阿里云
CDN

用户指南

文档版本：20190612

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
	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。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能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，恢复业务所需时间约10分钟。
	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。	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。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	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。	`swich` *`{stand | slave}`*

目录

法律声明.....I
通用约定.....I
1 控制台说明..... 1
2 CDN功能列表.....2
3 业务类型..... 7
3.1 类型1：图片小文件加速.....7
3.2 类型2：大文件下载加速.....8
3.3 类型3：视音频点播加速.....8
3.4 类型4：直播流媒体加速.....9
3.5 类型5：全站加速..... 10
3.6 类型6：移动加速..... 10
4 域名管理.....11
4.1 批量复制域名配置..... 11
4.2 标签管理..... 13
4.2.1 概述.....13
4.2.2 绑定标签.....14
4.2.3 解绑标签.....14
4.2.4 使用标签管理域名.....15
4.2.5 案例介绍.....16
4.2.6 使用标签筛选数据.....17
4.3 设置报警..... 18
4.4 基本配置..... 19
4.4.1 基本配置概述.....19
4.4.2 切换加速区域.....20
4.4.3 配置源站.....21
4.5 内容回源设置..... 22
4.5.1 设置回源HOST..... 22
4.5.2 设置协议跟随回源.....23
4.5.3 私有bucket回源授权..... 24
4.5.4 关闭私有Bucket回源..... 28
4.5.5 设置回源SNI..... 29
4.6 节点缓存设置..... 31
4.6.1 设置缓存过期时间.....32
4.6.2 设置状态码过期时间.....34
4.6.3 设置HTTP响应头..... 36
4.6.4 设置自定义页面.....37
4.6.5 重写.....38
4.7 HTTPS安全加速..... 40
4.7.1 概述.....40

4.7.2 配置HTTPS证书 43
4.7.3 证书格式说明 46
4.7.4 设置HTTP/2 49
4.7.5 设置强制跳转 51
4.7.6 设置TLS 53
4.7.7 设置HSTS 55
4.7.8 常见问题 58
4.8 访问控制设置 60
4.8.1 配置防盗链 60
4.8.2 配置URL鉴权 61
4.8.3 鉴权方式A 62
4.8.4 鉴权方式B 64
4.8.5 鉴权方式C 65
4.8.6 鉴权代码示例 67
4.8.7 配置IP黑/白名单 69
4.8.8 UsageAgent黑/白名单 70
4.9 性能优化设置 70
4.9.1 页面优化 71
4.9.2 智能压缩 71
4.9.3 Brotli压缩 72
4.9.4 过滤参数 73
4.10 高级设置 75
4.10.1 带宽封顶 75
4.11 视频相关配置 76
4.11.1 Range回源 77
4.11.2 拖拽播放 78
5 数据监控 80
6 统计分析 82
7 用量查询 83
7.1 用量查询 83
7.2 账单导出 84
7.3 明细导出 85
8 CDN WAF防护功能 87
9 刷新预热 89
9.1 概述 89
9.2 配置刷新预热 90
10 日志管理 92
10.1 日志下载 92
10.2 日志转存 93
10.3 实时日志推送 96
10.3.1 概述 96
10.3.2 配置实时日志推送 97
11 诊断工具 99

12 增值服务..... 100
12.1 图片鉴黄..... 100
13 CDN子账户使用指南..... 104
14 设置httpDNS..... 109

1 控制台说明

本文主要介绍阿里云CDN控制台界面上展示的相关功能。阿里云CDN控制台不仅可以帮助您完成配置域名等基本操作，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。

控制台指引

控制台的界面展示如下：

- 左侧导航栏：控制台左侧为域名管理操作菜单栏，详细功能介绍请参见*CDN功能列表*。
- 概览区：控制台中部为概览区，包括三个部分：您的昨日使用数据、CDN使用指南和其他加速产品。
  - 昨日使用数据：根据您的计费方式，系统会在这里展示您计费项中的使用数据。
  - CDN使用指南：您可以在这里查阅CDN相关的使用指南。如果您想了解更多，可以参考*CDN学习路径*。
  - 其他加速产品：您可以了解CDN的其他产品。如果您对安全有更高的需求，可以选择*安全加速SCDN*；如果您对动态加速有重点需求，可以选择*阿里云全站加速*。
- 右侧计费展示区：包括您的计费方式、资源包数量、域名数量和域名流量排名。

2 CDN功能列表

本文为您介绍了CDN的相关功能，具体功能信息请参见相关文档。

HTTPS安全加速

项目	说明	默认值
HTTPS安全加速	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。	未开启
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，将您的原请求方式进行强制跳转。	未开启
HTTP/2设置	开启HTTP/2，您可以享受二进制协议带来的更多扩展性、内容安全性、多路复用、头部压缩等优势。	未开启
TLS	TLS协议版本开启后，您的加速域名也将开启TLS握手。	目前TLSv1.0、TLSv1.1和TLSv1.2版本默认开启。
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。	未开启

回源设置

项目	说明	默认值
回源HOST	指定回源HOST域名，提供三种选项：加速域名、源站域名、自定义域名。	加速域名
协议跟随回源	开启该功能后，回源使用协议和客户端访问资源的协议保持一致。	未开启

项目	说明	默认值
私有Bucket回源	若加速域名想要回源至您账号下标记为私有的bucket时，需要首先进行授权，授权成功并开启授权配置后，您开启了私有bucket授权的域名有权限访问私有bucket。	未开启

缓存设置

项目	说明	默认值
缓存过期时间	自定义指定资源内容的缓存过期时间规则	未开启
设置HTTP头	可设置http请求头，目前提供10个http请求头参数可供自行定义取值。	未开启
自定义404页面	提供三种选项：默认404、公益404、自定义404。	默认404

访问控制

项目	说明	默认值
Refer防盗链	您可以通过配置访问的referer黑白名单来对访问者身份进行识别和过滤	未开启
鉴权配置	URL鉴权方式保护您源站资源	未开启
IP黑名单	您可以通过配置访问的 IP黑名单来对访问者身份进行识别和过滤	未开启

性能优化

项目	说明	默认值
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
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

项目	说明	默认值
过滤参数	勾选后，回源会去除url中？之后的参数。	未开启

视频相关设置

项目	说明	默认值
Range回源	指客户端通知源站服务器只返回指定范围的部分内容，对于较大文件的分发加速有很大帮助。	未开启
拖拽播放	开启即支持视音频点播的随机拖拽播放功能	未开启

高级配置

项目	说明	默认值
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。	未开启

刷新与预热

项目	说明	默认值
URL刷新和预热	· 通过提供文件URL的方式，强制CDN节点回源拉取最新的文件。 · 将指定的内容主动预热到CDN的L2节点上，您首次访问即可直接命中缓存，降低源站压力。	开启

数据监控与统计分析

项目	说明	默认值
数据监控	您可以选择想监控的域名、区域、运营商、时间粒度（1分钟、5分钟、1小时）以及想查询的时间段（今天、昨天、近7天、近30天或自定义）。	开启
统计分析	统计分析包含五个部分：PV和UV、地区和运营商、域名排名、热门Refer、热门URL。您可以导出原始详细数据，如网络带宽、流量，域名按流量占比排名以及访客区域、运营商分布等。	开启

用量查询

项目	说明	默认值
用量查询	查询并获取到某一段时间内的实际用量数据（流量、带宽或请求数），您可以使用用量查询功能。	开启
账单导出	导出按日计费，或者是按月计费的实际用量数据，以便于与费用中心的出账用量进行比对。	开启
明细导出	导出流量带宽及请求数的5分钟明细数据，便于您通过明细来核对或计算实际消费的计量数。	开启

日志管理

项目	说明	默认值
日志下载	您可以下载最近一个月的日志数据。	开启
实时日志	在借助CDN加速访问资源的过程中，CDN会产生大量的日志数据，这些日志数据CDN会进行实时的采集。	开启

项目	说明	默认值
日志转存	帮助您将日志存储更长的时间，目前CDN的离线日志服务，默认提供1个月的存储时间。如果您有更长时间的存储需求，可以将日志转存至OSS，方便您根据实际情况对日志进行保存和分析。	开启

其他设置

项目	说明	默认值
设置*httpDNS*	httpDNS是域名解析服务，通过HTTP协议直接访问阿里云CDN的服务器。	未开启

3 业务类型

3.1 类型1：图片小文件加速

网站或者应用的静态内容分发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/企业官网站点、娱乐游戏类站点或应用等。例如：各种类型的图像文件、html文件、flash动画、css和javascript文件等。

操作步骤

1. 添加加速域名。

   参见快速入门，注意选择业务类型为：图片小文件加速。

2. 域名配置。

   域名添加完成后，需要根据您的业务选择合适的功能对加速域名进行配置，当前所有域名配置为可选，鉴于图片小文件加速，推荐设置以下功能：

   - HTTPS安全加速，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，了解证书格式说明。
   - 缓存配置，可针对不同目录路径和文件名后缀的资源进行缓存服务器行为的设置，用户可自定义指定资源内容的缓存过期时间规则。
   - 访问控制相关设置，可以保证分发内容安全，防止盗链或者恶意请求造成不必要流量损失。
     - Refer防盗链
     - IP黑名单
   - 性能优化相关设置，智能压缩分发内容、忽略URL参数提升缓存命中率。
     - 页面优化
     - 智能压缩
     - 过滤参数
   - 更多功能参见CDN功能列表。

3.2 类型2：大文件下载加速

网站或者应用的静态大文件分发适用于下载类站点和音视频的应用。例如：游戏安装包`.apk`文件、应用更新文件`.rar`、补丁程序文件和音视频文件等相对较大的文件。

操作步骤

1. 添加加速域名。

   请参考快速入门，注意选择业务类型为：大文件下载加速。

2. 域名配置。

   域名添加完成后，需要根据您的业务选择合适的功能对加速域名进行配置，当前所有域名配置为可选，鉴于大文件下载加速，推荐设置如下功能：

   - HTTPS安全加速，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，了解证书格式说明。
   - 缓存配置，可针对不同目录路径和文件名后缀的资源进行缓存服务器行为的设置，用户可自定义指定资源内容的缓存过期时间规则。
   - 访问控制相关设置，可以保证分发内容安全，防止盗链或者恶意请求造成不必要流量损失。
     - Refer防盗链
     - IP黑名单
   - Range回源，开启该功能，可以减少回源流量消耗，并且提升资源响应时间。
   - URL预热，将源站的内容主动预热到L2 Cache节点上，用户首次访问可直接命中缓存，缓解源站压力。
   - 更多功能参见域名配置概览。

3.3 类型3：视音频点播加速

各类视音频站点，包括：影视类视频网站、在线教育类视频网站、新闻类视频站点、短视频社交类网站和音频类相关站点及应用。

操作步骤

1. 添加加速域名。

   请参考快速入门，注意选择业务类型为：视音频点播加速。

2. 域名配置。

域名添加完成后，需要根据您的业务选择合适的功能对加速域名进行配置，当前所有域名配置为可选，鉴于视音频点播加速，推荐设置如下功能。

- HTTPS安全加速，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，了解 证书格式说明。
- 缓存配置，可针对不同目录路径和文件名后缀的资源进行缓存服务器行为的设置，用户可自定义指定资源内容的缓存过期时间规则。
- 访问控制相关设置，可以保证分发内容安全，防止盗链或者恶意请求造成不必要流量损失。
  - 鉴权设置，URL鉴权功能是通过阿里云CDN加速节点与客户资源站点配合实现的一种更为安全可靠的源站资源防盗方法，能有效保护用户源站资源。
  - Refer防盗链
  - IP黑名单
- Range回源，开启该功能，可以减少回源流量消耗，并且提升资源响应时间。
- 拖拽播放，开启即支持视音频点播的随机拖拽播放功能
- URL预热，将源站的内容主动预热到L2 Cache节点上，用户首次访问可直接命中缓存，缓解源站压力。
- 更多功能参见域名配置概览。

3.4 类型4：直播流媒体加速

直播流媒体加速为各类视频直播平台提供高性能稳定直播技术支持，例如：交互性在线教育网站、游戏竞技类直播站点、个人秀场直播、事件类和垂直行业的直播平台等。当前支持RTMP、HLS和FLV三种格式直播内容加速。

应用场景介绍

目前，直播业务已经独立，请参考视频直播。

3.5 类型5：全站加速

全站加速是阿里云自主研发的融合了动态加速和静态加速技术的CDN产品，目前已经独立成为新产品，请您参考阿里云全站加速。

功能简介

全站加速一站式解决了页面动静态资源混杂、跨运营商、网络不稳定、单线源站、突发流量、网络拥塞等诸多因素导致的响应慢、丢包、服务不稳定的问题，提升全站性能和用户体验。全站加速的应用场景包括：

- 场景1：丰富和复杂的动态内容降低了页面加载速度，影响用户体验。
- 场景2：单线源站、突发流量、网络拥塞等导致页面延迟和内容交付失败。
- 场景3：游戏类客户，动态内容实时通信高并发，传统通信协议无法满足性能需求。
- 场景4：源站负载分配不均，突发访问造成的源站压力。
- 场景5：国内运营商环境复杂，网站被劫持，站点内容遭篡改，仅使用HTTP协议传输可能会有动态内容泄露风险，需要寻求更安全高效的网络链路和内容分发途径。

针对以上各种场景，阿里云CDN全站加速提供：

- 动静分离加速，动态内容采用智能路由、传输协议优化和链路复用技术，静态内容采用边缘缓存，提升整站资源加载速度。
- 实时探测及平滑跨网技术稳定高效处理高流量负载，提供全天候全网可用性。
- 回源负载均衡、多源主备、连接复用和有序回源技术降低源站压力和故障风险。
- 全链路HTTPS安全加速、防盗链、IP限流等保证源站安全。
- 自定义设置动静规则、缓存规则并配备全景信息监控和告警功能。

说明：

全站加速默认纯动态加速，即所有动静态请求都通过最优路由回源获取资源，可通过配置指定静态文件类型或路径，实现智能区分动静态资源，静态资源缓存在边缘节点上，动态资源使用动态加速，达到最快的加速效果。

3.6 类型6：移动加速

4 域名管理

4.1 批量复制域名配置

通过批量复制域名配置功能，您可以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。

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：

- 复制的内容会覆盖目标域名已经配置的内容，请您谨慎操作，以免造成服务不可用。
- 域名复制后，复制不可回退。请确认被复制的域名正在服务或已有配置，且流量带宽较大。请务必确认您的域名复制选择无误，谨慎复制。

操作步骤

1. 登录CDN控制台。
2. 在域名管理页，选择您想要复制配置的域名，单击复制配置。

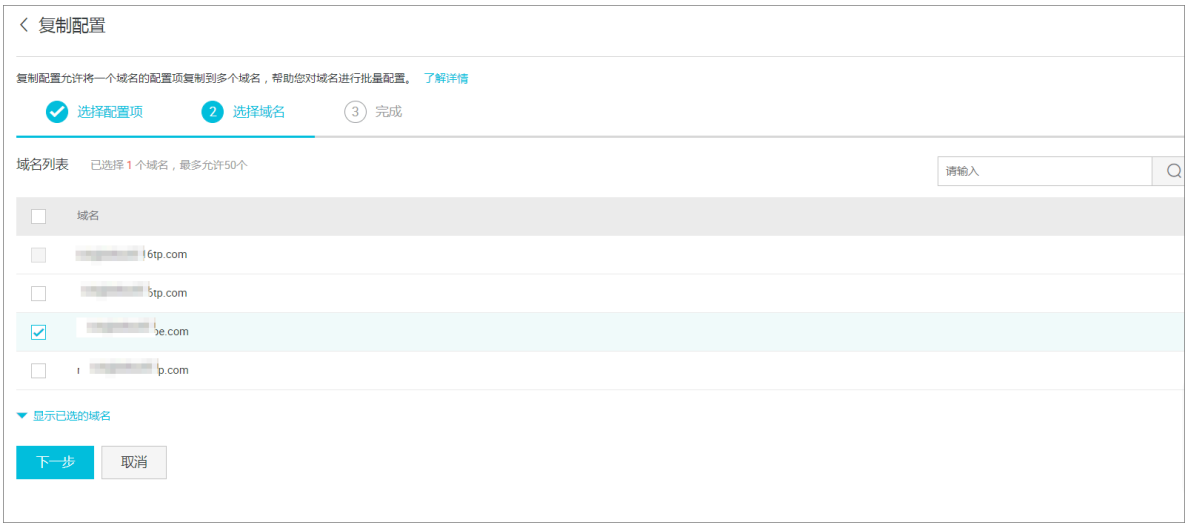
3. 勾选您想要复制的配置项，单击下一步。

> 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，假设您的A域名有2条回源头配置，您从B域名复制了5条内容，则你会有7条回源头配置内容。
> - HTTP头为非增量复制。假设您的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。

