ALIBABA CLOUD

阿里云

全站加速

域名管理

文档版本：20201110

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。

控制台指引

全站加速控制台界面展示如下图所示。

全站加速控制台界面说明如下表所示。

序号	区域	说明
1	左侧导航栏	全站加速域名导航栏。详细功能介绍，请参见域名管理功能列表。
2	基础数据	全站加速根据您服务的计费方式，展示计费项中的使用数据。详细功能介绍，请参见基础服务计费。
3	动态和静态请求数	您可以查看昨天静态和动态HTTP请求数，以及静态和动态HTTPS请求数。详细功能介绍，请参见请求数计费。
4	其他加速产品	您可以了解与全站加速相关的其他产品。
5	计费方式	您已选择的计费方式。您也可根据所需快速修改计费方式。详细功能介绍，请参见基础服务计费和IP应用加速计费。
6	资源包	您已购买的资源包。详细功能介绍，请参见预付费资源包。
7	全部域名	您可以通过快速入口对域名进行管理，并执行添加和刷新预热操作。

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	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	修改基础信息	修改加速区域。	无
	配置源站	修改源站配置。	无
	配置回源HOST	修改回源HOST域名。	开启

功能	参考文档	说明	默认值
回源配置	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
	开启私有Bucket回源授权	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
动态加速规则	配置静态文件路径	指定静态文件的路径。	未开启
	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
	配置协议跟随回源	动态资源回源使用协议需要和客户端访问资源的协议保持一致。	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HTTP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
	配置重写	对请求的URI进行修改和302重定向至目标URI。	无

功能	参考文档	说明	默认值
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	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
	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
	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

功能	参考文档	说明	默认值
性能优化	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
	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。	关闭
	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
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

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

前提条件

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

背景信息

您在批量复制某个域名的配置时，请注意：

- 域名复制成功后，操作不可逆，请您务必确认域名配置复制正确。
- 对于流量或带宽较大的域名，请您在复制配置时谨慎操作，以免带来经济损失。
- 对于通过工单进行的后端特殊配置，请您注意该特殊配置无法复制。

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，选择您需要复制配置的域名，单击**复制配置**。
4. 选中您需要复制的配置项，单击**下一步**。

   

   > **说明**
   > - 源站信息和非源站信息无法同时复制。
   > - 您无法复制HTTPS证书到其他域名，请您单独配置。
   > - 自定义回源头为增量复制。例如，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，则您会有7条回源头配置内容。
   > - HTTP头为非增量复制。例如，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。
   > - Referer或IP黑白名单将会覆盖域名原有配置。

5. 选中您想要批量配置的目标域名，单击**下一步**。

   > **说明** 您可以在搜索框总输入关键词查找域名。

   

6. 在弹出的批量复制对话框，单击**确定**。

   

3.基本配置

3.1. 修改基础信息

当您需要变更全站加速的服务区域时，您可以通过切换加速区域功能实现。

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**配置**。
4. 在**基本配置**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**，则需要工信部备案。域名备案方法，请参见加速域名备案。
全球	如果选择**全球**，则需要工信部备案。域名备案方法，请参见加速域名备案。
全球（不包含中国内地）	如果选择**全球（不包含中国内地）**，则无需工信部备案。

7. 单击**确定**。

3.2. 配置源站

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

背景信息

全站加速支持的源站类型包括OSS域名、IP和源站域名。其中，IP和源站域名支持多IP或多域名设置，并支持应用在多源站场景下，进行回源优先级设置。

> **说明** 源站健康检查：实行主动四层健康检查机制，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。

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

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**管理**。

4. 在**基本配置**页签，找到**源站信息**。
5. 在**源站信息**区域，单击**修改配置**。
6. 在**源站配置**对话框，设置源站类型、源站地址和端口。

   在**源站配置**对话框中，需要配置的参数说明如下：

   - 源站类型

源站类型	说明
IP	支持多个服务器外网IP地址。 如果您使用阿里云云服务器ECS，则可以免审核ECS的IP地址。详情请参见云服务器ECS。
源站域名	支持多个源站域名。 **说明** 源站域名不能与加速域名相同，否则会造成循环解析，无法回源。例如您的源站域名为img.yourdomain.com，则加速域名可设置为dcdn.yourdomain.com。
OSS域名	您可以手动输入阿里云OSS Bucket的外网域名，例如：xxx.oss-cn-hangzhou.aliyuncs.com。OSS外网域名可前往OSS控制台查看，也可直接选择同账号下的OSS Bucket。

   - 端口

端口	说明
80端口	资源以HTTP或HTTPS协议回源到80端口。
443端口	资源以HTTP或HTTPS协议回源到443端口。如果您的源站为单个IP地址提供多个域名服务，您需要完成配置回源操作。详情请参见配置回源SNI。
自定义端口	**说明** 目前仅支持以HTTP协议回源到自定义端口。如果您需要以HTTPS协议回源到自定义端口，请提交工单处理。 当源站选择OSS类型时，回源端口是否支持自定义端口，取决于OSS产品。 配置自定义端口回源，需要完成如下操作： ■ 将**静态协议跟随回源**配置为**HTTP**协议，操作方法请参见配置静态协议跟随回源。 ■ 将动态加速的**协议跟随回源**配置为**HTTP**协议，操作方法请参见配置协议跟随回源。

7. 单击**确定**。

4.回源配置

4.1. 概述

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，则会到源站获取，同时缓存到全站加速节点。您可以根据所需配置回源的相关功能，提升资源访问效率。

