ALIBABA CLOUD

阿里云

DDoS防护

DDoS高防新BGP&国际

文档版本：20220104

阿里云

法律声明

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

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

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

目录

1.API概览

本文汇总了DDoS高防（新BGP）和DDoS高防（国际）服务所有可调用的API。

> 注意 本文列举的接口适用于DDoS高防（新BGP）和DDoS高防（国际）服务。

在使用以下接口前，请确认您已经购买了DDoS高防（新BGP）或DDoS高防（国际）实例。具体操作，请参见购买DDoS高防实例。

如无特殊说明，以下接口同时适用于DDoS高防（新BGP）和DDoS高防（国际），个别仅适用于DDoS高防（新BGP）或DDoS高防（国际）的接口，在相关接口文档中有说明。关于DDoS高防（新BGP）和DDoS高防（国际）的功能差异，请参见DDoS高防（新BGP）和DDoS高防（国际）的功能差异。

更多API资源，请访问OpenAPI开发者门户。

实例

API	描述
DescribeInstanceIds	查询DDoS高防实例的ID信息。
DescribeInstances	查询DDoS高防实例的详细信息，包含业务转发状态、到期状态、欠费状态等。
DescribeInstanceStatus	查询指定的DDoS高防实例的状态，包含正常、过期、欠费、释放。
DescribeInstanceDetails	查询指定的DDoS高防实例的IP和线路信息。
DescribeInstanceSpecs	查询指定的DDoS高防实例的规格信息。
DescribeInstanceStatistics	查询指定的DDoS高防实例的统计信息，例如已防护的域名、端口数量等。
ModifyInstanceRemark	修改DDoS高防实例的备注。
DescribeElasticBandwidthSpec	查询指定的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。

域名接入

API	描述
DescribeDomains	查询已接入DDoS高防进行防护的网站域名。
DescribeWebRules	查询网站业务转发规则。
CreateWebRule	创建网站业务转发规则。
ModifyWebRule	修改网站业务转发规则。

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	修改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	修改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	修改网站业务转发规则的HTTP 2.0开关状态。
DescribeL7RsPolicy	查询网站业务转发规则的回源策略。
ConfigL7RsPolicy	为网站业务转发规则设置回源策略。

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	修改端口转发规则。
DeleteNetworkRule	删除端口转发规则。
DescribeHealthCheckList	查询端口转发规则的（四层或七层）健康检查配置。
ModifyHealthCheckConfig	修改端口转发规则的（四层或七层）健康检查配置。
DescribeHealthCheckStatus	查询源站健康检查状态信息。
ConfigLayer4RuleBakMode	修改端口转发规则的回源模式（启用或关闭主备回源）。
ConfigLayer4RulePolicy	为端口转发规则设置主、备源站IP地址。
ConfigLayer4Remark	为端口转发规则添加备注。
DescribeLayer4RulePolicy	查询端口转发规则的回源设置。

流量调度器

API	描述
DescribeSchedulerRules	查询流量调度器调度规则。
CreateSchedulerRule	创建流量调度器调度规则。
ModifySchedulerRule	修改流量调度器调度规则。
SwitchSchedulerRule	将业务流量切换到DDoS高防实例进行清洗、回切到联动资源。
DeleteSchedulerRule	删除流量调度器调度规则。

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	修改针对DDoS高防实例的区域封禁配置。
DescribeBlockStatus	查询DDoS高防（新BGP）实例的近源流量压制配置。
ModifyBlockStatus	修改DDoS高防（新BGP）实例的近源流量压制配置。
DescribeUnBlockCount	查询阿里云账号可用的近源流量压制次数。
DescribeUdpReflect	查询指定的DDoS高防实例上被UDP反射攻击防护策略过滤的反射源端口。

API	描述
ConfigUdpReflect	为DDoS高防实例添加UDP反射攻击防护策略，过滤指定的反射源端口。

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	修改网站业务AI智能防护的开关状态。
ModifyWebAIProtectMode	修改网站业务AI智能防护的模式。
ModifyWebIpSetSwitch	修改网站业务黑白名单（针对域名）的开关状态。
ConfigWebIpSet	修改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	修改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	修改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	修改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	修改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	修改网站业务区域封禁（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	修改网站业务区域封禁（针对域名）的封禁地区。

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	修改非网站业务AI智能防护的配置信息。
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	修改非网站业务端口转发规则的会话保持策略。

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	修改定制场景策略。
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。

攻击分析

API	描述
DescribeAttackAnalysisMaxQps	查询指定时间范围内DDoS攻击的峰值（qps）。
DescribeDDosEventMax	查询指定时间范围内的流量型攻击峰值（bps）、连接型攻击峰值（cps）、Web资源耗尽型攻击峰值（qps）。
DescribeDDosAllEventList	查询攻击事件列表。
DescribeDDosEventArea	查询某次流量型攻击的来源地域详情。
DescribeDDosEventAttackType	查询某次流量型攻击的攻击类型详情。
DescribeDDosEventIsp	查询某次流量型攻击的攻击来源网络运营商（ISP）信息。
DescribeDDosEventSrcIp	查询某次流量型攻击的攻击来源IP详情。

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高防实例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。
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。

API	描述
DescribeLogStoreExistStatus	查询是否已创建了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	修改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。
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	修改网站业务静态页面缓存的开关状态。
ModifyWebCacheMode	修改网站业务静态页面缓存的缓存模式。
ModifyWebCacheCustomRule	修改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	查询阿里云账号是否授权了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。
DescribeSystemLog	查询弹性业务带宽的账单详情。
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。

2.调用方式

DDoS高防接口支持HTTP调用和OpenAPI开发者门户调用。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。

请求结构如下：

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

参数说明：

- Endpoint：DDoS高防API的服务接入地址。取值：
  - *ddoscoo.cn-hangzhou.aliyuncs.com*：表示DDoS高防（新BGP）服务。
  - *ddoscoo.ap-southeast-1.aliyuncs.com*：表示DDoS高防（国际）服务。
- Action：要执行的操作。例如，调用DescribeInstanceIds，表示查询已创建的DDoS高防实例ID。
- Version：要使用的API的版本。DDoS高防的API版本是**2020-01-01**。
- Parameters：请求参数。多个请求参数之间用and符号（&）进行连接。
  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，具体内容，请参见公共参数。

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** 为了便于您查看，本文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开发者门户调用

OpenAPI开发者门户是一款可视化的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OpenAPI开发者门户调用API，也可以通过API文档中的调试功能进行调用。

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AccessKey Secret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( AccessKey Secret, 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）。
    i. 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。

ii. 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。
其他字符	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-urlencoded` MIME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;`
	`}`

iii. 将编码后的参数名称和值用英文等号（=）进行连接。

iv. 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他参数一样，按照RFC3986的规则进行URL编码。

示例

以DescribeInstanceIds接口为例，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
```

4.公共参数

本文介绍每个接口都需要使用的请求参数和返回数据。

公共请求参数

名称	类型	是否必须	描述
RegionId	String	是	DDoS高防实例所在地域ID。取值： • *cn-hangzhou*：表示中国内地，对应DDoS高防（新BGP）服务。 • *ap-southeast-1*：表示中国内地以外，对应DDoS高防（国际）服务。
Format	String	否	返回消息的格式。取值： • *JSON*（默认） • *XML*
Version	String	是	API版本号，使用YYYY-MM-DD日期格式。取值： *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ISO 8601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2020-01-01T12:00:00Z。
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号，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
```

公共返回数据

API返回结果采用统一格式，返回2xx HTTP状态码表示调用成功，返回4xx或5xx HTTP状态码表示调用失败。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，用于标识本次请求。

调用成功返回的数据格式有XML和JSON两种。您可以在发送请求时指定返回的数据格式，默认为JSON格式。

正常返回数据示例：

- 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*/
    }
```

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。

- AccessKey ID：用于标识用户。
- AccessKey Secret：用于验证用户的密钥。AccessKey Secret必须保密。

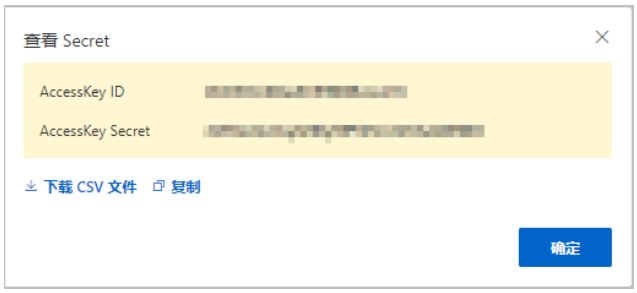
> **警告** 主账号AccessKey泄露会威胁您所有资源的安全。建议使用子账号（RAM用户）AccessKey进行操作，可以有效降低AccessKey泄露的风险。

操作步骤

1. 使用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**AccessKey管理**。
3. 获取账号AccessKey。

   您可以选择获取主账号AccessKey或者使用子用户AccessKey。

   - 获取主账号AccessKey
     a. 在**安全提示**对话框，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**AccessKey ID**和**AccessKey Secret**。可以单击**保存AK信息**，下载AccessKey信息。

   - 获取子账号AccessKey
     a. 在**安全提示**对话框，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**创建用户**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，单击**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**AccessKey ID**和**AccessKey Secret**。您可以单击**下载CSV文件**，下载AccessKey信息或者单击**复制**，复制AccessKey信息。

6.调用API创建DDoS高防实例

DDoS防护服务不提供创建实例的接口。您可以通过调用阿里云交易和账单管理API提供的CreateInstance接口来创建DDoS高防（新BGP、国际）实例。

背景信息

阿里云交易和账单管理API是一套通用的管理阿里云资源的接口，可以用于查询服务价格、管理实例、获取账单信息等。关于阿里云交易和账单管理API支持的所有接口，请参见API概览。

您可以调用阿里云交易和账单管理API提供的CreateInstance接口，创建DDoS高防（新BGP、国际）实例。关于该接口的调用方式，请参见请求结构。

下文介绍了调用CreateInstance接口创建DDoS高防（新BGP）实例、DDoS高防（国际）实例的请求方法和示例。

创建DDoS高防（新BGP）实例

您在调用CreateInstance接口创建DDoS高防（新BGP）实例时，需要完成以下API请求参数设置。

> 说明　关于调用该接口所需的公共请求参数，请参见公共参数。

请求参数：创建DDoS高防（新BGP）实例

名称	类型	是否必选	示例值	描述
Action	String	是	CreateInstance	要执行的操作。取值：*CreateInstance*。
ProductCode	String	是	ddos	实例所属服务的代码。 该参数设置为：*ddos*，表示DDoS高防服务。
ProductType	String	是	ddoscoo	实例所属服务的类型。 该参数设置为：*ddoscoo*，表示DDoS高防（新BGP）服务。
SubscriptionType	String	是	Subscription	实例的计费方式。 该参数设置为：*Subscription*，表示包年包月方式。
Period	Integer	是	1	购买时长，单位：月。 取值：*1*、*2*、*3*、*4*、*5*、*6*、*12*、*24*。
Parameter.N.Code	String	是	FunctionVersion	Parameter.N.Code表示一个实例配置项，Parameter.N.Value表示该配置项的值。 您通过设置Parameter.N.Code和Parameter.N.Value对，设置某项实例配置。其中，N表示配置项的序号，例如Parameter.1.Code和Parameter.1.Value配对，表示第1项配置。 关于DDoS高防（新BGP）实例的具体配置，请参见DDoS高防（新BGP）实例配置。
Parameter.N.Value	String	是	0	

名称	类型	是否必选	示例值	描述
RenewalStatus	String	否	ManualRenewal	实例的续费方式。取值： • *ManualRenewal*（默认）：表示手动续费。 • *AutoRenewal*：表示自动续费。
RenewPeriod	Integer	否	1	自动续费周期， 单位：月。 注意 RenewalStatus为*AutoRenewal*（表示开启自动续费）时，必须设置该参数。
ClientToken	String	否	123e4567-e89b-12d3-a456-42665544****	保证请求幂等性。从您的客户端生成一个参数值，确保不同请求间该参数值唯一。ClientToken只支持ASCII字符，且不能超过64个字符。更多信息，请参见如何保证幂等性。 说明 如果不设置该参数，则系统自动使用API请求的RequestId作为ClientToken标识。

创建DDoS高防（新BGP）实例时，您需要通过Parameter.N.Code和Parameter.N.Value对，完成下表描述的实例配置。

DDoS高防（新BGP）实例配置

配置项（Code）	类型	示例值（Value）	描述
Edition	String	coop	防护套餐类型。取值：coop，表示专业版。
FunctionVersion	String	0	功能套餐类型。取值： • 0：表示标准功能。 • 1：表示增强功能。
NormalQps	Float	3000	正常业务QPS。 取值范围：3000~100000，必须是100的整数倍。
PortCount	Float	50	防护端口数。 取值范围：50~400，必须是5的整数倍。
DomainCount	Float	50	防护域名数。 取值范围：50~2000，必须是10的整数倍。
ServiceBandwidth	Float	100	业务带宽，单位：Mbps。 取值范围：100~5000，必须是50的整数倍。

配置项（Code）	类型	示例值（Value）	描述
BaseBandwidth	Float	30	保底防护带宽，单位：GB。 取值：30、60、100、300、400、500、600。
Bandwidth	Float	50	弹性防护带宽，单位：GB。 弹性防护带宽必须大于或等于保底防护带宽。不同保底防护带宽（BaseBandwidth）支持的弹性防护带宽（Bandwidth）取值不同。具体说明如下： • BaseBandwidth为30时，Bandwidth取值：30、40、50、60、70、80、100、150、200、300。 • BaseBandwidth为60时，Bandwidth取值：60、70、80、100、150、200、300、400、500、600。 • BaseBandwidth为100时，Bandwidth取值：100、150、200、300、400、500、600。 • BaseBandwidth为300时，Bandwidth取值：300、400、500、600。 • BaseBandwidth为400时，Bandwidth取值：400、500、600。 • BaseBandwidth为500时，Bandwidth取值：500、600。 • BaseBandwidth为600时，Bandwidth取值：600。
ServicePartner	String	coop-line-001	防护线路类型。取值：coop-line-001，表示默认防护线路。

创建DDoS高防（国际）实例

您在调用CreateInstance接口创建DDoS高防（国际）实例时，需要完成以下API请求参数设置。

> **说明** 关于调用该接口所需的公共请求参数，请参见公共参数。

请求参数：创建DDoS高防（国际）实例

名称	类型	是否必选	示例值	描述
Action	String	是	CreateInstance	要执行的操作。取值：*CreateInstance*。
ProductCode	String	是	ddos	实例所属服务的代码。 该参数设置为：*ddos*，表示DDoS高防服务。
ProductType	String	是	ddosDip	实例所属服务的类型。 该参数设置为：*ddosDip*，表示DDoS高防（国际）服务。
SubscriptionType	String	是	Subscription	实例的计费方式。 该参数设置为：*Subscription*，表示包年包月方式。
Period	Integer	是	3	购买时长，单位：月。 取值：*3*、*6*、*12*、*24*。

名称	类型	是否必选	示例值	描述
Parameter.N.Code	String	是	FunctionVersion	Parameter.N.Code表示一个实例配置项，Parameter.N.Value表示该配置项的值。 您通过设置Parameter.N.Code和Parameter.N.Value对，设置某项实例配置。其中，N表示配置项的序号，例如Parameter.1.Code和Parameter.1.Value配对，表示第1项配置。 关于DDoS高防（国际）实例的具体配置，请参见DDoS高防（国际）实例配置。
Parameter.N.Value	String	是	0	
RenewalStatus	String	否	ManualRenewal	实例的续费方式。取值： • *ManualRenewal*（默认）：表示手动续费。 • *AutoRenewal*：表示自动续费。
RenewPeriod	Integer	否	1	自动续费周期， 单位：月。 **说明** RenewalStatus为AutoRenewal（表示开启自动续费）时，必须设置该参数。
ClientToken	String	否	123e4567-e89b-12d3-a456-42665544****	保证请求幂等性。从您的客户端生成一个参数值，确保不同请求间该参数值唯一。ClientToken只支持ASCII字符，且不能超过64个字符。更多信息，请参见如何保证幂等性。 **说明** 如果不设置该参数，则系统自动使用API请求的RequestId作为ClientToken标识。

创建DDoS高防（国际）实例时，您需要通过Parameter.N.Code和Parameter.N.Value对，完成下表描述的实例配置。

DDoS高防（国际）实例配置

配置项（Code）	类型	示例值（Value）	描述
Region	String	ap-southeast-1	服务地域。取值：ap-southeast-1，表示海外地区。
ProductPlan	String	0	实例类型。取值： • 0：表示保险版实例。 • 1：表示无忧版实例。 • 2：表示加速线路实例。 • 3：表示安全加速线路实例。

配置项（Code）	类型	示例值（Value）	描述
FunctionVersion	Strinig	0	功能套餐类型。取值： • 0：表示标准功能。 • 1：表示增强功能。 **说明** ProductPlan为2（表示创建加速线路实例）时，无需配置该参数。
NormalQps	Float	500	业务QPS。 不同实例类型（ProductPlan）支持的业务QPS（NormalQps）取值范围不同。具体说明如下： • ProductPlan为0时，NormalQps取值范围：500~100000，必须是100的整数倍。 • ProductPlan为1时，NormalQps取值范围：1000~100000，必须是100的整数倍。 • ProductPlan为2时，无需配置该参数。 • ProductPlan为3时，NormalQps取值范围：500~100000，必须是100的整数倍。
NormalBandwidth	String	100	业务带宽，单位：Mbps。 不同实例类型（ProductPlan）支持的业务带宽（NormalBandwidth）取值不同。具体说明如下： • ProductPlan为0时，NormalBandwidth取值：100、150、200、250、300。 • ProductPlan为1时，NormalBandwidth取值：100、150、200、250、300。 • ProductPlan为2时，NormalBandwidth取值：10、20、30、40、50、60、70、80、90、100。 • ProductPlan为3时，NormalBandwidth取值：10、20、30、40、50、60、70、80、90、100、150、200。
PortCount	Float	5	防护端口数。 不同实例类型（ProductPlan）支持的防护端口数（PortCount）取值范围不同。具体说明如下： • ProductPlan为0时，PortCount取值范围：5~400，必须是5的整数倍。 • ProductPlan为1时，PortCount取值范围：5~400，必须是5的整数倍。 • ProductPlan为2时，无需配置PortCount。 • ProductPlan为3时，PortCount取值范围：5~400，必须是5的整数倍。

配置项（Code）	类型	示例值（Value）	描述
DomainCount	Float	10	防护域名数。 不同实例类型（ProductPlan）支持的防护域名数（DomainCount）取值范围不同。具体说明如下： • ProductPlan为0时，DomainCount取值范围：10~200，必须是10的整数倍。 • ProductPlan为1时，DomainCount取值范围：10~200，必须是10的整数倍。 • ProductPlan为2时，无需配置DomainCount。 • ProductPlan为3时，DomainCount取值范围：10~200，必须是10的整数倍。

返回数据

名称	类型	示例值	描述
Code	String	Success	HTTP状态码。
Data	Struct		返回数据。
InstanceId	String	ddoscoo-cn-zvp28101****	已创建的实例的ID。
OrderId	String	20951253014****	已生成的订单ID。
Message	String	Successful!	响应信息。
RequestId	String	B03994C3-2A94-45FA-A44D-19E7BC39DC6D	本次请求的ID。
Success	Boolean	true	本次请求是否成功。取值： • *true*：表示请求成功。 • *false*：表示请求失败。

示例

- 示例1：创建DDoS高防（新BGP）实例
  请求示例

```
http(s)://[Endpoint]/?Action=CreateInstance
&ProductCode=ddos
&ProductType=ddoscoo
&SubscriptionType=Subscription
&Period=1
&Parameter.1.Code=Edition
&Parameter.1.Value=coop
&Parameter.2.Code=FunctionVersion
&Parameter.2.Value=0
&Parameter.3.Code=NormalQps
&Parameter.3.Value=3000
&Parameter.4.Code=PortCount
&Parameter.4.Value=50
&Parameter.5.Code=DomainCount
&Parameter.5.Value=50
&Parameter.6.Code=ServiceBandwidth
&Parameter.6.Value=200
&Parameter.7.Code=BaseBandwidth
&Parameter.7.Value=30
&Parameter.8.Code=Bandwidth
&Parameter.8.Value=50
&Parameter.9.Code=ServicePartner
&Parameter.9.Value='coop-line-001'
&<公共请求参数>
```

正常返回示例

- `XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<CreateInstanceResponse>
    <RequestId>B03994C3-2A94-45FA-A44D-19E7BC39DC6D</RequestId>
    <Message>Successful!</Message>
    <Data>
        <InstanceId>ddoscoo-cn-zvp28101****</InstanceId>
        <OrderId>20951253014****</OrderId>
    </Data>
    <Code>Success</Code>
    <Success>true</Success>
</CreateInstanceResponse>
```

- JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId": "B03994C3-2A94-45FA-A44D-19E7BC39DC6D",
  "Message": "Successful!",
  "Data": {
    "InstanceId": "ddoscoo-cn-zvp28101****",
    "OrderId": 20951253014****
  },
  "Code": "Success",
  "Success": true
}
```

- 示例2：创建DDoS高防（国际）保险版实例

请求示例

