WAF）指引

最近更新时间：2024-12-26 16:26:11

操作场景

本文档指导您将 SSL 证书部署到 Web 应用防火墙（WAF）。

前提条件

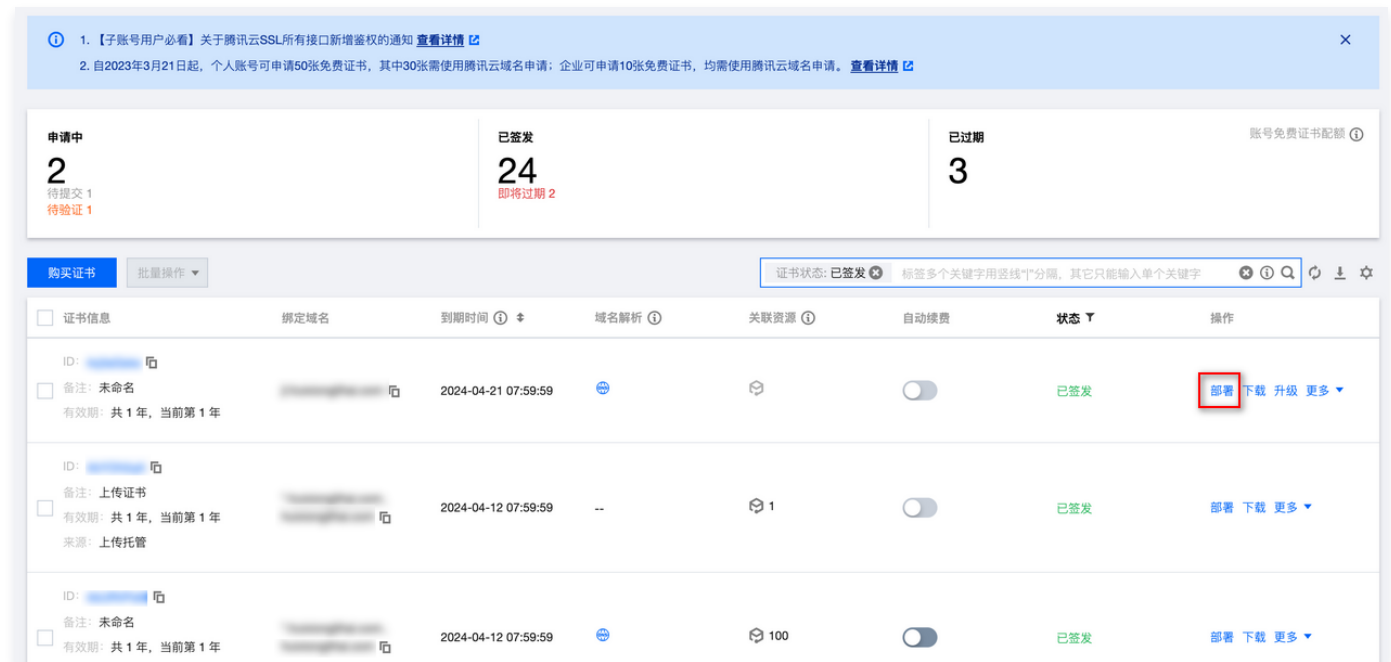
已在腾讯云申请 SSL 证书并成功颁发。

操作步骤

⚠ 注意：

操作之前，请确认您的 [Web 应用防火墙管理控制台](#) 是否有实例，若没有实例，请您先创建实例。

1. 登录 [SSL 证书控制台](#) > [证书列表](#)，选择您需要部署的证书，并单击部署。



2. 在证书部署页面，选择 **Web 应用防火墙**，按需选择对应的实例，如下图所示：

证书ID

4g3d3k0w

证书类型

TrustAsia TLS RSA CA

支持域名

37xwzmgfha.com

部署类型

☐ 负载均衡

☐ 内容分发网络

☐ 云直播

☒ Web应用防火墙

☐ DDoS防护

☐ API 网关

☐ EdgeOne

☐ 容器服务

☐ COS

☐ 轻量应用服务器

☐ 云点播

☐ 服务器

资源实例

中国大陆

选择域名

可输入域名进行搜索

☐ 域名

是否保持长连接

暂无匹配的域名，请先前往[Web应用防火墙](#)控制台添加资源

已选择 (0)

域名

是否保持长连接

↔

支持按住 shift 键进行多选

确定

体验吐槽 & 遇到问题? [加入SSL证书交流群](#)



注意

目前仅支持 SaaS 型 WAF 资源。

3. 单击**确定**，即可将SSL证书部署到 WAF 资源。



说明：

Web 应用防火墙相关设置与说明，您可以参考 [Web 应用防火墙相关文档](#)。

安装部署 SSL 证书到 DDoS 防护指引

最近更新时间：2024-12-05 15:11:02

概述

本文档指导您将 SSL 证书部署到 DDoS 防护。

前提条件

已登录 [SSL 证书控制台](#)，已成功申请并获取证书。

操作步骤

⚠ 注意

如果证书需部署至 DDoS 防护，请您先在 [DDoS 防护控制台](#) 接入域名，否则无法部署 SSL 证书，具体操作请参见 [域名接入](#)。

1. 单击已签发页签，选择您需要部署的证书，并单击证书 ID，进入证书详情页面，如下图所示：



2. 在证书详情页面，选择基本信息页签，在一键部署证书模块中，单击 DDoS 防护，如下图所示：

← lJZoZcQn 证书详情

有奖问卷, 产品体验您说了算 体验吐槽 & 遇到问题? 加入SSL证书交流群 帮助

基本信息 关联云资源 部署记录 更新记录 证书下载

证书ID 签名算法 RSA-SHA384 过期时间 2025-01-11 07:59:59 续期

状态 已签发 加密算法 RSA 服务年限 共 90 天

主域名 加密位数 2048 来源 腾讯云

所有域名 证书指纹 2AB5 C0280 备注 未命名

证书类型 TrustAsia C1 DV Free 购买时间 2024-10-12 标签

所属项目 默认项目 签发时间 2024-10-12

证书链信息

证书链一般由网站证书 > CA 中间证书机构 > CA 根证书机构构成, 中间证书还可能存在多层关系。 [查看介绍](#)

颁发给 TrustAsia RSA DV TLS CA G2

颁发者 AAA Certificate Services

颁发给 AAA Certificate Services

颁发者 AAA Certificate Services

证书托管功能

如果您的网站部署在云产品, 可以使用[证书托管功能](#)

一键部署证书

如果您的网站部署在以下云产品, 选择云产品一键部署证书。

负载均衡CLB

内容分发网络CDN

云直播LIVE

Web应用防火墙WAF

DDoS防护

API 网关

云原生API网关TSE

边缘安全加速平台EO

容器服务TKE

对象存储COS

轻量应用服务器

云点播VOD

云开发TCB

手动部署

证书安装遇到问题? 加入交流群咨询

如果您的网站部署在其他类型的云产品或者服务器资源上, 请手动部署证书: [下载证书](#) 后参照文档部署SSL证书。

不会部署证书? 使用[一键HTTPS](#) 帮您部署 [去部署](#)

部署文档

Linux

宝玑面板

Apache 服务器

Tomcat 服务器 (PFX 格式)

Tomcat 服务器 (JKS 格式)

Nginx 服务器

GlassFish 服务器

JBoss 服务器

Jetty 服务器

Windows

IIS 服务器

Weblogic 服务器

Apache 服务器

Tomcat 服务器

3. 在弹出的部署证书窗口中, 选择 **DDoS 防护**, 并勾选需要部署的 DDoS 资源, 如下图所示:

证书ID

证书类型 TrustAsia C1 DV Free

支持域名 st.cc, t.cc

部署类型 ☐ 内容分发网络CDN ☐ 负载均衡CLB ☐ 云直播LIVE ☐ Web应用防火墙WAF ☒ DDoS防护 ☐ API 网关 ☐ 边缘安全加速平台EO ☐ 容器服务TKE ☐ 对象存储COS ☐ 轻量应用服务器 ☐ 云点播VOD ☐ 云开发TCB ☐ 云原生API网关TSE ☐ 服务器SERVER

资源实例

选择域名

可输入域名进行搜索

域名

高防资源

协议

已绑定证书

已选择

域名

高防资源

协议

已绑定证书

确定

体验吐槽 & 遇到问题? 加入SSL证书交流群

4. 单击**确定**，等待配置成功后，您可以前往 [DDoS 防护控制台](#) 查看详情，如下图所示：



安装部署 SSL 证书到云直播（CSS）指引

最近更新时间：2024-03-07 16:36:01

概述

本文档指导您将 SSL 证书部署到云直播。

前提条件

已登录 [SSL 证书控制台](#)，并成功申请获取证书（参考 [如何免费申请域名型证书](#)）。

操作步骤

⚠ 注意

如证书需部署至云直播，请先在 [云直播控制台](#) 接入域名，否则无法部署 SSL 证书。具体操作请参考 [添加自有域名](#)。

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。如下图所示：

申请状态			
待提交 0	验证中 0	已签发 18	审核失败 7
Z[redacted]o	TrustAsia TLS RSA CA	vc[redacted].club	证书详情
Z[redacted]c	TrustAsia TLS RSA CA	qc[redacted]ow.com	证书详情
d[redacted]7	TrustAsia TLS RSA CA	wv[redacted]ow.com	证书详情
e[redacted]jH	TrustAsia TLS RSA CA	we[redacted].club	证书详情
el[redacted]90	TrustAsia TLS RSA CA	w[redacted]ow.com	证书详情
共 18 条			
⏪ ⏴ 1 / 4 页 ⏵ ⏩			

2. 进入“证书详情”管理页面，在“快速上手”模块单击**一键部署**。如下图所示：

快速上手

1

申请证书

当前证书已于 2021-03-25 08:00:00 签发成功。

2

使用证书

您可以下载证书进行安装，[查看安装说明](#) 或**一键部署**到其他云产品。

[下载证书](#) **一键部署**

3

证书过期

证书到期前，需要及时续费更新，避免影响您的业务正常运行 [查看续费流程](#)

3. 在弹出的“选择部署类型”窗口中，选择云直播，并勾选需要部署到云直播的域名。如下图所示：

选择部署类型

证书ID

jj

证书类型

TrustAsia TLS RSA CA

部署类型

☐ 负载均衡

☐ 内容分发网络

☒ 云直播

☐ Web应用防火墙

☐ DDoS防护

☐ 服务器

资源实例

选择云直播资源

可输入域名进行搜索

☐ 域名

HTTPS配置

☐ .cn

开启

已选择 (0)

同时开启HTTPS配置 ☒

域名

HTTPS配置

支持按住 shift 键进行多选

确定

取消

4. 单击确定，等待配置成功后，您可以前往 [云直播控制台](#) 查看详情。如下图所示：

部署成功

SSL证书关联云直播资源成功，是否前往云直播？

立即前往

取消

安装部署 SSL 证书到容器服务（Ingress）指引

最近更新时间：2024-12-03 11:38:42

操作场景

本文档将指导您如何在腾讯云容器服务 Ingress 中安装部署 SSL 证书，使部署在腾讯云容器服务的应用服务能够通过 HTTPS 方式访问您的业务域名。

说明：

若您需要类 Kubernetes（K8S）Ingress 上安装部署 SSL 证书，您可参考本文档进行操作，因标准与使用场景不同，详细操作步骤略有区别。

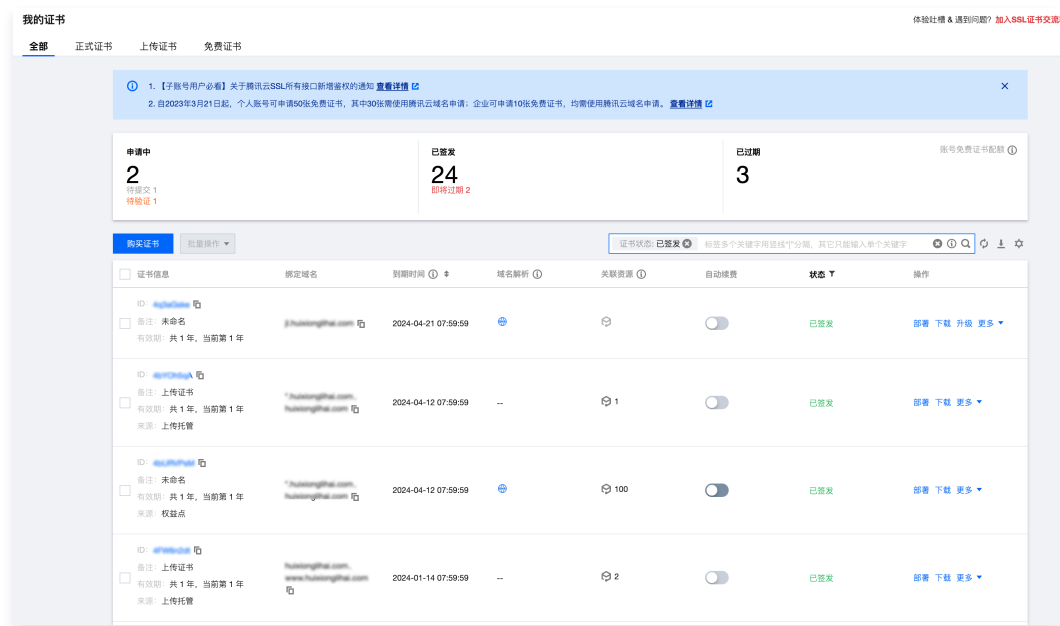
前提条件

- 已在腾讯云申请 SSL 证书并成功颁发。
- 已在腾讯云容器服务上配置了域名。

操作步骤

方式一：在 SSL 证书控制台部署到容器服务

1. 登录 SSL 证书控制台 > [我的证书](#) 页面，选择您需要部署的证书，并单击部署。



2. 进入证书部署页面，选择容器服务，根据选择对应的实例。如下图所示。

证书ID: myssl123456

证书类型: TrustAsia TLS Web CA

支持域名: mycompany.com

部署类型:

☐ 负载均衡

☐ 内容分发网络

☐ 云直播

☐ Web应用防火墙

☐ DDoS防护

☐ API 网关

☐ EdgeOne

☒ 容器服务

☐ COS

☐ 轻量应用服务器

☐ 云点播

☐ 服务器

资源实例:

华东地区（上海）

选择容器资源

隐藏已绑定资源

已选择 0/1000

一键清空

搜索实例集群/NS/实例

暂无数据

集群	命名空间	Secret	已绑定证书	状态	操作
----	------	--------	-------	----	----

确定

体验吐槽 & 遇到问题? 加入SSL证书交流群

3. 单击**确定**，等待部署即可，如下图所示：

证书部署到云资源后，还需等待云资源生效（不同云资源生效时间不同，CDN通常为5~10分钟），请您耐心等待。

刷新状态

一键重试

一键回退

域名	部署前绑定的证书	最后一次更新时间	资源部署状态	操作
test		2023-04-24 17:13:49	等待部署	刷新部署状态

共 1 条

10 / 页

1 / 1 页

方式二：在容器控制台配置 HTTPS 服务

1. 登录腾讯云 容器服务控制台。
2. 选择您需要部署的集群，单击 ID/名称，进入该集群基本信息页面，如下图所示：

集群 地域: 广州 1 其他地域(0)

云原生产品 优惠专区 新版体验反馈 返回旧版 扫码关注公众号 产品文档

TKE集群上线策略管理新特性，通过前置策略拦截误删行为，避免误删引起业务故障。详细介绍请参考策略管理

根据腾讯云容器服务 TKE 的版本支持机制，Kubernetes 1.26版本计划于2024年11月30日进入EOM阶段，您将无法创建EOM的 Kubernetes 集群，请您尽快升级您的集群版本，关于如何升级集群，请参见升级集群

新建

多个过滤标签用回车键分隔

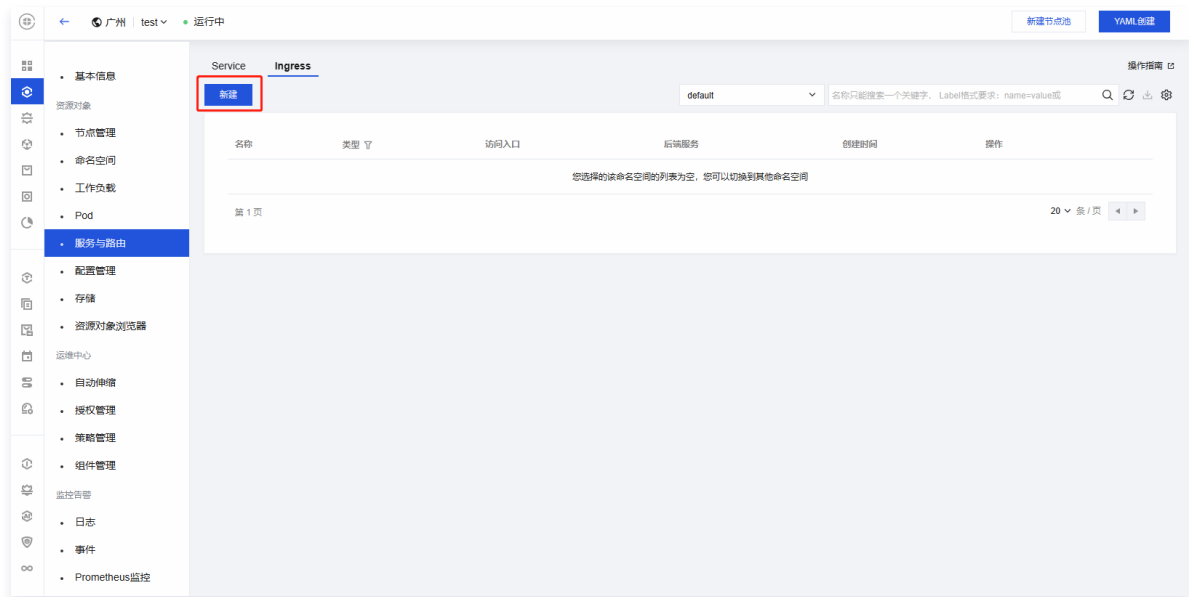
名称/ID	监控	状态	集群类型	kubernetes...	节点数	创建时间	资源量	腾讯云标签	操作
test		运行中	标准集群	1.30.0	2台 (全部正常)	2024-10-08 15:47:44	CPU: 2.44/3.86核 内存: 2.05/2.12GB	-	新建节点 查看集群凭证 更多

共 1 条

20 / 页

1 / 1 页

3. 在左侧菜单栏选择服务与路由 > Ingress，进入 Ingress 页面，单击新建，如下图所示：



4. 在新建服务与路由页面，输入您的相关配置信息，如下图所示：

Ingress名称

最长63个字符，只能包含小写字母、数字及分隔符("-")，且必须以小写字母开头，数字或小写字母结尾

描述

命名空间

default

Ingress类型

应用型 CLB

Others

详细对比

应用型负载均衡器（支持HTTP/HTTPS）

负载均衡相关配置

网络模式

☐ 采用负载均衡直连Pod模式

负载均衡直连Pod模式，将不再进行NodePort转发，支持会话保持和健康检查，[查看详情](#)

网络类型

公网

内网

负载均衡器

自动创建

使用已有

自动创建CLB用于公网/内网访问Service，CLB的生命周期由TKE管理。请勿手动修改由TKE创建的CLB监听器，[查看更多](#)

