ALIBABA CLOUD

阿里云

全站加速

域名管理

文档版本：20220712

阿里云

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
危险	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。	危险 重置操作将丢失用户配置数据。
警告	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。
注意	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。
说明	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	命令或代码。	执行 `cd /d C:/window` 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。	`switch {active|stand}`

目录

1.功能概述

阿里云全站加速控制台不仅可以帮助您完成域名配置等基本操作，也提供了实时数据分析的资源监控服务。同时您还可以了解自己的计费情况，随时变更计费方式。通过本文为您可以了解全站加速控制台界面展示和域名管理功能。

> **说明** 为了便于您对全站加速的学习和理解，本文从业务角度将全站加速控制台支持的功能划分为：域名管理和服务管理。

域名管理功能列表

功能	参考文档	说明	默认值
批量复制	批量复制域名配置	将某一个加速域名的一个或多个配置，复制到另外一个或多个域名上。	无
基本配置	切换加速区域	修改加速区域。	无
	配置源站	修改源站配置。	无
回源配置	配置回源HOST	修改回源HOST域名。	未开启
	配置静态协议跟随回源	全站加速根据设定的协议规则回源。回源使用的协议和客户端访问资源的协议保持一致。	未开启
	OSS私有Bucket回源	开通加速域名访问私有Bucket资源内容的权限。	未开启
	配置回源SNI	当源站IP绑定多个域名，且全站加速节点以HTTPS协议访问源站时，设置回源SNI，指明具体访问域名。	关闭
	配置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。	关闭
	回源请求超时时间	根据实际需求设置全站加速回源请求超时的最长等待时间。当回源请求等待时间超过配置的超时时间时，全站加速节点与源站的连接断开。	30秒
	配置自定义回源HTTP头	当HTTP请求回源时，可以添加或删除回源HTTP头。	关闭
	配置静态文件路径	指定静态文件的路径。	未开启

功能	参考文档	说明	默认值
动态加速规则	配置静态文件类型	指定静态文件的后缀名。	未开启
	配置静态文件URI	指定静态文件的URI	未开启
	动态内容回源配置	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。	未开启
缓存配置	配置缓存过期时间	自定义指定资源的缓存过期时间规则。	无
	配置自定义HTTP响应头	配置HTTP响应头，目前提供10个HTTP响应头参数可供自行定义取值。	无
	自定义页面	根据所需自定义HTTP或者HTTPS响应返回码跳转的完整URL地址。	404
	配置URI重写规则	对请求的URI进行修改和302重定向至目标URI。	无
HTTPS配置	配置HTTPS证书	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。	关闭
	配置HTTP/2	二进制协议带来更多扩展性、内容安全性、多路复用、头部压缩等优势。	未开启
	配置OCSP Stapling	查询OCSP（Online Certificate Status Protocol）信息，降低客户端验证请求延迟，减少等待查询结果的响应时间。	未开启
	配置强制跳转	加速域名开启HTTPS安全加速的前提下，支持自定义设置，将原请求方式进行强制跳转。	未开启
	配置TLS版本控制	TLS协议版本开启后，加速域名开启TLS握手。目前只支持TLSv1.0、TLSv1.1、TLSv1.2和TLSv1.3版本。	关闭

功能	参考文档	说明	默认值
	配置HSTS	HSTS的作用是强制客户端（如浏览器）使用HTTPS与服务器创建连接。	关闭
访问控制	配置Referer防盗链	通过配置访问的Refer黑名单和白名单来实现对访客身份的识别和过滤，从而限制访问全站加速资源的用户。	未开启
	配置URL鉴权	通过配置URL鉴权来保护用户站点的资源不被非法站点下载盗用。	未开启
	配置IP黑白名单	通过配置IP黑名单和白名单来实现对访客身份的识别和过滤，从而限制访问全站加速资源的用户。	未开启
	配置User-Agent黑白名单	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，从而限制访问全站加速资源的用户。	未开启
性能优化	页面优化	压缩与去除页面中无用的空行、回车等内容，有效缩减页面大小。	未开启
	智能压缩	支持多种内容格式的智能压缩，有效减少您传输内容的大小。	未开启
	Brotli压缩	开启Brotli压缩功能，全站加速节点向您返回请求的资源时，会对文本文件进行Brotli压缩，可以有效缩小传输文件的大小，提升文件传输效率，减少带宽消耗。	未开启
	过滤参数	当URL请求中携带 `?` 和*参数*时，全站加速节点在收到URL请求后，判断是否需要携带参数的URL返回源站。	未开启
	拖拽播放	开启拖拽播放功能后，当播放视音频时，随意拖拽播放进度，而不影响视音频的播放效果。	未开启

功能	参考文档	说明	默认值
安全配置	DCDN WAF防护（旧版）	DCDN结合Web应用防火墙功能，可以帮您主动防护各类Web应用漏洞，抵抗SQL注入、Webshell上传、XSS跨站等常见Web攻击。	未开启
	配置机器流量管理	为了帮助企业防控恶意爬取信息，恶意盗刷流量等业务风险。阿里云推出机器流量管理业务，该业务基于合法爬虫，威胁情报等多维度数据，配合AI智能，精准识别机器流量并自动应对，可对流量进行拦截、人机识别等处置手段。	未开启
	配置DDoS防护	阿里云全站加速为您提供DDoS防护功能，帮助您的加速域名更好地防御DDoS攻击。	未开启
	配置频次控制	如果您的网站因遭受恶意CC攻击导致响应缓慢，可通过频次控制功能提供的默认策略或自定义策略来拦截恶意流量，秒级阻断访问该网站的所有请求，提升网站的安全性。	未开启
	配置区域封禁	阿里云全站加速推出区域封禁功能，帮助您一键阻断来自指定区域的访问请求，解决部分地区高发的恶意请求问题。	未开启
	配置精准访问控制	精确访问控制使用常见的HTTP字段（例如IP、URL、Header等）设置匹配条件来筛选访问请求，并对命中条件的请求执行设定的操作，来满足业务场景的定制化防护需求。	未开启
高级配置	配置IPv6	开启IPv6开关后，IPv6的客户端请求将支持以IPv6协议访问全站加速，全站加速也将携带IPv6的客户端IP信息访问您的源站。	未开启

功能	参考文档	说明	默认值
WebSocket	配置WebSocket	您可以通过开启WebSocket功能，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。	未开启

2.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

背景信息

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.
5.

3.验证域名归属权

您首次将一个域名添加到全站加速控制台时，需要完成域名归属权验证。验证通过后您再次添加该域名或子域名时，无需再次验证。

您可以通过以下方法完成验证：

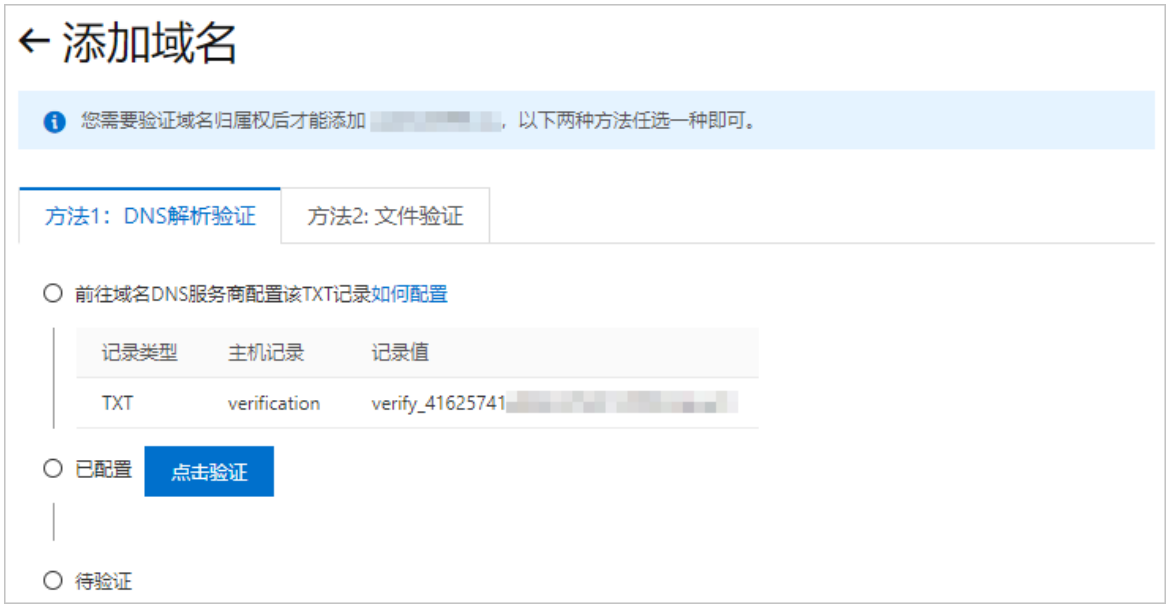
- 方法一：DNS解析验证（推荐）：该方式需要添加TXT的DNS记录。
- 方法二：文件验证。
- 通过API验证。

方法一：DNS解析验证（推荐）

本文以添加 `image.example.com` 为例，为您介绍如何通过DNS解析验证来验证域名归属权。

1. 在验证页面，单击**方法1：DNS解析验证**。

   > 注意 在验证完成前请不要关闭验证页面。

2. 在您的域名解析服务商，添加TXT记录。

   下文以阿里云的云解析为例介绍如何添加TXT记录，在其他域名解析服务商（例如：腾讯云、新网等）的配置方法类似。

   i. 登录云解析DNS控制台。

   ii. 在**域名解析**页面，找到 `example.com` 域名，在域名右侧单击**解析设置**。

   > 说明 域名解析记录的修改都是针对根域名，所以这里设置的对象是加速域名 `image.example.com` 的根域名 `example.com` 。

iii. 单击**添加记录**，填写步骤1中查看的记录类型、主机记录和记录值。

参数	说明
记录类型	选择**TXT**。
主机记录	填写步骤1中的主机记录。
解析线路	推荐您保持默认值。
记录值	填写步骤1中的记录值。
TTL	推荐您保持默认值。TTL为缓存时间，数值越小，修改记录后各地生效时间越快，默认为10分钟。

iv. 单击**确认**，完成添加。

3. 等待TXT解析生效（不同系统的TXT解析生效成功示例如下），返回全站加速控制台，单击**点击验证**，完成验证。

   如果系统提示“验证失败”，请检查TXT记录是否正确填写，并等待DNS记录生效后重新验证。

TXT解析生效成功示例：

> **说明**
>
> - 域名首次配置TXT解析记录后将会实时生效，修改TXT解析记录通常会在10分钟后生效（具体生效时间长短取决于域名DNS解析配置的TTL时长，默认为10分钟）。
> - 如果Linux系统没有安装dig命令程序，可以在Linux系统内运行 `yum install bind-utils` 来安装。

Windows系统示例 ❯

Linux系统示例 ❯

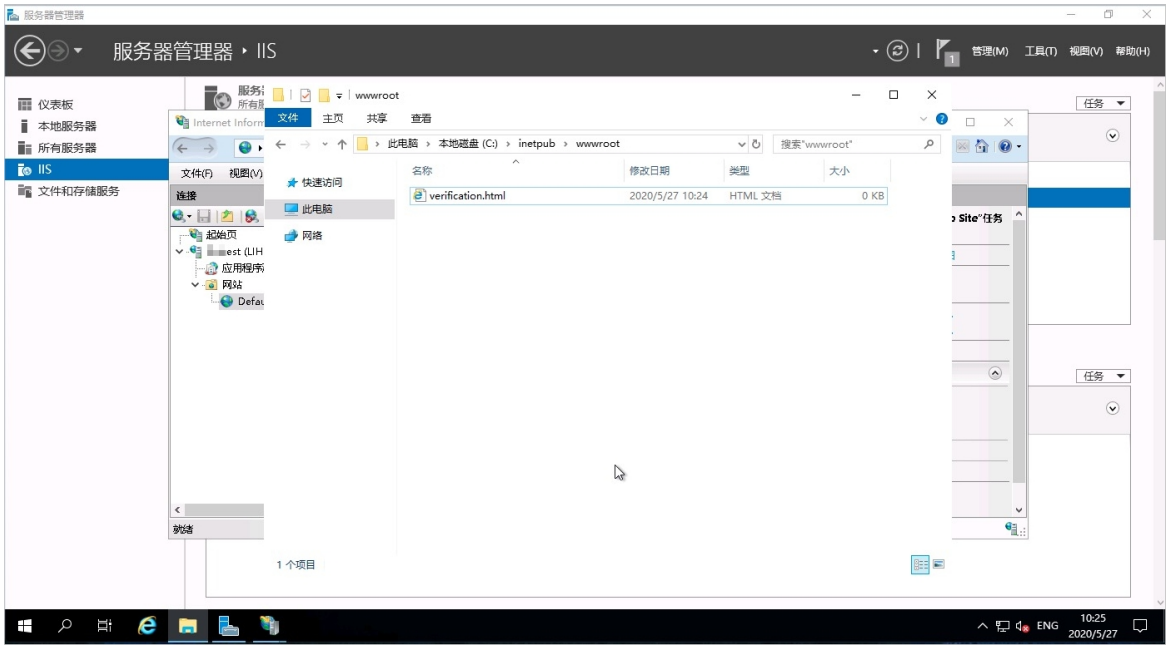
方法二：文件验证

1. 在验证页面，单击**方法2：文件验证**。

   在验证完成前请不要关闭验证页面。

2. 单击 `verification.html` ，下载验证文件。
3. 手动将验证文件上传到您域名源站服务器（例如您的ECS、OSS、CVM、COS、EC2等）的根目录。

   阿里云全站加速系统后台将访问您的源站 `http://example.com/verification.html` 获取验证文件，判断您是否按要求上传了指定的验证文件，请确保验证文件可被访问。



4. 单击**点击验证**，完成验证。

通过API验证

> **说明**
>
> - 建议您通过本文以上两种方法验证域名归属权，如果您不方便通过控制台界面来执行域名归属权验证的操作，您通过API接口来完成域名归属权验证。
> - API验证方式是一种验证操作方式，您可以在使用AddDcdnDomain（添加加速域名）或BatchAddDcdnDomain（批量添加加速域名）接口添加域名后使用VerifyDcdnDomainOwner（域名归属权校验）来验证域名归属权。

1. 调用AddCdnDomain或BatchAddCdnDomain接口添加加速域名。
2. 调用VerifyDcdnDomainOwner（域名归属权校验）来验证域名归属权。

   修改**VerifyType**入参确认验证方式。

   - **dnsCheck**：代表DNS解析验证，参考DNS解析验证中的步骤2添加TXT记录。
   - **fileCheck**：代表文件验证，自行创建 `verification.html` 文件并填入记录值（调用DescribeDcdnVerifyContent接口获取记录值（即字段Content值）），再参考文件验证中的步骤3上传文件。

常见问题

在添加新的加速域名时，您可能会遇到如下问题：

- Q：为什么要做域名归属权验证？
  A：为了确保域名只被真正的拥有者添加，避免出现用户A的域名被用户B添加导致域名冲突及安全隐患问题。
- Q：我有多个阿里云账号，每个账号首次添加新域名时都要做归属权验证吗？
  A：是的。多个账号视为多个不同的独立用户，每个账号都需要对新域名进行一次归属权验证。
- Q：我已完成DNS验证或文件验证，是否可以删除用作验证的DNS记录或文件？
  A：可以。要求您添加的DNS解析或文件，只用作添加域名时的归属权验证，验证通过后您可以删除记录或文件。

- Q：已经添加到阿里云全站加速控制台的存量域名，需要完成域名归属权验证吗？
  A：不需要。例如您已经在全站加速控制台添加了*.example.com，且配置了全站加速分配的CNAME在正常使用中，则视为您拥有example.com的解析权，您后续再添加**.example.com、***.example.com等任意example.com的子域名，都无需再验证。
- Q：通过API接口AddDcdnDomain添加域名需要完成域名归属权验证吗？
  A：需要。和控制台添加一样，您可以选择DNS解析验证或文件验证，先配置好DNS或在源站根目录放置好验证文件，再调用AddDcdnDomain接口添加加速域名。
- Q：我无法完成DNS验证或文件验证怎么办？
  A：您可以提交工单，说明无法完成域名归属权验证的原因，并提交可以证明您持有该域名的资料，阿里云将进行人工审核。

4.标签

4.1. 什么是标签

阿里云全站加速不对标签进行任何定义，仅严格按字符串对标签和域名进行匹配、筛选。标签可以标记域名，允许企业或个人将相同属性的域名分类，方便您识别、筛选和管理域名。

使用限制

标签的使用限制如下：

- 每个标签都由一个键值对 `Key:Value` 组成。
- 每个域名最多绑定20个标签。
- 同一个域名的标签键Key不能重复。如果对一个域名设置2个同Key不同Value的标签，新值将覆盖旧值。例如对域名 `example.aliyundoc.com` 先后设置了标签 `Key1:Value1` 和 `Key1:Value2` ，则最终 `example.aliyundoc.com` 只会绑定标签 `Key1:Value2` 。
- 键key不支持 `aliyun` 、 `acs:` 开头，不允许包含 `http://` 和 `https://` ，不允许为空字符串。
- 值value不允许包含 `http://` 和 `https://` ，允许为空字符串。
- 最大键key长度：64个Unicode字符。
- 最大值value长度：128个Unicode字符。
- 区分大小写。

> **说明** 如果您需要查询当前用户下的所有标签，只能通过API接口实现，请参见查询用户标签。

案例介绍

公司情况

某公司在阿里云全站加速上有100个域名，分属于电商、游戏、文娱三个部门，服务于营销活动、游戏A、游戏B、后期制作等业务，公司有三位运维负责人，分别是张三、李四、王五。

设置标签

为了方便管理，该公司使用标签对域名进行了分类，定义了以下标签键（Key）和标签值（Value）。

标签键（Key）	标签值（Value）
部门	电商、游戏、文娱。
业务	营销活动、游戏A、游戏B、后期制作。
负责人	张三、李四、王五。

根据上述标签键（Key）和标签值（Value）的对应关系，将标签的键和值绑定到各个域名上，域名与标签键值的对应关系见下表。

> **说明** 本文仅选取10个域名举例说明。

域名	Key为部门，Value为	Key为业务，Value为	Key为负责人，Value为
domain1	电商	营销活动	王五

域名	Key为部门，Value为	Key为业务，Value为	Key为负责人，Value为
domain2	电商	营销活动	王五
domain3	游戏	游戏A	张三
domain3	游戏	游戏B	张三
domain4	游戏	游戏B	张三
domain5	游戏	游戏B	李四
domain6	游戏	游戏B	李四
domain7	游戏	游戏B	李四
domain8	文娱	后期制作	王五
domain9	文娱	后期制作	王五
domain10	文娱	后期制作	王五

使用标签

- 如果您想筛选出王五负责的域名，则选择标签**负责人：王五**。
- 如果您想筛选出游戏部门中李四负责的域名，则选择标签**部门：游戏**和**负责人：李四**。

相关文档

您可以使用标签，对域名进行添加标签、使用标签管理域名、使用标签筛选数据和删除标签操作。更多信息，请参见标签管理。

4.2. 标签管理

标签是您为域名添加的标记，您可以根据添加的标签搜索和筛选域名。如果您的域名不再适用于当前的标签，您可以随时删除对应的标签。

使用限制

每个标签都由一对键值对（Key-Value）组成。标签的使用限制如下：

- 每个域名最多可以绑定20个标签。
- 同一个域名的标签键（Key）必须唯一。
  对同一个域名如果设置了两个同Key不同Value的标签，新值将覆盖旧值。例如，对域名 `test.example.com` 先后设置了标签 `Key1:Value1` 和 `Key1:Value2` ，则最终 `test.example.com` 只会绑定标签 `Key1:Value2` 。

添加标签

您可以为域名添加标签，实现统一管理。

1. 登录全站加速控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 添加标签。
   - 为单个域名添加标签

a. 在**域名管理**页面，找到您需要添加标签的域名，将光标移动到域名对应的标签图标上。

b. 在悬浮窗内，单击**编辑**。

c. 在**编辑标签**对话框中，根据以下信息配置标签，然后单击**确定**。
支持选择**选择已有标签**或**新建标签**。

配置	说明
键	标签键最多支持64个Unicode字符，不能以 `aliyun` 或 `acs:` 开头，不能包含 `http://` 和 `https://` ，且不能为空字符串。
值	标签值最多支持128个Unicode字符，不能以 `aliyun` 或 `acs:` 开头，不能包含 `http://` 和 `https://` ，可以为空字符串。

- 为多个域名批量添加标签

a. 在**域名管理**页面，选中您需要批量添加标签的域名，选择**标签管理 > 增加标签**。

b. 在**批量新增标签**对话框中，根据以下信息配置标签，然后单击**确定**。
支持选择**选择已有标签**或**新建标签**。

配置	说明
键	标签键最多支持64个Unicode字符，不能以 `aliyun` 或 `acs:` 开头，不能包含 `http://` 和 `https://` ，且不能为空字符串。
值	标签值最多支持128个Unicode字符，不能以 `aliyun` 或 `acs:` 开头，不能包含 `http://` 和 `https://` ，可以为空字符串。

使用标签管理域名

为域名添加标签后，您可以使用标签快速搜索域名。

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**选择标签**页签。
4. 选中一个或多个标签，即可筛选出标签对应的域名。

使用标签筛选数据

为域名添加标签后，您可以使用标签快速筛选域名，查询对应域名的流量使用情况等数据。

1. 登录全站加速控制台。
2. 筛选及查询数据。
   i. 在左侧导航栏，单击**业务监控 > 资源监控**。
   ii. 在**资源监控**页面单击**选择标签**。

   > **说明** 如果您同时选择了多个标签，查询结果将显示各个标签对应域名的交集。

   iii. 选中需要筛选的标签，单击**查询**，即可查询标签对应的数据。

删除标签

如果域名不再适用于当前已绑定的标签，您可以从域名中解绑标签。

1. 登录全站加速控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 选中您需要删除标签的域名，选择**标签管理 > 删除标签**。
4. 在**批量删除标签**对话框中，选择您需要删除的标签，单击**确定**。

> **说明** 一次最多可以删除20个标签。

5. 在**域名管理**页面，单击刷新图标，查看标签是否删除成功。

相关API

标签管理相关的API如下表所示。

功能	描述	API
添加标签	创建用于标记域名用途或对域名进行分组管理的标签。	TagDcdnResources
使用标签管理域名	域名绑定标签后，您可以使用标签快速筛选对应的域名，对域名进行分组管理。	DescribeDcdnTagResources
删除标签	删除已经不再适用于您当前某个或多个域名的标签。	UntagDcdnResources

5.基本配置

5.1. 概述

阿里云全站加速为您提供加速域名的基本配置功能。您可以在控制台查看加速域名的基础信息和源站信息，切换加速域名的加速区域及修改源站信息。
您可以在全站加速控制台进行以下基本配置。

功能	说明
切换加速区域	切换加速区域，变更全站加速的服务范围。
配置源站	修改源站类型、地址、优先级、权重、端口等源站信息。

5.2. 切换加速区域

您需要变更加速域名的全站加速服务范围时，您可以通过切换加速区域功能实现。

操作步骤

1. 登录全站加速控制台。
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**基本配置**页签，找到**基础信息**。
5. 在**基础信息**区域，单击**加速区域**右侧的**修改配置**。
6. 在**加速区域**对话框，选择您需要切换的加速区域。

参数	说明
仅中国内地	如果选择**仅中国内地**，代表全球用户访问均会调度至中国内地加速节点进行服务（海外用户的访问流量将会被调度至华东电信的全站加速节点）。同时需要工信部备案。域名备案方法，请参见使用限制。
全球	如果选择**全球**，全球用户访问将会择优调度至最近的加速节点进行服务。同时需要工信部备案。域名备案方法，请参见使用限制。

参数	说明
全球（不包含中国内地）	如果选择**全球（不包含中国内地）**，全球用户访问均会调度至中国香港、中国澳门、中国台湾以及其他国家和地区的加速节点进行服务（中国内地用户将会被调度至日本、新加坡和中国香港的CDN节点）。该选项无需工信部备案。

7. 单击**确定**。

5.3. 配置源站

阿里云全站加速支持的源站类型包括OSS域名、IP源和站域名，每种源站类型都支持配置多个源站地址，多源站场景下，支持设置源站的主备优先级和权重，实现负载均衡。本文介绍如何新增或修改源站信息及源站的健康检查策略。

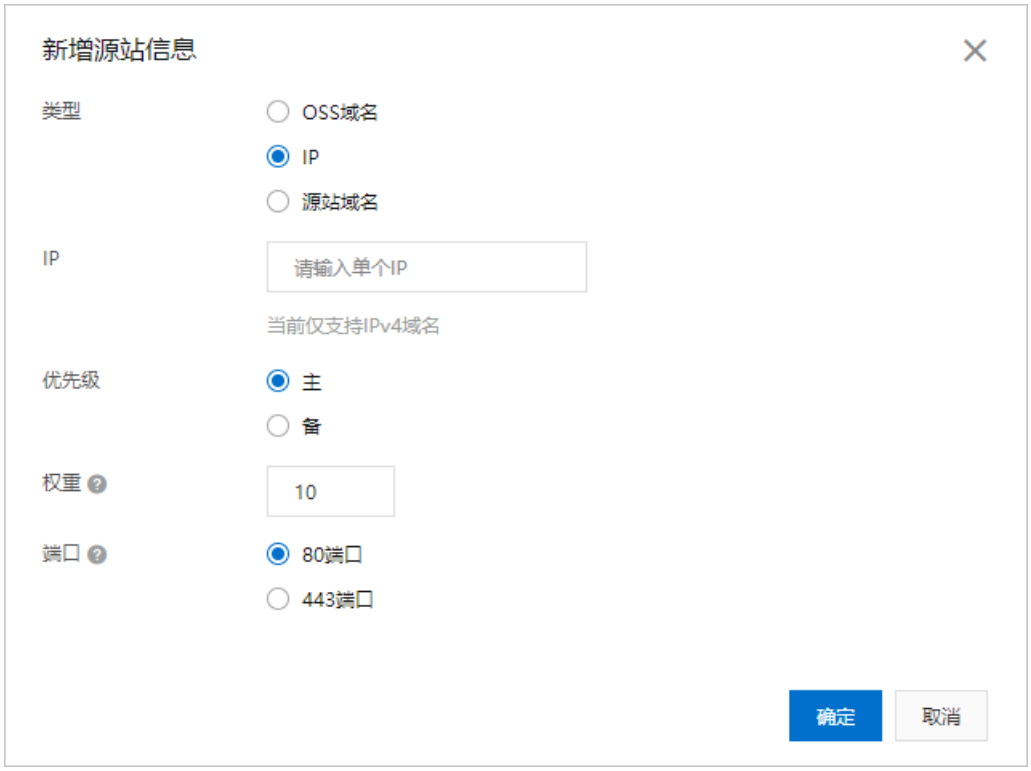
注意事项

- 全站加速回源从源站获取资源时，源站产生的流量宽带费用由源站来缴纳，比如源站是客户的IDC中心，产生的就是IDC中心的流量带宽费用；如果源站是OSS，产生的就是OSS的流量费。
- 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。