```
http(s)://[Endpoint]/?Action=CreateInstance
&ProductCode=ddos
&ProductType=ddosDip
&SubscriptionType=Subscription
&Period=3
&Parameter.1.Code=Region
&Parameter.1.Value='ap-southeast-1'
&Parameter.2.Code=ProductPlan
&Parameter.2.Value=0
&Parameter.3.Code=FunctionVersion
&Parameter.3.Value=0
&Parameter.4.Code=NormalQps
&Parameter.4.Value=500
&Parameter.5.Code=NormalBandwidth
&Parameter.5.Value=100
&Parameter.6.Code=PortCount
&Parameter.6.Value=5
&Parameter.7.Code=DomainCount
&Parameter.7.Value=10
&<公共请求参数>
```

正常返回示例

- XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<CreateInstanceResponse>
    <RequestId>4DA44417-7BF7-474A-A3DC-D157EF6BD7CA</RequestId>
    <Message>Successful!</Message>
    <Data>
        <InstanceId>ddosDip-cn-i7m282j****</InstanceId>
        <OrderId>20951829465****</OrderId>
    </Data>
    <Code>Success</Code>
    <Success>true</Success>
</CreateInstanceResponse>
```

- `JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId": "4DA44417-7BF7-474A-A3DC-D157EF6BD7CA",
  "Message": "Successful!",
  "Data": {
    "InstanceId": "ddosDip-cn-i7m282j****",
    "OrderId": 20951829465****
  },
  "Code": "Success",
  "Success": true
}
```

- 示例3：创建DDoS高防（国际）加速线路实例
  请求示例

```
http(s)://[Endpoint]/?Action=CreateInstance
&ProductCode=ddos
&ProductType=ddosDip
&SubscriptionType=Subscription
&Period=3
&Parameter.1.Code=Region
&Parameter.1.Value='ap-southeast-1'
&Parameter.2.Code=ProductPlan
&Parameter.2.Value=2
&Parameter.3.Code=NormalBandwidth
&Parameter.3.Value=10
&<公共请求参数>
```

  正常返回示例

  - `XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<CreateInstanceResponse>
    <RequestId>4DA44417-7BF7-474A-A3DC-D157EF6BD7CA</RequestId>
    <Message>Successful!</Message>
    <Data>
        <InstanceId>ddosDip-cn-i7m282j****</InstanceId>
        <OrderId>20951829465****</OrderId>
    </Data>
    <Code>Success</Code>
    <Success>true</Success>
</CreateInstanceResponse>
```

- JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId": "4DA44417-7BF7-474A-A3DC-D157EF6BD7CA",
  "Message": "Successful!",
  "Data": {
    "InstanceId": "ddosDip-cn-i7m282j****",
    "OrderId": 20951829465****
  },
  "Code": "Success",
  "Success": true
}
```

7.实例管理

7.1. DescribeInstanceIds

调用DescribeInstanceIds查询DDoS高防实例的ID、版本、备注、IP类型信息。

使用说明

本接口用于查询所有DDoS高防实例的ID、版本、备注、IP类型信息。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstanceIds	要执行的操作。取值：**DescribeInstanceIds**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。
Edition	Integer	否	9	要查询的DDoS高防实例的类型。取值： • **0**：表示DDoS高防（国际）保险版。 • **1**：表示DDoS高防（国际）无忧版。 • **2**：表示DDoS高防（国际）加速线路。 • **9**：表示DDoS高防（新BGP）专业版。
InstanceIds.N	String	否	ddoscoo-cn-zvp2eibz****	要查询的DDoS高防实例的ID。 不设置该参数表示查询所有DDoS高防实例。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	310A41FD-0990-5610-92E0-A6A55D7C6444	本次请求的ID。
InstanceIds	Array of Instance		DDoS高防实例的ID、版本、备注、IP类型信息。
IpMode	String	fnat	实例的IP转发模式。取值： • **fnat**：表示源站和客户端的IP版本一致，即IPv4地址客户端请求转发到IPv4地址源站、IPv6地址客户端请求转发到IPv6地址源站。 • **v6tov4**：表示IPv6和IPv4地址客户端请求都转发到IPv4地址源站。
Edition	Integer	9	实例的类型。取值： • **0**：表示DDoS高防（国际）保险版。 • **1**：表示DDoS高防（国际）无忧版。 • **2**：表示DDoS高防（国际）加速线路。 • **3**：表示DDoS高防（国际）安全加速线路。 • **9**：表示DDoS高防（新BGP）专业版。
InstanceId	String	ddoscoo-cn-zvp2eibz****	实例ID。
IpVersion	String	Ipv4	实例的IP协议版本。取值： • **Ipv4**：表示 IPv4版本。 • **Ipv6**：表示 IPv6版本。
Remark	String	test	实例的备注。

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

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeInstanceIdsResponse>
    <RequestId>310A41FD-0990-5610-92E0-A6A55D7C6444</RequestId>
    <InstanceIds>
        <IpMode>fnat</IpMode>
        <Edition>9</Edition>
        <InstanceId>ddoscoo-cn-zvp2eibz****</InstanceId>
        <IpVersion>Ipv4</IpVersion>
        <Remark>test</Remark>
    </InstanceIds>
</DescribeInstanceIdsResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "310A41FD-0990-5610-92E0-A6A55D7C6444",
  "InstanceIds" : [ {
    "IpMode" : "fnat",
    "Edition" : 9,
    "InstanceId" : "ddoscoo-cn-zvp2eibz****",
    "IpVersion" : "Ipv4",
    "Remark" : "test"
  } ]
}
```

错误码

访问错误中心查看更多错误码。

7.2. DescribeInstances

调用DescribeInstances查询DDoS高防实例的详情列表。

使用说明

本接口用于分页查询当前阿里云账号拥有的DDoS高防实例的详情，例如，实例的ID、版本、到期时间、业务转发状态等。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstances	要执行的操作。取值：**DescribeInstances**。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。
PageNumber	String	是	1	分页查询时，设置当前页面的页码。
PageSize	String	是	10	分页查询时，设置每页包含实例的数量。
Ip	String	否	203.107.XX.XX	要查询的DDoS高防实例的IP地址。
Remark	String	否	doc-test	要查询的DDoS高防实例的备注。支持模糊查询。
Edition	Integer	否	9	要查询的DDoS高防实例的防护套餐版本。取值： • **0**：表示DDoS高防（国际）保险版。 • **1**：表示DDoS高防（国际）无忧版。 • **2**： 表示DDoS高防（国际）加速线路。 • **9**：表示DDoS高防（新BGP）专业版。
Enabled	Integer	否	1	要查询的DDoS高防实例的业务流量转发状态。取值： • **0**：表示已停止转发业务流量。 • **1**：表示正常转发业务流量。
ExpireStartTime	Long	否	1640361500000	要查询的DDoS高防实例的最早到期时间（即查询到期时间在**ExpireStartTime**之后的DDoS高防实例）。使用时间戳表示，单位：毫秒。
ExpireEndTime	Long	否	1640361700000	要查询的DDoS高防实例的最晚到期时间（即查询到期时间在**ExpireEndTime**之前的DDoS高防实例）。使用时间戳表示，单位：毫秒。
InstanceIds.N	String	否	ddoscoo-cn-7pp2g9ed****	要查询的DDoS高防实例的ID。
Status.N	Integer	否	1	要查询的DDoS高防实例的状态。取值： • **1**：表示正常。 • **2**：表示已过期。

名称	类型	是否必选	示例值	描述
Tag.N.Key	String	否	test-key	要查询的DDoS高防实例绑定的标签键。 说明 标签键（Key）和标签值（Value）必须成对出现。
Tag.N.Value	String	否	test-value	要查询的DDoS高防实例绑定的标签值。 说明 标签键（Key）和标签值（Value）必须成对出现。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
TotalCount	Long	1	查询到的DDoS高防实例的总数量。
RequestId	String	A0AF40CC-814A-5A86-AEAA-6F19E88B8A39	本次请求的ID。
Instances	Array of Instance		DDoS高防实例的详情列表。
Status	Integer	1	实例的状态。取值： • **1**：表示正常。 • **2**：表示已过期。
IpMode	String	fnat	实例的IP转发模式。取值： • **fnat**：表示源站和客户端的IP版本一致，即IPv4地址客户端请求转发到IPv4地址源站、IPv6地址客户端请求转发到IPv6地址源站。 • **v6tov4**：表示IPv6地址客户端请求转发到IPv4地址源站。
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。

名称	类型	示例值	描述
Edition	Integer	9	实例的防护套餐版本。取值： • **0**：表示DDoS高防（国际）保险版。 • **1**：表示DDoS高防（国际）无忧版。 • **2**： 表示DDoS高防（国际）加速线路。 • **9**：表示DDoS高防（新BGP）专业版。
IpVersion	String	Ipv4	实例的IP协议版本。取值： • **Ipv4**：表示IPv4协议。 • **Ipv6**：表示IPv6协议。
ExpireTime	Long	1640361600000	实例的到期时间。使用时间戳表示，单位：毫秒。
Remark	String	doc-test	实例的备注。
CreateTime	Long	1637751953000	实例的创建时间。使用时间戳表示，单位：毫秒。
Enabled	Integer	1	实例的业务流量转发状态。取值： • **0**：表示已停止转发业务流量。 • **1**：表示正常转发业务流量。
InstanceId	String	ddoscoo-cn-7pp2g9ed****	实例的ID。

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

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeInstancesResponse>
    <TotalCount>1</TotalCount>
    <RequestId>A0AF40CC-814A-5A86-AEAA-6F19E88B8A39</RequestId>
    <Instances>
        <Status>1</Status>
        <IpMode>fnat</IpMode>
        <DebtStatus>0</DebtStatus>
        <Edition>9</Edition>
        <IpVersion>Ipv4</IpVersion>
        <ExpireTime>1640361600000</ExpireTime>
        <Remark>doc-test</Remark>
        <CreateTime>1637751953000</CreateTime>
        <Enabled>1</Enabled>
        <InstanceId>ddoscoo-cn-7pp2g9ed****</InstanceId>
        <ConnInstanceId>1</ConnInstanceId>
    </Instances>
</DescribeInstancesResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "TotalCount" : 1,
  "RequestId" : "A0AF40CC-814A-5A86-AEAA-6F19E88B8A39",
  "Instances" : [ {
    "Status" : 1,
    "IpMode" : "fnat",
    "DebtStatus" : 0,
    "Edition" : 9,
    "IpVersion" : "Ipv4",
    "ExpireTime" : 1640361600000,
    "Remark" : "doc-test",
    "CreateTime" : 1637751953000,
    "Enabled" : 1,
    "InstanceId" : "ddoscoo-cn-7pp2g9ed****",
    "ConnInstanceId" : "1"
  } ]
}
```

错误码

访问错误中心查看更多错误码。

7.3. DescribeInstanceStatus

调用DescribeInstanceStatus查询指定的DDoS高防实例的状态。

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	DescribeInstanceStatus	要执行的操作。取值：**DescribeInstanceStatus**。
InstanceId	String	是	ddoscoo-cn-6ja1y6p5****	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（新BGP）或DDoS高防（国际）实例的ID。
ProductType	Integer	是	1	要查询的DDoS高防实例的类型。取值： • **1**：表示DDoS高防（新BGP）实例。 • **2**：表示DDoS高防（国际）实例。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
InstanceId	String	ddoscoo-cn-6ja1y6p5****	DDoS高防实例的ID。
InstanceStatus	Integer	1	DDoS高防实例的状态。取值： • **1**：表示正常。 • **2**：表示已过期。 • **3**：表示存在欠费。 • **4**：表示已释放。
RequestId	String	112777CC-2AD6-46FC-A263-00B931406FCD	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeInstanceStatus
&InstanceId=ddoscoo-cn-6ja1y6p5****
&ProductType=1
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeInstanceStatusResponse>
   <RequestId>112777CC-2AD6-46FC-A263-00B931406FCD</RequestId>
   <InstanceId>ddoscoo-cn-6ja1y6p5****</InstanceId>
   <InstanceStatus>1</InstanceStatus>
</DescribeInstanceStatusResponse>
```

JSON 格式

```
{
    "RequestId": "112777CC-2AD6-46FC-A263-00B931406FCD",
    "InstanceId": "ddoscoo-cn-6ja1y6p5****",
    "InstanceStatus": 1
}
```

错误码
访问错误中心查看更多错误码。

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

使用说明
本接口用于查询DDoS高防实例的IP和线路信息，例如，实例的IP地址、状态、防护线路等。

QPS限制
本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstanceDetails	要执行的操作。取值：**DescribeInstanceDetails**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。
InstanceIds.N	String	是	ddoscoo-cn-zvp2eibz****	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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	3C814429-21A5-4673-827E-FDD19DC75681	本次请求的ID。
InstanceDetails	Array of InstanceDetail		DDoS高防实例的IP和线路信息。
Line	String	coop-line-001	DDoS高防实例的防护线路。
InstanceId	String	ddoscoo-cn-zvp2eibz****	DDoS高防实例ID。
EipInfos	Array of EipInfo		DDoS高防实例的IP信息。
Status	String	normal	DDoS高防IP的状态。取值： • **normal**：表示正常。 • **expired**：表示已过期。
IpMode	String	fnat	IP转发模式。取值： • **fnat**：表示源站和客户端的IP版本一致，即IPv4地址客户端请求转发到IPv4地址源站、IPv6地址客户端请求转发到IPv6地址源站。 • **v6tov4**：表示IPv6地址客户端请求转发到IPv4地址源站。
Eip	String	203.117.XX.XX	DDoS高防IP地址。
IpVersion	String	Ipv4	IP协议版本。取值： • **Ipv4**：表示IPv4协议。 • **Ipv6**：表示IPv6协议。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeInstanceDetails
&InstanceIds=["ddoscoo-cn-zvp2eibz****"]
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeInstanceDetailsResponse>
    <RequestId>3C814429-21A5-4673-827E-FDD19DC75681</RequestId>
    <InstanceDetails>
        <Line>coop-line-001</Line>
        <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
        <EipInfos>
            <Status>normal</Status>
            <IpMode>fnat</IpMode>
            <Eip>203.117.XX.XX</Eip>
            <IpVersion>Ipv4</IpVersion>
        </EipInfos>
    </InstanceDetails>
</DescribeInstanceDetailsResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "3C814429-21A5-4673-827E-FDD19DC75681",
  "InstanceDetails" : [ {
    "Line" : "coop-line-001",
    "InstanceId" : "ddoscoo-cn-mp91j1ao****",
    "EipInfos" : [ {
      "Status" : "normal",
      "IpMode" : "fnat",
      "Eip" : "203.117.XX.XX",
      "IpVersion" : "Ipv4"
    } ]
  } ]
}
```

错误码

访问错误中心查看更多错误码。

7.5. DescribeInstanceSpecs

调用DescribeInstanceSpecs查询DDoS高防实例的规格配置。

使用说明

本接口用于批量查询DDoS高防实例的规格配置，例如，实例的业务带宽、防护带宽、功能套餐版本、支持防护的域名和端口数量等。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstanceSpecs	要执行的操作。取值：**DescribeInstanceSpecs**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。
InstanceIds.N	String	是	ddoscoo-cn-zvp2eibz****	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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	03C4A2E8-F647-5783-995C-AE49B6ACE925	本次请求的ID。
InstanceSpecs	Array of InstanceSpec		DDoS高防实例的规格配置列表。
BaseBandwidth	Integer	30	基础防护带宽。单位：Gbps。
QpsLimit	Integer	3000	正常业务QPS。
BandwidthMbps	Integer	100	正常业务带宽。单位：Mbps。
ElasticBw	Integer	300	弹性业务带宽。单位：Mbps。

名称	类型	示例值	描述
DefenseCount	Integer	2	本月可用高级防护的次数。-1表示无限次。 说明 只有当请求参数RegionId为ap-southeast-1（表示查询DDoS高防国际实例）时，才会返回该参数。
SiteLimit	Integer	5	实例可防护站点的数量。
PortLimit	Integer	50	实例可防护端口的数量。
ElasticBandwidth	Integer	30	弹性防护带宽。单位：Gbps。
FunctionVersion	String	default	实例的功能套餐类型。取值： • default：表示标准功能套餐。 • enhance：表示增强功能套餐。 • cnhk：表示加速线路。 • cnhk_default：表示安全加速线路标准功能。 • cnhk_enhance：表示安全加速线路增强功能。
InstanceId	String	ddoscoo-cn-zvp2eibz****	实例ID。
DomainLimit	Integer	50	实例可防护域名的数量。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeInstanceSpecs
&InstanceIds=["ddoscoo-cn-zvp2eibz****"]
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeInstanceSpecsResponse>
    <RequestId>03C4A2E8-F647-5783-995C-AE49B6ACE925</RequestId>
    <InstanceSpecs>
        <BaseBandwidth>30</BaseBandwidth>
        <QpsLimit>3000</QpsLimit>
        <BandwidthMbps>100</BandwidthMbps>
        <ElasticBw>300</ElasticBw>
        <SiteLimit>5</SiteLimit>
        <PortLimit>50</PortLimit>
        <ElasticBandwidth>30</ElasticBandwidth>
        <FunctionVersion>default</FunctionVersion>
        <InstanceId>ddoscoo-cn-zvp2eibz****</InstanceId>
        <DomainLimit>50</DomainLimit>
    </InstanceSpecs>
</DescribeInstanceSpecsResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "03C4A2E8-F647-5783-995C-AE49B6ACE925",
  "InstanceSpecs" : [ {
    "BaseBandwidth" : 30,
    "QpsLimit" : 3000,
    "BandwidthMbps" : 100,
    "ElasticBw" : 300,
    "SiteLimit" : 5,
    "PortLimit" : 50,
    "ElasticBandwidth" : 30,
    "FunctionVersion" : "default",
    "InstanceId" : "ddoscoo-cn-zvp2eibz****",
    "DomainLimit" : 50
  } ]
}
```

错误码

访问错误中心查看更多错误码。

7.6. 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。

7.7. 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**
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
Remark	String	是	new-remark	为该实例设置备注。 支持使用中文字符、英文大小写字符、数字及部分特殊字符，例如：`,.+-*/_`。最长不允许超过500个字符。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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。

7.8. 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。

7.9. 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。

7.10. DescribeDefenseCountStatistics

调用DescribeDefenseCountStatistics查询DDoS高防（国际）服务的高级防护次数统计数据。

使用说明

本接口用于查询DDoS高防（国际）服务的高级防护次数统计数据，例如，当前自然月已使用的高级防护次数、高级防护资源包中剩余可用的高级防护次数等。

> 注意 本接口只适用于DDoS高防（国际）服务。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDefenseCountStatistics	要执行的操作。取值：**DescribeDefenseCountStatistics**。
RegionId	String	否	ap-southeast-1	DDoS高防实例所属地域ID。取值固定为**ap-southeast-1**，表示非中国内地，即DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文示例中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	310A41FD-0990-5610-92E0-A6A55D7C6444	本次请求的ID。
DefenseCountStatistics	Object		高级防护次数统计数据。
FlowPackCountRemain	Integer	0	高级防护资源包中剩余可用的保险版高级防护次数。
MaxUsableDefenseCountCurrentMonth	Integer	20	当前自然月可使用的高级防护次数（包含实例自带的高级防护和高级防护资源包提供的高级防护）的上限。
DefenseCountTotalUsageOfCurrentMonth	Integer	0	当前自然月已使用的高级防护总次数（包含实例自带的高级防护和高级防护资源包提供的高级防护）。

