# 阿里云
# CDN

## 用户指南

文档版本：20190318

# 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:**<br>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:**<br>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:**<br>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 新控制台说明..... 1
2 CDN功能列表.....4
3 增值服务..... 9
3.1 全站加速.....9
3.1.1 全站加速..... 9
3.1.2 动态协议跟随回源..... 9
3.1.3 特殊header头设置.....10
3.1.4 静态文件类型.....11
3.1.5 静态路径设置.....12
3.1.6 静态URI设置.....13
4 业务类型.....15
4.1 类型1：图片小文件加速..... 15
4.2 类型2：大文件下载加速..... 16
4.3 类型3：视音频点播加速..... 16
4.4 类型4：直播流媒体加速..... 17
4.5 类型5：全站加速..... 18
4.6 类型6：移动加速..... 18
5 域名管理.....19
5.1 批量复制.....19
5.2 标签管理.....25
5.3 HTTPS安全加速..... 31
5.3.1 HTTPS安全加速设置..... 32
5.3.2 证书格式说明.....37
5.3.3 强制跳转.....41
5.3.4 HTTP/2..... 43
5.3.5 TLS.....45
5.3.6 HSTS..... 46
5.4 内容回源设置.....48
5.4.1 源站设置.....48
5.4.2 私有bucket回源授权..... 51
5.4.3 协议跟随回源.....54
5.4.4 回源HOST.....54
5.4.5 回源SNI..... 57
5.5 节点缓存设置.....59
5.5.1 缓存配置.....59
5.5.2 设置HTTP响应头.....61
5.6 访问控制设置.....62

5.6.1 防盗链.....62
5.6.2 IP黑/白名单.....65
5.6.3 鉴权配置.....67
5.6.4 鉴权方式A.....69
5.6.5 鉴权方式B.....70
5.6.6 鉴权方式C.....71
5.6.7 鉴权代码示例.....73
5.7 性能优化设置.....75
5.7.1 智能压缩.....75
5.7.2 页面优化.....76
5.7.3 过滤参数.....77
5.8 视频相关配置.....78
5.8.1 Notify_URL设置.....78
5.8.2 拖拽播放.....79
5.8.3 Range回源.....81
5.9 高级设置.....82
5.9.1 带宽封顶.....82
6 数据监控.....85
7 统计分析.....89
8 用量查询.....91
8.1 用量查询.....91
8.2 账单导出.....95
8.3 明细导出.....97
9 刷新预热.....100
10 日志管理.....103
10.1 日志下载.....103
10.2 日志转存.....104
10.3 实时日志.....108
11 诊断工具.....111
12 图片鉴黄.....112
13 CDN子账户使用指南.....118
14 设置httpDNS.....123

# 1 新控制台说明

阿里云CDN新版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。本文档主要介绍阿里云CDN新版控制台界面上展示的相关功能。

## 新控制台发布说明

目前，阿里云CDN新版控制台已经发布。新版控制台新增了明细数据导出、用量查询、CDN计量账单导出等功能，方便您对数据的查询和维护。此外，新版控制台对原有操作和展示界面进行了调整和优化，让您更清楚地了解CDN服务的使用情况、更便捷地操作控制台。

## 新控制台指引

新版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，主要功能包括：域名管理、数据监控、统计分析、用量查询、刷新、日志、工具和增值服务。

| 功能 | 简述 |
| --- | --- |
| 域名管理 | 添加加速域名，删除或导出已有加速域名，并可以对加速域名基本信息和配置信息进行变更。目前包括HTTPS安全加速设置、内容回源设置、节点缓存设置、访问控制设置、性能优化设置、视频相关设置和高级设置，还新增了批量复制功能。 |
| 数据监控 | 包含资源监控和实时监控。 |
| 统计分析 | 您可以根据不同维度，查询PV和UV、地区和运营商、域名排名、热门Refer、热门URL等相关数据。 |
| 用量查询 | 您可以在该功能下查询用量、导出账单或导出明细。 |
| 刷新 | 您可以选择刷新或预热。目前刷新包含URL刷新和目录刷新两种方式；预热方式为URL预热。 |
| 日志 | 日志服务包含日志下载和日志转存两个功能。 |
| 工具 | 包含链路诊断工具、IP查询。 |
| 增值服务 | 目前的增值服务为图片鉴黄。 |

- 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

本文档简要介绍阿里云CDN新控制台的功能情况，您可以分别单击链接快速查询该功能的详细内容，进行相关基本操作。

### 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，将用户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 | 指定回源的 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。 | 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9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 | 用户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鉴权方式保护用户源站资源 | 未开启 |
| IP黑名单 | 用户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，有效减少用户传输内容的大小 | 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 |
| Notify_URL | 【直播适用】流状态实时信息回调，可以及时通知用户推流或断流操作结果 | 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。<br>· 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。 | 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 | 在借助访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，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。 | 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 增值服务

## 3.1 全站加速

### 3.1.1 全站加速

应用场景介绍

全站加速即动态加速，适用于各行业动静态内容混合、含较多动态资源请求（如asp、jsp、php等格式的文件）的站点，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。

注意:
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。

计费规则

全站加速为增值服务，计费项为“基础费用”+“请求数费用”。其中“基础费用”是根据CDN服务所选择的“按峰值带宽”或“按流量”计费的基础费用。“请求数费用”包含动态HTTP请求数、动态HTTPS请求数和静态HTTPS请求数，分别按照单价按日计费。全站加速详情参考 全站加速介绍。

### 3.1.2 动态协议跟随回源

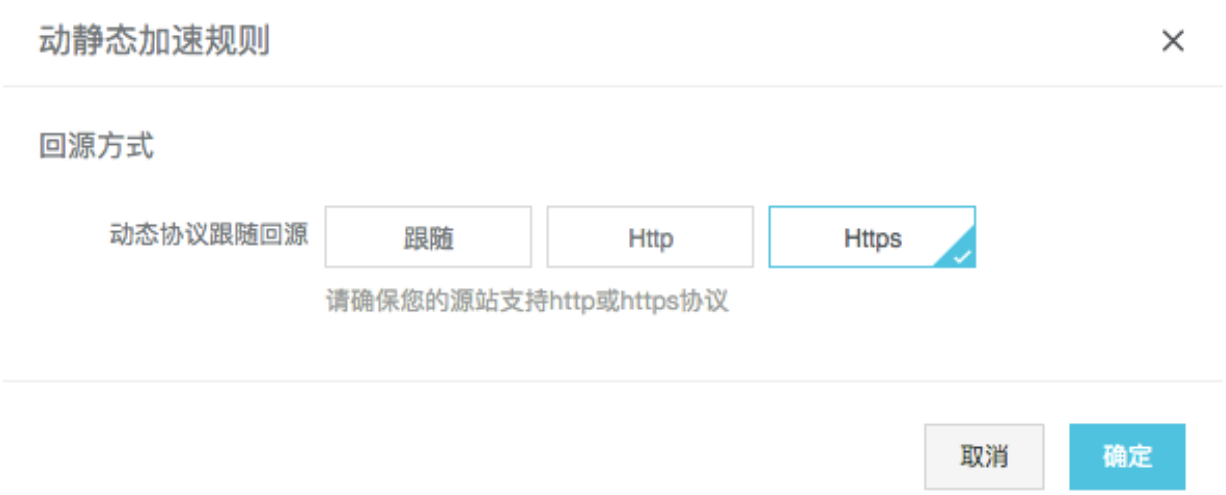
功能介绍

动态资源回源时使用协议和客户端访问资源的协议保持一致。例如，客户端以HTTP协议请求动态资源，CDN节点也会以HTTP协议回源获取资源，同理如果客户端以HTTPS协议请求动态资源，CDN节点会以HTTPS协议回源获取资源。

### 配置引导

域名管理，选择域名进入域名配置页面，设置动静态加速规则。


在动态协议跟随回源中进行选择：




**说明：**

动态协议跟随回源是针对动态资源的请求的配置，而源站设置里的协议跟随回源则是针对静态资源的请求的配置，二者有区别。

## 3.1.3 特殊header头设置

### 功能介绍

根据Header中的Cache-Control字段，选择是否动态加速。Header相应头的Cache-Control内容符合配置中任一规则就强制开启动态加速，不再检查其余配置。

### 配置引导

选择域名管理 > 域名配置页面 > 动静态加速规则设置：


选择特殊Header头设置 > 设置要强制开启动态加速的Cache-Control规则：


**说明：**

**例如：设置了规则为 no-cache，则所有响应头中的Cache-Control中带no-cache的资源都强制开启动态加速，不缓存在边缘节点上。**

## 3.1.4 静态文件类型

### 功能介绍

**全站加速默认为纯动态加速，即所有资源请求都使用动态加速，通过最优路由回源获取资源。因此静态资源也不会被边缘节点缓存。可通过配置指定静态文件的类型，以智能区分动静态资源，达到静态资源使用边缘缓存，动态资源用动态加速的最优方案**

### 配置引导

**选择域名管理 > 选择域名进入域名配置页面 > 动静态加速规则设置：**


选择静态文件类型进行配置。


勾选静态资源的文件类型，选中的资源类型将使用边缘缓存，而不用每次请求都回源获取资源。

## 3.1.5 静态路径设置

### 功能介绍

全站加速默认为纯动态加速，即所有资源请求都使用动态加速，通过最优路由回源获取资源。因此静态资源也不会被边缘节点缓存。可通过配置指定静态文件的路径，以区分动静态资源，达到静态资源使用边缘缓存，动态资源用动态加速的最优方案。