您可以通过回源配置功能，对域名执行如下操作。

功能	说明
配置回源HOST	当您需要自定义全站加速节点回源时需要访问的具体服务器域名时，需要配置回源HOST的域名类型。
配置静态协议跟随回源	当您通过客户端请求访问资源时，如果全站加速节点上未缓存该资源，则会根据您配置的协议跟随规则到源站获取资源，同时缓存到全站加速节点。
开启私有Bucket回源授权	当您的源站为OSS时，可以开通加速域名访问私有OSS Bucket资源的权限，有效防止资源盗链。
关闭私有Bucket回源授权	您可以通过RAM控制台，取消对应角色名称的授权，关闭私有Bucket回源功能。
配置回源SNI	如果您的源站IP绑定了多个域名，当全站加速节点以HTTPS协议访问您的源站时，您可以设置回源SNI，指明具体访问域名。
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。
回源请求超时时间	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。
配置自定义回源HTTP头	HTTP请求回源时，您可以添加或删除回源HTTP头。

4.2. 配置回源HOST

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

背景信息

回源HOST指全站加速节点在回源过程中，在源站访问的站点域名。

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

源站和回源HOST的区别：

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

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	加速域名是指您需要加速的域名，即终端用户直接访问到的域名，例如：`dcdntest.com`。当回源HOST的域名类型选择为**加速域名**的时候，回源HOST将会被配置为加速域名，例如：`dcdntest.com`。
源站域名	源站域名是指您的源站服务器的域名地址，即全站加速回源需要访问的域名地址，例如：`origin.com`。当回源HOST的域名类型选择为**源站域名**的时候，回源HOST将会被配置为源站域名，例如：`origin.com`。
自定义域名	当回源HOST的域名类型选择为**自定义域名**的时候，回源HOST将会被配置用户指定的任意域名。如果您的源站绑定了多个域名，则需要指定具体域名，否则回源会失败。

示例	源站类型	功能状态	域名	说明
示例一	域名类型	回源HOST功能默认关闭	加速域名：`dcdntest.com` 源站地址：`origin.com`	○ 域名类型选择**加速域名**，则回源HOST为`dcdntest.com`。 ○ 域名类型选择**源站域名**，则回源HOST为`origin.com`。 ○ 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	IP地址类型	回源HOST功能默认关闭	加速域名：`dcdntest.com` 源站地址：`1.1.1.1`	○ 域名类型选择**加速域名**，则回源HOST为`dcdntest.com`。 ○ 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。 **说明** 源站地址是IP地址类型，所以域名类型的**源站域名**选项被置灰，不可选择。

示例	源站类型	功能状态	域名	说明
示例三	OSS域名类型	回源HOST默认开启	加速域名： dcdntest.com 源站地址： test.oss-cn-hangzhou.aliyuncs.com	○ 域名类型选择**加速域名**，则回源HOST为 dcdntest.com 。 ○ 域名类型选择**源站域名**，则回源HOST为 test.oss-cn-hangzhou.aliyuncs.com 。 ○ 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。 **说明** 默认配置为： 域名类型：**源站域名** 域名地址：test.oss-cn-hangzhou.aliyuncs.com

7. 单击**确定**。

4.3. 配置静态协议跟随回源

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

背景信息

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

说明 源站需要同时支持80端口和443端口，否则有可能会造成回源失败。

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**配置**。
4. 在指定域名的左侧导航栏，单击**回源配置**。
5. 在**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，选择回源协议类型为**跟随**、**HTTP**或**HTTPS**。

当您需要全站加速回源时使用和客户端访问资源时一样的协议（即客户端使用HTTPS请求资源，全站加速节点也使用HTTPS回源；客户端使用HTTP请求资源，CDN节点也用HTTP回源），则需要开启协议跟随回源。

> **说明** 开启协议回源后，在全站加速控制台上设置的固定回源端口将失效。

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

8. 单击**确定**，完成配置。

4.4. 开启私有Bucket回源授权

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

背景信息

私有Bucket回源授权指如果加速域名需要回源至您账号下标记为私有Bucket的源站，则需要进行授权。授权成功并开启授权配置后，您开启的私有Bucket授权的域名才有权限访问私有Bucket。

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

> **注意**
>
> - 仅支持源站类型为OSS域名的加速域名开启私有Bucket回源功能。
> - 进行一次回源授权，即授权全站加速对您所有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内的资源内容。开启该功能前，请根据实际的业务情况，谨慎决策。如果您授权的私有Bucket内容并不适合作为全站加速域名的回源内容，请勿授权或者开启此功能。
> - 如果您的网站有被攻击的风险，请购买高防服务。同时，请勿授权或开启私有Bucket回源授权功能。

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**配置**。
4. 在指定域名的左侧导航栏，单击**回源配置**。
5. 在**回源配置**页签下找到**私有Bucket回源**。
6. 在**私有Bucket回源**区域，单击**点击授权**。

7. 单击**同意授权**。

8. 在**私有Bucket回源**区域，打开**私有Bucket回源**开关。

4.5. 关闭私有Bucket回源授权

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

背景信息

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

操作步骤

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

4. 单击待删除权限对应的**移除权限**。
5. 在移除权限确认对话框中，单击**确定**。
6. 返回**RAM角色管理**页面，单击待删除角色对应的**删除**。
7. 在**删除RAM角色**的确认对话框中，单击**确定**。

4.6. 配置回源SNI

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

背景信息

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

如果您的源站服务器使用单个IP提供多个域名的HTTPS服务，且您已经为您的全站加速设置了443端口回源（CDN节点以HTTPS协议访问您的服务器），您就需要设置回源SNI，指明所请求的具体域名。这样全站加速节点以HTTPS协议回源访问您的服务器时，服务器才会正确地返回对应的证书。

> **说明** 如果您的源站是阿里云OSS，则无需设置回源SNI。

回源SNI的工作原理如下图所示。

1. 全站加速节点以HTTPS协议访问源站时，在SNI中指定访问的域名。
2. 源站接收到请求后，根据SNI中记录的域名，返回对应域名的证书。

3. 全站加速节点收到证书，与服务器端建立安全连接。

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**配置**。
4. 在指定域名的左侧导航栏，单击**回源配置**。
5. 在**回源配置**页签下找到**回源SNI**。
6. 打开**回源SNI**开关，根据所需输入服务器源站提供服务的域名。

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

   

