ALIBABA CLOUD

阿里云

CDN

域名管理

文档版本：20200828

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	**单击设置> 网络> 设置网络类型。**
粗体	表示按键、菜单、页面名称等UI元素。	**在结果确认页面，单击确定。**
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.功能概述 07
2.批量复制 12
3.设置报警 14
4.标签管理 15
4.1. 概述 15
4.2. 绑定标签 15
4.3. 解绑标签 17
4.4. 使用标签管理域名 17
4.5. 使用标签筛选数据 18
4.6. 案例介绍 19
5.配置源站 21
5.1. 概述 23
5.2. 修改基础信息 23
5.3. 配置源站 24
6.回源配置 27
6.1. 概述 27
6.2. 配置回源HOST 27
6.3. 配置回源协议 29
6.4. 开启阿里云OSS私有Bucket回源授权 30
6.5. 关闭私有Bucket回源授权 31
6.6. 配置回源SNI 32
6.7. 配置自定义回源HTTP头 34
6.8. 配置回源请求超时时间 35
6.9. 改写回源URI 36
6.10. 改写回源参数 39
6.11. 配置回源HTTP请求头(新) 41

6.12. 配置回源HTTP响应头(新) 46
7.缓存配置 51
7.1. 概述 51
7.2. 配置缓存过期时间 52
7.3. 配置状态码过期时间 54
7.4. 配置HTTP头 55
7.5. 自定义页面 57
7.6. 配置重写 59
8.HTTPS配置 62
8.1. 什么是HTTPS加速 62
8.2. 证书格式说明 66
8.3. 配置HTTPS证书 69
8.4. 设置HTTP/2 72
8.5. 配置强制跳转 73
8.6. 配置TLS 75
8.7. 配置HSTS 76
8.8. 设置OCSP Stapling 78
8.9. 常见问题 81
9.访问控制 83
9.1. 概述 83
9.2. 配置Referer防盗链 83
9.3. URL鉴权配置 85
9.3.1. URL鉴权 85
9.3.2. 鉴权方式A说明 87
9.3.3. 鉴权方式B说明 89
9.3.4. 鉴权方式C说明 91
9.3.5. 鉴权示例 93
9.4. IP黑白名单 95

9.5. 配置UA黑/白名单 97
9.6. CDN的安全防护功能 100
10.性能优化 101
10.1. 概述 101
10.2. 页面优化 101
10.3. 智能压缩 102
10.4. 过滤参数 102
10.5. Brotli压缩 105
10.6. 自定义图片转换 106
11.视频相关 109
11.1. 概述 109
11.2. 配置Range回源 109
11.3. 拖拽播放 110
11.4. 听视频 112
11.5. 音视频试看 113
11.6. M3U8标准加密改写 114
12.安全配置 117
12.1. 配置WAF防护 117
12.2. 配置频次控制 119
12.3. 配置CDN联动DDoS高防 123
12.4. 区域封禁 125
13.高级配置 127
13.1. 概述 127
13.2. 配置带宽封顶 127
14.IPv6配置 129
15.域名管理FAQ 130

1.功能概述

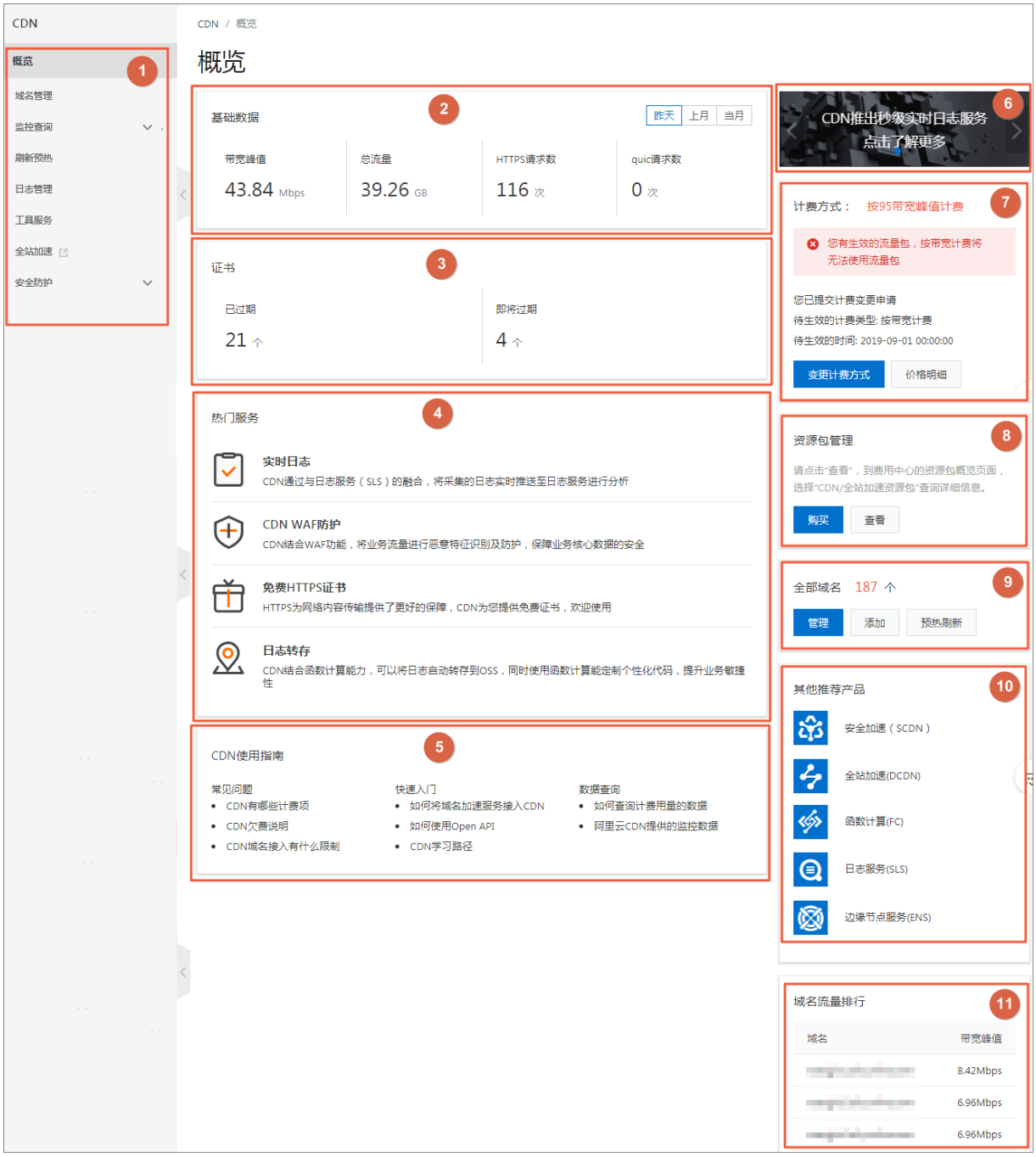
阿里云CDN控制台不仅可以帮助您完成域名配置等基本操作，也提供了实时数据分析的资源监控服务。同时您还可以了解自己的计费情况，随时变更计费方式。通过本文为您可以了解CDN控制台界面展示和域名管理功能。

阿里cdn库cdn列表cdn提供的页面选项

> 说明 为了便于您对CDN产品的学习和理解，本文档从业务角度将CDN控制台支持的功能划分为：域名管理和服务管理。

控制台指引

CDN控制台界面展示如下图所示。



CDN控制台界面说明如下表所示。

序号	区域	说明
1	左侧导航栏	CDN域名导航栏。详细功能介绍，请参见域名管理功能列表。
2	基础数据	CDN根据您服务的计费方式，展示计费项中的使用数据。详细功能介绍，请参见基础服务计费。
3	HTTPS证书	您可以查看已过期和即将过期的HTTPS证书。请参见配置HTTPS证书。
4	热门服务	CDN为您展示使用频率高的服务的快速快口。

序号	区域	说明
5	CDN使用指南	您可以查阅CDN相关的使用指南。如果您想了解更多，请参见CDN学习路径。
6	实时日志推送服务	实时日志推送服务快速入口。详细功能介绍，请参见配置实时日志推送。
7	计费方式	您已选择的计费方式。您也可根据所需快速修改计费方式。详细功能介绍，请参见基础服务计费和增值服务计费。
8	资源包	您已购买的资源包。详细功能介绍，请参见资源包。
9	全部域名	您可以通过快速入口对域名进行管理，并执行添加和刷新预热操作。
10	其他加速产品	您可以了解与CDN相关的其他产品。
11	域名流量排行	您可以了解流量排行前五的域名。

域名管理功能列表

CDN域名管理功能列表如下表所示。

功能	参考文档	说明	默认值
批量复制	批量复制	将某一个加速域名的一个或多个配置，复制到另外一个或多个域名上。	无
设置报警	设置报警	监控CDN域名的带宽峰值、4xx5xx返回码占比、命中率、公网下行流量和QPS监控项。当报警规则被触发时，阿里云监控会根据设置通过短信和邮件发送报警信息。	无
标签管理	绑定标签	标记域名或为域名分组。	无
	使用标签管理域名	使用标签快速筛选域名，进行分组管理。	无
	使用标签筛选数据	使用标签快速筛选域名，查询相关数据。	无
基本信息	修改基础信息	修改加速区域。	无
	配置源站	修改源站配置。	无
回源设置	配置回源HOST	修改回源HOST域名。	开启
	配置回源协议	CDN根据设定的协议规则回源。回源使用的协议和客户端访问资源的协议保持一致。	未开启
	开启阿里云OSS私有Bucket回源授权	开通加速域名访问私有bucket资源内容的权限。	未开启
	配置回源SNI	当源站IP绑定多个域名，且CDN节点以HTTPS协议访问源站时，设置回源SNI，指明具体访问域名。	关闭
	配置自定义回源HTTP头	当HTTP请求回源时，可以添加或删除回源HTTP头。	关闭

功能	参考文档	说明	默认值
	配置回源请求超时时间	根据实际需求设置CDN回源请求超时的最长等待时间。当回源请求等待时间超过配置的超时时间时，CDN节点与源站的连接断开。	30秒
缓存配置	配置缓存过期时间	自定义指定资源的缓存过期时间规则。	无
	配置状态码过期时间	配置资源的指定目录或文件后缀名的状态码过期时间。	无
	配置HTTP头	配置HTTP请求头，目前提供10个HTTP请求头参数可供自行定义取值。	无
	自定义页面	根据所需自定义HTTP或者HTTPS响应返回码跳转的完整URL地址。	404
	配置重写	对请求的URI进行修改和302重定向至目标URI。	无
HTTPS安全加速	配置HTTPS证书	提供全链路HTTPS安全加速方案，仅需开启安全加速模式后上传加速域名证书/私钥，并支持对证书进行查看、停用、启用、编辑操作。	关闭
	设置HTTP/2	二进制协议带来更多扩展性、内容安全性、多路复用、头部压缩等优势。	未开启
	配置强制跳转	加速域名开启HTTPS安全加速的前提下，支持自定义设置，将原请求方式进行强制跳转。	未开启
	配置TLS	TLS协议版本开启后，加速域名开启TLS握手。目前只支持TLSv1.0、TLSv1.1、TLSv1.2和TLSv1.3版本。	关闭
	配置HSTS	HSTS的作用是强制客户端（如浏览器）使用HTTPS与服务器创建连接。	关闭
访问控制	配置Referer防盗链	通过配置访问的Refer黑名单和白名单来实现对访客身份的识别和过滤，从而限制访问CDN资源的用户。	未开启
	URL鉴权	通过配置URL鉴权来保护用户站点的资源不被非法站点下载盗用。	未开启
	IP黑白名单	通过配置IP黑名单和白名单来实现对访客身份的识别和过滤，从而限制访问CDN资源的用户。	未开启
	配置UA黑/白名单	通过配置User-Agent黑名单和白名单来实现对访客身份的识别和过滤，从而限制访问CDN资源的用户。	未开启
	页面优化	压缩与去除页面中无用的空行、回车等内容，有效缩减页面大小。	未开启

功能	参考文档	说明	默认值
性能优化	智能压缩	支持多种内容格式的智能压缩，有效减少您传输内容的大小。	未开启
	Brotli压缩	对静态文本文件进行压缩时，可以开启此功能，有效减小传输内容大小，加速分发效果。	未开启
	过滤参数	当URL请求中携带 `?` 和*参数*时，CDN节点在收到URL请求后，判断是否需要携带参数的URL返回源站。	关闭
高级配置	配置带宽封顶	当统计周期（5分钟）产生的平均带宽超出所设置的带宽最大值时，为了保护域名安全，此时域名会自动下线，所有的请求会回到源站。	关闭
视频相关设置	Range回源	开启Range回源功能，可以减少回源流量消耗，并且提升资源响应时间。	关闭
	拖拽播放	开启拖拽播放功能后，当播放视音频时，随意拖拽播放进度，而不影响视音频的播放效果。	未开启
	听视频	开启听视频功能后，CDN节点会将视频文件中的音频分离，并返回给客户端，节省流量。	关闭
	音视频试看	开启音视频试看功能后，您可以试看音视频。	关闭
配置CDN WAF防护	配置WAF防护	CDN结合WAF能力，将业务流量进行恶意特征识别及防护，将正常、安全的流量回源到服务器。	未开启
IPv6	IPv6配置	开启IPv6开关后，IPv6的客户端请求将支持以IPv6协议访问CDN，CDN也将携带IPv6的客户端IP信息访问您的源站。	关闭

2.批量复制

您可以参考本文档的批量复制域名配置功能，将某一个加速域名的一个或多个配置，复制到另外一个或者多个域名上。通过本文档您可以了解批量复制域名配置的操作方法。

CDN批量复制

前提条件

您在进行批量复制前，请确保已经启用并配置了您想复制的域名，否则将无法批量复制。

背景信息

您在批量复制某个域名的配置时，请注意：

- 域名复制成功后，操作不可逆，请您务必确认域名配置复制正确。
- 对于流量或带宽较大的域名，请您在复制配置时谨慎操作，以免带来经济损失。
- 对于通过工单进行的后端特殊配置，请您注意该特殊配置无法复制。

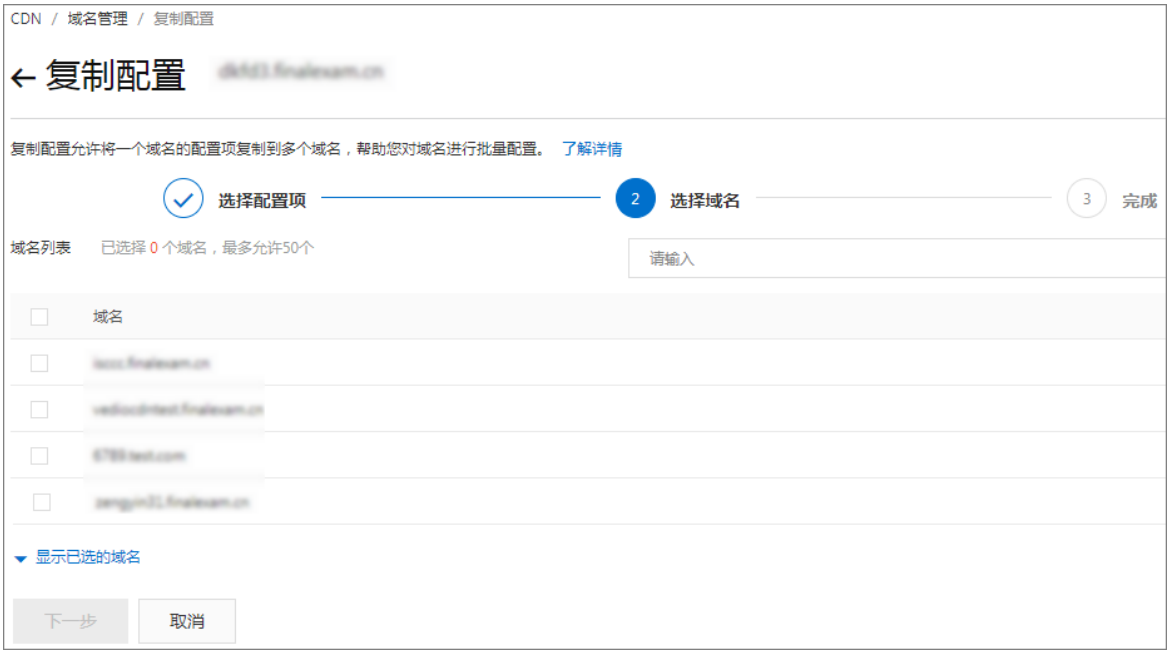
操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，选择您需要复制配置的域名，单击复制配置。

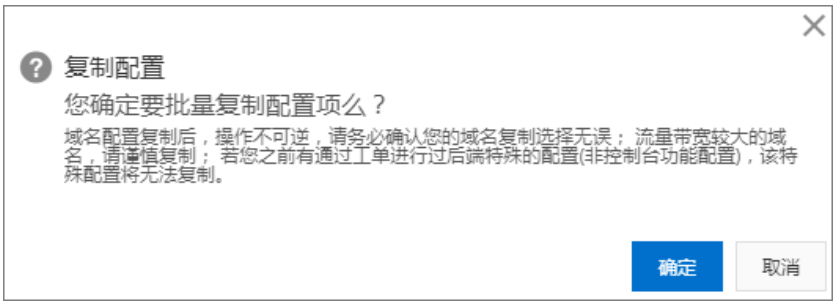
4. 勾选您需要复制的配置项，单击下一步。

> **说明**
>
> - 源站信息和非源站信息无法同时复制。
> - 您无法复制HTTPS证书到其他域名，请您单独配置。
> - 自定义回源头为增量复制。例如，您的A域名有2条回源头配置，您从B域名复制了5条内容，则您会有7条回源头配置内容。
> - HTTP头为非增量复制。例如，您的A域名配置了cache_control为private，您的B域名配置为public，复制后，您的cache_control为public。
> - 开关类的配置复制，将会覆盖域名原有的配置。
> - Referer或IP黑白名单将会覆盖域名原有配置。

5. 勾选您想要批量配置的目标域名，单击**下一步**。 您可以输入关键词查找域名。



6. 在**复制配置**对话框，单击**确定**。



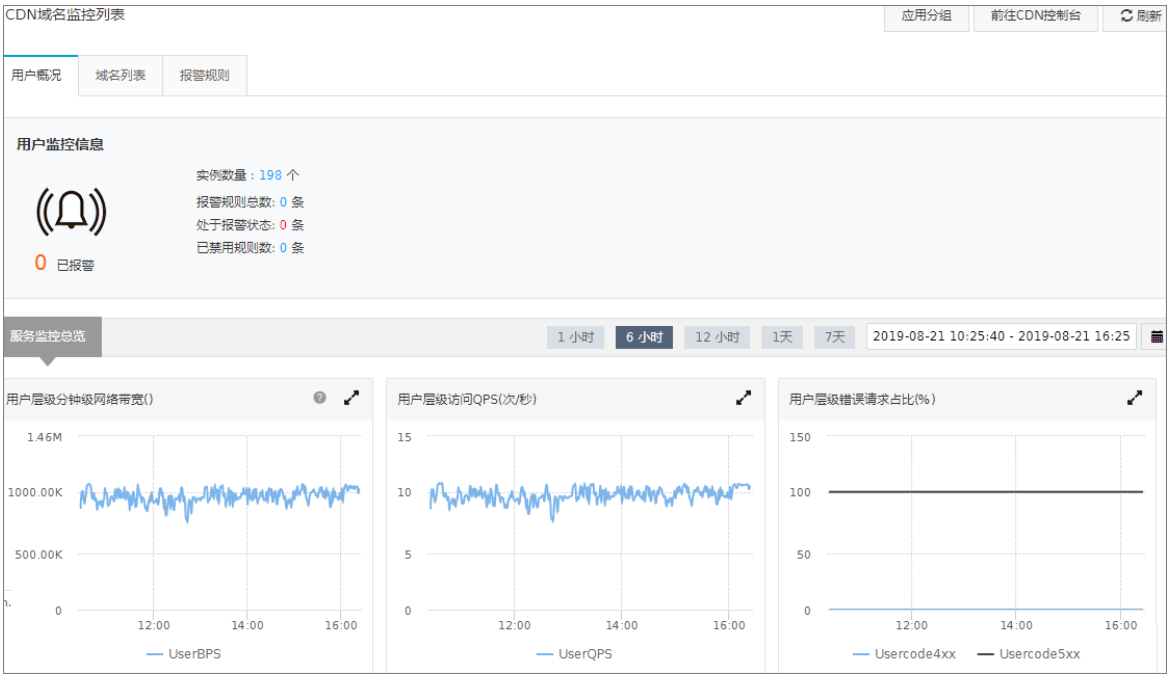
3.设置报警

当您需要监控CDN域名的带宽峰值、4xx5xx返回码占比、命中率、下行流量、QPS等监控项时，您可以直接在阿里云的云监控控制台设置报警规则。当报警规则被触发时，阿里云监控会根据您设置的短信、邮件等通知方式给您发送报警信息。

报警规则 CDN

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击报警设置，跳转到云监控控制台。



4. 选择云监控服务 > CDN，单击报警规则页签。
5. 单击创建报警规则。
6. 创建针对CDN的报警规则，详情请参见创建阈值报警规则。
7. 单击确定。

4.标签管理

4.1. 概述

阿里云CDN不对标签进行任何定义，仅严格按字符串对标签和域名进行匹配、筛选。您可以通过标签管理功能，对加速域名进行绑定标签、解绑标签、分组管理和筛选数据。

标签管理 绑定标签 解绑标签

使用限制

标签管理的使用限制如下：

- 每个标签都由一个键值对 `Key:Value` 组成。
- 每个域名最多绑定20个标签。
- 同一个域名的标签键Key不能重复。如果对一个域名设置2个同Key不同Value的标签，新值将覆盖旧值。例如对域名 `test.example.com` 先后设置了标签 `Key1:Value1` 和 `Key1:Value2` ，则最终 `test.example.com` 只会绑定标签 `Key1:Value2` 。
- 键key不支持 `aliyun` 、 `acs:` 开头，不允许包含 `http://` 和 `https://` ，不允许为空字符串。
- 值value不允许包含 `http://` 和 `https://` ，允许为空字符串。
- 最大键key长度：64个Unicode字符。
- 最大值value长度：128个Unicode字符。
- 区分大小写。

> **说明** 如果您需要查询当前用户下的所有标签，只能通过API接口实现，请参见获取用户标签。

相关功能

您可以使用标签，对域名进行如下操作。

功能	说明
绑定标签	创建用于标记域名的用途或对域名进行分组管理的标签。
解绑标签	删除已经不再适用于您当前某个或多个域名用途的标签。
使用标签管理域名	域名绑定标签后，您可以使用标签，快速筛选对应的域名，进行分组管理。
使用标签筛选数据	域名绑定标签后，您可以使用标签，快速筛选对应的域名，查询域名数据。

4.2. 绑定标签

您可以通过标签功能为域名绑定标签，实现标记域名或为域名分组。

绑定标签域名

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 域名绑定标签。
   - 增加标签
     a. 在域名管理页面，选择您需要设置标签的域名，将光标移动到对应标签上。
     b. 在浮窗内，单击编辑。
     c. 在编辑标签对话框，您可以选择已有标签或新建标签进行绑定。

     d. 单击确定。
   - 批量增加标签
     a. 选中您需要批量增加标签的域名，选择标签管理 > 增加标签。
     b. 在批量新增标签对话框，您可以选择已有标签或新建标签新建标签进行绑定。

c. 单击**确定**完成配置。

相关API

您可以调用API接口绑定标签，请参见添加资源标签。

4.3. 解绑标签

如果标签已经不再适用于您当前某个或多个域名的用途，您可以解绑域名标签。

解绑标签 CDN

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 勾选您需要删除标签的域名，选择**标签管理 > 删除标签**。
4. 在**批量删除标签**对话框，选择您需要删除的标签，单击**确定**。

API接口

您可以调用API接口解绑标签，请参见删除资源标签。

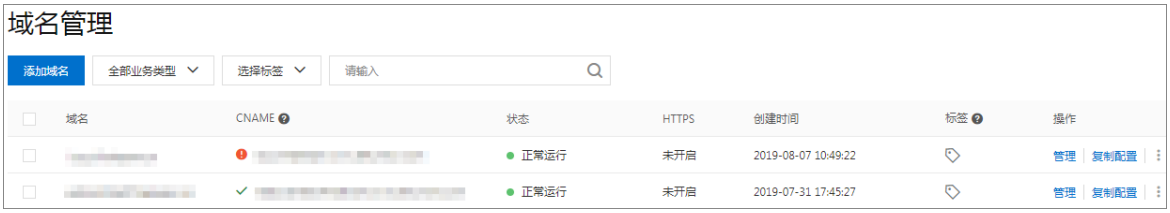
4.4. 使用标签管理域名

您可以在域名绑定标签后，使用标签快速筛选对应的域名，进行分组管理。

标签

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击选择标签。



4. 选中需要筛选的标签（可多选）进行管理。

调用接口

您可以调用API接口查询域名对应的标签，从而对域名进行管理，请参见获取资源对应的标签。

4.5. 使用标签筛选数据

如果您需要查询部分域名的数据，您可以在域名绑定标签后，使用标签快速筛选对应的域名，查询相关数据。

筛选数据 标签

操作步骤

1. 登录CDN控制台。
2. 您可以通过如下两种方式筛选并查询数据。

   > 说明 如果您同时选择多个标签，则查询的结果是各个标签对应域名的交集。

   - 在左侧导航栏，选择监控查询 > 资源监控。
     a. 在流量带宽页签，单击选择标签。
     b. 选中需要筛选的标签，单击查询。

   - 在左侧导航栏，选择监控查询 > 用量查询。
     a. 在用量查询页签，单击选择标签。
     b. 选中需要筛选的标签，单击查询。

4.6. 案例介绍

本文通过举例为您介绍如何使用标签进行域名的分组管理。

绑定标签 域名管理
某公司在阿里云CDN拥有100个域名，分属电商、游戏、文娱三个部门，服务于营销活动、游戏 A、游戏 B、后期制作等业务。公司有三位运维负责人，分别是张三、李四、王五。

