SSL 证书

常见问题

产品文档

腾讯云

文档目录

常见问题
选择 SSL 证书相关
如何选择 SSL 证书？
SSL 证书支持绑定 IP 的证书有哪些？
未开启网站服务前是否可以申请 SSL 证书？
CAA 记录说明
SSL 证书申请相关
免费 SSL 证书名额相关问题
如何填写 SSL 证书申请中的绑定域名？
泛域名 SSL 证书相关问题
为什么收到 CA 机构的通知，但订单状态没有变化？
SSL 证书配置的 TXT 解析是否可以删除？
什么是CSR？
如何制作 CSR 文件？
什么是私钥密码？
忘记私钥密码怎么办？
SSL 证书是否支持吊销？
RSA 加密算法与 ECC 加密算法的区别？
提交 SSL 证书吊销申请时，控制台提示 “证书已关联云资源，无法吊销” 怎么办？
重颁发证书与重新申请证书的区别？
哪些 SSL 证书类型支持小程序？
SSL 证书管理相关
一键 HTTPS 套餐即将到期如何处理？
我的资料相关
如何查看证书信息？
SSL 证书安装相关
IIS 下设置 https 主机名灰色无法编辑怎么办？
服务器如何开启443端口？
访问站点提示连接不安全？
如何安装 OpenSSL？
如何设置 SSL 证书的 TLS 协议版本？
如何补全 SSL 证书链？
腾讯云申请的 SSL 证书能用于 websocket 吗？
如何开启 IIS 服务？
SSL 证书过期后重新申请部署依然提示 HTTPS 不安全？

SSL 证书地域相关
SSL 证书安装存在地域限制吗？
SSL 证书审核相关
SSL 证书提交资料审核时长？
申请 SSL 证书审核失败的原因及处理方法
已购 SSL 证书提交申请审核后需要做什么？
如何查看域名型（DV）SSL 证书域名验证结果？
SSL 证书生效相关
服务器 IP 地址更换后原来的 SSL 证书能否生效？
如何在浏览器中检查 SSL 证书是否生效？
GlobalSign 证书 Windows 7 系统下不受信任怎么办？
免费 SSL 证书颁发时间过长或颁发失败排查方案
SSL 证书收费和购买相关
域名型（DV）SSL 证书是否永久免费？
SSL 证书有效期相关
SSL 证书快过期了怎么办？
SSL 证书过期后未及时更新有哪些影响？
查看 SSL 证书到期相关问题
SSL 证书成功续费后可以继续服务吗？

常见问题
选择 SSL 证书相关
如何选择 SSL 证书？

最近更新时间：2024-03-06 17:58:12

如何选择证书种类？

如果您的网站主体是个人（即没有企业营业执照），只能申请域名型（DV）免费证书或域名型（DV）付费证书。
对于金融、支付类企业，建议购买 EV 型证书。
对于一般企业，建议购买 OV 型及以上类型的 SSL 证书。
若作为移动端网站或接口调用，也建议您购买 OV 型及以上类型的 SSL 证书。

如何选择证书品牌？

您可以根据各 SSL 证书品牌浏览器兼容性测试报告以及企业的业务情况进行购买。
具体请查看 浏览器兼容性测试报告。

如何选择支持域名数量？

腾讯云提供以下四种域名类型，具体区别请查看如下内容：
单域名：只支持绑定1个域名，可以是二级域名 `tencent.com`，也可以是三级域名 `example.tencent.com`，均可以支持，**但不支持二级域名下的所有子域名**。域名级数最多可以支持100级。
多域名：单个证书可以绑定多个域名，最多可以支持域名数量以官网售卖为准。
泛域名：支持绑定一个且只有一个泛域名，泛域名只允许添加一个通配符，例如 `*.tencent.com`、`*.example.tencent.com`，最多支持100级；`*.*.tencent.com` 多个通配符的泛域名是不支持的。
通配符多域名：支持绑定多个泛域名，泛域名只允许添加一个通配符，例如 `*.tencent.com`、`*.example.tencent.com`，最多支持100级；`*.*.tencent.com` 多个通配符的泛域名是不支持的。

SSL 证书支持绑定 IP 的证书有哪些？

最近更新时间：2024-03-06 17:58:12

支持绑定 IP 的证书品牌与类型有那些？

腾讯云支持绑定 IP 的 SSL 证书请参考下表：

证书品牌	企业型（OV）	企业型专业版（OV Pro）	域名型（DV）	域名型免费版（DV）	增强型（EV）	增强型专业版（EV Pro）
SecureSite	不支持	不支持	不支持	不支持	不支持	不支持
GeoTrust	不支持	-	-	-	不支持	-
TrustAsia	支持	-	不支持	-	不支持	-
GlobalSign	不支持	-	-	-	不支持	-

未开启网站服务前是否可以申请 SSL 证书？

最近更新时间：2024-03-06 17:58:12

未开启网站服务前是否可以申请 SSL 证书？

已拥有域名并且具有解析权限，即可申请 SSL 证书（付费证书与免费证书都可申请）。

注意：

如果您申请证书时还未购买云服务资源，证书验证时将不支持文件验证的方式。

CAA 记录说明

最近更新时间：2024-03-06 17:58:12

什么是 CAA？

CAA（Certification Authority Authorization，证书颁发机构授权）是一项降低 SSL 证书错误颁发的控制措施，由互联网工程任务组（IETF）批准列为 IETF RFC6844 规范。2017年3月，CA 浏览器（CA/Browser Forum）论坛投票通过187号提案，要求 CA 机构从2017年9月8日起执行 CAA 强制性检查。

CAA 如何执行？

域名所有者通过设置 CAA 解析记录来授权指定的 CA 机构为其颁发 SSL 证书，同时 CA 机构根据规范要求，在颁发 SSL 证书时会强制性检查域名 CAA 记录，如果检查发现未获得授权，将拒绝为该域名颁发 SSL 证书，从而防止未授权的 SSL 证书错误颁发，规避安全风险。

说明：

若域名未设置 CAA 记录，那么任何 CA 机构都可以为该域名颁发 SSL 证书。

若您的域名在 DNSPod 进行托管，具体操作请参见 CAA 记录。

若申请域名添加了非腾讯云 CA 机构的 CAA 记录，将无法正常颁发，进行域名验证前，请先检查是否添加了 CAA 记录。若已添加，请删除后再进行域名验证。

SSL 证书申请相关
免费 SSL 证书名额相关问题

最近更新时间：2024-03-06 18:00:08

在腾讯云可以申请多少张免费证书？

申请类别	数量
同一腾讯云主账号	至多20张
同一主域	至多20张

一个腾讯云主账号至多可申请20张免费证书。
同一主域名下至多只能申请20张亚洲诚信品牌免费型 DV 版 SSL 证书。
注意：
二级域名及其子域名均属于同一主域，例如，`tencent.com`、`ssl.tencent.com`、`ssl.ssl.tencent.com` 都属于同一主域。
在其他平台申请过同一主域的亚洲诚信品牌免费型 DV 版 SSL 证书也将占用同一主域的20张免费名额。

如何释放腾讯云主账号的免费证书额度？

免费证书吊销或证书正常到期后，会立即释放已占用的腾讯云主账号的免费证书额度。

如何释放同一主域名的免费证书额度？

免费证书正常到期后才会立即释放已占用的主域名额度；吊销或删除证书并不会释放额度。

免费证书免费名额与腾讯云免费证书扩容包抵扣顺序？

申请免费时优先使用免费名额进行抵扣顺序，超出额度时将使用免费证书扩容包进行抵扣。

如何填写 SSL 证书申请中的绑定域名？

最近更新时间：2024-03-06 18:00:08

如何填写证书申请中的绑定域名？

当完成 SSL 证书购买后，您需要在 腾讯云证书管理控制台 提交证书申请的审核资料。证书管理控制台将会根据您购买的证书提示您需要输入的域名类型和数量。

说明：

SSL 证书目前暂不支持绑定到后缀为 **.ru** 的域名。

需正确填写证书绑定的域名信息，才可保证您的 SSL 证书顺利颁发并正常使用 HTTPS 服务。

部分证书可以绑定 IP，具体可查看 支持绑定 IP 的 SSL 证书说明。

腾讯云 SSL 证书服务，将会根据您购买的品牌和申请时填写的绑定域名，为您赠送相对的上级域，详情如下表：

证书类型 赠送规则	GlobalSign	TrustAsia（OV/EV）	TrustAsia (DV)	GeoTrust
绑定域名不带 www. 开头，赠送 www. 子域	不赠送	绑定域名为主域时赠送 www. 子域	绑定域名为主域时赠送 www. 子域	绑定域名为主域时赠送 www. 子域
绑定普通域名和通配符泛域名，赠送上级域	赠送	赠送	赠送	赠送

说明：

您绑定域名为主域时，部分品牌可赠送 www. 子域，如绑定域名为 `tencent.com`，则可赠送 `www.tencent.com`。

您绑定普通域名和通配符泛域名时，部分品牌可赠送相对的上级域，如绑定域名为 `*.tencent.com`，则可赠送 `tencent.com`。

普通域名以及通配符泛域名需为三级域名及以上，才可赠送上级域。

什么是泛域名？

带通配符的域名，例如：`*.tencent.com`、`*.cloud.tencent.com` 均为泛域名，包含同一级的全部子域名。

注意：

域名不支持跨级，例如 `*.tencent.com` 不包含 `*.cloud.tencent.com` 下一层级域名。

泛域名 SSL 证书相关问题

最近更新时间：2024-03-06 18:00:08

泛域名证书都支持哪些域名？

腾讯云 SSL 证书支持泛域名证书，您可以通过泛域名证书保护服务器的单个主域名和该主域名下同级别的所有子域名。
泛域名证书包含同一级的全部子域名。例如：`*.tencent.com`、`*.cloud.tencent.com` 均为泛域名。
泛域名证书目前仅支持通配符类型的域名、不支持普通域名（非通配符域名）。如需一张证书能包含多个通配符域名，建议购买通配符多域名类型 SSL 证书。

泛域名证书匹配域名的规则是什么？

泛域名证书只能匹配同级别的子域名，不能跨级匹配。例如，三级泛域名 `*.tencent.com` 不支持四级域名 `www.ssl.tencent.com`。

申请泛域名证书时，为什么不能使用文件验证？

自2021年12月01日起，使用文件验证的域名，只能为当前被验证的域名签发 SSL 证书，不支持签发通配符 SSL 证书和其下级子域名 SSL 证书。详情请查看 SSL 证书域名验证策略变更通知。

为什么收到 CA 机构的通知，但订单状态没有变化？

最近更新时间：2024-03-06 18:00:08

为什么收到 CA 机构的通知，但订单状态没有变化？

在资料审核环节和证书颁发环节，CA 机构可能会发送一封邮件通知您申请证书的进展。如果您发现腾讯云 SSL 证书控制台中的订单状态还没有发生变化，这是由于 CA 机构给腾讯云推送的订单状态会有延迟，建议您耐心等待一段时间才能看到订单的状态变化。

SSL 证书配置的 TXT 解析是否可以删除？

最近更新时间：2024-03-06 18:00:08

证书配置的 TXT 解析是否可以删除？

证书颁发完成后，您可以删除证书配置的 TXT 解析，对证书无影响。

什么是CSR？

最近更新时间：2024-03-06 18:00:08

什么是 CSR？

CSR 即证书签名申请（Certificate Signing Request），获取 SSL 证书，需要先生成 CSR 文件并提交给证书颁发机构（CA）。CSR 包含了公钥和标识名称（Distinguished Name），通常从 Web 服务器生成 CSR，同时创建加解密的公钥私钥对。

