

内容分发网络

管理说明

产品文档



腾讯云

【版权声明】

©2013-2019 腾讯云版权所有

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

【商标声明】

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

【服务声明】

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

文档目录

管理说明

域名管理

域名接入

域名操作

CNAME 配置

域名检索

配置管理

配置概览

基本配置

基本信息

源站配置

回源 HOST 配置

访问控制

过滤参数配置

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

缓存过期配置

回源配置

中间源配置

Range 回源配置

回源跟随301/302配置

带宽封顶配置

HTTPS 配置

SEO优化配置

鉴权配置

HTTP Header 配置

智能压缩

权限管理

权限说明

管理说明

域名管理

域名接入

最近更新时间：2019-08-15 15:16:37

您可以在 CDN 控制台中接入域名，享受腾讯云 CDN 为您提供的加速服务，具体操作步骤如下。

步骤1：添加域名

登录 [CDN 控制台](#)，单击左侧【域名管理】菜单，选择【添加域名】。

域名管理							
添加域名	启动CDN	部署至海外CDN	更多操作	<input type="text" value="按关键字搜索域名"/>			
<input type="checkbox"/>	域名	状态	CNAME	接入方式	业务类型	所属项目	操作
<input type="checkbox"/>		已启动		COS源	静态加速	默认项目	管理
<input type="checkbox"/>		已启动		自有源	流媒体直播...	默认项目	管理

进入添加域名页面，您可以在这里完成域名的相关配置。

域名配置

域名

添加的全部域名源站需完全相同

所属项目

源站类型

源站设置

可填写多个源站IP（一行一个，最多32个），或填写一个域名，支持配置端口（0-65535）

域名配置

1. 在**域名**位置填入需要加速的域名。支持泛域名接入，如：`*.test.com`。支持域名批量接入，通过单击【添加】按钮最多可添加10个域名。

域名需要满足以下条件：

- 域名已经在工信部进行过备案。
- 域名尚未被接入过腾讯云 CDN。

2. 在**所属项目**处选择域名对应的项目，进行域名的分项目管理，此处的项目为腾讯云所有产品共享，您可以在 [项目管理](#) 中添加项目。

3. 选择**源站类型**并填写**源站设置**。

源站类型可分为自有源和 [腾讯云对象存储（COS）](#) 源。

- 自有源：如果您已经拥有稳定运行的业务服务器（即源站），您可以通过自有源方式接入 CDN。源站本身无需做任何修改，仅通过 CDN 控制台接入流程，以及 DNS 配置即可享受加速服务。**源站设置**中填入的 IP 地址和源站域名需要满足以下条件：

- a. 若填入的为域名，则**必须不能**与访问域名（即接入的加速域名）一样。支持“域名：PORT”格式，端口号需 **> 0 且 ≤ 65535**。
- b. 若填入的为 IP，可填入多个 IP，支持“IP:PORT”格式，端口号 **> 0 且 ≤ 65535**。当填入多个 IP 的时候，回源请求会依次轮流访问各 IP。
- c. 当有多个 IP 时可配置权重，设置权重格式为 IP:PORT:WEIGHT，其中 PORT 可以省略，格式为 IP::WEIGHT，WEIGHT 取值范围为0 - 1000。（仅限于IPv4地址）

- d. 填入的 IP 不能是内网 IP。
- 腾讯云对象存储（COS）源：若您想使用 [腾讯云对象存储（COS）](#) 存储静态加速内容，可以直接使用 [腾讯云对象存储（COS）源接入方式](#)，将域名接入 CDN。接入方式如下：
 - a. 源站类型为 [腾讯云对象存储（COS）](#)，您可通过下拉菜单或输入关键字选择 Bucket 的域名。
 - b. 若对应项目下无存储桶，您需要登录 [腾讯云对象存储（COS）控制台](#) 创建存储桶（创建详情请参见 [创建存储桶](#)），或联系您的开发商账号为您分配对应的存储桶使用权限。
 - c. 选择了存储桶作为源站后，您可以在 [腾讯云对象存储（COS）控制台](#) 对源站内容进行管理。

注意：

- 从 CDN 接入 COS 源域名时，已全面切换为 COSV5 版本，若您需要添加 COSV4 的 bucket 作为源站，需要前往 COSV4 控制台，对相应 bucket 开启加速服务。
- 若您的 COSV5 bucket 为私有，需要先允许您的 CDN 服务访问对应 COS bucket，而后开启回源访问，此时所有私有 bucket 中的资源均可通过 CDN 公网分发，具有较高安全风险，请谨慎操作。

加速服务配置

选择加速服务业务类型及基础配置。

加速服务配置

业务类型

业务类型一经确认，无法再修改，请根据您的业务类型谨慎选择

基本配置 开启过滤参数 ⓘ

缓存过期配置

类型	内容	刷新时间	操作
全部	所有内容	30 天	
<input type="text" value="文件类型"/>	<input type="text" value=".php;.jsp;.asp;"/>	0 秒	删除
<input type="button" value="添加"/>			

1. 业务类型

业务类型选择决定了域名调度的资源平台，不同资源平台加速配置存在一定差异，请选择与您业务相匹配的业务类型：

- 静态加速：适用于电商类、网站类、游戏图片类静态资源加速场景。
- 下载加速：适用于游戏安装包、音视频原文件下载、手机固件分发等场景。
- 流媒体点播加速：适用于音视频点播加速等场景。

2. 基本配置

CDN 为您提供了过滤参数开关，您可以根据业务需要，控制是否对用户请求 URL 中 “?” 之后的参数进行过滤。您可以利用过滤参数灵活的进行版本控制，或对资源进行带有 Token 的鉴权。详情请参见 [过滤参数配置](#)。

3. 缓存过期配置

缓存过期配置是指 CDN 加速节点在缓存您的业务内容时遵循的一套过期规则。详情请参见 [缓存过期配置](#)。

接入完成

单击【提交】完成添加域名操作，请耐心等待域名配置下发至全网节点，下发时间约5 - 10分钟。



步骤2：配置 CNAME

添加成功的域名，在域名管理页面，可以查看到 CDN 为您的域名分配的加速 CNAME，您需要前往接入域名的 DNS 服务商（如 Dnspod）处，为此域名添加一条 CNAME 记录，待 **DNS 配置生效后**，即可进行加速服务。详情请参见 [CNAME 配置](#)。

域名操作

最近更新时间：2019-08-26 11:09:14

您可以在 CDN 控制台上，对接入 CDN 的加速域名进行加速服务启动、关闭、删除、修改所属项目等操作：

- 启动状态：正常提供加速服务。
- 关闭状态：域名关闭后，若用户请求到达 CDN 节点，则会直接返回404，无法正常服务。关闭状态的域名自定义配置在下一次开启时会继续保留。
- 删除状态：从域名列表删除，仅关闭状态的域名可删除。
- 项目：域名所属项目为涉及到 CDN 的子用户权限划分，请谨慎操作。
- 域名在90天内没有任何操作或流量/带宽消耗将会被回收（自动下线）。

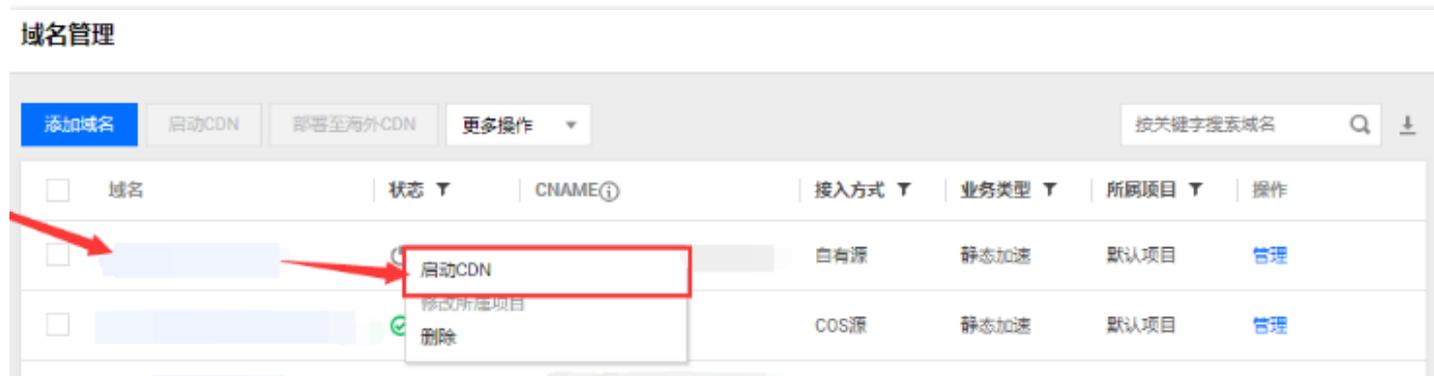
启动加速

对处于**已关闭**状态的域名，您可以对其进行**启动**操作。启动加速服务大约需要5分钟，具体操作如下。

登录 [CDN控制台](#)，单击【域名管理】进入相应页面。启动加速服务有2种方式：

单域名启动

右键单击要启动加速服务的域名，选择【启动 CDN】。



批量启动

勾选需要启动的域名，单击域名上方【启动 CDN】。



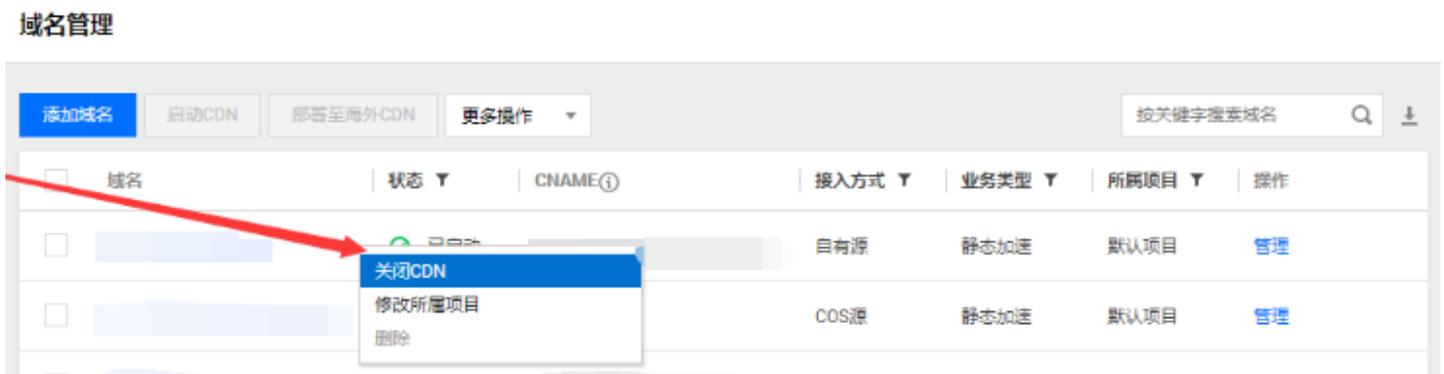
关闭加速

对处于**已启动**状态的域名，您可以对其进行**关闭**操作。关闭后的域名配置会保留（下次开启时无需再次配置），但不会继续为您提供加速服务。关闭过程大约需要5分钟，具体操作如下。

登录 [CDN 控制台](#)，单击【域名管理】进入相应页面。关闭域名加速有单域名关闭和批量关闭2种方式。

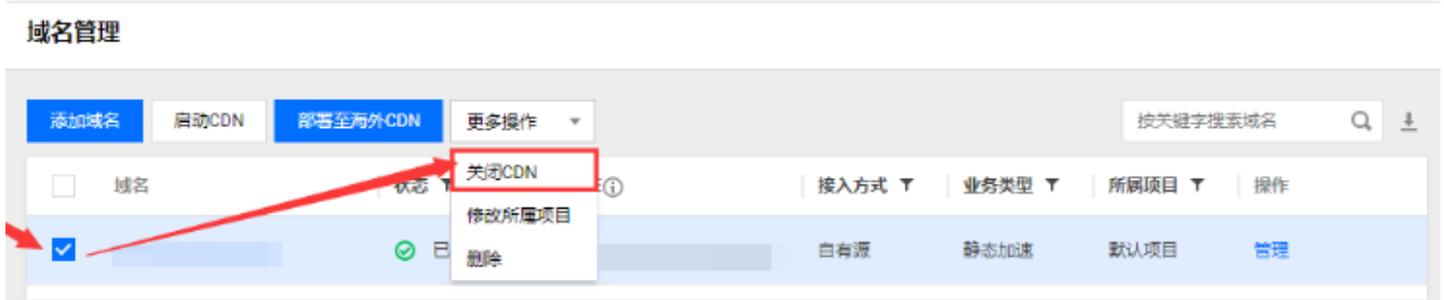
单域名关闭

右键单击要关闭加速服务的域名，选择【关闭 CDN】。



批量关闭

勾选需要关闭的域名，然后在【更多操作】下拉框中，选择【关闭 CDN】。



删除加速域名

对于处于**已关闭**状态的域名，您可以对其进行**删除**操作，删除域名后，其配置将不会保留，具体操作如下。登录 [CDN控制台](#)，单击【域名管理】进入相应页面。删除加速域名有单域名删除和批量删除2种方式。

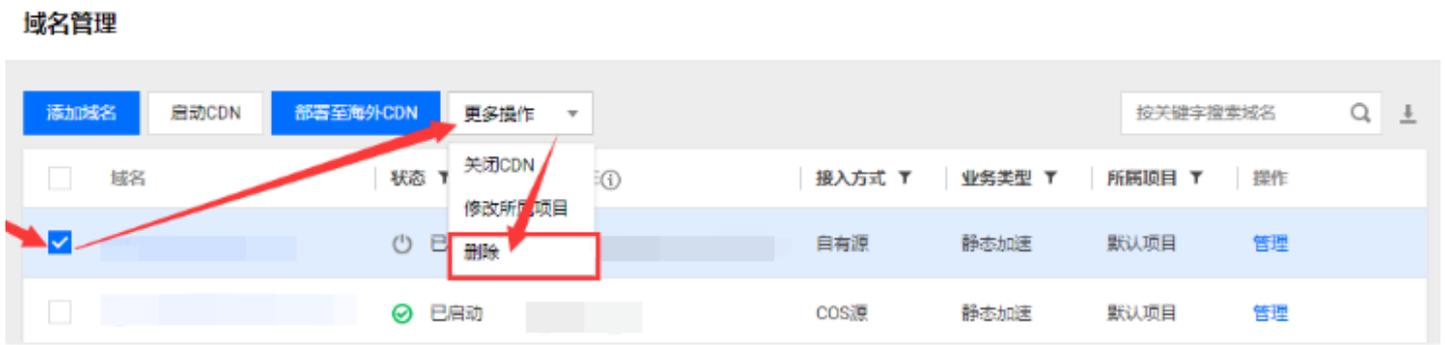
单域名删除

右键单击要删除的域名，选择【删除】。



批量删除

勾选需要删除的域名，然后在【更多操作】下拉框中，选择【删除】。



修改所属项目

登录 [CDN控制台](#)，单击【域名管理】进入相应页面。修改域名所属项目有单域名修改和批量修改2种方式。

单域名修改

右键单击要修改所属项目的域名，选择【修改所属项目】。



批量修改

您也可以勾选多个需要调整项目的域名，然后在【更多操作】下拉框中，选择【修改所属项目】。



将所属项目修改为目标项目即可。

修改所属项目 ×

所属项目

此操作会同时修改域名中国境内、境外所属项目

CNAME 配置

最近更新时间：2019-08-28 16:43:38

您的域名接入 CDN 后，系统会为您自动分配一个以 `.cdn.dnsv1.com` 为后缀的 CNAME 域名，可在 CDN 控制台 [域名管理页](#) 查看。CNAME 域名不能直接访问，您需要在域名服务提供商处完成 CNAME 配置，配置生效后，即可享受 CDN 加速服务。

