阿里云
DDoS高防IP

DDoS高防（新BGP）

文档版本：20200219

法律声明

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

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

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务时间约十分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 **注意:** 权重设置为0，该服务器不会再接受新请求。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	单击设置 > 网络 > 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击**确定**。
`Courier字体`	命令。	执行`cd /d C:/window`命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{}或者{a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1 产品简介

1.1 什么是DDoS高防

DDoS高防服务采用中国大陆地域独有的T级八线BGP带宽资源，可防御超大流量DDoS攻击。相比静态IDC高防IP服务，DDoS高防天然具有灾备能力、线路更稳定、访问速度更快。

优势

DDoS高防服务具有以下优势：

- **拥有中国大陆地域最大的BGP带宽资源，最高防护带宽达到1.5T，可以应对超大流量攻击。**
- **拥有中国大陆地域最优质的BGP带宽资源，BGP线路覆盖电信、联通、移动、教育等运营商线路，平均访问时延仅20ms左右。**
- **只需要一个IP，即可满足中国大陆地域内不同运营商线路的快速访问和DDoS防护需求。**

与静态IDC高防IP服务对比

对比项目	静态IDC高防IP服务（电信、联通、移动线路）	静态IDC高防IP服务（BGP线路）	DDoS高防服务
运营商覆盖	仅覆盖电信、联通和移动线路。	除了覆盖电信、联通和移动线路外，还能覆盖众多中小运营商。	除了覆盖电信、联通和移动线路外，还能覆盖众多中小运营商。
线路质量	中国大陆地域平均访问时延在30ms左右，且对于小运营商可能存在跨网访问。	中国大陆地域平均访问时延在20ms左右，且不存在运营商跨网访问。	中国大陆地域平均访问时延在20ms左右，且不存在运营商跨网访问。
专线回源	不支持。通过互联网回源，存在回源时延。	对于阿里云上的业务，提供专线回源，回源延时可忽略；对于非阿里云内业务，仍通过互联网回源。	对于阿里云上的业务，提供专线回源，回源延时可忽略；对于非阿里云内业务，仍通过互联网回源。
灾备能力	机房故障时，四层流量无法进行自动调度；七层流量自动调度受限于DNS解析生效时间，无法立即生效。	通过BGP路由实现全部流量自动调度，故障响应切换时间可达秒级左右。	通过BGP路由实现全部流量自动调度，故障响应切换时间可达秒级左右。

对比项目	静态IDC高防IP服务（电信、联通、移动线路）	静态IDC高防IP服务（BGP线路）	DDoS高防服务
IP数量	包含2个以上IP，配置工作量相对繁琐。	仅1个IP，配置工作量较少。	仅1个IP，配置工作量较少。
最高防护能力	提供最高1T的防护能力（仅支持电信和联通线路）。	提供最高100G的防护能力。	提供最高1.5T的防护能力。
四层防护能力	支持防御SYN Flood、ACK Flood、ICMP Flood、畸形包等流量攻击；防御空链接、真实肉鸡连接等攻击。	与静态IDC高防IP服务的防护能力一致。	与静态IDC高防IP服务的防护能力一致。
七层防护能力	支持防御CC攻击。	支持防御CC攻击。	支持防御CC攻击。

适用场景

如果您有以下DDoS防护需求，建议选购DDoS高防服务：

- **对线路质量有较高要求，包括访问时延、灾备能力、覆盖运营商线路范围等要求。**
- **需要20G以上保底防护带宽的BGP线路高防IP服务。**
- **具有大流量攻击防护需求（300G以上）。**

相关文档

- **开通*DDoS*高防**
- **计费方式**

2 产品定价

2.1 计费方式

DDoS高防服务提供T级BGP线路的DDoS防护能力，帮助您解决超大流量DDoS攻击（特别是300G以上的大流量攻击）。如果您的业务对访问时延比较敏感，建议您使用DDoS高防服务。本文介绍了DDoS高防服务的计费方式。

基础防护（按月-预付费）

DDoS防护能力	线路	标准功能费用	增强功能费用
30Gbps	八线BGP	20,800 元/月	28,800 元/月
60Gbps	八线BGP	46,800 元/月	54,800 元/月
100Gbps	八线BGP	328,000 元/年（包年优惠价）	424,000 元/年（包年优惠价）
300Gbps	八线BGP	528,000 元/年（包年优惠价）	624,000 元/年（包年优惠价）
400Gbps	八线BGP	968,000 元/年（包年优惠价）	1,064,000 元/年（包年优惠价）
500Gbps	八线BGP	3,753,600 元/年（包年优惠价）	3,849,600 元/年（包年优惠价）
600Gbps	八线BGP	标准功能：4,467,600 元/年（包年优惠价）	增强功能：4,563,600 元/年（包年优惠价）

说明:

- **关于不同功能套餐间的区别，请参见功能套餐说明。**
- **如果您需要更高的DDoS防护能力，请通过工单联系我们。**

同时，DDoS高防实例默认包含以下业务规格。

说明:

如果实际业务需要超出实例的默认业务规格，您可以通过升级实例或在购买实例时对相应规格进行扩展。

业务规格	规格说明	默认情况	扩展单价（元/月）
防护端口数	实例支持添加的TCP/UDP端口数量。	50个	每5个端口： 250 元/月
防护域名数	实例支持添加的HTTP/HTTPS域名数量。	50个 说明: 所有域名所属的一级域名总数不超过5个。	· 标准功能套餐：每10个域名300 元/月 · 增强功能套餐：每10个域名500 元/月 说明: 每增加10个域名可增加一个一级域名。
业务带宽	实例支持处理的无攻击情况下最大业务流量。	100 Mbps	每Mbps：100 元/月 说明: 当实例的总业务带宽规格超出600 Mbps时，超出部分的扩展业务带宽可享受优惠价（每Mbps：75 元/月）。
业务QPS	实例支持处理的无攻击情况下最大HTTP/HTTPS业务的并发请求速率。	3,000 QPS	每100 QPS： 1,000 元/月

弹性防护（按天-后付费）

DDoS高防实例的弹性防护费用，按照前一日实际发生的超出保底防护带宽的攻击流量部分的峰值（即选取当日内所遭受的DDoS攻击中的最大值后，扣除该实例的保底防护带宽值，得到超出部分的流量峰值）所对应的计费区间进行计算，生成后付费账单。

说明:
如果您将DDoS高防实例的弹性防护带宽设置为与保底防护带宽一致，则不会产生任何后付费账单，但您的DDoS高防实例也将不具备弹性防护能力。

例如，您的DDoS高防实例的保底防护带宽规格是30Gb，其弹性防护带宽设置为100Gb。当日该实例遭受两次DDoS攻击，其中一次攻击的峰值为80Gb，另一次攻击的峰值为40Gb，两次攻击均超过保底防护带宽。系统将选取当日所遭受的最大攻击峰值80Gb，并扣除实例的保底防护带宽30Gb，得到50Gb，按照“40 Gb<攻击峰值≤50 Gb”的计费区间计算当日所产生的弹性防护费用，即6,400元。

说明:

- 当日实际发生的DDoS攻击峰值不大于所购买的保底DDoS防护能力，则不会产生任何后付费。
- 当日实际发生的DDoS攻击峰值超过所设置的弹性防护带宽，则不会产生后付费账单。即如果当日实际遭受的DDoS攻击导致所防护的IP被黑洞，则不收取弹性防护费用。
- 当日的弹性防护费用账单一般在第二天上午八点至九点生成。

计费区间	弹性防护费用
0 Gb<攻击峰值≤5 Gb	¥ 800／天
5 Gb<攻击峰值≤10 Gb	¥ 1,200／天
10 Gb<攻击峰值≤20 Gb	¥ 2,200／天
20 Gb<攻击峰值≤30 Gb	¥ 3,600／天
30 Gb<攻击峰值≤40 Gb	¥ 4,880／天
40 Gb<攻击峰值≤50 Gb	¥ 6,400／天
50 Gb<攻击峰值≤60 Gb	¥ 7,800／天
60 Gb<攻击峰值≤70 Gb	¥ 9,200／天
70 Gb<攻击峰值≤80Gb	¥ 10,600／天
80Gb<攻击峰值≤100Gb	¥ 11,800／天
100Gb<攻击峰值≤150Gb	¥ 14,600／天
150Gb<攻击峰值≤200Gb	¥ 21,600／天
200Gb<攻击峰值≤300Gb	¥ 28,000／天
300Gb<攻击峰值≤400Gb	¥ 40,000／天
400Gb<攻击峰值≤500Gb	¥ 50,000／天
500Gb<攻击峰值≤600Gb	¥ 60,000／天
600Gb<攻击峰值≤700Gb	¥ 70,000／天
700Gb<攻击峰值≤800Gb	¥ 80,000／天
800Gb<攻击峰值≤900Gb	¥ 90,000／天
900Gb<攻击峰值≤1000Gb	¥ 100,000／天
1000Gb<攻击峰值≤1100Gb	¥ 110,000／天
1100Gb<攻击峰值≤1200Gb	¥ 120,000／天
1200Gb<攻击峰值≤1300Gb	¥ 130,000／天
1300Gb<攻击峰值≤1400Gb	¥ 140,000／天

计费区间	弹性防护费用
1400Gb<攻击峰值≤1500Gb	¥ 150,000／天

不支持退款声明

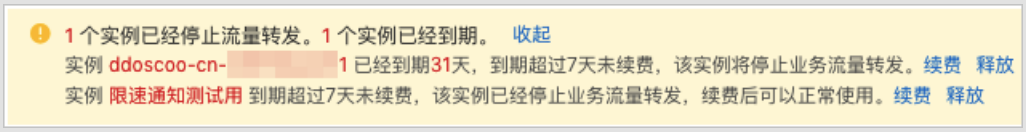
阿里云DDoS高防包年包月服务不支持提前退订，也不适用五天无理由退款。若您已使用了DDoS高防实例，一概不支持退款。

实例到期说明

- **高防实例到期后，防护能力立即降为5Gbps且无弹性防护能力，到期后的七天内可以维持业务转发正常。**
- **高防实例到期超过七天后，自动停止业务流量转发。**
  - **正常续费后，业务流量转发自动恢复，您可以继续正常使用高防。**
  - **阿里云将定期进行资源回收。如果实例到期超过7天且未及时续费，实例可能自动释放。**

说明:

建议您随时关注DDoS高防控制台上的已经到期的高防实例信息提示，并尽早续费或设置自动续费，避免因停止业务流量转发影响业务。



- **高防实例到期前、到期后、释放前，阿里云都会通过短信、邮件和站内信的方式为您发送通知。**
  - **高防实例到期前的七天、三天、一天，您将收到通知提醒您及时续费。**
  - **高防实例到期后，您将收到实例保留可用状态7天的通知，提醒您及时续费。**
  - **高防实例到期超过七天仍未完成续费，您将收到实例已经停止 业务流量转发的通知。**

选择业务带宽规格

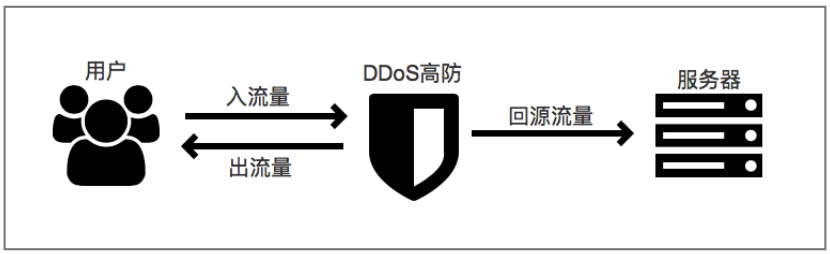
您可以根据所有已经或将要接入DDoS高防实例的业务的日常入方向或出方向总流量的峰值，选择合适的业务带宽规格。您选择的最大业务带宽应大于这些业务的网络入、出方向总流量峰值中较大的值。

说明:

一般情况下，网络出方向的流量会比较大。

您可以参考云服务器（ECS）管理控制台中的流量统计，或者通过您业务源站服务器上的其它流量监控工具来评估您的实际业务流量大小。此处的流量指的是正常的业务流量。

例如，您将业务的外部访问流量均接入DDoS高防进行防护。在业务正常访问（未遭受攻击）时，DDoS高防将这些正常访问流量回源到源站服务器；而当业务遭受攻击时，DDoS高防过滤、拦截异常流量后，仅将正常流量回源到源站服务器。因此，您在云服务器（ECS）管理控制台中查看您源站服务器的入方向及出方向的流量即是正常的业务流量。如果您的业务部署在多台源站服务器，则需要统计所有源站服务器的流量总和。



假设您需要将三个网站业务接入DDoS高防实例进行防护，每个业务出方向的正常业务流量峰值均不超过50 Mbps，业务流量总和不超过150 Mbps。这种情况下，您只需确保所购买的实例的最大业务带宽大于150 Mbps即可。

选择防护域名规格

每10个域名数规格包含1个一级域名。即DDoS高防实例默认支持添加50条域名配置记录，且仅支持接入5个不同的一级域名。

例如，默认情况下，您可以添加五个一级域名（例如，`abc.com`），且为这些域名本身和它们的子域名或泛域名（例如，`www.abc.com`，`*.abc.com`，`mail.abc.com`，`user.pay.abc.com`，`x.y.z.abc.com`等）添加50条域名配置记录。

> **说明:**
> 所添加的这些域名（包括一级域名`abc.com`）都将占用实例的防护域名数。

如果您想要添加更多的一级域名或它们的子域名接入DDoS高防实例进行防护，您需要扩展防护域名数。假设您已经添加五个不同的一级域名或其子域名进行防护，当您尝试添加另一个一级域名或其子域名进行防护时，您将收到以下域名数量限制提示：

当前主域名个数有限制，请升级服务，扩展防护域名数。

这种情况下，您需要升级DDoS高防实例额外增加10个防护域名数量。

2.2 功能套餐说明

DDoS高防提供标准功能和增强功能两种套餐供您选择。增强功能套餐在标准功能套餐的基础上，额外提供网站加速缓存、非标准业务端口、区域流量封禁等增强功能，增强DDoS高防的业务接入能力和DDoS攻击防护能力。您可以根据业务的情况和安全防护需求，选择适合的功能套餐。

购买DDoS高防实例时，系统默认选择标准功能套餐，您可以选择增强功能套餐来获得更强大的业务接入能力和DDoS攻击防护能力。增强功能套餐的售价为8,000元/月，即选择增强功能套餐将在标准功能套餐同规格实例的基础上增加8,000元/月的增强功能费用。

对于已购买的标准功能套餐实例，您可以通过升级DDoS高防实例规格为该实例开通增强功能。

说明:

新购或升级增强功能套餐后，对于已配置接入的网站域名业务您需要编辑域名配置关联增强功能套餐的DDoS高防实例，为网站域名业务使用增强功能。

标准功能与增强功能套餐

增强功能套餐在标准功能套餐的基础上提供更强大的业务接入能力和攻击防护能力。

功能分类	功能项	功能描述	标准功能套餐	增强功能套餐
防护算法	流量型攻击防护	支持常见的流量型DDoS攻击防护，包括畸形报文攻击防护和各类流量型Flood攻击防护。	✓	✓
	资源耗尽型攻击防护	支持常见的网络四层/七层资源耗尽型CC攻击防护，例如HTTP GET Flood、HTTP POST Flood攻击等。 详细信息，请参见#unique_10。	✓	✓

功能分类	功能项	功能描述	标准功能套餐	增强功能套餐
	AI智能防护	· 支持网络七层AI智能CC防护，缓解应用层精巧型CC攻击。 · 支持网络四层AI智能CC防护，缓解TCP连接耗尽型攻击。 详细信息，请参见设置AI智能防护。	✓	✓
防护规则	黑白名单	针对每个接入防护的域名业务支持最多200条访问IP白名单和200条访问IP黑名单规则配置。 详细信息，请参见#unique_12。	✓	✓
	精准访问控制	支持HTTP协议精准匹配防护规则。 详细信息，请参见#unique_13。	针对每个接入防护的域名业务支持配置最多五条规则，且仅支持IP、URL、Referer、User-Agent字段	针对每个接入防护的域名业务支持配置最多十条规则
	区域IP封禁	针对每个接入防护的域名业务的访问流量支持按区域进行封禁。 详细信息，请参见设置针对域名的区域封禁。	✗	✓
业务接入	HTTP（80/8080）、HTTPS（443/8443）标准端口转发	支持HTTP（80/8080）、HTTPS（443/8443）业务的DDoS攻击防护。	✓	✓

功能分类	功能项	功能描述	标准功能套餐	增强功能套餐
	HTTP、HTTPS非标准端口转发	支持HTTP、HTTPS非标准端口（不限于80、8080、443、8443端口）业务的DDoS攻击防护。 说明： 每个实例支持最多配置10不同非标端口的转发。	✗	✓
其它	静态页面缓存	支持网站静态页面加速缓存。 说明： 目前，自定义缓存规则处于公测阶段，每个接入防护的域名业务支持配置最多三条规则。 详细信息，请参见加速网站静态页面访问。	✗	✓

2.3 开通DDoS高防

本文介绍了开通DDoS高防实例的具体操作。

背景信息

关于DDoS高防的详细计费说明，请参见*DDoS高防计费方式*。

操作步骤

1. 访问阿里云*DDoS高防购买页面*，并登录您的阿里云账号。
2. 根据您的业务需要，完成DDoS高防实例的购买配置。配置描述见下表。

类型	配置项	说明
基本配置	防护套餐	默认为专业版，且不支持修改。
	保底防护带宽	选择DDoS高防实例的保底防护带宽。根据所选择的保底防护带宽及购买时长，生成预付费账单。

类型	配置项	说明
	弹性防护带宽	选择DDoS高防实例的最大弹性防护带宽。对于超出保底防护带宽的攻击进行弹性防护，并根据当时实际发生的超出保底防护带宽攻击峰值生成后付费账单。 说明: 如果您不需要启用弹性防护能力，只需将弹性防护带宽的值设置为与保底防护带宽的值一致即可，DDoS高防实例将不会产生任何后付费防护费用且该实例的最大防护带宽为保底防护带宽值。
	业务带宽	选择非DDoS攻击状态下DDoS高防实例所支持的正常业务消耗带宽。
资源组	资源组	选择DDoS高防实例隶属的资源组。
高级配置	功能套餐	DDoS高防实例提供标准功能套餐和增强功能套餐供您选择。 说明: 关于各功能套餐的具体介绍，请参见功能套餐说明。
	防护域名数	选择DDoS高防实例支持接入防护的HTTP/HTTPS域名数量。 说明: 每十个域名包含一个一级域名（且仅限一个一级域名）和该一级域名的子域名或泛域名。
	业务QPS	选择DDoS高防实例支持处理的无攻击情况下最大HTTP/HTTPS业务的并发请求速率。
	端口数	选择DDoS高防实例支持的最大转发端口数量，即通过TCP/UDP协议转发支持的最大条目数。
购买量	购买数量	选择要购买当前配置的实例的数量。

类型	配置项	说明
	购买时长	选择要购买实例的有效期。若勾选自动续费，则在实例到期前自动触发续费。 · 按月购买则自动续费周期为一个月。 · 按年购买则自动续费周期为一年。

3. 确认当前配置并单击立即购买。

4. 确认订单并完成支付。

预期结果

成功开通DDoS高防实例。您可以在实例列表页面查看和管理DDoS高防实例。

后续步骤

- 如果您需要接入网站业务到DDoS高防进行防护，请参见步骤1：添加网站配置。
- 如果您需要接入非网站业务接入DDoS高防进行防护，请参见步骤1：添加端口配置。

2.4 升级DDoS防护实例规格

您购买DDoS防护实例后，如果所购买的实例规格（如功能套餐、保底防护带宽、防护域名数、端口数或业务带宽等）已无法满足您的实际业务需要，您可以随时在云盾DDoS防护控制台升级当前高防实例规格。

背景信息

升级实例规格支持升级至增强功能套餐，扩展保底防护带宽、防护域名数、端口数和业务带宽。升级当前DDoS防护实例规格，您需要补齐升级差价。支付完成后，DDoS防护实例规格升级即时生效。

> 说明:
> 不支持降低已购买DDoS防护实例的规格，包括功能套餐、保底防护带宽、防护域名数、端口数和业务带宽。

升级功能套餐，增加防护域名数、端口数、业务带宽所产生的差价部分按以下方式计算：

- 功能套餐：升级增强功能套餐按8,000元/月的单价与当前服务剩余时长计算差价。
- 防护域名数：新增防护域名按每10个域名300元/月（增强功能套餐实例按每10个域名500元/月）的价格与当前服务剩余时长计算差价。
- 端口数：新增端口按50元/月的单价与当前服务剩余时长计算差价。
- 业务带宽： 扩展业务带宽按100元/月的单价（每增加1M）与当前服务剩余时长计算差价。

  > 说明:
  > DDoS防护实例的业务带宽采用分阶段定价。业务带宽在100M - 600M（含600M）区间内，每1M按100元/月的单价计算；业务带宽超出600M以上的部分每1M按75元/月的单价计算。

- 业务QPS：扩展业务带宽按每100QPS 1,000元/月的价格与当前服务剩余时长计算差价。

操作步骤

1. 登录云盾DDoS防护（新BGP）控制台。

2. 定位到管理 > 实例列表，选择待升级的DDoS防护实例，单击升级。

3. 在配置变更页面，选择功能套餐，扩展保底防护带宽、防护域名数、端口数、业务带宽，并单击去支付。

4. 完成支付，升级后的DDoS防护实例规格配置即时生效。

3 快速入门

3.1 防护网站业务

3.1.1 概览

本文将指导您在开通DDoS高防后，快速部署和使用DDoS高防，为您的网站配置DDoS防护策略。

使用DDoS高防防护网站业务时，您可以按照以下步骤进行操作。

任务名	描述
步骤1：添加网站配置	在DDoS高防控制台，为要防护的网站创建网站配置，为其关联DDoS高防实例和设置流量转发信息。
步骤2：业务接入DDoS高防配置	通过修改接入DDoS高防的域名的解析记录，将网站访问流量牵引至DDoS高防实例。 完成切换后，接入防护的域名的访问请求都会先经过DDoS高防清洗，再转发到您的源站服务器，从而实现由DDoS高防实例帮助您防御DDoS攻击流量。
步骤3：设置网站业务DDoS防护策略	网站业务接入DDoS高防后，默认启用DDoS智能防御模式，无需您进行额外操作。在遇到异常情况或特殊需求时，您可以选择调整DDoS防护策略。 支持调整的网站业务DDoS防护策略包括：AI智能防护、针对域名的黑白名单、针对域名的区域封禁、精确访问控制、频率控制。
步骤4：使用安全报表与日志	业务接入DDoS高防后，您可以在DDoS高防控制台，使用安全报表和日志功能查看防护数据。

3.1.2 步骤1：添加网站配置

要使用DDoS高防服务，您必须首先在DDoS高防中添加要防护的网站配置。

前提条件

已开通DDoS高防实例。您可以在云盾DDoS高防控制台的实例列表页面查看所有实例。关于如何开通服务，请参见开通DDoS高防。

操作步骤

1. 登录云盾DDoS高防（新BGP）控制台。
2. 在左侧导航栏，单击接入管理 > 域名接入。

3. 在网站配置页面，单击添加网站。

4. 在添加网站页面，完成填写网站信息任务，并单击添加。配置说明见下表。

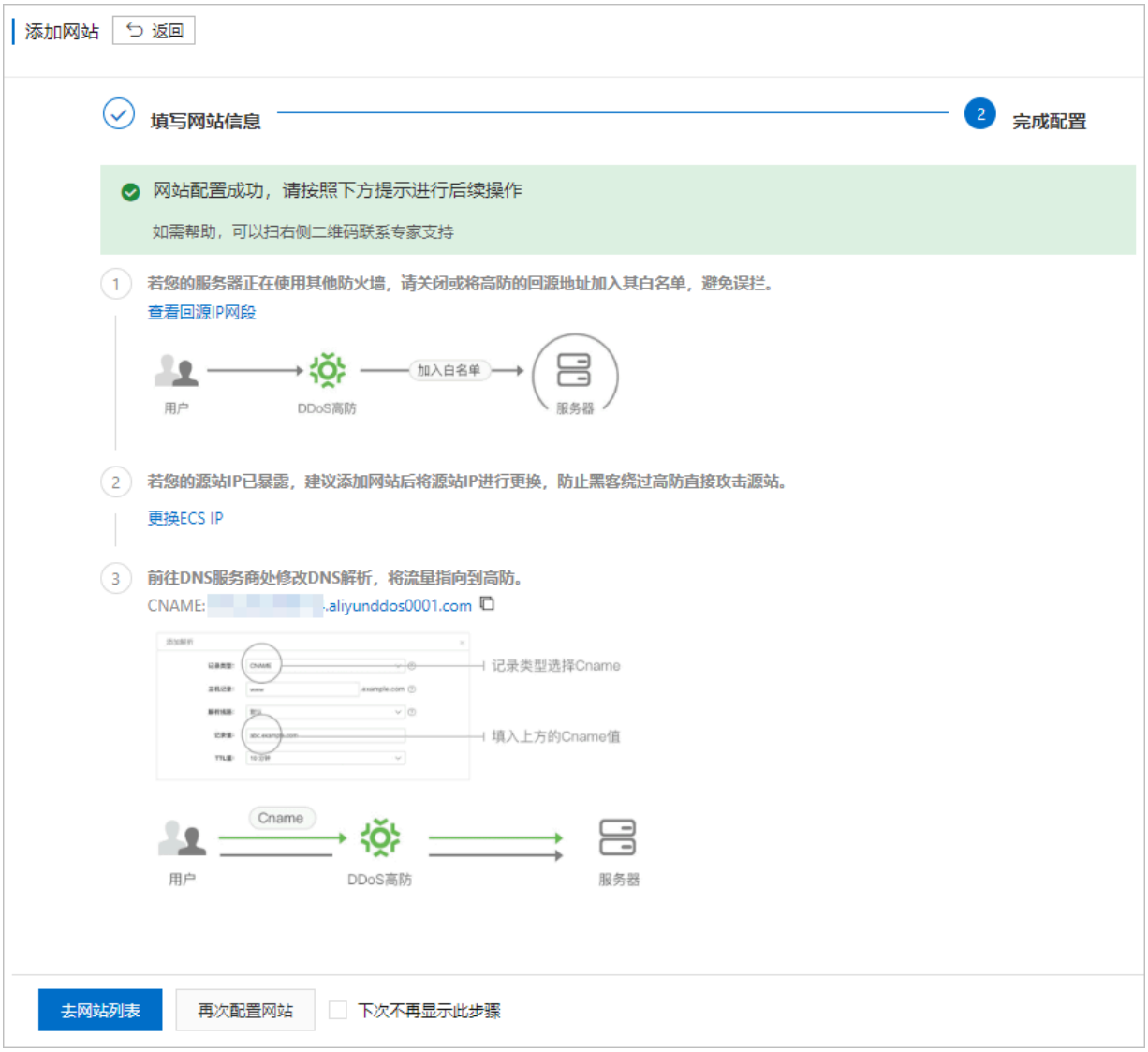
配置项	描述
功能套餐	选择要关联的DDoS高防实例的功能套餐规格，可选值： · 标准功能 · 增强功能 **说明：** 相比于标准功能套餐，增强功能套餐支持更丰富的防护规则配置和更高的业务接入能力。
实例	勾选要关联的DDoS高防实例。一个网站域名最多支持关联8个DDoS高防实例，且不支持关联不同功能套餐的实例。 **说明：** 根据您选择的功能套餐类型显示对应的DDoS高防实例供您选择。如果无可选实例，表示您当前无可用的该功能套餐规格的DDoS高防实例。您可以选择新购实例或升级已有的标准功能套餐实例。更多信息，请参见升级DDoS防护实例规格。
网站	填写要防护的网站域名。 **说明：** · 根据域名命名规则，域名可以由26个英文字母（a-z、A-Z，不区分大小写）、数字（0-9）以及连接符（-）组成，但是域名的首位必须是字母或数字。 · 支持填写泛域名，如`*.aliyun.com`。DDoS高防自动匹配该泛域名对应的子域名。 · 如果同时存在泛域名和精确域名配置（如`*.aliyun.com`和`www.aliyun.com`），DDoS高防优先使用精确域名所配置的转发规则和防护策略。

配置项	描述
协议类型	选择网站支持的协议类型，可选值： · HTTP（默认勾选） · HTTPS（默认勾选） · Websocket · Websockets 说明: 如果要防护的网站支持HTTPS加密认证，则必须勾选HTTPS。同时，您可以根据网站实际所支持的协议类型勾选其他协议类型。
服务器地址	选择源站地址类型，并指定源站服务器地址。支持的源站地址类型包括源站IP和源站域名。 · 源站IP：支持配置最多20个源站IP地址。配置多个源站IP后，DDoS高防实例将以IP Hash的方式转发网站访问流量至源站，自动实现源站的负载均衡。 · 源站域名：如果您在部署DDoS高防实例后还需要部署Web应用防火墙（WAF），以提升应用安全防护能力，您可以选择源站域名类型，并填写WAF实例分配给源站的CNAME地址。 具体配置方法，请参见高防IP+云盾WAF同时使用最佳实践。

配置项	描述
服务器端口	根据选择的协议类型指定服务器端口。 **说明:** 转发端口与服务器端口保持一致。 · 协议类型为HTTP或Websocket时，默认服务器端口为80。 · 协议类型为HTTPS或Websockets时，默认服务器端口为443。 **说明:** HTTP2.0协议的端口与HTTPS端口保持一致。 支持添加自定义端口。您可以单击自定义，并从可选端口范围中选择默认端口以外的端口。 · 标准功能套餐实例：可选的HTTP/Websocket端口范围为80，8080；可选的HTTPS/Websockets端口范围为443，8443。 · 增强功能套餐实例：支持特定非标端口，具体支持范围请参见自定义非标端口。 

预期结果

成功添加网站配置。DDoS高防为每个网站配置分配一个CNAME地址，用于更新网站的DNS解析CNAME记录，从而将网站访问请求转发到DDoS高防实例进行清洗。



单击去网站列表，您可以在网站配置列表中看到新添加的网站配置和其CNAME地址。

后续步骤

- **步骤2：业务接入*DDoS*高防配置**
- **上传*HTTPS*证书：若您的网站支持HTTPS协议，您必须上传HTTPS证书，才能使DDoS高防正常清洗HTTPS业务流量。**

3.1.3 步骤2：业务接入DDoS高防配置

添加DDoS高防网站配置后，您需要更新防护域名的DNS解析，将网站业务切换至DDoS高防实例进行清洗。本文以网站域名解析托管在阿里云云解析DNS为例，介绍了更新域名解析CNAME记录以接入DDoS高防的操作方法。

前提条件

修改DNS解析前，您需要完成以下任务：

- 添加网站配置。具体操作请参见步骤1：添加网站配置。
- 如果您的源站服务器部署了其他厂商的防火墙，请将DDoS高防的回源地址加入防火墙的白名单。 具体操作请参见放行DDoS高防回源IP。

> **注意:**
> 完成网站业务切换后，网站的正常访问流量经过DDoS高防实例清洗，并由DDoS高防回源IP地址转发至源站服务器。因此，如果DDoS高防的回源地址不在源站防火墙的白名单中，访问流量可能被错误拦截，导致网站无法访问。

- 验证转发配置。强烈建议您在切换网站访问流量前，验证并确认DDoS高防实例转发配置已经生效。具体操作请参见网站配置生效测试。

背景信息

以下操作描述建立在您的域名DNS托管在阿里云云解析DNS。

> **说明:**
> 云解析DNS是阿里云提供的域名解析服务，支持免费的公共DNS服务和付费版增值服务。如果您的域名已开通付费版云解析DNS服务，我们推荐您使用NS接入（即自动修改DNS）的方式接入DDoS高防。更多信息，请参见NS方式接入网站业务。

若您使用其他DNS服务商的域名解析服务，请登录服务商系统，更新防护域名的解析CNAME记录，下文内容仅供参考。

假设在步骤1添加网站配置中，已添加的防护域名为`bgp.ddostest.com`；以下操作示例描述了在云解析DNS控制台修改/新增域名解析CNAME记录的具体步骤。

操作步骤

1. 登录阿里云云解析DNS控制台。
2. 在域名解析页面，定位到要操作的域名（本示例中为`ddostest.com`），单击其操作列下的解析设置。

3. 在解析设置页面，定位到要修改的解析记录（本示例中，即主机记录为bgp的A记录或CNAME记录），单击其操作列下的修改。

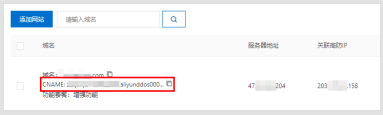
说明：

如果要操作的解析记录不在记录列表中，您可以单击添加记录。

4. 在修改记录（或添加记录）对话框，选择记录类型为CNAME，并将记录值修改为域名的DDoS高防CNAME地址。

说明：

在DDoS高防控制台添加域名配置后，DDoS高防为域名分配一个CNAME地址。您可以登录*DDoS高防（新BGP）控制台*，在网站配置页面（单击左侧导航栏的接入管理 > 域名接入）查看域名的DDoS高防CNAME地址。



5. 单击确定，等待修改后的解析设置生效。

后续步骤

步骤3：设置网站业务DDoS防护策略

3.1.4 步骤3：设置网站业务DDoS防护策略

网站业务接入DDoS高防后，默认启用AI智能防护，无需您进行额外操作。在遇到异常情况或有特殊需求时，您可以手动调整DDoS防护策略。

前提条件

添加网站配置。具体操作请参见步骤1：添加网站配置。

操作步骤

1. 在网站配置列表中，定位到要操作的域名，单击其操作列下的防护设置。

2. 在网站业务DDoS防护页签下，根据需要为目标域名设置DDoS防护策略。支持设置的DDoS防护策略包括AI智能防护、针对域名的黑白名单、针对域名的区域封禁、精确访问控制、频率控制。

- AI智能防护：默认开启，允许智能大数据分析引擎自学习业务流量基线，发现并阻断新型CC攻击，在流量异常时，基于历史流量分布，动态调整各执行模块策略阻断异常请求。支持手动修改防护模式和等级。更多信息，请参见设置AI智能防护。
- 黑白名单（针对域名）：开启网站访问黑白名单，则来自黑名单中的IP/IP段的访问请求将会被直接阻断，来自白名单中的IP/IP段的访问请求将被直接放行，且不经过任何防护策略过滤。更多信息，请参见设置针对域名的黑白名单。
- 区域封禁（针对域名）：开启针对域名的区域封禁，则您可以一键阻断来自指定地区（中国大陆省/市/区、海外区域）的来源IP的所有网站访问请求。更多信息，请参见设置针对域名的区域封禁。
- 精确访问控制：开启精确访问控制，则您可以使用常见的HTTP字段（如IP、URL、Referer、UA、参数等）设置匹配条件，用来筛选访问请求，并对命中条件的请求设置放行、封禁、挑战操作。更多信息，请参见设置精准访问控制规则。
- 频率控制：频率控制防护用来限制单一源IP对网站的访问频率，开启后自动生效。默认使用正常防护模式，帮助网站防御一般的CC攻击。支持手动调整防护模式和自定义访问频率控制规则。更多信息，请参见设置频率控制。

3.1.5 步骤4：使用安全报表与日志

业务接入DDoS高防后，您可以在DDoS高防控制台，使用安全报表和日志功能查看防护数据。

前提条件

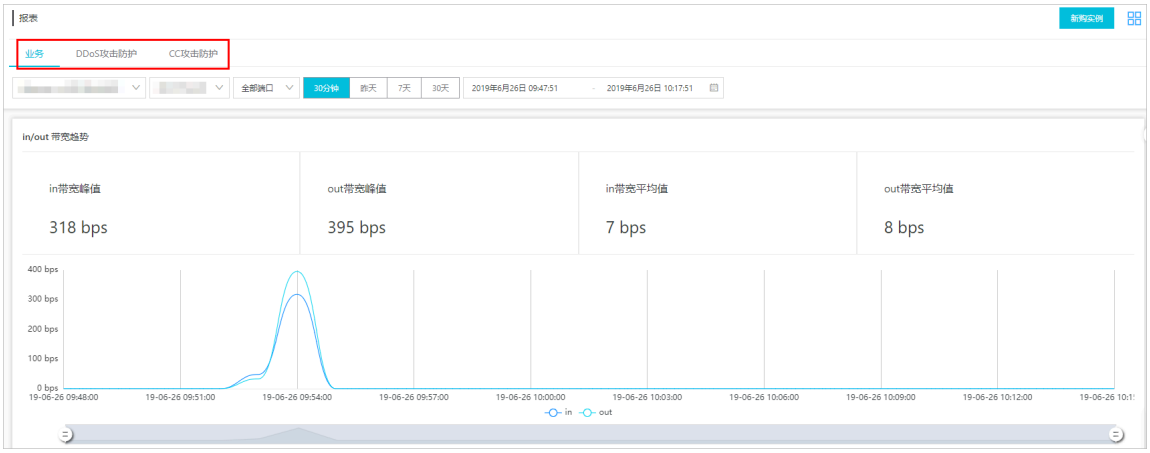
- 已添加网站配置。具体操作请参见步骤1：添加网站配置。
- 已将业务切换至DDoS高防。具体操作请参见步骤2：业务接入DDoS高防配置。

操作步骤

根据需要，选择执行以下操作。

- 查看安全报表

  在左侧导航栏，单击安全报表；在报表页面，根据页签选择要查看的报表类型：业务、DDoS攻击防护、CC攻击防护，查看对应报表记录。



每种报表都支持筛选功能，您可以指定要查看的时间范围，以及实例或IP、端口信息等。每种报表包含的信息见下表。

报表类型	支持查看的信息	支持的筛选项
业务	- in/out带宽趋势 - 并发连接数和新建连接数	- 时间 - 实例 - 高防IP - 转发端口
DDoS攻击防护	- 流量图（回源流量和清洗流量） - DDoS攻击记录	- 时间 - 实例 - 高防IP

报表类型	支持查看的信息	支持的筛选项
CC攻击防护	- QPS图（攻击QPS、总QPS） - CC攻击记录	- 时间 - 被防护域名

更多信息，请参见查看安全报表。

- 查询和分析日志

在左侧导航栏，单击调查分析 > 操作日志；在操作日志页面，查看对应日志记录。操作日志记录最近30天中的重要操作，如IP、抗D包、ECS实例操作等，支持通过时间筛选记录。

如果您希望对DDoS高防的日志内容进行实时分析和报表展示，推荐您开通DDoS高防全量日志服务。开通全量日志服务后，阿里云日志服务将对接DDoS高防的网站访问日志和CC攻击日志，并对采集到的日志数据进行实时检索与分析，以仪表盘形式向您展示查询结果。

DDoS高防全量日志服务是增值服务，需要单独开通并启用。要使用全量日志服务，您需要完成以下任务：

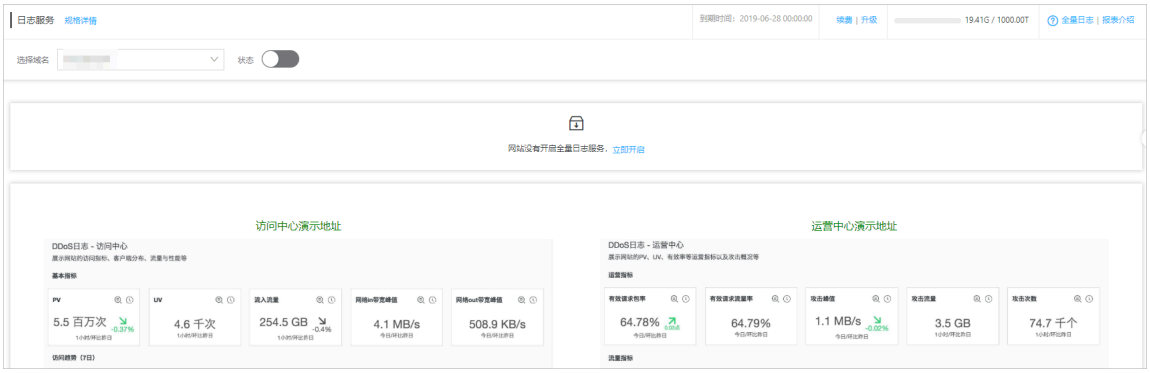
a. 开通全量日志服务，具体操作请参见开通全量日志。

b. 启用全量日志功能，具体操作请参见为网站启用全量日志。

开通并启用全量日志功能后，您可以在调查分析 > 全量日志分析页面，对采集到的日志数据进行实时查询与分析、查看或编辑仪表盘、设置监控告警等。

说明：

关于全量日志中记录并支持操作的字段，请参见全量日志字段说明。



3.2 防护非网站业务

3.2.1 概览

本文将指导您在开通DDoS高防后，快速部署和使用DDoS高防，为您的非网站业务（如端游、手游、APP等）配置DDoS防护，并将业务切入DDoS高防。

使用DDoS高防防护非网站业务时，您可以按照以下步骤进行操作。

任务名	描述
步骤1：添加端口配置	在DDoS高防控制台配置端口转发规则；然后，使用DDoS高防作为您的业务IP，实现业务切入。
步骤2：配置转发策略	添加端口转发规则后，您可以为其配置转发策略，具体包括：会话保持、健康检查、DDoS防护策略。
步骤3：查看业务流量	非网站业务接入DDoS高防后，您可以在DDoS高防控制台查看业务的流量转发数据。

3.2.2 步骤1：添加端口配置

要使用DDoS高防防护您的非网站业务（如端游、手游、APP等），您需要在购买DDoS高防实例后，配置端口转发规则，然后切换DDoS高防作为您的业务IP，实现业务接入。本文介绍了在DDoS高防控制台配置端口转发规则的具体操作。

前提条件

已开通DDoS高防实例。已开通的实例可以在DDoS高防控制台，资产管理 > 实例管理中查看。关于如何开通服务，请参见开通DDoS高防。

背景信息

与网站业务不同，非网站业务配置后只进行四层转发。DDoS高防不会解析七层报文的内容，也不提供基于七层报文的防护（如CC攻击、Web攻击等），只支持四层防护（如SYN Flood、UDP

Flood等）。在接入非网站业务时，您无需额外启用实例或选择高防节点，直接配置转发规则将非网站业务接入DDoS高防实例进行防护即可。

> **注意：**
> 根据工信部要求，为了防止未通过备案的域名业务接入防护，DDoS高防不支持添加纯网络四层80端口的配置接入；为了防止私自搭建DNS防护服务器，不支持添加纯网络四层53端口的配置接入。

关于转发规则冲突

若您已经使用DDoS高防实例接入网站防护，则网站配置添加成功后（具体操作请参见步骤1：添加网站配置），系统将自动在您所选择的DDoS高防实例中为该网站域名生成相应的转发规则，该网站的流量将根据这条转发规则进行转发。

- 如果网站域名设置的转发端口为80，则系统自动生成一条转发协议为TCP、转发端口为80的转发规则。如果该转发规则已经由其它网站域名配置自动生成，则不会再次生成新的转发规则。
- 如果网站域名设置的转发端口为443，则系统自动生成一条转发协议为TCP、转发端口为443的转发规则。如果该转发规则已经由其它网站域名配置自动生成，则不会再次生成新的转发规则。

通过网站配置自动生成的转发规则无法编辑和删除（您只能编辑或删除手动添加的转发规则）。只有当使用该转发规则的所有网站域名配置取消与该DDoS高防实例的关联（即所有网站域名配置均不通过该DDoS高防实例进行防护），相关的转发规则才会被自动删除。

> **注意：**
> 同一DDoS高防实例，同一转发协议下，每条转发规则的转发端口必须唯一。假设实例下已有通过网站配置自动生成的规则（例如，TCP协议-转发端口80或443规则），则在尝试添加同协议-同转发端口规则时，系统将提示转发规则冲突。

操作步骤

1. 登录云盾DDoS高防（新BGP）控制台。
2. 在左侧导航栏，单击接入管理 > 端口接入。

3. 在端口配置页面，选择要配置的DDoS高防实例，单击添加规则。

4. 在添加规则对话框，根据您的实际业务情况，完成规则配置。配置描述见下表。

配置项	说明
转发协议	指定源站使用的转发协议类型：TCP、UDP。
转发端口	指定DDoS高防实例使用的转发端口。 说明: 为了便于管理，一般建议转发端口与源站端口保持一致。
源站端口	指定源站使用的业务端口。

配置项	说明
源站IP	指定源站的IP。 **说明:** 支持设置多个源站IP以实现自动负载均衡；最多可配置20个源站IP。

5. 单击完成，为指定的业务创建相应转发规则。

   转发规则创建完成后，您可以根据需要配置会话保持、健康检查、非网站业务DDoS防护策略。具体操作请参见步骤2：配置转发策略。

   您也可以对手动创建的转发规则执行编辑或删除操作。

6. 将实际业务IP替换为所配置的DDoS高防实例的IP，正式将业务流量切换至DDoS高防实例。

   强烈建议您在正式切换业务前进行验证，确认转发规则配置已生效。关于转发规则配置的验证方法，请参见转发规则配置生效测试。

注意:
如果转发规则未生效就执行业务切换，将可能导致业务中断。

3.2.3 步骤2：配置转发策略

添加端口转发规则后，您可以为其配置转发策略，具体包括：会话保持、健康检查、非网站业务DDoS防护策略。

前提条件

已添加端口转发规则。具体操作请参见步骤1：添加端口配置。

背景信息

通过配置转发策略，您可以根据业务实际需求，优化转发功能。例如，

- 开启基于IP地址的会话保持后，可以将来自同一IP地址的请求转发到同一个后端服务器上。
- 开启健康检查后，检测后端服务器的可用性，在转发客户端请求时避开异常服务器。
- DDoS防护策略是基于IP地址和端口级别的防护，支持对接入DDoS高防的非网站业务的IP及端口的连接速度、包长度等参数进行限制，实现缓解小流量的连接型攻击的防护功能。

操作步骤

1. 在端口配置页面，选择要设置的DDoS高防实例。

2. 定位到要操作的转发规则，根据需要为其设置会话保持、健康检查、非网站业务DDoS防护策略。

   · 会话保持

   a. 单击会话保持列下的配置。

   b. 在会话保持对话框，根据需要启用或关闭会话保持：

   - 如果要启用会话保持，请设置超时时间，并单击完成。
   - 如果要关闭会话保持，直接单击关闭会话保持。

   · 健康检查

   a. 单击健康检查列下的配置。

   b. 在健康检查对话框中，完成健康检查配置。配置描述见下表（单击高级设置可以展开或隐藏高级设置选项）。

类型	健康检查配置项	说明
四层、七层	检查端口	健康检查服务访问后端服务器时的探测端口。默认使用源站端口，范围为1~65535。
仅七层	域名、检查路径	仅适用于TCP协议规则。七层健康检查默认由高防转发系统向该服务器应用配置的缺省首页发起HTTP HEAD请求。 - 如果您用来进行健康检查的页面并不是应用服务器的缺省首页，则需要指定域名和具体的检查路径。 - 如果您对HTTP HEAD请求限定了host字段的参数，您只需要指定检查路径，即用于健康检查页面文件的URI。域名不用填写，默认为后端服务器的IP。

类型	健康检查配置项	说明
高级设置	响应超时时间	每次健康检查的最大超时时间，取值范围为1~30秒。如果后端服务器在指定的时间内没有正确响应，则判定为健康检查失败。
高级设置	检查间隔	进行健康检查的时间间隔，取值范围为1~30秒。高防集群内所有节点，都会独立、并行地遵循该属性对后端服务器进行健康检查。由于各高防节点的检查时间并不同步，所以，如果从后端某一服务器上进行单独统计，会发现来自高防IP的健康检查请求在时间上没有遵循指定的时间间隔。
高级设置	不健康阈值	同一高防节点服务器针对同一后端服务器，在健康检查状态为成功时，连续多少次健康检查失败后，状态判定为失败，取值范围为1~10。

类型	健康检查配置项	说明
高级设置	健康阈值	同一高防节点服务器针对同一后端服务器，在健康检查状态为失败时，连续多少次健康检查成功后，状态判定为成功，取值范围为1~10。

c. 单击完成。成功开启健康检查。若您想关闭健康检查，单击配置后，直接在健康检查对话框中单击关闭健康检查即可。

- 非网站业务DDoS防护策略

a. 单击DDoS防护策略列下的配置。

b. 在非网站业务DDos防护页签下，根据需要为目标转发规则设置非网站业务DDoS防护策略。支持设置的DDoS防护策略包括虚假源、目的限速、包长度过滤、源限速。

- 虚假源：针对虚假IP发起的DDoS攻击进行校验过滤。
- 目的限速：以当前高防IP、端口为统计对象，当每秒访问频率超出阈值时，对当前高防IP的端口进行限速，其余端口不受限速影响。
- 包长度过滤：设置允许通过的包最小和最大长度，小于最小长度或者大于最大长度的包会被丢弃。

- 源限速：以当前高防IP、端口为统计对象，对访问频率超出阈值的源IP地址进行限速。访问速率未超出阈值的源IP地址，访问不受影响。源限速支持黑名单控制，对于60秒内5次超限的源IP，您可以启用将源IP加入黑名单的策略，并设置黑名单的有效时长。

更多信息，请参见设置DDoS防护策略。

3.2.4 步骤3：查看业务流量

非网站业务接入DDoS高防后，您可以在DDoS高防控制台查看业务的流量转发数据。

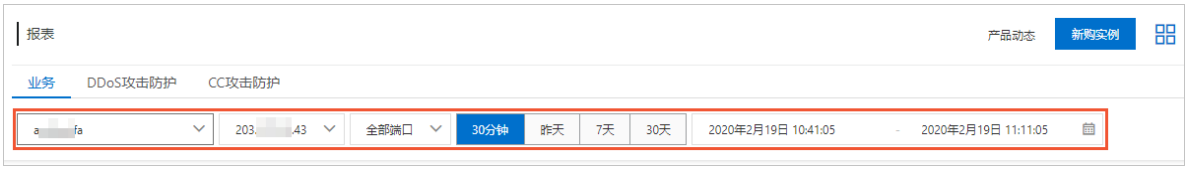
前提条件

已添加端口配置。具体操作请参见步骤1：添加端口配置。

操作步骤

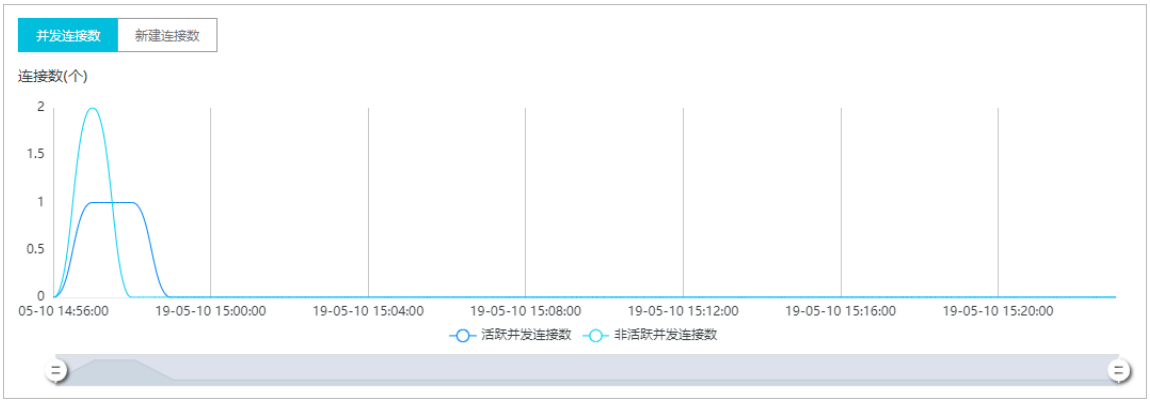
1. 在端口配置页面，选择要查看高防IP实例。
2. 定位到要查看的转发规则，单击其转发端口列下的跳转图标。

3. 在报表页面，业务页签下，设置查询时间（30分钟、昨天、7天、30天、近30天内自定义）后，查看指定时间段的业务流量数据。支持查看的信息包括以下内容：



- in/out带宽趋势：入带宽和出带宽曲线图、峰值、平均值

- 连接数：并发连接数和新建连接数曲线图



4 接入DDoS高防

4.1 域名接入

4.1.1 添加网站

网站配置定义了接入DDoS高防的网站业务的流量转发信息。网站业务接入DDoS高防时，您必须在DDoS高防中为其添加网站配置。网站配置支持批量操作。本文介绍了添加网站配置和批量导入网站配置的具体操作。

前提条件

已开通DDoS高防实例。 更多信息，请参见开通DDoS高防。

操作步骤

1. **登录云盾DDoS高防（新BGP）控制台。**
2. **在左侧导航栏，单击接入管理 > 域名接入。**
3. **在网站配置页面，单击添加网站。**

> **说明:**
> **您也可以批量导入网站配置，具体请参见批量导入。**

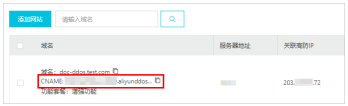
4. **在添加网站页面，完成填写网站信息任务，并单击添加。配置描述见下表。**

配置项	说明
功能套餐	**选择要关联的DDoS高防实例的功能套餐规格，可选值：** **· 标准功能** **· 增强功能** **说明:** **相比于标准功能套餐，增强功能套餐支持更丰富的防护规则配置和更高的业务接入能力。**

配置项	说明
实例	勾选要关联的DDoS高防实例。一个网站域名最多支持关联8个DDoS高防实例，且不支持关联不同功能套餐的实例。 **说明:** 根据您选择的功能套餐类型显示对应的DDoS高防实例供您选择。如果无可选实例，表示您当前无可用的该功能套餐规格的DDoS高防实例。您可以选择新购实例或升级已有的标准功能套餐实例。更多信息，请参见升级DDoS高防实例规格。
网站	填写要防护的网站域名。 **说明:** · 根据域名命名规则，域名可以由26个英文字母（a-z、A-Z，不区分大小写）、数字（0-9）以及连接符（-）组成，但是域名的首位必须是字母或数字。 · 支持填写泛域名，如`*.aliyun.com`。DDoS高防自动匹配该泛域名对应的子域名。 · 如果同时存在泛域名和精确域名配置（如`*.aliyun.com`和`www.aliyun.com`），DDoS高防优先使用精确域名所配置的转发规则和防护策略。
协议类型	选择网站支持的协议类型，可选值： · HTTP（默认勾选） · HTTPS（默认勾选） · Websocket · Websockets **说明:** 如果要防护的网站支持HTTPS加密认证，则必须勾选HTTPS。同时，您可以根据网站实际所支持的协议类型勾选其他协议类型。
服务器地址	选择源站地址类型，并指定源站服务器地址。支持的源站地址类型包括源站IP和源站域名。 · 源站IP：支持配置最多20个源站IP地址。配置多个源站IP后，DDoS高防实例将以IP Hash的方式转发网站访问流量至源站，自动实现源站的负载均衡。 · 源站域名：如果您在部署DDoS高防实例后还需要部署Web应用防火墙（WAF），以提升应用安全防护能力，您可以选择源站域名类型，并填写WAF实例分配给源站的CNAME地址。 具体配置方法，请参见高防IP+云盾WAF同时使用最佳实践。

配置项	说明
服务器端口	根据选择的协议类型指定服务器端口。 **说明:** 转发端口与服务器端口保持一致。 · 协议类型为HTTP或Websocket时，默认服务器端口为80。 · 协议类型为HTTPS或Websockets时，默认服务器端口为443。 **说明:** HTTP2.0协议的端口与HTTPS端口保持一致。 支持添加自定义端口。您可以单击自定义，并从可选端口范围中选择默认端口以外的端口。 · 标准功能套餐实例：可选的HTTP/Websocket端口范围为80，8080；可选的HTTPS/Websockets端口范围为443，8443。 · 增强功能套餐实例：支持特定非标端口，具体支持范围请参见自定义非标端口。 

成功添加网站配置。单击去网站列表，您可以在网站配置列表中看到新添加的网站配置和其CNAME地址。



下一步

添加网站配置后，DDoS高防为网站分配一个Cname地址，您只要将网站域名的DNS解析指向高防Cname地址，即可正式将业务流量切换到高防实例。建议您在正式切换业务前进行本地验证，确认网站转发配置已生效。更多信息，请参见本地验证转发配置生效。

注意:

如果网站转发配置未生效就执行业务切换，将可能导致业务中断。

添加网站配置后，您可以在网站配置页面完成以下操作：

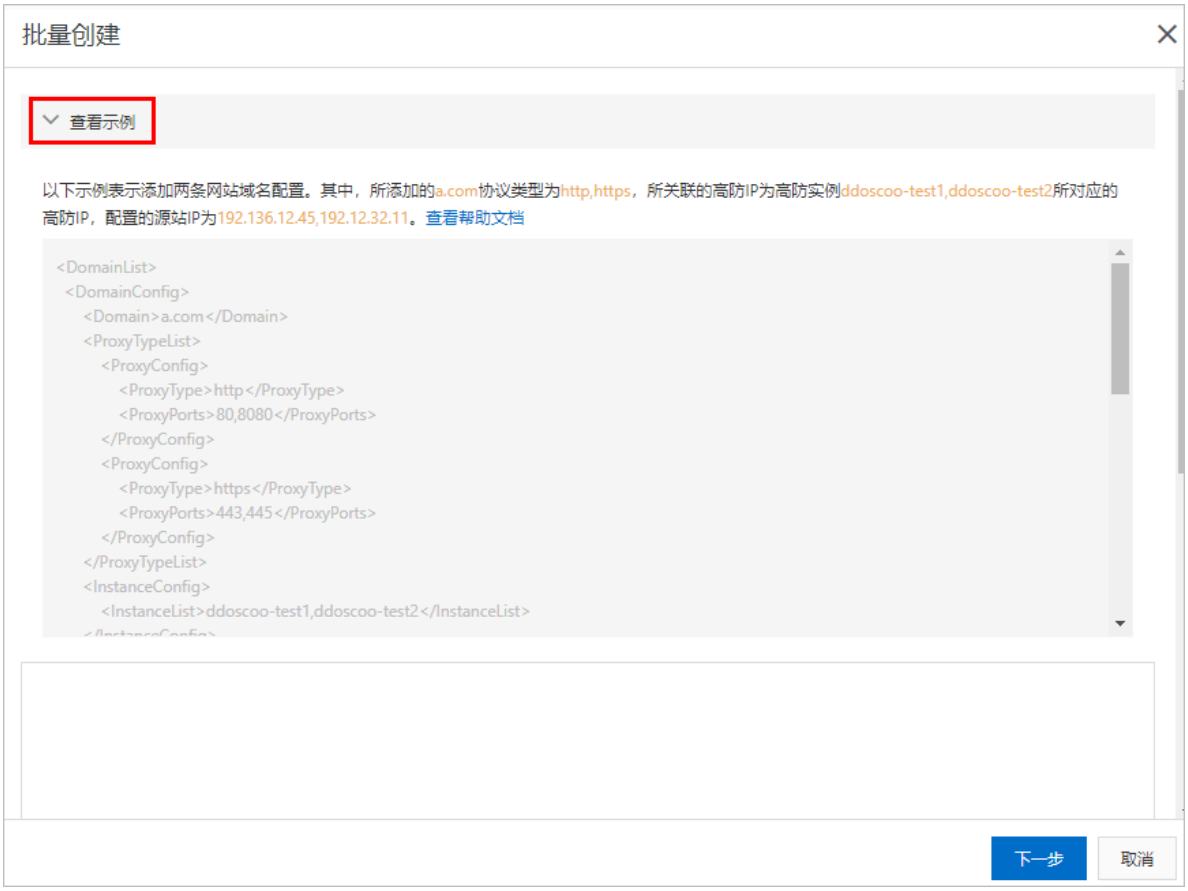
- 若源站服务器上存在防火墙等安全软件，您需要在源站设置放行DDoS高防回源IP。更多信息，请参见放行DDoS高防回源IP。
- 若接入网站存在HTTPS业务，您需要为其上传HTTPS证书。更多信息，请参见上传HTTPS证书。
- 若接入网站存在HTTPS业务，且已关联增强型DDoS高防实例，您可以为其自定义TLS安全策略。更多信息，请参见自定义TLS安全策略。
- 为网站配置DDoS七层防护设置，例如DDoS防护策略、CC防护策略、网络加速策略。更多信息，请参见防护设置。
- 编辑、删除网站配置。更多信息，请参见编辑网站、删除网站。
- 批量导出网站配置。更多信息，请参见批量导出。
- 若源站IP不慎暴露，建议您更换阿里云ECS云服务器的公网IP，防止黑客绕过DDoS高防直接攻击源站。更多信息，请参见更换源站ECS公网IP。

批量导入

1. 登录云盾DDoS高防控制台。
2. 在左侧导航栏，单击接入管理 > 域名接入。
3. 在网站配置页面，单击网站列表下方的批量导入。

4. 在批量创建页面，输入要导入的网站配置，并单击下一步。

   批量创建的网站配置采用XML文件格式传入，关于文件格式的说明，请参见网站配置*XML*格式说明。



   如果输入的XML配置参数文本内容正确，则其将被解析成所需导入的网站配置。

5. 在导入规则页面，勾选要导入的网站配置，并单击确定。

   成功上传网站配置。

6. 上传成功后，关闭上传完成页面。

4.1.2 编辑网站

若您需要为网站重新关联DDoS高防实例（例如由标准套餐更换为增强套餐）、修改源站IP等，您可以编辑网站配置。修改网站配置支持批量操作。本文介绍了编辑网站配置和批量修改网站配置的具体操作。

前提条件

已添加网站配置。更多信息，请参见添加网站。

操作步骤

1. 登录云盾DDoS高防控制台。
2. 在左侧导航栏，单击接入管理 > 域名接入。
3. 定位到要编辑的网站配置，单击其操作列下的编辑。

> **说明:**
> 您也可以批量修改网站配置，具体请参见批量修改。

4. 在编辑网站页面，修改网站配置信息，并单击确定。

   您可以修改除网站名称以外的配置信息。关于网站配置的描述，请参见网站配置描述。

   例如重新选择功能套餐和实例，为网站关联其他DDoS高防实例；重新输入源站IP，更新源站IP等。

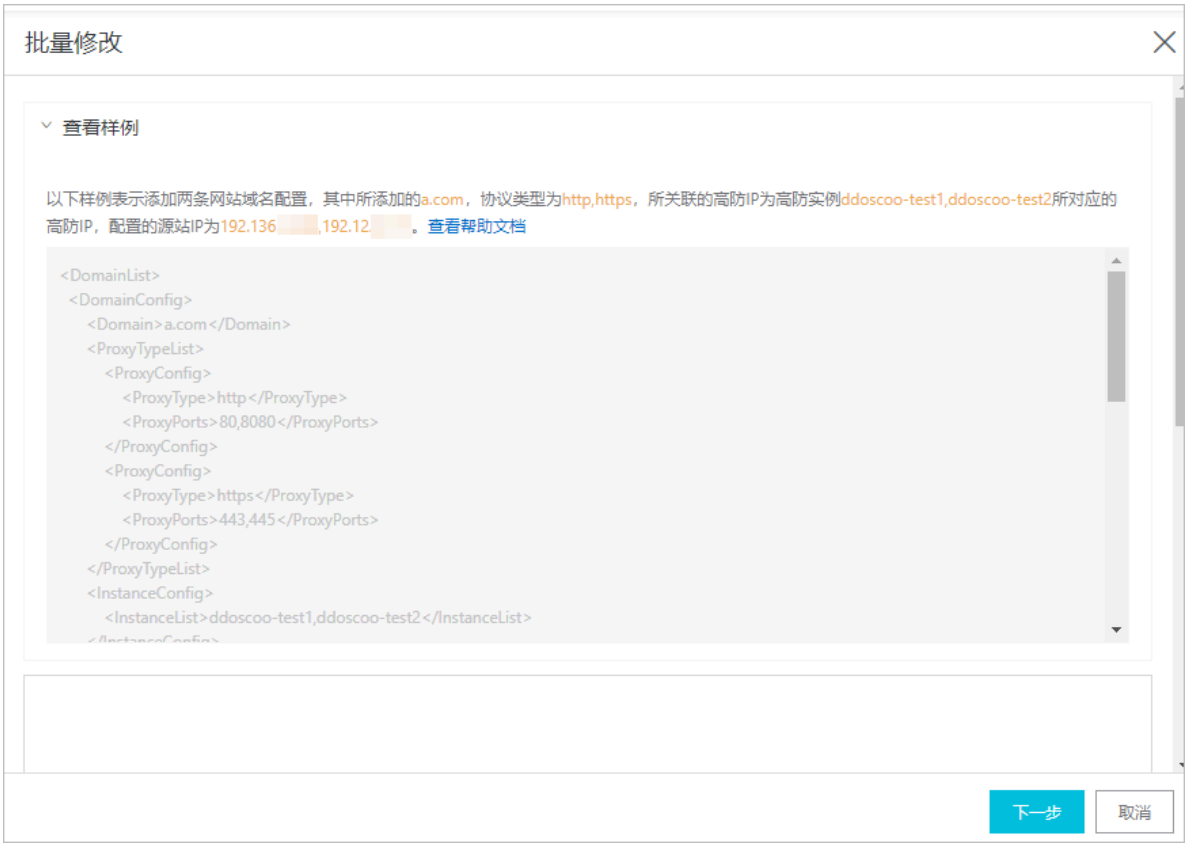
   成功修改网站配置。

批量修改

1. 登录云盾DDoS高防控制台。
2. 在左侧导航栏，单击接入管理 > 域名接入。
3. 在网站配置页面，单击网站列表下方的批量修改。

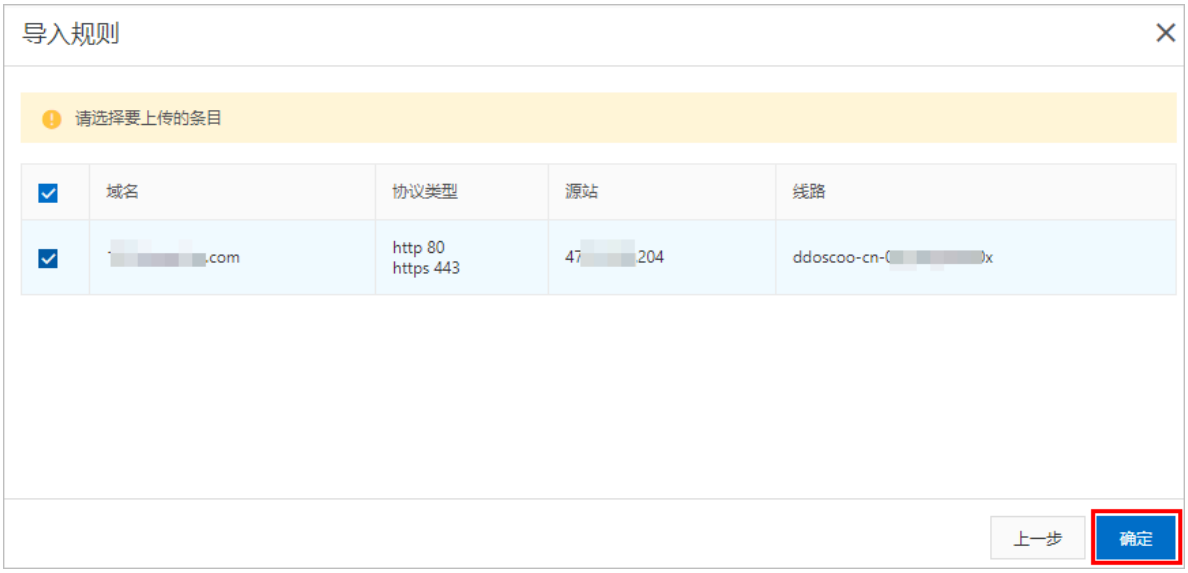
4. 在批量修改页面，输入新的网站配置，并单击下一步。

   批量修改的网站配置采用XML文件格式传入，关于文件格式的说明，请参见网站配置*XML*格式说明。



   如果输入的XML配置参数文本内容正确，则其将被解析成所需导入的网站配置。

5. 在导入规则页面，勾选要导入的网站配置，并单击确定。



   成功上传网站配置。

6. 上传成功后，关闭上传完成页面。

4.1.3 删除网站

若您的网站不再需要接入DDoS高防，您必须先为其恢复域名解析，即确保域名的DNS解析中不再使用高防IP、高防Cname、流量调度器Cname作为记录值；然后删除对应的网站配置。若您未恢复网站域名解析就删除网站配置，则可能导致业务中断。

前提条件

已恢复网站域名解析。

操作步骤

1. 登录云盾*DDoS*高防控制台。
2. 在左侧导航栏，单击接入管理 > 域名接入。
3. 定位到要删除的网站配置，单击其操作列下的删除。

   说明:

   如果要删除多个网站配置，您可以勾选要删除的网站配置，单击网站列表下方的批量删除。
4. 在删除提示对话框中，确认删除操作。

   成功删除网站配置。

4.1.4 批量导出

DDoS高防网站配置支持批量导出。您可以将DDoS高防的全部网站配置以XML格式导出并下载到本地。批量导出的网站配置格式与批量导入/修改网站配置保持一致。

操作步骤

1. 登录云盾*DDoS*高防控制台。
2. 在左侧导航栏，单击接入管理 > 域名接入。

3. 在网站列表下方，单击批量导出。

成功下发导出任务。

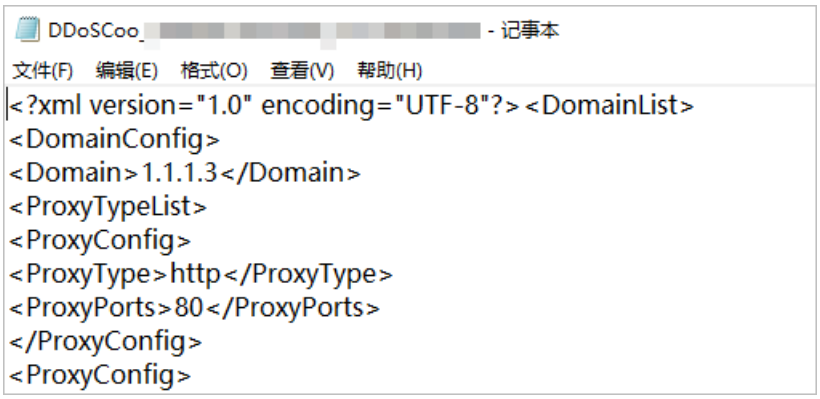
4. 单击页面右上角的导出任务图标。

5. 在任务列表侧边页，等待任务打包完成后，单击下载，下载导出文件到本地。

说明:

如果当前任务状态为待执行状态，请耐心等待导出任务完成。

成功下载导出文件到本地。您可以使用记事本、Notepad++等文本编辑工具打开下载的.xml文件，查看网站配置内容。更多信息，请参见网站配置*XML*格式说明。



6. （可选）在任务列表侧边页，定位到不再需要的任务，单击删除，将其移除。

4.1.5 自定义非标端口

DDoS高防标准功能套餐规格的实例针对网站业务默认支持HTTP（80、8080）和HTTPS（443、8443）标准端口的DDoS攻击防护。增强功能套餐实例支持更多的HTTP、HTTPS业务非标准端口，且对被防护域名使用的不同端口的总数有相应限制。

说明：
为网站配置添加HTTP、HTTPS非标端口，请确认您的网站域名已关联增强功能套餐规格的DDoS高防实例。

端口总数限制

针对每个DDoS高防增强功能规格的实例，由该实例防护的全部域名所使用的不同端口的总数最多为10个。

支持的端口

说明：

DDoS高防实例仅对所支持的HTTP、HTTPS端口提供防护。对于不支持的端口，DDoS高防既不会提供防护，也不会转发流量。例如，4444端口的业务流量到达DDoS高防实例后，将被直接丢弃。

- 针对HTTP和WebSocket协议，DDoS高防增强功能规格实例支持以下端口：

  80, 83, 84, 88, 89, 800, 808, 1000, 1090, 3333, 3501, 3601, 5000, 5222, 6001, 6666, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7060, 7070, 7081, 7082, 7083, 7088, 7097, 7777, 7800, 8000, 8001, 8002, 8003, 8008, 8009, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8106, 8181, 8334, 8336, 8800, 8686, 8787, 8888, 8889, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9999, 10000, 10001, 10080, 12601, 86, 9021, 9023, 9027, 9037, 9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48800, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, 33702
- 针对HTTPS和WebSockets协议，DDoS高防增强功能规格实例支持以下端口：

  443, 4443, 5443, 6443, 7443, 8443, 9443, 8553, 8663, 9553, 9663, 18980

4.1.6 上传HTTPS证书

要使DDoS高防帮助您清洗HTTPS业务流量，您必须在网站配置中勾选HTTPS协议，并上传HTTPS证书。已上传证书发生变化时，您也要在DDoS高防控制台及时更新证书。

前提条件

- 已添加网站配置（具体操作请参见添加网站）且网站支持HTTPS协议。
- 准备证书文件内容。

  如果您已将证书文件上传到云盾SSL证书服务进行统一管理，那么在上传证书时您可以直接选择已有证书；否则您需要准备好网站的证书和私钥文件，以完成上传操作。一般情况下，您需要准备的证书相关内容包括：

  - *.crt（公钥文件）或者*.pem（证书文件）
  - *.key（私钥文件）

操作步骤

1. 登录云盾DDoS高防控制台。
2. 在左侧导航栏，单击接入管理 > 域名接入。

3. 在网站配置列表中，定位到要操作的域名，单击其证书状态列下的上传图标。

4. 在上传证书和私钥对话框中，选择一种上传方式，并完成上传配置。可选择的上传方式包括以下两种：

   - （推荐）选择已有证书

     如果您的网站证书已经上传并托管在云盾SSL证书服务中，您可以直接从已有证书中选择并上传。

     即使您的证书未托管在SSL证书中，您也可以单击前往SSL证书控制台管理，上传并管理您的证书；然后再选择已有证书。关于如何在SSL证书服务控制台上传证书，请参见*#unique_53*。

   - 手动上传

     填写证书名称，并将证书文件和私钥文件中的文本内容分别复制粘贴到证书文件和私钥文件文本框中。

     说明:

     - 对于.pem、.cer、.crt格式的证书，您可以使用文本编辑器直接打开证书文件，并复制其中的文本内容；对于其他格式（如.pfx、.p7b等）的证书，您需要将证书文件转换成.pem格式后，才能用文本编辑器打开并复制其中的文本内容。

       关于证书格式的转换方式，请参见*HTTPS证书转换成PEM格式*。

- 如果该HTTPS证书有多个证书文件（如证书链），您需要将证书文件中的文本内容拼接合并后粘贴至证书文件文本框中。

证书文件文本内容样例

```
-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxvs6MTXcJSfN9Z7rZ9fmxWr2BFN2XbahgnsSXM48ixZJ4krc+1M+
j2kcubVpsE2cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir
+g92cL8IGOkjgvhlqt9vc65Cgb4mL+n5+DV9uOyTZTW/MojmlgfUekC2xiXa54nx
Jf17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvIAqYxXZ7wRwWWmv4TMxFhWRiN
Y7yZIo2ZUhl02SIDNggIEeg==
-----END CERTIFICATE-----
```

私钥文件文本内容样例

```
-----BEGIN RSA PRIVATE KEY-----
xxxxxxxxxxxxtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThL
yvsmLQKBgQCr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQ
ra6ZdwBcQJaiygoIYoaMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/
3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04RtKadOw==
-----END RSA PRIVATE KEY-----
```

5. 单击确定。

预期结果

成功上传证书后，证书状态会更新为有证书。

4.1.7 自定义TLS安全策略

DDoS高防支持TLS安全策略自定义功能，您可以根据实际业务需要选择合适的TLS协议。

前提条件

- 网站配置已关联增强功能套餐的DDoS高防实例。
- 已添加网站配置（具体操作请参见添加网站）且网站支持HTTPS协议。
- 已上传对应的HTTPS证书（具体操作请参见上传*HTTPS*证书）。

背景信息

如果您的业务需要通过PCI DSS 3.2认证，需要禁用TLS1.0协议；同时，您的另一个业务的访问终端仅支持TLS1.0协议，需要兼容TLS1.0协议。这种情况，您可以通过TLS安全策略自定义功能为不同业务灵活配置所需的TLS安全策略。

观看以下视频，快速了解如何在DDoS高防中自定义TLS协议版本和加密套件。

操作步骤

1. 登录云盾*DDoS*高防控制台。
2. 在左侧导航栏，单击接入管理 > 域名接入。
3. 选择已添加的网站业务配置，单击其证书状态列中的TLS安全策略。

4. 在TLS安全策略配置对话框中，选择TLS版本和加密套件。

- TLS版本：默认为支持TLS1.0及以上版本，兼容性最好，安全性较低。您可以根据安全需要选择仅支持TLS1.1或TLS1.2以上版本。
- 加密套件：
  - 仅支持强加密套件，安全性较高，兼容性较低

    仅支持以下强加密套件：

    ■ ECDHE-ECDSA-AES256-GCM-SHA384
    ■ ECDHE-RSA-AES256-GCM-SHA384
    ■ ECDHE-ECDSA-AES128-GCM-SHA256
    ■ ECDHE-RSA-AES128-GCM-SHA256
    ■ ECDHE-ECDSA-WITH-CHACHA20-POLY1305
    ■ ECDHE-RSA-WITH-CHACHA20-POLY1305
    ■ ECDHE-RSA-AES256-CBC-SHA
    ■ ECDHE-RSA-AES128-CBC-SHA
    ■ ECDHE-ECDSA-AES256-CBC-SHA
    ■ ECDHE-ECDSA-AES128-CBC-SHA
  - 全部加密套件，安全性较低，兼容性较高

    除上述强加密套件外，还支持以下四种弱加密套件：

    ■ RSA-AES256-CBC-SHA
    ■ RSA-AES128-CBC-SHA
    ■ ECDHE-RSA-3DES-EDE-CBC-SHA
    ■ RSA-3DES-EDE-CBC-SHA

4.1.8 网站配置XML格式说明

批量操作DDoS高防网站配置时（例如批量导入、修改、导出），网站配置按照固定的XML格式传递。本文介绍了网站配置的XML格式说明。

参数说明

网站配置参数内容必须以`<DomainList>`开始，`</DomainList>`结束，中间部分是网站配置的参数信息。其中，每个网站的配置参数均以`<DomainConfig>`开始，`</DomainConfig>`结束，中间部分为与该网站配置相关的具体参数，详见下表。

说明:
每多添加一个网站配置，则增加一个`<DomainConfig>……</DomainConfig>`数据结构体。

网站配置具体参数	说明
`<Domain>a.com</Domain>`	指定待配置的域名（只能输入一个域名）。
`<ProtocolConfig><ProtocolList>http,https</ProtocolList></ProtocolConfig>`	指定域名协议类型。指定多个协议类型时以英文“,”隔开，本示例表示该域名的协议类型为http和https。
`<InstanceConfig><InstanceList>ddoscoo-cn-4590lwcny001</InstanceList></InstanceConfig>`	指定为该网站配置的DDoS高防实例。 **说明:** 由于每个DDoS高防实例对应一个高防IP，只需填写DDoS高防的实例ID即可。指定多个实例时以英文字符“,”隔开。
`<RealServerConfig><ServerType>0</ServerType><ServerList>1.2.3.4</ServerList></RealServerConfig>`	指定源站信息。其中， • `<ServerType>0</ServerType>`：表示源站IP类型 • `<ServerType>1</ServerType>`：表示源站域名类型 在`<ServerList>1.2.3.4</ServerList>`中指定源站地址，指定多个地址时以英文字符“,”隔开。 **说明:** 配置某个域名的源站信息时，只能是源站IP或源站域名信息，两者不能同时存在。

示例

该示例表示添加以下两条网站配置。

- **网站一：域名是a.com，协议类型是http和https，关联高防实例ddoscoo-cn-xxxxxxxxx001，对应源站IP是1.x.x.4。**
- **网站二：域名b.com，协议类型是http、websocket和websockets，关联高防实例ddoscoo-cn-xxxxxxxxx002和ddoscoo-cn-xxxxxxxxx00d，对应源站域名q840a82zf2j23afs.xxxxxxxxx.com。**

```
<DomainList>
 <DomainConfig>
 <Domain>a.com</Domain>
 <ProtocolConfig>
 <ProtocolList>http,https</ProtocolList>
 </ProtocolConfig>
 <InstanceConfig>
 <InstanceList>ddoscoo-cn-xxxxxxxxx001</InstanceList>
 </InstanceConfig>
 <RealServerConfig>
 <ServerType>0</ServerType>
 <ServerList>1.2.3.4</ServerList>
 </RealServerConfig>
 </DomainConfig>
 <DomainConfig>
 <Domain>b.com</Domain>
 <ProtocolConfig>
 <ProtocolList>http,websocket,websockets</ProtocolList>
 </ProtocolConfig>
 <InstanceConfig>
 <InstanceList>ddoscoo-cn-xxxxxxxxx002,ddoscoo-cn-xxxxxxxxx00d</
InstanceList>
 </InstanceConfig>
 <RealServerConfig>
 <ServerType>1</ServerType>
 <ServerList>q840a82zf2j23afs.xxxxxxxxx.com</ServerList>
 </RealServerConfig>
 </DomainConfig>
 </DomainList>
```

4.2 端口接入

4.2.1 添加规则

端口配置定义了DDoS高防实例的业务转发规则。非网站业务接入DDoS高防时，您必须在高防IP的端口配置下为业务添加转发规则。端口配置也是DDoS高防网络四层防护设置的入口，您可以根据需要为已添加的转发规则设置会话保持、健康检查、DDoS防护策略。端口配置支持批量操作。

前提条件

已开通DDoS高防实例。更多信息，请参见开通DDoS高防。

操作步骤

1. **登录云盾DDoS高防（新BGP）控制台。**

2. 在左侧导航栏，单击接入管理 > 端口接入。
3. 在端口配置页面，选择要操作的DDoS高防实例和IP，并单击添加规则。

> **说明:**
> 您也可以使用批量操作添加规则，支持一次添加多条规则，具体请参见批量添加规则。

4. 在添加规则对话框，根据您的实际业务情况完成规则配置，并单击完成。配置描述见下表。

配置项	说明
转发协议	指定源站使用的转发协议类型：TCP、UDP。
转发端口	指定DDoS高防实例使用的转发端口。 **说明:** · 为了便于管理，建议转发端口与源站端口保持一致。 · 根据工信部要求，为了防止未通过备案的域名业务接入防护，DDoS高防不支持添加纯网络四层80端口的配置接入；为了防止私自搭建DNS防护服务器，不支持添加纯网络四层53端口的配置接入。 · 不允许使用已配置的转发端口。同一DDoS高防实例（IP）和转发协议下，每条转发规则的转发端口必须唯一。当您尝试添加同协议-同转发端口的规则时，系统将提示转发规则冲突。请注意不要与通过网站配置自动生成的转发规则冲突，具体请参见（添加网站）自动生成转发规则。
源站端口	指定源站使用的业务端口。

配置项	说明
源站IP	指定源站的IP。 **说明:** 支持添加多个源站IP以实现自动负载均衡。多个IP间以英文逗号（,）分隔。最多可配置20个源站IP。

成功添加转发规则。您可以在转发规则列表中看到新增的转发规则。

下一步

添加转发规则后，您只要将实际业务IP替换为所配置的DDoS高防IP，即可正式将业务流量切换至DDoS高防实例。建议您在正式切换业务前进行本地验证，确认转发规则配置已生效。更多信息，请参见本地验证转发配置生效。

注意:

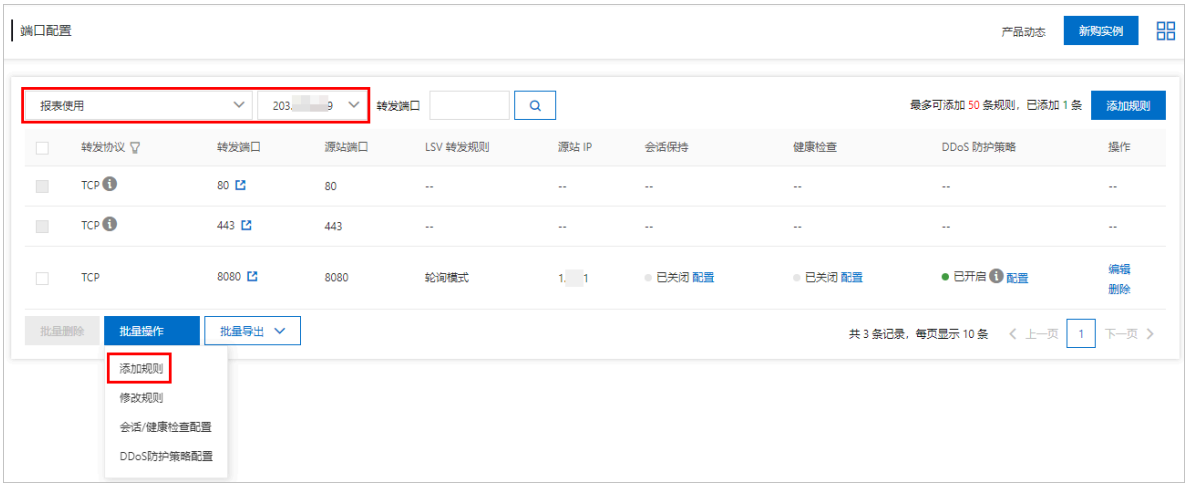
如果转发规则未生效就执行业务切换，将可能导致业务中断。

添加转发规则后，您可以在端口配置页面完成以下操作：

- **为转发规则配置DDoS四层防护设置，例如DDoS防护策略、健康检查、会话保持。更多信息，请参见配置转发策略。**
- **查看业务安全报表。单击转发端口后的跳转链接，查看当前高防IP上的业务数据，例如in/out带宽、连接数量等。更多信息，请参见查看安全报表。**
- **编辑、删除转发规则。更多信息，请参见编辑规则、删除规则。**
- **批量导出规则和防护设置。更多信息，请参见批量导出。**

批量添加规则

1. **登录云盾*DDoS*高防控制台。**
2. **在左侧导航栏，单击接入管理 > 端口接入。**
3. **在端口配置页面，选择要操作的DDoS高防实例和IP，并单击规则列表下方的批量操作 > 添加规则。**



4. 在添加规则对话框，按照格式要求填入要添加的规则配置，并单击添加。规则配置的格式要求如下。
   - 每行对应一条规则。
   - 每条规则包含四个字段，从左到右依次是协议、转发端口、源站端口、源站IP（字段的含义见规则配置描述），字段间以空格分隔。

5. 在添加规则对话框，勾选要上传的规则，确认后并单击上传。

成功上传转发规则。您可以在转发规则列表中看到新增的转发规则。

6. 上传完成后，关闭添加规则对话框。

（添加网站）自动生成转发规则

若您已为DDoS高防实例关联网站配置（具体操作请参见添加网站），则系统在高防实例下自动生成对应转发规则，用来转发网站流量。

- 若网站配置中的服务器端口为80，则自动生成一条转发协议为TCP、转发端口为80的转发规则。
- 若网站配置中的服务器端口为443，则自动生成一条转发协议为TCP、转发端口为443的转发规则。
- 如果上述转发规则已经由其它网站配置自动生成，则不会再次生成新的转发规则。

通过网站配置自动生成的转发规则不支持编辑和删除。只有当使用该转发规则的所有网站配置取消与当前DDoS高防实例的关联，系统生成的转发规则才会被自动删除。

4.2.2 编辑规则

手动添加的转发规则支持修改其源站IP，系统自动生成的转发规则不支持修改。若需要修改转发规则的源站IP，您可以编辑转发规则。若转发协议和端口发生变化，建议您添加新的转发规则。本文介绍了编辑规则和批量修改转发规则的具体操作。

前提条件

DDoS高防IP下已添加转发规则。更多信息，请参见添加规则。

操作步骤

1. 登录云盾DDoS高防控制台。
2. 在左侧导航栏，单击接入管理 > 端口接入。
3. 在端口配置页面，选择要操作的DDoS高防实例和IP。
4. 定位到要编辑的转发规则，单击其操作列下的编辑。

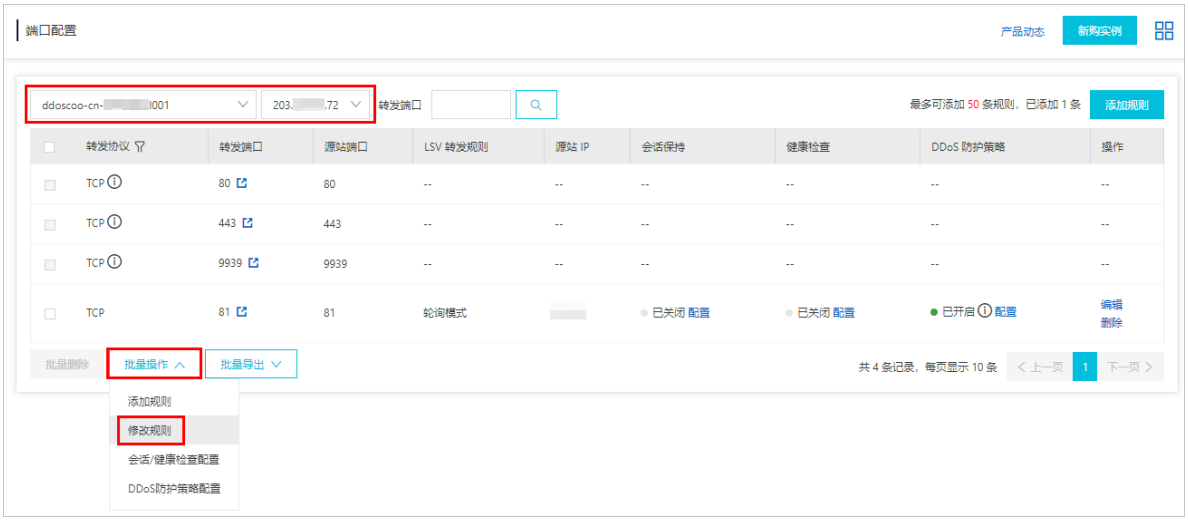
> **说明:**
> 您也可以使用批量操作修改规则，支持一次修改多条规则，具体请参见批量修改规则。

5. 在编辑规则对话框中，修改源站IP，并单击完成。

成功修改转发规则的源站IP。修改后的规则即时生效，DDoS高防IP会按照更新后转发规则转发业务流量。

批量修改规则

1. 登录云盾DDoS高防控制台。
2. 在左侧导航栏，单击接入管理 > 端口接入。
3. 在端口配置页面，选择要操作的DDoS高防实例和IP，并单击规则列表下方的批量操作 > 修改规则。



4. 在修改规则对话框，按照格式要求填入要修改的规则配置，并单击修改。规则配置的格式要求如下。

   - 每行对应一条规则。
   - 每条规则包含四个字段，从左到右依次是协议、转发端口、源站端口、源站IP（字段的含义见规则配置描述），字段间以空格分隔。

   说明:
   批量修改规则仅支持批量修改源站IP。

5. 在修改规则对话框，勾选要上传的规则，确认后并单击上传。

   成功上传修改后的规则。

6. 上传完成后，关闭修改规则对话框。

4.2.3 删除规则

对于手动添加的转发规则，若您不再需要DDoS高防IP对业务进行转发，您必须先恢复实际业务IP，即确保实际业务没有使用高防IP；然后删除对应的转发规则。若您未恢复实际业务IP就删除转发规则，则可能导致业务中断。

前提条件

已恢复实际业务IP。

操作步骤

1. **登录云盾*DDoS*高防控制台。**
2. **在左侧导航栏，单击接入管理 > 端口接入。**
3. **在端口配置页面，选择要操作的DDoS高防实例和IP。**
4. **定位到要删除的转发规则，单击其操作列下的删除。**

   说明:
   如果要删除多条规则，您可以勾选要删除的转发规则，单击规则列表下的批量删除。
5. **在删除提示对话框中，确认删除操作。**

   成功删除转发规则。

4.2.4 批量导出

DDoS高防端口配置支持批量导出。您可以将DDoS高防IP下的全部转发规则（仅限手动添加的规则）、会话/健康配置、DDoS防护策略以txt格式导出并下载到本地。批量导出的配置格式与批量操作（例如批量添加/修改规则、添加会话/健康检查配置、添加DDoS防护策略配置）保持一致。

操作步骤

1. **登录云盾*DDoS*高防控制台。**
2. **在左侧导航栏，单击接入管理 > 端口接入。**
3. **在端口配置页面，选择要操作的DDoS高防实例和IP。**

4. **在规则列表下方，根据要导出的内容类型，选择批量导出 > 导出规则、批量导出 > 导出会话/健康配置、批量导出 > 导出DDoS防护策略，创建相应导出任务。**

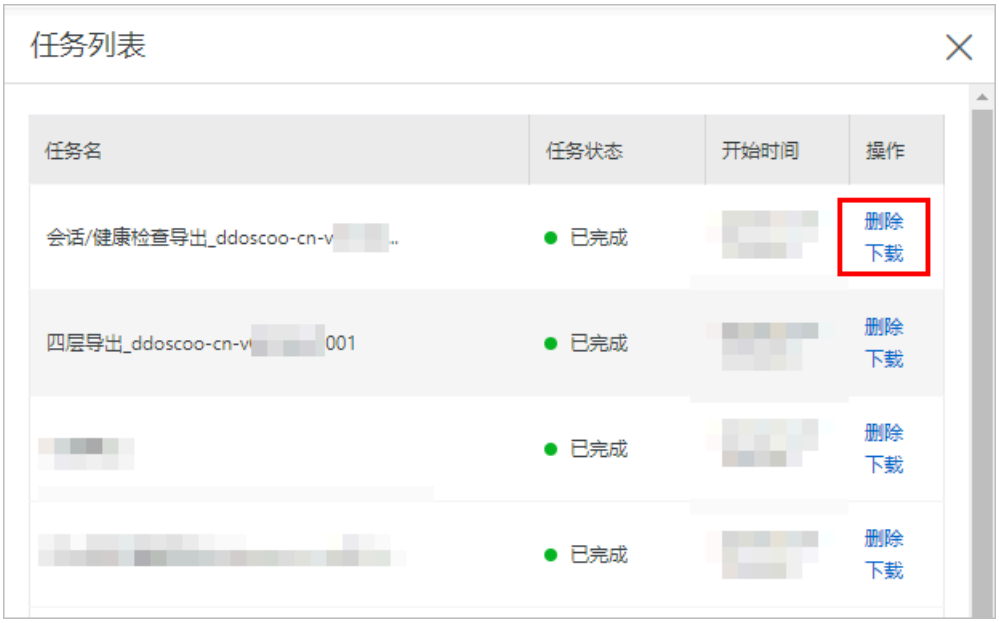
成功下发导出任务。

5. **单击页面右上角的导出任务图标。**

6. **在任务列表侧边页，等待任务打包完成后，单击下载，下载导出文件到本地。**

说明:

如果当前任务状态为待执行状态，请耐心等待导出任务完成。



成功下载导出文件到本地。您可以打开下载的txt文件，查看规则或配置内容。关于txt文件中配置内容的格式，请参见导出格式说明。

7. （可选）在任务列表侧边页，定位到不再需要的任务，单击删除，将其移除。

导出格式说明

导出的文件均为txt格式，根据批量导出类型的不同，导出内容的格式也有区别，具体说明如下。

- **规则文件**

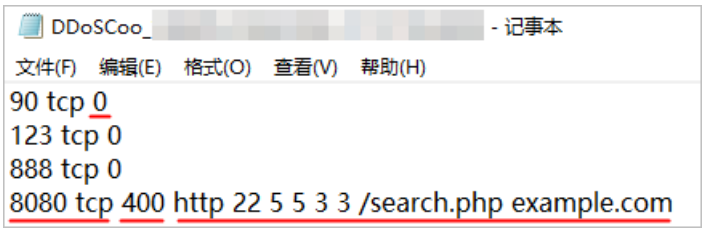
  每行对应一条规则，每条规则包含四个字段，从左到右依次是协议、转发端口、源站端口、源站IP。

  更多信息，请参见批量添加规则。

- **会话/健康配置文件**

  每行对应一个规则的配置，每条配置包含以下字段（从左到右）：转发协议端口、转发协议、会话保持超时时间（若为0则表示未开启会话保持）、健康检查类型（若为空则表示未开启健康检

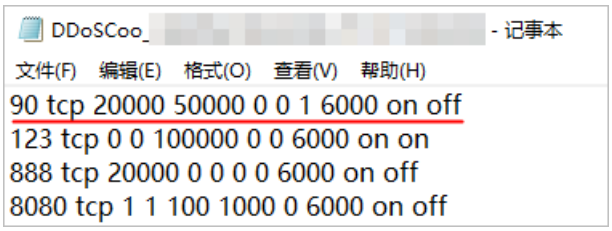
查，且后续字段均为空）、检查端口、检查超时时间、检查间隔、不健康阈值、健康阈值、检查路径（HTTP类型下存在）、域名（HTTP类型下存在）。



更多信息，请参见批量添加会话/健康配置。

- DDoS防护策略文件

每行对应一个规则的配置，每条配置包含以下字段（从左到右）：转发协议端口、转发协议、源新建连接限速、源并发连接限速、目的新建连接限速、目的并发连接限速、包长度最小值、包长度最大值、虚假源与空连接（仅TCP协议时生效，空连接开启前需要先开启虚假源）。



更多信息，请参见批量添加*DDoS*防护策略。

4.2.5 设置健康检查

DDoS高防为已接入防护的非网站业务提供网络四层和七层健康检查功能，适用于业务有多个源站IP时判断后端服务器的业务可用性。在DDoS高防实例（IP）下添加转发规则，接入非网站业务后，您可以单独设置某个端口转发规则的健康检查配置或批量添加会话保持/健康检查配置。本文介绍了具体的操作方法。

前提条件

已在端口配置中添加转发规则。更多信息，请参见添加规则。

背景信息

健康检查适用于配置了多个源站IP的业务。DDoS高防在转发业务流量回源时，通过健康检查判断源服务器的业务可用性，将流量优先转发到状态健康的源服务器，保证业务正常响应。如果在端口转发规则中仅配置了一个源站IP，请不要开启健康检查。更多信息，请参见负载均衡健康检查概述。

DDoS高防的端口配置接入方式为业务提供基于IP地址+端口级别的防护，对于已接入DDoS高防实例的IP和端口提供健康检查功能。您可以针对具体高防IP的转发端口设置健康检查规则。

DDoS高防支持网络四层和七层健康检查配置，具体配置项的描述如下表所示。

> **说明:**
> 高级设置仅在展开高级设置后显示，且建议您使用默认值。四层健康检查和七层健康检查均支持高级设置，且配置项一致。

类型	配置项	说明
四层健康检查	检查端口	健康检查服务访问后端服务器时的探测端口，取值范围：1~65535。默认值为配置监听时指定的后端端口。 **说明:** 适用于TCP和UDP协议规则。
七层健康检查	域名和检查路径	七层健康检查默认由高防转发系统向该服务器应用配置的缺省首页发起HTTP HEAD请求。 **说明:** 仅适用于TCP协议规则，且仅限HTTP协议。 · 如果您用来进行健康检查的页面并不是应用服务器的缺省首页，需要指定域名和具体的检查路径。 · 如果您对HTTP HEAD请求限定了host字段的参数，您只需要指定检查路径，即用于健康检查页面文件的URI。域名不用填写，默认为后端服务器的IP。
	检查端口	健康检查服务访问后端服务器时的探测端口，取值范围：1~65535。默认值为配置监听时指定的后端端口。
高级设置	响应超时时间	每次健康检查相应的最大超时时间，取值范围：1~30（秒）。如果后端服务器在指定的时间内没有正确响应，则判定为健康检查失败。
	检查间隔	进行健康检查的时间间隔，取值范围：1~30（秒）。 **说明:** 高防集群内所有节点都会独立、并行地遵循该属性对后端服务器进行健康检查。由于各高防节点的检查时间并不同步，所以，如果从后端某一服务器上进行单独统计，会发现来自高防IP的健康检查请求在时间上没有遵循指定的时间间隔。
	不健康阈值	同一高防节点服务器针对同一后端服务器，在健康检查状态为成功时，连续多少次健康检查失败后，状态判定为失败，取值范围：1~10。

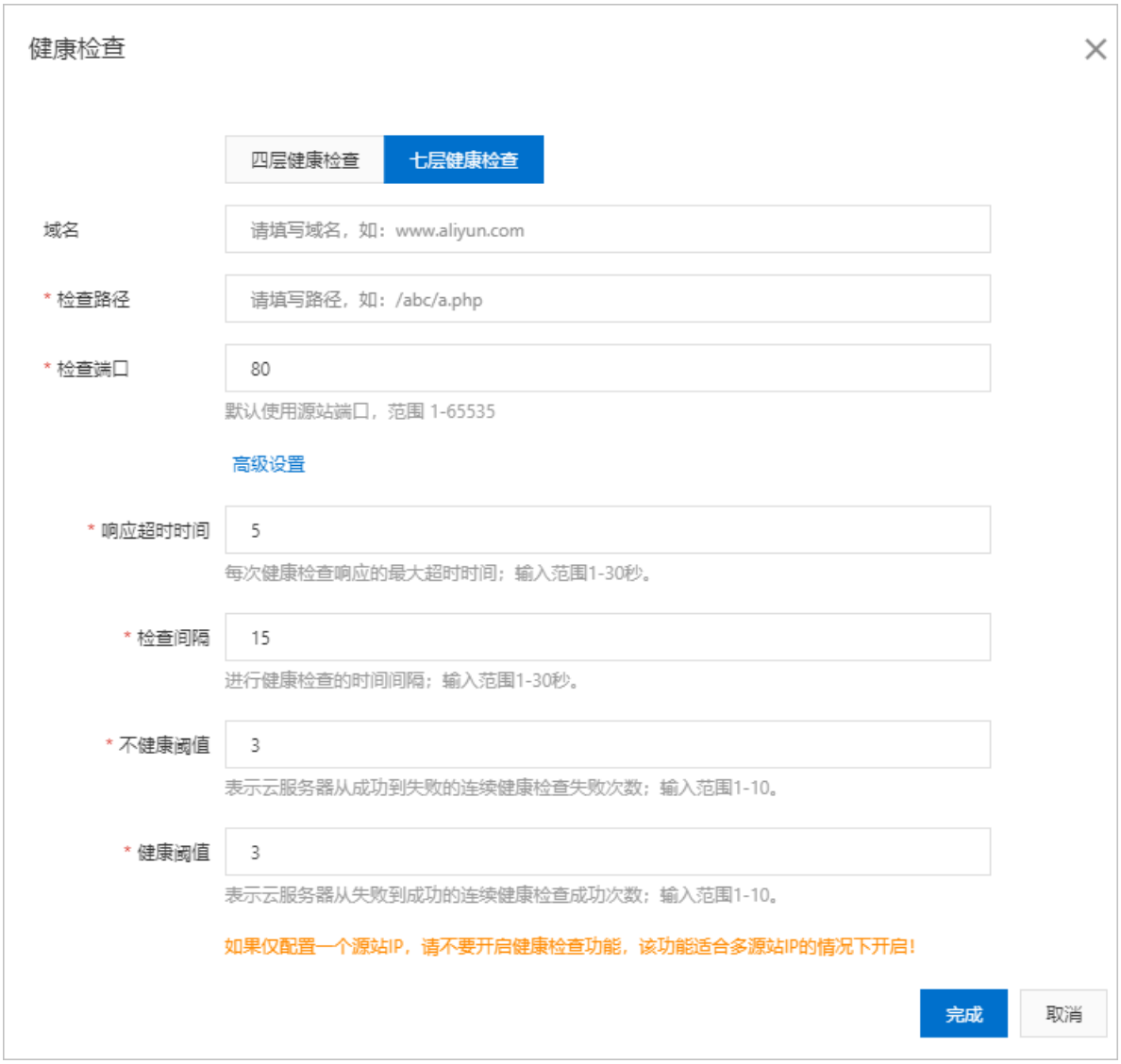
类型	配置项	说明
	健康阈值	同一高防节点服务器针对同一后端服务器，在健康检查状态为失败时，连续多少次健康检查成功，状态判定为成功，取值范围：1~10。

操作步骤

1. 登录云盾DDoS高防控制台。
2. 在左侧导航栏，单击接入管理 > 端口接入。
3. 在端口配置页面，选择DDoS高防实例和IP，并定位到要操作的转发规则，单击其健康检查列下的配置。

> **说明:**
> 您也可以在目标高防实例和IP下使用批量操作，批量调整会话保持/健康检查配置，具体请参见批量添加会话/健康配置。

4. 在健康检查对话框中，完成健康检查配置，并单击完成。健康检查的配置描述见健康检查配置项描述。



批量添加会话/健康配置

1. 登录云盾*DDoS*高防控制台。
2. 在左侧导航栏，单击接入管理 > 端口接入。

3. 在端口配置页面，选择DDoS高防实例和IP，并单击规则列表下方的批量操作 > 会话/健康检查配置。

4. 在添加会话/健康配置对话框中，按照格式要求输入要添加的会话保持/健康检查配置内容，并单击添加。会话保持/健康检查配置的格式要求如下。

> **说明:**
> 您也可以先批量导出当前会话/健康配置，在导出的txt文件中统一调整后再将内容复制粘贴进来。导出文件中的会话/健康配置格式和添加会话/健康配置的格式要求一致。更多信息，请参见批量导出。

- 每行对应一条转发规则的会话保持和健康配置。
- 每条会话/健康配置从左到右包含以下字段：转发协议端口、转发协议（tcp、udp）、会话保持超时时间（单位：秒，取值范围：30~3600）、健康检查类型、检查端口、检查超时时

间、检查间隔、不健康阈值、健康阈值、检查路径、域名。字段间以空格分隔。具体字段的含义见健康检查配置项描述。

- 转发协议端口必须是已添加规则的端口。
- 健康检查类型的取值包括：tcp、http、udp。转发规则协议为UDP时，建议配置udp健康检查；转发规则协议为TCP时，建议配置tcp（四层）或http（七层）健康检查。
- 健康检查类型为http时，检查路径必选，域名可选。

4.2.6 设置会话保持

DDoS高防为已接入防护的非网站业务提供会话保持功能，支持在指定时间范围内将同一客户端的请求转发至同一台后端服务器上。在DDoS高防实例（IP）下添加转发规则，接入非网站业务后，您可以单独设置某个端口转发规则的会话保持配置或批量添加会话保持/健康检查配置。本文介绍了具体的操作方法。

前提条件

已在端口配置中添加转发规则。更多信息，请参见添加规则。

背景信息

DoS高防的端口配置接入方式为业务提供基于IP地址+端口级别的防护，对于已接入DDoS高防实例的IP和端口提供会话保持功能。您可以针对具体高防IP的转发端口设置会话保持规则。

操作步骤

1. 登录云盾DDoS高防控制台。
2. 在左侧导航栏，单击接入管理 > 端口接入。

3. 在端口配置页面，选择DDoS高防实例和IP，并定位到要操作的转发规则，单击其会话保持列下的配置。

> **说明：**
> 您也可以在目标高防实例和IP下使用批量操作，批量调整会话/健康检查配置，具体请参见批量添加会话/健康配置。

4. 在会话保持对话框中，设置超时时间（单位：秒，取值范围：30~3600），并单击完成。

批量添加会话/健康配置

1. 登录云盾DDoS高防（新BGP）控制台。
2. 在左侧导航栏，单击接入管理 > 端口接入。

3. 在端口配置页面，选择DDoS高防实例和IP，并单击规则列表下方的批量操作 > 会话/健康检查配置。

4. 在添加会话/健康配置对话框中，按照格式要求输入要添加的会话保持/健康检查配置内容，并单击添加。会话保持/健康检查配置的格式要求如下。

> **说明:**
> 您也可以先批量导出当前会话/健康配置，在导出的txt文件中统一调整后再将内容复制粘贴进来。导出文件中的会话/健康配置格式和添加会话/健康配置的格式要求一致。更多信息，请参见批量导出。

- 每行对应一条转发规则的会话保持和健康配置。
- 每条会话/健康配置从左到右包含以下字段：转发协议端口、转发协议（tcp、udp）、会话保持超时时间（单位：秒，取值范围：30~3600）、健康检查类型、检查端口、检查超时时

间、检查间隔、不健康阈值、健康阈值、检查路径、域名。字段间以空格分隔。具体字段的含义见健康检查配置项描述。

- 转发协议端口必须是已添加规则的端口。
- 健康检查类型的取值包括：tcp、http、udp。转发规则协议为UDP时，建议配置udp健康检查；转发规则协议为TCP时，建议配置tcp（四层）或http（七层）健康检查。
- 健康检查类型为http时，检查路径必选，域名可选。

4.3 业务接入配置

4.3.1 修改DNS解析接入网站业务

在DDoS高防添加网站配置后，您必须更新网站域名的DNS解析，才能将网站业务流量切换至DDoS高防实例进行防护。本文以网站域名解析托管在阿里云云解析DNS为例，介绍了手动修改域名解析（CNAME或A记录）以接入DDoS高防的操作方法。

前提条件

在手动修改DNS解析接入网站业务前，您需要完成以下准备工作：

- 网站业务已添加网站配置。更多信息，请参见添加网站。
- 源站服务器已放行DDoS高防回源IP。如果您的源站服务器上部署了非阿里云安全软件（例如防火墙），请将DDoS高防的回源IP地址加入安全软件的白名单。更多信息，请参见放行DDoS高防回源IP。
- 验证转发配置生效。强烈建议您在切换网站访问流量前，在本地验证DDoS高防实例的业务转发配置已经生效。更多信息，请参见本地验证转发配置生效。

选择接入方式

在DDoS高防控制台添加网站时，您为网站选择关联DDoS高防实例（IP）；成功添加网站后，DDoS高防为网站分配一个CNAME地址。您可以登录DDoS高防（新BGP）控制台，在网站配置页面（单击左侧导航栏的接入管理 > 域名接入）查看域名的CNAME和关联高防IP。

手动修改DNS解析接入网站业务时，您可以选择将网站域名的解析指向高防CNAME地址或关联高防IP。

- 使用CNAME解析接入DDoS高防，只需完成一次解析修改，即使后续网站的关联高防IP发生变化，您无需重新修改解析，DDoS高防将通过CNAME自动完成调度；且在网站关联多个高防IP时，DDoS高防自动在多IP间切换流量。
- 若使用A记录解析接入，则当网站的关联高防IP发生变化时，您必须重新修改解析；在网站关联多个高防IP时，您必须手动在多IP间切换流量。

我们推荐您使用CNAME方式接入，仅在CNAME解析不被支持或与别的记录存在冲突时，再选择A记录方式接入。

操作步骤

以下操作描述建立在您的域名DNS托管在阿里云云解析DNS。

> **说明:**
> 云解析DNS是阿里云提供的域名解析服务，支持免费的公共DNS服务和付费版增值服务。如果您的域名已开通付费版云解析DNS服务，我们推荐您使用NS接入（即自动修改DNS）的方式接入DDoS高防。更多信息，请参见NS方式接入网站业务。

若您使用其他DNS服务商的域名解析服务，请登录服务商系统并修改网站域名的解析记录，下文内容仅供参考。

假设在DDoS高防控制台已添加网站的域名为`bgp.ddostest.com`；以下操作示例描述了在云解析DNS控制台修改/新增域名解析的具体操作。

1. 登录阿里云云解析DNS控制台。

2. 在域名解析页面，定位到要操作的域名（本示例中为ddostest.com），单击其操作列下的解析设置。

3. 在解析设置页面，定位到要修改的解析记录（本示例中，即主机记录为bgp的A记录或CNAME记录），单击其操作列下的修改。

说明:

如果要操作的解析记录不在记录列表中，您可以单击添加记录。

4. 在修改记录（或添加记录）对话框，选择一种接入方式，修改解析记录。

- （推荐）CNAME解析接入：选择记录类型为CNAME，并将记录值修改为域名的DDoS高防CNAME地址。

- A记录解析接入：选择记录类型为A，并将记录值修改为域名的关联高防IP。

5. 单击确定，等待修改后的解析设置生效。

6. 测试网站访问是否正常。

下一步

业务接入DDoS高防后，您可以根据需要完成以下任务：

- 启用流量调度器，设置DDoS高防与云资源间的联动规则，仅在特定场景下触发并切换启用DDoS高防。更多信息，请参见流量调度器。
- 更换源站ECS公网IP。若您的源站IP不慎暴露，攻击者有可能绕过高防直接攻击源站，这种情况下，您可以通过DDoS高防更换后端ECS的IP。更多信息，请参见更换源站ECS公网IP。

4.3.2 NS方式接入网站业务

网站业务接入DDoS高防时，您在网站配置中添加网站，然后修改网站域名的DNS解析，将业务流量切换到DDoS高防实例进行防护。开启NS方式接入帮助您自动修改域名DNS解析，但前提是您的域名解析托管在阿里云云解析DNS且已开通云解析DNS付费版服务。本文介绍了使用NS接入的操作方法。

前提条件

- 网站域名的DNS解析托管在阿里云云解析DNS，且已开通云解析DNS付费版。更多信息，请参见云解析DNS产品详情。
- 网站业务已添加网站配置。更多信息，请参见添加网站。
- 源站服务器已放行DDoS高防回源IP。如果您的源站服务器上部署了非阿里云安全软件（例如防火墙），请将DDoS高防的回源IP地址加入安全软件的白名单。更多信息，请参见放行DDoS高防回源IP。
- 验证转发配置生效。强烈建议您在切换网站访问流量前，在本地验证DDoS高防实例的业务转发配置已经生效。更多信息，请参见本地验证转发配置生效。

背景信息

开启NS方式接入后，DDoS高防将依据网站配置中的转发信息，自动更新云解析DNS中的解析记录，实现业务流量的简便切换。NS方式支持两种工作模式，即高防模式和回源模式。

- 高防模式：将业务流量牵引到DDoS高防，即开启DDoS防护。

- 回源模式：将业务流量直接指回源站，即关闭DDoS防护。

下文描述了开启和配置NS方式接入的具体操作。若因特殊情况无法使用NS方式（例如域名解析托管在其他DNS解析服务商且不方便迁移等），请通过手动修改DNS解析的方式接入网站业务。更多信息，请参见修改DNS解析接入网站业务。

操作步骤

1. 登录云盾DDoS高防控制台。
2. 在左侧导航栏，单击接入管理 > 域名接入。
3. 在网站配置列表中，定位到要操作的域名，单击其操作列下的DNS设置。

4. 在NS方式接入下，开启状态开关并选择接入模式：高防、回源。
   - 高防模式：自动更新云解析DNS配置，将当前域名的解析目标指向DDoS高防实例。
   - 回源模式：自动更新云解析DNS配置，将当前域名的解析目标指向源站。