设置标签

为了方便管理，该公司使用标签来分类管理对应的域名，定义了下述标签键（Key）和值（Value）。

键（Key）	值（Value）
部门	电商、游戏、文娱
业务	营销活动、游戏 A、游戏 B、后期制作
负责人	张三、李四、王五

将这些标签的键和值绑定到域名上，域名与标签键值的关系如下表所示：

域名	Key为部门，Value为	Key为业务，Value为	Key为负责人，Value为
domain1	电商	营销活动	王五
domain2	电商	营销活动	王五
domain3	游戏	游戏 A	张三
domain3	游戏	游戏 B	张三
domain4	游戏	游戏 B	张三
domain5	游戏	游戏 B	李四
domain6	游戏	游戏 B	李四
domain7	游戏	游戏 B	李四
domain8	文娱	后期制作	王五
domain9	文娱	后期制作	王五
domain10	文娱	后期制作	王五

使用标签

- 如果您想筛选出王五负责的域名，则选择标签**负责人：王五**。
- 如果您想筛选出游戏部门中李四负责的域名，则选择标签**部门：游戏**和**负责人：李四**。

5.配置源站

当您需要变更源站类型时，您可以阅读本文档，了解源站类型的修改方法，以及注意事项。

源站域名CDN

背景信息

> **注意** 您修改源站信息时，如果**源站信息**选择为**OSS域名**、**IP**或**源站域名**，则您可以根据实际情况自定义回源端口。目前CDN仅支持以HTTP协议回源到自定义端口。

阿里云CDN支持的源站类型包括OSS域名、IP、源站域名和函数计算域名。其中，IP和源站域名支持多IP或多域名设置，并支持用在多源站场景下，进行回源优先级设置。

> **说明** 源站健康检查：实行主动四层健康检查机制，探测源站的80、443或自定义端口。每2.5秒检查一次，连续3次失败标记为不可用。

CDN主要支持主备方式切换源站场景。当多个源站回源时，优先回源**优先级**为**主**的源站。如果主站连续3次健康检查均失败，则回源**优先级**为**备**的源站。如果该源站的主站健康检查成功，则该源站将重新标记为可用，恢复其优先级。当所有源站的回源优先级相同时，CDN将自动轮询回源。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**管理**。
4. 在**源站信息**区域，单击**修改配置**。
5. 在**源站配置**对话框，设置源站类型、源站地址和端口。

需要配置的参数说明如下：

> **说明**
>
> - 如果您选择的源站类型为**IP**或**源站域名**，则仍然按照外网流量价格计费。
> - 如果您选择的源站类型为**OSS域名**，即从CDN回源OSS，则按照内网的价格计费，具体价格请参见**OSS价格详情**。
> - 如果选择域名类型为**源站域名**，并设置了一个OSS的域名，则仍然按照外网流量价格计费。

- **源站类型**

源站类型	说明
IP	支持多个服务器外网IP地址。如果您使用阿里云云服务器ECS，则可以免审核ECS的IP地址。详情请参见云服务器ECS。
源站域名	支持多个源站域名。 **说明** 源站域名不能与加速域名相同，否则会造成循环解析，无法回源。例如您的源站域名为img.yourdomain.com，则加速域名可设置为cdn.yourdomain.com。
OSS域名	您可以手动输入阿里云OSS Bucket的外网域名，例如：xxx.oss-cn-hangzhou.aliyuncs.com。OSS外网域名可前往OSS控制台查看，也可直接选择同账号下的OSS Bucket。

源站类型	说明
函数计算域名	您需要选择函数计算区域和域名。设置函数计算域名的操作方法，请参见如何设置函数计算域名。

- 端口

端口	说明
80端口	资源以HTTP或HTTPS协议回源到80端口。
443端口	资源以HTTP或HTTPS协议回源到443端口。如果您的源站为单个IP地址提供多个域名服务，您需要完成配置回源操作。详情请参见配置回源SNI。
自定义端口	目前仅支持以HTTP协议回源到自定义端口。 如果您需要以HTTPS协议回源到自定义端口，则请提交工单。 注意 如果您配置了自定义端口，则请关闭协议跟随回源功能，自定义端口配置才能生效。关闭回源协议的操作方法，请参见配置回源协议。 当源站选择OSS类型时，回源端口是否支持自定义端口，取决于OSS产品。

6. 单击确定，完成配置。

5.1. 概述

阿里云CDN为你提供加速域名的基本配置功能。您可以在控制台查看加速域名的基础信息和源站信息，切换加速域名的加速区域及修改源站信息。

切换加速区域源站配置CDN

相关功能

您可以在CDN控制台进行以下基本配置：

- 修改基础信息，变更您的CDN服务范围。
- 配置源站，修改源站类型、源站地址、端口等源站信息。

5.2. 修改基础信息

当您需要变更CDN服务范围时，您可以通过切换加速区域功能实现。

加速区域 CDN

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在基础信息区域，单击修改。
5. 在加速区域对话框，选择您需要切换的加速区域。

参数	说明
仅中国内地	如果选择仅中国内地，则需要工信部备案。域名备案方法，请参见加速域名备案。
全球	如果选择全球，则需要工信部备案。域名备案方法，请参见加速域名备案。
全球（不包含中国内地）	如果选择全球（不包含中国内地），则无需工信部备案。

6. 单击确定。

5.3. 配置源站

当您需要变更源站类型时，您可以阅读本文档，了解源站类型的修改方法，以及注意事项。

源站域名CDN

背景信息

> **注意** 您修改源站信息时，如果**源站信息**选择为**OSS域名**、**IP**或**源站域名**，则您可以根据实际情况自定义回源端口。目前CDN仅支持以HTTP协议回源到自定义端口。

阿里云CDN支持的源站类型包括OSS域名、IP、源站域名和函数计算域名。其中，IP和源站域名支持多IP或多域名设置，并支持用在多源站场景下，进行回源优先级设置。

> **说明** 源站健康检查：实行主动四层健康检查机制，探测源站的80、443或自定义端口。每2.5秒检查一次，连续3次失败标记为不可用。

CDN主要支持主备方式切换源站场景。当多个源站回源时，优先回源**优先级**为**主**的源站。如果主站连续3次健康检查均失败，则回源**优先级**为**备**的源站。如果该源站的主站健康检查成功，则该源站将重新标记为可用，恢复其优先级。当所有源站的回源优先级相同时，CDN将自动轮询回源。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**管理**。
4. 在**源站信息**区域，单击**修改配置**。
5. 在**源站配置**对话框，设置源站类型、源站地址和端口。

需要配置的参数说明如下：

> 说明
> - 如果您选择的源站类型为IP或源站域名，则仍然按照外网流量价格计费。
> - 如果您选择的源站类型为OSS域名，即从CDN回源OSS，则按照内网的价格计费，具体价格请参见OSS价格详情。
> - 如果选择域名类型为源站域名，并设置了一个OSS的域名，则仍然按照外网流量价格计费。

- 源站类型

源站类型	说明
IP	支持多个服务器外网IP地址。如果您使用阿里云云服务器ECS，则可以免审核ECS的IP地址。详情请参见云服务器ECS。
源站域名	支持多个源站域名。 说明 源站域名不能与加速域名相同，否则会造成循环解析，无法回源。例如您的源站域名为img.yourdomain.com，则加速域名可设置为cdn.yourdomain.com。
OSS域名	您可以手动输入阿里云OSS Bucket的外网域名，例如：xxx.oss-cn-hangzhou.aliyuncs.com。OSS外网域名可前往OSS控制台查看，也可直接选择同账号下的OSS Bucket。
函数计算域名	您需要选择函数计算区域和域名。设置函数计算域名的操作方法，请参见如何设置函数计算域名。

- 端口

端口	说明
80端口	资源以HTTP或HTTPS协议回源到80端口。
443端口	资源以HTTP或HTTPS协议回源到443端口。如果您的源站为单个IP地址提供多个域名服务，您需要完成配置回源操作。详情请参见配置回源SNI。
自定义端口	目前仅支持以HTTP协议回源到自定义端口。 如果您需要以HTTPS协议回源到自定义端口，则请提交工单。 注意 如果您配置了自定义端口，则请关闭协议跟随回源功能，自定义端口配置才能生效。关闭回源协议的操作方法，请参见配置回源协议。 当源站选择OSS类型时，回源端口是否支持自定义端口，取决于OSS产品。

6. 单击确定，完成配置。

6.回源配置

6.1. 概述

当您通过客户端请求访问资源时，如果CDN节点上未缓存该资源，则会到源站获取，同时缓存到CDN节点。您可以根据所需配置回源的相关功能，提升资源访问效率。

您可以通过回源配置功能，对域名执行如下操作。

功能	说明
配置回源HOST	当您需要自定义CDN节点回源时需要访问的具体服务器域名时，需要配置回源HOST的域名类型。
配置回源协议	当您通过客户端请求访问资源时，如果CDN节点上未缓存该资源，则会根据您配置的协议跟随规则到源站获取资源，同时缓存到CDN节点。
开启阿里云OSS私有Bucket回源授权	当您的源站为OSS时，可以开通加速域名访问私有OSS Bucket资源的权限，有效防止资源盗链。
关闭私有Bucket回源授权	您可以通过RAM控制台，取消对应角色名称的授权，关闭私有Bucket回源功能。
配置回源SNI	如果您的源站IP绑定了多个域名，当CDN节点以HTTPS协议访问您的源站时，您可以设置回源SNI，指明具体访问域名。
配置自定义回源HTTP头	HTTP请求回源时，您可以添加或删除回源HTTP头。
配置回源请求超时时间	CDN加速节点的回源请求超时等待时间默认为30秒，您可以根据实际需求设置CDN回源请求的最长等待时间。当回源请求等待时间超过配置的超时时间时，CDN节点与源站的连接断开。

6.2. 配置回源HOST

如果您需要自定义CDN节点回源时需要访问的具体服务器域名，则需要配置回源HOST的域名类型。回源HOST可选域名类型包括：加速域名、源站域名和自定义域名。

回源HOST CDN节点回源

背景信息

回源HOST指CDN节点在回源过程中，在源站访问的站点域名。当您的源站有多个业务共用的情况时，可以通过用户回源请求里面携带的回源HOST来区分不同的业务。

> **说明** 如果您的源站绑定了多个域名或站点，则您需要在自定义域名中，指定具体域名，否则回源会失败。

源站和回源HOST的区别：

- 源站：源站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。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**管理**。
4. 在指定域名的左侧导航栏，单击**回源配置**。
5. 在**回源HOST**区域，单击**修改配置**。
6. 打开**回源HOST**开关，选择**域名类型**。

参数	说明
加速域名	加速域名是指您需要加速的域名，即终端用户直接访问到的域名，例如：`cdntest.com`。当回源HOST的域名类型选择为**加速域名**的时候，回源HOST将会被配置为加速域名，例如：`cdntest.com`。
源站域名	源站域名是指您的源站服务器的域名地址，即CDN回源需要访问的域名地址，例如：`origin.com`。当回源HOST的域名类型选择为**源站域名**的时候，回源HOST将会被配置为源站域名，例如：`origin.com`。
自定义域名	当回源HOST的域名类型选择为**自定义域名**的时候，回源HOST将会被配置用户指定的任意域名。如果您的源站绑定了多个域名，则需要指定具体域名，否则回源会失败。

示例	源站类型	功能状态	域名	说明
示例一	域名类型	回源HOST功能默认关闭	加速域名：`cdntest.com` 源站地址：`origin.com`	○ 域名类型选择**加速域名**，则回源HOST为`cdntest.com`。 ○ 域名类型选择**源站域名**，则回源HOST为`origin.com`。 ○ 域名类型选择**自定义域名**，则回源HOST为用户输入的自定义域名。

示例	源站类型	功能状态	域名	说明
示例二	IP地址类型	回源HOST功能默认关闭	加速域名： cdntest.com 源站地址： 1.1.1.1	○ 域名类型选择**加速域名**，则回源HOST为 cdntest.com 。 ○ 域名类型选择“**自定义域名**，则回源HOST为用户输入的自定义域名。 **说明** 源站地址是IP地址类型，所以域名类型的源站域名选项被置灰，不可选择。
示例三	OSS域名类型	回源HOST默认开启	加速域名： cdntest.com 源站地址： test.oss-cn-hangzhou.aliyuncs.com	○ 域名类型选择**加速域名**，则回源HOST为 cdntest.com 。 ○ 域名类型选择**源站域名**，则回源HOST为 test.oss-cn-hangzhou.aliyuncs.com 。 ○ 域名类型选择**自定义域名**，则回源HOST为用户输入的自定义域名。 **说明** 默认配置为： 域名类型：源站域名 域名地址： test.oss-cn-hangzhou.aliyuncs.com

7. 单击**确定**。

6.3. 配置回源协议

当您通过客户端请求访问资源时，如果CDN节点上未缓存该资源，则会根据您配置的协议跟随规则到源站获取资源，同时缓存到CDN节点。通过本文档，您可以了解配置回源协议的方法。

CDN回源 静态协议 动态协议

背景信息

协议跟随回源是指回源使用的协议和客户端访问资源的协议保持一致。如果客户端使用HTTPS方式请求资源，当节点上未缓存该资源时，会使用相同的HTTPS方式回源获取资源。同理，如果客户端使用HTTP协议，CDN节点也将使用HTTP协议回源。

说明 源站需要同时支持80端口和443端口，否则有可能会造成回源失败。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击回源配置。
5. 在回源协议区域，打开回源协议开关。
6. 单击修改配置。
7. 在静态协议跟随回源对话框，选择的回源协议类型为：跟随、HTTP或HTTPS。

参数	说明
跟随	客户端以HTTP或HTTPS协议请求CDN，CDN跟随客户端的协议请求源站。
HTTP	CDN只以HTTP协议回源。
HTTPS	CDN只以HTTPS协议回源。

8. 单击确定。

6.4. 开启阿里云OSS私有Bucket回源授权

当您的源站为OSS时，可以开通加速域名访问私有OSS Bucket资源的权限，有效防止资源盗链。通过本文档，您可以了解开启私有Bucket回源授权的操作方法。

OSS域名 私有Bucket CDN回源

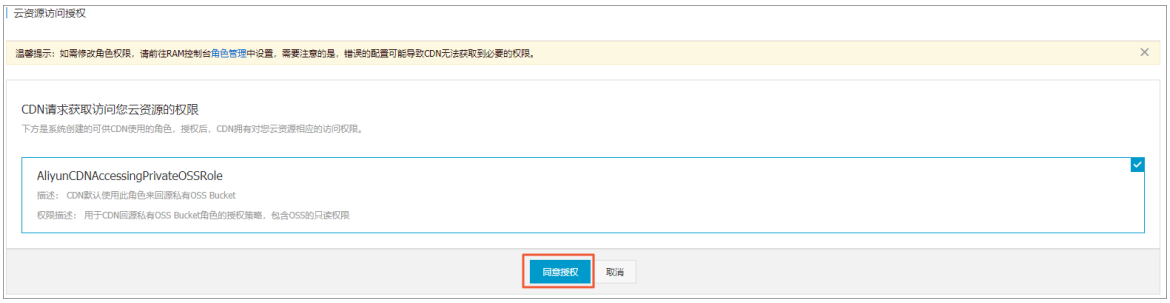
背景信息

您可以配合使用阿里云CDN提供的Refer防盗链功能、鉴权功能，有效保护您的资源安全。详细说明，请参见配置Referer防盗链和URL鉴权。

> 注意
>
> - 当您开启私有OSS Bucket回源授权后，即表示开启CDN对您所有Bucket的只读权限，不只针对当前Bucket授权。
> - 当您授权成功并开启了对应域名的私有Bucket回源授权功能后，该加速域名可以访问您的私有Bucket内的所有内容。
> - 请您在开启该功能前，根据实际业务，谨慎决策。如果您授权的私有Bucket内容并不适合作为CDN加速域名的回源内容，请勿授权或者开启该功能。
> - 如果您的网站有被攻击风险：
>   - 请购买高防服务。
>   - 请勿授权或开启私有Bucket回源授权功能。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击回源配置。
5. 在阿里云OSS私有Bucket回源区域，单击点击授权。
6. 单击同意授权。



> 说明 只有当您的源站为OSS时，可以开通加速域名访问私有OSS Bucket资源的权限。

7. 在阿里云OSS私有Bucket回源区域，打开阿里云OSS私有Bucket回源开关。 了解如何关闭私有Bucket，请参见关闭私有Bucket回源授权。

6.5. 关闭私有Bucket回源授权

本文档介绍了如何移除加速域名能够访问您私有Bucket内资源的权限。您可以通过访问控制 RAM（Resource Access Management）控制台，取消对应角色名称的授权，关闭私有Bucket回源功能。

回源授权私有Bucket

背景信息

若您的加速域名正在使用私有Bucket作为源站进行回源，请不要关闭或删除私有Bucket授权。

操作步骤

1. 登录RAM控制台。
2. 在左侧导航栏，单击RAM角色管理。
3. 在RAM角色管理页面，单击RAM角色名称AliyunCDNAccessingPrivateOSSRole。

4. 单击待删除权限对应的移除权限。
5. 在移除权限确认对话框中，单击确定。
6. 返回RAM角色管理页面，单击待删除角色对应的删除。
7. 在删除RAM角色的确认对话框中，单击确定。

6.6. 配置回源SNI

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

回源SNI CDN 源站

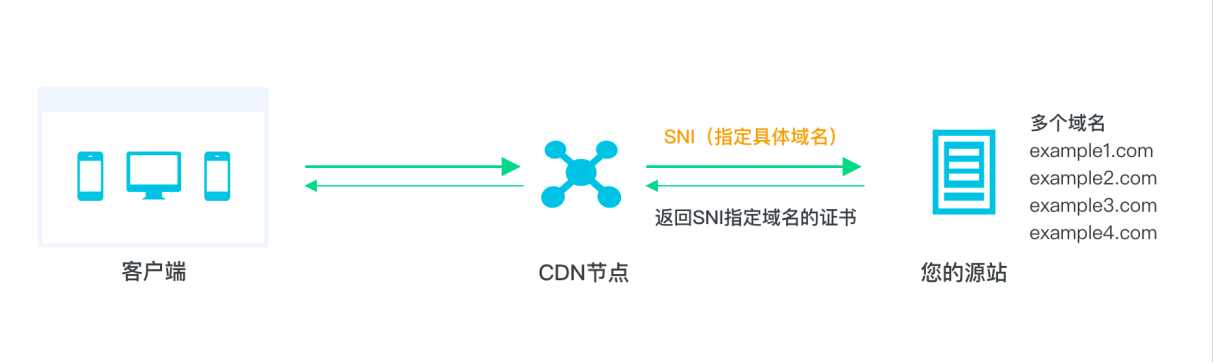
背景信息

服务器名称指示SNI（Server Name Indication）是一个扩展的传输层安全性协议TLS（Transport Layer Security）。在该协议下，握手过程开始时，客户端会返回正在连接的那台服务器即将要连接的主机名称，以允许该服务器在相同的IP地址和TCP端口号上呈现多个证书，即一台服务器可以为多个域名提供服务。因此，同一个IP地址上提供的多个安全的HTTPS网站（或其他任何基于TLS的服务），不需要使用相同的证书。

如果您的源站服务器使用单个IP提供多个域名的HTTPS服务，且您已经为CDN设置了443端口回源（CDN节点以HTTPS协议访问您的服务器），您就需要设置回源SNI，指明所请求的具体域名。这样CDN节点以HTTPS协议回源访问您的服务器时，服务器才会正确地返回对应的证书。

> **说明** 如果您的源站是阿里云OSS，则无需设置回源SNI。

回源SNI的工作原理如下图所示。

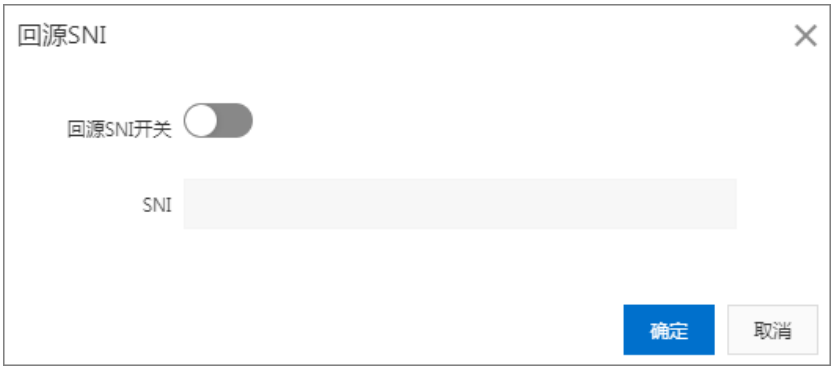


回源SNI的工作流程如下：

1. CDN节点以HTTPS协议访问源站时，在SNI中指定访问的域名。
2. 源站接收到请求后，根据SNI中记录的域名，返回对应域名的证书。
3. CDN节点收到证书，与服务器端建立安全连接。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**管理**。
4. 在指定域名的左侧导航栏，单击**回源配置**。
5. 在**回源SNI**区域，单击**修改配置**。
6. 打开**回源SNI开关**，输入服务器源站提供服务的域名。



> **说明** SNI在阿里云CDN产品中指源站域名。如果您的源站服务器使用单个IP地址提供多个域名的HTTPS服务，则需要设置回源SNI，指明所请求的具体域名，例如：cdn.console.aliyun.com。

7. 单击**确定**完成配置。

6.7. 配置自定义回源HTTP头

HTTP消息头是指，在超文本传输协议（ Hypertext Transfer Protocol，HTTP）的请求和响应消息中，协议头部的组件。HTTP消息头准确描述了正在获取的资源、服务器或客户端的行为，定义了HTTP事务中的具体操作参数。HTTP请求回源时，您可以添加或删除回源HTTP头。

回源HTTP头 回源

背景信息

在HTTP消息头中，按其出现的上下文环境，分为通用头、请求头、响应头等。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击回源配置。
5. 单击回源HTTP请求头。
6. 单击添加。
7. 在回源HTTP头页面，选择自定义回源头，设置自定义参数和取值。

> 注意 当您在配置回源HTTP头时，建议选择参数为自定义参数，根据您的实际需求自定义HTTP头， 不要选择参数列表中指定的HTTP头。

8. 单击确定。

后续操作

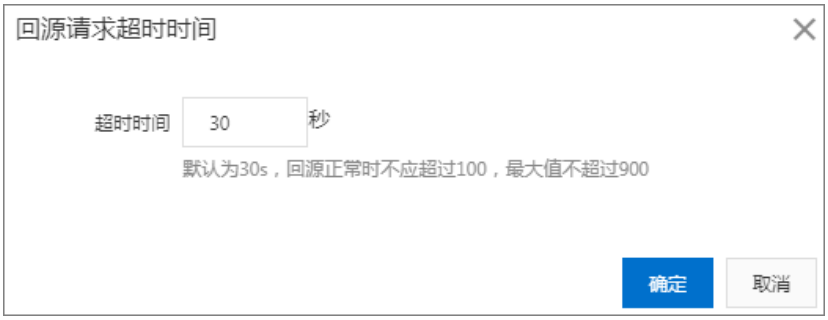
当您在配置回源HTTP头时，如果选择参数为自定义参数，则配置自定义参数后，系统可能报错，如下图所示。原因是您配置的字段是内部保留字段，请您重新配置。

6.8. 配置回源请求超时时间

当CDN节点没有您请求的资源，CDN节点会进行回源获取最新的内容。CDN加速节点的回源请求超时等待时间默认为30秒，您可以根据实际需求设置CDN回源请求的最长等待时间。当回源请求等待时间超过配置的超时时间时，CDN节点与源站的连接断开。通过本文档，您可以了解配置回源请求超时时间的操作方法。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击回源配置。
5. 在回源请求超时时间区域，单击修改配置。
6. 在回源请求超时时间对话框，设置超时时间。



CDN加速节点的回源请求超时时间正常不超过100秒，配置的最大值不能超过900秒。

7. 单击确定完成配置。

6.9. 改写回源URI

当您需要改写用户回源请求中的URI时，可以配置回源URI改写功能。通过本文档，您可以了解配置重写规则的操作方法。

背景信息

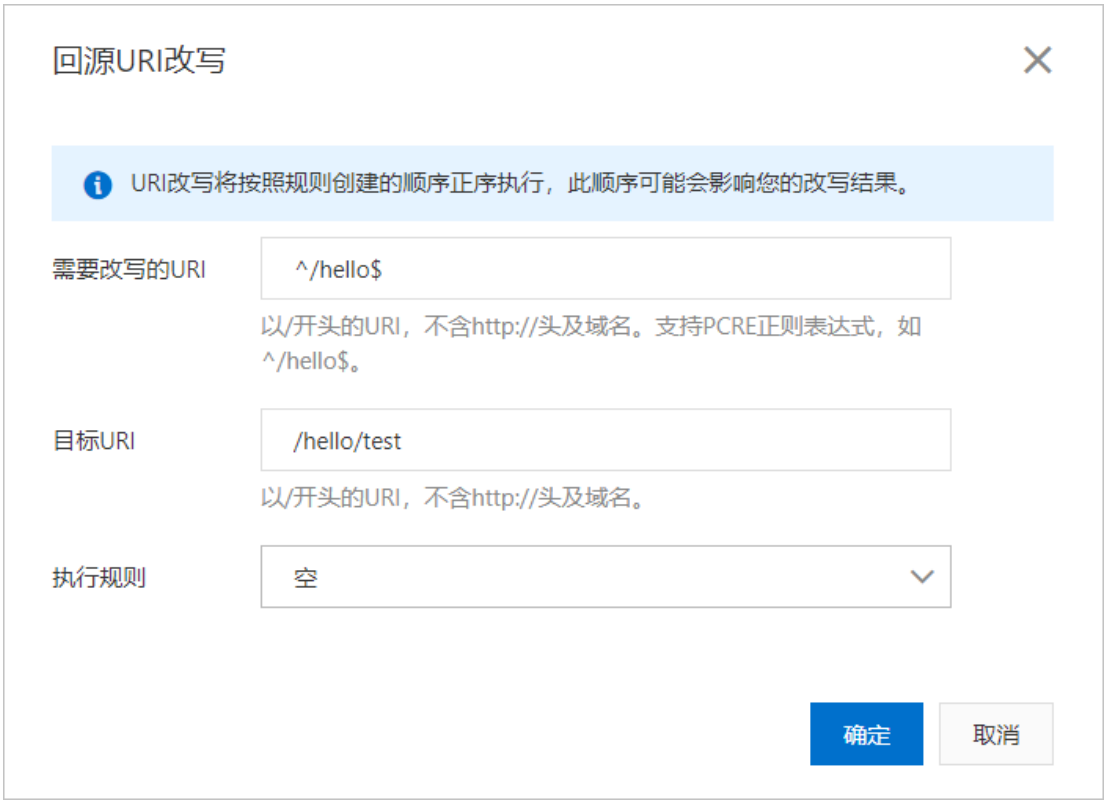
当用户回源请求的URI与源站的URI不匹配时，需要将用户回源请求的URI修改为与源站匹配的URI，您可以根据实际需要配置多条改写匹配规则。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击回源配置。
5. 单击回源URI改写。
6. 在回源URI改写页签，单击添加。
7. 根据您的需求，配置需要改写的URI、目标URI和执行规则。

