阿里云
全站加速

用户指南

文档版本：20191126

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. **阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，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。
	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务时间约十分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 **注意:** 权重设置为0，该服务器不会再接受新请求。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	单击设置 > 网络 > 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击**确定**。
`Courier字体`	命令。	执行`cd /d C:/window`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。	`switch {active|stand}`

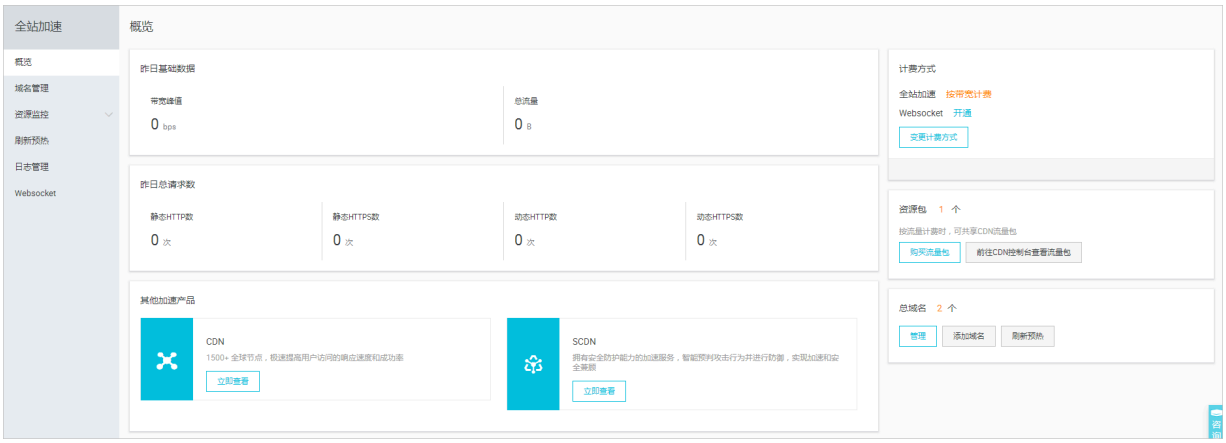
目录

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
配置回源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
配置重写	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
#unique_18	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
User-Agent黑白名单	根据请求的User-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

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。

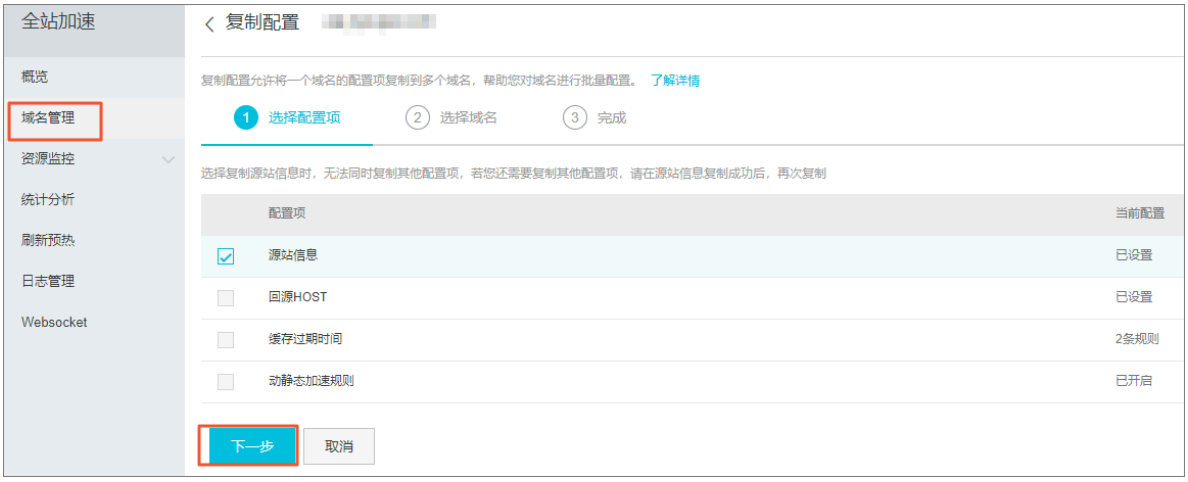
操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，选择您需要复制配置的域名，单击复制配置。
4. 勾选您需要复制的配置项，单击下一步。

说明：

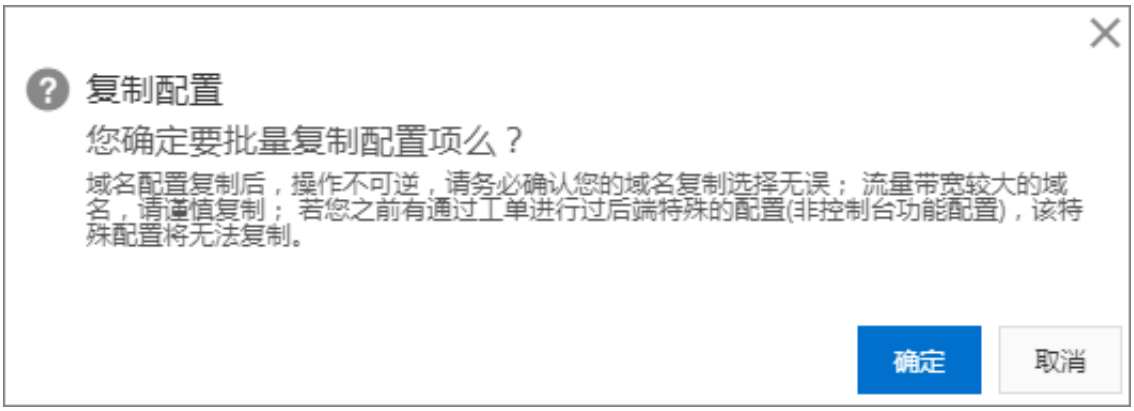
- 源站信息和非源站信息无法同时复制。
- 您无法复制HTTPS证书到其他域名，请您单独配置。
- 自定义回源头为增量复制。例如，假设您的A域名有2条回源头配置，您从B域名复制了5条内容，则你会有7条回源头配置内容。
- HTTP头为非增量复制。假设您的A域名配置了cache_control为private，您的B域名配置为public，复制后，您的cache_control为public。
- 开关类的配置复制，将会覆盖域名原有的配置。

- **Refer黑白名单或IP黑白名单将会覆盖域名原有配置。**

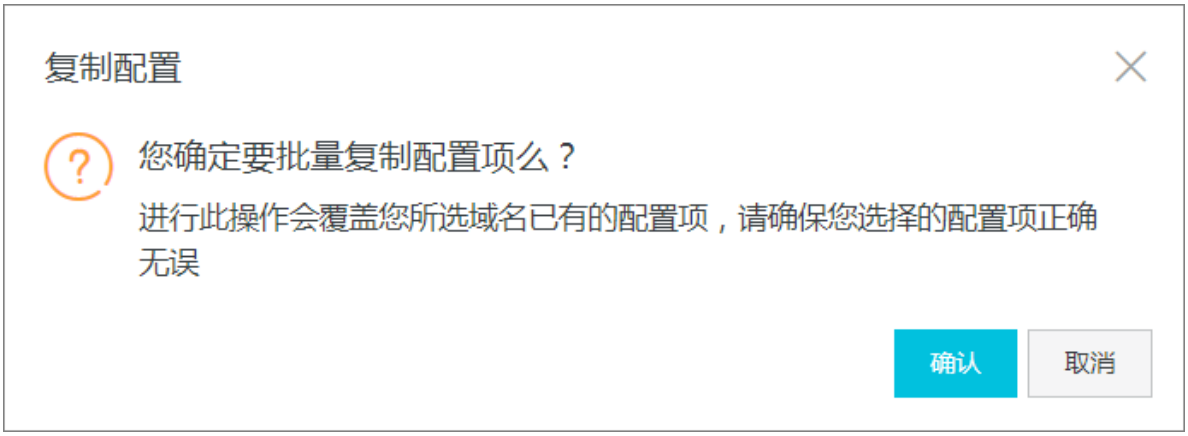


5. **勾选您想要批量配置的目标域名，单击下一步。**

   您也可以输入关键词查找域名。



6. **在复制配置对话框中，单击确认，批量复制成功。**



4 基本配置

4.1 修改基础信息

当您需要变更全站加速的服务区域时，您可以通过切换加速区域功能实现。

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，单击目标域名对应的配置。
4. 在基础信息区域，单击修改。
5. 在加速区域对话框，选择您需要切换的加速区域。

