ALIBABA CLOUD

阿里云

配置审计

API参考

文档版本：20200820

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 10
2.调用方式 18
3.签名机制 19
4.公共参数 22
5.获取AccessKey 24
6.实例 26
6.1. DescribeInstanceIds 26
6.2. DescribeInstances 28
6.3. DescribeInstanceDetails 32
6.4. DescribeInstanceSpecs 35
6.5. DescribeInstanceStatistics 38
6.6. ModifyInstanceRemark 40
6.7. DescribeElasticBandwidthSpec 42
6.8. ModifyElasticBandWidth 44
6.9. DescribeDefenseCountStatistics 45
6.10. ReleaseInstance 47
7.域名接入 50
7.1. DescribeDomains 50
7.2. DescribeWebRules 51
7.3. CreateWebRule 57
7.4. ModifyWebRule 59
7.5. DeleteWebRule 61
7.6. DescribeWebInstanceRelations 62
7.7. DescribeCerts 65
7.8. AssociateWebCert 68
7.9. DescribeWebCustomPorts 71

7.10. ModifyTlsConfig 73
7.11. ModifyHttp2Enable 75
7.12. DescribeWebAccessMode 77
7.13. ModifyWebAccessMode 79
7.14. DescribeCnameReuses 80
7.15. ModifyCnameReuse 82
8.端口接入 85
8.1. DescribeNetworkRules 85
8.2. CreateNetworkRules 88
8.3. ConfigNetworkRules 90
8.4. DeleteNetworkRule 92
8.5. DescribeHealthCheckList 93
8.6. ModifyHealthCheckConfig 97
8.7. DescribeHealthCheckStatus 99
9.流量调度器 103
9.1. DescribeSchedulerRules 103
9.2. CreateSchedulerRule 108
9.3. ModifySchedulerRule 110
9.4. DeleteSchedulerRule 113
10.基础设施防护策略 115
10.1. DescribeAutoCcListCount 115
10.2. DescribeAutoCcBlacklist 116
10.3. AddAutoCcBlacklist 119
10.4. DeleteAutoCcBlacklist 121
10.5. EmptyAutoCcBlacklist 122
10.6. DescribeAutoCcWhitelist 124
10.7. AddAutoCcWhitelist 127
10.8. DeleteAutoCcWhitelist 129

10.9. EmptyAutoCcWhitelist 130
10.10. DescribeUnBlackholeCount 131
10.11. DescribeBlackholeStatus 133
10.12. ModifyBlackholeStatus 135
10.13. DescribeNetworkRegionBlock 137
10.14. ConfigNetworkRegionBlock 139
10.15. DescribeBlockStatus 141
10.16. ModifyBlockStatus 144
10.17. DescribeUnBlockCount 146
11.网站业务防护策略 148
11.1. DescribeWebCcProtectSwitch 148
11.2. ModifyWebAIProtectSwitch 151
11.3. ModifyWebAIProtectMode 153
11.4. ModifyWebIpSetSwitch 155
11.5. ConfigWebIpSet 156
11.6. EnableWebCC 158
11.7. DisableWebCC 160
11.8. ConfigWebCCTemplate 161
11.9. EnableWebCCRule 163
11.10. DisableWebCCRule 164
11.11. DescribeWebCCRules 166
11.12. CreateWebCCRule 169
11.13. ModifyWebCCRule 171
11.14. DeleteWebCCRule 173
11.15. ModifyWebPreciseAccessSwitch 175
11.16. DescribeWebPreciseAccessRule 177
11.17. ModifyWebPreciseAccessRule 180
11.18. DeleteWebPreciseAccessRule 186

11.19. ModifyWebAreaBlockSwitch 187
11.20. DescribeWebAreaBlockConfigs 189
11.21. ModifyWebAreaBlock 199
12.非网站业务防护策略 203
12.1. DescribePortAutoCcStatus 203
12.2. ModifyPortAutoCcStatus 205
12.3. DescribeNetworkRuleAttributes 207
12.4. ModifyNetworkRuleAttribute 213
13.定制场景策略 215
13.1. DescribeSceneDefensePolicies 215
13.2. CreateSceneDefensePolicy 220
13.3. ModifySceneDefensePolicy 221
13.4. DeleteSceneDefensePolicy 223
13.5. DescribeSceneDefenseObjects 225
13.6. AttachSceneDefenseObject 227
13.7. DetachSceneDefenseObject 229
13.8. EnableSceneDefensePolicy 230
13.9. DisableSceneDefensePolicy 232
14.静态页面缓存 234
14.1. ModifyWebCacheSwitch 234
14.2. ModifyWebCacheMode 235
14.3. ModifyWebCacheCustomRule 237
14.4. DeleteWebCacheCustomRule 239
14.5. DescribeWebCacheConfigs 240
15.监控报表 244
15.1. DescribeDDoSEvents 244
15.2. DescribePortFlowList 247
15.3. DescribePortConnsList 251

15.4. DescribePortConnsCount 255
15.5. DescribePortMaxConns 257
15.6. DescribePortAttackMaxFlow 260
15.7. DescribePortViewSourceCountries 262
15.8. DescribePortViewSourceIsps 264
15.9. DescribePortViewSourceProvinces 268
15.10. DescribeDomainAttackEvents 270
15.11. DescribeDomainQPSList 273
15.12. DescribeDomainStatusCodeList 276
15.13. DescribeDomainOverview 280
15.14. DescribeDomainStatusCodeCount 282
15.15. DescribeDomainTopAttackList 285
15.16. DescribeDomainViewSourceCountries 288
15.17. DescribeDomainViewSourceProvinces 290
15.18. DescribeDomainViewTopCostTime 292
15.19. DescribeDomainViewTopUrl 295
15.20. DescribeDomainQpsWithCache 297
16.全量日志分析 303
16.1. DescribeSlsOpenStatus 303
16.2. DescribeSlsAuthStatus 304
16.3. DescribeLogStoreExistStatus 305
16.4. DescribeSlsLogstoreInfo 307
16.5. ModifyFullLogTtl 309
16.6. DescribeWebAccessLogDispatchStatus 310
16.7. DescribeWebAccessLogStatus 312
16.8. EnableWebAccessLogConfig 314
16.9. DisableWebAccessLogConfig 316
16.10. DescribeWebAccessLogEmptyCount 317

