阿里云
全站加速

用户指南

文档版本：20190715

法律声明

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

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

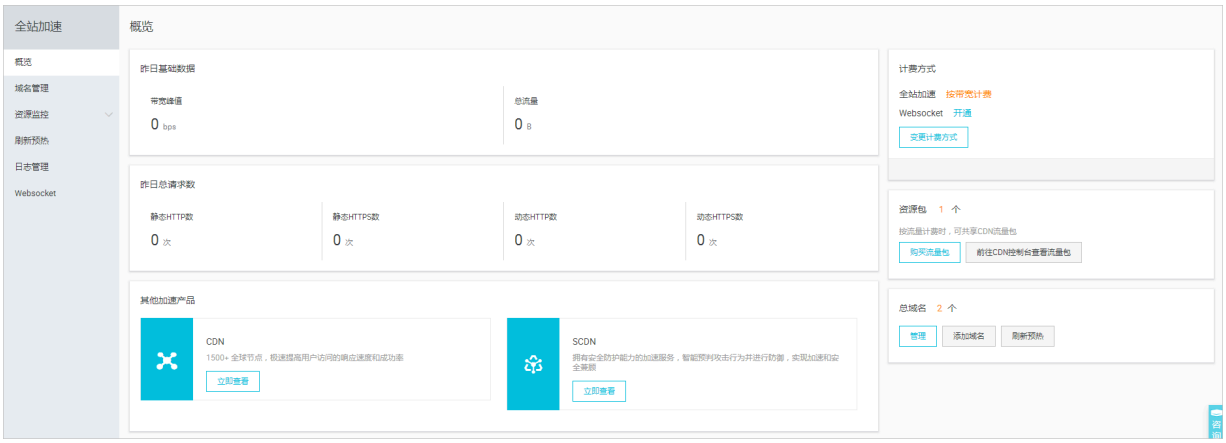
目录

1 控制台介绍

全站加速控制台可以帮助您完成添加加速域名、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。本文档主要介绍全站加速控制台相关功能。

全站加速运行概况总览

登录到全站加速控制台后，首页展示的就是当前账户下全站加速运行概况总览情况：



主要包括：

- 昨日基础数据
  - 带宽峰值
  - 总流量
- 昨日总请求数
  - 静态HTTP数
  - 静态HTTPS数
  - 动态HTTP数
  - 动态HTTPS数

左侧导航栏功能：

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。
资源监控	查看基础CDN加速实时信息，包括峰值带宽，总流量，命中率等信息。
刷新预热	提供刷新和预热的操作
日志管理	提供全站加速日志下载

2 全站加速功能列表

本文档为您介绍了阿里云全站加速产品的所有功能，具体功能信息请查看相关文档。

动静态加速规则配置

项目	说明	默认值
静态文件类型	指定静态文件的后缀名	未开启
静态文件URI	指定静态文件的URI	未开启
静态文件路径	指定静态文件的路径	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，包括动态协议跟随回源和静态协议跟随回源	未开启
私有OSS Bucket回源授权	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	未开启
Range回源	开启Range回源功能，可以减少回源流量消耗，并且提升资源响应时间	未开启
回源请求超时时间	回源请求超时时间默认为30秒，回源正常时不应超过100，最大值不超过900	未开启
设置回源SNI	设置回源SNI指明具体访问的域名	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

项目	说明	默认值
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
重写	重写功能可以配置多条rewrite匹配规则，您可以对请求的URI进行修改、重定向至目标URI	未开启

HTTPS安全加速

项目	说明	默认值
HTTPS设置	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安全加速前提下，支持自定义设置，将您的原请求方式进行强制跳转	未开启
HTTP/2	HTTP/2的优势包括二进制协议、多路复用、头部压缩等	未开启

访问控制

项目	说明	默认值
Refer防盗链	您可以通过配置访问的referer黑白名单来对访问者身份进行识别和过滤	未开启
URL鉴权	URL鉴权方式保护源站资源	未开启
IP黑名单	您可以借此对访问者身份进行识别和过滤	未开启
UsageAgent黑/白名单	根据请求的Usage-Agent字段进行访问控制，实现对请求过滤	未开启

性能优化

项目	说明	默认值
页面优化	压缩或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，有效缩减传输内容的大小	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
拖拽播放	可以在响应请求的时候直接向client响应从指定关键帧（FLV格式）或指定时间（MP4格式）开始的内容	未开启

3 批量复制域名配置

通过批量复制域名配置功能，您可以将某一个加速域名的一个或多个配置，复制到另外一个或者多个域名上。

前提条件

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

背景信息

您在批量复制某个域名的配置时，请注意：

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

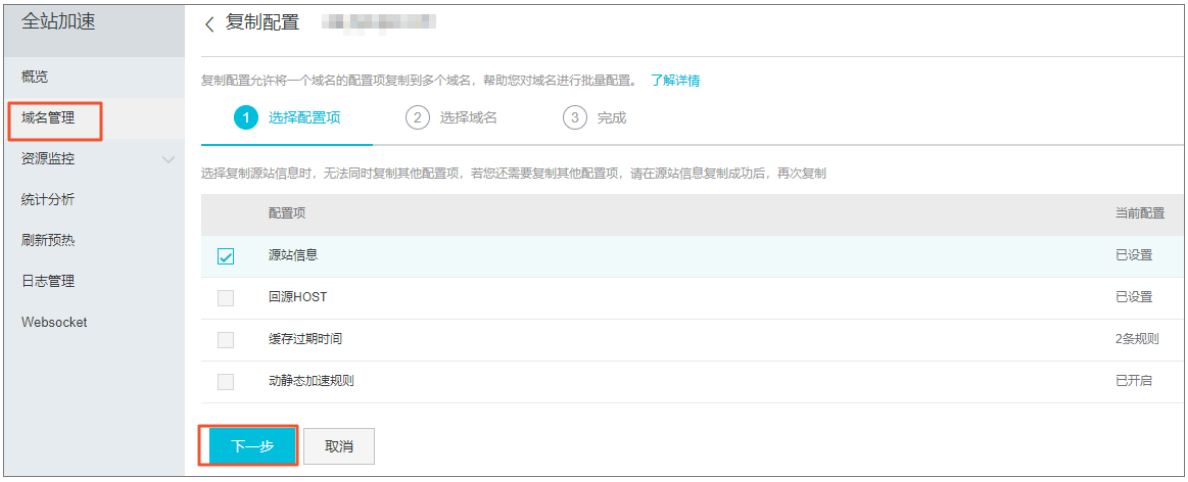
操作步骤

1. 登录全站加速控制台。
2. 在域名管理页面，选择您想要复制配置的域名，单击复制配置。

3. 勾选您想要复制的配置项，单击下一步。

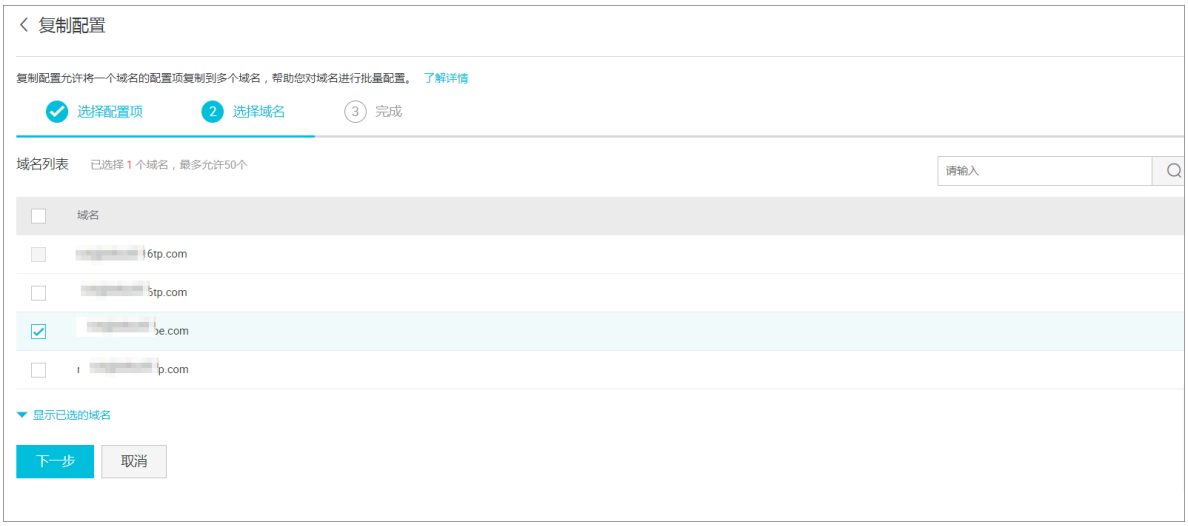
> **说明：**
>
> - 源站信息和非源站信息无法同时复制。
> - 您无法复制HTTPS证书到其他域名，请您单独配置。
> - 自定义回源头为增量复制。例如，假设您的A域名有2条回源头配置，您从B域名复制了5条内容，则你会有7条回源头配置内容。
> - HTTP头为非增量复制。假设您的A域名配置了cache_control为private，您的B域名配置为public，复制后，您的cache_control为public。
> - 开关类的配置复制，将会覆盖域名原有的配置。

· Refer黑白名单或IP黑白名单将会覆盖域名原有配置。

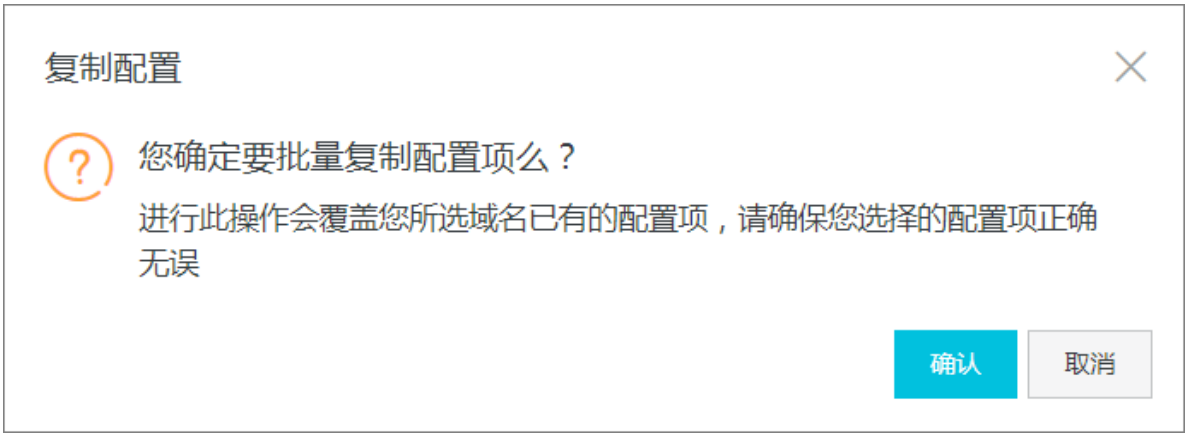


4. 勾选您想要批量配置的目标域名，单击下一步。

   您也可以输入关键词查找域名。



5. 在复制配置对话框中，单击确认，批量复制成功。



4 域名准入标准

本文档介绍了阿里云全站加速服务的域名准入标准和其他使用限制。

全站加速的加速域名准入标准

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. 域名审核：加速域名的源站内容，您可以选择保存于ECS或OSS。如源站内容审核不通过，请联系人工审核。
4. 添加CNAME记录：将您的域名指向全站加速生成的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%。
> · 请确保全站加速服务停止后，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