   选择加速区域时，注意事项如下：

   - 仅中国大陆

     如果选择仅中国大陆，则需要工信部备案。域名备案方法，请参见域名备案。
   - 全球

     如果选择全球，则需要工信部备案。域名备案方法，请参见域名备案。
   - 全球（不包含中国大陆）

     如果选择全球（不包含中国大陆），则无需工信部备案。

6. 单击确定。

4.2 配置源站

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

背景信息

全站加速支持的源站类型包括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:

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。

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

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，单击目标域名对应的配置。
4. 在源站信息区域，单击修改配置。
5. 在源站配置对话框，设置源站类型、源站地址和端口。

   在源站配置页面，需要配置的参数说明如下：

   - 源站类型

源站类型	说明
IP	支持多个服务器外网 IP， 阿里云ECS的IP可免审核。
源站域名	支持多个源站域名。  **说明:** 源站域名不能与加速域名相同，否则会造成循环解析，无法回源。 例如您的源站域名为img.yourdomain.com，则加速域名可设置为cdn.yourdomain.com。

源站类型	说明
OSS域名	您可以手动输入阿里云OSS Bucket的外网域名，如：xxx.oss-cn-hangzhou.aliyuncs.com。OSS外网域名可前往OSS控制台查看，也可直接选择同账号下的OSS Bucket。

- 端口

端口	说明
80端口	资源以HTTP或HTTPS协议回源到80端口。
443端口	资源以HTTP或HTTPS协议回源到443端口。如果您的源站为单个IP地址提供多个域名服务，您需要配置回源SNI。
自定义端口	目前仅支持以HTTP协议回源到自定义端口。请先将静态协议跟随回源配置为HTTP协议，再配置自定义端口，操作方法请参见配置静态协议跟随回源。 - 如果您的静态协议配置为跟随，则无法配置自定义端口。 - 如果您通过OpenAPI将回源协议设置为跟随，请确保您的回源协议和自定义端口均能正常使用。 - 如果您通过端口设置了回源协议（HTTP或HTTPS）和自定义端口，则无论您在CDN控制台如何设置，都按照端口配置回源。

6. 单击确定。

5 回源配置

5.1 配置回源HOST

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

背景信息

回源HOST指CDN节点在回源过程中，在源站访问的站点域名。

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

源站和回源HOST的区别：

- **源站：源站决定了回源时请求到的具体IP地址。**
- **回源HOST：回源HOST决定了回源请求访问到该IP地址上的具体站点。**

回源HOST的默认值为：

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

示例：

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

操作步骤

1. **登录全站加速控制台。**
2. **在左侧导航栏，单击域名管理。**
3. **在域名管理页面，单击目标域名对应的配置。**
4. **在指定域名的左侧导航栏，单击回源配置。**
5. **在回源HOST区域，单击修改配置。**

6. 打开回源HOST开关，选择域名类型。

7. 单击确定。

5.2 配置静态协议跟随回源

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

背景信息

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

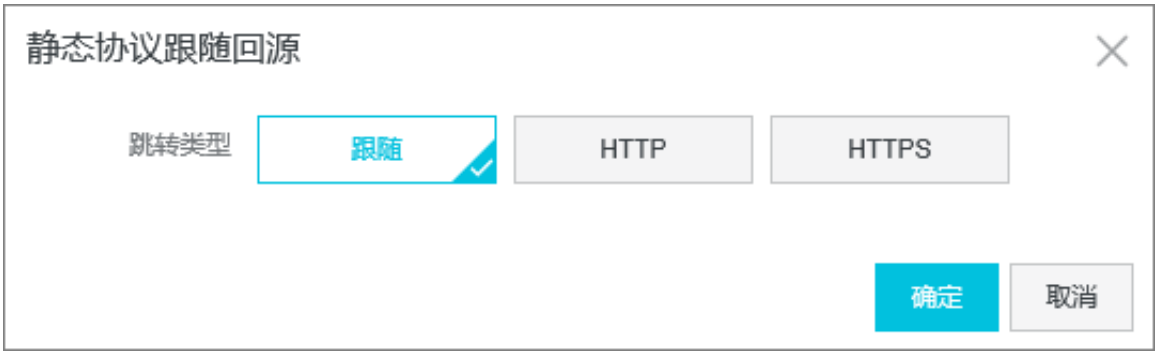
> **说明:**
> 源站需要同时支持80端口和443端口，否则有可能会造成回源失败。

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的配置。
4. 在指定域名的左侧导航栏，单击回源配置。
5. 在静态协议跟随回源区域，打开静态协议跟随回源开关。
6. 单击修改配置。

7. 在静态协议跟随回源对话框，选择的回源协议类型为：跟随、HTTP或HTTPS。

   - 跟随：客户端以HTTP或HTTPS协议请求全站加速，全站加速跟随客户端的协议请求源站。
   - HTTP：全站加速只以HTTP协议回源。
   - HTTPS：全站加速只以HTTPS协议回源。



8. 单击 确定。

5.3 开启私有Bucket回源授权

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

背景信息

私有Bucket回源授权指如果加速域名需要回源至您账号下标记为私有Bucket的源站，则需要进行授权。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。

您可以配合使用全站加速提供的Refer防盗链和鉴权功能，有效保护您的资源安全。详细说明，请参见*Referer*防盗链和配置*URL*鉴权。

> **注意:**
>
> - 仅支持源站类型为OSS域名的加速域名开启私有Bucket回源功能。
> - 进行一次回源授权，即授权CDN对您所有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回源授权功能，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。如果您授权的私有Bucket内容并不适合作为CDN加速域名的回源内容，请勿授权或者开启此功能。
> - 如果您的网站有被攻击的风险，请购买高防服务。同时，请勿授权或开启私有Bucket回源授权功能。

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，单击目标域名对应的配置。
4. 在指定域名的左侧导航栏，单击回源配置。
5. 在私有Bucket回源区域，单击点击授权。

6. 单击同意授权。

7. 在私有Bucket回源区域，打开私有Bucket回源开关。

5.4 关闭私有Bucket回源授权

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

背景信息

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

操作步骤

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

4. 单击待删除权限对应的移除权限。

   在移除权限确认对话框中，单击确认。

5. 返回RAM角色管理页面，单击待删除角色对应的删除。

   在删除RAM角色确认对话框中，单击确认。

5.5 配置回源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

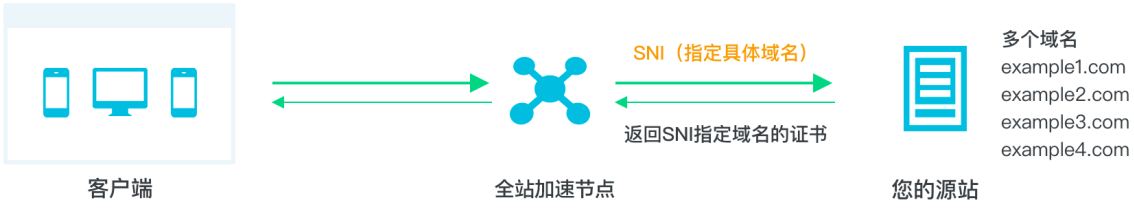
服务器名称指示 Server Name Indication（SNI）是一个扩展的传输层安全性协议 Transport Layer Security（TLS）。在该协议下，握手过程开始时，客户端会告诉它正在连接的那台服务器即将要连接的主机名称，以允许该服务器在相同的IP地址和TCP端口号上呈现多个证书，即一台服务器可以为多个域名提供服务。因此，同一个IP地址上提供的多个安全的HTTPS网站（或其他任何基于TLS的服务），不需要使用相同的证书。

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，则无需设置回源SNI。

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. **在域名管理页面，单击目标域名对应的配置。**
4. **在指定域名的左侧导航栏，单击回源配置。**
5. **在回源SNI区域，单击修改配置。**
6. **打开回源SNI开关，根据所需输入服务器源站提供服务的域名。**