IP版本

IPv4

IPv6 NAT64

IP版本在后续更新过程中不支持变更

运营商类型

BGP

网络计费模式

按带宽计费

按使用流量

共享带宽包

带宽上限

1Mbps

512Mbps

1024Mbps

2048Mbps

-

10

+

Mbps

实例规格

共享型

共享型实例中多个实例共享资源，单实例最大支持并发连接数5万、每秒新建连接数5000、每秒查询数（QPS）5000。

转发规则相关配置

重定向

无

手动

自动

转发配置

协议

监听端口

域名

路径

后端服务

服务端口

HTTPS

443

dnstest.cq

eg: /

暂无数据

暂无数据

×

添加转发规则

创建Ingress

取消

CLB费用 0.2 元/小时

带宽费用 0.8 元/GB

版权所有：腾讯云计算（北京）有限责任公司

第20 共115页

- **Ingress 名称**：可自定义。最长63个字符，只能包含小写字母、数字及分隔符("-")，且必须以小写字母开头，数字或小写字母结尾。
- **描述**：可自定义。请输入描述信息，不超过1000个字符。
- **命名空间**：默认 **default**。
- **Ingress 类型**：无需填写，系统自动展示。
- **网络模式**：负载均衡直连 Pod 模式，将不再进行 NodePort 转发，支持会话保持和健康检查。
- **网络类型**：若您通过外网访问您的业务应用，请选择**公网**。
- **负载均衡器**：若您已有应用 CLB 型负载均衡器请选择您的使用已有并勾选负载均衡器（CLB）。若无，请勾选**自动创建**。
- **IP 版本**：请根据您的容器实例进行选择，一般情况请选择 **IPv4**。
- **运营商类型**：**BGP**。
- **网络计费模式**：根据业务情况进行选择。
- **带宽上限**：请根据业务需求进行设置。
- **实例规格**：根据业务情况选择**共享型**或**性能容量型**。
 - 共享型：共享型实例中多个实例共享资源，单实例最大支持并发连接数5万、每秒新建连接数5000、每秒查询数（QPS）5000。
 - 性能容量型：提供性能保障，转发性能不受其它实例的影响，单实例最大可支持最大并发连接数10,000,000，新建连接数1,000,000，每秒查询数300,000。
- **重定向**：
 - 无：不开启重定向。
 - 手动：支持将一个转发配置重定向到另一个转发配置。注意：假设每条转发配置用英文字母 A、B、C 表示，A不能转发到 A；A 转发到 B 后，不支持 B 继续转发。支持 A 转发 B，C 转发到 B。
 - 自动：支持自动创建 HTTPS 的重定向配置。下列所有 HTTPS 协议的域名路径都会生成一个 HTTP 协议的域名路径，自动生成的 HTTP 协议的域名路径会重定向到对应的 HTTPS 协议的。
- **转发配置**：
 - 协议：请选择 **HTTPS**。
 - 监听端口：默认**443**
 - 域名：并输入您的业务域名。
 - 路径：请根据业务情况进行选择，默认情况下输入 / 即可。
 - 后端服务：请选择业务服务名称。
 - 服务端口：请选择业务端口。
- **TLS 配置**：

- **默认证书**：对于没有精确域名与泛域名绑定的，将以选定证书作为默认证书，更多请参见 [容器服务](#)。
- **域名**：请输入您的业务域名。
- **Secret**：Secret 请选择包含服务器证书信息的 Secret。若无，您可单击**新建密钥**，设置您的 Secret 信息，如下图所示：

新建密钥

×

名称

dnspod

-m .wC

最长63个字符，只能包含小写字母、数字及分隔符("-")，且必须以小写字母开头，数字或小写字母结尾

命名空间

default

服务器证书

未命名 (m .c)

↺

如您现有的证书不合适，请[新建服务器证书](#)

创建Secret

取消

5. 单击**创建 Ingress** 即可完成设置，即可在浏览器中使用 HTTPS 访问您的业务域名。

证书ID

证书类型

支持域名

部署类型

资源实例

TrustAsia TLS RSA CA

内容分发网络

负载均衡

云直播

Web应用防火墙

DDoS防护

API 网关

EdgeOne

容器服务

COS

轻量应用服务器

云点播

云开发

服务器

① 是否支持自动部署证书，取决于实例安装的镜像，当前仅支持自动部署到安装了以下镜像的轻量应用服务器实例：WordPress、WooCommerce、SRS音视频服务器、互动直播房间服务、Typecho、Cloudfre、Matomo、LAMP、Theia IDE、Cloud Studio、OpenFaaS；其它镜像请下载证书进行手动部署。

华东地区（上海）

选择域名

已选择 (0)

可输入域名进行搜索

实例名称

IP

域名

加载中...

实例名称

IP

域名

确定

体验吐槽 & 遇到问题? 加入SSL证书交流群

3. 单击确定。进入任务部署页面，等待部署完成即可。

证书部署到云资源后，还需等待云资源生效（不同云资源生效时间不同，CDN通常为5~10分钟），请您耐心等待。

刷新状态

一键重试

一键回退

域名	部署前绑定的证书	最后一次更新时间	资源部署状态	操作
tes		2023-04-24 17:13:49	等待部署	刷新部署状态

共 1 条

10 条 / 页

1 / 1 页

注意：

若部署错误，您可通过一键回退功能将云资源回退到这次部署前的证书。

安装部署 SSL 证书到 API 网关指引

最近更新时间：2024-10-22 17:13:32

操作场景

本文档指导您将 SSL 证书部署到腾讯云 API 网关。

前提条件

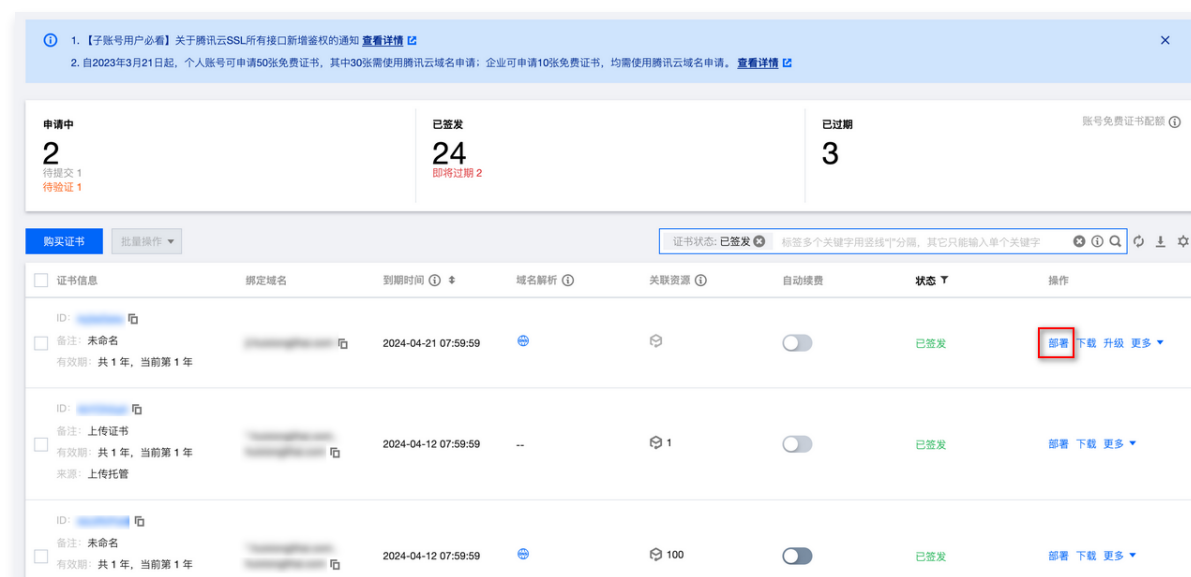
已在腾讯云申请 SSL 证书并成功颁发。

操作步骤

⚠ 注意：

操作之前，请确认您的 [API 网关控制台](#) 是否有实例，若没有实例，请您先创建实例。

1. 登录 [SSL 证书控制台](#) > [证书列表](#)，选择您需要部署的证书，并单击部署，如下图所示：



2. 在[证书部署](#)页面，根据页面提示，勾选跟证书域名匹配的 API 网关实例，单击[确定](#)。进入[任务部署](#)页面，等待部署完成即可。



 注意:

若部署错误，您可通过[一键回退](#)功能将云资源回退到这次部署前的证书。

如何选择 SSL 证书安装部署类型？

最近更新时间：2024-10-29 14:32:22

手动安装证书

证书安装目前有下列18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。详情请参考 [一键 HTTPS](#)。
- 目前仅提供以下18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	宝塔面板 SSL 证书安装
		Apache 服务器证书安装（Linux）
		Nginx 服务器证书安装（Linux）
		Tomcat 服务器 SSL 证书安装部署（JKS 格式）
		Tomcat 服务器 SSL 证书安装部署（PFX 格式）
		GlassFish 服务器证书安装
		JBoss 服务器证书安装
		Jetty 服务器证书安装
		Spring Boot 证书安装
		Node.js 环境 SSL 证书安装部署
	Windows 系统	IIS 服务器证书安装
		Nginx 服务器 SSL 证书安装部署（Windows）
		Weblogic 服务器证书安装
		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）（Windows）
国密标准证书（SM2）	Linux 系统	Apache 服务器国密证书安装
		Nginx For Linux 国密证书安装
	Windows 系统	Nginx For Windows 服务器国密证书安装

根证书下载

如果您的业务需要通过非浏览器客户端访问您的服务，则需要下载安装根证书，详情请参见 [SSL 根证书下载](#)。

证书部署至腾讯云云服务

目前证书支持以下方式部署至云服务，请您根据实际需求进行部署操作。

- [安装部署 SSL 证书到负载均衡（CLB）指引](#)
- [安装部署 SSL 证书到内容分发网络（CDN）指引](#)
- [安装部署 SSL 证书到 Web 应用防火墙（WAF）指引](#)
- [安装部署 SSL 证书到 DDoS 防护指引](#)

- [安装部署 SSL 证书到云直播（CSS）指引](#)
- [安装部署 SSL 证书到容器服务 Ingress](#)
- [安装部署 SSL 证书到轻量应用服务器（Lighthouse）指引](#)
- [安装部署 SSL 证书到对象存储（COS）指引](#)
- [安装部署 SSL 证书到 API 网关指引](#)
- [腾讯云实现全站 HTTPS 方案](#)

国际标准 SSL 证书安装

腾讯云宝塔面板 SSL 证书安装部署

最近更新时间：2024-12-05 15:11:02

操作场景

本文档指导您如何在腾讯云宝塔面板中安装 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。
- 当前服务器的操作系统为 CentOS 7.6，Web 服务为 Nginx，由于操作系统与 Web 服务不同，详细操作步骤略有区别。
- 安装 SSL 证书前，请您在服务器上开启“443”端口，避免证书安装后无法启用 HTTPS，具体请参见 [服务器如何开启443端口？](#)

前提条件

- 已下载 SSL 证书压缩包至本地计算机。
- 以宝塔 Linux 面板 9.2.0 为例，已登录宝塔 Web 面板。若您未安装腾讯云宝塔面板，您可以参考文档 [安装宝塔面板](#)。

操作步骤

注意：

操作过程如果出现问题，请您 [联系我们](#)。

证书安装

- 请在 [SSL 证书控制台](#) 中选择您需要安装的证书并单击**下载**。
- 在弹出的**下载证书**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（本安装部署流程中不使用，可忽略）
 - `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。

- 登录宝塔 Web 面板，单击**网站**，即可进入**网站管理**页面。
- 在**网站管理**页面中，选择您需要配置 SSL 证书的域名对应的站点并单击**设置**，如下图所示：



5. 在弹出的站点修改窗口中，依次单击 **SSL > 当前证书**，填写密钥以及证书文件，如下图所示：

站点修改[d...c] -- 添加时间[2024-12-03 21:13:21]

域名管理
子目录绑定
网站目录
访问限制
流量限制
伪静态
默认文档
配置文件

SSL

PHP
重定向
反向代理
防盗链
防盗改
网站安全
网站日志
网站告警
其他设置

当前证书 - [已部署SSL] 商用SSL证书 测试证书 Let's Encrypt 证书类 需求反馈

证书分类: 其他证书 证书品牌: TrustAsia RSA DV TLS CA G2
认证域名: d...c 到期时间: 2025-01-10
强制HTTPS: ☐ 到期提醒: ☐ 到期设置提醒

密钥(KEY) 证书(PEM格式)

-----BEGIN RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----

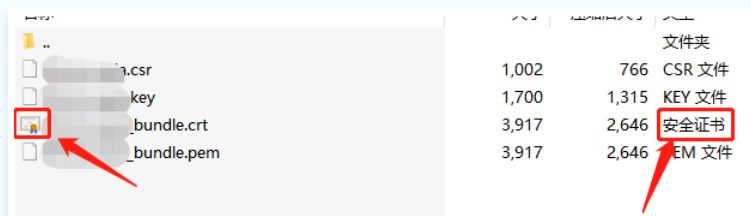
保存 下载证书 关闭SSL

- 粘贴您的*.key以及*.pem内容，然后保存即可[帮助]。
- 如果浏览器提示证书链不完整,请检查是否正确拼接PEM证书
- PEM格式证书 = 域名证书.crt + 根证书(root_bundle).crt
- 在未指定SSL默认站点时,未开启SSL的站点使用HTTPS会直接访问到已开启SSL的站点
- 如开启后无法使用HTTPS访问,请检查安全组是否正确放行443端口

- 密钥 (KEY)：使用文本编辑器打开 .key 私钥文件，并复制内容至对应区域，
- 证书 (PEM 格式)：使用文本编辑器打开 .crt 证书文件，并复制内容至对应区域。

❗ 说明：

部分电脑会隐藏 crt 后缀文件，可根据文件类型确定.crt 证书文件。



6. 单击**保存**并显示以下信息，即可部署成功。如下图所示：

已部署成功: 请在证书到期之前更换新的证书 证书品牌: TrustAsia T...

认证域名: ...com 到期时间: 2021-05-22

7. 部署成功后，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。如下图所示：



- 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

HTTP 自动跳转 HTTPS 的安全配置（可选）

！ 说明：

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. 请在弹出的“站点修改”窗口，单击开启**强制 HTTPS**即可完成配置，如下图所示：



- 1.
2. 您可以使用 `http://cloud.tencent.com` 进行访问。

Apache 服务器 SSL 证书安装部署（Linux）

最近更新时间：2024-12-05 15:11:02

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（ubuntu 系统也可参考此文），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。详情请参见 [上传文件到云服务器](#)。
- 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

注意：

操作过程如果出现问题，请 [联系我们](#)。

- 请在 [SSL 证书控制台](#) 中选择您需要安装的证书并单击**下载**。
- 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。详情请参见 [上传文件到云服务器](#)。

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 -p /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。如下图所示：



- 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

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。

Apache 服务器 SSL 证书安装部署（Windows）

最近更新时间：2024-12-05 15:11:02

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。具体请参见 [服务器如何开启443端口？](#)
- SSL 证书文件上传至服务器方法请参见 [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

注意：

操作过程如果出现问题，请您 [联系我们](#)。

步骤1：上传证书文件

- 请在 [SSL 证书控制台](#) 选择您需要安装的证书并单击**下载**。
- 在弹出的**下载证书**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：

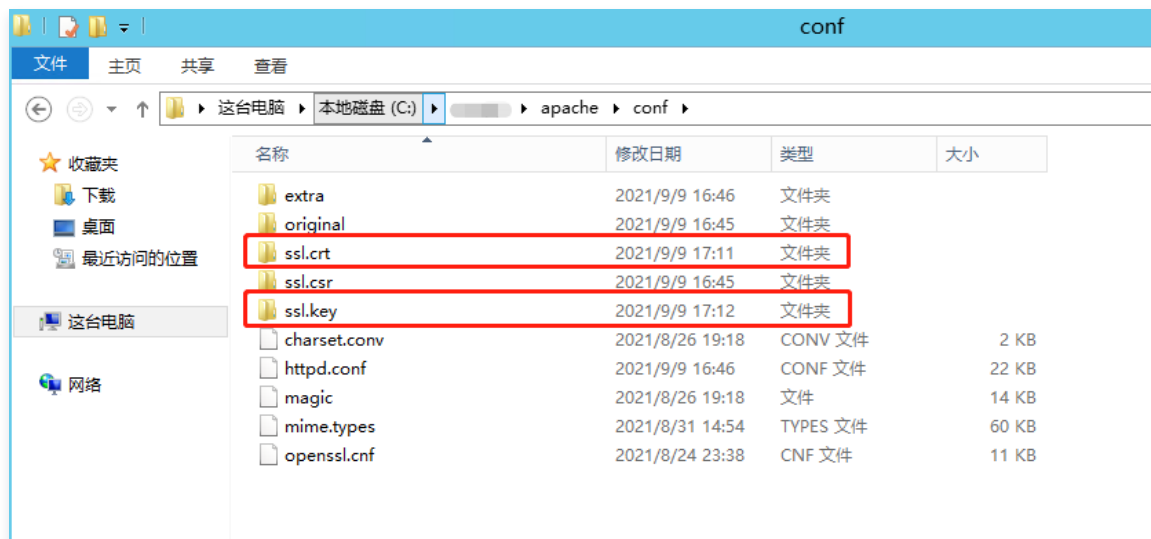
CSR 文件是申请证书时由您上传或系统在线生成的，提供给 CA 机构。安装时可忽略该文件。

- 通过 RDP 登录 Apache 服务器。

说明：

- 通过 RDP 上传文件请参见 [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，详情请参见 [上传文件到云服务器](#)。

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。对应文件目录如下图所示：



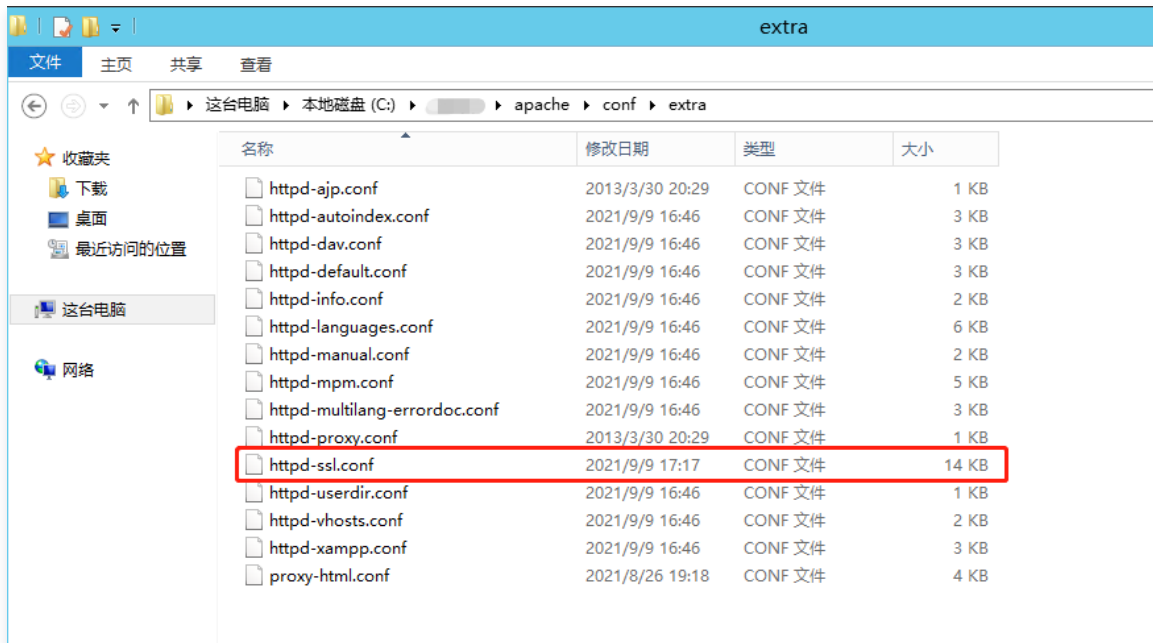
SSL 证书文件	对应文件夹
root_bundle.crt	ssl.crt
cloud.tencent.com.crt	
cloud.tencent.com.key	ssl.key