7. 单击**确定**。

4.7. 配置Range回源

Range回源是指客户端通知源站服务器只返回指定范围内的部分内容，有利于较大文件的分发加速。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。通过本文您可以了解开启Range回源的方法。

背景信息

配置Range回源时，需要源站支持Range请求，即HTTP请求头中包含Range字段，源站能够响应正确的206文件分片。

操作步骤

1. 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。

Range回源	具体描述	示例
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。

4.8. 回源请求超时时间

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。通过本文档，您可以了解配置回源请求超时时间的操作方法。

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**回源请求超时时间**，单击**修改配置**。
6. 在**回源请求超时时间**对话框，设置**超时时间**。全站加速的回源请求超时时间正常不超过100秒，配置的最大值不能超过900秒。

   
7. 单击**确定**。

4.9. 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，您可以添加或删除回源HTTP头。

背景信息

在HTTP消息头中，按其出现的上下文环境，分为通用头、请求头、响应头等。

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**HTTP头设置**页面，选择**参数**，并设置**取值**。

8. 单击**确定**。

5.动静态加速规则

5.1. 配置静态文件类型

全站加速支持以后缀名的方式设定静态文件类型。设定的静态文件不再使用动态加速，而采用更合适的静态加速，分配最佳的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自定义静态和动态资源的加速规则。静态和动态资源加速规则配置成功后，资源按照自定义的加速规则加速。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。您可以设置动态资源的回源协议和客户端访问资源的协议保持一致。

- 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**静态文件类型**页签下，单击**修改配置**。

   

7. 在**静态文件类型**对话框，**开启**或**关闭自适应缓存**。
8. 选择**静态文件类型**。

   > **说明** 如果您开启的是自定义静态文件，在配置静态缓存规则时，需要确保缓存规则的文件后缀在自定义静态文件类型内，否则自定义缓存规则不生效。

   

   支持的常见静态文件类型如下：

   - 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。

9. 单击**确定**。

5.2. 配置静态文件URI

支持以文件URI的方式区分出静态文件，设定的静态文件不再使用动态加速，而采用更合适的静态加速，分配最佳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自定义静态和动态资源的加速规则。静态和动态资源加速规则配置成功后，资源按照自定义的加速规则加速。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。您可以设置动态资源的回源协议和客户端访问资源的协议保持一致。

- 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. 单击**确定**。

5.3. 配置静态文件路径

支持以文件路径的方式区分出静态文件，设定的静态文件不再使用动态加速，而采用更合适的静态加速，分配最佳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自定义静态和动态资源的加速规则。静态和动态资源加速规则配置成功后，资源按照自定义的加速规则加速。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。您可以设置动态资源的回源协议和客户端访问资源的协议保持一致。

- 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. 单击**确定**。

5.4. 配置协议跟随回源

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

背景信息

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自定义静态和动态资源的加速规则。静态和动态资源加速规则配置成功后，资源按照自定义的加速规则加速。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。您可以设置动态资源的回源协议和客户端访问资源的协议保持一致。

- 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**协议跟随回源**页签下，单击**修改配置**。

7. 在**协议跟随回源**对话框，设置**跳转类型**。

参数	说明
跟随	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。
HTTP	全站加速只以HTTP协议请求源站。
HTTPS	全站加速只以HTTPS协议请求源站。

8. 单击**确定**。

6.缓存配置

6.1. 概述

加速静态资源时，将源站上的资源缓存到距离客户端最近的全站加速节点上。当您访问该静态资源时，直接从缓存中获取，避免通过较长的链路回源，提高访问效率。

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，以及优先级，使其在全站加速上按照缓存规则进行缓存。
配置HTTP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。
配置重写	您可以对请求的URI进行修改和302重定向至目标URI。

6.2. 配置缓存过期时间

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

背景信息

缓存过期时间可以针对拥有不同目录路径和文件名后缀的资源，进行缓存服务器行为的设置。您可以自主指定资源内容的缓存过期时间规则。

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

全站加速节点上资源的缓存策略如下图所示。

> **说明**
>
> - Cache的缓存策略用于配置文件的过期时间，在此配置的优先级高于源站配置。如果源站未配置Cache，则支持按完整目录和文件后缀名两种方式设置。
> - 全站加速节点上缓存的资源，可能由于热度较低而被提前从节点删除。

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击**域名管理**。

3. 在**域名管理**页面，单击目标域名对应的**配置**。
4. 在指定域名的左侧导航栏，单击**缓存配置**。
5. 在**缓存过期时间**页签下，单击**添加**。
6. 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。

配置项	说明
类型	○ 目录：指定路径下的缓存资源。 ○ 文件后缀名：指定文件类型的缓存资源。
内容	○ 添加单条目录（支持完整路径）时，须以正斜线（/）开头，例如*/directory/aaa*。 ○ 添加多个文件后缀名时，须以半角逗号（,）分隔，例如 `JPG,TXT` 。 支持的常见静态文件类型如下： ■ 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。
过期时间	资源对应的缓存时间。过期时间最多设置为3年，建议您参照以下规则进行配置： ○ 对于不经常更新的静态文件（如图片类型、应用下载类型等），建议您将缓存时间设置为1个月以上。 ○ 对于频繁更新的静态文件（例如js、css等），您可以根据实际业务情况设置。 ○ 对于动态文件（例如php、jsp、asp等），建议您将缓存时间设置为0s，即不缓存。
权重	缓存规则的优先级。 **说明** ○ 取值范围：1~99间的整数。数字越大，优先级越高，优先生效。 ○ 不推荐设置相同的权重，权重相同的两条缓存策略优先级随机。 示例：为加速域名 `example.aliyun.com` 配置三条缓存策略，缓存策略1优先生效。 ○ 缓存策略1：文件名后缀为.jpg和.png的所有资源过期时间设置为1月，权重设置为90。 ○ 缓存策略2：目录为*/www/dir/aaa*过期时间设置为1小时，权重设置为70。 ○ 缓存策略3：完整路径为*/www/dir/aaa/example.php*过期时间设置为0s，权重设置为80。