16.11. EmptySlsLogstore 319
17.系统配置与日志 321
17.1. DescribeStsGrantStatus 321
17.2. DescribeBackSourceCidr 322
17.3. DescribeOpEntities 324
17.4. DescribeDefenseRecords 329
17.5. DescribeAsyncTasks 332
17.6. CreateAsyncTask 336
17.7. DeleteAsyncTask 338
18.标签 340
18.1. DescribeTagKeys 340
18.2. DescribeTagResources 343
18.3. CreateTagResources 346
18.4. DeleteTagResources 348
19.错误码 351
20.中国地区&国家和地域代码 352

1.API概览

本文档汇总了DDoS高防服务所有可调用的API，具体接口信息请参见相关文档。

> 说明 本文档所列举的接口适用于DDoS高防（新BGP）和DDoS高防（国际）服务。
>
> - 在使用以下接口前，请确认您已经开通了DDoS高防（新BGP）或者DDoS高防（国际）实例。更多信息，请参见开通DDoS高防（新BGP&国际）。
> - 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）或者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。

关于更多API资源，请访问API Explorer。

实例

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

接入管理

域名接入

API	描述
DescribeDomains	查询已配置网站业务转发规则的域名。

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

端口接入

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

流量调度器

API	描述
DescribeSchedulerRules	查询流量调度器的调度规则。

API	描述
CreateSchedulerRule	创建流量调度器调度规则。
ModifySchedulerRule	编辑流量调度器调度规则。
DeleteSchedulerRule	删除流量调度器调度规则。

防护设置

基础设施防护策略

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

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。

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

非网站业务防护策略

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

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

定制场景策略

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

监控报表

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

API	描述
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。
DescribeLogStoreExistStatus	查询是否已创建DDoS高防的日志库。
DescribeSlsLogstoreInfo	查询DDoS高防的日志库信息，例如日志存储容量、日志存储时长等。
ModifyFullLogTtl	编辑DDoS高防全量日志的存储时长。
DescribeWebAccessLogDispatchStatus	查询所有域名的全量日志开关状态。
DescribeWebAccessLogStatus	查询单个网站业务的全量日志服务信息，例如开关状态、对接的日志项目、日志库。
EnableWebAccessLogConfig	为网站业务开启全量日志分析。
DisableWebAccessLogConfig	为网站业务关闭全量日志分析。

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

标签

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

静态页面缓存

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

系统配置与日志

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

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

HTTP调用

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

其请求结构如下：

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

其中：

- Endpoint：DDoS高防API的服务接入地址，取值如下。
  - *ddoscoo.cn-hangzhou.aliyuncs.com*：DDoS高防（新BGP）
  - *ddoscoo.ap-southeast-1.aliyuncs.com*：DDoS高防（国际）服务
- Action：要执行的操作，如调用DescribeInstanceIds查询已创建的DDoS高防实例ID。
- Version：要使用的API版本，DDoS高防的API版本是*2020-01-01*。
- Parameters：请求参数，每个参数之间用“&”分隔。

  请求参数由公共请求参数和API自定义参数组成。公共参数中包含API版本号、身份验证等信息，详情请参见公共参数。

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 为了便于用户查看，本文档中的示例都做了格式化处理。

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

OpenAPI Explorer调用

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

您可以直接访问OpenAPI Explorer页面调用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=CT9X0VtwR86fNW
Snsc6v8YGOjuE%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

介绍每个接口都需要使用的请求参数和返回参数。

公共请求参数

名称	类型	是否必须	描述
RegionId	String	是	DDoS高防服务地域ID。取值： • *cn-hangzhou*：表示DDoS高防（新BGP）服务 • *ap-southeast-1*：表示DDoS高防（国际）服务
Format	String	否	返回消息的格式。取值： • *JSON*（默认值） • *XML*
Version	String	是	API版本号，使用YYYY-MM-DD日期格式。取值： *2020-01-01*
AccessKeyId	String	是	访问服务使用的密钥ID。
Signature	String	是	签名结果串。
SignatureMethod	String	是	签名方式，取值： *HMAC-SHA1*
Timestamp	String	是	请求的时间戳，为日期格式。使用UTC时间按照 ISO8601标准，格式为YYYY-MM-DDThh:mm:ssZ。 例如，北京时间2020年1月1日20点0分0秒，表示为2020-01-01T20:00:00Z。
SignatureVersion	String	是	签名算法版本，取值： *1.0*
SignatureNonce	String	是	唯一随机数，用于防止网络重放攻击。 在不同请求间要使用不同的随机数值。
ResourceOwnerAccount	String	否	本次API请求访问到的资源拥有者账户，即登录用户名。

示例

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

公共返回参数

API返回结果采用统一格式，调用成功返回的数据格式有XML和JSON两种，可以在发送请求时指定返回的数据格式，默认为JSON格式。每次接口调用，无论成功与否，系统都会返回一个唯一识别码RequestId。

- 返回 `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。

公共返回参数示例如下：

- XML格式

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

- JSON格式

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

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

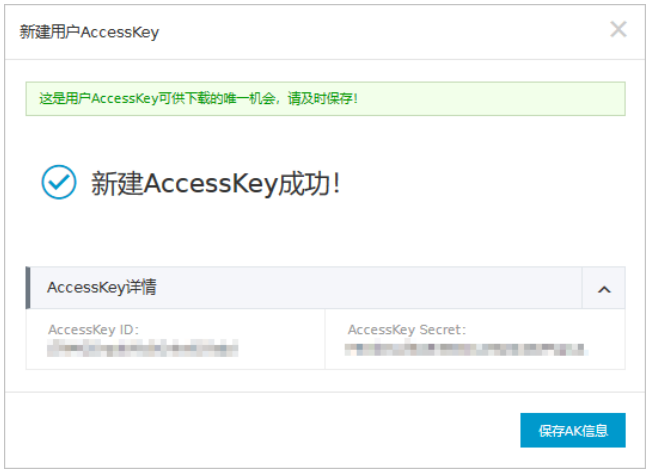
AccessKey包括AccessKey ID和AccessKey Secret。

- 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.实例

6.1. DescribeInstanceIds

调用DescribeInstanceIds查询DDoS高防实例的ID信息。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstanceIds	要执行的操作。取值：DescribeInstanceIds
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
Edition	Integer	否	9	DDoS高防实例的防护套餐类型。取值： • 0：DDoS高防（国际）保险版 • 1：DDoS高防（国际）无忧版 • 2：DDoS高防（国际）加速线路 • 9：DDoS高防（新BGP）专业版
InstanceIds.N	RepeatList	否	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。