> **说明** 源站健康检查：实行主动四层健康检查机制，探测源站的80、443或自定义端口。每2.5秒检查一次，连续3次失败标记为不可用。

新增或修改源站信息

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**基本配置**页签，找到**源站信息**。
5. 在**源站信息**区域，单击**编辑**。
6. 在**新增源站信息**对话框，完成以下配置。



参数	说明
类型	选择源站的类型，并填写源站地址。 ○ **OSS域名** ■ 资源已存储在阿里云OSS中，可直接输入阿里云OSS Bucket的外网域名作为源站（不支持OSS内网域名作为源站），例如：`***.oss-cn-hangzhou.aliyundoc.com`。 ■ 查看OSS外网域名：前往OSS控制台查看，或直接选择同账号下的OSS Bucket。 ○ **IP** 支持配置多个服务器外网IP作为源站地址，不支持内网IP，阿里云ECS的外网IP可免审核。 ○ **源站域名** 支持配置域名作为源站地址，可配置多个域名。 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。 ■ 域名仅支持全英文小写。 ■ 如果域名包含中文（例如：阿里云.网址），请以中文形式进行相关备案，再通过第三方工具punnycode将中文域名转换成为英文域名（例如：xn--fiq****.xn--eq****）后填入。

参数	说明
优先级	源站优先级支持设置主备，主优先级大于备优先级。用户请求通过阿里云全站加速回源时，会优先回源到优先级为主的源站地址。 例如，有A、B两个源站，A源站的优先级为主，B源站的优先级为备，则用户请求通过阿里云全站加速回源时会优先回源到A源站，如果A源站出现故障，将会回源到B源站，当A源站恢复正常后会从B源站切换回A源站。
权重	当多个源站的优先级相同时，阿里云全站加速会按照源站的权重分配用户请求回源到不同源站的比例，实现按权重的负载均衡。您可以根据业务需求，自行设置权限值。 ○ 取值范围：1~100，数值越大，源站分配到的用户请求比例越高。 ○ 默认值：10。 例如，有A、B两个源站，两个源站的优先级都是主，A源站的权重为80，B源站的权重为20，则用户请求将会按照8:2的比例在A、B两个源站之间分配。
端口	根据您源站的支持情况，选择回源端口。 ○ **80端口**：全站加速回源请求源站的80端口。 ○ **443端口**：全站加速回源请求源站的443端口，源站需要支持HTTPS访问。 **说明** 如果您需要自定义回源端口，请在成功添加域名后将“静态协议跟随回源”和“动态内容协议跟随回源”的跟随方式指定为HTTP，然后再设置自定义回源端口。具体操作，请参见配置静态协议跟随回源和动态内容回源配置。

7. 单击**确定**。

6.回源配置

6.1. 回源概述

回源指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，或者您部署预热任务给全站加速节点时，全站加速节点会回源站获取资源。您还可以根据业务的实际需要来配置回源相关功能。
阿里云提供丰富的回源配置功能：

功能	说明	文档链接
自定义全站加速节点回源时需要访问的具体服务器域名。	当您的源站的同一个IP地址上绑定了多个域名或站点，您可以通过配置HTTP请求头中的HOST信息，来指定全站加速节点回源时需要访问的站点。全站加速在回源过程中会根据HOST信息去对应站点获取资源。	配置回源HOST
设置回源协议类型（跟随、HTTP或HTTPS）。	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。	配置静态协议跟随回源
OSS私有Bucket回源。	当您的源站为OSS且Bucket设置为私有时，必须先打开阿里云OSS私有Bucket回源开关对全站加速授权，才能实现全站加速回源至私有OSS Bucket访问资源，从而有效防止资源盗链。	OSS私有Bucket回源
指定全站加速回源时具体访问的站点。	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，指明具体访问域名。	配置回源SNI
对客户端请求进行验证，拒绝白名单以外的请求访问源站。	全站加速节点通过HTTPS协议与源站建立连接时，系统会对客户端请求中携带的SNI（Server Name Indication）和源站返回证书的Common Name进行校验，从而确定该请求是接受还是拒绝。	配置Common Name白名单
源站服务器只返回指定范围内的部分内容。	较大文件的分发加速时开启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。	配置Range回源
设置全站加速回源请求的最长等待时间。	全站加速节点的回源请求超时等待时间默认为30秒，您可以根据实际需求设置全站加速回源请求的最长等待时间。当回源请求等待时间超过配置的超时时间时，全站加速节点与源站的连接断开。	回源请求超时时间
添加、修改或删除回源HTTP请求头。	HTTP请求回源时，您可以添加或删除回源HTTP头。	配置自定义回源HTTP头

6.2. 配置回源HOST

当您的源站有多个站点，且需要回源的站点不是加速域名对应的站点时，您需要配置回源HOST，阿里云全站加速在回源过程中会根据HOST信息去对应站点获取资源。

背景信息

源站和回源HOST的区别：

- 源站：指您的业务服务器，决定了回源时请求到的具体IP地址。

- 回源HOST：指全站加速回源请求头中携带的HOST字段值，决定了回源请求访问到该IP地址上的具体站点。

> **注意**
>
> - 对于普通域名（精准域名），回源HOST默认为加速域名。
> - 对于泛域名，回源HOST默认为实际访问的子域名。例如，泛域名是 *.aliyundoc.com，如果通过example.aliyundoc.com访问时，回源HOST即为example.aliyundoc.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**回源配置**页签下找到**回源HOST**。
6. 打开**回源HOST**开关，选择**域名类型**。

参数	说明
加速域名	以终端用户访问的域名回源。
源站域名	以源站服务器的域名地址回源。 **说明** ○ 源站信息为IP地址类型时，**源站域名**选项置灰，不可选择。 ○ 源站信息为OSS域名时，将会同步开启**回源HOST**功能，并且设置域名类型为**源站域名**。

参数	说明
自定义域名	以用户指定的域名回源。 **说明** ○ 自定义域名确保为您已经绑定的域名，否则回源失败。 ○ 您的源站绑定了多个域名，您希望用户从指定域名获取资源，否则回源失败。

7. 单击**确定**。

配置示例

示例一：当源站类型为域名。

域名	说明
加速域名：`image.example.com` 源站地址：`example.com`	• 域名类型选择**加速域名**，当全站加速回源时，会到 `example.com` 源站上的 `image.example.com` 的站点获取资源。 • 域名类型选择**源站域名**，当全站加速回源时，会到源站 `example.com` 获取资源。 • 域名类型选择**自定义域名**，则回源HOST为用户输入的自定义域名。

示例二：当源站类型为IP地址。

域名	说明
加速域名：`example.com` 源站地址：`10.10.10.10`	• 域名类型选择**加速域名**，当全站加速回源时，会到 `10.10.10.10` 这台主机上的 `example.com` 的站点获取资源。 • 域名类型选择**自定义域名**，当全站加速回源时，会到您输入的域名获取资源。

示例三：当源站类型为OSS域名。

域名	说明
加速域名：`example.com` 源站地址：`example.oss-cn-hangzhou.aliyuncs.com`	• 域名类型选择**加速域名**，当全站加速回源时，会到 `example.oss-cn-hangzhou.aliyuncs.com` OSS域名上的 `example.com` 站点获取资源。 • 域名类型选择**源站域名**，当全站加速回源时，会到OSS域名 `example.oss-cn-hangzhou.aliyuncs.com` 获取资源。 • 域名类型选择**自定义域名**，当全站加速回源时，会到您输入的域名获取资源。

相关文档

- 批量配置加速域名

6.3. 配置静态协议跟随回源

静态协议跟随回源指全站加速节点回源站请求资源时使用的协议。配置该功能后，全站加速节点将根据指定的协议回源到源站的80（HTTP）或443（HTTPS）端口请求资源。

背景信息

静态协议跟随回源功能默认关闭，该状态下默认的静态协议跟随回源以**基本信息 > 源站信息**中设置的回源端口为准：

- 回源端口设置为443：以HTTPS协议回源。
- 回源端口设置为80或其他：以HTTP协议回源。

> **说明** 静态协议跟随回源功能只支持回源到源站的80或443端口。开启静态协议跟随回源后，**源站信息**中的自定义端口会失效。如果您希望全站加速节点回源到自定义端口，请提交工单申请配置。

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**回源配置**。
5. 在**回源配置**页签下，找到**静态协议跟随回源**。
6. 打开**静态协议跟随回源**开关。
7. 在**静态协议跟随回源**对话框，选择静态协议跟随回源类型为**跟随客户端协议**、**HTTP**或**HTTPS**。

参数	说明
跟随客户端协议	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（源站需要同时支持80端口和443端口，否则可能会造成回源失败）。 **说明** 静态协议跟随回源主要是为了保证信息在传输过程中不被改写或记录。如果您仅需要对敏感的那部分数据（例如：用户身份验证数据）采用更安全的HTTPS协议传输，其他非敏感数据（例如：图片）采用HTTP协议传输。建议您跳转类型配置为**跟随**。

参数	说明
HTTP	全站加速以HTTP协议回源。
HTTPS	全站加速以HTTPS协议回源。 说明 ○ HTTPS协议的加密处理需要额外消耗源站服务器的处理器资源。 ○ 选择HTTPS协议回源时，默认使用443端口，如需配置自定义端口，请提交工单申请配置。

8. 单击**确定**，完成配置。

相关文档

- 批量配置加速域名

6.4. OSS私有Bucket回源

如果加速域名的源站使用的是阿里云的云存储OSS，并且OSS的Bucket被配置为私有模式（可以起到访问鉴权的作用，避免非授权的请求盗刷流量），该情况下您需要给加速域名开启OSS私有Bucket回源功能。本文为您介绍如何开启和关闭私有Bucket回源。

背景信息

您可以配合使用阿里云全站加速提供的Referer防盗链功能、URL鉴权功能，来更有效地保护您的资源不被盗刷，更多信息，请参见配置Referer防盗链和配置URL鉴权。

注意

- 开启OSS私有Bucket回源授权后，即授权全站加速对您所有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内的所有资源。开启该功能前，请根据您的实际业务情况谨慎决策。如果您授权的私有Bucket内容并不适合作为全站加速的回源内容，请勿授权或开启此功能。
- 如果您的网站有被攻击的风险，请购买高防服务，同时谨慎授权或开启私有Bucket回源授权功能。
- 全站加速回源OSS私有Bucket功能与OSS的静态网站托管功能的默认首页配置存在冲突，两个功能需要同时使用的情况下，请参见说明文档。

开启私有Bucket回源

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. （可选）您首次授权时，需要执行该步骤，在**阿里云OSS私有Bucket回源**区域，单击**点击授权**，继续单击**同意授权**。

6. 在**阿里云OSS私有Bucket回源**区域，打开**阿里云OSS私有Bucket回源**开关。

> **说明** 当全站加速回源OSS私有Bucket访问非加密文件时，完成以上配置即可正常访问文件。如果您在OSS上对文件进行了KMS加密，此时将无法直接访问，需要为AliyunCDNAccessingPrivateOSSRole角色添加AliyunKMSCryptoUserAccess权限才能正常访问文件。

7. （可选）为AliyunCDNAccessingPrivateOSSRole角色添加AliyunKMSCryptoUserAccess权限。
   i. 登录RAM控制台。
   ii. 在左侧导航栏，选择**身份管理 > 角色**。
   iii. 在**角色名称**列表下，找到AliyunCDNAccessingPrivateOSSRole角色。
   iv. 单击**添加权限**，**被授权主体**会自动填入。
   v. 在**系统策略**下搜索AliyunKMSCryptoUserAccess，并单击AliyunKMSCryptoUserAccess，会添加到**已选择**列表。
   vi. 单击**确定**，显示授权成功。
   vii. 单击**完成**。

关闭私有Bucket回源

如果您不希望加速域名能够访问您私有Bucket内资源的权限，您可以通过访问控制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。

1. 登录RAM控制台。
2. 在左侧导航栏，单击**身份管理 > 角色**。
3. 在**角色名称**列表下，单击AliyunCDNAccessingPrivateOSSRole角色。

4. 移除角色AliyunCDNAccessingPrivateOSSRole中的所有权限。
   i. 单击权限对应的**移除权限**。
   ii. 在移除权限的确认对话框中，单击**确定**。
5. 返回**身份管理 > 角色**页面，删除AliyunCDNAccessingPrivateOSSRole角色。
   i. 单击AliyunCDNAccessingPrivateOSSRole角色对应的**删除**。
   ii. 在**删除RAM角色**的确认对话框中，单击**确定**。

6.5. 配置回源SNI

如果您的源站IP绑定了多个域名，且全站加速回源协议为HTTPS时，需配置回源SNI，在回源SNI内指明所请求的具体域名，并使服务器根据该域名正确地返回对应的SSL证书。

背景信息

SNI（Server Name Indication）是对SSL/TLS协议的扩展，允许服务器在单个IP地址上承载多个SSL证书，可解决一个HTTPS服务器拥有多个域名但是无法预知客户端到底请求的是哪一个域名的服务问题。开启SNI后，在全站加速节点向源站发起TLS握手请求时，源站服务器会根据TLS握手请求中携带的SNI信息来确认被请求的业务域名，然后返回正确的SSL证书给客户端。

> **注意**
> - 源站的服务端需要支持全站加速节点发起的TLS握手请求包含的SNI信息的解析能力。
> - 如果加速域名配置了多个源站，通过控制台配置SNI功能，所有源站地址会共用一个回源SNI值，那么回源请求都会指向SNI值对应的域名。如果您希望不同的源站，配置不同的SNI值，您可以提交工单申请。

回源SNI的工作原理如下图所示。

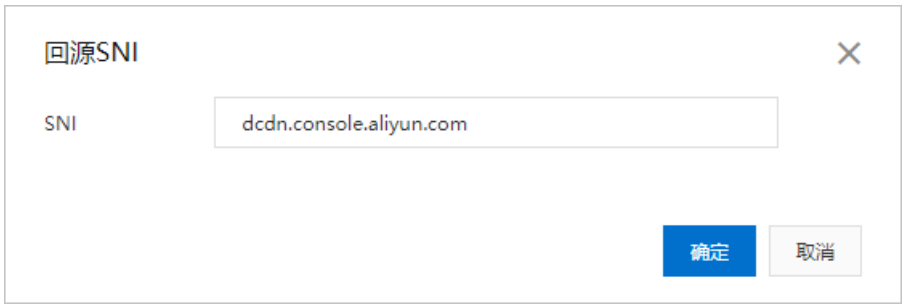
回源SNI的工作流程如下：

1. 当全站加速节点以HTTPS协议访问源站时，需要在SNI中指定访问的具体域名。
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**回源配置**页签下找到**回源SNI**。
6. 打开**回源SNI**开关，输入您希望客户端从哪个域名获取资源的域名名称（例如：dcdn.console.aliyun.com）。

   > **说明** 回源SNI配置的值只能是精确域名，不能是泛域名。

7. 单击**确定**。

相关文档

- 批量配置加速域名

6.6. 配置Common Name白名单

全站加速节点通过HTTPS协议与源站建立连接时，系统会对客户端请求中携带的SNI（Server Name Indication）和源站返回证书的Common Name进行校验。为了成功通过回源证书校验，使全站加速节点与源站成功建立连接，您可以开启并配置Common Name白名单功能。

背景信息

Common Name即公用名，是指申请SSL证书的具体网站域名。如下图所示，当客户端请求中携带的SNI（Server Name Indication）与源站返回证书的Common Name不一致时，该请求会被拒绝，全站加速节点无法通过HTTPS协议和源站建立连接。此时如果您开启了Common Name白名单功能，并且将domain2添加到了Common Name白名单中，则全站加速节点可以通过HTTPS协议和源站成功建立连接。

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**回源配置**页签下，找到**Common Name白名单 --Beta版**，打开**状态**开关。
6. 填写需要加入Common Name白名单的域名。

> **说明** 支持填写多个域名，多个域名用英文逗号（,）分隔。例如 `example.com,example.org,example.net` 。

7. 单击**确定**，完成配置。

6.7. 配置Range回源

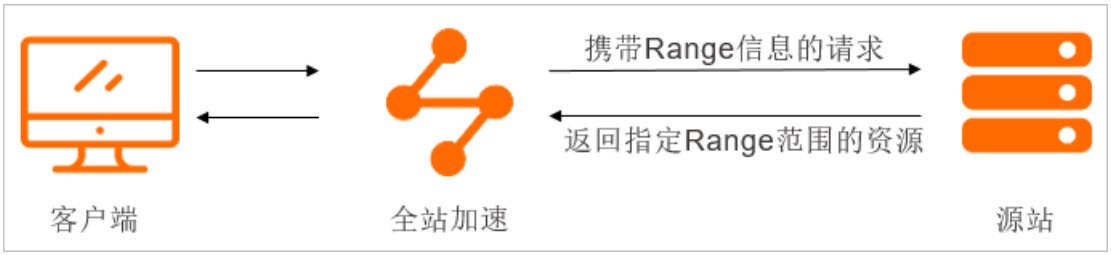
Range回源，指全站加速节点在回源的HTTP请求里面携带了Range信息，源站在收到全站加速节点的回源请求时，根据HTTP请求头中的Range信息返回指定范围的内容数据给全站加速节点。Range回源可有效提高文件分发效率，可以提高缓存命中率，减少回源流量消耗和源站压力，并且提升资源响应速度。

背景信息

Range是HTTP请求头之一，可用来指定需获取的内容的范围。例如， `Range: bytes=0-100` 表示回源请求该文件的前101个字节的数据内容。

开启Range回源功能后，全站加速收到用户的请求时，如果全站加速节点上未缓存该资源或资源已过期，全站加速节点回源会采用Range请求，从源站分段获取用户需要的部分资源并缓存到全站加速节点上。

开启Range回源的工作原理如下图所示：



注意事项

开启Range回源前需确认源站是否支持Range请求，即HTTP请求头中包含Range字段，并且源站能够响应正确的206文件分片。如果源站不支持Range请求，开启Range回源将导致资源无法缓存。

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**回源配置**页签下找到**Range回源**。
6. 打开或关闭**Range回源**开关。

Range回源	具体描述	示例
开启	当您需要访问资源文件指定范围内的部分内容时，为了提高资源响应效率，则需要开启**Range回源**。开启**Range回源**请求回源站后，源站需要依据**Range**，响应文件的字节范围，同时全站加速节点也会向客户端响应相应字节范围的内容。	如果客户端向源站服务器的请求中含有 `range:0~100` ，则源站收到的请求中也会含有 `range:0~100` 。源站响应全站加速节点，全站加速节点响应客户端字节范围为0~100，共101个字节。
关闭	当您需要访问资源文件的全部内容时，则需要关闭**Range回源**。关闭**Range回源**后，全站加速上层节点会向源站请求全部的文件，由于客户端收到Range定义的字节后自动断开HTTP连接，请求的文件没有缓存到全站加速节点上，最终导致缓存命中率较低，并且回源流量较大。	如果客户端向源站服务器的请求中含有 `range:0~100` ，则源站端收到的请求中没有Range这个参数。源站响应全站加速节点完整文件，全站加速节点响应给客户端的就是101个字节，由于链接断开，会导致该文件没有缓存到全站加速节点上。

6.8. 回源请求超时时间

阿里云全站加速回源站请求资源时，默认请求超时时间为30秒，若超时，会出现回源失败的情况。您可以根据源站数据处理速度及网络情况，合理配置回源请求超时时间，保障正常回源。通过本文，您可以了解配置回源请求超时时间的操作步骤。

注意事项

由于阿里云全站加速的L1（边缘节点）和L2（汇聚节点）节点之间默认的超时时间是36秒，所以“L1-L2-源站”的全链路回源请求超时时间默认为36秒，如果需要配置的全链路回源（L1-L2-源站）超时时间大于36秒，需提交工单申请。

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**回源配置**页签下找到**回源HTTP请求超时时间**，单击**修改配置**。
6. 在**回源HTTP请求超时时间**对话框，设置**超时时间**。

7. 单击**确定**。

相关文档

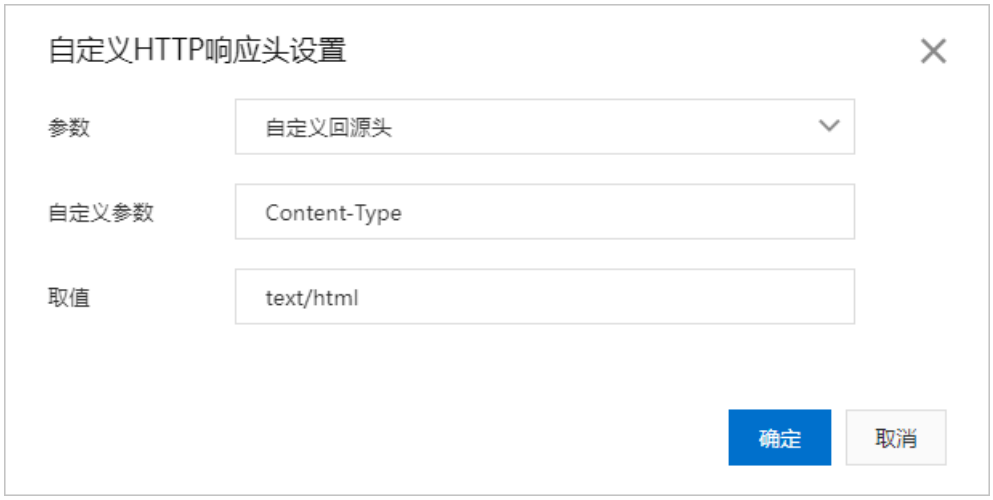
- 批量配置加速域名

6.9. 配置自定义回源HTTP头

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

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**页签。
6. 单击**添加**。
7. 在**自定义HTTP响应头设置**页面，选择**参数**，并设置**取值**。



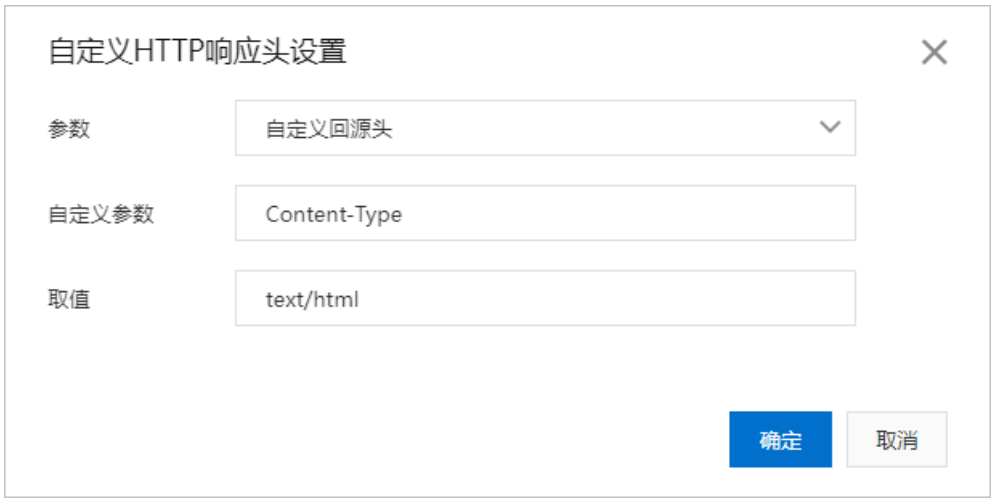
配置项	示例	说明
参数	自定义回源头	选择**自定义回源头**或选择已经预设好的响应头参数。
自定义参数	Conetent-Type	自定义响应头名称为Conetent-Type。
取值	text/html	一个响应头参数中可以配置多个值，多个值用英文逗号（,）分隔。

8. 单击**确定**。

配置示例

配置场景：如果您希望配置响应文档属于什么MIME类型。

配置方法：配置如下。



结果说明：在源站发送给全站加速节点的响应信息中声明内容类型为text/html，再次配置将覆盖旧值。

6.10. 改写回源URI

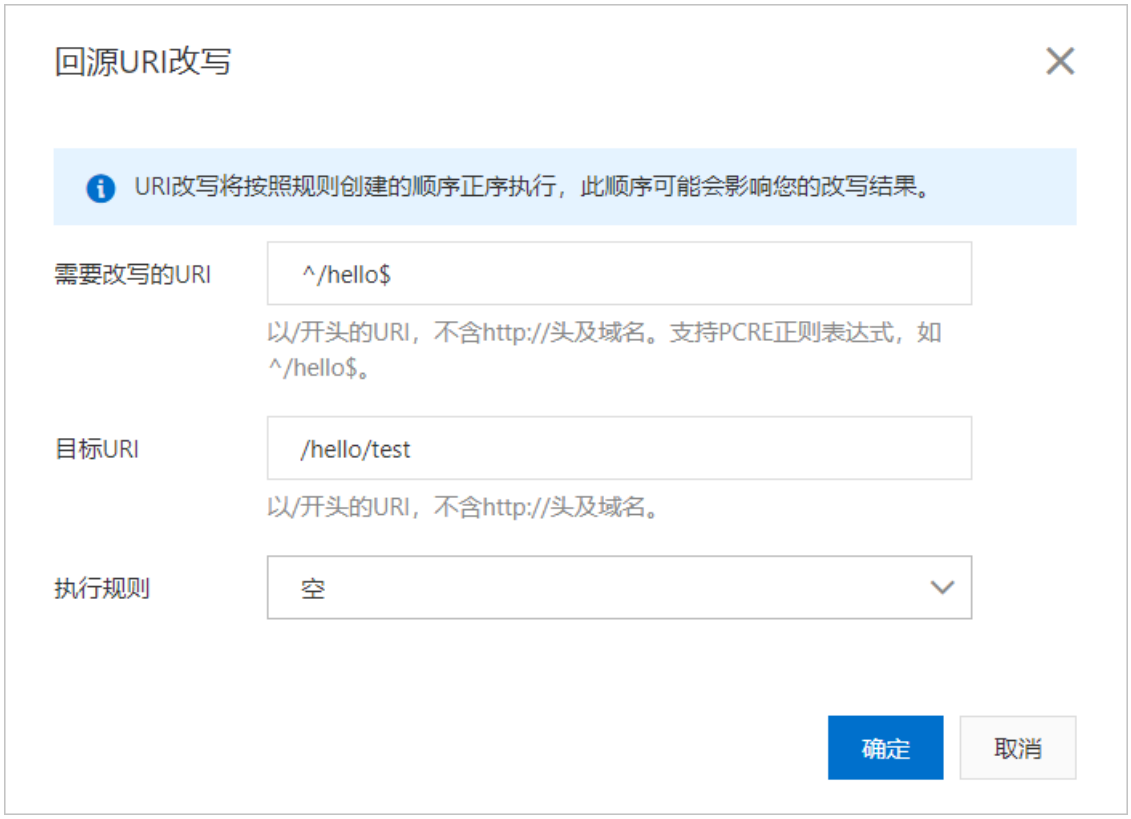
当您需要改写回源请求中的URI时，可以配置回源URI改写功能。通过本文您可以了解配置重写规则的操作方法。

