全站加速网络

配置管理

产品文档

腾讯云

文档目录

配置管理

配置概览

最近更新时间：2020-03-13 16:24:50

本文提供 ECDN 常见配置指引，您可以根据自身业务需要进行设置，优化您的 ECDN 加速效果。

基本配置

配置名称	文档内容概述
快速入门	提供产品服务自助开通和域名快速接入操作指引。
域名接入配置	提供将域名接入 ECDN 加速的详细操作指引。
CNAME 配置	提供域名 CNAME 配置指导。
域名状态切换	提供启动、关闭、删除域名加速服务等操作的指导。
项目配置	提供修改域名所属项目、加速区域指导说明。
源站配置	提供修改源站类型为源站 IP 或源站域名说明。

高级配置

配置名称	文档内容概述
HTTPS 设置	支持配置 HTTPS 实现安全加速。
HTTP Header 配置	支持添加 HTTP Header 配置，影响浏览器的响应行为。
缓存规则配置	支持为动静内容混合域名配置静态缓存策略。
告警监控配置	支持对加速服务进行监控及告警。
高级回源配置	支持分权重、分主备高级回源策略。

基本配置

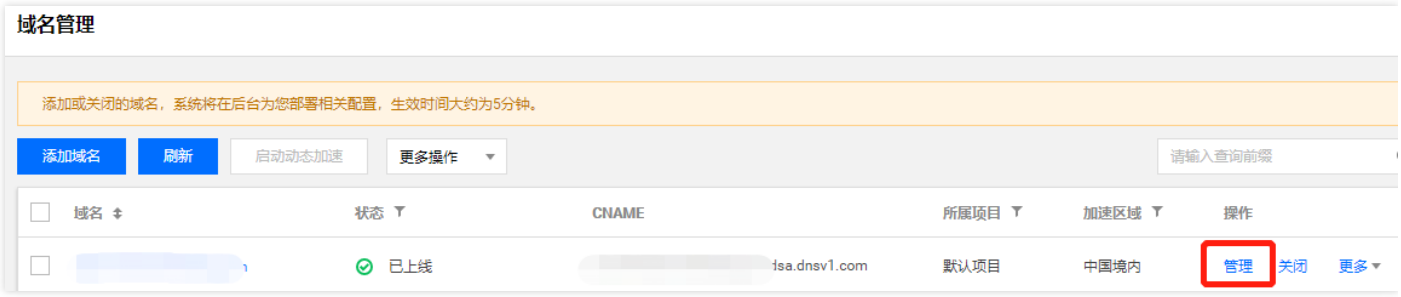
最近更新时间：2020-07-06 11:01:22

您可以在 ECDN 控制台中查看域名的基本信息和源站信息，然后根据需要对域名 **所属项目**、**源站类型** 和 **源站地址** 进行修改。

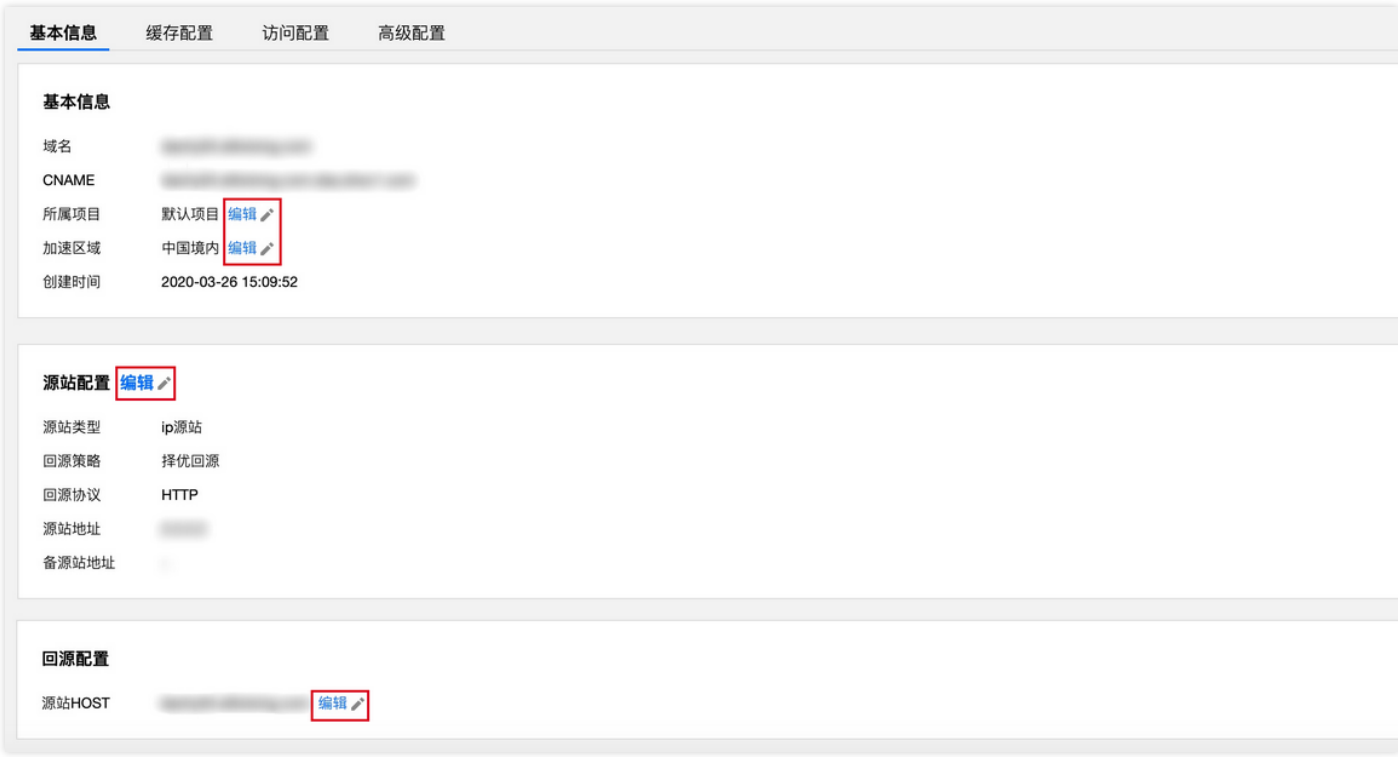
- 基本信息包括：加速域名、CNAME、所属项目及加速服务创建时间。
