

内容分发网络

工具说明

产品文档



腾讯云

【版权声明】

©2013-2019 腾讯云版权所有

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

【商标声明】

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

【服务声明】

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

文档目录

工具说明

诊断工具

节点 IP 归属查询

自助故障诊断

高级工具

证书管理

流量包管理

工具说明

诊断工具

节点 IP 归属查询

最近更新时间：2019-08-21 16:20:21

CDN 为您提供了节点 IP 归属查询工具。您可以通过本工具验证指定的 IP 是否为腾讯云 CDN 节点的 IP，详细操作步骤如下：

1. 登录 [CDN 控制台](#)。
2. 在左侧菜单中，选择【诊断工具】>【节点 IP 归属查询】，进入管理页面。



CDN节点IP归属查询

节点IP验证

请输入要查询的IP，一行一个，最多可一次性查询20个

验证

验证指定的 IP 是否为腾讯云 CDN 节点，支持 IPv6 地址查询

3. 在文本框中输入要查询的 IP，一行一个，最多可一次性查询20个，输入完成后，单击【验证】，得到如下结果：

- 若 IP 为 CDN 节点 IP，显示具体归属地。

CDN节点IP归属查询

节点IP验证

[验证](#)

验证指定的IP是否为腾讯云CDN节点的IP

IP	是否为腾讯云CDN节点	归属地
119.147.33.102	是	广东

- 若 IP 为非 CDN 节点 IP，显示归属地未知。

CDN节点IP归属查询

节点IP验证

[验证](#)

验证指定的IP是否为腾讯云CDN节点的IP

IP	是否为腾讯云CDN节点	归属地
	否	未知

自助故障诊断

最近更新时间：2019-07-15 15:48:25

CDN 为您提供了自助故障诊断工具，当发现某 URL 出现访问异常时，本工具能够帮助您进行自助检测，自助检测过程包括了接入域名的 DNS 解析探测、链路质量探测、节点状态探测、源站探测、数据访问一致性等一系列诊断项，帮助您定位问题，并给您提供解决建议。

⚠ 注意：

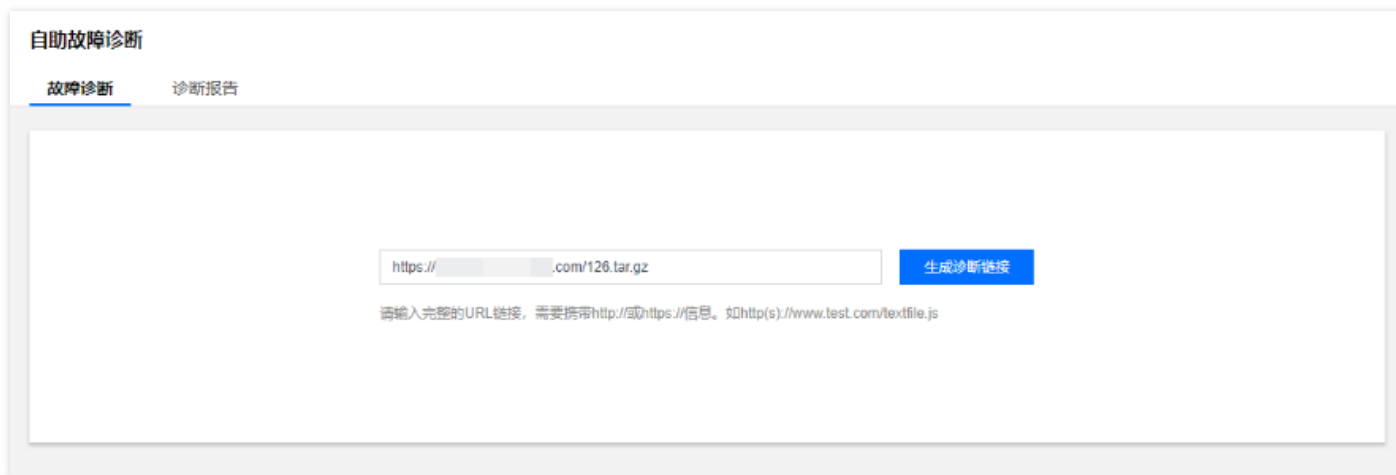
诊断的资源 URL 需要是您的账号下接入的状态为**已启动**的域名。诊断中产生的带宽将计入计费带宽，我们建议您诊断的目标资源不超过200MBytes。

故障诊断

诊断流程

当发现某个资源 URL 出现访问异常时，您可以通过**故障诊断**发起检测。步骤如下：

1. 登录 [CDN 控制台](#)，在左侧菜单中，单击【**诊断工具**】>【**自助故障诊断**】。
2. 在“故障诊断”页面中，输入您需要诊断的异常 URL，URL 需输入 `http://` 或 `https://` 前缀。