在创建 CSR 过程中，需要提供相关组织机构信息，web 服务器会根据提供的信息创建证书的标识名称，用来识别证书，内容如下：

国家或地区代码

您的组织机构依法注册所在的国家或地区的代码，以国际标准化组织（ISO）的两字母格式表示。

省或市或自治区

您的组织机构所在的省或市或自治区。

城市或地区

您的组织机构注册所在的城市或地区。

组织机构

您的企业依法注册所用的名称。

组织机构单位

此字段用于区分组织机构中的各部门，例如 “工程部” 或 “人力资源部”。

通用名称

在 CSR 的通用名称字段中输入的名称必须是您要为其使用证书的网站的完全限定域名（FQDN），例如 “www.domainnamegoeshere”。

但是腾讯云采用了在线生成 CSR 的方式，无需您生成和提交 CSR 文件，域名型证书仅需要提交通用名称即可申请，帮助您简化申请流程。

如何制作 CSR 文件？

最近更新时间：2024-03-06 18:00:08

如何制作 CSR 文件？

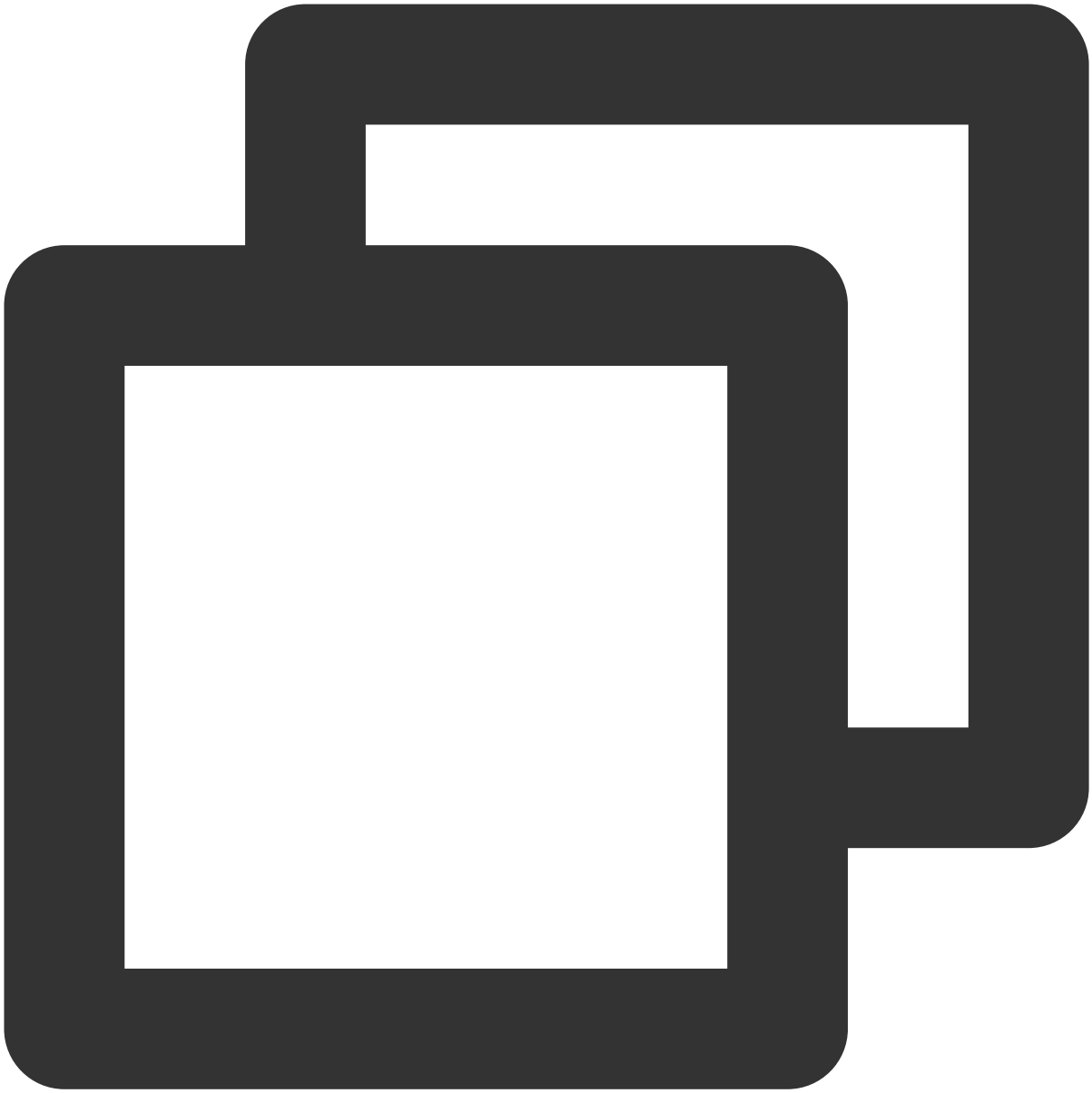
本文档指导您如何制作 CSR（Certificate Signing Request）文件。

前提条件

申请数字证书之前，您需要准备生成证书的密钥文件和 CSR 文件。CSR 文件是您的公钥证书原始文件，包含了您的服务器信息和您的单位信息，需要提交给 CA 认证中心进行审核。建议您使用系统创建的 CSR 文件，避免出现输入信息错误而导致审核失败。若您选择手动生成 CSR 文件，请务必妥善保管并备份您的密钥文件，手动生成 CSR 文件时需要注意以下信息：
输入的中文信息需要使用 UTF-8 编码格式，请在编辑 OpenSSL 工具时，指定支持 UTF-8 编码格式。
证书服务系统对 CSR 文件的密钥长度有严格要求，密钥长度必须是 2048bit，密钥类型必须是 RSA。
如果申请证书是多域名或者通配子域名，在 Common Name 或 What is your first and last name? 区域只需要输入一个域名。

使用 OpenSSL 工具生成 CSR 文件

1. 登录运行 Linux 系统的一台本地计算机或服务器。
2. 安装 OpenSSL 工具，详情可参考 如何安装 OpenSSL？
3. 执行以下命令，即可生成 CSR 文件。



```
openssl req -new -nodes -sha256 -newkey rsa:2048 -keyout [$Key_File] -out [$OpenSSL
```

说明：

new：指定生成一个新的 CSR 文件。

nodes：指定密钥文件不被加密。

sha256：指定摘要算法。

newkey rsa:2048：指定密钥类型和长度。

[$Key_File]：密钥文件名称。

[$OpenSSL_CSR]：加密后文件的存放路径。

4. 根据系统返回的提示，输入生成 CSR 文件所需的信息。以下是关于提示的说明：

Organization Name：公司名称，可以是中文或英文。

Organizational Unit Name：部门名称，可以是中文或英文。

Country Code：申请单位所属国家，只能是两个字母的国家码。例如，中国填写为 CN。

State or Province Name：州名或省份名称，可以是中文或英文。

Locality Name：城市名称，可以是中文或英文。

Common Name：申请 SSL 证书的具体网站域名。

Email Address：可选择不输入。

Challenge Password：可选择不输入。

5. 按照命令提示输入相应内容后，即可在当前目录下获取密钥文件和 CSR 文件。

什么是私钥密码？

最近更新时间：2024-03-06 18:00:08

什么是 SSL 证书私钥密码？

SSL 证书采用公钥加密技术和对称加密技术，对客户端和服务器端之间的数据传输进行加密，确保数据传输的机密性、完整性以及通信方身份真实性。SSL 证书私钥泄露会导致加密会话的密钥泄露，进而造成网站数据泄露风险。SSL 证书私钥密码则是为该私钥再添加一层保护，提高并确保 SSL 证书私钥的安全性。

在您申请腾讯云 SSL 证书时，腾讯云将为您提供私钥密码可选项，若您填写了私钥密码，颁发的 SSL 证书中的私钥文件将使用您填写的私钥密码进行保护。如未填写，腾讯云将为您自动生成私钥密码，私钥密码文件将提供在下载压缩包中。例如 `keystorePass.txt` 文件。

什么情况下会使用私钥密码？

一般情况下，您将 SSL 证书安装部署到 Web 服务中时，将会使用私钥密码。例如，在 Tomcat 服务器中安装部署 SSL 证书时，需填写的 `keystorePass=` 字段即为私钥密码。

关于私钥密码需要注意什么？

在您申请腾讯云 SSL 证书时，若您需自行填写私钥密码，请将私钥设置为复杂的保护密码。

妥善保管您的私钥密码，以免因私钥密码泄漏，影响您的 SSL 证书安全。

牢记私钥密码，腾讯云不会为您保存私钥密码信息。详情请参见 忘记私钥密码怎么办？

忘记私钥密码怎么办？

最近更新时间：2024-03-06 18:00:08

忘记私钥密码怎么办？

腾讯云不会替您保存证书的私钥密码，请牢记私钥密码。

如果遗失私钥密码，您可以通过以下方式进行操作：

重颁发证书：如您的私钥密码丢失，可通过重颁发操作重新生成一个证书。详情请参考 SSL 证书重颁发指引。

说明：

重颁发生成证书后需要重新部署，颁发后有效时长仍为原证书有效时长。

重新申请证书：如您的私钥密码丢失，您可以选择重新申请证书。

申请付费证书请参考 SSL 证书购买流程。

SSL 证书是否支持吊销？

最近更新时间：2024-03-06 18:00:08

证书是否支持吊销？

支持吊销，吊销流程请参考 证书吊销指引。

RSA 加密算法与 ECC 加密算法的区别？

最近更新时间：2024-03-06 18:00:09

RSA 加密算法与 ECC 加密算法的区别？

RSA 加密算法：国际标准算法，应用较早的算法之一，普遍性更强，同比 ECC 算法的适用范围更广，兼容性更好，一般采用2048位的加密长度，服务端性能消耗较高。
ECC 加密算法：椭圆加密算法，新一代算法趋势主流，一般采用256位加密长度（相当于 RSA 3072 位加密强度）更安全，抗攻击型更强，同比 RSA 算法加密速度快，效率更高，服务器资源消耗更低。
您可以通过下表对比项目查看两种加密算法的具体区别：

对比项目	ECC 加密算法	RSA 加密算法
密钥长度	256位	2048位
CPU 占用	较少	较高
内存占用	较少	较高
网络消耗	较少	较高
加密效率	较高	一般
抗攻击性	较强	一般
兼容范围	新版浏览器和操作系统均支持，但存在少数不支持的平台。例如 cPanel	均支持

