# 阿里云
# CDN

## 用户指南

文档版本：20180803

# 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。 |
| 斜体 | 表示参数、变量。 | `bae log list --instanceid` *`Instance_ID`* |
| []或者[a\|b] | 表示可选项，至多选择一个。 | `ipconfig` *`[-all\|-t]`* |
| {}或者{a\|b} | 表示必选项，至多选择一个。 | `swich` *`{stand \| slave}`* |

# 目录

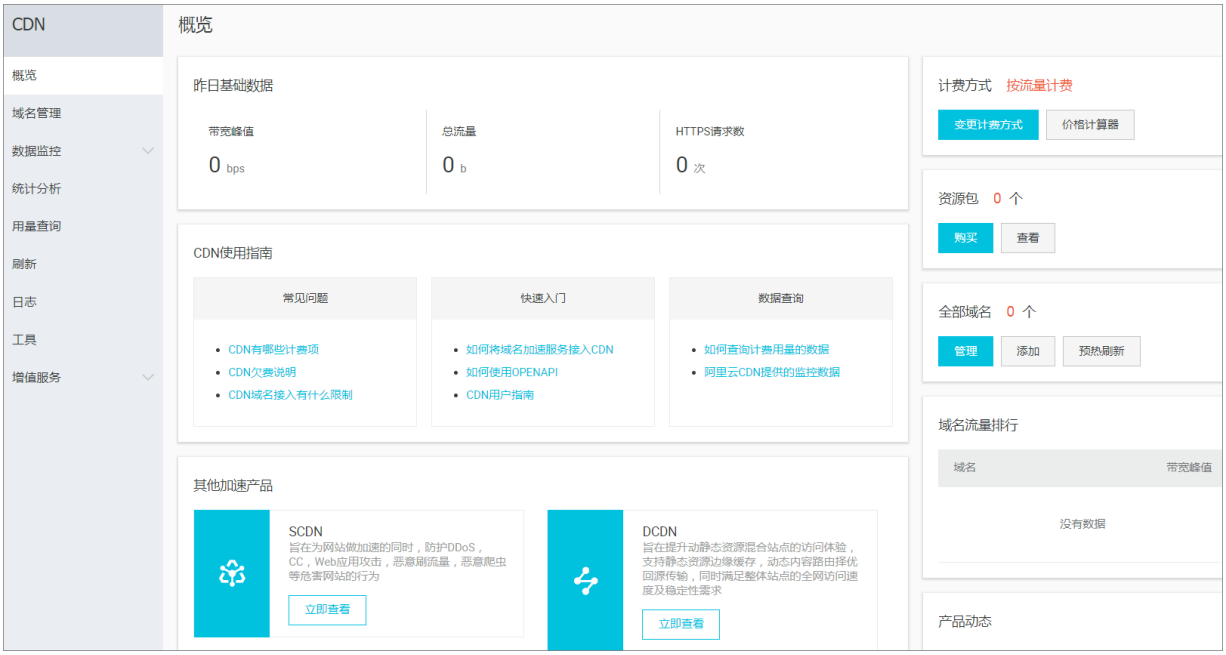
# 1 控制台介绍

## 快速开始

Alibaba Cloud CDN(内容分发网络)，建立并覆盖在承载网之上、由分布在不同区域的边缘节点服务器群组成的分布式网络，替代传统以WEB Server为中心的数据传输模式。CDN控制台可以帮助您完成添加CDN加速域名、刷新缓存等配置任务，也提供了实时数据分析的资源监控服务等。本文档主要介绍CDN控制台入门。

## CDN运行概况总览

登录到 *CDN控制台* 后，首页展示的就是当前账户下CDN运行概况总览情况，主要包括：




1. 计费类型展示及变更
2. 关键数据展示区，包含运行域名数、当月总流量等信息
3. 本月概览数据模块
   a. 加速域名产生的带宽峰值信息
   b. 按照下行流量累计值排名的Top4加速域名
   c. 访问加速资源的用户区域分布占比
   d. 用户访问加速资源的实时缓存命中率

> **说明：**
> 本月指自然月。

可以通过左侧的导航栏，完成相关的功能设置以及数据浏览：

| 功能 | 简述 |
| --- | --- |
| 域名管理 | 添加加速域名、管理或删除已有加速域名，并可以对加速域名基本信息和配置信息进行变更 |
| 监控 | 包含四部分，流量监控、用户访问监控、数据分析、安全防护 |
| 刷新 | 提供URL刷新和目录刷新两种方式 |
| 日志 | 日志下载、日志存储（即将上线）、云报表 |
| 工具 | 链路诊断工具、IP查询 |

# 2 CDN功能列表

**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 |

**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 |

**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 |
| 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 |

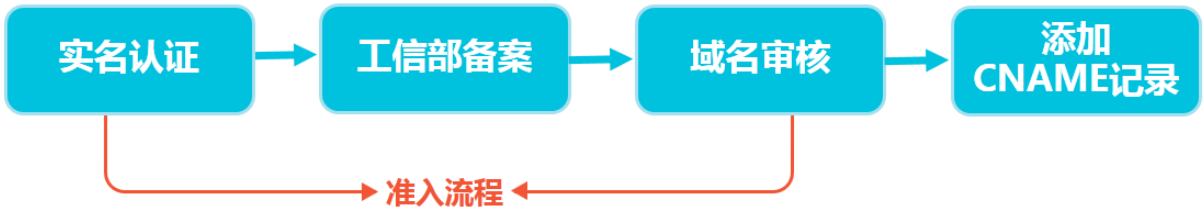
**其他设置**

| 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 域名准入标准

**CDN加速域名准入标准**

准入与生效流程




1. 实名认证：请登录阿里云官网完成。
2. 在工信部完成备案：推荐接入阿里云备案。
3. 在工信部完成备案：推荐接入阿里云备案。
4. 域名审核：加速域名的源站内容，您可以选择保存于ECS或OSS。如源站内容不在阿里云，接入前请联系人工审核。
5. 添加CNAME记录：将您的域名指向CDN生成的CNAME域名，即在DNS服务商处为您的域名添加CNAME记录，请参考如何配置*CNAME*。

> **说明：**
>
> - 如果你的源站部署在ECS上，请关注ECS带宽；建议您的带宽至少为你整体业务量的20%。
> - 源站安全软件设置中，请确保CDN缓存节点可访问源站。
> - 请确保CDN加速服务停止后，所有请求都将回源。
> - 添加完成配置后，你得到的CNAME域名不能直接访问，只能使用CNAME访问。
> - 对于大文件，不建议使用range：0~无穷大。

域名审核标准

所有接入CDN的域名都要经过审核。CDN目前不支持接入的加速域名类型包括但不限于:

- 无法正常访问或内容不含有任何实质信息
- 游戏私服类
- 传奇类游戏、纸牌类游戏
- 盗版软件等无版权下载网站
- P2P类金融网站
- 彩票类网站

- 违规医院和药品类网站
- 涉黄、涉毒、涉赌等
- 自动超时拒绝：您的域名因不符合CDN接入规则而拒绝，请您查看之前的反馈结果，合规后可再行申请提交审核。

属于以上违规内容的加速域名被攻击或者恶意下载导致的费用损失，阿里云CDN将不承担任何责任，全部损失将由您自行承担。

- 对于您已接入阿里云CDN的域名，会进行定期复审。如发现以上任何一种违规行为，系统将立即中止该域名的CDN加速，同时中止您所有域名的CDN服务。
- 若您的域名加速被无法正常访问或内容不含有任何实质信息理由拒绝，且您的业务又是合规业务，您可以开启一个工单，将网站的业务截图内容（截图包含该域名）通过工单发送。工单单独审核后，会告知您第二次的审核结果。

**数量限制**

| 数量 | 限制数量 |
| --- | --- |
| 数量 | 限制数量 |
| 域名 | 每个阿里云账户下，最多支持加速 **20**个 域名。 |
| IP源站 | 每个加速域名的默认IP源站数量限制为 **10**个IP地址。 |
| 缓存刷新类操作 | **URL**刷新：2000条/日/每账户。**目录刷新**：100个/日/每账户 |

如有大量域名加速需求，请提工单申请特殊支持。

**加速域名回收规则**

| 如果您的加速域名… | 系统会… | 如需继续使用**CDN**加速，您需要… |
| --- | --- | --- |
| 超过90天没有任何访问流量（包含处于“正常运行”状态） | 自动停用该域名仍保存该加速域名相关记录 | 启用加速域名。 |
| 处于“停用”状态超过120天（包含“审核未通过”状态） | 自动删除该域名相关记录 | 重新添加域名。 |

# 4 业务类型

## 4.1 类型1：图片小文件加速

应用场景介绍

网站或者应用的静态内容分发，例如各种类型的图像文件，html文件、flash动画、css、javascript文件等。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。

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：

   推荐配置：

   - *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

应用场景介绍

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

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：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。

   推荐配置

   - *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

应用场景介绍

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。

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。

   推荐配置

   - *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

应用场景介绍

为各类视频直播平台提供高性能稳定直播技术支持，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，FLV三种格式直播内容加速。

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：直播流媒体加速。

> 说明：
> 该业务类型不支持用户自定义直播中心服务器，统一采用阿里云CDN直播中心源站地址：**live-origin.alivecdn.com**。

2. 推流说明。

   推流地址

   ```
   rtmp://video-center.alivecdn.com/app-name/video-name?vhost=test.example.com
   ```

   控制台上的位置：在域名管理域选择用于直播的加速域名进行配置，进入配置页：


> 说明：
> - 默认推流数限制为20个
> - video-center.alivecdn.com是直播中心服务器域名，暂不支持自定义
> - app-name是应用名称，支持自定义：字母、数字、下划线组合，不要用特殊字符，可以更改，不能超过255个字符
> - video-name是流名称，支持自定义：字母、数字、下划线组合，不要用特殊字符，可以更改，不能超过255个字符
> - vhost参数是最终在边缘节点播放的域名，即你的加速域名（如示例中：test.example.com）。

