阿里云
DDoS防护

DDoS高防

文档版本：20200528

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。
斜体	表示参数、变量。	bae log list --instanceid Instance_ID
[]或者[a|b]	表示可选项，至多选择一个。	ipconfig [-all|-t]
{}或者{a|b}	表示必选项，至多选择一个。	switch {active|stand}

目录

1 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。

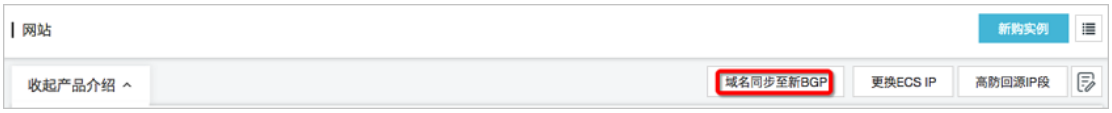
2. 将业务配置迁移至新BGP高防IP实例。

- **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。

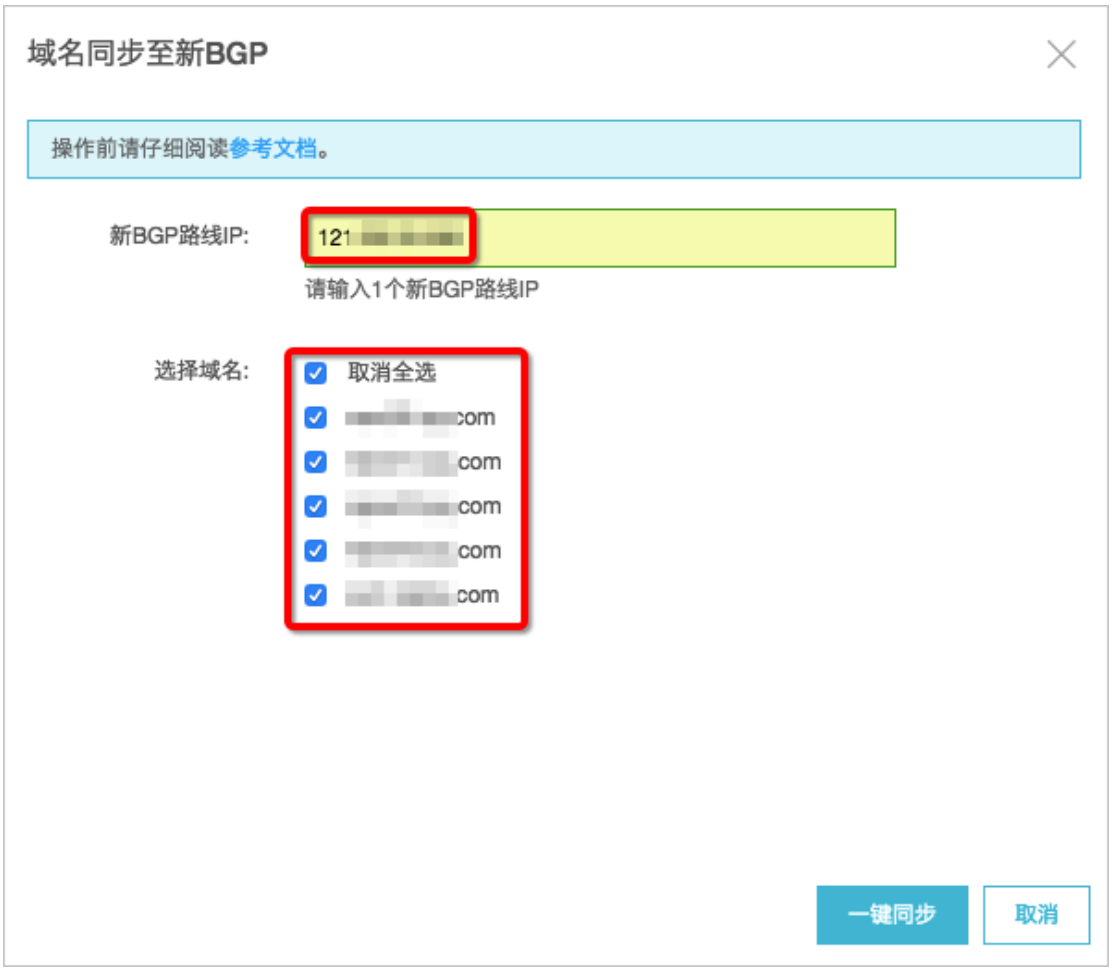
  a. 定位到**接入 > 网站**，单击**域名同步至新BGP**。

  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）。
- 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。

2 产品简介

2.1 什么是DDoS高防

DDoS高防（Anti-DDoS Pro/Premium）是阿里云提供的DDos攻击代理防护服务。当用户的互联网服务器遭受大流量的DDos攻击时，DDoS高防可以保护其应用服务持续可用。DDoS高防通过DNS解析调度流量到阿里云高防网络，代理接入阿里云DDoS防护系统，抵御流量型和资源耗尽型DDoS攻击。

DDoS高防-新BGP/国际

DDoS高防为用户业务服务器部署在中国内地、海外及港澳台地区的场景分别提供更有效的解决方案：

- DDoS高防（新BGP）：采用中国内地独有的T级八线BGP带宽资源，为部署在**中国内地**且主要目标用户为**中国内地**用户的业务防御超大流量DDoS攻击。
- DDoS高防（国际）：依托世界领先的分布式近源清洗能力，为部署在**海外及港澳台地区**且主要目标用户为**海外及港澳台地区**用户的业务提供不设上限的DDoS攻击全力防护能力。

工作原理

DDoS高防支持通过DNS解析和IP直接指向两种引流方式，实现网站域名和业务端口的接入防护。根据用户在DDoS高防服务中为业务配置的转发规则，DDoS高防将业务的DNS域名解析或业务IP指向DDoS高防实例IP或CNAME地址进行引流。

来自公网的访问流量都将优先经过高防机房，恶意攻击流量将在高防流量清洗中心进行清洗过滤，正常的访问流量通过端口协议转发的方式返回给源站服务器，从而保障源站服务器的稳定访问。

产品优势

与传统DDoS攻击安全解决方案相比，阿里云DDoS高防具有部署简便、BGP网络质量高、防护能力大、系统稳定可用，以及先进的AI智能防护技术等优势。

- 部署简便-五分钟完成部署

  根据用户业务特性，提供DNS解析和IP直接指向两种接入方式，实现网站域名和业务端口的接入防护。无需安装任何软硬件或调整路由配置，五分钟内即可完成部署和激活。

- 海量防御带宽资源

  DDoS高防拥有中国内地超过8T、海外及港澳台地区超过2T的海量防御带宽资源。

- AI智能防护

  在流量清洗技术方面，分别针对网络流量型攻击和资源耗尽型DDoS攻击，通过自动优化防护算法和深度学习业务流量基线，达到精准识别攻击IP并自动过滤清洗的目的。

- 网络流量型DDoS攻击防护

  大量针对网络传输层的攻击会使网络堵塞、机房不可用，而使用户业务中断或大面积瘫痪。在传统的代理、探测、反弹、认证、黑白名单、报文合规等标准技术的基础上，DDoS高防结合IP信誉、近源清洗，以及通过对网络指纹、用户行为、内容特征的深度包检测等多种技术的应用，可实现对威胁进行阻断和自定义过滤，并保证被防护的业务在遭受持续攻击时，仍可对外正常提供服务。

- 资源耗尽型DDoS攻击防护（CC攻击）

  当攻击使网络应用层的服务器业务中断时，DDoS高防将对应用层的资源耗尽型DDoS攻击全面集成AI智能防护引擎，通过自定义过滤频率和精细至URL级别的过滤特征来提升防护效率和成功率，同时也大大降低了安全运维人员的工作难度。AI智能防护引擎基于以下特征进行防护：

  - 自学习用户业务流量和特征
  - 动态生成正常业务基线
  - 快速发现流量和特征异常
  - 自动介入分析攻击特征
  - 自动生成多维度组合策略
  - 动态执行/撤销防护策略指令

- 稳定、可靠性强

  - DDoS高防采用高可用网络防护集群，避免单点故障和冗余，且处理性能支持弹性扩展。
  - 对流量清洗机房的所有入流量、所有服务器CPU和内存进行监控，保障机房可用性。同时，针对服务器的引擎进行可用状态监控，并且具备自动下线和恢复机制。
  - 针对回源链路进行可用性监控，一旦发现不稳定，自动切换至备用链路，保障链路可用性。
  - 针对接入防护的源站服务器进行健康检查，一旦发现异常，自动切换。针对源站服务器的HTTP状态码进行监控，发现异常后自动启用回源或者切换等操作。

- 具备流量调度能力

  阿里云DDoS高防服务可基于云产品的安全事件，通过DNS解析进行流量调度，实现在其他云产品未遭受DDoS攻击时不启用DDoS防护，而在遭受DDoS攻击时可以快速关联DDoS高防资源并启用DDoS防护功能。用户可根据自己的业务场景自定义配置调度模版，实现与云产品联动，自动化调度DDoS防护能力。流量调度模版包括：云产品联动、阶梯防护、中国内地出海加速等。

应用场景

阿里云DDoS高防适用于金融、电商、门户类网站，政府互联网出口、门户与开放平台，重大线上直播、活动推广促销的DDoS攻击防护场景，以及业务遭竞争对手恶意攻击、勒索，移动业务遭恶意注册、刷单、刷流量等安全防护场景。

在上述行业中，当业务存在以下安全风险时，推荐您使用阿里云DDoS高防：

- 遭受恶意攻击者的DDoS攻击勒索
- DDoS攻击已经导致业务不可用，需要紧急恢复
- 频繁遭受DDoS攻击，需要持续防护DDoS攻击，保护业务的稳定性

2.2 DDoS高防（新BGP）

DDoS高防（新BGP）服务采用中国内地独有的T级八线BGP带宽资源，为用户业务服务器部署在中国内地的场景，提供超大流量DDoS攻击的防御服务。相比静态IDC高防IP服务，DDoS高防（新BGP）天然具有灾备能力、线路更稳定、访问速度更快。

产品优势

DDoS高防（新BGP）服务具有以下优势：

- 拥有中国内地最大的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。
- 拥有中国内地最优质的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，即可满足中国内地不同运营商线路的快速访问和DDoS防护需求。

DDoS高防（新BGP）服务VS静态IDC高防IP服务

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（新BGP）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线路。
线路质量	中国内地平均访问时延在30ms左右，且对于小运营商可能存在跨网访问。	中国内地平均访问时延在20ms左右，且不存在运营商跨网访问。	中国内地平均访问时延在20ms左右，且不存在运营商跨网访问。

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（新BGP）服务
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。
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，以及空连接、真实傀儡机连接等攻击。	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。

应用场景

如果您有以下DDoS防护需求，建议您选购DDoS高防（新BGP）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300G以上大流量DDoS攻击的防护需求。

相关文档

- 计费方式
- 开通DDoS高防（新BGP）实例

2.3 DDoS高防（国际）

针对用户业务服务器部署在海外及港澳台地区的场景，阿里云提供DDoS高防（国际）服务，帮助业务降低DDoS攻击风险。

业务接入DDoS高防（国际）服务后，服务器遭受的攻击流量将被牵引至DDoS高防（国际）的独享IP。DDoS高防（国际）使用世界领先的分布式近源清洗方式清洗攻击流量，并将过滤后的正常流量返回至源站服务器，保障业务稳定运行。

功能特性

DDoS高防（国际）支持以下DDoS攻击防御功能。

功能项	描述
过滤畸形报文	过滤Frag flood、Smurf、stream flood、Land flood攻击，过滤IP畸形包、TCP畸形包、UDP畸形包等畸形报文。
防御传输层DDoS攻击	过滤Syn flood、Ack flood、UDP flood、ICMP flood、Rst flood等攻击。
防御Web应用DDoS攻击	过滤HTTP Get flood、HTTP Post flood、高频攻击。同时，支持根据HTTP特征、URI、Host等自定义更精细的访问控制规则。

产品优势

DDoS高防（国际）服务具有以下优势：

- 全球近源清洗

  通过Anycast通信模式充分利用全球各地阿里云流量清洗中心的能力作为DDoS高防（国际）服务的资源，采用分布式技术将DDoS攻击流量自动牵引至距离攻击源最近的流量清洗中心进行过滤，在将防护能力进行整合实现最大化的同时，也具备多机房备份容灾的能力。
- 无上限全力防护

  与DDoS高防（新BGP）服务不同，DDoS高防（国际）服务依托全球近源清洗能力，为每位用户提供不设上限的全力防护。

  注意：
  如果您的业务遭受的攻击影响到阿里云海外高防清洗中心的基础设施，则阿里云保留压制流量的权利。DDoS高防（国际）实例受到流量压制时，可能对您的业务造成一定影响，例如业务访问流量可能会被限速，甚至被黑洞。

- 独享IP资源

  DDoS高防（国际）服务为每位用户提供一个独享Anycast IP，各IP之间互相隔离，避免其它用户遭受的DDoS攻击对您的业务产生任何误伤，为您提供更加安全的DDoS防护服务。

- 安全防护报表

  DDoS高防（国际）服务为您实时提供详细的流量报表和攻击防护详细信息，让您及时、准确地了解当前业务的安全状态。

应用场景

互联网Internet通过各地网络运营商互联来实现全球范围内的互通访问，但由于各个区域的网络运营商的策略不同，导致网络访问互通的实际情况各不相同。因此您需要根据不同的业务场景选择最合适的DDoS安全防护解决方案。

说明：

基于当前网络运营商的路由互联策略，默认情况下从中国内地访问海外DDoS高防资源时，单独使用DDoS高防（国际）服务无法保证网络链路质量。

这种场景存在的问题包括：访问平均延迟高达300ms，并且可能受国际链路拥塞影响而导致间歇性丢包。因此，强烈建议您在中国内地部署服务器来服务中国内地用户，同时使用DDoS高防（新BGP）服务解决DDoS安全防护问题，并且遵守相关中国法律法规完成网站备案等合规手续。

对于服务器部署在海外及港澳台的业务，主要分为以下三个场景。

场景	推荐方案
业务服务器部署在**海外及港澳台**地区，且主要服务于**海外及港澳台**地区的用户	购买DDoS高防（国际）服务缓解DDoS攻击。

场景	推荐方案
业务服务器部署在**海外及港澳台**地区，主要服务于**中国内地**的用户	• 方案一 如果您的业务对网络延迟要求比较高（例如游戏业务服务器），建议您将服务器迁移至您的主要用户所在的中国内地地区，并且购买DDoS高防（新BGP）服务来缓解DDoS攻击。 • 方案二 如果您的业务服务器暂时无法迁移到中国内地，建议您联系销售或通过工单申请购买DDoS高防（国际）加速线路。开通后，阿里云技术支持人员将协助您完成DDoS高防智能切换方案配置，实现在无DDoS攻击时通过加速线路保障中国内地用户访问顺畅的需求。关于DDoS高防（国际）加速线路配置，请参见配置DDoS高防（国际）加速线路。
业务服务器部署在**海外及港澳台**地区，同时服务**中国内地**和**海外及港澳台**地区的用户	• 方案一 建议您分区域部署业务服务器，用部署在中国内地的服务器服务中国内地用户，部署在海外及港澳台地区的服务器服务海外及港澳台地区用户。同时，通过购买DDoS高防（新BGP）服务和DDoS高防（国际）服务分别保护中国内地和海外及港澳台地区的业务，缓解DDoS攻击。 • 方案二 如果您的业务服务器暂时无法迁移到中国内地，建议您联系销售或通过工单申请购买DDoS高防（国际）加速线路。开通后，阿里云技术支持人员将协助您完成DDoS高防智能切换方案配置，实现在无DDoS攻击时通过加速线路保障中国内地用户访问顺畅的需求。关于DDoS高防（国际）加速线路配置，请参见配置DDoS高防（国际）加速线路。

相关文档

- 计费方式
- 开通DDoS高防（国际）实例

- 配置DDoS高防（国际）加速线路

2.4 DDoS攻击损失保障

DDoS高防支持“DDoS攻击损失保障”服务，防止由于DDoS攻击导致您受DDoS高防保护的云服务器ECS、负载均衡SLB实例因使用量激增而产生额外的费用。如果为了响应DDoS攻击，这些受保护的实例产生了额外的后付费流量，您可以提交工单申请代金券补偿。

3 产品定价

3.1 DDoS高防（新BGP）

3.1.1 计费方式

本文介绍了DDoS高防（新BGP）服务的计费方式，以及实例规格和实例到期的相关说明。

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	4,467,600元/年（包年优惠价）	4,563,600元/年（包年优惠价）

说明：

- 关于标准功能和增强功能套餐间的区别，请参见功能套餐。
- 如果您需要更高的DDoS防护能力，请通过工单联系我们。

DDoS高防（新BGP）实例默认包含下表描述的业务规格。如果您的实际业务需要超出实例的默认业务规格，您可以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

业务规格	规格说明	默认情况	扩展单价（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	100Mbps	每Mbps：100元/月 **说明：** 当实例的总业务带宽规格超出600Mbps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	3,000QPS	每100QPS：1,000元/月

说明：

- 关于业务带宽的详细说明，请参见业务带宽。
- 关于防护域名数的详细说明，请参见防护域名数。

弹性防护（按天-后付费）

DDoS高防（新BGP）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（新BGP）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（新BGP）实例也将不具备弹性防护能力。

例如，您的DDoS高防（新BGP）实例的保底防护带宽规格是30Gbps，弹性防护带宽规格是100Gbps。当日该实例遭受两次DDoS攻击，其中一次攻击的峰值为80Gbps，另一次攻击的峰值为40Gbps，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80Gbps，并扣除

实例的保底防护带宽30Gbps，得到50Gbps，按照“40Gbps<攻击峰值≤50Gbps”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
0Gbps<攻击峰值≤5Gbps	¥800 / 天
5Gbps<攻击峰值≤10Gbps	¥1,200 / 天
10Gbps<攻击峰值≤20Gbps	¥2,200 / 天
20Gbps<攻击峰值≤30Gbps	¥3,600 / 天
30Gbps<攻击峰值≤40Gbps	¥4,880 / 天
40Gbps<攻击峰值≤50Gbps	¥6,400 / 天
50Gbps<攻击峰值≤60Gbps	¥7,800 / 天
60Gbps<攻击峰值≤70Gbps	¥9,200 / 天
70Gbps<攻击峰值≤80Gbps	¥10,600 / 天
80Gbps<攻击峰值≤100Gbps	¥11,800 / 天
100Gbps<攻击峰值≤150Gbps	¥14,600 / 天
150Gbps<攻击峰值≤200Gbps	¥21,600 / 天
200Gbps<攻击峰值≤300Gbps	¥28,000 / 天
300Gbps<攻击峰值≤400Gbps	¥40,000 / 天
400Gbps<攻击峰值≤500Gbps	¥50,000 / 天
500Gbps<攻击峰值≤600Gbps	¥60,000 / 天
600Gbps<攻击峰值≤700Gbps	¥70,000 / 天
700Gbps<攻击峰值≤800Gbps	¥80,000 / 天
800Gbps<攻击峰值≤900Gbps	¥90,000 / 天
900Gbps<攻击峰值≤1000Gbps	¥100,000 / 天
1000Gbps<攻击峰值≤1100Gbps	¥110,000 / 天
1100Gbps<攻击峰值≤1200Gbps	¥120,000 / 天

计费区间	弹性防护费用
1200Gbps<攻击峰值≤1300Gbps	¥130,000 / 天
1300Gbps<攻击峰值≤1400Gbps	¥140,000 / 天
1400Gbps<攻击峰值≤1500Gbps	¥150,000 / 天

不支持退款声明

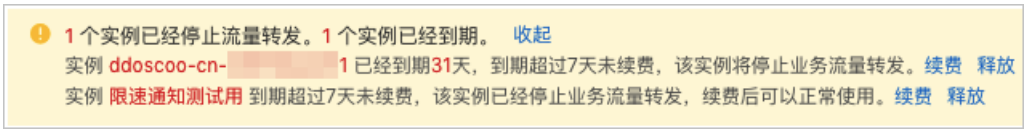
阿里云DDoS高防（新BGP）包年包月服务不支持提前退订，也不适用五天无理由退款。若您已使用了DDoS高防（新BGP）实例，一概不支持退款。

实例到期说明

- DDoS高防（新BGP）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。
- 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DDoS高防（新BGP）服务。
  - 阿里云将定期进行资源回收。如果实例到期超过七天且未及时续费，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。



- DDoS高防（新BGP）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。
  - 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。
  - 实例到期后，您将收到实例保留可用状态七天的通知，提醒您及时续费。
  - 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。

3.2 DDoS高防（国际）

3.2.1 计费方式

本文介绍了DDoS高防（国际）服务的计费方式，以及实例规格和实例到期的相关说明。

高级防护（无上限全力防护）

DDoS高防（国际）的高级防护以成功防护每一次DDoS攻击为目标，整合阿里云海外地区所有高防清洗中心能力全力保护用户业务。

大部分情况显示，持续使用DDoS高防服务并成功防护攻击的用户遭受攻击的风险将明显下降。一般来说，恶意攻击者发起攻击的目的是为了对目标业务造成损失。由于发起攻击本身也存在成本，如果攻击始终无法达到目的，攻击便会停止。因此，DDoS高防（国际）的高级防护不设防护上限，调用阿里云海外地区所有高防清洗中心能力，全力保障用户业务。

注意：

如果您的业务遭受的攻击影响到阿里云海外高防清洗中心的基础设施，则阿里云保留压制流量的权利。DDoS高防（国际）实例受到流量压制时，可能对您的业务造成一定影响，例如业务访问流量可能会被限速，甚至被黑洞。

套餐版本

DDoS高防（国际）服务提供**保险版**和**无忧版**两种套餐版本。

- **保险版**

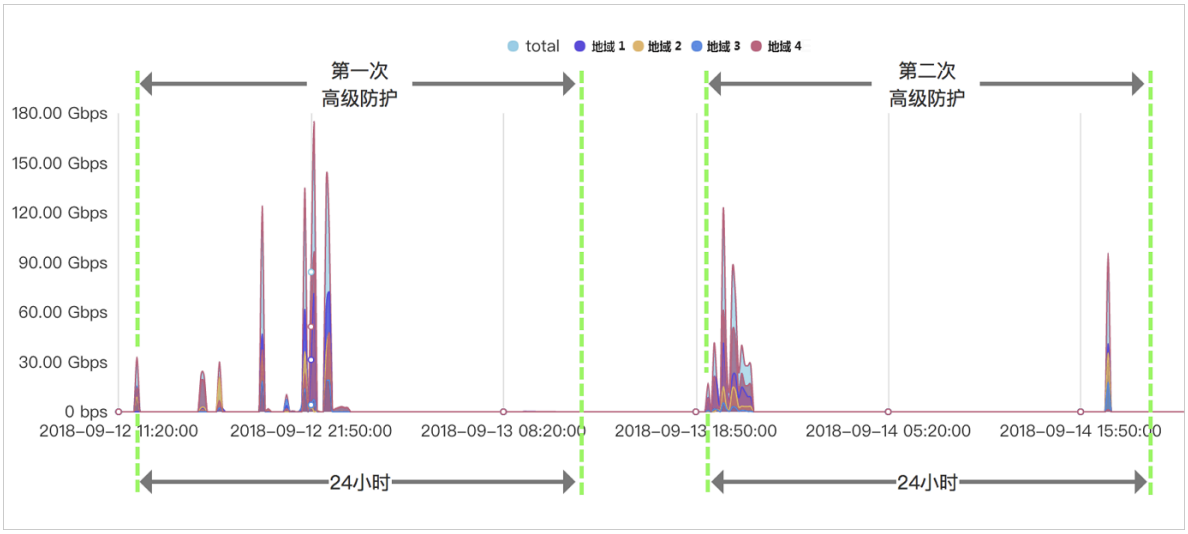
  DDoS高防（国际）保险版包含每月两次高级防护（无上限全力防护），自遭受流量攻击起24小时内为您的业务提供无上限全力防护，并消耗一次高级防护使用次数。每月初您的DDoS高防（国际）实例的高级防护使用次数将自动重置为两次。

  说明：

  如果您需要更多高级防护次数，可额外购买全局高级防护。更多信息，请参见全局高级防护次数。

  例如，自9月12日11:20:00起所防护的IP遭到流量攻击，触发高级防护，24小时内DDoS高防（国际）为该业务提供无上限全力防护。9月13日18:50:00该业务再次遭受流量攻击并触发高级防

护，24小时后无上限全力防护结束，且9月两次高级防护使用次数全部消耗。DDoS高防（国际）保险版实例的高级防护使用次数将在下月初（10月1日）自动重置。



保险版作为DDoS高防（国际）的入门方案，适用于受攻击风险较低的用户。

- **无忧版**

  DDoS高防（国际）无忧版为您提供无限次高级防护（无上限全力防护）。选购无忧版套餐，您无需担心攻击大小和攻击次数，DDoS高防（国际）服务将全面为您的业务保驾护航。

产品定价

DDoS高防（国际）实例的具体定价如下表所示。

套餐类型	业务带宽	高级防护	单价（元/月）
保险版	100Mbps	2次/月	17,500
无忧版		无限次	77,000
保险版	150Mbps	2次/月	22,750
无忧版		无限次	84,000
保险版	200Mbps	2次/月	28,000
无忧版		无限次	91,000
保险版	250Mbps	2次/月	33,250
无忧版		无限次	98,000
保险版	300Mbps	2次/月	37,100
无忧版		无限次	105,000

说明：

业务带宽指无攻击情况下DDoS高防（国际）实例支持处理的最大正常业务带宽。请确保实例的业务带宽大于所需接入实例防护的所有业务的网络入、出方向总流量峰值中较大的值。如果接入防护的正常业务带宽超出了DDoS高防（国际）实例的业务带宽规格，则会出现限流、随机丢包等现象，可能导致您的正常业务在一定时间内不可用、卡顿、延迟。

关于业务带宽的详细说明以及如何选择合适的业务带宽，请参见业务带宽。

如果您需要更高的业务带宽规格，请联系阿里云技术支持人员。

DDoS高防（国际）实例默认包含下表描述的业务规格。如果您的实际业务需要超出实例的默认业务规格，您可以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	5个	每5个端口：1,000元/月
防护域名数	实例支持添加的HTTP/HTTPS域名数量	10个 **说明：** 最多涉及一个一级域名。即所添加的域名所属的一级域名总数不超过1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	• 保险版：500QPS • 无忧版：1,000QPS	每100QPS：1,000元/月

说明：

关于防护域名数的详细说明，请参见防护域名数。

不支持退款声明

阿里云DDoS高防（国际）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（国际）实例，一概不支持退款。

到期说明

- DDoS高防（国际）服务距离到期时间前的29、27、3、1天，会通过短信/邮件的形式提醒您服务即将到期，并提醒您续费。

- 如果DDoS高防（国际）服务到期后没有续费，DDoS防护会恢复到默认的免费防护能力。
- 服务到期后，您的DDoS高防（国际）相关配置为您保留一个月（30天）。一个月内完成续费，则可继续使用原DDoS高防（国际）实例。一个月后，DDoS高防（国际）实例自动释放，服务将不可用。

3.2.2 加速线路

加速线路用于降低中国大陆地区用户对您部署在非中国大陆地区业务的访问延迟，大幅提升在无攻击情况下的访问质量。如果您的业务服务器部署在非中国大陆地区，则您可以为已开通的DDoS高防（国际）实例加购加速线路，实现中国大陆地区用户对您业务的访问加速。

说明：

加速线路不支持单独配置使用。加速线路实例本身不具备任何防护能力，因此必须与DDoS高防（国际）保险版或无忧版实例搭配使用。

关于加速线路的推荐应用场景，请参见应用场景。

购买加速线路实例后，您可以将加速线路与已购买的DDoS高防（国际）保险版或无忧版实例搭配使用，实现无攻击状态下业务针对中国大陆地区用户的加速访问。更多信息，请参见配置DDoS高防（国际）加速线路。

产品定价

DDoS高防（国际）加速线路的具体定价如下表所示。

业务带宽	单价（元/月）
10Mbps	10,000
20Mbps	20,000
30Mbps	30,000
40Mbps	40,000
50Mbps	50,000
60Mbps	60,000
70Mbps	70,000
80Mbps	80,000
90Mbps	90,000
100Mbps	100,000

说明：

业务带宽指无攻击情况下DDoS高防（国际）加速线路实例支持处理的最大正常业务带宽。请确保实例的业务带宽大于所需接入加速线路实例的所有业务的网络入、出方向总流量峰值中较大的值。如果接入防护的正常业务带宽超出了DDoS高防（国际）加速线路实例的业务带宽规格，则会出现限流、随机丢包等现象，可能导致您的正常业务在一定时间内出现不可用、卡顿、延迟等问题。

到期说明

- 服务距离到期时间前的29、27、3、1天，会通过短信/邮件的形式提醒您服务即将到期，并提醒您续费。
- 如到期后没有续费，加速线路实例将停止提供访问加速能力。
- 服务到期后您的加速线路实例相关配置为您保留一个月。一个月内完成续费，则可继续使用原加速线路实例。一个月后，加速线路实例自动释放，服务将不可用。

3.2.3 全局高级防护次数

如果DDoS高防（国际）保险版实例当月提供的两次高级防护次数已耗尽，您可以额外购买全局高级防护次数，获得更多高级防护（无上限全力防护）使用次数。

背景信息

DDoS高防（国际）保险版实例默认包含每月两次的高级防护（无上限全力防护），自遭受流量攻击起24小时内为您的业务提供无上限全力防护，并消耗一次高级防护使用次数。

如果所防护的业务遭受频繁的大流量攻击，保险版实例默认的两次高级防护可能无法完全保证业务的可用性，您可以购买全局高级防护补充您账号中所有DDoS高防（国际）保险版实例的高级防护使用次数。

下表描述了全局高级防护与DDoS高防（国际）实例高级防护之间的区别。

类型	所属范围	有效期	使用次数
无忧版实例高级防护	实例	根据实例有效期	无限次
保险版实例高级防护	实例	一个月 **说明：** 当月未消耗的高级防护次数在下月初将被清空。	两次/月
全局高级防护	云账号	一年	单独购买

产品定价

全局高级防护的具体定价如下表所示。

定价参数	说明
付费方式	预付费
有效时长	1年
购买单价	10,500元/次

注意：

全局高级防护次数不支持退款。

使用说明

当您的保险版实例当月默认的两次高级防护次数耗尽后，如果所防护的业务再次遭受大流量攻击且攻击流量超过基础防护阈值时，将消耗您所购买的全局高级防护次数为业务提供高级防护（无上限全力防护）。

全局高级防护次数无需绑定实例，可供您账号中所有符合使用条件的保险版实例使用。

使用条件

- 保险版实例在有效期内。
- 账号的高级防护功能未冻结。

说明：

当您账号中所有实例当月消耗的高级防护次数（包含当月已消耗的全局高级防护次数）已经超过10次，高级防护功能将自动被冻结，需要等到下个自然月方能恢复使用。

如果您的业务确实频繁遭受大流量攻击，建议您选购无忧版实例进行防护。

购买全局高级防护次数

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**非中国大陆**地域。
3. 在左侧导航栏，单击**资产管理** > **实例管理**。
4. 在**实例列表**右上方，单击**购买**。

5. 在全局高级防护购买页面中，选择需要购买的全局高级防护次数，单击**立即购买**。

> **说明：**
> 购买时请确认所选择的适用产品是**DDoS高防（国际）**。

6. 完成支付。

3.3 功能套餐

DDoS高防（新BGP/国际）提供标准功能和增强功能两种功能套餐。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，选择合适的功能套餐。

购买DDoS高防（新BGP/国际）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。更多信息，请参见升级DDoS高防实例规格。

> **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

下表描述了标准功能套餐和增强功能套餐在具体功能上的差异。

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。 更多信息，请参见设置频率控制。	✓	✓
	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。 更多信息，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配置最多200条访问IP白名单和200条访问IP黑名单规则。 更多信息，请参见设置黑白名单（针对域名）。	✓	✓
	精准访问控制	支持HTTP协议精准匹配防护规则。 更多信息，请参见设置精准访问控制。	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

功能分类	功能项	功能描述	标准功能套餐	增强功能套餐
	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。 更多信息，请参见设置区域封禁（针对域名）。	✗	✓
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。	✓	✓
	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：** 每个实例支持配置最多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。 更多信息，请参见设置静态页面缓存。	✗	✓

3.4 业务带宽

本文介绍了在开通DDoS高防实例时，如何选择合适的业务带宽规格。

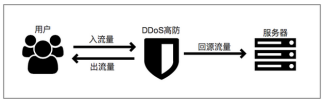
您可以根据所有已经或将要接入DDoS高防实例的业务的日常入方向或出方向总流量的峰值，选择合适的业务带宽规格。您选择的最大业务带宽应大于这些业务的网络入、出方向总流量峰值中较大的值。

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50Mbps，业务流量总和不超过150Mbps。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150Mbps即可。

3.5 防护域名数

本文介绍了在开通DDoS高防实例时，如何选择合适的防护域名规格。

每10个域名数规格包含一个一级域名。

- DDoS高防（新BGP）实例默认支持添加50条域名配置记录，且仅支持接入五个不同的一级域名。
- DDoS高防（国际）实例默认支持添加10条域名配置记录，且仅支持接入一个一级域名。

以DDoS高防（新BGP）服务为例，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将它们的子域名接入DDoS高防（新BGP）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（新BGP）实例，额外增加防护域名数量。

3.6 开通DDoS高防

本文介绍了开通DDoS高防（新BGP）、DDoS高防（国际）实例的具体操作。

背景信息

如果您的业务服务器部署在中国内地，推荐您开通DDoS高防（新BGP）服务；如果您的业务服务器部署在中国内地以外地区，推荐您开通DDoS高防（国际）服务。

说明：

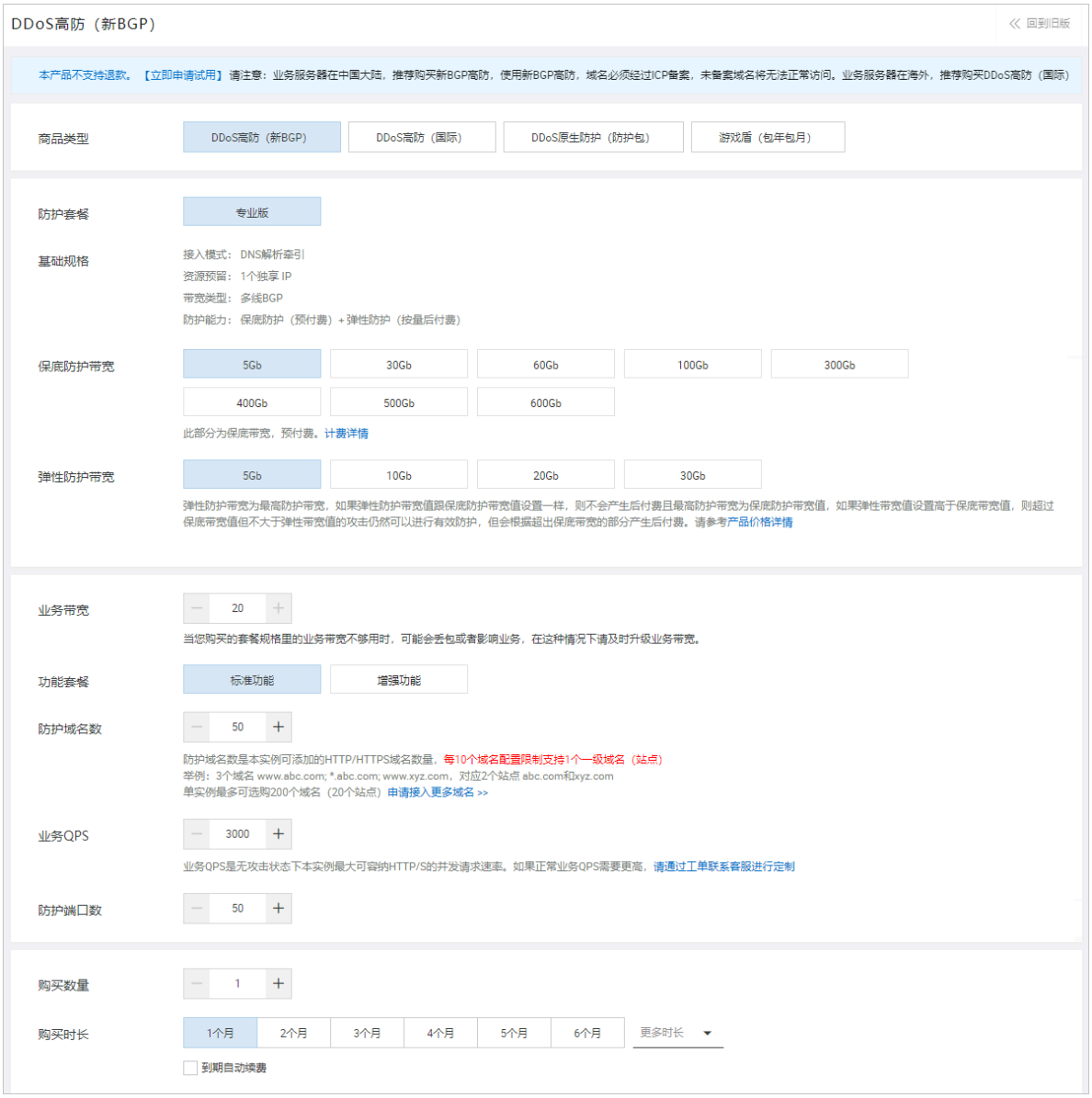
使用DDoS高防（新BGP）服务时，域名必须经过ICP备案，未备案域名将无法正常访问。

- 关于DDoS高防（新BGP）服务的详细计费说明，请参见计费方式。
- 关于DDoS高防（国际）服务的详细计费说明，请参见计费方式。

开通DDoS高防（新BGP）实例

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（新BGP）实例的购买配置。



参数	描述
防护套餐	默认为**专业版**，且不支持修改。
保底防护带宽	DDoS高防（新BGP）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。

参数	描述
弹性防护带宽	DDoS高防（新BGP）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。
资源组	DDoS高防（新BGP）实例所属的资源组。
业务带宽	无攻击状态下本实例最大可容纳的正常业务流量（按入流量或出流量其中的较大值计算）。 关于如何选择合适的业务带宽，请参见业务带宽。
功能套餐	可选项：**标准功能**、**增强功能**。 **说明:** 关于各功能套餐的具体介绍，请参见功能套餐。
防护域名数	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。 关于防护域名数的详细说明，请参见防护域名数。
业务QPS	支持处理的无攻击情况下最大HTTP/HTTPS业务的并发请求速率。
防护端口数	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。
购买数量	要购买当前配置的实例的数量。
购买时长	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。

开通DDoS高防（国际）实例

1. 访问DDoS高防（国际）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（国际）实例的购买配置。

参数	加速线路是否支持	描述
防护套餐	是	可选项：**保险版**、**无忧版**、**加速线路**。 • 关于保险版和无忧版的说明，请参见计费方式。 • 关于加速线路的说明，请参见加速线路。

参数	加速线路是否支持	描述
业务带宽	是	无攻击状态下本实例最大可容纳的正常业务流量（按入流量或出流量其中的较大值计算）。 关于如何选择合适的业务带宽，请参见业务带宽。
功能套餐	否	可选项：**标准功能**、**增强功能**。 **说明:** 关于各功能套餐的具体介绍，请参见功能套餐。
防护域名数	否	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。 关于防护域名数的详细说明，请参见防护域名数。
业务QPS	否	支持处理的无攻击情况下最大HTTP/HTTPS业务的并发请求速率。
防护端口数	否	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。
购买数量	是	要购买当前配置的实例的数量。
购买时长	是	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。

3.7 升级DDoS高防实例规格

开通DDoS高防实例后，如果实例规格（例如功能套餐、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DDoS高防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高防实例规格时，您需要补齐升级差价。支付完成后，DDoS高防实例规格升级即时生效。

说明：

不支持降低已购买DDoS高防实例的规格，包括功能套餐、防护域名数、端口数和业务带宽等。例如，从增强功能套餐降配为标准功能套餐、减少防护域名数量等。

操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**资产管理** > **实例管理**。
4. 定位到要操作的DDoS高防实例，单击其操作列下的**升级**。
5. 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**。
6. 完成支付，升级后的DDoS高防实例规格配置即时生效。

4 快速入门

4.1 防护网站业务

4.1.1 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，为网站业务配置DDoS防护。

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	描述
步骤1：添加网站业务转发规则	在DDoS高防控制台通过域名接入添加要防护的网站业务，关联DDoS高防实例并设置业务流量转发策略。
步骤2：接入网站业务流量	修改已接入DDoS高防的域名的解析记录，将网站业务流量牵引到DDoS高防实例。完成切换后，网站的访问流量都会先经过DDoS高防清洗，再转发到源站服务器，实现由DDoS高防实例帮助网站防御DDoS攻击流量。
步骤3：设置网站业务防护策略	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，您可以手动调整网站业务的DDoS防护策略，具体包括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：查看网站业务防护数据	网站业务接入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业务防护数据。 **说明：** 目前仅DDoS高防（新BGP）服务支持安全报表和操作日志功能。

4.1.2 步骤1：添加网站业务转发规则

使用DDoS高防防护网站业务时，您必须首先在DDoS高防中添加要防护的域名，设置业务流量的转发策略。

前提条件

已开通DDoS高防（新BGP/国际）实例。更多信息，请参见开通DDoS高防。

背景信息

注意：

DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和

配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

本文以DDoS高防（新BGP）服务为例描述具体操作。如果您使用DDoS高防（国际）服务，请参见添加网站。

操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**中国内地**地域。
3. 在左侧导航栏，单击**接入管理** > **域名接入**。
4. 在**域名接入**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网站配置。

5. 在**添加网站**页面，完成**填写网站信息**任务，并单击**添加**。

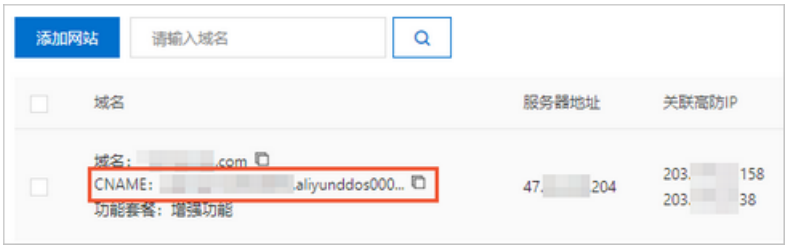
参数	描述
功能套餐	选择要关联的DDoS高防实例的功能套餐规格，可选值： • **标准功能** • **增强功能** **说明:** 关于不同功能套餐的详细说明，请参见功能套餐。

参数	描述
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八个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。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支持的协议类型勾选其他协议类型。
启用HTTP2	域名关联增强功能的高防实例时，选择是否开启HTTP2。开启后协议版本为HTTP2.0。 **说明：** 仅DDoS高防（新BGP）服务支持该配置。

参数	描述
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。
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端口包括80和8080，可选的HTTPS/Websockets端口包括443和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。 

参数	描述
Cname Reuse	选择是否开启CNAME复用。开启CNAME复用后，您只需将同服务器上多个域名的解析指向高防CNAME地址，即可将多个域名接入高防，无需为每个域名分别添加高防配置。更多信息，请参见 CNAME复用。 **说明:** 仅DDoS高防（国际）服务支持该配置。

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



预期结果

DDoS高防为已接入的网站业务分配一个CNAME地址。您只需将网站域名的DNS解析指向DDoS高防的CNAME地址，即可将网站访问流量转发到DDoS高防实例进行清洗。

后续步骤

- 步骤2：接入网站业务流量
- 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。

4.1.3 步骤2：接入网站业务流量

通过DDoS高防域名接入添加网站业务后，您需要更新域名的DNS解析，将网站业务流量牵引到DDoS高防。完成切换后，网站的访问流量都会先经过DDoS高防清洗，再转发到源站服务器。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：

- 已完成域名接入。更多信息，请参见步骤1：添加网站业务转发规则。
- 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

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。

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

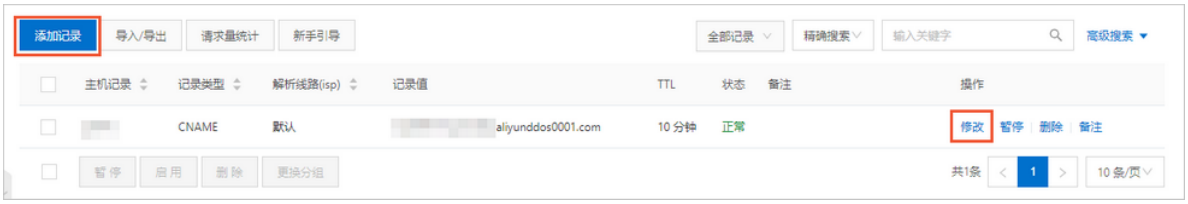
假设在DDoS高防控制台已添加网站的域名为bgp.ddostest.com。以下操作示例描述了在云解析DNS控制台修改/新增域名解析的步骤。

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（本示例中对应主机记录为**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。

5. 单击**确定**，等待修改后的解析设置生效。

后续步骤

步骤3：设置网站业务防护策略

4.1.4 步骤3：设置网站业务防护策略

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，您可以手动调整网站业务的DDoS防护策略，具体包括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。

前提条件

已完成域名接入。更多信息，请参见步骤1：添加网站业务转发规则。

操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **域名接入**。
4. 在**域名接入**页面，定位到要操作的域名，单击其操作列下的**防护设置**。

5. 在**网站业务DDoS防护**页签，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。由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）**：开启针对域名的访问源IP黑白名单后，黑名单IP/IP段对域名的访问请求将会被直接阻断，白名单IP/IP段对域名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，请参见设置黑白名单（针对域名）。
- **区域封禁（针对域名）**：开启针对域名的区域封禁后，您可以一键阻断来自指定地区（中国大陆省/市/区、非中国大陆地区）来源IP的所有网站访问请求。更多信息，请参见设置区域封禁（针对域名）。
- **精确访问控制**：开启精确访问控制后，您可以使用常见的HTTP字段（例如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。
- **频率控制**：开启频率控制后，您可以限制单一源IP对网站的访问频率。频率控制开启后自动生效，且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。

4.1.5 步骤4：查看网站业务防护数据

网站业务接入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业务防护数据。

前提条件

- 已完成域名接入。更多信息，请参见步骤1：添加网站业务转发规则。
- 已完成业务流量接入配置。更多信息，请参见步骤2：接入网站业务流量。

背景信息

目前仅DDoS高防（新BGP）服务支持安全报表和操作日志功能，下文以DDoS高防（新BGP）为例描述具体操作。如果您使用DDoS高防（国际）服务，建议您通过安全总览和全量日志分析了解业务防护情况。更多信息，请参见查看安全总览、全量日志分析。

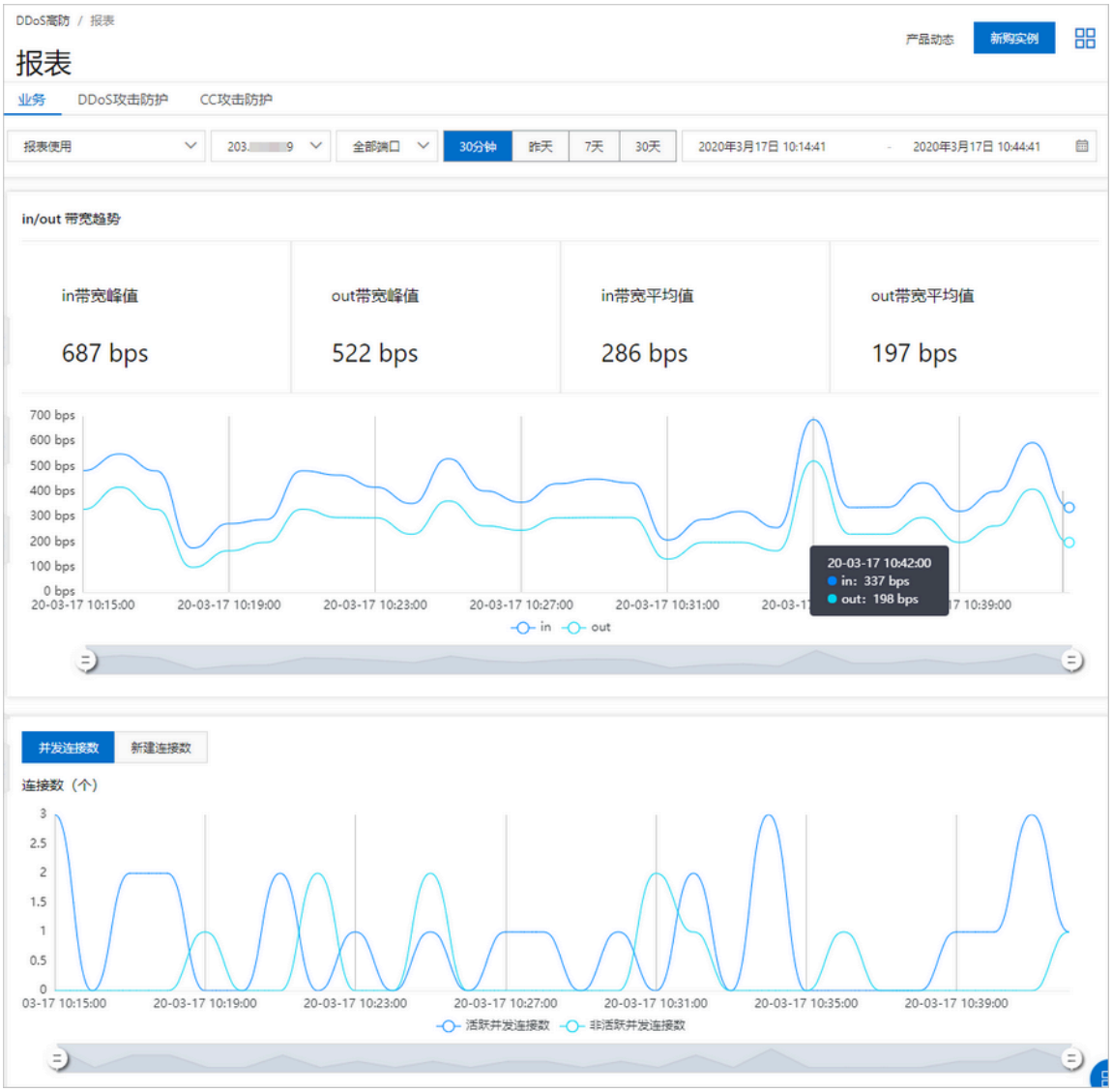
操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**中国内地**地域。

3. 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、实例、IP、端口信息等。每种报表包含的信息如下。

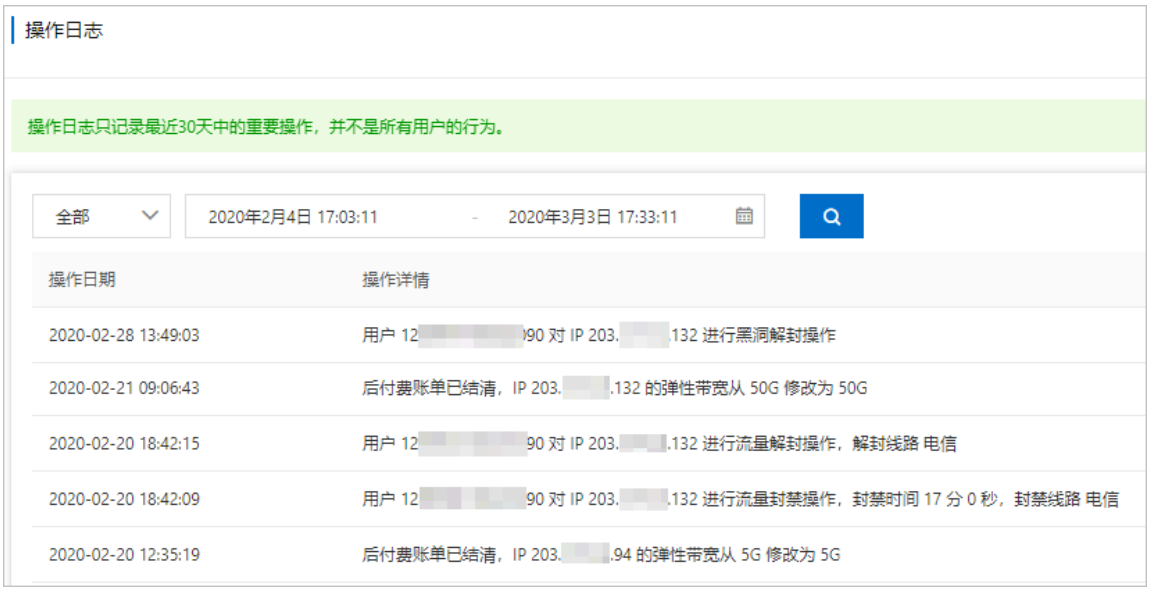
报表类型	支持查看的信息	支持的筛选项
业务	- in/out带宽趋势图 - 并发连接数和新建连接数趋势图	- 时间 - 实例 - 高防IP - 转发端口

报表类型	支持查看的信息	支持的筛选项
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
CC攻击防护	- QPS图（攻击QPS、总QPS） - CC攻击记录	- 时间 - 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**，并在**操作日志**页面，查看对应日志记录。操作日志记录了最近30天中的重要操作，例如IP、ECS实例操作等，支持通过时间筛选记录。



如果您希望对DDoS高防的日志进行实时分析和报表展示，推荐您开通DDoS高防全量日志分析。开通全量日志分析后，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。更多信息，请参见#unique_47。

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

a. 开通全量日志分析，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的字段，请参见全量日志字段说明。

4.2 防护非网站业务

4.2.1 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（例如端游、手游、app等）配置DDoS防护。

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：添加端口转发规则	在DDoS高防控制台通过端口接入添加要防护的非网站业务，并使用DDoS高防IP作为您的业务IP，将业务流量牵引到DDoS高防实例。完成切换后，业务流量都会先经过DDoS高防清洗，再转发到源站服务器。
步骤2：设置端口转发和防护策略	在DDoS高防实例下添加端口转发规则后，您可以根据需要设置端口转发策略，例如会话保持、（多源站IP）健康检查，也可以为非网站业务设置DDoS防护策略，例如虚假源检测、目的限速、包长度过滤、源限速。
步骤3：查看端口防护数据	非网站业务接入DDoS高防后，您可以在DDoS高防的安全总览页面查看端口流量转发数据。

4.2.2 步骤1：添加端口转发规则

使用DDoS高防防护非网站业务（例如端游、手游、app等）时，您必须在购买DDoS高防实例后，配置端口转发规则，然后使用DDoS高防IP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（新BGP/国际）实例。更多信息，请参见开通DDoS高防。

背景信息

注意:

DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

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（例如CC攻击、Web攻击防护等），只支持四层防护（例如防护SYN Flood、UDP Flood等）。接入非网站业务时，您只需配置DDoS高防实例的端口转发规则，然后使用DDoS高防IP作为业务IP即可。

操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务

3. 在左侧导航栏，单击**接入管理** > **端口接入**。
4. 在**端口接入**页面，选择要使用的DDoS高防实例，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。

5. 在**添加规则**对话框，根据您的实际业务情况完成规则配置。

参数	描述
转发协议	转发协议类型，可选值：**TCP**、**UDP**。

参数	描述
转发端口	DDoS高防实例使用的转发端口。 • 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，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	源站使用的业务端口。
源站IP	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。

6. 单击**完成**，创建端口转发规则。

   端口转发规则创建完成后，您可以根据需要设置会话保持、健康检查、非网站业务DDoS防护策略。更多信息，请参见步骤2：设置端口转发和防护策略。

   您也可以对手动创建的转发规则执行**编辑**或**删除**操作。

7. 将要防护的实际业务IP替换为DDoS高防IP，正式将业务流量牵引到DDoS高防。完成切换后，业务流量都会先经过DDoS高防清洗，再转发到源站服务器。

   强烈建议您在正式切换业务流量前进行验证，确认转发配置已生效。关于转发配置的验证方法，请参见本地验证转发配置生效。

   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。

4.2.3 步骤2：设置端口转发和防护策略

在DDoS高防实例下添加端口转发规则后，您可以根据需要配置端口转发策略，例如会话保持、（多源站IP）健康检查，也可以为非网站业务设置DDoS防护策略，例如虚假源检测、目的限速、包长度过滤、源限速。

前提条件

已完成端口接入。更多信息，请参见步骤1：添加端口转发规则。

背景信息

通过设置端口转发策略和非网站业务DDoS防护策略，您可以根据业务实际需求，优化DDoS高防的转发功能。

- 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。
- 开启健康检查后，可以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。
- 开启DDoS防护策略后，可以对接入DDoS高防的非网站业务的连接速度、包长度等参数进行限制，缓解小流量的连接型攻击。

操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **端口接入**。

4. 在**端口接入**页面，选择DDoS高防实例，并定位到要操作的转发规则，根据需要设置会话保持、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**。

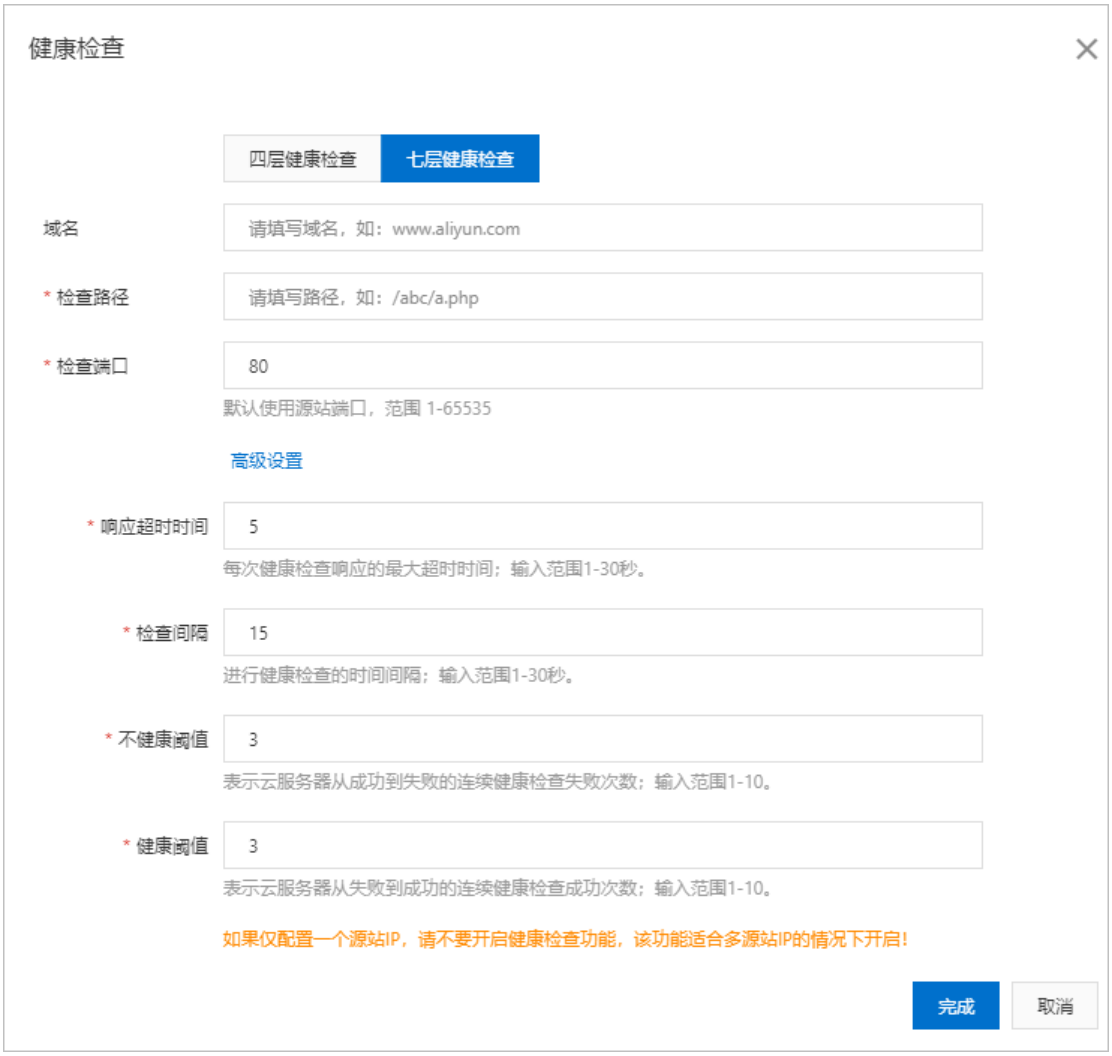
  b. 在**会话保持**对话框，根据需要开启或关闭会话保持。

  - 开启会话保持：设置**超时时间**，并单击**完成**。
  - 关闭会话保持：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，完成健康检查配置。配置描述请参见健康检查配置项说明。



c. 单击**完成**。

开启健康检查后，若您想关闭健康检查，只需单击**配置**，并在**健康检查**对话框单击**关闭健康检查**。

- 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，根据需要为当前转发规则设置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。