背景信息

当您的回源请求URI与源站的URI不匹配时，需要将您的回源请求URI修改为与源站匹配的URI，您可以根据实际需要配置多条改写匹配规则。

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. 在指定域名的左侧导航栏，单击**回源配置**。
5. 单击**回源URI改写**页签。
6. 在**回源URI改写**页签，单击**添加**。
7. 根据您的需求，配置需要改写的URI、目标URI和执行规则。



参数	示例	说明
需要改写的URI	^/hello$	以正斜线（/）开头的URI，不含http://头及域名。支持PCRE正则表达式。
目标URI	/hello/test	以正斜线（/）开头的URI，不含http://头及域名。
执行规则	空	如果配置了多条规则，在匹配执行当前规则后，继续匹配后续规则。
	break	如果配置了多条规则，在匹配执行当前规则后，后续规则将不再匹配，并且只修改URI部分，不修改URL的参数。
	enhance_break	如果配置了多条规则，在匹配执行当前规则后，后续规则将不再匹配，但是匹配和修改整个URL（包括URI+参数）。

注意

- **回源URI改写**功能中的执行规则“break”虽然不修改URL的参数部分，但是并不影响**回源参数改写**功能对URL中参数的改写。
- **回源URI改写**功能在配置执行规则“enhance_break”的情况下，对URL中参数的改写可能会与**回源参数改写**功能对URL中参数的改写相冲突，这两个功能同时配置的时候，需要注意避免配置冲突。
- **回源URI改写**功能在配置执行规则“enhance_break”的情况下，对URL中参数的改写可能会与**域名管理 > 性能优化**页签下的**保留参数**或**忽略参数**功能相冲突，这三个功能同时配置的时候，需要注意避免配置冲突。

8. 单击**确定**，使改写规则开始执行和生效。

您也可以在**回源URI改写**页面的规则列表中，单击**修改**或**删除**，对当前配置的规则进行相应操作。

> 注意
>
> - 单个域名可以配置的**回源URI改写**规则数量上限是50个。
> - 规则改写按照规则列表从上到下顺序执行的，此顺序可能会影响您的改写结果。
> - **回源URI改写**功能与**重写**功能的区别在于，**重写**功能的作用位置是在CDN边缘节点上面，会影响CDN内部链路，也会改写缓存key，而**回源URI改写**功能的作用位置是在CDN回源节点上面，不影响CDN内部链路，不改写缓存key。

样例一

待改写URI	^/hello$
目标URI	/index.html
执行规则	空
结果说明	原始请求：`http://aliyundoc.com/hello` 改写后的回源请求：`http://aliyundoc.com/index.html` 该请求将会继续匹配**回源URI改写**规则列表中其余的规则。

样例二

待改写URI	^/hello.jpg$
目标URI	/image/hello.jpg
执行规则	break
结果说明	原始请求：`http://aliyundoc.com/hello.jpg` 改写后的回源请求：`http://aliyundoc.com/image/hello.jpg` 该请求将不再继续匹配**回源URI改写**规则列表中其余的规则。

样例三

待改写URI	^/hello.jpg?code=123$
目标URI	/image/hello.jpg?code=321
执行规则	enhance_break
结果说明	原始请求：`http://aliyundoc.com/hello.jpg?code=123` 改写后的回源请求：`http://aliyundoc.com/image/hello.jpg?code=321` 该请求将不再继续匹配**回源URI改写**规则列表中其余的规则。

7.动静态加速规则

7.1. 动静态加速规则概述

开启动态加速功能，可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；关闭则无动态资源加速效果，仅保留静态资源边缘缓存功能。
您可以通过监控查询功能，执行如下操作。

功能	说明
配置静态文件类型	通过配置静态文件类型，可自定义静态资源的加速规则，使静态文件不再占用动态加速资源，而采用更合适的静态加速。
配置静态文件URI	以文件URI的方式区分出静态文件，设定的静态文件不再占用动态加速资源，而采用更合适的静态加速。
配置静态文件路径	以文件路径的方式区分出静态文件，设定的静态文件不再占用动态加速资源，而采用更合适的静态加速
动态内容回源配置	动态资源回源时的配置，包含动态内容回源协议的配置和开启动态负载均衡，您可以根据实际需求选择性地进行配置。

7.2. 配置静态文件类型

如果您需要同时加速动静态资源，可以开启动态加速功能，通过配置静态文件类型，可自定义静态资源的加速规则，使静态文件不再使用动态加速，而采用更合适的静态加速。实现将静态资源缓存至边缘节点，动态资源采用最优路由回源。

背景信息

动态和静态资源加速规则说明如下：

- 开启
  当您需要加速静态和动态资源时，需要打开**动态加速**开关。您可以根据自身业务需求，配置静态文件类型加速规则。静态资源加速规则配置成功后，资源按照您配置的加速规则加速。您可以自定义静态资源的边缘缓存文件类型、边缘缓存的静态文件URI和静态加速的资源目录。
- 关闭
  当您不需要加速动态资源时，可以关闭**动态加速**开关。关闭动态加速开关后，动态资源无加速效果，走静态边缘缓存逻辑，默认的静态文件加速规则有效，自行添加静态文件加速规则失效。

操作步骤

1. 配置静态文件类型。
   i. 登录全站加速控制台。
   ii. 在左侧导航栏，单击**域名管理**。
   iii. 在**域名管理**页面，单击目标域名对应的**配置**。
   iv. 在指定域名的左侧导航栏，单击**动静态加速规则**。
   v. 打开**动态加速**开关。
   vi. 在**静态文件类型**页签下，单击**修改配置**。

vii. 在**静态文件类型**对话框，选择开启或关闭**自适应缓存**，并配置**静态文件类型**。

参数	描述
自适应缓存	您可以根据静态文件类型和源站的缓存规则进行自适应缓存。 ■ 开启**自适应缓存** 开启自适应缓存后，**静态文件类型**中的规则优先级高于自适应缓存，在控制台配置的**缓存过期时间**中的缓存规则会全部生效。规则生效的优先级如下： ■ 第一优先级：在控制台配置了**缓存过期时间**，则遵循**缓存过期时间**中的缓存规则。 ■ 第二优先级：未在控制台配置**缓存过期时间**，则遵循源站配置的缓存规则。 ■ 第三优先级：未在控制台和源站配置缓存规则，则直接动态回源。 ■ 关闭**自适应缓存** ■ 关闭自适应缓存，但在控制台配置了**静态文件类型**和**缓存过期时间**，则遵循控制台配置的**缓存过期时间**中的缓存规则。 **说明** 需确保**缓存过期时间**中配置的文件后缀在**静态文件类型**内，否则在**缓存过期时间**中配置的缓存规则将不生效。 ■ 关闭自适应缓存，但在控制台配置了**静态文件类型**，未配置**缓存过期时间**，则遵循源站配置的缓存规则。
静态文件类型	支持的静态文件类型如下： ■ 图片：GIF、PNG、BMP、JPEG、JPG。 ■ 页面：HTML、HTM、SHTML。 ■ 音视频：MP3、WMA、FLV、MP4、WMV、OGG、AVI。 ■ 文本：DOC、DOCX、XLS、XLSX、PPT、PPTX、TXT、PDF。 ■ 其他：ZIP、EXE、TAT、ICO、CSS、JS、SWF、APK、M3U8、TS。

viii. 单击**确定**，完成配置。

2. 配置缓存过期时间。
   i. 在**缓存过期时间**区域下，单击**添加**。
   ii. 在**缓存过期时间**对话框，配置缓存规则，您可以选择按**目录**或**文件后缀名**进行配置。

iii. 单击**确定**，完成配置。

7.3. 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，分配最佳节点进行缓存和分发。

背景信息

动态和静态资源加速规则说明如下：

- 开启
  当您需要加速静态和动态资源时，需要打开**动态加速**开关。您可以根据自身业务需求，配置静态文件类型加速规则。静态资源加速规则配置成功后，资源按照您配置的加速规则加速。您可以自定义静态资源的边缘缓存文件类型、边缘缓存的静态文件URI和静态加速的资源目录。
- 关闭
  当您不需要加速动态资源时，可以关闭**动态加速**开关。关闭动态加速开关后，动态资源无加速效果，走静态边缘缓存逻辑，默认的静态文件加速规则有效，自行添加静态文件加速规则失效。

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**动静态加速规则**。
5. 打开**动态加速**开关。
6. 在**静态URI**页签下，单击**修改配置**。

7. 在**静态URI**对话框，配置**静态URI**。

8.

7.4. 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，分配最佳节点进行缓存和分发。

背景信息

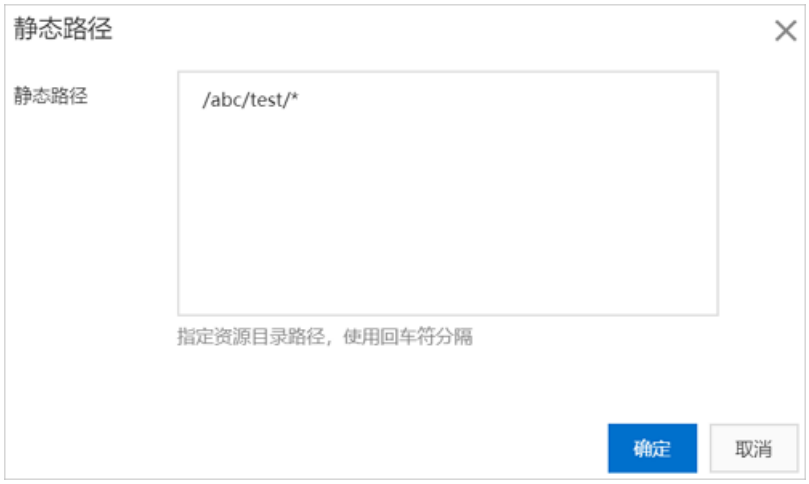
动态和静态资源加速规则说明如下：

- 开启
  当您需要加速静态和动态资源时，需要打开**动态加速**开关。您可以根据自身业务需求，配置静态文件类型加速规则。静态资源加速规则配置成功后，资源按照您配置的加速规则加速。您可以自定义静态资源的边缘缓存文件类型、边缘缓存的静态文件URI和静态加速的资源目录。
- 关闭
  当您不需要加速动态资源时，可以关闭**动态加速**开关。关闭动态加速开关后，动态资源无加速效果，走静态边缘缓存逻辑，默认的静态文件加速规则有效，自行添加静态文件加速规则失效。

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**动静态加速规则**。
5. 打开**动态加速**开关。
6. 在**静态路径**页签下，单击**修改配置**。

7. 在**静态路径**对话框，配置**静态路径**。



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

8.

7.5. 动态内容回源配置

全站加速对动态资源的加速是基于智能选路技术，从众多回源线路中选择最优质的一条线路进行传输。动态内容回源配置是针对动态资源回源时的配置，包含动态内容回源协议的配置和开启动态负载均衡，这两者没有关联，您可以根据实际需求选择性地进行配置。

配置动态内容回源协议

动态资源回源使用的协议需要和客户端访问资源的协议保持一致，如果不一致，您可以配置动态资源的回源协议。如果未配置，动态内容默认跟随源站端口回源。

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. 打开**动态加速**开关。
6. 单击**动态内容回源配置**页签。
7. 在**动态内容协议跟随回源**后单击**修改配置**。
8. 在**动态内容协议跟随回源**对话框，设置**跟随方式**。

参数	说明
跟随客户端协议	当客户端以HTTP或HTTPS协议请求资源时，全站加速跟随客户端的协议请求源站。
跟随源站端口	当客户端以HTTP或HTTPS协议请求资源时，全站加速跟随源站端口所属的协议请求源站。
HTTP	全站加速以HTTP协议请求源站。
HTTPS	全站加速以HTTPS协议请求源站。

9. 单击**确定**，完成配置。

开启动态负载均衡

动态资源默认按性能优先回源，如果您需要按权重回源，需要开启动态负载均衡，开启后全站加速节点将按照您设置的回源权重大小回源到不同的源站获取资源，实现负载均衡。

- 性能优先回源
  根据全站加速的智能探测结果，回源时选择性能最佳的源站。
- 按权重回源
  回源时优先按照设置的权重比例回源到不同的源站。如果需要修改回源权重，请参见配置源站。

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. 打开**动态加速**开关。
6. 单击**动态内容回源配置**页签。
7. 打开**动态负载均衡**开关，即可开启**动态负载均衡**。

8.缓存配置

8.1. 什么是缓存

您使用DCDN加速静态资源时，DCDN会将源站上的资源缓存到距离客户端最近的DCDN节点上。当您访问该静态资源时，可直接从DCDN的缓存节点上获取，有效避免通过较长的链路回源，提高资源访问效率。阿里云DCDN的所有节点上都包含缓存软件，在用户请求或者源站响应资源经过DCDN节点时，缓存软件可以根据需要对用户请求或者源站响应资源做各种处理，包括设置缓存时长、改写回源请求等。
您可以通过缓存配置功能，对域名执行如下操作。

功能	说明
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，使其在DCDN上按照缓存规则进行缓存。
配置状态码过期时间	您可以配置资源的指定目录或文件后缀名的状态码过期时间。
配置自定义HTTP响应头	您可以配置资源缓存过期的HTTP消息头。
自定义页面	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。
配置URI重写规则	您可以对请求的URI进行修改和302重定向至目标URI。

8.2. 配置缓存过期时间

缓存过期时间指源站资源在DCDN节点缓存的时长，超过预设的缓存时间，资源将会被DCDN节点标记为失效资源。如果客户端向DCDN节点请求的资源已经失效，那么DCDN会回源站获取最新资源并缓存到DCDN节点。您可以根据业务需求，按目录或文件后缀名配置静态资源的缓存过期时间。

您可以通过以下内容了解和配置缓存过期时间：

- 注意事项
- 操作步骤
- 阿里云DCDN缓存规则及优先级
- HTTP协议缓存控制机制说明
- 配置示例
- 相关API

注意事项

- 建议您源站的内容不使用同名更新，而是采用版本号的方式同步。
  为了能准确找到更新前和更新后的源站内容，建议您源站的内容以版本号的方式同步，即更新源站内容时采用不同的名称。例如，采用*img-v1.0.jpg*、*img-v2.1.jpg*的方式命名。
- 缓存过期时间会影响回源频率，建议根据实际业务需求设置资源缓存时长。
  缓存过期时间过短，会导致全站加速节点频繁回源，增加源站的流量消耗；缓存过期时间过长，会带来数据更新时间慢的问题。
- 缓存在DCDN节点上的资源，由于热度低可能被提前从节点上删除。
- DCDN节点在收到源站响应的静态文件资源的时候，会按照阿里云DCDN缓存规则及优先级来执行。

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**页签下，单击**添加**。
6. 在**缓存过期时间**对话框，配置缓存规则。

参数	说明
类型	支持**目录**或**文件后缀名**指定资源范围 ○ **目录**：为某一路径下所有资源设置相同缓存规则。 ○ **文件后缀名**：为某一文件类型资源的设置相同缓存规则。

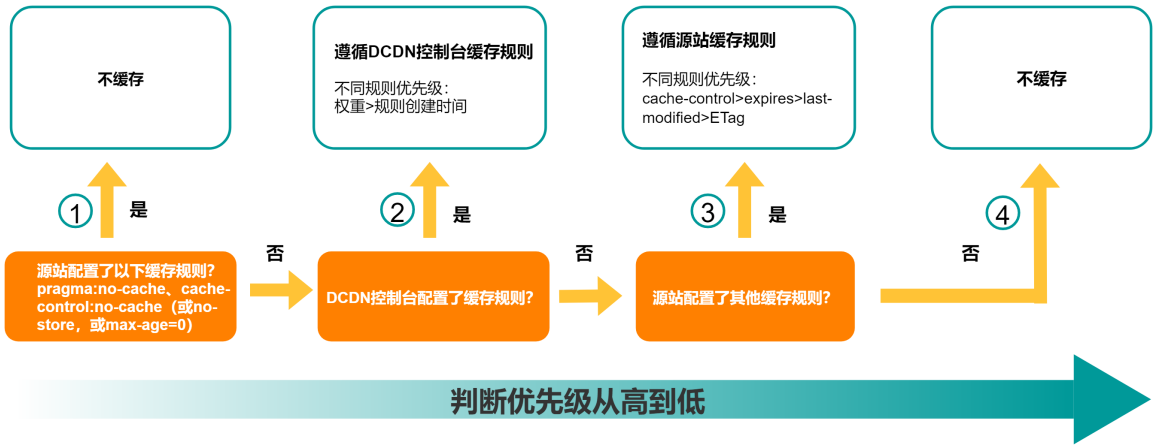
参数	说明
内容	指定待配置资源的目录或文件后缀名。 ○ 当类型选择**目录**时，填写说明如下： ■ 每次只能添加单条目录，可以用正斜线（/）匹配所有目录。 ■ 支持输入目录的完整路径，须以正斜线（/）开头，例如*/directory/aaa*。 ○ 当类型选择**文件后缀名**时，填写说明如下： ■ 支持输入一个或多个文件后缀名，多个文件后缀名用英文逗号（,）分隔，例如`jpg,txt`，大小写敏感，注意区分大小写。 支持的静态文件类型如下： ■ 图片：GIF、PNG、BMP、JPEG、JPG。 ■ 页面：HTML、HTM、SHTML。 ■ 音视频：MP3、WMA、FLV、MP4、WMV、OGG、AVI。 ■ 文本：DOC、DOCX、XLS、XLSX、PPT、PPTX、TXT、PDF。 ■ 其他：ZIP、EXE、TAT、ICO、CSS、JS、SWF、APK、M3U8、TS。 ■ 不支持用星号（*）匹配所有的文件类型。
过期时间	资源对应的缓存过期时间，最长可以设置3年。设置规则如下： ○ 不经常更新的静态文件：例如，图片类型、应用下载类型等，建议设置1个月以上。 ○ 频繁更新的静态文件：例如，JS、CSS等，您可以根据实际业务情况设置。 ○ 动态文件：例如，PHP、JSP、ASP等，建议设置为0s，即不缓存。
权重	权重即缓存规则的优先级。取值为1~99，数值越大优先级越高，对应规则优先生效。 **说明** ○ 有多条缓存规则的情况下，建议每条缓存规则都设置不同的权重，通过权重来控制规则执行优先级。 ○ 权重相同的规则生效优先级：先创建的 > 后创建的，与规则类型无关。 ○ 如果配置了多条缓存策略，其中一条缓存策略生效后将不再继续匹配其他的缓存策略。

7. 单击**确定**，完成配置。

   成功配置缓存过期时间后，您可以在**缓存过期时间**列表中，根据所需**修改**或**删除**配置。

阿里云DCDN缓存规则及优先级

DCDN节点在收到源站响应的静态文件资源的时候，会按照以下的缓存规则来执行（数值越小，优先级越高）：



1. 源站响应 `pragma:no-cache` 、 `cache-control:no-cache` （或者 `no-store` ，或者 `max-age=0` ）时，不缓存。
2. DCDN控制台设置的缓存过期时间或者状态码过期时间。

> **说明**
> 若DCDN请求同时命中多条规则，有且仅有一条规则会生效，优先级为：权重>规则创建时间。
> - 有多条缓存规则的情况下，建议每条缓存规则都设置不同的权重（权重越大优先级越高），通过权重来控制规则执行优先级。
> - 权重相同的规则生效优先级：先创建的 > 后创建的，与规则类型无关。

3. 源站配置其他缓存规则，优先级由高至低为：cache-control>expires>last-modified>etag。
   i. 源站响应中使用 `cache-control` 设置过期时间，取值为 `max-age` ，并且 `max-age` 大于0，例如：cache-control:max-age=3600。
   ii. 源站响应中使用 `expires` 设置过期时间，例如：expires:Tue, 25 Nov 2031 17:25:43 GMT。
   iii. 源站响应中携带了 `ETag` 或 `last-modified` ，则使用以下规则来计算缓存时间：
      a. 有 `last-modified` ，使用公式（当前时间-last_modified）* 0.1，计算结果在10秒~3600秒及之间的，取计算结果时间；小于10秒的，按照10秒处理；大于3600秒的，按照3600秒处理。
      b. 只有 `ETag` ，缓存10秒。
4. 源站返回的数据中 `ETag` 、 `last-modified` 、 `cache-control` 和 `expires` 这些缓存相关的响应头都没有携带，则默认不缓存。

HTTP协议缓存控制机制说明

在HTTP协议中定义了三种不同类型的协议头部来实现缓存控制相关的机制：

1. **过期时间校验机制**
   客户端在向服务端请求资源的过程中，双方将为资源约定一个过期时间，在该过期时间之前，该资源（缓存副本）就是有效的，过了过期时间后，该资源（缓存副本）就会失效。
   在HTTP协议中，控制缓存过期时间的Header常见的有下面这些：

头部名称	协议版本	作用	示例值	类型
Pragma	HTTP/1.0	Pragma用于表示内容是否为不缓存，通常取值no-cache，表示文件不缓存，常被用来兼容只支持HTTP1.0 协议的Server。	Pragma:no-cache	请求/响应
Expires	HTTP/1.0	Expires响应头包含日期/时间，表示在此时间之后，缓存内容将会过期。 如果使用了无效的日期，比如0，则代表该资源已经过期。	Expires: Wed, 21 Oct 2022 07:28:00 GMT	响应
Cache-Control	HTTP/1.1	Cache-Control响应头可以设置不同的指令来实现灵活的缓存控制，是目前主流客户端（如浏览器等）用于控制缓存的重要头部。	以下三个示例表示文件不缓存： ○ Cache-Control:no-cache ○ Cache-Control:no-store ○ Cache-Control:max-age=0 表示缓存有效期1小时的示例：Cache-Control:max-age=3600	请求/响应

2. **资源标签验证机制**
   客户端在首次向服务端请求资源的过程中，服务端将在响应头中带上资源标签，资源标签可以作为客户端再次请求同一资源时的校验标识。客户端再次请求同一资源时，请求头中将会携带资源标签，若服务端校验后认为该资源没有更新，则响应HTTP状态码304，告诉客户端该资源没有更新，客户端可以继续使用本地缓存；若服务端校验后发现资源标签不匹配，则告诉客户端该资源已经被修改或者已经过期，客户端需要重新获取资源内容。
   在HTTP协议中，控制缓存版本的Header常见的有下面这些：

头部名称	协议版本	作用	示例值	类型
Last-Modified	HTTP/1.0	Last-Modified表示资源的最后修改时间。	Last-Modified: Wed, 21 Oct 2015 07:28:00 GMT	响应
ETag	HTTP/1.1	ETag表示当前资源特定版本的唯一标识符。 对比ETag能判断资源是否变化，如果没有改变，源站服务器不需要发送完整的响应。	ETag: "33a64df551425fcc55e4d42a148795d9f25f89d4"	响应

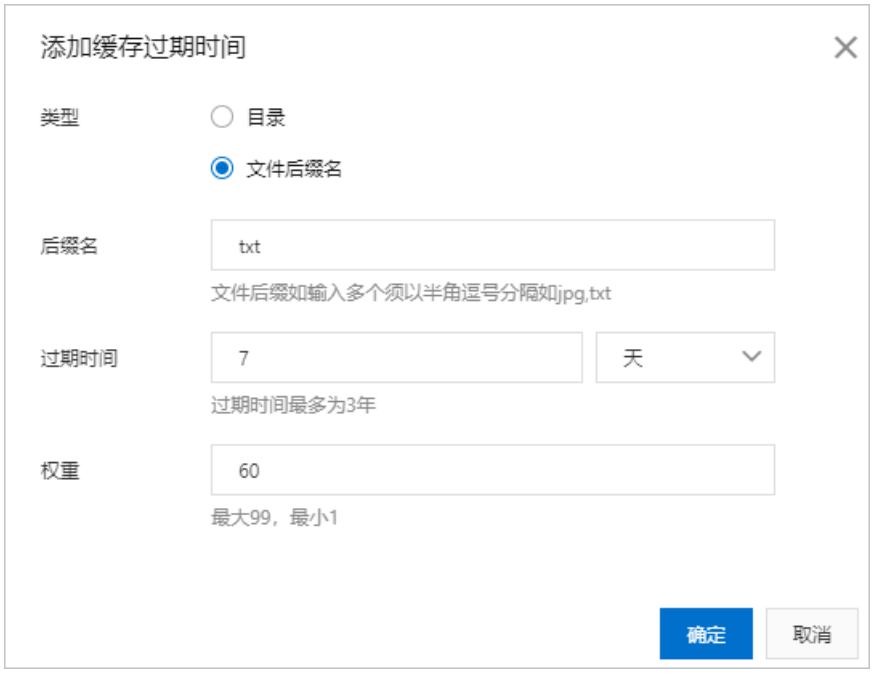
3. **多副本协商机制**
   缓存软件使用关键字索引在磁盘中缓存的对象，在HTTP/1.0中使用资源的URL作为关键字，但可能存在不同的资源基于同一个URL的情况，要区别它们还需要客户端提供更多的信息，例如：Accept-Language、Accept-Charset等头部，为了支持这种内容协商机制（content negotiation mechanism），HTTP/1.1在响应消息中引入了Vary头部，该头部列出了请求消息中需要包含哪些头部用于内容协商。

多副本协商机制通常使用HTTP协议的Vary头部来区分不同的缓存副本，实现不同的客户端请求同一个资源的时候可以拿到不同缓存副本：

头部名称	协议版本	说明	示例值	类型
Vary	HTTP/1.1	常用示例： ○ 服务端指定 `Vary: Accept-Encoding`，告知接收端（例如：DCDN节点）对于该资源需缓存两个版本（压缩和未压缩）。客户端向DCDN请求同一个资源时，老版本浏览器缓获取未压缩资源（避免兼容性问题），新版本浏览器获取压缩资源（减少数据传输流量）。 ○ 服务端指定 `Vary: User-Agent`，用来识别发送请求的浏览器类型，告知接收端（例如：DCDN节点），根据不同的浏览器类型缓存对应版本的资源。	Vary: Accept-Encoding Vary: Accept-Encoding,User-Agent	响应

配置示例

示例一：需要对“.txt”格式的文件缓存7天，在DCDN控制台增加一条文件名后缀为“.txt”的缓存规则，缓存过期时间设置为“7天”。



示例二：为加速域名 `demo.aliyun.com` 配置以下缓存策略，DCDN节点回源下载资源 `http://demo.aliyun.com/image/example.png`，虽然以下两条规则都匹配到了，但是因为这两条规则的权重相同，因此要判断规则创建的时间，先创建的规则优先级高于后创建的，因为目录/image这条规则创建的时间更早，所以系统最终生效的是目录类型这条规则。

相关API

BatchSetDcdnDomainConfigs

8.3. 配置状态码过期时间

DCDN节点从源站获取请求资源时，源站会返回响应状态码，您可以在阿里云DCDN上配置状态码缓存时间，当客户端再次请求相同资源时，实现由DCDN节点直接响应状态码，不会触发回源，减轻源站压力。当状态码超过设置的缓存时间，会重新触发回源。本文为您介绍如何配置状态码过期时间。