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，并删除以下字段前的 `#` 注释符。

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

2. 使用文本编辑器，打开 Apache 服务器 `conf\extra` 目录下 `httpd-ssl.conf` 文件，如下图所示：



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：

注意：

由于操作系统以及 Apache 安装方式不同，以上文件所处的位置也不同，下图示例仅供参考。

```
SSLCertificateFile "C:/apache/conf/ssl.crt/cloud.tencent.com.crt"
SSLCertificateKeyFile "C:/apache/conf/ssl.key/cloud.tencent.com.key"
SSLCertificateChainFile "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，如下图所示：



- 如果网站访问异常，请参见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

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，并删除以下字段前的 `#` 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 `http://cloud.tencent.com` 与 `https://cloud.tencent.com` 进行访问。访问后都将自动跳转到 `https://cloud.tencent.com`。

Nginx 服务器 SSL 证书安装部署（Linux）

最近更新时间：2024-08-16 21:16:21

以下视频将为您介绍进一步介绍在 Nginx 服务器安装 SSL 证书的操作过程：

[观看视频](#)

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。详情请参见 [上传文件到云服务器](#)。
- 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

- 请在 [SSL 证书控制台](#) 中选择您需要安装的证书并单击**下载**。
- 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
 - `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。详情请参见 [上传文件到云服务器](#)。

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 ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

- 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 /etc/www。
        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:!ADH:!RC4;
    #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/www。
        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。如下图所示：



- 最新版 Chrome 浏览器显示如下图标识，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](#)。

Nginx 服务器 SSL 证书安装部署（Windows）

最近更新时间：2024-12-27 14:55:52

操作场景

本文档指导您如何在 **Windows 操作系统** 上安装 SSL 证书。

说明：

- 本文以证书名称 `cloud.tencent.com` 为例。
- Nginx 版本以 `nginx/1.24.0` 为例。
- 当前服务器的操作系统为 **Windows Server 2022**，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，请您在服务器上开启 HTTPS 默认端口 443，避免证书安装后无法启用 HTTPS。

操作步骤

证书安装

注意：

操作过程如果出现问题，请您 [联系我们](#)。

1. 请在 [SSL 证书控制台](#) 中，选择您需要安装的证书并单击**下载**。
2. 在弹出的**下载证书**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. 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复制到服务器的 `C:\nginx\` 目录下（可以为任意不含中文字符和空格的目录，请根据实际情况操作）。

说明：

- 可使用“WinSCP”（即本地与远程计算机间的复制文件工具）登录 Nginx 服务器。
- WinSCP 上传文件操作请参见 [Windows 系统通过 MSTSC 上传文件到 Windows 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，详情请参见 [上传文件到云服务器](#)。

4. 编辑 `nginx.exe` 所在目录下的 `conf\nginx.conf` 文件。修改内容如下：

```
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;  
    #请填写证书文件的绝对路径。此路径仅供参考，具体请您按照实际目录操作  
    ssl_certificate C:\\nginx\\certificates\\cloud.tencent.com_bundle.crt;  
    #请填写私钥文件的绝对路径。此路径仅供参考，具体请您按照实际目录操作
```

```
ssl_certificate_key C:\\nginx\\certificates\\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。
    root C:\\html;
    index index.html index.htm;
}
}
```

5. 通过执行以下命令验证配置文件问题。

```
.\nginx.exe -t
```

- 若存在问题，请您重新配置或者根据提示修改存在问题。
- 若不存在问题，请执行 [步骤6](#)。

6. 通过执行以下命令启动 Nginx。

```
start .\nginx.exe
```

7. 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？](#)
 - [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](#)

Tomcat 服务器 SSL 证书安装部署（JKS 格式）（Linux）

最近更新时间：2024-08-16 21:16:21

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。请参考 [上传文件到云服务器](#)。
- 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

- 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。
- 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。详情请参考 [上传文件到云服务器](#)。

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 <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。

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"
      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" redirectPort="8443" />
    <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>
```

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。如下图所示：



- 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

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 `https://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：2024-10-22 17:13:32

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。
- 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

- 请在 [SSL 证书控制台](#) 中选择您需要安装的证书并单击下载。
- 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。如下图所示：

此电脑 > Windows (C:) > 用户 > [用户名] > 桌面 > tomcat-9.0.56 > conf

名称	修改日期	类型	大小
catalina.policy	2021/12/2 16:30	POLICY 文件	13 KB
catalina.properties	2021/12/2 16:30	PROPERTIES 文件	8 KB
context.xml	2021/12/2 16:30	XML 文档	2 KB
jaspic-providers.xml	2021/12/2 16:30	XML 文档	2 KB
jaspic-providers.xsd	2021/12/2 16:30	XSD 文件	3 KB
logging.properties	2021/12/2 16:30	PROPERTIES 文件	5 KB
server.xml	2021/12/2 16:30	XML 文档	8 KB
cloud.tencent.com.jks	2022/1/5 17:54	JKS 文件	5 KB
tomcat-users.xml	2021/12/2 16:30	XML 文档	3 KB
tomcat-users.xsd	2021/12/2 16:30	XSD 文件	3 KB
web.xml	2021/12/2 16:30	XML 文档	173 KB

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"
      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" redirectPort="443" />
    <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="" />
  <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://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。如下图所示：



- 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](#)

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。如下图所示：



名称	修改日期	类型	大小
catalina.policy	2021/12/2 16:30	POLICY 文件	13 KB
catalina.properties	2021/12/2 16:30	PROPERTIES 文件	8 KB
context.xml	2021/12/2 16:30	XML 文档	2 KB
jaspic-providers.xml	2021/12/2 16:30	XML 文档	2 KB
jaspic-providers.xsd	2021/12/2 16:30	XSD 文件	3 KB
logging.properties	2021/12/2 16:30	PROPERTIES 文件	5 KB
server.xml	2021/12/2 16:30	XML 文档	8 KB
tomcat-users.xml	2021/12/2 16:30	XML 文档	3 KB
tomcat-users.xsd	2021/12/2 16:30	XSD 文件	3 KB
web.xml	2021/12/2 16:30	XML 文档	173 KB

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 `http://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：2024-10-22 17:13:32

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）。
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。详情请参见[上传文件到云服务器](#)。
- 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

- 请在[SSL 证书控制台](#)中选择您需要安装的证书并单击下载。
- 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）
- 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。

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。详情请参见 [上传文件到云服务器](#)。

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

修改 `server.xml` 文件，添加 Connector 属性，内容如下：

```
<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_RSA_WITH_AES_128_CBC_S
HA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_S
HA256"/>
```

方式2：手动选择 SSL

修改 `server.xml` 文件，添加 Connector 属性，内容如下：

```
<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替换为证书保存的路
径、证书密码请替换为 keystorePass.txt 密码文件中的内容。-->
    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。

- 如果浏览器地址栏显示安全锁标识，则说明证书安装成功。如下图所示：



- 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

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：2024-12-09 18:29:31

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，具体请参见 [服务器如何开启443端口？](#)
- SSL 证书文件上传至服务器方法请参见 [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，详情请参见 [上传文件到云服务器](#)。
- 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

注意：

操作过程如果出现问题，请您 [联系我们](#)。

- 请在 [SSL 证书控制台](#) 选择您需要安装的证书并单击下载。
- 在弹出的下载证书窗口中，证书格式分别选择 **Apache** 和 **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。例如，使用 **“PuTTY” 工具** 登录。

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`。

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，详情请参见 [上传文件到云服务器](#)。

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。如下所示：

```
openssl pkcs12 -export -in cloud.tencent.com.crt -inkey cloud.tencent.com.key -out mycert.p12 -name s1as
```

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 -srcstoretype PKCS12 -alias s1as
```

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.crt -alias s1as
```

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9和步骤10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="http-listener-1"
thread-pool="http-thread-pool"></network-listener>
  <network-listener port="443" protocol="http-listener-2" transport="tcp" name="http-listener-2"
thread-pool="http-thread-pool"></network-listener>
  <network-listener port="4848" protocol="admin-listener" transport="tcp" name="admin-listener"
thread-pool="admin-thread-pool"></network-listener>
</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，如下图所示：



- 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

JBoss 服务器 SSL 证书安装部署

最近更新时间：2024-12-09 18:29:31

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。详情请参见 [上传文件到云服务器](#)。
- 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

注意：

操作过程如果出现问题，请 [联系我们](#)。

- 请在 [SSL 证书控制台](#) 中选择您需要安装的证书并单击下载。
- 在弹出的下载证书窗口中，证书格式选择 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 上传文件操作可参见 [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。详情请参见 [上传文件到云服务器](#)。

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>
<socket-binding-group name="standard-sockets" default-interface="public" port-
offset="{jboss.socket.binding.port-offset:0}">
  <socket-binding name="management-native" interface="management"
port="{jboss.management.native.port:9999}"/>
  <socket-binding name="management-http" interface="management"
port="{jboss.management.http.port:9990}"/>
  <socket-binding name="management-https" interface="management"
port="{jboss.management.https.port:9443}"/>
  <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" native="false">
  <connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http"/>
  <connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https"
    secure="true">
    <ssl name="https" password="*****" certificate-key-
      file="../../standalone/configuration/cert/cloud.tencent.com.jks" cipher-
      suite="TLS_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC
      _SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CB
      C_SHA" protocol="TLSv1,TLSv1.1,TLSv1.2"/>
    </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。如下图所示：



- 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

Jetty 服务器 SSL 证书安装部署

最近更新时间：2024-03-07 16:36:01

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。详情请参见 [上传文件到云服务器](#)。
- 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

- 请在 [SSL 证书控制台](#) 中选择您需要安装的证书并单击下载。
- 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）
- 远程登录 Jetty 服务器。例如，使用“[PuTTY](#)”工具登录。
- 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。详情请参见 [上传文件到云服务器](#)。

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://www.eclipse.org/jetty/configure_9_3.dtd">
<!-- ===== --><!-- SSL ContextFactory
configuration --><!--
===== -->
<!--
  To configure Includes / Excludes for Cipher Suites or Protocols see tweak-ssl.xml example at
  https://www.eclipse.org/jetty/documentation/current/configuring-ssl.html#configuring-
  sslcontextfactory-cipherSuites
-->
<Configure id="sslContextFactory" class="org.eclipse.jetty.util.ssl.SslContextFactory$Server">
  <Set name="Provider"><Property name="jetty.sslContext.provider"/></Set>
  <Set name="KeyStorePath"><Property name="jetty.base" default="." /></Property
name="jetty.sslContext.keyStorePath" deprecated="jetty.keystore"
default="etc/cert/cloud.tencent.com.jks"/></Set>
  <Set name="KeyStorePassword"><Property name="jetty.sslContext.keyStorePassword"
deprecated="jetty.keystore.password" default="4d5jtdq238j1l"/></Set>
  <Set name="KeyStoreType"><Property name="jetty.sslContext.keyStoreType" default="JKS"/></Set>
  <Set name="KeyStoreProvider"><Property name="jetty.sslContext.keyStoreProvider"/></Set>
  <Set name="KeyManagerPassword"><Property name="jetty.sslContext.keyManagerPassword"
deprecated="jetty.keymanager.password" default="4d5jtdq238j1l"/></Set>
  <Set name="TrustStorePath"><Property name="jetty.base" default="." /></Property
name="jetty.sslContext.trustStorePath" deprecated="jetty.truststore"
default="etc/cert/cloud.tencent.com.jks"/></Set>
  <Set name="TrustStorePassword"><Property name="jetty.sslContext.trustStorePassword"
deprecated="jetty.truststore.password"/></Set>
  <Set name="TrustStoreType"><Property name="jetty.sslContext.trustStoreType"/></Set>
  <Set name="TrustStoreProvider"><Property name="jetty.sslContext.trustStoreProvider"/></Set>
  <Set name="EndpointIdentificationAlgorithm"><Property
name="jetty.sslContext.endpointIdentificationAlgorithm"/></Set>
  <Set name="NeedClientAuth"><Property name="jetty.sslContext.needClientAuth"
deprecated="jetty.ssl.needClientAuth" default="false"/></Set>
  <Set name="WantClientAuth"><Property name="jetty.sslContext.wantClientAuth"
deprecated="jetty.ssl.wantClientAuth" default="false"/></Set>
  <Set name="useCipherSuitesOrder"><Property name="jetty.sslContext.useCipherSuitesOrder"
default="true"/></Set>
  <Set name="sslSessionCacheSize"><Property name="jetty.sslContext.sslSessionCacheSize"
default="-1"/></Set>
  <Set name="sslSessionTimeout"><Property name="jetty.sslContext.sslSessionTimeout" default="-1"/>
</Set>
```

```
<Set name="RenegotiationAllowed"><Property name="jetty.sslContext.renegotiationAllowed"
default="true"/></Set>
<Set name="RenegotiationLimit"><Property name="jetty.sslContext.renegotiationLimit" default="5"/>
</Set>
<Set name="SniRequired"><Property name="jetty.sslContext.sniRequired" default="false"/></Set>
<!-- Example of how to configure a PKIX Certificate Path revocation Checker
<Call id="pkixPreferCrls" class="java.security.cert.PKIXRevocationChecker$Option" name="valueOf">
<Arg>PREFER_CRLS</Arg></Call>
<Call id="pkixSoftFail" class="java.security.cert.PKIXRevocationChecker$Option" name="valueOf">
<Arg>SOFT_FAIL</Arg></Call>
<Call id="pkixNoFallback" class="java.security.cert.PKIXRevocationChecker$Option" name="valueOf">
<Arg>NO_FALLBACK</Arg></Call>
<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>
<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"
deprecated="ssl.acceptors" default="-1"/></Arg>
    <Arg name="selectors" type="int"><Property name="jetty.ssl.selectors"
deprecated="ssl.selectors" default="-1"/></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>
    <Set name="host"><Property name="jetty.ssl.host" deprecated="jetty.host" /></Set>
    <Set name="port"><Property name="jetty.ssl.port" deprecated="ssl.port" default="443" /></Set>
    <Set name="idleTimeout"><Property name="jetty.ssl.idleTimeout" deprecated="ssl.timeout"
default="30000"/></Set>
    <Set name="acceptorPriorityDelta"><Property name="jetty.ssl.acceptorPriorityDelta"
deprecated="ssl.acceptorPriorityDelta" default="0"/></Set>
    <Set name="acceptQueueSize"><Property name="jetty.ssl.acceptQueueSize"
deprecated="ssl.acceptQueueSize" default="0"/></Set>
    <Get name="SelectorManager">
      <Set name="connectTimeout"><Property name="jetty.ssl.connectTimeout" default="15000"/></Set>
```

```
</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。如下图所示：



- 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](#)。

Spring Boot 安装 SSL 证书

最近更新时间：2024-12-06 14:39:22

操作场景

本文档指导您如何为 Spring Boot 配置安装 PFX 格式 SSL 证书。

- ❗ 说明：
- 文档以证书名称 `cloud.tencent.com` 为例。
 - Spring Boot 版本以 `3.0.2` 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，具体请参见 [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，具体请参见 [服务器如何开启443端口？](#)

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。详情请参见 [上传文件到云服务器](#)。
- 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）。
- 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。

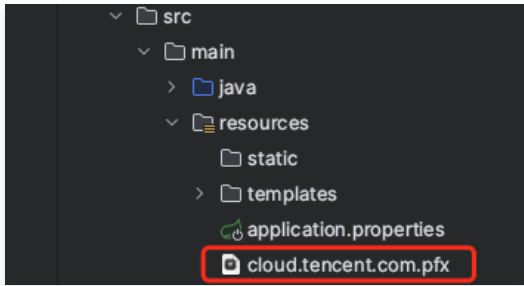
操作步骤

- ⚠ 注意：
- 操作过程如果出现问题，请您 [联系我们](#)。

- 请在 [SSL 证书控制台](#) 中选择您需要安装的证书并单击**下载**。
- 在弹出的**下载证书**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）
- 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。

- ❗ 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。详情请参见 [上传文件到云服务器](#)。

4. 将已获取到的 `cloud.tencent.com.pfx` 证书文件从本地目录拷贝至 Spring Boot 项目的 `src/main/resources` 目录下。如下图所示：



5. 远程登录 Spring Boot 服务器。例如，使用 “PuTTY” 工具 登录。

6. 编辑 Spring Boot 项目的 `application.properties` 或 `application.yml` 文件。并根据实际需求从以下方式中选择一种进行操作：

○ 方式1

修改 `application.properties` 文件，添加如下内容：

```
server.address=cloud.tencent.com
server.port = 443
server.ssl.key-store = classpath:cloud.tencent.com.pfx
server.ssl.key-store-password = *****
server.ssl.keyStoreType = PKCS12
```

○ 方式2

修改 `application.yml` 文件，添加如下内容：