返回数据

名称	类型	示例值	描述
InstanceIds	Array		DDoS高防实例的ID信息。

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

示例

请求示例

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

正常返回示例

`XML` 格式

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

`JSON` 格式

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


错误码

访问错误中心查看更多错误码。

6.2. DescribeInstances

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstances	要执行的操作。取值：DescribeInstances
PageNumber	String	是	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写1。
PageSize	String	是	10	页面显示的记录数量。最大值：50
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
InstanceIds.N	RepeatList	否	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
Ip	String	否	203.***.***.117	使用IP地址查询，指定要查询的DDoS高防实例的IP地址。支持精确匹配查询。
Remark	String	否	test	使用实例备注查询，指定要查询的DDoS高防实例的备注。支持模糊查询。
Edition	Integer	否	9	使用防护套餐查询，指定要查询的DDoS高防实例的防护套餐版本。取值： • 0：DDoS高防（国际）保险版 • 1：DDoS高防（国际）无忧版 • 2： DDoS高防（国际）加速线路 • 9：DDoS高防（新BGP）专业版
Enabled	Integer	否	1	使用业务转发状态查询，指定要查询的DDoS高防实例的业务转发状态。取值： • 0：已停止转发业务 • 1：正常转发业务
ExpireStartTime	Long	否	1584460800000	使用实例到期时间查询，指定要查询的DDoS高防实例的到期开始时间。时间戳格式，单位：毫秒。
ExpireEndTime	Long	否	1584560800000	使用实例到期时间查询，指定要查询的DDoS高防实例的到期结束时间。时间戳格式，单位：毫秒。
Status.N	RepeatList	否	1	使用实例的到期状态查询，指定要查询的DDoS高防实例的到期状态。取值： • 1：正常 • 2：到期

名称	类型	是否必选	示例值	描述
Tag.N.Key	String	否	testkey	使用实例标签查询，指定要查询的DDoS高防实例的标签键。 说明 标签键（Tag.N.Key）与标签值（Tag.N.Value）必须键值匹配。
Tag.N.Value	String	否	a	使用实例标签查询，指定要查询的DDoS高防实例的标签值。 说明 标签键（Tag.N.Key）与标签值（Tag.N.Value）必须键值匹配。

返回数据

名称	类型	示例值	描述
Instances	Array		DDoS高防实例的版本和状态信息。
CreateTime	Long	1581946582000	实例创建时间。时间戳格式，单位：毫秒。
DebtStatus	Integer	0	实例的欠费状态。取值固定为0，表示不欠费，因为DDoS高防服务目前只支持包年包月的预付费计费方式。
Edition	Integer	9	防护套餐版本。取值： • 0：DDoS高防（国际）保险版 • 1：DDoS高防（国际）无忧版 • 2： DDoS高防（国际）加速线路 • 9：DDoS高防（新BGP）专业版
Enabled	Integer	1	实例的业务转发状态。取值： • 0：已停止转发业务 • 1：正常转发业务

名称	类型	示例值	描述
ExpireTime	Long	1584460800000	实例到期时间。时间戳格式，单位：毫秒。
InstanceId	String	ddoscoo-cn-mp91j1ao****	实例ID。
Remark	String	test	实例备注。
Status	Integer	1	实例的到期状态。取值： • 1：正常 • 2：到期
RequestId	String	A09C1F98-4CC1-4A31-B8F3-9E4B7437189F	本次请求的ID。
TotalCount	Long	1	DDoS高防实例的总数。

示例

请求示例

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

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

访问错误中心查看更多错误码。

6.3. DescribeInstanceDetails

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

调试

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

请求参数

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

返回数据

名称	类型	示例值	描述
InstanceDetails	Array		DDoS高防实例的IP和线路信息。
EipInfos	Array		DDoS高防实例的IP信息。
Eip	String	203.***.**.117	DDoS高防实例的IP地址。
Status	String	normal	DDoS高防IP的状态。取值： • normal：正常 • cleaning：清洗中 • blackhole：黑洞中
InstanceId	String	ddoscoo-cn-mp91j1ao****	DDoS高防实例ID。

名称	类型	示例值	描述
Line	String	coop-line-001	DDoS高防实例的线路。例如，coop-line-001。
RequestId	String	3C814429-21A5-4673-827E-FDD19DC75681	本次请求的ID。

示例

请求示例

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

正常返回示例

`XML` 格式

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

`JSON` 格式

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


错误码

访问错误中心查看更多错误码。

6.4. DescribeInstanceSpecs

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstanceSpecs	要执行的操作。取值：DescribeInstanceSpecs
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	要查询的DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。

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
InstanceSpecs	Array		DDoS高防实例的规格信息。
BandwidthMbps	Integer	100	正常业务带宽，单位：Mbps。
BaseBandwidth	Integer	30	基础防护带宽，单位：Gbps。
DefenseCount	Integer	1	本月可用高级防护次数。-1表示无限次，即实例的防护套餐类型为无忧版。 说明 只有DDoS高防（国际）实例拥有该属性。
DomainLimit	Integer	50	可防护的域名数量。
ElasticBandwidth	Integer	30	弹性防护带宽，单位：Gbps。
FunctionVersion	String	default	功能套餐类型。取值： • default：标准功能 • enhance：增强功能
InstanceId	String	ddoscoo-cn-mp91j1ao****	DDoS高防实例ID。
PortLimit	Integer	50	可防护的端口数量。
QpsLimit	Integer	3000	正常业务QPS。
SiteLimit	Integer	5	可防护的站点数量。

名称	类型	示例值	描述
RequestId	String	23B0245A-0CCC-4637-A8C6-7CA0479395B2	本次请求的ID。

示例

请求示例

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

正常返回示例

`XML` 格式

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

`JSON` 格式

```
{
"RequestId": "23B0245A-0CCC-4637-A8C6-7CA0479395B2",
"InstanceSpecs": [
{
"QpsLimit": 3000,
"BaseBandwidth": 30,
"PortLimit": 50,
"InstanceId": "ddoscoo-cn-mp91j1ao****",
"DomainLimit": 50,
"FunctionVersion": "default",
"ElasticBandwidth": 30,
"SiteLimit": 5,
"BandwidthMbps": 100
}
]
}
```


错误码

访问错误中心查看更多错误码。

6.5. DescribeInstanceStatistics

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstanceStatistics	要执行的操作。取值：DescribeInstanceStatistics
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	要查询的DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。

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
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。