- 源站信息包括：源站类型和源站地址。

域名配置页面

1. 登录 ECDN 控制台，单击左侧菜单栏的【域名管理】，进入管理页面。
2. 单击您要配置的域名右侧的【管理】，进入域名配置页面。



3. 域名【基本信息】页面展示域名基本配置信息，包括域名 CNAME、所属项目、加速区域、源站信息、回源 HOST 等。



基本配置项目

修改域名所属项目

1. 单击所属项目右侧【修改】。
2. 在弹出的项目列表框中，选择合适的项目名称，单击【确认】提交。

修改域名加速区域

1. 单击加速区域右侧【修改】。
2. 选择域名加速区域，加速区域目前支持中国境内、中国境外和全球选项。
3. 为了避免操作失误，当您需要删除某个加速区域配置时，请提交 需求工单 进行修改。

> 说明：
> 中国境外加速服务限量开放中，若您的账号无法修改加速区域，表示您还未获得中国境外加速权限。您可以通过 ECDN 全球加速资格申请页面 提交申请，系统将在5个工作日内完成审批，并通过短信和站内信通知您。

修改源站配置

1. 单击源站配置右侧修改按钮进入源站修改页面。
2. 在弹框中，修改您的源站类型、回源策略和源站地址信息，如有需要，请查看 高级回源策略说明。
3. 修改完成后，单击【确认】提交，系统后台将为域名下发新的源站配置，预计约3 - 5分钟生效。

修改回源配置

单击源站 HOST 后面的【编辑】，在对话框中修改回源 HOST：


修改源站HOST
回源HOST
回源HOST是回源时在源站访问的站点域名。什么是回源HOST?
请保证您的配置的回源HOST域名能支持访问，否则会导致回源失败
确定
取消