名称	类型	示例值	描述
SecHighSpeedCountRemain	Integer	0	高级防护资源包中剩余可用的安全加速线路高级防护次数。

示例

请求示例

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

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeDefenseCountStatisticsResponse>
    <RequestId>310A41FD-0990-5610-92E0-A6A55D7C6444</RequestId>
    <DefenseCountStatistics>
        <FlowPackCountRemain>0</FlowPackCountRemain>
        <MaxUsableDefenseCountCurrentMonth>20</MaxUsableDefenseCountCurrentMonth>
        <DefenseCountTotalUsageOfCurrentMonth>0</DefenseCountTotalUsageOfCurrentMonth>
        <SecHighSpeedCountRemain>0</SecHighSpeedCountRemain>
    </DefenseCountStatistics>
</DescribeDefenseCountStatisticsResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "310A41FD-0990-5610-92E0-A6A55D7C6444",
  "DefenseCountStatistics" : {
    "FlowPackCountRemain" : 0,
    "MaxUsableDefenseCountCurrentMonth" : 20,
    "DefenseCountTotalUsageOfCurrentMonth" : 0,
    "SecHighSpeedCountRemain" : 0
  }
}
```

错误码

访问错误中心查看更多错误码。

7.11. ReleaseInstance

调用ReleaseInstance释放已经到期的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。

- 建议您在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，建议您在DDoS高防实例到期前恢复已接入防护的业务IP（不再使用DDoS高防IP作

为业务IP）或业务DNS解析（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高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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。

8.域名接入

8.1. DescribeDomains

调用DescribeDomains查询所有已配置网站业务转发规则的域名。

\<ph>测试ph</ph>

<ph props="china">测试ph</ph>

只发布国内站

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高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。关于资源组的更多信息，请参见创建资源组。
InstanceIds.N	RepeatList	否	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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
Domains	List	["www.aliyun.com"]	已配置网站业务转发规则的域名列表。

名称	类型	示例值	描述
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。

8.2. DescribeWebRules

调用DescribeWebRules查询网站业务转发规则的配置。

使用说明

本接口用于分页查询您已创建的网站业务转发规则的配置，例如，转发协议类型、源站服务器地址、HTTPS配置、IP黑名单配置等。

调用本接口前，您必须已经调用CreateWebRule创建了网站业务转发规则。

QPS限制

本接口的单用户QPS限制为50次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeWebRules	要执行的操作。取值：**DescribeWebRules**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。
Domain	String	否	www.aliyundoc.com	要查询的网站域名。 **说明** 域名必须已经配置过网站业务转发规则。您可以调用DescribeDomains查询所有已经配置过网站业务转发规则的域名。
QueryDomainPattern	String	否	fuzzy	查询匹配模式。取值： • **fuzzy**（默认）：表示模糊查询。 • **exact**：表示精确查询。
PageNumber	Integer	否	1	分页查询时，设置当前页面的页码。默认值为**1**。
PageSize	Integer	是	10	分页查询时，设置每页包含转发规则的数量。
InstanceIds.N	String	否	ddoscoo-cn-i7m27nf3****	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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
TotalCount	Long	1	查询到的网站业务转发规则的总数量。

名称	类型	示例值	描述
RequestId	String	0F5B72DD-96F4-423A-B12B-A5151DD746B8	本次请求的ID。
WebRules	Array of WebRule		网站业务转发规则的配置。
Domain	String	www.aliyundoc.com	网站域名。
Http2HttpsEnable	Boolean	true	是否开启了HTTPS强制跳转功能。取值： • **true**：表示已开启。 • **false**：表示未开启。
SslProtocols	String	tls1.0	支持的TLS协议版本。取值： • **tls1.0**：表示支持TLS 1.0及以上版本。 • **tls1.1**：表示支持TLS 1.1及以上版本。 • **tls1.2**：表示支持TLS 1.2及以上版本。
PunishReason	Integer	1	域名受到违规处罚的原因。取值： • **1**：表示域名未履行ICP备案。 • **2**：表示域名经营的业务不符合监管要求。 如果同时包含原因1和2，该参数返回2。
CcTemplate	String	default	频率控制防护（CC防护）的模式。取值： • **default**：表示正常模式。 • **gf_under_attack**：表示攻击紧急模式。 • **gf_sos_verify**：表示严格模式。 • **gf_sos_enhance**：表示超级严格模式。
CcEnabled	Boolean	true	是否开启了频率控制防护（CC防护）。取值： • **true**：表示已开启。 • **false**：表示未开启。
SslCiphers	String	default	加密套件的类型。取值： • **default**：表示自定义加密套件。 • **all**：表示全部加密套件，包含强加密套件和弱加密套件。 • **strong**：表示强加密套件。
Ssl13Enabled	Boolean	false	是否开启了TLS 1.3协议支持。取值： • **true**：表示已开启。 • **false**：表示未开启。

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**：表示已开启。 • **false**：表示未开启。
OcspEnabled	Boolean	false	是否启用了OCSP（Online Certificate Status Protocol）功能。取值： • **true**：表示已开启。 • **false**：表示未开启。
PunishStatus	Boolean	true	域名是否受到违规处罚。取值： • **true**：表示已受到违规处罚。您可以通过**PunishReason**查看受到违规处罚的具体原因。 • **false**：表示未受到违规处罚。
ProxyEnabled	Boolean	true	网站业务转发是否开启。取值： • **true**：表示已开启。 • **false**：表示未开启。
CertName	String	testcert	证书名称。
PolicyMode	String	ip_hash	回源负载算法的类型。取值： • **ip_hash**：表示IP Hash算法。根据请求来源IP进行HASH映射，将同一个IP的所有请求定向到一个源站服务器。 • **rr**：表示轮转算法。将所有请求轮流分配给不同源站服务器。 • **least_time**：表示Least Time算法。该算法通过智能DNS解析能力，保证业务流量从接入防护节点到转发回源站服务器整个链路的时延最短。
Cname	String	o8fzz0ocxere****.aliyunddos****.com	网站域名对应的DDoS高防CNAME地址。
Http2Enable	Boolean	true	是否开启了HTTP 2.0协议支持。取值： • **true**：表示已开启。 • **false**：表示未开启。
Https2HttpEnable	Boolean	true	是否开启了HTTP回源功能。取值： • **true**：表示已开启。 • **false**：表示未开启。
ProxyTypes	Array of ProxyConfig		转发协议和端口配置。

名称	类型	示例值	描述
ProxyType	String	https	转发协议类型。取值： • **http**：表示HTTP协议。 • **https**：表示HTTPS协议。 • **websocket**：表示WebSocket协议。 • **websockets**：表示WebSockets协议。
ProxyPorts	Array of String	443	端口。
RealServers	Array of RealServer		源站服务器地址信息。
RsType	Integer	0	源站服务器地址的类型。取值： • **0**：表示源站服务器的IP地址。 • **1**：表示源站服务器的域名地址。通常适用于源站和高防之间还部署有其他代理服务（例如WAF）的场景，具体指代理服务的跳转地址（例如WAF CNAME地址）。
RealServer	String	192.0.XX.XX	源站服务器地址。
WhiteList	Array of String	192.1.XX.XX	针对该域名的白名单IP。 **说明** 仅在您已经为该域名配置了IP白名单（针对域名）时返回该结果。您可以调用ConfigWebIpSet为网站域名配置IP黑白名单。
BlackList	Array of String	192.2.XX.XX	针对该域名的黑名单IP。 **说明** 仅在您已经为该域名配置了IP黑名单（针对域名）时返回该结果。您可以调用ConfigWebIpSet为网站域名配置IP黑白名单。
CustomCiphers	Array of String	ECDHE-ECDSA-AES128-GCM-SHA256	自定义加密套件。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeWebRules
&Domain=www.aliyun.com
&QueryDomainPattern=fuzzy
&PageNumber=1
&PageSize=10
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeWebRulesResponse>
    <TotalCount>1</TotalCount>
    <RequestId>0F5B72DD-96F4-423A-B12B-A5151DD746B8</RequestId>
    <WebRules>
        <Domain>www.aliyundoc.com</Domain>
        <Http2HttpsEnable>true</Http2HttpsEnable>
        <SslProtocols>tls1.0</SslProtocols>
        <PunishReason>1</PunishReason>
        <CcTemplate>default</CcTemplate>
        <CcEnabled>true</CcEnabled>
        <SslCiphers>default</SslCiphers>
        <Ssl13Enabled>false</Ssl13Enabled>
        <CcRuleEnabled>false</CcRuleEnabled>
        <OcspEnabled>false</OcspEnabled>
        <PunishStatus>true</PunishStatus>
        <ProxyEnabled>true</ProxyEnabled>
        <CertName>testcert</CertName>
        <PolicyMode>ip_hash</PolicyMode>
        <Cname>o8fzz0ocxere****.aliyunddos****.com</Cname>
        <Http2Enable>true</Http2Enable>
        <Https2HttpEnable>true</Https2HttpEnable>
        <ProxyTypes>
            <ProxyType>https</ProxyType>
            <ProxyPorts>443</ProxyPorts>
        </ProxyTypes>
        <RealServers>
            <RsType>0</RsType>
            <RealServer>192.0.XX.XX</RealServer>
        </RealServers>
        <WhiteList>192.1.XX.XX</WhiteList>
        <BlackList>192.2.XX.XX</BlackList>
        <CustomCiphers>ECDHE-ECDSA-AES128-GCM-SHA256</CustomCiphers>
    </WebRules>
</DescribeWebRulesResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "TotalCount" : 1,
  "RequestId" : "0F5B72DD-96F4-423A-B12B-A5151DD746B8",
  "WebRules" : [ {
    "Domain" : "www.aliyundoc.com",
    "Http2HttpsEnable" : true,
    "SslProtocols" : "tls1.0",
    "PunishReason" : 1,
    "CcTemplate" : "default",
    "CcEnabled" : true,
    "SslCiphers" : "default",
    "Ssl13Enabled" : false,
    "CcRuleEnabled" : false,
    "OcspEnabled" : false,
    "PunishStatus" : true,
    "ProxyEnabled" : true,
    "CertName" : "testcert",
    "PolicyMode" : "ip_hash",
    "Cname" : "o8fzz0ocxere****.aliyunddos****.com",
    "Http2Enable" : true,
    "Https2HttpEnable" : true,
    "ProxyTypes" : [ {
      "ProxyType" : "https",
      "ProxyPorts" : [ "443" ]
    } ],
    "RealServers" : [ {
      "RsType" : 0,
      "RealServer" : "192.0.XX.XX"
    } ],
    "WhiteList" : [ "192.1.XX.XX" ],
    "BlackList" : [ "192.2.XX.XX" ],
    "CustomCiphers" : [ "ECDHE-ECDSA-AES128-GCM-SHA256" ]
  } ]
}
```

错误码

访问错误中心查看更多错误码。

8.3. CreateWebRule

调用CreateWebRule创建一条网站业务转发规则。

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**。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。 关于资源组的更多信息，请参见创建资源组。
Domain	String	是	www.aliyun.com	要接入DDoS高防进行防护的网站域名。
RsType	Integer	是	0	源站服务器的地址类型。取值： • **0**：表示源站服务器的IP地址。 • **1**：表示源站服务器的域名地址。通常适用于源站和高防之间还部署有其他代理服务（例如WAF）的场景，具体指代理服务的跳转地址（例如WAF CNAME地址）。

Rules	String	是	[{"ProxyRules":[{"ProxyPort":443,"RealServers":["192.XX.XX.1"]}],"ProxyType":"https"}]	网站业务转发规则的详细配置。使用JSON数组转化的字符串格式表示。JSON数组中的每个元素是一个JSON结构体，包含以下字段：
				• **ProxyRules**：JSONArray类型 | 必选 | 源站服务器信息，包括端口号和服务器地址。数组中每个元素是一个JSON结构体，包含以下字段：
				  ◦ **ProxyPort**：Integer类型 | 必选 | 协议对应的端口号。
				  ◦ **RealServers**：StringArray类型 | 必选 | 服务器地址。
				• **ProxyType**：String类型 | 必选 | 网站协议类型。取值：**http** | **https** | **websocket** | **websockets**。

名称	类型	是否必选	示例值	描述
HttpsExt	String	否	{"Http2":1,"Http2https":1，"Https2http":1}	HTTPS高级设置，仅在网站协议类型支持HTTPS（**ProxyType**包含**https**）时生效。使用JSON结构体转化的字符串格式表示，JSON结构体包含以下字段： • **Http2https**：Integer类型 | 可选 | 是否开启HTTPS的强制跳转功能，取值：**0**（表示关闭）| **1**（表示开启），默认关闭。 适用于您的网站同时支持HTTP和HTTPS协议。开启该设置后，所有HTTP请求将强制转换为HTTPS请求，且默认跳转到443端口。 • **Https2http**：Integer类型 | 可选 | 是否开启HTTP回源功能，取值：**0**（表示关闭）| **1**（表示开启），默认关闭。 适用于您的网站不支持HTTPS回源。开启该设置后，所有HTTPS协议请求将通过HTTP回源（Websockets协议会通过Websocket回源），且默认回源端口为80。 • **Http2**：Integer类型 | 可选 | 是否启用HTTP2.0协议类型，取值：**0**（表示关闭）| **1**（表示开启），默认关闭。 开启该设置后，协议版本为HTTP2.0。
DefenseId	String	否	aaa.bbb.cn	要关联的防护ID。该参数适用于其他云服务（例如对象存储OSS）集成了DDoS高防的场景。 **说明** 该参数在内部测试中，暂时请勿使用。 示例：如果您的OSS服务集成了DDoS高防，则高防会为OSS生产账号分配一组IP资源池，每一个IP资源对应唯一的防护ID。防护ID是一个CNAME地址，该CNAME默认解析到对应的高防IP。防护ID（即CNAME）可以通过解析复用同一个IP，便于灵活调度。 **说明** 不允许同时填写InstanceIds和DefenseId。

名称	类型	是否必选	示例值	描述
InstanceIds.N	String	否	ddoscoo-cn-i7m27nf3****	要关联的DDoS高防实例的ID。不设置该参数表示只添加网站域名，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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	CB3261D2-7D1B-4ADA-9E98-A200B2CDA2DC	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":443,"RealServers":["192.XX.XX.1"]}],"ProxyType":"https"}]
&HttpsExt={"Http2":1,"Http2https":1, "Https2http":1}
&InstanceIds=["ddoscoo-cn-i7m27nf3****"]
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<CreateWebRuleResponse>
    <RequestId>CB3261D2-7D1B-4ADA-9E98-A200B2CDA2DC</RequestId>
</CreateWebRuleResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "CB3261D2-7D1B-4ADA-9E98-A200B2CDA2DC"
}
```

错误码

访问错误中心查看更多错误码。

8.4. ModifyWebRule

调用ModifyWebRule修改已创建的网站业务转发规则。您可以修改网站业务转发规则中的源站服务器和协议信息、关联的DDoS高防实例、HTTPS高级设置。

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	ModifyWebRule	要执行的操作。取值：**ModifyWebRule**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。关于资源组的更多信息，请参见创建资源组。
Domain	String	是	www.aliyun.com	要操作的网站业务的域名。 **说明** 域名必须已经配置过网站业务转发规则。您可以调用DescribeDomains查询所有已经配置过网站业务转发规则的域名。
ProxyTypes	String	是	[{"ProxyType":"https","ProxyPorts":[443]}]	网站业务转发规则的协议信息。使用JSON数组转化的字符串格式表示。JSON数组中的每个元素是一个JSON结构体，包含以下字段： • **ProxyType**：String类型 | 必选 | 网站协议类型。取值：**http** | **https** | **websocket** | **websockets**。 • **ProxyPort**：Integer类型 | 必选 | 协议对应的端口号。

名称	类型	是否必选	示例值	描述
RsType	Integer	是	0	源站服务器的地址类型。取值： • **0**：表示源站服务器的IP地址。 • **1**：表示源站服务器的域名地址。通常适用于源站和高防之间还部署有其他代理服务（例如WAF）的场景，具体指代理服务的跳转地址（例如WAF CNAME地址）。
HttpsExt	String	否	{"Http2":1,"Http2https":1，"Https2http":1}	HTTPS高级设置，仅在网站协议类型支持HTTPS（**ProxyType**包含**https**）时生效。使用JSON结构体转化的字符串格式表示，JSON结构体包含以下字段： • **Http2https**：Integer类型 | 可选 | 是否开启HTTPS的强制跳转功能，取值：**0**（表示关闭）| **1**（表示开启），默认关闭。 适用于您的网站同时支持HTTP和HTTPS协议。开启该设置后，所有HTTP请求将强制转换为HTTPS请求，且默认跳转到443端口。 • **Https2http**：Integer类型 | 可选 | 是否开启HTTP回源功能，取值：**0**（表示关闭）| **1**（表示开启），默认关闭。 适用于您的网站不支持HTTPS回源。开启该设置后，所有HTTPS协议请求将通过HTTP回源（Websockets协议会通过Websocket回源），且默认回源端口为80。 • **Http2**：Integer类型 | 可选 | 是否启用HTTP2.0协议类型，取值：**0**（表示关闭）| **1**（表示开启），默认关闭。 开启该设置后，协议版本为HTTP2.0。
RealServers.N	String	是	192.XX.XX.2	源站服务器地址。
InstanceIds.N	String	否	ddoscoo-cn-i7m27nf3****	要关联的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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	CB3261D2-7D1B-4ADA-9E98-A200B2CDA2DC	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyWebRule
&Domain=www.aliyun.com
&ProxyTypes=[{"ProxyType":"https","ProxyPorts":[443]}]
&RsType=0
&HttpsExt={"Http2":1,"Http2https":1, "Https2http":1}
&RealServers=["192.XX.XX.2"]
&InstanceIds=["ddoscoo-cn-i7m27nf3****"]
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyWebRuleResponse>
    <RequestId>CB3261D2-7D1B-4ADA-9E98-A200B2CDA2DC</RequestId>
</ModifyWebRuleResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "CB3261D2-7D1B-4ADA-9E98-A200B2CDA2DC"
}
```

错误码

访问错误中心查看更多错误码。

8.5. DeleteWebRule

调用DeleteWebRule删除网站业务转发规则。

> **说明** 删除网站业务转发规则前，请确保您已经网站域名的解析切回源站服务器。如果您在网站域名的解析指向DDoS高防的情况下，删除了对应的网站业务转发规则，将会导致网站无法访问。

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**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。关于资源组的更多信息，请参见创建资源组。
Domain	String	是	www.aliyun.com	要删除的网站业务的域名。 **说明** 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有已配置网站业务转发规则的域名。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	9EC62E89-BD30-4FCD-9CB8-FA53865FF0D7	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

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DeleteWebRuleResponse>
    <RequestId>9EC62E89-BD30-4FCD-9CB8-FA53865FF0D7</RequestId>
</DeleteWebRuleResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "9EC62E89-BD30-4FCD-9CB8-FA53865FF0D7"
}
```

错误码

访问错误中心查看更多错误码。

8.6. 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。

名称	类型	示例值	描述
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。
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。

8.7. 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。

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
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。

8.8. 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**

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。
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/MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvIAqYxXZ7wRwWWmv4TMxFhWRiNY7yZIo2ZUhl02SIDNgglEeg== -----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**。
Key	String	否	-----BEGIN RSA PRIVATE KEY----- DADTPZoOHd9WtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThLyvsmLQKBgQCr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJaiygoIYoaMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04RtKadOw== -----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。

8.9. 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。

8.10. 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。

8.11. 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	ModifyHttp2Enable	要执行的操作。取值：**ModifyHttp2Enable**
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。
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。

8.12. 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。

名称	类型	示例值	描述
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。

8.13. 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
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。

8.14. 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。

名称	类型	示例值	描述
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。

8.15. 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。
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。

8.16. DescribeL7RsPolicy

调用DescribeL7RsPolicy查询网站业务转发规则的回源策略。

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	DescribeL7RsPolicy	要执行的操作。取值：**DescribeL7RsPolicy**。
Domain	String	是	www.aliyun.com	要查询的网站业务的域名。 **说明** 域名必须已经配置过网站业务转发规则。您可以调用DescribeDomains查询所有已经配置过网站业务转发规则的域名。
RegionId	String	否	cn-hangzhou	DDoS高防服务的地域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。

名称	类型	是否必选	示例值	描述
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。 关于资源组的更多信息，请参见创建资源组。
RealServers.N	RepeatList	否	1.***.***.1	要查询的源站服务器地址列表。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
Attributes	Array of AttributeItem		回源参数信息。
Attribute	Struct		回源参数。
Weight	Integer	100	服务器的权重。仅在使用轮询算法（**ProxyMode**为**rr**）时生效。 权重取值范围：**1~100**，默认值为**100**。权重越高的服务器分配到的请求越多。
RealServer	String	1.***.***.1	源站服务器地址。
RsType	Integer	0	源站服务器的地址类型。取值： • **0**：表示源站服务器的IP地址。 • **1**：表示源站服务器的域名地址。
ProxyMode	String	rr	回源负载均衡算法。取值： • **ip_hash**：表示IP Hash算法。根据请求来源IP进行HASH映射，将同一个IP的所有请求定向到一个源站服务器。 • **rr**：表示轮询算法。将所有请求轮流分配给不同源站服务器。 • **least_time**：表示Least Time算法。该算法通过智能DNS解析能力，保证业务流量从接入防护节点到转发回源站服务器整个链路的时延最短。
RequestId	String	9E7F6B2C-03F2-462F-9076-B782CF0DD502	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeL7RsPolicy
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeL7RsPolicyResponse>
   <RequestId>9E7F6B2C-03F2-462F-9076-B782CF0DD502</RequestId>
   <Attributes>
      <RealServer>1.***.***.1</RealServer>
      <Attribute>
         <Weight>100</Weight>
      </Attribute>
   </Attributes>
   <Attributes>
      <RealServer>2.***.***.2</RealServer>
      <Attribute>
         <Weight>100</Weight>
      </Attribute>
   </Attributes>
   <ProxyMode>rr</ProxyMode>
</DescribeL7RsPolicyResponse>
```

`JSON` 格式

```
{
 "RequestId": "9E7F6B2C-03F2-462F-9076-B782CF0DD502",
 "Attributes": [
  {
   "RealServer": "1.***.***.1",
   "Attribute": {
    "Weight": 100
   }
  },
  {
   "RealServer": "2.***.***.2",
   "Attribute": {
    "Weight": 100
   }
  }
 ],
 "ProxyMode": "rr"
}
```

错误码

访问错误中心查看更多错误码。

8.17. ConfigL7RsPolicy

调用ConfigL7RsPolicy为已经创建的网站业务转发规则设置回源策略。

如果接入DDoS高防的网站配置了多个源站服务器，您可以通过回源策略修改回源负载算法。默认使用IP Hash算法，支持修改为轮询或Leaset Time算法。具体说明请参见请求参数**Policy**的描述。

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	ConfigL7RsPolicy	要执行的操作。取值：**ConfigL7RsPolicy**。
Domain	String	是	www.aliyun.com	要操作的网站业务的域名。 **说明** 域名必须已经配置过网站业务转发规则。您可以调用DescribeDomains查询所有已经配置过网站业务转发规则的域名。