### 配置引导

选择域名管理 > 选择域名进入域名配置页面 > 动静态加速规则设置：


**选择静态路径设置，指定静态资源的路径：**


**静态路径的资源将使用边缘节点缓存，供用户就近获取，达到更好的加速效果。**

## 3.1.6 静态URI设置

### 功能介绍

**全站加速默认为纯动态加速，即所有资源请求都使用动态加速，通过最优路由回源获取资源。因此静态资源也不会被边缘节点缓存。可通过配置指定静态文件的URI，以区分动静态资源，达到静态资源使用边缘缓存，动态资源用动态加速的最优方案。**

### 配置引导

**选择域名管理 > 选择域名进入域名配置页面 > 动静态加速规则设置：**


**选择静态URI设置，指定静态URI：**


**静态URI的资源将使用静态资源加速，缓存在边缘节点上，供用户就近获取。**

# 4 业务类型

## 4.1 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。

## 4.2 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。

## 4.3 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。

## 4.4 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。

## 4.5 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。

## 4.6 类型6：移动加速

# 5 域名管理

## 5.1 批量复制

### 功能介绍

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，实现批量配置域名的效果。

> 说明:
> 您只能选择状态为正常运行的域名进行复制。

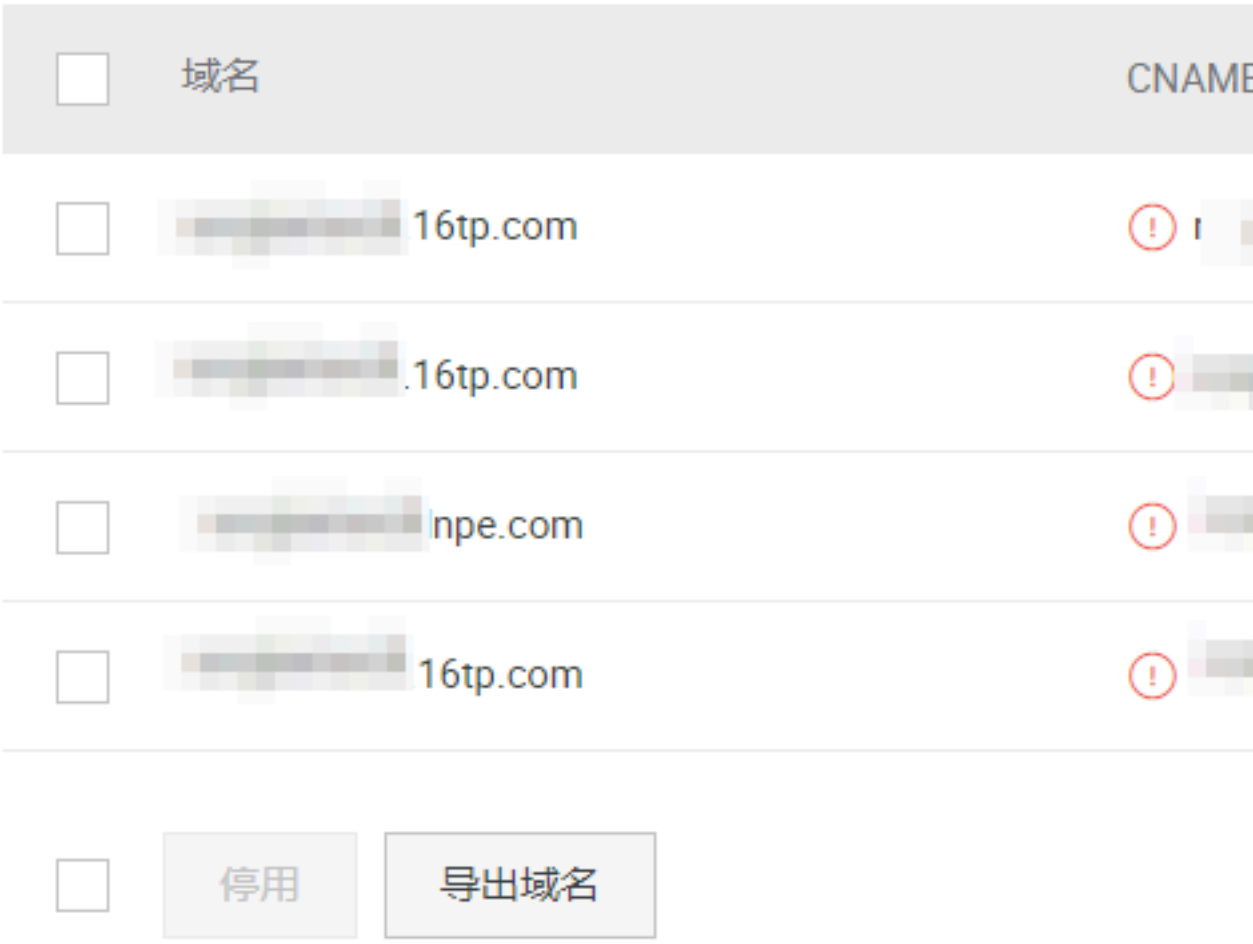
### 操作步骤

请确保您已经配置过您想复制配置的域名，否则将无法批量复制。

> 说明:
> 您无法复制HTTPS证书到其他域名，请您单独配置。

> 警告:
> 域名复制后，复制不可回退。请确认该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。

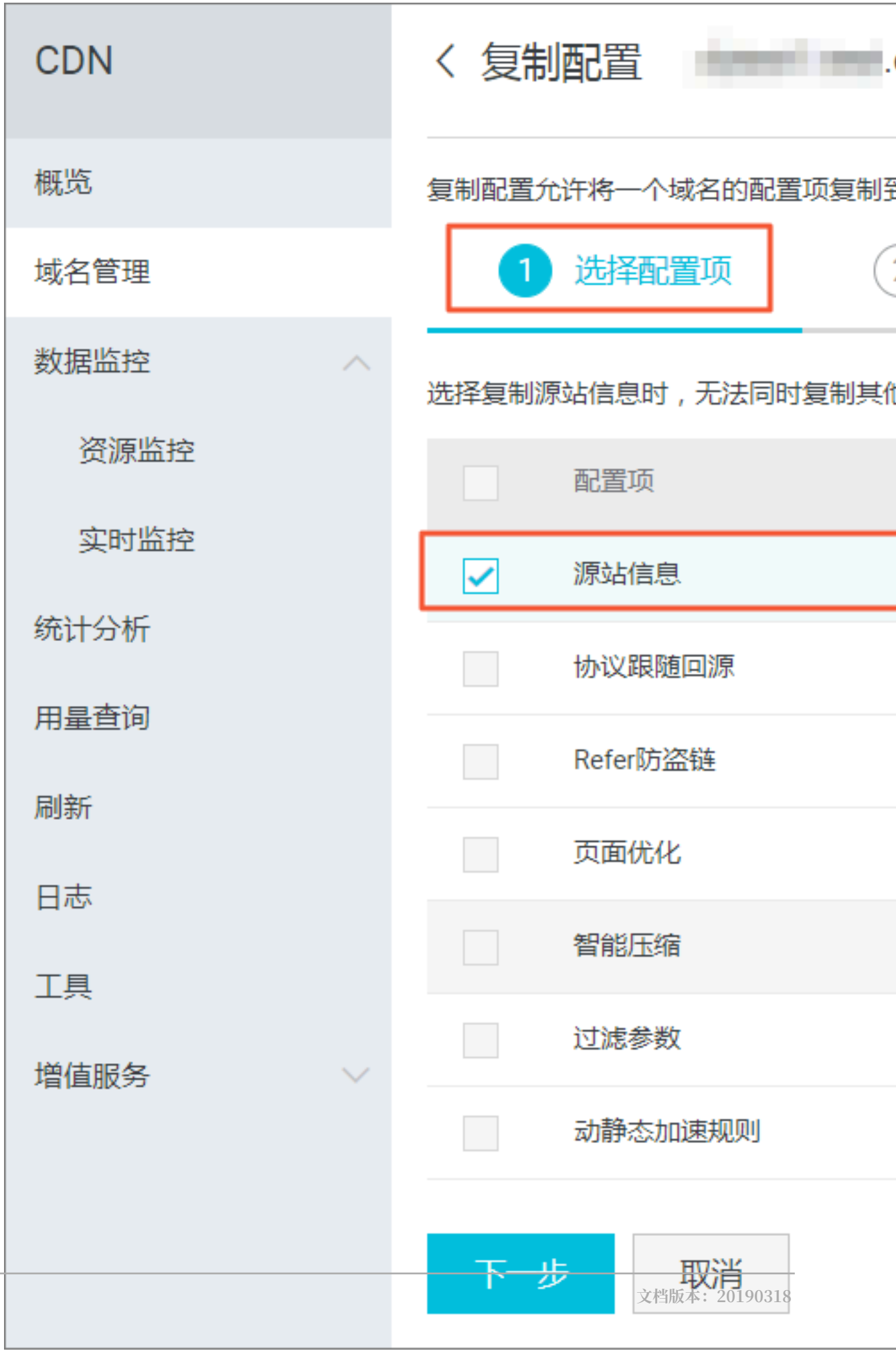
1. 在域名概览页，选择您想要复制配置的域名，单击复制配置。




2. 勾选您想要复制的配置项，单击下一步。

说明:

**您无法同时复制源站信息和非源站信息。**


CDN
概览
域名管理
数据监控
资源监控
实时监控
统计分析
用量查询
刷新
日志
工具
增值服务
复制配置
复制配置允许将一个域名的配置项复制到
1 选择配置项
选择复制源站信息时，无法同时复制其他
配置项
源站信息
协议跟随回源
Refer防盗链
页面优化
智能压缩
过滤参数
动静态加速规则
下一步
取消

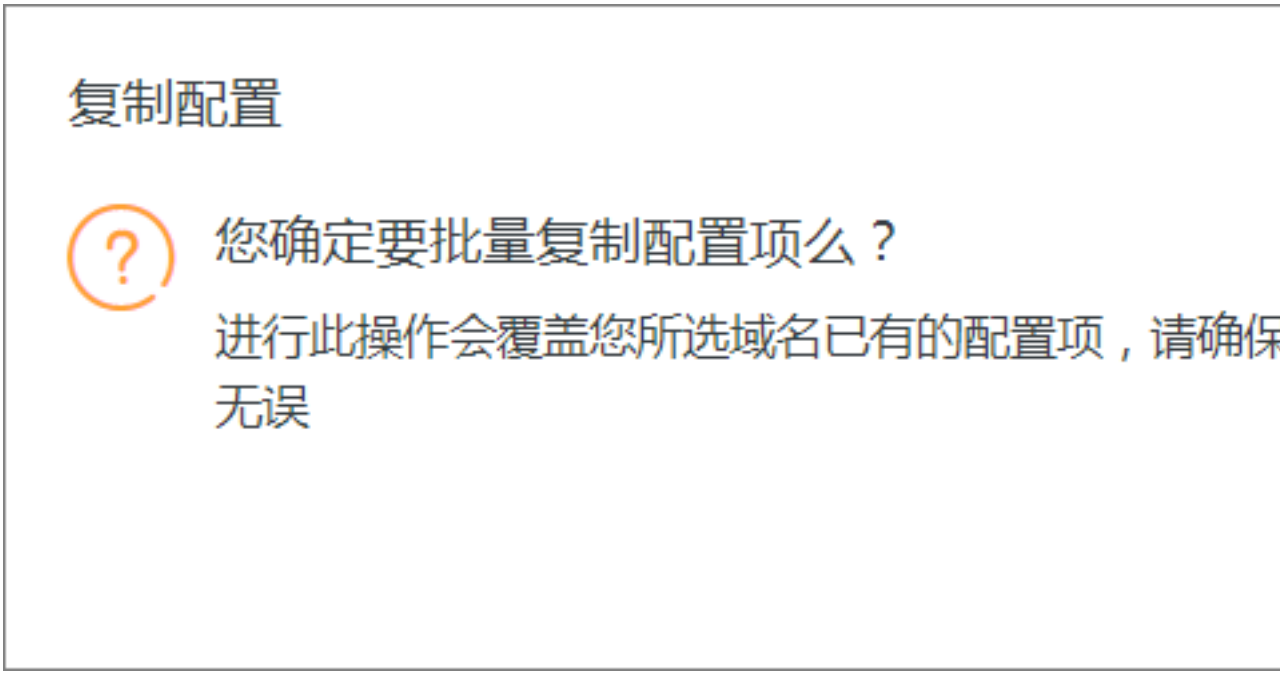
3. 勾选您想要的被批量配置的目标域名（您想要应用上一步中复制到的配置的域名），单击下一步。

   您也可以输入关键词查找域名。


复制配置
复制配置允许将一个域名的配置项复制到多个域名，帮助您对域名进行批
选择配置项
2
选择域名
3
域名列表
已选择 1 个域名，最多允许50个
域名
6tp.com
6tp.com
be.com
p.com
显示已选的域名
下一步
取消

> **说明:**
> 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。

4. 在单弹窗中单击确认，批量复制成功。




注意事项

- 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。

## 5.2 标签管理

您可以在CDN控制台上给您的加速域名打标签，标签的用途由您来决定，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。

功能介绍

您可以用标签标记域名的用途，也可以用标签给域名分组，打标后可以在域名列表页、资源监控页和用量查询页，使用标签快速筛出对应域名的数据，方便您查询数据和域名分组管理。

使用限制

- 每个标签都由一个键值对（Key:Value）组成。

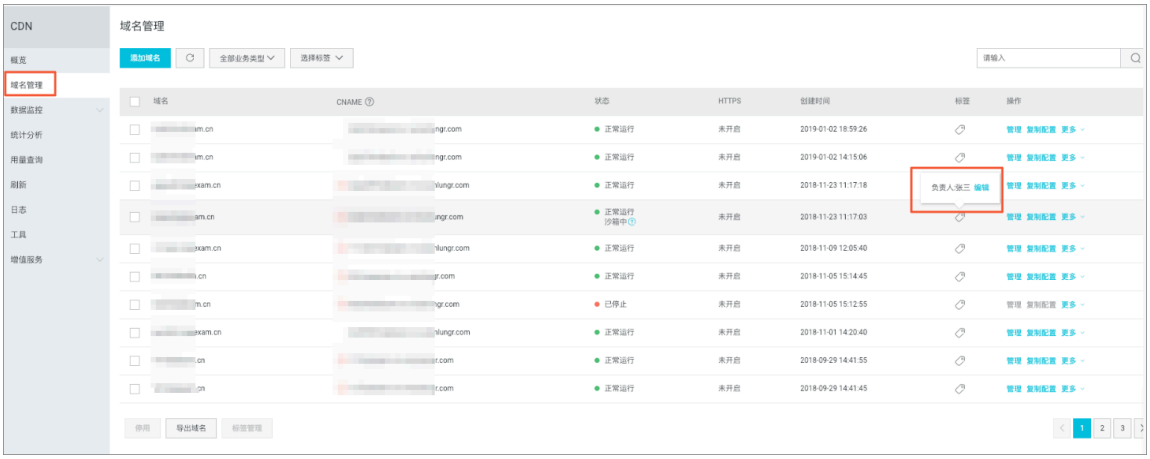
- 每个域名最多绑定 20 个标签。
- 同一个域名的标签键（Key）不能重复。如果对一个域名设置2个同Key不同Value的标签，新值将覆盖旧值。例如对域名 test.example.com 先后设置了标签 Key1:Value1 和 Key1:Value2，则最终 test.example.com 只会绑定 Key1:Value2 这个标签。
- 键（key）不支持 aliyun、acs: 开头。不允许包含http:// 和 https:// 。不允许为空字符串。
- 值（value）不允许包含http:// 和 https:// 。允许为空字符串。
- 最大键（key）长度：64 个 Unicode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

操作步骤

编辑标签

- 单个域名

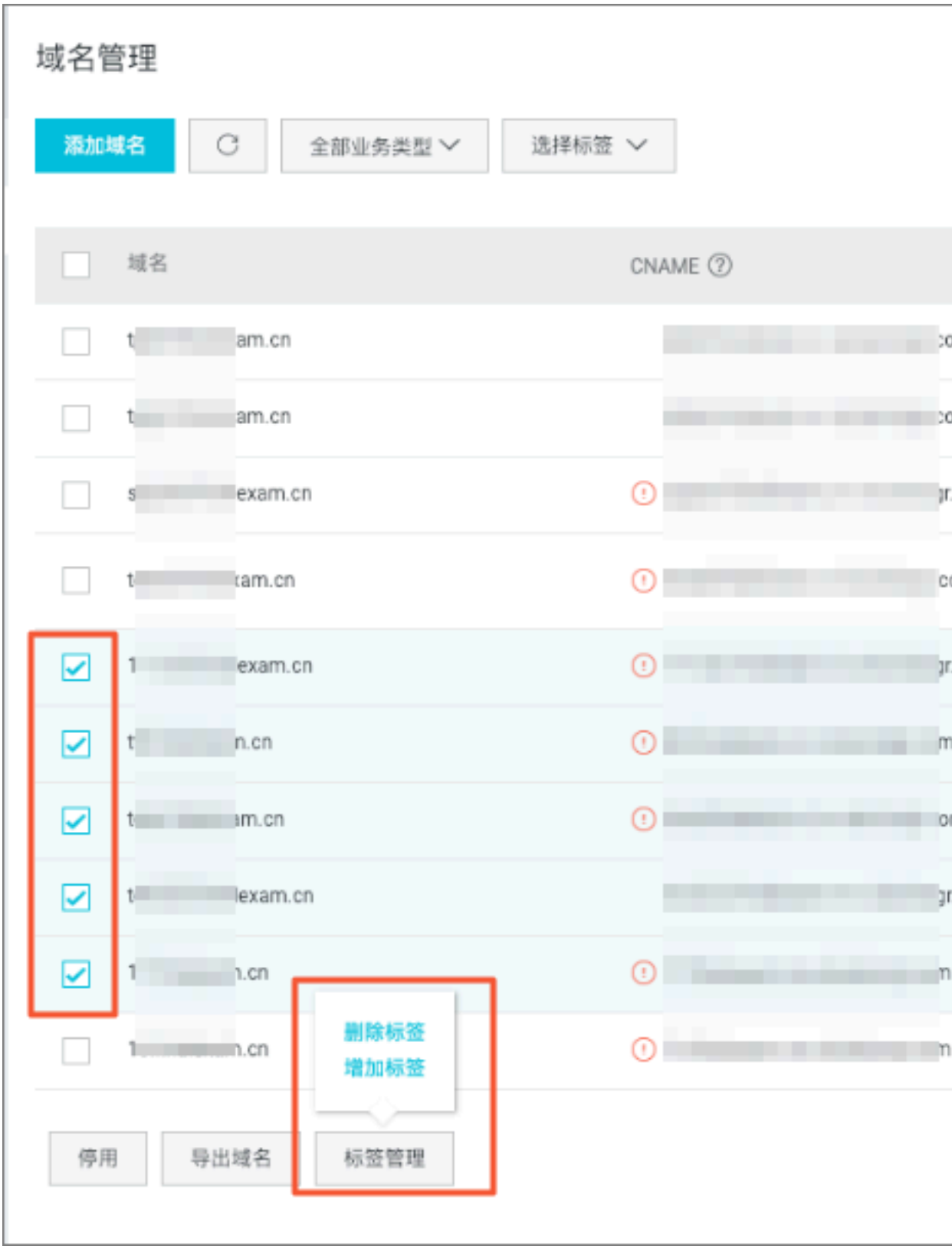
1. 登录CDN控制台，单击域名管理
2. 选择您想要设置标签的域名，将鼠标移动到对应标签上。
3. 在浮窗内，单击编辑。




4. 在编辑标签页，您可以选择已有标签或新建标签。编辑完成后，单击确定。

- 批量处理

  1. 登录CDN控制台，单击域名管理
  2. 批量勾选您想要处理的域名，单击标签管理。




  3. 选择删除标签或增加标签。

**筛选数据**

1. 登录*CDN*控制台
2. 在域名管理页、资源监控页或用量查询页，（任意页签内）选择对应的键（Key）和值（Value）标签，单击查询。

**说明:**

如果您同时选择多个标签，则查询的是各个标签对应的域名的交集的查询结果。

图 5-1: 域名管理


图 5-2: 资源监控


图 5-3: 用量查询

**案例**

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）/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/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2个标签 部门：游戏和负责人：李四。

## 5.3 HTTPS安全加速

## 5.3.1 HTTPS安全加速设置

安全超文本传输协议（Hyper Text Transfer Protocol over Secure Socket Layer，简称HTTPS），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。

### 功能优势

- 传输过程中对用户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。
- 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，了解更多使用*HTTPS*防止流量劫持。

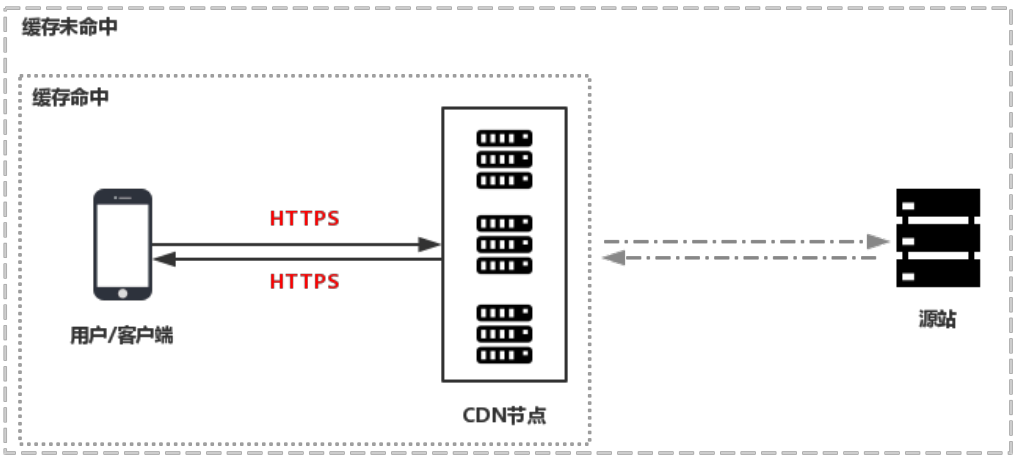
阿里云CDN 提供了HTTPS安全加速方案。您只需要开启HTTPS后上传证书和私钥，并支持对证书进行查看、停用、启用、编辑操作。