6.6. ModifyInstanceRemark

调用ModifyInstanceRemark编辑DDoS高防实例的备注。

调试

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

请求参数

名称	类型	是否必选	示例值	描述

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

返回数据

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

示例

请求示例

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

正常返回示例

XML 格式

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

JSON 格式

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

错误码

访问错误中心查看更多错误码。

6.7. DescribeElasticBandwidthSpec

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

> 说明 该接口仅适用于DDoS高防（新BGP）服务。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeElasticBandwidthSpec	要执行的操作。取值：DescribeElasticBandwidthSpec
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值：cn-hangzhou，表示DDoS高防（新BGP）服务。

返回数据

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

示例

请求示例

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

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

访问错误中心查看更多错误码。

6.8. ModifyElasticBandWidth

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

> 说明 该接口仅适用于DDoS高防（新BGP）服务。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyElasticBandWidth	要执行的操作。取值：ModifyElasticBandWidth
ElasticBandwidth	Integer	是	50	要设置的弹性防护带宽，单位：Gbps。 说明 您可以调用DescribeElasticBandwidthSpec查询可选的弹性防护带宽规格。
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。

6.9. DescribeDefenseCountStatistics

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

> **说明** 该接口仅适用于DDoS高防（国际）服务。

调试

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

请求参数

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

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

返回数据

名称	类型	示例值	描述
DefenseCountStatistics	Struct		防护次数统计信息。
DefenseCountTotalUsageOfCurrentMonth	Integer	1	本月已用的高级防护次数。
FlowPackCountRemain	Integer	1	剩余可用的全局高级防护次数。 说明 全局高级防护仅在有效的DDoS高防（国际）保险版实例中的免费高级防护次数耗尽之后生效。
MaxUsableDefenseCountCurrentMonth	Integer	2	本月最大可消耗的高级防护次数。 说明 仅对DDoS高防（国际）保险版实例有效，包含每月免费的高级防护次数和单独购买的全局高级防护次数。
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。

示例

请求示例

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

正常返回示例

XML 格式

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

JSON 格式

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

错误码

访问错误中心查看更多错误码。

6.10. 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。
RegionId	String	否	cn-hangzhou	DDoS高防服务的地域ID。取值： • cn-hangzhou：中国内地地域，表示DDoS高防（新BGP）服务 • ap-southeast-1：非中国内地地域，表示DDoS高防（国际）服务
InstanceId	String	否	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。

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。

7.域名接入

7.1. DescribeDomains

调用DescribeDomains查询已配置网站业务转发规则的域名。

调试

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

请求参数

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

返回数据

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

示例

请求示例

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

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

访问错误中心查看更多错误码。

7.2. DescribeWebRules

调用DescribeWebRules查询网站业务转发规则。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeWebRules	要执行的操作。取值：DescribeWebRules
PageSize	Integer	是	10	页面显示的记录数量。最大值：10

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

返回数据

名称	类型	示例值	描述
RequestId	String	89E69DD6-C5DD-4636-9AD6-CCF6BEAB59AC	本次请求的ID。
TotalCount	Long	1	返回的网站业务转发规则总数。
WebRules	Array		网站业务转发规则信息。

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

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

示例

请求示例

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

正常返回示例

`XML` 格式

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

`JSON` 格式

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


错误码

访问错误中心查看更多错误码。

7.3. CreateWebRule

调用CreateWebRule创建网站业务转发规则。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateWebRule	要执行的操作。取值：CreateWebRule
Domain	String	是	www.aliyun.com	网站业务的域名。
RsType	Integer	是	0	服务器地址类型。取值： • 0：源站IP • 1：源站域名

Rules	String	是	[{"ProxyRules":[{"ProxyPort":80,"RealServers":["1.1.1.1"]}],"ProxyType":"http"},{"ProxyRules":[{"ProxyPort":443,"RealServers":["1.1.1.1"]}],"ProxyType":"https"}]	网站业务转发规则的详细信息。使用JSON格式的字符串表达，具体结构如下。
				• ProxyRules：Array类型，必选，协议信息。具体结构如下。
				  ◦ ProxyPort：Integer类型，必选，端口号。
				  ◦ RealServers：Array类型，必选，服务器地址。
				• ProxyType：String类型，必选，协议类型。取值：
				  ◦ http
				  ◦ https
				  ◦ websocket
				  ◦ websockets

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
InstanceIds.N	RepeatList	否	ddoscoo-cn-mp91j1ao****	要关联的DDoS高防实例的ID。不传入该参数表示只添加域名，不关联高防实例。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。

返回数据

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

示例

请求示例

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

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

访问错误中心查看更多错误码。

7.4. ModifyWebRule

调用ModifyWebRule编辑网站业务转发规则。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyWebRule	要执行的操作。取值：ModifyWebRule
Domain	String	是	www.aliyun.com	网站业务的域名。 说明 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

ProxyTypes	String	是	[{"ProxyType":"http","ProxyPorts":[80]},{"ProxyType":"https","ProxyPorts":[443]}]	网站业务转发规则的协议信息。使用JSON格式的字符串表达，具体结构如下。
				• ProxyType：String类型，必选，协议类型。取值：
				  ○ http
				  ○ https
				  ○ websocket
				  ○ websockets
				• ProxyPort：Integer类型，必选，端口号。

RealServers.N	RepeatList	是	1.1.1.1	服务器地址列表。
RsType	Integer	是	0	服务器地址类型。取值： • 0：源站IP • 1：源站域名

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

返回数据

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

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyWebRule
&Domain=www.aliyun.com
&ProxyTypes=[{"ProxyType":"http","ProxyPorts":[80]},{"ProxyType":"https","ProxyPorts":[443]}]
&RealServers.1=1.1.1.1
&RsType=0
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

JSON 格式

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

错误码

访问错误中心查看更多错误码。

7.5. DeleteWebRule

调用DeleteWebRule删除网站业务转发规则。

调试

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

请求参数

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

返回数据

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

示例

请求示例

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

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

访问错误中心查看更多错误码。

7.6. DescribeWebInstanceRelations

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述

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

返回数据

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

7.7. DescribeCerts

调用DescribeCerts查询网站业务的证书信息。

调试

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

请求参数

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

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。
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。

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=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。

7.8. AssociateWebCert

调用AssociateWebCert为网站业务转发规则关联SSL证书。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	AssociateWebCert	要执行的操作。取值：AssociateWebCert
Domain	String	是	www.aliyun.com	网站业务的域名。 说明 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