3. 输入 URL 后，单击【生成诊断链接】，页面将出现诊断链接地址。



4. 单击诊断链接后，将会新打开诊断页面，并开始收集诊断信息（请不要在诊断过程中关闭检测页面，诊断结束后可以手动关闭此页面）。



5. 您也可以将诊断链接发送给他人进行本地故障检测，检测完成后，需要手动关闭浏览器页面。

⚠ 注意：

- 每一条 URL 生成的诊断链接有效时间为24小时，最多可以单击10次故障诊断。
- 可以在"诊断报告"页面重新复制已经生成的可用诊断链接。

诊断报告

报告查看

1. 诊断完成后，单击【诊断报告】进入页面，可以看到已经产生的诊断报告按时间顺序展示在表格中，列表依次展示了：

- 生成诊断链接的 URL。
- URL 对应的诊断链接。
- 诊断链接的生成时间。
- 诊断链接的失效时间。
- 诊断链接可用诊断次数。

自助故障诊断

故障诊断 诊断报告

请输入检测的URL搜索 🔍 ↻

诊断URL	诊断链接	生成时间 ⚙	失效时间 ⓘ	剩余诊断次数 ⓘ	操作
▶ https://[redacted].	诊断链接 📄	2019-05-27 16:55:12	2019-05-28 16:55:12	5	展开
▶ https://[redacted].	诊断链接	2019-05-27 15:34:36	2019-05-28 15:34:36	0	展开
▶ https://[redacted].	诊断链接 📄	2019-05-27 15:15:06	2019-05-28 15:15:06	8	展开
▶ https://[redacted].	诊断链接 📄	2019-05-27 15:03:53	2019-05-28 15:03:53	8	展开
▶ https://[redacted].	诊断链接 📄	2019-05-27 10:50:59	2019-05-28 10:50:59	2	展开

2. 在操作栏单击【展开】，可以查看每一次诊断产生的报告及其结果。

诊断URL	诊断链接	生成时间	失效时间	剩余诊断次数	操作
▶ https://diagnos[redacted]	诊断链接	2019-05-27 17:29:10	2019-05-28 17:29:10	9	展开
▼ https://diagnos[redacted]	诊断链接	2019-05-27 16:55:12	2019-05-28 16:55:12	5	收起

客户端IP	所在区域	检测时间	检测结果	报告详情
14 [redacted]	广东省-中国电信	2019-05-27 17:08:36	正常	查看报告
14 [redacted]	广东省-中国电信	2019-05-27 17:02:30	正常	查看报告
	-	2019-05-27 16:57:56	诊断页面异常关闭	查看报告
14 [redacted]	广东省-中国电信	2019-05-27 16:57:49	正常	查看报告
1 [redacted]	广东省-中国电信	2019-05-27 16:55:17	正常	查看报告

