内容分发网络 CDN

配置指南

产品文档

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2022 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】

腾讯云

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。

文档目录

配置指南
域名管理
域名操作
域名检索
复制配置
批量变更配置
域名配置
配置概览
基本配置
基本信息
源站配置
高级回源配置
HTTPS 回源算法说明
访问控制
防盗链配置
IP 黑白名单配置
IP 访问限频配置
视频拖拽配置
鉴权配置
配置说明
TypeA
TypeB
TypeC
TypeD
UA 黑白名单配置
下行限速配置
远程鉴权
境内访问端口配置
缓存配置
缓存键规则配置
节点缓存过期配置
状态码缓存配置
HTTP 头部缓存配置
访问 URL 重写配置
浏览器缓存过期配置

版权所有：腾讯云计算（北京）有限责任公司

缓存配置常见问题
回源配置
分片回源配置
回源301/302跟随
回源超时时间配置
回源 HTTP 请求头配置
回源 URL 重写
回源 SNI
HTTPS 配置
HTTPS 配置须知
HTTPS 配置指南
强制跳转配置
HTTP2.0 配置
OCSP 装订配置
HSTS 配置
TLS 版本配置
QUIC
HTTPS 相关常见问题
高级配置
用量封顶配置
HTTP 响应头配置
SEO 配置
智能压缩配置
自定义错误页面
POST 请求大小配置
WebSocket 配置
图片优化
统计分析
实时监控
面板配置
数据对比
访问监控
回源监控
状态码说明
数据分析
统计分析常见问题
刷新预热
缓存刷新

版权所有：腾讯云计算（北京）有限责任公司

缓存预热
操作记录
刷新预热常见问题
日志服务
日志下载
实时日志
插件中心
概述
APK 动态打包
定时刷新预热
区域访问控制
性能监测
CDN 测速
SaaS 证书
安全加速
服务查询
全网状态监控
流量包管理
IP 归属查询
回源节点查询
自助诊断工具
内容合规
配额管理

配置指南
域名管理
域名操作

最近更新时间：2021-05-06 16:12:00

操作场景

将域名接入腾讯云 CDN 加速服务后，若您需要对已经接入的加速域名进行管理，可以登录 CDN 控制台，在左侧菜单栏选择【域名管理】进入到域名管理页进行相关操作。

腾讯云 CDN 支持自定义调整域名列表、批量开启/关闭域名加速服务和批量变更域名的项目/标签/配置等操作，帮助您高效管理域名。

操作指南

自定义调整列表

单击搜索框右侧 ，打开列表配置弹窗，可指定展示或取消展示某一些域名配置项，且支持调整列表展示顺序。

域名配置导出

单击搜索框右侧的 ，即可导出域名列表中的域名基础配置清单，格式为Excel，每次导出域名上限为1000个。

编辑项目

支持对正常运行的域名变更所属项目。

- 单域名操作：单击域名右侧【更多】操作修改域名所属项目。

- 批量操作：选中多个域名，在上方【更多操作】中点击“编辑项目”。（注：单次最多可选50个域名）

编辑标签

- 单域名操作：单击进入域名，在域名【基本信息】中的“标签”处修改。
- 批量操作：选中多个域名，在上方【更多操作】中点击“编辑标签”。（注：单次最多可选50个域名；变更后非即刻生效，需刷新后查看最新的标签内容）

关闭加速服务

对正常运行的域名，可关闭加速服务。关闭后，全网 CDN 加速节点上域名相关配置会下线，此时若该域名访问仍然到达 CDN 节点，会直接返回404，无法正常服务。故关闭域名前需要确认域名对应的解析已经配置为非腾讯云 CDN 分配的 CNAME 地址。

> ⚠ 注意：
> 域名加速服务完全关闭后，将不再产生任何消耗。

- 单域名操作：单击右侧【更多】操作关闭域名。
- 批量操作：勾选【已启动】状态的域名，在上方【更多操作】中进行批量关闭。

开启加速服务

对已关闭的域名可再次开启加速服务，通过开启加速服务重新将域名配置下发至全网加速节点：

- 单域名操作：若域名状态为【已关闭】，可单击右侧【更多】操作开启域名。
- 批量操作：勾选【已关闭】状态的域名，在上方【更多操作】中进行批量启动。

> ⚠ 注意：
> 已启动状态的域名，若三个月内无任何操作或消耗产生，会被判定为失活域名，腾讯云 CDN 系统会进行自动关闭其加速服务。

删除加速域名

版权所有：腾讯云计算（北京）有限责任公司

仅当域名状态为【已关闭】时才可进行删除操作。删除后域名与其对应的配置将直接清空无法找回，且不再支持其统计数据查看，请谨慎操作：

- 单域名操作：单击右侧【更多】操作删除域名。
- 批量操作：勾选【已关闭】状态的域名，在上方【更多操作】中进行批量删除。

批量变更配置

批量变更配置功能可同时对多个加速域名变更域名配置。当您需要对多个域名变更某项域名配置时，不用再一个一个域名地操作，可使用此功能进行批量操作，提升配置效率。详细说明请查看 批量变更配置。

复制配置

复制配置功能可将存量加速域名的配置复制到一个或多个新添加速域名。您可按需选择某一个存量域名，将其域名配置复制到新添域名上。详细说明请查看 复制配置。

域名检索

最近更新时间：2021-05-19 10:28:51

检索场景

接入腾讯云 CDN 加速服务后，需要根据域名或其指定特性进行筛选列表查看，或根据标签、项目等进行云资源管理。

腾讯云 CDN 支持通过域名、源站、标签和项目等多条件组合查询，支持多关键字筛选。

点击查看视频

> 说明：
> 标签是腾讯云提供的用于标识云上资源的标记，您可以通过 标签，了解并管理标签。

操作指南

开始检索

1. 登录 CDN 控制台，在左侧菜单中单击【域名管理】，进入管理页面。
2. 单击激活域名检索输入框，选择域名、源站、标签及所属项目其中一个或多个资源属性，并输入对应值进行域名检索过滤。

3. 若对输入资源属性或输入格式有疑问，可通过单击【i】图标，获得 检索示例。

检索说明

各检索项说明：

- 域名检索：支持完整域名或部分域名进行模糊匹配，支持单个关键字检索。
- 源站检索：支持完整或部分源站内容进行匹配，支持模糊匹配，当前仅检索主源站，暂不支持备用源站或区域特殊源站配置，支持单个关键字检索。
- 标签检索：输入完整标签名，返回包含输入标签名的域名列表，标签名**不支持模糊检索**。
- 项目检索：支持选择一个或多项目进行筛选。

> ⚠ **注意：**
>
> 未指定检索项时，默认为针对【域名】进行检索，即输入单个关键字时，检索框内容为：域名:www.test.com；黏贴字符时，检索框内容为：域名:test|abc 。

检索能力说明：

- 支持多条件筛选：即选定域名、源站、标签和所属项目其中一个或多个条件共同筛选，当多条件筛选时以回车分隔。
- 支持多关键字筛选：即每个筛选条件允许输入多个关键字，每个关键字之间由“|”分隔。

检索示例

类别	输入格式	例子	搜索框示例	说明
单个关键字	【关键字】	www.test.com	www.test.com	过滤包含字符"www.test.com"的域名。
单域名属性	【属性】:【关键词】	源站：1.1.1.1	源站: 1.1.1.1	过滤源站包含“1.1.1.1”的域名。
多域名属性	【属性】:【关键词】【回车】【属性】:【关键词】	域名：test 源站：1.1.1.1	域名: test 源站: 1.1.1.1	过滤域名包含字符“test”，源站包含“1.1.1.1”的域名。

类别	输入格式	例子	搜索框示例	说明
单域名属性多关键字	【属性】:【关键词】|【关键词】	所属项目：test1|test2	所属项目: test1 | test2	过滤所属项目包含“test1”或“test2”的域名。域名、源站属性暂不支持多关键字检索。
复制字符	（黏贴的字符）	test abc	域名: test | abc	过滤包含字符“test”或“abc”的域名。

复制配置

最近更新时间：2021-05-28 14:51:42

配置场景

复制配置功能支持将存量加速域名的配置复制到一个或多个新添加速域名。您可按需选择某一个存量域名，将其域名配置复制到新添域名上，不用再为新添域名单独一个个地配置控制台的域名配置，更方便快捷地接入域名。

注意：

- 已关闭/已封禁/备案过期/含自有证书/存在不支持的区域差异化历史配置的域名，不支持复制配置功能。
- 若被复制域名存在后端特殊配置（非控制台配置），该特殊配置无法复制。

配置指南

登录 CDN 控制台，在左侧菜单栏选择【域名管理】，单击域名操作列的【复制配置】，即可进入复制配置页面。

您可添加新的加速域名，提交后，当前加速域名的配置将被复制到新添域名上。

说明：

- 提交后无法中断操作，新域名添加成功后，您可正常管理其域名配置。
- 域名添加后会将相关域名配置下发至全网 CDN 加速节点，并不会直接影响您的现网业务。如需正式开启加速，需要进行 CNAME 配置，具体步骤可查看 配置 CNAME。

批量变更配置

最近更新时间：2021-05-28 11:22:25

功能场景

批量变更配置功能支持同时对多个加速域名变更域名配置。当您需要对多个域名变更某项域名配置时，不用再一个一个域名地操作，可使用此功能进行批量操作，提升配置效率。

> 说明：
> 此功能并未覆盖域名的全部配置项，某些配置项还未支持，后续会逐步更新发布。

操作指南

登录 CDN 控制台，在左侧菜单栏选择【域名管理】，进入域名管理页。选中2个及2个以上已启动的域名时，在上方【更多操作】中选择【批量变更配置】，即可进入批量变更配置页面。

域名管理

> 注意：
> - 变更后的新配置将覆盖所选域名对应配置项的原有配置。
> - 已关闭/已封禁/已锁定的域名，不支持批量变更配置功能。
> - 若所选域名存在后端特殊配置（非控制台配置），该特殊配置无法变更。

更多说明

- 配置变更操作不可逆，变更成功后可正常管理域名配置。
- 因一些配置项和加速区域/业务类型/HTTPS 证书配置相关联，建议您选择加速区域/业务类型/HTTPS 配置状态相同的域名进行批量变更。
- 批量变更 HTTPS 证书配置，请前往证书管理页面，此处不支持。
- 单次最多支持同时变更20个域名，域名越多，变更提交下发的时间越长，建议您单次批量变更时不要选择太多域名。

版权所有：腾讯云计算（北京）有限责任公司

域名配置
配置概览

最近更新时间：2021-07-21 14:18:15

配置概览

腾讯云 CDN 在请求的各阶段支持多项自定义配置，您可以根据自身业务需要进行调整。

基本配置

基本配置包括域名的加速服务基本信息，如加速区域、业务类型等，及源站相关配置，为 CDN 加速必须配置的内容。

配置名称	功能说明
基本信息	修改域名所属项目、加速区域、业务类型等基础信息。
源站配置	支持多 IP 轮询回源配置、域名回源、权重回源、回源 Host 设置、回源协议设置。 支持热备源站配置。 **全球加速域名支持境内境外分开配置。**

访问控制

访问控制配置根据用户实际请求内容，配置各类规则进行访问拦截或放行。

配置名称	功能说明
防盗链配置	referer 黑白名单配置，根据访问 HTTP 请求中的 referer 头部，判定是否拒绝/放行请求。 **全球加速域名支持境内境外分开配置。**
IP 黑白名单配置	IP 黑白名单配置，根据访问 HTTP 请求的 Client IP，判定是否拒绝/放行请求。 **全球加速域名支持境内境外分开配置。**
IP 访问限频配置	设置单 IP 单节点访问限频，超出访问频次的 Client IP 发起的请求将直接被拒绝。
鉴权配置	时间戳防盗链配置，支持多种时间戳签名算法及规则。 **全球加速域名支持境内境外分开配置。**
视频拖拽	用于流媒体点播加速场景。 开启视频拖拽功能后，支持通过 start 参数指定视频开始播放位置。

版权所有：腾讯云计算（北京）有限责任公司

配置名称	功能说明
UA 黑白名单配置	UA 黑白名单配置，根据访问 HTTP 请求的 User-Agent 头部，判定是否拒绝/放行请求。
下行限速配置	设置单链接下行限速配置，一定程度上可控制 CDN 访问带宽 。
境内访问端口配置	支持按需关闭80/8080/443访问端口。

缓存配置

缓存配置控制了 CDN 节点的缓存行为。

配置名称	功能说明
缓存键规则配置	设置节点缓存资源时，是否忽略访问 URL ？之后的参数。 **若您的业务通过 URL 后参数代表不同内容，建议不要开启忽略参数配置。**
缓存过期配置	支持根据路径、文件类型配置文件在 CDN 节点上的缓存过期时间。
状态码缓存配置	支持配置状态码缓存过期时间，由 CDN 节点直接响应非2XX状态码，减轻源站压力。
HTTP 头部缓存配置	默认情况下 CDN 节点将缓存所有源站响应头部，可按需关闭。
忽略大小写缓存配置	默认情况下 CDN 节点区分大小写缓存，可按需忽略大小写。
URL 重写配置	支持自定义 URL 重写配置，将 URL 302 重定向到目标 URL。

回源配置

回源配置控制了 CDN 节点将请求发送至源站的行为。

配置名称	功能说明
Range 回源配置	默认情况下 CDN 节点回源均为分片回源，若源站不支持，可关闭此项配置。
回源 Request Header 配置	请求回源时按需添加指定头部信息，如携带真实 Client IP 等。
回源跟随301/302配置	支持开启回源跟随301/302配置。
回源超时时间配置	配置回源 TCP 连接超时时间(默认 5秒)及回源加载时间(默认 10秒)。

HTTPS 加速配置

HTTPS 加速配置模块支持各项 HTTPS 相关配置。

配置名称	功能说明
HTTPS 配置	上传自有证书或使用已托管的证书，启动 HTTPS 加速。
HTTP2.0 配置	开启后 CDN 边缘节点支持 HTTP2.0 协议。 **开启 HTTP2.0 协议前需要先进行证书配置。**
强制跳转配置	未配置/已配置证书情况下，均可设置 HTTPS 强制跳转为 HTTP 请求。 已配置证书情况下，可配置 HTTP 强制跳转为 HTTPS 请求。
OCSP 装订配置	开启后支持 OCSP 装订。 **开启 OCSP 装订前需要先进行证书配置。**
HSTS 配置	开启后添加 strict-transport-security 头部。 **开启 HSTS 配置前需要先进行证书配置。**

高级配置

配置名称	功能说明
带宽封顶配置	支持设置境内、境外加速封顶带宽，超出后可按需停止加速服务。 **全球域名支持境内境外分开配置。**
SEO 优化配置	开启后可自动识别访问 IP 是否为搜索引擎。 确认后自动回源，尽量保证搜索引擎权重的稳定性。
Response Header 配置	按需进行 HTTP Response Header 设置，在响应请求中返回给客户端。
智能压缩配置	指定文件类型和文件范围进行 Gzip 或 Brotli 压缩。

基本配置
基本信息

最近更新时间：2022-05-12 11:06:33

> **公告：**
> 内容分发网络 CDN 加速类型的名称已更新：原「静态加速」已更名为「网页小文件」，原「下载加速」已更名为「下载大文件」，原「流媒体加速」已更名为「音视频点播」。（仅名称变化，其他逻辑不变。）

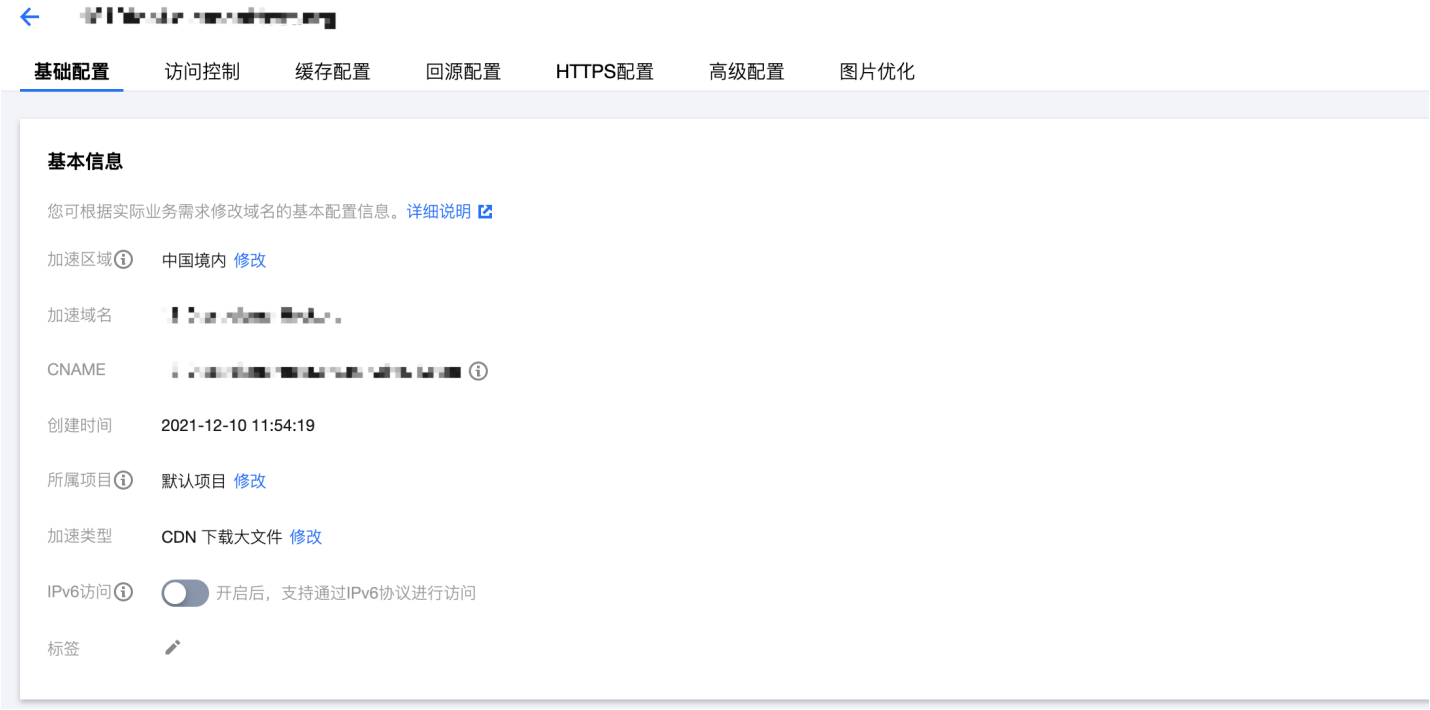
配置场景

针对已经接入腾讯云 CDN 的服务，您可以在域名基本信息模块查看域名创建时间及其对应 CNAME 域名、加速区域、项目、业务类型、协议支持等信息，也可按需对加速区域、业务类型、所属项目和标签等信息进行修改。

配置指南

查看基本信息

登录 CDN 控制台，在菜单栏里选择**域名管理**，单击域名右侧**管理**，即可进入域名配置页面，第一栏展示的即为域名基本信息。



修改域名加速区域

单击加速区域右侧**修改**，可调整域名的加速区域：

- 若域名为全球加速，则全球 CDN 加速节点按需进行就近调度，一般情况下中国境内节点服务境内用户，境外节点服务境外用户。
- 若域名为境内加速，则全球用户访问均由中国境内加速节点服务。
- 若域名为境外加速，则全球用户访问均由中国境外加速节点服务。

> ⚠ 注意：
>
> - 中国境内与中国境外加速服务分开独立计费，价格存在差异，具体计费策略 单击查看。
> - 从中国境内/中国境外修改至全球时，域名的配置将被同步至中国境外/中国境内。若域名含有后端特殊配置，此类配置的同步过程有一定延时，请耐心等待。

修改所属项目

单击所属项目右侧**修改**，可针对域名所属项目进行调整。

> ⚠ 注意：
>
> - 调整域名所属项目会造成项目维度数据统计及按照项目划分权限的子用户权限变更，请谨慎操作。
> - 创建或管理已有项目，可前往 项目管理。

修改业务类型

腾讯云 CDN 针对不同业务类型进行了针对性的加速性能优化，建议选择与自身业务更加贴近的业务类型，来获取更优质的加速效果，如需调整，可单击业务类型右侧**修改**进行调整：

> ⚠ 注意：
>
> - 切换业务类型会调整 CDN 底层加速平台，期间可能产生少量失败请求，并造成回源带宽增高，建议在业务低峰期进行切换。
> - 若您的域名无法看到**修改**按钮，表示域名存在特殊配置，暂时无法修改。若域名没有现网业务，建议删除重新接入。

修改 IPv6 访问

单击 IPv6 访问开关，可进行修改。开启后，支持通过 IPv6 协议访问 CDN 节点。

> ⚠ 注意：
>
> - 部分平台正在升级中，暂不支持开启 IPv6 访问，请等待后续全量发布。
> - 仅中国境内支持 IPv6 访问。若域名的加速区域为全球，则开启 IPv6 访问开关后，仅中国境内生效。若域名的加速区域为中国境外，则不可开启。

版权所有：腾讯云计算（北京）有限责任公司

- 若域名加速区域为“全球”且 IPv6 访问开关为开启状态，则切换加速区域为“中国境外”后，IPv6 访问开关会自动关闭，且不可开启。

修改域名标签

支持变更当前域名的标签。变更后非即刻生效，需刷新后查看最新的标签内容。

> 说明：
> 若需要批量对多个域名修改标签，可在域名管理页进行批量操作，详情可查看 域名操作。

源站配置

最近更新时间：2022-06-29 16:13:49

配置场景

若您需要修改域名源站基本信息、回源请求协议、回源 HOST等信息，可在源站配置模块进行相关操作。

> ⚠ 注意：
> 建议您的源站根据加速区域配置相同地域的源站，例如，加速区域为中国境内，请配置为境内源站回源，如果源站位于中国香港或境外，由于回源存在跨境访问，将无法为您保障回源效果。
> 如果您的加速区域为全球加速，可以在域名配置-源站配置中，设立区域独立源站，境内、境外根据不同区域回源到不同的源站内，以保障回源效果。

配置指南

主源站配置

登录 CDN 控制台，在菜单栏里选择【域名管理】，单击域名右侧【管理】，即可进入域名配置页面，第一栏中基本信息下方即为源站配置模块：

源站类型

自有源站	已经拥有稳定运行的业务服务器（即源站），填充对应的 IP 地址列表、或一个域名作为源站地址。
COS 源	选择云存储中的一个 bucket 作为源站，支持开启私有存储桶访问。

自有源站	已经拥有稳定运行的业务服务器（即源站），填充对应的 IP 地址列表、或一个域名作为源站地址。
第三方对象存储	腾讯云以外的第三方对象存储，当前支持的第三方为：AWS S3 和阿里云 OSS。 **注：**部分平台暂不支持第三方对象存储，请等待后续全量发布。

回源协议

CDN 加速节点回源到用户源站时使用的协议，HTTP 或 HTTPS。

HTTP 回源	HTTP/HTTPS 访问均使用 HTTP 回源。
HTTPS 回源	HTTP/HTTPS 访问均使用 HTTPS 回源，可以避免您的回源数据被窃取或者篡改，会少量消耗您源站的处理器资源（源站需要支持 HTTPS 访问）。
协议跟随	HTTP 访问使用 HTTP 回源，HTTPS 访问使用 HTTPS 回源。如果您仅需对部分关键的敏感数据采用 HTTPS 协议传输，其他业务采用 HTTP 协议传输，建议您选择"协议跟随"（源站需要支持 HTTPS 访问）。

⚠ **注意：**

- **存在 HTTPS 回源情况下，请保证源站支持 HTTPS 访问，否则会导致回源失败。**
- **目前暂时仍可通过证书管理页面调整此项配置，后续会进行迁移。**

源站地址

自有源	• 支持填充多个 IP 源站（一行一个）或一个域名源站： **多 IP 轮询回源：**支持填充多个 IP 源站（一行一个），轮询回源。CDN 默认开启源站检测能力，当某一个 IP 回源失败超出一定经验阈值时，则不再回源到此 IP 地址，会自动屏蔽 600s 后自动恢复。 **域名回源：**支持单独配置一个域名作为源站，此域名不可与 CDN 加速域名相同。不支持 IPv6 域名回源。 **注：**源站地址若为已接入的 CDN 加速域名，会造成循环解析，无法正常回源。 • 支持增加端口（0 – 65535）和权重（1 – 100）配置：源站:端口:权重（端口可缺省：源站::权重） **注：**回源协议为 HTTPS 和协议跟随时，仅支持配置443端口或不配置端口。 • 源站地址处最多可输入511个字符。
COS 源	• 选择腾讯云对象存储中的一个存储桶作为源站。 • 根据存储桶处的配置和您的实际业务场景，选择默认域名或静态网站类型。 • 若您的 COS 存储桶的读写权限设置了私有读访问，请授权 CDN 并开启回源鉴权，即开启私有存储桶访问。

第三方对象存储	• 若资源已存储在第三方对象存储中，请输入有效的存储桶访问地址作为源站，当前支持的第三方为：AWS S3 和阿里云 OSS。 **示例：**不可包含 http:// 或 http:// 协议头，my-bucket.s3.ap-east-1.amazonaws.com 或 my-bucket.oss-cn-beijing.aliyuncs.com。 • 回源至第三方私有存储桶，需填写有效密钥并开启回源鉴权，即开启私有存储桶访问。

回源 HOST

即回源域名，CDN 节点在回源时，访问的源站 IP 地址下具体的站点域名。具体配置示例说明可见 回源域名配置。

> 说明：
>
> 源站地址和回源 HOST 的区别如下：
>
> • 源站地址：源站地址决定了回源时请求到的具体 IP 地址。
> • 回源 HOST：回源 HOST 决定了回源请求访问到该 IP 地址上的具体站点。

自有源	默认为当前加速域名。若接入泛域名，则默认为泛域名，且实际回源 HOST 为访问域名。您可根据实际业务情况自行修改。
COS 源	默认为存储桶访问地址，与源站地址一致，不可修改。
第三方对象存储	默认为存储桶访问地址，与源站地址一致，不可修改。

热备源站配置

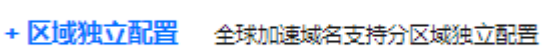
您可以为您的主源站添加热备源站，所有回源请求均会先访问主源站，若返回为 4XX/5XX 错误码，或链接超时、协议不兼容等情况后，会再次回源至热备源站进行资源拉取，保障用户回源高可用。

支持针对热备源站独立配置源站地址和回源 HOST。

> **注意：**
>
> - 热备源的源站类型不支持 COS 源和第三方对象存储。
> - 若主源站开启了 IPv6 源站，则不支持添加热备源站。
> - 热备源站不支持配置权重。

区域特殊配置

若您加速域名的服务区域为全球，为避免跨国流量产生，希望针对加速域名不同服务区域设置不同源站，可单击下方【添加特殊配置】实现：



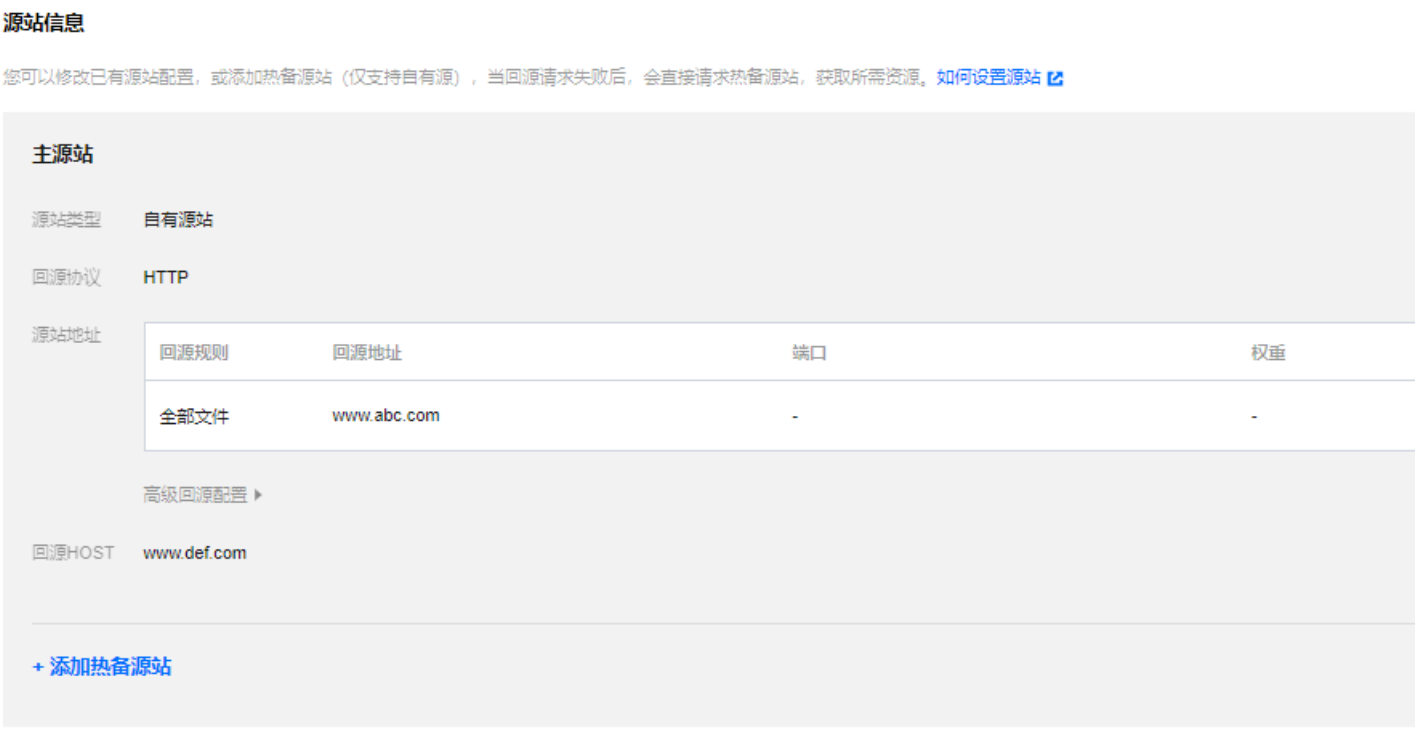
选择需要不同回源策略的区域，并填充对应的源站信息即可。具体配置示例说明可见 区域特殊配置。

> **注意：**
>
> - 源站类型为第三方对象存储时不支持添加区域特殊配置。

配置示例

回源域名配置

若 CDN 源站配置如下，假设加速域名 www.test.com 配置如下：

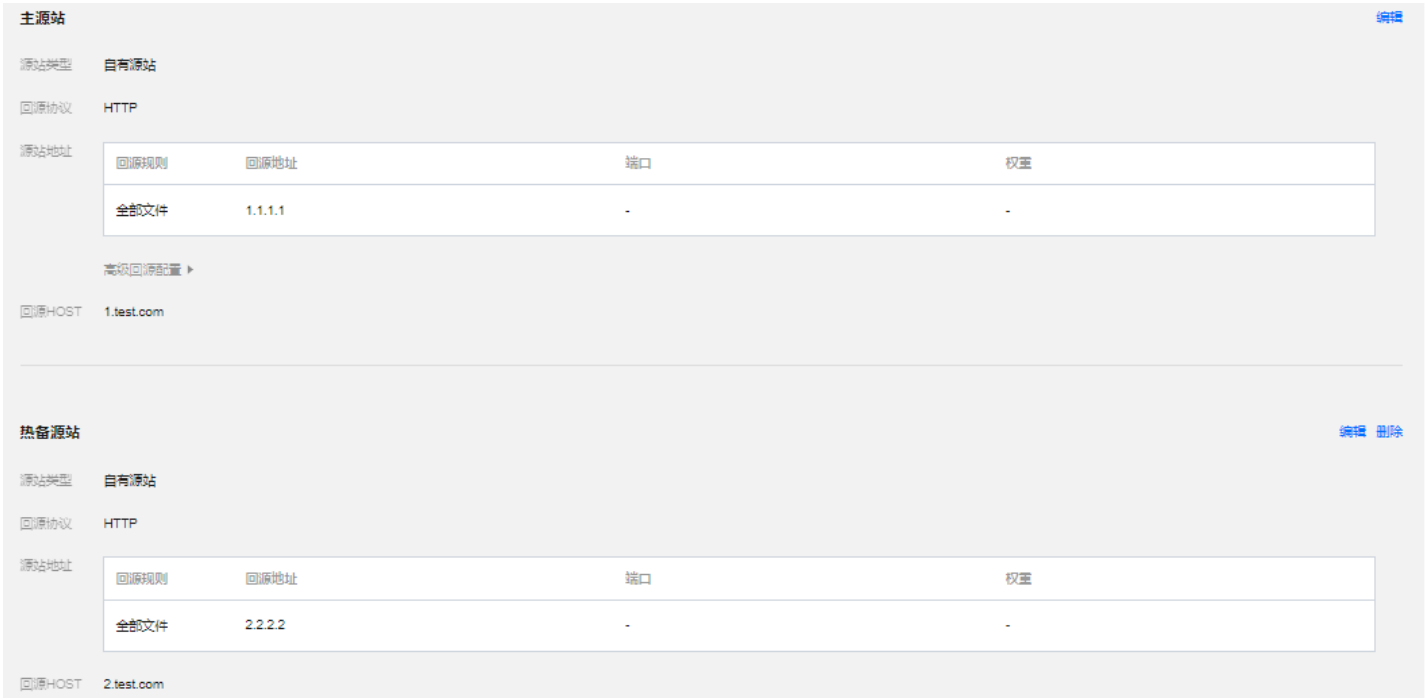


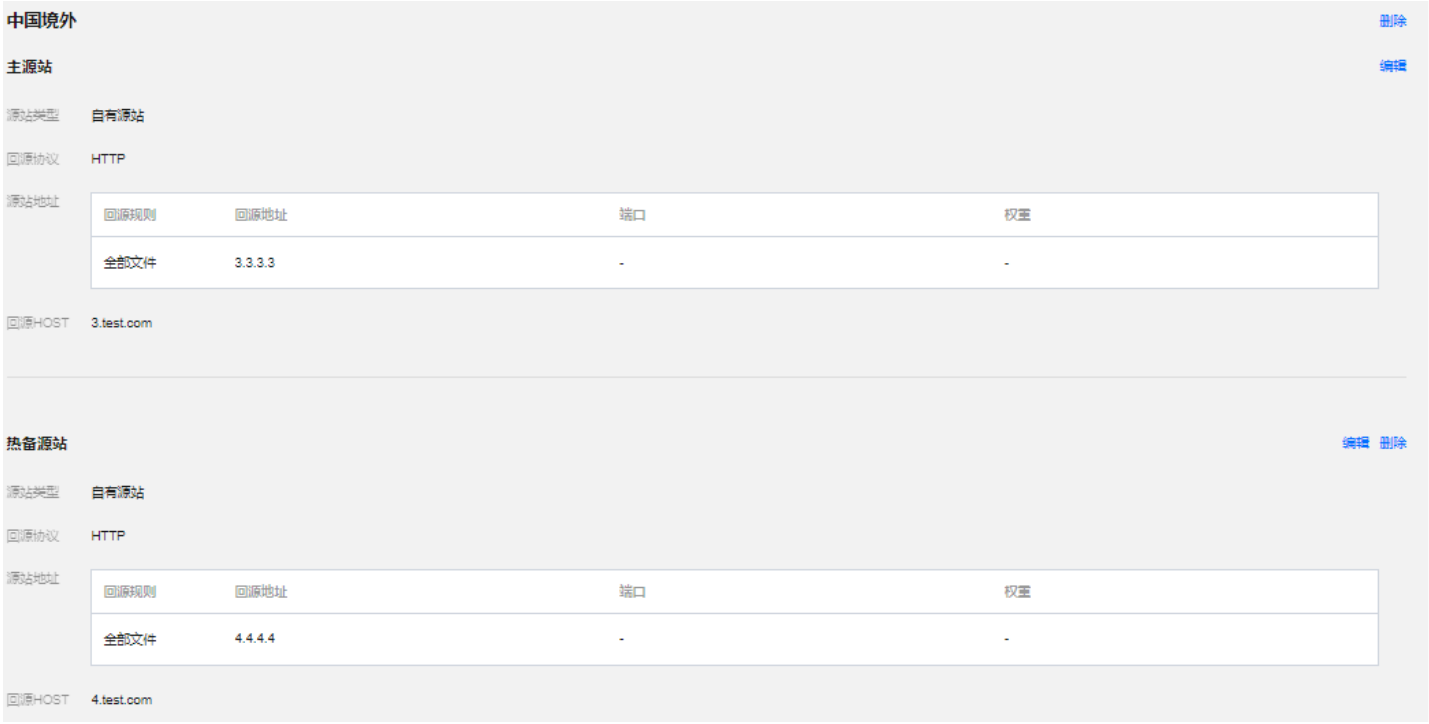
则用户访问路径如下：

用户访问资源 http://www.test.com/test.txt ，此时 CDN 节点尚未缓存该资源，则 CDN 节点回源是针对 www.abc.com 域名进行解析，得到源站服务器地址，假设为 1.1.1.1 ，则访问 1.1.1.1 服务器，在其上的 Web 网站 www.def.com 路径下，找到 test.txt 文件，返回给用户。

区域特殊配置

若腾讯云 CDN 源站配置如下，假设加速域名 www.test.com 配置如下：





则实际回源场景为：

1. **中国境内用户访问**http://www.test.com/test.txt**文件，境内节点尚未缓存该资源，则回源请求到达服务器**1.1.1.1**，找到 Web 网站**1.test.com**下的 test.txt 文件，若有该资源则直接返回给客户，若无，则进行步骤2。**
2. **CDN 境内节点回主源站失败，未找到资源，则回源请求到达服务器**2.2.2.2**，找到 Web 网站**2.test.com**下的 test.txt 文件，返回给用户并进行缓存。**
3. **此时中国境外的用户也访问**http://www.test.com/test.txt**文件，境外节点尚未缓存该资源，则回源请求到达服务器**3.3.3.3**，找到 Web 网站**3.test.com**下的 test.txt 文件，若有该资源则直接返回给客户，若无，则进行步骤4。**
4. **CDN 境外节点回境外主源站失败，未找到资源，回源请求到达服务器**4.4.4.4**，找到 Web 网站**4.test.com**下的 test.txt 文件，返回给境外用户并进行缓存。**

高级回源配置

最近更新时间：2021-11-05 17:59:13

腾讯云 CDN 支持更细粒度的回源配置，根据不同规则回源到不同的源站地址。例如：分路径回源（指定文件类型、文件夹、全路径文件（如：/test/1.jpg）、首页回源），根据 Client IP 所在区域回源等。

> ⚠ 注意：
>
> - 根据 Client IP 所在区域回源正在灰度中，尚未全量，请等待后续全量发布。
> - 暂仅支持主线路，基于主源站进行更细粒度的回源配置（源站类型和回源 HOST 均默认继承主源站，不支持根据不同规则进行变更）。

配置指南

登录 CDN 控制台，在左侧菜单栏选择【域名管理】，单击域名操作列的【管理】，进入域名配置页面，Tab【基础配置】页中【源站信息】模块最下方即可看到【高级回源配置】，单击可展开。

新增规则

您可按需添加高级回源配置规则，单击【编辑】主源站，点击【高级回源配置】即可编辑：

配置约束

- 单个域名至多可添加50条规则。
- 单条规则中的回源地址支持输入一个 IP/域名源站及端口（0 – 65535），端口可缺省。若回源协议已选择 HTTPS 或协议跟随，端口仅可配置为443或不配置端口。
- 更多操作：支持对多条规则调整优先级；支持批量编辑/删除多条规则。

说明：

- 底部优先级大于顶部 – 此相对位置的优先级调整仅限于同类型回源规则中，例如：多条分路径回源规则（指定文件类型/文件夹/全路径文件/首页回源规则）中，或多条根据 Client IP 所在区域回源规则中。
- 当同一个请求符合不同类型的回源规则时，按照类型的优先级来执行，顺序为：分路径 > Client IP。例如：配置了 Client IP 属于：江苏回源到 1.1.1.1 和 /test 回源到 2.2.2.2，则属于江苏的 Client IP 访问 /test 时，回源到 2.2.2.2。

HTTPS 回源算法说明

最近更新时间：2021-11-05 10:20:07

目前 HTTPS 回源可支持的算法如下表所示（顺序无先后之分）：

ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA384	ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA	ECDHE-ECDSA-AES256-SHA384	ECDHE-ECDSA-AES256-GCM-SHA384
SRP-AES-256-CBC-SHA	SRP-RSA-AES-256-CBC-SHA	SRP-DSS-AES-256-CBC-SHA
DH-RSA-AES256-SHA	DH-RSA-AES256-SHA256	DH-RSA-AES256-GCM-SHA384
DH-DSS-AES256-SHA	DH-DSS-AES256-SHA256	DH-DSS-AES256-GCM-SHA384
DHE-RSA-AES256-SHA	DHE-RSA-AES256-SHA256	DHE-RSA-AES256-GCM-SHA384
DHE-DSS-AES256-SHA	DHE-DSS-AES256-SHA256	DHE-DSS-AES256-GCM-SHA384
CAMELLIA256-SHA	DH-RSA-CAMELLIA256-SHA	DHE-RSA-CAMELLIA256-SHA
PSK-3DES-EDE-CBC-SHA	DH-DSS-CAMELLIA256-SHA	DHE-DSS-CAMELLIA256-SHA
ECDH-RSA-AES256-SHA	ECDH-RSA-AES256-SHA384	ECDH-RSA-AES256-GCM-SHA384

ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA384	ECDHE-RSA-AES256-GCM-SHA384
ECDH-ECDSA-AES256-SHA	ECDH-ECDSA-AES256-SHA384	ECDH-ECDSA-AES256-GCM-SHA384
AES256-SHA	AES256-SHA256	AES256-GCM-SHA384
ECDHE-RSA-AES128-SHA	ECDHE-RSA-AES128-SHA256	ECDHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA	ECDHE-ECDSA-AES128-SHA256	ECDHE-ECDSA-AES128-GCM-SHA256
SRP-AES-128-CBC-SHA	SRP-RSA-AES-128-CBC-SHA	SRP-DSS-AES-128-CBC-SHA
DH-RSA-AES128-SHA	DH-RSA-AES128-SHA256	DH-RSA-AES128-GCM-SHA256
DH-DSS-AES128-SHA	DH-DSS-AES128-SHA256	DH-DSS-AES128-GCM-SHA256
DHE-RSA-AES128-SHA	DHE-RSA-AES128-SHA256	DHE-RSA-AES128-GCM-SHA256
DHE-DSS-AES128-SHA	DHE-DSS-AES128-SHA256	DHE-DSS-AES128-GCM-SHA256
ECDH-RSA-AES128-SHA	ECDH-RSA-AES128-SHA256	ECDH-RSA-AES128-GCM-SHA256

版权所有：腾讯云计算（北京）有限责任公司

ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA384	ECDHE-RSA-AES256-GCM-SHA384
ECDH-ECDSA-AES128-SHA	ECDH-ECDSA-AES128-SHA256	ECDH-ECDSA-AES128-GCM-SHA256
CAMELLIA128-SHA	DH-RSA-CAMELLIA128-SHA	DHE-RSA-CAMELLIA128-SHA
PSK-RC4-SHA	DH-DSS-CAMELLIA128-SHA	DHE-DSS-CAMELLIA128-SHA
AES128-SHA	AES128-SHA256	AES128-GCM-SHA256
SEED-SHA	DH-RSA-SEED-SHA	DH-DSS-SEED-SHA
DES-CBC3-SHA	DHE-RSA-SEED-SHA	DHE-DSS-SEED-SHA
IDEA-CBC-SHA	PSK-AES256-CBC-SHA	PSK-AES128-CBC-SHA
EDH-RSA-DES-CBC3-SHA	ECDH-RSA-DES-CBC3-SHA	ECDHE-RSA-DES-CBC3-SHA
EDH-DSS-DES-CBC3-SHA	ECDH-ECDSA-DES-CBC3-SHA	ECDHE-ECDSA-DES-CBC3-SHA
RC4-SHA	ECDH-RSA-RC4-SHA	ECDHE-RSA-RC4-SHA
RC4-MD5	ECDH-ECDSA-RC4-SHA	ECDHE-ECDSA-RC4-SHA
SRP-3DES-EDE-CBC-SHA	SRP-RSA-3DES-EDE-CBC-SHA	SRP-DSS-3DES-EDE-CBC-SHA

版权所有：腾讯云计算（北京）有限责任公司

ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA384	ECDHE-RSA-AES256-GCM-SHA384
DH-DSS-DES-CBC3-SHA	DH-RSA-DES-CBC3-SHA	-

访问控制
防盗链配置

最近更新时间：2022-05-11 10:57:12

防盗链配置

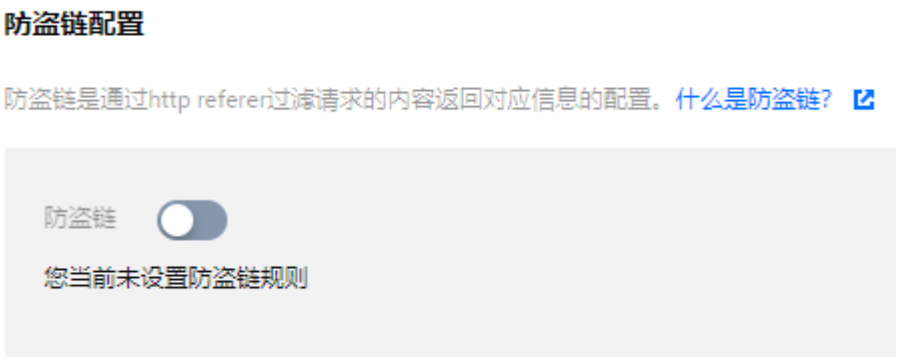
若您希望对业务资源的访问来源进行控制，腾讯云 CDN 为您提供了 referer 防盗链配置功能。

通过对用户 HTTP Request Header 中 referer 字段的值设置访问控制策略，从而限制访问来源，避免恶意用户盗刷。

配置指南

查看配置

登录 CDN 控制台，在菜单栏里选择**域名管理**，单击域名右侧**管理**，即可进入域名配置页面，第二栏【 访问控制 】中可看到防盗链配置，默认情况下，防盗链配置为关闭状态：



开启配置

单击开关，选择防盗链类型并填入列表，即可启用防盗链配置：

referer 黑名单：

- 若请求的 referer 字段匹配黑名单内设置的内容，CDN 节点拒绝返回该请求信息，直接返回403状态码。
- 若请求的 referer 不匹配黑名单内设置的内容，则 CDN 节点正常返回请求信息。
- 空referer选项勾选**拒绝空 referer访问** 选项时，此时若请求 referer 字段为空或无 referer 字段（如浏览器请求），则 CDN 节点拒绝返回该请求信息，返回403状态码。

referer白名单：

- 若请求的 referer 字段匹配白名单设置的内容，则 CDN 节点正常返回请求信息。
- 若请求的 referer 字段不匹配白名单设置的内容，则 CDN 节点拒绝返回该请求信息，会直接返回状态码403。
- 当设置白名单时，CDN 节点只能返回符合该白名单内字符串内容的请求。
- 空referer选项勾选**允许空 referer访问** 选项时，此时若请求 referer 字段为空或无 referer 字段（如浏览器请求），则 CDN 正常返回请求信息。

配置约束：

- **防盗链支持域名 / IP 规则，匹配方式为前缀匹配（仅支持路径情况下，域名的前缀匹配不支持），即假设配置名单为**www.abc.com，则www.abc.com/123**匹配，**www.abc.com.cn**不匹配；假设配置名单为**127.0.0.1，则127.0.0.1/123**也会匹配。**
- **防盗链支持通配符匹配，即假设名单为** *.qq.com，则 www.qq.com、a.qq.com **均会匹配，**qq.com **因其域名级别与** *.qq.com **的域名级别不同，则不会被匹配。**