您可以通过以下内容，了解和配置状态码过期时间：

适用场景

正常情况下DCDN节点成功从源站获取到所请求的资源，即源站响应了2xx状态码时，会按照DCDN节点配置的缓存过期规则进行处理。

如果源站无法迅速响应所有状态码（例如非2xx状态码），且不希望所有请求全部由源站响应，可以配置状态码过期时间，由DCDN节点直接响应状态码，减轻源站压力。

典型场景：文件A在源站已被删除，但客户端仍持续访问，DCDN节点没有缓存文件A，所有请求转发回源，由源站响应4xx状态码，加剧源站压力。如果配置了缓存4xx状态码，DCDN节点首次回源后，会缓存4xx状态码，预设缓存时间内，当客户端再次请求文件A时，由DCDN直接响应4xx状态码，无需回源。

> **说明**
>
> - 对于303、304、401、407、600和601状态码，全站加速不进行缓存。
> - 对于204、305、400、403、404、405、414、500、501、502、503和504状态码，如果源站响应了Pragma、Cache-Control或者Expires的HTTP缓存规则，则遵循源站响应的HTTP缓存规则；如果源站没有相应HTTP缓存规则，全站加速也未设置状态码过期时间，则缓存时间默认为1秒。

多条规则生效说明

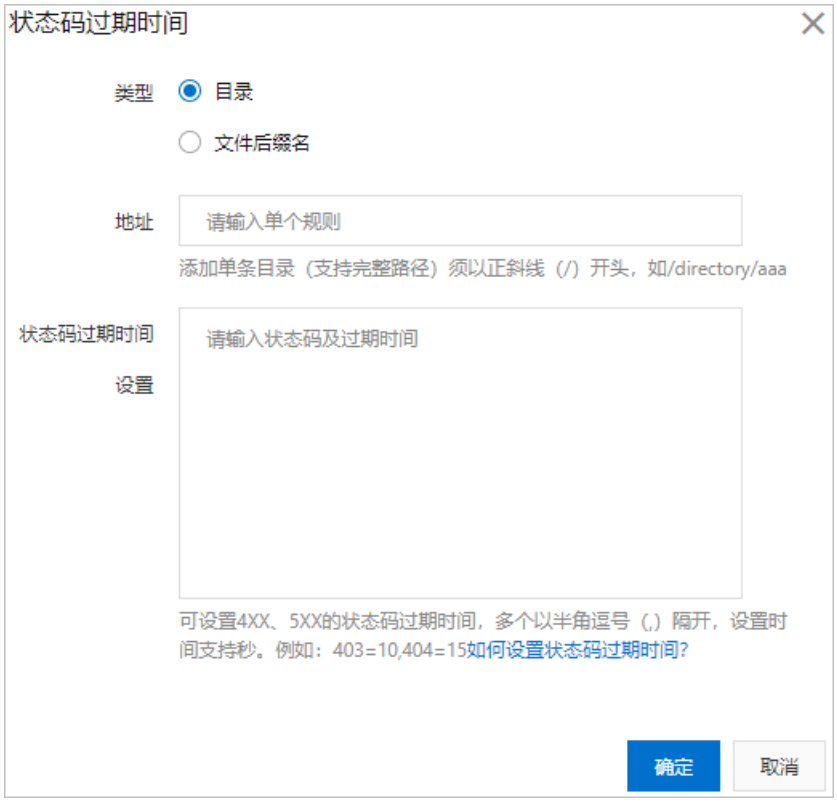
支持设置多条状态码缓存规则，当某个请求同时匹配了多条规则时，只会有一条规则生效，生效规则如下：

- **判断顺序**：
  先判断规则类型（文件后缀名 > 目录），再判断规则创建时间（先创建的 > 后创建的）。
- **不同类型规则的生效优先级：文件后缀名 > 目录。**
  例如，如果用户的请求同时匹配了2条规则（均配置了404状态码），规则类型分别为文件后缀名和目录类型，404状态码的过期时间以类型为文件后缀名的规则为准。具体示例，请参见配置示例。
- **相同类型规则的生效优先级：先创建的 > 后创建的**（规则列表由上而下）。
  例如，如果用户的请求同时匹配2条规则（均配置了404状态码），规则类型相同（均为文件后缀名或均为目录类型），404状态码的过期时间以“最早创建”的规则为准。具体示例，请参见配置示例。

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**状态码过期时间**页签。
6. 单击**添加**，配置状态码过期时间。



类型	注意事项
类型	支持**目录**和**文件后缀名**这两种类型，请根据您的实际需求选择。 **说明** 不同类型规则的生效优先级：文件后缀名 > 目录，具体请参见多条规则生效说明。

类型	注意事项
地址	○ 类型选择为**目录**，填写说明如下： ■ 每次只能添加一条目录。 ■ 支持输入目录的完整路径，须以正斜线（/）开头，例如*/directory/aaa*。 ○ 类型选择为**文件后缀名**，填写说明如下： ■ 支持输入一个或多个文件后缀名，多个文件后缀名用半角逗号（,）分隔，例如`JPG,TXT`。 **说明** 不同记录中配置的文件后缀名类型完全相同，仅有大小写区分时，后面创建的会覆盖掉前面创建的，例如创建JPG,TXT规则后，再创建jpg,txt规则时，会覆盖掉之前创建的JPG,TXT记录。此时，如果需要配置小写规则，可以单独创建txt和jpg的规则。配置规则实际生效的时候是严格区分大小写。 ■ 不支持用星号（*）匹配所有的文件类型。
状态码过期时间设置	需要缓存的状态码及其缓存时间，最长可设置3年，单位：秒，配置规则如下： ○ 多个状态码用半角逗号（,）分隔。 ○ 对于2xx、3xx状态码，仅支持单个精准配置，不支持模糊批量配置。例如，201=10（支持），2xx=12（不支持）。 ○ 对于4xx、5xx状态码，既支持单个精准配置，也支持模糊批量配置。例如，401=10（支持），4xx=12（也支持）。

7. 单击**确定**，完成配置。

   成功配置状态码过期时间后，您可以在**状态码过期时间**列表中，对当前的配置进行**修改**或**删除**操作。

配置示例

- **示例一：目录类型规则**

  创建目录类型规则如下图所示：

地址	类型	状态码过期时间	状态	操作
/directory/aaa	目录	4xx=10,201=15	成功	修改 | 删除

  在/directory/aaa目录下，所有4xx状态码缓存时间为10秒，201状态码缓存时间为15秒，在该时间区间内，由DCDN节点直接响应对应的访问请求；超过该时间后，会触发回源。

- **示例二：文件后缀名类型规则**

  创建文件后缀名类型规则如下图所示：

地址	类型	状态码过期时间	状态	操作
jpg,txt	文件后缀名	403=10,404=15	成功	修改 | 删除

  文件后缀为.jpg或.txt类型，403状态码缓存时间为10秒，404状态码缓存时间为15秒，在该时间区间内，由DCDN节点直接响应对应的访问请求；超过该时间后，会触发回源。

- **示例三：不同类型规则的生效优先级**

分别创建了一条“目录类型规则”和一条“文件后缀名类型规则”，设置了不同的状态码过期时间，如下图所示：

地址	类型	状态码过期时间	状态	操作
/directory/aaa	目录	503=10,404=15	成功	修改 | 删除
jpg,txt	文件后缀名	403=20,404=20	配置中	修改 | 删除

用户请求 `http://example.com/directory/aaa/test.jpg`，DCDN节点上没有缓存资源，DCDN节点向源站请求资源，源站响应了404状态码，这里同时匹配上了“目录类型规则”和“文件后缀名类型规则”，因为在规则类型不同的情况下，规则生效优先级是**文件后缀名 > 目录**，所以“文件后缀名类型规则”生效，404状态码的实际缓存时间是20秒。

- **示例四：相同类型多条规则的生效优先级**
  先创建了一条“目录类型规则一”，匹配的地址是“/directory”，然后再创建另一条“目录类型规则二”，匹配的地址是“/directory/aaa”，设置了不同的状态码过期时间，如下图所示：

地址	类型	状态码过期时间	状态	操作
/directory	目录	503=10,404=15	成功	修改 | 删除
/directory/aaa	目录	403=20,404=20	配置中	修改 | 删除

用户请求 `http://example.com/directory/aaa/test.jpg`，DCDN节点上没有缓存资源，DCDN节点向源站请求资源，源站响应了404状态码，这里同时匹配上了两条“目录类型规则”，因为在规则类型相同的情况下，规则生效优先级是**早创建的 > 晚创建**的，所以最早创建的“目录类型规则一”生效，404状态码的实际缓存时间是15秒。

相关API

BatchAddDcdnDomain

8.4. 配置自定义HTTP响应头

HTTP响应头是HTTP响应消息头的组成部分之一，可携带特定响应参数并传递给客户端。通过配置自定义HTTP响应头，当用户请求加速域名下的资源时，DCDN返回的响应消息会携带您配置的响应头，从而实现特定功能（比如，实现跨域访问）。

适用场景

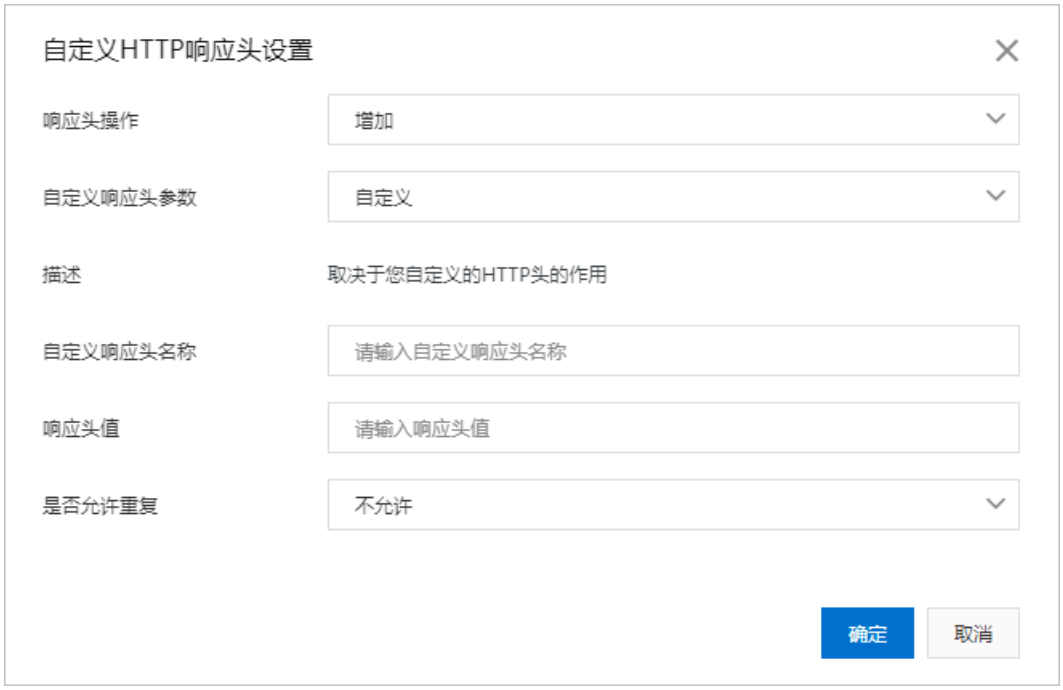
场景一：告知客户端全站加速响应文件的资源类型。添加响应头Content-Type: text/html告知客户端全站加速响应文件的格式是HTML格式。

场景二：实现跨域资源访问。当用户请求DCDN上某个域名的资源时，您可以在DCDN返回的响应消息中配置响应头Access-Control-Allow-Origin，以实现跨域访问，请参考DCDN如何配置跨域资源共享（CORS）及注意事项；另外，全站加速还支持按照已配置CORS规则对接收到的用户的跨域请求进行校验，以实现更灵活的跨域资源访问控制。

> **说明**
>
> - HTTP响应头的配置属于域名维度的配置，一旦配置生效，便会对域名下所有资源的响应消息生效。
> - 配置HTTP响应头仅影响客户端（例如浏览器）的响应行为，不会影响到全站加速节点的缓存行为。泛域名暂不支持配置自定义HTTP响应头。

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**自定义HTTP响应头**对话框，单击**添加**，根据下表中的参数含义设置自定义HTTP响应头。



参数	说明
响应头操作	您可以增加、删除、变更和替换指定的响应头。
自定义响应头参数	选择自定义响应头参数。详细信息，请参见响应头参数。
描述	您自定义的HTTP头的作用。
自定义响应头名称	当**自定义响应头参数**选择为**自定义**时，需要配置自定义响应头名称。自定义响应头名称要求如下： ○ 由大小写字母、短划线（-）和数字组成。 ○ 长度为1~100个字符。
响应头值	输入您要设置的响应头值。详细信息，请参见响应头参数。
是否允许重复	○ **允许**：允许重复将会保留源站返回的头，同时会加上一个同名的头。 ○ **不允许**：如果不允许重复，源站返回的头会被新配置的同名头覆盖。

参数	说明
跨域校验	跨域校验默认为关闭状态，只有在**响应头操作**为“增加”，**自定义响应头参数**为“Access-Control-Allow-Origin”的时候才可以配置。 ○ **开启**：开启状态下全站加速节点将按以下规则对用户做跨域校验，并根据校验结果响应“Access-Control-Allow-Origin”的值。 ○ **关闭**：关闭状态下全站加速节点不会校验用户请求中携带的Origin头，只会固定响应已配置的Access-Control-Allow-Origin值。 **说明** 跨域校验规则： ○ 如果自定义响应头参数“Access-Control-Allow-Origin”的值设置为“*”不论用户请求里面是否携带“Origin”参数，也不论携带的“Origin”参数为何值，都固定返回“Access-Control-Allow-Origin:*”。 ○ 如果跨域资源共享的响应头值设置了单个或者多个值（多个值之间用“,”分隔）。 ■ 如果用户请求头里携带的“Origin”参数值与被设置的任意一个值精确匹配，就会响应对应的跨域头。 ■ 如果都没有精确匹配上，则不响应跨域头。 ○ 如果跨域资源共享的响应头值设置了泛域名，则会校验请求头中Origin值是否能匹配上“Access-Control-Allow-Origin”的泛域名。 配置示例请参见DCDN如何配置跨域资源共享（CORS）及注意事项。

6. 单击**确定**，完成配置。

   在**HTTP头**列表中，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。

响应头参数

响应头参数	说明	示例
自定义	支持添加自定义响应头。自定义响应头名称要求如下： • 由大小写字母、短划线（-）和数字组成。 • 长度为1~100个字符。	Test-Header

响应头参数	说明	示例
Content-Type	指定浏览器响应对象的内容类型。	text/html
Cache-Control	指定客户端程序请求和响应遵循的缓存机制。	no-cache
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。	examplefile.txt
Content-Language	指定浏览器响应对象的语言。	en-US
Expires	指定浏览器响应对象的过期时间。	Wed, 21 Oct 2015 07:28:00 GMT
Pragma	Pragma HTTP 1.0是用于实现特定指令的响应头，具有通过请求和响应链实现各种效果的功能，可用于兼容HTTP 1.1。	no-cache
Access-Control-Allow-Origin	指定允许的跨域请求的来源。填写星号（*）表示全部域名；您也可以填写完整域名，例如 `http://www.aliyun.com` 。 **说明** • 响应头值支持配置为“*”，表示任意来源。 • 响应头值非“*”的情况下，支持配置单个或者多个IP、域名、或者IP和域名混合。相互间用“,”分隔。 • 响应头值非“*”的情况下，必须包含协议头“http://”或者“https://”。 • 响应头值支持携带端口。 • 响应头值支持泛域名。	• * • http://www.aliyun.com
Access-Control-Allow-Methods	指定允许的跨域请求方法。可同时设置多个方法，多个方法用英文逗号（,）分隔。	POST,GET
Access-Control-Allow-Headers	指定允许的跨域请求字段。	X-Custom-Header
Access-Control-Max-Age	指定客户端程序对特定资源的预请求返回结果的缓存时间，单位为秒。	600
Access-Control-Expose-Headers	指定允许访问的自定义头信息。	Content-Length
Access-Control-Request-Method	发出请求时报头用于预检请求让服务器知道哪些HTTP方法的实际请求时将被使用。	POST
Access-Control-Request-Headers	发出请求时报头用于预检请求让服务器知道哪些HTTP头的实际请求时将被使用。	X-PINGOTHER

响应头参数	说明	示例
Access-Control-Allow-Credentials	该响应头表示是否可以将对请求的响应暴露给页面。 • 返回true：表示可以暴露。 • 返回其他值：表示不可以暴露。	true

8.5. 自定义页面

当页面访问出错时，客户端会显示默认错误页面，例如404 Not Found。您可以通过全站加速自定义报错页面，当页面出现报错时，会在客户端展示您自定义的报错页面，优化网站体验。本文介绍配置自定义错误页面的方法。

背景信息

阿里云DCDN提供了在出现指定错误码的时候，能够让用户跳转到自定义页面的功能。

当客户端通过浏览器请求Web服务时，如果请求的URL不存在，Web服务器默认会返回404报错页面。Web服务器默认的报错页面通常不美观，为了提升访问者的体验，您可以配置自定义页面，根据所需自定义HTTP或HTTPS响应状态码跳转的完整URL地址。

> **说明**
> - 仅支持针对400、403、404、405、414、416、500、501、502、503、504这些状态码设置自定义页面。
> - 自定义页面如果使用的是DCDN加速的资源，那么将会按照正常的DCDN内容分发来计费。

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**页签。
6. 在**自定义页面**页签下，单击**添加**，配置自定义页面的错误码和链接。

7. 单击**确定**，完成配置。

   在**自定义页面**列表中，您也可以单击**修改**或**删除**，对当前配置进行相应操作。

配置示例

您希望将404页面显示为自定义页面，假设您已经将自定义404页面 `error404.html` 存放在源站的根目录下，并且通过加速域名 `example.aliyundoc.com` 可以访问到这个404页面，这个时候您可以通过以下配置来实现404状态码的自定义错误页面。

- 错误码：404
- 链接：您自定义的URL页面，例如：http://example.aliyundoc.com/error404.html。
- 结果：访问返回404报错时，会跳转到http://example.aliyundoc.com/error404.html页面。

8.6. 配置URI重写规则

如果客户端实际请求的URI与全站加速节点上缓存资源的URI不匹配，可通过URI重写功能，将请求URI重定向到目标URI。

您可以通过以下内容了解和使用URI重写规则：

背景信息

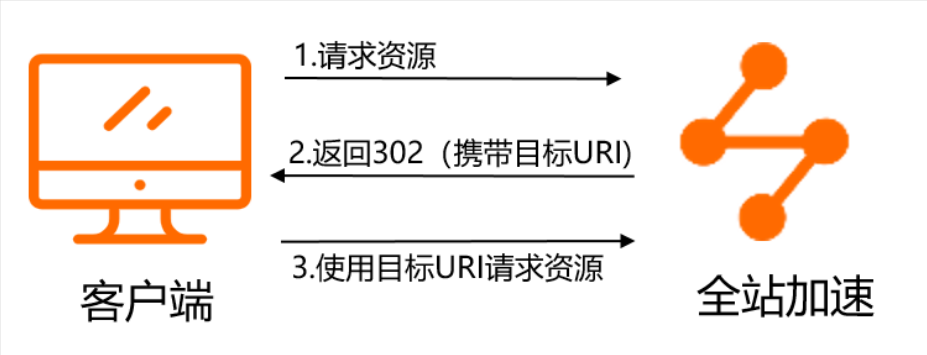
HTTP 302状态码（即302 Found），可表示资源被临时改变了位置。配置URI重写后，全站加速节点会在给客户端发送的302状态码响应信息的HTTP Location头部中放置新的URI地址信息，客户端收到302状态码响应之后，将会向新的URI地址发起请求。

配置URI重写规则后，全站加速节点默认给客户端发送302重定向状态码，同时也支持303和307重定向状态码，如果您需要修改重定向状态码，可以通过提交工单申请。

编码	含义	处理方法	典型应用场景
302	Found	GET方法不会发生变更，其他方法有可能会变更为GET方法。	由于不可预见的原因该页面暂不可用。在这种情况下，搜索引擎不会更新它们的链接。
303	See Other	GET方法不会发生变更，其他方法会变更为GET 方法（消息主体会丢失）。	用于PUT或POST请求完成之后进行页面跳转，防止由于页面刷新导致的操作的重复触发。
307	Temporary Redirect	方法和消息主体都不发生变化。	由于不可预见的原因该页面暂不可用。在这种情况下，搜索引擎不会更新它们的链接。当站点支持非 GET 方法的链接或操作的时候，该状态码优于 302 状态码。

适用场景

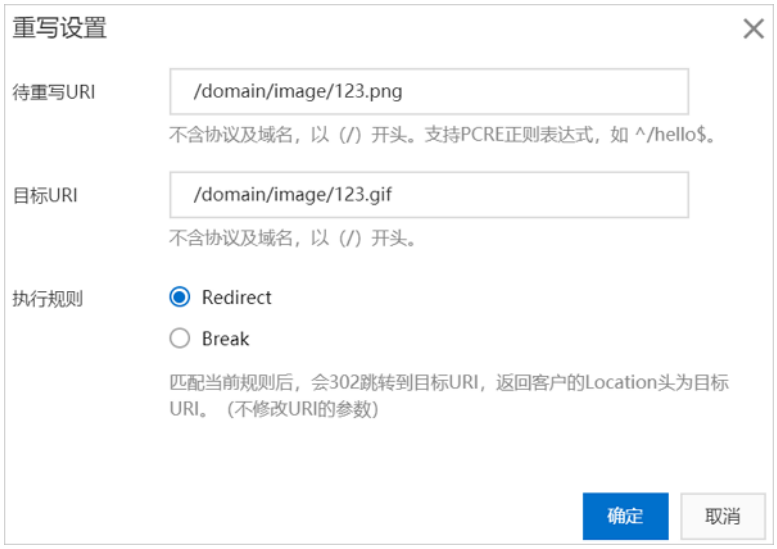
客户源站的资源存放路径发生了变更，全站加速节点上的资源存放路径也发生了变更，但是用户请求URL里面包含的资源路径没有变更，这时就需要全站加速节点来改写用户请求里面的资源路径。例如：图片文件原先存放在目录“/download/”，现在变更为“/image/”。



操作步骤

> **注意** 单个域名最多可以配置50条重写规则。配置多条规则时，按照全站加速控制台URI重写列表由上而下的顺序执行。

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**重写**页签。
6. 单击**添加**，根据您的实际需求，配置**待重写URI**、**目标URI**和**执行规则**。



参数	说明
待重写URI	以正斜线（/）开头的URI，不含http://头及域名。支持PCRE正则表达式，例如：^/hello$。
目标URI	以正斜线（/）开头的URI，不含http://头及域名，例如：/index.html。

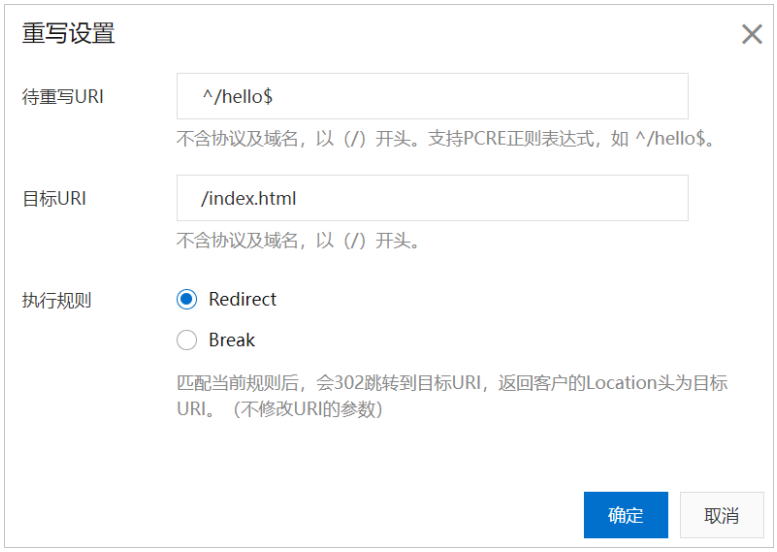
参数	说明
执行规则	支持**Redirect**和**Break**这两种规则。 ○ **Redirect**：如果请求的URI匹配了当前规则，该请求将被302重定向到目标URI。执行完当前规则后，当存在其他配置规则时，会继续匹配剩余规则。 ○ **Break**：如果请求的URI匹配了当前规则，请求将被改写为目标URI。执行完当前规则后，当存在其他配置规则时，将不再匹配剩余规则。

7. 单击**确定**，完成配置。

   成功配置重写功能后，您可以在重写列表中，对当前的配置进行**修改**或**删除**操作。

配置示例

URI重写规则按照正则表达式配置如下图所示：



客户端请求 `http://example.aliyundoc.com/hello` 时，请求中包含 `/hello` ，全站加速节点会在302状态码的Location信息里写入新的URI地址 `http://example.aliyundoc.com/index.html` ，并返回给客户端，客户端对 `http://example.aliyundoc.com/index.html` 发起请求。

相关API

BatchSetDcdnDomainConfigs

9.HTTPS配置

9.1. 什么是HTTPS证书

本文介绍了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节点之间请求的HTTPS加密，保障数据传输的安全性。

您可通过以下内容了解和使用HTTPS加速：

- 什么是HTTPS?
- 工作原理
- 计费说明
- 功能优势
- 应用场景
- HTTPS功能使用说明
- 如何开启HTTPS安全加速

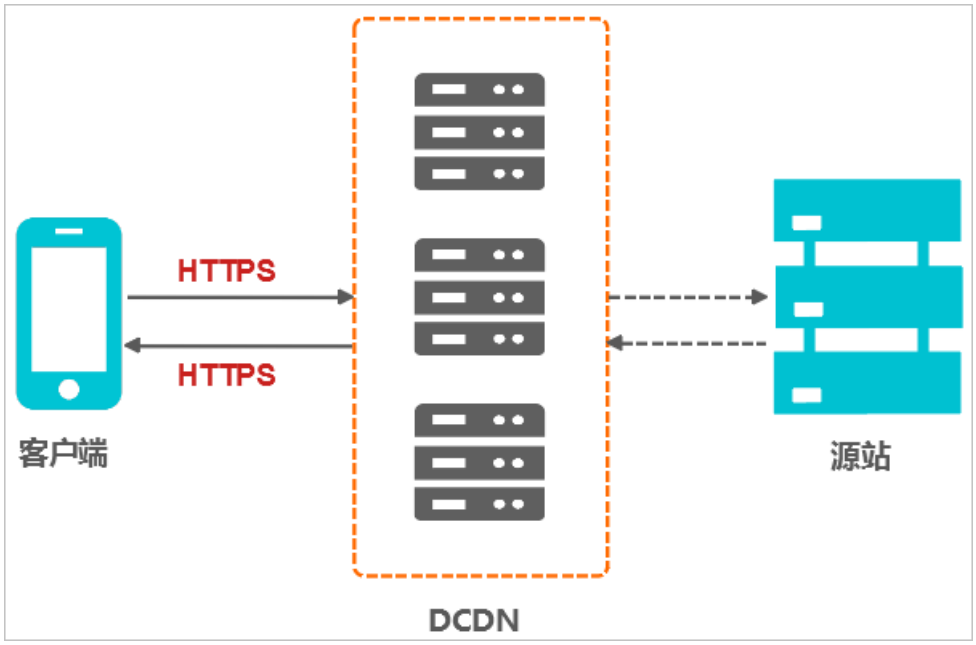
什么是HTTPS?