缓存过期时间推荐配置如下表所示。

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

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

7. 单击**确定**。

   您也可以在缓存过期时间列表中，单击**修改**或**删除**，对当前配置的缓存策略执行相应操作。

6.3. 配置HTTP头

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

背景信息

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

在HTTP消息头中，按其出现的上下文环境，分为通用头、请求头、响应头等。

配置HTTP响应头时，注意事项如下：

- HTTP响应头的设置会影响该加速域名下所有资源，当您通过客户端（例如浏览器）访问资源时，会影响请求响应，但不会影响缓存服务器。
- 关于参数 `Access-Control-Allow-Origin` 的取值，您可以填写 `*` 表示全部域名；也可以填写完整域名，例如 `www.aliyun.com` 。
- 目前不支持泛域名设置。

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**配置**。
4. 在指定域名的左侧导航栏，单击**缓存配置**。
5. 在**HTTP头**页签下，单击**添加**。
6. 在**HTTP头设置**对话框，根据下表中的参数含义配置HTTP头的参数和取值。

   目前阿里云全站加速提供10个HTTP响应头参数可供您自行定义取值，参数解释如下表所示。如果您有其他HTTP头设置需求，请提交工单反馈。

参数	描述	示例
Content-Type	指定客户端程序响应对象的内容类型。	image
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。	123.txt
Content-Language	指定客户端程序响应对象的语言。	zh-CN
Expires	指定客户端程序响应对象的过期时间。	Wed, 21 Oct 2015 07:28:00 GMT
Access-Control-Allow-Origin	指定允许的跨域请求的来源。	* **说明** 您可以填写 * 表示全部域名；也可以填写完整域名，例如 www.aliyun.com 。
Access-Control-Allow-Headers	指定允许的跨域请求的字段。	X-Custom-Header
Access-Control-Allow-Methods	指定允许的跨域请求方法。	POST, GET **说明** 如果您需要同时添加POST和GET，请使用英文逗号（,）隔开。
Access-Control-Max-Age	指定客户端程序对特定资源的预取请求返回结果的缓存时间。	600
Access-Control-Expose-Headers	指定允许访问的自定义头信息。	Content-Length

7. 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。

6.4. 自定义页面

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

背景信息

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

- 默认值：HTTP响应返回404时，服务器返回默认404 Not Found页面。
- 自定义404：HTTP响应返回404时，将会跳转到自定义的404页面，需要自定义跳转页的完整URL地址。

> 说明
> - 404页面属于阿里云公益资源，不会产生任何费用。
> - 自定义页面属于个人资源，按照正常分发计费。
> - 返回404页面的原因，请参见出现自定义404页面的原因是什么？。

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**自定义页面**页签下，单击**添加**。
6. 在**自定义页面**对话框，配置自定义页面的**错误码**和**链接**。本文以自定义错误码404为例，假设您需要将404页面 `error404.html` 与其他静态文件同时存放在源站域名下，并通过加速域名 `exp.aliyun.com` 访问。您只需选择**404**，并填写完整的加速域名URL即可，URL为： `http://exp.aliyun.com/error404.html` 。

   

7. 单击**确定**。

   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。

6.5. 配置重写

当您需要将请求URI中的HTTP重定向为HTTPS，或您访问的URI与源站URI不匹配时，需要将URI修改为与源站匹配的URI。您修改URI中指定内容时，需要配置重写规则，规则匹配后，会302跳转到目标URI。您还可以根据实际需求配置多条重写匹配规则。通过本文档，您可以了解配置重写规则的操作方法。

背景信息

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

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**重写**页签下，单击**添加**。

6. 在**重写设置**对话框，根据您的需求，配置**待重写URI**、**目标URI**和**执行规则**。

参数	示例	说明
待重写URI	/domain/image/123.png	不含协议及域名，以正斜线（/）开头。支持PCRE正则表达式。
目标URI	/domain/image/123.gif	不含协议及域名，以正斜线（/）开头。
执行规则	Redirect	若请求的URI匹配了当前规则，该请求将被302重定向跳转到目标URI。
	Break	若请求的URI匹配了当前规则，执行完当前规则后，将不再匹配剩余规则。

7. 单击**确定**。

在**重写**列表中，您可以单击**修改**或**删除**，对当前配置的重写规则进行相应操作。

> **说明** 单个域名可以配置的重写规则数量上限是50个。

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

7.HTTPS配置

7.1. 什么是HTTPS证书

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

什么是HTTPS？

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

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

工作原理

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

HTTPS加密流程如下图所示。

1. 客户端发起HTTPS请求。
2. 服务端提前准备好公钥和私钥。

   > **说明** 公钥和私钥可以自己制作，可以向专业组织申请，也可以使用阿里云CDN控制台申请免费证书。

3. 服务端将相应的公钥传送给客户端。
4. 客户端解析证书的正确性。
   - 如果证书正确，则会生成一个随机数（密钥），并用公钥进行加密，传输给服务端。
   - 如果证书不正确，则SSL握手失败，需要重新上传证书进行认证。

   > **说明** 正确性包括以下内容：
   > - 证书未过期。
   > - 发行服务器证书的CA可靠。
   > - 发行者证书的公钥能够正确解开服务器证书的发行者的数字签名。
   > - 服务器证书上的域名和服务器的实际域名相匹配。

5. 服务端用之前的私钥进行解密，得到随机数（密钥）。
6. 服务端用随机数（密钥）对传输的数据进行加密。
7. 客户端用随机数（密钥）对服务端的加密数据进行解密，拿到相应的数据。

功能优势

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。
- 主流浏览器对HTTPS网站进行搜索加权，主流浏览器均支持HTTP/2，而支持HTTP/2必须支持HTTPS。无论从安全、市场或用户体验来看，普及HTTPS是未来的一个方向，所以强烈建议您将访问协议升级到HTTPS。