<input type="checkbox"/> 域名	状态 ▾	CNAME①	接入方式 ▾	业务类型 ▾	所属项目 ▾
<input type="checkbox"/>	已启动	cdn.dnsv1.com	自有源	静态加速	默认项目
<input type="checkbox"/>	已启动	dn.dnsv1.com	自有源	静态加速	默认项目

腾讯云设置方法

注意：

域名解析各种记录类型之间是有优先级差异的，在主机记录相同的情况下，同一条线路有几种不同的记录类型不能共存，否则将会提示冲突。CNAME 记录与除 CNAME 记录以外的任何记录类型都冲突，需要先删除掉其他记录，再进行配置。详情请参见 [为什么添加解析记录的时候提示“记录有冲突”](#)。

若您的 DNS 服务商为腾讯云，您可通过如下步骤添加 CNAME 记录。

1. 登录 [域名服务](#) 控制台，在列表中，找到需要添加 CNAME 记录的域名所在行，单击操作栏的【解析】。

<input type="checkbox"/> 域名	服务状态 ①	注册时间 ↕	到期时间 ↕	操作
<input type="checkbox"/>	实名认证失败 ①	2017-11-30	2019-11-30 已开启自动续费	解析 管理 更多 ▾
<input type="checkbox"/>	正常	2017-08-23	2022-08-23 已开启自动续费	解析 管理 更多 ▾

2. 在跳转到的页面中，单击【添加记录】。



3. 在 **主机记录** 处填写域名前缀（如：www），将 **记录类型** 设置为 CNAME，在 **记录值** 处填写 CNAME 域名，单击【保存】，即可添加 CNAME 记录。



DNSPod 设置方法

若您的 DNS 服务商为 DNSPod，您可通过如下步骤添加 CNAME 记录。

CNAME记录的添加方式



A.主机记录处填子域名（比如需要添加www.123.com的解析，只需要在主机记录处填写www即可；如果只是想添加123.com的解析，主机记录直接留空，系统会自动填一个“@”到输入框内，@的CNAME会影响到MX记录的正常解析，添加时慎重考虑）。

B.记录类型为CNAME。

C.线路类型（默认为必填项，否则会导致部分用户无法解析；在上图中，默认的作用为：除了联通用户之外的所有用户，都会指向1.com）。

D.记录值为CNAME指向的域名，只可以填写域名，记录生成后会自动在域名后面补一个“.”，这是正常现象。

E.MX优先级不需要填写。

F.TTL不需要填写，添加时系统会自动生成，默认为600秒（TTL为缓存时间，数值越小，修改记录各地生效时间越快）。

万网设置方法

若您的 DNS 服务商为万网，您可通过如下步骤添加 CNAME 记录。

域名CNAME解析设置方法

别名（CNAME）解析允许您将多个域名映射到同一台计算机。例如，有一台计算机名为“host.mydomain.com”（A记录），它同时提供WWW和MAIL服务；为了便于用户访问服务，可以为该计算机设置两个别名（CNAME）：WWW和MAIL。这两个别名的全称就是“www.mydomain.com”和“mail.mydomain.com”。实际上他们都指向“host.mydomain.com”。

注意：CNAME解析时记录值只能填写另一个域名，即domain，而非网址；且CNAME记录与其它各类型的同名记录会存在冲突，不能有重复前缀的解析记录存在，例如您的域名为abc.com您设置了一条www.abc.com就不能再设置www.abc.com的其它类型的解析记录，否则会导致所有解析记录冲突不生效。

域名CNAME解析设置方法

- 1、登录万网会员中心；
- 2、点击会员中心左侧导航栏中的【产品管理】--“我的云解析”进入万网云解析列表页。
- 3、点击要解析的域名，进入解析记录页。
- 4、进入解析记录页后，点击新增解析按钮，开始设置解析记录。

hichina.com



验证 CNAME 是否生效

不同的 DNS 服务商，CNAME 生效的时间略有不同，一般会在半个小时之内生效。您也可以通过命令行中的 PING 命令来查询 CNAME 是否生效，如果 PING 到后缀为 `.sp.spcdntip.com` 的域名表示域名 CNAME 已生效。

域名检索

最近更新时间：2019-08-30 15:41:03

操作场景

您可以使用域名检索的综合搜索功能快速查找出指定的域名。支持域名、源站、标签和项目的多条件及多关键字筛选。

操作步骤

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搜索过滤。



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 [搜索帮助](#)。



注意：

- 只支持主源站搜索，备源站暂不支持搜索。
- 多 IP 源站情况下的搜索，源站之间用";"分隔。
- 域名、源站只支持单个关键字搜索。

搜索说明

- 域名搜索：输入完整或部分域名进行匹配，支持模糊搜索。

域名管理

添加域名 启动CDN 部署至海外CDN 更多操作

域名: 2 关键字用"|"分隔

<input type="checkbox"/>	域名	状态	CNAME	接入方式	业务类型	所属项目	操作
<input type="checkbox"/>	2.11...	已启动		自有源	静态加速	默认项目	管理
<input type="checkbox"/>	32	已启动		自有源	静态加速	默认项目	管理

- 源站搜索：输入完整或部分源站进行匹配，支持模糊搜索。
- 标签搜索：输入完整标签名，返回包含输入标签名的域名列表，标签名不支持模糊搜索。
- 所属项目搜索：允许选择多项目进行筛选。

域名管理

添加域名 启动CDN 部署至海外CDN 更多操作

所属项目: 默认项目 | nine | nine2

<input type="checkbox"/>	域名	状态	CNAME	接入方式	业务类型	所属项目	操作
<input type="checkbox"/>		已启动		自有源	静态加速	默认项目	
<input type="checkbox"/>		已启动		自有源	流媒体点播...	默认项目	
<input type="checkbox"/>		已启动		自有源	静态加速	test	
<input type="checkbox"/>		已启动		自有源	静态加速	op	
<input type="checkbox"/>		已启动		自有源	静态加速	默认项目	

所属项目筛选列表:

- 全部项目
- 默认项目
- nine
- nine2
- open3
- open4
- forsvn
- test
- taet1

完成 取消

- 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。

搜索帮助

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	<input type="text" value="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	<input type="text" value="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 : text 源站 : 1.1.1.1	<input type="text" value="域名: text 源站: 1.1.1.1"/>	过滤域名包含字符 "text"，源站包含 "1.1.1.1" 的域名。
单域名属性 多关键字	【属性】:【关键词】 【关键词】	所属项目 : test1 test2	<input type="text" value="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	<input type="text" value="域名: test abc"/>	过滤包含字符 "test" 或 "abc" 的域名。

注意：

未填充属性时，CDN 无法做到全局搜索，因此默认添加上【域名】属性进行搜索，即输入单个关键字时，搜索框内容为：`域名:www.test.com`；黏贴字符时，搜索框内容为：`域名:test|abc`。

配置管理

配置概览

最近更新时间：2019-08-26 11:34:50

CDN 支持多项自定义配置，您可以根据自身业务需要进行设置，优化您的 CDN 加速效果。

基本配置

配置名称	功能描述
基本信息	支持修改域名所属项目、域名对应业务类型
源站配置	支持热备源站配置、源站修改，保障回源
回源 HOST 配置	指定 CDN 回源到源站时的访问域名

访问控制

配置名称	功能描述
过滤参数配置	指定节点是否忽略用户的访问 URL 中"?"之后的参数
防盗链配置	配置 HTTP referer 黑白名单
IP 黑白名单配置	支持设置 IP 黑白名单，进行访问控制
IP 访问限频配置	支持单 IP 单节点访问限频配置
视频拖拽配置	支持开启视频拖拽配置

缓存过期配置

配置名称	功能描述
缓存过期配置	配置指定资源内容的缓存过期时间规则
状态码缓存配置	404状态码缓存时间配置

配置名称	功能描述
HTTP 头部缓存	头部缓存策略配置

回源配置

配置名称	功能描述
中间源配置	指定是否使用中间源
Range 回源配置	开启/关闭 Range 分片回源
回源跟随302配置	开启/关闭源站返回302时，是否跟随跳转

安全配置

配置名称	功能描述
鉴权配置	配置 URL 鉴权

高级配置

配置名称	功能描述
带宽封顶配置	对域名设置带宽封顶阈值，超出阈值时关闭 CDN 服务，访问回源站
HTTPS 配置	配置 HTTPS 实现安全加速，支持 HTTPS 强制跳转
SEO 优化配置	开启 SEO 优化配置，保证搜索引擎权重稳定性
HTTP Header 配置	添加 HTTP Header 配置

跨国专线配置

配置名称	功能描述
跨国专线配置（内测中）	境外 CDN 加速时，开启/关闭跨国专线，保障回源质量

基本配置

基本信息

最近更新时间：2019-07-19 16:10:09

您可以在 CDN 控制台中查看域名的基本信息，包括加速域名、CNAME、创建时间，及其所属项目、业务类型。您可以根据需要对域名**所属项目**或**业务类型**进行修改。

⚠ 注意：

调整业务类型会导致加速平台、优化模型发生变化，请确保您的修改操作与业务类型相匹配。部分腾讯云签约大客户无法手动切换业务类型，您可以联系我们的售前、售后架构师，或提交工单联系我们进行后台调整。

配置指引

登录 [CDN 控制台](#)，选择左侧菜单栏的【域名管理】，单击您所要编辑的域名右侧的【管理】。

域名管理



<input type="checkbox"/>	域名	状态	CNAME	接入方式	业务类型	所属项目	操作
<input type="checkbox"/>		部署中		自有源	静态加速	默认项目	管理
<input type="checkbox"/>		已启动		COS源	静态加速	默认项目	管理
<input type="checkbox"/>		已启动		自有源	流媒体直播...	默认项目	管理
<input type="checkbox"/>		已启动		COS源	静态加速	默认项目	管理

单击【基本配置】，您可以看到**基本信息**模块，查看域名的基本信息。

单击**所属项目**右侧的【修改】图标，进行所属项目的调整，也可按照 [域名操作](#) 中说明进行批量域名项目调整、管

理。

基本配置

访问控制

缓存配置

回源配置

安全配置

高级配置

基本信息

域名: [redacted].com

CNAME: [redacted]:cdn.dnsv1.com ⓘ

创建时间: 2019-07-08 11:18:26

所属项目: 默认项目 [修改](#)

业务类型: 静态加速 ⓘ

[如何查看腾讯云项目信息？](#)

源站配置

最近更新时间：2019-07-25 16:17:30

您可以对域名的源站配置进行修改：

- 多活 IP

配置多个 IP 作为源站时，CDN 回源采取轮询策略，随机挑选一个 IP 进行回源；CDN 还会进行源站探测，一旦发现某源站 IP 异常，则会自动屏蔽一定时间（默认为60s），轮询时会跳过此 IP。

- 域名源站

支持设置指定域名为源站，设置为源站的域名需要与加速域名不一致。

- COS bucket 源站

选定 COS 对应 bucket 的外网域名作为 CDN 回源的源站。

- 备站配置

支持自有源域名配置热备源站，当回源请求至主源站错误（包括 4XX、5XX 错误码及 TCP 连接错误）后，会直接回源至热备源站。配置热备源站能够有效降低回源失败率，提升服务质量。热备源站暂时不支持 HTTPS 回源，配置了热备源站的域名在配置证书时，请勿选择 HTTPS 回源。

⚠ 注意：

- 仅支持修改用户自行接入的域名的源站，不支持修改 [对象存储](#) 中 Bucket 自动创建的 CDN 加速域名的源站。
- 根据有关部门规定，源站为腾讯云 CVM 的加速域名，回源 HOST 配置的域名需要在腾讯云备案。

配置指引

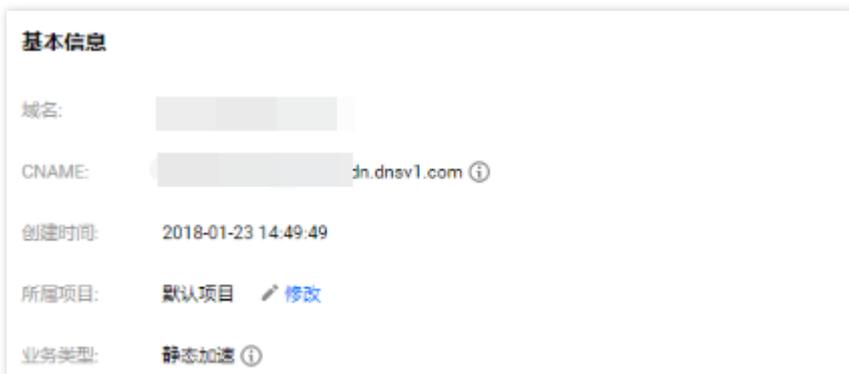
查看配置

1. 登录 [CDN 控制台](#)，在左侧目录中，单击【域名管理】，进入管理页。

2. 在列表中，找到您需要编辑的域名所在行，单击操作栏的【管理】。



3. 在“基本配置”页面，可以看到源站信息模块，可查看域名当前的源站配置。



修改源站

1. 在“基本配置”页面，可以看到源站信息模块。



2. 单击主源站右上角【编辑】图标，可以对主源站类型进行修改：



自有源站：源站地址可以配置为多个 IP 模式或一个域名模式。支持指定端口回源，格式为“域名:PORT/IP:PORT”，端口取值范围为0 - 65535。

- 当源站地址为 IP 模式时，支持源站权重配置，格式为 “IP:PORT:WEIGHT”，权重取值范围为0 - 1000。
 - 单个源站不能设置权重。
 - 源站为多个 IP 时，不允许只为部分IP设置回源权重。
 - 源站为域名格式时不能设置权重，仅当源站为 IP 时可以设置权重。
 - 设置权重格式为 IP:PORT:WEIGHT，其中 PORT 可以省略，格式为 IP::WEIGHT。
 - 目前仅支持 IPv4 地址的权重配置，暂不支持 IPv6。

COS源站：指定 COS bucket 作为源站。

备站添加

1. 针对源站为【自有源】类型的域名，可为其添加热备源站配置，当回源请求至主源站错误（包括 4XX、5XX 错误码及 TCP 连接错误）后，会直接回源至热备源站。



2. 备站仅可添加自有源类型，源站地址可配置为多个 IP 模式，或者一个域名，支持指定端口回源，端口号需要为 0 - 65535 之间。

添加热备源站

加速域名

源站类型 自有源

源站地址

可填写多个源站IP(一行一个)，或填写一个域名，支持配置端口(0-65535)