   SNI在阿里云全站加速产品中指源站域名。如果您的源站服务器使用单个IP地址提供多个域名的HTTPS服务，则需要设置回源SNI，指明所请求的具体域名。

7. **单击确定。**

5.6 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。

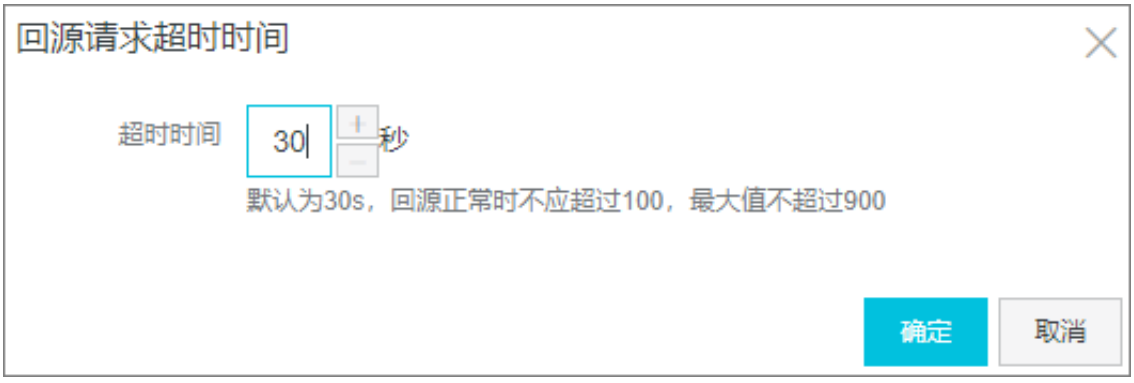
5.7 回源请求超时时间

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

   全站加速的回源请求超时时间正常不超过100秒，配置的最大值不能超过900秒。



7. 单击确定。

5.8 配置自定义回源HTTP头

HTTP请求回源时，您可以添加或删除回源HTTP头。

背景信息

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

在HTTP消息头中，按其出现的上下文环境，分为通用头、请求头、响应头等。

说明:
如果您在配置自定义回源HTTP头时，出现下图情况，请您重新配置（无法添加的是“内部保留”字段）。

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，单击目标域名对应的配置。
4. 在指定域名的左侧导航栏，单击回源配置。
5. 单击自定义回源HTTP头。
6. 单击添加。
7. 在HTTP头设置页面，选择回源参数，并设置取值。

8. 单击确定。

6 动静态加速规则配置

6.1 配置静态文件类型

全站加速支持以后缀名的方式设定静态文件类型。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。

背景信息

- **开启**

  只有开启动态加速开关时，您才可以自定义动静态资源加速规则，静态资源使用边缘缓存，动态资源采用最优路由回源。

- **关闭**

  当关闭动态加速开关时，动态资源无加速效果，仅保留静态资源的边缘缓存功能。

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，单击目标域名对应的配置。**
4. **在指定域名的左侧导航栏，单击动静态加速规则。**
5. **在动态加速页面，打开动态加速开关。**

6. 在静态文件类型对话框，单击修改配置。
7. 选择静态文件类型。

8. 单击确定。

6.2 配置静态文件URI

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CDN节点进行缓存和分发。

背景信息

- 开启

  只有开启动态加速开关时，您才可以自定义动静态资源加速规则，静态资源使用边缘缓存，动态资源采用最优路由回源。

- 关闭

  当关闭动态加速开关时，动态资源无加速效果，仅保留静态资源的边缘缓存功能。

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，单击目标域名对应的配置。
4. 在指定域名的左侧导航栏，单击动静态加速规则。

5. **在动态加速页面，打开动态加速开关。**

6. **单击静态URI。**
7. **在静态URI对话框，单击修改配置。**
8. **设置静态URI。**

9. **单击确定。**

6.3 配置静态文件路径

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CDN节点进行缓存和分发。

背景信息

- **开启**

  只有开启动态加速开关时，您才可以自定义动静态资源加速规则，静态资源使用边缘缓存，动态资源采用最优路由回源。

- **关闭**

  当关闭动态加速开关时，动态资源无加速效果，仅保留静态资源的边缘缓存功能。

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，单击目标域名对应的配置。**
4. **在指定域名的左侧导航栏，单击动静态加速规则。**
5. **在动态加速页面，打开动态加速开关。**

6. **单击静态路径。**
7. **在静态路径对话框，单击修改配置。**

8. 设置静态路径。

说明:

通配符是一种特殊语句，包括符号：*和?，用来模糊搜索静态文件路径。*代替零个、单个或多个字符，?代替1个字符。

9. 单击确定。

6.4 配置协议跟随回源

动态资源回源使用协议需要和客户端访问资源的协议保持一致。如果未配置协议跟随回源类型，则全站加速默认跟随源站端口回源。

背景信息

- 开启

  只有开启动态加速开关时，您才可以自定义动静态资源加速规则，静态资源使用边缘缓存，动态资源采用最优路由回源。

- 关闭

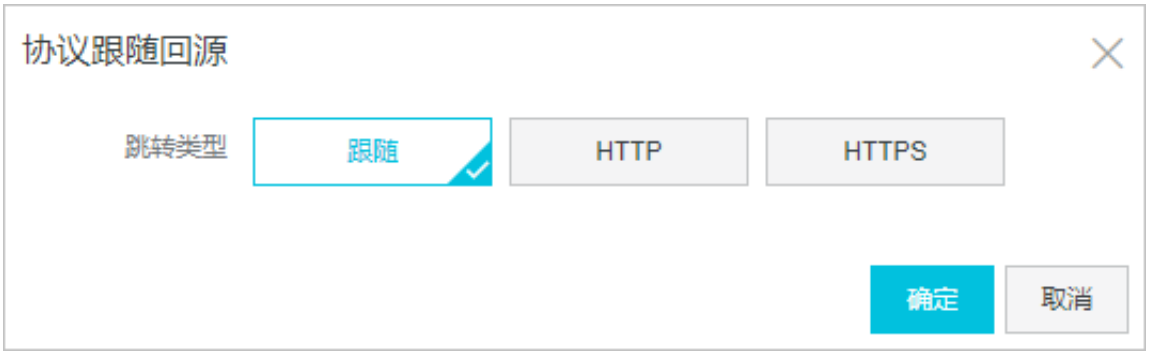
  当关闭动态加速开关时，动态资源无加速效果，仅保留静态资源的边缘缓存功能。

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，单击目标域名对应的配置。

4. 在指定域名的左侧导航栏，单击动静态加速规则。
5. 在动态加速页面，打开动态加速开关。

6. 单击协议跟随回源。
7. 在协议跟随回源对话框，单击修改配置。
8. 设置静态路径。
   - 跟随：客户端以HTTP或HTTPS协议请求全站加速，全站加速跟随客户端的协议请求源站。
   - HTTP：全站加速只以HTTP协议回源。
   - HTTPS：全站加速只以HTTPS协议回源。



9. 单击确定。

7 节点缓存设置

7.1 配置缓存过期时间

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

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。

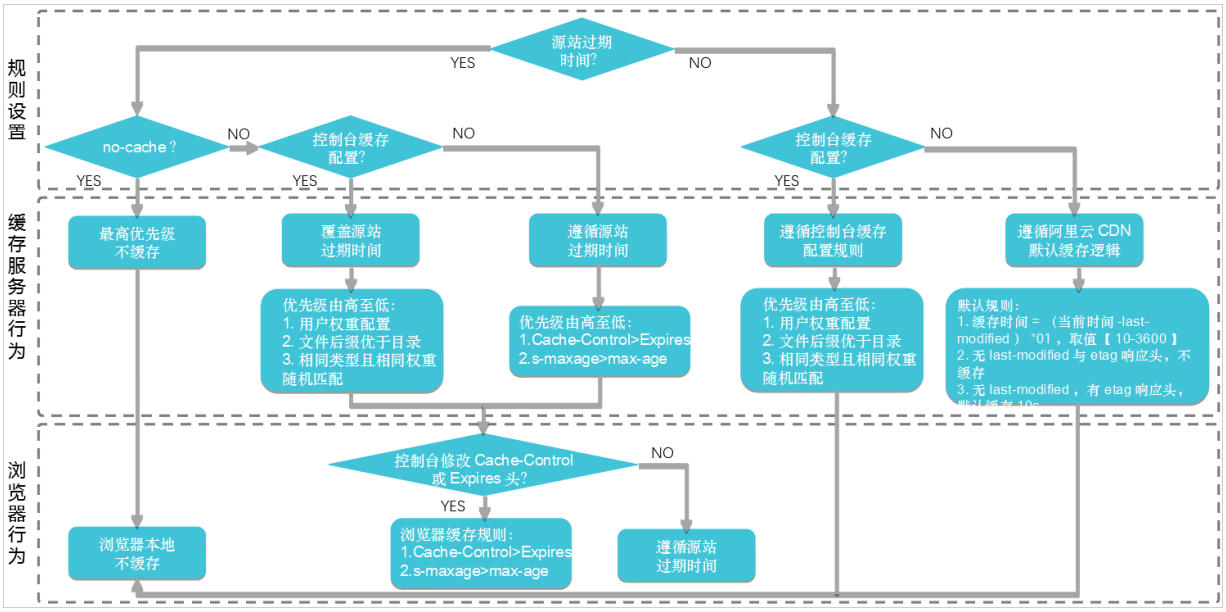
- **支持用户自定义缓存策略优先级。**
- **Cache的默认缓存策略：**
  - **如果源站已经有Cache配置，则缓存过期时间的配置，其优先级高于源站的配置。**
  - **如果源站没有Cache配置，则支持按目录、文件后缀名两种方式设置缓存过期时间（支持设置完整路径缓存策略）。**