提交 SSL 证书吊销申请时，控制台提示 “证书已关联云资源，无法吊销” 怎么办？

最近更新时间：2024-03-06 18:00:08

提交 SSL 证书吊销申请时，控制台提示 “证书已关联云资源，无法吊销” 怎么办？

请您检查需要吊销的 SSL 证书是否已绑定腾讯云的云资源，例如 CLB、CDN 等。如已绑定相关资源，请先进行解绑后再进行吊销证书操作。

重颁发证书与重新申请证书的区别？

最近更新时间：2024-03-06 18:00:08

重颁发证书与重新申请证书的区别？

重颁发和重新申请证书的主要区别在于是否基于原订单生成证书。

重颁发证书：重颁发证书不会更改证书到期时间，重颁发免费、付费型证书均不可以修改绑定域名。

重新申请证书：可修改证书信息，重新申请免费证书，将会占用免费证书额度，重新申请付费证书，则需重新付款。

哪些 SSL 证书类型支持小程序？

最近更新时间：2024-03-06 18:00:09

哪些 SSL 证书类型支持小程序？

除国密标准证书以外，其他证书类型均支持小程序。

SSL 证书管理相关
一键 HTTPS 套餐即将到期如何处理？

最近更新时间：2024-03-06 18:00:37

一键 HTTPS 套餐即将到期如何处理？

若您需继续使用一键 HTTPS 功能，您可前往腾讯云 SSL 证书管理控制台 进行续费升级操作。
若您不再继续使用，建议您在一键 HTTPS 套餐到期前将接入域名解析切换至源站，避免套餐到期后影响正常访问。
若您的接入域名在 DNSPod 进行解析，您可参考以下步骤进行操作：

1. 登录 DNSPod DNS 解析管理控制台。
2. 单击您在一键 HTTPS 接入的**域名**，进入 “记录管理” 页面。
3. 查找接入域名的 CNAME 记录类型，并将记录值修改为您的源站地址。

注意：

若您的源站地址为 IP 地址，请将记录类型修改为 A 记录并在记录值处填写您的源站 IP 地址。

4. 单击**确认**，即可完成设置。

我的资料相关

最近更新时间：2024-03-06 18:00:37

企业资料创建后找不到修改入口？

SSL 证书企业资料创建后暂不支持修改或删除，建议您重新创建企业资料进行审核。

我的资料中可创建多少个实例？

最多可支持添加10个公司的资料。若您的需求超出限制，请 联系我们。

提交企业资料后中多久可以完成审核？

请您注意接听 CA 机构审核电话，一般情况下可在1个工作日内完成审核。

注意：

资料审核申请较多的情况下，由于 CA 机构审核繁忙，会优先审核提交付费证书申请相关公司资料。

如何查看证书信息？

最近更新时间：2024-03-06 18:00:37

如何查看证书信息？

1. 登录 腾讯云 SSL 证书控制台，进入 “我的证书” 管理页面，并单击需要查看的证书 ID 。

说明：

若您使用的是卡片式控制台，您可以直接单击证书卡片。

2. 在证书详情页，即可查看证书基本信息，包含证书类型、过期时间等信息。

SSL 证书安装相关
IIS 下设置 https 主机名灰色无法编辑怎么办？

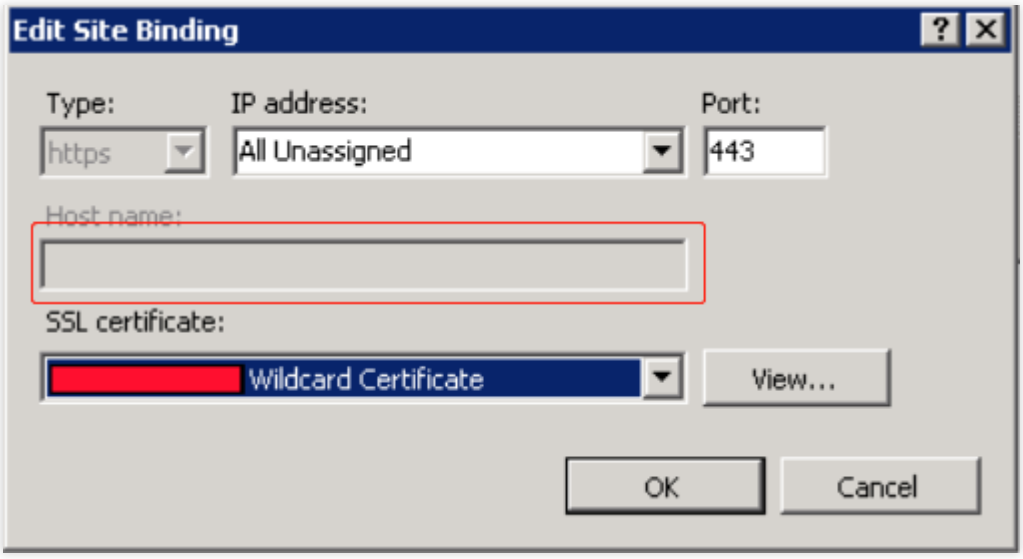
最近更新时间：2024-03-06 18:01:41

IIS 下设置 https 主机名灰色无法编辑怎么办？

在安装证书时，若您使用 IIS 管理器进行安装，将 pfx 证书文件导入后，在添加网站绑定域名过程中，类型选择为“https”时，出现主机名显示无法编辑的情况，您可以通过以下步骤解决该问题。

场景

在 IIS 设置中，选择 https，选择相应的 SSL 证书，主机名无法填写。如下图所示：



解决办法

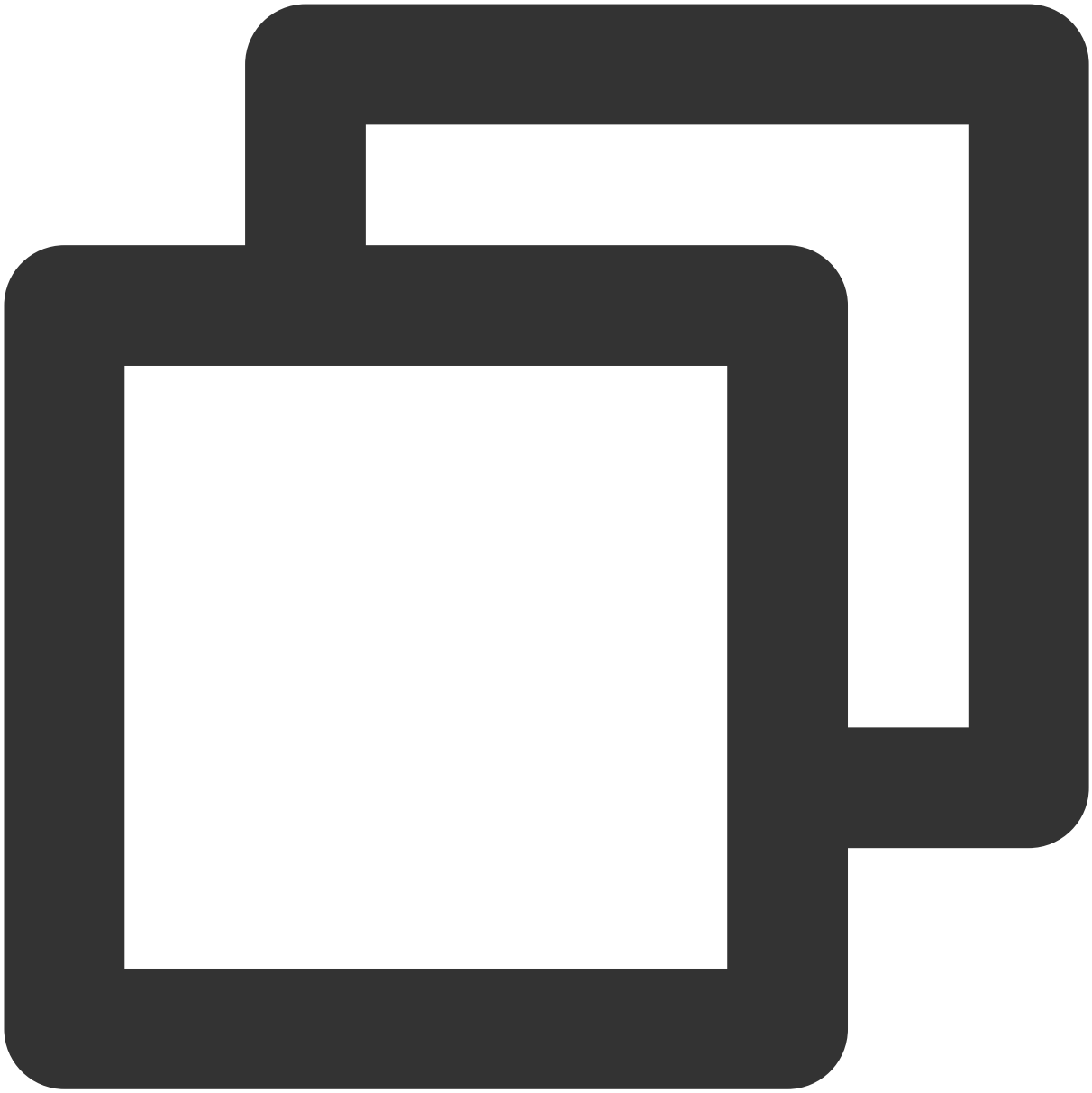
1. 请按路径 `C:\\Windows\\system32\\inetsrv\\config\\applicationHost.config` 打开 `applicationHost.config` 文件。
2. 修改内容如下：

说明：

以“tencent.com”域名为例。

将 `<binding protocol="https" bindingInformation="*:443:" />` 修改为 `<binding protocol="https" bindingInformation="*:443:tencent.com" />`。

文件无法直接修改时，可以尝试使用管理员权限进行修改或复制文件到桌面修改后，进行替换。



```
<site name="example.tencent.com" id="8">
            <application path="/">
                <virtualDirectory path="/" physicalPath="D:\\web\\tencent" />
            </application>
            <bindings>
                <binding protocol="http" bindingInformation="*:80:example.tencent.
                <binding protocol="http" bindingInformation="*:80:www.tencent.com"
                <binding protocol="https" bindingInformation="*:443:" />
            </bindings>
        </site>
```

3. 文件保存后，重新添加网站绑定即可。

服务器如何开启443端口？

最近更新时间：2024-03-06 18:01:41

服务器如何开启443端口？

请对应您使用的服务器进行操作：

腾讯云轻量应用服务器，则已默认开启443端口。如需了解更多信息，请参考 管理防火墙。

腾讯云云服务器，请参考文档 添加安全组规则 开启443端口。

其他云厂商云服务器，请参考云厂商提供的相关文档。

访问站点提示连接不安全？

最近更新时间：2024-03-06 18:01:41

SSL 证书部署以后，访问站点提示“连接不安全”，是否是证书部署失败？

证书已成功部署，也会出现这个问题，是因为采用 HTTPS 协议的站点访问。如果网页中包含未经加密的 HTTP 内容时，会被浏览器认为是不安全的，需要对代码进行改造。