备站修改

添加好备站后，可在控制台进行一键主备切换，或修改、删除备站。

源站信息

您可以修改已有源站配置，或添加热备源站（仅支持自有源），当回源请求失败后，会直接请求热备源站，获取所需资源。[如何设置源站？](#)

主源站	热备源站
<p>源站类型 自有源</p> <p>源站地址 <input type="text"/></p>	<p>源站类型 自有源</p> <p>源站地址 <input type="text"/></p>

主备切换

配置案例

用户请求：`http://www.test.com/1.jpg`，未在节点命中，回源站获取。

1. 若源站配置如下：



服务器 1.1.1.1 上无该资源，会直接返回404，此时回源层的 CDN 节点收到 response 后，会直接返回给请求客户端，客户无法获取该图片。

2. 若源站配置如下：



服务器 1.1.1.1 上无该资源，会直接返回404，此时回源层的 CDN 节点收到 response 后，再次向备用源站 2.2.2.2 请求该资源，若 2.2.2.2 返回200，则节点会将成功获取到的内容反馈给请求客户端，客户成功获取图片。

回源 HOST 配置

最近更新时间：2019-07-19 15:44:42

什么是回源 HOST

回源 HOST 指 CDN 节点在回源过程中，在源站访问的站点域名。请保证您配置的回源 HOST 域名能够支持访问，否则会导致回源失败的情况，影响您的业务。您可以根据自身业务情况配置自定义回源 HOST。

说明：

- 源站与回源 HOST：源站配置的 IP/域名能够指引 CDN 节点回源时找到对应的源站服务器，服务器上可能存在若干 Web 站点，回源 HOST 指明了资源所在的站点。
- 根据有关部门规定，源站为腾讯云 CVM 的加速域名，回源 HOST 配置的域名需要在腾讯云备案。

配置指引

查看配置

1. 登录 [CDN 控制台](#)，单击左侧目录的【域名管理】，进入管理页面。
2. 在列表中找到您需要编辑的域名所在行，单击操作栏的【管理】。

域名	状态	CNAME	接入方式	业务类型	所属项目	操作
[模糊]	部署中	[模糊]	自有源	静态加速	默认项目	管理
[模糊]	已启动	[模糊]	COS源	静态加速	默认项目	管理
[模糊]	已启动	[模糊]	自有源	流媒体直播...	默认项目	管理

3. 在基本配置页面最下方，可以看到回源 HOST 配置信息。

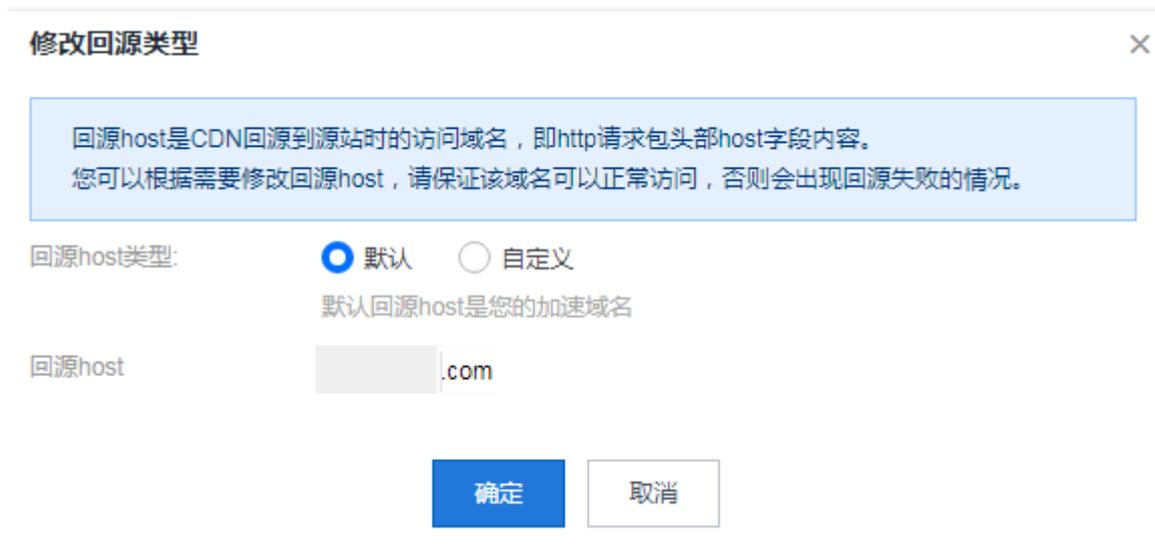


默认情况下，子域名的回源 HOST 为所配置的加速域名，泛域名回源 HOST 为访问域名：

- 若您接入的加速域名为 `www.test.com`，则此节点对此域名下资源发起回源请求时，Request HTTP Header 中 HOST 字段的值为 `www.test.com`。
- 若您接入的加速域名为泛域名，如 `*.test.com`，若访问域名为 `abc.test.com`，则回源 HOST 为 `abc.test.com`。

修改回源 HOST

在回源配置信息处，单击【编辑】，可以对回源 HOST 配置进行调整。**仅支持自有源站回源 HOST 编辑，不支持 COS 源编辑。**



配置案例

用户访问域名为 `www.test.com`，源站配置为域名 `origin.test.com`，`origin.test.com` 对应的 A 记录为 `1.1.1.1`。用户请求为：`http://www.test.com/1.jpg`。

1. 若配置如下：

修改回源类型

回源host是CDN回源到源站时的访问域名，即http请求包头部host字段内容。
您可以根据需要修改回源host，请保证该域名可以正常访问，否则会出现回源失败的情况。

回源host类型: 默认 自定义
默认回源host是您的加速域名

回源host .com

确定 **取消**

默认情况下，回源 HOST 为加速域名，回源时实际请求发往 1.1.1.1。

获取的资源为：`http://www.test.com/1.jpg`。

2. 若配置如下：

修改回源类型

回源host是CDN回源到源站时的访问域名，即http请求包头部host字段内容。
您可以根据需要修改回源host，请保证该域名可以正常访问，否则会出现回源失败的情况。

回源host类型: 默认 自定义
您可以自定义回源host，请保证该域名可以访问源站

回源host

确定 **取消**

回源 HOST 为 `origin.test.com`，回源时实际请求发往 1.1.1.1。

获取的资源为：`http://origin.test.com/1.jpg`。

访问控制

过滤参数配置

最近更新时间：2019-07-19 15:05:03

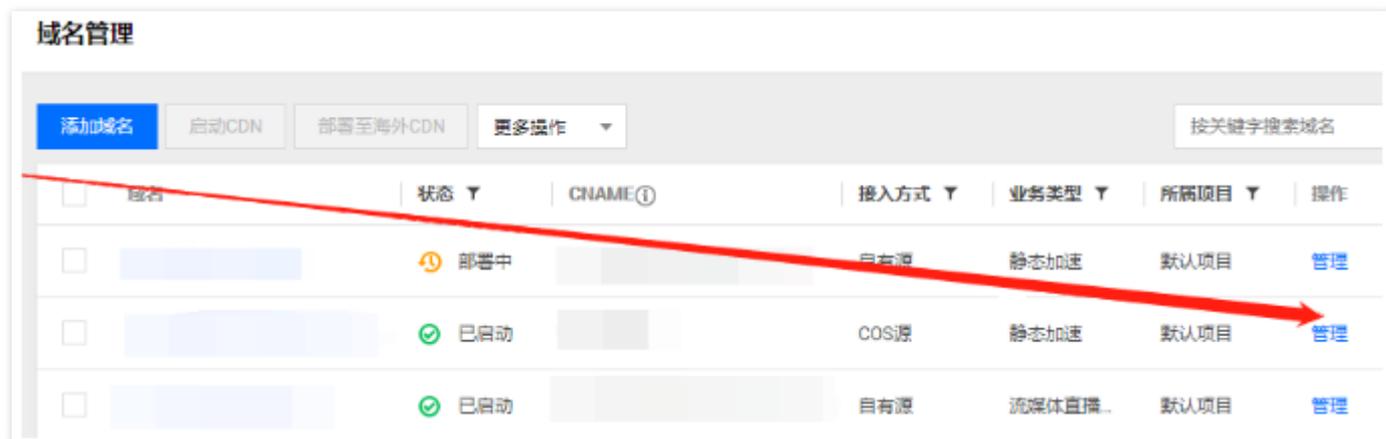
CDN 为您提供了过滤参数开关，您可以根据业务需要，控制在缓存时是否对用户请求 URL 中“?”之后的参数进行过滤。您可以利用过滤参数灵活的进行版本控制，或对资源进行带有 Token 的鉴权。

① 说明：

若您的资源 URL 中不同参数代表相同的内容，建议开启过滤参数，有效提升缓存命中率。

配置指引

1. 登录 [CDN 控制台](#)，在左侧目录单击【域名管理】，进入管理页面。
2. 在列表中，找到您要编辑的域名所在行，单击操作栏中的【管理】。



3. 单击【访问控制】选项卡，在**过滤参数配置**模块，进行过滤参数配置。



① 说明：

若您的加速类型为下载、点播、直播，则过滤参数默认为开启状态，若您接入时加速类型选择为静态，过滤参数默认为关闭状态。

配置案例

CDN 在节点存储结构上缓存资源时，根据 `cache_key` 作为索引，来查找存储的资源。

1. 若配置如下：



- 用户 A 请求 URL 为：`http://www.test.com/1.jpg?version=1.1` 的资源，节点存储资源时，对应的 `cache_key` 为 `www.test.com/1.jpg`，忽略了 "?" 之后的参数。
- 用户 B 也请求 URL 为：`http://www.test.com/1.jpg?version=1.2` 的资源，也按照 `cache_key` 为 `www.test.com/1.jpg` 查找资源，因此与用户 A 请求的为同一份内容，可直接命中。

2. 若配置如下：



- 用户 A 请求 URL 为：`http://www.test.com/1.jpg?version=1.1` 的资源，节点存储资源时，对应的 `cache_key` 为 `www.test.com/1.jpg?version=1.1`，未忽略 "?" 之后的参数。
- 用户 B 也请求 URL 为：`http://www.test.com/1.jpg?version=1.2` 的资源，按照 `cache_key` 为 `www.test.com/1.jpg?version=1.2` 来查找资源，未命中，因此会重新回源站获取对应内容，进行缓存。

防盗链配置

最近更新时间：2019-07-19 15:02:28

若您希望对业务资源的访问来源进行控制，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。

配置指引

1. 登录 [CDN 控制台](#)，在左侧目录中，单击【域名管理】，进入管理页面。
2. 在列表中，找到您需要编辑的域名所在行，单击操作栏的【管理】。



3. 单击【访问控制】选项卡，可在**防盗链配置**模块进行配置。



默认情况下，防盗链未启用，无黑/白名单。referer 黑名单、白名单二者不兼容，同一时间只能生效一种类型，防盗链输入内容最多可输400条，以换行符相隔，一行输入一个。

注意：

- 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。

referer 白名单

1. 单击防盗链配置处【编辑】图标，选中【referer 白名单】，可进行白名单配置。

假设用户为域名 `www.test.com` 配置了 referer 白名单，白名单内容如下：`www.abc.com`，且未勾选**包含空 referer**，则表示用户仅允许 referer 值为 `www.abc.com` 的请求访问，其他请求均返回403。

2. 配置须知：

- 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。
- 当勾选**包含空 referer**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。

修改防盗链配置

不需要输入网址符http://，以换行符相隔，一行输入一个，不可重复；
当未勾选“包含空referer”且输入内容为空时，表示当前未开启referer防盗链功能

防盗链类型 referer黑名单 referer白名单

包含空referer ⓘ

`www.abc.com`

还可输入399个。

确认 取消

referer 黑名单

1. 单击防盗链配置处【编辑】图标，选中【referer 黑名单】，可进行黑名单配置。

假设用户为域名 `www.abc.com` 配置了 referer 黑名单，黑名单内容如下：`www.test.com`，且未勾选**包含空 referer**，则 referer 值为 `www.test.com` 的请求均返回403，其他请求情况均返回正常内容。

2. 配置须知：

- 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。
- 当勾选**包含空 referer**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。

修改防盗链配置 ×

不需要输入网址符http//，以换行符相隔，一行输入一个，不可重复；
 当未勾选“包含空referer”且输入内容为空时，表示当前未开启referer防盗链功能

防盗链类型 referer黑名单 referer白名单

包含空referer ⓘ

www.abc.com

还可输入399个。

确认
取消

配置案例

若域名 referer 配置如下：

修改防盗链配置 ×

不需要输入网址符http//，以换行符相隔，一行输入一个，不可重复；
 当未勾选“包含空referer”且输入内容为空时，表示当前未开启referer防盗链功能

防盗链类型 referer黑名单 referer白名单

包含空referer ⓘ

www.abc.com

还可输入399个。

确认
取消

-
- 用户请求 URL 为 `http://www.test.com/1.jpg?version=1.1` 的资源，通过浏览器访问，请求 referer 为空，此时正常返回内容。
 - 用户请求 URL 为 `http://www.test.com/1.jpg?version=1.1` 的资源，请求 referer 为 `www.abcd.com`，此时未在白名单中，因此直接返回403。

IP黑白名单配置

最近更新时间：2019-07-19 15:00:20

CDN 为您提供 IP 黑白名单配置功能，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。

配置指引

1. 登录 [CDN 控制台](#)，在左侧目录中，单击【域名管理】，进入管理页面。
2. 在列表中，找到您需要编辑的域名所在行，单击操作栏中【管理】。



3. 单击【访问控制】选项卡，可以在 **IP 黑白名单配置** 模块进行配置。
 - 默认情况下，IP 黑白名单未启用，无黑/白名单。IP 黑名单、白名单二者不兼容，同一时间只能生效一种类型，黑名单最多可输100条，白名单最多可输入50条，以换行符相隔，一行输入一个。
 - 目前仅支持如下格式的网段：/8、/16、/24、/32，其他网段格式暂不支持。当 IP 黑名单、白名单输入内容均为空时，表示当前未开启 IP 黑白名单功能。



白名单配置

1. 在 **IP 黑白名单配置** 模块，单击【编辑】，选中【IP 白名单】，可进行白名单配置。

修改IP黑白名单配置

以换行符分隔，一行输入一个，不可重复；
当IP黑名单、白名单输入内容均为空时，表示当前未开启IP黑/白名单功能；
支持如下格式的网段：127.0.0.1/8、127.0.0.1/16、127.0.0.1/24、
127.0.0.1/32；其他网段格式暂不支持

类型 IP黑名单 IP白名单

127.0.0.1/8

还可输入49个。

确认 取消

2. 在输入框中输入名单并提交，即可开启 IP 白名单功能，仅当客户源 IP 匹配列表中的 IP 或 IP 段时，访问能够正常返回所请求的内容，其他请求均直接返回403。

黑名单配置

1. 在 **IP 黑白名单配置** 模块，单击【编辑】，选中【IP 黑名单】，可进行黑名单配置。

修改IP黑白名单配置

以换行符分隔，一行输入一个，不可重复；
当IP黑名单、白名单输入内容均为空时，表示当前未开启IP黑/白名单功能；
支持如下格式的网段：127.0.0.1/8、127.0.0.1/16、127.0.0.1/24、
127.0.0.1/32；其他网段格式暂不支持