3. 根据每一个步骤的检测，诊断报告会整体判定为：

- 正常。
- 异常。
- 诊断页面异常关闭（大多为诊断未完成时关闭诊断页面导致）。

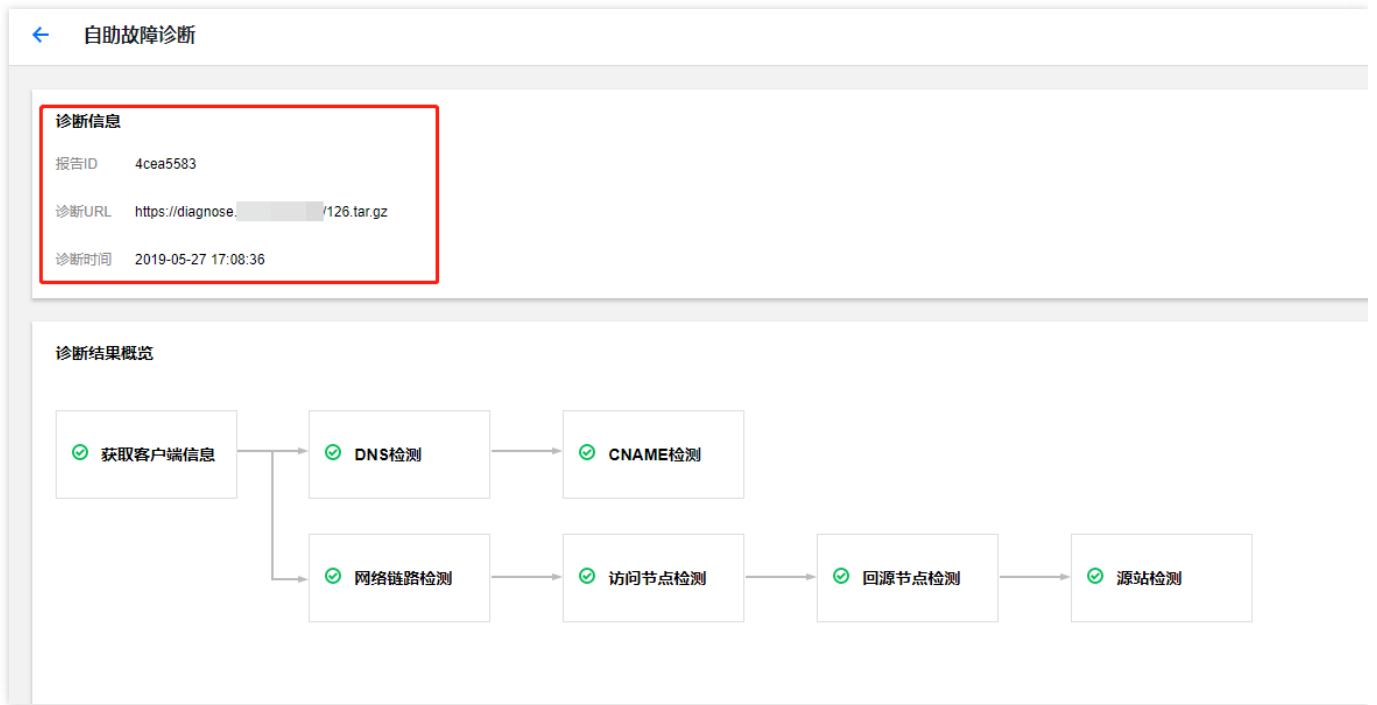
4. 单击右侧【查看报告】，可以看到更多诊断详情，以及异常情况的处理建议。

报告解读

1. 报告的第一部分，用于展示诊断信息，包含：

- 诊断报告 ID。
- 需要诊断的 URL。

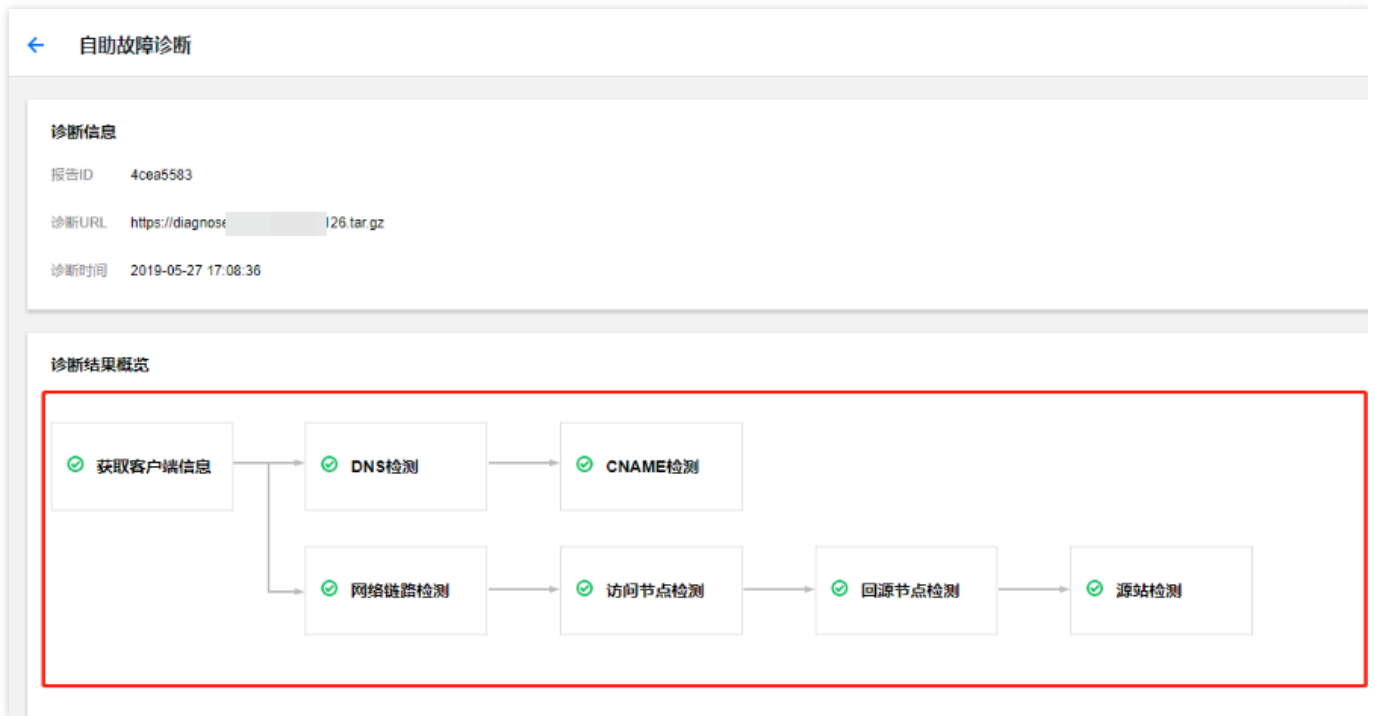
- 触发诊断的时间。



2. 报告的第二部分，针对诊断流程及每一个模块的结果进行了概览介绍，可以直观地发现异常模块，诊断模块包含：

- 客户端信息检测结果。
- DNS 检测结果。
- CNAME 检测结果。
- 网络链路检测结果。
- 访问节点检测结果。
- 回源节点检测结果。

- 源站检测结果。



3. 报告的第三部分针对诊断结果进行了详细说明：

第一项：客户端信息

获取的客户端 IP 信息、对应的省份/运营商，以及发起 Http/Https 请求的 User-Agent、Referer、Request Mode 等信息。若未成功获取客户端信息，则后续部分检测将无法进行。

第二项：DNS 检测

获取客户端本地 DNS IP，通过客户端 IP 与 DNS IP 归属是否一致，可判定是否由于本地 DNS 配置异常，导致无法调度至最优加速节点。

诊断结果详情	
诊断项	操作
▼ ✔ 获取客户信息	展开
▼ ✔ DNS检测	收起
DNS IP ██████ 广东省-中国电信 ██████ 广东省-中国电信 ██████ 广东省-中国电信	

第三项：CNAME 检测

获取检测域名 CNAME 配置，域名的 CNAME 解析需要配置为正确的 *.cdn.dnsv1.com（默认）后缀域名，否则请求将无法到达 CDN 节点。

诊断结果详情	
诊断项	操作
▼ ✔ 获取客户信息	展开
▼ ✔ DNS检测	展开
▼ ✔ CNAME检测	收起
解析配置 CNAME diagnose ██████ :cdn.dnsv1.com	