参数	示例	说明
需要改写的URI	^/hello$	以正斜线（/）开头的URI，不含htttp://头及域名。支持PCRE正则表达式。
目标URI	/hello/test	以正斜线（/）开头的URI，不含htttp://头及域名。

参数	示例	说明
执行规则	空	如果配置了多条规则，在匹配执行当前规则后，继续匹配后续规则。
	break	如果配置了多条规则，在匹配执行当前规则后，后续规则将不再匹配，并且只修改URI部分，不修改URL的参数。
	enhance_break	如果配置了多条规则，在匹配执行当前规则后，后续规则将不再匹配，但是匹配和修改整个URL（包括URI+参数）。



注意

- **回源URI改写**功能中的执行规则“break”虽然不修改URL的参数部分，但是并不影响**回源参数改写**功能对URL中参数的改写。
- **回源URI改写**功能在配置执行规则“enhance_break”的情况下，对URL中参数的改写可能会与**回源参数改写**功能对URL中参数的改写相冲突，这两个功能同时配置的时候，需要注意避免配置冲突。
- **回源URI改写**功能在配置执行规则“enhance_break”的情况下，对URL中参数的改写可能会与**域名管理 > 性能优化**页签下的**保留参数**或**忽略参数**功能相冲突，这三个功能同时配置的时候，需要注意避免配置冲突。

8. 单击**确定**，使改写规则开始执行和生效。

您也可以在**回源URI改写**页面的规则列表中，单击**修改**或**删除**，对当前配置的规则进行相应操作。

> **注意**
>
> - 单个域名可以配置的**回源URI改写**规则数量上限是50个。
> - 规则改写按照规则列表从上到下顺序执行的，此顺序可能会影响您的改写结果。
> - **回源URI改写**功能与**重写**功能的区别在于，**重写**功能的作用位置是在CDN边缘节点上面，会影响CDN内部链路，也会改写缓存key，而**回源URI改写**功能的作用位置是在CDN回源节点上面，不影响CDN内部链路，不改写缓存key。

样例一：

待改写URI	^/hello$
目标URI	/index.html
执行规则	空
结果说明	原始请求：`http://domain.com/hello` 改写后的回源请求：`http://domain.com/index.html` 该请求将会继续匹配**回源URI改写**规则列表中其余的规则。

样例二：

待改写URI	^/hello.jpg$
目标URI	/image/hello.jpg
执行规则	break
结果说明	原始请求：`http://domain.com/hello.jpg` 改写后的回源请求：`http://domain.com/image/hello.jpg` 该请求将不再继续匹配**回源URI改写**规则列表中其余的规则。

样例三：

待改写URI	^/hello.jpg?code=123$
目标URI	/image/hello.jpg?code=321
执行规则	enhance_break
结果说明	原始请求：`http://domain.com/hello.jpg?code=123` 改写后的回源请求：`http://domain.com/image/hello.jpg?code=321` 该请求将不再继续匹配**回源URI改写**规则列表中其余的规则。

6.10. 改写回源参数

当您需要改写用户回源请求URL中的参数时，可以配置回源参数改写功能。通过本文档，您可以了解配置回源参数改写功能的操作方法。

背景信息

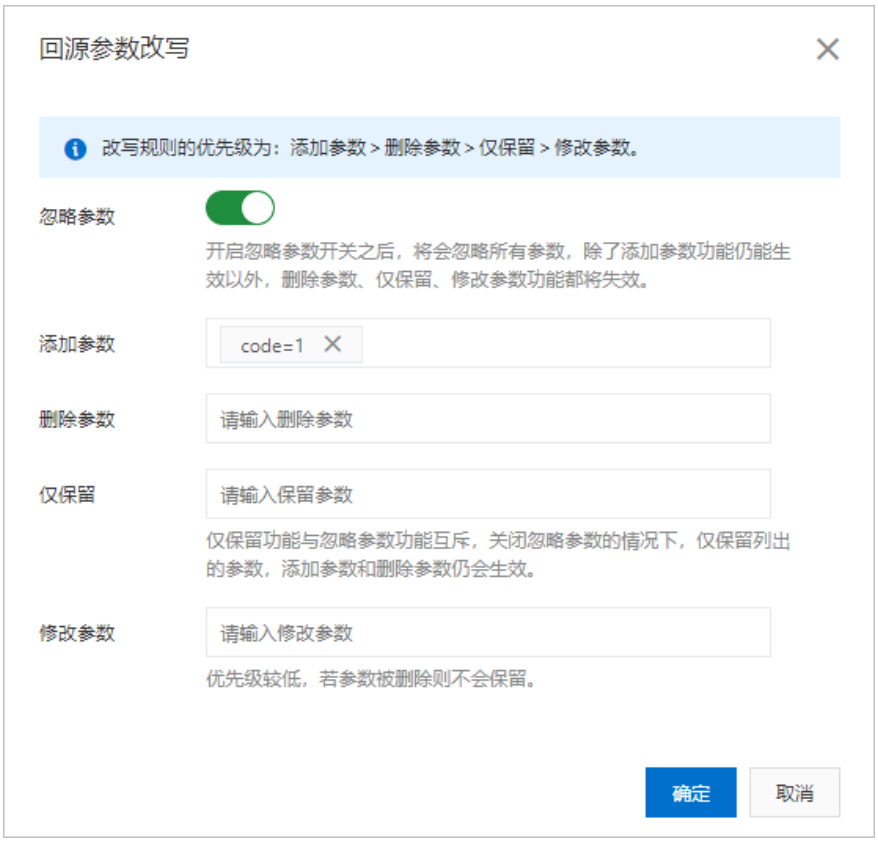
当用户请求URL中携带的参数信息与您需要发送给源站的参数信息不一致时，您可以配置多个回源参数改写规则，实现忽略、添加、删除、保留、修改等多种操作。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**管理**。
4. 在指定域名的左侧导航栏，单击**回源配置**。
5. 单击**回源参数改写**。
6. 在**回源参数改写**页签，打开**使用回源参数改写**开关。

7. 配置回源参数改写操作。

   您可以根据需求配置不同的操作类型，也可以在一种操作类型的参数框里面添加多个参数。



8. 单击**确定**，使改写操作开始执行和生效。

   您也可以在**回源参数改写**页面，单击**修改配置**，对当前配置的规则进行修改操作。

   改写回源参数需要注意如下事项：

   - 改写规则的优先级为：**添加参数** > **删除参数** > **仅保留** > **修改参数**。
   - **忽略参数**功能和**仅保留**功能互斥，要避免出现两个功能同时配置的情况，以免出现功能冲突。
   - 开启**忽略参数**功能（同时**仅保留**功能的输入框留空）的情况下，将会忽略原始URL中携带的所有参数，但是由于添加参数和删除参数操作的优先级更高，添加参数和删除参数操作仍会生效。
   - 在**仅保留**功能的输入框内填写需要保留的参数（同时关闭**忽略参数**功能），将只会保留原始URL中携带的指定参数，但是由于添加参数和删除参数操作的优先级更高，添加参数和删除参数操作仍会生效。

   > **说明**
   >
   > 与其他功能的冲突说明如下：
   >
   > - **回源参数改写**功能对URL中参数的改写，可能会与**回源URI改写**功能在配置执行规则“enhance_break”的情况下相冲突，这两个功能同时配置的时候，需要注意避免配置冲突。
   > - **回源参数改写**功能对URL中参数的改写，可能会与**域名管理** > **性能优化**页签下的**保留参数**或**忽略参数**功能相冲突，这三个功能同时配置的时候，需要注意避免配置冲突。
   > - **回源参数改写**功能的作为位置是在CDN回源节点上面，不影响CDN内部链路，不改写缓存key，而**保留参数**或**忽略参数**功能的作用位置是在CDN边缘节点上面，会影响CDN内部链路，也会改写缓存key。

样例一：

忽略参数	开启
添加参数	无
删除参数	无
仅保留	无
修改参数	无

结果说明	原始请求：`http://domain.com/index.html?code1=1&code2=2&code3=3` 改写后的回源请求：`http://domain.com/index.html`

样例二：

忽略参数	无
添加参数	无
删除参数	无
仅保留	code2
修改参数	无
结果说明	原始请求：`http://domain.com/index.html?code1=1&code2=2&code3=3` 改写后的回源请求：`http://domain.com/index.html?code2=2`

样例三：

忽略参数	无
添加参数	code4=4
删除参数	code2
仅保留	无
修改参数	code3=0
结果说明	原始请求：`http://domain.com/index.html?code1=1&code2=2&code3=3` 改写后的回源请求：`http://domain.com/index.html?code1=1&code3=0&code4=4`

6.11. 配置回源HTTP请求头(新)

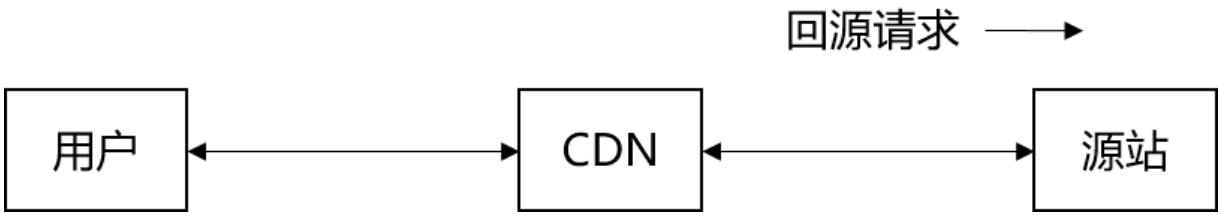
当您需要改写用户回源请求URL中的HTTP Header时，可以通过配置回源HTTP请求头参数实现。通过本文档，您可以了解配置回源HTTP请求头的操作方法。

HTTP请求头 CDN 跨域请求

背景信息

HTTP消息头是指，在超文本传输协议HTTP（Hypertext Transfer Protocol）的请求和响应消息中，协议头部的组件。

在HTTP消息头中，按其出现的上下文环境，分为通用头、请求头、响应头等。



> 说明
> - 回源请求是指用户请求中该加速域名下有通过CDN返回源站的HTTP消息。
> - 回源HTTP请求头的配置只会影响通过CDN回源的HTTP消息，对于CDN节点直接响应给用户的HTTP消息不做修改。
> - 目前不支持泛域名设置。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**管理**。
4. 在指定域名的左侧导航栏，单击**回源配置**。
5. 单击**回源HTTP请求头（新）**。
6. 在**回源HTTP请求头（新）**页签，单击**添加**。
7. 配置回源HTTP请求头信息。

> 注意 当不同的操作方式同时作用于同一个回源请求头参数的时候，将会存在操作冲突的情况。此时按照操作类型的优先级来执行，优先级顺序为**替换** > **增加** > **变更/删除**。例如：当增加和删除操作同时作用于同一个参数时，会先增加，再删除。

   - **增加请求头参数**

配置项	示例	说明
请求头操作	增加	在回源HTTP请求中增加指定的请求头参数。
自定义请求头参数	自定义请求头	可以选择在配置弹窗中已经预制的请求头参数，也可以在下拉框里选择**自定义请求头**，配置自定义请求头参数。
自定义请求头名称	x-code	自定义请求头名称为x-code。
请求头值	key1	一个请求头参数里面，可以配置多个值，不同值之间用逗号（,）隔开。
	key1, key2	
是否允许重复	允许	当**是否允许重复**设置为**允许**时，可以添加重复的请求头参数。例如：`x-code:key1`，`x-code:key2`。
	不允许	当**是否允许重复**设置为**不允许**时，添加同一个请求头参数，后面添加的值会覆盖前面添加的值。例如：先添加`x-code:key1`后，再添加`x-code:key2`，最终的值为`x-code:key2`。

- **删除请求头参数**

配置项	示例	说明
请求头操作	删除	删除所有与请求头参数名称匹配的参数值，无论是否有重复的请求头参数。
自定义请求头参数	自定义请求头	可以选择在配置弹窗中已经预制的请求头参数，也可以在下拉框里选择**自定义请求头**，删除自定义请求头参数。
自定义请求头名称	x-code	自定义请求头名称为x-code。

- **变更请求头参数**

配置项	示例	说明
请求头操作	变更	当请求头参数不存在重复时，可以正常变更参数，有多个重复请求头参数的情况下，不允许进行变更操作。
自定义请求头参数	自定义请求头	可以选择在配置弹窗中已经预制的请求头参数，也可以在下拉框里选择**自定义请求头**，变更自定义请求头参数。

配置项	示例	说明
自定义请求头名称	x-code	自定义请求头名称为x-code。
请求头变更为	key1, key3	一个请求头参数里面，可以配置多个值，不同值之间用号（,）隔开。

- **替换请求头参数**

配置项	示例	说明
请求头操作	替换	当请求头参数不存在重复时，可以正常替换参数，有多个重复请求头参数的情况下，不允许进行替换操作。
自定义请求头参数	自定义请求头	可以选择在配置弹窗中已经预制的请求头参数，也可以在下拉框里选择**自定义请求头**，变更自定义请求头参数。
自定义请求头名称	x-code	自定义请求头名称为x-code。
查找	key	正则表达式查找需要替换的参数值。
替换为	abc	正则表达式替换需要替换的参数值。
匹配	匹配所有	当**匹配**选项设置为**匹配所有**时，所有被匹配的值都会被替换。例如：`x-code:key1,key2,key3`，正则匹配值key替换为abc，替换后的结果为`x-code:abc1,abc2,abc3`。

配置项	示例	说明
	仅匹配第一个	当匹配选项设置为仅匹配第一个时，只有第一个被匹配的值会被替换。例如：`x-code:key1,key2,key3`，正则匹配值key替换为abc，替换后的结果为`x-code:abc1,key2,key3`。

8. 单击确定。

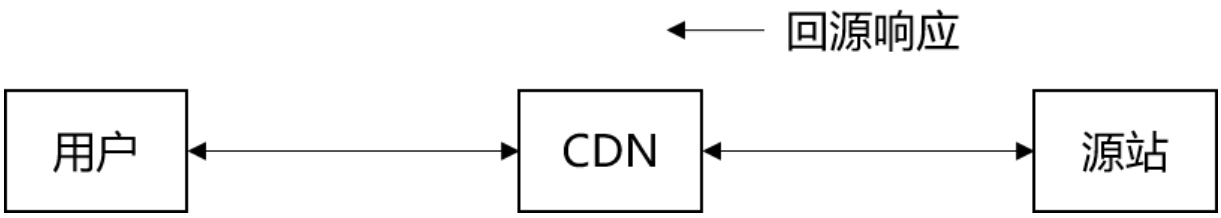
6.12. 配置回源HTTP响应头(新)

当您需要改写用户回源响应请求URL中的HTTP Header时，可以配置功能。通过本文档，您可以了解配置回源HTTP响应头（新）功能的操作方法。

背景信息

HTTP消息头是指，在超文本传输协议HTTP（Hypertext Transfer Protocol）的请求和响应消息中，协议头部的组件。

在HTTP消息头中，按其出现的上下文环境，分为通用头、请求头、响应头等。



说明

- 回源请求是指用户请求中该加速域名下有通过CDN返回源站的HTTP消息。
- 回源HTTP响应头的配置只会影响通过CDN回源的HTTP消息，对于CDN节点直接响应给用户的HTTP消息不做修改。
- 目前不支持泛域名设置。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击回源配置。
5. 单击回源HTTP响应头（新）。
6. 在回源HTTP响应头（新）页签，单击添加。
7. 配置回源HTTP响应头信息。

注意 当不同的操作方式同时作用于同一个回源响应头参数的时候，将会存在操作冲突的情况。此时按照操作类型的优先级来执行，优先级顺序为替换 > 增加 > 变更/删除。例如：当增加和删除操作同时作用于同一个参数时，会先增加，再删除。

- 增加响应头参数

配置项	示例	说明
响应头操作	增加	在回源HTTP请求中增加指定的响应头参数。
自定义响应头参数	自定义响应头	可以选择在配置弹窗中已经预制的响应头参数，也可以在下拉框里选择**自定义响应头参数**，配置自定义响应头参数。
自定义响应头名称	x-code	自定义响应头名称为x-code。
响应头值	key1	一个响应头参数里面，可以配置多个值，不同值之间用逗号（,）隔开。
	key1, key2	
是否允许重复	允许	当**是否允许重复**设置为**允许**时，可以添加重复的响应头参数。例如：`x-code:key1`，`x-code:key2`。
	不允许	当**是否允许重复**设置为**不允许**时，添加同一个响应头参数，后面添加的值会覆盖前面添加的值。例如：先添加`x-code:key1`后，再添加`x-code:key2`，最终的值为`x-code:key2`。

- 删除响应头参数

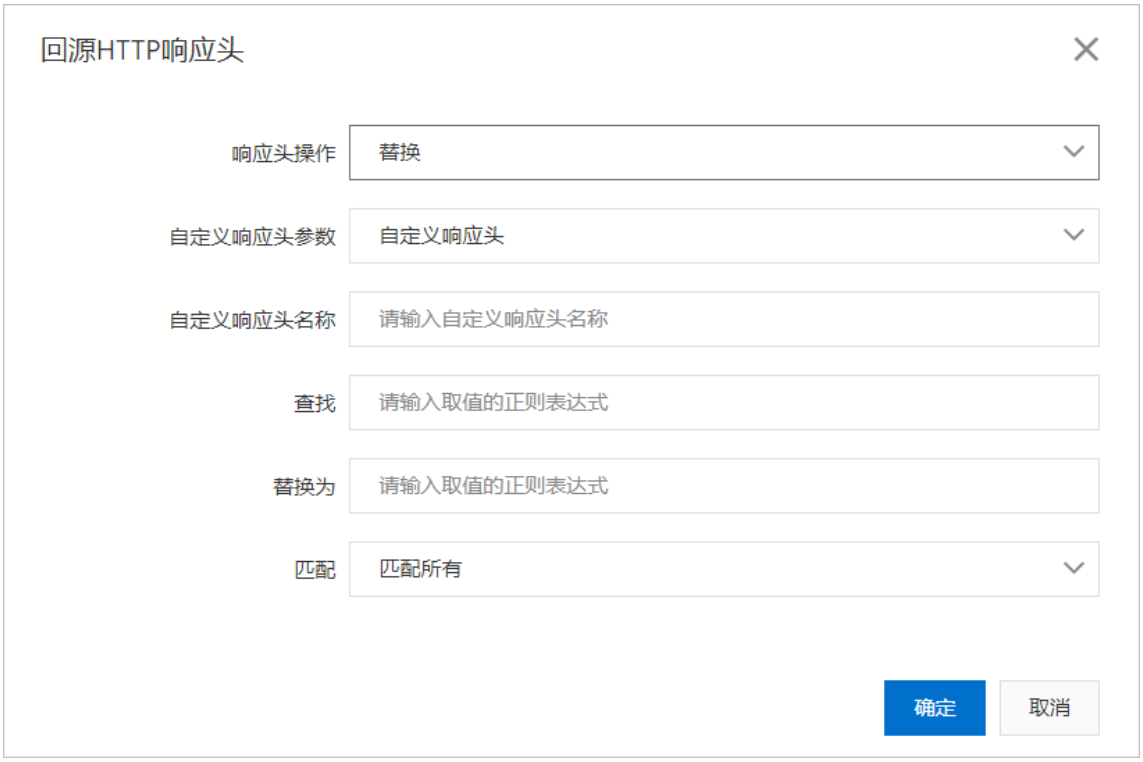
配置项	示例	说明
响应头操作	删除	删除所有与响应头参数名称匹配的参数值，无论是否有重复的响应头参数。
自定义响应头参数	自定义响应头	可以选择在配置弹窗中已经预制的响应头参数，也可以在下拉框里选择**自定义响应头参数**，删除自定义响应头参数。
自定义响应头名称	x-code	自定义响应头名称为x-code。

- **变更响应头参数**

配置项	示例	说明
响应头操作	变更	当响应头参数不存在重复时，可以正常变更参数，有多个重复响应头参数的情况下，不允许进行变更操作。
自定义响应头参数	自定义响应头	可以选择在配置弹窗中已经预制的响应头参数，也可以在下拉框里选择**自定义响应头参数**，变更自定义响应头参数。

配置项	示例	说明
自定义响应头名称	x-code	自定义响应头名称为x-code。
响应头变更为	key1, key3	一个响应头参数里面，可以配置多个值，不同值之间用逗号（,）隔开。

- **替换响应头参数**



配置项	示例	说明
响应头操作	替换	当响应头参数不存在重复时，可以正常替换参数，有多个重复响应头参数的情况下，不允许进行替换操作。
自定义响应头参数	自定义响应头	可以选择在配置弹窗中已经预制的响应头参数，也可以在下拉框里选择**自定义响应头参数**，变更自定义响应头参数。
自定义响应头名称	x-code	自定义响应头名称为x-code。
查找	key	正则表达式查找需要替换的参数值。
替换为	abc	正则表达式替换需要替换的参数值。
匹配	匹配所有	当**匹配**选项设置为**匹配所有**时，所有被匹配的值都会被替换。例如：`x-code:key1,key2,key3`，正则匹配值key替换为abc，替换后的结果为`x-code:abc1,abc2,abc3`。

配置项	示例	说明
	仅匹配第一个	当**匹配**选项设置为**仅匹配第一个**时，只有第一个被匹配的值会被替换。例如：`x-code:key1,key2,key3`，正则匹配值key替换为abc，替换后的结果为`x-code:abc1,key2,key3`。

8. 单击**确定**。

7.缓存配置

7.1. 概述

CDN加速静态资源时，将源站上的资源缓存到距离客户端最近的CDN节点上。当您访问该静态资源时，直接从缓存中获取，避免通过较长的链路回源，提高访问效率。

缓存时间计算

- t =（curtime-last_modified）*0.1
- t = max（10，t）
- t = min（t，3600）

缓存时间为t，单位秒。

默认缓存规则

- 当对象 `last-modified` 为 `20140801 00:00:00` ，当前时间为 `20140801 00:01:00` ，（curtime-Last_modified）*0.1=6s，那么缓存时间为10s，因为最小值为10s。
- 当对象 `last-modified` 为 `20140801 00:00:00` ，当前时间为 `20140802 00:00:00` ，（curtime-Last_modified）*0.1=8640s，那么缓存时间为3600s。
- 当对象 `last-modified` 为 `20140801 00:00:00` ，当前时间为 `20140801 00:10:00` ，（curtime-Last_modified）*0.1=60s，那么缓存时间为60s。
- 如果源站没有 `last-modified` 响应头，但有 `ETag` ，则该对象极有可能是静态资源，将其默认缓存时间设置为 `dft_expires` 指令配置的最小值。
- 如果源站没有 `last-modified` ，也没有 `ETag` ，则认为该对象为动态内容，将其默认缓存时间设置为0，每次都回源。

> **说明**
>
> 因为网站开发及其相关技术人员更清楚自身网站的业务逻辑、静态和动态因素，所以建议用户通过控制台按照文件类型和目录设置缓存时间，操作方法请参见配置缓存过期时间。

相关功能

您可以通过缓存配置功能，对域名执行如下操作。

功能	说明
配置缓存过期时间	您可以针对静态资源配置指定目录和文件后缀名的缓存过期时间，以及优先级，使其在CDN上按照缓存规则进行缓存。
配置状态码过期时间	您可以配置资源的指定目录或文件后缀名的状态码过期时间。
配置HTTP头	您可以配置资源缓存过期的HTTP消息头。
自定义页面	您可以根据所需自定义HTTP或者HTTPS响应返回码跳转的完整URL地址。
配置重写	您可以对请求的URI进行修改和302重定向至目标URI。

7.2. 配置缓存过期时间

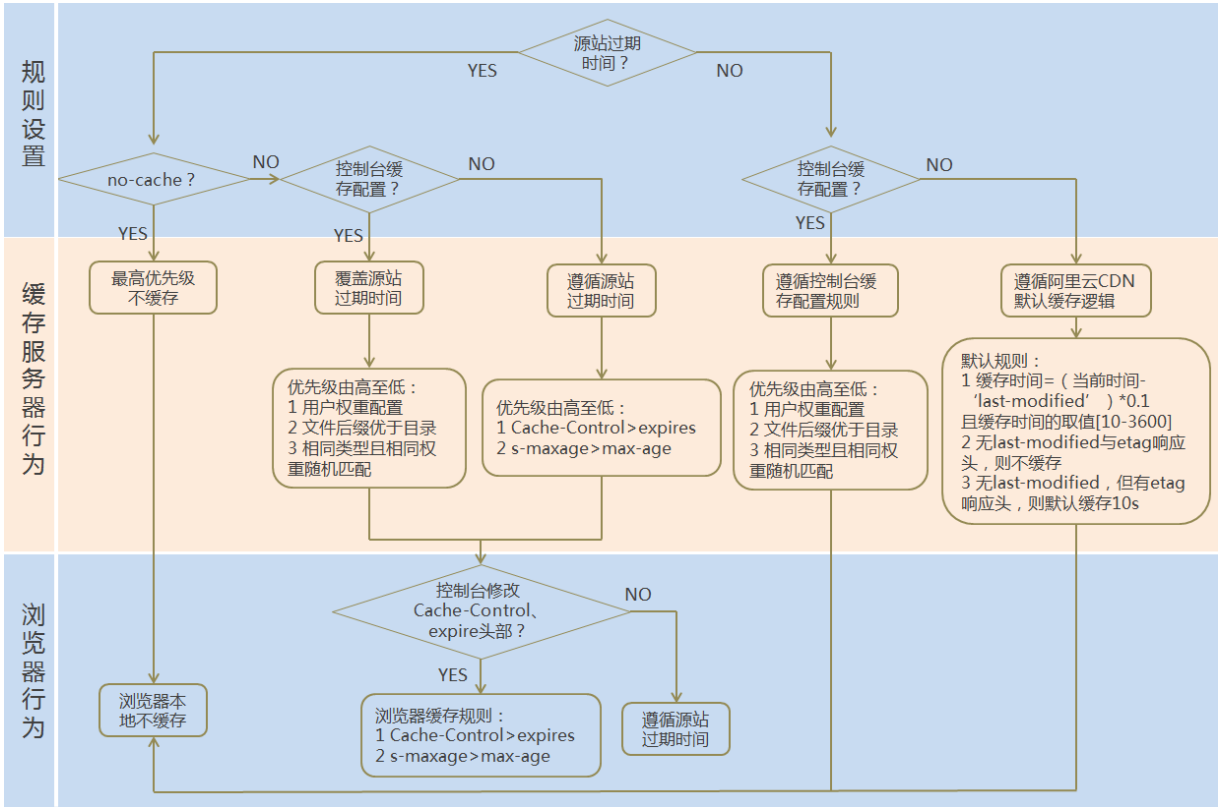
您可以针对静态资源配置指定目录和文件后缀名的缓存过期时间和优先级，资源过期后，自动从CDN节点删除。通过本文，您可以了解资源在CDN上的缓存策略，以及缓存过期时间的配置方法。

