SSL 证书

故障处理

产品文档

腾讯云

文档目录

故障处理
域名验证时提示验证失败

最近更新时间：2024-03-06 17:56:24

现象描述

申请 SSL 证书进行域名验证并已添加对应操作时，证书域名验证详情页单击**查看域名验证状态**提示验证失败。

可能原因

请您单击**查看域名验证状态**，并根据提示分类说明进行排查。

使用 DNS 解析验证

原因1：未检测到指定解析值，请您耐心等待解析值生效，或确认已为该域名添加指定解析记录

域名为无法正常进行解析的状态。
添加的解析记录未生效。

原因2：解析记录值错误，请检查解析记录值是否配置正确，或等待 DNS 缓存更新

添加解析记录中主机记录、记录值等输入内容错误。
错误信息修正后，域名 DNS 缓存暂未更新。

原因3：您的域名已检测到验证值，请耐心等待 CA 机构进行审核

解析缓存或者验证地址限制了境外 CA 机构进行访问。

原因4：您的域名 CA 机构已审核通过，请耐心等待状态变更

系统已检测到验证值，但还没未进行颁发操作。

原因5：操作过于频繁，请等待5分钟后再试

多次单击**查看域名验证状态**，CA 机构进行限频。

注意：

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 解析记录。若已添加，请删除后再进行域名验证。

使用文件验证验证

原因1：未检测到指定验证值，请确认已为该域名添加指定验证值或耐心等待 CA 机构进行审核

验证文件未上传至申请证书网站根目录下。
无法访问网站验证文件或验证文件路径错误。
网站使用了多级跳转。

原因2：您的域名 CA 机构已审核通过，请耐心等待状态变更

CA 机构已审核通过，CA 机构暂时对其进行状态变更。

解决思路

使用 DNS 解析验证

添加的解析记录未生效

解析在全球生效时间是0 - 72小时，该期间也有可能影响解析生效，请耐心等待。

添加解析记录中主机记录、记录值等输入时发生手误

请检查并修改证书域名验证详情页中提供的记录值与域名解析处添加的解析记录值是否匹配对应的记录值。

错误信息修正后，域名 DNS 缓存暂未更新

解析记录值修改后在全球生效时间是0 - 72小时，这期间也有可能影响解析生效，请耐心等待。

解析缓存或者验证地址限制了境外 CA 机构进行访问

请耐心等待 dns 缓存更新，或者检查境外地址是否能够访问网站并对其进行开放。

系统已检测到验证值，但还没未进行颁发操作

系统已经检测到验证值，颁发时间预计在15分钟以内，请耐心等待系统颁发证书。

多次单击查看域名验证状态，CA 机构进行限频

请勿同一时间多次重复进行验证，请耐心等待间隔5分钟后进行尝试。

使用文件验证验证

验证文件未上传至申请证书网站根目录下

请将域名验证详情页中提供的验证文件，上传至网站根目录下。

无法访问网站验证文件或验证文件路径错误

请检查网站验证文件是否具备访问权限和验证文件是否正确放置申请证书网站根目录下，使浏览器访问文件时可见。如申请证书的域名网站为 `cloud.tencent.com`，网站验证文件 fileauth.txt 中验证内容为 `tencxxxent`。

浏览器使用 https 或 http 协议访问地址 `cloud.tencent.com/.well-known/pki-validation/fileauth.txt` 时，浏览器显示验证内容 `tencxxxent` 。