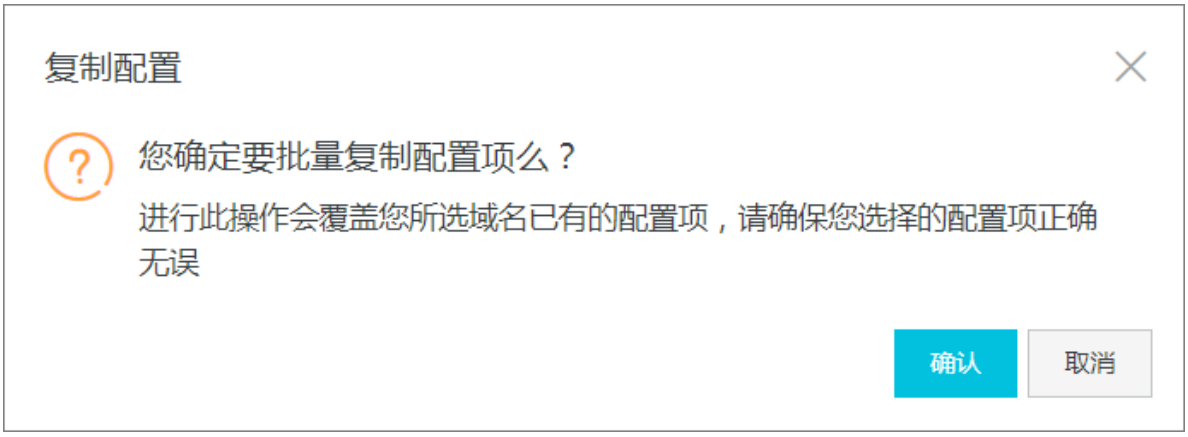
- 开关类的配置复制，将会覆盖域名原有的配置。
- Refer黑白名单或IP黑白名单将会覆盖域名原有配置。

4. 勾选您想要批量配置的目标域名，单击下一步。

   您也可以输入关键词查找域名。



5. 在复制配置对话框中，单击确认，批量复制成功。



4.2 标签管理

4.2.1 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。

使用限制

- 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。

相关功能

您可以使用标签，对域名进行以下操作：

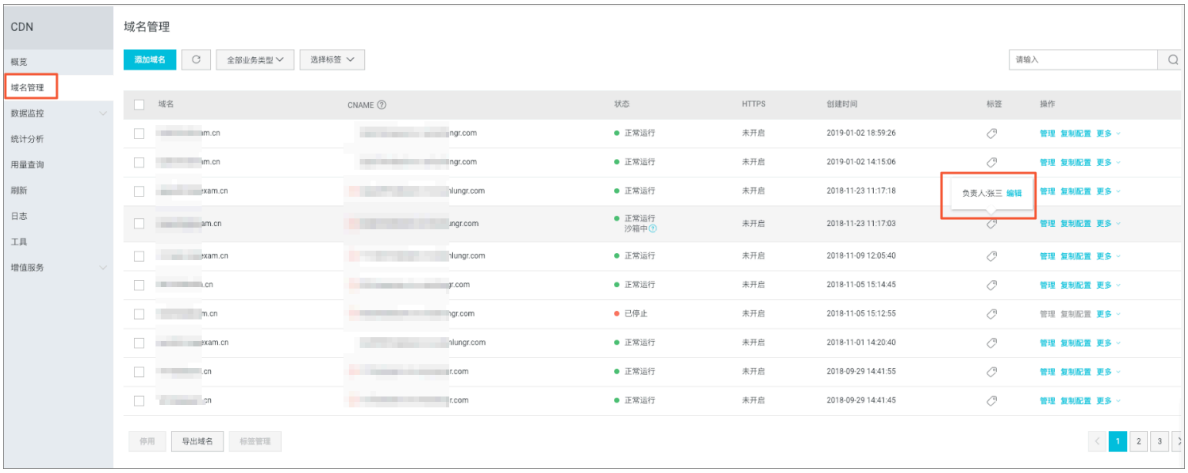
- 绑定标签，创建用于标记域名的用途或对域名进行分组管理的标签。
- 解绑标签，删除已经不再适用于您当前某个或多个域名用途的标签。
- 使用标签管理域名，域名绑定标签后，您可以使用标签，快速筛选对应的域名，进行分组管理。
- 使用标签筛选数据，域名绑定标签后，您可以使用标签，快速筛选对应的域名，查询域名数据。

4.2.2 绑定标签

如果您需要标记域名的用途或为域名分组，您可以通过标签功能为该域名绑定标签。

操作步骤

1. 登录CDN控制台。
2. 单击域名管理。
3. 选择您想要设置标签的域名，将鼠标移动到对应标签上。
4. 在浮窗内，单击编辑。



5. 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。

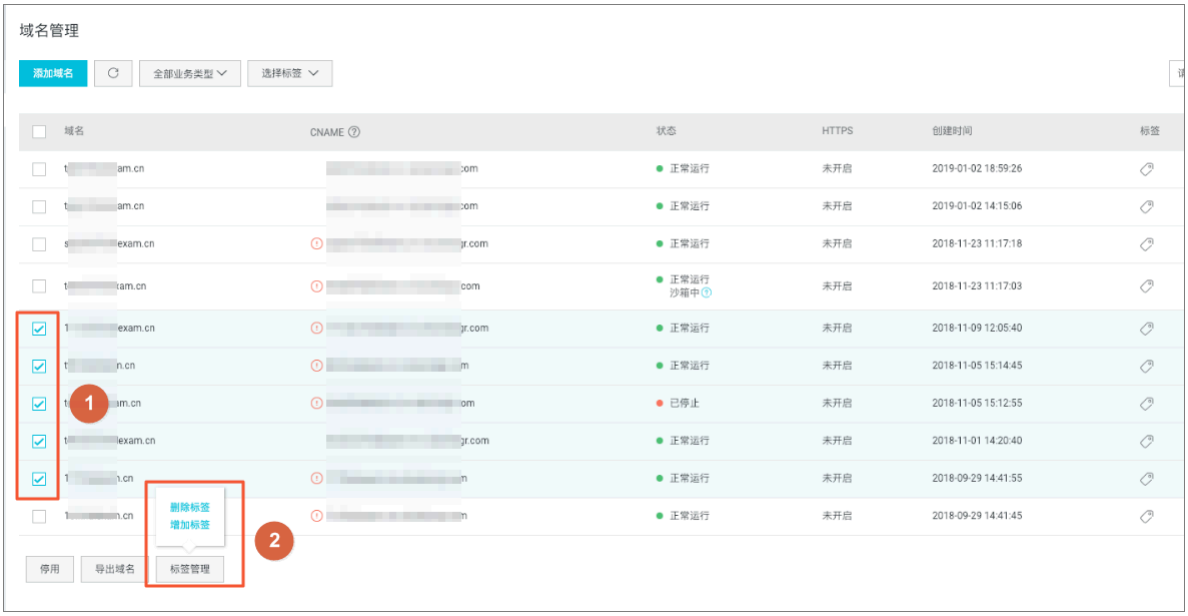
6. 编辑完成后，单击确定。

4.2.3 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时，您可以参照本文档，解绑您的域名标签。

操作步骤

1. 登录CDN控制台。
2. 单击域名管理。
3. 勾选您想要处理的域名，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并单击确定，完成解绑。

4.2.4 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。

操作步骤

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

4.2.5 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。

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

域名	Key为部门，Value为	Key为业务，Value为	Key为负责人，Value为
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。

4.2.6 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。

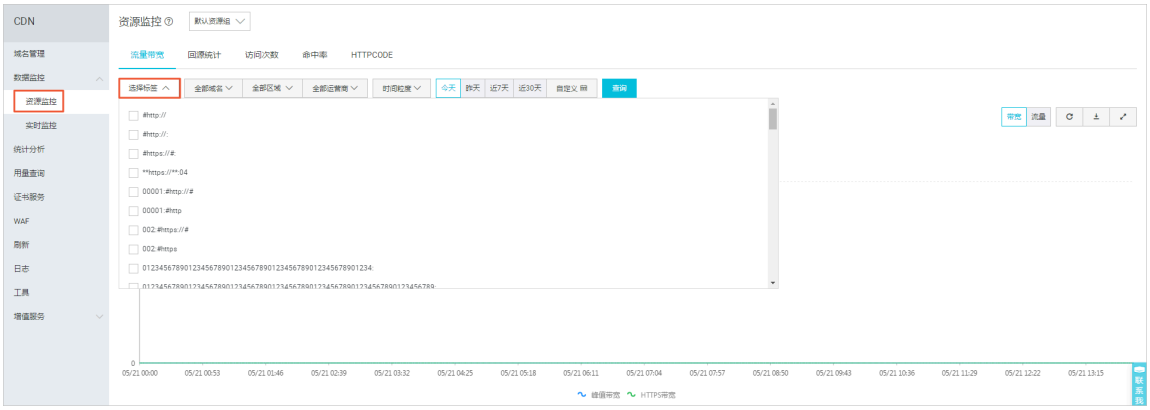
操作步骤

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。

- 选择数据监控 > 资源监控，选择对应的键（Key）和值（Value）标签，单击查询。



- 单击用量查询，选择对应的键（Key）和值（Value）标签，单击查询。

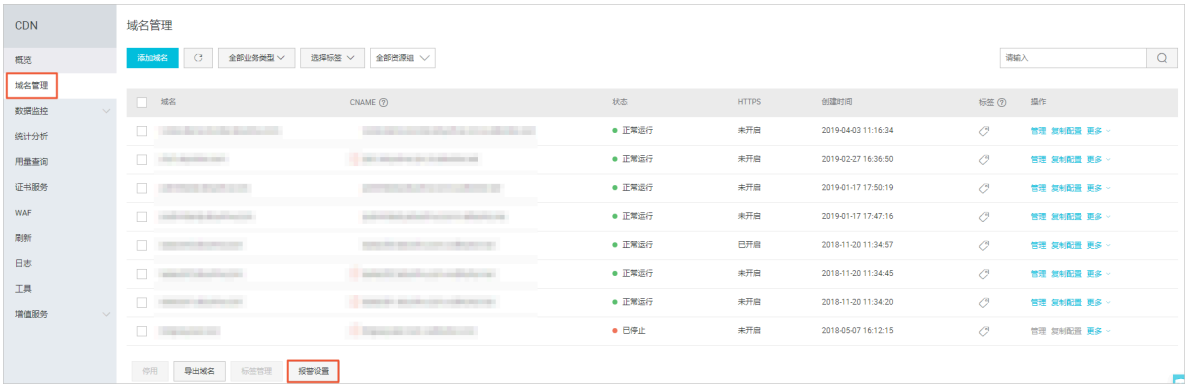
4.3 设置报警

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，您可以直接使用阿里云监控产品设置报警规则。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。

操作步骤

1. 登录CDN控制台。
2. 单击域名管理。

3. 单击报警设置，跳转到阿里云监控产品的配置页面。



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，创建针对CDN的报警规则，详情请参见创建阈值报警规则。

4.4 基本配置

4.4.1 基本配置概述

通过基本配置功能，您可以查看加速域名的基础信息和源站信息。此外，您还可以进行切换域名的加速区域和源站设置。

功能介绍

加速域名的基础信息包括：CNAME地址、创建时间和加速区域。阿里云CDN支持三种类型回源域名，包括OSS域名、IP和源站域名。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:

- 多源优先级的设置只支持IP和源站域名类型，OSS域名不支持多源优先级功能。您可以根据实际需求，选择适合自己的源站类型及设置合理的优先级。

- 源站健康检查：实行主动四层健康检查机制，测试源站的80端口。每2.5秒检查一次，连续3次失败标记为不可用。

多个源站的回源策略：用户100%回源流量都将首先回源优先级为主的源站，如果某个源站连续3次健康检查都失败，则100%回源流量将选择优先级为备的源站回源。如果该源站主动健康检查成功，那么该源站将重新标记为可用，恢复原来优先级。当所有源站的回源优先级一样时，CDN将自动轮询回源。

主要支持场景：主备方式切换源站。

计费说明

- 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。

4.4.2 切换加速区域

当您需要变更您的CDN服务范围时，您可以通过切换加速区域功能实现。

操作步骤

1. 登录*CDN*控制台。
2. 单击域名管理。
3. 在域名管理页面，单击目标域名后的管理。
4. 单击基本配置。
5. 在基础信息区域框单击修改配置。

6. 在加速区域对话框选择您需要切换的加速区域，单击确定，设置成功。

4.4.3 配置源站

如果您的源站信息需要修改（如源站类型、源站地址、端口），通过本文档，您可以在源站配置页面修改源站信息。

背景信息

在配置源站时，您需要注意以下几点：

- 如果您的业务类型为直播流媒体，则不支持源站设置。
- 当源站类型设置为IP或源站域名时，可设置多个源站。添加多个源站时，需要为每个源站设置优先级，优先级分为主和备。
- 您可以在开通白名单后，设置自定义端口。自定义端口支持范围为0 ~ 65535。
  - 如果您的静态或动态协议设置为跟随，则无法设置自定义端口。
  - 如果您通过OpenAPI将回源协议设置为跟随，请确保您的回源协议和自定义端口均能正常使用。
  - 如果您通过端口设置了回源协议（HTTP或HTTPS）和自定义端口，则无论您在控制台如何设置，回源都将按照端口的配置进行。

操作步骤

1. 登录CDN控制台。
2. 单击域名管理。
3. 在域名管理页面，单击目标域名后的管理。
4. 单击基本配置。

5. 在源站信息区域框单击修改配置。
6. 在源站配置对话框，设置源站类型、源站地址和端口（您可以选择的回源端口类型为：80端口、443端口和自定义端口）。

7. 单击确认，设置成功。

4.5 内容回源设置

4.5.1 设置回源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，可以参照本文档，设置回源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。

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。

> **说明:**
> 如果您的源站绑定了多个域名或站点时，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。
- 回源HOST：回源HOST决定了回源请求访问到该IP上的具体站点。