缓存策略缓存过期时间CDN

背景信息

配置静态资源的缓存过期时间之前，建议您源站的内容不使用同名更新（即更新源站内容时采用不同的名称），以版本号的方式同步，即采用*img-v1.0.jpg*、*img-v2.1.jpg*的命名方式。

CDN节点上资源的缓存策略如下图所示。



说明

- Cache的默认缓存策略用于配置文件过期时间，在此配置的优先级高于源站配置。如果源站未配置Cache，则支持按完整目录或文件后缀名两种方式设置。
- CDN节点上缓存的资源，可能由于热度较低而被提前从节点删除。
- 在源站响应给CDN节点的内容里面携带了etag信息，并且客户端请求也有携带if-match信息的情况下，如果if-match值=etag值，CDN节点会将缓存的内容直接响应给客户端；如果if-match值≠etag值，CDN节点将会先回源获取最新的内容，然后将最新的内容响应给客户端，同时在CDN节点上用最新的内容替代原先旧的内容。即客户端请求中的if-match信息与缓存文件中的etag信息的校验优先级高于CDN节点上配置的缓存规则。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。

3. 在**域名管理**页面，单击目标域名对应的**管理**。
4. 在指定域名的左侧导航栏，单击**缓存配置**。
5. 在**缓存过期时间**页签，单击**添加**。
6. 配置缓存规则，您可以选择按目录或文件后缀名进行配置。

配置项	说明
类型	○ 目录：指定路径下的缓存资源。 ○ 文件后缀名：指定文件类型的缓存资源。
地址	○ 添加单条目录（支持完整路径）时，须以正斜线（/）开头，例如*/directory/aaa*。 ○ 添加多个文件后缀名时，须以半角逗号（,）分隔，例如 `JPG,TXT` 。
过期时间	资源对应的缓存时间。过期时间最多设置为3年，建议您参照以下规则进行配置： ○ 对于不经常更新的静态文件（如图片类型、应用下载类型等），建议您将缓存时间设置为1个月以上。 ○ 对于频繁更新的静态文件（如JS、CSS等），您可以根据实际业务情况设置。 ○ 对于动态文件（如PHP、JSP、ASP等），建议您将缓存时间设置为0s，即不缓存。

配置项	说明
权重	缓存规则的优先级。 说明 ○ 取值范围：1~99间的整数。数字越大，优先级越高，优先生效。 ○ 不推荐设置相同的权重，权重相同的两条缓存策略优先级随机。 示例：为加速域名 example.aliyun.com 配置三条缓存策略，缓存策略1优先生效。 ○ 缓存策略1：文件名后缀为.jpg和.png的所有资源过期时间设置为1月，权重设置为90。 ○ 缓存策略2：目录为*/www/dir/aaa*过期时间设置为1小时，权重设置为70。 ○ 缓存策略3：完整路径为*/www/dir/aaa/example.php*过期时间设置为0s，权重设置为80。

7. 单击**确定**。
   您也可以单击**修改**或**删除**，对当前配置的缓存策略进行相应操作。

7.3. 配置状态码过期时间

您可以针对静态资源配置指定目录和文件后缀名的状态码过期时间，资源过期后，自动从CDN节点删除。通过本文您可以了解状态码过期时间的配置方法。

状态码过期时间 CDN

背景信息

您在设置状态码过期时间时，注意事项如下：

- 对于状态码303、304、401、407、600和601，不进行缓存。
- 对于状态码204、305、400、403、404、405、414、500、501、502、503和504，如果源站响应了Cache-Control，则遵循源站的Cache-Control原则。如果未设置状态码，则缓存时间默认为1秒。
- 如果您同时设置了目录和文件后缀名这两种类型的状态码过期时间，那么先设置的类型生效。

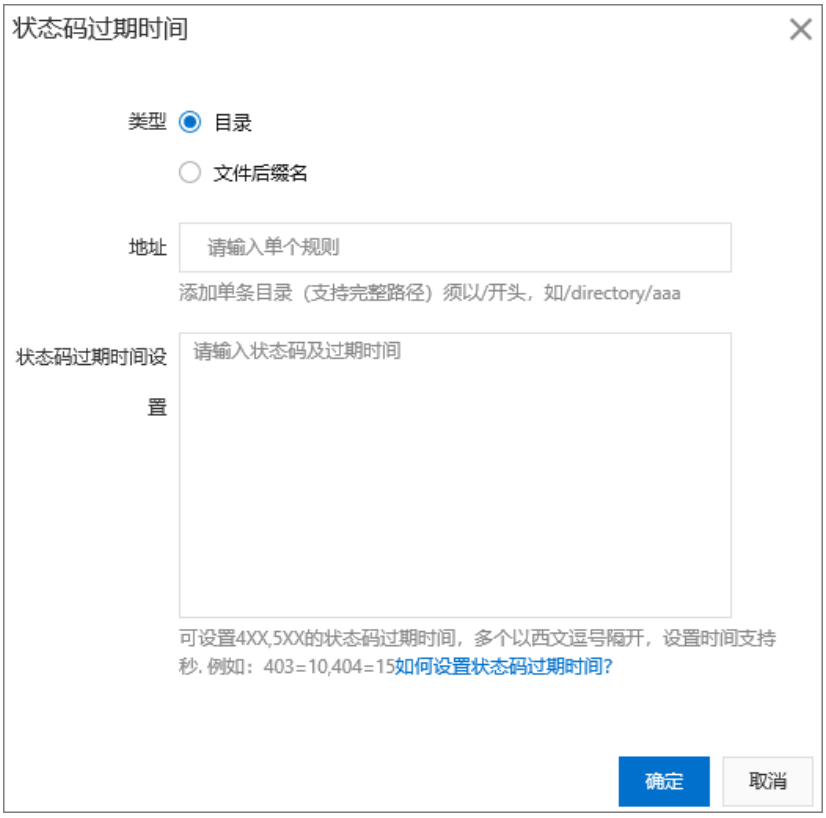
操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**管理**。
4. 在指定域名的左侧导航栏，单击**缓存配置**。
5. 单击**状态码过期时间**。
6. 在**状态码过期时间**页签，设置文件、目录和状态码的过期时间。

   设置文件和目录状态码过期时间

   i. 在**状态码过期时间**区域，单击**添加**。

ii. 配置状态码过期时间，您可以选择按目录或文件后缀名进行配置。



类型	注意事项
目录	■ 添加单条目录（支持完整路径）须以/开头，如*/directory/aaa*。 ■ 不支持配置状态码2xx和3xx。
文件后缀名	■ 输入多个文件后缀名，须以半角逗号分隔，如 `txt,jpg` 。 ■ 不支持 `*` 匹配所有类型文件。 ■ 不支持配置状态码2xx和3xx。

iii. 单击**确定**，配置成功。

您也可以在**状态码过期时间**列表中，单击**修改**或**删除**，对当前状态码过期时间的配置进行相应操作。

7.4. 配置HTTP头

HTTP消息头准确描述了正在获取的资源、服务器或客户端的行为，定义了HTTP事务中的具体操作参数。通过本文档，您可以了解设置HTTP头响应的操作方法。

HTTP响应头CDN跨域请求

背景信息

HTTP消息头是指，在超文本传输协议（ Hypertext Transfer Protocol，HTTP）的请求和响应消息中，协议头部的组件。

在HTTP消息头中，按其出现的上下文环境，分为通用头、请求头、响应头等。

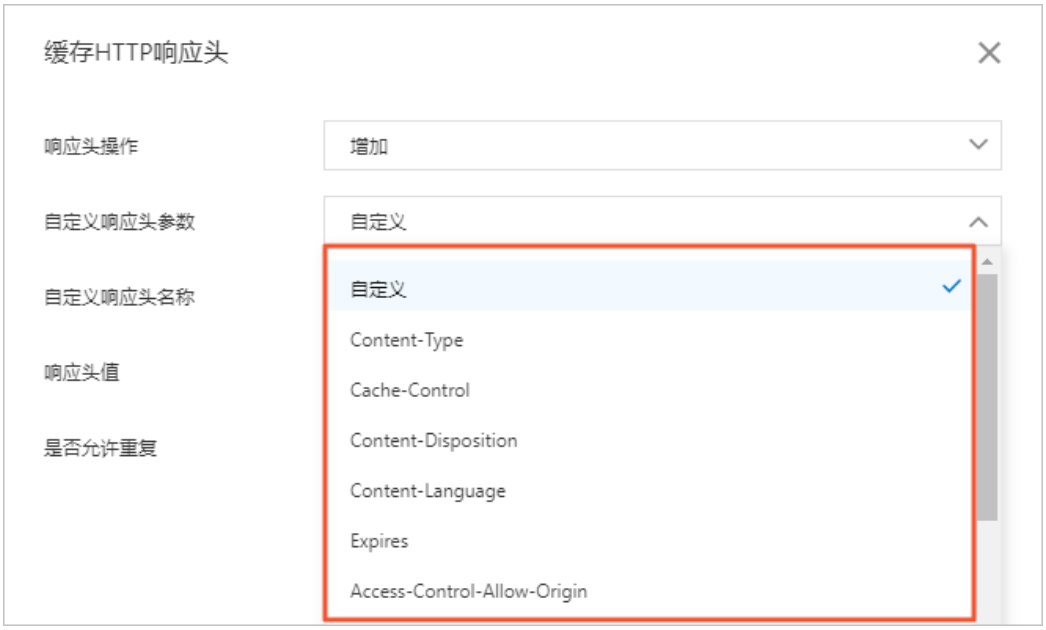
> 注意
>
> - HTTP响应头的设置会影响该加速域名下所有资源，当您通过客户端（例如浏览器）访问资源时，会影响请求响应，但不会影响缓存服务器。
> - 目前不支持泛域名设置。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击缓存配置。
5. 单击缓存HTTP响应头。
6. 在缓存HTTP响应头页签，单击添加。
7. 配置HTTP响应头的参数和取值。

   目前阿里云CDN加速提供10个HTTP响应头参数可供您自定义取值，参数解释如下表所示。 如果您有其他HTTP头设置需求，请提交工单处理。

   > 说明 增加HTTP响应头时您可以设置是否允许重复。允许表示允许重复，即源站返回的头会保留，同时会加上一个同名的头。不允许表示不允许重复，即源站返回的头会被新配置的同名头覆盖。



参数	描述	示例
Content-Type	指定客户端程序响应对象的内容类型。	image

参数	描述	示例
Cache-Control	指定客户端程序请求和响应遵循的缓存机制。	no-cache
Content-Disposition	指定客户端程序把请求所得的内容存为一个文件时提供的默认的文件名。	123.txt
Content-Language	指定客户端程序响应对象的语言。	zh-CN
Expires	指定客户端程序响应对象的过期时间。	Wed, 21 Oct 2015 07:28:00 GMT
Access-Control-Allow-Origin	指定允许的跨域请求的来源。	* 说明 您可以填写 * 表示全部域名；也可以填写完整域名，例如 www.aliyun.com 。
Access-Control-Allow-Headers	指定允许的跨域请求的字段。	X-Custom-Header
Access-Control-Allow-Methods	指定允许的跨域请求方法。	POST、GET 说明 如果您需要同时添加POST和GET，请使用英文逗号（,）隔开。
Access-Control-Max-Age	指定客户端程序对特定资源的预取请求返回结果的缓存时间。	600
Access-Control-Expose-Headers	指定允许访问的自定义头信息。	Content-Length

8. 单击**确定**。

   在**缓存HTTP响应头**列表中，您可以单击**修改**或**删除**，对当前配置的HTTP响应头进行相应操作。

7.5. 自定义页面

当客户端通过浏览器请求Web服务时，如果请求的URL不存在，则Web服务默认会返回404报错页面。Web服务器预设的报错页面通常不美观，为了提升访问者体验，您可以根据所需自定义HTTP或者HTTPS响应返回码跳转的完整URL地址。通过本文，您可以了解自定义错误页面的操作方法。

自定义页面 设置状态码页面 CDN

背景信息

阿里云提供两种状态码返回页面，分别是默认页面和自定义页面。以返回码404为例，介绍默认页面和自定义页面的差异。

- 默认值：HTTP响应返回404时，服务器返回默认404 Not Found页面。
- 自定义404：HTTP响应返回404时，将会跳转到自定义的404页面，需要自定义跳转页的完整URL地址。

> 说明
> - 404页面属于阿里云公益资源，不会产生任何费用。
> - 自定义页面属于个人资源，按照正常分发计费。
> - 返回404页面的原因，请参见出现自定义404页面的原因是什么？。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击缓存配置。
5. 单击自定义页面。
6. 在自定义页面页签，单击添加。

7. 配置自定义页面的参数和取值。

本文以自定义错误码404为例，假设您需要将404页面 error404.html ，与其他静态文件同时存放在源站域名下，并通过加速域名 exp.aliyun.com 访问。那么，您只需选择404，并填写完整的加速域名URL即可，URL为： http://exp.aliyun.com/error404.html 。

8. 单击确定。

   在自定义页面列表中，您也可以单击修改或删除，对当前配置进行相应操作。

7.6. 配置重写

当您访问的URI与源站URI不匹配时，需要将URI修改为与源站匹配的URI。您修改URI中指定参数时，需要配置重写规则，规则匹配后，会302重定向到目标URI。您还可以根据实际需求配置多条重写匹配规则。通过本文档，您可以了解配置重写规则的操作方法。

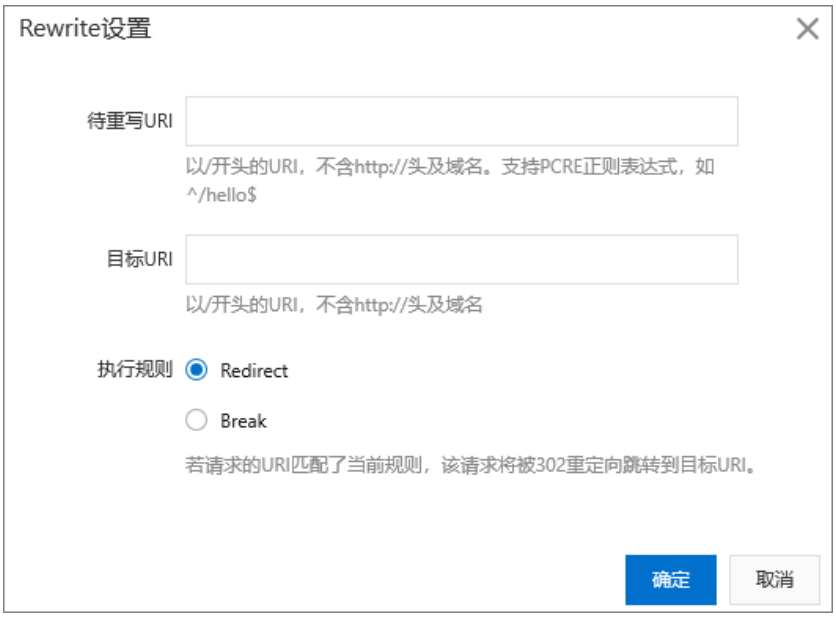
重写缓存

背景信息

如果您需要对请求URI进行修改，请添加重写功能。例如：您的某些用户或者客户端仍然使用HTTP协议访问 http://example.com/hello ，您可以通过该功能配置，所有 http://example.com/hello 请求都重定向到 http://example.com/index.html 。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击缓存配置。
5. 单击重写。
6. 在重写页签，单击添加。
7. 根据您的需求，配置待重写URI、目标URI和执行规则。



参数	说明
Redirect	若请求的URI匹配了当前规则，该请求将被302重定向跳转到目标URI。
Break	若请求的URI匹配了当前规则，执行完当前规则后，将不再匹配剩余规则。

8. 单击确定。

您也可以在重写列表中，单击修改或删除，对当前配置的重写规则进行相应操作。

> 说明 单个域名可以配置的重写规则数量上限是50个。

样例	待重写URI	目标URI	执行规则	结果说明
样例一	/hello	/index.html	Redirect	客户端请求 `http://domain.com/hello`，CDN节点将返回302让客户端重新请求 `http://domain.com/index.html` 的内容。
样例二	^/hello$	/index.html	Break	客户端请求 `http://domain.com/hello`，CDN节点将返回 `http://domain.com/index.html` 的内容。且该请求不再继续匹配其余的重写规则。
样例三	^/$	/index.html	Redirect	客户端请求 `http://domain.com`，CDN节点将返回302让客户端重新请求 `http://domain.com/index.html` 的内容。
样例四	/hello	/hello/index.html	Redirect	客户端请求 `http://domain.com/hello`，CDN节点将返回302让客户端重新请求 `http://domain.com/hello/index.html` 的内容。

8.HTTPS配置

8.1. 什么是HTTPS加速

本文档介绍了HTTPS安全加速的工作原理、优势和注意事项。您可以通过开启HTTPS安全加速，实现客户端和CDN节点之间请求的HTTPS加密，保障数据传输的安全性。

HTTPS加速 CDN

什么是HTTPS？

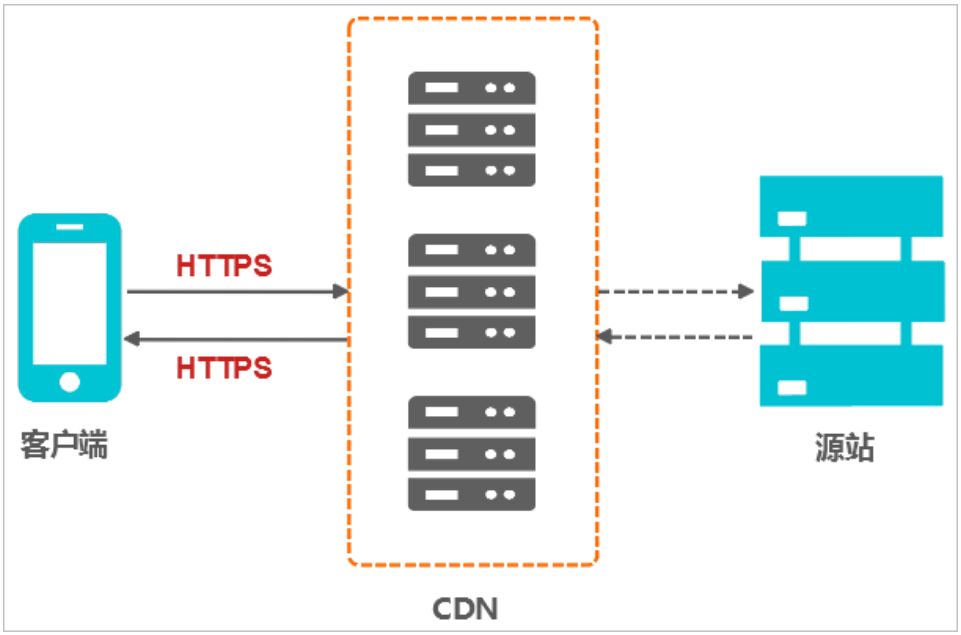
HTTP协议以明文方式发送内容，不提供任何方式的数据加密。HTTPS协议是以安全为目标的HTTP通道，简单来说，HTTPS是HTTP的安全版，即将HTTP用SSL/TLS协议进行封装，HTTPS的安全基础是SSL/TLS协议。HTTPS提供了身份验证与加密通讯方法，被广泛用于万维网上安全敏感的通讯，例如交易支付。

根据2017年EFF（Electronic Frontier Foundation）发布的报告，目前全球已有超过一半的网页端流量采用了加密的HTTPS进行传输。

工作原理

在阿里云CDN控制台开启的HTTPS协议，将实现客户端和阿里云CDN节点之间请求的HTTPS加密。CDN节点返回从源站获取的资源给客户端时，按照源站的配置方式进行。建议源站配置并开启HTTPS，实现全链路的HTTPS加密。

HTTPS加密流程如下图所示。



1. 客户端发起HTTPS请求。
2. 服务端提前准备好公钥和私钥。

   > 说明 公钥和私钥可以自己制作，可以向专业组织申请，也可以使用阿里云CDN控制台申请免费证书。

3. 服务端将相应的公钥传送给客户端。
4. 客户端解析证书的正确性。
   - 如果证书正确，则会生成一个随机数（密钥），并用公钥进行加密，传输给服务端。
   - 如果证书不正确，则SSL握手失败，需要重新上传证书进行认证。

   > 说明
   >
   > 正确性包括：
   >
   > - 证书未过期。
   > - 发行服务器证书的CA可靠。
   > - 发行者证书的公钥能够正确解开服务器证书的发行者的数字签名。
   > - 服务器证书上的域名和服务器的实际域名相匹配。

5. 服务端用之前的私钥进行解密，得到随机数（密钥）。
6. 服务端用随机数（密钥）对传输的数据进行加密。
7. 客户端用随机数（密钥）对服务端的加密数据进行解密，拿到相应的数据。

功能优势

HTTPS安全传输的优势：

- HTTPS安全传输，有效防止HTTP明文传输中的窃听、篡改、冒充和劫持风险。
- 数据传输过程中对您的关键信息进行加密，防止类似Session ID或者Cookie内容被攻击者捕获造成的敏感信息泄露等安全隐患。
- 数据传输过程中对数据进行完整性校验，防止DNS或内容遭第三方劫持、篡改等中间人攻击（MITM）隐患，详情请参见使用HTTPS防止流量劫持。
- HTTPS是主流趋势：未来主流浏览器会将HTTP协议标识为不安全，谷歌浏览器Chrome 70以上版本以及Firefox已经在2018年将HTTP网站标识为不安全，若坚持使用HTTP协议，除了安全会埋下隐患外，终端客户在访问网站时出现的不安全标识，也将影响访问。
- 主流浏览器对HTTPS网站进行搜索加权，主流浏览器均支持HTTP/2，而支持HTTP/2必须支持HTTPS。无论从安全、市场或用户体验来看，普及HTTPS是未来的一个方向，所以强烈建议您将访问协议升级到HTTPS。

应用场景

主要将应用场景分为五类，如下表所示 。

应用场景	说明
企业应用	若网站内容包含crm、erp等信息，这些信息属于企业级的机密信息，若在访问过程中被劫持或拦截窃取，对企业是灾难级的影响。
政务信息	政务网站的信息具备权威性，正确性等特征，需预防钓鱼欺诈网站和信息劫持，避免出现信息劫持或泄露引起社会公共的信任危机。
支付体系	支付过程中，涉及到敏感信息如姓名，电话等，防止信息劫持和伪装欺诈，需启用HTTPS加密传输，避免出现下单后，下单客户会立即收到姓名、地址、下单内容，然后以卡单等理由要求客户按指示重新付款之类诈骗信息，造成客户和企业的双重损失。
API接口	保护敏感信息或重要操作指令的传输，避免核心信息在传输过程中被劫持。
企业网站	激活绿色安全标识（DV/OV）或地址栏企业名称标识（EV），为潜在客户带来更可信、更放心的访问体验。

HTTPS功能使用说明

HTTPS安全加速功能使用说明，如下表所示。

分类	注意事项

分类	注意事项

配置	• 支持开启HTTPS安全加速功能的业务类型如下：
	  ◦ 图片小文件
	  主要适用于各种门户网站、电子商务类网站、新闻资讯类站点或应用、政府或企业官网站点、娱乐游戏类站点或应用等。
	  ◦ 大文件下载
	  主要适用于下载类站点和音视频的应用。
	  ◦ 视音频点播
	  主要适用于各类视音频站点，如影视类视频网站、在线教育类视频网站、新闻类视频站点、短视频社交类网站以及音频类相关站点和应用。
	  ◦ 全站加速
	  主要适用于电商、社交、政企、游戏和金融平台。
	• 您可以配置泛域名的HTTPS服务。
	• 您可以启用或停止HTTPS安全加速。
	  ◦ 启用：您可以修改证书，系统默认兼容HTTP和HTTPS请求。您也可以配置强制跳转，自定义源请求方式。
	  ◦ 停用：停用后，系统不再支持HTTPS请求且不再保留证书或私钥信息。再次开启HTTPS安全加速时，需要重新上传证书或私钥。详细说明，请参见配置HTTPS证书。
	• 您可以查看证书，但由于私钥信息敏感，不支持私钥查看。请妥善保管证书相关信息。
	• 您可以更新证书，但请谨慎操作。更新HTTPS证书后1分钟内全网生效。