> 说明:
> 如果您有SNI回源的需要，请提交工单。

### 工作原理

在阿里云CDN控制台开启的HTTPS，将实现用户和阿里云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。

以下是HTTPS加密流程：




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。

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：图片小文件加速、大文件下载加速、视音频点播加速、直播流媒体加速。
- 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，系统默认兼容用户的HTTP和HTTPS请求。您也可以自定义对原请求方式设置强制跳转。
  - 停用：停用后，系统不再支持HTTPS请求且将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。
- 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。
- 你可以更新证书，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，当前计费标准详见 HTTPS计费详情。

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，您需要上传证书，包含证书和私钥，均为 PEM 格式。

  说明:
  由于CDN采用的Tengine服务基于Nginx，因此只支持Nginx能读取的证书，即PEM格式)。具体方法，请看参考证书格式说明及转化方法。
- 只支持携带SNI信息的SSL/TLS握手。
- 您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。

操作步骤

1. 购买证书。您需要具备匹配加速域名的证书才能开启HTTPS安全加速。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。
2. 登录CDN控制台，进入CDN域名管理页。选择域名，单击管理。
3. 在HTTPS设置 > HTTPS证书，单击修改配置。

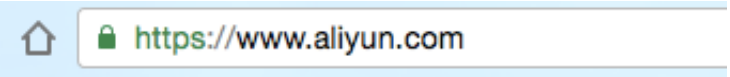

4. 在HTTPS设置对话框中，开启HTTPS安全加速。

5. 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。目前仅支持 `PEM` 的证书格式。

   - 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的免费证书的只适用于CDN的HTTP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。设置免费证书后，大约需要等候10分钟生效。


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
证书类型
云盾
自定义
云盾证书服务
证书名称
dd
内容
2KsQYOfTSDe4BHJo
QoAvl4MgGrlrxX1TI++eqLt8nmTWWh7pcBEMDFjxK
LkPUyBo2/U+6Lrmx
aBX+VNAOYgPmUVhY24b+pyau9hL2pYjGg1CoMN
H+W6s/y03D129Kzt583
D/5+nqpExJD3nqMHHwIrG1VDIVfYTCAXRIECAwEA
QwggGwMAwGA1UdEwEB
/wQCMAAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGC
FBwMCMA4GA1UdDwEB/wQE
AwIFoDA3BgNVHR8EMDAuMCygKqAohiZodHRwOi8
mdvZGFkZHkuY29tL2dk
pem编码参考样例
私钥
信息敏感证书私钥不可见

6. 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，表明当前与网站建立的是私密连接，HTTPS安全加速生效。




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，直接在HTTPS设置页选择想替换的目标证书类型（即云盾或免费证书）即可。
- 如果您想更换为自定义证书，在HTTPS设置页，选择自定义，然后将新证书的名称和内容填入对应框内，提交信息即可。

## 5.3.2 证书格式说明

在您开启 *HTTPS*安全加速 服务之前，您需要配置证书。您可以选择在 阿里云云盾 托管或购买的证书、阿里云CDN的免费证书或自行上传的自定义证书。自定义上传只支持PEM格式证书、证书及私钥格式及其他格式转PEM格式方法。

证书格式要求

CA 机构提供的证书一般包括以下几种。其中阿里云CDN使用的是 Nginx （.crt为证书，.key为私钥）：


- 如果证书是通过 root CA机构颁发，则您的证书为唯一的一份。
- 如果证书是通过中级CA机构颁发的证书，则您的证书文件包含多份证书，需要手工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，中间不要有空行。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。

示例

请确认格式正确后上传。

Root CA机构颁发的证书

证书格式为linux环境下 PEM 格式为：

```
-----BEGIN CERTIFICATE-----
MIIE+TCCA+GgAwIBAgIQU306HIX4KsioTW1s2A2krTANBgkqhkiG9w0BAQUFADCB
tTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSoAYykwOTEvMC0GA1UEAxMm
VmVyaVNpZ24gQ2xhc3MgMyBTZWN1cmUgU2VydmVyIENBIC0gRzIwHhcNMTAxMDA4
MDAwMDAwWhcNMTMxMDA3MjM1OTU5WjBqMQswCQYDVQQGEwJVUzETMBEGA1UECBMK
V2FzaGluZ3RvbjEQMA4GA1UEBxQHU2VhdHRsZTEYMBYGA1UEChQPQW1hem9uLmNv
bSBJbmMuMRowGAYDVQQDFBFpYW0uYW1hem9uYXdzLmNvbTCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEA3Xb0EGea2dB8QGEUwLcEpwvGawEkUdLZmGL1rQJZdeeN
3vaF+ZTm8Qw5Adk2Gr/RwYXtpx04xvQXmNm+9YmksHmCZdruCrW1eN/P9wBfqMMZ
X964CjVov3NrF5AuxU8jgtw0yu//C3hWn0uIVGdg76626gg0oJSaj48R2n0MnVcC
AwEAAaOCAdEwggHNMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMEUGA1UdHwQ+MDww
OqA4oDaGNGh0dHA6Ly9TVlJTZWN1cmUtRzItY3JsLnZlcmlzaWduLmNvbS9TVlJT
ZWN1cmVHMi5jcmwwRAYDVR0gBD0wOzA5BgtghkgBhvhFAQcXAzAqMCgGCCsGAQUF
BwIBFhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMB0GA1UdJQQWMBQGCCsG
AQUFBwMBBggrBgEFBQcDAjAfBgNVHSMEGDAWgBSl7wsRzsBBA6NKZZBIshzgVy19
RzB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlz
aWduLmNvbTBABggrBgEFBQcwAoY0aHR0cDovL1NWUlNlY3VyZS1HMi1haWEudmVy
aXNpZ24uY29tL1NWUlNlY3VyZUcyLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFow
WDBWFglpbWFnZS9naWYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEF
GDAmFiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZI
hvcNAQEFBQADggEBALpFBXeG782QsTtGwEE9zBcVCuKjrsl3dWK1dFiq3OP4y/Bi
ZBYEywBt8zNuYFUE25Ub/zmvmpe7p0G76tmQ8bRp/4qkJoiSesHJvFgJ1mksr3IQ
3gaE1aN2BSUIHxGLn9N4F09hYwwbeEZaCxfgBiLdEIodNwzcvGJ+2LlDWGJOGrNI
NM856xjqhJCPxYzk9buuCl1B4Kzu0CTbexz/iEgYV+DiuTxcfA4uhwMDSe0nynbn
1qiwRk450mCOnqH4ly4P4lXo02t4A/DI1I8ZNct/Qfl69a2Lf6vc9rF7BELT0e5Y
R7CKx7fc5xRaeQdyGj/dJevm9BF/mSdnclS5vas=
-----END CERTIFICATE-----
```

**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。**

**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。**
- `-----BEGIN RSA PRIVATE KEY-----`**开头，**`-----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-----`**、**

```
-----END PRIVATE
      KEY-----
```