回源HOST的默认值为：

- 在您源站类型是IP的情况下，您的回源HOST类型默认为加速域名。

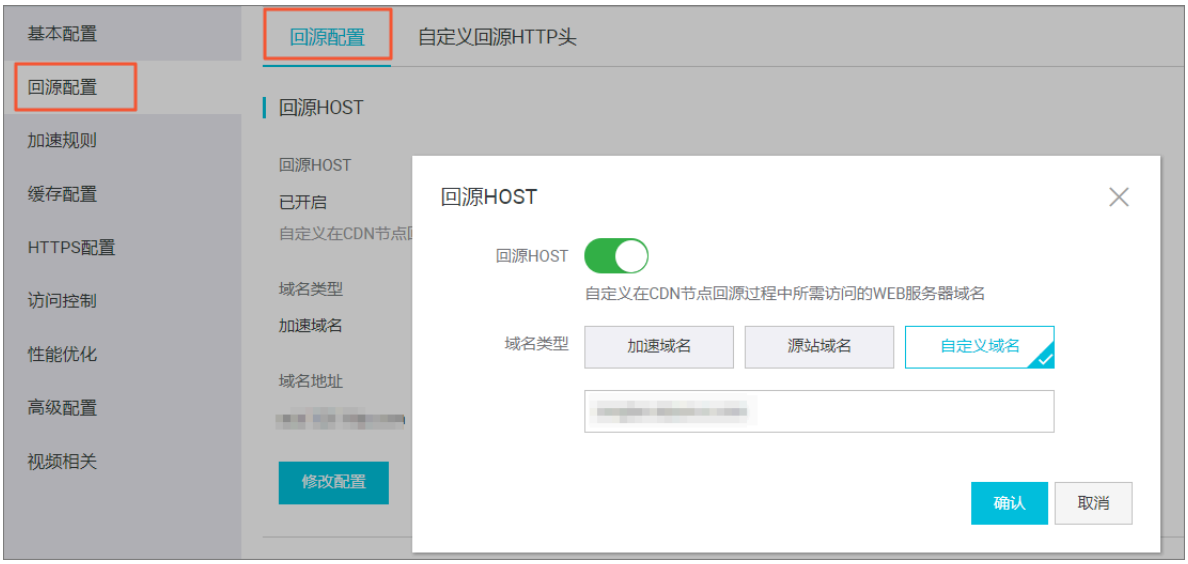
- 在您源站类型是OSS域名的情况下，您的回源HOST类型默认为源站域名。

示例：

- 在您的源站是域名源站www.a.com的情况下，您选择将回源HOST设置为www.b.com，则实际回源的是www.a.com解析到的IP站点www.b.com。
- 在您的源站是IP源站1.1.1.1的情况下，您选择将回源HOST设置为www.b.com，则实际回源的是1.1.1.1对应的主机上的站点www.b.com。

操作步骤

1. 登录CDN控制台。
2. 单击域名管理。
3. 在域名管理页面，单击目标域名后的管理。
4. 单击回源配置。
5. 在回源HOST区域框，单击修改配置。
6. 打开回源HOST开关，选择域名类型，单击确定，配置成功。



4.5.2 设置协议跟随回源

本文档介绍了什么是协议跟随回源，开启该功能后，您可以按照您设定的协议规则进行回源。

背景信息

协议跟随回源，指回源使用的协议和客户端访问资源的协议保持一致，即如果客户端使用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. 单击域名管理。
3. 在域名管理页面，单击目标域名后的管理。
4. 单击回源配置，在协议跟随回源区域框中，打开协议跟随回源开关，开启该功能。
5. 单击修改配置，您可以选择的回源协议类型为：跟随、HTTP或HTTPS。

- 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。

6. 单击确定，配置成功。

4.5.3 私有bucket回源授权

功能介绍

私有bucket回源授权是指若加速域名想要回源至该用户账号下标记为私有的bucket时，需要首先进行授权，授权成功并开启授权配置后，用户开启了私有bucket授权的域名有权限访问私有bucket。

您可以配合使用cdn提供的refer防盗链功能，鉴权等功能，有效保护您的资源安全。

警告：

- 进行一次回源授权，即授权CDN对用户所有Bucket的只读权限，不只是对当前bucket授权。

- 授权成功并开启了对应域名的私有bucket功能，该加速域名可以访问您的私有bucket内的资源内容。开启该功能前，请根据实际的业务情况，谨慎决策。若您授权的私有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。
- 若您的网站有攻击风险，请购买高防服务，请勿授权或开启私有bucket功能。

操作步骤

如何开启私有bucket回源授权?

1. 进入域名管理页面，选择需要设置的域名，单击管理。

2. 在回源配置 > 私有Bucket回源设置中，开启该功能。

3. 单击立即授权。

4. 授权成功，为该域名开启私有bucket回源配置，单击确定。
5. 设置成功。

如何关闭私有bucket回源授权?

> **说明:**
> 若您的加速域名正在使用私有bucket做为源站进行回源，请不要关闭或删除私有bucket授权。

1. 进入访问控制 > 角色管理。
2. 删除AliyunCDNAccessingPrivateOSSRole授权。
3. 私有bucket授权删除成功。

4.5.4 关闭私有Bucket回源

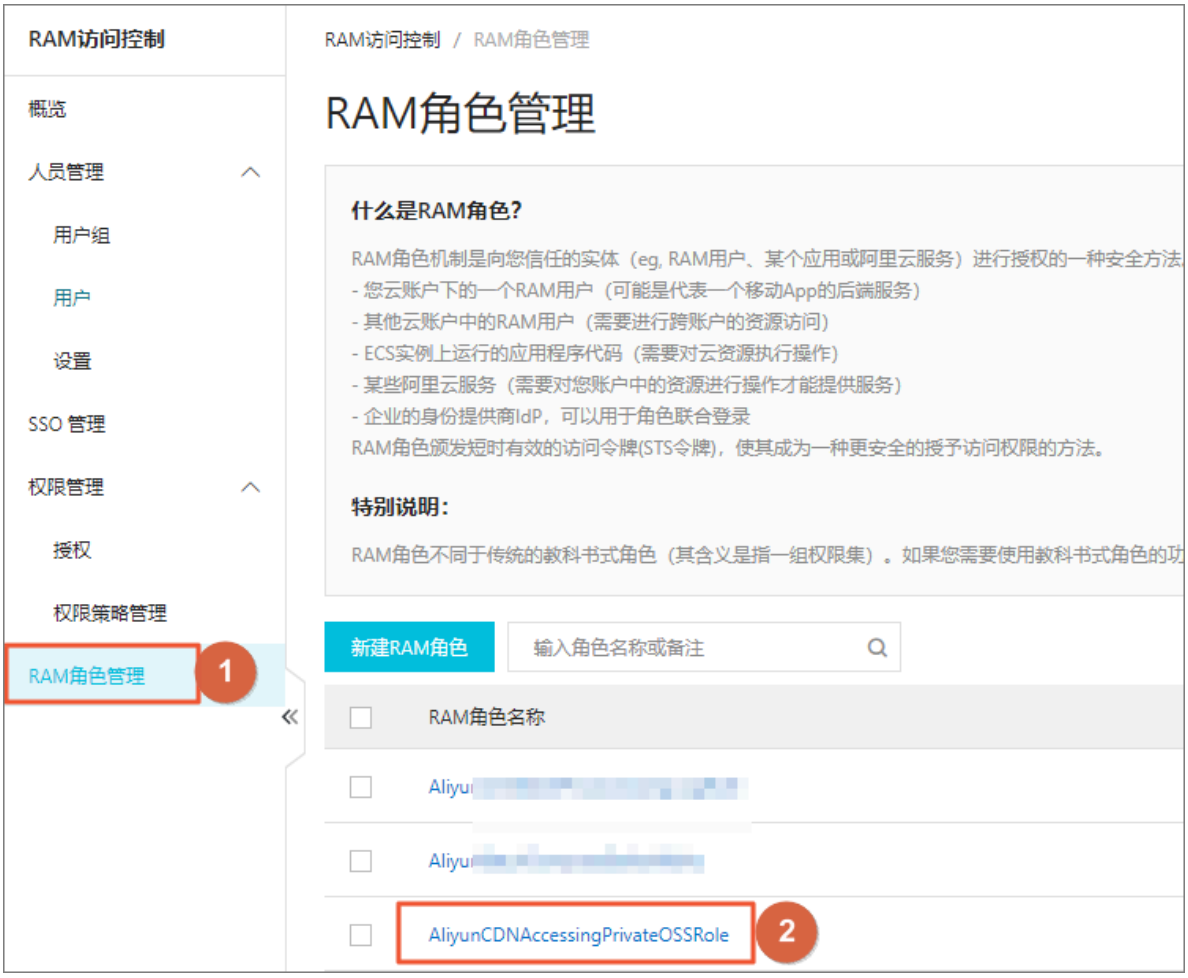
本文档介绍了如何移除加速域名能够访问您私有bucket内资源内容的权限。您可以通过RAM（Resource Access Management）控制台，取消对应角色名称的授权，关闭私有Bucket回源功能。

背景信息

> **说明:**
> 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. 单击移除权限。

5. 返回RAM角色管理页面，单击删除，单击确认。

了解如何开启私有Bucket回源，请参见开启私有Bucket回源。

4.5.5 设置回源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，您可以参照本文档，设置回源SNI指明具体访问的域名。

背景信息

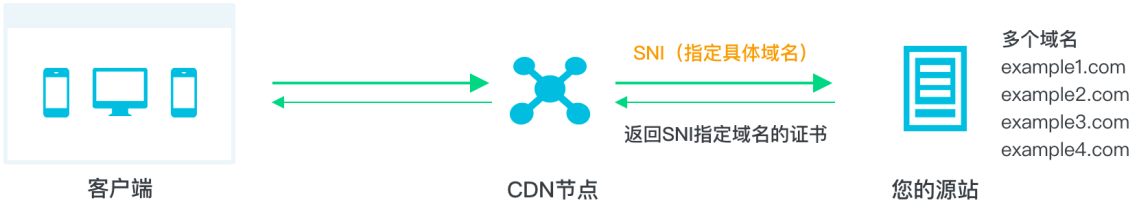
服务器名称指示 Server Name Indication（SNI）是一个扩展的传输层安全性协议 Transport Layer Security（TLS）。在该协议下，握手过程开始时，客户端会告诉它正在连接的那台服务器即将要连接的主机名称，以允许该服务器在相同的IP地址和TCP端口号上呈现多个证书，即一台服务器可以为多个域名提供服务。因此，同一个IP地址上提供的多个安全的HTTPS网站（或其他任何基于TLS的服务），不需要使用相同的证书。

但是，如果您的源站服务器使用单个IP提供多个域名的HTTPS服务，且您已经为您的CDN设置了以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的，则无需设置回源SNI。