应用场景

主要将应用场景分为五类，如下表所示 。

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

使用说明

HTTPS安全加速功能使用说明，如下表所示。

功能分类	说明

配置	• 您可以配置泛域名的HTTPS服务。
	• 您可以启用或停止HTTPS安全加速。
	  ◦ 启用：您启用HTTPS安全加速后，可以修改证书。系统默认兼容HTTP和HTTPS请求。您也可以配置强制跳转，自定义源请求方式。
	  ◦ 停用：您停用HTTPS安全加速后，系统不再支持HTTPS请求，且不再保留证书或私钥信息。当您再次开启HTTPS安全加速时，需要重新上传证书或私钥，配置方法，请参见配置HTTPS证书。
	• 您可以查看证书，但由于私钥信息敏感，不支持私钥查看。请妥善保管证书相关信息。
	• 您可以更新证书，但请谨慎操作。更新HTTPS证书后1分钟内全网生效。

功能分类	说明
计费	HTTPS计费标准请参见HTTPS计费详情。 说明 HTTPS根据请求数单独计费，请确保账户余额充足再开通HTTPS服务，以免因HTTPS服务欠费影响您的全站加速服务。
证书	• 开启HTTPS安全加速功能的加速域名，您需要上传格式均为 PEM 的证书和私钥。 说明 由于全站加速采用的Tengine服务基于Nginx，因此只支持Nginx能读取的 PEM 格式的证书。详细说明，请参见证书格式说明。 • 上传的证书需要和私钥匹配，否则会校验出错。 • 不支持带密码的私钥。 • 只支持携带SNI信息的SSL/TLS握手。 其他证书相关的常见问题，请参见更多证书问题。

相关功能

为了数据传输的安全，您可以根据实际业务需求，配置相关功能，如下表所示。

功能	说明
配置HTTPS证书	实现HTTPS安全加速。
配置HTTP/2	HTTP/2是最新的HTTP协议，Chrome、 IE11、Safari以及Firefox等主流浏览器已经支持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TLS	保障您互联网通信的安全性和数据完整性。
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。

7.2. 证书格式说明

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

您开启HTTPS服务之前，需要配置证书。您可以直接选择在 阿里SSL证书管理控制台购买的证书、免费证书或上传自定义证书。自定义上传证书只支持 PEM 格式和其他格式转换的PEM格式。

Root CA机构颁发的证书

Root CA机构提供的证书是唯一的，一般包括Apache、IIS、Nginx和Tomcat。阿里云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CDN控制台填写证书部分，私钥无需填写。

- PFX转换为PEM

  PFX格式一般出现在Windows Server中。

  - 证书转化：

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

  - 私钥转化：

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

免费证书

您在使用免费证书时，注意事项如下：

- 免费证书通常会在1~2个工作日签发。等待期间，您也可以重新选择上传自定义证书或者选择托管证书。

  > **说明** 根据CA中心审核流程，您申请的证书有可能会在几个小时内完成签发，也有可能需要2个工作日才完成签发，都属于正常现象，请您耐心等待即可。

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

其他证书相关

使用其他证书时的注意事项如下：

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

其他证书的相关常见问题，请参见更多证书问题。

7.3. 配置HTTPS证书

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

前提条件

配置HTTPS证书前，您需要先购买证书，您可以在SSL证书控制台快速申请免费证书或购买高级证书。

背景信息

目前全站加速仅支持PEM格式的证书，如果您的证书不是PEM格式，请先转换成PEM格式，具体操作请参见证书格式说明。

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

根据证书认证级别分类如下：

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

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**配置**。
4. 在指定域名的左侧导航栏，单击**HTTPS配置**。
5. 在**HTTPS证书**区域，单击**修改配置**。
6. 在**HTTPS设置**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计费标准请参考请求数计费。
7. 在弹出的对话框中选中并确认开启HTTPS，单击**确定**。
8. 在**HTTPS设置**页面，配置证书相关参数。

参数	说明
证书来源	○ **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，您可以选择上传自定义证书。您需要在设置证书名称后，上传证书公钥和私钥，该证书将会在阿里云SSL证书服务中保存。您可以在SSL证书控制台中查看。 ○ **免费证书** 免费证书只适用于HTTPS安全加速业务，因此您无法在阿里云SSL证书控制台管理该证书，也无法查看到公钥和私钥。 ■ 免费证书通常会在1~2个工作日签发。等待期间，您也可以重新选择上传自定义证书或云盾证书。 **说明** 根据CA中心审核流程，您申请的证书有可能会在几个小时内完成签发，也有可能需要2个工作日才完成签发，都属于正常现象，请您耐心等待即可。 ■ 免费证书的有效期为1年，在您使用过程中，如果关闭了HTTPS安全加速，当再次开启使用免费证书时，将直接使用已申请但未过期的证书。若开启时证书已过期，您需要重新申请免费证书。 **云盾（SSL）证书中心**的证书、**自定义上传（证书+私钥）**证书和**免费证书**之间可以相互切换。
证书名称	当**证书来源**选择**云盾（SSL）证书中心**或**自定义上传（证书+私钥）**时，需要配置证书名称。
证书（公钥）	当**证书来源**选择**自定义上传（证书+私钥）**时，需要配置该参数。配置方法请参见**证书（公钥）**输入框下方的**pem编码参考样例**。
私钥	当**证书来源**选择**自定义上传（证书+私钥）**时，需要配置该参数。配置方法请参见**私钥**输入框下方的**pem编码参考样例**。

9. 单击**确定**，完成配置。

后续步骤

更新HTTPS证书1分钟后全网生效。您可以验证证书是否生效，使用HTTPS方式访问资源，如果浏览器中出现锁的HTTPS标识，则HTTPS安全加速生效。

7.4. 配置HTTP/2

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

前提条件

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

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

背景信息

HTTP/2也被称为HTTP 2.0，相对于HTTP 1.1的新增多路复用、压缩HTTP头、划分请求优先级、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、 IE11、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。
- 内容安全：HTTP/2基于HTTPS，具有安全特性。使用HTTP/2特性可以避免单纯使用HTTPS引起的性能下降问题。
- 多路复用（MultiPlexing）：通过该功能，在一条连接上，您的浏览器可以同时发起无数个请求，并且响应可以同时返回。另外，多路复用中支持了流的优先级（Stream dependencies）设置，允许客户端告知服务器最优资源，可以优先传输。
- Header压缩（Header compression）：HTTP请求头带有大量信息，而且每次都要重复发送。HTTP/2采用HPACK格式进行压缩传输，通讯双方各自缓存一份头域索引表，相同的消息头只发送索引号，从而提高效率和速度。