类型 IP黑名单 IP白名单

127.0.0.1/8

还可输入99个。

确认 取消

2. 在下方输入框中输入名单并提交后，即开启了 IP 黑名单功能，当客户源 IP 匹配列表中的 IP 或 IP 段时，访问直接返回403，其他访问能够正常返回所请求内容。

配置案例

若域名 `www.test.com` IP 黑白名单配置如下：



修改IP黑白名单配置

以换行符相隔，一行输入一个，不可重复；
当IP黑名单、白名单输入内容均为空时，表示当前未开启IP黑/白名单功能；
支持如下格式的网段：127.0.0.1/8、127.0.0.1/16、127.0.0.1/24、127.0.0.1/32；其他网段格式暂不支持

类型 IP黑名单 IP白名单

1.0.0/8
2.1.1.1

还可输入48个。

确认 取消

则：

- IP 为 `1.1.1.1` 的用户访问资源 `http://www.test.com/1.jpg`，匹配白名单，正常返回内容。
- IP 为 `2.2.2.2` 的用户访问资源 `http://www.test.com/1.jpg`，未匹配白名单，返回403。

IP访问限频配置

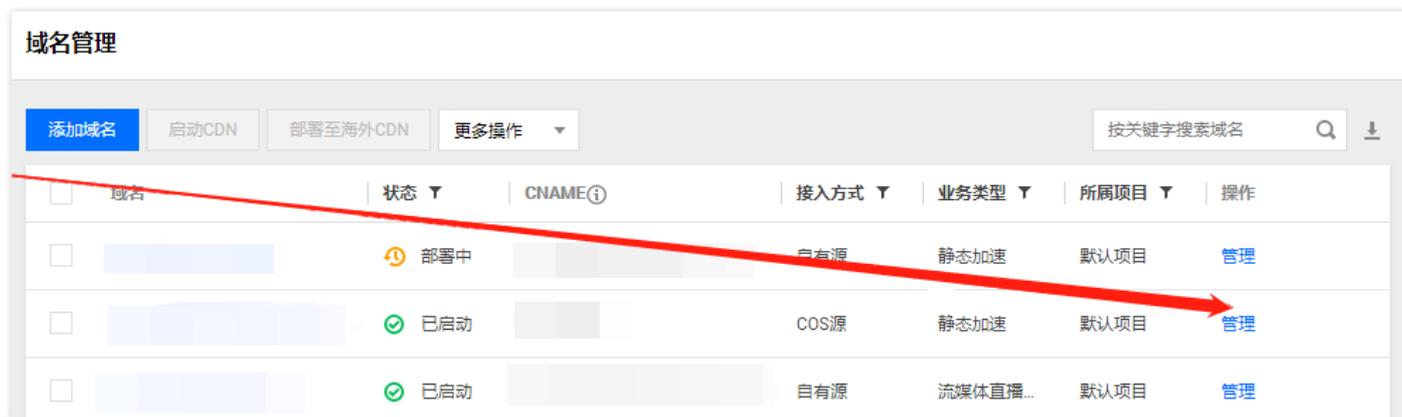
最近更新时间：2019-07-19 14:52:09

CDN 为您提供了 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。

配置指引

配置查看

1. 登录 [CDN 控制台](#)，在左侧目录中，单击【域名管理】，进入管理页面。
2. 在列表中，找到您需要编辑的域名所在行，单击操作栏中的【管理】。



3. 单击【访问控制】选项卡，可以在IP 访问限频配置模块进行配置。
默认情况下，IP 访问限频配置为关闭状态。



修改限频配置

1. 在 **IP 访问限频配置** 模块，开启 IP 访问限频开关，此时系统会根据您最近30天的单 IP 平均访问量，给出一个建议阈值，您可以在下方**当前单 IP 访问阈值**看到给定的默认阈值。

默认阈值的算法为：计算区间为最近30天，每一天有288统计点（五分钟一个），每一个统计点计算单 IP 平均访问频次，取每天的最大值计算平均，为默认阈值。默认阈值最小为10QPS，仅供参考，建议您根据业务波动合理设置阈值。

2. 单击【编辑】。

IP访问限频配置

通过对单IP单节点QPS限制，可防御部分CC攻击。 [什么是IP访问限频？](#)

IP访问限频:

当前单IP访问阈值: 10QPS [编辑](#)

- 1、默认阈值为该域名最近30天单IP平均访问量；
- 2、单IP访问限频可防御部分CC攻击，但也可能会影响您的网站访问，请谨慎修改。

3. 设置单 IP 访问阈值，单击【确定】即可。

单IP访问阈值

单IP访问限频可防御部分CC攻击，但也可能会影响您的网站访问，请谨慎修改。

访问阈值 次/秒

配置案例

若域名 `www.test.com` IP 访问限频配置如下：

IP访问限频配置

通过对单IP单节点QPS限制，可防御部分CC攻击。 [什么是IP访问限频？](#)

IP访问限频:

当前单IP访问阈值: 10QPS [编辑](#)

- 1、默认阈值为该域名最近30天单IP平均访问量；
- 2、单IP访问限频可防御部分CC攻击，但也可能会影响您的网站访问，请谨慎修改。

则：

- IP 为 `1.1.1.1` 的用户，在1s中请求了11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11条访问日志，其中有一条因超出 QPS 限制，状态码为514。
- IP 为 `2.2.2.2` 的用户，在1s中请求了11次资源 `http://www.test.com/1.jpg`，访问平均分布在多个 CDN 加速节点上，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：2019-07-19 14:44:02

- 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。

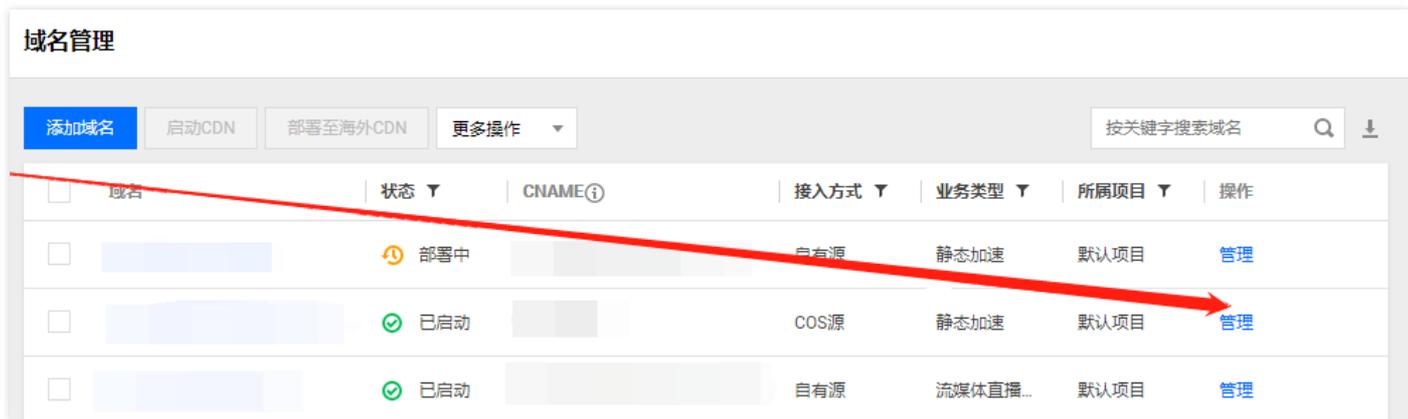
- 开启视频拖拽时，需要同时开启过滤参数，且源站需要支持 range 请求。支持的文件格式为：mp4、flv、ts：

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）	<pre>http://www.test.com/demo.mp4?start=10</pre> 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）	<pre>http://www.test.com/demo.flv?start=10</pre> 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）	<pre>http://www.test.com/demo.ts?start=10</pre> 表示从第10秒开始播放

配置指引

1. 登录 [CDN 控制台](#)，在左侧目录中，单击【域名管理】，进入管理页面。
2. 在列表中，找到您需要编辑的域名所在行，单击操作栏的【管理】。



3. 单击【访问控制】选项卡，可以在[视频拖拽](#)模块进行配置。
默认情况下，视频拖拽配置为关闭状态。

视频拖拽

开启此配置可以通过start指定视频播放的开始位置，支持mp4、flv与ts，开启此配置需同时开启过滤参数配置。 [什么是视频拖拽?](#)

视频拖拽:

4. 开启视频拖拽开关，若 [过滤参数配置](#) 为关闭状态，开启视频拖拽会自动开启过滤参数。



缓存过期配置

最近更新时间：2019-07-19 14:32:20

什么是缓存过期配置

- 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，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。
 - 若资源处于过期状态（即超过了设置的有效时间），用户请求会由节点发送至源站，重新获取内容并缓存至节点，同时返回给用户。
- 腾讯云 CDN 支持各维度的内容缓存时间设置、自定义优先级调整、cache 继承策略（高级缓存配置）、404 状态码缓存过期时间设置及 HTTP Response Header 缓存策略配置。合理的配置缓存时间，能够有效的提升命中率，降低回源率，节省您的带宽。

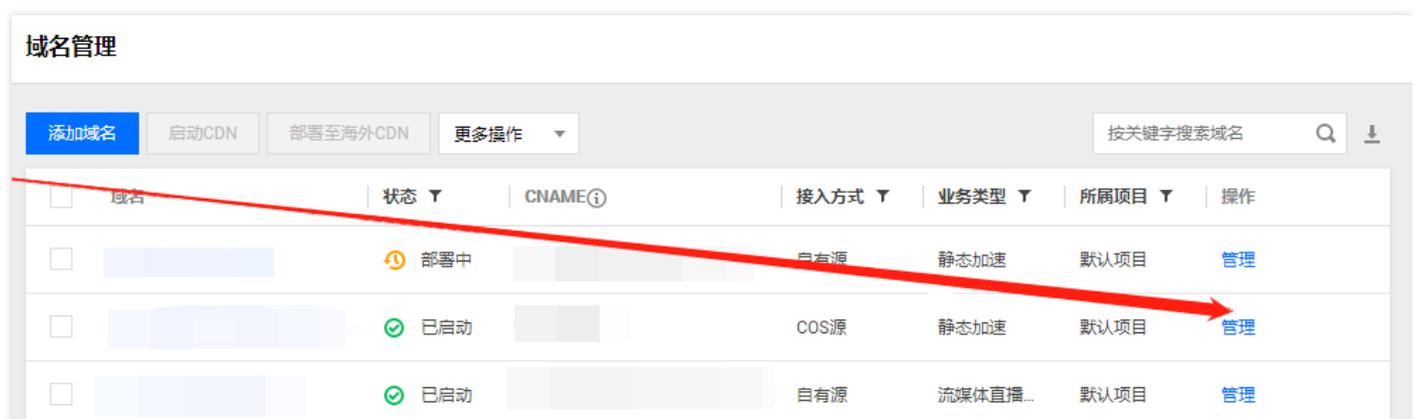
说明：

CDN 的缓存在节点存储资源优先的情况下，有可能由于访问量太少以及资源过冷而提前被剔除掉。

内容缓存

配置指引

- 登录 [CDN 控制台](#)，单击左侧菜单栏的【域名管理】，单击您所要编辑的域名右侧的【管理】。



2. 单击【缓存配置】，您可以看到缓存过期配置模块：



3. 在域名接入时，默认配置如下：

- 自有源域名接入：除常规动态文件（如 .php .jsp .asp .aspx）默认缓存过期时间为0，对此类动态文件请求会直接回源外，其他所有文件默认30天缓存过期时间。
- COS 源域名接入：所有文件默认30天缓存过期时间。
- 默认关闭高级缓存过期设置。

修改配置

单击【新增缓存配置】可以添加缓存配置，您可以根据自身业务需求，在默认配置上添加缓存时间配置，CDN 支持以下几种方式的缓存过期时间设置：

- 按文件类型设置缓存过期时间。**

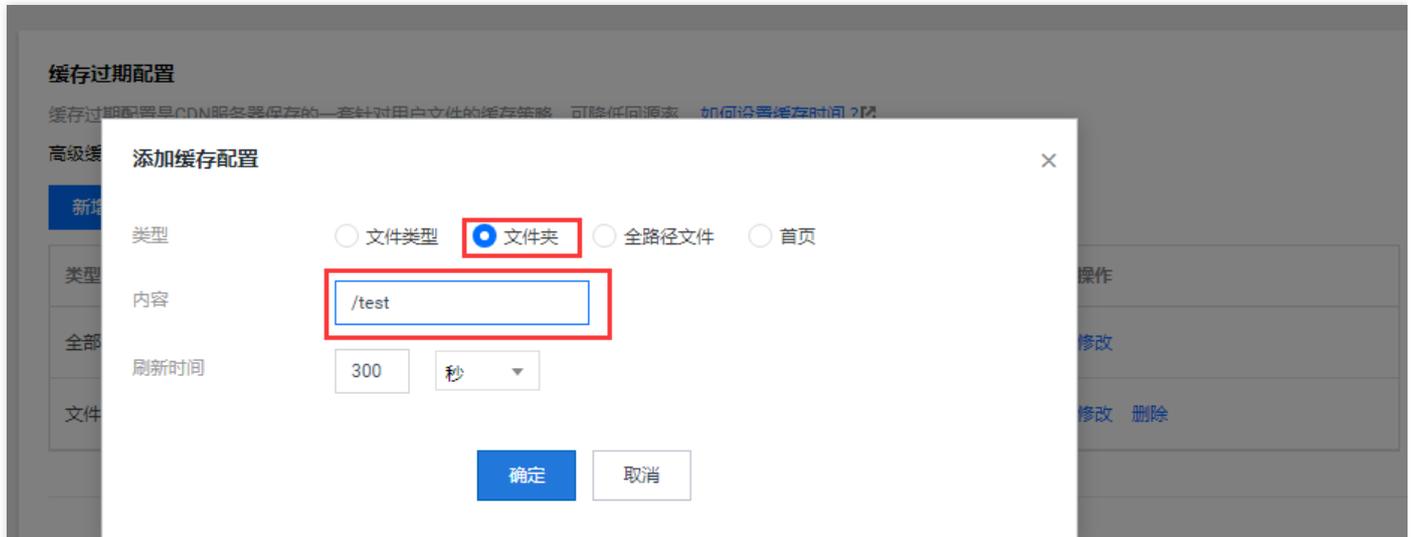
您可以填充文件类型后缀，根据类型来设置缓存时间，如下所示：



配置缓存时间时可填入多项，每项用；隔开，内容区分大小写，必须是以.开头的文件后缀，如.png。刷新时间设置为0时，不缓存，所有请求转发至用户源站；缓存时间设置最大值不能超过365天。

