ALIBABA CLOUD

阿里云

安全加速 SCDN
用户指南

文档版本：20220111

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.SCDN控制台介绍

您可以在SCDN控制台完成域名配置等基本操作，也可以通过资源监控服务进行实时数据分析，同时您还可以了解自己的计费情况，随时变更计费方式。本文主要为您介绍SCDN控制台相关功能。

控制台功能概览

登录SCDN控制台，首页展示了您当前阿里云账号下SCDN的运行概况，SCDN控制台界面展示如下图所示。

序号	区域	说明
①	左侧导航栏	SCDN域名导航栏，包含域名管理、资源管理、安全监控、统计分析、用量查询等功能。
②	昨日基础数据	SCDN根据您服务的计费方式，展示计费项中的使用数据。
③	其他加速产品	您可以了解与SCDN相关的其他加速产品。
④	计费方式	展示您已经选择的计费方式，您也可以根据所需快速修改计费方式。
⑤	总域名	您可以通过快速入口对域名进行管理或添加域名。

2.回源配置

2.1. 回源HOST

自定义在SCDN节点回源时要访问的Web服务器域名。

背景信息

源站：源站决定了回源时，请求到哪个IP。

回源HOST：回源HOST决定回源请求访问到该IP上的哪个站点。

根据源站类型不同，分为以下两种情况：

- 源站是域名。源站为 `www.example.com` ，回源HOST为 `www.aliyundoc.com` ，那么实际回源的是 `www.example.com` 解析到的IP，对应的主机上的站点 `www.aliyundoc.com` 。
- 源站是IP。源站为 `10.10.10.10` ，回源HOST为 `www.aliyundoc.com` ，那么实际回源的是 `10.10.10.10` 对应的主机上的站点 `www.aliyundoc.com` 。

> **注意**
>
> 目前不支持SNI回源。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**配置**。
4. 在左侧导航栏选择**回源配置**，修改回源HOST的配置。

> 说明
>
> 回源HOST为可选配置项，默认值为：
>
> - 如果源站是IP类型，回源HOST默认是加速域名。
> - 如果源站是OSS源站类型，回源HOST默认是源站域名。

2.2. 协议跟随回源

开启该功能后，回源使用协议和客户端访问资源的协议保持一致，即如果客户端使用 HTTPS 方式请求资源，SCDN节点会使用相同的 HTTPS 方式回源获取资源。HTTP请求同理。

> **注意** 源站需要同时支持 80 端口和 443 端口，否则会造成回源失败。

操作步骤

1. 进入SCDN**域名管理**页，选择相应域名进入**配置**页：

2. 选择**回源配置**，可进行协议跟随回源的开启和关闭：

2.3. 开启私有Bucket回源授权

当您的源站为OSS时，可以开通加速域名访问私有OSS Bucket资源的权限，有效防止资源盗链。本文为您介绍开启私有Bucket回源授权的操作方法。

背景信息

私有Bucket回源授权是指加速域名如果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功能后，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SCDN提供的Refer防盗链和鉴权功能，有效保护您的资源安全，具体请参见防盗链和鉴权配置。

> **注意**
>
> - 仅支持源站类型为OSS域名的加速域名开启私有Bucket回源授权功能，开启回源授权后即授权SCDN对所有Bucket的只读权限。
> - 开启对应域名的私有Bucket回源授权功能后，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SCDN域名的回源内容，请勿开启此功能。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，定位目标域名，在目标域名右侧单击**配置**。

4. 在指定域名的左侧导航栏，单击**回源配置**。
5. 找到**私有Bucket回源**，打开**私有Bucket回源**开关即可。

2.4. 配置回源SNI

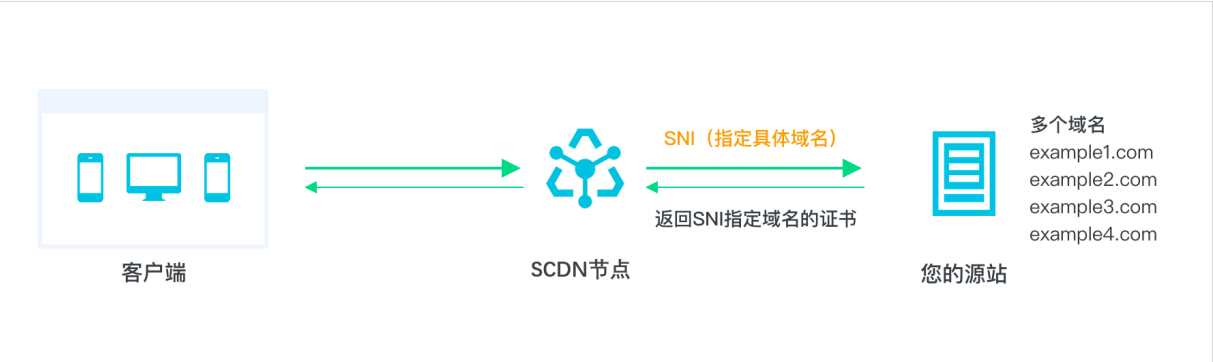
如果您的源站IP绑定了多个域名，当SCDN节点以HTTPS协议访问您的源站时，您需要设置回源SNI，指明具体访问的域名。

背景信息

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SCDN设置了443端口回源（SCDN节点以HTTPS协议访问您的服务器），此时您需要设置回源SNI，指明所请求的具体域名。当SCDN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。



回源SNI的工作流程如下：

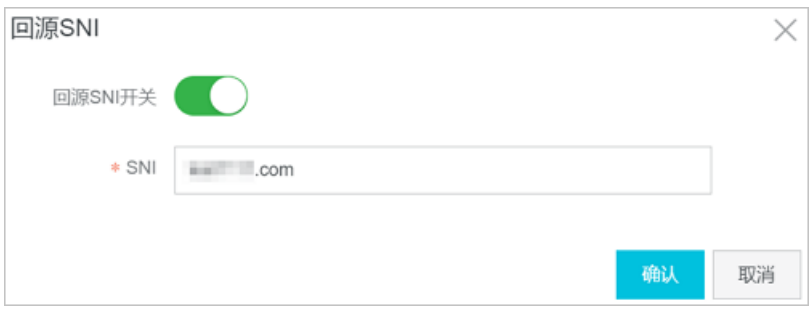
1. SCDN节点以HTTPS协议访问源站时，在SNI中指定访问的域名。
2. 源站接收到请求后，根据SNI中记录的域名，返回对应域名的证书。
3. SCDN节点收到证书后与服务器端建立安全连接。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，定位目标域名，在目标域名右侧单击**配置**。

4. 在指定域名的左侧导航栏，单击**回源配置**。
5. 找到**回源SNI**，单击**修改配置**。
6. 在**回源SNI**对话框，打开**回源SNI开关**，输入服务器源站提供服务的域名。

> **说明** SNI在阿里云SCDN产品中指源站域名。如果您的源站服务器使用单个IP地址为多个域名提供HTTPS服务，则需要设置回源SNI，指明所请求的具体域名，例如：example.com。



7. 单击**确认**，完成配置。

2.5. 多源优先级设置

阿里云SCDN支持三种类型回源域名，包括OSS回源域名、IP和自定义域名。其中**IP**和**自定义域名**支持多IP或多域名设置，并支持用在多源站场景下进行回源优先级设置。

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

用户所有回源流量将首先回源优先级高的源站。如果某个源站健康检查连续3次失败，则所有流量将选择优先级第二的源站回源。如果主动健康检查成功，该源站会重新标记为可用，恢复原来的优先级。当所有源站回源优先级一样时，SCDN将自动轮询回源。