缓存配置

最近更新时间：2020-07-06 11:14:32

功能介绍

ECDN 将根据您配置的规则自动识别动静态内容访问请求，智能地选择合适的加速方案，一站式满足动静内容混合站点的访问加速需求。

- 对于静态内容请求，优先采用边缘节点缓存内容响应，提升访问效果，降低回源流量。
- 对于动态内容请求，直接通过智能路由和优质资源快速回源，降低平均响应时延。

功能配置指导

1. 登录 ECDN 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，在右侧操作栏下单击【管理】，进入域名配置管理页面。
3. 在“缓存配置”页面下，进行内容缓存规则配置管理。
   - 过滤参数缓存配置：
     开启过滤参数缓存开关，可在缓存时对用户请求 URL 中 “?” 之后的参数进行过滤。例如，URL 为： `http://www.example.com/1.jpg?version=1.1` 的资源，节点存储资源时，对应的 cache_key 为 `www.example.com/1.jpg` ，忽略了 "?" 之后的参数。当用户请求时 ，也将忽略"?"后参数，按照 cache_key为 `www.example.com/1.jpg` 查找资源，可直接命中。

   - 内容缓存配置：
     单击【编辑缓存规则】，可添加新的缓存规则或对现有规则进行修改，单击【保存】，规则生效。

缓存规则类型

缓存类型	类型说明	设置举例	注意事项
文件类型	根据文件后缀类型设置缓存时间	.jpg;.png;.jsp	1. 内容区分大小写，必须是以“.”开头的文件后缀。 2. 不同文件类型使用“;”隔开。
文件夹	根据文件夹设置缓存时间	/access;/pic	1. 内容区分大小写，不同路径使用“;”隔开。 2. 必须是以“/”开头的文件夹。 3. 内容不能以“/”结尾。
全路径文件	为指定的文件设置缓存时间	/a.jpg;/b.png	1. 内容区分大小写，不同路径文件使用“;”隔开。 2. 支持“*”正则匹配某一类型文件，如“/test/abc/*.jpg”。 3. 必须是以“/”开头的文件夹。
首页	指定首页设置缓存时间	/	首页缓存的内容默认为“/”，无需修改。

缓存刷新时间

缓存刷新时间说明

- 缓存刷新时间支持按秒、分、小时、天设置，最长缓存刷新时间不超过30天。
- 缓存刷新时间等于0时，表示为动态内容，所有请求直接透传回源，并且响应内容不作缓存处理。
- 缓存刷新时间大于0时，表示为静态内容，开启边缘缓存功能：
  - 当用户访问的内容已经在边缘节点缓存，且缓存时间未过期，则本次请求无需回源，直接使用缓存内容响应，让用户就近获取访问内容。
  - 当用户访问的内容未在边缘节点缓存，或缓存内容已过期，则本次请求需回源获取内容响应给用户，并缓存在节点。
- 域名接入时，默认所有文件的缓存刷新时间为0秒，表示默认不采用动态加速服务。

缓存刷新时间设置建议

文件类型	场景示例	缓存时间建议
基本不更新的静态内容	图片文件、音视频文件	缓存刷新时间设置为30天。
需要频繁更新的静态内容	js、css 等类型文件	按照更新周期设置缓存时间，一般可以按天或小时级别设置缓存时间。
频繁更新的，且允许用户共享访问的动态内容	天气查询、分地区门户内容	设置分钟或秒级别缓存时间。
动态生成的，或不允许用户重复访问的内容	用户注册、登录接口	不缓存，缓存刷新时间设置成0秒。

缓存规则优先级

当您设置了多条缓存策略时，规则之间可能会有重复，导致同一请求可能符合多条设置规则，因此我们对缓存规则设置了优先等级。

- 配置列表底部的优先级高于列表顶部优先级，新增的缓存规则默认设置最高优先等级。
- 用户请求按照规则优先等级从高到低匹配，首次命中的缓存规则决定了该次请求的缓存刷新时间。
- 您可以通过调整优先级设置调整不同规则的优先等级。

单击【编辑缓存规则】，通过**鼠标拖拽小图标**的方式调整缓存规则优先等级。

缓存继承问题

当您设置静态内容使用边缘缓存功能时，ECDN 系统将默认以平台配置的缓存规则处理用户静态请求，源站 Response Header 中存在的 Cache-Control 字段节点默认不继承处理。但是如果源站 Cache-control 字段为 private、no-store 或 no-cache，此时 ECDN 节点对此资源不做缓存。

访问配置
IP 访问限频配置

最近更新时间：2020-06-30 17:24:21

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 ECDN 为您提供了 IP 访问限频配置。通过对用户端 IP 在每一个节点每一秒钟访问次数进行限制，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 ECDN 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，【访问配置】中可看到 IP 访问限频配置，默认情况下配置为关闭状态：