前端改造上，可以有参考以下几点：

使用相对路径引用资源。

引用绝对路径时，采用 `//` 引用资源，例如 `//img.qcloud.com/example.png`，表示遵从当前页面的协议，浏览器会进行自动补齐。

如何安装 OpenSSL？

最近更新时间：2024-03-06 18:01:41

如何安装 OpenSSL？

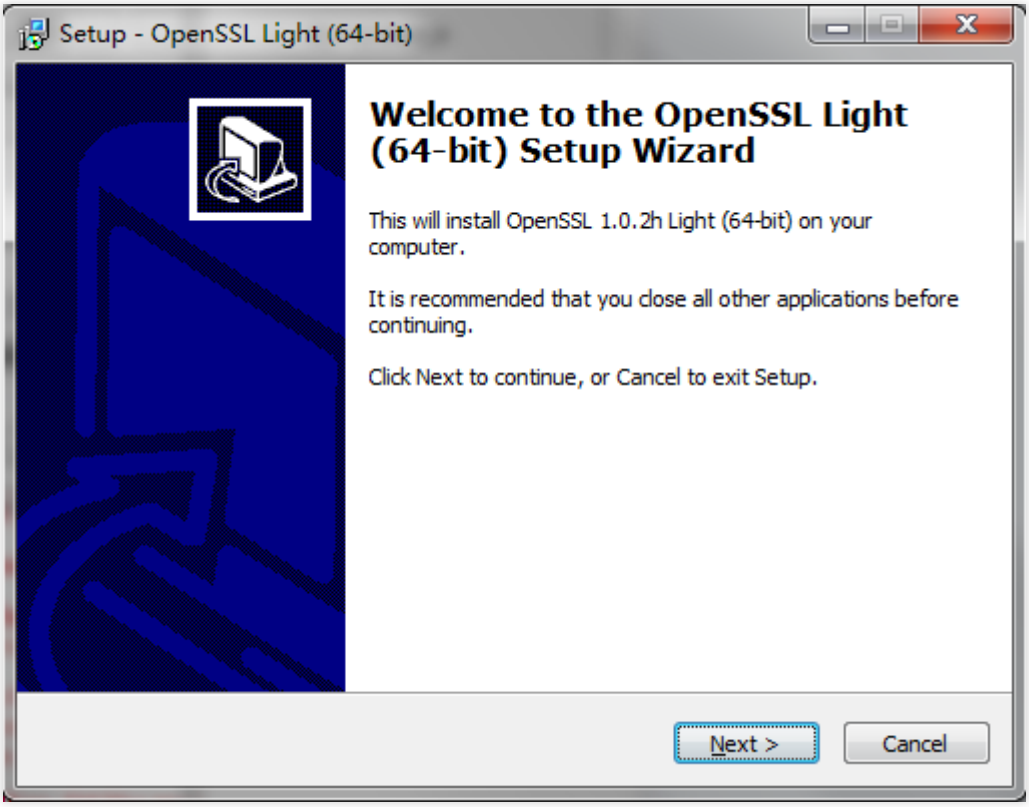
OpenSSL 是用于安全通信的著名开源密码学工具包，包括主要的密码算法、常见密码和证书封装功能。

OpenSSL 官网

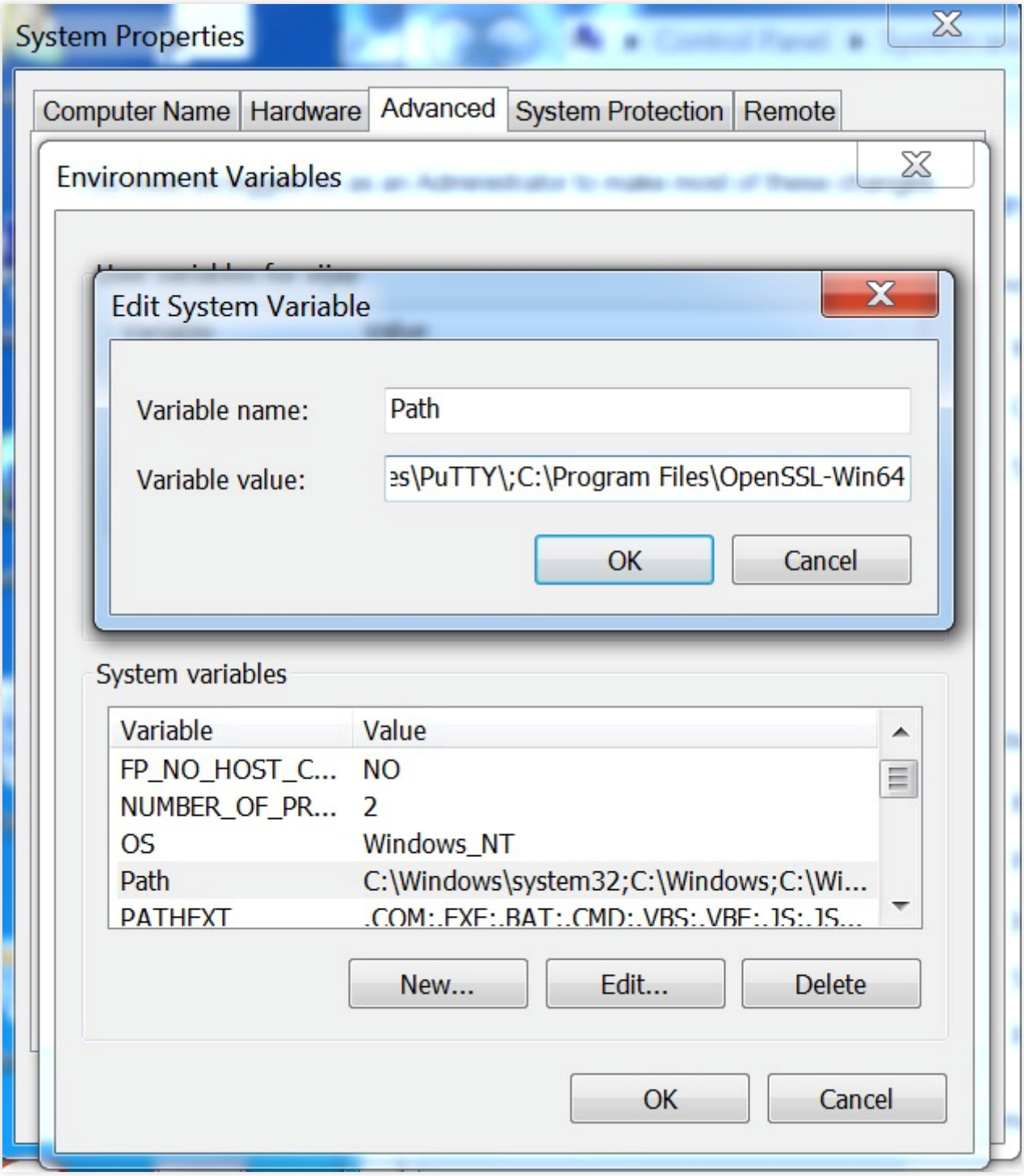
官方下载地址： 请单击此处。

Windows 安装方法

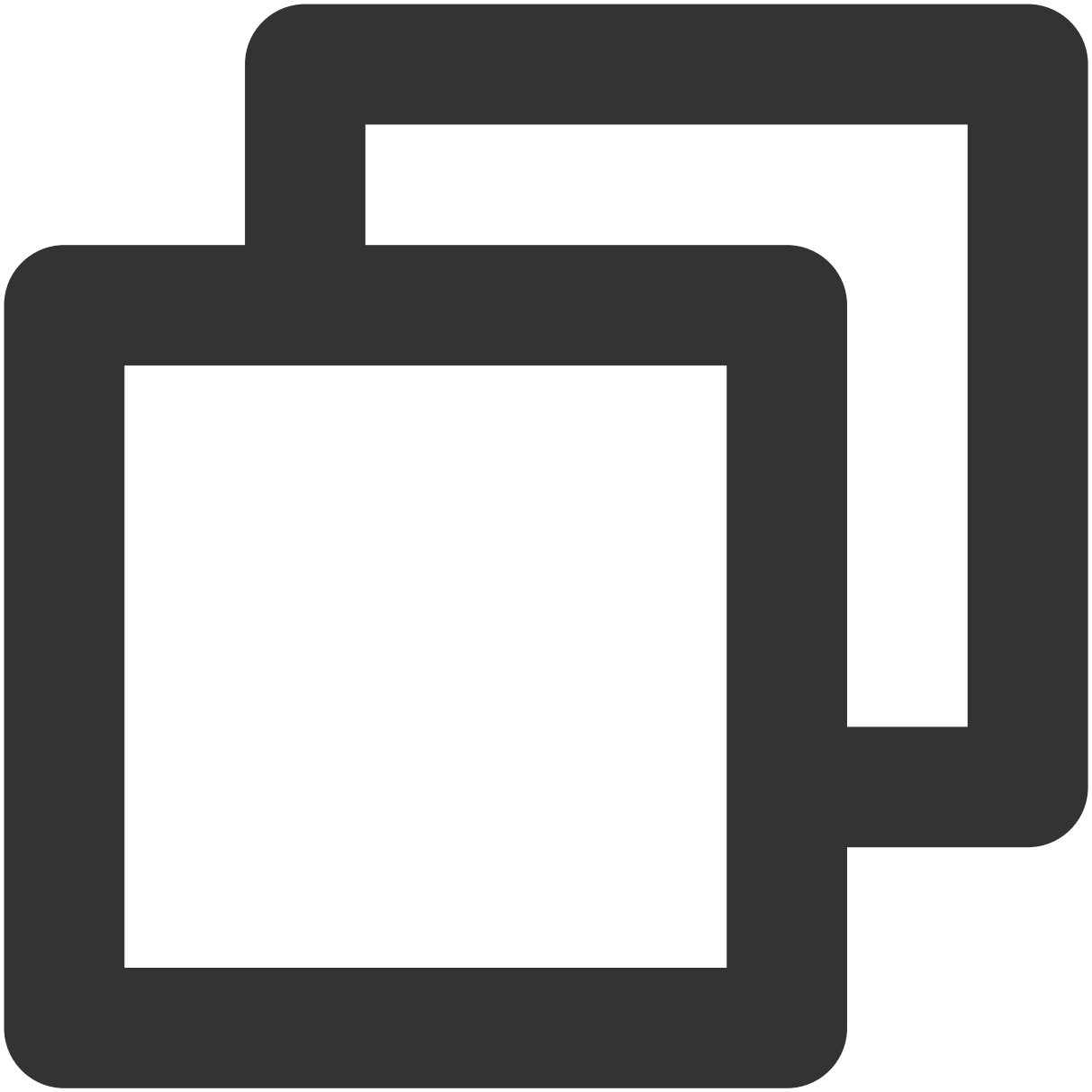
OpenSSL 官网没有提供 Windows 版本的安装包，可以选择其他开源平台提供的工具。请单击此处，
以该工具为例，安装步骤和使用方法如下：
1. 选择32位或者64位合适的版本下载，例如 `Win64OpenSSL_Light-1_0_2h.exe` 。如下图所示：



2. 设置环境变量，例如，工具安装在 `C:\\OpenSSL-Win64` ，则将 `C:\\OpenSSL-Win64\\bin；` 复制到 Path 中。如下图所示：