如果当前阿里云账号已开通云解析DNS付费版服务，开关将正常开启；如果未开通云解析DNS付费版服务，将提示无法使用NS方式。

5. 完成配置后，等待域名解析生效。您可以通过第三方DNS测试平台检测该域名的最新解析结果是否符合预期。

4.3.3 CNAME解析接入非网站业务

非网站（四层）业务接入DDoS高防时，您在端口配置中添加转发规则，并将业务地址设置为高防IP即可。但在某些场景下，您可能需要用域名来接入四层业务，并实现业务关联多高防IP且多高防IP间自动切换流量。这种情况下，推荐您通过添加域名并修改CNAME解析来接入非网站业务。

背景信息

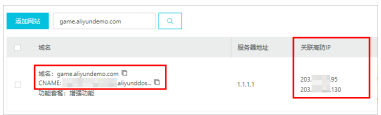
假设您要为游戏业务接入DDoS高防，并希望用户通过解析游戏服务器的域名（game.aliyundemo.com）来获取服务器IP（也就是DDoS高防IP），游戏的TCP端口为1234和5678，源站为1.1.1.1。

操作步骤

1. 在网站配置中添加网站，获取CNAME地址。
   a) 登录云盾DDoS高防（新BGP）控制台。
   b) 在左侧导航栏，单击接入管理 > 域名接入。
   c) 在网站配置页面，单击添加网站。
   d) 在添加网站页面，完成填写网站信息任务，并单击添加。要添加的配置描述如下。
      - 功能套餐和实例：选择要关联的DDoS高防实例（IP）。本示例中假设关联增强功能下的两个实例。
      - 网站：填写业务域名。本示例中是game.aliyundemo.com。
      - 协议类型和服务器端口：保持默认。
      - 服务器地址：选择源站IP，并根据实际情况填写。
        - 如果业务域名下有真实的网站业务，则必须提供正确的协议类型和源站IP。
        - 否则，您可以随意填写源站IP，因为该网站配置不用于实际业务转发。实际业务转发通过在步骤2中添加的端口转发规则实现。

   更多信息，请参见添加网站。

   成功添加网站，DDoS高防为域名分配一个CNAME地址。



2. 在端口配置中添加转发规则。

a) 在左侧导航栏，单击管理 > 端口配置。

b) 在端口配置页面，选择要操作的DDoS高防实例和IP，并单击添加规则。

> **说明:**
> 此处的DDoS高防IP即步骤1为域名关联的高防IP。本示例中有两个，选择其中任意一个。

c) 在添加规则对话框，根据您的实际业务情况完成规则配置，并单击完成。要添加的配置描述如下。

- 转发协议：本示例中选择TCP。
- 转发端口：本示例中填写1234。
- 源站端口：本示例中填写1234。
- 源站IP：填写真实源站IP，本示例中是1.1.1.1。

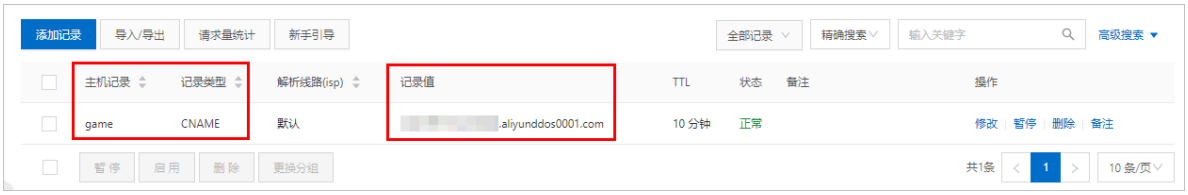
更多信息，请参见添加规则。

成功添加转发规则。

d) 重复上述两个步骤，在当前高防实例和IP下再添加一个转发规则，将转发端口和源站端口设置为5678。

e) 参照上述三个步骤，为其他DDoS高防实例配置同样的转发规则。

3. 前往域名（game.aliyundemo.com）的DNS解析服务商，手动修改域名的DNS解析，启用CNAME解析并将解析指向步骤1中获得的CNAME地址。



更多信息，请参见修改DNS解析接入网站业务。

4.3.4 修改CNAME解析接入流量调度器

使用流量调度器添加调度规则后，您必须更新规则对应域名的DNS解析CNAME记录，将网站业务流量切换至流量调度器，使规则生效。本文以网站域名解析托管在阿里云云解析DNS为例，介绍了手动修改域名解析CNAME记录以接入流量调度器的操作方法。

前提条件

已使用流量调度器添加防护调度规则、CDN联动。更多信息，请参见流量调度器。

背景信息

使用流量调度器添加防护调度规则或CDN联动后，流量调度器为规则或域名分配一个CNAME地址。您可以登录DDoS高防（新BGP）控制台，在接入管理 > 流量调度器页面查看规则或域名的CNAME。

修改CNAME解析接入流量调度器时，您将网站域名的解析指向流量调度器CNAME地址。

- 防护调度规则：将联动云资源IP对应的域名解析指向防护调度规则的CNAME地址。
- CDN联动：将开启CDN联动的域名的解析指向流量调度器CNAME地址。

以下操作描述建立在您的域名DNS托管在阿里云云解析DNS。

若您使用其他DNS服务商的域名解析服务，请登录服务商系统并修改网站域名的解析记录，下文内容仅供参考。

假设调度规则对应的网站域名为`bgp.ddostest.com`；以下操作示例描述了在云解析DNS控制台修改/新增域名解析的具体操作。

操作步骤

1. 登录阿里云云解析DNS控制台。
2. 在域名解析页面，定位到要操作的域名（本示例中为ddostest.com），单击其操作列下的解析设置。

3. 在解析设置页面，定位到要修改的解析记录（本示例中，即主机记录为bgp的A记录或CNAME记录），单击其操作列下的修改。

> **说明:**
> 如果要操作的解析记录不在记录列表中，您可以单击添加记录。

4. 在修改记录（或添加记录）对话框，选择记录类型为CNAME，并将记录值修改为防护调度规则或CDN联动域名的CNAME地址。

5. 单击确定，等待修改后的解析设置生效。

6. 测试网站访问是否正常。

4.4 流量调度器

DDoS高防流量调度器允许您设置DDoS高防与云资源间的联动规则，仅在特定场景下触发并切换启用DDoS高防，保证无DDoS攻击时日常业务的流畅体验以及发生DDoS攻击时更好的防护效果。流量调度器提供云产品联动、阶梯防护、CDN联动功能。本文介绍了它们的使用场景和配置方法。

使用场景

下表描述了DDoS高防流量调度器的不同功能的使用场景。

功能	使用场景	使用效果
云产品联动	日常不使用高防，不增加延迟；被攻击时，需要将DDoS高防前置，防护DDoS攻击。	无攻击时，高防做备用，不增加延迟；被攻击时，自动切换至DDoS高防。 
阶梯防护	日常使用防护包防御DDoS，无延迟增加；被大流量攻击的时候，需要切到DDoS高防。	防护包抵御日常攻击，不增加延迟；大流量攻击时，切换至DDoS高防。 
CDN联动	网站使用CDN加速，又需要防御DDoS攻击；当攻击发生时，需要从CDN切换至DDoS高防。	无攻击时，就近使用CDN节点加速；被攻击时，切换至DDoS高防。 

使用限制

下表描述了DDoS高防流量调度器的不同功能的使用限制。

功能	限制条件	说明
云产品联动	高防实例规格	DDoS高防实例的QPS、业务带宽等规格满足正常业务防护需求，当流量切至高防时，确保可以承载业务流量。
	高防配置	DDoS高防实例预先完成被防护业务的转发配置。
阶梯防护	防护包	购买并使用防护包企业版。
	实例规格	防护包业务带宽规格满足防护需求。

功能	限制条件	说明
	高防配置	DDoS高防实例预先完成被防护业务的转发配置。
	防护包配置	云资源在防护包的防护对象中。
CDN联动	CDN状态	域名不允许是切入沙箱状态。  说明: 如果域名已经被CDN切入沙箱，建议您只用DDoS高防，不用联动。
	攻击频率	不适合被攻击频率太高的网站，例如高于每周3次以上。
	防护生效敏感度	不适合对防护生效速度要求比较高的场景。  说明: 调度到DDoS高防时，防护生效时间受DNS TTL生效时间限制。
	业务流量	不适合正常业务流量和QPS比较大的场景。  说明: 若超过3 Gbps、10000 QPS时，请提交工单进行评估。
	业务类型	只适合HTTP和HTTPS业务，不支持视频直播。
	高防版本	仅支持增强功能版本的DDoS高防实例。

配置概述

功能	配置说明
云产品联动	云产品联动分为云产品与DDoS高防一对一切换、云产品与DDoS高防多对一切换。 配置步骤如下。 1. 配置DDoS高防转发。参见添加网站配置。 2. 验证高防实例可以正常转发。参见验证配置生效。 3. 配置流量调度器。 · 一对一切换，参见添加防护调度规则。 · 多对一切换，包括以下两种配置模式： - 优先使用云产品，无可用云产品IP时，切换高防。配置方法同一对一切换，在添加防护调度规则时，选择添加多个需要联动的云资源IP即可。 - 云产品多路分摊流量，每路被攻击单独切换高防。配置方法参见多路分摊切换配置示例。 4. 将DNS解析到流量调度器。修改域名的DNS解析，应用CNAME解析并将解析目标设置为调度器分配的CNAME地址。 说明: 关于修改域名DNS解析CNAME记录的操作步骤，业务接入DDoS高防配置可供参考，但请注意应该应用流量调度器分配的CNAME地址，而不是DDoS高防CNAME地址。
阶梯防护	阶梯防护分为防护包中云产品与DDoS高防一对一切换、防护包中云产品与DDoS高防多对一切换。配置步骤与云产品联动相同。
CDN联动	配置步骤如下。 1. 预先配置好CDN，并解析到CDN，经测试可用。 参见添加加速域名。 说明: 如果配置了源站防护（安全组），则需要将CDN回源地址加入白名单。 2. 配置DDoS高防转发。参见添加网站配置。 3. 验证高防实例可以正常转发。参见验证配置生效。 4. 配置流量调度器。参见添加CDN联动。 5. 将DNS解析到流量调度器。修改域名的DNS解析，应用CNAME解析并将解析目标设置为调度器分配的CNAME地址。 说明: 关于修改域名DNS解析CNAME记录的操作步骤，业务接入DDoS高防配置可供参考，但请注意应该应用流量调度器分配的CNAME地址，而不是DDoS高防CNAME地址。

添加防护调度规则

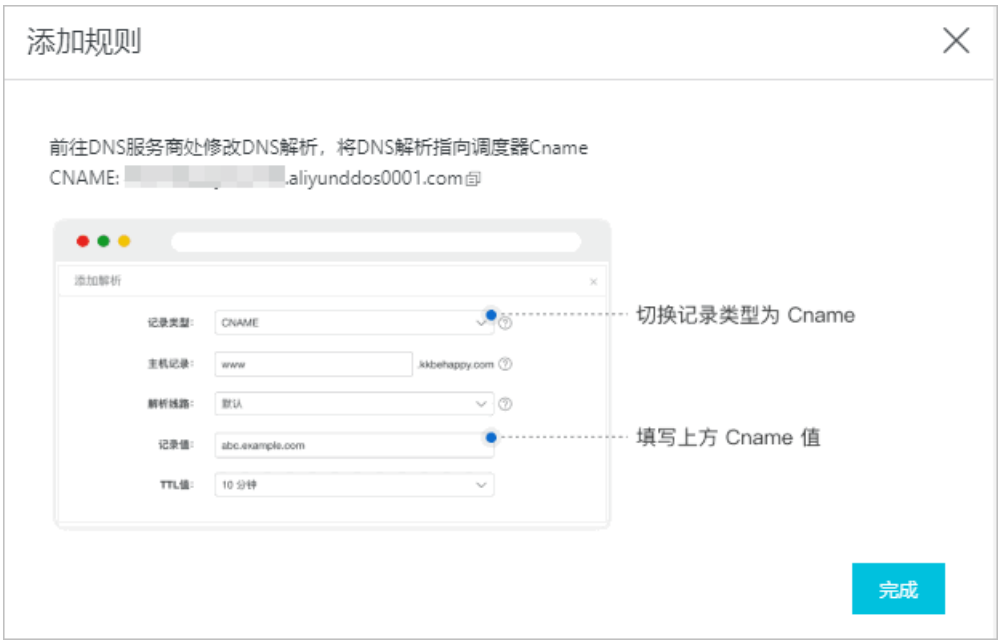
1. 登录云盾DDoS高防控制台。
2. 在左侧导航栏，单击接入管理 > 流量调度器。
3. 在防护调度页签下，单击添加规则。

4. 在添加规则侧边页，完成联动规则配置，并单击下一步。联动规则的配置描述见下表。

配置项	说明
联动场景	选择规则类型，取值： · 云产品联动 · 阶梯防护（仅支持DDoS防护包防护对象中的云资源，包括ECS、EIP、SLB、WAF）
规则名	为规则命名。规则名由英文字母、数字和下横线（_）组成，且不超过128个字符。
高防IP	选择要联动的高防实例。

配置项	说明
云资源	设置要联动的云资源。选择云资源所在地域，并输入云资源IP地址。单击添加源资源IP，可以添加多个云资源。最多支持添加20个IP。

成功添加规则，调度器为新建规则分配一个CNAME地址。要使调度规则生效，您需要前往云资源的DNS服务商处修改其DNS解析，应用CNAME解析并将解析目标设置为调度器分配的CNAME地址。



您可以在防护调度规则列表中查看新建的规则和CNAME地址。

添加CDN联动

启用CDN联动功能时，您需要设置访问QPS阈值，作为CDN和DDoS高防间相互切换的条件。访问QPS指所有客户端访问当前域名配置的CDN域名的QPS，而不是CDN回源QPS。CDN和DDoS高防间相互切换满足以下逻辑。

- **CDN切换到高防**
  - **连续3分钟内3次触发访问QPS超过阈值或连续10分钟内出现6次以上，则触发切换流程。**
  - **CDN上流量不超过10 Gbps。**
- **高防切换到CDN**
  - **连续12小时以上，域名QPS低于QPS阈值的80%。**
  - **连续12小时以上，CC阻断率低于10%。**
  - **回切检查：要切回的高防IP不在清洗黑洞中且1小时内不存在清洗、黑洞事件。**
  - **回切时间范围：8:00~23:00。**

> **说明:**
> **其他时间范围不触发回切。**

1. **在左侧导航栏，单击接入管理 > 流量调度器。**
2. **打开CDN联动调度页签。**
   CDN联动调度页签展示了所有已添加到DDoS防护中的网站域名。
3. **定位到要配置的域名，单击其操作列下的添加联动。**

4. 在添加联动侧边页，确认域名信息满足要求后，配置切换至高防条件，即访问QPS的最小值，并单击下一步。

   要添加联动，域名信息应满足以下要求。

   - 高防资源：已开通增强功能。

   - 联动资源：已完成阿里云CDN配置。

   说明：

   建议您在设置QPS阈值时，考虑业务突增的情形，将阈值设置为业务历史峰值的2~3倍以上。即使网站QPS较低，QPS阈值也建议不要低于500。

   成功添加联动，调度器为新建规则分配一个CNAME地址。要使调度规则生效，您需要前往云资源的DNS服务商处修改其DNS解析，应用CNAME解析并将解析目标设置为调度器分配的CNAME地址。

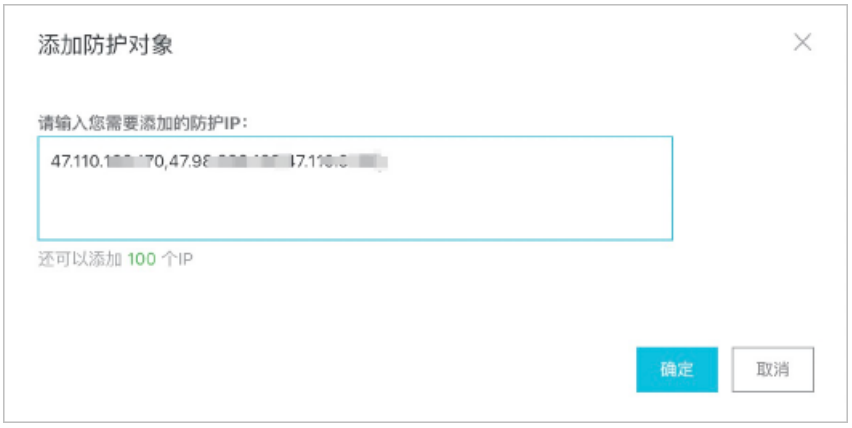
   

   您可以在CDN联动调度规则列表中看到域名的CDN联动状态更新为已开启，并查看其CNAME地址。

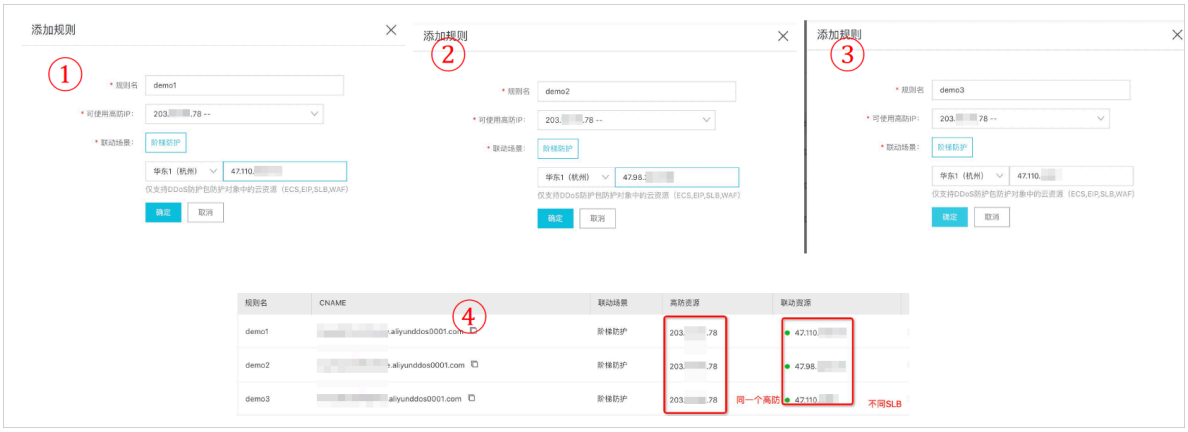
多路分摊切换配置示例

以多防护包切换DDoS高防为例，介绍云产品与DDoS高防多对一切换（云产品多路分摊流量，每路被攻击单独切换高防模式）的具体配置方法。其中，CNAME解析记录的更新以阿里云云解析DNS为例截图说明。

1. 防护包配置。在防护包中添加多个防护对象，示例中是三个。



2. 流量调度器配置。为步骤1中的三个防护对象各添加一条阶梯防护规则，三条规则关联同一个高防IP。



3. 域名解析配置。使用同一个主机记录，添加三条CNAME解析记录，记录值分别是步骤2中三条阶梯防护规则的CNAME地址。

4. 验证结果。在*http://tool.chinaz.com/*上验证步骤3中添加的CNAME记录生效。

4.5 放行DDoS高防回源IP

为网站启用DDoS高防服务时，为了避免DDoS高防的回源流量被源站服务器上的安全软件误拦截，建议您设置放行DDoS高防回源IP。

背景信息

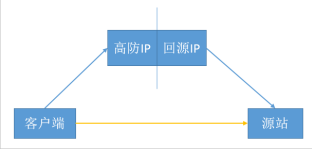
如果您的源站服务器上部署了非阿里云安全软件（例如防火墙），请将DDoS高防的回源IP地址加入安全软件的白名单。

注意:

完成网站业务切换后，网站的正常访问流量经过DDoS高防实例清洗，并由DDoS高防回源IP地址转发至源站服务器。因此，如果DDoS高防的回源地址不在源站防火墙的白名单中，访问流量可能被错误拦截，导致网站无法访问。

网站成功接入DDoS高防后，所有网站访问请求将先流转到DDoS高防，经DDoS高防实例清洗后再返回到源站服务器。流量经DDoS高防实例返回源站的过程称为回源。

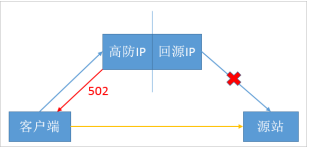
DDoS高防作为一个反向代理，其中包含了一个Full NAT的架构。



没有启用DDoS高防代理时，对于源站来说真实客户端的地址是非常分散的，且正常情况下每个源IP的请求量都不大。

启用DDoS高防代理后，由于高防回源的IP段固定且有限，对于源站来说所有的请求都是来自高防回源IP段，因此分摊到每个回源IP上的请求量会增大很多（可能被误认为回源IP在对源站进行攻击）。此时，如果源站有其它防御DDoS的安全策略，很可能对回源IP进行拦截或者限速。

例如，最常见的502错误，即表示高防IP转发请求到源站，但源站却没有响应（因为回源IP可能被源站的防火墙拦截）。

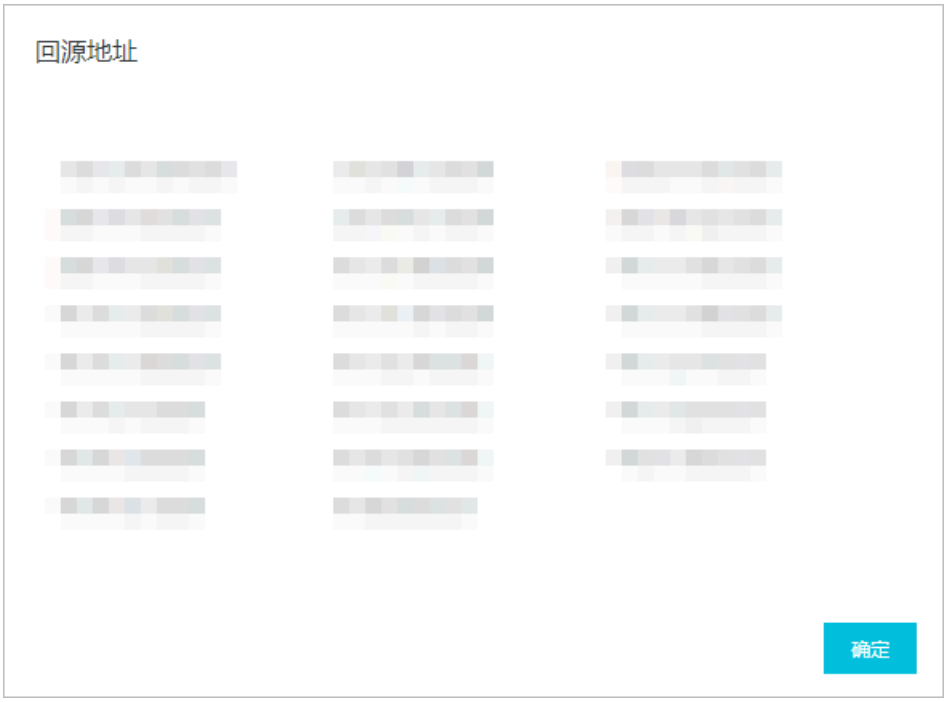


所以，在配置完转发规则后，强烈建议您关闭源站上的防火墙和其他任何安全类软件（如安全狗等），确保高防的回源IP不受源站本身安全策略的影响；或者请参见以下操作步骤，在源站服务器的安全软件中设置放行DDoS高防的回源IP地址。同时，建议您参考高防源站保护通过安全组或白名单功能为您的源站配置保护措施。

操作步骤

1. 登录云盾DDoS高防控制台。
2. 在左侧导航栏，单击接入管理 > 域名接入。
3. 在网站配置页面上方，单击查看BGP高防的回源地址。

4. 在回源地址对话框中，查看并复制DDoS高防的回源地址。



5. 打开源站服务器上的安全软件，将复制的IP段添加到白名单。

4.6 本地验证转发配置生效

成功添加DDoS高防网站或端口配置后，DDoS高防预期会把请求高防IP对应端口的报文转发到源站（真实服务器）的对应端口。为了保证业务的稳定，我们建议您在进行业务接入高防配置前先完成本地验证，确保转发配置已经生效。本文将指导您完成本地验证。

前提条件

- 已在DDoS高防控制台添加网站或端口配置。更多信息，请参见添加网站、添加规则。
- 已在源站服务器上设置放行DDoS高防回源IP。更多信息，请参见放行DDoS高防回源IP。

背景信息

对于需要通过域名访问的业务（例如客户端中使用的服务器地址是域名而不是IP），在为该类型业务接入DDoS高防时，您需要添加网站配置。添加网站配置后，您可以通过修改本地hosts文件或者使用高防Cname地址访问服务器的方式验证转发配置生效。

有的四层业务（例如游戏业务）可能不需要域名，直接通过IP进行交互。在为该类型业务接入DDoS高防时，您需要添加端口转发规则。添加转发规则后，您可以通过使用高防IP访问服务器的方式验证转发配置生效。

注意:

如果转发配置未生效就执行业务切换，将可能导致业务中断。

修改本地hosts文件

1. **修改本地hosts文件，使本地对于被防护站点的请求经过高防。以Windows操作系统为例，操作步骤如下。**
   a) **定位到hosts文件。一般hosts文件存储在**`C:\Windows\System32\drivers\etc\`**文件夹下。**
   b) **用记事本或Notepad++等文本编辑器打开hosts文件。**
   c) **在最后一行添加如下内容：**`高防IP地址 网站域名`**。**
   例如高防IP是`180.xx.xx.173`**，域名是**`www.aliyundemo.com`**，则在hosts文件最后一行添加的内容为**`180.xx.xx.173 www.aliyundemo.com`**。**

   d) **保存修改后的hosts文件。**
2. **在本地计算机对被防护的域名运行Ping命令。**
   预期解析到的IP地址是在hosts文件中绑定的高防IP地址。如果依然是源站地址，请尝试刷新本地的DNS缓存（在Windows的命令提示符中运行`ipconfig/flushdns`**命令。）**
3. **确认本地解析已经切换到高防IP以后，使用原来的域名进行测试，如果能正常访问则说明配置已经生效。**

使用高防Cname地址访问服务器

如果客户端支持填写服务器域名，您可以把原来的域名替换成DDoS高防服务分配的接入Cname地址，测试访问是否正常。

说明:
成功添加网站配置后，DDoS高防为域名分配一个Cname地址，用于业务接入配置。您可以在网站配置列表中查看域名对应的Cname地址。

如果无法正常访问，请确认前提条件中的配置正确。如问题依然存在，请联系阿里云售后技术支持。

使用高防IP访问服务器

假设高防IP是99.99.99.99，配置了端口1234的转发，源站IP是11.11.11.11，对应服务端口也是1234。

添加端口配置后，您可以直接在本地通过telnet命令访问高防IP 99.99.99.99的1234端口，telnet命令能连通则说明转发成功。

如果本地客户端支持直接填写服务器IP，您也可以直接填入高防IP进行测试。

4.7 更换源站ECS公网IP

若您的源站IP已暴露，建议您更换阿里云ECS云服务器的公网IP，防止黑客绕过DDoS高防直接攻击源站。您可以在DDoS高防管理控制台更换后端ECS的IP，每个账号最多可更换10次。

背景信息

> **说明:**
> 更换ECS IP功能仅支持使用经典网络公网IP的ECS更换IP。

操作步骤

1. 单击更换ECS IP。

   > **注意:**
   > 更换ECS IP会使您的业务暂时中断几分钟，建议您在操作前先备份好数据。

2. 更换ECS IP需要将ECS停机，若您已将需要更换IP的ECS停机，请直接跳转到步骤6。在更换ECS IP对话框，单击前往ECS，并在ECS管理控制台将需要更换IP的ECS实例停机。
   a) 在实例列表中找到目标ECS实例，单击其实例ID。
   b) 在实例详情页，单击停止。
   c) 选择停止方式，并单击确定。

      > **注意:**
      > 停止ECS实例是敏感操作，稳妥起见，需要您输入手机校验码。

   d) 等待ECS实例状态变成已停止。
3. 返回更换ECS IP对话框，输入ECS实例ID，并单击下一步。
4. 确认当前ECS实例信息准确无误（尤其是ECS IP）后，单击释放IP。
5. 成功释放原IP后，单击下一步，为该ECS实例自动分配新的IP。
6. ECS IP更换成功，单击确认，完成操作。

   > **说明:**
   > 更换IP成功后，请您将新的IP隐藏在BGP高防后面，不要对外暴露。

5 查看安全总览

业务接入DDoS高防并切换业务流量至DDoS高防实例后，您可以在DDoS高防控制台的安全总览页面实时查看业务指标和DDoS攻击事件的防护情况。

背景信息

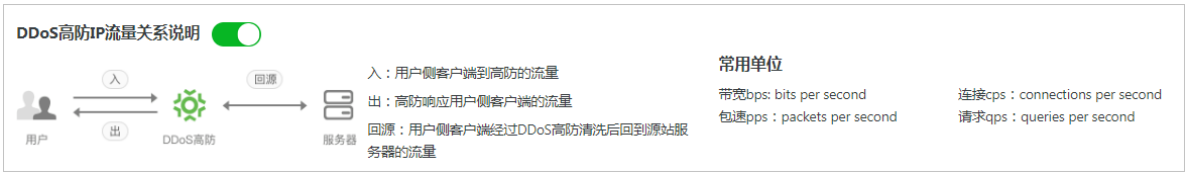
DDoS高防的安全总览页面向您展示以下业务指标和DDoS攻击事件的概览：

- 业务指标：业务带宽、业务QPS、业务CPS、接入防护的域名、接入防护的端口。
- DDoS攻击事件：流量型、连接型和Web资源消耗型三种DDoS攻击事件的记录。

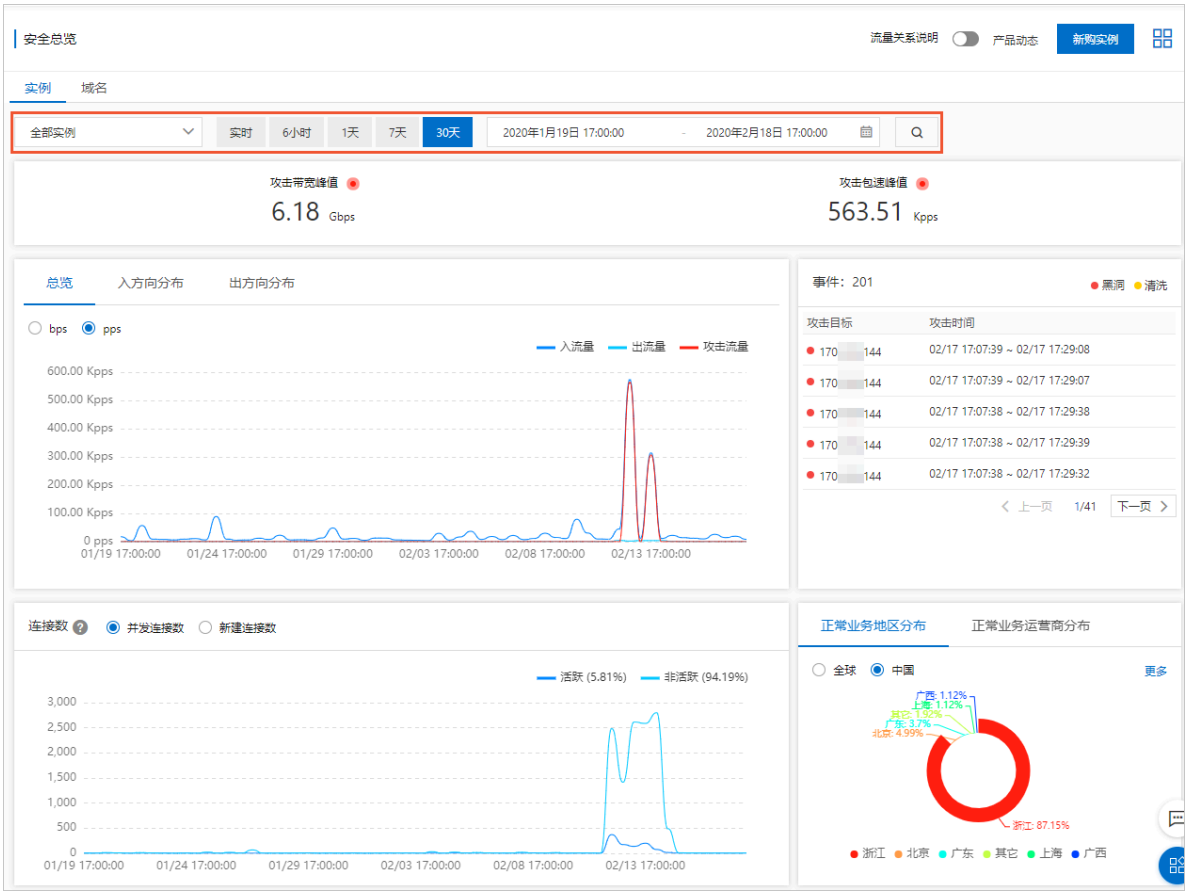
操作步骤

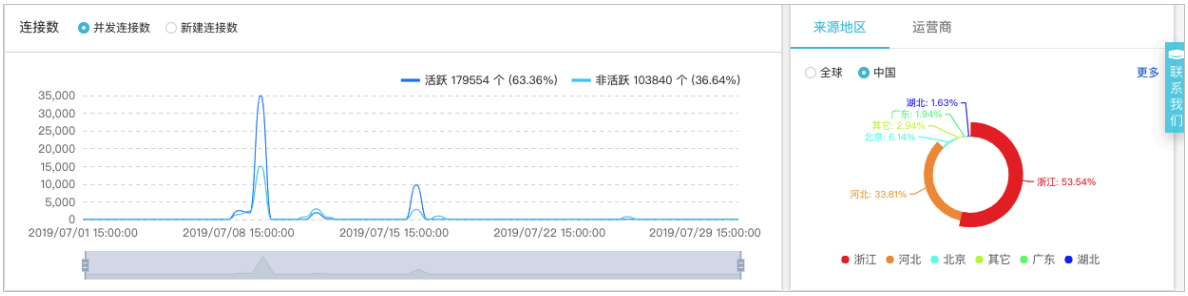
1. 登录云盾DDoS高防（新BGP）控制台。
2. 在左侧导航栏，单击安全总览。
3. （可选）展开流量关系说明，查看并熟悉DDoS高防IP的背景信息及相关概念。

   DDoS高防IP流量关系说明展示了DDoS高防IP的流量关系说明、高防数据指标的名词解释和常用数据单位。



4. 打开实例页签，设置要查询的时间范围，查看指定实例对应业务的相关信息。





支持查看的实例业务信息包括以下内容。

- 攻击带宽峰值和攻击包速峰值
- 带宽趋势（入流量、攻击流量、出流量）
- （攻击）事件

  将鼠标放到被攻击的IP或端口上，可以展示被攻击的IP和端口信息、攻击的类型和峰值、防护结果。

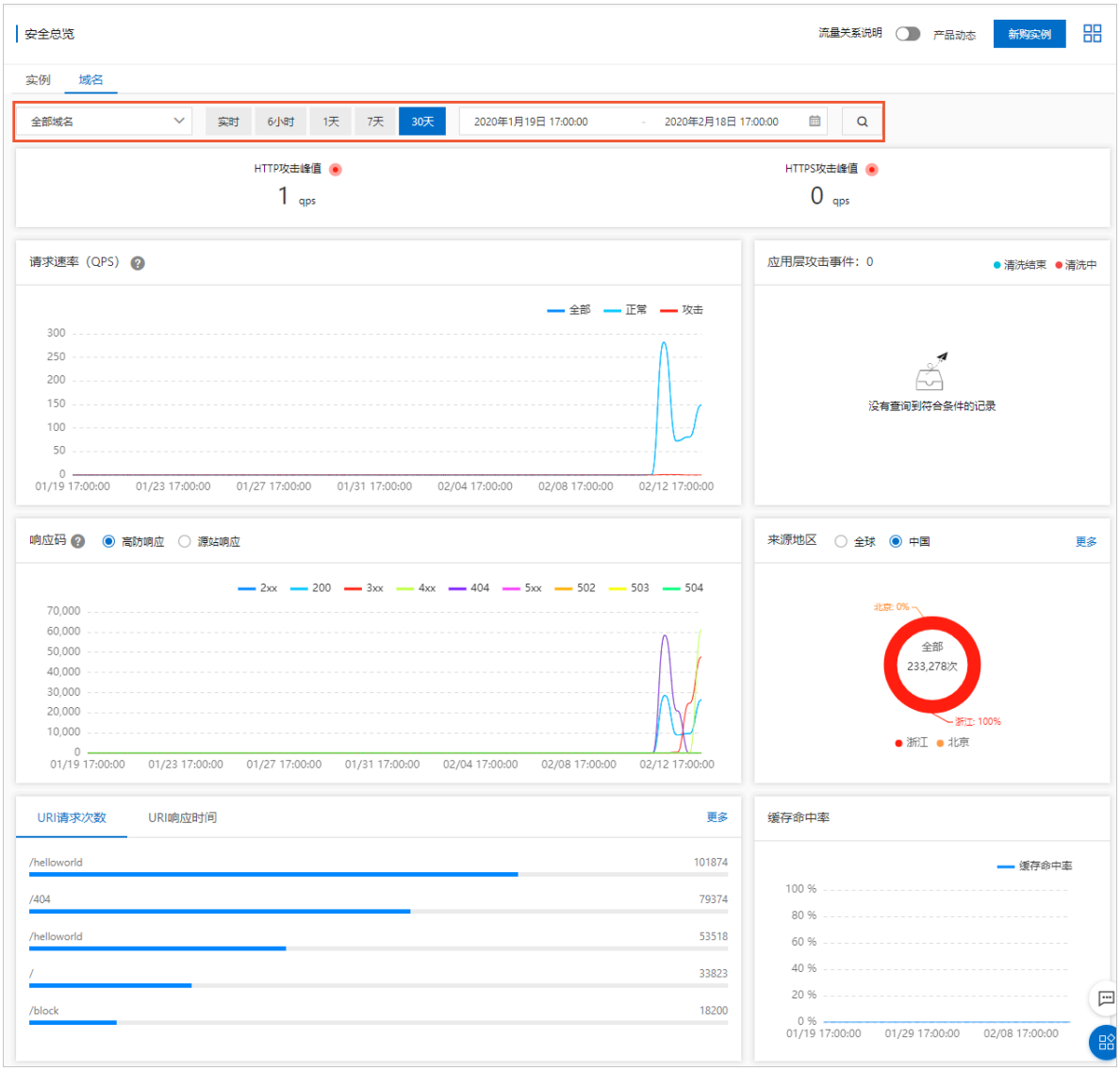
- （端口）连接数
  - 并发连接数：客户端同一时间与高防建立的TCP连接数量
  - 新建连接数：客户端每秒内新增的与高防通信的TCP连接数

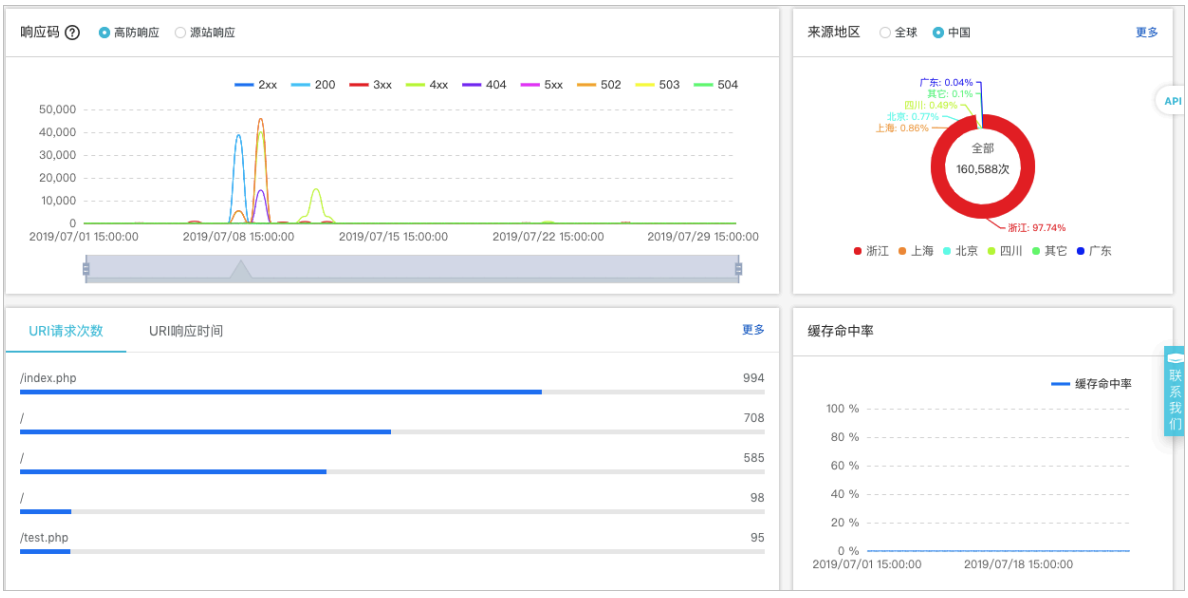
说明：

只有选择单个实例时，连接数报表处才会显示当前实例IP的不同端口的连接数；如果选择1个以上实例，则无法区别端口，只能显示全部端口的连接数。

- 访问来源区域和运营商分布

5. 打开域名页签，设置要查询的时间范围，查看指定域名对应业务的相关信息。





支持查看的域名业务信息包括以下内容。

- HTTP攻击峰值和HTTPS攻击峰值
- 请求次数趋势图

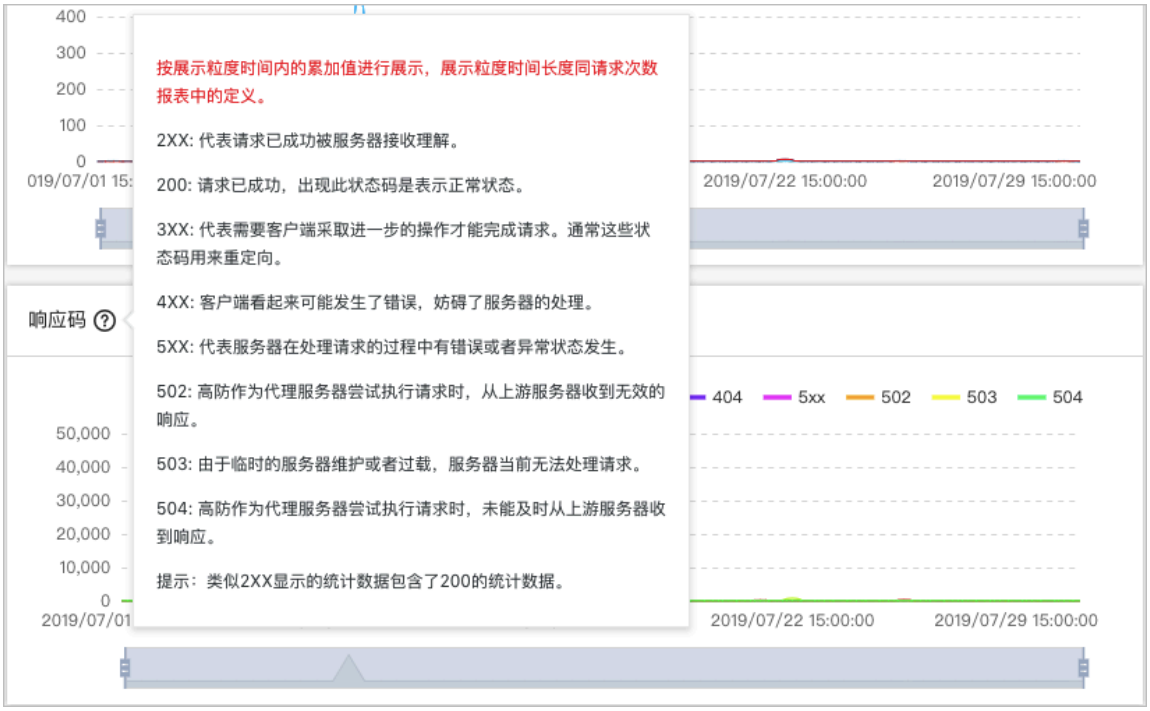
  请求次数趋势图按峰值展示，不同的查询时间间隔对应的展示粒度不同，具体如下：

  - 1小时以内，展示粒度为1分钟；
  - 1-6小时以内，展示粒度为10分钟；
  - 6-24小时，展示粒度30分钟；
  - 1-7天，展示粒度为1小时；
  - 7天-15天，展示粒度为4小时；
  - 其它，展示粒度为12小时。
- 应用层攻击事件

  将鼠标放到被攻击的域名上，可以展示被攻击的域名信息、攻击的峰值和攻击类型。

- 响应码信息

  响应码记录的数量对应展示粒度时间内的累加值，展示粒度的时间长度定义同请求次数趋势图中的定义。您可以通过响应码旁的帮助信息了解具体响应码的含义。



- **访问来源地区分布**
- **URI请求次数和URI响应时间记录**
- **缓存命中率记录**

> **说明:**
> **只有开通网站缓存加速功能，才会有缓存命中率数据。更多信息，请参见加速网站静态页面访问。**

6 查看安全报表

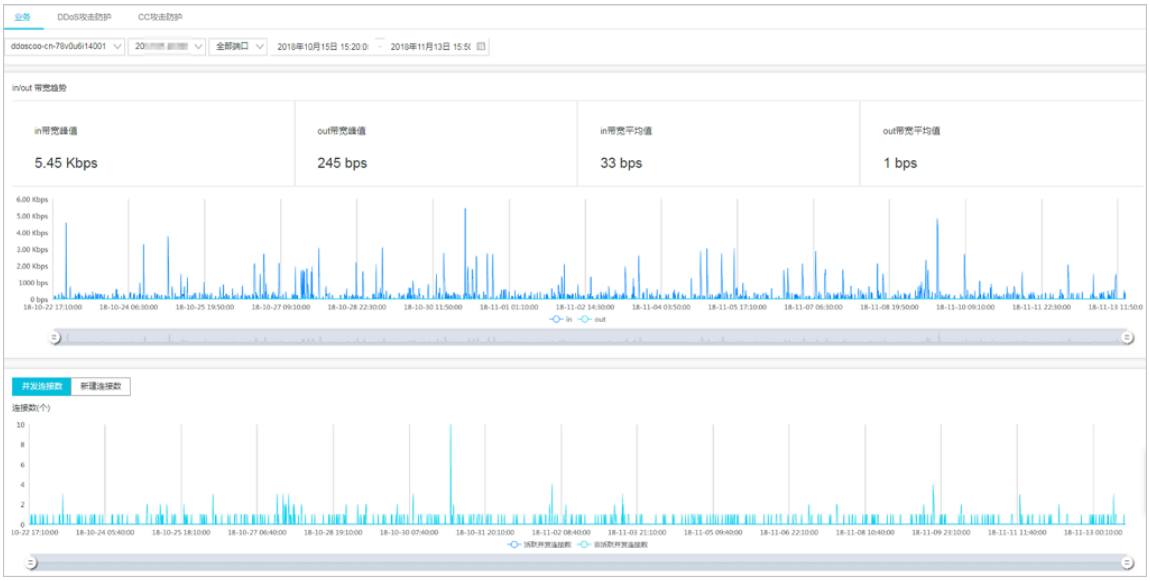
业务接入DDoS高防且切换业务流量至DDoS高防实例后，您可以在DDoS高防控制台的安全报表页面查看业务流量情况与DDoS攻击防护情况。

操作步骤

1. 在左侧导航栏，单击安全报表。
2. 在报表页面，选择查看业务、DDoS攻击防护、CC防护报表。
   - 查看业务报表

     单击业务页签，选择DDoS高防实例和端口，设置查询时间范围，查看指定实例中已防护的业务的出/入带宽流量趋势、连接数情况。

     > **说明:**
     > 支持查询最多30天以内的业务流量和连接数信息。

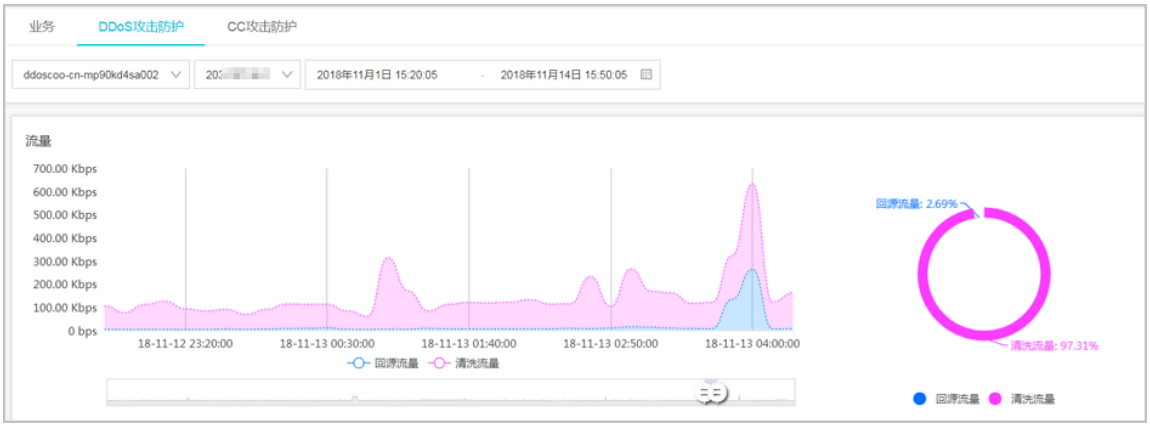
     您可以拖动趋势图下方的滑块，快速调整查询时间范围，聚焦指定时间段。

   - 查看DDoS攻击防护报表

     单击DDoS攻击防护页签，选择DDoS高防实例，设置查询时间范围，查看指定实例中已防护的业务的流量情况及DDoS攻击事件。

     > **说明:**

支持查询最多30天以内的流量信息及DDoS攻击事件。



说明:

高防IP服务会自动过滤网络流量中存在的一些畸形包（例如SYN小包、SYN标志位异常等不符合TCP协议的数据包），使您的业务服务器无需浪费资源处理这些明显的畸形包。这类被过滤的畸形包也将被计入清洗流量中，因此可能出现您的服务器流量未达清洗阈值，但流量图表中出现清洗流量的情况。

- 查看CC攻击防护报表

  单击CC攻击防护页签，选择已接入防护的域名，设置查询时间范围，查看该域名的访问QPS情况及CC攻击事件。

  说明:

  支持查询最多30天以内的QPS信息及CC攻击事件。

7 防护设置

7.1 基础设施DDoS防护

7.1.1 设置针对目的IP的黑白名单

DDoS高防实例的流量黑白名单用于封禁或者放行来自指定源IP的四层访问流量。您可以根据业务需要，为DDoS高防实例单独配置流量黑名单、白名单，例如添加、移除IP。流量黑名单中也包含DDoS高防智能防御算法标记的恶意IP。同时，流量黑白名单支持导出到本地。本文介绍了流量黑白名单的具体操作方法。

背景信息

流量黑白名单针对具体的DDoS高防实例生效。

- 黑名单IP的访问流量将被DDoS高防实例直接丢弃。黑名单IP存在有效期，并非永久生效。如果是智能防御算法标记的恶意IP，其有效期由智能防御算法动态计算，最短5分钟，最长1小时（如果该恶意IP在有效期间有持续的恶意攻击行为，系统将自动延长有效期）。通过手动添加的IP，在添加时需要指定其有效期。
- 白名单IP的访问流量将被DDoS高防实例直接放行。白名单IP永久生效。如果黑名单和白名单中的IP出现冲突，遵循白名单优先原则。如果IP已经被添加至白名单，则无法将该IP添加至黑名单中。

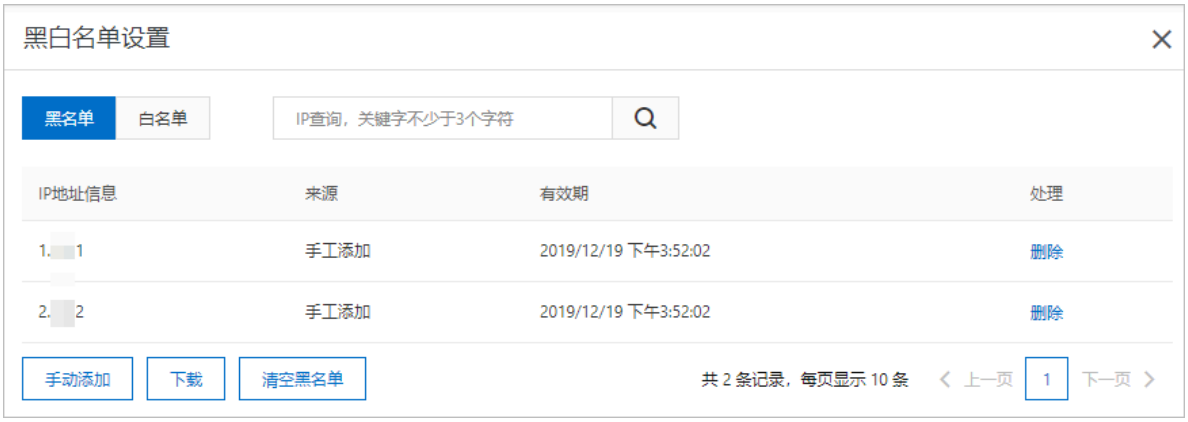
操作步骤

1. 登录云盾DDoS高防（新BGP）控制台。
2. 在左侧导航栏，单击防护设置 > 通用防护策略。
3. 在基础设施DDoS防护页签下，从左侧实例列表中选择要设置的DDoS高防实例。

> **说明:**
> 您可以使用实例ID、实例备注搜索目标实例。

4. 定位到黑白名单（针对目的IP）功能区域，单击设置。

   进入黑白名单设置侧边页。您可以单击黑名单或白名单，分别管理黑名单、白名单。黑名单管理请参见步骤5，白名单管理请参见步骤6。



5. （可选） 管理流量黑名单。以黑名单为例，您可以执行以下操作。

   · 手动添加黑名单IP

   a. 单击手动添加。

   b. 在黑名单配置对话框中，输入要拉黑的请求来源IP并选择拉黑时间。

   说明:

黑名单最多支持手动添加2000个IP。

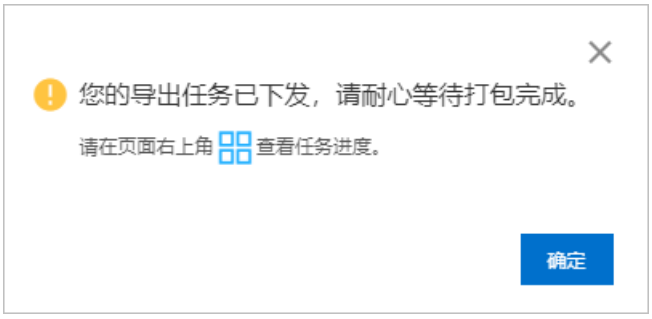
c. 单击添加。

成功添加黑名单IP，新添加的黑名单IP在有效期内的所有访问请求将被丢弃；有效期过后，限制自动解除。

- 搜索黑名单IP：在搜索框中输入IP关键字，单击查询图标，即可查询黑名单中符合条件的IP。
- 清空黑名单：单击清空黑名单，将当前黑名单中的所有IP直接移除。您也可以单击某个IP后的删除，单独将其从黑名单中移除。
- 下载黑名单

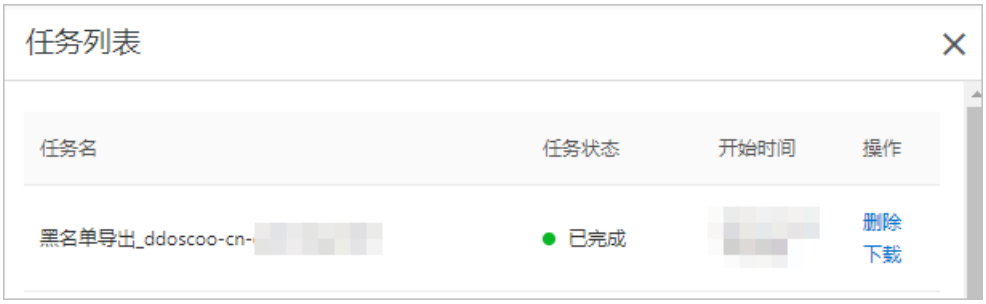
a. 单击下载，下发黑名单导出任务。

b. 在导出任务已下发提示中，单击确定。

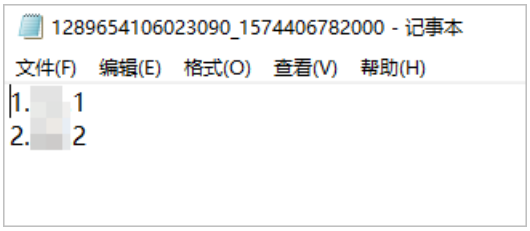


c. 单击页面右上角的任务图标（），展开任务列表。

d. 定位到黑名单导出任务，等待任务状态变为已完成，单击其操作列下的下载。



成功下载txt文本文件格式的黑名单IP到本地。您可以打开txt文件查看黑名单明细。



6. **（可选）管理白名单。以白名单为例，您可以执行以下操作。**

   - **手动添加白名单IP**

     a. **单击手动添加。**

     b. **在白名单配置对话框中，输入要放行的请求来源IP。**

     说明:

白名单最多支持手动添加2000个IP。

c. 单击添加。

成功添加白名单IP，新添加的白名单IP永久有效，其所有访问请求均直接放行。

- 搜索白名单IP：在搜索框中输入IP关键字，单击查询图标，即可查询白名单中符合条件的IP。
- 清空白名单：单击清空白名单，将当前白名单中的所有IP直接移除。您也可以单击某个IP后的删除，单独将其从白名单中移除。
- 下载白名单