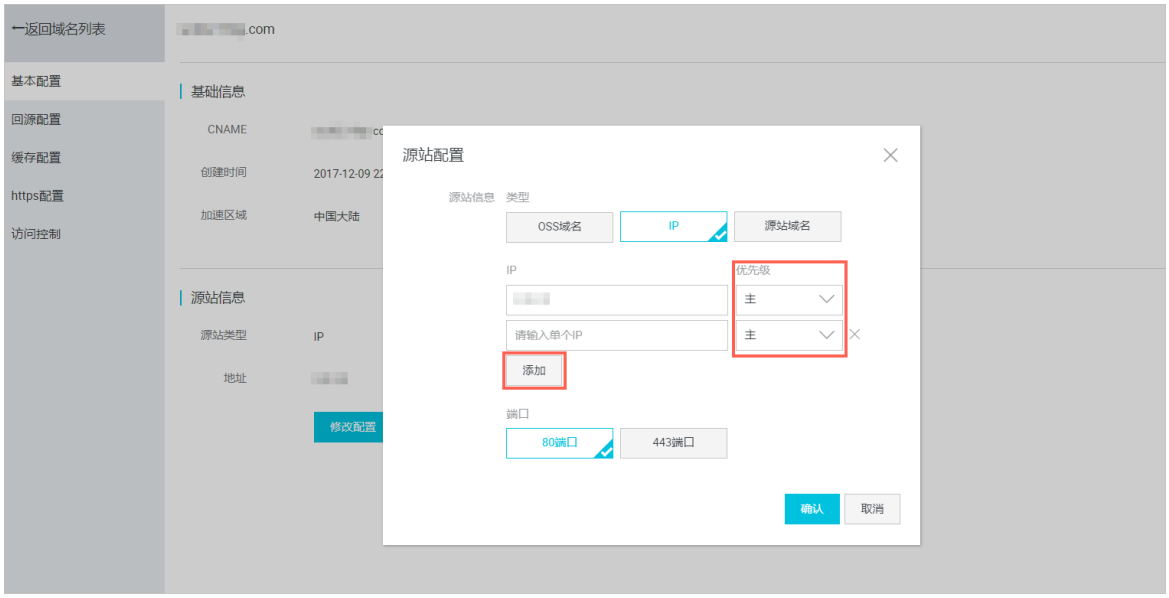
源站健康检查：实行主动四层健康检查机制，每5秒主动健康检查一次。

主要支持场景：主备方式切换源站。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，单击目标域名对应的**配置**。
4. 在左侧导航栏选择**基本配置**，在**源站信息**区域，单击**修改配置**。

5. 添加多源站，并设置主备优先级。


←返回域名列表
基本配置
回源配置
缓存配置
https配置
访问控制
基础信息
CNAME
创建时间
加速区域
中国大陆
源站信息
源站类型
IP
地址
修改配置
源站配置
源站信息
类型
OSS域名
IP
源站域名
IP
优先级
主
请输入单个IP
主
添加
端口
80端口
443端口
确认
取消

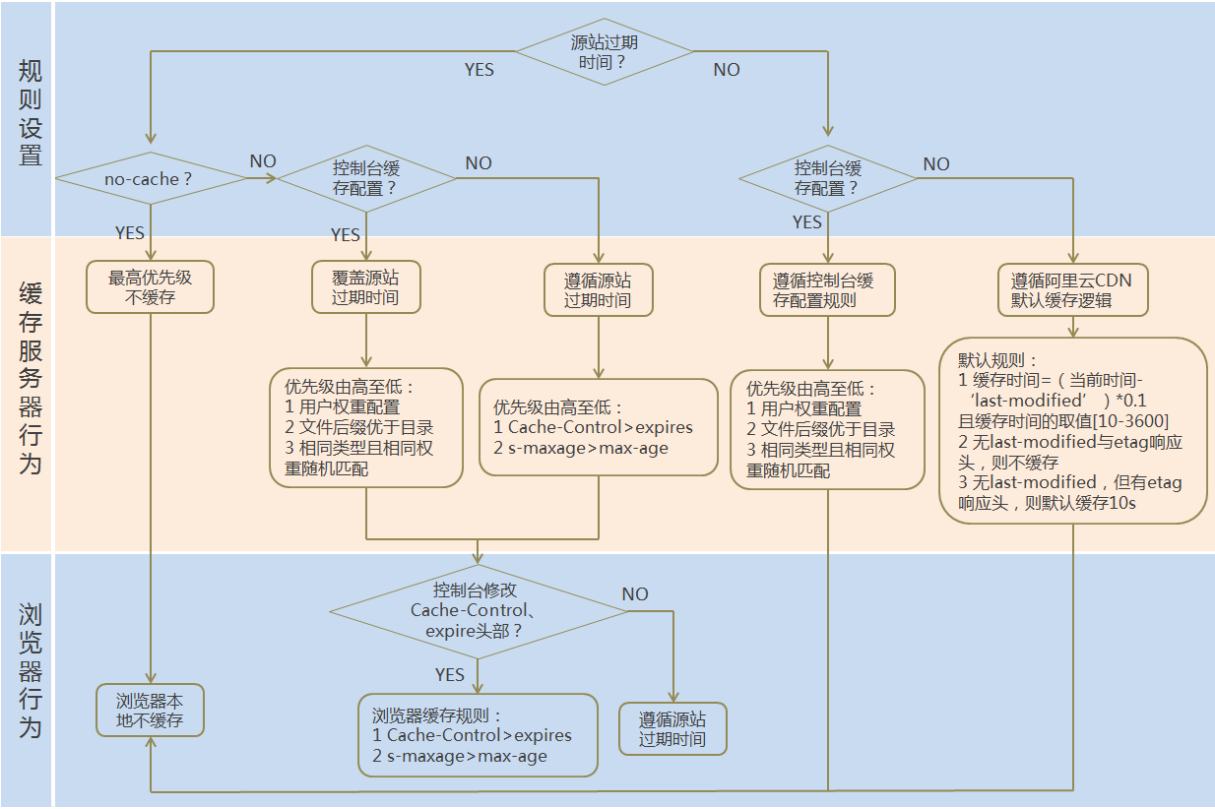
3.缓存配置

3.1. 缓存配置

通过本文您可以详细了解缓存配置的功能介绍和操作步骤。

功能介绍

- 该功能可以针对不同“目录路径”和“文件名后缀”的资源进行Cache节点行为的设置，您可以自定义指定资源内容的缓存过期时间规则。
- 支持用户自定义缓存策略优先级。
- Cache的默认缓存策略。



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

注意事项

- 对于不经常更新的静态文件，建议将缓存时间设置为1个月以上（eg：图片类型，应用下载类型）。
- 对于需要更新并且更新很频繁的静态文件，可以将缓存时间设置短些，视业务情况而定（eg：js,css等）。

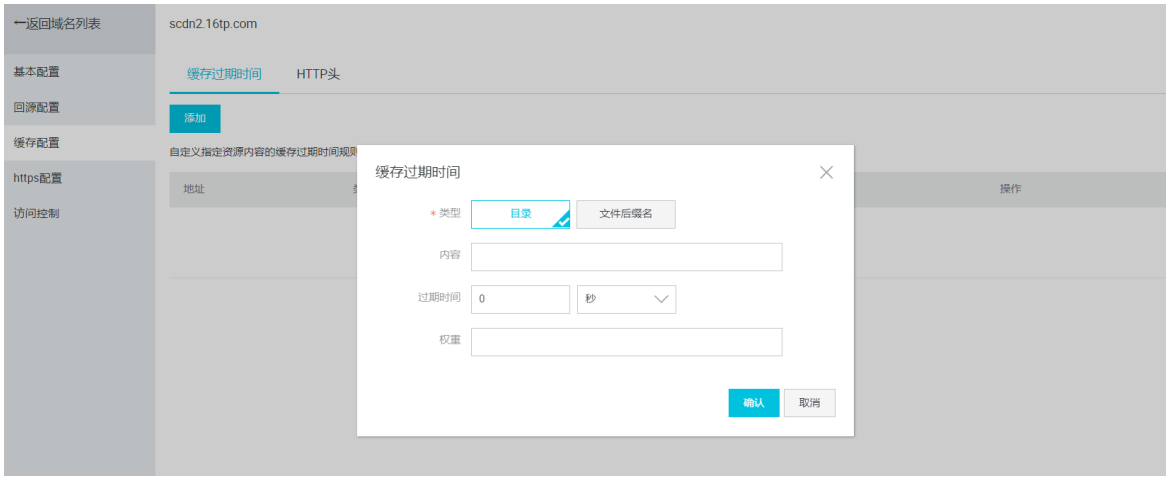
- 对于动态文件（eg：php|jsp|asp），建议设置缓存时间为0s，即不缓存；若动态文件内容更新频率较低，例如php文件，推荐设置较短缓存时间。
- 建议源站的内容不要使用同名更新，以版本号的方式方步，即采用img-v1.0.jpg、img-v2.1.jpg的命名方式。