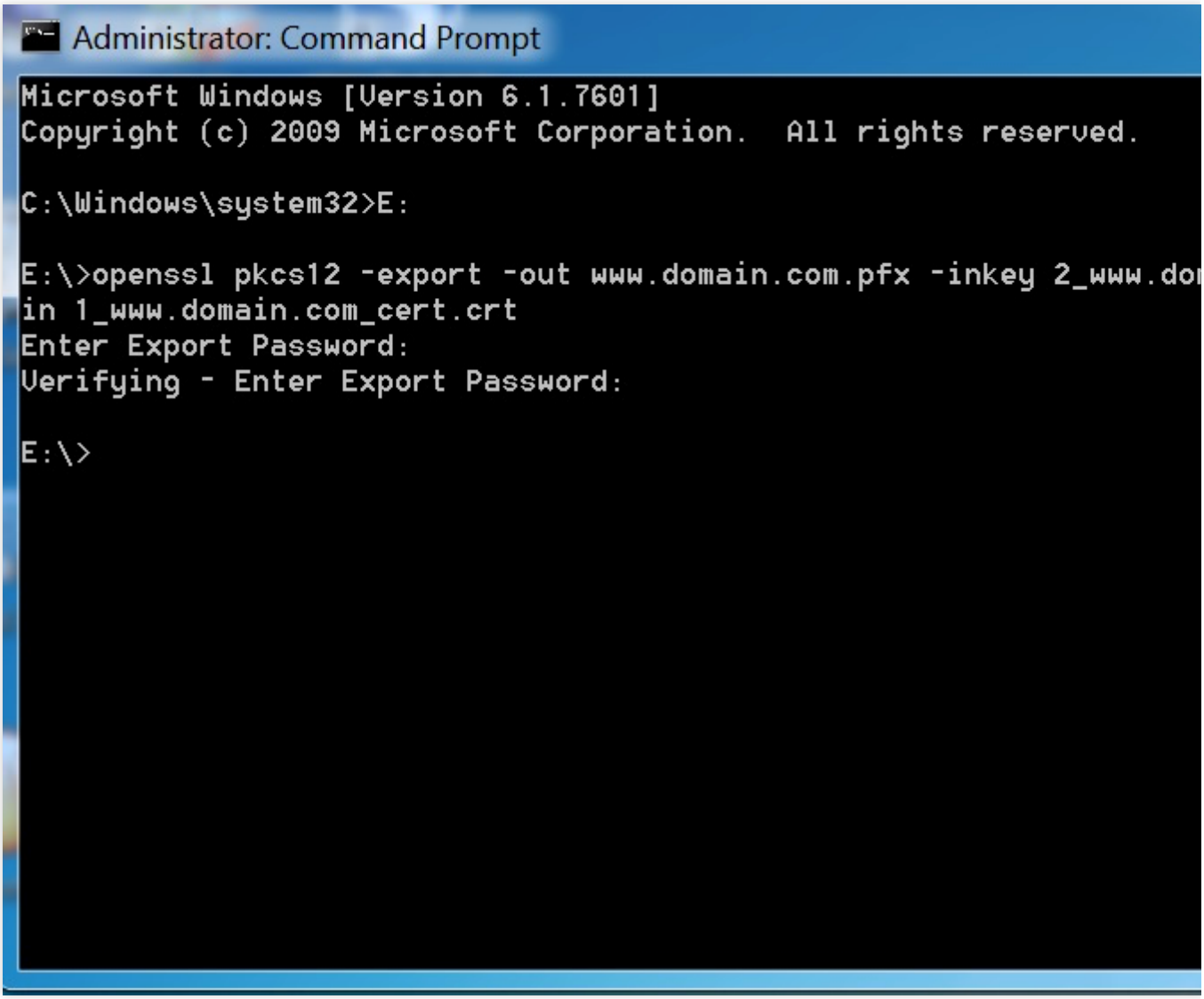


3. 打开命令行程序 cmd（以管理员身份运行），进入 `2_www.tencent.com.key` 、 `1_www.tencent.com_cert.crt` 文件所在目录，运行以下命令。



```
openssl pkcs12 -export -out www.tencent.com.pfx -inkey 2_www.tencent.com.key -in 1_
```

例如，key 和 crt 文件保存在 D:\\，运行情况如下：



注意：

Export Password 不需要的情况下，请直接回车不进行输入。

4. 在 D:\\ 已生成的 www.tencent.com.pfx 文件，可以继续完成在 IIS 管理器中的证书安装。

如何设置 SSL 证书的 TLS 协议版本？

最近更新时间：2024-03-06 18:01:41

TLS 协议版本包括 TLSv1.0、TLSv1.1、TLSv1.2、TLSv1.3 等，您可根据您的实际需求在腾讯云相关产品或服务器 Web 服务上设置证书的 TLS 协议版本。

腾讯云相关产品

如果您的证书部署到以下腾讯云产品，请参考以下文档进行配置：

负载均衡（CLB）：HTTPS 转发配置入门指南

内容分发网络（CDN）：TLS 版本配置

服务器 Web 服务

如果您的证书安装在服务器 Web 服务上，请在 Web 服务的证书配置文件中找到 `ssl_protocols TLSv1 TLSv1.1 TLSv1.2`，并根据实际需求进行修改。

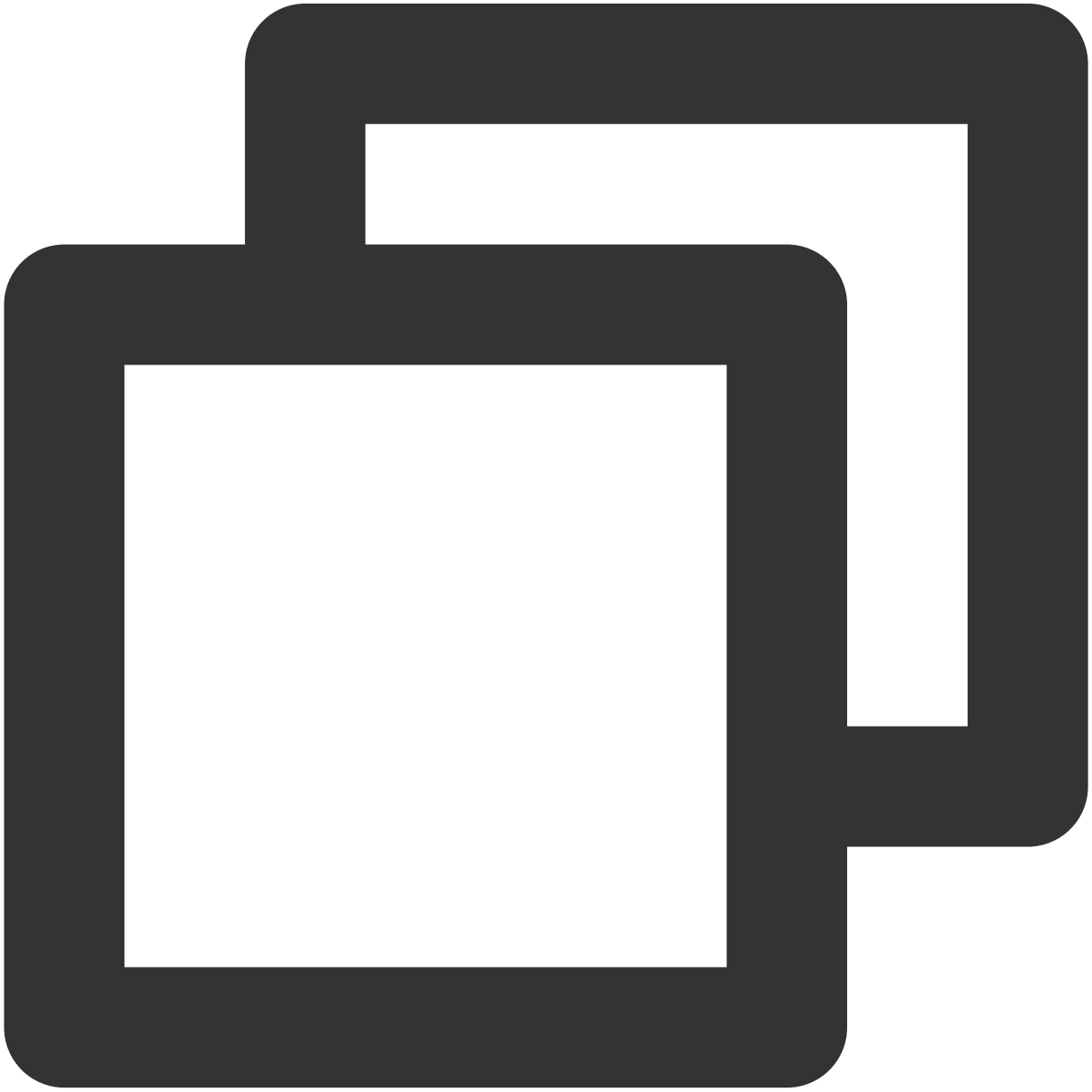
例如：您的证书需要支持 TLSv1.1 和 TLSv1.2 版本，则在 `ssl_protocols TLSv1 TLSv1.1 TLSv1.2` 中去掉 `TLSv1` 即可。

如何补全 SSL 证书链？

最近更新时间：2024-03-06 18:01:41

通常情况下 PC 端浏览器都可以通过 Authority Info Access（权威信息访问）的 URL 链接获得中间证书，但在部分 Android 系统的浏览器上访问时会出现证书不可信或无法访问等问题。

主要原因在于部分 Android 系统的浏览器并不支持通过 Authority Info Access（权威信息访问）的 URL 链接获得中间证书，这时您需要把证书链文件按照 SSL 证书链的结构合并为一个文件重新部署到服务器上，浏览器在与服务器连接时将会下载用户证书和中间证书，使您的浏览器访问时显示为可信证书。SSL 证书链结构如下所示：



```
-----BEGIN CERTIFICATE-----
网站证书
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

CA 中间证书机构
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

CA 根证书机构

-----END CERTIFICATE-----
```

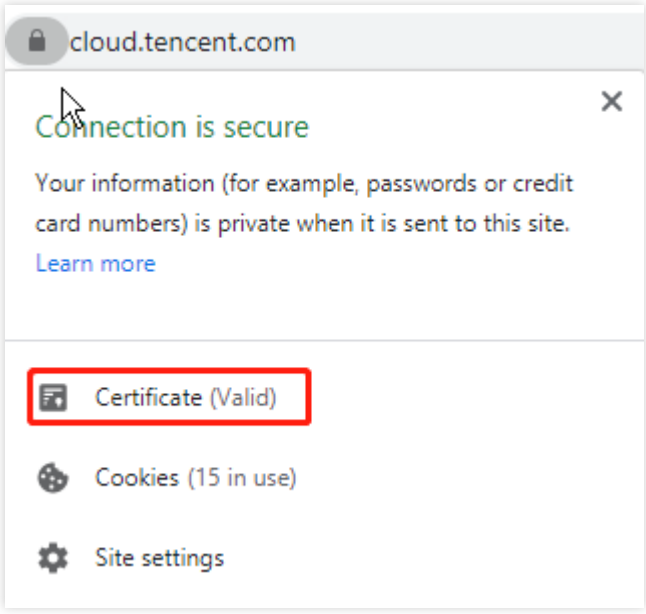
说明：

SSL 证书链的结构，一般是由**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。腾讯云提供的 SSL 国际标准证书为完整的证书链，无需进行补齐即可正常使用。