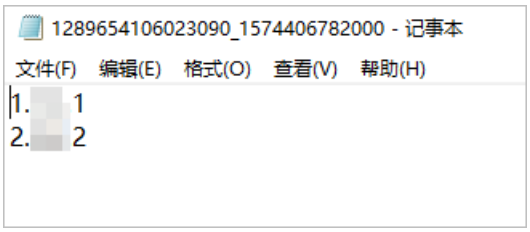
a. 单击下载，下发白名单导出任务。

b. 在导出任务已下发提示中，单击确定。

c. 单击页面右上角的任务图标（），展开任务列表。

d. 定位到白名单导出任务，等待任务状态变为已完成，单击其操作列下的下载。

成功下载txt文本文件格式的白名单IP到本地。您可以打开txt文件查看白名单明细。



7.1.2 设置近源流量压制

近源流量压制指对DDoS高防实例中的电信/联通线路的海外流量实行主动封禁。每个用户总共拥有10次触发流量封禁的额度，且在流量封禁期间支持随时解除封禁。

背景信息

当您遭遇特大流量攻击，且发现攻击流量有超过最大防护能力的趋势时，建议您考虑使用近源流量压制。一般情况下，假如海外攻击流量占比30%左右，通过封禁海外流量即可大大缓解防御压力，将攻击规模控制在自身最大防护能力范围内。

开启近源流量压制会将特定流量在机房侧丢弃，降近源流量压制低DDoS高防电信/联通线路被攻击进入黑洞状态的可能性。由于黑洞涉及攻击流量大小、攻击流量来源区域等多近源流量压制启用流量封禁可在一定情况下降低被黑洞的概率。

操作步骤

1. 在左侧导航栏，单击防护设置 > 通用防护策略。
2. 在基础设施DDoS防护页签下，从左侧实例列表中选择要设置的DDoS高防实例。

说明:

您可以使用实例ID、实例备注搜索目标实例。

3. **定位到近源流量压制功能区域，根据需要执行以下封禁操作。**

   - **封禁电信海外流量：单击电信海外后的封禁，并在流量封禁对话框中设置封禁时长，完成后单击确定。**

     说明:
     每次封禁时长最短15分钟，最长23小时59分钟。

   - **封禁联通海外流量：单击联通海外后的封禁，并在流量封禁对话框中设置封禁时长，完成后单击确定。**

     说明:

每次封禁时长最短15分钟，最长23小时59分钟。

说明:

- 建议您优先封禁电信海外流量，并观察攻击规模的变化趋势。如果流量还是很大，超过当前防护能力，则可以再考虑封禁联通海外流量。
- 一个阿里云账号总共拥有10次封禁机会，封禁次数不会每天刷新。封禁一次电信或联通海外流量都会消耗一次额度。

如果近源流量压制失败，您会收到失败提示信息，请根据提示排查后再次尝试。如果未出现任何提示信息，则表示近源流量压制已成功。

4. （可选） 回到近源流量压制功能区域，单击查看封禁信息，在近源流量封禁侧边页查看本次封禁的区域和时间范围。

5. （可选） 解除封禁。

流量封禁期间，封禁操作变为解除封禁，您可以单击解除封禁，提前解除对应线路的海外流量封禁。

7.1.3 设置区域封禁

区域封禁指针对访问高防IP的源IP，按地理区域在清洗机房进行一键封禁，帮助您一键阻断来自指定（国内、海外）地区的来源IP的所有访问请求。该功能针对增强功能套餐的DDoS高防IP生效。为高防IP设置并启用区域封禁后，由封禁地区到高防IP的流量将被丢弃。本文介绍了设置和启用区域封禁的操作方法。

前提条件

- 已开通增强功能套餐的DDoS高防实例。更多信息，请参见开通DDoS高防。
- 已在端口配置中添加转发规则。更多信息，请参见添加规则。

背景信息

区域封禁通过直接丢弃来自指定（国内、海外）地区的来源IP的所有访问请求，达到阻断非业务来源请求的目的。区域封禁在高防清洗机房内部实现，在靠近被攻击目标的位置丢弃特定区域的流量。区域封禁根据源IP的归属区域在DDoS高防中识别过滤，并不能减小进入BGP高防网络的攻击流量，适用于防护连接资源消耗型攻击。

说明:

近源流量压制一般通过运营商骨干网核心路由器，在靠近攻击源的位置丢弃特定区域的流量。更多信息，请参见设置近源流量压制。

假设访问高防IP的正常用户均来自中国大陆（含港澳台特别行政区），您可以为该高防IP设置区域封禁，封禁来自海外地区的访问请求。

说明:

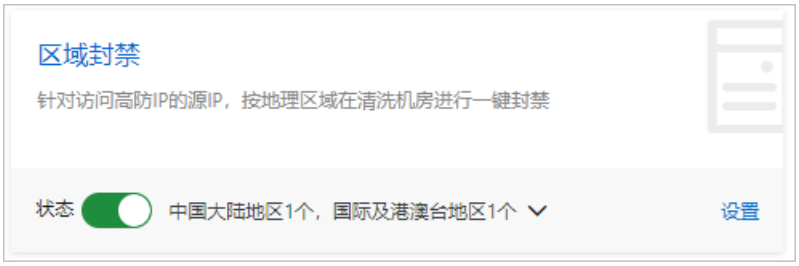
- 区域封禁针对高防IP生效。如果您需要对多个不同高防IP启用区域封禁，则需要对不同高防IP分别进行设置；不支持对多个高防IP批量设置。

- 针对域名的区域封禁功能和区域封禁功能一起使用时，区域封禁功能优先生效。例如，针对高防IP已经通过区域封禁功能封禁了海外区域的流量，关联该高防IP的域名无论有没有设置（域名）区域封禁功能，海外用户都不能访问。如果需要实现部分业务封禁海外访问，部分业务不封禁海外访问，建议您设置针对域名的区域封禁，而非针对高防IP设置区域封禁。

操作步骤

1. 在左侧导航栏，单击防护设置 > 通用防护策略。
2. 在基础设施DDoS防护页签下，从左侧实例列表中选择要设置的DDoS高防实例。

> **说明:**
> 您可以使用实例ID、实例备注搜索目标实例。



3. 定位到区域封禁功能区域，单击设置。

4. 在封禁区域设置页面，勾选要封禁的访问请求的来源地区，并单击确定。

   以下图中配置为例，配置生效后，海外流量将无法访问对应高防IP。

5. 回到区域封禁功能区域，开启区域封禁的状态开关，为DDoS高防实例应用区域封禁设置。

7.1.4 手动解除黑洞状态

对于已接入DDoS高防的业务，如果因为其保底防护带宽或弹性带宽不足被突发大流量攻击造成黑洞，您可以在DDoS高防控制台使用黑洞解封来快速恢复业务。解除黑洞操作方便您在意外进入黑洞时快速恢复业务，建议您在解除黑洞前先提升保底或弹性防护能力，避免高防IP被持续打入黑洞。

背景信息

使用限制：每个阿里云账号每天共拥有五次黑洞解封的机会。

操作步骤

1. 在左侧导航栏，单击防护设置 > 通用防护策略。

2. 在基础设施DDoS防护页签下，从左侧实例列表中选择要设置的DDoS高防实例。

> **说明:**
> 您可以使用实例ID、实例备注搜索目标实例。

3. 定位到黑洞解封功能区域，根据当前实例状态，执行黑洞解封。

   - 如果当前实例处于黑洞状态，且您不希望等待黑洞自动解封，则您可以单击解封，耐心等待黑洞状态成功解除。

     > **说明:**
     > - 每个用户每天拥有五次黑洞解除机会，每天零点会自动恢复成五次；只有成功解除黑洞状态才会消耗一次解除额度。
     > - 当天第一次解封一般可以即刻解除黑洞状态，如果同一天内连续使用黑洞解封，则相邻两次解除操作的间隔必须大于10分钟。

   - 如果当前实例是正常状态，则解封按钮不可操作。

预期结果

- 由于黑洞解封涉及阿里云后台系统的风控管理策略，黑洞解封可能失败（解封失败不会扣减您的解封次数）。如果黑洞解封失败，您会收到失败提示信息，请耐心等待一段时间后再尝试。
- 如果系统提示“受机房风控影响，暂时无法解封，请10分钟后再尝试”，则请您耐心等待下再尝试。
- 如果无任何提示信息，则表示解封成功，您可以刷新线路状态确认该DDoS高防线路是否已恢复正常。

7.2 网站业务DDoS防护

7.2.1 设置针对域名的黑白名单

DDoS高防支持对已接入防护的网站业务设置针对域名的黑白名单。开启网站访问黑白名单，则来自黑名单中的IP/IP段的访问请求将会被直接阻断，来自白名单中的IP/IP段的访问请求将被直接放行，且不经过任何防护策略过滤。本文介绍了设置网站访问黑白名单的方法。

前提条件

已在DDoS高防网站配置中添加要防护的网站业务。更多信息，请参见添加网站。

背景信息

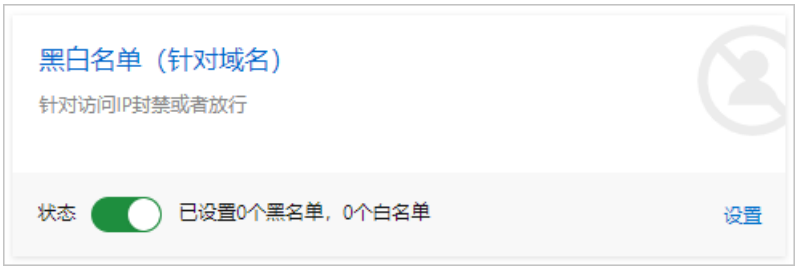
网站业务接入DDoS高防后，若存在对网站业务访问量较大的恶意IP，您可以将这些IP添加至网站访问黑名单，拦截其访问请求。对于企业内部办公网的IP段、业务接口调用IP或其它已确认正常的IP，您可以将这些IP添加至网站访问白名单予以放行，来自白名单中IP的访问请求和流量将不会被拦截。

注意事项

- 网站访问黑白名单仅支持防护网站业务。对于非网站业务若有类似需求，建议您设置DDoS防护策略下的黑白名单。更多信息，请参见设置针对目的IP的黑白名单。
- 网站访问黑白名单的设置仅针对单个网站域名生效，而不是针对整个DDoS高防实例。
- 对于单个网站域名，您最多可分别配置200条黑名单、白名单记录。

操作步骤

1. 登录云盾DDoS高防（新BGP）控制台。
2. 在左侧导航栏，单击防护设置 > 通用防护策略。
3. 在通用防护策略页面，单击网站业务DDoS防护页签。
4. 从左侧域名列表中选择要设置的域名。
5. 定位到黑白名单（针对域名）功能区域，单击设置。



6. 在黑白名单设置对话框中，分别设置黑名单和白名单，并单击确定。

- 选择黑名单页签，填写需要拦截其访问请求的恶意IP或IP段。
- 选择白名单页签，填写需要放行其访问请求的正常IP或IP段。

说明:

- IP或IP段支持以IP或IP/掩码的格式填写。
- 黑名单或白名单下最多均支持添加200个IP或IP段，多个IP或IP段之间用英文逗号（,）分隔。
- 黑名单支持添加0.0.0.0/0，表示拦截来自除白名单中配置的正常IP外所有IP的访问请求。

7. 回到黑白名单（针对域名）功能区域，打开状态开关，开启黑白名单。

说明:

若您使用旧版本防护设置，则必须开启CC安全防护功能，才能使黑白名单设置生效。

预期结果

成功开启网站访问黑白名单。黑白名单设置将应用到所有与当前网站业务关联的DDoS高防实例，并针对当前网站的访问流量即刻生效。

说明:

在部分情况下，可能需要经过一些访问流量和时间后，黑白名单设置才会真正生效。如果黑白名单开启后，设置未立即生效，请尝试继续访问网站数次。

7.2.2 设置针对域名的区域封禁

DDoS高防支持对已接入防护的网站业务设置基于地理区域的网站访问封禁策略。开启针对域名的区域封禁功能，则您可以一键阻断来自指定地区（中国大陆省/市/区、海外区域）的来源IP的所有网站访问请求。本文介绍了设置针对域名的区域封禁的方法。

前提条件

- 已在DDoS高防网站配置中添加要防护的网站业务，且为网站业务关联增强功能套餐的DDoS高防实例。更多信息，请参见添加网站。
- 已开启新版防护设置。

背景信息

网站业务接入DDoS高防后，假设网站的正常用户均来自中国大陆（含港澳台特别行政区），则您可以为域名开启区域封禁，封禁来自海外地区的访问请求。同理，您可以设置封禁其它非正常网站用户来源的区域。设置区域封禁时，您只需选择要封禁的区域即可，具体包括以下区域。

- 中国大陆省/市/区

上海市、云南省、内蒙古自治区、北京市、台湾省、吉林省、四川省、天津、宁夏回族自治区、安徽省、山东省、陕西省、山西省、广东省、广西壮族自治区、新疆维吾尔自治区、江苏省、江西省、河北省、河南省、浙江省、海南省、湖北省、湖南省、澳门特别行政区、甘肃省、福建省、西藏自治区、贵州省、辽宁省、重庆市、青海省、香港特别行政区、黑龙江省

- 海外区域

亚洲（国内除外）、欧洲、北美洲、南美洲、非洲、大洋洲、南极洲

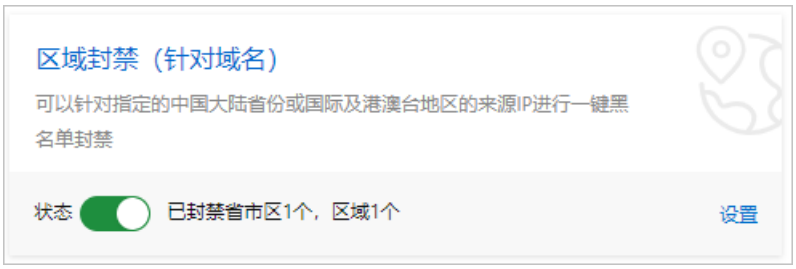
注意事项

- 区域封禁仅支持防护网站业务。对于非网站业务若有类似需求，建议您设置DDoS防护策略下的流量封禁。更多信息，请参见设置近源流量压制、设置区域封禁。
- 区域封禁针对域名生效。如果您需要为多个不同网站域名设置区域封禁，则需要为不同域名分别设置，不支持对多个域名批量设置区域封禁。
- 区域封禁根据源IP的归属区域在DDoS高防中识别过滤，并不能减小进入BGP高防网络的攻击流量。

操作步骤

1. 在左侧导航栏，单击防护设置 > 通用防护策略。

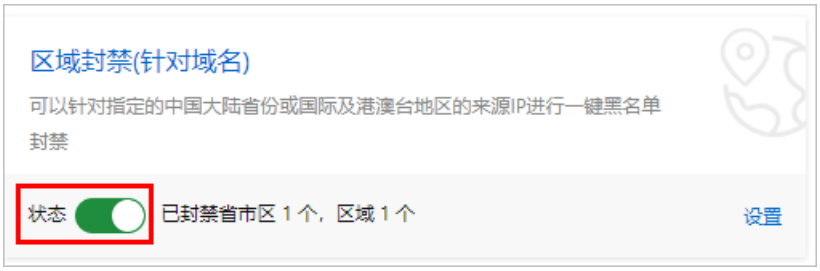
2. 在通用防护策略页面，单击网站业务DDoS防护页签，并从左侧域名列表中选择要设置的域名。
3. 定位到区域封禁（针对域名）功能区域，单击设置。



4. 在选择需要封禁的区域对话框中，勾选要封禁的区域，并单击确定。

   以下图中的配置为例，配置生效后，则海外流量将无法访问网站。

5. 回到区域封禁（针对域名）功能区域，开启状态开关，应用针对域名的区域封禁设置。



预期结果

成功开启针对域名的区域封禁。区域封禁设置将应用到所有与当前网站业务关联的DDoS高防实例，并针对当前网站的访问流量即刻生效。

7.2.3 设置精准访问控制规则

DDoS高防支持对已接入防护的网站业务设置精准访问控制策略。开启精确访问控制，则您可以使用常见的HTTP字段（如IP、URL、Referer、UA、参数等）设置匹配条件，用来筛选访问请求，并对命中条件的请求设置放行、封禁、挑战操作。精准访问控制支持业务场景定制化的防护策略，可用于盗链防护、网站管理后台保护等。

前提条件

- 已在DDoS高防网站配置中添加要防护的网站业务。更多信息，请参见添加网站。
- 已开启新版防护设置。

背景信息

网站业务接入DDoS高防后，若您需要针对性地管理具有固定特征的访问请求，则您可以为域名开启精确访问控制并设置精确访问控制规则。精准访问控制规则由匹配条件与匹配动作构成。

- 匹配条件定义了要识别的请求特征，具体指访问请求中HTTP字段的属性特征。精确访问控制规则支持匹配的HTTP字段如下表所示。

> **说明:**
> 不同字段适用的匹配逻辑不同，例如请求源IP字段“属于/不属于”具体的值，请求URI“包括/不包括”具体的内容等，详见下表中适用的逻辑符一列。

匹配字段	字段描述	适用的逻辑符
IP	访问请求的来源IP。	属于/不属于
URI	访问请求的URI地址。	包括/不包括 、等于/不等于、长度小于/长度等于/长度大于
User-Agent	发起访问请求的客户端浏览器标识等相关信息。	包括/不包括 、等于/不等于、长度小于/长度等于/长度大于

匹配字段	字段描述	适用的逻辑符
Cookie	访问请求中的携带的Cookie信息。	包括/不包括 、等于/不等于、长度小于/长度等于/长度大于、不存在
Referer	访问请求的来源网址，即该访问请求是从哪个页面跳转产生的。	包括/不包括 、等于/不等于、长度小于/长度等于/长度大于、不存在
Content-Type	访问请求指定的响应HTTP内容类型，即MIME类型信息。	包括/不包括 、等于/不等于、长度小于/长度等于/长度大于
X-Forwarded-For	访问请求的客户端真实IP。	包括/不包括 、等于/不等于、长度小于/长度等于/长度大于、不存在
Content-Length	访问请求的所包含的字节数。	值小于/值等于/值大于
Post-Body	访问请求的内容信息。	包含/不包含、等于/不等于
Http-Method	访问请求的方法，具体包括GET 、POST、DELETE、PUT、OPTIONS、CONNECT、HEAD、TRACE。	等于/不等于
Header	访问请求的头部信息，用于自定义HTTP头部字段及匹配内容。	包括/不包括 、等于/不等于、长度小于/长度等于/长度大于、不存在
Params	访问请求的URL地址中的参数部分，通常指URL中?后面的部分。例如，`www.abc.com/index.html?action=login`中的`action=login`就是参数部分。	包括/不包括 、等于/不等于、长度小于/长度等于/长度大于

- 匹配动作定义了访问请求命中匹配条件时，对访问请求执行的动作，具体包括放行、封禁、挑战（即通过挑战算法对请求的源IP地址发起校验）。

使用限制

根据网站业务关联的DDoS高防实例类型，精确访问控制规则具有如下使用限制。

限制	标准功能套餐实例	增强功能套餐实例
自定义规则数量	不超过五条	不超过十条
可使用的匹配字段	IP、URL、Referer、User-Agent	所有支持匹配的字段

操作步骤

1. 在左侧导航栏，单击防护设置 > 通用防护策略。
2. 在通用防护策略页面，单击网站业务DDoS防护页签，并从左侧域名列表中选择要设置的域名。

3. 定位到精确访问控制功能区域，单击设置。

4. 在精确访问控制页面，为域名设置精确访问控制规则。

- 新增规则

a. 单击新增规则。

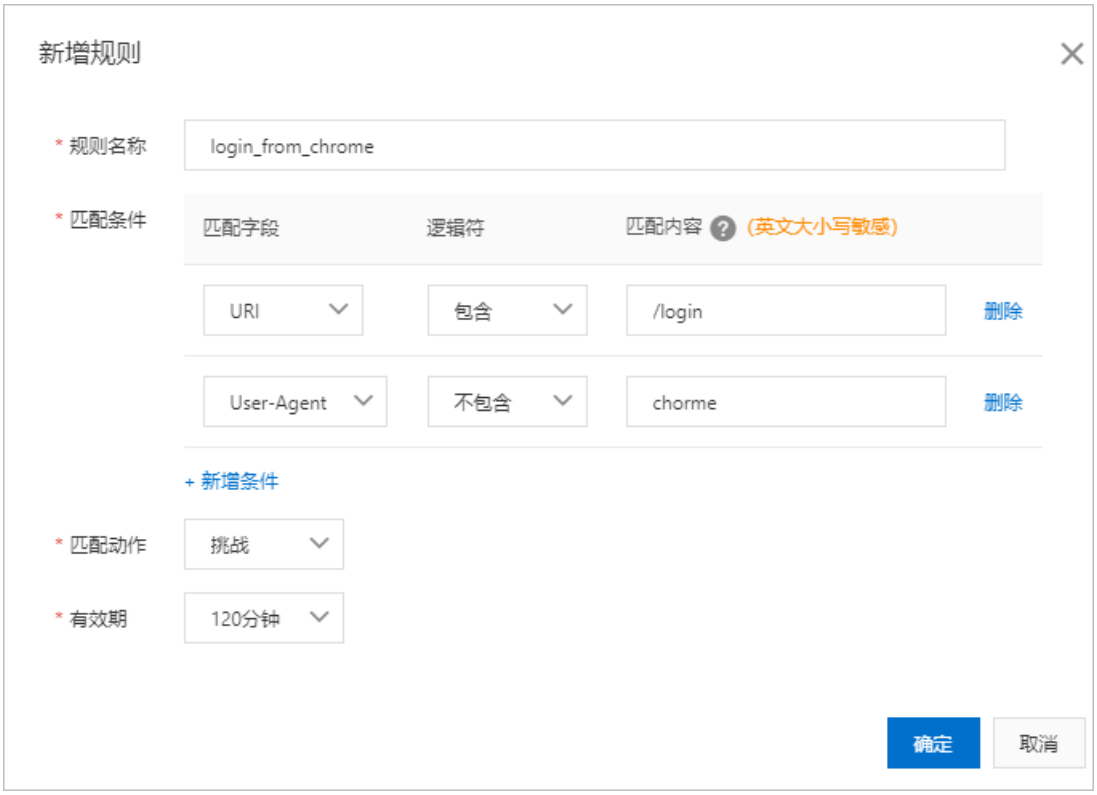
> 说明:
> 若自定义规则数量达到限制，则新增规则不可操作。

b. 在新增规则对话框中，完成规则配置，并单击确定。规则配置的描述如下。

配置项	说明
规则名称	规则的名称，由英文字母、数字和下划线（_）组成，不超过128个字符。
匹配条件	规则的匹配条件。单击新增条件添加一个条件，每个条件由匹配字段、逻辑符和匹配内容组成。 - 关于匹配字段和逻辑符的取值范围，参见支持的匹配字段。 - 匹配内容根据匹配字段填写，大小写敏感。暂时不支持通过正则表达式描述，但允许设置为空值。 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。
匹配动作	当访问请求命中匹配条件时，对请求执行的操作，取值： - 封禁：阻断命中匹配条件的访问请求。 - 放行：放行命中匹配条件的访问请求。 - 挑战：通过挑战算法对命中匹配条件的访问请求的源IP地址发起校验。

配置项	说明
有效期	规则的有效期，取值：5分钟、10分钟、30分钟、60分钟、90分钟、120分钟、永久。

以下图为例，配置完成后，对于包含`/login`页面的请求，如果其UserAgent字段中包含`chrome`，则对请求的源IP发起校验。该规则自创建成功起在120分钟内生效。

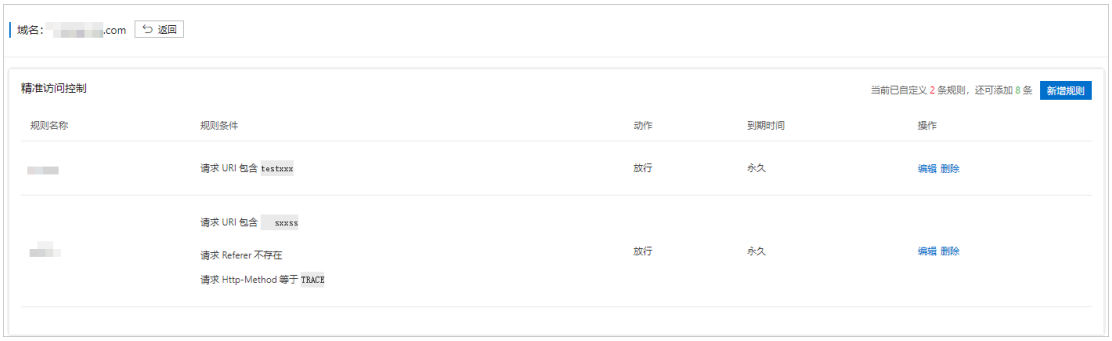


成功添加精确访问控制规则。您可以根据需要继续添加多条规则。

说明:

- 如果您设置了多条规则，则规则的优先级遵循其在规则列表中的排列顺序，排序越靠前，优先级越高。访问请求根据规则顺序依次进行匹配，顺序较前的精准访问控制规则优先匹配。

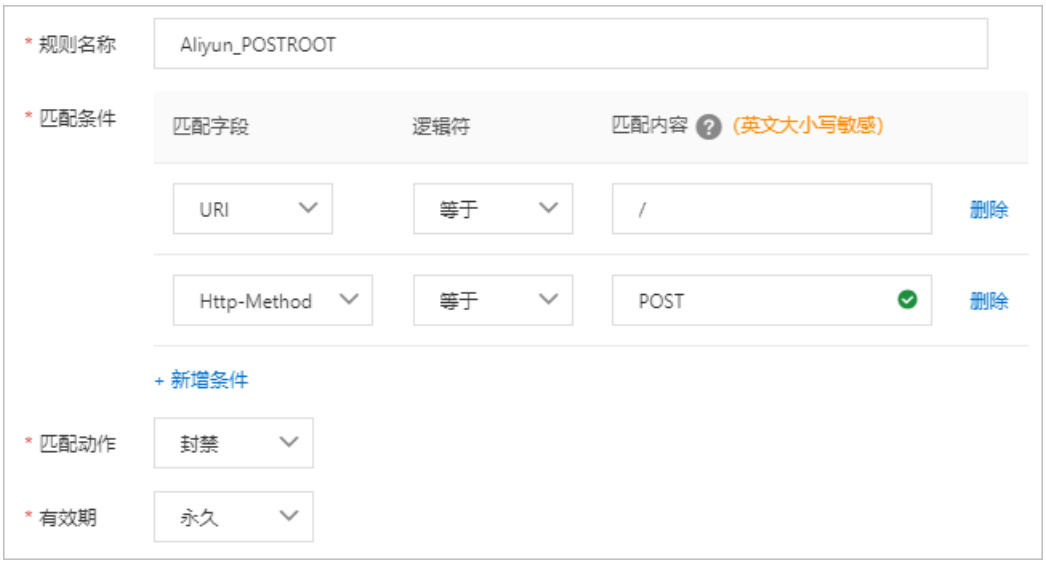
- 如果一个请求同时命中多个匹配条件，则匹配动作取所有命中的规则中，排序最靠前的访问控制规则中的匹配动作。



规则配置示例

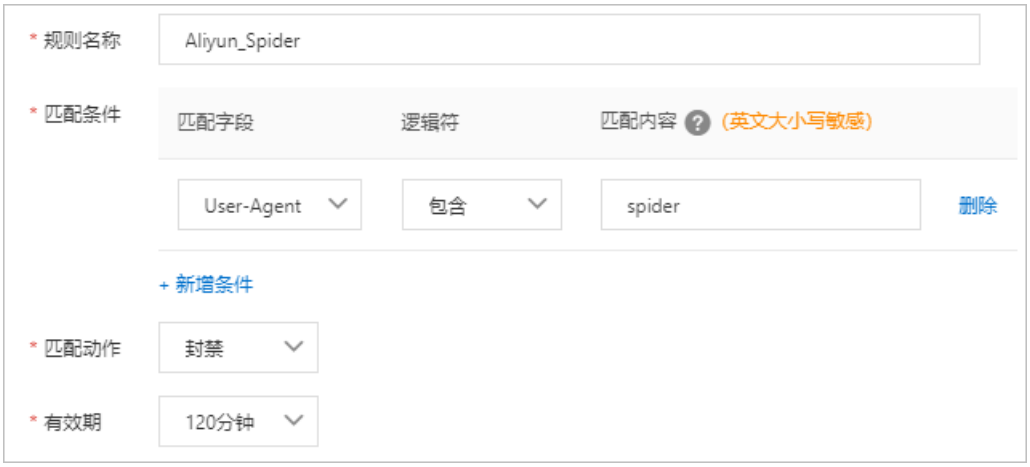
- **拦截特定的攻击请求**

  一般情况下，正常业务不存在POST根目录的请求信息。如果被CC攻击时，发现客户端的请求中存在大量的POST根目录请求，可以评估请求的合法性。如果确认其为非正常业务请求，可以通过精准访问控制规则，执行拦截动作。规则配置示例如下。



- **拦截一段时间内爬虫的访问请求**

  如果在某段时间内，您发现网站的访问流量中有大量爬虫请求，若不排除是攻击傀儡机模拟爬虫进行CC攻击，则可以对爬虫的请求执行拦截操作。规则配置示例如下。



- 编辑规则

  a. 在规则列表中，定位到要操作的规则，单击其操作列下的编辑。

  b. 在编辑规则对话框中，修改规则配置，并单击确定。规则配置的描述见新增规则，其中，规则名称不可更改。

- 删除规则

  a. 在规则列表中，定位到要删除的规则，单击其操作列下的删除。

  b. 在删除提示对话框中，单击确定。

5. 回到精确访问控制功能区域，开启状态开关，应用精确访问控制规则。

成功开启精确访问控制。

7.2.4 设置频率控制

DDoS高防为已接入防护的网站业务提供频率控制防护，支持限制源IP的访问频率。频率控制防护开启后自动生效，默认使用正常防护模式，帮助网站防御一般的CC攻击。频率控制防护提供多种防护模式，供您在不同场景下调整使用；您也可以自定义频率控制规则，限制单一源IP在短期内异常频繁地访问某个页面。

前提条件

- 已在DDoS高防网站配置中添加要防护的网站业务。更多信息，请参见添加网站。

- 已开启新版防护设置。

背景信息

网站业务接入DDoS高防后，您可以为网站开启频率控制防护，防御HTTP Flood攻击（即CC攻击）。频率控制防护提供不同的防护模式，允许您根据网站的实时流量异常调整频率控制策略，具体包括以下模式。

- 正常（默认）：网站无明显流量异常时建议采用此模式。正常模式的频率控制防护策略相对宽松，可以防御一般的CC攻击，对于正常请求不会造成误杀。
- 攻击紧急：当发现网站响应、流量、CPU、内存等指标出现异常时，可切换至此模式。攻击紧急模式的频率控制防护策略相对严格。相比正常模式，此模式可以防护更为复杂和精巧的CC攻击，但可能会对少部分正常请求造成误杀。
- 严格：严格模式的频率控制防护策略较为严格。该模式会对被保护网站的所有访问请求实行全局级别的人机识别验证，即针对每个访问者进行验证，只有通过认证后访问者才允许访问网站。

  说明:
  对于严格模式的全局算法认证，如果是真人通过浏览器的访问请求均可以正常响应；但如果被访问网站的业务是API或原生App应用，将无法正常响应该算法认证，导致网站业务无法正常访问。
- 超级严格：超级严格模式的频率控制防护策略非常严格。该模式会对被保护网站的所有访问请求实行全局级别的人机识别验证，即针对每个访问者都将进行验证，只有通过认证后后才允许访问网站。 相比于严格模式，超级严格模式所使用的全局算法认证在验证算法中还增加反调试、反机器验证等功能。

  说明:
  对于超级严格模式的全局算法认证，如果是真人通过浏览器的访问请求均可以正常响应（可能存在极少部分浏览器处理异常导致无法访问，关闭浏览器后再次重试即可正常访问）；但如果被访问网站的业务是API或原生App应用，将无法正常响应该算法认证，导致网站业务无法正常访问。

除了不同防护模式外，频率控制防护还支持通过自定义防护规则进行更精准的CC攻击拦截。您可以为需要重点保护的URL自定义频率控制策略，限制单一源IP在短期内异常频繁地访问某个页面。

设置频率控制防护模式

1. 在左侧导航栏，单击防护设置 > 通用防护策略。
2. 在通用防护策略页面，单击网站业务DDoS防护页签，并从左侧域名列表中选择要设置的域名。

3. 定位到频率控制功能区域，选择要应用的内置模式（正常、攻击紧急、严格、超级严格），并开启状态开关，应用频率控制防护。

成功开启频率控制防护。

自定义频率控制防护规则

1. 在左侧导航栏，单击防护设置 > 通用防护策略。
2. 在通用防护策略页面，单击网站业务DDoS防护页签，并从左侧域名列表中选择要设置的域名。
3. 定位到频率控制功能区域，开启自定义规则开关，并单击设置。

4. 在CC防护自定义规则页面，为域名设置频率控制防护规则。
   - 新增规则
     a. 单击新增规则。

     说明:
     最多支持自定义20条规则。若规则数量达到限制，则新增规则不可操作。

     b. 在新增规则对话框中，完成规则配置，并单击确定。规则配置的描述如下。

配置项	说明
规则名称	为该规则命名。

配置项	说明
URI	指定需要防护的具体地址，如*/register*。支持在地址中包含参数，如*/user?action=login*。
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，只要是请求的URI以此处配置的URI开头就会被统计。例如，如果设置URI为*/register*，则*/register.html*会被统计。
检测时长	指定统计访问次数的周期。需要和单一IP访问次数配合。
单一IP访问次数	指定在检测时长内，允许单个源IP访问被防护地址的次数。

配置项	说明
阻断类型	指定触发条件后的操作（封禁、人机识别），以及请求被阻断后阻断动作的时长。 - 封禁：触发条件后，直接断开连接。 - 人机识别：触发条件后，用重定向的方式去访问客户端（返回200状态码），通过验证后才放行。例如，单个IP在20s内访问超过5次则进行人机识别判断，在10分钟内该IP的访问请求都需要通过人机识别，如果被识别为非法将会被拦截，只有被识别为合法才会放行。

成功添加频率控制自定义规则。您可以根据需要继续添加多条规则。

- 编辑规则

  a. 在规则列表中，定位到要操作的规则，单击其操作列下的编辑。

  b. 在编辑规则对话框中，修改规则配置，并单击确定。规则配置的描述见新增规则，其中，规则名称和URI不可更改。

- 删除规则

a. 在规则列表中，定位到要删除的规则，单击其操作列下的删除。

b. 在删除提示对话框中，单击确定。

5. 回到频率控制功能区域，开启状态开关，应用频率控制自定义规则。

成功应用频率控制自定义规则。

频率控制防护设置最佳实践

频率控制防护各模式的防护效果排序依次为：超级严格模式 > 严格模式 > 紧急模式 > 正常模式。同时，各防护模式导致误杀的可能性排序依次为：超级严格模式 > 严格模式 > 紧急模式 > 正常模式。

正常情况下，建议您为已接入防护的域名选择正常频率控制防护模式。该模式的防护策略较为宽松，只会针对访问频次较大的IP进行封禁。当您的网站遭遇大量HTTP Flood攻击时，且正常模式的安全防护效果已经无法满足要求，建议您切换至攻击紧急模式或严格模式。

如果您的网站业务是API或原生App应用，由于无法正常响应严格模式中的相关算法认证，无法使用严格或超级严格模式进行防护。因此，需要通过配置频率控制防护自定义规则对被攻击的URL配置针对性的防护策略拦截攻击请求。

7.2.5 设置AI智能防护

DDoS高防为已接入防护的网站业务提供AI智能防护。AI智能防护基于阿里云的大数据能力，能够自学习网站业务流量基线，结合算法分析攻击异常，并自动下发精确访问控制规则，动态调整业务防护模型，帮助您及时发现并阻断恶意攻击，例如恶意Bot、HTTP Flood攻击。本文介绍了AI智能防护的使用方法。

前提条件

- 已在DDoS高防网站配置中添加要防护的网站业务。更多信息，请参见添加网站。
- 已开启新版防护设置。

背景信息

网站业务接入DDoS高防后，您可以为网站开启AI智能防护，让智能分析引擎自学习网站业务流量基线，并结合精确访问控制规则实现自主防御恶意Web攻击。

AI智能防护支持预警和防护两种工作模式。

- 预警：检测发现恶意请求时，仅记录攻击预警日志，不会阻断任何访问请求，帮助您了解AI智能防护的效果。

  使用预警模式时，您可以结合全量日志，查询与AI智能防护有关的攻击预警记录，确认其攻击防护能力。更多信息，请参见查看攻击预警日志。

- 防护：检测发现恶意请求时，直接下发能够阻断恶意请求的精确访问控制规则，拦截恶意请求。

  > **说明:**
  > AI智能防护通过精确访问控制规则触发防护动作，要使防护生效，您必须开启精确访问控制。更多信息，请参见设置精确访问控制规则。

  一般情况下，建议您先使用预警模式，并通过全量日志报表观察攻击日志记录；在完全确认AI智能防护的效果后，再开启防护模式，使AI智能防护真实生效。

开启AI智能防护时，您也可以根据网站性能和防护需求，选择应用不同的防护等级。AI智能防护提供宽松、正常和严格三种防护等级。

防护等级	防护效果	适用场景
宽松	仅拦截已知的特定恶意攻击，不会对正常请求造成误拦截。	适合于比较大型的网站且自身处理性能比较强劲的用户，适用于大促等特定场景。
正常（推荐）	一般情况下，不对请求进行任何处置。当检测到流量对网站造成威胁时，对恶意攻击进行智能防御，对网站的正常业务影响极低。	适合请求量平稳且服务器处理性能在处理正常流量的基础上尚有冗余。
严格	对恶意攻击进行严格的智能防御，可能存在部分误拦截的现象。	适合网站性能较差或防护效果不佳的情况。

操作步骤

1. 在左侧导航栏，单击防护设置 > 通用防护策略。
2. 在通用防护策略页面，单击网站业务DDoS防护页签，并从左侧域名列表中选择要设置的域名。
3. 定位到AI智能防护功能区域，单击修改设置。

4. 在AI智能防护对话框中，选择智能防护的模式和等级，并开启状态开关。

   - 模式：预警、防护
   - 等级：宽松、正常、严格

成功开启AI智能防护。开启AI智能防护后，当检测到恶意攻击行为时，DDoS高防自动生成精确访问控制防护规则。您可以在精确访问控制模块中查看具体防护规则。

查看AI智能防护规则

1. 在左侧导航栏，单击防护设置 > 通用防护策略。
2. 在通用防护策略页面，单击网站业务DDoS防护页签，并从左侧域名列表中选择要设置的域名。
3. 定位到精确访问控制配置区域，单击设置。

4. 在精确访问控制页面，查看名称以smartcc_ 开头的规则。

   AI智能防护自动生成的精确访问控制规则的名称均以“smartcc_”开头。与自定义的精确访问控制规则不同，AI智能防护规则具有以下特性：

   - 规则动作可能是预警。在预警模式下，AI智能防护自动生成的精准防护规则的动作均是预警（只记录攻击日志，不进行拦截）。
   - 具有时效性。AI智能防护下发的规则存在有效期，超过有效期，防护规则自动失效并清除。
   - 不支持手动删除。如果您关闭AI智能防护，则所有AI智能防护规则立即清空。

查看攻击预警日志

网站业务开启AI智能防护后，当DDoS高防检测到恶意攻击行为且命中AI智能防护的防护规则时，DDoS高防的全量日志功能将记录相应的攻击日志。您可以在全量日志中查询与AI智能防护的防护规则关联的攻击预警日志，了解AI智能防护的防护效果。

前提条件

- 在执行查询操作前，请确认您已为网站域名开启全量日志功能。更多信息，请参见全量日志。
- 已为网站域名开启AI智能防护，且使用预警模式。

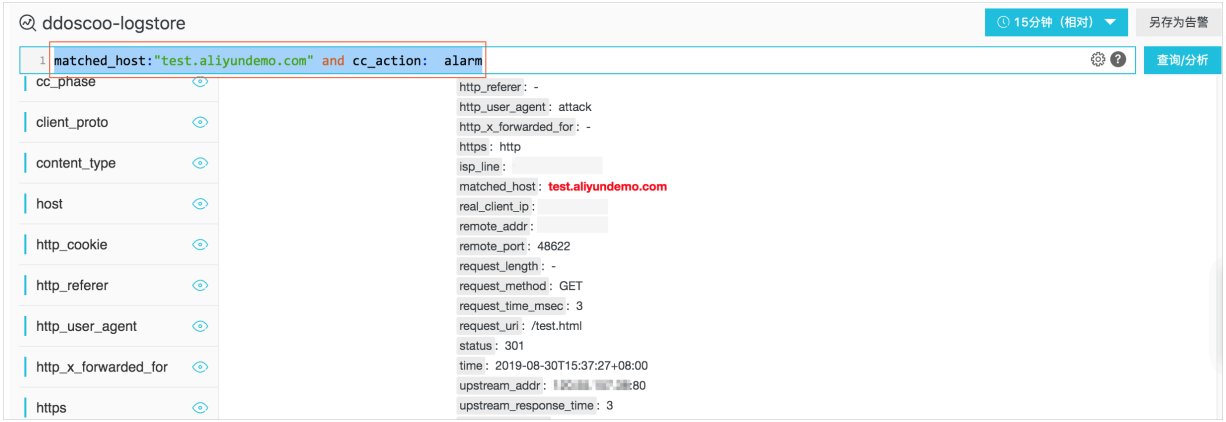
查询语句

登录云盾DDoS高防（新BGP）控制台，在统计 > 全量日志页面，选择域名并输入以下查询语句，查看与AI智能防护相关的攻击预警日志：

说明:

请将`test.aliyundemo.com`替换为您的网站域名。

```
matched_host:"test.aliyundemo.com" and cc_action:alarm
```



7.3 非网站业务DDoS防护

7.3.1 设置DDoS防护策略

DDoS高防提供针对网络四层DDoS攻击的防护策略设置功能，例如开启虚假源和空连接检测、源限速、目的限速，适用于优化调整非网站业务的DDoS防护策略。在DDoS高防实例（IP）下添加转发规则，接入非网站业务后，您可以单独设置某个端口转发规则的DDoS防护策略或批量添加DDoS防护策略。本文介绍了具体的操作方法。

前提条件

已在端口配置中添加转发规则。更多信息，请参见添加规则。

背景信息

非网站业务的DDoS防护策略是基于“IP地址+端口”级别的防护，对于已接入DDoS高防实例的非网站业务的“IP+端口”的连接速度、包长度等参数进行限制，实现缓解小流量的连接型攻击的防护能力。DDoS防护策略配置针对端口级别生效。

DDoS高防为已接入的非网站业务提供以下DDoS防护策略设置。

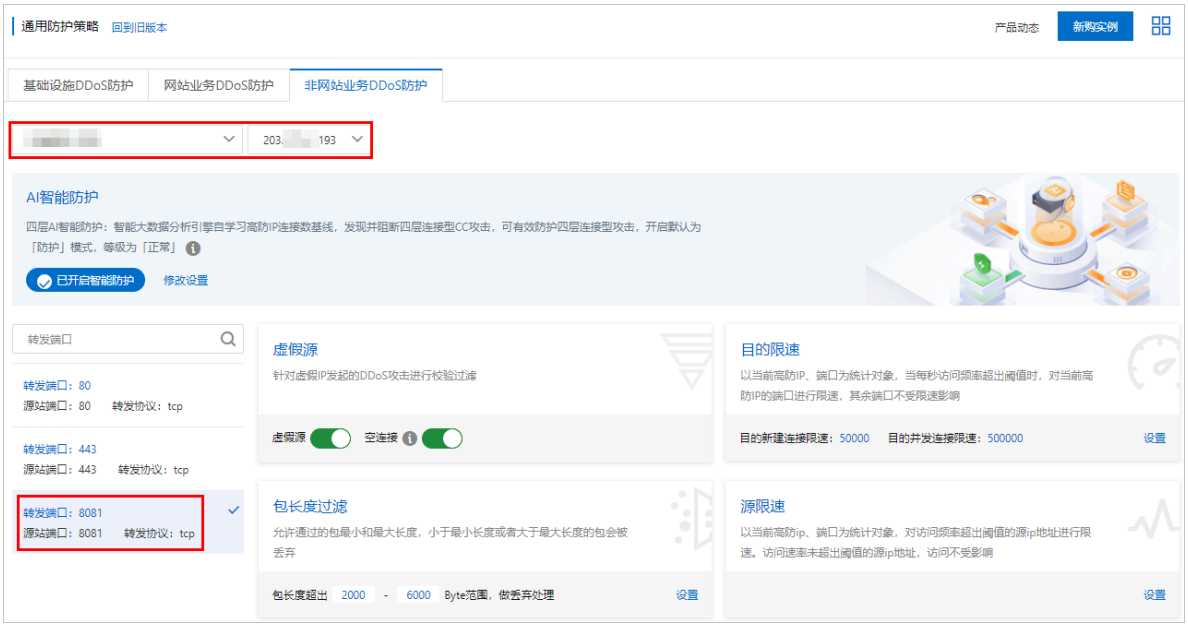
- 虚假源：针对虚假IP发起的DDoS攻击进行校验过滤。
- 目的限速：以当前高防IP、端口为统计对象，当每秒访问频率超出阈值时，对当前高防IP的端口进行限速，其余端口不受限速影响。
- 包长度过滤：设置允许通过的包最小和最大长度，小于最小长度或者大于最大长度的包会被丢弃。
- 源限速：以当前高防IP、端口为统计对象，对访问频率超出阈值的源IP地址进行限速。访问速率未超出阈值的源IP地址，访问不受影响。源限速支持黑名单控制，对于60秒内5次超限的源IP，您可以启用将源IP加入黑名单的策略，并设置黑名单的有效时长。

操作步骤

以下步骤描述了单独设置高防IP下某一条转发规则的DDoS防护策略的方法，您也可以在高防IP下批量添加DDoS防护策略，具体请参见批量添加DDoS防护策略。

1. 登录云盾DDoS高防（新BGP）控制台。
2. 在左侧导航栏，单击防护设置 > 通用防护策略。
3. 在通用防护策略页面，单击非网站业务DDoS防护页签。

4. 选择要设置的DDoS高防实例，并在转发规则列表中单击要操作的转发规则。



5. 为指定的转发规则设置虚假源、目的限速、包长度过滤、源限速。

- 虚假源：在虚假源下开启或关闭虚假源和空连接开关。

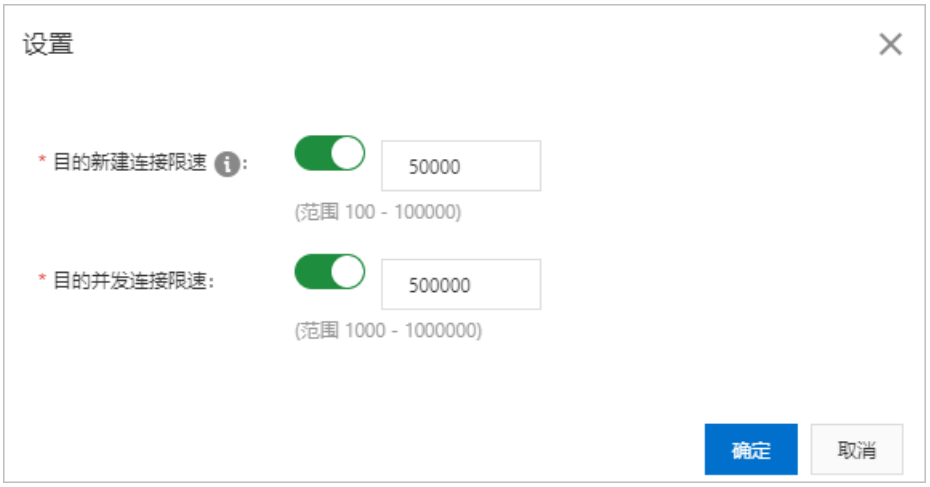
说明
虚假源地址攻击防护开关。开启后将自动过滤虚假源IP地址的连接请求。 说明： 仅适用于TCP协议规则。

说明	
空连接防护开关。开启后，将自动过滤空连接请求。 **说明：** 仅适用于TCP协议规则，且要开启空连接，必须先开启虚假源。	

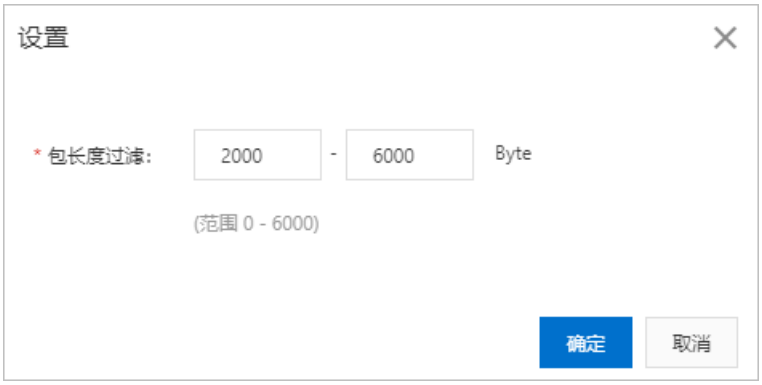
- 目的限速：单击目的限速下的设置，并在设置对话框中完成以下配置，完成后单击确定。

说明	
限制高防IP端口每秒最大的新建连接数，取值范围：100~100000（个）。超过限制的新建连接将被丢弃。 **说明：** 由于防护设备为集群化部署，新建连接限速存在一定误差。	

说明	
限制高防IP端口的最大并发连接数量，取值范围：并00~100000（个）。超过限制的并发连接将被丢弃。 接 限 速	



- 包长度过滤：单击包长度过滤下的设置，并在设置对话框中设置允许通过高防IP端口的报文所含payload的最小和最大长度，取值范围：0~6000（Byte）。完成后单击确定。



- 源限速：单击源限速下的设置，并在源限速设置侧边页完成以下配置，完成后单击确定。

配置项	说明
源新建连接限速	限制单一源IP的每秒新建连接数量，取值范围：1~50000（个）。超过限制的新建连接将被丢弃。支持自动和手动模式。 - 启用自动防护模式后，系统将动态自动计算源新建连接限速阈值，无需手动设置。 - 如果选择手动模式，则需要手动设置源新建连接限速阈值。 说明: 由于防护设备为集群化部署，新建连接限速存在一定误差。 黑名单策略 - 支持源新建连接60秒内5次超限，将该源IP加入黑名单选项，源IP若进入黑名单，则其连接请求都将被丢弃。 - 开启黑名单策略时，需要设置黑名单有效时长，取值范围：1~10080（分钟），默认为30分钟。源IP被加入黑名单时，经有效时长后自动被释放。
源并发连接限速	限制单一源IP的并发连接数量，取值范围：1~50000（个）。超过限制的并发连接将被丢弃。 黑名单策略 - 支持源并发连接60秒内5次超限，将该源IP加入黑名单选项，源IP若进入黑名单，则其连接请求都将被丢弃。 - 开启黑名单策略时，需要设置黑名单有效时长，取值范围：1~10080（分钟），默认为30分钟。源IP被加入黑名单时，经有效时长后自动被释放。
源PPS限速	限制单一源IP的包转发数量，取值范围：1~100000（Packets/s）。超过限制的数据包将被丢弃。 黑名单策略 - 支持源PPS连接60秒内5次超限，将该源IP加入黑名单选项，源IP若进入黑名单，则其连接请求都将被丢弃。 - 开启黑名单策略时，需要设置黑名单有效时长，取值范围：1~10080（分钟），默认为30分钟。源IP被加入黑名单时，经有效时长后自动被释放。

配置项	说明
源带宽限速	限制单一源IP的源请求带宽，取值范围：1024~268435456（Byte/s）。 黑名单策略 - 支持源带宽连接60秒内5次超限，将该源IP加入黑名单选项，源IP若进入黑名单，则其连接请求都将被丢弃。 - 开启黑名单策略时，需要设置黑名单有效时长，取值范围：1~10080（分钟），默认为30分钟。源IP被加入黑名单时，经有效时长后自动被释放。

批量添加DDoS防护策略

1. **登录云盾*DDoS*高防控制台。**
2. **在左侧导航栏，单击接入管理 > 端口接入。**

3. 在端口配置页面，选择DDoS高防实例和IP，并单击规则列表下方的批量操作 > DDoS防护策略配置。

4. 在批量添加DDoS防护策略对话框中，按照格式要求输入要添加的防护策略内容，并单击添加。DDoS防护策略的格式要求如下。

说明:

您也可以先批量导出当前DDoS防护策略，在导出的txt文件中统一调整后再将内容复制粘贴进来。导出文件中的DDoS防护策略格式和批量添加DDoS防护策略的格式要求一致。更多信息，请参见批量导出。

- 每行对应一条转发规则的DDoS防护策略。
- 每条DDoS防护策略从左到右包含以下字段：转发协议端口、转发协议（tcp、udp）、源新建连接限速、源并发连接限速、目的新建连接限速、目的并发连接限速、包长度最小值、

包长度最大值、虚假源开关、空连接开关（字段的含义和取值范围见*DDoS*防护策略配置项说明）。字段间以空格分隔。

- 转发协议端口必须是已添加规则的端口。
- 虚假源开关和空连接开关的取值是：on、off。若为空则表示关闭（即off）。

7.3.2 设置四层AI智能防护等级

DDoS高防实例默认启用智能防护功能，通过算法自主学习接入业务的历史流量，自适应调整四层流量清洗策略，提供最佳防御效果。业务接入DDoS高防后，将直接获得正常等级的智能防护能力，无需您手动设置。若正常等级的防御效果不够理想，您可以根据实际需求选择更宽松或严格的智能防护等级。

背景信息

针对网络四层DDoS攻击，DDoS高防智能防护结合历史业务流量及阿里云攻防安全专家的经验，提供宽松、正常、严格三种智能防护等级供您选择。默认情况下，您所购买的DDoS高防实例自动开启四层AI智能防护，并选用正常防御等级。您可以根据实际情况自由调整智能防护等级。

由于智能防护功能通过算法学习您的历史业务流量情况，因此业务初次接入DDoS高防进行防护时，系统需要三天左右时间完成对您业务流量的学习和训练，从而达到最佳防御效果。

对于带有明显攻击特征的恶意IP，智能防护算法将根据需要自动将其添加到高防实例的流量黑名单中，在一定时间内丢弃其全部访问请求。您可以随时查看或删除IP黑名单中的IP，也可以在IP黑名单中手动添加其他恶意IP进行防御。同时，您还可以将特定的IP添加至流量白名单，系统将直接放行来自这些IP的业务访问流量。更多信息，请参见管理流量黑白名单。

操作步骤

1. 在通用防护策略页面，单击非网站业务DDoS防护页签。
2. 选择要设置的DDoS高防实例，并在AI智能防护区域，单击修改设置。

3. 在AI智能防护对话框中，根据攻击情况选择要应用的防护等级，并单击确定。 不同防护等级的说明如下。
   - 宽松：对来自带有明显攻击特征的恶意IP的流量进行自动清洗。该等级可能无法拦截所有四层流量攻击，但误杀率低。
   - 正常：对来自带有明显攻击特征的恶意IP和疑似恶意IP的流量进行自动清洗。该等级默认启用，能够充分平衡防护效果和误杀率，建议您在一般情况下选择该等级。
   - 严格：对当前正在发生的攻击行为具有最强防御效果，但可能存在一定误杀。

成功修改智能防护等级，目标DDoS高防实例将按照调整后的防御等级工作。

7.3.3 源限速配置

源限速配置允许您对源IP到指定高防IP端口的访问频率和流量大小进行限制。启用源限速配置后，超出访问限制的源IP将触发请求限速或加入黑名单处理。源IP一旦被添加到黑名单，则所有来自该IP的访问请求会被丢弃。本文介绍了配置源限速的具体操作。

前提条件

DDoS高防IP下已添加转发规则。更多信息，请参见添加规则。

背景信息

DDoS高防支持对源IP到特定高防IP端口的访问频率进行限制，限制维度包括源新建和源并发等；也支持对源IP到特定高防IP端口的流量大小进行限制，限制维度包括源带宽（bps）和源报文数量（pps）。针对超过访问频率或流量阈值的IP，高防对其进行限速和设置黑名单处理。上述功能适用于防护四层连接型CC攻击，能够起到快速压制攻击源的目的，效果明显。

假设访问高防IP 8000端口的源IP1，其新建连接异常高，超出正常水平十多倍。您可以为该高防IP的8000端口配置源新建限速，反复超限的源IP自动设置成黑名单，丢弃该攻击源的访问请求。

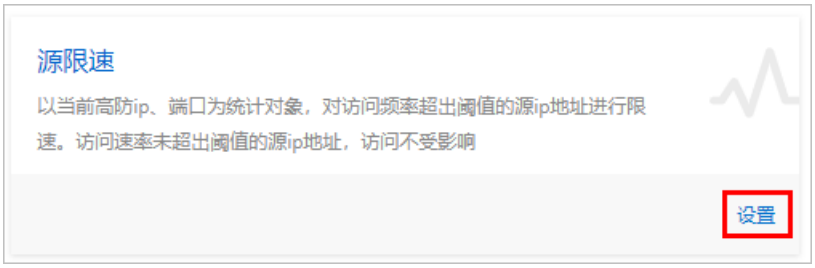
说明:

源限速配置针对高防IP的具体端口生效。如果您需要对多个不同高防IP的端口启用源限速，则需要对不同高防IP的端口分别进行配置；暂不支持批量配置。

操作步骤

1. 登录云盾DDoS高防控制台。
2. 在左侧导航栏，单击接入管理 > 端口接入。
3. 在端口配置页面，选择要操作的DDoS高防实例和IP。
4. 定位到要操作的转发规则，单击其DDoS防护策略列下的配置。

5. 单击源限速下的设置。

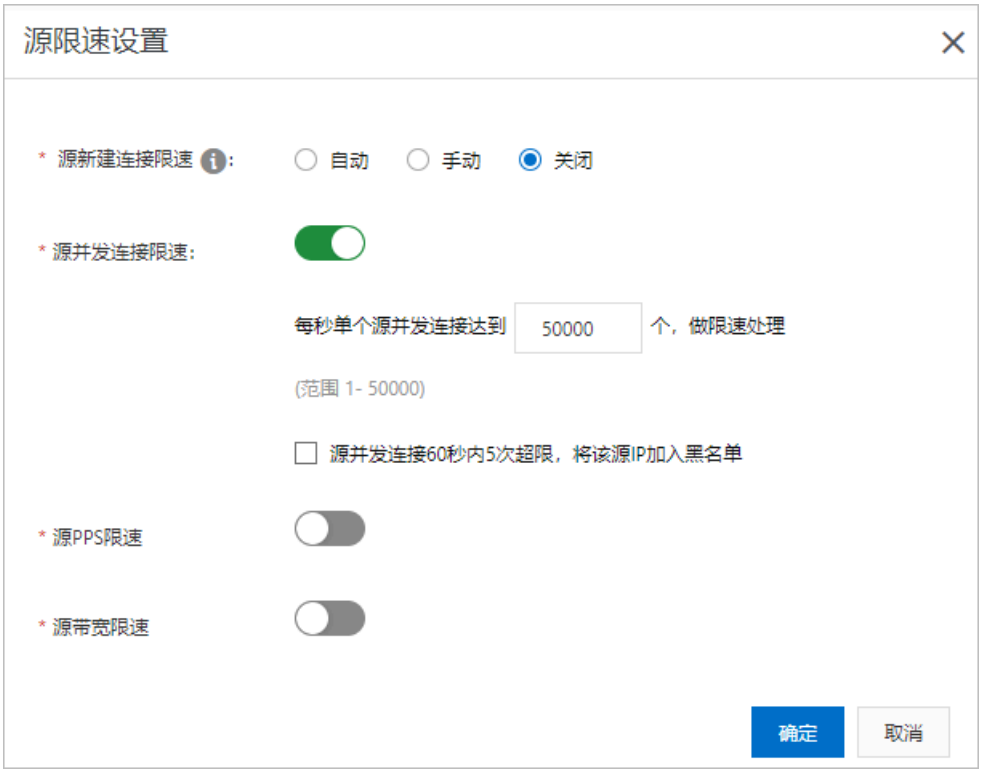


6. 在源限速设置对话框中，完成限速配置。

   以下图中配置为例，配置生效后，访问该高防端口的源并发最大不能超过50000个/秒，超过的源IP将被限速。如果勾选源并发连接60秒内5次超限，将该源IP加入黑名单，则DDoS高防将

统计每个超限源IP在1分钟内的超限次数；如果大于5次，该源IP将被加入黑名单，所有来自该源IP的请求将被丢弃。

源新建连接限速、源PPS限速和源带宽限速的使用方法同上。更多信息，请参见设置DDoS防护策略。



7. 单击确定，使配置生效。

7.4 加速网站静态页面访问

DDoS高防在流量清洗中心集成网页缓存技术，在为网站业务提供DDoS防护的同时还可以加速网站静态页面的访问。

前提条件

使用静态页面缓存功能前，请确认您的网站域名已接入增强功能套餐的DDoS高防实例。

背景信息

您可以通过静态页面缓存功能加速已接入DDoS高防的网站域名访问。同时，您还可以通过自定义规则为域名中的指定页面设置缓存策略。

操作步骤

1. 登录云盾DDoS高防（新BGP）控制台。
2. 在左侧导航栏，单击DDoS防护实验室 > 网页缓存加速
3. 在网络加速策略页面，选择要开启静态页面缓存的域名。

4. 定位到静态页面缓存功能区域，选择静态页面缓存的模式，并开启静态页面缓存状态开关。静态页面缓存支持标准、增强、不缓存三种模式。

   - 标准：仅对该网站域名的静态文件请求（.css，.js，.txt）尝试进行缓存。
   - 增强：对该网站域名的所有请求尝试进行缓存。
   - 不缓存：不对该网站域名的请求进行缓存。

5. 为网站下指定URI自定义静态页面缓存规则。

   a) 在静态页面缓存功能区域，单击设置。

   b) 在静态页面缓存自定义规则页面，单击新增规则。

   c) 在新增规则对话框中，设置规则名称，填写指定页面的URI，选择缓存模式，并根据需要设置页面缓存的过期时间。

> **说明:**

页面缓存规则中的URI无需填写参数，且不支持通配符。例如，填写/a/即指定www.a.com/a/路径下的所有页面。

d) 完成规则配置后，单击确定。

成功添加静态页面缓存自定义规则。

7.5 定制场景策略

DDoS高防的定制场景策略允许您在特定的业务突增时段（例如新业务上线、双11大促销等）选择应用独立于通用防护策略的定制防护策略模板，保证适应业务需求的防护效果。您可以根据需要设置定制场景策略。

背景信息

注意:

- 如果业务无明显突增且容易遭受攻击，建议您采用通用防护策略，不要启用定制场景防护策略。
- 定制场景策略功能仅在新版防护引擎中开放。如果您使用的不是新版防护引擎，建议您切换到新版防护引擎再开启定制场景策略。

定制场景策略提供基于业务场景定制的DDoS防护策略模板供您选择。创建定制场景策略时，您只需根据业务场景类型选择要应用的模板，并配置要应用策略的活动对象（目前仅支持域名对象）即可。定制场景策略在有效时间段内生效。策略生效期间，域名的DDoS防护策略以防护策略模板的定义为准，暂时忽略通用防护策略配置。

支持的策略模板

目前仅提供重大活动策略模板，后续将开放其他基于场景定制的策略模板。

应用示例

当网站有重大活动时，网站整体请求量较大，流量表现会与平时差异较大。这种情况下，如果使用正常业务模式的DDoS防护策略，可能带来误杀。建议您使用定制场景策略-重大活动功能，该功能会在指定的活动期间自动调整DDoS防护策略。自动调整策略的逻辑如下：

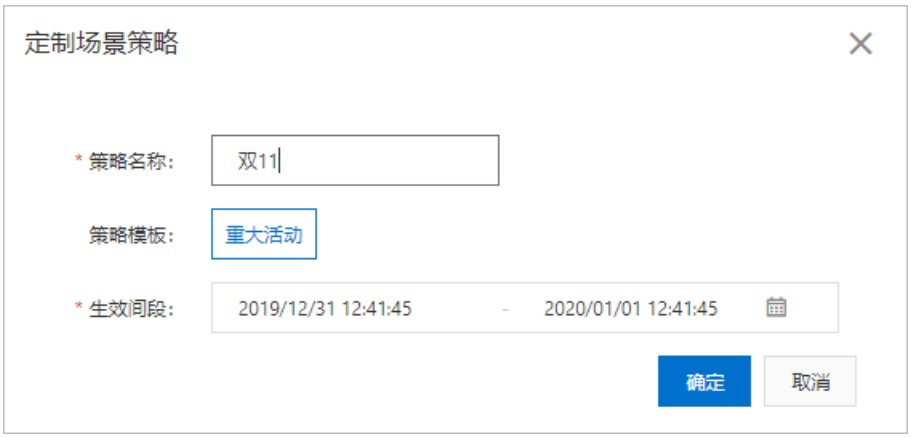
- **活动开始时，自动记录AI智能防护、频率控制的开关配置，并自动将这两个功能的开关设置为关闭，避免误伤。**
- **活动结束时，自动将这两个功能的开关恢复为先前配置。**
- **若您在活动期间手动开启这两个功能的开关，则以手动配置为准。**

操作步骤

1. **在左侧导航栏，单击防护设置 > 定制场景策略。**
2. **在定制场景策略页面，单击新建策略。**
3. **在定制场景策略对话框，完成以下配置，并单击确定。**

配置项	说明
策略名称	为策略命名。
策略模板	选择要应用的定制策略模板，可选值：重大活动。

配置项	说明
生效间断	选择策略的有效时间段。 **说明:** 应用同一个策略模板的策略的生效间断不允许重合。

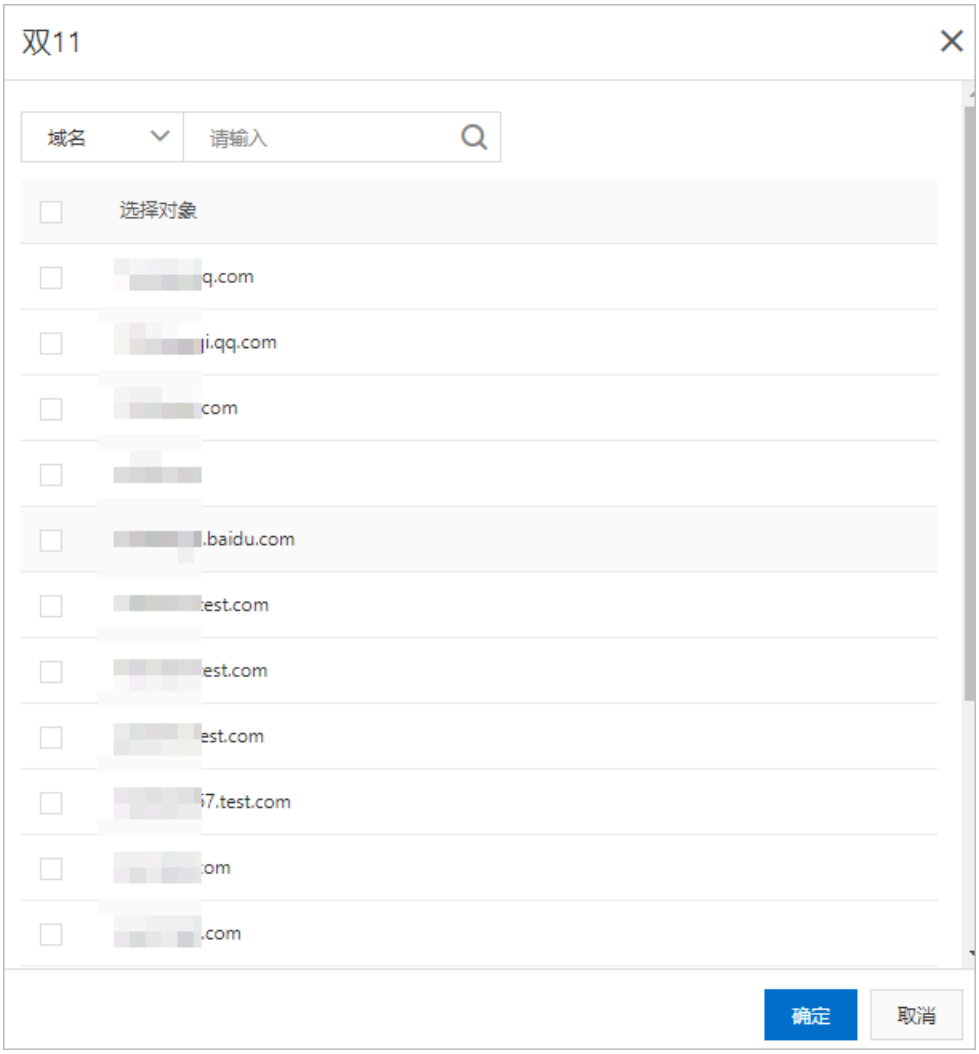


成功添加策略，已添加策略默认开启。您可以在策略列表中看到新建的策略，并通过策略的状态了解策略是否生效。不同策略状态的含义说明如下。

- 等待生效：当前时间还未到活动生效时间段。
- 生效中：活动策略下发生效中，需要1~2分钟完成。
- 运行生效：当前时间处于活动生效时间段。
- 已经失效：当前时间晚于活动生效时间段。
- 已被禁用：策略被禁用。即使当前时间处于活动生效时间段内，活动策略也不会生效。

4. 在策略列表中，定位到新建的策略，单击其操作列下的配置对象。

5. 在域名侧边页，从已接入DDoS高防的域名中勾选要应用当前策略的域名，并单击确定。



成功应用策略。策略的防护对象信息已更新。您可以将光标悬置在防护对象信息上，查看应用当前策略的域名。

后续步骤

根据需要在定制场景策略页面管理所有定制场景策略，例如禁用/启用策略、编辑策略、删除策略。

8 调查分析

8.1 全量日志分析

DDoS高防的网站访问日志（包含CC攻击日志）与阿里云日志服务联动，为您提供实时分析与报表中心功能。DDoS高防全量日志为增值服务，需要开通后使用。开通全量日志，则日志服务实时采集接入DDoS高防的网站业务的访问日志、CC攻击日志，并对采集到的日志数据进行实时检索与分析，以仪表盘形式展示查询结果。

背景信息

根据*APNIC 2017*年*DDoS*风险报告，超过80%的DDoS攻击都会混合HTTP攻击，而其中混合的CC攻击尤其隐蔽，因此通过日志对访问和攻击行为进行即时分析研究并附加防护策略就显得尤其重要。

DDoS高防全量日志基于阿里云日志服务，在DDoS高防控制台为您提供日志查询与分析界面，方便您对接入DDoS高防的网站业务进行自主分析。开通全量日志后，您也可以使用日志服务提供的日志消费和投递等功能，全面管理DDoS高防的网站访问日志。

阿里云日志服务（Log Service，简称 LOG）是针对日志类数据的一站式服务，在阿里巴巴集团经历大量大数据场景锤炼而成。您无需开发就能快捷完成日志数据采集、消费、投递以及查询分析等功能，提升运维、运营效率，建立DT时代海量日志处理能力。更多信息，请参见什么是日志服务。

开通全量日志服务

1. 在左侧导航栏，单击调查分析 > 全量日志分析。
2. 在日志服务页面，单击立即购买。
3. 在全量日志服务购买页面，将适用产品设置为新BGP高防，并根据您的业务需要，选择合适的全量日志服务规格。
   - 日志存储量：日志信息的最大存储空间，单位TB。当您选购的日志存储空间占满后，将不再继续存储新的日志信息。建议您关注日志存储空间的使用量，及时升级日志存储量规格。
   - 使用时长：全量日志服务的有效期。全量日志服务有效期到期后，将停止存储新的日志信息。服务到期七天后如仍未续费延长服务有效期，将自动删除所有日志信息。

   全量日志服务的单价为500元/TB（日志存储量）/月（使用时长）。

   说明:

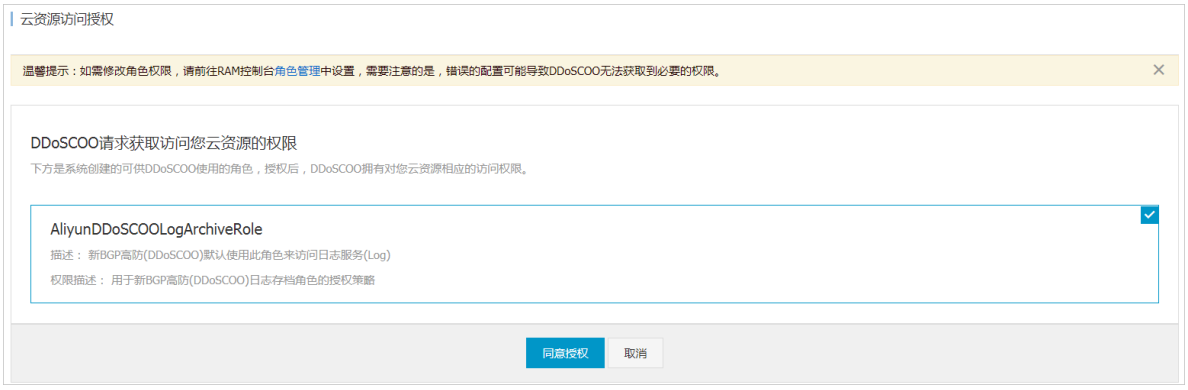
当全量日志服务的日志存储量足够大且在服务有效期内，将从使用全量日志服务的第一天开始，连续存储180天的日志信息。第181天的日志信息，将覆盖第一天存储的日志信息，即始终保持存储最近180天的全量日志信息。

日志存储量选择示例

一般情况下，每条请求日志大约占用2 KB存储空间，如果您的业务的平均请求量为500 QPS，则一天的日志存储所需要的存储空间为：500*60*60*24*2 = 86,400,000 KB（即82 GB）；系统默认的存储周期为180天，如果您需要存储最近180天的日志，则需要选择的日志存储量规格为14,832 GB（约14.5 TB）。

4. **单击立即购买，完成支付。**
5. **回到DDoS高防（新BGP）控制台，在日志服务页面，单击立即授权。**

6. 在云资源访问授权页面中，单击同意授权，授权DDoS高防服务将日志存储至您的日志服务专属日志库中。



开通全量日志服务并完成云资源访问授权后，您可以在日志服务页面单击规格详情，查看当前的全量日志服务规格信息。

说明:

建议您在全量日志服务使用期间，定期关注全量日志存储空间的使用情况和服务有效期。

- 当日志存储空间使用量超过70%时，请及时升级日志存储量规格，避免新产生的日志无法存储影响日志存储的连续性。
- 当日志存储空间长期空闲时，您也可以根据实际日志量的大小，降低日志存储规格。

为网站启用全量日志

1. 在左侧导航栏，单击调查分析 > 全量日志分析。
2. 在日志服务页面，选择网站域名，开启其状态开关，为网站域名启用全量日志。
   启用全量日志后，您可以在日志服务页面对采集到的日志数据进行实时查询与分析、查看或编辑仪表盘、设置监控告警等。

关于DDoS高防服务的日志分析与日志报表功能，请参见#unique_83和#unique_84。

使用全量日志

依托于阿里云日志服务强大的功能，为网站域名启用全量日志后，在全量日志页面您可以对所采集的网站访问日志和攻击防护日志进行深入的分析、以可视化的方式展示、根据所设定的阈值实现监控报警等。

功能项	说明	更多信息
查询和分析	对采集到的日志数据进行实时查询分析，查询分析语句由查询语句（Search）和分析语句（Analytics）两个部分组成，查询和分析语句之间通过|进行分割。 例如，您可以通过以下查询分析语句查询域名的访问量： `* | SELECT COUNT(*) as times, host GROUP by host ORDER by times desc limit 100` 更多查询语句示例，请参见下文常用查询语句示例。	查询与分析
分析图表	查询分析语句中包含分析语法，语句执行后默认按表格方式展示分析结果。同时，您还可以选择折线图、柱状图、饼图等多种图形方式进行展示。	分析图表
仪表盘	仪表盘是日志服务提供的实时数据分析大盘。您将常用的查询语句以图表形式展示后，可将分析图表保存到仪表盘中。 同时，全量日志服务默认为您提供DDoS访问中心和DDoS运营中心两个仪表盘。 您还可以通过订阅仪表盘功能，通过邮件或者钉钉群消息将仪表盘内容定时推送给指定对象。	仪表盘
监控告警	您可以根据仪表盘中的查询图表设置告警，实现实时的服务状态监控。	告警

全量日志应用场景

全量日志可以满足您在以下访问日志分析场景中的需求。

- **排查网站访问异常**

  配置日志服务采集DDoS高防日志后，您可以对采集到的日志进行实时查询与分析。使用SQL语句分析网站访问日志，对网站的访问异常进行快速排查和问题分析，并查看读写延时、运营商分布等信息。

  例如，通过以下语句查看网站访问日志：

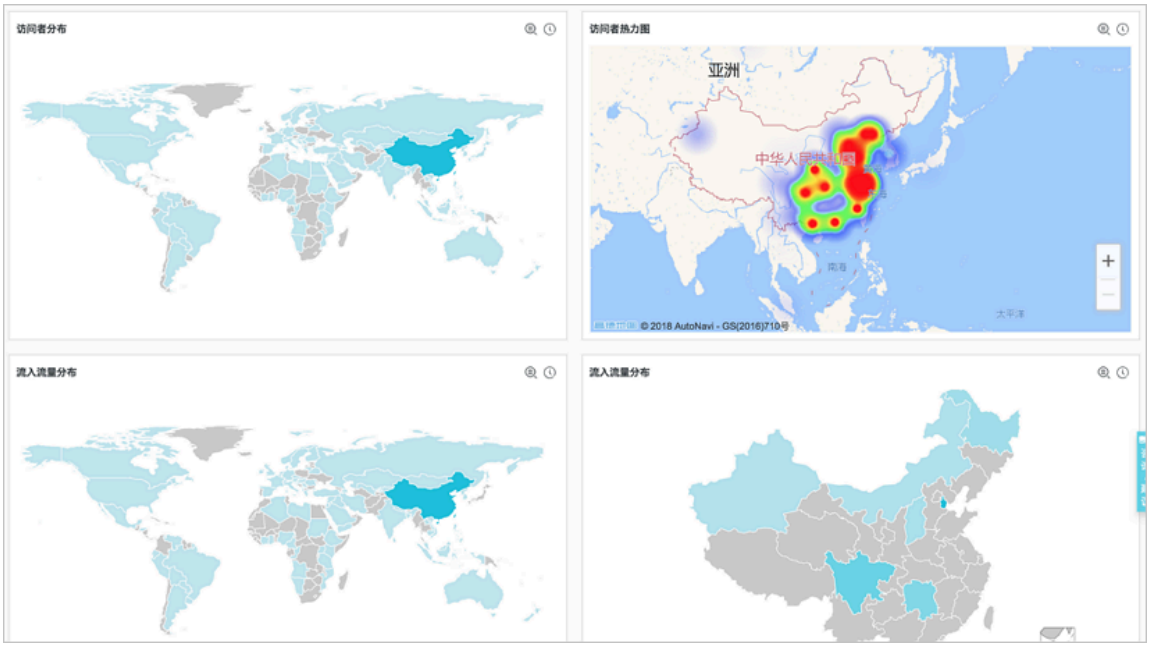
  ```
  __topic__: DDoS_access_log
  ```

- **追踪CC攻击者来源**

  访问日志中记录了CC攻击者的分布及来源，通过对DDoS访问日志进行实时查询与分析，您可以对CC攻击者进行来源追踪、溯源攻击事件，为您的应对策略提供参考。

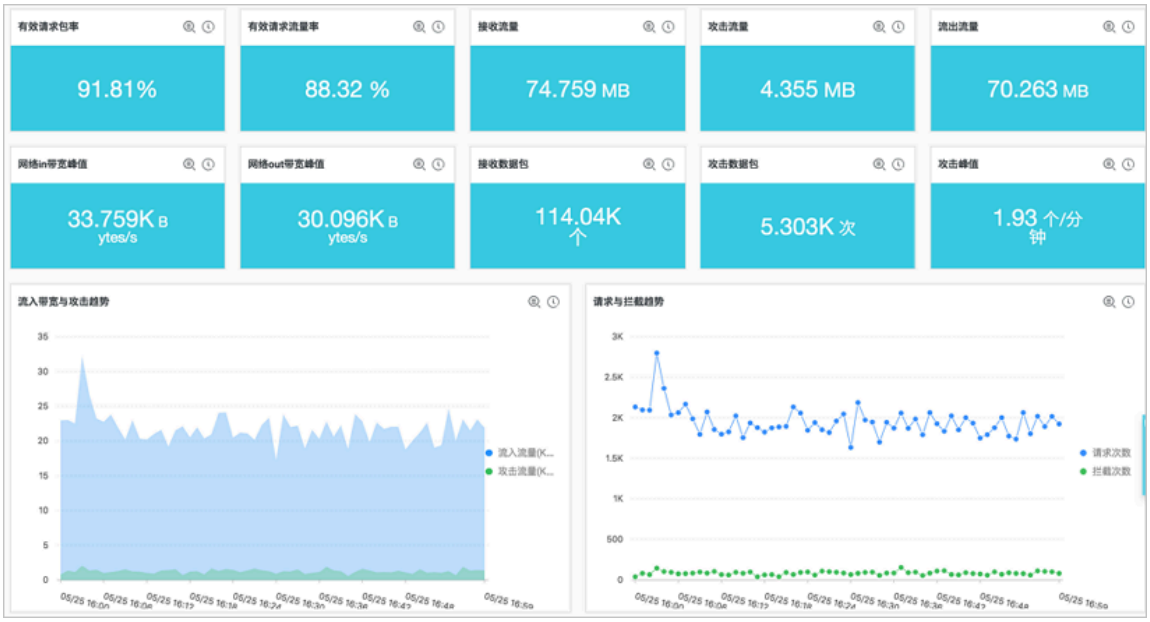
  - **例如，通过以下语句分析DDoS访问日志中记录的CC攻击者国家分布：**

    ```
    __topic__: DDoS_access_log and cc_blocks > 0| SELECT ip_to_country
    (if(real_client_ip='-', remote_addr, real_client_ip)) as country,
    count(1) as "攻击次数" group by country
    ```

  - **例如，通过以下语句查看访问PV：**

    ```
    __topic__: DDoS_access_log | select count(1) as PV
    ```

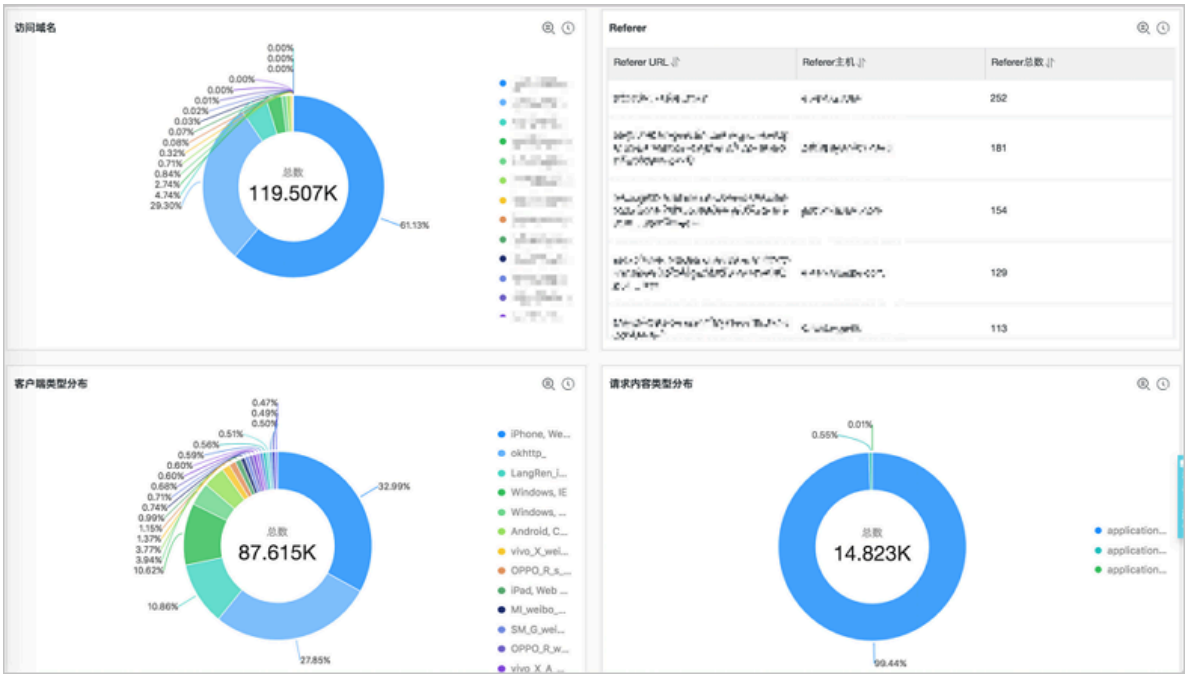
    

- **网站运营分析**

  网站访问日志中实时记录网站访问数据，您可以对采集到的访问日志数据进行SQL查询分析，得到实时的访问情况，例如判断网站热门程度、访问来源及渠道、客户端分布等，并以此辅助网站运营分析。

  例如，查看来自各个网络服务提供商的访问者流量分布：

```
__topic__: DDoS_access_log | select ip_to_provider(if(real_client_ip
='-', remote_addr, real_client_ip)) as provider, round(sum(request_le
ngth)/1024.0/1024.0, 3) as mb_in group by provider having ip_to_prov
ider(if(real_client_ip='-', remote_addr, real_client_ip)) <> '' order
by mb_in desc limit 10
```



常用查询语句示例

- **拦截类型查询**

```
* | select cc_action,cc_phase,count(*) as t group by cc_action,
cc_phase order by t desc limit 10
```

- **QPS查询**

```
* | select time_series(__time__,'15m','%H:%i','0') as time,count(*)/
900 as QPS group by time order by time
```

- **被攻击域名查询**

```
* and cc_blocks:1 | select cc_action,cc_phase,count(*) as t group by
 cc_action,cc_phase order by t desc limit 10
```

- **被攻击URL查询**

```
* and cc_blocks:1 | select count(*) as times,host,request_path group
 by host,request_path order by times
```

- **请求详情**

```
* | select date_format(date_trunc('second',__time__),'%H:%i:%s')
as time,host,request_uri,request_method,status,upstream_status,
querystring limit 10
```

- **5XX状态码查询**

```
* and status>499 | select host,status,upstream_status,count(*)as t
group by host,status,upstream_status order by t desc
```

- **请求时延分布**

```
* | SELECT count_if(upstream_response_time<20) as "<20",
count_if(upstream_response_time<50 and upstream_response_time>20) as
 "<50",
count_if(upstream_response_time<100 and upstream_response_time>50)
as "<100",
count_if(upstream_response_time<500 and upstream_response_time>100)
as "<500",
count_if(upstream_response_time<1000 and upstream_response_time>500
) as "<1000",
count_if(upstream_response_time>1000) as ">1000"
```

相关文档

- **全量日志字段说明**
- **日志查询语法**
- *SQL*分析语法

8.2 全量日志字段说明

DDoS高防的全量日志功能记录丰富的日志字段。

您可以在当前的全量日志页面对采集到的日志进行实时查询与分析等操作。详细的日志字段说明，参见下表。

字段	说明	示例
__topic__	日志主题（Topic），固定为ddos_access_log。	-
body_bytes_sent	请求发送Body的大小，单位为字节。	2
content_type	内容类型。	application/x-www-form-urlencoded
host	源网站。	api.abc.com
http_cookie	请求cookie。	k1=v1;k2=v2
http_referer	请求referer，若没有，显示为-。	http://xyz.com
http_user_agent	请求User Agent。	Dalvik/2.1.0 (Linux; U; Android 7.0; EDI-AL10 Build/HUAWEIEDISON-AL10)
http_x_forwarded_for	通过代理跳转的上游用户IP。	-
https	该请求是否为HTTPS请求，其中： · true：该请求是HTTPS请求。 · false：该请求是HTTP请求。	true
matched_host	匹配的配置的源站，可能是泛域名。未匹配则为-。	*.zhihu.com
real_client_ip	访问客户的真实IP，获取不到时为-。	1.2.3.4
isp_line	线路信息，例如BGP、电信、联通等。	电信
remote_addr	请求连接的客户端IP。	1.2.3.4
remote_port	请求连接的客户端端口号。	23713

字段	说明	示例
request_length	请求长度，单位为字节。	123
request_method	请求的HTTP方法。	GET
request_time_msec	请求时间，单位为毫秒。	44
request_uri	请求路径。	/answers/377971214/banner
server_name	匹配到的host名，没有匹配到则为`default`。	api.abc.com
status	HTTP状态。	200
time	时间。	2018-05-02T16:03:59+08:00
cc_action	CC防护策略行为，例如none、challenge、pass、close、captcha、wait、login等。	close
cc_blocks	表示是否被CC防护策略阻断，其中： · `1`：表示阻断。 · 其他内容表示通过。 说明： 部分情况下，日志中可能不存在该字段。而是以`last_result`字段记录请求是否被CC防护策略阻断。	1
last_result	表示是否被CC防护策略阻断，其中： · ok：表示通过。 · failed：表示不通过，包括校验未通过和阻断。 说明： 部分情况下，日志中可能不存在该字段。而是以`cc_blocks`字段记录请求是否被CC防护策略阻断。	failed

字段	说明	示例
cc_phase	CC防护策略，包括seccookie、server_ip_blacklist、static_whitelist、server_header_blacklist、server_cookie_blacklist、server_args_blacklist、qps_overmax等。	server_ip_blacklist
ua_browser	浏览器。 说明: 部分情况下，日志中可能不存在该字段。	ie9
ua_browser_family	浏览器系列。 说明: 部分情况下，日志中可能不存在该字段。	internet explorer
ua_browser_type	浏览器类型。 说明: 部分情况下，日志中可能不存在该字段。	web_browser
ua_browser_version	浏览器版本。 说明: 部分情况下，日志中可能不存在该字段。	9.0
ua_device_type	客户端设备类型。 说明: 部分情况下，日志中可能不存在该字段。	computer
ua_os	客户端操作系统。 说明: 部分情况下，日志中可能不存在该字段。	windows_7

字段	说明	示例
ua_os_family	客户端操作系统系列。 说明: 部分情况下，日志中可能不存在该字段。	windows
upstream_addr	回源地址列表，格式为IP:Port，多个地址用逗号分隔。	1.2.3.4:443
upstream_ip	实际回源地址IP。	1.2.3.4
upstream_response_time	回源响应时间，单位为秒。	0.044
upstream_status	回源请求HTTP状态。	200
user_id	阿里云账号ID。	12345678
querystring	请求字符串。	token=bbcd&abc=123

8.3 操作日志

您可以在云盾DDoS高防控制台的日志页面，查看近30天的重要操作日志。

说明:
操作日志只记录最近30天中的重要操作，并非记录所有用户行为。

操作日志内容	支持情况
ECS更换IP日志	支持
黑洞解封操作日志	支持
流量封禁/解封操作日志	支持
四层流量清洗模式变更操作日志	支持
CC防护模式变更操作日志	支持
弹性防护带宽变更操作日志	支持

9 资产管理

9.1 设置实例标签

DDoS高防提供标签管理功能，方便您标记DDoS高防实例资源，实现分类批量管理。

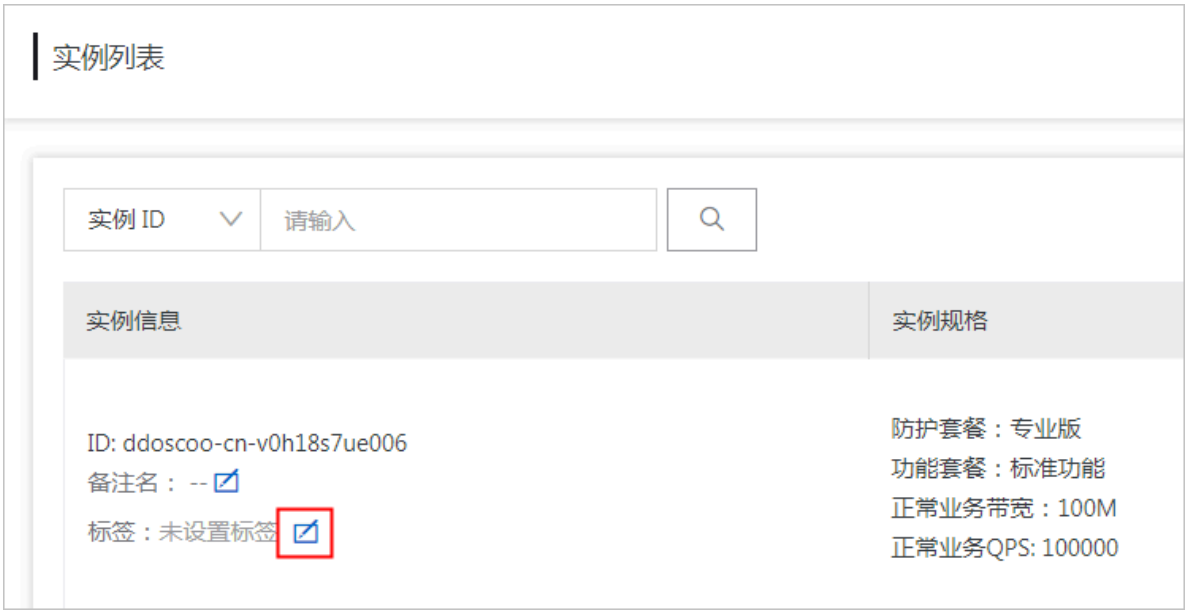
背景信息

每个标签都由一对键值对（Key-Value）组成，DDoS高防实例标签存在以下使用限制：

- **一个实例最多可以绑定20个标签。**
- **一个实例上的每个标签的标签键必须唯一，相同标签键的标签值会被覆盖。**
- **不支持未绑定实例的空标签存在，即标签必须绑定在某个DDoS高防实例上。**

添加标签

1. **在左侧导航栏，单击资产管理 > 实例管理。**
2. **在实例列表页面，定位到要操作的高防实例，单击实例信息列中的编辑标签按钮。**



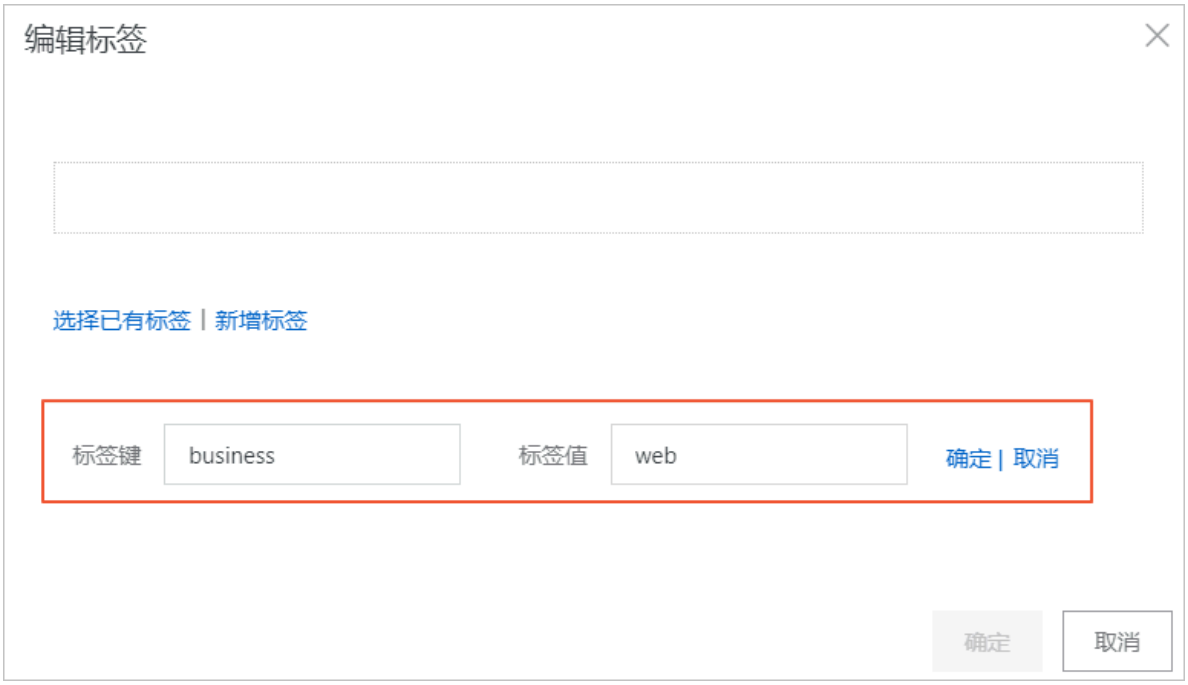
3. **在编辑标签对话框中，单击新增标签。**

> **说明:**
> **如果您已设置过标签，可以单击选择已有标签，为目标实例添加已设置的标签。**

4. **填写标签键和标签值，单击确定。**

> **说明:**

如果您选择添加已设置的标签，在列表中直接选择标签即可。

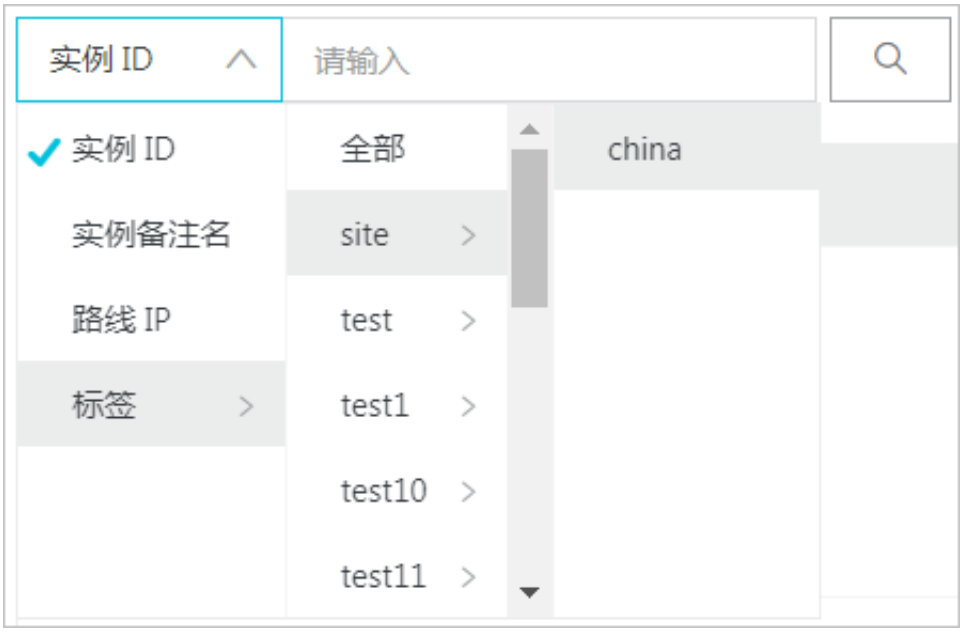


5. 单击确定，即为目标实例添加新增的标签。您可以在编辑标签对话框中为目标添加多个标签。

通过标签搜索实例

1. 在左侧导航栏，单击资产管理 > 实例管理。

2. 在实例列表页面，单击搜索项，在下拉列表中依此选择标签、标签键和标签值。

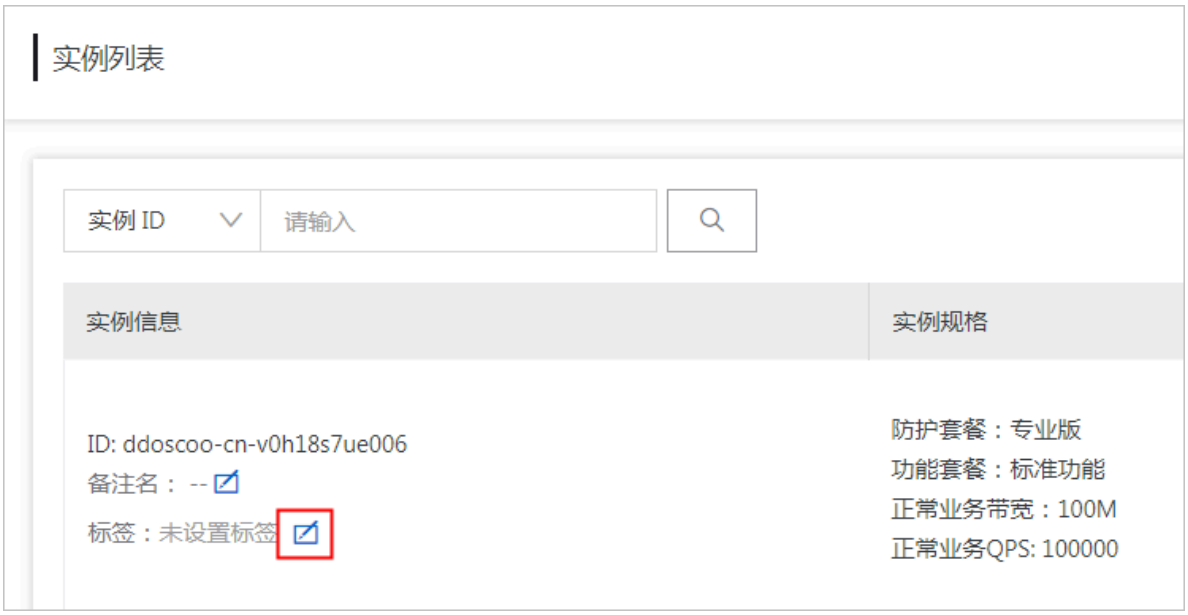


符合您选择条件的实例将显示在实例列表。

删除标签

DDoS高防不支持批量删除多个实例的标签，您只能单独对某一个实例进行标签删除操作。

1. 在左侧导航栏，单击资产管理 > 实例管理。
2. 在实例列表页面，定位到要操作的高防实例，单击实例信息列中的编辑标签按钮。



3. 在编辑标签对话框，单击要移除的标签的删除图标，然后单击确定。

> **说明:**
> 当一个标签从一个实例上移除后，如果该标签键没有和其他实例绑定，系统将自动删除该标签。

9.2 DDoS高防抗D包

DDoS高防抗D包是面向DDoS高防用户提供的一项增值服务，帮助您减少DDoS攻击峰值大于保底带宽时产生的弹性防护成本。

什么是抗D包

一般情况下，针对DDoS攻击峰值大于保底防护带宽，您可以选择使用弹性防护带宽防御攻击或者在业务遭受攻击触发黑洞策略后解除黑洞状态。

- 若使用弹性防护，您根据攻击峰值调整弹性防护值；成功防护后，基于当日成功防护的攻击峰值相对保底防护带宽的超出部分产生后付费（查看弹性防护计费方式）。这种方式带来额外的成本投入。
- 若选择不使用弹性防护（即弹性防护带宽始终等于保底防护带宽），那么当攻击流量超过保底防护带宽时，将触发黑洞；待攻击结束后，使用黑洞解除功能再恢复业务。使用这种方式，您的业务将在一定程度上受到影响，但不产生额外的弹性后付费成本投入。

DDoS高防抗D包可以在不增加额外成本投入的情况下，帮助您防护超过保底防护带宽的DDoS攻击。抗D包的主要规格参数是：防护规格和可用防护次数。以300G防护规格，可用防护3次的抗D包为例，其中，

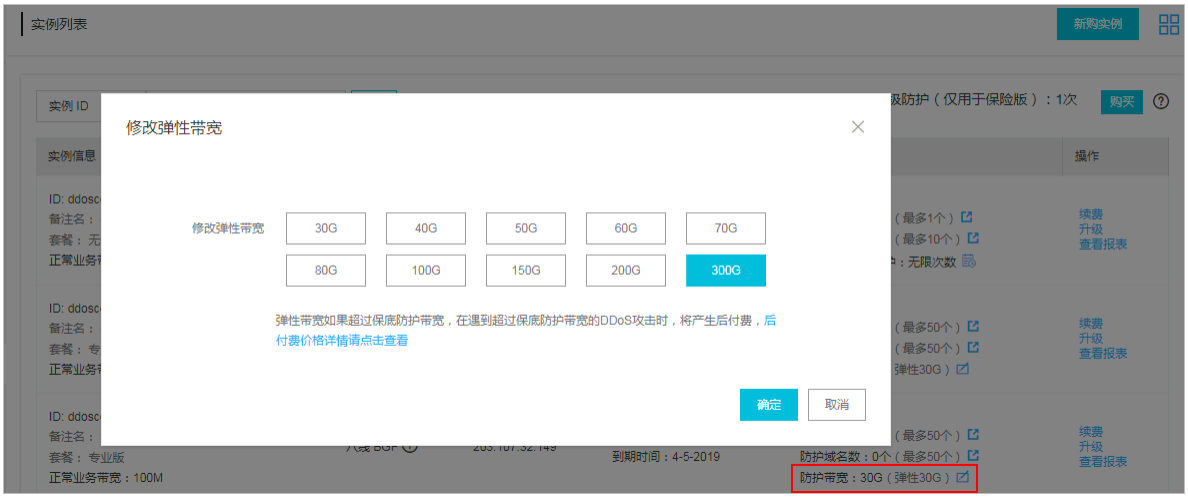
- 防护规格300G：表示该抗D包最大可抵扣保底防护带宽+300G 的攻击峰值所产生的后付费。假如攻击峰值大于保底防护值+300G，那么300G抗D包将抵扣失败；抵扣失败时，如果符合DDoS高防后付费产生条件，将会正常产生相应的后付费。
- 可用防护3次：表示该抗D包共可使用3次。无论每日遭受多少次攻击，最多只消耗一次抗D包防护次数。

使用DDoS高防抗D包时，请注意以下内容。

- 抗D包不提升防护能力，仅用于抵扣一次抗D包规格范围内的弹性后付费。您的防护能力仍取决于保底和弹性防护值。

  建议拥有抗D包的高防用户，手动调整弹性防护带宽，以便真正使用上抗D包。您可以将弹性防护带宽最大调整到“保底防护值+抗D包规格”。

  例如，保底30G，抗D包防护规格是300G，则理论上建议将弹性防护带宽调整为330G，但仍以实际弹性带宽可调范围为准。



- 只有当攻击峰值-保底防护值=<抗D包规格时，才可以通过抗D包成功抵扣弹性后付费。
- 抗D包的可用防护次数消耗到0时，为避免生成不必要的弹性后付费，建议您及时调整弹性防护带宽，使其等于保底防护值。
- 抗D包只能抵扣获取该抗D包日期之后产生的后付费（含抗D包获取当天），如果后付费已经产生账单，则无法用抗D包抵扣。

表 9-1: 新BGP抗D包和静态高防抗D包的区别

对比项目	静态高防抗D包	新BGP抗D包
使用条件	需要绑定具体高防IP才能使用。	无需绑定DDoS高防实例。应用时自动匹配剩余有效期最短的抗D包。
抵扣对象	抵扣该抗D包规格范围内攻击峰值的后付费。	抵扣攻击峰值减去保底带宽值的超出部分在该抗D包规格范围内的后付费。

如何获得抗D包

目前，DDoS高防抗D包仅以增值服务的方式向您赠送。如果您符合以下任意一种情况，可以通过客户经理、钉钉服务群或工单向我们申请，免费获得抗D包：

- **首次开通DDoS高防**
- **首次连续使用DDoS高防 3个月以上**
- **包年开通DDoS高防**

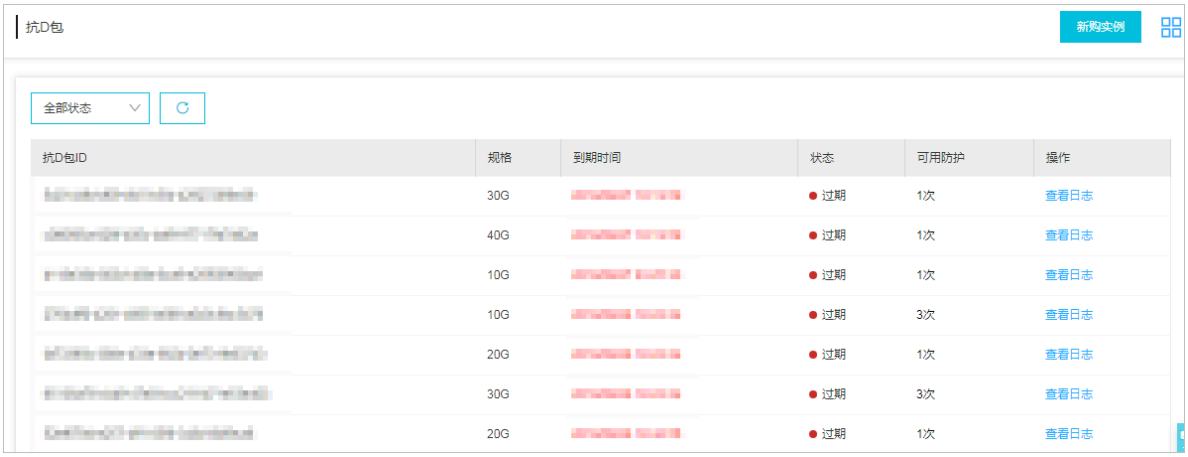
如何使用抗D包

获得DDoS高防抗D包以后，抗D包会在DDoS攻击触发其防护条件时自动被应用，您可以在DDoS高防控制台查看抗D包详情和消费记录。只有可用防护次数大于0，且未过期的抗D包才是有效的抗D包，可以正常使用。

1. 在左侧导航栏，单击资产管理 > 抗D包。

2. 在抗D包页面，查看所有抗D包详情。

   - 抗D包ID：抗D包的唯一识别标识。
   - 规格：抗D包的防护规格。
   - 到期时间：抗D包的有效日期。
   - 状态：抗D包的状态，分为有效、耗尽和过期。
   - 可用防护：抗D包的可用防护次数。



3. 单击一个抗D包下的查看日志可以查询其操作记录。

10 最佳实践

10.1 安全专家指导服务

阿里云DDoS高防产品为您免费提供一对一的专家指导咨询服务。

背景信息

如果您在使用云盾DDoS高防产品过程中遇到任何问题，可以随时通过云盾DDoS高防管理控制台的专家咨询服务入口，申请加入阿里云企业安全服务钉钉群。

届时，您在DDoS高防产品使用过程中遇到的任何问题，都将得到高防产品专家的妥善解决和处理。

操作步骤

1. 将鼠标移至有问题？找专家！图标，使用钉钉扫描显示的二维码申请加入阿里云企业安全服务钉钉群。

说明:

您可以在云盾DDoS高防管理控制台的左侧导航栏、实例列表页面等位置找到专家咨询服务入口。

2. 成功加入阿里云企业安全服务钉钉群后，安全专家将通过钉钉为您提供一对一指导服务，帮助您妥善解决DDoS高防产品使用过程中遇到的任何问题。

> 说明:
> 您也可以选择通过电话联系我的方式，留下您的联系电话，安全专家收到您的申请后将会第一时间联系您。

10.2 设置DDoS高防报警规则

本实践介绍了使用阿里云云监控配置DDoS高防报警通知的操作方法。通过设置DDoS高防报警通知，您可以及时获知高防IP上的流量和连接异常情况，并在发生故障时第一时间发现问题，缩短故障处理时间，以便尽快恢复业务。

背景信息

云监控（CloudMonitor）是一项针对阿里云资源和互联网应用进行监控的服务。云监控为您提供监控数据的报警功能。您可以通过设置报警规则来定义报警系统如何检查监控数据，并在监控数

据满足报警条件时发送报警通知。您对重要监控指标设置报警规则后，便可在第一时间得知指标数据发生的异常，迅速处理故障。

云监控报警功能兼容DDoS高防，您可以在云监控中配置DDoS高防的报警通知规则。云监控支持监控以下DDoS高防的数据指标。

说明:

高防IP回源流量指通过高防清洗后回源到源站服务器的干净业务流量。

表 10-1: DDoS高防监控指标

监控项	维度	单位
高防IP出流量	实例维度、IP维度	bit/s
高防IP入流量	实例维度、IP维度	bit/s
高防IP回源流量	实例维度、IP维度	bit/s
活跃连接数	实例维度、IP维度	个
非活跃连接数	实例维度、IP维度	个
新建连接数	实例维度、IP维度	个

操作步骤

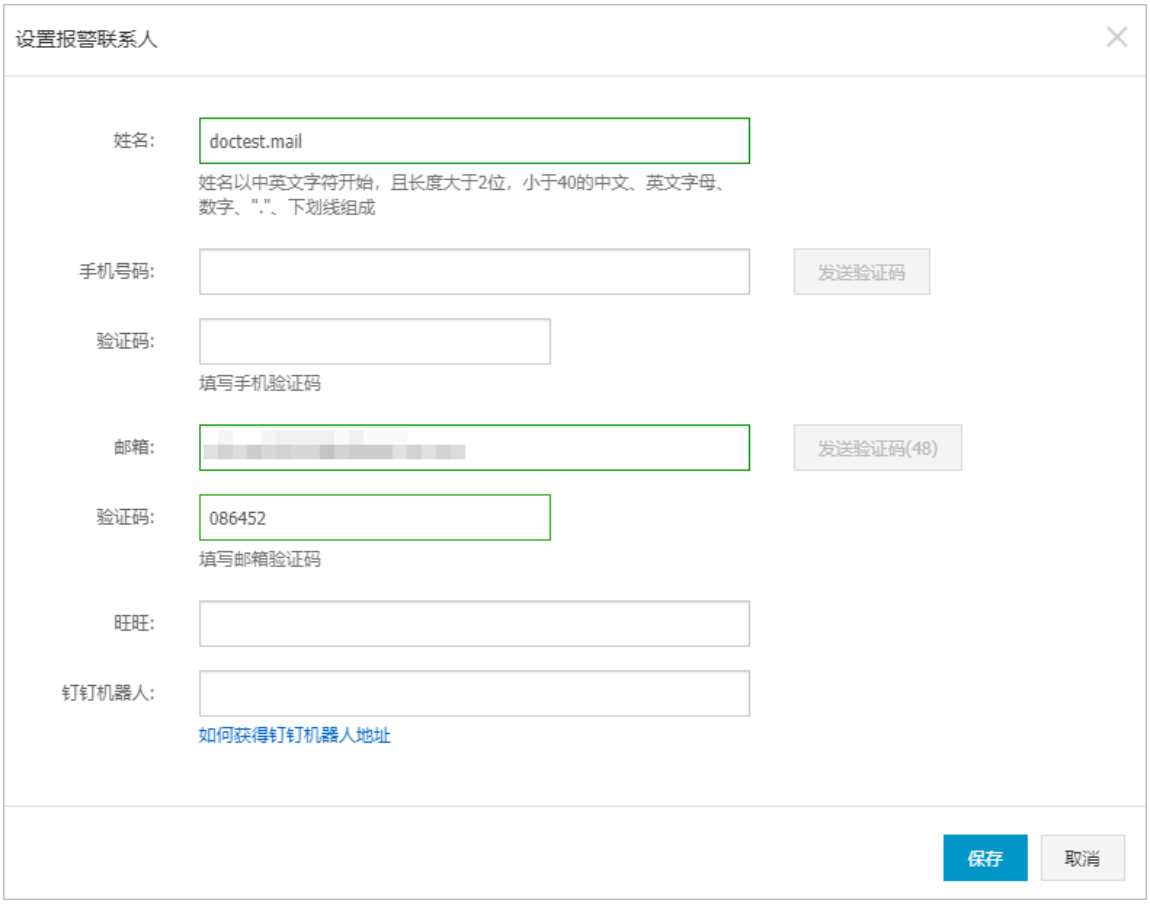
1. 登录阿里云云监控控制台。

2. （可选） 创建报警联系人。若已有联系人，请跳过此步骤。

   a) 在左侧导航栏，单击报警服务 > 报警联系人。

   b) 在报警联系人页签下，单击新建联系人。

   c) 在设置报警联系人对话框中，填写联系人信息，通过手机号码或者邮箱完成验证后，单击保存。



   成功新建报警联系人。

3. （可选） 创建报警联系组。若已有联系人组，请跳过此步骤。

   说明:

报警通知的接收对象必须是联系人组，您可以在联系人组中添加一个或多个联系人。

a) 在左侧导航栏，单击报警服务 > 报警联系人。

b) 在报警联系组页签下，单击新建联系组。

c) 在新建联系组对话框中，设置组名，从已有联系人中选择并添加联系人到当前组，单击确定。

成功新建报警联系组。

4. 创建报警规则。

a) 在左侧导航栏，单击报警服务 > 报警规则。

b) 在阈值报警页签下，单击创建报警规则。

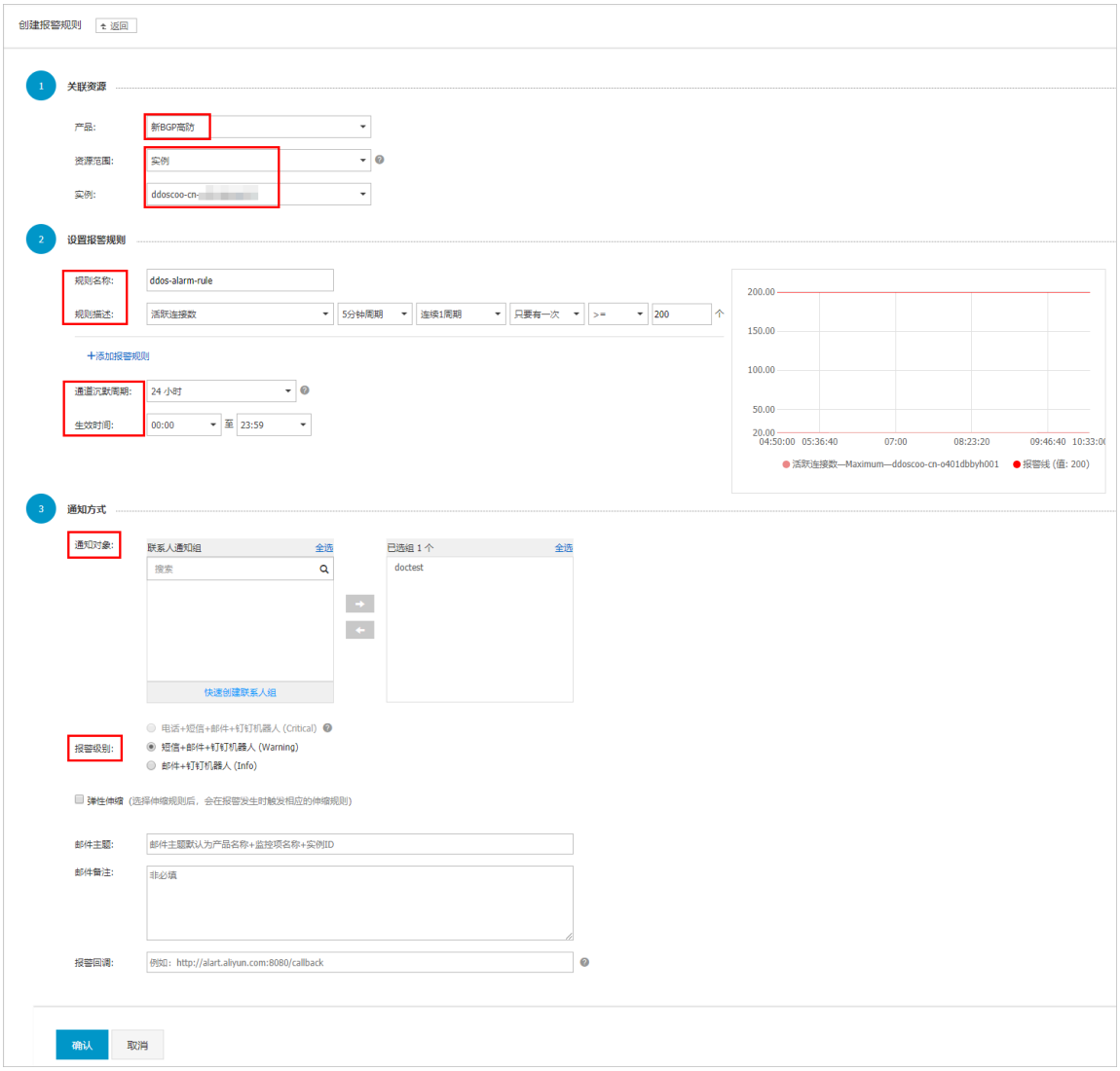
c) 在创建报警规则页面，完成报警规则配置，并单击确认。报警规则的配置描述如下。

类别	配置项	说明
关联资源	产品	选择新BGP高防。
	资源范围	报警规则的作用范围，分为全部资源、实例。 · 全部资源：资源范围选择全部资源，则所有DDoS高防实例满足报警规则描述时，都会发送报警通知。 · 实例：资源范围选择指定的实例，则选中的DDoS高防实例满足报警规则描述时，才会发送报警通知。
设置报警规则	规则名称	报警规则的名称。

类别	配置项	说明
	规则描述	报警规则的主体，定义在监控数据满足何种条件时，触发报警规则。 说明： 建议您根据实际业务情况设置各项监控指标（参见表 10-1: DDoS高防监控指标）的报警阈值。阈值太低会频繁触发报警，影响监控服务体验。阈值太高，在触发阈值后没有足够的预留时间来响应和处理攻击。 报警规则举例说明： · 新建连接数5分钟周期连续3周期只要有一次>200个， 含义是报警服务会探测任意连续3周期的新建连接数数据（单个DDoS高防监控指标60秒上报一个数据点，5分钟有5个数据点，连续3周期有15个数据点），只要有一次大于200个，结果就符合报警规则，发送报警通知。 · 高防IP出流量5分钟周期连续3周期只要有一次≥50Mbit/s，含义是报警服务会探测任意连续3周期的高防IP出流量数据（单个DDoS高防监控指标60秒上报一个数据点，5分钟有5个数据点，连续3周期有15个数据点），只要有一次大于等于50Mbit/s，结果就符合报警规则，发送报警通知。 单击添加报警规则，可以添加多个规则，每个规则单独设置规则名称和规则描述。 
	通道沉默时间	报警发生后如果未恢复正常，间隔多久重复发送一次报警通知。最短为5分钟，最长为24小时。
	生效时间	报警规则的生效时间，报警规则只在生效时间内发送报警通知，非生效时间内产生的报警只记录报警历史。
通知方式	通知对象	接收报警通知的联系人组。

类别	配置项	说明
	报警级别	分为Critical 、Warning、Info三个级别，不同级别对应不同的通知方式。 · 电话+短信+邮件+钉钉机器人（Critical） 说明: 购买云监控电话报警资源包后才可以选择。 · 短信+邮件+钉钉机器人（Warning） · 邮件+钉钉机器人（Info）
	弹性伸缩	选择弹性伸缩规则后，会在报警发生时触发相应的弹性伸缩规则。无需勾选。
	邮件备注	自定义报警邮件补充信息，非必填。填写邮件备注后，发送报警的邮件通知中会附带您的备注。

类别	配置项	说明
	报警回调	云监控会将报警信息通过POST请求推送到您填写的公网URL地址，目前仅支持HTTP协议。



成功创建DDoS高防报警规则。当DDoS高防监控指标满足报警条件时，报警规则中指定的联系人组会收到报警通知 。

10.3 设置DDoS高防黑洞和清洗事件监控

本实践介绍了使用阿里云云监控配置DDoS高防黑洞和清洗事件报警通知的操作方法。通过为DDoS高防配置事件监控，您能够及时获知高防IP上的黑洞和清洗事件，并在发生故障时第一时间发现问题，缩短故障处理时间，以便尽快恢复业务。

背景信息

云监控（CloudMonitor）是一项针对阿里云资源和互联网应用进行监控的服务。云监控支持事件监控功能，为您提供各类云产品产生的系统事件的统一查询和统计入口，使您明确知晓云产品的使用状态，让云更透明。

您可以通过事件监控查询DDoS高防上发生的黑洞和清洗事件，并为DDoS高防添加黑洞和清洗事件的报警通知。事件监控支持根据事件等级配置报警，通过短信、邮件、钉钉等接收通知或设置报警回调，使您第一时间知晓严重事件并及时进行处理，形成线上自动化运维闭环。更多信息，请参见事件监控概览。

操作步骤

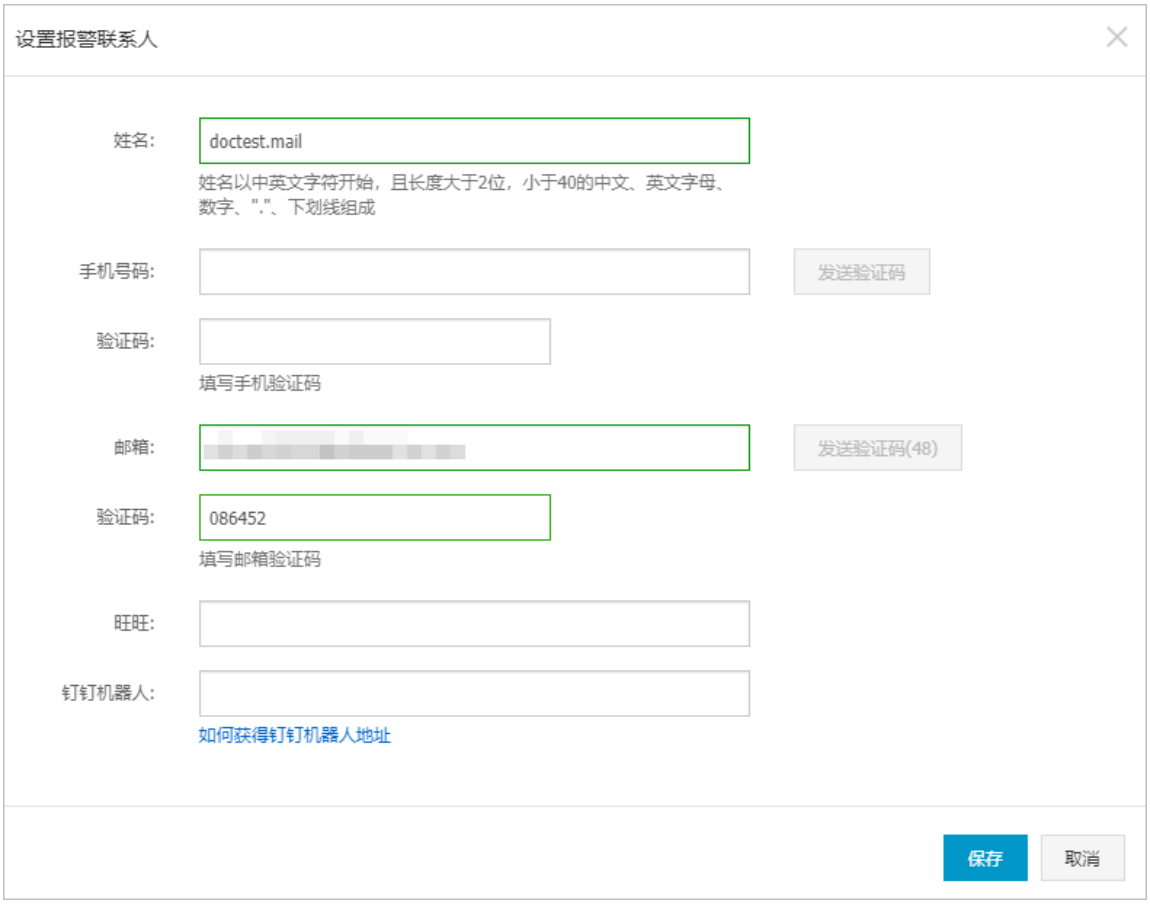
1. 登录阿里云云监控控制台。

2. （可选） 创建报警联系人。若已有联系人，请跳过此步骤。

   a) 在左侧导航栏，单击报警服务 > 报警联系人。

   b) 在报警联系人页签下，单击新建联系人。

   c) 在设置报警联系人对话框中，填写联系人信息，通过手机号码或者邮箱完成验证后，单击保存。



   成功新建报警联系人。

3. （可选） 创建报警联系组。若已有联系人组，请跳过此步骤。

   说明:

报警通知的接收对象必须是联系人组，您可以在联系人组中添加一个或多个联系人。

a) 在左侧导航栏，单击报警服务 > 报警联系人。

b) 在报警联系组页签下，单击新建联系组。

c) 在新建联系组对话框中，设置组名，从已有联系人中选择并添加联系人到当前组，单击确定。

成功新建报警联系组。

4. 创建云产品事件报警规则。

a) 在左侧导航栏，单击事件监控。

b) 在报警规则页签下，选择系统事件，并单击创建事件报警。

c) 在创建/修改事件报警侧边页，完成报警配置，并单击确定。报警配置的描述如下。

类型	配置项	说明
基本信息	报警规则名称	为报警规则命名。
事件报警规则	事件类型	选择系统事件。
	产品类型	选择新BGP高防。
	事件类型	选择要通知的事件类型，支持ddos黑洞和ddos清洗。可以多选。
	事件等级	选择要通知的事件等级，支持严重、警告、信息。可以多选，且必须包含严重等级。
	事件名称	选择要通知的事件，可以多选。 · DDoS黑洞类型事件包括黑洞进行中和黑洞解除，事件等级均为严重。 · DDoS清洗类型事件包括清洗进行中、清洗解除，事件等级均为严重。
	资源范围	选择全部资源。
报警方式	报警通知	勾选报警通知，并设置联系人组和通知方式。 · 联系人组：选择一个已有联系人组。 · 通知方式：选择Warning（短息+邮箱+钉钉机器人）或者Info（邮箱+钉钉机器人）方式。 若单击添加操作，可以设置多个联系人组和通知方式。
	消息服务队列	无需勾选。
	函数计算	无需勾选。
	URL回调	无需勾选。

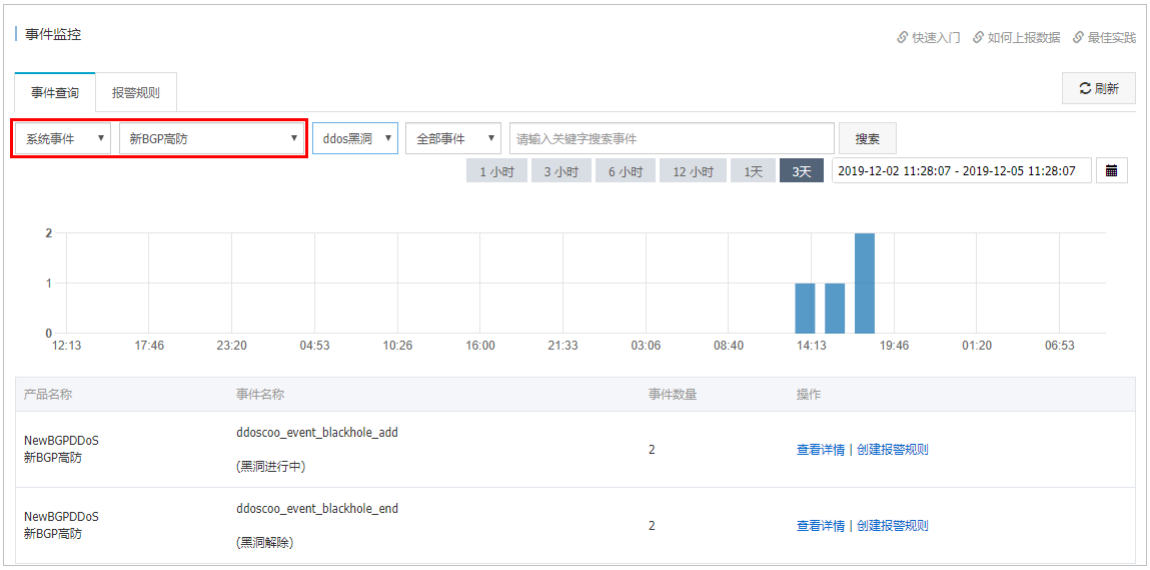
类型	配置项	说明
	日志服务	无需勾选。

成功创建DDoS高防事件监控报警规则。当DDoS高防IP上发生黑洞或者清洗事件时，报警规则中指定的联系人组会收到报警通知 。

5. （可选） 查询事件。您也可以在云监控查询近期发生的DDoS高防黑洞和清洗事件。

   a) 前往事件监控页面，并打开事件查询页签。

   b) 选择系统事件和新BGP高防产品，并设置要查询的事件类型和时间范围，查询相关历史事件。



   c) 在历史事件记录中，您可以单击事件后的查看详情，展开事件详情。

10.4 创建DDoS高防监控大盘

本实践介绍了使用阿里云云监控创建和自定义DDoS高防（新BGP）实时监控大盘和数据图表的操作方法。自定义DDoS高防监控大盘和数据图表能够帮助您直观、全面地了解DDoS高防的业务防护情况。

背景信息

云监控（CloudMonitor） 是一项针对阿里云资源和互联网应用进行监控的服务。云监控的Dashboard功能为您提供自定义查看监控数据的功能。您可以在一张监控大盘中跨产品、跨实例查看监控数据，将相同业务的不同产品实例集中展现。

云监控Dashboard功能兼容DDoS高防，您可以在云监控中配置DDoS高防监控大盘。云监控支持监控以下DDoS高防的数据指标。

说明:
高防IP回源流量指通过高防清洗后回源到源站服务器的干净业务流量。

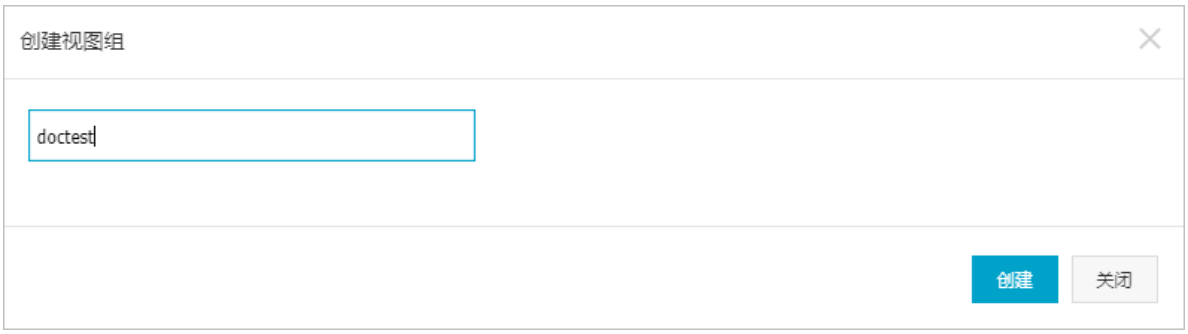
表 10-2: DDoS高防监控指标

监控项	维度	单位
高防IP出流量	实例维度、IP维度	bit/s
高防IP入流量	实例维度、IP维度	bit/s
高防IP回源流量	实例维度、IP维度	bit/s
活跃连接数	实例维度、IP维度	个
非活跃连接数	实例维度、IP维度	个
新建连接数	实例维度、IP维度	个

操作步骤

1. 登录阿里云云监控控制台。
2. 前往Dashboard > 自定义大盘页面，单击创建监控大盘。

3. 在创建视图组对话框中设置大盘名称，单击创建。

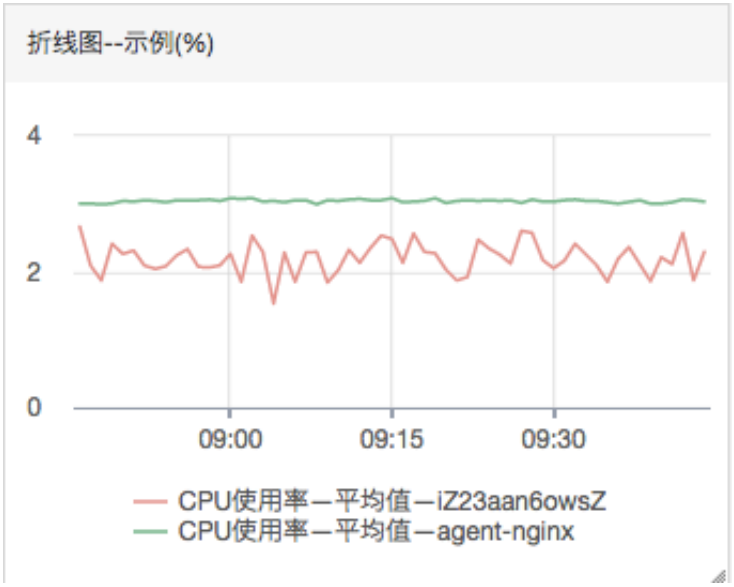


成功添加监控大盘，页面跳转到新建的监控大盘。您可以通过当前监控大盘选项切换要查看或操作的监控大盘。

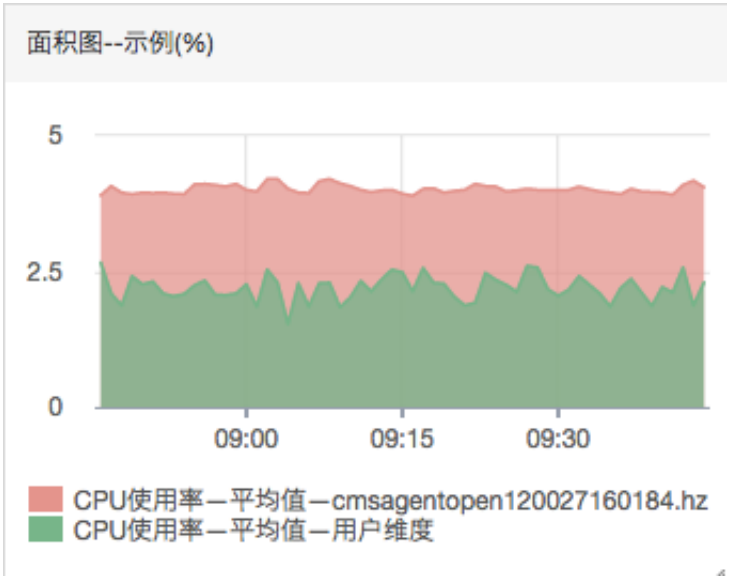
4. 进入监控大盘，单击添加图表，并在添加图表侧边页中自定义图表内容。

a) 选择图表类型。支持的类型包括折线图、面积图、TopN表格、热力图、饼图。

- 折线图：按时间序列展示监控数据，可以添加多个监控项。



- 面积图：按时间序列显示监控数据，可以添加多个监控项。

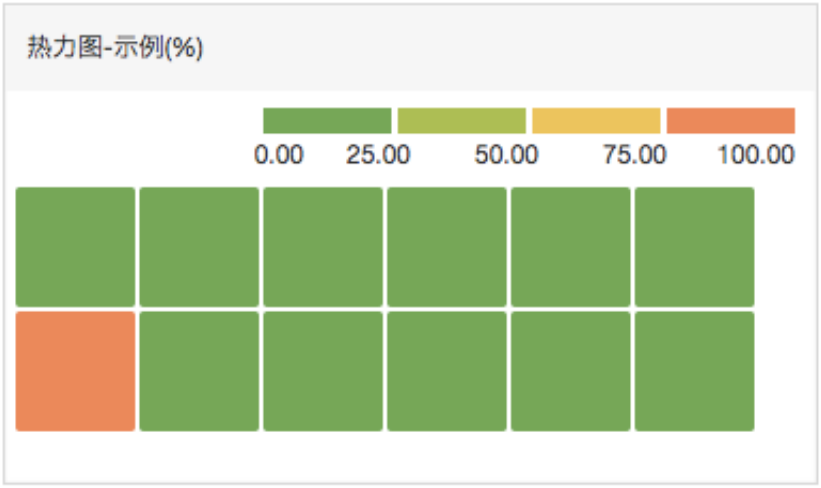


- TopN表格：显示最近三小时内最后时刻监控数据的排序，最多显示正序的1000条或倒序的1000条数据。例如ECS分组中所有机器CPU使用率从大到小的排序。只能添加一个监控项。

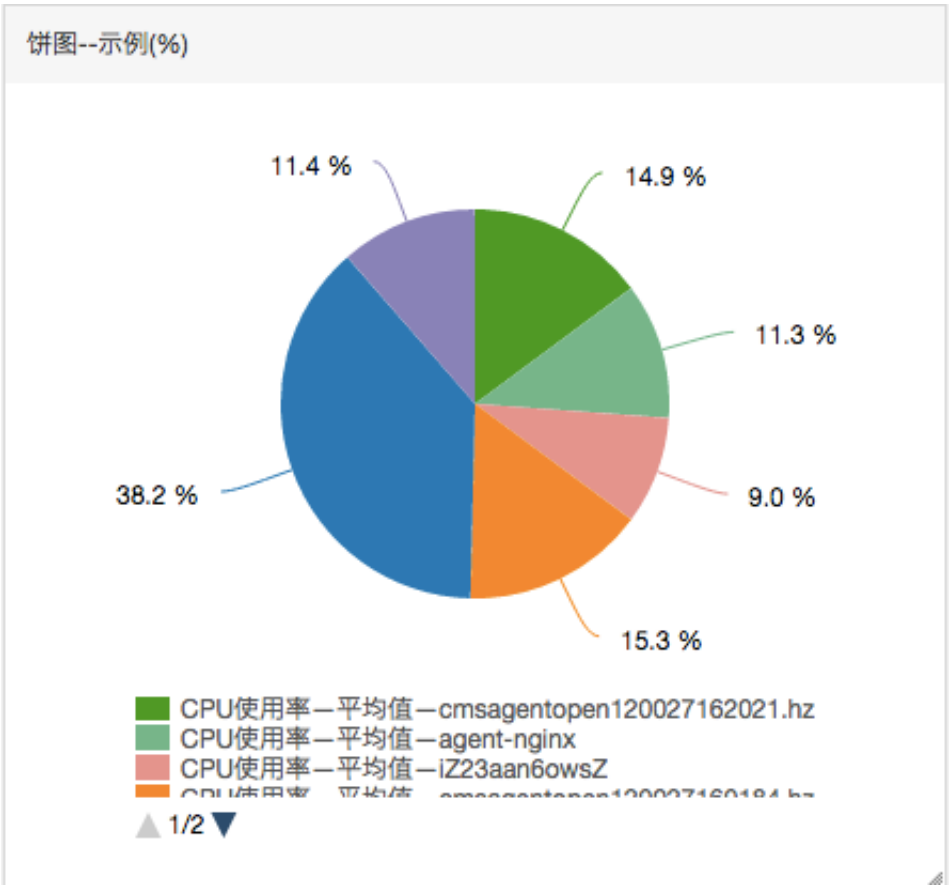
表格--示例(%)

时间	实例	平均值
2016-07-05 09:47:00	.hz	10.31
2016-07-05 09:47:00	.hz	4.47
2016-07-05 09:47:00	.hz	4.44
2016-07-05 09:47:00	.hz	4.15
2016-07-05 09:47:00	.hz	4.14
2016-07-05 09:47:00	.hz	4.1

- **热力图：显示监控项的实时数据，用于展示多个实例指定监控项的实时监控数据分布与对比。例如展示多个实例CPU使用率的水位分布情况。只能添加一个监控项。**

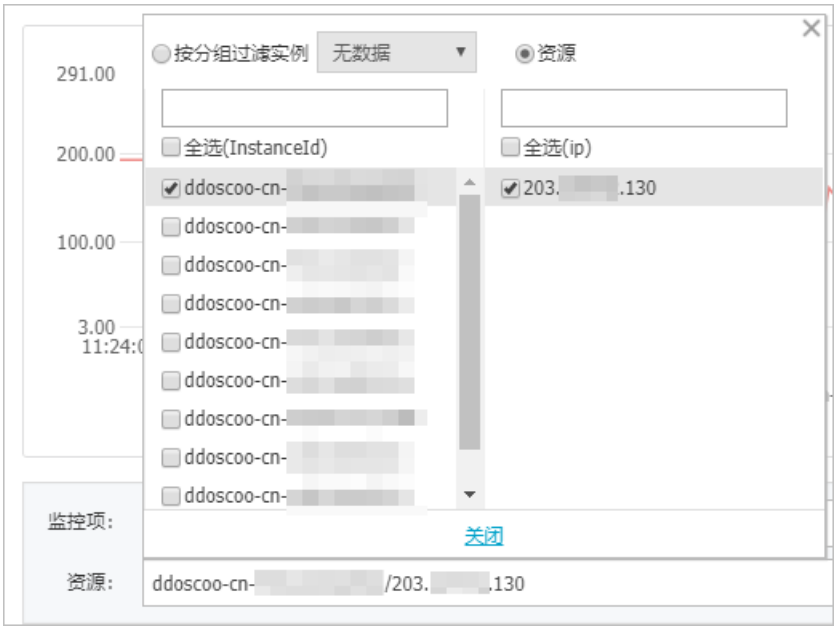


- **饼图：显示监控项的实时数据，常用于数据的对比。只能添加一个监控项。**



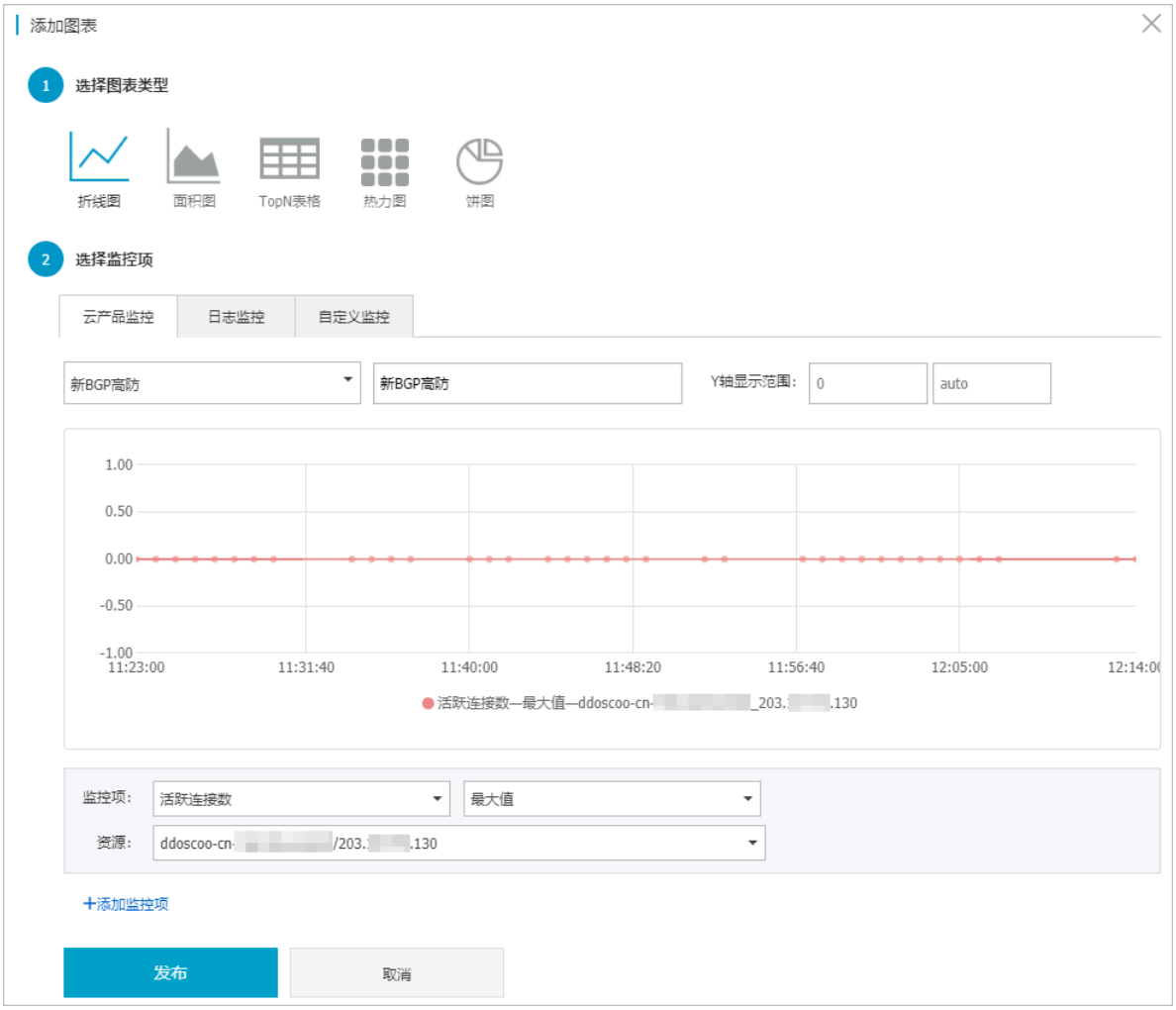
b) 选择监控项。选择云产品监控，并设置产品为新BGP高防，进一步配置监控项和资源。

- **监控项：选择要监控的DDoS高防数据指标（参见*DDoS*高防监控指标）。**
- **资源：选择要监控的DDoS高防实例和IP。**

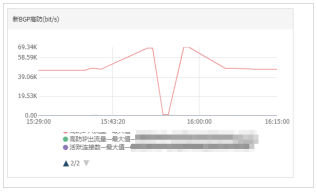


单击添加监控项可以在当前图表中定义多个监控项。

c) 单击发布，生成监控图表。



成功生成DDoS高防监控图表。



5. **您可以重复步骤4，在当前监控大盘下继续添加图表。更多信息，请参见*#unique_101*、*#unique_102*。**

10.5 从高防IP迁移至新BGP高防IP

背景信息

距离阿里云静态高防IP服务机房上线已经过了三年时间，随着用户业务对链路稳定性要求的提升，这三年间我们一直致力于改善我们的高防IP产品。

在此，我们很高兴地通知您，阿里云目前已可以为您提供支持八线BGP网络的高防IP服务——*新BGP高防IP*。

新BGP高防IP重构了底层网络，新BGP高防IP服务的网络架构与阿里云BGP线路机房互通，彻底解决以往单线电信、单线联通网络中存在的跨网访问质量问题，实现全国各地与新BGP高防IP的平均延迟在20ms以内。同时，在新BGP高防IP架构中，每个运营商遭受的攻击流量都将在对应运营商的网内解决，使得新BGP高防IP服务在网络层灾备和攻击防护能力方面都有质的提升。

新BGP高防IP规格说明

- 基础防护能力：最低支持30G保底防护带宽（月单价20,800元起）
- 弹性防护能力：与您当前高防IP实例的弹性防护带宽一致，最高支持600G弹性防护带宽（超过600G以上的防护能力需求可联系我们定制）

迁移至新BGP高防IP

为了让您能享受新BGP高防IP稳定、快速、安全的服务，现诚邀您将在用的静态机房的高防业务迁移至新BGP高防IP，立即体验稳定和快速的新BGP高防IP服务。

您可以在现有高防服务到期前，购买新BGP高防IP服务，将原静态机房的高防业务平滑地迁移至新BGP高防IP服务。

> 说明:
> 建议您在获得新BGP高防IP实例后尽快完成新BGP高防IP实例的配置。迁移过程中，您的待迁移高防IP实例将与新BGP高防IP实例共存，且都可以正常转发业务流量。

开始之前

> 注意:
> 强烈建议您在正式开始迁移前参考业务配置批量导入导出，在云盾DDoS高防IP管理控制台中使用域名配置/转发规则批量导出功能，将当前的网站和非网站业务接入配置导出备份。在您将域名配置迁移至新BGP高防IP实例后，原高防IP实例中将无法查看到原有域名配置信息。

1. 登录云盾DDoS高防IP管理控制台。

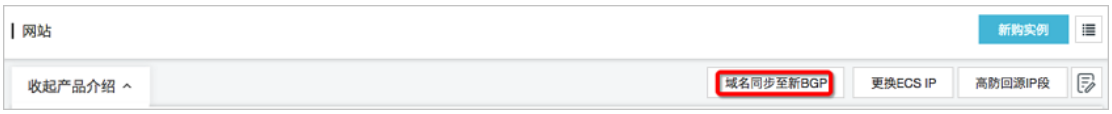
2. 将业务配置迁移至新BGP高防IP实例。

- 网站域名配置迁移

  域名配置迁移前注意事项：

  - 请勿在新BGP高防IP实例中添加80或443的端口转发配置。因为新BGP高防IP的域名配置默认占用80或443端口进行转发，如果在新BGP高防IP实例中已添加80或443端口配置，将导致所迁移的域名配置无法正常关联新BGP高防IP实例。
  - 如果您之前通过提交工单在后台开通HTTP2或HTTPS强制转HTTP回源的功能，请务必在域名同步前关闭这些功能。
  - 当所迁移的域名与其它账号的泛域名配置存在冲突时，将导致所迁移的域名配置无法正常关联新BGP高防IP实例。如果您拥有多个阿里云账号，请注意检查是否存在此类冲突。

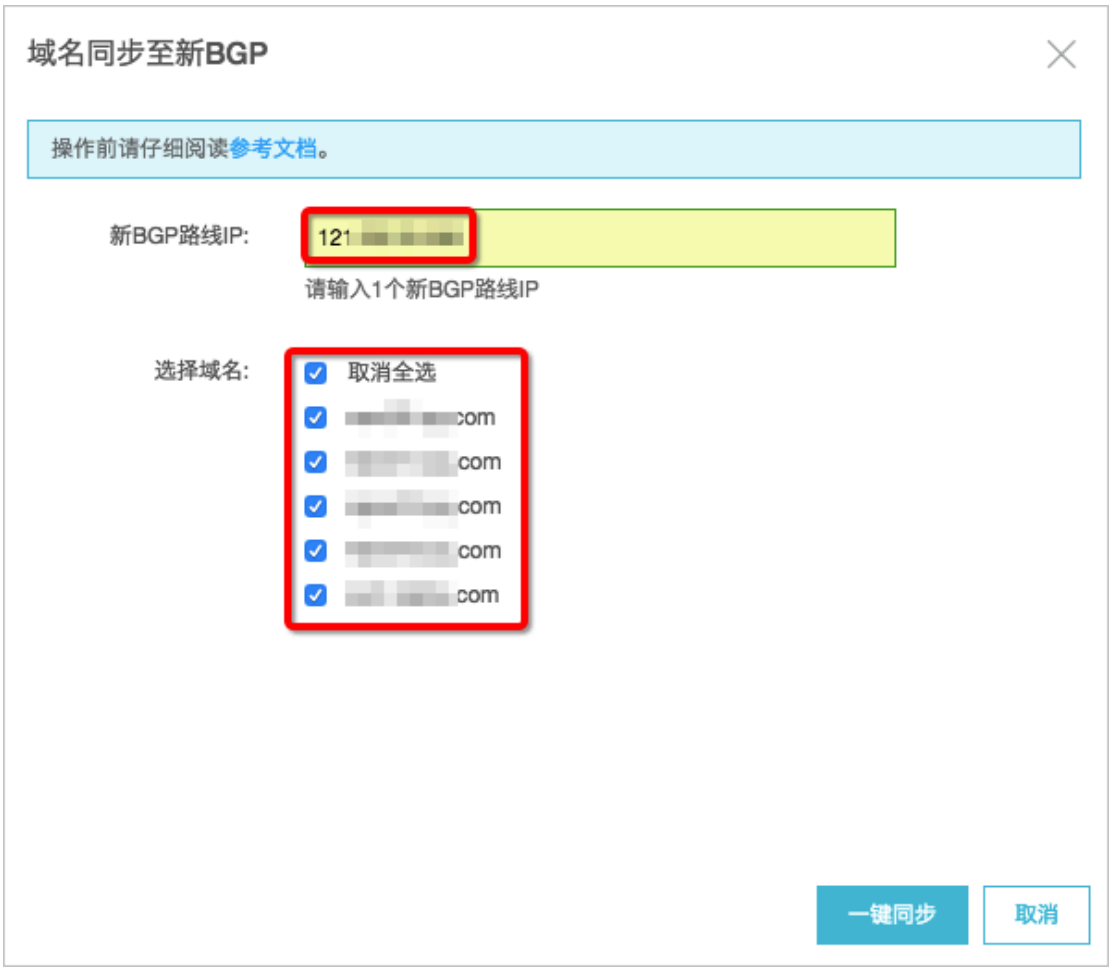
  a. 定位到接入 > 网站，单击域名同步至新BGP。

  b. 输入阿里云为您创建的新BGP高防IP实例的IP，选择所需迁移的域名配置。

  说明：

一次最多支持选择五个域名。如果原高防IP实例中包含超过五个需要迁移的域名配置，请分多次进行域名同步。



c. **单击一键同步，并确认，将所选择的域名配置迁移至新BGP高防IP实例。您可以在新BGP高防IP管理控制台的管理 > 网站配置页面中查看已迁移的域名配置信息。**

说明：

此时，您的网站业务流量依然由原高防IP实例转发，对您的业务防护不会产生任何影响。

域名同步操作注意事项：

- **如果所需迁移的域名配置仅关联一个高防IP实例，您只需按上述步骤将所有域名配置同步至新BGP高防IP即可。**
- **如果您拥有多个高防IP实例，且部分域名关联多个高防IP实例，则必须先明确所需迁移的域名及这些域名当前已关联的高防IP实例情况。如果其中存在部分高防IP实例**

将继续使用且短期内不会释放，建议您先将所需迁移的域名与这些高防IP实例解除关联，再按上述步骤进行迁移。

> **注意:**
> 域名同步完成后，您在云盾DDoS高防IP管理控制台中将无法看到已迁移的域名配置，但实际上这些域名与原高防IP实例的关联关系依然存在且生效，而原高防IP实例中显示的已关联域名数量不会变化。您可以在新BGP高防IP管理控制台的管理 > 网站配置页面中查看已迁移的域名配置信息。因此，为了避免在云盾DDoS高防IP管理控制台中对已迁移的域名配置进行错误变更，因此在云盾DDoS高防IP管理控制台中隐藏这些域名配置记录。

d. 域名同步完成后，建议您将在新BGP高防IP管理控制台的管理 > 网站配置页面中查看到的已迁移的域名配置与迁移前导出的域名配置信息进行比对。如果发现迁移后的配置存在差异，您需要在新BGP高防IP管理控制台中按照原配置信息手动更改域名配置。

域名配置迁移后注意事项：

- 新BGP高防IP使用的回源网段与高防IP不同，如果您的源站对访问IP存在限制，请在管理 > 网站配置页面中单击查看BGP高防的回源地址，并将所有网段地址添加至源站访问控制策略的白名单中。
- 如果您的域名尚未通过阿里云备案，您可以通过工单或钉钉服务群联系我们申请暂时放行。强烈建议您尽快为该域名完成阿里云备案。

· 非网站业务配置迁移

a. 定位到接入 > 非网站，选择所需迁移的高防IP实例和高防IP。

b. 单击导出规则/配置，选择导出规则。

c. 在新BGP高防IP管理控制台的管理 > 端口配置页面，选择实例，单击批量操作，选择添加规则。

d. 将从原高防IP实例中导出的规则配置信息粘贴至文本框中，单击添加，即可将端口转发规则配置迁移至新BGP高防IP实例。

> **说明:**
> 关于配置的批量导入导出的具体操作，参考业务配置批量导入导出。同时，在完成端口配置迁移后，您也可以通过该方式将原高防IP实例中非网站业务的会话保持/健康检查配置或DDoS防护策略配置迁移至新BGP高防IP。

3. 参考本地验证配置通过本地修改Host文件的方式绑定新BGP高防IP实例的IP，逐条检查网站和非网站配置是否生效。

4. 验证通过后，前往您域名对应的DNS服务商提供的域名解析管理页面，修改域名DNS解析设置，通过A记录的方式，将域名解析指向新BGP高防IP实例。

   说明:

   如果您的非网站业务未使用域名进行连接，将您业务IP替换为所配置的新BGP高防IP实例的IP，即可正式将业务流量切换至新BGP高防IP实例。

5. 在您确认所有业务均已迁移至新BGP高防IP实例后，如果您的原高防IP实例仍在服务期内，您可以通过工单申请退回原高防IP实例的余款。

   说明:

   原高防IP实例与新BGP高防IP实例共存期间，您无法在新BGP高防IP管理控制台中删除所迁移的网站域名配置。只有在该域名所关联的原高防IP实例释放后，才可删除该域名配置。

其它注意事项

- 整个业务配置迁移同步过程中将不会对您的业务造成任何影响。如果您需要回滚业务配置，请通过工单或钉钉服务群的方式联系我们进行操作。
- 在原高防IP实例与新BGP高防IP实例共存期间和迁移过程中，为避免产生不必要的弹性后付费，建议您将原高防IP实例的弹性防护带宽设置为与保底防护带宽一致。

常见问题

新BGP高防IP产品有哪些优势?

关于新BGP高防IP的优势，请查看什么是新BGP高防IP。

新BGP高防IP产品的价格明细?

关于新BGP高防IP产品的产品定价，请查看新BGP高防IP计费方式。

新BGP高防IP产品的链路质量如何?

您可以通过以下第三方测试工具测试新BGP高防IP产品的线路延迟情况：http://ping.chinaz.com/203.107.32.57

测试IP：203.107.32.57

业务迁移至新BGP高防IP大约需要多久?

- 网站类业务：通常由于DNS刷新等原因，需要1-3天左右完成。
- IP类业务：需要根据您的业务实际情况进行评估。

业务迁移会导致业务中断吗?

一般情况下，迁移至新BGP高防IP实例的过程中不会对您的业务产生影响，但具体情况仍需要您根据实际业务进行评估。阿里云保证您的新BGP高防IP实例与原有高防IP实例将共存一段时间，当您将全部业务流量都迁移至新BGP高防IP实例后，阿里云将再次确认业务流量已经全部迁移完成后，才会释放原有的高防IP实例。

整个迁移过程中，阿里云都将以保障您的业务访问作为第一优先级。

迁移至新BGP高防IP还有哪些注意事项?

- 新BGP高防IP实例使用的是BGP线路的IP，天然具备故障发生时的自动切换线路能力（且相比通过DNS解析切换更快、更稳定）。因此，新BGP高防IP服务不支持通过CNAME方式接入，您需要以A记录的方式接入新BGP高防IP实例。
- 新BGP高防IP实例的回源IP段信息与原高防IP实例不同。如果您在高防IP实例后端配置了回源IP地址限制等策略，您需要手动更新回源IP段信息。

11 API 参考

11.1 API概览

本文档汇总了BGP高防IP所有可调用的API，具体接口信息请参阅相关文档。

关于更多API资源，请访问*API Explorer*。

实例

API	描述
DescribeInstances	查询实例列表。
DescribeInstanceDetails	查询实例详情列表。
DescribeInstanceSpecs	查询实例规格列表。
DescribeInstanceStatistics	查询实例统计信息。
DescribeElasticBandwidthSpec	查询弹性带宽规格。
ModifyElasticBandWidth	修改弹性防护带宽。
ModifyInstanceRemark	修改实例备注信息。

4层规则

API	描述
CreateLayer4Rule	创建4层转发规则。
ConfigLayer4Rule	编辑4层转发规则。
DeleteLayer4Rule	删除4层转发规则。
ConfigLayer4RuleAttribute	配置4层转发规则属性（会话保持和DDoS防护策略）。
ConfigHealthCheck	配置4层/7层健康检查。
DescribeLayer4Rules	查询四层转发规则列表。
DescribeLayer4RuleAttributes	查询四层转发属性列表（会话保持和DDoS防护策略）。
DescribeHealthCheckList	查询4层/7层健康检查列表。
DescribeHealthCheckStatusList	查询健康检查状态。

7层规则

API	描述
DescribeDomains	查询7层转发规则。
CreateLayer7Rule	创建7层转发规则。
ConfigLayer7Rule	编辑7层转发规则。
DeleteLayer7Rule	删除7层转发规则。
ConfigLayer7Cert	设置证书。
ConfigLayer7BlackWhiteList	设置7层防护黑白名单。
DescribleLayer7InstanceRelations	查询7层防护实例对应关系。
DescribleCertList	查询证书列表。
EnableLayer7CC	启用7层CC防护。
DisableLayer7CC	禁用7层CC防护。
EnableLayer7CCRule	启用7层CC规则。
DisableLayer7CCRule	禁用7层CC规则。
AddLayer7CCRule	添加7层CC规则。
ConfigLayer7CCRule	编辑7层CC规则。
DescribeLayer7CCRules	查询7层CC规则。
DeleteLayer7CCRule	删除7层CC规则。
ConfigLayer7CCTemplate	设置7层CC防护模板。
DescribeDomainAccessMode	查询域名接入模式。
ConfigDomainAccessMode	设置域名接入模式。
DescribeBackSourceCidr	查询回源网段。

事件任务

API	描述
ListAsyncTask	查询异步任务列表。
CreateAsyncTask	创建异步任务。
DeleteAsyncTask	删除异步任务。

日志

API	描述
DescribeOpEntities	查询操作日志。

11.2 调用方式

BGP高防IP接口调用是向BGP高防IP的API的服务端地址发送HTTP GET请求，并按照接口说明在请求中加入相应请求参数，调用后系统会返回处理结果。请求及返回结果都使用UTF-8字符集进行编码。

请求结构

BGP高防IP的API是RPC风格，您可以通过发送HTTP GET请求调用BGP高防IP API。

其请求结构如下：

```
https://Endpoint/?Action=xx&Parameters
```

其中：

- `Endpoint`：**BGP高防IP API的服务接入地址为**`ddoscoo.cn-hangzhou.aliyuncs.com`。
- `Action`：**要执行的操作，如使用**`DescribeInstances`**，查询所有实例列表。**
- `Version`：**要使用的API版本，BGP高防IP的API版本是**`2017-12-28`。
- `Parameters`：**请求参数，每个参数之间用“&”分隔。**
- **请求参数由公共请求参数和API自定义参数组成。公共参数中包含API版本号、身份验证等信息，详情参见公共参数。**

下面是一个调用DescribeInstances接口查询所有BGP高防IP实例列表的示例：

说明：

为了便于您查看，本文档中的示例都做了格式化处理。

```
https://ddoscoo.cn-hangzhou.aliyuncs.com/?Action=DescribeInstances
&Region=cn
&InstanceId=ddoscoo-cn-XXXX1
&Format=xml
&Version=2017-12-28
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2012-06-01T12:00:00Z
```

```
...
```

API授权

为了确保您的账号安全，建议您使用子账号的身份凭证调用API。如果您使用RAM账号调用BGP高防IP API，您需要为该RAM账号创建、附加相应的授权策略。

API签名

BGP高防IP服务会对每个API请求进行身份验证，无论使用HTTP还是HTTPS协议提交请求，都需要在请求中包含签名（Signature）信息。

BGP高防IP通过使用AccessKey ID和AccessKey Secret进行对称加密的方法来验证请求的发送者身份。AccessKey是为阿里云账号和RAM用户发布的一种身份凭证（类似于用户的登录密码），其中AccessKey ID用于标识访问者的身份，AccessKey Secret是用于加密签名字符串和服务器端验证签名字符串的密钥，必须严格保密。

RPC API需按如下格式在请求中增加签名（Signature）：

```
https://endpoint/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&
Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D&SignatureNonce=3ee8c1b8-83d3-
44af-a94f-4e0ad82fd6cf
```

以DescribeInstances为例，假设AccessKey ID是 testid， AccessKey Secret是 testsecret，则签名前的请求URL如下：

```
https://ddoscoo.cn-hangzhou.aliyuncs.com/?Action=DescribeInstances
&Region=cn
&InstanceId=ddoscoo-cn-XXXX1
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2017-12-28
&SignatureVersion=1.0
```

完成以下步骤计算签名：

1. 使用请求参数创建待签名字符串：

```
GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeDomainNames&Region
%3Dcn&InstanceId%3Dwaf_elasticity-cn-0xldbqtm005&Format%3DXML&
SignatureMethod%3DHMAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-
```

```
a94f-4e0ad82fd6cf&SignatureVersion%3D1.0&TimeStamp%3D2016-02-23T12%
253A46%253A24Z&Version%3D2018-01-17
```

2. **计算待签名的HMAC的值。**

   在AccessKey Secret后添加一个“&”作为计算HMAC值的key。本示例中的key为 `testsecret&`。

```
CT9X0VtwR86fNWSnsc6v8YGOjuE=
```

3. **将签名加到请求参数中：**

```
https://ddoscoo.cn-hangzhou.aliyuncs.com/?Action=DescribeInstances
&Region=cn
&InstanceId=ddoscoo-cn-XXXX1
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2017-12-28
&SignatureVersion=1.0
&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D
```

11.3 公共参数

介绍调用新BGP高防IP API时要用到的公共参数。

公共请求参数

公共请求参数是每个接口都需要使用到的请求参数。

名称	类型	是否必需	描述
Region	String	是	BGP高防IP实例所在的地域。取值：cn-hangzhou（表示中国大陆地区）。
Format	String	否	返回消息的格式。取值： · JSON（默认） · XML
Version	String	是	API版本号，使用YYYY-MM-DD日期格式。取值：2017-12-28。
AccessKeyId	String	是	访问服务使用的密钥ID。
Signature	String	是	签名结果串。
SignatureMethod	String	是	签名方式，取值：HMAC-SHA1。

名称	类型	是否必需	描述
Timestamp	String	是	请求的时间戳，为日期格式。使用UTC时间按照ISO8601标，格式为YYYY-MM-DDThh:mm:ssZ。例如，北京时间2013年1月10日20点0分0秒，表示为2013-01-10T12:00:00Z。
SignatureVersion	String	是	签名算法版本，取值：1。
SignatureNonce	String	是	唯一随机数，用于防止网络重放攻击。在不同请求间要使用不同的随机数值。
ResourceOwnerAccount	String	否	本次API请求访问到的资源拥有者账户，即登录用户名。

示例

```
https://ddoscoo.cn-hangzhou.aliyuncs.com/?Action=DescribeInstances
&Region=cn
&InstanceId=ddoscoo-cn-XXXX1
&Timestamp=2014-05-19T10%3A33%3A56Z
&Format=xml
&AccessKeyId=testid
&SignatureMethod=Hmac-SHA1
&SignatureNonce=NwDAxvLU6tFE0DVb
&Version=2017-12-28
&SignatureVersion=1.0
&Signature=Signature
```

公共返回参数

API返回结果采用统一格式，返回2xx HTTP状态码代表调用成功；返回4xx或5xx HTTP状态码代表调用失败。调用成功返回的数据格式有XML和JSON两种，可以在发送请求时指定返回的数据格式，默认为XML格式。

每次接口调用，无论成功与否，系统都会返回一个唯一识别码 RequestId。

- **XML格式**

```
<?xml version="1.0" encoding="utf-8"?>
    <!--结果的根结点-->
    <接口名称+Response>
        <!--返回请求标签-->
        <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
        <!--返回结果数据-->
    </接口名称+Response>
```

- **JSON格式**

```
{
    "RequestId":"4C467B38-3910-447D-87BC-AC049166F216",
    /*返回结果数据*/
```

```
    }
```

11.4 实例

11.4.1 DescribeInstances

调用DescribeInstances分页查询新BGP高防实例信息列表。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstances	要执行的操作。取值：DescribeInstances。
PageNo	String	是	1	分页页号，即从几页开始显示。最小值是1。
PageSize	String	是	10	分页大小，即每页显示多少条结果。最大值是50。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
RegionId	String	否	xx	地域ID。
ResourceGroupId	String	否	xx	资源组ID。
InstanceIds	String	否	["ddoscoo-cn-XXXXX"]	通过实例Id查询实例信息，传入要查询的实例Id数组（JSON字符串）。支持精确匹配。例如，["ddoscoo-cn-XXXX1", "ddoscoo-cn-XXXX2"]。 **说明:** 若传入该参数，则无需传入Ip和Remark。

名称	类型	是否必选	示例值	描述
Ip	String	否	1.1.1.1	通过实例IP查询实例信息，传入要查询的实例IP地址。支持精确匹配查询。  说明: 若传入该参数，则无需传入InstanceIds和Remark。
Remark	String	否	testRemark	通过实例备注查询实例信息，传入要查询的实例的备注信息。支持模糊查询。  说明: 若传入该参数，则无需传入InstanceIds和Ip。
Edition	Integer	否	9	防护套餐版本，取值：9（专业版）。
Enabled	Integer	否	1	实例工作状态，取值： · 1：正常转发业务 · 0：已停止业务转发
Status.N	RepeatLis	否	1	实例售卖状态，取值： · 1：正常 · 2：过期 · 3：释放
Tag.N.Key	String	否	key	实例标签的标签键。N的取值范围：1~20。一旦传入该值，则不允许为空字符串。最多支持128个字符，不能以aliyun和acs:开头，且不能包含 http:// 或者 https:// 。  说明: 标签键（Tag.N.Key）与标签值（Tag.N.Value）必须键值匹配。