注意：

CNAME 配置未检查通过，请求不会到达节点，将不会进行后续检测。

第四项：网络链路检测

通过客户端本地探测多个互网站点，获取客户端网络状态。若由于本地代理等配置导致站点无法访问，会导致网络链路检测失败，无法进行后续检测。

诊断结果详情	
诊断项	操作
▼ ✔ 获取客户信息	展开
▼ ✔ DNS检测	展开
▼ ✔ CNAME检测	展开
▼ ✔ 网络链路检测	收起
探测延迟 76ms	

第五项：访问节点探测

客户端发起请求后，到达的 CDN 节点信息采集，包含节点 IP、节点省份/运营商、以及节点返回的状态码、命中状态及资源 MD5：

- 若节点已缓存此资源，将直接命中，不会进行回源节点检测。
- 若节点未命中，继续进行后续回源节点检测。
- 若 URL 反馈的状态码为301、302、504 时，无法正常获取节点检测信息，无法进行后续检测。
- 若域名配置访问控制策略，访问节点会直接返回403，命中情况为**已命中**。

▼ ✔ 网络链路检测	展开
▼ ✔ 访问节点检测	收起
节点IP ██████████	
所在区域 广东-电信	
状态码 200	
文件MD5 8c7d81e ██████████ 138aff	
命中情况 节点命中	

第六项：回源节点检测

- 当资源由 CDN 节点直接返回，此时访问节点与回源节点的命中状态均为**已命中**，CDN 会继续进行源站检测，方便校验源站返回状态码及内容是否与节点保持一致。

▼ ✔ 回源节点检测
收起

命中情况 访问节点已命中

▼ ✔ 源站检测
收起

源站IP 1 [redacted]

所在区域 广东省-腾讯网络

回源host diagnose [redacted]

状态码 200

文件MD5 8c7d81a [redacted] 25138aff

ii. 当资源不由 CDN 节点直接返回，此时访问节点与回源节点状态均为**未命中**，此时内容由源站返回：

▼ ✔ 回源节点检测
收起

节点IP 5 [redacted]

所在区域 广东-电信

命中情况 节点未命中

▼ ✔ 源站检测
收起

源站IP 1 [redacted]

所在区域 重庆市-中国电信

回源host [redacted] coscq.myqcloud.com

状态码 200

文件MD5 4d3afa931 [redacted] fe2823

iii. 此时若产生异常状态码，您可以通过对比源站状态码、文件 MD5 与访问节点模块返回的状态码、文件 MD5，判断异常是由 CDN 节点产生还是由源站产生，进行修复。

① 说明：

若诊断报告无法解决您的问题，我们建议您 [提交工单](#)，或联系腾讯云技术人员排查问题。

高级工具

证书管理

最近更新时间：2019-08-21 16:17:16

您可以对已经接入 CDN 的域名进行 HTTPS 证书配置。CDN 支持配置您已有的证书，或腾讯云 [SSL 证书管理](#) 控制台中托管或颁发的证书。

说明：

证书过期前30天、前15天、前7天及过期当天腾讯云都会以短信、邮件、站内信形式向用户账号发送到期提醒。现已支持SSL证书自定义告警接收人，您可进入 [消息订阅](#) 配置。

证书及私钥

若您要为您的域名配置已有证书，请先了解以下内容。



说明：

若您配置的是腾讯云 [SSL 证书管理](#) 控制台中托管或颁发的证书，可跳过此部分内容，直接查阅后文 [配置证书](#) 流程。

CA 机构提供的证书一般包括以下几种，其中 CDN 使用的是 **Nginx**。

 Apache	2017/8/9 10:46	文件夹
 IIS	2017/8/9 10:46	文件夹
 Nginx	2017/8/9 10:46	文件夹
 Tomcat	2017/8/9 10:46	文件夹

进入 Nginx 文件夹，使用文本编辑器打开 “.cert”（证书）文件和 “.key”（私钥）文件，即可看到 PEM 格式的证书内容及私钥内容。

 1_ [redacted] .cert	2017/8/7 9:16	安全证书	4 KB
 2_ [redacted] .key	2017/8/7 9:16	KEY 文件	2 KB