修改配置

1. 修改配置

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。

2. 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：

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 ECDN 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 ECDN 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。

IP 黑白名单配置

最近更新时间：2020-06-30 17:24:16

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 ECDN 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 ECDN 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，【访问配置】中可看到 IP 黑白名单配置：

修改配置

1. 修改配置

单击【编辑】，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 ECDN 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 ECDN 节点时将直接返回403状态码。

名单规则

- IP 黑名单与 IP 白名单二选一，不可同时配置。
- IP 段仅支持 /8、/16、/24、/32 网段，不支持其他网段。
- 不支持 `IP：端口` 形式的黑白名单，名单最多可输入50个。

配置示例

若加速域名 www.test.com 的 IP 黑白名单配置如下：

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，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。

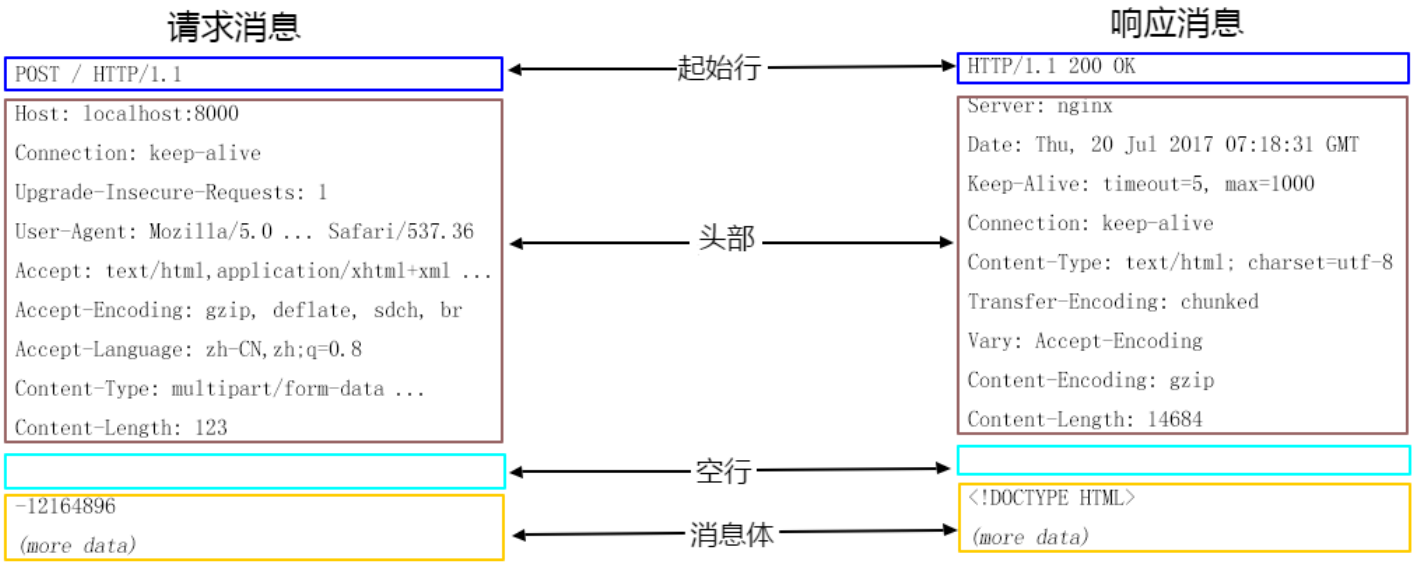
高级配置
HTTP Header 配置

最近更新时间：2020-07-06 11:27:38

HTTP 的消息通常包括：

- 客户端向服务端发送的请求消息。
- 服务端向服务端发送的响应消息。

以上几种类型的消息均由一个起始行，一个或多个头部，一个标明头部结束的空行和可选的消息体组成。



其中 HTTP 头部分为：通用头、请求头、响应头、实体头。每一个头部由域名、冒号（:）、域值组成，如：`Connection:keep-alive` 。
使用腾讯云 ECDN 提供的 HTTP Header 配置功能，当您的用户请求业务资源时，会在返回的**响应消息**中添加您配置的头部，以实现跨域访问等目的。

注意：

- 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 ECDN 节点的缓存行为。

配置说明

ECDN 提供以下几种头部的配置：

- Content-Disposition：激活客户端下载资源及设置默认的文件名。
- Content-Language：指定资源在客户端（如浏览器）响应的语言。
- 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。