网站使用了多级跳转

文件验证需直接响应 200 状态码，不支持任何形式的跳转。建议您先调整网站跳转为可直接响应 200 状态码，等待域名验证通过后在添加跳转。

CA 机构已审核通过，CA 机构暂未对其进行状态变更

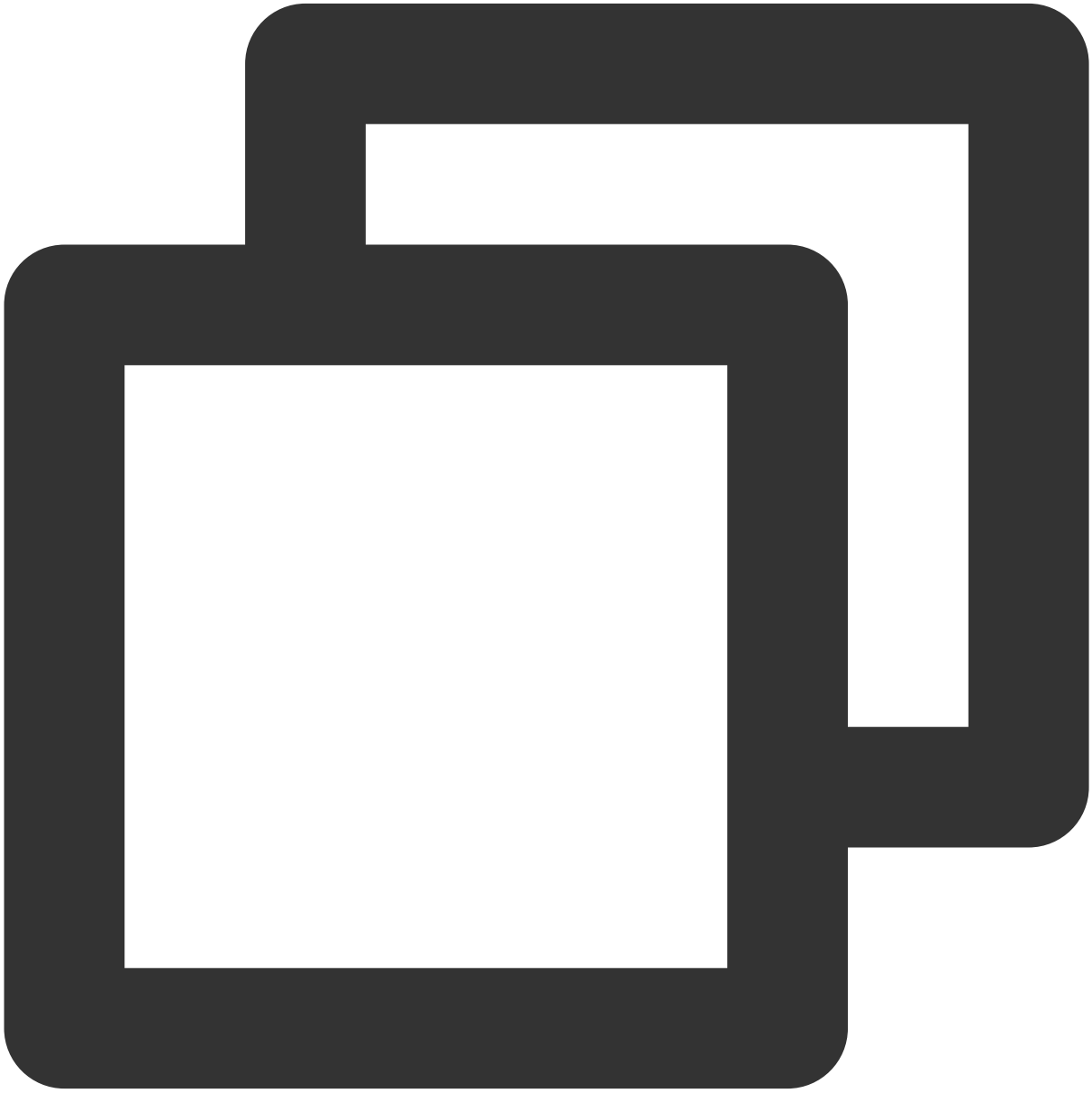
等待 CA 机构对其进行状态变更即可或刷新浏览器页面查看是否已颁发证书。

域名安全审查未通过

最近更新时间：2024-03-06 17:56:24

现象描述

申请免费域名型（DV）SSL 证书时订单审核失败并收到以下提示：



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

可能原因

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，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		-