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

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

7.9. DescribeWebCustomPorts

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述

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。

7.10. ModifyTlsConfig

调用ModifyTlsConfig编辑网站业务转发规则的TLS安全策略。

调试

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

请求参数

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

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

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。

7.11. ModifyHttp2Enable

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

> 说明 该接口仅适用于DDoS高防（新BGP）服务。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	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。

7.12. DescribeWebAccessMode

调用DescribeWebAccessMode查询网站业务的接入模式。

调试

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

请求参数

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

返回数据

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

示例

请求示例

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

正常返回示例

`XML` 格式

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

`JSON` 格式

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


错误码

访问错误中心查看更多错误码。

7.13. ModifyWebAccessMode

调用ModifyWebAccessMode设置网站业务的接入模式。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyWebAccessMode	要执行的操作。取值：ModifyWebAccessMode
AccessMode	Integer	是	2	网站业务的接入模式。取值： • 0：A记录 • 1：高防模式 • 2：回源模式
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

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。

7.14. DescribeCnameReuses

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

> **说明** 该接口仅适用于DDoS高防（国际）服务。

调试

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

请求参数

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

返回数据

名称	类型	示例值	描述
CnameReuses	Array		CNAME复用信息。
Cname	String	4o6ep6q217k9****.aliyunddos0004.com	复用的CNAME值。
Domain	String	www.aliyun.com	网站域名。
Enable	Integer	1	是否已开启CNAME复用。取值： • 0：未开启 • 1：已开启

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=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。

7.15. ModifyCnameReuse

调用ModifyCnameReuse为网站业务开启或关闭CNAME复用。

> 说明 该接口仅适用于DDoS高防（国际）服务。

调试

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

请求参数

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

8.1. DescribeNetworkRules

调用DescribeNetworkRules查询端口转发规则。

调试

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

请求参数

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

返回数据

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

示例

请求示例

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

正常返回示例

`XML` 格式

```
<DescribeNetworkRulesResponse>
<TotalCount>2</TotalCount>
<NetworkRules>
<IsAutoCreate>true</IsAutoCreate>
<InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
<BackendPort>80</BackendPort>
<RealServers>112.***.***.139</RealServers>
<FrontendPort>80</FrontendPort>
<Protocol>tcp</Protocol>
</NetworkRules>
<NetworkRules>
<IsAutoCreate>false</IsAutoCreate>
<InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
<BackendPort>8080</BackendPort>
<RealServers>1.1.1.1</RealServers>
<RealServers>2.2.2.2</RealServers>
<RealServers>3.3.3.3</RealServers>
<FrontendPort>8080</FrontendPort>
<Protocol>tcp</Protocol>
</NetworkRules>
<RequestId>8597F235-FA5E-4FC7-BAD9-E4C0B01BC771</RequestId>
</DescribeNetworkRulesResponse>
```

`JSON` 格式

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


错误码

访问错误中心查看更多错误码。

8.2. CreateNetworkRules

调用CreateNetworkRules创建端口转发规则。

调试

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

请求参数

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

返回数据

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

示例

请求示例

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

正常返回示例

`XML` 格式

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

JSON 格式

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

错误码

访问错误中心查看更多错误码。

8.3. ConfigNetworkRules

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

调试

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

请求参数

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

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

返回数据

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

示例

请求示例

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

正常返回示例

`XML` 格式

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

JSON 格式

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

错误码

访问错误中心查看更多错误码。

8.4. DeleteNetworkRule

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

调试

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

请求参数

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

8.5. DescribeHealthCheckList

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述

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

返回数据

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

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

示例

请求示例

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

正常返回示例

XML 格式

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

`JSON` 格式

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

错误码

访问错误中心查看更多错误码。

8.6. ModifyHealthCheckConfig

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyHealthCheckConfig	要执行的操作。取值：ModifyHealthCheckConfig
ForwardProtocol	String	是	tcp	转发协议。取值： • tcp • udp
FrontendPort	Integer	是	8080	转发端口。

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

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。

8.7. DescribeHealthCheckStatus

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

调试

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

请求参数

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

返回数据

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

名称	类型	示例值	描述
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.流量调度器

9.1. DescribeSchedulerRules

调用DescribeSchedulerRules查询流量调度器的调度规则。

调试

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

请求参数

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

返回数据

名称	类型	示例值	描述
RequestId	String	11C55595-1757-4B17-9ACE-4ACB68C2D989	本次请求的ID。
SchedulerRules	Array of SchedulerRule		流量调度规则信息。

名称	类型	示例值	描述
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。
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

名称	类型	示例值	描述
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。

9.2. CreateSchedulerRule

调用CreateSchedulerRule创建流量调度器调度规则。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateSchedulerRule	要执行的操作。取值：CreateSchedulerRule
RuleName	String	是	testrule	规则名称。

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

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。

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。

9.3. ModifySchedulerRule

调用ModifySchedulerRule编辑流量调度器调度规则。

调试

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

请求参数

名称	类型	是否必选	示例值	描述

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。

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。

9.4. DeleteSchedulerRule

调用DeleteSchedulerRule删除流量调度器调度规则。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteSchedulerRule	要执行的操作。取值：DeleteSchedulerRule
RuleName	String	是	testrule	要删除的规则名称。
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=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。

10.基础设施防护策略

10.1. DescribeAutoCcListCount

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

调试

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

请求参数

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

返回数据

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

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

示例

请求示例

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

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

访问错误中心查看更多错误码。

10.2. DescribeAutoCcBlacklist

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

调试

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

请求参数

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

返回数据

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

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

示例

请求示例

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

正常返回示例

`XML` 格式

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

JSON 格式


```
{
"TotalCount": 2,
"RequestId": "E78C8472-0B15-42D5-AF22-A32A78818AB2",
"AutoCcBlacklist": [
{
"Type": "manual",
"SourceIp": "1.1.1.1",
"EndTime": "1584093569",
"DestIp": "203.***.***.132"
},
{
"Type": "manual",
"SourceIp": "2.2.2.2",
"EndTime": "1584093569",
"DestIp": "203.***.***.132"
}
]
}
```


错误码

访问错误中心查看更多错误码。

10.3. AddAutoCcBlacklist

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	AddAutoCcBlacklist	要执行的操作。取值：AddAutoCcBlacklist
Blacklist	String	是	[{"src":"1.1.1.1"},{"src":"2.2.2.2"}]	黑名单IP的详细信息，使用JSON格式的字符串表述，具体结构如下。 • src：String类型，必选，黑名单IP。