操作步骤

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

7.5. 配置强制跳转

当您在配置HTTPS证书时，如果使用了Nginx证书，则需要将HTTP强制跳转到HTTPS。您还可以根据所需将客户端到边缘节点的请求强制重定向为HTTP或HTTPS方式。通过本文您可以了解配置强制跳转的操作方法。

前提条件

执行该操作前，请您确保已成功配置HTTPS证书，操作方法请参见配置HTTPS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. 在**强制跳转**区域，单击**修改配置**。
6. 在**强制跳转**对话框，选择**跳转类型**。

跳转类型	说明
默认	同时支持HTTP和HTTPS方式的请求。
HTTPS -> HTTP	您可以根据所需将客户端到边缘节点的请求强制重定向为HTTP方式。
HTTP -> HTTPS	当您在配置HTTPS证书时，如果使用了Nginx证书，则需要将HTTP强制跳转到HTTPS。您还可以根据所需将客户端到边缘节点的请求强制重定向为HTTPS方式，确保访问安全。

以**跳转类型**为**HTTP -> HTTPS**为例，介绍强制跳转功能。

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

7. 单击**确定**。

7.6. 配置TLS

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

前提条件

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

背景信息

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

操作步骤

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

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

TLS协议说明如下表所示。

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

7.7. 配置HSTS

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

前提条件

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

背景信息

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

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

参数	说明
max-age	单位是秒。
Strict-Transport-Security	在浏览器缓存的时间，浏览器处理域名的HTTP访问时，若该域名的Strict-Transport-Security没有过期，则在浏览器内部做一次307重定向到HTTPS，从而避免浏览器和服务器之间301和302重定向被劫持的风险。
includeSubDomains	可选参数。如果指定这个参数，说明这个域名所有子域名也适用上面的规则。

参数	说明
preload	可选参数，支持preload列表。

说明

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

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**配置**。
4. 在指定域名的左侧导航栏，单击**HTTPS配置**。
5. 在**HSTS**区域，打开**HSTS**开关，配置**过期时间**和**包含子域名**。

6. 单击**确定**。

8.访问控制

8.1. 概述

您可以通过设置Refer、IP、UsageAgent黑名单和白名单，以及URL鉴权，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的Referer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。
配置URL鉴权	您可以通过配置URL鉴权功能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。
配置IP黑白名单	您可以通过配置IP黑名单和白名单来实现对访客身份的识别和过滤，限制访问全站加速资源的用户。
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，限制访问全站加速资源的用户。

8.2. 配置Referer防盗链

您可以通过配置访问的Referer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Referer防盗链的配置方法。

背景信息

- 防盗链功能基于HTTP协议支持的Referer机制，通过Referer跟踪来源，对来源进行识别和判断。
- 目前防盗链功能支持黑名单或白名单机制，您对资源发起请求后，请求到达全站加速节点，全站加速节点会根据您预设的防盗链黑名单或白名单，对访客的身份进行过滤。符合规则的用户可以顺利请求到资源，不符合规则的用户，请求会返回403响应码。

> 注意
>
> - 防盗链是可选配置，默认不启用。
> - 黑白名单互斥，同一时间您只能选择一种方式。
> - 配置防盗链后，全站加速支持自动添加泛域名。例如，如果您填写a.com，则最终配置生效的是*.a.com，所有子级域名都会生效。
> - 您可以设置是否允许空Referer字段访问资源，即允许通过浏览器地址栏直接访问资源URL。

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**Referer防盗链**页签，打开**Referer防盗链**开关。
6. 根据界面提示，设置**黑名单**或**白名单**。

参数	说明
Referer类型	Refer防盗链类型如下： ○ **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。 黑名单和白名单互斥，同一时间只支持其中一种方式生效。
规则	使用回车符分隔多个Refer黑名单或白名单，支持通配符如 `a.*b.com` ，可以匹配到 `a.aliyun.b.com` 或 `a.img.b.com` 等。

7. 单击**确定**。

8.3. URL鉴权配置

8.3.1. 配置URL鉴权

URL鉴权功能主要用于保护用户站点的内容资源不被非法站点下载盗用。通过Referer防盗链功能添加Referer黑名单和白名单的方式可以解决一部分盗链问题。由于Referer内容可以伪造，所以Referer防盗链功能无法彻底保护您的站点资源，您可以采用URL鉴权方式保护源站资源，确保源站资源安全有效。

背景信息

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。

- 全站加速客户站点提供加密URL，URL中包含权限验证信息。
- 用户使用加密后的URL向加速节点发起请求。
- 加速节点对加密URL中的权限信息进行验证，判断请求的合法性。正常响应合法请求，拒绝非法请求。

如果您想了解Python鉴权代码示例，请参见鉴权示例。

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**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
鉴权类型	阿里云全站加速兼容并支持三种鉴权方式。您可以根据自己的业务情况，选择合适的鉴权方式，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。

8. 单击**确定**。

后续步骤

生成鉴权URL的操作方法如下：

1. 在**生成鉴权测试URL**区域，配置**原始URL**和鉴权信息。

参数	说明
原始URL	您可以输入完整的原始URL地址，例如：`https://www.aliyun.com`。
鉴权类型	您可以根据所需，选择合适的URL鉴权类型： ○ 鉴权方式A说明 ○ 鉴权方式B说明 ○ 鉴权方式C说明
鉴权KEY	您可以根据所需，设置鉴权密码。**鉴权KEY**是**鉴权URL设置**中配置的**主KEY**或**备KEY**。
有效时间	您可以根据所需，设置URL鉴权的有效时长。单位为秒，例如1800。