计费	HTTPS安全加速属于增值服务，开启后将产生HTTPS请求数计费，详细计费标准请参见静态HTTPS请求数。 说明 HTTPS根据请求数单独计费，费用不包含在CDN流量包内。请确保账户余额充足再开通HTTPS服务，以免因HTTPS服务欠费影响您的CDN服务。
证书	• 开启HTTPS安全加速功能的加速域名，您需要上传格式均为 PEM 的证书和私钥。 说明 由于CDN采用的Tengine服务基于Nginx，因此只支持Nginx能读取的 PEM 格式的证书。详细说明，请参见证书格式说明。 • 上传的证书需要和私钥匹配，否则会校验出错。 • 不支持带密码的私钥。 • 只支持携带SNI信息的SSL/TLS握手。 其他证书相关的常见问题，请参见更多证书问题。

相关功能

为了数据传输的安全，您可以根据实际业务需求，配置相关功能，如下表所示。

功能	说明
配置HTTPS证书	实现HTTPS安全加速。
设置HTTP/2	HTTP/2是最新的HTTP协议，Chrome、 IE11、Safari以及Firefox等主流浏览器已经支持HTTP/2协议。
配置强制跳转	强制重定向终端用户的原请求方式。
配置TLS	保障您互联网通信的安全性和数据完整性。
配置HSTS	强制客户端（如浏览器）使用HTTPS与服务器创建连接，降低第一次访问被劫持的风险。

8.2. 证书格式说明

您需要配置HTTPS证书，才能通过HTTPS方式访问资源，实现HTTPS安全加速。本文为您介绍了阿里云CDN支持的证书格式和不同证书格式的转换方式。

证书格式 HTTPS安全加速 PEM格式

ROOT CA机构颁发的证书

Root CA机构提供的证书是唯一的，一般包括Apache、IIS、Nginx和Tomcat。阿里云全站加速使用的证书是Nginx，证书格式为 `.crt` ，证书私钥格式为 `.key` 。

证书上传格式为：

- 请将开头 `-----BEGIN CERTIFICATE-----` 和结尾 `-----END CERTIFICATE-----` 一并上传。
- 每行64字符，最后一行不超过64字符。

在Linux环境下， `PEM` 格式的证书示例如下图。

```
-----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
AQUFBwMBBggrBgEFBQcDAjAfBgNVHSMEGDAWgBS17wsRzsBBA6NKZZBIshzgVy19
RzB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlz
aWduLmNvbTBABggrBgEFBQcwAoY0aHR0cDovL1NWUlNlY3VyZS1HMi1haWEudmVy
aXNpZ24uY29tL1NWUlNlY3VyZUcyLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFow
WDBWFglpbWFnZS9naWYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEF
GDAmFiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZI
hvcNAQEFBQADggEBALpFBXeG782QsTtGwEE9zBcVCuKjrsl3dWK1dFiq3OP4y/Bi
ZBYEywBt8zNuYFUE25Ub/zmvmpe7p0G76tmQ8bRp/4qkJoiSesHJvFgJ1mksr3IQ
3gaE1aN2BSUIHxGLn9N4F09hYwwbeEZaCxfgBiLdEIodNwzcvGJ+2LlDWGJOGrNI
NM856xjqhJCPxYzk9buuCl1B4Kzu0CTbexz/iEgYV+DiuTxcfA4uhwMDSe0nynbn
1qiwRk450mCOnqH4ly4P4lXo02t4A/DI1I8ZNct/Qfl69a2Lf6vc9rF7BELT0e5Y
R7CKx7fc5xRaeQdyGj/dJevm9BF/mSdnclS5vas=
-----END CERTIFICATE-----
```

中级机构颁发的证书

中级机构颁发的证书文件包含多份证书，您需要将服务器证书与中间证书拼接后，一起上传。

> 说明 拼接规则为：服务器证书放第一份，中间证书放第二份。一般情况下，机构在颁发证书的时候会有对应说明， 请注意规则说明。

中级机构颁发的证书链：

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

证书链规则：

- 证书之间不能有空行。
- 每一份证书遵守证书上传的格式说明。

RSA私钥格式要求

RSA私钥规则：

- 本地生成私钥：`openssl genrsa -out privateKey.pem 2048`。其中，`privateKey.pem`为您的私钥文件。
- 以`-----BEGIN RSA PRIVATE KEY-----`开头，以`-----END RSA PRIVATE KEY-----`结尾，请将这些内容一并上传。
- 每行64字符，最后一行长度可以不足64字符。

如果您并未按照上述方案生成私钥，得到如`-----BEGIN PRIVATE KEY-----`或`-----END PRIVATE KEY-----`样式的私钥时，您可以按照如下方式转换：

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

然后将`new_server_key.pem`的内容与证书一起上传。

证书格式转换方式

HTTPS配置只支持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。

  - 证书转化：

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

  - 私钥转化：

    ```
    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。

  - 证书转化：

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

    获取 `outcertificat.cer` 里面 `-----BEGIN CERTIFICATE-----` ， `-----END CERTIFICATE-----` 的内容作为证书上传。

  - 私钥转化：P7B证书无私钥，您只需在CDN控制台填写证书部分，私钥无需填写。

- PFX转换为PEM

  PFX格式一般出现在Windows Server中。

  - 证书转化：

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

  - 私钥转化：

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

8.3. 配置HTTPS证书

HTTPS是以安全为目标的HTTP通道，为CDN的网络内容传输提供了更好的保障。客户端在极速访问内容的同时，可以更安全有效的浏览网站内容。本文为您介绍了不同类型的HTTPS证书的认证方式和配置方法。

HTTPS安全加速加速域名CDN

前提条件

配置HTTPS证书前，您需要先购买证书，您可以在SSL证书服务控制台快速申请免费的证书或购买高级证书。

背景信息

目前，CDN仅支持 `PEM` 格式的证书。如果您的证书不是 `PEM` 格式，请进行格式转换，操作方法请参见证书格式转换方式。

HTTPS功能为增值服务，开启HTTPS将产生HTTPS请求数计费，该费用单独按量计费，不包含在CDN流量包内。HTTPS计费介绍，请参见增值服务计费。

根据认证级别不同，证书分类如下：

- DV（Domain Validation）：仅认证域名所有权通常是验证域名下指定文件内容，或者验证与域名相关TXT记录，显示明显的安全锁。
- OV（Organization Validation）：验证企业组织真实性的标准型SSL证书，比DV SSL证书更安全可信、审核更严格、审核周期也更长。一般多用于电商、教育、游戏等领域。
- EV（Extended Validation）：CA/Browser Forum指定的全球统一标准，通过证书Object Identifier（OID）来识别，显示完整企业名称，是目前全球较高等级的SSL证书，多用于金融支付、网上银行等领域。

> 说明 CDN的HTTPS证书不支持3DES算法。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**管理**。
4. 在指定域名的左侧导航栏，单击**HTTPS配置**。
5. 在**HTTPS证书**区域，单击**修改配置**。
6. 在**HTTPS设置**界面，打开**HTTPS安全加速**开关，配置证书相关参数。

> 说明 当您打开HTTPS安全加速开关时，系统弹出确认开启HTTPS界面，该操作单独计费，您可以根据所需选择是否开启。HTTPS计费标准请参见增值服务计费。


HTTPS设置
更新HTTPS证书后1分钟后全网生效。
HTTPS安全加速
HTTPS安全加速属于增值，服务开启后将产生HTTPS请求数计费。
证书类型
云盾证书
自定义上传（证书+私钥）
自定义上传（证书）
免费证书
证书名称
请选择证书
内容
pem编码参考样例
私钥
信息敏感证书私钥不可见
pem编码参考样例
您可以前往SSL证书控制台 管理上传证书 或 一键签发
确定
取消

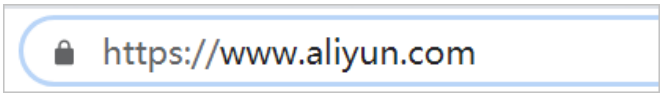
参数	说明

参数	说明
证书类型	○ **云盾证书** 您可以在SSL证书服务控制台快速申请各种品牌及各种类型证书。 ○ **自定义上传（证书+私钥）** 如果证书列表中无当前适配的证书，您可以选择自定义上传。您需要在设置证书名称后，上传证书内容和私钥，该证书将会在阿里云云盾的证书服务中保存。您可以在我的证书中查看。 ○ **自定义上传（证书）** 如果证书列表中无当前适配的证书，您可以选择自定义上传。**自定义上传（证书）**适合不希望自助上传私钥的用户，您需要在CDN证书服务中申请CSR文件后前往CA机构申请证书。具体操作请参见CSR生成工具。 ○ **免费证书** 免费证书只适用于HTTPS安全加速业务，因此您无法在阿里云云盾控制台管理该证书，也无法查看到公钥和私钥。 ■ 免费证书通常会在1~2个工作日签发。等待期间，您也可以重新选择上传自定义证书或云盾证书。 说明 根据CA中心审核流程，您申请的证书有可能会在几个小时内完成签发，也有可能需要2个工作日才完成签发，都属于正常现象，请您耐心等待即可。 ■ 免费证书有效期为1年，到期后自动续签。 ■ 在您使用过程中，如果关闭HTTPS安全加速，当再次开启使用免费证书时，将直接使用已申请但未过期的证书。若开启时证书已过期，您需要重新申请免费证书。 **云盾证书、自定义上传（证书+私钥）、自定义上传（证书）和免费证书之间可以相互切换。**
证书名称	当证书类型选择云盾证书或自定义上传（证书+私钥）时，需要配置证书名称。
内容	当证书类型选择自定义上传（证书+私钥）或自定义上传（证书）时，需要配置该参数。配置方法请参考内容输入框下方的pem编码参考样例。
私钥	当证书类型选择自定义上传（证书+私钥）时，需要配置该参数。配置方法请参考私钥输入框下方的pem编码参考样例。

7. 单击**确定**，完成配置。

后续步骤

更新HTTPS证书1分钟后全网生效。您可以验证证书是否生效，使用HTTPS方式访问资源，如果浏览器中出现锁的HTTPS标识，则HTTPS安全加速生效。



8.4. 设置HTTP/2

HTTP/2是最新的HTTP协议，提高了资源访问效率。通过本文档，您可以了解HTTP/2协议的概念、优势和设置方法。

HTTP/2协议 配置证书 CDN HTTP 2.0

前提条件

执行该操作前，请您确保已成功配置HTTPS证书，操作方法请参见配置HTTPS证书。

> 说明
> - 如果您是第一次配置HTTPS证书，则需要等证书配置完成且生效后，才能开启HTTP/2。
> - 如果您开启HTTP/2后，关闭了HTTPS证书功能，HTTP/2会自动失效。

背景信息

HTTP/2也被称为HTTP 2.0，相对于HTTP 1.1的新增多路复用、压缩HTTP头、划分请求优先级、服务端推送等特性，解决了在HTTP 1.1中一直存在的问题，优化了请求性能，同时兼容了HTTP 1.1的语义。目前，Chrome、 IE11、Safari和Firefox等浏览器已经支持HTTP/2协议。

HTTP/2的优势：

- 二进制协议：相比于HTTP 1.x基于文本的解析，HTTP/2将所有的传输信息分割为更小的消息和帧，并对它们采用二进制格式编码。基于二进制可以使协议有更多的扩展性，例如，引入帧来传输数据和指令。
- 内容安全：HTTP/2基于HTTPS，具有安全特性。使用HTTP/2特性可以避免单纯使用HTTPS引起的性能下降问题。
- 多路复用（MultiPlexing）：通过该功能，在一条连接上，您的浏览器可以同时发起无数个请求，并且响应可以同时返回。另外，多路复用中支持了流的优先级（Stream dependencies）设置，允许客户端告知服务器最优资源，可以优先传输。
- Header压缩（Header compression）：HTTP请求头带有大量信息，而且每次都要重复发送。HTTP/2采用HPACK格式进行压缩传输，通讯双方各自缓存一份头域索引表，相同的消息头只发送索引号，从而提高效率和速度。
- 服务端推送（Server push）：同SPDY一样，HTTP/2也具有客户端推送功能。目前，大多数网站已经启用HTTP/2，如淘宝。使用浏览器Chrome登录控制台，您可以查看是否启用HTTP/2。

> 说明 SPDY是基于TCP的应用层协议，用以最小化网络延迟，提升网络速度，优化用户的网络体验。SPDY并不是一种用于替代HTTP的协议，而是对HTTP协议的增强。新协议的功能包括：数据流的多路复用、请求优先级和HTTP报头压缩，与HTTP/2相似。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击HTTPS配置。
5. 在HTTP/2设置区域，打开HTTP/2开关，开启该功能。

8.5. 配置强制跳转

您可以通过配置强制跳转功能，将客户端至L1的原请求方式强制重定向为HTTP或者HTTPS。通过本文档，您可以了解配置强制跳转的操作方法。

强制跳转 CDN HTTPS安全加速

前提条件

执行该操作前，请您确保已成功配置HTTPS证书，操作方法请参见配置HTTPS证书。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击HTTPS配置。
5. 在强制跳转区域，单击修改配置。
6. 在强制跳转对话框，选择跳转类型。

跳转类型	说明
默认	同时支持HTTP和HTTPS方式的请求。
HTTPS -> HTTP	客户端到L1的请求将强制重定向为HTTP方式。
HTTP -> HTTPS	客户端到L1的请求将强制重定向为HTTPS方式，确保访问安全。

以跳转类型为HTTP -> HTTPS为例，介绍强制跳转功能。

当您设置了强制HTTPS跳转后，客户端发起一个HTTP请求，服务端返回301重定向响应，原HTTP请求强制重定向为HTTPS请求，如下图所示。

```
$ curl http://[redacted]/' -i
HTTP/1.1 301 Moved Permanently
Server: Tengine
Date: Mon, 03 Jun 2019 13:26:01 GMT
Content-Type: text/html
Content-Length: 278
Connection: keep-alive
Location: https://[redacted]/
Via: cache2.cn201[,0]
Timing-Allow-Origin: *
EagleId: 2a786b0215595683612635433e

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<h1>301 Moved Permanently</h1>
<p>The requested resource has been assigned a new permanent URI.</p>
<hr/>Powered by Tengine</body>
</html>
```

7. 单击确定。

8.6. 配置TLS

为了保障您互联网通信的安全性和数据完整性，阿里云CDN提供TLS版本控制功能。您可以根据不同域名的需求，灵活地配置TLS协议版本。通过本文档，您可以了解配置TLS协议的操作方法。

TLS协议 HTTPS证书

前提条件

执行该操作前，请您确保已成功配置HTTPS证书，操作方法请参见配置HTTPS证书。

背景信息

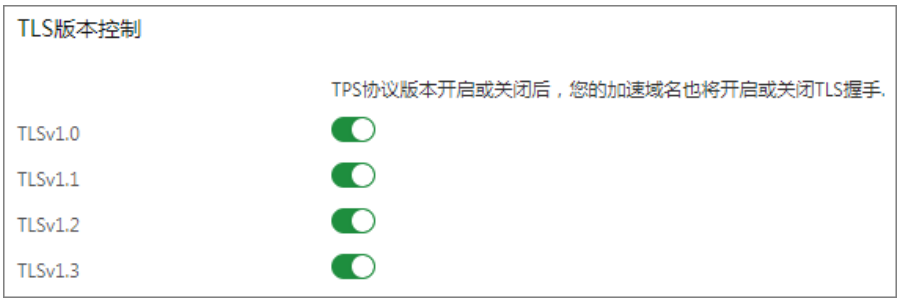
TLS（Transport Layer Security）即安全传输层协议，在两个通信应用程序之间提供保密性和数据完整性。最典型的应用就是HTTPS。HTTPS，即HTTP over TLS，就是安全的HTTP，运行在HTTP层之下，TCP层之上，为HTTP层提供数据加解密服务。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击HTTPS配置。
5. 在TLS版本控制区域，根据所需开启或关闭对应的TLS版本。

   TLS协议说明如下表所示。

协议	说明	支持的主流浏览器
TLSv1.0	RFC2246，1999年发布，基于SSLv3.0，该版本易受各种攻击（如BEAST和POODLE），除此之外，支持较弱加密，对当今网络连接的安全已失去应有的保护效力。不符合PCI DSS合规判定标准。	○ IE6+ ○ Chrome 1+ ○ Firefox 2+
TLSv1.1	RFC4346，2006年发布，修复TLSv1.0若干漏洞。	○ IE 11+ ○ Chrome 22+ ○ Firefox 24+ ○ Safri 7+
TLSv1.2	RFC5246，2008年发布，目前广泛使用的版本。	○ IE 11+ ○ Chrome 30+ ○ Firefox 27+ ○ Safri 7+
TLSv1.3	RFC8446，2018年发布，最新的TLS版本，支持0-RTT模式（更快），只支持完全前向安全性密钥交换算法（更安全）。	○ Chrome 70+ ○ Firefox 63+



> 说明 目前TLSv1.0、TLSv1.1和TLSv1.2版本默认开启。

8.7. 配置HSTS

通过开启HSTS（HTTP Strict Transport Security）功能，您可以强制客户端（例如：浏览器）使用HTTPS与服务器创建连接，降低第一次访问请求被拦截的风险。

HSTS CDN HTTPS连接

前提条件

执行该操作前，请您确保已成功配置HTTPS证书，操作方法请参见配置HTTPS证书。

背景信息

当您全站使用HTTPS请求时，在浏览器输入或直接单击HTTP链接，服务器会将该HTTP请求301或302重定向到HTTPS。该操作过程中请求可能被拦截，导致重定向后的请求未发送到服务器，该问题可以通过HSTS来解决。

浏览器处理域名的HTTP访问时，若该域名的HSTS没有过期，则在浏览器内部做一次307重定向到HTTPS，从而避免浏览器和服务器之间301或302重定向请求被拦截的风险。

HSTS响应头结构为：`Strict-Transport-Security:max-age=expireTime [;includeSubDomains] [;preload]`，参数说明如下表所示。

参数	说明
max-age	HSTS Header的过期时间，单位为秒。
includeSubDomains	可选参数。如果包含这个参数，说明该域名及其所有子域名均开启HSTS。
preload	可选参数。当您申请将域名加入到浏览器内置列表时需要使用preload列表。

> 说明
>
> - HSTS生效前，第一次需要将301或302重定向到HTTPS。
> - HSTS响应头在HTTPS访问的响应中有效，在HTTP访问的响应中无效。
> - 仅对443端口有效，对其他端口无效。
> - 仅对域名有效，对IP无效。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击HTTPS配置。
5. 在HSTS区域，单击修改配置。
6. 在HSTS设置对话框，打开HSTS开关。
7. 配置过期时间，打开包含子域名开关。

> 说明
> - 过期时间表示HSTS响应头在浏览器的缓存时间，建议填入60天，可填时间范围为0~730天。
> - 开启包含子域名开关前，请确保该加速所有子域名都已开启HTTPS，否则会导致子域名自动跳转到HTTPS后无法访问。

8. 单击确定。

8.8. 设置OCSP Stapling

OCSP Stapling功能是由CDN服务器查询OCSP（Online Certificate Status Protocol）信息，可以降低客户端验证请求延迟，减少等待查询结果的响应时间。通过本文档，您可以了解OCSP Stapling功能的使用场景和控制台开启该功能的操作步骤。

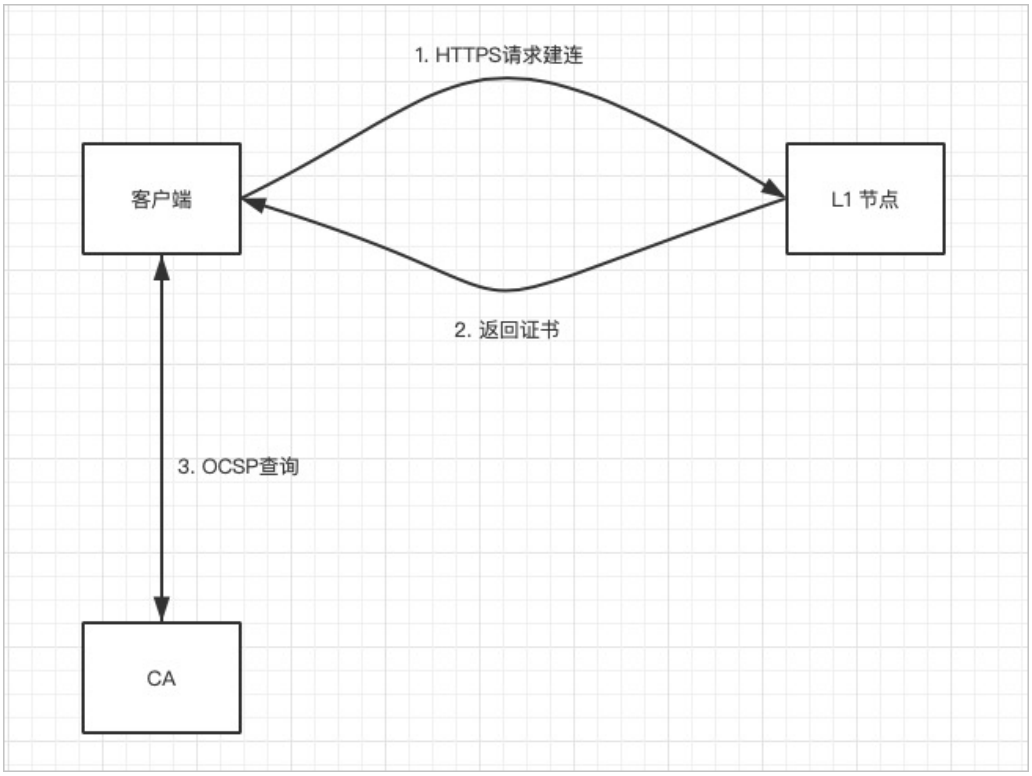
前提条件

使用OCSP Stapling功能需要客户端支持OCSP扩展字段，客户端不支持，则无法生效。

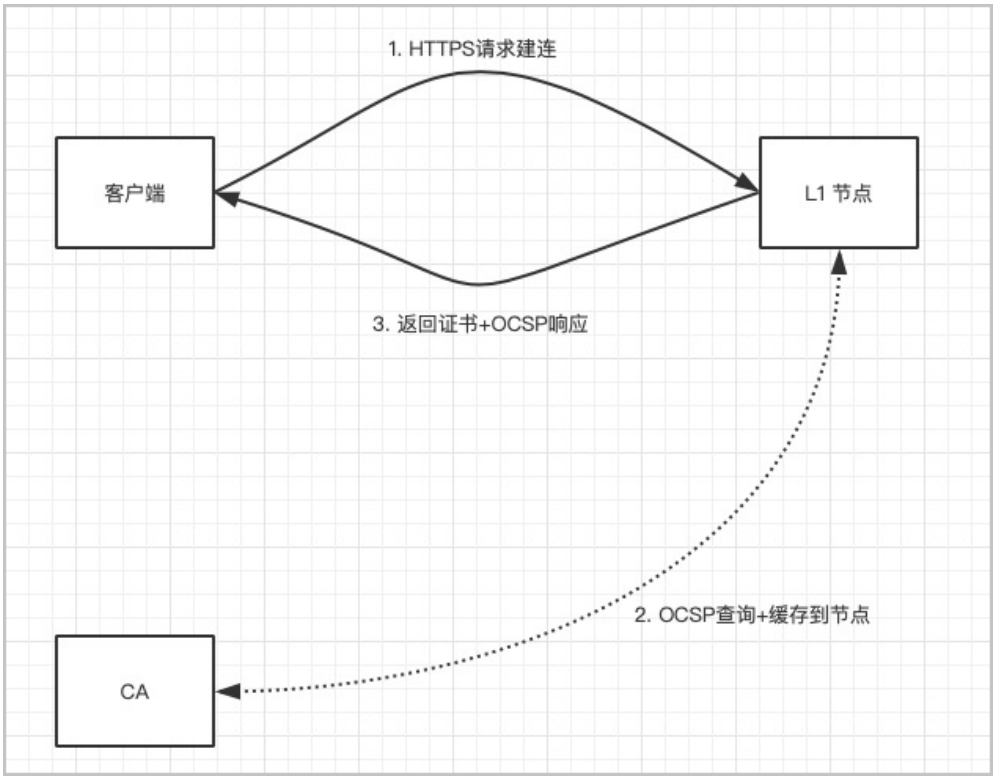
背景信息

OCSP信息是由数字证书颁发机构CA（Certificate Authority）提供，用于在线实时验证证书的合法性和有效性。

痛点：客户端（例如：浏览器）根据证书中的OCSP信息，将查询请求发送到CA的验证地址，检查此证书是否合法、有效。在网络状况不佳的情况下，客户端在等待获取查询结果时，会造成长时间的页面空白，阻塞您终端用户的后续操作。



功能解决痛点：OCSP Stapling功能将查询OCSP信息的工作由CDN服务器完成。CDN通过低频次查询，将查询结果缓存到服务器中。当客户端向服务器发起TLS握手请求时，CDN服务器将证书的OCSP信息和证书链一起发送到客户端。这样可以避免客户端验证会产生的阻塞问题。由于OCSP信息是无法伪造的，因此这一过程不会产生额外的安全问题。



说明

- OCSP Stapling的功能开启后，默认平台缓存时间60分钟。
- OCSP Stapling缓存过期时，第一个访问请求OCSP Stapling是不生效。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击HTTPS配置。
5. 在OCSP Stapling区域，打开开关。

8.9. 常见问题

本文为您介绍了HTTPS配置常见问题。

- CDN开启HTTPS加速后，会有额外收费吗？
- 开启HTTPS加速，会消耗更多资源或降低访问速度吗？
- 站点只有登录才需要HTTPS，其他都不需要HTTPS吗？
- 常见的HTTP攻击类型有哪些？

CDN开启HTTPS加速后，会有额外收费吗？

会额外收费。CDN开启HTTPS加速，开启的是客户端到CDN边缘节点这段链路的HTTPS。因为SSL协议的握手、内容解密都需要计算，所以会增加CDN服务器的CPU资源损耗。但是不会增加客户源站的服务器资源损耗，因为CDN边缘节点到客户源站这段链路使用的仍然是HTTP协议，对客户源站没有额外增加损耗。