4.2.4 步骤3：查看端口防护数据

非网站业务接入DDoS高防后，您可以在DDoS高防的安全总览页面查看端口流量转发数据。

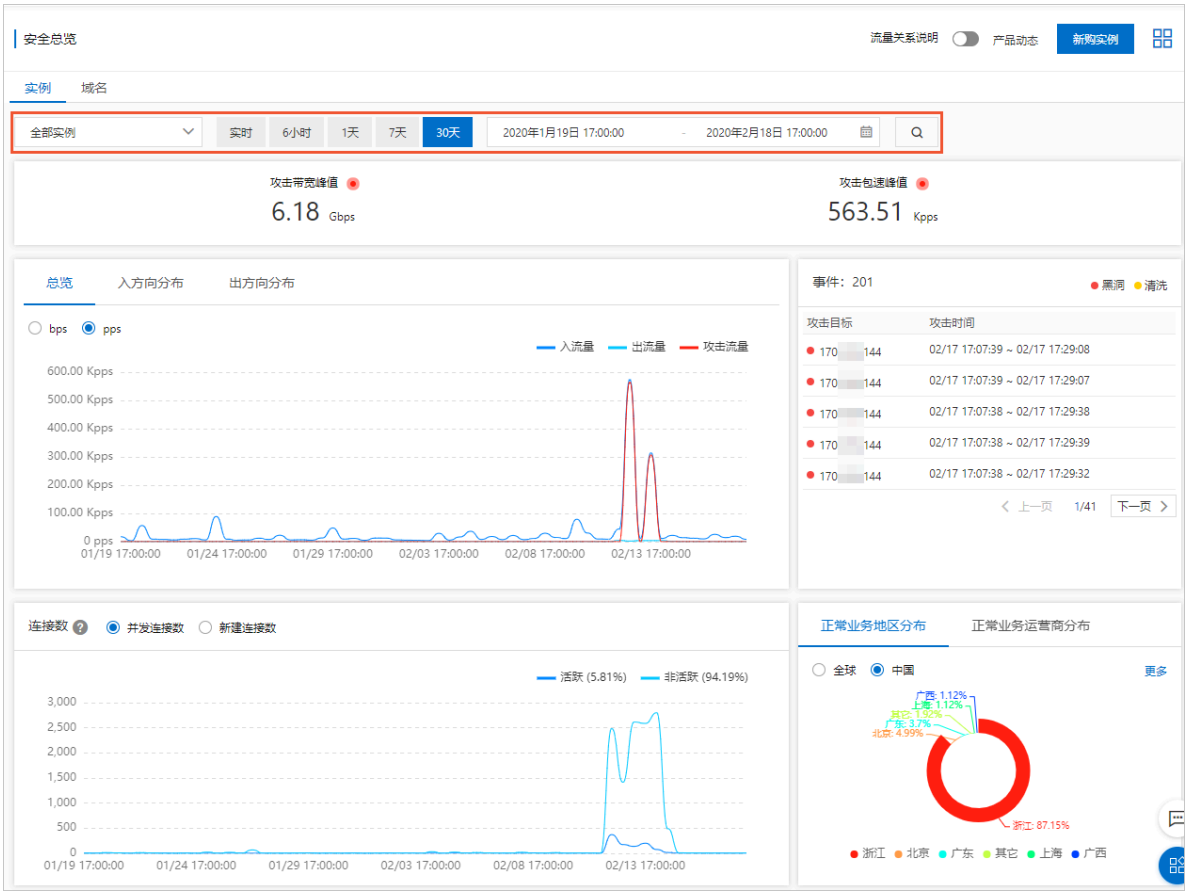
前提条件

已完成端口接入。更多信息，请参见步骤1：添加端口转发规则。

操作步骤

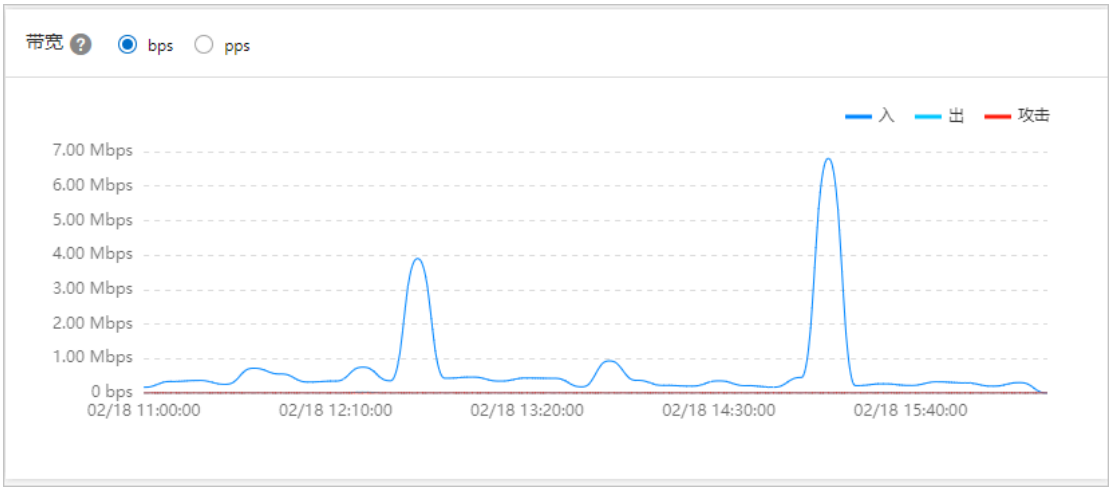
1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**安全总览**。

4. 打开**实例**页签，设置要查询的实例和时间范围，查看指定实例对应业务的相关信息。

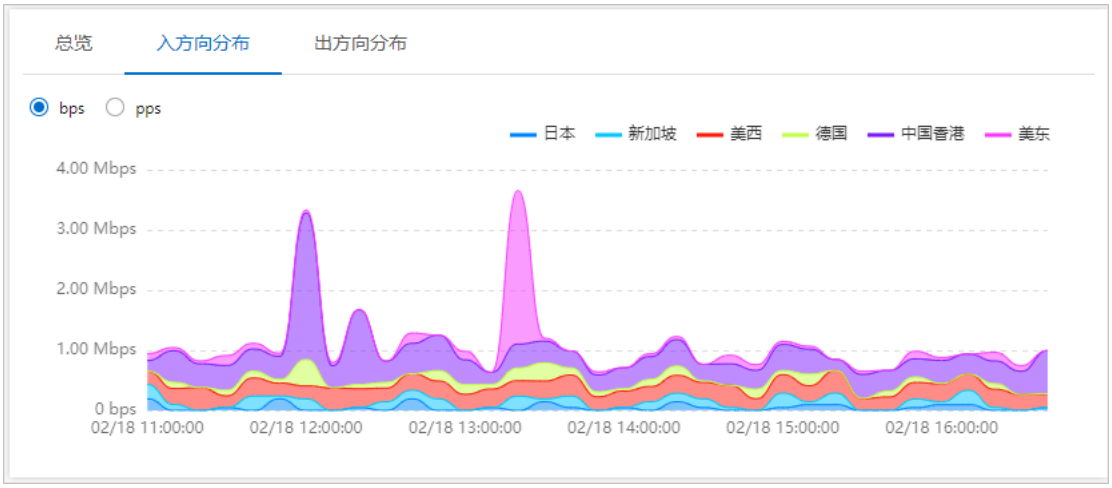


支持查看的实例业务信息包括以下内容。

- **攻击带宽峰值**和**攻击包速峰值**
- 流量趋势信息
  - DDoS高防（新BGP）服务提供**带宽**趋势图，以**bps**/**pps**展示指定时间段内实例上的入流量、出流量、攻击流量趋势。



- DDoS高防（国际）提供三个页签，分别是**总览**（同带宽趋势图）、**入方向分布**（入方向流量的分布信息）、**出方向分布**（出方向流量的分布信息）。



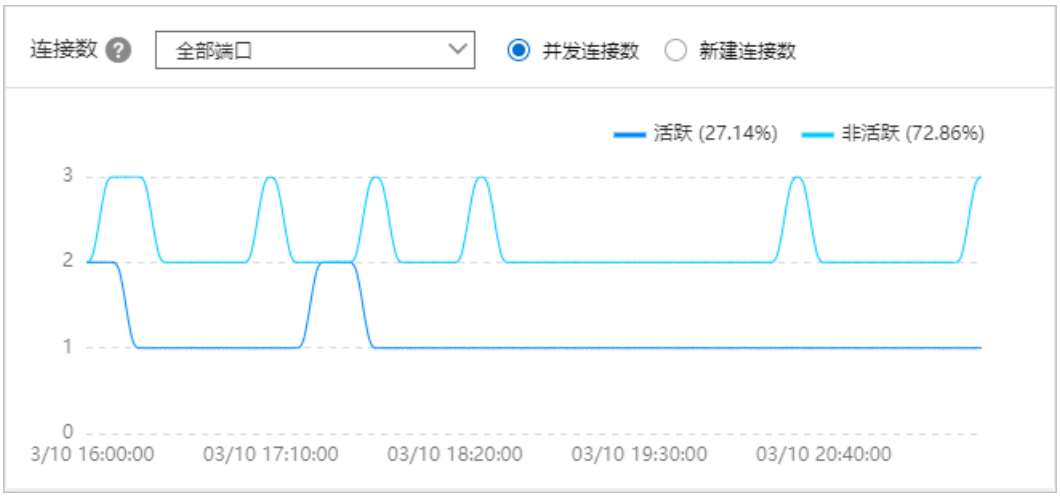
- （黑洞和清洗）**事件**记录表

  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。如果选择一个以上实例，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 接入DDoS高防

5.1 域名接入

5.1.1 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（新BGP）或DDoS高防（国际）实例。更多信息，请参见开通DDoS高防。

DDoS高防（BGP）和DDoS高防（国际）服务差异

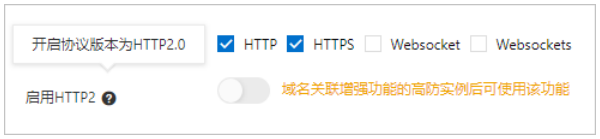
注意：

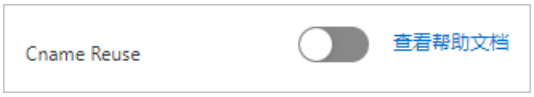
DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

DDoS高防（BGP）和DDoS高防（国际）在网站配置上存在以下功能差异。

说明：

下表仅罗列存在差异的功能点，不包括在DDoS高防（BGP）和DDoS高防（国际）中完全相同的功能点。

功能	描述	DDoS高防（BGP）	DDoS高防（国际）
启用HTTP2	域名关联增强功能的高防实例后可开启。开启后协议版本为HTTP2.0。 	支持	不支持

功能	描述	DDoS高防（BGP）	DDoS高防（国际）
Cname Reuse	开启CNAME复用后，您只需将同服务器上多个域名的解析指向高防CNAME地址，即可将多个域名接入高防，无需为每个域名分别添加高防配置。更多信息，请参见 CNAME复用。 	不支持	支持

添加网站配置

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **域名接入**。
4. 在**域名接入**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网站配置。

5. 在**添加网站**页面，完成**填写网站信息**任务，并单击**添加**。

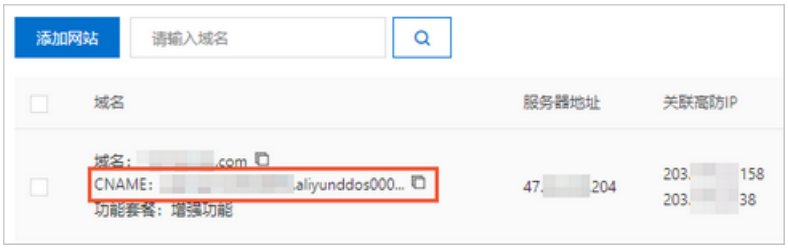
参数	描述
功能套餐	选择要关联的DDoS高防实例的功能套餐规格，可选值： • **标准功能** • **增强功能** **说明:** 关于不同功能套餐的详细说明，请参见功能套餐。

参数	描述
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八个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。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支持的协议类型勾选其他协议类型。
启用HTTP2	域名关联增强功能的高防实例时，选择是否开启HTTP2。开启后协议版本为HTTP2.0。 **说明：** 仅DDoS高防（新BGP）服务支持该配置。

参数	描述
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。
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端口包括80和8080，可选的HTTPS/Websockets端口包括443和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。 

参数	描述
Cname Reuse	选择是否开启CNAME复用。开启CNAME复用后，您只需将同服务器上多个域名的解析指向高防CNAME地址，即可将多个域名接入高防，无需为每个域名分别添加高防配置。更多信息，请参见 CNAME复用。 **说明:** 仅DDoS高防（国际）服务支持该配置。

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

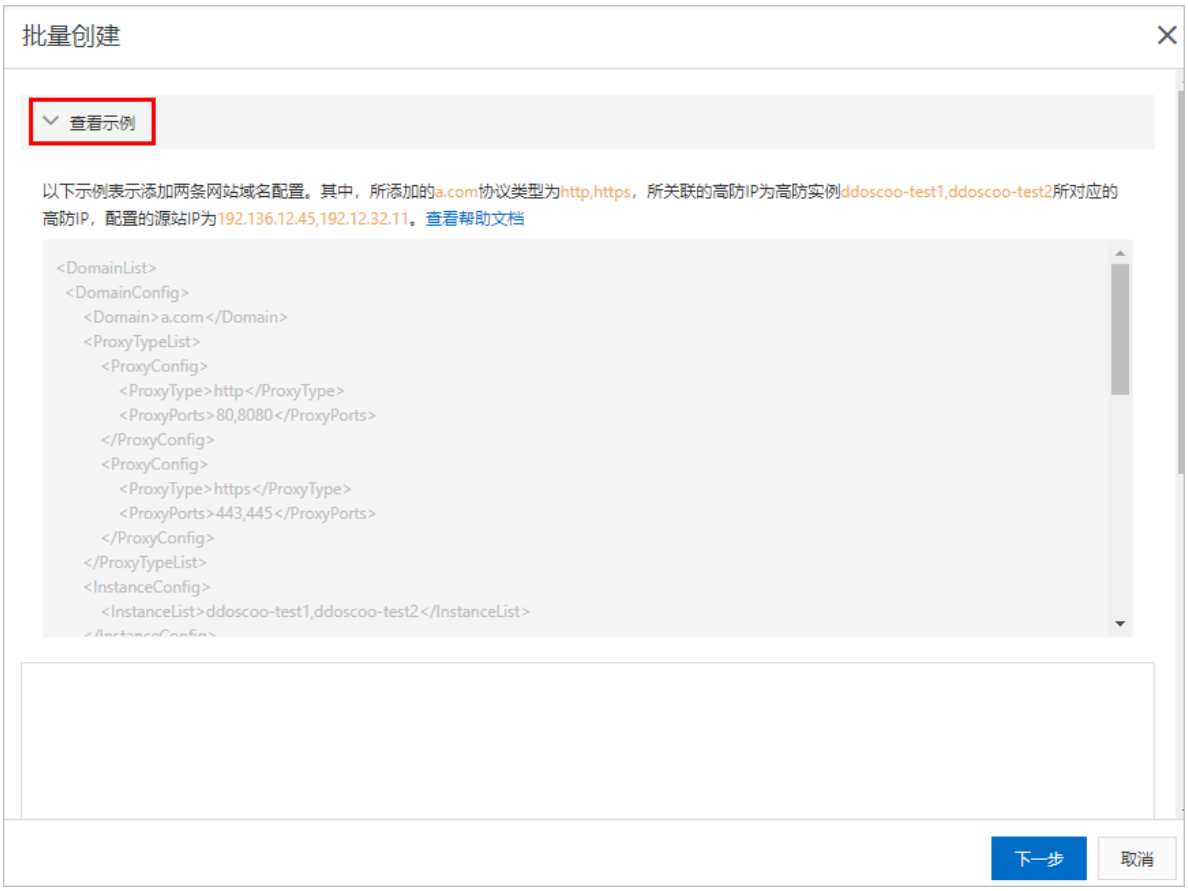


批量导入网站配置

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **域名接入**。
4. 在**域名接入**页面，单击网站列表下方的**批量导入**。

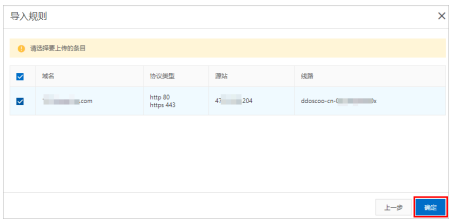
5. 在**批量创建**页面，输入要导入的网站配置，并单击**下一步**。

   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。

6. 在**导入规则**页面，勾选要导入的网站配置，并单击**确定**。



7. 成功上传网站配置后，关闭**上传完成**页面。

相关操作

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**域名接入**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。

5.1.2 编辑网站

若您需要为网站重新关联DDoS高防实例（例如由标准功能套餐更换为增强功能套餐）、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。

编辑网站配置

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **域名接入**。
4. 定位到要编辑的网站配置，单击其操作列下的**编辑**。

> **说明：**
> 如果您使用DDoS高防（新BGP）服务，则您也可以批量修改网站配置，具体请参见批量修改网站配置。

5. 在**编辑网站**页面，修改网站配置信息，并单击**确定**。

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

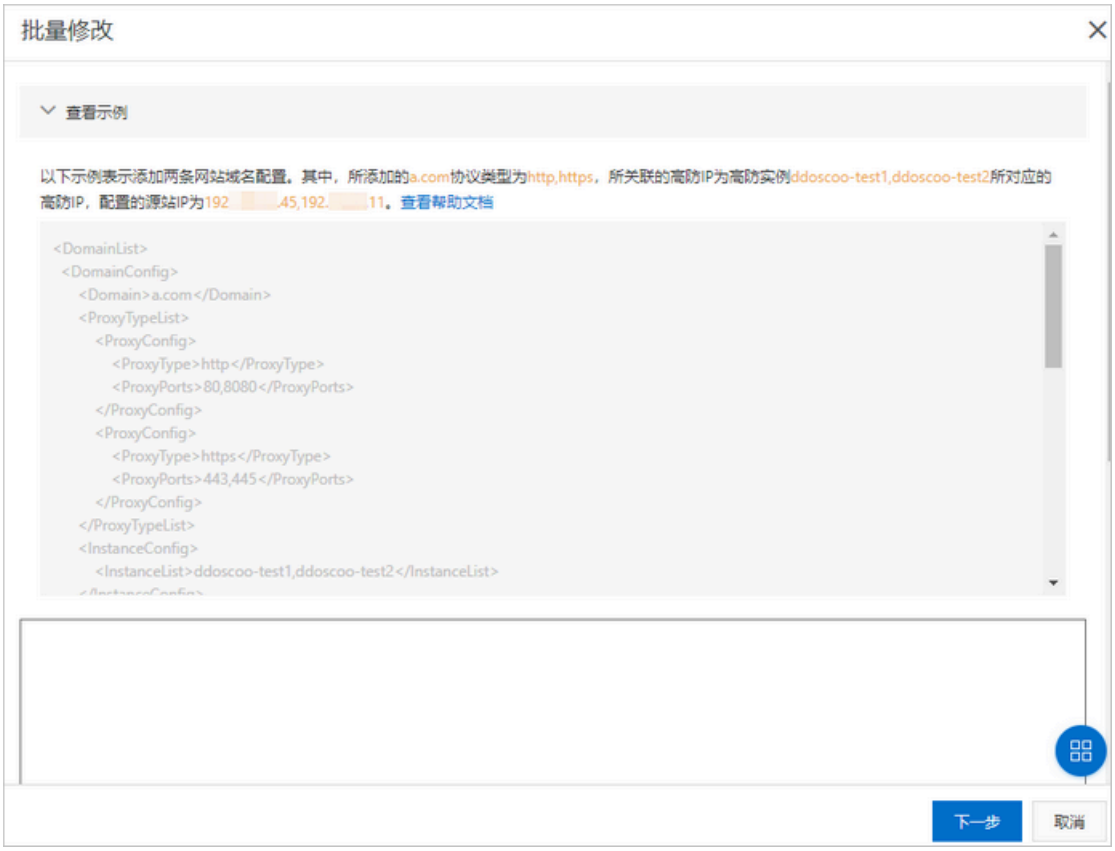
   例如重新选择**功能套餐**和**实例**，为网站关联其他DDoS高防实例，或者重新输入**源站IP**，更新源站IP等。

批量修改网站配置

> **说明：**
> 仅DDoS高防（新BGP）服务支持批量修改网站配置。

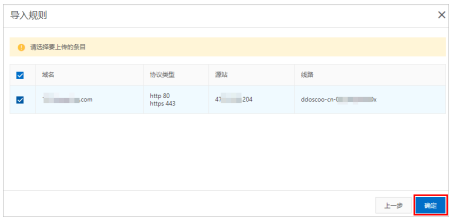
1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**中国内地**地域。
3. 在左侧导航栏，单击**接入管理** > **域名接入**。
4. 在**域名接入**页面，单击网站列表下方的**批量修改**。
5. 在**批量修改**页面，输入新的网站配置，并单击**下一步**。

   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。

6. 在**导入规则**页面，勾选要导入的网站配置，并单击**确定**。



7. 成功上传网站配置后，关闭**上传完成**页面。

5.1.3 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DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **域名接入**。
4. 定位到要删除的网站配置，单击其操作列下的**删除**。

> **说明：**
> 如果您使用DDoS高防（新BGP）服务，则您也可以批量删除多个网站配置。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**。

5. 在删除提示对话框中，确认删除操作。

5.1.4 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DDoS高防控制台。

2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **域名接入**。
4. 在网站列表下方，单击**批量导出**，下发导出任务。
5. 导出任务已下发后，单击页面右上角的任务图标。

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后，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。

说明：

如果您使用DDoS高防（新BGP）服务，则导出文件的名称以DDoSCoo_开头。如果您使用DDoS高防（国际）服务，则导出文件的名称以DDoSDip_开头。使用DDoS高防（新BGP）和DDoS高防（国际）服务导出的内容格式相同。

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。

5.1.5 自定义非标端口

DDoS高防标准功能套餐针对网站业务默认支持HTTP（80、8080）和HTTPS（443、8443）标准端口的防护。增强功能套餐支持更多的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非标端口前，请确认您的网站域名已关联增强功能套餐的DDoS高防实例。

端口总数限制

针对每个DDoS高防增强功能实例，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高防增强功能实例支持以下端口：

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

5.1.6 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

- 已添加网站配置且网站支持HTTPS协议。更多信息，请参见添加网站。
- 准备证书文件内容。

  如果您已将证书文件上传到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DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **域名接入**。

4. 在**域名接入**页面，定位到要操作的域名，单击其**证书状态**列下的上传图标。

5. 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证书并上传。

     即使您的证书未托管在SSL证书服务中，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_66。

   - **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**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，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#unique_67。
- 如果该HTTPS证书有多个证书文件（例如证书链），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**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
ra6ZdwBcQJaiygolYoaMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/
3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04RtKadOw==
-----END RSA PRIVATE KEY-----
```

6. 单击**确定**。

预期结果

成功上传证书后，证书状态会更新为正常。

5.1.7 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

- 已添加网站配置，且网站配置已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。
- 网站配置中支持HTTPS协议，且已上传对应的HTTPS证书。更多信息，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，希望禁用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。这种情况下，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。

操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **域名接入**。
4. 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**。

5. 在**TLS安全策略配置**对话框中，选择**TLS版本**和**加密套件**，并单击**确定**。

- **TLS版本**
  - **支持TLS1.0及以上版本，兼容性最好，安全性较低**（默认）
  - **支持TLS1.1及以上版本，兼容性较好，安全性较好**
  - **支持TLS1.2及以上版本，兼容性较好，安全性很高**
- **加密套件**
  - **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

5.1.8 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>	待配置的域名（只能输入一个域名）。
<ProtocolConfig><ProtocolList>http,https</ProtocolList></ProtocolConfig>	域名协议类型。多个协议类型间以英文逗号（,）隔开。本示例表示该域名的协议类型为http和https。
<InstanceConfig><InstanceList>ddoscoo-cn-xxxxxxxxx001</InstanceList></InstanceConfig>	网站关联的DDoS高防实例。 **说明：** 由于每个DDoS高防实例对应一个ID，所以只需填写DDoS高防实例ID即可。多个实例ID间以英文逗号（,）隔开。
<RealServerConfig><ServerType>0</ServerType><ServerList>1.x.x.4</ServerList></RealServerConfig>	源站信息。结构说明如下： • <ServerType>0</ServerType>：表示源站IP类型 • <ServerType>1</ServerType>：表示源站域名类型 <ServerList>1.x.x.4</ServerList>表示源站地址，多个地址间以英文逗号（,）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