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。

工作原理

在阿里云全站加速控制台开启的HTTPS协议，将实现客户端和阿里云全站加速节点之间请求的HTTPS加密。如果需要实现全链路HTTPS加密，还需要配置全站加速节点以HTTPS协议回源到源站服务器（源站服务器需要支持HTTPS协议）。

HTTPS加密流程如下图所示。



1. 通过全站加速控制台在全站加速节点上提前准备好SSL证书的公钥和私钥。

> **说明** 公钥和私钥通过申请证书或者上传证书来获取。

2. 全站加速节点将相应的SSL证书公钥传送给客户端。
3. 客户端解析SSL证书公钥的正确性。
   - 如果SSL证书公钥正确，则会生成一个随机数（密钥），并用公钥进行加密，并传输给全站加速节点。
   - 如果SSL证书公钥不正确，则SSL握手失败，需要重新配置HTTPS证书。

   > **说明** 正确性包括以下内容：
   > - 证书未过期。
   > - 发行证书的CA可靠。
   > - 发行者证书的公钥能够正确解开证书的发行者的数字签名。
   > - 证书上的域名和全站加速实际加速的域名相匹配。

4. 全站加速节点用之前的私钥进行解密，得到随机数（密钥）。
5. 全站加速节点用随机数（密钥）对传输的数据进行加密。
6. 客户端用随机数（密钥）对全站加速节点的加密数据进行解密，拿到相应的数据。

计费说明

HTTPS安全加速属于增值服务，开启后将产生HTTPS请求数计费，详细计费标准，请参见HTTPS请求数/动态HTTP请求数。

> **说明** HTTPS根据请求数单独计费，无法使用全站加速流量包来抵扣。请确保账户余额充足再开通HTTPS服务，以免因额外消耗的HTTPS请求数费用导致账号欠费，从而影响您的全站加速服务。

功能优势

HTTPS安全传输的优势：

- HTTPS安全传输，有效防止HTTP明文传输中的窃听、篡改、冒充和劫持风险。
- 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。
- 主流搜索引擎都已经对HTTPS网站进行搜索加权，使用HTTPS协议访问的网站将会得到更高的搜索排名。新版的HTTP/2协议访问体验更好，已经得到越来越多的支持，而支持HTTP/2必须支持HTTPS。因此，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。

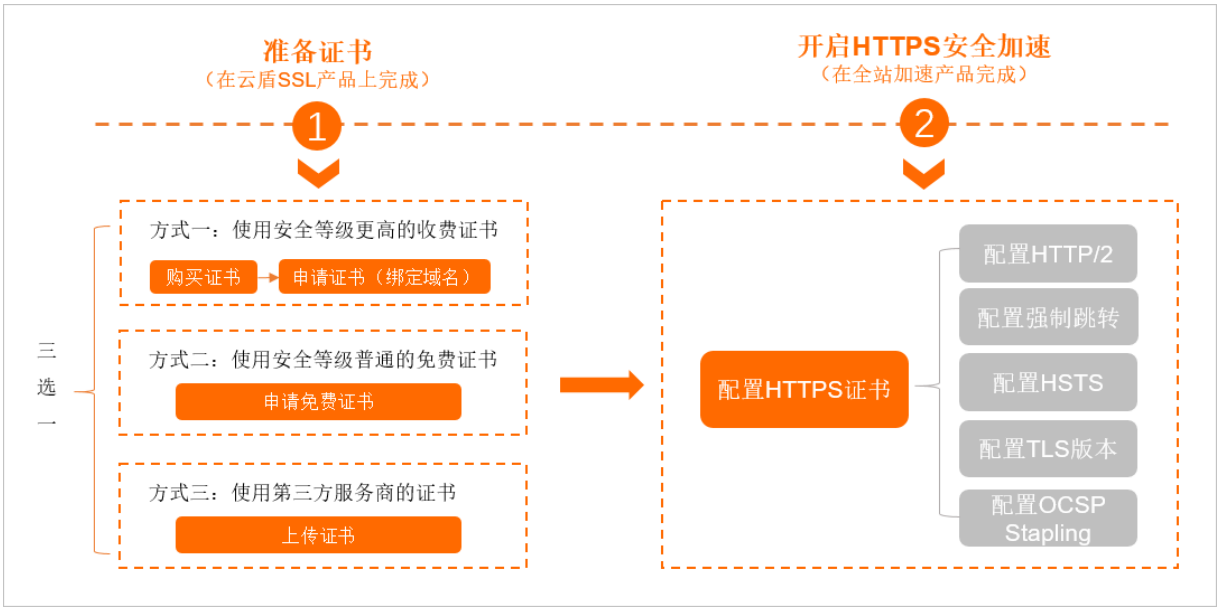
应用场景	说明
企业应用	若网站内容包含CRM、ERP等信息，这些信息属于企业级的机密信息，若在访问过程中被劫持或拦截窃取，对企业是灾难级的影响。
政务信息	政务网站的信息具备权威性，正确性等特征，需预防钓鱼欺诈网站和信息劫持，避免出现信息劫持或泄露引起社会公共的信任危机。
支付体系	支付过程中涉及到敏感信息，例如姓名、电话等，防止信息被劫持和伪装欺诈，需启用HTTPS加密传输，避免出现下单后下单客户会立即收到姓名、地址、下单内容，然后以卡单等理由要求客户按指示重新付款之类的诈骗信息，造成客户和企业的双重损失。
API接口	保护敏感信息或重要操作指令的传输，避免核心信息在传输过程中被劫持。
企业网站	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。

HTTPS功能使用说明

HTTPS安全加速功能使用说明，如下表所示。

分类	注意事项
适用场景	• 所有的域名业务类型都支持开启HTTPS安全加速。 • 支持为泛域名配置HTTPS加速服务。 • 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。 启用/停用HTTPS加速。 • 启用：您可以修改证书。您也可以配置强制跳转，通过HTTP协议来访问的用户也能跳转到更安全的HTTPS协议。 • 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HTTPS安全加速时，需要重新从云盾SSL证书中心选择需要使用的证书。详细说明，请参见配置HTTPS证书。
计费	HTTPS安全加速属于增值服务，开启后将产生HTTPS请求数计费，详细计费标准，请参见HTTPS请求数/动态HTTP请求数。 **说明** HTTPS根据请求数单独计费，费用不包含在全站加速流量包内。请确保账户余额充足再开通HTTPS服务，以免因HTTPS服务欠费影响您的全站加速服务。
证书管理	• 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。 • 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。 其他证书相关的常见问题，请参见更多证书问题。

如何开启HTTPS安全加速



1. 准备证书（在云盾SSL产品上完成）。
   支持以下三种证书（三选一），请根据证书类型在阿里云SS证书产品上完成对应操作。
   - 收费证书（安全等级更高）：购买证书>申请证书。
   - 免费证书（安全等级普通）：申请免费DV试用证书。
   - 第三方服务商证书：需先上传至阿里云SSL证书平台，具体操作参见上传证书。
2. 开启HTTPS安全加速（在全站加速产品上完成）。
   i. 准备证书后，需配置HTTPS证书，才能开启HTTPS安全加速。
   ii. （可选）您可根据实际需求，配置高阶功能（例如强制跳转）。

功能	说明
配置HTTP/2	HTTP/2（HTTP2.0）是继HTTP1.1版本之后的新版HTTP协议，支持二进制分帧、多路复用、首部压缩等最新的特性，能够大幅度提高Web性能，降低数据交互延迟，目前Chrome、Edge、Safari以及Firefox等主流浏览器都已经支持HTTP/2协议。
配置强制跳转	强制重定向终端用户的原请求方式。
配置HSTS	强制客户端（如浏览器）使用HTTPS与服务器创建连接，降低第一次访问被劫持的风险。
配置TLS版本控制	保障您互联网通信的安全性和数据完整性。
配置OCSP Stapling	全站加速预先缓存在线证书验证结果并下发给客户端，无需浏览器直接向CA站点查询证书状态，从而减少用户验证时间。

9.2. 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。本文介绍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。

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。阿里云全站加速使用的证书是Nginx，证书格式为 `.crt` ，证书私钥格式为 `.key` 。

证书上传规则为：

- 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 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，您只需在全站加速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
```

9.3. 配置HTTPS证书

全站加速支持HTTPS加速服务，您可以上传自定义证书或将已经托管在阿里云SSL证书服务的证书部署至全站加速平台，启用HTTPS加速服务，实现全网数据加密传输。本文介绍配置和更新HTTPS证书的操作方法。

前提条件

- 已经拥有HTTPS证书。如果需要购买证书，您可以在SSL证书控制台申请免费证书或购买高级证书。
- 自有证书需满足证书格式要求。详细信息，请参见证书格式说明。

背景信息

根据认证级别不同，可分为多种类型的证书，不同类型证书的安全性和适用的网站类型不同。详细信息，请参见支持选购的证书类型。

全站加速仅支持 `PEM` 格式的证书，如果证书不是 `PEM` 格式，需转换成 `PEM` 格式。转换方法，请参见证书格式转换方式。

> **说明**
>
> - CRT后缀文件是Certificate的简称，可能是PEM编码格式，也可能是DER编码格式。进行证书格式转换前请仔细确认您的证书格式是否需要转换。
> - PEM（Privacy Enhanced Mail）一般为文本格式，以“-----BEGIN ***-----”开头，以“-----END ***-----结尾”，中间的内容是Base64编码。这种格式可以保存证书和私钥，为了区分证书与私钥，一般会将PEM格式的私钥后缀改为 `.key` 。

步骤一：配置或更新HTTPS证书

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HTTPS请求数/动态HTTP请求数。

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**对话框，打开**HTTPS安全加速**开关。

   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HTTPS请求数/动态HTTP请求数。
7. 配置证书相关参数。

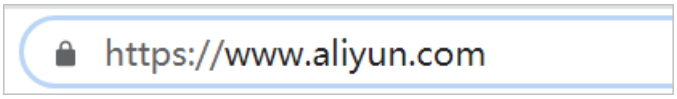
参数	说明

参数	说明
证书来源	证书来源包含以下三种，三种证书之间可以相互切换。 ○ 云盾（SSL）证书中心 您可以在SSL证书控制台快速申请各种品牌及各种类型的证书。 ○ 自定义上传（证书+私钥） 如果证书列表中无当前适配的证书，您可以上传自定义证书。您需要在设置证书名称后，上传证书内容和私钥，该证书将在阿里云SSL证书服务中保存。您可以在我的证书中查看。 说明 a. 上传该类型的证书时如果提示证书重复，您可以修改证书名称后再上传。 b. 如果您不希望将私钥暴露在阿里云CDN以外的环境中，那么您可以使用数字证书管理服务提供的 CSR（Certificate Signing Request） 管理工具，生成基于RSA、ECC、SM2（国密）密钥算法的CSR和私钥，或上传已有的CSR，请参见管理CSR。 ○
证书名称	当证书来源为以下两种时，需要配置证书名称。 ○ 云盾（SSL）证书中心 ○ 自定义上传（证书+私钥）
证书（公钥） 私钥	当证书来源选择自定义上传（证书+私钥）时，需要配置证书（公钥）和私钥。配置方法参见证书（公钥）和私钥输入框下方的pem编码参考样例。

8. 单击**确定**，完成配置。

步骤二：验证HTTPS配置是否生效

更新HTTPS证书1分钟后将全网生效。您可以使用HTTPS方式访问资源，如果浏览器中出现锁的HTTPS标识，表示HTTPS安全加速已生效。



步骤三：关闭HTTPS安全加速

如果您不再使用HTTPS安全加速功能，可随时在全站加速控制台关闭HTTPS安全加速。关闭HTTPS安全加速实时生效，关闭后您将无法继续使用HTTPS安全加速功能。

9.4. 配置HTTP/2

HTTP/2（HTTP2.0）是继HTTP1.1版本之后的新版HTTP协议，支持二进制分帧、多路复用、首部压缩等最新的特性，能够大幅度提高Web性能，降低数据交互延迟。本文主要介绍HTTP/2的概念、优势、使用场景和配置方法。

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。
> - 如果您关闭了HTTPS证书功能，HTTP/2设置系统默认置灰，无法开启。
> - 如果您开启HTTP/2后，关闭了HTTPS证书功能，HTTP/2也会自动失效。

什么是HTTP/2

HTTP/2也被称为HTTP 2.0，相对于HTTP 1.1新增了多路复用、压缩HTTP头、划分请求优先级和服务端推送等特性，解决了在HTTP 1.1中一直存在的问题，优化了请求性能，同时兼容了HTTP 1.1的语义。目前，Chrome、Edge、Safari和Firefox等浏览器已经支持HTTP/2协议。

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。
- 多路复用（MultiPlexing）：在HTTP1.x中，我们经常会使用到雪碧图、使用多个域名等方式来优化性能，因为浏览器限制了同一个域名下的请求数量，当页面需要请求很多资源的时候，队头阻塞（Head of line blocking）会导致在达到最大请求时，资源需要等待其他资源请求完成后才能继续发送。HTTP2.0中，基于二进制分帧层，HTTP2.0可以在共享TCP连接的基础上同时发送请求和响应，在另一端根据流标识符和首部将他们重新组装起来，通过该技术，可以避免HTTP旧版本的队头阻塞问题，极大提高传输性能。
- 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）：服务端可以对一个客户端请求发送多个响应，服务端向客户端推送资源无需客户端明确的请求。

开启或关闭HTTP/2

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**区域，打开HTTP/2开关，开启该功能。

9.5. 配置OCSP Stapling

OCSP Stapling功能，可实现由全站加速预先缓存在线证书验证结果并下发给客户端，无需浏览器直接向CA站点查询证书状态，从而减少用户验证时间。本文主要介绍OCSP Stapling功能的概念、使用前提和配置方法。

您可通过以下内容了解和使用OCSP Stapling功能：

- 功能说明
- 前提条件
- 操作步骤

功能说明

OCSP（Online Certificate Status Protocol，在线证书状态协议）是由数字证书颁发机构CA（Certificate Authority）提供，客户端通过OCSP可实时验证证书的合法性和有效性。

启用OCSP Stapling功能后，OCSP信息查询的工作将由全站加速服务器完成。全站加速通过低频次查询，将查询结果缓存到服务器中（默认缓存时间60分钟）。当客户端向服务器发起TLS握手请求时，全站加速服务器将证书的OCSP信息和证书一起发送到客户端，供用户验证，无需用户再向数字证书认证机构（CA）发送查询请求。极大地提高了TLS握手效率，节省了用户验证时间。

注意

- OCSP Stapling功能默认关闭。
- OCSP Stapling功能默认缓存时间是1小时，缓存过期后第一个访问请求OCSP Stapling将不生效，直到重新获取OCSP Stapling信息为止。
- 配置了HTTPS加速的域名，可启用或者关闭OCSP Stapling功能，删除证书配置后，OCSP Stapling功能会同步失效。
- OCSP信息是无法伪造的，因此这一过程不会产生额外的安全问题。

前提条件

执行配置前，请您确保：

- 您已成功配置HTTPS证书，操作方法请参见配置HTTPS证书。
- 客户端支持OCSP扩展字段，如果客户端不支持OCSP扩展字段，则功能无法生效。
- 您的业务有一定量的QPS以保证全网触发，QPS过低可能导致配置无法生效。

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**OCSP Stapling**区域，打开**OCSP Stapling**开关，即可完成配置。

9.6. 配置强制跳转

您可以通过配置强制跳转功能，将客户端到边缘节点的原请求方式强制重定向为HTTP或者HTTPS请求。

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。

适用场景

HTTP和HTTPS强制跳转功能适用以下场景：

- 已经配置了HTTPS证书的加速域名，可配置强制跳转，默认通过301重定向方式，将客户端到全站加速节点的HTTP请求强制跳转为HTTPS请求，HTTPS请求更安全。