- **按文件夹设置缓存过期时间。**

您可以填充文件夹路径，根据文件夹来设置缓存时间，如下所示：



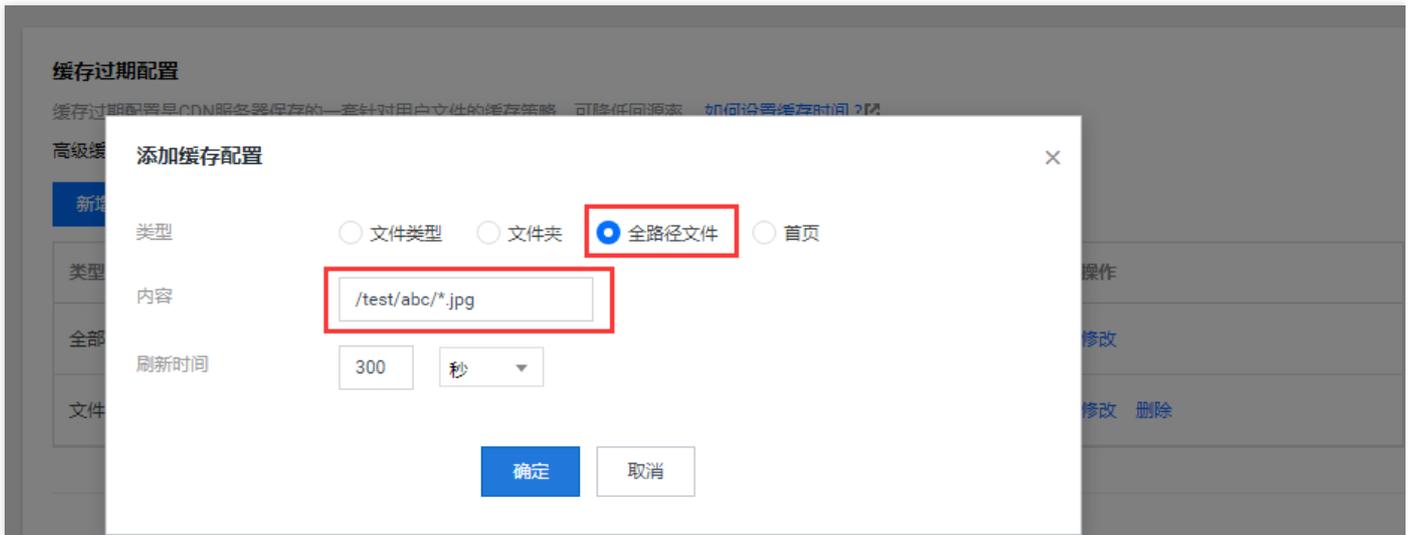
配置缓存时间时可填入多项，每项用；隔开，内容区分大小写，必须是以/开头的文件夹。刷新时间设置为0时，不缓存，所有请求转发至用户源站；缓存时间设置最大值不能超过365天。

- **全路径文件设置缓存过期时间。**

您可以为某一具体文件设置缓存时间，如下所示：

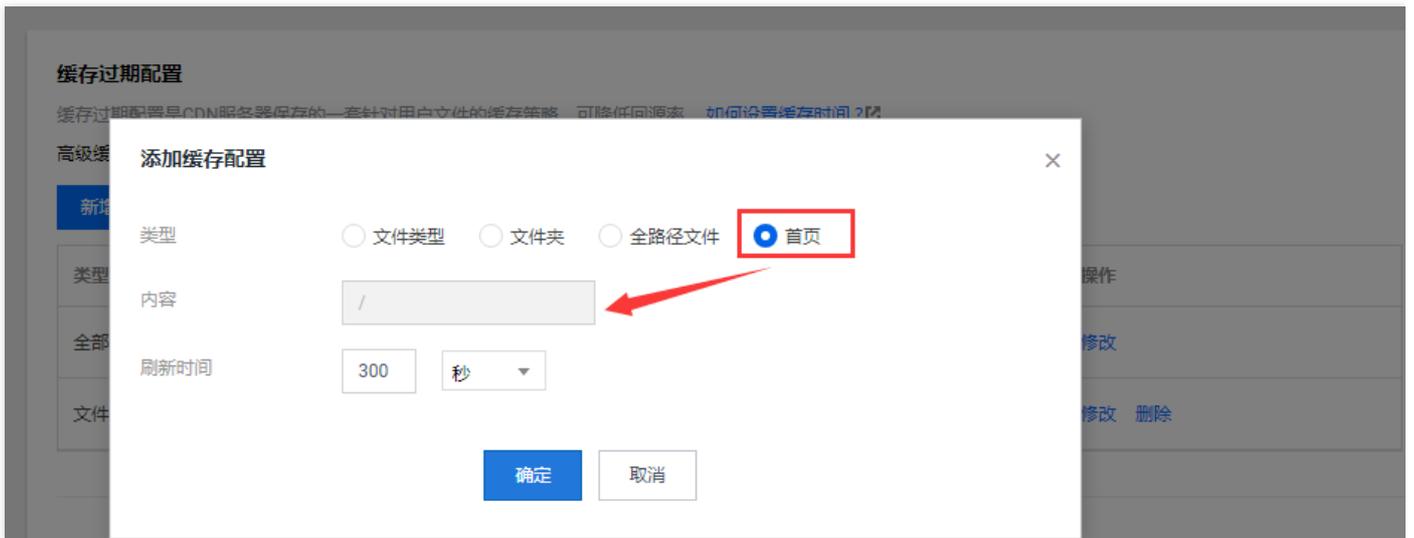


配置缓存时间时可填入多项，每项用；隔开，内容区分大小写，支持 * 匹配某一类型文件，如 /test/abc/*.jpg：



• 首页设置缓存过期时间。

您可以指定首页设置缓存时间，如下所示：



优先级

1. 当设置了多条缓存策略时，相互之间会有重复。

注意：

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

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

- 匹配第一条所有文件，命中，此时缓存时间为30天。
- 匹配第二条，未命中。
- 匹配第三条，命中，此时缓存时间为300秒。
- 匹配第四条，命中，此时缓存时间为400秒。
- 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。

3. 单击【调整优先级】可以添加缓存配置，您可以根据业务情况自定义调整已经添加的缓存过期配置顺序。

基本配置 访问控制 **缓存配置** 回源配置 安全配置 高级配置

缓存过期配置

缓存过期配置是CDN服务器保存的一套针对用户文件的缓存策略，可降低回源率。 [如何设置缓存时间？](#)

高级缓存过期设置:

[新增缓存配置](#) **调整优先级**

类型	内容	刷新时间	操作
全部	all	30天	修改
文件类型	.php;.jsp;.asp;.aspx	0秒	修改 删除

4. 使用右侧上下箭头调整缓存过期时间配置的顺序，单击【保存】即可完成调整。



缓存继承

当用户请求您某一业务资源时，源站对应的 Response HTTP Header 中存在 Cache-Control 字段，此时默认策略如下：

- Cache-Control 字段为 max-age，对该资源的缓存时间以配置的缓存时间为主，不继承 max-age 指定时间。
- Cache-Control 字段为 no-cache 或者 no-store，此时 CDN 节点对此资源不做缓存。
- 无 Cache-Control 字段，CDN 会默认添加：Cache-Control:max-age = 600 头部。

高级缓存配置

1. 在缓存过期配置模块中可以找到高级缓存过期设置开关，单击即可打开。



2. 开启了高级缓存过期设置开关后，用户请求源站某资源时 Response HTTP Header 中带有 Cache-Control 字段，且值为 `max-age = xxxx`，此时节点对该资源的缓存时间取配置的过期时间与 `max-age` 中的最小值：
 - 用户源站配置 `/index.html` 的 `max-age` 为200秒，CDN 对应配置的缓存时间为600秒，则文件实际过期时间为200秒。
 - 用户源站配置 `/index.html` 的 `max-age` 为800秒，CDN 对应的缓存时间为600秒，则文件实际过期时间为600秒。
3. 开启了高级缓存过期设置开关后，若源站没有返回 Last-Modified 字段时，CDN 会默认添加 Last-Modified 字段，每10分钟变一次。

头部缓存

当资源在节点命中缓存时，CDN 默认会缓存以下来自于源站头部，并返回给用户。

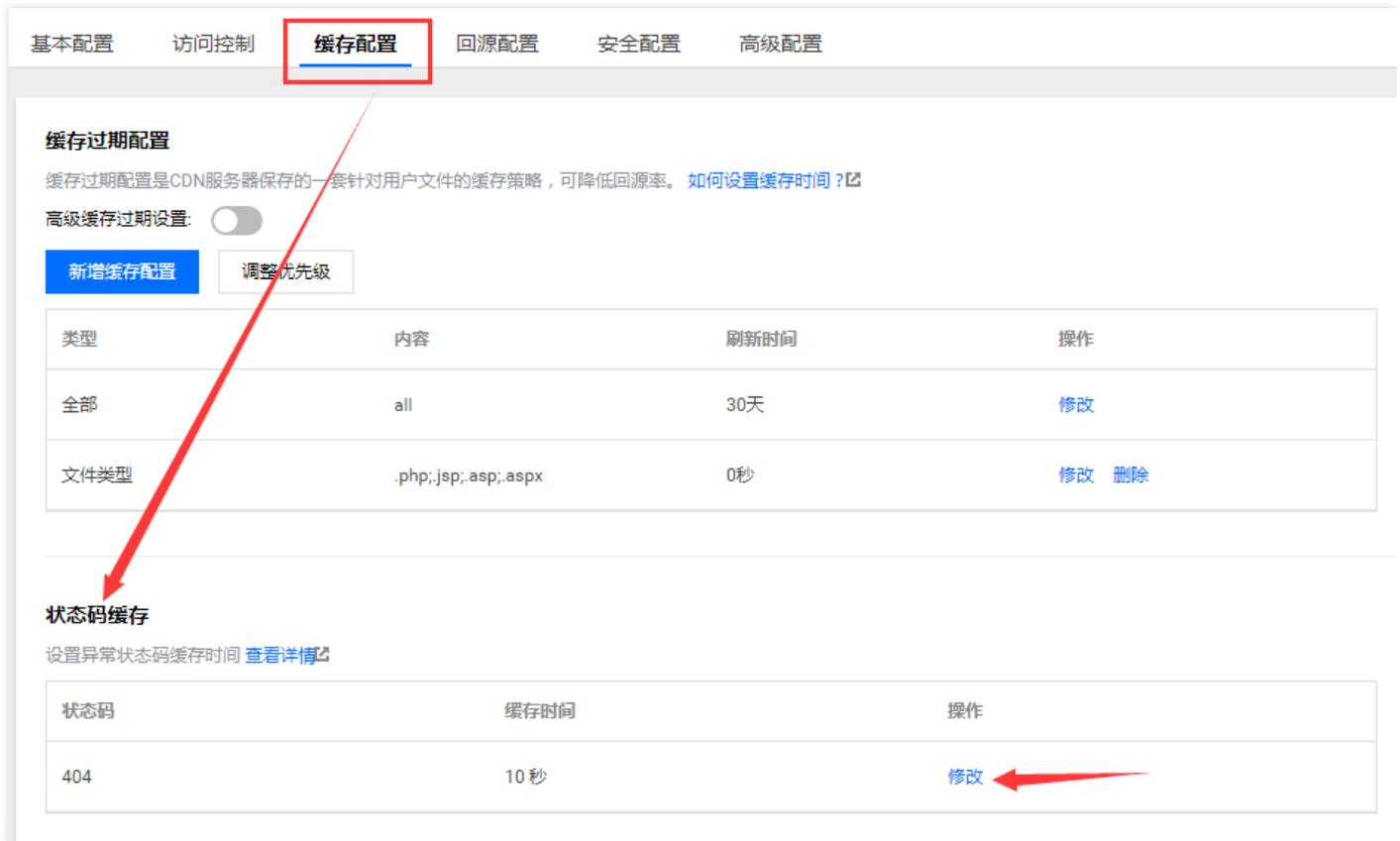
- Access-Control-Allow-Origin
- Timing-Allow-Origin
- Content-Disposition
- Accept-Ranges

您可以前往【域名管理】中【缓存配置】模块，手动开启【缓存源站所有头部】功能，CDN 将缓存所有源站返回头部信息。

状态码缓存

1. 节点请求源站资源时，除上述缓存策略外，还会根据状态码按照如下默认缓存策略进行：
 - 200/206：按照正常缓存策略进行。
 - 3XX：默认不缓存。
 - 4XX：404缓存10s，其他默认不缓存。
 - 5XX：默认不缓存。

2. 您可以在【缓存配置】中【状态码缓存】模块调整404缓存时间：



缓存配置

缓存过期配置

缓存过期配置是CDN服务器保存的一套针对用户文件的缓存策略，可降低回源率。 [如何设置缓存时间？](#)

高级缓存过期设置:

[新增缓存配置](#) [调整优先级](#)

类型	内容	刷新时间	操作
全部	all	30天	修改
文件类型	.php;.jsp;.asp;.aspx	0秒	修改 删除

状态码缓存

设置异常状态码缓存时间 [查看详情](#)

状态码	缓存时间	操作
404	10秒	修改

404状态码缓存时间可调整至0 - 3600秒。

⚠ 注意：

若文件对应的缓存过期时间为0，产生404后，仍遵循不缓存原则，直接透传。

回源配置

中间源配置

最近更新时间：2019-09-04 17:50:16

中间源是位于业务服务器（即源站）和 CDN 节点（境外 CDN 用户则为境外 CDN 节点）的一个中间层的回源服务器。当用户发起请求时，请求会先到达 CDN 边缘节点，若节点无所需资源，则会向中间源发起资源请求，若仍未在中间源命中，中间源会向源站发起请求。

注意：

为提升加速服务效果，2018年10月15日起，接入域名时将默认开启中间源，而且不支持手动关闭。默认开启中间源配置后，在控制台中对应配置项不可见。

配置指引

登录 [CDN 控制台](#)，单击左侧目录的【域名管理】，进入管理页面，在列表中找到您需要编辑的域名所在行，单击操作栏的【管理】。

添加域名	启动CDN	部署至境外	更多操作	关键字用“ ”分隔，过滤标签用回车键分隔				
域名	状态	CNAME	接入方式	业务类型	所属项目	回源HOST	主源站配置	操作
<input type="checkbox"/>	已启动		自有源	静态加速	默认项目			管理
<input type="checkbox"/>	已启动		自有源	静态加速	默认项目			管理
<input type="checkbox"/>	已启动		自有源	静态加速	默认项目			管理
<input type="checkbox"/>	已启动		COS源	静态加速	test			管理

单击【回源配置】，若未看到“中间源配置”模块，则表示您的域名已经**默认开启中间源配置**，用户的请求回源行为会在中间源进行收敛，由中间源统一回源获取数据，提升您的 CDN 加速效果，有效缓解回源后源站的访问压力。