- 若您购买不同类型的证书，则需要额外付费。

  > 说明 您可以直接登录CDN控制台。申请免费证书。免费证书等级为DV，每个加速域名可以申请一个免费证书，证书有效期为一年，到期后可以免费自动续签。

- 设置好HTTPS证书后，该域名的所有在CDN上的HTTPS请求数会收费，静态HTTPS请求数收费标准为每万次0.05元。

开启HTTPS加速，会消耗更多资源或降低访问速度吗？

不会消耗更多服务资源，也不会降低访问速度。

您首次访问HTTPS站点比HTTP要慢，因为建立SSL连接需要的时间更长，首次页面加载速度慢了约10%。但是浏览器建立了活跃的keep-alive HTTPS连接后，后续的页面刷新性能和HTTP几乎无差别。

站点只有登录才需要HTTPS，其他都不需要HTTPS吗？

不是。

- 从安全看，一些页面为HTTP，一些页面为HTTPS，当通过HTTP或不安全的CDN服务加载其他资源（例如JS或CSS文件）时网站也存在用户信息暴露的风险，而全站HTTPS是防止这种风险最简单的方法。
- 从性能看，当网站存在HTTPS和HTTP两种协议时，跳转需对服务器进行大量的重定向，当这些重定向被触发时会减慢页面加载速度。
- 从全网来看，浏览器对HTTPS的支持会更友好，搜索引擎也对HTTPS的收录有更好的支持。

常见的HTTP攻击类型有哪些？

HTTPS只是安全访问的其中一环，如需全面保证网络安全，则还需要接入WAF、DDoS等防御能力，以下为常见的HTTP攻击类型：

- SQL注入：它是利用现有应用程序，将（恶意）的SQL命令注入到后台数据库引擎执行的能力，它可以通过在Web表单中输入（恶意）SQL语句得到一个存在安全漏洞的网站上的数据库，而不是按照设计者意图去执行SQL语句。
- 跨站脚本攻击：跨站脚本攻击XSS（Cross-site scripting）是最常见和基本的攻击WEB网站的方法。攻击者在网页上发布包含攻击性代码的数据。当浏览者看到此网页时，特定的脚本就会以浏览者用户的身份和权限来执行。通过XSS可以比较容易地修改用户数据、窃取用户信息。
- 跨站请求伪造攻击：跨站请求伪造CSRF（Cross-site request forgery）是另一种常见的攻击。攻击者通过各种方法伪造一个请求，模仿用户提交表单的行为，从而达到修改用户的数据，或者执行特定任务的目的。为了假冒用户的身份，CSRF攻击常常和XSS攻击配合起来做，但也可以通过其它手段，例如诱使用户单击一个包含攻击的链接。
- Http Heads攻击：凡是用浏览器查看任何WEB网站，无论您的WEB网站采用何种技术和框架，都用到了HTTP协议。HTTP协议在Response header和content之间，有一个空行，即两组CRLF（0x0D 0A）字符。这个空行标志着headers的结束和content的开始。“聪明”的攻击者可以利用这一点。只要攻击者有办法将任意字符“注入”到 Headers中，这种攻击就可以发生。
- 重定向攻击：一种常用的攻击手段是“钓鱼”。钓鱼攻击者，通常会发送给受害者一个合法链接，当链接被点击时，用户被导向一个似是而非的非法网站，从而达到骗取用户信任、窃取用户资料的目的。为防止这种行为，我们必须对所有的重定向操作进行审核，以避免重定向到一个危险的地方。常见解决方案是白名单，将合法的要重定向的URL加到白名单中，非白名单上的域名重定向时拒绝。第二种解决方案是重定向token，在合法的URL上加上token，重定向时进行验证。

9.访问控制

9.1. 概述

您可以通过设置Referer、IP、UsageAgent黑名单和白名单，以及URL鉴权，来实现对访客身份的识别和过滤，从而限制访问CDN资源的用户，提升CDN的安全性。

您可以通过CDN的访问控制功能，对域名执行如下操作。

功能	说明
配置Referer防盗链	您可以通过配置访问的Referer黑名单和白名单来实现对访客身份的识别和过滤，限制访问CDN资源的用户。
URL鉴权	您可以通过配置URL鉴权功能保护用户站点的资源不被非法站点下载盗用。URL鉴权比Referer防盗链安全性更高。
IP黑白名单	您可以通过配置IP黑名单和白名单来实现对访客身份的识别和过滤，限制访问CDN资源的用户。
配置UA黑/白名单	您可以通过配置UsageAgent黑名单和白名单来实现对访客身份的识别和过滤，限制访问CDN资源的用户。

9.2. 配置Referer防盗链

您可以通过配置访问的Referer黑名单和白名单来实现对访客身份的识别和过滤，从而限制访问CDN缓存节点资源的用户，提升CDN的安全性。通过本文，您可以了解Referer防盗链的配置方法。

防盗链 CDN

背景信息

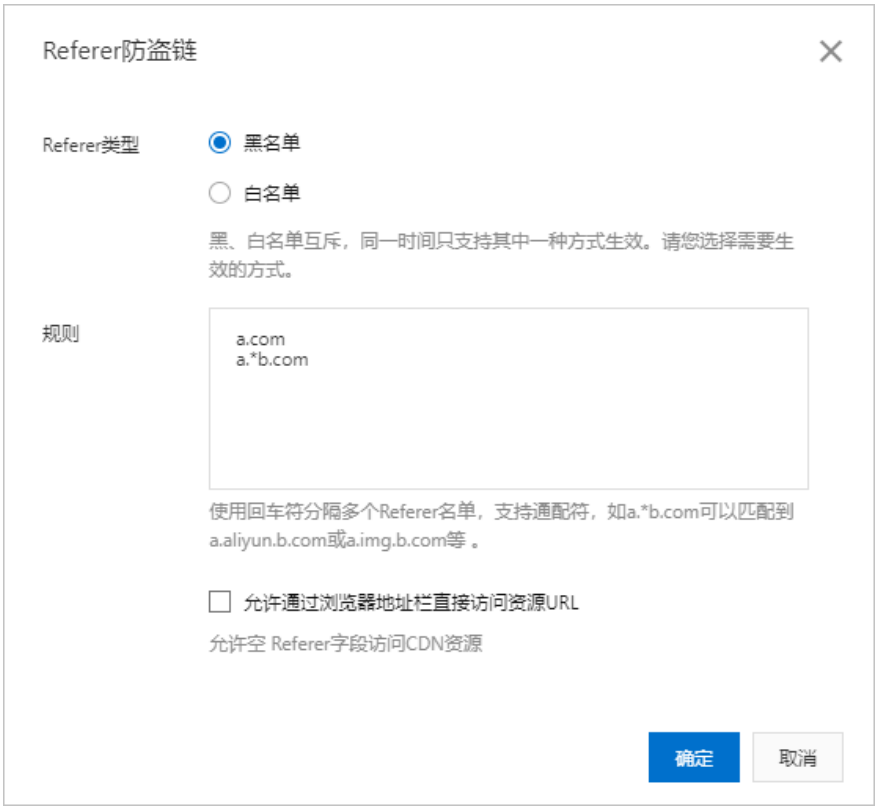
- 防盗链功能基于HTTP协议支持的Referer机制，通过Referer跟踪来源，对来源进行识别和判断。
- 目前防盗链功能支持黑名单或白名单机制，您对资源发起请求后，请求到达CDN节点，CDN节点会根据您预设的防盗链黑名单或白名单，对访客的身份进行过滤。符合规则的用户可以顺利请求到资源，不符合规则的用户，请求会返回403响应码。

> 注意
>
> - 防盗链是可选配置，默认不启用。
> - 黑白名单互斥，同一时间您只能选择一种方式。
> - 配置防盗链后，CDN支持自动添加泛域名。例如，如果您填写 `a.com` ，则最终配置生效的是 `*.a.com` ，所有子级域名都会生效。
> - 您可以设置是否允许空Referer字段访问资源，即允许通过浏览器地址栏直接访问资源URL。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击访问控制。
5. 在Referer防盗链区域，单击修改配置。
6. 根据界面提示，设置黑名单或白名单。

参数	说明
Referer类型	Referer防盗链类型如下： ○ 黑名单 黑名单内的域名均无法访问当前的资源。 ○ 白名单 只有白名单内的域名能访问当前资源，白名单以外的域名均无法访问当前的资源。 黑名单和白名单互斥，同一时间只支持其中一种方式生效。
规则	使用回车符分隔多个Referer黑名单或白名单，并支持通配符（*）。例如配置 a.*b.com ，可以匹配到 a.aliyun.b.com 或 a.img.b.com 等。



7. 单击确定完成配置。

9.3. URL鉴权配置

9.3.1. URL鉴权

URL鉴权功能主要用于保护用户站点的资源不被非法站点下载盗用。通过防盗链方法添加Referer黑名单和白名单的方式可以解决一部分盗链问题，由于Referer内容可以伪造，所以Referer防盗链方式无法彻底保护站点资源。因此，您可以采用URL鉴权方式保护源站资源更为安全有效。

鉴权 CDN 访问控制

背景信息

URL鉴权功能通过阿里云CDN加速节点与客户资源站点配合，形成了更为安全可靠的源站资源防盗方法。

- CDN客户站点提供加密URL，URL中包含权限验证信息。
- 用户使用加密后的URL向加速节点发起请求。
- 加速节点对加密URL中的权限信息进行验证，判断请求的合法性。正常响应合法请求，拒绝非法请求。

如果您想了解Python鉴权代码示例，请参见 鉴权示例。

> 注意 您的请求URL经过CDN鉴权后，URL中的特殊字符，例如：`=`、`+`等会被转义。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**管理**。
4. 在指定域名的左侧导航栏，单击**访问控制**。
5. 在右侧域名管理区域，单击**URL鉴权**。
6. 在**鉴权URL设置**区域，单击**修改配置**。
7. 打开**URL鉴权**开关，配置URL鉴权信息。

参数	说明
鉴权类型	阿里云CDN兼容并支持三种鉴权方式。您可以根据自己的业务情况，选择合适的鉴权方式，来实现对源站资源的有效保护。URL鉴权类型如下： ○ 鉴权方式A说明 ○ 鉴权方式B说明 ○ 鉴权方式C说明 说明 URL鉴权错误，都会返回403报错。 ○ MD5计算类错误 例如：X-Tengine-Error:denied by req auth: invalid md5hash=de7bfdc915ced05e17380a149bd760be ○ 时间类报错 例如：X-Tengine-Error:denied by req auth: expired timestamp=1439469547
主KEY	输入鉴权方式对应的主用密码。
备KEY	输入鉴权方式对应的备用密码。

8. 单击确定。

后续步骤

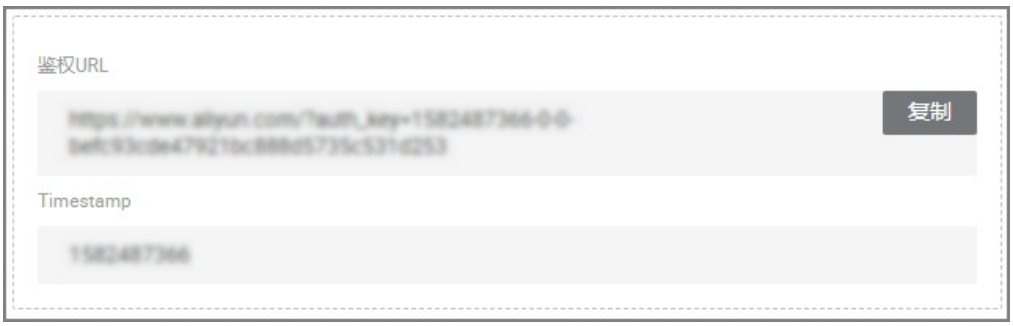
生成鉴权URL的操作方法如下：

1. 在生成鉴权URL区域，配置原始URL和鉴权信息。

参数	说明
原始URL	您可以输入完整的原始URL地址，例如：`https://www.aliyun.com`。
鉴权类型	您可以根据所需，选择合适的URL鉴权类型： ○ 鉴权方式A说明 ○ 鉴权方式B说明 ○ 鉴权方式C说明
鉴权KEY	您可以根据所需，设置鉴权密码。鉴权KEY是鉴权URL设置中配置的主KEY或备KEY。
有效时间	您可以根据所需，设置URL鉴权的有效时长。单位为：秒，例如：1800。

2. 单击开始生成。

   获得鉴权URL和Timestamp。



9.3.2. 鉴权方式A说明

URL鉴权功能主要用于保护用户站点资源不被非法站点下载盗用。阿里云CDN为您提供了三种鉴权方式，本文为您详细介绍鉴权方式A的原理和示例说明。

阿里云cdn鉴权 cdn鉴权

原理说明

访问加密URL构成：

```
http://DomainName/Filename?auth_key=timestamp-rand-uid-md5hash
```

鉴权字段描述如下表所示。

字段	描述
DomainName	CDN站点的域名。
Filename	实际回源访问的URL，鉴权时Filename需以正斜线（ / ）开头。
auth_key	您设定的鉴权密钥。
timestamp	失效时间，整型正数，固定长度10，值为1970年1月1日以来的当前时间秒数+过期时间秒数。用来控制失效时间，过期时间由客户端设置，若设置为1800s，您访问CDN的时间超过1800s后，该鉴权失效。 例如，您设置访问时间为2020-08-15 15:00:00，则链接的真正失效时间为2020-08-15 15:30:00。
rand	随机数。建议使用UUID，不能包含中划线（ - ），例如：477b3bbc253f467b8def6711128c7bec。
uid	用户ID，暂未使用（设置成0即可）。
md5hash	通过md5算法计算出的字符串，由数字0-9和小写英文字母a-z混合组成，固定长度32。

CDN服务器接到资源访问请求后，判断最终生成鉴权URL请求中的 timestamp + *鉴权key的有效时间* 是否小于当前时间。

- 如果 timestamp + 鉴权key的有效时间 小于当前时间，服务器判定过期失效，并返回HTTP 403错误。
- 如果 timestamp + 鉴权key的有效时间 大于当前时间，构造出一个同样的字符串，参考下方 sstring 字符串，然后使用MD5算法算出 HashValue 的值，再与请求中 md5hash 的值进行比对。
  - 结果一致，鉴权通过，返回资源请求。
  - 结果不一致，鉴权失败，返回HTTP 403错误。

  HashValue 的值是通过以下字符串计算得到的。

```
sstring = "URI-Timestamp-rand-uid-PrivateKey"（URI是用户的请求对象相对地址，不包含参数，如/Filename
）
HashValue = md5sum(sstring)
```

示例说明

通过以下示例说明，您可以准确理解鉴权方式A的实现方式。

1. 通过 `req_auth` 请求对象。

   ```
   http:// cdn.example.com/video/standard/1K.html
   ```

2. 设置密钥为：aliyuncdnexp1234。
3. 设置鉴权配置文件有效时间为：2015年10月10日00:00:00，计算出秒数为：1444435200。
4. CDN服务器会构造一个用于计算 `Hashvalue` 的签名字符串。

   ```
   /video/standard/1K.html-1444435200-0-0-aliyuncdnexp1234
   ```

5. 根据该签名字符串，CDN服务器会计算出 `Hashvalue` 。

   ```
   HashValue = md5sum("/video/standard/1K.html-1444435200-0-0-aliyuncdnexp1234") = 80cd3862d699
   b7118eed99103f2a3a4f
   ```

6. 加密URL请求。

   ```
   http://cdn.example.com/video/standard/1K.html?auth_key=1444435200-0-0-80cd3862d699b7118eed9
   9103f2a3a4f
   ```

如果计算出来的 `HashValue` 值与请求中带的 `md5hash` 值相同，都为*80cd3862d699b7118eed99103f2a3a4f*，则鉴权通过；反之鉴权失败。

9.3.3. 鉴权方式B说明

URL鉴权功能主要用于保护用户站点资源不被非法站点下载盗用。阿里云CDN为您提供了三种鉴权方式，本文为您详细介绍鉴权方式B的原理和示例说明。

阿里云cdn鉴权 cdn鉴权

原理说明

访问加密URL格式：

```
http://DomainName/timestamp/md5hash/FileName
```

当鉴权通过时，实际回源的URL格式：

```
http://DomainName/FileName
```

鉴权字段描述如下表所示。

字段	描述
DomainName	CDN站点的域名。
timestamp	资源失效时间，作为URL的一部分，同时作为计算 `md5hash` 的一个因子，格式为：YYYYMMDDHHMM，有效时间1800s。 例如您设置访问时间为2020-08-15 15:00:00，则链接的真正失效时间为2020-08-15 15:30:00。
md5hash	通过md5算法计算出的验证串，由数字0-9和小写英文字母a-z混合组成，固定长度32。
Filename	实际回源访问的URL，鉴权时Filename需以 `/` 开头。

示例说明

通过以下示例说明，您可以准确理解鉴权方式B的实现方式。

1. 回源请求对象。

   ```
   http://cdn.example.com/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3
   ```

2. 密钥为：aliyuncdnexp1234。
3. 访问源服务器时间为： 201508150800。
4. CDN服务器构造一个用于计算 `Hashvalue` 的签名字符串。

   ```
   aliyuncdnexp1234201508150800/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3
   ```

5. 服务器根据签名字符串 `Hashvalue` 计算 `md5hash` 。

   ```
   md5hash = md5sum("aliyuncdnexp1234201508150800/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3")
   = 9044548ef1527deadafa49a890a377f0
   ```

6. 加密URL请求。

   ```
   http://cdn.example.com/201508150800/9044548ef1527deadafa49a890a377f0/4/44/44c0909bcfc20a01
   afaf256ca99a8b8b.mp3
   ```

如果计算出来的 `md5hash` 值与请求中带的 `md5hash` 值相同，都为*9044548ef1527deadafa49a890a377f0*，则鉴权通过；反之鉴权失败。

9.3.4. 鉴权方式C说明

URL鉴权功能主要用于保护用户站点资源不被非法站点下载或盗用。阿里云CDN为您提供了三种鉴权方式，本文为您详细介绍鉴权方式C的原理和示例说明。

阿里云cdn鉴权 cdn鉴权

原理说明

访问加密URL格式如下：

- 格式1

```
http://DomainName/{<md5hash>/<timestamp>}/FileName
```

- 格式2

```
http://DomainName/FileName{&KEY1=<md5hash>&KEY2=<timestamp>}
```

> 说明 {} 中的内容表示在标准URL基础上添加的加密信息。

鉴权字段描述如下表所示。

字段	描述
DomainName	CDN站点的域名。
FileName	实际回源访问的URL，鉴权时Filename需以 / 开头。
timestamp	访问源服务器时间，取UNIX时间。未加密的字符串，以明文表示。固定长度10，1970年1月1日以来的秒数，表示为十六进制。
md5hash	通过md5算法计算出的字符串，由数字0-9和小写英文字母a-z混合组成，固定长度32。

示例说明

通过以下示例说明，您可以准确理解鉴权方式C的实现方式。

- PrivateKey取值：`aliyuncdnexp1234`。
- FileName取值：`/test.flv`。
- timestamp取值：`55CE8100`。
- md5hash计算值为：

  ```
  md5hash = md5sum(aliyuncdnexp1234/test.flv55CE8100) = a37fa50a5fb8f71214b1e7c95ec7a1bd
  ```

- 生成加密URL：
  - 格式一：

    ```
    http://cdn.example.com/a37fa50a5fb8f71214b1e7c95ec7a1bd/55CE8100/test.flv
    ```

  - 格式二：

    ```
    http://cdn.example.com/test.flv?KEY1=a37fa50a5fb8f71214b1e7c95ec7a1bd&KEY2=55CE8100
    ```

当您使用加密URL访问CDN加速节点时，CDN服务器先把加密串1提取出来，并得到原始URL的`FileName`和访问时间，然后按照定义的业务逻辑进行验证，验证步骤如下：

1. 使用原始的URL中的`Filename`、请求时间及`PrivateKey`进行md5加密得到一个加密串2。
2. 比较加密串2与加密串1是否一致，如果不一致则拒绝。
3. 取加速节点服务器当前时间，并与从访问URL中所带的时间相减，判断是否超过设置的时限t，时间域值t默认为1800s。
   - 时间差小于设置时限，请求合法，CDN加速节点正常响应。
   - 时间差大于设置时限，拒绝该请求，并返回HTTP 403。

> 说明 有效时间1800s是指，当您访问源服务器时间超过自定义时间的1800s后，鉴权失效。例如，您设置了访问时间2020-08-15 15:00:00，链接真正失效时间是2020-08-15 15:30:00。

9.3.5. 鉴权示例

本文以Python Demo为您示例，介绍三种鉴权方式的实现方法。

鉴权

Python版本

鉴权方式说明，请参见：

- 鉴权方式A说明
- 鉴权方式B说明
- 鉴权方式C说明

Demo示例如下所示。

> 说明 如果URL中包含中文，请进行UrlEncode编码。

```
import re
import time
import hashlib
import datetime
def md5sum(src):
m = hashlib.md5()
m.update(src)
return m.hexdigest()
#鉴权方式A
def a_auth(uri, key, exp):
p = re.compile("^(http://|https://)?([^/?]+)(/[^?]*)?(\\?.*)?$")
if not p:
return None
m = p.match(uri)
scheme, host, path, args = m.groups()
if not scheme: scheme = "http://"
if not path: path = "/"
if not args: args = ""
rand = "0" # "0" by default, other value is ok
uid = "0" # "0" by default, other value is ok
sstring = "%s-%s-%s-%s-%s" %(path, exp, rand, uid, key)
hashvalue = md5sum(sstring)
auth_key = "%s-%s-%s-%s" %(exp, rand, uid, hashvalue)
if args:
return "%s%s%s%s&auth_key=%s" %(scheme, host, path, args, auth_key)
else:
return "%s%s%s%s?auth_key=%s" %(scheme, host, path, args, auth_key)
#鉴权方式B
def b_auth(uri, key, exp):
p = re.compile("^(http://|https://)?([^/?]+)(/[^?]*)?(\\?.*)?$")
if not p:
return None
m = p.match(uri)
scheme, host, path, args = m.groups()
if not scheme: scheme = "http://"
if not path: path = "/"
if not args: args = ""
# convert unix timestamp to "YYmmDDHHMM" format
nexp = datetime.datetime.fromtimestamp(exp).strftime('%Y%m%d%H%M')
```

```
sstring = key + nexp + path
hashvalue = md5sum(sstring)
return "%s%s/%s/%s%s%s" %(scheme, host, nexp, hashvalue, path, args)
#鉴权方式C
def c_auth(uri, key, exp):
p = re.compile("^(http://|https://)?([^/?]+)(/[^?]*)?(\\?.*)?$")
if not p:
return None
m = p.match(uri)
scheme, host, path, args = m.groups()
if not scheme: scheme = "http://"
if not path: path = "/"
if not args: args = ""
hexexp = "%x" %exp
sstring = key + path + hexexp
hashvalue = md5sum(sstring)
return "%s%s/%s/%s%s%s" %(scheme, host, hashvalue, hexexp, path, args)
def main():
uri = "http://xc.cdnpe.com/ping?foo=bar" # original uri
key = "<input private key>" # private key of authorization
exp = int(time.time()) + 1 * 3600 # expiration time: 1 hour after current itme
authuri = a_auth(uri, key, exp) # auth type: a_auth / b_auth / c_auth
print("URL : %s\nAUTH: %s" %(uri, authuri))
if __name__ == "__main__":
main()
```

9.4. IP黑白名单

您可以通过配置IP黑名单和白名单来实现对访客身份的识别和过滤，从而限制访问CDN资源的用户，提升CDN的安全性。通过本文您可以了解IP黑/白名单的配置方法。

cdn白名单ip黑名单ip白名单

背景信息

- IP黑名单：黑名单内的IP均无法访问当前资源。

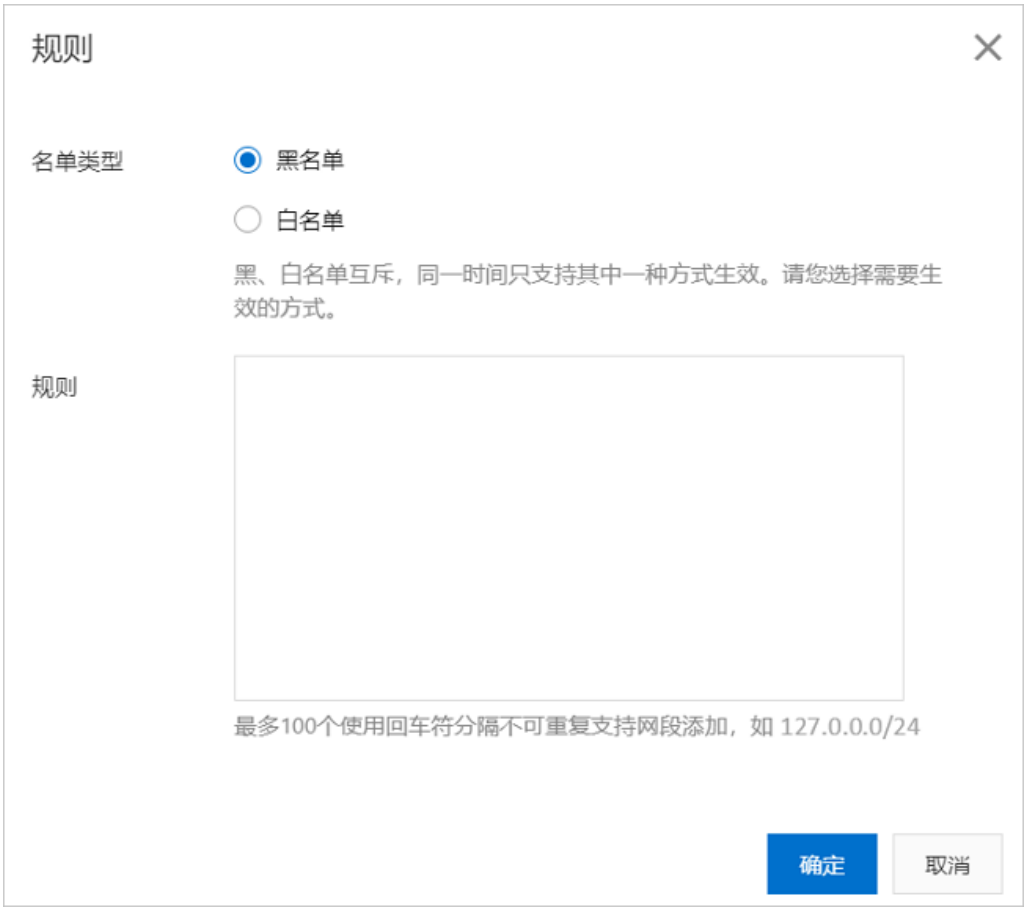
  如果您的IP被加入黑名单，该IP的请求仍可访问到CDN节点，但是会被CDN节点拒绝并返回403，CDN日志中仍会记录这些黑名单中的IP请求记录。