```
$ 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>
```

- 对于安全性要求不高的业务应用，对应的加速域名可配置强制跳转，默认通过301重定向方式，将客户端到全站加速节点的HTTPS请求强制跳转为HTTP请求。

强制跳转功能默认使用301重定向方式，同时也支持308重定向方式，如果您需要修改重定向方式，可以通过提交工单申请。

编码	含义	处理方法	典型应用场景
301	Moved Permanently	GET方法不会发生变更，其他方法有可能会变更为GET方法。	网站重构。
308	Permanent Redirect	方法和消息主体都不发生变化。	网站重构，用于非GET方法。(with non-GET links/operations)

强制跳转前后请求数计费说明

- **跟随方式**选择**HTTPS -> HTTP**时：强制跳转前的HTTPS请求会产生请求数计费，跳转后的HTTP请求免费。
- **跟随方式**选择**HTTP -> HTTPS**时：强制跳转前的HTTP请求免费，跳转后的HTTPS请求会产生请求数计费。

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，单击目标域名对应的**配置**。
4. 在指定域名的左侧导航栏，单击**HTTPS配置**。

5. 在**强制跳转**区域，单击**修改配置**。
6. 在**强制跳转**对话框，选择**跟随方式**。

跟随方式	说明
默认	同时支持HTTP和HTTPS方式的请求。
HTTPS -> HTTP	将客户端到全站加速节点的请求强制301重定向为HTTP方式。
HTTP -> HTTPS	将客户端到全站加速节点的请求强制301重定向为HTTPS方式，以确保访问安全。

7. 单击**确定**，完成配置。

9.7. 配置TLS版本控制

阿里云全站加速提供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，低版本的TLS协议将提供对老版本浏览器的支持，但是协议的安全性相对更差一些，高版本的TLS协议将提供更高的安全性，但是对老版本浏览器的兼容性相对差一些。通过本文，您可以了解TLS的概念、使用场景和版本配置方法。

TLS版本说明

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，就是更安全的HTTP，运行在HTTP层之下，TCP层之上，为HTTP层提供数据加解密服务。

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+
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+

操作步骤

执行操作前，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** 默认开启TLSv1.0、TLSv1.1和TLSv1.2版本。

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。

推荐配置

场景	配置
兼容老客户同时对安全协议没那么高要求。	开启TLSv1.0、TLSv1.1和TLSv1.2版本。
对浏览器安全协议要求非常高（牺牲一部分用户体验换取更安全的协议）。	仅开启TLSv1.2版本。
尝鲜新技术	开启TLSv1.0、TLSv1.1、TLSv1.2和TLSv1.3版本。

9.8. 配置HSTS

通过开启HSTS（HTTP Strict Transport Security）功能，您可以强制客户端（例如：浏览器）使用HTTPS与全站加速节点创建连接，降低用户的第一次访问请求被恶意拦截的风险。

前提条件

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

背景信息

HSTS（HTTP Strict Transport Security，HTTP 严格传输安全），是一种网站用来声明他们只能使用安全连接（HTTPS）访问的方法。网站可通过声明HSTS，来强制客户端（如浏览器）只能使用HTTPS与服务器连接，拒绝所有的HTTP连接并阻止用户接受不安全的SSL证书，降低第一次访问请求被拦截的风险。

例如：未开启HSTS的情况下，当您的域名在全站加速上开启HTTPS安全加速时，在浏览器输入HTTP协议开头的URL链接，用户请求访问到全站加速节点上的时候，在配置了HTTP协议跳转HTTPS协议的情况下，全站加速节点会将该HTTP请求301或302重定向到HTTPS，在用户的首次请求以HTTP协议访问全站加速节点的过程中，HTTP请求可能被恶意拦截或者篡改，存在安全隐患。开启了HSTS以后，客户端只能使用HTTPS协议访问全站加速节点，这样就可以杜绝这类隐患。

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

参数	说明
max-age	HSTS Header的过期时间，单位为秒。
includeSubDomains	可选参数。如果包含这个参数，说明该域名及其所有子域名均开启HSTS。
preload	可选参数。当您申请将域名加入到浏览器内置列表时需要使用preload列表。

约束限制

- HSTS生效前，可以通过配置强制跳转功能实现在用户首次请求使用HTTP协议访问的情况下，能够通过301重定向的方式让客户端使用HTTPS协议发起访问。
- 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，打开**HSTS**开关，同时配置**过期时间**和**包含子域名**。
   - 过期时间：HSTS响应头在浏览器的缓存时间，建议填入60天，可填时间范围为0~730天。
   - 包含子域名：请谨慎开启，开启前，请确保该加速所有子域名都已开启HTTPS，否则会导致子域名自动跳转到HTTPS后无法访问。

6. 单击**确定**。

9.9. 配置国密HTTPS

阿里云为您提供更安全的国密HTTPS功能，通过本文您可以了解如何开通国密HTTPS。

前提条件

- 已在SSL证书控制台上购买并部署国密证书，具体方法请参见步骤。

  > **说明** 国密证书要单独购买，且必须在SSL证书产品购买，不支持自定义国密证书上传。

- 已配置HTTPS证书，具体操作请参见配置HTTPS证书。

背景信息

- 国密HTTPS是指支持SM2（椭圆曲线公钥密码算法）国产密码算法和国密安全协议，使用国密算法实现高强度SSL加密连接及服务器身份认证，支持国密浏览器。
- 阿里云全站加速支持SM2（椭圆曲线公钥密码算法）和SM3（杂凑算法）标准，提供更加安全的HTTPS传输协议（即国密HTTPS加密能力）。
- 支持的加密算法套件（验证国密算法时配置）：ECC-SM2-WITH-SM4-SM3和ECDHE-SM2-WITH-SM4-SM3。
- 国密算法HTTPS仅支持Linux系统（如果您使用Alios系统，需要部署Babassl）。

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏**全站分发服务**区域，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**国密HTTPS**区域，打开**国密HTTPS**开关。
6. （可选）如果提示**无可用云盾SSL国密证书**，单击**去购买和配置证书**完成相关操作：
   i. 购买证书：SSL证书控制台。
   ii. 上传证书：上传证书。
   iii. 部署证书：部署证书到阿里云产品。

7. 如果系统检测到有可用证书，选择证书，单击**确定**开启国密HTTPS。

8. （可选）如果您想关闭**国密HTTPS**功能，在**国密HTTPS**区域，关闭**国密HTTPS**开关即可。

相关API

API	功能说明
SetDcdnDomainSMCertificate	设置指定域名下是否启用国密证书功能。
DescribeDcdnSMCertificateDetail	获取国密证书的详细信息。
DescribeDcdnSMCertificateList	获取指定加速域名下国密证书列表信息。

9.10. 配置客户端证书认证

默认情况，HTTPS证书仅支持客户端单向验证服务器的安全性。阿里云全站加速支持客户端证书认证，通过自定义的CA证书实现服务器对客户端进行身份验证，从而实现双向认证，加强网站通信的安全性。本文为您介绍如何开启和配置客户端证书认证。

前提条件

- 您已开启并配置HTTPS证书功能，请参见配置HTTPS证书。
- 您已经自行签发一份**客户端CA证书**。

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. 打开**客户端证书认证**并输入自行签发的**客户端CA证书**。

   打开**客户端证书认证**。

输入自行签发的**客户端CA证书**。

6. 单击**确定**。
   开启**客户端证书认证**后，客户端以HTTPS请求访问资源时，全站加速会验证客户端证书有效性，验证成功，通过请求；验证失败，则拒绝访问。

10.访问控制

10.1. 概述

您可以通过设置Referer防盗链、URL鉴权、IP黑白名单和User-Agent黑白名单来实现对访客身份的识别和过滤，从而限制访问全站加速资源的用户，提升全站加速的安全性。
您可以通过全站加速的访问控制功能，对域名执行如下操作。

功能	说明
配置Referer防盗链	您可以通过配置访问请求来源的域名（即Referer黑名单和白名单），实现对访客身份的识别和过滤，限制访问全站加速资源的用户，禁止其他网站引用您的资源链接。
配置URL鉴权	URL鉴权是指用户按照指定的签名方式对于特定的URL增加鉴权认证，您可以通过自行配置校验鉴权URL中的加密串和时间戳，保护用户站点的资源不被非法站点下载盗用。URL鉴权比Referer防盗链安全性更高，适合于安全密级较高的文件。
配置IP黑白名单	您可以通过配置访问请求来源的IP地址（即IP黑名单和白名单），来实现对访客身份的识别和过滤，限制访问全站加速资源的用户，防止恶意IP盗刷、攻击等问题。
配置User-Agent黑白名单	User-Agent是访问请求客户端的标识，当您想指定访问的客户端时，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，保证用户只从您允许的客户端访问。

10.2. 配置Referer防盗链

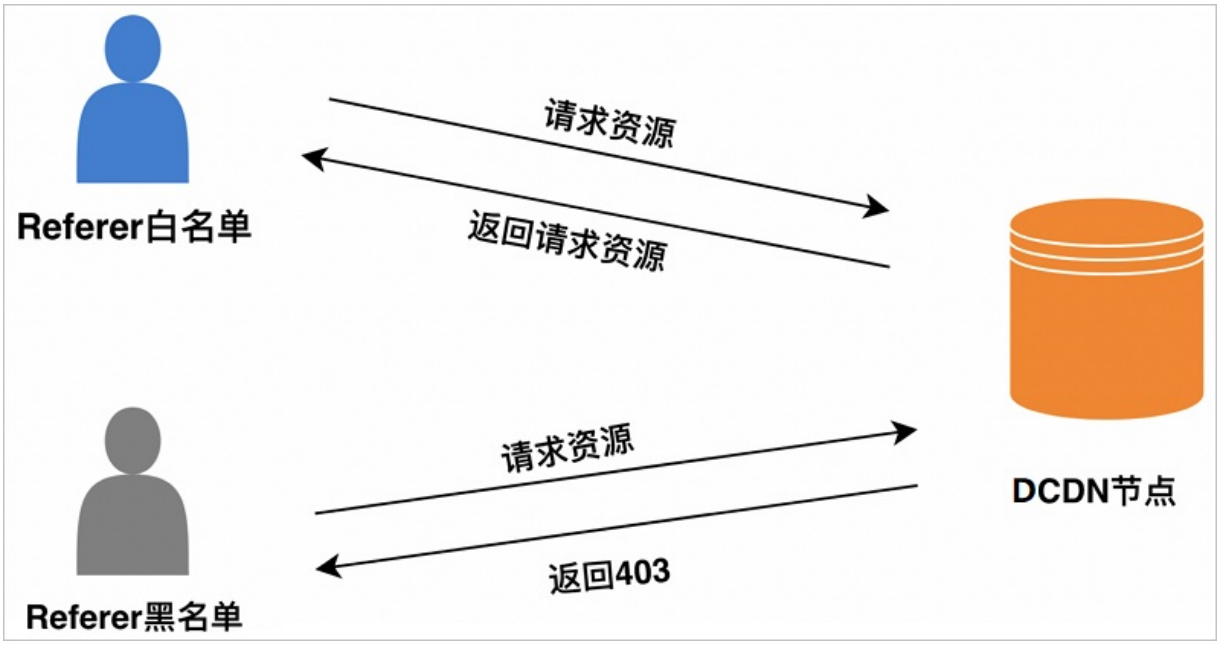
Referer防盗链，是基于HTTP请求头中Referer字段（例如，Referer黑白名单）来设置访问控制规则，实现对访客的身份识别和过滤，防止网站资源被非法盗用。本文介绍如何配置Referer防盗链。

背景信息

> **注意**
>
> - 该功能默认不启用。
> - 将某个域名添加到Referer黑名单或白名单后，全站加速会默认将该域名的泛域名加入对应的规则名单。例如，如果您填写 `aliyundoc.com` ，则最终配置生效的是 `*.aliyundoc.com` ，即所有子级域名都会生效。

Referer是HTTP请求头的一部分，携带了HTTP请求的来源地址信息（协议+域名+查询参数），可用于识别请求来源。

配置Referer黑白名单后，全站加速会根据名单识别请求身份，允许或拒绝访问请求。允许访问请求，全站加速会返回资源链接；拒绝访问请求，全站加速会返回403响应码。



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**访问控制**。
5. 在**Referer防盗链**页签，打开**Referer防盗链**开关。
6. 根据业务需求，设置Referer**黑名单**或**白名单**。

参数	说明
Referer类型	◦ **黑名单** 黑名单内的域名均无法访问当前的资源。 ◦ **白名单** 只有白名单内的域名能访问当前资源，白名单以外的域名均无法访问当前的资源。 **说明** 黑名单和白名单互斥，同一时间您只能选择其中一种方式。
规则	◦ 支持添加多个Referer名单，使用回车符进行分隔。 ◦ 支持使用星号（*）作为通配符。例如，配置 `*.developer.aliyundoc.com` ，可以匹配到 `image.developer.aliyundoc.com` 或 `video.developer.aliyundoc.com` 等。
允许通过浏览器地址栏直接访问资源URL	当选中该选项时，无论配置的是Referer黑名单还是白名单，请求Referer字段为空或无Referer字段（例如浏览器请求），全站加速节点都将允许用户访问当前的资源。

7. 单击**确定**，完成配置。

10.3. URL鉴权配置

10.3.1. 配置URL鉴权

在全站加速分发的内容默认为公开资源，用户拿到URL后均可访问，为防止站点资源被恶意下载盗用，除了通过Referer防盗链、IP黑白名单等防控方式，您还可以采用URL鉴权，自行配置校验鉴权URL中的加密串和时间戳，更安全有效地保护源站资源。本文主要介绍鉴权URL的逻辑、开启或关闭鉴权、以及验证方法。

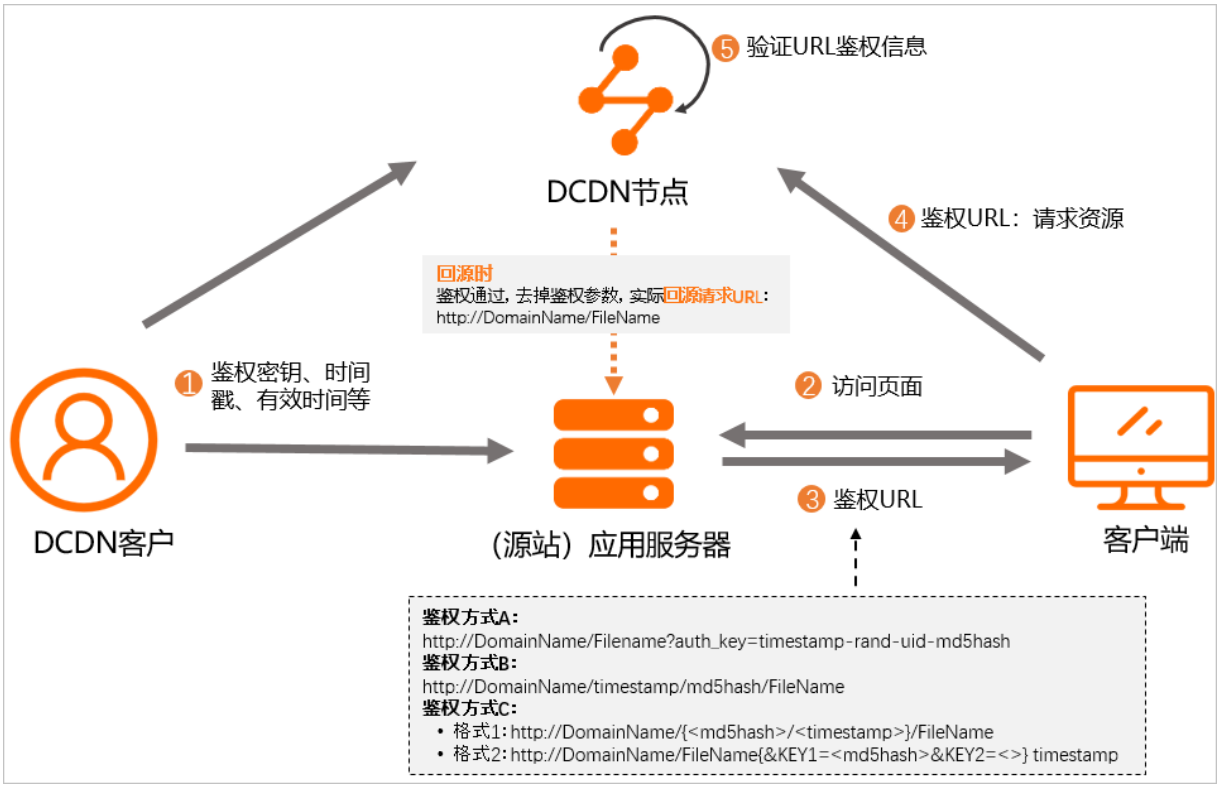
您可以通过以下内容了解和使用URL鉴权：

- 鉴权逻辑
- 配置鉴权URL并开启鉴权
- 验证鉴权URL正确性
- 关闭URL鉴权

鉴权逻辑

URL鉴权功能通过阿里云全站加速节点与客户资源站点配合，形成了更为安全可靠的源站资源防盗方法。主要由以下几个部分配合：

- 源站应用服务器：根据鉴权URL生成规则（包括鉴权算法、密钥）生成鉴权URL返回给客户端。
- 客户端：发起资源请求，并发送鉴权URL给全站节点进行验证。
- 全站加速节点：对鉴权URL中的鉴权信息（鉴权字符串、时间戳等）进行验证。



1. 全站加速客户在源站应用服务器配置鉴权URL的生成规则（包括鉴权算法和密钥）。
   假设鉴权URL为：`http://DomainName/timestamp/md5hash/FileName`。
2. 客户端访问源站应用的页面时，源站应用服务器将会按照鉴权URL的生成规则生成鉴权URL，并且把鉴权URL包含在应用页面上返回给客户端（图中②和③）。
3. 客户端使用鉴权URL向全站加速节点发起资源请求（图中④）。
4. 全站加速节点对鉴权URL中的鉴权信息（包括鉴权字符串、时间戳等）进行验证，判断请求的合法性（图中⑤）。
   - **鉴权失败，拒绝访问请求。**

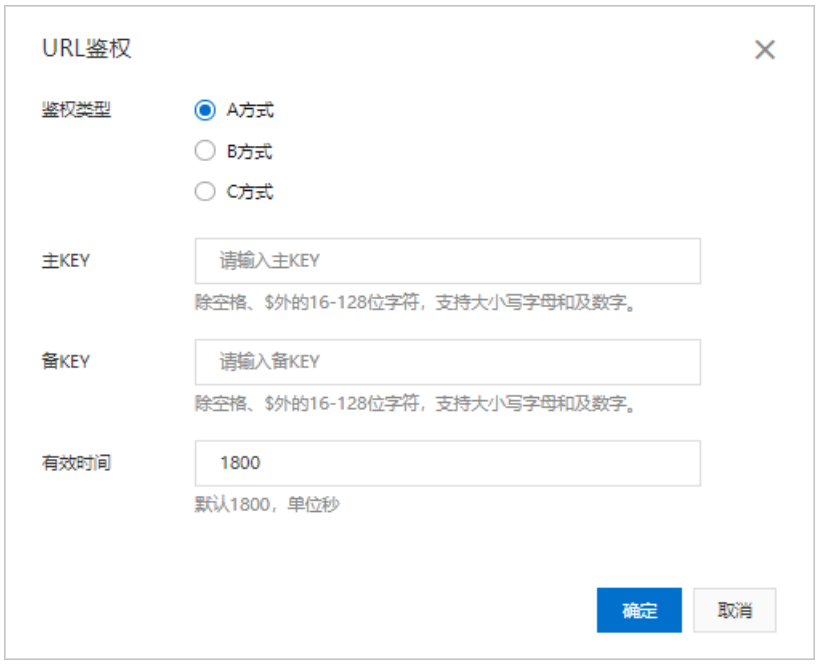
- **鉴权通过，正常响应合法请求。**

> **说明**
>
> - 若全站加速节点没有缓存资源，全站加速节点回源前，会去掉鉴权URL中的鉴权参数，将鉴权URL还原为原始URL（例如：`http://DomainName/FileName`），再使用原始URL生成缓存key或者发起回源请求。
> - 您的请求URL经过全站加速鉴权后，URL中的特殊字符，例如`=`、`+`等会被转义。

配置鉴权URL并开启鉴权

> **注意**
>
> - 请确保您已经在您的源站应用服务器配置了鉴权URL的生成规则（包括鉴权算法、密钥）。
> - 全站加速配置的URL鉴权逻辑必须与您的源站应用服务器的URL鉴权逻辑保持一致。

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**访问控制**。
5. 单击**URL鉴权**页签。
6. 打开**鉴权URL设置**开关。
7. 在**URL鉴权**对话框，根据界面提示，配置URL鉴权信息。



参数	说明

参数	说明
鉴权类型	阿里云全站加速提供了3种鉴权签名计算方式。您可以根据访问加密URL格式，选择合适的鉴权方式，实现对源站资源的有效保护。URL鉴权类型如下： ○ 鉴权方式A说明 ○ 鉴权方式B说明 ○ 鉴权方式C说明 **说明** 如果URL鉴权错误，会返回403报错，具体如下： ○ MD5计算类错误 例如：`X-Tengine-Error:denied by req auth: invalid md5hash=de7bfdc915ced05e17380a149bd760be` ○ 时间类报错 例如：`X-Tengine-Error:denied by req auth: expired timestamp=1439469547`
主KEY	输入鉴权方式对应的主用密码。
备KEY	输入鉴权方式对应的备用密码。
有效时间	全站加速配置的鉴权URL有效时间，用户可在（timestamp+全站加速上鉴权URL有效时间）时间区间内访问全站加速，超出该区间，鉴权失效。 ○ 单位：秒 ○ 取值范围：1~31536000 ○ 默认值：1800（30分钟） ○ 示例：例如签算服务器生成鉴权URL的时间（timestamp）为2020-08-15 15:00:00（UTC+8），全站加速上鉴权URL有效时长为1800秒，则鉴权URL失效时间为2020-08-15 15:30:00（UTC+8）。

8. 单击**确定**。

验证鉴权URL正确性

为保证服务器正确实现了鉴权逻辑，配置鉴权URL后，建议您在全站加速控制台生成对应的鉴权URL，校验鉴权URL的正确性。

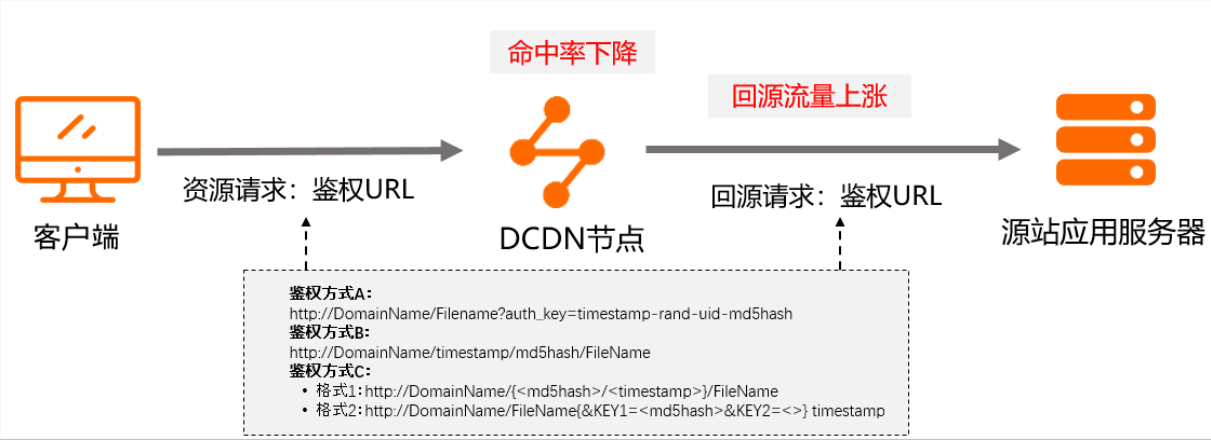
1. 在**生成鉴权URL**区域，配置**原始URL**和鉴权信息。

参数	说明
原始URL	输入完整的原始URL地址，例如：`https://www.aliyun.com`。
鉴权类型	按照您在配置鉴权URL并开启鉴权的配置，选择URL鉴权类型。
鉴权KEY	按照您在配置鉴权URL并开启鉴权的配置，输入您配置的**主KEY**或**备KEY**。
有效时间	按照您在配置鉴权URL并开启鉴权的配置，输入URL鉴权的有效时长，单位为秒。

2. 单击**开始生成**，即可获得**鉴权URL**和Timestamp。

关闭URL鉴权

注意 如果全站加速节点上的URL鉴权功能已经关闭了，但是客户端发起的请求URL里面依然携带鉴权参数的话，就会导致全站加速无法把客户端发起的请求URL（带鉴权参数）还原为原始URL，最终所有请求都无法命中缓存，均会透传回源站，导致源站的流量大涨，同时也会增加源站的流量费用。因此，如果您需要停止使用URL鉴权，需同时关闭源站和全站加速的URL鉴权功能。



1. 在全站加速控制台的鉴权URL设置区域，关闭URL鉴权开关。
2. 在您的应用服务器中去掉请求URL的鉴权参数。

10.3.2. 鉴权方式A说明

URL鉴权功能主要用于保护用户站点资源不被非法站点下载盗用。阿里云全站加速为您提供了三种鉴权方式，本文为您详细介绍鉴权方式A的原理和示例说明。

原理说明

- **鉴权方式A加密URL构成**

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

- **鉴权字段说明**

字段	描述
DomainName	全站加速站点的域名。
Filename	实际回源访问的URL，鉴权时Filename需以正斜线（/）开头。
auth_key	您设定的鉴权密钥。
timestamp	签算服务器生成鉴权URL的时间，与有效时间共同控制鉴权URL的失效时间。时间点取自签算服务器的Unix时间戳（Unix时间戳是从UTC时间1970年01月01日00时00分00秒到现在的总秒数，是十进制的整型正数，固定长度为10，与时区无关）。 **说明** 多数情况下，鉴权URL的有效时长为全站加速配置的有效时间。有时在签算增加鉴权URL的有效时长的，此时，timestamp=签算服务器上的Unix时间戳+签算服务器上加的有效时长；鉴权URL实际有效时长=timestamp+全站加速配置的鉴权URL有效时间。
rand	随机数。建议使用UUID，不能包含短划线（-），例如：477b3bbc253f467b8def6711128c7bec。
uid	用户ID，暂未使用，设置成0即可。

字段	描述
md5hash	通过MD5算法计算出的字符串，由数字0~9和小写英文字母a~z混合组成，固定长度为32。`md5hash`的值通过以下字符串计算得到。 `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） `md5hash = md5sum(sstring)`

- **鉴权逻辑说明**
  全站加速服务器接到资源访问请求后，判断最终生成鉴权URL请求中的timestamp+有效时间是否小于当前时间。
  - 如果timestamp+有效时间小于当前时间，服务器判定过期失效，并返回HTTP 403错误。
  - 如果timestamp+有效时间大于当前时间，则以`sstring`方式构造出一个字符串（参考表格中`sstring`构造方式），然后使用MD5算法算出`md5hash`的值，再将计算出的`md5hash`值与用户访问请求中携带的`md5hash`的值进行比对。
    - 结果一致，鉴权通过，返回资源请求。

      说明 当鉴权通过时，会去掉URL中与鉴权相关的那部分参数，可以提高缓存命中率，减少回源流量：
      - 实际生成缓存key的URL格式：`http://DomainName/FileName`
      - 实际回源的URL格式：`http://DomainName/FileName`
    - 结果不一致，鉴权失败，返回HTTP 403错误。

示例说明

通过以下示例说明，您可以准确理解鉴权方式A的实现方式。

- **示例条件**
  - 回源请求对象：

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

    说明 如果您的回源请求对象中有中文汉字，请先对其进行URL转码（即Encode），再进行鉴权URL的拼接。
  - 设置密钥为：aliyuncdnexp1234。
  - 签算服务器生成鉴权URL的时间：2015年10月10日08:00:00（UTC+8），转换为十进制的整形数值为1444435200。
- **拼接流程**
  i. 全站加速服务器构造出一个用于计算`md5hash`的签名字符串。

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

  ii. 根据该签名字符串，全站加速服务器会计算出`md5hash`。

```
md5hash = md5sum("/video/standard/1K.html-1444435200-0-0-aliyuncdnexp1234") = 80cd3862d699b7118eed99103f2a3a4f
```

iii. 生成鉴权URL。

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

当使用客户端提供的加密URL进行访问时，如果全站加速服务器计算出来的 `md5hash` 值与访问请求中带的 `md5hash` 值相同，都为*80cd3862d699b7118eed99103f2a3a4f*，则鉴权通过，反之鉴权失败。

10.3.3. 鉴权方式B说明

URL鉴权功能主要用于保护用户站点资源不被非法站点下载盗用。阿里云全站加速为您提供了三种鉴权方式，本文为您详细介绍鉴权方式B的原理和示例说明。

原理说明

- **鉴权方式B加密URL构成**

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

- **鉴权字段说明**

字段	描述
DomainName	全站加速站点的域名。
timestamp	签算服务器生成鉴权URL的时间，与**有效时间**共同控制鉴权URL的失效时间。时间点取自签算服务器的“UTC+8”时间，格式为：YYYYMMDDHHMM。 **说明** 多数情况下，鉴权URL的有效时长为全站加速配置的有效时间。有时在签算增加鉴权URL的有效时长的，此时，timestamp=签算服务器上的Unix时间戳+签算服务器上加的有效时长；鉴权URL实际有效时长=timestamp+全站加速配置的鉴权URL有效时间。
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。
FileName	实际回源访问的URL，鉴权时Filename需以正斜线（/）开头。

- **鉴权逻辑说明**
  全站加速服务器接到资源访问请求后，判断最终生成鉴权URL请求中的timestamp+有效时间是否小于当前时间。
  - 如果timestamp+有效时间小于当前时间，服务器判定过期失效，并返回HTTP 403错误。

- 如果timestamp+有效时间大于当前时间，则以 `sstring` 方式构造出一个字符串，然后使用MD5算法算出 `md5hash` 的值，再将计算出的 `md5hash` 值与用户访问请求中携带的 `md5hash` 的值进行比对。
  - 结果一致，鉴权通过，返回资源请求。

    > **说明** 当鉴权通过时，会去掉URL中与鉴权相关的那部分参数，可以提高缓存命中率，减少回源流量：
    > - 实际生成缓存key的URL格式： `http://DomainName/FileName`
    > - 实际回源的URL格式： `http://DomainName/FileName`

  - 结果不一致，鉴权失败，返回HTTP 403错误。

示例说明

通过以下示例说明，您可以准确理解鉴权方式B的实现方式。

- **示例条件**
  - 回源请求对象。

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

    > **说明** 如果您的回源请求对象中有中文汉字，请先对其进行URL转码（即Encode），再进行鉴权URL的拼接。

  - 设置密钥为：aliyuncdnexp1234。
  - 签算服务器生成鉴权URL的时间： 201508150800。
- **拼接流程**
  i. 全站加速服务器构造一个用于计算 `md5hash` 的签名字符串。

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

  ii. 根据该签名字符串，全站加速服务器会计算出 `md5hash` 。

  ```
  md5hash = md5sum("aliyuncdnexp1234201508150800/4/44/44c0909bcfc20a01afaf256ca99a8b8b.mp3") = 9044548ef1527deadafa49a890a377f0
  ```

  iii. 生成鉴权URL。

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

当使用客户端提供的加密URL进行访问时，如果全站加速服务器计算出来的 `md5hash` 值与访问请求中带的 `md5hash` 值相同，都为*9044548ef1527deadafa49a890a377f0*，则鉴权通过；反之鉴权失败。

10.3.4. 鉴权方式C说明

URL鉴权功能主要用于保护用户站点资源不被非法站点下载或盗用。阿里云全站加速为您提供了三种鉴权方式，本文为您详细介绍鉴权方式C的原理和示例说明。

原理说明

- **鉴权方式C加密URL构成**
  - 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。

- **鉴权字段说明**

字段	描述
DomainName	全站加速站点的域名。
FileName	实际回源访问的URL，鉴权时Filename需以正斜线（/）开头。
timestamp	签算服务器生成鉴权URL的时间，与有效时间共同控制鉴权URL的失效时间。时间点取自签算服务器的Unix时间戳（Unix时间戳是从UTC时间1970年01月01日00时00分00秒到现在的总秒数，是十进制的整型正数，固定长度为10，与时区无关），以十六进制形式表示。 **说明** 多数情况下，鉴权URL的有效时长为全站加速配置的有效时间。有时在签算增加鉴权URL的有效时长的，此时，timestamp=签算服务器上的Unix时间戳+签算服务器上加的有效时长；鉴权URL实际有效时长=timestamp+全站加速配置的鉴权URL有效时间。
md5hash	通过MD5算法计算出的字符串，由数字0~9和小写英文字母a~z混合组成，固定长度32。

- **鉴权逻辑说明**
  全站加速服务器接到资源访问请求后，判断最终生成鉴权URL请求中的timestamp+有效时间是否小于当前时间。
  - 如果timestamp+有效时间小于当前时间，服务器判定过期失效，并返回HTTP 403错误。
  - 如果timestamp+有效时间大于当前时间，则以 `sstring` 方式构造出一个字符串，然后使用MD5算法算出 `md5hash` 的值，再将计算出的 `md5hash` 值与用户访问请求中携带的 `md5hash` 的值进行比对。
    - 结果一致，鉴权通过，返回资源请求。

      > **说明** 当鉴权通过时，会去掉URL中与鉴权相关的那部分参数，可以提高缓存命中率，减少回源流量：
      > - 格式1和格式2，实际生成缓存key的URL格式：`http://DomainName/FileName`
      > - 格式1和格式2，实际回源的URL格式：`http://DomainName/FileName`

    - 结果不一致，鉴权失败，返回HTTP 403错误。

示例说明

通过以下示例说明，您可以准确理解鉴权方式C的实现方式。

- **示例条件**
  - 回源请求对象：

    ```
    http://dcdn.example.com/test.flv
    ```

    > **说明** 如果您的回源请求对象中有中文汉字，请先对其进行URL转码（即Encode），再进行鉴权URL的拼接。

  - PrivateKey取值：`aliyuncdnexp1234`。
  - timestamp取值：`55CE8100`。
- **拼接流程**

  i. 根据该签名字符串，全站加速服务器会计算出`md5hash`。