所有接入全站加速的域名都要经过审核。阿里云全站加速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：您的域名因不符合全站加速接入规则而拒绝，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，阿里云全站加速将不承担任何责任，全部损失将由您自行承担。

- 对于您已接入阿里云全站加速的域名，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全站加速，同时中止您所有域名的全站加速服务。
- 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 50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…	如需继续使用全站加速，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。

5 基本配置

5.1 源站信息

本文通过源站类型、多个源站、端口三个方面为您介绍了阿里云全站加速的源站信息。

源站类型

源站类型可以为 IP、阿里云对象存储OSS、域名。

- IP：填写服务器外网 IP。支持填写多个 IP并设置优先级，阿里云ECS的IP可免审核。
- 对象存储OSS：可直接选择同账号下的OSS Bucket，或手动填写OSS的外网域名，如：`xxx.oss-cn-hangzhou.aliyuncs.com`。您可以在OSS控制台查看OSS的外网域名。
- 域名：填写您的源站域名。支持多个源站域名并设置优先级。

> **说明:**
> 源站域名不能与加速域名相同，否则会造成循环回源。例如，您的加速域名为`cdn.example.com`，建议将资源源站设置为`src.example.com`。

多个源站

源站为IP或域名时，都支持填写多个源站，并设置优先级。加速节点回源时按优先级回源。

端口

如果您通过端口设置了回源协议（HTTP或HTTPS）和自定义端口，则无论您在控制台如何设置，回源都将按照端口的配置进行。

5.2 设置多源优先级

功能介绍

全站加速中，目前 动态资源 和 静态资源的回源策略，均支持优先级设置。

- 全站加速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，优先级的等级：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失败3次，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，该源站将会重新标记为可用，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5S主动健康检查源站一次。

主要支持场景：主备方式切换源站。

操作步骤

1. 在 域名管理 页，选择域名，单击 配置。
2. 在 基本配置 > 源站信息 栏，单击 修改配置。
3. 设置回源 源站地址 和 优先级。

4. 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，并合理设置优先级。

6 回源设置

6.1 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。

- 回源host是可选配置项，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。

操作步骤

1. 在 域名管理页，选择域名，单击 配置。
2. 在 回源配置 > 回源Host 栏，单击 修改配置。

3. 选择您要加速的域名类型，单击 确认。

源站和回源Host的区别

- 源站： 源站决定了回源时，请求到的具体IP地址。
- 回源host：回源host决定回源请求访问到该IP上地址上的具体站点。

案例	例一	例二
源站	www.a.com	1.1.1.1
回源host	www.b.com	www.b.com
实际回源是请求到	www.a.com对应的主机上的站点 www.b.com	1.1.1.1对应的主机上的 站点 www.b.com

6.2 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，客户端使用 HTTP 方式请求资源，节点回源时以 HTTP 方式请求。

目前，全站加速支持动态协议跟随回源和静态协议跟随回源。

说明:

源站需要 同时支持 80 端口和 443 端口，否则有可能会造成回源失败。

操作步骤

协议跟随回源

1. 在 域名管理页，选择域名，单击 配置。

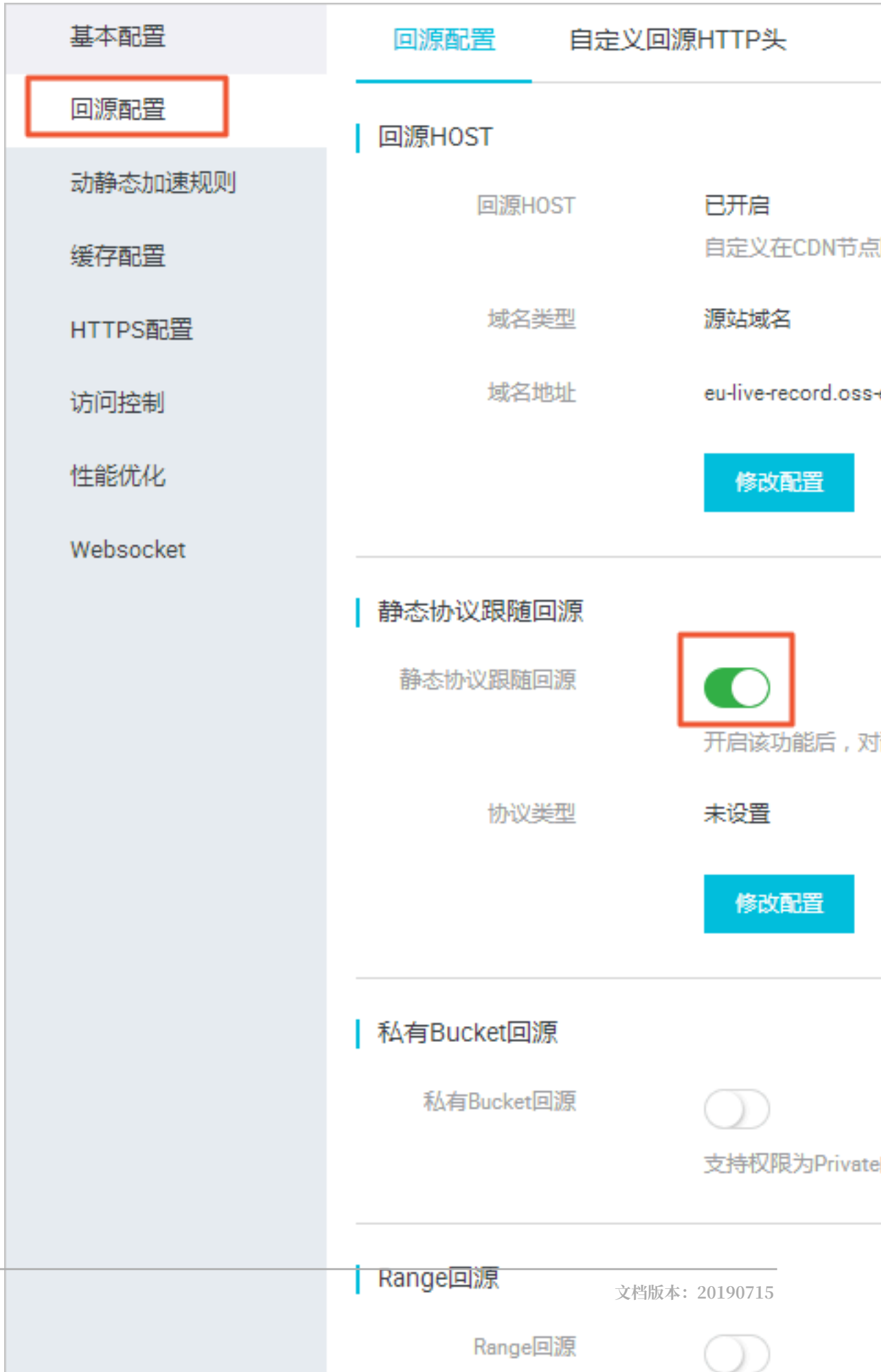
2. 在 动静态加速规则 > 协议跟随回源 栏，单击 修改配置。

3. 选择协议跟随回源的跳转类型：跟随、HTTP 或 HTTPS。

静态协议跟随回源

1. 在 域名管理 页，选择域名，单击 配置。

2. 在 回源配置 > 静态协议跟随回源 中，开启开关。



6.3 私有Bucket回源授权

功能介绍

私有Bucket回源授权指若加速域名想要回源至您账号下标记为私有Bucket，需要首先进行授权。授权成功并开启授权配置后，您开启的私有Bucket授权的域名才有权限访问私有Bucket。

风险提示

- 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。

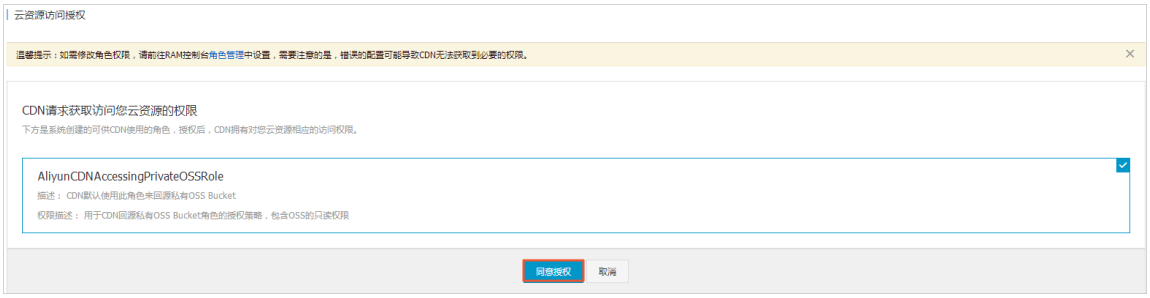
  说明:
  若您授权的私有Bucket内容并不适合作为CDN加速域名的回源内容，请勿授权或者开启该功能。
- 您可以配合使用CDN提供的OSS防盗链(Referer)、鉴权等功能，有效保护您的资源安全。
- 若您的网站有攻击风险，请购买高防服务。同时，请勿授权或开启私有OSS Bucket功能。

操作步骤

- 开启私有 Bucket回源授权

1. 登录CDN控制台，在域名管理页，选择域名，单击管理。
2. 在基本配置 > 源站信息区域框，单击修改配置，设置源站类型为OSS域名。
3. 在回源配置 > 私有Bucket回源设置区域框，单击点击授权。