注意：

历史已经接入的域名，若在【回源配置】处可以看见中间源配置为关闭状态，建议手动开启该配置，提升您的加速效果。开启后，此配置项将被屏蔽，不支持关闭操作。

配置案例

- 若配置如下：

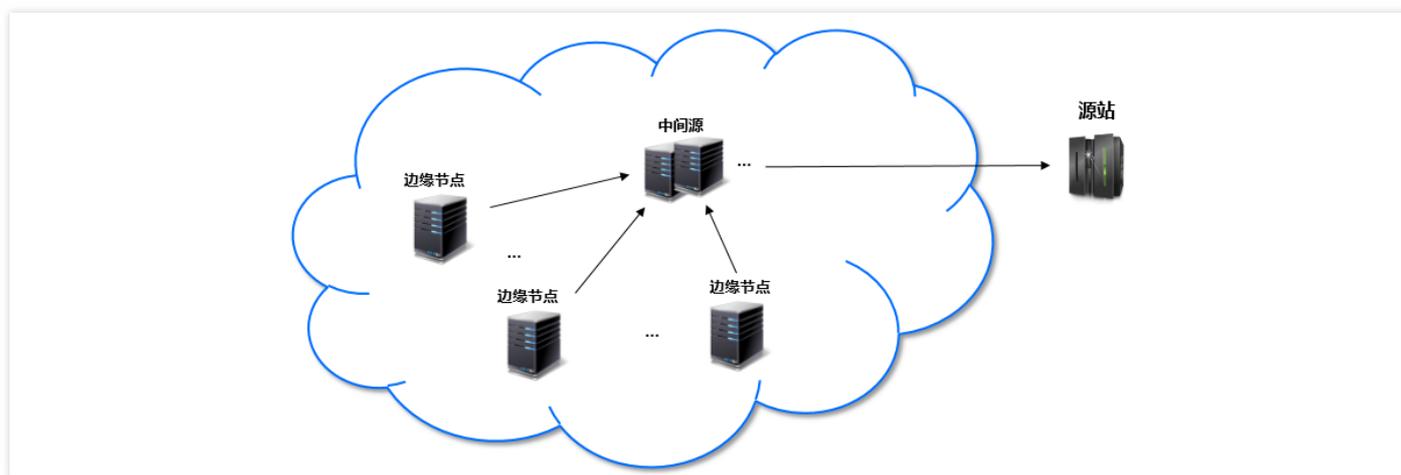
基本配置 访问控制 缓存配置 **回源配置** 安全配置 高级配置

中间源配置

中间源服务器，是位于业务服务器(即源站)和CDN节点的一个中间层的回源服务器。可降低回源后源站的访问压力。 [什么是中间源?](#)

中间源:

用户请求到达各边缘节点，若边缘节点未命中资源，则会回源至父层节点，若父层节点仍未命中，才回源至客户源站。CDN 的架构如图：



- 若配置如下：

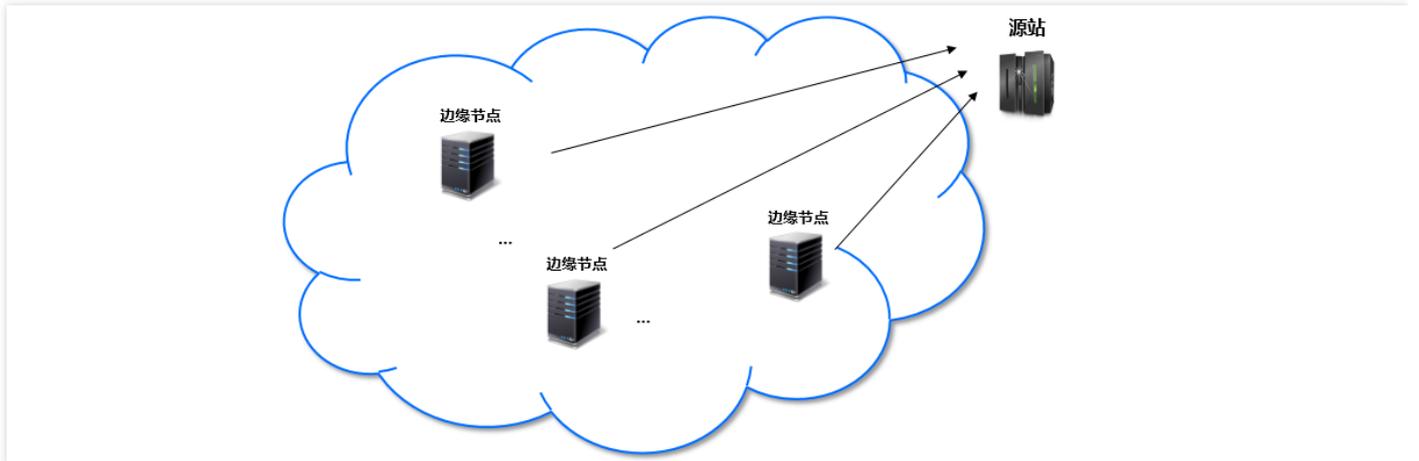
基本配置 访问控制 缓存配置 **回源配置** 安全配置 高级配置

中间源配置

中间源服务器，是位于业务服务器(即源站)和CDN节点的一个中间层的回源服务器。可降低回源后源站的访问压力。 [什么是中间源?](#)

中间源:

用户请求到达各边缘节点，若边缘节点未命中资源，直接回源至客户源站获取。CDN 的架构如图：



Range 回源配置

最近更新时间：2019-07-19 10:56:39

说明：

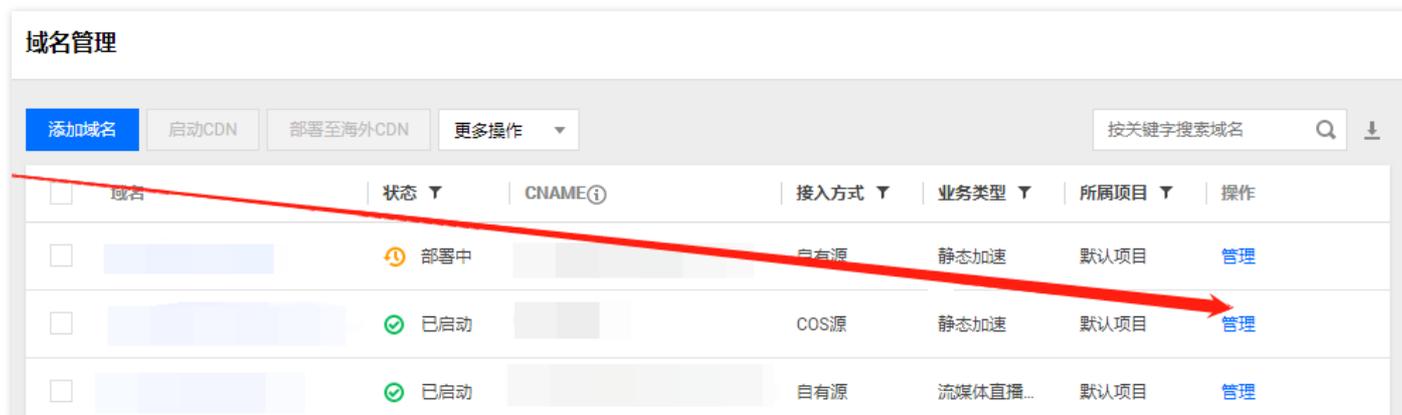
CDN 为您提供 Range 回源配置功能，Range 是 HTTP 请求头，用于文件指定部分的请求。如：Range: bytes = 0-999 就是请求该文件的前1000个字节。开启 Range 回源配置能够有效提高大文件分发效率，提升响应速度。

源站需要支持 Range 请求，否则会导致回源失败。

开启 Range 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。

配置指引

1. 登录 [CDN 控制台](#)，选择左侧菜单栏的【域名管理】，单击右侧操作栏下的【管理】。



域名管理

添加域名 启动CDN 部署至海外CDN 更多操作

按关键字搜索域名

域名	状态	CNAME	接入方式	业务类型	所属项目	操作
	部署中		自有源	静态加速	默认项目	管理
	已启动		COS源	静态加速	默认项目	管理
	已启动		自有源	流媒体直播...	默认项目	管理

2. 单击【回源配置】，您可以看到“Range 回源配置”模块，默认情况下，Range 回源配置为开启状态。



配置案例

- 若域名 `www.test.com`，Range 回源配置如下：



用户 A 请求资源：`http://www.test.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。若此时用户乙发起的也为 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。

- 若域名 `www.test.com` ，Range 回源配置如下：



用户 A 请求资源：`http://www.test.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，节点会直接向源站获取整个资源，待完整获取资源后再返回给用户。

回源跟随301/302配置

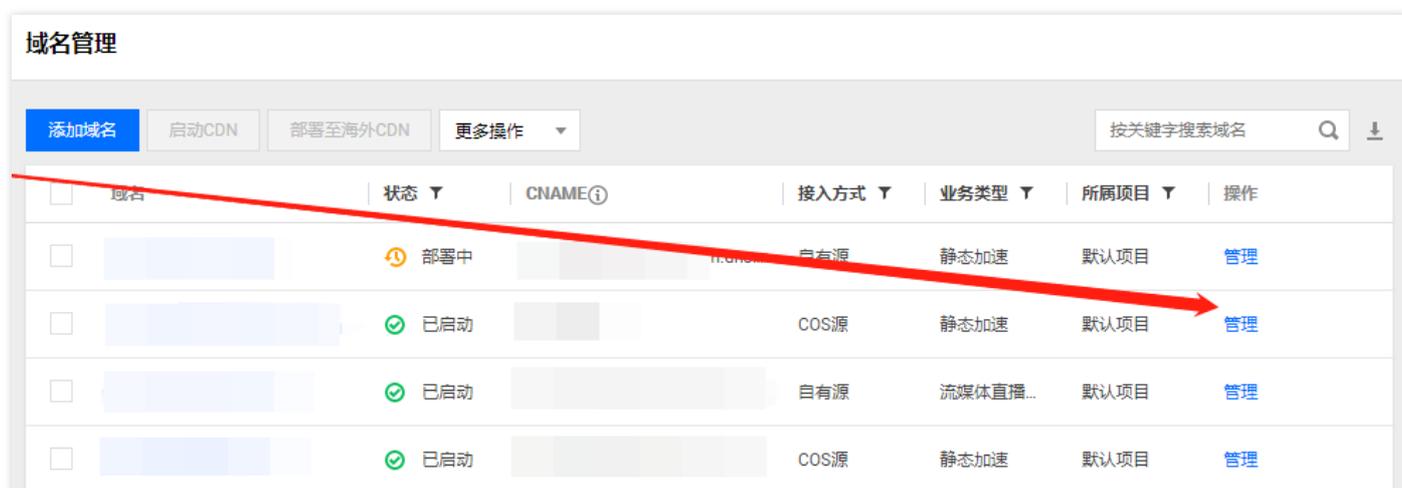
最近更新时间：2019-07-16 14:16:15

说明：

CDN 为您提供回源跟随301/302配置功能。当节点回源请求返回301/302状态码时，CDN 节点会直接向跳转地址请求资源而不返回301/302给用户。

配置指引

1. 登录 [CDN 控制台](#)，选择左侧菜单栏的【域名管理】，单击右侧操作栏下的【管理】：



2. 单击【回源配置】，您可以看到“回源跟随301/302配置”模块，默认情况下，回源跟随301/302配置为关闭状态。



配置案例

- 域名为 `www.test.com`，回源跟随301/302配置如下：



用户 A 请求资源：`http://www.test.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://www.abc.com/1.jpg`，则：

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

- 域名为 `www.test.com` ，回源跟随301/302配置如下：



用户 A 请求资源：`http://www.test.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://www.abc.com/1.jpg`，则：

- 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。
- 获取到所需资源后，缓存至节点，并返回给用户。
- 此时用户 B 也向 `http://www.test.com/1.jpg` 发起请求，则会在节点直接命中并返回给用户。
- 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。

带宽封顶配置

最近更新时间：2019-07-16 10:34:52

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。

配置指引

1. 登录 [CDN 控制台](#)，选择左侧菜单栏的【域名管理】，单击您所要编辑的域名右侧的【管理】。



2. 单击【高级配置】选项卡后，可以看到**带宽封顶配置**模块，默认情况下，带宽封顶配置为关闭状态。



3. 单击按钮开启带宽封顶，开启后默认情况下，带宽阈值为**10Gbps**，到达阈值后会**访问回源**，单击【编辑】图标，可以设置带宽阈值及超出阈值后对用户请求的处理方式。
4. 若您的目的是抵抗超强 DDoS 攻击，为保护您的源站，推荐您设置为“访问返回404”。

5. 若您的目的是控制 CDN 费用，为不影响您的服务，推荐您设置为“访问回源”。

配置封顶带宽 ✕

当统计周期（5分钟）产生消耗超出所设阈值后，CDN将关闭服务。
您可以在域名管理页面重新上线域名，恢复CDN服务。

带宽阈值 Gbps ▾

超出阈值 访问回源 访问返回404

确定
取消

6. 超出封顶阈值后，我们会通过站内信、邮件、短信方式通知您，您可以在 CDN 控制台查看域名状态。不论设置为“访问回源”还是“访问返回404”，域名均转为**已关闭**状态。“访问回源”/“访问返回404”行为生效时间约为**5 - 15 分钟**。

域名管理

添加域名
启动CDN
部署至海外CDN
更多操作 ▾

	域名	状态 ▾	CNAME ⓘ	接入方式 ▾	业务类型 ▾
<input type="checkbox"/>	[域名]	🔌 已关闭	[CNAME]	COS源	静态加速
<input type="checkbox"/>	[域名]	🔌 启动	[CNAME]	COS源	静态加速
<input type="checkbox"/>	[域名]	🔌 启动	[CNAME]	自有源	流媒体直播...