操作步骤

1. 在SCDN**域名管理**页，选择相应域名进入**配置**页面。

2. 选择**缓存配置**，可以对缓存规则进行添加、修改、删除。

3. 单击**添加**，增加缓存规则，按目录或者按文件后缀。



举例：为加速域名 `example.aliyundoc.com` 设置三则缓存配置规则：

- 缓存策略1：文件名后缀为 `jpg、png` 的所有资源过期时间为1月，权重设置为90。

- 缓存策略2：目录为 `/www/dir/aaa` 过期时间为1小时，权重设置为70。
- 缓存策略3：完整路径为 `/www/dir/aaa/example.php` 过期时间为0s，权重设置为80。

则这三个缓存策略的生效顺序是：策略1-->策略3-->策略2。权重可设置1~99，数字越大优先级越高，优先生效；不推荐设置相同的权重，权重相同的两条缓存策略优先级随机。

3.2. 设置HTTP头

通过本文您可以详细了解HTTP头设置的功能介绍和操作步骤。

功能介绍

您可以设置HTTP响应头，目前提供9个HTTP请求头参数供您自行定义取值，参数解释如下。

参数	说明
Content-Type	指定客户程序响应对象的内容类型。
Cache-Control	指定客户程序请求和响应遵循的缓存机制。
Content-Disposition	指定客户程序响应对象时激活文件下载设置默认的文件名。
Content-Language	指定客户程序响应对象的语言。
Expires	指定客户程序响应对象的过期时间。
Access-Control-Allow-Origin	指定允许的跨域请求的来源。
Access-Control-Allow-Methods	指定允许的跨域请求方法。
Access-Control-Max-Age	指定客户程序对特定资源的预取请求返回结果的缓存时间。
Access-Control-Expose-Headers	指定允许访问的自定义头信息。

注意事项

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

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，定位目标域名，在目标域名右侧单击**配置**。

4. 在指定域名的左侧导航栏，单击**缓存配置**。
5. 单击**HTTP头**页签。
6. 在**HTTP头**页签下，单击**添加**。
7. 在**HTTP头设置**对话框，自定义设置HTTP头的参数和取值。
8. 单击**确认**，完成配置。

3.3. 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HTTPS响应返回码跳转的完整URL地址。本文为您介绍自定义错误页面的配置方法。

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。本文以返回错误码404为例，为您介绍默认页面和自定义页面的差异。

-

> 说明
>
> -
> - 自定义页面如果使用的是CDN加速的资源，那么将会按照正常的CDN内容分发来计费。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，定位目标域名，在目标域名右侧单击**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**。
7. 在**自定义页面**对话框，配置自定义页面的**错误码**和**链接**。

   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 `example.aliyundoc.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://example.aliyundoc.com/error404.html` 。

8. 单击**确认**，完成配置。

   在**自定义页面**列表中，您可以单击**修改**或**删除**，修改或删除当前的配置。

3.4. 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。本文为您介绍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SCDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，定位目标域名，在目标域名右侧单击**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. 在**重写**页签下，单击**添加**。
7. 在**Rewrite设置**对话框，根据您的需求，配置**待重写URI**和**目标URI**，并选择**执行规则**。

> **说明** 单个域名最多可添加50条重写规则。

参数	示例	说明
待重写URI	`/example/image/image_01.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	`/example/image/image_02.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。

8. 单击**确认**，完成配置。

在**重写**列表中，您可以单击**修改**或**删除**，修改或删除当前的配置。

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://example.com/hello`，SCDN节点将返回302让客户端重新请求 `http://example.com/index.html` 的内容。
样例二	^/hello$	/index.html	Break	客户端请求 `http://example.com/hello`，SCDN节点将返回 `http://example.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	待重写URI	目标URI	执行规则	结果说明
样例三	^/$	/index.html	Redirect	客户端请求 `http://example.com` ，SCDN节点将返回302让客户端重新请求 `http://example.com/index.html` 的内容。
样例四	/hello	/hello/index.html	Redirect	客户端请求 `http://example.com/hello` ，SCDN节点将返回302让客户端重新请求 `http://example.com/hello/index.html` 的内容。

4.HTTPS配置

4.1. HTTPS配置

通过本文您可以详细了解HTTPS配置的功能介绍和操作步骤。

功能介绍

- 安全超文本传输协议HTTPS（Hyper Text Transfer Protocol over Secure Socket Layer）是以安全为目标的HTTP通道，可以简单理解为是HTTP的安全版。即将HTTP用SSL/TLS协议进行封装，HTTPS的安全基础是SSL/TLS。
- HTTPS加速优势：
  - 传输过程中对用户的关键信息进行加密，防止类似Session ID或者Cookie内容被攻击者捕获造成的敏感信息泄露等安全隐患。
  - 传输过程中对数据进行完整性校验，防止DNS或内容遭第三方劫持、篡改等中间人攻击（MITM）隐患，更多信息，请参见使用HTTPS防止流量劫持。
- 阿里云SCDN提供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和私钥，并支持对证书进行查看、停用、启用和编辑操作。推荐您直接在阿里云云盾快速申请**免费的证书**或购买高级证书，阿里云云盾购买的证书可直接在CDN控制台选择，免手动上传证书。
- 证书配置正确及开启状态，同时支持HTTP访问和HTTPS访问；证书不匹配或者停用证书，仅支持HTTP访问。

> **说明**
>
> 目前不支持SNI回源。

注意事项

配置相关

- 支持泛域名HTTPS服务。
- 支持该功能的“停用”和“启用”：
  - 启用：支持修改证书，默认兼容用户的HTTP和HTTPS请求。
  - 停用：不支持HTTPS请求且不再保留证书和私钥信息，再次开启证书，需要重新上传证书和私钥。
- 允许用户查看证书，但是只支持查看证书，由于私钥信息敏感不支持查看私钥，请妥善保管证书相关信息。
- 支持修改编辑证书，但注意生效时间是10分钟，请慎重操作。

证书相关

- 自定义上传证书包含证书和私钥，均为PEM格式，详细信息，请参见证书格式说明。

> **说明**
>
> SCDN采用的Tengine服务基于Nginx，因此只支持Nginx能读取的证书，即PEM格式。

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

操作步骤

1. 购买证书。

   开启HTTPS安全加速，需要您具备匹配加速域名的证书。您可以在云盾证书服务购买证书。

2. 加速域名配置。

   在SCDN**域名管理**页，选择相应域名进入**配置**页。

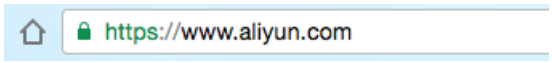
3. 单击**HTTPS配置**。

4. 进行HTTPS的**开关**及证书的**上传**和**更换**。

- 在云盾证书服务购买过的证书，可以通过证书名称直接选择适配该加速域名。
- 若证书列表中无当前适配的证书可以选择自定义上传，需要设置证书名称后上传证书内容和私钥，该证书将会在云盾证书服务中保存，可以在“我的证书”中查看。
- 自定义上传证书仅支持PEM的证书格式，更多信息，请参见证书格式说明。