解决方案

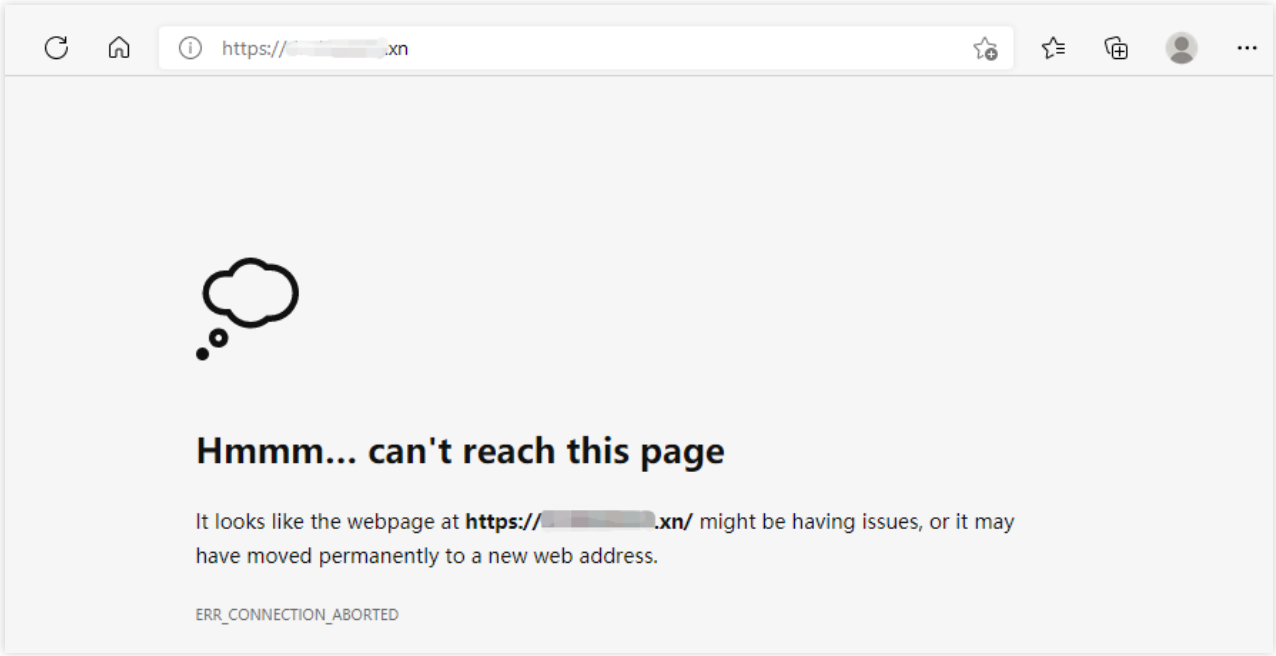
您可参考以下两种方法解决问题：
购买非 DV 型 SSL 证书进行绑定您的域名。
申请其他不包含敏感词的域名。

无法使用 HTTPS 访问网站

最近更新时间：2024-03-06 17:56:24

现象描述

在服务器上安装部署 SSL 证书后，使用 HTTPS 协议访问网站，页面加载缓慢、空白或提示 “无法访问”。



可能原因

服务器防火墙未开启443端口：若您的服务器防火墙未开启443端口，将导致您无法使用 HTTPS 正常访问您网站，请开启服务器443端口后，再进行尝试。
安全组未开启：安全组是一种虚拟防火墙，具备有状态的数据包过滤功能，用于厂商设置云服务器、负载均衡、云数据库等实例的网络访问控制，控制实例级别的出入流量，是重要的网络安全隔离手段，默认情况下为关闭状态。请开启服务器的安全组设置后，再进行尝试。
浏览器缓存污染：浏览器缓存可以节约网络资源加速浏览，通常情况下浏览器会对最近请求过的资源进行缓存。当访问者再次请求这个页面时，浏览器将可能会以已缓存信息进行展示。
配置文件未配置正确：服务器的 Web 服务配置文件未配置正确，导致网站无法正确处理请求导致网站无法访问。

解决办法

服务器防火墙未开启443端口

若您使用的是腾讯云的云服务器（CVM），您无需进行该项设置，云服务器（CVM）默认为开启状态，建议您检查安全组是否开启。
若您使用的是腾讯云轻量应用服务器（Lighthouse），请参考管理防火墙开启443端口设置。
若您使用的是其他云厂商云服务器，请咨询您的云厂商。