工作原理

回源SNI的工作原理如下图所示：

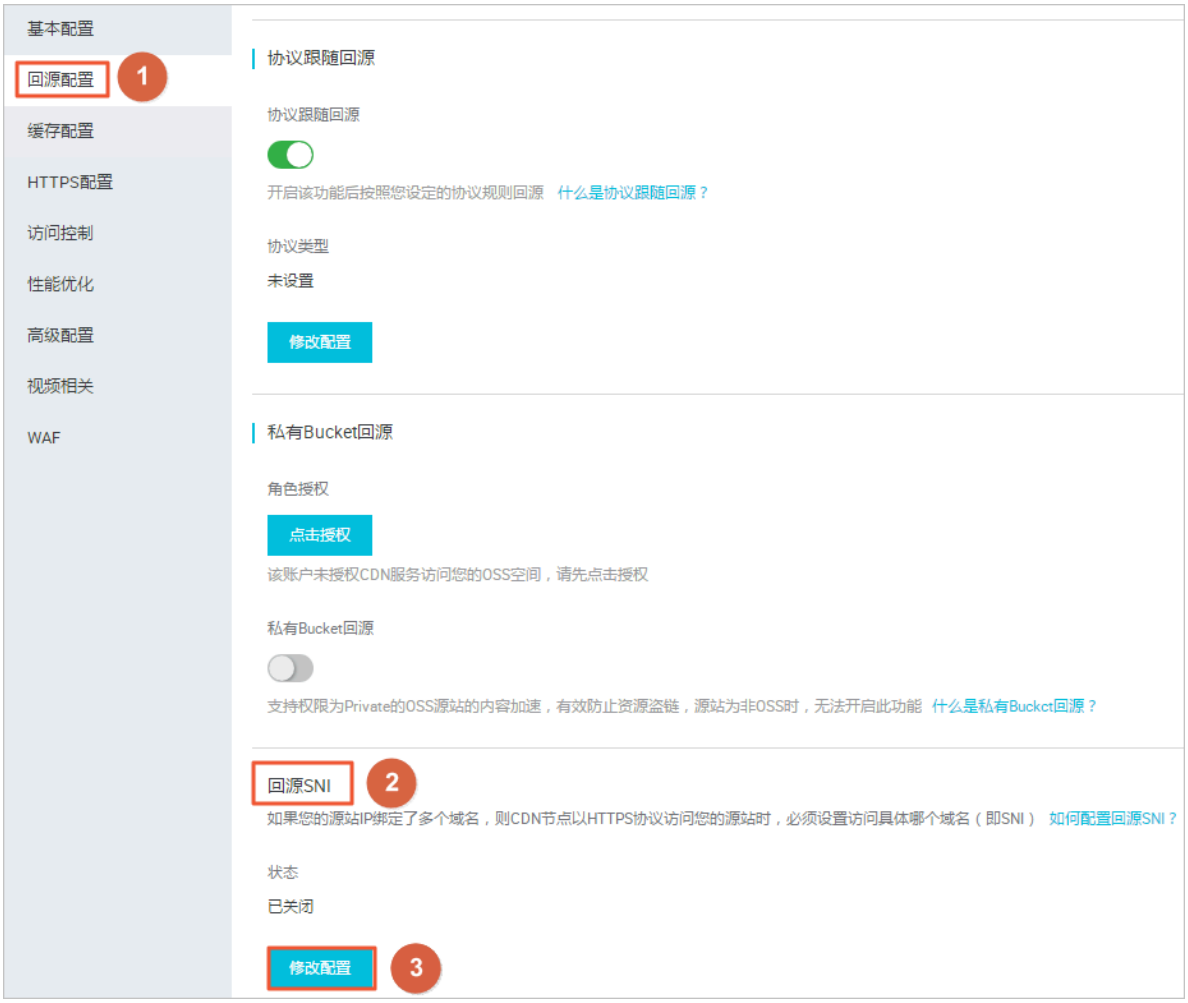


1. CDN节点以HTTPS协议访问源站时，在SNI中指定访问的域名。
2. 源站接收到请求后，根据SNI中记录的域名，返回对应域名的证书。
3. CDN节点收到证书，与服务器端建立安全连接。

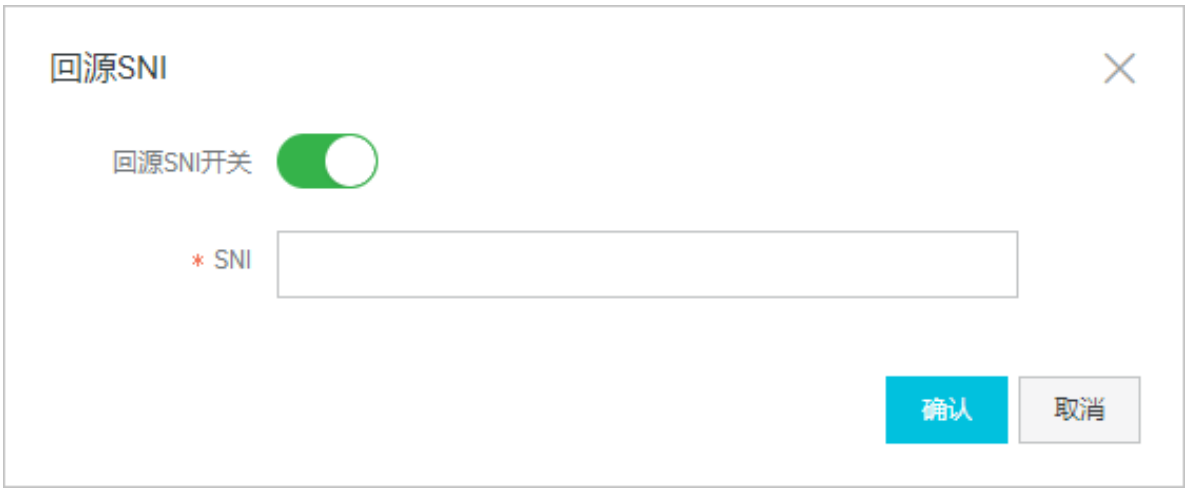
操作步骤

1. 登录*CDN*控制台。
2. 单击域名管理。
3. 在域名管理页面，单击目标域名后的管理。
4. 单击回源配置。

5. 在回源SNI区域框，单击修改配置。



6. 打开回源SNI开关，填入您服务器源站提供服务的具体域名，单击确认，完成配置。



4.6 节点缓存设置

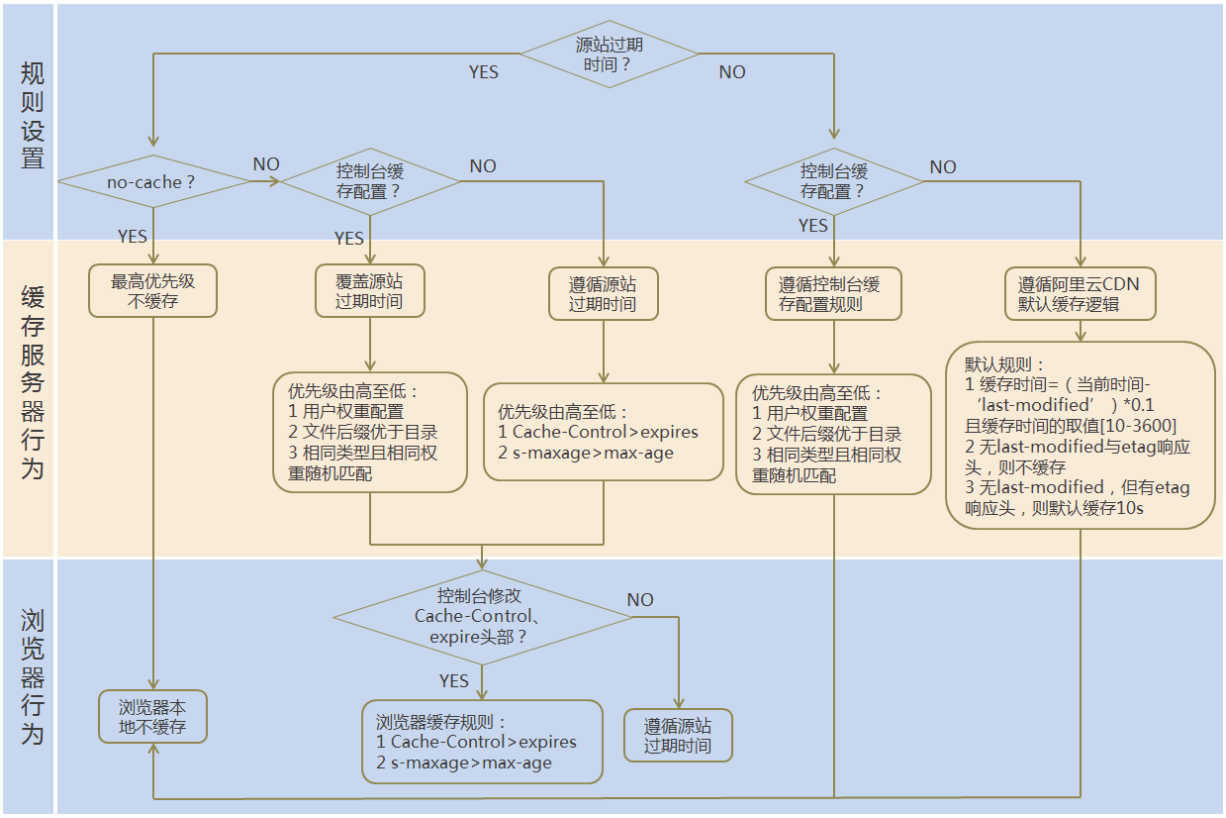
4.6.1 设置缓存过期时间

通过本文档，您可以针对不同目录路径或文件名后缀的资源，自定义指定资源内容的缓存过期时间规则和缓存策略优先级，设置它们的缓存过期时间。

背景信息

配置缓存资源的过期时间前，建议您源站的内容不使用同名更新，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。

关于CDN节点上缓存资源的缓存策略流程图如下：



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配置，则支持按目录、文件后缀两种方式设置（支持设置完整路径缓存策略）。
- 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。

操作步骤

1. 登录CDN控制台。
2. 单击域名管理。
3. 在域名管理页面，单击目标域名后的管理。
4. 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“/”开头，如*/directory/aaa*。 · 添加多个文件后缀名时，须以半角逗号分隔，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：文件名后缀为jpg、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。 那么，缓存策略1优先生效。

7. 单击确认，配置成功。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。

4.6.2 设置状态码过期时间

本文为您介绍了如何设置状态码的缓存策略。通过设置状态码过期时间，您可以设置缓存在CDN节点上资源的过期时间。

背景信息

您在设置状态码过期时间时，请注意：

· 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(negative_ttl)为一秒。
· 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，单击目标域名后的管理。
4. 在左侧导航栏，单击缓存配置。
5. 在状态码过期时间页签，单击添加，增加状态码的缓存策略。

6. 在状态码过期时间对话框，选择类型并进行相关设置。

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。

类型	注意事项
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。

7. 单击确认，配置成功。您也可以单击修改或删除，对当前状态码过期时间的配置进行相应操作。

4.6.3 设置HTTP响应头

当您的客户端请求加速域名下的资源时，通过本文档，您可以在返回的响应消息中配置HTTP头，实现跨域访问等目的。

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。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。

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。目前阿里云提供10个HTTP响应头参数可供您自行定义取值，参数解释如下：

参数	描述
Content-Type	指定客户端程序响应对象的内容类型。
Cache-Control	指定客户端程序请求和响应遵循的缓存机制。
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。
Content-Language	指定客户端程序响应对象的语言。
Expires	指定客户端程序响应对象的过期时间。
Access-Control-Allow-Origin	指定允许的跨域请求的来源。
Access-Control-Allow-Headers	指定允许的跨域请求的字段。
Access-Control-Allow-Methods	指定允许的跨域请求方法。
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。
Access-Control-Expose-Headers	指定允许访问的自定义头信息。

注意事项

· HTTP响应头的设置会影响该加速域名下所有资源客户端程序（例如浏览器）的响应行为，但不会影响缓存服务器的行为。

- 目前仅支持上述HTTP头参数取值设置。如果您有其他HTTP头部设置需求，请提交工单反馈。
- 关于参数Access-Control-Allow-Origin的取值，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`。
- 目前不支持泛域名设置。

操作步骤

1. 登录*CDN*控制台。
2. 单击域名管理。
3. 单击目标域名后的管理。
4. 单击缓存配置 > HTTP头。
5. 单击添加，选择参数，并输入取值。

6. 单击确认，配置成功。您也可以单击修改或删除，对当前HTTP响应头的配置进行相应操作。

4.6.4 设置自定义页面

本文档介绍了如何自定义设置状态码返回的页面。您可以通过自定义HTTP或者HTTPS响应返回码跳转的完整URL地址，优化用户体验。

背景信息

阿里云提供两种状态码返回时的页面，分别是默认页面和自定义页面。

以返回码404为例：

- 默认值：http响应返回404时，服务器返回默认404 Not Found页面。
- 公益404：http响应返回404时，将会跳转到实时更新的公益*404*页面。
- 自定义404：http响应返回404时，将会跳转到自行设计和编辑的404页面，需要自定义跳转页的完整URL地址。

注意事项

- 公益404页面属于阿里云公益资源，不会造成用户的任何流量费用，完全免费。
- 自定义页面属于个人资源，按照正常分发计费。

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，单击目标域名后的管理。
4. 在左侧导航栏，单击缓存配置。
5. 在自定义页面页签，单击添加，增加自定义返回码的页面内容。

本文以自定义错误码404为例，假设您需要将404页面`error404.html`资源如其他静态文件一样存储到源站域名下，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`http://exp.aliyun.com/error404.html`即可。（包含`http://`）

6. 单击确认，配置成功。您也可以单击修改或删除，对当前配置进行相应操作。

4.6.5 重写

本文档为您介绍了重写功能介绍、使用场景及控制台操作步骤。重写功能可以配置多条rewrite匹配规则，您可以对请求的URI进行修改、重定向至目标URI。

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，您可以通过该功能配置，所有http://example.com请求都重定向到https://example.com。

执行规则说明：

- 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。

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. 在您需要设置的域名，单击管理。
4. 在左侧导航栏，单击缓存配置。
5. 在重写区域框中，单击添加。
6. 根据您的需求进行配置，选择Redirect或Break，单击确定。

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。

4.7 HTTPS安全加速

4.7.1 概述

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。

什么是HTTPS?

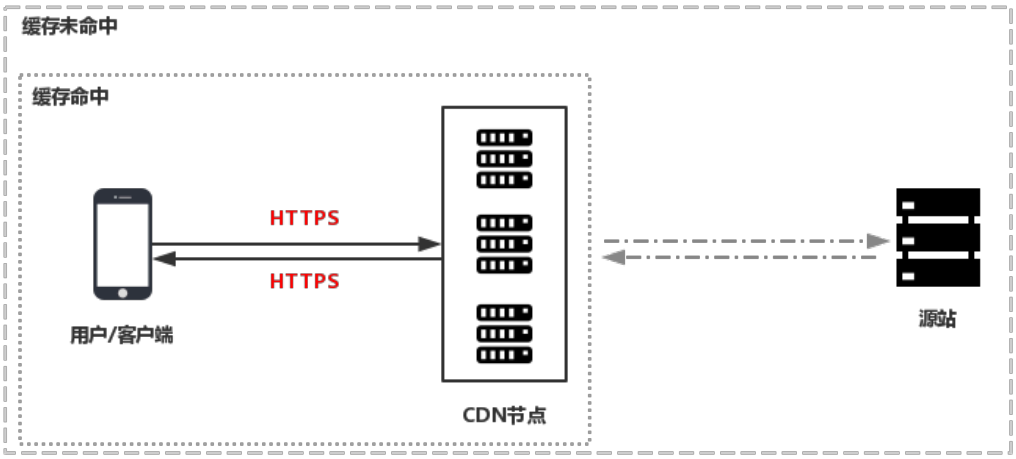
HTTP协议以明文方式发送内容，不提供任何方式的数据加密。HTTPS协议是以安全为目标的HTTP通道，简单来说，HTTPS是HTTP的安全版，即将HTTP用SSL/TLS协议进行封装，HTTPS的安全基础是SSL/TLS协议。HTTPS提供了身份验证与加密通讯方法，被广泛用于万维网上安全敏感的通讯，例如交易支付方面。

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，将实现客户端和阿里云CDN节点之间请求的HTTPS加密。而CDN节点返回源站获取资源的请求仍按您源站配置的方式进行。建议您源站也配置并开启HTTPS，实现全链路的HTTPS加密。

HTTPS加密流程如下：



1. 客户端发起HTTPS请求。
2. 服务端生成公钥和私钥（可以自己制作，也可以向专业组织申请）。
3. 服务端把相应的公钥证书传送给客户端。

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），并用公钥该随机数进行加密，传输给服务端。
   - 如果证书不正确，则SSL握手失败。

   
   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. 服务端用密钥对传输的数据进行加密。
7. 客户端用密钥对服务端的加密数据进行解密，拿到相应的数据。

优势

- HTTP明文传输，存在各类安全风险：
  - 窃听风险：第三方可以获知通信内容。
  - 篡改风险：第三方可以修改通信内容。
  - 冒充风险：第三方可以冒充他人身份参与通信。
  - 劫持风险：包括流量劫持、链路劫持、DNS劫持等。
- HTTPS安全传输的优势：
  - 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，终端客户在访问自身网站的时出现的不安全标识，也将极大的影响访问者的访问行为。
  - 百度与Google均对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。可以看出来，无论从安全，还是市场还是用户体验来看，普及HTTPS未来的一个方向，所以也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以下五类：

- 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或信任危机。
- 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。

注意事项

- 配置相关
  - 支持开启HTTPS安全加速功能的业务类型包括：
    - 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。
    - 直播流媒体，主要适用于交互性在线教育网站、游戏竞技类直播站点、个人秀场直播、事件类和垂直行业的直播平台等。
  - 支持泛域名HTTPS服务。
  - 支持HTTPS安全加速的启用和停用。
    - 启用：您可以修改证书，系统默认兼容HTTP和HTTPS请求。您也可以设置强制跳转，自定义原请求方式。
    - 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。再次开启证书，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。

- 计费相关

  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。

- 证书相关

  - 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，配置以下功能：

- 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。
- 设置强制跳转，强制重定向终端用户的原请求方式。
- 设置TLS，保障您互联网通信的安全性和数据完整性。
- 设置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。

4.7.2 配置HTTPS证书

阿里云CDN仅支持pem格式的证书和私钥，您需要上传HTTPS证书至CDN开启HTTPS安全加速。本文档介绍了不同类型的HTTPS证书的认证方式以及如何设置HTTPS证书。

前提条件

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

背景信息

从证书的认证级别来看，证书分为DV、OV、EV三种类型：

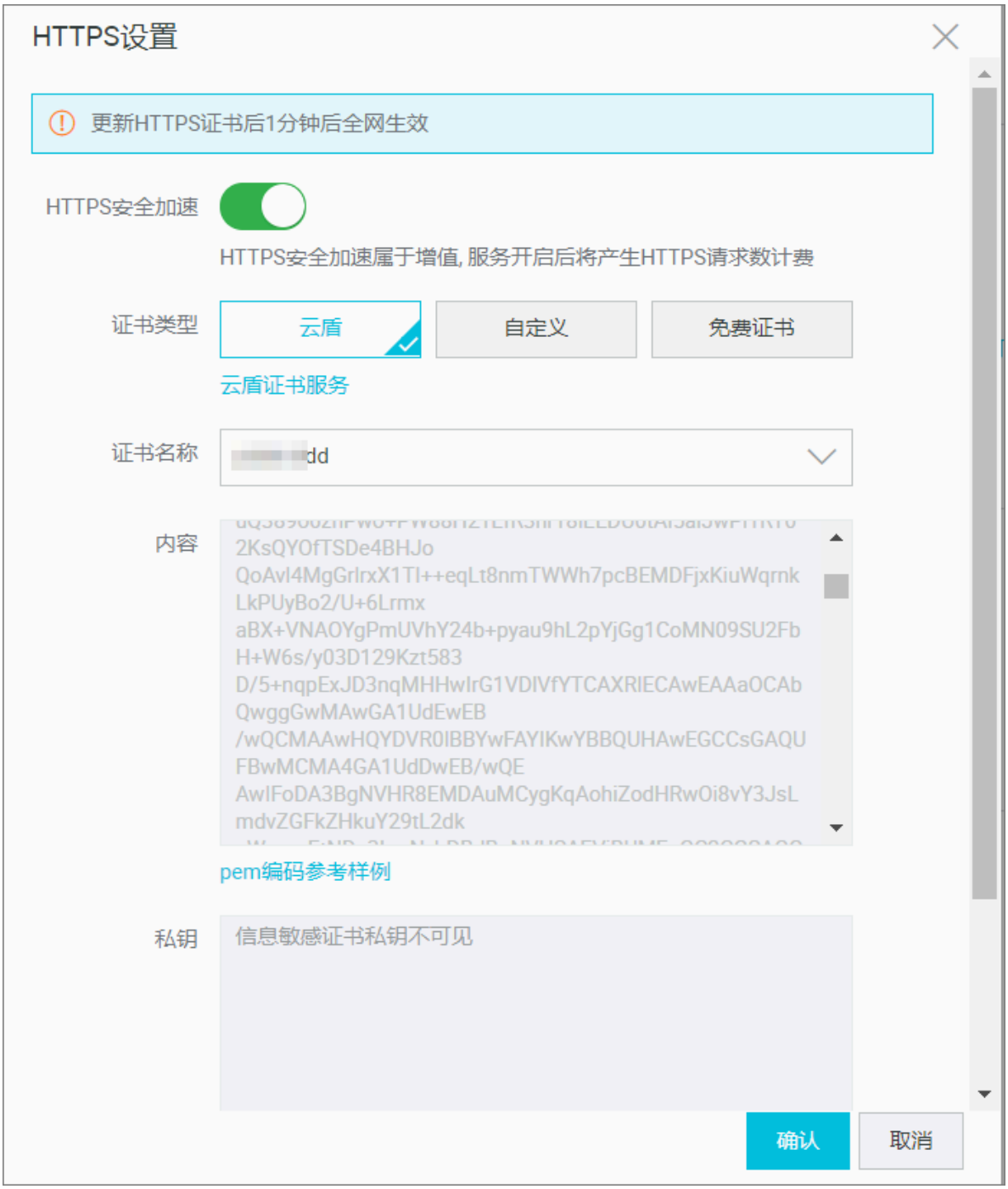
- DV是Domain Validation，仅认证域名所有权，通常是验证域名下某个指定文件的内容，或者验证与域名相关的某条TXT记录，显示明显的安全锁。
- OV是Organization Validation，指需要验证企业组织真实性的标准型SSL证书，比DV SSL证书更加安全可信，安全保险也会更高。同时审核也会更加严格，审核周期也更长。一般多用于电商，教育，游戏等领域。
- EV是Extended Validation，CA/browser forum指定的全球统一标准，通过证书object identifier（OID）来识别，显示完整企业名称，是目前全球最高等级的SSL证书多用于金融支付，网上银行等领域。