5. 验证证书是否生效。

   设置完成待证书生效后（设置HTTPS证书后约10分钟后生效），使用HTTPS方式访问资源，如果浏览器中出现绿色HTTPS标识，表明当前与网站建立的是私密连接，HTTPS安全加速生效。



4.2. 证书格式说明

SCDN开启HTTPS需上传您的证书，且只支持 `PEM` 格式证书。本文为您介绍阿里云SCDN支持的证书格式和不同证书格式间的转换方式。

常用证书申请流程

1. 本地生成私钥。

   本地生成私钥 `openssl genrsa -out privateKey.pem 2048` ，其中 `privateKey.pem` 为您的私钥文件，请妥善保管。

2. 生成证书请求文件。

   生成证书请求文件 `openssl req -new -key privateKey.pem -out server.csr` ，其中 `server.csr` 是您的证书请求文件，可用证书请求文件去申请证书。

3. 获取请求文件中的内容并前往CA等机构申请证书。

Root CA机构颁发的证书

Root CA机构颁发的证书是唯一的，一般包括Apache、IIS、Nginx和Tomcat。阿里云SCDN使用的证书是Nginx，证书格式为 `.crt` ，证书私钥格式为 `.key` 。

证书上传格式要求如下：

- 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。

在Linux环境下， `PEM` 格式的证书示例如下图所示。

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：服务器证书放第一份，中间证书放第二份，中间不能有空行。通常证书颁发机构在颁发证书时会有相应的说明，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-----
```

证书链规则要求如下：

- 证书之间不能有空行。
- 每一份证书需遵守证书上传的格式说明。

RSA私钥格式要求

RSA私钥规则：

- 本地生成私钥为 `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。

如果您不是按照上述方案生成私钥，得到 `-----BEGIN PRIVATE KEY-----` 或 `-----END PRIVATE KEY-----` 样式的私钥时，您可以按照如下方式转换，然后将 `new_server_key.pem` 的内容与证书一起上传。

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

证书格式转换方式

SCDN HTTPS安全加速只支持PEM格式的证书，其他格式的证书需要转换成PEM格式，建议您通过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SCDN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
```

其它证书相关问题

- 只支持带SNI信息的SSL/TLS握手。
- 您上传的证书和私钥要匹配，否则校验会出错。
- 更新证书的生效时间是10分钟。
- 不支持带密码的私钥。

4.3. 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。本文为您介绍HTTP/2协议的概念、优势和开启HTTP/2的操作方法。

前提条件

您已成功配置HTTPS证书，具体操作请参见HTTPS配置。

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

背景信息

HTTP/2即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、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等浏览器已支持HTTP/2协议。

HTTP/2有以下优势：

- 二进制协议：相对于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，并对其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）：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SCDN控制台。
2. 在左侧导航栏，单击**域名管理**。

3. 在**域名管理**页面，定位目标域名，在目标域名右侧单击**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**开关即可。

4.4. 配置强制跳转

配置HTTPS证书时如果您使用了Nginx证书，则需要将HTTP强制跳转到HTTPS。您也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。本文为您介绍配置强制跳转的方法。

前提条件

您已成功配置HTTPS证书，具体操作请参见HTTPS配置。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，定位目标域名，在目标域名右侧单击**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。您也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。

7. 单击**确认**，完成配置。

执行结果

下面以**跳转类型**为**HTTP -> HTTPS**为例，为您介绍强制跳转功能。

4.5. 配置TLS

为了保障互联网通信的安全性和数据完整性，SCDN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。本文为您介绍TLS协议的配置方法。

前提条件

您已成功配置HTTPS证书，具体操作请参见HTTPS配置。

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，最典型的应用为HTTPS。HTTPS即HTTP over TLS，是安全的HTTP，运行在TCP层之上，HTTP层之下，为HTTP层提供数据加密和解密服务。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，定位目标域名，在目标域名右侧单击**配置**。

4. 在指定域名的左侧导航栏，单击**HTTPS配置**。
5. 在**TLS版本控制**区域，根据所需开启或关闭对应的TLS版本。

   TLS协议说明如下表所示。

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

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

4.6. 配置HSTS

开启HSTS功能后您可以强制客户端使用HTTPS与服务器创建连接，帮助网站进行全局加密，降低第一次访问被劫持的风险。

前提条件

您已成功配置HTTPS证书，具体操作请参见HTTPS配置。

背景信息

HSTS（HTTP Strict Transport Security）是国际互联网工程组织IETE推行的Web安全协议，通过强制客户端（例如浏览器等）使用HTTPS与服务器创建连接，帮助网站进行全局加密。

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。该操作过程中请求可能被劫持，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，HSTS的响应头结构为：`Strict-Transport-Security: max-age=expireTime [; includeSubDomains] [; preload]`，具体参数说明如下表所示。

参数	说明
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。
max-age	HSTS Header的过期时间，单位为秒。
includeSubDomains	可选参数。如果指定这个参数，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的内置列表时需要使用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。
> - HSTS仅对域名和403端口有效，对IP和其他端口无效。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，定位目标域名，在目标域名右侧单击**配置**。

4. 在指定域名的左侧导航栏，单击**HTTPS配置**。
5. 在**HSTS**区域，单击**修改配置**。
6. 打开**HSTS**开关，根据您的实际需求，配置**过期时间**和**包含子域名**。
7. 单击**确认**，完成配置。

5.访问控制

5.1. 防盗链

通过本文您可以详细了解防盗链的功能介绍和操作步骤。

功能介绍

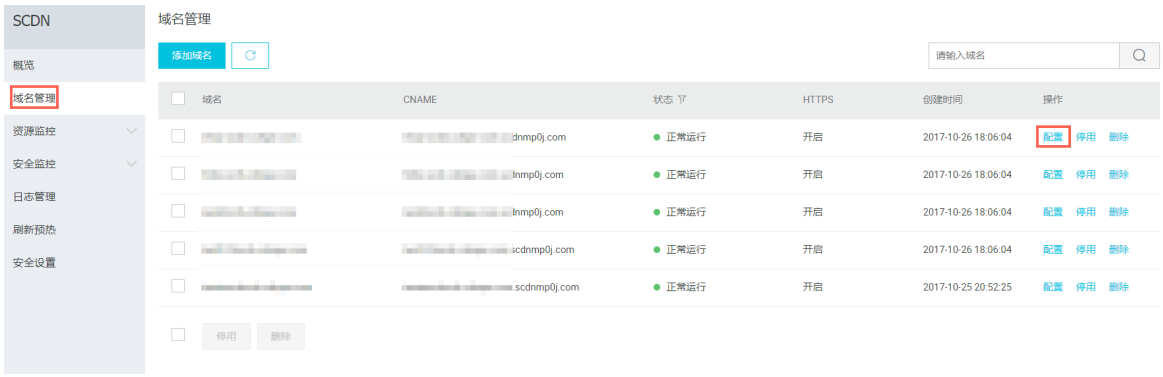
- 防盗链功能基于 HTTP 协议支持的 Referer 机制，通过 referer 跟踪来源，对来源进行识别和判断，用户可以通过配置访问的 referer 黑白名单来对访问者身份进行识别和过滤，从而限制 SCDN 资源被访问的情况。
- 目前防盗链功能支持黑名单或白名单机制，访客对资源发起请求后，请求到达 SCDN 节点，SCDN节点会根据用户预设的防盗链黑名单或白名单，对访客的身份进行过滤，符合规则可以顺利请求到资源；若不符合规则，该访客请求被禁止，返回403响应码。