证书

证书扩展名一般为“.pem”，“.crt”或“.cer”，在文本编辑器中打开证书文件，可以看到与下图格式相似的证书内容。

证书 PEM 格式：以“-----BEGIN CERTIFICATE-----”作为开头，“-----END CERTIFICATE-----”作为结尾。中间的内容每行 64 字符，最后一行长度可以不足 64 字符。

```
-----BEGIN CERTIFICATE-----
MIIE+TCCA+GgAwIBAgIQU306HIX4KsioTW1s2A2krTANBgkqhkiG9w0BAQUFADCB
tTELMakGA1UEBhMCVVMxZzZ4ZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZl
ExZWZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZl
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYS0AYykw0TEvMC0GA1UEAxMm
VmVyaVNPZ24gQ2xhc3MgMyBTZW51cmUgU2VydMvYIENBIC0gRzIwHhcNMTA4MDA4
MDAwMDAwHhcNMTA4MDA3MjM1OTU5WjBqMQswCQYDVQGEwJVUzETMBEGA1UECBMK
V2FzaGluZ3Rvb3RlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZl
bSBjbmMuMR0wGAYDVQQDDBFpYW0uYW1hem9uYXZzLmNvbTCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwGykCgYEA3Xb0EGea2d8QGEUwLcEpwvGawEkUdLZmGL1rQJZdeeN
3vaF+zTm8Qw5Adk2Gr/RwYXtpx04xvQXmNm+9YmksHmCZdruCrW1eN/P9w8fqMMZ
X964CjVov3NrF5AuxU8jgtw0yu//C3hWn0uIVGdg76626gg0oJSaj48R2n0MnVcC
AwEAAaOCAdEwggHNAkGA1UdEwQCAAwCwYDVR0PBAQDAgWgMEUGA1UdHwQ+MDww
OqA4oDaGNGh0dHA6Ly9TVlJTZW51cmUuRzIuY3J5LnZlcm1zaWduLmNvbS9TVlJT
ZW51cmVHMj5jcmwwRAYDVR0gBD0wOzA5BgtghkgBhvhFAQCXAqMCgGCCsGAQUF
BwIBFhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMB0GA1UdJQ0wMmBQGCCsG
AQUFBwMBBggrBgEFBQcDAjAFBgNVHSMEGDAWgBS17wsRzsBBA6NKZ2BIshzgVy19
RzB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGGh0dHA6Ly9vY3NwLnZlcm1z
aWduLmNvbTBABggrBgEFBQcAwAoY0aHR0cDovL1NWU1N1Y3VyZS1HMi1haWEudmVy
aXNpZ24uY29tL1NWU1N1Y3VyZUcyLmN1cjBuBggrBgEFBQcBDARiMGChXqBcMFow
WDBWFglpbWFnZS9naWYwITAFMacGBS0AwIaBBRLa7koLgYMu9BS0JsprEsHiyEF
GDAmFiRodHRwOi8vbG9nb3552ZXJpc2lnbi5jb20vdmNsb2dvMSSnaWYwDQYJKoZI
hvcNAQEFBQADggEBALpFBXeG782QsTtGwEE9zBcVCuKjrs13dWK1dFiq30P4y/Bi
ZBYEywBt8zNuYFUE25Uub/zmvmp7p0G76tmQ8bRp/4qkJoISesHJvFgJ1mksr3IQ
3gaE1aN2BSUThxGLn9N4F09hYwwbeEzAcxfBilLdEiodNwzcvGJ+2LlDWGJ0GrNI
NM856xjqhJCPxYzk9buuCl1B4Kzu0CTbexz/iEgYV+DiuTxcFA4uhwMDSe0nynbn
1qiwrk450mC0nqH4ly4P4lXo02t4A/DI1I8Znct/QfL69a2L f6vc9rF7BELT0e5Y
R7CKx7Fc5xRaeQdyGj/dJevm9BF/mSdncLS5vas=
-----END CERTIFICATE-----
```

如果是通过中级 CA 机构颁发的证书，您拿到的证书文件包含多份证书，需要人为地将服务器证书与中间证书拼接在一起上传。拼接规则为：服务器证书放第一份，中间证书放第二份，中间不要有空行。一般情况下，机构在颁发证书的时候会有对应说明，请注意查阅规则说明。

注意：

- 证书之间不能有空行。
- 每一份证书均为 PEM 格式。

中级机构颁发的证书链格式如下：

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



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

私钥

私钥扩展名一般为“.pem”或“.key”，在文本编辑器中打开私钥文件，可以看到与下图格式相似的私钥内容。

私钥 PEM 格式：以“-----BEGIN RSA PRIVATE KEY-----”作为开头，“-----END RSA PRIVATE KEY-----”作为结尾。中间的内容每行 64 字符，最后一行长度可以不足 64 字符。

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAzVSSChH67bmT8mFykAxQ1tKCYukwBiWZwkOStFEBTWHy8K
tTHSFD1u9TL6qycrHEG7cjYD4DK+kVIHU/Of/pUWj9LLnrE3W34DaVzQdKA00I3A
Xw95grqFJMjclva2khNKA1+tNPSCPJoo9DDrP7wx7cQx7LbMb0dfz8858KIoluzJ
/fD0XyuWoqaIePZtK9Qnjin957ZEPHjtUpVZuhS3409DDM/tJ3T18aaNYWhrPBc0
jNcz0Z6XQGf1rZG/Ve520GX6rb5dUYpdcfXzN5MM6xYg8a1L7UHDHHPi4AYsatdG
z5TmPnmEfyZPUYudTLxgMVAovJr09Dq+SDm3QIDAQAABaoIBAGl68Z/nnFyRHrFi
LaF6+Wen8ZvNqkm0hAMQwIjH1Vp1fL74//8Qyea/EvUtuJHyB6T/2PZQoNVhxe35
cgQ93Tx424WgpCwUshSfxewfbAYGf3ur8W0xq0uU07BAxaKHncmNG7dGyo1UowRu
S+yXLrpVzH1YkuH8TT53udd6TeTWi77r8dkGi9KSAZ0pRa19B7t+CHKIzm6ybs/2
06W/zHZ4YAxwkTYLKGHjoiEys111ah1AJvICVgTc3+LzG2pIpM7I+K0nHC5eswvM
i5x9h/OT/ujZsyX9P0PaAyE2bqy0t080tGexM076Ssv0KVhKfVwJLUnhf6WcqFCD
xqhxkECgYEA+PftNb6eyX1+/Y/U8NM2fg3+rSCms0j9Bg+9+yZzF5GhagHu0edU
ZXIhrJ9u6B1XE1arpijVs/WHmFhYSTm6DbdD7S1tLy0BY4cPTRhziFTKt8AkIXMK
605u0UiWsq0Z8hn1X141ox2cW9ZQa/HC9udeyQotP4NsMJWgpBV7tC0CgYEAwvNf
0f+/jUjt0HoyxCh4SIAqk4U0o4+hBCQbWcXv5qCz4mRyTaWzFEG8/AR3Md2rhmZi
GnJ5fdfe7uY+JsQfX2Q5JjwTadlBW4led0Sa/uKRa04UzVgnYp2aJKxtuWffvVbU
+kf728JRA6azSLvGmA8hu/GL6bgfU3fkSkw03ECgYBpYK7TT7JvvnAErMtJf2yS
ICRkbQaB3gPSe/lCgzy1nhtaFOUbNxEuowLAZR0wrz7X3TZqHEDcYoJ7mK346of
QhGLITyoehkbYkAUtq038Y04EKH6S/IzMzB0frXiPKg9s8UKQzkU+GSE7ootli+a
R8Xzu835EwxI6BwNN1abpQKBgQC8TialClq1FteXQyGcNdcReLMncUHKIKcP/+xn
R3kV106MZCFAdqirAjiQWaPkh9Bxbp2eHCrB81MFAWLRQSlOk79b/jVmTZMC3upd
EJ/iSWjZKpBw7hCFARtPhxyNTJ5idEiu9U8EQid8111giPgn0p3sE0HpDI89qZX
aaiMEQKBgQDK2bsnzE9y0ZWhGTeu94vziKmFrSkJMGH8pLaTiliwiRhRYWJysZ9
BOIDxnrmwiPa9bCtEpK80zq28dq7qxpCs9CavQRcv0Bh5Hx0yy23m9hFRzfDeQ7z
NTKh193HHF1joNM81LHFyGRFEWrrroW5gfBudR6USRnr/6iQ11xZXw==
-----END RSA PRIVATE KEY-----
```

如果您得到的是以“-----BEGIN PRIVATE KEY-----”作为开头，“-----END PRIVATE KEY-----”作为结尾的私钥，建议您通过 openssl 工具进行格式转换，命令如下。