> **说明:**
> 目前仅支持PEM格式的证书，如果您的证书不是PEM格式，请参见证书格式转换方式进行格式转换。

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，单击目标域名后的管理。
4. 在左侧导航栏，单击HTTPS配置。
5. 在HTTPS证书区域框，单击修改配置。

6. 在HTTPS设置对话框中，打开HTTPS安全加速开关，选择证书。您可以选择的证书类型包括：云盾、自定义和免费证书。



- 您可以选择云盾。若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。您可以在我的证书里查看。
- 您也可以选择免费证书，即阿里云的Digicert免费型DV版SSL证书。CDN的免费证书只适用于CDN的*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。

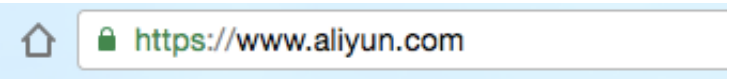
- 免费证书的申请需要5~10分钟。等待期间，您也可以重新选择上传自定义证书或者选择托管证书。
- 无论您启用的是自定义证书、托管证书，还是免费证书，都可以相互切换。
- 免费证书有效期为1年，到期后自动续签。
- 在您使用过程中，如果关闭HTTPS安全加速后，当再次开启使用免费证书时，将直接使用已申请但未过期的证书。若开启时证书已过期，您需要重新申请免费证书。

7. 单击确认，完成配置。

   您可以停用、启用和修改证书。停用证书后，系统将不再保留证书信息。再次开启证书时，需要重新上传证书或私钥。

   > 说明:
   > 关于更换证书：
   > · 如果您想更换为免费证书或阿里云云盾证书，可以在步骤7中，选择对应证书类型（即云盾或免费证书）即可。
   > · 如果您想更换为自定义证书，可以在步骤7中，选择自定义证书类型，填写新证书的名称和内容并提交即可。

8. 验证证书是否生效。证书生效后（约1小时），使用HTTPS方式访问资源。如果浏览器中出现绿色HTTPS标识，说明当前与网站建立的是私密连接，HTTPS安全加速生效。

4.7.3 证书格式说明

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

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CDN使用的证书是Nginx，.crt为证书，.key为私钥。

证书规则为：

· 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。

Linux环境下，`PEM`格式的证书示例如下：

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。

- 每一份证书遵守第一点关于证书的格式说明。

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-----`这种样式的私钥时，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 outcertifi
    cate.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
    ```

4.7.4 设置HTTP/2

通过本文档，您可以了解什么是HTTP/2协议，以及它的优势和配置方法。

前提条件

开启HTTP/2功能前，您需要确保已经成功配置*HTTPS*证书。

说明：

- 若您是第一次配置HTTPS证书，需要等证书配置完成且生效后，才能开启HTTP/2。
- 若您已经开启了HTTP/2，但是又关闭了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，是最新的HTTP协议。目前，Chrome、 IE11、Safari以及Firefox等主流浏览器已经支持HTTP/2协议。HTTP/2优化了性能，兼容了HTTP/1.1的语义，与SPDY相似，与HTTP/1.1有巨大区别。

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。基于二进制可以让协议有更多的扩展性，比如引入了帧来传输数据和指令。
- 内容安全：HTTP/2基于HTTPS，因此天然具有安全特性。通过HTTP/2的特性可以避免单纯使用HTTPS的性能下降。
- 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，允许客户端告诉服务器哪些内容是更优先级的资源，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Chrome浏览器登陆控制台，您可以查看是否启用HTTP/2。

> **说明:**
> SPDY是Google开发的基于TCP的应用层协议，用以最小化网络延迟，提升网络速度，优化用户的网络使用体验。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、请求优先级以及HTTP报头压缩，与HTTP/2相似。

操作步骤

1. 登录*CDN*控制台。
2. 单击域名管理。
3. 在域名管理页面，单击目标域名后的管理。
4. 单击HTTPS配置。

5. 在HTTP/2设置页签，打开HTTP/2开关，开启该功能。

4.7.5 设置强制跳转

本文档介绍了如何设置客户端请求的强制跳转类型。您可以通过设置强制跳转功能，将客户端至L1的原请求方式强制重定向为HTTP或者HTTPS。

前提条件

配置强制跳转类型前，您需要配置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，单击目标域名后的管理。
4. 在左侧导航栏，单击HTTPS配置。

5. 在强制跳转区域框，单击修改配置。

6. 在强制跳转对话框，选择跳转类型，单击确认。

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。

跳转类型	说明
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。

本文以设置跳转类型为HTTP -> HTTPS为例：

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>
```

4.7.6 设置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。

前提条件

开启TLS功能前，您需要确保已成功配置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。

目前，TLS主要有4个版本：

- 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。支持的主流浏览器： IE6+、Chrome 1+、Firefox 2+。
- TLSv1.1：RFC4346，2006年发布，修复TLSv1.0若干漏洞。支持的主流浏览器：IE11+、Chrome22+、Firefox24+、Safri7+。
- TLSv1.2：RFC5246，2008年发布，目前广泛使用的版本。支持的主流浏览器：IE11+、Chrome30+、Firefox27+、Safri7+。
- 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）。支持的主流浏览器：Chrome 70+和Firefox 63+。

操作步骤

1. 登录*CDN*控制台。
2. 单击域名管理。
3. 单击目标域名后的管理。
4. 单击HTTPS配置。

5. 在TLS版本控制区域框，根据您的需要，开启或关闭对应的TLS版本。

说明:

目前TLSv1.0、TLSv1.1和TLSv1.2版本默认开启。

4.7.7 设置HSTS

通过开启HSTS（HTTP Strict Transport Security）功能，您可以强制客户端（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。

前提条件

开启HSTS功能前，您需要确保已经成功配置HTTPS证书。

背景信息

当您网站全站使用HTTPS后，需要将所有HTTP请求301/302重定向到HTTPS。如果您从浏览器输入HTTP链接，或在其他地方单击了HTTP链接，则服务器会将该HTTP请求301/302重定向到HTTPS。但是这个过程可能被劫持，导致重定向后的请求没有到服务器，这个问题可以通过HSTS来解决。

HSTS是一个响应头：`Strict-Transport-Security: max-age=expireTime [; includeSubDomains] [; preload]`，各参数说明如下：

- max-age：单位是秒。
- Strict-Transport-Security： 在浏览器缓存的时间，浏览器处理域名的HTTP访问时，若该域名的Strict-Transport-Security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301/302重定向被劫持的风险。
- includeSubDomains：可选参数。如果指定这个参数，说明这个域名所有子域名也适用上面的规则。
- preload：可选参数，支持preload列表。

 说明：

- HSTS生效前仍然需要第一次301/302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。
- 启用HSTS之后，一旦网站证书错误，在缓存时间。

操作步骤

1. 登录*CDN*控制台。
2. 单击域名管理。
3. 在域名管理页面，单击目标域名后的管理。
4. 单击HTTPS配置。

5. 在HSTS区域框，单击修改配置。

6. 在HSTS设置对话框，打开HSTS开关，填写过期时间，单击确定。

4.7.8 常见问题

- CDN开启HTTPS加速后#会有额外收费吗#
- 开启HTTPS加速后#会消耗更多服务资源或者降低访问速度吗#
- 我的站点只有登录才需要HTTPS#其他都不需要HTTPS了#
- 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:
  您可以直接在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加速后，会消耗更多服务资源或者降低访问速度吗?

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。

我的站点只有登录才需要HTTPS，其他都不需要HTTPS了?

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了大量的重定向，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，若想要全面的保证网络安全，还需要接入WAF，DDOS等防御能力全面来保证网站安全，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，例如诱使用户点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，无论你的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。

4.8 访问控制设置

4.8.1 配置防盗链

本文为您介绍了如何配置防盗链功能。通过配置防盗链功能，可以实现对访客身份进行过滤。

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。用户可以通过配置访问的Referer黑名单和白名单来对访问者身份进行识别和过滤，从而限制CDN资源被访问的情况。
- 目前防盗链功能支持黑名单或白名单机制，访客对资源发起请求后，请求到达CDN节点，CDN节点会根据用户预设的防盗链黑名单或白名单，对访客的身份进行过滤。符合规则可以顺利请求到资源；若不符合规则，则该访客请求会返回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。
> - 配置后会自动添加泛域名支持。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CDN资源，即允许在浏览器地址栏输入地址直接访问资源URL。

操作步骤

1. 登录*CDN控制台*。
2. 在域名管理页面，选择您想设置的域名，单击管理。

3. 在访问控制 > Refer防盗链区域框中，单击修改配置。

4. 单击黑名单或白名单，在规则内输入想要添加的网段。

5. 单击确认，您已完成配置防盗链功能。

4.8.2 配置URL鉴权

URL鉴权功能主要用于保护用户站点的内容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。

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，实现了一种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（包含权限验证信息）。
- 您使用加密后的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以判断请求的合法性。正常响应合法请求，拒绝非法请求。

阿里云CDN兼容并支持鉴权方式A、鉴权方式B、鉴权方式C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。

如果您想了解Python鉴权代码示例，请参见 鉴权代码示例。

操作步骤

1. 登录CDN控制台。
2. 在域名管理 页面，选择您需要设置的域名，单击配置。
3. 在访问控制 > URL鉴权区域框中，单击修改配置。

4. 打开URL鉴权开关，选择鉴权类型，并填写主KEY和备KEY。

4.8.3 鉴权方式A

本文为您介绍了鉴权方式A的原理并用示例说明。鉴权功能主要用于保护用户站点的内容资源不被非法站点下载盗用。

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

字段	描述
DomainName	CDN站点的域名。

字段	描述
timestamp	失效时间，整形正数，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。
PrivateKey	您设定的鉴权密钥。
Filename	实际回源访问的URL，鉴权时Filename需以/开头。

CDN服务器接收请求后，会首先判断请求中的timestamp是否小于当前时间。

- 如果小于当前时间，服务器判定过期失效并返回HTTP 403错误。
- 如果大于当前时间，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，再和请求中md5hash进行比对。
  - 结果一致，鉴权通过，返回文件。
  - 结果不一致，鉴权失败，返回HTTP 403错误。

HashValue是通过以下字符串计算出来的：

```
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

您可以通过以下示例说明更好地理解鉴权方式A的实现。

1. 通过req_auth请求对象。

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

2. 设置密钥为：aliyuncdnexp1234（您可以自行配置）。
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") = 80cd3862d699b7118eed99103f2a3a4f
```

6. 请求时url为：

```
http://cdn.example.com/video/standard/1K.html?auth_key=1444435200-0-
0-80cd3862d699b7118eed99103f2a3a4f
```

如果计算出的HashValue与您请求中带

的md5hash=80cd3862d699b7118eed99103f2a3a4f值一致，则鉴权通过。

鉴权方式B和鉴权方式C具体原理和示例，请参见鉴权方式B、鉴权方式C。

4.8.4 鉴权方式B

阿里云CDN鉴权功能为您提供了三种方式，本文档为您介绍了鉴权方式B的原理并用示例说明。鉴权功能主要用于保护用户站点的内容资源不被非法站点下载盗用。

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是：

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

鉴权字段描述

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。
PrivateKey	您设定的鉴权密钥。

字段	描述
Filename	实际回源访问的URL，鉴权时Filename需以/开头。

示例说明

您可以通过以下示例说明更好地理解鉴权方式B的实现。

1. 回源请求对象：

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

2. 密钥设为：aliyuncdnexp1234 (您自行设置)。
3. 访问源服务器时间为 201508150800（格式为： YYYYMMDDHHMM）。
4. CDN服务器会构造一个用于计算Hashvalue的签名字符串。

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

5. 服务器根据该签名字符串计算md5hash。

```
md5hash = md5sum("aliyuncdnexp1234201508150800/4/44/44c0909bcf
c20a01afaf256ca99a8b8b.mp3") = 9044548ef1527deadafa49a890a377f0
```

6. 请求url为：

```
http://cdn.example.com/201508150800/9044548ef1527deadafa49a890a377f0
/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3
```

如果计算出来的md5hash与您请求中带的md5hash

值（9044548ef1527deadafa49a890a377f0 ）一致，鉴权通过。

鉴权方式A和鉴权方式C具体原理和示例，请参见鉴权方式A、鉴权方式C。

4.8.5 鉴权方式C

本文为您介绍了鉴权方式C的原理并用示例说明。

原理说明

访问加密URL格式有如下两种格式。

- 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

字段	描述
PrivateKey	您设定的鉴权密钥。
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。
DomainName	CDN站点的域名。

示例说明

- PrivateKey取值：`aliyuncdnexp1234`。
- FileName取值：`/test.flv`。
- timestamp取值：`55CE8100`。

- md5hash计算值为：

```
md5hash = md5sum(aliyuncdnexp1234/test.flv55CE8100) = a37fa50a5f
b8f71214b1e7c95ec7a1bd
```

- 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=a37fa50a5fb8f71214b1
e7c95ec7a1bd&KEY2=55CE8100
```

当您使用加密URL访问加速节点，CDN服务器先把加密串1提取出来，并得到原始的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中所带的明文时间相减，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，视作合法请求，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，该鉴权失效。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。