关闭配置

您可以通过防盗链开关，一键关闭防盗链配置，开关为关闭状态时，即便下方存在已有配置，仍不会现网生效，下次单击开启时，会先行进行配置的二次确认，不会立即发布至全网生效：

区域特殊配置

若您的加速域名服务区域为全球加速，想针对境内、境外加速区域进行不同的 referer 防盗链配置，可点击配置下方的**添加特殊配置**进行设置：

> ⚠ **注意：**
>
> **区域特殊配置添加后，暂时无法直接删除，您可以通过关闭配置来禁用。**

配置示例

若加速域名 www.test.com 的防盗链配置如下：

则实际访问情况如下：

1. 中国境内用户请求，携带的 referer 信息为1.1.1.1，则命中境内配置的白名单，可直接返回内容。
2. 中国境外用户请求，携带的 referer 为空，匹配**拒绝空 referer访问**命中境外配置的黑名单，直接返回403。

IP 黑白名单配置

最近更新时间：2022-05-18 10:06:46

配置场景

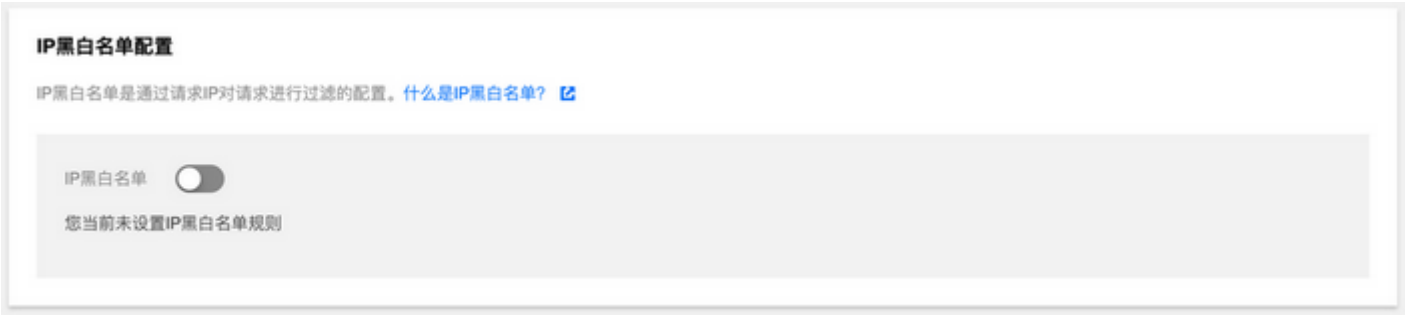
若您希望对业务资源的访问来源进行控制，腾讯云 CDN 为您提供了 IP 黑白名单配置功能。

通过对用户请求端 IP 配置访问控制策略，可以有效限制访问来源，阻拦恶意 IP 盗刷、攻击等问题。

配置指南

查看配置

登录 CDN 控制台，在菜单栏里选择**域名管理**，单击域名右侧**管理**，即可进入域名配置页面，第二栏**访问控制**中可看到 IP 黑白名单配置，默认情况下为关闭状态：



开启配置

单击开关，选择黑名单 / 白名单，并填入 IP 或 IP 段列表并单击**确认**，即可启用 IP 黑 / 白名单配置：

IP 黑名单

用户端 IP 匹配黑名单中的 IP 或 IP 段时，访问 CDN 节点时将直接返回403状态码。

IP 白名单

用户端 IP 未匹配白名单中的 IP 或 IP 段时，访问 CDN 节点时将直接返回403状态码。

配置约束

- IP 黑名单与 IP 白名单二选一，不可同时配置。
- IP 黑白名单各至多可输入200个。
- IPv4仅支持 /8、/16、/24 网段，不支持其他网段；IPv6支持全网段。
- 不支持IP:端口形式的黑白名单。

关闭配置

您可以通过 IP 黑白名单配置开关进行一键关闭，开关为关闭状态时，即便下方存在已有配置，仍不会现网生效，下次单击开启时，会先行进行配置的二次确认，不会立即发布至全网生效：

> **注意：**
> 若您的加速域名服务区域为全球加速，设置的 IP 黑名单与白名单会全球生效，不支持境内、境外差异化配置。

配置示例

若加速域名 www.test.com 的 IP 白名单配置如下：

则实际访问情况如下：

1. 用户端 IP 为1.1.1.1的用户访问资源 http://www.test.com/test.txt，匹配白名单1.0.0.0/8，正常返回内容。
2. 用户端 IP 为2.1.1.1的用户访问资源 http://www.test.com/test.txt，未匹配白名单，返回403。

若加速域名 www.test.com 的 IP 黑名单配置如下：

则实际访问情况如下：

1. 用户端 IP 为1.1.1.1的用户访问资源 http://www.test.com/test.txt，匹配黑名单1.0.0.0/8，返回403。
2. 用户端 IP 为2.1.1.1的用户访问资源 http://www.test.com/test.txt，未匹配黑名单，正常返回内容。

IP 访问限频配置

最近更新时间：2022-06-28 16:08:44

配置场景

若您希望对业务资源的访问来源进行控制，腾讯云 CDN 为您提供了 IP 访问限频配置。通过对单 IP 单节点在每一秒钟的访问次数进行限制，可进行高频 CC 攻击抵御、防恶意用户盗刷等。

配置指南

查看配置

登录 CDN 控制台，在菜单栏里选择【域名管理】，单击域名右侧【管理】，即可进入域名配置页面，第二栏【访问控制】中可看到 IP 访问限频配置，默认情况下配置为关闭状态，阈值为空：

开启配置

单击开关，填充频次控制阈值并单击【确认】，即可启用 IP 访问限频控制：

配置说明

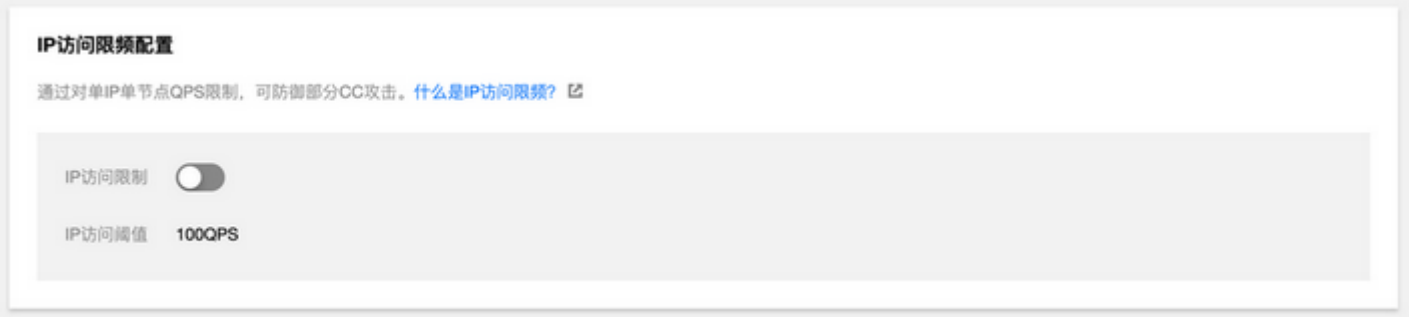
- 配置开启后，超出 QPS 限制的请求会直接返回514，设置较低频次限制可能会影响您的正常高频用户的使用，请根据业务情况、使用场景合理设置阈值。
- 限频仅针对与单 IP 单节点访问次数进行约束，若恶意用户海量 IP 针对性的进行全网节点攻击，则通过此功能无法进行有效控制。

版权所有：腾讯云计算（北京）有限责任公司

- 同一个域名下有多个不同 URL，若同时请求不同 URL 时，单 IP 单节点超出阈值的 URL 均直接返回514。

关闭配置

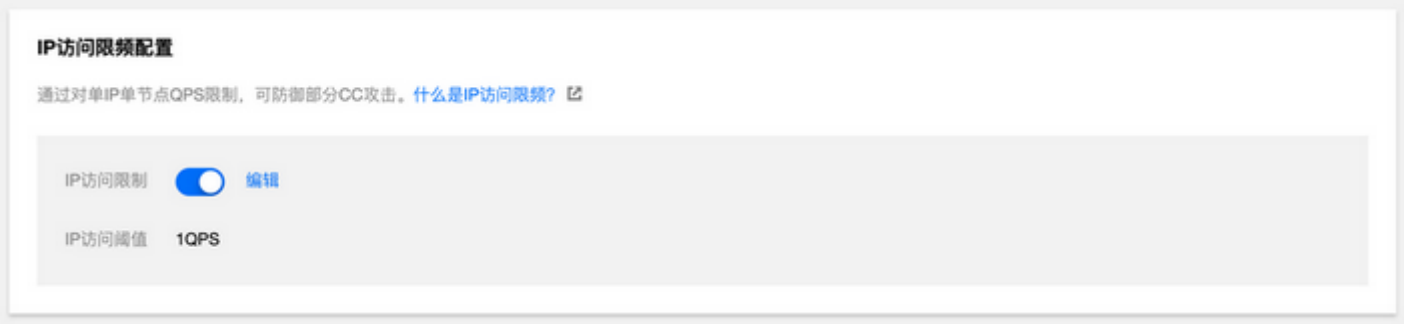
您可以通过配置开关进行一键关闭，开关为关闭状态时，即便下方存在已有配置，仍不会现网生效，下次单击开启时，会发布至全网生效：



> **注意：**
> 若您的加速域名服务区域为全球加速，设置的 IP 访问限频会全球生效，不支持境内、境外差异化配置

配置示例

若加速域名 www.test.com 的 IP 访问限频配置如下：



则实际访问情况如下：

1. 客户端 IP 为1.1.1.1的用户，在一秒内请求了10次资源http://www.test.com/1.jpg，均访问至 CDN 加速节点 A 中的一台 server，此时在该 server 上产生10条访问日志，其中有9条因超出 QPS 限制，状态码为514。
2. 客户端 IP 为2.2.2.2的用户，在一秒内请求了2次资源http://www.test.com/1.jpg，受网络影响，可能访问被分别调度至两个 CDN 加速节点上进行处理，此时每一个加速节点均会正常返回内容。

视频拖拽配置

最近更新时间：2021-12-24 10:08:34

配置场景

- 视频拖拽主要产生于视频点播场景中，当用户拖拽播放进度时，会向服务端发起类似如下请求：
  http://www.test.com/test.flv?start=10
  此时会返回第10字节开始的数据，由于点播类视频文件均缓存在各 CDN 节点上，开启此项配置，各节点可直接响应此类请求。
- 开启视频拖拽需同步开启忽略参数配置，即 缓存键规则 中所有规则的忽略参数配置需为“全部忽略”，且源站需要支持 range 请求。支持的文件格式为：mp4、flv、ts。

文件类型	meta 信息	start 参数说明	请求示例
MP4	源站视频的 meta 信息必须在文件头部，不支持 meta 信息在尾部的视频	start 参数表示的是时间，单位是秒，支持小数以表示毫秒（如 start = 1.01，表示开始时间是1.01s），CDN 会定位到 start 所表示时间的前一个关键帧（如果当前 start 不是关键帧）	http://www.test.com/demo.mp4?start=10 表示从第10秒开始播放
FLV	源站视频必须带有 meta 信息	start 参数表示字节，CDN 会自动定位到 start 参数所表示的字节的前一个关键帧（如果 start 当前不是关键帧）	http://www.test.com/demo.flv?start=10 表示从第10个字节开始播放

文件类型	meta 信息	start 参数说明	请求示例
TS	无特殊要求	start 参数表示字节，CDN 会自动定位到 start 参数所表示的字节	http://www.test.com/demo.ts?start=10 表示从第10个字节开始播放

查看配置

登录 CDN 控制台，在左侧菜单栏选择【域名管理】，选择业务类型为流媒体点播加速的域名，进入域名配置页面，Tab【访问控制】页中即可找到【视频拖拽】，默认为关闭状态。

鉴权配置
配置说明

最近更新时间：2021-11-05 10:21:47

配置场景

一般情况下，在 CDN 上分发的内容默认为公开资源，用户拿到 URL 后均可进行访问，为避免恶意用户盗刷您的内容进行牟利，除了通过 referer 黑白名单、IP 黑白名单、IP 访问限频等访问控制策略外，也可通过设置高级时间戳鉴权来进行盗刷防护。

> ⚠ 注意：
> 配置时间戳防盗链后，客户端在发起请求时需要按照配置计算签名并携带至服务端，CDN 节点进行服务端校验，校验通过后才继续放行。

配置指南

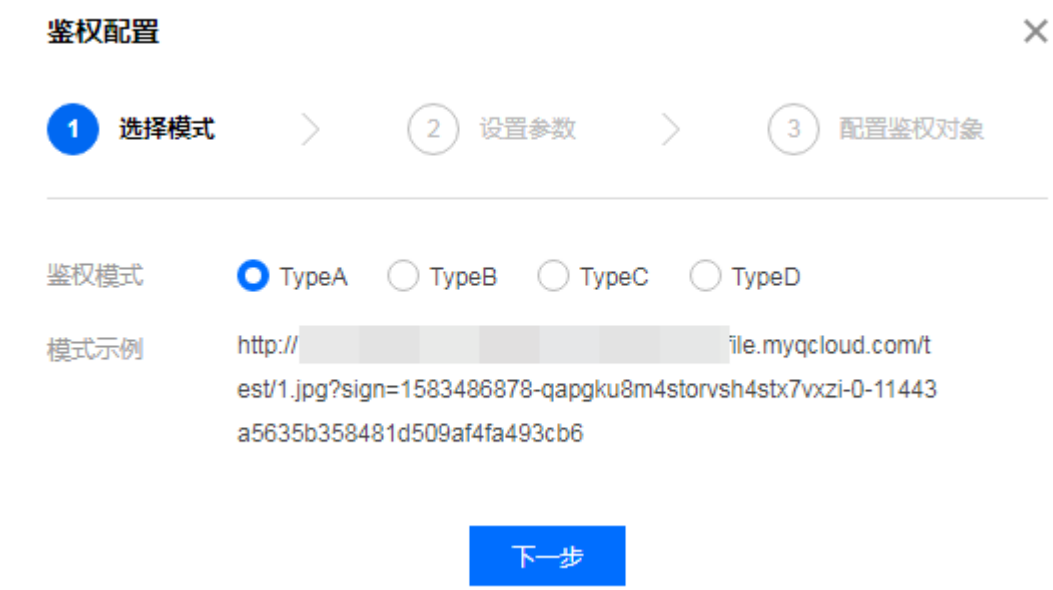
查看配置

登录 CDN 控制台，在菜单栏里选择【域名管理】，单击域名右侧【管理】，即可进入域名配置页面，【访问控制】中可看到鉴权配置，默认情况下，鉴权配置为关闭状态：

修改配置

1. 修改配置

CDN 提供了四种鉴权签名计算方式供您选择，也可以通过上方【鉴权计算器】来查看不同鉴权模式、配置后最终效果，具体算法说明请参见 TypeA、TypeB、TypeC、TypeD 等算法说明文档：



2. 关闭配置

您可以通过鉴权配置开关，一键关闭配置，开关为关闭状态时，即便下方存在已有配置，仍不会现网生效，下次单击开启时，会先行进行配置的二次确认，不会立即发布至全网生效：

3. 区域特殊配置

若您的加速域名服务区域为全球加速，想针对境内、境外加速区域进行不同的鉴权配置，可单击配置下方的【添加特殊配置】进行设置：

> **注意：**
> 区域特殊配置添加后，暂时无法直接删除，您可以通过关闭配置来禁用。

配置示例

若域名 cloud.tencent.com 为全球加速域名，鉴权配置如下：

则实际生效场景如下：

1. 中国境内用户实际访问资源http://cloud.tencent.com/1.jpg时，可直接发起请求。
2. 中国境外用户实际访问资源http://cloud.tencent.com/1.jpg，请求 URL 格式为 http://cloud.tencent.com/509301d10da7b862052927ed7a947f43/5e561139/1.jpg。

示例代码

各鉴权计算方式如下，以 Python Demo 为例：

```
import requests
import json
import sys
```

```
import time
import hashlib

def generate_url(category, ts=None):
url = 'http://www.test.com' # 测试域名
path = '/1.txt' # 访问路径
suffix = '?a=1&b=2' # URL参数
key = 'abc123456789' # 鉴权密钥
now = int(time.mktime(time.strptime(ts, "%Y%m%d%H%M%S")) if ts else time.time()) # 如果输入了时间，用输入ts，否则用当前ts
sign_key = 'key' # url签名字段
time_key = 't' # url时间字段
ttl_format = 10 # 时间进制，10或16，只有typeD支持
if category == 'A': #Type A
ts = now
rand_str = '123abc'
sign = hashlib.md5('%s-%s-%s-%s-%s' % (path, ts, rand_str, 0, key)).hexdigest()
request_url = '%s%s?%s=%s' % (url, path, sign_key, '%s-%s-%s-%s' % (ts, rand_str, 0, sign))
print(request_url)
elif category == 'B': #Type B
ts = time.strftime('%Y%m%d%H%M', time.localtime(now))
sign = hashlib.md5('%s%s%s' % (key, ts, path)).hexdigest()
request_url = '%s/%s/%s%s%s' % (url, ts, sign, path, suffix)
print(request_url)
elif category == 'C': #Type C
ts = hex(now)[2:]
sign = hashlib.md5('%s%s%s' % (key, path, ts)).hexdigest()
request_url = '%s/%s/%s%s%s' % (url, sign, ts, path, suffix)
print(request_url)
elif category == 'D': #Type D
ts = now if ttl_format == 10 else hex(now)[2:]
sign = hashlib.md5('%s%s%s' % (key, path, ts)).hexdigest()
request_url = '%s%s?%s=%s&%s=%s' % (url, path, sign_key, sign, time_key, ts)
print(request_url)


if __name__ == '__main__':
if len(sys.argv) == 1:
```

```
print('usage: python generate_url.py A 20200501000000')
args = sys.argv[1:]
generate_url(*args)
```

TypeA

最近更新时间：2022-06-28 15:46:44

为保护您的站点资源不被非法站点下载盗用，您可按需选择 Type ABCD 四种鉴权方式的某一种，本文为您详细介绍 Type A 的的各个参数字段和原理。

算法说明

- **访问 URL 格式**
  http://DomainName/Filename?sign=timestamp-rand-uid-md5hash

  > **注意：**
  > 访问 URL 中不能包含中文。

- **鉴权字段说明**

字段	说明
DomainName	CDN 域名。
Filename	资源访问路径，鉴权时Filename需以正斜线（ / ）开头。
timestamp	服务端生成鉴权 URL 的时间，使用十进制整型正数的 Unix 时间戳，是从 UTC 时间1970年01月01日00时00分00秒到现在的总秒数，其定义与所在时区无关。
rand	随机字符串，0 - 100位随机字符串，由大小写字母与数字组成。
uid	用户 ID，暂未使用，直接设置为0即可。
md5hash	通过 MD5 算法计算出的固定长度为32位的字符串。md5hash 具体的计算公式如下： • md5hash = md5sum(uri-timestamp-rand-uid-pkey) • uri 资源访问路径以正斜线（/）开头 • timestamp：取值为上述中的timestamp • rand： 取值为上述的rand • uid： 取值为上述的uid • pkey：自定义密钥：由6 - 40位大小写字母、数字构成，密钥需要严格保密，仅客户端与服务端知晓。

- **鉴权逻辑说明**
  CDN 服务器接受到客户请求后，解析出 url 中的 timestamp 参数 + 鉴权 URL 有效时长与当前时间比较。

i. 如果 timestamp + 鉴权 URL 有效时长小于当前时间，则服务器判定过期失效，并返回 HTTP 403错误。
ii. 如果 timestamp + 鉴权 URL 有效时长大于当前时间，则使用 MD5 算法算出 md5hash 的值，再比较计算出来的 md5hash 值与 url 中传入的 md5hash 值，如果一致则放过，不一致则返回HTTP 403错误。

配置指南

以 Type-A 鉴权的配置为例，参数和控制台配置如下：

- **字段配置**
  - 鉴权密钥：dimtm5evg50ijsx2hvuwyfoiu65
  - 签名参数：sign
  - 鉴权URL有效时长为：1s

  - 签算服务器生成鉴权URL的时间：2020年02月27日16:10:32（UTC+8），转换为十进制的整形数值为1582791032(timestamp)
  - 请求源站地址：http://cloud.tencent.com/test.jpg
- **生成过程**
  - 获取鉴权参数

参数	值
uri	资源访问路径为 /test.jpg
timestamp	1582791032
rand	生成随机数为 im1acp76sx9sdqe601v
uid	设置为0
pkey	dimtm5evg50ijsx2hvuwyfoiu65

  - 拼接签名串：/test.jpg-1582791032-im1acp76sx9sdqe601v-0-dimtm5evg50ijsx2hvuwyfoiu65
  - 计算签名串的 md5 值：md5hash =md5sum(uri-timestamp-rand-uid-pkey)= md5sum(/test.jpg-1582791032-im1acp76sx9sdqe601v-0-dimtm5evg50ijsx2hvuwyfoiu65) = 3fbb88382c9356b6faaf9d68c7b2ae3a
- **生成鉴权 URL：** http://cloud.tencent.com/test.jpg?sign=1582791032-im1acp76sx9sdqe601v-0-3fbb88382c9356b6faaf9d68c7b2ae3a
  当客户端通过加密URL进行访问时，如果CDN服务器计算出来的 md5hash 值与访问请求中带的md5hash值相同，都为3fbb88382c9356b6faaf9d68c7b2ae3a，则鉴权通过，反之鉴权失败。

注意事项

缓存命中率

开启了 TypeA 鉴权模式的域名，访问 URL 会携带鉴权参数，在 CDN 节点进行资源缓存时，会自动忽略对应的参数进行缓存，不会影响域名缓存命中率。

> ⚠ 注意：
> 因配置后会自动忽略对应的参数，即会忽略配置的鉴权参数，所以会影响鉴权范围内文件的缓存键，且此处的优先级高于**缓存配置 – 缓存键规则配置**处的缓存键规则。
> 例如，此处 TypeA 配置为： 鉴权参数：sign – 鉴权范围：jpg，则 jpg 类型的文件会自动忽略“sign”参数，即使**缓存配置 – 缓存键规则配置**处已配置：全部文件 – 不忽略参数。

回源策略

开启了 TypeA 鉴权模式的域名，访问格式为：
http://DomainName/Filename?sign=timestamp-rand-uid-md5hash

鉴权通过后，未命中 CDN 节点，节点会发起回源请求，**格式与访问请求保持一致，会保留签名参数**，源站可按需进行忽略或二次校验。

TypeB

最近更新时间：2022-06-28 15:46:47

为保护您的站点资源不被非法站点下载盗用，您可按需选择 Type ABCD 四种鉴权方式的某一种，本文为您详细介绍 Type B 的的各个参数字段和原理。

算法说明

- **访问 URL 格式**
  http://DomainName/timestamp/md5hash/FileName

> ⚠ **注意：**
> 访问 URL 中不能包含中文。

- **鉴权字段说明**

字段	说明
DomainName	CDN 域名。
Filename	资源访问路径，鉴权时Filename需以正斜线（ / ）开头。
timestamp	服务端生成鉴权 URL 的时间，使用十进制整型正数的 Unix 时间戳，是从 UTC 时间1970年01月01日00时00分00秒到现在的总秒数，其定义与所在时区无关。
md5hash	通过 MD 5算法计算出的固定长度为32位的字符串。具体计算公式如下： • md5hash = md5sum(pkeytimestampuri) 参数之间无任何符号 • pkey：自定义密钥：由6 - 40位大小写字母、数字构成，密钥需要严格保密，仅客户端与服务端知晓。 • uri 资源访问路径以正斜线（/）开头。 • timestamp：取值为上述中的timestamp。

- **鉴权逻辑说明**
  CDN 服务器接受到客户请求后，解析出 url 中的 timestamp 参数 + 鉴权 URL 有效时长与当前时间比较。
  i. 如果 timestamp + 鉴权 URL 有效时长小于当前时间，则服务器判定过期失效，并返回 HTTP 403错误。
  ii. 如果 timestamp + 鉴权 URL 有效时长大于当前时间，则使用 MD5 算法算出 md5hash 的值，再比较计算出来的 md5hash 值与 url 中传入的 md5hash 值，如果一致则放过，不一致则返回 HTTP 403错误。

配置指南

以 Type-B 鉴权的配置为例，参数和控制台配置如下：

- **字段配置**
  - 鉴权密钥：dimtm5evg50ijsx2hvuwyfoiu65
  - 鉴权URL有效时长为：1s

  - 签算服务器生成鉴权URL的时间：2020年02月27日16:10:32（UTC+8），转换为十进制的整形数值为1582791032(timestamp)
  - 请求源站地址：http://cloud.tencent.com/test.jpg
- **生成过程**
  - 获取鉴权参数

参数	值
uri	资源访问路径为 /test.jpg
timestamp	1582791032
pkey	dimtm5evg50ijsx2hvuwyfoiu65

  - 拼接签名串：dimtm5evg50ijsx2hvuwyfoiu651582791032/test.jpg
  - 计算签名串的md5值：md5hash = md5sum(pkeytimestampuri) =md5sum(dimtm5evg50ijsx2hvuwyfoiu651582791032/test.jpg) = ea68b93ac23ebbc6eebf7f163c6e9c4c
- **生成鉴权 URL**

  http://cloud.tencent.com/1582791032/ea68b93ac23ebbc6eebf7f163c6e9c4c/test.jpg

  当客户端通过加密 URL 进行访问时，如果 CDN 服务器计算出来的 md5hash 值与访问请求中带的 md5hash 值相同，都为 ea68b93ac23ebbc6eebf7f163c6e9c4c，则鉴权通过，反之鉴权失败。

注意事项

缓存命中率

开启了 TypeB 鉴权模式的域名，访问 URL 路径中会携带签名及时间戳，在 CDN 节点进行资源缓存时，会自动忽略路径中的字段进行缓存，不会影响域名缓存命中率。

回源策略

开启了 TypeB 鉴权模式的域名，访问格式为：
http://DomainName/timestamp/md5hash/FileName

鉴权通过后，若未命中 CDN 节点，节点会发起回源请求，**回源请求会去掉路径中的 md5hash 及 timestamp**，源站无需做特殊处理。

TypeC

最近更新时间：2022-06-28 15:46:50

为保护您的站点资源不被非法站点下载盗用，您可按需选择 Type ABCD 四种鉴权方式的某一种，本文为您详细介绍 Type C 的的各个参数字段和原理。

算法说明

- **访问 URL 格式**
  http://DomainName/md5hash/timestamp/FileName

  > **注意：**
  > 访问 URL 中不能包含中文。

- **鉴权字段说明**

字段	说明
DomainName	CDN 域名。
Filename	资源访问路径，鉴权时 Filename 需以正斜线（ / ）开头。
timestamp	服务端生成鉴权 URL 的时间，使用十进制整型正数的 Unix 时间戳，是从 UTC 时间1970年01月01日00时00分00秒到现在的总秒数，其定义与所在时区无关。
md5hash	通过 MD5 算法计算出的固定长度为32位的字符串。具体计算公式如下： • md5hash = md5sum(pkeytimestampuri) 参数之间无任何符号 • pkey： 自定义密钥：由6 – 40位大小写字母、数字构成，密钥需要严格保密，仅客户端与服务端知晓。 • uri 资源访问路径以正斜线（/）开头。 • timestamp: 取值为上述中的timestamp。

- **鉴权逻辑说明**
  CDN 服务器接受到客户请求后，解析出 url 中的 timestamp 参数 + 鉴权 URL 有效时长与当前时间比较。
  i. 如果 timestamp + 鉴权 URL 有效时长小于当前时间，则服务器判定过期失效，并返回 HTTP 403错误。
  ii. 如果 timestamp + 鉴权 URL 有效时长大于当前时间，则使用 MD5 算法算出 md5hash 的值，再比较计算出来的 md5hash 值与 url 中传入的 md5hash 值，如果一致则放过，不一致则返回 HTTP 403错误。

配置指南

版权所有：腾讯云计算（北京）有限责任公司

以 Type-C 鉴权的配置为例，参数和控制台配置如下：

- **字段配置**
  - 鉴权密钥：dimtm5evg50ijsx2hvuwyfoiu65
  - 鉴权URL有效时长为：1s

  - 签算服务器生成鉴权URL的时间：2020年02月27日16:10:32（UTC+8），转换为十进制的整形数值为1582791032(timestamp)
  - 请求源站地址：http://cloud.tencent.com/test.jpg

- **生成过程**
  - 获取鉴权参数

参数	值
uri	资源访问路径为 /test.jpg
timestamp	1582791032
pkey	dimtm5evg50ijsx2hvuwyfoiu65

  - 拼接签名串：dimtm5evg50ijsx2hvuwyfoiu651582791032/test.jpg
  - 计算签名串的 md5 值：md5hash = md5sum(pkeytimestampuri) =md5sum(dimtm5evg50ijsx2hvuwyfoiu651582791032/test.jpg) = ea68b93ac23ebbc6eebf7f163c6e9c4c

- **生成鉴权 URL：**
  http://cloud.tencent.com/ea68b93ac23ebbc6eebf7f163c6e9c4c/1582791032/test.jpg

当客户端通过加密URL进行访问时，如果 CDN 服务器计算出来的 md5hash 值与访问请求中带的 md5hash 值相同，都为ea68b93ac23ebbc6eebf7f163c6e9c4c，则鉴权通过，反之鉴权失败。

注意事项

缓存命中率

开启了 TypeC 鉴权模式的域名，访问 URL 路径中会携带签名及时间戳，在 CDN 节点进行资源缓存时，会自动忽略鉴权路径进行缓存，不会影响域名缓存命中率。

回源策略

开启了 TypeC 鉴权模式的域名，访问格式为：

http://DomainName/md5hash/timestamp/FileName

鉴权通过后，未命中 CDN 节点，节点会发起回源请求，**回源请求会去掉路径中的 md5hash 及 timestamp 路径**，源站无需做特殊处理。

TypeD

最近更新时间：2022-06-28 15:46:53

为保护您的站点资源不被非法站点下载盗用，您可按需选择 Type ABCD 四种鉴权方式的某一种，本文为您详细介绍 Type D 的的各个参数字段和原理。

算法说明

- **访问 URL 格式**
  http://DomainName/FileName?sign=md5hash&t=timestamp

  > ⚠ **注意：**
  > 访问 URL 中不能包含中文。

- **鉴权字段说明**

字段	说明
DomainName	CDN 域名。
Filename	资源访问路径，鉴权时 Filename 需以正斜线（ / ）开头。
timestamp	服务端生成鉴权 URL 的时间，使用十进制整型正数的 Unix 时间戳，是从 UTC 时间1970年01月01日00时00分00秒到现在的总秒数，其定义与所在时区无关。
md5hash	通过MD5算法计算出的固定长度为32位的字符串。具体计算公式如下：md5hash = md5sum(pkeyuritimestamp) 参数之间无任何符号pkey： 自定义密钥：由6 - 40位大小写字母、数字构成，密钥需要严格保密，仅用户端与服务端知晓。uri 资源访问路径以正斜线（/）开头。

- **鉴权逻辑说明**
  CDN 服务器接受到客户请求后，解析出 url 中的 timestamp 参数 + 鉴权 URL 有效时长与当前时间比较。
  i. 如果 timestamp + 鉴权 URL 有效时长小于当前时间，则服务器判定过期失效，并返回 HTTP 403错误。
  ii. 如果 timestamp + 鉴权 URL 有效时长大于当前时间，则使用 MD5 算法算出 md5hash 的值，再比较计算出来的 md5hash 值与 url 中传入的 md5hash 值，如果一致则放过，不一致则返回 HTTP 403错误。

配置指南

以 Type-D 鉴权的配置为例，参数和控制台配置如下：

- **字段配置**
  - 鉴权密钥：dimtm5evg50ijsx2hvuwyfoiu65
  - 鉴权URL有效时长为：1s

  - 签算服务器生成鉴权 URL 的时间：2020年02月27日16:10:32（UTC+8），转换为十进制的整形数值为1582791032(timestamp)
  - 请求源站地址：http://cloud.tencent.com/test.jpg
- **生成过程**
  - 获取鉴权参数

参数	值
uri	资源访问路径为 /test.jpg
timestamp	1582791032
pkey	dimtm5evg50ijsx2hvuwyfoiu65

  - 拼接签名串：dimtm5evg50ijsx2hvuwyfoiu65/test.jpg1582791032
  - 计算签名串的 md5 值：md5hash = md5sum(pkeyuritimestamp) =md5sum(dimtm5evg50ijsx2hvuwyfoiu65/test.jpg1582791032) =900a5049aa8ac1ab144527d9c2be4cea
- **生成鉴权 URL**

http://cloud.tencent.com/test.jpg?sign=900a5049aa8ac1ab144527d9c2be4cea&t=1582791032

当客户端通过加密URL进行访问时，如果CDN服务器计算出来的md5hash值与访问请求中带的md5hash值相同，都为900a5049aa8ac1ab144527d9c2be4cea，则鉴权通过，反之鉴权失败。

注意事项

缓存命中率

开启了 TypeD 鉴权模式的域名，访问 URL 会携带鉴权参数，在 CDN 节点进行资源缓存时，会自动忽略对应的参数进行缓存，不会影响域名缓存命中率。

> ⚠ 注意：
>
> 因配置后会自动忽略对应的参数，即会忽略配置的鉴权参数及时间戳参数，所以会影响鉴权范围内文件的缓存键，且此处的优先级高于**缓存配置 - 缓存键规则配置**处的缓存键规则。
> 例如，此处 TypeD 配置为： 鉴权参数：sigh - 时间戳参数：t - 鉴权范围：jpg，则 jpg 类型的文件会自动忽略“sign”和“t”参数，即使**缓存配置 - 缓存键规则配置**处已配置：全部文件 - 不忽略参数。

回源策略

开启了 TypeD 鉴权模式的域名，访问格式为：

http://DomainName/FileName?sign=md5hash&t=timestamp

鉴权通过后，未命中 CDN 节点，节点会发起回源请求， **格式与访问请求保持一致，会保留 sign/t 参数**，源站可按需进行忽略或二次校验。

UA 黑白名单配置

最近更新时间：2021-11-05 10:05:40

配置场景

腾讯云 CDN 支持通过配置 User-Agent 黑白名单规则实现访问控制。
通过对用户 HTTP 请求头中的 User-Agent 进行规则判断，按需放行或拒绝用户访问。

配置指南

查看配置

登录 CDN 控制台，在菜单栏里选择【域名管理】，单击域名右侧【管理】，即可进入域名配置页面，第二栏【访问控制】中可看到 UA 黑白名单配置，默认情况下为关闭状态：

新增规则

单击【新增规则】，可按需逐条添加黑(白)名单：

配置约束

- 仅支持全部设置为黑名单或全部设置为白名单，不支持同时设置黑、白名单规则。
- 最多可配置 10 条黑或白名单规则。
- 规则内容支持通配符*，多个值情况下使用 |分隔。
- 生效类型支持全部文件、文件类型、文件目录、指定文件路径四种模式，暂不支持正则匹配。

> ⚠ 注意：
>
> 1. 仅支持通配符*，暂时不支持其他正则表达式。
> 2. 无*情况下，其他字符均为完全匹配。

配置示例

若加速域名 cloud.tencent.com 的 UA 黑白名单配置如下：

当 HTTP Request Header 中 User-Agent 如下时：

```
user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36
```

命中黑名单，将直接返回403。

下行限速配置

最近更新时间：2022-06-06 16:13:10

配置场景

腾讯云 CDN 为您提供了下行限速配置，对服务端单链接下行最大吞吐速度进行设置。
通过下行限速配置，可在一定程度上控制 CDN 峰值带宽值，多用于电商大促、游戏新版本发布更新等场景。

> ⚠ 注意：
> 下行限速配置成功后，将会对访问此域名的全网用户生效，一定程度上会影响用户访问体验及 CDN 加速效果，请谨慎使用。

配置指南

查看配置

登录 CDN 控制台，在菜单栏里选择【域名管理】，单击域名右侧【管理】，即可进入域名配置页面，第二栏【访问控制】中可看到下行限速配置，默认情况下为关闭状态：

新增规则

单击【新增限速规则】，可进行规则配置：

配置约束

- 下行限速规则最多可配置 10 条。
- 限速单位为 KB/s，需要填充为正整数，取值区间为1 – 1000000。
- 生效类型支持全部文件、文件类型、文件目录、指定文件路径四种模式，暂不支持正则匹配。
- 多条规则优先级为从上到下从低到高，底部优先级高于顶部。

配置示例

若加速域名 cloud.tencent.com 的下行限速配置如下：

若用户访问资源为 http://cloud.tencent.com/test.mp4 ，则服务端按照下行速度 200KB/s 响应内容。

若用户访问资源为 http://cloud.tencent.com/test.flv ，则服务端按照下行限速 400KB/s 响应内容。

远程鉴权

最近更新时间：2021-11-03 18:26:58

远程鉴权

配置场景

为了避免客户的资源被非法用户访问，腾讯云除了支持在 CDN 边缘进行 高级时间戳鉴权 之外，也同时支持将请求转发至客户指定的远程鉴权服务器，由该鉴权服务器对用户请求进行校验，CDN 根据远程鉴权服务器返回的校验结果来决定是否继续提供服务。

远程鉴权的请求流程如下：

1. 终端用户对资源发起请求。
2. CDN 将请求同步转发至远程鉴权服务器。
3. 远程鉴权服务器返回鉴权结果。
4. CDN 节点根据鉴权结果来决定是否继续响应该用户的请求。

> ⚠ 注意：
>
> - CDN 节点根据远程服务器返回的状态码来判断是否鉴权通过，鉴权通过的状态码为200/206/304，其他状态码均为鉴权失败。鉴权通过则放行（返回200），失败则拦截（返回403）。
> - 当前仅支持同步远程鉴权，即 CDN 收到远程鉴权服务器返回鉴权结果后才能进行响应。
> - 部分海外平台不支持远程鉴权配置，修改域名加速区域可能导致远程鉴权功能失效。
> - 点播加速当前暂不支持远程鉴权配置。

配置指南

登录 CDN 控制台，在菜单栏里选择**域名管理**，单击域名右侧**管理**，进入域名配置页面，**访问控制**中即可进行远程鉴权相关的配置：

- 远程鉴权地址：支持 HTTP/HTTPS 协议，可填写域名或者IP地址。
- 请求方法：向远程服务器发起请求的方法，支持遵循终端用户请求方法，或者指定 GET/POST/HEAD 等请求方法。
- 鉴权文件类型：设置鉴权文件生效的范围，支持针对**全部内容/指定文件后缀/指定文件目录/指定文件**开启远程鉴权。
- 鉴权超时时长：设置远程鉴权服务器的响应超时时间，最大不超过30,000毫秒。
- 超时执行动作：设置远程鉴权超时后的执行动作，默认动作为放行。

版权所有：腾讯云计算（北京）有限责任公司

示例说明

假设客户的加速域名为 www.example.com **，设置的远程鉴权配置如下：**

- **远程鉴权地址：**www.remoteauth.com。
- **请求方法：遵循终端用户请求方法。**
- **鉴权文件类型：全部内容。**
- **鉴权超时时长：1500毫秒。**
- **超时执行动作：拦截。**

此时用户请求响应的流程示例如下：

1. **用户发起 GET 请求：**http://www.example.com/v001/test.txt?token=Gf6Gq04ymjdSTXusvTmh8yalO82YsuKUQb63ToXOFc&e=1467565695283&sign=854124740723b575a7cfa4fc40f0be30。
2. **CDN 收到请求，向远程鉴权服务器发起 GET 请求：**http://www.remoteauth.com/v001/test.txt?token=Gf6Gq04ymjdSTXusvTmh8yalO82YsuKUQb63ToXOFc&e=1467565695283&sign=854124740723b575a7cfa4fc40f0be30。
3. **远程鉴权服务器返回状态码 200。**
4. **CDN 判断鉴权通过，返回状态码 200，并正常响应内容。**

境内访问端口配置

最近更新时间：2021-06-18 10:31:43

配置场景

CDN 默认开启80/8080/443访问端口。您可根据业务的实际需求，自助关闭某一访问端口。

> ⚠ 注意：
>
> - 访问端口配置暂不支持中国境外。若域名的加速区域为全球，则配置变更后仅生效中国境内。
> - 部分平台正在升级中，暂未开放此配置功能。

配置指南

查看配置

登录 CDN 控制台，在左侧菜单栏选择【域名管理】，单击域名操作列的【管理】，进入域名配置页面，切换 Tab 至【访问控制】，即可找到【境内访问端口配置】。

默认情况下，80/8080/443访问端口均为开启状态：

修改配置

您可按需关闭已开启的访问端口。关闭后，可再次开启。

修改约束

- 若域名已开启 HTTPS 或强制跳转 HTTPS，则不可关闭443访问端口。
- 不可同时关闭80访问端口和8080访问端口。

配置示例

若加速域名 www.test.com 的**境内访问端口配置**如下：

则实际访问情况如下：

CDN 节点会拒绝8080端口的访问

- 若域名的加速区域为全球，则仅生效中国境内，CDN 中国境内节点会拒绝8080端口的访问。

缓存配置
缓存键规则配置

最近更新时间：2022-05-09 11:25:15

配置场景

腾讯云 CDN 在进行缓存时使用的是 Key-Value 格式进行资源映射，其中的 Key 即缓存键，Value即资源在CDN中的缓存。您可通过缓存键规则配置，只保留对资源内容有影响的参数作为缓存键，将同一个资源的一类请求转化为统一的缓存键并命中同一份缓存，以提升命中率。

忽略参数

若在您的业务场景下，资源 URL 路径中问号后的参数对资源内容有影响，需要保留作为缓存键；反之，若参数对资源内容没有影响，则参数需不作为缓存键。

不忽略参数的场景：

- 用户通过 URL 进行资源访问时，可能会携带一些具有特殊作用的参数，如使用以下链接来表示两张不同的图片：
  http://cloud.tencent.com/1.jpg?version=1
  http://cloud.tencent.com/1.jpg?version=2
  这种场景下需要选择“不忽略”，保留URL所有参数及值作为缓存键，分别进行图片内容的缓存，来进行资源区分。

保留指定参数的场景：

- 若 URL 中除了对资源内有影响的 version 参数以外，还携带其他不影响图片内容的参数，如时间戳 time 来记录请求时间：
  http://cloud.tencent.com/1.jpg?version=1&time=1651752741
  http://cloud.tencent.com/1.jpg?version=1&time=1651752742
  http://cloud.tencent.com/1.jpg?version=2&time=1651752743
  这种场景下需要选择"保留指定参数"，指定保留对图片内容有影响的 version 参数作为缓存键，而忽略不影响图片内容的 time 参数。
  - 对于参数 version 值相同的请求，忽略参数 time 及值，将共用一份缓存；
  - 对于参数 version 值不同的请求，忽略参数 time 及值，将区分缓存。

参数全部忽略的场景：

- 在音视频场景下，若使用时间戳签名参数来进行访问认证：
  http://cloud.tencent.com/1.mp4?sign=XXXXXX

版权所有：腾讯云计算（北京）有限责任公司

这种场景下需要选择“全部忽略”，由“?”之前的链接 http://cloud.tencent.com/1.mp4 作为缓存键。节点仅缓存一份资源，即使时间戳签名不断变化，通过签名校验后可直接命中缓存。

忽略大小写

若在您的业务场景下，资源 URL 路径中大小写差异与资源内容无关，则可开启忽略大小写配置，提升命中率。

> ⚠ 注意：
> 平台升级中，暂不支持开启忽略大小写。

配置指南

查看配置

登录 CDN 控制台，在左侧菜单栏选择**域名管理**，单击域名操作列的**管理**，进入域名配置页面，切换 Tab 至**缓存配置**，即可找到**缓存键规则配置**。

添加加速域名时，根据不同的业务类型，忽略参数默认关闭或开启：

- 若加速域名选择网页小文件业务类型，默认不开启忽略参数。缓存键规则配置中，全部文件规则的**忽略参数**同步为“不忽略”。
- 若加速域名选择下载大文件、音视频点播业务类型，默认开启忽略参数。缓存键规则配置中，全部文件规则的**忽略参数**同步为“全部忽略”。

新增规则

您可按需添加缓存键规则。

配置约束

- 单个域名至多可添加20条缓存键规则（包含默认规则）。
- 多条规则支持调整优先级：底部优先级大于顶部（默认规则不可调整优先级）。
- 单条文件类型/文件夹/全路径文件规则中，至多可输入100组内容，不同内容之间用“;”分隔。例如：文件类型 – jpg;png。
- 忽略参数 – 保留指定参数
  - 全部文件：至多可填6个参数名，每个参数名不可超过20个字符。
  - 文件类型/文件夹/全路径文件：至多可填5个参数名，每个参数名不可超过20个字符。
    多个参数名之间用“;”分隔，例如：key1;key2;key3。

修改规则

对已添加的缓存键规则，可进行修改。单击缓存键规则操作列的**修改**即可。

> ⚠ 注意：
> 默认规则仅支持修改忽略参数和忽略大小写配置，不支持修改类型和内容。

删除规则

可删除已添加的缓存键规则。单击缓存键规则操作列的**删除**即可。（默认规则不可删除）

配置示例

若加速域名 www.test.com 的**缓存键规则配置**如下：

则实际访问情况如下：

客户端请求资源 www.test.com/abc.jpg?version=1&colour=red 和 www.test.com/abc.JPG?version=1&colour=red，假设请求均访问到 CDN 节点 X，节点 X 无上述两个资源的缓存：

- 请求回源站获取abc.jpg图片资源，并缓存在 CDN 节点 X 上，因已开启忽略参数：全部忽略，则由“?”之前的链接www.test.com/abc.jpg作为缓存键。
- 当客户端请求www.test.com/abc.JPG?version=1&colour=red时，因忽略大小写未开启，则无法命中之前缓存的www.test.com/abc.jpg资源，请求回源站获取abc.JPG图片资源，并缓存在 CDN 节点 X 上，其对应的缓存键为www.test.com/abc.JPG?version=1&colour=red

节点缓存过期配置

最近更新时间：2022-06-24 19:22:53

节点缓存过期配置可以设置源站资源在 CDN 节点的缓存过期时间，以调整源站资源在 CDN 节点缓存更新频率。您可以根据业务需求，按目录、文件后缀名、文件全路径配置资源的缓存过期时间。

功能介绍

CDN 会根据节点缓存过期配置的缓存过期时间，判断 CDN 节点的缓存资源是否过期。

- 若用户访问的资源在 CDN 节点的缓存未过期，CDN 节点直接将缓存返回给用户；
- 若用户访问的资源在 CDN 节点未缓存该资源或缓存已过期，则 CDN 节点会回源站获取最新资源并缓存到 CDN 节点，同时返回给用户。

若源站资源更新后，需要立刻更新 CDN 节点的缓存，可使用 缓存刷新 功能主动更新 CDN 节点未过期的缓存，使 CDN 节点缓存与源站资源保持一致。

注意事项

- 缓存过期时间会影响回源频率，建议根据实际业务需求设置资源缓存时长。缓存过期时间过短，会导致 CDN 频繁回源，增加源站的带宽；缓存过期时间过长，会导致 CDN 缓存更新慢，影响用户获取最新的资源。
- CDN 节点会按照 腾讯云 CDN 缓存规则及优先级 缓存资源。但 CDN 节点的缓存资源也可能因请求频率过低，在未达到缓存过期时间就提前从节点中删除。
- 建议您源站资源更新前后使用不同的名称，如以版本号（img-v1.jpg、img-v2.jpg）的方式命名内容不同的资源，避免源站变更资源的内容后，CDN 节点因缓存未过期仍使用旧的资源返回给用户。
- 若您仍使用旧版本（基础模式）的节点缓存过期配置，建议您按高级模式配置提交升级为最新版的节点缓存过期配置，以支持更多功能。需注意升级高级模式后不可恢复至原基础模式。旧版本的节点缓存过期配置文档查看：节点缓存过期配置 (旧)
- 源站可通过设置响应头 Cache-Control 控制 CDN 节点的缓存过期时间（缓存选项为：遵循源站），同时 CDN 节点将 Cache-Control 响应头传递给用户，实现控制浏览器的缓存时间。若需要由 CDN 节点设置浏览器的缓存时间，可通过 浏览器缓存过期配置 修改 CDN 节点响应给用户的 Cache-Control 头部。