  ```
  md5hash = md5sum(aliyuncdnexp1234/test.flv55CE8100) = a37fa50a5fb8f71214b1e7c95ec7a1bd
  ```

  ii. 生成鉴权URL。

  - 格式一：

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

  - 格式二：

    ```
    http://dcdn.example.com/test.flv?KEY1=a37fa50a5fb8f71214b1e7c95ec7a1bd&KEY2=55CE8100
    ```

当使用客户端提供的加密URL进行访问时，如果全站加速服务器计算出来的`md5hash`值与访问请求中带的`md5hash`值相同，都为*a37fa50a5fb8f71214b1e7c95ec7a1bd*，则鉴权通过，反之鉴权失败。

10.4. 配置IP黑白名单

通过识别客户端IP来过滤用户请求，拦截特定IP的访问或者允许特定IP的访问，可以用来解决恶意IP盗刷、攻击等问题。本文介绍如何配置IP黑白名单。

注意事项

- 该功能默认关闭，IP黑名单与IP白名单二选一，不可同时配置。
- 配置IP黑名单后，黑名单中IP的请求仍可访问到全站加速节点，但会被全站加速节点拒绝并返回403状态码，全站加速日志中仍会记录黑名单中这些IP的请求记录。
- 由于IP黑白名单功能采用的是七层HTTP协议的IP识别技术，因此在恶意请求被全站加速节点拦截的同时，会产生少量的流量费用，如果客户端使用HTTPS协议访问，还会产生HTTPS请求数费用（因为拦截恶意IP的时候，也同时消耗了全站加速节点的处理资源）。

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**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**访问控制**。
5. 单击右侧的**IP黑/白名单**页签。

6. 打开**IP黑/白名单**开关，根据界面提示，配置IP的**黑名单**或**白名单**。

参数	说明
名单类型	IP名单类型如下： ○ **黑名单** 黑名单内的IP无法访问加速域名下的所有资源。 ○ **白名单** 只有白名单内的IP能访问加速域名下的资源，白名单以外的IP均无法访问。
规则	输入IP段（不可重复，例如：192.0.2.1/24）或IP地址（例如192.168.0.1）。支持IPv6地址、IPv4地址，最多配置100个IP地址，配置多个IP时使用回车符分隔。 IPv6：IP黑名单和白名单均支持IPv6地址（地址中的字母仅支持大写字母）。例如：2001:DB8:0:23:8:800:200C:****或2001:0DB8:0000:0023:0008:0800:200C:****。IPv6地址不支持缩写格式，例如：不支持2001:0DB8::0008:0800:200C:****。

7. 单击**确定**，完成配置。

配置示例

- **白名单**
  规则：192.0.2.1/24
  结果：只有客户端IP在192.0.2.1~192.0.2.254地址范围（包含192.0.2.1和192.0.2.254）时，才能访问该加速域名下的资源。
- **黑名单**
  规则：192.168.0.1
  结果：当客户端IP为192.168.0.1时，禁止访问该加速域名下的所有资源。

10.5. 配置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，从而限制访问全站加速资源的用户，提升全站加速的安全性。通过本文您可以了解User-Agent黑/白名单的配置方法。

背景信息

User-Agent是HTTP请求头的一部分，包含用户访问时所使用的操作系统及版本、浏览器类型及版本等标识信息。

配置User-Agent黑白名单后，用户请求资源时，全站加速将获取用户请求时HTTP请求头中的User-Agent字段，同配置中的黑/白名单进行匹配：

- **User-Agent黑名单**：若HTTP请求头中的User-Agent字段命中黑名单，用户将无法访问所请求的资源，并返回403状态码。
- **User-Agent白名单**：只有HTTP请求头中的User-Agent字段命中白名单，用户才能访问所请求的资源。

> **说明**
>
> - User-Agent黑名单与User-Agent白名单二选一，不可同时配置。
> - 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全站加速节点，但是会被全站加速节点拒绝并返回403，全站加速日志中仍会记录这些黑名单中的User-Agent字段请求记录。

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**访问控制**。
5. 单击右侧的**User-Agent黑/白名单**页签。
6. 打开**User-Agent黑/白名单**开关，根据界面提示，配置User-Agent的**黑名单**或**白名单**。

参数	说明
名单类型	User-Agent名单类型如下： ○ **黑名单** HTTP请求头中的User-Agent字段命中黑名单的情况下，用户将无法访问加速域名下的所有资源。 ○ **白名单** 只有HTTP请求头中的User-Agent字段命中白名单的情况下，用户才能访问加速域名下的资源。
规则	配置User-Agent字段时，用竖线（|）分割多个值，支持通配符号（*）。例如：`*curl*|*IE*|*chrome*|*firefox*`。 **说明** 您可以使用`^$`表示，黑白名单规则下允许HTTP请求Header中的User-Agent字段为空。 ○ 白名单下：规则中包含`^$`，表示如果请求中的User-Agent为空，则允许该请求。 ○ 黑名单下：规则中包含`^$`，表示如果请求中的User-Agent为空，则拒绝该请求。

7. 单击**确定**。

配置示例

- 示例一：黑名单

规则： `*IE*|*^$*`
结果说明：当请求来源于IE浏览器或请求头不携带User-Agent字段时，均不可访问所请求的资源。

- 示例二：白名单
  规则： `*IE*|*firefox*`
  结果说明：只有当请求来源于IE或者火狐浏览器时，才可以访问所请求的资源，其余请求均不可访问。

11.性能优化

11.1. 性能优化概述

性能优化指的是通过去除页面冗余内容、文件压缩、图像处理、过滤参数（提高缓存命中率）等方式来提升用户请求的响应速度和文件下载速度。
您可以通过性能优化功能，对域名执行如下操作。

功能	说明
页面优化	开启页面优化功能，全站加速会自动删除页面的冗余内容，例如HTML页面、内嵌JavaScript和CSS中的注释以及重复的空白符，可以有效去除页面的冗余信息，缩小文件体积，提高加速分发效率，同时也可以提升页面的可阅读性。
智能压缩	开启智能压缩功能，全站加速节点向您返回请求的资源时，会对文本文件进行Gzip压缩，可以有效缩小传输文件的大小，提升文件传输效率，减少带宽消耗。
Brotli压缩	开启Brotli压缩功能，全站加速节点向您返回请求的资源时，会对文本文件进行Brotli压缩，可以有效缩小传输文件的大小，提升文件传输效率，减少带宽消耗。
图像处理	通过图像处理功能，全站加速可直接在回源节点对图片行处理和分发，可减轻源站压力，减少回源链路，节省回源流量。
过滤参数	当您的URL请求中携带 `?` 和*参数*时，全站加速节点在收到URL请求后，判断是否需要携带参数的URL返回源站。
拖拽播放	开启拖拽播放功能后，当播放视音频时，随意拖拽播放进度，而不影响视音频的播放效果。

11.2. 页面优化

开启页面优化功能，全站加速会自动删除页面的冗余内容，例如HTML页面、内嵌JavaScript和CSS中的注释以及重复的空白符，可以有效去除页面的冗余信息，缩小文件体积，提高加速分发效率，同时也可以提升页面的可阅读性。

注意事项

- 如果源站文件配置了MD5校验机制，请不要开启页面优化功能。
  开启页面优化功能，全站加速进行页面优化时，会改变文件的MD5值，导致优化后文件的MD5值和源站文件的MD5值不一致。
- 如果源站开启了Gzip压缩或Brotli压缩，全站加速的页面优化功能将会失效，全站加速会将源站压缩后的文件透传给客户端。
- 如果您同时开启了页面优化和压缩功能（智能压缩或者Brotli压缩），页面优化功能将会失效，全站加速只会对文件进行压缩。

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**性能优化**。
5. 在**页面优化**区域，您可以选择开启**HTML优化**、**CSS优化**或**JavaScript优化**。

> **说明** “HTML优化”这个开关是页面优化功能的总开关，如果仅打开“HTML优化”开关，则只会开启HTML优化功能；如果要开启CSS优化或JavaScript优化，需要先打开“HTML优化”开关，然后再打开“CSS优化”或者“JavaScript优化”开关，CSS优化或者JavaScript优化才会生效。

- 开启**HTML优化**：即可实现对HTML页面的优化。
- 开启**CSS优化**：即可实现对CSS的优化。
- 开启**JavaScript优化**：即可实现对JavaScript的优化。

相关API

BatchSetDcdnDomainConfigs

11.3. 智能压缩

开启智能压缩功能后，全站加速节点会对资源进行智能压缩后返回，缩小传输文件大小，提升文件传输效率，减少带宽消耗。

背景信息

- 压缩分为Gzip压缩和Brotli压缩，智能压缩功能主要针对Gzip压缩，Brotli压缩详情请参见Brotli压缩。
- 当源站文件的大小超过1 KB时，您可以使用智能压缩或Brotli压缩来压缩文件（即1 KB以下的文件不做压缩）。
- 智能压缩支持的文件类型有text/xml、text/plain、text/css、application/javascript、application/x-javascript、application/rss+xml、text/javascript、image/tiff、image/svg+xml、application/json、application/xml。
- 客户端请求携带请求头 `Accept-Encoding: gzip` ：客户端希望获取对应资源时进行Gzip压缩。
- 服务端响应携带响应头 `Content-Encoding: gzip` ：服务端响应的内容为Gzip压缩的资源。

注意事项

- 智能压缩（Gzip压缩）兼容所有浏览器，Brotli压缩不兼容较老版本的浏览器，您可以根据业务需要查询浏览器的兼容情况。
- 全站加速对静态文件进行压缩时，会改变文件的MD5值，如果源站文件配置了MD5校验机制，请关闭智能压缩和Brotli压缩功能。
- 源站开启了压缩功能，且服务端响应中携带了 `content_encoding` ，则全站加速的压缩功能将不再生效。
- 同时开启智能压缩和Brotli压缩，且客户端请求头 `Accept-Encoding` 同时携带 `br` 和 `gzip` 时，仅Brotli压缩生效。
- 如果您同时开启了页面优化和压缩功能（智能压缩或者Brotli压缩），页面优化功能将会失效，全站加速只会对文件进行压缩。
- 常见的图片文件类型（PNG、JPG、JPEG等）和视频文件类型（MP4、AVI、WMV等）已经做了内容的压缩处理，开启智能压缩或者Brotli压缩没有效果，建议您关闭智能压缩或者Brotli压缩功能。如果您需要进一

步降低图片文件的体积可以使用图像处理功能；如果您需要进一步降低视频文件的体积可以使用视频转码功能。

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**性能优化**。
5. 在**智能压缩**区域，打开**智能压缩**开关。

   成功开启智能压缩功能后，您可以对比查看原始请求收到的文件类型和开启智能压缩之后收到的文件类型，如果收到.gzip后缀的文件，说明文件已经被压缩了。

相关API

BatchSetDcdnDomainConfigs

11.4. Brotli压缩

Brotli是开源的一种新型压缩算法，Brotli压缩比智能压缩性能更好。开启Brotli压缩功能后，全站加速节点会对资源进行智能压缩后返回，缩小传输文件大小，提升文件传输效率，减少带宽消耗。

背景信息

- 压缩分为Gzip压缩和Brotli压缩，智能压缩功能主要针对Gzip压缩，智能压缩详情请参见智能压缩。
- 当源站文件的大小超过1 KB时，您可以使用智能压缩或Brotli压缩来压缩文件（即1 KB以下的文件不做压缩），Brotli压缩比智能压缩性能更好，性能提升约15%~25%。
- Brotli压缩支持的文件类型有text/xml、text/plain、text/css、application/javascript、application/x-javascript、application/rss+xml、text/javascript、image/tiff、image/svg+xml、application/json、application/xml。
- 服务端响应携带响应头`Content-Encoding: br`：服务端响应的内容是经过Brotli压缩后的资源。
- 客户端请求携带请求头`Accept-Encoding: br`：客户端希望获取对应资源时进行Brotli压缩。

注意事项

- 全站加速对静态文件进行压缩时，会改变文件的MD5值，如果源站文件配置了MD5校验机制，请关闭智能压缩功能。
- 源站开启了压缩功能，且服务端响应中携带了`content_encoding`，则全站加速的压缩功能将不再生效。
- 同时开启Brotli压缩和智能压缩，且客户端请求头`Accept-Encoding`同时携带`br`和`gzip`时，仅Brotli压缩生效。
- 如果您同时开启了页面优化和压缩功能（智能压缩或者Brotli压缩），页面优化功能将会失效，全站加速只会对文件进行压缩。
- Brotli压缩只兼容部分浏览器，您可以根据业务需要查询浏览器的兼容情况。
- 常见的图片文件类型（PNG、JPG、JPEG等）和视频文件类型（MP4、AVI、WMV等）已经做了内容的压缩处理，开启智能压缩或者Brotli压缩没有效果，建议您关闭压缩功能。如果您需要进一步减小图片文件的

体积可以使用图像处理功能，如果您需要进一步减小视频文件的体积可以使用视频转码功能。“图像处理”和“视频转码”都会影响文件清晰度。

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**性能优化**。
5. 在**Brotli压缩**区域，打开**Brotli压缩**开关，完成配置。

   成功开启Brotli压缩功能后，您可以对比查看原始请求收到的文件类型和开启智能压缩之后收到的文件类型，如果收到.br后缀的文件，说明文件已经被压缩了。

相关API

BatchSetDcdnDomainConfigs

11.5. 图像处理

11.5.1. 图像处理方法及优势

通过图像处理功能，全站加速可直接在回源节点对图片行处理和分发，可减轻源站压力，减少回源链路，节省回源流量。使用图像处理功能，您可以对全站加速上的原图进行缩放、裁剪、添加水印等操作，满足多种业务场景下的图片需求。阿里云CDN、全站加速和OSS的图片处理都是独立的功能，不能相互混用。

> **说明**
>
> - 图像处理功能处于内测阶段，您需提交工单申请开通。
> - 图像处理为付费服务，内测期间**暂不收费**，收费时间另行通知。

适用场景

使用图像处理功能前，您需要先在全站加速上添加加速域名，添加成功后才能开通图像处理功能。通过全站加速进行图片处理，所有的图片处理和缓存都通过全站加速节点完成，源站无感知。

下表为您列出了图像处理常见的适用场景，适用场景较多，不仅限于以下场景。

适用场景	说明
电商平台	• 多种样式处理满足多终端图片显示场景，图片编辑更加高效便捷。 • 可对商品图、图片评论等进行压缩，缩小图片质量，达到省流的目的。 • 支持添加水印，用于版权保护，具有品牌标识、宣传推广作用。
社交软件	• 简单、灵活的图片编辑方式满足社交图片标准处理的需求。 • 支持添加水印，保护个人信息不被盗用。

适用场景	说明
在线教育	• 简单、灵活的图片编辑方式满足在线教育课件图等标准处理的需求。 • 您可以根据不同场景需求使用不同压缩功能，平衡压缩收益与视觉体验。
素材网站	• 多种样式处理满足多终端图片显示场景，图片编辑更加高效便捷。 • 针对需要使用高清大图的素材网站及平台，您可以使用图片自动瘦身进行视觉无损压缩，在不损失视觉观感的情况下最大化压缩比，提升图片加载速度。

功能优势

- **更快分发**
  原图在回源节点被缓存后，边缘触发的多尺寸图片访问需求直接在回源节点进行处理和分发，减少回源链路，更快到达边缘。
- **减少源站压力**
  衍生图大量消耗源站的存储和计算能力，增加了源站的维护成本。通过全站加速进行图片处理，所有的图片处理和缓存都通过全站加速节点完成，您的源站无感知。
- **提升刷新预热效率**
  当原图失效后，处理后的目标图也会全部失效且无法访问，对图片进行处理可降低提交刷新预热的次数和回源的带宽，加速新图片的更新，避免原图和目标图访问失效问题。
- **边缘需求定制**
  通过图片处理参数对图片处理进行控制，可以根据不同的浏览器和客户端版本定制不同的图片处理需求，满足不同的业务能力。

使用限制

使用图像处理功能时有如下限制：

- 原图限制
  - 图片格式只支持JPEG、PNG、WebP、BMP、GIF、TIFF、JPEG 2000。
  - 原图大小不能超过10 MB。
  - 原图的宽×高不能超过16777216 px。

    > **说明** 若图片为GIF格式时，GIF图片的原图宽×高为所有帧相加之和，您可以使用ImageMagick等工具查看GIF图片的帧信息。

- 处理后的图片限制
  - 图片的宽×高不能超过16777216 px。
  - 转WebP格式时，图片的宽×高不能超过16777216 px，且宽和高单边均不能超过16,384 px。

图像处理操作方法

图像处理操作方法说明

全站加速支持边缘图片处理，处理的类型以参数形式传入。图片处理的请求参数为`image_01`，支持携带多个转换参数，例如`crop`、`rotate`等，多个转换参数用正斜线（/）分隔。全站加速将按图像处理转换参数的顺序处理图片，例如`image_01=resize,w_200/rotate,90`表示将图片先按比例缩放至宽200 px，再将图片旋转90°。

通过图片访问URL处理图片

您可以在图片的访问URL后添加相应的图片处理参数处理图片，具体如下：

- 格式：`http://example.com/image_01.jpg?image_process=action,param_value`
  - `example.com`：您的加速域名。
  - `image_01.jpg`：图片名称。
  - `image_01`：固定参数，标明使用图片处理参数对图片文件进行处理。
  - `action,param_value`：图像处理的操作（action）即转换参数、参数（param）和值（value），用于定义图片处理的方式。图像处理支持的转换参数，请参见图像处理转换参数。
- 示例：`http://example.com/image_01.jpg?image_process=resize,w_200/rotate,90`

图像处理转换参数

全站加速支持携带一个或多个转换参数处理图片，下表汇总了图片处理的转换参数，您可以根据实际需求，对全站加速上的原图进行处理。

图片处理功能	转换参数	说明
格式转换	format	转换图片格式。
质量转换	quality	调整图片的质量。
图片裁剪	crop	裁剪指定大小的图片。
图片缩放	resize	将图片缩放至指定大小。
图片旋转	• 图片自动旋转：auto-orient • 按指定方向旋转：rotate	将携带旋转参数的图片进行自适应旋转或按指定角度以顺时针方向旋转图片。
图片色彩	• 图片亮度：bright • 图片对比度：contrast • 图片锐化：sharpen	调整图片的亮度、对比度和清晰度。
水印管理	watermark	为图片添加图片水印或文字水印。
获取信息	info	获取图片信息，包括图片的长、宽、高、图片格式和图片质量等信息。

11.5.2. 格式转换

图片格式转换包含自适应WEBP和普通图片格式转换，您可以通过转换参数将全站加速上的图片转换为指定的图片格式。本文介绍图片格式转换所用到的参数及示例。

> **说明**
> - 图像处理功能处于内测阶段，您需提交工单申请开通。
> - 图像处理为付费服务，内测期间**暂不收费**，收费时间另行通知。

自适应WEBP

WEBP是一种支持有损压缩和无损压缩的图片文件格式。全站加速支持自适应WEBP，开启自适应WEBP，通过对请求头Accept的判断，如果请求头包含 `image/webp` ，则全站加速会将其他格式图片自动转换为WEBP格式进行访问。

> **注意** 开启该功能后，短时间内会导致命中率下降，过后会自动恢复正常，请勿在业务高峰期开启。

操作示例

下方的Accept内容仅作为示例，实际的Accept内容以真实情况为准。示例中Accept里包含了 `image/webp` ，表示支持自适应WEBP功能。

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
```

图片格式转换

参数说明

操作名称： `format`

下表列出了支持转换的图片格式。

支持转换的图片格式	说明
JPEG	将原图保存为JPG或JPEG格式。
PNG	将原图保存为PNG格式。
WEBP	将原图保存为WEBP格式。
BMP	将原图保存为BMP格式。
GIF	将原图保存为GIF格式。 **说明** GIF有动图效果，若转换为其他图片格式，则只保留静图效果。
TIFF	将原图保存为TIFF格式。
JPEG 2000	将原图保存为JPEG 2000格式，图片后缀为JP2。

操作示例

```
image_process=format,bmp
```

11.5.3. 质量转换

图片质量转换包含图片自动瘦身、绝对质量转换和相对质量转换。质量转换是使用原图本身的格式对图片进行压缩，您可以通过质量转换参数，修改全站加速上原图的质量。

> 说明
> - 图像处理功能处于内测阶段，您需提交工单申请开通。
> - 图像处理为付费服务，内测期间**暂不收费**，收费时间另行通知。

图片自动瘦身

图片自动瘦身仅支持JPG和WebP格式，开启图片自动瘦身可以在不改变原图的宽×高和格式的前提下对图片进行压缩，对图片进行压缩，缩小图片质量，节省访问流量。

图片质量转换

参数说明

操作名称：`quality`

参数说明见下表。

参数	说明	取值范围
Q	图片的绝对质量。按绝对质量进行转换，转换成指定大小的质量，如果当前质量小于待转换的质量，则不转换。	0<Q<100，且Q必须是5的倍数，不在质量值范围内的其他值均不支持。 **说明** 质量值越大图片质量越高，图片越清晰；质量值越小图片质量越低，图片越不清晰，推荐设置为95。
q	图片的相对质量。按相对质量进行转换，根据当前图片的质量乘以待转换系数，得到最终要转换的图片质量。	0<q<100，且q必须是5的倍数，不在质量值范围内的其他值均不支持。 **说明** 质量值越大图片质量越高，图片越清晰；质量值越小图片质量越低，图片越不清晰，推荐设置为95。

操作示例

- 绝对质量转换：`example.com/image01.png?image_process=quality,Q_90`，如果当前质量是80，转换后质量仍为80。
- 相对质量转换：`example.com/image01.png?image_process=quality,q_90`，如果当前质量是80，转换后质量为72。

11.5.4. 图片裁剪

您可以通过图片裁剪参数，在原图上裁剪指定大小的图片。本文介绍图片裁剪所用到的参数及示例。

> 说明
> - 图像处理功能处于内测阶段，您需提交工单申请开通。
> - 图像处理为付费服务，内测期间**暂不收费**，收费时间另行通知。

参数说明

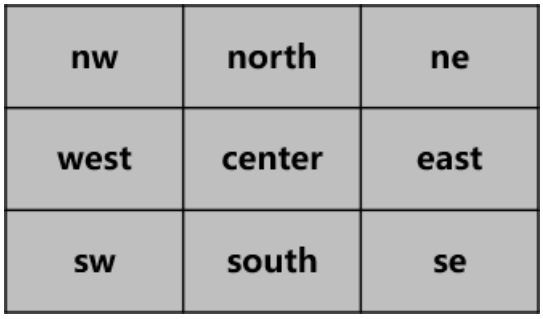
操作名称：`crop`

参数说明见下表。

> **说明** 当任意参数值为负数时，将不对图片进行任何处理直接返回原图。

参数	描述	取值范围
w	指定裁剪宽度。	默认值为0，宽×高不能超过16777216 px。
h	指定裁剪高度。	
x	指定裁剪起点横坐标（默认左上角为原点）。	
y	指定裁剪起点纵坐标（默认左上角为原点）。	
g	设置裁剪的原点位置。原点按照九宫格的形式分布，一共有九个位置可以设置，为每个九宫格的左上角顶点。	• nw：左上 • north：中上 • ne：右上 • west：左中 • center：中部 • east：右中 • sw：左下 • south：中下 • se：右下 详情请参见下方裁剪原点位置示意图。

裁剪原点位置示意图。



操作示例

下表列出了图片裁剪方式和示例。

图片裁剪方式	说明	示例
圆切	指定圆半径进行剪切，半径不超过原图的一半。	`example.com/image01.png?image_process=circle,200`

图片裁剪方式	说明	示例
九宫格切	设置原点位置，原点按九宫格分布。	`example.com/image01.png?image_process=crop,w_200,h_200,g_se`
指定X、Y轴剪切	按指定x、y、宽和高裁剪，以x和y为起点，裁剪宽×高大小的图片内容。	`example.com/image01.png?image_process=crop,x_10,y_10,w_400,h_200`
图片居中剪切	从图片居中部分裁剪指定宽和高的图片内容。	`example.com/image01.png?image_process=crop,mid,w_400,h_200`

11.5.5. 图片缩放

您可以通过图片缩放参数，调整原图的图片大小。本文介绍图片缩放所用到的参数及示例。

> **说明**
> - 图像处理功能处于内测阶段，您需提交工单申请开通。
> - 图像处理为付费服务，内测期间**暂不收费**，收费时间另行通知。

参数说明

操作名称：`resize`

参数说明见下表。

> **说明** 当任意参数值为负数时，将不对图片进行任何处理直接返回原图。

参数	说明	取值范围
w	指定目标缩放图的宽度。	默认值为0，宽×高不能超过16777216 px。
h	指定目标缩放图的高度。	
l	指定目标缩放图的最长边。	
s	指定目标缩放图的最短边。	
fw、fh	指定目标缩放图的宽高。	
p	按原图长宽比例进行缩放。	[0,100]

操作示例

下表列出了图片缩放方式和示例。

图片缩放方式	说明	示例
原图比例缩放	按原图长宽比例进行缩放。	`example.com/image01.png?image_process=resize,p_80`
按条件缩放	当图片大于等于1024000字节时，进行缩放，单位为Byte。 **说明** 这里的1024000为举例所用的示例值，实际取值需根据您的实际情况设置。	`example.com/image01.png?image_process=resize,l_200/threshold,1024000`
按长边固定自适应等比缩放	长边固定长度，短边自适应缩放。	`example.com/image01.png?image_process=resize,l_200`
按短边固定自适应等比缩放	短边固定长度，长边自适应缩放。	`example.com/image01.png?image_process=resize,s_200`
按宽固定自适应等比缩放	固定宽度，长度自适应。	`example.com/image01.png?image_process=resize,w_200`
按高固定自适应等比缩放	固定高度，宽边自适应。	`example.com/image01.png?image_process=resize,h_200`
指定宽高缩放	指定缩放的宽高。	`example.com/image01.png?image_process=resize,fw_200,fh_200`

11.5.6. 图片旋转

图片旋转包含图片自动旋转和按指定方向旋转。您可以通过图片旋转参数，将全站加速上的原图进行自动旋转或按指定方向旋转。本文介绍图片旋转所用到的参数及示例。

> 说明
> - 图像处理功能处于内测阶段，您需提交工单申请开通。
> - 图像处理为付费服务，内测期间**暂不收费**，收费时间另行通知。

图片自动旋转

某些手机拍摄出来的照片可能带有旋转参数，图片自动旋转只对带有旋转参数的图片生效。开启图片自动旋转，可自动调正图片，方便用户查看。

> **注意** 开启该功能后，短时间内会导致命中率下降，过后会自动恢复正常，请勿在业务高峰期开启。

操作名称：`auto-orient`

操作示例

```
image_01=auto-orient
```

指定旋转方向

指定旋转方向是指将图片按顺时针和指定的角度进行旋转，只支持90°、180°和270°三个旋转角度。

操作名称：`rotate`

操作示例

```
example.com/image01.png?image_process=rotate,180
```

11.5.7. 图片色彩

图片色彩包含图片的亮度、对比度和图片锐化。您可以通过亮度参数、对比度参数和锐化参数来调节全站加速上原图的亮度、对比度和清晰度。本文介绍图片色彩所用到的参数及示例。

> 说明
> - 图像处理功能处于内测阶段，您需提交工单申请开通。
> - 图像处理为付费服务，内测期间**暂不收费**，收费时间另行通知。

参数说明

图片亮度、对比度和图片锐化对应的操作名称如下：

- 图片亮度：`bright`
- 图片对比度：`contrast`
- 图片锐化：`sharpen`

操作示例

下表列出了图片色彩包含的操作方式和示例。

操作方式	说明	示例
图片亮度	设置图片的亮度，亮度值范围为[-100,100]。	`example.com/image01.png?image_process=bright,50`
图片对比度	设置图片的对比度，对比度值范围为[-100,100]。	`example.com/image01.png?image_process=contrast,50`
图片锐化	设置图片锐化，锐化值范围为[50,399]，推荐您使用50、100、150、200、250和300这六个锐化值。	`example.com/image01.png?image_process=sharpen,100`

11.5.8. 水印管理

全站加速支持图片水印和文字水印。您可以通过水印参数为图片文件添加图片水印和水印文字。本文为您介绍为图片添加水印时所用到的功能及参数。

> **说明**
> - 图像处理功能处于内测阶段，您需提交工单申请开通。
> - 图像处理为付费服务，内测期间**暂不收费**，收费时间另行通知。

图片水印

操作名称：`watermark`

下表列出了图片水印支持的功能及功能对应的参数。

> **说明**
> - 图片水印暂不支持缩放，水印图片原图不能超过1 MB。
> - 支持同时添加多个水印，且支持同时添加图片水印和文字水印，最多支持添加5个。

支持的功能	功能描述	参数	取值范围

支持的功能	功能描述	参数	取值范围
水印地址	指定可以访问的图片水印地址，水印地址可以公开访问，若有鉴权或权限设置，可能导致获取水印地址失败。 水印地址需进行Base64编码。详细信息，请参见水印编码。	image	Base64编码后的字符串。

操作示例

- 图片水印

```
example.com/image01.png?image_process=watermark,image_Base64编码后的图片请求,x_20,y_20,g_se
,t_70
```

- 文字和图片水印

```
example.com/image01.png?image_process=watermark,text_Base64编码后的文字内容,x_10,y_10,g_nw,
size_24,color_FF0000,t_70/watermark,image_Base64编码后的图片请求,x_20,y_20,g_se,t_70
```

文字水印

操作名称：`watermark`

下表列出了文字水印支持的功能及功能对应的参数。

> **说明** 支持同时添加多个水印，且支持同时添加图片水印和文字水印，最多支持添加5个。

支持的功能	功能描述	参数	取值范围
文字内容	指定文字水印的文字内容，文字内容需进行Base64编码。详细信息，请参见水印编码。	text	Base64编码后的字符串，最大长度不能超过60个字符。
文字字体	指定文字水印的字体，字体名称需进行Base64编码。详细信息，请参见水印编码。	type	共支持10种文字字体，字体及字体编码请参见文字字体。 **说明** 如果您使用的是10种文字字体之外的其他字体，系统会识别出您使用的是默认字体alihyaihei。
文字颜色	指定文字水印的文字颜色，参数值为RGB颜色值。	color	RGB颜色值，例如：000000表示黑色，FFFFFF表示白色。 默认值：000000（黑色）。
文字旋转	指定文字顺时针旋转角度。	rotate	支持按顺时针旋转90°、180°和270°。
文字铺满	指定是否将文字水印铺满原图。	fill	取值范围[0,1]，默认值为0。 • 0：表示不将文字水印铺满全图。 • 1：表示将文字水印铺满原图。