```
server:
  port: 443
  ssl:
    key-store: classpath:cloud.tencent.com.pfx
    key-store-type: PKCS12
    key-store-password: yourpassword
    key-alias: cloud.tencent.com
```

配置文件的主要参数说明如下：

- **classpath:** 指的是项目的 `src/main/java` 和 `src/main/resources` 路径。存放在这两个路径下的文件都可以使用 `classpath` 作为路径来引用。
- **key-store:** 证书文件的存放位置。即 [操作步骤4](#) 存放证书文件的路径。
- **key-store-password:** 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。
- **key-alias:** 密钥别名。在 [SSL 证书控制台](#) 下载的，别名为证书的绑定域名。如：`cloud.tencent.com`。

7. 重启 Spring Boot 服务。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，如下图所示：



IIS 服务器 SSL 证书安装部署

最近更新时间：2024-03-07 16:36:01

操作场景

本文档指导您如何在 IIS 中安装 SSL 证书。

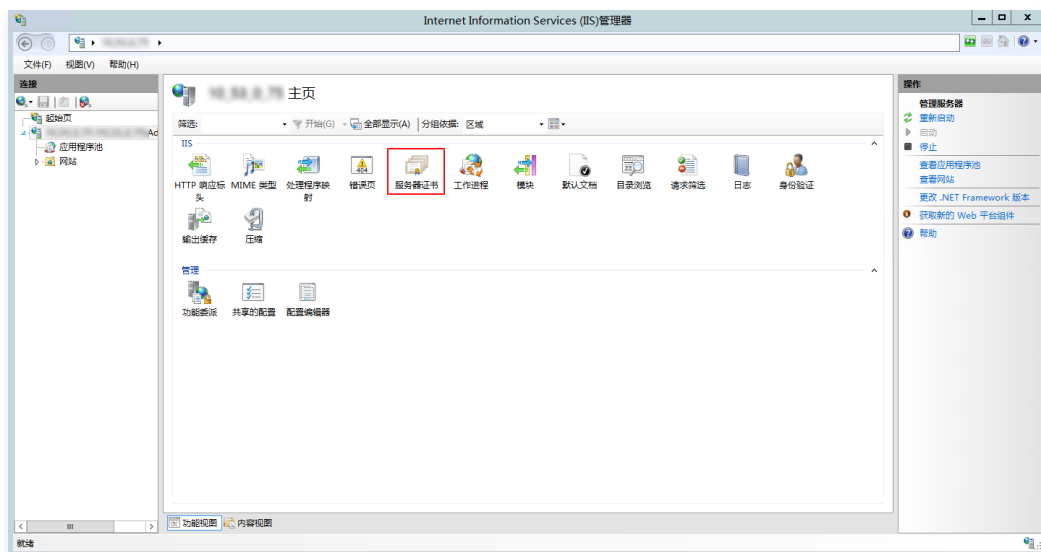
说明

- 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](#)。

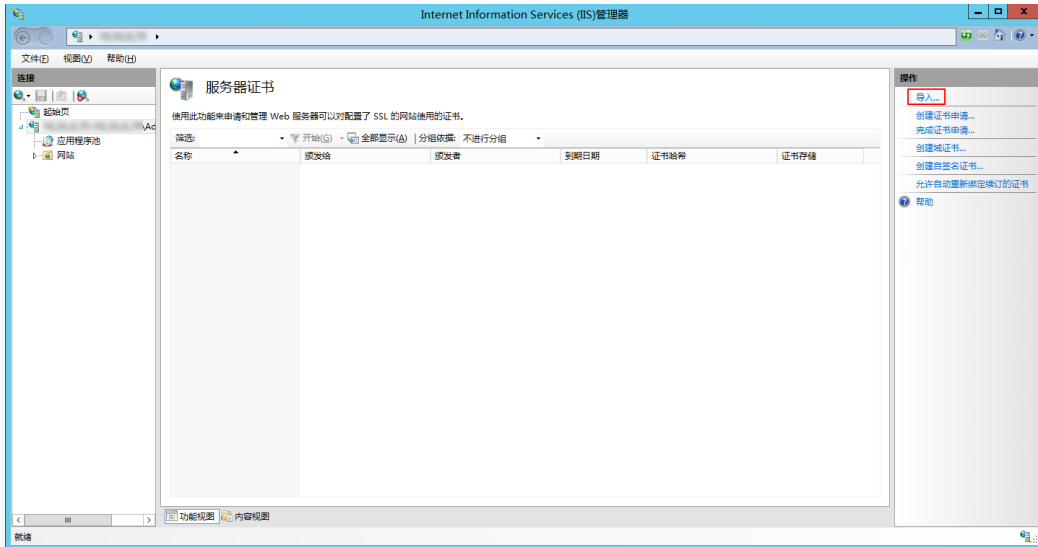
操作步骤

证书安装

- 请在 [SSL 证书控制台](#) 中选择您需要安装的证书并单击下载。
- 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）
- 打开 IIS 服务管理器，选择计算机名称，双击打开 “服务器证书”。如下图所示：



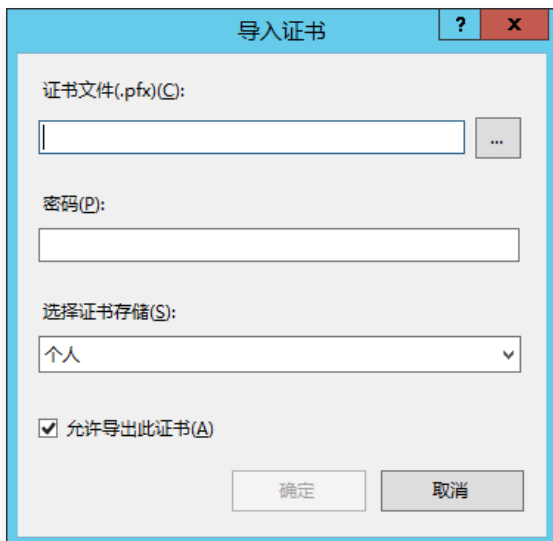
4. 在服务器证书窗口的右侧“操作”栏中，单击**导入**。如下图所示：



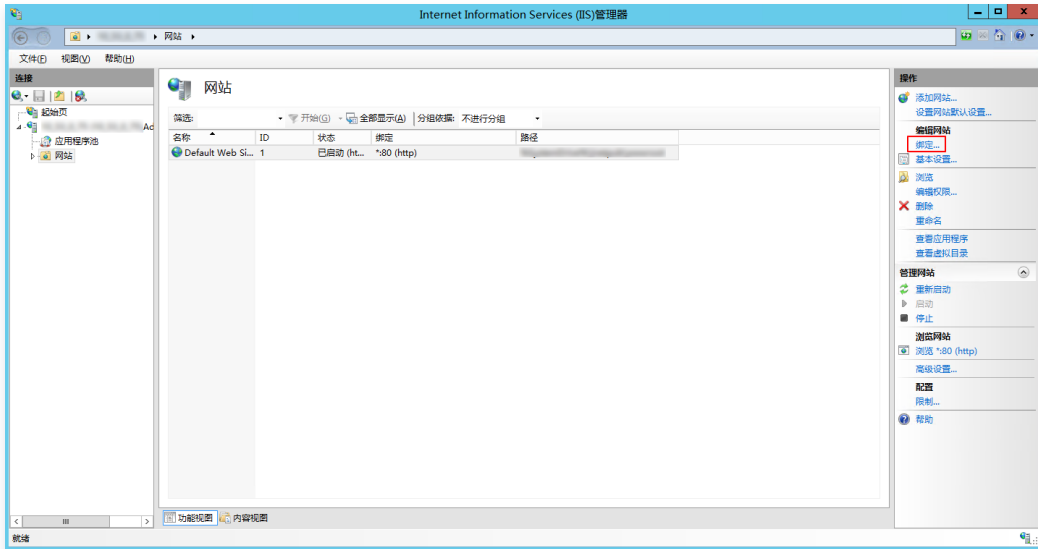
5. 在弹出的“导入证书”窗口中，选择证书文件存放路径，输入密码，单击**确定**。如下图所示：

说明

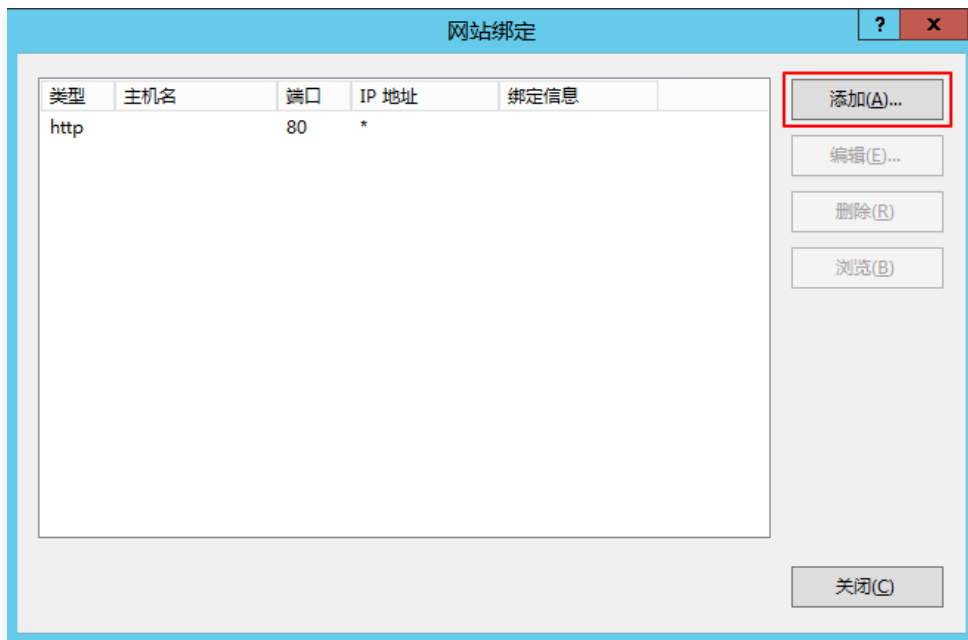
- 申请证书时若设置了私钥密码，输入密码时，请输入私钥密码。若申请证书时未设置私钥密码，输入密码时，请输入 `cloud.tencent.com.iis` 文件夹中 `keystorePass.txt` 文件的密码。
- 如果私钥密码不慎遗忘，请 [工单联系](#) 腾讯云工程师删除该证书，然后重新申请该域名证书。



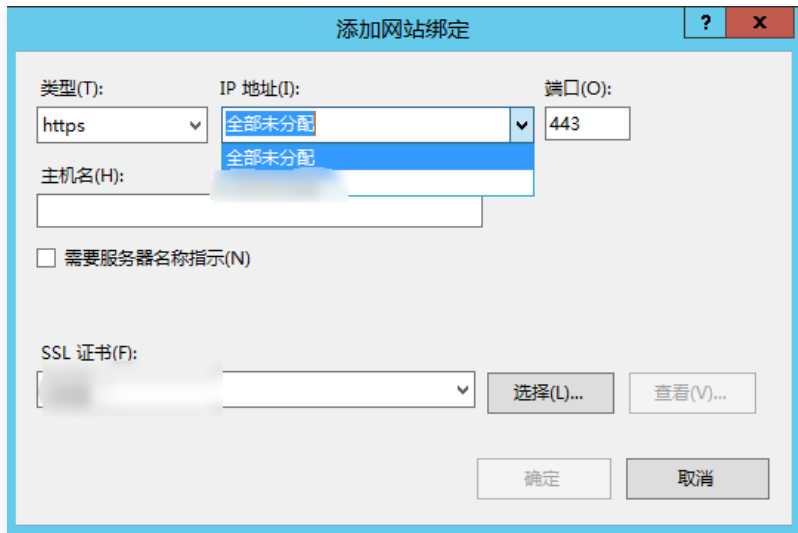
6. 选择网站下的站点名称，并单击右侧“操作”栏的**绑定**。如下图所示：



7. 在弹出的“网站绑定”窗口中，单击**添加**。如下图所示：



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**。如下图所示：



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。如下图所示：



- 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

HTTP 自动跳转 HTTPS 的安全配置（可选）

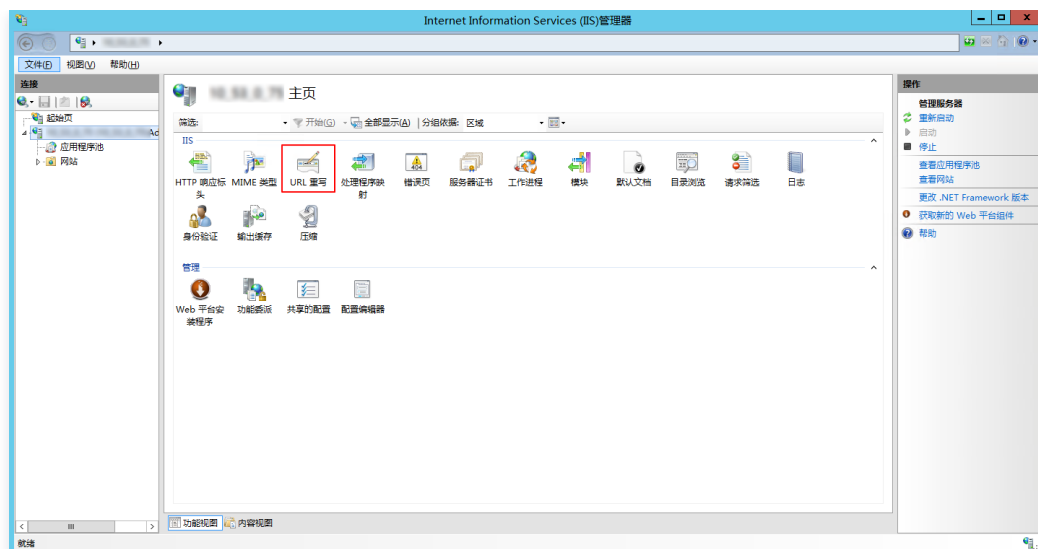
说明

- 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。

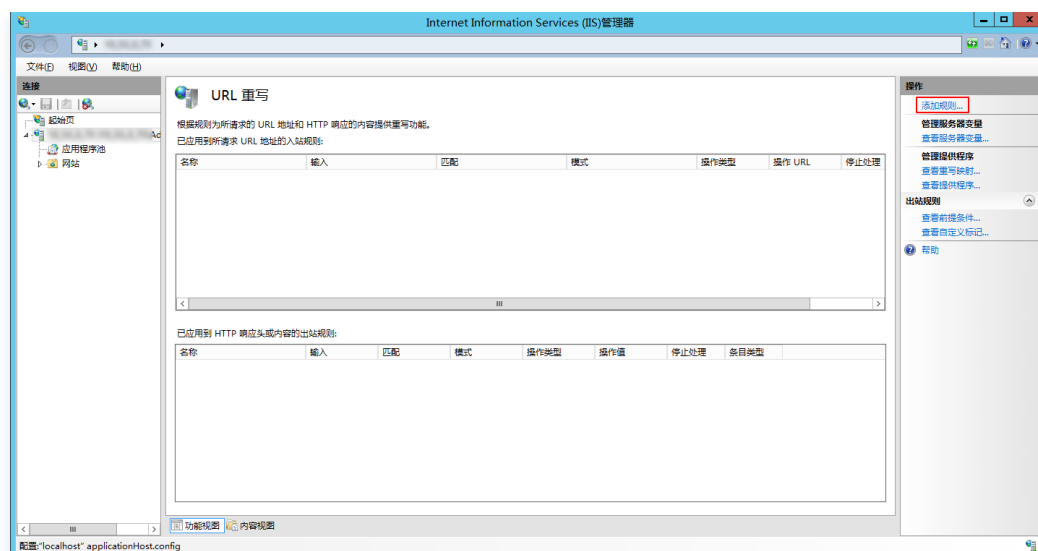
- 打开 IIS 服务管理器。
- 选择网站下的站点名称，双击打开“URL 重写”。如下图所示：

注意

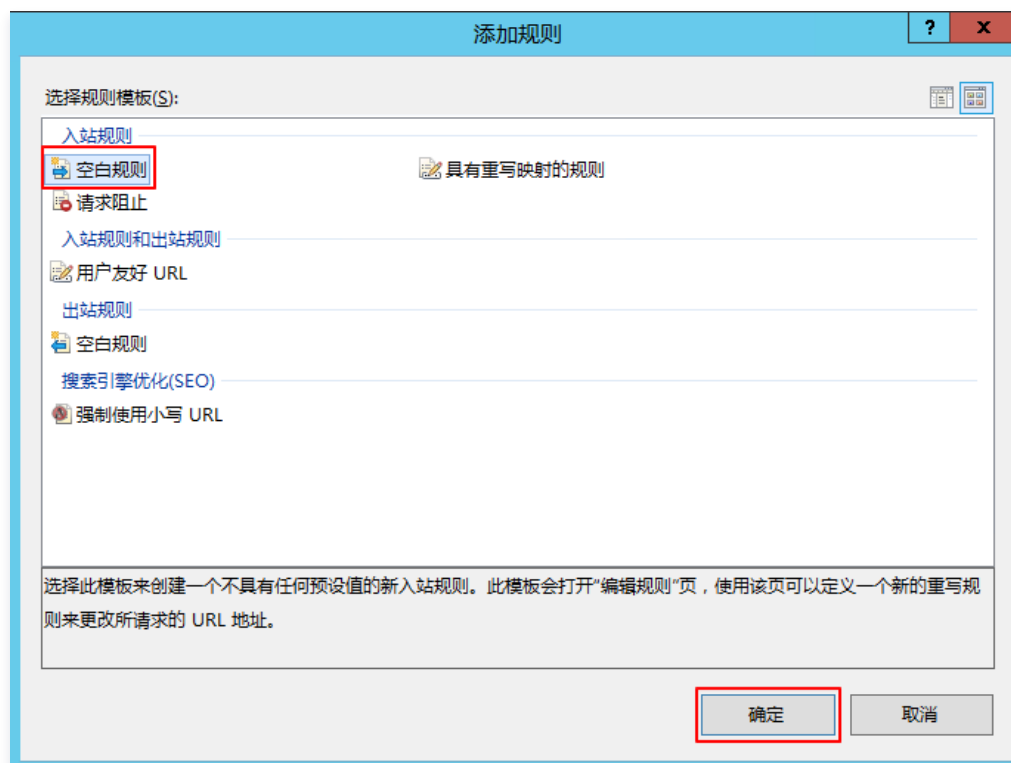
执行该步骤前请下载安装 [rewrite 模块](#)。



3. 进入“URL 重写”页面，并单击右侧“操作”栏的添加规则。如下图所示：



4. 在弹出的“添加规则”窗口中，选择空白规则，单击确定。如下图所示：



5. 进入“编辑入站规则”页面。如下图所示：



编辑入站规则

名称(N):

匹配 URL

请求的 URL(R):

与模式匹配

使用(S):

正则表达式

模式(I):

测试模式(P)...

☒ 忽略大小写(I)

条件

逻辑分组(G):

全部匹配

输入	类型	模式
{HTTPS}	与模式匹配	^OFF\$

添加...

编辑...

删除

上移

下移

☐ 跨条件跟踪捕获组(K)

服务器变量

操作

操作类型(Y):

重定向

操作属性

重定向 URL:

☒ 附加查询字符串(Q)

重定向类型:

参阅其他(303)

- 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 `https://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：2024-08-29 14:42:01

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。

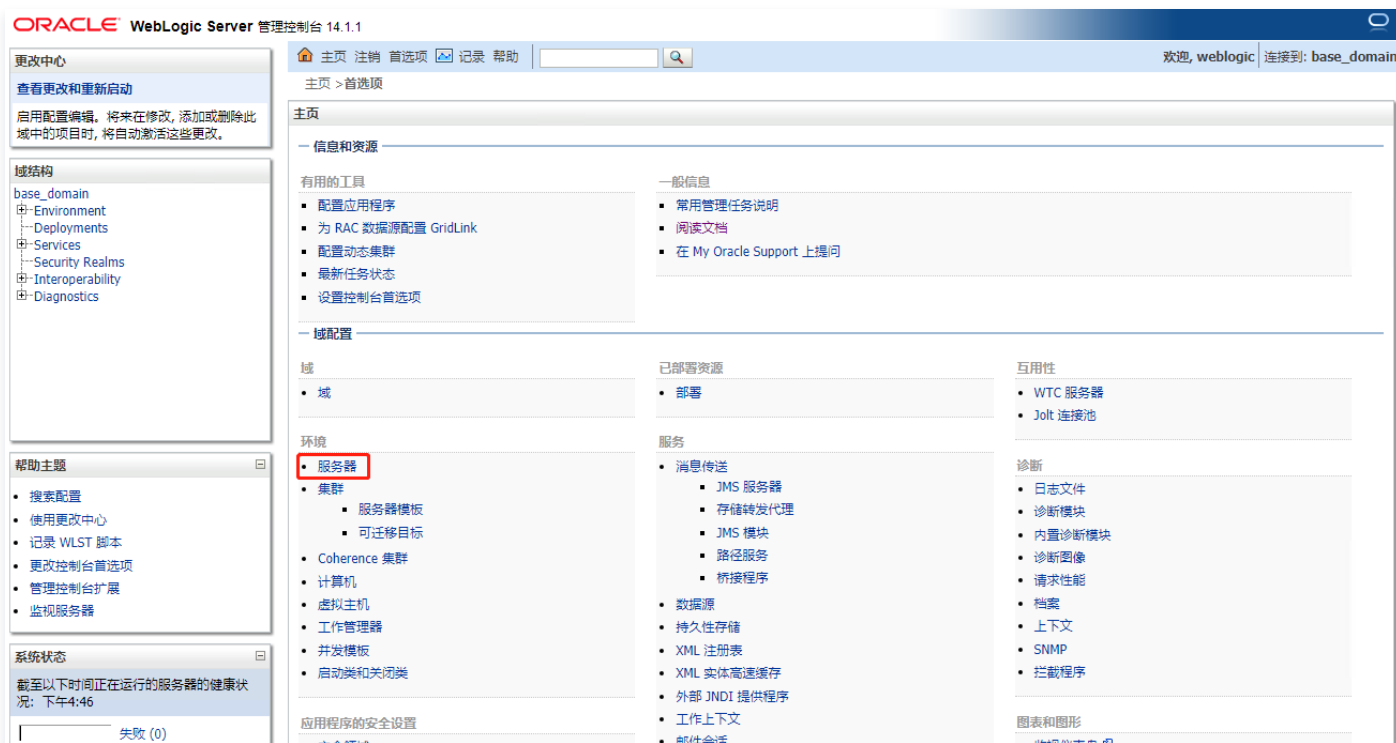
1. 请在 [SSL 证书控制台](#) 中选择您需要安装的证书并单击**下载**。
2. 在弹出的“证书下载”窗口中，服务器类型选择 **JKS**，单击**下载并解压缩** `cloud.tencent.com` 证书文件包到本地目录。
解压缩后，可获得相关类型的证书文件。其中包含 `cloud.tencent.com_jks` 文件夹：
 - 文件夹名称：`cloud.tencent.com_jks`
 - 文件夹内容：
 - `cloud.tencent.com.jks` 证书文件
 - `keystorePass.txt` 密码文件（若已设置私钥密码，则无 `keystorePass.txt` 密码文件）

说明：

- 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 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。操作方法如下：访问 [转换工具](#)。
- 未提供 JKS 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。

3. 请登录服务器，请在 C 盘中创建新的文件夹，以 `temp` 为例。
4. 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。
5. 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。

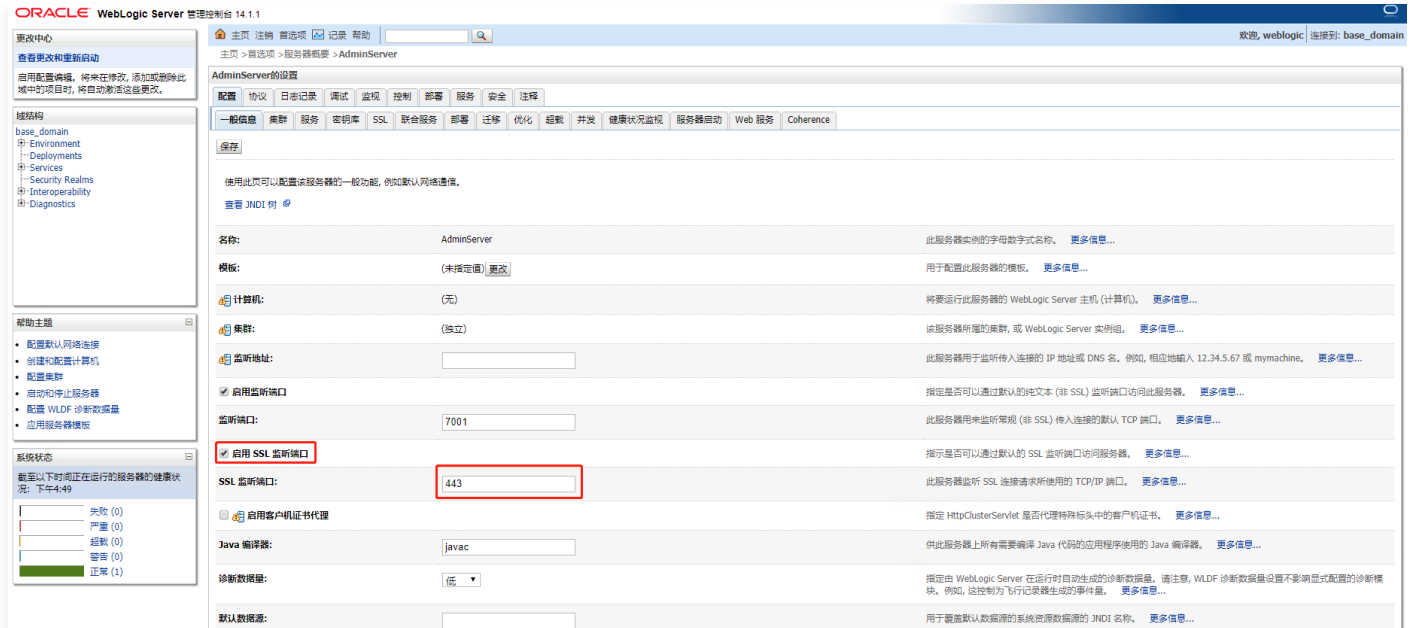
6. 单击域配置 > 服务器。进入“服务器概要”管理页面。如下图所示：



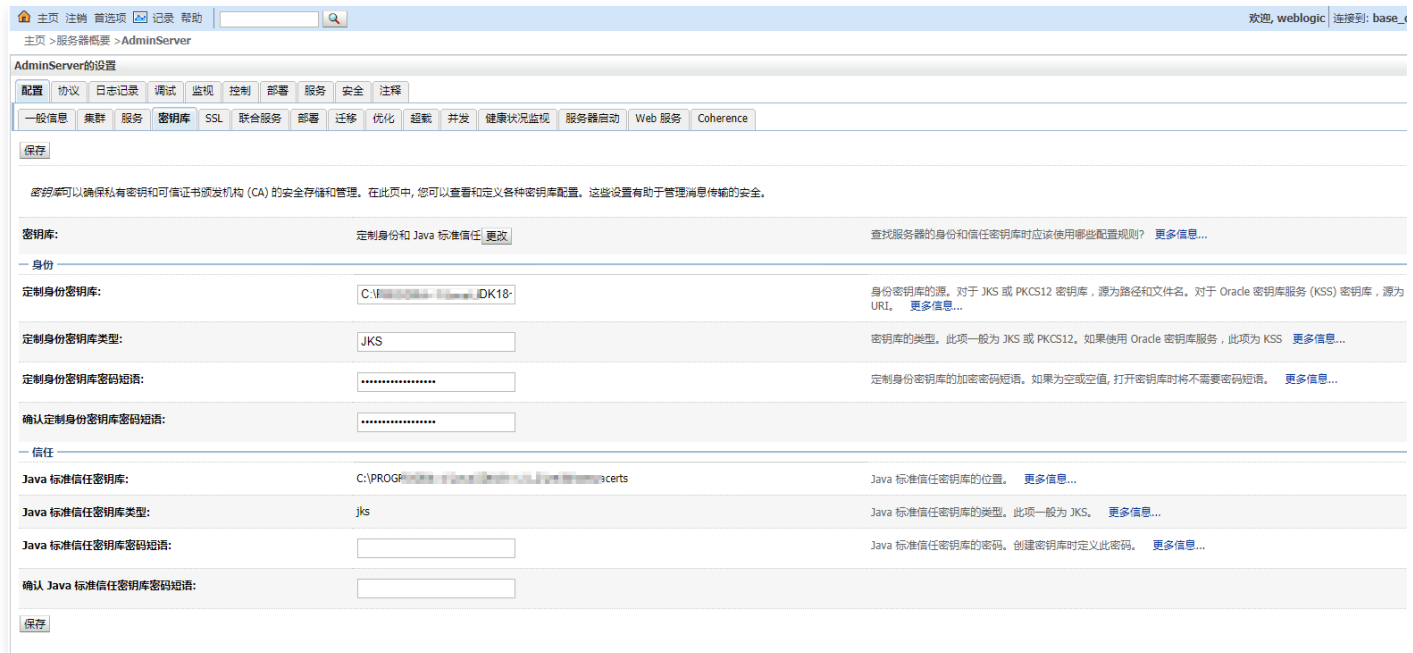
7. 选择您要配置的服务器名称，以 AdminServer 为例。如下图所示：



8. 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：



9. 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。

10. 在 AdminServer 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：

AdminServer 的设置

配置 协议 日志记录 调试 监视 控制 部署 服务 安全 注释

一般信息 集群 服务 密钥库 SSL 联合服务 部署 迁移 优化 超载 开发 健康状况监视 服务器启动 Web 服务 Coherence

保存

在此页中，您可以查看和定义此服务器实例的各种安全套接字层 (SSL) 设置。这些设置有助于管理消息传输的安全。

身份和信任位置: 密钥库 [更改](#) 指示 SSL 应在何处查找服务器的身份 (证书和私有密钥) 以及服务器的信任 (可信证书颁发机构)。 [更多信息...](#)

身份

私有密钥位置: 来自定制身份密钥库 定义私有密钥文件位置的密钥库属性。 [更多信息...](#)

私有密钥别名: 定义用于存储和检索服务器私有密钥的字符串别名的密钥库属性。 [更多信息...](#)

私有密钥密码短语: 密钥库属性，定义用来检索服务器私有密钥的密码短语。 [更多信息...](#)

确认私有密钥密码短语:

证书位置: 来自定制身份密钥库 用于定义可信证书位置的密钥库属性。 [更多信息...](#)

信任

可信证书颁发机构: 来自 Java 标准信任密钥库 用于定义证书颁发机构位置的密钥库属性。 [更多信息...](#)

高级

保存

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。

❗ 说明

默认为证书域名，例如为 *.dnspod.cn，则填写 *.dnspod.cn；如为 dnspod.cn，则填写 dnspod.cn。

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。

11. 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：

主页 注销 首选项 记录 帮助

主页 > 服务器概要 > AdminServer

消息

✓ 已激活所有更改。不需要重新启动。

✓ 设置更新成功。

AdminServer 的设置

配置 协议 日志记录 调试 监视 控制 部署 服务 安全 注释

一般信息 集群 服务 密钥库 SSL 联合服务 部署 迁移 优化 超载 开发 健康状况监视 服务器启动 Web 服务 Coherence

保存

在此页中，您可以查看和定义此服务器实例的各种安全套接字层 (SSL) 设置。这些设置有助于管理消息传输的安全。

12. 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。如下图所示：



- 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](#)

Node.js 环境 SSL 证书安装部署

最近更新时间：2025-01-22 14:26:21

操作场景

本文档指导您如何通过 Node.js 安装 SSL 证书。

说明：

- 本文档以 Nginx 服务器为例。
- 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。
- 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。详情请参见 [上传文件到云服务器](#)。
- 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）。

操作步骤

证书安装

1. 请在 [SSL 证书控制台](#) 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
 - `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。详情请参见 [上传文件到云服务器](#)。

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. 执行以下命令，新建 `https_server_test.js` 项目文件。