Policy	String	是	{"ProxyMode":"rr","Attributes":[{"RealServer":"1.***.***.1","Attribute":{"Weight":100}},{"RealServer":"2.***.***.2","Attribute":{"Weight":100}}]}	回源策略。使用JSON结构体转化的字符串格式表示，JSON结构体包含以下字段：
				• **ProxyMode**：String类型 | 必选 | 回源负载均衡算法。取值：
				  ○ **ip_hash**：表示IP Hash算法。根据请求来源IP进行HASH映射，将同一个IP的所有请求定向到一个源站服务器。
				  ○ **rr**：表示轮询算法。将所有请求轮流分配给不同源站服务器。使用该算法时，您可以根据不同服务器的性能为服务器设置权重。
				  ○ **least_time**：表示Least Time算法。该算法通过智能DNS解析能力，保证业务流量从接入防护节点到转发回源站服务器整个链路的时延最短。
				• **Attributes**：JSONArray类型 | 可选 | 回源参数信息。数组中每个元素包含以下字段：
				  ○ **RealServer**：String类型 | 可选 | 源站服务器地址。
				  ○ **Attribute**：JSONObject类型 | 可选 | 回源参数。包含以下字段：
				  ■ **Weight**：Integer类型 | 可选 | 服务器的权重。仅在使用轮询算法（**ProxyMode**为**rr**）时生效。权重取值范围：**1~100**，默认值为**100**。权重越高的服务器分配到的请求越多。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防服务的地域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	rg-acfm2pz25js****	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。 关于资源组的更多信息，请参见创建资源组。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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=ConfigL7RsPolicy
&Domain=www.aliyun.com
&Policy={\"ProxyMode\":\"rr\",\"Attributes\":[{\"RealServer\":\"1.***.***.1\",\"Attribute\":{
\"Weight\":100}},{\"RealServer\":\"2.***.***.2\",\"Attribute\":{\"Weight\":100}}]}
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<ConfigL7RsPolicyResponse>
   <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigL7RsPolicyResponse>
```

`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。

9.端口接入

9.1. 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。

名称	类型	示例值	描述
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。

9.2. 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。

9.3. 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。

9.4. 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。
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。

9.5. 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。

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
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。
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**

名称	类型	示例值	描述
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。

9.6. 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。
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。

9.7. 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。

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
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。
Protocol	String	tcp	转发协议。取值： • **tcp** • **udp**
RealServerStatusList	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。

9.8. ConfigLayer4RuleBakMode

调用ConfigLayer4RuleBakMode修改端口转发规则的回源模式（启用或关闭主备回源）。

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	ConfigLayer4RuleBakMode	要执行的操作。取值：**ConfigLayer4RuleBakMode**。
Listeners	String	是	[{\"InstanceId\":\"ddosDip-sg-4hr2b3l****\",\"FrontendPort\":2020,\"Protocol\":\"udp\"}]	要设置的端口转发规则。 该参数使用JSON数组转换的字符串表示。JSON数组的每个元素表示一个已创建的端口转发规则。一次最多可以设置1个端口转发规则。 **说明** 您可以调用DescribeNetworkRules查询所有已创建的端口转发规则。 每个端口转发规则包含以下字段： • **InstanceId**：String类型，必选，DDoS高防实例的ID。 • **Protocol**：String类型，必选，端口转发协议类型。取值：**tcp**、**udp**。 • **FrontendPort**：Integer类型，必选，转发端口。
BakMode	String	是	1	设置回源模式。取值： • **0**：表示默认回源模式，即DDoS高防将业务流量转发到您调用CreateNetworkRules创建该端口转发规则时指定的源站IP地址。 • **1**：表示主备回源模式，即DDoS高防将业务流量转发到您调用ConfigLayer4RulePolicy设置的主源站IP地址或备源站IP地址。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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=ConfigLayer4RuleBakMode
&BakMode=1
&Listeners=[{\"InstanceId\":\"ddosDip-sg-4hr2b3l****\",\"FrontendPort\":2020,\"Protocol\":\"udp\"}]
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<ConfigLayer4RuleBakModeResponse>
   <RequestId>CC042262-15A3-4A49-ADF0-130968EA47BC</RequestId>
</ConfigLayer4RuleBakModeResponse>
```

`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。

9.9. ConfigLayer4RulePolicy

调用ConfigLayer4RulePolicy为端口转发规则设置主、备源站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

名称	类型	是否必选	示例值	描述
Action	String	是	ConfigLayer4RulePolicy	要执行的操作。取值：**ConfigLayer4RulePolicy**。
Listeners	String	是	[{\"InstanceId\":\"ddosDip-sg-4hr2b3l****\",\"Protocol\":\"udp\",\"FrontendPort\":2020,\"BackendPort\":2022,\"PriRealServers\":[{\"RealServer\":\"192.0.2.1\"},{\"RealServer\":\"192.0.2.2\"}],\"SecRealServers\":[{\"RealServer\":\"192.0.2.3\"},{\"RealServer\":\"192.0.2.4\"}],\"CurrentRsIndex\":1}]	设置端口转发规则。 该参数使用JSON数组转换的字符串表示。JSON数组的每个元素表示一个已创建的端口转发规则。一次最多可以设置1个端口转发规则。 **说明** 您可以调用DescribeNetworkRules查询所有已创建的端口转发规则。 每个端口转发规则包含以下字段： • **InstanceId**：String类型，必选，DDoS高防实例的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。 • **PriRealServers**：JSON数组类型，必选，主源站IP地址列表。JSON数组的每个元素表示一个主源站IP地址。最多支持设置20个主源站IP地址。 每个主源站IP地址包含以下字段： ○ **RealServer**：String类型，必选，主源站IP地址。 • **SecRealServers**：JSON数组类型，必选，备源站IP地址列表。JSON数组的每个元素表示一个备源站IP地址。最多支持设置20个备源站IP地址。 每个备源站IP地址包含以下字段： ○ **RealServer**：String类型，必选，备源站IP地址。 • **CurrentRsIndex**：Integer类型，必选，要生效的源站类型。取值： ○ **1**：表示主源站设置生效（DDoS高防将业务流量转发到主源站IP地址）。 ○ **2**：表示备源站设置生效（DDoS高防将业务流量转发到备源站IP地址）。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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=ConfigLayer4RulePolicy
&Listeners=[{\"InstanceId\":\"ddosDip-sg-4hr2b3l****\",\"Protocol\":\"udp\",\"FrontendPort\":
2020,\"BackendPort\":2022,\"PriRealServers\":[{\"RealServer\":\"192.0.2.1\"},{\"RealServer\":
\"192.0.2.2\"}],\"SecRealServers\":[{\"RealServer\":\"192.0.2.3\"},{\"RealServer\":\"192.0.2.
4\"}],\"CurrentRsIndex\":1}]
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<ConfigLayer4RulePolicyResponse>
   <RequestId>CC042262-15A3-4A49-ADF0-130968EA47BC</RequestId>
</ConfigLayer4RulePolicyResponse>
```

`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。

9.10. ConfigLayer4Remark

调用ConfigLayer4Remark为端口转发规则添加备注。

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	ConfigLayer4Remark	要执行的操作。取值：**ConfigLayer4Remark**。
Listeners	String	是	[{\"InstanceId\":\"ddosDip-sg-4hr2b3l****\",\"FrontendPort\":2020,\"Protocol\":\"udp\",\"Remark\":\"test\"}]	要设置的端口转发规则。 该参数使用JSON数组转换的字符串表示。JSON数组的每个元素表示一个已创建的端口转发规则。一次最多可以设置1个端口转发规则。 **说明** 您可以调用DescribeNetworkRules查询所有已创建的端口转发规则。 每个端口转发规则包含以下字段： • **InstanceId**：String类型，必选，DDoS高防实例的ID。 • **Protocol**：String类型，必选，端口转发协议类型。取值：**tcp**、**udp**。 • **FrontendPort**：Integer类型，必选，转发端口。 • **Remark**：String类型，必选，备注。支持使用中文字符、英文大小写字符、数字及部分特殊字符，例如：`,.+-*/_`。最长不允许超过200个字符。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	6E46CC51-36BE-1100-B14C-DAF8381B8F73	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigLayer4Remark
&Listeners=[{\"InstanceId\":\"ddosDip-sg-4hr2b3l****\",\"FrontendPort\":2020,\"Protocol\":\"udp\",\"Remark\":\"test\"}]
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<ConfigLayer4RemarkResponse>
   <RequestId>6E46CC51-36BE-1100-B14C-DAF8381B8F73</RequestId>
</ConfigLayer4RemarkResponse>
```

`JSON` 格式

```
{
    "RequestId": "6E46CC51-36BE-1100-B14C-DAF8381B8F73"
}
```

错误码

访问错误中心查看更多错误码。

9.11. DescribeLayer4RulePolicy

调用DescribeLayer4RulePolicy查询端口转发规则的回源设置。

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	DescribeLayer4RulePolicy	要执行的操作。取值：**DescribeLayer4RulePolicy**。

名称	类型	是否必选	示例值	描述
Listeners	String	是	[{\"InstanceId\":\"ddosDip-sg-4hr2b3l****\",\"FrontendPort\":2020,\"Protocol\":\"udp\"}]	要查询的端口转发规则。 该参数使用JSON数组转换的字符串表示。JSON数组的每个元素表示一个已创建的端口转发规则。一次最多可以查询1个端口转发规则。 **说明** 您可以调用DescribeNetworkRules查询所有已创建的端口转发规则。 每个端口转发规则包含以下字段： • **InstanceId**：String类型，必选，DDoS高防实例的ID。 • **Protocol**：String类型，必选，端口转发协议类型。取值：**tcp**、**udp**。 • **FrontendPort**：Integer类型，必选，转发端口。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
BackendPort	Integer	2022	源站端口。
BakMode	String	1	回源模式。取值： • 0：表示默认回源模式，即DDoS高防将业务流量转发到您调用CreateNetworkRules创建该端口转发规则时指定的源站IP。 • 1：表示主备回源模式，即DDoS高防将业务流量转发到您调用ConfigLayer4RulePolicy设置的主源站IP地址或备源站IP地址。
CurrentIndex	Integer	1	当前生效的源站类型。取值： • **1**：表示主源站设置生效（DDoS高防将业务流量转发到主源站IP地址）。 • **2**：表示备源站设置生效（DDoS高防将业务流量转发到备源站IP地址）。

名称	类型	示例值	描述
ForwardProtocol	String	udp	转发协议类型。
FrontendPort	Integer	2020	转发端口。
InstanceId	String	ddosDip-sg-4hr2b3l****	DDoS高防实例的ID。
PriRealServers	Array of PriRealServers		主源站信息，包括主源站IP地址、转发协议类型、转发端口等。
CurrentIndex	Integer	1	当前生效的源站类型。取值： • 1：表示主源站设置生效（DDoS高防将业务流量转发到主源站IP地址）。 • 2：表示备源站设置生效（DDoS高防将业务流量转发到备源站IP地址）。
Eip	String	203.107.XX.XX	DDoS高防实例的IP。
FrontendPort	Integer	2020	转发端口。
InstanceId	String	ddosDip-sg-4hr2b3l****	DDoS高防实例的ID。
Protocol	String	udp	转发协议类型。
RealServer	String	192.0.2.1	主源站IP地址。
RequestId	String	6E46CC51-36BE-1100-B14C-DAF8381B8F73	本次请求的ID。
SecRealServers	Array of SecRealServers		备源站信息，包括备源站IP地址、转发协议类型、转发端口等。
CurrentIndex	Integer	1	当前生效的源站类型。取值： • 1：表示主源站设置生效（DDoS高防将业务流量转发到主源站IP地址）。 • 2：表示备源站设置生效（DDoS高防将业务流量转发到备源站IP地址）。
Eip	String	203.107.XX.XX	DDoS高防实例的IP。
FrontendPort	Integer	2020	转发端口。
InstanceId	String	ddosDip-sg-4hr2b3l****	DDoS高防实例的ID。
Protocol	String	udp	转发协议类型。
RealServer	String	192.0.2.3	备源站IP地址。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeLayer4RulePolicy
&Listeners=[{\"InstanceId\":\"ddosDip-sg-4hr2b3l****\",\"FrontendPort\":2020,\"Protocol\":\"udp\"}]
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeLayer4RulePolicyResponse>
   <RequestId>BB95151E-FCAD-1C3C-872F-77166555E396</RequestId>
   <InstanceId>ddosDip-sg-4hr2b3l****</InstanceId>
   <BackendPort>2022</BackendPort>
   <FrontendPort>2020</FrontendPort>
   <CurrentIndex>1</CurrentIndex>
   <bakMode>1</bakMode>
   <ForwardProtocol>udp</ForwardProtocol>
   <PriRealServers>
      <RealServer>192.0.2.1</RealServer>
      <InstanceId>ddosDip-sg-4hr2b3l****</InstanceId>
      <FrontendPort>2020</FrontendPort>
      <CurrentIndex>1</CurrentIndex>
      <Protocol>udp</Protocol>
      <Eip>203.107.XX.XX</Eip>
   </PriRealServers>
   <PriRealServers>
      <RealServer>192.0.2.2</RealServer>
      <InstanceId>ddosDip-sg-4hr2b3l****</InstanceId>
      <FrontendPort>2020</FrontendPort>
      <CurrentIndex>1</CurrentIndex>
      <Protocol>udp</Protocol>
      <Eip>203.107.XX.XX</Eip>
   </PriRealServers>
   <SecRealServers>
      <RealServer>192.0.2.3</RealServer>
      <InstanceId>ddosDip-sg-4hr2b3l****</InstanceId>
      <FrontendPort>2020</FrontendPort>
      <CurrentIndex>1</CurrentIndex>
      <Protocol>udp</Protocol>
      <Eip>203.107.XX.XX</Eip>
   </SecRealServers>
   <SecRealServers>
      <RealServer>192.0.2.4</RealServer>
      <InstanceId>ddosDip-sg-4hr2b3l****</InstanceId>
      <FrontendPort>2020</FrontendPort>
      <CurrentIndex>1</CurrentIndex>
      <Protocol>udp</Protocol>
      <Eip>203.107.XX.XX</Eip>
   </SecRealServers>
</DescribeLayer4RulePolicyResponse>
```

JSON 格式


```
{
    "RequestId": "BB95151E-FCAD-1C3C-872F-77166555E396",
    "InstanceId": "ddosDip-sg-4hr2b3l****",
    "BackendPort": 2022,
    "FrontendPort": 2020,
    "CurrentIndex": 1,
    "bakMode": 1,
    "ForwardProtocol": "udp",
    "PriRealServers": [
        {
            "RealServer": "192.0.2.1",
            "InstanceId": "ddosDip-sg-4hr2b3l****",
            "FrontendPort": 2020,
            "CurrentIndex": 1,
            "Protocol": "udp",
            "Eip": "203.107.XX.XX"
        },
        {
            "RealServer": "192.0.2.2",
            "InstanceId": "ddosDip-sg-4hr2b3l****",
            "FrontendPort": 2020,
            "CurrentIndex": 1,
            "Protocol": "udp",
            "Eip": "203.107.XX.XX"
        }
    ],
    "SecRealServers": [
        {
            "RealServer": "192.0.2.3",
            "InstanceId": "ddosDip-sg-4hr2b3l****",
            "FrontendPort": 2020,
            "CurrentIndex": 1,
            "Protocol": "udp",
            "Eip": "203.107.XX.XX"
        },
        {
            "RealServer": "192.0.2.4",
            "InstanceId": "ddosDip-sg-4hr2b3l****",
            "FrontendPort": 2020,
            "CurrentIndex": 1,
            "Protocol": "udp",
            "Eip": "203.107.XX.XX"
        }
    ]
}
```


错误码

访问错误中心查看更多错误码。

10.流量调度器

10.1. 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 of SchedulerRule		流量调度规则信息。
Cname	String	4eru5229a843****.aliyunddos0001.com	CNAME值。
Param	Struct		全球加速实例联动DDoS高防的规则。
ParamData	Struct		联动资源。

名称	类型	示例值	描述
CloudInstanceId	String	ga-bp1htlajy5509rc99****	全球加速实例的ID。
ParamType	String	GA	联动资源的类型。取值：**GA**，表示全球加速实例。
RuleName	String	doctest	规则名称。
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 of Rule		规则列表。
Priority	Integer	100	规则优先级。
RegionId	String	1	地域ID。 **说明** 仅在阶梯防护规则（RuleType为2）中返回。
RestoreDelay	Integer	60	回切时间，单位为分钟。
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>
       <Param>
          <ParamData>
             <CloudInstanceId>ga-bp1htlajy5509rc99****</CloudInstanceId>
          </ParamData>
          <ParamType>GA</ParamType>
       </Param>
       <RuleType>6</RuleType>
       <Cname>4eru5229a843****.aliyunddos0001.com</Cname>
       <Rules>
          <Status>0</Status>
          <Type>A</Type>
          <RestoreDelay>60</RestoreDelay>
          <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": [
        {
            "Param": {
                "ParamData": {
                    "CloudInstanceId": "ga-bp1htlajy5509rc99****"
                },
                "ParamType": "GA"
            },
            "RuleType": 6,
            "Cname": "4eru5229a843****.aliyunddos0001.com",
            "Rules": [
                {
                    "Status": 0,
                    "Type": "A",
                    "RestoreDelay": 60,
                    "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。

10.2. 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

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。

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
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

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。

10.3. 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	ModifySchedulerRule	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
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

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。

10.4. SwitchSchedulerRule

调用SwitchSchedulerRule将业务流量切换到DDoS高防实例进行清洗、回切到联动资源。

使用说明

本接口用于修改单个流量调度规则的当前生效资源，例如，将业务流量切换到DDoS高防实例进行清洗、回切到联动资源。

调用本接口前，您必须已经调用CreateSchedulerRule创建了流量调度规则。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	SwitchSchedulerRule	要执行的操作。取值：**SwitchSchedulerRule**。
RuleName	String	是	testrule	要操作的流量调度规则的名称。 **说明** 您可以调用DescribeSchedulerRules查询所有流量调度规则的名称。

名称	类型	是否必选	示例值	描述
RuleType	Integer	是	6	流量调度规则的类型。取值： • **2**：表示阶梯防护规则。 • **3**：表示出海加速规则。 • **5**：表示CDN联动规则。 • **6**：表示云产品联动规则。

SwitchData	String	是	[{"Value":"39.104.XX.XX","State":0,"Interval":-1}]	业务流量切换操作的配置。使用JSON数组转化的字符串表示，JSON数组的每个元素是一个结构体，结构体包含以下字段：
				• **Value**：String类型 | 必选 | 联动资源的IP地址。
				• **State**：Integer类型 | 必选 | 操作类型。取值：
				  ◦ **0**：表示将业务流量从联动资源切换到DDoS高防实例进行清洗。
				  ◦ **1**：表示将业务流量回切到联动资源。
				• **Interval**：Integer类型 | 可选 | 回切时间，单位：分钟。使用说明：
				  ◦ **State**为**0**（表示切换到高防时），必须设置该参数为**-1**，否则会调用失败。
				  ◦ **State**为**1**（表示回切到云资源时，无需设置该参数。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	7E3C301F-84BB-50E4-9DB9-2937B2429C1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=SwitchSchedulerRule
&RuleName=testrule
&RuleType=6
&SwitchData=[{"Value":"39.104.XX.XX","State":0,"Interval":-1}]
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<SwitchSchedulerRuleResponse>
    <RequestId>7E3C301F-84BB-50E4-9DB9-2937B2429C1E</RequestId>
</SwitchSchedulerRuleResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "7E3C301F-84BB-50E4-9DB9-2937B2429C1E"
}
```

错误码

访问错误中心查看更多错误码。

10.5. 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。
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。

11.基础设施防护策略

11.1. 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。
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。

11.2. 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**
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。

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
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。
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。

11.3. 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。
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。

11.4. 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。

11.5. 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。
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。

11.6. 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。

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。
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。

11.7. AddAutoCcWhitelist

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

使用说明

本接口用于为单个DDoS高防实例添加白名单IP，使DDoS高防实例直接放行指定IP的请求流量。

白名单IP经添加后，默认永久有效。如果后续不再需要白名单IP，您可以调用EmptyAutoCcWhitelist清空已添加的白名单IP列表。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	AddAutoCcWhitelist	要执行的操作。取值：**AddAutoCcWhitelist**。
RegionId	String	否	cn-hangzhou	DDoS高防服务的地域ID。取值： • **cn-hangzhou**：表示中国内地，即DDoS高防（新BGP）服务。 • **ap-southeast-1**：表示海外地区，即DDoS高防（国际）服务。
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	要添加白名单IP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。
Whitelist	String	是	[{"src":"192.XX.XX.1"},{"src":"192.XX.XX.2"}]	要添加的白名单IP的配置。使用JSON数组转化的字符串表示。JSON数组的每个元素是一个白名单IP结构体，具体包含以下参数： • **src**：String类型 | 必选 | 要添加到白名单的IP地址。
ExpireTime	Integer	否	0	该参数已废弃。 **说明** 该参数表示黑名单IP的有效期。白名单IP默认永久有效，无需设置该参数。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	AB5025DA-5C52-5207-B6AC-3F198758B678	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=AddAutoCcWhitelist
&InstanceId=ddoscoo-cn-mp91j1ao****
&Whitelist=[{"src":"192.XX.XX.1"},{"src":"192.XX.XX.2"}]
&ExpireTime=0
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<AddAutoCcWhitelistResponse>
    <RequestId>AB5025DA-5C52-5207-B6AC-3F198758B678</RequestId>
</AddAutoCcWhitelistResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "AB5025DA-5C52-5207-B6AC-3F198758B678"
}
```

错误码

访问错误中心查看更多错误码。

11.8. 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。

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

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。

11.9. 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**
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。

11.10. 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。

11.11. 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。

名称	类型	示例值	描述
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。

11.12. 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。

11.13. 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**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。
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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
Config	Object		区域封禁的配置信息。
RegionBlockSwitch	String	on	区域封禁的开关状态。取值： • **on**：开启 • **off**：关闭
Provinces	Array of String	11	被封禁的中国地域代码。例如，**11**表示北京市、**12**表示天津市。 **说明** 关于中国地域代码的详细信息，请参见地域类型参数取值说明。
Countries	Array of String	2	被封禁的海外地域代码。例如，**2**表示澳大利亚。 **说明** 关于海外地域代码的详细信息，请参见地域类型参数取值说明。

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

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeNetworkRegionBlockResponse>
    <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
    <Config>
        <RegionBlockSwitch>on</RegionBlockSwitch>
        <Provinces>11</Provinces>
        <Countries>2</Countries>
    </Config>
</DescribeNetworkRegionBlockResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "Config" : {
    "RegionBlockSwitch" : "on",
    "Provinces" : [ "11" ],
    "Countries" : [ "2" ]
  }
}
```