4. 单击同意授权，授权成功。



5. 打开私有Bucket回源开关，该域名开启私有Bucket回源配置成功。

- 关闭私有Bucket回源授权

  1. 登录RAM控制台，单击RAM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。

6.4 Range回源

功能介绍

Range回源，即分片回源，是指客户端通知源站服务器只返回部分内容，以及这部分内容的范围。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，对于较大文件的分发加速有很大帮助。

- 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：如果客户端向全站加速请求中含有range: 0-100，则源站端收到的请求中也会含有range：0-100这个参数。此时，源站响应给全站加速节点，再由全站加速节点响应给客户端的，都是101个字节（范围为0-100）的内容。

- 关闭Range回源，全站加速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：如果客户端向全站加速请求中含有range：0-100，则服务器端收到的请求中没有range这个参数。此时，源站响应给全站加速节点完整文件，但CDN节点响应给客户端的则是101个字节。然而，由于连接断开，该文件无法缓存到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。

操作步骤

1. 在 域名管理 页，选择域名，单击 配置。

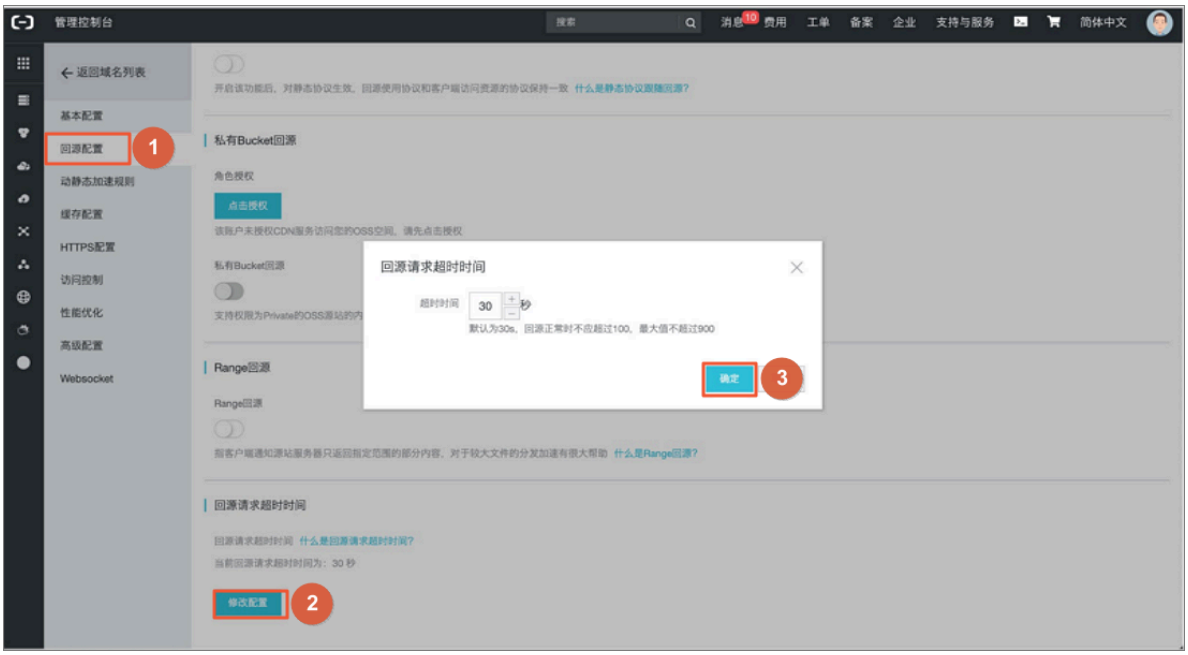
2. 在 回源配置 > Range回源 栏，开启功能。

6.5 回源请求超时时间

本文档为您介绍了回源请求超时时间功能在控制台上的操作步骤，您可以根据需求设置回源请求最长时间。

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击域名管理。
3. 在您需要设置的域名右侧，单击配置。
4. 在左侧导航栏，单击回源配置。
5. 在回源请求超时时间区域框，单击修改配置。



6. 根据您的需求，配置超时时间，单击确认，回源请求超时时间配置成功。

> **说明:**
> 回源请求超时时间默认为30秒，回源正常时不应超过100，最大值不超过900。

6.6 设置回源SNI

如果您的源站IP绑定了多个域名，当全站加速节点以HTTPS协议访问您的源站时，您可以参照本文档，设置回源SNI指明具体访问的域名。

背景信息

服务器名称指示 Server Name Indication（SNI）是一个扩展的传输层安全性协议 Transport Layer Security（TLS）。在该协议下，握手过程开始时，客户端会告诉它正在连接的那台服务器

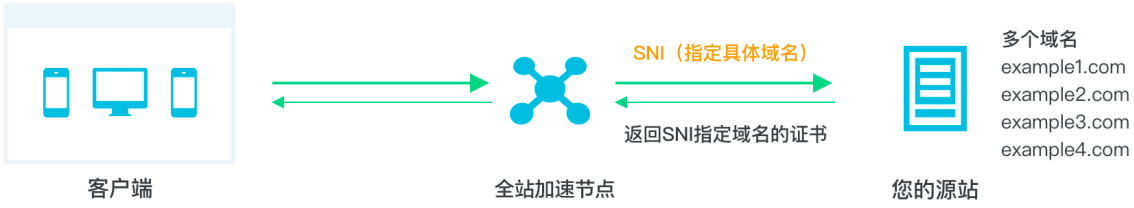
即将要连接的主机名称，以允许该服务器在相同的IP地址和TCP端口号上呈现多个证书，即一台服务器可以为多个域名提供服务。因此，同一个IP地址上提供的多个安全的HTTPS网站（或其他任何基于TLS的服务），不需要使用相同的证书。

但是，如果您的源站服务器使用单个IP提供多个域名的HTTPS服务，且您已经为您的全站加速设置了以443端口回源（全站加速节点以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。这样全站加速节点以HTTPS协议回源访问您的服务器时，服务器才会正确地返回对应的证书。

说明:
如果您的源站是阿里云OSS的，则无需设置回源SNI。

工作原理

回源SNI的工作原理如下图所示：

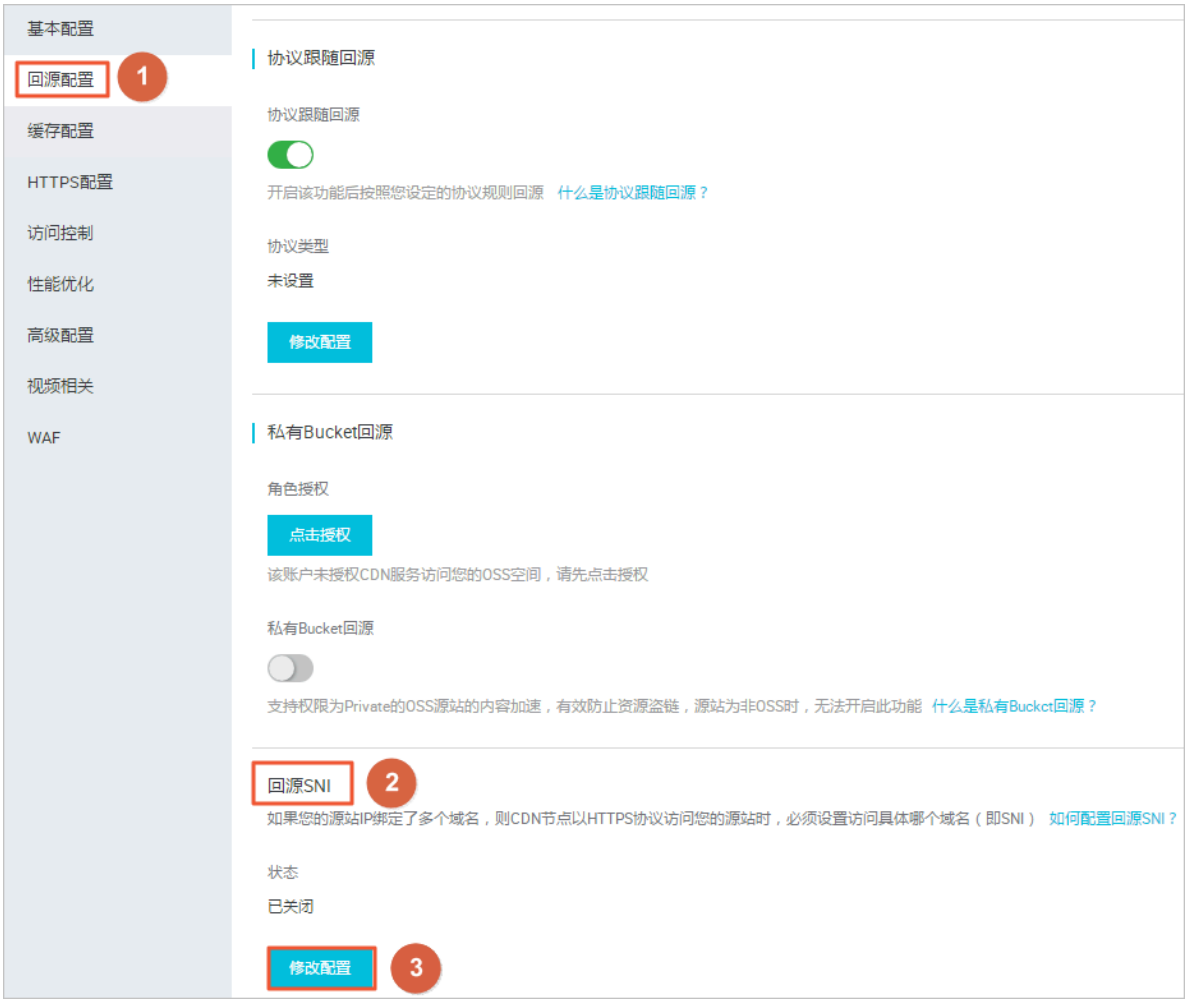


1. 全站加速节点以HTTPS协议访问源站时，在SNI中指定访问的域名。
2. 源站接收到请求后，根据SNI中记录的域名，返回对应域名的证书。
3. 全站加速节点收到证书，与服务器端建立安全连接。