```
cd /home
sudo touch https_server_test.js
```

7. 执行以下命令，修改 `https_server_test.js` 文件。

```
vim https_server_test.js
```

8. 将以下内容添加至 `https_server_test.js` 文件中，具体内容如下所示：

```
// 启动https服务需要https包
// 读取文件需要fs包
const https = require('https');
const fs = require('fs');
// 将两个证书文件读取放到options对象中
// 使用readFileSync()方法，顺序地执行读文件和启动服务操作
const options = {
  key: fs.readFileSync('/etc/nginx/cloud.tencent.com.key'),
  cert: fs.readFileSync('/etc/nginx/cloud.tencent.com.crt')
};

// 创建服务器，启动服务器，设置监听端口号
https.createServer(options, (req, res) => {
  res.end('hello world\n');
}).listen(443);
```

9. 添加完成后，保存并退出文件。

10. 执行以下命令，使 SSL 证书生效。

```
sudo node https_server_test.js
```

11. 您可使用 `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，如下图所示：



- 最新版 Chrome 浏览器显示如下图标识，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](#)。

SSL 根证书下载

最近更新时间：2024-12-26 16:26:11

概述

根证书是属于证书颁发机构（CA）的公钥证书，是 SSL 证书信任链的起始点。本文将指导您如何下载根证书。

使用场景

- 如果您的业务通过浏览器进行访问，例如网站，则无需关注根证书。因为根证书已经内置在浏览器中，您只需在 Web 服务上安装已颁发的 SSL 证书，即可实现浏览器与 Web 服务的 HTTPS 通信。详情请参见 [如何选择 SSL 证书安装部署类型？](#)
- 如果您的业务需要通过非浏览器客户端访问您的服务，由于客户端没有预先内置根证书，您需要在对应客户端中安装根证书，保证客户端与服务端的正常通信。

⚠ 注意：

- 在非浏览器客户端中安装根证书，可能会因为根证书过期失效或策略变更等原因导致您的业务受到影响。推荐您使用系统默认信任库等方式进行客户端校验。
- 由于各客户端服务类型不同，安装根证书请咨询您的客户端开发商或开发者。

操作步骤

- 登录 [腾讯云 SSL 证书控制台](#)。
- 选择您需要下载根证书的 SSL 证书并单击**下载**，如下图所示：

购买证书			申请免费证书		上传证书		批量操作		证书状态 已签发		Q		三	
☐ 绑定域名/备注	证书信息	证书品牌	加密算法	到期时间	关联资源	状态	操作							
☐ st*.cn 未命名	证书ID: oR 有效期: 共 1 年, 当前第 1 年 所属项目: 默认项目	TrustAsia TLS ECC CA	ECC 256	2022-06-26 07:59:59	1	已签发	部署 下载 更多							

- 在弹出的**证书下载**窗口中，单击**下载**，即可下载根证书，如下图所示：

证书下载



请根据您的服务器类型选择证书下载：

服务器类型	操作
Tomcat (pfx格式)	下载
Tomcat (JKS格式)	下载
Apache	帮助 下载
Nginx	帮助 下载
IIS	帮助 下载
其他	帮助 下载
根证书下载	下载

网站代理 HTTPS 服务

不用安装证书，不用纠结各种安全套件的选择，不用担心私钥泄漏，网站代理 HTTPS 服务器 [立即使用](#) 助您解决网站 HTTPS 问题。

[取消](#)

国密标准（SM2）SSL 证书安装

Wotrus

Apache 服务器国密 SSL 证书（Wotrus）安装部署

最近更新时间：2025-04-16 11:06:12

操作场景

本文档指导您如何在 Apache 服务器中安装国密标准 SSL 证书。

说明：

- 国密标准 SSL 证书目前仅支持 Linux 环境下 Apache 服务器。
- 本文档以证书名称 `cloud.tencent.com` 为例。
- Apache 版本建议使用版本 `apache-2.4.46` 或 `apache-2.4.62`，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，具体请参见 [服务器如何开启443端口？](#)
- SSL 证书文件上传至服务器方法请参见 [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，详情请参见 [上传文件到云服务器](#)。
- 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）。
- 已购买国密标准（SM2）SSL 证书。
- 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

注意

操作过程如果出现问题，请 [联系我们](#)。

环境配置

说明：

- 国密标准 SSL 证书安装在 Apache 服务器上，Apache 服务器需具备相关环境支持模块。下文将指导您编译配置支持国密标准 SSL 证书的 Apache 服务器。
- 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. 远程登录 Apache 服务器。例如，使用 [PuTTY 工具](#) 登录。

2. 安装编译工具：如果您的系统是全新的，请先在服务器上安装 C++ 开发环境，为编译提供环境支持。您可以使用如下命令进行安装。

```
yum install -y gcc
yum install -y gcc-c++
```

3. 下载并编译安装 apr（以 apr 1.7.5 版本为例），您可以通过在服务器上输入以下命令，下载 apr 至服务器并编译安装，由于操作系统的版本不同，详细操作步骤略有区别。

```
#切换至 /usr/local/ 目录下
cd /usr/local/
#下载 apr 1.7.5
wget -c http://mirrors.tencent.com/apache/apr/apr-1.7.5.tar.gz
#解压已下载的 apr 1.7.5 压缩包
tar -zxvf apr-1.7.5.tar.gz
#进入解压后的 apr 1.7.5 文件夹并指定编译目录路径。
cd apr-1.7.5/
./configure --prefix=/usr/local/apr
#编译安装 apr
make && make install
```

4. 下载并编译安装 apr-util（推荐使用 apr-util-1.5 版本，以 apr-util-1.5 版本为例）。

```
#切换至 /usr/local/ 目录下
cd /usr/local/
#下载 apr-util-1.5.4
wget -c http://archive.apache.org/dist/apr/apr-util-1.5.4.tar.gz
#解压已下载的 apr-util-1.5.4 压缩包
tar -zxvf apr-util-1.5.4.tar.gz
#进入解压后的 apr-util-1.5.4 文件夹并指定编译目录路径。
cd /usr/local/apr-util-1.5.4/
./configure --prefix=/usr/local/apr-util --with-apr=/usr/local/apr
#编译安装 apr-util
make && make install
```

❗ 说明：

执行 make 命令时如果出现 #include <expat.h> ^ compilation terminated. 报错信息，请输入命令
yum install -y expat-devel 安装依赖库。

5. 安装 pcre。您可以通过以下两种方式进行安装。

- 推荐使用 yum 进行安装。

```
yum install -y pcre-devel
```

- 编译安装。

```
#切换至 /usr/local/ 目录下
cd /usr/local/
#下载 pcre-8.45
wget -c https://sourceforge.net/projects/pcre/files/pcre/8.45/pcre-8.45.tar.gz/download
#解压已下载的 pcre-8.45 压缩包
tar -zxvf pcre-8.45.tar.gz
#进入解压后的pcre-8.45文件夹并指定编译目录路径。
cd pcre-8.45/
./configure --prefix=/usr/local/pcre
#编译安装 pcre
```

```
make && make install
```

6. **Apache 服务器安装：**上述三个文件编译安装完成后，请下载 Apache 国密版和国密模块至 `/usr/local` 目录下进行编译安装。

⚠ 注意：

- 国密模块文件名 `wotrus_ssl.tar.gz` 在解压与安装中请勿修改，否则可能会导致安装错误。
- 如果在安装 Apache 的过程中找不到 `pcre`、`apr-util` 或 `apr` 等相关文件，请将 `/pcr/bin`、`/apr-util/bin` 或 `/apr/bin` 等文件加入系统路径。

```
#下载 Apache httpd-2.4.62 压缩包
wget -c http://mirrors.tencent.com/apache/httpd/httpd-2.4.62.tar.gz
#下载国密模块
wget -c https://www.wotrus.com/download/wotrus_ssl.tar.gz
#解压已下载的 wotrus_ssl 压缩包
tar -zxvf wotrus_ssl.tar.gz
#解压已下载的 httpd-2.4.62 压缩包
tar -zxvf httpd-2.4.62.tar.gz
#进入解压后的 httpd-2.4.62 文件夹并指定编译目录路径。
cd httpd-2.4.62/
./configure --prefix=/usr/local/httpd --enable-so --enable-ssl --enable-cgi --enable-rewrite --
enable-modules=most --enable-mpms-shared=all --with-mpm=prefork --with-zlib --with-
apr=/usr/local/apr --with-apr-util=/usr/local/apr-util --with-ssl=/usr/local/wotrus_ssl2.0
#编译安装 Apache
make && make install
```

国密标准证书安装

1. 已在 [SSL 证书控制台](#) 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 Apache 文件夹和 CSR 文件：

- 文件名称：`cloud.tencent.com_apache`
- 文件夹内容：
 - `root_sign_bundle.crt` 证书文件
 - `root_encrypt_bundle.crt` 证书文件
 - `cloud.tencent.com_sign.crt` 证书文件
 - `cloud.tencent.com_encrypt.crt` 证书文件
 - `cloud.tencent.com.key` 私钥文件
- CSR 文件内容：
 - `cloud.tencent.com_sign.csr` 文件
 - `cloud.tencent.com_encrypt.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。

2. 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 上传文件操作请参见 [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，详情请参见 [上传文件到云服务器](#)。

3. 进入 `/usr/local/httpd/conf` 目录，新建 `cert` 目录，将已获取到的 `root_sign_bundle.crt` 证书文件、`root_encrypt_bundle.crt` 证书文件、`cloud.tencent.com_sign.crt` 证书文件、`cloud.tencent.com_encrypt.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 `/usr/local/httpd/conf/cert` 目录下。

4. 进入 `/usr/local/httpd/conf` 目录，按照以下步骤编辑 `httpd.conf` 文件：

4.1 请在 `#ServerName www.example.com:80` 下增加 `ServerName (您的域名):80`。

4.2 请去掉 `LoadModule ssl_module modules/mod_ssl.so` 前的 `#`。

4.3 请在 `#Include conf/extra/httpd-ssl.conf` 下增加 `Include conf/ssl.conf` 文件内容后保存并退出。

5. 在 `/usr/local/httpd/conf` 目录下，新建一个 `ssl.conf` 文件，添加如下配置：