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	1s	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。

CDN节点上资源的缓存策略如下图所示。



说明:

- Cache的默认缓存策略用于配置文件过期时间，在此配置的优先级高于源站配置。如果源站未配置cache，则支持按目录、文件后缀两种方式设置（支持设置完整路径缓存策略）。
- CDN节点上缓存的资源，可能由于热度较低而被提前从节点删除。

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的配置。
4. 在指定域名的左侧导航栏，单击缓存配置。
5. 在缓存过期时间页签，单击添加。
6. 配置缓存规则，您可以选择按目录或文件后缀名进行配置。

配置项	说明
类型	· 目录：指定路径下的缓存资源。 · 文件后缀名：指定文件类型的缓存资源。
内容	· 添加单条目录（支持完整路径）时，须以“/”开头，如*/directory/aaa*。 · 添加多个文件后缀名时，须以半角逗号分隔，例如：`JPG,txt`。

配置项	说明
过期时间	资源对应的缓存时间。过期时间最多设置为3年，建议您参照以下规则进行配置： · 对于不经常更新的静态文件（如图片类型、应用下载类型等），建议您将缓存时间设置为1个月以上。 · 对于频繁更新的静态文件（如js、css等），您可以根据实际业务情况设置。 · 对于动态文件（如php、jsp、asp等），建议您将缓存时间设置为0s，即不缓存。
权重	缓存规则的优先级。 **说明:** · 取值范围：1～99间的整数。数字越大，优先级越高，优先生效。 · 不推荐设置相同的权重，权重相同的两条缓存策略优先级随机。 · 缓存策略1：文件名后缀为jpg、png的所有资源过期时间设置为1月，权重设置为90。 · 缓存策略2：目录为*/www/dir/aaa*过期时间设置为1小时，权重设置为70。 · 缓存策略3：完整路径为*/www/dir/aaa/example.php*过期时间设置为0s，权重设置为80。

7. 单击确定。

您也可以单击修改或删除，对当前配置的缓存策略进行相应操作。

7.2 配置HTTP头

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

背景信息

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

在HTTP消息头中，按其出现的上下文环境，分为通用头、请求头、响应头等。目前阿里云全站加速提供10个HTTP响应头参数可供您自行定义取值，参数解释如下表所示。

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。

- HTTP响应头的设置会影响该加速域名下所有资源，当您通过客户端（例如浏览器）访问资源时，会影响请求响应，但不会影响缓存服务器。
- 目前仅支持上述HTTP头设置。如果您有其他HTTP头设置需求，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，单击目标域名对应的配置。
4. 在指定域名的左侧导航栏，单击缓存配置。
5. 单击HTTP头。
6. 在HTTP头设置页签，单击添加。

7. 配置HTTP头的参数和取值。
8. 单击确定，配置成功。

   您也可以单击修改或删除，对当前配置的HTTP头进行相应操作。

7.3 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。

Web服务器返回HTTP 404状态码时，会自动跳转到404 Not Found页面。由于网页URL生成规则改变、网页文件更名或移动位置、导入链接拼写错误等，导致原来的URL地址无法访问；当Web服务器接收到类似请求时，会返回一个404状态码，告诉浏览器需要请求的资源并不存在。导致这个错误的原因如下：

- 无法在所请求的端口上访问Web站点。
- Web服务扩展锁定策略阻止本请求。
- MIME映射策略阻止本请求。

说明:

访问单个资源时，若出现资源无法找到返回404状态码，将会跳转到404页面；若访问URL链接中包含多个资源，只有部分资源不能正常访问，则该页面不会发生404页面跳转。

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，单击目标域名对应的配置。
4. 在指定域名的左侧导航栏，单击缓存配置。
5. 单击自定义页面。
6. 在自定义页面页签，单击添加。

7. 配置自定义页面的参数和取值。

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

8. 单击确定。

   您也可以单击修改或删除，对当前配置进行相应操作。

7.4 配置重写

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。

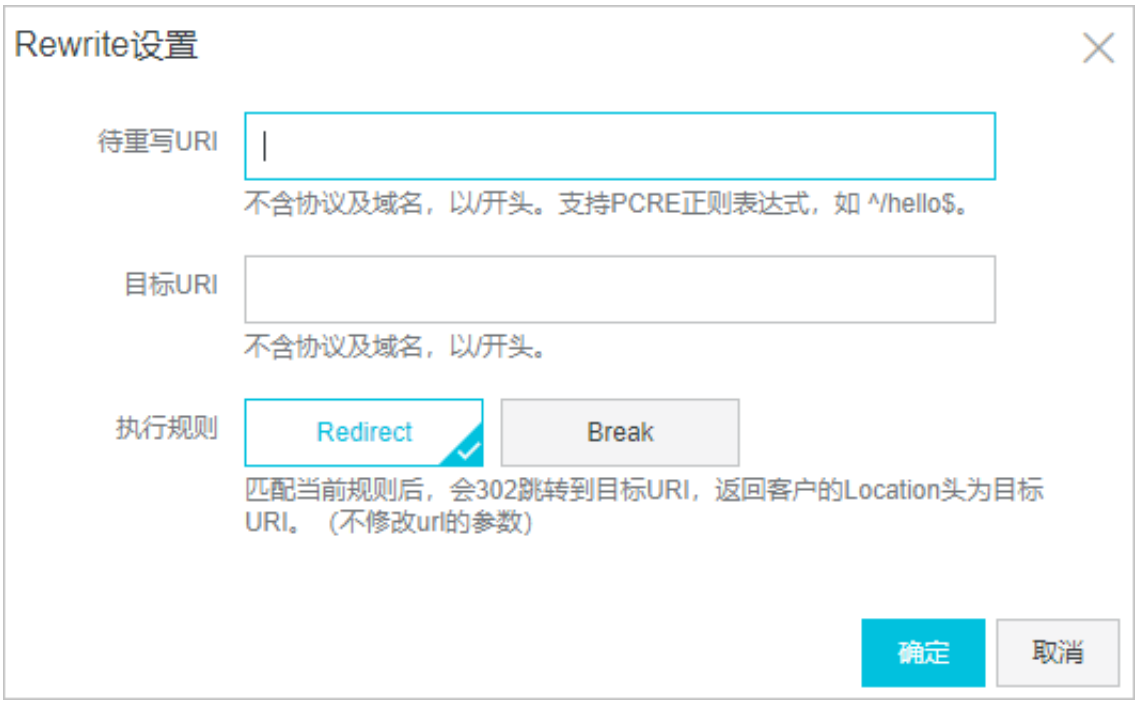
操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的配置。
4. 在左侧导航栏，单击缓存配置。
5. 单击重写。
6. 在重写区域框中，单击添加。

7. 根据您的需求，配置待重写URI、目标URI和执行规则。

   重写执行规则如下：

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



8. 单击确定。

   您也可以单击修改或删除，对当前配置的重写规则进行相应操作。

> **说明:**
> 单个域名可以配置的重写规则数量上限是50个。

样例	待重写URI	目标URI	执行规则	结果说明
样例一	/hello	/index.html	Redirect	客户端请求`http://domain.com/hello`，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	待重写URI	目标URI	执行规则	结果说明
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。

8 HTTPS设置

8.1 什么是HTTPS证书

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

什么是HTTPS?