```
openssl rsa -in old_server_key.pem -out new_server_key.pem
```

配置证书

1. 登录 [CDN 控制台](#)，在左侧菜单栏【高级工具】下单击【证书管理】进入管理页面。

2. 单击【配置证书】进入配置证书页面。

配置证书	批量配置	域名	证书备注	证书来源	到期时间 ↑	回源方式
		te: [模糊]		腾讯云默认证书	-	HTTP回源
		e: [模糊]		腾讯云默认证书	-	HTTP回源

选择域名

在【域名】下拉菜单中选择您要配置证书的域名。

← 配置证书

您配置证书的域名需要已接入腾讯云CDN，且域名状态需要处于部署中或已启动。

选择要配置证书的域名

域名

注意：

- 配置证书的域名需要已接入腾讯云 CDN，且域名状态为**部署中**或**已启动**。**已关闭**状态的域名无法部署证书。
- 使用腾讯云**对象存储**或**万象优图**服务开启 CDN 加速后，默认的 `.file.myqcloud.com` 或 `.image.myqcloud.com` 域名无法配置证书。

选择证书

您可以选择使用自有证书或腾讯云托管证书。

自有证书

选中【自有证书】，将证书内容、私钥内容粘贴入对文本框，您可以给证书添加备注信息以便区分。

← 配置证书

您配置证书的域名需要已接入腾讯云CDN，且域名状态需要处于部署中或已启动。

选择要配置证书的域名

域名

选择证书

证书来源



自有证书



腾讯云托管证书

证书内容

```
-----BEGIN CERTIFICATE-----  
cQzfhiiG7ASjiPakw5wXoycHt5GCvLG5htp2TKVzgv9QT  
liA3gtfv6oV4zRZx7X1  
Ofi6hVgErtHaXJheuPVeW6eAW8mHBoEfvDAfU3y9wa  
YrtUevSl07643bzKL6v+Qd  
DUBTx0AvSYfXTtI90EAxEG/bJJyOm5LqoiA=  
-----END CERTIFICATE-----
```

[查看样例](#)

私钥内容