2. 单击**开始生成**，即可获得**鉴权URL**和**时间戳**。

8.3.2. 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。

阿里云全站加速鉴权 全站加速鉴权

原理说明

访问加密URL构成：

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

鉴权字段描述如下表所示。

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

全站加速服务器接到资源访问请求后，首先判断请求中的 timestamp 是否小于当前时间。

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

  HashValue 是通过以下字符串计算所得。

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

示例说明

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。

1. 通过 `req_auth` 请求对象。

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

2. 设置密钥为：aliyuncdnexp1234。
3. 设置鉴权配置文件有效时间为：2015年10月10日00:00:00，计算出秒数为：1444435200。
4. 全站加速服务器会构造一个用于计算 `Hashvalue` 的签名字符串。

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

5. 根据该签名字符串，全站加速服务器会计算出 `Hashvalue` 。

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

6. 加密URL请求。

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

如果计算出来的 `HashValue` 值与请求中带的 `md5hash` 值相同，都为*80cd3862d699b7118eed99103f2a3a4f*，则鉴权通过；反之鉴权失败。

8.3.3. 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。

阿里云全站加速鉴权 全站加速鉴权

原理说明

访问加密URL格式：

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

当鉴权通过时，实际回源的URL格式：

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

鉴权字段描述如下表所示。

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

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。

1. 回源请求对象。

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

2. 密钥为：aliyuncdnexp123。
3. 访问源服务器时间为： 201508150800。
4. 全站加速服务器构造一个用于计算 `Hashvalue` 的签名字符串。

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

5. 服务器根据签名字符串 `Hashvalue` 计算 `md5hash` 。

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

6. 加密URL请求。

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

如果计算出来的 `md5hash` 值与请求中带的 `md5hash` 值相同，都为*9044548ef1527deadafa49a890a377f0*，则鉴权通过；反之鉴权失败。

8.3.4. 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。

阿里云全站加速鉴权 全站加速鉴权

原理说明

访问加密URL格式如下：

- 格式1

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

- 格式2

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

> **说明** {} 中的内容表示在标准URL基础上添加的加密信息。

鉴权字段描述如下表所示。

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 / 开头。
timestamp	访问源服务器时间，取UNIX时间。未加密的字符串，以明文表示。固定长度10，1970年1月1日以来的秒数，表示为十六进制。
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。

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。

- PrivateKey取值：`aliyuncdnexp1234`。
- FileName取值：`/test.flv`。
- timestamp取值：`55CE8100`。
- md5hash计算值为：

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

- 生成加密URL：
  - 格式一：

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

  - 格式二：

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

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

1. 使用原始的URL中的`Filename`、请求时间及`PrivateKey`进行md5加密得到一个加密串2。
2. 比较加密串2与加密串1是否一致，如果不一致则拒绝。
3. 取加速节点服务器当前时间，并与从访问URL中所带的时间相减，判断是否超过设置的时限t，时间域值

t默认为1800s。

- 时间差小于设置时限，请求合法，全站加速节点正常响应。
- 时间差大于设置时限，拒绝该请求，并返回HTTP 403。

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

8.4. 配置IP黑白名单

您可以通过配置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，提升全站加速的安全性。通过本文您可以了解IP黑名单和白名单的配置方法。

背景信息

配置IP黑名单和白名单功能说明如下：

- IP黑名单：黑名单内的IP均无法访问当前资源。

  如果您的IP被加入黑名单，该IP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IP请求记录。
- IP白名单：只有白名单内的IP能访问当前资源，白名单以外的IP均无法访问当前资源。

> **说明**
>
> - IP黑名单和白名单均支持IPv6地址，例如：2001:db8:0:23:8:800:200c:417a或2001:0db8:0000:0023:0008:0800:200c:417a。IPv6地址不支持缩写格式，例如：2001:0db8::0008:0800:200c:417a。
> - IP黑名单和白名单均支持IP网段添加。例如：192.168.0.0/24，24表示采用子网掩码中的前24位有效位，即用32-24=8bit来表示主机号，该子网可以容纳2^8-2=254台主机。所以192.168.0.0/24表示IP网段范围：192.168.0.1~192.168.0.254。

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

参数	说明
名单类型	IP名单类型如下： ○ **黑名单** 黑名单内的IP均无法访问当前资源。 ○ **白名单** 只有白名单内的IP能访问当前资源，白名单以外的IP均无法访问当前资源。 黑名单和白名单互斥，同一时间只支持其中一种方式生效。
规则	最多配置100个IP地址，使用回车符分隔。不可配置重复网段，例如：`192.168.0.1/24`。

7. 单击**确定**，完成配置。

8.5. 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

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

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

  如果您的User-Agent字段被加入黑名单，该带有User-Agent字段的请求仍可访问到全站加速节点，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。
- User-Agent白名单：只有白名单内的User-Agent字段才能访问当前资源，白名单以外的User-Agent字段均无法访问当前资源。

操作步骤

1. 登录全站加速控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**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

参数	说明
名单类型	User-Agent名单类型如下： ○ **黑名单** 黑名单内的User-Agent字段均无法访问当前资源。 ○ **白名单** 只有白名单内的User-Agent字段能访问当前资源，白名单以外的User-Agent字段均无法访问当前资源。 黑名单和白名单互斥，同一时间只支持其中一种方式生效。
规则	配置User-Agent字段时，用|分割多个值，支持通配符号*。例如：`*curl*|*IE*|*chrome*|*firefox*`。

7. 单击**确定**。

9.性能优化

9.1. 概述

您可以通过设置加速域名的性能优化功能，缩小访问文件的体积，提升加速效率和页面可读性。

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	当您开启页面优化功能时，全站加速自动清除HTML页面冗余的注释和重复的空白符，缩小文件体积，提升页面可阅读性。
智能压缩	当您开启智能压缩功能时，全站加速自动对静态文件进行Gzip压缩。通过智能Gzip压缩方式，可以有效减小传输文件大小，提升加速效率。
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。
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。