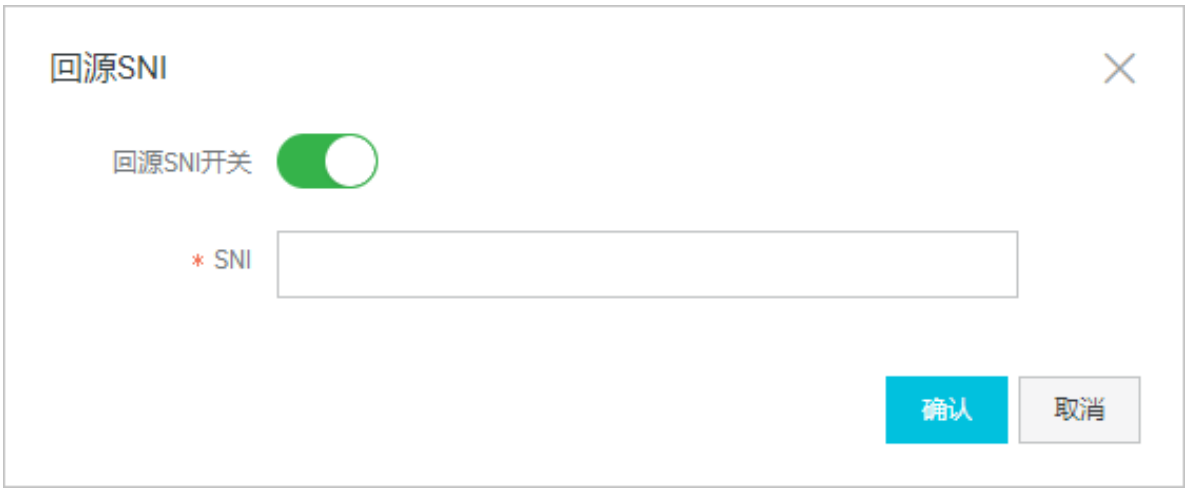
操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击域名管理。
3. 在您需要设置的域名右侧，单击配置。
4. 在左侧导航栏，单击回源配置。

5. 在回源SNI区域框，单击修改配置。



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



7 动静态加速规则

7.1 设置静态文件路径

功能介绍

支持以文件路径的方式区分出静态文件，设定的静态文件不再使用动态加速，而采用更合适的 静态加速，分配最佳的边缘节点进行缓存和分发。

操作步骤

1. 在 域名管理 页，选择域名，单击 配置。
2. 在 动静态加速规则 > 静态路径 栏，单击 修改配置。

3. 指定目录路径。

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。

7.2 设置静态文件类型

功能介绍

全站加速支持以 后缀名的方式设定静态文件的类型。设定的静态文件不再使用动态加速，而采用更合适的 静态加速，分配最佳的CDN节点进行缓存和分发。

操作步骤

1. **在 域名管理 页，选择域名，单击 配置。**
2. **在 动静态加速规则 > 静态文件类型 栏，单击 修改配置。**
3. **选择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。**

7.3 设置静态文件URI

功能介绍

支持以文件URI的方式区分出静态文件，设定的静态文件不再使用动态加速，而采用更合适的 静态加速，分配最佳的边缘节点进行缓存和分发。

操作步骤

1. 在 域名管理页，选择域名，单击 配置。
2. 在 动静态加速规则 > 静态URI 栏，单击 修改配置。
3. 输入指定的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。

8 节点缓存设置

8.1 设置缓存过期时间

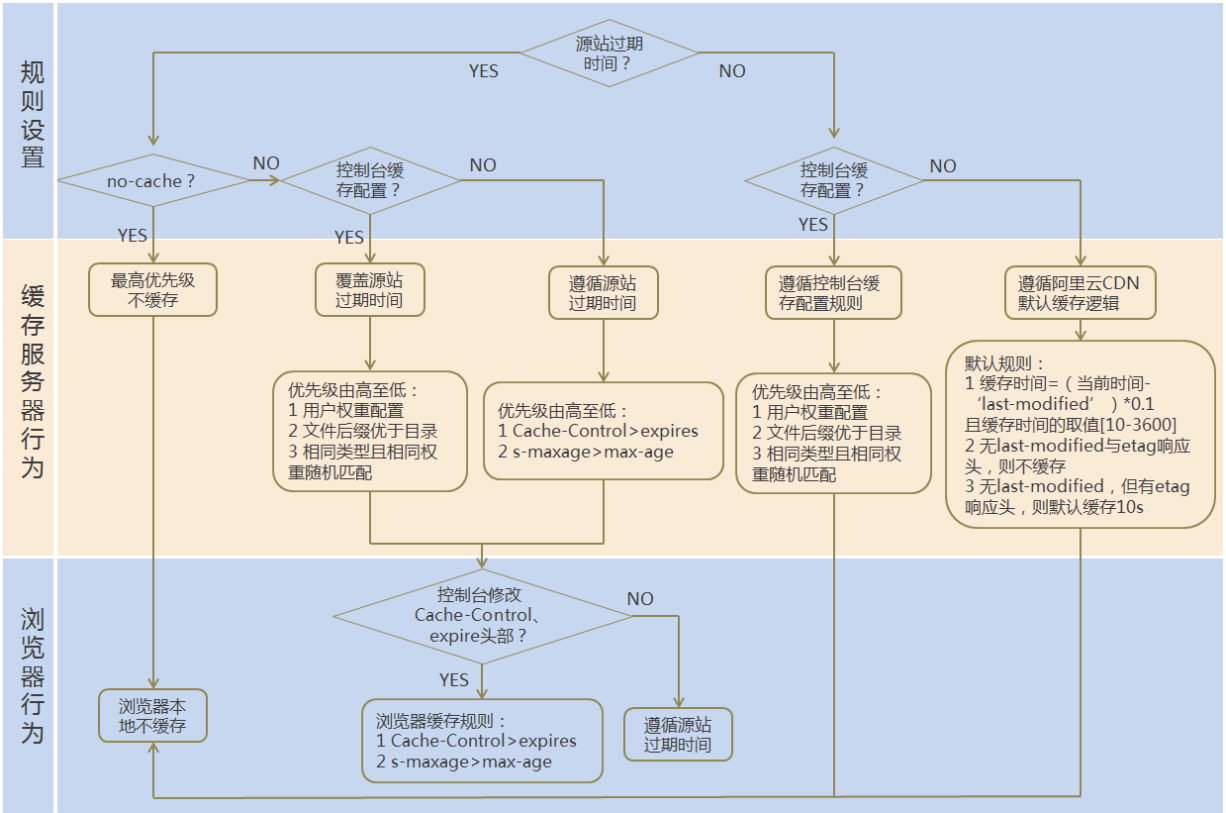
本文为您介绍了缓存过期时间的功能信息及如何设置缓存过期时间。

背景信息

缓存过期时间可以针对拥有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。您可以自主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：
  - 如果源站已经有Cache配置，则缓存过期时间的配置，其优先级高于源站的配置。
  - 如果源站没有Cache配置，则支持按目录、文件后缀名两种方式设置缓存过期时间(支持设置完整路径缓存策略)。

具体缓存策略，如下图所示，详情请参见CDN节点默认缓存策略。



说明:

CDN的缓存可能由于热度较低被提前剔除出CDN节点。

缓存过期时间推荐配置如下表所示。

文件类型	缓存时间设置	举例
更新不频繁的静态文件	1个月以上	图片类型、应用下载类型
需要更新并且更新频繁的静态文件	稍短于1个月	js、css
动态文件	较短缓存时间	php文件内容更新
更新频繁的动态文件	0s（不缓存）	php、jsp、asp

说明:

建议源站的内容不要使用同名更新，请您以版本号的方式，即采用`img-v1.0.jpg`、`img-v2.1.jpg`的命名方式。

操作步骤

1. 登录全站加速控制台。
2. 在 域名管理页面，选择您需要设置的域名，单击 配置。
3. 选择缓存配置 > 缓存过期时间 ，您可以对缓存规则进行添加、修改、删除等操作和管理。

4. 单击添加，您可以选择按 目录 或 文件后缀名两种方式，然后填写内容、过期时间、权重，单击确认。

   例如：为加速域名`example.aliyun.com`设置三个缓存过期时间规则。

   - 缓存策略1：文件后缀名为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。

   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，数字越大的，会优先生效。
   - 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。

8.2 自定义回源HTTP头

功能介绍

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
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

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：

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。

操作步骤

1. 在 域名管理页，选择域名，单击 修改配置。
2. 在 缓存配置 > HTTP头 栏，单击 添加。

3. 您可以自定义选择参数和取值，设置HTTP头。

8.3 自定义错误页面

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

背景信息

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

- 默认值：http响应返回404时，服务器返回默认404 Not Found页面。

- 自定义404：http响应返回404时，将会跳转到自定义的404页面，需要自定义跳转页的完整URL地址。

> 说明:
>
> - 404页面属于阿里云公益资源，不会产生任何费用。
> - 自定义页面属于个人资源，按照正常分发计费。

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名后的配置。
4. 在左侧导航栏，单击缓存配置。
5. 单击自定义页面。
6. 在自定义页面，单击 添加，增加自定义返回码的页面内容。

本文以自定义错误码404为例，假设您需要将404页面资源`error404.html`，与其他动态文件一样存储到源站域名下，并通过加速域名`exp.aliyun.com`访问。那么，您只需选择404并填写完整的加速域名URL即可，URL为：`http://exp.aliyun.com/error404.html`。

7. 单击确认。

您也可以单击修改或删除，对当前配置进行相应操作。

8.4 重写

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

背景信息

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

执行规则说明：

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

操作步骤

1. 登录全站加速控制台。
2. 在您需要设置的域名，单击配置。
3. 在左侧导航栏，单击缓存配置。
4. 在重写区域框中，单击添加。
5. 根据您的需求进行配置，选择Redirect或Break，单击确定。

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

9 HTTPS设置

9.1 HTTPS设置

功能介绍

HTTPS是以安全为目标的HTTP通道，即将HTTP用SSL/TLS协议进行封装，可以称为HTTP的安全版。HTTPS的安全基础是SSL/TLS协议。

- 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，造成敏感信息泄露等安全问题。
  - 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）。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/私钥即可使用。同时，支持用户对证书进行查看、停用、启用、编辑等操作。
- 您可以在阿里云云盾快速申请免费证书或购买高级证书。在阿里云云盾购买的证书，可在CDN控制台直接选择，无需上传。
- 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。
- 目前不支持SNI 回源。