安全组未开启

若您使用的是腾讯云的云服务器，请参考 添加安全组规则 开启443端口。
若您使用的是腾讯云轻量应用服务器（Lighthouse），则无该功能设置，建议您检查 防火墙是否开启443端口。
若您使用的是其他云厂商云服务器，请咨询您的云厂商是否有该策略，如有该策略，咨询如何开启443端口；如无该策略，建议您检查 防火墙是否开启443端口。

浏览器缓存污染

请清除您的浏览器缓存或使用其他浏览器进行访问测试。

配置文件未配置正确

请您检查配置文件是否正确，您可以参考对应的部署文档进行检查或在云市场 购买证书部署服务。
说明：
如您是按照腾讯云的文档进行证书安装部署，具体操作可参考 SSL 证书安装部署。

在 IIS 服务上部署 SSL 证书后访问资源出现 404 报错

最近更新时间：2024-03-06 17:56:24

现象描述

在 IIS 服务上部署 SSL 证书后访问资源出现 404 报错。

可能原因

HTTPS 和对应的 HTTPS 服务绑定的站点不统一。
站点信息配置错误。

解决方案

成功部署证书后，通过 HTTP 协议访问资源正常，通过 HTTPS 协议无法访问资源并出现404错误提示。如您在 IIS 服务中配置了 SSL 证书，且防火墙开启了443端口，可参考以下两个方面排查问题：
HTTP 和 HTTPS 可以设置不同的网站根目录，在 IIS 服务器中，检查站点的443端口绑定情况，并确认443端口绑定的站点与期望显示的 HTTP 服务80端口绑定的站点相同。
检查端口绑定情况时，检查设置站点的 IP 地址、主机名的正确性。

部署 SSL 证书后，浏览器提示 “网站连接不安全”

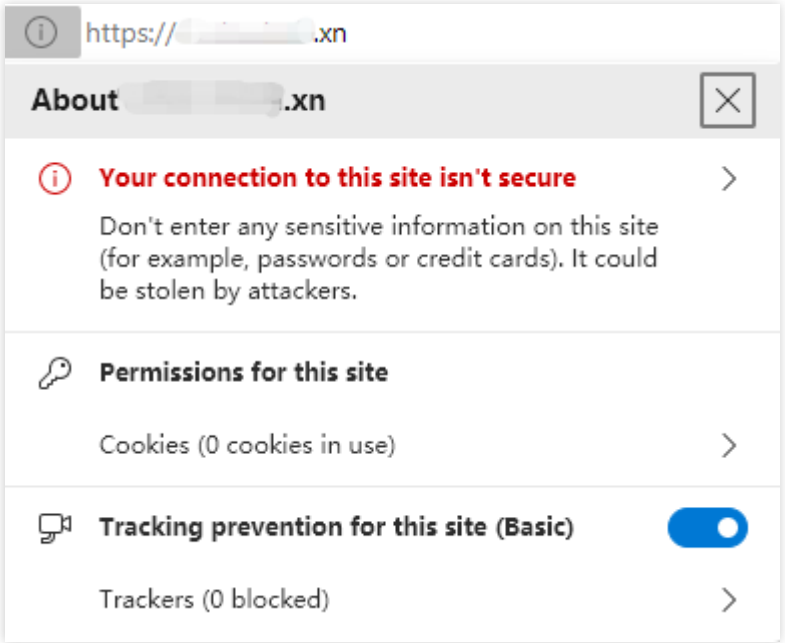
最近更新时间：2024-03-06 17:56:24

现象描述

部署 SSL 证书后，使用 HTTPS 协议访问网站，浏览器地址栏中域名前显示

图标和 “不安全” 字样。单击

，将提示红字警告 “你与此网站之间建立的连接不安全”。



可能原因

SSL 证书过期：为了确保私钥安全，SSL 证书均存在有效期限，最新的国际标准 SSL 证书最长有效期为1年。如 SSL 证书过了有效期，没有及时替换新证书，网站会出现红色 “不安全” 警告。