配置说明

操作流程

1. 登录 CDN 控制台；
2. 单击左侧菜单内的**域名管理**，进入域名管理列表；
3. 选择需要配置的域名，单击**管理**进入域名配置页面；

4. 单击**缓存配置**，切换至缓存配置标签页，在标签页中，即可查看**节点缓存过期配置**；

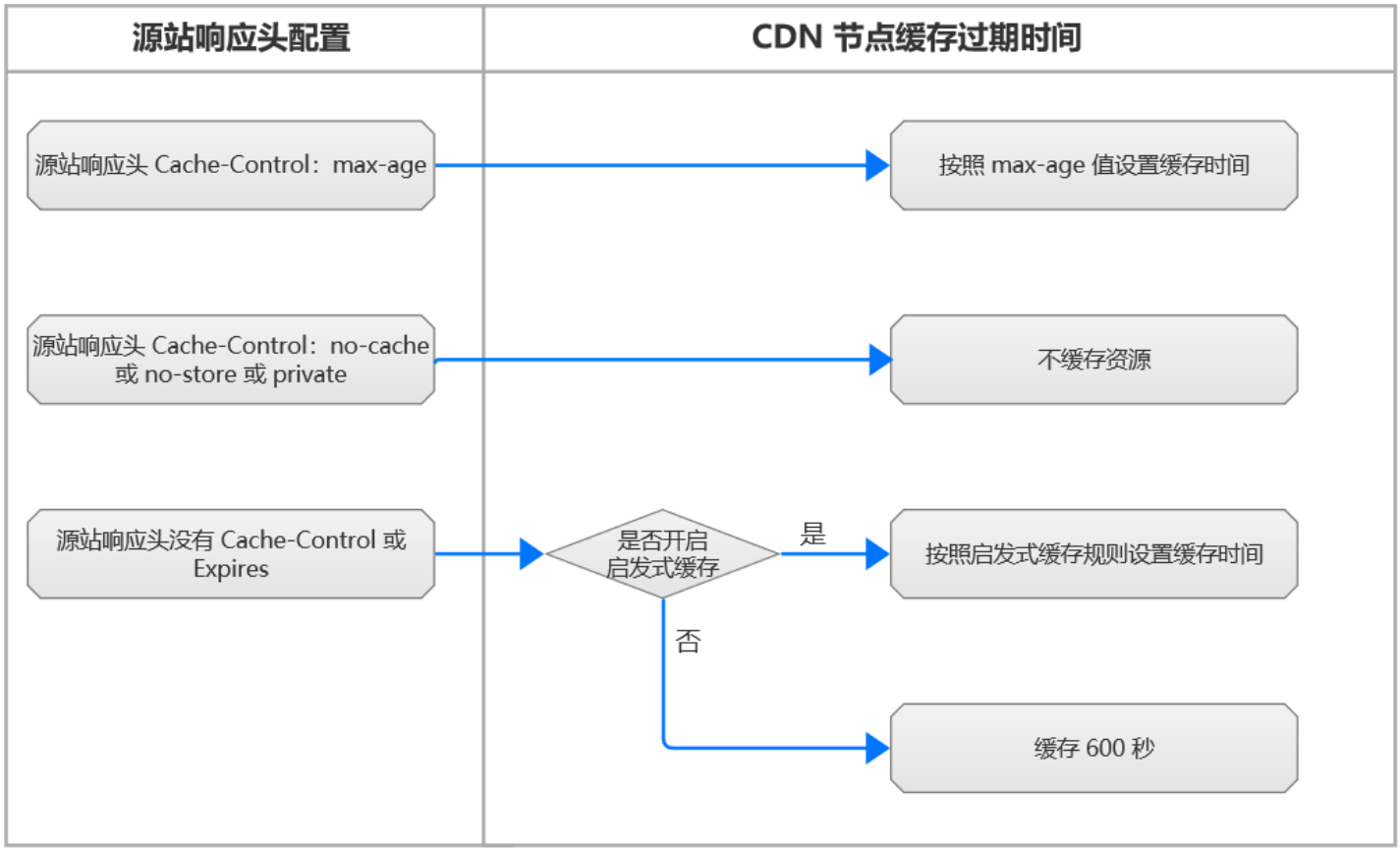
5. 单击**新增规则**，可进入新增规则页面，新增节点缓存过期配置。

配置项	说明
类型	支持对全部文件、文件后缀、文件目录、全路径文件、首页进行配置： 全部文件：指定全部文件设置规则，默认规则。 文件后缀：指定文件的后缀设置规则。 文件目录：指定文件的目录设置规则。 全路径文件：指定文件的完整路径设置规则。 首页：指定域名根目录设置规则。
内容	根据选择不同的文件类型，内容输入约束： 类型为全部文件时：固定为全部文件。 类型为文件后缀时：支持输入文件后缀名，多个以 “;” 为间隔。例如，jpg;png;css。 类型为文件目录时：支持输入文件目录，不能以 “/” 结尾，多个以 “;” 分隔。例如，/test;/a/b/c。 类型为全路径文件时：支持输入文件完整路径，多个以 “;” 分隔。例如，/index.html;/test/.jpg。

配置项	说明
缓存选项	支持按照遵循源站、缓存、不缓存规则配置： 遵循源站：按照源站响应头 Cache-Control 头部，设置 CDN 节点缓存时间，支持设置启发式缓存。 缓存：自定义设置 CDN 节点的缓存时间，支持设置强制缓存。 不缓存：设置 CDN 节点 不缓存资源。

腾讯云 CDN 缓存规则及优先级

缓存选项为：遵循源站



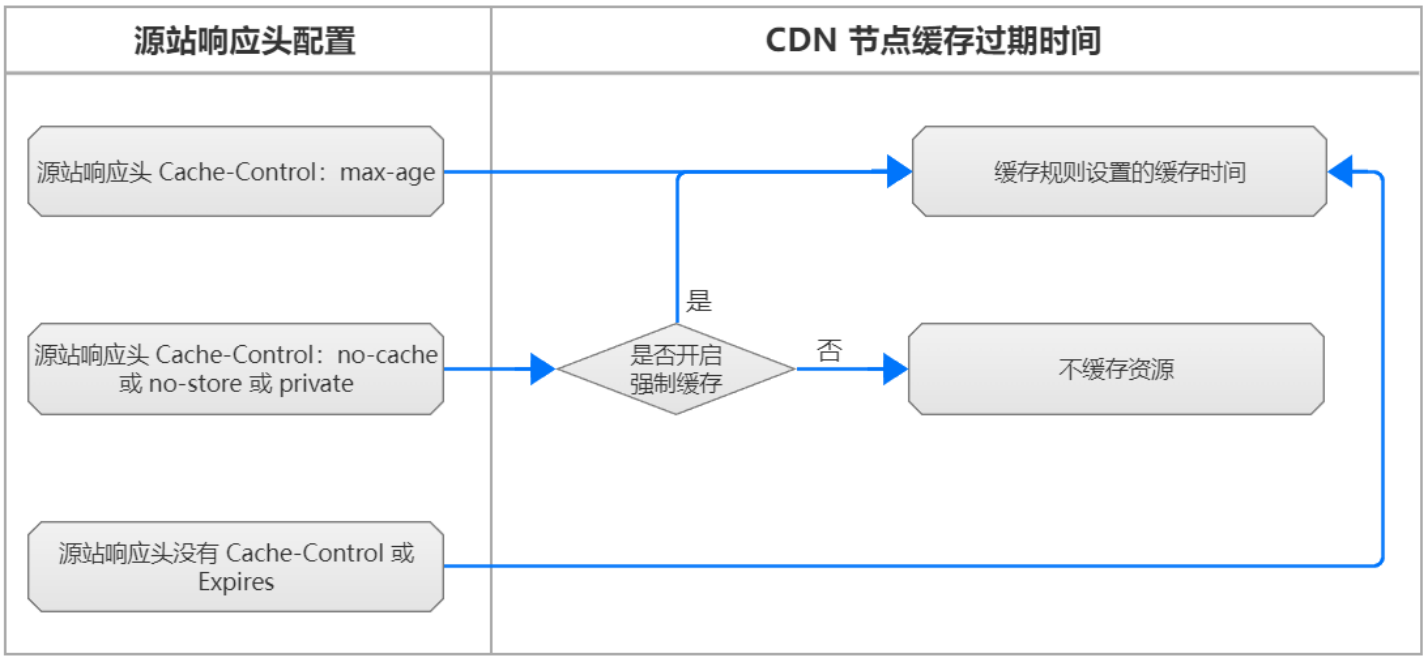
CDN 节点将遵循源站响应头 Cache-Control 头部设置缓存时间。

- 源站响应头 Cache-Control 字段为 max-age，按照 max-age 值设置 CDN 节点缓存时间，如 Cache-Control：max-age=300，则缓存时间为 300 秒；
  - 源站响应头 Cache-Control 字段为 no-cache 或 no-store 或 private，CDN 节点不缓存资源；
  - 源站响应头没有 Cache-Control 或 Expires 时，按照启发式缓存状态设置缓存规则，详情如下：
    - 关闭启发式缓存，当源站响应头没有：Cache-Control 或 Expires 时，则缓存时间为 600 秒。
    - 开启启发式缓存，当源站响应头没有：Cache-Control 或 Expires 时，按照如下规则设置启发式缓存时间：

      i. 默认配置：如果源站响应头存在 Last-Modified，则缓存时间=（当前时间 - Last-Modified）* 0.1，如果源站响应头不存在 Last-Modified，则默认缓存时间为 600 秒。

ii. **自定义策略**：可自定义设置启发式缓存的时间。

缓存选项为：缓存



自定义设置 CDN 节点的缓存时间。

- 关闭强制缓存：
  - 源站响应头 Cache-Control 字段为 max-age 或 源站响应头没有 Cache-Control ，按照自定义 CDN 节点缓存规则缓存。
  - 源站响应头 Cache-Control 字段为 no-cache 或 no-store 或 private，CDN 节点不缓存资源

- 开启强制缓存：忽略源站响应头Cache-Control ，按照自定义 CDN 节点缓存规则缓存。

缓存选项为：不缓存

设置 CDN 节点 不缓存资源。该资源的每个用户请求，CDN 节点都将直接回源获取资源响应给用户。

多条缓存规则优先级

若同时配置多条缓存规则时，底部规则**优先级大于**顶部规则。可通过单击**调整优先级**，拖动缓存规则顺序调整优先级。

推荐配置

- 不常更新的静态文件（例如，图片类型、应用下载类型等），建议设置30天。
- 频繁更新的静态文件（例如，js、css等），建议根据业务的更新频率设置缓存时间。
- 动态文件（例如，php、jsp、asp、aspx等动态文件），**需设置不缓存**。
- 其他涉及 **站点登入**（例如，wordpress 后台登入目录 /wp-admin）或 **接口查询** 等需要和源站直接交互的请求，**需设置不缓存**，否则可能导致访问错误。

配置约束

- 单个域名至多可添加100条缓存规则。
- 多条缓存规则优先级：底部优先级大于顶部。
- 单条文件后缀/文件目录/全路径文件规则中，至多可输入100组内容，不同内容之间用“;”分隔。例如：文件后缀 jpg;png。
- 若您未配置任何规则或请求未命中配置的规则时，CDN 节点将遵循源站响应头 Cache-Control 头部设置缓存时间；若源站响应头没有 Cache-Control 字段，CDN 节点默认对该资源缓存600s。
- CDN 节点仅缓存 GET、HEAD 请求类型的请求内容，其余 POST、OPTIONS 等请求类型的请求内容，CDN 节点不缓存。

配置示例

示例1

原缓存规则为：php;jsp;asp;aspx文件后缀的资源不缓存，其余全部文件缓存30天。

现需要增加：jpg、png文件后缀的资源缓存10天，且需要忽略源站响应头 Cache-Control ，即开启强制缓存；其余全部文件的缓存规则修改为遵循源站。

1. 单击**新增规则**，类型为文件后缀，内容为jpg;png，缓存选项为缓存，缓存时间为10天，强制缓存为是，单击**确定**。

2. 选择全部文件的缓存规则，单击**修改**，修改缓存选项为遵循源站，单击**确定**。

3. 调整完成后的缓存规则为：
   - jpg、png 文件后缀的资源缓存10天，强制缓存；
   - php;jsp;asp;aspx 文件后缀的资源不缓存；
   - 其余全部文件缓存30天。

则实际缓存情况如下：
   - www.test.com/abc.jpg 资源节点缓存时间为10天，即使源站响应头 Cache-Control 字段为 no-cache 或 no-store 或 private。
   - www.test.com/def.php 资源不会缓存至节点；

示例2

使用 WordPress 建站的节点缓存过期配置建议：

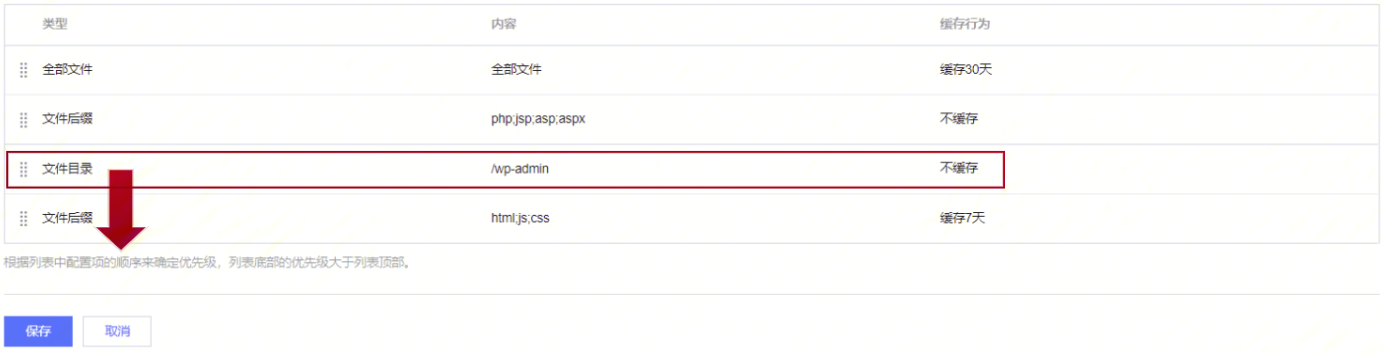
- 后台登入地址/wp-admin目录下的资源，需要设置不缓存，否则会导致后台登入相关资源被缓存，登录出错。如果有其他接口相关的资源，同样需要设置不缓存。
- php;jsp;asp;aspx 动态文件后缀的资源，需要设置不缓存（CDN 默认缓存规则）；
- html;js;css 后缀文件更新较频繁，需要根据更新频率设置缓存时间。建议设置缓存时间7天，不设置强制缓存；
- 其余全部文件缓存30天（CDN 默认缓存规则）。

在 CDN 默认缓存规则的基础下，按如下操作新增规则：

1. 单击**新增规则**，类型为目录，内容为 /wp-admin，缓存选项为不缓存，单击**确定**。

2. 单击**新增规则**，类型为文件后缀，内容为 html;js;css，缓存选项为缓存，缓存时间为7天，强制缓存为否，单击**确定**。

3. 按照优先级顺序，底部优先级高于顶部，单击**调整优先级**，拖动"/wp-admin目录不缓存规则"规则调整至底部，使该规则优先级最高。



4.调整完成后的缓存规则为： - /wp-admin 目录下的所有资源不缓存； - html;js;css 文件后缀的资源缓存7天； - php;jsp;asp;aspx 文件后缀的资源不缓存； - 其余全部文件缓存30天。

常见问题

- 源站变更文件后，CDN 加速节点上的缓存会主动、实时更新的吗?
- 如何判断用户访问是否命中 CDN 节点缓存?

状态码缓存配置

最近更新时间：2021-11-05 10:22:13

配置场景

正常情况下，CDN 节点成功从源站拉取到所请求的资源（2XX状态码）时，将按照节点缓存过期配置的规则进行处理。
若源站无法迅速响应非2XX状态码，且不希望所有请求全部透传回源站，可通过配置状态码缓存过期时间，由 CDN 节点直接响应非2XX状态码，减轻源站压力。
当前支持以下状态码：

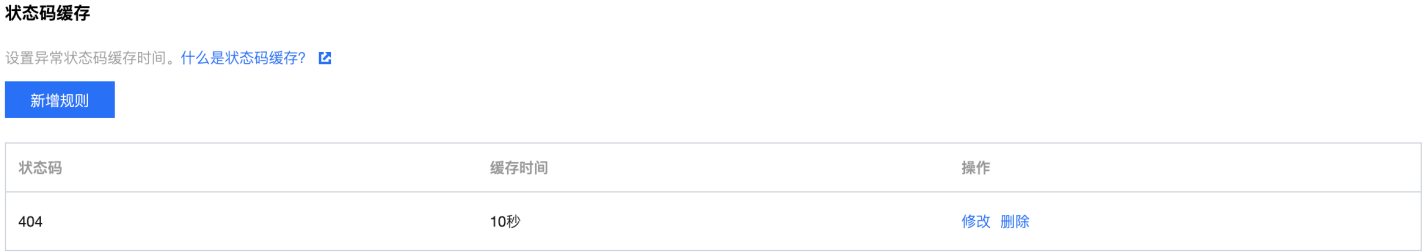
- 4XX：400、401、403、404、405、407、414
- 5XX：500、501、502、503、504、509、514

> ⚠ 注意：
>
> - 部分平台升级中，暂仅支持404和403状态码。
> - 中国境外暂仅支持404和403状态码。若域名的加速区域为全球，则404和403以外的状态码缓存规则仅生效中国境内。

配置指南

查看配置

登录 CDN 控制台，在菜单栏里选择【域名管理】，单击域名操作列的【管理】，进入域名配置页面，切换 Tab 至【缓存配置】，即可找到【状态码缓存】。
默认情况下，有一条“404 - 缓存10秒”的规则：



新增规则

您可按需添加状态码缓存规则，单击【新增状态码缓存】：

配置约束：

- 一个状态码仅支持添加一条规则，不可重复添加。
- 缓存时间为0时，即不缓存。

HTTP 头部缓存配置

最近更新时间：2022-06-20 10:12:48

配置场景

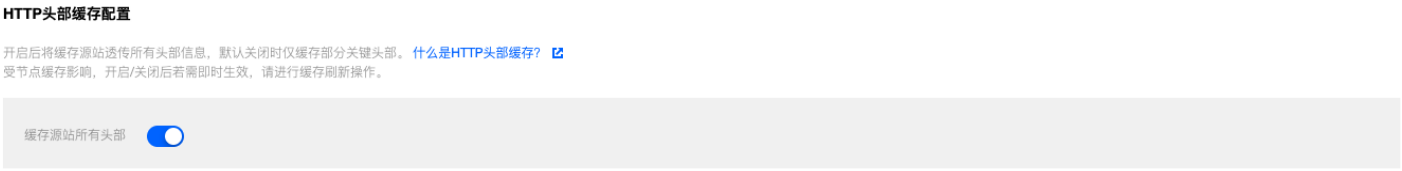
HTTP 头部缓存配置可以设置腾讯云 CDN 是否缓存源站 HTTP 头部：

- 开启：CDN 将缓存所有源站 HTTP 头部，若通过 HTTP 响应头配置 修改头部，则优先匹配 CDN 配置；
- 关闭：CDN 只缓存下述源站 HTTP 头部：
  - Access-Control-Allow-Origin
  - Timing-Allow-Origin
  - Content-Disposition
  - Accept-Ranges

配置指南

查看配置

登录 CDN 控制台，在菜单栏里选择【域名管理】，单击域名右侧【管理】，即可进入域名配置页面，第三栏【缓存配置】中可看到 HTTP 头部缓存配置，默认情况下为开启状态，您可按需自主关闭配置。



访问 URL 重写配置

最近更新时间：2021-06-30 11:47:57

配置场景

若您需要将实际访问的 URL 修改为与源站匹配的 URL，腾讯云 CDN 为您提供了访问 URL 重写配置功能。

您可通过自定义访问 URL 重写配置，将 URL 302 重定向到目标 URL。

配置指南

查看配置

登录 CDN 控制台，在左侧菜单栏选择【域名管理】，单击域名操作列的【管理】，进入域名配置页面，切换 Tab 至【缓存配置】，即可找到【访问 URL 重写配置】。

默认情况下，访问 URL 重写配置为关闭状态：

新增规则

您可按需添加重写规则，单击【新增重写规则】：

配置约束

- 单个域名至多可添加100条重写规则。
- 多条规则支持调整优先级：底部优先级大于顶部。
- 待重写 URL：以/开头，支持全路径匹配（例如：/test/a.jpg）和通配符 * 匹配（例如：/test/*/*.jpg）。若指定文件目录，不能以“/”结尾（例如：/test）。
- 目标 Host：默认为当前域名（默认带http头），可修改为其他域名，必须包含 http:// 或 https:// 头。
- 目标 Path：以/开头（例如：/newtest/b.jpg），通配符 * 可通过 $n 捕获（n=1,2,3...，例如：/newtest/$1/$2.jpg）。若指定文件目录，不能以“/”结尾（例如：/test）。
- 通配符 * 最多可输入5个，捕获占位符 $n 最多可输入10个。
- 不支持提交中文内容，输入框中的内容长度不可超过1024个字符

配置示例

若加速域名 www.test.com 的 **访问 URL 重写配置** 如下：

则实际访问情况如下：

- **客户端请求** www.test.com/test/a.jpg，**CDN 节点将返回** www.test.com/newtest/b.jpg **的内容。**
- **客户端请求** www.test.com/test/a.png，**CDN 节点将返回** www.newtest.com/newtest/a.png **的内容。**

版权所有：腾讯云计算（北京）有限责任公司

浏览器缓存过期配置

最近更新时间：2021-11-05 10:04:00

功能介绍

浏览器缓存过期配置支持自定义配置客户端浏览器的缓存策略，降低回源率。

> **说明：**
> 请求资源时，若浏览器有缓存，会优先返回资源。浏览器无缓存就会去节点请求，若节点有缓存则返回资源，无缓存就回源获取。

配置指南

查看配置

登录 CDN 控制台，在左侧菜单栏选择【域名管理】，单击域名操作列的【管理】，进入域名配置页面，切换 Tab 至【缓存配置】，即可找到【浏览器缓存过期配置】。

新增规则

您可按需添加浏览器缓存过期规则，单击【新增规则】，支持指定文件类型/文件目录/文件路径/首页配置缓存行为：

- 遵循源站：遵循源站的 Cache-Control 头部。源站无 CC 头部或 CC 头部为 no-cache/no-store/private，则浏览器不缓存资源。
- 缓存：源站 CC 头部不为 no-cache/no-store/private 时，遵循控制台浏览器缓存配置规则，否则，浏览器不缓存资源。
- 不缓存：浏览器不缓存资源。

配置约束

- 单个域名至多可添加20条规则，全部文件和首页类型规则，至多可添加1条。
- 多条规则支持调整优先级：底部优先级大于顶部。
- 单条文件类型/文件目录/文件路径规则中，至多可输入50组内容，不同内容之间用“;”分隔。例如：文件类型 - jpg;png。
- 不支持提交中文内容。

平台默认策略

若您未配置任何规则或请求未命中配置的规则时，默认遵循以下平台策略：

- 当用户请求您某一业务资源时，若源站对应的 HTTP Response Header 中存在 Cache-Control 字段，则遵循该 Cache-Control 。
- 若源站对应的 HTTP Response Header 中无 Cache-Control 字段，则：浏览器默认对该资源缓存 600s。

若您已配置/命中控制台 节点缓存过期配置 时：

- 若源站对应的 HTTP Response Header 中无 Cache-Control 字段，则浏览器不缓存资源。
- 若源站对应的 HTTP Response Header 中存在 Cache-Control 字段，则浏览器缓存遵循该 Cache-Control。

缓存配置常见问题

最近更新时间：2022-06-08 12:00:33

什么是节点缓存过期配置?

节点缓存过期配置是指配置 CDN 加速节点在缓存您的业务内容时遵循的一套过期规则。
CDN 节点上缓存的用户资源都面临“过期”问题。若资源处于未过期状态，当用户请求到达节点后，节点会将此资源直接返回给用户，提升获取速度；当资源处于过期状态（即超过了设置的有效时间），此时用户请求会由节点发送至源站，若源站内容已更新，则重新获取内容并缓存至节点，同时返回给用户，若源站内容未更新，则仅更新资源在节点的缓存时间。合理地配置缓存时间，能够有效的提升命中率，降低回源率，节省您的带宽。

如何控制文件在浏览器的缓存时间?

控制台已支持配置浏览器缓存过期时间，详情请见 浏览器缓存过期配置。

CDN 如何设置部分文件缓存，部分文件不缓存直接回源?

您可以按照目录、文件路径、文件类型设置对应的缓存时间。详情请参见 节点缓存配置。
当缓存选项为不缓存时，CDN 节点不缓存该资源，用户每次发送访问请求至 CDN 节点时，CDN 节点都会直接回源站拉取相应文件。例如，需要设置 php;jsp;asp;aspx 动态文件不缓存，html 文件缓存1天，其余文件缓存30天。则按照优先级规则底部优先级大于顶部，则节点缓存过期配置如下图：

类型	内容	缓存行为	操作
全部文件	全部文件	缓存30天，强制缓存	修改 | 删除
文件后缀	html	缓存1天	修改 | 删除
文件后缀	php;jsp;asp;aspx	不缓存	修改 | 删除

CDN支持哪些缓存过期配置?

CDN 支持配置各文件类型的缓存过期时间、是否忽略参数、是否忽略大小写、是否遵循源站、启发式缓存等缓存规则。合理地配置缓存规则，能够有效提升命中率，降低回源率，节省您的带宽。详情请参见 缓存配置 和 节点缓存配置 。

CDN 默认的缓存配置是什么?

接入加速域名时，根据不同的业务类型，CDN 会添加默认的节点缓存过期规则，您可按需调整：

- CDN – 网页小文件/下载大文件/音视频点播 & ECDN – 动静加速：常规的动态文件（如 php;jsp;asp;aspx）不缓存，其他文件默认缓存30天。
- ECDN – 动态加速：全部文件不缓存。

若您未配置任何规则或请求未命中配置的规则时，默认遵循以下平台策略：

- 当用户请求您某一业务资源时，若源站对应的 HTTP Response Header 中存在 Cache-Control 字段，则遵循该 Cache-Control 。
- 若源站对应的 HTTP Response Header 中无 Cache-Control 字段，则：CDN 节点默认对该资源缓存600s。

缓存的匹配方式是什么?

当设置了多条缓存策略时，相互之间会有重复，配置项列表底部优先级高于顶部优先级。假设某域名配置了如下缓存配置：

```
所有文件30天
.php .jsp .aspx 0秒
.jpg .png .gif 300秒
/test/*.jpg 400秒
/test/abc.jpg 200秒
```

假设域名为 www.test.com ，资源为 www.test.com/test/abc.jpg ，其匹配方式如下：

1. 匹配第一条所有文件，命中，此时缓存时间为30天。
2. 匹配第二条，未命中。
3. 匹配第三条，命中，此时缓存时间为300秒。
4. 匹配第四条，命中，此时缓存时间为400秒。
5. 匹配第五条，命中，此时缓存时间为200秒。

因此最终缓存时间为200秒，以最后一次匹配生效。

如何判断用户访问是否命中 CDN 节点缓存?

可以根据 HTTP 响应头的 X-Cache-Lookup 的值判断是否命中 CDN 节点缓存，可能同时存在多个 X-Cache-Lookup 头，用于表示不同层级的命中状态。
当 X-Cache-Lookup 有返回以下任意一个值，即代表缓存命中，否则代表缓存未命中。
X-Cache-Lookup: Hit From MemCache
X-Cache-Lookup: Hit From Disktank

X-Cache-Lookup: Cache Hit

源站变更文件后，CDN 加速节点上的缓存会主动、实时更新的吗?

CDN 加速节点上的缓存内容不会主动、实时更新。

- CDN 节点根据您在控制台配置的 节点缓存过期配置 规则更新缓存；若源站变更文件，但 CDN 缓存未达到过期时间，不会主动回源更新文件，此时将造成源站文件和 CDN 缓存的文件不一致。
- 若源站资源更新后，需要立刻更新 CDN 节点的缓存，可使用 缓存刷新 功能主动更新 CDN 节点未过期的缓存，使 CDN 节点缓存与源站资源保持一致。
- 若您需要定时更新某个文件的缓存，可以通过 定时刷新预热 按时触发刷新任务。

回源配置
分片回源配置

最近更新时间：2021-12-15 10:38:05

配置场景

腾讯云 CDN 在缓存资源时，为提高存储效率会将文件进行切片存储，并且支持 Range 请求，若请求时携带 HTTP 头部 Range: bytes = 0-999 ，则返回文件的前1000个字节给用户。

开启分片回源配置，若用户请求的部分文件已过期，CDN 会根据用户请求进行分片回源，仅拉取用户需要的部分文件进行缓存，同时返回给用户；关闭分片回源配置，即便用户请求的是部分文件，CDN 在回源时仍会拉取整个文件，而后进行缓存，并响应给用户其要求的部分文件。

开启分片回源配置能够有效提高大文件分发效率，提升响应速度，降低源站压力。

> 说明：
>
> - 开启分片回源配置后，资源在节点上分片缓存，但所有分片的缓存过期时间保持一致，按照用户指定的缓存过期规则。
> - 若您的资源都是静态小文件，或源站为 COS 源站且**已使用**数据处理类功能（例如：图片处理），不建议开启分片回源，开启后会影响回源。
> - 若您的资源都是静态大文件，且源站已支持 Range 请求，或源站为 COS 源站且**未使用**数据处理类功能（例如：图片处理），建议开启分片回源，提升分发效率和响应速度。
> - 开启分片回源配置时，需要确认源站已经支持 Range 请求，否则可能会导致回源失败。

配置指南

添加域名

添加加速域名时，根据不同的业务类型和源站类型，分片回源默认关闭或开启，您可按需调整，或添加域名后前往此配置项管理配置规则。

管理域名

域名添加后，单击域名操作列的**管理**，进入域名配置页面，切换 Tab 至**回源配置**，即可找到**分片回源配置**。

配置约束

1. 全部文件规则 – 默认最低优先级，不可调整优先级，不可删除。
2. 支持添加按文件后缀/文件目录/全路径文件配置的规则，最多可添加20条规则，可调整优先级。

配置示例

若域名 cloud.tencent.com 的分片回源配置如下：

用户 A 请求资源： http://cloud.tencent.com/test.apk ，节点收到请求后，发现缓存的 test.apk 文件已过期，此时发起回源请求，节点回源使用 Range 请求，分片获取资源并缓存。若此时用户 B 发起的也为 Range 请求，当节点上存储的分片已满足 Range 中指定的字节段，则会直接返回给用户，无需等所有分片获取完毕。

回源301/302跟随

最近更新时间：2021-11-05 10:31:34

配置场景

腾讯云 CDN 默认不缓存301/302状态码，当源站返回301/302请求后，CDN 节点默认会将响应返回给用户端，由用户端重定向到对应的资源进行访问。

通过开启回源跟随301/302配置，CDN 节点在回源时遭遇301/302时会主动跟随跳转，直至获取所需资源（最多可跟随3次），返回实际的资源给到用户端，用户端无需跳转。

点击查看视频

配置指南

登录 CDN 控制台，在左侧菜单栏选择【域名管理】，单击域名操作列的【管理】，进入域名配置页面，切换 Tab 至【回源配置】，即可找到【回源跟随301/302配置】。默认情况下为关闭状态，您可按需自主开启配置。

配置示例

若域名 cloud.tencent.com 的回源跟随301/302配置如下：

用户 A 请求资源： http://cloud.tencent.com/1.jpg ，在节点未命中缓存，则节点会请求源站获取所需资源，若源站返回的 HTTP Response 状态码为302，跳转指向地址为 http://cloud.tencent.com/2.jpg ，则：

1. 开启回源跟随301/302配置后，节点收到状态码为301/302的 HTTP Response 后，会直接向跳转指向的地址发起请求。
2. 获取到所需资源后，缓存至节点，并返回给用户。
3. 此时用户 B 也向http://cloud.tencent.com/1.jpg发起请求，则会在节点直接命中并返回给用户。

4. 开启回源跟随301/302配置后，最多仅跟随3次跳转，超出限制则会直接返回301/302给客户。

若域名 cloud.tencent.com 的回源跟随301/302配置如下：

用户 A 请求资源： http://cloud.tencent.com/1.jpg ，在节点未命中缓存，则节点会请求源站获取所需资源，若源站返回的 HTTP Response 状态码为301/302，跳转指向地址为 http://xxx.tencent.com/1.jpg ，则：

1. 节点将该 HTTP Response 直接返回给用户。
2. 用户向http://xxx.tencent.com/1.jpg发起请求，若该域名未接入 CDN，则不会有加速效果。
3. 若此时用户 B 也向http://cloud.tencent.com/1.jpg 发起请求，则会重复上述流程。

回源超时时间配置

最近更新时间：2021-11-05 10:19:37

配置场景

腾讯云 CDN 在返回用户源站时，默认情况下 TCP 连接超时时间为5秒，回源加载数据超时时间为10秒，若回源时超出上述时间设置，往往会出现回源失败的情况。

您可以根据源站数据处理情况及网络情况，调整回源 TCP 连接超时时间、回源加载数据超时时间，保障正常回源。

配置指南

查看配置

登录 CDN 控制台，在菜单栏里选择【域名管理】，单击域名右侧【管理】，即可进入域名配置页面，【回源配置】中可看到回源超时配置，默认情况下：

- TCP 连接超时时间为5秒。
- 回源加载超时时间为10秒。

修改配置

通过单击右侧【编辑】，可按需修改对应的超时时间：

- TCP 连接超时时间可设置为5 – 60秒。

- 回源加载超时时间可设置为5 – 60秒。

> **注意：**
> 若您的加速域名服务区域为全球加速，设置的回源超时时间为全球生效，不支持境内、境外差异化配置。

回源 HTTP 请求头配置

最近更新时间：2021-12-07 14:46:32

功能介绍

腾讯云 CDN 默认支持携带一些头部回源，也支持自定义配置回源 HTTP 请求头部，供您统计和分析源站业务状况。

> ⚠ 注意：
>
> - 腾讯云 CDN 默认支持携带 X-Forwarded-For（真实客户端 IP）和 X-Forwarded-Proto（真实客户端请求协议），您无需再配置。
> - 若您已对全部文件配置增加头部 X-Forward-For，建议您删除该规则，使用默认的标准头部 X-Forwarded-For 即可（**请注意此处头部参数的名称变化**）。
> - 2021年12月6日后创建的域名，会默认配置头部 Tencent-Acceleration-Domain-Name（加速域名），您可在配置处修改删除。

操作指南

查看配置

登录 CDN 控制台，在菜单栏里选择【域名管理】，单击域名右侧【管理】，即可在【回源配置】中看到回源 HTTP 请求头配置，默认情况下为关闭状态，无任何配置：

操作类型

操作类型	说明
设置	变更指定请求头部参数的取值为设置后的值。 若设置的头部不存在，则会增加该头部。 若回源请求头部参数已存在，则设置的请求头会覆盖原有头部且唯一。

操作类型	说明
增加	增加指定的回源请求头部参数。 若设置的头部已存在，则增加的请求头会覆盖原有头部且唯一。
删除	删除指定的请求头参数。

⚠ 注意：

- 底部优先级大于顶部 – 此相对位置的优先级仅限于同类型头部操作中，例如多条增加头部规则之间、多条删除头部规则之间或多条设置头部规则之间。
- 当不同的头部操作类型同时作用于同一个回源请求头参数的时候，按照操作类型的优先级来执行，顺序为：增加 > 删除 > 设置。例如：同时存在增加、删除和设置X-CDN头部的规则时，会先增加，再删除，最后再设置。

头部参数

头部参数	说明
X-Forward-Port	用于携带用户端真实端口的头部。其值默认为 $remote_port 变量，不允许修改。
Tencent-Acceleration-Domain-Name	用于携带用户加速域名的头部，其值为 $host 变量。
自定义头部	自定义头部的Key 值长度默认为1 – 100个字符，由数字0 – 9、字符a – z、A – Z，及特殊符 - 组成。 Value 长度为1 – 1000个字符，不支持中文。 部分标准头部不支持自助设置/增加/删除，具体清单请参见文档 注意事项。

⚠ 注意：

- 回源 HTTP 请求头配置规则最多可配置10条。
- 生效类型支持全部文件、文件类型、文件目录、指定文件路径四种模式，暂不支持正则匹配。

配置示例

若加速域名 cloud.tencent.com 的回源 HTTP 请求头配置如下：

若访问资源为： http://cloud.tencent.com/test/test.mp4

命中 mp4 文件后缀及 /test 目录，因是同一头部操作类型 – 增加，则底部优先级大于顶部，因此增加 x-cdn:Tencent 头部。

注意事项

以下标准头部暂时不支持设置/增加/删除回源 HTTP 请求头：

www-authenticate	authorization	proxy-authenticate	proxy-authorization
age	cache-control	clear-site-data	expires
pragma	warning	accept-ch	accept-ch-lifetime
early-data	content-dpr	dpr	device-memory
save-data	viewport-width	width	last-modified
etag	if-match	if-none-match	if-modified-since
if-unmodified-since	vary	connection	keep-alive
accept	accept-charset	expect	max-forwards

www-authenticate	authorization	proxy-authenticate	proxy-authorization
access-control-allow-origin	access-control-max-age	access-control-allow-headers	access-control-allow-methods
access-control-expose-headers	access-control-allow-credentials	access-control-request-headers	access-control-request-method
origin	timing-allow-origin	dnt	tk
content-disposition	content-length	content-type	content-encoding
content-language	content-location	forwarded	x-forwarded-host
x-forwarded-proto	via	from	host
referer-policy	allow	server	accept-ranges
range	if-range	content-range	cross-origin-embedder-policy
cross-origin-opener-policy	cross-origin-resource-policy	content-security-policy	content-security-policy-report-only
expect-ct	feature-policy	strict-transport-security	upgrade-insecure-requests

www-authenticate	authorization	proxy-authenticate	proxy-authorization
x-content-type-options	x-download-options	x-frame-options(xfo)	x-permitted-cross-domain-policies
x-powered-by	x-xss-protection	public-key-pins	public-key-pins-report-only
sec-fetch-site	sec-fetch-mode	sec-fetch-user	sec-fetch-dest
last-event-id	nel	ping-from	ping-to
report-to	transfer-encoding	te	trailer
sec-websocket-key	sec-websocket-extensions	sec-websocket-accept	sec-websocket-protocol
sec-websocket-version	accept-push-policy	accept-signature	alt-svc
date	large-allocation	link	push-policy
retry-after	signature	signed-headers	server-timing
service-worker-allowed	sourcemap	upgrade	x-dns-prefetch-control
x-firefox-spdy	x-pingback	x-requested-with	x-robots-tag
x-ua-compatible	max-age		

回源 URL 重写

最近更新时间：2021-11-17 15:03:02

配置场景

若您需要将回源请求 URL 修改为与源站匹配的 URL，腾讯云 CDN 为您提供了回源 URL 重写配置功能。

> **注意：**
> ECDN 域名暂不支持此功能配置。

配置指南

查看配置

登录 CDN 控制台，在左侧菜单栏选择【域名管理】，单击域名操作列的【管理】，进入域名配置页面，切换 Tab 至【回源配置】，即可找到【回源 URL 重写配置】。

新增规则

您可按需添加重写规则，单击【新增规则】：

配置约束

- 单个域名至多可添加100条重写规则。
- 多条规则支持调整优先级：底部优先级大于顶部。
- 待重写回源 URL：以 / 开头，默认为前缀匹配，支持通配符 * 匹配（例如：/test/*/*.jpg）。若指定文件目录，不能以“/”结尾（例如：/test）。如需全路径匹配，可在上方匹配设置中勾选开启，开启后将不支持通配符* 。
- 目标回源 Host：默认为当前域名，可修改，不包含 http:// 或 https:// 头。
- 目标回源 Path：以 / 开头（例如：/newtest/b.jpg），通配符 * 可通过 $n 捕获（n=1,2,3...，例如：/newtest/$1/$2.jpg）。若指定文件目录，不能以“/”结尾（例如：/test）。
- 通配符 * 最多可输入5个，捕获占位符 $n 最多可输入10个。
- 不支持提交中文内容，目标回源 Host 不可超过250个字符，其他输入框中的内容长度不可超过1024个字符。

配置示例：

若加速域名 www.test.com 的 **回源 URL 重写配置** 如下：

如上配置，则实际回源情况如下：

- 回源请求 www.test.com/images/2.jpg，命中第2、3、4条规则，则底部优先级最大，实际回源请求为 www.test.com/index.html。
- 回源请求 www.test.com/images，命中第3条规则，则实际回源请求为 www.test.com/goodboy.html。
- 回源请求 www.test.com/images/1.jpg，命中第1、2、3、4条规则，底部优先级最大，实际回源请求为 www.test.com/index.html。

版权所有：腾讯云计算（北京）有限责任公司

回源 SNI

最近更新时间：2021-07-26 11:39:30

配置场景

若您的源站 IP 绑定了多个域名，当 CDN 节点以 HTTPS 协议访问源站时，您可以设置回源 SNI，指明具体的访问域名。

> ⚠ 注意：
>
> - 回源 SNI 暂仅支持中国境内加速域名。
> - 部分平台正在升级中，暂未开放此配置功能。

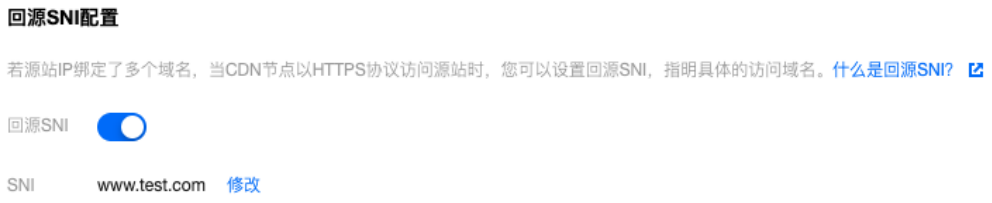
配置指南

查看配置

默认情况下，回源 SNI 为关闭状态，您可按照实际需要自主开启。

编辑配置

开启后，需要设置回源 SNI，配置具体的访问域名。也可以再关闭配置开关，开关为关闭状态时，即使下方存在具体的配置，仍不会现网生效，仅当开启开关时，才会发布至现网。



HTTPS 配置
HTTPS 配置须知

最近更新时间：2021-11-29 17:35:21

若您要为您的域名上传并配置自有证书，请先了解以下内容。若您要配置的是来源于腾讯云 SSL 证书管理中已有的证书，可跳过上传证书部分，直接查看 托管证书 的相关内容。

上传证书

CA 机构提供的证书一般包括以下几种，其中 CDN 使用的是 Nginx：

进入 Nginx 文件夹，使用文本编辑器打开 “.crt”（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：

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
tTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSoAYykwOTEvMC0GA1UEAxMm
VmVyaVNpZ24gQ2xhc3MgMyBTZWN1cmUgU2VydmVyIENBIC0gRzIwHhcNMTAxMDA4
MDAwMDAwWhcNMTMxMDA3MjM1OTU5WjBqMQswCQYDVQQGEwJVUzETMBEGA1UECBMK
V2FzaGluZ3RvbjEQMA4GA1UEBxQHU2VhdHRsZTEYMBYGA1UEChQPQW1hem9uLmNv
bSBJbmMuMRowGAYDVQQDFBFpYW0uYW1hem9uYXdzLmNvbTCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEA3Xb0EGea2dB8QGEUwLcEpwvGawEkUdLZmGL1rQJZdeeN
3vaF+ZTm8Qw5Adk2Gr/RwYXtpx04xvQXmNm+9YmksHmCZdruCrW1eN/P9wBfqMMZ
X964CjVov3NrF5AuxU8jgtw0yu//C3hWnOuIVGdg76626ggOoJSaj48R2n0MnVcC
AwEAAaOCAdEwggHNMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMEUGA1UdHwQ+MDww
OqA4oDaGNGh0dHA6Ly9TVlJTZWN1cmUtRzItY3JsLnZlcmlzaWduLmNvbS9TVlJT
ZWN1cmVHMi5jcmwwRAYDVR0gBD0wOzA5BgtghkgBhvhFAQcXAzAqMCgGCCsGAQUF
BwIBFhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMB0GA1UdJQQWMBQGCCsG
AQUFBwMBBggrBgEFBQcDAjAfBgNVHSMEGDAWgBSl7wsRzsBBA6NKZZBIshzgVy19
RzB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlz
aWduLmNvbTBABggrBgEFBQcwAoY0aHR0cDovL1NWUlNlY3VyZS1HMi1haWEudmVy
aXNpZ24uY29tL1NWUlNlY3VyZUcyLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFow
WDBWFglpbWFnZS9naWYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEF
GDAmFiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZI
hvcNAQEFBQADggEBALpFBXeG782QsTtGwEE9zBcVCuKjrsl3dWK1dFiq30P4y/Bi
ZBYEywBt8zNuYFUE25Ub/zmvmpe7p0G76tmQ8bRp/4qkJoiSesHJvFgJ1mksr3IQ
3gaE1aN2BSUIHxGLn9N4F09hYwwbeEZaCxfgBiLdEIodNwzcvGJ+2LlDWGJOGrNI
NM856xjqhJCPxYzk9buuCl1B4Kzu0CTbexz/iEgYV+DiuTxcfA4uhwMDSe0nynbn
1qiwRk450mCOnqH4ly4P4lXo02t4A/DI1I8ZNct/Qfl69a2Lf6vc9rF7BELT0e5Y
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，机构在颁发证书时会有对应说明，请注意查阅规则说明。

> ⚠ 注意：
>
> - 证书之间不能存在空行
> - 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。

如果您得到是以 “-----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
```

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
```

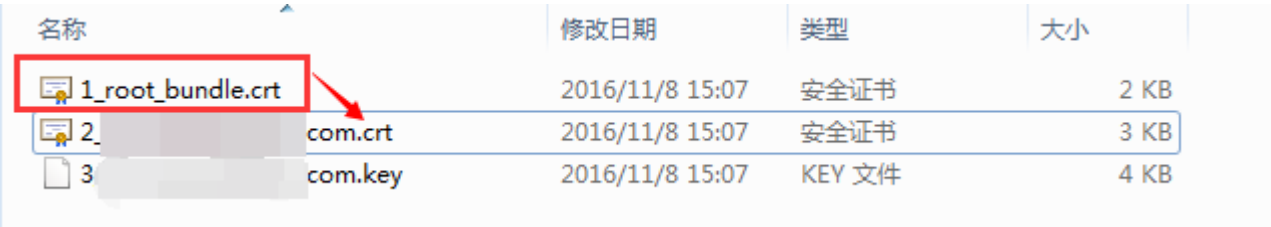
私钥转换：

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

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，您可以参考以下方式补齐证书链：

1. 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。



2. 您也可以参考 其它工具 补齐证书链接后再进行上传配置。

托管证书

腾讯云提供证书托管产品，即 SSL 证书，可将已有证书上传至 SSL 证书管理平台进行统一托管，部署至其他云产品，也可进行证书购买、申请。

腾讯云 SSL 证书为每一个用户免费提供20本由 TrustaAsia 颁发的 DV SSL 证书。

HTTPS 配置指南

最近更新时间：2022-02-28 22:46:05

配置场景

腾讯云 CDN 支持 HTTPS 加速服务，您可以通过上传证书进行部署，也可以将已经托管至腾讯云 SSL 证书管理的证书，直接部署至 CDN 平台，启用 HTTPS 加速服务，实现全网数据加密传输。

配置指南

查看配置

登录 CDN 控制台，在菜单栏里选择**域名管理**，单击域名右侧**管理**，即可进入域名配置页面 **Https 配置**中，查看指定域名的 HTTPS 配置情况：

也可前往左侧菜单栏**证书管理**页面，查看账号下所有配置了 HTTPS 加速的域名列表、证书列表。

- 域名列表：展示已配置证书的域名列表。

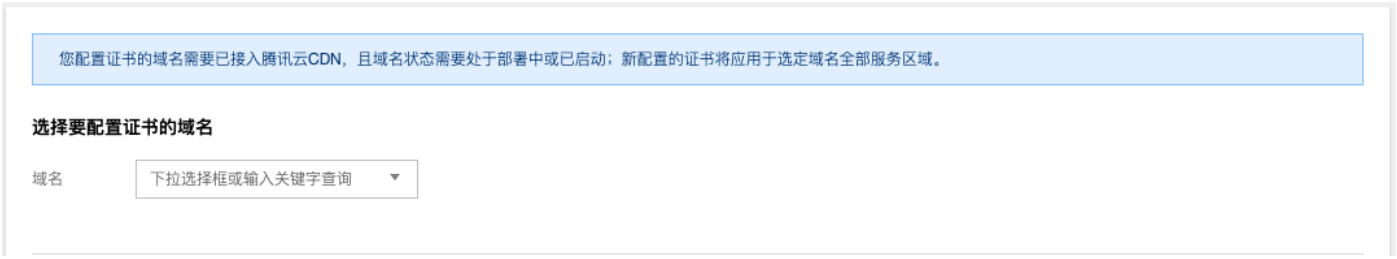
- 证书列表：展示已托管证书列表。

证书配置

1. 选择域名

在**证书管理**菜单栏下，单击**配置证书**，选中需要配置证书的加速域名：

- 加速域名的状态需要为“部署中”或“已启动”，关闭状态的加速域名不可进行 HTTPS 加速配置。
- .file.myqcloud.com后缀为腾讯云对象存储默认加速域名，无需配置证书可直接进行 HTTPS 加速。
- .image.myqcloud.com后缀域名为腾讯云数据万象默认加速域名，无需配置证书可直接进行 HTTPS 加速服务。



2. 选择证书

若已有证书，可直接将 PEM 格式的证书内容和私钥粘贴入对应位置即可：

- 腾讯云 CDN 现已支持 ECC 证书部署。
- 证书内容需要为 PEM 格式，非此格式证书请参考 PEM 格式转换。

- 可选择腾讯云托管证书，直接进行一键部署。

批量配置

单击上方**批量配置**，可通过上传证书，自动匹配适配的域名，进行批量配置：

1. 选择证书

若已有证书，可直接将 PEM 格式的证书内容和私钥粘贴入对应位置即可：

- 腾讯云 CDN 现已支持 ECC 证书部署。
- 证书内容需要为 PEM 格式，非此格式证书请参考 PEM 格式转换。

- 可选择已托管证书，直接进行一键部署。

2. 选择域名

根据上传 / 选择的证书，CDN 会自动匹配出允许配置的域名列表，可按需进行勾选配置：

变更证书

证书修改

单击证书右侧**编辑**，可指定域名进行证书更新，也可重新进行批量配置，覆盖原有证书配置。

域名	加速类型	证书备注	证书来源	到期时间	证书状态	操作
[redacted]	CDN 网页小文件	--	上传托管证书	2023-01-21 10:29:30	配置成功	编辑 删除
[redacted]	CDN 网页小文件	--	上传托管证书	2023-01-21 10:51:22	配置成功	编辑 删除

更新证书全网逐节点生效，无缝切换，不会影响现网 HTTPS 服务，也可单击**删除**，取消 HTTPS 加速服务。

证书过期

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。

区域特殊配置

若加速域名服务区域为全球，则所配置的 HTTPS 证书会境内、境外一起生效，暂时不支持境内境外配置不同证书。

若域名存在境内、境外证书配置不一致的特殊场景，可在**证书管理**页面看到中国境内、中国境外等标识，表明该域名存在遗留的区域特殊配置：

域名	证书备注	证书来源	到期时间	回源协议	证书状态	操作
.com 中国境内	新的泛域名证书	自有证书		协议跟随	配置成功	编辑 删除
.com 中国境外	新的泛域名证书	自有证书		HTTP回源	配置成功	--

在域名高级配置中，也可看见两份配置：

HTTPS配置

HTTPS提供对网络服务器的身份认证，保护交换数据的隐私和完整性。什么是HTTPS?