```
<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.x.x.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>
```

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。

5.2 端口接入

5.2.1 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（新BGP）或DDoS高防（国际）实例。更多信息，请参见开通DDoS高防。

注意：

DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和

配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

添加转发规则

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **端口接入**。
4. 在**端口接入**页面，选择要操作的DDoS高防实例，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。

5. 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**。

参数	描述
转发协议	转发协议类型，可选值：**TCP**、**UDP**。
转发端口	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	源站使用的业务端口。

参数	描述
源站IP	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。

成功添加转发规则后，您可以在转发规则列表中看到新增的转发规则。

批量添加规则

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **端口接入**。
4. 在**端口接入**页面，选择要操作的DDoS高防实例，并单击规则列表下方的**批量操作** > **添加规则**。
5. 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（字段的含义请参见规则配置描述），字段间以空格分隔。

6. 在**添加规则**对话框，勾选要上传的规则，确认后并单击**上传**。

7. 成功上传转发规则后，关闭**添加规则**对话框。您可以在转发规则列表中看到新增的转发规则。

相关操作

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。

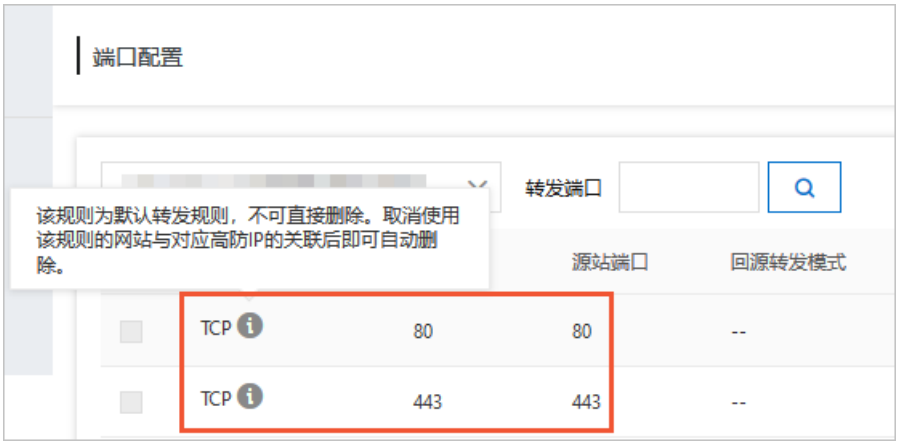
添加转发规则后，您可以在**端口接入**页面完成以下操作：

- 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。
- 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。

（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。

5.2.2 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高防实例下已添加转发规则。更多信息，请参见添加规则。

编辑转发规则

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **端口接入**。
4. 在**端口接入**页面，选择要操作的DDoS高防实例。
5. 定位到要编辑的转发规则，单击其操作列下的**编辑**。

> **说明：**
> 如果您使用DDoS高防（新BGP）服务，则您也可以通过批量操作修改规则，支持一次修改多条规则，具体请参见批量修改规则。

6. 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后，DDoS高防IP会按照更新后的转发规则转发业务流量。

批量修改规则

> **说明：**
> 仅DDoS高防（新BGP）服务支持批量修改规则。

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**中国内地**地域。
3. 在左侧导航栏，单击**接入管理** > **端口接入**。
4. 在**端口接入**页面，选择要操作的DDoS高防实例，并单击规则列表下方的**批量操作** > **修改规则**。

5. 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（字段的含义请参见规则配置描述），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。

6. 在**修改规则**对话框，勾选要上传的规则，确认后并单击**上传**。

7. 上传完成后，关闭**修改规则**对话框。

5.2.3 删除规则

对于手动添加的转发规则，如果您不再需要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。如果您未恢复实际业务IP就删除转发规则，那么可能导致业务中断。

前提条件

已恢复实际业务IP。

操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **端口接入**。
4. 在**端口接入**页面，选择要操作的DDoS高防实例。
5. 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，单击规则列表下方的**批量删除**。
6. 在删除提示对话框中，确认删除操作。

5.2.4 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、批量添加会话/健康检查配置、批量添加DDoS防护策略配置）保持一致。

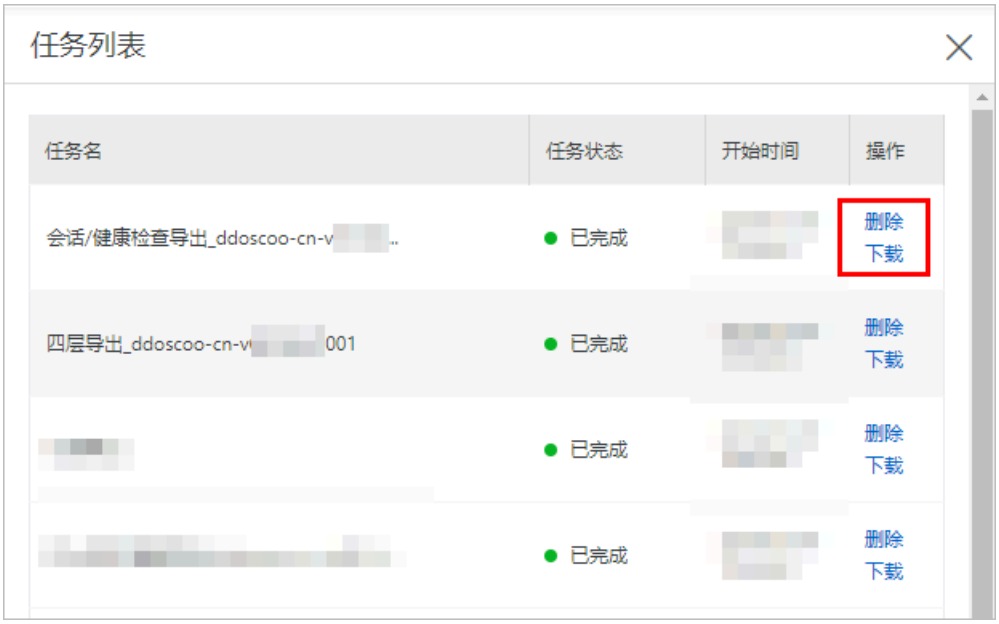
操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **端口接入**。
4. 在**端口接入**页面，选择要操作的DDoS高防实例。
5. 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**，下发相应导出任务。

6. 导出任务已下发后，单击页面右上角的任务图标。

7. 在**任务列表**页面，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后，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。

8. （可选）在**任务列表**页面，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。

> **说明：**
> 如果您使用DDoS高防（新BGP）服务，则导出文件的名称以DDoSCoo_开头。如果您使用DDoS高防（国际）服务，则导出文件的名称以DDoSDip_开头。使用DDoS高防（新BGP）和DDoS高防（国际）服务导出的内容格式相同。

- 规则文件

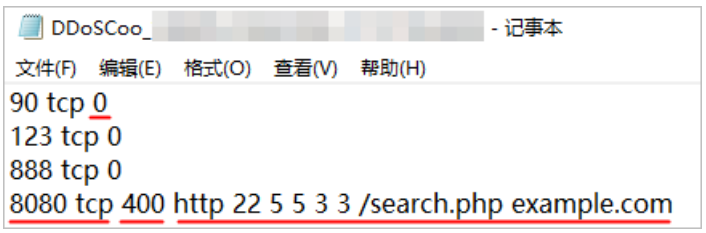
  每行对应一条规则，每条规则包含四个字段，从左到右依次是协议、转发端口、源站端口、源站IP。

  更多信息，请参见批量添加规则。

- 会话/健康配置文件

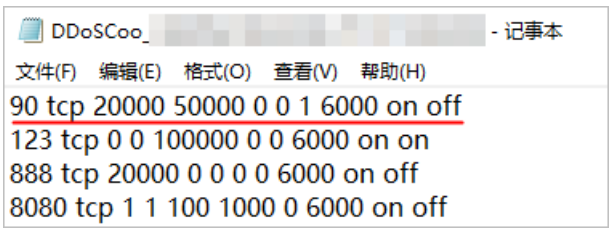
  每行对应一个规则的配置，每条配置包含以下字段（从左到右）：转发协议端口、转发协议、会话保持超时时间（若为0则表示未开启会话保持）、健康检查类型（若为空则表示未开启健康检查，且后续字段均为空）、检查端口、检查超时时间、检查间隔、不健康阈值、健康阈值、检查路径（HTTP类型下存在）、域名（HTTP类型下存在）。

  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。

5.2.5 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高防实例下添加转发规则，接入非网站业务后，您可

以单独为某个端口转发规则设置健康检查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

已在端口接入中配置非网站业务端口转发规则。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，对已接入DDoS高防实例的IP和端口提供健康检查功能。您可以为具体高防实例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**	每次健康检查响应的最大超时时间，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。

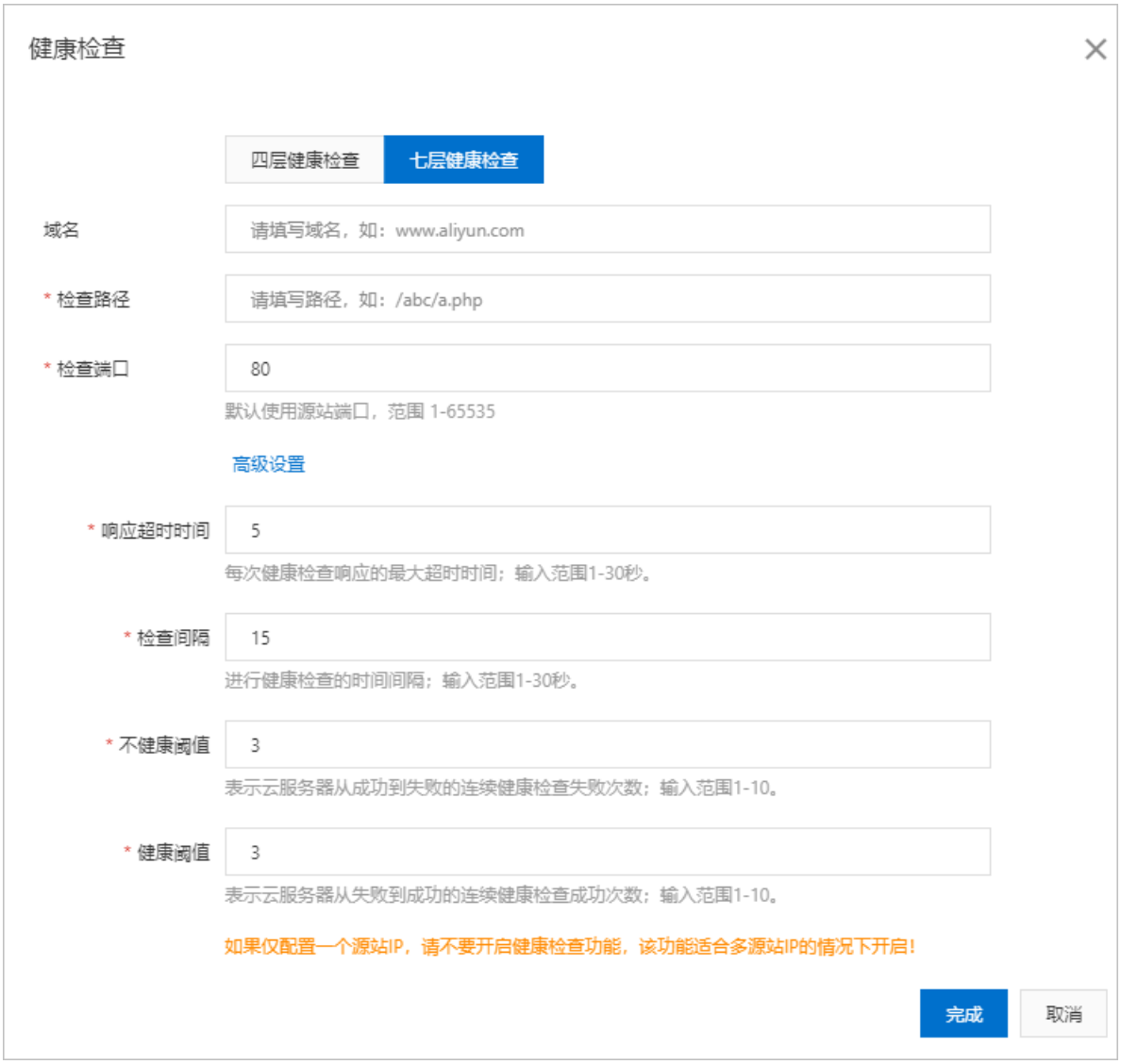
类型	配置项	说明
	检查间隔	进行健康检查的时间间隔，取值范围：1~30（秒）。 **说明：** 高防集群内所有节点都会独立、并行地遵循该属性对后端服务器进行健康检查。由于各高防节点的检查时间并不同步，如果从后端某一服务器上进行单独统计，会发现来自高防IP的健康检查请求在时间上没有遵循指定的时间间隔。
	不健康阈值	同一高防节点服务器针对同一后端服务器，在健康检查状态为成功时，连续多少次健康检查失败后，状态判定为失败，取值范围：1~10。
	健康阈值	同一高防节点服务器针对同一后端服务器，在健康检查状态为失败时，连续多少次健康检查成功，状态判定为成功，取值范围：1~10。

设置端口健康检查

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理 > 端口接入**。
4. 在**端口接入**页面，选择DDoS高防实例，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。

5. 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请参见健康检查配置项描述。



批量添加会话/健康配置

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **端口接入**。
4. 在**端口接入**页面，选择要操作的DDoS高防实例，并单击规则列表下方的**批量操作** > **会话/健康检查配置**。

5. 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**。

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。

会话保持/健康检查配置的格式要求如下。

- 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。具体字段的含义请参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。

5.2.6 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高防实例下添加转发规则，接入非网站业务后，您可以单

独为某个端口转发规则设置会话保持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

已在端口接入中配置非网站业务端口转发规则。更多信息，请参见添加规则。

背景信息

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，并对已接入DDoS高防实例的IP和端口提供会话保持功能。您可以为具体高防实例的转发端口设置会话保持规则。

设置端口会话保持

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **端口接入**。
4. 在**端口接入**页面，选择要操作的DDoS高防实例，并定位到要设置的转发规则，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。

5. 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DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **端口接入**。
4. 在**端口接入**页面，选择要操作的DDoS高防实例，并单击规则列表下方的**批量操作** > **会话/健康检查配置**。

5. 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**。

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。

会话保持/健康检查配置的格式要求如下。

- 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。具体字段的含义请参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。

5.3 业务接入配置

5.3.1 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：

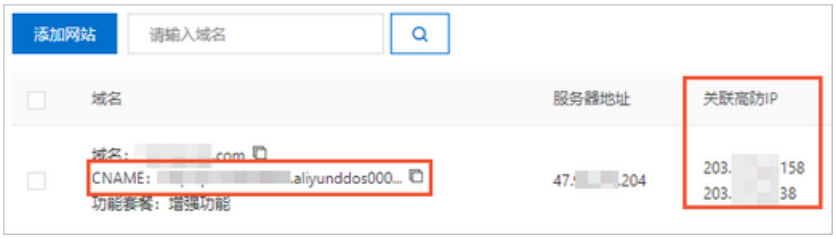
- 网站业务已添加网站配置。更多信息，请参见添加网站。
- 源站服务器已放行DDoS高防回源IP。如果您的源站服务器上部署了非阿里云安全软件（例如防火墙），请将DDoS高防的回源IP地址加入安全软件的白名单。更多信息，请参见放行DDoS高防回源IP。
- 验证转发配置生效。强烈建议您在切换网站访问流量前，在本地验证DDoS高防实例的业务转发配置已经生效。更多信息，请参见本地验证转发配置生效。

选择接入方式

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。

说明：

网站域名的高防CNAME地址和关联高防IP地址均可在**网站接入**页面查询。



- 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，无需重新修改解析，DDoS高防将通过CNAME自动完成调度。在网站关联多个高防IP时，DDoS高防自动在多IP间切换流量。
- 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。

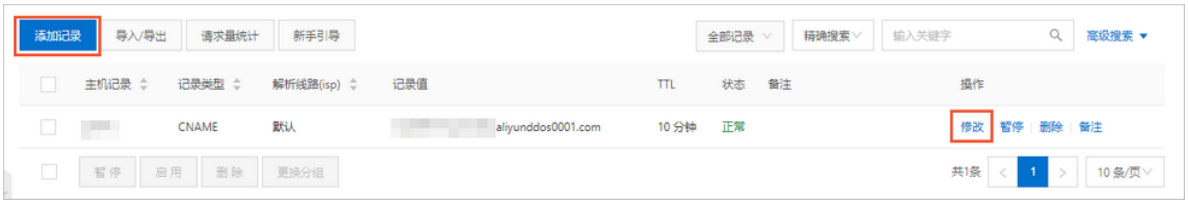
如果您使用其他DNS服务商的域名解析服务，请登录服务商系统修改网站域名的解析记录，下文内容仅供参考。

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（本示例中对应主机记录为**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。

相关操作

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。

5.3.2 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

- 已开通DDoS高防（新BGP）实例。

> **说明：**
> 目前仅DDoS高防（新BGP）服务支持NS接入，如果您使用DDoS高防（国际）服务，建议您使用修改DNS解析的方式接入DDoS高防。更多信息，请参见修改DNS解析接入网站业务。

- 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方式支持以下两种工作模式：

- DDoS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。如果因为特殊情况无法使用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DDoS高防控制台。
2. 在顶部导航栏，选择**中国内地**地域。
3. 在左侧导航栏，单击**接入管理** > **域名接入**。
4. 在**域名接入**页面，定位到要操作的域名，单击其操作列下的**DNS设置**。

5. 在**DNS设置**页面，定位到**NS方式接入**模块，开启**状态**开关并选择一种接入模式：**DDoS高防**、**回源**。

   - DDoS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。

6. 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。

5.3.3 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DDoS高防控制台。

   b) 在顶部导航栏，选择服务所在地域：

   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务

   c) 在左侧导航栏，单击**接入管理** > **域名接入**。

   d) 在**域名接入**页面，单击**添加网站**。

   e) 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。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。

   成功添加网站后，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**接入管理** > **端口接入**。

   b) 在**端口接入**页面，选择要操作的DDoS高防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：

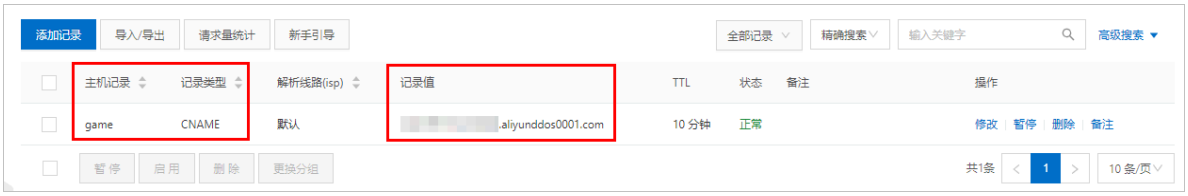
- **转发协议**：本示例中选择TCP。
- **转发端口**：本示例中填写1234。
- **源站端口**：本示例中填写1234。
- **源站IP**：填写真实源站IP，本示例中是1.1.1.1。

更多信息，请参见添加规则。

d) 重复上述两个步骤，在当前DDoS高防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IP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。

5.3.4 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通用联动规则、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通用联动规则或CDN联动后，流量调度器为规则/域名分配一个CNAME地址。修改CNAME解析接入流量调度器时，您需要将网站域名的解析指向流量调度器CNAME地址。

说明：

流量调度器CNAME地址可在**流量调度器**页面查询。

- 通用联动规则：将联动云资源IP对应的域名解析指向通用联动规则对应的CNAME地址。

- CDN联动：将开启CDN联动的域名的解析指向域名对应的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。

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

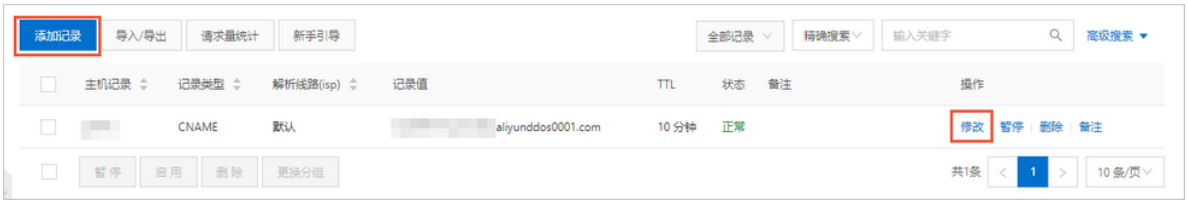
假设调度规则对应的网站域名为bgp.ddostest.com；以下操作示例描述了在云解析DNS控制台修改/新增域名解析的具体操作。

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（本示例中对应主机记录为**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**修改为通用联动规则或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。

5.4 流量调度器

DDoS高防提供流量调度器，允许您设置DDoS高防和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攻击时日常业务流畅运行、发生DDoS攻击时可切换至DDoS高防，为您的业务提供防护。流量调度器提供云产品联动、阶梯防护、CDN/DCDN联动、出海加速（仅限海外地区）功能。本文介绍流量调度器的使用场景和配置方法。

DDoS高防（新BGP）和DDoS高防（国际）服务差异

注意：

DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

DDoS高防（BGP）和DDoS高防（国际）在流量调度器上存在以下功能差异。

说明：

下表仅罗列存在差异的功能点，不包括在DDoS高防（BGP）和DDoS高防（国际）中完全相同的功能点。

功能	描述	DDoS高防（新BGP）	DDoS高防（国际）
出海加速	使用DDoS高防（国际）防护业务，无攻击时，业务使用加速IP；被攻击时，切换到DDoS高防。	不支持	支持

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，防止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攻击，无延迟增加；被大流量攻击的时候，需要切换到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/DCDN联动	网站使用CDN或DCDN加速，又需要防御DDoS攻击；当攻击发生时，需要从CDN或DCDN切换至DDoS高防。	无攻击时，就近使用CDN或DCDN节点加速；被攻击时，切换至DDoS高防。 

功能	使用场景	使用效果
出海加速 **说明：** 仅DDoS高防（国际）服务支持该功能。	使用DDoS高防（国际）防护业务，无攻击时，业务使用加速IP；被攻击时，需要切换到DDoS高防。	无攻击时，使用加速线路IP；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。
	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。
出海加速 **说明：** 仅DDoS高防（国际）服务支持该功能。	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。
CDN/DCDN联动	CDN/DCDN状态	域名不允许是切入沙箱状态。 **说明：** 如果域名已经被CDN或DCDN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。

功能	限制条件	说明
	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。

CDN/DCDN和DDoS高防切换条件

启用CDN/DCDN联动功能时，您需要设置访问QPS阈值，作为CDN/DCDN和DDoS高防间相互切换的条件。CDN/DCDN和DDoS高防间相互切换满足以下逻辑和限制。

- CDN/DCDN切换到高防
  - 连续3分钟内3次触发QPS超过阈值或连续10分钟内出现6次以上，并且CDN/DCDN上流量不超过10 Gbps，则触发切换流程。

    说明：
    10 Gbps流量超出了DDoS高防的售卖规格。
  - 当高防侧监测到域名进入沙箱状态，并且CDN/DCDN上流量不超过10 Gbps，触发切换流程。
- 高防切换到CDN/DCDN
  - 连续12小时以上，域名QPS低于QPS阈值的80%、CC阻断率低于10%，则触发回切流程。
  - 回切检查：要切回的高防IP不在清洗中、黑洞中和沙箱状态且1小时内不存在清洗、黑洞事件。
  - 回切时间范围：上午8时到晚上23时，其他时间不触发回切。

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。具体操作请参见添加网站。 2. 验证高防实例可以正常转发。具体操作请参见本地验证转发配置生效。 3. 配置流量调度器。 • 一对一切换，具体操作请参见添加通用联动规则。 • 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，在添加通用联动规则时，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。配置方法请参见多路分摊切换配置。 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，请参见修改CNAME解析接入流量调度器。
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。
出海加速 **说明：** 仅DDoS高防（国际）服务支持该功能。	配置步骤如下。 1. 配置DDoS高防转发。具体操作请参见添加网站。 2. 验证高防实例可以正常转发。具体操作请参见本地验证转发配置生效。 3. 配置流量调度器。具体操作请参见添加通用联动规则。 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，请参见修改CNAME解析接入流量调度器。

功能	配置说明
CDN/DCDN联动	配置步骤如下。 1. 预先配置好CDN/DCDN，并解析到CDN/DCDN，经测试可用。 具体操作请参见#unique_79。 **说明：** 如果配置了源站防护（安全组），则需要将CDN/DCDN回源地址加入白名单。 2. 配置DDoS高防转发。具体操作请参见添加网站。 3. 验证高防实例可以正常转发。具体操作请参见本地验证转发配置生效。 4. 配置流量调度器。具体操作请参见添加CDN/DCDN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，请参见修改CNAME解析接入流量调度器。

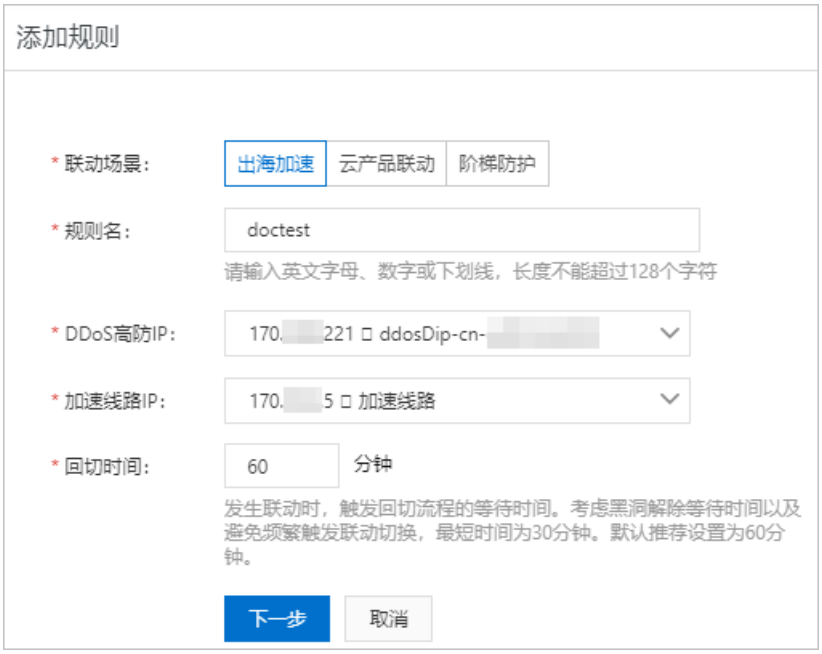
添加通用联动规则

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **流量调度器**。
4. 在**通用联动**页签下，单击**添加规则**。

5. 在**添加规则**页面，完成联动规则配置，并单击**下一步**。

图 5-1: DDoS高防（新BGP）云产品联动配置示例

图 5-2: DDoS高防（国际）出海加速配置示例



参数	描述
联动场景	选择规则类型，取值： • **出海加速** **说明：** 仅DDoS高防（国际）服务支持该选项。 • **阶梯防护** **说明：** 仅支持DDoS防护包防护对象中的云资源，包括ECS、EIP、SLB、WAF。 • **云产品联动**
规则名	为规则命名。规则名由英文字母、数字和下横线（_）组成，不超过128个字符。
DDoS高防IP	选择要联动的高防实例。
加速线路IP	在**出海加速**场景下，选择要联动的加速线路IP。 **说明：** 仅DDoS高防（国际）服务支持该选项。
云资源	在**云产品联动**和**阶梯防护**场景下，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**添加云资源IP**，可以添加多个云资源。最多支持添加20个IP。
回切时间	发生联动后，允许触发回切流程的等待时间。 考虑到黑洞解除的等待时间以及避免频繁触发联动切换，回切时间的最小值为30分钟。推荐您设置为60分钟。

成功添加规则后，流量调度器为新建规则分配一个CNAME地址。要使联动规则生效，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流量调度器分配的CNAME地址。您可以在规则列表中查看新建的规则和CNAME地址。

执行一键回切

通用联动规则添加生效后，如果云资源流量被调度到DDoS高防，您可以根据需要执行一键回切，将流量切回到云资源。

执行回切操作时，可能出现的异常结果如下：

- 如果联动资源全部在黑洞中，回切动作将会失败。
- 如果存在部分联动资源已经解除黑洞，部分联动资源还在黑洞中，流量将先回切到已经解除黑洞的联动资源上，其他资源等待黑洞解除后自动恢复流量。

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **流量调度器**。
4. 在**通用联动**页签，定位到要操作的规则，单击其操作列下的**回切**并确认操作。

> **说明：**
> 只有当发生了联动且流量联动到DDoS高防的时间不小于规则的**回切时间**，**回切**操作才会出现。

添加CDN/DCDN联动

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **流量调度器**。
4. 单击**云产品联动**页签。
   CDN/DCDN联动调度页面展示了所有已添加到DDoS高防中的网站域名。

5. 定位到要配置的域名，单击其操作列下的**添加联动**。

6. 在**添加联动**页面，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：

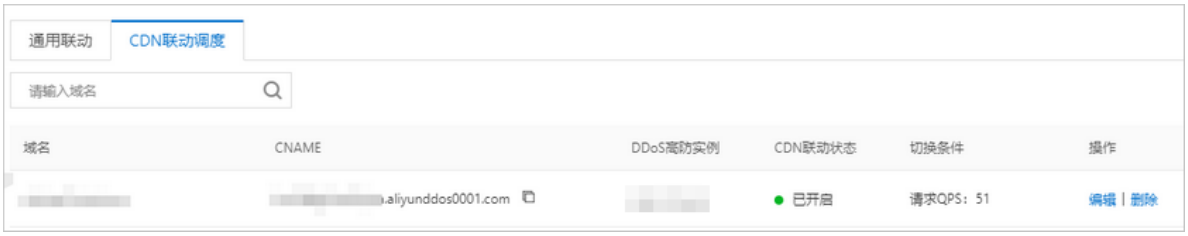
- **DDoS高防实例**：已开通增强功能。
- **联动资源**：已完成阿里云CDN/DCDN配置。

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。

成功添加联动后，流量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流量调度

器分配的CNAME地址。您可以在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

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。

1. 防护包配置。在防护包中添加多个防护对象，例如三个。具体操作请参见#unique_80。
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DDoS高防IP。具体操作请参见添加通用联动规则。
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。具体操作请参见修改CNAME解析接入流量调度器。
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。

5.5 CNAME复用

若您在同一个服务器上有多个网站域名需要接入DDoS高防（国际）服务，您可以申请开通CNAME复用，实现只添加一次高防配置，而使高防配置的CNAME地址供多个域名复用。开启CNAME复用后，您只需将同服务器上多个域名的解析指向高防CNAME地址，即可将多个域名接入高防，无需为每个域名分别添加高防配置。

前提条件

CNAME复用需要申请开放后才能使用。若有相关需求，请通过工单提交申请。本文操作描述建立在已开放CNAME复用的前提下。

说明：
仅DDoS高防（国际）服务支持CNAME复用。如果您使用DDoS高防（新BGP）服务，则暂时不支持使用CNAME复用。

使用场景

CNAME复用适用于以下场景：

- 场景1：代理商、ISV、分销商有大量域名（大部分域名的源站是同一个服务器）需要接入DDoS高防，且域名有频繁增删。每个域名都做高防配置太麻烦。
- 场景2：同一个业务使用大量不同一级域名做推广、SEO。每个域名都做高防配置太麻烦。
- 场景3：同一个业务使用大量备用域名。每个域名都做高防配置太麻烦。

使用限制

下表描述了CNAME复用的使用限制。

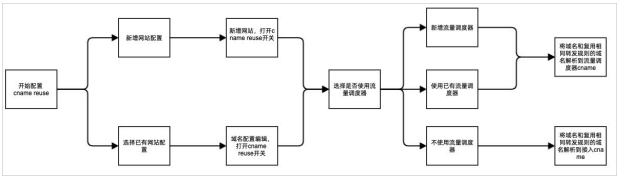
限制条件	说明
协议类型	仅支持HTTP协议，不支持HTTPS协议。
源站	复用CNAME的一组域名必须对应同一个源站。

开启CNAME复用

CNAME复用支持结合流量调度器使用，在开启CNAME复用时，您根据需要选择是否结合流量调度器。关于流量调度器的说明，请参见流量调度器。

- 若结合流量调度器使用，则需要关联对应的通用联动规则，且域名解析中将复用联动规则的CNAME地址。
- 若不使用流量调度器，则域名解析中将复用高防网站配置的CNAME地址。

下图描述了CNAME复用的配置流程。



为便于后续操作描述，做以下假设：

- 源站服务器有两个IP：1.1.1.1、2.2.2.2。
- 源站（1.1.1.1）有三个域名：a.test、b.test、c.test。

以下操作描述了使用CNAME复用，将一个源站IP（1.1.1.1）下多个域名（a.test、b.test、c.test）接入DDoS防护（国际）的配置方法。

1. 在网站配置中开启Cname Reuse。

   a) 登录DDoS高防控制台。

   b) 在顶部导航栏，选择**非中国内地**地域。

   c) 在左侧导航栏，单击**接入管理** > **域名接入**。

   d) 添加一个网站配置或者编辑已有网站配置，在网站配置中开启**Cname Reuse**。关于添加网站配置的具体操作，请参见添加网站。

   示例：源站IP是1.1.1.1，网站是a.test（也可以是b.test、c.test）。

2. 选择是否结合流量调度器及更新域名CNAME解析。

   在启用CnameReuse时，您需要选择是否结合流量调度器。

   - 不使用流量调度器

     a. 在**选择流量调度器**对话框中，选择**不使用流量调度器**，并单击**确定**。

     b. 成功添加网站配置后，记录网站配置的CNAME地址。

     c. 前往域名服务商，更新源站（1.1.1.1）对应的所有网站（a.test、b.test、c.test）的域名解析，应用CNAME解析并将记录值更新为网站配置的CNAME地址。

   - 使用流量调度器

     a. 在**选择流量调度器**对话框中，选择**使用流量调度器**，并选择对应的流量调度规则，单击**确定**。

     流量调度器规则应联动网站配置中用到的源站IP（1.1.1.1）和DDoS高防IP。若您还未创建对应规则，请单击**新建流量调度规则**添加对应规则（见下图示例），再选择应用规则。

     说明：

联动规则中的DDoS高防IP必须和网站配置中关联的DDoS高防实例一致。

b. 成功选择流量调度器规则后，记录调度规则的CNAME地址。

c. 前往域名服务商，更新源站（1.1.1.1）对应的所有网站（a.test、b.test、c.test）的域名解析，应用CNAME解析并将记录值更新为调度规则的CNAME地址。

3. （可选）若仍需要为不同源站（2.2.2.2）对应的域名接入DDoS防护，请重复步骤1~2进行配置。

关闭CNAME复用

若不再需要使用CNAME复用，您可以在网站配置中关闭Cname Reuse。

注意：
关闭Cname Reuse前，请确保所有复用高防CNAME的域名已不再解析到高防，否则关闭功能后会导致网站流量转发失败。

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**非中国内地**地域。
3. 在左侧导航栏，单击**接入管理** > **域名接入**。
4. 编辑已有网站配置，并在网站配置中关闭**Cname Reuse**。
5. 根据需要选择是否保留网站配置和防护调度规则。
   - 若保留网站配置，则网站配置中的转发逻辑继续生效。
   - 若保留防护调度规则，则流量调度器继续生效。

5.6 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

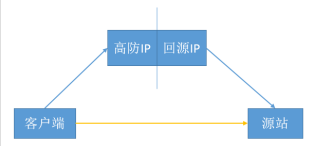
如果您的源站服务器上部署了非阿里云安全软件（例如防火墙），请将DDoS高防的回源IP地址加入安全软件的白名单。

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。

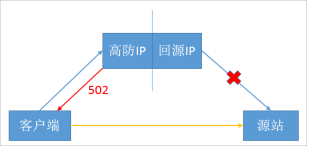
DDoS高防作为一个反向代理，其中包含了一个Full NAT的架构。



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。

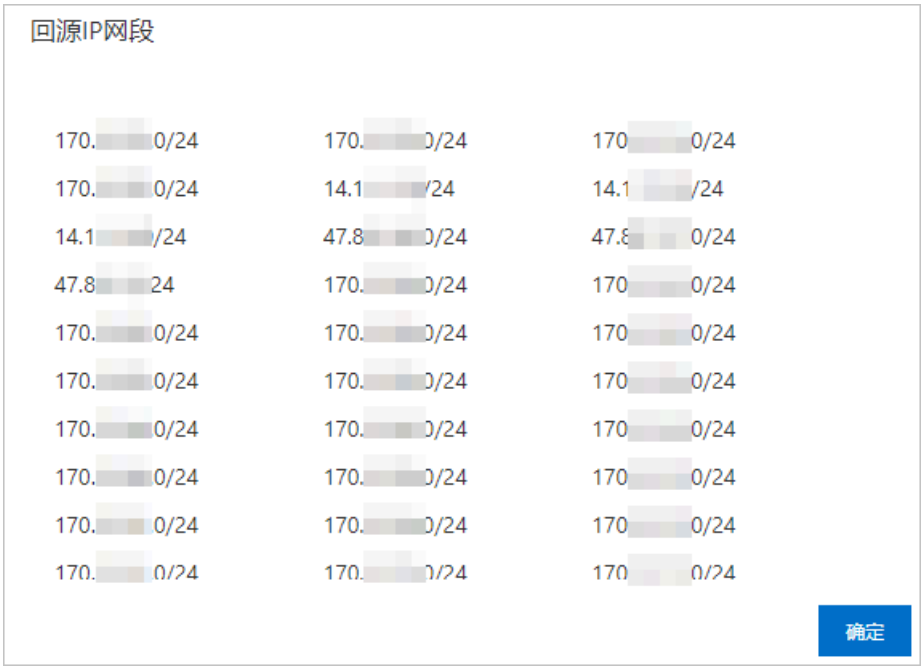
例如，最常见的502错误，即表示高防IP转发请求到源站，但源站却没有响应（因为回源IP可能被源站的防火墙拦截）。



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。

操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **域名接入**。
4. 在**域名接入**页面右上方，单击**查看回源IP网段**。
5. 在**回源IP网段**对话框中，查看并复制DDoS高防的回源地址。



6. 打开源站服务器上的安全软件，将复制的回源地址添加到白名单。

5.7 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。您可以在域名接入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。

5.8 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

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. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **域名接入**。
4. 在**域名接入**页面右上方，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。
5. 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**。

6. 返回**更换ECS IP**对话框，输入**ECS实例ID**，并单击**下一步**。
7. 确认当前ECS实例信息准确无误（尤其是ECS IP）后，单击**释放IP**。
8. 成功释放原IP后，单击**下一步**，为该ECS实例自动分配新的IP。
9. ECS IP更换成功后，单击**确认**，完成操作。

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

5.9 配置DDoS高防（国际）加速线路

DDoS高防（国际）加速线路需要与DDoS高防（国际）保险版或无忧版结合使用，用于实现中国内地地区用户对您部署在非中国内地地区业务的快速访问。

前提条件

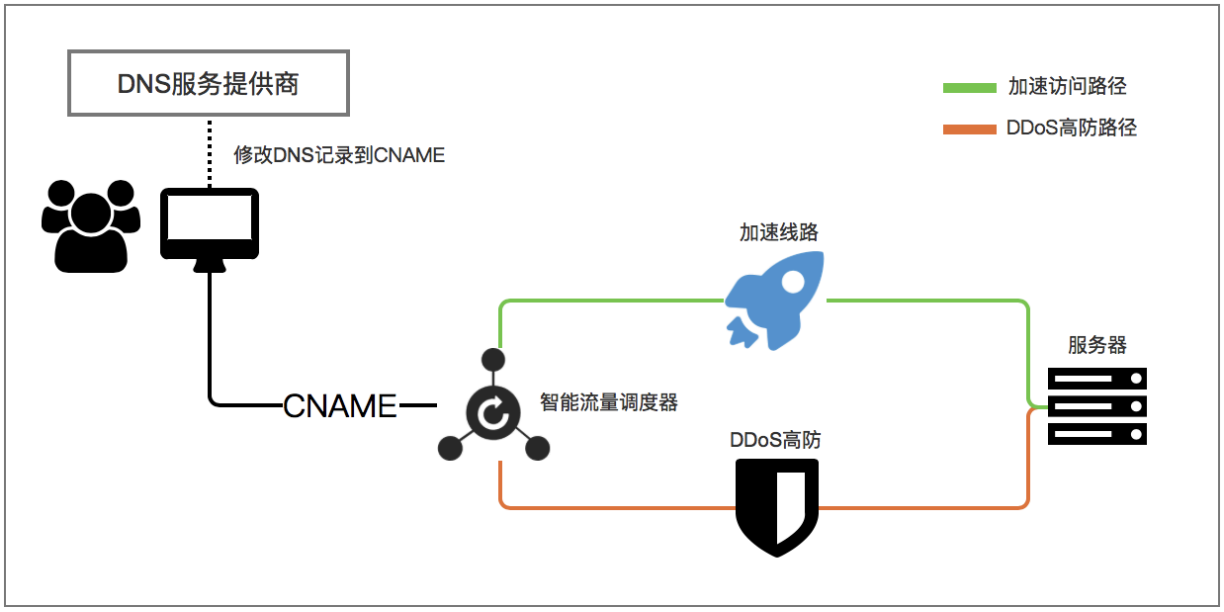
已开通DDoS高防（国际）实例。

> **说明：**
> 仅DDoS高防（国际）服务支持加速线路。如果您使用DDoS高防（新BGP），则无法使用该功能。

背景信息

为DDoS高防（国际）保险版或无忧版配置加速线路，可以实现当您的业务在无攻击的情况下，通过加速线路实现业务的快速访问，而当遭受攻击时自动切换至DDoS高防（国际）线路缓解DDoS攻击。

关于建议配置加速线路的场景说明，请参见DDoS高防（国际）应用场景。



您可以为网站域名（七层）或业务端口（四层）配置DDoS高防（国际）加速线路。

购买DDoS高防（国际）加速线路和保险版、无忧版套餐后，在DDoS高防（国际）管理控制台中将您的网站域名或业务端口配置接入DDoS高防（国际）实例进行防护，配置智能流量调度器实现业务流量在加速线路和DDoS高防线路的自动切换，最终将正常流量回送到源站服务器。

操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**非中国内地**地域。
3. 将您的网站业务或非网站业务配置接入DDoS高防（国际）保险版、无忧版实例和加速线路实例。

> **说明：**
> 您只需完成网站或非网站业务接入配置，无需修改DNS解析。

- 网站域名接入DDoS高防（国际）实例：请参见添加网站进行接入配置。您在选择高防独享IP时，需要同时选择DDoS高防（国际）保险版、无忧版实例和加速线路实例的两个独享IP。
- 业务端口接入DDoS高防（国际）实例：请参见添加规则进行配置。您需要在DDoS高防（国际）保险版、无忧版实例和加速线路实例中配置转发规则，即分别选择DDoS高防（国际）保险版、无忧版实例和加速线路实例为您的非网站业务配置转发规则。

> **说明：**
> 业务端口配置接入DDoS高防（国际）加速线路仅支持通过域名指定服务器地址的非网站业务。对于业务直接通过IP访问的场景，无法实现业务流量的自动调度。

4. 前往**流量调度器**页面，打开**防护调度**页签，并单击**添加规则**。

5. 在**添加规则**侧边页，设置规则条件，并单击**下一步**。

   - **联动场景**：选择**出海加速**。
   - **规则名**：为规则命名。
   - **高防IP**：设置为DDoS高防（国际）保险版、无忧版实例的独享IP。
   - **加速线路IP**：设置为DDoS高防（国际）加速线路实例的独享IP。

   通过该规则，在业务无攻击的情况下，优先使用加速线路实现快速访问；在遭受攻击的情况下，流量调度器将自动将流量切换至防护线路进行流量清洗。

   流量调度规则创建后将生成CNAME，您只需将业务域名的DNS解析指向该CNAME即可通过安全流量调度器实现流量的自动调度。

   说明：
   请务必确认调度节点中所选择的独享IP已经完成业务接入配置，可以将流量正常转发回源站服务器。

6. 在域名解析服务提供商处，修改该域名的DNS解析记录。

   将域名解析至安全流量调度规则提供的CNAME，正式将业务流量切换到安全流量调度器，实现自动调度。

   说明：
   流量自动调度功能基于CNAME，因此域名解析必须使用CNAME方式。

6 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。

前提条件

已开通DDoS高防（新BGP/国际）实例并完成业务接入。

背景信息

注意：

DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

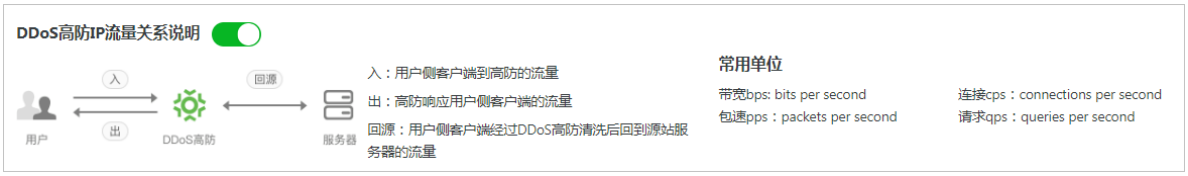
DDoS高防的安全总览页面向您展示以下业务指标和DDoS攻击事件的概览：

- 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。

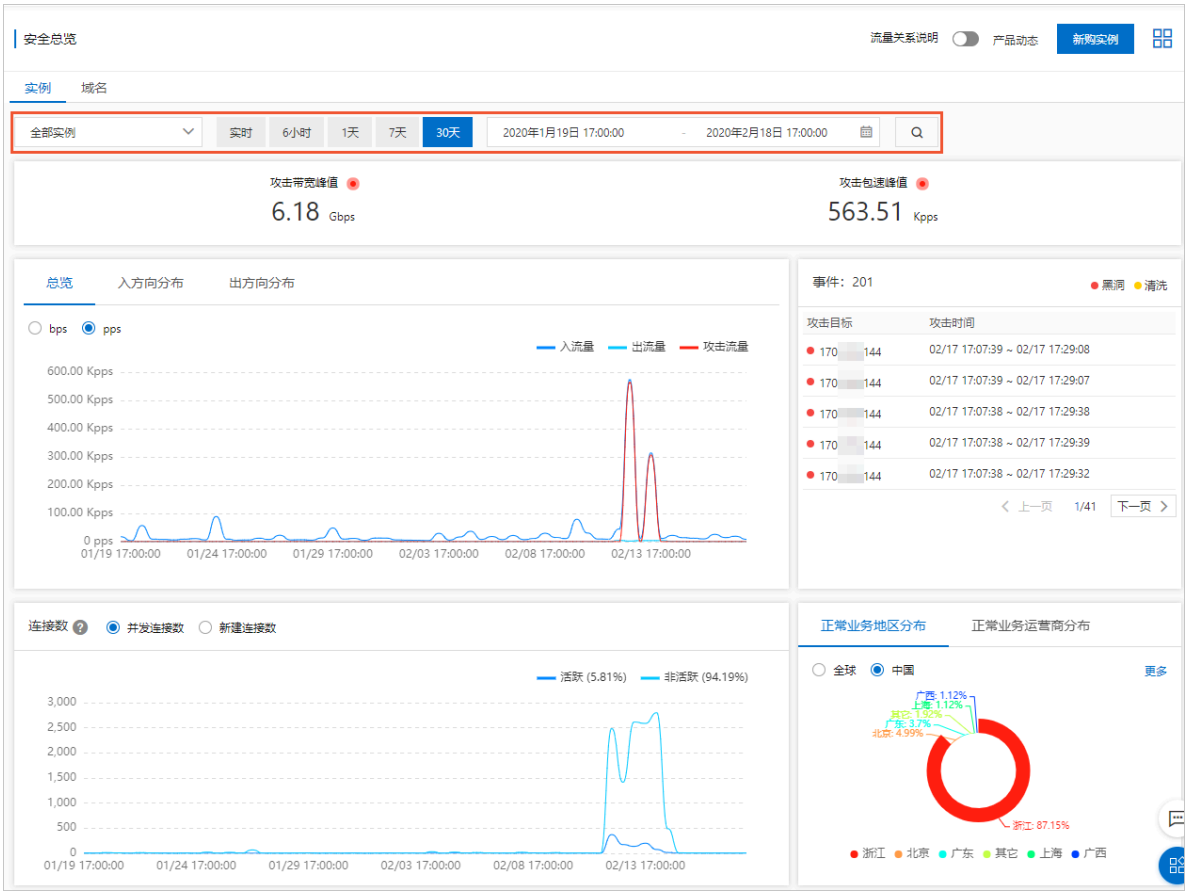
操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**安全总览**。
4. （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。

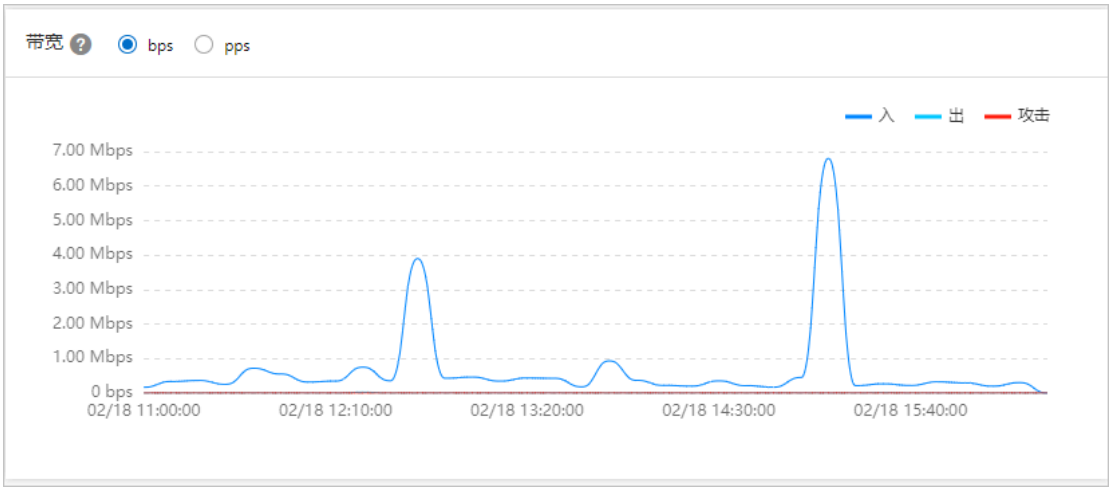


5. 打开**实例**页签，设置要查询的实例和时间范围，查看指定实例对应业务的相关信息。

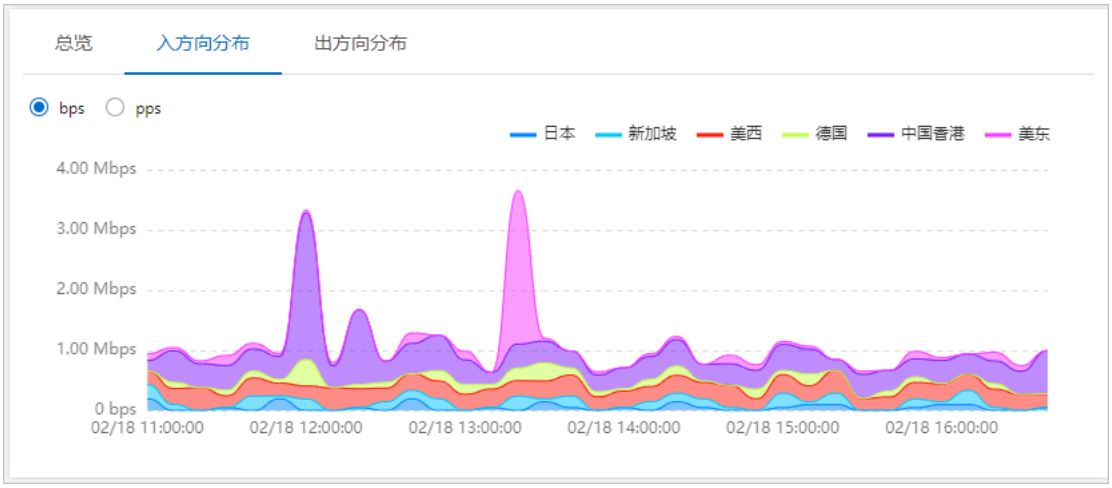


支持查看的实例业务信息包括以下内容。

- **攻击带宽峰值**和**攻击包速峰值**
- 流量趋势信息
  - DDoS高防（新BGP）服务提供**带宽**趋势图，以**bps**/**pps**展示指定时间段内实例上的入流量、出流量、攻击流量趋势。



- DDoS高防（国际）提供三个页签，分别是**总览**（同带宽趋势图）、**入方向分布**（入方向流量的分布信息）、**出方向分布**（出方向流量的分布信息）。



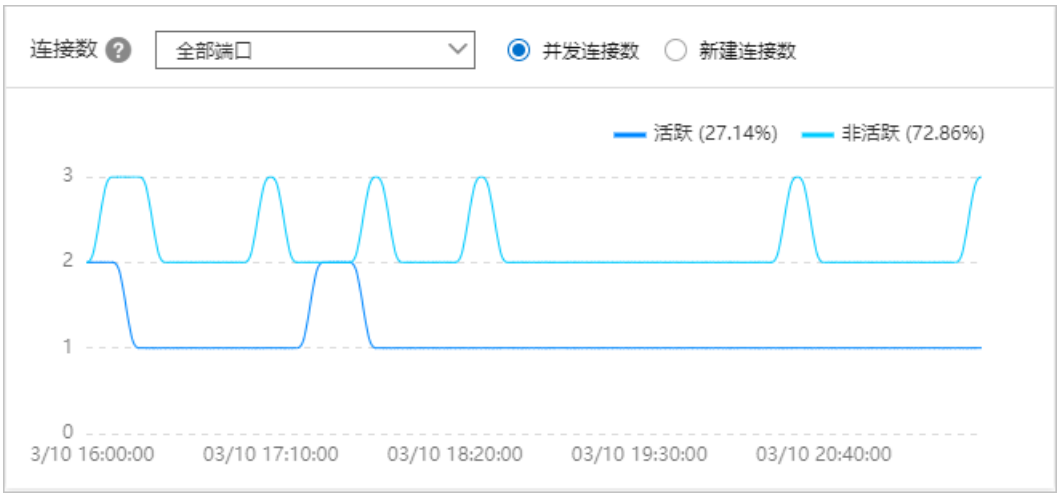
- （黑洞和清洗）**事件**记录表

  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

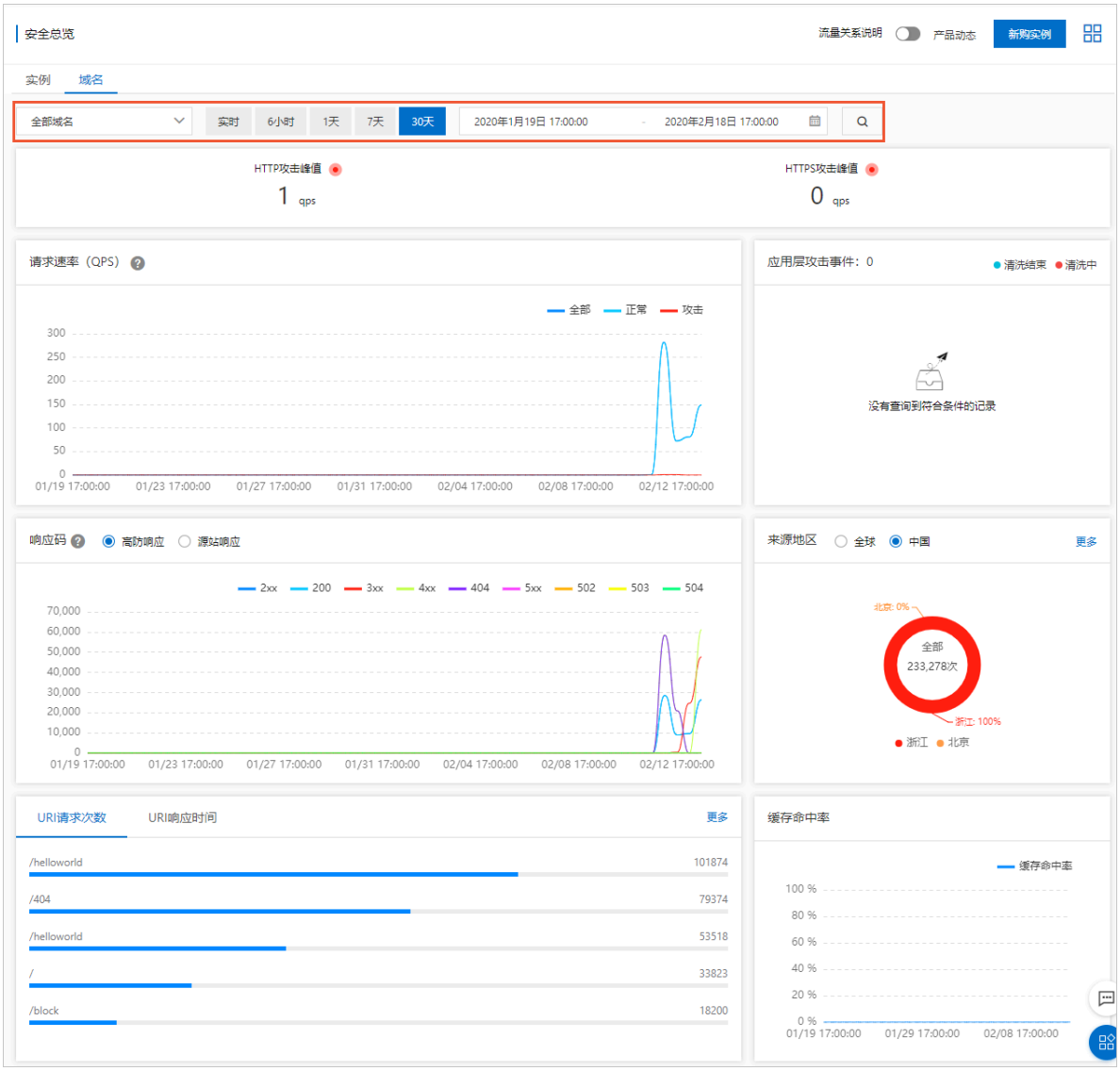
说明：

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。如果选择一个以上实例，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

6. 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

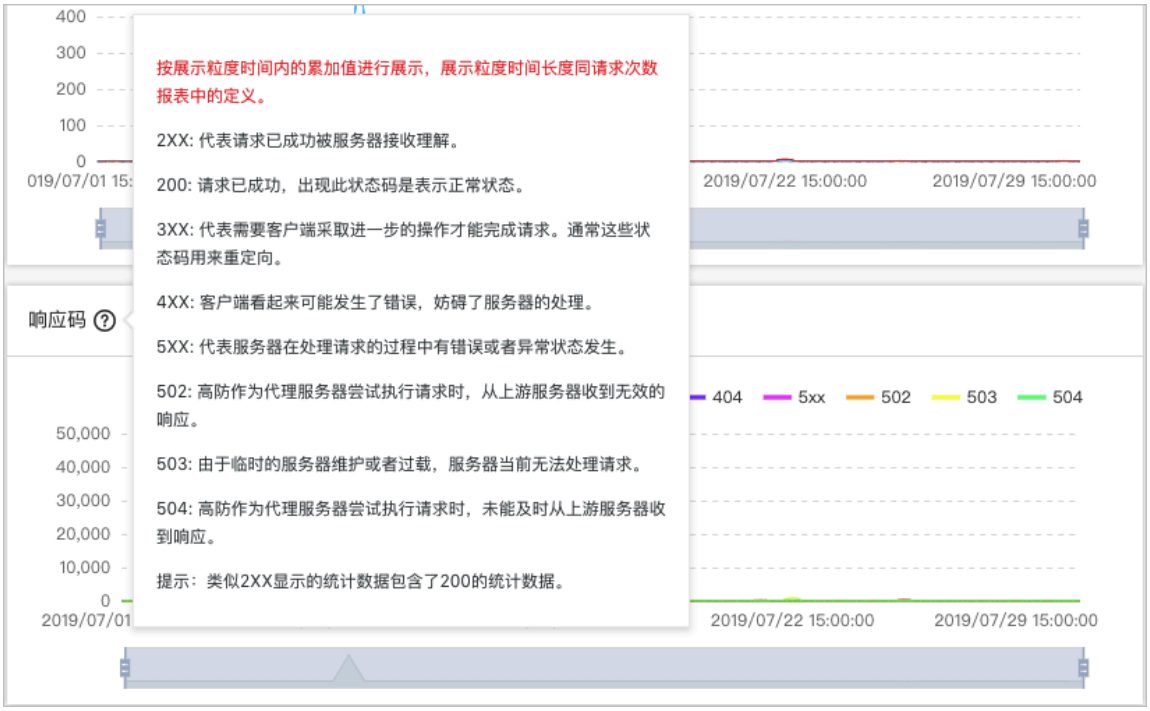
  请求次数趋势图按峰值展示，不同的查询时间间隔对应的展示粒度不同，具体如下：

  - 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，请参见设置静态页面缓存。

7 查看安全报表

业务接入DDoS高防（新BGP）且切换业务流量至DDoS高防（新BGP）实例后，您可以在安全报表页面查看业务流量统计与DDoS攻击防护情况。

前提条件

已开通DDoS高防（新BGP）实例并完成业务接入。

> **说明：**
> 目前仅DDoS高防（新BGP）服务支持安全报表功能。如果您使用DDoS高防（国际）服务，则暂时无法使用安全报表，建议您通过安全总览页面了解业务防护情况。

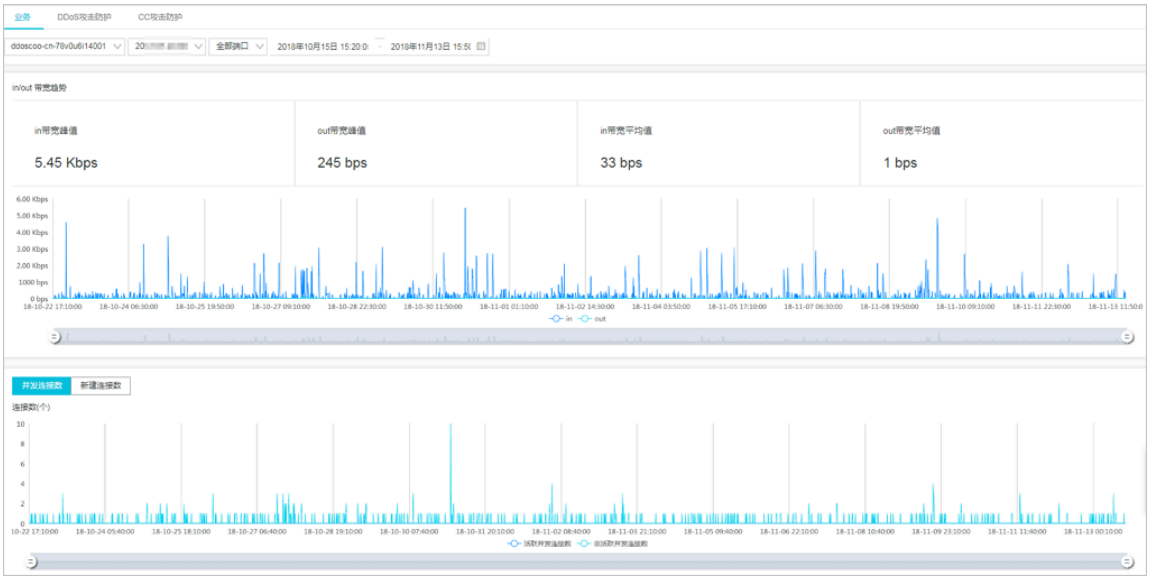
操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**中国内地**地域。
3. 在左侧导航栏，单击**安全报表**。
4. 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。



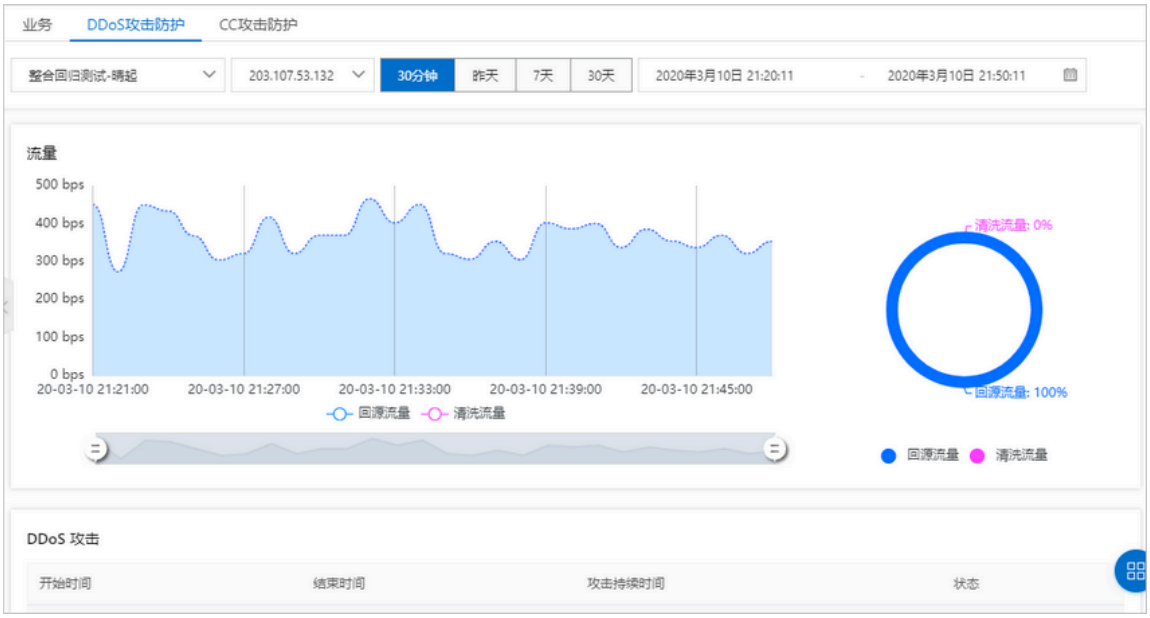
您可以拖动趋势图下方的滑块，快速调整查询时间范围，聚焦指定时间段。

- 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：

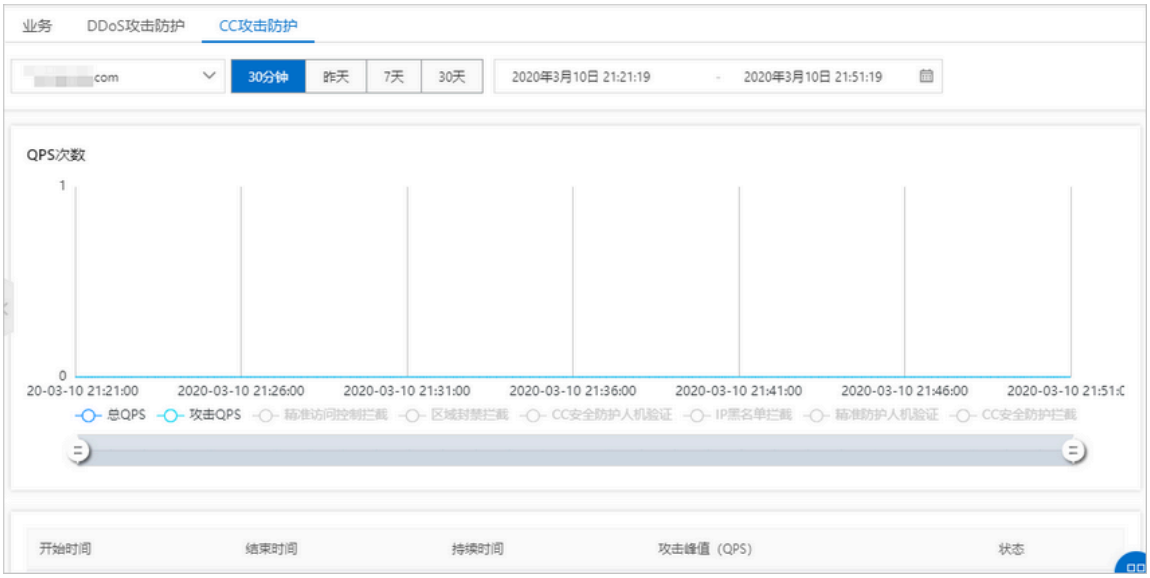
DDoS高防服务会自动过滤网络流量中存在的一些畸形包（例如SYN小包、SYN标志位异常等不符合TCP协议的数据包），使您的业务服务器无需浪费资源处理这些明显的畸形包。这类被过滤的畸形包也将被计入清洗流量中，因此可能出现您的服务器流量未达清洗阈值，但流量图表中出现清洗流量的情况。

- 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。



8 防护设置

8.1 基础设施DDoS防护

8.1.1 设置黑白名单（针对目的IP）

黑白名单（针对目的IP）允许您针对访问DDoS高防实例的源IP设置封禁或者放行。您可以根据业务需要为DDoS高防实例单独配置黑名单、白名单，例如添加、移除IP。黑名单中也包含DDoS高防智能防御算法标记的恶意IP。同时，黑白名单支持导出到本地。本文介绍了黑白名单的具体操作方法。

前提条件

已开通DDoS高防（新BGP）实例。

> **说明：**
> 目前仅DDoS高防（新BGP）服务支持黑白名单（针对目的IP）功能。如果您使用DDoS高防（国际）服务，则暂时无法使用该功能。

背景信息

> **注意：**
> DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

黑白名单（针对目的IP）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。如果恶意IP在有效期内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。如果某个IP已经在白名单中，则无法被添加至黑名单中。

操作步骤

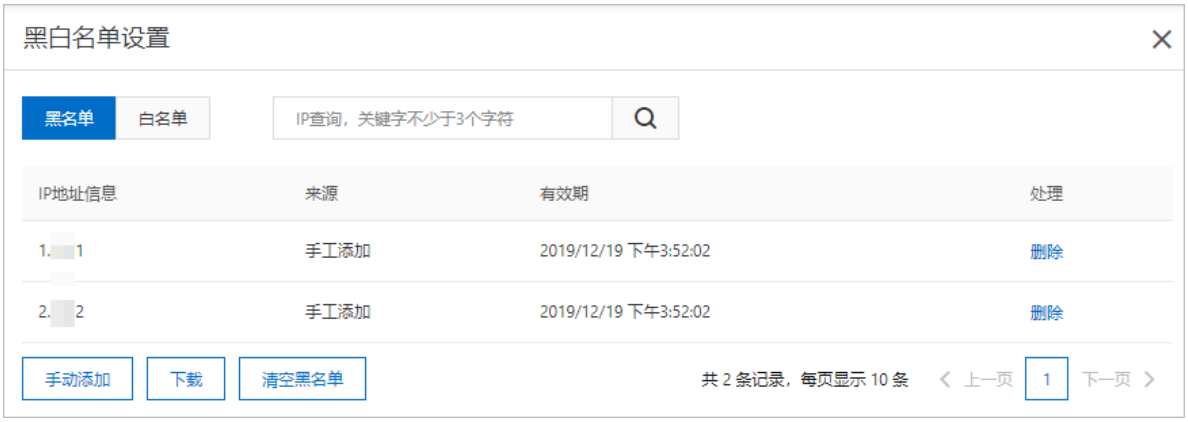
1. 登录DDoS高防控制台。

2. 在顶部导航栏，选择**中国内地**地域。
3. 在左侧导航栏，单击**防护设置** > **通用防护策略**。
4. 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。

5. 定位到**黑白名单（针对目的IP）**配置区域，单击**设置**。

6. 在**黑白名单设置**页面，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7。
- 白名单管理请参见步骤8。

7. （可选） 管理黑名单。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，输入要拉黑的请求来源IP并选择**拉黑时间**。

> **说明：**

黑名单中最多支持手动添加2000个IP。

c. 单击**添加**。

成功添加黑名单IP后，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

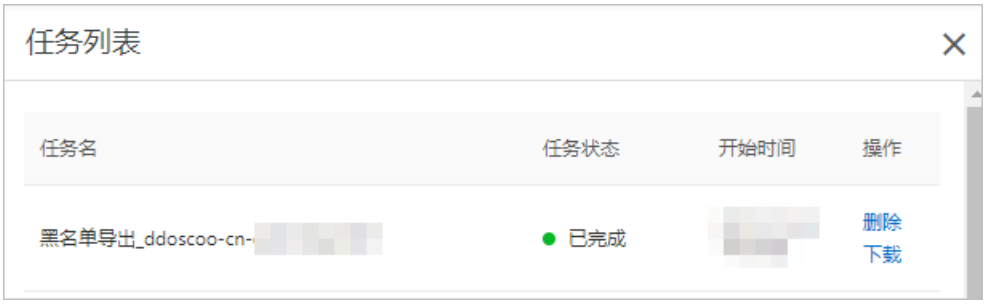
a. 单击**下载**，下发黑名单导出任务。

b. 在导出任务已下发提示中，单击**确定**。

c. 关闭当前**黑白名单设置**页面，返回上一级页面。

d. 单击页面右上角的任务图标（ ），展开任务列表。

e. 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**。



成功下载黑名单IP到本地后，您可以打开下载的txt文件查看黑名单明细。

8. （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：

白名单中最多支持手动添加2000个IP。

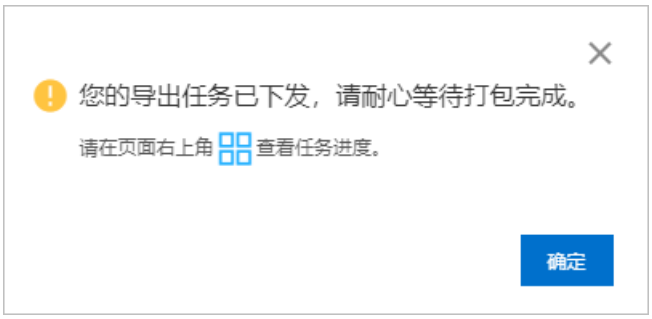
c. 单击**添加**。

成功添加白名单IP后，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. 关闭当前**黑白名单设置**页面，返回上一级页面。

d. 单击页面右上角的任务图标（ ），展开任务列表。

e. 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**。

成功下载白名单IP到本地后，您可以打开下载的txt文件查看白名单明细。

8.1.2 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。

前提条件

已开通DDoS高防（新BGP）实例。

说明：

目前仅DDoS高防（新BGP）服务支持近源流量压制功能。如果您使用DDoS高防（国际）服务，则暂时无法使用该功能。

背景信息

注意：

DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

当您的DDoS高防实例遭遇特大流量攻击，且发现攻击流量有超过实例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，将攻击规模控制在实例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种因素，开启流量封禁可在一定情况下降低被黑洞的概率。

操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**中国内地**地域。

3. 在左侧导航栏，单击**防护设置** > **通用防护策略**。
4. 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。

5. 定位到**近源流量压制**配置区域，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。如果攻击流量还是很大，超过当前防护能力，则可以考虑再封禁联通海外流量。
- 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，请根据提示排查问题后再次尝试。如果未出现任何提示信息，则表示近源流量压制已成功。

6. （可选）回到**近源流量压制**配置区域，单击**查看封禁信息**，在**近源流量封禁**页面查看本次封禁的区域和时间范围。

7. （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。

8.1.3 设置区域封禁

区域封禁指针对访问DDoS高防实例的源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地区的源IP的访问请求。该功能针对增强功能套餐的DDoS高防实例生效。开启区域封禁后，由封禁地区到DDoS高防实例的流量将被丢弃。本文介绍了设置和开启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。

背景信息

注意：

DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

区域封禁通过直接丢弃来自指定中国地区、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。假设访问DDoS高防实例的正常用户均来自中国，您可以为DDoS高防实例设置区域封禁，封禁来自海外地区的访问请求。

说明：

区域封禁针对DDoS高防实例生效。如果您需要对多个不同DDoS高防实例开启区域封禁，则需要对不同DDoS高防实例分别进行设置。不支持对多个DDoS高防实例批量设置。

区域封禁VS近源流量压制

区域封禁在DDoS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（近目的流量封禁）。区域封禁根据源IP的归属区域在DDoS高防中识别过滤，并不能减小进入高防网络的攻击流量，适用于防护连接资源消耗型攻击。

相比于区域封禁，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。

说明：

目前仅DDoS高防（新BGP）服务支持近源流量压制功能。

区域封禁VS针对域名的区域封禁

针对域名的区域封禁功能和（针对DDoS高防实例的）区域封禁功能一起使用时，后者优先生效。

例如，针对DDoS高防实例已经通过区域封禁功能封禁了海外地区的流量，关联该DDoS高防实例的域名无论有没有设置区域封禁（针对域名）功能，海外地区用户都不能访问。如果需要实现部分业务封禁海外地区访问，部分业务不封禁海外地区访问，建议您设置针对域名的区域封禁，而非针对DDoS高防实例设置区域封禁。更多信息，请参见设置区域封禁（针对域名）。

操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**防护设置** > **通用防护策略**。
4. 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。

5. 定位到**区域封禁**配置区域，单击**设置**。

6. 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**。

7. 回到**区域封禁**配置区域，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。

8.1.4 黑洞解封

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防护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DDoS高防实例被持续打入黑洞。

前提条件

已开通DDoS高防（新BGP）实例。

> **说明:**
> 目前仅DDoS高防（新BGP）服务支持黑洞解封功能。如果您使用DDoS高防（国际）服务，则暂时无法使用该功能。

背景信息

> **注意:**
> DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

每个阿里云账号每天共拥有五次黑洞解封机会，每天零点自动恢复成五次。只有成功解除黑洞状态才会消耗一次解封机会。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，则相邻两次解封操作的间隔必须大于10分钟。

操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**中国内地**地域。
3. 在左侧导航栏，单击**防护设置** > **通用防护策略**。
4. 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。

5. 定位到**黑洞解封**配置区域，根据当前实例状态，执行黑洞解封。

- 如果实例处于**黑洞**状态，且您不希望等待黑洞自动解封，您可以单击**解封**，耐心等待黑洞状态成功解除。
- 如果实例是**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”，则请您耐心等待后再尝试。
- 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。

8.2 网站业务DDoS防护

8.2.1 设置AI智能防护

DDoS高防为已接入防护的网站业务提供AI智能防护功能。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高防域名接入中配置要防护的网站业务。更多信息，请参见添加网站。
- 已开启新版防护设置。

背景信息

注意：

DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和

配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

网站业务接入DDoS高防后，您可以为其开启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智能防护模式

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分析，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，请参见设置精准访问控制。

  一般情况下，建议您先使用预警模式，并通过全量日志分析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。

AI智能防护等级

开启AI智能防护时，您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	应用场景
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的场景。
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场景。

操作步骤

1. 登录DDoS高防控制台。

2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**防护设置** > **通用防护策略**。
4. 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。
5. 定位到**AI智能防护**配置区域，单击**修改设置**。

6. 在**AI智能防护**对话框，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智能防护后，DDoS高防在检测到恶意攻击行为时，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. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**防护设置** > **通用防护策略**。
4. 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。

5. 定位到**精确访问控制**配置区域，单击**设置**。

6. 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高防的全量日志分析功能将记录相应的攻击日志。您可以在全量日志分析中查询与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分析功能。更多信息，请参见全量日志分析。
- 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DDoS高防控制台，前往**调查分析** > **全量日志分析**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
```

8.2.2 设置黑白名单（针对域名）

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。开启黑白名单（针对域名），则黑名单IP/IP段对域名的访问请求会被直接阻断，白名单IP/IP段对域名的访问请求会被直接放行，且不经过任何防护策略过滤。本文介绍了设置针对域名的黑白名单的方法。

前提条件

已在DDoS高防域名接入中配置要防护的网站业务。更多信息，请参见添加网站。

背景信息

注意：

DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

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添加至针对域名的黑名单，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添加至针对域名的白名单予以放行，来自白名单IP的访问请求不会被拦截。

注意事项

- 针对域名的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，建议您设置基础设施DDoS防护策略下的黑白名单。更多信息，请参见设置黑白名单（针对目的IP）。

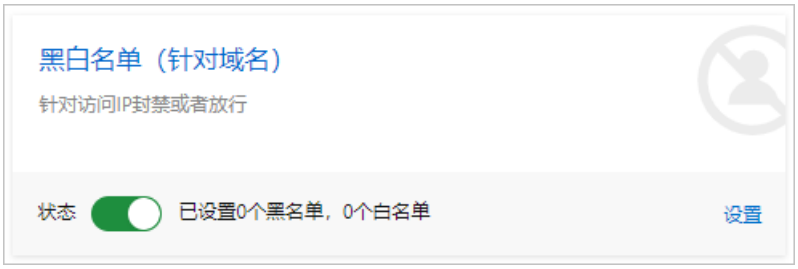
  说明：

  目前仅DDoS高防（新BGP）服务支持黑白名单（针对目的IP）功能。
- 黑白名单（针对域名）的设置仅对单个域名生效，而不是对整个DDoS高防实例。
- 针对单个域名，您最多可以分别配置200个黑名单、白名单IP或IP段。

操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务

3. 在左侧导航栏，单击**防护设置** > **通用防护策略**。
4. 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。
5. 定位到**黑白名单（针对域名）**配置区域，单击**设置**。



6. 在**黑白名单设置**对话框，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）**配置区域，开启**状态**开关，使黑白名单设置生效。

> **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

成功开启针对域名的黑白名单后，黑白名单设置将应用到所有与域名关联的DDoS高防实例，并针对域名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（针对域名）设置才会真正生效。如果黑白名单（针对域名）开启后，设置未立即生效，请尝试继续访问域名数次。

8.2.3 设置区域封禁（针对域名）

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访问请求封禁策略。开启针对域名的区域封禁功能后，您可以一键阻断指定地区来源IP对网站业务的所有访问请求。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高防域名接入中配置要防护的网站业务，且关联了增强功能套餐的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

注意：

DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

网站业务接入DDoS高防后，假设网站的正常用户均来自中国，则您可以开启区域封禁（针对域名），封禁来自非中国地区的访问请求。同理，您可以设置封禁其他非正常网站用户来源的区域。设置区域封禁（针对域名）时，您只需选择要封禁的区域即可，具体包括以下区域。

- 中国地区

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

- 国际地区

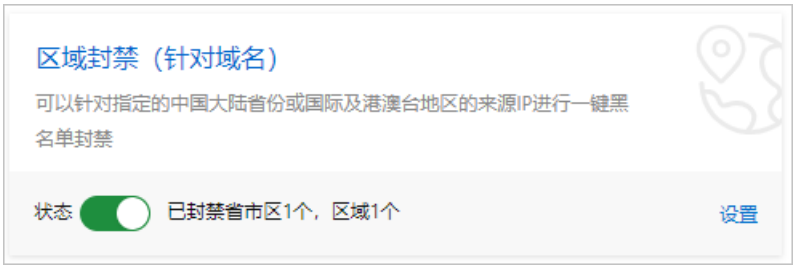
亚洲（国内除外）、欧洲、北美洲、南美洲、非洲、大洋洲、南极洲

注意事项

- 区域封禁（针对域名）仅支持防护网站业务。对于非网站业务若有类似需求，建议您设置基础设施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（目前仅新BGP高防支持）、设置区域封禁。
- 区域封禁（针对域名）对域名生效。如果您需要为多个域名设置区域封禁，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（针对域名）根据源IP的归属区域在DDoS高防中识别过滤，并不能减小进入高防网络的攻击流量。

操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**防护设置** > **通用防护策略**。
4. 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。
5. 定位到**区域封禁（针对域名）**配置区域，单击**设置**。



6. 在**选择需要封禁的区域**对话框，选中要封禁的区域，并单击**确定**。
7. 回到**区域封禁（针对域名）**配置区域，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后，区域封禁设置将应用到所有与域名关联的DDoS高防实例，并针对域名的访问流量即刻生效。

8.2.4 设置精准访问控制

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。开启精确访问控制后，您可以使用常见的HTTP字段（例如IP、URL、Referer、UA、参数等）设置匹配条件，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场景。

前提条件

- 已在DDoS高防域名接入中配置要防护的网站业务。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
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

匹配字段	字段描述	适用的逻辑符
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（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高防实例的功能套餐类型，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. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**防护设置** > **通用防护策略**。
4. 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。
5. 定位到**精确访问控制**配置区域，单击**设置**。

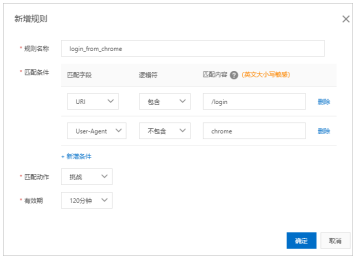
6. 为域名设置精确访问控制规则。

- 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，完成规则配置，并单击**确定**。



参数	描述
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，请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。

参数	描述
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。
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。

以上图为例，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后，您可以根据需要继续添加多条规则。

说明：

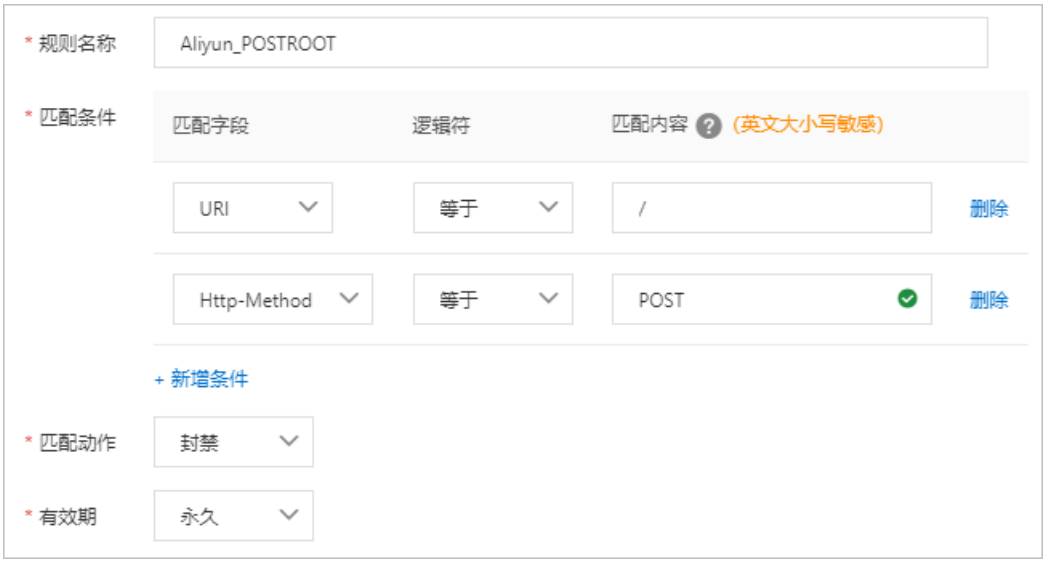
- 如果您设置了多条规则，则规则的优先级遵循其在规则列表中的排列顺序，排序越靠前，优先级越高。访问请求根据规则顺序依次进行匹配，顺序较前的精准访问控制规则优先匹配。

- 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

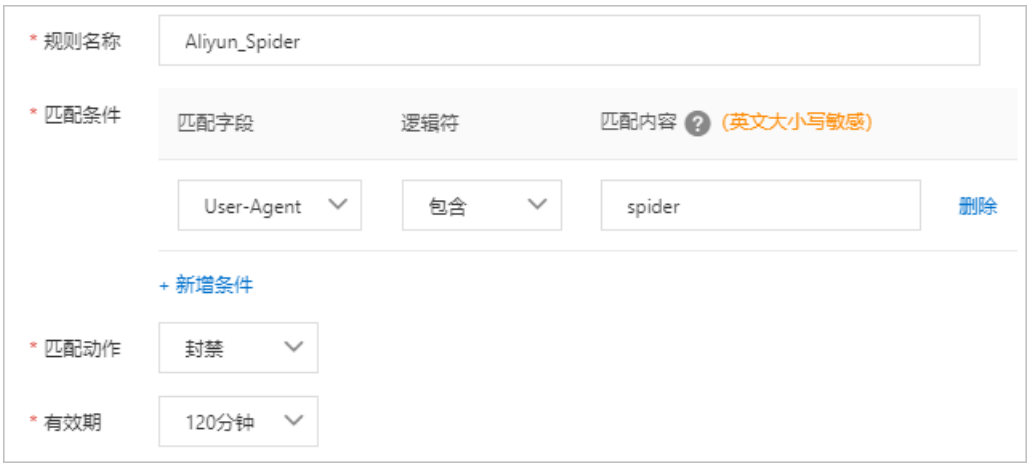
- 拦截特定的攻击请求

一般情况下，正常业务不存在POST根目录的请求信息。如果网站业务上发生CC攻击，且您发现客户端的请求中存在大量的POST根目录请求，则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**。

7. 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。

8.2.5 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高防域名接入中配置要防护的网站业务。更多信息，请参见添加网站。
- 已开启新版防护设置。

背景信息

注意:

DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

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，只有通过认证的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，即针对每个访问者进行验证，只有通过认证的访问者才允许访问网站。 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确的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. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**防护设置** > **通用防护策略**。
4. 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。

5. 定位到**频率控制**配置区域，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。

自定义频率控制防护规则

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**防护设置 > 通用防护策略**。
4. 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。
5. 定位到**频率控制**配置区域，开启**自定义规则**开关，并单击**设置**。

6. 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，完成规则配置，并单击**确定**。

参数	说明
规则名称	为该规则命名。
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。

参数	说明
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。
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后，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**。

7. 回到**频率控制**配置区域，开启**状态**开关，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。

8.3 非网站业务DDoS防护

8.3.1 设置四层AI智能防护

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。

前提条件

已开通DDoS高防（新BGP/国际）实例。更多信息，请参见开通DDoS高防。

背景信息

注意：

DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

针对网络四层DDoS攻击，DDoS高防智能防护结合历史业务流量和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，并选用正常防护等级。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，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针对DDoS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黑名单中的IP，也可以在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，请参见设置黑白名单（针对目的IP）。

说明：

目前仅DDoS高防（新BGP）服务支持针对目的IP的黑白名单功能。

操作步骤

1. 登录DDoS高防控制台。

2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**防护设置** > **通用防护策略**。
4. 在**通用防护策略**页面，单击**非网站业务DDoS防护**页签，并在页面上方选择要设置的DDoS高防实例。
5. 定位到**AI智能防护**配置区域，单击**修改设置**。

6. 在**AI智能防护**对话框，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后，目标DDoS高防实例将按照调整后的防护等级工作。

8.3.2 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高防实例下添加端口转发规则，接入非网站业务后，您可以单独设置某个端口的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

已在端口接入中配置非网站业务端口转发规则。更多信息，请参见添加规则。

背景信息

> **注意：**
> DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

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。

- 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，您可以开启将源IP加入黑名单的策略，并设置黑名单的有效时长。

设置端口DDoS防护策略

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DDoS高防控制台。

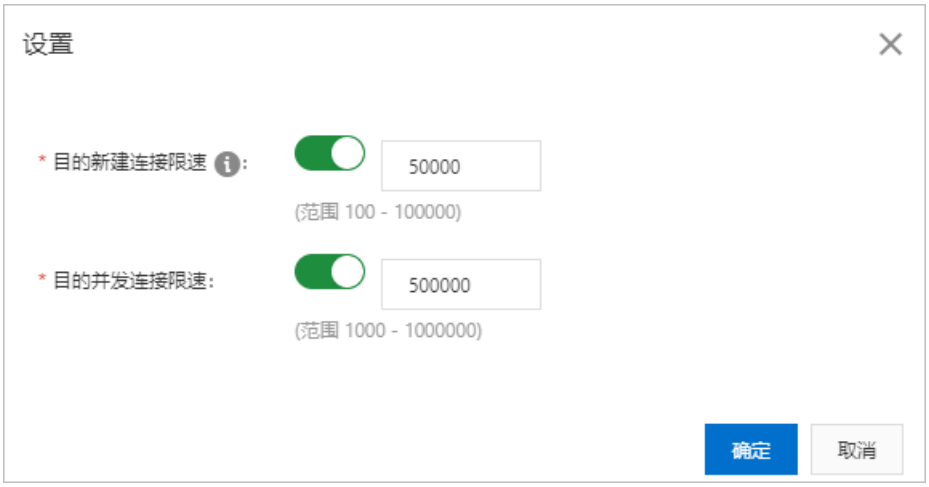
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**防护设置 > 通用防护策略**。
4. 在**通用防护策略**页面，单击**非网站业务DDoS防护**页签，并在页面上方选择要设置的DDoS高防实例。
5. 从左侧转发规则列表中单击要设置的转发规则。

6. 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。

描述	
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。	

描述	
空连接防护开关。开启后，高防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。	

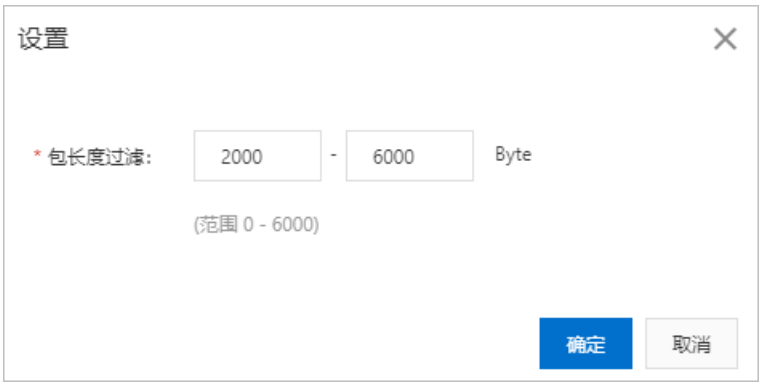
- **目的限速**：单击**目的限速**下的**设置**，在**设置**对话框完成以下配置，并单击**确定**。



描述	
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。	

描述	
限制高防IP端口的最大并发连接数量，取值范围：并000~1000000（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**，在**设置**对话框设置允许通过高防IP端口的报文所含payload的最小和最大长度，取值范围：0~6000（Byte），并单击**确定**。



- **源限速**：单击**源限速**下的**设置**，在**源限速设置**页面完成以下配置，并单击**确定**。


源限速设置
* 源新建连接限速 :
自动
手动
关闭
* 源并发连接限速:
每秒单个源并发连接达到 1 个，做限速处理
(范围 1- 50000)
源并发连接60秒内5次超限，将该源IP加入黑名单
黑名单有效时长 30 分钟
(范围 1 - 10080)
* 源PPS限速
当源PPS达到 1 Packet/s，做限速处理
(范围 1 - 100000)
源PPS连接60秒内5次超限，将该源IP加入黑名单
黑名单有效时长 30 分钟
(范围 1 - 10080)
* 源带宽限速
当源带宽达到 1024 Byte/s，做限速处理
(范围 1024 - 268435456)
源带宽连接60秒内5次超限，将该源IP加入黑名单
黑名单有效时长 30 分钟
(范围 1 - 10080)
确定
取消

参数	描述
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（Packet/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。

参数	描述
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DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **端口接入**。
4. 在**端口接入**页面，选择DDoS高防实例，并单击规则列表下方的**批量操作** > **DDoS防护策略配置**。

5. 在**批量添加DDoS防护策略**对话框，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配置转发规则的端口。
- 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）。

8.3.3 设置源限速

源限速允许您对源IP到DDoS高防实例端口的访问频率和流量大小进行限制。开启源限速后，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。本文介绍了设置源限速的具体操作。

前提条件

已在端口接入中配置非网站业务端口转发规则。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DDoS高防实例端口的访问频率进行限制，限制维度包括源新建和并发连接等，也支持对源IP到特定DDoS高防实例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源IP，DDoS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。

假设某个源IP访问DDoS高防实例的8000端口，新建连接异常高，超出正常水平十多倍。您可以为高防实例的8000端口配置源新建连接限速，且开启黑名单策略，将反复超限的源IP自动添加成黑名单，丢弃源IP的访问请求。

说明：

源限速针对DDoS高防实例的具体端口生效。如果您需要对多个不同DDoS高防实例的端口开启源限速，则需要对不同DDoS高防实例的端口分别设置。

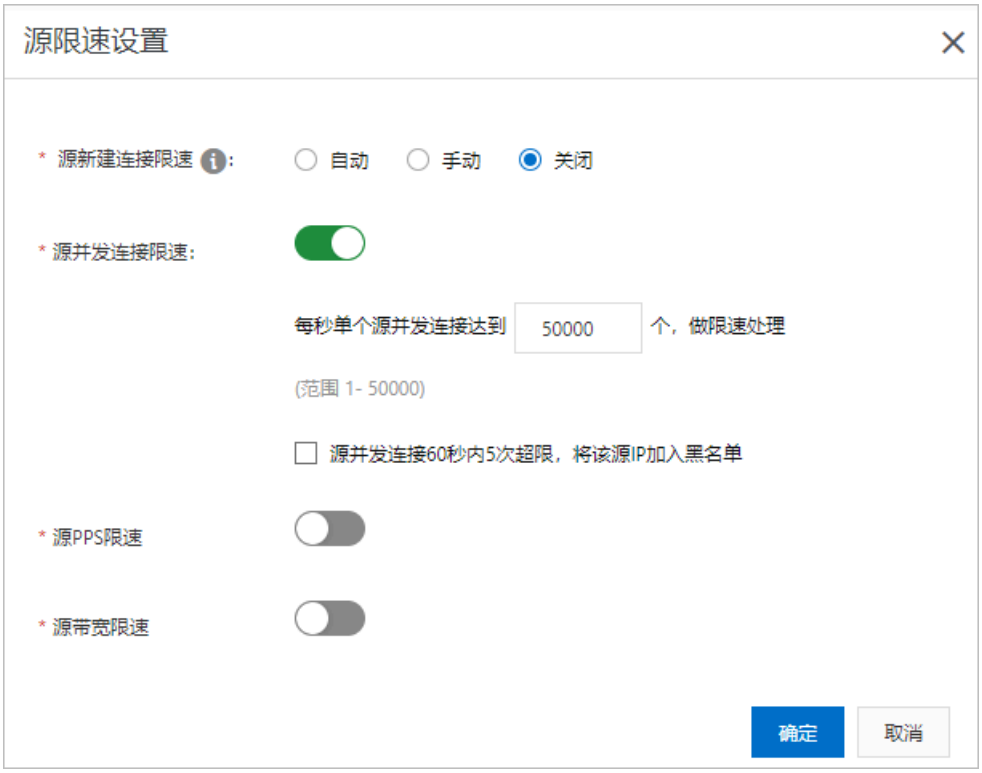
操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**接入管理** > **端口接入**。
4. 在**端口接入**页面，选择要操作的DDoS高防实例。
5. 定位到要操作的转发规则，单击其**DDoS防护策略**列下的**配置**。

6. 单击**源限速**下的**设置**。

7. 在**源限速设置**对话框，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连接不能超过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。

8. 单击**确定**，使配置生效。

8.4 设置静态页面缓存

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，请确认您的网站业务已接入增强功能套餐的DDoS高防实例。

背景信息

注意：

DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和

配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

网站业务接入DDoS高防后，您可以为网站开启静态页面缓存功能。开启静态页面缓存后，DDoS高防将从客户端对网站域名的访问请求中自动检测发现符合缓存策略的资源类型，并尝试缓存相关页面。已缓存页面将被写入网站对应的DDoS防护节点中，在下次客户端请求页面时直接返回，提升页面访问速度。

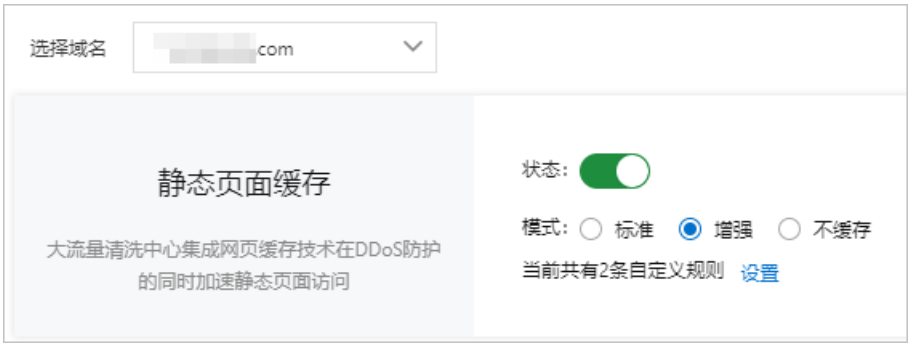
为网站开启静态页面缓存时，您可以应用不同的静态页面缓存策略，具体包括：

- **标准**模式：被请求页面包含静态文件资源（CSS、JS、TXT）时，尝试缓存相关页面。
- **增强**模式：尝试缓存所有被请求的页面。
- **不缓存**：不缓存任何被请求的页面。

静态页面缓存也支持自定义规则，方便您只为指定的页面开启缓存功能。

操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**DDoS防护实验室** > **网站加速**。
4. 选择要开启静态页面缓存的域名。
5. 定位到**静态页面缓存**区域，选择一种缓存**模式**（**标准**、**增强**、**不缓存**），并开启**状态**开关。