注意事项

配置相关：

- 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流量包或预付费套餐里。请确保账户余额充足后，再开通HTTPS服务，以免因此欠费，影响CDN服务。

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。 参见证书格式说明。

  > 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。

- 只支持带SNI信息的SSL/TLS握手。
- 您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。

操作步骤

1. 购买证书。

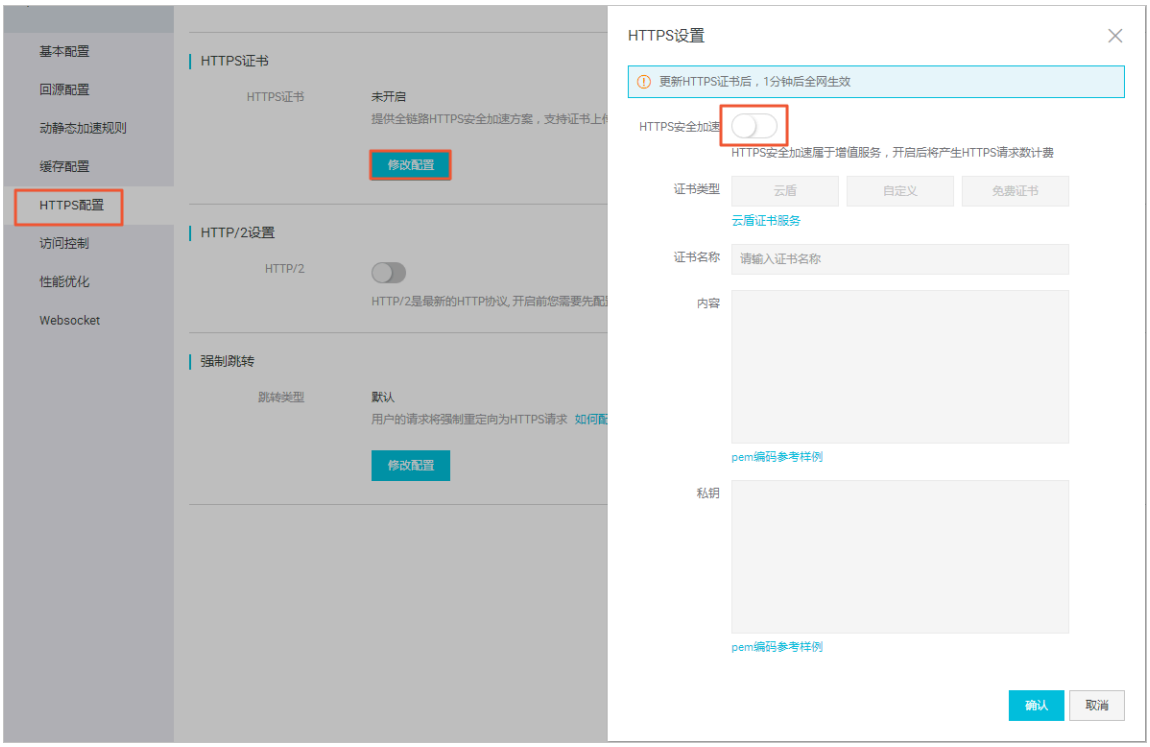
   开启HTTPS安全加速，需要您具备匹配加速域名的证书。您可以在阿里云云盾快速申请免费的证书或购买高级证书。

2. 加速域名配置。

a. 在域名管理页，选择域名，单击管理。

b. 在 HTTPS配置 > HTTPS证书栏，单击修改配置。

c. 打开HTTPS安全加速开关。



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。

d. 选择证书。

- 您可以在阿里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。
- 仅支持PEM的证书格式，了解更多。证书格式说明。

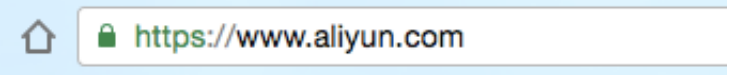
e. 支持设置 强制跳转：自定义将用户的原请求方式进行强制跳转。

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。如下图：



9.2 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 阿里云盾 托管购买的证书、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。其中阿里云全站加速使用的是 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//C3hWnOuIVGdg76626ggOoJSaj48R2n0MnVcC
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

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 outcertifi
    cate.cer
    ```

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

  - 私钥转化：P7B证书无私钥，因此 只需在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。

其它证书相关

- 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，请参见更多证书问题。

9.3 设置强制跳转

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

前提条件

配置强制跳转类型前，您需要配置HTTPS证书。详细说明，请参见HTTPS设置。

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名后的管理。

4. 在左侧导航栏，单击HTTPS配置。
5. 在强制跳转区域框，单击修改配置。

6. 在强制跳转对话框，选择跳转类型，单击确认。

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

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

本文以设置跳转类型为HTTP -> HTTPS为例：

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

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

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

9.4 HTTP/2设置

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。


基本配置
回源配置
动静态加速规则
缓存配置
HTTPS配置
访问控制
性能优化
Websocket
HTTPS证书
HTTPS证书
未开启
提供全链路HTTPS
修改配置
HTTP/2设置
HTTP/2
HTTP/2是最新的H
强制跳转
跳转类型
默认
用户的请求将强制
修改配置

10 访问控制

10.1 IP黑白名单

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。

- IP黑名单当前支持ip网段添加，例如：127.0.0.1/24。
- 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. 在 域名管理 页，选择域名，单击 配置。
2. 在 访问控制 > IP黑名单 栏，单击 修改配置。

3. 添加IP后确认开启。

10.2 Referer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，对访问者身份进行识别和过滤，从而限制全站加速资源被访问的情况。
- 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 全站加速节点，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，否则该访客请求将被禁止，返回403响应码。

注意事项

- 系统默认不启用，您可以自行选择是否配置。
- 黑白名单互斥。开启功能后，您只能选择编辑Refer黑名单或者白名单，同一时间只支持一种方式。
- 支持设置是否允许空 Referer 字段访问全站加速资源。（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，则最终配置生效的是*.a.com，所有子级域名都会生效。

操作步骤

1. 在 域名管理页，选择域名，单击 配置。

2. 在 访问控制 > Refer防盗链 栏，单击 修改配置。

3. 选择 黑名单 或 白名单。

10.3 配置URL鉴权

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

背景信息

URL鉴权功能通过阿里云全站加速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。

- 全站加速客户站点提供加密URL（包含权限验证信息）。
- 您使用加密后的URL向加速节点发起请求。

- 加速节点对加密URL中的权限信息进行验证以判断请求的合法性。正常响应合法请求，拒绝非法请求。

阿里云全站加速兼容并支持鉴权方式A、鉴权方式B、鉴权方式C三种鉴权方式。您可以根据自己的业务情况，选择合适的鉴权方式，来实现对源站资源的有效保护。

如果您想了解Python鉴权代码示例，请参见鉴权代码示例。

操作步骤

1. 登录全站加速控制台。
2. 在域名管理 页面，选择您需要设置的域名，单击配置。
3. 选择访问控制 > URL鉴权，单击修改配置。

4. 打开URL鉴权开关，选择鉴权类型，并填写主KEY和备KEY。URL鉴权功能配置成功。

10.4 鉴权方式A

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

原理说明

访问加密URL构成：

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

鉴权字段描述

字段	描述
DomainName	CDN站点的域名。

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

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

- 如果小于当前时间，服务器判定过期失效并返回HTTP 403错误。
- 如果大于当前时间，构造出一个同样的字符串，参考下方`sstring`字符串，然后使用MD5算法算出`HashValue`，再和请求中`md5hash`进行比对。
  - 结果一致，鉴权通过，返回文件。
  - 结果不一致，鉴权失败，返回HTTP 403错误。

`HashValue`是通过以下字符串计算出来的：

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

示例说明

您可以通过以下示例说明更好地理解鉴权方式A的实现。

1. 通过`req_auth`请求对象。

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

2. 设置密钥为：aliyuncdnexp1234（您可以自行配置）。
3. 设置鉴权配置文件有效时间为：2015年10月10日00:00:00，计算出秒数为1444435200。

4. CDN服务器会构造一个用于计算Hashvalue的签名字符串。

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

5. 根据该签名字符串，CDN服务器会计算出HashValue。

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

6. 请求时url为：

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

如果计算出的HashValue与您请求中带

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

鉴权方式B和鉴权方式C具体原理和示例，请参见鉴权方式B、鉴权方式C。

鉴权方式B和鉴权方式C具体原理和示例，请参见鉴权方式B、鉴权方式B。

10.5 鉴权方式B

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

原理说明

访问加密URL格式：

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

当鉴权通过时，实际回源的URL是：

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

鉴权字段描述

字段	描述
DomainName	CDN站点的域名。
timestamp	资源失效时间，作为URL的一部分，同时作为计算`md5hash`的一个因子，格式为：YYYYMMDDHHMM，有效时间1800s。 例如您设置访问时间为2020-08-15 15:00:00，则链接的真正失效时间为2020-08-15 15:30:00。

字段	描述
md5hash	通过md5算法计算出的验证串，由数字0-9和小写英文字母a-z混合组成，固定长度32。
PrivateKey	您设定的鉴权密钥。
Filename	实际回源访问的URL，鉴权时Filename需以/开头。

示例说明

您可以通过以下示例说明更好地理解鉴权方式B的实现。

1. 回源请求对象：

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

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

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

5. 服务器根据该签名字符串计算`md5hash`。

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

6. 请求url为：

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

如果计算出来的`md5hash`与您请求中带的`md5hash`

值（9044548ef1527deadafa49a890a377f0 ）一致，鉴权通过。

鉴权方式A和鉴权方式C具体原理和示例，请参见鉴权方式A、鉴权方式C。

鉴权方式A和鉴权方式C具体原理和示例，请参见鉴权方式A、鉴权方式C。

10.6 鉴权方式C

本文为您介绍了鉴权方式A的原理并用示例说明。

原理说明

访问加密URL格式有如下两种格式。

- 格式1

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

- 格式2

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

说明:

`{}`中的内容表示在标准URL基础上添加的加密信息。

鉴权字段描述

字段	描述
PrivateKey	您设定的鉴权密钥。
FileName	实际回源访问的URL，鉴权时Filename需以/开头。
timestamp	访问源服务器时间，取UNIX时间。未加密的字符串，以明文表示。固定长度10，1970年1月1日以来的秒数，表示为十六进制。
DomainName	CDN站点的域名。