3. 播流说明

根据上述中心推的流，边缘支持三种方式读：

| 方式 | URL |
| --- | --- |
| RTMP | `rtmp://test.example.com/app-name/video-name` |
| FLV | `http://test.example.com/app-name/video-name.flv` |
| M3U8 | `http://test.example.com/app-name/video-name.m3u8` |

控制台上的位置如下所示：


4. 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“直播流媒体”加速，推荐设置如下功能。

- 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。

> **说明：**
>
> - 目前采用推流播流采用同一套鉴权方案
> - 只有进行鉴权配置后，该加速域名才能正常进行推流和播流，当前直播业务类型仅支持A类型鉴权方式。

- 推流和播流地址需要分别进行鉴权签名计算，每一个签名都是严格按照URL计算的，故不可使用推流URL计算得到的签名应用到播流地址，同理每一种播流地址都会对应不同的鉴权计算结果
- 计算签名时的URL无需携带参数，例如计算推流鉴权签名时，无需携带`?vhost=test.yourcompany.com`

举例如下：

| 操作步骤 | 内容 |
| --- | --- |
| 资源URL | `rtmp://video-center.alivecdn.com/app-name/video-name` |
| 鉴权设置 | 鉴权方式：A方式鉴权Key：test123有效时间3600s |
| 推流地址 | `rtmp://video-center.alivecdn.com/app-name/video-name?auth_key=1449030595-0-0-dee5f3819d7b62a9830ee2913caf111c&vhost=test.example.com` |
| 播流地址（以FLV格式为例） | `http://test.example.com/app-name/video-name.flv?auth_key=1449030834-0-0-5e1c604710241001fd7a367bc96a17b7` |

- *Notify_URL*设置，流状态实时反馈，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，默认返回 1 表示接收成功；0代表接收失败。

## 4.5 类型6：移动加速

# 5 增值服务

# 6 域名管理

## 6.1 HTTPS安全加速

### 6.1.1 HTTPS安全加速设置

**功能介绍**

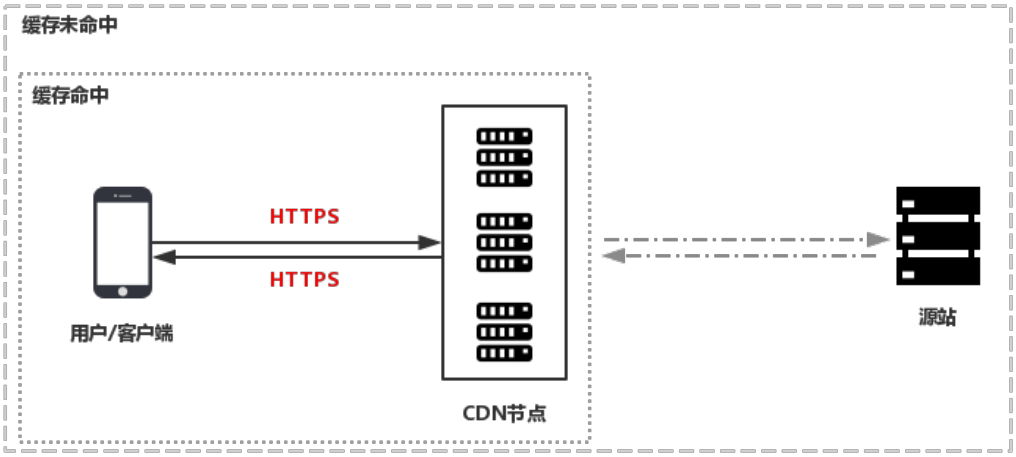
- HTTPS是以安全为目标的HTTP通道，简单讲是HTTP的安全版。即将HTTP用SSL/TLS协议进行封装，HTTPS的安全基础是SSL/TLS。
- HTTPS加速优势：
  - 传输过程中对用户的关键信息进行加密，防止类似Session ID或者Cookie内容被攻击者捕获造成的敏感信息泄露等安全隐患；
  - 传输过程中对数据进行完整性校验，防止DNS或内容遭第三方劫持、篡改等中间人攻击（MITM）隐患，了解更多使用HTTPS防止流量劫持。
- 阿里云CDN 提供HTTPS安全加速方案，仅需开启HTTPS后上传证书和私钥，并支持对证书进行查看、停用、启用、编辑操作。用户自定义上传的证书仅支持PEM格式的证书，具体请看 证书格式说明及转化方法。
- 您可以在 阿里云云盾快速申请免费的证书或购买高级证书。
- 证书配置正确及开启状态，同时支持HTTP访问和HTTPS访问；证书不匹配或者停用证书，仅支持HTTP访问。

**说明：**

目前不支持sni 回源。

**功能示意图**

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：




注意事项

配置相关

- 支持开启**HTTPS**安全加速功能的业务类型为：
  - 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
  - 暂不支持移动加速业务类型
- 支持泛域名HTTPS服务。
- 支持该功能的**停用**和**启用**：
  - 启用：支持修改证书，默认兼容用户的HTTP和HTTPS请求，支持**强制跳转**设置。
  - 停用：不支持HTTPS请求且将不再保留证书/私钥信息，再次开启证书，需要重新上传证书/私钥。
- 允许用户查看证书，但是只支持查看证书，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。
- 支持修改编辑证书，但注意生效时间大约为10分钟，请慎重操作。

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HTTPS服务导致欠费影响CDN服务。
> - 附：如何查看*HTTPS*请求数使用情况。

证书相关

- 开启**HTTPS**安全加速功能的加速域名，须要上传证书，包含证书/私钥，均为 PEM 格式。

  > 说明：
  > CDN采用的Tengine服务是基于Nginx的，因此只支持Nginx能读取的证书，即PEM格式)。具体请看 证书格式说明及转化方法。

- 只支持带SNI信息的SSL/TLS握手。
- 用户上传的证书和私钥要匹配，否则会校验出错。
- 更新证书的生效时间约为10分钟。
- 不支持带密码的私钥。

配置引导

1. 购买证书。开启HTTPS安全加速，需要您具备匹配加速域名的证书，可以在 阿里云云盾 快速申请免费的证书或购买高级证书。
2. 加速域名配置。

   登录*CDN*控制台，进入CDN域名列表页，选择域名进入配置页面，HTTPS设置，修改配置。


   单击修改配置，可以进行相应设置：


1. 确认当前域名**HTTPS**设置是否开启，单击**修改配置**按钮进入设置界面并开启。

   > **说明：**
   > HTTPS安全加速属于增值服务，开启后将产生HTTPS请求数计费，了解计费详情。

2. 选择证书：

   - 可在 阿里云云盾证书服务快速申请免费证书或购买高级证书， 云盾的证书，可以通过证书名称直接选择适配该加速域名；
   - 若证书列表中无当前适配的证书可以选择自定义上传，需要设置证书名称后上传证书内容和私钥，该证书将会在“云盾证书服务”中保存，可以在**我的证书**部分查看。

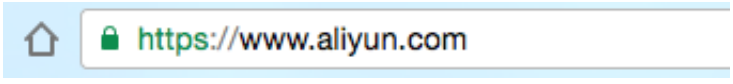
3. 仅支持 PEM 的证书格式。具体请看 证书格式说明及转化方法。

4. 支持**设置强制跳转**：自定义将用户的原请求方式进行强制跳转：

   - 例如开启**强制HTTPS跳转**后，用户发起了一个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。
   - 默认：兼容用户的HTTP和HTTPS请求。
   - 强制HTTPS跳转：用户的请求将强制重定向为HTTPS请求。
   - 强制HTTP跳转：用户的请求将强制重定向为HTTP请求。

3. 验证证书是否生效。

   设置完成待证书生效后（设置HTTPS证书后约1小时后生效），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。



# 6.1.2 证书格式说明

在您 开启*HTTPS* 服务之前，需要配置证书。您可以直接选择在 阿里云云盾 托管或购买的证书，免费证书或自行上传自定义证书。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