为域名开启静态页面缓存后，缓存策略对域名下所有URI生效。

如果您希望只对指定的URI开启缓存功能，建议您将缓存**模式**设置为**不缓存**，并参照下一步自定义静态页面缓存规则。

6. （可选）为域名下指定URI自定义静态页面缓存规则。

a) 在**静态页面缓存**区域，单击**设置**。

b) 单击**新增规则**。

c) 在**新增规则**对话框，完成以下规则设置，并单击**确定**。

参数	描述
规则名称	设置规则的名称。 支持使用英文字母、数字或下划线，且长度不允许超过128个字符。
URI	页面的URI。 **URI**中无需填写请求参数，且不支持使用通配符。 示例：填写/a/即表示<域名>/a/路径下的所有页面。
模式	选择要应用的缓存策略。可选项：**标准模式**、**强力模式**、**不缓存**。 关于不同缓存策略的含义，请参见缓存策略。

参数	描述
过期时间缓存	选择缓存的有效时间。默认为**遵循源站配置**，也可以设置为**1小时**、**1天**、**10天**、**30天**。

成功添加针对指定URI的自定义规则后，自定义规则将优先于针对域名的缓存策略生效。

8.5 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:

DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

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。

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。

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。

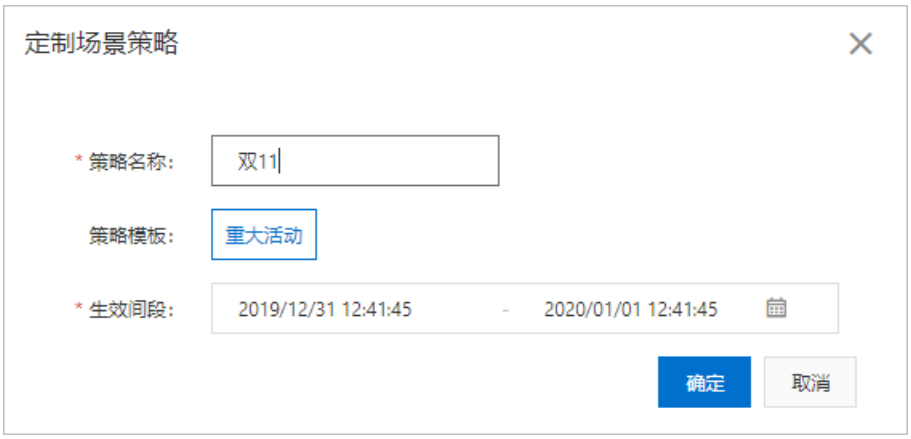
应用示例

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. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**防护设置** > **定制场景策略**。
4. 单击**新建策略**。
5. 在**定制场景策略**对话框，完成以下配置，并单击**确定**。



参数	描述
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**。

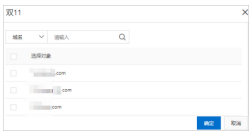
参数	描述
生效间段	选择策略的有效时间段。 **说明：** 应用同一个策略模板的策略的生效间断不允许重合。

成功添加策略后，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。

6. 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**。

7. 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**。



成功应用策略后，策略的**防护对象**信息自动更新。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。

9 调查分析

9.1 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

注意：

DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

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. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**调查分析** > **全量日志分析**。
4. 在**日志服务**页面，单击**立即购买**。

5. 在全量日志服务购买页面，选择**适用产品**（**新BGP高防**、**DDoS高防（国际）**），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。

   新BGP高防全量日志服务的单价为500元/TB（日志存储量）/月（使用时长）。

   DDoS高防（国际）全量日志服务的单价为1000元/TB（日志存储量）/月（使用时长）。

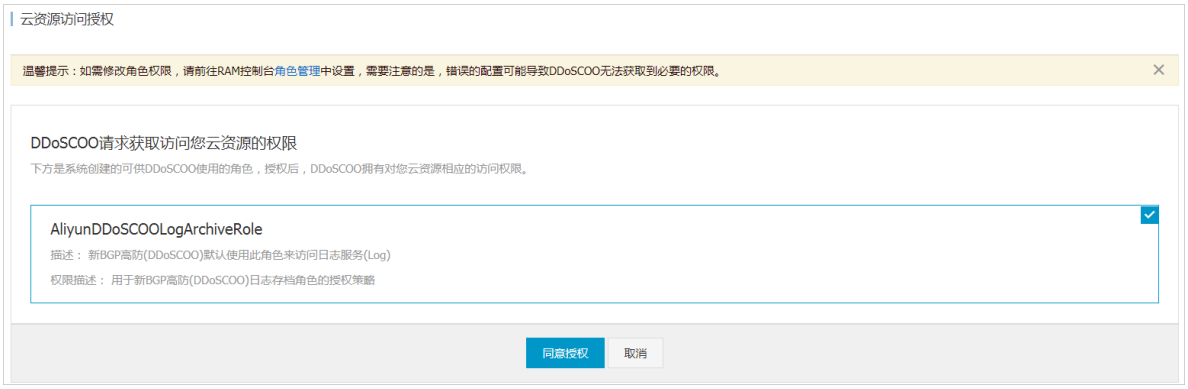
   说明：
   当全量日志服务的日志存储量足够大且在服务有效期内，将从使用全量日志服务的第一天开始，连续存储180天的日志信息。第181天的日志信息，将覆盖第一天存储的日志信息，即始终保持存储最近180天的全量日志信息。

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）。

6. 单击**立即购买**，完成支付。
7. 回到DDoS高防控制台，在**日志服务**页面，单击**立即授权**。

8. 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. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**调查分析** > **全量日志分析**。
4. 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（新BGP）服务的日志分析与日志报表功能，请参见#unique_94和#unique_95。

关于DDoS高防（国际）服务的日志分析与日志报表功能，请参见#unique_94和#unique_95。

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

功能项	说明	更多信息
仪表盘	仪表盘是日志服务提供的实时数据分析大盘。使用常用查询语句获取分析结果后，您可以将结果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：

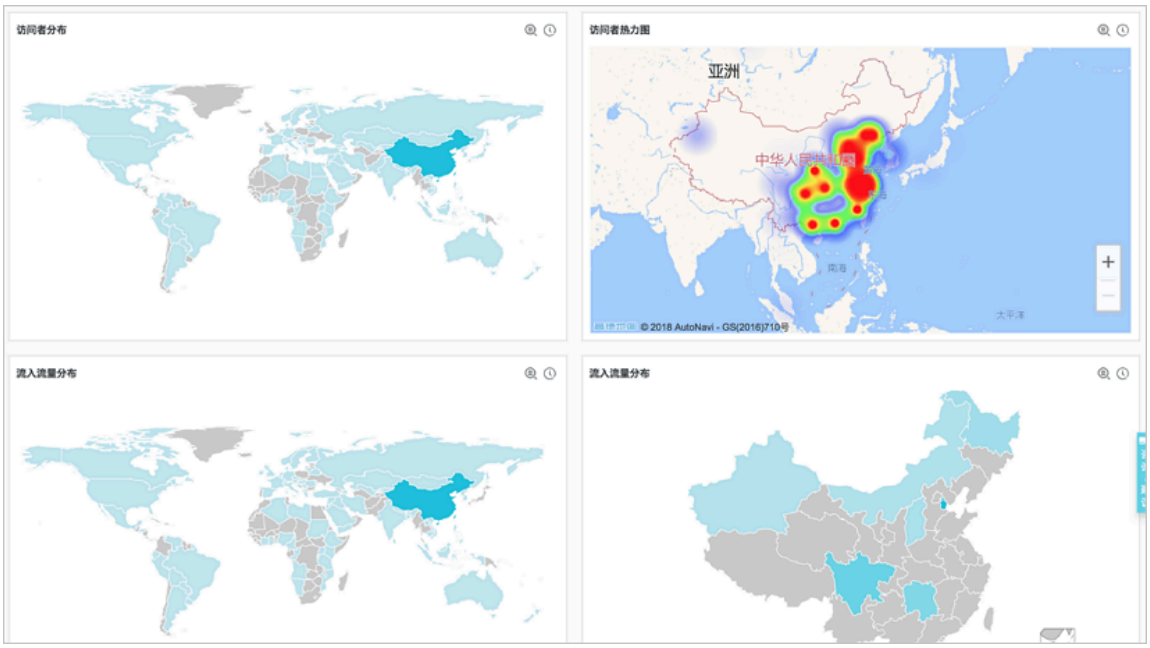
  ```
  __topic__: DDoS_access_log
  ```

- 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。

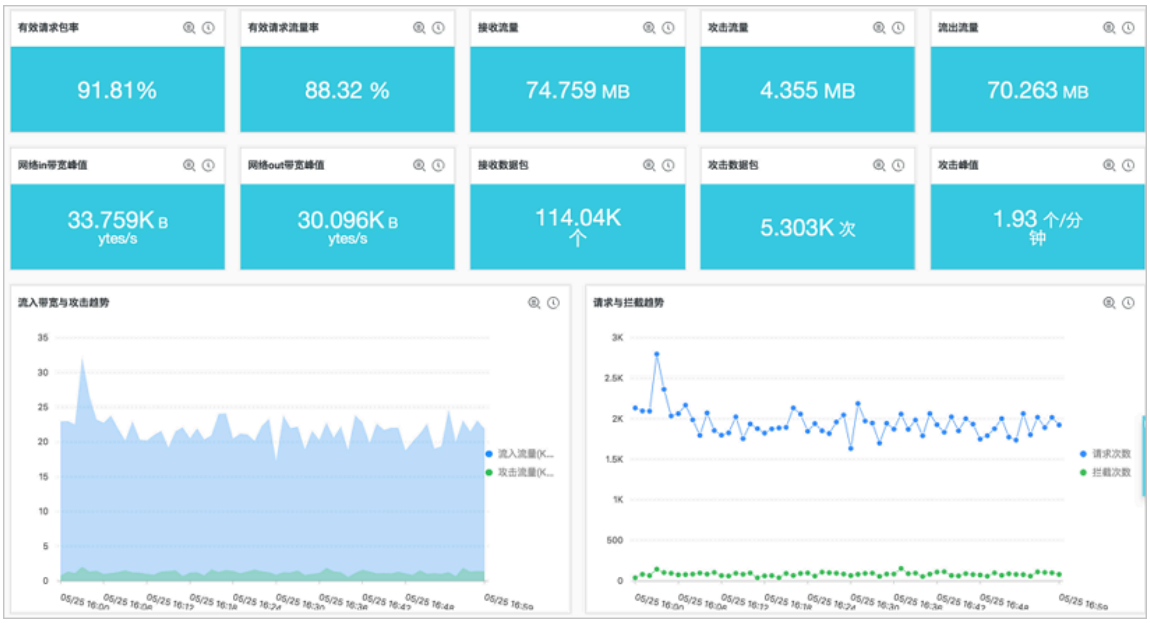
  - 例如，通过以下语句分析DDoS访问日志中记录的CC攻击者国家分布：

    ```
    __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
    ```

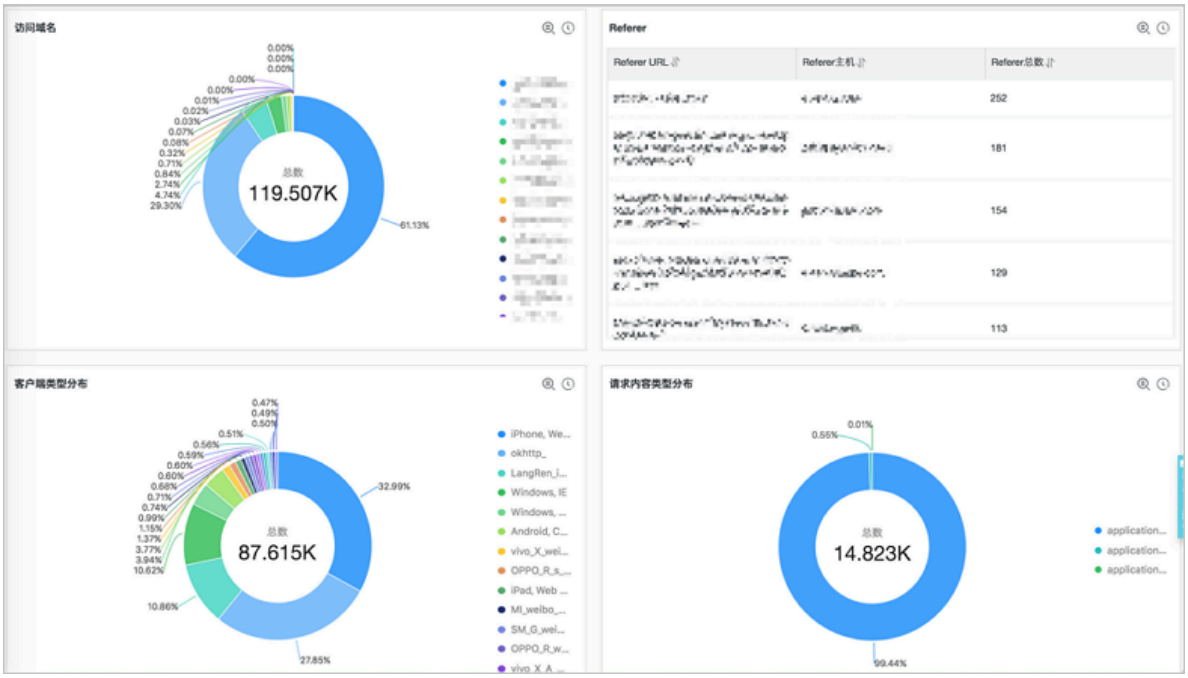
    

- 网站运营分析

  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_length)/1024.0/1024.0, 3) as mb_in group by provider having ip_to_provider(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

9.2 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
request_length	请求长度，单位为字节。	123

字段	说明	示例
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

9.3 查看操作日志

如果您使用DDoS高防（新BGP）服务，则您可以在DDoS高防控制台的操作日志页面查看近30天的重要操作日志。

前提条件

已开通DDoS高防（新BGP）实例。

说明：
目前仅DDoS高防（新BGP）服务支持操作日志。如果您使用DDoS高防（国际）服务，则暂时无法使用该功能。

背景信息

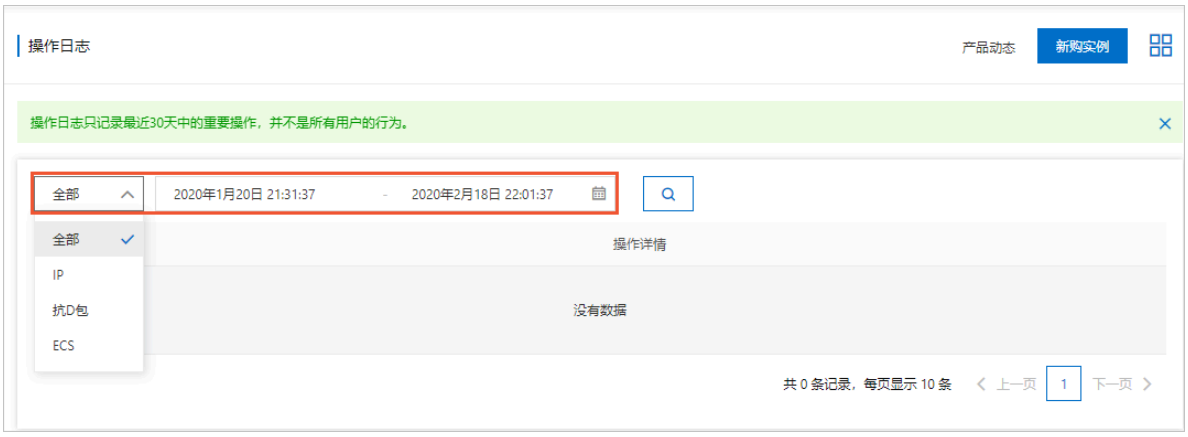
操作日志只记录最近30天中的重要操作，并非记录所有用户行为。

DDoS高防（新BGP）支持查看的操作日志类型如下：

- ECS更换IP日志
- 黑洞解封操作日志
- 流量封禁和解封操作日志
- 四层流量清洗模式变更操作日志
- CC防护模式变更操作日志
- 弹性防护带宽变更操作日志

操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**中国内地**地域。
3. 在左侧导航栏，单击**调查分析** > **操作日志**。
4. 在**操作日志**页面，设置要查看的操作日志类型（**IP**、**抗D包**、**ECS**）和时间范围，查看对应数据。



9.4 查看高级防护日志

如果您使用DDoS高防（国际）服务，则您可以在DDoS高防控制台的高级防护日志页面查看近30天的全局高级防护记录。

前提条件

已开通DDoS高防（国际）实例。

操作步骤

1. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**非中国内地**地域。
3. 在左侧导航栏，单击**调查分析** > **高级防护日志**。
4. 在**高级防护日志**页面，选择要查询的实例和时间范围，查看对应数据。

10 监控与告警

10.1 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。

表 10-1: DDoS高防监控指标

监控项	监控维度	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 **说明:** 通过高防清洗后回源到源站服务器的干净业务流量。	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

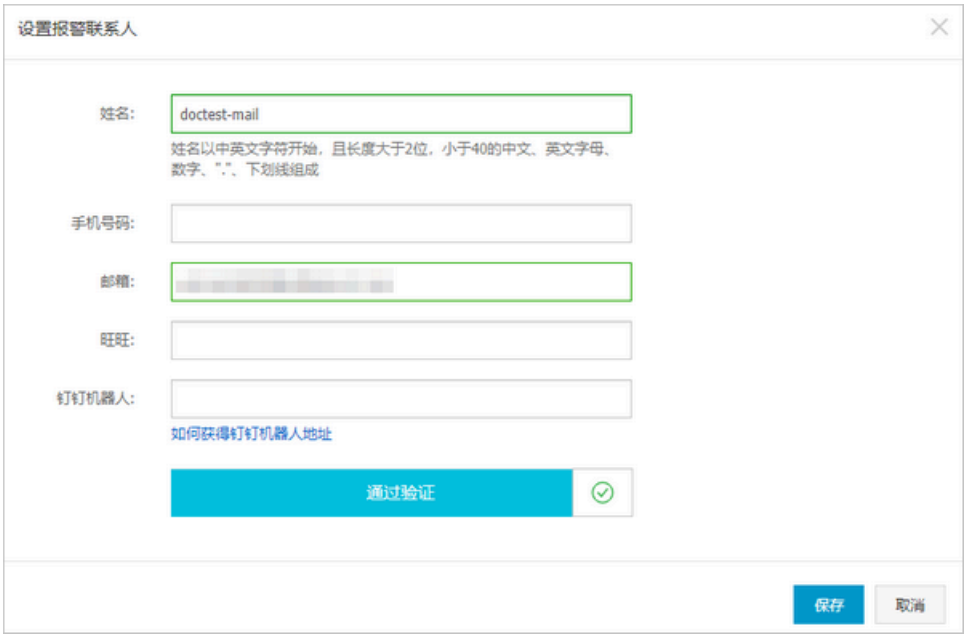
1. 登录阿里云云监控控制台。

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，填写联系人信息并完成滑块验证，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**。

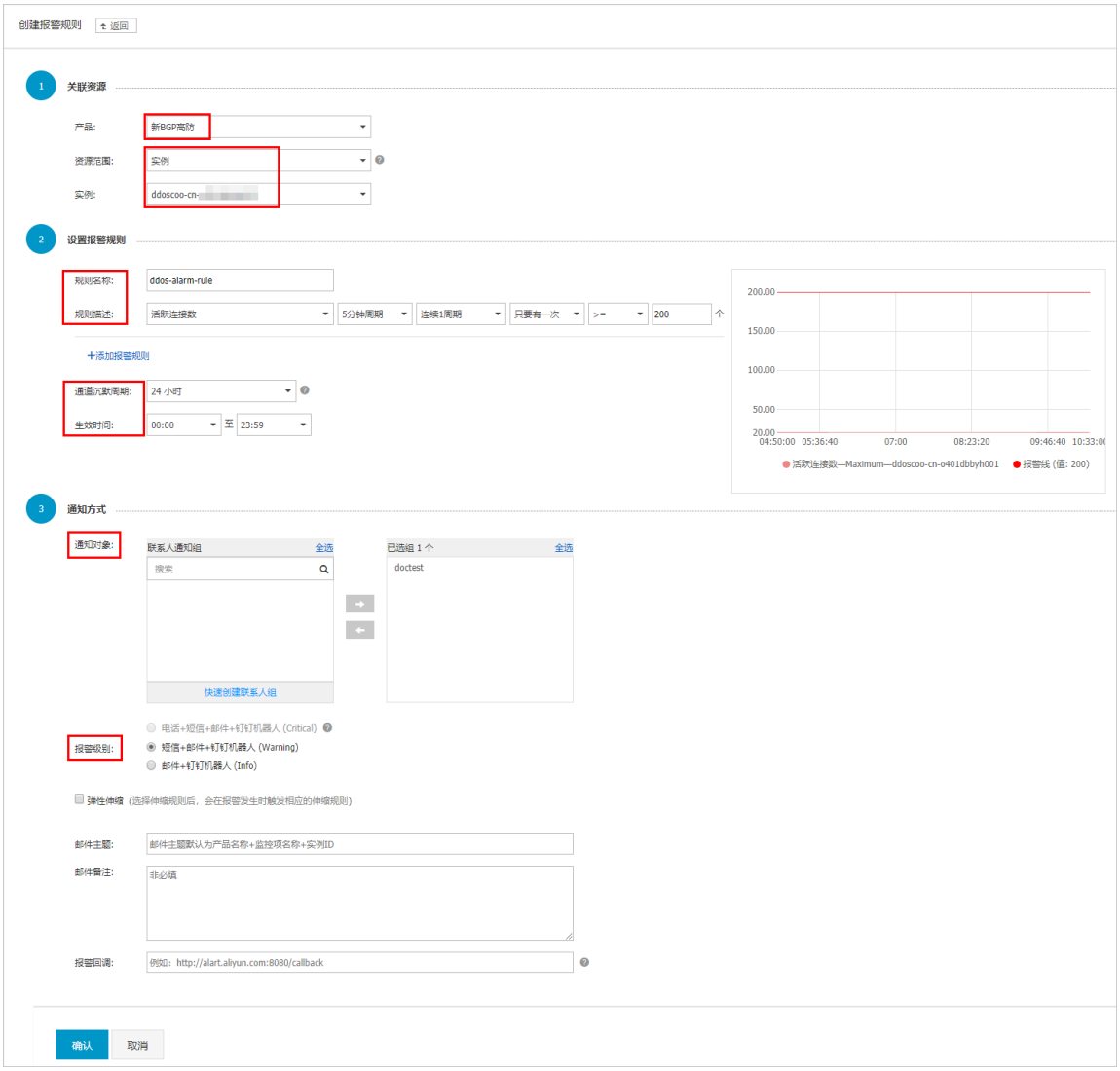
成功新建报警联系组。

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	报警规则的内容，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： • 规则描述设置为新建连接数 | 5分钟周期 | 连续3周期 | 只要有一次 | > | 200个， 表示报警服务会探测任意连续3个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个周期有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。 • 规则描述设置为 高防IP出流量 | 5分钟周期 | 连续3周期 | 只要有一次 | ≥ | 50 Mbit/s，表示报警服务会探测任意连续3个周期的高防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个周期有15个数据点），只要有一次大于等于50 Mbit/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**。 
	通道沉默周期	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。

类别	配置项	说明
通知方式	**通知对象**	接收报警通知的联系人组。
	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。
	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高防报警规则后，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。

10.2 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

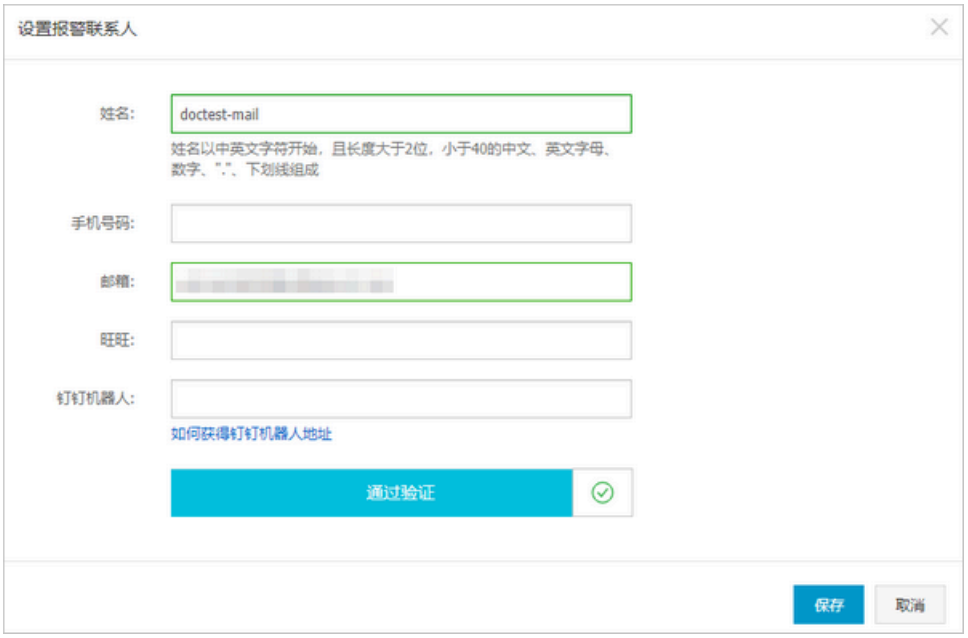
1. 登录阿里云云监控控制台。

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，填写联系人信息并完成滑块验证，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。

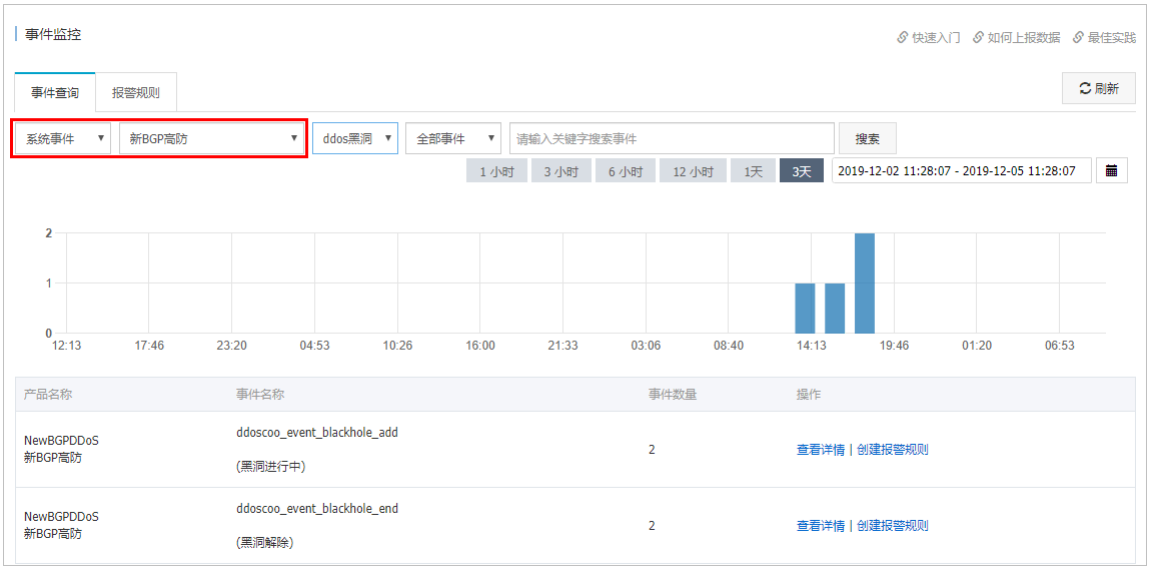
类型	配置项	说明
	日志服务	无需勾选。

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。

10.3 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。

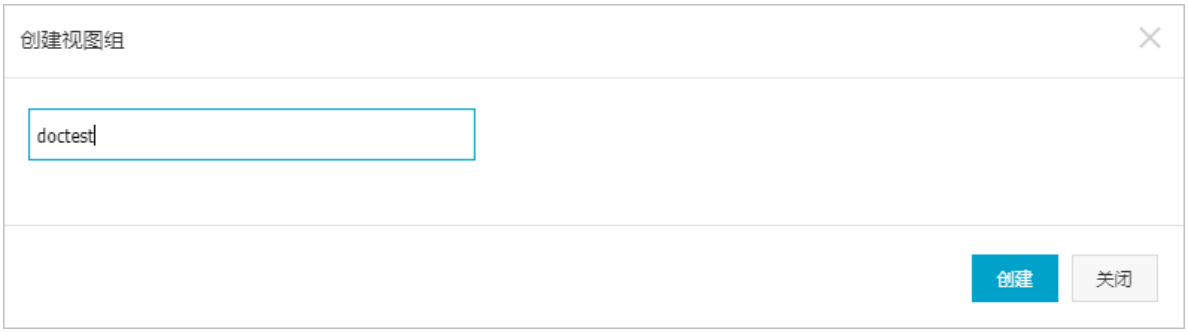
表 10-2: DDoS高防监控指标

监控项	监控维度	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 **说明:** 通过高防清洗后回源到源站服务器的干净业务流量。	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**。

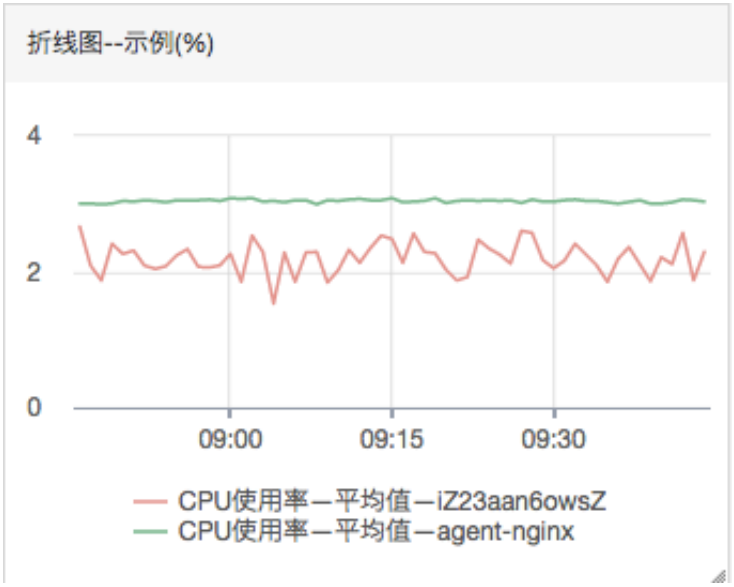


成功添加监控大盘，页面跳转到新建的监控大盘。您可以通过**当前监控大盘**选项切换要查看或操作的监控大盘。

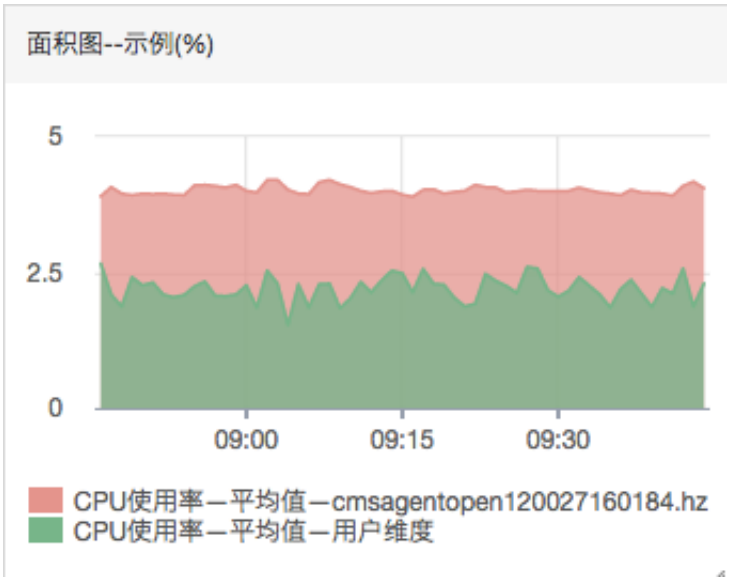
4. 进入监控大盘，单击**添加图表**，并在**添加图表**侧边页中自定义图表内容。

   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。

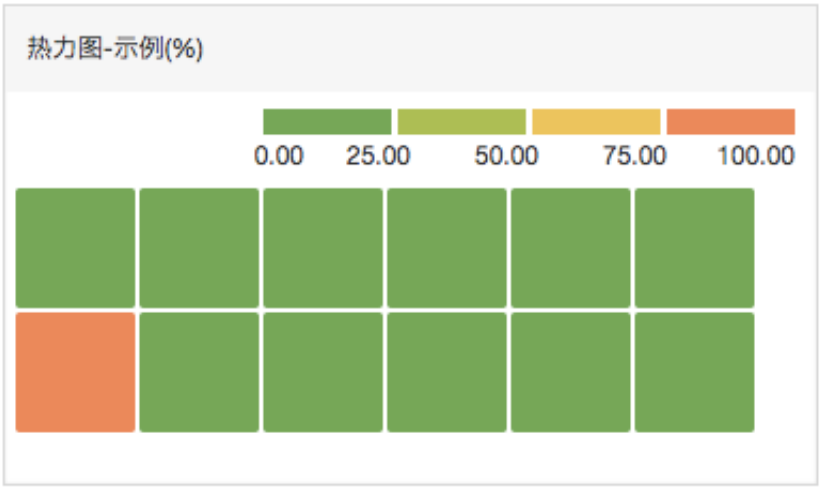


   - **TopN表格**：显示最近三小时内最后时刻监控数据的排序，最多显示正序的1000条或倒序的1000条数据。例如ECS分组中所有机器CPU使用率从大到小的排序。只能添加一个监控项。

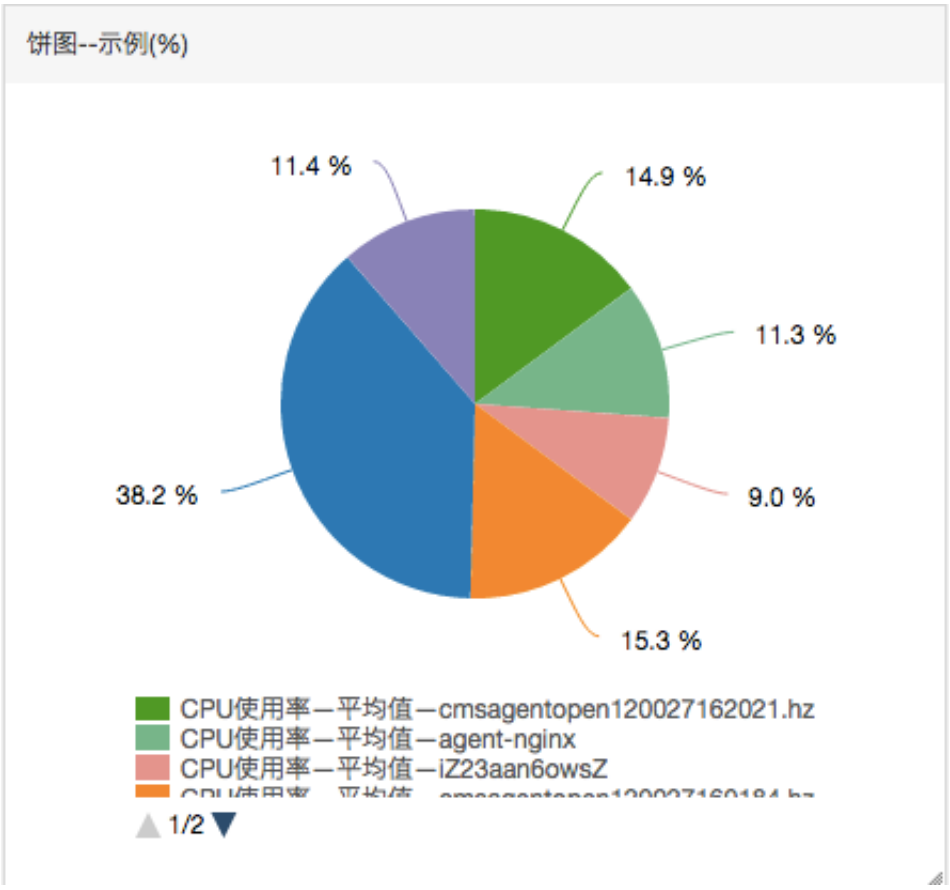
表格--示例(%)

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。

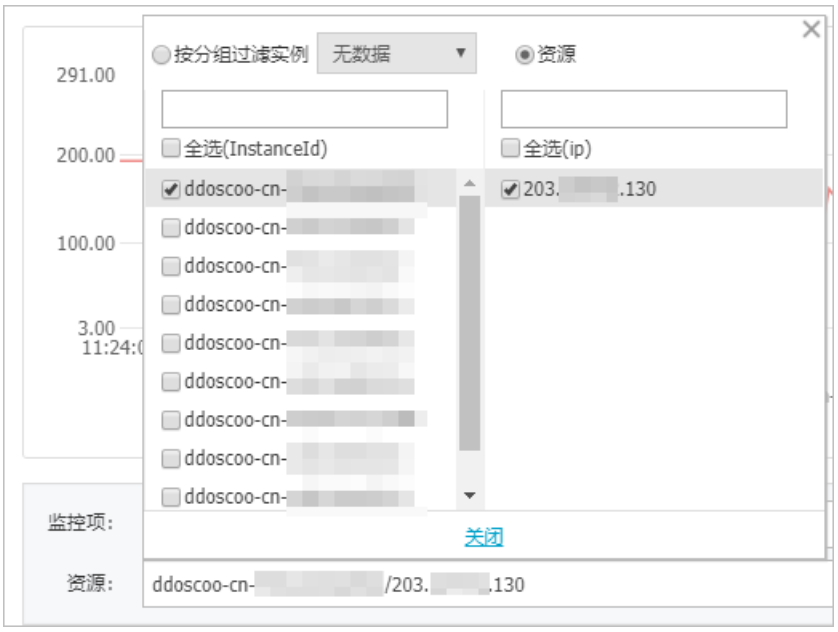


- **饼图**：显示监控项的实时数据，常用于数据的对比。只能添加一个监控项。



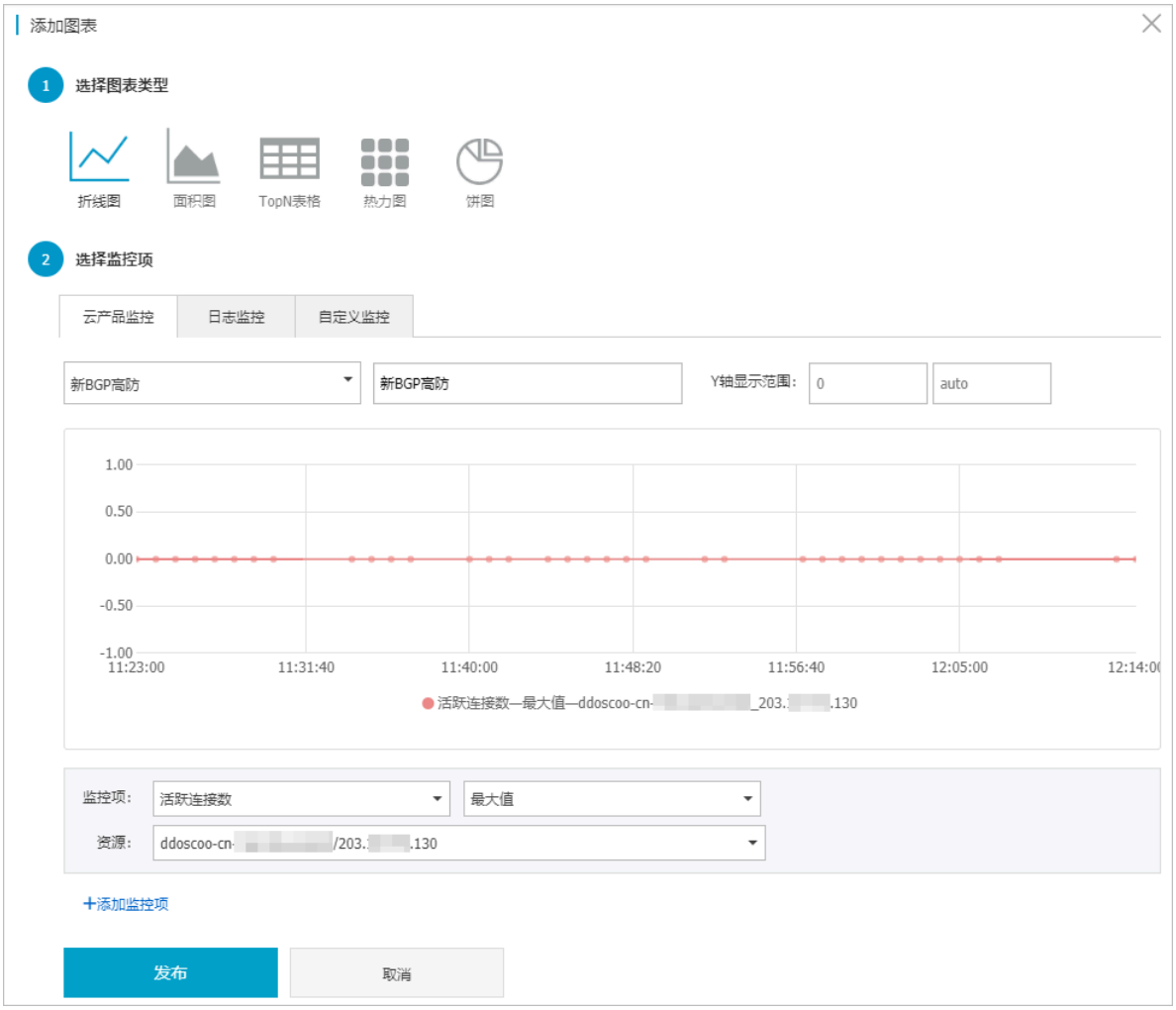
b) **选择监控项**。选择**云产品监控**，并设置产品为**新BGP高防**，进一步配置**监控项**和**资源**。

- 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。

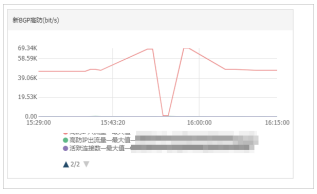


单击**添加监控项**可以在当前图表中定义多个监控项。

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_109、#unique_110。

11 资产管理

11.1 管理实例标签

DDoS高防实例支持通过自定义标签进行分类和检索。您可以自定义标签并标记具有相同用途、属性的DDoS高防实例，实现实例分类和批量检索。本文介绍了为DDoS高防实例创建并绑定标签、移除标签，以及通过标签搜索实例的操作方法。

背景信息

> **注意:**
> DDoS高防控制台在顶部导航栏新增地域切换菜单，方便您切换选择DDoS高防（新BGP）、DDoS高防（国际）服务。地域切换菜单支持**中国内地**和**非中国内地**选项，您可以通过切换地域分别管理和配置DDoS高防（新BGP）和DDoS高防（国际）实例。在使用DDoS高防服务时，请确认您已选择正确的地域。

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. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**资产管理** > **实例管理**。

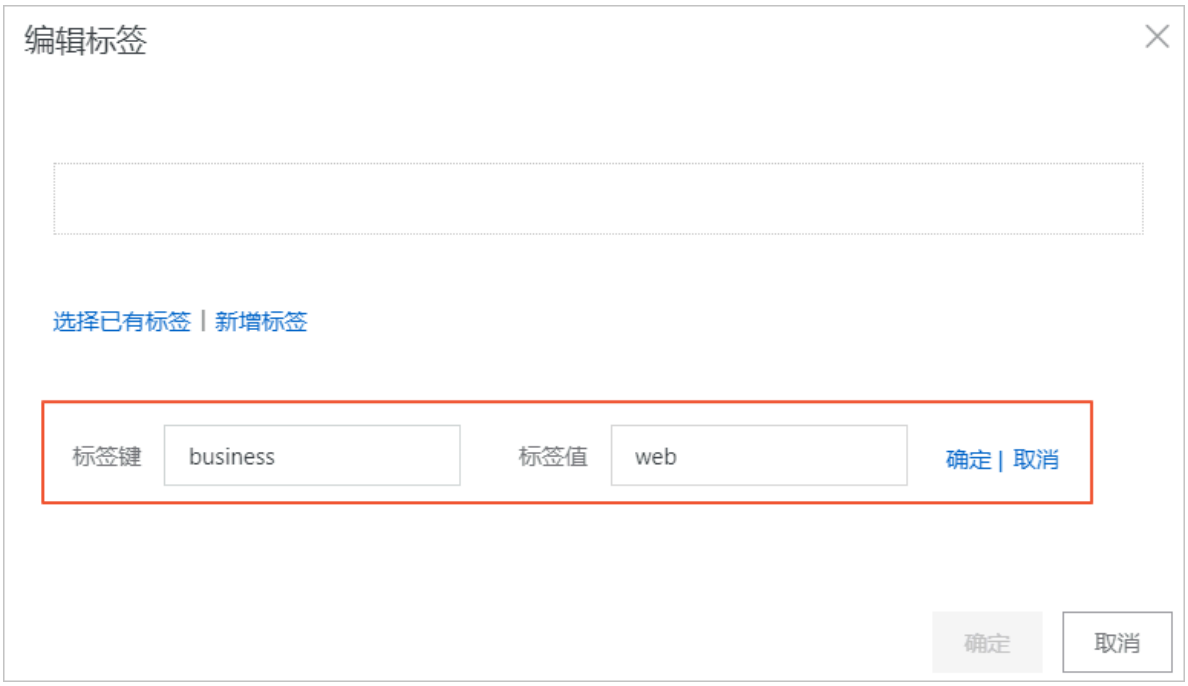
4. 在**实例列表**页面，定位到要操作的实例，单击**实例信息**列中的标签编辑图标。

5. 在**编辑标签**对话框，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。

6. 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。

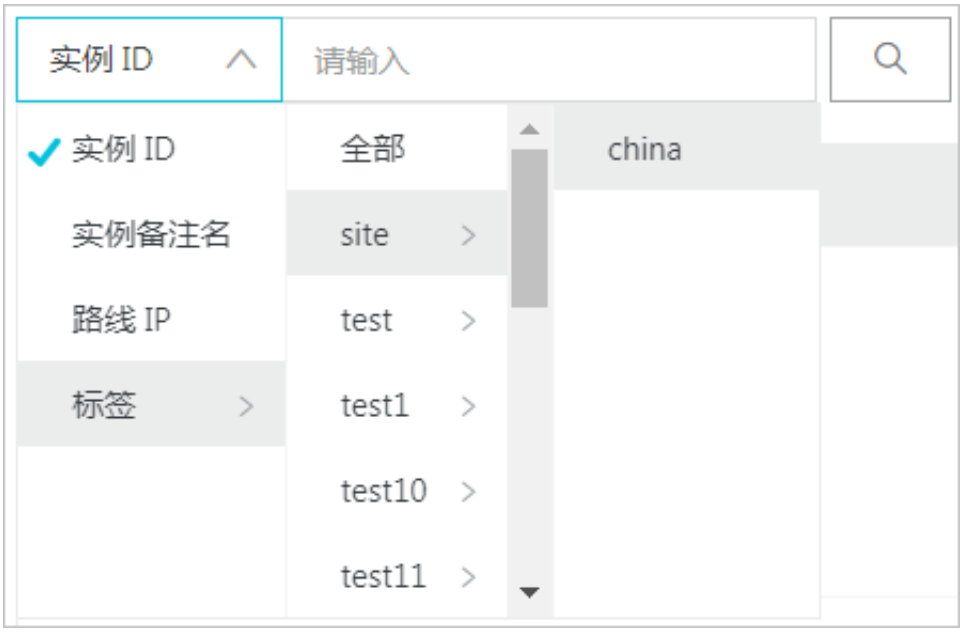


7. 单击**确定**，即为目标实例添加新增的标签。您可以在**编辑标签**对话框中为目标添加多个标签。

通过标签搜索实例

1. 登录DDoS高防控制台。

2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**资产管理** > **实例管理**。
4. 在**实例列表**页面，从搜索项列表中选择**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. 登录DDoS高防控制台。
2. 在顶部导航栏，选择服务所在地域：
   - **中国内地**：DDoS高防（新BGP）服务
   - **非中国内地**：DDoS高防（国际）服务
3. 在左侧导航栏，单击**资产管理** > **实例管理**。
4. 在**实例列表**页面，定位到要操作的实例，单击**实例信息**列中的标签编辑图标。
5. 在**编辑标签**对话框，单击要移除的标签的删除图标，并单击**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。

11.2 DDoS高防抗D包

DDoS高防抗D包是面向DDoS高防（新BGP）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。

说明：
仅DDoS高防（新BGP）支持抗D包。如果您使用DDoS高防（国际），则无法使用抗D包。

抗D包的主要规格参数是：防护规格和可用防护次数。以300 Gbit/s防护规格，可用防护3次的抗D包为例，其中，

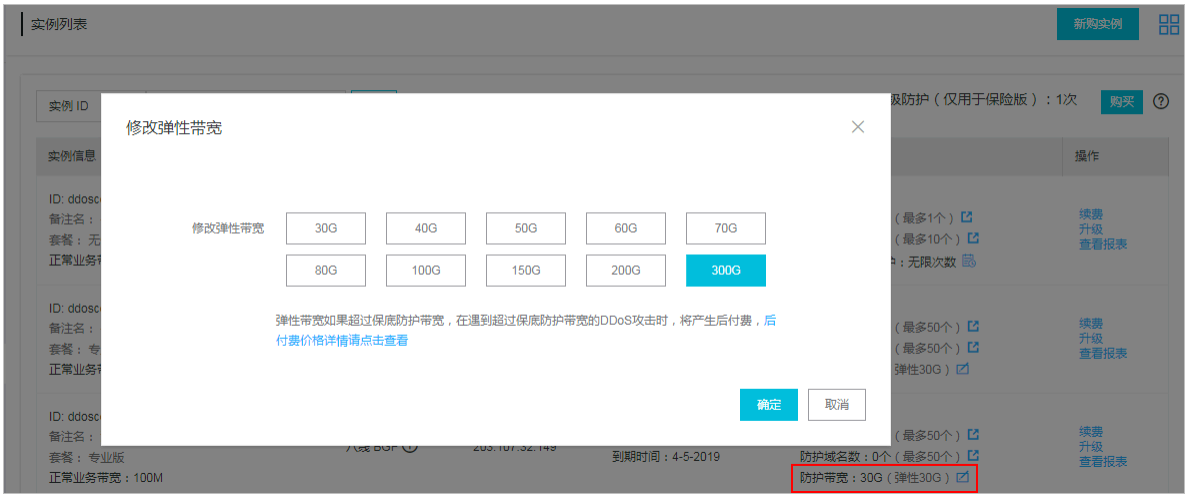
- 防护规格300 Gbit/s：表示该抗D包最大可抵扣保底防护带宽+300 Gbit/s 的攻击峰值所产生的后付费。假如攻击峰值大于保底防护带宽+300 Gbit/s，那么300 Gbit/s 抗D包将抵扣失败；抵扣失败时，如果符合DDoS高防后付费产生条件，将会正常产生相应的后付费。
- 可用防护3次：表示该抗D包共可使用3次。无论每日遭受多少次攻击，最多只消耗一次抗D包防护次数。

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“保底防护带宽+抗D包规格”。

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



- 只有当攻击峰值-保底防护带宽=<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，使其等于保底防护带宽。
- 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 11-1: 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：

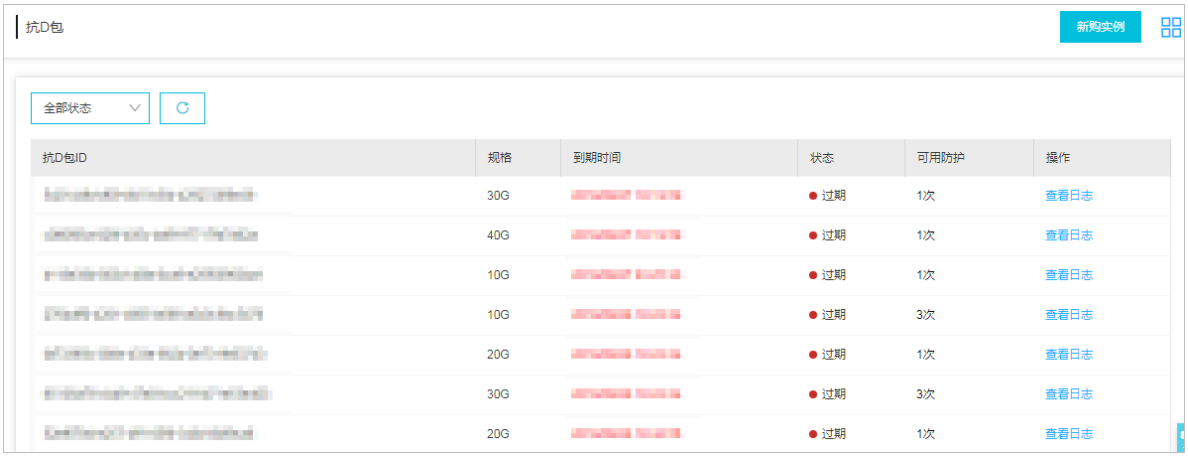
- 首次开通DDoS高防
- 首次连续使用DDoS高防 3个月以上

- 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. 登录DDoS高防控制台。
2. 在顶部导航栏，选择**中国内地**地域。
3. 在左侧导航栏，单击**资产管理** > **抗D包**。
4. 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、耗尽和无效。
   - **可用防护**：抗D包的可用防护次数。



5. 单击一个抗D包下的**查看日志**可以查询其操作记录。

12 安全服务

12.1 概述

安全服务帮助您处理DDoS高防使用过程中遇到的问题，协助您完成网站接入、防护配置、安全分析等任务。

根据服务形式和计费方式的不同，DDoS高防提供以下安全服务：

- 安全专家指导服务：加入阿里云企业安全服务钉钉群，免费享受安全专家通过钉钉为您提供的一对一指导服务。

  您必须使用钉钉沟通工具，才可以使用该服务。关于钉钉，请参见阿里云钉钉官网首页。
- 高防产品托管服务：通过预付费方式开通高防产品托管服务，可以享受阿里云原厂安全服务团队提供的全面的DDoS高防技术支持，例如接入设置、防护策略优化、监控与告警设置、安全报表定制等。

  该服务适用于需要外包专业人员协助进行安全产品服务运营的用户，采用专属钉钉群、电话会议等方式进行交付。

  使用该服务时，您需要开通服务授权，允许阿里云安全服务专家查看您的业务场景数据，以便提供有针对性的防护咨询和日志数据深度分析建议。更多信息，请参见开通高防安全服务授权。

12.2 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. 在左侧导航栏，将鼠标悬置在**有问题？找专家！**图标上，并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。

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。

12.3 高防产品托管服务

云盾DDoS高防支持产品托管服务。开通高防产品托管后，您可以在阿里云安全产品专家的帮助下完成高防接入配置、安全监控和巡检、防护策略优化，并享有安全事件响应、安全咨询、安全培训和案例分享、安全报告等服务。

概述

高防产品托管由阿里云原厂安全服务团队提供技术支持，面向云盾DDoS防护用户提供产品托管服务。高防产品托管帮助您更有效地使用高防产品保护Web资产，降低业务安全风险，减少运维人力投入。

高防产品托管适用于已开通阿里云DDoS高防产品，但缺乏业务持续监控能力和缺少可应对安全漏洞风险的安全工程师的业务场景。该服务适合需要外包专业人员协助来进行安全产品服务运营的用户。

说明:

由于托管服务的部分工作内容（包括但不局限于防护策略优化、监控和预警设置、安全报告定制等）需要使用DDoS高防日志服务，如果您未购买DDoS高防日志服务，上述托管服务可能存在无法交付的风险。建议您在选购高防产品托管服务的同时，购买DDoS高防日志服务功能。更多信息，请参见开通全量日志服务。

服务内容

高防产品托管为您提供完整的高防产品接入和使用支持，下表描述了具体的服务内容。

服务类型	描述
接入配置	• 在高防上配置保护对象的域名策略。 • 协助用户配置和上传HTTPS证书（用户可自行上传）。 • 按照客户要求配置合理的防护阈值。 • 协助用户配置ECS和SLB的源站保护策略。 • 产品适配和访问测试验证。 • 用户保护域名变化时，调整相关配置。
防护策略优化	• 在高防上的业务出现异常时，提供诊断和排错服务。 • 基于攻防日志，优化用户安全防护策略和配置。 • 安全事件响应时，调整防护策略和提供方案，帮助用户缓解事件影响。 • 提供故障处理、CC防护规则、精准访问控制规则、数据风控等高防防护配置建议。

服务类型	描述
监控和预警	• 系统自动化监控高防集群可用性故障。 • 系统自动化监控DDoS攻击导致的高危时事件。 • 人工在线判断和过滤监控事件预警。
安全报告	• 根据用户要求提供定制化安全报告内容。 • 提供服务日报和服务月报，其中日报包括当天操作信息，月报包括操作数据和攻防数据分析。

安全事件响应时间

开通高防产品托管后，当您遇到安全事件需要紧急协助时，服务团队响应您的时间遵循下表描述。

表 12-1: 安全事件响应时间

序号	优先级	定义	响应时间
1	危险	用户核心业务严重受损或完全不可用	15分钟
2	紧急	用户核心业务出现非全局异常	30分钟
3	高	用户非核心业务严重受损或不可用	2小时
4	中	用户非核心业务出现非全局异常	4小时
5	低	用户日常技术咨询	8小时

服务交付方式

下表描述了高防产品托管的服务交付方式。

表 12-2: 服务交付方式

类别	描述
服务交付方式	远程在线服务
服务语言	中文和英语
服务周期	与用户购买周期一致
支持的服务渠道	• 电子邮件 • 钉钉 • 电话

定价和售卖方式

高防产品托管服务支持通过预付费方式开通，并且可按月或者按年续费。 购买高防产品托管服务，立即前往高防产品托管服务售卖页。

注意：
由于服务支持系统和服务人力资源投入的特殊性，高防产品托管服务在支付购买后暂不支持退款。

12.4 服务授权

12.4.1 开通高防安全服务授权

通过高防安全专家服务，您将获得阿里云安全服务专家和第三方安全专家针对您业务场景的提供的高防产品安全服务，帮助您基于业务实际情况更好地使用高防产品功能，保障业务的网络应用安全。

背景信息

安全专家可以为您提供高防中的域名防护咨询服务，也会对您的业务日志数据进行深度分析，有针对性地为您提供高防防护配置的相关建议等。

购买高防产品安全服务后，您需要开通服务授权，允许阿里云安全服务专家和第三方安全专家通过阿里云安全服务平台为您提供产品服务。

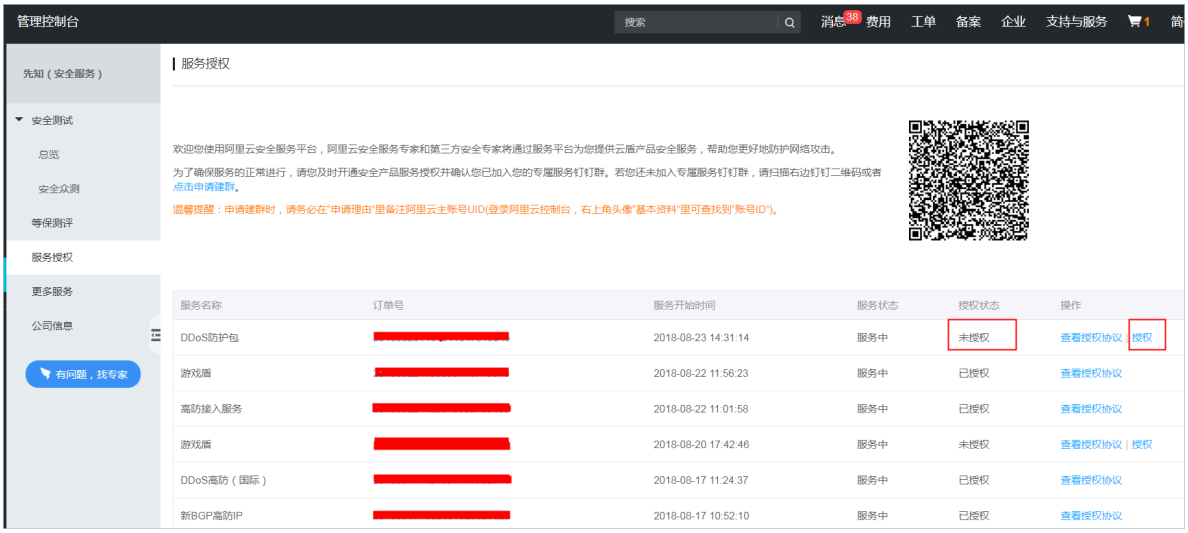
说明：
您必须已购买或开通云盾高防产品，才能享受高防安全专家服务。

操作步骤

1. 登录云盾先知（安全服务）管理控制台。
2. 定位到**服务授权**页面，您可以查看到您的高防产品安全服务订单的授权情况。

说明：

一般情况下，新创建的安全服务订单状态为未授权。



3. 单击查看授权协议，确认并同意授权书内容后，单击**确定**。

4. 单击**授权**。
5. 在服务订单所对应的云资源RAM角色授权页面，单击**同意授权**。

说明：

为了确保与安全专家的交流，确认您已申请并开通与安全专家的专属钉钉服务群。

预期结果

授权完成后，在云盾先知（安全服务）管理控制台的**服务授权**页面，该服务订单的状态显示为**已授权**，您可以随时单击**查看授权协议**查看授权书。

完成授权后，您的专属安全专家可以通过阿里云安全服务平台直接查看您的高防中相应的业务数据及配置数据，为您的业务提供专属的安全策略和建议。安全专家通过阿里云安全服务平台查看您高防控制台进行的所有操作都将产生相应的操作日志，您可以随时登录阿里云控制台查看安全专家操作记录。

12.4.2 查看安全专家操作日志

获得授权的安全专家可以通过阿里云安全服务平台访问并查看您高防控制台。安全专家在您的控制台上的所有操作都将产生操作日志。您可以随时登录阿里云操作审计管理控制台查看并审计这些操作行为。