**这种样式的私钥，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

**CDN HTTPS安全加速只支持 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，因此 只需在CDN控制台只需填写证书部分，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
```

**免费证书**

**CDN免费证书，即阿里云的Digicert免费型DV版SSL证书。CDN的免费证书的只适用于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设置后，再次开启使用免费证书时，会直接使用已经申请过但未过期的证书。若开启时证书已过期，会重新申请免费证书。

其他证书相关

- 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。请参考*HTTPS*安全加速设置。
- 只支持带SNI信息的SSL/TLS“握手”。
- 请确保上传的证书和私钥匹配。
- 更新证书的生效时间为10分钟。
- 不支持带密码的私钥。

其他证书相关的常见问题，请见更多证书问题。

## 5.3.3 强制跳转

如果您的加速域名开启了HTTPS安全加速，您可以自定义设置，将终端用户的原请求方式进行强制跳转。

操作步骤

1. 进入域名管理页面，选择需要设置的域名，单击管理。
2. 在HTTPS设置 > 强制跳转开启功能。

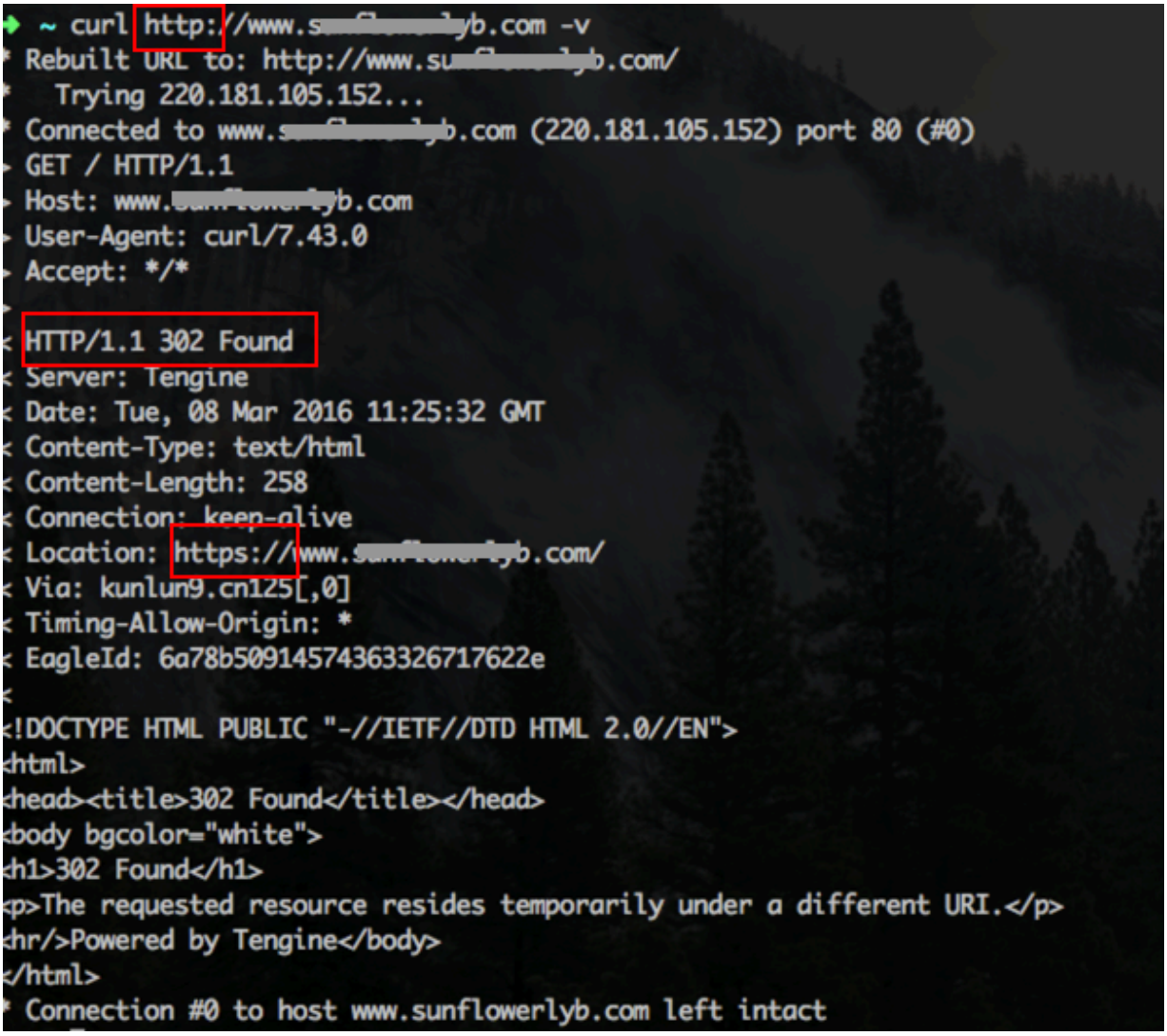

| 跳转类型 | 说明 |
| --- | --- |
| 默认 | 同时支持HTTP和HTTPS方式的请求。 |
| 强制HTTP跳转 | 用户的请求将强制重定向为HTTP请求。 |

| 跳转类型 | 说明 |
| --- | --- |
| 强制HTTPS跳转 | 用户的请求将强制重定向为HTTPS请求。 |

**说明:**
您只有在启用HTTPS安全加速功能后才能设置强制跳转。同时支持HTTP和HTTPS方式的请求。

示例

当您开启强制HTTPS跳转后，终端用户发起一个HTTP请求，服务端返回302重定向响应，原来的HTTP请求强制重定向为HTTPS请求，如图所示：



## 5.3.4 HTTP/2

### 功能介绍

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。

> 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。

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，有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 。

### 操作步骤

1. 在 域名管理页面，选择域名，单击 配置。
2. 在 HTTPS配置 > HTTP/2设置 栏进行配置。

> 说明:
> 开启HTTP/2前，请确保HTTPS的证书已经配置成功。
>
> - 若您是第一次配置HTTPS证书，需要等证书配置完成且生效后，才能打开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。

3. 打开后保存即可。


返回域名列表
.com
基本配置
回源配置
缓存配置
HTTPS配置
访问控制
性能优化
高级配置
视频相关
HTTPS证书
HTTPS证书
已关闭
提供全链路HTTPS安全加速方案, 支
修改配置
HTTP/2设置
HTTP/2
HTTP/2是最新的HTTP协议, 开启前

# 5.3.5 TLS

本文档介绍了TLS功能及其操作步骤。

## 功能介绍

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+，Firefox 63+。

> 说明:
> 目前TLSv1.0、TLSv1.1和TLSv1.2版本默认开启。

## 操作步骤

> 说明:
> 请首先配置HTTPS证书，然后才可以开启TLS功能。

1. 登录*CDN*控制台。
2. 在左侧导航栏，单击域名管理。
3. 在准备配置的域名后，单击管理。

4. 在左侧导航栏，单击HTTPS设置。


5. 在TLS版本控制栏，根据您的需要，开启或关闭对应的TLS版本。

## 5.3.6 HSTS

本文档介绍了HSTS功能的原理、使用场景和阿里云控制台的操作步骤。

### 功能介绍

HSTS (HTTP Strict Transport Security)，RFC6797，其作用是强制客户端（如浏览器）使用 HTTPS 与服务器创建连接。

### 使用场景

当您网站全站使用 HTTPS后，必须要将所有 HTTP 请求 301/302 重定向到 HTTPS。如果您从浏览器输入 HTTP 链接，或在他处点击了 HTTP 链接，则服务器则将该 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期服务器，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，表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

说明:

请首先配置HTTPS证书，然后才可以开启TLS功能。

1. 登录*CDN*控制台。
2. 在左侧导航栏，单击域名管理。
3. 在准备配置的域名后，单击管理。

4. 在左侧导航栏，单击HTTPS设置。


5. 在HTST栏，单击修改配置。完成配置即可。

## 5.4 内容回源设置

### 5.4.1 源站设置

本文档介绍了CDN源站的类型及设置方法、流量回源原理和自定义端口相关信息。

#### 功能介绍

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:
> 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”。

所有流量首先回源优先级高的源站，如果某个源站连续3次健康检查都失败，此时所有流量将选择第二优先级的源站回源。如果该源站健康检查成功，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。

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。

主要支持场景：主备方式切换源站。

#### 操作步骤

1. 进入域名管理页面，选择需要设置的域名，单击管理。

2. 在基本配置 > 源站信息源站配置，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）。

   - 如果您选择的源站类型为 IP 或 源站域名，则您仍然按照外网流量标准进行计费。
   - 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。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，那么仍然按照外网流量价格计费。


基本配置
回源配置
加速规则
缓存配置
HTTPS配置
访问控制
性能优化
高级配置
视频相关
基础信息
CNAME
rongbeitest.cdnpe.
启用CDN加速服务
创建时间
2018-07-19 16:18:1
加速区域
中国大陆
源站信息
类型
IP
地址
77.44.6.55
修改配置
源站配置
源站

3. 设置完成后，单击确认，设置成功。

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。
- 直播加速不支持源站设置。

自定义端口

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。

- 当您的静态或动态协议设置为跟随时，无法设置自定义端口。
- 如果您通过OpenAPI，设置自己的回源协议为跟随，请确保您的回源协议和自定义端口均能正常使用。
- 当您通过端口设置了回源协议（HTTP或HTTPS）和自定义端口时，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。

## 5.4.2 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。

## 5.4.3 协议跟随回源

### 功能介绍

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，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；同理类似 HTTP 协议的请求。

> **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。

### 配置说明

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 > 静态协议跟随回源开启功能。
3. 您可以选择跳转类型：跟随、HTTP或HTTPS。


## 5.4.4 回源HOST

使用回源HOST，您可以自定义CDN节点回源时需要访问的具体服务器域名。可选域名类型包括：OSS域名、IP和源站域名。

> **说明:**
> 如果您的一个IP源站绑定了多个域名或站点，就需要指定回源HOST回到的具体域名，否则回源会失败。

回源HOST的默认值为：

- 如果源站类型是IP，回源HOST默认为加速域名。
- 如果源站类型是OSS域名，回源HOST默认为源站域名。

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。

说明:
目前不支持SNI回源。

操作步骤

1. 登录CDN控制台，在左树菜单栏，单击域名管理。
2. 进入域名管理页，选择域名，单击管理。
3. 单击内容回源。
4. 在回源HOST项，单击修改配置。

5. 开启回源HOST，并选择域名类型。单击确定，配置成功。


示例

例一

如果您的源站是域名源站www.a.com，且将回源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。

例二

如果您的源站是IP源站`1.1.1.1`，且将回源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`。

## 5.4.5 回源SNI

本文档通过对SNI的应用场景和工作原理的介绍，让您了解是否需要设置回源SNI功能。同时，还提供了具体的操作步骤。

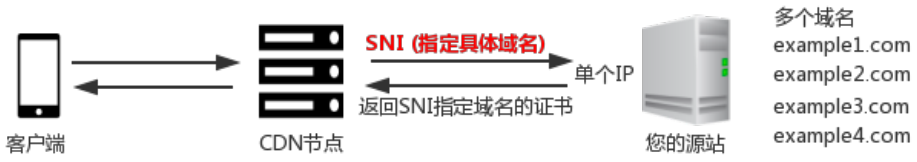
### 功能介绍

随着现代服务器对虚拟主机的支持，一台服务器可以为多个域名提供服务，但是一台服务器使用单个IP提供多个域名的HTTPS服务时，访问服务器的请求就必须要携带SNI（Server Name Indication）信息，SNI指明所请求的具体域名，才能让服务器正确地返回对应域名的证书。

如果您的源站服务器是上述的“单个IP提供多个域名的HTTPS服务”的情形，且您在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。

### 示意图




### 操作步骤

1. 登录*CDN*控制台，并单击域名管理。
2. 选择您要配置SNI的域名，单击该域名右侧的管理。

3. 单击回源配置，在回源SNI区域框单击修改配置。

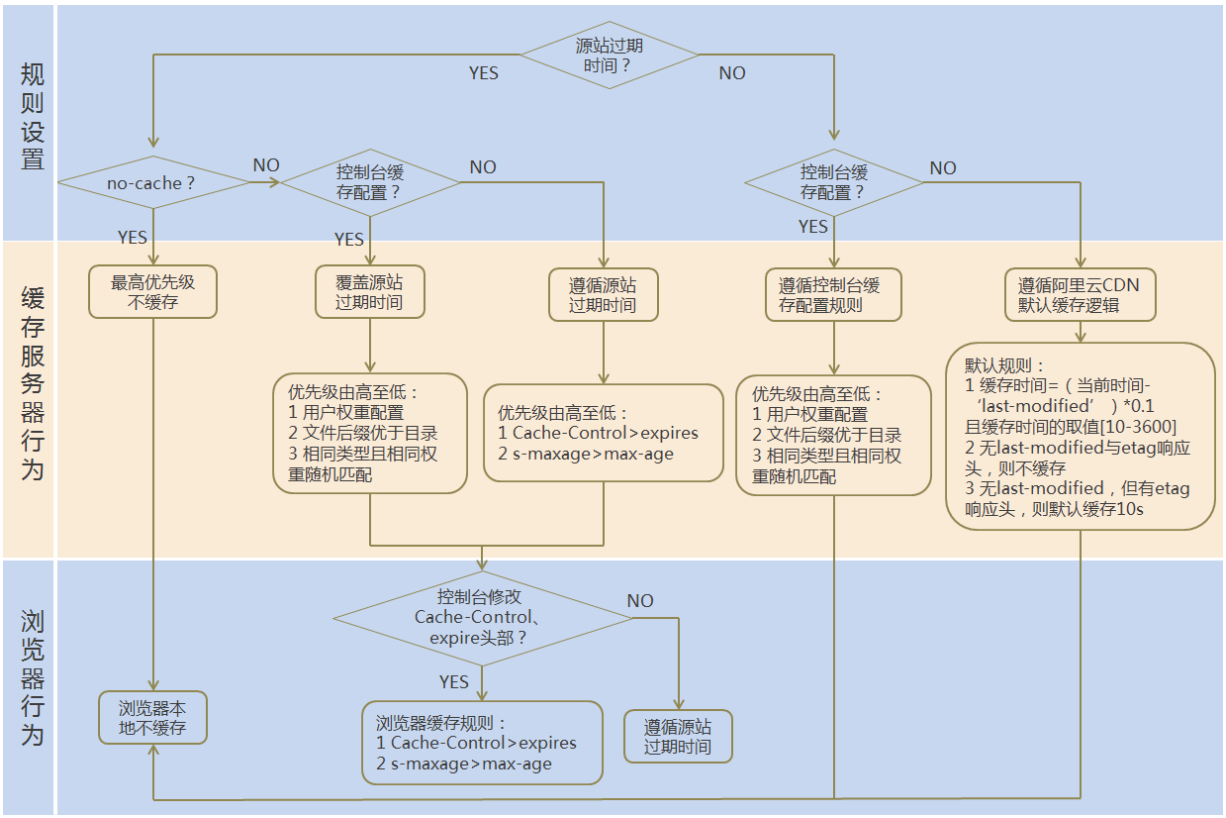
4. 填入您服务器源站里提供服务的具体域名，单击确认，完成开启SNI功能。

## 5.5 节点缓存设置

### 5.5.1 缓存配置

缓存配置，指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，可自定义指定资源内容的缓存过期时间规则，支持自定义缓存策略优先级。

功能介绍




**说明:**

- Cache的默认缓存策略用于配置文件过期时间，在此配置的优先级会高于源站配置。如果源站未配置cache配置，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的缓存是有可能由于热度较低被提前剔除出CDN节点的。

注意事项

- 对于不经常更新的静态文件，建议将缓存时间设置为1个月以上（eg：图片类型，应用下载类型）；
- 对于需要更新并且更新很频繁的静态文件，可以将缓存时间设置短些，视业务情况而定（eg：js,css等）；

- 对于动态文件（eg：php | jsp | asp），建议设置缓存时间为0s，即不缓存；若动态文件例如php文件内容更新频率较低，推荐设置较短缓存时间；
- 建议源站的内容不要使用同名更新，以版本号的方式方步，即采用img-v1.0.jpg、img-v2.1.jpg的命名方式。

操作步骤

1. 进入CDN域名概览页，选择域名进入域名管理页面，缓存配置。
2. 单击修改配置，可以管理缓存规则，添加、修改、删除。
3. 单击添加，增加缓存规则，按目录或者按文件后缀。


举例：为加速域名 `example.aliyun.com` 设置三则缓存配置规则：

- 缓存策略1：文件名后缀为jpg、png的所有资源 过期时间为1月，权重设置为90。
- 缓存策略2：目录为/www/dir/aaa 过期时间为1小时，权重设置为70。
- 缓存策略3：完整路径为/www/dir/aaa/example.php 过期时间为0s，权重设置为80。

则这三个缓存策略的生效顺序是：策略1—>策略3—>策略2。

说明:

- 权重可设置1-99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。

## 5.5.2 设置HTTP响应头

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。

### 功能介绍

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，进入域名管理页面，选择需要设置的域名，单击管理。

2. 在缓存配置 > HTTP头，您可以单击修改或删除对HTTP的参数进行相应操作。您也可以单击添加，选择参数，并输入取值，然后单击确认，添加自定义HTTP头参数。


## 5.6 访问控制设置

### 5.6.1 防盗链

功能介绍

- 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。

操作步骤

1. 进入域名管理页面，选择需要设置的域名，单击管理。

2. 在访问控制 > Refer防盗链，单击修改配置。


3. 单击黑名单或白名单，在下框内输入想要添加的网段。

4. 单击确认。

注意事项

- 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。

## 5.6.2 IP黑/白名单

通过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。

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节点以403拒绝。所以CDN日志中仍会记录这些黑名单中的IP的请求记录。
- 当前，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. 进入域名管理页面，选择需要设置的域名，单击管理。

2. 在访问控制 > IP黑/白名单，单击修改配置。

3. 单击黑名单或白名单，在下框内输入想要添加的网段。
4. 单击确认。

## 5.6.3 鉴权配置

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。虽然，通过防盗链方法添加 Referer 黑、白名单的方式可以解决一部分盗链问题。但是，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，采用URL鉴权方式保护用户源站资源更为安全有效。

### 工作原理

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。

1. CDN客户站点提供加密 URL（包含权限验证信息）。
2. 您使用加密后的 URL 向加速节点发起请求。
3. 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。

### 鉴权方式

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。

### 鉴权代码示例

您可以查看 鉴权代码示例。

### 配置引导

1. 在CDN控制台页面下的域名管理 页，选择需要设置的域名，单击配置。

2. 在访问控制 > 鉴权配置栏，单击修改配置。

3. 单击开启URL鉴权配置，选择鉴权类型，并主KEY。

## 5.6.4 鉴权方式A

**工作原理**

**用户访问加密 URL 构成**

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

**鉴权字段描述**

- `PrivateKey` 字段用户可以自行设置
- 有效时间1800s指用户访问客户源服务器时间超过自定义失效时间（timestamp字段指定）的1800s后，该鉴权失效。例如用户设置访问时间为2020-08-15 15:00:00，则链接的真正失效时间为2020-08-15 15:30:00。

| 字段 | 描述 |
| --- | --- |
| timestamp | 失效时间，整形正数，固定长度为10，是1970年1月1日以来的秒数。<br>控制失效时间，10位整数，有效时间1800s。 |
| rand | 随机数，建议使用UUID (不能包含中划线”-“，如: 477b3bbc253f467b8def6711128c7bec 格式)。 |
| uid | 暂未使用（设置成0即可) |
| md5hash | 通过md5算法计算出的验证串，由数字和小写英文字母混合组成0-9a-z，固定长度32。 |

CDN服务器拿到请求后，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，则认为过期失效并返回HTTP 403错误。
- 如果 `timestamp` 大于当前时间，则构造出一个同样的字符串(参考以下sstring构造方式)。然后使用MD5算法算出 `HashValue` ，再和请求中带来的 `md5hash` 进行比对。比对结果一致，则认为鉴权通过，返回文件。否则鉴权失败，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)
```

**鉴权实例**

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HashValue:**

```
HashValue = md5sum("/video/standard/1K.html-1444435200-0-0-
aliyuncdnexp1234") = 80cd3862d699b7118eed99103f2a3a4f
```

6. **则请求时url为:**

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

**如果计算出的HashValue与用户请求中带的 md5hash = 80cd3862d699b7118eed 99103f2a3a4f 值一致，则鉴权通过。**

## 5.6.5 鉴权方式B

**原理说明**

**用户访问加密 URL 格式**

**用户访问的 URL 如下:**

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

**加密URL的构造:域名后跟生成URL的时间（精确到分钟）(timestamp)再跟md5值(md5hash )，最后拼接回源服务器的真实路径(FileName)，URL有效时间为1800s。**

**当鉴权通过时，实际回源的URL是:**

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

**鉴权字段描述**

- **注意：`PrivateKey` 由CDN客户自行设置**

- 有效时间1800s是指，用户访问客户源服务器时间超过自定义失效时间(timestamp字段指定)的1800s后，该鉴权失效；例如用户设置访问时间2020-08-15 15:00:00，链接真正失效时间是2020-08-15 15:30:00

| 字段 | 描述 |
| --- | --- |
| DomainName | CDN客户站点的域名 |
| 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 |
| md5hash | 以timestamp、FileName和预先设定好的PrivateKey 共同做MD5获得的字符串，即md5(`PrivateKey` + `timestamp` + `FileName` ) |
| FileName | 实际回源访问的URL (注意，鉴权时候FileName要以/开头) |

示例说明

1. 回源请求对象:

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

2. 密钥设为：aliyuncdnexp1234 (用户自行设置)。
3. 用户访问客户源服务器时间为 201508150800（格式为： YYYYMMDDHHMM）。
4. 则CDN服务器会构造一个用于计算 md5hash 的签名字符串：

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

5. 服务器会根据该签名字符串计算 md5hash：

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

6. 请求CDN时url：

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

计算出来的 md5hash 与用户请求中带的 md5hash = 9044548ef1527deadafa49a890a377f0 值一致，于是鉴权通过。

## 5.6.6 鉴权方式C

原理说明

**用户访问加密 URL 格式**

**格式1**

```
http://DomainName/{/}/FileName
```

**格式2**

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

- **花括号中的内容表示在标准的URL基础上添加的加密信息。**
- `<md5hash>`**是验证信息经过 MD5 加密后的字符串;**
- `<timestamp>`**是未加密的字符串，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。**
- **采用格式一进行URL加密，例如：**

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

  `<md5hash>` **为 a37fa50a5fb8f71214b1e7c95ec7a1bd**`<timestamp>` **为 55CE8100。**

**鉴权字段描述**

- `<md5hash>` **部分字段描述。**

| 字段 | 描述 |
| --- | --- |
| PrivateKey | 干扰串，不同客户采用不同的干扰串 |
| FileName | 实际回源访问的URL (注意，鉴权时候path要以/开头) |
| time | 用户访问源服务器时间，取 UNIX 时间，以十六进制数字字符表示。 |

- **PrivateKey 取值** `aliyuncdnexp1234`
- **FileName 取值** `/test.flv`
- **time 取值** `55CE8100`

- 因此 md5hash 值为：

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

- 明文: `timestamp = 55CE8100`

  这样生成加密 URL:

  格式一：

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

  格式二：

```
http://cdn.example.com/test.flv?KEY1=a37fa50a5fb8f71214b1e7c95ec7a1
bd&KEY2=55CE8100
```

示例说明

用户使用加密的 URL 访问加速节点,CDN服务器会先把加密串 1 提取出来, 并得到原始的 URL 的 `<FileName>` 部分，用户访问时间，然后按照定义的业务逻辑进行验证：

1. 使用原始的 URL 中的 `<FileName>` 部分,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)。
4. 有效时间1800s是指，用户访问客户源服务器时间超过自定义时间的1800s后，该鉴权失效；例如用户设置访问时间2020-08-15 15:00:00，链接真正失效时间是2020-08-15 15:30:00。
5. 时间差小于设置时限的为合法请求，CDN加速节点才会给予正常的响应，否则拒绝该请求，返回 http 403错误。

## 5.6.7 鉴权代码示例

URL鉴权规则请查阅 URL鉴权，通过这个 demo 您可以根据业务需要，方便的对URL进行鉴权处理。以下Python Demo包含三种鉴权方式：A鉴权方式、B鉴权方式、C鉴权方式，分别描述了三种不同鉴权方式的请求URL构成、哈希字符串构成等内容。

Python版本

```
import re
import time
import hashlib
```

```
import datetime
def md5sum(src):
    m = hashlib.md5()
    m.update(src)
    return m.hexdigest()
def a_auth(uri, key, exp):
    p = re.compile("^(http://|https://)?([^/?]+)(/[^?]*)?(\\?.*)?$")
    if not p:
        return None
    m = p.match(uri)
    scheme, host, path, args = m.groups()
    if not scheme: scheme = "http://"
    if not path: path = "/"
    if not args: args = ""
    rand = "0"      # "0" by default, other value is ok
    uid = "0"       # "0" by default, other value is ok
    sstring = "%s-%s-%s-%s-%s" %(path, exp, rand, uid, key)
    hashvalue = md5sum(sstring)
    auth_key = "%s-%s-%s-%s" %(exp, rand, uid, hashvalue)
    if args:
        return "%s%s%s%s&auth_key=%s" %(scheme, host, path, args,
auth_key)
    else:
        return "%s%s%s%s?auth_key=%s" %(scheme, host, path, args,
auth_key)
def b_auth(uri, key, exp):
    p = re.compile("^(http://|https://)?([^/?]+)(/[^?]*)?(\\?.*)?$")
    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)
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()
```

# 5.7 性能优化设置

## 5.7.1 智能压缩

**功能介绍**

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

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。

**操作步骤**

> **注意:**
> 当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。如果使用时，您对源站文件本身的md5值有校验机制，则请勿开启此功能。

1. 进入域名管理页面，选择需要设置的域名，单击管理。
2. 在性能优化 > 智能压缩开启功能。

## 5.7.2 页面优化

### 功能介绍

开启页面优化功能，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。

### 操作步骤

> 注意:
> 当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。如果您对源站文件本身配置有MD5值校验机制，请勿开启页面优化功能。

1. 登录CDN控制台，单击域名管理。
2. 在域名管理页面，单击需要设置域名后的管理。
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。

5.

## 5.7.3 过滤参数

功能介绍

过滤参数：URL请求中，如果携带“？”（半角）和参数，则请求到CDN节点时，CDN节点在收到该请求后是否将该带参数的请求URL请求回源站。

- 如果开启过滤参数，该请求到CDN节点后会截取到没有参数的URL向源站请求，且CDN节点仅保留一份副本。
  - 由于http 请求中大多包含参数，但往往参数内容优先级不高，可以忽略参数浏览文件，适合开启该功能；开启后可以有效提高文件缓存命中率，提升分发效率。
  - 若参数有重要含义，例如包含文件版本信息等，推荐设置“保留参数”。您可以设置多个保留参数。如请求中包含任一“保留参数”，会携保留参数回源。
- 如果关闭过滤参数，则每个不同的URL都缓存不同的副本在CDN的节点上。

过滤参数包括保留忽略参数和删除忽略参数这两个功能。

- 保留忽略参数：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。
- 删除忽略参数：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。

示例

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

- 开启“过滤参数”功能后，
  1. CDN节点向源站发起请求 `http://www.abc.com/a.jpg` （忽略参数x=1）。
  2. 源站响应该请求内容后，响应到达CDN节点。
  3. 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。
  4. 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“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。

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。

操作步骤

1. 进入域名管理页，选择需要设置的域名，单击配置。
2. 选择性能优化 > 过滤参数，单击修改配置。

   您可以在此开启或关闭过滤参数，并设置保留过滤参数或忽略参数。


# 5.8 视频相关配置

## 5.8.1 Notify_URL设置

功能介绍

流状态实时信息回调，可以及时通知用户推流或断流操作结果。

注意事项

- 原理：通过 HTTP 接口向用户服务器发送GET请求，将视频流推送成功，断流成功的状态实时反馈给用户，用户服务器通过 200 响应返回接口返回结果。
- URL无需标识，只需可正常访问，URL 的应答有要求如下：
- 如果访问超时，会重试这个 URL，目前超时时间是 5s，重试次数是 5 次，重试间隔为 1s。

配置引导

支持在控制台配置，为可选配置。


**举例如下：**

```
http://1.1.1.1/pub?action=publish&app=xc.cdnpe.com&appname=hello&id=
world&ip=42.120.74.183&node=cdnvideocenter010207116011.cm3
```

| 参数 | 取值说明 |
| --- | --- |
| time | unix 时间戳 |
| usrargs | 用户推流的参数 |
| action | publish表示推流，publish_done表示断流 |
| app | 默认为自定义的推流域名，如果未绑定推流域名即为播放域名 |
| appname | 应用名称 |
| id | 流名称 |
| node | cdn接受流的节点或者机器名 |
| ip | 推流的客户端ip |

## 5.8.2 拖拽播放

**功能介绍**

**拖拽播放功能是指：在视频点播场景中，如果用户拖拽播放进度时，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。此时，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。**

**开启该功能，CDN节点可以支持此项配置，可以在响应请求时直接向client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）（FLV格式）或第10s（MP4格式）开始的内容。**

### 注意事项

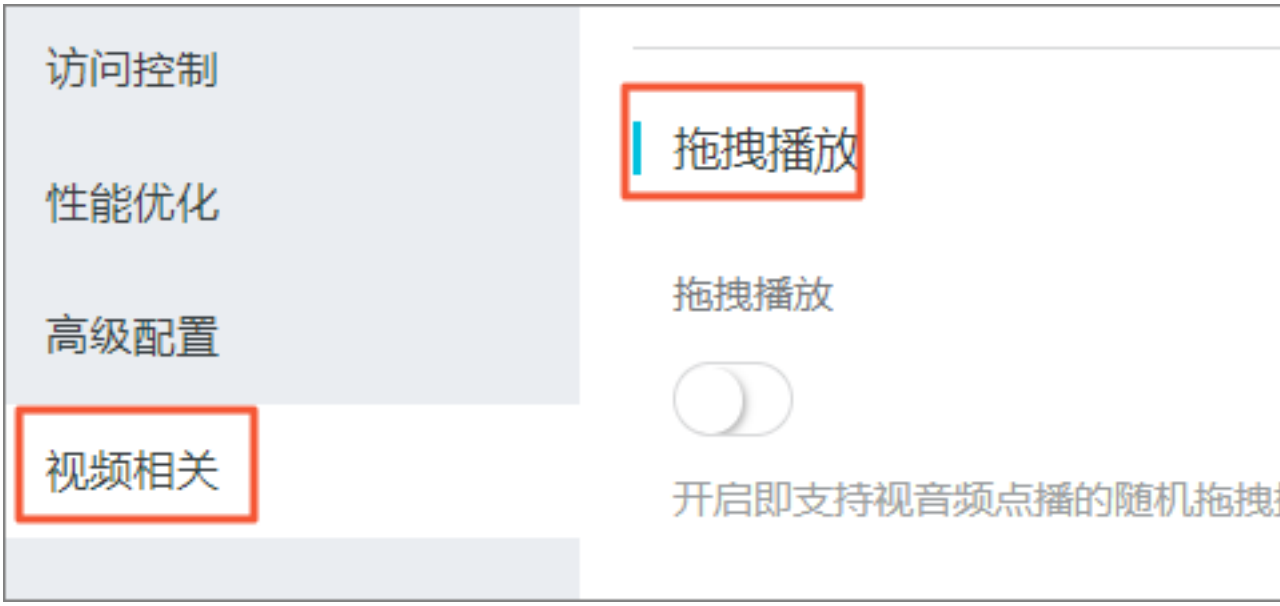
- 需要源站支持range请求，即如果http请求头中包含 Range 字段，源站需要能够响应正确的206文件分片。请参考Range回源。
- 目前支持文件格式有：MP4和FLV。
- 目前FLV只支持音频为aac，且视频为avc的编码格式。

| 文件类型 | 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. 进入域名管理页，选择需要设置的域名，单击配置。

2. 在视频相关 > 拖拽播放栏，开启该功能。




## 5.8.3 Range回源

功能介绍

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。这对于较大文件的分发加速有很大帮助。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。

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 | 具体描述 | 示例 |
| --- | --- | --- |
| 开启 | 该参数可以请求回源站。此时源站需要依据 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这个参数。并且源站响应给CDN节点，然后CDN节点响应给客户端的就是范围是0-100的一共101个字节内容。 |
| 关闭 | CDN上层节点会向源站请求全部的文件，并且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server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，但是由于连接断开了，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。

操作步骤

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。

1. 进入CDN域名管理页面，选择域名，单击管理。
2. 在视频相关 > Range回源，选择修改配置。
3. 选择 开启、关闭或强制Range回源功能。

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。

您还可以参考Range回源的API文档，使用该功能。

## 5.9 高级设置

### 5.9.1 带宽封顶

功能介绍

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。此时CDN将停止加速服务，避免异常流量带来的非日常消费。域名下线后，你可以在控制台重新启动该域名。

说明:
带宽封顶的功能，泛域名暂不支持，设置后不会生效。

RAM子账号需云监控授权后使用，请授权AliyunCloudMonitorFullAccess策略组。

操作步骤

说明:
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，谨慎设置带宽峰值。

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. 在左侧导航栏，单击高级设置。

4. 单击修改配置。
5. 开启带宽封顶开关。
6. 输入带宽上限值，并选择单位Mbps、Gbps、Tbps。然后单击确认。

> **说明:**
> 带宽进制为1000。

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。

# 6 数据监控

数据监控主要包括两个部分：资源监控、实时监控。

## 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。 |
| 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。

说明:

命中率不支持选择区域或运营商。

## 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：

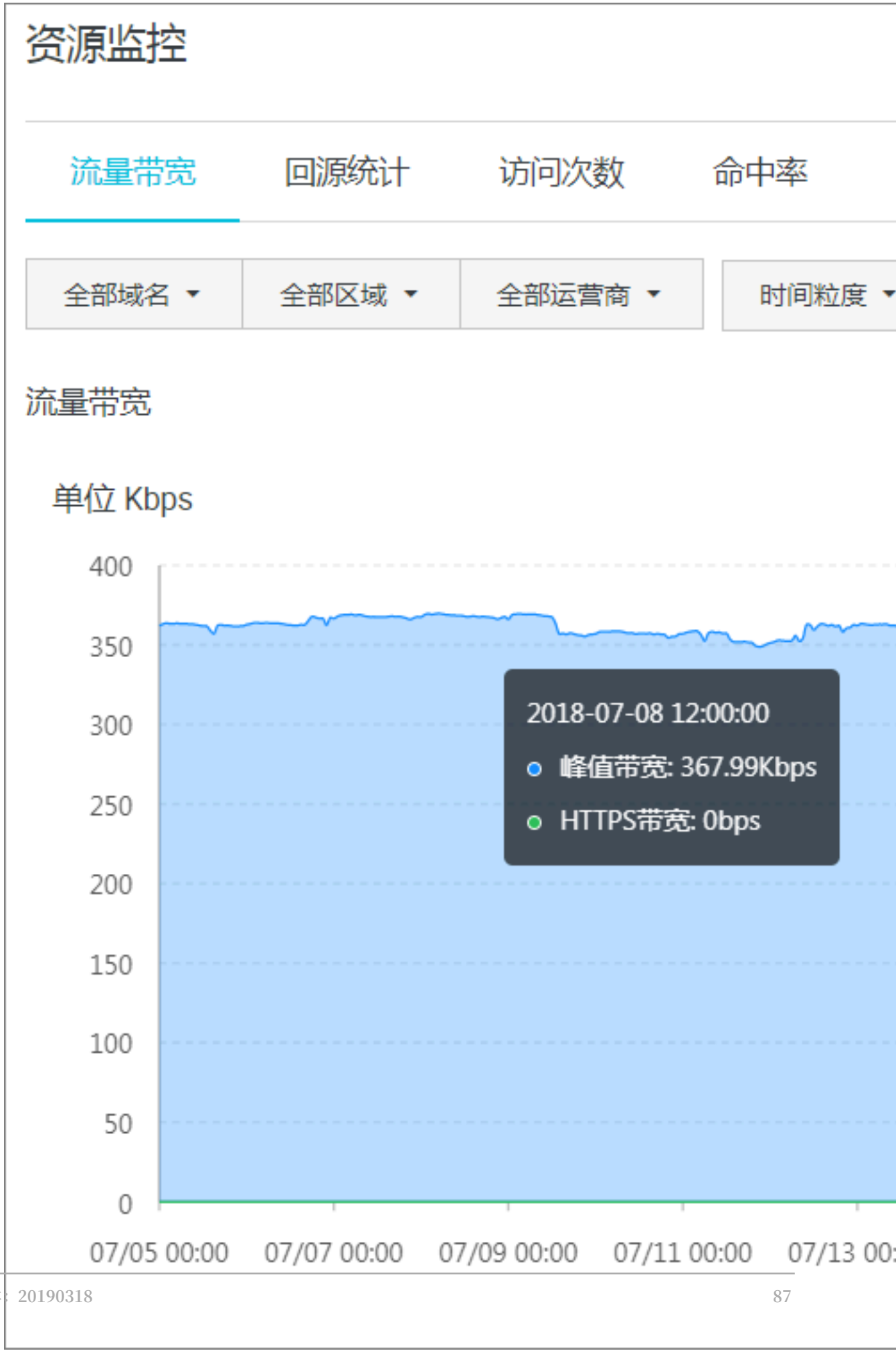
| 监控项 | 监控指标 |
| --- | --- |
| 基础数据 | 带宽、流量、请求次数、QPS。 |
| 回源流量 | 回源流量、回源带宽。 |
| 质量监控 | 请求命中率、字节命中率、5xx状态码、4xx状态码、3xx状态码、2xx状态码。 |

## 操作步骤

1. 登录CDN控制台，进入域名管理页面，选择需要设置的域名，单击管理。

2. 在数据监控 > 资源监控或实时监控，选择您想要查看的监控项和指标，点击查询。

   资源监控：


资源监控
流量带宽
回源统计
访问次数
命中率
全部域名
全部区域
全部运营商
时间粒度
流量带宽
单位 Kbps
400
350
300
250
200
150
100
50
0
2018-07-08 12:00:00
峰值带宽: 367.99Kbps
HTTPS带宽: 0bps
07/05 00:00
07/07 00:00
07/09 00:00
07/11 00:00
07/13 00:

**实时监控：**

# 7 统计分析

## 功能介绍

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。 | 今天、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。 | 今天、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。 | 今天、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，进入域名管理页面，选择需要设置的域名，单击管理。