示例说明

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

- md5hash计算值为：

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

- 生成加密URL:
  - 格式一：

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

  - 格式二：

```
http://cdn.example.com/test.flv?KEY1=a37fa50a5fb8f71214b1
e7c95ec7a1bd&KEY2=55CE8100
```

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

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

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

10.7 UsageAgent黑/白名单

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

背景信息

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

> 说明:

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

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击域名管理。
3. 在您需要设置的域名，单击配置。
4. 在左侧导航栏，单击访问控制。
5. 在UserAgent黑/白名单区域框中，单击修改配置。
6. 根据您的需求配置黑白名单的规则，单击确定。

11 性能优化

11.1 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`。

操作步骤

1. 在 域名管理页，选择域名，单击 配置。
2. 在 性能优化 > 智能压缩 栏，单击开启开关。

11.2 拖拽播放

功能介绍

拖拽播放通常发生在视频点播场景中。当用户进行拖拽播放时，客户端会向server端发送类似 `http://www.aliyun.com/test.flv?start=10` 的URL请求（这里用10举例），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，全站加速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。

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。	表示时间，单位是s，支持小数表示ms（如start=1.01，表示开始时间是1.01s）。全站加速会定位到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。	表示字节，全站加速会自动定位到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。

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。

操作步骤

1. 在 域名管理 页，选择域名，单击 配置。

2. 在 性能优化 > 拖拽播放 栏，开启开关。

11.3 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节点时，CDN节点在收到该请求后会判断是否将该带参数的请求URL请求回源站。

- 如果开启该功能，该请求到CDN节点后会截取到没有参数的URL向源站请求。同时，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。

功能推荐

- 由于http 请求中大多包含参数，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。系统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。

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。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 功能后，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。

操作步骤

1. 在 域名管理 页，选择域名，单击 配置。
2. 在 性能优化 > 过滤参数 栏，单击 修改配置。
3. 单击 过滤参数 开启按钮。

11.4 页面优化

功能介绍

开启页面优化功能后，您可以删除 html中的注释及重复的空白符，有效去除页面冗余内容，减小文件体积，提高加速分发效率

操作步骤

1. 在 域名管理 页，选择域名，单击 配置。

2. 在 性能优化 > 页面优化 栏，单击开启按钮。

12 Websocket

本文档介绍了Websocket功能的原理、优势、使用场景和操作指南。

什么是Websocket

WebSocket协议是基于TCP的一种新的网络协议。它实现了浏览器与服务器全双工(full-duplex)通信，即允许服务器主动发送信息给客户端。因此，在 WebSocket中，浏览器和服务器只需要完成一次握手，两者之间就直接可以创建持久性的连接，并进行双向数据传输，客户端和服务器之间的数据交换变得更加简单。

Websocket的优势

- 小Header：互相沟通的Header非常小，只有 2 Bytes左右。
- 服务器不再被动接收到浏览器的请求之后才返回数据，而是在有新数据时就主动推送给浏览器。

现在，很多网站为了实现推送技术，所用的技术都是 Ajax 轮询。轮询是在特定的时间间隔（如每1秒），由浏览器对服务器发出HTTP请求，然后由服务器返回最新的数据给客户端的浏览器。

这种传统的模式带来很明显的缺点，即浏览器需要不断的向服务器发出请求。然而HTTP请求可能包含较长的头部，其中真正有效的数据可能只是很小的一部分，显然这样会浪费很多的带宽等资源。HTML5 定义的 WebSocket 协议，能更好的节省服务器资源和带宽，并且能够更实时地进行通讯。

HTML5 定义的 WebSocket 协议，能更好的节省服务器资源和带宽，并且能够更实时地进行通讯。

使用场景

- 弹幕

  终端用户A在自己的手机端发送了一条弹幕信息，但是您也需要在客户A的手机端上将其他N个客户端发送的弹幕信息一并展示。需要通过websocket协议将其他客户端发送的弹幕信息从服务端全部推送至客户A的手机端，从而使客户A可以同时看到自己发送的弹幕和其他用户发送的弹幕。

- 在线教育

  老师进行一对多的在线授课，在客户端内编写的笔记、大纲等信息，需要实时推送至多个学生的客户端，需要通过websocket协议来完成。

- 股票等金融产品实时报价股

  股票黄金等价格变化迅速，变化后，可以通过websocket协议将变化后的价格实时推送至世界各地的客户端，方便交易员迅速做出交易判断。

- 体育实况更新

  由于全世界体育爱好者数量众多，因此比赛实况成为他们最为关心的热点。这类新闻中最好的体验就是利用Websocket达到实时的更新。

- 视频会议和聊天

  尽管视频会议并不能代替和真人相见，但是应用场景众多。Websocket可以帮助两端或多端接入会议的用户实时传递信息。

- 基于位置的应用

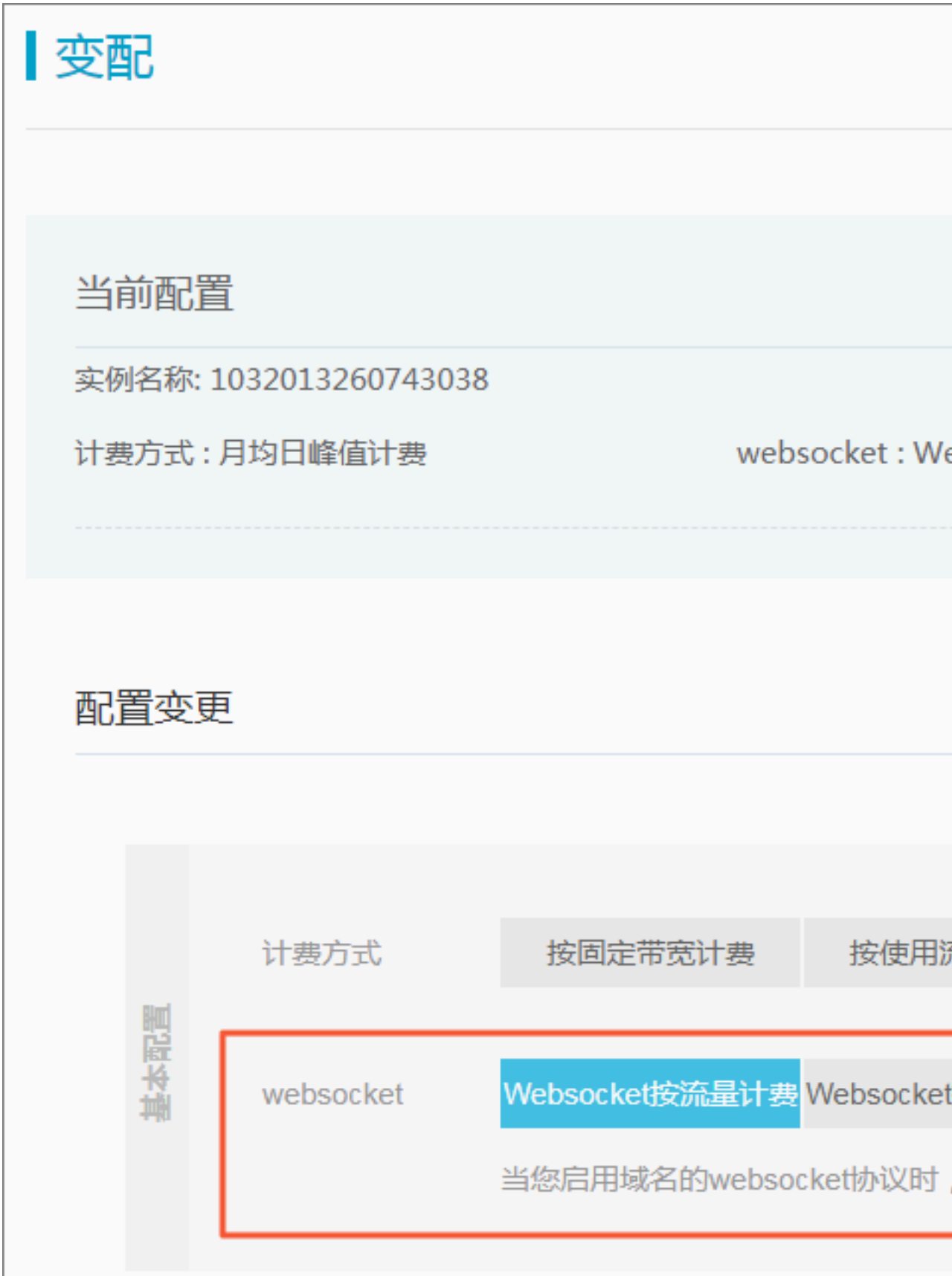
  越来越多的开发者借用移动设备的GPS功能来实现他们基于位置的网络应用。如果您一直记录终端用户的位置(比如您的 App 记录用户的运动轨迹)，就可以收集到更加细致化的数据。

开通Websocket

您需要通过指定websocket计费类型并且计费类型生效后，才能正式使用websocket功能。

1. 登录全站加速控制台。

2. 单击变更计费方式。


变配
当前配置
实例名称: 1032013260743038
计费方式：月均日峰值计费
websocket : We
配置变更
基本配置
计费方式
按固定带宽计费
按使用流
websocket
Websocket按流量计费
Websocket
当您启用域名的websocket协议时

3. 单击去开通，即可开通Websocket。
4. 等待Websocket生效。

> 说明:
>
> · 如果您是新用户：websocket计费立即生效。
>
> · 如果您是老用户：若您全站加速的计费类型为按日计费，生效时间为下一个自然日；若您全站加速计费类型为按月计费，生效时间为下个月1日0点。（如果全站加速计费类型没有变更需求，请保持与当前计费项一致）。