域名于 2018-01-25 01:10:00 超出封顶阈值 1Kbps，已配置为 请求回源，您可以手动开启恢复CDN服务。

① 说明：

触发封顶带宽导致域名关闭后，若您希望继续使用 CDN 服务，可以在 [CDN 控制台](#) 中重新启动域名加速，具体操作请参见 [域名操作](#)。

配置案例

若域名 `www.test.com` 配置如下：



基本配置 访问控制 缓存配置 回源配置 安全配置 **高级配置**

带宽封顶配置

当统计周期（5分钟）产生的带宽超出所设置阈值时，可以根据配置关闭CDN服务，或请求直接返回源站。 [什么是带宽封顶配置？](#)

带宽封顶:

带宽阈值及超出处理: **1Kbps** | 访问回源 [编辑](#)

CDN 会定频检测该域名最近的带宽统计监控数据，若12:15:00 发现该域名在12:05:00 时间点（代表12:05:00 - 12:10:00产生的数据）带宽值大于1Kbps，超出设置上限，会立即下发配置，使请求回源，由于全网 CDN 节点的配置是批量下发，逐步生效，因此带宽会慢慢下降，约在12:20:00左右全网生效。

HTTPS 配置

最近更新时间：2019-08-05 10:09:53

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。

说明：

- 对象存储或万象优品服务开启 CDN 加速后，默认的 .file.myqcloud.com 后缀域名，或 .image.myqcloud.com 后缀域名，可直接支持 HTTPS 请求，无需配置证书。
- 腾讯云 CDN 目前针对 HTTP2.0 协议支持已经全面公测，可直接开启使用。

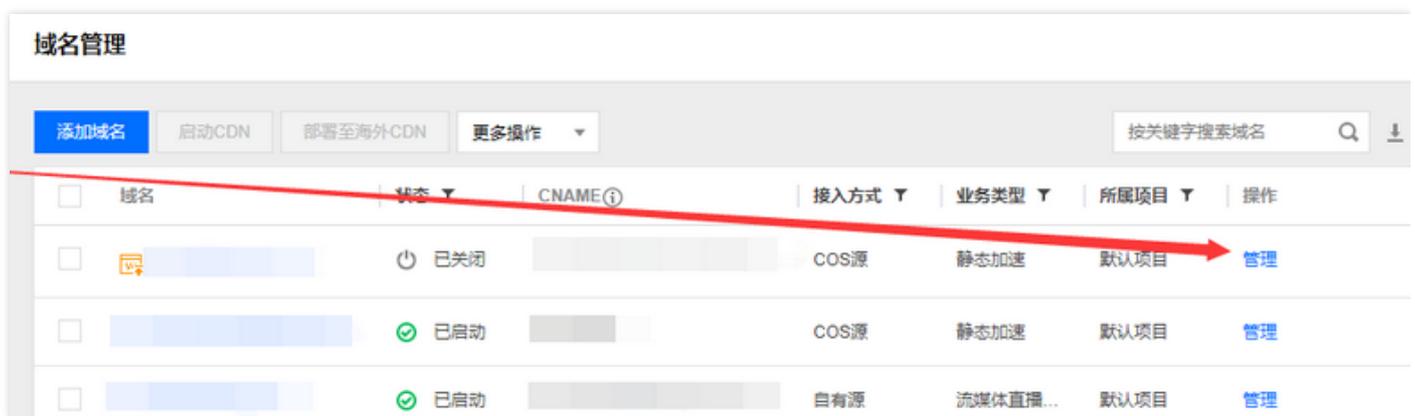
配置指引

腾讯云 CDN 目前支持两种方式部署证书。

- 自有证书：将自有证书、私钥内容上传至 CDN 进行部署，全程加密传输，证书不落地，保障您的证书安全。
- 腾讯云托管证书：您可以通过 [SSL 证书管理](#)，将已有证书托管至腾讯云，以用于多个云产品，您也可以在该平台申请由亚洲诚信免费提供的第三方证书，将其直接部署至 CDN。

配置 HTTPS 证书

- 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：



- 单击【高级配置】，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 [证书管理](#)。



3. 证书配置成功后，会出现【强制跳转 HTTPS】开关。开启后，即使用户发起 HTTP 请求，也会强制跳转为 HTTPS 请求进行访问：



HTTP2.0 配置

在成功为域名配置了 HTTPS 证书后，可以开启 HTTP2.0。

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?](#)

强制跳转HTTPS:

证书来源	证书备注	到期时间	回源方式	证书状态	更多操作
腾讯云托管证书		2018-08-24	HTTP回源	配置成功	前往配置

HTTP2.0配置

您需要先配置HTTPS证书才可开启此项配置。 [什么是HTTP2.0?](#)

HTTP2.0:

[开启HTTP2.0配置](#)

了解更多 HTTP2.0 相关特性，请参见 [HTTP2.0 的新特性](#)。

说明：

file.myqcloud.com 后缀域名暂不支持 HTTP2.0。

HTTPS 回源支持的算法

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
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
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

DH-DSS-DES-CBC3-SHA	DH-RSA-DES-CBC3-SHA	-
---------------------	---------------------	---

SEO优化配置

最近更新时间：2019-07-16 12:19:17

SEO 优化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。

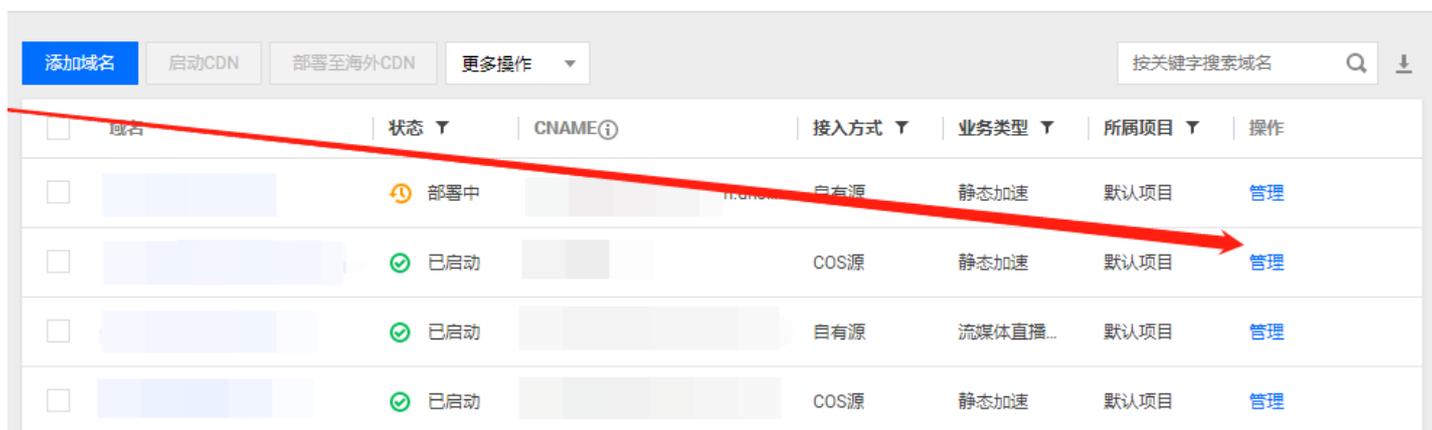
⚠ 注意：

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。

配置指引

登录 [CDN 控制台](#)，选择左侧菜单栏的【域名管理】，单击您所要编辑的域名右侧的【管理】。

域名管理



<input type="checkbox"/>	域名	状态	CNAME	接入方式	业务类型	所属项目	操作
<input type="checkbox"/>		部署中		自有源	静态加速	默认项目	管理
<input type="checkbox"/>		已启动		COS源	静态加速	默认项目	管理
<input type="checkbox"/>		已启动		自有源	流媒体直播...	默认项目	管理
<input type="checkbox"/>		已启动		COS源	静态加速	默认项目	管理

单击【高级配置】，您可以看到**SEO 优化配置**模块。默认情况下，搜索引擎自动回源为关闭状态。

⚠ 注意：

SEO 优化配置功能只在域名接入方式为**自有源**时可使用。开启 SEO 优化配置功能后，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。



←

基本配置 访问控制 缓存配置 回源配置 安全配置 **高级配置**

带宽封顶配置

当统计周期（5分钟）产生的带宽超出所设置阈值时，可以根据配置关闭CDN服务，或请求直接返回。

带宽封顶:

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?](#)

[前往配置](#)

HTTP2.0配置

您需要先配置HTTPS证书才可开启此项配置。 [什么是HTTP2.0?](#)

HTTP2.0:

SEO优化配置

自定义搜索引擎回源，保证搜索引擎权重的稳定性。 [什么是SEO配置?](#)

搜索引擎自动回源 ⓘ:

若当前域名的 CNAME 为旧版 CNAME，还需更新为新版 CNAME 后才可使用 SEO 优化配置功能。

CNAME 更新的具体操作步骤如下：

1. 提交工单变更相应域名的 CNAME 为新版 CNAME。
2. 在您的域名解析服务商处将对应域名的 CNAME 解析切换为新版 CNAME。

[基本配置](#)[高级配置](#)

SEO优化配置

自定义搜索引擎回源，保证搜索引擎权重的稳定性。 [什么是SEO配置？](#)

搜索引擎自动回源 ×

当前域名的CNAME： ast.cdntip.com为旧版CNAME，请按如下步骤变更为新版CNAME后，再使用SEO优化配置：

(1)、请提交工单变更相应域名的CNAME为新版CNAME： .in.dnsv1.com；

(2)、请在您的域名解析服务商处将对应域名的CNAME解析切换为： cdn.dnsv1.com；

鉴权配置

最近更新时间：2019-09-06 15:14:15

功能介绍

CDN 上分发的内容默认为公开资源，为了避免恶意用户盗刷内容进行牟利，腾讯云 CDN 支持 URL 鉴权配置。

算法说明

TypeA

- 访问 URL 格式：`http://DomainName/Filename?sign=timestamp-rand-uid-md5hash`
- 算法说明：
 - timestamp：十进制（UNIX 时间戳）。
 - 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：0。
 - md5hash：MD5（文件路径-timestamp-rand-uid-自定义密钥）。

注意：

若请求原始 URL 为 `http://www.test.com/test/1.jpg`，此时计算 MD5 时文件路径为 `/test/1.jpg`。

TypeB

- 访问 URL 格式：`http://DomainName/timestamp/md5hash/FileName`
- 算法说明：
 - timestamp：时间戳，格式为 YYYYMMDDHHMM。
 - md5hash：MD5（自定义密钥 + timestamp + 文件路径）。

注意：

若请求原始 URL 为 `http://www.test.com/test/1.jpg`，此时计算 MD5 时文件路径为 `/test/1.jpg`。

TypeC

- 访问 URL 格式：`http://DomainName/md5hash/timestamp/FileName`
- 算法说明：

- timestamp : 十六进制 (UNIX 时间戳) 。
- md5hash : MD5 (自定义密钥 + 文件路径 + timestamp) 。

注意：

若请求原始 URL 为 `http://www.test.com/test/1.jpg` ，此时计算 MD5 时文件路径为 `/test/1.jpg` 。

TypeD

- 访问 URL 格式：`http://DomainName/FileName?sign=md5hash&t=timestamp`
- 算法说明：
 - timestamp : 十进制/十六进制 (UNIX 时间戳) 可选。
 - md5hash : MD5 (自定义密钥 + 文件路径 + timestamp) 。

注意：

若请求原始 URL 为 `http://www.test.com/test/1.jpg` ，此时计算 MD5 时文件路径为 `/test/1.jpg` 。

配置指引

1. 登录 [CDN 控制台](#)，单击左侧目录的【域名管理】，进入管理页面，在列表中找到您需要编辑的域名所在行，单击操作栏的【管理】。

添加域名	启动CDN	部署至境外	更多操作	关键字用“ ”分隔，过滤标签用回车键分隔				
域名	状态	CNAME	接入方式	业务类型	所属项目	回源HOST	主网站配置	操作
<input type="checkbox"/>	已启动		自有源	静态加速	默认项目			管理
<input type="checkbox"/>	已启动		自有源	静态加速	默认项目			管理
<input type="checkbox"/>	已启动		自有源	静态加速	默认项目			管理
<input type="checkbox"/>	已启动		COS源	静态加速	test			管理

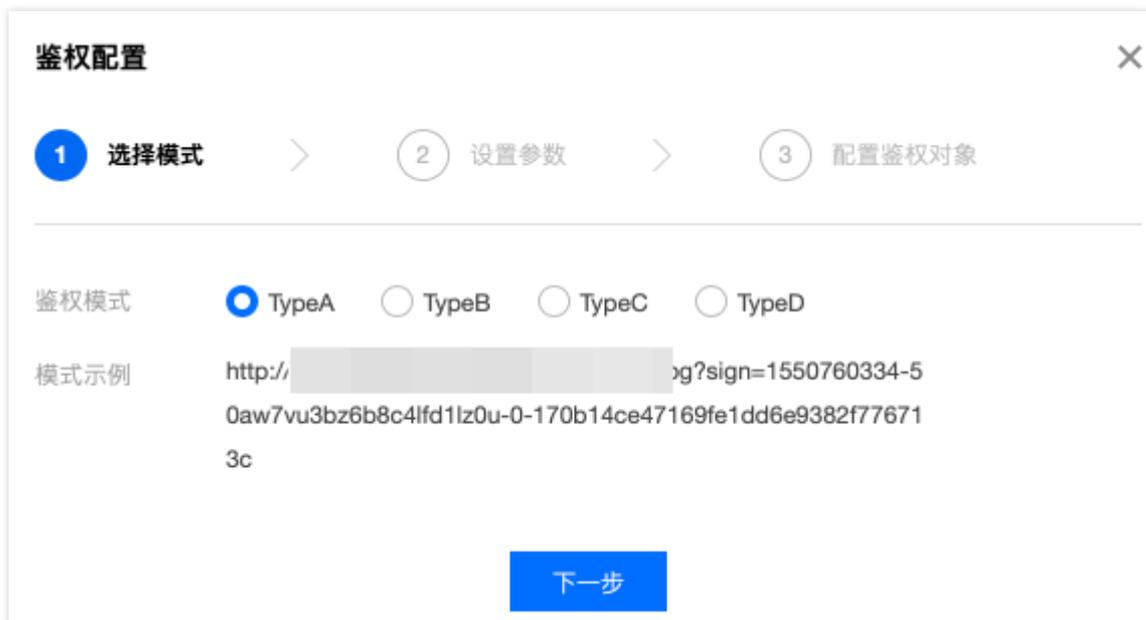
2. 单击【安全配置】，您可以看到鉴权配置模块，默认情况下为关闭状态。



3. 在鉴权配置模块下，单击开启【鉴权配置】，目前提供三类模式可选：

注意：

TypeB 功能升级中，暂无法选择。



4. 选定类型后，可进行鉴权参数配置（以 TypeA 为例）：

- 鉴权密钥：可根据自身业务情况指定字符串作为鉴权密钥。
- 签名参数：设置携带签名串的参数名称，默认填充为 **sign**，可指定为其他参数名。
- 有效时间：服务端会通过签名解析出来的 **timestamp**，加上有效时间，与当前时间对比，判定签名是否有效。

鉴权配置
✕

✓ 选择模式 >
 2 设置参数 >
 3 配置鉴权对象

鉴权密钥

输入6-32位大小写字母、数字构成的密钥 [随机生成](#)

签名参数

输入 1-100 位大小写字母、数字、下划线构成的参数名 (不能以数字开头)

有效时间 秒

最大可设置为 31536000

时间格式 十进制 (Unix 时间戳)

上一步
下一步

5. 完成鉴权参数配置后，需指定鉴权范围与对象：

鉴权配置
✕

✓ 选择模式 >
 ✓ 设置参数 >
 3 配置鉴权对象

鉴权范围

所有文件
 指定文件类型鉴权
 指定文件类型不鉴权

鉴权对象

请输入文件后缀名，用;分割，例如：.jpg;.html;.css

上一步
保存

鉴权计算器

说明：

您可以使用鉴权计算器来核对请求路径、签名是否计算正确。

在鉴权配置模块中，单击【鉴权计算器】，目前提供三类模式可选，选定类型并配置鉴权参数后可计算出鉴权 URL（以 **TypeA** 为例）：

鉴权计算器

鉴权模式 TypeA TypeB ⓘ TypeC TypeD

鉴权密钥
输入6-32位大小写字母、数字构成的密钥 [随机生成](#)

签名参数

访问路径

时间设置 ⓘ

时间格式 十进制 (Unix 时间戳)

有效时间 秒

[生成](#)

注意：

- TypeB 功能升级中，暂无法选择。
- 若访问路径是包含有中文的 URL，您需要先进行 URL 编码转义后再进行鉴权配置。

HTTP Header 配置

最近更新时间：2019-07-16 12:16:48

使用腾讯云提供的 HTTP Header 配置功能，当您的用户请求业务资源时，可以在返回的**响应消息**添加您配置的头部，以实现跨域访问等目的。

当资源在节点未命中时会进行回源，此时源站返回的头部信息会一起返回给用户。当资源在节点命中缓存时，静态内容加速、下载加速场景下，CDN 默认会将缓存的源站的 Access-Control-Allow-Origin、Timing-Allow-Origin、Content-Disposition、Accept-Ranges 头部信息返回给用户。