- 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**

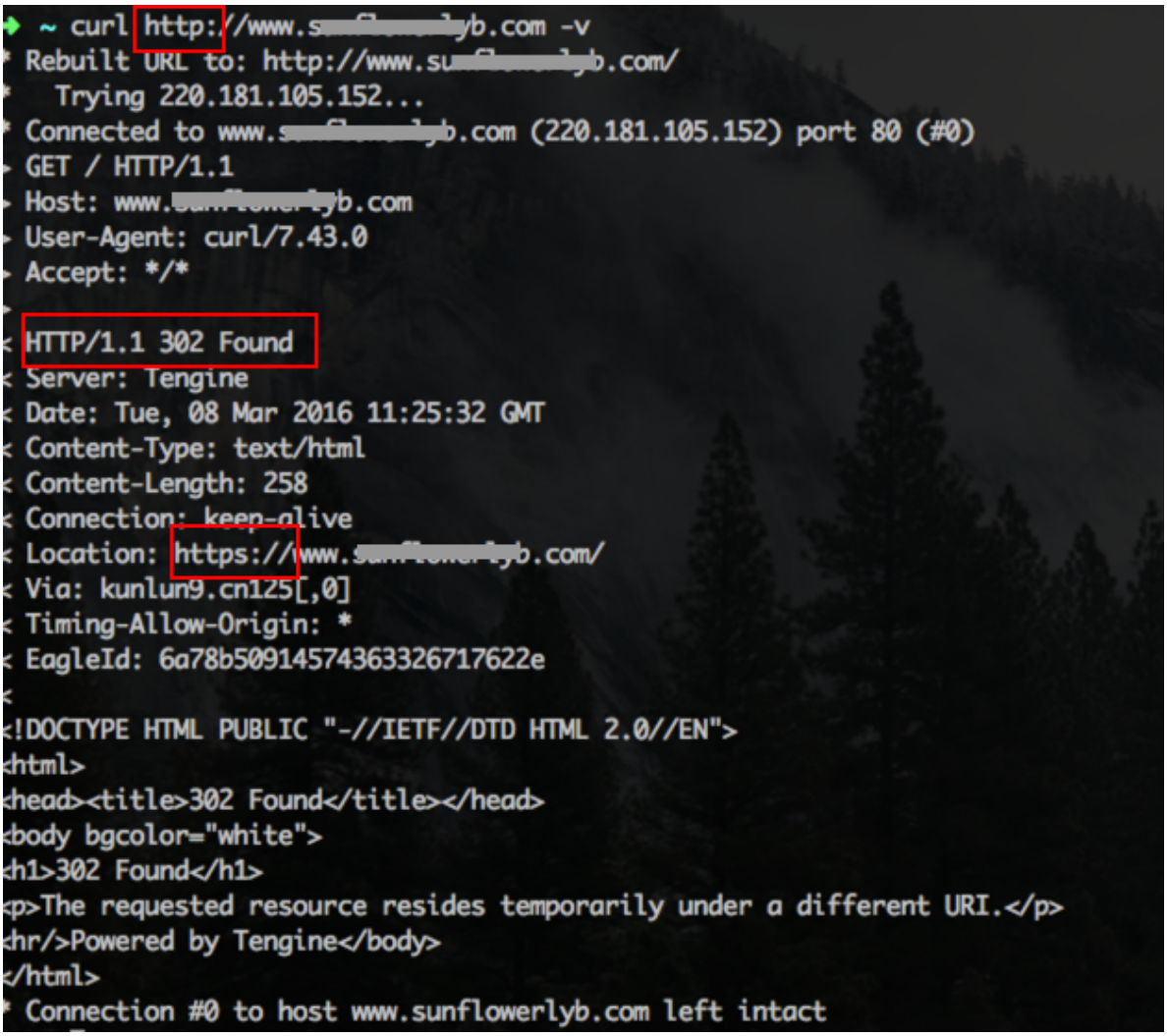
- 您可以停用、启用和修改证书。停用证书后，系统将不再保留证书信息。再次开启证书时，需要重新上传证书或私钥。请参考*HTTPS安全加速设置*。
- 只支持带SNI信息的SSL/TLS“握手”。
- 请确保上传的证书和私钥匹配。
- 更新证书的生效时间为10分钟。
- 不支持带密码的私钥。

其他证书相关的常见问题，请见更多证书问题。

## 6.1.3 强制跳转

**功能介绍**

- 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。
- 例如开启强制**HTTPS**跳转后，用户发起了一个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：




注意事项

- 仅支持启用**HTTPS**安全加速功能后设置，同时支持HTTP和HTTPS方式的请求。
- 默认为不强制跳转。

配置引导

- 强制跳转为可选配置项，默认设置同时支持HTTP和HTTPS方式的请求。
- 可选项分别是：默认、强制**HTTPS**跳转、强制**HTTP**跳转。

  — 强制**HTTPS**跳转：用户的请求将强制重定向为HTTPS请求。

  — 强制**HTTP**跳转：用户的请求将强制重定向为HTTP请求。

- 变更配置：

  CDN域名管理页，选择域名进入配置页面，HTTPS设置，强制跳转，修改配置， 在设置页底部可设置强制跳转类型。


## 6.1.4 HTTP/2

什么是**HTTP/2**？

HTTP/2是最新的HTTP协议，已于2015年5月份正式发布， Chrome、 IE11、Safari以及Firefox 等主流浏览器已经支持 HTTP/2协议

HTTP/2优化了性能而且兼容了HTTP/1.1的语义，其几大特性与SPDY差不多，与HTTP/1.1有巨大区别，比如它不是文本协议而是二进制协议，而且HTTP头部采用HPACK进行压缩，支持多路复用、服务器推送等等。

**HTTP/2的优势**

- 采用二进制协议
- 头部压缩：HTTP/2消息头采用HPACK格式进行压缩传输，并对消息头建立索引表，相同的消息头只发送索引号，从而提高效率和速度。
- 多路复用：在HTTP/2中，不用按照次序一一对应，而且并发的多个请求或者响应中任何一个请求阻塞了不会影响其他的请求或者响应，这样就避免了“队头堵塞”。
- 服务器推送：在HTTP/2中服务器未经请求可以主动给客户端推送资源，大大提高了网页加载的速度。
- 安全：HTTPS将是未来的趋势，HTTP/2基于HTTPS也是未来的趋势，安全也是HTTP/2的重要特性之一。

如何开启**HTTP/2**？

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，需要等到证书配置完成并且证书生效后，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。

如何设置：

进入域名配置 > **HTTPS**设置 > **HTTP/2**设置，单击修改配置：


单击打开后，保存即可。

# 6.2 内容回源设置

## 6.2.1 多源优先级设置

设置多源优先级

功能介绍

阿里云CDN支持三种类型回源域名，包括oss回源域名、IP和自定义域名。其中IP和自定义域名支持多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。

当用户选择的回源源站类型为IP或自定义域名时，可设置多个源站，并为多源站设置优先级。添加多源站时，源站优先级为“主”和“备”，优先级为“主”>“备”。

用户100%回源流量都将首先回源优先级高的源站，如果某个源站健康检查连续3次都是失败的话，则100%的流量都将选择优先级第二的源站回源。如果主动健康检查成功的话，该源站就会重新标记为可用，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，每5秒主动健康检查源站一次。

主要支持场景：主备方式切换源站

配置说明

进入CDN域名管理列表页，选择相应域名进入配置页面，可在回源设置里，设置**多源优先级功能**。

1. 从域名列表单击 **配置**，在域名配置页面打开源站设置功能。
2. 设置回源源站 和 优先级。
   - 如果您选择的源站信息为 **IP** 或 **源站域名**，则您仍然按照外网流量标准进行计费。
   - 如果您选择的源站信息为 **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。
3. 设置完成后，单击**确认**，设置成功。


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。

**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。

**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。

## 6.2.2 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。

**说明：**

- 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。
- 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。
- 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。

**配置说明**

如何开启私有bucket回源授权？

1. 域名配置，源站设置，单击私有**Bucket**回源设置 > 开启。

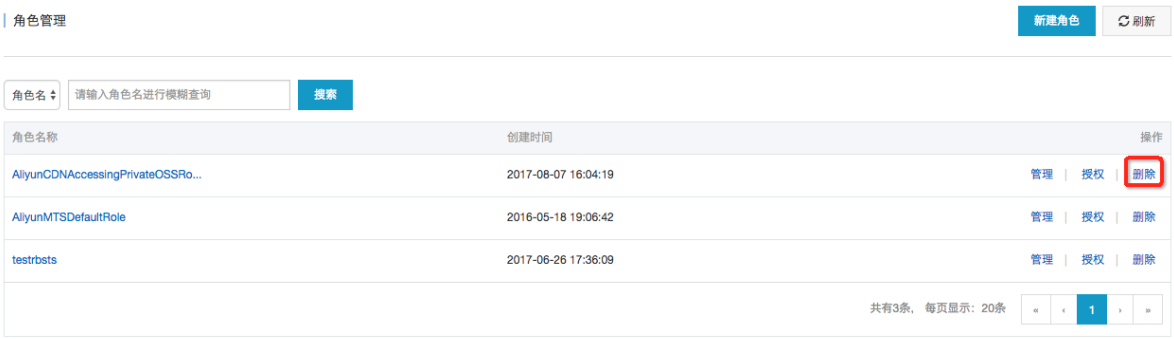

2. 单击立即授权。


3. 授权成功，为该域名开启私有bucket回源配置，单击确定。

4. 设置成功。

如何关闭私有bucket回源授权？

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。

> 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。

## 6.2.3 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**

进入CDN域名管理列表页，选择相应域名进入配置页面，可在回源设置里，开启或关闭协议跟随回源功能。


## 6.2.4 回源HOST

### 功能介绍

自定义在CDN节点回源时所需访问的具体域名（如果您 一个IP源站绑定了多个域名/站点的时候，就需设置回源**Host**指定回到具体哪个域名，否则会回源失败）。

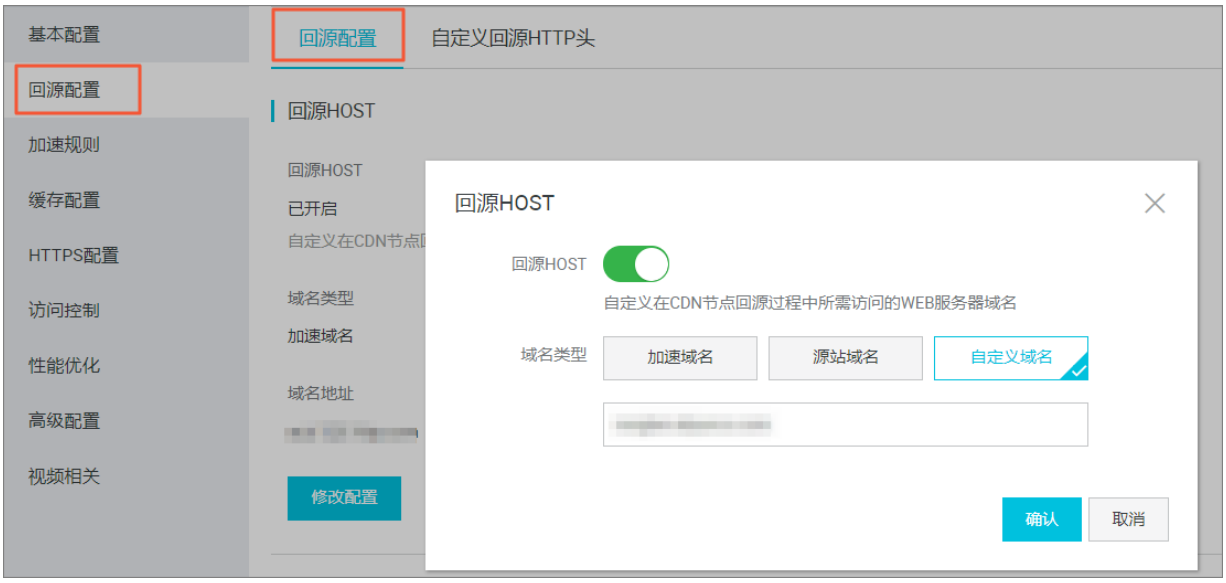
- 回源**host**为可选配置项，默认值为：
  - 如果源站是 **IP**类型，回源host默认加速域名。
  - 如果源站是 **OSS**源站类型，回源host默认是源站域名。
- 可选项分别是：加速域名、源站域名、自定义域名。