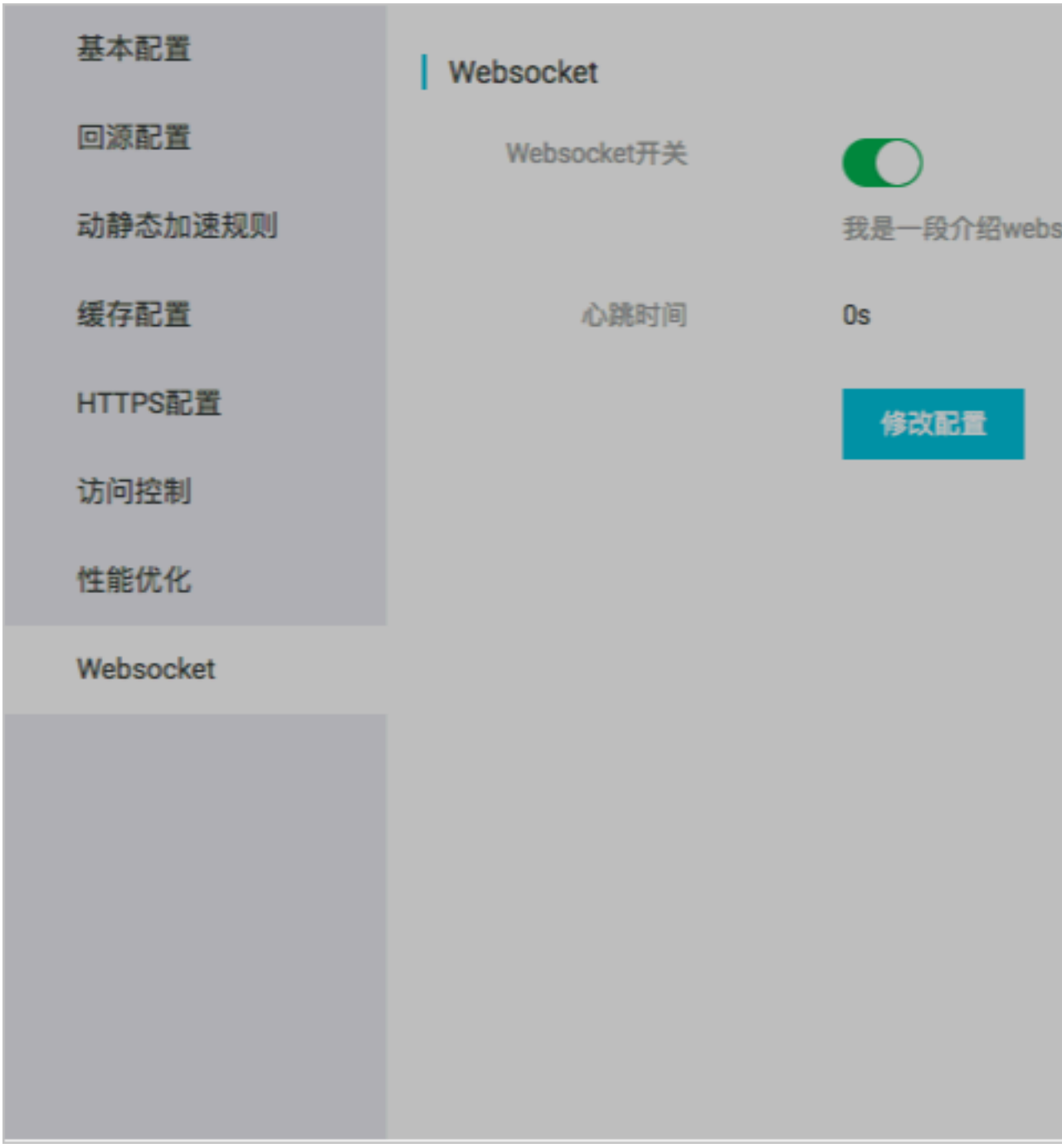
关于Websocket计费问题，请参考计费详情。

使用Websocket

在Websocket生效后，您可以具体配置该功能。

1. 在域名配置页，选择您想要使用Websocket的域名，单击配置。
2. 单击左侧导航栏 Websocket。

3. 打开Websocket开关，设置心跳时间和回源协议。



说明:

心跳时间默认60秒。 回源协议默认为不选定，您需要自行指定。

- 心跳时间：每隔一段时间客户端会向服务器发送一个数据包，告诉服务端当前客户端的状态，服务端也会返回一个数据包到客户端，同步服务端的状态，这样客户端和服务端可以知晓彼此是否处于正常连接的状态。这段时间，就是心跳时间。
- 回源协议：websocket协议回到源站时需要遵循的协议类型，HTTP/HTTPS/跟随。

Websocket的数据统计

不同统计类型在不同时间维度，支持的粒度如下：

统计类型	3天以内	4-31天	大于等于32天
流量带宽统计	支持5分钟、1小时	支持1小时、1天	支持1天
HTTPcode统计			

支持地区、运营商、域名、时间范围进行查询，最长跨度为3个月。

13 刷新与预热

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。

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

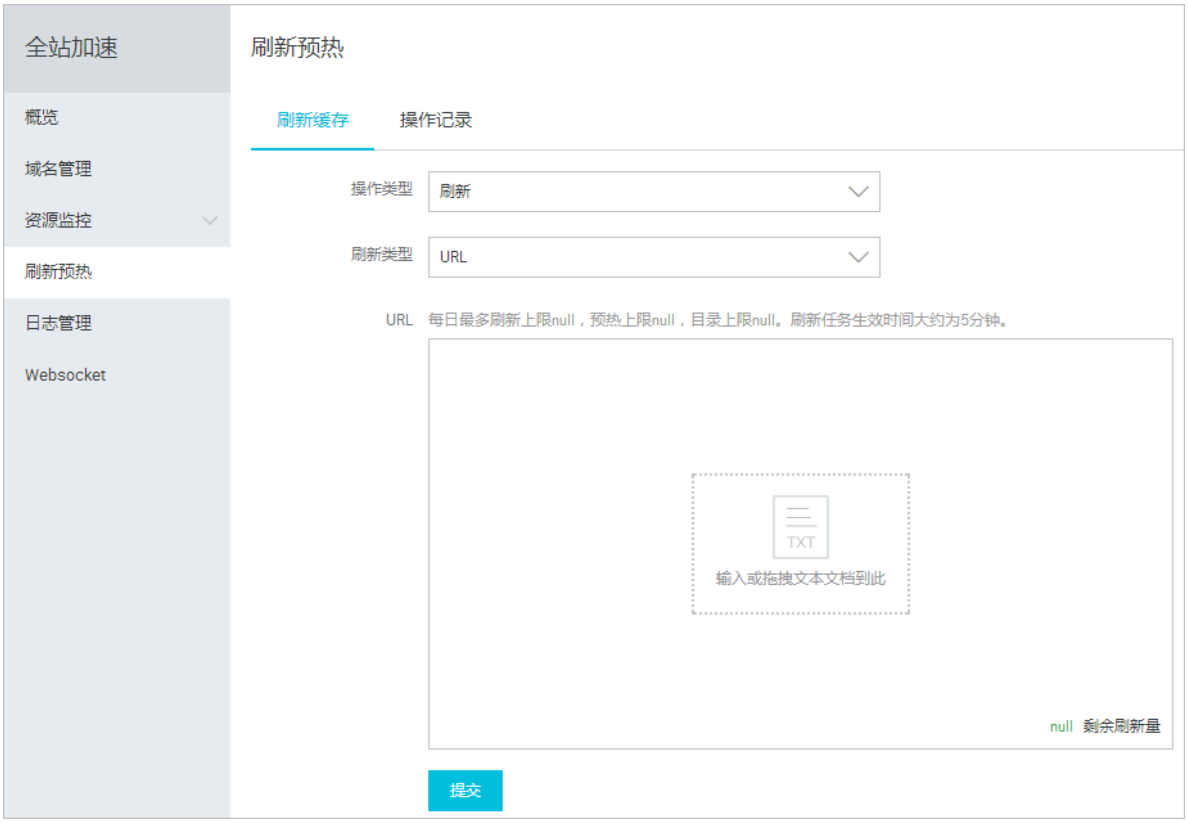
原理：通过提供文件目录的方式，强制CDN节点回源拉取最新的文件。

任务生效时间：5-10 分钟。

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。

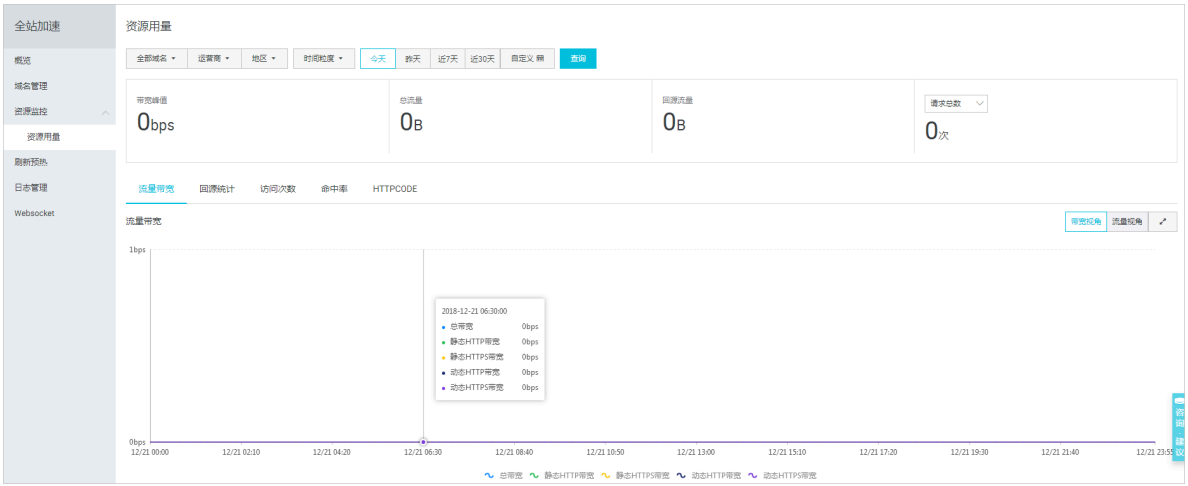
注意事项：

- 输入的 URL 必须带有 `http://`或`https://`。
- 同一个 ID 每天最多只能预热刷新共 2000 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，详见 资源预热API。

14 资源监控

监控页面功能说明

- 资源监控包含：流量带宽、回源统计、访问次数、命中率、HTTPCode。支持以域名、地区、运营商和时间粒度、自定义时间区间等为条件筛选查询。
- 支持原始数据导出和下载，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 。

15 日志管理

日志管理规则

- 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。
- 日志文件最多保存2周。
- 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	无
responsetime(单位 ms)	1542
referer	无
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

控制台位置如下图所示：


全站加速
概览
域名管理
资源监控
刷新预热
日志管理
Websocket
日志管理
请选择域名
2018-12-21
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
操作
没有数据