4.8.6 鉴权代码示例

通过本文档中的Demo，结合您的业务需要，您可以方便地对URL进行鉴权处理。URL鉴权规则请查阅鉴权配置。

Python版本

以下Python Demo包含三种鉴权方式：鉴权方式A、鉴权方式B、鉴权方式C，它们分别描述了三种不同鉴权方式的请求URL构成和哈希字符串构成。

> 说明:
> 如果URL中包含中文，请进行urlencod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()
```

4.8.7 配置IP黑/白名单

本文为您介绍了如何配置IP黑/白名单。通过配置IP黑名单功能，您可以添加IP到黑名单，从而使该IP无法访问当前加速域名。通过配置IP白名单功能，您可以添加IP到白名单，则只有该IP能够访问当前加速域名。

背景信息

说明:

- 如果您的IP被加入黑名单，则该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，所以CDN日志中仍会记录这些黑名单中的IP的请求记录。
- IP黑/白名单支持IP网段添加。例如：127.0.0.1/24，24表示采用子网掩码中的前24位为有效位，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127.0.0.1/24表示IP网段范围是：127.0.0.1~127.0.0.255。

操作步骤

1. 登录CDN控制台。
2. 进入域名管理页面，选择需要设置的域名，单击管理。
3. 选择访问控制 > IP黑/白名单，单击修改配置。

4. 单击黑名单或白名单，在规则框内输入您想要添加的网段，然后单击确认。

4.8.8 UsageAgent黑/白名单

本文为您介绍了UsageAgent黑/白名单原理、使用场景和控制台操作步骤。您可以配置UsageAgent黑/白名单功能，CDN节点服务器会根据您请求的Usage-Agent字段进行黑白名单的管理。

背景信息

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

> 说明:
>
> - User-Agent规则不区分大小写，且支持 `*`通配符。例如：`*curl*|*IE*|*chrome*|*firefox*` ，多个值用|分割。
> - 黑白名单互斥，只支持同时启用其中一个名单。

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. 在您需要设置的域名，单击管理。
4. 在左侧导航栏，单击访问控制。
5. 在UserAgent黑/白名单区域框中，单击修改配置。
6. 根据您的需求配置黑白名单的规则，单击确定。

4.9 性能优化设置

4.9.1 页面优化

本文为您介绍了页面优化功能及如何开启该功能，方便您更好的体验CDN服务。

背景信息

开启页面优化功能，系统将自动删除html中的注释以及重复的空白符，这样可以有效地去除页面的冗余内容，减小文件体积，提高加速分发效率。

> **注意:**
> 系统进行页面压缩优化时，文件的md5值会更改，导致得到的文件的md5值和源站文件的md5值不一致，如果您的源站文件自身有md5校验机制，请勿开启页面优化功能。

操作步骤

1. 登录CDN控制台。
2. 进入域名管理页面，选择您需要设置的域名，单击管理。
3. 在左侧导航栏，单击性能优化。
4. 在页面优化区域框中，打开页面优化开关。

4.9.2 智能压缩

开启智能压缩功能后，您可以对大多数静态文件进行压缩。通过智能gzip压缩方式，有效减少传输内容大小，加速分发效果。

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。
- 适用业务类型：所有。

- 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`Conetnt-Encoding: gzip`：服务端响应的内容为gzip压缩的资源 。

> 注意：
> - 进行页面压缩优化时，文件的md5值会更改，导致得到的文件的md5值和源站文件的md5值不一致。如果您的源站文件自身有md5校验机制，请勿开启此功能。
> - 源站的相应内容大小要超过1024B，才会进行gzip压缩。
> - Internet Explorer6对gzip的兼容性较差，如果有Internet Explorer6的访问需求，不建议开启gzip压缩功能。

操作步骤

1. 登录控制台。
2. 进入域名管理页面，选择您需要设置的域名，单击管理。
3. 在性能优化 > 智能压缩区域框中，打开智能压缩开关。

4.9.3 Brotli压缩

本文档为您介绍了Brotli压缩功能及开通步骤。开启Brotli压缩功能，可以有效减少传输内容大小，加速分发效果。

背景信息

Brotli是开源的一种新型压缩算法。开启该功能后，CDN节点返回请求的资源时，会对html、js、css等文本文件进行Brotli压缩。在文本文件资源下载方面会比Gzip性能提升约15~25%。当您需要对静态文本文件进行优化压缩，可以开启此功能。

- 当客户端的请求携带请求头`Accept-Encoding: br`时表示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`Conetnt-Encoding: br`时表示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，且客户端`Accept-Encoding`请求头同时带`br`和`gzip`时，CDN节点将优先选择Brotli压缩。

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. 在您需要设置的域名，单击管理。
4. 在左侧导航栏，单击性能优化。
5. 在Brotli压缩区域框中，打开开关。

4.9.4 过滤参数

本文档为您介绍了过滤参数功能及操作步骤。过滤参数是指在请求URL中，如果携带`?`和参数，例如：`http://alibaba.com/content?a=10`，CDN节点在收到请求URL后判断是否将该带参数的URL返回源站。

背景信息

- 开启过滤参数，请求URL到CDN节点后会截取到没有参数的请求URL，且CDN节点仅保留一份副本。
  - 由于大部分Http请求中包含参数，但往往参数内容优先级不高，可以忽略参数浏览文件，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，推荐您设置为保留过滤参数。您可以设置最多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。
- 关闭过滤参数，则每个不同的URL都缓存不同的副本在CDN的节点上。

过滤参数包括保留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，多个参数逗号隔开，未指定的参数将不会被保留。
- 忽略参数：删除指定的参数，多个参数之间用空格隔开，剩余参数将不会被忽略。

适用业务类型：所有。

说明:

URL鉴权功能的优先级高于过滤参数。由于A类型鉴权信息包含在http请求的参数部分，所以系统会先进行鉴权判断，鉴权通过后在CDN节点缓存一份副本。配置URL鉴权，请参见配置URL鉴权。

操作步骤

1. 登录CDN控制台。
2. 进入域名管理页面，选择需要设置的域名，单击管理。
3. 进入性能优化，在过滤参数区域框中，单击修改配置。您可以打开或关闭过滤参数开关，并设置保留参数或忽略参数。

4. 单击确认，过滤参数功能设置成功。

示例说明：

`http://www.abc.com/a.jpg?x=1`请求URL到CDN节点。

- 开启保留过滤参数功能：
  a. CDN节点向源站发起请求`http://www.abc.com/a.jpg`（忽略参数x=1）。
  b. 源站响应该请求内容后，响应到达CDN节点。
  c. CDN节点会保留一份副本，然后继续向终端响应 `http://www.abc.com/a.jpg` 的内容。
  d. 所有类似的请求`http://www.abc.com/a.jpg?`参数均响应CDN副本`http://www.abc.com/a.jpg` 的内容。
- 关闭保留过滤参数功能：`http://www.abc.com/a.jpg?x=1`和`http://www.abc.com/a.jpg?x=2`会响应不同参数源站的响应内容。

4.10 高级设置

4.10.1 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非日常消费。域名下线后，您可以在控制台重新启动该域名。通过本文，您可以快速了解如何开通带宽封顶功能。

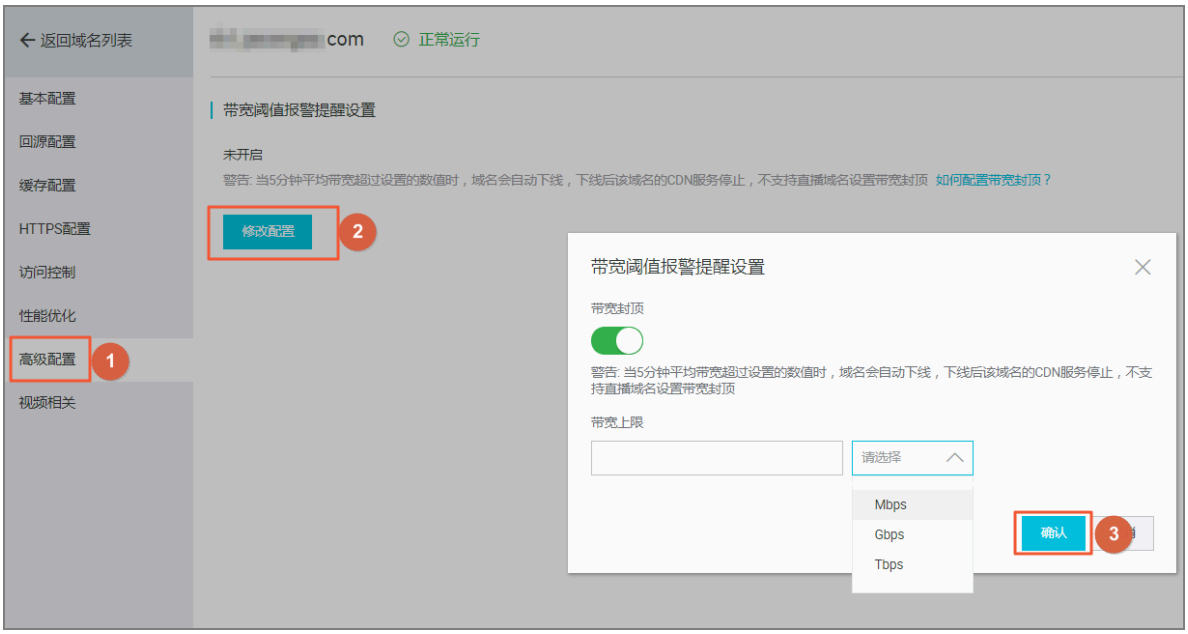
背景信息

注意:

- 如果RAM子账号要开通带宽封顶功能，需要您在RAM控制台新增系统权限策略AliyunCloudMonitorFullAccess。
- 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触发下线，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。

操作步骤

1. 登录CDN控制台。
2. 进入域名管理页面，选择需要设置的域名，单击管理。
3. 进入高级设置页面，在带宽封顶区域框，单击修改配置。
4. 打开带宽封顶开关。
5. 输入带宽上限值，并选择单位Mbps、Gbps、Tbps。然后单击确认。



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。

4.11 视频相关配置

4.11.1 Range回源

本文为您介绍了Range回源的相关信息及如何开启Range回源功能。Range回源是指客户端通知源站服务器只返回部分内容以及部分内容的范围，这有利于较大文件的分发加速。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。

背景信息

Range回源	具体描述	示例
开启	参数可以请求回源站。源站需要依据Range的参数，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。	客户端向CDN请求中含有`range:0-100`，则源站端收到的请求中也会含有`range:0-100`，并且源站响应给CDN节点，然后CDN节点响应给客户端字节内容是0-100这个范围，一共101个字节。
关闭	CDN上层节点会向源站请求全部的文件，由于客户端会在收到Range定义的字节后自动断开http链接，请求的文件没有缓存到CDN节点上，最终导致缓存的命中率较低，并且回源流量较大。	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。源站响应给CDN节点完整文件，但是CDN节点响应给客户端的就是101个字节，由于连接断开了，会导致该文件没有缓存到CDN节点上。

说明:

- 需要源站支持Range请求，即对于http请求头中包含Range字段，源站能够响应正确的206文件分片。
- Range回源是可选配置项，默认不开启。您可以变更配置，开启Range回源。

操作步骤

1. 登录*CDN*控制台。
2. 进入CDN域名管理页面，选择域名，单击管理。
3. 进入视频相关页面，在Range回源区域框，单击修改配置。

4. 选择 开启、关闭或强制，单击确认。

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。

您还可以通过调用API使用该功能，详情请参见*SetRangeConfig*。

4.11.2 拖拽播放

本文为您介绍了拖曳播放功能及如何开启该功能，通过开启该功能，可降低回源率，加快分发速度。

背景信息

拖拽播放功能是指在视频点播场景中，如果您拖拽播放进度时，客户端会向服务器端发送类似`http://www.aliyun.com/test.flv?start=10`的URL请求，服务器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。

注意:

- 需要源站支持Range请求，即如果Http请求头中包含Range字段，源站需要能够响应正确的206文件分片，详情请参见*Range回源*。
- 支持文件格式:
  - MP4。
  - FLV（FLV只支持音频为aac且视频为avc的编码格式）。

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参数表示的是时间，单位是s，支持小数以表示ms（如start=1.01，表示开始时间是1.01s），CDN会定位到start所表示时间的前一个关键帧（如果当前start不是关键帧）。	请求http://domain/video.mp4?start=10就是从第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参数所表示的字节的前一个关键帧（如果start当前不是关键帧）。	对于http://domain/video.flv，请求http://domain/video.flv?start=10就是从第10字节的前一个关键帧（如果start=10不是关键帧所在位置）开始播放视频。

操作步骤

1. 登录CDN控制台。
2. 进入域名管理页面，选择您需要设置的域名，单击配置。
3. 进入视频相关页面，在拖曳播放区域框中，开启该功能。

5 数据监控

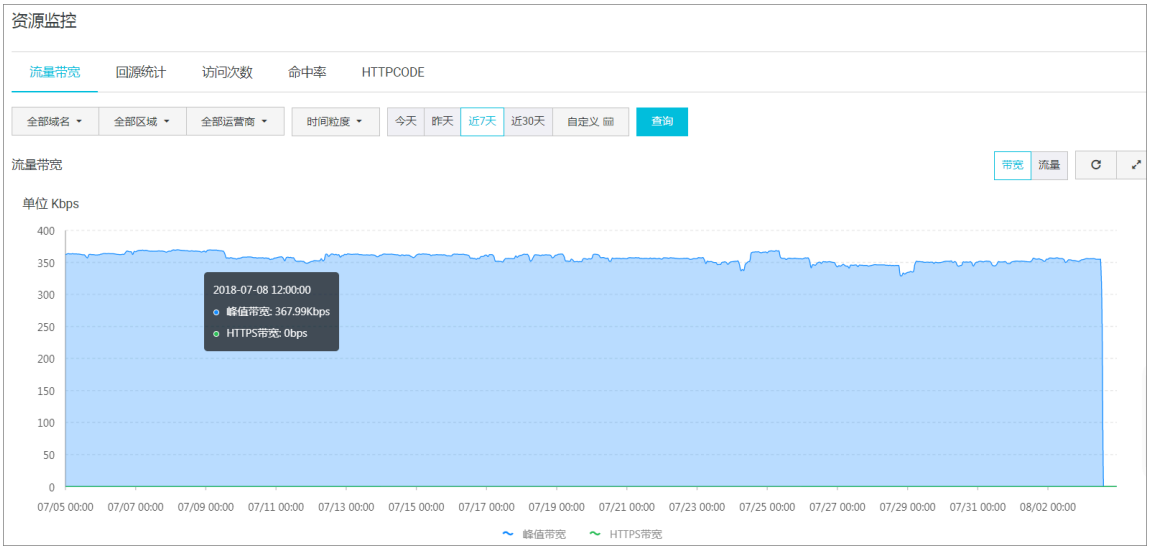
数据监控主要包括资源监控和实时监控。通过数据监控功能，您可以了解CDN的运行情况。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，选择数据监控 > 资源监控或实时监控。
3. 您可以在资源监控或实时监控页面，选择您想要查看的监控项和指标，单击查询。

   · 资源监控

   您可以选择想监控的域名、区域、运营商、时间粒度（1分钟、5分钟、1小时）以及想查询的时间段（今天、昨天、近7天、近30天或自定义），查看以下各监控项各指标的具体情况：



监控项	监控指标
流量带宽	带宽、流量。
回源统计	回源带宽、回源流量。
访问次数	请求次数、QPS。
命中率	无。

监控项	监控指标
HTTPCODE	5xx、4xx、3xx、2xx。

资源监控部分的曲线图数据和计费数据有一定差别。例如30天统计曲线取点粒度为14400s，计费数据粒度则为300s，故曲线图会忽略掉其中的一些计量点作图，主要用作带宽趋势描述。精确粒度的计费数据则主要用于您使用带宽的依据。

- 实时监控

您可以选择想监控的域名、区域、运营商以及想查询的时间段（1小时实时、近6小时、近12小时或自定义），查看以下监控维度下各监控指标的具体情况：

监控项	监控指标
基础数据	带宽、流量、请求次数、QPS。
回源流量	回源流量、回源带宽。
质量监控	请求命中率、字节命中率、5xx状态码、4xx状态码、3xx状态码、2xx状态码。

6 统计分析

通过统计分析功能，您可以查看昨天及之前的离线分析数据。

背景信息

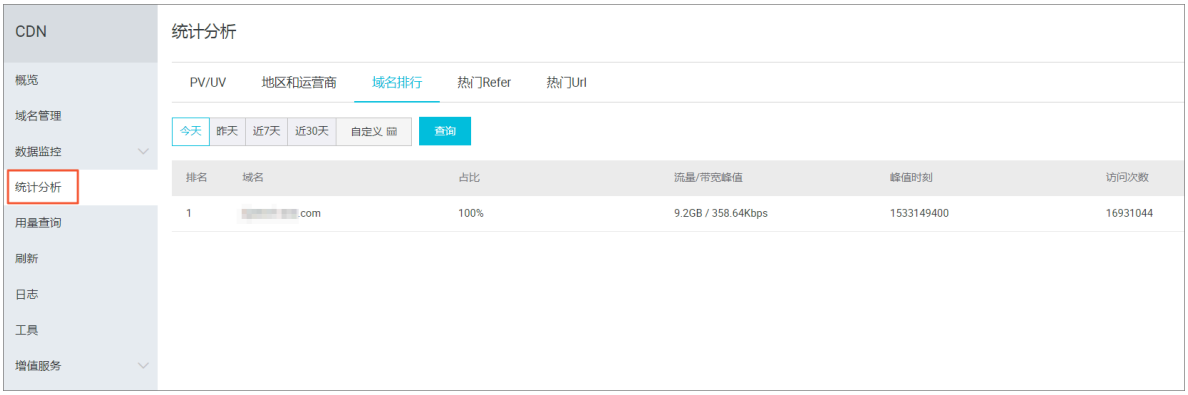
统计分析包含五个部分：PV和UV、地区和运营商、域名排名、热门Refer、热门URL。您可以导出原始详细数据，如网络带宽、流量、域名按流量占比排名以及访客区域、运营商分布等。

> 说明:
> 原始数据采集粒度随时间段变化，日维度导出数据，粒度为300s；周维度导出数据，粒度为3600s；月维度导出数据，粒度为14400s 。

项目	监控指标	可选时间
PV和UV	PV、UV、用户区域分布、运营商占比。	昨天、7 天内、30 天、自定义（90天内）。
地区和运营商	排名、区域、总流量、流量占比、访问次数、访问占比、响应时间。	昨天、7 天内、30 天、自定义（90天内）。
域名排名	各个加速域名的访问排名。	昨天、7 天内、30 天、自定义（90天内）。
热门Refer	流量、流量占比、访问次数、访问占比。	支持查看单日数据、自定义（90天内）。
热门URL	流量、流量占比、访问次数、访问占比。	支持查看单日数据、自定义（90天内）。

操作步骤

1. 登录CDN控制台。
2. 在统计分析页面，选择您想要查看的监控项和指标，单击查询。



7 用量查询

7.1 用量查询

本文档为您介绍了用量查询的功能介绍和控制台操作步骤。您可以根据您的需求来查询某段时间的用量数据，根据不同的数据来帮助您更好地进行业务决策。

背景信息

如果您希望查询并获取到某一段时间内的实际用量数据，可以使用用量查询功能。

您可以通过设置下列不同条件，按照不同维度查询您所需要的数据。

- 不同的域名和用户。
- 流量、带宽、请求数。
- 不同计费大区。详细计费请参见计费大区划分。

说明:

您可以自定义时间段进行查询。上线后，您可以查询最多3个月的数据。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏单击用量查询。

3. 在用量查询区域框中，您可以根据需求，选择不同的维度查询用量，例如：流量带宽、请求数、域名、查询时间、地域，然后单击查询。

说明:

如果您需要导出账单或明细，请参见账单导出或明细导出。

7.2 账单导出

本文档为您介绍了账单导出的功能介绍和控制台操作步骤，帮助您了解自己的用量，及时对业务进行决策。

背景信息

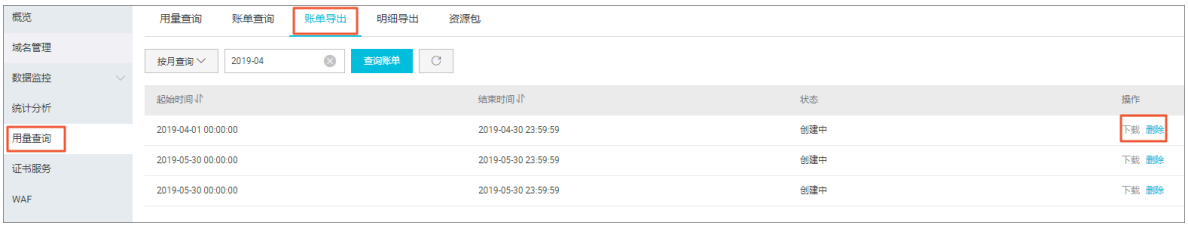
您可以按日计费或按月计费导出实际用量数据，以便于与费用中心的出账用量进行比对。

- 您只能按账户维度导出。
- 您只能导出某一天或者某个整月的数据。
- 导出数据格式：PDF。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏单击用量查询。

3. 在账单导出区域框中，根据您的需求选择按日查询或者按月查询，然后单击查询账单。您可以对账单进行下载和删除操作。



说明:

如果您想通过账单了解更多，请参见明细导出。

7.3 明细导出

本文档为您介绍了明细导出的功能介绍和控制台操作步骤，帮助您了解自己的用量，及时对业务进行决策。

背景信息

通过明细导出功能，您可以导出流量带宽和请求数的5分钟明细数据，便于您通过明细来核对或计算实际消费的计量数。您可以通过设置下列不同条件，按照不同维度查询您所需要的数据。

- 流量带宽、请求数。
- 账户、资源组、域名。

说明:

- 导出的时间段不可以重复。
- 您在导出资源组时，会将资源组下所有域名也一并导出。支持最多可以导出100个域名，超过100时，只保留资源组明细。
- 导出的所有数据，均为每五分钟一个点。
- 下载的数据格式：CSV。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏单击用量查询。
3. 在账单导出区域框，单击创建导出任务。

4. 根据您的需求，填写任务名称，选择导出对账类型、查询时间、导出内容、导出频次，然后单击确认。创建导出任务成功。

8 CDN WAF防护功能

本文档介绍了阿里云CDN的WAF防护功能及其使用场景。目前CDN的WAF功能正在公测。

功能介绍

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。

云盾Web应用防火墙基于云安全大数据能力，用于防御SQL注入、XSS跨站脚本、常见Web服务器插件漏洞、木马上传、非授权核心资源访问等OWASP常见攻击，并过滤海量恶意CC攻击，避免您的网站资产数据泄露，保障网站的安全与可用性。关于具体的WAF功能，请参见什么是Web应用防火墙。

适用场景

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。

操作步骤

目前阿里云CDN的WAF功能属于公测阶段，您暂时无法自动在控制台开启WAF功能。（仅支持开启后自动关闭WAF功能）

您可以扫下图二维码加入CDN WAF钉钉讨论群或提工单，我们在了解您的需求后，会为您进行WAF配置。

费用说明

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。

公测期间，请求数按每小时计算。WAF的计费规则如下：

每小时请求数	费用
1-20000	0.4元（固定付费）
20001-500000	0.2元/万次请求
500001-5000000	0.18元/万次请求
大于5000000	0.15元/万次请求

计费案例：以用户A和用户B分别在2019年2月28日10:20开通了2个域名的CDN WAF功能为例，他们产生的费用如下表所示：

用户	10：20-11：20 产生请求次数	11：21分收到账单金额（元）
A	15000	0.4
B	350000	7 （350000/10000*0.2）

9 刷新预热

9.1 概述

本文档为您介绍了阿里云CDN刷新预热功能的原理、任务生效时间及请求说明，目前阿里云CDN支持URL刷新、目录刷新、URL预热三种方式。

- 刷新：提交URL刷新或目录刷新请求后，CDN节点的缓存内容将会被强制过期。当您向CDN节点请求资源时，CDN会直接回源站拉取对应的资源返回给您，并将其缓存。
- 预热：提交URL预热请求后，源站将会主动将对应的资源缓存到CDN节点。当您首次请求时，就能直接从CDN节点缓存中获取到最新的请求资源，无需再回源站拉取。

URL刷新

原理：通过提供目录下文件的方式，强制CDN节点回源拉取最新的文件。

任务生效时间：5分钟内生效。

> 说明：
>
> - 同一个ID每天最多提交2000个刷新请求，每次请求最多只能提交1000条URL刷新。
> - 输入的URL，需以`http://`或者`https://`开始，以/结束。

提供批量刷新缓存的接口，详情请参见*RefreshObjectCaches*。

目录刷新

原理：通过提供目录及目录下所有文件的方式，强制CDN节点回源拉取最新的文件。

任务生效时间：5分钟内生效。

> 说明：
>
> - 同一个ID每天最多提交100个刷新请求，可一次性全部提交。
> - 输入的URL，需以`http://`或者`https://`开始，以/结束。

提供批量刷新缓存的接口，详情请参见*RefreshObjectCaches*。

URL预热

原理：将指定的内容主动预热到CDN的L2节点上，用户首次访问即可直接命中缓存，降低源站压力。

任务生效时间：预热是CDN节点主动访问您的源站获取资源，因此预热完成的时间取决于文件的大小和源站的网络情况。

说明:

- 同一个ID每天最多只能预热共500个URL，每次请求最多只能提交100条URL预热。
- 输入的URL必须带有`http://`或`https://`。
- 资源预热完成时间将取决于用户提交预热文件的数量、文件大小、源站带宽情况、网络状况等诸多因素。

提供批量预热资源的接口，详情请参见。*PushObjectCache*。

9.2 配置刷新预热

本文档为您介绍了阿里云CDN刷新预热功能和控制台的操作步骤。CDN节点的缓存内容不实时更新，只有当缓存内容到期后才能回源拉取最新的内容您在源站上更新资源后，如果希望访问不再获取旧资源，直接获取新资源，您可以使用URL刷新或目录刷新功能。如果希望CDN预先将资源由源站主动缓存至CDN节点，则可以使用URL预热功能。

背景信息

阿里云CDN刷新预热支持URL刷新、目录刷新、URL预热三种方式，详情请参见概述。

操作步骤

1. 登录*CDN控制台*。
2. 在左侧导航栏，单击刷新。

3. 根据您的需求，选择操作类型和刷新类型，填写URL，然后单击提交。

说明:

当你需要刷新或预热多条请求，请您按照一行一个URL进行输入。

4. 您可以在操作记录页面，填写查询时间和查询域名，选择操作类型，单击查询。这样您可以查看资源刷新或预热的进度。

说明:

阿里云CDN提供查询进度的API，详情请参见*DescribeRefreshTasks* 。

10 日志管理

10.1 日志下载

本文档为您介绍了日志下载功能的使用说明、字段格式说明和操作步骤。通过日志下载功能，您可以查看对应域名的相关日志。

背景信息

使用说明

- 日志文件延迟时间：非高峰时段延迟4小时，高峰时段延迟4-8小时。您可以在日志管理模块查询到4小时之前的日志文件。
- 日志每隔一小时生成一次。具体分割成的文件数量根据该生成小时的日志量，动态调整。
- 您可以下载最近一个月的日志数据。
- 日志命名规则：加速域名_年_月_日_时间开始_时间结束。例如：www.test.com_2018_10_30_000000_010000.gz

字段格式说明

- 示例日志：