默认配置

强制跳转HTTPS

客户端双向认证

证书来源	证...	到...	回...	证书...	更多...
腾讯云托管证书...	新...	201...	协...	配置...	前往配

境外配置

强制跳转HTTPS

客户端双向认证

证书来源	证...	到...	回...	证书...	更多...
腾讯云托管证书	新...	2019-09-23	HTT...	配置...	--

强制跳转配置

最近更新时间：2022-01-10 14:15:03

配置场景

腾讯云 CDN 支持配置 HTTPS/HTTP 强制跳转：

- 已经配置了证书进行 HTTPS 加速的域名，可指定301/302跳转方式，将所有到达 CDN 节点的 HTTP 请求强制跳转为 HTTPS。
- 也可指定301/302跳转方式，将所有到达 CDN 节点的 HTTPS 请求强制跳转为 HTTP 请求。
- 跳转时默认不携带 Response header，可变更。

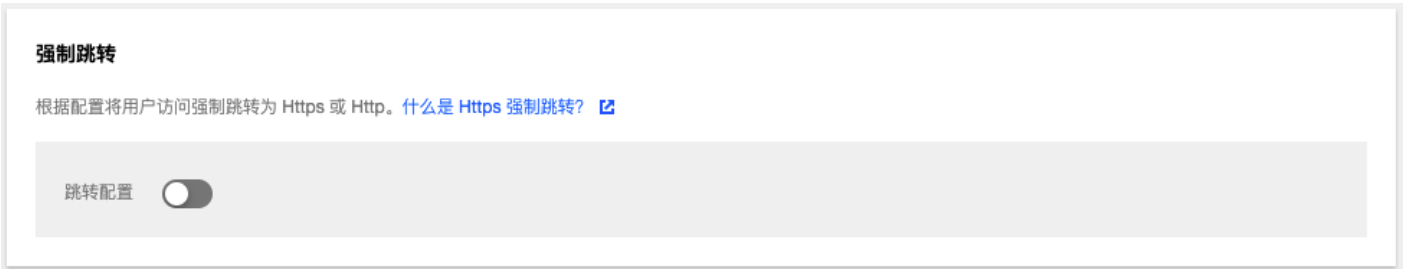
配置指南

配置约束

配置 HTTPS 强制跳转，需要先在 CDN 启用 HTTPS 加速。

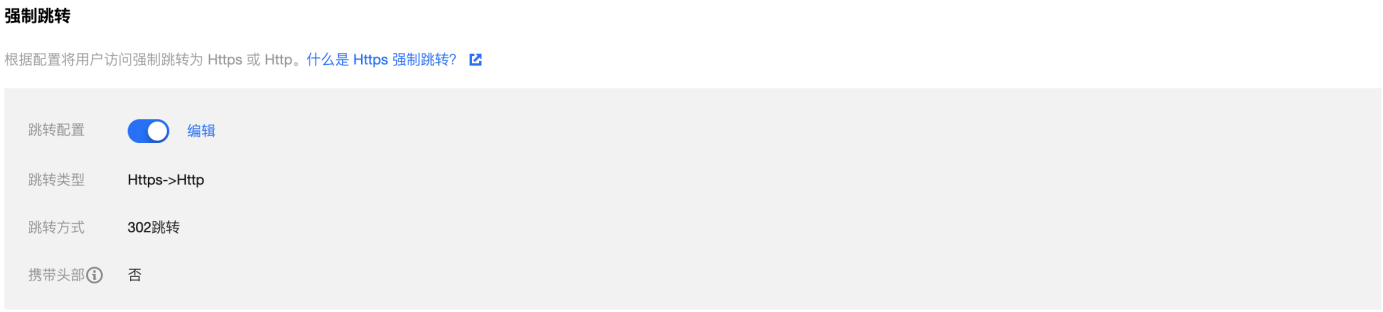
配置说明

登录 CDN 控制台，在菜单栏里选择【域名管理】，单击域名右侧【管理】，即可在【Https 配置】中可看到【强制跳转】配置开关，默认情况下为关闭状态，默认不进行任何跳转：



单击开启，可配置跳转类型、跳转方式及是否携带头部：

单击确认后，即可直接发布配置至现网：



HTTP2.0 配置

最近更新时间：2022-02-11 14:56:59

配置场景

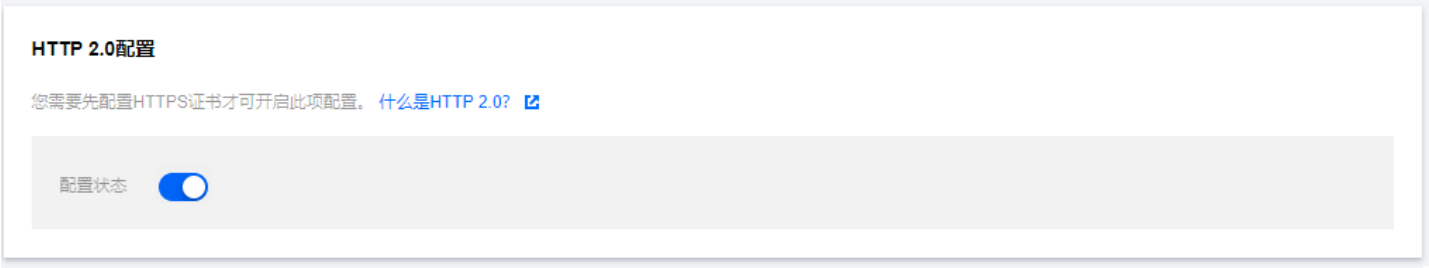
HTTP2.0 作为最新的 HTTP 协议，大幅提升了 Web 性能，进一步减少了网络延迟。已配置证书启用 HTTPS 加速的域名，可自助开启 HTTP2.0 协议支持。

> ⚠ 注意：
> 目前仅支持 HTTP2.0 访问，暂不支持 HTTP2.0 协议回源。

配置指南

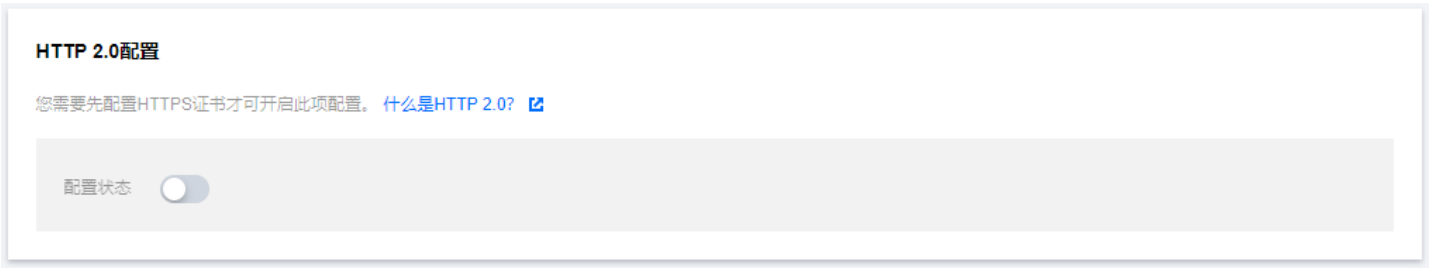
查看配置

登录 CDN 控制台，在菜单栏里选择【域名管理】，单击域名右侧【管理】，即可进入域名配置页面【Https 配置】中，可看到【HTTP2.0 配置】：



修改配置

通过单击开关，可对 HTTP2.0 配置进行开启或关闭操作，删除证书配置后，HTTP2.0 配置会同步失效：



> ⚠ 注意：
> 若域名的服务区域为全球，则配置的 HTTP2.0 会全球生效，暂不支持境内、境外分别配置。

OCSP 装订配置

最近更新时间：2021-11-05 10:20:32

配置场景

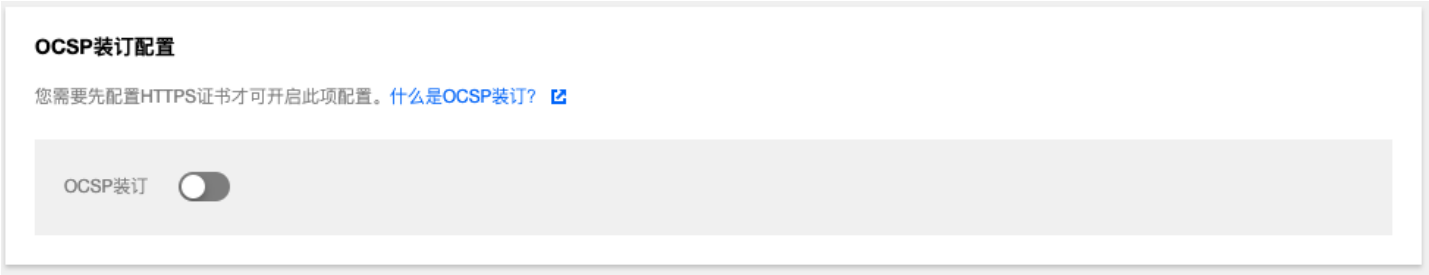
启用 OCSP 装订（TLS 证书状态查询扩展）后， 服务器在 TLS 握手时会发送事先缓存的在线证书状态协议（OCSP）响应，供用户验证，无需用户再向数字证书认证机构（CA）发送查询请求。OCSP 装订极大地提高了 TLS 握手效率，节省了用户验证时间。

腾讯云 CDN 支持自助开启或关闭 OCSP 装订配置。

配置指南

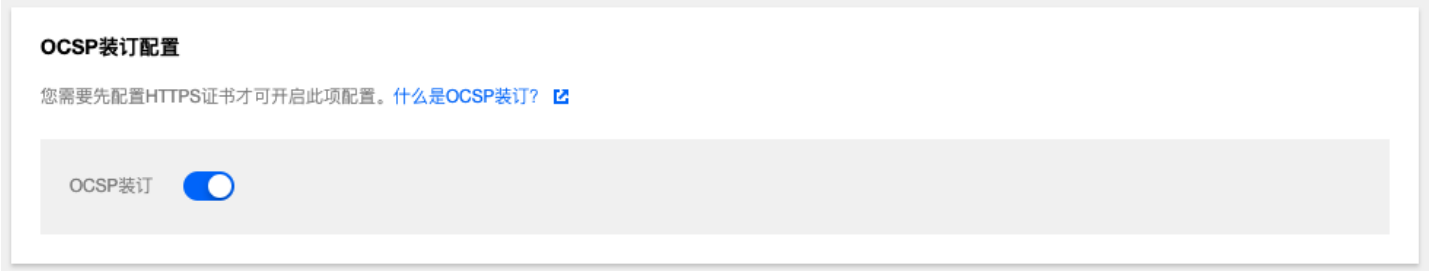
查看配置

登录 CDN 控制台，在菜单栏里选择【域名管理】，单击域名右侧【管理】，即可进入域名配置页面【Https 配置】中，可看到【OCSP 装订配置】，默认情况下为关闭状态：



修改配置

配置了 HTTPS 加速的域名，可直接通过单击开关，对 OCSP 装订配置进行开启或关闭操作，删除证书配置后，OCSP 装订配置会同步失效：



> ⚠ 注意：
> 若域名的服务区域为全球，则配置的 OCSP 装订会全球生效，暂不支持境内、境外分别配置。

HSTS 配置

最近更新时间：2022-04-15 15:45:11

配置场景

HSTS 即 HTTP Strict Transport Security，是国际互联网工程组织 IETE 推行的 Web 安全协议，通过强制客户端（浏览器等）使用 HTTPS 与服务器创建链接，帮助网站进行全局加密。

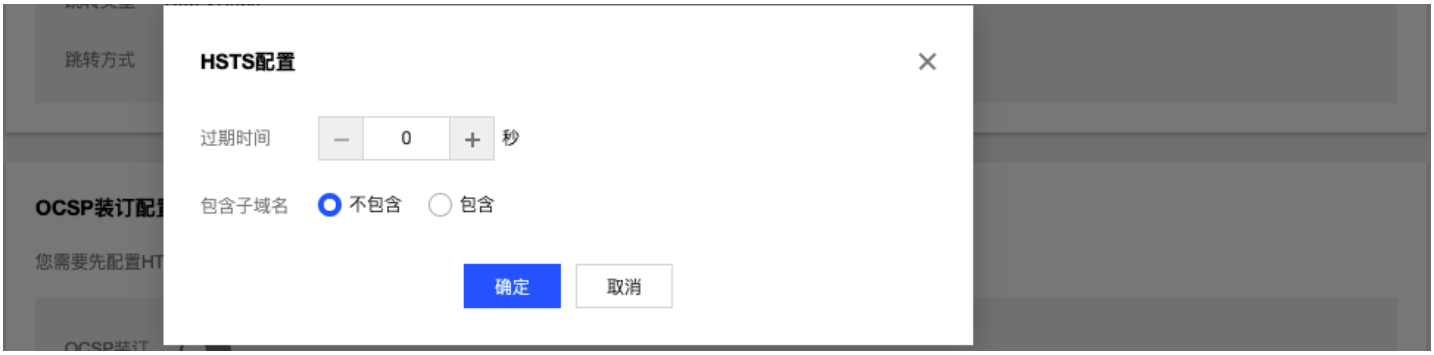
配置约束

- expireTime 约束为0 – 365天，配置时单位为秒。
- 可通过勾选是否包含子域名，来控制 includeSubDomain 参数。
- 开启 HSTS 配置需要先完成 HTTPS 加速配置。
- 开启 HSTS 后，建议您同步开启 强制跳转 HTTP->HTTPS 配置，否则当请求为 HTTP 时，浏览器将不会进行 HSTS 缓存。

配置指南

登录 CDN 控制台，在菜单栏里选择【域名管理】，单击域名右侧【管理】，即可进入域名配置页面，【Https 配置】中可看到 HSTS 配置模块，默认情况下为关闭状态：

单击开启，可进行相关配置：

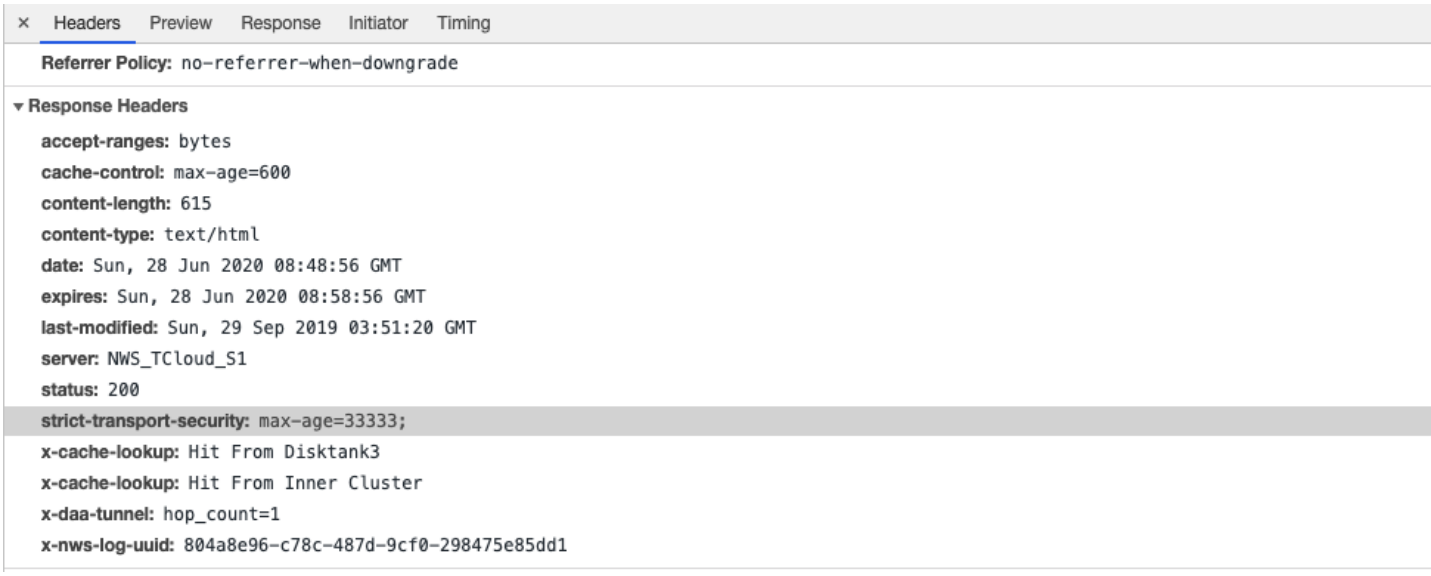


单击【确定】后，根据所配置的内容决定响应头值，可单击【编辑】进行修改：

配置示例

假设域名 cloud.tencent.com 的 HSTS 配置如下：

访问时其 Response Header 为：



TLS 版本配置

最近更新时间：2022-05-11 10:57:36

背景信息

传输层安全性协议（TLS：Transport Layer Security），目的是为了保证两个应用程序在通信过程中数据的安全性和保密性，目前有四个版本的 TLS 协议：TLS1.0/1.1/1.2/1.3，版本越低兼容性越好，但是安全性越差；版本越高安全性越强，但是兼容性会弱一些。

TLS 协议版本	支持的主流浏览器
TLS 1.0	IE6+
	Chrome 1+
	Firefox 2+
TLS 1.1	IE 11+
	Chrome 22+
	Firefox 24+
	ME 12+
	Safri 7+
	Opera 12.1+
TLS 1.2	IE 11+
	Chrome 30+
	ME 12+
	Firefox 27+
	Safri 7+
	Opera 16+
TLS 1.3	Chrome 70+
	Firefox 63+
	ME 79+

版权所有：腾讯云计算（北京）有限责任公司

TLS 协议版本	支持的主流浏览器
	Safri 14+
	Opera 57+

功能介绍

腾讯云 CDN 默认开启 TLS 1.0/1.1/1.2 ，关闭 TLS 1.3，您可按需关闭/开启指定 TLS 版本。

> ⚠ 注意：
>
> - 配置前需确保已成功配置 HTTPS 证书。
> - TLS 版本配置暂不支持中国境外。若域名的加速区域为全球，则配置变更后仅生效中国境内。
> - 部分平台正在升级中，暂未开放此配置功能。

配置指南

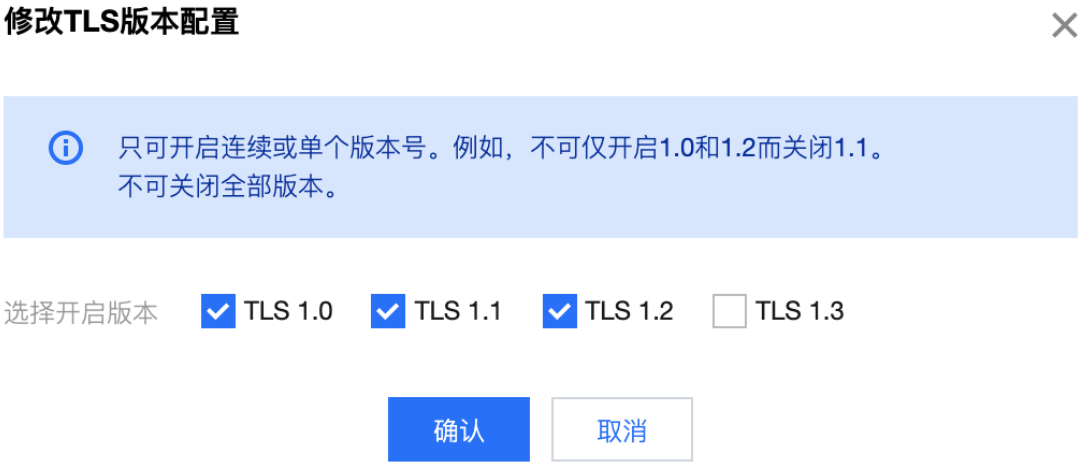
查看配置

登录 CDN 控制台，在左侧菜单栏选择【域名管理】，单击域名操作列的【管理】，进入域名配置页面，切换 Tab 至【HTTPS 配置】，即可找到【TLS 版本配置】。

默认情况下，TLS 1.0/1.1/1.2为开启状态，TLS 1.3为关闭状态：

修改配置

您可按需关闭/开启指定 TLS 版本，单击【修改配置】：



配置约束

- 只可开启连续或单个版本号。例如，不可仅开启1.0和1.2而关闭1.1。
- 不可关闭全部版本。

QUIC

最近更新时间：2022-04-11 15:29:49

功能介绍

QUIC (Quick UDP Internet Connections) 是一个通用的网络协议，能够保障网络安全性，同时减少传输和连接时的延时，避免网络拥塞。您可开启 QUIC 协议，保障客户端访问 CDN 节点时数据传输的安全性，提升访问效率。

当前默认支持 h3-29, h3-Q050, h3-Q046,h3-Q043,Q050,Q046, Q043 版本。

操作指引

开启 QUIC

登录 CDN 控制台 成功添加域名后，可进入域名管理，切换 Tab 至 **HTTPS 配置**，即可找到 **QUIC** 配置：默认为关闭状态，您可自助开启。

注：开启前请先配置 HTTPS 证书。

> ⚠ 注意：
>
> - 业务类型切换涉及资源平台调度，接入 QUIC 平台后，建议您不要再切换域名的业务类型。
> - 当前不支持 QUIC 回源。
> - 部分平台不支持 QUIC，正在升级，敬请期待。

配置约束：

流媒体点播加速业务类型的域名暂不支持 QUIC。

关闭 QUIC

进入控制台域名管理 > HTTPS 配置 > QUIC，即可关闭 QUIC 功能。

计费规则

QUIC 访问属于增值服务，按 QUIC 请求数次数计费，按量后付费，详情见 计费说明 。

HTTPS 相关常见问题

最近更新时间：2022-06-27 10:45:57

什么是 HTTPS?

HTTPS，是指超文本传输安全协议（Hypertext Transfer Protocol Secure），是一种在 HTTP 协议基础上进行传输加密的安全协议，能够有效保障数据传输安全。配置 HTTPS 时，需要您提供域名对应的证书，将其部署在全网 CDN 节点，实现全网数据加密传输功能。

CDN 是否支持 HTTPS 配置?

腾讯云 CDN 目前已经全面支持 HTTPS 配置。您可以上传自有证书进行部署，或前往 证书管理控制台 申请由亚洲诚信免费提供的第三方证书。

如何配置 HTTPS 证书?

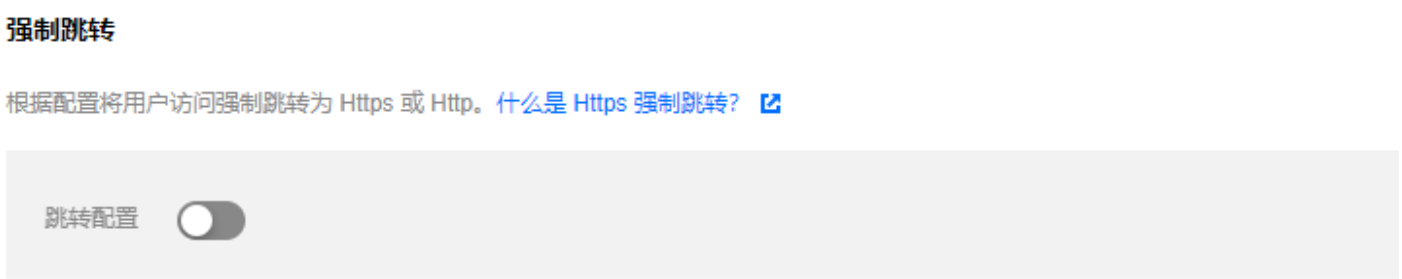
您可以在 CDN 控制台 中配置 HTTPS 证书，详情请参见 HTTPS 配置。

源站的 HTTPS 证书更新了，CDN 上需要同步更新吗?

不需要。源站的 HTTPS 证书更新后不会影响 CDN 上的 HTTPS 证书，当您在 CDN 上配置的 HTTPS 证书将要到期或者已经到期时，您才需要在 CDN 上更新 HTTPS 证书。

CDN 有没有方法让用户控制只允许 HTTPS 访问，禁止 HTTP 访问?

使用 强制跳转功能。HTTPS 证书配置成功后，可以开启 Http->Https 功能，开启后，即使用户发起 HTTP 请求，也会强制跳转为 HTTPS 进行访问。



配置了 CDN，HTTPS 无法访问?

要使用 HTTPS 访问，操作如下：

1. 登录 CDN 控制台，单击左侧导航栏的【域名管理】进入域名管理页面。单击域名右侧【管理】按钮，进入管理页面。

2. 单击【Https 配置】，找到 HTTPS 配置模块。单击【前往配置】，跳转至证书管理页面配置证书。配置流程请参阅 证书配置。

证书配置成功后即可开启 HTTPS 访问。

CDN 支持哪些 TLS 版本

您好，腾讯云 CDN 默认开启TLS 1.0/1.1/1.2 ，关闭 TLS 1.3，您可按需关闭/开启指定 TLS 版本。

注意：

- 配置前需确保已成功配置 HTTPS 证书。
- TLS 版本配置暂不支持中国境外。若域名的加速区域为全球，则配置变更后仅生效中国境内。
- 部分平台正在升级中，暂未开放此配置功能。
- 只可开启连续或单个版本号。例如，不可仅开启1.0和1.2而关闭1.1。
- 不可关闭全部版本。如需配置可参考文档 配置指南。

CDN 如何开启 QUIC?

CDN 支持 QUIC，如何开启请参考 QUIC。

CDN 是否支持证书自动续签?

自定义上传证书和您于 SSL 控制台申请的免费证书暂不支持自动续签新的证书，若您于 SSL 控制台购买了多年期证书可实现自动签发第二张证书，详情见 多年期证书方案说明。

CDN 支持 HTTP 2.0吗?

客户端到 CDN 节点已支持 HTTP 2.0，开启 HTTP 2.0 前请先配置 HTTPS 证书，CDN 节点回源到源站不支持 HTTP2.0。

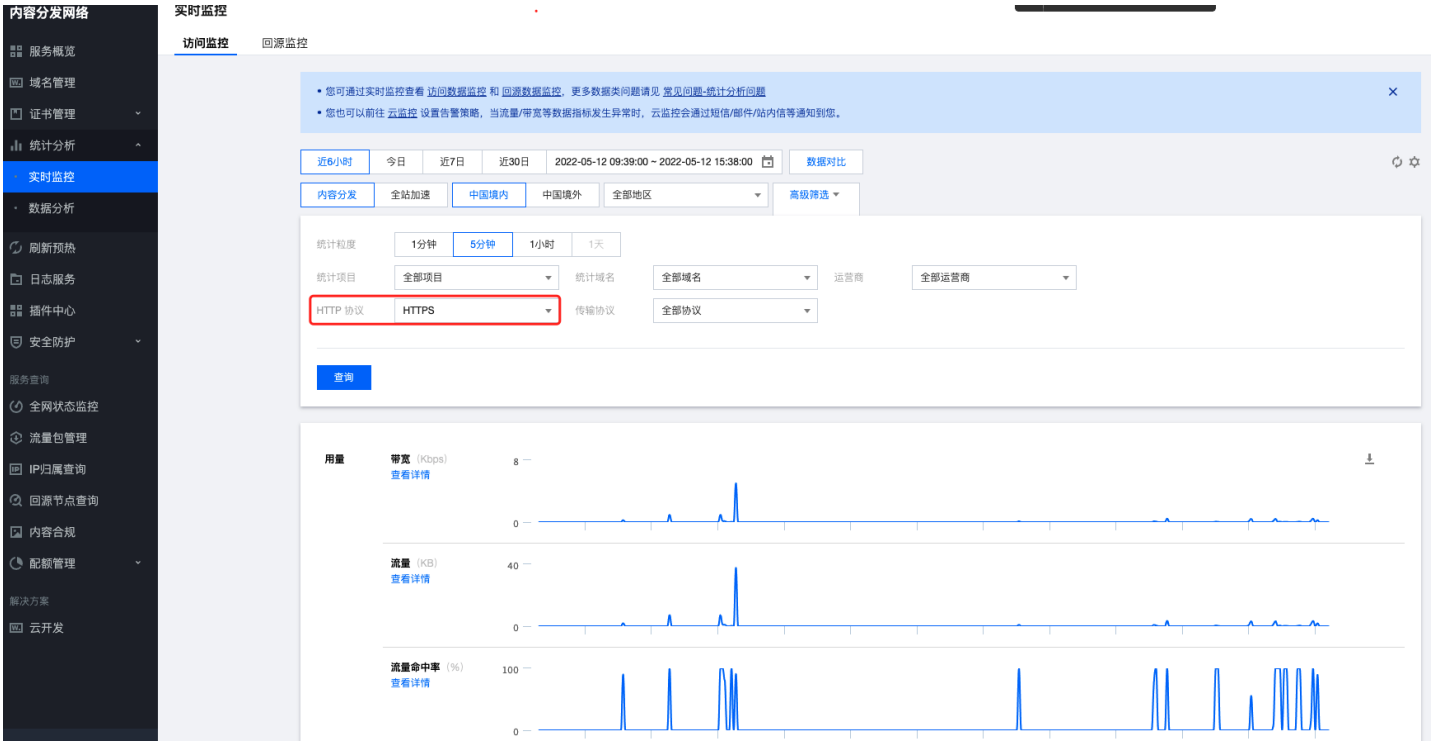
如何批量配置 CDN 证书?

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。

请参考证书管理中的 批量配置证书 。

如何查看 HTTPS 请求数的使用情况

您可在控制台通过**实时监控 > 访问监控**，在 HTTP 协议选择 HTTPS 单击**查询**即可获取到 HTTPS 使用数据。



CDN 上的 HTTPS 证书和源站服务器的证书冲突了怎么办?

CDN 上的 HTTPS 证书和源站服务器上的 HTTPS 证书两者是独立存在的，不会影响。

配置HTTPS后还可以使用HTTP访问吗?

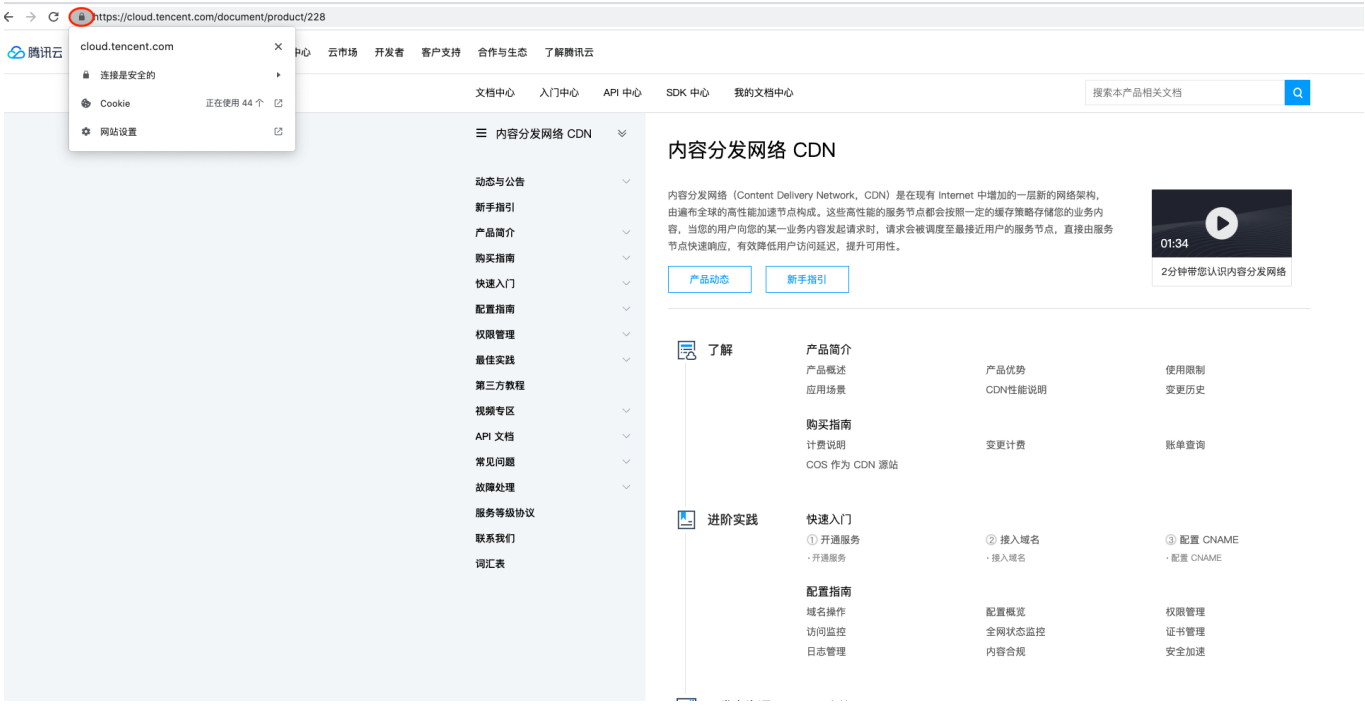
配置 HTTPS 后，可同时支持 HTTP 访问和 HTTPS 访问。

如何验证 CDN 证书是否部署成功?

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 HTTPS 证书 生效情况：

1. 打开浏览器（以 Chrome 浏览器为例），在浏览器地址栏中以 HTTPS格式 输入证书已绑定的域名地址。
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 HTTPS证书 已生效。如下图所示：



网站提示证书风险，如何处理?

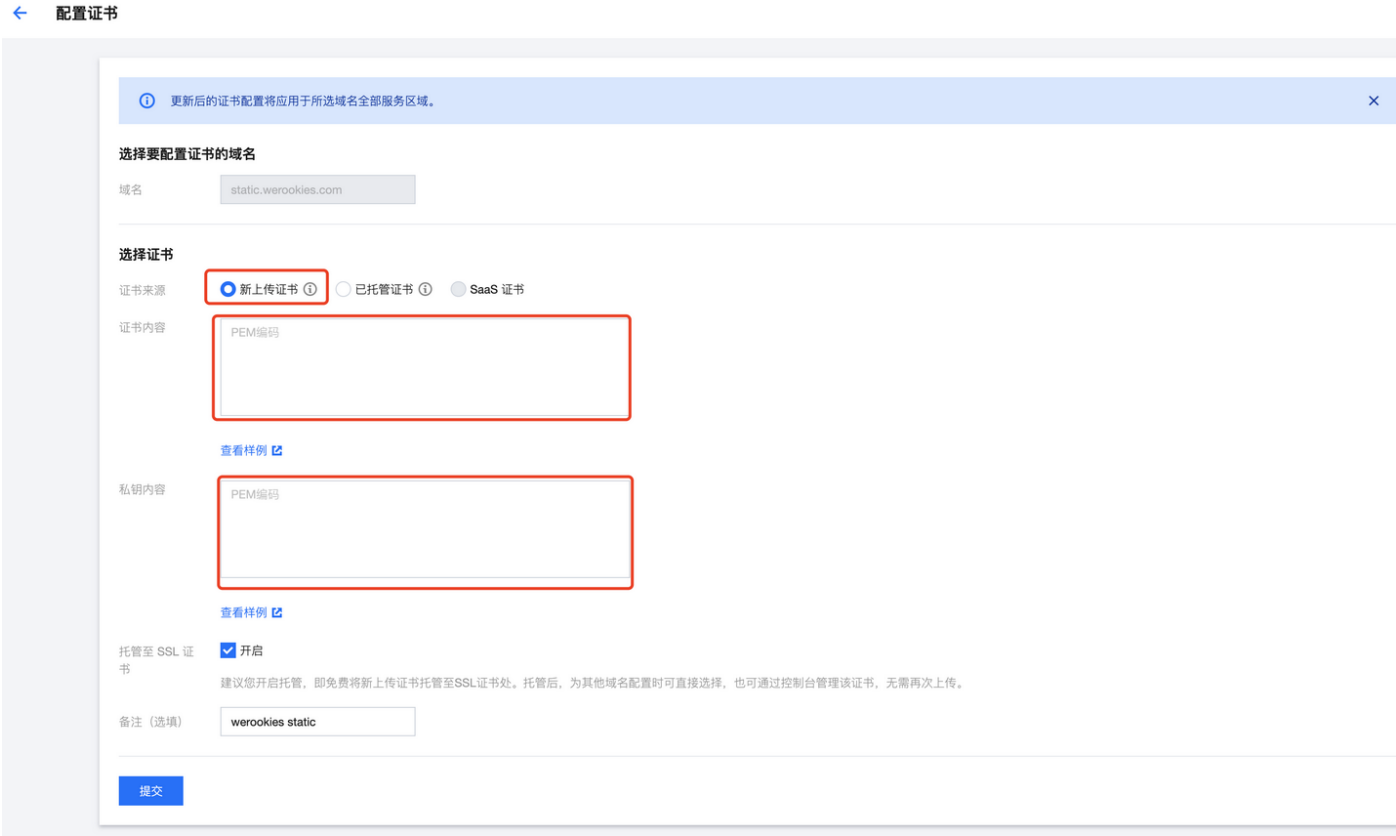
如果您在 CDN 节点已配置了 HTTPS 证书，但是验证却未生效，可能的原因有：

- 证书已过期。
  证书存在有效期，当证书出现过期后会出现证书失效进而导致网站 HTTPS 访问出现异常的情况。
  处理方案：您需要前往控制台更换证书，自定义上传证书和您于 SSL 控制台申请的免费证书暂不支持自动续签新的证书，若您于SSL控制台购买了多年期证书可实现自动签发第二张证书，详情见多年期证书方案说明
- 应用了自签名 HTTPS 证书。
  非 CA 机构签发，由自己生成的证书称为自签名证书，此类证书不受各大浏览器信任，容易被伪造，存在安全风险。
  处理方案：建议您在腾讯云 SSL 控制台申请由 CA 机构颁发的证书。
- 系统时间不正确。
  系统时间不正确会导致证书过期或校验不成功 。
  处理方案：将系统时间配置正确
- 网页内有 HTTP 链接资源，即网页使用了 HTTP 协议的链接。
  如：网页使用了 HTTP 的图片链接
  处理方案：将 HTTP 协议链接调整 HTTPS 协议链接
- 过低的 TLS 版本
  低版本的 TLS 存在许多安全漏洞，这些漏洞存在被攻击的去安全风险。
  处理方案：腾讯云 CDN 默认开启TLS 1.0/1.1/1.2 ，关闭 TLS 1.3，TLSv1.2 和 TLSv1.3 是目前公认的安全性更高的协议，您可根据您的需要关闭 TLS 1.0/1.1，开启 TLSv1.2 和 TLSv1.3。

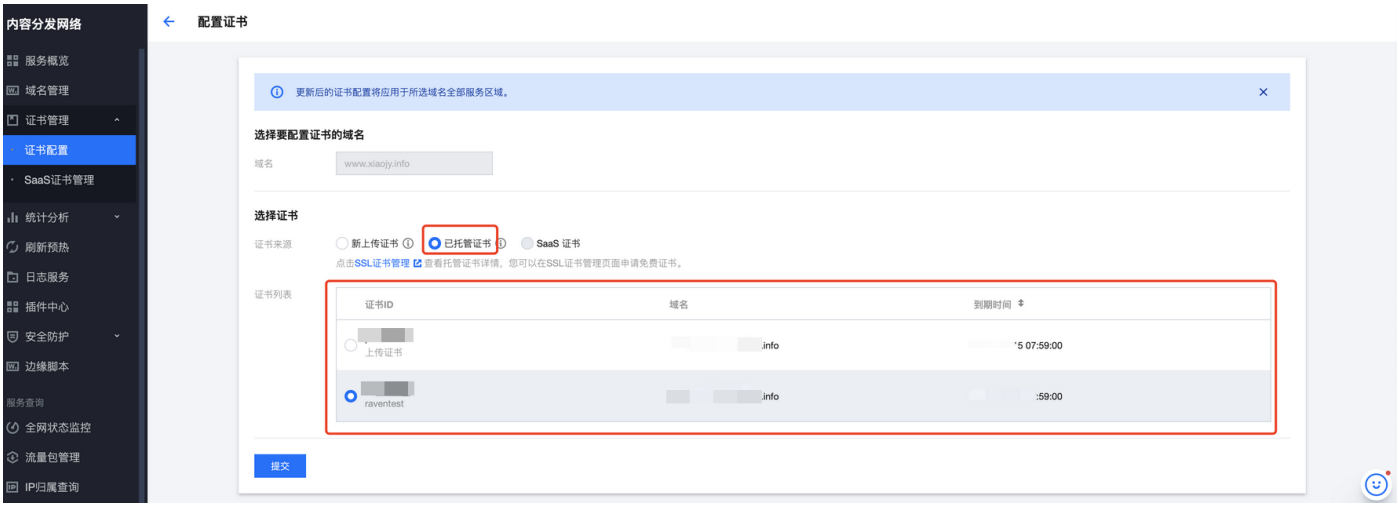
- 使用了弱密码加密套件。
  弱密码套件存在较多安全漏洞，这些漏洞存在被攻击的安全风险。
  处理方案：安全加密和身份验证建议您使用128位的 AEC、GCM 配置；密钥交换机制建议使用 ECDHE_RSA。

证书过期后怎么办?