注意事项

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

操作步骤

1. 在SCDN**域名管理**页，选择相应的域名进入**配置**页。



2. 选择**访问控制台**，可进行Refer黑白名单的设置。

5.2. 鉴权配置

通过本文您可以详细了解鉴权配置的功能原理和操作步骤。

概述

URL鉴权功能旨在保护用户站点的内容资源不被非法站点下载盗用。采用防盗链方法添加referer黑、白名单方式可以解决部分盗链问题。但由于referer内容可以伪造，referer防盗链方式还不能很好的保护站点资源，因此采用URL鉴权方式保护用户源站资源更为安全有效。

原理

URL鉴权功能是通过阿里云SCDN加速节点与客户资源站点配合实现的一种更为安全可靠的源站资源防盗方法。由SCDN客户站点提供给用户加密URL（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以判断请求的合法性，对合法请求给予正常响应，拒绝非法请求，从而有效保护SCDN客户站点资源。

URL鉴权方式

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

A鉴权方法

原理说明

用户访问加密URL构成

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

鉴权字段描述

- `PrivateKey` 字段用户可以自行设置。
- 有效时间1800s是指，用户访问客户源服务器时间超过自定义失效时间（timestamp字段指定）的1800s后，该鉴权失效；例如用户设置访问时间2020-08-15 15:00:00，链接真正失效时间是2020-08-15 15:30:00。

字段	描述
timestamp	失效时间，整形正数，固定长度10，1970年01月01日以来的秒数。用来控制失效时间，10位整数，有效时间1800s。
rand	随机数，一般设成0。
uid	暂未使用（设置成0即可）。
md5hash	通过MD5算法计算出的验证串，数字和小写英文字母混合0~9、a~z，固定长度32。

SCDN服务器拿到请求后，首先会判断请求中的 `timestamp` 是否小于当前时间，如果小于，则认为过期失效并返回HTTP 403错误。如果 `timestamp` 大于当前时间，则构造出一个同样的字符串（参考以下sstring构造方式）。然后使用MD5算法算出 `HashValue` ，再和请求中带来的 `md5hash` 进行比对。比对结果一致，则认为鉴权通过，返回文件。否则鉴权失败，返回HTTP 403错误。

- `HashValue` 是通过以下字符串计算出来的：

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

示例说明

1. 通过 `req_auth` 请求对象：

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

2. 密钥设为：aliyuncdnexp1234（由用户自行设置）。
3. 鉴权配置文件失效日期为：2015年10月10日00:00:00，计算出来的秒数为1444435200。
4. 则SCDN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. SCDN服务器会根据该签名字符串计算HashValue：

```
HashValue = md5sum("/video/standard/1K.html-1444435200-0-0-aliyuncdnexp1234") = 80cd386
2d699b7118eed99103f2a3a4f
```

6. 则请求时URL为：

```
http://cdn.example.com/video/standard/1K.html?auth_key=1444435200-0-0-80cd3862d699b7118
eed99103f2a3a4f
```

计算出来的HashValue与用户请求中带的md5hash=80cd3862d699b7118eed99103f2a3a4f值一致，于是鉴权通过。

B鉴权方式

原理说明

用户访问加密 URL 格式

- 用户访问的URL如下：

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

加密URL的构造：域名后跟生成URL的时间（精确到分钟）（timestamp）再跟MD5值（md5hash），最后拼接回源服务器的真实路径（FileName），URL有效时间为1800s。

- 当鉴权通过时，实际回源的URL是：

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

鉴权字段描述

- 注意：`PrivateKey`由CDN客户自行设置。
- 有效时间1800s是指，用户访问客户源服务器时间超过自定义失效时间（timestamp字段指定）的1800s后，该鉴权失效；例如用户设置访问时间2020-08-15 15:00:00，链接真正失效时间是2020-08-15 15:30:00。

字段	描述
DomainName	SCDN客户站点的域名
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`
md5hash	以timestamp、FileName和预先设定好的 PrivateKey 共同做MD5获得的字符串，即md5(`PrivateKey` + `timestamp` + `FileName`)
FileName	实际回源访问的URL（注意，鉴权时候FileName要以/开头）

示例说明

1. 回源请求对象：

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

2. 密钥设为：aliyuncdnexp1234（用户自行设置）。
3. 用户访问客户源服务器时间为201508150800（格式为： `YYYYMMDDHHMM` ）。
4. 则CDN服务器会构造一个用于计算md5hash的签名字符串：

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

5. 服务器会根据该签名字符串计算md5hash：

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

6. 请求SCDN时URL:

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

计算出来的md5hash与用户请求中带的md5hash=9044548ef1527deadafa49a890a377f0值一致，于是鉴权通过。

C鉴权方式

原理说明

用户访问加密 URL 格式

格式1: `http://DomainName/{<md5hash>/<timestamp>}/FileName`

格式2: `http://DomainName/FileName{&KEY1=<md5hash>&KEY2=<timestamp>}`

- 花括号中的内容表示在标准的URL基础上添加的加密信息。
- `<md5hash>` 是验证信息经过MD5加密后的字符串。
- `<timestamp>` 是未加密的字符串，以明文表示。固定长度10，1970年01月01日以来的秒数，表示为十六进制。
- 采用格式一进行URL加密，例如：

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

`<md5hash>` 为a37fa50a5fb8f71214b1e7c95ec7a1bd `<timestamp>` 为 55CE8100。

鉴权字段描述

- `<md5hash>` 部分字段描述：

字段	描述
PrivateKey	干扰串，不同客户采用不同的干扰串。
FileName	实际回源访问的URL（注意，鉴权时候path要以/开头）。
time	用户访问源服务器时间，取UNIX时间，以十六进制数字字符表示。

- PrivateKey取值 `aliyuncdnexp1234`。

- FileName取值 `/test.flv`。
- time取值 `55CE8100`。
- 因此md5hash值为：

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

- 明文： `timestamp = 55CE8100`。
- 这样生成加密URL。

格式一：

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

格式二：

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

示例说明

用户使用加密的URL访问加速节点，SCDN服务器会先把加密串1提取出来，并得到原始的URL的 `<FileName>` 部分，用户访问时间，然后按照定义的业务逻辑进行验证：

1. 使用原始的URL中的 `<FileName>` 部分，请求时间及PrivateKey进行MD5加密得到一个加密串2。
2. 比较加密串2与加密串1是否一致，如果不一致则拒绝。
3. 取加速节点服务器当前时间，并与从访问URL中所带的明文时间相减，判断是否超过设置的时限t（时间域值t默认为1800s）。
4. 有效时间1800s是指，用户访问客户源服务器时间超过自定义时间的1800s后，该鉴权失效；例如用户设置访问时间2020-08-15 15:00:00，链接真正失效时间是2020-08-15 15:30:00。
5. 时间差小于设置时限的为合法请求，SCDN节点才会给予正常的响应，否则拒绝该请求，返回http 403错误。

操作步骤

1. SCDN**域名管理**页，选择相应域名进入**配置**页。

2. 选择**访问控制-URL鉴权**。

3. 即可进行鉴权规则设置。

5.3. 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SCDN资源的用户，提升SCDN的安全性。本文为您介绍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均无法访问当前的加速域名。

  如果您的IP被加入黑名单，该IP的请求仍可访问到SCDN节点，但是会被SCDN节点拒绝并返回403，SCDN的日志中仍会记录这些黑名单中的IP请求记录。

- IP白名单：开启白名单功能后，只有白名单内的IP能访问当前的加速域名，白名单以外的IP均无法访问当前的加速域名。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，定位目标域名，在目标域名右侧单击**配置**。