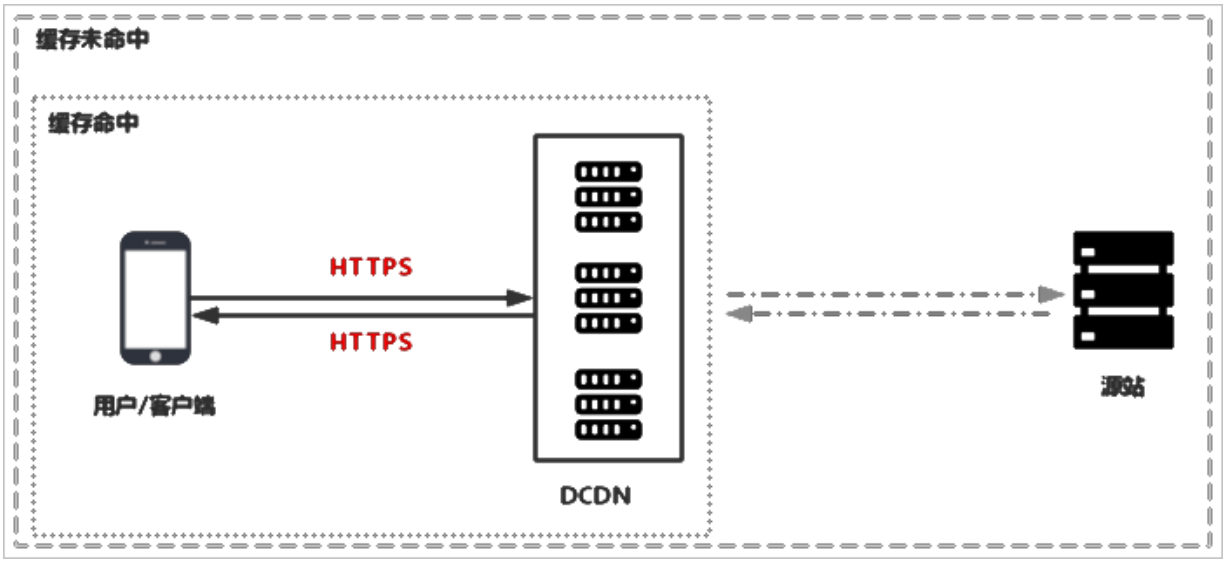
HTTP协议以明文方式发送内容，不提供任何方式的数据加密。HTTPS协议是以安全为目标的HTTP通道，简单来说，HTTPS是HTTP的安全版，即将HTTP用SSL/TLS协议进行封装，HTTPS的安全基础是SSL/TLS协议。HTTPS提供了身份验证与加密通讯方法，被广泛用于万维网上安全敏感的通讯，例如交易支付。

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

工作原理

在阿里云全站加速控制台开启的HTTPS协议，将实现客户端和全站加速之间请求的HTTPS加密。从源站获取的资源给客户端时，按照源站的配置方式进行。建议源站配置并开启HTTPS，实现全链路的HTTPS加密。

HTTPS加密流程如下图所示。



1. 客户端发起HTTPS请求。

2. 服务端生成公钥和私钥（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。

功能优势

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

应用场景

主要将应用场景分为五类，如下表所示 。

应用场景	说明
企业应用	若网站内容包含crm、erp等信息，这些信息属于企业级的机密信息，若在访问过程中被劫持或拦截窃取，对企业是灾难级的影响。

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

注意事项

HTTPS安全加速功能注意事项，如下表所示。

分类	注意事项
配置	· 支持泛域名HTTPS服务。 · 支持HTTPS安全加速的启用和停用。 - 启用：您可以修改证书，系统默认兼容HTTP和HTTPS请求。您也可以设置强制跳转，自定义源请求方式。 - 停用：停用后，系统不再支持HTTPS请求且不再保留证书或私钥信息。再次开启证书，需要重新上传证书或私钥。详细说明，请参见配置HTTPS证书。 · 您可以查看证书，但由于私钥信息敏感，不支持私钥查看。请妥善保管证书相关信息。 · 您可以更新证书，但请谨慎操作。更新HTTPS证书后1分钟内全网生效。
计费	HTTPS计费标准请参见HTTPS计费详情。 说明: HTTPS根据请求数单独计费，请确保账户余额充足再开通HTTPS服务，以免因HTTPS服务欠费影响您的全站加速服务。

分类	注意事项
证书	· 开启HTTPS安全加速功能的加速域名，您需要上传格式均为PEM的证书和私钥。 说明: 由于全站加速采用的Tengine服务基于Nginx，因此只支持Nginx能读取的PEM格式的证书。详细说明，请参见证书格式说明。 · 上传的证书需要和私钥匹配，否则会校验出错。 · 不支持带密码的私钥。 · 只支持携带SNI信息的SSL/TLS握手。 其他证书相关的常见问题，请参见更多证书问题。

8.2 证书格式说明

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

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、免费证书或上传自定义证书。自定义上传证书只支持PEM格式和其他格式转的PEM格式。

Root CA机构颁发的证书

Root CA机构提供的证书是唯一的，一般包括Apache、IIS、Nginx和Tomcat。阿里云CDN使用的证书是Nginx，.crt为证书，.key为私钥。

证书规则为：

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

Linux环境下，PEM格式的证书示例如下图。

中级机构颁发的证书

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

说明：

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

中级机构颁发的证书链：

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

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

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

证书链规则：

- **证书之间不能有空行。**

- **每一份证书遵守第一点关于证书的格式说明。**

RSA私钥格式要求

RSA私钥规则：

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

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

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

然后将`new_server_key.pem`**的内容与证书一起上传。**

证书格式转换方式

HTTPS配置只支持PEM格式的证书，其他格式的证书需要转换成PEM格式，建议通过openssl工具进行转换。下面是几种比较流行的证书格式转换为PEM格式的方法。

- **DER转换为PEM**

  DER格式一般出现在Java平台中。

  - **证书转化：**

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

  - **私钥转化：**

    ```
    openssl rsa -inform DER -outform pem -in privatekey.der -out
    privatekey.pem
    ```

- **P7B转换为PEM**

  P7B格式一般出现在Windows Server和Tomcat中。

  - **证书转化：**

    ```
    openssl pkcs7 -print_certs -in incertificat.p7b -out outcertifi
    cate.cer
    ```

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

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

- **PFX转换为PEM**

  PFX格式一般出现在Windows Server中。

  - **证书转化：**

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

  - **私钥转化：**

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

免费证书

您在使用免费证书时，注意事项如下：

- **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。**
- **无论您启用自定义证书、托管证书或免费证书，都可以相互切换。**
- **免费证书有效期为1年，到期后自动续签。**
- **在使用免费证书过程中，如果您关闭HTTPS安全加速，再次开启并使用免费证书时，会直接使用已经申请过但未过期的证书。如果开启HTTPS安全加速时，证书已过期，则会重新申请免费证书。**

其他证书相关

使用其他证书时的注意事项如下：

- 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，操作方法请参见配置*HTTPS*证书。
- 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。

其他证书的相关常见问题，请参见更多证书问题。

8.3 配置HTTPS证书

HTTPS以安全为目标的HTTP通道，HTTPS在全站加速上的应用，为全站加速的网络内容传输提供了更好的保障， 客户端在极速访问内容的同时，可以更安全有效的浏览网站内容。本文档介绍了不同类型的HTTPS证书的认证方式和配置方法。

前提条件

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

背景信息

目前全站加速仅支持PEM格式的证书，如果您的证书不是PEM格式，请进行格式转换，操作方法请参见证书格式说明。

HTTPS功能为增值服务，开启HTTPS将产生HTTPS请求数计费，该费用单独按量计费，不包含在全站加速流量包内。HTTPS计费介绍，请参见*#unique_55*。

根据证书认证级别分类如下：

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

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，单击目标域名对应的配置。
4. 在指定域名的左侧导航栏，单击HTTPS配置。
5. 在HTTPS证书区域，单击修改配置。