操作步骤

1. 登录操作审计管理控制台，选择**华东1（杭州）**。

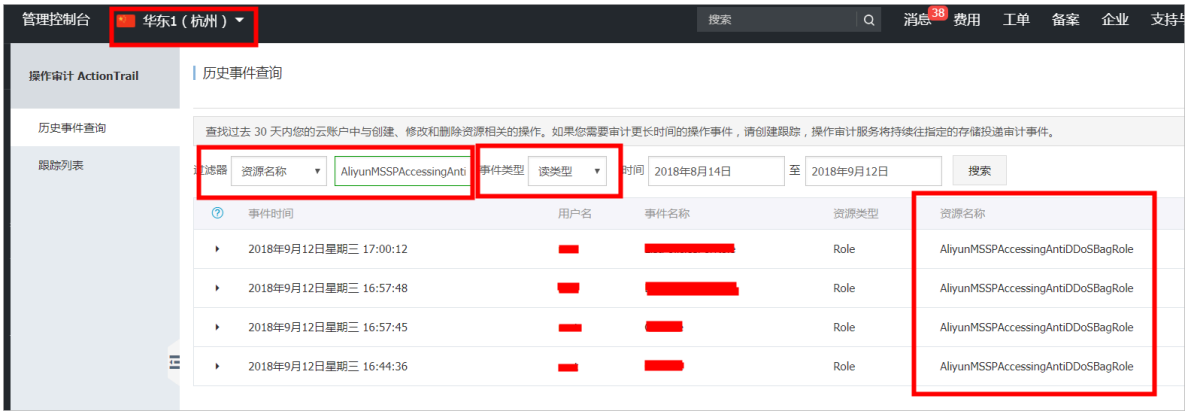
2. 定位到**历史事件查询**页面，设置以下查询条件，单击**搜索**，查询您的专属安全专家在高防控制台中的操作记录日志。

   - **资源名称**：包含AliyunMSSPAccessingAntiDDoSBagRole
   - **事件类型**：所有类型

   > **说明：**
   > 目前高防安全服务仅授权安全专家查看您高防控制台中的数据，不具备更改配置等权限。因此，您也可以将事件类型条件设置为读类型，查询到的事件记录与选择所有事件类型得到的查询结果一致。

   - **时间**：选择您想查询的时间范围。

   > **说明：**
   > 历史事件查询支持查看最近30天内的操作记录。



3. 在事件列表中，单击**操作记录**可展开查看事件详情。

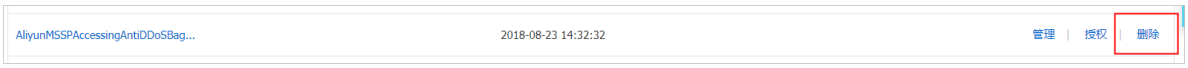
4. 单击**查看事件**可查看该事件的详细参数。

12.4.3 取消高防安全服务授权

高防安全服务授权开通后，您可以随时在访问控制（RAM）管理控制台中删除高防安全服务的授权角色，取消高防安全服务授权。

操作步骤

1. 登录访问控制（RAM）管理控制台。
2. 定位到**角色管理**页面，通过搜索**角色名**（包含“MSSP”）找到授权服务订单时生成的MSSP安全产品服务的授权角色。
   - 高防IP对应角色名称为：**AliyunMSSPAccessingYundunHighRole**
   - 高防（国际）对应角色名称为：**AliyunMSSPAccessingDDoSDIPRole**
   - 新BGP高防对应角色名称为：**AliyunMSSPAccessingDDoSCOORole**
   - 游戏盾对应角色名称为：**AliyunMSSPAccessingGameShieldRole**
   - DDoS防护包对应角色名称为：**AliyunMSSPAccessingAntiDDoSBagRole**
3. 单击相应角色后的**删除**。



4. 在**删除角色**对话框中勾选**强制解除关联关系**，并单击**确定**。

5. 获取并输入手机验证码，单击**确定**，通过手机验证。

预期结果

授权角色删除成功后，在云盾先知（安全服务）管理控制台的**服务授权**页面中相应服务订单的状态将变更为**未授权**。


服务授权
欢迎您使用阿里云安全服务平台，阿里云安全服务专家和第三方安全专家将通过服务平台为您提供云盾产品安全服务，帮助您更好地防护网络攻击。
为了确保服务的正常进行，请您及时开通安全产品服务授权并确认您已加入您的专属服务钉钉群。若您还未加入专属服务钉钉群，请扫描右边钉钉二维码或者点击申请建群。
温馨提醒：申请建群时，请务必在"申请理由"里备注阿里云主账号UID(登录阿里云控制台，右上角头像"基本资料"里可查找到"账号ID")。
服务名称
订单号
服务开始时间
服务状态
授权状态
操作
高防接入服务
服务中
未授权
查看授权协议
共有31条，每页显示：10条
« ‹ 2 3 4 › »

13 API参考

13.1 API概览

本文档汇总了DDoS高防服务所有可调用的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
DescribeInstanceIds	查询DDoS高防实例的ID信息。
DescribeInstances	查询DDoS高防实例的版本和状态信息，例如业务转发状态、到期状态、欠费状态等。
DescribeInstanceDetails	查询DDoS高防实例的IP和线路信息。
DescribeInstanceSpecs	查询DDoS高防实例的规格信息。
DescribeInstanceStatistics	查询DDoS高防实例的统计信息，例如已防护的域名、端口数量等。
ModifyInstanceRemark	编辑DDoS高防实例的备注。
DescribeElasticBandwidthSpec	查询DDoS高防（新BGP）实例的可选弹性防护带宽规格。
ModifyElasticBandWidth	修改DDoS高防（新BGP）实例的弹性防护带宽。
DescribeDefenseCountStatistics	查询DDoS高防（国际）服务的防护次数统计信息，例如可用和已用的高级防护次数。
ReleaseInstance	释放某个已经到期的DDoS高防实例。

接入管理

表 13-1: 域名接入

API	描述
DescribeDomains	查询已配置网站业务转发规则的域名。
DescribeWebRules	查询网站业务转发规则。
CreateWebRule	创建网站业务转发规则。
ModifyWebRule	编辑网站业务转发规则。

API	描述
DeleteWebRule	删除网站业务转发规则。
DescribeWebInstanceRelations	查询网站业务关联的DDoS高防实例信息。
AssociateWebCert	为网站业务转发规则关联SSL证书。
ModifyTlsConfig	编辑网站业务转发规则的TLS安全策略。
DescribeWebCustomPorts	查询DDoS高防支持的网站业务自定义端口范围。
DescribeWebAccessMode	查询网站业务的接入模式。
ModifyWebAccessMode	设置网站业务的接入模式。
DescribeCerts	查询网站业务的证书信息。
DescribeCnameReuses	查询网站业务的CNAME复用信息。
ModifyCnameReuse	为网站业务开启或关闭CNAME复用。
ModifyHttp2Enable	设置网站业务转发规则的HTTP2.0开关状态。

表 13-2: 端口接入

API	描述
DescribeNetworkRules	查询端口转发规则。
CreateNetworkRules	创建端口转发规则。
ConfigNetworkRules	编辑端口转发规则，修改源站IP地址。
DeleteNetworkRule	删除端口转发规则。
DescribeHealthCheckList	查询端口转发规则的健康检查配置（四层或七层）。
ModifyHealthCheckConfig	编辑端口转发规则的健康检查配置（四层或七层）。
DescribeHealthCheckStatus	查询源站健康检查状态信息。

表 13-3: 流量调度器

API	描述
DescribeSchedulerRules	查询流量调度器的调度规则。
CreateSchedulerRule	创建流量调度器调度规则。
ModifySchedulerRule	编辑流量调度器调度规则。
DeleteSchedulerRule	删除流量调度器调度规则。

防护设置

表 13-4: 基础设施防护策略

API	描述
DescribeAutoCcListCount	查询针对DDoS高防实例的黑名单和白名单IP的数量。
DescribeAutoCcBlacklist	查询针对DDoS高防实例的黑名单IP。
AddAutoCcBlacklist	添加针对DDoS高防实例的黑名单IP。
DeleteAutoCcBlacklist	删除针对DDoS高防实例的黑名单IP。
EmptyAutoCcBlacklist	清空针对DDoS高防实例的黑名单IP。
DescribeAutoCcWhitelist	查询针对DDoS高防实例的白名单IP。
AddAutoCcWhitelist	添加针对DDoS高防实例的白名单IP。
DeleteAutoCcWhitelist	删除针对DDoS高防实例的白名单IP。
EmptyAutoCcWhitelist	清空针对DDoS高防实例的白名单IP。
DescribeUnBlackholeCount	查询黑洞解封次数。
DescribeBlackholeStatus	查询DDoS高防实例的黑洞状态。
ModifyBlackholeStatus	执行黑洞解封。
DescribeNetworkRegionBlock	查询针对DDoS高防实例的区域封禁配置。
ConfigNetworkRegionBlock	设置针对DDoS高防实例的区域封禁。
DescribeBlockStatus	查询DDoS高防（新BGP）实例的近源流量压制配置。
ModifyBlockStatus	设置DDoS高防（新BGP）实例的近源流量压制。
DescribeUnBlockCount	查询可用的近源流量压制次数。

表 13-5: 网站业务防护策略

API	描述
DescribeWebCcProtectSwitch	查询网站业务各防护功能的开关状态。
ModifyWebAIProtectSwitch	设置网站业务AI智能防护的开关状态。
ModifyWebAIProtectMode	设置网站业务AI智能防护的模式。
ModifyWebIpSetSwitch	设置网站业务黑白名单（针对域名）的开关状态。

API	描述
ConfigWebIpSet	设置针对网站业务的黑名单和白名单IP。
EnableWebCC	开启网站业务频率控制防护（CC防护）的开关。
DisableWebCC	关闭网站业务频率控制防护（CC防护）的开关。
ConfigWebCCTemplate	设置网站业务频率控制防护（CC防护）的防护模式。
EnableWebCCRule	开启网站业务频率控制防护（CC防护）的自定义规则开关。
DisableWebCCRule	关闭网站业务频率控制防护（CC防护）的自定义规则开关。
DescribeWebCCRules	查询网站业务频率控制防护（CC防护）的自定义规则。
CreateWebCCRule	创建网站业务频率控制防护（CC防护）的自定义规则。
ModifyWebCCRule	编辑网站业务频率控制防护（CC防护）的自定义规则。
DeleteWebCCRule	删除网站业务频率控制防护（CC防护）的自定义规则。
ModifyWebPreciseAccessSwitch	设置网站业务精确访问控制的开关状态。
DescribeWebPreciseAccessRule	查询网站业务精确访问控制规则。
ModifyWebPreciseAccessRule	编辑网站业务精确访问控制规则。
DeleteWebPreciseAccessRule	删除网站业务精确访问控制规则。
ModifyWebAreaBlockSwitch	设置网站业务区域封禁（针对域名）的开关状态。
DescribeWebAreaBlockConfigs	查询网站业务区域封禁（针对域名）的配置信息。
ModifyWebAreaBlock	设置网站业务区域封禁（针对域名）的封禁地区。

表 13-6: 非网站业务防护策略

API	描述
DescribePortAutoCcStatus	查询非网站业务AI智能防护的配置信息。
ModifyPortAutoCcStatus	设置非网站业务AI智能防护。

API	描述
DescribeNetworkRuleAttributes	查询非网站业务端口转发规则的防护配置，包括会话保持和DDoS防护策略。
ModifyNetworkRuleAttribute	编辑非网站业务端口转发规则的会话保持策略。

表 13-7: 定制场景策略

API	描述
DescribeSceneDefensePolicies	查询定制场景策略的详细信息。
CreateSceneDefensePolicy	创建定制场景策略。
ModifySceneDefensePolicy	编辑定制场景策略。
DeleteSceneDefensePolicy	删除定制场景策略。
DescribeSceneDefenseObjects	查询定制场景策略的防护对象。
AttachSceneDefenseObject	为定制场景策略添加防护对象。
DetachSceneDefenseObject	为定制场景策略移除防护对象。
EnableSceneDefensePolicy	启用定制场景策略。
DisableSceneDefensePolicy	禁用定制场景策略。

监控报表

API	描述
DescribeDDoSEvents	查询针对DDoS高防实例的攻击事件。
DescribePortFlowList	查询DDoS高防实例的流量数据列表。
DescribePortConnsList	查询DDoS高防实例的端口连接数列表。
DescribePortConnsCount	查询DDoS高防实例的端口连接数统计信息。
DescribePortMaxConns	查询DDoS高防实例的端口连接峰值信息。
DescribePortAttackMaxFlow	查询指定时间段内DDoS高防受到的攻击带宽和包速峰值。
DescribePortViewSourceCountries	查询指定时间段内DDoS高防实例的请求来源国家分布。
DescribePortViewSourceProvinces	查询指定时间段内DDoS高防实例的请求来源（中国）省份分布。
DescribePortViewSourceIsps	查询指定时间段内DDoS高防实例的请求来源运营商分布。
DescribeDomainAttackEvents	查询针对网站业务的攻击事件。

API	描述
DescribeDomainQPSList	查询网站业务的QPS统计信息。
DescribeDomainQpsWithCache	查询网站业务的QPS数据列表，例如总QPS、由不同防护功能阻断的QPS、缓存命中数等。
DescribeDomainOverview	查询网站业务攻击总览，包括HTTP攻击峰值、HTTPS攻击峰值。
DescribeDomainStatusCodeList	查询网站业务的各类响应状态码统计列表。
DescribeDomainStatusCodeCount	查询指定时间段内网站业务的各类响应状态码的统计信息。
DescribeDomainTopAttackList	查询指定时间段内网站业务的QPS峰值数据，包括攻击QPS、总QPS。
DescribeDomainViewSourceCountries	查询指定时间段内网站业务的请求来源国家分布。
DescribeDomainViewSourceProvinces	查询指定时间段内网站业务的请求来源（中国）省份分布。
DescribeDomainViewTopCostTime	查询指定时间段内网站业务的请求耗时最大的前N个URL。
DescribeDomainViewTopUrl	查询指定时间段内网站业务访问量最大的前N个URL。

全量日志分析

API	描述
DescribeSlsOpenStatus	查询阿里云日志服务SLS（Log Service）的开通状态。
DescribeSlsAuthStatus	查询DDoS高防全量日志分析服务的授权状态，即是否授权DDoS高防访问日志服务。
DescribeLogStoreExistStatus	查询是否已创建DDoS高防的日志库。
DescribeSlsLogstoreInfo	查询DDoS高防的日志库信息，例如日志存储容量、日志存储时长等。
ModifyFullLogTtl	编辑DDoS高防全量日志的存储时长。
DescribeWebAccessLogDispatchStatus	查询所有域名的全量日志开关状态。
DescribeWebAccessLogStatus	查询单个网站业务的全量日志服务信息，例如开关状态、对接的日志项目、日志库。
EnableWebAccessLogConfig	为网站业务开启全量日志分析。
DisableWebAccessLogConfig	为网站业务关闭全量日志分析。

API	描述
DescribeWebAccessLogEmptyCount	查询可用的清空日志库的次数。
EmptySlsLogstore	清空DDoS高防的日志库。

标签

API	描述
DescribeTagKeys	查询所有标签键。
DescribeTagResources	查询资源关联的标签信息。
CreateTagResources	为资源关联标签。
DeleteTagResources	为资源移除标签。

静态页面缓存

API	描述
DescribeWebCacheConfigs	查询网站业务静态页面缓存的配置。
ModifyWebCacheSwitch	设置网站业务静态页面缓存的开关状态。
ModifyWebCacheMode	设置网站业务静态页面缓存的缓存模式。
ModifyWebCacheCustomRule	设置网站业务静态页面缓存的自定义规则。
DeleteWebCacheCustomRule	删除网站业务静态页面缓存的自定义规则。

系统配置与日志

API	描述
DescribeStsGrantStatus	查询是否授权DDoS高防服务访问其他云产品。
DescribeBackSourceCidr	查询DDoS高防的回源IP网段。
DescribeOpEntities	查询DDoS高防（新BGP）的操作日志。
DescribeDefenseRecords	查询DDoS高防（国际）的高级防护日志。
DescribeAsyncTasks	查询异步导出任务的详细信息，例如任务ID、任务开始和结束时间、任务状态、任务参数、任务结果等。
CreateAsyncTask	创建异步导出任务，例如导出网站业务转发规则、端口转发规则、会话保持和健康检查配置、DDoS防护策略、IP黑白名单。
DeleteAsyncTask	删除异步导出任务。

13.2 调用方式

DDoS高防接口支持HTTP调用和OpenAPI Explorer调用。DDoS高防接口调用是向DDoS高防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。

HTTP调用

DDoS高防的API是RPC风格，您可以通过发送HTTP GET请求调用DDoS高防API。

其请求结构如下：

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

其中：

- **Endpoint**：DDoS高防API的服务接入地址，取值如下。
  - ddoscoo.cn-hangzhou.aliyuncs.com：DDoS高防（新BGP）
  - ddoscoo.ap-southeast-1.aliyuncs.com：DDoS高防（国际）服务
- **Action**：要执行的操作，如调用**DescribeInstanceIds**查询已创建的DDoS高防实例ID。
- **Version**：要使用的API版本，DDoS高防的API版本是2020-01-01。
- **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，详情请参见#unique_259。

下面是一个调用**DescribeInstanceIds**接口查询已创建的DDoS高防实例ID的示例：

说明：
为了便于用户查看，本文档中的示例都做了格式化处理。

```
https://ddoscoo.cn-hangzhou.aliyuncs.com/?Action=DescribeInstanceIds
&Format=xml
&Version=2020-01-01
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2020-01-01T12:00:00Z
...
```

OpenAPI Explorer调用

OpenAPI Explorer是一款可视化的API调用工具。通过该工具，您可以通过网页或者命令行调用各云产品以及API市场上开放的API，查看每次的API请求和返回结果，并生成相应SDK调用示例。

您可以直接访问https://api.aliyun.com/调用API也可以通过API文档中的调试功能进行调用。

13.3 签名机制

为保证API的安全调用，在调用API时阿里云会对每个API请求通过签名（Signature）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信息。

概述

RPC API要按以下格式在API请求的Query中增加签名（Signature）。

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

其中：

- **SignatureMethod**：签名方式，目前支持HMAC-SHA1。
- **SignatureVersion**：签名算法版本，目前版本是1.0。
- **SignatureNonce**：唯一随机数，用于防止网络重放攻击。用户在不同请求间要使用不同的随机数值，建议使用通用唯一识别码（Universally Unique Identifier，UUID）。
- **Signature**：使用AccessKey Secret对请求进行对称加密后生成的签名。

签名算法遵循RFC 2104 HMAC-SHA1规范，使用AccessSecret对编码、排序后的整个请求串计算HMAC值作为签名。签名的元素是请求自身的一些参数，由于每个API请求内容不同，所以签名的结果也不尽相同。可参考本文的操作步骤，计算签名值。

```
Signature = Base64( HMAC-SHA1( AccessSecret, UTF-8-Encoding-Of( StringToSign)) )
```

步骤一：构造待签名字符串

1. 使用请求参数构造规范化的请求字符串（Canonicalized Query String）。

   a. 按照参数名称的字典顺序对请求中所有的请求参数（包括公共请求参数和接口的自定义参数，但不包括公共请求参数中的Signature参数）进行排序。

   说明：

当使用GET方法提交请求时，这些参数就是请求URI中的参数部分，即URI中“?”之后由“&”连接的部分。

b. 对排序之后的请求参数的名称和值分别用UTF-8字符集进行URL编码。编码规则请参见下表。

字符	编码方式
A-Z、a-z和0-9以及“-”、“_”、“.”和“~”	不编码。
其它字符	编码成%XY的格式，其中XY是字符对应ASCII码的16进制表示。例如英文的双引号（”）对应的编码为%22。
扩展的UTF-8字符	编码成%XY%ZA...的格式。

英文空格	编码成%20，而不是加号（+）。
	该编码方式和一般采用的application/x-www-form-urlencodedMIME格式编码算法（例如Java标准库中的java.net.URLEncoder的实现）存在区别。编码时可以先用标准库的方式进行编码，然后把编码后的字符串中的加号（+）替换成 %20，星号（*）替换成 %2A，%7E替换回波浪号（~），即可得到上述规则描述的编码字符串。本算法可以用下面的percentEncode方法来实现：
	`private static final String ENCODING = "UTF-8";`
	`private static String percentEncode(String value)`
	`throws UnsupportedEncodingException`
	`{`
	`return value != null ? URLEncoder.encode(value,`
	`ENCODING).replace("+", "%20").replace("*", "%2A").`
	`replace("%7E", "~") : null;`
	`}`

c. 将编码后的参数名称和值用英文等号（=）进行连接。

d. 将等号连接得到的参数组合按步骤 i 排好的顺序依次使用“&”符号连接，即得到规范化请求字符串。

2. 将第一步构造的规范化字符串按照下面的规则构造成待签名的字符串。

```
StringToSign=
    HTTPMethod + “&” +
    percentEncode( “/” ) + ” &” +
```

```
percentEncode(CanonicalizedQueryString)
```

其中：

- **HTTPMethod**是提交请求用的HTTP方法，例如GET。
- **percentEncode(“/”)**是按照步骤1- ⅰ 中描述的URL编码规则对字符 “/” 进行编码得到的值，即%2F。
- **percentEncode(CanonicalizedQueryString)**是对步骤1- ⅰ 中构造的规范化请求字符串按步骤1- ⅱ 中描述的URL编码规则编码后得到的字符串。

步骤二：计算签名值

1. 按照RFC2104的定义，计算待签名字符串（StringToSign）的HMAC值。

   说明：

   计算签名时使用的Key就是您持有的AccessKey Secret并加上一个 “&” 字符（ASCII:38），使用的哈希算法是SHA1。

2. 按照Base64编码规则把上面的HMAC值编码成字符串，即得到签名值（Signature）。
3. 将得到的签名值作为**Signature**参数添加到请求参数中。

   说明：

   得到的签名值在作为最后的请求参数值提交时要和其它参数一样，按照RFC3986的规则进行URL编码。

示例

以**DescribeInstanceIds**API 为例，假设使用的AccessKey Id为testid，AccessKey Secret为testsecret。签名前的请求URL如下：

```
http://ddoscoo.cn-hangzhou.aliyuncs.com/?Timestamp=2020-01-01T12%3A00%3A00Z&Format=XML&AccessKeyId=testid&Action=DescribeInstanceIds&SignatureMethod=HMAC-SHA1&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&Version=2020-01-01&SignatureVersion=1.0
```

使用testsecret&，计算得到的签名值是：

```
OLeaidS1JvxuMvnyHOwuJ+uX5qY=
```

将签名作为**Signature**参数加入到URL请求中，最后得到的URL为：

```
http://ddoscoo.cn-hangzhou.aliyuncs.com/?SignatureVersion=1.0&Action=DescribeInstanceIds&Format=XML&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&
```

```
Version=2020-01-01&AccessKeyId=testid&Signature=OLeaidS1JvxuMvnyHOwuJ+uX5qY=&
SignatureMethod=HMAC-SHA1&Timestamp=2020-01-01T12%3A00%3A00Z
```

13.4 公共参数

介绍每个接口都需要使用的请求参数和返回参数。

公共请求参数

名称	类型	是否必须	描述
RegionId	String	是	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
Format	String	否	返回消息的格式。取值： • JSON（默认值） • XML
Version	String	是	API版本号，使用YYYY-MM-DD日期格式。取值： 2020-01-01
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
Timestamp	String	是	请求的时间戳，为日期格式。使用UTC时间按照 ISO8601标准，格式为YYYY-MM-DDThh:mm:ssZ。 例如，北京时间2020年1月1日20点0分0秒，表示为2020-01-01T20:00:00Z。
SignatureVersion	String	是	签名算法版本，取值： 1.0
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

```
http://ddoscoo.cn-hangzhou.aliyuncs.com/?Action=DescribeInstanceIds
&RegionId=cn-hangzhou
&TimeStamp=2020-01-01T20%3A00%3A00Z
&Format=xml
&AccessKeyId=testid
&SignatureMethod=Hmac-SHA1
&SignatureNonce=NwDAxvLU6tFE0DVb
&Version=2020-01-01
&SignatureVersion=1.0
&Signature=Signature
```

公共返回参数

API返回结果采用统一格式，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JSON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**。

- 返回2xxHTTP状态码表示调用成功。
- 返回4xx或5xxHTTP状态码表示调用失败。

公共返回参数示例如下：

- 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*/
  }
```

13.5 获取AccessKey

您可以为阿里云主账号和子账号创建一个访问密钥（AccessKey）。在调用阿里云API时您需要使用AccessKey完成身份验证。

背景信息

AccessKey包括AccessKey ID和AccessKey Secret。

- AccessKeyId：用于标识用户。
- AccessKeySecret：用于验证用户的密钥。AccessKeySecret必须保密。

警告：

主账号Accesskey泄露会威胁您所有资源的安全。建议使用子账号（RAM用户）Accesskey进行操作，可以有效降低Accesskey泄露的风险。

操作步骤

1. 以主账号登录阿里云管理控制台。
2. 将鼠标置于页面右上方的账号图标，单击**accesskeys**。
3. 在**安全提示**页面，选择获取主账号还是子账号的Accesskey。

4. 获取账号Accesskey。

   - 获取主账号AccessKey

     a. 单击**继续使用AccessKey**。

     b. 在**安全信息管理**页面，单击**创建AccessKey**。

     c. 在**手机验证**页面，获取验证码，完成手机验证，单击**确定**。

     d. 在**新建用户AccessKey**页面，展开**AccessKey详情**，查看AccessKeyId和AccessKeySecret。可以单击**保存AK信息**，下载AccessKey信息。

   - 获取子账号AccessKey

     a. 单击**开始使用子用户AccessKey**。

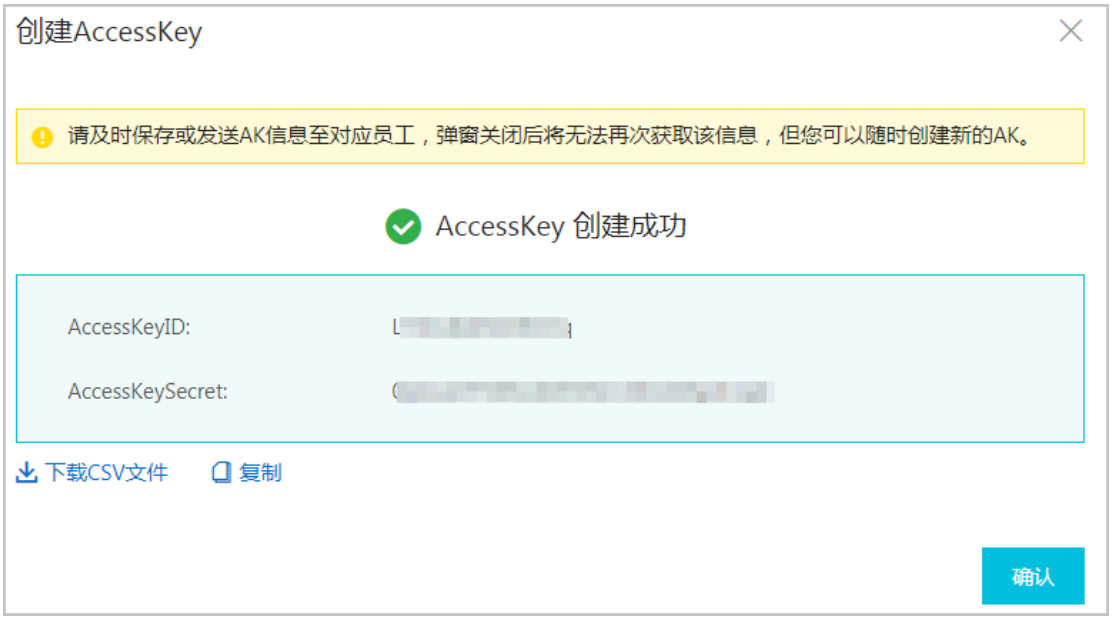
     b. 如果未创建RAM用户，在系统跳转的RAM访问控制台的**新建用户**页面，创建RAM用户。如果是获取已有RAM用户的Accesskey，则跳过此步骤。

     c. 在RAM访问控制台的左侧导航栏，选择**人员管理** > **用户**，搜索需要获取AccessKey的用户。

     d. 单击用户登录名称，在用户详情页**认证管理**页签下的**用户AccessKey**区域，单击**创建新的AccessKey**

     e. 在**手机验证**页面，获取验证码，完成手机验证，单击**确定**。

     f. 在**创建AccessKey**页面，查看AccessKeyId和AccessKeySecret。可以单击**下载CSV文件**，下载AccessKey信息或者单击**复制**，复制AccessKey信息。



13.6 实例

13.6.1 DescribeInstanceIds

调用DescribeInstanceIds查询DDoS高防实例的ID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	DescribeInstanceIds	要执行的操作。取值：**DescribeInstanceIds**
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

名称	类型	是否必选	示例值	描述
Edition	Integer	否	9	DDoS高防实例的防护套餐类型。取值： • **0**：DDoS高防（国际）保险版 • **1**：DDoS高防（国际）无忧版 • **2**：DDoS高防（国际）加速线路 • **9**：DDoS高防（新BGP）专业版
InstanceIds.N	RepeatList	否	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。

返回数据

名称	类型	示例值	描述
InstanceIds	Array		DDoS高防实例的ID信息。
Edition	Integer	9	DDoS高防实例的防护套餐类型。取值： • **0**：DDoS高防（国际）保险版 • **1**：DDoS高防（国际）无忧版 • **2**：DDoS高防（国际）加速线路 • **9**：DDoS高防（新BGP）专业版
InstanceId	String	ddoscoo-cn-v0h12g3z****	DDoS高防实例ID。
Remark	String	test	DDoS高防实例备注。
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribeInstanceIdsResponse>
  <InstanceIds>
```

```
    <InstanceId>ddoscoo-cn-v0h12g3z****</InstanceId>
    <Edition>9</Edition>
    <Remark>test</Remark>
  </InstanceIds>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeInstanceIdsResponse>
```

JSON 格式

```
{
  "InstanceIds": [{
    "InstanceId": "ddoscoo-cn-v0h12g3z****",
    "Edition":9,
    "Remark": "test"
  }],
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

13.6.2 DescribeInstances

调用DescribeInstances查询DDoS高防实例的版本和状态信息，例如业务转发状态、到期状态、欠费状态等。

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**
PageNumber	String	是	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写**1**。
PageSize	String	是	10	页面显示的记录数量。最大值：**50**

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
InstanceIds.N	RepeatList	否	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
Ip	String	否	203.***.***.117	使用IP地址查询，指定要查询的DDoS高防实例的IP地址。支持精确匹配查询。
Remark	String	否	test	使用实例备注查询，指定要查询的DDoS高防实例的备注。支持模糊查询。
Edition	Integer	否	9	使用防护套餐查询，指定要查询的DDoS高防实例的防护套餐版本。取值： • **0**：DDoS高防（国际）保险版 • **1**：DDoS高防（国际）无忧版 • **2**： DDoS高防（国际）加速线路 • **9**：DDoS高防（新BGP）专业版
Enabled	Integer	否	1	使用业务转发状态查询，指定要查询的DDoS高防实例的业务转发状态。取值： • **0**：已停止转发业务 • **1**：正常转发业务

名称	类型	是否必选	示例值	描述
ExpireStartTime	Long	否	1584460800000	使用实例到期时间查询，指定要查询的DDoS高防实例的到期开始时间。时间戳格式，单位：毫秒。
ExpireEndTime	Long	否	1584560800000	使用实例到期时间查询，指定要查询的DDoS高防实例的到期结束时间。时间戳格式，单位：毫秒。
Status.N	RepeatList	否	1	使用实例的到期状态查询，指定要查询的DDoS高防实例的到期状态。取值： • **1**：正常 • **2**：到期
Tag.N.Key	String	否	testkey	使用实例标签查询，指定要查询的DDoS高防实例的标签键。 **说明：** 标签键（**Tag.N.Key**）与标签值（**Tag.N.Value**）必须键值匹配。
Tag.N.Value	String	否	a	使用实例标签查询，指定要查询的DDoS高防实例的标签值。 **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
Instances	Array		DDoS高防实例的版本和状态信息。
CreateTime	Long	1581946582000	实例创建时间。时间戳格式，单位：毫秒。

名称	类型	示例值	描述
DebtStatus	Integer	0	实例的欠费状态。取值固定为**0**，表示不欠费，因为DDoS高防服务目前只支持包年包月的预付费计费方式。
Edition	Integer	9	防护套餐版本。取值： • **0**：DDoS高防（国际）保险版 • **1**：DDoS高防（国际）无忧版 • **2**： DDoS高防（国际）加速线路 • **9**：DDoS高防（新BGP）专业版
Enabled	Integer	1	实例的业务转发状态。取值： • **0**：已停止转发业务 • **1**：正常转发业务
ExpireTime	Long	1584460800000	实例到期时间。时间戳格式，单位：毫秒。
InstanceId	String	ddoscoo-cn-mp91j1ao****	实例ID。
Remark	String	test	实例备注。
Status	Integer	1	实例的到期状态。取值： • **1**：正常 • **2**：到期
RequestId	String	A09C1F98-4CC1-4A31-B8F3-9E4B7437189F	本次请求的ID。
TotalCount	Long	1	DDoS高防实例的总数。

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribeInstancesResponse>
  <Instances>
    <Status>1</Status>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
    <CreateTime>1581946582000</CreateTime>
    <Enabled>1</Enabled>
    <ExpireTime>1584460800000</ExpireTime>
    <Edition>9</Edition>
    <Remark>test</Remark>
    <DebtStatus>0</DebtStatus>
  </Instances>
  <TotalCount>1</TotalCount>
  <RequestId>A09C1F98-4CC1-4A31-B8F3-9E4B7437189F</RequestId>
</DescribeInstancesResponse>
```

JSON 格式

```
{
 "Instances": [
  {
   "Status": 1,
   "InstanceId": "ddoscoo-cn-mp91j1ao****",
   "CreateTime": 1581946582000,
   "Enabled": 1,
   "ExpireTime": 1584460800000,
   "Edition": 9,
   "Remark": "test",
   "DebtStatus": 0
  }
 ],
 "TotalCount": 1,
 "RequestId": "A09C1F98-4CC1-4A31-B8F3-9E4B7437189F"
}
```

错误码

访问错误中心查看更多错误码。

13.6.3 DescribeInstanceDetails

调用DescribeInstanceDetails查询DDoS高防实例的IP和线路信息。

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	要执行的操作。取值：**DescribeInstanceDetails**

名称	类型	是否必选	示例值	描述
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	要查询的DDoS高防实例的ID。 **说明:** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值: • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
InstanceDetails	Array		DDoS高防实例的IP和线路信息。
EipInfos	Array		DDoS高防实例的IP信息。
Eip	String	203.***.**.117	DDoS高防实例的IP地址。
Status	String	normal	DDoS高防IP的状态。取值: • **normal**：正常 • **cleaning**：清洗中 • **blackhole**：黑洞中
InstanceId	String	ddoscoo-cn-mp91j1ao****	DDoS高防实例ID。
Line	String	coop-line-001	DDoS高防实例的线路。例如，**coop-line-001**。
RequestId	String	3C814429-21A5-4673-827E-FDD19DC75681	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeInstanceDetails
```

```
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeInstanceDetailsResponse>
  <InstanceDetails>
    <Line>coop-line-001</Line>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
    <EipInfos>
      <Status>normal</Status>
      <Eip>203.***.**.117</Eip>
    </EipInfos>
  </InstanceDetails>
  <RequestId>3C814429-21A5-4673-827E-FDD19DC75681</RequestId>
</DescribeInstanceDetailsResponse>
```

JSON 格式

```
{
 "InstanceDetails": [
  {
   "Line": "coop-line-001",
   "InstanceId": "ddoscoo-cn-mp91j1ao****",
   "EipInfos": [
    {
     "Status": "normal",
     "Eip": "203.***.**.117"
    }
   ]
  }
 ],
 "RequestId": "3C814429-21A5-4673-827E-FDD19DC75681"
}
```

错误码

访问错误中心查看更多错误码。

13.6.4 DescribeInstanceSpecs

调用DescribeInstanceSpecs查询DDoS高防实例的规格信息。

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	DescribeInstanceSpecs	要执行的操作。取值：**DescribeInstanceSpecs**
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	要查询的DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
InstanceSpecs	Array		DDoS高防实例的规格信息。
BandwidthMbps	Integer	100	正常业务带宽，单位：Mbps。
BaseBandwidth	Integer	30	基础防护带宽，单位：Gbps。
DefenseCount	Integer	1	本月可用高级防护次数。**-1**表示无限次，即实例的防护套餐类型为无忧版。 **说明：** 只有DDoS高防（国际）实例拥有该属性。
DomainLimit	Integer	50	可防护的域名数量。
ElasticBandwidth	Integer	30	弹性防护带宽，单位：Gbps。

名称	类型	示例值	描述
FunctionVersion	String	default	功能套餐类型。取值： • **default**：标准功能 • **enhance**：增强功能
InstanceId	String	ddoscoo-cn-mp91j1ao****	DDoS高防实例ID。
PortLimit	Integer	50	可防护的端口数量。
QpsLimit	Integer	3000	正常业务QPS。
SiteLimit	Integer	5	可防护的站点数量。
RequestId	String	23B0245A-0CCC-4637-A8C6-7CA0479395B2	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeInstanceSpecs
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeInstanceSpecsResponse>
  <RequestId>23B0245A-0CCC-4637-A8C6-7CA0479395B2</RequestId>
  <InstanceSpecs>
    <QpsLimit>3000</QpsLimit>
    <BaseBandwidth>30</BaseBandwidth>
    <PortLimit>50</PortLimit>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
    <DomainLimit>50</DomainLimit>
    <FunctionVersion>default</FunctionVersion>
    <ElasticBandwidth>30</ElasticBandwidth>
    <SiteLimit>5</SiteLimit>
    <BandwidthMbps>100</BandwidthMbps>
  </InstanceSpecs>
</DescribeInstanceSpecsResponse>
```

JSON 格式

```
{
 "RequestId": "23B0245A-0CCC-4637-A8C6-7CA0479395B2",
 "InstanceSpecs": [
  {
```

```
  "QpsLimit": 3000,
  "BaseBandwidth": 30,
  "PortLimit": 50,
  "InstanceId": "ddoscoo-cn-mp91j1ao****",
  "DomainLimit": 50,
  "FunctionVersion": "default",
  "ElasticBandwidth": 30,
  "SiteLimit": 5,
  "BandwidthMbps": 100
 }
 ]
}
```


错误码

访问错误中心查看更多错误码。

13.6.5 DescribeInstanceStatistics

调用DescribeInstanceStatistics查询DDoS高防实例的统计信息，例如已防护的域名、端口数量等。

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	要执行的操作。取值：**DescribeInstanceStatistics**
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	要查询的DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
InstanceStatistics	Array		DDoS高防实例的统计信息。
DefenseCountUsage	Integer	1	本月已用高级防护次数。 **说明:** 只有DDoS高防（国际）实例拥有该属性。
DomainUsage	Integer	1	已防护的域名数量。
InstanceId	String	ddoscoo-cn-mp91j1ao****	DDoS高防实例ID。
PortUsage	Integer	2	已防护的端口数量。
SiteUsage	Integer	1	已防护的站点数量。
RequestId	String	642319A9-D1F2-4459-A447-E57CFC599FDE	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeInstanceStatistics
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeInstanceStatisticsResponse>
  <InstanceStatistics>
    <PortUsage>2</PortUsage>
    <SiteUsage>1</SiteUsage>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
    <DomainUsage>1</DomainUsage>
  </InstanceStatistics>
  <RequestId>642319A9-D1F2-4459-A447-E57CFC599FDE</RequestId>
</DescribeInstanceStatisticsResponse>
```

`JSON` 格式

```
{
```

```
 "InstanceStatistics": [
  {
   "PortUsage": 2,
   "SiteUsage": 1,
   "InstanceId": "ddoscoo-cn-mp91j1ao****",
   "DomainUsage": 1
  }
 ],
 "RequestId": "642319A9-D1F2-4459-A447-E57CFC599FDE"
}
```


错误码

访问错误中心查看更多错误码。

13.6.6 ModifyInstanceRemark

调用ModifyInstanceRemark编辑DDoS高防实例的备注。

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	要执行的操作。取值：**ModifyInstanceRemark**
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
InstanceId	String	否	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
Remark	String	否	new-remark	实例的备注。

返回数据

名称	类型	示例值	描述
RequestId	String	7EFA2BA6-9C0A-4410-B735-FC337EB634A1	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyInstanceRemark
&InstanceId=ddoscoo-cn-mp91j1ao****
&Remark=new-remark
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<ModifyInstanceRemarkResponse>
  <RequestId>7EFA2BA6-9C0A-4410-B735-FC337EB634A1</RequestId>
</ModifyInstanceRemarkResponse>
```

`JSON` 格式

```
{
 "RequestId": "7EFA2BA6-9C0A-4410-B735-FC337EB634A1"
}
```

错误码

访问错误中心查看更多错误码。

13.6.7 DescribeElasticBandwidthSpec

调用DescribeElasticBandwidthSpec查询DDoS高防（新BGP）实例的可选弹性防护带宽规格。

说明:

该接口仅适用于DDoS高防（新BGP）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	DescribeElasticBandwidthSpec	要执行的操作。取值：**DescribeElasticBandwidthSpec**
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明:** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值：**cn-hangzhou**，表示DDoS高防（新BGP）服务。

返回数据

名称	类型	示例值	描述
ElasticBandwidthSpec	List	[5,10,20,30]	可选的弹性防护带宽规格列表。单位：Gbps。
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeElasticBandwidthSpec
&InstanceId=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

XML 格式

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

```
</DescribeElasticBandwidthSpecResponse>
```

JSON 格式

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

错误码

访问错误中心查看更多错误码。

13.6.8 ModifyElasticBandWidth

调用ModifyElasticBandWidth修改DDoS高防（新BGP）实例的弹性防护带宽。

说明:
该接口仅适用于DDoS高防（新BGP）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	ModifyElasticBandWidth	要执行的操作。取值：**ModifyElasticBandWidth**
ElasticBandwidth	Integer	是	50	要设置的弹性防护带宽，单位：Gbps。 **说明:** 您可以调用DescribeElasticBandwidthSpec查询可选的弹性防护带宽规格。

名称	类型	是否必选	示例值	描述
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明:** 实例必须处于正常状态。您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值：**cn-hangzhou**，表示DDoS高防（新BGP）服务。

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=ModifyElasticBandWidth
&ElasticBandwidth=50
&InstanceId=ddoscoo-cn-mp91j1ao****
&<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。

13.6.9 DescribeDefenseCountStatistics

调用DescribeDefenseCountStatistics查询DDoS高防（国际）服务的防护次数统计信息，例如可用和已用的高级防护次数。

说明：
该接口仅适用于DDoS高防（国际）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	DescribeDefenseCountStatistics	要执行的操作。取值：**DescribeDefenseCountStatistics**
RegionId	String	否	ap-southeast-1	DDoS高防服务地域ID。取值：**ap-southeast-1**，表示DDoS高防（国际）服务。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
DefenseCountStatistics	Struct		防护次数统计信息。
DefenseCountTotalUsageOfCurrentMonth	Integer	1	本月已用的高级防护次数。

名称	类型	示例值	描述
FlowPackCountRemain	Integer	1	剩余可用的全局抗D次数。 **说明:** 全局抗D防护由DDoS高防在新用户首次开通服务时赠送获得，可用于抵扣一次攻击。
MaxUsableDefenseCountCurrentMonth	Integer	2	本月可用的高级防护次数。
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。

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

```
<DescribeDefenseCountStatisticsResponse>
  <DefenseCountStatistics>
    <DefenseCountTotalUsageOfCurrentMonth>1</DefenseCountTotalUsageOfCurrentMonth>
    <FlowPackCountRemain>1</FlowPackCountRemain>
    <MaxUsableDefenseCountCurrentMonth>2</MaxUsableDefenseCountCurrentMonth>
  </DefenseCountStatistics>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeDefenseCountStatisticsResponse>
```

JSON 格式

```
{
  "DefenseCountStatistics": {
    "DefenseCountTotalUsageOfCurrentMonth": 1,
    "FlowPackCountRemain": 1,
    "MaxUsableDefenseCountCurrentMonth": 2
  },
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

13.6.10 ReleaseInstance

调用ReleaseInstance释放某个已经到期的DDoS高防实例。

DDoS高防实例到期后，将停止提供DDoS攻击防御服务，且实例到期7天后，将停止业务流量转发。

- 建议您的实例到期前及时续费，避免实例到期对业务防护和转发带来影响。您可以调用DescribeInstances查询实例的到期时间。如果需要续费，请前往DDoS高防控制台进行操作。
- 如果您不计划续费实例，则建议您在DDoS高防实例到期前恢复已接入防护的业务IP（例如不再使用DDoS高防IP作为业务IP）或业务DNS解析（例如不再将业务流量解析到DDoS高防的CNAME地址），停止将业务转发到DDoS高防实例，避免实例到期对正常业务转发带来影响。

实例到期后，您可以调用本接口释放指定的DDoS高防实例。

说明：
释放指定实例前，请务必确认您已经恢复接入防护的业务IP或业务DNS解析。

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	ReleaseInstance	要执行的操作。取值：**ReleaseInstance**。
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	要释放的实例ID。 **说明：** 只允许释放已到期的实例。您可以调用DescribeInstances查询所有DDoS高防实例的ID和到期状态信息。
RegionId	String	是	cn-hangzhou	DDoS高防服务的地域ID。取值： • **cn-hangzhou**：中国内地地域，表示DDoS高防（新BGP）服务 • **ap-southeast-1**：非中国内地地域，表示DDoS高防（国际）服务

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=ReleaseInstance
&InstanceId=ddoscoo-cn-mp91j1ao****
&RegionId=cn-hangzhou
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.7 域名接入

13.7.1 DescribeDomains

调用DescribeDomains查询已配置网站业务转发规则的域名。

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	要执行的操作。取值：**DescribeDomains**。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
InstanceIds.N	RepeatList	否	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明:** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。

返回数据

名称	类型	示例值	描述
Domains	List	["www.aliyun.com"]	域名列表。
RequestId	String	F908E959-ADA8-4D7B-8A05-FF2F67F50964	本次请求的ID。

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribeDomainsResponse>
```

```
  <Domains>www.aliyun.com</Domains>
  <RequestId>F908E959-ADA8-4D7B-8A05-FF2F67F50964</RequestId>
</DescribeDomainsResponse>
```

JSON 格式

```
{
 "Domains": [
  "www.aliyun.com"
 ],
 "RequestId": "F908E959-ADA8-4D7B-8A05-FF2F67F50964"
}
```

错误码

访问错误中心查看更多错误码。

13.7.2 DescribeWebRules

调用DescribeWebRules查询网站业务转发规则。

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	DescribeWebRules	要执行的操作。取值：**DescribeWebRules**
PageSize	Integer	是	10	页面显示的记录数量。最大值：**10**
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

名称	类型	是否必选	示例值	描述
Domain	String	否	www.aliyun.com	网站业务的域名。  **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
QueryDomainPattern	String	否	fuzzy	查询匹配模式。取值: • **fuzzy**:模糊查询(默认) • **exact**:精确查询
PageNumber	Integer	否	1	分页查询请求时返回的页码。例如,查询第一页的返回结果,则填写**1**。
InstanceIds.N	RepeatList	否	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。  **说明:** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。

返回数据

名称	类型	示例值	描述
RequestId	String	89E69DD6-C5DD-4636-9AD6-CCF6BEAB59AC	本次请求的ID。
TotalCount	Long	1	返回的网站业务转发规则总数。
WebRules	Array		网站业务转发规则信息。
BlackList	List	[1.***.***.1]	IP黑名单(针对域名)列表。
CcEnabled	Boolean	true	是否开启了频率控制防护(CC防护)。取值: • **true**:已开启 • **false**:未开启

名称	类型	示例值	描述
CcRuleEnabled	Boolean	false	是否开启了自定义频率控制防护（CC防护）。取值： • **true**：已开启 • **false**：未开启
CcTemplate	String	default	频率控制防护（CC防护）的模式。取值： • **default**：正常 • **gf_under_attack**：攻击紧急 • **gf_sos_verify**：严格 • **gf_sos_enhance**：超级严格
CertName	String	testcert	证书名称。
Cname	String	64687s1jf898****.aliyunddos0001.com	CNAME地址。
Domain	String	www.aliyun.com	网站域名。
Http2Enable	Boolean	true	是否开启了HTTP2.0。取值： • **true**：已开启 • **false**：未开启
ProxyTypes	Array		协议信息。
ProxyPorts	List	80	服务器端口。
ProxyType	String	http	协议类型。取值： • **http** • **https** • **websocket** • **websockets**
RealServers	Array		服务器地址信息。
RealServer	String	1.***.***.1	服务器地址。

名称	类型	示例值	描述
RsType	Integer	0	地址类型。取值： • **0**：源站IP • **1**：源站域名
SslCiphers	String	default	加密套件类型。取值： • **default**：默认，仅包含强加密套件 • **all**：全部加密套件，包含强加密套件和弱加密套件 • **strong**：强加密套件
SslProtocols	String	tls1.0	TLS版本。取值： • **tls1.0**：支持TLS1.0及以上 • **tls1.1**：支持TLS1.1及以上 • **tls1.2**：支持TLS1.2及以上
WhiteList	List	[1.***.***.1]	IP白名单（针对域名）列表。

示例

请求示例

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

正常返回示例

`XML` 格式

```
<DescribeWebRulesResponse>
  <TotalCount>1</TotalCount>
  <WebRules>
    <CcEnabled>true</CcEnabled>
    <SslProtocols>tls1.0</SslProtocols>
    <ProxyTypes>
      <ProxyPorts>443</ProxyPorts>
      <ProxyType>https</ProxyType>
    </ProxyTypes>
    <ProxyTypes>
      <ProxyPorts>80</ProxyPorts>
      <ProxyType>http</ProxyType>
    </ProxyTypes>
    <RealServers>
      <RealServer>1.***.***.1</RealServer>
      <RsType>0</RsType>
    </RealServers>
    <CcRuleEnabled>false</CcRuleEnabled>
    <SslCiphers>default</SslCiphers>
```

```
    <CertName></CertName>
    <Domain>www.aliyun.com</Domain>
    <Http2Enable>false</Http2Enable>
    <Cname>64687s1jf898****.aliyunddos0001.com</Cname>
    <CcTemplate>default</CcTemplate>
  </WebRules>
  <RequestId>89E69DD6-C5DD-4636-9AD6-CCF6BEAB59AC</RequestId>
</DescribeWebRulesResponse>
```

JSON 格式

```
{
 "TotalCount": 1,
 "WebRules": [
  {
   "CcEnabled": true,
   "SslProtocols": "tls1.0",
   "ProxyTypes": [
    {
     "ProxyPorts": [
      443
     ],
     "ProxyType": "https"
    },
    {
     "ProxyPorts": [
      80
     ],
     "ProxyType": "http"
    }
   ],
   "RealServers": [
    {
     "RealServer": "1.***.***.1",
     "RsType": 0
    }
   ],
   "CcRuleEnabled": false,
   "SslCiphers": "default",
   "CertName": "",
   "Domain": "www.aliyun.com",
   "Http2Enable": false,
   "Cname": "64687s1jf898****.aliyunddos0001.com",
   "CcTemplate": "default"
  }
 ],
 "RequestId": "89E69DD6-C5DD-4636-9AD6-CCF6BEAB59AC"
}
```

错误码

访问错误中心查看更多错误码。

13.7.3 CreateWebRule

调用CreateWebRule创建网站业务转发规则。

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	CreateWebRule	要执行的操作。取值：**CreateWebRule**
Domain	String	是	www.aliyun.com	网站业务的域名。
RsType	Integer	是	0	服务器地址类型。取值： • **0**：源站IP • **1**：源站域名
Rules	String	是	[{"ProxyRules":[{"ProxyPort":80,"RealServers":["1.1.1.1"]}],"ProxyType":"http"},{"ProxyRules":[{"ProxyPort":443,"RealServers":["1.1.1.1"]}],"ProxyType":"https"}]	网站业务转发规则的详细信息。使用JSON格式的字符串表达，具体结构如下。 • **ProxyRules**：Array类型，必选，协议信息。具体结构如下。 - **ProxyPort**：Integer类型，必选，端口号。 - **RealServers**：Array类型，必选，服务器地址。 • **ProxyType**：String类型，必选，协议类型。取值： - **http** - **https** - **websocket** - **websockets**

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
InstanceIds.N	RepeatList	否	ddoscoo-cn-mp91j1ao****	要关联的DDoS高防实例的ID。不传入该参数表示只添加域名，不关联高防实例。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。

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=CreateWebRule
&Domain=www.aliyun.com
&RsType=0
&Rules=[{"ProxyRules":[{"ProxyPort":80,"RealServers":["1.1.1.1"]}],"ProxyType":"http"},{"
ProxyRules":[{"ProxyPort":443,"RealServers":["1.1.1.1"]}],"ProxyType":"https"}]
&<公共请求参数>
```

正常返回示例

XML 格式

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

```
</CreateWebRuleResponse>
```

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。

13.7.4 ModifyWebRule

调用ModifyWebRule编辑网站业务转发规则。

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	ModifyWebRule	要执行的操作。取值：**ModifyWebRule**
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RealServers.N	RepeatList	是	1.1.1.1	服务器地址列表。
RsType	Integer	是	0	服务器地址类型。取值： • **0**：源站IP • **1**：源站域名
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

名称	类型	是否必选	示例值	描述
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
ProxyTypes	String	否	[{"ProxyType":"http","ProxyPorts":[80]},{"ProxyType":"https","ProxyPorts":[443]}]	网站业务转发规则的协议信息。使用JSON格式的字符串表达，具体结构如下。 • **ProxyType**：String类型，必选，协议类型。取值： - **http** - **https** - **websocket** - **websockets** • **ProxyPort**：Integer类型，必选，端口号。
InstanceIds.N	RepeatList	否	ddoscoo-cn-mp91j1ao****	要关联的DDoS高防实例的ID。如果不传入该参数，表示只添加域名，不关联DDoS高防实例。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。

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=ModifyWebRule
&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

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

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。

13.7.5 DeleteWebRule

调用DeleteWebRule删除网站业务转发规则。

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	DeleteWebRule	要执行的操作。取值：**DeleteWebRule**
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

名称	类型	是否必选	示例值	描述
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=DeleteWebRule
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.7.6 DescribeWebInstanceRelations

调用DescribeWebInstanceRelations查询网站业务关联的DDoS高防实例信息。

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	DescribeWebInstanceRelations	要执行的操作。取值：**DescribeWebInstanceRelations**
Domains.N	RepeatList	是	www.aliyun.com	网站业务的域名。  **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
RequestId	String	0222382B-5FE5-4FF7-BC9B-97EE31D58818	本次请求的ID。
WebInstanceRelations	Array		网站业务关联的DDoS高防实例信息。
Domain	String	www.aliyun.com	网站域名。
InstanceDetails	Array		关联的DDoS高防实例信息。
EipList	List	203.***.***.158	DDoS高防IP列表。

名称	类型	示例值	描述
FunctionVersion	String	enhance	功能套餐类型。取值： • **default**：标准功能 • **enhance**：增强功能
InstanceId	String	ddoscoo-cn-0pp163pd****	DDoS高防实例ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeWebInstanceRelations
&Domains.1=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeWebInstanceRelationsResponse>
  <RequestId>0222382B-5FE5-4FF7-BC9B-97EE31D58818</RequestId>
  <WebInstanceRelations>
    <InstanceDetails>
      <EipList>203.***.***.158</EipList>
      <InstanceId>ddoscoo-cn-0pp163pd****</InstanceId>
      <FunctionVersion>enhance</FunctionVersion>
    </InstanceDetails>
    <InstanceDetails>
      <EipList>203.***.***.38</EipList>
      <InstanceId>ddoscoo-cn-45917cd3****</InstanceId>
      <FunctionVersion>enhance</FunctionVersion>
    </InstanceDetails>
    <Domain>www.aliyun.com</Domain>
  </WebInstanceRelations>
</DescribeWebInstanceRelationsResponse>
```

`JSON` 格式

```
{
 "RequestId": "0222382B-5FE5-4FF7-BC9B-97EE31D58818",
 "WebInstanceRelations": [
  {
   "InstanceDetails": [
    {
     "EipList": [
      "203.***.***.158"
     ],
     "InstanceId": "ddoscoo-cn-0pp163pd****",
     "FunctionVersion": "enhance"
    },
    {
     "EipList": [
      "203.***.***.38"
     ],
```

```
    "InstanceId": "ddoscoo-cn-45917cd3****",
    "FunctionVersion": "enhance"
   }
  ],
  "Domain": "www.aliyun.com"
 }
]
}
```


错误码

访问错误中心查看更多错误码。

13.7.7 DescribeCerts

调用DescribeCerts查询网站业务的证书信息。

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	DescribeCerts	要执行的操作。取值：**DescribeCerts**
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
Domain	String	否	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

返回数据

名称	类型	示例值	描述
Certs	Array		网站业务的证书信息。
Common	String	www.aliyun.com	证书关联的域名。
DomainRelated	Boolean	true	证书是否关联域名。取值： • **true**：已关联 • **false**：未关联
EndDate	String	2021-09-12	证书到期日期。字符串格式。
Id	Integer	81	证书ID。
Issuer	String	Symantec	证书颁发机构。
Name	String	testcert	证书名称。
StartDate	String	2019-09-12	证书签发日期。字符串格式。
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。

示例

请求示例

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

正常返回示例

`XML` 格式

```
<DescribeCertsResponse>
    <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
    <Certs>
        <Id>81</Id>
        <Name>testcert</Name>
        <Common>www.aliyun.com</Common>
        <DomainRelated>true</DomainRelated>
        <Issuer>Symantec</Issuer>
        <StartDate>2019-09-12</StartDate>
        <EndDate>2021-09-12</EndDate>
    </Certs>
```

```
</DescribeCertsResponse>
```

JSON 格式

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
  "Certs": [
    {
      "Id": 81,
      "Name": "testcert",
      "Common": "www.aliyun.com",
      "DomainRelated": true,
      "Issuer": "Symantec",
      "StartDate": "2019-09-12",
      "EndDate": "2021-09-12"
    }
  ]
}
```

错误码

访问错误中心查看更多错误码。

13.7.8 AssociateWebCert

调用AssociateWebCert为网站业务转发规则关联SSL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	AssociateWebCert	要执行的操作。取值：**AssociateWebCert**
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
CertId	Integer	否	2404693	要关联的证书ID。如果要关联的证书已经在SSL证书服务中签发，您可以传入证书ID直接关联。  **说明：** 传入证书ID后，无需传入**CertName**、**Cert**和**Key**。
CertName	String	否	example-cert	要关联的证书名称。该参数必须与**Cert**和**Key**一同使用。  **说明：** 传入**CertName**、**Cert**和**Key**后，无需传入**CertId**。

名称	类型	是否必选	示例值	描述
Cert	String	否	-----BEGIN CERTIFICATE----- 62EcYPWd2Oy1vs6MTXcJSfN9Z7rZ9fmxWr2BFN2XbahgnsSXM48ixZJ4krc+1M+j2kcubVpsE2cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOkjgvhlqt9vc65Cgb4mL+n5+DV9uOyTZTW/MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvIAqYxXZ7wRwWWmv4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg== -----END CERTIFICATE-----	要关联的证书公钥。该参数必须与**CertName**和**Key**一同使用。 **说明:** 传入**CertName**、**Cert**和**Key**后，无需传入**CertId**。

名称	类型	是否必选	示例值	描述
Key	String	否	-----BEGIN RSA PRIVATE KEY----- DADTPZoOHd 9WtZ3UKHJT RgNQmioPQn 2bqdKHop+B/ dn/4VZL7Jt8zS DGM9sTMThL yvsmLQKBgQ Cr+ujntC1kN6p GBj2Fw2l/EA /W3rYEce2ty hjgmG7rZ+A /jVE9fld5sQ ra6ZdwBcQJ aiygoIYoaM F2EjRwc0qw Haluq0C15f 6ujSoHh2e+ D5zdmkTg/ 3NKNjqNv6x A2gYpinVDz FdZ9Zujxvu h9o4Vqf0YF 8bv5UK5G04 RtKadOw== -----END RSA PRIVATE KEY----- 	要关联的证书私钥。该参数必须与**CertName**和**Cert**一同使用。 **说明:** 传入**CertName**、**Cert**和**Key**后，无需传入**CertId**。

返回数据

名称	类型	示例值	描述
RequestId	String	40F11005-A75C-4644-95F2-52A4E7D43E91	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=AssociateWebCert
&Domain=www.aliyun.com
```

```
&CertId=2404693
&<公共请求参数>
```

正常返回示例

XML 格式

```
<AssociateWebCertResponse>
  <RequestId>40F11005-A75C-4644-95F2-52A4E7D43E91</RequestId>
</AssociateWebCertResponse>
```

JSON 格式

```
{
 "RequestId": "40F11005-A75C-4644-95F2-52A4E7D43E91"
}
```

错误码

访问错误中心查看更多错误码。

13.7.9 DescribeWebCustomPorts

调用DescribeWebCustomPorts查询DDoS高防支持的网站业务自定义端口范围。

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	DescribeWebCustomPorts	要执行的操作。取值：**DescribeWebCustomPorts**
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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。
WebCustomPorts	Array		网站业务自定义端口信息。
ProxyPorts	List	[80,8080]	可选端口范围。
ProxyType	String	http	协议类型。取值： • **http** • **https**

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribeWebCustomPortsResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
  <WebCustomPorts>
    <ProxyType>https</ProxyType>
    <ProxyPorts>443</ProxyPorts>
    <ProxyPorts>8443</ProxyPorts>
  </WebCustomPorts>
  <WebCustomPorts>
    <ProxyType>http</ProxyType>
    <ProxyPorts>80</ProxyPorts>
    <ProxyPorts>8080</ProxyPorts>
  </WebCustomPorts>
</DescribeWebCustomPortsResponse>
```

JSON 格式

```
{
   "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "WebCustomPorts": [
      {
         "ProxyType": "https",
         "ProxyPorts": [
            443,
            8443
         ]
      },
```