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。常用配置：`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，才能让前者成功获得数据。

Access-Control-Allow-Origin

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，也可以设置通配符“*”，允许被所有域请求。常用配置如下：

- `Access-Control-Allow-Origin: *`
- `Access-Control-Allow-Origin: http://www.test.com`

配置 Access-Control-Allow-Origin，有以下限制条件：

- 不支持泛域名，如 `*.qq.com`。
- 仅可配置为“*”，或指定一个 URI。

- 在配置指定域名时，需要加上 “http://” 或 “https://” 前缀。

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 以外的方式发起的请求，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： `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 指定跨域请求时，允许访问的头部信息。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：
`Access-Control-Expose-Headers: Content-Length，QCloud-DSA-MyCustom-HeaderY`

那么服务器就会允许请求中包含 Content-Length，QCloud-DSA-MyCustom-HeaderY 这两个字段。

自定义头部

ECDN 支持用户添加自定义头部，您可以根据业务需要，添加自定义头部字段。
以下字段暂不支持添加：

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

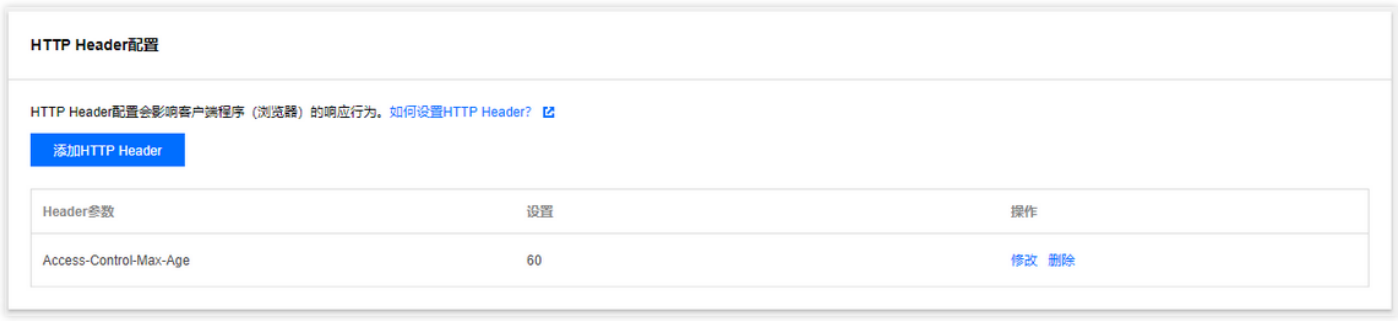
配置流程

1. 登录 ECDN 控制台，单击左侧菜单栏的【域名管理】，进入管理页面，在页面中，单击您要配置的域名右侧的【管理】，进入域名配置页面。

2. 单击【高级配置】，在 **HTTP Header 配置** 模块中单击【添加 HTTP Header】。

3. 在弹出的窗口中选择要添加的 HTTP Header，填写对应的值，单击【新增参数】可以继续添加头部字段，最后单击【确定】提交。

4. 配置生效时间约为5分钟，在下方表格中可以查看添加的 HTTP Header。单击 Header 右侧的【修改】或【删除】可以对该 Header 进行操作。



5. 您可以通过再次单击【添加 HTTP Header】继续添加 HTTP Header，每个 HTTP Header 只能添加一次。

HTTPS 设置

最近更新时间：2020-03-13 15:47:44

配置说明

HTTPS 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 ECDN 节点，实现全网数据加密传输功能。

> 注意：
> 您配置 HTTPS 的域名需已接入 ECDN，且状态为**部署中**或**已上线**。

配置新增

选择域名

1. 登录 ECDN 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【管理】，进入详情页后，选择【高级配置】。
3. 开启 HTTPS 功能需要先部署域名证书，单击【前往配置】进入域名证书配置页面。

配置证书

进入证书配置页面，您可以为域名配置自有证书、腾讯云托管证书或 COS 上传加速证书。域名证书配置详细流程请参见 证书管理。

注意：
COS 上传加速证书仅允许 COS 上传加速域名使用。

选择回源方式

- 选择【HTTP 回源】，ECDN 节点回源时，所有请求将全部采用 HTTP 协议。
- 选择【协议跟随】，ECDN 节点的回源方式将遵循用户的请求方式，即 HTTP 请求采用 HTTP 协议回源，HTTPS 请求采用 HTTPS 协议回源。