```
Listen 443
<VirtualHost *:443>
#填写证书名称
ServerName cloud.tencent.com
#填写网站文件路径
DocumentRoot website根目录
#启用 SSL 功能
SSLEngine on
# SM2 证书 sign 配置
SSLCertificateFile /usr/local/httpd/conf/cert/cloud.tencent.com_sign.crt
SSLCertificateKeyFile /usr/local/httpd/conf/cert/cloud.tencent.com.key
SSLCertificateChainFile /usr/local/httpd/conf/cert/root_sign_bundle.crt
# SM2 证书 encrypt 配置
SSLCertificateFile /usr/local/httpd/conf/cert/cloud.tencent.com_encrypt.crt
SSLCertificateKeyFile /usr/local/httpd/conf/cert/cloud.tencent.com.key
SSLCertificateChainFile /usr/local/httpd/conf/cert/root_encrypt_bundle.crt
# sign 和 encrypt 配置中的 .key 为同一个
#请按照以下协议配置
SSLProtocol all -SSLv2 -SSLv3
#请按照以下套件配置，配置加密套件，写法遵循 openssl 标准。
SSLCipherSuite ECC-SM4-SM3:SM2-WITH-SM4-SM3:ECDH:AESGCM:HIGH:MEDIUM:!RC4:!DH:!MD5:!aNULL:!eNULL
SSLHonorCipherOrder on
<Directory "website根目录">
Options -Indexes -FollowSymLinks +ExecCGI
AllowOverride None
Order allow,deny
Allow from all
Require all granted
</Directory>
</VirtualHost>
```

❗ 说明：

以上配置内容仅为参考，具体的证书名称，证书目录，`Directory` 等配置请根据实际环境配置。

6. 您通过执行以下命令验证配置文件问题。

```
/usr/local/httpd/bin/httpd -t
```

- 若提示 `Syntax OK`，则表示配置正常，可以启动 Apache 服务器。
- 若提示非 `Syntax OK`，请您重新配置或者根据提示修改存在问题。

7. 执行以下命令重新启动 Apache 服务器，即可使用 `https://cloud.tencent.com` 进行访问。

```
/usr/local/httpd/bin/httpd -k restart
```

- 如果浏览器地址栏显示安全锁标识，则说明证书安装成功。如下图所示：



- 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

国际标准证书与国密标准证书双安装（可选）

若您需要通过国际标准证书与国密标准证书双证书安装的方式解决浏览器兼容性问题，您可以通过以下操作设置：

说明：

腾讯云提供免费的 DV 型 SSL 证书以供购买了国密标准 DNSPod 证书的用户顺利解决浏览器兼容问题。申请证书请查看 [域名型（DV）免费 SSL 证书](#)。

1. 使用“WinSCP”（即本地与远程计算机间的复制文件工具），将已获取到的国际标准证书中的 `1_root_bundle.crt` 证书文件、`2_cloud.tencent.com.crt` 证书文件以及 `3_cloud.tencent.com.key` 私钥文件从本地目录拷贝到 Apache 服务器的 `/usr/local/httpd/conf` 目录下。

说明：

- WinSCP 上传文件操作请参见 [通过 WinSCP 上传文件到 Linux 云服务器](#)。
- 若您需部署到腾讯云服务器，建议使用云服务器的文件上传功能，详情请参见 [上传文件到云服务器](#)。

2. 编辑 `/usr/local/httpd/conf` 目录下的 `ssl.conf` 文件。
3. 请在 `SSLEngine on` 下面换行，并添加如下内容：

```
SSLCertificateFile /usr/local/httpd/conf/cert/2_cloud.tencent.com.crt
SSLCertificateKeyFile /usr/local/httpd/conf/cert/3_cloud.tencent.com.key
SSLCertificateChainFile /usr/local/httpd/conf/cert/1_root_bundle.crt
```

说明：

以上配置内容仅为参考，具体的证书名称，证书目录，请根据实际环境配置。

4. 您通过执行以下命令验证配置文件问题。

```
/usr/local/httpd/bin/httpd -t
```

- 若提示 `Syntax OK`，则表示配置正常，可以启动 Apache 服务器。
 - 若提示非 `Syntax OK`，请您重新配置或者根据提示修改存在问题。
5. 重新启动 Apache 服务器，即可解决浏览器兼容问题。

Nginx For Linux 国密 SSL 证书（Wotrus）安装部署

最近更新时间：2024-12-06 14:39:22

操作场景

本文档指导您如何在 Nginx 服务器中安装国密标准 SSL 证书。

说明：

- Nginx 版本以 `nginx/1.18.0` 为例。
- 本文档以证书名称 `cloud.tencent.com` 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“443”端口，避免证书安装后无法启用 HTTPS，具体请参见 [服务器如何开启443端口？](#)
- SSL 证书文件上传至服务器方法请参见 [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。详情请参见 [上传文件到云服务器](#)。
- 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）。
- 已购买国密标准（SM2）SSL 证书。
- 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

注意：

操作过程如果出现问题，请 [联系我们](#)。

环境配置

说明：

- 国密标准 SSL 证书安装在 Nginx 服务器上，Nginx 服务器需具备相关环境支持模块。下文将指导您编译配置支持国密标准 SSL 证书的 Nginx 服务器。
- 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. 远程登录 Nginx 服务器。例如，使用 [PuTTY 工具](#) 登录。
2. **安装编译工具：**如果您的系统是全新的，请先在服务器上安装 C++ 开发环境、`pcre-devel`、`zlib-devel` 软件为编译提供环境支持。您可以使用如下命令进行安装。

```
#安装 C++ 开发环境
yum install -y gcc gcc-c++
#安装 pcre-devel
```

```
yum install pcre-devel -y
#安装 zlib-devel
yum install zlib-devel -y
```

3. 下载并编译安装 Nginx: 您可以通过在服务器上按以下顺序输入命令, 下载 Nginx 国密版和国密模块至服务器并编译安装, 由于操作系统的版本不同, 详细操作步骤略有区别。

⚠ 注意:

- 以 nginx-1.18.0 为例, 目录为 /usr/local, 请根据您的实际环境与需求进行确定。
- 国密模块文件名 wotrus_ssl.tar.gz 在解压与安装中请勿修改, 否则可能会导致安装错误。

```
#切换至 /usr/local/ 目录下
cd /usr/local/
#下载 nginx-1.18.0
wget -c http://nginx.org/download/nginx-1.18.0.tar.gz
#下载国密SM2模块
wget -c https://www.wotrus.com/download/wotrus_ssl.tar.gz
#解压已下载的 nginx-1.18.0 压缩包
tar -zxvf nginx-1.18.0.tar.gz
#解压已下载的国密SM2模块压缩包
tar -zxvf wotrus_ssl.tar.gz
#进入解压后的 nginx-1.18.0 文件夹
cd nginx-1.18.0/
#指定编译目录路径与编译模块。如需其他模块可自行增加
./configure --prefix=/usr/local/nginx --with-http_stub_status_module --with-stream --with-
http_ssl_module --with-stream_ssl_module --with-openssl=/usr/local/wotrus_ssl2.0
#编译安装 Nginx
make && make install
```

4. 如果编译执行过程中出现 make[1]: *** [/usr/local/wotrus_ssl2.0/.openssl/include/openssl/ssl.h] Error 127 错误。则需要进入 nginx-1.18.0/auto/lib/openssl 目录, 编辑 conf 文件。需修改如下内容:

```
CORE_INCS="$CORE_INCS $OPENSSL/include"
CORE_DEPS="$CORE_DEPS $OPENSSL/include/openssl/ssl.h"
CORE_LIBS="$CORE_LIBS $OPENSSL/lib/libssl.a"
CORE_LIBS="$CORE_LIBS $OPENSSL/lib/libcrypto.a"
```

修改为:

```
CORE_INCS="$CORE_INCS $OPENSSL/include"
CORE_DEPS="$CORE_DEPS $OPENSSL/include/openssl/ssl.h"
CORE_LIBS="$CORE_LIBS $OPENSSL/lib/libssl.a"
CORE_LIBS="$CORE_LIBS $OPENSSL/lib/libcrypto.a"
```

5. 保存文件后, 需先执行 make clean 清除编译配置, 再重新进入 nginx-1.18.0 文件夹执行

```
./configure --prefix=/usr/local/nginx --with-http_stub_status_module --with-stream --with-http_ssl_module --
with-stream_ssl_module --with-openssl=/usr/local/wotrus_ssl2.0
```

与 make && make install。

国密标准证书安装

1. 已在 [SSL 证书控制台](#) 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 Nginx 目录和 CSR 文件:

- 文件夹名称: cloud.tencent.com_nginx
- 文件夹内容:

- `cloud.tencent.com_sign_bundle.crt` 证书公钥
- `cloud.tencent.com_sign_bundle.pem` 证书公钥
- `cloud.tencent.com_encrypt_bundle.crt` 证书公钥
- `cloud.tencent.com.key` 私钥文件
- **CSR 文件内容:**
 - `cloud.tencent.com_sign.csr` 文件
 - `cloud.tencent.com_encrypt.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。

2. 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。详情请参见 [上传文件到云服务器](#)。

3. 进入 `/usr/local/nginx/conf` 目录, 新建 `sm2` 目录, 将已获取到的 `cloud.tencent.com_sign_bundle.crt` 证书文件、`cloud.tencent.com_encrypt_bundle.crt` 证书文件、`cloud.tencent.com.key` 私钥文件从本地目录拷贝到该 `sm2` 目录下。
4. 进入 `/usr/local/nginx/conf` 目录, 编辑 `nginx.conf` 文件, 添加如下配置:

```
server {
    listen 443 ssl;
    server_name cloud.tencent.com;
    ssl_certificate /usr/local/nginx/conf/sm2/cloud.tencent.com_sign_bundle.crt;
    ssl_certificate_key /usr/local/nginx/conf/sm2/cloud.tencent.com.key;
    ssl_certificate /usr/local/nginx/conf/sm2/cloud.tencent.com_encrypt_bundle.crt;
    ssl_certificate_key /usr/local/nginx/conf/sm2/cloud.tencent.com.key;
    #先配置签名证书, 再配置加密证书, 签名加密证书私钥key为同一个!
    ssl_session_timeout 5m;
    ssl_protocols TLSv1.1 TLSv1.2 TLSv1.3;
    ssl_ciphers ECC-SM4-SM3:ECDH:AESGCM:HIGH:MEDIUM:!RC4:!DH:!MD5:!aNULL:!eNULL;
    ssl_prefer_server_ciphers on;
    location / {
        root html;
        index index.html index.htm;
    }
}
```

说明:

以上配置内容仅为参考, 具体的证书名称, 证书目录, `location` 等配置请根据实际环境配置。

5. 请您通过执行以下命令验证配置文件问题。

```
/usr/local/nginx/sbin/nginx -t
```

- 若提示 `test is successful`, 则表示配置正常, 可以启动 Nginx 服务器。
- 若提示 `test failed`, 请您重新配置或者根据提示修改存在问题。

6. 重新启动 Nginx 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。如下图所示：



- 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

国际标准证书与国密标准证书双安装（可选）

若您需要通过国际标准证书与国密标准证书双证书安装的方式解决浏览器兼容性问题，您可以通过以下操作设置：

❗ 说明：

腾讯云提供免费的 DV 型 SSL 证书以供购买了国密标准 DNSPod 证书的用户顺利解决浏览器兼容问题。申请证书请查看 [域名型（DV）免费 SSL 证书](#)。

1. 使用“WinSCP”（即本地与远程计算机间的复制文件工具），将已获取到的国际标准证书压缩包中 Nginx 文件夹的 `root_bundle.crt` 证书文件、`cloud.tencent.com.key` 私钥文件从本地目录拷贝到 Nginx 服务器的 `/usr/local/nginx/conf/sm2` 目录下。

❗ 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服务器，建议使用云服务器的文件上传功能。详情请参见 [上传文件到云服务器](#)。

2. 编辑 `/usr/local/nginx/conf` 目录下的 `nginx.conf` 文件。
3. 请在 `cloud.tencent.com` 下面换行，并添加如下内容：

```
ssl_certificate /usr/local/nginx/conf/sm2/cloud.tencent.com_bundle.crt;
ssl_certificate_key /usr/local/nginx/conf/sm2/cloud.tencent.com.key;
```

❗ 说明：

以上配置内容仅为参考，具体的证书名称，证书目录，请根据实际环境配置。

4. 您通过执行以下命令验证配置文件问题。

```
/usr/local/nginx/sbin/nginx -t
```

- 若提示 `test is successful`，则表示配置正常，可以启动 Nginx 服务器。
 - 若提示 `test failed`，请您重新配置或者根据提示修改存在问题。
5. 重新启动 Nginx 服务器，即可解决浏览器兼容问题。

Nginx For Windows 国密 SSL 证书（Wotrus）安装部署

最近更新时间：2024-12-03 11:38:42

操作场景

本文档指导您如何在国密版 Nginx 服务器中安装国密标准 SSL 证书（Wotrus）。

说明

- 国密标准 SSL 证书仅支持安装在国密版本的 Nginx 服务器上。
- 目前仅提供64位 `nginx/1.16.0` 国密版与32位 `nginx/1.17.0` 国密版，如您需其它版本，请您使用 [在线咨询](#)，腾讯云工程师将为您提供其他版本与帮助。
- Nginx 版本以国密版 `nginx/1.16.0` 为例。
- 本文档以证书名称 `cloud.tencent.com` 为例。
- 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，请您开启服务器上“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](#)。

下载 Windows For Nginx 国密版

Nginx 版本	32位	64位
1.16.0	—	单击下载
1.17.0	单击下载	—

前提条件

- 已在服务器中下载国密版 Nginx 压缩包。
- 已购买国密标准（SM2）SSL 证书。
- 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

国密标准证书安装

注意

下述步骤中的目录均为测试环境的目录，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 Nginx 目录和 CSR 文件：

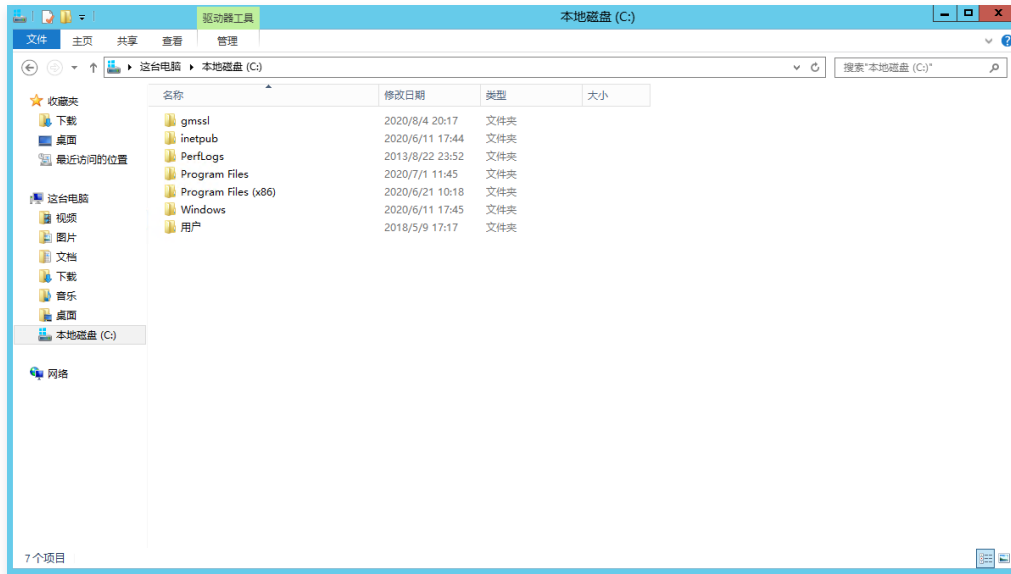
- 文件夹名称：`cloud.tencent.com_nginx`
- 文件夹内容：

- cloud.tencent.com_sign_bundle.crt 证书文件
- cloud.tencent.com_sign_bundle.pem 证书文件
- cloud.tencent.com_encrypt_bundle.crt 证书文件
- cloud.tencent.com_encrypt_bundle.pem 证书文件
- cloud.tencent.com.key 私钥文件
- CSR 文件内容:
 - cloud.tencent.com_sign.csr 文件
 - cloud.tencent.com_encrypt.csr 文件

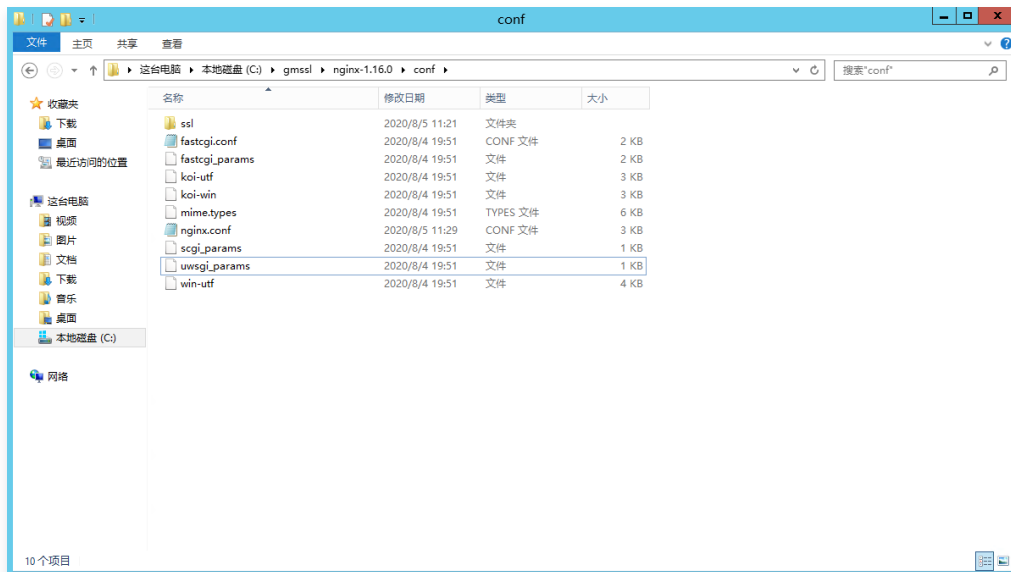
说明

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。

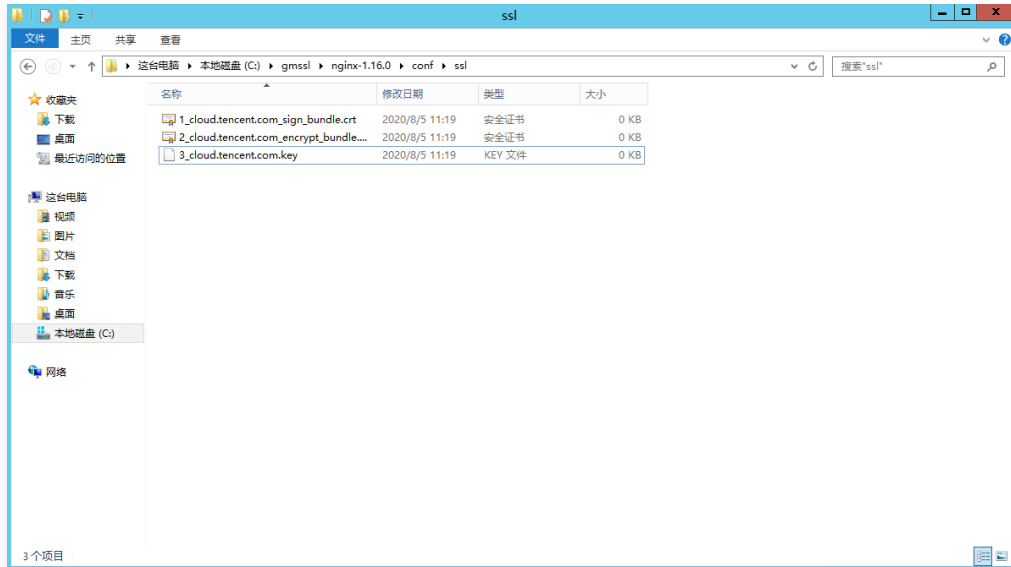
2. 登录服务器，解压已下载的国密版 Nginx 压缩包到相应的目录，例如 `c:\gmssl`。如下图所示：



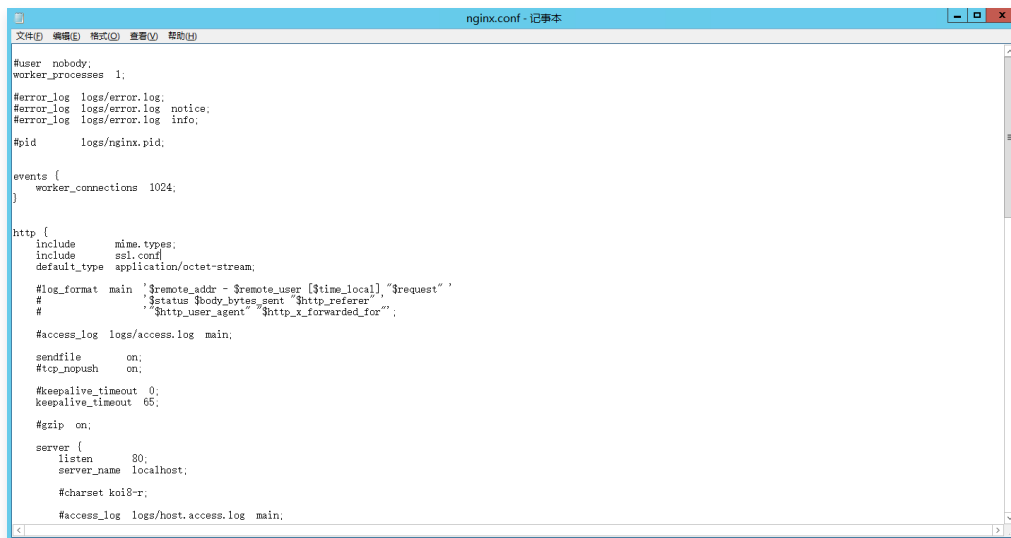
3. 在 `/nginx-1.16.0/conf` 目录下创建存放证书的文件夹，例如设置为 `ssl` 目录。如下图所示：



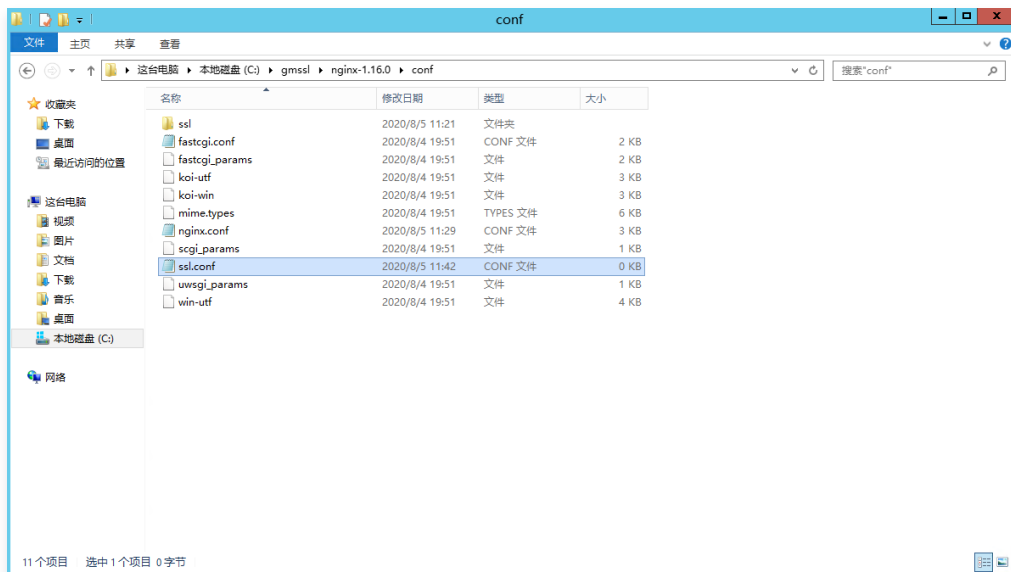
4. 将解压后的 crt 证书文件与 key 私钥文件放在已创建的 `ssl` 目录中，如下图所示：



5. 编辑 `/nginx-1.16.0/conf` 目录下的 `nginx.conf` 文件，在 `http{}` 中，添加 `include ssl.conf;` 文件内容。如下图所示：



6. 请在 `/nginx-1.16.0/conf` 目录下新建 `ssl.conf` 文件。如下图所示：



7. 编辑新建的 `ssl.conf` 文件，添加证书配置，如下所示：