```
    {
      "ProxyType": "http",
      "ProxyPorts": [
        80,
        8080
      ]
    }
  ]
}
```

错误码

访问错误中心查看更多错误码。

13.7.10 ModifyTlsConfig

调用ModifyTlsConfig编辑网站业务转发规则的TLS安全策略。

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	ModifyTlsConfig	要执行的操作。取值：**ModifyTlsConfig**
Config	String	是	{"ssl_protocols":"tls1.0","ssl_ciphers":"all"}	TLS安全策略的详细信息，使用JSON格式的字符串表达，具体结构如下。 • **ssl_protocols**：String类型，必选，TLS版本。取值： - **tls1.0**：支持TLS1.0及以上 - **tls1.1**：支持TLS1.1及以上 - **tls1.2**：支持TLS1.2及以上 • **ssl_ciphers**：String类型，必选，加密套件类型。取值： - **all**：全部加密套件，包含强加密套件和弱加密套件 - **strong**：强加密套件 - **default**：默认，仅包含强加密套件

名称	类型	是否必选	示例值	描述
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值: • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyTlsConfig
&Config={"ssl_protocols":"tls1.0","ssl_ciphers":"all"}
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ModifyTlsConfigResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</ModifyTlsConfigResponse>
```

JSON 格式

```
{
```

```
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

访问错误中心查看更多错误码。

13.7.11 ModifyHttp2Enable

调用ModifyHttp2Enable设置网站业务转发规则的HTTP2.0开关状态。

> **说明:**
> 该接口仅适用于DDoS高防（新BGP）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	ModifyHttp 2Enable	要执行的操作。取值：**ModifyHttp 2Enable**
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明:** 域名必须已配置网站业务转发规则且关联了增强功能套餐的DDoS高防实例。您可以调用DescribeDomains查询所有域名。
Enable	Integer	是	1	HTTP2.0的开关状态。取值： • **0**：关闭 • **1**：开启
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值：**cn-hangzhou**，表示DDoS高防（新BGP）服务。

名称	类型	是否必选	示例值	描述
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyHttp2Enable
&Domain=www.aliyun.com
&Enable=1
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ModifyHttp2EnableResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</ModifyHttp2EnableResponse>
```

JSON 格式

```
{
   "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

访问错误中心查看更多错误码。

13.7.12 DescribeWebAccessMode

调用DescribeWebAccessMode查询网站业务的接入模式。

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	DescribeWebAccessMode	要执行的操作。取值：**DescribeWebAccessMode**
Domains.N	RepeatList	是	www.aliyun.com	网站业务的域名。 **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
DomainModes	Array		网站业务的接入模式信息。
AccessMode	Integer	0	接入模式。取值： • **0**：A记录接入 • **1**：高防模式 • **2**：回源模式
Domain	String	www.aliyun.com	网站域名。
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeWebAccessMode
&Domains.1=www.aliyun.com
```

```
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeWebAccessModeResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
  <DomainModes>
    <Domain>www.aliyun.com</Domain>
    <AccessMode>0</AccessMode>
  </DomainModes>
</DescribeWebAccessModeResponse>
```

JSON 格式

```
{
   "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "DomainModes": [
      {
         "Domain": "www.aliyun.com",
         "AccessMode": 0
      }
   ]
}
```

错误码

访问错误中心查看更多错误码。

13.7.13 ModifyWebAccessMode

调用ModifyWebAccessMode设置网站业务的接入模式。

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	ModifyWebAccessMode	要执行的操作。取值： **ModifyWebAccessMode**
AccessMode	Integer	是	2	网站业务的接入模式。取值： • **0**：A记录 • **1**：高防模式 • **2**：回源模式

名称	类型	是否必选	示例值	描述
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值: • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

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=ModifyWebAccessMode
&AccessMode=2
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

`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。

13.7.14 DescribeCnameReuses

调用DescribeCnameReuses查询网站业务的CNAME复用信息。

> **说明：**
> 该接口仅适用于DDoS高防（国际）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	DescribeCnameReuses	要执行的操作。取值：**DescribeCnameReuses**
Domains.N	RepeatList	是	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	ap-southeast-1	DDoS高防服务地域ID。取值：**ap-southeast-1**，表示DDoS高防（国际）服务。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
CnameReuses	Array		CNAME复用信息。
Cname	String	4o6ep6q217k9****.aliyunddos0004.com	复用的CNAME值。
Domain	String	www.aliyun.com	网站域名。
Enable	Integer	1	是否已开启CNAME复用。取值： • **0**：未开启 • **1**：已开启
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeCnameReuses
&Domains.1=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeCnameReusesResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
  <CnameReuses>
    <Domain>www.aliyun.com</Domain>
    <Cname>4o6ep6q217k9****.aliyunddos0004.com</Cname>
    <Enable>1</Enable>
  </CnameReuses>
</DescribeCnameReusesResponse>
```

`JSON` 格式

```
{
   "RequestId":"0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "CnameReuses":[{
     "Domain": "www.aliyun.com",
      "Cname":"4o6ep6q217k9****.aliyunddos0004.com",
      "Enable": 1
    }
   ]
```

```
}
```

错误码

访问错误中心查看更多错误码。

13.7.15 ModifyCnameReuse

调用ModifyCnameReuse为网站业务开启或关闭CNAME复用。

> **说明:**
> 该接口仅适用于DDoS高防（国际）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	ModifyCnameReuse	要执行的操作。取值：**ModifyCnameReuse**
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
Enable	Integer	是	1	是否开启CNAME复用。取值： • **1**：开启 • **2**：关闭
RegionId	String	否	ap-southeast-1	DDoS高防服务地域ID。取值：**ap-southeast-1**，表示DDoS高防（国际）服务。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

名称	类型	是否必选	示例值	描述
Cname	String	否	4o6ep6q217k9****.aliyunddos0004.com	要复用的CNAME值。

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=ModifyCnameReuse
&Domain=www.aliyun.com
&Enable=1
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

`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。

13.8 端口接入

13.8.1 DescribeNetworkRules

调用DescribeNetworkRules查询端口转发规则。

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	DescribeNetworkRules	要执行的操作。取值：**DescribeNetworkRules**
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明:** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
PageNumber	Integer	是	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写**1**。
PageSize	Integer	是	10	页面显示的记录数量。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ForwardProtocol	String	否	tcp	转发协议。取值： • **tcp** • **udp**
FrontendPort	Integer	否	80	转发端口。

返回数据

名称	类型	示例值	描述
NetworkRules	Array		端口转发规则信息。
BackendPort	Integer	80	源站端口。
FrontendPort	Integer	80	转发端口。
InstanceId	String	ddoscoo-cn-mp91j1ao****	DDoS高防实例ID。
IsAutoCreate	Boolean	true	是否自动创建。取值： • **true**：是 • **false**：否
Protocol	String	tcp	转发协议。取值： • **tcp** • **udp**
RealServers	List	["112.***.***.139"]	源站IP地址列表。
RequestId	String	8597F235-FA5E-4FC7-BAD9-E4C0B01BC771	本次请求的ID。
TotalCount	Long	2	端口转发规则总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeNetworkRules
&InstanceId=ddoscoo-cn-mp91j1ao****
&PageNumber=1
&PageSize=10
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeNetworkRulesResponse>
  <TotalCount>2</TotalCount>
  <NetworkRules>
    <IsAutoCreate>true</IsAutoCreate>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
```

```
    <BackendPort>80</BackendPort>
    <RealServers>112.***.***.139</RealServers>
    <FrontendPort>80</FrontendPort>
    <Protocol>tcp</Protocol>
  </NetworkRules>
  <NetworkRules>
    <IsAutoCreate>false</IsAutoCreate>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
    <BackendPort>8080</BackendPort>
    <RealServers>1.1.1.1</RealServers>
    <RealServers>2.2.2.2</RealServers>
    <RealServers>3.3.3.3</RealServers>
    <FrontendPort>8080</FrontendPort>
    <Protocol>tcp</Protocol>
  </NetworkRules>
  <RequestId>8597F235-FA5E-4FC7-BAD9-E4C0B01BC771</RequestId>
</DescribeNetworkRulesResponse>
```

JSON 格式

```
{
 "TotalCount": 2,
 "NetworkRules": [
  {
   "IsAutoCreate": true,
   "InstanceId": "ddoscoo-cn-mp91j1ao****",
   "BackendPort": 80,
   "RealServers": [
    "112.***.***.139"
   ],
   "FrontendPort": 80,
   "Protocol": "tcp"
  },
  {
   "IsAutoCreate": false,
   "InstanceId": "ddoscoo-cn-mp91j1ao****",
   "BackendPort": 8080,
   "RealServers": [
    "1.1.1.1",
    "2.2.2.2",
    "3.3.3.3"
   ],
   "FrontendPort": 8080,
   "Protocol": "tcp"
  }
 ],
 "RequestId": "8597F235-FA5E-4FC7-BAD9-E4C0B01BC771"
}
```

错误码

访问错误中心查看更多错误码。

13.8.2 CreateNetworkRules

调用CreateNetworkRules创建端口转发规则。

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	CreateNetworkRules	要执行的操作。取值：**CreateNetworkRules**
NetworkRules	String	是	[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort":8080,"BackendPort":8080,"RealServers":["1.1.1.1","2.2.2.2"]}]	端口转发规则的详细信息，使用JSON格式的字符串表述，具体结构如下。 • **InstanceId**：String类型，必选，DDoS高防实例ID。 • **Protocol**：String类型，必选，转发协议类型。取值：**tcp**、**udp**。 • **FrontendPort**：Integer类型，必选，转发端口。 • **BackendPort**：Integer类型，必选，源站端口。 • **RealServers**：JSON数组类型，必选，源站IP地址列表。最多支持20个IP地址。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	ADCA45A5-D15C-4B7D-9F81-138B0B36D0BD	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateNetworkRules
&NetworkRules=[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort
":8080,"BackendPort":8080,"RealServers":["1.1.1.1","2.2.2.2"]}]
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<CreateNetworkRulesResponse>
  <RequestId>ADCA45A5-D15C-4B7D-9F81-138B0B36D0BD</RequestId>
</CreateNetworkRulesResponse>
```

`JSON` 格式

```
{
 "RequestId": "ADCA45A5-D15C-4B7D-9F81-138B0B36D0BD"
}
```

错误码

访问错误中心查看更多错误码。

13.8.3 ConfigNetworkRules

调用ConfigNetworkRules编辑端口转发规则，修改源站IP地址。

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	ConfigNetworkRules	要执行的操作。取值：**ConfigNetworkRules**

名称	类型	是否必选	示例值	描述
NetworkRules	String	是	[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort":8080,"BackendPort":8080,"RealServers":["1.1.1.1","2.2.2.2","3.3.3.3"]}]	端口转发规则的详细信息，使用JSON格式的字符串表述，具体结构如下。 • **InstanceId**：String类型，必选，DDoS高防实例ID。 • **Protocol**：String类型，必选，转发协议类型。取值：**tcp**、**udp**。 • **FrontendPort**：Integer类型，必选，转发端口。 • **BackendPort**：Integer类型，必选，源站端口。 • **RealServers**：JSON数组类型，必选，源站IP地址列表。最多支持20个IP地址。 **说明:** 编辑端口转发规则时，只可以修改**RealServers**，即源站IP地址。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	CC042262-15A3-4A49-ADF0-130968EA47BC	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigNetworkRules
&NetworkRules=[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort":8080,"BackendPort":8080,"RealServers":["1.1.1.1","2.2.2.2","3.3.3.3"]}]
```

```
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ConfigNetworkRulesResponse>
  <RequestId>CC042262-15A3-4A49-ADF0-130968EA47BC</RequestId>
</ConfigNetworkRulesResponse>
```

JSON 格式

```
{
 "RequestId": "CC042262-15A3-4A49-ADF0-130968EA47BC"
}
```

错误码

访问错误中心查看更多错误码。

13.8.4 DeleteNetworkRule

调用DeleteNetworkRule删除端口转发规则。目前不支持批量删除，每次只允许删除一个对象。

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	DeleteNetworkRule	要执行的操作。取值：**DeleteNetworkRule**
NetworkRule	String	是	[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort":8080}]	要删除的端口转发规则，使用JSON格式的字符串表述，具体结构如下。 • **InstanceId**：String类型，必选，DDoS高防实例ID。 • **Protocol**：String类型，必选，转发协议类型。取值：**tcp**、**udp**。 • **FrontendPort**：Integer类型，必选，转发端口。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	49AD2F34-694A-4024-9B0E-DDCFC59CCC13	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteNetworkRule
&NetworkRule=[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort
":8080}]
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DeleteNetworkRuleResponse>
  <RequestId>49AD2F34-694A-4024-9B0E-DDCFC59CCC13</RequestId>
</DeleteNetworkRuleResponse>
```

JSON 格式

```
{
 "RequestId": "49AD2F34-694A-4024-9B0E-DDCFC59CCC13"
}
```

错误码

访问错误中心查看更多错误码。

13.8.5 DescribeHealthCheckList

调用DescribeHealthCheckList查询端口转发规则的健康检查配置（四层或七层）。

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	要执行的操作。取值：**DescribeHealthCheckList**
NetworkRules	String	是	[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort":8080}]	要查询的端口转发规则，使用JSON格式的字符串表述，具体结构如下。 • **InstanceId**：String类型，必选，DDoS高防实例ID。 • **Protocol**：String类型，必选，转发协议类型。取值：**tcp**、**udp**。 • **FrontendPort**：Integer类型，必选，转发端口。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
HealthCheckList	Array		健康检查配置列表。
FrontendPort	Integer	8080	转发端口。
HealthCheck	Struct		健康检查配置信息。

名称	类型	示例值	描述
Domain	String	www.aliyun.com	域名。 **说明:** 仅适用于七层健康检查。
Down	Integer	3	不健康阈值。取值范围：**1~10**。
Interval	Integer	15	检查间隔。取值范围：**1~30**，单位：秒。
Port	Integer	8080	检查端口。
Timeout	Integer	5	响应超时时间。取值范围：**1~30**，单位：秒。
Type	String	tcp	协议类型。取值： • **tcp**：四层 • **http**：七层
Up	Integer	3	健康阈值。取值范围：**1~10**。
Uri	String	/abc	检查路径。 **说明:** 仅适用于七层健康检查。
InstanceId	String	ddoscoo-cn-mp91j1ao****	DDoS高防实例ID。
Protocol	String	tcp	转发协议。取值： • **tcp** • **udp**
RequestId	String	83B4AF42-E8EE-4DC9-BD73-87B7733A36F9	本次请求的ID。
TotalCount	String	1	健康检查配置的总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeHealthCheckList
&NetworkRules=[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort
":8080}]
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeHealthCheckListResponse>
  <RequestId>83B4AF42-E8EE-4DC9-BD73-87B7733A36F9</RequestId>
  <HealthCheckList>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
    <FrontendPort>8080</FrontendPort>
    <HealthCheck>
      <Type>tcp</Type>
      <Down>3</Down>
      <Timeout>5</Timeout>
      <Port>8080</Port>
      <Up>3</Up>
      <Interval>15</Interval>
    </HealthCheck>
    <Protocol>tcp</Protocol>
  </HealthCheckList>
    <TotalCount>1</TotalCount>
</DescribeHealthCheckListResponse>
```

JSON 格式

```
{
   "RequestId": "83B4AF42-E8EE-4DC9-BD73-87B7733A36F9",
   "HealthCheckList": [
      {
         "InstanceId": "ddoscoo-cn-mp91j1ao****",
         "FrontendPort": 8080,
         "HealthCheck": {
            "Type": "tcp",
            "Down": 3,
            "Timeout": 5,
            "Port": 8080,
            "Up": 3,
            "Interval": 15
         },
         "Protocol": "tcp"
      }
   ],
   "TotalCount": 1
}
```

错误码

访问错误中心查看更多错误码。

13.8.6 ModifyHealthCheckConfig

调用ModifyHealthCheckConfig编辑端口转发规则的健康检查配置（四层或七层）。

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	ModifyHealthCheckConfig	要执行的操作。取值：**ModifyHealthCheckConfig**
ForwardProtocol	String	是	tcp	转发协议。取值： • **tcp** • **udp**
FrontendPort	Integer	是	8080	转发端口。

名称	类型	是否必选	示例值	描述
HealthCheck	String	是	{"Type":"tcp","Timeout":10,"Port":8080,"Interval":10,"Up":10,"Down":40}	健康检查配置的详细信息，使用JSON格式的字符串表述，具体结构如下。 • **Type**：String类型，必选，协议类型。取值：**tcp**（四层）、**http**（七层）。 • **Domain**：String类型，可选，域名。 **说明：** 仅适用于七层健康检查。 • **Uri**：String类型，可选，检查路径。 **说明：** 仅适用于七层健康检查。 • **Timeout**：Integer类型，可选，响应超时时间。取值范围：**1~30**，单位：秒。 • **Port**：Integer类型，可选，检查端口。 • **Interval**：Integer类型，可选，检查间隔。取值范围：**1~30**，单位：秒。 • **Up**：Integer类型，可选，健康阈值。取值范围：**1~10**。 • **Down**：Integer类型，可选，不健康阈值。取值范围：**1~10**。
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

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=ModifyHealthCheckConfig
&ForwardProtocol=tcp
&FrontendPort=8080
&HealthCheck={"Type":"tcp","Timeout":10,"Port":8080,"Interval":10,"Up":10,"Down":40}
&InstanceId=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

`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。

13.8.7 DescribeHealthCheckStatus

调用DescribeHealthCheckStatus查询源站健康检查状态信息。

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	DescribeHealthCheckStatus	要执行的操作。取值：**DescribeHealthCheckStatus**
NetworkRules	String	是	[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort":8080}]	要查询的端口转发规则，使用JSON格式的字符串表述，具体结构如下。 • **InstanceId**：String类型，必选，DDoS高防实例ID。 • **Protocol**：String类型，必选，转发协议类型。取值：**tcp**、**udp**。 • **FrontendPort**：Integer类型，必选，转发端口。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
HealthCheckStatus	Array		源站健康检查状态信息。
FrontendPort	Integer	8080	转发端口。
InstanceId	String	ddoscoo-cn-mp91j1ao****	DDoS高防实例ID。

名称	类型	示例值	描述
Protocol	String	tcp	转发协议。取值： • **tcp** • **udp**
RealServer StatusList	Array		源站IP地址健康检查状态列表。
Address	String	1.1.1.1	源站IP地址。
Status	String	abnormal	当前IP地址健康检查状态。取值： • **normal**：健康 • **abnormal**：不健康
Status	String	normal	源站健康检查状态。取值： • **normal**：健康 • **abnormal**：不健康
RequestId	String	DE9FF9E1-569C-4B6C-AB6A-0F6D927BB27C	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeHealthCheckStatus
&NetworkRules=[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort
":8080}]
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeHealthCheckStatusResponse>
  <RequestId>DE9FF9E1-569C-4B6C-AB6A-0F6D927BB27C</RequestId>
  <HealthCheckStatus>
    <Status>abnormal</Status>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
    <FrontendPort>8080</FrontendPort>
    <RealServerStatusList>
      <Status>abnormal</Status>
      <Address>1.1.1.1</Address>
    </RealServerStatusList>
    <RealServerStatusList>
      <Status>abnormal</Status>
      <Address>2.2.2.2</Address>
    </RealServerStatusList>
```

```
    <RealServerStatusList>
      <Status>abnormal</Status>
      <Address>3.3.3.3</Address>
    </RealServerStatusList>
    <Protocol>tcp</Protocol>
  </HealthCheckStatus>
</DescribeHealthCheckStatusResponse>
```

JSON 格式

```
{
 "RequestId": "DE9FF9E1-569C-4B6C-AB6A-0F6D927BB27C",
 "HealthCheckStatus": [
  {
   "Status": "abnormal",
   "InstanceId": "ddoscoo-cn-mp91j1ao****",
   "FrontendPort": 8080,
   "RealServerStatusList": [
    {
     "Status": "abnormal",
     "Address": "1.1.1.1"
    },
    {
     "Status": "abnormal",
     "Address": "2.2.2.2"
    },
    {
     "Status": "abnormal",
     "Address": "3.3.3.3"
    }
   ],
   "Protocol": "tcp"
  }
 ]
}
```

错误码

访问错误中心查看更多错误码。

13.9 流量调度器

13.9.1 DescribeSchedulerRules

调用DescribeSchedulerRules查询流量调度器的调度规则。

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	DescribeSchedulerRules	要执行的操作。取值：**DescribeSchedulerRules**
PageSize	Integer	是	10	页面显示的记录数量。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属的地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
RuleName	String	否	testrule	规则名称。
PageNumber	Integer	否	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写**1**。

返回数据

名称	类型	示例值	描述
RequestId	String	11C55595-1757-4B17-9ACE-4ACB68C2D989	本次请求的ID。
SchedulerRules	Array		流量调度规则信息。
Cname	String	4eru5229a843****.aliyunddos0001.com	CNAME值。
RuleName	String	doctest	规则名称。

名称	类型	示例值	描述
RuleType	String	6	规则类型。取值： • **2**：阶梯防护 • **3**：出海加速 • **5**：CDN联动 • **6**：云产品联动
Rules	Array		规则列表。
Priority	Integer	100	规则优先级。
RegionId	Integer	1	地域ID。 **说明：** 仅在阶梯防护规则（**RuleType**为**2**）中返回。
Status	Integer	0	规则生效状态。取值： • **0**：未生效 • **1**：生效
Type	String	A	资源地址的格式。取值： • **A**：IPv4地址 • **CNAME**：CNAME地址
Value	String	203.***.***.39	资源地址。
ValueType	Integer	1	资源地址类型。取值： • **1**：DDoS高防IP • **2**：（阶梯防护）云资源IP • **3**：（出海加速）加速线路IP • **5**：（CDN联动）加速域名 • **6**：（云产品联动）云资源IP
TotalCount	String	1	流量调度规则的总数。

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribeSchedulerRulesResponse>
  <TotalCount>1</TotalCount>
  <RequestId>11C55595-1757-4B17-9ACE-4ACB68C2D989</RequestId>
  <SchedulerRules>
    <RuleType>6</RuleType>
    <Cname>4eru5229a843****.aliyunddos0001.com</Cname>
    <Rules>
      <Status>0</Status>
      <Type>A</Type>
      <ValueType>1</ValueType>
      <Priority>100</Priority>
      <Value>203.***.***.39</Value>
      <RegionId></RegionId>
    </Rules>
    <Rules>
      <Status>1</Status>
      <Type>A</Type>
      <ValueType>6</ValueType>
      <Priority>50</Priority>
      <Value>47.***.***.47</Value>
      <RegionId>cn-hangzhou</RegionId>
    </Rules>
    <RuleName>doctest</RuleName>
  </SchedulerRules>
</DescribeSchedulerRulesResponse>
```

JSON 格式

```
{
 "TotalCount": 1,
 "RequestId": "11C55595-1757-4B17-9ACE-4ACB68C2D989",
 "SchedulerRules": [
  {
   "RuleType": 6,
   "Cname": "4eru5229a843****.aliyunddos0001.com",
   "Rules": [
    {
     "Status": 0,
     "Type": "A",
     "ValueType": 1,
     "Priority": 100,
     "Value": "203.***.***.39",
     "RegionId": ""
    },
    {
     "Status": 1,
     "Type": "A",
     "ValueType": 6,
```

```
    "Priority": 50,
    "Value": "47.***.***.47",
    "RegionId": "cn-hangzhou"
   }
  ],
  "RuleName": "doctest"
 }
]
}
```


错误码

访问错误中心查看更多错误码。

13.9.2 CreateSchedulerRule

调用CreateSchedulerRule创建流量调度器调度规则。

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	CreateSchedulerRule	要执行的操作。取值：**CreateSchedulerRule**
RuleName	String	是	testrule	规则名称。

名称	类型	是否必选	示例值	描述
Rules	String	是	[{"Type":"A", "Value":"1.1.1.1", "Priority":80,"ValueType":2, "RegionId":"cn-hangzhou" },{"Type":"A", "Value":"203.***.***.199", "Priority":80,"ValueType":1}]	通用联动规则的详细信息，使用JSON格式的字符串表述，具体结构如下。 • **Type**：String类型，必选，联动资源的地址格式。取值： - **A**：IP地址 - **CNAME**：域名 • **Value**：String类型，必选，联动资源的地址。 • **Priority**：Integer类型，必选，规则优先级。取值范围：**0**~**100**，取值越大，优先级越高。 • **ValueType**：Integer类型，必选，联动资源的类型。取值： - **1**：DDoS高防IP - **2**：（阶梯防护）云资源IP - **3**：（出海加速）加速线路IP - **5**：（CDN联动）加速域名 - **6**：（云产品联动）云资源IP • **RegionId**：String类型，可选（**ValueType**为**2**时必选），地域ID。
RuleType	Integer	是	2	规则类型。取值： • **2**：阶梯防护 • **3**：出海加速 • **5**：CDN联动 • **6**：云产品联动
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

名称	类型	是否必选	示例值	描述
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
Param	String	否	{"ParamType":"cdn","ParamData":{"Domain":"cdn.test.com","Cname":"cdncname.test.com","AccessQps":100,"UpstreamQps":100}}	CDN联动规则的详细信息，使用JSON格式的字符串表达，具体结构如下。 • **ParamType**：必选，String类型，CDN联动类型。取值：**cdn**，表示CDN联动。 • **ParamData**：必选，Map类型，CDN联动参数。具体结构如下。 - **Domain**：必选，String类型，CDN加速域名。 - **Cname**：必选，String类型，加速域名CNAME地址。 - **AccessQps**：必选，Integer类型，访问QPS阈值。超过阈值切换到DDoS高防。 - **UpstreamQps**：可选，Integer类型，回源QPS阈值。低于阈值切换到CDN。

返回数据

名称	类型	示例值	描述
Cname	String	48k7b372gpl4****.aliyunddos0001.com	规则对应的流量调度器CNAME值。 **说明：** 您必须将业务解析到流量调度器的CNAME，才能启用规则。
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。
RuleName	String	testrule	规则名称。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateSchedulerRule
&RuleName=testrule
&Rules=[{"Type":"A", "Value":"1.1.1.1", "Priority":80,"ValueType":2, "RegionId":"cn-
hangzhou" },{"Type":"A", "Value":"203.***.***.199", "Priority":80,"ValueType":1}]
&RuleType=2
&<公共请求参数>
```

正常返回示例

XML 格式

```
<CreateSchedulerRuleResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
    <Cname>48k7b372gpl4****.aliyunddos0001.com</Cname>
    <RuleName>testrule</RuleName>
</CreateSchedulerRuleResponse>
```

JSON 格式

```
{
   "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "Cname": "48k7b372gpl4****.aliyunddos0001.com",
   "RuleName": "testrule"
}
```

错误码

访问错误中心查看更多错误码。

13.9.3 ModifySchedulerRule

调用ModifySchedulerRule编辑流量调度器调度规则。

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	ModifyScheduler Rule	要执行的操作。取值：**ModifySchedulerRule**
RuleName	String	是	testrule	要编辑的规则名称。

名称	类型	是否必选	示例值	描述
Rules	String	是	[{"Type":"A", "Value":"1.1.1.1", "Priority":80,"ValueType":2, "RegionId":"cn-hangzhou" },{"Type":"A", "Value":"203.***.***.199", "Priority":80,"ValueType":1}]	通用联动规则的详细信息，使用JSON格式的字符串表述，具体结构如下。 • **Type**：String类型，必选，联动资源的地址格式。取值： - **A**：IP地址 - **CNAME**：域名 • **Value**：String类型，必选，联动资源的地址。 • **Priority**：Integer类型，必选，规则优先级。取值范围：**0**~**100**，取值越大，优先级越高。 • **ValueType**：Integer类型，必选，联动资源的类型。取值： - **1**：DDoS高防IP - **2**：（阶梯防护）云资源IP - **3**：（出海加速）加速线路IP - **5**：（CDN联动）加速域名 - **6**：（云产品联动）云资源IP • **RegionId**：String类型，可选（**ValueType**为**2**时必选），地域ID。
RuleType	Integer	是	2	规则类型。取值： • **2**：阶梯防护 • **3**：出海加速 • **5**：CDN联动 • **6**：云产品联动
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

名称	类型	是否必选	示例值	描述
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
Param	String	否	{"ParamType":"cdn","ParamData":{"Domain":"cdn.test.com","Cname":"cdncname.test.com","AccessQps":100,"UpstreamQps":100}}	CDN联动规则的详细信息，使用JSON格式的字符串表达，具体结构如下。 • **ParamType**：必选，String类型，CDN联动类型。取值：**cdn**，表示CDN联动。 • **ParamData**：必选，Map类型，CDN联动参数。具体结构如下。 - **Domain**：必选，String类型，CDN加速域名。 - **Cname**：必选，String类型，加速域名CNAME地址。 - **AccessQps**：必选，Integer类型，访问QPS阈值。超过阈值切换到DDoS高防。 - **UpstreamQps**：可选，Integer类型，回源QPS阈值。低于阈值切换到CDN。

返回数据

名称	类型	示例值	描述
Cname	String	48k7b372gpl4****.aliyunddos0001.com	规则对应的流量调度器CNAME值。 **说明：** 您必须将业务解析到流量调度器的CNAME，才能启用规则。
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。
RuleName	String	testrule	规则名称。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifySchedulerRule
&RuleName=testrule
&Rules=[{"Type":"A", "Value":"1.1.1.1", "Priority":80,"ValueType":2, "RegionId":"cn-hangzhou" },{"Type":"A", "Value":"203.***.***.199", "Priority":80,"ValueType":1}]
&RuleType=2
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ModifySchedulerRuleResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
    <Cname>48k7b372gpl4****.aliyunddos0001.com</Cname>
    <RuleName>testrule</RuleName>
</ModifySchedulerRuleResponse>
```

JSON 格式

```
{
   "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "Cname": "48k7b372gpl4****.aliyunddos0001.com",
   "RuleName": "testrule"
}
```

错误码

访问错误中心查看更多错误码。

13.9.4 DeleteSchedulerRule

调用DeleteSchedulerRule删除流量调度器调度规则。

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	DeleteSchedulerRule	要执行的操作。取值：**DeleteSchedulerRule**
RuleName	String	是	testrule	要删除的规则名称。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=DeleteSchedulerRule
&RuleName=testrule
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.10 基础设施防护策略

13.10.1 DescribeAutoCcListCount

调用DescribeAutoCcListCount查询针对DDoS高防实例的黑名单和白名单IP的数量。

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	DescribeAutoCcListCount	要执行的操作。取值：**DescribeAutoCcListCount**
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明：** 您可以调用**DescribeInstanceIds**查询所有DDoS高防实例的ID信息。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
QueryType	String	否	manual	要查询的黑白名单IP的来源。取值： • **manual**：手动添加 • **auto**：自动添加

返回数据

名称	类型	示例值	描述
BlackCount	Integer	0	黑名单IP的数量。
RequestId	String	5AC3785F-C789-4622-87A4-F58BE7F6B184	本次请求的ID。

名称	类型	示例值	描述
WhiteCount	Integer	2	白名单IP的数量。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeAutoCcListCount
&InstanceId=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeAutoCcListCountResponse>
  <BlackCount>0</BlackCount>
  <RequestId>5AC3785F-C789-4622-87A4-F58BE7F6B184</RequestId>
  <WhiteCount>2</WhiteCount>
</DescribeAutoCcListCountResponse>
```

`JSON` 格式

```
{
 "BlackCount": 0,
 "RequestId": "5AC3785F-C789-4622-87A4-F58BE7F6B184",
 "WhiteCount": 2
}
```

错误码

访问错误中心查看更多错误码。

13.10.2 DescribeAutoCcBlacklist

调用DescribeAutoCcBlacklist查询针对DDoS高防实例的黑名单IP。

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	DescribeAutoCcBlacklist	要执行的操作。取值：**DescribeAutoCcBlacklist**

名称	类型	是否必选	示例值	描述
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。  **说明:** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
PageNumber	Integer	是	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写**1**。
PageSize	Integer	是	10	页面显示的记录数量。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
KeyWord	String	否	138	使用源IP关键字查询，指定要查询的源IP的前缀。  **说明:** 必须大于3个字符。

返回数据

名称	类型	示例值	描述
AutoCcBlacklist	Array		针对DDoS高防实例的黑名单IP列表。
DestIp	String	203.***.***.132	DDoS高防实例的IP。
EndTime	Long	1584093569	黑名单IP的失效时间。时间戳格式，单位：秒。
SourceIp	String	1.1.1.1	黑名单IP。

名称	类型	示例值	描述
Type	String	manual	黑名单IP的来源。取值： • **manual**：手动添加 • **auto**：自动添加
RequestId	String	E78C8472-0B15-42D5-AF22-A32A78818AB2	本次请求的ID。
TotalCount	Long	2	黑名单IP的总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeAutoCcBlacklist
&InstanceId=ddoscoo-cn-mp91j1ao****
&PageNumber=1
&PageSize=10
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeAutoCcBlacklistResponse>
  <TotalCount>2</TotalCount>
  <RequestId>E78C8472-0B15-42D5-AF22-A32A78818AB2</RequestId>
  <AutoCcBlacklist>
    <Type>manual</Type>
    <SourceIp>1.1.1.1</SourceIp>
    <EndTime>1584093569</EndTime>
    <DestIp>203.***.***.132</DestIp>
  </AutoCcBlacklist>
  <AutoCcBlacklist>
    <Type>manual</Type>
    <SourceIp>2.2.2.2</SourceIp>
    <EndTime>1584093569</EndTime>
    <DestIp>203.***.***.132</DestIp>
  </AutoCcBlacklist>
</DescribeAutoCcBlacklistResponse>
```

JSON 格式

```
{
 "TotalCount": 2,
 "RequestId": "E78C8472-0B15-42D5-AF22-A32A78818AB2",
 "AutoCcBlacklist": [
  {
   "Type": "manual",
   "SourceIp": "1.1.1.1",
   "EndTime": "1584093569",
   "DestIp": "203.***.***.132"
```

```
  },
  {
   "Type": "manual",
   "SourceIp": "2.2.2.2",
   "EndTime": "1584093569",
   "DestIp": "203.***.***.132"
  }
 ]
}
```

错误码

访问错误中心查看更多错误码。

13.10.3 AddAutoCcBlacklist

调用AddAutoCcBlacklist添加针对DDoS高防实例的黑名单IP。

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	AddAutoCcBlacklist	要执行的操作。取值：**AddAutoCcBlacklist**
Blacklist	String	是	[{"src":"1.1.1.1"},{"src":"2.2.2.2"}]	黑名单IP的详细信息，使用JSON格式的字符串表述，具体结构如下。 • **src**：String类型，必选，黑名单IP。
ExpireTime	Integer	是	300	过期时间。取值范围：**300~7200**，单位：秒。
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明：** 您可以调用**DescribeInstanceIds**查询所有DDoS高防实例的ID信息。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=AddAutoCcBlacklist
&Blacklist=[{"src":"1.1.1.1"},{"src":"2.2.2.2"}]
&ExpireTime=300
&InstanceId=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

XML 格式

```
<AddAutoCcBlacklistResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</AddAutoCcBlacklistResponse>
```

JSON 格式

```
{
 "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

访问错误中心查看更多错误码。

13.10.4 DeleteAutoCcBlacklist

调用DeleteAutoCcBlacklist删除针对DDoS高防实例的黑名单IP。

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	DeleteAutoCcBlacklist	要执行的操作。取值：**DeleteAutoCcBlacklist**
Blacklist	String	是	[{"src":"1.1.1.1"},{"src":"2.2.2.2"}]	黑名单IP的详细信息，使用JSON格式的字符串表述，具体结构如下。 • **src**：String类型，必选，黑名单IP。
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteAutoCcBlacklist
&Blacklist=[{"src":"1.1.1.1"},{"src":"2.2.2.2"}]
&InstanceId=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DeleteAutoCcBlacklistResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</DeleteAutoCcBlacklistResponse>
```

JSON 格式

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

访问错误中心查看更多错误码。

13.10.5 EmptyAutoCcBlacklist

调用EmptyAutoCcBlacklist清空针对DDoS高防实例的黑名单IP。

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	EmptyAutoCcBlacklist	要执行的操作。取值：**EmptyAutoCcBlacklist**
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=EmptyAutoCcBlacklist
&InstanceId=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<EmptyAutoCcBlacklistResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</EmptyAutoCcBlacklistResponse>
```

`JSON` 格式

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

访问错误中心查看更多错误码。

13.10.6 DescribeAutoCcWhitelist

调用DescribeAutoCcWhitelist查询针对DDoS高防实例的白名单IP。

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	DescribeAutoCcWhitelist	要执行的操作。取值：**DescribeAutoCcWhitelist**
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明:** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
PageNumber	Integer	是	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写**1**。
PageSize	Integer	是	10	页面显示的记录数量。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
KeyWord	String	否	138	使用源IP关键字查询，指定要查询的源IP的前缀。 **说明:** 必须大于3个字符。

返回数据

名称	类型	示例值	描述
AutoCcWhitelist	Array		针对DDoS高防实例的白名单IP列表。
DestIp	String	203.***.***.117	DDoS高防实例的IP。
EndTime	Long	0	白名单IP的失效时间，单位：秒。**0**表示永久生效。
SourceIp	String	2.2.2.2	白名单IP。
Type	String	manual	白名单IP类型。取值： • **manual**：手动添加 • **auto**：自动添加
RequestId	String	F09D085E-5E0F-4FF2-B32E-F4A644049162	本次请求的ID。
TotalCount	Long	2	白名单IP的总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeAutoCcWhitelist
&InstanceId=ddoscoo-cn-mp91j1ao****
&PageNumber=1
&PageSize=10
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeAutoCcWhitelistResponse>
  <AutoCcWhitelist>
    <Type>manual</Type>
    <SourceIp>4.4.4.4</SourceIp>
    <EndTime>0</EndTime>
    <DestIp>203.***.***.117</DestIp>
  </AutoCcWhitelist>
  <AutoCcWhitelist>
    <Type>manual</Type>
    <SourceIp>2.2.2.2</SourceIp>
    <EndTime>0</EndTime>
    <DestIp>203.***.***.117</DestIp>
  </AutoCcWhitelist>
```

```
  <TotalCount>2</TotalCount>
  <RequestId>F09D085E-5E0F-4FF2-B32E-F4A644049162</RequestId>
</DescribeAutoCcWhitelistResponse>
```

JSON 格式

```
{
 "AutoCcWhitelist": [
  {
   "Type": "manual",
   "SourceIp": "4.4.4.4",
   "EndTime": "0",
   "DestIp": "203.***.***.117"
  },
  {
   "Type": "manual",
   "SourceIp": "2.2.2.2",
   "EndTime": "0",
   "DestIp": "203.***.***.117"
  }
 ],
 "TotalCount": 2,
 "RequestId": "F09D085E-5E0F-4FF2-B32E-F4A644049162"
}
```

错误码

访问错误中心查看更多错误码。

13.10.7 AddAutoCcWhitelist

调用AddAutoCcWhitelist添加针对DDoS高防实例的白名单IP。

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	AddAutoCcWhitelist	要执行的操作。取值： **AddAutoCcWhitelist**
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。

名称	类型	是否必选	示例值	描述
Whitelist	String	是	[{"src":"1.1.1.1"},{"src":"2.2.2.2"}]	白名单IP的详细信息，使用JSON格式的字符串表述，具体结构如下。 • **src：String**类型，必选，白名单IP。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ExpireTime	Integer	否	3600	白名单IP有效时间，单位：秒。**0**表示永久生效。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=AddAutoCcWhitelist
&InstanceId=ddoscoo-cn-mp91j1ao****
&Whitelist=[{"src":"1.1.1.1"},{"src":"2.2.2.2"}]
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<AddAutoCcWhitelistResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</AddAutoCcWhitelistResponse>
```

`JSON` 格式

```
{
 "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
```

```
}
```

错误码

访问错误中心查看更多错误码。

13.10.8 DeleteAutoCcWhitelist

调用DeleteAutoCcWhitelist删除针对DDoS高防实例的白名单IP。

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	DeleteAutoCcWhitelist	要执行的操作。取值：**DeleteAutoCcWhitelist**
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
Whitelist	String	是	[{"src":"1.1.1.1"},{"src":"2.2.2.2"}]	白名单IP的详细信息，使用JSON格式的字符串表述，具体结构如下。 • **src：String**类型，必选，白名单IP。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteAutoCcWhitelist
&InstanceId=ddoscoo-cn-mp91j1ao****
&Whitelist=[{"src":"1.1.1.1"},{"src":"2.2.2.2"}]
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DeleteAutoCcWhitelistResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</DeleteAutoCcWhitelistResponse>
```

`JSON` 格式

```
{
 "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

访问错误中心查看更多错误码。

13.10.9 EmptyAutoCcWhitelist

调用EmptyAutoCcWhitelist清空针对DDoS高防实例的白名单IP。

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	EmptyAutoCcWhitelist	要执行的操作。取值：**EmptyAutoCcWhitelist**

名称	类型	是否必选	示例值	描述
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。  **说明:** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值: • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=EmptyAutoCcWhitelist
&InstanceId=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<EmptyAutoCcWhitelistResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</EmptyAutoCcWhitelistResponse>
```

`JSON` 格式

```
{
 "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

访问错误中心查看更多错误码。

13.10.10 DescribeUnBlackholeCount

调用DescribeUnBlackholeCount查询黑洞解封次数。

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	DescribeUnBlackholeCount	要执行的操作。取值：**DescribeUnBlackholeCount**
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
RemainCount	Integer	5	剩余的黑洞解封次数。
RequestId	String	232929FA-40B6-4C53-9476-EE335ABA44CD	本次请求的ID。
TotalCount	Integer	5	黑洞解封总次数。

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribeUnBlackholeCountResponse>
  <TotalCount>5</TotalCount>
  <RequestId>232929FA-40B6-4C53-9476-EE335ABA44CD</RequestId>
  <RemainCount>5</RemainCount>
</DescribeUnBlackholeCountResponse>
```

JSON 格式

```
{
 "TotalCount": 5,
 "RequestId": "232929FA-40B6-4C53-9476-EE335ABA44CD",
 "RemainCount": 5
}
```

错误码

访问错误中心查看更多错误码。

13.10.11 DescribeBlackholeStatus

调用DescribeBlackholeStatus查询DDoS高防实例的黑洞状态。

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	DescribeBlackholeStatus	要执行的操作。取值：**DescribeBlackholeStatus**
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明:** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
BlackholeStatus	Array		DDoS高防实例的黑洞状态信息。
BlackStatus	String	blackhole	黑洞状态。取值： • **blackhole**：黑洞中 • **normal**：正常
EndTime	Long	1540196323	黑洞结束时间。时间戳格式，单位：秒。
Ip	String	203.***.***.132	DDoS高防实例的IP。
StartTime	Long	1540195323	黑洞开始时间。时间戳格式，单位：秒。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeBlackholeStatus
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeBlackholeStatusResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <BlackholeStatus>
    <Ip>203.***.***.132</Ip>
    <BlackStatus>blackhole</BlackStatus>
    <StartTime>1540195323</StartTime>
    <EndTime>1540196323</EndTime>
  </BlackholeStatus>
</DescribeBlackholeStatusResponse>
```

`JSON` 格式

```
{
   "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
   "BlackholeStatus": [
      {
         "Ip": "203.***.***.132",
         "BlackStatus": "blackhole",
         "StartTime": 1540195323,
```

```
        "EndTime": 1540196323
      }
    ]
}
```

错误码

访问错误中心查看更多错误码。

13.10.12 ModifyBlackholeStatus

调用ModifyBlackholeStatus执行黑洞解封。

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	ModifyBlackholeStatus	要执行的操作。取值：**ModifyBlackholeStatus**
BlackholeStatus	String	是	undo	设置黑洞状态。取值：**undo**，表示解除黑洞。
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明:** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyBlackholeStatus
&BlackholeStatus=undo
&InstanceId=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ModifyPortAutoCcStatusResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</ModifyPortAutoCcStatusResponse>
```

JSON 格式

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

访问错误中心查看更多错误码。

13.10.13 DescribeNetworkRegionBlock

调用DescribeNetworkRegionBlock查询针对DDoS高防实例的区域封禁配置。

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	DescribeNetworkRegionBlock	要执行的操作。取值：**DescribeNetworkRegionBlock**。
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明:** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
Config	Struct		区域封禁的配置信息。
Countries	List	[1,2]	被封禁的海外地区代码列表。 **说明：** 关于海外地区代码的详细信息，请参见中国和海外地区代码中的**海外地区代码**说明。 例如，[1,2]表示中国和澳大利亚。
Provinces	List	[11,12]	被封禁的中国地区代码列表。 **说明：** 关于中国地区代码的详细信息，请参见中国和海外地区代码中的**中国地区代码**说明。 例如，[11,12]表示北京市和天津市。
RegionBlockSwitch	String	on	区域封禁的开关状态。取值： • **on**：开启 • **off**：关闭
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeNetworkRegionBlock
&InstanceId=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeNetworkRegionBlockResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <Config>
    <RegionBlockSwitch>off</RegionBlockSwitch>
    <Countries>1</Countries>
    <Countries>2</Countries>
    <Provinces>11</Provinces>
    <Provinces>12</Provinces>
  </Config>
</DescribeNetworkRegionBlockResponse>
```

JSON 格式

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "Config": {
    "RegionBlockSwitch": "off",
    "Countries": [
      1,
      2
    ],
    "Provinces": [
      11,
      12
    ]
  }
}
```

错误码

访问错误中心查看更多错误码。

13.10.14 ConfigNetworkRegionBlock

调用ConfigNetworkRegionBlock设置针对DDoS高防实例的区域封禁。

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	ConfigNetworkRegionBlock	要执行的操作。取值：**ConfigNetworkRegionBlock**。
Config	String	是	{"RegionBlockSwitch":"off","Countries":[],"Provinces":[11,12,13,14,15,21,22,23,31,32,33,34,35,36,37,41,42,43,44,45,46,50,51,52,53,54,61,62,63,64,65,71,81,82]}	区域封禁的配置信息，使用JSON格式的字符串表述，具体结构如下。 • **RegionBlockSwitch**：String类型，必选，区域封禁的开关状态。取值： - **on**：开启 - **off**：关闭 • **Countries**：Array类型，可选，要封禁的海外地区代码列表。 **说明：** 关于海外地区代码的详细信息，请参见中国和海外地区代码中的**海外地区代码**说明。 例如，[1,2]表示中国和澳大利亚。 • **Provinces**：Array类型，可选，要封禁的中国地区代码列表。 **说明：** 关于中国地区代码的详细信息，请参见中国和海外地区代码中的**中国地区代码**说明。 例如，[11,12]表示北京市和天津市。

名称	类型	是否必选	示例值	描述
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。  **说明:** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值: • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigNetworkRegionBlock
&Config={"RegionBlockSwitch":"off","Countries":[],"Provinces":[11,12,13,14,15,21,22,23,31
,32,33,34,35,36,37,41,42,43,44,45,46,50,51,52,53,54,61,62,63,64,65,71,81,82]}
&InstanceId=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ConfigNetworkRegionBlockResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</ConfigNetworkRegionBlockResponse>
```

JSON 格式

```
{
 "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

访问错误中心查看更多错误码。

13.10.15 DescribeBlockStatus

调用DescribeBlockStatus查询DDoS高防（新BGP）实例的近源流量压制配置。

> **说明：**
> 该接口仅适用于DDoS高防（新BGP）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	DescribeBlockStatus	要执行的操作。取值：**DescribeBlockStatus**
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值：**cn-hangzhou**，表示DDoS高防（新BGP）服务。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
StatusList	Array		DDoS高防实例的近源流量压制配置。

名称	类型	示例值	描述
BlockStatusList	Array		近源流量压制配置。
BlockStatus	String	areablock	流量封禁状态。取值： • **areablock**：封禁中 • **normal**：正常
EndTime	Long	1540196323	封禁结束时间。时间戳格式，单位：秒。
Line	String	cut	封禁区域。取值： • **ct**：电信海外 • **cut**：联通海外
StartTime	Long	1540195323	封禁开始时间。时间戳格式，单位：秒。
Ip	String	203.***.***.88	DDoS高防实例的IP。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeBlockStatus
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeBlockStatusResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <StatusList>
    <Ip>203.***.***.88</Ip>
    <BlockStatusList>
      <BlockStatus>areablock</BlockStatus>
      <Line>cut</Line>
      <StartTime>1540195323</StartTime>
      <EndTime>1540196323</EndTime>
    </BlockStatusList>
  </StatusList>
</DescribeBlockStatusResponse>
```

JSON 格式

```
{
   "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
   "StatusList": [
      {
```

```
        "Ip": "203.***.***.88",
        "BlockStatusList": [
          {
            "BlockStatus": "areablock",
            "Line": "cut",
            "StartTime": 1540195323,
            "EndTime": 1540196323
          }
        ]
      }
    ]
}
```

错误码

访问错误中心查看更多错误码。

13.10.16 ModifyBlockStatus

调用ModifyBlockStatus设置DDoS高防（新BGP）实例的近源流量压制。

> **说明:**
> 该接口仅适用于DDoS高防（新BGP）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	ModifyBlockStatus	要执行的操作。取值：**ModifyBlockStatus**。
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明:** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
Status	String	是	do	近源流量压制的状态。取值： • **do**：开启流量压制 • **undo**：解除流量压制

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值：**cn-hangzhou**，表示DDoS高防（新BGP）服务。
Duration	Integer	否	10	封禁时间。取值范围：**5~43200**，单位：分钟。  **说明：** **Status**为**do**时必须传入该参数。
Lines.N	RepeatList	否	ct	封禁线路。取值： • **ct**：电信海外 • **cut**：联通海外

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyBlockStatus
&InstanceId=ddoscoo-cn-mp91j1ao****
&Status=do
&Duration=10
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<ModifyBlockStatusResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</ModifyBlockStatusResponse>
```

`JSON` 格式

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
```

```
}
```

错误码

访问错误中心查看更多错误码。

13.10.17 DescribeUnBlockCount

调用DescribeUnBlockCount查询可用的近源流量压制次数。

说明:

该接口仅适用于DDoS高防（新BGP）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	DescribeUnBlockCount	要执行的操作。取值：**DescribeUnBlockCount**
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值：**cn-hangzhou**，表示DDoS高防（新BGP）服务。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
RemainCount	Integer	7	剩余可用的近源流量压制次数。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
TotalCount	Integer	10	总共可用的近源流量压制次数。

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribeUnBlockCountResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <TotalCount>10</TotalCount>
  <RemainCount>7</RemainCount>
</DescribeUnBlockCountResponse>
```

JSON 格式

```
{
   "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
   "TotalCount": 10,
   "RemainCount": 7
}
```

错误码

访问错误中心查看更多错误码。

13.11 网站业务防护策略

13.11.1 DescribeWebCcProtectSwitch

调用DescribeWebCcProtectSwitch查询网站业务各防护功能的开关状态。

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	DescribeWebCcProtectSwitch	要执行的操作。取值：**DescribeWebCcProtectSwitch**

名称	类型	是否必选	示例值	描述
Domains.N	RepeatList	是	www.aliyun.com	网站业务的域名。 **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值: • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
ProtectSwitchList	Array		网站业务各防护功能的开关状态。
AiMode	String	defense	AI智能防护的模式。取值: • **watch**：预警模式 • **defense**：防护模式
AiRuleEnable	Integer	1	AI智能防护的开关状态。取值: • **0**：关闭 • **1**：开启
AiTemplate	String	level60	AI智能防护的等级。取值: • **level30**：宽松 • **level60**：正常 • **level90**：严格

名称	类型	示例值	描述
BlackWhiteListEnable	Integer	1	黑白名单（针对域名）的开关状态。取值： • **0**：关闭 • **1**：开启
CcCustomRuleEnable	Integer	0	自定义频率控制防护（CC防护）的开关状态。取值： • **0**：关闭 • **1**：开启
CcEnable	Integer	1	频率控制防护（CC防护）的开关状态。取值： • **0**：关闭 • **1**：开启
CcTemplate	String	default	频率控制防护（CC防护）的模式。取值： • **default**：正常 • **gf_under_attack**：攻击紧急 • **gf_sos_verify**：严格 • **gf_sos_enhance**：超级严格
Domain	String	www.aliyun.com	网站域名。
PreciseRuleEnable	Integer	0	精确访问控制的开关状态。取值： • **0**：关闭 • **1**：开启
RegionBlockEnable	Integer	0	区域封禁（针对域名）的开关状态。取值： • **0**：关闭 • **1**：开启
RequestId	String	3ADD9EED-CA4B-488C-BC82-01B0B899363D	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeWebCcProtectSwitch
&Domains.1=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeWebCcProtectSwitchResponse>
  <RequestId>3ADD9EED-CA4B-488C-BC82-01B0B899363D</RequestId>
  <ProtectSwitchList>
    <CcEnable>1</CcEnable>
    <BlackWhiteListEnable>1</BlackWhiteListEnable>
    <AiRuleEnable>1</AiRuleEnable>
    <CcCustomRuleEnable>0</CcCustomRuleEnable>
    <PreciseRuleEnable>0</PreciseRuleEnable>
    <Domain>www.aliyun.com</Domain>
    <AiMode>defense</AiMode>
    <RegionBlockEnable>0</RegionBlockEnable>
    <CcTemplate>default</CcTemplate>
    <AiTemplate>level60</AiTemplate>
  </ProtectSwitchList>
</DescribeWebCcProtectSwitchResponse>
```

JSON 格式

```
{
 "RequestId": "3ADD9EED-CA4B-488C-BC82-01B0B899363D",
 "ProtectSwitchList": [
  {
   "CcEnable": 1,
   "BlackWhiteListEnable": 1,
   "AiRuleEnable": 1,
   "CcCustomRuleEnable": 0,
   "PreciseRuleEnable": 0,
   "Domain": "www.aliyun.com",
   "AiMode": "defense",
   "RegionBlockEnable": 0,
   "CcTemplate": "default",
   "AiTemplate": "level60"
  }
 ]
}
```

错误码

访问错误中心查看更多错误码。

13.11.2 ModifyWebAIProtectSwitch

调用ModifyWebAIProtectSwitch设置网站业务AI智能防护的开关状态。

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	ModifyWebAIProtectSwitch	要执行的操作。取值：**ModifyWebAIProtectSwitch**
Config	String	是	{"AiRuleEnable": 1}	AI智能防护配置的详细信息，使用JSON格式的字符串表述，具体结构如下。 • **AiRuleEnable**：Integer类型，必选，AI智能防护功能的开关状态。取值： - **0**：关闭 - **1**：开启
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=ModifyWebAIProtectSwitch
&Config={"AiRuleEnable": 1},
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.11.3 ModifyWebAIProtectMode

调用ModifyWebAIProtectMode设置网站业务AI智能防护的模式。

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	ModifyWebAIProtectMode	要执行的操作。取值：**ModifyWebAIProtectMode**

名称	类型	是否必选	示例值	描述
Config	String	是	{"AiTemplate":"level60","AiMode":"defense"}	AI智能防护配置的详细信息，使用JSON格式的字符串表述，具体结构如下。 • **AiTemplate**：String类型，必选，AI智能防护功能的防护等级。取值： - **level30**：宽松 - **level60**：正常 - **level90**：严格 • **AiMode**：String类型，必选，AI智能防护功能的防护模式。取值： - **watch**：预警模式 - **defense**：防护模式
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=ModifyWebAIProtectMode
&Config={"AiTemplate":"level60","AiMode":"defense"}
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.11.4 ModifyWebIpSetSwitch

调用ModifyWebIpSetSwitch设置网站业务黑白名单（针对域名）的开关状态。

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	ModifyWebIpSetSwitch	要执行的操作。取值：**ModifyWebIpSetSwitch**

名称	类型	是否必选	示例值	描述
Config	String	是	{"BwlistEnable":1}	黑白名单（针对域名）的详细信息，使用JSON格式的字符串表述，具体结构如下。 • **Bwlist_Enable**：Integer类型，必选，黑白名单（针对域名）功能的开关状态。取值： - **0**：关闭 - **1**：开启
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=ModifyWebIpSetSwitch
&Config={"BwlistEnable":1}
&Domain=www.aliyun.com
```

```
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.11.5 ConfigWebIpSet

调用ConfigWebIpSet设置针对网站业务的黑名单和白名单IP。

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	ConfigWebIpSet	要执行的操作。取值：**ConfigWebIpSet**
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

名称	类型	是否必选	示例值	描述
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
BlackList.N	RepeatList	否	1.1.1.1	黑名单IP地址/地址段列表。N的最大值：200，即最多可配置200个黑名单IP地址/地址段。
WhiteList.N	RepeatList	否	2.2.2.2/24	白名单IP地址/地址段列表。N的最大值：200，即最多可配置200个白名单IP地址/地址段。

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=ConfigWebIpSet
&Domain=www.aliyun.com
&BlackList.1=1.1.1.1
&WhiteList.1=2.2.2.2/24
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.11.6 EnableWebCC

调用EnableWebCC开启网站业务频率控制防护（CC防护）的开关。

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	EnableWebCC	要执行的操作。取值：**EnableWebCC**
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=EnableWebCC
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.11.7 DisableWebCC

调用DisableWebCC关闭网站业务频率控制防护（CC防护）的开关。

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	DisableWebCC	要执行的操作。取值：**DisableWebCC**

名称	类型	是否必选	示例值	描述
Domain	String	是	www.aliyun.com	网站业务的域名。  **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值: • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=DisableWebCC
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

`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。

13.11.8 ConfigWebCCTemplate

调用ConfigWebCCTemplate设置网站业务频率控制防护（CC防护）的防护模式。

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	ConfigWebCCTemplate	要执行的操作。取值：**ConfigWebCCTemplate**
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
Template	String	是	default	频率控制防护（CC防护）的防护模式。取值： • **default**：正常 • **gf_under_attack**：攻击紧急 • **gf_sos_verify**：严格 • **gf_sos_enhance**：超级严格
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

名称	类型	是否必选	示例值	描述
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=ConfigWebCCTemplate
&Domain=www.aliyun.com
&Template=default
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

`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。

13.11.9 EnableWebCCRule

调用EnableWebCCRule开启网站业务频率控制防护（CC防护）的自定义规则开关。

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	EnableWebCCRule	要执行的操作。取值：**EnableWebCCRule**
Domain	String	是	www.aliyun.com	网站业务的域名。  **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=EnableWebCCRule
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

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

```
</EnableWebCCRuleResponse>
```

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。

13.11.10 DisableWebCCRule

调用DisableWebCCRule关闭网站业务频率控制防护（CC防护）的自定义规则开关。

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	DisableWebCCRule	要执行的操作。取值：**DisableWebCCRule**
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=DisableWebCCRule
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.11.11 DescribeWebCCRules

调用DescribeWebCCRules查询网站业务频率控制防护（CC防护）的自定义规则。

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	DescribeWebCCRules	要执行的操作。取值：**DescribeWebCCRules**

名称	类型	是否必选	示例值	描述
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
PageSize	String	是	10	页面显示的记录数量。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值: • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
PageNumber	Integer	否	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写**1**。

返回数据

名称	类型	示例值	描述
RequestId	String	EAED912D-909E-45F0-AF74-AC0CCDCAE314	本次请求的ID。
TotalCount	Long	1	频率控制（CC防护）自定义规则的总数。
WebCCRules	Array		频率控制（CC防护）自定义规则。
Act	String	close	阻断类型。取值: • **close**：封禁 • **captcha**：人机识别

名称	类型	示例值	描述
Count	Integer	3	单一IP访问次数。取值范围：**2~2000**。
Interval	Integer	5	检测间隔。取值范围：**5~10800**，单位：秒。
Mode	String	prefix	匹配模式。取值： • **prefix**：前缀匹配 • **match**：完全匹配
Name	String	wq	规则名称。
Ttl	Integer	60	封禁时长。取值范围：**1~1440**，单位：分钟。
Uri	String	/hello	检测路径。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeWebCCRules
&Domain=www.aliyun.com
&PageSize=10
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeWebCCRulesResponse>
  <TotalCount>1</TotalCount>
  <RequestId>EAED912D-909E-45F0-AF74-AC0CCDCAE314</RequestId>
  <WebCCRules>
    <Act>close</Act>
    <Mode>prefix</Mode>
    <Count>3</Count>
    <Ttl>60</Ttl>
    <Uri>/hello</Uri>
    <Name>wq</Name>
    <Interval>5</Interval>
  </WebCCRules>
</DescribeWebCCRulesResponse>
```

`JSON` 格式

```
{
 "TotalCount": 1,
 "RequestId": "EAED912D-909E-45F0-AF74-AC0CCDCAE314",
```

```
 "WebCCRules": [
  {
   "Act": "close",
   "Mode": "prefix",
   "Count": 3,
   "Ttl": 60,
   "Uri": "/hello",
   "Name": "wq",
   "Interval": 5
  }
 ]
}
```


错误码

访问错误中心查看更多错误码。

13.11.12 CreateWebCCRule

调用CreateWebCCRule创建网站业务频率控制防护（CC防护）的自定义规则。

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	CreateWebCCRule	要执行的操作。取值：**CreateWebCCRule**
Act	String	是	close	阻断类型。取值： • **close**：封禁 • **captcha**：人机识别
Count	Integer	是	60	单一IP访问次数。取值范围：**2~2000**。
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

名称	类型	是否必选	示例值	描述
Interval	Integer	是	20	检测时长。取值范围：**5~10800**，单位：秒。
Mode	String	是	prefix	匹配模式。取值： • **prefix**：前缀匹配 • **match**：完全匹配 **说明:** 检测路径**URI**中包含参数时，请选择前缀匹配。
Name	String	是	testrule	规则名称。允许使用英文字母、数字或下划线（_），长度不能超过128个字符
Ttl	Integer	是	10	封禁时长。取值范围：**1~1440**，单位：分钟。
Uri	String	是	/abc/a.php	检测路径。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=CreateWebCCRule
&Act=close
&Count=60
&Domain=www.aliyun.com
&Interval=20
&Mode=prefix
&Name=testrule
&Ttl=10
&Uri=/abc/a.php
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