配置修改

- **开启 HTTP2.0 功能**
  已配置证书的域名，可以在高级配置页面开启HTTP2.0功能。
- **开启 HTTPS 强制跳转功能**
  已配置证书的域名，可以开启 HTTPS 强制跳转功能，功能开启后，所有 HTTP 请求将强制跳转成 HTTPS 请求。
  开启HTTPS强制跳转，您还可以指定使用301或302状态码跳转，默认使用302状态码。
- **修改证书及回源方式**
  已配置证书的域名，可以单击【前往配置】，进入证书管理页面，修改证书内容或修改回源方式。

告警监控配置

最近更新时间：2020-07-06 11:31:01

ECDN 接入云监控系统说明

ECDN 已正式接入腾讯云监控系统，当前版本支持的告警指标包括：

指标类别	详细指标	1分钟告警粒度	5分钟告警粒度
访问流量相关指标	总请求次数	支持	支持
	访问带宽	支持	支持
	访问流量（上行）	支持	支持
	访问流量（下行）	支持	支持
回源流量相关指标	总回源次数	支持	支持
	回源失败次数	支持	支持
	回源失败率	支持	支持
	回源带宽	支持	支持
访问性能相关指标	平均响应时间	支持	支持
状态码相关指标	200，206，2XX 等状态码次数及占比	支持	支持
	302，304，3XX 等状态码次数及占比	支持	支持
	401，403，404，416，4XX 等状态码次数及占比	支持	支持
	500，502，5XX 等状态码次数及占比	支持	支持

说明：

- 您可以免费开通和使用腾讯云监控服务。
- 系统免费通过邮件、微信和回调接口发送告警信息，并且您每月还享有免费的短信告警配额。
- 当超出当月免费告警短信额度后，需要购买短信配额才可以继续通过短信接收告警信息。
- 告警数据实时采集上报，具有一定数据偏差，数据延迟时长约5分钟。