```
-----BEGIN RSA PRIVATE KEY-----  
9DzQ5NkPkTCJi0sqbl8/03IUKTgT6hcbpWdDXa7m8J3  
wRr3o5nUB+TPQ5nzAbthM  
zWX931YQeACcwhxvHQJBAN5mTzzJD4w4Ma6YTaN  
HyXakdYfyAWrOkPIWZxfhMfXe  
DrINdiysTI4Dd1dLeErVpjsckAaOW/JDG5PCSwkaMxk=  
-----END RSA PRIVATE KEY-----
```

[查看样例](#)

备注(选填)

请填写备注信息

注意：

- 证书内容需要为 PEM 格式，非此格式证书请参考后文 [PEM 格式转换](#)。

- 当您的证书有证书链时，请将证书链内容，转化为 PEM 格式内容，与证书内容合并上传，证书链补齐问题请参见后文[证书链补齐](#)。

腾讯云托管证书

您可以登录 [SSL 证书管理](#) 控制台，申请由亚洲诚信免费提供的第三方证书，或是将已有证书托管至腾讯云。

选中【腾讯云托管证书】，即可看到该域名可用的证书列表。从证书列表中选择要使用的证书，证书列表中展示格式为“证书 ID（备注）”。

← 配置证书

您配置证书的域名需要已接入腾讯云CDN，且域名状态需要处于部署中或已启动。

选择要配置证书的域名

域名

选择证书

证书来源 自有证书 腾讯云托管证书

点击 [SSL证书管理](#) 查看托管证书详情，您可以在SSL证书管理页面申请免费证书。

证书列表

回源方式

配置证书后，您可以选择 CDN 节点回源站获取资源时的回源方式，CDN 支持 **HTTP** 和**协议回源**两种回源方式。

选择证书

证书来源 自有证书 腾讯云托管证书
点击 [SSL证书管理](#) 查看托管证书详情，您可以在SSL证书管理

证书列表

选择回源方式

回源方式 HTTP 协议跟随
您的源站需要部署有效证书，否则会导致回源失败。

注意：

- 选择 **HTTP** 回源配置成功后，用户至 CDN 节点请求支持 HTTPS/HTTP，CDN 节点回源站请求均为 HTTP。
- 选择**协议跟随**回源配置，您的源站需要部署有效证书，否则将导致回源失败。配置成功后，用户至 CDN 节点请求为 HTTP 时，CDN 节点回源请求也为 HTTP。用户至 CDN 节点请求为 HTTPS 时，CDN 节点回源请求也为 HTTPS。
- 若域名源站修改 HTTPS 端口为非 443 端口，会导致配置失败。
- COS 源或 FTP 源域名仅支持 HTTP 回源。

配置成功

单击【提交】，您可以在【证书管理】页面看到已经配置成功的域名及证书信息。

证书管理

• 若您已有证书，可直接上传进行配置，同时可以在本页面对证书进行无缝切换、删除等操作；
 • 您可以前往 [SSL证书管理](#) 免费申请由亚洲诚信提供的DV SSL证书。

域名	证书备注	证书来源	到期时间 ↑	回源方式	证书状态	操作
		腾讯云托管证书	2019-09-23 20:00:00	HTTP回源	配置成功	编辑 删除

批量配置证书

若您拥有多域名证书或泛域名证书，可适用于多个 CDN 加速域名，您可以通过批量配置，一次性为多个域名添加配置。

1. 登录 [CDN 控制台](#)，在左侧菜单栏【高级工具】下单击【证书管理】进入管理页面。
2. 单击【批量配置】进入批量管理页面。

域名	证书备注	证书来源	到期时间 ↑	回源方式
te		腾讯云默认证书	-	HTTP回源
e:		腾讯云默认证书	-	HTTP回源

上传证书

将 PEM 编码的证书内容和私钥贴在页面对应文本框中，您可以通过修改备注名标识配置的证书，完成后单击【下一步】。

← 批量管理

- 1 上传证书 > 2 关联域名、选择回源方式 > 3 完成

- 根据您上传的证书，CDN为您筛选出可使用该证书的加速域名，您可以根据需要进行勾选；
- 状态为部署中或已启动的加速域名才能够进行证书配置。

证书来源 自有证书 腾讯云托管证书

点击 [SSL证书管理](#) 查看托管证书详情，您可以在SSL证书管理页面申请免费证书。

证书内容

```
-----BEGIN CERTIFICATE-----
MIICXzCCBgkqhkiG9w0BBQwwFQ0xHZAQwEgYKCZgcggKAgQw
cQzfhiiG7ASjiPakw5wXoycHt5GCvLG5htp2TKVzgv9QT
liA3gtfv6oV4zRZx7X1
Ofi6hVgErtHaXJheuPVeW6eAW8mHBoEfvDAfU3y9wa
YrtUevSI07643bzKL6v+Qd
DUBTxOAvSYfXTtI90EAxEG/bJJyOm5LqoiA=
-----END CERTIFICATE-----
```

[查看样例](#)

私钥内容

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA9DzQ5NkPkTCJi0sqbl8/03lUKTgT6hcbpWdDXa7m8J3
wRr3o5nUB+TPQ5nzAbthM
zWX931YQeACcwhxvHqJBAN5mTzzJD4w4Ma6YTaN
HyXakdYfyAWrOkPIWZxfhMfXe
DrlNdiysTI4Dd1dLeErVpjsckAaOW/JDG5PCSwkaMxk=
-----END RSA PRIVATE KEY-----
```

[查看样例](#)

备注(选填)

下一步

关联域名和选择回源方式

CDN 系统会识别出可使用您上传证书的 CDN 加速域名（域名状态需要为**部署中**或**已启动**），您可以勾选需要关联的域名及选择回源方式。

选择关联域名

关联域名 仅显示已配置证书域名

<input type="checkbox"/>	域名	证书状态	到期时间
暂无可用域名。			
已选 0 项，共 0 项			

选择回源方式

回源方式 HTTP 协议跟随

注意：

- 一次最多可勾选10个加速域名进行配置。
- 选择 **HTTP** 回源配置成功后，用户至 CDN 节点请求支持 HTTPS/HTTP，CDN 节点回源站请求均为 HTTP。
- 选择 **HTTPS** 回源配置，您的源站需要部署有效证书，否则将导致回源失败。配置成功后，用户至 CDN 节点请求为 HTTP 时，CDN 节点回源请求也为 HTTP。用户至 CDN 节点请求为 HTTPS 时，CDN 节点回源

请求也为 HTTPS。

- 若批量勾选的域名中，有源站修改 HTTPS 端口为非 443 端口，会导致配置失败。
- 若批量勾选的域名中存在 COS 源或 FTP 源的域名，仅支持 HTTP 回源。