网页存在不安全因素：网站已经部署 SSL 证书，但是网页中调用了非 HTTPS 的外部资源（图片或 js）时，网站会存在不安全因素，对这类情况，网站浏览器也会标记 “你与此网站之间建立的连接不安全”，如果用户选择加载不安全内容，浏览器就会升级为红色 “不安全” 警告。

解决办法

SSL 证书过期

请尽快替换已过期 SSL 证书，重新申请新证书并安装部署至网站服务器上，您可以参考以下文档进行操作：
1. 如何选择 SSL 证书安装部署类型？

网页存在不安全因素

可以将外链复制到 URL 中，并通过在 http 后添加 “s” 进行访问，测试此外链是否支持 https 协议的链接。
若可以访问，请直接在代码中修改 http 为 https 的链接。
若不可以访问，则可以下载该资源到本地服务器上，并修改资源路径指向到服务器上，并使用相对路径如 `image/button.gif` 或者完整的 https 路径如 `https://***/image/button.gif` 。

上传证书时提示 “解析失败，请检查证书是否符合标准”

最近更新时间：2024-03-06 17:56:24

现象描述

在 SSL 证书管理控制台 上传第三方 SSL 证书时提示 “解析失败，请检查证书是否符合标准”。

可能原因

原因1：上传的证书格式错误。
原因2：上传的证书链不完整。
原因3：因证书格式校验，需删除多余空格。

解决办法

上传的证书格式错误

请检查上传的证书格式是否正确。
证书文件以 “-----BEGIN CERTIFICATE-----” 开头，以 “-----END CERTIFICATE-----” 结尾。
私钥格式以 “-----BEGIN (RSA) PRIVATE KEY-----” 开头，以 “-----END (RSA) PRIVATE KEY-----” 结尾。

上传的证书链不完整

请检查上传的证书链是否完整，详情请参考 如何补全 SSL 证书链。

因证书格式校验，需删除多余空格

请检查上传的证书内容是否包含多余空格。

域名在西部数码进行托管，自动 DNS 验证无法验证

最近更新时间：2024-03-06 17:56:24

现象描述

域名在西部数码进行托管，选择自动 DNS 验证未验证通过。

解决办法

因西部数码 DNS 服务器目前添加域名的 TXT 记录值无法进行验证，不会自动跳转 CNAME 验证，导致托管在西部数码的域名无法验证所有权。

您可以参考以下两种方式进行处理：

您可以将域名的 DNS 服务器地址指向腾讯云 DNS 服务器地址并在腾讯云进行解析。

说明：

DNS 解析 DNSPod 不同解析套餐对应的 DNS 地址不同。

使用自动文件验证进行域名所有权验证。

IIS 下设置 https 主机名灰色无法编辑

最近更新时间：2024-03-06 17:56:24

现象描述

使用 IIS 管理器进行安装证书时，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，主机名显示无法编辑。