9.2. 页面优化

当您开启页面优化功能时，全站加速自动清除HTML页面冗余的注释和重复的空白符，缩小文件体积，提升页面可阅读性。本文为您详细介绍开启页面优化功能的方法。

背景信息

开启页面优化功能后，全站加速自动删除当前域名下所有HTML页面中冗余的注释和重复的空白符，这样可以有效地去除页面的冗余信息，减小文件体积，提高加速分发效率。

如果源站文件配置了MD5校验机制，则请勿开启该功能。当全站加速进行页面优化时，该文件的MD5值会被更改，导致优化后文件的MD5值和源站文件的MD5值不一致。

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，打开**页面优化**开关。

9.3. 智能压缩

当您开启智能压缩功能时，全站加速自动对静态文件进行Gzip压缩。通过智能Gzip压缩方式，可以有效减小传输文件大小，提升加速效率。本文为您详细介绍开启智能压缩功能的方法。

背景信息

- 目前智能压缩支持的内容格式：text/html 、text/xml 、text/plain 、text/css 、application/javascript 、application/x-javascript 、application/rss+xml 、text/javascript 、image/tiff 、image/svg+xml 、application/json 、application/xmltext 。
- 客户端请求携带请求头 Accept-Encoding: gzip ：客户端希望获取对应资源的gzip压缩响应。
- 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
>
> - 如果源站文件配置了MD5校验机制，则请勿开启该功能。当全站加速对静态文件进行压缩优化时，该文件的MD5值会被更改，导致压缩优化后文件的MD5值和源站文件的MD5值不一致。
> - 只有当源站文件大小超过1024B时，全站加速才会进行Gzip压缩。
> - Internet Explorer 6对Gzip的兼容性较差，如果有Internet Explorer 6的访问需求，不建议开启智能压缩功能。

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。

9.4. 过滤参数

如果您的URL请求中携带大量参数，需要忽略参数浏览文件时，则可以开启过滤参数，过滤携带参数的URL返回源站，提高缓存命中率。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。

  开启过滤参数后，请求URL到全站加速节点后，会截取到没有该参数请求的URL，且全站加速节点仅保留一份副本。

  - 如果您的URL请求中携带大量问号（ ? ）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://www.****.com/1.jpg ，全站加速没有缓存，直接回源访问数据；第二次访问 http://www.****.com/1.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CDN缓存 http://www.****.com/1.jpg 。
  - 如果您的HTTP请求中的参数有重要含义，例如，包含文件版本信息等，则推荐您将该参数设置为保留过滤参数。您最多可以设置10个保留参数，如果请求URL中包含您设置的保留参数，则会携带该参数回源。

- 关闭过滤参数。

当每个URL都缓存不同的副本在全站加速节点上。

如果您的URL请求中携带 ?*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，您访问URL会精确匹配 ? 之后的参数，提高请求的精确性。例如：第一次访问 http://www.****.com/1.jpg ，全站加速没有缓存，直接回源访问数据；第二次访问 http://www.****.com/1.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://www.****.com/1.jpg ，需要重新回源获取 http://www.****.com/1.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. 在**过滤参数**区域，打开**过滤参数**开关，配置**过滤参数**。

   > **说明** 打开**过滤参数**开关后，资源回源时会去除URL中 ? 之后的参数，提升文件缓存命中率。

参数	说明
保留参数	配置需要保留的参数。最多可以配置10个保留参数，用半角逗号分隔 。例如： http://www.abc.com/a.jpg?x ，**保留参数**配置为 x 。

   示例说明：

   全站加速节点向源站发起请求 http://www.abc.com/a.jpg?x ， x 保留。所有类似的请求 http://www.abc.com/a.jpg?x 均响应全站加速副本 http://www.abc.com/a.jpg?x 的内容。

6. 单击**确定**。

9.5. 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/video.mp4?start=10` 就是从第10秒开始播放视频。
FLV	源站视频必须带有meta信息。	start参数表示字节，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。

10.Websocket

10.1. 概述

通过本文您可以了解Websocket的概念、优势和使用场景。

什么是Websocket

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

Websocket的优势

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。
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。

10.2. 配置Websocket

Websocket协议使客户端和服务器之间的数据交换变得更加简单，允许服务端主动向客户端推送数据。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。通过本文您可以了解开通和配置Websocket的操作方法。

操作步骤

1. 开通Websocket。您需要通过指定Websocket计费类型并且计费类型生效后，才能正式使用Websocket功能。开通Websocket的操作方法请参见开通全站加速服务。

   > **说明**
   > - 如果您是新用户，则Websocket计费立即生效。
   > - 如果您是老用户，且全站加速的计费类型为**按日计费**，则生效时间为第二个自然日零点；如果您全站加速计费类型为**按月计费**，则生效时间为次月1日零点。

2. 配置Websocket。
   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**Websocket**。
   v. 打开**Websocket**开关。
   vi. 单击**修改配置**。

vii. 在**Websocket设置**对话框，配置**心跳时间**和**回源协议**。

参数	说明
心跳时间	心跳时间是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。平台心跳时间默认60秒。心跳时间建议配置规则：A<=B<=C。 **说明** A：客户端心跳时间，B：全站加速平台心跳时间，C：源站心跳时间。 如果客户端心跳时间大于服务端的心跳时间，会导致用户端还处于活跃状态，而服务端已经断开链接，导致服务异常。例子：假设A的时间为80秒，B的时间为60秒，C的时间为80秒。当第61秒没有数据传输，B的心跳时间60秒已经过了，而A在第70秒发起状态同步，而B已经断开了；则会导致服务过程异常。
回源协议	Websocket协议回到源站时需要遵循的协议类型。 ■ HTTP Websocket以HTTP协议回源。 ■ HTTPS Websocket以HTTPS协议回源。 ■ 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。

viii. 单击**确定**，完成配置。

11.高级配置

11.1. 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。