4. 在指定域名的左侧导航栏，单击**访问控制**。
5. 单击**IP黑/白名单**页签。
6. 在**IP黑/白名单**页签下，单击**修改配置**。
7. 在**规则**对话框，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均无法访问当前的加速域名。 ○ 白名单：开启白名单功能后，只有白名单内的IP能访问当前的加速域名，白名单以外的IP均无法访问当前的加速域名。 **说明** 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	最多支持配置100条，使用回车符分隔，不可配置重复网段。 **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:****或2001:0db8:0000:0023:0008:0800:200c:****。IPv6地址不支持缩写格式，例如2001:0db8::0008:0800:200c:****。 ○ IP黑名单和白名单均支持添加IP网段，例如192.168.0.1/24，24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192.168.0.1/24表示的IP网段范围是192.168.0.1~192.168.0.254。

8. 单击**确认**，完成配置。

   配置成功后您可以单击**修改配置**或**删除配置**，对当前的配置进行修改或删除操作。

5.4. 配置可信IP

为了避免触发封禁规则，您可以开启可信IP功能，将IP地址加入白名单。加入白名单的IP地址不会被封禁规则触发，始终可以正常访问资源。本文为您介绍添加可信IP的方法。

背景信息

当您开启了频次控制、机器流量管理等功能时，根据您设置的条件，如果触发了封禁规则会断开资源的访问连接，为了避免某些IP地址的访问不被限制，您可以将IP地址加入白名单。

操作步骤

1. 登录SCDN控制台。

2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，定位目标域名，在目标域名右侧单击**配置**。

4. 在指定域名的左侧导航栏，单击**访问控制**。
5. 单击**可信IP**页签。
6. 在**可信IP**页签下，单击**修改配置**。
7. 在**可信IP**对话框，输入需要加入白名单的IP地址。

> 说明
> - 最多支持输入100条，使用回车符隔开，同一个IP地址不能重复添加。
> - 支持添加网段，例如192.168.0.1/24。

8. 单击**确认**，完成配置。

   配置成功后您可以单击**修改配置**或**删除配置**，对当前的配置进行修改或删除操作。

5.5. 配置UserAgent黑白名单

您可以配置UserAgent黑名单和白名单实现对访客身份的识别和过滤，从而限制访问SCDN资源的用户，提高SCDN的安全性。本文为您介绍UserAgent黑白名单的配置方法。

背景信息

当您需要根据请求的UserAgent字段进行访问控制时，请通过UserAgent黑白名单功能对访问请求进行过滤。

> **说明** UserAgent黑白名单功能默认是关闭状态，您可以根据自己的实际需求，设置UserAgent黑名单或白名单。

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

  如果您的UserAgent字段被加入黑名单，该带有UserAgent字段的请求仍可访问到SCDN节点，但是会被SCDN节点拒绝并返回403，同时SCDN的日志中仍会记录这些黑名单中的UserAgent字段请求记录。
- UserAgent白名单：白名单内的UserAgent字段才能访问当前资源，白名单以外的UserAgent字段均无法访问当前资源。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，定位目标域名，在目标域名右侧单击**配置**。

4. 在指定域名的左侧导航栏，单击**访问控制**。
5. 单击**UserAgent黑/白名单**页签。
6. 在**UserAgent黑/白名单**页签下，单击**修改配置**。
7. 在**规则**对话框，根据界面提示，配置UserAgent的**黑名单**或**白名单**。

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

8. 单击**确认**，完成配置。

   配置成功后您可以单击**修改配置**或**删除配置**，对当前的配置进行修改或删除操作。

6.安全配置

6.1. 配置频次控制

当您的网站遭受恶意CC攻击响应缓慢时，通过频次控制功能，可以秒级阻断访问该网站的请求，提升网站的安全性。本文为您介绍频次控制的配置方法。

配置频次控制（单个域名）

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，定位目标域名，在目标域名右侧单击**配置**。

4. 在指定域名的左侧导航栏，单击**安全配置**。
5. 单击**频次控制模式**页签。
6. 在**频次控制模式**页签下，单击**修改配置**。
7. 在**频次控制**对话框，打开**频次控制**开关，并选择**防护模式**。

参数	描述
频次控制	您可以开启或关闭频次控制，默认是关闭状态。
防护模式	支持**正常**和**紧急**两种防护模式，具体说明如下： ○ **正常**：默认的频次控制模式，如果您的网站流量无明显异常，建议采用该模式，避免被误杀。 ○ **紧急**：当您的网站响应缓慢，且流量、CPU、内存等指标异常时，建议采用该模式。

8. 单击**确认**，完成配置。

配置频次控制（全部域名）

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**安全设置**。
3. 在**安全设置**页面，单击**修改配置**。
4. 在**频次控制**对话框，选择**防护模式**和**选择域名**。

参数	描述
频次控制	您可以开启或关闭频次控制，默认是关闭状态。
防护模式	支持**正常**和**紧急**两种防护模式，具体说明如下： ○ **正常**：默认的频次控制模式，如果您的网站流量无明显异常，建议采用该模式，避免被误杀。 ○ **紧急**：当您的网站响应缓慢，且流量、CPU、内存等指标异常时，建议采用该模式。
选择域名	选择需要防护的域名，仅支持选择**全部域名**。

5. 单击**确认**，完成配置。

6.2. 自定义频次控制规则

阿里云SCDN支持自定义设置频次控制规则，可以帮助您更精准地拦截网络攻击，防止Web攻击、恶意访问等。本文为您介绍自定义频次控制规则的配置方法。

前提条件

设置自定义频次控制规则前，需确保您已经开启了频次控制功能，具体请参见配置频次控制。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，定位目标域名，在目标域名右侧单击**配置**。

4. 在指定域名的左侧导航栏，单击**安全配置**。
5. 单击**频次控制规则**页签。
6. 在**频次控制规则**页签下，单击**添加**。
7. 在**频次控制规则**对话框，完成以下配置。

参数	描述
名称	规则名称，长度为4~30个字符，支持英文和数字，同一个域名中规则名称不可重复。
URI	指定需要防护的具体地址，例如 `/abc` 。支持输入的参数，例如 `/abc?action=login` 。
匹配规则	支持**前缀匹配**和**完全匹配**两种匹配规则。 ○ **完全匹配**：即精确匹配，请求地址必须与配置的URI完全一样才会被统计。 ○ **前缀匹配**：即包含匹配，请求的URI以此处配置的URI开头就会被统计。例如设置URI为 `/abc` ，则 `/abc.html` 会被统计。

参数	描述
监测时长	指定统计访问次数的周期，需要和访问次数配合。监测时长大于等于10秒。
单IP访问次数	指定在统计周期内，允许单个源IP访问该URI的次数。
阻断类型	指定触发条件后的操作，可以是**封禁**或**人机识别**。 ○ **封禁**：触发条件后直接断开连接，所有请求返回403。 ○ **人机识别**：触发条件后用重定向的方式访问客户端，且系统会自动识别正常访问和攻击，对于攻击行为进行封禁，只有验证通过后才放行。
阻断时长	指定执行阻断动作的时间，阻断时间大于等于10秒。

> **说明** 以上图中的配置为例，表示单个IP访问目标地址（完全匹配）时，在10秒内访问超过20次，对应的IP就会被封禁600秒。

8. 单击**确认**，完成配置。

   在**频次控制规则**列表中，您可以单击**修改**或**删除**，修改或删除当前的配置。

相关文档

查看频次控制监控信息，具体请参见频次控制监控。

6.3. 配置机器流量管理

机器流量管理功能采用了大数据分析技术，通过匹配在系统后台已经建立好的机器流量模型，如果命中后台的机器流量IP库，即可实现秒级阻断恶意机器流量IP。本文为您介绍机器流量管理功能的配置方法。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，定位目标域名，在目标域名右侧单击**配置**。