**说明：**

目前不支持sni 回源。

### 配置引导

变更配置：进入CDN域名管理页，选择域名进入配置页面，回源设置，可修改回源host的配置。




源站和回源host的区别（一个IP/主机是能绑定 多个域名/站点的，因此需要通过设置回源Host指定回源时回到哪个域名/站点）：

- 源站： 源站决定了回源时，请求到哪个IP。
- 回源host：回源host决定回源请求访问到该IP上的哪个站点。（如果您 一个IP源站 绑定了 多个域名/站点时，就需设置 回源**Host** 指定回源到具体哪个域名，否则会回源失败）。

**说明：**

- 例一：源站是域名源站为`www.a.com`回源host设置为`www.b.com`， 那么实际回源是请到m `www.a.com`解析到的IP上对应的具体的站点：`www.b.com`。
- 例二：源站是IP源站为`1.1.1.1` 回源host设置为`www.b.com`那么实际回源的是`1.1.1.1`上对应的具体站点：`www.b.com`

## 6.2.5 回源HOST

**功能介绍**

自定义在CDN节点回源过程中所需访问的WEB服务器域名。

源站： 源站决定了回源时，请求到哪个IP。

回源**host**：回源host决定回源请求访问到该IP上的哪个站点。

- 例一：源站是域名源站为`www.a.com` 回源host为`www.b.com`。 那么实际回源是请求到`www.a.com` 解析到的IP，对应的主机上的站点`www.b.com`。

- 例二：源站是IP源站为`1.1.1.1`回源host为`www.b.com` 那么实际回源的是`1.1.1.1`对应的主机上的 站点`www.b.com`。

> 说明：
> 目前不支持sni 回源。

配置引导

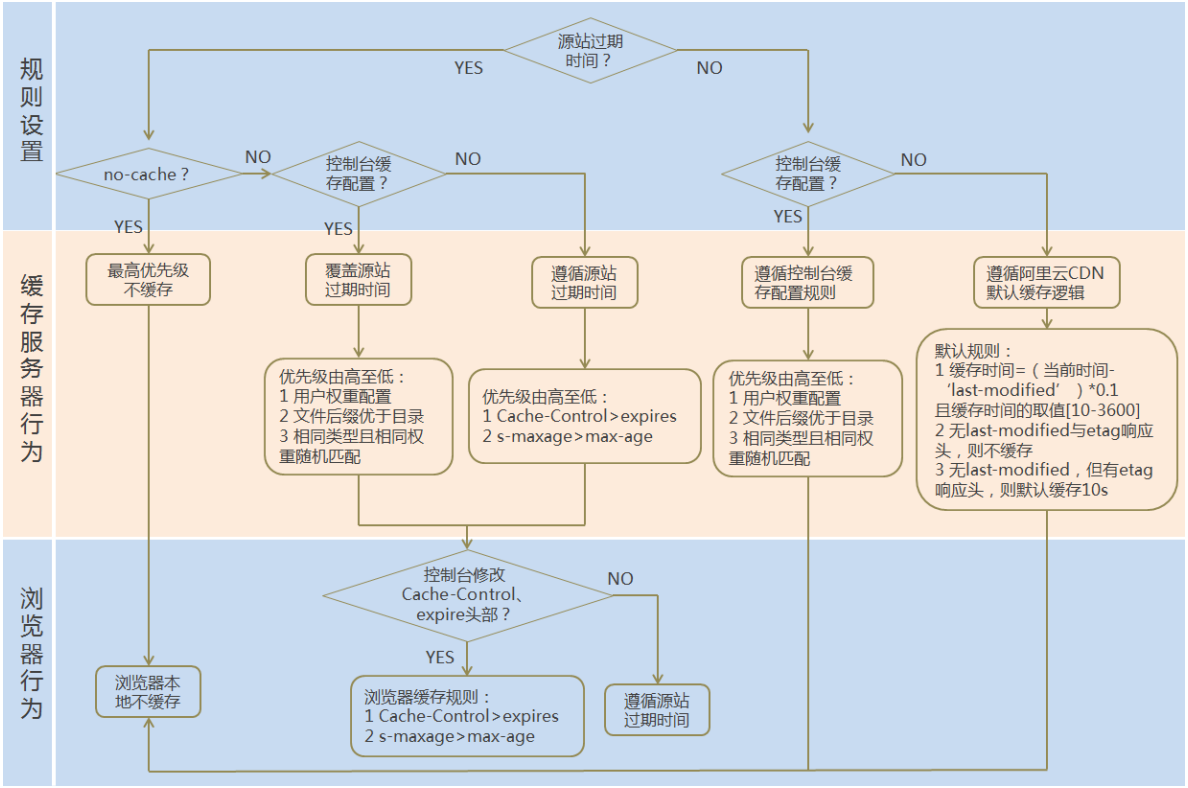
- 回源**host**为可选配置项，默认值为：
  - 如果源站是**IP**类型，回源host默认加速域名。
  - 如果源站是**OSS**源站类型，回源host默认是源站域名。
- 可选项分别是：加速域名、源站域名、自定义域名。
- 变更配置：进入CDN域名管理页，选择域名进入配置页面，回源设置，可修改回源host的配置。


# 6.3 节点缓存设置

## 6.3.1 缓存配置

功能介绍

- 该功能可以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。
- 支持用户自定义缓存策略优先级。
- Cache的默认缓存策略。




**说明：**

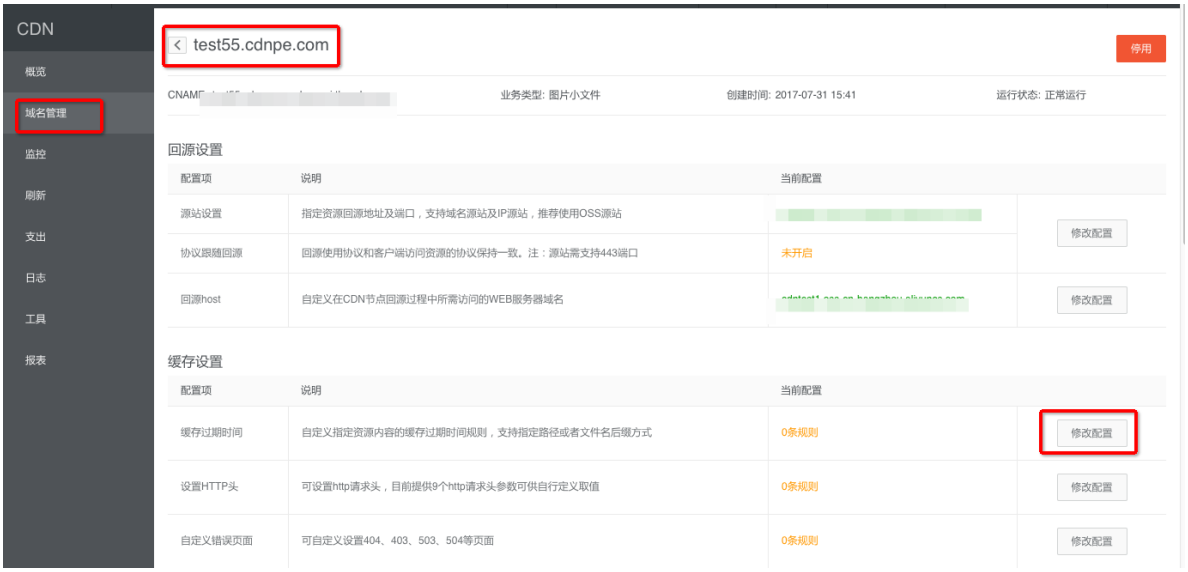
- 用于配置文件过期时间，在此配置的优先级会高于源站配置。如果源站未配置cache配置，支持按目录、文件后缀两种方式设置（支持设置完整路径缓存策略）。
- 了解详细*CDN节点默认缓存策略*。
- CDN的缓存是有可能由于热度较低被提前剔除出CDN节点的。

**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。

## 配置引导

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。

## 6.3.2 自定义错误页面

**功能介绍**

客户可以自行定义状态码时返回的页面，优化用户体验。提供三种选项：默认页面、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主题 404 页面，查看公益*404*页面。