6. 在HTTPS设置界面，打开HTTPS安全加速开关，配置证书相关参数。

   当您打开HTTPS安全加速开关时，系统弹出确认开启HTTPS界面，该操作单独计费，您可以根据所需选择是否开启。HTTPS计费标准请参考*#unique_55*。

参数	说明
证书类型	· 云盾 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。 · 自定义 如果证书列表中无

参数	说明
证书名称	当证书类型选择云盾或自定义时，需要配置证书名称。

参数	说明
内容	当证书类型选择自定义时，需要配置该参数。 配置方法请参考内容输入框下方的pem编码参考样例。

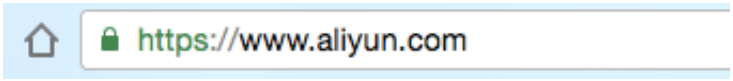
参数	说明
私钥	当证书类型选择自定义时，需要配置该参数。配置方法请参考私钥输入框下方的pem编码参考样例。

7. 单击确定。

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。

8. 验证证书是否生效。

更新HTTPS证书1分钟后全网生效，使用HTTPS方式访问资源，如果浏览器中出现绿色HTTPS标识，则HTTPS安全加速生效。



8.4 设置HTTP/2

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

前提条件

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

说明:

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

背景信息

HTTP/2也被称为HTTP 2.0，是最新的HTTP协议。目前，Chrome、 IE11、Safari和Firefox等主流浏览器已经支持HTTP/2协议。HTTP/2优化了性能，兼容了HTTP/1.1的语义，与SPDY相似，与HTTP/1.1有巨大区别。

HTTP/2的优势：

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

- 服务端推送（Server push）：同SPDY一样，HTTP/2也具有客户端推送功能。目前，大多数网站已经启用HTTP/2，如淘宝。使用浏览器Chrome登录控制台，您可以查看是否启用HTTP/2。

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

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的配置。
4. 在指定域名的左侧导航栏，单击HTTPS配置。
5. 在HTTP/2设置页签，打开HTTP/2开关，开启该功能。