由于 HTTP Header 配置是针对域名，因此一旦配置生效，用户对该域名下任意一个资源的响应消息中均会加入所配置头部。配置 HTTP Header 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。

配置指引

1. 登录 [CDN 控制台](#)，单击左侧菜单栏的【域名管理】，单击您所要编辑的域名右侧的【管理】。



2. 在【高级配置】中找到【HTTP Header 配置】模块，可自助添加头部。



可控制 缓存配置 回源配置 安全配置 **高级配置**

带宽封顶配置

当统计周期（5分钟）产生的带宽超出所设置阈值时，可以根据配置关闭CDN服务，或请求直接返回

带宽封顶:

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?](#)

强制跳转HTTPS:

证书来源	证书备注	到期时间
腾讯云默认证书	腾讯云默认证书	--

HTTP2.0配置

您需要先配置HTTPS证书才可开启此项配置。 [什么是HTTP2.0?](#)

HTTP2.0:

HTTP Header配置

HTTP Header配置会影响客户程序（浏览器）的响应行为。 [什么是HTTP Header?](#)

[添加HTTP Header](#)

3. 单击【添加 HTTP Header】可添加头部。

参数	取值	操作
<div style="border: 1px solid #ccc; padding: 5px;"><ul style="list-style-type: none">Access-Control-Allow-Origin<li style="background-color: #e0e0e0;">Access-Control-Allow-OriginAccess-Control-Allow-MethodsAccess-Control-Max-AgeAccess-Control-Expose-HeadersContent-DispositionContent-Language自定义</div>	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;">请仅输入 *, 或多行域名形式 (如 https://test.com), 多行域名时回车分隔</div>	
+ 新增参数		

确定 取消

CDN 提供以下常见的6类头部设置，也可支持自定义头部设置：

- Access-Control-Allow-Origin：指定跨域请求时，允许访问资源的请求来源。
- Access-Control-Allow-Methods：指定跨域请求时，允许的跨域请求方法。
- Access-Control-Max-Age：指定跨域请求时，对特定资源的预请求返回结果的缓存时间。
- Access-Control-Expose-Headers：指定跨域请求时，客户端可见的头部集合。
- Content-Disposition：激活客户端下载资源及设置默认的文件名。
- Content-Language：用于定义页面所使用的语言代码。
- 自定义：自定义头部。

通用配置

Content-Disposition

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

Content-Language 是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`

跨域配置

跨域是指某一个域名，如 `www.abc.com` 下的某资源，向另一个域名 `www.def.com` 下的某资源发起请求，此时由于资源所属域名不同，即出现 **跨域**，不同的协议、不同的端口均会造成跨域访问的出现。此时必须在 Response Header 中增加跨域相关配置，才能让前者成功拿到数据。

Access-Control-Allow-Origin

- 功能介绍

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，支持配置最多 10 个域，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。

- 操作步骤

- i. 登录 [CDN 控制台](#)，进入【域名管理】页面，选择需要设置的域名，单击【管理】。
- ii. 在【高级配置】中找到【HTTP Header 配置】模块，单击【添加 HTTP Header】可添加头部：



⚠ 注意：

支持最多10个域名配置，一个一行，每个以回车分隔。

- 匹配模式介绍

匹配模式	域值	说明
全匹配	*	设置为 * 时，则返回 response-header 中添加头部：Access-Control-Allow-Origins，且值为：*。

匹配模式	域值	说明
固定匹配	http://www.test.com https://www.test.com http://www.b.com	<ul style="list-style-type: none"> 若来源为 https://www.test.com ，在列表中命中，则返回 response-header 中添加头部：Access-Control-Allow-Origins，且值为：https://www.test.com。 若来源为 https://www.b.com ，未在列表中命中，因此返回 response-header 中无需添加头部：Access-Control-Allow-Origins。
二级泛域名匹配	http://*.test.com	<ul style="list-style-type: none"> 若来源为 http://www.test.com ，匹配，则返回 response-header 中添加头部：Access-Control-Allow-Origins，且值为：http://www.test.com。 若来源为 https://www.test.com ，不匹配，因此返回 response-header 中无需添加头部：Access-Control-Allow-Origins。
端口匹配	https://www.test.com:8080	<ul style="list-style-type: none"> 若来源为 https://www.test.com:8080 ，匹配，则返回 response-header 中添加头部：Access-Control-Allow-Origins，且值为：https://www.test.com:8080。 若来源为 https://www.test.com ，不匹配，因此返回 response-header 中无需添加头部：Access-Control-Allow-Origins。

⚠ 注意：

若存在特殊端口，则需要返回列表中填写相关信息，不支持任意端口匹配，必须指定。

Access-Control-Allow-Methods

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

Access-Control-Max-Age 用于指定预请求的有效时间。

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。

Access-Control-Max-Age 的单位为秒，设置示例如下：

```
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

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。

```
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。

自定义头部

支持添加自定义 Header，自定义 key-value 设置：

设置HTTP Header ×

参数	取值	操作
<div style="border: 1px solid #ccc; padding: 5px;"><ul style="list-style-type: none">Access-Control-Allow-Origin<li style="background-color: #e0e0e0;">Access-Control-Allow-OriginAccess-Control-Allow-MethodsAccess-Control-Max-AgeAccess-Control-Expose-HeadersContent-DispositionContent-Language<li style="border: 2px solid red;">自定义</div>	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;">请仅输入 *，或多行域名形式（如 https://test.com），多行域名时回车分隔</div>	
+ 新增参数		

确定 取消

设置HTTP Header



参数	取值	操作
<input type="text" value="自定义"/> <input type="text" value="X-test-header"/>	<input type="text" value="test"/>	
+ 新增参数		

暂不支持以下 Header 添加：

- 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**

多条 Header 重复添加时，底部优先级高于顶部优先级，由最底部配置直接覆盖。

智能压缩

最近更新时间：2019-03-15 17:09:21

开启智能压缩后，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。

默认配置

接入加速域名后，CDN 会自动启用智能压缩，默认对满足以下条件的资源进行 GZIP 压缩：

- 大小为256Byte - 2048KB范围内的资源。
- 后缀为 .js、.html、.css、.json、.shtml、.htm 的资源。

⚠ 注意：

- 新资源在第一次请求时，由于 CDN 节点无此资源，会请求回源，返回的为未压缩版本（源站未压缩），后续请求将返回节点压缩后版本。
- 智能压缩目前仅支持静态加速和下载加速两种业务类型。

配置指引

1. 登录 [CDN 控制台](#)，在左侧目录中，单击【域名管理】，进入管理页面。
2. 在列表中，找到需要配置的域名，单击操作栏中的【管理】。

域名	状态 ▾	CNAME ①	接入方式 ▾	业务类型 ▾	所属项目 ▾	操作
tesl	已关闭	无需配置	COS源	静态加速	默认项目	管理

3. 在选项卡中，单击【高级配置】。

基本配置 访问控制 缓存配置 回源配置 安全配置 **高级配置**

带宽封顶配置

当统计周期（5分钟）产生的带宽超出所设置阈值时，可以根据配置关闭CDN服务，或请求直接返回源站。 [什么是带宽封顶配置？](#)

带宽封顶:

4. 在列表底部的【智能压缩】配置模块中，您可以查看默认配置信息。

智能压缩 NEW

开启智能压缩服务，节省传输流量 [什么是智能压缩？](#)

智能压缩 [编辑](#)

压缩对象 js; html; css; xml; json; shtml; htm

文件范围 256B ~ 2048KB

压缩方式 GZIP

5. 单击【编辑】，可以按需调整压缩对象、文件大小范围及压缩方式：

- 支持指定后缀压缩。
- GZIP支持压缩范围为0 - 30MB。
- Brotli压缩功能升级中，暂不支持开启。

智能压缩配置 ×

文件类型

请输入文件后缀，用 ; 分隔，例如：.jpg; .html; .css

压缩范围 ~

设置大小区间，指定范围内将压缩后传输

压缩方式 GZIP Brotli

6. 如您不需要此项配置，单击【关闭】，即可关闭智能压缩配置。

智能压缩 NEW

开启智能压缩服务，节省传输流量 [什么是智能压缩？](#)

智能压缩 [编辑](#)

压缩对象 js; html; css; xml; json; shtml; htm

文件范围 256B ~ 2048KB

压缩方式 GZIP

权限管理

权限说明

最近更新时间：2019-01-29 14:54:14

CDN 已经接入了腾讯云云资源访问管理 (Cloud Access Management) 系统，您可以在 [访问管理](#) 控制台进行用户组、用户、角色、策略等一系列相关管理操作。

由于 CDN 目前处于权限系统升级过渡阶段，您可以通过以下几种方式为您的子用户和角色分配 CDN 管理权限。

默认策略

目前 CDN 可适配的默认策略如下：

- AdministratorAccess：关联了此策略的子用户，可以管理账户内含 CDN 服务在内的所有云服务资产、财务相关信息、用户及权限。
- QCloudResourceFullAccess：关联了此策略的子用户，可以管理账户内含 CDN 服务在内的所有云服务资产。

项目权限

项目管理授权

CDN 支持按项目分配权限，即设置项目管理员。通过创建【项目管理】策略，分配项目，子用户可拥有该项目中所有 CDN 资源的管理权限，创建步骤如下：

1. 单击【按产品功能或项目权限创建】。
2. 为策略命名，并在服务类型中单击【项目管理】。
3. 开启【管理 CDN 业务项目内云资源】。
4. 关联指定项目。

上述策略创建完成并关联子用户后，被关联的子用户可以操作此项目内所有云资源（包括 CDN）。

功能 - 项目授权

CDN 支持按照预设的功能集，进行项目级别的授权操作。通过创建【内容分发网络】服务策略，子用户可以拥有该项目指定功能的权限，创建步骤如下：

1. 单击【按产品功能或项目权限授权】。
2. 为策略命名，并在服务类型中单击【内容分发网络】。
3. 开启所需功能集合，如【查看消耗数据及统计量】。

4. 关联指定项目。

上述策略创建完成并关联子用户后，被关联的子用户可以通过以下接口，查询项目内的资源（域名）对应的统计数据。

API 注意事项

CDN 目前对外提供的接口大部分为 API2.0 接口，进行项目级别的资源授权的子用户，仅可调用以下 API 接口进行相关操作。未在列表中的 API 接口暂不支持子用户调用。

权限集合	API2.0	API3.0	是否需要授权
查询消耗数据及统计量	DescribeCdnHostInfo DescribeCdnHostDetailedInfo GetCdnStatusCode GetCdnStatTop GetCdnProvIspDetailStat	DescribeCdnData DescribeOriginData ListTopData DescribeIpVisit	是
查询域名信息	GetHostInfoById GetHostInfoByHost	暂未上线	是
查询 CDN 日志下载链接	GenerateLogList GetCdnLogList	暂未上线	是
添加域名	AddCdnHost	暂未上线	是
上线/下线域名	OnlineHost OfflineHost	暂未上线	是
删除域名	DeleteCdnHost	暂未上线	是
修改域名配置	UpdateCdnConfig	暂未上线	是
刷新预热	RefreshCdnDir RefreshCdnUrl GetCdnRefreshLog CdnPusherV2 GetPushLogs CdnOverseaPushser	暂未上线	是
服务查询	QueryCdnIp	暂未上线	否

控制台注意事项

- 查看消耗数据及统计量：若策略开启了【查看消耗数据及统计量】并关联项目，则可查看控制台以下模块信息：

- 概览页
- 统计分析：实时监控
- 统计分析：数据分析
- 全网数据监控
- 查询域名信息：若策略开启了【查询域名信息】并关联项目，则在控制台【域名管理】页面查看有权限的项目中域名列表及详细配置信息。
- 查询 CDN 日志下载链接：若策略开启了【查询 CDN 日志下载链接】并关联项目，则在控制台【日志管理】页面，可查询访问日志下载链接。
- 添加域名：若策略开启了【添加域名】并关联项目，则可向指定项目中添加域名。
- 上线/下线域名：若策略开启了【上线/下线域名】并关联项目，则可上线/下线指定项目中的加速域名。
- 删除域名：若策略开启了【删除域名】并关联项目，则可删除指定项目中的加速域名，删除域名需要为下线状态。因此若需要删除一个上线状态的域名，需要具备【上线/下线域名】权限。
- 修改域名配置：若策略开启了【修改域名配置】并关联项目，则可以修改指定项目中的加速域名配置。

⚠ 注意：

在控制台【证书管理】页面，可以修改对应 HTTPS 配置，API 2.0 接口暂不支持。

- 刷新预热：若策略开启了【刷新预热】并关联项目，则可以在【刷新缓存】页面提交对应的刷新、预热（白名单）任务，并查询刷新预热任务的执行状态。

⚠ 注意：

预热目前尚未全量开放，仅部分内测中用户可见。

域名权限

为方便用户更加细粒度的配置域名查询、管理权限，CDN 系统目前在进行权限策略的升级，将逐步支持策略语法能力，用户可通过自定义策略语句，实现域名级别的权限分配。

目前新增的 API3.0 接口及新版的统计分析控制台，已经全面支持策略语法，对应的 Action 如下：

- DescribeCdnData：查询域名访问监控数据，带宽、流量、流量命中率、请求数、状态码、响应时间等实时指标，支持1分钟粒度；对应控制台【统计分析】中实时监控页面，访问监控页面数据。
- DescribeOriginData：查询域名回源监控数据，回源带宽、回源流量、回源请求数、回源失败率、回源状态码等实时指标，支持1分钟粒度；对应控制台【统计分析】中实时监控页面，回源监控页面数据。
- ListTopData：支持多条件组合排序结果查询，如指定时间区间、按域名流量从大到小排序，或指定时间区间、按 URL 流量从大到小排序能；对应控制台【统计分析】中相关列表部分。

- DescribeVisit：支持 IP 活跃查询，5分钟粒度活跃 IP 查询及天粒度日活跃数据查询；对应控制台【数据分析】页面中对应模块。

策略语法

使用策略语法授权域名权限时，语法如下：

```
{
  "version": "2.0",
  "statement": [
    {
      "action": [
        "*"
      ],
      "resource": [
        "qcs::cdn::uin/987654321:domain/www.test.com"
      ],
      "effect": "allow"
    }
  ]
}
```

语法说明

- action：表示需要授权的 Action，仅支持 DescribeCdnData、DescribeOriginData、ListTopData、DescribeVisit 这4个 Action 授权，详情请参见 [域名权限](#)。
- resource：表示需要授权的对象，对 CDN 服务而言，仅支持域名级别的授权，格式需要按示例所示。
- effect：授权允许，即允许对 resource 调用 action，可配置为 deny，即禁止对 resource 调用 action。
- statement 允许配置多条，当域名存在重复配置 deny 与 allow 时，deny 优先。

⚠ 注意：

- 策略语法仅支持上述 DescribeCdnData、DescribeOriginData、ListTopData、DescribeVisit 这4个 Action 授权，详情请参见 [域名权限](#)。因此若配置为 *，则表示对这几个 Action 均做授权。
- 允许同时按照项目授权、策略语法进行域名级别授权。若授权了项目 A 的数据访问权限，在策略语法中又拒绝了项目 A 中 a 域名的数据查询权限，则没有项目 A 的权限，但是有项目 A 下其他域名权限。