1. 如果您的证书属于自有证书，您可通过单击**编辑**更新证书和私钥内容，完成更新后，单击**提交**。



2. 如果您的证书属于已托管证书，您可前往 SSL 控制台更新证书，并更新域名和证书的关联关系。



高级配置
用量封顶配置

最近更新时间：2022-06-29 16:05:30

配置场景

当您的预付费资源包（流量包）用尽时，会计入腾讯云 CDN 按量后付费。若您担心由于恶意用户盗刷产生大量带宽或者流量，导致产生高额账单，可通过用量封顶功能进行用量控制。

当统计周期内产生的带宽或者流量超出配置的告警阈值时，CDN 会推送消息通知您；超出配置的访问阈值，您可选择关闭 CDN 服务，或请求直接返回源站，避免产生更多 CDN 服务费用。

> ⚠ 注意：
> 用量封顶配置生效存在一定延迟（10分钟左右），期间产生的消耗会正常计费。更多说明请参见 攻击风险预防方案。

配置指南

查看配置

登录 CDN 控制台，在菜单栏里选择**域名管理**，单击域名右侧**管理**，即可进入域名配置页面，在**高级配置**中可看到用量封顶配置，默认情况下配置为关闭状态：

详细配置

1. 开启配置

单击开启配置开关，进行具体配置：

- 统计类型：
  - 瞬时用量：对每5分钟内的流量/带宽进行用量统计。
  - 累计用量：相比瞬时用量，有更长的统计周期，支持对按小时/按自然天的流量进行用量统计。

> ⚠ 注意：
> 加速类型为 ECDN 动态加速和 ECDN 动静加速的域名不支持「累计用量」封顶配置。

- 统计周期：支持分钟（每5分钟）、小时（每1小时）、自然天（当天24点前）的统计周期。

> ⚠ 注意：
>
> - 统计周期的起始时间为配置时间往前推5分钟粒度整点时间：
> 如：在09:05:01 – 09:09:59期间配置的规则，则09:05:00为统计周期起始时间点。
> - 若统计周期选择“每1小时”，则：（1）对于设置后的首个小时的数据统计周期，会不足1个小时的统计时长；（2）进入次个数据统计周期，按自然小时进行用量统计。
> 如：2022-01-13 9:23:10配置规则，首个数据统计周期为 9:20:00 – 9:59:59；次个统计周期为 10:00:00 – 10:59:59。
> - 若统计周期选择“当天24点前”，则累计周期为 2022-01-13 9:20:00 – 2022-01-13 23:59:59。

- 封顶配置：瞬时用量支持流量/带宽封顶；累计用量仅支持流量封顶。
  - 流量封顶：即统计域名的流量消耗。流量阈值，为用户访问该域名的流量上限值。
  - 带宽封顶：即统计域名的带宽消耗。带宽阈值，为用户访问该域名的带宽上限值。
- 解封时间：支持定时解封/永不解封。
  - 定时解封：定时解封周期支持 60分钟、12小时、24小时、3天。
    例如，设置 ex.com 域名超出阈值后访问返回404（关闭 CDN 服务），自动解封时间为 60分钟。当域名超出设定的累计用量封顶的阈值后将会关闭 CDN 服务，下线加速域名。60分钟后，将自动解封域名，开启域名加速。
  - 永不解封：如您担心域名将可能遭受大流量/带宽攻击，可设置永不解封。若设置超出阈值后访问返回404（关闭 CDN 服务）。当域名超出设定的累计用量封顶的阈值后，域名将会下线，您需自行前往控制台开启域名加速。
- 超出阈值：支持回源或关闭 CDN 服务。
  - 访问回源：超出阈值的请求直接返回源站。
  - 访问返回404：超出阈值，会直接关闭该域名的 CDN 服务。可前往域名管理页面重新上线域名，恢复 CDN 服务。
    注：对源站类型为 COS 源/第三方对象存储，仅支持访问返回404（即关闭 CDN 服务）。
- 告警阈值：
  当访问带宽/流量阈值的比值超出配置的百分比时（仅可填写10的倍数，10% – 90%），CDN 将推送告警消息。

> ⚠ 注意：
>
> - 检测到域名带宽（流量）超出阈值后，访问回源或访问返回404配置均需要全网节点逐步下发生效，因此会有一定的生效延迟。

- 若已开启告警阈值：因扫描粒度为5min，若短时间内用量剧增或百分比设置的数值较大，可能上一次扫描还未触发百分比告警的阈值，下一次扫描直接达到了访问阈值。此场景下 CDN 会依次发送百分比告警和访问阈值告警两个通知消息。

2. 区域特殊配置

若您的加速域名服务区域为全球加速，想针对境内、境外加速区域进行不同的用量封顶配置，可单击配置下方的**添加特殊配置**进行设置：

注意：

- 区域特殊配置添加后，暂时无法直接删除，您可以通过关闭配置来禁用。
- 加速类型为 ECDN 动态加速和 ECDN 动静加速的域名不支持「区域特殊配置」。

配置示例

若加速域名 cloud.tencent.com 为全球加速域名，新增区域特殊配置（中国境外）用量封顶如下：

- 境内外配置互不影响：区域特殊配置选择“中国境外”，则初始配置会在中国境内生效。境内流量在统计周期(5分钟)内达到4G，则所有境内请求会回源，不影响境外服务；当境外流量在统计周期(当天24点前)内到达 11G 时，则所有境外请求会返回404，不影响境内服务。
- 域名切换加速区域：若全球加速域名切换为中国境内加速域名，则用量封顶境外配置会默认关闭，不可编辑。

3. 关闭配置

您可以通过用量封顶开关，一键关闭配置，开关为关闭状态时，即便下方存在已有配置，仍不会现网生效，再次开启时，会进行配置的二次确认，不会立即发布至全网生效。

HTTP 响应头配置

最近更新时间：2021-08-11 17:14:04

配置场景

当您的业务用户请求业务资源时，您可以在返回的**响应消息**中配置头部，以实现跨域访问等目的。
响应头部配置是域名维度的，因此一旦配置生效，会对域名下任意一个资源的响应消息生效。配置响应头部仅影响客户端（如浏览器）的响应行为，不会影响到 CDN 节点的缓存行为。

配置指南

查看配置

登录 CDN 控制台，在菜单栏里选择【域名管理】，单击域名右侧【管理】，即可进入域名配置页面，在【高级配置】中可看到响应头部配置，默认情况下配置为关闭状态，单击【新增规则】可配置 HTTP 响应头规则：

操作类型

操作类型	说明
设置	变更指定响应头部参数的取值为设置后的值。 若设置的头部不存在，则会增加该头部。 若存在多个重复的头部参数，则会全部变更，同时合并为一个头部。 即当配置规则为【设置 x-cdn: value1】，若请求中包含有多个 x-cdn 头部，则多个头部均会变更，合并为一个头部 x-cdn: value1。
删除	删除指定的响应头参数。

注意：

- 部分头部不支持自助设置/删除，具体清单请参见文档 注意事项。
- HTTP 响应头配置规则最多可配置10条。

- 多条规则支持调整优先级：底部优先级大于顶部。若同一头部参数配置了多条规则，则生效最底部，即优先级最高的那条。

头部参数

头部参数	说明
Access-Control-Allow-Origin	用于解决资源的跨域权限问题，域值定义了允许访问该资源的域。若来源请求 Host 在域名配置列表之内，则直接填充对应值在返回头部中。也可以设置通配符 “*”，允许被所有域请求。更多说明请见 Access-Control-Allow-Origin 匹配模式介绍。 支持输入“*” ，或多个域名 / IP / 域名与 IP 混填（必须包含 http:// 或 https://，填写示例：http://test.com,http://1.1.1.1， 逗号隔开）（注意：输入框最多可输入1000字符）。
Access-Control-Allow-Methods	用于设置跨域允许的 HTTP 请求方法，可同时设置多个方法，如下：Access-Control-Allow-Methods: POST, GET, OPTIONS。
Access-Control-Max-Age	用于指定预请求的有效时间，单位为秒。 非简单的跨域请求，在正式通信之前，需要增加一次 HTTP 查询请求，称为“预请求”，用来查明这个跨域请求是不是安全可以接受的，如下请求会被视为非简单的跨域请求： 以 GET、HEAD 或者 POST 以外的方式发起，或者使用 POST，但是请求数据类型为 application / x-www-form-urlencoded、multipart / form-data、text / plain 以外的数据类型，如 application / xml 或者 text / xml。 使用自定义请求头为：Access-Control-Max-Age:1728000，表明在1728000秒（20天）内，对该资源的跨域访问不再发送另外一条预请求。
Access-Control-Expose-Headers	用于指定哪些头部可以作为响应的一部分暴露给客户端。 默认情况下，只有6种头部可以暴露给客户端：Cache-Control、Content-Language、Content-Type、Expires、Last-Modified、Pragma。 如果想让客户端访问到其他的头部信息，可以进行如下设置，当输入多个头部时，需用 “,” 隔开，如：Access-Control-Expose-Headers: Content-Length,X-My-Header，表明客户端可以访问到 Content-Length 和 X-My-Header 这两个头部信息。

头部参数	说明
Content-Disposition	用来激活浏览器的下载，同时可以设置默认的下载的文件名。 服务端向客户端浏览器发送文件时，如果是浏览器支持的文件类型，如 TXT、JPG 等类型，会默认直接使用浏览器打开，如果需要提示用户保存，则可以通过配置 Content-Disposition 字段覆盖浏览器默认行为。常用的配置如下： Content-Disposition：attachment;filename=FileName.txt
Content-Language	用于定义页面所使用的语言代码。常用配置如下： Content-Language: zh-CN Content-Language: en-US
自定义	支持添加自定义 Header，自定义 key-value 设置。 自定义头部参数：由大小写字母、数字及 - 组成，长度支持1 - 100个字符。 自定义头部取值：长度为1 - 1000个字符，不支持中文。

Access-Control-Allow-Origin 匹配模式介绍

匹配模式	域值	说明
全匹配	*	设置为 * 时，则响应添加头部： Access-Control-Allow-Origin:*
固定匹配	http://cloud.tencent.com https://cloud.tencent.com http://www.b.com	来源https://cloud.tencent.com，命中列表，则响应添加头部： Access-Control-Allow-Origin: https://cloud.tencent.com 来源为 https://www.qq.com，未命中列表，响应无变化。
二级泛域名匹配	https://*.tencent.com	来源 https://cloud.tencent.com，命中列表，则响应添加头部： Access-Control-Allow-Origin: https://cloud.tencent.com 来源为 https://cloud.qq.com，未命中列表，响应无变化。
端口匹配	https://cloud.tencent.com:8080	来源为 https://cloud.tencent.com:8080，命中列表，则响应添加头部： Access-Control-Allow-Origin:https://cloud.tencent.com:8080 来源为 https://cloud.tencent.com，未命中列表，响应无变化。

> ⚠ 注意：
> 若存在特殊端口，则需要在列表中填写相关信息，不支持任意端口匹配，必须指定。

注意事项

此功能不支持以下头部，即以下头部不会生效：

```
Date
Expires
Content-Type
Content-Encoding
Content-Length
Transfer-Encoding
Cache-Control
If-Modified-Since
Last-Modified
Connection
Content-Range
ETag
Accept-Ranges
Age
Authentication-Info
Proxy-Authenticate
Retry-After
Set-Cookie
Vary
WWW-Authenticate
Content-Location
Content-MD5
Content-Range
Meter
Allow
Error
```

SEO 配置

最近更新时间：2021-07-21 20:45:10

配置场景

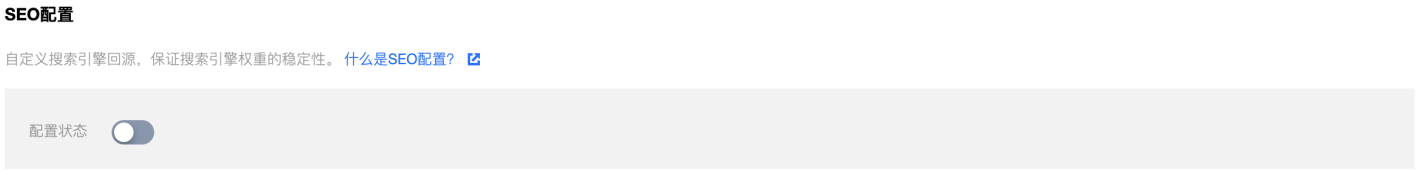
SEO 配置是解决域名接入 CDN 后，因 CDN 频繁变更 IP 而影响域名搜索结果权重问题的功能。通过识别访问 IP 是否属于搜索引擎，用户可选择直接回源访问资源，来保证搜索引擎权重的稳定性。

> ⚠ 注意：
>
> - 由于搜索引擎 IP 更新较为频繁，腾讯云 CDN 仅能确保能识别绝大多数的搜索引擎 IP。
> - SEO 配置功能只在域名的源站类型为 自有源 时可使用。开启 SEO 配置功能后，若域名有多个源站地址，则默认回源地址为添加的第一个源站地址。
> - 中国境外暂不支持。若域名的加速区域为中国境外，则不支持开启 SEO 配置。若域名的加速区域为全球，则 SEO 配置开启后仅中国境内生效。

配置指南

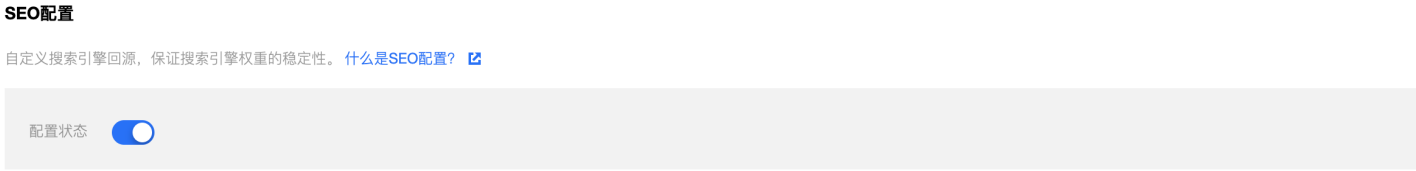
查看配置

登录 CDN 控制台，在菜单栏里选择【域名管理】，单击域名右侧【管理】，即可进入域名配置页面，在【高级配置】中可看到 SEO 配置，默认情况下为关闭状态：



修改配置

您可以通过 SEO 配置开关，自助进行服务开启或关闭操作：



智能压缩配置

最近更新时间：2021-12-09 11:10:16

配置场景

通过智能压缩配置，CDN 在返回内容时会按照设定规则对资源进行 Gzip 、 Brotli 压缩，有效减少传输内容大小，节省开销。

> ⚠ 注意：
>
> - 若域名的加速区域为全球，则智能压缩配置开启后会全球生效，暂不支持境内、境外配置不一致。
> - 中国境外加速区域暂不支持配置文件 Content-Type 类型 和 Brotli 压缩方式

配置指南

查看配置

登录 CDN 控制台，在菜单栏里选择**域名管理**，单击域名右侧**管理**，即可进入域名配置页面，在**高级配置**中可看到智能压缩配置，默认为开启状态：

- 接入加速域名后，CDN 会默认为后缀 .js、.html、.css、.xml、.json、.shtml、.htm，大小为 256Byte - 2MB 范围内的资源开启 Gzip 压缩。

修改配置

可单击操作列的**修改**，对压缩规则进行修改：

配置约束

- 类型默认为文件后缀，可添加全部文件，Content-Type 类型。
- 文件后缀类型的内容总长度不可超过200个字符。
- 文件 Content-Type 类型的内容默认为 text/html, text/xml, text/plain, text/css, text/javascript, application/json, application/javascript, application/x-javascript, application/rss+xml, application/xmltext, image/svg+xml, image/tiff，您可按需自行配置：不可超过100组，不同组内容用 ";" 分隔，每组内容不可超过50个字符。
- 部分平台正在升级中，暂未开放文件 Content-Type 类型 和 Brotli 压缩方式。

> 说明：
>
> - 关闭状态下仍可修改下方配置，但不会发布至现网，仅当开启此开关时，进行现网配置下发。
> - 同时选择 Gzip 和 Brotli 压缩时，会根据请求压缩头，来返回对应的压缩文件。
> - 仅开启 Brotli 压缩时，若请求压缩头不支持 Brotli 压缩，则压缩不会生效，将返回原始资源。

自定义错误页面

最近更新时间：2021-11-05 10:04:28

功能介绍

自定义错误页面配置功能支持按需将返回指定错误状态码的请求重定向至指定目标地址。

当前支持以下状态码：

- 4XX：400,403,404,405,414,416,451
- 5XX：500,501,502,503,504

> ⚠ 注意：
>
> - 部分平台正在升级中，暂不支持此配置功能。
> - 此功能为回源错误状态码的重定向，不支持 UA 黑白名单等访问控制功能产生的状态码重定向。

配置指南

查看配置

登录 CDN 控制台，在左侧菜单栏选择【域名管理】，单击域名操作列的【管理】，进入域名配置页面，切换 Tab 至【高级配置】，即可找到【自定义错误页面配置】。

默认情况下，自定义错误页面配置为关闭状态：

新增规则

您可按需添加自定义错误页面规则，单击【新增规则】：

配置约束

- 一个状态码仅支持添加一条规则，不可重复添加。
- 重定向：可选301或302。
- 目标地址：必须包含 http://或 https://。
- 不支持提交中文内容，输入框中的内容长度不可超过1024个字符。

POST 请求大小配置

最近更新时间：2021-07-05 19:45:09

功能说明

腾讯云 CDN 的 POST 请求大小上限，即请求 body 大小的上限，默认为 32MB。您可根据业务实际情况调整此处的上限。

配置指南

查看配置

登录 CDN 控制台，在左侧菜单栏选择【域名管理】，单击域名操作列的【管理】，进入域名配置页面，切换 Tab 至【高级配置】，即可找到【POST 请求大小配置】，最大可调整为 200MB。

> **注意：**
> 部分平台无 POST 请求大小的限制，域名暂不支持此功能。

WebSocket 配置

最近更新时间：2022-06-07 17:51:36

如果您的业务有弹幕聊天、互动直播、社交订阅、协同会话、多玩家游戏、行情播报、体育实况更新、在线教育和物联网等场景，您可在 ECDN 全站加速配置WebSocket。

功能介绍

WebSocket 协议是基于 TCP 的一种持久化协议，它实现了客户端与服务器全双工（full-duplex）通信，允许服务器主动发送信息给客户端。在 Websocket 协议之前，实现客户端和服务端双工通讯的 Web App 需要通过不断发送 HTTP 请求呼叫来进行询问，这导致了服务成本增加和效率低下的问题。WebSocket 具有全双工通信的优势，客户端和服务器只需要完成一次握手，两者之间就可创建持久性的连接并能实现双向数据的传输，能更好地节省服务器资源和带宽，并且能够更实时地进行通讯。

注意事项

1. WebSocket 是 ECDN 全站加速特性功能，配置WebSocket前请先选择 ECDN 全站加速域名。
2. WebSocket 属于动态资源，无需配置任何缓存规则，同时需要源站支持 WebSocket。
3. WebSocket 超时时间配置最大可以设置300s，如果已配置时间内没有消息传递，将默认关闭连接。

配置说明

域名管理内配置

1. 登录 CDN 控制台；
2. 单击左侧菜单内的 **域名管理**，进入域名管理列表；
3. 选择需要配置的 ECDN 全站加速域名，单击**管理进入**域名配置页面；
4. 单击**高级配置**，找到 WebSocket 超时时间配置，即可启用 WebSocket；

5. 启用 WebSocket 后，您可以在 0- 300s 内自定义编辑超时时间。

推荐配置

WebSocket 是客户端和源站间建立的会话连接，建议根据您的心跳包机制配置 WebSocke t超时时间，若您的 WebSocket 没有心跳包机制则您的 WebSocket 超时时间建议配置成60s

配置约束

WebSocket 超时时间配置仅支持ECDN全站加速域名，若您域名不属于 ECDN 全站加速域名（加速类型为 ECDN 动静加速和 ECDN 动态加速），您的域名将无法配置 WebSocket。

配置示例

示例一

若 WebSocket 为关闭状态，域名 cloud.tencent.com 的 WebSocket 超时时间配置项如下：

cloud.tencent.com 不支持 WebSocket协议，如有 WebSocket 请求，连接容易断开或失败。

示例二

若 WebSocket 为开启状态，并且超时时间配置100s，域名 cloud.tencent.com 的 WebSocket 超时时间配置项如下：

cloud.tencent.com 支持 WebSocket 协议，协议的会话保持时间遵循 WebSocket 超时时间配置的100s做会话保持，超过100s 无通讯请求即断开连接。

关联的常见问题

CDN 支持 WebSocket 吗?

图片优化

最近更新时间：2021-10-18 11:55:29

配置场景

在使用腾讯云 CDN 进行海量图片分发时，可通过开启图片优化，对符合要求的图片请求，自动进行 webp、guetzli、tpg 格式图片压缩，可有效降低因图片产生的下行流量，降低成本。

配置指南

登录 CDN 控制台，在菜单栏里选择**域名管理**，单击域名右侧**管理**，即可进入域名配置页面，源站为 COS 对象存储时，可看到**图片优化**菜单栏：

- 源站为 COS 对象存储且版本为 COS V5 时，才可进行相关配置。
- 若您尚未开通数据万象服务，可在此页面一键开通数据万象服务，而后进行图片处理的相关配置。
- 若您已开通数据万象服务，可直接进行配置开启。

> 说明：
> 数据万象 是腾讯云提供的安全、稳定、高效的云端数据处理服务，Webp、Guetzli、TPG 等图像处理会产生一定的数据万象费用，单击 查看计费说明。

Webp 自适应

开启了 Webp 自适应图片压缩功能后，满足以下条件的请求，将直接返回 Webp 处理后的图片，若不满足下述条件，仍返回原图：

- HTTP 请求头中 accept 头部包含 image/webp。
- 图片后缀为 jpg、jpeg、bmp、gif、png。

> 注意：
> - Webp 图片压缩产生的费用归属于数据万象-基础图片处理费用。
> - 处理图片的原图大小不能超过20MB、宽高不超过30000像素且总像素不超过1亿像素，处理结果图宽高设置不超过9999像素。
> - 针对动图，原图宽 * 高 * 帧数不超过1亿像素，GIF 帧数限300帧。

Guetzli 自适应

Guetzli 图片压缩是数据万象推出的视觉无损压缩服务，能够对 JPG 图像进行高比例压缩，为使用者节省下载流量，并加快用户下载速度，提升体验。它利用人眼对于部分色域及图片细节的不敏感性，在不影响视觉效果的前提下有选择地丢弃细节信息，使得在相同视觉效果下比原图节省约35% - 50%的图片流量。

开启了 Guetzli 自适应图片压缩功能后，满足以下条件的请求，将直接返回 Guetzli 处理后的图片：

- HTTP 请求头中 accept 头部包含 image/guetzli。
- 图片后缀为 jpg、jpeg。

> ⚠ 注意：
>
> - Guetzli 图片压缩产生的费用归属于数据万象-Guetzli 压缩费用。
> - 开启 Guetzli 后，首次访问图片会返回普通 JPG 原图，同时启动异步 Guetzli 处理，处理完成后再次请求该图片会得到压缩后的结果图。
> - 当前 Guetzli 图片压缩服务仅对质量 q>70、像素小于400万像素的 JPG 图片做处理。

TPG 自适应

TPG 压缩是腾讯云数据万象提供的高级图片压缩功能。通过该功能可将指定格式图片转码为 TPG 格式，大幅减小图片大小，从而显著降低图片流量，提升页面加载速度。

开启了 TPG 自适应图片压缩功能后，满足以下条件的请求，将直接返回 TPG 处理后的图片：

- HTTP 请求头中 accept 头部包含 image/tpg。
- 图片后缀为 jpg、jpeg、bmp、gif、png、webp。

> ⚠ 注意：
>
> TPG 图片压缩产生的费用归属于数据万象-高级图片压缩费用。

注意事项

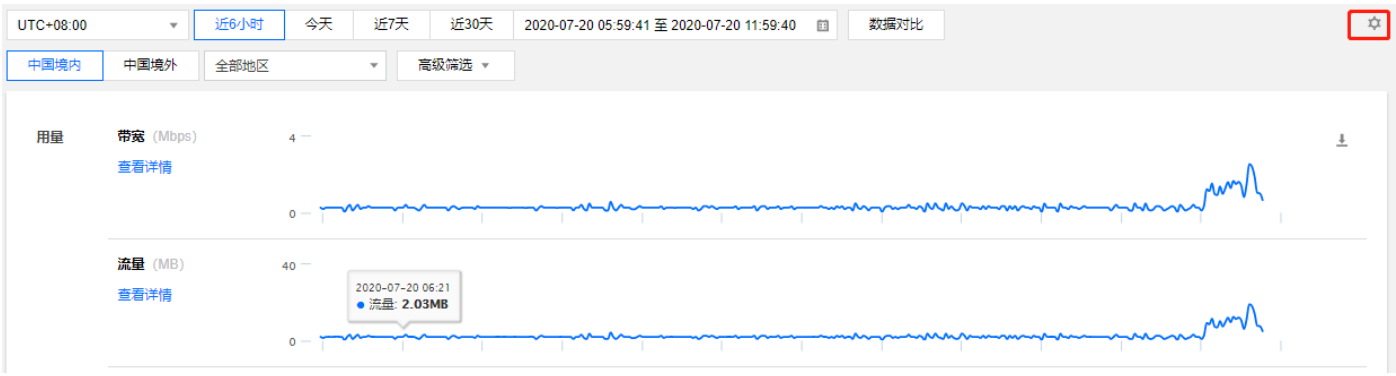
开启自适应图片压缩功能后，访问 URL 的缓存键会发生变化，但**缓存配置 - 缓存键规则配置**处缓存键规则的优先级更高。
例如，若 jpg 类型文件开启了图片优化，则请求 URL `http://www.test.com/a.jpg?colour=red` 会变更为 `http://www.test.com/a.jpgxxxxxx?colour=red`，若**缓存配置 - 缓存键规则配置**处已配置：全部文件 - 忽略全部参数，优先级更高，则忽略全部参数会生效，请求 URL 最终变更为 `http://www.test.com/a.jpgxxxxxx` 。

统计分析
实时监控
面板配置

最近更新时间：2022-04-15 15:53:27

新版实时监控页面支持按需调整指标面板，方便您查看所关注指标的监控曲线。

1. 登录 CDN 控制台，在左侧目录中，选择【统计分析】>【实时监控】，进入管理页面。
2. 单击右侧配置图标，进入配置页面。



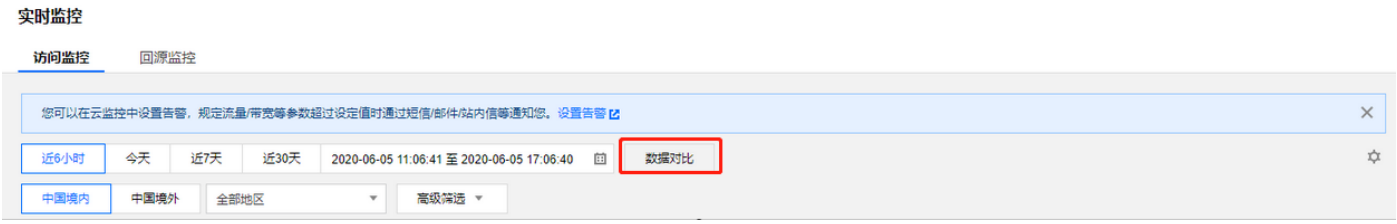
3. 按需选择在总览页展示的数据指标：被勾选中的指标，将在概览页直接展示，取消勾选，将默认不再展示。
   实时监控【访问监控】和【回源监控】总览页面，均可分别配置自定义面板。

数据对比

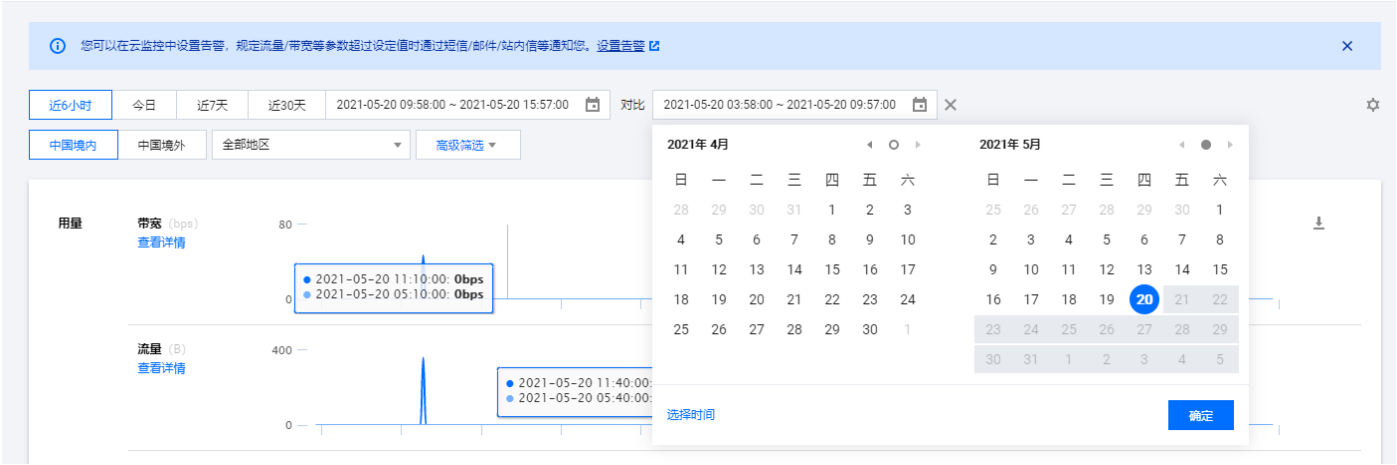
最近更新时间：2021-05-20 16:40:09

新版实时监控页面的各子页面，均支持数据曲线对比功能。

1. 登录 CDN 控制台，在左侧目录中，选择【统计分析】>【实时监控】，进入管理页面。
2. 查询指定时间区间监控曲线后，单击【数据对比】，指定时间周期，即可进行数据对比展示。



为了方便您的使用，指定开始时间后，系统将自动往后补齐结束时间；指定结束时间，系统将自动向前补齐开始时间，保证对比的时间周期一致。



访问监控

最近更新时间：2021-05-19 10:33:37

指标说明

概览页指标说明

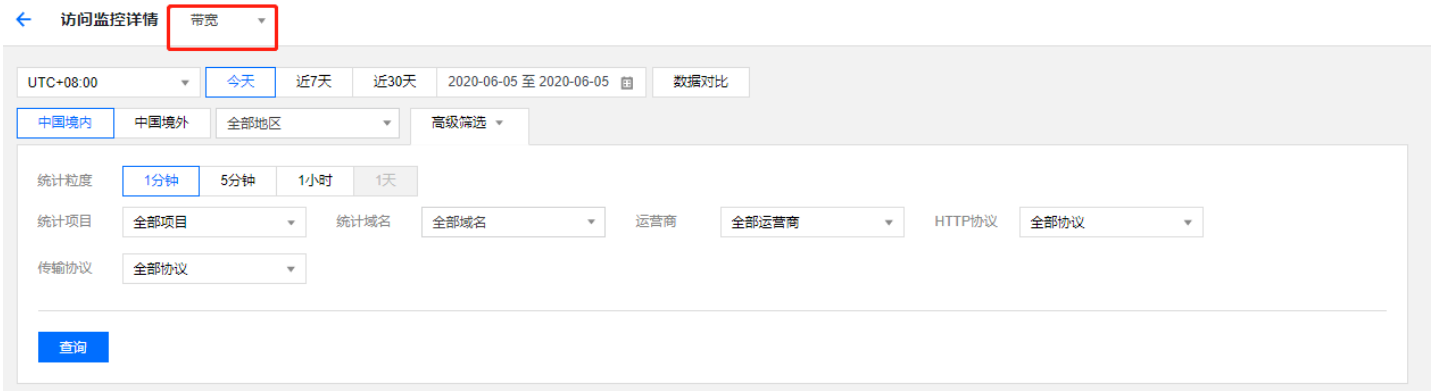
登录 CDN 控制台，在左侧目录中，选择【统计分析】>【实时监控】，进入管理页面后，默认显示【访问监控】子页面。返回全部域名近6小时1分钟粒度监控曲线，包含指标如下：

- 带宽：根据1分钟总流量除以时间（60秒）折算而来。
- 流量命中率：1分钟内（总下行流量 - 回源流量）/ 总下行流量计算而来。
- 请求数状态码占比：所选时间区间 2XX/3XX/4XX/5XX 占比图。
- 请求数状态码 2XX：2XX 状态码监控，产生的状态码都会统计在内。
- 请求数状态码 3XX：3XX 状态码监控，产生的状态码都会统计在内。
- 请求数状态码 4XX：4XX 状态码监控，产生的状态码都会统计在内。
- 请求数状态码 5XX：5XX 状态码监控，产生的状态码都会统计在内。

详情页数据说明

单击每一个指标下方【查看详情】，即可进入指标详情页面。

也可在详情页中，通过左上方进行指标快速切换。



在详情页可以查看以下数据：

- 带宽：总峰值带宽、实时带宽曲线、域名带宽排行（从大到小）。
- 流量：总流量、实时流量曲线、域名流量排行（从大到小）、URL 流量排行（从大到小）。
- 流量命中率：流量命中率、实时流量命中率曲线、域名流量命中率排行（从大到小）。
- 请求数：总请求数、实时请求数曲线、域名请求数排行（从大到小）、URL 请求数排行（从大到小）。
- 状态码占比：2XX、3XX、4XX、5XX 状态码占比环装图，及各具体状态码数量及占比。
- 状态码 2XX：2XX 状态码实时监控曲线及组成 2XX 的各子状态码监控曲线，2XX 状态码域名排行（从大到小）。
- 状态码 3XX：3XX 状态码实时监控曲线及组成 3XX 的各子状态码监控曲线，3XX 状态码域名排行（从大到小）。
- 状态码 4XX：4XX 状态码实时监控曲线及组成 4XX 的各子状态码监控曲线，4XX 状态码域名排行（从大到小）。
- 状态码 5XX：5XX 状态码实时监控曲线及组成 5XX 的各子状态码监控曲线，5XX 状态码域名排行（从大到小）。

粒度说明

总览页面粒度说明

监控页面提供1分钟、5分钟、1小时、1天粒度的曲线展示选项，根据所选时间区间不同，最小可展示的时间粒度不同：

- 时间区间 ≤ 6小时，最小时间粒度为1分钟，1分钟粒度监控曲线目前的延迟约为5 – 10分钟。
- 时间区间 > 6小时且 ≤ 24小时，最小时间粒度为5分钟，5分钟数据延迟为5 – 10分钟。
- 时间区间 > 24小时且 ≤ 31天，最小时间粒度为1小时。
- 时间区间 > 31天，最小时间粒度为1天。

详情页面粒度说明

进入指标详情页面，时间粒度如下：

- 时间区间 ≤ 1天，最小时间粒度为1分钟，1分钟粒度监控曲线目前的延迟约为5 – 10分钟。
- 时间区间 > 1天且 ≤ 31 天，最小时间粒度为5分钟，1小时、1天（可选）。
- 时间区间 > 31天，最小时间粒度为1天。

> ⚠ 注意：
>
> - 1分钟统计粒度数据查询目前仅支持中国境内，历史数据最小可查询粒度为5分钟。
> - 最大可查询时间区间为近90天。

聚合说明

根据数据指标不同，从1分钟粒度聚合为5分钟、1小时、1天方式各有不同：

- 带宽：CDN 提供的带宽监控最细粒度数据为1分钟数据，根据业内标准，计费通常使用的5分钟粒度数据，是由1分钟数据 AVG 而来，因此1小时、1天周期的带宽数据，使用5分钟粒度求 MAX。
- 流量：5分钟、1小时、1天周期的流量数据，均使用1分钟粒度流量数据累加而来。
- 流量命中率：流量命中率根据所选时间粒度，仍利用（总下行流量 - 回源流量）/ 总下行流量同一个公式计算而来，而非利用1分钟结果数据做算术平均。
- 请求数、状态码：5分钟、1小时、1天数据，均使用1分钟粒度数据累加而来。

数据源说明

计费数据与日志数据

- 加速域名日志中记录的下行字节数统计而来的数据，是应用层数据，实际网络传输中，产生的网络流量要比纯应用层流量多5% - 15%：
  - TCP/IP 包头消耗：基于 TCP/IP 协议的 HTTP 请求，每一个包的大小最大是1500个字节，包含了 TCP 和 IP 协议的40个字节的包头，包头部分会产生流量，但是无法被应用层统计到，这部分的开销大致为3%左右。
  - TCP 重传：正常网络传输过程中，发送的网络包会有3% - 10%左右会被互联网丢掉，丢掉后服务器会对丢弃的部分进行重传，此部分流量应用层也无法统计，占比约为3% - 7%。
- 在业内标准中，计费所用数据一般是在应用层数据的基础上加上上述开销，腾讯云 CDN 取10%。因此，监控展示的计费流量 / 带宽约为日志计算数据的110%左右。
- 除流量带宽外，其他指标项均为应用层统计量，监控展示的数据与日志数据统计仅存在微小差异，主要是受网络波动影响，从节点拉取日志分析或服务器上报数据时，均可能存在一定丢失，导致无法完全一致。

数据源说明

- 未筛选“统计地区”或“运营商”选项时，查询到的数据均为计费数据。
- 筛选“统计地区”或“运营商”时，需要根据访问日志中 Client IP 匹配计算，查询到的数据均为日志数据。

筛选说明

- 当前暂不支持“统计地区”、“运营商”双项指定查询，仅支持指定省份查询全部运营商，或指定运营商查询全部地区。
- 回源监控暂不支持“统计地区”、“运营商”筛选。
- 回源监控暂不支持 HTTPS/HTTP 请求筛选。

回源监控

最近更新时间：2022-01-07 09:51:07

指标说明

概览页指标说明

登录 CDN 控制台，在左侧目录中，选择【统计分析】>【实时监控】，进入管理页面后，默认显示【访问监控】子页面，单击上方【回源监控】，可进入回源监控指标页面，返回全部域名近6小时1分钟粒度监控曲线，包含指标如下：

- 回源带宽：根据1分钟总回源流量除以时间（60秒）折算而来。
- 回源流量：最后一层加速节点总回源流量。
- 回源请求数：最后一层加速节点总回源请求数。
- 回源失败率：回源失败请求在总回源请求中占比。
- 回源状态码占比：所选时间区间回源产生的 2XX/3XX/4XX/5XX 占比图。
- 回源状态码 2XX：回源 2XX 状态码监控，产生的状态码都会统计在内。
- 回源状态码 3XX：回源 3XX 状态码监控，产生的状态码都会统计在内。
- 回源状态码 4XX：回源 4XX 状态码监控，产生的状态码都会统计在内。
- 回源状态码 5XX：回源 5XX 状态码监控，产生的状态码都会统计在内。

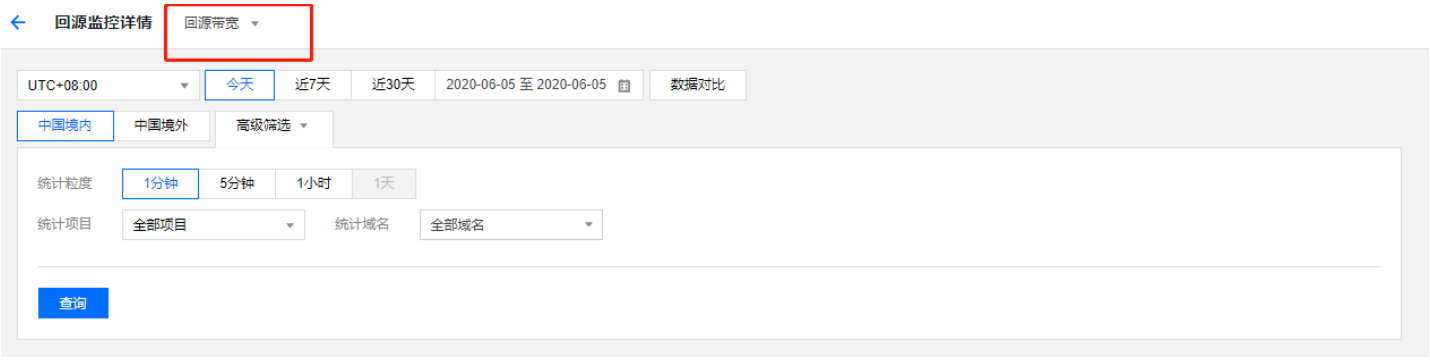
以下情况会计算入回源失败请求：

- 回源数据接收超时。
- 回源请求发送超时。
- 回源 tcp connect 超时。
- 源站主动关闭连接。
- 源站 HTTP 协议兼容性错误。

详情页数据说明

单击每一个指标下方的【查看详情】，即可进入指标详情页面。

也可在详情页中，通过左上方进行指标快速切换。



粒度说明

总览页面粒度说明

监控页面提供1分钟、5分钟、1小时、1天粒度的曲线展示选项，根据所选时间区间不同，最小可展示的时间粒度不同：

- 时间区间 ≤ 6小时，最小时间粒度为1分钟，1分钟粒度监控曲线目前的延迟约为3分钟左右。
- 时间区间 > 6小时且 ≤ 24小时，最小时间粒度为5分钟，5分钟数据延迟为5 – 10分钟。
- 时间区间 > 24小时且 ≤ 31天，最小时间粒度为1小时。
- 时间区间 > 31天，最小时间粒度为1天。

详情页面粒度说明

进入指标详情页面，时间粒度如下：

- 时间区间 ≤ 24小时，最小时间粒度为1分钟，1分钟粒度监控曲线目前的延迟约为3分钟左右。
- 时间区间 > 24小时且 ≤ 31天，最小时间粒度为5分钟，1小时、1天（可选）。
- 时间区间 > 31天，最小时间粒度为1天。

> ⚠ 注意：
>
> - 1分钟粒度数据新版本上线后才可查询，历史数据最小可查询粒度为5分钟。
> - 最大可查询时间区间为最近90天。

聚合说明

根据数据指标不同，从1分钟粒度聚合为5分钟、1小时、1天方式各有不同：

- 回源带宽：CDN 提供的带宽监控最细粒度数据为1分钟数据，根据业内标准，计费通常使用的5分钟粒度数据，是由1分钟数据 AVG 而来，因此1小时、1天周期的带宽数据，使用5分钟粒度求 MAX。
- 回源流量：5分钟、1小时、1天周期的流量数据，均使用1分钟粒度流量数据累加而来。

版权所有：腾讯云计算（北京）有限责任公司

- 回源请求数：5分钟、1小时、1天周期的流量数据，均使用1分钟粒度请求数累加而来。
- 回源失败率：根据所选时间粒度，总回源失败数 / 总回源请求数计算所得。
- 回源状态码：5分钟、1小时、1天周期的状态码数据，均使用1分钟粒度状态码数据累加而来。

状态码说明

最近更新时间：2021-12-10 16:38:00

以下为 CDN 内部状态码含义说明：

状态码	含义	处理建议
0	获取到响应给请求的状态码前，请求结束	请检查客户端是否过早的主动断开请求，或检查回源是否失败。
400	HTTP 请求语法错误服务器无法解析	请检查请求语法是否正确。
403	请求拒绝	请检查是否配置 referer 黑白名单、IP 黑白名单，鉴权配置等访问控制功能。
413	POST 长度超出限制	请检查客户端 POST 内容大小（默认大小限制为32MB）。
414	URL 长度超出限制	URL 默认大小限制为2KB。
423	回环请求	请检查回源跟随301/302配置，HTTPS 配置回源方式，源站 rewrite 的处理方式。
499	客户端主动断开连接	请检查客户端状态或超时时间设置。
502	网关错误	请检查业务源站是否正常。
503	触发 COS 频控	请检查缓存配置或 COS 源站返回 no-cache/no-store。

版权所有：腾讯云计算（北京）有限责任公司

状态码	含义	处理建议
504	网关超时	请与网站官方联系。
509	触发 CC 攻击被封禁	请 联系我们 或 提交工单 解封。
514	超出 IP 访问限频	请检查 CDN 控制台 IP 访问限频配置。
531	HTTPS 请求回源域名解析错误	请检查源站域名解析配置。
532	HTTPS 请求回源站建连失败	请检查源站443端口状态及证书配置或源站可用性。
533	HTTPS 请求回源站连接超时	请检查源站443端口状态及证书配置或源站可用性。
537	HTTPS 请求接受源站数据超时	请检查业务源站稳定性。
538	HTTPS 请求 SSL 握手失败	请检查源站协议和算法的兼容性。
539	HTTPS 请求证书校验失败	请检查源站证书是否正常配置（是否过期、是否证书链齐全）。

状态码	含义	处理建议
540	HTTPS 请求证书域名校验不通过	请检查源站证书是否正常配置。
562	HTTPS 请求建连失败	请 联系我们 并提供 X-NWS-LOG-UUID 信息或 提交工单 进行排查。
563	HTTPS 请求连接超时	请 联系我们 并提供 X-NWS-LOG-UUID 信息或 提交工单 进行排查。
564	HTTPS 请求回源失败	若配置为 HTTP 回源方式，请检查源站负载及带宽使用率，或源站访问限制。 若配置为协议跟随方式，请检查源站443端口状态及证书配置。 若排查源站无异常，请 联系我们 并提供 X-NWS-LOG-UUID 信息或 提交工单 进行排查。

数据分析

最近更新时间：2022-04-29 16:25:08

功能介绍

腾讯云内容分发网络 CDN 主要通过分析访问日志数据，在数据分析页面提供多种数据指标，供您多维度了解业务数据。

> ⚠ 注意：
>
> - 受时延和算法影响，访问用户区域分布和 URL 排行等 TOP 排行类数据仅供参考，请以实际日志数据分析为准。
> - 监控数据与日志数据有差异，此为正常现象。详细说明和更多数据类问题请见 常见问题-统计分析问题。

详细说明

登录 CDN 控制台，在左侧目录中，单击**统计分析** > **数据分析**，进入数据分析页面。

查询条件

请您根据实际需要选择正确的查询条件查询数据：

- 统计类型：即产品类型。“内容分发”指内容分发网络 CDN，“全站加速”指全站加速网络 ECDN。
  注：不同产品支持的数据指标能力不同。我们在持续补齐和更新数据分析能力中，请关注 产品动态。
- 统计地域：即域名的加速区域。
  注：不同统计地域支持的数据指标能力不同。我们在持续补齐和更新数据分析能力中，请关注 产品动态。
- 统计项目：即域名当前最新归属的项目。
- 统计域名：即要查询的域名范围。
- 时间选择：即要查询的时间范围。
  注：大部分数据指标支持的查询的时间范围为：近90天内。
- 展示数据：即支持的数据指标范围

数据概览

数据总量概览，因基础计费方式而异：

- 流量计费时展示：总流量（监控数据）；平均流量命中率；请求数。
- 带宽计费时展示：峰值带宽（监控数据），回源峰值带宽；请求数。

访问用户区域分布

您的业务用户的区域分布，即客户端地区分布。通过客户端 IP 识别出访问用户所在区域，供您了解业务用户的区域分布情况。

- 中国境内按不同省份统计，中国境外按不同区域统计。
- 默认按流量排行，可选择按请求数排行。

> ⚠ 注意：
> ECDN 暂不支持此数据指标。

流量

流量用量的趋势图

- 默认为计费流量（即访问流量），可选择回源流量

带宽

带宽用量的趋势图

- 默认为计费带宽（即访问带宽），可选回源带宽，可选择显示峰值带宽曲线。

请求数

请求数的趋势图。

错误码

错误码总量及不同错误码的数量及占比。

TOP 1000 URL

访问 URL 排行数据

- 默认按流量排行，可选择按请求数排行。

TOP 10 项目

项目排行数据，因基础计费方式而异：

- 带宽计费：按计费带宽排行
- 流量计费：按计费流量排行

> ⚠ 注意：
> 仅当查询时间为完整自然月，例如10月1日至10月30日时，才可选择此数据指标。

TOP 100 域名

加速域名排行数据，因基础计费方式而异：

- 带宽计费：按计费带宽排行
- 流量计费：按计费流量排行

> ⚠ 注意：
> 仅当查询时间为完整自然月，例如10月1日至10月30日时，才可选择此数据指标。

独立 IP 访问数

独立 IP 访问数是对访问日志数据中的访问来源客户端 IP 去重计算得出。

- 查询时间小于等于1天时，提供5分钟粒度去重 IP 数曲线。
- 域名情况按全天去重计算日活，多域名/项目/账号情况则按每一个域名日活5分钟粒度累加。

> ⚠ 注意：
> - 仅支持查询近30天内的数据。
> - ECDN 暂不支持此数据指标。

用户运营商分布

您的业务用户所在运营商的分布，通过统计访问来源客户端 IP 识别出的用户所在运营商而来。

- 默认按流量统计，可选择按请求数统计。

TOP 100 客户端 IP（Beta）

客户端 IP 排行数据

- 默认按流量排行，可选择按请求数排行

> ⚠ 注意：
> ECDN 暂不支持此数据指标。

TOP UA（Beta）

UA 信息排行数据

- 支持三种类型可选：设备，浏览器和操作系统，默认选中设备
  - 设备：用户在访问时最常使用的设备类型，例如桌面设备或移动设备
  - 浏览器：用户访问时最常使用的浏览器名称（或名称和版本），例如Chrome 或 Firefox

版权所有：腾讯云计算（北京）有限责任公司

- 操作系统：用户访问时最常用的操作系统名称（或名称和版本），例如Linux、Mac OS X 或 Windows
- 默认按流量排行，可选择按请求数排行

> **注意：**
> ECDN 暂不支持此数据指标。

TOP 100 Referer (Beta)

Referer 信息排行数据

- 默认按流量排行，可选择按请求数排行

> **注意：**
> - ECDN 暂不支持此数据指标。
> - TOP 100 客户端 IP (Beta)，TOP UA（Beta）和TOP 100 Referer (Beta)支持的最早可查询时间为 2021-09-20，在此之前无数据统计。此三项数据指标为测试版本，数据仅供参考。如需精确数据，请以实际日志数据分析为准。

统计分析常见问题

最近更新时间：2021-07-21 14:35:33

访问监控中的带宽数据是如何统计的?

各 CDN 节点会实时采集流量数据，上报至计算中心，汇总为域名总流量数据。按照时间周期，使用流量/时间，折算为带宽数据进行展示。
例如：

- 某1分钟产生的总流量为6MB，则对应的带宽为（6 * 8）/ 60 = 0.8Mbps。
- 带宽计费时使用5分钟粒度数据结算，则对应带宽值 = 5分钟粒度总流量 ÷ 300秒。

为什么监控流量与日志计算流量对不上，有什么区别?