`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。

13.11.13 ModifyWebCCRule

调用ModifyWebCCRule编辑网站业务频率控制防护（CC防护）的自定义规则。

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	ModifyWebCCRule	要执行的操作。取值：**ModifyWebCCRule**

名称	类型	是否必选	示例值	描述
Act	String	是	close	阻断类型。取值： • **close**：封禁 • **captcha**：人机识别
Count	Integer	是	3	单一IP访问次数。取值范围：**2~2000**。
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
Interval	Integer	是	30	检测时长。取值范围：**5~10800**，单位：秒。
Mode	String	是	prefix	匹配模式。取值： • **prefix**：前缀匹配 • **match**：完全匹配
Name	String	是	testrule	规则名称。
Ttl	Integer	是	10	封禁时长。取值范围：**1~1440**，单位：分钟。
Uri	String	是	/abc	检测路径。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=ModifyWebCCRule
&Act=close
&Count=3
&Domain=www.aliyun.com
&Interval=30
&Mode=prefix
&Name=testrule
&Ttl=10
&Uri=/abc
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

`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。

13.11.14 DeleteWebCCRule

调用DeleteWebCCRule删除网站业务频率控制防护（CC防护）的自定义规则。

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	DeleteWebCCRule	要执行的操作。取值：**DeleteWebCCRule**
Domain	String	是	www.aliyun.com	网站业务的域名。  **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
Name	String	是	wq	要删除的自定义频率控制（CC防护）规则的名称。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=DeleteWebCCRule
&Domain=www.aliyun.com
&Name=wq
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.11.15 ModifyWebPreciseAccessSwitch

调用ModifyWebPreciseAccessSwitch设置网站业务精确访问控制的开关状态。

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	ModifyWebPreciseAccessSwitch	要执行的操作。取值：**ModifyWebPreciseAccessSwitch**
Config	String	是	{"PreciseRuleEnable":0}	精确访问控制的开关状态配置，使用JSON格式的字符串表述，具体结构如下。 • **PreciseRuleEnable**：Integer类型，必选，精确访问控制的开关状态。取值： - **0**：关闭 - **1**：开启

名称	类型	是否必选	示例值	描述
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值: • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=ModifyWebPreciseAccessSwitch
&Config={"PreciseRuleEnable":0}
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.11.16 DescribeWebPreciseAccessRule

调用DescribeWebPreciseAccessRule查询网站业务精确访问控制规则。

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	DescribeWebPreciseAccessRule	要执行的操作。取值：**DescribeWebPreciseAccessRule**
Domains.N	RepeatList	是	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
PreciseAccessConfigList	Array		网站业务精确访问控制规则。

名称	类型	示例值	描述
Domain	String	www.aliyun.com	网站域名。
RuleList	Array		规则列表。
Action	String	accept	匹配动作。取值： • **accept**：放行 • **block**：封禁 • **challenge**：挑战
ConditionList	Array		匹配条件列表。
Content	String	1.1.1.1	匹配内容。
Field	String	ip	匹配字段。
HeaderName	String	null	自定义HTTP头部字段名称。 **说明：** 仅在**Field**为**header**时有效。
MatchMethod	String	belong	逻辑符。
Expires	Long	0	规则有效期。单位：秒。规则的匹配动作为阻断时（**action**为**block**）生效，在规则有效期内阻断访问请求。**0**表示永久生效。
Name	String	testrule	规则名称。
Owner	String	manual	规则来源。取值： • **manual**：手动添加（默认） • **auto**：自动生成
RequestId	String	209EEFBF-B0C7-441E-8C28-D0945A57A638	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeWebPreciseAccessRule
&Domains.1=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeWebPreciseAccessRuleResponse>
  <PreciseAccessConfigList>
    <RuleList>
      <Owner>manual</Owner>
      <Action>accept</Action>
      <ConditionList>
        <MatchMethod>belong</MatchMethod>
        <Field>ip</Field>
        <HeaderName></HeaderName>
        <Content>1.***.***.2</Content>
      </ConditionList>
      <Expires>0</Expires>
      <Name>testrule</Name>
    </RuleList>
    <Domain>www.aliyun.com</Domain>
  </PreciseAccessConfigList>
  <RequestId>209EEFBF-B0C7-441E-8C28-D0945A57A638</RequestId>
</DescribeWebPreciseAccessRuleResponse>
```

JSON 格式

```
{
 "PreciseAccessConfigList": [
  {
   "RuleList": [
    {
     "Owner": "manual",
     "Action": "accept",
     "ConditionList": [
      {
       "MatchMethod": "belong",
       "Field": "ip",
       "HeaderName": "",
       "Content": "1.***.***.2"
      }
     ],
     "Expires": 0,
     "Name": "testrule"
    }
   ],
   "Domain": "www.aliyun.com"
  }
 ],
 "RequestId": "209EEFBF-B0C7-441E-8C28-D0945A57A638"
```

```
}
```

错误码

访问错误中心查看更多错误码。

13.11.17 ModifyWebPreciseAccessRule

调用ModifyWebPreciseAccessRule编辑网站业务精确访问控制规则。

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	ModifyWebPreciseAccessRule	要执行的操作。取值：**ModifyWebPreciseAccessRule**
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

名称	类型	是否必选	示例值	描述
Rules	String	是	[{"action":"block","name":"testrule","condition":[{"field":"uri","match_method":"contain","content":"/test/123"}]}]	精确访问控制规则的配置，使用JSON格式的字符串表述，具体结构如下。 • **action**：String类型，必选，匹配动作。取值： - **accept**：放行 - **block**：封禁 - **challenge**：挑战 • **name**：String类型，必选，规则名称。 • **condition**：Map类型，必选，匹配条件。具体结构如下。 **说明：** 如果设置了多个匹配条件，则多个条件间是且的关系。 - **field**：String类型，必选，匹配字段。 - **match_method**：String类型，必选，匹配方法。 **说明：** 关于**field**和**match_method**的取值，请参见请求参数表下的补充描述。 - **content**：String类型，必选，匹配内容。 • **header_name**：String类型，可选，头部字段名称。仅在**field**为**header**时生效。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

名称	类型	是否必选	示例值	描述
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
Expires	Integer	否	600	规则有效期。单位：秒。规则的匹配动作为阻断时（**action**为**block**）生效，在规则有效期内阻断访问请求。不传入该参数表示永久生效。

field和match_method的取值及对应关系

匹配字段（field）	描述	适用的逻辑符（match_method）
ip	访问请求的来源IP。	**belong**： 属于 **nbelong**： 不属于
uri	访问请求的URI地址。	**contain**： 包含 **ncontain**： 不包含 **equal**： 等于 **nequal**： 不等于 **lless**： 长度小于 **lequal**： 长度等于 **lgreat**： 长度大于 **regular**： 正则匹配

匹配字段（field）	描述	适用的逻辑符（match_method）
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。	**contain**： 包含 **ncontain**： 不包含 **equal**： 等于 **nequal**： 不等于 **lless**： 长度小于 **lequal**： 长度等于 **lgreat**： 长度大于 **nexist**： 不存在 **regular**： 正则匹配
user-agent	发起访问请求的客户端的浏览器标识、渲染引擎标识和版本信息等浏览器相关信息。	**contain**： 包含 **ncontain**： 不包含 **equal**： 等于 **nequal**： 不等于 **lless**： 长度小于 **lequal**： 长度等于 **lgreat**： 长度大于 **regular**： 正则匹配
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。	**contain**： 包含 **ncontain**： 不包含 **equal**： 等于 **nequal**： 不等于 **lless**： 长度小于 **lequal**： 长度等于 **lgreat**： 长度大于

匹配字段（field）	描述	适用的逻辑符（match_method）
cookie	访问请求中的Cookie信息。	**contain**： 包含 **ncontain**： 不包含 **equal**： 等于 **nequal**： 不等于 **lless**： 长度小于 **lequal**： 长度等于 **lgreat**： 长度大于 **nexist**： 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。	**contain**： 包含 **ncontain**： 不包含 **equal**： 等于 **nequal**： 不等于 **lless**： 长度小于 **lequal**： 长度等于 **lgreat**： 长度大于
x-forwarded-for	访问请求的客户端真实IP。X-Forwarded-For（XFF）用来识别通过HTTP代理或负载均衡方式转发的访问请求的客户端最原始的IP地址的HTTP请求头字段，只有通过HTTP代理或者负载均衡服务器转发的访问请求才会包含该项。	**contain**： 包含 **ncontain**： 不包含 **equal**： 等于 **nequal**： 不等于 **lless**： 长度小于 **lequal**： 长度等于 **lgreat**： 长度大于 **nexist**： 不存在 **regular**： 正则匹配

匹配字段（field）	描述	适用的逻辑符（match_method）
content-length	访问请求的所包含的字节数。	**vless**： 值小于 **vequal**： 值等于 **vgreat**： 值大于
post-body	访问请求的内容信息。	**contain**： 包含 **ncontain**： 不包含 **equal**： 等于 **nequal**： 不等于 **regular**： 正则匹配
http-method	访问请求的方法，如GET、POST等。	**equal**： 等于 **nequal**： 不等于
header	访问请求的头部信息，用于自定义HTTP头部字段。	**contain**： 包含 **ncontain**： 不包含 **equal**： 等于 **nequal**： 不等于 **lless**： 长度小于 **lequal**： 长度等于 **lgreat**： 长度大于 **nexist**： 不存在

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=ModifyWebPreciseAccessRule
&Domain=www.aliyun.com
&Rules=[{"action":"block","name":"testrule","condition":[{"field":"uri","match_method":"
contain","content":"/test/123"}]}]
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.11.18 DeleteWebPreciseAccessRule

调用DeleteWebPreciseAccessRule删除网站业务精确访问控制规则。

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	DeleteWebPreciseAccessRule	要执行的操作。取值：**DeleteWebPreciseAccessRule**
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

名称	类型	是否必选	示例值	描述
RuleNames.N	RepeatList	是	testrule	要删除的精确访问控制规则的名称。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=DeleteWebPreciseAccessRule
&Domain=www.aliyun.com
&RuleNames.1=testrule
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

`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。

13.11.19 ModifyWebAreaBlockSwitch

调用ModifyWebAreaBlockSwitch设置网站业务区域封禁（针对域名）的开关状态。

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	ModifyWebAreaBlockSwitch	要执行的操作。取值：**ModifyWebAreaBlockSwitch**
Config	String	是	{"RegionblockEnable": 1}	区域封禁（针对域名）的开关状态，使用JSON格式的字符串表述，具体结构如下。 • **RegionblockEnable**：Integer类型，必选，区域封禁（针对域名）的开关状态。取值： - **1**：开启 - **0**：关闭
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=ModifyWebAreaBlockSwitch
&Config={"RegionblockEnable": 1}
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.11.20 DescribeWebAreaBlockConfigs

调用DescribeWebAreaBlockConfigs查询网站业务区域封禁（针对域名）的配置信息。

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	DescribeWebAreaBlockConfigs	要执行的操作。取值：**DescribeWebAreaBlockConfigs**

名称	类型	是否必选	示例值	描述
Domains.N	RepeatList	是	www.aliyun.com	网站业务的域名。 **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值: • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
AreaBlockConfigs	Array		区域封禁（针对域名）的配置信息。
Domain	String	www.aliyun.com	网站域名。
RegionList	Array		封禁地区信息。
Block	Integer	0	封禁状态。取值: • **0**：未封禁 • **1**：已封禁
Region	String	CN-SHANGHAI	地区。
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeWebAreaBlockConfigs
&Domains.1=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeWebAreaBlockConfigsResponse>
  <AreaBlockConfigs>
    <RegionList>
      <Block>1</Block>
      <Region>CN-YUNNAN</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-HEILONGJIANG</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>OVERSEAS-ANTARCTICA</Region>
    </RegionList>
    <RegionList>
      <Block>1</Block>
      <Region>OVERSEAS-EUROPE</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-BEIJING</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-HENAN</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-HUNAN</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-FUJIAN</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-JIANGSU</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-ZHEJIANG</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-HAINAN</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-TIBET</Region>
```

```
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-INNERMONGOLIA</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-NINGXIA</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-SHAANXI</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-GUANGDONG</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-QINGHAI</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>OVERSEAS-NAMERICA</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>OVERSEAS-SAMERICA</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-SHANGHAI</Region>
    </RegionList>
    <RegionList>
      <Block>1</Block>
      <Region>CN-GUANGXI</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>OVERSEAS-ASIA</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>OVERSEAS-OCEANIA</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-MACAU</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-GUIZHOU</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-JILIN</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-ANHUI</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-JIANGXI</Region>
```

```
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-HEBEI</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-CHONGQING</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>OVERSEAS-AFRICA</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-SICHUAN</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-TIANJIN</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-XINJIANG</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-LIAONING</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-GANSU</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-HONGKONG</Region>
    </RegionList>
    <RegionList>
      <Block>1</Block>
      <Region>CN-TAIWAN</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-SHANDONG</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-SHANXI</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-HUBEI</Region>
    </RegionList>
    <Domain>www.aliyun.com</Domain>
  </AreaBlockConfigs>
  <RequestId>044D33A9-80B9-4F07-BA63-9207CAD53263</RequestId>
</DescribeWebAreaBlockConfigsResponse>
```

JSON 格式

```
{
 "AreaBlockConfigs": [
  {
```

```
"RegionList": [
 {
  "Block": 1,
  "Region": "CN-YUNNAN"
 },
 {
  "Block": 0,
  "Region": "CN-HEILONGJIANG"
 },
 {
  "Block": 0,
  "Region": "OVERSEAS-ANTARCTICA"
 },
 {
  "Block": 1,
  "Region": "OVERSEAS-EUROPE"
 },
 {
  "Block": 0,
  "Region": "CN-BEIJING"
 },
 {
  "Block": 0,
  "Region": "CN-HENAN"
 },
 {
  "Block": 0,
  "Region": "CN-HUNAN"
 },
 {
  "Block": 0,
  "Region": "CN-FUJIAN"
 },
 {
  "Block": 0,
  "Region": "CN-JIANGSU"
 },
 {
  "Block": 0,
  "Region": "CN-ZHEJIANG"
 },
 {
  "Block": 0,
  "Region": "CN-HAINAN"
 },
 {
  "Block": 0,
  "Region": "CN-TIBET"
 },
 {
  "Block": 0,
  "Region": "CN-INNERMONGOLIA"
 },
 {
  "Block": 0,
  "Region": "CN-NINGXIA"
 },
 {
  "Block": 0,
  "Region": "CN-SHAANXI"
 },
 {
  "Block": 0,
  "Region": "CN-GUANGDONG"
```

```
    },
    {
     "Block": 0,
     "Region": "CN-QINGHAI"
    },
    {
     "Block": 0,
     "Region": "OVERSEAS-NAMERICA"
    },
    {
     "Block": 0,
     "Region": "OVERSEAS-SAMERICA"
    },
    {
     "Block": 0,
     "Region": "CN-SHANGHAI"
    },
    {
     "Block": 1,
     "Region": "CN-GUANGXI"
    },
    {
     "Block": 0,
     "Region": "OVERSEAS-ASIA"
    },
    {
     "Block": 0,
     "Region": "OVERSEAS-OCEANIA"
    },
    {
     "Block": 0,
     "Region": "CN-MACAU"
    },
    {
     "Block": 0,
     "Region": "CN-GUIZHOU"
    },
    {
     "Block": 0,
     "Region": "CN-JILIN"
    },
    {
     "Block": 0,
     "Region": "CN-ANHUI"
    },
    {
     "Block": 0,
     "Region": "CN-JIANGXI"
    },
    {
     "Block": 0,
     "Region": "CN-HEBEI"
    },
    {
     "Block": 0,
     "Region": "CN-CHONGQING"
    },
    {
     "Block": 0,
     "Region": "OVERSEAS-AFRICA"
    },
    {
     "Block": 0,
     "Region": "CN-SICHUAN"
```

```
    },
    {
     "Block": 0,
     "Region": "CN-TIANJIN"
    },
    {
     "Block": 0,
     "Region": "CN-XINJIANG"
    },
    {
     "Block": 0,
     "Region": "CN-LIAONING"
    },
    {
     "Block": 0,
     "Region": "CN-GANSU"
    },
    {
     "Block": 0,
     "Region": "CN-HONGKONG"
    },
    {
     "Block": 1,
     "Region": "CN-TAIWAN"
    },
    {
     "Block": 0,
     "Region": "CN-SHANDONG"
    },
    {
     "Block": 0,
     "Region": "CN-SHANXI"
    },
    {
     "Block": 0,
     "Region": "CN-HUBEI"
    }
   ],
   "Domain": "www.aliyun.com"
  }
 ],
 "RequestId": "044D33A9-80B9-4F07-BA63-9207CAD53263"
}
```


错误码

访问错误中心查看更多错误码。

13.11.21 ModifyWebAreaBlock

调用ModifyWebAreaBlock设置网站业务区域封禁（针对域名）的封禁地区。

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	ModifyWebAreaBlock	要执行的操作。取值： **ModifyWebAreaBlock**
Domain	String	是	www.aliyun.com	网站业务的域名。  **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

名称	类型	是否必选	示例值	描述
Regions.N	RepeatList	否	CN-SHANGHAI	要封禁的区域列表。不传入表示取消区域封禁（针对域名）。取值： 中国地区 • **CN-SHANGHAI**：上海市 • **CN-YUNNAN**：云南省 • **CN-INNERMONGOLIA**：内蒙古自治区 • **CN-BEIJING**：北京市 • **CN-TAIWAN**：台湾省 • **CN-JILIN**：吉林省 • **CN-SICHUAN**：四川省 • **CN-TIANJIN**：天津省 • **CN-NINGXIA**：宁夏回族自制区 • **CN-ANHUI**：安徽省 • **CN-SHANDONG**：山东省 • **CN-SHAANXI**：陕西省 • **CN-SHANXI**：山西省 • **CN-GUANGDONG**：广东省 • **CN-GUANGXI**：广西壮族自治区 • **CN-XINJIANG**：新疆维吾尔自治区 • **CN-JIANGSU**：江苏省 • **CN-JIANGXI**：江西省 • **CN-HEBEI**：河北省 • **CN-HENAN**：河南省 • **CN-ZHEJIANG**：浙江省 • **CN-HAINAN**：海南省 • **CN-HUBEI**：湖北省 • **CN-HUNAN**：湖南省 • **CN-MACAU**：澳门特别行政区 • **CN-GANSU**：甘肃省 • **CN-FUJIAN**：福建省 • **CN-TIBET**：西藏自治区 • **CN-GUIZHOU**：贵州省 • **CN-LIAONING**：辽宁省 • **CN-CHONGQING**：重庆市 • **CN-QINGHAI**：青海省 • **CN-HONGKONG**：香港特别行政区
				• **CN-HEILONGJIANG**：黑龙江省 海外地区

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=ModifyWebAreaBlock
&Domain=www.aliyun.com
&Regions.1=CN-SHANGHAI
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.12 非网站业务防护策略

13.12.1 DescribePortAutoCcStatus

调用DescribePortAutoCcStatus查询非网站业务AI智能防护的配置信息。

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	DescribePortAutoCcStatus	要执行的操作。取值：**DescribePortAutoCcStatus**
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。  **说明:** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
PortAutoCcStatus	Array		非网站业务AI智能防护的配置信息。
Mode	String	normal	AI智能防护的模式。取值： • **normal**：正常 • **loose**：宽松 • **strict**：严格
Switch	String	on	AI智能防护的开关状态。取值： • **on**：开启 • **off**：关闭
WebMode	String	normal	80和443端口的防护模式。取值： • **normal**：正常 • **loose**：宽松 • **strict**：严格

名称	类型	示例值	描述
WebSwitch	String	off	80和443端口的防护开关状态。取值： • **on**：开启 • **off**：关闭
RequestId	String	BC3C6403-F248-4125-B2C9-8733ED94EA85	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePortAutoCcStatus
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribePortAutoCcStatusResponse>
  <RequestId>BC3C6403-F248-4125-B2C9-8733ED94EA85</RequestId>
  <PortAutoCcStatus>
    <WebSwitch>off</WebSwitch>
    <Switch>on</Switch>
    <WebMode>normal</WebMode>
    <Mode>normal</Mode>
  </PortAutoCcStatus>
</DescribePortAutoCcStatusResponse>
```

`JSON` 格式

```
{
 "RequestId": "BC3C6403-F248-4125-B2C9-8733ED94EA85",
 "PortAutoCcStatus": [
  {
   "WebSwitch": "off",
   "Switch": "on",
   "WebMode": "normal",
   "Mode": "normal"
  }
 ]
}
```

错误码

访问错误中心查看更多错误码。

13.12.2 ModifyPortAutoCcStatus

调用ModifyPortAutoCcStatus设置非网站业务AI智能防护。

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	ModifyPortAutoCcStatus	要执行的操作。取值：**ModifyPortAutoCcStatus**
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明:** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
Mode	String	是	normal	非网站业务AI智能防护的模式。取值： • **normal**：正常 • **loose**：宽松 • **strict**：严格
Switch	String	是	on	非网站业务AI智能防护的开关状态。取值： • **on**：开启 • **off**：关闭
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

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=ModifyPortAutoCcStatus
&InstanceId=ddoscoo-cn-mp91j1ao****
&Switch=on
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

`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。

13.12.3 DescribeNetworkRuleAttributes

调用DescribeNetworkRuleAttributes查询非网站业务端口转发规则的防护配置，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	DescribeNetworkRuleAttributes	要执行的操作。取值：**DescribeNetworkRuleAttributes**
NetworkRules	String	是	[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort":8080}]	要查询的端口转发规则，使用JSON格式的字符串表述，具体结构如下。 • **InstanceId**：String类型，必选，DDoS高防实例ID。 • **Protocol**：String类型，必选，转发协议类型。取值：**tcp**、**udp**。 • **FrontendPort**：Integer类型，必选，转发端口。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
NetworkRuleAttributes	Array		非网站业务端口转发规则的防护配置，包括会话保持和DDoS防护策略。
Config	Struct		端口转发规则的防护配置。
Cc	Struct		源连接频繁超限控制策略。
Sblack	Array		源连接多次超限，将源IP加入黑名单的策略。
Cnt	Integer	5	源连接超过限制的次数。取值固定为**5**，表示如果源连接在检查间隔内超过限制5次，将源IP加入黑名单。

名称	类型	示例值	描述
During	Integer	60	检查间隔。取值固定为**60**，单位：秒。
Expires	Integer	600	黑名单有效时长。取值范围：**60~604800**，单位：秒。
Type	Integer	1	源IP黑名单配置类型。取值： • **1**：源新建连接限速IP黑名单 • **2**：源并发连接限速IP黑名单 • **3**：源PPS限速IP黑名单 • **4**：源带宽限速IP黑名单
NodataConn	String	off	空连接过滤的开关状态。取值： • **on**：开启 • **off**：关闭
PayloadLen	Struct		包长度过滤配置。
Max	Integer	6000	包长度的最大值。取值范围：**0~6000**，单位：Byte。
Min	Integer	0	包长度的最小值。取值范围：**0~6000**，单位：Byte。
PersistenceTimeout	Integer	0	会话保持的超时时间。取值范围：**30~3600**，单位：秒。默认为**0**，表示关闭。
Sla	Struct		目的限速配置。
Cps	Integer	100000	目的新建连接限速。取值范围：**100~100000**。
CpsEnable	Integer	1	目的新建连接限速的开关状态。取值： • **0**：关闭 • **1**：开启
Maxconn	Integer	1000000	目的并发连接限速。取值范围：**1000~1000000**。

名称	类型	示例值	描述
MaxconnEnable	Integer	0	目的并发连接限速的开关状态。取值： • **0**：关闭 • **1**：开启
Slimit	Struct		源限速配置。
Bps	Long	0	源带宽限速。取值范围：**1024~268435456**，单位：Byte/s。默认为**0**，表示未开启源带宽限速。
Cps	Integer	0	源新建连接限速。取值范围：**1~500000**，单位：个。
CpsEnable	Integer	0	源新建连接限速的开关状态。取值： • **0**：关闭 • **1**：开启
CpsMode	Integer	1	源新建连接限速的模式。取值： • **1**：手动 • **2**：自动
Maxconn	Integer	0	源并发连接限速。取值范围：**1~500000**，单位：个。
MaxconnEnable	Integer	0	源并发连接限速的开关状态。取值： • **0**：关闭 • **1**：开启
Pps	Long	0	源PPS限速。取值范围：**1~100000**，单位：Packet/s。默认为**0**，表示未开启源PPS限速。
Synproxy	String	off	虚假源过滤的开关状态。取值： • **on**：开启 • **off**：关闭
FrontendPort	Integer	8080	转发端口。

名称	类型	示例值	描述
InstanceId	String	ddoscoo-cn-mp91j1ao****	DDoS高防实例ID。
Protocol	String	tcp	转发协议。取值： • **tcp** • **udp**
RequestId	String	F9F2F77D-307C-4F15-8D02-AB5957EEBF97	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeNetworkRuleAttributes
&NetworkRules=[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort
":8080}]
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeNetworkRuleAttributesResponse>
  <NetworkRuleAttributes>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
    <Config>
      <NodataConn>off</NodataConn>
      <Cc></Cc>
      <PersistenceTimeout>0</PersistenceTimeout>
      <PayloadLen>
        <Min>0</Min>
        <Max>6000</Max>
      </PayloadLen>
      <Sla>
        <Cps>100000</Cps>
        <CpsEnable>1</CpsEnable>
        <MaxconnEnable>0</MaxconnEnable>
        <Maxconn>1000000</Maxconn>
      </Sla>
      <Slimit>
        <CpsMode>1</CpsMode>
        <Pps>0</Pps>
        <Bps>0</Bps>
        <Cps>0</Cps>
        <CpsEnable>0</CpsEnable>
        <MaxconnEnable>0</MaxconnEnable>
        <Maxconn>0</Maxconn>
      </Slimit>
      <Synproxy>on</Synproxy>
    </Config>
    <FrontendPort>8080</FrontendPort>
    <Protocol>tcp</Protocol>
```

```
  </NetworkRuleAttributes>
  <RequestId>F9F2F77D-307C-4F15-8D02-AB5957EEBF97</RequestId>
</DescribeNetworkRuleAttributesResponse>
```

JSON 格式

```
{
 "NetworkRuleAttributes": [
  {
   "InstanceId": "ddoscoo-cn-mp91j1ao****",
   "Config": {
    "NodataConn": "off",
    "Cc": {
     "Sblack": []
    },
    "PersistenceTimeout": 0,
    "PayloadLen": {
     "Min": 0,
     "Max": 6000
    },
    "Sla": {
     "Cps": 100000,
     "CpsEnable": 1,
     "MaxconnEnable": 0,
     "Maxconn": 1000000
    },
    "Slimit": {
     "CpsMode": 1,
     "Pps": 0,
     "Bps": 0,
     "Cps": 0,
     "CpsEnable": 0,
     "MaxconnEnable": 0,
     "Maxconn": 0
    },
    "Synproxy": "on"
   },
   "FrontendPort": 8080,
   "Protocol": "tcp"
  }
 ],
 "RequestId": "F9F2F77D-307C-4F15-8D02-AB5957EEBF97"
}
```

错误码

访问错误中心查看更多错误码。

13.12.4 ModifyNetworkRuleAttribute

调用ModifyNetworkRuleAttribute编辑端口转发规则的会话保持设置。

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	ModifyNetworkRuleAttribute	要执行的操作。取值：**ModifyNetworkRuleAttribute**
Config	String	是	{"PersistenceTimeout":900}	端口转发规则的会话保持设置。使用JSON格式的字符串表述，具体结构描述如下。 • **PersistenceTimeout**：Integer类型，必选，会话保持的超时时间。取值范围：**30~3600**，单位：秒。默认为**0**，表示关闭。
ForwardProtocol	String	是	tcp	转发协议。取值： • **tcp** • **udp**
FrontendPort	Integer	是	8080	转发端口。
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

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=ModifyNetworkRuleAttribute
&Config={"PersistenceTimeout":900}
&ForwardProtocol=tcp
&FrontendPort=8080
&InstanceId=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.13 定制场景策略

13.13.1 DescribeSceneDefensePolicies

调用DescribeSceneDefensePolicies查询定制场景策略的详细信息。

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	DescribeSceneDefensePolicies	要执行的操作。取值：**DescribeSceneDefensePolicies**

名称	类型	是否必选	示例值	描述
Template	String	否	promotion	策略模板。取值： • **promotion**：重大活动 • **bypass**：全量转发
Status	String	否	1	策略生效状态。取值： • **0**：禁用 • **1**：等待生效 • **2**：生效中 • **3**：过期
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
Policies	Array		定制场景策略的详细信息。
Done	Integer	1	策略执行状态。取值： • **1**：未执行或执行完成 • **0**：执行中 • **-1**：执行失败
EndTime	Long	1586016000000	生效结束时间。时间戳格式，单位：毫秒。
Name	String	testpolicy	策略名称。
ObjectCount	Integer	1	防护对象数量。

名称	类型	示例值	描述
PolicyId	String	321a-fd31-df51-****	策略ID。
RuntimePolicies	Array		策略运行规则。
NewValue	String	{"cc_rule_enable": false }	策略生效时的防护规则。 **PolicyType**为**1**时，取值：**{"cc_rule_enable": false }**，表示禁用频率控制。 **PolicyType**为**2**时，取值：**{"ai_rule_enable": 0}**，表示禁用AI智能防护。
PolicyType	Integer	1	策略生效时触发的防护功能变更类型。取值： • **1**：频率控制 • **2**：AI智能防护
Status	Integer	3	策略运行状态。取值： • **0**：未下发或策略恢复成功 • **1**：正在生效中（策略生效） • **2**：正在恢复中（策略恢复） • **3**：策略生效成功 • **4**：策略生效失败 • **5**：策略恢复失败 • **6**：策略对应对象的配置不存在（可能已删除）
oldValue	String	{"cc_rule_enable": true}	策略生效前的防护规则。 **PolicyType**为**1**时，取值：**{"cc_rule_enable": true}**，表示启用了频率控制。 **PolicyType**为**2**时，取值：**{"ai_rule_enable": 1}**，表示启用了AI智能防护。
StartTime	Long	1585670400000	生效开始时间。时间戳格式，单位：毫秒。

名称	类型	示例值	描述
Status	Integer	1	策略生效状态。取值： • **0**：禁用 • **1**：等待生效 • **2**：生效中 • **3**：过期
Template	String	promotion	策略模板。取值： • **promotion**：重大活动 • **bypass**：全量转发
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	本次请求的ID。
Success	Boolean	true	是否成功调用、取值： • **true**：是 • **false**：否

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribeSceneDefensePoliciesResponse>
  <Policies>
    <PolicyId>321a-fd31-df51-****</PolicyId>
    <Name>testpolicy</Name>
    <Template>promotion</Template>
    <StartTime>1585670400000</StartTime>
    <EndTime>1586016000000</EndTime>
    <Status>1</Status>
    <ObjectCount>1</ObjectCount>
    <Done>1</Done>
    <RuntimePolicies>
      <Status>4</Status>
      <PolicyType>1</PolicyType>
      <NewValue>
        <cc_rule_enable>false</cc_rule_enable>
      </NewValue>
      <oldValue>
        <cc_rule_enable>true</cc_rule_enable>
      </oldValue>
```

```
    </RuntimePolicies>
    <RuntimePolicies>
      <Status>3</Status>
      <PolicyType>2</PolicyType>
      <NewValue>
        <ai_rule_enable>0</ai_rule_enable>
      </NewValue>
      <oldValue>
        <ai_rule_enable>1</ai_rule_enable>
      </oldValue>
    </RuntimePolicies>
  </Policies>
  <Success>true</Success>
  <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
</DescribeSceneDefensePoliciesResponse>
```

JSON 格式

```
{
  "Policies": [
    {
      "PolicyId": "321a-fd31-df51-****",
      "Name": "testpolicy",
      "Template": "promotion",
      "StartTime": 1585670400000,
      "EndTime": 1586016000000,
      "Status": 1,
      "ObjectCount": 1,
      "Done": 1,
      "RuntimePolicies": [
        {
          "Status": 4,
          "PolicyType": 1,
          "NewValue": {
            "cc_rule_enable": false
          },
          "oldValue": {
            "cc_rule_enable": true
          }
        },
        {
          "Status": 3,
          "PolicyType": 2,
          "NewValue": {
            "ai_rule_enable": 0
          },
          "oldValue": {
            "ai_rule_enable": 1
          }
        }
      ]
    }
  ],
  "Success": true,
  "RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D"
}
```

错误码

访问错误中心查看更多错误码。

13.13.2 CreateSceneDefensePolicy

调用CreateSceneDefensePolicy创建定制场景策略。

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	CreateSceneDefensePolicy	要执行的操作。取值：**CreateSceneDefensePolicy**
EndTime	Long	是	1586016000000	生效结束时间。时间戳格式，单位：毫秒。
Name	String	是	testpolicy	策略名称。
StartTime	Long	是	1585670400000	生效开始时间。时间戳格式，单位：毫秒。
Template	String	是	promotion	策略模板。取值： • **promotion**：重大活动 • **bypass**：全量转发
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	本次请求的ID。

名称	类型	示例值	描述
Success	Boolean	true	是否成功创建策略。取值： • **true**：是 • **false**：否

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateSceneDefensePolicy
&EndTime=1586016000000
&Name=testpolicy
&StartTime=1585670400000
&Template=promotion
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<CreateSceneDefensePolicyResponse>
  <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
  <Success>true</Success>
</CreateSceneDefensePolicyResponse>
```

`JSON` 格式

```
{
  "RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
  "Success": true
}
```

错误码

访问错误中心查看更多错误码。

13.13.3 ModifySceneDefensePolicy

调用ModifySceneDefensePolicy编辑定制场景策略。

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	ModifyScenEDefensePolicy	要执行的操作。取值：**ModifySceneDefensePolicy**
EndTime	Long	是	1586016000000	生效结束时间。时间戳格式，单位：毫秒。
Name	String	是	testpolicy	策略名称。
PolicyId	String	是	321a-fd31-df51-****	要编辑的策略ID。  **说明：** 您可以调用DescribeSceneDefensePolicies查询所有策略ID。
StartTime	Long	是	1585670400000	生效开始时间。时间戳格式，单位：毫秒。
Template	String	是	promotion	策略模板。取值： • **promotion**：重大活动 • **bypass**：全量转发
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	本次请求的ID。

名称	类型	示例值	描述
Success	Boolean	true	是否成功调用。取值： • **true**：是 • **false**：否

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifySceneDefensePolicy
&EndTime=1586016000000
&Name=testpolicy
&PolicyId=321a-fd31-df51-****
&StartTime=1585670400000
&Template=promotion
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ModifySceneDefensePolicyResponse>
  <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
  <Success>true</Success>
</ModifySceneDefensePolicyResponse>
```

JSON 格式

```
{
  "RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
  "Success":true
}
```

错误码

访问错误中心查看更多错误码。

13.13.4 DeleteSceneDefensePolicy

调用DeleteSceneDefensePolicy删除定制场景策略。

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	DeleteSceneDefensePolicy	要执行的操作。取值：**DeleteSceneDefensePolicy**
PolicyId	String	是	321a-fd31-df51-****	要删除的策略ID。 **说明:** 您可以调用DescribeSceneDefensePolicies查询所有策略ID。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	本次请求的ID。
Success	Boolean	true	是否成功调用。取值： • **true**：是 • **false**：否

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteSceneDefensePolicy
&PolicyId=321a-fd31-df51-****
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DeleteSceneDefensePolicyResponse>
  <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
```

```
  <Success>true</Success>
</DeleteSceneDefensePolicyResponse>
```

JSON 格式

```
{
 "RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
 "Success":true
}
```

错误码

访问错误中心查看更多错误码。

13.13.5 DescribeSceneDefenseObjects

调用DescribeSceneDefenseObjects查询定制场景策略的防护对象。

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	DescribeSceneDefenseObjects	要执行的操作。取值：**DescribeSceneDefenseObjects**
PolicyId	String	是	321a-fd31-df51-****	要查询的策略ID。 **说明:** 您可以调用DescribeSceneDefensePolicies查询所有策略ID。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
Objects	Array		防护对象信息。
Domain	String	www.aliyun.com	域名。
PolicyId	String	321a-fd31-df51-****	策略ID。
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	本次请求的ID。
Success	Boolean	true	是否成功调用。取值： • **true**：是 • **false**：否

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeSceneDefenseObjects
&PolicyId=321a-fd31-df51-****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeSceneDefenseObjectsResponse>
  <Objects>
    <PolicyId>321a-fd31-df51-****</PolicyId>
    <Domain>www.aliyun.com</Domain>
  </Objects>
  <Success>true</Success>
  <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
</DescribeSceneDefenseObjectsResponse>
```

`JSON` 格式

```
{
  "Objects": [
    {
      "PolicyId": "321a-fd31-df51-****",
      "Domain": "www.aliyun.com"
    }
  ],
  "Success": true,
  "RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D"
```

```
}
```

错误码

访问错误中心查看更多错误码。

13.13.6 AttachSceneDefenseObject

调用AttachSceneDefenseObject为定制场景策略添加防护对象。

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	AttachSceneDefenseObject	要执行的操作。取值：**AttachSceneDefenseObject**
Objects	String	是	www.aliyun.com	要添加的防护对象。多个对象间使用英文逗号（,）分隔。
ObjectType	String	是	Domain	对象类型。取值：**Domain**，表示域名。
PolicyId	String	是	321a-fd31-df51-****	策略ID。 **说明:** 您可以调用DescribeSceneDefensePolicies查询所有策略ID。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	本次请求的ID。
Success	Boolean	true	是否成功调用。取值： • **true**：是 • **false**：否

示例

请求示例

```
http(s)://[Endpoint]/?Action=AttachSceneDefenseObject
&Objects=www.aliyun.com
&ObjectType=Domain
&PolicyId=321a-fd31-df51-****
&<公共请求参数>
```

正常返回示例

XML 格式

```
<AttachSceneDefenseObjectResponse>
  <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
  <Success>true</Success>
</AttachSceneDefenseObjectResponse>
```

JSON 格式

```
{
  "RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
  "Success":true
}
```

错误码

访问错误中心查看更多错误码。

13.13.7 DetachSceneDefenseObject

调用DetachSceneDefenseObject为定制场景策略移除防护对象。

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	DetachSceneDefenseObject	要执行的操作。取值：**DetachSceneDefenseObject**
Objects	String	是	www.aliyun.com	要移除的防护对象。多个对象间使用英文逗号（,）分隔。
PolicyId	String	是	321a-fd31-df51-****	策略ID。 **说明：** 您可以调用DescribeSceneDefensePolicies查询所有策略ID。
ObjectType	String	否	Domain	对象类型。取值：**Domain**，表示域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	本次请求的ID。
Success	Boolean	true	是否成功调用。取值 • **true**：是 • **false**：否

示例

请求示例

```
http(s)://[Endpoint]/?Action=DetachSceneDefenseObject
&Objects=www.aliyun.com
```

```
&PolicyId=321a-fd31-df51-****
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DetachSceneDefenseObjectResponse>
  <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
  <Success>true</Success>
</DetachSceneDefenseObjectResponse>
```

JSON 格式

```
{
  "RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
  "Success":true
}
```

错误码

访问错误中心查看更多错误码。

13.13.8 EnableSceneDefensePolicy

调用EnableSceneDefensePolicy启用定制场景策略。

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	EnableSceneDefensePolicy	要执行的操作。取值：**EnableSceneDefensePolicy**
PolicyId	String	是	321a-fd31-df51_****	要启用的策略ID。 **说明：** 您可以调用DescribeSceneDefensePolicies查询所有策略ID。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	本次请求的ID。
Success	Boolean	true	是否成功调用。取值： • **true**：是 • **false**：否

示例

请求示例

```
http(s)://[Endpoint]/?Action=EnableSceneDefensePolicy
&PolicyId=321a-fd31-df51-****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<EnableSceneDefensePolicyResponse>
  <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
  <Success>true</Success>
</EnableSceneDefensePolicyResponse>
```

`JSON` 格式

```
{
  "RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
  "Success":true
}
```

错误码

访问错误中心查看更多错误码。

13.13.9 DisableSceneDefensePolicy

调用DisableSceneDefensePolicy禁用定制场景策略。

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	DisableSceneDefensePolicy	要执行的操作。取值：**DisableSceneDefensePolicy**
PolicyId	String	是	321a-fd31-df51-****	要禁用的策略ID。 **说明:** 您可以调用DescribeSceneDefensePolicies查询所有策略ID。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	本次请求的ID。
Success	Boolean	true	是否成功调用。取值： • **true**：是 • **false**：否

示例

请求示例

```
http(s)://[Endpoint]/?Action=DisableSceneDefensePolicy
```

```
&PolicyId=321a-fd31-df51-****
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DisableSceneDefensePolicyResponse>
  <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
  <Success>true</Success>
</DisableSceneDefensePolicyResponse>
```

JSON 格式

```
{
  "RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
  "Success":true
}
```

错误码

访问错误中心查看更多错误码。

13.14 静态页面缓存

13.14.1 ModifyWebCacheSwitch

调用ModifyWebCacheSwitch设置网站业务静态页面缓存的开关状态。

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	ModifyWebCacheSwitch	要执行的操作。取值：**ModifyWebCacheSwitch**
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明:** 域名必须已配置网站业务转发规则且关联了增强功能套餐的DDoS高防实例。您可以调用DescribeDomains查询所有域名。

名称	类型	是否必选	示例值	描述
Enable	Integer	是	1	静态页面缓存的开关状态。取值： • **1**：开启 • **0**：关闭
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=ModifyWebCacheSwitch
&Domain=www.aliyun.com
&Enable=1
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.14.2 ModifyWebCacheMode

调用ModifyWebCacheMode设置网站业务静态页面缓存的缓存模式。

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	ModifyWebCacheMode	要执行的操作。取值：**ModifyWebCacheMode**
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则且关联了增强功能套餐的DDoS高防实例。您可以调用DescribeDomains查询所有域名。
Mode	String	是	standard	静态页面缓存的模式。取值： • **standard**：标准模式 • **aggressive**：强力模式 • **bypass**：不缓存
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=ModifyWebCacheMode
&Domain=www.aliyun.com
&Mode=standard
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.14.3 ModifyWebCacheCustomRule

调用ModifyWebCacheCustomRule设置网站业务静态页面缓存的自定义规则。

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	ModifyWebCacheCustomRule	要执行的操作。取值：**ModifyWebCacheCustomRule**

名称	类型	是否必选	示例值	描述
Domain	String	是	www.aliyun.com	网站业务的域名。  **说明:** 域名必须已配置网站业务转发规则且关联了增强功能套餐的DDoS高防实例。您可以调用DescribeDomains查询所有域名。
Rules	String	是	[{"Name": "test","Uri": "/a","Mode": "standard","CacheTtl": 3600}]	静态页面缓存的自定义规则信息，使用JSON格式的字符串表述，具体结构如下。 • **Name**：String类型，必选，规则名称。 • **Uri**：String类型，必选，缓存页面的路径。 • **Mode**：String类型，必选，缓存模式。取值： - **standard**：标准模式 - **aggressive**：强力模式 - **bypass**：不缓存 • **CacheTtl**：Integer类型，必选，页面缓存的过期时间。单位：秒。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=ModifyWebCacheCustomRule
&Domain=www.aliyun.com
&Rules=[{"Name": "test","Uri": "/a","Mode": "standard","CacheTtl": 3600}]
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.14.4 DeleteWebCacheCustomRule

调用DeleteWebCacheCustomRule删除网站业务静态页面缓存的自定义规则。

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	DeleteWebCacheCustomRule	要执行的操作。取值：**DeleteWebCacheCustomRule**

名称	类型	是否必选	示例值	描述
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明:** 域名必须已配置网站业务转发规则且关联了增强功能套餐的DDoS高防实例。您可以调用DescribeDomains查询所有域名。
RuleNames.N	RepeatList	是	test	要删除的规则的名称。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值: • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=DeleteWebCacheCustomRule
&Domain=www.aliyun.com
&RuleNames.1=test
&<公共请求参数>
```

正常返回示例

XML 格式

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

```
</DeleteWebCacheCustomRuleResponse>
```

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。

13.14.5 DescribeWebCacheConfigs

调用DescribeWebCacheConfigs查询网站业务静态页面缓存的配置。

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	DescribeWebCacheConfigs	要执行的操作。取值：**DescribeWebCacheConfigs**
Domains.N	RepeatList	是	www.aliyun.com	网站业务的域名。 **说明:** 域名必须已配置网站业务转发规则且关联了增强功能套餐的DDoS高防实例。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
DomainCacheConfigs	Array		静态页面缓存的配置信息。
CustomRules	Array		自定义规则信息。
CacheTtl	Long	86400	页面缓存的过期时间。单位：秒。
Mode	String	standard	缓存模式。取值： • **standard**：标准模式 • **aggressive**：强力模式 • **bypass**：不缓存
Name	String	c1	规则名称。
Uri	String	/blog/	缓存页面的路径。
Domain	String	www.aliyun.com	网站域名。
Enable	Integer	1	开关状态。取值： • **1**：开启 • **0**：关闭
Mode	String	bypass	缓存模式。取值： • **standard**：标准模式 • **aggressive**：强力模式 • **bypass**：不缓存
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeWebCacheConfigs
&Domains.1=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeWebCacheConfigsResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
  <DomainCacheConfigs>
    <Domain>www.aliyun.com</Domain>
    <Enable>1</Enable>
    <Mode>bypass</Mode>
    <CustomRules>
      <Name>c1</Name>
      <Uri>/blog/</Uri>
      <Mode>standard</Mode>
      <CacheTtl>86400</CacheTtl>
    </CustomRules>
  </DomainCacheConfigs>
</DescribeWebCacheConfigsResponse>
```

JSON 格式

```
{
   "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "DomainCacheConfigs": [
     {
       "Domain": "www.aliyun.com",
       "Enable": 1,
       "Mode": "bypass",
       "CustomRules": [
         {
           "Name": "c1",
           "Uri": "/blog/",
           "Mode": "standard",
           "CacheTtl": 86400
         }
       ]
     }
   ]
}
```

错误码

访问错误中心查看更多错误码。

13.15 监控报表

13.15.1 DescribeDDoSEvents

调用DescribeDDoSEvents查询针对DDoS高防实例的攻击事件。

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	DescribeDDoSEvents	要执行的操作。取值：**DescribeDDoSEvents**
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。  **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
PageNumber	Integer	是	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写**1**。
PageSize	Integer	是	10	页面显示的记录数量。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。  **说明：** 必须为整点分钟。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
EndTime	Long	否	1583683200	查询结束时间。时间戳格式，单位：秒。  **说明：** 必须为整点分钟。

返回数据

名称	类型	示例值	描述
DDoSEvents	Array		DDoS攻击事件列表。
Bps	Long	0	攻击流量带宽大小。单位：bps。
EndTime	Long	1583933330	攻击结束时间。时间戳格式，单位：秒。
EventType	String	blackhole	攻击事件类型。取值： • **defense**：清洗事件 • **blackhole**：黑洞事件
Ip	String	203.***.***.132	攻击来源IP。
Port	String	80	被攻击端口。
Pps	Long	0	攻击流量包转发率。单位：pps。
Region	String	cn	攻击来源地区。取值： • **cn**：中国内地 • **alb-ap-northeast-1-gf-x**：日本 • **alb-ap-southeast-gf-x**：新加坡 • **alb-cn-hongkong-gf-x**：中国香港 • **alb-eu-central-1-gf-x**：德国 • **alb-us-west-1-gf-x**：美国西部 **说明：** **cn**以外的取值只有在DDoS高防（国际）服务（**RegionId**为**ap-southeast-1**）中提供。
StartTime	Long	1583933277	攻击开始时间。时间戳格式，单位：秒。
RequestId	String	0CA72AF5-1795-4350-8C77-50A448A2F334	本次请求的ID。
Total	Long	1	攻击事件总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDDoSEvents
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&PageNumber=1
&PageSize=10
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeDDoSEventsResponse>
  <RequestId>0CA72AF5-1795-4350-8C77-50A448A2F334</RequestId>
  <Total>1</Total>
  <DDoSEvents>
    <Pps>0</Pps>
    <Bps>0</Bps>
    <EndTime>1583933330</EndTime>
    <EventType>blackhole</EventType>
    <Ip>203.***.***.132</Ip>
    <Port></Port>
    <StartTime>1583933277</StartTime>
  </DDoSEvents>
</DescribeDDoSEventsResponse>
```

JSON 格式

```
{
 "RequestId": "0CA72AF5-1795-4350-8C77-50A448A2F334",
 "Total": 1,
 "DDoSEvents": [
  {
   "Pps": 0,
   "Bps": 0,
   "EndTime": 1583933330,
   "EventType": "blackhole",
   "Ip": "203.***.***.132",
   "Port": "",
   "StartTime": 1583933277
  }
 ]
}
```

错误码

访问错误中心查看更多错误码。

13.15.2 DescribePortFlowList

调用DescribePortFlowList查询DDoS高防实例的流量数据列表。

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	DescribePortFlowList	要执行的操作。取值：**DescribePortFlowList**
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
Interval	Integer	是	1000	返回数据的步长，单位为秒，即每隔多少秒返回一个结果。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

名称	类型	是否必选	示例值	描述
ResourceGroupId	String	否	null	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
PortFlowList	Array		流量数据。
AttackBps	Long	0	攻击带宽，单位：bps。
AttackPps	Long	0	攻击包转发率，单位：pps。
InBps	Long	2176000	入方向带宽，单位：bps。
InPps	Long	2934	入方向包转发率，单位：pps。
Index	Long	0	返回数据的索引号。
OutBps	Long	4389	出方向带宽，单位：bps。
OutPps	Long	5	出方向包转发率，单位：pps。
Region	String	cn	访问流量来源地区。取值： • **cn**：中国内地 • **alb-ap-northeast-1-gf-x**：日本 • **alb-ap-southeast-gf-x**：新加坡 • **alb-cn-hongkong-gf-x**：中国香港 • **alb-eu-central-1-gf-x**：德国 • **alb-us-west-1-gf-x**：美国西部 **说明：** **cn**以外的取值只有在DDoS高防（国际）服务（**RegionId**为**ap-southeast-1**）中提供。
Time	Long	1582992000	统计时间。时间戳格式，单位：秒。

名称	类型	示例值	描述
RequestId	String	FFC77501-BDF8-4BC8-9BF5-B295FBC3189B	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePortFlowList
&EndTime=1583683200
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&Interval=1000
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribePortFlowListResponse>
  <RequestId>FFC77501-BDF8-4BC8-9BF5-B295FBC3189B</RequestId>
  <PortFlowList>
    <OutPps>5</OutPps>
    <OutBps>4389</OutBps>
    <InBps>2176000</InBps>
    <InPps>2934</InPps>
    <Region>cn</Region>
    <Index>0</Index>
    <AttackBps>0</AttackBps>
    <AttackPps>0</AttackPps>
        <Time>1582992000</Time>
  </PortFlowList>
  <PortFlowList>
    <OutPps>5</OutPps>
    <OutBps>4155</OutBps>
    <InBps>4648000</InBps>
    <InPps>6268</InPps>
    <Region>cn</Region>
    <Index>1</Index>
    <AttackBps>0</AttackBps>
    <AttackPps>0</AttackPps>
        <Time>1582993000</Time>
  </PortFlowList>
</DescribePortFlowListResponse>
```

`JSON` 格式

```
{
 "RequestId": "FFC77501-BDF8-4BC8-9BF5-B295FBC3189B",
 "PortFlowList": [
  {
   "OutPps": 5,
   "OutBps": 4389,
   "InBps": 2176000,
   "InPps": 2934,
   "Region": "cn",
```

```
  "Index": 0,
  "AttackBps": 0,
  "AttackPps": 0,
        "Time": 1582992000
 },
 {
  "OutPps": 5,
  "OutBps": 4155,
  "InBps": 4648000,
  "InPps": 6268,
  "Region": "cn",
  "Index": 1,
  "AttackBps": 0,
  "AttackPps": 0,
        "Time": 1582993000
 }
]
}
```


错误码

访问错误中心查看更多错误码。

13.15.3 DescribePortConnsList

调用DescribePortConnsList查询DDoS高防实例的端口连接数列表。

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	DescribePortConnsList	要执行的操作。取值：**DescribePortConnsList**
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。

名称	类型	是否必选	示例值	描述
Interval	Integer	是	1000	返回数据的步长，单位为秒，即每隔多少秒返回一个结果。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 **说明:** 必须为整点分钟。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
Port	String	否	null	要查询的端口号。不传入表示查询所有端口。

返回数据

名称	类型	示例值	描述
ConnsList	Array		端口连接数据列表。
ActConns	Long	2	活跃连接数。
Conns	Long	20	并发连接数。
Cps	Long	0	新建连接数。
InActConns	Long	4	不活跃连接数。
Index	Long	0	返回数据的索引。
Time	Long	1582992000	统计时间。时间戳格式，单位：秒。

名称	类型	示例值	描述
RequestId	String	7E6BF16F-27A9-49BC-AD18-F79B409DE753	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePortConnsList
&EndTime=1583683200
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&Interval=1000
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribePortConnsListResponse>
  <ConnsList>
    <Conns>20</Conns>
    <Cps>0</Cps>
    <Index>0</Index>
    <ActConns>2</ActConns>
    <InActConns>4</InActConns>
        <Time>1582992000</Time>
  </ConnsList>
  <ConnsList>
    <Conns>24</Conns>
    <Cps>0</Cps>
    <Index>1</Index>
    <ActConns>2</ActConns>
    <InActConns>5</InActConns>
        <Time>1582993000</Time>
  </ConnsList>
  <RequestId>7E6BF16F-27A9-49BC-AD18-F79B409DE753</RequestId>
</DescribePortConnsListResponse>
```

JSON 格式

```
{
 "ConnsList": [
  {
   "Conns": 20,
   "Cps": 0,
   "Index": 0,
   "ActConns": 2,
   "InActConns": 4,
         "Time": 1582992000
  },
  {
   "Conns": 24,
   "Cps": 0,
   "Index": 1,
   "ActConns": 2,
```

```
  "InActConns": 5,
        "Time": 1582993000
 }
 ],
 "RequestId": "7E6BF16F-27A9-49BC-AD18-F79B409DE753"
}
```


错误码

访问错误中心查看更多错误码。

13.15.4 DescribePortConnsCount

调用DescribePortConnsCount查询DDoS高防实例的端口连接数统计信息。

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	DescribePortConnsCount	要执行的操作。取值：**DescribePortConnsCount**
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
Port	String	否	80	要查询的端口号。不传入该参数表示查询所有端口号。

返回数据

名称	类型	示例值	描述
ActConns	Long	159	活跃的连接数量。
Conns	Long	46340	并发连接数量。
Cps	Long	0	新建连接数量。
InActConns	Long	121	不活跃的连接数量。
RequestId	String	48859E14-A9FB-4100-99FF-AAB75CA46776	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePortConnsCount
&EndTime=1583683200
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribePortConnsCountResponse>
```

```
  <Conns>46340</Conns>
  <RequestId>48859E14-A9FB-4100-99FF-AAB75CA46776</RequestId>
  <Cps>0</Cps>
  <ActConns>159</ActConns>
  <InActConns>121</InActConns>
</DescribePortConnsCountResponse>
```

JSON 格式

```
{
 "Conns": 46340,
 "RequestId": "48859E14-A9FB-4100-99FF-AAB75CA46776",
 "Cps": 0,
 "ActConns": 159,
 "InActConns": 121
}
```

错误码

访问错误中心查看更多错误码。

13.15.5 DescribePortMaxConns

调用DescribePortMaxConns查询DDoS高防实例的端口连接峰值信息。

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	DescribePortMaxConns	要执行的操作。取值：**DescribePortMaxConns**。
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。

名称	类型	是否必选	示例值	描述
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 **说明:** 必须为整点分钟。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
PortMaxConns	Array		DDoS高防实例的端口连接峰值信息。
Cps	Long	100	最大每秒连接数。
Ip	String	203.***.***.117	DDoS高防实例的IP。
Port	String	80	DDoS高防实例的端口。
RequestId	String	08F79110-2AF5-4FA7-998E-7C5E75EACF9C	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePortMaxConns
&EndTime=1583683200
&InstanceIds.1= ddoscoo-cn-mp91j1ao****
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribePortMaxConnsResponse>
  <PortMaxConns>
    <Port>80</Port>
    <Ip>203.***.***.117</Ip>
    <Cps>0</Cps>
  </PortMaxConns>
  <PortMaxConns>
    <Port>443</Port>
    <Ip>203.***.***.117</Ip>
    <Cps>0</Cps>
  </PortMaxConns>
  <RequestId>08F79110-2AF5-4FA7-998E-7C5E75EACF9C</RequestId>
</DescribePortMaxConnsResponse>
```

JSON 格式

```
{
 "PortMaxConns": [
  {
   "Port": "80",
   "Ip": "203.***.***.117",
   "Cps": 0
  },
  {
   "Port": "443",
   "Ip": "203.***.***.117",
   "Cps": 0
  }
 ],
 "RequestId": "08F79110-2AF5-4FA7-998E-7C5E75EACF9C"
}
```

错误码

访问错误中心查看更多错误码。

13.15.6 DescribePortAttackMaxFlow

调用DescribePortAttackMaxFlow查询指定时间段内DDoS高防受到的攻击带宽和包速峰值。

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	DescribePortAttackMaxFlow	要执行的操作。取值：**DescribePortAttackMaxFlow**

名称	类型	是否必选	示例值	描述
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
Bps	Long	149559	攻击带宽峰值。单位：bps。
Pps	Long	23	攻击包速峰值。单位：pps。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePortAttackMaxFlow
&EndTime=1583683200
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribePortAttackMaxFlowResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <Bps>149559</Bps>
  <Pps>23</Pps>
</DescribePortAttackMaxFlowResponse>
```

JSON 格式

```
{
   "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
   "Bps": 149559,
   "Pps": 23
}
```

错误码

访问错误中心查看更多错误码。

13.15.7 DescribePortViewSourceCountries

调用DescribePortViewSourceCountries查询指定时间段内DDoS高防实例的请求来源国家分布。

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	DescribePortViewSourceCountries	要执行的操作。取值：**DescribePortViewSourceCountries**。

名称	类型	是否必选	示例值	描述
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。  **说明：** 必须为整点分钟。
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。  **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。  **说明：** 必须为整点分钟。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
SourceCountrys	Array		DDoS高防实例的请求来源国家信息。
Count	Long	3390671	请求数量。

名称	类型	示例值	描述
CountryId	String	cn	国家简称。详见中国和海外地区代码中的**海外地区代码**说明。例如，**cn**表示中国，**us**表示美国。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePortViewSourceCountries
&EndTime=1583683200
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribePortViewSourceCountriesResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <SourceCountries>
    <Count>3390671</Count>
    <CountryId>cn</CountryId>
  </SourceCountries>
</DescribePortViewSourceCountriesResponse>
```

JSON 格式

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "SourceCountries": [
    {
      "Count": 3390671,
      "CountryId": "cn"
    }
  ]
}
```

错误码

访问错误中心查看更多错误码。

13.15.8 DescribePortViewSourceIsps

调用DescribePortViewSourceIsps查询指定时间段内DDoS高防实例的请求来源运营商分布。

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	DescribePortViewSourceIsps	要执行的操作。取值：**DescribePortViewSourceIsps**
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。不传入表示使用当前时间作为结束时间。  **说明：** 必须为整点分钟。
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。  **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。  **说明：** 必须为整点分钟。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
Isps	Array		DDoS高防实例的请求来源运营商信息。

名称	类型	示例值	描述
Count	Long	3390671	请求数量。
IspId	String	100017	运营商ID。详见返回参数表下的运营商代码说明，运营商ID对应表中的代码。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

运营商代码

代码	运营商
100017	电信
100026	联通
100025	移动
100027	教育网
100020	铁通
1000143	鹏博士
100080	歌华
1000139	广电
100023	有线通
100063	方正宽带
1000337	皓宽网络
100021	世纪互联
1000333	华数传媒
100093	网宿

代码	运营商
1000401	腾讯
100099	百度
1000323	阿里云
100098	阿里巴巴

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePortViewSourceIsps
&EndTime=1583683200
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribePortViewSourceIspsResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <Isps>
    <Count>3390671</Count>
    <IspId>100017</IspId>
  </Isps>
</DescribePortViewSourceIspsResponse>
```

JSON 格式

```
{
   "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
   "Isps": [
      {
         "Count": 3390671,
         "IspId": "100017"
      }
   ]
}
```

错误码

访问错误中心查看更多错误码。

13.15.9 DescribePortViewSourceProvinces

调用DescribePortViewSourceProvinces查询指定时间段内DDoS高防实例的请求来源（中国）省份分布。

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	DescribePortViewSourceProvinces	要执行的操作。取值：**DescribePortViewSourceProvinces**。
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

名称	类型	是否必选	示例值	描述
EndTime	Long	否	1583683200	查询结束时间。时间戳格式，单位：秒。不传入表示使用当前时间作为结束时间。  **说明：** 必须为整点分钟。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
SourceProvinces	Array		DDoS高防实例的请求来源（中国）省份信息。
Count	Long	3390671	请求数量。
ProvinceId	String	440000	省份ID。详见中国和海外地区代码中的**中国地区代码**说明。例如，**110000**表示北京市，**120000**表示天津市。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePortViewSourceProvinces
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribePortViewSourceProvincesResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <SourceProvinces>
    <Count>3390671</Count>
    <ProvinceId>440000</ProvinceId>
  </SourceProvinces>
```

```
</DescribePortViewSourceProvincesResponse>
```

JSON 格式

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "SourceProvinces": [
    {
      "Count": 3390671,
      "ProvinceId": "440000"
    }
  ]
}
```

错误码

访问错误中心查看更多错误码。

13.15.10 DescribeDomainAttackEvents

调用DescribeDomainAttackEvents查询针对网站业务的攻击事件。

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	要执行的操作。取值：**DescribeDomainAttackEvents**
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 **说明:** 必须为整点分钟
PageNumber	Integer	是	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写**1**。
PageSize	Integer	是	10	页面显示的记录数量。