错误码

访问错误中心查看更多错误码。

11.14. ConfigNetworkRegionBlock

调用ConfigNetworkRegionBlock设置针对DDoS高防实例的区域封禁，为某个DDoS高防实例封禁来自指定地域的流量。

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	ConfigNetworkRegionBlock	要执行的操作。取值：**ConfigNetworkRegionBlock**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。
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

Config	String	是	{"RegionBlockSwitch":"on","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，要封禁的国际地域代码列表。
				说明 关于国际地域代码的详细信息，请参见地域类型参数取值说明。
				例如，`[1,2]`表示中国和澳大利亚。
				• **Provinces**：Array类型，可选，要封禁的中国地域代码列表。
				说明 关于中国地域代码的详细信息，请参见地域类型参数取值说明。
				例如，`[11,12]`表示北京市和天津市。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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
&InstanceId=ddoscoo-cn-mp91j1ao****
&Config={"RegionBlockSwitch":"on","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]}
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ConfigNetworkRegionBlockResponse>
    <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</ConfigNetworkRegionBlockResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码
访问错误中心查看更多错误码。

11.15. DescribeBlockStatus
调用DescribeBlockStatus查询DDoS高防（新BGP）实例的近源流量压制配置。

使用说明
本接口用于查询DDoS高防（新BGP）实例的近源流量压制配置。

> **说明** 本接口只适用于DDoS高防（新BGP）服务。

QPS限制
本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeBlockStatus	要执行的操作。取值：**DescribeBlockStatus**。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值固定为**cn-hangzhou**（默认），表示中国内地，即DDoS高防（新BGP）实例。

名称	类型	是否必选	示例值	描述
InstanceIds.N	String	是	ddoscoo-cn-zvp2eibz****	要查询近源流量压制配置的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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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 of StatusItem		DDoS高防实例的近源流量压制配置。
Ip	String	203.XX.XX.88	DDoS高防实例的IP。
BlockStatusList	Array of BlockStatusItem		近源流量压制配置。
EndTime	Long	1540196323	封禁结束时间。使用时间戳表示，单位：秒。
StartTime	Long	1540195323	封禁开始时间。使用时间戳表示，单位：秒。
Line	String	cut	封禁线路类型。取值： • **ct**：表示电信海外线路。 • **cut**：表示联通海外线路。
BlockStatus	String	areablock	流量封禁状态。取值： • **areablock**：表示封禁中。 • **normal**：表示正常（未封禁）。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeBlockStatus
&InstanceIds=["ddoscoo-cn-zvp2eibz****"]
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeBlockStatusResponse>
    <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
    <StatusList>
        <Ip>203.XX.XX.88</Ip>
        <BlockStatusList>
            <EndTime>1540196323</EndTime>
            <StartTime>1540195323</StartTime>
            <Line>cut</Line>
            <BlockStatus>areablock</BlockStatus>
        </BlockStatusList>
    </StatusList>
</DescribeBlockStatusResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "StatusList" : [ {
    "Ip" : "203.XX.XX.88",
    "BlockStatusList" : [ {
      "EndTime" : 1540196323,
      "StartTime" : 1540195323,
      "Line" : "cut",
      "BlockStatus" : "areablock"
    } ]
  } ]
}
```

错误码

访问错误中心查看更多错误码。

11.16. ModifyBlockStatus

调用ModifyBlockStatus为DDoS高防（新BGP）实例开启或关闭近源流量压制。

> **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。
Lines.N	RepeatList	是	ct	要设置的线路。取值： • **ct**：表示海外电信线路。 • **cut**：表示海外联通线路。
Status	String	是	do	设置近源流量压制的状态。取值： • **do**：表示开启近源流量压制。 • **undo**：表示关闭近源流量压制。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值：**cn-hangzhou**，表示中国内地，即DDoS高防（新BGP）服务。
Duration	Integer	否	10	要封禁的时长。取值范围：**15~43200**，单位：分钟。 **说明** Status为do（表示开启近源流量压制）时，该参数必选。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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****
&Lines.1=ct
&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。

11.17. 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。

11.18. ConfigUdpReflect

调用ConfigUdpReflect为DDoS高防实例添加UDP反射攻击防护策略，过滤指定的反射源端口。

使用说明

本接口用于为DDoS高防实例添加UDP反射攻击防护策略，过滤指定的反射源端口。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ConfigUdpReflect	要执行的操作。取值：**ConfigUdpReflect**。
InstanceId	String	是	ddoscoo-cn-i7m25564****	要操作的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。
Config	String	是	{\"UdpSports\":[17,19]}	要添加的UDP反射攻击防护策略的配置。该参数使用JSON结构体转换的字符串表示。JSON结构体包含以下字段： • **UdpSports**：Array类型，必选，要封禁的UDP反射源端口，示例：`[17,19]`。 推荐您封禁以下常见的UDP反射攻击的源端口： ◦ UDP 17：QOTD反射攻击 ◦ UDP 19：CharGEN反射攻击 ◦ UDP 69：TFTP反射攻击 ◦ UDP 111：Portmap反射攻击 ◦ UDP 123：NTP反射攻击 ◦ UDP 137：NetBIOS反射攻击 ◦ UDP 161：SNMPv2反射攻击 ◦ UDP 389：CLDAP反射攻击 ◦ UDP 1194：OpenVPN反射攻击 ◦ UDP 1900：SSDP反射攻击 ◦ UDP 3389：RDP反射攻击 ◦ UDP 11211：Memcached反射攻击
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述

名称	类型	示例值	描述
RequestId	String	9EC62E89-BD30-4FCD-9CB8-FA53865FF0D7	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigUdpReflect
&Config={\"UdpSports\":[17,19]}
&InstanceId=ddoscoo-cn-i7m25564****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<?xml version="1.0" encoding="UTF-8" ?>
<ConfigUdpReflectResponse>
 <RequestId>9EC62E89-BD30-4FCD-9CB8-FA53865FF0D7</RequestId>
</ConfigUdpReflectResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "9EC62E89-BD30-4FCD-9CB8-FA53865FF0D7"
}
```

错误码

访问错误中心查看更多错误码。

11.19. DescribeUdpReflect

调用DescribeUdpReflect查询指定的DDoS高防实例上被UDP反射攻击防护策略过滤的反射源端口。

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

名称	类型	是否必选	示例值	描述
InstanceId	String	是	ddoscoo-cn-i7m25564****	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。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	F97A8766-FB4D-411A-9CD5-2CFF701B592F	本次请求的ID。
UdpSports	List	[17,19,69,111,123,137,161,389,1194,1900,3389,11211,11212]	被UDP反射攻击防护策略过滤的反射源端口列表。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeUdpReflect
&InstanceId=ddoscoo-cn-i7m25564****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeUdpReflectResponse>
   <RequestId>F97A8766-FB4D-411A-9CD5-2CFF701B592F</RequestId>
   <UdpSports>17</UdpSports>
   <UdpSports>19</UdpSports>
   <UdpSports>69</UdpSports>
   <UdpSports>111</UdpSports>
   <UdpSports>123</UdpSports>
   <UdpSports>137</UdpSports>
   <UdpSports>161</UdpSports>
   <UdpSports>389</UdpSports>
   <UdpSports>1194</UdpSports>
   <UdpSports>1900</UdpSports>
   <UdpSports>3389</UdpSports>
   <UdpSports>11211</UdpSports>
   <UdpSports>11212</UdpSports>
</DescribeUdpReflectResponse>
```

`JSON` 格式

```
{
  "RequestId": "F97A8766-FB4D-411A-9CD5-2CFF701B592F",
  "UdpSports": [
    17,
    19,
    69,
    111,
    123,
    137,
    161,
    389,
    1194,
    1900,
    3389,
    11211,
    11212
  ]
}
```

错误码

访问错误中心查看更多错误码。

12.网站业务防护策略

12.1. 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**
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

名称	类型	示例值	描述
AiTemplate	String	level60	AI智能防护的等级。取值： • **level30**：宽松 • **level60**：正常 • **level90**：严格
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。

12.2. 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。

12.3. 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**

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。

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=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。

12.4. 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**

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。

12.5. 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
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。

12.6. 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**

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=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。

12.7. 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**
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。

12.8. 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
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。

12.9. 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**

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=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。

12.10. 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。

12.11. 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**
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
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。

12.12. 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**。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。 关于资源组的更多信息，请参见创建资源组。
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	testrule	规则名称。支持使用英文字母、数字或下划线（_），且长度不能超过128个字符。
Act	String	是	close	对命中防护规则的请求执行的动作。取值： • **close**：表示封禁该请求。 • **captcha**：表示发起人机识别验证。
Count	Integer	是	60	单一IP访问次数。取值范围：**2~2000**。
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**：表示前缀匹配。 • **match**：表示完全匹配。 **说明** 检测路径URI中包含参数时，请选择前缀匹配（prefix）。
Ttl	Integer	是	60	封禁时长。取值范围：**60~86400**，单位：秒。
Uri	String	是	/abc/a.php	检测路径。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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=60
&Uri=/abc/a.php
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<?xml version="1.0" encoding="UTF-8" ?>
<CreateWebCCRuleResponse>
 <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</CreateWebCCRuleResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

错误码

访问错误中心查看更多错误码。

12.13. 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**
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。

12.14. 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。

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=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。

12.15. 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

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。

12.16. 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。

12.17. 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。

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。

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。
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
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

匹配字段（field）	描述	适用的逻辑符（match_method）
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
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
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

匹配字段（field）	描述	适用的逻辑符（match_method）
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":"conta
in","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。

12.18. 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。
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。

12.19. ModifyWebAreaBlockSwitch
调用ModifyWebAreaBlockSwitch设置网站业务区域封禁（针对域名）的开关状态。

使用说明
本接口用于设置网站业务区域封禁（针对域名）的开关状态。

QPS限制
本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyWebAreaBlockSwitch	要执行的操作。取值：**ModifyWebAreaBlockSwitch**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。
Domain	String	是	www.aliyundoc.com	要设置区域封禁功能的域名。 **说明** 您可以调用DescribeDomains查询所有已接入DDoS高防防护的域名。

名称	类型	是否必选	示例值	描述
Config	String	是	{"RegionblockEnable": 1}	区域封禁（针对域名）的开关状态。使用JSON结构体转化的字符串表示，JSON结构体包含以下参数： • **RegionblockEnable**：Integer类型，必选，区域封禁（针对域名）的开关状态。取值： ○ **1**：表示开启。 ○ **0**：表示关闭。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyWebAreaBlockSwitch
&Domain=www.aliyundoc.com
&Config={"RegionblockEnable": 1}
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyWebAreaBlockSwitchResponse>
    <RequestId>6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1</RequestId>
</ModifyWebAreaBlockSwitchResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1"
}
```

错误码

访问错误中心查看更多错误码。

12.20. 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**
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。

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=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。

12.21. ModifyWebAreaBlock

调用ModifyWebAreaBlock设置网站业务区域封禁（针对域名）功能，为某个域名封禁来自指定地域的流量。

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

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。 关于资源组的更多信息，请参见创建资源组。
Domain	String	是	www.aliyun.com	要操作的域名。 **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。
Regions.N	String	否	CN-310000	要封禁的地域列表。支持封禁中国地域（省市区维度）和国际地域（国家维度），例如，**CN-310000**表示上海市、**OVERSEAS-US**表示美国。不设置该参数表示关闭区域封禁（针对域名）功能。 **说明** 关于该参数的取值说明，请参见地域类型参数取值说明。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	5AA2BD65-E289-4E91-9DD9-3E1FB2140D17	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyWebAreaBlock
&Domain=www.aliyun.com
&Regions=["CN-310000"]
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyWebAreaBlockResponse>
    <RequestId>5AA2BD65-E289-4E91-9DD9-3E1FB2140D17</RequestId>
</ModifyWebAreaBlockResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "5AA2BD65-E289-4E91-9DD9-3E1FB2140D17"
}
```

错误码

访问错误中心查看更多错误码。

13.非网站业务防护策略

13.1. 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

名称	类型	示例值	描述
WebMode	String	normal	80和443端口的防护模式。取值： • **normal**：正常 • **loose**：宽松 • **strict**：严格
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。

13.2. 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。

13.3. 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。

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
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。
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。

名称	类型	示例值	描述
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**。
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。

13.4. 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。

14.定制场景策略

14.1. DescribeSceneDefensePolicies

调用DescribeSceneDefensePolicies查询定制场景策略的详细配置。

使用说明

本接口用于查询已创建的定制场景策略的详细配置，例如，策略的状态、防护对象、防护规则等。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeSceneDefensePolicies	要执行的操作。取值：**DescribeSceneDefensePolicies**。
Template	String	否	promotion	要查询的策略使用的模板类型。取值： • **promotion**：表示重大活动模板。 • **bypass**：表示全量转发模板。
Status	String	否	1	要查询的策略的生效状态。取值： • **0**：表示已被禁用。 • **1**：表示等待生效。 • **2**：表示生效中。 • **3**：表示已过期。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
Success	Boolean	true	本次请求是否成功调用成功。取值： • **true**：表示调用成功。 • **false**：表示调用失败。
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	本次请求的ID。
Policies	Array of Policy		定制场景策略的详细配置。
Done	Integer	1	策略执行状态。取值： • **1**：表示未执行或执行完成。 • **0**：表示执行中。 • **-1**：表示执行失败。
EndTime	Long	1586016000000	策略结束生效的时间。使用时间戳表示，单位：毫秒。
Status	Integer	1	策略的生效状态。取值： • **0**：表示已被禁用。 • **1**：表示等待生效。 • **2**：表示生效中。 • **3**：表示已过期。
StartTime	Long	1585670400000	策略开始生效的时间。使用时间戳表示，单位：毫秒。
ObjectCount	Integer	1	策略的防护对象数量。
Template	String	promotion	策略使用的模板类型。取值： • **promotion**：表示重大活动模板。 • **bypass**：表示全量转发模板。
PolicyId	String	321a-fd31-df51-****	策略ID。
Name	String	testpolicy	策略名称。
RuntimePolicies	Array of Policy		策略运行规则。

名称	类型	示例值	描述
Status	Integer	3	策略运行状态。取值： • 0：表示未下发或策略恢复成功。 • 1：表示正在生效中（策略生效）。 • 2：表示正在恢复中（策略恢复）。 • 3：表示策略生效成功 。 • 4：表示策略生效失败。 • 5：表示策略恢复失败。 • 6：表示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。
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：表示频率控制功能变更。 • 2：表示AI智能防护功能变更。

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

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeSceneDefensePoliciesResponse>
    <Success>true</Success>
    <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
    <Policies>
        <Done>1</Done>
        <EndTime>1586016000000</EndTime>
        <Status>1</Status>
        <StartTime>1585670400000</StartTime>
        <ObjectCount>1</ObjectCount>
        <Template>promotion</Template>
        <PolicyId>321a-fd31-df51-****</PolicyId>
        <Name>testpolicy</Name>
        <RuntimePolicies>
            <Status>3</Status>
            <oldValue>{"cc_rule_enable": true}</oldValue>
            <NewValue>{"cc_rule_enable": false }</NewValue>
            <PolicyType>1</PolicyType>
        </RuntimePolicies>
    </Policies>
</DescribeSceneDefensePoliciesResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "Success" : true,
  "RequestId" : "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
  "Policies" : [ {
    "Done" : 1,
    "EndTime" : 1586016000000,
    "Status" : 1,
    "StartTime" : 1585670400000,
    "ObjectCount" : 1,
    "Template" : "promotion",
    "PolicyId" : "321a-fd31-df51-****",
    "Name" : "testpolicy",
    "RuntimePolicies" : [ {
      "Status" : 3,
      "oldValue" : "{\"cc_rule_enable\": true}",
      "NewValue" : "{\"cc_rule_enable\": false }",
      "PolicyType" : 1
    } ]
  } ]
}
```

错误码

访问错误中心查看更多错误码。

14.2. CreateSceneDefensePolicy

调用CreateSceneDefensePolicy创建一条定制场景策略。

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**。
Name	String	是	testpolicy	策略名称。
Template	String	是	promotion	策略模板类型。取值固定为**promotion**，表示重大活动。
StartTime	Long	是	1585670400000	该策略开始生效的时间。使用时间戳格式，单位：毫秒。
EndTime	Long	是	1586016000000	该策略结束生效的时间。使用时间戳格式，单位：毫秒。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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	是否成功创建策略。取值： • **true**：表示是。 • **false**：表示否。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateSceneDefensePolicy
&Name=testpolicy
&Template=promotion
&StartTime=1585670400000
&EndTime=1586016000000
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<CreateSceneDefensePolicyResponse>
    <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
    <Success>true</Success>
</CreateSceneDefensePolicyResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
  "Success" : true
}
```

错误码

访问错误中心查看更多错误码。

14.3. ModifySceneDefensePolicy

调用ModifySceneDefensePolicy修改已创建的定制场景策略。

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**。
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。

名称	类型	是否必选	示例值	描述
Name	String	是	testpolicy	策略名称。
Template	String	是	promotion	策略模板类型。取值固定为**promotion**，表示重大活动。
StartTime	Long	是	1585670400000	该策略开始生效的时间。使用时间戳格式，单位：毫秒。
EndTime	Long	是	1586016000000	该策略结束生效的时间。使用时间戳格式，单位：毫秒。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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	是否调用成功。取值： • **true**：表示是。 • **false**：表示否。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifySceneDefensePolicy
&PolicyId=321a-fd31-df51-****
&Name=testpolicy
&Template=promotion
&StartTime=1585670400000
&EndTime=1586016000000
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifySceneDefensePolicyResponse>
    <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
    <Success>true</Success>
</ModifySceneDefensePolicyResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
  "Success" : true
}
```

错误码

访问错误中心查看更多错误码。

14.4. 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。

14.5. DescribeSceneDefenseObjects

调用DescribeSceneDefenseObjects查询定制场景策略的防护对象。

使用说明

本接口用于查询定制场景策略的防护对象。

调用本接口前，您必须已经调用CreateSceneDefensePolicy创建了定制场景策略。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeSceneDefenseObjects	要执行的操作。取值：**DescribeSceneDefenseObjects**。
PolicyId	String	是	47e07ebd-0ba5-4afc-957b-59d15b90****	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高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
Success	Boolean	true	本次请求是否成功调用。取值： • **true**：表示调用成功。 • **false**：表示调用失败。
RequestId	String	FE07E73F-F19E-4A51-B62F-AC59E3B962D8	本次请求的ID。
Objects	Array of Object		定制场景策略的防护对象信息。
Domain	String	www.aliyundoc.com	策略防护的域名。
PolicyId	String	47e07ebd-0ba5-4afc-957b-59d15b90****	定制场景策略的ID。
Vip	String	203.XX.XX.119	策略防护的高防实例IP。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeSceneDefenseObjects
&PolicyId=47e07ebd-0ba5-4afc-957b-59d15b90****
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeSceneDefenseObjectsResponse>
    <Success>true</Success>
    <RequestId>FE07E73F-F19E-4A51-B62F-AC59E3B962D8</RequestId>
    <Objects>
        <Domain>www.aliyundoc.com</Domain>
        <PolicyId>47e07ebd-0ba5-4afc-957b-59d15b90****</PolicyId>
    </Objects>
</DescribeSceneDefenseObjectsResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "Success" : true,
  "RequestId" : "FE07E73F-F19E-4A51-B62F-AC59E3B962D8",
  "Objects" : [ {
    "Domain" : "www.aliyundoc.com",
    "PolicyId" : "47e07ebd-0ba5-4afc-957b-59d15b90****"
  } ]
}
```

错误码

访问错误中心查看更多错误码。

14.6. 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**

名称	类型	是否必选	示例值	描述
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。

14.7. DetachSceneDefenseObject

调用DetachSceneDefenseObject移除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	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。

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=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。

14.8. 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**

名称	类型	是否必选	示例值	描述
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。
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。

14.9. 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。

15.静态页面缓存

15.1. ModifyWebCacheSwitch

调用ModifyWebCacheSwitch设置网站业务静态页面缓存的开关状态。

使用说明

本接口用于设置网站业务静态页面缓存的开关状态。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyWebCacheSwitch	要执行的操作。取值：**ModifyWebCacheSwitch**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。
Domain	String	是	www.aliyundoc.com	要设置静态页面缓存的域名。 **说明** 您可以调用DescribeDomains查询所有已接入DDoS高防防护的域名。
Enable	Integer	是	1	设置静态页面缓存的开关状态。取值： • **1**：表示开启。 • **0**：表示关闭。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1	本次请求的ID。

示例

请求示例

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

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyWebCacheSwitchResponse>
    <RequestId>6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1</RequestId>
</ModifyWebCacheSwitchResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1"
}
```