可能原因

Windows Server 2008不支持该操作，需要修改对应文件。

解决办法

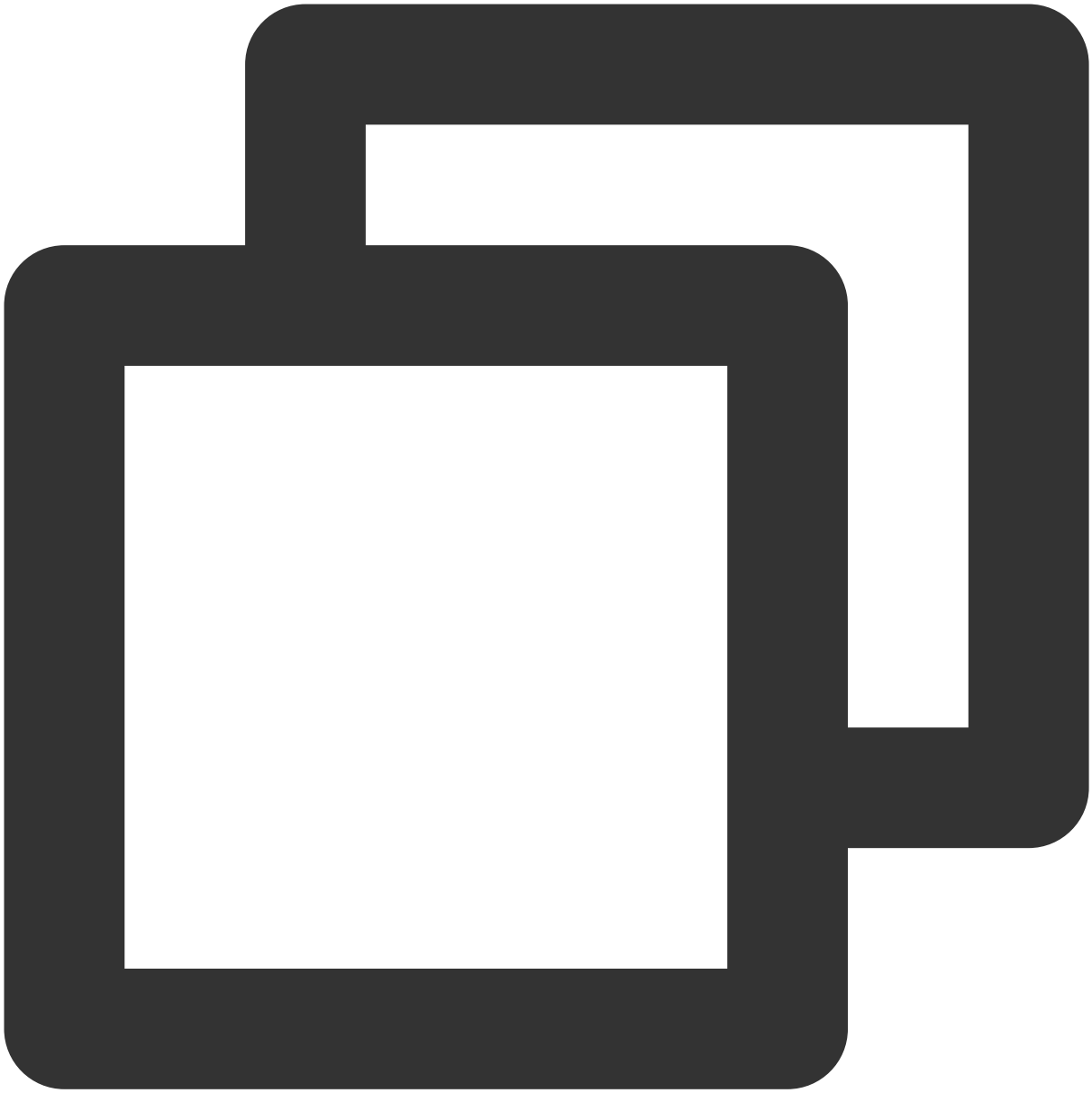
1. 请按路径 `C:\\Windows\\system32\\inetsrv\\config\\applicationHost.config` 打开 `applicationHost.config` 文件。
2. 修改内容如下：

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。

IIS 部署免费 SSL 证书提示证书链中的一个或多个中间证书丢失

最近更新时间：2024-03-06 17:56:24

现象描述

IIS Web 服务部署免费 SSL 证书时提示 “证书链中的一个或多个中间证书丢失，要解决此问题，请确保安装了所有中间证书”。

可能原因

中间证书缺失。

解决办法

步骤1：查看证书加密算法

登录腾讯云 SSL 证书控制台，查看您的证书加密算法类型。

步骤2：下载中间证书文件

根据您的证书加密算法类型下载中间证书至您的云服务器中。
RSA 加密算法类型：单击下载。
ECC 加密算法类型：单击下载。

步骤3：安装中间证书

1. 在您需要部署证书的服务器上，双击中间证书文件并在打开的窗口中单击**安装证书**。
2. 在证书导入向导中存储位置选择**本地计算机**，并单击**下一页**。
3. 证书存储选择**将所有的证书都放入下列存储 > 中间证书颁发机构**，并单击**下一页**。
4. 确认您安装的证书位置是否正确，并单击**完成**。
5. 显示 “导入成功” 即可完成设置，请再次尝试部署您的 SSL 证书。