4. 在指定域名的左侧导航栏，单击**安全配置**。
5. 单击**机器流量管理**页签。
6. 在**机器流量管理**页签下，单击**修改配置**。
7. 在**机器流量管理**对话框，打开**机器流量管理**开关，并选择**阻断类型**。
   - **封禁**：默认为封禁模式，所有检测到的机器流量请求均返回403。
   - **观察**：只记录日志不阻断机器流量的请求。

8. 单击**确认**，完成配置。

> **说明** 开启机器流量防护后，您可以配置可信IP，放行指定的机器流量。具体操作请参见配置可信IP。

7.性能优化

7.1. 页面优化

开启页面优化功能后，SCDN会自动删除当前域名下所有HTML页面中的冗余注释和重复的空白符，可以有效去除页面的冗余信息，减小文件体积，提高加速分发效率。本文为您介绍开启页面优化功能的方法。

操作步骤

> **注意** 如果源站文件配置了MD5校验机制，请勿开启该功能。当SCDN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。

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，定位目标域名，在目标域名右侧单击**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。

   开启页面优化功能后即时生效，可以有效去除页面的冗余信息，减小文件体积，提高加速分发效率。

7.2. 智能压缩

开启智能压缩功能后，SCDN会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的大小，提升加速效率。本文为您介绍开启智能压缩功能的方法。

背景信息

- 智能压缩即Gzip（GNU zip）压缩，支持的内容格式如下：

  `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，请勿开启该功能。当SCDN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。
> - 当源站文件大小超过1024 Byte时，SCDN才会进行Gzip压缩。
> - IE6.0对Gzip的兼容性较差，如果有IE6.0的访问需求，不建议开启智能压缩功能。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**域名管理**。
3. 在**域名管理**页面，定位目标域名，在目标域名右侧单击**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**开关即可。

7.3. 过滤参数

通过本文您可以详细了解攻击告警配置的功能介绍和示例说明。

功能介绍

过滤参数是指：URL请求中，如果携带 `?` 和参数，则请求到SCDN节点时，SCDN节点在收到该请求后是否将该带参数的请求URL请求回源站。

- 如果开启过滤参数，该请求到SCDN节点后会截取到没有参数的URL向源站请求，且SCDN节点仅保留一份副本。
  - 由于HTTP请求中大多包含参数，但往往参数内容优先级不高，可以忽略参数浏览文件，适合开启该功能；开启后可以有效提高文件缓存命中率，提升分发效率。
  - 若参数有重要含义，例如包含文件版本信息等，推荐设置“保留参数”。您可以设置多个保留参数。如请求中包含任一“保留参数”，会携保留参数回源。
- 如果关闭过滤参数，则每个不同的URL都缓存不同的副本在SCDN的节点上。

> **说明**
>
> 适用业务类型：所有。

示例

例如：`http://www.example.com/image_01.jpg?x=1` 请求URL到SCDN节点。

- 开启“过滤参数”功能后，整个请求流程如下：
  i. SCDN节点向源站发起请求 `http://www.example.com/image_01.jpg`（忽略参数x=1）。
  ii. 源站响应该请求内容后，响应到达SCDN节点。
  iii. SCDN节点会保留一份副本，然后继续向终端响应 `http://www.example.com/image_01.jpg` 的内容。

iv. 所有类似的请求 `http://www.example.com/image_01.jpg?参数` 均响应SCDN副本 `http://www.example.com/image_01.jpg` 的内容。

- 关闭“过滤参数”功能，`http://www.example.com/image_01.jpg?x=1` 和 `http://www.example.com/image_01.jpg?x=2` 会响应不同参数源站的响应内容。

8.资源监控

8.1. 资源用量

通过本文您可以详细了解资源监控的功能说明。

监控页面功能说明

- 资源监控包含：流量带宽、回源统计、访问次数、命中率、HTTPCode。支持以域名、地区、运营商和时间粒度、自定义时间区间等为条件筛选查询。
- 支持原始数据导出和下载，如网络带宽、流量，域名按流量占比排名以及访客区域、运营商分布等详细数据。
- 资源监控部分的曲线图数据和计费数据有一定差别，如30天统计曲线取点粒度为14400s，计费数据粒度为300s，故曲线图会忽略掉其中的一些计量点作图，主要用作带宽趋势描述，带宽使用以精确粒度的计费数据为准。

> **说明** 原始数据采集粒度随时间段变化，日维度导出数据，粒度为300s；周维度导出数据，粒度为3600s；月维度导出数据，粒度为14400s 。

8.2. 实时监控

通过实时监控功能，您可以实时查看当前账号下所有域名的基础数据、回源流量和加速质量，便于您及时作出业务决策。通过本文您可以了解SCDN实时监控的指标以及查询方法。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**资源监控 > 实时监控**。
3. 在**实时监控**页面，选择您想要查看的监控项和指标，单击**查询**。

   您可以选择需要监控的**域名**、**地区**、**运营商**以及需要查询的**时间段**，查看以下监控项和监控指标的具体情况。

监控项	监控指标
基础数据	带宽、流量、请求次数和QPS。
回源流量	回源带宽和回源流量。
质量监控	请求命中率、字节命中率、2xx状态码、3xx状态码、4xx状态码和5xx状态码。

9.安全监控

9.1. 网络攻击监控

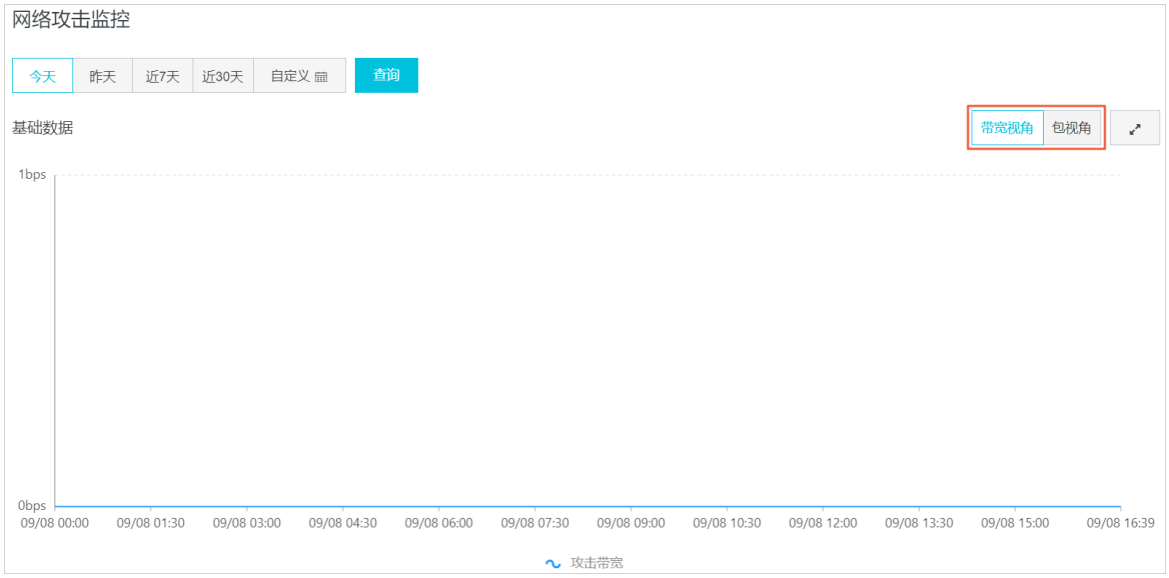
通过网络攻击监控功能，您可以查询网络攻击带宽和攻击数据包信息。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**安全监控 > 网络攻击监控**。
3. 在**网络攻击监控**页面，选择查询时间，单击**查询**。