名称	类型	是否必选	示例值	描述
Tag.N.Value	String	否	value	实例标签的标签值。N的取值范围：1~20。一旦传入该值，可以为空字符串。最多支持128个字符，不能以aliyun和acs:开头，且不能包含 http:// 或者 https:// 。  说明: 标签键（Tag.N.Key）与标签值（Tag.N.Value）必须键值匹配。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
Total	Long	10	实例总数。
Instances	Array		实例信息列表。
InstanceId	String	ddoscoo-cn-XXXXX	实例ID。
Remark	String	testRemark	实例备注信息。最大500字节。
Status	Integer	1	实例售卖状态，取值： · 1：正常 · 2：过期 · 3：释放
DebtStatus	Integer	0	固定取值：0，表示预付费实例。
ExpireTime	Long	2308402384	实例到期时间。格式为时间戳，单位：毫秒。
GmtCreate	Long	2308402384	实例创建时间。格式为时间戳，单位：毫秒。

名称	类型	示例值	描述
Edition	Integer	9	防护套餐版本，固定取值：9（专业版）。
Enabled	Integer	1	实例工作状态，取值： · 1：正常转发业务 · 0：已停止业务转发

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeInstances
&PageNo=1
&PageSize=10
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<Total>1</Total>
<Instances>
    <Status>1</Status>
    <Edition>9</Edition>
    <ExpireTime>1578931200000</ExpireTime>
    <InstanceId>ddoscoo-cn-xxxxxxx</InstanceId>
    <DebtStatus>0</DebtStatus>
    <GmtCreate>1576236360000</GmtCreate>
</Instances>
<RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```

`JSON` **格式**

```
{
  "Total": 1,
  "Instances": [
  {
   "Status": 1,
   "Edition": 9,
   "ExpireTime": 1578931200000,
   "InstanceId": "ddoscoo-cn-xxxxxxx",
   "DebtStatus": 0,
   "GmtCreate": 1576236360000
  }
  ],
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.4.2 DescribeInstanceDetails

调用DescribeInstanceDetails查询指定实例的详情信息。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstanceDetails	系统规定参数。取值：DescribeInstanceDetails。
InstanceIds	String	是	["ddoscoo-cn-XXXX1", "ddoscoo-cn-XXXX2"]	通过实例Id查询实例信息，传入要查询的实例Id数组（JSON字符串）。支持精确匹配。例如，["ddoscoo-cn-XXXX1", "ddoscoo-cn-XXXX2"]。
RegionId	String	否	xx	地域ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
InstanceDetails	Array		实例详情列表。
EipInfoList	Array		与该实例绑定的EIP信息列表。
Eip	String	1.1.1.1	EIP值。
Status	String	normal	EIP状态，取值： · normal：正常 · cleaning：清洗中 · blackhole：黑洞中

名称	类型	示例值	描述
InstanceId	String	ddoscoo-cn-XXXXX	实例ID。
Line	String	coop-line-001	实例线路。例如，coop-line-001。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeInstanceDetails
&InstanceIds=["ddoscoo-cn-XXXX1", "ddoscoo-cn-XXXX2"]
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeInstanceDetailsResponse>
     <InstanceDetails>
          <element>
               <EipInfoList>
                    <element>
                         <Eip>1.1.1.1</Eip>
                         <Status>normal</Status>
                    </element>
               </EipInfoList>
               <InstanceId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</
InstanceId>
               <Line>coop-line-001</Line>
          </element>
     </InstanceDetails>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeInstanceDetailsResponse>
```

`JSON` **格式**

```
{
 "InstanceDetails":[
  {
   "InstanceId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "Line":"coop-line-001",
   "EipInfoList":[
    {
     "Status":"normal",
     "Eip":"1.1.1.1"
    }
   ]
  }
 ],
```

```
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.4.3 DescribeInstanceSpecs

调用DescribeInstanceSpecs查询指定实例的规格。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstanceSpecs	系统规定参数。取值：DescribeInstanceSpecs。
InstanceIds	String	是	["ddoscoo-cn-XXXXX"]	要查询的实例ID数组（JSON字符串）。

返回数据

名称	类型	示例值	描述
InstanceSpecs	Array		实例规格列表。
BandwidthMbps	Integer	20000	业务带宽值。
BaseBandwidth	Integer	20	基础带宽值。
DefenseCount	Integer	10	防护次数。
DomainLimit	Integer	50	最大域名个数。
ElasticBandwidth	Integer	20	弹性带宽值。

名称	类型	示例值	描述
FunctionVersion	String	default	功能版本，取值： · default：标准版 · enhance：增强版
InstanceId	String	ddoscoo-cn-XXXXX	实例ID。
PortLimit	Integer	50	最大防护端口数。
QpsLimit	Integer	1000	QPS限制。
SiteLimit	Integer	10	站点防护数限制。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeInstanceSpecs
&InstanceIds=["ddoscoo-cn-XXXXX"]
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeInstanceSpecsResponse>
     <InstanceSpecs>
          <element>
               <BandwidthMbps>100</BandwidthMbps>
               <BaseBandwidth>20</BaseBandwidth>
               <DefenseCount>10</DefenseCount>
               <DomainLimit>20</DomainLimit>
               <ElasticBandwidth>10</ElasticBandwidth>
               <FunctionVersion>default</FunctionVersion>
               <InstanceId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</
InstanceId>
               <PortLimit>10</PortLimit>
               <SiteLimit>10</SiteLimit>
               <QpsLimit>1000</QpsLimit>
          </element>
     </InstanceSpecs>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```

```
</DescribeInstanceSpecsResponse>
```

JSON 格式

```
{
 "InstanceSpecs":[
  {
   "QpsLimit":1000,
   "DomainLimit":20,
   "FunctionVersion":"default",
   "SiteLimit":10,
   "BandwidthMbps":100,
   "PortLimit":10,
   "DefenseCount":10,
   "InstanceId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "ElasticBandwidth":10,
   "BaseBandwidth":20
  }
 ],
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.4.4 DescribeInstanceStatistics

调用DescribeInstanceStatistics查询指定实例的统计信息。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstanceStatistics	系统规定参数。取值：DescribeInstanceStatistics。
InstanceIds	String	是	["ddoscoo-cn-XXXX1","ddoscoo-cn-XXXX2"]	通过实例Id查询实例信息，传入要查询的实例Id数组（JSON字符串）。支持精确匹配。例如，["ddoscoo-cn-XXXX1","ddoscoo-cn-XXXX2"]。
RegionId	String	否	cn	地域ID。

名称	类型	是否必选	示例值	描述
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
InstanceStatistics	Array		实例的统计信息列表。
DefenseCountUsage	Integer	1	已使用防护次数。
DomainUsage	Integer	10	已使用域名的数量。
InstanceId	String	ddoscoo-cn-XXXXX	实例ID。
PortUsage	Integer	20	已使用四层规则的数量。
SiteUsage	Integer	1	已添加站点的数量。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeInstanceStatistics
&InstanceIds=["ddoscoo-cn-XXXX1", "ddoscoo-cn-XXXX2"]
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeInstanceStatisticsResponse>
     <InstanceStatistics>
          <element>
               <DomainUsage>10</DomainUsage>
               <InstanceId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</
InstanceId>
               <PortUsage>20</PortUsage>
          </element>
     </InstanceStatistics>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```

```
</DescribeInstanceStatisticsResponse>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
 "InstanceStatistics":[
  {
   "DomainUsage":10,
   "PortUsage":20,
   "InstanceId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
  }
 ]
}
```

错误码

访问错误中心查看更多错误码。

11.4.5 DescribeElasticBandwidthSpec

调用DescribeElasticBandwidthSpec查询指定实例的弹性带宽规格。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeElasticBandwidthSpec	系统规定参数。取值：DescribeElasticBandwidthSpec。
InstanceId	String	是	ddoscoo-cn-XXXXX	要查询的实例ID。单次请求只支持查询1个实例。
RegionId	String	否	cn-hangzhou	地域ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
ElasticBandwidthSpec	List	[5, 10, 20, 30]	弹性带宽规格。单位：Gbps。

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeElasticBandwidthSpec
&InstanceId=ddoscoo-cn-XXXXX
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeElasticBandwidthSpecResponse>
     <ElasticBandwidthSpec>
          <element>5</element>
          <element>10</element>
          <element>20</element>
          <element>30</element>
     </ElasticBandwidthSpec>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeElasticBandwidthSpecResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
 "ElasticBandwidthSpec":[
  5,
  10,
  20,
  30
 ]
}
```

错误码

访问**错误中心**查看更多错误码。

11.4.6 ModifyElasticBandWidth

调用ModifyElasticBandWidth修改指定实例的弹性防护带宽。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyElasticBandWidth	系统规定参数。取值：ModifyElasticBandWidth。
ElasticBandwidth	Integer	是	30	新的弹性防护带宽值。 说明: 关于如何设置弹性防护带宽，参见计费方式中的弹性防护部分内容。
InstanceId	String	是	ddoscoo-cn-XXXXX	要操作的实例ID。单次请求只支持修改1个实例的弹性防护带宽，且目标实例必须是正常状态。
RegionId	String	否	cn-hangzhou	地域ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyElasticBandWidth
&ElasticBandwidth=30
&InstanceId=ddoscoo-cn-XXXXX
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ModifyElasticBandWidthResponse>
```

```
    <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ModifyElasticBandWidthResponse>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.4.7 ModifyInstanceRemark

调用ModifyInstanceRemark修改指定实例的备注信息。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyInstanceRemark	系统规定参数。取值：ModifyInstanceRemark。
InstanceId	String	否	ddoscoo-cn-XXXXX	要操作的实例ID。单次请求只支持修改一个实例的备注信息。
RegionId	String	否	cn-hangzhou	地域ID。
Remark	String	否	测试备注名1	新的备注信息。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyInstanceRemark
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ModifyInstanceRemarkResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ModifyInstanceRemarkResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.4.8 DescribeDefenseCountStatistics

调用DescribeDefenseCountStatistics查询DDoS高防的抗D包防护次数统计信息。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDefenseCountStatistics	系统规定参数。取值：DescribeDefenseCountStatistics。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
DefenseCountStatistics	Struct		防护次数统计信息。
DefenseCountTotalUsageOfCurrentMonth	Integer	0	本月已消耗的抗D包防护次数。
FlowPackCountRemain	Integer	10	剩余可用的抗D包防护次数。
MaxUsableDefenseCountCurrentMonth	Integer	0	本月最大可用防护次数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDefenseCountStatistics
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DefenseCountStatistics>
    <DefenseCountTotalUsageOfCurrentMonth>0</DefenseCountTotalUsa
geOfCurrentMonth>
    <FlowPackCountRemain>10</FlowPackCountRemain>
    <MaxUsableDefenseCountCurrentMonth>0</MaxUsableDefenseCoun
tCurrentMonth>
</DefenseCountStatistics>
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

`JSON` **格式**

```
{
  "DefenseCountStatistics": {
      "DefenseCountTotalUsageOfCurrentMonth": 0,
      "FlowPackCountRemain": 10,
      "MaxUsableDefenseCountCurrentMonth":0
  },
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80"
```

```
}
```

错误码

访问错误中心查看更多错误码。

11.5 图表

11.5.1 DescribeIpTraffic

调用DescribeIpTraffic查询指定IP的业务流量信息。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeIpTraffic	系统规定参数。取值：DescribeIpTraffic。
Eip	String	是	1.1.1.1	要查询的EIP地址。
EndTime	Long	是	1536734120	结束时间戳（秒）。
Interval	Integer	是	60	采样间隔（秒），必须是60秒的倍数，默认值60s。采样结果可缩放。
StartTime	Long	是	1536734112	开始时间戳（秒）。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xxx	资源组ID。

名称	类型	是否必选	示例值	描述
Port	Integer	否	233	要查询的端口。  说明: 若不传入该参数，则查询EIP下所有端口的流量。
QueryProtocol	String	否	http	要查询的协议类型。  说明: 若不传入该参数，则查询EIP下所有协议类型的流量。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
MaxInBps	Long	10000	最大入带宽，单位：bps。
AvgInBps	Long	10000	平均入带宽，单位：bps。
MaxOutBps	Long	10000	最大出带宽，单位：bps。
AvgOutBps	Long	10000	平均出带宽，单位：bps。
IpTrafficPoints	Array		具体的时间点列表。
Time	Long	1536734112	时间点（时间戳），单位：秒。
MaxInbps	Long	10000	最大入带宽，单位：bps。
MaxOutbps	Long	10000	最大出带宽，单位：bps。
Cps	Integer	100	连接新建速率。
ActConns	Integer	100	活跃的并发连接数。

名称	类型	示例值	描述
InactConns	Integer	100	非活跃的并发连接数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeIpTraffic
&Eip=1.1.1.1
&EndTime=1536734120
&Interval=60
&StartTime=1536734112
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<MaxInBps>10000</MaxInBps>
<AvgInBps>10000</AvgInBps>
<MaxOutBps>10000</MaxOutBps>
<AvgOutBps>10000</AvgOutBps>
<IpTrafficPoints>
    <Time>1536734112</Time>
    <MaxInBps>10000</MaxInBps>
    <MaxOutBps>10000</MaxOutBps>
    <Cps>100</Cps>
    <ActConns>100</ActConns>
    <InactConns>100</InactConns>
</IpTrafficPoints>
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

`JSON` **格式**

```
{
  "MaxInBps": 10000,
  "AvgInBps": 10000,
  "MaxOutBps": 10000,
  "AvgOutBps": 10000,
  "IpTrafficPoints": [
    {
      "Time": 1536734112,
   "MaxInBps": 10000,
      "MaxOutBps": 10000,
   "Cps":100,
   "ActConns": 100,
   "InactConns":100
    }
  ],
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

错误码

访问错误中心查看更多错误码。

11.5.2 DescribeDDoSTraffic

调用DescribeDDoSTraffic查询指定IP的DDoS攻击流量信息。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDDoSTraffic	系统规定参数。取值：DescribeDDoSTraffic。
Eip	String	是	1.1.1.1	要查询的EIP地址。
EndTime	Long	是	3289457398	结束时间戳，单位：秒。
Interval	Integer	是	60	采样间隔，单位：秒。必须是60秒的倍数，默认60s。返回结果可缩放。
StartTime	Long	是	3289457324	查询开始时间戳（秒）。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
DefenseInBytes	Long	23482234	清洗流量，单位：byte。

名称	类型	示例值	描述
SourceInBytes	Long	19284762	回源流量，单位：byte。
DDoSTrafficPoints	Array		各时间点攻击流量信息。
Time	Long	234082304	时间点（时间戳），单位：秒。
DefenseMaxInBps	Long	129867	该时间点的攻击流量，单位：bps。
SourceMaxInBps	Long	129867	该时间点的总流量，单位：bps。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDDoSTraffic
&Eip=1.1.1.1
&EndTime=3289457398
&Interval=60
&StartTime=3289457324
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DefenseInBytes>23482234</DefenseInBytes>
<SourceInBytes>19284762</SourceInBytes>
<DDoSTrafficPoints>
    <Time>234082304</Time>
    <DefenseMaxInBps>129867</DefenseMaxInBps>
    <SourceMaxInBps>129867</SourceMaxInBps>
</DDoSTrafficPoints>
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

`JSON` **格式**

```
{
  "DefenseInBytes": 23482234,
  "SourceInBytes": 19284762,
  "DDoSTrafficPoints": [
    {
      "Time": 234082304,
   "DefenseMaxInBps": 129867,
   "SourceMaxInBps": 129867
    }
  ],
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80"
```

```
}
```

错误码

访问错误中心查看更多错误码。

11.5.3 DescribeDDoSEvents

调用DescribeDDoSEvents查询指定IP的DDoS攻击事件。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDDoSEvents	系统规定参数。取值：DescribeDDoSEvents。
Eip	String	是	1.1.1.1	要查询的EIP地址。
EndTime	Long	是	3289457324	流量查询的结束时间戳，单位：秒。
Offset	Integer	是	1	返回结果开始位置，即从几个结果开始返回。 说明: 若不传入该参数，则从第0个结果开始返回。
PageSize	String	是	10	分页大小，即每页显示的结果个数。最大值50。
StartTime	Long	是	3289457398	流量查询的开始时间戳，单位：秒。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
Total	Long	1	结果总数。
Events	Array		DDoS攻击事件。
StartTime	Long	3289457324	事件开始时间，单位：毫秒。
EndTime	Long	3289457398	事件结束时间，单位：毫秒。
Interval	Integer	12	事件持续时间，单位：秒。
Status	String	blackhole_start	事件类型： · lackhole_start：黑洞中 · blackhole_end：黑洞结束 · defense_start：清洗中 · defense_end：清洗结束

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDDoSEvents
&Eip=1.1.1.1
&EndTime=3289457324
&Offset=1
&PageSize=10
&StartTime=3289457398
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<Total>1</Total>
<Events>
    <StartTime>3289457324</StartTime>
    <EndTime>3289457398</EndTime>
    <Interval>12</Interval>
    <Status>blackhole_start</Status>
</Events>
```

```
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

JSON 格式

```
{
  "Total":1,
  "Events":[
    {
      "StartTime":3289457324,
      "EndTime":3289457398,
      "Interval":12,
      "Status":"blackhole_start"
    }
  ],
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

错误码

访问错误中心查看更多错误码。

11.5.4 DescribeDomainQps

调用DescribeDomainQps查询指定域名的QPS次数信息。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainQps	系统规定参数。取值：DescribeDomainQps。
Domain	String	是	www.aliyun.com	要查询的域名。
EndTime	Long	是	1577721600	结束时间戳，单位：秒。
StartTime	Long	是	1575129600	开始时间戳，单位：秒。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
RegionId	String	否	cn-hangzhou	地域ID。

名称	类型	是否必选	示例值	描述
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
Interval	Integer	60	相隔两个数据之间的时间差，单位：秒。
StartTime	Long	1575129600	开始时间戳，单位：秒。
Totals	List	[10,40,20]	总的请求次数，单位：QPS。
Blocks	List	[0,0,0]	攻击请求次数，单位：QPS。
CacheHits	List	[0,0,0]	命中页面缓存加速规则的请求次数，单位：QPS。
PreciseBlocks	List	[0,0,0]	精准防护规则拦截的请求次数，单位：QPS。
RegionBlocks	List	[0,0,0]	地域封禁拦截的QPS。
IpBlockQps	List	[0,0,0]	IP封禁拦截的请求次数，单位：QPS。
CcJsQps	List	[0,0,0]	命中频率控制规则触发人机识别的请求次数，单位：QPS。
PreciseJsQps	List	[0,0,0]	命中精准防护规则的挑战校验的请求次数，单位：QPS。
CcBlockQps	List	[0,0,0]	频率控制拦截的请求次数，单位：QPS。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainQps
&Domain=www.aliyun.com
&EndTime=230842000
&StartTime=23084000
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<Interval>60</Interval>
<StartTime>1575129600</StartTime>
<Totals>10</Totals>
<Totals>40</Totals>
<Totals>20</Totals>
<CacheHits>0</CacheHits>
<CacheHits>0</CacheHits>
<CacheHits>0</CacheHits>
<Blocks>0</Blocks>
<Blocks>0</Blocks>
<Blocks>0</Blocks>
<CcBlockQps>0</CcBlockQps>
<CcBlockQps>0</CcBlockQps>
<CcBlockQps>0</CcBlockQps>
<CcJsQps>0</CcJsQps>
<CcJsQps>0</CcJsQps>
<CcJsQps>0</CcJsQps>
<IpBlockQps>0</IpBlockQps>
<IpBlockQps>0</IpBlockQps>
<IpBlockQps>0</IpBlockQps>
<PreciseBlocks>0</PreciseBlocks>
<PreciseBlocks>0</PreciseBlocks>
<PreciseBlocks>0</PreciseBlocks>
<PreciseJsQps>0</PreciseJsQps>
<PreciseJsQps>0</PreciseJsQps>
<PreciseJsQps>0</PreciseJsQps>
<RegionBlocks>0</RegionBlocks>
<RegionBlocks>0</RegionBlocks>
<RegionBlocks>0</RegionBlocks>
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

`JSON` **格式**

```
{
  "Interval": 60,
  "StartTime": 1575129600,
  "Totals": [10,40,20],
  "CacheHits": [0,0,0],
  "Blocks": [0,0,0],
  "CcBlockQps": [0,0,0],
  "CcJsQps": [0,0,0],
  "IpBlockQps": [0,0,0],
  "PreciseBlocks": [0,0,0],
  "PreciseJsQps": [0,0,0],
  "RegionBlocks": [0,0,0],
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80"
```

```
}
```

错误码

访问错误中心查看更多错误码。

11.5.5 DescribeDomainQpsWithCache

调用DescribeDomainQps查询指定域名的QPS次数信息以及缓存命中次数。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainQpsWithCache	系统规定参数。取值：DescribeDomainQpsWithCache。
EndTime	Long	是	1577796336	结束时间戳，单位：秒。
StartTime	Long	是	1577794536	开始时间戳，单位：秒。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。
Domain	String	否	www.example.com	要查询的域名。 说明: 不指定该参数，则默认查询第一个域名配置记录的域名。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
Interval	Integer	60	相隔两个数据之间的时间差，单位：秒。
StartTime	Long	1577794500	开始时间戳，单位：秒。
Totals	List	[10,40,20]	总的请求次数，单位：QPS。
Blocks	List	[0,0,0]	拦截的攻击请求次数，单位：QPS。
CacheHits	List	[0,0,0]	命中页面缓存加速规则的请求次数，单位：QPS。
PreciseBlocks	List	[0,0,0]	精准防护规则拦截的请求次数，单位：QPS。
RegionBlocks	List	[0,0,0]	地域封禁拦截的QPS。
IpBlockQps	List	[0,0,0]	IP封禁拦截的请求次数，单位：QPS。
CcJsQps	List	[0,0,0]	命中频率控制规则触发人机识别的请求次数，单位：QPS。
PreciseJsQps	List	[0,0,0]	命中精准防护规则的挑战校验的请求次数，单位：QPS。
CcBlockQps	List	[0,0,0]	频率控制拦截的请求次数，单位：QPS。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainQpsWithCache
&EndTime=1577796336
&StartTime=1577794536
&<公共请求参数>
```

正常返回示例

XML 格式

```
<Interval>60</Interval>
<StartTime>1577794500</StartTime>
<Totals>10</Totals>
<Totals>40</Totals>
<Totals>20</Totals>
<CacheHits>0</CacheHits>
<CacheHits>0</CacheHits>
<CacheHits>0</CacheHits>
<Blocks>0</Blocks>
<Blocks>0</Blocks>
<Blocks>0</Blocks>
<CcBlockQps>0</CcBlockQps>
<CcBlockQps>0</CcBlockQps>
<CcBlockQps>0</CcBlockQps>
<CcJsQps>0</CcJsQps>
<CcJsQps>0</CcJsQps>
<CcJsQps>0</CcJsQps>
<IpBlockQps>0</IpBlockQps>
<IpBlockQps>0</IpBlockQps>
<IpBlockQps>0</IpBlockQps>
<PreciseBlocks>0</PreciseBlocks>
<PreciseBlocks>0</PreciseBlocks>
<PreciseBlocks>0</PreciseBlocks>
<PreciseJsQps>0</PreciseJsQps>
<PreciseJsQps>0</PreciseJsQps>
<PreciseJsQps>0</PreciseJsQps>
<RegionBlocks>0</RegionBlocks>
<RegionBlocks>0</RegionBlocks>
<RegionBlocks>0</RegionBlocks>
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

JSON 格式

```
{
  "Interval": 60,
  "StartTime": 1577794500,
  "Totals": [10,40,20],
  "CacheHits": [0,0,0],
  "Blocks": [0,0,0],
  "CcBlockQps": [0,0,0],
  "CcJsQps": [0,0,0],
  "IpBlockQps": [0,0,0],
  "PreciseBlocks": [0,0,0],
  "PreciseJsQps": [0,0,0],
  "RegionBlocks": [0,0,0],
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

错误码

访问错误中心查看更多错误码。

11.5.6 DescribeDomainAttackEvents

调用DescribeDomainAttackEvents查询指定域名的攻击事件。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainAttackEvents	系统规定参数。取值：DescribeDomainAttackEvents。
Domain	String	是	www.aliyun.com	要查询的域名。
EndTime	Long	是	3289457398	流量查询的结束时间戳，单位：毫秒。时间间隔最大30天。
Offset	Integer	是	0	返回结果开始位置，即从第几个结果开始返回。 说明: 如不传入该参数，则从第0个结果开始返回。
PageSize	String	是	50	分页大小，即每页显示多少条记录。最大值50。
StartTime	Long	是	3289457324	流量查询的开始时间戳，单位：毫秒。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
Total	Long	1	结果总数。
Events	Array		域名攻击事件。
StartTime	Long	3289457324	事件开始时间，单位：毫秒。
EndTime	Long	3289457398	事件结束时间，单位：毫秒。
Duration	Integer	12	事件持续时间，单位：分。
Finished	Boolean	true	攻击是否结束： · true：表示已结束 · false：表示未结束
MaxQps	Integer	100	最大攻击QPS。
BlockCount	Long	100	拦截的请求数量。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainAttackEvents
&Domain=www.aliyun.com
&EndTime=3289457398
&Offset=0
&PageSize=50
&StartTime=3289457324
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<Total>1</Total>
<Events>
    <StartTime>3289457324</StartTime>
    <EndTime>3289457398</EndTime>
    <Duration>12</Duration>
    <Finished>true</Finished>
    <MaxQps>100</MaxQps>
```

```
    <BlockCount>100</BlockCount>
</Events>
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

JSON 格式

```
{
  "Total": 1,
  "Events": [
    {
      "StartTime": 3289457324,
      "EndTime": 3289457398,
      "Duration": 12,
      "Finished": true,
      "MaxQps": 100,
      "BlockCount":100
    }
  ],
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

错误码

访问错误中心查看更多错误码。

11.6 四层规则

11.6.1 CreateLayer4Rule

调用CreateLayer4Rule创建4层转发规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateLayer4Rule	系统规定参数。取值：CreateLayer4Rule。

名称	类型	是否必选	示例值	描述
Listeners	String	是	[{"InstanceId":"ddoscoo-cn-xxxxxxx","Protocol":"tcp","FrontendPort":80,"BackendPort":5,"RealServers":["1.1.1.1","2.2.2.2"]}]	传入要操作的Listeners的JSON数组串，每个Listener的具体结构描述如下： · InstanceId，String类型，必选，实例ID。 · Protocol，String类型，必选，协议类型。 · FrontendPort，Integer类型，必选，前端使用的端口，取值范围：0-65535。 · BackendPort，Integer类型，必选，后端使用的端口，取值范围：0-65535。 · RealServers，Json数组类型，必选，源站IP地址。
RegionId	String	否	cn-hangzhou	地域ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateLayer4Rule
&Listeners=[{"InstanceId":"xxxxxx-xxxxxx-xxxxxx-xxxxxxx","Protocol":"
tcp","FrontendPort":80,"BackendPort":5,"RealServers":"1.1.1.1","2.2.2.
2"}]
&<公共请求参数>
```

正常返回示例

XML 格式

```
<CreateLayer4RuleResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```

```
</CreateLayer4RuleResponse>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.6.2 ConfigLayer4Rule

调用ConfigLayer4Rule编辑4层转发规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ConfigLayer4Rule	系统规定参数。取值：ConfigLayer4Rule。
Listeners	String	是	[{"InstanceId":"xxxxxx-xxxxxx-xxxxxx-xxxxxxx","Protocol":"tcp","FrontendPort":80,"BackendPort":5,"RealServers":["1.1.1.1","2.2.2.2"]}]	传入要操作的Listeners的JSON数组串，每个Listener的具体结构描述如下。 · InstanceId，String类型，必选，实例ID。 · Protocol，String类型，必选，协议类型。 · FrontendPort，Integer类型，必选，前端使用的端口，取值范围：0-65535。 · BackendPort，Integer类型，必选，后端使用的端口，取值范围：0-65535。 · RealServers，Json数组类型，必选，源站IP地址。
RegionId	String	否	cn-hangzhou	地域ID。

返回数据

名称	类型	示例值	描述
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigLayer4Rule
&Listeners=[{"InstanceId":"xxxxxx-xxxxxx-xxxxxx-xxxxxxx","Protocol":"
tcp","FrontendPort":80,"BackendPort":5,"RealServers":["1.1.1.1","2.2.2
.2"]}]
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ConfigLayer4RuleResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigLayer4RuleResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.6.3 DeleteLayer4Rule

调用DeleteLayer4Rule删除4层转发规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteLayer4Rule	系统规定参数。取值：DeleteLayer4Rule。
Listeners	String	是	[{"InstanceId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc","Protocol":"tcp","FrontendPort":80}]	传入要操作的Listeners的JSON数组串，每个Listener的具体结构描述如下： 说明: 目前不支持批量删除，每次只允许删除一个对象。 · InstanceId，String类型，必选，实例ID。 · Protocol，String类型，必选，协议类型。 · FrontendPort，Integer类型，必选，前端使用的端口，取值范围：0-65535。
RegionId	String	否	cn-hangzhou	地域ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteLayer4Rule
&Listeners=[{"InstanceId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc","
Protocol":"tcp","FrontendPort":80}]
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DeleteLayer4RuleResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DeleteLayer4RuleResponse>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.6.4 ConfigLayer4RuleAttribute

调用ConfigLayer4RuleAttribute配置4层转发规则属性，包括会话保持和DDoS防护策略。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ConfigLayer4RuleAttribute	系统规定参数。取值：ConfigLayer4RuleAttribute。

名称	类型	是否必选	示例值	描述
Config	String	是	{"Slimit":{"CpsEnable":1,"MaxconnEnable":1,"Cps":1,"Maxconn":1,"Pps":1,"Bps":1024},"Synproxy":"on","NodataConn":"off","Sla":{"CpsEnable":1,"MaxconnEnable":1,"Cps":100,"Maxconn":1000},"PayloadLen":{"Min":0,"Max":6000},"Cc":{"Sblack":[]}}	配置信息，传入TcpConfig或UdpConfig对象JSON串。 TcpConfig的具体结构描述见如下： · Cc，Struct类型，必选，源连接配置。Cc结构体中仅包含一个Array类型参数Sblack，表示源连接IP黑名单配置。Sblack参数中包含的详细参数描述见Sblack。如果不开启任何IP黑名单配置，则在Sblack参数中传入空值。 · PersistenceTimeout，Integer类型，必选，会话保持的超时时间，单位为秒。默认为0，表示关闭。 · Synproxy，String类型，必选，DDoS防护策略的虚假源，取值：off、on。 · NodataConn，String类型，必选，DDoS防护策略的空连接，取值：off、on。 · Sla，Struct类型，必选，目的限制配置。具体结构描述见Sla。 · Slimit，Struct类型，必选，源限制配置。具体结构描述见Slimit。 · PayloadLen，Struct类型，必选，包过滤配置。具体结构描述见PayloadLen。 UdpConfig的具体结构描述如下： · Cc，Struct类型，必选，源连接配置。Cc结构体中仅包含一个Array类型参数Sblack，表示源连接IP黑名单配置。Sblack参数中包含的详细参数描述见Sblack。如果不开启任何IP黑名单配置，则在Sblack参数中传入空值。 · PersistenceTimeout，Integer类型，必选，会话保持的超时时间，单位为秒。默认为0，表示关闭。

名称	类型	是否必选	示例值	描述
ForwardProtocol	String	是	TCP	转发协议，取值：TCP、UDP。
FrontendPort	Integer	是	233	前端端口。
InstanceId	String	是	ddoscoo-cn-XXXXX	要操作的实例ID。
RegionId	String	否	cn	地域ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigLayer4RuleAttribute
&Config={"Slimit":{"CpsEnable":1,"MaxconnEnable":1,"Cps":1,"Maxconn
":1,"Pps":1,"Bps":1024},"Synproxy":"on","NodataConn":"off","Sla":{"
CpsEnable":1,"MaxconnEnable":1,"Cps":100,"Maxconn":1000},"PayloadLen":
{"Min":0,"Max":6000},"Cc":{"Sblack":[]}}
&ForwardProtocol=TCP
&FrontendPort=233
&InstanceId=ddoscoo-cn-XXXXX
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ConfigLayer4RuleAttributeResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigLayer4RuleAttributeResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.6.5 ConfigHealthCheck

调用ConfigHealthCheck配置四层或七层健康检查。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ConfigHealthCheck	系统规定参数。取值：ConfigHealthCheck。
ForwardProtocol	String	是	tcp	转发协议，取值： · TCP（四层） · UDP（四层） · HTTP（七层）
FrontendPort	Integer	是	233	前端端口。

名称	类型	是否必选	示例值	描述
HealthCheck	String	是	{"Type":"tcp","Timeout":10,"Port":80,"Interval":10,"Up":10,"Down":10}"}	传入HealthCheck对象JSON串，具体结构描述如下： · Type，String类型，必选，协议类型。取值：TCP（四层）、HTTP（七层）。 · Domain，String类型，可选，健康检查/七层健康检查/域名。 · Uri，String类型，可选，健康检查/七层健康检查/检查路径。 · Timeout，Integer类型，可选，健康检查/四层健康检查/响应超时时间（可设置范围：1~30秒）。 · Port，Integer类型，可选，健康检查/四层健康检查/检查端口。 · Interval，Integer类型，可选，健康检查/四层健康检查/检查间隔（可设置范围：1~30秒）。 · Up，Integer类型，可选，健康检查/四层健康检查/健康阈值（表示云服务器从失败到成功的连续健康检查成功次数，可设置范围：1~10）。 · Down，Integer类型，可选，健康检查/四层健康检查/不健康阈值（表示云服务器从成功到失败的连续健康检查失败次数，可设置范围：1~10）。
InstanceId	String	是	ddoscoo-cn-XXXXXX	要操作的实例ID。
RegionId	String	否	cn-hangzhou	地域ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigHealthCheck
&ForwardProtocol=tcp
&FrontendPort=233
&HealthCheck={"Type":"tcp","Timeout":10,"Port":80,"Interval":10,"Up":
10,"Down":10}"}
&InstanceId=ddoscoo-cn-XXXXXX
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ConfigHealthCheckResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigHealthCheckResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.6.6 DescribeLayer4Rules

调用DescribeLayer4Rules查询指定实例的四层转发规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeLayer4Rules	系统规定参数。取值：DescribeLayer4Rules。
InstanceId	String	是	ddoscoo-cn-XXXXX	要查询的实例ID。
Offset	Integer	是	0	开始索引位置，即从第几个结果开始返回。 说明: 如果不传入该参数，则从第0个结果开始返回。
PageSize	String	是	50	分页大小，即每页显示多少个结果。最大值50。
ForwardProtocol	String	否	tcp	转发协议，取值：TCP。
FrontendPort	Integer	否	233	前端端口。
RegionId	String	否	cn-hangzhou	地域ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
Listeners	Array		Listeners数组。
BackendPort	Integer	233	后端使用的端口，范围：0-65535。
FrontendPort	Integer	233	前端使用的端口，范围：0-65535。
InstanceId	String	ddoscoo-cn-XXXXX	实例ID。

名称	类型	示例值	描述
IsAutoCreate	Boolean	false	是否自动创建。如果是，则不允许删除和修改。
Protocol	String	tcp	协议类型。
RealServers	List	["1.1.1.1"]	源站IP地址。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
Total	Long	10	结果总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeLayer4Rules
&InstanceId=ddoscoo-cn-XXXXX
&Offset=0
&PageSize=50
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeLayer4RulesResponse>
     <Listeners>
          <element>
               <BackendPort>80</BackendPort>
               <FrontendPort>80</FrontendPort>
               <InstanceId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</
InstanceId>
               <IsAutoCreate>true</IsAutoCreate>
               <Protocol>tcp</Protocol>
               <RealServers>
                    <element>1.1.1.1</element>
                    <element>2.2.2.2</element>
               </RealServers>
          </element>
     </Listeners>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
     <Total>1</Total>
</DescribeLayer4RulesResponse>
```

`JSON` **格式**

```
{
 "Listeners":[
```

```
  {
   "RealServers":[
    "1.1.1.1",
    "2.2.2.2"
   ],
   "BackendPort":80,
   "FrontendPort":80,
   "InstanceId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "IsAutoCreate":true,
   "Protocol":"tcp"
  }
 ],
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
 "Total":1
}
```


错误码

访问错误中心查看更多错误码。

11.6.7 DescribeLayer4RuleAttributes

调用DescribeLayer4RuleAttributes查询四层转发属性，包括会话保持和DDoS防护策略。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeLayer4RuleAttributes	系统规定参数。取值：DescribeLayer4RuleAttributes。

名称	类型	是否必选	示例值	描述
Listeners	String	是	[{"InstanceId":"ddoscoo-cn-XXXXX","Protocol":"tcp","FrontendPort":80}]	传入要查询的Listener数组JSON串，每个Listener的具体结构描述如下： · InstanceId，String类型，必选，实例ID。 · Protocol，String类型，必选，协议类型。 · FrontendPort，Integer类型，必选，前端使用的端口，取值范围：0-65535。 · BackendPort，Integer类型，可选，后端使用的端口，取值范围：0-65535。 · RealServers，Json数组类型，可选，源站IP地址。 · IsAutoCreate，Boolean类型，可选，是否自动创建。如果是，则不允许删除和修改。
RegionId	String	否	cn-hangzhou	地域ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
Listeners	Array		Listener数组JSON串。
Config			TCP配置。
Cc			源连接配置。
Sblack	Array		源连接IP黑名单配置。
Cnt	Integer	5	新建连接次数，固定取值5。
During	Integer	60	间隔时长。单位秒，固定取值60。

名称	类型	示例值	描述
Expires	Integer	1800	黑名单有效时长，单位秒，取值范围：60~604800。
Type	Integer	1	IP黑名单配置类型，取值： · 1：表示源新建连接IP黑名单。 · 2：表示源并发连接IP黑名单。 · 3：表示源PPS连接IP黑名单。 · 4：表示源带宽连接IP黑名单。
NodataConn	String	on	DDoS防护策略的空连接，取值：off、on。
PayloadLen			包过滤配置。
Max	Integer	2	DDoS防护策略/包长度过滤，包长度的最大值。
Min	Integer	1	DDoS防护策略/包长度过滤，包长度的最小值。
PersistenceTimeout	Integer	0	会话保持的超时时间，单位为秒。默认为0，表示关闭。
Sla			目的限制配置。
Cps	Integer	100	DDoS防护策略/源新建连接限速，取值范围：100~100,000。
CpsEnable	Integer	0	是否启用Cps，取值： · 0：禁用cps · 1：启用cps（默认）
Maxconn	Integer	1000	DDoS防护策略/源并发连接限速，取值范围：1,000~1,000,000。

名称	类型	示例值	描述
MaxconnEnable	Integer	0	是否启用Maxconnection，取值： · 0：禁用maxconn · 1：启用maxconn（默认）
Slimit			源限制配置。
Bps	Long	0	源带宽限速，单位Byte/s，取值范围：1024 ~ 268435456。 说明: 当参数值为0时，表示未开启源带宽限速。
Cps	Integer	100	DDoS防护策略/源新建连接限速，取值范围：100~100,000。
CpsEnable	Integer	0	是否启用Cps，取值： · 0：禁用cps · 1：启用cps（默认）
CpsMode	Integer	2	源新建连接限速，取值： · 1：手动 · 2：自动
Maxconn	Integer	1000	DDoS防护策略/源并发连接限速，取值范围：1,000~1,000,000。
MaxconnEnable	Integer	0	是否启用Maxconnection，取值： · 0：禁用maxconn · 1：启用maxconn（默认）
Pps	Long	0	源PPS限速，单位Packet/s，取值范围：1 ~ 100000。 说明: 当参数值为0时，表示未开启源PPS限速。

名称	类型	示例值	描述
Synproxy	String	on	DDoS防护策略的虚假源，取值：off、on。
FrontendPort	Integer	233	前端使用的端口，范围：0-65535。
InstanceId	String	ddoscoo-cn-XXXXX	实例ID。
Protocol	String	tcp	协议类型。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeLayer4RuleAttributes
&Listeners=[{"InstanceId":"ddoscoo-cn-XXXXX","Protocol":"tcp","
FrontendPort":80}]
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<Listeners>
    <InstanceId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</InstanceId>
    <Protocol>tcp</Protocol>
    <FrontendPort>80</FrontendPort>
    <Config>
        <Cc>
            <Sblack>
                <Type>1</Type>
                <Cnt>5</Cnt>
                <Expires>1800</Expires>
                <During>60</During>
            </Sblack>
        </Cc>
        <PersistenceTimeout>80</PersistenceTimeout>
        <Synproxy>off</Synproxy>
        <NodataConn>on</NodataConn>
        <Sla>
            <Cps>10</Cps>
            <Maxconn>10</Maxconn>
            <CpsEnable>1</CpsEnable>
            <MaxconnEnable>1</MaxconnEnable>
        </Sla>
        <Slimit>
            <bps>0</bps>
```

```
            <Cps>10</Cps>
            <Maxconn>10</Maxconn>
            <CpsEnable>1</CpsEnable>
            <MaxconnEnable>1</MaxconnEnable>
            <pps>0</pps>
        </Slimit>
        <PayloadLen>
            <Min>1</Min>
            <Max>2</Max>
        </PayloadLen>
    </Config>
</Listeners>
<RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```

JSON 格式

```
{
 "Listeners":[
  {
   "Config":{
    "Synproxy":"off",
    "NodataConn":"on",
    "PayloadLen":{
     "Max":2,
     "Min":1
    },
    "Sla":{
     "MaxconnEnable":1,
     "Maxconn":10,
     "Cps":10,
     "CpsEnable":1
    },
    "Cc":{
     "Sblack":[
      {
       "Type":1,
       "Expires":1800,
       "During":60,
       "Cnt":5
      }
     ]
    },
    "Slimit":{
     "bps":0,
     "pps":0,
     "MaxconnEnable":1,
     "Maxconn":10,
     "Cps":10,
     "CpsEnable":1
    },
    "PersistenceTimeout":80
   },
   "FrontendPort":80,
   "InstanceId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "Protocol":"tcp"
  }
 ],
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
```

```
}
```

错误码

访问错误中心查看更多错误码。

11.6.8 DescribeHealthCheckList

调用DescribeHealthCheckList查询四层或七层健康检查列表。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeHealthCheckList	系统规定参数。取值：DescribeHealthCheckList。
Listeners	String	是	[{"InstanceId":"ddoscoo-cn-XXXXX","Protocol":"tcp","FrontendPort":80}]	要查询的Listeners数组JSON串，每个Listener的具体结构描述如下： · InstanceId，String类型，必选，实例ID。 · Protocol，String类型，必选，协议类型。 · FrontendPort，Integer类型，必选，前端使用的端口，取值范围：0-65535。 · BackendPort，Integer类型，可选，后端使用的端口，取值范围：0-65535。 · RealServers，Json数组类型，可选，源站IP地址。 · IsAutoCreate，Boolean类型，可选，是否自动创建。如果是，则不允许删除和修改。
RegionId	String	否	cn-hangzhou	地域ID。

名称	类型	是否必选	示例值	描述
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
Listeners	Array		返回的Listener信息。
FrontendPort	Integer	233	转发端口。
HealthCheck			健康检查信息。
Domain	String	www.aliyun.com	健康检查/七层健康检查/域名。
Down	Integer	500	健康检查/四层健康检查/不健康阈值。
Interval	Integer	15	健康检查/四层健康检查/检查间隔。
Port	Integer	233	健康检查/四层健康检查/检查端口。
Timeout	Integer	1000	健康检查/四层健康检查/响应超时时间。
Type	String	tcp	协议类型，取值： · TCP：四层 · HTTP：七层
Up	Integer	1000	健康检查/四层健康检查/健康阈值。
Uri	String	/a/b/c	健康检查/七层健康检查/检查路径。
InstanceId	String	ddoscoo-cn-XXXXX	新BGP高防实例ID。
Protocol	String	tcp	协议类型。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeHealthCheckList
&Listeners=[{"InstanceId":"ddoscoo-cn-XXXXX","Protocol":"tcp","
FrontendPort":80}]
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeHealthCheckListResponse>
     <HealthCheck>
          <element>
               <FrontendPort>80</FrontendPort>
               <HealthCheck>
                    <Down>20</Down>
                    <Interval>10</Interval>
                    <Port>80</Port>
                    <Timeout>10</Timeout>
                    <Type>tcp</Type>
                    <Up>10</Up>
               </HealthCheck>
               <InstanceId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</
InstanceId>
               <Protocol>tcp</Protocol>
          </element>
     </HealthCheck>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeHealthCheckListResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
 "HealthCheck":[
  {
   "FrontendPort":80,
   "InstanceId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "HealthCheck":{
    "Down":20,
    "Port":80,
    "Timeout":10,
    "Interval":10,
    "Up":10,
    "Type":"tcp"
   },
   "Protocol":"tcp"
  }
 ]
}
```

错误码

访问错误中心查看更多错误码。

11.6.9 DescribeHealthCheckStatusList

调用DescribeHealthCheckStatusList查询健康检查状态。

查询健康检查状态列表

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeHealthCheckStatusList	系统规定参数。取值：DescribeHealthCheckStatusList。
Listeners	String	是	[{"InstanceId":"ddoscoo-cn-XXXXX","Protocol":"tcp","FrontendPort":80}]	要查询的转发规则Listeners数组（JSON字符串），每个Listener的具体结构描述如下： · InstanceId，String类型，必选，实例ID。 · Protocol，String类型，必选，协议类型。 · FrontendPort，Integer类型，必选，前端使用的端口，取值范围：0-65535。 · BackendPort，Integer类型，可选，后端使用的端口，取值范围：0-65535。 · RealServers，Json数组类型，可选，源站IP地址。 · IsAutoCreate，Boolean类型，可选，是否自动创建。如果是，则不允许删除和修改。
RegionId	String	否	cn-hangzhou	地域ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
HealthCheckStatusList	Array		健康检查状态列表。
FrontendPort	Integer	233	前端端口。
InstanceId	String	ddoscoo-cn-XXXXX	实例Id。
Protocol	String	tcp	协议类型。
RealServerStatusList	Array		源站状态JSON数组。
Address	String	1.1.1.1	源站IP。
Status	String	normal	状态，取值：normal、abnormal。
Status	String	normal	状态，取值：normal、abnormal。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeHealthCheckStatusList
&Listeners=[{"InstanceId":"ddoscoo-cn-XXXXX","Protocol":"tcp","
FrontendPort":80}]
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeHealthCheckStatusListResponse>
     <HealthCheckStatusList>
          <element>
               <FrontendPort>80</FrontendPort>
               <InstanceId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</
InstanceId>
               <Protocol>tcp</Protocol>
               <RealServerStatusList>
                    <Address>1.1.1.1</Address>
                    <Status>normal</Status>
               </RealServerStatusList>
```

```
                <Status>normal</Status>
            </element>
        </HealthCheckStatusList>
        <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeHealthCheckStatusListResponse>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
 "HealthCheckStatusList":[
  {
   "Status":"normal",
   "FrontendPort":80,
   "InstanceId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "RealServerStatusList":{
    "Status":"normal",
    "Address":"1.1.1.1"
   },
   "Protocol":"tcp"
  }
 ]
}
```

错误码

访问错误中心查看更多错误码。

11.7 七层规则

11.7.1 DescribeDomains

调用DescribeDomains查询7层转发规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomains	系统规定参数。取值：DescribeDomains。
Offset	Integer	是	0	开始索引位置，即从第几条结果开始显示。默认从0开始。

名称	类型	是否必选	示例值	描述
PageSize	String	是	10	分页大小，即每页显示多少条记录。最大值10。
Domain	String	否	www.aliyun.com	要查询的域名。
InstanceIds.N	RepeatList	否	ddoscoo-cn-XXXXXX	DDoS高防实例ID。若指定多个实例，依次传入InstanceIds.1, InstanceIds.2, InstanceIds.3, …
QueryDomainPattern	String	否	fuzzy	查询匹配模式。取值： · fuzzy：模糊查询（默认） · exact：精确查询
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	test	资源组ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
Total	Long	10	域名总数。
Domains	Array		域名列表。
BlackList	List	["1.1.1.1/1","1.1.1.2/2"]	黑名单IP列表。
CcEnabled	Boolean	true	是否启用CC防护。
CcRuleEnabled	Boolean	true	是否启用CC规则。

名称	类型	示例值	描述
CcTemplate	String	normal	CC防护模板。
CertName	String	testCertName	证书名称。
Cname	String	xxxxxxx.aliyunddos1006.com	DDoS高防实例分配的CNAME地址。
Domain	String	www.aliyun.com	域名。
Http2Enable	Boolean	true	是否开启HTTP2。
ProxyTypeList	Array		协议类型列表。
ProxyPorts	List	111	协议端口。
ProxyType	String	http	协议类型。取值： · http · https · websocket · websockets
RealServers	Array		源站列表。
RealServer	String	1.1.1.1	源站地址。
RsType	Integer	0	源站类型。取值： · 0：IP · 1：域名
SslCiphers	String	xx	SSL加密套件类型。
SslProtocols	String	xx	SSL协议类型。
WhiteList	List	["1.1.1.1/1","1.1.1.2/2"]	白名单IP列表。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomains
&Offset=0
&PageSize=10
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<Total>2</Total>
<RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
<Domains>
    <Domain>www.alibaba.com</Domain>
    <ProxyTypeList>
        <ProxyType>http</ProxyType>
        <ProxyPorts>80</ProxyPorts>
        <ProxyPorts>8080</ProxyPorts>
    </ProxyTypeList>
    <RealServers>
        <RealServer>1.1.1.1</RealServer>
        <RsType>0</RsType>
    </RealServers>
    <RealServers>
        <RealServer>1.1.1.2</RealServer>
        <RsType>1</RsType>
    </RealServers>
    <CcEnabled>false</CcEnabled>
    <Cname>xxxxxxx.aliyunddos1006.com</Cname>
    <CcRuleEnabled>true</CcRuleEnabled>
    <CcTemplate>default</CcTemplate>
    <BlackList>1.1.1.1/1</BlackList>
    <BlackList>1.1.1.2/2</BlackList>
    <WhiteList>1.1.1.1/1</WhiteList>
    <WhiteList>1.1.1.2/2</WhiteList>
    <CertName>www_alibaba_com.pem</CertName>
</Domains>
<Domains>
    <Domain>www.alibaba.com</Domain>
    <ProxyTypeList>
        <ProxyType>http</ProxyType>
        <ProxyPorts>80</ProxyPorts>
        <ProxyPorts>8080</ProxyPorts>
    </ProxyTypeList>
    <RealServers>
        <RealServer>1.1.1.1</RealServer>
        <RsType>0</RsType>
    </RealServers>
    <RealServers>
        <RealServer>1.1.1.2</RealServer>
        <RsType>1</RsType>
    </RealServers>
    <CcEnabled>false</CcEnabled>
    <Cname>xxxxxxx.aliyunddos1006.com</Cname>
    <CcRuleEnabled>true</CcRuleEnabled>
    <CcTemplate>default</CcTemplate>
    <BlackList>1.1.1.1/1</BlackList>
```

```
    <BlackList>1.1.1.2/2</BlackList>
    <WhiteList>1.1.1.1/1</WhiteList>
    <WhiteList>1.1.1.2/2</WhiteList>
    <CertName>www_alibaba_com.pem</CertName>
</Domains>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
 "Domains":[
  {
   "Cname":"xxxxxxx.aliyunddos1006.com",
   "BlackList":[
    "1.1.1.1/1",
    "1.1.1.2/2"
   ],
   "Domain":"www.alibaba.com",
   "ProxyTypeList":[
    {
     "ProxyPorts":[
      80,
      8080
     ],
     "ProxyType":"http"
    }
   ],
   "RealServers":[
    {
     "RealServer":"1.1.1.1",
     "RsType":0
    },
    {
     "RealServer":"1.1.1.2",
     "RsType":1
    }
   ],
   "CcTemplate":"default",
   "CertName":"www_alibaba_com.pem",
   "CcRuleEnabled":true,
   "WhiteList":[
    "1.1.1.1/1",
    "1.1.1.2/2"
   ],
   "CcEnabled":false
  },
  {
   "Cname":"xxxxxxx.aliyunddos1006.com",
   "BlackList":[
    "1.1.1.1/1",
    "1.1.1.2/2"
   ],
   "Domain":"www.alibaba.com",
   "ProxyTypeList":[
    {
     "ProxyPorts":[
      80,
      8080
     ],
     "ProxyType":"http"
    }
   ],
   "RealServers":[
```

```
    {
     "RealServer":"1.1.1.1",
     "RsType":0
    },
    {
     "RealServer":"1.1.1.2",
     "RsType":1
    }
   ],
   "CcTemplate":"default",
   "CertName":"www_alibaba_com.pem",
   "CcRuleEnabled":true,
   "WhiteList":[
    "1.1.1.1/1",
    "1.1.1.2/2"
   ],
   "CcEnabled":false
  }
 ],
 "Total":2
}
```


错误码

访问错误中心查看更多错误码。

11.7.2 CreateLayer7Rule

调用CreateLayer7Rule创建7层转发规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateLayer7Rule	系统规定参数。取值：CreateLayer7Rule。
Domain	String	是	www.aliyun.com	要添加的域名。
RsType	Integer	是	0	源站类型，取值： · 0：IP · 1：域名

名称	类型	是否必选	示例值	描述
Rules	String	是	[{"ProxyRules":[{"ProxyPort":443,"RealServers":["1.1.1.1:443"]}],"ProxyType":"https"},{"ProxyRules":[{"ProxyPort":80,"RealServers":["1.1.1.1:80"]}],"ProxyType":"http"}]	传入7层规则Layer7Rule数组JSON串。具体结构描述如下： · ProxyRules，数组类型，必选，规则对象数组，包含以下元素： - ProxyPort，Integer类型，必选，协议端口，取值：80、443。 - RealServers，String类型，必选，用户源站。例如，1.1.1.1:443。 · ProxyType，String类型，必选，协议类型，取值：http、https、websocket、websockets。
InstanceIds.N	RepeatList	否	ddoscoo-cn-XXXXX	要绑定的实例ID。若有多个实例，依次传入InstanceIds.1，InstanceIds.2, InstanceIds.3, .. 说明： 若不传入该参数，则只添加域名，不绑定到具体IP。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateLayer7Rule
&Domain=www.aliyun.com
&RsType=0
```

```
&Rules=[{"ProxyRules":[{"ProxyPort":443,"RealServers":["1.1.1.1:443
"]}],"ProxyType":"https"},{"ProxyRules":[{"ProxyPort":80,"RealServers
":["1.1.1.1:80"]}],"ProxyType":"http"}]
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<CreateLayer7RuleResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</CreateLayer7RuleResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.7.3 ConfigLayer7Rule

调用ConfigLayer7Rule编辑7层转发规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ConfigLayer7Rule	系统规定参数。取值：ConfigLayer7Rule。
Domain	String	是	www.aliyun.com	要操作的域名。
RealServers.N	RepeatList	是	1.1.1.1	源站IP。若有多个源站IP，依次传入RealServers.1, RealServers.2, RealServers.3, ...
RsType	Integer	是	0	源站类型，取值： · 0：IP · 1：域名

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	test	资源组ID。
ProxyTypeList	String	否	[{"ProxyPorts":[80,8080],"ProxyType":"http"},{"ProxyPorts":[443],"ProxyType":"https"}]	协议数组。具体结构描述如下： · ProxyType，String类型，必选，协议类型，取值：http、https、websocket、websockets。 · ProxyPorts，Integer类型，必选，协议端口。
ProxyTypes.N	RepeatList	否	http	协议类型，取值：http、https、websocket、websockets。若设置多个协议类型，依次传入ProxyTypes.1, ProxyTypes.2, ProxyTypes.3, ...
InstanceIds.N	RepeatList	否	ddoscoo-cn-XXXXXX	要绑定的实例Id。若有多个实例，依次传入InstanceIds.1, InstanceIds.2, InstanceIds.3, ... 说明: 若不传入该参数，则只添加域名，不绑定到具体IP。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigLayer7Rule
&Domain=www.aliyun.com
&RealServers.1=1.1.1.1
&RsType=0
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ConfigLayer7RuleResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigLayer7RuleResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.7.4 DeleteLayer7Rule

调用DeleteLayer7Rule删除7层转发规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteLayer7Rule	系统规定参数。取值：DeleteLayer7Rule。
Domain	String	是	www.aliyun.com	要操作的域名。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteLayer7Rule
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DeleteLayer7RuleResponse>
      <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DeleteLayer7RuleResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.7.5 ConfigLayer7Cert

调用ConfigLayer7Cert为指定域名配置7层证书。

设置证书。新BGP高防的证书上传功能已接入云盾证书服务，您可以直接调用该接口从证书服务拉取对应的证书上传到新BGP高防服务。当您选择重新上传一组证书和私钥时，我们会将您的这组证书和私钥重新上传到云盾证书服务，以便您可以重复使用这组证书。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ConfigLayer7Cert	系统规定参数。取值：ConfigLayer7Cert。
Domain	String	是	www.aliyun.com	要操作的域名。
Cert	String	否	xx	证书公钥。  说明: 若传入此参数，则必须同时传入CertName和Key。若传入CertName、Cert、Key组合，则无需传入CertId。
CertId	Integer	否	1234	证书ID。  说明: 若传入此参数，则无需传入CertName、Cert、Key。
CertName	String	否	testCertName	证书名称。  说明: 若传入此参数，则必须同时传入Cert和Key。若传入CertName、Cert、Key组合，则无需传入CertId。
Key	String	否	xx	证书私钥。  说明: 若传入此参数，则必须同时传入CertName和Cert。若传入CertName、Cert、Key组合，则无需传入CertId。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigLayer7Cert
&Domain=www.aliyun.com
&CertId=1
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ConfigLayer7CertResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigLayer7CertResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.7.6 ConfigLayer7BlackWhiteList

调用ConfigLayer7BlackWhiteList为指定域名设置7层防护黑白名单。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ConfigLayer7BlackWhiteList	系统规定参数。取值：ConfigLayer7BlackWhiteList。

名称	类型	是否必选	示例值	描述
Domain	String	是	www.aliyun.com	要配置的域名。
BlackList.N	RepeatList	否	1.1.1.1	黑名单列表。若有多个加黑地址，依次传入BlackList.1, BlackList.2, BlackList.3, ...
ResourceGroupId	String	否	test	资源组ID。
WhiteList.N	RepeatList	否	1.1.1.1	白名单列表。若有多个加白地址，依次传入WhiteList.1, WhiteList.2, WhiteList.3, ...