- IP白名单：只有白名单内的IP能访问当前资源，白名单以外的IP均无法访问当前资源。

> 说明
>
> - IP黑名单和白名单均支持IPv6地址（地址中的字母仅支持大写字母），例如：2001:DB8:0:23:8:800:200C:417A或2001:0DB8:0000:0023:0008:0800:200C:417A。IPv6地址不支持缩写格式，例如：2001:0DB8::0008:0800:200C:417A。
> - IP黑名单和白名单均支持IP网段添加。例如：192.168.0.0/24，24表示采用子网掩码中的前24位有效位，即用32-24=8bit来表示主机号，该子网可以容纳2^8-2=254台主机。故192.168.0.0/24表示IP网段范围是：192.168.0.1~192.168.0.254。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**管理**。
4. 在指定域名的左侧导航栏，单击**访问控制**。
5. 在右侧域名管理区域，单击**IP黑/白名单**。
6. 在**IP黑/白名单**区域，单击**修改配置**。
7. 根据界面提示，配置IP的**黑名单**或**白名单**。



参数	说明
名单类型	IP名单类型如下： ◦ 黑名单 黑名单内的IP均无法访问当前资源。 ◦ 白名单 只有白名单内的IP能访问当前资源，白名单以外的IP均无法访问当前资源。 黑名单和白名单互斥，同一时间只支持其中一种方式生效。
规则	最多配置100个IP地址，使用回车符分隔，不可配置重复网段，例如：127.0.0.0/24。

8. 单击确定。

9.5. 配置UA黑/白名单

您可以通过配置UserAgent黑名单和白名单来实现对访客身份的识别和过滤，从而限制访问CDN资源的用户，提升CDN的安全性。通过本文，您可以了解UserAgent黑/白名单的配置方法。

黑白名单UserAgent

背景信息

当您需要根据请求的UserAgent字段进行访问控制时，请配置UserAgent黑/白名单功能，实现对请求过滤。

- UserAgent黑名单：黑名单内的UserAgent字段均无法访问当前资源。

  如果您的UserAgent字段被加入黑名单，该带有UserAgent字段的请求仍可访问到CDN节点，但是会被CDN节点拒绝并返回403，CDN日志中仍会记录这些黑名单中的UserAgent字段请求记录。

- UserAgent白名单：只有白名单内的UserAgent字段才能访问当前资源，白名单以外的UserAgent字段均无法访问当前资源。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击访问控制。
5. 在右侧域名管理区域，单击UA黑/白名单。
6. 在UA黑/白名单页签，单击修改配置。
7. 根据界面提示，配置UserAgent的黑名单或白名单。

参数	说明
名单类型	UserAgent名单类型如下： ○ 黑名单 黑名单内的UserAgent字段均无法访问当前资源。 ○ 白名单 只有白名单内的UserAgent字段能访问当前资源，白名单以外的UserAgent字段均无法访问当前资源。 黑名单和白名单互斥，同一时间只支持其中一种方式生效。
规则	配置UserAgent字段时，用竖线（|）分割多个值，支持通配符号（*）。例如：*curl*|*IE*|*chrome*|*firefox*

8. 单击确定。

9.6. CDN的安全防护功能

通过本文您可以了解CDN提供的基本安全防护功能。

如果您需要CDN加速域名具有抗DDoS和CC攻击的功能，则请使用SCDN（安全加速）产品，请参见SCDN。CDN基本防护配置如下：

- Referer防盗链功能

  该功能是根据HTTP请求的Referer字段来对请求来源的域名进行筛选和链接。CDN支持三种防盗链设置：白名单、黑名单以及是否允许空refer。防盗链功能主要通过URL过滤的方法对来源Host的地址进行过滤，您可指定请求来源的域名，其中黑名单和白名单只能有一种生效，通过该功能可以对请求来源进行限制。具体设置方法，请参见配置Referer防盗链。

- IP黑名单

  可以设置相应的IP黑名单针对来源IP进行限制。具体设置方法，请参见IP黑白名单。

- URL鉴权

  该功能是CDN为保护用户安全系数较高的URL的安全功能，需要用户按照指定的签名方式对于特定的URL增加鉴权认证。该功能适合于安全密级较高的文件，不建议一般的文件使用，因为每次签名都需要通过客户端临时生成。相比于正常的访问会增加其访问时间。具体设置方法，请参见URL鉴权。

10.性能优化

10.1. 概述

您可以阅读本文档，设置加速域名的性能优化功能，缩小访问文件的体积，提升加速业务的效率和页面可读性。

扛住双11流量洪峰：凭借全国加速节点、智能弹性调度系统及安全防护能力，完美支持过亿QPS峰值，保证全球数亿买家快速浏览高清图片和视频，流畅下单。

您可以通过性能优化功能，对域名执行如下操作。

功能	说明
页面优化	当您开启页面优化功能时，CDN自动清除HTML页面冗余的注释和重复的空白符，缩小文件体积，提升页面可阅读性。
智能压缩	当您开启智能压缩功能时，CDN自动对静态文件进行Gzip压缩。通过智能Gzip压缩方式，可以有效减小传输文件大小，提升加速业务的效率。
Brotli压缩	当您需要对静态文本文件进行压缩时，可以开启此功能，有效减小传输内容大小，加速分发效果。
过滤参数	当您的URL请求中携带问号（?）和参数时，CDN节点在收到URL请求后，判断是否需要将携带参数的URL返回源站。

10.2. 页面优化

当您开启页面优化功能时，CDN自动清除HTML页面冗余的注释和重复的空白符，缩小文件体积，提升页面可阅读性。本文为您详细介绍开启页面优化功能的方法。

页面优化 性能优化

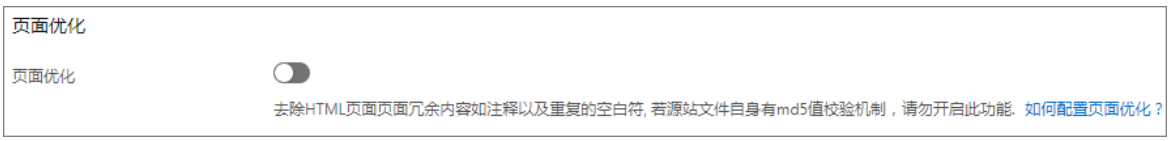
背景信息

开启页面优化功能后，CDN自动删除当前域名下所有HTML页面中冗余的注释和重复的空白符，这样可以有效地去除页面的冗余信息，减小文件体积，提高加速分发效率。

如果源站文件配置了MD5校验机制，则请勿开启该功能。当CDN进行页面优化时，该文件的MD5值会被更改，导致优化后文件的MD5值和源站文件的MD5值不一致。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击性能优化。
5. 在页面优化区域框中，打开页面优化开关。



10.3. 智能压缩

当您开启智能压缩功能时，CDN会自动对静态文件进行Gzip压缩。智能压缩可以有效压缩传输文件的大小，从而提升传输效率。本文为您详细介绍开启智能压缩功能的方法。

加速分发 智能压缩 Gzip 性能优化

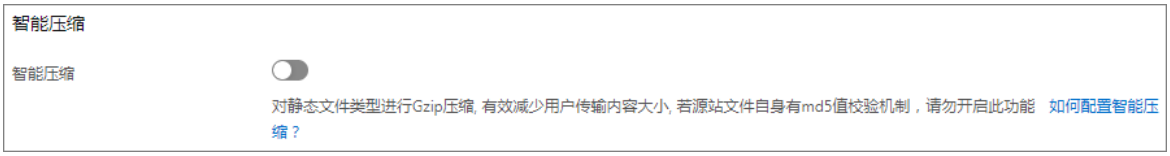
背景信息

- 目前智能压缩支持的内容格式：text/html、text/xml、text/plain、text/css、application/javascript、application/x-javascript、application/rss+xml、text/javascript、image/tiff、image/svg+xml、application/json、application/xmltext。
- 客户端请求携带请求头 `Accept-Encoding: gzip` ：客户端希望获取对应资源的Gzip压缩响应。
- 服务端响应携带响应头 `Content-Encoding: gzip` ：服务端响应的内容为Gzip压缩的资源。

> 注意
>
> - 如果源站文件配置了MD5校验机制，则请勿开启该功能。当CDN对静态文件进行压缩优化时，该文件的MD5值会被更改，导致压缩优化后文件的MD5值和源站文件的MD5值不一致。
> - 只有当源站文件大小超过1024B时，CDN才会进行Gzip压缩。
> - Internet Explorer 6对Gzip的兼容性较差，如果有Internet Explorer 6的访问需求，不建议开启智能压缩功能。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**管理**。
4. 在指定域名的左侧导航栏，单击**性能优化**。
5. 在**智能压缩**区域框中，打开智能压缩开关。



10.4. 过滤参数

如果您的URL请求中携带 `?` 和*参数*，则CDN节点在收到URL请求后，判断是否需要将携带参数的URL请求返回源站。本文为您详细介绍配置过滤参数的方法。

过滤参数 参数过滤 保留参数

背景信息

阿里云CDN的过滤参数功能可分为保留参数和过滤参数，具体说明如下：

- 保留参数

  在大部分URL请求中会包含参数，但是参数内容优先级不高，可以设置忽略参数浏览文件，开启后可以有效提高文件缓存命中率，提升分发效率。

  如果参数有重要含义，例如，包含文件版本信息等，则推荐您设置为保留过滤参数。您最多可以设置10个保留参数，如果请求URL中包含您设置的保留参数，则会携带该参数回源。

  开启过滤参数的作用是忽略URL请求中 `?` 之后的参数，提高CDN缓存的命中率。例如：第一次访问 `http://www.****.com/1.jpg` ，CDN没有缓存，直接回源访问数据；第二次访问 `http://www.****.com/1.jpg?test1` ，由于开启了过滤参数，所以 `?` 后的参数无需匹配，即可命中CDN缓存 `http://www.****.com/1.jpg` 。

- 过滤参数

  每个URL都缓存不同的副本在CDN节点上。

  关闭过滤参数后，访问URL需精确匹配 `?` 之后的参数，提高请求的精确性。例如：第一次访问 `http://www.****.com/1.jpg` ，CDN没有缓存，直接回源访问数据；第二次访问 `http://www.****.com/1.jpg?test1` ，由于关闭了过滤参数，所以 `?` 后的参数需精确匹配，即无法响应CDN缓存内容 `http://www.****.com/1.jpg` ，需要重新回源获取 `http://www.****.com/1.jpg?test1` 。

过滤参数包括 过滤参数和忽略参数这两个功能。

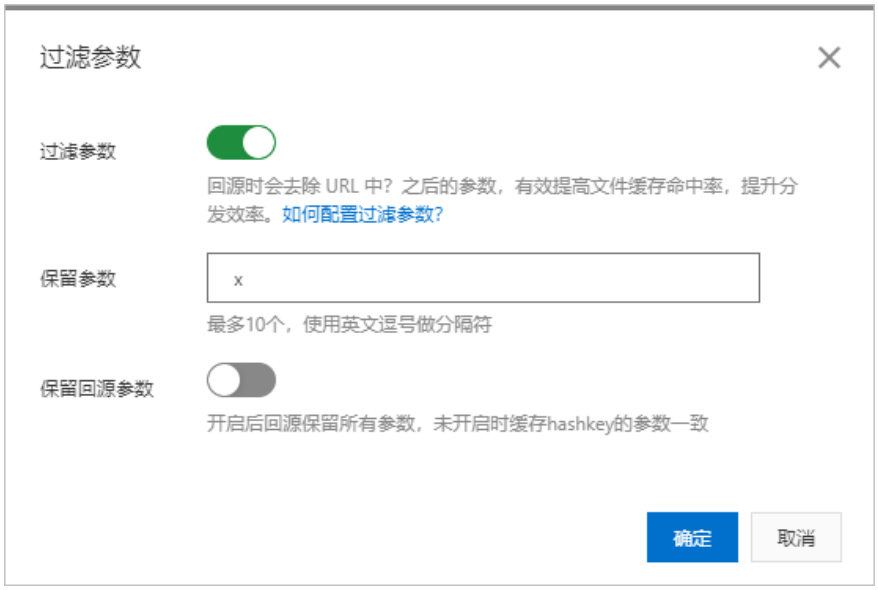
- 保留过滤参数：保留指定参数，多个参数之间用英文逗号隔开，未指定的参数将不会被保留。
- 忽略参数：删除指定参数，多个参数之间用空格隔开，剩余参数将不会被忽略。

> 说明 URL鉴权功能的优先级高于过滤参数。由于鉴权方式A中的鉴权信息包含HTTP请求的参数部分，所以CDN优先进行鉴权判断，鉴权通过后在CDN节点缓存一份副本。配置URL鉴权的操作方法，请参见配置URL鉴权。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**管理**。
4. 在指定域名的左侧导航栏，单击**性能优化**。
5. 配置保留参数和过滤参数。
   - 保留参数
     a. 单击**保留参数**区域的**修改配置**。
     b. 打开**过滤参数**开关。

c. 您可以根据所需配置保留参数。



参数	说明
过滤参数	过滤参数开关。打开过滤参数开关后，资源回源时会去除URL中 ? 之后的参数，提高文件缓存命中率。
保留参数	配置需要保留的参数。最多可以配置10个保留参数，用逗号（,）作分隔符 。例如：http://www.abc.com/a.jpg?x ，保留参数配置为 x 。
保留回源参数	保留回源参数开关。打开保留回源参数开关后，资源回源时，保留所有参数。

示例说明：

CDN节点向源站发起请求 http://www.abc.com/a.jpg?x ，x=1保留。所有类似的请求 http://www.abc.com/a.jpg?x 均响应CDN副本 http://www.abc.com/a.jpg?x 的内容。

d. 单击确定完成配置。

- 过滤参数

a. 单击过滤参数区域的修改配置。

b. 打开过滤参数开关。

c. 您可以根据所需配置忽略参数。

参数	说明
过滤参数	过滤参数开关。打开过滤参数开关后，资源回源时会删除指定参数，剩余参数将不会被删除。
忽略参数	配置需要忽略的参数。最多可以配置10个忽略参数，用空格作分隔符。例如：`http://www.abc.com/a.jpg?x`，忽略参数配置为 `x`。
保留回源参数	保留回源参数开关。打开保留回源参数开关后，资源回源时，保留所有参数。

示例说明：

CDN节点向源站发起请求 `http://www.abc.com/a.jpg?x`，x忽略，`http://www.abc.com/a.jpg?x` 会响应不同参数源站的响应内容。

d. 单击确定完成配置。

10.5. Brotli压缩

当您需要对静态文本文件进行压缩时，可以开启此功能，有效减小传输内容大小，加速分发效果。本文为您详细介绍开启Brotli压缩功能的方法。

Brotli压缩 性能优化

背景信息

Brotli是开源的一种新型压缩算法。开启Brotli压缩功能后，CDN节点返回请求资源时，会对html、js、css等文本文件进行Brotli压缩。压缩文本文件时，Brotli压缩比智能压缩性能提升约15~25%。

- 客户端请求携带请求头 `Accept-Encoding: br` ：客户端希望获取对应资源时进行Brotli压缩。
- 服务端响应携带响应头 `Content-Encoding: br` ：服务端响应的内容是Brotli压缩的资源。

> 注意
>
> - 当Brotli压缩和Gzip压缩同时开启时，且客户端请求头 `Accept-Encoding` 同时带 `br` 和 `gzip` 时，CDN节点将优先选择Brotli压缩。
> - 如果源站已经开启压缩功能，并且响应中携带 `content_encoding` ，则无法开启Brotli压缩功能。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**管理**。
4. 在指定域名的左侧导航栏，单击**性能优化**。
5. 在**Brotli压缩**区域框中，打开**Brotli压缩**开关。

10.6. 自定义图片转换

阿里云CDN为您提供自定义图片转换功能。您可以阅读本文，了解自定义图片转换的功能介绍及操作方法。

功能介绍

您可以根据自定义条件对图片做多种类型转换。

目前，该功能处于内测阶段，请您提交工单申请。

基本配置

CDN支持边缘图片转换，转换的类型以参数形式传入，参数名： `image_process`

支持多个转换参数，以正斜线（/）分隔。

转换方法格式： `image_process=action1,param_value1/action2,param_value2`

示例： `image_process=resize,l_200/quality,q_90/format,webp`

支持如下配置：

- image_transform_enable：是否开启自定义图片转换功能，取值：*on|off*。
- image_transform_filetype：支持转换的图片格式，包括原图和目标图都要在指定的格式里面。取值：*jpg|png|webp*。

图片缩放

操作名称：`resize`

- 按长边固定自适应等比缩放。示例：`image_process=resize,l_200`
- 按短边固定自适应等比缩放。示例：`image_process=resize,s_200`
- 按宽固定自适应等比缩放。示例：`image_process=resize,w_200`
- 按高固定自适应等比缩放。示例：`image_process=resize,h_200`
- 按固定宽高缩放。示例：`image_process=resize,fw_200,fh_200`

任意参数值为负时，不处理返回原图。

图片裁剪

操作名称：`crop`

- 按指定*x*、*y*、*width*及*height*裁剪，以*x*和*y*为起点，裁剪*width* x *height*（宽x高）大小的图片内容。示例：`image_process=crop,x_10,y_10,w_400,h_200`
- 从图片居中部分裁剪指定*width*和*height*的图片内容。示例：`image_process=crop,mid,w_400,h_200`

任意参数值为负时，不处理返回原图。

图片质量调节

操作名称：`quality`

- 按绝对质量进行转换，转换成指定大小的质量，如果当前质量小于待转换的质量，则不转换。示例：`image_process=quality,Q_90`，如果当前质量是*80*，经过转换后质量仍为*80*。
- 按相对质量进行转换，根据当前图片的质量乘以待转换系数，得到最终要转换的图片质量。示例：`image_process=quality,q_90`，如果当前质量是*80*，经过转换后，质量为*72*。

质量值范围：*0* < quality < *100*，并且 quality % 5 == 0。其他值都不支持。

图片锐化

操作名称：`sharpen`

对图片进行锐化，使图片更清晰，只支持*50*、*100*、*150*、*200*、*250*及*300*六个锐化参数。

示例：`image_process=sharpen,100`

图片旋转

操作名称：`rotate`

将图片按顺时针+指定的角度做旋转，只支持*90*、*180*、*270*三个角度。示例：`image_process=rotate,180`

自适应方向

操作名称：`auto-orient`

某些手机拍摄出来的照片可能带有旋转参数。可以设置是否对这些图片进行旋转。示例：`image_process=auto-orient`

图片格式转换

操作名称： `format`

将图片转换为指定的图片格式。示例： `image_process=format,webp`

一键瘦身

当您完成提交工单并开启自定义图片转换功能后，该操作一并开启。可在不改变分辨率和图片格式的前提下，并且不影响肉眼观看，对域名下全部的图片做质量转换。

自适应webp

当您完成提交工单并开启自定义图片转换功能后，该操作一并开启。可通过对请求头Accept的判断，如果支持 `image/webp` ，CDN就把图片转换为webp格式返回： `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9`

11.视频相关

11.1. 概述

您可以通过设置Range回源和拖拽播放功能，减少回源流量消耗，并且提升视音频的播放效果。

您可以通过视频相关功能，对域名执行如下操作。

功能	说明
配置Range回源	开启Range回源功能，可以减少回源流量消耗，并且提升资源响应时间。
拖拽播放	开启拖拽播放功能后，当播放视音频时，随意拖拽播放进度，而不影响视音频的播放效果。

11.2. 配置Range回源

本文为您介绍了在控制台配置Range回源的具体操作和注意事项。您在完成配置Range回源后，可以减少回源流量消耗，并且提升资源响应时间，有利于音视频等较大文件的内容分发。

Range 回源

背景信息

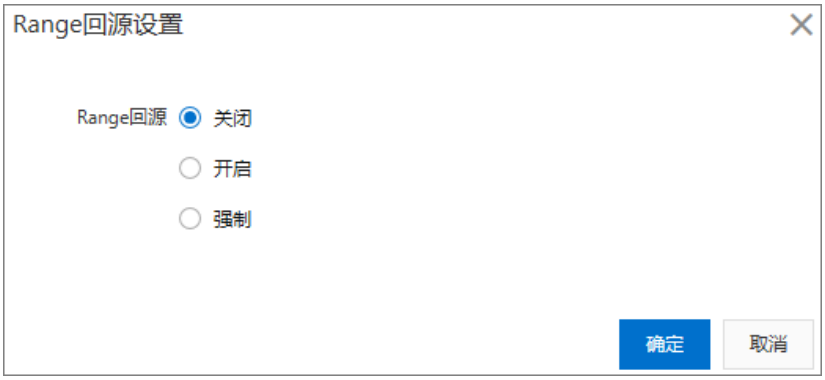
Range回源是指客户端通知源站服务器只返回指定范围内的部分内容。

配置Range回源的注意事项如下：

- 配置Range回源之前，需要源站支持Range请求，即HTTP请求头中包含Range字段，并且源站能够响应正确的206文件分片。
- Range回源是可选配置项，CDN控制台默认不开启。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击视频相关。
5. 在Range回源区域，单击修改。
6. 选择Range回源为开启、关闭或强制。



Range回源设置	具体描述	示例
开启	当您需要访问资源文件指定范围内的部分内容时，为了提高资源响应效率，则需要开启Range回源。开启Range请求回源后，源站需要依据Range，响应文件的字节范围，同时CDN节点也会向客户端响应相应字节范围的内容。	如果客户端向CDN的请求中含有 range:0-100 ，则源站收到的请求中也会含有 range:0-100 。源站响应CDN节点，CDN节点响应客户端字节范围为0~100，共101个字节。
关闭	当您需要访问资源文件的全部内容时，则需要关闭Range回源。关闭Range回源后，CDN上层节点会向源站请求全部的文件，由于客户端收到Range定义的字节后自动断开HTTP连接，请求的文件没有缓存到CDN节点上，最终导致缓存命中率较低，并且回源流量较大。	如果客户端向CDN请求中含有 range:0-100 ，则源站端收到的请求中没有Range这个参数。源站响应CDN节点完整文件，CDN节点响应给客户端的就是101个字节，由于链接断开，会导致该文件没有缓存到CDN节点上。
强制	参数请求强制回源站。	当选择Range回源为强制，请确保源站支持参数Range。 说明 您指定Range回源为强制后，任何分片请求都会强制分片回源。

7. 单击确定完成配置。

11.3. 拖拽播放

当您播放视音频时，需要随意拖拽播放进度，而不影响视音频的播放效果，可以开启拖拽播放。通过本文您可以了解配置拖拽播放功能的操作方法。

拖拽播放 视频拖拽

背景信息

拖拽播放功能是指在视音频点播场景中，如果您拖拽播放进度，则客户端会向服务器端发送URL请求，例如：`http://www.aliyun.com/test.flv?start=10`，服务端会向客户端响应从第10字节的前一个关键帧（如果start=10不是关键帧所在位置）的数据内容。

配置拖拽播放功能之前，需要确认源站支持Range请求。如果HTTP请求头中包含Range字段，则源站需要响应正确的206文件分片。

拖拽播放功能支持的文件和URL格式如下表所示。

文件格式	Meta信息	Start参数	举例
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参数表示时间，CDN会自动定位到start参数所表示时间的前一个关键帧（如果当前start不是关键帧所在位置）。start参数的单位是s，支持以小数表示，例如start=1.01，表示开始时间是1.01s。	URL请求为`http://domain/video.mp4?start=10`表示从第10秒开始播放视频。
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参数所表示字节的前一个关键帧（如果当前start不是关键帧所在位置）。	URL请求为`http://domain/video.flv?start=10`表示从第10字节的前一个关键帧开始播放视频。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**管理**。
4. 在指定域名的左侧导航栏，单击**视频相关**。
5. 在**拖拽播放**区域，打开**拖拽播放**开关。
6. （可选）开启FLV文件按时间拖拽。 打开**FLV按时间拖拽** 开关。开启该功能后，FLV视音频点播将支持按时间随机拖拽播放。
7. （可选）自定义开始和结束时间的参数名。
   i. 单击**自定义参数** 配置项对应的**修改**，配置拖拽播放的**开始参数** 和**结束参数** 。

> **说明**
> - 开始参数默认为start，结束参数默认为end。
> - 自定义参数只能使用大小写字母、数字、以及下划线“_”。例如：123、aabbAABB、aa_BB123。

   ii. 单击**确定**

11.4. 听视频

开启听视频功能后，CDN节点会将视频文件中的音频分离，并返回给客户端，节省流量。通过本文档，您可以了解开启音视频分离的操作方法。

背景信息

当客户端请求访问视频文件时，向服务器端发送URL请求，例如：`http://www.aliyun.com/test.flv?ali_audio_only=1`，CDN服务器端仅向客户端发送音频数据。

客户端必须支持传输方式：`Transfer-Encoding:chunked`。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**管理**。
4. 在指定域名的左侧导航栏，单击**视频相关**。
5. 在**听视频** 区域，打开听视频开关。

   开启听视频功能后，需要配合请求参数 `ali_audio_only` 使用。支持的文件格式如下表所示。

文件格式	meta信息	ali_audio_only参数	举例
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。	`ali_audio_only` 参数表示该请求为音视频请求，服务端只返回meta信息和音频信息，视频信息会被过滤掉。如果不带该参数或参数值非1，则该功能失效。	请求 `http: //domain/video.mp4?ali_audio_only=1` 。
FLV	无要求。	`ali_audio_only` 参数表示该请求为音视频请求，服务端只返回meta信息和音频信息，视频信息会被过滤掉。如果不带该参数或参数值非1，则该功能失效。	请求 `http:// domain/video.flv?ali_audio_only=1` 。