16 IP应用加速

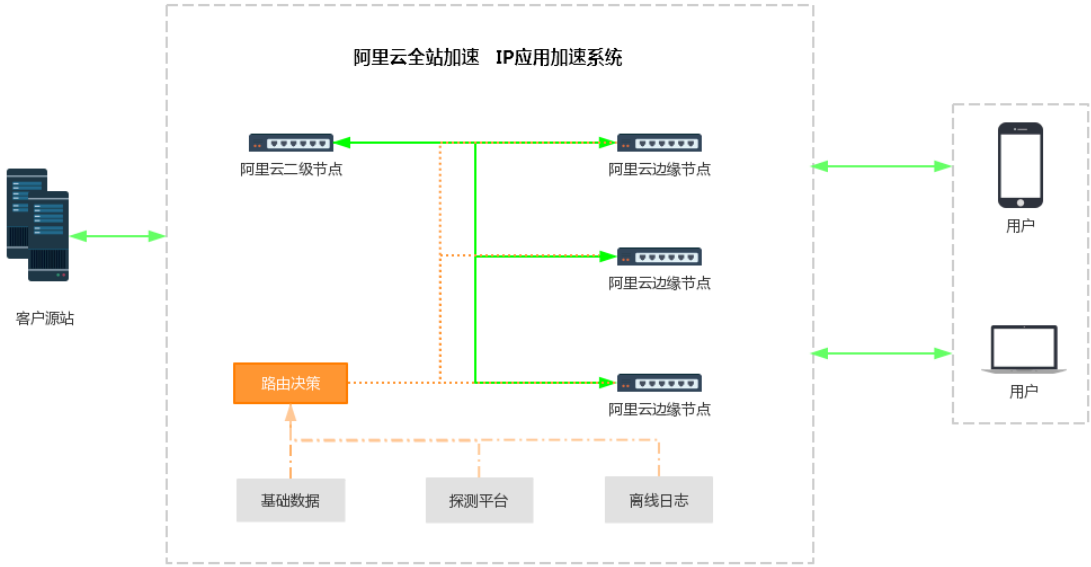
16.1 什么是IP应用加速?

IP应用加速旨在提供非标准HTTP协议用户，特别是四层私有协议服务场景下，如金融类、游戏类、语音交互类等客户提供网络传输加速，降低服务的延迟和提升访问的可用性。

产品简介

IP应用加速(IPA)提供基于四层协议应用的接入和传输加速，立足于阿里云CDN基础设施，内部协议优化以及智能选路选路系统，大幅提升传输速率和可用性，在弱网环境下传输改善尤为效果。可以做到对客户业务透明转发，无任何侵入，保护客户隐私。同时，源站只需简单适配，即可具备获取客户端IP的能力。

加速原理



- 边缘节点跟二级节点间利用私有协议做传输控制，保证了高可能性和稳定快速的传输效率。
- 使用智能选路系统，可以在网络内快速找到终端用户到源站的最优路径，进一步提升可用性及其传输速率。

设置源站透传

将客户端源IP传递给源站，目前支持TOA和Proxy Protocol两种方式。

- TOA

  启用该选项携带客户端真实IP，需要源站安装TOA内核模块，服务程序无需改造。

- Proxy Protocol

  启用该选项携带客户端真实IP，Nginx开源版本默认支持，其他源站服务软件需自行兼容。

16.2 开通IP应用加速

本文为您介绍了如何开通IP应用加速。IP应用加速功能为您提供网络传输加速，降低服务的延迟和提升访问的可用性。

前提条件

您需要先开通全站加速服务，详情请参见步骤一：开通服务。

操作步骤

1. 登录全站加速控制台。
2. 进入IP应用加速页面，单击开通IP应用加速。

3. 选择适合您的计费方式，单击立即开通。

4. 返回到IP应用加速页面，单击添加域名。

5. 在添加域名页面，根据您的需求，填写对应项，业务类型请选择IP应用加速，单击下一步。

说明:

目前只支持添加一个端口，如果您想要添加多个端口，请您提交工单。

6. **在域名列表页面，状态显示为正常运行即表示您添加域名成功。此时记录下对应的CNAME值就可以在DNS服务的后台管理里面，将加速域名的解析指向该CNAME值，即可体验IP应用加速的服务。配置CNAME，详情请参见步骤三：配置CNAME。**

16.3 设置源站透传协议

本文为您介绍了如何设置源站透传协议，通过设置源站透传协议，您可以对IP地址进行更好的收集与分析，更好地帮助您处理业务需求。

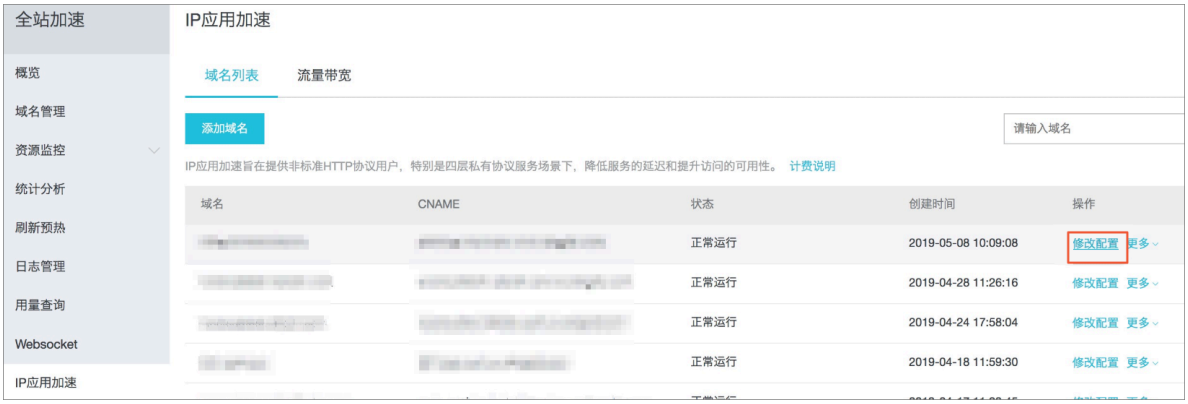
背景信息

将客户端源IP传递给源站，目前支持TOA和Proxy Protocol两种方式。

- TOA：启用该选项携带客户端真实IP，需要源站安装TOA内核模块，服务程序无需改造。
- Proxy Protocol：启用该选项携带客户端真实IP，Nginx开源版本默认支持，其他源站服务软件需自行兼容。

操作步骤

1. 登录全站加速控制台。
2. 进入IP应用加速页面，在您需要设置的域名右侧，单击修改配置。



3. 在IP应用加速区域框中，单击修改配置。

4. 选择您需要设置的协议类型，单击确认。源站透传协议开通成功，您现在可以更好的体验全站加速服务。

16.4 获取客户端真实IP

本文为您介绍了如何从源站获取客户端真实IP。

获取方式介绍

经过加速后源站的服务器获取到的源IP地址为CDN加速设备的IP地址。如果您需要从源站获取客户端的真实IP地址，有如下两种方式：

- Linux系统安装toa内核模块，使用方便且对应用完全透明，无需修改源站Linux服务器的应用程序即可获取真实客户端IP。
- Proxy Protocol（本文简称PP），对系统内核没有要求，需要应用程序配合修改，通过解析文本字符串获取客户端IP。目前，Nginx和HAProxy已经支持。

安装toa模块

如果源站的入口系统是Linux系统，并且版本符合要求，可以通过安装toa模块的RPM包来获取用户真实IP。

支持的Linux版本	RPM包下载
CentOS 6.5	CentOS 6.5 RPM
CentOS 6.9	CentOS 6.9 RPM
CentOS 7.0	CentOS 7.0 RPM
CentOS 7.1	CentOS 7.1 RPM
CentOS 7.2	CentOS 7.2 RPM
CentOS 7.3	CentOS 7.3 RPM
CentOS 7.4	CentOS 7.4 RPM
CentOS 7.5	CentOS 7.5 RPM
alicdn.alios7	alicdn.alios7 RPM

1. 通过`rpm`指令安装对应版本的包。

```
# rpm -ivh tcp-toa-1.2.7-alicdn.alios7.x86_64.rpm
Preparing...
 ################################# [100%]
Updating / installing...
   1:tcp-toa-1.2.7-alicdn.alios7
 ################################# [100%]
```

2. 运行toa模块。

```
# service tcp_toa start
[Starting tcp_toa]:
Checking installed modules...
        tcp_toa not installed.
Checking module files...                [OK]
Installing tcp_toa...                   [OK]
```

3. 查看toa模块运行状态。

```
# lsmod | grep toa
```

```
tcp_toa                 12916  0
```

4. 停止toa模块。

```
# service tcp_toa stop
[StoPPing tcp_toa]:
Checking installed modules...
        tcp_toa installed.
Checking installed tcp_toa...           [OK]
Uninstalling tcp_toa...                 [OK]
```

5. 您可以通过输入`rpm -e tcp-toa`卸载toa模块。

```
# rpm -e tcp-toa
[StoPPing tcp_toa]:
Checking installed modules...
        tcp_toa installed.
Checking installed tcp_toa...           [OK]
Uninstalling tcp_toa...                 [OK]
```

Proxy Protcol

PP方式获取IP需要在控制台配置进行使用，功能打开后，加速服务器和源站建立TCP连接，在传输第一个用户payload前，会传递PP协议文本。

配置Nginx接受PP，只需要将参数`proxy_protocol`添加在`server`块中的`listen`指令后，详情请参见Accepting the PROXY Protocol。

```
http {
    #...
    server {
        listen 80   proxy_protocol;
        listen 443  ssl proxy_protocol;
        #...
    }
}
```

说明:

其他支持PP的应用请参见Proxy Protcol。

不支持PP的应用程序，需要在TCP连接建立后，读取PP的文本行并进行字符串解析来获取客户端IP，字符示例如下所示。

```
PROXY TCP4 1.1.1.2 2.2.2.2 12345 80\r\n
```

解析时先读取行直至\n，在按照协议进行解析，各字段定义如下。

```
PROXY_STRING + single space + INET_PROTOCOL + single space + CLIENT_IP
 + single space + PROXY_IP + single space + CLIENT_PORT + single space
 + PROXY_PORT + "\r\n"
```

真实输出的PP文本行相对以上格式，在 \r\n 之前可能还包含全局唯一的ID，用于全链路监控，如果不需要您可以忽略它。

```
"id"="xxxx"
```