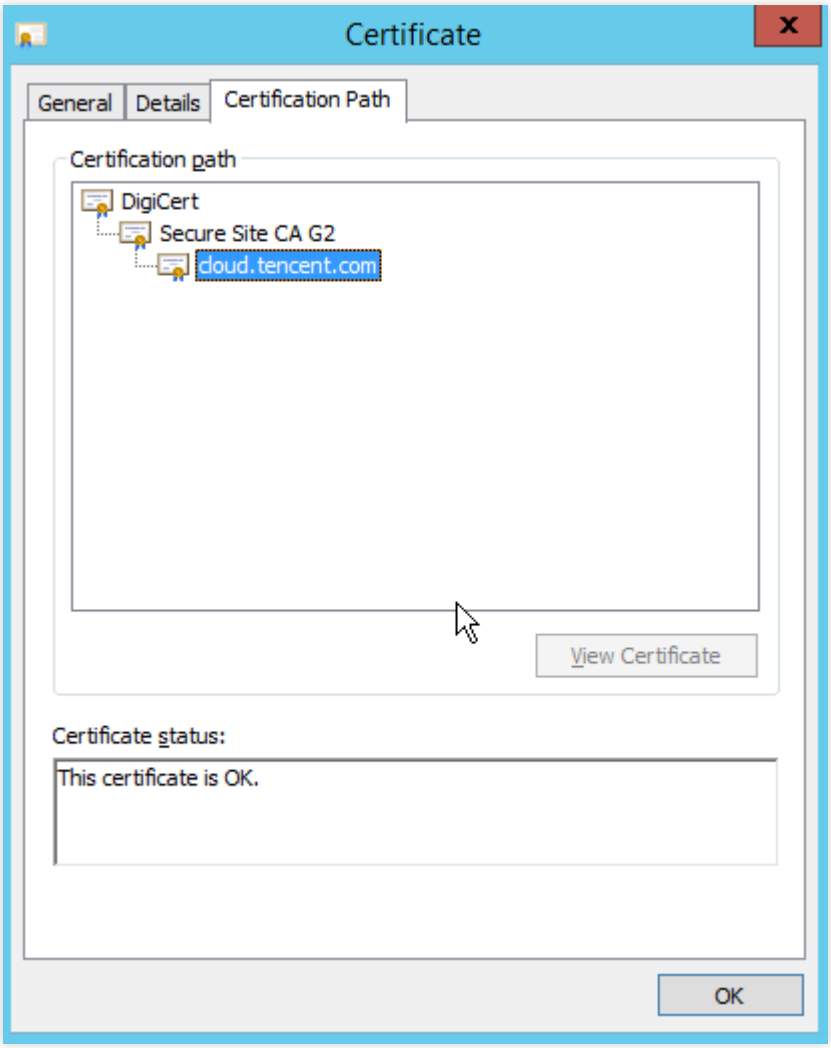
如何查看 SSL 证书链？

1. 打开 Chrome 浏览器访问安装部署 SSL 证书成功的网站。此处以 Chrome 浏览器为例。
2. 在浏览器地址栏单击

小锁图标，并在弹出的信息卡片中，单击**证书**。如下图所示：



3. 在弹出的 “证书” 信息窗口中，单击**证书路径**，即可查看 SSL 证书链。如下图所示：


Certificate
General
Details
Certification Path
Certification path
DigiCert
Secure Site CA G2
cloud.tencent.com
View Certificate
Certificate status:
This certificate is OK.
OK

腾讯云申请的 SSL 证书能用于 websocket 吗？

最近更新时间：2024-03-06 18:01:41

腾讯云申请的 SSL 证书能用于 websocket 吗 ？

能用于 websocket 服务，您可直接将 SSL 证书部署至您的 websocket 服务中进行加密传输。

如何开启 IIS 服务？

最近更新时间：2024-03-06 18:01:41

如何开启 IIS 服务？

1. 搜索 “控制面板”，并打开 “控制面板” 窗口。
2. 单击**程序与功能**，进入 “程序与功能” 管理页面。
3. 在左侧菜单栏中，单击**启用或关闭 Windows 功能**。
4. 在弹出的 “Windows 功能” 窗口中，查找并勾选 “Internet Information Services” 的所有选项。
5. 单击**确定**，即可启用成功。

SSL 证书过期后重新申请部署依然提示 HTTPS 不安全？

最近更新时间：2024-03-06 18:01:41

SSL 证书过期后重新申请部署依然提示 HTTPS 不安全？

SSL 证书过期后会导致浏览器提示 HTTPS 不安全，若您在 SSL 证书过期后访问该网站，浏览器将会缓存您的证书信息，因此，您在替换新证书后依然提示 HTTPS 不安全。建议您的证书在过期前替换为新证书，可确保您的业务不受影响。

说明：

若 SSL 证书为过期后再重新部署的情况下，清除浏览器缓存后再次访问即可。

SSL 证书地域相关

SSL 证书安装存在地域限制吗？

最近更新时间：2024-03-06 18:03:03

SSL 证书安装存在地域限制吗?

证书购买和颁发后，安装部署不受地域的限制。

SSL 证书审核相关

SSL 证书提交资料审核时长？

最近更新时间：2024-03-06 18:03:03

证书申请提交资料过程中，如涉及到人工审核流程，则需要等待审核，各证书类型人工审核所需时间如下：

说明：

由于 DV 型证书无人工审核流程，通常情况下 CA 机构检测到您的域名验证操作成功后，即可颁发证书。

证书类型	时长
DV 型证书	-
OV 型证书	3 - 5个工作日
EV 型证书	5 - 7个工作日

申请 SSL 证书审核失败的原因及处理方法

最近更新时间：2024-03-06 18:03:03

申请证书审核失败的原因及处理方法

本文主要介绍申请证书审核失败的可能原因和解决方法。

验证文件配置错误

说明：

建议您执行 `curl -k -v` 命令或者 `wget -S` 命令验证文件 URL 是否生效。同时，需要分别对 HTTPS 和 HTTP 两种协议的 URL 进行验证。

问题原因：

如果您在提交 SSL 证书审核时使用文件验证方式进行域名验证，可能会因为此问题造成订单审核失败。该场景下的 SSL 证书审核申请失败的可能原因如下：

站点部分页面已启用 HTTPS 访问方式，而验证文件仅部署在 HTTP 服务路径下，并没有部署在 HTTPS 服务路径下，导致用 HTTPS 协议请求时找不到对应的文件。

访问验证文件时，站点返回错误代码。

启用了 CDN 服务，而 CDN 服务节点未完成境外同步。

解决方法：

将验证文件部署在 HTTP 及 HTTPS 服务路径下，确认可以通过 HTTPS 协议访问。或者暂时关闭该站点所有页面的 HTTPS 服务。

确认通过 CA 机构中心指定的验证文件 URL 能够直接访问到正确的验证文件内容，并确认最终的验证文件不是通过重定向等方式显示在 Web 浏览器中。

说明：

可通过浏览器地址是否发生变化来检测是否存在重定向。

将验证文件同步到境外 CDN 服务节点，或者临时关闭 CDN 境外加速服务。

说明：

如果无法对 CDN 节点服务器进行变更操作，建议您改用 DNS 验证方式进行域名验证。

DNS 配置错误

问题原因

如果您在提交 SSL 证书审核时使用 DNS 验证方式进行域名验证，可能会因为此问题造成订单审核失败。该场景下的 SSL 证书审核申请失败可能存在的部分原因如下：

DNS 解析记录值配置错误。

使用部分域名解析服务商的服务时，因域名解析服务商对不存在的主机记录的查询返回值与预期的返回值不同，导致CA 机构中心验证返回值不准确。

DNS 解析记录超时，您提交申请信息后。您将有3个自然日时间完成 DNS 解析记录的添加，否则审核将会失败。

启用了动态域名解析服务，相应的解析记录值未能及时同步到境外权威 DNS 服务器。

解决方法

配置正确的 DNS 主机记录及记录值。

忽略域名解析设置提示的相关错误，按要求配置 DNS 的解析记录，完成域名验证。

重新提交申请信息，并在3个自然日时间内完成 DNS 解析记录的添加。

请确认动态解析服务正常，并确保境外的解析服务能够正常解析新增的解析记录。

说明：

修改已存在的记录值时，解析记录值会根据 TTL 值决定生效时间，而新增记录值则可以很快生效。因此建议您通过新增记录值完成验证。待域名验证通过后，可删除相关的解析记录信息。

单位的电话号码不能为空或不正确

当您申请 OV、EV 类型数字证书时，如果您未填写单位电话号码，将收到该审核失败信息。

问题原因

OV、EV 类型证书产品，单位电话号码为必填字段。当单位电话号码为空、或填写不符合规则时，需要重新填写。

解决方法

请填写能够及时联系到您的单位电话号码，以确保在 CA 机构中心进行组织信息验证时能够联系到您。

CSR 文件已用于其他订单

问题原因

出于证书密钥安全考虑，在请求一个全新的订单时，不允许使用之前已使用过的 CSR 信息。

解决方法

如果之前已使用一个 CSR 文件成功提交过订单，在后续的新订单中，请重新生成新的 CSR 文件。确保每张 SSL 证书都有其唯一的密钥对，有助于提升证书应用中的安全性。

证书绑定的域名格式不正确

问题原因

合法的域名仅允许包含**字母+数字+“-”**的任意组合，且域名的最大长度不得超过64个字符。

解决方法

请检查 CSR 请求文件及订单中填写的域名信息，确保您使用了正确的域名提交订单。

主域名不能为空

问题原因

创建 CSR 文件时未正确填写 `Common Name` 字段。

说明：

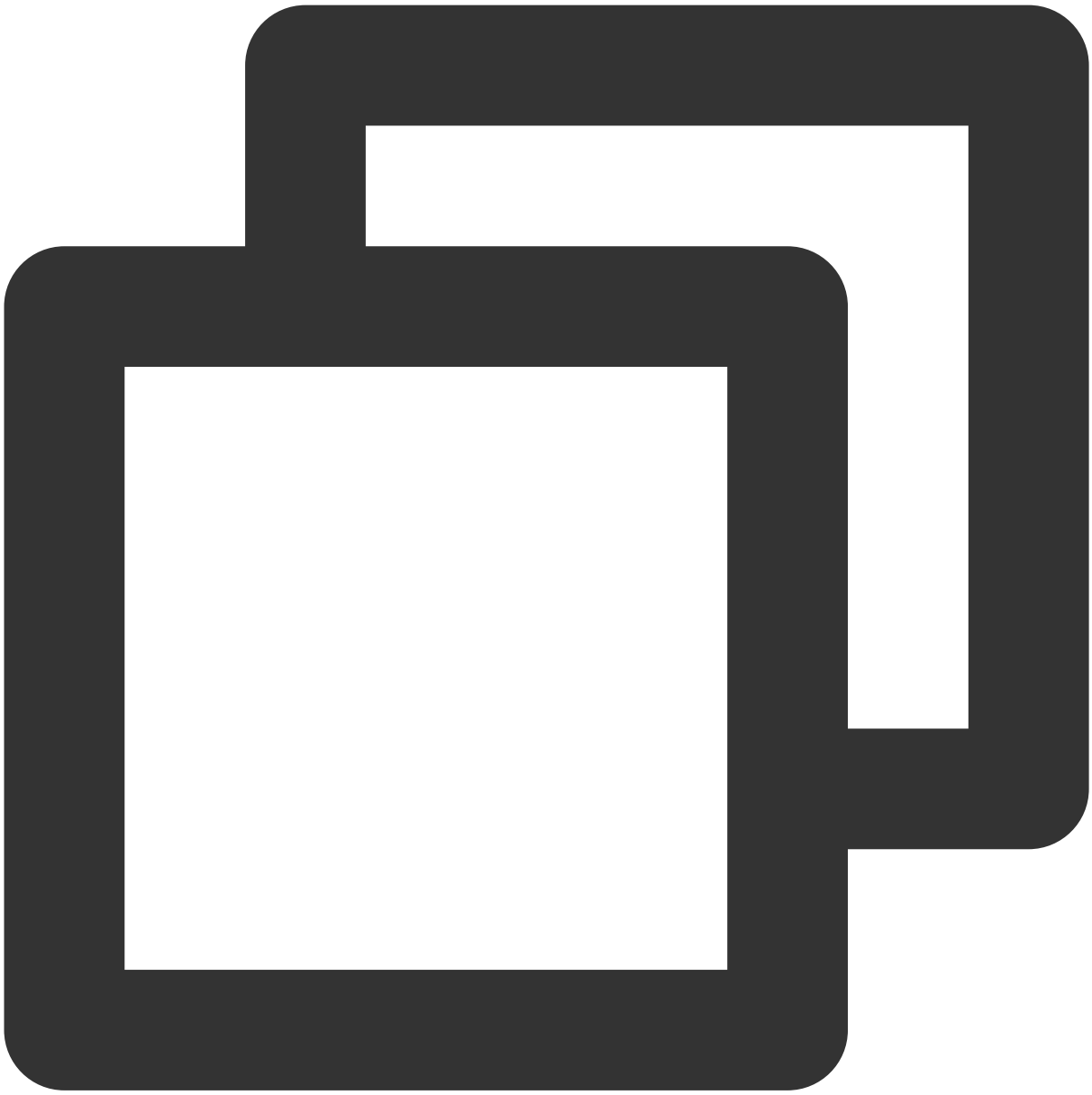
`Common Name` 必须是绑定域名中的其中一个域名。

解决方法

建议您使用系统提供的在线生成 CSR 文件功能。

域名安全审核失败

当您申请 SSL 证书时，您可能收到审核失败提示。
提示如下：



抱歉，该域名未通过 CA 机构安全审查，无法申请域名型证书。请购买企业型或增强型证书，您也可尝试使用其

问题原因

由于 CA 机构的反钓鱼机制，一般是域名信息中包含敏感词，例如 bank、pay 等，会引起安全审查失败，具体敏感词由 CA 机构定义，同时部分不常用的根域名也可能会审核失败，例如，`www.qq.pw` 、`www.qcloud.pw` 等以 .pw 根域名后缀的无法通过审核。