```
[9/Jun/2015:01:58:09 +0800] 188.165.15.75 - 1542 "-" "GET http://www.aliyun.com/index.html" 200 191 2830 MISS "Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)" "text/html"
```

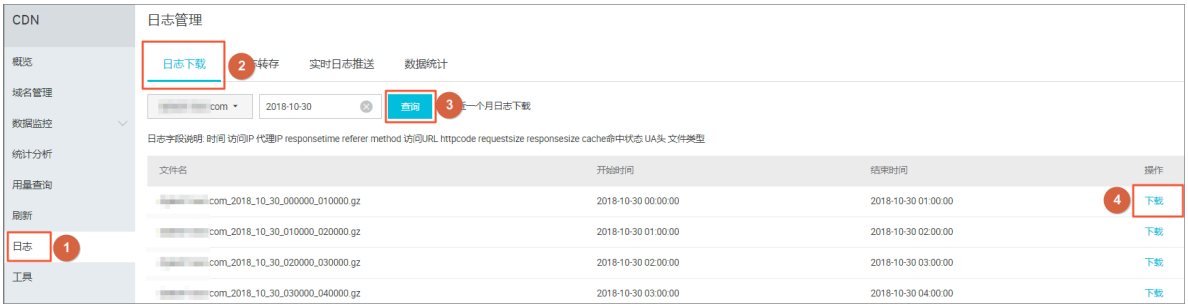
- 字段含义：

字段	描述
[9/Jun/2015:01:58:09 +0800]	时间
188.165.15.75	访问IP
-	代理IP
1542	responsetime(单位：ms)
"-"	referer
GET	method
http://www.aliyun.com/index.html	访问url
200	httpcode
191	requestsize(单位：byte)
2830	responsesize(单位：byte)

字段	描述
MISS	cache命中状态
Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)	UA头
text/html	文件类型

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击日志。
3. 在日志下载页面下，选择域名和查询时间，单击查询。
4. 在您需要查看的日志右侧，单击下载。



10.2 日志转存

日志转存是阿里云CDN配合函数计算，共同推出的一项日志服务，可以帮助您将日志存储更长的时间，便于您基于长时间的日志做出自定义的数据分析。这将有助于您更好地了解您CDN的服务质量，以及您的终端客户的访问详情，提高您的业务决策能力。

前提条件

CDN的日志转存服务搭载函数计算来实现转存。使用日志转存服务时，您需要开通函数计算服务。授权CDN后，CDN会帮您一键创建函数计算服务来实现日志转存。此外，您也可以登录函数计算控制台，通过已有的函数计算服务来完成日志转存的服务。

背景信息

- 目前CDN的离线日志服务，只能默认提供1个月的存储时间。如果您有更长时间的存储需求，可以将日志转存至OSS，方便您根据实际情况对日志进行保存和分析。

- 计费： CDN不收取任何日志转存费用。当您通过函数计算完成日志转存时，会消耗函数计算的计算资源，因此函数计算会收取非常低廉合理的费用，函数计算每月也提供一定免费使用额度。具体价格，请参见函数计算计费方式。

  计费： CDN不收取任何日志转存费用。当您通过函数计算完成日志转存时，会消耗函数计算的计算资源，因此函数计算会收取非常低廉合理的费用，函数计算每月也提供一定免费使用额度。具体价格，请参见函数计算计费方式。
- CDN和函数计算无缝集成，使您可以为CDN的各种事件设置处理函数，并通过事件中的域名等参数进行过滤，只接收自己感兴趣的域名的数据。当CDN系统捕获到指定类型的、满足过滤条件的事件后，会自动调用函数处理。
- 函数计算已经支持了多种CDN的场景，包括：日志转存、刷新预热、资源封禁、域名添加和删除、域名启用和停用。触发这些场景的具体方式，请参见CDN事件触发器。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击日志。
3. 在日志转存页面，单击创建日志转存。
4. 在授权与创建区域框，根据你的需求，填写服务名称，选择OSS Bucket，然后单击下一步。

5. 单击点击授权，并选择域名关联函数服务。然后单击创建。

6. 单击完成。您的日志转存功能配置完成。

10.3 实时日志推送

10.3.1 概述

本文档为您介绍了实时日志的功能介绍、使用优势、计费详情和适用场景。

什么是实时日志

在借助CDN访问各种的图片，文字或者视频资源时，CDN会产生大量的日志数据，这些日志数据CDN会进行实时的采集。阿里云CDN通过与日志服务（SLS）的融合，将采集的实时日志实时推送至日志服务进行日志分析。通过日志的实时分析，您可以快速发现和定位问题，通过对日志数据的挖掘，提高数据的决策能力，将您的业务推向一个新的高度。

CDN提供的实时日志服务与日志下载的区别

- CDN实时日志为实时采集的日志数据，日志数据延迟不超过3分钟。同时，CDN打通了日志服务分析的能力，为您定制4张分析报表，帮助您快速对日志进行分析，发现问题，及时决策。
- 通过CDN提供的离线日志下载，您可以下载4小时前的每小时日志数据。

实时日志服务的优势

- 传统的日志分析模式，需要您将日志下载后，重新上传至数据仓库，在数据仓库进行一系列的清洗和数据模型定义后，再进数据分析，这个过程需要维护的人力较多，时间较长。
- 实时日志延时小（秒级延时），可以帮助您快速的了解到CDN的访问详情，开通服务后，CDN将日志数据自动投递到日志服务(SLS)，免去繁琐的传统日志分析的流程，实时查看日志分析结果。

计费详情

您需要按照实时日志推送成功条数，每万条0.06元进行付费，该费用已经包含日志服务分析的费用。因此，在一定使用边界内，您无需支付任何的日志服务费用。

但是在以下情况下，您还需要支付日志服务的费用：

- 日志存储超过7天的存储部分，由日志服务单独收费。
- 日志服务的外网读写费用。

关于日志服务收费，请参见价格详情。

适用场景

实时日志可以帮助您分析加速域名遇到的异常问题，也可以帮助您了解您的用户的访问情况。当前阿里云CDN提供4类日志数据报表如下表所示。

数据种类	描述
基础数据	帮助您了解CDN网络的访问性能。通过分析该数据您可以快速了解到CDN整体的服务质量以及终端用户的访问效率，同时也可以根据突发的异常情况及时的进行处理。
错误码数据	帮助您在加速域名访问出现异常时，快速定位到CDN服务本身出现的访问问题。例如：源站访问出现故障、节点不可用、终端用户的网络故障，地域特性问题。
热门资源数据	帮助您了解业务详情，分析出热门的访问地区，热门资源。您也可以从热门数据了解到您的运营活动效果是否正常、热点时间内的流量、下载的上涨是否符合预期需求，帮助您及时调整运营策略。
用户分析	帮助您更好的了解您的用户构成，包括用户的热门访问省份、热门终端、热门用户等。

如果您想开通实时日志推送服务，请参见配置实时日志推送。

10.3.2 配置实时日志推送

本文档为您介绍了实时日志推送在控制台的操作步骤，通过创建实时日志推送服务，可您以快速对日志进行分析，发现问题，及时决策。

前提条件

使用该服务前，您首先需要开通日志服务。

操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击日志。
3. 在实时日志推送界面，单击创建实时日志推送服务。
4. 配置Project名称、Logstore名称（可选）、地区，单击下一步。

5. 选择关联域名并绑定，然后单击创建。

说明:

- 迁移域名：A域名的数据需要从logstore1推送至logstore2，迁移未成功前，A数据会一直推送至logstore1，成功后直接推logstore2，中间的数据不会中断。
- 服务暂停和启用：logstore和域名的关联关系保留，但是您可以停止或者开启数据的推送，可以对logstore或某个域名进行暂停。
- 查询数据：可以查询您某一段时间内，某个用户总数据或某个logstore的推送数据。
- CDN实时日志推送列表展示的内容，只包含logstore和CDN域名管理的logstore，不展示用户账号下的所有logstore。
- 关联域名时，一次性可以最多绑定5个域名。
- 数据推送至logstore后，您可以直接查看4张报表，通过CDN打开查看报表可以默认查看。

如果阿里云CDN提供的数据报表不能满足您的需求，您可以在日志服务控制台进行自定义报表进行分析，您也可以提交工单，我们将根据您的意见提供更好的日志分析报表。

- 关于CDN实时日志的发布讯息，请参见实时日志发布。
- 关于CDN实时日志的更多信息，请参见CDN实时日志的前世今生。

11 诊断工具

本文档为您介绍了诊断工具IP检测的使用场景及操作步骤。当您需要验证指定的IP是否为阿里云CDN节点的IP地址时，可以通过该功能进行检测。

操作步骤

1. 登录*CDN*控制台。
2. 在左侧导航栏，单击工具。
3. 输入您想检测的IP地址，单击检测。

12 增值服务

12.1 图片鉴黄

图片鉴黄是CDN加速的一项增值服务，基于云计算平台，能对海量数据进行快速检测，可以帮助用户节省90%以上的人力成本。开通图片鉴黄功能后，系统会自动检测通过CDN加速的图片是否涉黄，违规图片的URL将会被记录下来供您导出和删除。

背景信息

产品定价

CDN图片鉴黄按照扫描张数计费，以回源的图片作为检测基数，同一条图片URL只会被检测一次，不会重复计费，同时您还可以设置每日检测张数的上限，控制消费额度。

- CDN图片鉴黄计费规则：
  - 计费周期为1天1次。
  - 按照当日扫描量收费，每日扫描量越大，单价越低。
  - 算法确定部分和待人工确认部分按照不同的单价计费。
- 后付费模式的详细计费标准如下：

阶梯（张/日）	算法确定部分 单价（元/千张）	待人工确认部分 单价（元/千张）
>0	¥1.80	¥0.45
>5000	¥1.62	¥0.41
>50000	¥1.53	¥0.38
>130000	¥1.44	¥0.36
>260000	¥1.35	¥0.34
>850000	¥1.26	¥0.32

- 鉴黄资源包的价格如下：

鉴黄包规格	价格	对应折扣
50万张	810元	9折
300万张	4590元	8.5折
500万张	7200元	8折
1000万张	13500元	7.5折

鉴黄包规格	价格	对应折扣
1亿张	126000元	7折
5亿张	540000元	6折

- 鉴黄资源包抵扣规则：

  算法确定部分按照1：1抵扣，待人工确认部分按照1：0.25抵扣。

操作步骤

1. 登录CDN控制台。
2. 单击规则设置，设置待检测域名和限额。

   说明：
   首次进入图片鉴黄功能配置页，未设置检测域名，您需要将CDN中的域名添加到检测列表才会开始检测。

3. 在左侧选择要检测的域名，添加到右侧检测中的域名栏中，单击设置保存后，云端即开始检测通过CDN加速的新增图片。

说明:

- 首次开通服务后，第二天00:00开始检测。
- 该功能对已有的存量图片不会检测。如需检测存量图片，可以通过手动刷新缓存的方式实现，刷新缓存后，您下次通过CDN访问该图片后即会自动检测，整个检测结果会延迟3~4小时。

4. 查看统计数据及操作。配置完成后等待云端开始检测，3~4个小时后会有第一批结果出来。
   - 单击统计分析，查看检测的统计数据信息，包括今日已检测的总量、疑似色情的图片量以及判定为色情的图片量。
   - 单击图片列表，选择查询条件，筛选查看图片。

说明:

您可以在图片列表中，查看所有检测过的图片。如果图片在源站被删除，则可能会导致控制台上无法显示此图片。

- 手工打标色情图片。 由于检测系统判定无法做到100%准确率，会出现少量图片被识别成疑似色情或识别结果不对的情况，此时您可以通过手工打标的方式，将图片打标为色情或正常，您还可以同时选中多张图片批量打标。

5. 单击导出违规图片，导出涉黄图片列表，系统会将检测结果和手工打标的结果综合起来判定图片是否违规。

   您可以根据导出的列表到自己的系统中进行删除，然后刷新对应的CDN缓存。

13 CDN子账户使用指南

针对有CDN域名资源组管理需求的客户，可以通过子账户+资源组授权的方式实现不同部门之间资源的隔离操作。

操作步骤

1. 使用主账号登录企业控制台，关于企业控制台的使用请参见企业控制台使用手册。

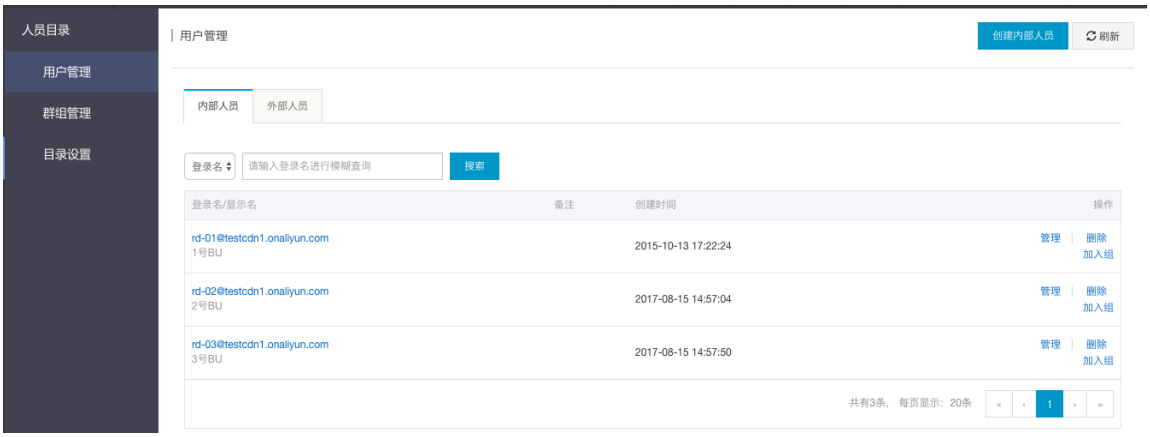
> **说明:**
> 资源组设置和子账号管理需要在企业控制台完成，设置好相应的资源组和权限后，子账号登录CDN控制台就会按照已定的规则进行有限的资源查看和操作，保证子账户间的操作和资源展示完全隔离。

2. 创建子账户。

a) 进入人员目录模块，首次进入需要创建目录，一个用户只能归属于某一个目录下。

b) 创建目录后，您可以在人员目录 > 用户管理中创建子账户。

根据业务需求，您还可以通过群组管理功能创建群组，统一管理子账户。



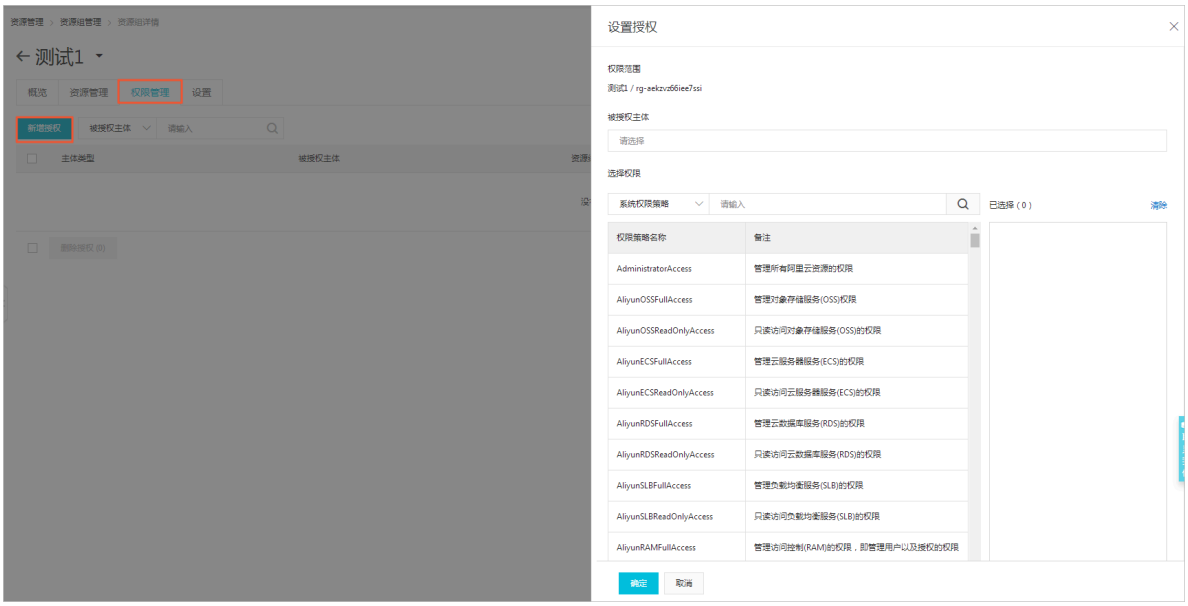
3. 创建资源组。

a) 进入资源管理模块，单击新建资源组，创建资源组测试1如下：

b) 选择需要管理的资源组，完成该组内的资源管理、权限管理和基本信息设置。

c) 单击资源管理，选择产品类型为CDN共享带宽，选择需要加入该资源组的加速域名，单击转入资源，完成资源组内加速域名设置。

4. 授权。权限管理完成子账户的授权，单击新增授权，您可以选择需要管理本资源组的子账户，并完成策略授权。



当前RAM模板策略

- AliyunCDNFullAccess：CDN管理授权，支持增删查改。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "cdn:*",
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

- AliyunCDNReadOnlyAccess：CDN只读权限。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "cdn:Describe*",
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
```

```
}
```