名称	类型	是否必选	示例值	描述
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。

10.4. DeleteAutoCcBlacklist

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteAutoCcBlacklist	要执行的操作。取值：DeleteAutoCcBlacklist
Blacklist	String	是	[{"src":"1.1.1.1"},{"src":"2.2.2.2"}]	黑名单IP的详细信息，使用JSON格式的字符串表述，具体结构如下。 • src：String类型，必选，黑名单IP。
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。

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

返回数据

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

示例

请求示例

```
http(s)://[Endpoint]/?Action=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。

10.5. EmptyAutoCcBlacklist

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	EmptyAutoCcBlacklist	要执行的操作。取值：EmptyAutoCcBlacklist
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
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。

10.6. DescribeAutoCcWhitelist

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeAutoCcWhitelist	要执行的操作。取值：DescribeAutoCcWhitelist
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
PageNumber	Integer	是	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写1。
PageSize	Integer	是	10	页面显示的记录数量。

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
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。

10.7. AddAutoCcWhitelist

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	AddAutoCcWhitelist	要执行的操作。取值：AddAutoCcWhitelist
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。

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

返回数据

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

示例

请求示例

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

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

访问错误中心查看更多错误码。

10.8. DeleteAutoCcWhitelist

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

调试

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

请求参数

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

返回数据

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

示例

请求示例

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

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

访问错误中心查看更多错误码。

10.9. EmptyAutoCcWhitelist

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	EmptyAutoCcWhitelist	要执行的操作。取值：EmptyAutoCcWhitelist
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。

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

返回数据

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

示例

请求示例

```
http(s)://[Endpoint]/?Action=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。

10.10. DescribeUnBlackholeCount

调用DescribeUnBlackholeCount查询黑洞解封次数。

调试

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

请求参数

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

返回数据

名称	类型	示例值	描述
RemainCount	Integer	5	剩余的黑洞解封次数。
RequestId	String	232929FA-40B6-4C53-9476-EE335ABA44CD	本次请求的ID。
TotalCount	Integer	5	黑洞解封总次数。

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribeUnBlackholeCountResponse>
<TotalCount>5</TotalCount>
<RequestId>232929FA-40B6-4C53-9476-EE335ABA44CD</RequestId>
<RemainCount>5</RemainCount>
</DescribeUnBlackholeCountResponse>
```

JSON 格式

```
{
"TotalCount": 5,
"RequestId": "232929FA-40B6-4C53-9476-EE335ABA44CD",
"RemainCount": 5
}
```

错误码

访问错误中心查看更多错误码。

10.11. DescribeBlackholeStatus

调用DescribeBlackholeStatus查询DDoS高防实例的黑洞状态。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeBlackholeStatus	要执行的操作。取值：DescribeBlackholeStatus
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。

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
BlackholeStatus	Array		DDoS高防实例的黑洞状态信息。
BlackStatus	String	blackhole	黑洞状态。取值： • blackhole：黑洞中 • normal：正常
EndTime	Long	1540196323	黑洞结束时间。时间戳格式，单位：秒。
Ip	String	203.***.***.132	DDoS高防实例的IP。
StartTime	Long	1540195323	黑洞开始时间。时间戳格式，单位：秒。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

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

正常返回示例

`XML` 格式

```
<DescribeBlackholeStatusResponse>
<RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
<BlackholeStatus>
<Ip>203.***.***.132</Ip>
<BlackStatus>blackhole</BlackStatus>
<StartTime>1540195323</StartTime>
<EndTime>1540196323</EndTime>
</BlackholeStatus>
</DescribeBlackholeStatusResponse>
```

JSON 格式

```
{
"RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
"BlackholeStatus": [
{
"Ip": "203.***.***.132",
"BlackStatus": "blackhole",
"StartTime": 1540195323,
"EndTime": 1540196323
}
]
}
```

错误码

访问错误中心查看更多错误码。

10.12. ModifyBlackholeStatus

调用ModifyBlackholeStatus执行黑洞解封。

调试

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

请求参数

名称	类型	是否必选	示例值	描述

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。

10.13. DescribeNetworkRegionBlock

调用DescribeNetworkRegionBlock查询针对DDoS高防实例的区域封禁配置。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeNetworkRegionBlock	要执行的操作。取值：DescribeNetworkRegionBlock。
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
Config	Struct		区域封禁的配置信息。
Countries	List	[1,2]	被封禁的海外地区代码列表。 说明 关于海外地区代码的详细信息，请参见中国和海外地区代码中的海外地区代码说明。 例如，[1,2] 表示中国和澳大利亚。
Provinces	List	[11,12]	被封禁的中国地区代码列表。 说明 关于中国地区代码的详细信息，请参见中国和海外地区代码中的中国地区代码说明。 例如，[11,12] 表示北京市和天津市。
RegionBlockSwitch	String	on	区域封禁的开关状态。取值： • on：开启 • off：关闭
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribeNetworkRegionBlockResponse>
<RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
<Config>
<RegionBlockSwitch>off</RegionBlockSwitch>
<Countries>1</Countries>
<Countries>2</Countries>
<Provinces>11</Provinces>
<Provinces>12</Provinces>
</Config>
</DescribeNetworkRegionBlockResponse>
```

`JSON` 格式

```
{
"RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
"Config": {
"RegionBlockSwitch": "off",
"Countries": [
1,
2
],
"Provinces": [
11,
12
]
}
}
```

错误码

访问错误中心查看更多错误码。

10.14. ConfigNetworkRegionBlock

调用ConfigNetworkRegionBlock设置针对DDoS高防实例的区域封禁。

调试

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

请求参数

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

Config	String	是	{"RegionBlockSwitch":"off","Countries":[],"Provinces":[11,12,13,14,15,21,22,23,31,32,33,34,35,36,37,41,42,43,44,45,46,50,51,52,53,54,61,62,63,64,65,71,81,82]}	区域封禁的配置信息，使用JSON格式的字符串表述，具体结构如下。
				• RegionBlockSwitch：String类型，必选，区域封禁的开关状态。取值：
				  ○ on：开启
				  ○ off：关闭
				• Countries：Array类型，可选，要封禁的海外地区代码列表。
				说明 关于海外地区代码的详细信息，请参见中国和海外地区代码中的海外地区代码说明。
				例如，[1,2]表示中国和澳大利亚。
				• Provinces：Array类型，可选，要封禁的中国地区代码列表。
				说明 关于中国地区代码的详细信息，请参见中国和海外地区代码中的中国地区代码说明。
				例如，[11,12]表示北京市和天津市。

InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务

返回数据

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

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigNetworkRegionBlock
&Config={"RegionBlockSwitch":"off","Countries":[],"Provinces":[11,12,13,14,15,21,22,23,31,32,33,34,35,36,
37,41,42,43,44,45,46,50,51,52,53,54,61,62,63,64,65,71,81,82]}
&InstanceId=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

访问错误中心查看更多错误码。

10.15. DescribeBlockStatus

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

> 说明 该接口仅适用于DDoS高防（新BGP）服务。

调试

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

请求参数

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

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
StatusList	Array		DDoS高防实例的近源流量压制配置。
BlockStatusList	Array		近源流量压制配置。
BlockStatus	String	areablock	流量封禁状态。取值： • areablock：封禁中 • normal：正常
EndTime	Long	1540196323	封禁结束时间。时间戳格式，单位：秒。
Line	String	cut	封禁区域。取值： • ct：电信海外 • cut：联通海外
StartTime	Long	1540195323	封禁开始时间。时间戳格式，单位：秒。

名称	类型	示例值	描述
Ip	String	203.***.***.88	DDoS高防实例的IP。

示例

请求示例

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

正常返回示例

`XML` 格式

```
<DescribeBlockStatusResponse>
<RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
<StatusList>
<Ip>203.***.***.88</Ip>
<BlockStatusList>
<BlockStatus>areablock</BlockStatus>
<Line>cut</Line>
<StartTime>1540195323</StartTime>
<EndTime>1540196323</EndTime>
</BlockStatusList>
</StatusList>
</DescribeBlockStatusResponse>
```

`JSON` 格式

```
{
"RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
"StatusList": [
{
"Ip": "203.***.***.88",
"BlockStatusList": [
{
"BlockStatus": "areablock",
"Line": "cut",
"StartTime": 1540195323,
"EndTime": 1540196323
}
]
}
]
}
```


错误码

访问错误中心查看更多错误码。

10.16. ModifyBlockStatus

调用ModifyBlockStatus设置DDoS高防（新BGP）实例的近源流量压制。

> 说明 该接口仅适用于DDoS高防（新BGP）服务。

调试

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

请求参数

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

名称	类型	是否必选	示例值	描述
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
Status	String	是	do	近源流量压制的状态。取值： • do：开启流量压制 • undo：解除流量压制
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值：cn-hangzhou，表示DDoS高防（新BGP）服务。
Duration	Integer	否	10	封禁时间。取值范围：5~43200，单位：分钟。 说明 Status为do时必须传入该参数。
Lines.N	RepeatList	否	ct	封禁线路。取值： • ct：电信海外 • cut：联通海外

返回数据

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

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyBlockStatus
&InstanceId=ddoscoo-cn-mp91j1ao****
&Status=do
&Duration=10
&<公共请求参数>
```

正常返回示例

XML 格式

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

JSON 格式

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

错误码

访问错误中心查看更多错误码。

10.17. DescribeUnBlockCount

调用DescribeUnBlockCount查询可用的近源流量压制次数。

> 说明 该接口仅适用于DDoS高防（新BGP）服务。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeUnBlockCount	要执行的操作。取值：DescribeUnBlockCount
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值：cn-hangzhou，表示DDoS高防（新BGP）服务。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
RemainCount	Integer	7	剩余可用的近源流量压制次数。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
TotalCount	Integer	10	总共可用的近源流量压制次数。

示例

请求示例

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

正常返回示例

`XML` 格式

```
<DescribeUnBlockCountResponse>
<RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
<TotalCount>10</TotalCount>
<RemainCount>7</RemainCount>
</DescribeUnBlockCountResponse>
```

`JSON` 格式

```
{
"RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
"TotalCount": 10,
"RemainCount": 7
}
```

错误码

访问错误中心查看更多错误码。

11.网站业务防护策略

11.1. DescribeWebCcProtectSwitch

调用DescribeWebCcProtectSwitch查询网站业务各防护功能的开关状态。

调试

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

请求参数

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

名称	类型	示例值	描述
AiRuleEnable	Integer	1	AI智能防护的开关状态。取值： • 0：关闭 • 1：开启
AiTemplate	String	level60	AI智能防护的等级。取值： • level30：宽松 • level60：正常 • level90：严格
BlackWhiteList Enable	Integer	1	黑白名单（针对域名）的开关状态。取值： • 0：关闭 • 1：开启
CcCustomRule Enable	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。
PreciseRuleEn able	Integer	0	精确访问控制的开关状态。取值： • 0：关闭 • 1：开启
RegionBlockEn able	Integer	0	区域封禁（针对域名）的开关状态。取值： • 0：关闭 • 1：开启

名称	类型	示例值	描述
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。

11.2. ModifyWebAIProtectSwitch

调用ModifyWebAIProtectSwitch设置网站业务AI智能防护的开关状态。

调试

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

请求参数

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

名称	类型	是否必选	示例值	描述
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。

11.3. ModifyWebAIProtectMode

调用ModifyWebAIProtectMode设置网站业务AI智能防护的模式。

调试

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

请求参数

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

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

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=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。

11.4. ModifyWebIpSetSwitch

调用ModifyWebIpSetSwitch设置网站业务黑白名单（针对域名）的开关状态。

调试

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

请求参数

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

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

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=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。

11.5. ConfigWebIpSet

调用ConfigWebIpSet设置针对网站业务的黑名单和白名单IP。

调试

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

请求参数

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

11.6. EnableWebCC

调用EnableWebCC开启网站业务频率控制防护（CC防护）的开关。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	EnableWebCC	要执行的操作。取值：EnableWebCC
Domain	String	是	www.aliyun.com	网站业务的域名。 说明 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

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=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。

11.7. DisableWebCC

调用DisableWebCC关闭网站业务频率控制防护（CC防护）的开关。

调试

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

请求参数

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

11.8. ConfigWebCCTemplate

调用ConfigWebCCTemplate设置网站业务频率控制防护（CC防护）的防护模式。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ConfigWebCCTemplate	要执行的操作。取值：ConfigWebCCTemplate
Domain	String	是	www.aliyun.com	网站业务的域名。 说明 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

名称	类型	是否必选	示例值	描述
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。

11.9. EnableWebCCRule

调用EnableWebCCRule开启网站业务频率控制防护（CC防护）的自定义规则开关。

调试

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

请求参数

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

返回数据

名称	类型	示例值	描述

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。

11.10. DisableWebCCRule

调用DisableWebCCRule关闭网站业务频率控制防护（CC防护）的自定义规则开关。

调试

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

请求参数

名称	类型	是否必选	示例值	描述

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。

11.11. DescribeWebCCRules

调用DescribeWebCCRules查询网站业务频率控制防护（CC防护）的自定义规则。

调试

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

请求参数

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

名称	类型	是否必选	示例值	描述
PageNumber	Integer	否	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写1。

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。

11.12. CreateWebCCRule

调用CreateWebCCRule创建网站业务频率控制防护（CC防护）的自定义规则。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateWebCCRule	要执行的操作。取值：CreateWebCCRule
Act	String	是	close	阻断类型。取值： • close：封禁 • captcha：人机识别
Count	Integer	是	60	单一IP访问次数。取值范围：2~2000。
Domain	String	是	www.aliyun.com	网站业务的域名。 说明 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
Interval	Integer	是	20	检测时长。取值范围：5~10800，单位：秒。
Mode	String	是	prefix	匹配模式。取值： • prefix：前缀匹配 • match：完全匹配 说明 检测路径URI中包含参数时，请选择前缀匹配。

名称	类型	是否必选	示例值	描述
Name	String	是	testrule	规则名称。允许使用英文字母、数字或下划线（_），长度不能超过128个字符
Ttl	Integer	是	10	封禁时长。取值范围：1~1440，单位：分钟。
Uri	String	是	/abc/a.php	检测路径。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

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

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateWebCCRule
&Act=close
&Count=60
&Domain=www.aliyun.com
&Interval=20
&Mode=prefix
&Name=testrule
&Ttl=10
&Uri=/abc/a.php
&<公共请求参数>
```