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigLayer7BlackWhiteList
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ConfigLayer7BlackWhiteListResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigLayer7BlackWhiteListResponse>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
```

```
}
```

错误码

访问错误中心查看更多错误码。

11.7.7 DescribleLayer7InstanceRelations

调用DescribleLayer7InstanceRelations查询七层防护实例和EIP的对应关系。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribleLayer7InstanceRelations	系统规定参数。取值：DescribleLayer7InstanceRelations。
DomainList.N	RepeatList	是	www.aliyun.com	要查询的域名列表。
RegionId	String	否	cn	地域ID。
ResourceGroupId	String	否	test	资源组ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
Layer7InstanceRelations	Array		七层实例的防护关系列表。
Domain	String	www.aliyun.com	域名。
InstanceDetails	Array		实例信息列表。
EipList	List	["203.107.0.0"]	绑定的EIP列表。

名称	类型	示例值	描述
FunctionVersion	String	default	功能版本，取值： · default：标准版 · enhance：增强版
InstanceId	String	ddoscoo-cn-XXXXX	实例ID
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribleLayer7InstanceRelations
&DomainList.1=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribleLayer7InstanceRelationsResponse>
     <Layer7InstanceRelations>
          <element>
               <Domain>1.aliyun.com</Domain>
               <InstanceDetails>
                    <element>
                         <EipList>
                              <element>203.x.x.0</element>
                              <element>203.x.x.1</element>
                         </EipList>
                         <InstanceId>xxxxxx</InstanceId>
                    </element>
                    <element>
                         <EipList>
                              <element>203.x.x.0</element>
                              <element>203.x.x.1</element>
                         </EipList>
                         <FunctionVersion>default</FunctionVersion>
                         <InstanceId>xxxxxx</InstanceId>
                    </element>
               </InstanceDetails>
          </element>
     </Layer7InstanceRelations>
</DescribleLayer7InstanceRelationsResponse>
```

`JSON` **格式**

```
{
 "Layer7InstanceRelations":[
```

```
  {
   "InstanceDetails":[
    {
     "FunctionVersion":"default",
     "InstanceId":"xxxxxx",
     "EipList":[
      "203.x.x.0",
      "203.x.x.1"
     ]
    },
    {
     "InstanceId":"xxxxxx",
     "EipList":[
      "203.x.x.0",
      "203.x.x.1"
     ]
    }
   ],
   "Domain":"1.aliyun.com"
  }
 ]
}
```

错误码

访问错误中心查看更多错误码。

11.7.8 DescribleCertList

调用DescribleCertList查询所有证书列表。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribleCertList	系统规定参数。取值：DescribleCertList。
Domain	String	否	www.aliyun.com	要查询的域名。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	test	资源组ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
CertList	Array		证书列表。
Common	String	www.aliyun.com	证书绑定的域名。
DomainRelated	Boolean	false	是否已绑定域名配置。
EndDate	String	2020-09-23	证书到期日期。
Id	Integer	123	证书ID。
Issuer	String	DigiCert Inc	证书签发者。
Name	String	testCertName	证书名称。
StartDate	String	2019-09-24	证书开始日期。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribleCertList
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<RequestId>1F2AD7D5-EDB6-4E4B-B81F-8AA68B2E3340</RequestId>
<CertList>
    <Name>leidantest</Name>
    <Issuer>Alibaba</Issuer>
    <EndDate>2029-06-07</EndDate>
    <DomainRelated>false</DomainRelated>
    <StartDate>2019-06-10</StartDate>
    <Id>2329174</Id>
    <Common>www.aliyun.com</Common>
```

```
</CertList>
```

JSON 格式

```
{
 "RequestId":"1F2AD7D5-EDB6-4E4B-B81F-8AA68B2E3340",
 "CertList":[
  {
   "Name":"leidantest",
   "Issuer":"Alibaba",
   "EndDate":"2029-06-07",
   "StartDate":"2019-06-10",
   "DomainRelated":false,
   "Id":2329174,
   "Common":"www.aliyun.com"
  }
 ]
}
```

错误码

访问错误中心查看更多错误码。

11.7.9 EnableLayer7CC

调用EnableLayer7CC为指定域名启用7层CC防护。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	EnableLayer7CC	系统规定参数。取值：EnableLayer7CC。
Domain	String	是	www.aliyun.com	要操作的域名。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	test	资源组ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=EnableLayer7CC
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<EnableLayer7CCResponse>
      <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</EnableLayer7CCResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问**错误中心**查看更多错误码。

11.7.10 DisableLayer7CC

调用DisableLayer7CC为指定域名禁用7层CC防护。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DisableLayer7CC	系统规定参数。取值：DisableLayer7CC。

名称	类型	是否必选	示例值	描述
Domain	String	是	www.aliyun.com	要操作的域名。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	test	资源组ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DisableLayer7CC
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DisableLayer7CCResponse>
      <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DisableLayer7CCResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.7.11 EnableLayer7CCRule

调用EnableLayer7CCRule为指定域名启用7层CC规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	EnableLayer7CCRule	系统规定参数。取值：EnableLayer7CCRule。
Domain	String	是	www.aliyun.com	要操作的域名。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	test	资源组ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=EnableLayer7CCRule
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

```
<EnableLayer7CCRuleResponse>
```

```
    <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</EnableLayer7CCRuleResponse>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.7.12 DisableLayer7CCRule

调用DisableLayer7CCRule为指定域名禁用7层CC规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DisableLayer7CCRule	系统规定参数。取值：DisableLayer7CCRule。
Domain	String	是	www.aliyun.com	要操作的域名。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	test	资源组ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DisableLayer7CCRule
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DisableLayer7CCRuleResponse>
      <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DisableLayer7CCRuleResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.7.13 AddLayer7CCRule

调用AddLayer7CCRule为指定域名添加7层CC规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Act	String	是	close	规则触发后的操作，取值： · close：封禁 · captcha：人机识别
Action	String	是	AddLayer7CCRule	系统规定参数。取值： AddLayer7CCRule。

名称	类型	是否必选	示例值	描述
Count	Integer	是	2	访问次数，与Interval结和使用。当同一个IP在Interval指定的间隔时间内连续访问Count中指定的访问次数，则触发规则。取值范围为2~2,000。
Domain	String	是	www.aliyun.com	要操作的域名。
Interval	Integer	是	5	间隔时间，与Count结和使用。当同一个IP在Interval指定的间隔时间内连续访问Count中指定的访问次数，则触发规则。取值范围为5~10,800。
Mode	String	是	match	URI匹配模式，取值： · match：完全匹配。访问请求的URI与指定的Uri完全相同，才计入访问次数。 · prefix：前缀匹配。访问请求的URI包含指定的Uri，则计入访问次数。
Name	String	是	testCcRule1	CC自定义规则名。
Ttl	Integer	是	60	若规则触发后动作指定为封禁，设置封禁时间，单位为秒，取值范围为60~86,400。
Uri	String	是	/a/b/c	被防护的URI。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=AddLayer7CCRule
&Act=close
&Count=2
&Domain=www.aliyun.com
&Interval=5
&Mode=match
&Name=testCcRule1
&Ttl=60
&Uri=/a/b/c
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<AddLayer7CCRuleResponse>
      <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</AddLayer7CCRuleResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.7.14 ConfigLayer7CCRule

调用ConfigLayer7CCRule编辑7层CC规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Act	String	是	close	规则触发后的操作，取值： · close：封禁 · captcha：人机识别
Action	String	是	ConfigLayer7CCRule	系统规定参数。取值：ConfigLayer7CCRule。
Count	Integer	是	2	访问次数，与Interval结和使用。当同一个IP在Interval指定的间隔时间内连续访问Count中指定的访问次数，则触发规则。取值范围为2~2,000。
Domain	String	是	www.aliyun.com	要操作的域名。
Interval	Integer	是	5	间隔时间，与Count结和使用。当同一个IP在Interval指定的间隔时间内连续访问Count中指定的访问次数，则触发规则。取值范围为5~10,800。
Mode	String	是	match	URI匹配模式，取值： · match：完全匹配。访问请求的URI与指定的Uri完全相同，才计入访问次数。 · prefix：前缀匹配。访问请求的URI包含指定的Uri，则计入访问次数。
Name	String	是	testCcRule1	CC自定义规则名。
Ttl	Integer	是	60	若规则触发后动作指定为封禁，设置封禁时间，单位为秒，取值范围为60~86,400。

名称	类型	是否必选	示例值	描述
Uri	String	是	/a/b/c	被防护的URI。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigLayer7CCRule
&Act=close
&Count=2
&Domain=www.aliyun.com
&Interval=5
&Mode=match
&Name=testCcRule1
&Ttl=60
&Uri=/a/b/c
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ConfigLayer7CCRuleResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigLayer7CCRuleResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.7.15 DescribeLayer7CCRules

调用DescribeLayer7CCRules查询7层CC规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeLayer7CCRules	系统规定参数。取值：DescribeLayer7CCRules。
Domain	String	是	www.aliyun.com	要查询的域名。
Offset	Integer	是	0	开始索引位置，即从第几个结果开始返回。 说明: 若不传入该参数，则从第0个结果开始返回。
PageSize	String	是	10	分页大小，即每页显示过少个结果。最大值10。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
Layer7CCRules			CC规则数组。
Act	String	close	规则触发后的操作，取值： · close：封禁 · captcha：人机识别

名称	类型	示例值	描述
Count	Integer	100	访问次数，与Interval结和使用。当同一个IP在Interval指定的间隔时间内连续访问Count中指定的访问次数，则触发规则。
Interval	Integer	60	间隔时间，与Count结和使用。当同一个IP在Interval指定的间隔时间内连续访问Count中指定的访问次数，则触发规则。
Mode	String	match	URI匹配模式，取值： · match：完全匹配。访问请求的URI与指定的Uri完全相同，才计入访问次数。 · prefix：前缀匹配。访问请求的URI包含指定的Uri，则计入访问次数。
Name	String	testCcRule1	CC自定义规则名。
Ttl	Integer	1000	若规则触发后动作指定为封禁，设置封禁时间。
Uri	String	/a/b/c	被防护的URI。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
Total	Long	10	规则总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeLayer7CCRules
&Domain=www.aliyun.com
&Offset=0
&PageSize=10
```

```
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeLayer7CCRulesResponse>
     <Layer7CCRules>
          <element>
               <Act>close</Act>
               <Count>11</Count>
               <Interval>5</Interval>
               <Mode>match</Mode>
               <Name>XXXX</Name>
               <Ttl>1</Ttl>
               <Uri>/a/b/c.htm</Uri>
          </element>
          <element>
               <Act>close</Act>
               <Count>11</Count>
               <Interval>5</Interval>
               <Mode>match</Mode>
               <Name>XXXX</Name>
               <Ttl>1</Ttl>
               <Uri>/a/b/c.htm</Uri>
          </element>
     </Layer7CCRules>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
     <Total>10</Total>
</DescribeLayer7CCRulesResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
 "Layer7CCRules":[
  {
   "Name":"XXXX",
   "Interval":5,
   "Count":11,
   "Act":"close",
   "Ttl":1,
   "Uri":"/a/b/c.htm",
   "Mode":"match"
  },
  {
   "Name":"XXXX",
   "Interval":5,
   "Count":11,
   "Act":"close",
   "Ttl":1,
   "Uri":"/a/b/c.htm",
   "Mode":"match"
  }
 ],
 "Total":10
```

```
}
```

错误码

访问错误中心查看更多错误码。

11.7.16 DeleteLayer7CCRule

调用DeleteLayer7CCRule删除7层CC规则。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteLayer7CCRule	系统规定参数。取值：DeleteLayer7CCRule。
Domain	String	是	www.aliyun.com	要操作的域名。
Name	String	是	testCcRule1	要删除的CC自定义规则名。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteLayer7CCRule
&Domain=www.aliyun.com
&Name=testCcRule1
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DeleteLayer7CCRuleResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DeleteLayer7CCRuleResponse>
```

`JSON` 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.7.17 ConfigLayer7CCTemplate

调用ConfigLayer7CCTemplate为指定域名设置7层CC防护模式。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ConfigLayer7CCTemplate	系统规定参数。取值：ConfigLayer7CCTemplate。
Domain	String	是	www.aliyun.com	要操作的域名。
Template	String	是	default	要应用的CC防护模式，取值： · default：正常 · gf_under_attack：攻击紧急 · gf_sos_verify：严格 · gf_sos_enhance：超级严格
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigLayer7CCTemplate
&Domain=www.aliyun.com
&Template=default
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ConfigLayer7CCTemplateResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigLayer7CCTemplateResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问**错误中心**查看更多错误码。

11.7.18 DescribeDomainAccessMode

调用DescribeDomainAccessMode查询域名的接入模式。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainAccessMode	系统规定参数。取值：DescribeDomainAccessMode。

名称	类型	是否必选	示例值	描述
DomainList.N	RepeatLis	是	www.aliyun.com	要查询的域名。所有多个域名，依次传入DomainList.1, DomainList.2, DomainList.3, ...
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
DomainModeList	Array		模式配置。
AccessMode	Integer	1	接入模式，取值： · 0：A记录 · 1：高防 · 2：回源
Domain	String	www.aliyun.com	域名。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainAccessMode
&DomainList.1=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDomainAccessModeResponse>
     <DomainModeList>
          <element>
               <AccessMode>1</AccessMode>
               <Domain>www.alibaba.com</Domain>
          </element>
          <element>
               <AccessMode>2</AccessMode>
```

```
                <Domain>www.aliyun.com</Domain>
            </element>
        </DomainModeList>
        <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeDomainAccessModeResponse>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
 "DomainModeList":[
  {
   "AccessMode":1,
   "Domain":"www.alibaba.com"
  },
  {
   "AccessMode":2,
   "Domain":"www.aliyun.com"
  }
 ]
}
```

错误码

访问错误中心查看更多错误码。

11.7.19 ConfigDomainAccessMode

调用ConfigDomainAccessMode设置域名接入模式。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
AccessMode	Integer	是	2	接入模式，取值： · 0：A记录 · 1：高防 · 2：回源
Action	String	是	ConfigDomainAccessMode	系统规定参数。取值：ConfigDomainAccessMode。
Domain	String	是	www.aliyun.com	要操作的域名。

名称	类型	是否必选	示例值	描述
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigDomainAccessMode
&AccessMode=2
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ConfigDomainAccessModeResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigDomainAccessModeResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.7.20 DescribeBackSourceCidr

调用DescribeBackSourceCidr查询回源网段。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeBackSourceCidr	系统规定参数。取值：DescribeBackSourceCidr。
Line	String	否	coop-line-001	要查询的防护线路。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	test	资源组ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
CidrList	List	["47.97.128.0/25","47.97.128.128/25"]	回源IP段列表。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeBackSourceCidr
&Line=coop-line-001
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeBackSourceCidrResponse>
      <CidrList>
            <element>47.xx.xx.0/25</element>
            <element>47.xx.xx.128/25</element>
      </CidrList>
      <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```

```
</DescribeBackSourceCidrResponse>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
 "CidrList":[
  "47.xx.xx.0/25",
  "47.xx.xx.128/25"
 ]
}
```

错误码

访问错误中心查看更多错误码。

11.7.21 ListLayer7CustomPorts

调用ListLayer7CustomPorts获取7层转发规则中可添加的端口列表。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ListLayer7CustomPorts	系统规定参数。取值：ListLayer7CustomPorts。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
Lang	String	否	cn	系统语言ID。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

名称	类型	示例值	描述
Layer7CustomPorts	Array		可添加的端口信息。
ProxyType	String	https	协议类型。
ProxyPorts	List	[443,4443,5443,6443,7443,7988,8443,9443,8553,8663,9553,9663,10050,10443,18980,30050]	端口列表。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ListLayer7CustomPorts
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<Layer7CustomPorts>
    <ProxyPorts>80</ProxyPorts>
    <ProxyPorts>83</ProxyPorts>
    <ProxyPorts>84</ProxyPorts>
    <ProxyPorts>88</ProxyPorts>
    <ProxyPorts>89</ProxyPorts>
    <ProxyPorts>800</ProxyPorts>
    <ProxyPorts>808</ProxyPorts>
    <ProxyPorts>1000</ProxyPorts>
    <ProxyPorts>1090</ProxyPorts>
    <ProxyPorts>3333</ProxyPorts>
    <ProxyPorts>3501</ProxyPorts>
    <ProxyPorts>3601</ProxyPorts>
    <ProxyPorts>5000</ProxyPorts>
    <ProxyPorts>5222</ProxyPorts>
    <ProxyPorts>6001</ProxyPorts>
    <ProxyPorts>6666</ProxyPorts>
    <ProxyPorts>7000</ProxyPorts>
    <ProxyPorts>7001</ProxyPorts>
    <ProxyPorts>7002</ProxyPorts>
    <ProxyPorts>7003</ProxyPorts>
    <ProxyPorts>7004</ProxyPorts>
    <ProxyPorts>7005</ProxyPorts>
    <ProxyPorts>7006</ProxyPorts>
    <ProxyPorts>7009</ProxyPorts>
    <ProxyPorts>7010</ProxyPorts>
    <ProxyPorts>7011</ProxyPorts>
    <ProxyPorts>7012</ProxyPorts>
    <ProxyPorts>7013</ProxyPorts>
    <ProxyPorts>7014</ProxyPorts>
    <ProxyPorts>7015</ProxyPorts>
```

```
    <ProxyPorts>7016</ProxyPorts>
    <ProxyPorts>7018</ProxyPorts>
    <ProxyPorts>7019</ProxyPorts>
    <ProxyPorts>7020</ProxyPorts>
    <ProxyPorts>7021</ProxyPorts>
    <ProxyPorts>7022</ProxyPorts>
    <ProxyPorts>7023</ProxyPorts>
    <ProxyPorts>7024</ProxyPorts>
    <ProxyPorts>7025</ProxyPorts>
    <ProxyPorts>7026</ProxyPorts>
    <ProxyPorts>7060</ProxyPorts>
    <ProxyPorts>7070</ProxyPorts>
    <ProxyPorts>7081</ProxyPorts>
    <ProxyPorts>7082</ProxyPorts>
    <ProxyPorts>7083</ProxyPorts>
    <ProxyPorts>7088</ProxyPorts>
    <ProxyPorts>7097</ProxyPorts>
    <ProxyPorts>7777</ProxyPorts>
    <ProxyPorts>7800</ProxyPorts>
    <ProxyPorts>8000</ProxyPorts>
    <ProxyPorts>8001</ProxyPorts>
    <ProxyPorts>8002</ProxyPorts>
    <ProxyPorts>8003</ProxyPorts>
    <ProxyPorts>8008</ProxyPorts>
    <ProxyPorts>8009</ProxyPorts>
    <ProxyPorts>8020</ProxyPorts>
    <ProxyPorts>8021</ProxyPorts>
    <ProxyPorts>8022</ProxyPorts>
    <ProxyPorts>8025</ProxyPorts>
    <ProxyPorts>8026</ProxyPorts>
    <ProxyPorts>8077</ProxyPorts>
    <ProxyPorts>8078</ProxyPorts>
    <ProxyPorts>8080</ProxyPorts>
    <ProxyPorts>8081</ProxyPorts>
    <ProxyPorts>8082</ProxyPorts>
    <ProxyPorts>8083</ProxyPorts>
    <ProxyPorts>8084</ProxyPorts>
    <ProxyPorts>8085</ProxyPorts>
    <ProxyPorts>8086</ProxyPorts>
    <ProxyPorts>8087</ProxyPorts>
    <ProxyPorts>8088</ProxyPorts>
    <ProxyPorts>8089</ProxyPorts>
    <ProxyPorts>8090</ProxyPorts>
    <ProxyPorts>8091</ProxyPorts>
    <ProxyPorts>8106</ProxyPorts>
    <ProxyPorts>8181</ProxyPorts>
    <ProxyPorts>8334</ProxyPorts>
    <ProxyPorts>8336</ProxyPorts>
    <ProxyPorts>8800</ProxyPorts>
    <ProxyPorts>8686</ProxyPorts>
    <ProxyPorts>8787</ProxyPorts>
    <ProxyPorts>8888</ProxyPorts>
    <ProxyPorts>8889</ProxyPorts>
    <ProxyPorts>8999</ProxyPorts>
    <ProxyPorts>9000</ProxyPorts>
    <ProxyPorts>9001</ProxyPorts>
    <ProxyPorts>9002</ProxyPorts>
    <ProxyPorts>9003</ProxyPorts>
    <ProxyPorts>9080</ProxyPorts>
    <ProxyPorts>9200</ProxyPorts>
    <ProxyPorts>9999</ProxyPorts>
    <ProxyPorts>10000</ProxyPorts>
    <ProxyPorts>10001</ProxyPorts>
    <ProxyPorts>10080</ProxyPorts>
```

```
    <ProxyPorts>12601</ProxyPorts>
    <ProxyPorts>86</ProxyPorts>
    <ProxyPorts>9021</ProxyPorts>
    <ProxyPorts>9023</ProxyPorts>
    <ProxyPorts>9027</ProxyPorts>
    <ProxyPorts>9037</ProxyPorts>
    <ProxyPorts>9081</ProxyPorts>
    <ProxyPorts>9082</ProxyPorts>
    <ProxyPorts>9201</ProxyPorts>
    <ProxyPorts>9205</ProxyPorts>
    <ProxyPorts>9207</ProxyPorts>
    <ProxyPorts>9208</ProxyPorts>
    <ProxyPorts>9209</ProxyPorts>
    <ProxyPorts>9210</ProxyPorts>
    <ProxyPorts>9211</ProxyPorts>
    <ProxyPorts>9212</ProxyPorts>
    <ProxyPorts>9213</ProxyPorts>
    <ProxyPorts>48800</ProxyPorts>
    <ProxyPorts>87</ProxyPorts>
    <ProxyPorts>97</ProxyPorts>
    <ProxyPorts>7510</ProxyPorts>
    <ProxyPorts>9180</ProxyPorts>
    <ProxyPorts>9898</ProxyPorts>
    <ProxyPorts>9908</ProxyPorts>
    <ProxyPorts>9916</ProxyPorts>
    <ProxyPorts>9918</ProxyPorts>
    <ProxyPorts>9919</ProxyPorts>
    <ProxyPorts>9928</ProxyPorts>
    <ProxyPorts>9929</ProxyPorts>
    <ProxyPorts>9939</ProxyPorts>
    <ProxyPorts>28080</ProxyPorts>
    <ProxyPorts>33702</ProxyPorts>
    <ProxyType>http</ProxyType>
</Layer7CustomPorts>
<Layer7CustomPorts>
    <ProxyPorts>443</ProxyPorts>
    <ProxyPorts>4443</ProxyPorts>
    <ProxyPorts>5443</ProxyPorts>
    <ProxyPorts>6443</ProxyPorts>
    <ProxyPorts>7443</ProxyPorts>
    <ProxyPorts>7988</ProxyPorts>
    <ProxyPorts>8443</ProxyPorts>
    <ProxyPorts>9443</ProxyPorts>
    <ProxyPorts>8553</ProxyPorts>
    <ProxyPorts>8663</ProxyPorts>
    <ProxyPorts>9553</ProxyPorts>
    <ProxyPorts>9663</ProxyPorts>
    <ProxyPorts>10050</ProxyPorts>
    <ProxyPorts>10443</ProxyPorts>
    <ProxyPorts>18980</ProxyPorts>
    <ProxyPorts>30050</ProxyPorts>
    <ProxyType>https</ProxyType>
</Layer7CustomPorts>
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

JSON 格式

```
{
    "Layer7CustomPorts":[
        {
            "ProxyPorts":[80,83,84,88,89,800,808,1000,1090,3333,3501,
3601,5000,5222,6001,6666,7000,7001,7002,7003,7004,7005,7006,7009,7010
,7011,7012,7013,7014,7015,7016,7018,7019,7020,7021,7022,7023,7024,7025
```

```
,7026,7060,7070,7081,7082,7083,7088,7097,7777,7800,8000,8001,8002,8003
,8008,8009,8020,8021,8022,8025,8026,8077,8078,8080,8081,8082,8083,8084
,8085,8086,8087,8088,8089,8090,8091,8106,8181,8334,8336,8800,8686,8787
,8888,8889,8999,9000,9001,9002,9003,9080,9200,9999,10000,10001,10080
,12601,86,9021,9023,9027,9037,9081,9082,9201,9205,9207,9208,9209,9210
,9211,9212,9213,48800,87,97,7510,9180,9898,9908,9916,9918,9919,9928,
9929,9939,28080,33702],
            "ProxyType":"http"
        },
        {
            "ProxyPorts":[443,4443,5443,6443,7443,7988,8443,9443,8553,
8663,9553,9663,10050,10443,18980,30050],
            "ProxyType":"https"
        }
    ],
    "RequestId":"CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

错误码

访问错误中心查看更多错误码。

11.8 日志

11.8.1 DescribeSimpleDomains

调用DescribeSimpleDomains查询已接入DDoS高防的域名列表。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeSimpleDomains	系统规定参数。取值：DescribeSimpleDomains。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
Lang	String	否	cn	系统语言ID。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。

名称	类型	是否必选	示例值	描述
InstanceIds.N	RepeatList	否	ddoscoo-cn-XXXXXX	DDoS高防实例ID。若指定多个实例，依次传入InstanceIds.1, InstanceIds.2, InstanceIds.3, … 说明: 若不指定，则默认查询所有实例。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
DomainList	List	["1.example.com","2.example.com"]	域名列表。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeSimpleDomains
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DomainList>1.example.com</DomainList>
<DomainList>2.example.com</DomainList>
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

`JSON` **格式**

```
{
    "DomainList":["1.example.com","2.example.com"],
    "RequestId":"CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

错误码

访问错误中心查看更多错误码。

11.8.2 DescribeLogStoreExistStatus

调用DescribeLogStoreExistStatus查询是否已存在日志库。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeLogStoreExistStatus	系统规定参数。取值：DescribeLogStoreExistStatus。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
Lang	String	否	cn	系统语言ID。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
ExistStatus	Boolean	true	是否已存在日志库。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeLogStoreExistStatus
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ExistStatus>true</ExistStatus>
```

```
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

JSON 格式

```
{
    "ExistStatus":true,
    "RequestId":"CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

错误码

访问错误中心查看更多错误码。

11.8.3 DescribeSlsAuthStatus

调用DescribeSlsAuthStatus查询是否已授权DDoS高防服务将日志存储至日志服务的专属日志库中。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeSlsAuthStatus	系统规定参数。取值：DescribeSlsAuthStatus。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
Lang	String	否	cn	系统语言ID。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

名称	类型	示例值	描述
SlsAuthStatus	Boolean	true	是否已授权DDoS高防服务将日志存储至日志服务的专属日志库中。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeSlsAuthStatus
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<SlsAuthStatus>true</SlsAuthStatus>
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

`JSON` **格式**

```
{
    "SlsAuthStatus":true,
    "RequestId":"CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

错误码

访问错误中心查看更多错误码。

11.8.4 DescribeSlsOpenStatus

调用DescribeSlsOpenStatus查询是否已开通日志服务。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeSlsOpenStatus	系统规定参数。取值：DescribeSlsOpenStatus。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

名称	类型	是否必选	示例值	描述
Lang	String	否	cn	系统语言ID。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
SlsOpenStatus	Boolean	true	是否已开通日志服务： · true：表示是 · false：表示否

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeSlsOpenStatus
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<SlsOpenStatus>true</SlsOpenStatus>
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

`JSON` **格式**

```
{
    "SlsOpenStatus":true,
    "RequestId":"CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

错误码

访问错误中心查看更多错误码。

11.8.5 DescribeSlsLogstoreInfo

调用DescribeSlsLogstoreInfo查询对应的日志服务日志库信息。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeSlsLogstoreInfo	系统规定参数。取值：DescribeSlsLogstoreInfo。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
Lang	String	否	cn	系统语言ID。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
Quota	Long	5497558138880	日志库容量，单位：字节（Byte）。
LogStore	String	ddoscoo-logstore	日志库名称。
Used	Long	0	已存储的日志量，单位：Byte（字节）。
Project	String	ddoscoo-project-xxxx-cn-hangzhou	日志项目名称。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeSlsLogstoreInfo
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<Project>ddoscoo-project-xxxx-cn-hangzhou</Project>
<Quota>5497558138880</Quota>
<Used>0</Used>
<LogStore>ddoscoo-logstore</LogStore>
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

`JSON` **格式**

```
{
    "Project":"ddoscoo-project-xxxx-cn-hangzhou",
    "Quota":5497558138880,
    "Used":0,
    "LogStore":"ddoscoo-logstore",
    "RequestId":"CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

错误码

访问错误中心查看更多错误码。

11.8.6 DescribeSlsEmptyCount

调用DescribeSlsEmptyCount查询剩余日志库清空次数。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeSlsEmptyCount	系统规定参数。取值：DescribeSlsEmptyCount。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

名称	类型	是否必选	示例值	描述
Lang	String	否	cn	系统语言ID。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
AvailableCount	Integer	0	可用的日志库清空次数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeSlsEmptyCount
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<AvailableCount>0</AvailableCount>
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

`JSON` **格式**

```
{
    "AvailableCount":0,
    "RequestId":"CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

错误码

访问错误中心查看更多错误码。

11.8.7 DescribeDomainSlsStatus

调用DescribeDomainSlsStatus查询指定域名的全量日志分析的状态和对应日志库。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainSlsStatus	系统规定参数。取值：DescribeDomainSlsStatus。
Domain	String	是	www.example.com	要查询的域名。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
Lang	String	否	cn	系统语言ID。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
SlsStatus	Boolean	true	是否启用全量日志分析功能： · true：表示已启用 · false：表示已关闭
SlsLogstore	String	ddoscoo-logstore	对应的日志库。
SlsProject	String	ddoscoo-project-xxxx-cn-hangzhou	对应的日志项目名称。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainSlsStatus
&Domain=www.example.com
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<SlsProject>ddoscoo-project-xxxx-cn-hangzhou</SlsProject>
<SlsStatus>true</SlsStatus>
<SlsLogstore>ddoscoo-logstore</SlsLogstore>
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

`JSON` **格式**

```
{
    "SlsProject":"ddoscoo-project-xxxx-cn-hangzhou",
    "SlsStatus":true,
    "SlsLogstore":"ddoscoo-logstore",
    "RequestId":"CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

错误码

访问错误中心查看更多错误码。

11.8.8 DescribeBatchSlsDispatchStatus

调用DescribeBatchSlsDispatchStatus接口分页查询域名的全量日志分析启用状态。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeBatchSlsDispatchStatus	系统规定参数。取值：DescribeBatchSlsDispatchStatus。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
Lang	String	否	cn	系统语言ID。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。
PageNo	Integer	否	1	当前页数，从1开始。
PageSize	Integer	否	10	分页大小，最大值20。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
TotalCount	Integer	1	域名记录总数。
SlsConfigStatusList	Array		域名的全量日志分析启用状态列表。
Enable	Boolean	true	是否启用全量日志分析功能： · true：表示已启用 · false：表示已关闭
Domain	String	www.example.com	域名名称。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeBatchSlsDispatchStatus
&<公共请求参数>
```

正常返回示例

XML 格式

```
<SlsConfigStatusList>
    <Domain>www.example.com</Domain>
    <Enable>true</Enable>
</SlsConfigStatusList>
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

```
<Total>1</Total>
```

JSON 格式

```
{
 "SlsConfigStatusList":[
  {
   "Domain":"www.example.com",
   "Enable":true
  }
 ],
 "RequestId":"CF33B4C3-196E-4015-AADD-5CAD00057B80",
 "Total":1
}
```

错误码

访问错误中心查看更多错误码。

11.8.9 OpenDomainSlsConfig

调用OpenDomainSlsConfig为指定域名启用全量日志分析功能。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	OpenDomainSlsConfig	系统规定参数。取值：OpenDomainSlsConfig。
Domain	String	是	www.example.com	要启用全量日志分析功能的域名。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
Lang	String	否	cn	系统语言ID。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=OpenDomainSlsConfig
&Domain=www.example.com
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

`JSON` **格式**

```
{
    "RequestId":"CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

错误码

访问**错误中心**查看更多错误码。

11.8.10 CloseDomainSlsConfig

调用CloseDomainSlsConfig接口关闭指定域名的全量日志分析功能。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CloseDomainSlsConfig	系统规定参数。取值：CloseDomainSlsConfig。

名称	类型	是否必选	示例值	描述
Domain	String	是	www.example.com	已启用全量日志分析功能的网站域名。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
Lang	String	否	cn	系统语言ID。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CloseDomainSlsConfig
&Domain=www.example.com
&<公共请求参数>
```

正常返回示例

XML 格式

```
<RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```

JSON 格式

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.8.11 ModifyFullLogTtl

调用ModifyFullLogTtl修改日志存储时长。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyFullLogTtl	系统规定参数。取值：ModifyFullLogTtl。
Ttl	Integer	是	30	日志存储时长，单位：天。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
Lang	String	否	cn	系统语言ID。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyFullLogTtl
&Ttl=30
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

`JSON` 格式

```
{
    "RequestId":"CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

错误码

访问错误中心查看更多错误码。

11.8.12 EmptySlsLogstore

调用EmptySlsLogstore清空日志库。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	EmptySlsLogstore	系统规定参数。取值：EmptySlsLogstore。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
Lang	String	否	cn	系统语言ID。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=EmptySlsLogstore
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

`JSON` **格式**

```
{
    "RequestId":"CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

错误码

访问错误中心查看更多错误码。

11.8.13 ListValueAdded

调用ListValueAdded查看DDoS高防增值服务（全量日志分析）信息。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ListValueAdded	系统规定参数。取值：ListValueAdded。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
ValueAddedList	Array		DDoS高防增值服务信息。
InstanceId	String	ddos_fl_pre-cn-xxxx	服务实例ID。
Status	Integer	1	开通状态： · 0：表示未开通 · 1：表示已开通
ExpireTime	Long	1580918400000	服务到期时间戳，单位：毫秒。
GmtCreate	Long	1575527305000	服务开通时间戳，单位：毫秒。
LogSize	Long	5497558138880	日志库容量，单位：Byte（字节）。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ListValueAdded
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ValueAddedList>
    <Status>1</Status>
    <GmtCreate>1575527305000</GmtCreate>
    <LogSize>5497558138880</LogSize>
    <InstanceId>ddos_fl_pre-cn-xxxx</InstanceId>
    <ExpireTime>1580918400000</ExpireTime>
</ValueAddedList>
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

`JSON` **格式**

```
{
    "ValueAddedList":[{
        "Status":1,
        "GmtCreate":1575527305000,
        "LogSize":5497558138880,
```

```
        "InstanceId":"ddos_fl_pre-cn-xxxx",
        "ExpireTime":1580918400000
    }],
    "RequestId":"CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

错误码

访问错误中心查看更多错误码。

11.8.14 ReleaseValueAdded

调用ReleaseValueAdded释放DDoS高防增值服务实例（全量日志分析功能）。

说明:

该接口将释放全量日志分析服务实例，请谨慎调用。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ReleaseValueAdded	系统规定参数。取值：ReleaseValueAdded。
InstanceId	String	是	ddos_fl_pre-cn-xxxx	增值服务实例ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ReleaseValueAdded
&InstanceId=ddos_fl_pre-cn-xxxx
```

```
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
```

`JSON` **格式**

```
{
    "RequestId":"CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

错误码

访问错误中心查看更多错误码。

11.8.15 DescribeOpEntities

调用DescribeOpEntities查询操作日志。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeOpEntities	要执行的操作。取值：DescribeOpEntities。
EndTime	Long	是	1536715558000	结束时间。格式为时间戳，单位：毫秒。
PageNo	Integer	是	1	页号，即从第几页开始显示。
PageSize	Integer	是	10	分页大小，即每页显示多少条结果。最大值50。
StartTime	Long	是	1534123558000	开始时间。格式为时间戳，单位：毫秒。

名称	类型	是否必选	示例值	描述
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	test	资源组ID。
EntityType	Integer	否	1	过滤条件对象，取值： · 1：表示IP。 · 2：表示抗D包。 · 3：表示ECS。 说明: 结合EntityObject参数，根据指定的过滤条件对象进行精确匹配，筛选操作日志记录。
EntityObject	String	否	xx	过滤条件内容，仅支持精确匹配。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
Total	Long	10	记录总数。
OpEntities	Array		操作日志。
GmtCreate	Long	1536715558000	创建日志的时间戳，单位：毫秒。
EntityType	Integer	1	操作对象类型。取值：1（IP类型）。
EntityObject	String	2.2.2.2	操作对象的值，即操作的IP地址。
OpAction	Integer	1	操作类型。取值：1（修改弹性带宽）。
OpAccount	String	123	操作人。

名称	类型	示例值	描述
OpDesc	String	{"newEntity":{"elasticBandwidth":30},"oldEntity":{"elasticBandwidth":200}}	操作详情。OpDesc的JSON字符串，具体结构描述如下： · oldValue，Struct类型，旧值，具体结构描述如下： - elasticBandwidth，Integer类型，弹性带宽值。 · newValue，Struct类型，新值，具体结构描述如下： - elasticBandwidth，Integer类型，弹性带宽值。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeOpEntities
&EndTime=1536715558000
&PageNo=1
&PageSize=10
&StartTime=1534123558000
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeOpEntitiesResponse>
     <OpEntities>
          <element>
               <entityObject>1.1.1.1</entityObject>
               <gmtCreate>1120384</gmtCreate>
               <opAction>2</opAction>
               <opDesc>
                    <newValue>
                         <elasticBandwidth>30</elasticBandwidth>
                    </newValue>
                    <oldValue>
                         <elasticBandwidth>10</elasticBandwidth>
                    </oldValue>
               </opDesc>
               <opResult>1</opResult>
          </element>
     </OpEntities>
     <Total>10</Total>
</DescribeOpEntitiesResponse>
```

`JSON` **格式**

```
{
  "Total": 10,
```

```
  "OpEntities": [
    {
      "gmtCreate": 1120384,
      "entityObject": "1.1.1.1",
      "opAction": 2,
      "opDesc": {
     "oldValue": {
    "elasticBandwidth": 10
  },
  "newValue": {
    "elasticBandwidth": 30
  }
   },
      "opResult": 1
    }
  ]
}
```

错误码

访问错误中心查看更多错误码。

11.9 标签

11.9.1 TagResources

调用TagResources接口为指定资源（DDoS高防实例）绑定标签。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	TagResources	要执行的操作。取值：TagResources。
RegionId	String	是	cn-hangzhou	DDoS高防实例的地域ID。
ResourceId.N	RepeatLis	是	ddoscoo-cn-v0h1fmwbc024	要操作的DDoS高防实例的ID。n的取值范围为 [1, 50]，用于指定多个实例，最多50个。例如：ResourceId.1，ResourceId.2，...，ResourceId.50。
ResourceType	String	是	INSTANCE	资源的类型，取值：INSTANCE。

名称	类型	是否必选	示例值	描述
ResourceGroupId	String	否	test	资源组ID。
Tag.N.Key	String	否	testKey1	要绑定的标签键。n的取值范围为 [1, 20]，用于指定多个标签键，最多20个。例如：Tag.1.Key，Tag.2.Key，...，Tag.20.Key。
Tag.N.Value	String	否	testValue1	要绑定的标签值。n的取值范围为 [1, 20]，用于指定多个标签值，最多20个。例如：Tag.1.Value，Tag.2.Value，...，Tag.20.Value。

返回数据

名称	类型	示例值	描述
RequestId	String	7078CD1E-F609-47A4-9C39-B288CC27C686	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=TagResources
&RegionId=cn-hangzhou
&ResourceId.1=ddoscoo-cn-v0h1fmwbc024
&ResourceType=INSTANCE
&Tag.1.Key=testKey1
&Tag.1.Value=testValue1
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<TagResourcesResponse>
      <requestId>7078CD1E-F609-47A4-9C39-B288CC27C686</requestId>
</TagResourcesResponse>
```

`JSON` **格式**

```
{
"requestId":"7078CD1E-F609-47A4-9C39-B288CC27C686"
```

```
}
```

错误码

访问错误中心查看更多错误码。

11.9.2 UntagResources

调用UntagResources接口移除指定资源（DDoS高防实例）的标签。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	UntagResources	要执行的操作。取值：UntagResources。
RegionId	String	是	cn-hangzhou	DDoS高防实例的地域ID。
ResourceId.N	RepeatList	是	ddoscoo-cn-v0h1fmwbc024	要操作的DDoS高防实例的ID。n的取值范围为 [1, 50]，用于指定多个实例，最多50个。例如：ResourceId.1，ResourceId.2，...，ResourceId.50。
ResourceType	String	是	INSTANCE	资源类型，取值：INSTANCE。
ResourceGroupId	String	否	test	资源组ID。
TagKey.N	RepeatList	否	testKey1	要移除的标签键。n的取值范围为 [1, 20]，用于指定多个标签键，最多20个。例如：Tag.1.Key，Tag.2.Key，...，Tag.20.Key。
All	Boolean	否	false	是否移除实例上的所有标签。

返回数据

名称	类型	示例值	描述
RequestId	String	F2D86AED-BA27-4584-BADC-B43BDA7EEBCA	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=UntagResources
&RegionId=cn-hangzhou
&ResourceId.1=ddoscoo-cn-v0h1fmwbc024
&ResourceType=INSTANCE
&TagKey.1=testKey1
&All=false
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<UntagResourcesResponse>
      <requestId>F2D86AED-BA27-4584-BADC-B43BDA7EEBCA</requestId>
</UntagResourcesResponse>
```

`JSON` **格式**

```
{
"requestId":"F2D86AED-BA27-4584-BADC-B43BDA7EEBCA"
}
```

错误码

访问错误中心查看更多错误码。

11.9.3 ListTagKeys

调用ListTagKeys接口查询所有标签。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ListTagKeys	要执行的操作。取值：ListTagKeys。
RegionId	String	是	cn-hangzhou	要查询的地域ID。
ResourceType	String	是	INSTANCE	资源类型，取值：INSTANCE。
ResourceGroupId	String	否	test	资源组ID。
PageSize	Integer	否	20	分页查询时设置的每页行数，最大值为50，默认值为10。
CurrentPage	Integer	否	1	列表的页码，起始值为1，默认值为1。

返回数据

名称	类型	示例值	描述
RequestId	String	97935DF1-0289-4AA2-9DD1-72377838B16B	本次请求的ID。
CurrentPage	Integer	1	列表的页码。
PageSize	Integer	20	每页的行数。
TotalCount	Integer	6	标签的总数。
TagKeys	Array		标签信息。
TagKey	String	a	标签键。
TagCount	Integer	1	标签键下标签值的总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ListTagKeys
&RegionId=cn-hangzhou
&ResourceType=INSTANCE
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ListTagKeysResponse>
     <CurrentPage>1</CurrentPage>
     <PageSize>20</PageSize>
     <RequestId>97935DF1-0289-4AA2-9DD1-72377838B16B</RequestId>
     <TagKeys>
          <element>
               <TagCount>1</TagCount>
               <TagKey>a</TagKey>
          </element>
          <element>
               <TagCount>1</TagCount>
               <TagKey>testKey1</TagKey>
          </element>
          <element>
               <TagCount>1</TagCount>
               <TagKey>testKey2</TagKey>
          </element>
          <element>
               <TagCount>2</TagCount>
               <TagKey>testKey3</TagKey>
          </element>
          <element>
               <TagCount>1</TagCount>
               <TagKey>testKey4</TagKey>
          </element>
          <element>
               <TagCount>1</TagCount>
               <TagKey>x</TagKey>
          </element>
     </TagKeys>
     <TotalCount>6</TotalCount>
</ListTagKeysResponse>
```

`JSON` **格式**

```
{
 "RequestId":"97935DF1-0289-4AA2-9DD1-72377838B16B",
    "TotalCount": 6,
    "PageSize": 20,
    "CurrentPage": 1,
    "TagKeys": [
      {
        "TagCount": 1,
        "TagKey": "a"
      },
      {
        "TagCount": 1,
```

```
        "TagKey": "testKey1"
      },
      {
        "TagCount": 1,
        "TagKey": "testKey2"
      },
      {
        "TagCount": 2,
        "TagKey": "testKey3"
      },
      {
        "TagCount": 1,
        "TagKey": "testKey4"
      },
      {
        "TagCount": 1,
        "TagKey": "x"
      }
    ]
  }
```

错误码

访问错误中心查看更多错误码。

11.9.4 ListTagResources

调用ListTagResources接口查询资源（DDoS高防实例）和标签的对应关系。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ListTagResources	要执行的操作。取值：ListTagResources。
RegionId	String	是	cn-hangzhou	DDoS高防实例的地域ID。
ResourceType	String	是	INSTANCE	资源类型，取值：INSTANCE。
ResourceGroupId	String	否	test	资源组ID。

名称	类型	是否必选	示例值	描述
ResourceId.N	RepeatLis	否	ddoscoo-cn-o4017n9q9004	指定要查询的DDoS高防实例ID，查询实例的标签。n的取值范围为 [1, 50]，用于指定多个实例，最多50个。例如：ResourceId.1，ResourceId.2，...，ResourceId.50。  说明: 您必须指定ResourceId或者Tag.Key和Tag.Value组合。
Tag.N.Key	String	否	testKey1	指定要查询的标签键，查询标签下的实例。n的取值范围为 [1, 20]，用于指定多个标签键，最多20个。例如：Tag.1.Key，Tag.2.Key，...，Tag.20.Key。  说明: 您必须指定ResourceId或者Tag.Key和Tag.Value组合。
Tag.N.Value	String	否	testValue1	指定要查询的标签值，查询标签下的实例。n的取值范围为 [1, 20]，用于指定多个标签值，最多20个。例如：Tag.1.Value，Tag.2.Value，...，Tag.20.Value。  说明: 您必须指定ResourceId或者Tag.Key和Tag.Value组合。指定标签值时，必须指定标签键；指定标签键后，标签值可以留空。
NextToken	String	否	RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCffomr	指定下一个查询开始的Token。如果没有下一个查询，请留空。

返回数据

名称	类型	示例值	描述
RequestId	String	C3F7E6AE-43B2-4730-B6A3-FD17552B8F65	本次请求的ID。
NextToken	String	RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCffomr	下一个查询开始的Token。没有下一个查询时为空。
TagResources	Array		资源和标签的关系列表。
ResourceType	String	INSTANCE	资源类型，取值：INSTANCE。
ResourceId	String	ddoscoo-cn-o4017n9q9004	DDoS高防实例ID。
TagKey	String	testKey1	标签键。
TagValue	String	testValue1	标签值。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ListTagResources
&RegionId=cn-hangzhou
&ResourceType=INSTANCE
&ResourceId.1=ddoscoo-cn-o4017n9q9004
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ListTagResourcesResponse>
     <NextToken>RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCffomr</
NextToken>
     <RequestId>C3F7E6AE-43B2-4730-B6A3-FD17552B8F65</RequestId>
     <TagResources>
          <TagResource>
               <element>
                    <ResourceId>ddoscoo-cn-o4017n9q9004</ResourceId>
                    <ResourceType>INSTANCE</ResourceType>
                    <TagKey>testKey4</TagKey>
                    <TagValue>testValue4</TagValue>
               </element>
```

```
            </TagResource>
        </TagResources>
</ListTagResourcesResponse>
```

JSON 格式

```
{
    "RequestId":"C3F7E6AE-43B2-4730-B6A3-FD17552B8F65",
 "NextToken": "RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCffomr",
    "TagResources": {
      "TagResource": [
        {
          "ResourceId": "ddoscoo-cn-o4017n9q9004",
          "TagKey": "testKey4",
          "ResourceType": "INSTANCE",
          "TagValue": "testValue4"
        }
      ]
    }
  }
```

错误码

访问错误中心查看更多错误码。

11.10 事件任务

11.10.1 ListAsyncTask

调用ListAsyncTask查询异步任务列表。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ListAsyncTask	系统规定参数。取值：ListAsyncTask。
PageNo	Integer	是	1	当前页数，从1开始。
PageSize	Integer	是	10	分页大小，最大值20。
Lang	String	否	cn	系统语言ID。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	xx	资源组ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
AsyncTasks	Array		任务列表。
EndTime	Long	1533866201000	任务结束时间戳，单位：毫秒。
StartTime	Long	1533866201000	任务开始时间戳，单位：毫秒。
TaskId	Long	123	任务ID，使用该ID可进行任务的删除操作。
TaskParams	String	{"instanceId": "ddoscoo-1234-qrq2134"}	任务执行参数，为一个JSONObject类型的字符串，具体结构描述如下： · instanceId，String类型，新BGP高防实例ID。 · domain，String类型，用户域名。
TaskResult	String	{"instanceId": "ddoscoo-1234-qrq2134", "url": "https://oss.xxx.xxx"}	任务执行结果，JSONObject类型的字符串，具体结构描述如下： · instanceId，String类型，新BGP高防实例ID。 · url，String类型，文件下载OSS地址。
TaskStatus	Integer	1	任务状态，取值： · 0：任务初始化 · 1：任务进行中 · 2：任务成功 · 3：任务失败

名称	类型	示例值	描述
TaskType	Integer	1	任务类型，取值： · 1：4层转发规则批量导出任务 · 2：7层防护规则批量导出任务 · 3：会话和健康检查配置导出任务 · 4：DDoS防护策略导出任务
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
Total	Integer	10	域名总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ListAsyncTask
&PageNo=1
&PageSize=10
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ListAsyncTaskResponse>
     <AsyncTasks>
          <element>
               <EndTime>156927362</EndTime>
               <StartTime>156927362</StartTime>
               <TaskId>1</TaskId>
               <TaskParams></TaskParams>
               <TaskResult></TaskResult>
               <TaskStatus>2</TaskStatus>
               <TaskType>1</TaskType>
          </element>
     </AsyncTasks>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
     <Total>2</Total>
</ListAsyncTaskResponse>
```

`JSON` **格式**

```
{
 "AsyncTasks":[
  {
   "TaskResult":"{}",
   "TaskStatus":2,
   "EndTime":156927362,
   "StartTime":156927362,
```

```
    "TaskId":1,
    "TaskParams":"{}",
    "TaskType":1
   }
  ],
  "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
  "Total":2
}
```

错误码

访问错误中心查看更多错误码。

11.10.2 CreateAsyncTask

调用CreateAsyncTask创建异步任务。

创建新BGP合作机房支持的异步任务，当前支持7层配置的导出、4层配置的导出以及会话保持、健康检查等功能配置的导出。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateAsyncTask	系统规定参数。取值：CreateAsyncTask。

名称	类型	是否必选	示例值	描述
TaskParams	String	是	{"timestamp": 1530276554, "instanceId": "ddoscoo-woieuroi234"}	任务参数，一组json字符串，根据TaskType不同有所区别。 · TaskType为1时，传入需要导出规则的新BGP高防实例Id。例如，{"instanceId": "ddoscoo-cn-XXXXX"} · TaskType为2时，传入一个空对象的字符串即可。例如，{} · TaskType为3时，传入需要导出规则的新BGP高防实例Id。例如，{"instanceId": "ddoscoo-cn-XXXXX"} · TaskType为4时，传入需要导出规则的新BGP高防实例Id。例如，{"instanceId": "ddoscoo-cn-XXXXX"}
TaskType	Integer	是	1	任务类型，取值： · 1：4层转发规则批量导出任务 · 2：7层防护规则批量导出任务 · 3：会话和健康检查配置导出任务 · 4：DDoS防护策略导出任务
RegionId	String	否	cn-hangzhou	地域ID。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateAsyncTask
```

```
&TaskParams={"timestamp": 1530276554, "instanceId": "ddoscoo-
woieuroi234"}
&TaskType=1
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<CreateAsyncTaskResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</CreateAsyncTaskResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.10.3 DeleteAsyncTask

调用DeleteAsyncTask删除指定的异步任务。

调试

您可以在*OpenAPI Explorer*中直接运行该接口，免去您计算签名的困扰。运行成功后，*OpenAPI Explorer*可以自动生成*SDK*代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteAsyncTask	系统规定参数。取值：DeleteAsyncTask。
TaskId	Integer	是	123	要删除的任务ID。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteAsyncTask
&TaskId=123
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DeleteAsyncTaskResponse>
     <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DeleteAsyncTaskResponse>
```

`JSON` **格式**

```
{
 "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

11.11 错误码

错误代码	描述	语义
InvalidOrderType	Invalid Order Type.	无效的订单类型。
InvalidBaseBandwidth	Invalid Base Bandwidth.	无效的基础带宽。
InvalidElasticBandwidth	Invalid Elastic Bandwidth.	无效的弹性带宽。
InvalidPortLimit	Invalid Port Limit.	无效的端口数量。
InvalidDomainLimit	Invalid Domain Limit.	无效的域名数量。
InvalidNormalBandwidth	Invalid Normal Bandwidth.	无效的业务带宽。
InvalidInstanceId	Invalid Instance Id.	无效的实例ID。

错误代码	描述	语义
InvalidAliUid	Invalid Ali Uid.	无效的aliUid。
InstanceIdFormatError	Instance Id format error.	实例ID格式错误。
InvalidPageNo	Invalid Page No.	无效的页号。
InvalidPageSize	Invalid Page Size.	无效的分页大小。
InvalidLine	Invalid Line.	无效的合营资源。
InvalidStatus	Invalid Status.	无效的状态。
InvalidExpireTime	Invalid Expire Time.	无效的过期时间。
InvalidProductType	Invalid Product Type.	无效的产品类型。
InvalidStartTime	Invalid Start Time.	无效的开始时间。
InvalidEndTime	Invalid End Time.	无效的结束时间。
InvalidInstanceIdsSize	Invalid instanceIds size.	实例ID个数超长。
InvalidInstanceRemark	Invalid instance remark.	无效的实例备注。
InternalError	Internal Error!	内部错误。
ddos_coop3000	unknown error	未知错误。
ddos_coop3001	error request method	无效的请求方式。
ddos_coop3002	http call failed	http请求调用失败。
ddos_coop3003	no authority to do request	无权请求。
ddos_coop3004	receive unknown action	无效的操作请求。
ddos_coop3005	auth failed	认证失败。
ddos_coop3006	query db failed	查询数据库失败。
ddos_coop3007	remote call selb central failed	调用中心管控服务失败。
ddos_coop3008	remote call ddos web failed	调用服务失败。
ddos_coop3101	encoding json failed	编码失败。
ddos_coop3102	decoding json failed	解码失败。
ddos_coop3103	failed parse string to int	从字符串解析数字失败。
ddos_coop3201	no enough params in request	传入的参数不足。
ddos_coop3202	params out of range	传入的参数超出允许的范围。

错误代码	描述	语义
ddos_coop3203	start time must less then end time	开始时间必须早于结束时间。
ddos_coop3301	no instance for process in db	在数据库中未找到指定实例。
ddos_coop3302	reache port limit in spec	达到端口规格上限。
ddos_coop3303	l4 rule port is exist	转发规则已存在。
ddos_coop3304	invalid rs ip address	无效的IP地址信息。
ddos_coop12001	backend service exception	服务异常。
ddos_coop12003	system exception	系统异常。
ddos_coop12010	illegal sign	无效签名。
ddos_coop12020	illegal timestamp	无效时间戳。
ddos_coop12030	illegal format	无效数据返回格式。
ddos_coop12040	illegal service	服务不存在。
ddos_coop12052	illegal aliyun idkp	aliUid参数没传或为空。
ddos_coop12302	listener not exists	指定监听不存在。
ddos_coop12610	lb or vs 或not exist	指定LB或监听不存在。
ddos_coop13000	db failed	数据库连接异常。
ddos_coop13001	failed	配置参数错误。
ddos_coop13010	json err	格式错误。
ddos_coop13020	param not enough	配置参数缺失。
ddos_coop13104	eip is released	ip已被释放。
ddos_coop13105	eip not exist	ip不存在。
ddos_coop15001	action not exist	指定操作不存在。
ddos_coop16020	auth fail	身份验证失败。
ddos_coop20403	auth failed	认证失败。
ddos_coop20404	not found	服务未发现。
ddos_coop21001	invalid parameter	无效参数。
ddos_coop21002	invalid method	无效方法。
ddos_coop21003	invalid product	无效产品。
ddos_coop21004	invalid region	无效区域。

错误代码	描述	语义
ddos_coop21005	no action found	无此操作。
ddos_coop21006	invalid action	无效操作。
ddos_coop221007	action disabled	接口被禁用。
ddos_coop29999	system error	系统错误。