加速域名日志中记录的下行字节数统计而来的流量数据，是应用层数据。在实际网络传输中，产生的网络流量要比纯应用层流量多5% - 15%。

- TCP/IP 包头消耗：基于 TCP/IP 协议的 HTTP 请求，每一个包的大小最大是1500个字节，包含了 TCP 和 IP 协议的40个字节的包头，包头部分会产生流量，但是无法被应用层统计到，这部分的开销大致为3%左右。
- TCP 重传：正常网络传输过程中，发送的网络包会有3% - 10%左右会被互联网丢掉，丢掉后服务器会对丢弃的部分进行重传，此部分流量应用层也无法统计，占比约为3% - 7%。

在业内标准中，计费用流量一般在应用层流量的基础上加上上述开销，腾讯云 CDN 取10%，因此监控流量约为日志计算流量的110%。

如何计算流量命中率?

CDN 默认为用户开启二级缓存（边缘层、中间层），只要由 CDN 任意一个层级命中，响应请求，则算做命中 CDN 节点。
流量命中率 =（总下行流量 - 回源流量）/ 总下行流量。

如何处理流量命中率偏低问题?

详情请参见 流量命中率偏低。

状态码统计会统计所有产生的状态码吗?

会，CDN 统计分析新版上线后，只要是源站产生的状态码，都会产生对应的监控曲线，方便您排查异常问题。

如何计算省份、运营商统计数据?

省份、运营商统计数据，是从访问日志中利用 client IP 信息计算而来的，由于采用的是纯日志计算，因此累加起来与选择“全部省份”、“全部运营商”时，采用的计费数据存在一定差值，具体原因详情请参考上述 第二个问题。

版权所有：腾讯云计算（北京）有限责任公司

CDN 回源流量是怎么产生的?

以下三种情况会产生 CDN 回源流量:

1. CDN 节点上没有资源，需要到源站拉取的时候。
2. 手动刷新源站时同步到节点的时候。
3. 源站刷新时间到了自动刷新的时候。

CDN 流量异常/遭受 DDOS、CC 攻击。

您好，如果您认为您的业务访问量并不大，可以下载日志根据您的业务访问情况，来做出相关访问限制。CDN 并不清楚您的业务逻辑，所以默认是不会对访问作出限制的，需要您自行按照业务情况去配置，详情请参见 高额账单风险警示。

为避免您的站点被盗刷流量或者遭遇类似 CC、DDOS 等攻击，强烈建议做如下配置:

1. 防盗链配置：对业务资源的访问来源进行控制，通过对用户 HTTP Request Header 中 referer 字段的值设置访问控制策略，从而限制访问来源，避免恶意用户盗刷。详情请参见 防盗链配置。
2. IP 黑白名单配置：您可以根据业务需要对用户请求的源 IP 配置过滤策略，帮助您解决恶意 IP 盗刷、攻击等问题，详情请参见 IP 黑白名单配置。
3. IP 访问限频配置：通过对客户端 IP 在每一个节点每一秒钟访问次数进行限制，进行 CC 攻击的抵御。配置开启后，超出QPS限制的请求会直接返回514，设置较低频次限制可能会影响您的正常高频用户的使用，请根据业务情况、使用场景合理设置阈值，详情请参见 IP 访问限频配置。
4. 带宽封顶配置：您可以对域名设置带宽封顶阈值，当域名在一个统计周期（5分钟）内产生的带宽超过指定阈值时，会根据您的配置将所有访问返回给源站，或直接关闭 CDN 服务，所有访问均返回 404，详情请参见 带宽封顶配置。

> 说明:
> 您也可以使用 安全加速 ，在为您业务提供快速稳定的内容分发服务的基础上，提供全面的网络攻击防护能力。

请问使用 API 接口查询数据时会有延迟吗，延迟有多大?

使用 API 查询数据是有一定延迟的。访问数据、计费数据等的实时数据查询，时延在5-10分钟左右，TOP 数据等分析类的查询时延在半小时左右。后台在凌晨3点左右会对数据进行校准。

刷新预热
缓存刷新

最近更新时间：2022-04-08 11:55:27

功能介绍

内容分发网络（CDN）提供基础缓存配置能力，可根据指定业务类型、目录、具体 URL 等各类规则设置缓存过期时间，来达到定期清理节点缓存资源，回源站重新拉取最新资源重新缓存的目的。

除此之外，CDN 提供了缓存刷新的能力，可批量指定 URL 或目录进行刷新操作：

- 刷新 URL：删除 CDN 所有节点上对应资源的缓存。
- 刷新目录：选择 “刷新变更资源” 模式，当用户访问匹配目录下资源时，会回源获取资源的 Last-Modify 信息，若与当前缓存资源一致，则直接返回已缓存资源，若不一致，回源拉取资源并重新缓存；选择 “刷新全部资源” 时，当用户访问匹配目录下资源时，直接回源拉取新资源返回给用户，并重新缓存新资源。

> 说明：
> 刷新成功执行后，节点上对应资源无有效缓存，当用户再次发起访问时，节点回源站拉取所需资源，并重新缓存在节点上。因此提交大量的刷新任务，会清空较多缓存，从而导致回源请求突增，源站会产生较大压力。

适用场景

新资源发布

在源站点将新资源覆盖至同名旧资源后，为避免全网用户受节点缓存影响仍访问到旧的资源上，可通过提交对应资源的 URL/目录进行刷新，清空全网缓存后，全网用户可直接访问到最新资源。

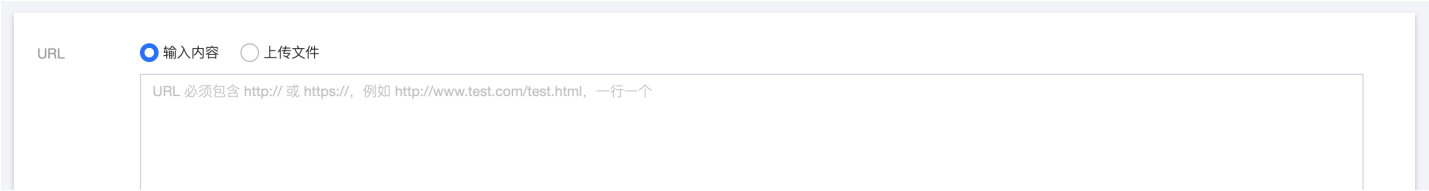
违规资源清理

当站点上存在违规资源（如涉黄、涉毒、涉赌）被发现时，删除源站资源后，由于节点缓存资源仍可被访问到，为维护网络环境，可通过 URL 刷新删除缓存资源，保证及时清理。

操作指南

登录 CDN 控制台，单击左侧目录的**刷新预热**，进入后可按需提交 **URL 刷新**及**目录刷新**任务：

- 内容分发网络 CDN 与 全站加速 ECDN 域名的 URL/目录支持混合填写提交。
- 支持输入内容和上传 txt 文件两种提交方式。



内容规范

请您先关注确认提交的内容是否符合规范：

- URL 必须包含 http:// 或 https:// 协议标识，例如 http://www.test.com/test.html，一行一个。
- 请避免提交已关闭/被锁定/未接入当前账号的域名。
- 若您选择了上传文件的提交方式，需确保文件格式为 txt，大小不超过10M。
- 不支持提交 http://*.test.com/ 格式的 URL – 即使接入的加速域名为泛域名，也需要提交对应的子域名。
- URL 刷新不支持提交包含通配符的 URL。
- 若 URL 含有中文，请开启 URL Encode 开关，对中文编码转换。

提交限额

- **URL 刷新：**
  每一个账号单日 URL 刷新限额为10000个，开通了中国境外加速的客户，中国境外单日 URL 刷新限额为10000个，与境内配额相互独立：
  - 若您选择了自行输入内容的提交方式，单次可提交的 URL 刷新限额为1000个。
  - 若您选择了上传文件的提交方式，无单次提交限额，会直接扣除提交的个数作为剩余配额。

  > 说明：
  > 若您的刷新或预热当日剩余限额不足时，可通过**控制台 > 服务查询 > 配额管理**，申请提升配额。

- **目录刷新：**
  每一个账号单日目录刷新限额为100个，开通了中国境外加速的客户，中国境外单日目录刷新限额为100条，与境内配额相互独立：
  - 若您选择了自行输入内容的提交方式，单次可提交的目录刷新限额为500个。
  - 若您选择了上传文件的提交方式，无单次提交限额，会直接扣除提交的个数作为剩余配额。

提交刷新任务时，默认按照 URL 中域名所在加速区域全区域刷新。域名加速区域为全球时，会同时消耗中国境内和中国境外的配额。

查询操作记录请见 操作记录。

子用户权限配置

URL 刷新、目录刷新和查询刷新记录已经接入权限系统，支持资源（域名）维度权限配置，详细说明请参见 权限配置。

使用案例

目录刷新-刷新变更资源

加速域名为：purge-test-1251991073.file.myqcloud.com，源站为腾讯云对象存储（COS），源站资源如下：

1. 分别发起请求访问资源 1.txt 与 2.txt，根据 X-Cache-Lookup: Hit From Disktank3 与 Server: NWS_SPMid 可以判定命中节点， 由节点直接返回资源：

```
[redacted] curl http://purge-test-1251991073.file.myqcloud.com/fileTest/1.txt -sv
*   Trying 14.215.85.233...
* TCP_NODELAY set
* Connected to purge-test-1251991073.file.myqcloud.com (14.215.85.233) port 80 (#0)
> GET /fileTest/1.txt HTTP/1.1
> Host: purge-test-1251991073.file.myqcloud.com
> User-Agent: curl/7.54.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: NWS_SPMid
< Connection: keep-alive
< Date: Wed, 04 Sep 2019 23:20:46 GMT
< Cache-Control: max-age=600
< Expires: Wed, 04 Sep 2019 23:30:46 GMT
< Last-Modified: Wed, 04 Sep 2019 23:01:37 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 19
< X-NWS-UUID-VERIFY: 72e4a2dbd2e9e5304c17d2beb0bf39d5
< X-NWS-LOG-UUID: 5673286006122774168 b5f0e763fad18324d85b241a7e6695c4
< X-Cache-Lookup: Hit From Disktank3
< Accept-Ranges: bytes
< X-Daa-Tunnel: hop_count=1
< X-Cache-Lookup: Hit From Upstream
<
* Connection #0 to host purge-test-1251991073.file.myqcloud.com left intact
```

```
[redacted] curl http://purge-test-1251991073.file.myqcloud.com/fileTest/2.txt -sv
*   Trying 14.215.85.233...
* TCP_NODELAY set
* Connected to purge-test-1251991073.file.myqcloud.com (14.215.85.233) port 80 (#0)
> GET /fileTest/2.txt HTTP/1.1
> Host: purge-test-1251991073.file.myqcloud.com
> User-Agent: curl/7.54.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: NWS_SPMid
< Connection: keep-alive
< Date: Wed, 04 Sep 2019 23:22:03 GMT
< Cache-Control: max-age=600
< Expires: Wed, 04 Sep 2019 23:32:03 GMT
< Last-Modified: Wed, 04 Sep 2019 23:01:37 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 19
< X-NWS-UUID-VERIFY: e7112793c4a1bdde407954fb943e43fb
< X-NWS-LOG-UUID: 14628995741359757299 b5f0e763fad18324d85b241a7e6695c4
< X-Cache-Lookup: Hit From Disktank3
< Accept-Ranges: bytes
< X-Daa-Tunnel: hop_count=1
< X-Cache-Lookup: Hit From Upstream
<
* Connection #0 to host purge-test-1251991073.file.myqcloud.com left intact
```

2. 在源站替换掉同名文件 1.txt，文件修改时间发生改变，2.txt 保持不变：

基本信息

对象名称	1.txt
对象大小	19B
修改时间	2019-09-04 23:01:37
ETag	"2752a0cf4777c342ac1f23ee606aed99"
对象地址	https://purge-test-1251991073.cos.ap-chengdu.myqcloud.com/fileTest/1.txt
临时链接	复制临时链接 下载对象 刷新有效期

临时链接携带签名参数，在签名有效期内可使用临时链接访问对象，签名有效期为 1 小时（2019-09-05 00:23:30）。
请注意保管好您的临时链接，避免其外泄，否则可能使您的对象被其他用户访问。

基本信息

对象名称	1.txt
对象大小	23B
修改时间	2019-09-04 23:24:17
ETag	"325daac4e71e82db89ee26922d7435b7"
对象地址	https://purge-test-1251991073.cos.ap-chengdu.myqcloud.com/fileTest/1.txt
临时链接	复制临时链接 下载对象 刷新有效期

临时链接携带签名参数，在签名有效期内可使用临时链接访问对象，签名有效期为 1 小时（2019-09-05 00:24:22）。
请注意保管好您的临时链接，避免其外泄，否则可能使您的对象被其他用户访问。

3. 此时再发起请求，由于缓存尚未过期，访问资源 1.txt 仍为旧的内容：

```
[redacted] curl http://purge-test-1251991073.file.myqcloud.com/fileTest/1.txt -sv
*   Trying 113.105.165.187...
* TCP_NODELAY set
* Connected to purge-test-1251991073.file.myqcloud.com (113.105.165.187) port 80 (#0)
> GET /fileTest/2.txt HTTP/1.1
> Host: purge-test-1251991073.file.myqcloud.com
> User-Agent: curl/7.54.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: NWS_SPMid
< Connection: keep-alive
< Date: Wed, 04 Sep 2019 23:34:19 GMT
< Cache-Control: max-age=600
< Expires: Wed, 04 Sep 2019 23:44:19 GMT
< Last-Modified: Wed, 04 Sep 2019 23:01:37 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 19
< X-NWS-UUID-VERIFY: 72e4a2dbd2e9e5304c17d2beb0bf39d5
< X-NWS-LOG-UUID: 567328600612277 4168 b5f0e763fad18324d85b241a7e6695c4
< X-Cache-Lookup: Hit From Disktank3
< Accept-Ranges: bytes
< X-Daa-Tunnel: hop_count=1
< X-Cache-Lookup: Hit From Upstream
<
* Connection #0 to host purge-test-1251991073.file.myqcloud.com left intact
```

4. 提交目录刷新，选择【刷新变更资源】，等待刷新完成：

5. 刷新完成后，由于文件 1.txt Last-Modified 发生变更，请求直接回源，而文件 2.txt 由于未做变更，即使提交目录刷新，仍被节点命中返回：

```
curl http://purge-test-1251991073.file.myqcloud.com/fileTest/1.txt -sv
*   Trying 113.105.165.187...
* TCP_NODELAY set
* Connected to purge-test-1251991073.file.myqcloud.com (113.105.165.187) port 80 (#0)
> GET /fileTest/1.txt HTTP/1.1
> Host: purge-test-1251991073.file.myqcloud.com
> User-Agent: curl/7.54.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: tencent-cos
< Connection: keep-alive
< Date: Wed, 04 Sep 2019 23:33:22 GMT
< Last-Modified: Wed, 04 Sep 2019 23:24:17 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 23
< X-NWS-UUID-VERIFY: 6a4ea0410342aee319550d46b866cd37
< Accept-Ranges: bytes
< ETag: "325daac4e71e82db89ee26922d7435b7"
< x-cos-request-id: NWQ2ZmQ5NDJfMjZiMjU4NjRfMzY0Yl81MmU1YWI=
< X-Daa-Tunnel: hop_count=2
< X-NWS-LOG-UUID: 14013390993447302634 2107abdde3874148ff95a672f195831b
< X-Cache-Lookup: Hit From Upstream
< X-Cache-Lookup: Hit From Upstream
<
* Connection #0 to host purge-test-1251991073.file.myqcloud.com left intact
```

```
curl http://purge-test-1251991073.file.myqcloud.com/fileTest/2.txt -sv
*   Trying 113.105.165.187...
* TCP_NODELAY set
* Connected to purge-test-1251991073.file.myqcloud.com (113.105.165.187) port 80 (#0)
> GET /fileTest/2.txt HTTP/1.1
> Host: purge-test-1251991073.file.myqcloud.com
> User-Agent: curl/7.54.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: NWS_SPMid
< Connection: keep-alive
< Date: Wed, 04 Sep 2019 23:34:19 GMT
< Cache-Control: max-age=600
< Expires: Wed, 04 Sep 2019 23:44:19 GMT
< Last-Modified: Wed, 04 Sep 2019 23:01:37 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 19
< X-NWS-UUID-VERIFY: e7112793c4a1bdde407954fb943e43fb
< X-NWS-LOG-UUID: 1690084127387779050 2107abdde3874148ff95a672f195831b
< X-Cache-Lookup: Hit From Disktank3
< Accept-Ranges: bytes
< X-Daa-Tunnel: hop_count=1
< X-Cache-Lookup: Hit From Upstream
<
* Connection #0 to host purge-test-1251991073.file.myqcloud.com left intact
```

缓存预热

最近更新时间：2022-05-23 12:09:14

功能介绍

腾讯云 CDN 提供资源预热功能，可将指定资源主动从源站加载至 CDN 加速节点并缓存。当用户首次请求资源时，可直接从 CDN 加速节点获取缓存的资源，无需再次回源。

> ⚠ 注意：
>
> - 中国境内区域预热，资源默认加载至中国境内中间层节点；中国境外区域预热，资源默认加载至中国境外边缘节点。预热加载资源至边缘节点，所产生的边缘层流量会计入计费流量。
> - 节点预热时，若其缓存的同名资源尚未过期，则不会进行资源加载。建议在同名文件更新时，先进行全网刷新再提交预热。
> - 节点预热时，会回源拉取所需内容，因此提交大批量预热任务后，会造成源站带宽增大。
> - 预热可理解为由CDN主动模拟用户发起首次请求，需要提交具体资源的URL地址，因此无法支持目录预热。

适用场景

安装包发布

新版本安装包或是升级包发布前，提前将资源预热至 CDN 加速节点。正式上线后，海量用户的下载请求将直接由全球加速节点响应，提升下载速度的同时，大幅度降低源站压力。

运营活动

运营活动发布前，提前将活动页涉及到的静态资源预热至 CDN 加速节点。活动开始后，用户访问中所有静态资源均由加速节点响应，海量带宽储备保障用户服务可用性，提升用户体验。

操作指南

登录 CDN 控制台，单击左侧目录的**刷新预热**，进入后可按需提交 **URL 预热**任务：

- 内容分发网络 CDN 与 全站加速 ECDN 域名的 URL支持混合填写提交。
- 支持输入内容和上传 txt 文件两种提交方式。
- 支持指定预热区域：预热地域对应域名的加速区域，请按需选择。

内容规范

请您先关注确认提交的内容是否符合规范

- URL 必须包含 http:// 或 https:// 协议标识，例如 http://www.test.com/test.html，一行一个。
- 请避免提交已关闭/被锁定/未接入当前账号的域名。
- 若您选择了上传文件的提交方式，需确保文件格式为 txt，大小不超过10M。
- 不支持提交 http://*.test.com/ 格式的 URL – 即使接入的加速域名为泛域名，也需要提交对应的子域名。
- 不支持提交包含通配符的 URL。
- 不支持路径中携带中文的 URL。

提交限额

每一个账号单日 URL 预热限额为1000个，开通了中国境外加速的客户，中国境外单日 URL 刷新限额为1000个，与境内配额相互独立：

- 若您选择了自行输入内容的提交方式，单次可提交的 URL 预热限额为500个。
- 若您选择了上传文件的提交方式，无单次提交限额，会直接扣除提交的个数作为剩余配额。
- 域名加速区域为全球，指定预热地域为全球时，会同时消耗中国境内和中国境外的配额。

> 说明：
> 若您的刷新或预热当日剩余限额不足时，可通过**控制台 > 服务查询 > 配额管理**，申请提升配额。

查询操作记录请见 操作记录。

子用户权限配置

URL 预热和查询预热记录已经接入权限系统，支持资源（域名）维度权限配置，详细说明请参见 权限配置。

操作记录

最近更新时间：2021-08-24 19:20:26

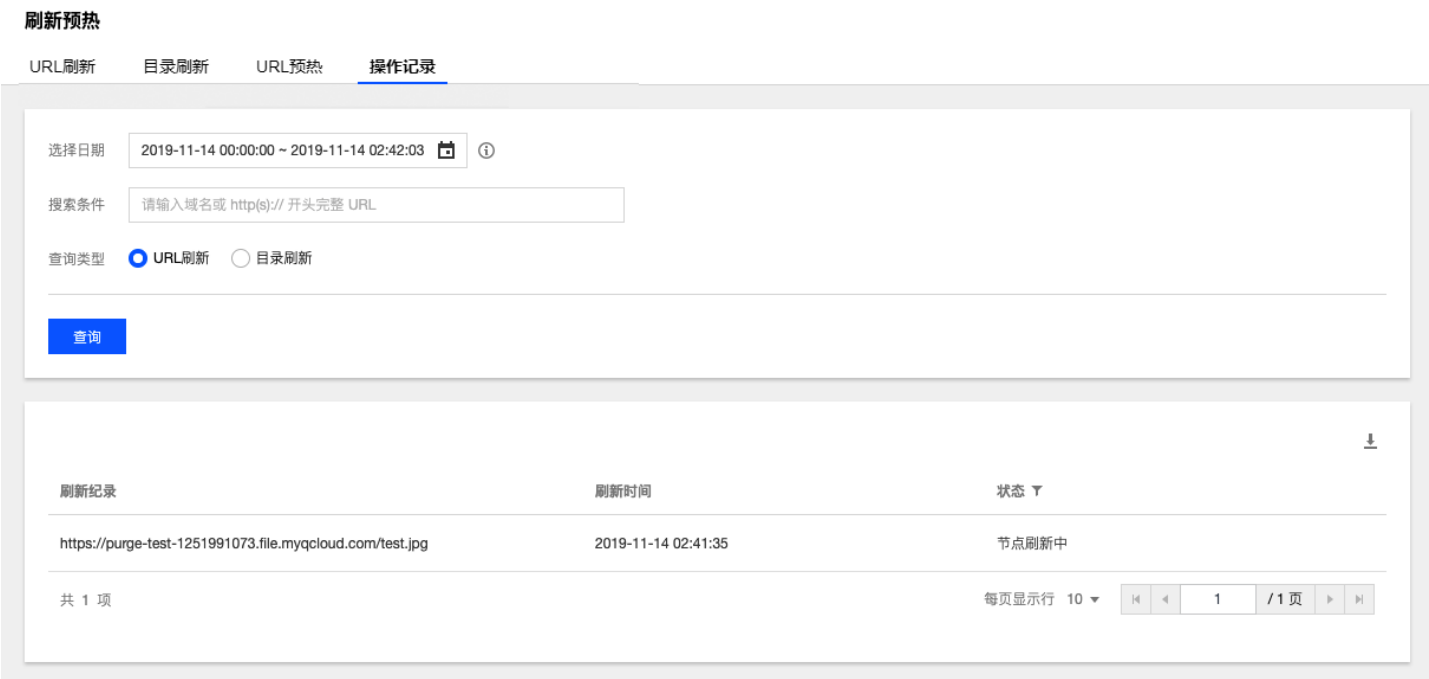
功能介绍

提交刷新预热任务后，您可以在**操作记录**页中，查看资源刷新预热的详细记录和状态。

操作指南

使用方式

1.登录 CDN 控制台，单击左侧目录的**刷新预热**后，单击**操作记录**。
2.对指定时间周期、关键字、刷新任务类型进行查询，关键字仅支持指定域名查询，或指定完整的刷新 URL/目录查询。



使用说明

控制台最多可一次性返回 10000 条操作记录，并支持导出为完整的 excel 形式，若您的刷新任务较多，请分段批量查询导出。

刷新预热常见问题

最近更新时间：2021-09-03 11:18:03

什么情况下需要用到刷新预热功能?

- 刷新：当您的源站有资源更新/需要清理违规资源/域名有配置变更，为避免全网用户受节点缓存影响仍访问到旧的资源/受旧配置的影响，可提交刷新任务，保证全网用户可访问到最新资源或正常访问。详细说明请见 缓存刷新。
- 预热：当您有运营活动或安装包/升级包发布等，可提交预热任务，提前将静态资源预热至 CDN 加速节点，降低源站压力，提升用户服务可用性和用户体验。详细说明请见 缓存预热。

刷新与预热区别是什么?

- 刷新后，会删除该资源在全网 CDN 节点上的缓存。当用户请求到达节点时，节点会回源站拉取对应资源，返回给用户并缓存到节点，保证用户获取到最新资源。
- 预热后，该资源会提前缓存到全网 CDN 节点。当用户请求到达节点时，可以直接在节点获取到资源。

刷新预热有什么要求? 需要多久生效?

- 缓存刷新
  - URL 刷新：每日 URL 刷新数量最多不超过10000个，每次刷新提交的 URL 数量不超过1000个，刷新任务生效时间约为5分钟。当文件配置的缓存过期时间少于5分钟时，建议不使用刷新工具，而是等待超时更新。
  - 目录刷新：每日目录刷新数量最多不超过100个，每次刷新提交的 URL 目录数量不超过20个，刷新任务生效时间约为5分钟。当文件夹配置的缓存过期时间少于5分钟，建议不使用刷新工具，而是等待超时更新。
- 资源预热
  - URL 预热：每日 URL 预热数量最多不超过1000个，每次预热提交的 URL 数量不超过20个，预热任务生效时间依据预热文件大小而定，约需要5到30分钟。

CDN 加速节点上的缓存内容是实时更新的吗?

目前 CDN 加速节点上的缓存内容不会实时更新。CDN 节点根据您在控制台配置的 缓存过期配置 来更新缓存，若您需要实时更新某个文件的缓存，您可以通过 缓存刷新 的手段来进行。

怎么查看刷新预热的记录?

您可以在 CDN 控制台中查看刷新预热的记录，详情请参见 操作记录。

预热时能携带自定义请求头预热吗?

暂不支持。

版权所有：腾讯云计算（北京）有限责任公司

日志服务
日志下载

最近更新时间：2021-11-22 16:42:59

功能介绍

将域名接入内容分发网络（CDN）后，所有用户侧资源请求将调度至 CDN 节点进行响应，若节点已缓存该资源，则直接返回内容，若 CDN 节点均未缓存该资源，会将请求透传至域名配置的源站，拉取所需资源。

由于 CDN 节点响应了绝大部分的用户请求，为了方便客户对用户访问进行分析，CDN 对全网访问日志进行了小时粒度打包，默认存储 30 天，并且提供下载服务。

> 说明：
>
> - 暂时仅提供节点访问日志，不提供回源日志。
> - ECDN 域名离线日志暂不支持分区域查询，ECDN 离线日志字段说明请参考 ECDN 产品文档。

适用场景

访问行为分析

客户可以通过下载访问日志，按自身需要进行热门资源分析、活跃用户分析等。

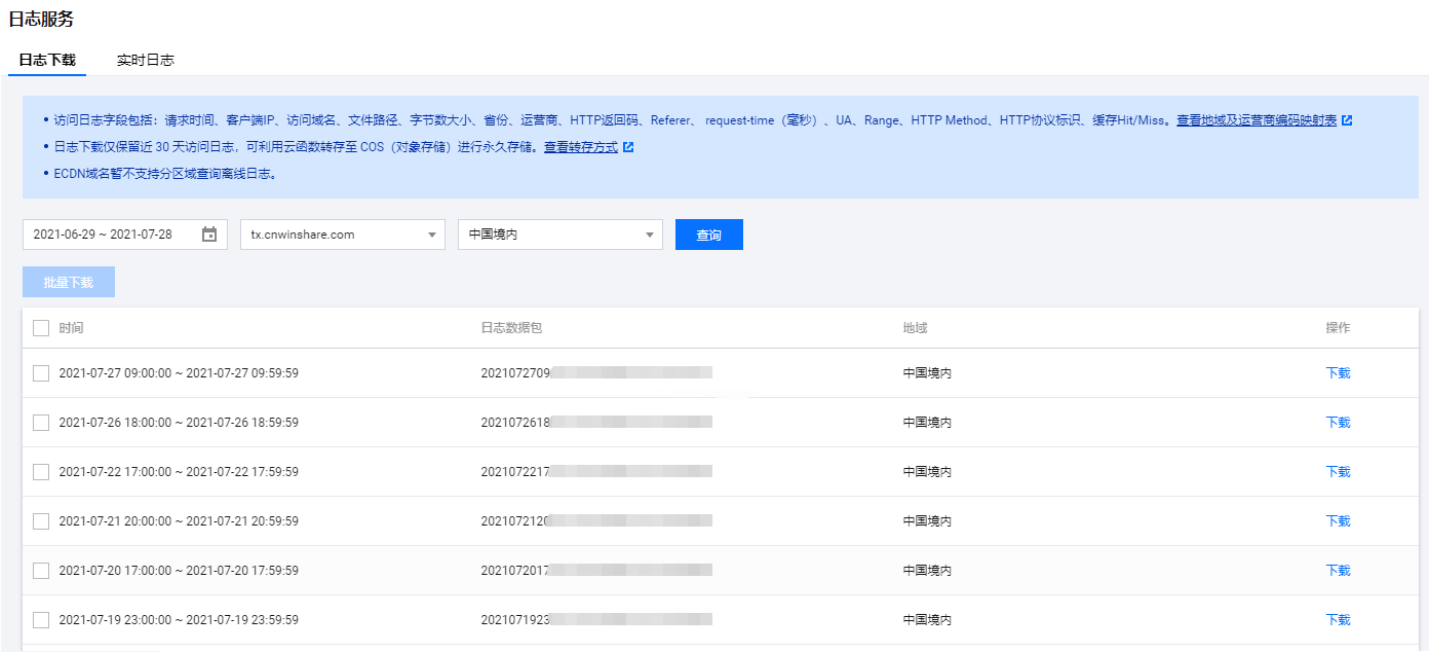
服务质量监控

通过下载访问日志，可以掌握全盘 CDN 节点服务状态，计算平均响应时间、平均下载速度等指标。

操作指南

使用方式

登录 CDN 控制台，单击左侧目录的【日志服务】，可选择域名、时间进行访问日志查询，支持勾选多个日志包，批量下载到本地：



注意：

- 访问日志默认按小时打包，若某个小时里域名无任何请求，则不会产生该时间区间的日志包。
- 同一个域名的境外访问日志跟境内访问日志是分开打包的，日志数据包的命名格式为 “时间-域名-加速区域”。
- 访问日志从各 CDN 加速节点收集而来，因此延迟上各有差异，一般情况下日志包可查询、下载延迟约30分钟，日志包会不断追加，一般24小时左右趋于稳定。
- 域名历史访问日志仅保留 30 天内的日志包，您可以按照以下 指引，利用 SCF 函数将日志包转存至对象存储 COS，进行永久存储。

字段说明

日志中对应的字段顺序（从左到右）及含义如下表所示：

顺序	日志内容
1	请求时间
2	客户端 IP
3	域名
4	请求路径
5	本次访问字节数大小（包含文件本身大小及请求 header 头部大小）
6	境内日志代表省份编号，境外日志代表地区编号（映射表见下文）

顺序	日志内容
7	境内日志代表运营商编号，境外日志统一为 -1（映射表见下文）
8	HTTP 状态码
9	Referer 信息
10	响应时间（毫秒），指节点从收到请求后响应所有回包再到客户端所花费的时间
11	User-Agent 信息
12	Range 参数
13	HTTP Method
14	HTTP 协议标识
15	缓存 HIT/MISS，在 CDN 边缘节点命中、父节点命中均标记为 HIT
16	客户端与 CDN 节点建立连接的端口，若无则为 -

区域 / 运营商映射表

境内省份映射

区域 ID	地区	区域 ID	地区	区域 ID	地区
22	北京	86	内蒙古	146	山西
1069	河北	1177	天津	119	宁夏
152	陕西	1208	甘肃	1467	青海
1468	新疆	145	黑龙江	1445	吉林
1464	辽宁	2	福建	120	江苏
121	安徽	122	山东	1050	上海
1442	浙江	182	河南	1135	湖北
1465	江西	1466	湖南	118	贵州
153	云南	1051	重庆	1068	四川
1155	西藏	4	广东	173	广西

版权所有：腾讯云计算（北京）有限责任公司

区域 ID	地区	区域 ID	地区	区域 ID	地区
1441	海南	0	其他	1	港澳台
-1	境外				

境内运营商映射

运营商 ID	运营商	运营商 ID	运营商	运营商 ID	运营商
2	中国电信	26	中国联通	38	教育网
43	长城宽带	1046	中国移动	3947	中国铁通
-1	境外运营商	0	其他运营商		

境外地区映射

区域 ID	地区	区域 ID	地区	区域 ID	地区
2000000001	亚太一区(服务地区)	765	斯洛伐克	1613	安哥拉
2000000002	亚太二区(服务地区)	766	塞尔维亚	1617	科特迪瓦
2000000003	亚太三区(服务地区)	770	芬兰	1620	苏丹
2000000004	中东(服务地区)	773	比利时	1681	毛里求斯
2000000005	北美(服务地区)	809	保加利亚	1693	摩洛哥
2000000006	欧洲(服务地区)	811	斯洛文尼亚	1695	阿尔及利亚
2000000007	南美(服务地区)	812	摩尔多瓦	1698	几内亚
2000000008	非洲(服务地区)	813	马其顿	1730	塞内加尔
-20	亚洲(客户端地区)	824	爱沙尼亚	1864	突尼斯
-21	南美洲(客户端地区)	835	克罗地亚	1909	乌拉圭
-22	北美洲(客户端地区)	837	波兰	1916	格陵兰
-23	欧洲(客户端地区)	852	拉脱维亚	2026	中国台湾
-24	非洲(客户端地区)	857	约旦	2083	缅甸
-25	大洋洲(客户端地区)	884	吉尔吉斯斯坦	2087	文莱

版权所有：腾讯云计算（北京）有限责任公司

区域 ID	地区	区域 ID	地区	区域 ID	地区
35	尼泊尔	896	爱尔兰	2094	斯里兰卡
57	泰国	901	利比亚	2150	巴拿马
73	印度	904	亚美尼亚	2175	哥伦比亚
144	越南	921	也门	2273	摩纳哥
192	法国	926	白俄罗斯	2343	安道尔
207	英国	971	卢森堡	2421	土库曼斯坦
208	瑞典	1036	新西兰	2435	老挝
209	德国	1044	日本	2488	东帝汶
213	意大利	1066	巴基斯坦	2490	汤加
214	西班牙	1070	马耳他	2588	菲律宾
386	阿联酋	1091	巴哈马	2609	委内瑞拉
391	以色列	1129	阿根廷	2612	玻利维亚
397	乌克兰	1134	孟加拉	2613	巴西
398	俄罗斯	1158	柬埔寨	2623	哥斯达黎加
417	哈萨克斯坦	1159	中国澳门	2626	墨西哥
428	葡萄牙	1176	新加坡	2639	洪都拉斯
443	希腊	1179	马尔代夫	2645	萨尔瓦多
471	沙特阿拉伯	1180	阿富汗	2647	巴拉圭
529	丹麦	1185	斐济	2661	秘鲁
565	伊朗	1186	蒙古	2728	尼加拉瓜
578	挪威	1195	印度尼西亚	2734	厄瓜多尔
669	美国	1200	中国香港	2768	危地马拉
692	叙利亚	1233	卡塔尔	2999	阿鲁巴
704	塞浦路斯	1255	冰岛	3058	埃塞俄比亚

版权所有：腾讯云计算（北京）有限责任公司

区域 ID	地区	区域 ID	地区	区域 ID	地区
706	捷克	1289	阿尔巴尼亚	3144	波黑
707	瑞士	1353	乌兹别克斯坦	3216	多米尼加
708	伊拉克	1407	圣马力诺	3379	韩国
714	荷兰	1416	科威特	3701	马来西亚
717	罗马尼亚	1417	黑山	3839	加拿大
721	黎巴嫩	1493	塔吉克斯坦	4450	澳大利亚
725	匈牙利	1501	巴林	4460	中国大陆
726	格鲁吉亚	1543	智利	-15	亚洲其他
731	阿塞拜疆	1559	南非	-14	南美洲其他
734	奥地利	1567	埃及	-13	北美洲其他
736	巴勒斯坦	1590	肯尼亚	-12	欧洲其他
737	土耳其	1592	尼日利亚	-11	非洲其他
759	立陶宛	1598	坦桑尼亚	-10	大洋洲其他
763	阿曼	1611	马达加斯加	-2	境外其他

境外运营商映射

运营商 ID	运营商
-1	境外运营商

注意事项

通过访问日志第五个字段中记录的字节数，统计计算而来的流量 / 带宽数据与 CDN 计费流量 / 带宽数据不一致。原因如下：

- 访问日志中仅可记录应用层数据，在实际网络传输中，产生的网络流量要比纯应用层流量多5% - 15%。由两部分组成：
  - TCP/IP 包头消耗，基于 TCP/IP 协议的 HTTP 请求，每一个包的大小最大是1500个字节，包含了 TCP 和 IP 协议的40个字节的包头，包头部分会产生流量，但是无法被应用层统计到，这部分的开销大致为3%左右；

- TCP 重传，正常网络传输过程中，发送的网络包会有3% – 10%左右会被互联网丢掉，丢掉后服务器会对丢弃的部分进行重传，此部分流量应用层也无法统计，占比约为3% – 7%。
- 在业内标准中，计费用流量一般在应用层流量的基础上加上上述开销，腾讯云 CDN 取10%，因此监控流量约为日志计算流量的110%。

使用案例

境内访问日志示例

```
20170719174306 10.10.10.10 www.test.com /test.png 77487 3 2 0 NULL 1408 "Mozilla/
20170719174407 10.10.10.10 www.test.com /test2.png 72488 5 2 200 NULL 13569 "Mozi
20170719174520 10.10.10.10 www.test.com /test3.png 74864 4 2 200 NULL 9474 "Mozil
20170719174544 10.10.10.10 www.test.com /test4.png 81453 2 2 200 NULL 9218 "Mozil
20170719174532 10.10.10.10 www.test.com /test5.png 54678 7 2 200 NULL 9041 "Mozil
```

境外访问日志示例

2019111210-shary.oversea.elliotxing.com — 已编辑

```
20191112103527 150.109.22.184 www.test.com /autotest.txt 465 1176 -1 200 NULL 1 "python-requests/2.11.1" "(null)" GET HTTP/1.1 hit
20191112103526 119.28.119.119 www.test.com /autotest.txt 369 1176 -1 200 NULL 664 "python-requests/2.11.1" "(null)" HEAD HTTP/1.1 miss
20191112103527 119.28.119.119 www.test.com /autotest.txt 397 1176 -1 200 NULL 1 "python-requests/2.11.1" "(null)" GET HTTP/1.1 hit
20191112103435 119.28.99.11 www.test.com /autotest.txt 465 1176 -1 200 NULL 1 "python-requests/2.11.1" "(null)" GET HTTP/1.1 hit
20191112103435 119.28.99.11 www.test.com /autotest.txt 410 1176 -1 200 NULL 1073 "python-requests/2.11.1" "(null)" HEAD HTTP/1.1 miss
20191112103734 119.28.99.132 www.test.com /autotest.txt 368 1176 -1 200 NULL 2562 "python-requests/2.11.1" "(null)" HEAD HTTP/1.1 miss
20191112103734 119.28.99.132 www.test.com /autotest.txt 397 1176 -1 200 NULL 1 "python-requests/2.11.1" "(null)" GET HTTP/1.1 hit
20191112103529 119.28.110.232 www.test.com /autotest.txt 409 1176 -1 200 NULL 2748 "python-requests/2.11.1" "(null)" HEAD HTTP/1.1 miss
20191112103529 119.28.110.232 www.test.com /autotest.txt 466 1176 -1 200 NULL 1 "python-requests/2.11.1" "(null)" GET HTTP/1.1 hit
20191112103528 119.28.102.58 www.test.com /autotest.txt 409 1176 -1 200 NULL 3536 "python-requests/2.11.1" "(null)" HEAD HTTP/1.1 miss
20191112103528 119.28.102.58  /autotest.txt 465 1176 -1 200 NULL 1 "python-requests/2.11.1" "(null)" GET HTTP/1.1 hit
20191112103528 150.109.15.108 www.test.com /autotest.txt 409 1176 -1 200 NULL 1659 "python-requests/2.11.1" "(null)" HEAD HTTP/1.1 miss
20191112103529 150.109.15.108 www.test.com /autotest.txt 395 1176 -1 200 NULL 685 "python-requests/2.11.1" "(null)" GET HTTP/1.1 miss
20191112103952 150.109.23.116 www.test.com /autotest.txt 369 1176 -1 200 NULL 1424 "python-requests/2.11.1" "(null)" HEAD HTTP/1.1 miss
20191112103952 150.109.23.116 www.test.com /autotest.txt 397 1176 -1 200 NULL 1 "python-requests/2.11.1" "(null)" GET HTTP/1.1 hit
20191112103717 119.28.99.132 www.test.com /autotest 623 1176 -1 301 NULL 338 "python-requests/2.11.1" "(null)" GET HTTP/1.1 miss
20191112103716 119.28.110.232 www.test.com /autotest 622 1176 -1 301 NULL 650 "python-requests/2.11.1" "(null)" GET HTTP/1.1 miss
20191112103718 119.28.119.119 www.test.com /autotest 622 1176 -1 301 NULL 2007 "python-requests/2.11.1" "(null)" GET HTTP/1.1 miss
20191112103050 119.28.98.180 www.test.com /autotest 439 1176 -1 301 NULL 257 "python-requests/2.11.1" "(null)" HEAD HTTP/1.1 miss
20191112103051 119.28.98.180 www.test.com /autotest 623 1176 -1 301 NULL 233 "python-requests/2.11.1" "(null)" GET HTTP/1.1 miss
20191112103716 119.28.99.11 www.test.com /autotest 581 1176 -1 301 NULL 479 "python-requests/2.11.1" "(null)" GET HTTP/1.1 miss
20191112103715 150.109.23.116 www.test.com /autotest 439 1176 -1 301 NULL 259 "python-requests/2.11.1" "(null)" HEAD HTTP/1.1 miss
20191112103715 150.109.23.116 www.test.com /autotest 622 1176 -1 301 NULL 256 "python-requests/2.11.1" "(null)" GET HTTP/1.1 miss
20191112103713 150.109.23.12 www.test.com /autotest 439 1176 -1 301 NULL 138 "python-requests/2.11.1" "(null)" HEAD HTTP/1.1 miss
20191112105058 49.51.8.223 www.test.com /autotest.txt 409 3839 -1 200 NULL 987 "python-requests/2.18.4" "(null)" HEAD HTTP/1.1 miss
20191112105059 49.51.8.223 www.test.com /autotest.txt 396 3839 -1 200 NULL 967 "python-requests/2.18.4" "(null)" GET HTTP/1.1 miss
20191112105405 49.51.9.82 www.test.com /autotest 622 3839 -1 301 NULL 1406 "python-requests/2.11.1" "(null)" GET HTTP/1.1 miss
20191112103526 150.109.23.116 www.test.com /autotest.txt 409 1176 -1 200 NULL 1387 "python-requests/2.11.1" "(null)" HEAD HTTP/1.1 miss
20191112103526 150.109.23.116 www.test.com /autotest.txt 466 1176 -1 200 NULL 1 "python-requests/2.11.1" "(null)" GET HTTP/1.1 hit
20191112103527 119.28.110.232 www.test.com /autotest.txt 410 1176 -1 200 NULL 862 "python-requests/2.11.1" "(null)" HEAD HTTP/1.1 miss
```

实时日志

最近更新时间：2021-12-22 15:02:16

功能介绍

腾讯云内容分发网络（CDN）实时日志服务：通过对 CDN 访问日志的实时采集与推送，实现对日志数据的快速检索与分析。您可通过 CDN 控制台一站式快捷接入，享受从日志采集、日志存储到日志检索等全方位稳定可靠的日志服务。

适用场景

通过访问日志数据实时地多维度查看 / 分析业务情况。

操作指南

登录 CDN 控制台，单击左侧目录的**日志服务**，上方 Tab 切换至**实时日志**，即可进入实时日志页面。

启用实时日志服务

为启用实时日志服务，请先开通 日志服务（CLS）并授权 CDN 以创建免费的日志集

> 说明：
>
> - 建议您使用主账号启用服务，若为子账号或协作者，请参考 子账号或协作者开通实时日志的方法。
> - 在您开通 CDN 实时日志服务时，CDN 会默认创建免费的日志集，用于承载 CDN 日志（一个地域对应一个日志集）
> - CDN 目前支持投递至上海，北京，成都，重庆，南京，广州和新加坡地域。我们正在计划支持更多地域，请关注产品动态。

创建日志主题

您可通过在日志集下创建日志主题，将目标加速域名的访问日志投递至 日志服务（CLS），启用实时日志服务。

> 注意：
>
> - 一个日志集下至多可创建500个日志主题。
> - 新建日志主题名称不可与现存日志主题名称相同。
> - 同一个日志主题下不可混选内容分发网络 CDN 与全站加速网络 ECDN 域名。
> - CDN 加速域名的中国境内日志仅支持投递至上海，北京，成都，重庆，南京，广州地域，中国境外日志仅支持投递至新加坡地域。

版权所有：腾讯云计算（北京）有限责任公司

- ECDN 暂不支持中国境外日志投递。

日志检索

日志检索支持多种类型的检索分析方式及图表分析形式，详细说明可见 日志检索。

以日志主题为单元进行日志检索。选择您需要检索的日志主题，单击**检索**，进入日志检索页面。

管理日志主题和日志集

您可于 CDN 控制台管理创建的日志主题，单击操作栏的：

- 管理：更新日志主题下绑定的域名列表
- 停止：停止日志投递到日志主题。停止后，所有绑定该日志主题域名的日志将不再继续投递至该主题，已经投递的日志将会继续保留。
- 启动：启动日志投递到日志主题。启动后，所有绑定该日志主题域名的日志将继续投递至该日志主题。
- 删除：删除日志主题。删除后，所有该日志主题下绑定域名的日志将不再继续投递至该日志主题，已经投递的日志将会被全部清空。

您可后续通过 日志服务（CLS）侧管理日志集等模块，如修改日志集名称。

实时日志字段说明

日志字段	原始日志类型	日志服务类型	说明
app_id	Integer	long	腾讯云账号 APPID
client_ip	String	text	客户端 IP
file_size	Integer	long	文件大小
hit	String	text	缓存 HIT / MISS，在 CDN 边缘节点命中、父节点命中均标记为 HIT

日志字段	原始日志类型	日志服务类型	说明
host	String	text	域名
http_code	Integer	long	HTTP 状态码
isp	String	text	运营商
method	String	text	HTTP Method
param	String	text	URL 携带的参数
proto	String	text	HTTP 协议标识
prov	String	text	运营商省份
referer	String	text	Referer 信息，HTTP 来源地址
request_range	String	text	Range 参数，请求范围
request_time	Integer	long	响应时间（毫秒），指节点从收到请求后响应所有回包再到客户端所花费的时间
remote_port	String	long	客户端与 CDN 节点建立连接的端口，若无则为 -

日志字段	原始日志类型	日志服务类型	说明
rsp_size	Integer	long	返回字节数
time	Integer	long	请求时间，UNIX 时间戳，单位为：秒。
ua	String	text	User-Agent 信息
url	String	text	请求路径
uuid	String	text	请求的唯一标识
version	Integer	long	CDN 实时日志版本

名词解释

日志集

日志集（Logset）是日志服务的项目管理单元，用于区分不同项目的日志，一个日志集对应一个项目或应用。CDN 日志集有以下基本属性信息：

- 地域：日志集所属 地域 。

> 说明：
> 目前支持上海，北京，成都，重庆，南京，广州和新加坡地域。我们正在计划支持更多地域，请关注产品动态。

- 日志集名称：日志集命名
- 日志保留时间：当前日志集里数据的保存时间周期
- 创建时间：日志集创建时间

日志主题

日志主题（Topic）是日志服务的基本管理单元，一个日志集可以包含多个日志主题。一个日志主题对应一类应用或服务，建议将不同机器上的同类日志收集到同一个日志主题中。例如，一个业务项目有三种日志：操作日志、应用程序日志、访问日志，每种类型可以创建一个日志主题。

日志服务系统以日志主题为单位，区分管理用户不同的日志数据，每个日志主题都可以配置不同的数据源、不同的索引规则和投递规则。因此，日志主题是日志服务配置、管理日志数据的基本单元，创建日志主题后需配置相关规则，才能如期有效地进行日志采集，并使用检索分析和投递等功能。

从场景功能上理解，日志主题主要提供：

- 采集日志到日志主题。
- 以日志主题为单元存储管理日志。
- 以日志主题为单元检索分析日志。
- 以日志主题为单元投递日志到其他平台。
- 从日志主题下载、消费日志。

> 说明：
> 以上信息摘自日志服务（CLS）产品文档，请以日志服务（CLS）侧的说明为准。

常见问题

为什么我在日志服务（CLS）控制台里的一些日志集和日志主题在 CDN 控制台看不到?