```
server {
    listen 443 ssl;
    server_name cloud.tencent.com;
    ssl_certificate c:/gmssl/nginx-1.16.0/conf/ssl/1_cloud.tencent.com_sign_bundle.crt;
    ssl_certificate_key c:/gmssl/nginx-1.16.0/conf/ssl/3_cloud.tencent.com.key;
    ssl_certificate c:/gmssl/nginx-1.16.0/conf/ssl/2_cloud.tencent.com_encrypt_bundle.crt;
    ssl_certificate_key c:/gmssl/nginx-1.16.0/conf/ssl/3_cloud.tencent.com.key;
    #先配置签名证书，再配置加密证书，签名加密证书私钥 key 为同一个!
    ssl_session_timeout 5m;
    ssl_protocols TLSv1.2;
    ssl_ciphers SM2-WITH-SM4-SM3:ECDH:AESGCM:HIGH:MEDIUM:!RC4:!DH:!MD5:!aNULL:!eNULL;
    ssl_prefer_server_ciphers on;
    location / {
        root html;
        index index.html index.htm;
    }
}
```

❗ 说明

- 建议使用 Administrator 账户配置证书，若用非管理员权限账户配置，可能出现找不到证书的错误。
- 以上配置仅为参考，具体配置请根据实际环境配置。

8. 配置完成后，您可以通过在服务器 dos 命令下，执行 cd 命令行进入 `nginx-1.16.0` 目录，例如 `cd c:\gmssl\nnginx-1.16.0`，输入 `nginx -t`，检测 Nginx 配置是否正常。

- 若看到以下提示，则表示配置正常，可以启动 Nginx 服务器。

```
nginx: the configuration file /path/nginx.conf syntax is ok
nginx: configuration file /path/nginx.conf test is successful
```

- 若看到非上述提示，请您重新配置或者根据提示修改存在问题。

9. 启动 Nginx 服务器，进入 `/nginx-1.16.0` 目录，双击运行 `nginx.exe` 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。如下图所示：



- 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

国际标准证书与国密标准证书双安装（可选）

若您需要通过国际标准证书与国密标准证书双证书安装的方式解决浏览器兼容性问题。您可以通过以下操作设置：

❗ 说明

- 腾讯云提供免费的 DV 型 SSL 证书以供购买了国密标准 DNSPod 证书的用户顺利解决浏览器兼容问题。申请证书请查看 [域名型（DV）免费 SSL 证书](#)。
- 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. 将已获取到的国际标准证书压缩包中 Nginx 文件夹的 `1_root_bundle.crt` 证书文件、`2_cloud.tencent.com.key` 解压缩后放在已创建的 `ssl` 目录中。

⚠ 注意

执行以下操作前请确保已关闭全部 Nginx 服务，避免资源占用，导致无法正常访问最新配置的 Nginx 服务。

2. 编辑 `/nginx-1.16.0/conf` 目录下 `ssl.conf` 文件。
3. 请在 `server_name cloud.tencent.com` 下面换行，并添加如下内容：

```
ssl_certificate c:/gm_nginx-1.16.0/nginx-1.16.0/conf/ssl/1_cloud.tencent.com_bundle.crt;  
ssl_certificate_key c:/gm_nginx-1.16.0/nginx-1.16.0/conf/ssl/2_cloud.tencent.com.key;
```

4. 配置完成后，您可以通过在服务器 dos 命令下，执行 `cd` 命令行进入 `nginx-1.16.0` 目录，例如 `cd c:\gmssl\nginx-1.16.0`，输入 `nginx -t`，检测 Nginx 配置是否正常。

- 若看到以下提示，则表示配置正常，可以启动 Nginx 服务器。

```
nginx: the configuration file /path/nginx.conf syntax is ok  
nginx: configuration file /path/nginx.conf test is successful
```

- 若看到非上述提示，请您重新配置或者根据提示修改存在问题。

5. 启动 Nginx 服务器，进入 `/nginx-1.16.0` 目录，双击运行 `nginx.exe`，即可解决浏览器兼容性问题。

⚠ 注意

操作过程如果出现问题，请 [联系我们](#)。

DNSPod

Nginx For Linux 国密 SSL 证书安装（DNSPod）

最近更新时间：2024-12-06 14:39:23

操作场景

本文档指导您如何在 Nginx 服务器中安装国密标准 DNSPod SSL 证书。

说明：

- Nginx 版本以 nginx/1.18.0 为例。
- 本文档以证书名称 cloud.tencent.com 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“443”端口，避免证书安装后无法启用 HTTPS。具体请参见 [服务器如何开启443端口？](#)
- SSL 证书文件上传至服务器方法请参见 [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。详情请参见 [上传文件到云服务器](#)。
- 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）。
- 已购买国密标准（SM2）DNSPod SSL 证书。
- 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。
密码	登录服务器的密码。
用户名	登录服务器的用户名。

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

注意：

操作过程如果出现问题，请您 [联系我们](#)。

环境配置

说明：

- 国密标准 DNSPod SSL 证书安装在 Nginx 服务器上，Nginx 服务器需具备相关环境支持模块。下文将指导您编译配置支持国密标准 DNSPod SSL 证书的 Nginx 服务器。
- 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. 远程登录 Nginx 服务器。例如，使用 **PuTTY工具** 登录。
2. 安装编译依赖包。如果您的系统是全新的，请先在服务器上安装以下依赖包，为编译提供环境支持。您可以使用如下命令进行安装。

```
yum install -y gcc gcc-c++ wget make perl pcre-devel zlib-devel
```

3. 下载并编译安装 Nginx。您可以通过在服务器上按以下顺序输入命令，下载 Nginx 国密版和国密模块至服务器并编译安装，由于操作系统的版本不同，详细操作步骤略有区别。

注意：

DNSPod 国密模块文件名 `gmssl_openssl_2021.1011.tar.gz` 在解压与安装中请勿修改，否则可能会导致安装错误。以 `nginx-1.18.0` 为例，目录为 `/usr/local`，请根据您的实际环境与需求进行确定。

3.1 下载 Nginx 国密版和国密模块。

```
# 切换至 /usr/local/ 目录下
cd /usr/local/
# 下载 nginx-1.18.0
wget -c http://nginx.org/download/nginx-1.18.0.tar.gz
# 下载 DNSPod 国密模块
wget -c https://certificate-1258344699.cos.ap-
guangzhou.myqcloud.com/public/gmssl_openssl_2021.1011.tar.gz
# 解压已下载的 nginx-1.18.0 压缩包
tar -zxvf nginx-1.18.0.tar.gz
# 解压已下载的 gmssl_openssl_2021.1011 压缩包
tar -zxvf gmssl_openssl_2021.1011.tar.gz
```

3.2 编辑 `/usr/local/nginx-1.18.0/auto/lib/openssl/conf` 文件，指向静态 gmssl，修改内容如下：

修改前：

```
CORE_INCS="$CORE_INCS $OPENSSL/include"
CORE_DEPS="$CORE_DEPS $OPENSSL/include/openssl/ssl.h"
CORE_LIBS="$CORE_LIBS $OPENSSL/lib/libssl.a"
CORE_LIBS="$CORE_LIBS $OPENSSL/lib/libcrypto.a"
```

修改后：

```
CORE_INCS="$CORE_INCS $OPENSSL/include"
CORE_DEPS="$CORE_DEPS $OPENSSL/include/openssl/ssl.h"
CORE_LIBS="$CORE_LIBS $OPENSSL/lib/libssl.a"
CORE_LIBS="$CORE_LIBS $OPENSSL/lib/libcrypto.a"
```

3.3 编译安装 Nginx。

```
# 切换至 /usr/local/ 目录下
cd /usr/local/nginx-1.18.0
# 指定编译目录路径与编译模块。如需其他模块可自行增加
./configure --prefix=/usr/local/nginx --without-http_gzip_module --with-http_ssl_module --with-
http_stub_status_module --with-http_v2_module --with-file-aio --with-openssl="/usr/local/gmssl" -
-with-cc-opt="-I/usr/local/gmssl/include" --with-ld-opt="-lm"
# 编译安装
make && make install
```

国密标准证书安装

1. 已在 [SSL 证书控制台](#) 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 Nginx 文件夹和 CSR 文件：

- 文件夹名称：`cloud.tencent.com_nginx`
- 文件夹内容：
 - `cloud.tencent.com.key` 私钥文件

- `cloud.tencent.com._sign_bundle.crt` 签名证书文件
- `cloud.tencent.com._sign.key` 签名证书私钥文件
- `cloud.tencent.com._sign_bundle.pem` (可忽略该文件)
- `cloud.tencent.com._encrypt_bundle.crt` 加密证书文件
- `cloud.tencent.com._encrypt.key` 加密证书私钥文件
- `cloud.tencent.com._encrypt_bundle.pem` (可忽略该文件)

○ CSR 文件内容:

- `cloud.tencent.com._sign.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。

2. 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 上传文件操作请参见 [通过 WinSCP 上传文件到 Linux 云服务器](#)。
- 若您需部署到腾讯云服务器, 建议使用云服务器的文件上传功能。详情请参见 [上传文件到云服务器](#)。

3. 进入 `/usr/local/nginx/conf` 目录, 新建 `cert` 目录。

```
cd /usr/local/nginx/conf/  
mkdir cert
```

将已获取到的 `cloud.tencent.com.key` 私钥文件、`cloud.tencent.com._sign_bundle.crt` 签名证书文件、`cloud.tencent.com._sign.key` 签名证书私钥文件、`cloud.tencent.com._encrypt_bundle.crt` 加密证书文件、`cloud.tencent.com._encrypt.key` 加密证书私钥文件从本地目录拷贝到 Nginx 服务器的 `/usr/local/nginx/conf/cert` 目录下。

4. 进入 `/usr/local/nginx/conf` 目录, 编辑 `nginx.conf` 文件, 添加如下配置:

```
server  
{  
    listen 443 ssl;  
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;  
    # 国密算法加密套件  
    ssl_ciphers ECC-SM4-GCM-SM3:ECC-SM4-CBC-SM3:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA:DES-CBC3-SHA;  
    ssl_verify_client off;  
    # 签名证书/私钥  
    ssl_certificate /usr/local/nginx/conf/cert/cloud.tencent.com._sign_bundle.crt;  
    ssl_certificate_key /usr/local/nginx/conf/cert/cloud.tencent.com._sign.key;  
    # 加密证书/私钥  
    ssl_certificate /usr/local/nginx/conf/cert/cloud.tencent.com._encrypt_bundle.crt;  
    ssl_certificate_key /usr/local/nginx/conf/cert/cloud.tencent.com._encrypt.key;  
    location /  
    {  
        root html;  
        index index.html index.htm;  
    }  
}
```

5. 配置国密 license 许可。

请在 [SSL 证书控制台](#) 国密 DNSPod 证书详情页下载国密 license 文件 (文件名: `gmssl_XXXX.lic`) 到本地目录, 并将其上传到 Nginx 服务器的 `/etc` 目录下。

6. 您可通过执行以下命令验证配置文件问题。

```
/usr/local/nginx/sbin/nginx -t
```

- 若提示 test is successful，则表示配置正常，可以启动 Nginx 服务。
- 若提示 test failed，请您重新配置或者根据提示修改存在问题。
- test is successful

7. 执行以下命令启动 Nginx 服务，即可使用 `https://cloud.tencent.com` 进行访问。

```
cd /usr/local/nginx/sbin  
./nginx
```

- 如果浏览器地址栏显示安全锁标识，则说明证书安装成功。如下图所示：



- 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](#)

国际标准证书与国密标准证书双安装（可选）

若您需要通过国际标准证书与国密标准证书双证书安装的方式解决浏览器兼容性问题。您可以通过以下操作设置：

① 说明：

腾讯云提供免费的 DV 型 SSL 证书以供购买了国密标准 DNSPod 证书的用户顺利解决浏览器兼容问题。申请证书请查看 [域名型（DV）免费 SSL 证书](#)。

1. 使用 WinSCP（即本地与远程计算机间的复制文件工具），将已获取到的国际标准证书中的 `1_root_bundle.crt` 证书文件、`2_cloud.tencent.com.crt` 证书文件以及 `3_cloud.tencent.com.key` 私钥文件从本地目录拷贝到 Nginx 服务器的 `/usr/local/nginx/conf/cert` 目录下。

① 说明：

- WinSCP 上传文件操作请参见 [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。详情请参见 [上传文件到云服务器](#)。

2. 编辑 `/usr/local/nginx/conf/` 目录下的 `nginx.conf` 文件，并添加如下内容：

```
SSLCertificateFile /usr/local/nginx/conf/cert/2_cloud.tencent.com.crt  
SSLCertificateKeyFile /usr/local/nginx/conf/cert/3_cloud.tencent.com.key  
SSLCertificateChainFile /usr/local/nginx/conf/cert/1_root_bundle.crt
```

3. 您通过执行以下命令验证配置文件问题。

```
/usr/local/nginx/sbin/nginx -t
```

- 若提示 test is successful，则表示配置正常，可以启动 Nginx 服务。
- 若提示 test failed，请您重新配置或者根据提示修改存在问题。

4. 重新加载 Nginx 服务配置，即可解决浏览器兼容问题。

```
/usr/local/nginx/sbin/nginx -s reload
```

Apache 服务器国密 SSL 证书安装部署（DNSPod）

最近更新时间：2024-12-06 14:39:23

操作场景

本文档指导您如何在 Apache 服务器中安装国密标准 DNSPod SSL 证书。

说明：

- 国密标准 DNSPod SSL 证书目前仅支持 Linux 环境下 Apache 服务器。
- 本文档以证书名称 cloud.tencent.com 为例。
- Apache 版本建议使用版本 apache-2.4.46 或 apache-2.4.48，您可前往 [Apache 官网](#) 进行下载或 [单击此处](#) 快速下载 apache-2.4.48。
- 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，具体请参见 [服务器如何开启443端口？](#)
- SSL 证书文件上传至服务器方法请参见 [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）。
若您需部署到腾讯云服务器，建议使用云服务器的文件上传功能，详情请参见 [上传文件到云服务器](#)。
- 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）。
- 已购买国密标准（SM2）DNSPod SSL 证书。

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

说明：

操作过程如果出现问题，请您 [联系我们](#)。

环境配置

说明：

- 国密标准 DNSPod SSL 证书安装在 Apache 服务器上，Apache 服务器需具备相关环境支持模块。下文将指导您编译配置支持国密标准 DNSPod SSL 证书的 Apache 服务器。
- 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。

- 远程登录 Apache 服务器。例如，使用 [PuTTY 工具](#) 登录。
- 安装编译依赖包：如果您的系统是全新的，请先在服务器上安装以下依赖包，为编译提供环境支持。您可以使用如下命令进行安装。