名称	类型	是否必选	示例值	描述
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
Domain	String	否	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

返回数据

名称	类型	示例值	描述
DomainAttackEvents	Array		网站业务DDoS攻击事件信息。
Domain	String	www.aliyun.com	被攻击域名。
EndTime	Long	1560320160	攻击结束时间。时间戳格式，单位：秒。
MaxQps	Long	1000	攻击峰值QPS。
StartTime	Long	1560312900	攻击开始时间。时间戳格式，单位：秒。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

名称	类型	示例值	描述
TotalCount	Long	1	攻击事件的总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainAttackEvents
&EndTime=1583683200
&PageNumber=1
&PageSize=10
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDomainAttackEventsResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <TotalCount>1</TotalCount>
  <DomainAttackEvents>
    <Domain>www.aliyun.com</Domain>
    <MaxQps>1000</MaxQps>
    <StartTime>1560312900</StartTime>
    <EndTime>1560320160</EndTime>
  </DomainAttackEvents>
</DescribeDomainAttackEventsResponse>
```

`JSON` 格式

```
{
   "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
   "TotalCount": 1,
   "DomainAttackEvents": [{
      "Domain": "www.aliyun.com",
      "MaxQps": 1000,
      "StartTime": 1560312900,
      "EndTime": 1560320160
    }]
}
```

错误码

访问错误中心查看更多错误码。

13.15.11 DescribeDomainQPSList

调用DescribeDomainQPSList查询网站业务的QPS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	DescribeDomainQPSList	要执行的操作。取值：**DescribeDomainQPSList**
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。
Interval	Long	是	1000	返回数据的步长，单位为秒，即每隔多少秒返回一个结果。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

名称	类型	是否必选	示例值	描述
Domain	String	否	www.aliyun.com	网站业务的域名。不传入表示查询所有域名的QPS统计信息。  **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

返回数据

名称	类型	示例值	描述
DomainQPSList	Array		网站业务QPS统计信息。
AttackQps	Long	1	攻击QPS。
CacheHits	Long	0	缓存命中数。
Index	Long	0	返回数据的索引号。
MaxAttackQps	Long	37	攻击QPS峰值。
MaxNormalQps	Long	93	正常QPS峰值。
MaxQps	Long	130	总QPS峰值。
Time	Long	1582992000	统计时间。时间戳格式，单位：秒。
TotalCount	Long	20008	总访问次数。
TotalQps	Long	1	总QPS。
RequestId	String	327F2ABB-104D-437A-AAB5-D633E29A8C51	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainQPSList
&Interval=1000
```

```
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDomainQPSListResponse>
  <DomainQPSList>
    <MaxAttackQps>37</MaxAttackQps>
    <TotalQps>1</TotalQps>
    <TotalCount>20008</TotalCount>
    <MaxQps>130</MaxQps>
    <MaxNormalQps>93</MaxNormalQps>
    <AttackQps>1</AttackQps>
    <Index>0</Index>
    <Time>1582992000</Time>
    <CacheHits>0</CacheHits>
  </DomainQPSList>
  <RequestId>327F2ABB-104D-437A-AAB5-D633E29A8C51</RequestId>
</DescribeDomainQPSListResponse>
```

`JSON` 格式

```
{
 "DomainQPSList": [
  {
   "MaxAttackQps": 37,
   "TotalQps": 1,
   "TotalCount": 20008,
   "MaxQps": 130,
   "MaxNormalQps": 93,
   "AttackQps": 1,
   "Index": 0,
   "Time": 1582992000,
   "CacheHits": 0
  }
 ],
 "RequestId": "327F2ABB-104D-437A-AAB5-D633E29A8C51"
}
```

错误码

访问错误中心查看更多错误码。

13.15.12 DescribeDomainStatusCodeList

调用DescribeDomainStatusCodeList查询网站业务的响应状态码统计信息。

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	DescribeDomainStatusCodeList	要执行的操作。取值：**DescribeDomainStatusCodeList**
Interval	Long	是	1000	返回数据的步长，单位为秒，即每隔多少秒返回一个结果。
QueryType	String	是	gf	查询数据的来源。取值： • **gf**：高防响应 • **upstrem**：源站响应
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。  **说明：** 必须为整点分钟。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
EndTime	Long	否	1583683200	查询结束时间。时间戳格式，单位：秒。  **说明：** 必须为整点分钟。

名称	类型	是否必选	示例值	描述
Domain	String	否	www.aliyun.com	网站业务的域名。不传入表示查询所有域名的响应状态码统计信息。 **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

返回数据

名称	类型	示例值	描述
RequestId	String	3B63C0DD-8AC5-44B2-95D6-064CA9296B9C	本次请求的ID。
StatusCodeList	Array		响应状态码的统计信息。
Index	Integer	0	返回数据的索引号。
Status200	Long	15520	200状态码的统计值。
Status2XX	Long	15520	2XX类状态码的统计值。
Status3XX	Long	0	3XX类状态码的统计值。
Status403	Long	0	403状态码的统计值。
Status404	Long	0	404状态码的统计值。
Status405	Long	0	405状态码的统计值。
Status4XX	Long	4486	4XX类状态码的统计值。
Status501	Long	0	501状态码的统计值。
Status502	Long	0	502状态码的统计值。
Status503	Long	0	503状态码的统计值。

名称	类型	示例值	描述
Status504	Long	0	504状态码的统计值。
Status5XX	Long	0	5XX类状态码的统计值。
Time	Long	1582992000	统计时间。时间戳格式，单位：秒。

示例

请求示例

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

正常返回示例

`XML` 格式

```
<DescribeDomainStatusCodeListResponse>
  <RequestId>3B63C0DD-8AC5-44B2-95D6-064CA9296B9C</RequestId>
  <StatusCodeList>
    <Status501>0</Status501>
    <Status502>0</Status502>
    <Status403>0</Status403>
    <Index>0</Index>
    <Time>1582992000</Time>
    <Status503>0</Status503>
    <Status404>0</Status404>
    <Status504>0</Status504>
    <Status405>0</Status405>
    <Status2XX>15520</Status2XX>
    <Status200>15520</Status200>
    <Status3XX>0</Status3XX>
    <Status4XX>4486</Status4XX>
    <Status5XX>0</Status5XX>
  </StatusCodeList>
</DescribeDomainStatusCodeListResponse>
```

`JSON` 格式

```
{
 "RequestId": "3B63C0DD-8AC5-44B2-95D6-064CA9296B9C",
 "StatusCodeList": [
  {
   "Status501": 0,
   "Status502": 0,
   "Status403": 0,
   "Index": 0,
   "Time": 1582992000,
   "Status503": 0,
   "Status404": 0,
   "Status504": 0,
   "Status405": 0,
   "Status2XX": 15520,
```

```
  "Status200": 15520,
  "Status3XX": 0,
  "Status4XX": 4486,
  "Status5XX": 0
 }
]
}
```

错误码

访问错误中心查看更多错误码。

13.15.13 DescribeDomainOverview

调用DescribeDomainOverview查询网站业务攻击总览，包括HTTP攻击峰值、HTTPS攻击峰值。

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	DescribeDomainOverview	要执行的操作。取值：**DescribeDomainOverview**
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 **说明:** 必须为整点分钟。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

名称	类型	是否必选	示例值	描述
EndTime	Long	否	1583683200	查询结束时间。时间戳格式，单位：秒。不传入表示使用当前时间作为结束时间。 **说明：** 必须为整点分钟。
Domain	String	否	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

返回数据

名称	类型	示例值	描述
MaxHttp	Long	1000	HTTP攻击峰值。单位：qps。
MaxHttps	Long	1000	HTTPS攻击峰值。单位：qps。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainOverview
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeDomainOverviewResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <MaxHttps>1000</MaxHttps>
  <MaxHttp>1000</MaxHttp>
```

```
</DescribeDomainOverviewResponse>
```

JSON 格式

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "MaxHttps": 1000,
  "MaxHttp": 1000
}
```

错误码

访问错误中心查看更多错误码。

13.15.14 DescribeDomainStatusCodeCount

调用DescribeDomainStatusCodeCount查询指定时间段内网站业务的各类响应状态码的统计信息。

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	DescribeDomainStatusCodeCount	要执行的操作。取值：**DescribeDomainStatusCodeCount**
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
Domain	String	否	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
Status200	Long	951159	查询时间段内200状态码的数量。
Status2XX	Long	951472	查询时间段内2XX类状态码的数量。
Status3XX	Long	133209	查询时间段内3XX状态码的数量。
Status403	Long	0	查询时间段内403状态码的数量。
Status404	Long	897	查询时间段内404状态码的数量。
Status405	Long	0	查询时间段内405状态码的数量。
Status4XX	Long	5653	查询时间段内4XX状态码的数量。
Status501	Long	0	查询时间段内501状态码的数量。
Status502	Long	0	查询时间段内502状态码的数量。
Status503	Long	0	查询时间段内503状态码的数量。

名称	类型	示例值	描述
Status504	Long	0	查询时间段内504状态码的数量。
Status5XX	Long	14	查询时间段内5XX状态码的数量。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainStatusCodeCount
&EndTime=1583683200
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDomainStatusCodeCountResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <Status2XX>951472</Status2XX>
  <Status200>951159</Status200>
  <Status3XX>133209</Status3XX>
  <Status4XX>5653</Status4XX>
  <Status403>0</Status403>
  <Status404>897</Status404>
  <Status405>0</Status405>
  <Status5XX>14</Status5XX>
  <Status501>0</Status501>
  <Status502>0</Status502>
  <Status503>0</Status503>
  <Status504>0</Status504>
</DescribeDomainStatusCodeCountResponse>
```

`JSON` 格式

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "Status2XX": 951472,
  "Status200": 951159,
  "Status3XX": 133209,
  "Status4XX": 5653,
  "Status403": 0,
  "Status404": 897,
  "Status405": 0,
  "Status5XX": 14,
  "Status501": 0,
  "Status502": 0,
  "Status503": 0,
  "Status504": 0
}
```

错误码

访问错误中心查看更多错误码。

13.15.15 DescribeDomainTopAttackList

调用DescribeDomainTopAttackList查询指定时间段内网站业务的QPS峰值数据，包括攻击QPS、总QPS。

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	DescribeDomainTopAttackList	要执行的操作。取值：**DescribeDomainTopAttackList**
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
AttackList	Array		网站业务的QPS峰值数据。
Attack	Long	0	攻击QPS。单位：qps。
Count	Long	294	全部QPS，包含正常业务请求和攻击。单位：qps。
Domain	String	www.aliyun.com	网站域名。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainTopAttackList
&EndTime=1583683200
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDomainTopAttackListResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <AttackList>
    <Count>294</Count>
    <Attack>0</Attack>
    <Domain>www.aliyun.com</Domain>
  </AttackList>
</DescribeDomainTopAttackListResponse>
```

`JSON` 格式

```
{
   "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
   "AttackList": [
      {
         "Count": 294,
         "Attack": 0,
         "Domain": "www.aliyun.com"
      }
   ]
```

```
}
```

错误码

访问错误中心查看更多错误码。

13.15.16 DescribeDomainViewSourceCountries

调用DescribeDomainViewSourceCountries查询指定时间段内网站业务的请求来源国家分布。

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	DescribeDomainViewSourceCountries	要执行的操作。取值：**DescribeDomainViewSourceCountries**。
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 **说明:** 必须为整点分钟。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 **说明:** 必须为整点分钟。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

名称	类型	是否必选	示例值	描述
Domain	String	否	www.aliyun.com	网站业务的域名。 **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
SourceCountrys	Array		网站业务的请求来源国家信息。
Count	Long	3390671	请求数量。
CountryId	String	cn	国家简称。详见中国和海外地区代码中的**海外地区代码**说明。例如，**cn**表示中国，**us**表示美国。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainViewSourceCountries
&EndTime=1583683200
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeDomainViewSourceCountriesResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <SourceCountries>
    <Count>3390671</Count>
    <CountryId>cn</CountryId>
  </SourceCountries>
```

```
</DescribeDomainViewSourceCountriesResponse>
```

JSON 格式

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "SourceCountries": [
    {
      "Count": 3390671,
      "CountryId": "cn"
    }
  ]
}
```

错误码

访问错误中心查看更多错误码。

13.15.17 DescribeDomainViewSourceProvinces

调用DescribeDomainViewSourceProvinces查询指定时间段内网站业务的请求来源（中国）省份分布。

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	DescribeDomainViewSourceProvinces	要执行的操作。取值：**DescribeDomainViewSourceProvinces**。
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。

名称	类型	是否必选	示例值	描述
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
Domain	String	否	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
SourceProvinces	Array		网站业务的请求来源（中国）省份信息。
Count	Long	3390671	请求数量。
ProvinceId	String	440000	省份ID。详见中国和海外地区代码中的**中国地区代码**说明。例如，**110000**表示北京市，**120000**表示天津市。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainViewSourceProvinces
&EndTime=1583683200
&StartTime=1582992000
```

```
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeDomainViewSourceProvincesResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <SourceProvinces>
    <Count>3390671</Count>
    <ProvinceId>440000</ProvinceId>
  </SourceProvinces>
</DescribeDomainViewSourceProvincesResponse>
```

JSON 格式

```
{
   "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
   "SourceProvinces": [
     {
        "Count": 3390671,
        "ProvinceId": "440000"
     }
   ]
}
```

错误码

访问错误中心查看更多错误码。

13.15.18 DescribeDomainViewTopCostTime

调用DescribeDomainViewTopCostTime查询指定时间段内网站业务的请求耗时最大的前N个URL。

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	DescribeDomainViewTopCostTime	要执行的操作。取值：**DescribeDomainViewTopCostTime**
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。

名称	类型	是否必选	示例值	描述
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 **说明：** 必须为整点分钟。
Top	Integer	是	5	返回URL的数量。取值范围：**1~100**。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
Domain	String	否	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
UrlList	Array		请求耗时TOP URL列表。
CostTime	Float	3000	请求延时时长。单位：毫秒。
Domain	String	www.aliyun.com	网站域名。

名称	类型	示例值	描述
Url	String	Lw==	URL。使用BASE64加密表示。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainViewTopCostTime
&EndTime=1583683200
&StartTime=1582992000
&Top=5
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDomainViewTopCostTimeResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <UrlList>
    <CostTime>3000</CostTime>
    <Domain>www.aliyun.com</Domain>
    <Url>Lw==</Url>
  </UrlList>
</DescribeDomainViewTopCostTimeResponse>
```

`JSON` 格式

```
{
   "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
   "UrlList": [
     {
        "CostTime": 3000,
        "Domain": "www.aliyun.com",
        "Url": "Lw=="
     }
   ]
}
```

错误码

访问错误中心查看更多错误码。

13.15.19 DescribeDomainViewTopUrl

调用DescribeDomainViewTopUrl查询指定时间段内网站业务访问量最大的前N个URL。

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	DescribeDomainViewTopUrl	要执行的操作。取值：**DescribeDomainViewTopUrl**
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。  **说明：** 必须为整点分钟。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。  **说明：** 必须为整点分钟。
Top	Integer	是	5	返回URL的数量。取值：**1~100**。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
Domain	String	否	www.aliyun.com	网站业务的域名。  **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
UrlList	Array		网站业务的访问量TOP URL列表。
Count	Long	3390671	请求数量。
Domain	String	www.aliyun.com	网站域名。
Url	String	Lw==	URL。使用BASE64加密表示。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainViewTopUrl
&EndTime=1583683200
&StartTime=1582992000
&Top=5
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDomainViewTopUrlResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <UrlList>
    <Count>3390671</Count>
    <Domain>www.aliyun.com</Domain>
    <Url>Lw==</Url>
  </UrlList>
</DescribeDomainViewTopUrlResponse>
```

`JSON` 格式

```
{
   "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
   "UrlList": [
      {
         "Count": 3390671,
         "Domain": "www.aliyun.com",
         "Url": "Lw=="
      }
   ]
```

```
}
```

错误码

访问错误中心查看更多错误码。

13.15.20 DescribeDomainQpsWithCache

调用DescribeDomainQpsWithCache查询网站业务的QPS数据列表，例如总QPS、由不同防护功能阻断的QPS、缓存命中数等。

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	要执行的操作。取值：**DescribeDomainQpsWithCache**
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 **说明:** 必须为整点分钟。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 **说明:** 必须为整点分钟。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

名称	类型	是否必选	示例值	描述
Domain	String	否	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

返回数据

名称	类型	示例值	描述
Blocks	List	[20,30,20]	攻击QPS。
CacheHits	List	[0.3,0.4,0.5]	缓存命中率。使用小数表示，例如0.5表示缓存命中率是50%。
CcBlockQps	List	[1,0,0]	由频率控制阻断的QPS。
CcJsQps	List	[1,0,0]	由频率控制触发人机识别的QPS。
Interval	Integer	20384	返回数据的步长，单位为秒，即相邻两个数据的时间差。
IpBlockQps	List	[1,0,0]	由黑名单（针对域名）阻断的QPS。
PreciseBlocks	List	[1,0,0]	由精确访问控制阻断的QPS。
PreciseJsQps	List	[1,0,0]	由精确访问控制触发挑战的QPS。
RegionBlocks	List	[1,0,0]	由区域封禁阻断的QPS。
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。
StartTime	Long	1582992000	开始时间。时间戳格式，单位：秒。
Totals	List	[100,400,200]	总QPS。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainQpsWithCache
&EndTime=1583683200
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeDomainQpsWithCacheResponse>
  <Interval>20384</Interval>
  <StartTime>1582992000</StartTime>
  <Totals>100</Totals>
  <Totals>400</Totals>
  <Totals>200</Totals>
  <Blocks>20</Blocks>
  <Blocks>30</Blocks>
  <Blocks>20</Blocks>
  <CacheHits>0.3</CacheHits>
  <CacheHits>0.4</CacheHits>
  <CacheHits>0.5</CacheHits>
  <CcBlockQps>1</CcBlockQps>
  <CcBlockQps>0</CcBlockQps>
  <CcBlockQps>0</CcBlockQps>
  <CcJsQps>1</CcJsQps>
  <CcJsQps>0</CcJsQps>
  <CcJsQps>0</CcJsQps>
  <IpBlockQps>1</IpBlockQps>
  <IpBlockQps>0</IpBlockQps>
  <IpBlockQps>0</IpBlockQps>
  <PreciseBlocks>1</PreciseBlocks>
  <PreciseBlocks>0</PreciseBlocks>
  <PreciseBlocks>0</PreciseBlocks>
  <PreciseJsQps>1</PreciseJsQps>
  <PreciseJsQps>0</PreciseJsQps>
  <PreciseJsQps>0</PreciseJsQps>
  <RegionBlocks>1</RegionBlocks>
  <RegionBlocks>0</RegionBlocks>
  <RegionBlocks>0</RegionBlocks>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeDomainQpsWithCacheResponse>
```

JSON 格式

```
{
    "Interval": 20384,
    "StartTime": 1582992000,
    "Totals": [
        100,
        400,
        200
    ],
    "Blocks": [
        20,
        30,
        20
```

```
    ],
    "CacheHits": [
        0.3,
        0.4,
        0.5
    ],
    "CcBlockQps": [
        1,
        0,
        0
    ],
    "CcJsQps": [
        1,
        0,
        0
    ],
    "IpBlockQps": [
        1,
        0,
        0
    ],
    "PreciseBlocks": [
        1,
        0,
        0
    ],
    "PreciseJsQps": [
        1,
        0,
        0
    ],
    "RegionBlocks": [
        1,
        0,
        0
    ],
    "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```


错误码

访问错误中心查看更多错误码。

13.16 全量日志分析

13.16.1 DescribeSlsOpenStatus

调用DescribeSlsOpenStatus查询阿里云日志服务SLS的开通状态。

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	DescribeSlsOpenStatus	要执行的操作。取值：**DescribeSlsOpenStatus**
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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。取值： • **true**：已开通 • **false**：未开通

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

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

```
</DescribeSlsOpenStatusResponse>
```

JSON 格式

```
{
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
  "SlsOpenStatus": true
}
```

错误码

访问错误中心查看更多错误码。

13.16.2 DescribeSlsAuthStatus

调用DescribeSlsAuthStatus查询DDoS高防全量日志分析服务的授权状态，即是否授权DDoS高防访问日志服务。

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	DescribeSlsAuthStatus	要执行的操作。取值：**DescribeSlsAuthStatus**
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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	DDoS高防全量日志分析服务的授权状态。取值： • **true**：已授权 • **false**：未授权

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

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

`JSON` 格式

```
{
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
  "SlsAuthStatus": true
}
```

错误码

访问错误中心查看更多错误码。

13.16.3 DescribeLogStoreExistStatus

调用DescribeLogStoreExistStatus查询是否已创建DDoS高防的日志库。

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	要执行的操作。取值：**DescribeLogStoreExistStatus**

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
ExistStatus	Boolean	true	是否已创建DDoS高防的日志库。取值： • **true**：已创建 • **false**：未创建
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

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

```
<?xml version="1.0" encoding="UTF-8" ?>
<DescribeLogStoreExistStatus?
 <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
 <ExistStatus>true</ExistStatus>
</DescribeLogStoreExistStatus?
```

JSON 格式

```
{
   "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
   "ExistStatus": true
```

```
}
```

错误码

访问错误中心查看更多错误码。

13.16.4 DescribeSlsLogstoreInfo

调用DescribeSlsLogstoreInfo查询DDoS高防的日志库信息，例如日志存储容量、日志存储时长等。

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	要执行的操作。取值：**DescribeSlsLogstoreInfo**
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
LogStore	String	ddoscoo-logstore	DDoS高防服务对接的日志库。
Project	String	ddoscoo-project-181071506993****-cn-hangzhou	DDoS高防服务对接的日志项目。
Quota	Long	3298534883328	可用的日志存储容量。单位：Byte。

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
Ttl	Integer	180	日志存储时长。单位：天。
Used	Long	0	已经使用的存储容量。单位：Byte。 **说明：** 日志服务的统计结果约有两个小时的延迟。

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

```
<?xml version="1.0" encoding="UTF-8" ?>
<DescribeSlsLogstoreInfoResponse>
 <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</requestId>
 <LogStore>ddoscoo-logstore</LogStore>
 <Project>ddoscoo-project-181071506993****-cn-hangzhou</Project>
 <Quota>3298534883328</Quota>
 <Ttl>180</Ttl>
 <Used>0</Used>
</DescribeSlsLogstoreInfoResponse>
```

`JSON` 格式

```
{
   "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
   "LogStore": "ddoscoo-logstore",
   "Project": "ddoscoo-project-181071506993****-cn-hangzhou",
   "Quota": 3298534883328,
   "Ttl": 180,
   "Used": 0
}
```

错误码

访问错误中心查看更多错误码。

13.16.5 ModifyFullLogTtl

调用ModifyFullLogTtl编辑DDoS高防全量日志的存储时长。

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	ModifyFull LogTtl	要执行的操作。取值：**ModifyFull LogTtl**
Ttl	Integer	是	30	DDoS高防网站业务日志的存储时长。取值范围：**30~180**，单位：天。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=ModifyFullLogTtl
&Ttl=30
```

```
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.16.6 DescribeWebAccessLogDispatchStatus

调用DescribeWebAccessLogDispatchStatus查询所有域名的全量日志开关状态。

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	DescribeWebAccessLogDispatchStatus	要执行的操作。取值：**DescribeWebAccessLogDispatchStatus**
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

名称	类型	是否必选	示例值	描述
PageNumber	Integer	否	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写**1**。
PageSize	Integer	否	10	页面显示的记录数量。

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。
SlsConfigStatus	Array		域名的全量日志开关状态信息。
Domain	String	www.aliyun.com	域名。
Enable	Boolean	true	是否开启全量日志。取值： • **true**：已开启 • **false**：未开启
TotalCount	Integer	1	域名的总数。

示例

请求示例

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

正常返回示例

`XML` 格式

```
<?xml version="1.0" encoding="UTF-8" ?>
<DescribeWebAccessLogDispatchStatus>
 <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</requestId>
 <TotalCount>1</TotalCount>
 <SlsConfigStatus>
  <Enable>true</Enable>
  <Domain>www.aliyun.com</Domain>
 </SlsConfigStatus>
```

```
</DescribeWebAccessLogDispatchStatus>
```

JSON 格式

```
{
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
  "TotalCount": 1,
  "SlsConfigStatus": [
    {
      "Enable": true,
      "Domain": "www.aliyun.com"
    }
  ]
}
```

错误码

访问错误中心查看更多错误码。

13.16.7 DescribeWebAccessLogStatus

调用DescribeWebAccessLogStatus查询单个网站业务的全量日志服务信息，例如开关状态、对接的日志项目、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	DescribeWebAccessLogStatus	要执行的操作。取值：**DescribeWebAccessLogStatus**
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

名称	类型	是否必选	示例值	描述
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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。
SlsLogstore	String	ddoscoo-logstore	DDoS高防服务对接的日志库。
SlsProject	String	ddoscoo-project-128965410602****-cn-hangzhou	DDoS高防服务对接的日志服务项目。
SlsStatus	Boolean	true	网站业务是否开启全量日志。取值： • **true**：已开启 • **false**：未开启

示例

请求示例

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

正常返回示例

`XML` 格式

```
<?xml version="1.0" encoding="UTF-8" ?>
<DescribeWebAccessLogStatusResponse>
 <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</requestId>
 <SlsStatus>true</SlsStatus>
 <SlsProject>ddoscoo-project-128965410602****-cn-hangzhou</SlsProject>
 <SlsLogstore>ddoscoo-logstore</SlsLogstore>
</DescribeWebAccessLogStatusResponse>
```

`JSON` 格式

```
{
   "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
   "SlsStatus": true,
```

```
    "SlsProject": "ddoscoo-project-128965410602****-cn-hangzhou",
    "SlsLogstore": "ddoscoo-logstore"
}
```

错误码

访问错误中心查看更多错误码。

13.16.8 EnableWebAccessLogConfig

调用EnableWebAccessLogConfig为网站业务开启全量日志分析。

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	EnableWebAccessLogConfig	要执行的操作。取值：**EnableWebAccessLogConfig**
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明：** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=EnableWebAccessLogConfig
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

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

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。

13.16.9 DisableWebAccessLogConfig

调用DisableWebAccessLogConfig为网站业务关闭全量日志分析。

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	DisableWebAccessLogConfig	要执行的操作。取值：**DisableWebAccessLogConfig**

名称	类型	是否必选	示例值	描述
Domain	String	是	www.aliyun.com	网站业务的域名。 **说明:** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值: • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=DisableWebAccessLogConfig
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

```
<?xml version="1.0" encoding="UTF-8" ?>
<DisableWebAccessLogConfigResponse>
 <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</requestId>
</DisableWebAccessLogConfigResponse>
```

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。

13.16.10 DescribeWebAccessLogEmptyCount

调用DescribeWebAccessLogEmptyCount查询可用的清空日志库的次数。

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	DescribeWebAccessLogEmptyCount	要执行的操作。取值：**DescribeWebAccessLogEmptyCount**
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
AvailableCount	Integer	10	可用的清空日志库的次数。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribeWebAccessLogEmptyCountResponse>
  <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
  <AvailableCount>10</AvailableCount>
</DescribeWebAccessLogEmptyCountResponse>
```

JSON 格式

```
{
   "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
   "AvailableCount": 10
}
```

错误码

访问错误中心查看更多错误码。

13.16.11 EmptySlsLogstore

调用EmptySlsLogstore清空DDoS高防的日志库。

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	要执行的操作。取值：**EmptySlsLogstore**
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务

名称	类型	是否必选	示例值	描述
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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

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

`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。

13.17 系统配置与日志

13.17.1 DescribeStsGrantStatus

调用DescribeStsGrantStatus查询是否授权DDoS高防服务访问其他云产品。

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	DescribeStsGrantStatus	要执行的操作。取值：**DescribeStsGrantStatus**
Role	String	是	AliyunDDoSCOODefaultRole	要查询到角色名称。取值：**AliyunDDoSCOODefaultRole**，表示DDoS高防服务的默认角色。 **说明：** DDoS高防服务默认使用此角色来访问您在其他云产品中的资源。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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。
StsGrant	Struct		DDoS高防服务的授权状态。

名称	类型	示例值	描述
Status	Integer	1	授权状态。取值： • **0**：未授权 • **1**：已授权

示例

请求示例

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

正常返回示例

`XML` 格式

```
<?xml version="1.0" encoding="UTF-8" ?>
<DescribeStsGrantStatus
 <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
 <StsGrant>
  <Status>1</Status>
 </StsGrant>
</DescribeStsGrantStatus
```

`JSON` 格式

```
{
   "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "StsGrant": {
      "Status": 1
   }
}
```

错误码

访问错误中心查看更多错误码。

13.17.2 DescribeBackSourceCidr

调用DescribeBackSourceCidr查询DDoS高防的回源IP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	要执行的操作。取值：**DescribeBackSourceCidr**
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
Line	String	否	coop-line-001	要查询的线路。

返回数据

名称	类型	示例值	描述
Cidrs	List	["47.***.***.0/25","47.***.***.128/25"]	DDoS高防的回源IP网段列表。
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。

示例

请求示例

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

正常返回示例

`XML` 格式

```
<DescribeBackSourceCidrResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
  <Cidrs>47.***.***.0/25</Cidrs>
  <Cidrs>47.***.***.128/25</Cidrs>
```

```
</DescribeBackSourceCidrResponse>
```

JSON 格式

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
  "Cidrs": [
    "47.***.***.0/25",
    "47.***.***.128/25"
  ]
}
```

错误码

访问错误中心查看更多错误码。

13.17.3 DescribeOpEntities

调用DescribeOpEntities查询DDoS高防（新BGP）的操作日志。

说明:
该接口仅适用于DDoS高防（新BGP）服务。

操作日志的类型包括：设置实例弹性防护规格、执行黑洞解封、设置近源流量压制、抵扣抗D包、更换ECS IP、清空全量日志等。

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	1583683200000	查询结束时间。时间戳格式，单位：毫秒。 **说明:** 查询时间的跨度不允许超过近30天。

名称	类型	是否必选	示例值	描述
PageNumber	Integer	是	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写**1**。
PageSize	Integer	是	10	页面显示的记录数量。最大值：**50**。
StartTime	Long	是	1582992000000	查询开始时间。时间戳格式，单位：毫秒。  **说明：** 查询时间的跨度不允许超过近30天。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值：**cn-hangzhou**，表示DDoS高防（新BGP）服务。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
EntityType	Integer	否	1	使用操作对象筛选结果，传入要查询的操作对象的类型。取值： • **1**：DDoS高防IP • **2**：DDoS高防抗D包 • **3**：ECS实例 • **4**：全量日志
EntityObject	String	否	203.***.***.132	使用操作对象筛选结果，传入要查询的操作对象。

返回数据

名称	类型	示例值	描述
OpEntities	Array		操作日志记录。
EntityObject	String	203.***.***.132	操作对象。

名称	类型	示例值	描述
EntityType	Integer	1	操作对象的类型。取值： • **1**：DDoS高防IP • **2**：DDoS高防抗D包 • **3**：ECS实例 • **4**：全量日志
GmtCreate	Long	1584451769000	操作时间。时间戳格式，单位：毫秒。
OpAccount	String	128965410602****	执行操作的阿里云账号ID。
OpAction	Integer	9	操作类型。取值： • **1**：设置弹性防护带宽。 • **5**：抵扣抗D包。 • **8**：更换ECS IP。 • **9**：执行黑洞解封。 • **10**：设置近源流量压制。 • **11**：清空全量日志。 • **12**：降级实例规格，表示实例到期或账号存在欠费时，降低弹性防护带宽。 • **13**：恢复实例规格，表示实例续费或账号欠费结清时，恢复弹性防护带宽。

名称	类型	示例值	描述
OpDesc	String	{"newEntity":{"actionMethod":"undo"}}	操作的描述信息，使用JSON格式的字符串表述，具体结构如下： • **newEntity**：String类型，操作后的参数。 • **oldEntity**：String类型，操作前的参数。 **newEntity**和**oldEntity**均使用JSON格式的字符串表述。不同操作类型（**OpAtion**）对应的操作参数不同。 **OpAction**为**1**、**12**、**13**时，操作参数的结构描述如下： • **elasticBandwidth**：Integer类型，弹性防护带宽值，单位：Gbps。 示例：{"newEntity":{"elasticBandwidth":300},"oldEntity":{"elasticBandwidth":300}} **OpAction**为**5**时，操作参数的结构描述如下： • **bandwidth**：Integer类型，弹性防护带宽，单位：Gbps。 • **count**：Integer类型，抗D包数量。 • **deductCount**：Integer类型，抵扣的抗D包数量。 • **expireTime**：Long类型，抗D包的到期时间。时间戳格式，单位：毫秒。 • **instanceId**：String类型，DDoS高防实例ID。 • **peakFlow**：Integer类型，峰值流量，单位：bps。 示例：{"newEntity":{"bandwidth":100,"count":4,"deductCount":1,"expireTime":1616299196000,"instanceId":"ddoscoo-cn-v641kpmq****","peakFlow":751427000}} **OpAction**为**8**时，操作参数的结构描述如

名称	类型	示例值	描述
RequestId	String	FB24D70C-71F5-4000-8CD8-22CDA0C53CD1	本次请求的ID。
TotalCount	Long	1	操作记录的总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeOpEntities
&EndTime=1583683200000
&PageNumber=1
&PageSize=10
&StartTime=1582992000000
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeOpEntitiesResponse>
  <TotalCount>1</TotalCount>
  <RequestId>FB24D70C-71F5-4000-8CD8-22CDA0C53CD1</RequestId>
  <OpEntities>
    <EntityType>1</EntityType>
    <GmtCreate>1584451769000</GmtCreate>
    <OpAccount>128965410602****</OpAccount>
    <OpDesc>
      <newEntity>
        <actionMethod>undo</actionMethod>
      </newEntity>
    </OpDesc>
    <OpAction>9</OpAction>
    <EntityObject>203.***.***.132</EntityObject>
  </OpEntities>
</DescribeOpEntitiesResponse>
```

JSON 格式

```
{
  "TotalCount": 1,
  "RequestId": "FB24D70C-71F5-4000-8CD8-22CDA0C53CD1",
  "OpEntities": [
    {
      "EntityType": 1,
      "GmtCreate": 1584451769000,
      "OpAccount": "128965410602****",
      "OpDesc": {
        "newEntity": {
          "actionMethod": "undo"
        }
      },
      "OpAction": 9,
      "EntityObject": "203.***.***.132"
```

```
    }
  ]
}
```

错误码

访问错误中心查看更多错误码。

13.17.4 DescribeDefenseRecords

调用DescribeDefenseRecords查询DDoS高防（国际）的高级防护日志。

> **说明：**
> 该接口仅适用于DDoS高防（国际）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	DescribeDefenseRecords	要执行的操作。取值：**DescribeDefenseRecords**
EndTime	Long	是	1583683200000	查询结束时间。时间戳格式，单位：毫秒。 **说明：** 查询时间的跨度不允许超过90天。
PageNumber	Integer	是	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写**1**。
PageSize	Integer	是	10	页面显示的记录数量。最大值：**50**

名称	类型	是否必选	示例值	描述
StartTime	Long	是	1582992000000	查询开始时间。时间戳格式，单位：毫秒。 **说明：** 查询时间的跨度不允许超过近90天。
RegionId	String	否	ap-southeast-1	DDoS高防服务地域ID。取值：**ap-southeast-1**，表示DDoS高防（国际）服务。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
InstanceId	String	否	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。

返回数据

名称	类型	示例值	描述
DefenseRecords	Array		高级防护日志记录。
AttackPeak	Long	6584186000	攻击峰值。单位：bps。
EndTime	Long	1583683200000	防护结束时间。时间戳格式，单位：毫秒。
EventCount	Integer	2	被攻击次数。
InstanceId	String	ddoscoo-cn-mp91j1ao****	DDoS高防实例ID。
StartTime	Long	1582992000000	防护开始时间。时间戳格式，单位：毫秒。

名称	类型	示例值	描述
Status	Integer	0	高级防护的状态。取值： • **0**：使用中 • **1**：已使用
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。
TotalCount	Long	1	高级防护总次数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDefenseRecords
&EndTime=1583683200000
&PageNumber=1
&PageSize=10
&StartTime=1582992000000
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeDefenseRecordsResponse>
  <TotalCount>1</TotalCount>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
  <DefenseRecords>
    <StartTime>1582992000000</StartTime>
    <EndTime>1583683200000</EndTime>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
    <Status>0</Status>
    <AttackPeak>10</AttackPeak>
    <EventCount>1</EventCount>
  </DefenseRecords>
</DescribeDefenseRecordsResponse>
```

JSON 格式

```
{
   "TotalCount": 1,
   "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
   "DefenseRecords": [
      {
         "StartTime": 1582992000000,
         "EndTime": 1583683200000,
         "InstanceId": "ddoscoo-cn-mp91j1ao****",
         "Status": 0,
         "AttackPeak": 10,
         "EventCount": 1
      }
```

```
    ]
}
```

错误码

访问错误中心查看更多错误码。

13.17.5 DescribeAsyncTasks

调用DescribeAsyncTasks查询异步导出任务的详细信息，例如任务ID、任务开始和结束时间、任务状态、任务参数、任务结果等。

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	DescribeAsyncTasks	要执行的操作。取值：**DescribeAsyncTasks**
PageNumber	Integer	是	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写**1**。
PageSize	Integer	是	10	页面显示的记录数量。最大值：**20**
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
AsyncTasks	Array		异步导出任务的详细信息。
EndTime	Long	157927362000	任务结束时间。时间戳格式，单位：毫秒。
StartTime	Long	156927362000	任务开始时间。时间戳格式，单位：毫秒。
TaskId	Long	1	任务ID。
TaskParams	String	{"instanceId": "ddoscoo-cn-mp91j1ao****"}	任务参数。使用JSON格式的字符串表达。不同**TaskType**的任务参数不完全相同。 **TaskType**为**1**、**3**、**4**、**5**、**6**时，任务参数的结构如下。 • **instanceId**：String类型，DDoS高防实例的ID。 **TaskType**为**2**时，任务参数的结构如下。 • **domain**：String类型，网站业务的域名。

名称	类型	示例值	描述
TaskResult	String	{"instanceId": "ddoscoo-cn-mp91j1ao****","url": "https://****.oss-cn-beijing.aliyuncs.com/heap.bin?Expires=1584785140&OSSAccessKeyId=TMP.3KfzD82FyRJevJdEkRX6JEFHhbvRBBb75PZJnyJmksA2QkMm47xFAFDgMhEV8Nm6Vxr8xExMfiy9LsUFAcLcTBrN3rDu3v&Signature=Sj8BNcsxJLE8l5qm4cjNlDt8gv****"}	任务结果。使用JSON格式的字符串表达。不同**TaskType**的任务参数不完全相同。 **TaskType**为**1**、**3**、**4**、**5**、**6**时，任务参数的结构如下。 • **instanceId**：String类型，DDoS高防实例的ID。 • **url**：String类型，导出文件的OSS下载地址。 **TaskType**为**2**时，任务参数的结构如下。 • **domain**：String类型，网站业务的域名。 • **url**：String类型，导出文件的OSS下载地址。
TaskStatus	Integer	2	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	5	任务类型。取值： • **1**：四层导出任务，导出DDoS高防实例的端口转发规则 • **2**：七层导出任务，导出网站业务转发规则 • **3**：会话、健康检查导出任务，导出DDoS高防实例的会话、健康检查配置 • **4**：DDoS防护策略导出任务，导出DDoS高防实例的DDoS防护策略配置 • **5**：黑名单（针对目的IP）下载任务，导出针对DDoS高防实例的黑名单IP • **6**：白名单（针对目的IP）下载任务，导出针对DDoS高防实例的白名单IP
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。
TotalCount	Integer	1	异步导出任务的总数。

示例

请求示例

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

正常返回示例

`XML` 格式

```
<DescribeAsyncTasksResponse>
  <TotalCount>1</TotalCount>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
  <AsyncTasks>
    <TaskId>1</TaskId>
    <TaskType>5</TaskType>
    <TaskStatus>2</TaskStatus>
    <StartTime>156927362</StartTime>
    <EndTime>157927362</EndTime>
    <TaskParams>
```

```
      <instanceId>ddoscoo-cn-mp91j1ao****</instanceId>
    </TaskParams>
    <TaskResult>
      <instanceId>ddoscoo-cn-mp91j1ao****</instanceId>
      <url>https://****.oss-cn-beijing.aliyuncs.com/heap.bin?Expires=1584785140&
amp;OSSAccessKeyId=TMP.3KfzD82FyRJevJdEkRX6JEFHhbvRBBb75PZJnyJmksA2QkMm47
xFAFDgMhEV8Nm6Vxr8xExMfiy9LsUFAcLcTBrN3rDu3v&amp;Signature=Sj8BNcsxJL
E8l5qm4cjNlDt8gv****</url>
    </TaskResult>
  </AsyncTasks>
</DescribeAsyncTasksResponse>
```

JSON 格式

```
{
  "TotalCount": 1,
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
  "AsyncTasks": [
    {
      "TaskId": 1,
      "TaskType": 5,
      "TaskStatus": 2,
      "StartTime": 156927362,
      "EndTime": 157927362,
      "TaskParams": {
        "instanceId": "ddoscoo-cn-mp91j1ao****"
      },
      "TaskResult": {
        "instanceId": "ddoscoo-cn-mp91j1ao****",
        "url": "https://****.oss-cn-beijing.aliyuncs.com/heap.bin?Expires=1584785140
&OSSAccessKeyId=TMP.3KfzD82FyRJevJdEkRX6JEFHhbvRBBb75PZJnyJmksA2QkMm47
xFAFDgMhEV8Nm6Vxr8xExMfiy9LsUFAcLcTBrN3rDu3v&Signature=Sj8BNcsxJLE8l5qm4cjN
lDt8gv****"
      }
    }
  ]
}
```

错误码

访问错误中心查看更多错误码。

13.17.6 CreateAsyncTask

调用CreateAsyncTask创建异步导出任务，例如导出网站业务转发规则、端口转发规则、会话保持和健康检查配置、DDoS防护策略、IP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	CreateAsyncTask	要执行的操作。取值：**CreateAsyncTask**
TaskParams	String	是	{"instanceId":"ddoscoo-cn-mp91j1ao****"}	任务参数信息。使用JSON格式的字符串表达。不同**TaskType**需要传入的任务参数不完全相同。 **TaskType**为**1**、**3**、**4**、**5**、**6**时，任务参数的结构如下。 • **instanceId**：String类型，必选，DDoS高防实例的ID。 **TaskType**为**2**时，任务参数的结构如下。 • **domain**：String类型，可选，网站业务的域名。不传入表示导出所有网站业务的转发规则。
TaskType	Integer	是	5	要创建的任务类型。取值： • **1**：四层导出任务，导出DDoS高防实例的端口转发规则 • **2**：七层导出任务，导出网站业务转发规则 • **3**：会话、健康检查导出任务，导出DDoS高防实例的会话、健康检查配置 • **4**：DDoS防护策略导出任务，导出DDoS高防实例的DDoS防护策略配置 • **5**：黑名单（针对目的IP）下载任务，导出针对DDoS高防实例的黑名单IP • **6**：白名单（针对目的IP）下载任务，导出针对DDoS高防实例的白名单IP

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=CreateAsyncTask
&TaskParams={"instanceId": "ddoscoo-cn-mp91j1ao****"}
&TaskType=5
&<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。

13.17.7 DeleteAsyncTask

调用DeleteAsyncTask删除异步导出任务。

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	要执行的操作。取值：**DeleteAsyncTask**
TaskId	Integer	是	1	要删除的任务ID。 **说明：** 您可以调用DescribeAsyncTasks查询所有异步导出任务ID。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • **cn-hangzhou**：表示DDoS高防（新BGP）服务 • **ap-southeast-1**：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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=DeleteAsyncTask
&TaskId=1
```

```
&<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。

13.18 标签

13.18.1 DescribeTagKeys

调用DescribeTagKeys查询所有标签键。

说明:

仅DDoS高防（新BGP）服务支持标签功能。

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	DescribeTagKeys	要执行的操作。取值：**DescribeTagKeys**。
RegionId	String	是	cn-hangzhou	DDoS高防服务地域ID。取值：**cn-hangzhou**，表示DDoS高防（新BGP）服务。

名称	类型	是否必选	示例值	描述
ResourceType	String	是	INSTANCE	资源类型。取值：**INSTANCE**，表示DDoS高防实例。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
PageSize	Integer	否	10	页面显示的记录数量。
PageNumber	Integer	否	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写**1**。

返回数据

名称	类型	示例值	描述
PageNumber	Integer	1	分页查询请求时返回的页码。
PageSize	Integer	10	页面显示的记录数量。
RequestId	String	1B0D6FCD-ED11-46B7-9903-D5A45509EC11	本次请求的ID。
TagKeys	Array		标签键信息。
TagCount	Integer	6	标签键关联的资源总数。
TagKey	String	aa1	标签键。
TotalCount	Integer	3	标签键的总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeTagKeys
&RegionId=cn-hangzhou
&ResourceType=INSTANCE
```

```
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeTagKeysResponse>
  <TotalCount>3</TotalCount>
  <PageSize>10</PageSize>
  <RequestId>1B0D6FCD-ED11-46B7-9903-D5A45509EC11</RequestId>
  <PageNumber>1</PageNumber>
  <TagKeys>
    <TagCount>6</TagCount>
    <TagKey>aa1</TagKey>
  </TagKeys>
  <TagKeys>
    <TagCount>1</TagCount>
    <TagKey>aa134</TagKey>
  </TagKeys>
  <TagKeys>
    <TagCount>6</TagCount>
    <TagKey>aa2</TagKey>
  </TagKeys>
</DescribeTagKeysResponse>
```

JSON 格式

```
{
 "TotalCount":3,
 "PageSize":10,
 "RequestId":"1B0D6FCD-ED11-46B7-9903-D5A45509EC11",
 "PageNumber":1,
 "TagKeys":[
  {
   "TagCount":6,
   "TagKey":"aa1"
  },
  {
   "TagCount":1,
   "TagKey":"aa134"
  },
  {
   "TagCount":6,
   "TagKey":"aa2"
  }
 ]
}
```

错误码

访问错误中心查看更多错误码。

13.18.2 DescribeTagResources

调用DescribeTagResources查询资源关联的标签信息。

说明:

仅DDoS高防（新BGP）服务支持标签功能。

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	DescribeTagResources	要执行的操作。取值：**DescribeTagResources**。
RegionId	String	是	cn-hangzhou	DDoS高防服务地域ID。取值：**cn-hangzhou**，表示DDoS高防（新BGP）服务。
ResourceType	String	是	INSTANCE	资源类型。取值：**INSTANCE**，表示DDoS高防实例。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
ResourceIds.N	RepeatList	否	ddoscoo-cn-mp91j1ao****	根据资源ID进行筛选，传入要查询的DDoS高防实例的ID。 **说明：** 必须传入**ResourceId**或者**Tag.N.Key**和**Tag.N.Value**的组合。您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
Tags.N.Key	String	否	testkey	根据标签进行筛选，传入要查询的标签键（Key）。 **说明：** 必须传入**ResourceId**或者**Tag.N.Key**和**Tag.N.Value**的组合。**Tag.N.Key**必须与**Tags.N.Value**成对存在。

名称	类型	是否必选	示例值	描述
Tags.N.Value	String	否	testvalue	根据标签进行筛选，传入要查询的标签值（Value）。 **说明：** 必须传入**ResourceId**或者**Tag.N.Key**和**Tag.N.Value**的组合。**Tag.N.Key**必须与**Tags.N.Value**成对存在。
NextToken	String	否	RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCf****	传入下一个查询开始的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
NextToken	String	RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCf****	下一个查询开始的Token。没有下一个查询时为空。
RequestId	String	36E698F7-48A4-48D0-9554-0BB4BAAB99B3	本次请求的ID。
TagResources	Array		资源关联的标签信息。
TagResource			
ResourceId	String	ddoscoo-cn-mp91j1ao****	资源ID，具体指DDoS高防实例的ID。
ResourceType	String	INSTANCE	资源类型。取值：**INSTANCE**，表示DDoS高防实例。
TagKey	String	aa1	资源关联的标签键。
TagValue	String	aa1_1	资源关联的标签值。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeTagResources
&RegionId=cn-hangzhou
&ResourceType=INSTANCE
&ResourceIds.1=ddoscoo-cn-mp91mf6x****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeTagResources>
  <NextToken>RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCf****</NextToken>
  <RequestId>36E698F7-48A4-48D0-9554-0BB4BAAB99B3</RequestId>
  <TagResources>
    <ResourceId>ddoscoo-cn-mp91j1ao****</ResourceId>
    <TagKey>aa1</TagKey>
    <ResourceType>INSTANCE</ResourceType>
    <TagValue>aa1_1</TagValue>
  </TagResources>
</DescribeTagResources>
```

`JSON` 格式

```
{
 "NextToken":"RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCf****",
 "RequestId":"36E698F7-48A4-48D0-9554-0BB4BAAB99B3",
 "TagResources":[
  {
   "ResourceId":"ddoscoo-cn-mp91j1ao****",
   "TagKey":"aa1",
   "ResourceType":"INSTANCE",
   "TagValue":"aa1_1"
  }
 ]
}
```

错误码

访问错误中心查看更多错误码。

13.18.3 CreateTagResources

调用CreateTagResources为资源关联标签。

说明:

仅DDoS高防（新BGP）服务支持标签功能。

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	CreateTagResources	要执行的操作。取值：**CreateTagResources**。
RegionId	String	是	cn-hangzhou	DDoS高防服务地域ID。取值：**cn-hangzhou**，表示DDoS高防（新BGP）服务。
ResourceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	要操作的资源ID，具体指DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
ResourceType	String	是	INSTANCE	资源类型。取值：**INSTANCE**，表示DDoS高防实例。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
Tags.N.Key	String	否	testkey	要关联的标签键。
Tags.N.Value	String	否	testvalue	要关联的标签值。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateTagResources
&RegionId=cn-hangzhou
&ResourceIds.1=ddoscoo-cn-mp91j1ao****
&ResourceType=INSTANCE
&Tag.1.Key=testkey
&Tag.1.Value=testvalue
&<公共请求参数>
```

正常返回示例

XML 格式

```
<CreateTagResourcesResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</CreateTagResourcesResponse>
```

JSON 格式

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

访问错误中心查看更多错误码。

13.18.4 DeleteTagResources

调用DeleteTagResources为资源移除标签。

说明:

仅DDoS高防（新BGP）服务支持标签功能。

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	DeleteTagResources	要执行的操作。取值：**DeleteTagResources**。

名称	类型	是否必选	示例值	描述
RegionId	String	是	cn-hangzhou	DDoS高防服务地域ID。取值：**cn-hangzhou**，表示DDoS高防（新BGP）服务。
ResourceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	要操作的资源ID，具体指DDoS高防实例的ID。 **说明：** 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
ResourceType	String	是	INSTANCE	资源类型。取值：**INSTANCE**，表示DDoS高防实例。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
TagKey.N	RepeatList	否	testkey	要移除的标签键。
All	Boolean	否	false	是否移除资源上的所有标签。取值： • **true**：是 • **false**：否

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteTagResources
&RegionId=cn-hangzhou
&ResourceIds.1=ddoscoo-cn-mp91j1ao****
&ResourceType=INSTANCE
&All=true
```

```
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DeleteTagResourcesResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</DeleteTagResourcesResponse>
```

JSON 格式

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

访问错误中心查看更多错误码。

13.19 错误码

本文介绍了DDoS高防API调用失败时返回的错误码及其含义。

错误码（Error Code）	描述
DomainNotExist	域名不存在。
DomainExist	域名属于别的用户。
WebRulePortDeny	端口已用于网站业务转发，禁止配置。
InvalidParameter.JSONError	JSON格式不正确。
ExceedFuncSpec	超过功能套餐规格。
ExceedNoStardardPort	无效的非标端口。
InvalidWebRule	无效的网站业务转发规则。
NetworkRuleExist	端口已配置转发规则。
NetworkRuleConflict	端口转发规则冲突。
ExceedWebRuleLimit	超过防护域名数规格。
ExceedNetworkRuleLimit	超过防护端口数规格。
InvalidDomain	无效的域名。
UnBlackholeLimit	超过解除封禁次数限制。
InvalidIp	无效的IP地址/地址段。
DomainOwnerError	域名属于别的用户。

错误码（Error Code）	描述
InvalidParams	没有权限。
SchedulerNameConflict	流量调度规则冲突。
CcRuleExist	频率控制规则已存在。
CDNDomainExist	CDN域名已经存在。
IpBlackholing	IP在黑洞中。
InvalidSwitch	不允许切换默认线路的最后一条调度器规则的状态。
ParamsConflict	参数冲突，例如记录类型、记录值、线路、地域ID。
UnkownError	未知错误。
InstanceNotExist	实例不存在。

13.20 中国和海外地区代码

本文介绍了在调用DDoS高防的基础设施防护策略-区域封禁和查询请求来源分布相关接口时用到的中国地区代码、海外地区代码，方便您查询使用。

相关接口

本文描述的中国地区代码、海外地区代码适用于在调用以下相关接口时查询使用。

类型	接口	使用场景
基础设施防护策略-区域封禁	ConfigNetworkRegionBlock	查询请求参数**Config**结构中的**Countries**和**Provinces**参数的取值。
	DescribeNetworkRegionBlock	查询返回参数**Config**结构中的**Countries**和**Provinces**参数的取值。
监控报表	DescribeDomainViewSourceCountries	查询返回参数**CountryId**对应的海外地区名称。
	DescribeDomainViewSourceProvinces	查询返回参数**ProvinceId**对应的中国地区名称。
	DescribePortViewSourceCountries	查询返回参数**CountryId**对应的海外地区名称。
	DescribePortViewSourceProvinces	查询返回参数**ProvinceId**对应的中国地区名称。

中国地区代码

① 适用于基础设施防护策略-区域封禁相关接口。

② 适用于监控报表相关接口。

名称	代码 ①	ProvinceId ②
北京市	11	110000
天津市	12	120000
河北省	13	130000
山西省	14	140000
内蒙古自治区	15	150000
辽宁省	21	210000
吉林省	22	220000
黑龙江省	23	230000
上海市	31	310000
江苏省	32	320000
浙江省	33	330000
安徽省	34	340000
福建省	35	350000
江西省	36	360000
山东省	37	370000
河南省	41	410000
湖北省	42	420000
湖南省	43	430000
广东省	44	440000
广西壮族自治区	45	450000
海南省	46	460000
重庆市	50	500000
四川省	51	510000
贵州省	52	520000
云南省	53	530000
西藏自治区	54	540000
陕西省	61	610000
甘肃省	62	620000
青海省	63	630000
宁夏回族自治区	64	640000

名称	代码 ①	ProvinceId ②
新疆维吾尔自治区	65	650000
香港特别行政区	81	810000
台湾省	71	710000
澳门特别行政区	82	820000

海外地区代码

① 适用于基础设施防护策略-区域封禁相关接口。

② 适用于监控报表相关接口。

名称	代码 ①	CountryId ②
中国	1	CN
澳大利亚	2	AU
日本	3	JP
泰国	4	TH
印度	5	IN
美国	7	US
德国	8	DE
荷兰	9	NL
马来西亚	10	MY
安哥拉	11	AO
韩国	12	KR
新加坡	13	SG
柬埔寨	14	KH
菲律宾	16	PH
越南	17	VN
法国	18	FR
波兰	19	PL
西班牙	20	ES
俄罗斯	21	RU
瑞士	22	CH

名称	代码 ①	CountryId ②
英国	23	GB
意大利	24	IT
捷克	25	CZ
爱尔兰	26	IE
丹麦	27	DK
葡萄牙	28	PT
瑞典	29	SE
加纳	30	GH
土耳其	31	TR
喀麦隆	32	CM
南非	33	ZA
芬兰	34	FI
匈牙利	35	HU
阿联酋	36	AE
希腊	37	GR
巴西	38	BR
奥地利	39	AT
约旦	40	JO
比利时	41	BE
罗马尼亚	42	RO
卢森堡	43	LU
阿根廷	44	AR
乌干达	45	UG
亚美尼亚	46	AM
坦桑尼亚	47	TZ
布隆迪	48	BI
乌拉圭	49	UY
保加利亚	50	BG
乌克兰	51	UA
以色列	52	IL

名称	代码 ①	CountryId ②
卡塔尔	53	QA
伊拉克	54	IQ
立陶宛	55	LT
摩尔多瓦	56	MD
乌兹别克斯坦	57	UZ
斯洛伐克	58	SK
哈萨克斯坦	59	KZ
克罗地亚	60	HR
格鲁吉亚	61	GE
爱沙尼亚	62	EE
直布罗陀	63	GI
拉脱维亚	64	LV
挪威	65	NO
巴勒斯坦	66	PS
塞浦路斯	67	CY
沙特阿拉伯	68	SA
伊朗	69	IR
加拿大	70	CA
美属萨摩亚	71	AS
叙利亚	72	SY
科威特	73	KW
巴林	74	BH
黎巴嫩	75	LB
阿曼	76	OM
阿塞拜疆	77	AZ
赞比亚	78	ZM
津巴布韦	79	ZW
刚果民主共和国	80	CD
塞尔维亚	81	RS
冰岛	82	IS

名称	代码 ①	CountryId ②
斯洛文尼亚	83	SI
马其顿	84	MK
列支敦士登	85	LI
泽西岛	86	JE
波斯尼亚和黑塞哥维那（波黑）	87	BA
智利	88	CL
秘鲁	89	PE
吉尔吉斯斯坦	90	KG
留尼汪岛	91	RE
塔吉克斯坦	92	TJ
马恩岛	93	IM
根西岛	94	GG
马耳他	95	MT
利比亚	96	LY
也门	97	YE
白俄罗斯	98	BY
马约特	99	YT
瓜德罗普	100	GP
法属圣马丁	101	MF
马提尼克	102	MQ
圭亚那	103	GY
科索沃	104	XK
印度尼西亚	105	ID
北马里亚纳群岛	106	MP
多米尼加	107	DO
墨西哥	108	MX
关岛	109	GU
尼日利亚	110	NG
委内瑞拉	111	VE
波多黎各	112	PR

名称	代码 ①	CountryId ②
蒙古	113	MN
新西兰	114	NZ
孟加拉	115	BD
巴基斯坦	116	PK
巴布亚新几内亚	117	PG
特立尼达和多巴哥	118	TT
莱索托	119	LS
哥伦比亚	120	CO
哥斯达黎加	121	CR
厄瓜多尔	123	EC
斯里兰卡	124	LK
埃及	125	EG
英属维尔京群岛	126	VG
牙买加	127	JM
圣卢西亚	128	LC
开曼群岛	129	KY
格林纳达	130	GD
库拉索	131	CW
巴拿马	132	PA
巴巴多斯	133	BB
巴哈马	134	BS
尼泊尔	135	NP
托克劳	136	TK
马尔代夫	137	MV
阿富汗	138	AF
新喀里多尼亚	139	NC
斐济	140	FJ
瓦利斯和富图纳群岛	141	WF
阿尔巴尼亚	142	AL
圣马力诺	143	SM

名称	代码 ①	CountryId ②
黑山	144	ME
东帝汶	145	TL
摩纳哥	146	MC
几内亚	147	GN
缅甸	148	MM
格陵兰	149	GL
百慕大	150	BM
圣文森特和格林纳丁斯	151	VC
美属维尔京群岛	152	VI
苏里南	153	SR
圣巴泰勒米	154	BL
海地	155	HT
安提瓜和巴布达	156	AG
利比里亚	157	LR
肯尼亚	158	KE
博茨瓦纳	159	BW
莫桑比克	160	MZ
塞内加尔	161	SN
马达加斯加	162	MG
纳米比亚	163	NA
科特迪瓦	164	CI
苏丹	165	SD
马拉维	166	MW
加蓬	167	GA
马里	168	ML
贝宁	169	BJ
乍得	170	TD
佛得角	171	CV
卢旺达	172	RW
刚果共和国	173	CG

名称	代码 ①	CountryId ②
冈比亚	174	GM
毛里求斯	175	MU
阿尔及利亚	176	DZ
斯威士兰	177	SZ
布基纳法索	178	BF
塞拉利昂	179	SL
索马里	180	SO
尼日尔	181	NE
中非	182	CF
多哥	183	TG
南苏丹	184	SS
赤道几内亚	185	GQ
塞舌尔	186	SC
吉布提	187	DJ
摩洛哥	188	MA
毛里塔尼亚	189	MR
科摩罗	190	KM
英属印度洋领地	191	IO
突尼斯	192	TN
老挝	193	LA
文莱	194	BN
不丹	195	BT
瑙鲁	196	NR
瓦努阿图	197	VU
密克罗尼西亚联邦	198	FM
法属波利尼西亚	199	PF
汤加	200	TO
洪都拉斯	201	HN
玻利维亚	202	BO
萨尔瓦多	203	SV

名称	代码 ①	CountryId ②
危地马拉	204	GT
尼加拉瓜	205	NI
伯利兹	206	BZ
巴拉圭	207	PY
法属圭亚那	208	GF
安道尔	209	AD
法罗群岛	210	FO
纽埃	211	NU
基里巴斯	212	KI
马绍尔群岛	213	MH
帕劳	214	PW
萨摩亚	215	WS
所罗门群岛	216	SB
图瓦卢	217	TV
朝鲜	218	KP
梵蒂冈	219	VA
厄立特里亚	220	ER
埃塞俄比亚	221	ET
几内亚比绍	222	GW
圣多美和普林西比	223	ST
土库曼斯坦	224	TM
古巴	225	CU
多米尼克	226	DM
圣基茨和尼维斯	227	KN
阿鲁巴	228	AW
福克兰群岛	229	FK
特克斯和凯科斯群岛	230	TC
荷兰加勒比	231	BQ
荷属圣马丁	232	SX
蒙塞拉特岛	233	MS

名称	代码 ①	CountryId ②
安圭拉	234	AI
圣皮埃尔和密克隆群岛	235	PM
奥兰群岛	236	AX
诺福克岛	237	NF
南极洲	238	AQ
库克群岛	239	CK
圣诞岛	240	CX
欧洲其他	241	EU