2. 在统计分析页面，选择您想要查看的监控项和指标，点击查询。

# 8 用量查询

## 8.1 用量查询

### 功能介绍

如果您希望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。您可以自定义时间段进行查询。上线后，您最长可以查询3个月的数据。

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：

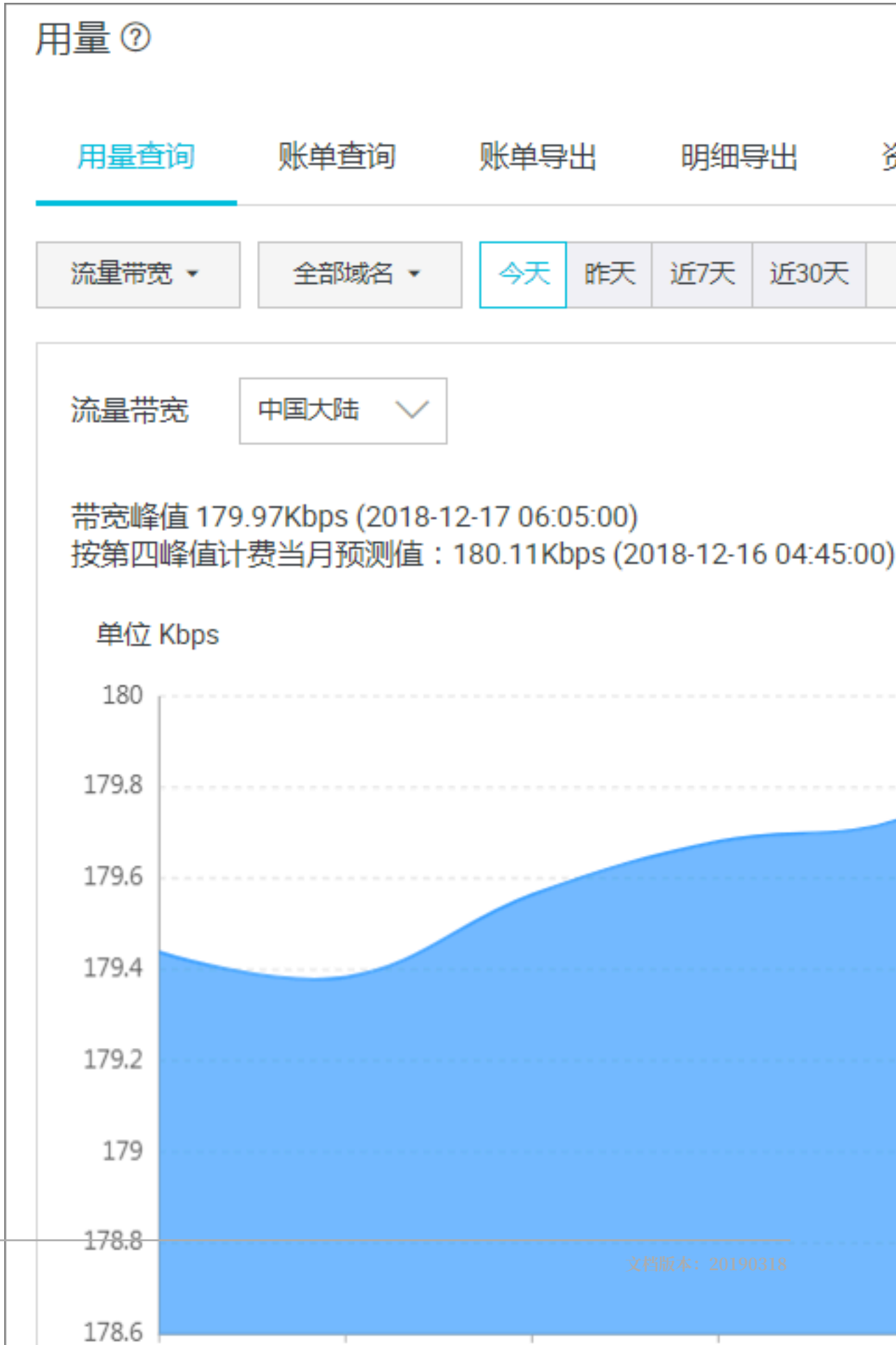
- 不同的域名和用户。
- 流量、带宽，或请求数。
- 不同计费大区。了解更多，请参考计费大区划分。

说明：

在用量查询页，您只能查询数据，不能导出。如有需要，请到账单导出或明细导出页导出相关数据。

**操作步骤**

1. 登录CDN控制台，单击用量查询。



2. 在用量页面，单击用量查询。
3. 设置查询条件，（包含流量带宽或请求数、域名、时间），单击查询。

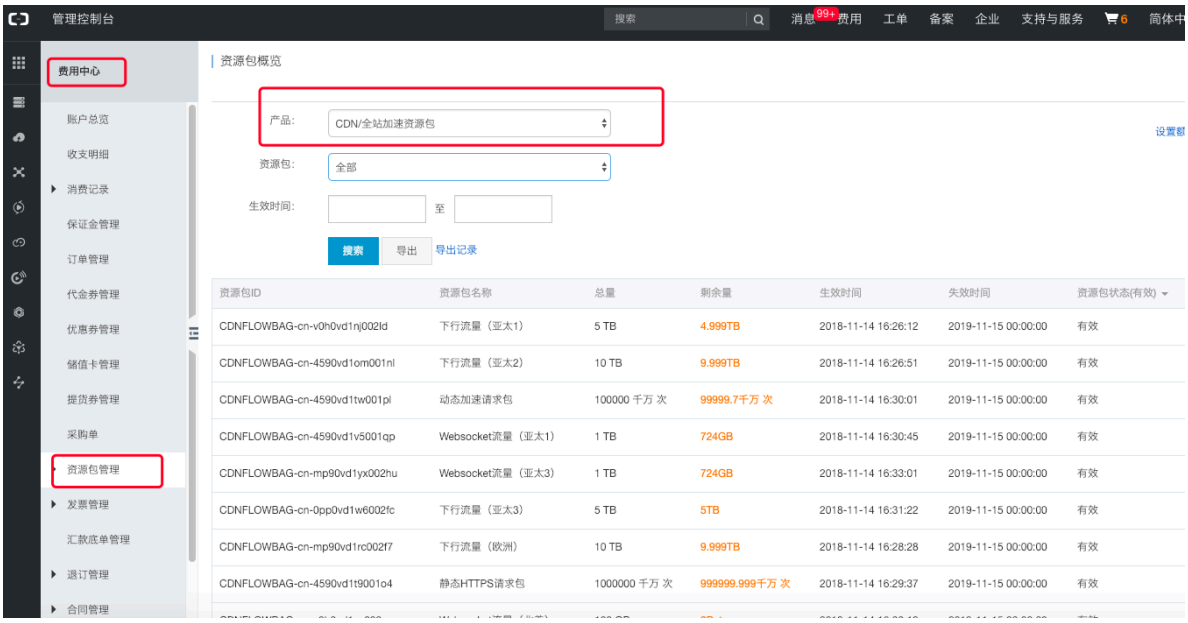
资源包用量查询

通过单击跳转 费用中心，可以查询您所有资源包详情。

- 查看CDN/全站加速资源包概况

  CDN/全站加速资源包概况包括：总量、剩余量、生效时间、失效时间和状态。

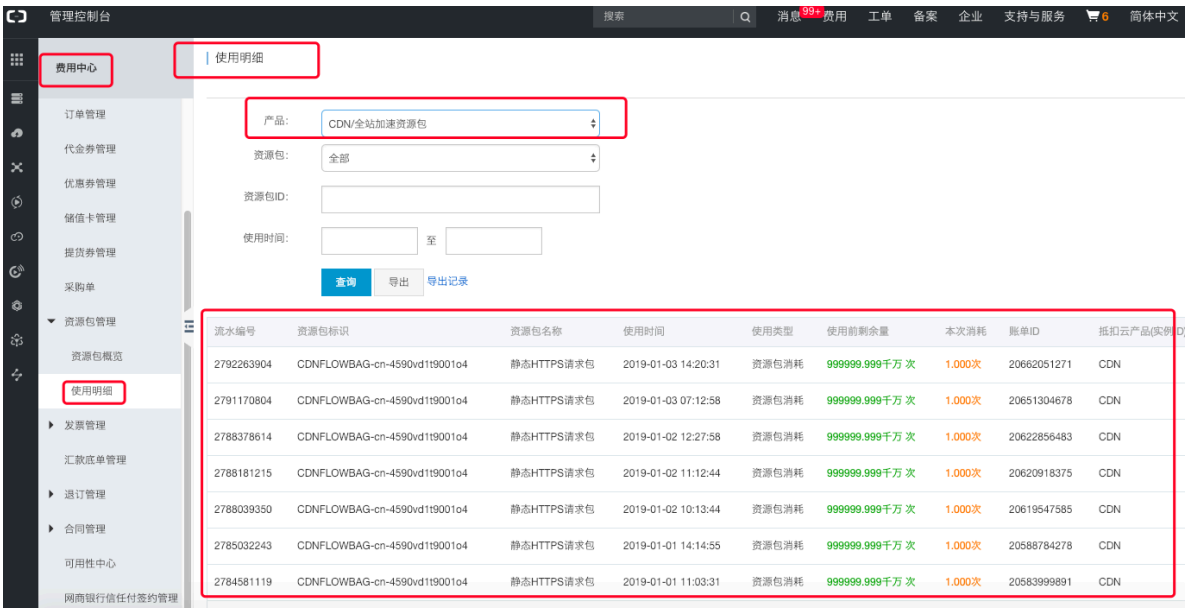
  选择CDN/全站加速资源包，您可以按资源包生效时间、资源包类别进行筛选，还可以导出资源包概览数据。



- 查看CDN/全站加速资源包使用明细

  CDN/全站加速资源包使用明细包括：名称、使用时间、使用前余量和最近1次使用量等。

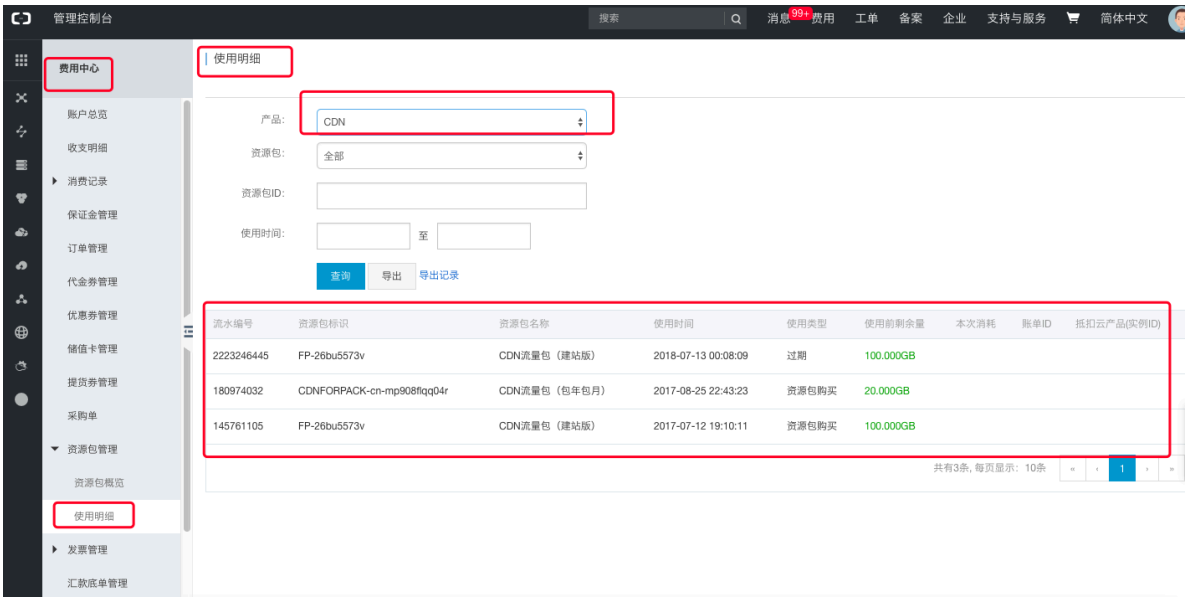
  选择CDN/全站加速资源包，您可以按照资源包类型、资源包生效时间或资源包ID进行筛选，还可以导出资源包使用明细数据。




- 查看CDN资源包使用明细

  CDN资源包使用明细包括：名称、使用时间、使用前余量和最近1次使用量等。

  选择CDN，您可以按照资源包类型、资源包生效时间或资源包ID进行筛选，还可以导出资源包使用明细数据。



其他

- 您可以点击账单查询，按日查询账单。
- 您可以点击账单导出，导出账单。
- 您可以点击明细导出，导出账单明细。
- 您可以点击资源包，查询您所有资源包的总量、剩余、生效时间、失效时间、状态。

## 8.2 账单导出

功能介绍

您可以导出按日计费，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。

- 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CDN域名概览页，单击用量查询。
3. 在用量查询页，选择账单导出。

4. 选择日期，然后单击查询账单。


5. 您可以单击下载，下载您需要的账单。

# 8.3 明细导出

## 功能介绍

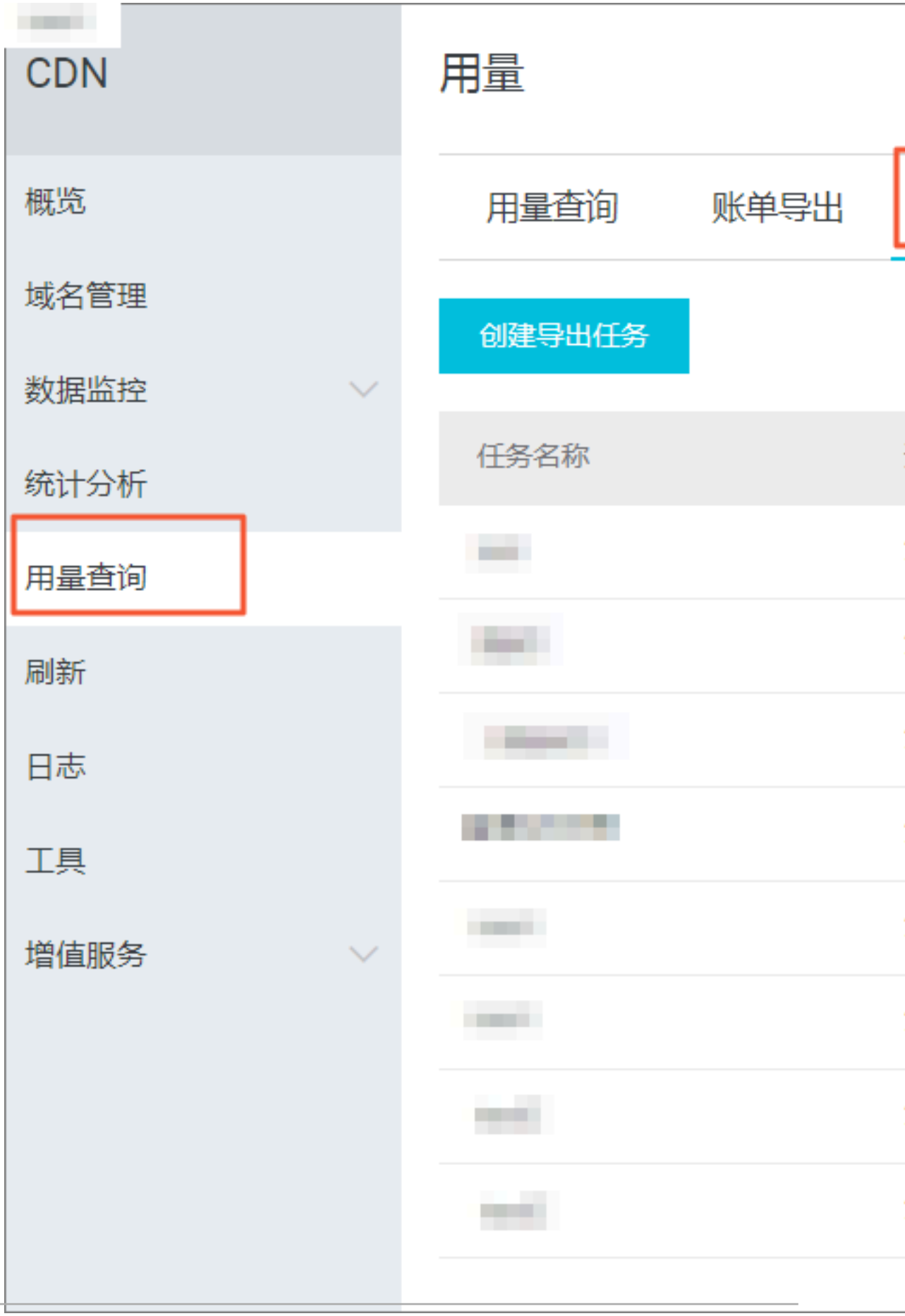
通过明细导出功能，您可以导出流量带宽及请求数的5分钟明细数据，便于您通过明细来核对或计算实际消费的计量数。