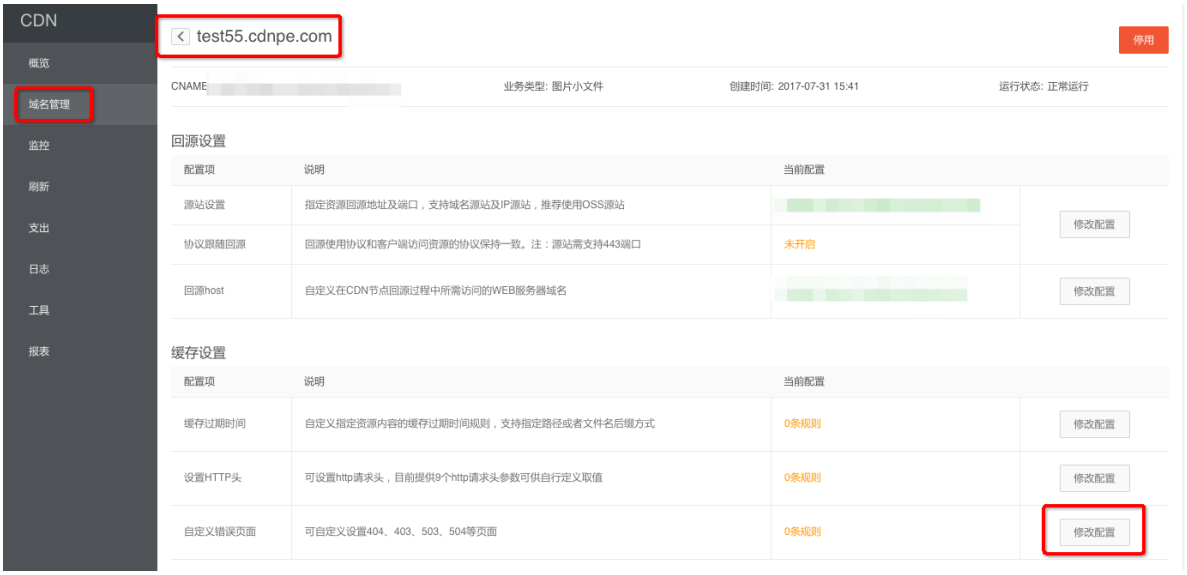
- 自定义404，http 响应返回 404 时，将会跳转到自行设计和编辑的 404 页面，需要自定义跳转页的完整URL地址。

注意事项

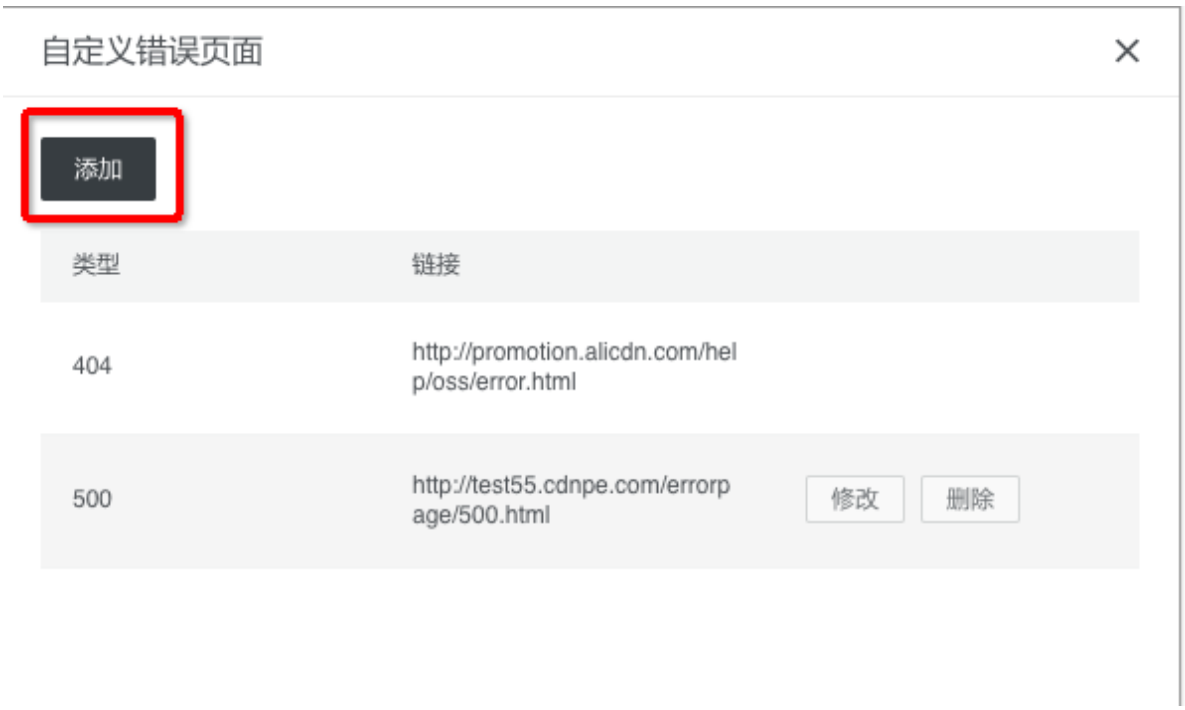
- 公益 404 页面属于阿里云公益资源，不会造成用户的任何流量费用，完全免费。
- 自定义页面属于个人资源，按照正常分发计费。

配置引导

1. 进入CDN域名概览页，选择域名进入域名配置页面，设置自定义错误页面功能。




2. 单击修改配置，可以查看和管理当前自定义错误页面列表。



3. 单击添加，增加自定义返回码的页面内容。


若选择自定义 **404**选项，将该页面资源如其他静态文件一样存储到源站域名下，并通过加速域名访问即可，只需填写完整的加速域名URL（包含http://）。

例如：加速域名为 `exp.aliyun.com`404页面为`error404.html` ，并将`error404.html`页面存储到源站中选择“自定义404”，填写： `http://exp.aliyun.com/error404.html` 即可。

## 6.3.3 设置HTTP头

**功能介绍**

可设置http响应头，目前提供9个http请求头参数可供自行定义取值，参数解释如下：

| 参数 | 解释 |
| --- | --- |
| Content-Type | 指定客户程序响应对象的内容类型 |
| Cache-Control | 指定客户程序请求和响应遵循的缓存机制 |
| Content-Disposition | 指定客户程序响应对象时激活文件下载设置默认的文件名 |
| Content-Language | 指定客户程序响应对象的语言 |
| Expires | 指定客户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-Methods | 指定允许的跨域请求方法 |

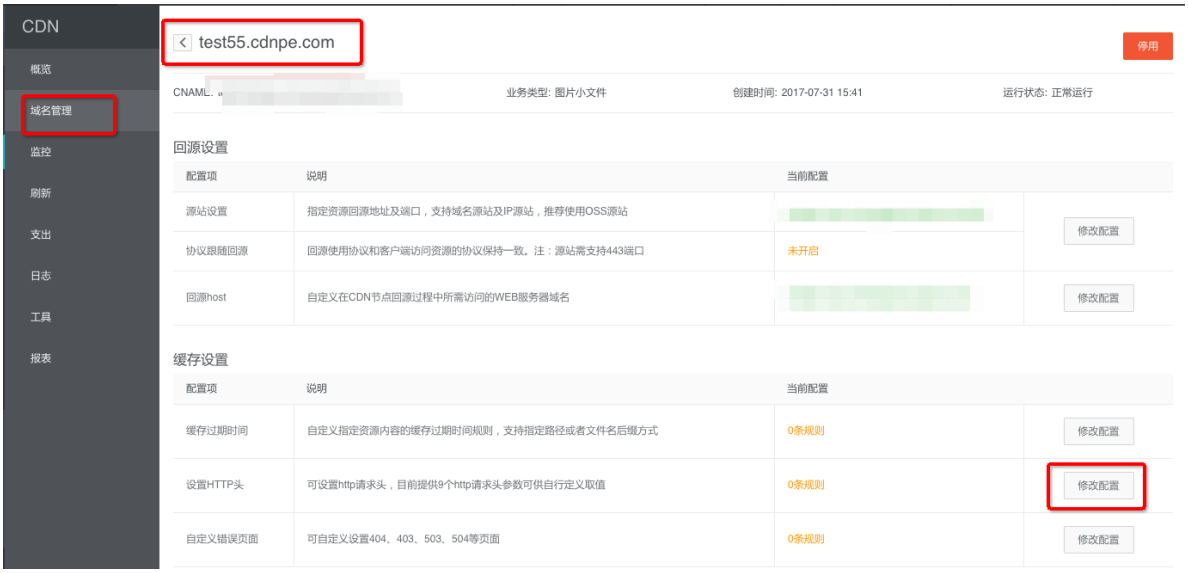
| 参数 | 解释 |
| --- | --- |
| Access-Control-Max-Age | 指定客户程序对特定资源的预取请求返回结果的缓存时间 |
| Access-Control-Expose-Headers | 指定允许访问的自定义头信息 |

注意事项

- HTTP响应头的设置会影响该加速域名下所有资源的客户程序（例如浏览器）的响应行为，而不会影响缓存服务器的行为。
- 目前仅支持这些http头参数取值设置，有其他HTTP头部设置需求，请提工单反馈。
- Access-Control-Allow-Origin参数的取值，支持*(表示全部域名)或者完整域名例如：`www.aliyun.com`；目前不支持泛域名设置。

配置引导

1. CDN域名概览页，选择域名进入**域名配置**页面，设置HTTP头。




2. 单击**修改配置**，可以管理当前http header的规则列表。


3. 单击添加，增加HTTP HEADER自定义设置。


## 6.4 访问控制设置

# 6.4.1 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，该访客请求被禁止，返回403响应码。

## 注意事项

- 可选配置，默认不启用。
- 开启功能，选择编辑refer黑名单或者白名单，黑白名单互斥，同一时间只支持一种方式。
- 支持设置是否允许空 Referer 字段访问CDN资源。（即允许通过浏览器地址栏直接访问资源URL）。
- 配置后会自动添加泛域名支持，例如填写a.com，最终配置生效的是*.a.com，所有子级域名都会生效。