以下为可能导致无法通过的域名敏感词汇，仅作示例，具体由 CA 机构定义：

内、外网 IP 地址	主机名	live（不包含 .live 顶级域名）	bank
banc	alpha	test	example
credit	pw (包含 .pw 顶级域名)	apple	ebay
trust	root	amazon	android
visa	google	discover	financial
wordpress	pal	hp	lv
free	scp	-	-

解决方法

建议更换域名中的主机名部分，重新尝试提交订单。如果多次更换主机名，仍提示以上错误，则建议选择收费证书产品，或选择更换主域名申请证书。

说明：

域名型 SSL 证书通过自动认证快速颁发，不会人工介入审核，会用较为严格的敏感词来加强审核标准。

已购 SSL 证书提交申请审核后需要做什么？

最近更新时间：2024-03-06 18:03:03

已购证书提交申请审核后需要做什么？

您购买 SSL 证书后需申请证书并提交审核，审核通过后才能使用该证书并将证书部署到您的云服务资源上。
当您购买的是付费型证书时，提交审核后，CA 机构工作人员会联系您确认证书审核的相关信息。请您随时保持手机畅通（提交审核时填写的手机号码），并及时查看您的邮箱（提交审核时填写的邮箱），以免错过 CA 机构发送的确认通知。
当您的证书订单提交审核后，您可以登录 证书管理控制台，在证书列表中查看您证书审核申请的状态和后续流程。
您的证书订单提交审核后，包含以下两种状态：
验证中：证书申请为待验证的状态时，请您单击**证书详情**，进入证书详情页面查看域名验证方式，完成验证后，等待证书状态为**已签发**才能使用该证书。
审核失败：证书审核失败时，请您单击**证书详情**，进入证书详情页面确认证书审核失败的原因，并根据失败原因修改证书申请信息，修改完成后您需要重新提交申请。

不同证书类型颁发时长为多长时间？

OV、EV类型证书审核时长：OV 型证书颁发等待时间为3 - 5个工作日，EV 型证书颁发等待时间为5 - 7个工作日。
DV 型或免费型证书审核时长：DV 型证书颁发等待时间为10分钟 - 24小时。
说明：
免费型证书申请后会在1个自然日内颁发。由于 CA 机构中心审核流程耗时不同，您的证书有可能会在几个小时内就完成颁发，也有可能需要1个自然日才能完成颁发，请您耐心等待。

如何查看域名型（DV）SSL 证书域名验证结果？

最近更新时间：2024-03-06 18:03:03

如何查看 DV 型证书域名验证结果？

在您提交证书申请后，CA 机构中心将对您的域名及所提交的信息进行审核。域名验证成功后，CA 机构中心才会对证书进行颁发，若您的证书一直未颁发，建议您根据以下内容检验域名验证结果。

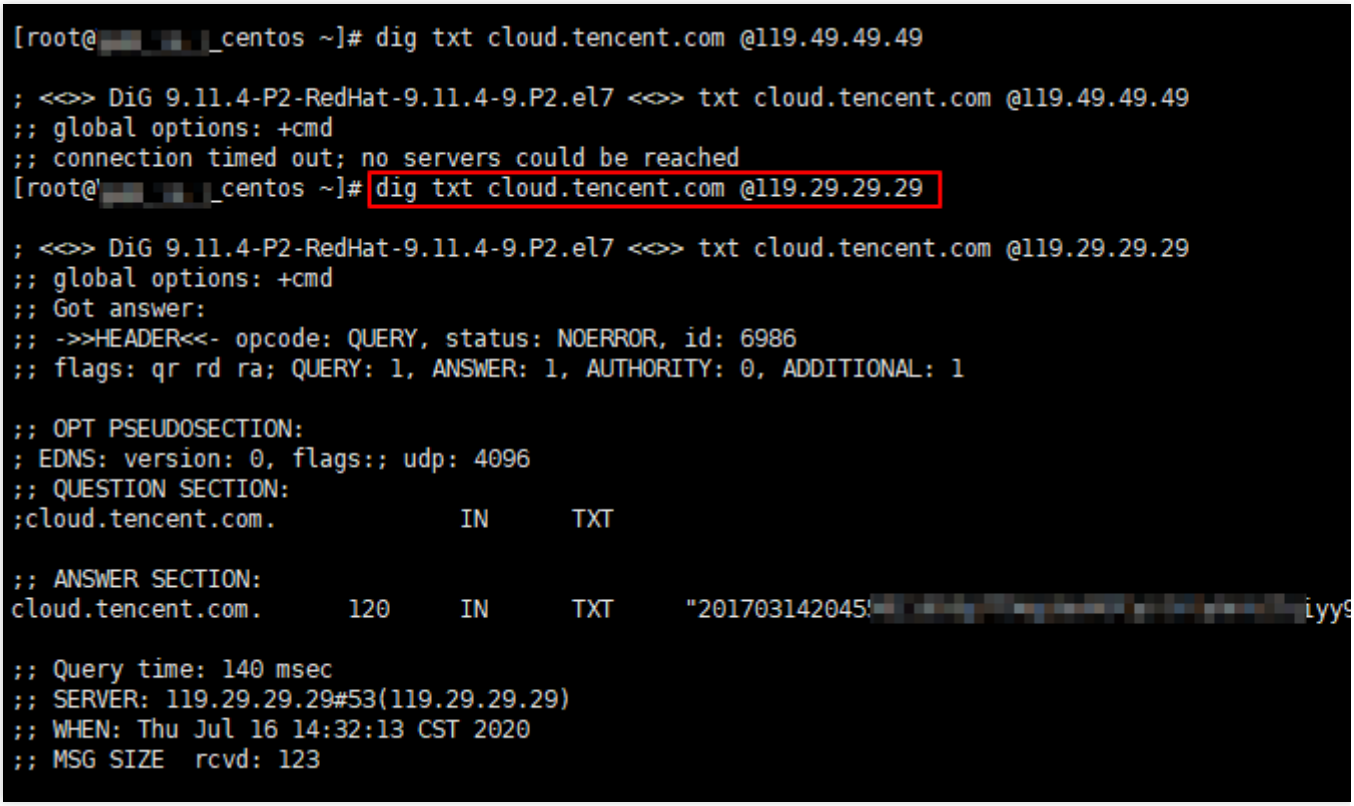
说明：

腾讯云 SSL 证书服务提供的主机记录是全域名的，如果您的域名管理系统不支持全域名的主机记录，请去掉根域名的后缀部分。

DNS 验证类型

1. 请登录您的域名服务器，执行 dig 命令查询域名 DNS 解析。
2. 执行 `dig + 记录类型 + @119.29.29.29` 命令指定使用 DNSPod 的 DNS 进行验证。

例如 `dig txt cloud.tencent.com @119.29.29.29`



如果返回结果中存在类似图示中的 TXT 记录，且记录值与证书控制台中证书详情页面中的记录值一致，表示您的 DNS 配置正确且已生效。

如果返回结果中不存在 TXT 记录，可能是 DNS 解析配置有误或者配置未生效。

若 DNS 解析配置错误，请登录 证书管理控制台，单击**待验证**页签，进入该证书的详情页面。将证书详情中的记录值

复制，并在您的 DNS 域名解析服务商更新解析。如果配置长时间未生效，请联系您的域名托管商。

说明：

具体操作请您参考 DNS 验证。

文件验证类型

1. 请登录 证书管理控制台 ，单击**待验证**页签，进入该证书的详情页面。

2. 单击访问验证 URL 地址，若访问页面中显示的内容和证书详情页面中的验证文件内容一致，说明可正常访问，若不一致，请从以下几个方面着重进行检查：

检查该验证 URL 地址是否已存在 HTTPS 可访问的地址。若存在，请在浏览器中使用 HTTPS 地址重新访问，如果浏览器提示 “证书不可信” 或者显示的内容不正确，请您暂时关闭该域名的 HTTPS 服务。

确保验证 URL 地址在任何一个地方都能正确访问。由于每个品牌证书的检测服务器区域不同，请确认您的站点是否有国外镜像，或者是否使用了智能 DNS 服务等。

文件验证需要直接响应200状态码和文件内容，不支持任何形式的跳转。检查该验证 URL 地址是否存在301或302跳转。如存在此类重定向跳转，请取消相关设置关闭跳转。

说明：

您可执行 `wget -S URL 地址` 命令检测该验证 URL 地址是否存在跳转。

SSL 证书生效相关
服务器 IP 地址更换后原来的 SSL 证书能否生效？

最近更新时间：2024-03-06 18:03:04

服务器 IP 地址更换后原来的 SSL 证书能否生效？

如果您的 SSL 证书是绑定域名的，则不受服务器更换 IP 地址的影响。
证书绑定的域名不变，可以重新解析到新的 IP 地址，原来的 SSL 证书仍然可以生效，不需要更换新的证书。

如何在浏览器中检查 SSL 证书是否生效？

最近更新时间：2024-03-06 18:03:04

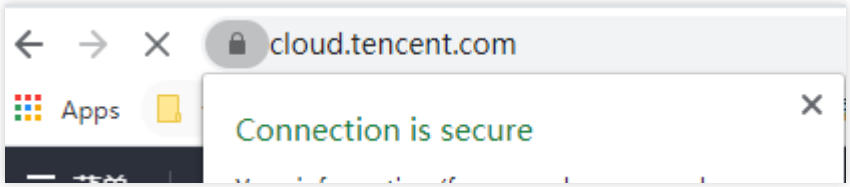
如何在浏览器中检查 SSL 证书是否生效？

证书安装成功并解析至服务器 IP 后，您可以按照以下步骤检查 SSL 证书生效情况：

1. 打开浏览器（本文以 Chrome 浏览器为例），在浏览器地址栏中以 https 格式输入 SSL 证书绑定的域名地址。
2. 按回车键，访问域名地址。检查是否具备以下情况：