- 您可以按照账户、资源组、域名维度进行导出。
- 导出资源组时，会将资源组下所有域名也一并导出。
- 您一次性最多可以导出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。
- 导出的时间段不可以重复。

## 操作步骤

1. 登录*CDN*控制台。
2. 在CDN域名概览页，单击用量查询。

3. 在用量查询页面，单击明细导出。



4. 单击创建导出任务。
5. 填写相应导出任务的任务名称（必填），并选择导出对账类型、查询时间（必选）和导出内容和导出频次。


6. 单击确定，创建导出任务成功。

# 9 刷新预热

本文档介绍URL刷新、目录刷新和URL预热的原理、操作步骤和相关操作步骤以及如何查看资源刷新或预热的进度。

登录CDN控制台，单击刷新，进行刷新配置。

## URL刷新

原理：通过提供文件URL的方式，强制CDN节点回源拉取最新的文件。

任务生效时间：5-10 分钟之内生效。

注意事项：

- 输入的 URL 必须带有 `http://`或者 `https://`
- 同一个 ID 每天最多只能预热刷新共 2000 个 URL。
- 提供批量刷新缓存的接口，详情参见 刷新缓存API。


CDN
概览
域名管理
数据监控
统计分析
用量查询
刷新
日志
工具
增值服务
刷新预热
刷新缓存
操作记录
操作类型
刷新
刷新类型
URL
URL
每日最多刷新上限2000
提交

目录刷新

原理：通过提供文件目录的方式，强制CDN节点回源拉取最新的文件。

任务生效时间：5-10 分钟之内生效。

注意事项：

- 一天最多提交 100 个刷新请求。
- 所输入内容，需以 `http://`或者 `https://`开始，以/结束。
- 提供批量刷新缓存的接口，详见 刷新缓存*API*。

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：5-10 分钟之内生效。

注意事项：

- 输入的 URL 必须带有 `http://`或`https://`
- 同一个 ID 每天最多只能预热共 500 个 URL。
- 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，详情参见 资源预热*API*。

进度查看

- 可在CDN控制台 刷新 > 操作记录，查看资源刷新或预热的进度。
- 阿里云CDN提供查询进度的API： 查询刷新预热进度 。

# 10 日志管理

## 10.1 日志下载

本文档介绍了日志下载功能的使用限制、字段格式说明和控制台位置。

### 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。如：
  www.test.com_2018_10_30_000000_010000.gz

### 字段格式说明

日志内容：

```
[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"
```

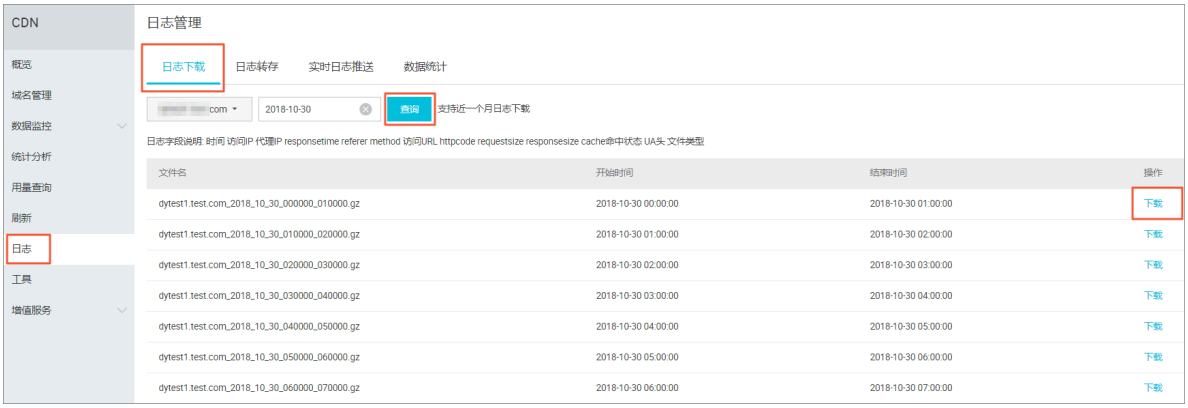
字段含义：

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

| 字段 | 参数 |
| --- | --- |
| UA头 | Mozilla/5.0 (compatible; AhrefsBot/5.0; + http://ahrefs.com/robot/) |
| 文件类型 | text/html |

操作步骤

1. 登录CDN控制台，单击日志。




2. 在日志下载页签下，选择域名和目标时间，单击查询。
3. 选择目标文件，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。

功能介绍

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。

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。

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，请参考函数计算计费方式。

### CDN与函数计算

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。

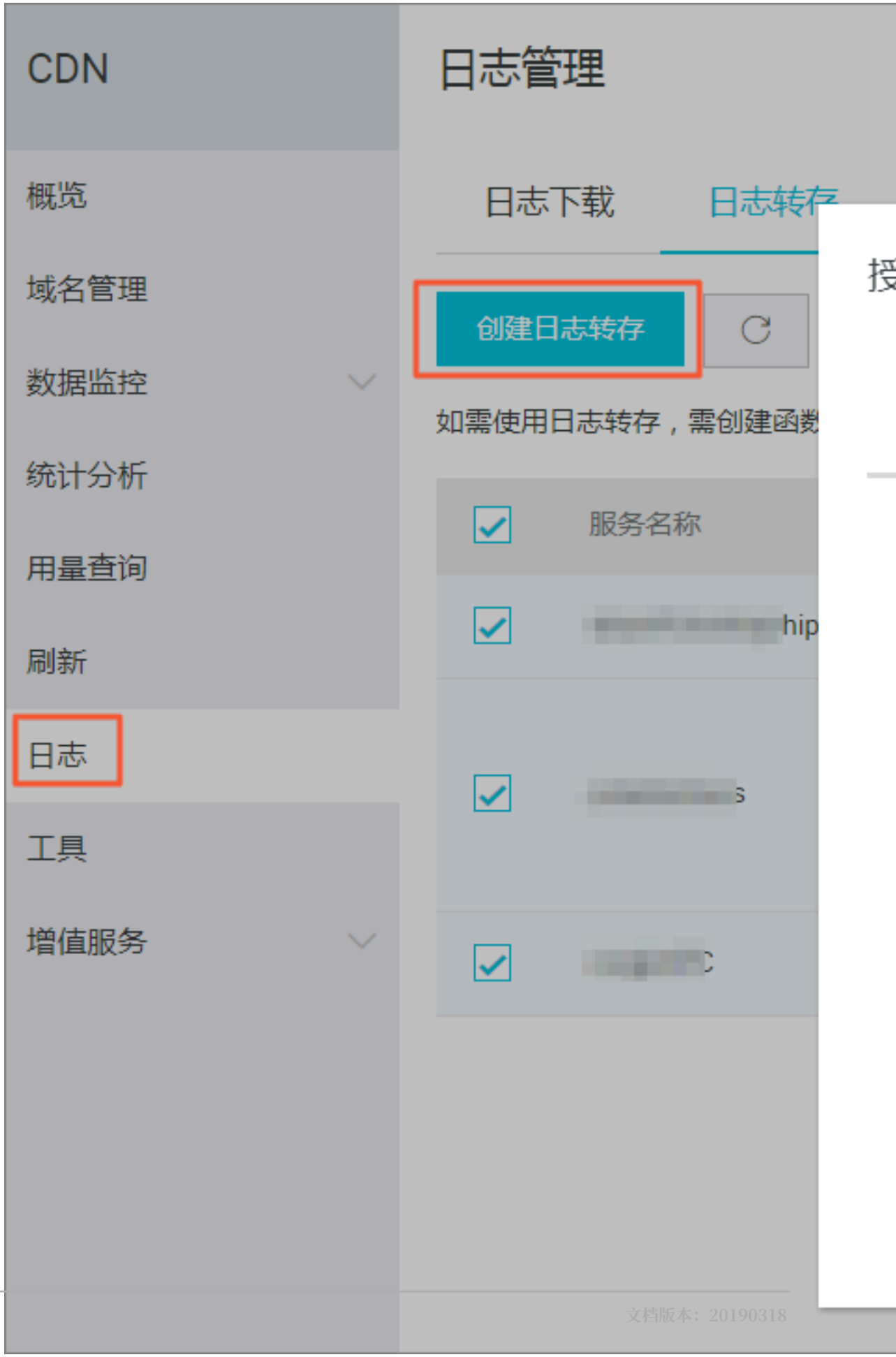
目前函数计算已经支持了多种CDN的场景，包括：日志转存、刷新、预热、资源封禁、域名添加和删除，域名启用和停用。触发这些场景的具体方式，请参考*CDN*事件触发器。

此外，函数计算已经和阿里云多个云产品联合使用，包括*OSS*、*VPC*、日志服务、*API*网关等，帮助您快速构建应用。

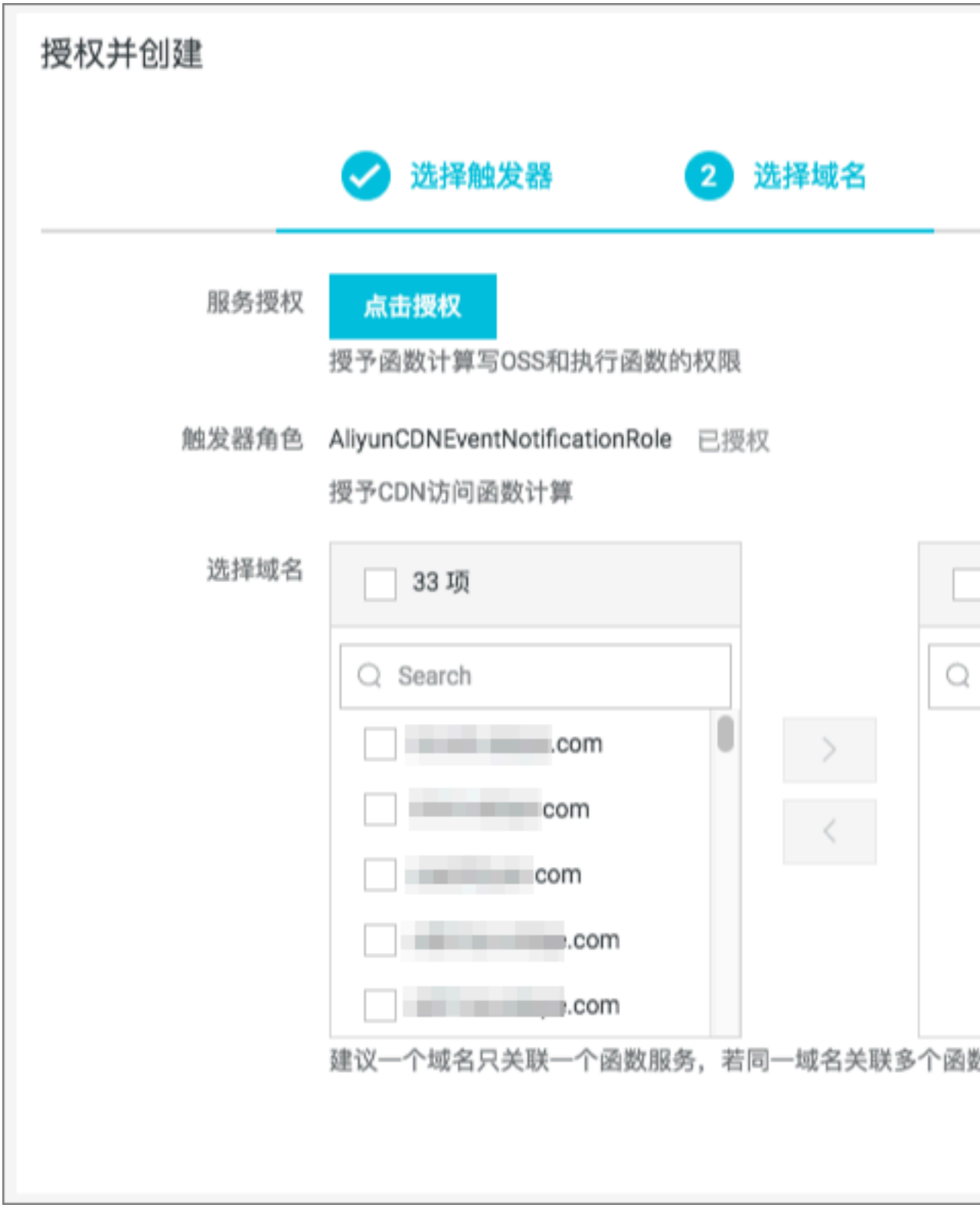
### 操作步骤

1. 登录CDN控制台，进入域名管理页面，选择需要设置的域名，单击管理。
2. 在日志管理 > 日志转存页面，单击创建日志转存。

3. 输入服务名称，选择OSS Bucket。然后单击下一步。



4. 单击点击授权，并选择域名关联函数服务。然后单击创建。



5. 单击完成。


## 10.3 实时日志

本文档介绍了实时日志的具体功能、功能优势、适用场景和具体的控制台操作。

### 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，为客户定制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CDN提供4类日志数据报表，包括：

- 基础数据：帮助您了解CDN网络的访问性能，通过该数据您可以快速了解到CDN整体的服务质量以及终端客户的访问效率，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：帮助你在加速域名访问出现异常时，快速定位是由于CDN服务本身出现的访问问题，例如源站访问出现故障，节点不可用等，还是由于终端用户的网络故障，或地域特性等问题。
- 热门资源数据：帮助您了解业务详情，分析出哪些是热门的访问地区，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：帮助您更好的了解你的用户构成，包括用户的热门访问省份，热门终端，热门用户等。

### 操作步骤

1. 登录CDN控制台。
2. 在左侧导航栏，单击日志。
3. 在日志页，单击实时日志推送。
4. 单击一键创建日志服务。
5. 配置Project、Logstore、地域等信息，然后单击下一步。
6. 选择关联域名并绑定，然后单击创建。

说明：

- 使用该服务前，你需要首先开通日志服务。
- 数据推送至logstore后，您可以直接查看4张报表，该已经内置在日志服务中，通过cdn打开查看报表可以默认查看。
- 迁移域名是指：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。
- 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。
- 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。