11.5. 音视频试看

阿里云CDN音视频试看功能可以为您提供“非会员试看试听xx秒”的体验，本文为您介绍了音视频试看功能及控制台具体操作。

音视频试看 视频 cdn

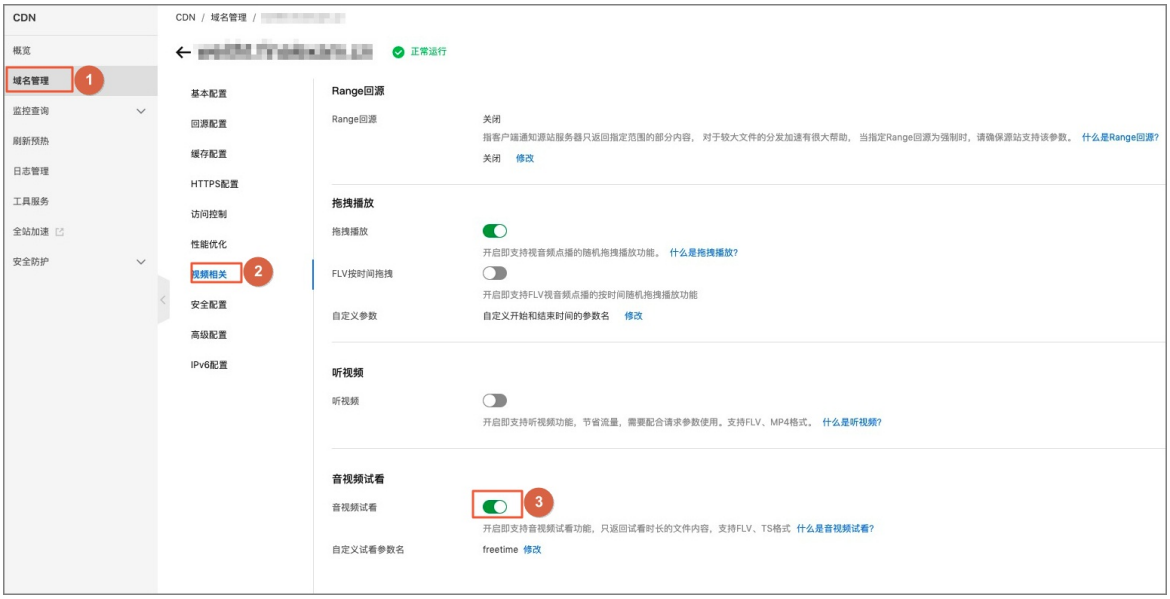
背景信息

音视频试看功能可以使CDN节点只给客户端返回指定时长的音视频文件。

音视频试看支持TS和MP3格式文件。FLV和MP4格式文件试看可以通过拖拽播放的自定义参数 `end` 实现，拖拽播放操作请参见拖拽播放。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击视频相关。
5. 在音视频试看区域，打开音视频试看开关。



6. 单击自定义试看参数名对应的修改。
7. 设置自定义试看参数名。

   客户端返回试看音视频文件的时间，单位为秒。例如：设置自定义试看参数名为free_time，客户端的请求字段为free_time=15，表示CDN节点只需返回15秒的音视频文件内容。

   > 说明 自定义试看参数名的数值不够精确，建议客户端设置的值稍大点，更加稳妥。例如：用户需要试看13秒的音视频，建议在客户端上设置15秒。

8. 单击确定。

11.6. M3U8标准加密改写

本文为您介绍M3U8标准加密改写功能和操作流程。

功能介绍

HLS（HTTP Live Streaming）标准加密改写是改写HLS中M3U8文件的 `#EXT-X-KEY` 标签，改写成功后会在 `#EXT-X-KEY` 标签中的URI末尾追加一个参数，该参数的值由客户端请求携带。

M3U8标准加密改写功能支持开启HLS（M3U8）标准加密改写，开启加密后可自定义追加参数名称，以配合您的客户端使用个性化的加密参数名。如果不设置自定义参数名，则默认的参数名为 `MtsHlsUriToken` 。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击视频相关。
5. 在M3U8标准加密改写区域，打开M3U8标准加密改写开关。

> 说明 开启M3U8标准加密改写功能后，默认的参数名为 `MtsHlsUriToken` 。

6. 如果您需要配合您的客户端修改参数名，请执行以下操作步骤。
   i. 单击自定义参数名对应的修改。
   ii. 在自定义参数名对话框，设置参数名。

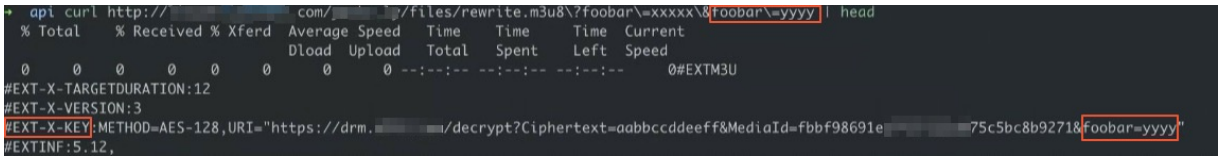
> 说明 参数名大小写敏感，请确保设置的参数名和客户端请求携带的参数名完全一致。例如客户端请求携带 `foobar` 参数，如果在CDN控制台设置自定义参数名为 `FooBar` 将不生效。

   iii. 单击确定，完成配置。

示例展示

在CDN控制台开启**M3U8标准加密改写**，并设置自定义参数名为 `foobar` ，如下图所示。

客户端请求中携带 `foobar` 参数，参数的值为 `yyyy` ，当CDN解密播放时，会将 `foobar=yyyy` 追加到M3U8文件中 `#EXT-X-KEY` 标签的URI末尾。



12.安全配置

12.1. 配置WAF防护

CDN结合WAF能力，将业务流量进行恶意特征识别及防护，将正常、安全的流量回源到服务器。避免网站服务器被恶意入侵，保障业务的核心数据安全，解决因恶意攻击导致的服务器性能异常问题。 通过本文档，您可以了解WAF防护功能、使用场景、费用说明和设置方法。

前提条件

- 您已在CDN控制台开通WAF功能（开通方式：选择**安全防护 > WAF**，单击**开通**。）。
- 目前CDN仅支持中国内地加速节点的WAF防护，开启前请您确认域名的加速区域。修改域名加速区域的操作方法，请参见修改基础信息。

背景信息

阿里云CDN的WAF功能，是指CDN融合了云盾Web应用防火墙（Web Application Firewall，简称 WAF）能力，在CDN节点上，提供WAF防护功能。WAF防护具体功能，请参见版本功能说明。

CDN的WAF服务主要适用于金融、电商、O2O、互联网+、游戏、政府、保险等行业，保护您的网站在使用CDN加速的同时，免受因外部恶意攻击而导致的意外损失。

使用CDN WAF功能后，可以帮助您解决以下问题：

- 防数据泄密，避免因黑客的注入入侵攻击，导致网站核心数据被拖库泄露。
- 阻止木马上传网页篡改，保障网站的公信力。
- 提供虚拟补丁，针对网站被曝光的最新漏洞，最大可能地提供快速修复规则。

当您开启WAF功能后，CDN WAF会对此域名的所有请求进行检测，并按照账户维度，对域名开启WAF功能的请求次数汇总，然后收费。CDN WAF计费价格，请参见增值服务计费-CDN WAF计费。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**管理**。
4. 在指定域名的左侧导航栏，单击**安全配置**。
5. 在**WAF**页面，打开**WAF功能配置**开关。
6. 单击**修改配置**。

7. 根据页面提示，配置Web应用攻击防护和精准访问控制。

项目	参数	说明
Web应用攻击防护状态	状态	Web应用攻击防护开关。
	模式	Web应用攻击防护模式如下： ○ **防护** 发现攻击后直接阻断。 ○ **预警** 发现攻击后只告警不阻断。
	防护规则策略	Web应用攻击防护规则如下： ○ **宽松规则** 当您发现在**中等规则**下存在较多误拦截时，建议您选择**宽松规则**。宽松模式下对业务的误报程度最低，但也容易漏过攻击。 ○ **中等规则** 默认使用中等规则。 ○ **严格规则** 当您需要更严格地防护路径穿越、SQL注入、命令执行时，建议您选择**严格规则**。 在发现防护规则有对正常业务有阻拦时，可调整防护策略的模式。宽松模式下对业务的误报程度最低，但也容易漏过攻击。
精准访问控制	状态	精准访问控制开关。
	规则	CDN提供一条默认规则。您可以根据所需，单击**前去配置**，添加新规则，并编辑默认规则。当前每一条规则中最多允许三个条件组合，并且条件之间是“与”的逻辑关系，即必须三个条件同时满足才能与规则匹配。

角色授权

当您需要CDN边缘Web应用防火墙自动角色授权时，可以使用CDN WAF功能，CDN将自动为您创建AliyunServiceRoleForCDNAccessingWAF角色，并授权CDN使用该角色，并授权CDN访问WAF产品中的资源。

AliyunServiceRoleForCDNAccessingWAF角色中包含的权限包括如下接口：

- DescribePayInfo
- CreatePostpaidInstance
- CreateOutputDomainConfig
- DeleteOutputDomainConfig
- DescribeDomainWebAttackTypePv
- ModifyLogServiceStatus
- DescribeProtectionModuleMode
- DescribeDomainRuleGroup
- DescribeRegions
- ModifyProtectionRuleStatus
- ModifyProtectionRuleCacheStatus
- DescribePeakValueStatisticsInfo
- DescribeDomainAccessStatus
- DescribeFlowStatisticsInfo
- DescribeDomainTotalCount
- DescribeResponseCodeStatisticsInfo
- DescribeDDosCreditThreshold
- ModifyDomainClusterType
- DescribeInstanceInfo
- DescribeOutputDomains
- CreateOutputDomain
- DeleteOutputDomain
- DeleteInstance
- DescribeInstanceSpecInfo
- DescribeDomainBasicConfigs

如果您希望删除该AliyunCDNAccessingWAFRole角色，您需要提交工单删除CDN WAF实例，关闭所有域名的CDN WAF功能，然后才能在RAM中删除该SLR。

12.2. 配置频次控制

当您的网站遭受恶意CC攻击响应缓慢时，通过频次控制功能，可以秒级阻断访问该网站的请求，提升网站的安全性。通过本文档您可以了解访问频次的配置方法。

安全 频次控制

背景信息

目前CDN频次控制功能需要您申请开通，如需开通请加入钉钉群：23184221。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击安全配置。
5. 在频次控制页面，打开频次控制设置开关。
6. 单击修改配置。
7. 在频次控制对话框，打开参数检测开关，并选择控制模式。

参数	说明
参数检测	当您开启参数检测开关时，频次控制规则中的URI会带上完整的参数进行匹配。参数检测仅与URI匹配相关，与自定义规则中的匹配规则无关。
控制模式	您可以选择以下控制模式： ○ 正常 默认频次控制模式。当您的网站流量无明显异常时，采用该模式，避免误杀。 ○ 紧急 当您的网站响应缓慢，且流量、CPU、内存等指标异常时，采用该模式。 ○ 自定义 当您需要根据所需自定义频次控制规则时，采用该模式。自定义模式不提供任何后台规则策略，按照用户自定义规则进行匹配。配置自定义规则的操作方法，请参见步骤8。

8. 当您控制模式选择为自定义时，需要配置自定义规则。
   i. 单击自定义规则对应的添加规则。

   > 说明 CDN控制台上最多支持添加5条自定义规则。

   ii. 根据界面提示和如下表格配置自定义规则。

参数	说明
规则名称	规则名称长度为4~30个字符，支持英文、数字，同一域名中规则名称不可重复。

参数	说明
URI	指定需要防护的具体地址，例如：`/register`。支持在地址中包含的参数，同时需要打开参数检测开关才可生效，例如：`/user?action=login`。
匹配方式	您可以选择以下匹配规则： 默认按照完全匹配、前缀匹配、模糊匹配的顺序排序并执行。您可在同类规则中进行优先级调整，优先级按列表顺序排序，执行规则时按照优先级进行执行。 ■ **完全匹配** 即精确匹配，请求地址必须与配置的URI完全一样才会被统计。 ■ **前缀匹配** 即包含匹配，只要是请求的URI以此处配置的URI开头就会被统计。例如，如果设置URI为`/register`，则`/register.html`会被统计。 ■ **模糊匹配** 即根据表达式匹配，当请求的URI与此处的表达式匹配就会被统计。模糊匹配仅支持英文句号（.）和星号（*）匹配，英文句号（.）表示匹配任何单个字符，星号（*）表示匹配任意重复字符。
检测时长	指定统计访问次数的周期。需要和检测对象配合。检测时长大于等于10秒，小于等于600秒。
检测及阻断对象	频次控制支持的检测对象如下： ■ **源IP** ■ **请求Header中指定字段** ■ **访问域名** ■ **请求URL中指定参数**
匹配规则	您可以单击**添加规则**，配置规则的**类型**、**参数**、**逻辑符**和**值**。
阻断类型	指定触发条件后的操作（封禁、人机识别），以及请求被阻断后阻断动作的时长。 ■ **封禁** 触发条件后，直接返回403。 ■ **人机识别** 触发条件后，用重定向的方式去访问客户端（返回200状态码），通过验证后才放行。例如，单个IP在20秒内访问超过5次则进行人机识别判断，在10分钟内该IP的访问请求都需要通过人机识别，如果被识别为非法将会被拦截，只有被识别为合法才会放行。
阻断时长	阻断时间大于等于60秒。

自定义规则场景样例，如下表所示。

场景	检测对象	检测时长	匹配规则	阻断类型	阻断时长

场景	检测对象	检测时长	匹配规则	阻断类型	阻断时长
4xx/5xx异常	IP	10秒	"status_ratio|404">60% && "count">50	封禁	10分钟
QPS异常	域名	10秒	"count">*N*	人机识别	10分钟
单一URL被集中访问	IP	1分钟	"uri_num"<2 && "count">*N*	封禁	10分钟
通过随机User-Agent访问	IP	10秒	"header_num|user-agent">10	封禁	10分钟

> 说明 *N*表示可以取任意值，您可以根据业务所需设置。

iii. 单击**确定**。

12.3. 配置CDN联动DDoS高防

阿里云CDN推出联动DDoS高防功能，帮助您的加速域名更好地防御DDoS攻击。本文为您介绍在控制台配置CDN联动DDoS高防功能的具体操作。

前提条件

在进行配置DDoS高防前，您需要购买DDoS高防实例，详情请参见DDoS高防控制台。

背景信息

如果您的业务使用CDN加速，并且需要防御DDoS攻击。当攻击发生时，需要从CDN切换至DDoS高防，您可以使用该功能进行自动化调度。当DDoS攻击结束后，可以自动将流量切换回CDN进行正常业务分发。

CDN联动功能正在邀测中，主要针对金融、零售、交通、传媒及政府等企业级用户开放，您可以加入钉钉群（32615821）进行咨询和开通该功能。

使用场景包括但不限于以下：

- 金融行业

  保障业务分发高可用，提升跨国访问体验，同时关注信息、交易、数据资产的安全防护，避免网络攻击给企业造成重大风险。

- 零售行业

  保障企业官网，电商平台，订票平台，内部办公协同软件的网络分发质量，同时防护网络安全攻击，保证业务的持续可用性。

- 传媒行业

  保障公共媒体内容高效传播，同时通过网络安全防护保障，避免业务突增和网络攻击对业务稳定性的影响。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 选择安全配置 > CDN联动DDoS。

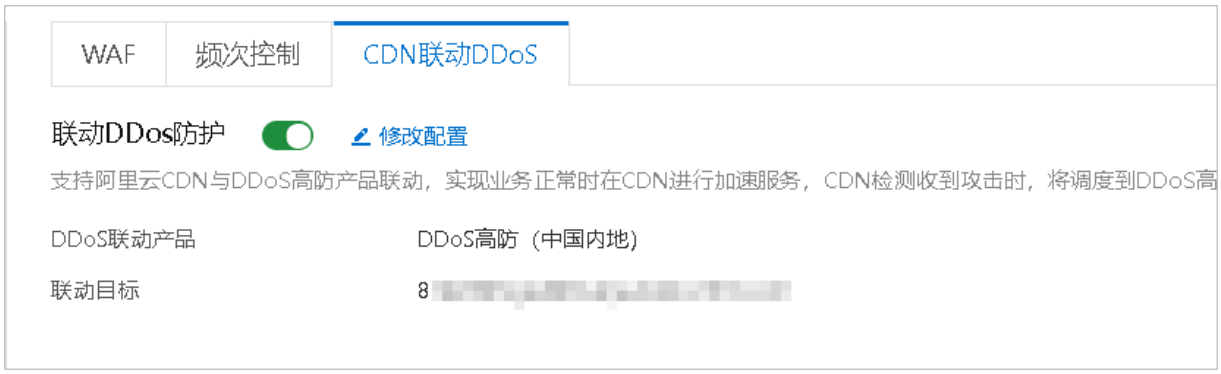
   如果还未开通该功能，请单击申请开通跳转到钉钉群进行咨询和开通。
5. 打开联动DDoS防护开关。
6. 配置DDoS联动产品、联动目标类型及联动目标。

> **说明** 当前域名没有查询到DDoS高防配置。
>
> - 未购买DDoS高防：您需要前往DDoS高防控制台购买高防实例。
> - 已购买DDoS高防：您需要在DDoS高防控制台进行域名配置。

7. 单击确定完成配置。

执行结果

返回CDN联动DDoS功能页面，可查看是否配置成功。



您使用联动DDoS功能，CDN将自动为您创建AliyunServiceRoleForCDNAccessingDDoS角色，并授权CDN使用该角色授权CDN访问DDoS高防产品中的资源。AliyunServiceRoleForCDNAccessingDDoS角色中包含的权限包括如下接口：

- DescribeDomainAttackEvents：查询针对网站业务的攻击事件。
- DescribeDomainDDoSAttackEvents：查询DDoS的攻击事件。
- DescribeDDoSEvents：查询针对DDoS高防实例的攻击事件。
- DescribeWebRules：查询网站业务转发规则。
- DescribeDomainQPSList：查询网站业务的QPS统计信息。
- DescribeCdnLinkageRules：查询联动配置。

如果您希望删除该AliyunCDNAccessingDDoSRole角色，您需要关闭所有域名的DDoS联动功能，然后才能在RAM中删除该SLR。详情请参见SLR详细介绍。

12.4. 区域封禁

阿里云CDN推出区域封禁功能，帮助您一键阻断来自指定区域的访问请求，解决部分地区高发的恶意请求问题。

背景信息

目前CDN区域封禁功能需要您申请开通，如需开通请加入钉钉群：31327650。

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击安全配置。
5. 在区域封禁页面，单击修改配置
6. 在封禁设置对话框，选择封禁类型 和区域设置。

参数	说明
封禁类型	○ 黑名单 黑名单内的区域均无法访问当前资源。 ○ 白名单 只有白名单内的区域能访问当前资源，白名单以外的区域均无法访问当前资源。 黑名单和白名单互斥，同一时间只支持其中一种方式生效。
区域设置	设置黑白名单的区域。

7. 单击确定
8. 当您需要删除该配置时，单击删除配置。

13.高级配置

13.1. 概述

您可以通过配置带宽封顶功能，保证数据传输和加速域名安全。

您可以通过高级配置功能，对域名执行如下操作。

功能	说明
配置带宽封顶	如果您设置的带宽达到阈值，则系统为了保护您的域名安全，自动下线，所有的请求会回到源站，CDN停止加速服务。

13.2. 配置带宽封顶

带宽封顶功能是指当统计周期（5分钟）产生的平均带宽超出您设置的带宽最大值时，为了保护您的域名安全，此时域名会自动下线，所有的请求会回到源站，CDN将停止加速服务，避免异常流量给您带来的异常消费。域名下线后，您可以在控制台重新启用该域名。通过本文，您可以快速了解开通带宽封顶功能的方法和注意事项。

阿里云cdn带宽带宽封顶

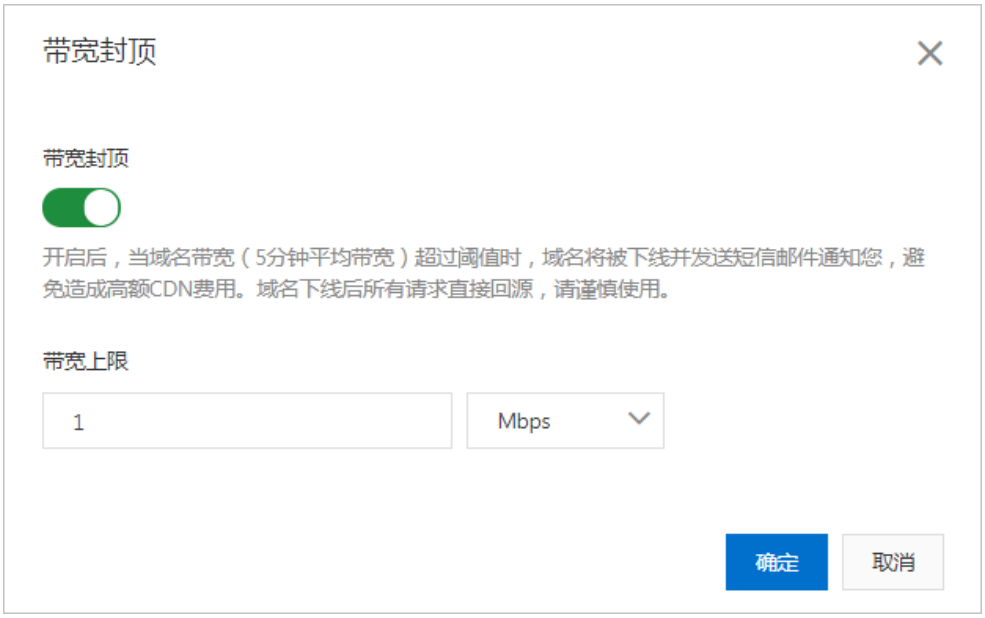
背景信息

配置带宽封顶功能的注意事项如下：

- 如果RAM子账号需要开通带宽封顶功能，则您需要登录RAM控制台，新增管理CDN的权限AliyunCDNFullAccess。
- 泛域名暂不支持带宽封顶功能，设置后不会生效。
- 开启带宽封顶功能后，您的业务会受到带宽封顶的限制而下线，为了不影响您的域名业务，建议您合理评估，谨慎设置您的带宽峰值。
- 如果您的CDN加速服务因带宽封顶而下线，则可以在CDN控制台的**域名管理**页面，选中该域名对应的复选框，单击**启用**，重新启用该域名。
- 域名每次下线后，1小时内将不会再被触发下线。
- 由于带宽的数据监控存在一定延迟，因此域名将在带宽到达阈值后0~15分钟左右被执行下线。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 在指定域名的左侧导航栏，单击高级配置。
5. 在带宽封顶区域框，单击修改配置。



6. 打开带宽封顶开关，配置带宽上限值。

> **说明**
> - 各个单位之间进制为1000。例如：1Tbps=1000Gbps，1Gbps=1000Mbps。
> - 您可以根据域名的实际使用情况，选择开启或者关闭带宽封顶功能。

7. 单击确定。

14.IPv6配置

本文为您介绍了阿里云CDN IPv6功能在控制台的操作步骤，通过开启IPv6开关，IPv6的客户端请求将支持以IPv6协议访问CDN，CDN也将携带IPv6的客户端IP信息访问您的源站。

背景信息

阿里云CDN大部分节点已经支持接收IPv6协议的请求，您可以在域名配置中开启IPv6开关。

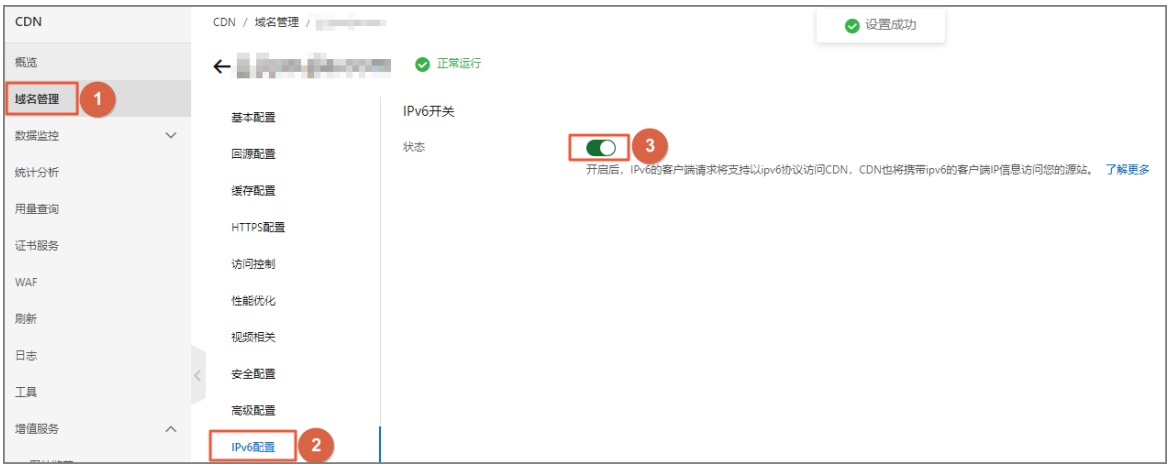
开启开关后，当您的用户处于IPv6环境，且就近的CDN节点也支持IPv6的请求时，客户端可以通过IPv6协议访问CDN节点。当用户就近区域的CDN节点不支持IPv6协议时，客户端仍可以IPv4协议访问CDN节点。

> 说明 目前海外、中国香港、中国澳门和中国台湾节点不支持IPv6配置。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的管理。
4. 单击IPv6配置。
5. 打开IPv6开关。

   IPv6功能开启，您可以在客户端通过IPv6协议访问CDN节点，阿里云CDN节点也将携带IPv6协议信息访问您的源站。



15.域名管理FAQ

本文汇总了使用阿里云CDN时，域名相关问题及处理方法。

- 域名相关概念
  - 什么是静态内容和动态内容？
  - 什么是域名解析？
- 域名相关问题
  - CDN支持泛域名加速吗？
  - CDN回源地址有哪些？
  - 如何处理源站的302跳转？
  - 如何处理未备案域名？
  - CDN节点与镜像站点的区别是什么？
  - 阿里云CDN的健康检查机制是什么？
  - 切换加速区域后的影响是什么？
  - CDN支持的调用方式有哪些？
  - 如何测试CNAME解析是否正常？
  - 出现自定义404页面的原因是什么？