因为 CDN 控制台仅支持和展示以 CDN 服务角色创建的日志信息，即专属 CDN 的实时日志服务，其他日志集及日志主题不会同步过来。

为什么我的实时日志检索不到数据，出现了丢数据的情况?

可能是因为您的日志数据量较大，但日志主题是单分区或关闭了自动分裂。创建日志主题时，分区数量默认为1，默认开启自动分裂。
建议您按照自己的日志量预估所需的分区，前往 日志服务（CLS） 在日志主题的高级选项里面配置，详细可参考 主题分区。

我可以删除 CDN 的日志集吗?

可以，您需前往日志服务（CLS）控制台删除该日志集，删除前需先删除日志集下所有的日志主题。CDN 侧会同步此删除状态，若您后续有需要，可于 CDN 控制台重新创建日志集和日志主题。

插件中心

概述

最近更新时间：2022-03-02 15:18:21

插件中心为腾讯云 CDN 的增值插件功能的集中仓库，主要聚焦内容处理和内容安全方向的延伸功能，联动腾讯云其他服务为客户提供有价值的增值服务。部分插件属于收费功能，开通前请仔细阅读各插件功能帮助文档的费用说明模块。

版权所有：腾讯云计算（北京）有限责任公司

APK 动态打包

最近更新时间：2022-07-01 16:20:53

功能介绍

APK 动态打包插件功能识别终端用户请求 URL 中的特定参数，在 CDN 边缘将该参数携带的信息动态地写入 APK ，实现在 CDN 边缘对 APK 进行动态打包。APK 动态打包要求使用腾讯云 COS 作为源站。

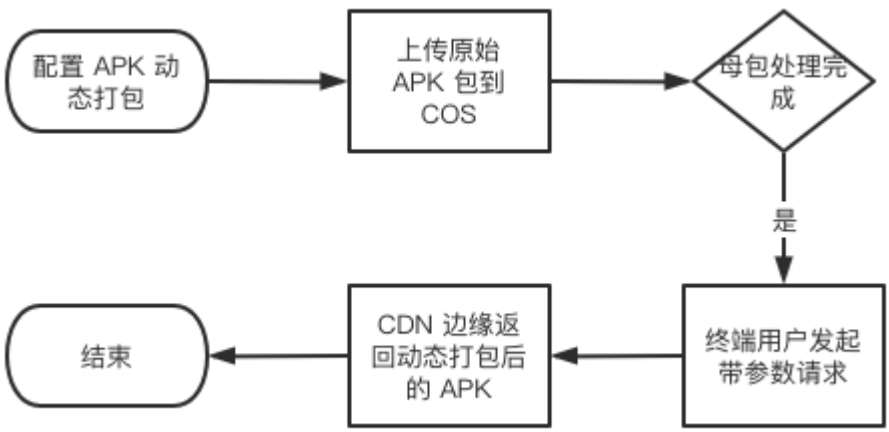
> 说明：
> 当前仅中国境内节点支持 APK 动态打包功能。

适用场景

- App 多渠道投放，如应用市场、网盟、搜索引擎、效果广告，但又不希望手工维护成千上百的渠道包。
- App 热启动，在 APK 包动态插入链接，实现 App 首次激活启动，自动跳转至指定页面。

使用流程

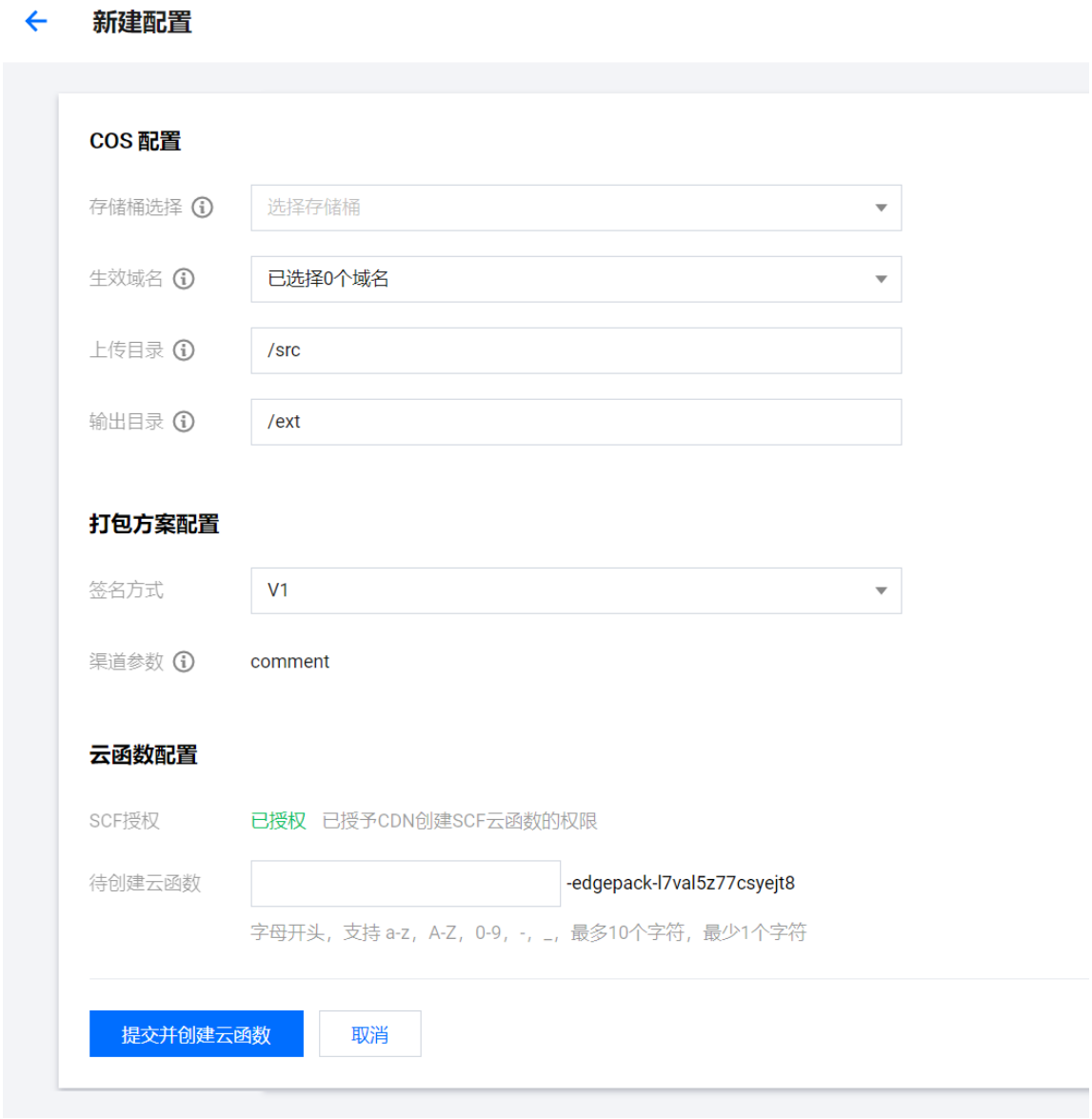
1. 登录 CDN 控制台在插件中心中，完成 APK 动态打包插件功能的相关配置。
2. 上传原始 APK 至 COS 源站指定上传目录。
3. 等待 CDN 节点将母包处理完成。
4. 终端用户发起带参数的请求。
5. CDN 边缘返回动态打包之后的 APK 文件。



配置指南

步骤一：新增动态打包配置

登录 CDN 控制台，在菜单栏里选择**插件中心**，单击 APK 动态打包插件功能卡片的开关按钮，开通 APK 动态打包，即可进入配置新增页面。功能开通之后，可以通过卡片底部的**基础配置**、**用量统计**进入相应的配置列表和用量查看页面。



- 存储桶选择：选择 COS 源站。本功能必须使用 **北京/上海/广州/成都** 的 COS 作为源站。
- 生效域名：系统将自动全选采用该 COS 作为源站的域名，该域名用于发布 APK 。可自行增删。
- 上传目录：设置原始 APK 在 COS 上的上传目录。配置完成后，需手动上传原始APK至该目录。
- 输出目录：设置 CDN 节点处理完母包之后的输出目录。上传原始 APK 后，系统会自动处理、生成同名母包，并将母包上传至该目录。**构造请求 URL 时，请将用户请求指向该目录**，而非上传目录。
- 签名方式：当前支持对采用 Android V1/V2 签名方式的 APK 进行动态打包，V2签名支持 WALLE/VASDOLLY 等开源多渠道打包方案。同时支持将注释信息写入指定的自定义 Block ID。
- 渠道参数：固定为 comment，不可修改。
- 云函数配置：授权之后，系统将根据配置自动生成云函数。

> **注意：**
> 请不要在 SCF 控制台删除该云函数！

步骤二：上传原始 APK

登录 COS 控制台 ，并上传原始 APK 到指定的上传目录

> **说明：**
> 原始 APK 大小不可超过10GB。

步骤三：等待母包处理完成

在 APK 动态打包功能页，单击**母包状态**查看 CDN 节点对母包的处理进展。

步骤四：发布动态打包 URL

母包处理完毕后，即可发布动态打包 URL。具体示例如下：

```
存储桶：example.cos.ap-chengdu.myqcloud.com
生效域名：www.example.com
上传目录：/src
输出目录：/ext
渠道参数：comment
渠道名称：pipeline
apk名称：test.apk
```

则对应发布的 URL 为： https://www.example.com/ext/test.apk?comment=pipeline 。

用户请求该 URL，即可获得 CDN 边缘写入 pipeline 渠道信息之后的 APK 包。

费用说明

- APK 动态打包为付费功能，按照请求数收费。采用小时结后付费、阶梯到达计费模式。阶梯价格如下：

请求阶梯 (万次请求)	阶梯价格（元/万次请求）
0 – 1 万次请求（不含）	10 元
1 – 5 万次请求（不含）	5元
5 – 20 万次请求（不含）	2元
20 万次请求以上	1元

- APK 采用 SCF 触发母包处理任务，SCF为收费服务，具体请见 云函数计费说明。

> 说明：
> 如需 APK 动态打包月结计费，请 联系我们。

定时刷新预热

最近更新时间：2022-07-01 16:21:07

定时刷新预热通过腾讯云 SCF 云函数，设置定时触发的刷新/预热任务。定时刷新预热任务被包括在每日刷新/预热的配额之内，执行当天如超过当日配额可能导致任务失败。

配置说明

登录 CDN 控制台，在菜单栏里选择【插件中心】，单击定时刷新预热插件功能卡片，开通定时刷新预热，即可进入任务配置页面。首次开通之后，也可以单击卡片底部的【基础配置】进入定时刷新预热的任务列表页面进行配置。

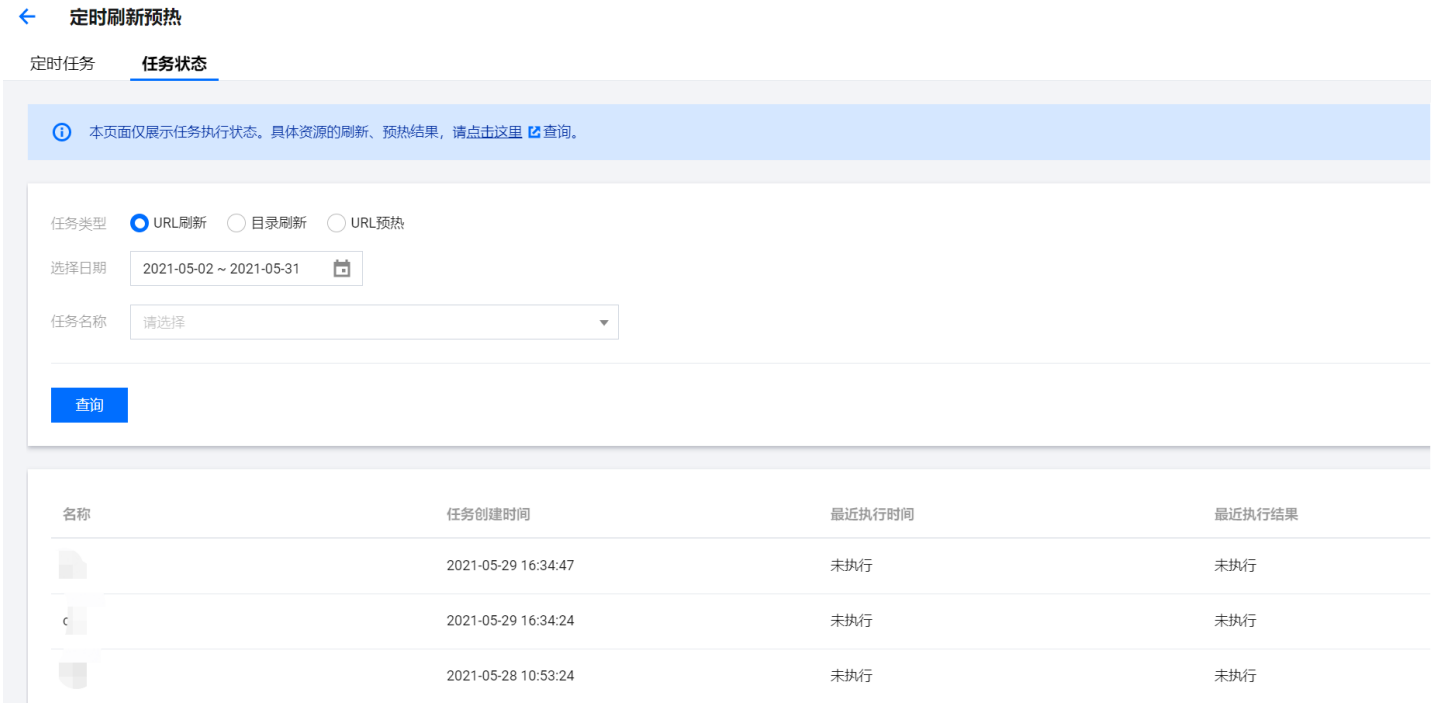
在新建定时任务界面，选择相应的任务类型、设置 Cron 定时表达式（见下文）、输入对应的刷新/预热 URL，并进行 SCF 授权，系统即可自动生成对应的 SCF 云函数，并按时触发对应的任务。

版权所有：腾讯云计算（北京）有限责任公司

注意：

请不要在 SCF 控制台删除该云函数！

在任务状态页面，可以查看定时任务最近一次的执行情况。



Cron 表达式

Cron 表达式一共包含7个位值，每个位值之间必须用空格隔开。

位数	字段	取值范围	通配符
第一位	秒	0 – 59的整数	, – * /
第二位	分钟	0 – 59的整数	, – * /
第三位	小时	0 – 23的整数	, – * /
第四位	日	1 – 31的整数（需要考虑月的天数）	, – * /
第五位	月	1 – 12的整数或 JAN,FEB,MAR,APR,MAY,JUN,JUL,AUG,SEP,OCT,NOV,DEC	, – * /
第六位	星期	0 – 6的整数或 SUN,MON,TUE,WED,THU,FRI,SAT。其中0指星期日，1指星期一，以此类推	, – * /
第七位	年	1970 – 2099的整数	, – * /

通配符的意义如下：

通配符	含义

通配符	含义
,（逗号）	代表取用逗号隔开的字符的并集。例如：在“小时”字段中 1,2,3 表示1点、2点和3点
-（破折号）	包含指定范围的所有值。例如：在“日”字段中，1 - 15包含指定月份的1号到15号
*（星号）	表示所有值。在“小时”字段中，* 表示每个小时
/（正斜杠）	指定增量。在“分钟”字段中，输入1/10以指定从第一分钟开始的每隔十分钟重复。例如，第11分钟、第21分钟和第31分钟，以此类推

> **注意：**
> 在 Cron 表达式中的“日”和“星期”字段同时指定值时，两者为“或”关系，即两者的条件分别均生效。

示例

一次性任务

- 33 22 11 6 7 * 2021 表示在 2021-7-6 11:22:33 触发任务
- 00 00 20 25 10 * 2021 表示在 2021-10-25 20:00:00 触发任务

周期性任务

- */5 * * * * * * 表示每5秒触发一次任务。
- 0 0 2 1 * * * 表示在每月的1日的凌晨2点触发任务。
- 0 15 10 * * MON-FRI * 表示在周一到周五每天上午10:15触发任务。
- 0 0 10,14,16 * * * * 表示在每天上午10点，下午2点，4点触发任务。
- 0 */30 9-17 * * * * 表示在每天上午9点到下午5点每半小时触发任务。
- 0 0 12 * * WED * 表示在每个星期三中午12点触发任务。

费用说明

定时刷新预热功能本身免费，但是会调用 SCF 创建定时任务，SCF为收费服务，具体请见 云函数计费说明 。

区域访问控制

最近更新时间：2022-07-01 15:11:22

区域访问控制通过 Client IP 识别终端用户所在地，允许客户针对全部内容或者指定目录，设置各区域终端用户的访问权限，腾讯云定期更新全球各地区的 IPv4 数据库，少部分未在数据库内的 IP 终端无法进行识别。

配置说明

登录 CDN 控制台，在菜单栏里选择**插件中心**，找到区域访问控制功能卡片并单击开通。首次开通之后，单击卡片底部的**前往查看**进入区域访问控制配置列表页。

单击**新增规则**，即可针对全部内容/指定目录设置区域访问控制黑/白名单。终端用户所在区域支持多选。

规则类型	描述

规则类型	描述
白名单	已选择的地区允许访问，其他地区拒绝访问
黑名单	已选择的地区拒绝访问，其他地区允许访问

说明：

- 单个域名最多可配置 20 条区域访问控制的规则。
- 已开启 IPv6 访问的域名暂不支持开启区域访问控制插件。
- 同一个域名的同一个目录（或者全部内容），仅能设置一次白名单。
- 单一域名建议配置一种规则类型（黑/白名单），避免理解过于复杂的生效条件。

费用说明

1. 区域访问控制在内测期间暂不收取费用。
2. 服务未覆盖地区或业务高峰时段，可访问地区的客户端请求可能会路由至其他可服务的大区，期间可能会产生其他区域的计费流量，详情见 计费说明。
3. 对于拒绝访问的终端请求，返回403时包含极小的请求数据，会产生微量的流量。

版权所有：腾讯云计算（北京）有限责任公司

性能监测

最近更新时间：2022-03-30 16:52:14

功能介绍

性能监测是一站式前端监控解决方案，专注于 Web，小程序等前端场景监控。用户只需要安装 SDK 到自己的项目中，通过简单配置化，即可实现对用户页面质量的全方位守护。真正做到了低成本使用和无侵入的监控，实现页面性能和前端质量的实时可观测。

适用场景

- **页面性能分析**：包括首屏耗时、建立 TCP 连接耗时、TTFB 耗时、SSL 耗时等。同时还支持最新的 Web Vitals（谷歌针对网页加载速度和体验所提出的一套指标）标准。全方位协助您优化用户体验。
- **页面异常分析**：包括页面卡顿、页面崩溃、操作后无反应、页面无法操作等，协助您快速定位异常。
- **页面日志查询**：支持检索用户日志，还原异常发生现场，获取足够的信息来定位问题。
- **用户访问分析**：支持查看业务 PV/UV 数据，每个页面访问的 TOP 数据等，支持通过网络、浏览器、地区等多维度分析用户访问数据。
- **API 监控**：通过嵌入 SDK，自主上报前端请求的 API，前端性能监控将会统计 API 请求耗时、HTTP Code 成功率等 API 关键指标，方便您快速定位 API 异常。
- **静态资源优化**：包括 JS 、CSS 和图片等加载时长，您可以静态资源监控定位问题根因，对静态资源加载进行优化，提升用户体验。
- **自定义信息上报**：若 SDK 主动上报的数据不能满足您的需求，您还可以自定义上报日志、事件、资源测速等。

配置流程

1. 登录 CDN 控制台在插件中心，开通性能监测服务。
2. 选择接入方式并在接入应用。
3. 通过汇总分析、页面分析等分析页面性能和前端质量。
4. 您还可以针对关键指标配置告警，在指标异常时第一时间通知您采取措施。

配置指南

步骤一 开通性能监测服务

1. 登录 CDN 控制台在插件中心。

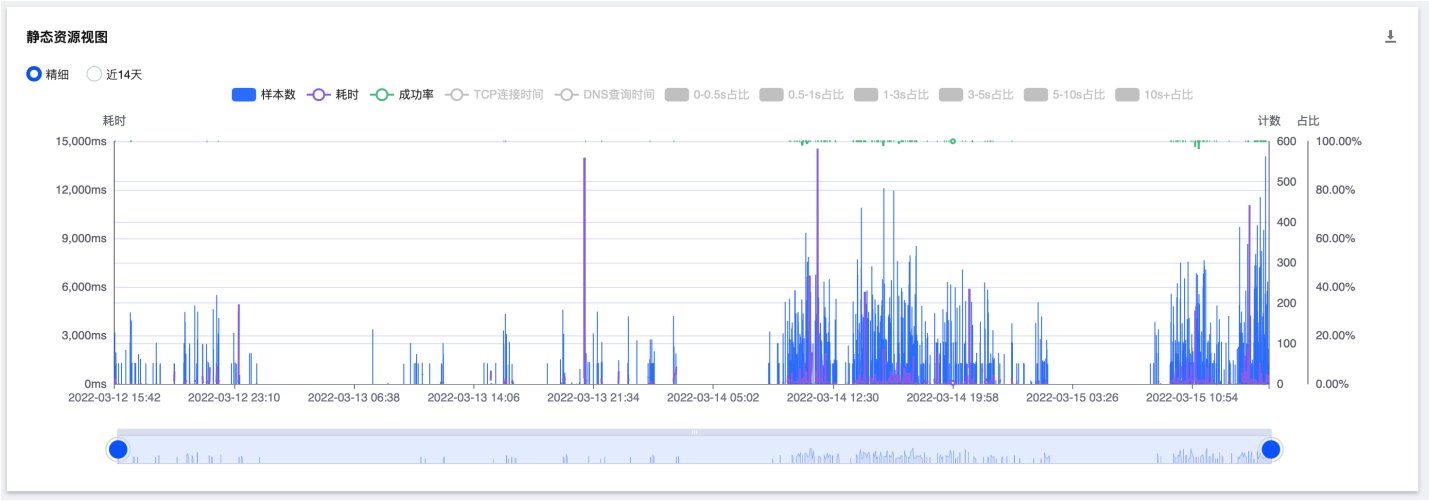
2. 找到性能监测功能卡片，点击性能监测右侧的开启按钮，确认开通性能监测服务。

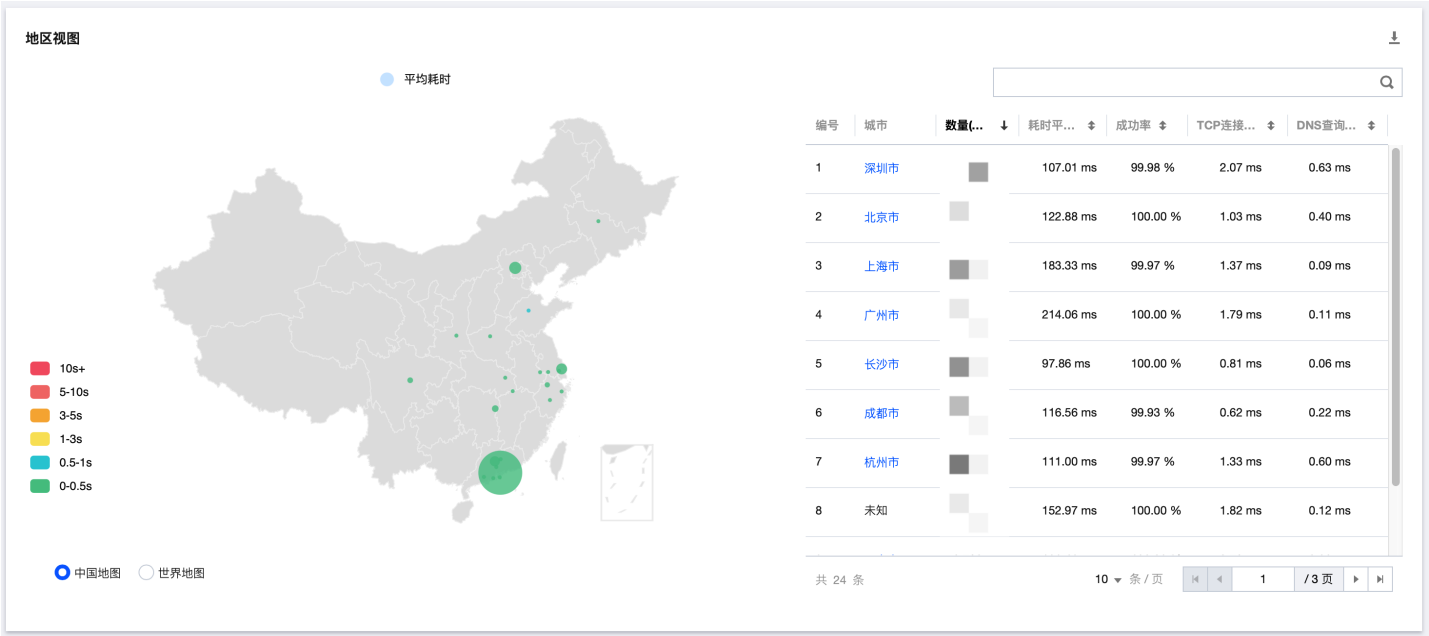
步骤二 接入应用

成功开通性能监测服务后，将会跳转到应用列表，单击新建应用接入。根据页面提示选择需要接入的域名，并根据页面提示接入性能监测 SDK。

步骤三 分析性能

成功接入应用性能 SDK 后，等待数分钟，您即可在性能监测功能卡片中点击汇总分析，查看静态资源汇总情况。切换上方的菜单为“页面分析”，您还可以查看单个页面的静态资源加载情况。





步骤四 配置告警

在性能观测管理页面，切换上方菜单栏为“告警配置”，并参考 新建告警策略文档。

费用说明

性能监测每应用每天50万免费上报数据量额度，对超过50万上报次数的部分进行计费，计费价格为：0.34/万次。详情请参考 前端性能监控–计费说明

CDN 测速

最近更新时间：2022-05-05 11:42:12

功能介绍

CDN 测速是借助腾讯云云拨测（CAT）设置定时任务从分布全球的真实终端节点访问目标资源，通过模拟真实用户访问体验，实现针对 CDN 性能的测试与监控。零代码、无侵入即可实现对于全地域 CDN 资源下载准确性、质量以及稳定性的持续监控。

适用场景

CDN 性能预验证

CDN 选型或迁移前，不修改现网前提下，快速预验证接入 CDN 后，国内外全地域/指定地域的性能情况，并针对性的制定 CDN 优化、迁移方案及策略。

CDN 性能监测

周期性拨测及告警，针对源站/CDN 不可用造成的可用性问题进行监控。同时端到端详细分阶段耗时（DNS 解析、TCP 建联、 CDN 服务器响应、首包到达、文件加载完毕）帮助持续监控 CDN 服务性能。

资源更新验证

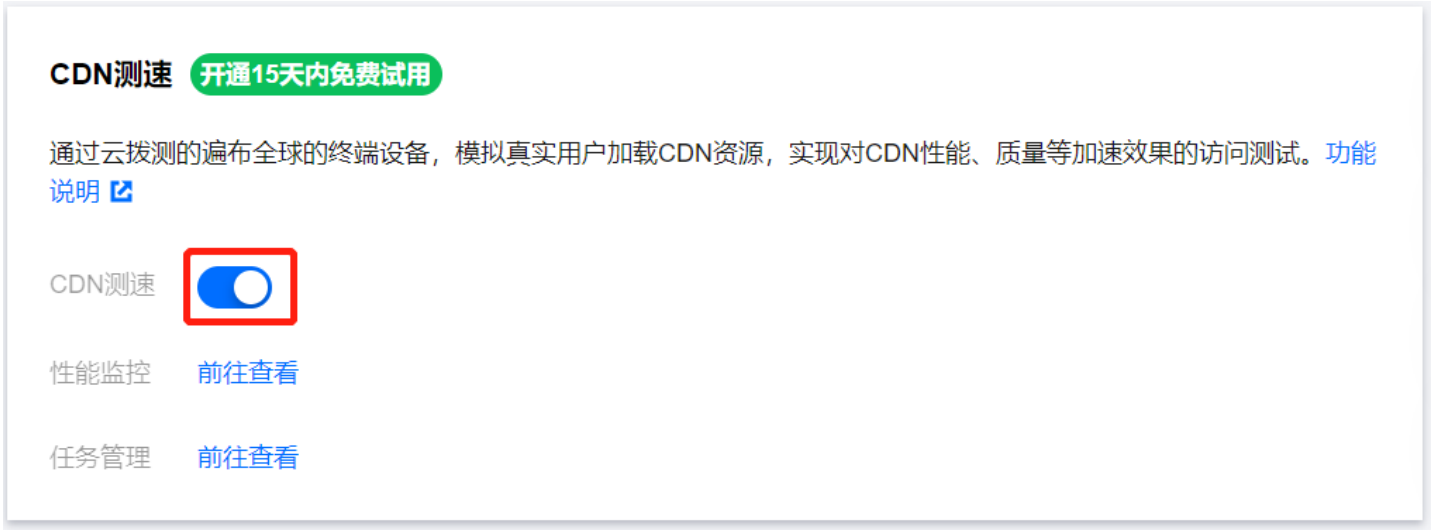
CDN 资源更新后，通过主动拨测并比对资源 MD5 结果，确认各个接入点的缓存资源及时更新，避免因资源更新失败，影响用户体验，造成业务损失。

网络故障、点播直播体验监控、页面性能分析等更多场景及最佳实践，请参考 云拨测 – 操作指南 。

配置说明

步骤一 开通 CDN 测速服务

登录 CDN 控制台。找到 CDN 测速功能卡片，首次开通需要创建服务预设角色并授予内容分发网络相关权限，授权成功后单击 CDN 测速右侧的开启按钮。

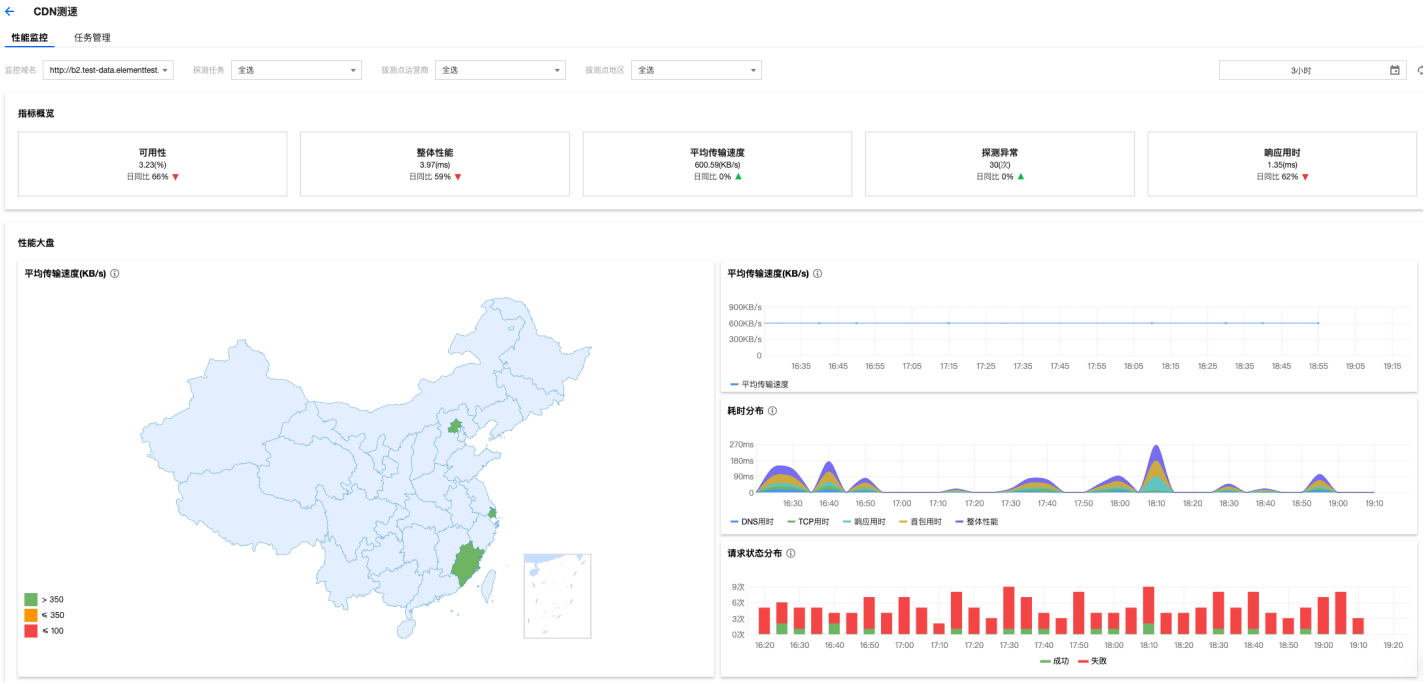


步骤二 创建监测任务

1. 进入任务列表页面，单击新建任务按钮。
2. 可在拨测地址中选择需要模拟访问的 URL（最多支持同时监控5个拨测地址），选择期望模拟客户端发起请求的对应区域运营商的拨测点，模拟真实用户访问，开启拨测任务。

步骤三 多维性能分析

创建任务10 – 20分钟后，拨测数据会从遍布全球各地的拨测点回传，您即可在性能大盘中，看到对应资源的各项核心指标。页面中部，您可以针对特定指标，特定的线路进行分析，查看不同地域、运营商、具体线路的性能差异。



步骤四 详情分析及故障排查

单击单次任务，您可以查看更为丰富的详细数据指标，包含各阶段耗时、网络层跃点路径， 文件 MD5 码等完整的任务日志。针对元素下载或网络问题，您可以针对性的创建页面性能或网络质量任务，获得更为详细的指标数据。

费用说明

云拨测为所有用户提供15天免费试用，试用期到期后，任务会自动暂停，您可按需开通按量后付费或购买预付费资源包后继续使用。试用期使用限制及价格详情，请参考 云拨测 – 计费概述。

SaaS 证书

最近更新时间：2022-06-08 14:38:27

功能介绍

CDN SaaS 证书功能提供域名证书的全生命周期管理服务，包括 ssl/tls 证书的批量申请、绑定、证书过期自动更新等服务，对于已接入腾讯云 CDN 的域名，支持通过控制台、API 的方式进行一键申请使用，助力网站建站等 SaaS 服务提供商降低运维成本，提供安全的域名访问。

适用场景

1. 域名证书批量申请、绑定

用户加速域名具有 HTTPS 访问诉求时，需要为该域名申请绑定 ssl 证书，此时需要完成证书申请（提交资料-验证域名-等待机构签发证书）、绑定域名等操作。面对10w+级别的域名接入时（集中在泛互出海建站用户），此时使用传统的证书、申请步骤批量操作域名流程繁琐、用时较长。

2. 域名证书批量自动续签，代维

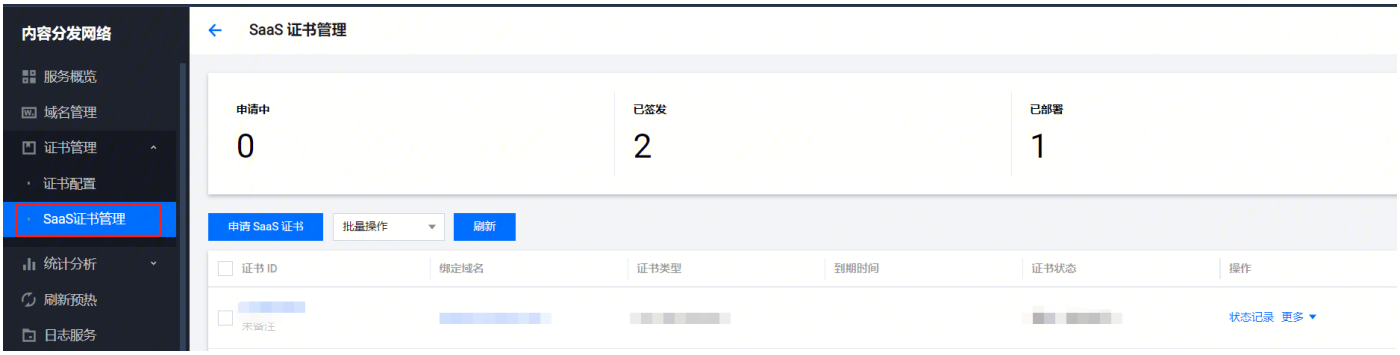
使用传统托管证书、证书存在有效期，过期后，可能会造成访问异常，需要为域名重新申请并绑定证书，若需要管理大量的域名，此时运维难度较大巨大，通过 SaaS 证书功能， 会实时检测证书过期时间，并自动完成续签和部署的动作。

使用流程

步骤一：开通插件中心-SAAS 证书功能

1. 登录 CDN 控制台，在菜单栏里选择**插件中心**，单击 **SaaS 证书**插件功能卡片的开关按钮。

2. 开通 SaaS 证书功能，功能开通之后，可通过证书管理–SaaS 证书管理进入配置页面。



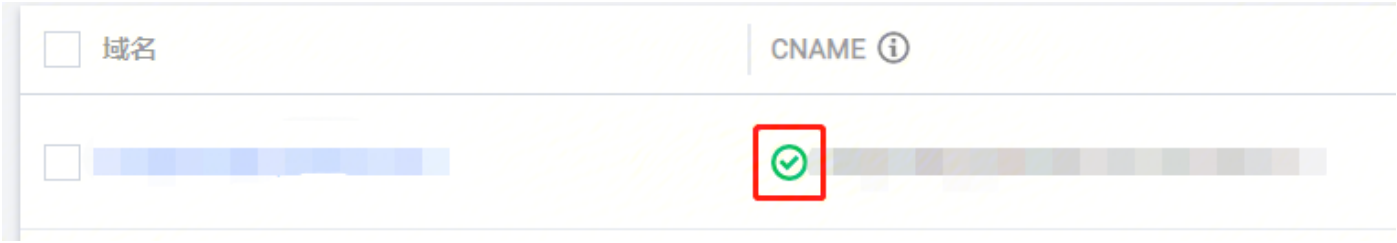
步骤二：为需要绑定证书的域名申请证书

1. 选择您要绑定证书的域名，可单选或者多选

2. 选择证书算法
   - 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。
3. 自动进行域名验证

   SaaS 证书通过 HTTP 验证的方式进行域名归属验证，请您签发证书前，先确保域名 CNAME 解析正常，否则

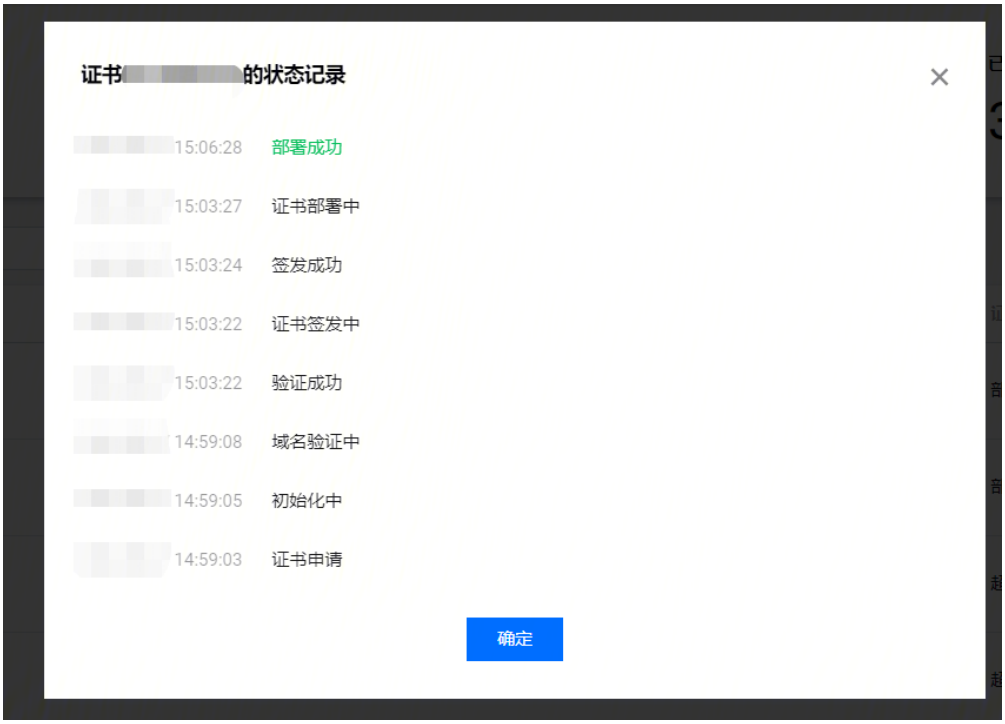
可能导致证书签发失败。



4. 单击**确认**，进入 SaaS 证书管理页面

步骤三：等待证书签发、部署

证书签发部署过程约5 – 10分钟，您可通过状态记录查看进度



费用说明

SAAS证书 在内测期间暂不收取费用。

安全加速

最近更新时间：2021-10-14 17:16:32

安全加速（Secure Content Delivery Network，SCDN），在为用户业务提供快速稳定的内容分发服务的基础上，提供全面的网络攻击防护能力。已接入并开启腾讯云 内容分发网络（Content Delivery Network，CDN）或 全站加速网络（Enterprise Content Delivery Network，ECDN）服务的域名，可一键开启 SCDN 安全加速，对 DDoS 攻击、CC 攻击、Web 攻击、BOT 爬虫等网络攻击类型进行全方位防护，为业务安全保驾护航。

> 说明：
> 更多安全加速相关介绍可前往 安全加速 SCDN 产品文档产查阅。

服务查询
全网状态监控

最近更新时间：2021-11-05 10:33:09

功能介绍

内容分发网络（CDN）可实时监控中国境内各省份运营商和中国境外各地区的时延与可用性状态。CDN 根据遍布全球的探测点，不断向监测文件发起请求，并收集这些请求的响应数据。您可以在 CDN 控制台查看全网实时状态概览及详情。

> 说明：
> 全网状态监控为全平台的服务状态监控，非客户真实服务状态。

操作指南

登录 CDN 控制台，单击左侧目录的【全网状态监控】，即可进入全网状态监控页面。

全网实时状态概览

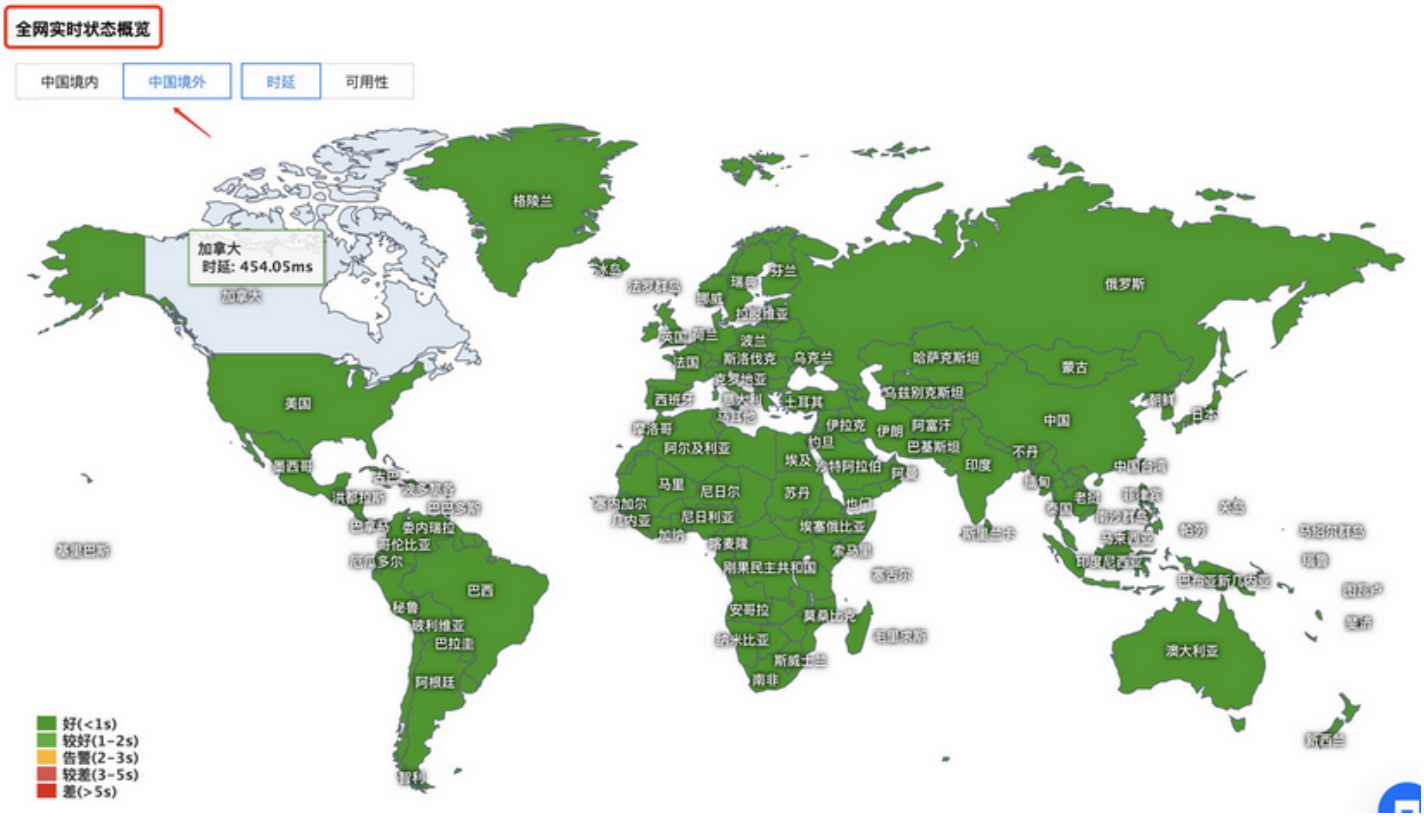
您可以在**全网实时状态概览**查看中国境内各省份运营商和中国境外各地区的时延与可用性状态概览。鼠标悬浮在地图中各区域时会显示对应区域的数据。