错误码

访问错误中心查看更多错误码。

15.2. 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**

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。
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。

15.3. 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**
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

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=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。

15.4. DeleteWebCacheCustomRule

调用DeleteWebCacheCustomRule删除网站业务静态页面缓存的自定义规则。

使用说明

本接口用于批量删除网站业务静态页面缓存的自定义规则。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteWebCacheCustomRule	要执行的操作。取值：**DeleteWebCacheCustomRule**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。
Domain	String	是	www.aliyundoc.com	要删除静态页面缓存自定义规则的域名。 **说明** 您可以调用DescribeDomains查询所有已接入DDoS高防防护的域名。
RuleNames.N	String	是	doc-test-rule	要删除的规则的名称。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteWebCacheCustomRule
&Domain=www.aliyundoc.com
&RuleNames=["doc-test-rule"]
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DeleteWebCacheCustomRuleResponse>
    <RequestId>6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1</RequestId>
</DeleteWebCacheCustomRuleResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1"
}
```

错误码

访问错误中心查看更多错误码。

15.5. DescribeWebCacheConfigs

调用DescribeWebCacheConfigs查询网站业务静态页面缓存的配置。

使用说明

本接口用于查询网站业务静态页面缓存的配置，例如，缓存模式、自定义缓存规则等。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeWebCacheConfigs	要执行的操作。取值：**DescribeWebCacheConfigs**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。

名称	类型	是否必选	示例值	描述
Domains.N	String	是	www.aliyundoc.com	要查询静态页面缓配置的域名。 **说明** 您可以调用DescribeDomains查询所有已接入DDoS高防防护的域名。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1	本次请求的ID。
DomainCacheConfigs	Array of CacheConfig		静态页面缓存的配置信息。
Domain	String	www.aliyundoc.com	网站域名。
Mode	String	bypass	缓存模式。取值： • **standard**：表示标准模式。 • **aggressive**：表示强力模式。 • **bypass**：表示不缓存。
Enable	Integer	1	开关状态。取值： • **1**：表示开启。 • **0**：表示关闭。
CustomRules	Array of CustomRule		自定义缓存规则配置。
Mode	String	standard	缓存模式。取值： • **standard**：表示标准模式。 • **aggressive**：表示强力模式。 • **bypass**：表示不缓存。
CacheTtl	Long	86400	页面缓存的过期时间。单位：秒。
Name	String	c1	规则名称。
Uri	String	/blog/	缓存页面的路径。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeWebCacheConfigs
&Domains=["www.aliyundoc.com"]
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeWebCacheConfigsResponse>
    <RequestId>6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1</RequestId>
    <DomainCacheConfigs>
        <Domain>www.aliyundoc.com</Domain>
        <Mode>bypass</Mode>
        <Enable>1</Enable>
        <CustomRules>
            <Mode>standard</Mode>
            <CacheTtl>86400</CacheTtl>
            <Name>c1</Name>
            <Uri>/blog/</Uri>
        </CustomRules>
    </DomainCacheConfigs>
</DescribeWebCacheConfigsResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1",
  "DomainCacheConfigs" : [ {
    "Domain" : "www.aliyundoc.com",
    "Mode" : "bypass",
    "Enable" : 1,
    "CustomRules" : [ {
      "Mode" : "standard",
      "CacheTtl" : 86400,
      "Name" : "c1",
      "Uri" : "/blog/"
    } ]
  } ]
}
```

错误码

访问错误中心查看更多错误码。

16.攻击分析

16.1. DescribeAttackAnalysisMaxQps

调用DescribeAttackAnalysisMaxQps查询指定时间段内DDoS攻击的峰值（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	DescribeAttackAnalysisMaxQps	要执行的操作。取值：**DescribeAttackAnalysisMaxQps**。
EndTime	Long	是	1619798400	查询结束时间。使用时间戳格式，单位：秒。
StartTime	Long	是	1622476799	查询开始时间。使用时间戳格式，单位：秒。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
Qps	Long	41652	DDoS攻击的峰值，单位：qps。
RequestId	String	8DFB602D-1AAC-46C4-90F2-C84086E7A6E4	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeAttackAnalysisMaxQps
&EndTime=1619798400
&StartTime=1622476799
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeAttackAnalysisMaxQpsResponse>
   <RequestId>8DFB602D-1AAC-46C4-90F2-C84086E7A6E4</RequestId>
   <Qps>41652</Qps>
</DescribeAttackAnalysisMaxQpsResponse>
```

`JSON` 格式

```
{
 "RequestId": "8DFB602D-1AAC-46C4-90F2-C84086E7A6E4",
 "Qps": "41652"
}
```

错误码

访问错误中心查看更多错误码。

16.2. DescribeDDosEventMax

调用DescribeDDosEventMax查询指定时间范围内的流量型攻击峰值（bps）、连接型攻击峰值（cps）、Web资源耗尽型攻击峰值（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	DescribeDDosEventMax	要执行的操作。取值：**DescribeDDosEventMax**。
EndTime	Long	是	1604073600	查询结束时间戳，单位：秒。
StartTime	Long	是	1598889600	查询开始时间戳，单位：秒。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
Cps	Long	1302	连接型攻击峰值，单位：cps。
Mbps	Long	6809	流量型攻击峰值，单位：Mbps。
Qps	Long	26314	Web资源耗尽型攻击峰值，单位：qps。
RequestId	String	5AE2FC86-C840-41AE-9F1A-3A2747C7C1DF	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDDosEventMax
&EndTime=1604073600
&StartTime=1598889600
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDDosEventMaxResponse>
   <RequestId>5AE2FC86-C840-41AE-9F1A-3A2747C7C1DF</RequestId>
   <Qps>26314</Qps>
   <Cps>1302</Cps>
   <Mbps>6809</Mbps>
 </DescribeDDosEventMaxResponse>
```

`JSON` 格式

```
{
 "RequestId": "5AE2FC86-C840-41AE-9F1A-3A2747C7C1DF",
 "Qps": 26314,
 "Cps": 1302,
 "Mbps": 6809
}
```

错误码

访问错误中心查看更多错误码。

16.3. DescribeDDosAllEventList

调用DescribeDDosAllEventList查询DDoS攻击事件列表。

使用说明

本接口用于分页查询指定时间范围内的DDoS攻击事件列表。DDoS攻击事件包含以下信息：攻击的起止时间、攻击类型、受攻击的对象、攻击流量的峰值（带宽峰值或包转发率峰值）等。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDDosAllEventList	要执行的操作。取值：**DescribeDDosAllEventList**。

名称	类型	是否必选	示例值	描述
EventType	String	否	defense	要查询的DDoS攻击事件的类型。取值： • **web-cc**：表示Web资源耗尽型攻击。 • **cc**：表示连接型攻击。 • **defense**：表示流量型攻击（清洗事件）。 • **blackhole**：表示流量型攻击（黑洞事件）。 支持同时设置多个类型，多个类型间使用半角逗号（,）分隔。 不设置该参数表示查询所有类型的攻击事件。
StartTime	Long	是	1609430400	设置开始时间，查询在**StartTime**后发生的DDoS攻击事件。使用时间戳表示，单位：秒。
EndTime	Long	是	1640966399	设置结束时间，查询在**EndTime**前发生的DDoS攻击事件。使用时间戳表示，单位：秒。
PageNumber	Integer	是	1	分页查询时，设置当前页面的页码。
PageSize	Integer	是	10	分页查询时，设置每页包含攻击事件的数量。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
Total	Long	1	查询到的攻击事件的总数量。
RequestId	String	25D83ED5-28CB-5683-9CF7-AECE521F3005	本次请求的ID。
AttackEvents	Array of AttackEvent		攻击事件列表。
EndTime	Long	1634546030	攻击结束时间。使用时间戳表示，单位：秒。
StartTime	Long	1634543764	攻击开始时间。使用时间戳表示，单位：秒。

名称	类型	示例值	描述
EventType	String	cc	DDoS攻击事件的类型。取值： • **web-cc**：表示Web资源耗尽型攻击。 • **cc**：表示连接型攻击。 • **defense**：表示流量型攻击（清洗事件）。 • **blackhole**：表示流量型攻击（黑洞事件）。
Mbps	Long	101899	攻击流量的带宽峰值。单位：Mbps。
Ip	String	203.107.XX.XX	被攻击的对象。不同攻击事件类型对应的被攻击对象不同，具体说明如下： • Web资源耗尽型攻击（**EventType**为**web-cc**）：该参数表示被攻击的网站域名。 • 连接型攻击（**EventType**为**cc**）：该参数表示被攻击的高防IP。 • 流量型攻击（**EventType**为**defense**或**blackhole**）：该参数表示被攻击的高防IP。
Area	String	cn	攻击来源地域。取值： • **cn**：表示中国内地。 • **alb-cn-hongkong-gf-2**：表示中国香港。 • **alb-us-west-1-gf-2**：表示美国（硅谷）。 • **alb-ap-northeast-1-gf-1**：表示日本（东京）。 • **alb-ap-southeast-gf-1**：表示新加坡。 • **alb-eu-central-1-gf-1**：表示德国（法兰克福）。 • **alb-eu-west-1-gf-1**、**selb-eu-west-1-gf-1a**：表示英国（伦敦）。 • **alb-us-east-gf-1**：表示美国（弗吉尼亚）。 • **CT-yundi**：表示中国香港。该取值只适用于DDoS高防（国际）安全加速线路实例。
Port	String	80	被攻击的端口号。 **说明** Web资源耗尽型攻击（**EventType**为**web-cc**）不返回该参数。
Pps	Long	9664270	攻击流量的包转发率峰值。单位：pps。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDDosAllEventList
&StartTime=1609430400
&EndTime=1640966399
&PageNumber=1
&PageSize=10
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeDDosAllEventListResponse>
    <Total>1</Total>
    <RequestId>25D83ED5-28CB-5683-9CF7-AECE521F3005</RequestId>
    <AttackEvents>
        <EndTime>1634546030</EndTime>
        <StartTime>1634543764</StartTime>
        <EventType>cc</EventType>
        <Mbps>101899</Mbps>
        <Ip>203.107.XX.XX</Ip>
        <Area>cn</Area>
        <Port>80</Port>
        <Pps>9664270</Pps>
    </AttackEvents>
</DescribeDDosAllEventListResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "Total" : 1,
  "RequestId" : "25D83ED5-28CB-5683-9CF7-AECE521F3005",
  "AttackEvents" : [ {
    "EndTime" : 1634546030,
    "StartTime" : 1634543764,
    "EventType" : "cc",
    "Mbps" : 101899,
    "Ip" : "203.107.XX.XX",
    "Area" : "cn",
    "Port" : "80",
    "Pps" : 9664270
  } ]
}
```

错误码

访问错误中心查看更多错误码。

16.4. DescribeDDosEventArea

调用DescribeDDosEventArea查询某次流量型攻击的来源地域详情。

> **说明** 目前该接口仅适用于查询流量型攻击的数据，不适用于查询Web资源消耗型和连接型攻击的数据。

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	DescribeDDosEventArea	要执行的操作。取值：**DescribeDDosEventArea**。
EventType	String	是	defense	要查询的攻击事件类型。取值： • **defense**：表示流量型攻击清洗事件。 • **blackhole**：表示流量型攻击黑洞事件。
StartTime	Long	是	1598948471	要查询事件的开始时间戳，单位：秒。 **说明** 您可以调用DescribeDDosAllEventList查询所有事件的开始时间信息。
Ip	String	是	203.XX.XX.199	受攻击的DDoS高防IP。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	11710C9F-BC5E-481A-BEC5-C6D8FBFCA827	本次请求的ID。
Areas	Array of EventArea		攻击来源地域信息。
InPkts	Long	228	攻击来源地域的请求包数量。

名称	类型	示例值	描述
Area	String	110000	攻击来源地域的代码，包含中国地域（省市区维度）和国际地域（国际维度）。例如，**110000**表示中国北京市、**us**表示美国。 **说明** 关于该参数的取值说明，请参见地域类型参数取值说明。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDDosEventArea
&EventType=defense
&StartTime=1598948471
&Ip=203.XX.XX.199
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeDDosEventAreaResponse>
    <RequestId>11710C9F-BC5E-481A-BEC5-C6D8FBFCA827</RequestId>
    <Areas>
        <InPkts>228</InPkts>
        <Area>110000</Area>
    </Areas>
</DescribeDDosEventAreaResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "11710C9F-BC5E-481A-BEC5-C6D8FBFCA827",
  "Areas" : [ {
    "InPkts" : 228,
    "Area" : "110000"
  } ]
}
```

错误码

访问错误中心查看更多错误码。

16.5. DescribeDDosEventAttackType

调用DescribeDDosEventAttackType查询某次流量型攻击的攻击类型详情。

> **说明** 目前该接口仅适用于查询流量型攻击的数据，不适用于查询Web资源消耗型和连接型攻击的数据。

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	DescribeDDosEventAttackType	要执行的操作。取值：**DescribeDDosEventAttackType**。
EventType	String	是	defense	要查询的攻击事件的类型。取值： • **defense**：表示流量型攻击清洗事件。 • **blackhole**：表示流量型攻击黑洞事件。
Ip	String	是	203.***.***.199	受攻击的高防IP。
StartTime	Long	是	1598948471	要查询事件的开始时间戳，单位：秒。 **说明** 您可以调用DescribeDDosAllEventList查询所有事件的开始时间信息。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
AttackTypes	Array of EventAttackType		攻击类型信息。
			攻击类型。取值： • **QOTD-Reflect-Flood**：QOTD反射攻击 • **CharGEN-Reflect-Flood**：CharGEN反射攻击 • **DNS-Reflect-Flood**：DNS反射攻击 • **TFTP-Reflect-Flood**：TFTP反射攻击 • **Portmap-Reflect-Flood**：Portmap反射攻击 • **NTP-Reflect-Flood**：NTP反射攻击

名称	类型	示例值	描述
AttackType	String	Tcp-Syn	• **NetBIOS-Reflect-Flood**：NetBIOS反射攻击 • **SNMPv2-Reflect-Flood**：SNMPv2反射攻击 • **CLDAP-Reflect-Flood**：CLDAP反射攻击 • **Ripv1-Reflect-Flood**：Ripv1反射攻击 • **OpenVPN-Reflect-Flood**：OpenVPN反射攻击 • **SSDP-Reflect-Flood**：SSDP反射攻击 • **NetAssistant-Reflect-Flood**：NetAssistant反射攻击 • **WSDiscovery-Reflect-Flood**：WSDiscovery反射攻击 • **Kad-Reflect-Flood**：Kad反射攻击 • **mDNS-Reflect-Flood**：mDNS反射攻击 • **10001-Reflect-Flood**：10001反射攻击 • **Memcached-Reflect-Flood**：Memcached反射攻击 • **QNP-Reflect-Flood**：QNP反射攻击 • **DVR-Reflect-Flood**：DVR反射攻击 • **CoAP-Reflect-Flood**：CoAP反射攻击 • **ADDP-Reflect-Flood**：ADDP反射攻击 • **Tcp-Syn**：TCP SYN Flood攻击 • **Tcp-Fin**：TCP FIN Flood攻击 • **Tcp-Ack**：TCP ACK Flood攻击 • **Tcp-Rst**：TCP RST Flood攻击 • **Tcp-Pushack**：TCP PSH+ACK Flood攻击 • **Tcp-Synack**：TCP SYN+ACK Flood攻击 • **Udp-None**：UDP攻击 • **Udp-Ssh**：UDP SSH协议攻击 • **Udp-Dns**：UDP DNS协议攻击 • **Udp-Http**：UDP HTTP协议攻击 • **Udp-Https**：UDP HTTPS协议攻击 • **Udp-Ntp**：UDP NTP协议攻击 • **Udp-Ldap**：UDP LDAP协议攻击 • **Udp-Ssdp**：UDP SSDP协议攻击 • **Udp-Memcached**：Memcache UDP反射放大攻击 • **Tcp-Other**：TCP其他类型攻击 • **Icmp**：ICMP Flood攻击 • **Igmp**：IGMP Flood攻击 • **Ipv6**：IPv6攻击
InPkts	Long	145902	该攻击类型的请求包数量。

名称	类型	示例值	描述
RequestId	String	6F644A6E-40E7-483F-9DBB-CC27E16BB555	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDDosEventAttackType
&EventType=defense
&Ip=203.***.***.199
&StartTime=1598948471
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDDosEventAttackTypeResponse>
   <RequestId>6F644A6E-40E7-483F-9DBB-CC27E16BB555</RequestId>
   <AttackTypes>
      <AttackType>Tcp-Syn</AttackType>
      <InPkts>145902</InPkts>
   </AttackTypes>
   <AttackTypes>
      <AttackType>Tcp-Other</AttackType>
      <InPkts>3</InPkts>
   </AttackTypes>
  </DescribeDDosEventAttackTypeResponse>
```

`JSON` 格式

```
{
 "RequestId": "6F644A6E-40E7-483F-9DBB-CC27E16BB555",
 "AttackTypes": [
  {
   "AttackType": "Tcp-Syn",
   "InPkts": 145902
  },
  {
   "AttackType": "Tcp-Other",
   "InPkts": 3
  }
 ]
}
```

错误码

访问错误中心查看更多错误码。

16.6. DescribeDDosEventIsp

调用DescribeDDosEventIsp查询某次流量型攻击的攻击来源网络运营商（ISP）信息。

> **说明** 目前该接口仅适用于查询流量型攻击的数据，不适用于查询Web资源消耗型和连接型攻击的数据。

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	DescribeDDosEventIsp	要执行的操作。取值：**DescribeDDosEventIsp**。
EventType	String	是	defense	要查询的攻击事件类型。取值： • **defense**：流量型攻击清洗事件。 • **blackhole**：流量型攻击黑洞事件。
Ip	String	是	203.***.***.199	受攻击的高防IP。
StartTime	Long	是	1598948471	要查询事件的开始时间戳，单位：秒。 > **说明** 您可以调用DescribeDDosAllEventList查询所有事件的开始时间信息。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
Isps	Array of EventIsp		攻击来源网络运营商信息。
InPkts	Long	230	来自该网络运营商的请求包数量。

名称	类型	示例值	描述
Isp	String	1000323	攻击来源网络运营商的代码。取值： • 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 • 1000401：腾讯 • 100099：百度 • 1000323：阿里云 • 100098：阿里巴巴
RequestId	String	C4A3BCD1-4A32-4342-941A-4745AE69508C	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDDosEventIsp
&EventType=defense
&Ip=203.***.***.199
&StartTime=1598948471
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDDosEventIspResponse>
   <RequestId>C4A3BCD1-4A32-4342-941A-4745AE69508C</RequestId>
   <Isps>
      <InPkts>230</InPkts>
      <Isp>1000323</Isp>
   </Isps>
   <Isps>
      <InPkts>24</InPkts>
      <Isp>100098</Isp>
   </Isps>
  </DescribeDDosEventIspResponse>
```

`JSON` 格式

```
{
    "RequestId": "C4A3BCD1-4A32-4342-941A-4745AE69508C",
    "Isps": [
        {
            "InPkts": 230,
            "Isp": "1000323"
        },
        {
            "InPkts": 24,
            "Isp": "100098"
        }
    ]
}
```

错误码

访问错误中心查看更多错误码。

16.7. DescribeDDosEventSrcIp

调用DescribeDDosEventSrcIp查询某次流量型攻击的攻击来源IP详情。

> **说明** 目前该接口仅适用于查询流量型攻击的数据，不适用于查询Web资源消耗型和连接型攻击的数据。

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

名称	类型	是否必选	示例值	描述
EventType	String	是	defense	要查询的攻击事件的类型。取值： • **defense**：表示流量型攻击清洗事件。 • **blackhole**：表示流量型攻击黑洞事件。
StartTime	Long	是	1598948471	要查询事件的开始时间戳，单位：秒。 **说明** 您可以调用DescribeDDosAllEventList查询所有事件的开始时间信息。
Ip	String	是	203.XX.XX.199	受攻击的DDoS高防IP。
Range	Long	是	2	要返回的攻击来源IP的个数。按照攻击流量由大到小排序，默认返回前5个IP。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	38A0224E-FDBC-4733-A362-B391827FC1E9	本次请求的ID。
Ips	Array of EventSrcIp		攻击来源IP信息。
SrcIp	String	218.XX.XX.24	攻击来源IP。
AreaId	String	110000	攻击来源地域的代码，包含中国地域（省市区维度）和国际地域（国家维度）。例如，**110000**表示中国北京市、**us**表示美国。 **说明** 关于该参数的取值说明，请参见地域类型参数取值说明。