如果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，或提交工单。我们将根据您的意见提供更好的日志分析报表。

更多信息

关于CDN实时日志的发布讯息，请参考CDN的实时日志发布。

关于CDN实时日志的更多信息，请参考CDN的前世今生。

# 11 诊断工具

**控制台的工具页面提供IP地址检测工具，可以验证输入的IP是否为阿里云CDN节点的IP。**

# 12 图片鉴黄

## 产品介绍

- CDN图片鉴黄是CDN加速的一项增值服务，开通此功能后，用户在使用CDN服务过程中，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将会被记录下来供用户导出和删除。
- 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，同时用户还可以设置每日检测张数的上限，控制消费额度。
- CDN的图片鉴黄基于云计算平台，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。

## 使用方法

图片鉴黄功能可在CDN控制台的增值服务中使用：

1. 设置待检测域名和限额：首次进入未设置检测域名，CDN中的域名需要在设置中添加到检测列表才会开始检测：


单击马上设置后进入设置菜单：


- 检测域名的设置：在左侧选择要检测的域名，添加到右侧检测中的域名栏中。
- 最后点击确定保存后，云端即开始检测通过CDN加速的新增图片。

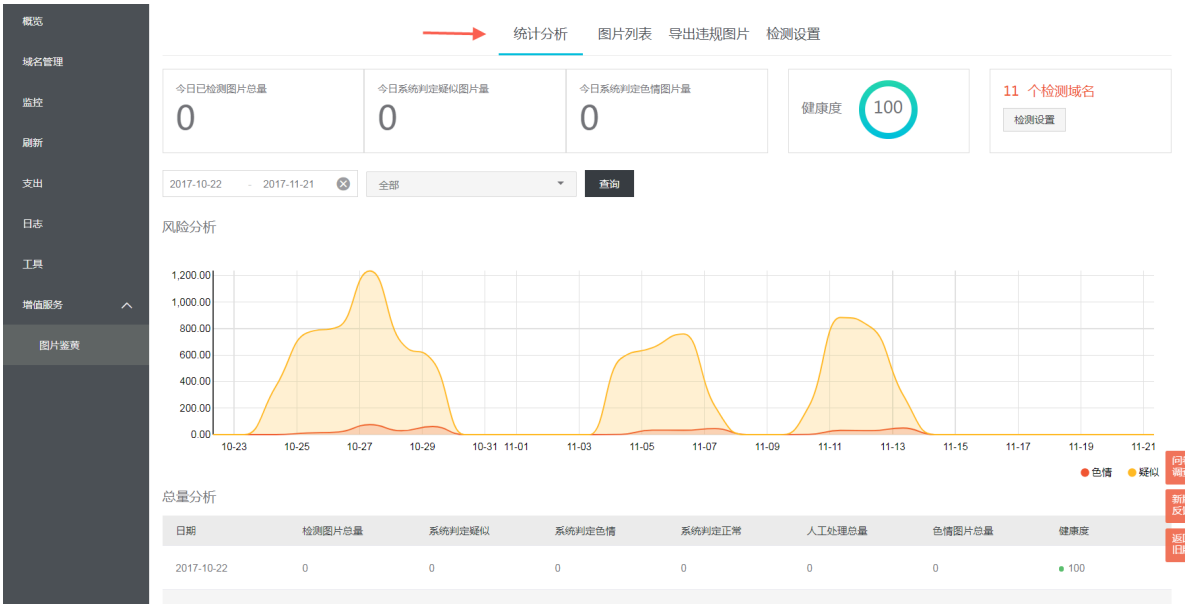
**说明：**

首次开通服务是第二天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，待下次用户通过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。

2. 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。

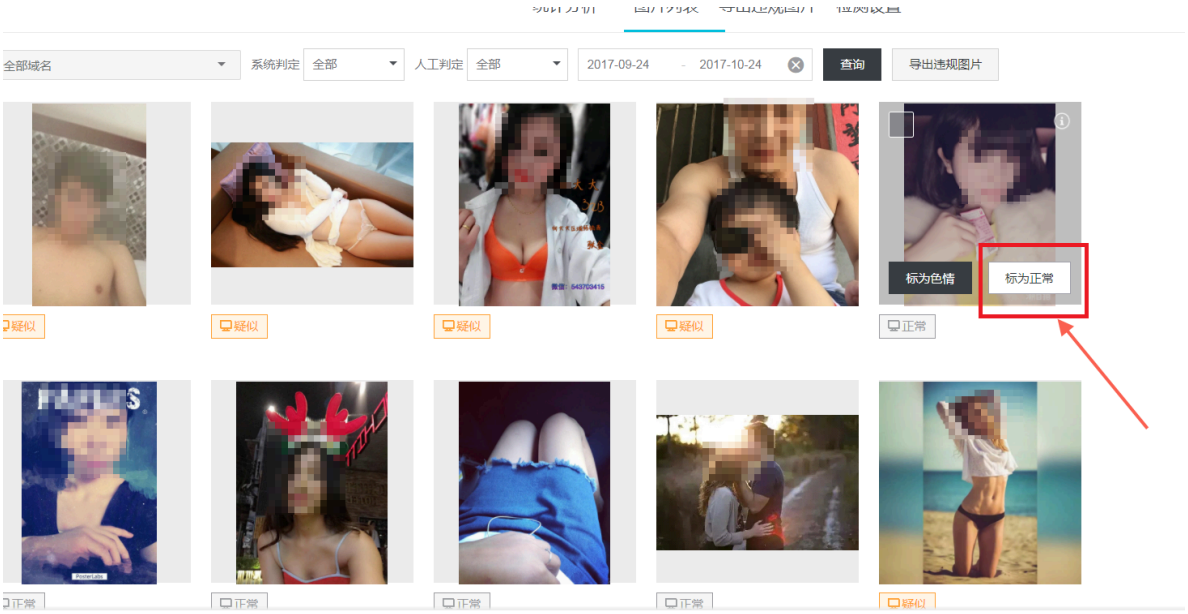
打开图片鉴黄菜单可以看到检测的统计数据信息，包括今日已检测的总量，疑似色情的图片量以及判定为色情的图片量：




单击图片列表标签可查看图片列表，选择查询条件可以筛选图片：


下方可以翻页，图片列表中可以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无法显示此图片）。

色情图片手工打标。 由于检测系统判定无法做到100%准确率，会有少量图片会识别成疑似色情或识别结果不对，此时可以通过手工打标的方式将图片打标为色情或正常。还可以同时选中多张图片批量打标：




3. 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，通过导出违规图片按钮将所有违规图片导出：


用户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。

## 产品定价

- 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；
  - 算法确定部分和待用户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） | 确定部分 单价（元/千张） | 待用户确认部分 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 |
| 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，待用户确认部分按照1：0.25抵扣。

# 13 CDN子账户使用指南

本文档提供给CDN域名资源组管理需求的客户，通过子账户+资源组授权实现不同部门之间资源的隔离操作，接入流程如下。

## 接入流程

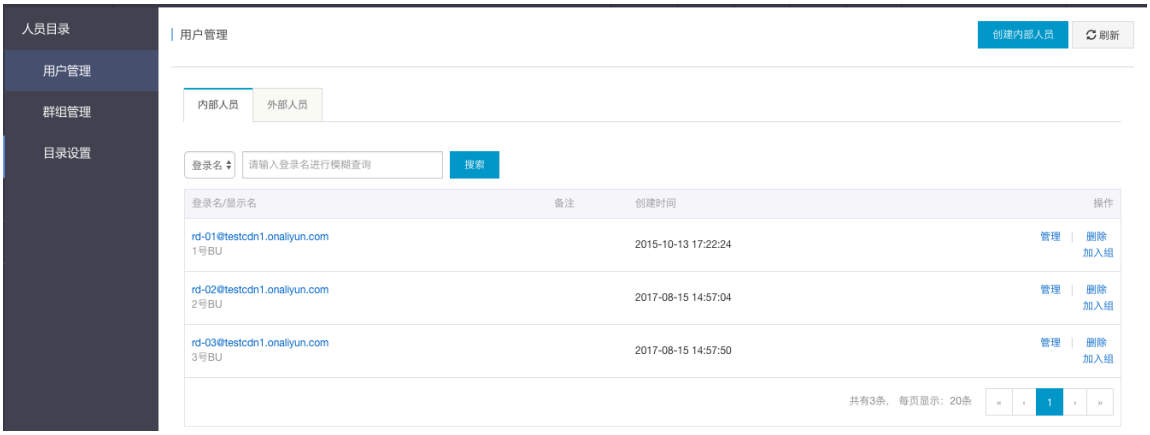
1. 登录企业控制台。

> **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。

使用主账号登录企业控制台（附：企业控制台使用手册）。

2. 创建子账户。

- 进入人员管理模块，初次进入需要创建目录,一个用户必须且只能归属于某一个目录下。
- 创建目录后，可以在人员管理 > 用户管理中创建子账户。

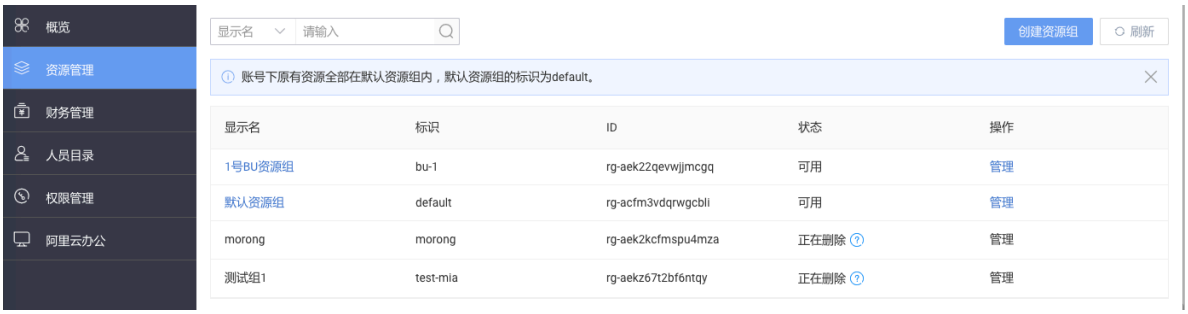



**说明:**

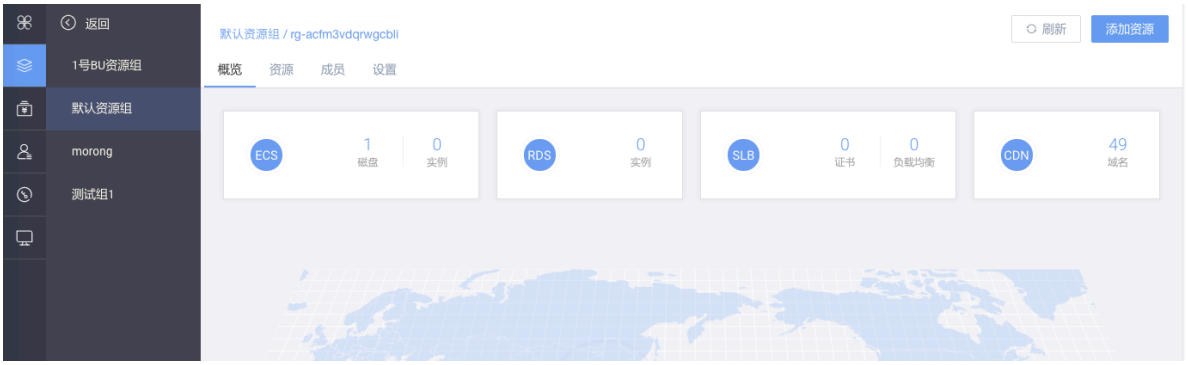
根据业务需求还可以创建群组，统一管理。

3. 创建资源组 + 授权。

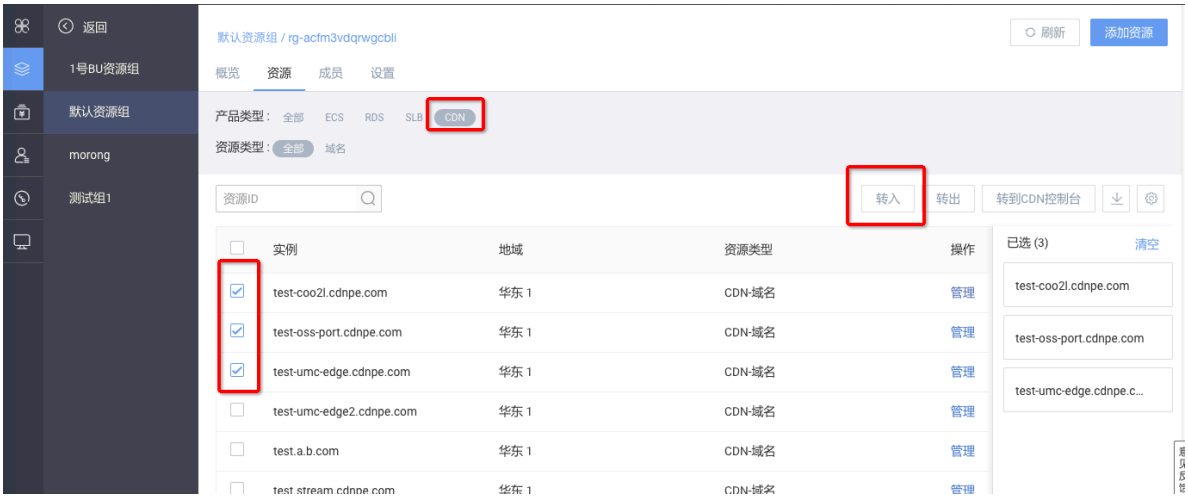
进入资源管理模块，创建资源组，如下创建 1号BU资源组。




择需要管理的资源组，完成该组内的资源、成员和基础信息设置。




进入资源管理 > 资源 实现加速域名分组设置，在筛选区选择产品CDN，勾选需要加入该资源组的加速域名，单击转入，完成资源组内加速域名设置。

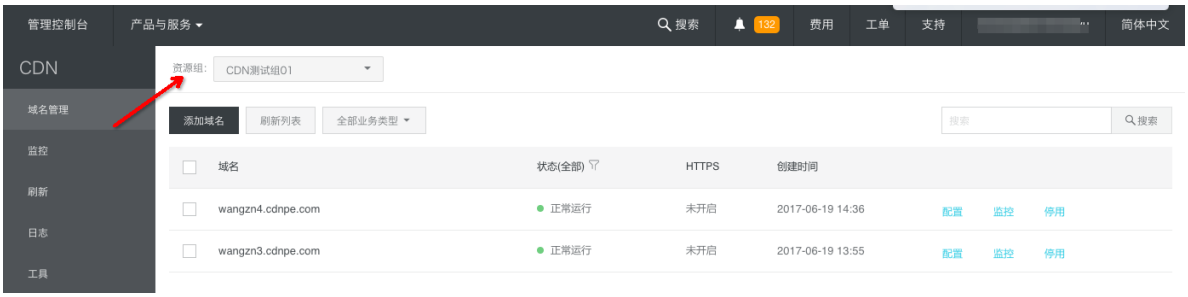



进入资源管理 > 成员完成子账户的授权，单击新增成员，可以选择需要管理本资源组的子账户，并完成策略授权，附：授权模板说明。


4. 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。




   自账户支持 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，请参考 快速入门。

## 附录

### 当前RAM模板策略

1. CDN管理授权：支持增删查改。

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

2. CDN只读权限。

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

```
      }
    ]
}
```

# 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}
```