操作示例

- 文字水印

```
example.com/image01.png?image_process=watermark,text_Base64编码后的文字内容,type_YWxpaHlhaWhlaQ,x_10,y_10,g_se,size_24,color_FF0000,t_70,rotate_45,fill_0
```

- 文字和图片水印

```
example.com/image01.png?image_process=watermark,text_Base64编码后的文字内容,x_10,y_10,g_nw,size_24,color_FF0000,t_70/watermark,image_Base64编码后的图片请求,x_20,y_20,g_se,t_70
```

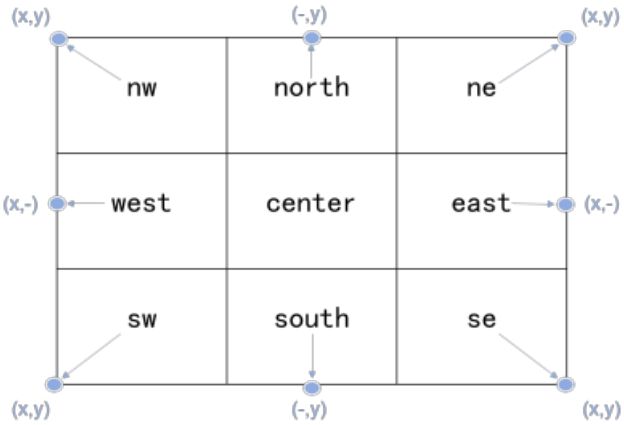
下表列出了文字水印支持的10种文字字体。

文字字体

文字字体	中文含义	编码值
alihyaihei	阿里汉仪智能黑体，默认字体	YWxpaHlhaWhlaQ
hysong	汉仪宋体	aHlzb25n
hyhei	汉仪黑体	aHloZWk
hyshuangxian	汉仪双线体	aHlzaHVhbmd4aWFu
fzltzhk	方正兰亭中黑	ZnpsdHpoaw
fzshengsks	方正盛世楷书	ZnpzaGVuZ3Nrcw
fzqusongjian	方正趣宋简体	ZnpxdXNvbmdqaWFu
zzgfxingyan	造字工房星岩	enpnZnhpbmd5YW4
comfortaa	Comfortaa	Y29tZm9ydGFh
notosans	NotoSans	bm90b3NhbnM

水印位置

图片水印和文字水印均可以按照九宫格定位、水印垂直边距和水印水平边距来设置水印的位置。九宫格定位、垂直边距和水平边距不仅可以调节水印在图片中的位置，当图片存在多重水印时，还可以调节水印在图中的布局。区域数值以及每个区域对应的基准点如下图所示。



参数	说明	取值范围
t	指定水印图片或水印文字的透明度。	[0,100] 默认值为100， 表示透明度100%（即不透明）。
g	指定水印在图片中的位置。	• nw：左上 • north：中上 • ne：右上 • west：左中 • center：中部 • east：右中 • sw：左下 • south：中下 • se：右下 详情请参见上方基准点图片。
x	指定水印的水平边距， 即距离图片边缘的水平距离。这个参数只有当水印位置是左上、左中、左下、右上、右中、右下才有意义。	[0,4096] 默认值为10 ，单位：px（像素）。
y	指定水印的垂直边距，即距离图片边缘的垂直距离。 这个参数只有当水印位置是左上、中上、右上、左下、中下、右下才有意义。	[0,4096] 默认值为10， 单位：px（像素）。

水印编码

添加水印时，文字水印的文字内容、文字字体和图片水印的水印地址需进行URL安全的Base64编码。编码方式如下：

1. 将内容编码成Base64。
   推荐使用URL-safe Baes64编码工具对文字水印的文字内容、文字字体和图片水印的水印地址进行编码。水印编码后的内容仅适合应用在水印操作的特定参数中，请勿将其用在签名字符串（Signature）的内容里。
2. 替换编码结果中的部分编码。
   - 将结果中的加号（+）替换成短划线（-）。
   - 将结果中的正斜线（/）替换成下划线（_）。
   - 将结果中尾部的等号（=）省略。

11.5.9. 获取信息

本文介绍如何获取处理后的图片信息，以及获取图片信息所用到的参数及示例。

参数说明

操作名称： `info`

返回的图片信息为JSON格式，返回的参数包括图片的长、宽、高、图片格式、图片质量和图片方向。

```
{
  "Length":1055089,
  "Width":1920,
  "Height":1080,
  "Quality":100,
  "Format":"JPEG",
  "Orientation":"UNDEFINED"}
```

操作示例

```
example.com/image01.png?image_process=info
```

11.6. 过滤参数

开启过滤参数功能后，回源获取资源时会去除URL请求中携带 ? 之后的参数，有效提高文件缓存命中率，减少回源次数，节省回源流量，同时提升分发效率。本文为您详细介绍配置过滤参数的方法。

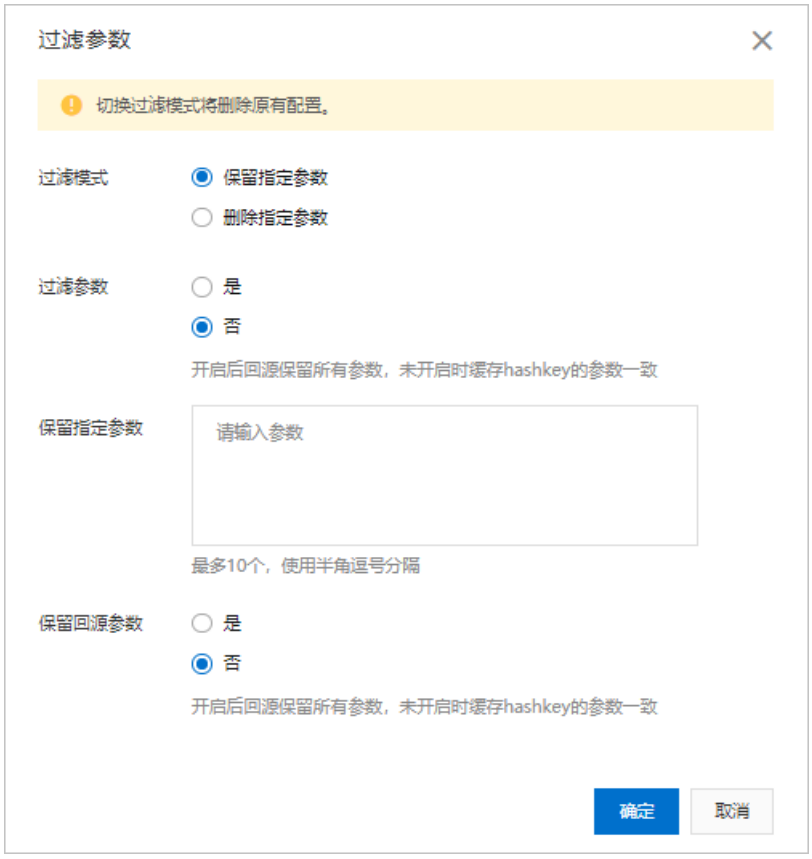
背景信息

- 开启过滤参数
  如果您的URL请求中携带 ? 和参数，例如： http://alibaba.com/content?a ，但是这些参数内容优先级不高，可以忽略参数浏览文件时，建议您开启过滤参数。开启过滤参数的作用是忽略URL请求中 ? 之后的参数，提高全站加速缓存的命中率。
  例如：第一次访问 http://example.aliyundoc.com/image_01.jpg ，全站加速没有缓存，直接回源访问数据；第二次访问 http://example.aliyundoc.com/image_01.jpg?test1 ，由于开启了过滤参数，所以 ? 后的参数无需匹配，即可命中全站加速缓存 http://example.aliyundoc.com/image_01.jpg。
- 关闭过滤参数
  如果您的URL请求中携带 ? 和参数，但是参数有重要含义，则建议您关闭过滤参数。关闭过滤参数后，访问URL需精确匹配 ? 之后的参数，提高请求的精确性。
  例如：第一次访问 http://example.aliyundoc.com/image_01.jpgg ，全站加速没有缓存，直接回源访问数据；第二次访问 http://example.aliyundoc.com/image_01.jpg?test1 ，由于关闭了过滤参数，所以 ? 后的参数需精确匹配，即无法响应全站加速缓存内容 http://example.aliyundoc.com/image_01.jpg ，需要重新回源获取 http://example.aliyundoc.com/image_01.jpg?test1 。

> **说明** URL鉴权功能的优先级高于过滤参数。由于鉴权方式A中的鉴权信息包含HTTP请求的参数部分，所以全站加速优先进行鉴权判断，鉴权通过后在全站加速节点缓存一份副本。配置URL鉴权的操作方法，请参见配置URL鉴权。

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**性能优化**。
5. 单击**过滤参数**区域的**修改配置**，如下图所示。



> **说明** 切换过滤模式将删除原有配置。

当您的**过滤模式**选择**保留指定参数**或者**删除指定参数**时，可参考如下表格完成设置。

过滤模式	参数	说明
	过滤参数	○ **是**：资源回源时会去除URL中 ? 之后的参数，提高文件缓存命中率。 > **说明** 如果仅开启**过滤参数**开关，不设置具体的**保留指定参数**时，表示去除 ? 之后的所有参数。 ○ **否**：资源回源时需精确匹配 ? 之后的参数，提高请求的精确性。

过滤模式	参数	说明
保留指定参数	**保留指定参数**	配置需要保留的参数。最多可以配置10个保留参数，用逗号（,）作分隔符。 **说明** 仅配置**保留指定参数**没有实际意义。需要配合**过滤参数**和**保留回源参数**使用。 示例： ○ 示例一：仅开启**过滤参数**，**保留回源参数**默认关闭。 原始URL：http：//example.com/image_01.png?key1=123&key2=321 缓存key：http：//example.com/image_01.png 回源URL：http：//example.com/image_01.png ○ 示例二：开启**过滤参数**，配置**保留指定参数**key1。 原始URL：http：//example.com/image_01.png?key1=123&key2=321 缓存key：http：//example.com/image_01.png?key1=123 回源URL：http：//example.com/image_01.png?key1=123 ○ 示例三：开启**过滤参数**，开启**保留回源参数**。 原始URL：http：//example.com/image_01.png?key1=123&key2=321 缓存key：http：//example.com/image_01.png 回源URL：http：//example.com/image_01.png?key1=123&key2=321 ○ 示例四：开启**过滤参数**，配置**保留指定参数**key1，开启**保留回源参数**。 原始URL：http：//example.com/image_01.png?key1=123&key2=321 缓存key：http：//example.com/image_01.png?key1=123 回源URL：http：//example.com/image_01.png?key1=123&key2=321
	保留回源参数	○ **是**：资源回源时，保留所有参数。 ○ **否**：资源回源时，仅保留指定参数。

过滤模式	参数	说明
删除指定参数	**删除指定参数**	配置需要忽略的参数。最多可以配置10个忽略参数，用空格作分隔符。 示例：配置**删除指定参数**key1，开启**保留回源参数**。 原始URL：http：//example.com/image_01.png?key1=123&key2=321 缓存key：http：//example.com/image_01.png?key2=321 回源URL：http：//example.com/image_01.png?key1=123&key2=321
	保留回源参数	○ **是**：资源回源时，保留所有参数。 ○ **否**：资源回源时，删除指定参数。

6. 单击**确定**。

11.7. 拖拽播放

当您播放视音频时，需要随意拖拽播放进度，而不影响视音频的播放效果，可以开启拖拽播放。通过本文您可以了解配置拖拽播放功能的操作方法。

背景信息

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

- 配置拖拽播放功能之前，需要确认源站支持Range请求。如果HTTP请求头中包含Range字段，则源站需要响应正确的206文件分片。
- 拖拽播放功能支持的文件和URL格式如下表所示。

文件格式	meta信息	start参数	举例
MP4	源站视频的meta信息必须在文件头部，不支持meta信息在尾部的视频。	start参数表示的是时间，单位是s，支持小数以表示ms（如start=1.01，表示开始时间是1.01s），系统会定位到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/lesson-01.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，系统会自动定位到start参数所表示的字节的前一个关键帧（如果start当前不是关键帧）。	对于`http：//domain/video.flv`，请求`http:// domain/video.flv?start=10`就是从第10字节的前一个关键帧（如果start=10不是关键帧所在位置）开始播放视频。

操作步骤

1. 登录全站加速控制台。
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**性能优化**。

5. 在**拖拽播放**区域，打开**拖拽播放**开关。

12.安全配置

12.1. 配置机器流量管理

为了帮助企业防控恶意爬取信息，恶意盗刷流量等业务风险。阿里云推出机器流量管理业务，该业务基于合法爬虫，威胁情报等多维度数据，配合AI智能，精准识别机器流量并自动应对，可对流量进行拦截、人机识别等处置手段。本文为您介绍机器流量管理功能开通和配置方法。

背景信息

您已在全站加速控制台开通机器流量管理功能（您可以加入钉钉群（34334246）进行咨询和开通该功能。）

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**安全设置**。
5. 在**机器流量管理**页签下，根据页面提示，配置**合法爬虫**、**威胁情报**和**AI智能防护**。

配置项	说明
合法爬虫	合法爬虫开关。 **说明** 合法爬虫功能提供合法搜索引擎白名单，为域名放行合法爬虫的访问请求。单击**修改配置**，观察、放行或者关闭合法爬虫。
威胁情报	威胁情报开关。 **说明** 威胁情报提供机器流量指纹库、机器流量IP库、秒播代理IP库，便于快速设置，阻断恶意流量访问请求。单击**修改配置**，观察、放行或者关闭威胁情报。

配置项	说明
AI智能防护	AI智能防护开关。 **说明** AI智能防护基于智能算法对业务流量进行分析和自动化学习，生成有针对性的机器流量指纹，并针对恶意流量设置防护规则。单击**修改配置**，观察、放行或者关闭AI智能防护。

12.2. 配置精准访问控制

通过本文您可以了解精准访问控制的定义、开通方式和配置方法。

功能介绍

精确访问控制使用常见的HTTP字段（例如IP、URL、Header等）设置匹配条件来筛选访问请求，并对命中条件的请求执行设定的操作，来满足业务场景的定制化防护需求。

规则排序

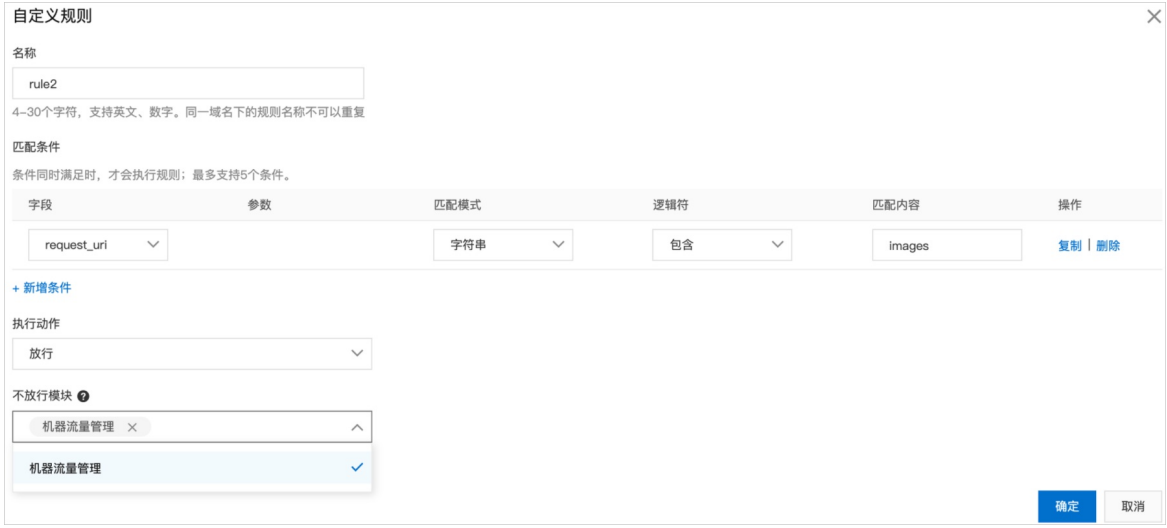
精准访问控制规则由匹配条件与匹配动作构成，并支持设置多条规则。如果您设置了多条规则，靠前的规则优先执行。请求如果命中了靠前的规则，则不再检查后面的规则。

申请开通

目前精准访问控制功能需要您申请开通，如需开通请加入钉钉群：34368392。

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. 单击**安全配置**，并选择**精准访问控制**。
5. 自定义规则。



匹配条件定义了要识别的请求中HTTP字段的属性特征。

> 说明
>
> - 支持添加多个匹配条件。若添加多个匹配条件，则只有当访问请求满足所有条件时才算命中。
> - 匹配条件由5个部分组成：字段、参数、匹配模式、逻辑符和匹配内容。输入条件时，如果一个部分没有输入框，表示该条件的匹配不依赖于它，可以不定义。

匹配字段和逻辑符等的说明，请参见下表：

字段	参数	匹配模式	逻辑符	匹配内容
requst_uri	N/A	正则	匹配，不匹配	字符串
		字符串	包含，不包含，等于，不等于	字符串
header	请求头名称	正则	匹配，不匹配	字符串
		字符串	包含，不包含，等于，不等于	字符串
		字符串	不存在	N/A
method	N/A	字符串	等于，不等于	字符串
ip	N/A	字符串	属于，不属于	逗号分隔的IP地址
referer	N/A	正则	匹配，不匹配	字符串
		字符串	包含，不包含，等于，不等于	字符串
user-agent	N/A	正则	匹配，不匹配	字符串
		字符串	包含，不包含，等于，不等于	字符串
cookie	N/A	正则	匹配，不匹配	字符串
		字符串	包含，不包含，等于，不等于	字符串
content-type	N/A	正则	匹配，不匹配	字符串
		字符串	包含，不包含，等于，不等于	字符串
x-forwarded-for	N/A	正则	匹配，不匹配	字符串
		字符串	包含，不包含，等于，不等于	字符串
		正则	匹配，不匹配	字符串

字段	参数	匹配模式	逻辑符	匹配内容
post-body		字符串	包含，不包含，等于，不等于	字符串
params	N/A	正则	匹配，不匹配	字符串
		字符串	包含，不包含，等于，不等于	字符串

执行动作当访问请求命中匹配条件时，对请求执行的操作。取值：

- *观察*：放行请求，并在日志中做标记。回源时会携带一个header用来定义该请求的风险等级，方便源站做进一步的处理。
- *拦截*：拒绝命中匹配条件的访问请求，返回403状态码。
- *放行*：放行请求。您需要进一步选择不该放行的模块，不被勾选的模块会放行该请求。

6. 完成自定义规则配置后，单击**确定**。
7. （可选）根据需求继续添加多条规则，并支持调整规则优先级。

13.高级配置

13.1. 配置IPv6

本文为您介绍了阿里云全站加速IPv6功能在控制台的操作步骤。开启IPv6开关后，IPv6的客户端请求将支持以IPv6协议访问全站加速，全站加速也将携带IPv6的客户端IP信息访问您的源站。

背景信息

阿里云全站加速大部分节点已经支持接收IPv6协议的请求，您可以在域名配置中开启IPv6开关。

开启开关后，当您的用户处于IPv6环境，且就近的全站加速节点也支持IPv6的请求时，客户端可以通过IPv6协议访问全站加速节点。当用户就近区域的全站加速节点不支持IPv6协议时，客户端仍可以IPv4协议访问全站加速节点。

> **说明** 目前海外、中国香港、中国澳门和中国台湾节点不支持IPv6配置。

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**高级配置**。
5. 打开**IPv6开关**。

开启IPv6功能后，您可以在客户端通过IPv6协议访问全站加速节点，阿里云全站加速节点也将携带IPv6协议信息访问您的源站。

14.WebSocket

14.1. 什么是WebSocket

通过本文您可以了解WebSocket的概念、优势和使用场景。

> 注意
>
> - WebSocket默认不开通，控制台不会显示WebSocket配置项，开通后才会显示。如果需要开通WebSocket，请提交申请。
> - 当前WebSocket协议分别和DCDN WAF、配置HTTP/2功能不兼容，无法同时开启。
> - WebSocket仅用于动态加速。

简介

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

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协议优势如下：

- 小Header：互相沟通的Header非常小，只有2Bytes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。
- 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

业务场景	场景概述
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，因此比赛实况成为其最为关心的热点。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。

业务场景	场景概述
基于位置的应用	越来越多的开发者借用移动设备的GPS功能来实现基于位置的网络应用。如果您一直记录终端用户的位置（例如：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。

14.2. 配置WebSocket

WebSocket协议允许服务端主动向客户端推送数据，使得客户端和服务器之间的数据交换变得更加简单。开启WebSocket后，可以更好地节省服务器的资源和带宽，且能够实现实时通讯。本文介绍开通和配置WebSocket的方法。

> **注意**
> - WebSocket默认不开通，控制台不会显示WebSocket配置项，开通后才会显示。如果需要开通WebSocket，请提交申请。
> - 当前WebSocket协议分别和DCDN WAF、配置HTTP/2功能不兼容，无法同时开启。
> - WebSocket仅用于动态加速。

本文将从以下内容指导您开通和使用WebSocket功能：

- 开通WebSocket
- 启用WebSocket
- 查询WebSocket流量带宽和HTTP状态码信息
- 关闭WebSocket

开通WebSocket

开通方式：请提交申请。

目前仅支持企业客户申请，不支持源站在海外且加速区域为仅中国内地或全球的域名开通WebSocket。

申请后由阿里云售后专员审核，审核结果将在1天内以短信和邮件的方式通知您。审核通过后，您即可在控制台域名配置页面开启WebSocket。

> **注意** WebSocket为增值服务，单独计费。WebSocket计费详情，请参见全站加速产品定价。

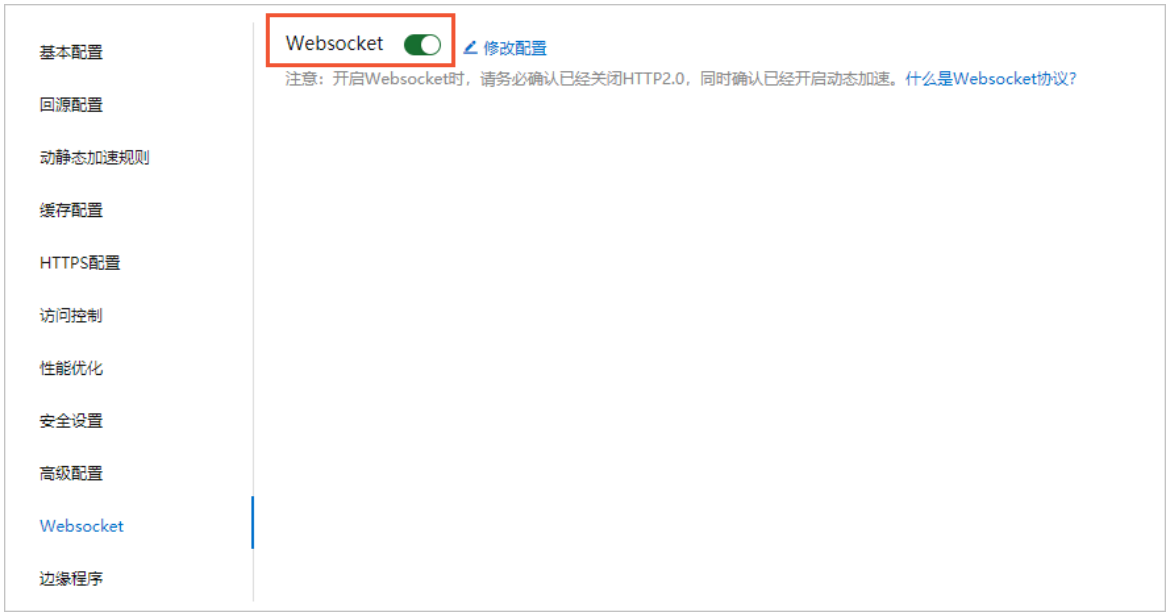
启用WebSocket

> **说明** 启用WebSocket功能前，您需要已完成账号的企业认证，且账号下有备案通过的域名。

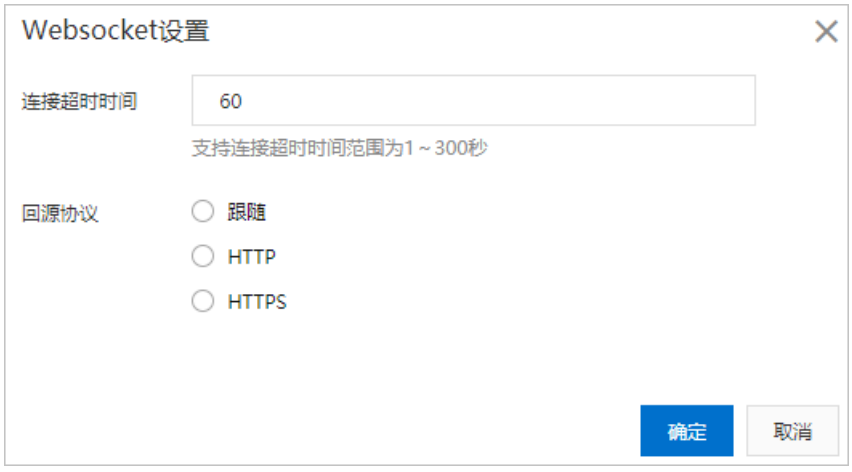
1. 登录全站加速控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**配置**。
4. （可选）开启**动态加速**，如您已经开启该功能可跳过该步骤。
   i. 在目标域名的左侧导航栏，单击**动静态加速规则**。

ii. 打开**动态加速**开关。

5. 在目标域名的左侧导航栏，单击**Websocket**，打开**Websocket**开关。



6. 单击**修改配置**。
7. 在**Websocket**对话框，配置连接超时时间和回源协议。



参数	说明

参数	说明
连接超时时间	指客户端向服务器发送数据包相互同步当前状态的间隔时间： ○ 默认值：60秒。 ○ 单位：秒。 ○ 建议配置规则为：A<=B<=C。 ■ A：客户端连接超时时间。 ■ B：全站加速平台连接超时时间。 ■ C：源站连接超时时间。 **说明** 如果客户端的连接超时时间大于服务端的连接超时时间，会导致服务异常。
回源协议	您可以根据业务需求，选择WebSocket协议回源站时遵循的协议类型。 ○ **跟随**：客户端以HTTP或HTTPS协议回源，WebSocket跟随客户端的协议请求源站（**源站需支持443或者80端口**）。 ○ **HTTP**：WebSocket以HTTP协议回源。 ○ **HTTPS**：WebSocket以HTTPS协议回源（**源站需支持443端口**）。

8. 单击**确定**。

查询WebSocket流量带宽和HTTP状态码信息

成功配置并使用WebSocket后，您可以在全站加速控制台的左侧导航栏，单击**Websocket**，查看WebSocket的**流量带宽**和**HTTP CODE**监控信息。

关闭WebSocket

如果您不想继续使用WebSocket功能，可随时在全站加速控制台关闭WebSocket。关闭WebSocket实时生效。