提交配置

单击【提交】，CDN 会对所选域名配置证书，每一个域名配置需要5分钟左右，请耐心等待。您可以在【证书管理】页面查看证书配置状态。

注意：

- 若配置失败，您可以通过单击域名右侧的【编辑】按钮，重新进行证书配置。
- 若批量配置的域名中存在已配置了证书的域名，则该操作会覆盖域名原有证书，若覆盖失败，该域名的证书状态会变为【更新失败】。此时原来配置的证书仍然有效，您可以通过单击域名右侧的【编辑】按钮，重新进行覆盖操作。

编辑证书

对于已经配置成功的证书，您可以通过单击域名右侧的【编辑】按钮更新证书。

← 编辑证书

选择要配置证书的域名

域名

选择证书

证书来源 自有证书 腾讯云托管证书

点击 [SSL证书管理](#) 查看托管证书详情，您可以在SSL证书管理页面申请免费证书。

证书列表

选择回源方式

回源方式 HTTP 协议跟随

提交

您可以在自有证书和腾讯云托管证书之间进行切换，以及重新选择回源方式。单击【提交】即可完成部署。部署过

程为无缝覆盖，不会影响您的业务使用。

选择证书

证书来源 自有证书 腾讯云托管证书

点击 [SSL证书管理](#) 查看托管证书详情，您可以在SSL证书管理页面申请免费证书。

证书列表

无可用证书

选择回源方式

回源方式

HTTP 协议跟随

您的源站需要部署有效证书，否则会导致回源失败。

提交

删除证书

您可以通过单击域名右侧的【删除】按钮，将您部署的证书在 CDN 上删除。

证书管理

- 若您已有证书，可直接上传进行配置，同时可以在本页面证书进行无缝切换、删除等操作；
- 您可以前往 [SSL证书管理](#) 免费申请由亚洲诚信提供的DV SSL证书。

配置证书

批量配置

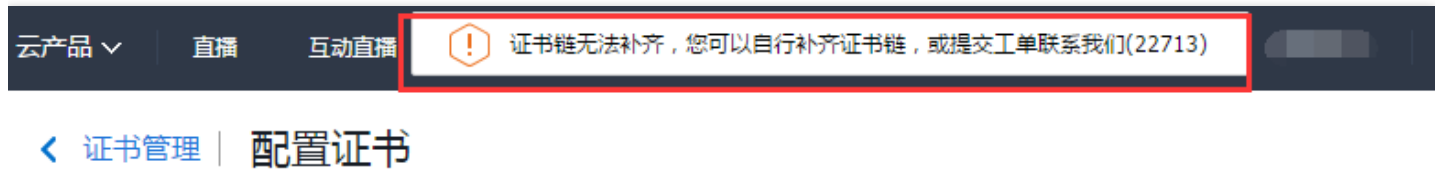
输入域名搜索



域名	证书备注	证书来源	到期时间 ↑	回源方式	证书状态	操作
		腾讯云托管证书	2019-09-23 20:00:00	HTTP回源	配置成功	编辑 删除
		腾讯云托管证书	2019-09-23 20:00:00	HTTP回源	配置成功	编辑 删除

证书链补齐

在使用自有证书配置过程中，可能会出现**证书链无法补齐**的情况，如下图所示。



您可以通过将 CA 的证书（PEM 格式）内容贴入域名证书（PEM 格式）尾部，来补齐证书链。也可以提交工单联系我们。

名称	修改日期	类型	大小
1_root_bundle.crt	2016/11/8 15:07	安全证书	2 KB
2_...com.crt	2016/11/8 15:07	安全证书	3 KB
3_...com.key	2016/11/8 15:07	KEY 文件	4 KB

PEM 格式转换

目前 CDN 只支持 PEM 格式的证书，其他格式的证书需要转换成 PEM 格式，建议通过 openssl 工具进行转换。下面是几种比较流行的证书格式转换为 PEM 格式的方法。

DER 转换为 PEM

DER 格式一般出现在 Java 平台中。

证书转换：

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

私钥转换：

```
openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem
```

P7B 转换为 PEM

P7B 格式一般出现在 Windows Server 和 tomcat 中。

证书转换：

```
openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer
```

用文本编辑器打开 outcertificat.cer 即可查看 PEM 格式的证书内容。

私钥转换：私钥一般在 IIS 服务器里可导出。

PFX 转换为 PEM

PFX 格式一般出现在 Windows Server 中。

证书转换：

```
openssl pkcs12 -in certname.pfx -nokeys -out cert.pem
```

私钥转换：

```
openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes
```

流量包管理

最近更新时间：2019-07-31 11:44:17

若您的计费模式为**流量计费**，您可以购买流量包进行费用抵扣，更加优惠。您可以在 CDN 控制台查看流量包的使用情况，便于您实时了解流量包的剩余状态，及时补充，以免影响您正常使用 CDN 服务。

1. 登录 [CDN 控制台](#)。
2. 在左侧菜单中，选择【高级工具】>【流量包管理】，进入管理页面。
3. 您可以看到现有流量包和已过期流量包的购买情况及使用情况。

流量包管理					购买流量包
我的流量包		已过期			
类型	使用情况	领取/购买时间	到期时间	来源	
日常流量包	已使用：500.00GB(共：500.00GB) 	2018-10-26 11:19	2019-04-26	腾讯云	
日常流量包	已使用：100.00GB(共：100.00GB) 	2018-10-26 11:19	2019-04-26	腾讯云	
COS老用户流量包	已使用：50.00GB(共：50.00GB) 	2019-04-01 01:57	2019-05-01	腾讯云	
赠送流量包	已使用：10.00GB(共：10.00GB) 	2019-04-01 00:26	2019-05-01	腾讯云	