8.5 设置强制跳转

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

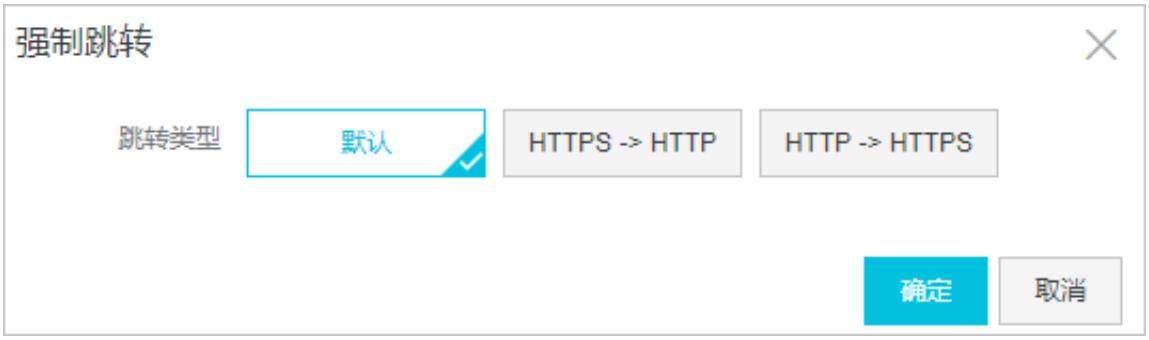
前提条件

配置强制跳转类型前，您需要配置HTTPS证书。详细说明，请参见*#unique_18*。

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。
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>
```

8.6 配置TLS

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

前提条件

执行该操作前，请您确保已成功配置HTTPS证书，操作方法请参见*#unique_18*。

背景信息

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

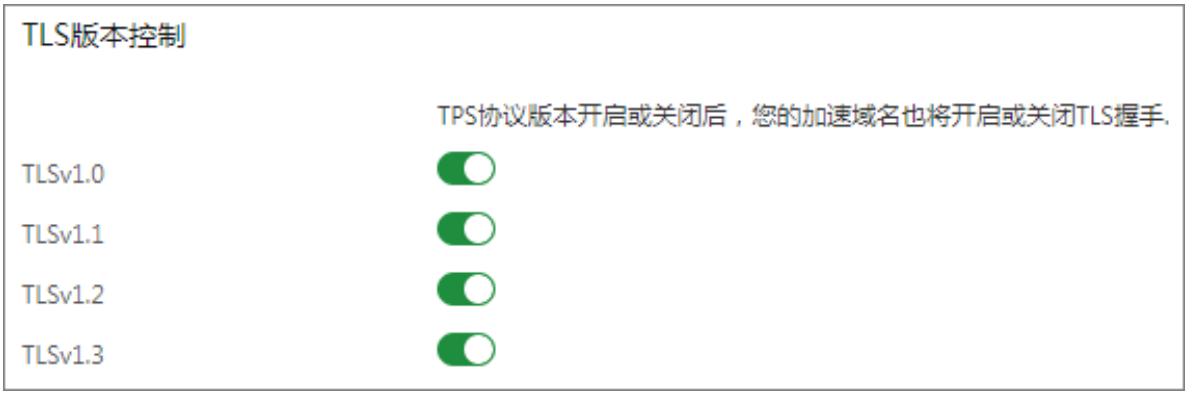
操作步骤

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

   TLS协议说明如下表所示。

协议	说明	支持的主流浏览器
TLSv1.0	RFC2246，1999年发布，基于SSLv3.0，该版本易受各种攻击（如BEAST和POODLE），除此之外，支持较弱加密，对当今网络连接的安全已失去应有的保护效力。不符合PCI DSS合规判定标准。	· IE6+ · Chrome 1+ · Firefox 2+
TLSv1.1	RFC4346，2006年发布，修复TLSv1.0若干漏洞。	· IE 11+ · Chrome 22+ · Firefox 24+ · Safri 7+
TLSv1.2	RFC5246，2008年发布，目前广泛使用的版本。	· IE 11+ · Chrome 30+ · Firefox 27+ · Safri 7+

协议	说明	支持的主流浏览器
TLSv1.3	RFC8446，2018年发布，最新的TLS版本，支持0-RTT模式（更快），只支持完全前向安全性密钥交换算法（更安全）。	· Chrome 70+ · Firefox 63+



说明:

目前TLSv1.0、TLSv1.1和TLSv1.2版本默认开启。

8.7 配置HSTS

通过开启HSTS（HTTP Strict Transport Security）功能，您可以强制客户端（如浏览器）使用HTTPS与服务器创建连接，降低第一次访问被劫持的风险。

前提条件

执行该操作前，请您确保已成功配置HTTPS证书，操作方法请参见*#unique_18*。

背景信息

当您的网站全站使用HTTPS后，需要将所有HTTP请求的301和302重定向到HTTPS。如果您在浏览器输入或直接单击HTTP链接，则服务器会将该HTTP请求的301和302重定向到HTTPS。该操作过程可能被劫持，导致重定向后的请求未发送到服务器，该问题可以通过HSTS来解决。

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

参数	说明
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。

参数	说明
includeSubDomains	可选参数。如果指定这个参数，说明这个域名所有子域名也适用上面的规则。
preload	可选参数，支持preload列表。

说明:

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

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击域名管理。
3. 在域名管理页面，单击目标域名对应的配置。
4. 在指定域名的左侧导航栏，单击HTTPS配置。
5. 在HSTS区域，单击修改配置。

6. 在HSTS设置对话框，打开HSTS开关，配置过期时间和包含子域名。
7. 单击确定。

9 访问控制

9.1 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。

9.2 URL鉴权配置

9.3 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#unique_64。

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。

9.4 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。
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*#unique_65*、*#unique_66*。

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*。

9.5 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*#unique_67*、*#unique_66*。

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*。

9.6 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。**

9.7 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。

9.8 User-Agent黑白名单

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

背景信息

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

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

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

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