> 注意：
> 图中实时数据刷新时间为1分钟。

1.中国境内

> **注意：**
>
> 图中展示了三大运营商数据，包括移动、联通、电信。计算平均时延或可用性时，包含了中小型运营商的数据。

2.中国境外



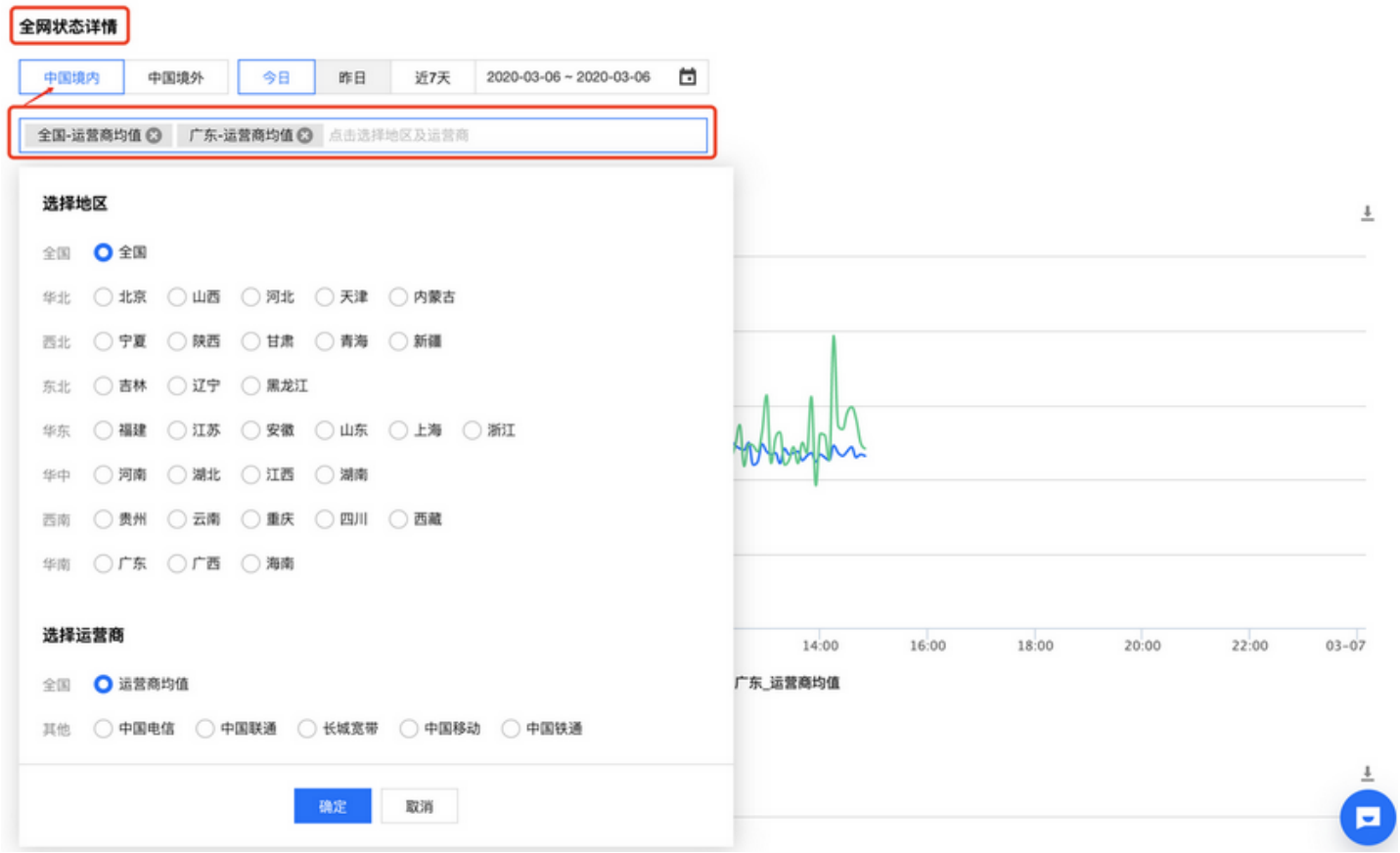
全网状态详情

您可以在**全网状态详情**中查看中国境内指定时间区间、地区和运营商，中国境外指定时间区间和地区的历史时延及可用性曲线。

> ⚠ **注意：**
>
> 时间区间：支持最近30天访问情况统计查询，查询跨度最大为30天。

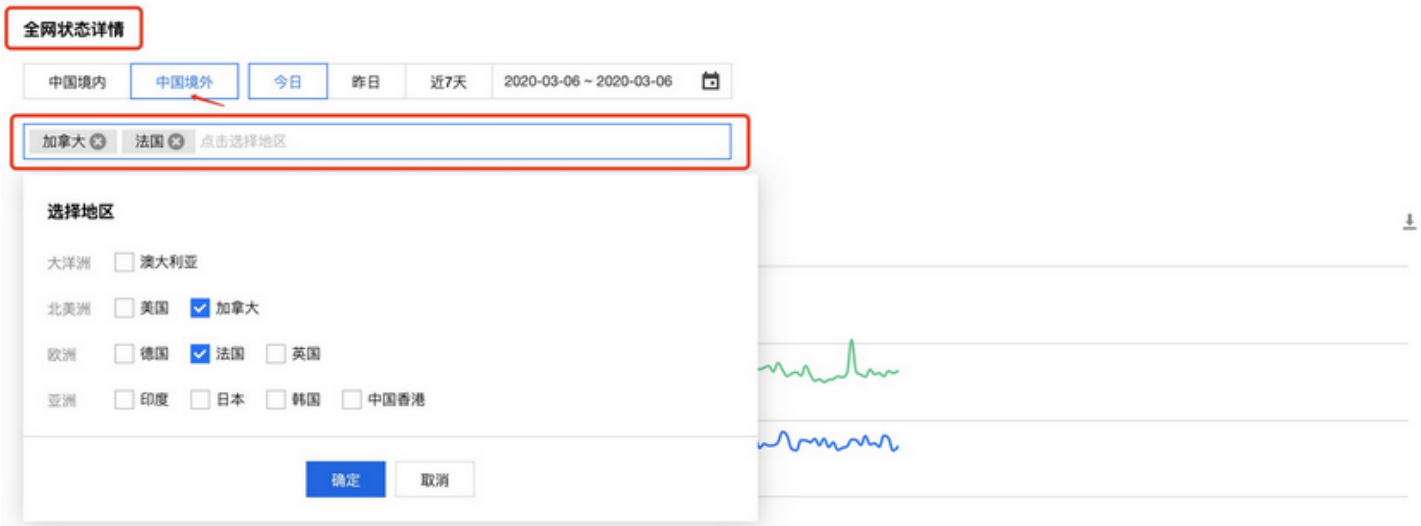
1.中国境内

您可同时添加多个查询条件，查看多条曲线。



2.中国境外

您可同时选择多个地区，查看多条曲线。



流量包管理

最近更新时间：2022-04-13 10:27:20

配置场景

若您的计费模式为**流量计费**，使用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，实时了解流量包的剩余状态，及时补充。

同时,腾讯云 CDN 支持对流量包进行余额告警配置、流量包自动续订配置、未使用的流量包自助退费等功能。

> ⚠ 注意：
> ECDN 暂不支持预付费流量包。

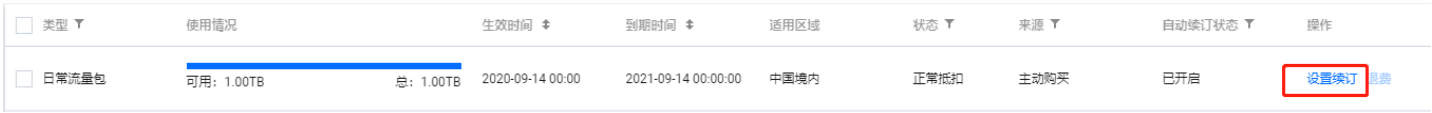
配置指南

查看配置

登录 CDN 控制台，选择左侧目录的【流量包管理】可查看账号下流量包余额、自动续订状态、告警配置和流量包自助退费等功能。

自动续订

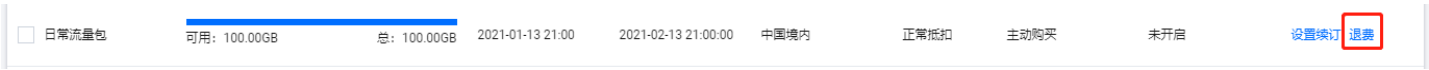
选择对应的流量包点击【设置续订】，即可在弹窗中根据自身需求开启或关闭自动续订功能，自动续订开启后，系统将于原流量包到期次日按照原规格续订。



> ⚠ 注意：
>
> - 续订的流量包有效期与原流量包保持一致。
> - 10G, 50G 的日常流量包无法设置自动续订。
> - 请保证腾讯云账号余额充足，扣费失败将会导致自动续订功能失效。
> - 流量包未到期但用量耗尽，不会立刻自动续订新的流量包，系统仍将于原流量包到期次日按照原规格续订。
> - 取消自动续订需在到期日前一天23：59：59前取消，取消操作不会产生任何额外费用，否则系统将照常续订。

自助退费

在需要操作的流量包处点击【退费】即可，详情请参见 退费说明。



> ⚠ 注意：
>
> - 仅支持来源为主动购买或者自动续订，同时状态为未过期且未使用的流量包退费。
> - 如出现疑似异常或恶意退款，腾讯云 CDN 有权拒绝您的退款申请。
> - 抵扣或代金券不予以退还，退还金额将全部原路退回到您的腾讯云账户。

自定义流量包告警阈值

在【流量包告警设置】处点击【编辑】即可，系统默认值为5%，15%，30%。您可以通过此功能自定义设置3个百分比提醒阈值，系统可以分别在流量包剩余到达设定的阈值时，向您发送给提醒消息。

> ⚠ 注意：
>
> - 当前仅支持1%，2%，3%，4%以及5%的正整数倍数且不大于50%的比例。
> - 默认三个阈值档位，支持根据需要添加或删除告警阈值
> - 告警消息发送存在延时，若在短时间内产生较大的流量，横跨数个告警档位，则 CDN 仅会发送一条最接近最低阈值的告警信息。

IP 归属查询

最近更新时间：2021-06-25 13:12:45

功能介绍

内容分发网络（CDN）为您提供了 IP 归属查询工具，您可以通过此工具查询指定的 IP 是否为腾讯云 CDN 全球加速节点，以及 IP 所在加速服务区域、省份及运营商信息。

适用场景

在排障类场景可使用此工具协助排查，当用户访问出现异常时，将客户端请求实际访问的 IP 在此处进行查询：

- 若不归属于腾讯云 CDN，则域名解析配置可能出现异常，前往域名解析服务商处查看 CNAME 是否配置正常；
- 若归属于腾讯云 CDN，可通过查看节点服务状态，是否出现节点上下线导致请求中断。

操作指南

查询方式

登录 CDN 控制台，选择左侧目录的【 节点查询 】，进入功能页。

IP 归属查询

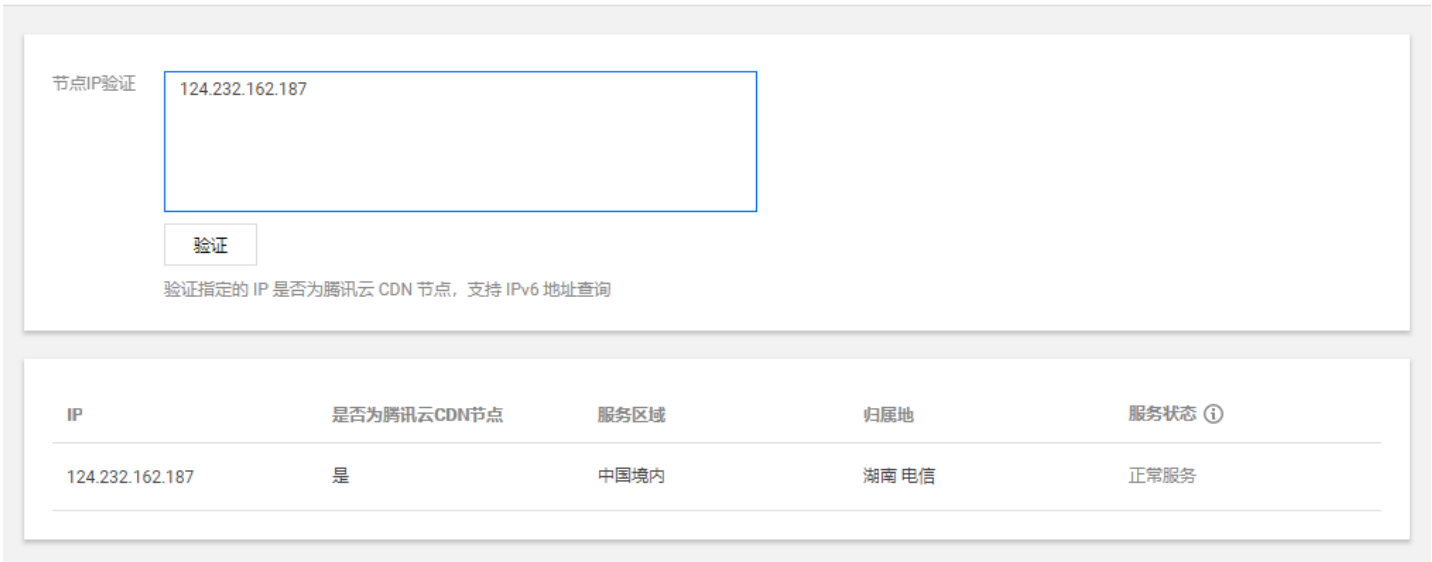
使用约束

- 在文本框中输入多条需要验证的 IP 地址，一行一个。
- 最多可一次性验证20个 IP。
- 支持 IPv4、IPv6 地址验证。
- 支持全球范围内加速节点验证，中国境内节点会返回所在省份运营商数据，中国境外节点会返回所在国家数据。
- 支持查看节点**近三个小时**服务状态变更，若存在上下线变动，可查看出对应的操作时间。

使用案例

IP 归属于中国境内

IP 归属查询



IP 归属于中国境外

IP 归属查询

IPv6 归属查询

IP 归属查询

节点IP验证

2409:8c3c:1300:f:25::

验证

验证指定的 IP 是否为腾讯云 CDN 节点，支持 IPv6 地址查询

IP	是否为腾讯云CDN节点	服务区域	归属地	服务状态
2409:8c3c:1300:f:25::	是	中国境内	山东 移动	正常服务

回源节点查询

最近更新时间：2022-06-20 10:10:45

功能介绍

腾讯云 CDN 支持查询加速域名的回源节点 IP，支持 IP 段和 IP 地址两种类型。

适用场景

业务访问控制需要。

操作指南

登录 CDN 控制台，选择左侧菜单目录**服务查询** > **回源节点查询**。

使用说明：

- 请正确输入已接入 CDN 且已启动的加速域名。
- 查询区域请选择加速域名对应的加速区域。
- 请根据业务需要选择对应的查询类型。
- 中国境外暂不支持运营商信息。
- 查询结果支持下载至本地。

版权所有：腾讯云计算（北京）有限责任公司

自助诊断工具

最近更新时间：2021-06-07 10:06:39

CDN 为您提供了自助诊断工具，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，并为您提供解决建议。

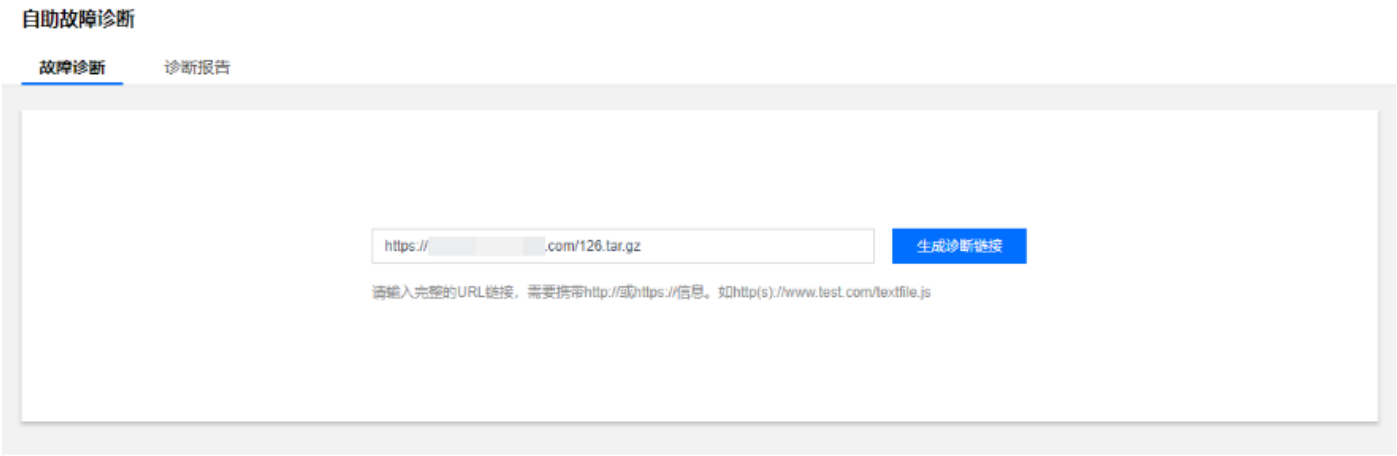
> **注意：**
> 诊断的资源 URL 需要是您的账号下接入的状态为**已启动**的域名。诊断中产生的带宽将计入计费带宽，我们建议您诊断的目标资源不超过200MBytes。

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，选择【诊断工具】>【自助诊断工具】。
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。

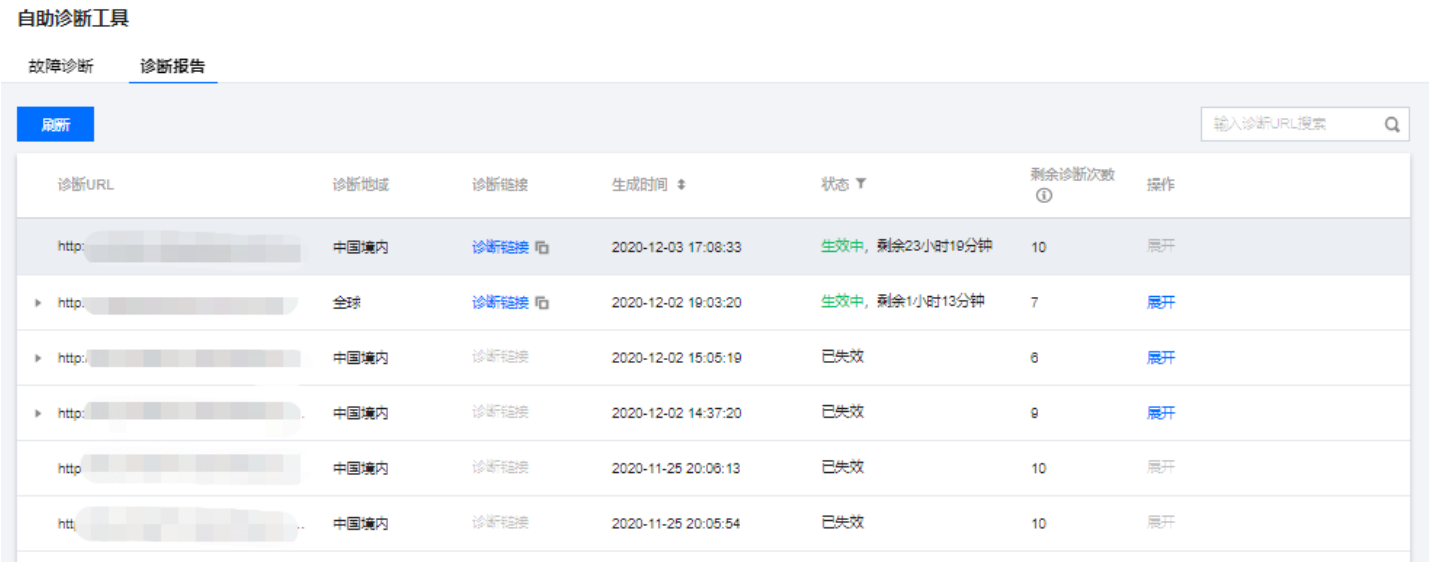
> ⚠ 注意：
>
> - 每一条 URL 生成的诊断链接有效时间为24小时，最多可以单击10次故障诊断。
> - 可以在"诊断报告"页面重新复制已经生成的可用诊断链接。

诊断报告

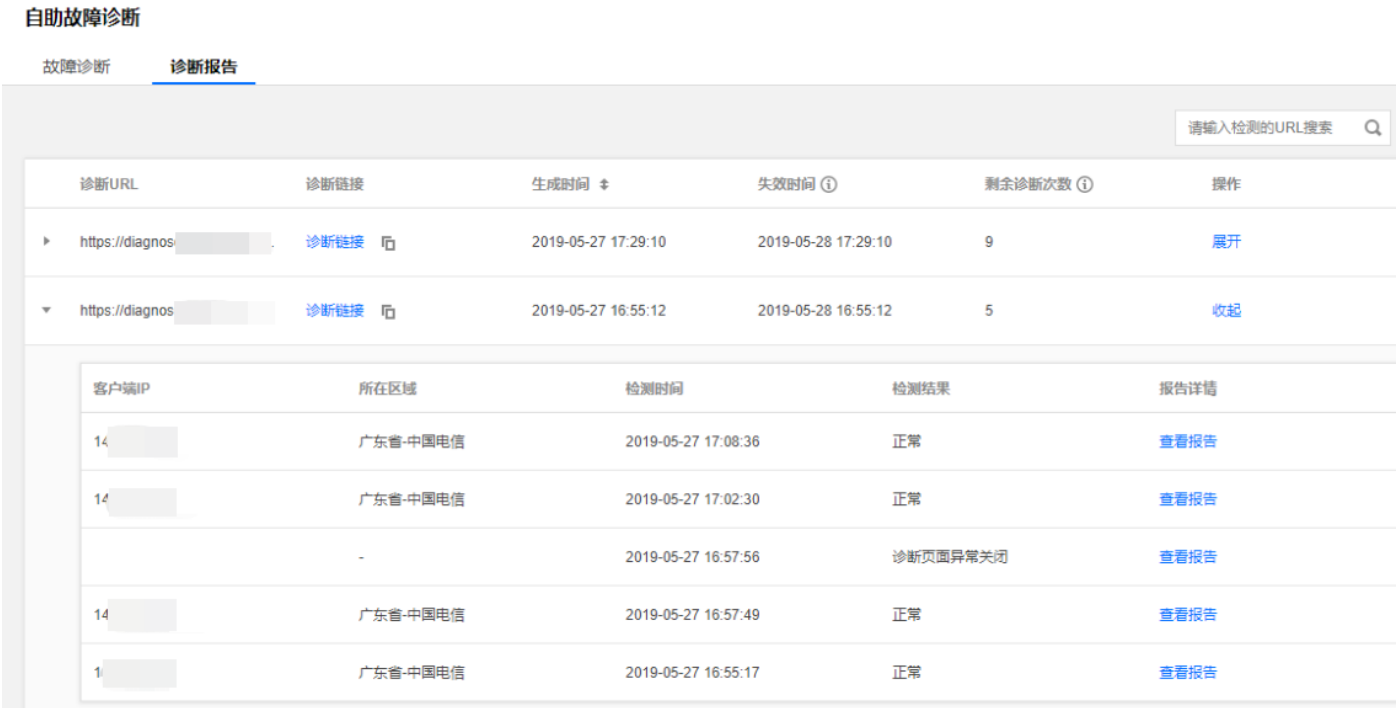
报告查看

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 对应的诊断地域。
- URL 对应的诊断链接。
- 诊断链接的生成时间。
- 诊断链接的生效状态。
- 诊断链接可用诊断次数。



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。



3. 根据每一个步骤的检测，诊断报告会整体判定为：

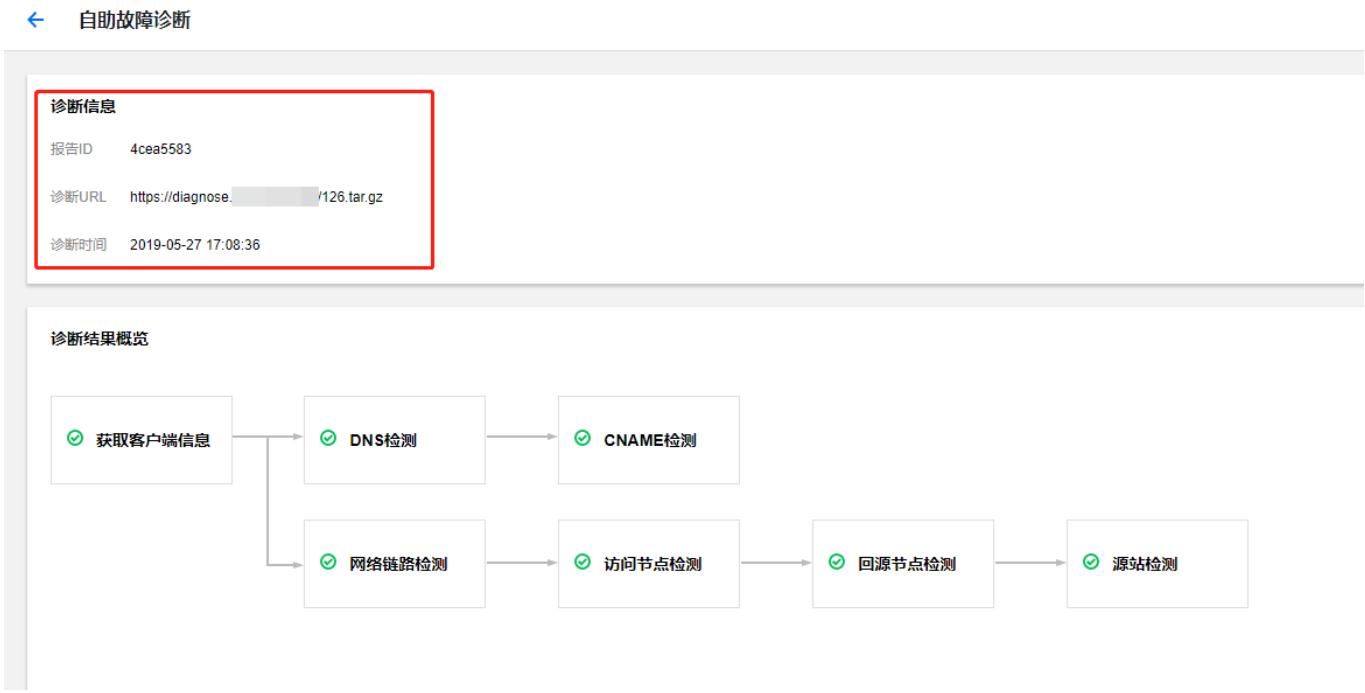
- 正常。
- 异常。

- 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。

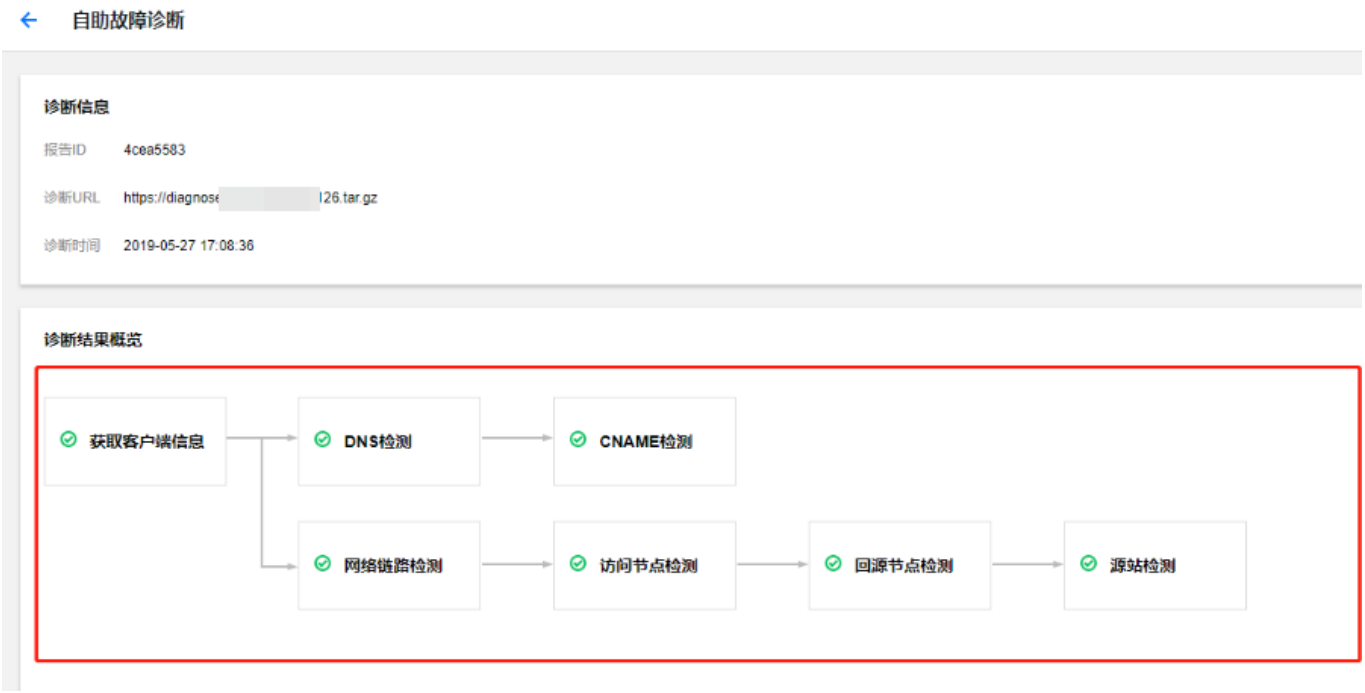
报告解读

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，可以直观的发现异常模块，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。

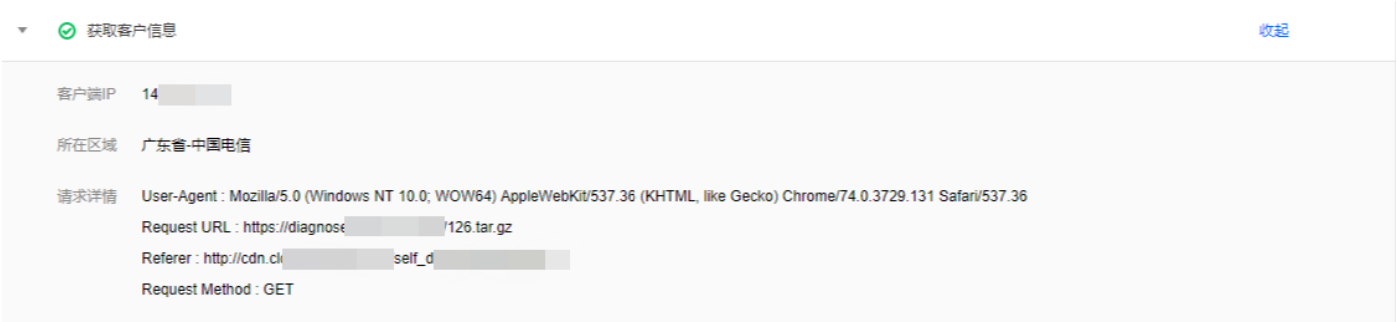
- 源站检测结果。



3. 报告的第三部分针对诊断结果进行了详细说明：

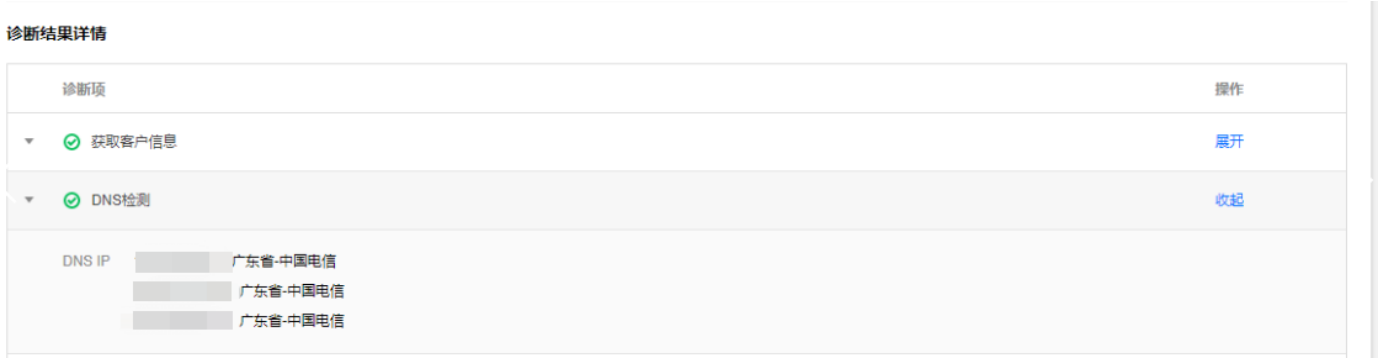
第一项：客户端信息

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 Method 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。



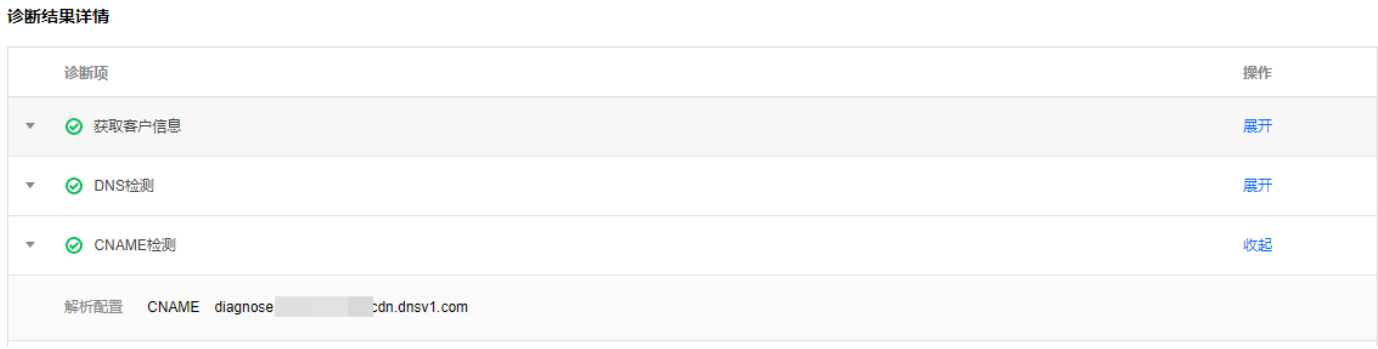
第二项：DNS 检测

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。



第三项：CNAME 检测

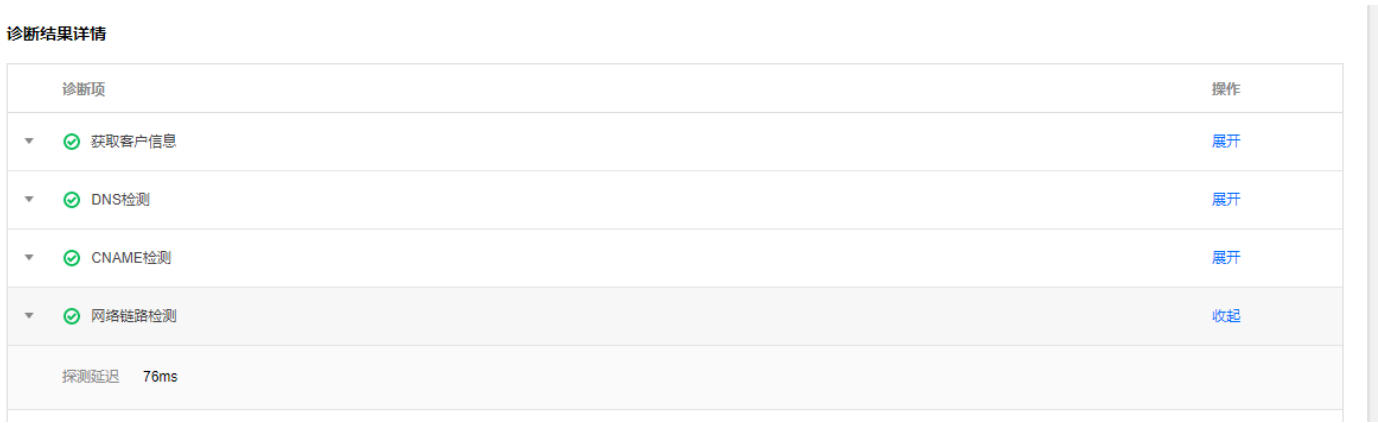
获取检测域名 CNAME 配置，域名的 CNAME 解析需要配置为正确的 *.cdn.dnsv1.com（默认）后缀域名，否则请求将无法到达 CDN 节点。



> **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

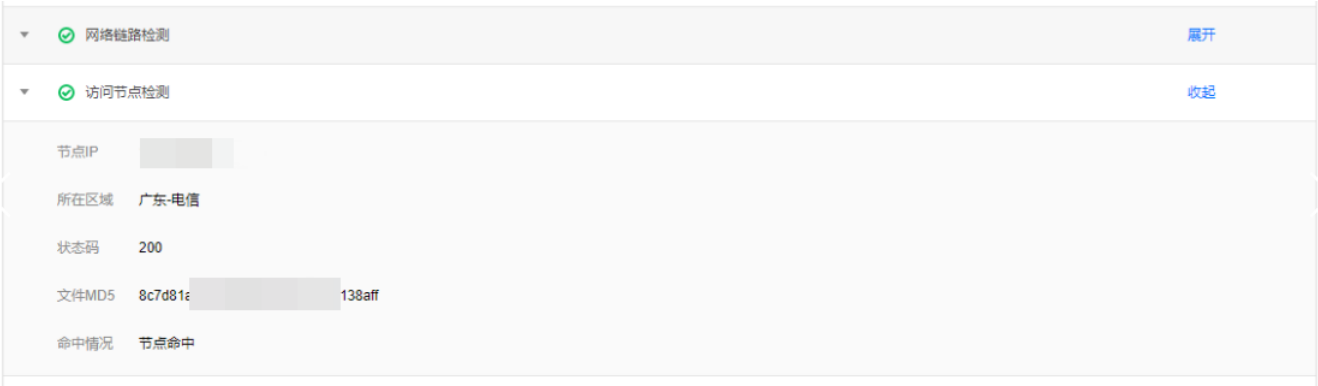
通过客户端本地探测多个互联网站点，获取客户端网络状态。若由于本地代理等配置导致站点无法访问，会导致网络链路检测失败，无法进行后续检测。



第五项：访问节点探测

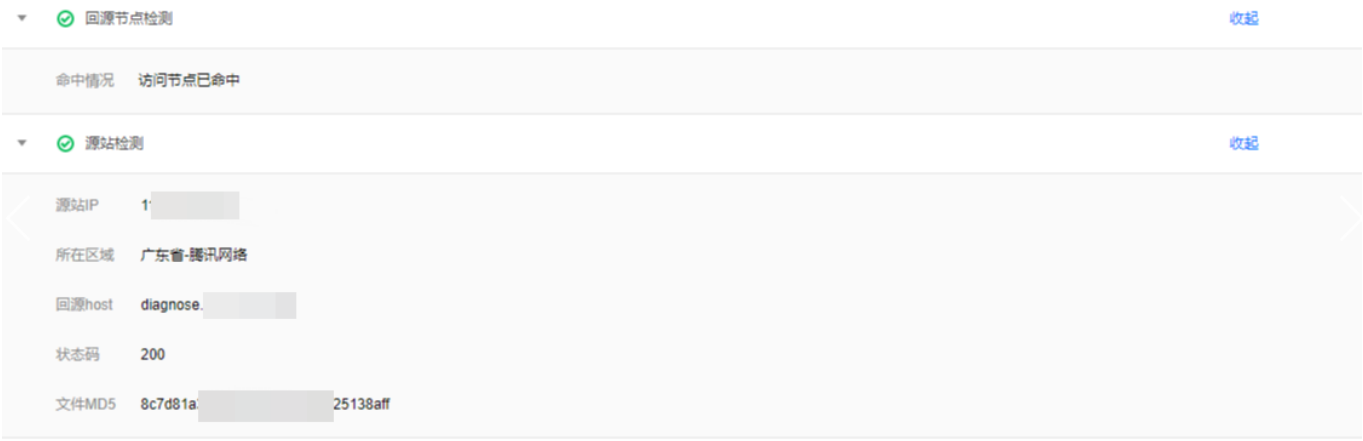
客户端发起请求后，到达的 CDN 节点信息采集，包含节点 IP、节点省份/运营商、以及节点返回的状态码、命中状态及资源 MD5：

- 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**。

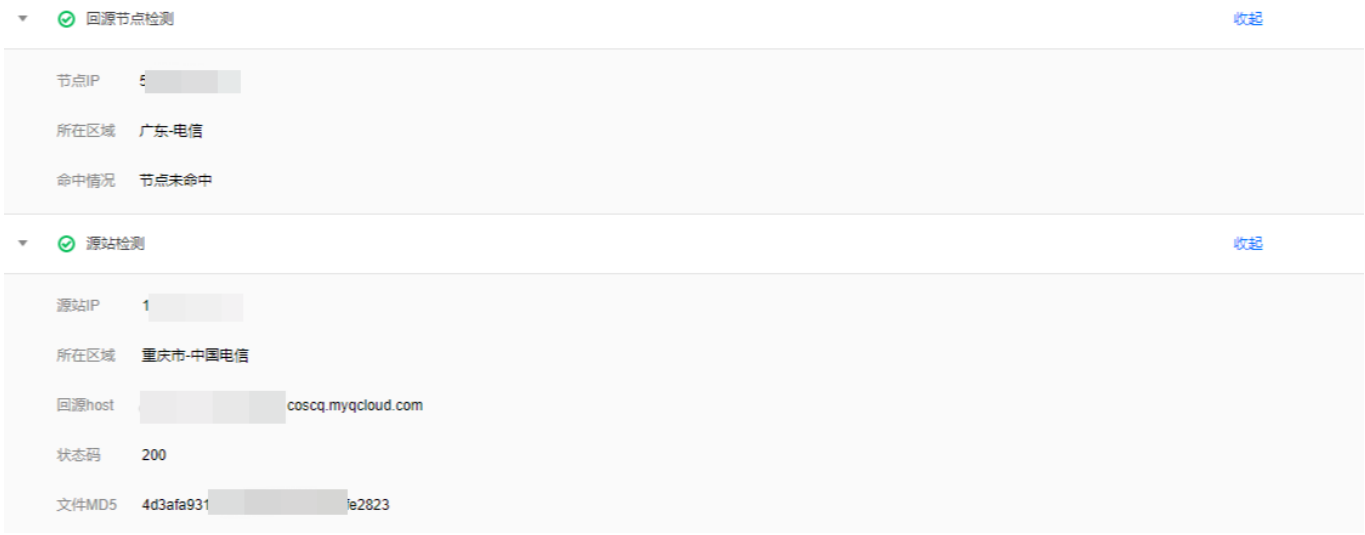


第六项：回源节点检测

i. 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。



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：



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。

内容合规

最近更新时间：2021-11-05 10:28:53

功能介绍

腾讯云 CDN 加速内容需要符合相关法律法规要求，若您在公网分发的内容存在违规，腾讯云合规团队将对其进行处置。内容合规功能，将会对被合规团队处置的违规内容及处置时间，同步展示在控制台，供您查看与确认。

> **说明：**
> 为了更好地提升业务合规性，推荐您使用腾讯云 T-Sec 天御内容安全产品，进一步加强 CDN 内容安全管理。

查看配置

登录 CDN 控制台，在侧菜单中选择【诊断工具】>【内容合规】，进入内容合规页面。

配额管理

最近更新时间：2022-06-21 15:57:30

功能介绍

内容分发网络（CDN）配额详情可以查看 CDN 相关配额上限和使用情况，并可以根据业务需求提前申请提升临时配额或永久配额。当前已支持配额：URL 刷新配额、目录刷新配额、URL 预热配额、CDN 域名上限。

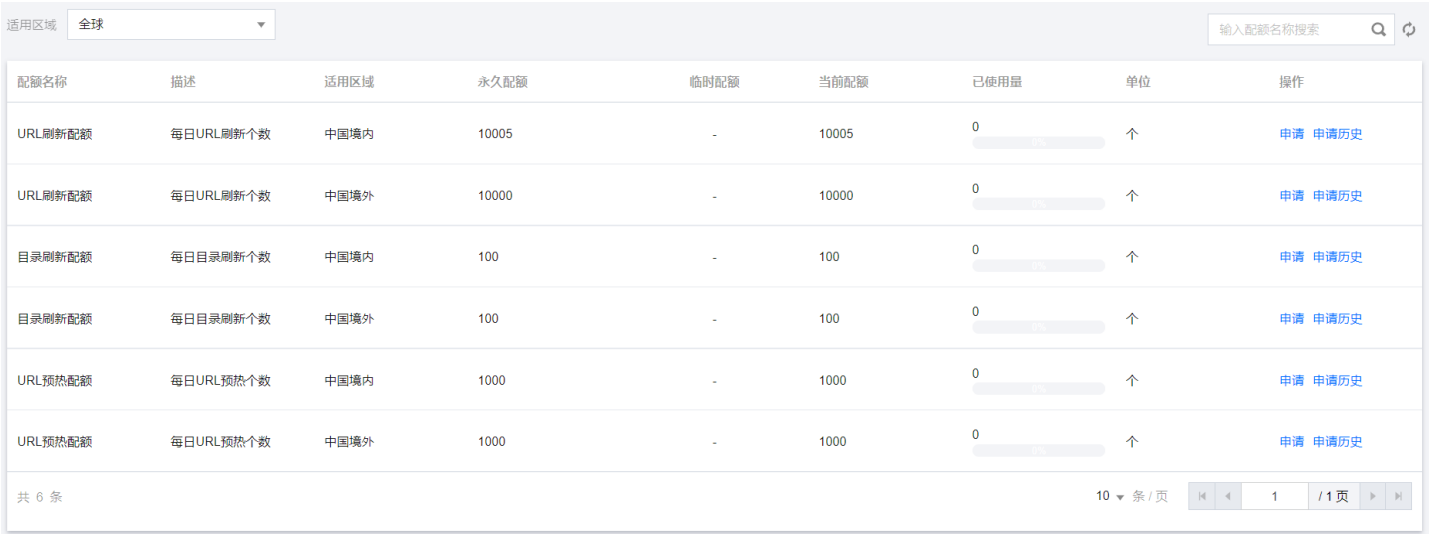
适用场景

- **临时配额**：当业务活动、运营场景需要临时增加配额时，可以通过配额管理申请所需时间范围的临时配额。临时配额有效期过期后，当前配额将恢复至永久配额。
- **永久配额**：当现有配额无法满足您业务日常需求时，可以通过配额管理申请对应功能的永久配额。永久配额审批耗时较长，建议您临时业务需求可申请临时配额。

操作指南

配额查看

登录 CDN 控制台，单击左侧目录的选择**配额管理** > **配额详情**，进入配额详情页面，您可以查看配额现状或申请配额。



> **说明：**
>
> - 当前配额表示该配额的当前配额上限，若当前时间有多个生效的临时配额，当前配额取值为所有临时配额及永久配额中的最大值。
> - 临时配额将在开始日期的00:00生效，结束日期的24:00结束，结束后额度恢复至永久配额。
> - URL 刷新配额、目录刷新配额、URL 预热配额均为每日生效配额，已使用量将在每日00:00重置。

- 中国境内、中国境外的配额相互独立，需要单独申请提升。
- CDN 域名上限均为永久配额，不区分地域，永久生效。

配额申请

单击**申请**，可进入所选配额申请页面，填写并提交配额申请信息。

说明：

- 申请配额可输入范围最小值为所选配额的永久配额+1，最大值为10000000。
- 配额类型为临时配额，可选临时配额有效日期，日期可选范围为90天内，最大生效时长为7天。
- 请您填写合理配额数值和详尽的申请理由，以提升配额申请审批通过几率。
- 如果您当前申请配额为 CDN 域名上限配额，建议当前域名已使用量超70%且申请域名配额数量不超过当前配额的2倍，否则可能被拒绝。

版权所有：腾讯云计算（北京）有限责任公司

申请历史

单击**申请历史**，或单击左侧目录的选择**配额管理** > **申请历史**，进入申请历史页面，您可以查看配额申请的审批情况。

> 说明：
>
> - 申请结果为**已通过**时，表示配额申请已审批通过；若审批未通过，建议申请**临时配额**，或调整申请配额及申请理由重新提交。
> - 临时配额有效日期结束后，状态为过期，表示该临时配额已失效，当前配额将恢复为永久配额或其他生效的临时配额。