## 配置引导

进入CDN域名概览页，进入域名管理页面，选择需要设置的域名，单击配置。



## 6.4.2 IP黑名单

### 功能介绍

支持黑名单规则，添加了黑名单的IP，表示此IP无法访问当前加速域名。

### 注意事项

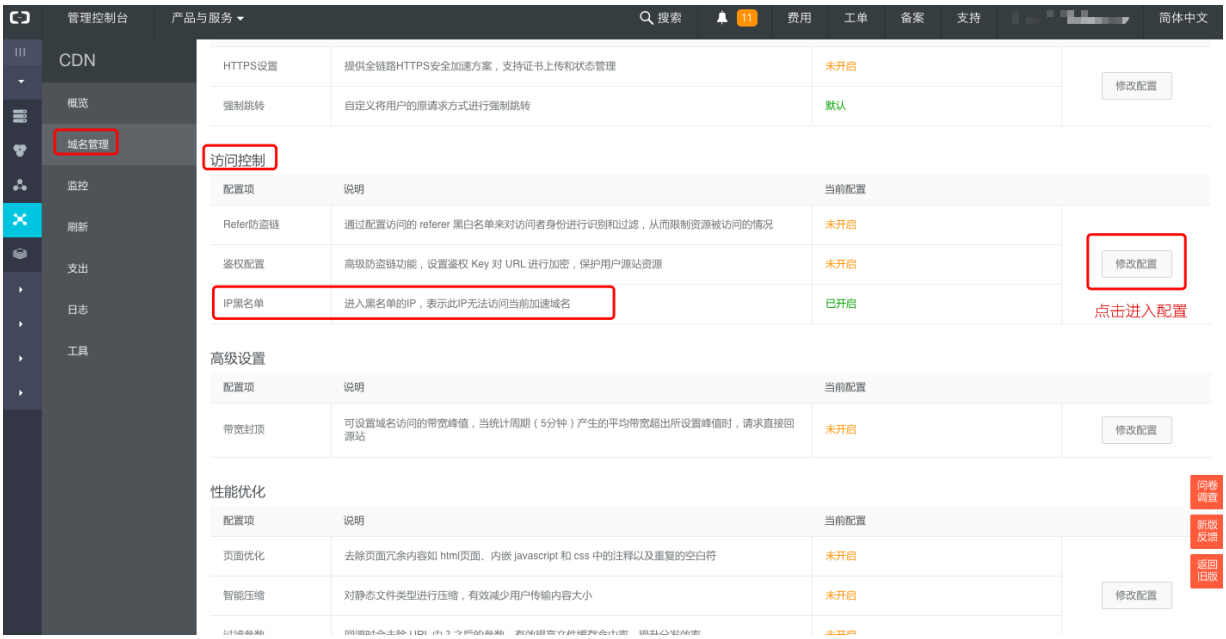
IP黑名单当前支持ip网段添加，例如127.0.0.1/24。

> **说明：**
> 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。

### 配置引导

进入CDN域名概览页，进入域名管理页面，选择需要设置的域名，单击配置。


管理控制台
产品与服务
搜索
费用
工单
备案
支持
简体中文
CDN
概览
域名管理
监控
刷新
支出
日志
工具
域名
状态(全部)
HTTPS
创建时间
test123456.aliyun.com
1.确认配置加速域名
正常运行
未开启
2017-07-26 15:22
配置
监控
停用
2.点击进入配置
批量配置
启用
停用


HTTPS设置
提供全链路HTTPS安全加速方案，支持证书上传和状态管理
未开启
强制跳转
自定义将用户的原请求方式进行强制跳转
默认
修改配置
访问控制
配置项
说明
当前配置
Refer防盗链
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，从而限制资源被访问的情况
未开启
鉴权配置
高级防盗链功能，设置鉴权 Key 对 URL 进行加密，保护用户源站资源
未开启
IP黑名单
进入黑名单的IP，表示此IP无法访问当前加速域名
已开启
修改配置
点击进入配置
高级设置
带宽封顶
可设置域名访问的带宽峰值，当统计周期（5分钟）产生的平均带宽超出所设置峰值时，请求直接回源站
未开启
性能优化
页面优化
去除页面冗余内容如 html页面、内嵌 javascript 和 css 中的注释以及重复的空白符
智能压缩
对静态文件类型进行压缩，有效减少用户传输内容大小


访问控制
规则
多个参数请使用西文逗号分隔开，总数不超过100个
允许通过浏览器地址栏直接访问资源URL
IP黑名单
黑名单
开启
3.选择开启或者关闭，默认开启
规则
127.0.0.1/24
4.填写黑名单的IP，支持ip网段添加
URL鉴权设置
鉴权说明
鉴权URL计算器
鉴权配置
开启
关闭
类型
A方式
B方式
C方式
主KEY
备KEY
注意不要有空格
取消
确定
5.点击“确定”保存设置

## 6.4.3 鉴权概述

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、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，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。

### 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**。

## 6.4.4 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 = 80cd3862d699b7118eed99103f2a3a4f 值一致，则鉴权通过。

## 6.4.5 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 |

| 字段 | 描述 |
| --- | --- |
| 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。