```
yum install -y gcc gcc-c++ wget make perl pcre-devel expat-devel bison bison-devel flex flex-devel
```

3. 下载并编译安装 apr（以 apr 1.7.5 版本为例），您可以通过在服务器上输入以下命令，下载 apr 至服务器并编译安装，由于操作系统的版本不同，详细操作步骤略有区别。

```
# 切换至 /usr/local/ 目录下
cd /usr/local/
# 下载 apr 1.7.5
wget -c http://mirrors.tencent.com/apache/apr/apr-1.7.5.tar.gz
# 解压已下载的 apr 1.7.5 压缩包
tar -zxvf apr-1.7.5.tar.gz
# 进入解压后的 apr 1.7.5 文件夹并指定编译目录路径。
cd apr-1.7.5/
./configure --prefix=/usr/local/apr
# 编译安装 apr
make && make install
```

4. 下载并编译安装 apr-util（以 apr-util-1.6 版本为例）。

```
# 切换至 /usr/local/ 目录下
cd /usr/local/
# 下载 apr-util-1.6.1
wget -c http://archive.apache.org/dist/apr/apr-util-1.6.1.tar.gz
# 解压已下载的 apr-util-1.6.1 压缩包
tar -zxvf apr-util-1.6.1.tar.gz
# 进入解压后的 apr-util-1.6.1 文件夹并指定编译目录路径。
cd /usr/local/apr-util-1.6.1/
./configure --prefix=/usr/local/apr-util --with-apr=/usr/local/apr
# 编译安装 apr-util
make && make install
```

5. Apache 服务安装：上述步骤编译安装完成后，请下载 Apache 国密版和国密模块至 `/usr/local` 目录下进行编译安装。

① 说明：

DNSPod 国密模块文件名 `gmssl_openssl_2021.1011.tar.gz` 在解压与安装中请勿修改，否则可能会导致安装错误。

如果在安装 Apache 的过程中找不到 `pcre`、`apr-util` 或 `apr` 等相关文件，请将 `/pcre/bin`、`/apr-util/bin` 或 `/apr/bin` 等文件加入系统路径。

```
# 切换至 /usr/local/ 目录下
cd /usr/local/
# 下载 Apache httpd-2.4.62 压缩包
wget -c http://mirrors.tencent.com/apache/httpd/httpd-2.4.62.tar.gz
# 下载 DNSPod 国密模块
wget -c https://certificate-1258344699.cos.ap-guangzhou.myqcloud.com/public/gmssl_openssl_2021.1011.tar.gz
# 解压已下载的 gmssl_openssl_2021.1011 压缩包
tar -zxvf gmssl_openssl_2021.1011.tar.gz
# 解压已下载的 httpd-2.4.62 压缩包
tar -zxvf httpd-2.4.62.tar.gz
# 进入解压后的 httpd-2.4.62 文件夹并指定编译目录路径。
cd httpd-2.4.62/
./configure --prefix=/usr/local/httpd --enable-so --enable-ssl --enable-cgi --enable-rewrite --enable-modules=most --enable-mpms-shared=all --with-mpm=prefork --with-zlib --with-apr=/usr/local/apr --with-apr-util=/usr/local/apr-util --with-ssl=/usr/local/gmssl LDFLAGS=-lm
```

```
# 编辑 build/config_vars.mk, 修改 ssl 为静态链接
vi build/config_vars.mk
找到 ab_LIBS = -lssl -lcrypto -lrt -lcrypt -lpthread -ldl
替换为: ab_LIBS = /usr/local/gmssl/lib/libssl.a /usr/local/gmssl/lib/libcrypto.a -lssl -lcrypto -lrt
-lcrypt -lpthread -ldl
# 编译安装 Apache
make install
```

国密标准证书安装

1. 已在 [SSL 证书控制台](#) 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 Apache 文件夹和 CSR 文件:

- 文件夹名称: cloud.tencent.com_apache
- 文件夹内容:
 - cloud.tencent.com.key 私钥文件
 - cloud.tencent.com._encrypt.crt 加密证书文件
 - cloud.tencent.com._encrypt.key 加密证书私钥文件
 - root_encrypt_bundle.crt 加密证书链文件
 - cloud.tencent.com._sign.crt 签名证书文件
 - cloud.tencent.com._sign.key 签名证书私钥文件
 - root_sign_bundle.crt 签名证书链文件
- CSR 文件内容:
 - cloud.tencent.com._sign.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。

2. 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 上传文件操作请参见 [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, 详情请参见 [上传文件到云服务器](#)。

3. 进入 /usr/local/httpd/conf 目录, 新建 cert 目录。

```
cd /usr/local/httpd/conf/
mkdir cert
```

将已获取到的 cloud.tencent.com.key 私钥文件、cloud.tencent.com._encrypt.crt 加密证书文件、cloud.tencent.com._encrypt.key 加密证书私钥文件、root_encrypt_bundle.crt 加密证书链文件、cloud.tencent.com._sign.crt 签名证书文件、cloud.tencent.com._sign.key 签名证书私钥文件、root_sign_bundle.crt 签名证书链文件从本地目录拷贝到 Apache 服务器的 /usr/local/httpd/conf/cert 目录下。

4. 进入 /usr/local/httpd/conf 目录, 按照以下步骤编辑 httpd.conf 文件:

- 4.1 请在 #ServerName www.example.com:80 下增加 ServerName (您的域名):80 。
- 4.2 请去掉 LoadModule ssl_module modules/mod_ssl.so 前的 # 。
- 4.3 请去掉 Include conf/extra/httpd-ssl.conf 前的 # 。

5. 编辑 /usr/local/httpd/conf/extra/httpd-ssl.conf 文件, 进行以下修改:

```
# 编辑文件
vi /usr/local/httpd/conf/extra/httpd-ssl.conf
```

5.1 注释掉所有带 `SSLSessionCache` 的配置行，即在前面加上 `#`。

5.2 注释掉默认证书和key，即在前面加上 `#`，参考如下：

```
# SSLCertificateFile "/usr/local/httpd/conf/server.crt"
# SSLCertificateKeyFile "/usr/local/httpd/conf/server.key"
```

5.3 文件中添加以下配置内容：

```
# 配置算法
SSLCipherSuite HIGH:ECC-SM4-SM3:ECDHE-SM4-SM3
# 签名证书/私钥/证书链
SSLCertificateFile "/usr/local/httpd/conf/cert/cloud.tencent.com._sign.crt"
SSLCertificateKeyFile "/usr/local/httpd/conf/cert/cloud.tencent.com._sign.key"
SSLCertificateChainFile "/usr/local/httpd/conf/cert/root_sign_bundle.crt"
# 加密证书/私钥/证书链
SSLCertificateFile "/usr/local/httpd/conf/cert/cloud.tencent.com._encrypt.crt"
SSLCertificateKeyFile "/usr/local/httpd/conf/cert/cloud.tencent.com._encrypt.key"
SSLCertificateChainFile "/usr/local/httpd/conf/cert/root_encrypt_bundle.crt"
```

6. 配置国密 license 许可：

请在 [SSL 证书控制台](#) 国密 DNSPod 证书详情页下载国密 license 文件（文件名：`gmssl_XXXX.lic`）到本地目录，并将其上传到 Apache 服务器的 `/etc` 目录下。

7. 您可通过执行以下命令验证配置文件问题。

```
/usr/local/httpd/bin/httpd -t
```

- 若提示 Syntax OK，则表示配置正常，可以启动 Apache 服务。
- 若提示非 Syntax OK，请您重新配置或者根据提示修改存在问题。

8. 执行以下命令启动 Apache 服务，即可使用 `https://cloud.tencent.com` 进行访问。

```
/usr/local/httpd/bin/httpd -k start
```

- 如果浏览器地址栏显示安全锁标识，则说明证书安装成功。如下图所示：



- 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](#)

国际标准证书与国密标准证书双安装（可选）

若您需要通过国际标准证书与国密标准证书双证书安装的方式解决浏览器兼容性问题。您可以通过以下操作设置：

❗ 说明：

腾讯云提供免费的 DV 型 SSL 证书以供购买了国密标准 DNSPod 证书的用户顺利解决浏览器兼容问题。申请证书请参见 [域名型（DV）免费 SSL 证书](#)。

1. 使用 “WinSCP”（即本地与远程计算机间的复制文件工具），将已获取到的国际标准证书中的 `1_root_bundle.crt` 证书文件、`2_cloud.tencent.com.crt` 证书文件以及 `3_cloud.tencent.com.key` 私钥文件从本地目录拷贝到 Apache 服务器的 `/usr/local/httpd/conf/cert` 目录下。

- **说明：**
 - WinSCP 上传文件操作请参见 [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。详情请参见 [上传文件到云服务器](#)。

2. 编辑 `/usr/local/httpd/conf/extra/` 目录下的 `httpd-ssl.conf` 文件，并添加如下内容：

```
SSLCertificateFile /usr/local/httpd/conf/cert/2_cloud.tencent.com.crt
SSLCertificateKeyFile /usr/local/httpd/conf/cert/3_cloud.tencent.com.key
SSLCertificateChainFile /usr/local/httpd/conf/cert/1_root_bundle.crt
```

3. 您通过执行以下命令验证配置文件问题。

```
/usr/local/httpd/bin/httpd -t
```

- 若提示 Syntax OK，则表示配置正常，可以启动 Apache 服务器。
- 若提示非 Syntax OK，请您重新配置或者根据提示修改存在问题。

4. 重新启动 Apache 服务，即可解决浏览器兼容问题。

```
/usr/local/httpd/bin/httpd -k restart
```

一键 HTTPS

最近更新时间：2024-10-29 16:20:02

概述

一键 HTTPS 是 SSL 证书结合腾讯云 Web 应用防火墙（WAF）服务开发的快速部署 HTTPS 功能，帮助用户网站的 HTTPS 访问升级。

使用该功能，您无需进行繁琐的 SSL 证书部署操作，仅需配置一个 CNAME 解析，即可实现从 HTTP 到 HTTPS 的能力升级。

本文将指导您如何在 [SSL 证书控制台](#) 一键添加 WAF 接入域名并配置 HTTPS。

⚠ 注意：

一键 HTTPS 套餐到期后，如您需继续使用，可进行续费升级操作，如不再使用，避免影响您的访问，需修改您配置的 CNAME 记录。具体操作请查看 [一键 HTTPS 套餐即将到期如何处理？](#)

一键 HTTPS 与传统服务器部署 SSL 证书的区别

- 传统服务器部署 SSL 证书除了需具备基础技术知识的同时，整个部署过程中您还需要输入一系列操作命令和编辑相关配置文件，整个过程的繁琐性不仅增加了维护成本，同时也容易出现操作性事故，造成不可挽回的损失。如下图所示：

下载 SSL 证书 → 登录服务器 → 上传 SSL 证书 → 配置 Web 服务 → 重启 Web 服务

- 一键 HTTPS 是结合腾讯云 Web 应用防火墙（WAF）服务开发的快速部署 HTTPS 功能，整个部署过程相对传统服务器部署要简单易操作，仅需配置一个 CNAME 解析，即可实现从 HTTP 到 HTTPS 的能力升级。不仅能够降低维护成本，简单的配置方式也可降低操作性事故发生的可能性。如下图所示：

添加域名 → 配置 CNAME 记录 → 等待解析生效

前提条件

已在 [证书管理控制台](#) 申请颁发 SSL 证书。

限制说明

- SSL 证书默认开通 WAF 小微版。支持1个二级域名、8个子域名、50 QPS。

⚠ 注意：

www 子域名占用一个子域名名额，例如 `www.tencent.com`。

- 若您一键 HTTPS 域名已使用腾讯云 CDN 或 CLB，则无法使用一键 HTTPS 功能。

操作指南

步骤1：添加一键 HTTPS 域名

- 登录证书管理控制台，并单击左侧菜单栏 [一键 HTTPS](#)，进入一键 HTTPS 管理页面。
- 在一键 HTTPS 管理页面中，单击[一键添加](#)。如下图所示：

📌 说明：

如果您是首次使用，请单击[前往选购](#)，购买后即可使用。

一键HTTPS

套餐
小微版

峰值QPS ①
0 [查看详情](#)

网站QPS阈值
50
2022-06-01 00:00:00截止

一键添加

搜索证书ID或者域名

域名	证书ID	cname	接入状态	证书到期时间	操作
暂无数据					

3. 在弹出的“一键添加”窗口中，配置相关信息。如下图所示：

一键添加

×

填写域名

由于Web应用防火墙限制，未在腾讯云侧备案的域名无法使用一键HTTPS服务，请广大用户感知。

选择证书

.cn (0(DR)

源站地址
☒ IP ☐ 域名

请输入源站IPv4或v6地址，用回车分隔多个IP，最多支持输入20个

请输入您的公网IP，一般是您的服务器IP地址。

强制HTTPS
☒

浏览器

腾讯云

源站

http → 302 → https

开启该功能，浏览器端的每个HTTP请求都会被转换成HTTPS请求。

回源协议
☒ HTTP

浏览器

腾讯云

源站

http/https → http

腾讯云将使用您选择的协议访问源站。

回源端口
☒ 80 ☐ 8080
注意：HTTP回源端口仅支持80/8080两个端口，请确保与源站端口一致，且源站端口处于开放状态。

高级选项 ▶

确定

取消

- **填写域名：**请输入您需要进行一键 HTTPS 的域名。

① 说明：

填写的域名需要在腾讯云完成备案，否则将无法正常进行接入。您可根据 [腾讯云可备案类型](#) 进行备案。

- **选择证书：**请选择已成功申请的证书。

① 说明：

选择的证书需与填写域名输入框填写的域名对应。例如，填写的域名为 `cloud.tencent.com`，则选择绑定域名为 `cloud.tencent.com` 的证书。

- **源站地址**：请根据您的实际需求选择 **IP 与域名**。
 - **IP**：请输入需要防护网站的真实 IP 源站地址，即源站的公网 IP 地址。
 - **域名**：请输入需要防护网站的真实源站域名。
- **强制 HTTPS**：开启该功能，浏览器端的每个 HTTP 请求都会被跳转成 HTTPS 请求。例如，当浏览器使用 HTTP 协议访问 `http://cloud.tencent.com` 时，将返回302状态码重定向到 HTTPS 协议访问 `https://cloud.tencent.com`。
- **回源协议**：开启该功能，腾讯云将使用 HTTP 协议访问源站。
- **回源端口**：请根据您的实际需求选择回源端口。默认情况下支持80或8080端口。
- **高级选项（可选）**：

高级选项 ▼

回源连接方式 ☐ 短连接 ☒ 长连接
默认使用长连接回源，请确认源站是否支持长连接，若不支持，即使设置长连接，也会使用短连接回源。

开启HTTP2.0 ☒ 否 ☐ 是
若您的源站不支持HTTP2.0，从腾讯云到源站链路将降级为HTTP1.1。

开启WebSocket ☒ 否 ☐ 是
如果您的网站使用了Websocket，建议您选择是。

- **回源连接方式**：默认使用长连接回源，请确认源站是否支持长连接，若不支持，即使设置长连接，也会使用短连接回源。
- **开启 HTTP2.0**：若您的源站不支持 HTTP2.0，从腾讯云到源站链路将降级为 HTTP1.1。源站支持 HTTP2.0 情况下建议您选择开启 HTTP2.0，将提高您网站的访问速率。
- **开启 WebSocket**：若您的网站使用了 WebSocket 建议您选择开启 WebSocket，将提高轮询的效率以及降低资源浪费。

4. 单击**确定**，即可生成配置实例。如下图所示：

域名	证书ID	cname	接入状态	证书到期时间	操作
example.com	12345678	d75t...gj.com	异常①	2022-06-27 07:59:59	编辑 删除

步骤2：配置 CNAME 记录

① 说明：

- 添加一键 HTTPS 域名后，还需配置对应的 CNAME 记录后，接入才可正常生效。CNAME 记录可查看 [什么是 CNAME 记录？](#)
- 配置 CNAME 记录步骤以腾讯云配置 CNAME 记录为例，若您的一键 HTTPS 域名解析未在 DNSPod DNS 解析托管，具体操作请咨询您的域名解析商或将域名托管至 DNSPod DNS 解析后，再进行配置 CNAME 记录。详情请参见 [域名托管至 DNSPod DNS 解析](#)。
- 若您需进一步了解 DNS 知识，详情请参考：[云解析 DNS](#)。

一键添加 CNAME 记录

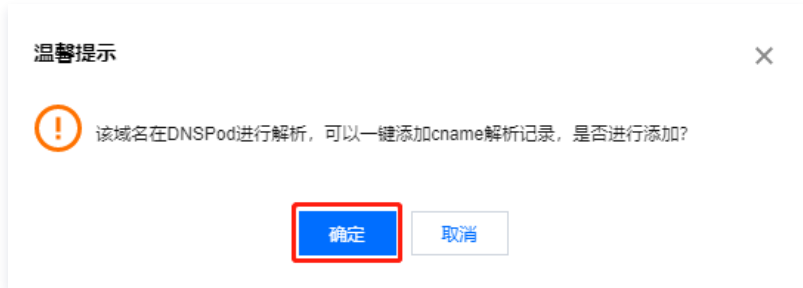
① 说明：

若您的域名解析已在 DNSPod DNS 解析进行托管，可直接一键添加 CNAME 记录。

1. 在 "一键 HTTPS" 管理页面，查看您需要配置 CNAME 记录的实例，单击 。如下图所示：

域名	证书ID	cname	接入状态	证书到期时间	操作
study.com	12345678	60cdf...gj.com	异常①	2022-07-05 07:59:59	编辑 删除

2. 在弹出的“温馨提示”窗口中，单击**确定**，即可添加记录，如下图所示：



手动添加 CNAME 记录

1. 登录 [DNSPod 管理控制台](#)。

2. 在“我的域名”中，选择需要配置记录的一键 HTTPS 域名，单击域名名称，即可进入该域名的记录管理页面。如下图所示：



3. 单击**添加记录**，填写记录信息。如下图所示：



- **主机记录**：填写子域名。例如，添加 `cs.dnspod.com` 的一键 HTTPS 域名，您在“主机记录”处填写“cs”即可。
- **记录类型**：选择“CNAME”。
- **线路类型**：选择“默认”类型，否则会导致部分用户无法解析。
- **记录值**：填写证书控制台新增实例提供的 CNAME 域名。如下图所示：



- **权重**：同一条主机记录相同的线路，可以针对不同的记录值设置权重，解析时将根据设置的权重比例进行返回。输入范围为0 - 100的整数。
- **MX 优先级**：不需要填写。
- **TTL**：为缓存时间，数值越小，修改记录各地生效时间越快，默认为600秒。

4. 单击**确定**，即可添加记录。

5. 完成添加后，请耐心等待解析生效，解析生效后即可接入成功。

说明：
一般情况下，解析生效时间与您设置 TTL 值相同。

说明：
防护配置是对 WAF 防护进行策略调整，如需进行防护配置，请参考 [Web 应用防火墙产品文档](#) 进行设置。

常见问题

最近更新时间：2024-12-26 16:26:12

证书安装过程可能遇到的问题，具体问题参考如下：

- [服务器如何开启443端口？](#)
- [访问站点提示连接不安全？](#)
- [如何设置 SSL 证书的 TLS 协议版本？](#)
- [苹果 ATS 证书如何配置？](#)