5. 使用子账号登录CDN控制台。登录地址：*http://signin.aliyun.com/<自定义域>.onaliyun.com/login.htm*

   子账户登录后，可以选择展示当前子账户拥有权限的资源组，根据资源组罗列加速域名。

   子账户支持域名管理、监控、刷新和日志下载，其他操作同主账号完全一致，请参见快速入门。

14 设置httpDNS

功能简介

- 传统的DNS解析是通过访问运营商Local DNS获得解析结果，这种方式容易引发域名劫持、域名解析错误、流量跨网等问题， 从而导致网站无法访问或访问缓慢。
- httpDNS是域名解析服务，通过HTTP协议直接访问阿里云CDN的服务器，由于绕过了运营商的Local DNS，因此可以避免DNS劫持并获得实时精确的DNS解析结果。
- 原理： 客户端发起请求，通过HTTP协议访问阿里云CDN指定httpDNS服务端，该服务端依托遍布各地的二级DNS节点解析域名，获得域名解析结果并最终返回给客户端。

httpDNS 接口

支持通过HTTP接口直接访问，访问方式如下：

1. 服务URL：

```
http://umc.danuoyi.alicdn.com/multi_dns_resolve
```

2. 请求方法：`POST`
3. 支持参数： `client_ip=x.x.x.x` 如果使用发起httpDNS请求的客户端IP，该参数可以忽略。
4. 请求示例： 待解析的多个域名放到POST的body中，域名之间以空白分隔，空白可以是空格、TAB和换行符。

```
#curl 'http://umc.danuoyi.alicdn.com/multi_dns_resolve?client_ip=182
.92.253.16
' -d 'd.tv.taobao.com'
```

5. 返回格式： json 数据，解析后提取域名对应的ip，多个ip之间可以做轮询，需要遵循ttl进行缓存和过期。

```
{"dns":[{"host":"d.tv.taobao.com","ips":[{"ip":"115.238.23.240","
spdy":0},{"ip":"115.238.23.250","spdy":0}],"ttl":300,"port":80}],"
port":80}
```

6. 多个域名请求事例：
   - 请求示例

```
#curl 'http://umc.danuoyi.alicdn.com/multi_dns_resolve?client_ip=
182.92.253.16
' -d 'd.tv.taobao.com vmtstvcdn.alicdn.com'
```

   - 返回示例

```
{"dns":[{"host":"vmtstvcdn.alicdn.com","ips":[{"ip":"115.238.23.
250","spdy":0},{"ip":"115.238.23.240","spdy":0}],"ttl":300,"port":
80},{"host":"d.tv.taobao.com","ips":[{"ip":"115.238.23.240","spdy
```

```
":0},{"ip":"115.238.23.250","spdy":0}],"ttl":300,"port":80}],"port
":80}
```