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User-Agent黑/白名单页签，单击修改配置。

6. 根据您的需求配置黑白名单规则，单击确定。

10 性能优化

10.1 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。**

10.2 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。

10.3 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。

10.4 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 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

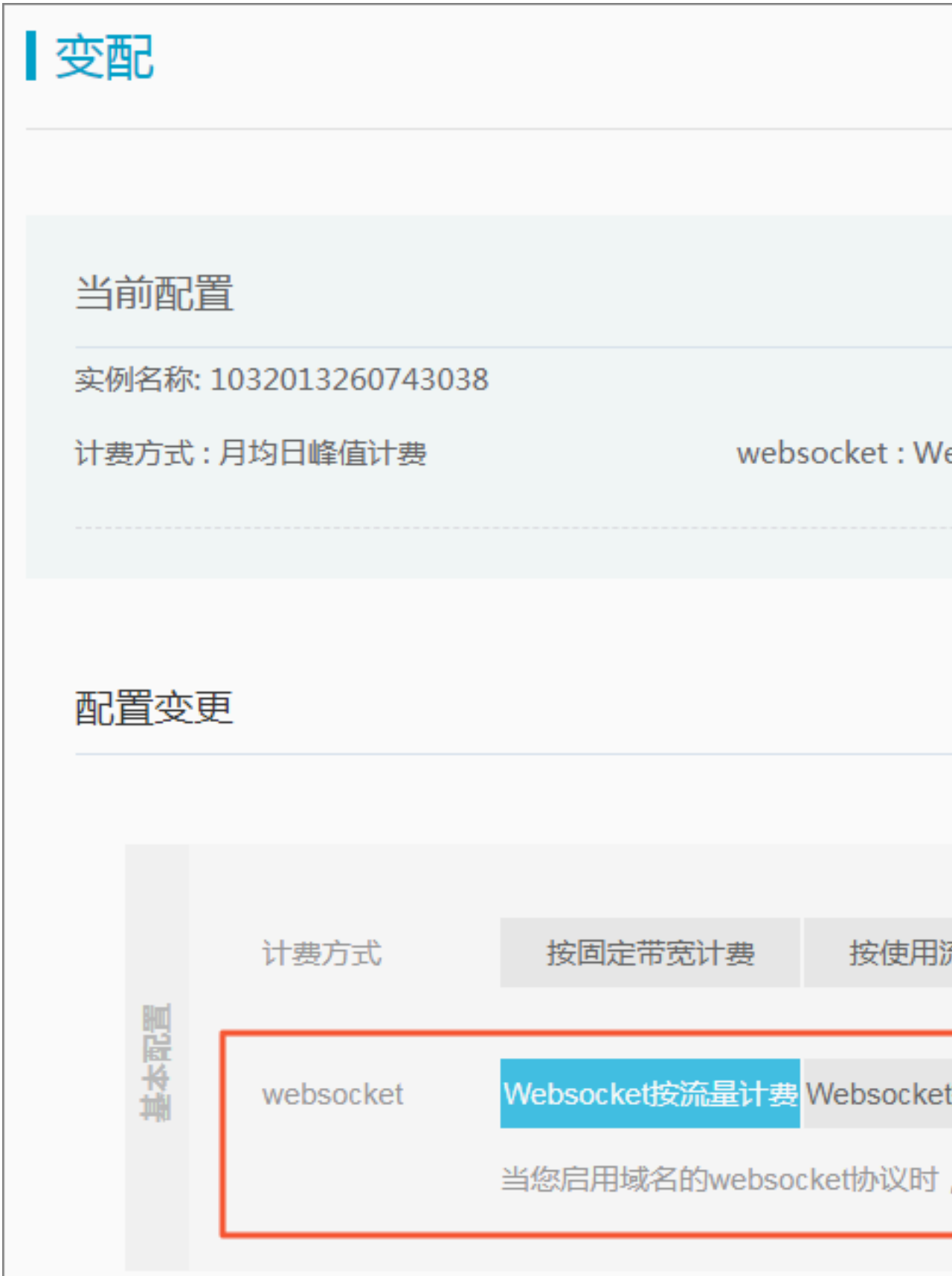
  越来越多的开发者借用移动设备的GPS功能来实现他们基于位置的网络应用。如果您一直记录终端用户的位置(比如您的 App 记录用户的运动轨迹)，就可以收集到更加细致化的数据。

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）。

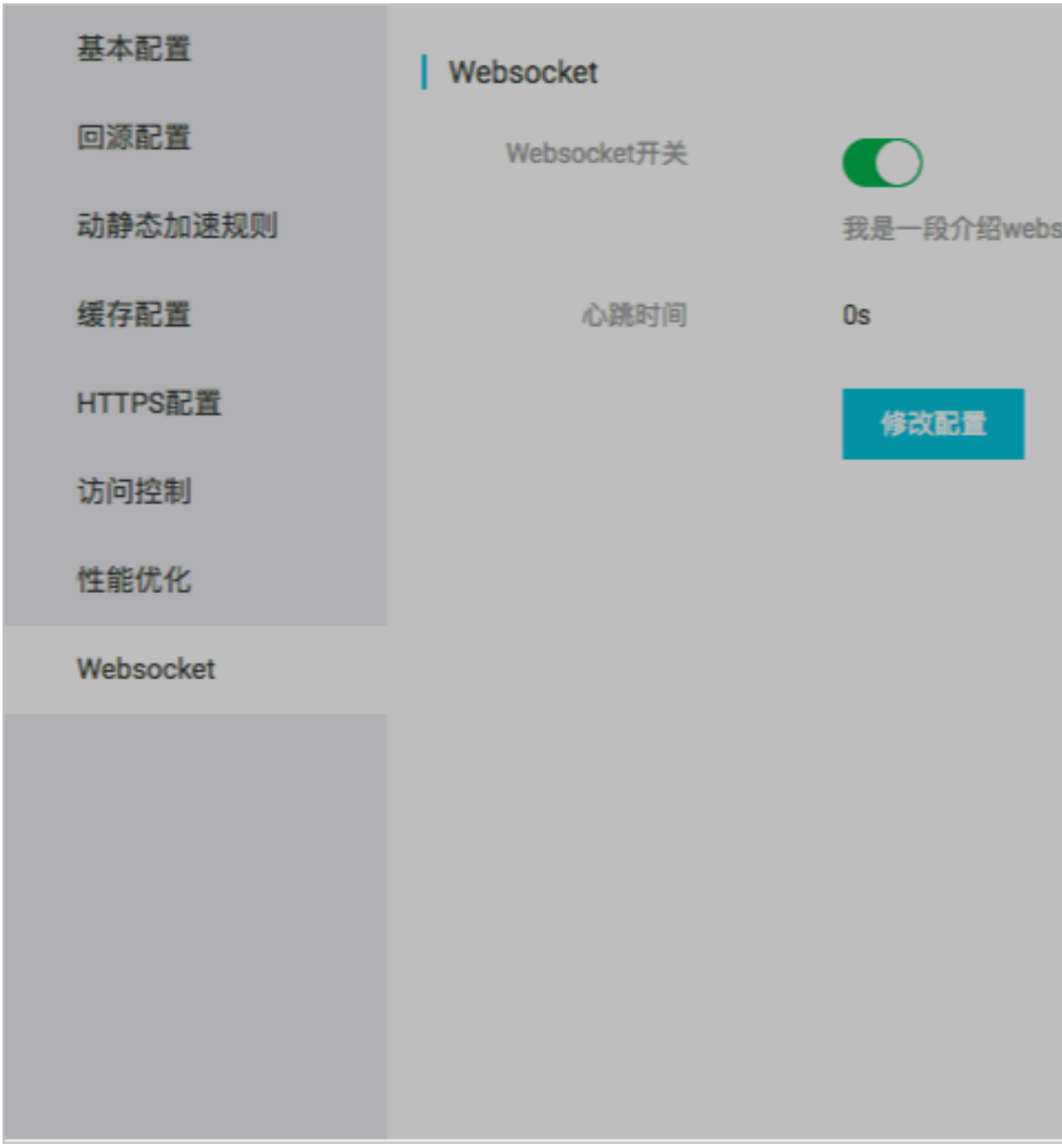
关于Websocket计费问题，请参考计费详情。

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。

12 配置刷新和预热

全站加速提供资源的刷新和预热功能。通过刷新功能，您可以强制CDN节点回源并获取最新文件；通过预热功能您可以在业务高峰期预热热门资源，提高资源访问效率。通过本文您可以了解刷新和预热功能的配置方法，也可以查询其操作记录。

背景信息

全站加速提供资源的刷新和预热功能的概念如下：

- 刷新功能是指提交URL刷新或目录刷新请求后，CDN节点的缓存内容将会被强制过期，当您向CDN节点请求资源时，CDN会直接回源站获取对应的资源返回给您，并将其缓存。刷新功能会降低缓存命中率。
- 预热功能是指提交URL预热请求后，源站将会主动将对应的资源缓存到CDN节点，当您首次请求时，就能直接从CDN节点缓存中获取到最新的请求资源，无需再回源站获取。预热功能会提高缓存命中率。

刷新和预热功能的详细说明如下表所示。

分类	原理	注意事项	生效时间
URL刷新	通过提供目录下文件的方式，强制CDN节点回源获取最新文件。	输入的URL必须带有`http://`或`https://`。 同一个ID每天最多提交2000个刷新请求，每次最多只能提交1000条。	5分钟内
目录刷新	通过提供目录及目录下所有文件的方式，强制CDN节点回源获取最新文件。	输入的URL，需以`http://`或`https://`开始，以`/`结束。 同一个ID每天最多提交100个刷新请求，一次可全部提交。	
URL预热	将指定的资源主动预热到CDN的二级节点上，用户首次访问即可直接命中缓存。	输入的URL必须带有`http://`或`https://`。 同一个ID每天最多预热500个URL，每次最多只能提交100条。	

说明:

资源刷新和预热完成时间将取决于您提交预热文件的数量、文件大小、源站带宽和网络状况等诸多因素。

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，单击目标域名对应的配置。**
4. **在左侧导航栏，单击刷新预热。**
5. **在刷新缓存区域，您可以根据所需，配置刷新或预热信息。**

6. **单击提交。**
7. **单击操作记录。**
8. **在操作记录区域，配置查询时间、操作类型、域名或URL，单击查询。**

   您可以查看资源刷新或预热的详细记录，包括：操作内容、操作类型、操作时间、状态和进度。

API接口

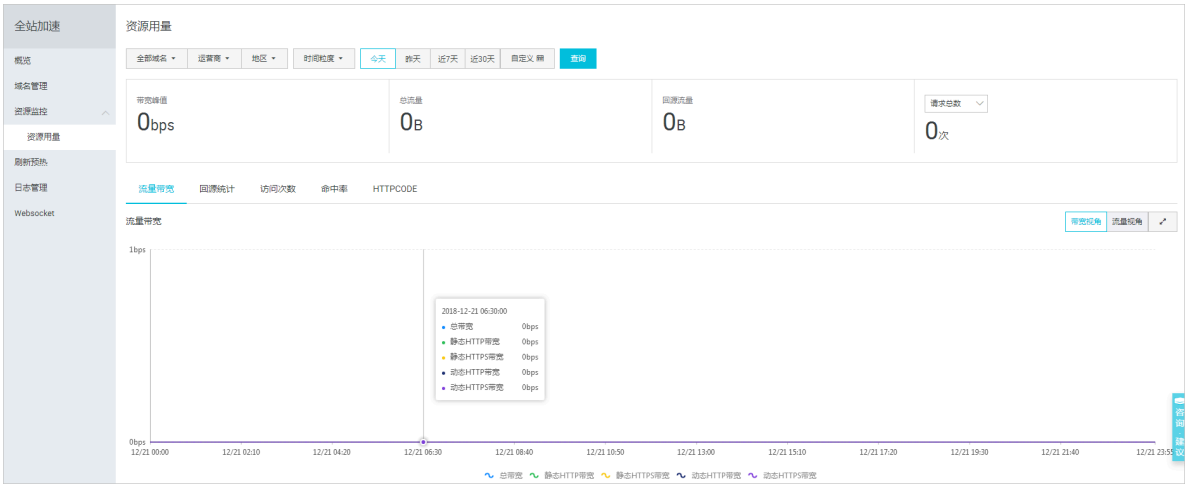
您可以调用API接口，实现资源的刷新和预热，详情如下表所示。

API	描述
DescribeDcdnRefreshTasks	调用DescribeDcdnRefreshTasks查询刷新、预热状态是否在全网生效。
RefreshDcdnObjectCaches	调用RefreshDcdnObjectCaches刷新节点上的文件内容、刷新指定URL内容至Cache节点。支持URL批量刷新。
PreloadDcdnObjectCaches	调用PreloadDcdnObjectCaches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。
DescribeDcdnRefreshQuota	调用DescribeDcdnRefreshQuota查询当日刷新URL、预热URL及刷新目录的上限和剩余次数。

13 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 。

14 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

15 IP应用加速

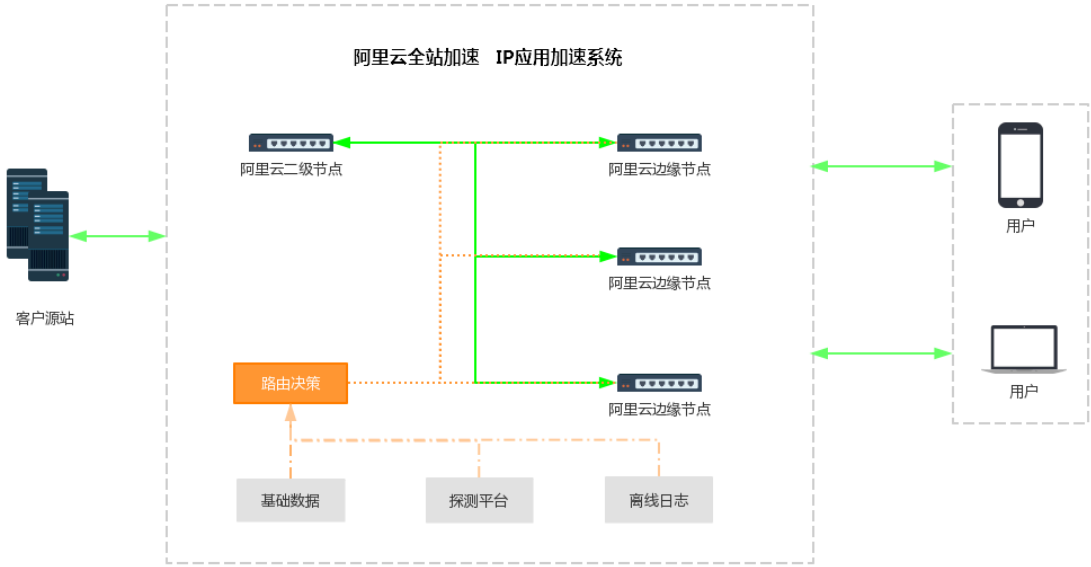
15.1 什么是IP应用加速?

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。

15.2 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*#unique_80*。

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*#unique_81*。**

15.3 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。

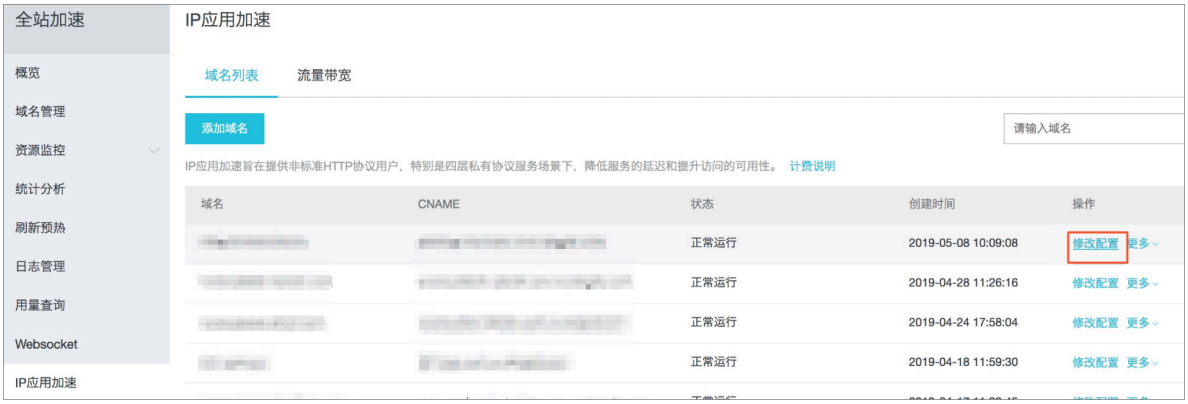
背景信息

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。

15.4 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"
```