域名地址可以成功访问网站。

浏览器地址栏左侧显示安全锁标志，则说明您的 SSL 数字证书已生效。如下图所示：



GlobalSign 证书 Windows 7 系统下不受信任怎么办？

最近更新时间：2024-03-06 18:03:04

背景

2019年5月27日，GlobalSign 正式使用新的中级 CA 为 SSL 证书产品签名。因 Windows 7 系统中没有新根支持，致使 Windows 7 系统访问2019年5月27日之后签发（包括更新或者重颁发的证书）的 GlobalSign 证书时，网站不受信任。

解决办法

请使用文本编辑器，打开已下载证书中 Nginx 目录下的 .crt 文件，将以下交叉证书复制粘贴放置于证书链最后位置。重启 Nginx 服务，证书即可正常使用。
交叉证书下载请单击此处。

免费 SSL 证书颁发时间过长或颁发失败排查方案

最近更新时间：2024-03-06 18:03:04

本文将介绍您在腾讯云申请免费 SSL 证书时，验证域名所有权中超时导致颁发失败如何排查处理。

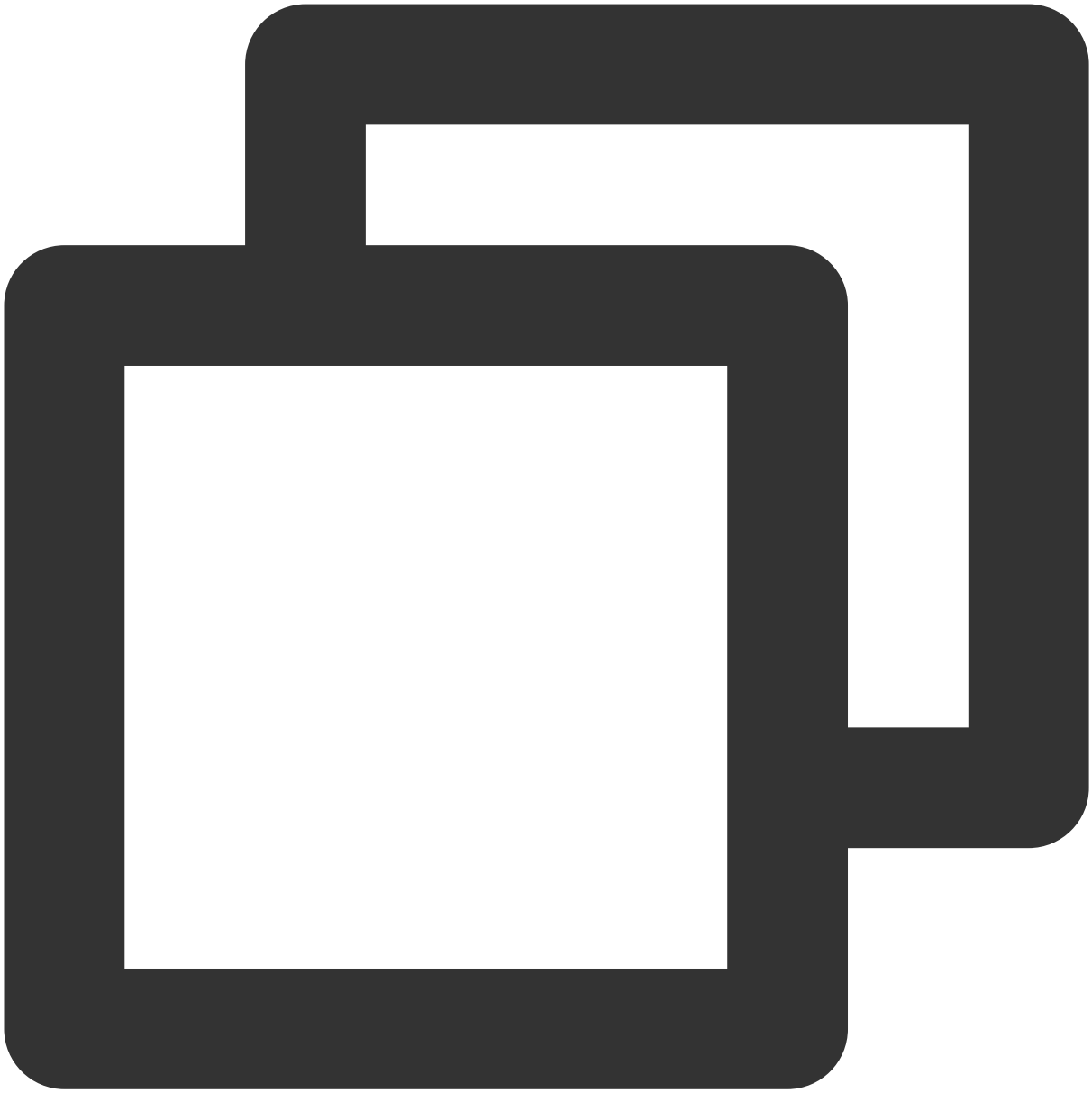
说明：

免费 SSL 证书颁发时间一般不超过30分钟，若超过您可参考本文自行排查导致超时原因。

排查 CAA 记录

无论是文件验证或 DNS 验证都需要检查 CAA 记录，无 CAA 记录或 CAA 记录中包含 `0 issuewild "sectigo.com"` 和 `0 issue "sectigo.com"` 均可通过 CAA 记录检查。

dig 命令



```
dig 域名名称 CAA
```

返回值为空或包含 `0 issuewild "sectigo.com"` 和 `0 issue "sectigo.com"` 即为正常。如下图所示：

```
rttw@Kincaid:~$ dig dnstest.cc caa

; <<>> DiG 9.18.1-1+0~20220316.73+debian11~1.gbp965910-Debian <<>> dnstest.cc c
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18535
;; flags: qr rd ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;dnstest.cc.                    IN      CAA

;; ANSWER SECTION:
dnstest.cc.             0       IN      CAA     0 issue "sectigo.com"
dnstest.cc.             0       IN      CAA     0 issuewild "sectigo.com"

;; Query time: 1270 msec
;; SERVER: 172.29.112.1#53(172.29.112.1) (UDP)
;; WHEN: Tue Mar 29 13:06:58 CST 2022
;; MSG SIZE  rcvd: 102

rttw@Kincaid:~$
```

DNS 诊断工具

前往 DNS 诊断工具，输入主域名并选择 CAA 记录后点击检测，返回值为空或包含 `0 issuewild "sectigo.com"` 和 `0 issue "sectigo.com"` 即为正常。

说明：

若出现检测失败或只有部分地区可以正常检测的情况，请检查域名 DNS 解析设置。

解决方法

若返回检测结果不为空且不包含 `0 issuewild "sectigo.com"` 和 `0 issue "sectigo.com"`，请前往域名解析处添加以下记录：

主机记录	记录类型	线路类型	记录值
@	CAA	默认	0 issuewild "sectigo.com"
@	CAA	默认	0 issue "sectigo.com"

排查验证 DNS 记录

检查完 CAA 记录后请确认验证记录是否已经添加，若为自建 NS 或部分存在境外解析限制的 NS 请检查境外解析是否正常，可使用 DNS 诊断工具或 DNSCHCKER 工具进行检测，一般情况下，所有监测点均能正常返回且返回值相同。

1. 确定检测域名。

检测域名应为 `主机记录.域名` ，例如，证书主机记录为 `_26A56EBADCE479E******5D304C0D8.blog` ，域名为 `dnspod.cn` ，则要检测域名为 `_26A56EBADCE479E******5D304C0D8.blog.dnspod.cn` 。

2. 前往 DNS 诊断工具，输入检测域名并选择 CNAME 记录后，单击**检测**，返回值为控制台提示的记录值即为正常。

排查服务器是否屏蔽验证 IP

使用文件验证方式通过后进入 “等待机构签发” 时，长时间不颁发证书的原因一般为服务器或机房屏蔽了 CA 的验证 IP，请将 CA 验证 IP 加白： `64.78.193.238` 、 `216.168.247.9` 。

SSL 证书收费和购买相关
域名型（DV）SSL 证书是否永久免费？

最近更新时间：2024-03-06 18:03:04

域名型证书是否永久免费？

首先，SSL 证书无论是免费的域名型或者是付费的企业型，CA 机构都规定了有效期的，从安全性上考虑，不能保证一个合法网站永远不会成为一个钓鱼站点，CA 机构需要定期审核，所以不会颁发永久有效的证书。
其次，当网站的私钥丢失时可以申请吊销，CA 机构会将吊销的证书加入证书吊销列表（Certificate Revocation List，简称：CRL），每次 HTTPS 站点被访问时，浏览器会向 CA 机构获取 CRL，判断是否能信任该证书；然而永久有效的证书会导致 CRL 不断增加，不会减少，会增加浏览器的请求流量压力，所以指定证书的有效期是更科学的处理方式。
腾讯云目前提供免费的域名型证书，型号为 **TrustAsia DV SSL CA - G5**，证书有效期**时长1年**。证书过期**前一个月**即可重新申请，域名型证书能在一个工作日内快速颁发，您有充足的时间为站点切换证书。

SSL 证书有效期相关
SSL 证书快过期了怎么办？

最近更新时间：2024-03-06 18:03:04

SSL 证书过期了怎么办？

SSL 证书过期之后将无法继续使用，您需要在证书到期前及时续费，并重新绑定域名和提交审核。
审核通过后，您将获得一张新的证书，您需要在服务器上重新安装新的证书替换即将过期的证书。
说明：
如果您使用的是免费域名型（DV） 证书需重新申请。
证书到期前您需预留3 - 10个工作日进行重新购买，避免因证书过期导致证书审核未通过。
详细信息请参见 付费型 SSL 证书续费流程。

SSL 证书过期后未及时更新有哪些影响？

最近更新时间：2024-03-06 18:03:04

SSL 证书过期后未及时更新有哪些影响？

如果SSL证书过期，没有及时更新证书，可能会产生如下影响：
用户访问网站时，浏览器会提示网站的安全证书已过期的告警信息。
用户收到上述告警信息后，可能对该网站失去信任，甚至选择停止访问该网站，对企业的品牌形象、用户量等有不利影响。
黑客等不法分子可能会利用过期的 SSL 证书，篡改或窃取浏览器和服务器之间传输的信息和数据，从而影响用户的数据安全。
证书到期导致的业务意外中断，无法正常运营，导致资金损失。
损害网站的 SEO 排名等。

查看 SSL 证书到期相关问题

最近更新时间：2024-03-06 18:03:04

如何收到 SSL 证书到期的系统通知？

证书到期前，您可在 腾讯云 SSL 证书控制台 的证书信息状态列查看证书到期的相关信息。
您也可以通过消息订阅来设置接收证书相关的系统消息通知。
说明：
如未设置消息订阅并且未在**产品消息**中勾选 **SSL 证书相关通知**与**产品服务相关通知**，您将不会收到证书到期的站内信、邮箱或手机短信通知。
其他厂商上传至腾讯云的证书，如已设置消息订阅，证书到期前也会接收相关通知。
证书到期提醒时间：证书将于到期30天内开启续费通道，到期提醒将于开启续费通道第二天进行发送。

如何设置接收证书相关的系统消息通知？

1. 请您登录 消息中心控制台 。
2. 在**消息订阅**管理页面，您可在**产品消息**中勾选 **SSL 证书相关通知**与**产品服务相关通知**以及您需要的通知类型。

SSL 证书成功续费后可以继续服务吗？

最近更新时间：2024-03-06 18:03:04

证书成功续费后可以继续服务吗？

不能。证书续费后，您需要重新提交证书申请审核并等待新证书颁发后重新部署到您的云服务资源上。