## 6.4.6 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。

## 6.4.7 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()
```

## 6.5 性能优化设置

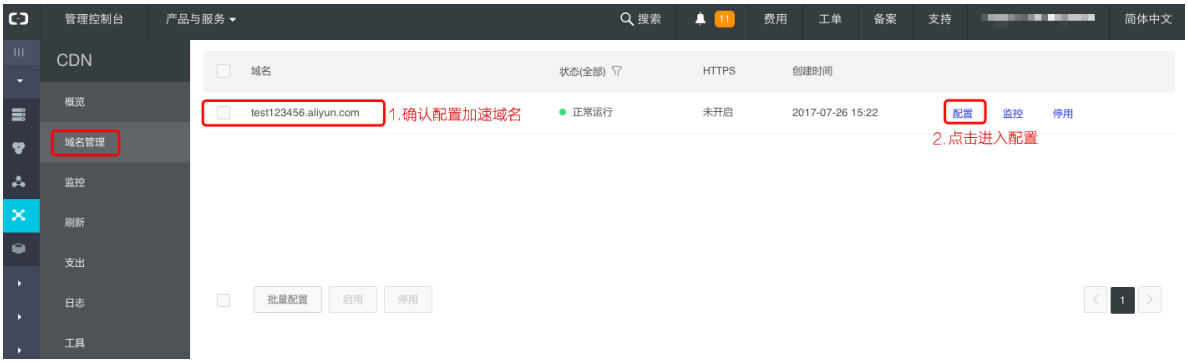
# 6.5.1 智能压缩

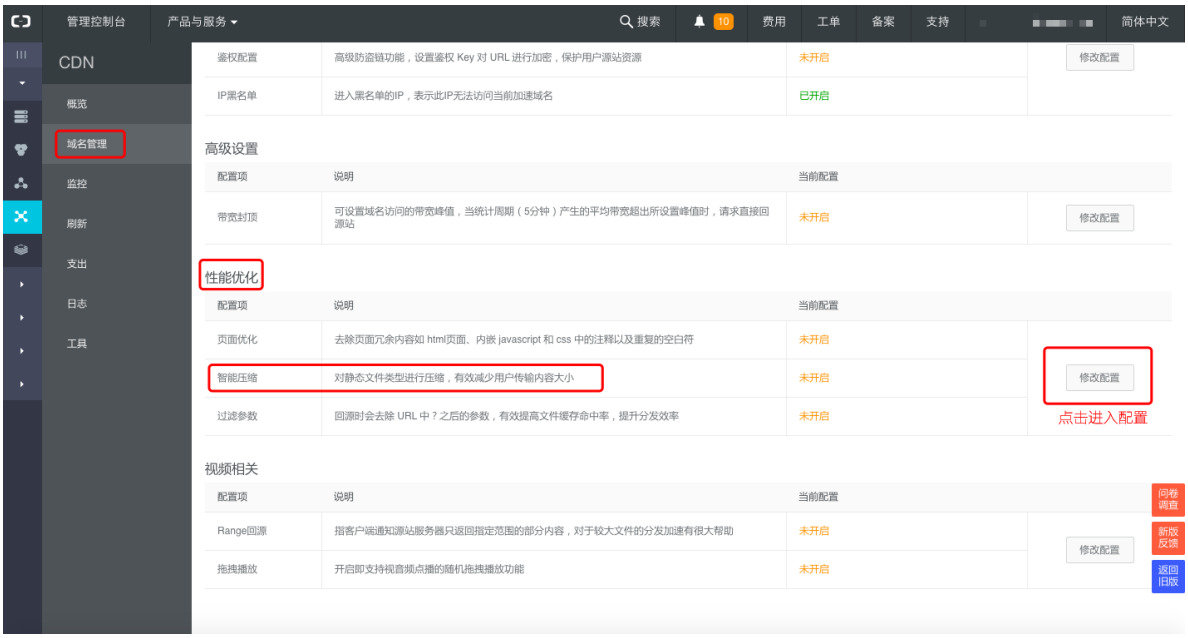
## 功能介绍

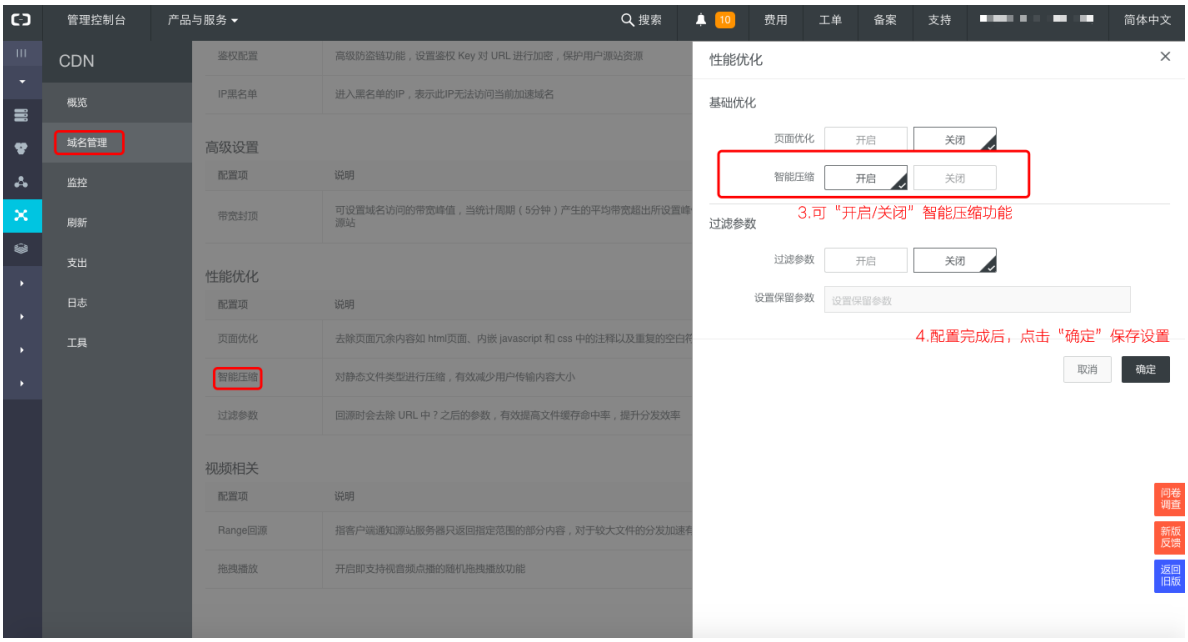
- 开启智能压缩功能，可以对大多数静态文件类型进行压缩，有效减少用户传输内容大小，加速分发效果。
- 当前支持的压缩内容格式有：“content-type：text/xml ，text/plain ，text/css ，application/javascript ，application/x-javascript ，application/rss+xml， text/javascript ，image/tiff， image/svg+xml，application/json”。

## 配置引导

- 适用业务类型：所有
- 变更配置CDN域名概览页，进入域名管理页面，选择需要设置的域名，单击配置。



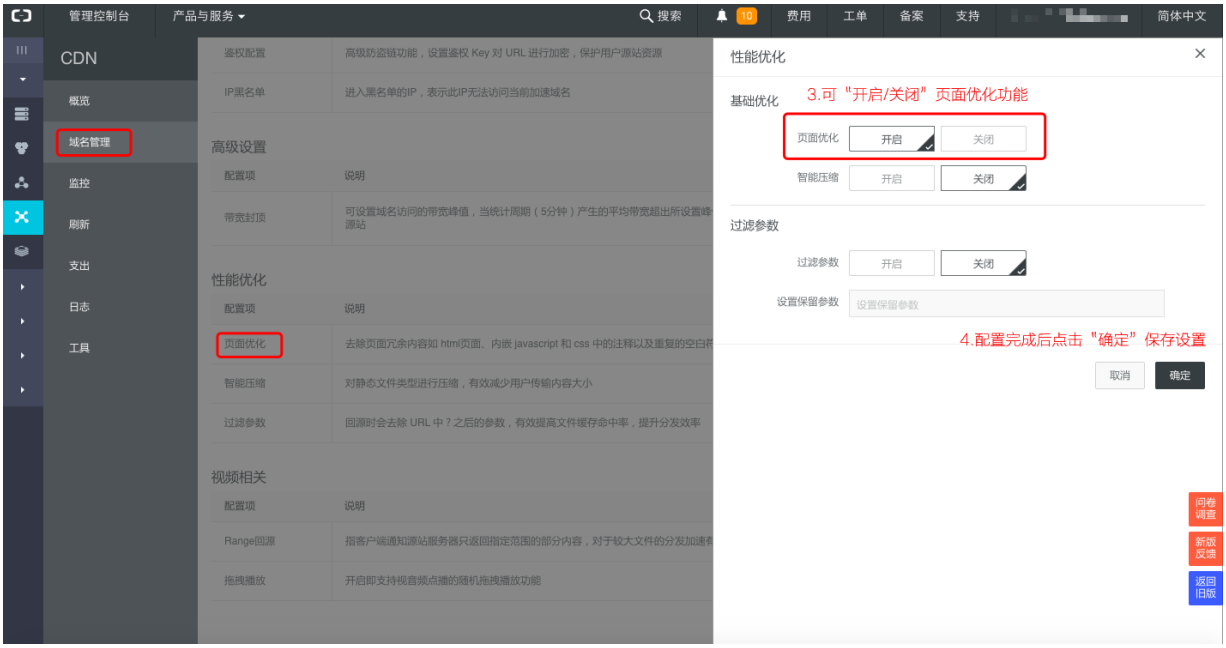



## 6.5.2 页面优化

### 功能介绍

开启页面优化功能，可以删除 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。

### 配置引导


## 6.5.3 过滤参数

### 功能介绍

- 过滤参数是指当URL请求中带？并携带参数请求到CDN节点的时候，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。如果开启过滤参数的话，该请求到CDN节点后会截取到没有参数的URL向源站请求。并且CDN节点仅保留一份副本。如果关闭该功能，则每个不同的URL都缓存不同的副本在CDN的节点上
- http 请求中多包含参数，但是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”，支持设置多个保留参数，如请求中包含任一“保留参数”，会带保留参数回源，保留参数不忽略

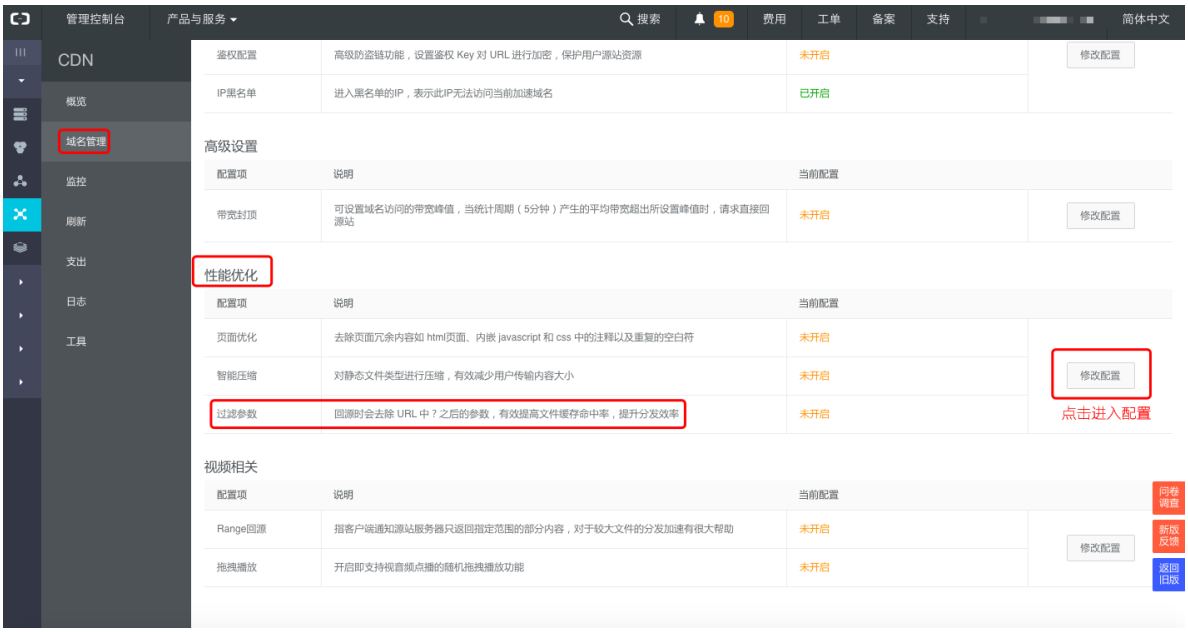
> **说明：**
> 使用示例：
>
> - 例如：`http://www.abc.com/a.jpg?x=1` 请求URL到CDN节点；
> - 开启“过滤参数”功能后CDN节点向源站发起请求 `http://www.abc.com/a.jpg`（忽略参数x=1）待源站响应该请求内容后，响应到达CDN节点后，CDN节点会保留一份副本；然后继续向终端响应 `http://www.abc.com/a.jpg` 的内容。所有类似的请求 `http://www.abc.com/a.jpg?参数` 均响应CDN副本 `http://www.abc.com/a.jpg` 的内容。
> - 关闭“过滤参数”功能则每个不同的URL都缓存不同的副本在CDN的节点上。例如：`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。

**注意事项**

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，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。

**配置引导**

- 适用业务类型：所有。
- 变更配置CDN域名概览页，进入**域名管理**页面，选择需要设置的域名，单击**配置**。





# 6.6 视频相关配置

## 6.6.1 Notify_URL设置

### 功能介绍

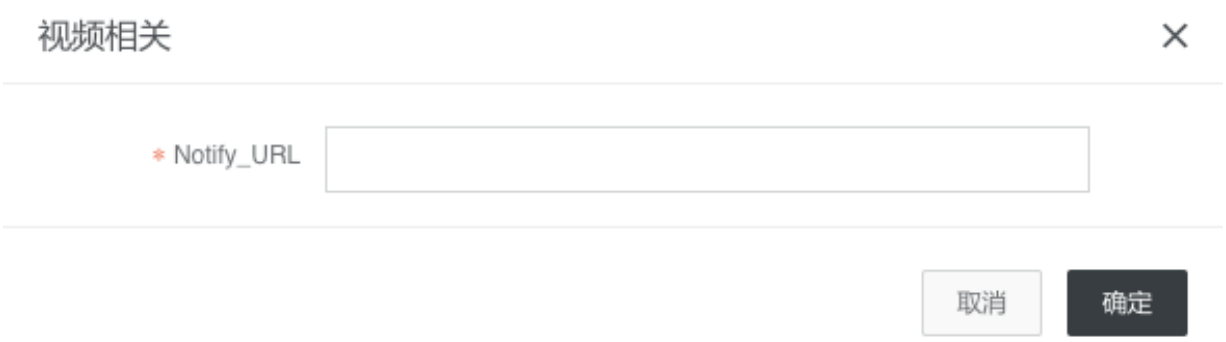
流状态实时信息回调，可以及时通知用户推流或断流操作结果。

**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 |

## 6.6.2 拖拽播放

### 功能介绍

- 拖拽播放是指在视频点播场景中，发生拖拽播放进度时，客户端会向server端发送类似 `http://www.aliyun.com/test.flv?start=10` ，这样的URL请求，然后server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节点则可以支持此项配置，可以在响应请求的时候直接向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。
- 目前支持文件格式有：MP4和FLV。
- 目前对于flv只支持音频aac并且视频是avc编码格式，其余编码格式不支持拖拽。

| 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 |

### 配置引导

- 可选配置项，默认不开启
- 变更配置

CDN域名管理页面，单击**配置**，视频相关 开启/关闭**拖拽播放**功能。


## 6.6.3 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
- 开启**Range**回源，则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。

  **说明：**
  例如：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**Range**回源，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。

  **说明：**
  例如：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。

**注意事项**

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。

**配置引导**

- 可选配置项，默认不开启。

- 变更配置。

进入CDN域名管理页面，单击**配置**，选择 开启/关闭**Range**回源功能。


# 6.7 高级设置

## 6.7.1 带宽封顶

**功能介绍**

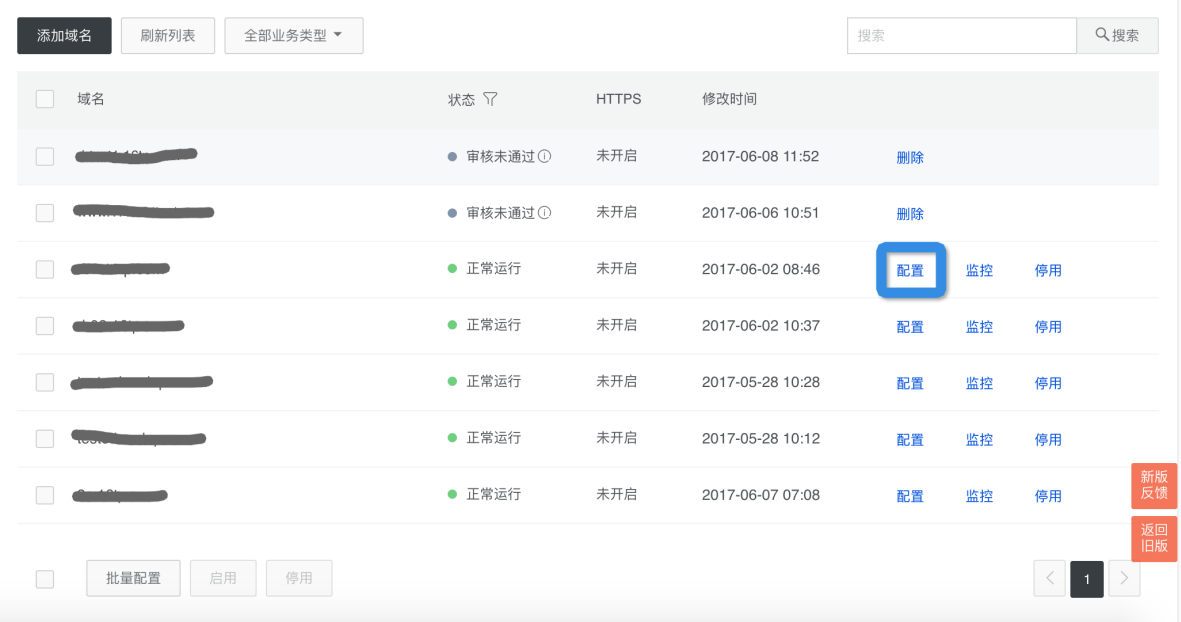
带宽封顶功能是指当统计周期（5分钟）产生的平均带宽超出所设置的带宽最大值时，为了保护您的域名安全，此时域名会自动下线，所有的请求会回到源站。此时CDN将停止加速服务，避免异常流量带来的非日常消费。域名下线后，你可以在控制台重新启动域名。

**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。

**如何开启带宽封顶功能**

1. 域名列表单击**配置**后，在选中域名配置页面找到**安全设置**，单击**修改配置**。





2. 开启带宽封顶功能，带宽单位支持Mbps, Gbps, Tbps。

> **说明：**
> 带宽进制为1000。

3. 带宽封顶功能成功开启。


4. 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。

**注意事项**

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。

# 7 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}
```