名称	类型	示例值	描述
Isp	String	100026	攻击来源网络运营商。取值： • 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 • 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=DescribeDDosEventSrcIp
&EventType=defense
&StartTime=1598948471
&Ip=203.XX.XX.199
&Range=2
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeDDosEventSrcIpResponse>
    <RequestId>38A0224E-FDBC-4733-A362-B391827FC1E9</RequestId>
    <Ips>
        <SrcIp>218.XX.XX.24</SrcIp>
        <AreaId>110000</AreaId>
        <Isp>100026</Isp>
    </Ips>
</DescribeDDosEventSrcIpResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "38A0224E-FDBC-4733-A362-B391827FC1E9",
  "Ips" : [ {
    "SrcIp" : "218.XX.XX.24",
    "AreaId" : "110000",
    "Isp" : "100026"
  } ]
}
```

错误码

访问错误中心查看更多错误码。

17.监控报表

17.1. 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。
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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
DDoSEvents	Array of Data		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	被攻击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。

17.2. 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**。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。关于资源组的更多信息，请参见创建资源组。
EndTime	Long	是	1583683200	设置查询结束时间。使用时间戳格式，单位：秒。 **说明** 必须设置成整点分钟。
StartTime	Long	是	1582992000	设置查询开始时间。使用时间戳格式，单位：秒。 **说明** 必须设置成整点分钟。
Interval	Integer	是	1000	设置返回数据的步长，单位为秒，即每隔多少秒返回一个结果。查询时间范围（由StartTime和EndTime决定）不同，支持的步长取值范围不同，设置建议如下： • 查询时间范围不大于1小时，建议最小步长为60秒，最大不超过查询时间范围。 • 查询时间范围大于1小时但不超过6小时，建议最小步长为600秒，最大不超过查询时间范围。 • 查询时间范围大于6小时但不超过24小时，建议最小步长为1800秒，最大不超过查询时间范围。 • 查询时间范围大于24小时但不超过7天，建议最小步长为3600秒，最大不超过查询时间范围。 • 查询时间范围大于7天但不超过15天，建议最小步长为14400秒，最大不超过查询时间范围。 • 查询时间范围大于15天，建议最小步长为43200秒，最大不超过查询时间范围。

名称	类型	是否必选	示例值	描述
InstanceIds.N	String	是	ddoscoo-cn-zz120cjv****	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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	FFC77501-BDF8-4BC8-9BF5-B295FBC3189B	本次请求的ID。
PortFlowList	Array of PortFlow		查询到的流量数据。
Index	Long	0	返回数据的索引号。
Time	Long	1582992000	统计时间。时间戳格式，单位：秒。
InPps	Long	2934	入方向包转发率，单位：pps。
InBps	Long	2176000	入方向带宽，单位：bps。
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。
OutPps	Long	5	出方向包转发率，单位：pps。
AttackPps	Long	0	攻击包转发率，单位：pps。
OutBps	Long	4389	出方向带宽，单位：bps。

名称	类型	示例值	描述
AttackBps	Long	0	攻击带宽，单位：bps。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePortFlowList
&ResourceGroupId=rg-acfm2pz25js****
&EndTime=1583683200
&StartTime=1582992000
&Interval=1000
&InstanceIds=["ddoscoo-cn-zz120cjv****"]
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribePortFlowListResponse>
    <RequestId>FFC77501-BDF8-4BC8-9BF5-B295FBC3189B</RequestId>
    <PortFlowList>
        <Index>0</Index>
        <Time>1582992000</Time>
        <InPps>2934</InPps>
        <InBps>2176000</InBps>
        <Region>cn</Region>
        <OutPps>5</OutPps>
        <AttackPps>0</AttackPps>
        <OutBps>4389</OutBps>
        <AttackBps>0</AttackBps>
    </PortFlowList>
</DescribePortFlowListResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "FFC77501-BDF8-4BC8-9BF5-B295FBC3189B",
  "PortFlowList" : [ {
    "Index" : 0,
    "Time" : 1582992000,
    "InPps" : 2934,
    "InBps" : 2176000,
    "Region" : "cn",
    "OutPps" : 5,
    "AttackPps" : 0,
    "OutBps" : 4389,
    "AttackBps" : 0
  } ]
}
```

错误码

访问错误中心查看更多错误码。

17.3. 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。
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。

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。
Port	String	否	null	要查询的端口号。不传入表示查询所有端口。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
ConnsList	Array of Conn		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。
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。

17.4. 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。

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。
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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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。

17.5. 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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
PortMaxConns	Array of PortMaxConns		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。

17.6. 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。

使用说明
本接口用于查询指定时间段内DDoS高防受到的攻击带宽和包速峰值。

QPS限制
本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribePortAttackMaxFlow	要执行的操作。取值：**DescribePortAttackMaxFlow**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。
EndTime	Long	是	1583683200	要查询的流量数据的结束时间。使用时间戳表示，单位：秒。 **说明** 必须为整点分钟。
StartTime	Long	是	1582992000	要查询的流量数据的开始时间。使用时间戳表示，单位：秒。 **说明** 必须为整点分钟。
InstanceIds.N	String	是	ddoscoo-cn-zvp2eibz****	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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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。
Bps	Long	149559	攻击带宽峰值。单位：bps。
Pps	Long	23	攻击包速峰值。单位：pps。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePortAttackMaxFlow
&EndTime=1583683200
&StartTime=1582992000
&InstanceIds=["ddoscoo-cn-zvp2eibz****"]
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribePortAttackMaxFlowResponse>
    <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
    <Bps>149559</Bps>
    <Pps>23</Pps>
</DescribePortAttackMaxFlowResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "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。

17.7. 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
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。关于资源组的更多信息，请参见创建资源组。
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。
InstanceIds.N	String	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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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 of Country		DDoS高防实例的请求来源国家信息。

名称	类型	示例值	描述
CountryId	String	cn	请求来源国家的简称。例如，cn表示中国，us表示美国。 说明 关于该参数的取值，请参见地域类型参数取值说明。
Count	Long	3390671	请求次数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePortViewSourceCountries
&EndTime=1583683200
&StartTime=1582992000
&InstanceIds=["ddoscoo-cn-mp91j1ao****"]
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribePortViewSourceCountriesResponse>
    <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
    <SourceCountrys>
        <CountryId>cn</CountryId>
        <Count>3390671</Count>
    </SourceCountrys>
</DescribePortViewSourceCountriesResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "SourceCountrys" : [ {
    "CountryId" : "cn",
    "Count" : 3390671
  } ]
}
```

错误码

访问错误中心查看更多错误码。

17.8. 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。

使用说明

本接口用于查询指定时间段内DDoS高防实例的请求来源运营商分布。

> **说明** 由于DDoS高防的四层传输层身份统计算法更新，目前本接口返回数据不能反应真实流量的大小，仅可用于计算不同运营商请求数量的比例（即请求的来源运营商分布情况）。如果您想获取请求流量数据，推荐您调用DescribePortFlowList。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribePortViewSourceIsps	要执行的操作。取值：**DescribePortViewSourceIsps**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。
EndTime	Long	是	1583683200	要查询的请求数据的结束时间。使用时间戳表示，单位：秒。 **说明** 必须为整点分钟。
StartTime	Long	是	1582992000	要查询的请求数据的开始时间。使用时间戳表示，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
InstanceIds.N	String	是	ddoscoo-cn-zvp2eibz****	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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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。
Isps	Array of Isp		DDoS高防实例的请求来源运营商信息。
Count	Long	3390671	相对请求数量。 **说明** 该数据不表示真实请求数量的大小，目前您可以使用该数据来计算不同运营商请求数量的比例。
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。

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

代码	运营商
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
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
&StartTime=1582992000
&InstanceIds=["ddoscoo-cn-zvp2eibz****"]
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribePortViewSourceIspsResponse>
    <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
    <Isps>
        <Count>3390671</Count>
        <IspId>100017</IspId>
    </Isps>
</DescribePortViewSourceIspsResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "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。

17.9. DescribePortViewSourceProvinces

调用DescribePortViewSourceProvinces查询指定时间段内DDoS高防实例的请求来源中国地域分布。

> **说明** 由于DDoS高防的四层传输层身份统计算法更新，目前该接口返回数据不能反应真实流量的大小，仅可用于计算不同中国地域请求数量的比例（即请求的来源中国地域分布情况）。如果您想获取请求流量数据，推荐您调用DescribePortFlowList。

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**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。关于资源组的更多信息，请参见创建资源组。
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。

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。
InstanceIds.N	String	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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
SourceProvinces	Array of Province		DDoS高防实例的请求来源中国地域信息。
ProvinceId	String	440000	请求来源中国地域的ID。例如，**110000**表示北京市，**120000**表示天津市。 说明 关于该参数的取值，请参见地域类型参数取值说明。
Count	Long	3390671	相对请求数量。 说明 该数据不表示真实请求数量的大小，目前您可以使用该数据来计算不同省份请求数量的比例。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePortViewSourceProvinces
&EndTime=1583683200
&StartTime=1582992000
&InstanceIds=["ddoscoo-cn-mp91j1ao****"]
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribePortViewSourceProvincesResponse>
    <SourceProvinces>
        <ProvinceId>440000</ProvinceId>
        <Count>3390671</Count>
    </SourceProvinces>
    <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</DescribePortViewSourceProvincesResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "SourceProvinces" : [ {
    "ProvinceId" : "440000",
    "Count" : 3390671
  } ],
  "RequestId" : "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

访问错误中心查看更多错误码。

17.10. 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。
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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
DomainAttackEvents	Array of Data		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。
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。

17.11. 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**。

名称	类型	是否必选	示例值	描述
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。 关于资源组的更多信息，请参见创建资源组。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。
StartTime	Long	是	1582992000	查询开始时间。使用时间戳格式，单位：秒。 **说明** 必须为整点分钟。
EndTime	Long	是	1583683200	查询结束时间。使用时间戳格式，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。
Domain	String	否	www.aliyun.com	要查询的网站业务的域名。不设置该参数表示查询所有域名的数据。 **说明** 域名必须已接入DDoS高防进行防护。您可以调用DescribeDomains查询所有已接入DDoS高防的域名。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
DomainQPSList	Array of DomainQPS		网站业务QPS统计信息。
Index	Long	0	返回数据的索引号。
Time	Long	1582992000	统计时间。时间戳格式，单位：秒。

名称	类型	示例值	描述
MaxAttackQps	Long	37	攻击QPS峰值。
AttackQps	Long	1	攻击QPS。
MaxQps	Long	130	总QPS峰值。
MaxNormalQps	Long	93	正常QPS峰值。
TotalQps	Long	1	总QPS。
TotalCount	Long	20008	总访问次数。
CacheHits	Long	0	缓存命中次数。
RequestId	String	327F2ABB-104D-437A-AAB5-D633E29A8C51	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainQPSList
&StartTime=1582992000
&EndTime=1583683200
&Interval=1000
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeDomainQPSListResponse>
    <DomainQPSList>
        <Index>0</Index>
        <Time>1582992000</Time>
        <MaxAttackQps>37</MaxAttackQps>
        <AttackQps>1</AttackQps>
        <MaxQps>130</MaxQps>
        <MaxNormalQps>93</MaxNormalQps>
        <TotalQps>1</TotalQps>
        <TotalCount>20008</TotalCount>
        <CacheHits>0</CacheHits>
    </DomainQPSList>
    <RequestId>327F2ABB-104D-437A-AAB5-D633E29A8C51</RequestId>
</DescribeDomainQPSListResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "DomainQPSList" : [ {
    "Index" : 0,
    "Time" : 1582992000,
    "MaxAttackQps" : 37,
    "AttackQps" : 1,
    "MaxQps" : 130,
    "MaxNormalQps" : 93,
    "TotalQps" : 1,
    "TotalCount" : 20008,
    "CacheHits" : 0
  } ],
  "RequestId" : "327F2ABB-104D-437A-AAB5-D633E29A8C51"
}
```

错误码

访问错误中心查看更多错误码。

17.12. 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**。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。关于资源组的更多信息，请参见创建资源组。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。
StartTime	Long	是	1582992000	查询开始时间。使用时间戳格式，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
EndTime	Long	否	1583683200	查询结束时间。使用时间戳格式，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查询结果。
Domain	String	否	www.example.com	网站业务的域名。 说明 您可以调用DescribeDomains查询所有已接入DDoS高防防护的网站业务的域名。
QueryType	String	是	gf	查询数据的来源。取值： • gf：表示高防响应数据。 • upstream：表示源站响应数据。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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 of StatusCode		响应状态码的统计信息。
Status502	Long	0	502状态码的统计值。
Index	Integer	0	返回数据的索引号。
Time	Long	1582992000	统计时间。时间戳格式，单位：秒。
Status405	Long	0	405状态码的统计值。
Status3XX	Long	0	3XX类状态码的统计值。
Status503	Long	0	503状态码的统计值。
Status4XX	Long	4486	4XX类状态码的统计值。
Status2XX	Long	15520	2XX类状态码的统计值。

名称	类型	示例值	描述
Status5XX	Long	0	5XX类状态码的统计值。
Status504	Long	0	504状态码的统计值。
Status403	Long	0	403状态码的统计值。
Status200	Long	15520	200状态码的统计值。
Status404	Long	0	404状态码的统计值。
Status501	Long	0	501状态码的统计值。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainStatusCodeList
&ResourceGroupId=rg-acfm2pz25js****
&StartTime=1582992000
&EndTime=1583683200
&Interval=1000
&Domain=www.example.com
&QueryType=gf
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeDomainStatusCodeListResponse>
    <RequestId>3B63C0DD-8AC5-44B2-95D6-064CA9296B9C</RequestId>
    <StatusCodeList>
        <Status502>0</Status502>
        <Index>0</Index>
        <Time>1582992000</Time>
        <Status405>0</Status405>
        <Status3XX>0</Status3XX>
        <Status503>0</Status503>
        <Status4XX>4486</Status4XX>
        <Status2XX>15520</Status2XX>
        <Status5XX>0</Status5XX>
        <Status504>0</Status504>
        <Status403>0</Status403>
        <Status200>15520</Status200>
        <Status404>0</Status404>
        <Status501>0</Status501>
    </StatusCodeList>
</DescribeDomainStatusCodeListResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "3B63C0DD-8AC5-44B2-95D6-064CA9296B9C",
  "StatusCodeList" : [ {
    "Status502" : 0,
    "Index" : 0,
    "Time" : 1582992000,
    "Status405" : 0,
    "Status3XX" : 0,
    "Status503" : 0,
    "Status4XX" : 4486,
    "Status2XX" : 15520,
    "Status5XX" : 0,
    "Status504" : 0,
    "Status403" : 0,
    "Status200" : 15520,
    "Status404" : 0,
    "Status501" : 0
  } ]
}
```

错误码

访问错误中心查看更多错误码。

17.13. DescribeDomainOverview

调用DescribeDomainOverview查询指定时间段内网站业务的HTTP清洗峰值（qps）和HTTPS清洗峰值（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	DescribeDomainOverview	要执行的操作。取值：**DescribeDomainOverview**。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。关于资源组的更多信息，请参见创建资源组。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。

名称	类型	是否必选	示例值	描述
StartTime	Long	是	1619798400	查询开始时间。使用时间戳格式，单位：秒。 **说明** 必须为整点分钟。
EndTime	Long	否	1623462364	查询结束时间。使用时间戳格式，单位：秒。不设置该参数表示使用当前时间作为查询结束时间。 **说明** 必须为整点分钟。
Domain	String	否	www.aliyun.com	要查询的网站业务的域名。不设置该参数表示查询所有域名的数据。 **说明** 域名必须已接入DDoS高防进行防护。您可以调用DescribeDomains查询所有已接入DDoS高防的域名。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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。
MaxHttps	Long	0	HTTPS清洗峰值，单位：qps。
MaxHttp	Long	41652	HTTP清洗峰值，单位：qps。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainOverview
&StartTime=1619798400
&EndTime=1623462364
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeDomainOverviewResponse>
    <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
    <MaxHttps>0</MaxHttps>
    <MaxHttp>41652</MaxHttp>
</DescribeDomainOverviewResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "MaxHttps" : 0,
  "MaxHttp" : 41652
}
```

错误码

访问错误中心查看更多错误码。

17.14. 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**。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。关于资源组的更多信息，请参见创建资源组。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。

名称	类型	是否必选	示例值	描述
StartTime	Long	是	1582992000	查询开始时间。使用时间戳格式，单位：秒。 **说明** 必须为整点分钟。
EndTime	Long	是	1583683200	查询结束时间。使用时间戳格式，单位：秒。 **说明** 必须为整点分钟。
Domain	String	否	www.aliyun.com	要查询的网站业务的域名。不设置该参数表示查询所有域名的数据。 **说明** 域名必须已接入DDoS高防进行防护。您可以调用DescribeDomains查询所有已接入DDoS高防的域名。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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。
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。
Status403	Long	0	查询时间段内403状态码的数量。
Status503	Long	0	查询时间段内503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。
Status504	Long	0	查询时间段内504状态码的数量。
Status2XX	Long	951472	查询时间段内2XX类状态码的数量。

名称	类型	示例值	描述
Status200	Long	951159	查询时间段内200状态码的数量。
Status3XX	Long	133209	查询时间段内3XX状态码的数量。
Status4XX	Long	5653	查询时间段内4XX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
&StartTime=1582992000
&EndTime=1583683200
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeDomainStatusCodeCountResponse>
    <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
    <Status501>0</Status501>
    <Status502>0</Status502>
    <Status403>0</Status403>
    <Status503>0</Status503>
    <Status404>897</Status404>
    <Status405>0</Status405>
    <Status504>0</Status504>
    <Status2XX>951472</Status2XX>
    <Status200>951159</Status200>
    <Status3XX>133209</Status3XX>
    <Status4XX>5653</Status4XX>
    <Status5XX>14</Status5XX>
</DescribeDomainStatusCodeCountResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "Status501" : 0,
  "Status502" : 0,
  "Status403" : 0,
  "Status503" : 0,
  "Status404" : 897,
  "Status405" : 0,
  "Status504" : 0,
  "Status2XX" : 951472,
  "Status200" : 951159,
  "Status3XX" : 133209,
  "Status4XX" : 5653,
  "Status5XX" : 14
}
```

错误码

访问错误中心查看更多错误码。

17.15. 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。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-hangzhou	DDoS高防服务的地域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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
AttackList	Array of Data		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。

17.16. 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**。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。关于资源组的更多信息，请参见创建资源组。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。
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。
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
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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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 of Country		网站业务的请求来源国家信息。
CountryId	String	cn	请求来源国家的简称。例如，**cn**表示中国，**us**表示美国。 **说明** 关于该参数的取值，请参见地域类型参数取值说明。
Count	Long	3390671	请求数量。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainViewSourceCountries
&StartTime=1582992000
&EndTime=1583683200
&Domain=www.aliyun.com
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeDomainViewSourceCountriesResponse>
    <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
    <SourceCountrys>
        <CountryId>cn</CountryId>
        <Count>3390671</Count>
    </SourceCountrys>
</DescribeDomainViewSourceCountriesResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "SourceCountrys" : [ {
    "CountryId" : "cn",
    "Count" : 3390671
  } ]
}
```

错误码

访问错误中心查看更多错误码。

17.17. DescribeDomainViewSourceProvinces

调用DescribeDomainViewSourceProvinces查询指定时间段内网站业务的请求来源中国地域分布。

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**。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。关于资源组的更多信息，请参见创建资源组。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，对应DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，对应DDoS高防（国际）实例。

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。
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。
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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
SourceProvinces	Array of Province		网站业务的请求来源中国地域信息。
ProvinceId	String	440000	请求来源中国地域的ID。例如，**110000**表示北京市，**120000**表示天津市。 说明 关于该参数的取值，请参见地域类型参数取值说明。
Count	Long	3390671	请求数量。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainViewSourceProvinces
&StartTime=1582992000
&EndTime=1583683200
&Domain=www.aliyun.com
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeDomainViewSourceProvincesResponse>
    <SourceProvinces>
        <ProvinceId>440000</ProvinceId>
        <Count>3390671</Count>
    </SourceProvinces>
    <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</DescribeDomainViewSourceProvincesResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "SourceProvinces" : [ {
    "ProvinceId" : "440000",
    "Count" : 3390671
  } ],
  "RequestId" : "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

访问错误中心查看更多错误码。

17.18. 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**。

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。
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。
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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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 of Url		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。
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。

17.19. 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**。

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。
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。
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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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 of Url		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。

17.20. 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**。

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。
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。
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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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。

名称	类型	示例值	描述
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。

18.全量日志分析

18.1. 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。

18.2. 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。

18.3. 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。

18.4. 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。
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。

18.5. 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	ModifyFullLogTtl	要执行的操作。取值：**ModifyFullLogTtl**
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。

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=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。

18.6. DescribeWebAccessLogDispatchStatus

调用DescribeWebAccessLogDispatchStatus查询所有域名的全量日志开关状态。

使用说明

本接口用于查询所有已接入DDoS高防防护的域名的全量日志开关状态。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeWebAccessLogDispatchStatus	要执行的操作。取值：**DescribeWebAccessLogDispatchStatus**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。
PageNumber	Integer	否	1	分页查询时，设置当前页面的页面。默认值为**1**。
PageSize	Integer	否	10	分页查询时，设置每页包含域名的数量。默认值为**10**。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
TotalCount	Integer	1	查询到的域名的总数量。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
SlsConfigStatus	Array of SlsConfigStatus		域名的全量日志开关状态。
Domain	String	www.aliyundoc.com	域名。
Enable	Boolean	true	是否开启全量日志采集。取值： • **true**：表示已开启。 • **false**：表示未开启。

示例

请求示例

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

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeWebAccessLogDispatchStatusResponse>
    <TotalCount>1</TotalCount>
    <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
    <SlsConfigStatus>
        <Domain>www.aliyundoc.com</Domain>
        <Enable>true</Enable>
    </SlsConfigStatus>
</DescribeWebAccessLogDispatchStatusResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "TotalCount" : 1,
  "RequestId" : "CF33B4C3-196E-4015-AADD-5CAD00057B80",
  "SlsConfigStatus" : [ {
    "Domain" : "www.aliyundoc.com",
    "Enable" : true
  } ]
}
```

错误码

访问错误中心查看更多错误码。

18.7. 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
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