> **说明** 支持按天或自定义时间区间进行查询。

4. 查询结果支持以**带宽视角**和**包视角**显示，可以查询到网络攻击带宽和攻击数据包信息。



9.2. 频次控制监控

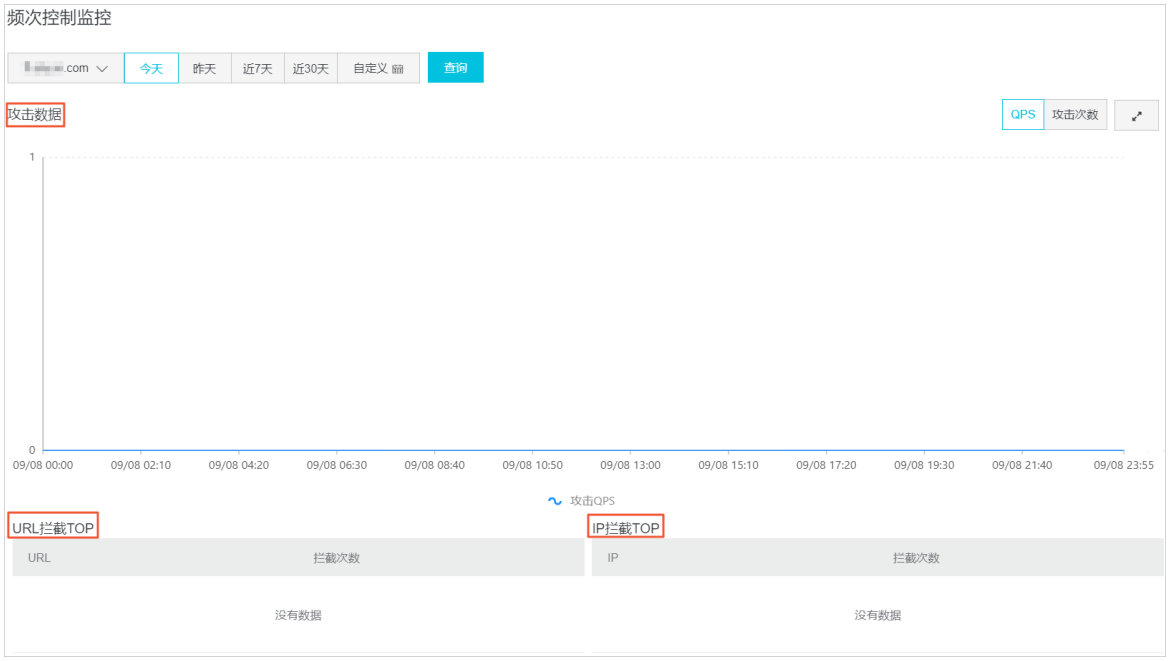
通过频次控制监控功能，您可以查询攻击数据、URL拦截TOP和IP拦截TOP信息。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**安全监控 > 频次控制监控**。
3. 在**频次控制监控**页面，选择需要查询的域名和时间，单击**查询**。

> **说明** 支持按天或自定义时间区间进行查询。

4. 查询结果会显示**攻击数据**、**URL拦截TOP**和**IP拦截TOP**信息。


频次控制监控
.com
今天
昨天
近7天
近30天
自定义
查询
攻击数据
QPS
攻击次数
1
0
09/08 00:00
09/08 02:10
09/08 04:20
09/08 06:30
09/08 08:40
09/08 10:50
09/08 13:00
09/08 15:10
09/08 17:20
09/08 19:30
09/08 21:40
09/08 23:55
攻击QPS
URL拦截TOP
URL
拦截次数
没有数据
IP拦截TOP
IP
拦截次数
没有数据

10.统计分析

通过统计分析功能，您可以查看加速域名当天及之前的离线分析数据，便于您及时了解SCDN的运行情况。

背景信息

统计分析包含**PV/UV**、**地区和运营商**、**域名排名**、**热门Refer**和**热门URL**五个部分。您可以导出原始详细数据，例如网络带宽、流量、域名按流量占比排名以及访客区域、运营商分布等。

> **说明** 原始数据采集粒度随时间段变化，日维度导出数据粒度为300s；周维度导出数据粒度为3600s；月维度导出数据粒度为14400s。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**统计分析**。
3. 在**统计分析**页面，选择您需要查看的监控项和指标，单击**查询**。

   您可以查询到下表中的相关数据。

项目	监控指标	可选时间
PV/UV	指定域名下的PV和UV的分布。	今天、昨天、近7天、近30天和自定义（90天内）。
地区和运营商	排名、区域、总流量、流量占比、访问次数、访问占比和响应时间。	今天、昨天、近7天、近30天和自定义（90天内）。
域名排名	各个加速域名的排名、占比、流量或带宽峰值、峰值时刻和访问次数。	今天、昨天、近7天、近30天和自定义（90天内）。
热门Refer	指定域名下的Refer流量、流量占比、访问次数和访问占比。	查询近三个月中某天的数据。
热门URL	指定域名下的URL流量、流量占比、访问次数和访问占比。	查询近三个月中某天的数据。

11.账单查询

您可以根据所需查询SCDN的账单，便于您及时了解收费明细，更好地进行业务决策。本文为您介绍查询账单的方法。

背景信息

支持按日或按月查询SCDN的账单，具体说明如下：

- 按日查询

  只能查询当天或之前355天的账单。计费周期例如：2019-07-08 00:00:00至2019-07-08 23:59:59。

- 按月查询

  只能查询前一个月或之前10个月的账单。计费周期例如：2019-06-01 00:00:00至2019-06-30 23:59:59。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**用量查询**。
3. 在**账单查询**页签下，选择按日或按月查询，单击**查询**，即可查询到实际的账单。

12.配置刷新和预热

SCDN提供资源的刷新和预热功能。刷新功能可以强制SCDN节点回源并获取最新文件，预热功能可以在业务高峰之前预热热门资源，提高资源访问效率。本文为您介绍刷新和预热功能的配置方法。

背景信息

SCDN提供资源的刷新和预热功能：

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

适用场景

下表为您详细列出了缓存刷新和预热功能的适用场景。

刷新预热	适用场景
缓存刷新	• 新资源发布 源站点的新资源覆盖同名旧资源后，为避免您受节点缓存影响仍访问到旧资源，可通过提交对应资源的URL或目录进行刷新，清空全网缓存后您可以直接访问到最新的资源。 • 违规资源清理 当站点上存在的违规资源（例如涉黄、涉毒、涉赌）被发现时，删除源站资源后节点缓存资源仍可被访问到，为维护网络环境，可通过URL刷新删除缓存资源，保证违规资源被及时清理。
缓存预热	• 安装包发布 新版本安装包或升级包发布前，提前将资源预热至SCDN加速节点，待正式上线后海量用户的下载请求将直接由SCDN节点响应，可以提升下载速度和大幅度降低源站压力。 • 运营活动 运营活动发布前，提前将活动页涉及到的静态资源预热至SCDN加速节点，活动开始后用户访问所有静态资源均由加速节点响应，海量带宽储备保障用户服务可用性，提升用户体验。

操作步骤

1. 登录SCDN控制台。
2. 在左侧导航栏，单击**刷新预热**。
3. 在**刷新缓存**页签下，根据您的实际需求，配置刷新或预热信息。

   刷新和预热功能的详细说明如下表所示。

分类	原理	注意事项	生效时间

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

> **说明**
> - 刷新或预热时如果需要通过文件提交URL信息，只支持提交TXT格式的文件。
> - 资源刷新和预热完成时间将取决于您提交预热文件的数量、文件大小、源站带宽和网络状况等诸多因素。

4. 配置完成后单击**提交**。

   您可以在**操作记录**页签下，查看资源刷新或预热的详细记录，包括操作内容、操作类型、操作时间、状态和进度等。