- 监控告警数据仅可用于辅助运营，不可作为计费或 SLA 依据。

监控配置入口

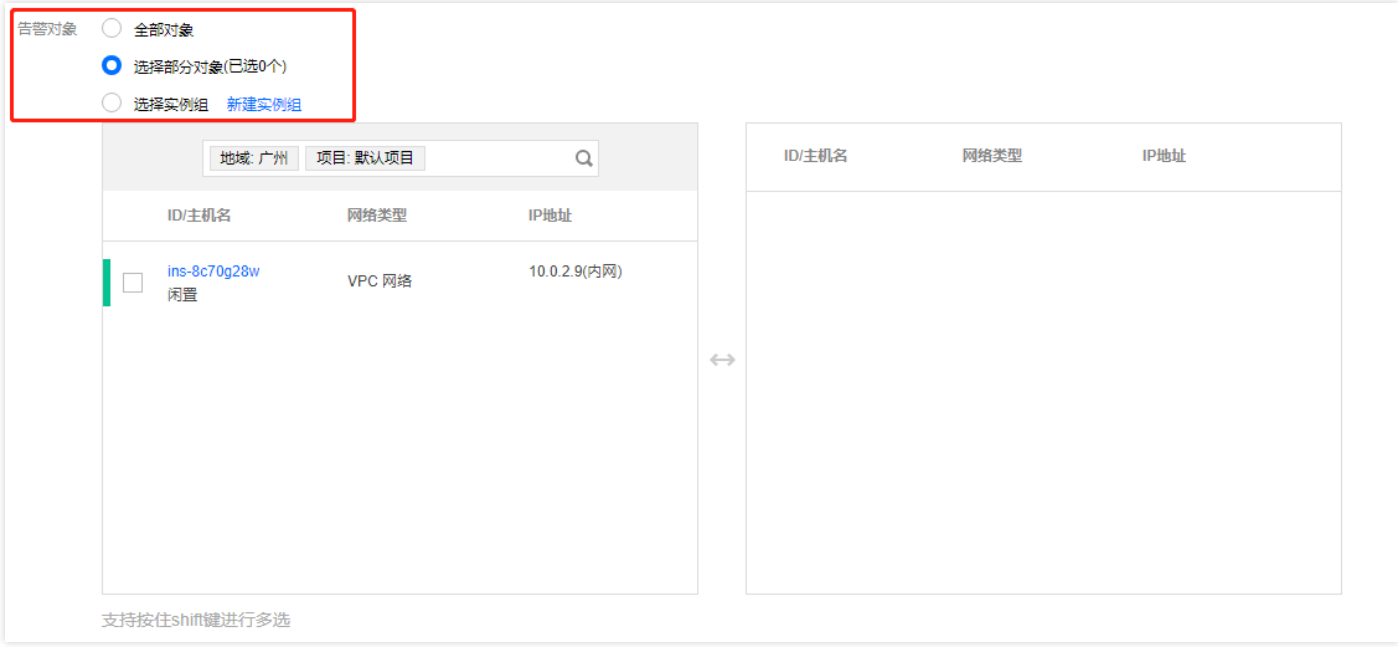
登录 云监控控制台，在左侧目录中，单击【告警策略】，进入管理页面。

新增告警配置

新增告警策略配置步骤如下图所示。

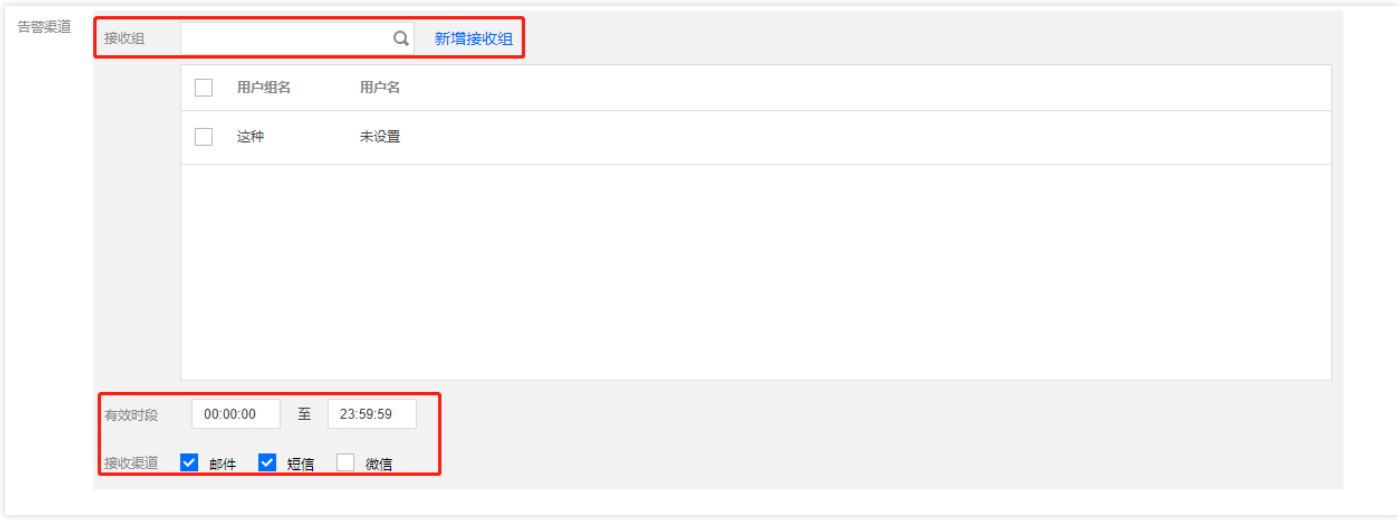
1. 填写策略名称、备注提示并选择 ECDN 动态加速告警策略类型。

2. 选择告警对象。



3. 设置告警触发条件，您可以同时设置多条触发条件。

4. 设置告警接收对象、告警时间段和告警方式。

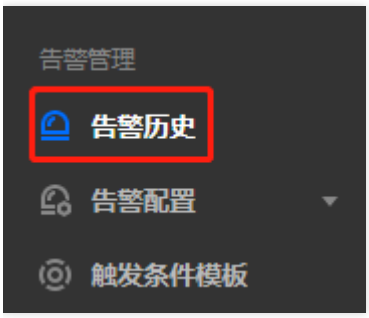


5. 设置告警回调接口。

6. 单击【完成】，确认提交。

查看告警

在云监控告警历史页面，您可以查看详细告警信息列表。



其他告警策略

告警策略更多配置说明，请参见 创建告警策略 文档。