```
<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。

18.8. 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。

18.9. 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。

18.10. 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。

18.11. 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
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。

19.系统配置与日志

19.1. DescribeStsGrantStatus

调用DescribeStsGrantStatus查询是否授权DDoS高防服务访问其他云产品。

使用说明

本接口用于查询当前阿里云账号是否已授权DDoS高防服务访问其他云产品。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeStsGrantStatus	要执行的操作。取值：**DescribeStsGrantStatus**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。
Role	String	是	AliyunDDoSCOODefaultRole	要查询的RAM角色名称。取值固定为**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。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述

名称	类型	示例值	描述
RequestId	String	6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1	本次请求的ID。
StsGrant	Object		DDoS高防服务的授权状态。
Status	Integer	1	授权状态。取值： • **0**：表示未授权DDoS高防服务访问其他云产品资源。 • **1**：表示已授权DDoS高防服务访问其他云产品资源。

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

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeStsGrantStatusResponse>
    <RequestId>6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1</RequestId>
    <StsGrant>
        <Status>1</Status>
    </StsGrant>
</DescribeStsGrantStatusResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1",
  "StsGrant" : {
    "Status" : 1
  }
}
```

错误码

访问错误中心查看更多错误码。

19.2. 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。

19.3. 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。
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。

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。
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。
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。
			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。

名称	类型	示例值	描述

OpDesc	String	{"newEntity":{"actionMethod":"undo"}}	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下：
			• instanceId：String类型，更换IP的ECS实例ID。
			示例：`{"newEntity":{"instanceId":"i-wz9h6nc313zptbqn****"}}`
			OpAction为9时，操作参数的结构描述如下：
			• actionMethod：String类型，操作方法。取值：undo，表示解除黑洞。
			示例：`{"newEntity":{"actionMethod":"undo"}}`
			OpAction为10时，操作参数的结构描述如下：
			• actionMethod：String类型，操作方法。取值：
			  ◦ do：开启近源流量压制
			  ◦ undo：取消近源流量压制
			• lines：Array类型，操作的线路类型。取值：
			  ◦ ct：电信海外线路
			  ◦ cut：联通海外线路
			示例：`{"newEntity":{"actionMethod":"undo","lines":["ct"]}}`
			OpAction为11时，无操作参数，操作描述为空。

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。

19.4. 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。
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。

19.5. DescribeSystemLog

调用DescribeSystemLog查询弹性业务带宽的账单详情。

使用说明

本接口用于查询DDoS高防服务的系统日志。系统日志目前只包含弹性业务带宽的出账日志。

如果您已经启用弹性业务带宽，可以调用本接口查询弹性业务带宽的账单详情。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeSystemLog	要执行的操作。取值：**DescribeSystemLog**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。
EntityType	Integer	否	20	要查询的系统日志的类型。取值固定为**20**，表示弹性业务带宽出账日志。 **说明** 必须设置该参数，否则会调用失败。
EntityObject	String	否	203.107.XX.XX	要查询的DDoS高防实例的IP地址。 **说明** 您可以调用DescribeInstanceDetails查询DDoS高防实例的IP地址。
StartTime	Long	是	1609430400000	设置起始时间，查询在该起始时间后出账的弹性业务带宽账单。使用时间戳表示，单位：毫秒。
EndTime	Long	是	1640966400000	设置结束时间，查询在该结束时间前出账的弹性业务带宽账单。使用时间戳表示，单位：毫秒。
PageNumber	Integer	是	1	分页查询时，设置当前页面的页码。
PageSize	Integer	是	10	分页查询时，设置每页包含日志的数量。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
Total	Long	1	查询到的弹性业务带宽出账日志的总数量。
RequestId	String	8BC3A33A-F832-58DB-952F-7682A25AD14C	本次请求的ID。
SystemLog	Array of SystemLog		弹性业务带宽出账日志的详情列表。
Status	Integer	1	账单的状态。取值： • **0**：表示待出账。 • **1**：表示已出账。 • **2**：表示终止出账。
EntityType	Integer	20	系统日志的类型。取值固定为**20**，表示弹性业务带宽出账日志。
EntityObject	String	203.107.XX.XX	DDoS高防实例的IP地址。
GmtCreate	Long	1631793531000	账单的创建时间。使用时间戳表示，单位：毫秒。
OpAction	Integer	100	操作类型。取值固定为**100**，表示新增弹性业务带宽出账记录。
GmtModified	Long	1635425407000	账单最后一次被修改的时间。使用时间戳表示，单位：毫秒。
OpAccount	String	171986973287****	账单所属阿里云账号的ID。

名称	类型	示例值	描述
OpDesc	String	{"newEntity":{"billValue":"60","instanceId":"ddoscoo-cn-zz121ogz****","ip":"203.107.XX.XX","maxBw":"300","month":1627747200000,"overBandwidth":"120","peakTime":1629871200,"startTimestamp":1629871200}}	账单详情。使用JSON结构体转化的字符串表示，JSON结构体包含以下字段： • **newEntity**：Object类型，表示账单记录，具体包含以下字段： ◦ **billValue**：Integer类型 | 计费月份的弹性业务带宽用量，单位：Mbps。 ◦ **instanceId**：String类型 | DDoS高防实例的ID。 ◦ **ip**：String类型 | DDoS高防实例的IP地址。 ◦ **maxBw**：String类型 | 计费月份的实际业务流量峰值（月95峰值），单位：Mbps。 ◦ **month**：Long类型 | 账单出具月份（计费月份为账单出具月份的上个自然月），使用时间戳表示，单位：毫秒。 ◦ **overBandwidth**：Integer类型 | 实际业务流量峰值超出实例业务带宽规格的带宽大小，单位：Mbps。 ◦ **peakTime**：Long类型 | 实际业务流量峰值的计量时刻，使用时间戳表示，单位：秒。 ◦ **startTimestamp**：Long类型 | 实例业务流量峰值区间的起始时刻，使用时间戳表示，单位：秒。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeSystemLog
&EndTime=1640966400000
&PageNumber=1
&PageSize=10
&StartTime=1609430400000
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeSystemLogResponse>
    <Total>1</Total>
    <RequestId>8BC3A33A-F832-58DB-952F-7682A25AD14C</RequestId>
    <SystemLog>
        <Status>1</Status>
        <EntityType>20</EntityType>
        <EntityObject>203.107.XX.XX</EntityObject>
        <GmtCreate>1631793531000</GmtCreate>
        <OpAction>100</OpAction>
        <GmtModified>1635425407000</GmtModified>
        <OpAccount>171986973287****</OpAccount>
        <OpDesc>{"newEntity":{"billValue":"60","instanceId":"ddoscoo-cn-zz121ogz****","ip":"2
03.107.XX.XX","maxBw":"300","month":1627747200000,"overBandwidth":"120","peakTime":1629871200
,"startTimestamp":1629871200}}</OpDesc>
    </SystemLog>
</DescribeSystemLogResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "Total" : 1,
  "RequestId" : "8BC3A33A-F832-58DB-952F-7682A25AD14C",
  "SystemLog" : [ {
    "Status" : 1,
    "EntityType" : 20,
    "EntityObject" : "203.107.XX.XX",
    "GmtCreate" : 1631793531000,
    "OpAction" : 100,
    "GmtModified" : 1635425407000,
    "OpAccount" : "171986973287****",
    "OpDesc" : "{\"newEntity\":{\"billValue\":\"60\",\"instanceId\":\"ddoscoo-cn-zz121ogz****
\",\"ip\":\"203.107.XX.XX\",\"maxBw\":\"300\",\"month\":1627747200000,\"overBandwidth\":\"120
\",\"peakTime\":1629871200,\"startTimestamp\":1629871200}}"
  } ]
}
```

错误码

访问错误中心查看更多错误码。

19.6. DescribeAsyncTasks

调用DescribeAsyncTasks查询异步导出任务的详细信息。

使用说明

本接口用于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。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeAsyncTasks	要执行的操作。取值：**DescribeAsyncTasks**。
RegionId	String	否	cn-hangzhou	DDoS高防实例所属地域ID。取值： • **cn-hangzhou**（默认）：表示中国内地，即DDoS高防（新BGP）实例。 • **ap-southeast-1**：表示非中国内地，即DDoS高防（国际）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。
PageNumber	Integer	是	1	分页查询时，设置当前页面的页码。
PageSize	Integer	是	10	分页查询时，设置每页包含异步导出任务的数量。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
TotalCount	Integer	1	查询到的异步导出任务的总数量。
RequestId	String	6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1	本次请求的ID。
AsyncTasks	Array of AsyncTask		异步导出任务的详细信息。
EndTime	Long	157927362000	任务结束时间。使用时间戳表示，单位：毫秒。

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，表示导出DDoS高防实例的端口转发规则。 • **2**：七层导出任务，表示导出网站业务转发规则。 • **3**：会话、健康检查导出任务，表示导出DDoS高防实例的会话、健康检查配置。 • **4**：DDoS防护策略导出任务，表示导出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，表示导出针对DDoS高防实例的黑名单IP。 • **6**：白名单（针对目的IP）下载任务，表示导出针对DDoS高防实例的白名单IP。
StartTime	Long	156927362000	任务开始时间。使用时间戳表示，单位：毫秒。
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。
TaskStatus	Integer	2	任务状态。取值： • **0**：表示任务初始化。 • **1**：表示任务进行中。 • **2**：表示任务成功。 • **3**：表示任务失败。
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。
TaskId	Long	1	任务ID。

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

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeAsyncTasksResponse>
    <TotalCount>1</TotalCount>
    <RequestId>6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1</RequestId>
    <AsyncTasks>
        <EndTime>157927362000</EndTime>
        <TaskType>5</TaskType>
        <StartTime>156927362000</StartTime>
        <TaskParams>{"instanceId": "ddoscoo-cn-mp91j1ao****"}</TaskParams>
        <TaskStatus>2</TaskStatus>
        <TaskResult>{"instanceId": "ddoscoo-cn-mp91j1ao****","url": "https://****.oss-cn-beij
ing.aliyuncs.com/heap.bin?Expires=1584785140&amp;OSSAccessKeyId=TMP.3KfzD82FyRJevJdEkRX6JEFHh
bvRBBb75PZJnyJmksA2QkMm47xFAFDgMhEV8Nm6Vxr8xExMfiy9LsUFAcLcTBrN3rDu3v&amp;Signature=Sj8BNcsxJ
LE8l5qm4cjNlDt8gv****"}</TaskResult>
        <TaskId>1</TaskId>
    </AsyncTasks>
</DescribeAsyncTasksResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "TotalCount" : 1,
  "RequestId" : "6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1",
  "AsyncTasks" : [ {
    "EndTime" : 157927362000,
    "TaskType" : 5,
    "StartTime" : 156927362000,
    "TaskParams" : "{\"instanceId\": \"ddoscoo-cn-mp91j1ao****\"}",
    "TaskStatus" : 2,
    "TaskResult" : "{\"instanceId\": \"ddoscoo-cn-mp91j1ao****\",\"url\": \"https://****.oss-
cn-beijing.aliyuncs.com/heap.bin?Expires=1584785140&OSSAccessKeyId=TMP.3KfzD82FyRJevJdEkRX6JE
FHhbvRBBb75PZJnyJmksA2QkMm47xFAFDgMhEV8Nm6Vxr8xExMfiy9LsUFAcLcTBrN3rDu3v&Signature=Sj8BNcsxJL
E8l5qm4cjNlDt8gv****\"}",
    "TaskId" : 1
  } ]
}
```

错误码

访问错误中心查看更多错误码。

19.7. 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
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。

19.8. 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**

名称	类型	是否必选	示例值	描述
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。

20.标签

20.1. DescribeTagKeys

调用DescribeTagKeys查询所有标签键及标签键关联的DDoS高防（新BGP）实例的数量。

使用说明

本接口用于分页查询所有标签键及标签键关联的DDoS高防（新BGP）实例的数量。

> 说明 只有DDoS高防（新BGP）服务支持标签功能。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeTagKeys	要执行的操作。取值：**DescribeTagKeys**。
RegionId	String	是	cn-hangzhou	DDoS高防实例所属地域ID。取值固定为**cn-hangzhou**，表示中国内地，即DDoS高防（新BGP）服务。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。
ResourceType	String	是	INSTANCE	资源类型。取值固定为**INSTANCE**，表示DDoS高防实例。
PageSize	Integer	否	10	分页查询时，设置每页包含标签键的数量。默认值为**10**。
PageNumber	Integer	否	1	分页查询时，设置当前页面的页码。默认值为**1**。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述

名称	类型	示例值	描述
RequestId	String	6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1	本次请求的ID。
PageNumber	Integer	1	当前页面的页码。
PageSize	Integer	10	每页包含标签键的数量。
TotalCount	Integer	1	查询到的标签键的总数量。
TagKeys	Array of TagKey		标签键详情列表。
TagCount	Integer	2	标签键关联的DDoS高防（新BGP）实例的数量。
TagKey	String	aa1	标签键。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeTagKeys
&RegionId=cn-hangzhou
&ResourceType=INSTANCE
&PageSize=10
&PageNumber=1
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeTagKeysResponse>
    <RequestId>6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1</RequestId>
    <PageNumber>1</PageNumber>
    <PageSize>10</PageSize>
    <TotalCount>1</TotalCount>
    <TagKeys>
        <TagCount>2</TagCount>
        <TagKey>aa1</TagKey>
    </TagKeys>
</DescribeTagKeysResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1",
  "PageNumber" : 1,
  "PageSize" : 10,
  "TotalCount" : 1,
  "TagKeys" : [ {
    "TagCount" : 2,
    "TagKey" : "aa1"
  } ]
}
```

错误码

访问错误中心查看更多错误码。

20.2. DescribeTagResources

调用DescribeTagResources查询DDoS高防（新BGP）实例绑定的标签信息。

使用说明

本接口用于查询DDoS高防（新BGP）实例绑定的标签信息。

> **说明** 只有DDoS高防（新BGP）服务支持标签功能。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeTagResources	要执行的操作。取值：**DescribeTagResources**。
RegionId	String	是	cn-hangzhou	DDoS高防实例所属地域ID。取值固定为**cn-hangzhou**，表示中国内地，即DDoS高防（新BGP）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。
ResourceType	String	是	INSTANCE	资源类型。取值固定为**INSTANCE**，表示DDoS高防实例。

名称	类型	是否必选	示例值	描述
NextToken	String	否	RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCf****	查询凭证（Token）。取值为上一次调用本接口返回的**NextToken**参数值。 说明 初次调用本接口时无需设置该参数。
ResourceIds.N	String	否	ddoscoo-cn-zz121ogz****	要查询的DDoS高防（新BGP）实例的ID。 说明 • ResourceIds.N与Tags.N.Key不能同时为空。 • 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID。
Tags.N.Key	String	否	testkey	要查询的标签键。 说明 • ResourceIds.N与Tags.N.Key不能同时为空。 • 您可以调用DescribeTagKeys查询所有标签键。
Tags.N.Value	String	否	testvalue	要查询的标签值。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
NextToken	String	RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCf****	本次调用返回的查询凭证（Token）。
RequestId	String	36E698F7-48A4-48D0-9554-0BB4BAAB99B3	本次请求的ID。
TagResources	Array of TagResource		DDoS高防（新BGP）实例绑定的标签列表。
TagResource			

名称	类型	示例值	描述
TagValue	String	testkey	DDoS高防（新BGP）实例绑定的标签值。
ResourceType	String	INSTANCE	资源类型。取值固定为**INSTANCE**，表示DDoS高防实例。
ResourceId	String	ddoscoo-cn-zz121ogz****	DDoS高防（新BGP）实例的ID。
TagKey	String	testvalue	DDoS高防（新BGP）实例绑定的标签键。

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

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeTagResourcesResponse>
    <NextToken>RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCf****</NextToken>
    <RequestId>36E698F7-48A4-48D0-9554-0BB4BAAB99B3</RequestId>
    <TagResources>
        <TagValue>testkey</TagValue>
        <ResourceType>INSTANCE</ResourceType>
        <ResourceId>ddoscoo-cn-zz121ogz****</ResourceId>
        <TagKey>testvalue</TagKey>
    </TagResources>
</DescribeTagResourcesResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "NextToken" : "RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCf****",
  "RequestId" : "36E698F7-48A4-48D0-9554-0BB4BAAB99B3",
  "TagResources" : [ {
    "TagValue" : "testkey",
    "ResourceType" : "INSTANCE",
    "ResourceId" : "ddoscoo-cn-zz121ogz****",
    "TagKey" : "testvalue"
  } ]
}
```

错误码

访问错误中心查看更多错误码。

20.3. CreateTagResources

调用CreateTagResources为DDoS高防（新BGP）实例绑定标签。

使用说明

本接口用于批量为DDoS高防（新BGP）实例绑定标签。

> 说明 DDoS高防（国际）实例不支持标签功能。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateTagResources	要执行的操作。取值：**CreateTagResources**。
RegionId	String	是	cn-hangzhou	DDoS高防实例所属地域ID。取值固定为**cn-hangzhou**，表示中国内地，即DDoS高防（新BGP）实例。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。
ResourceType	String	是	INSTANCE	资源类型。取值固定为**INSTANCE**，表示DDoS高防实例。
ResourceIds.N	String	是	ddoscoo-cn-mp91j1ao****	要绑定标签的DDoS高防（新BGP）实例的ID。 > 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID。
Tags.N.Key	String	否	testkey	要绑定的标签键。
Tags.N.Value	String	否	testvalue	要绑定的标签值。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

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
&ResourceGroupId=rg-acfm2pz25js****
&ResourceType=INSTANCE
&ResourceIds=["ddoscoo-cn-mp91j1ao****"]
&Tags=[{"Key":"testkey","Value":"testvalue"}]
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<?xml version="1.0" encoding="UTF-8" ?>
<CreateTagResourcesResponse>
 <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</CreateTagResourcesResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

访问错误中心查看更多错误码。

20.4. DeleteTagResources

调用DeleteTagResources为DDoS高防（新BGP）实例移除标签。

使用说明

本接口用于为DDoS高防（新BGP）实例移除标签。

> 说明 只有DDoS高防（新BGP）服务支持标签功能。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteTagResources	要执行的操作。取值：**DeleteTagResources**。
RegionId	String	是	cn-hangzhou	DoS高防实例所属地域ID。取值固定为**cn-hangzhou**，表示中国内地，即DDoS高防（新BGP）服务。
ResourceGroupId	String	否	rg-acfm2pz25js****	DDoS高防实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。
ResourceType	String	是	INSTANCE	资源类型。取值固定为**INSTANCE**，表示DDoS高防实例。
All	Boolean	否	false	是否移除资源上的所有标签。取值： • **true**：表示是。 • **false**（默认）：表示否。
ResourceIds.N	String	是	ddoscoo-cn-zvp2eibz****	要移除标签的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。
TagKey.N	String	否	doc-test-key	要移除的标签键。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteTagResources
&RegionId=cn-hangzhou
&ResourceType=INSTANCE
&All=false
&ResourceIds=["ddoscoo-cn-zvp2eibz****"]
&TagKey=["doc-test-key"]
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DeleteTagResourcesResponse>
    <RequestId>6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1</RequestId>
</DeleteTagResourcesResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "6623EA1F-30FB-5BC8-BEC9-74D55F6F08F1"
}
```

错误码

访问错误中心查看更多错误码。

21.地域类型参数取值说明

本文列举了DDoS高防API中与地域设置有关的参数及参数取值说明，方便您查询使用。

> **说明** 为了提升您查询地域类型参数的体验，我们改进了本文档的内容结构。我们希望听到您的声音：目前这种查询方式是否便于使用？您是否有其他更好的方式向我们推荐？
> 您可以选中本文任意一行文字，并单击**文档反馈**，留下您宝贵的意见。

Area

使用场景：您调用DescribeDDosEventArea接口获得的返回数据中，Area表示攻击来源地域的代码。

查看Area取值说明 ❯

AreaId

使用场景：您调用DescribeDDosEventSrcIp接口获得的返回数据中，AreaId表示攻击来源地域的代码。

查看AreaId取值说明 ❯

Countries和Provinces

使用场景：

- 您调用ConfigNetworkRegionBlock接口，在请求参数Config中设置Countries和Provinces，分别表示要封禁的国际地域的代码、中国地域的代码。
- 您调用DescribeNetworkRegionBlock接口获得的返回数据中，Countries和Provinces分别表示被封禁的国际地域的代码、中国地域的代码。

查看Countries取值说明 ❯

查看Provinces取值说明 ❯

CountryId

使用场景：

- 您调用DescribeDomainViewSourceCountries接口获得的返回数据中，CountryId表示网站业务对应的请求来源国家代码。
- 您调用DescribePortViewSourceCountries接口获得的返回数据中，CountryId表示DDoS高防实例对应的请求来源国家代码。

查看CountryId取值说明 ❯

ProvinceId

使用场景：

- 您调用DescribeDomainViewSourceProvinces接口获得的返回数据中，ProvinceId表示网站业务对应的请求来源中国地域代码。
- 您调用DescribePortViewSourceProvinces接口获得的返回数据中，ProvinceId表示DDoS高防实例对应的请求来源中国地域代码。

查看ProvinceId取值说明 ❯

Regions

使用场景：您调用ModifyWebAreaBlock接口，在请求参数中设置Regions，表示要封禁的中国地域和国际地域的代码。

查看Regions取值说明 ❯

22.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。
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。