# 8 数据监控

资源监控部分的曲线图数据和计费数据有一定差别，如30天统计曲线取点粒度为14400s，计费数据粒度为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，带宽使用以精确粒度的计费数据为准。

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），查看以下监控维度下各监控指标的具体情况：

| 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 |

**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 |

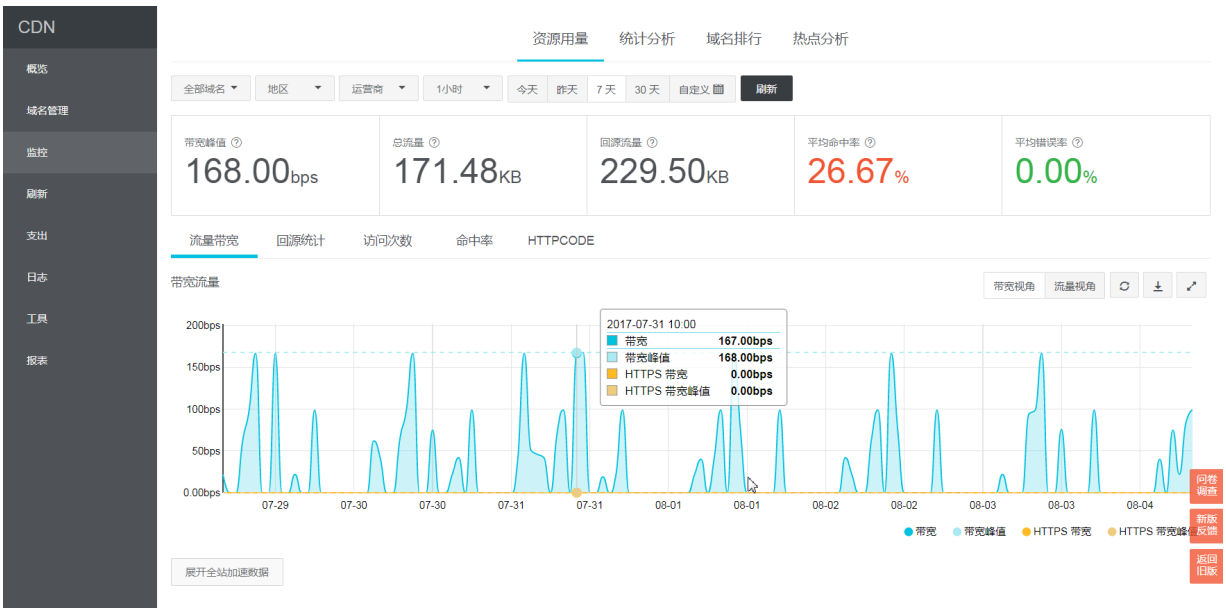
# 9 资源监控

监控页面功能说明

- 资源监控包含四部分，资源用量、统计分析、域名排名、热点分析。
- 支持原始数据导出，如网络带宽、流量，域名按流量占比排名以及访客区域、运营商分布等详细数据。
- 资源监控部分的曲线图数据和计费数据有一定差别，如30天统计曲线取点粒度为14400s，计费数据粒度为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，带宽使用以精确粒度的计费数据为准。

**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 |
| --- | --- | --- |
| 资源用量 | 网络流量、域名排行、回源流量、按日流量统计 | 今天、昨天、7 天内、30 天、自定义90天内 |
| 统计分析 | 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 |
| 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 |

| 项目 | 监控指标 | 可选时间 |
| --- | --- | --- |
| 热点分析 | 文件响应占比、URL 访问次数统计、页面引用 URL 占比 | 支持查看单日数据，自定义90天内 |

# 10 用量查询

### 用量查询

如果您希望通过某一段时间的查询，获取到这段时间内的实际用量数据（流量/带宽/请求数），您可以使用用量查询。您可以自定义时间段进行查询，上线后最长时间支持3个月的查询。

- 可以通过域名和用户维度进行查询。
- 查询时，您需要区分查询流量、带宽，或者请求数。
- 当查询流量或带宽时，用户可以查询每一个计费大区的用量数据。计费大区总共有8个：中国大陆、亚太1，亚太2、亚太3、南美洲、北美洲、中东/非洲、欧洲。

查询图表和列表展示规则：

| | 趋势图 | 数据列表 |
|---|---|---|
| 1-3天 | 小时 | 按流量计费：展示小时。<br>按带宽计费：展示天。 |
| 4天以上 | 天 | 天 |

**说明：**

用量查询页面不支持导出。

### 账单导出

您可以导出按日计费，或者是按月计费的实际用量的数据，用于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。
- 导出数据格式：PDF。

### 明细导出

您可以导出一段时间内的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。当域名超过100时，只保留资源组明细。
- 域名导出时，一次性最多导出100个域名。

- 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。

# 11 日志管理

## 11.1 日志下载

- 日志文件延迟4小时，可以在日志管理模块查询到4小时之前的日志文件。
- 日志文件按小时粒度分割。
- 支持 1月 的日志数据下载。
- 日志命名规则：加速域名_年_月_日_时间开始_时间结束。
- 日志字段格式说明。

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

控制台位置：


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
日志管理
全部域名
2018-07-18
查询
支持近一个月日志下载
日志字段说明: 时间 访问IP 代理IP responsetime referer method 访问URL httpcode requestsize responsesize cache命中状态 UA头 文件类型
文件名
开始时间
结束时间
没有数据
1
2
3

# 12 刷新缓存


**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*。

**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 。

# 13 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。