正常返回示例

XML 格式

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

JSON 格式

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

错误码

访问错误中心查看更多错误码。

11.13. ModifyWebCCRule

调用ModifyWebCCRule编辑网站业务频率控制防护（CC防护）的自定义规则。

调试

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

请求参数

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

名称	类型	是否必选	示例值	描述
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。

11.14. DeleteWebCCRule

调用DeleteWebCCRule删除网站业务频率控制防护（CC防护）的自定义规则。

调试

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

请求参数

名称	类型	是否必选	示例值	描述

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteWebCCRule	要执行的操作。取值：DeleteWebCCRule
Domain	String	是	www.aliyun.com	网站业务的域名。 说明 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
Name	String	是	wq	要删除的自定义频率控制（CC防护）规则的名称。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

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

示例

请求示例

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

正常返回示例

XML 格式

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

JSON 格式

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

错误码

访问错误中心查看更多错误码。

11.15. ModifyWebPreciseAccessSwitch

调用ModifyWebPreciseAccessSwitch设置网站业务精确访问控制的开关状态。

调试

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

请求参数

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

Config	String	是	{"PreciseRuleEnable":0}	精确访问控制的开关状态配置，使用JSON格式的字符串表述，具体结构如下。
				• PreciseRuleEnable：Integer类型，必选，精确访问控制的开关状态。取值：
				  ○ 0：关闭
				  ○ 1：开启

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

返回数据

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

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyWebPreciseAccessSwitch
&Config={"PreciseRuleEnable":0}
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

访问错误中心查看更多错误码。

11.16. DescribeWebPreciseAccessRule

调用DescribeWebPreciseAccessRule查询网站业务精确访问控制规则。

调试

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

请求参数

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

返回数据

名称	类型	示例值	描述
PreciseAccessConfigList	Array		网站业务精确访问控制规则。

名称	类型	示例值	描述
Domain	String	www.aliyun.com	网站域名。
RuleList	Array		规则列表。
Action	String	accept	匹配动作。取值： • accept：放行 • block：封禁 • challenge：挑战
ConditionList	Array		匹配条件列表。
Content	String	1.1.1.1	匹配内容。
Field	String	ip	匹配字段。
HeaderName	String	null	自定义HTTP头部字段名称。 说明 仅在Field为header时有效。
MatchMethod	String	belong	逻辑符。
Expires	Long	0	规则有效期。单位：秒。规则的匹配动作为阻断时（action为block）生效，在规则有效期内阻断访问请求。0表示永久生效。
Name	String	testrule	规则名称。
Owner	String	manual	规则来源。取值： • manual：手动添加（默认） • auto：自动生成
RequestId	String	209EEFBF-B0C7-441E-8C28-D0945A57A638	本次请求的ID。

示例

请求示例

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

正常返回示例

`XML` 格式

```
<DescribeWebPreciseAccessRuleResponse>
<PreciseAccessConfigList>
<RuleList>
<Owner>manual</Owner>
<Action>accept</Action>
<ConditionList>
<MatchMethod>belong</MatchMethod>
<Field>ip</Field>
<HeaderName></HeaderName>
<Content>1.***.***.2</Content>
</ConditionList>
<Expires>0</Expires>
<Name>testrule</Name>
</RuleList>
<Domain>www.aliyun.com</Domain>
</PreciseAccessConfigList>
<RequestId>209EEFBF-B0C7-441E-8C28-D0945A57A638</RequestId>
</DescribeWebPreciseAccessRuleResponse>
```

`JSON` 格式

```
{
"PreciseAccessConfigList": [
{
"RuleList": [
{
"Owner": "manual",
"Action": "accept",
"ConditionList": [
{
"MatchMethod": "belong",
"Field": "ip",
"HeaderName": "",
"Content": "1.***.***.2"
}
],
"Expires": 0,
"Name": "testrule"
}
],
"Domain": "www.aliyun.com"
}
],
"RequestId": "209EEFBF-B0C7-441E-8C28-D0945A57A638"
}
```


错误码

访问错误中心查看更多错误码。

11.17. ModifyWebPreciseAccessRule

调用ModifyWebPreciseAccessRule编辑网站业务精确访问控制规则。

调试

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

请求参数

名称	类型	是否必选	示例值	描述

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

匹配字段（field）	描述	适用的逻辑符（match_method）
referer	访问请求的来源网址，即该访问请求是从哪个页面跳转产生的。	contain：包含 ncontain：不包含 equal：等于 nequal：不等于 lless：长度小于 lequal：长度等于 lgreat：长度大于 nexist：不存在 regular：正则匹配
user-agent	发起访问请求的客户端的浏览器标识、渲染引擎标识和版本信息等浏览器相关信息。	contain：包含 ncontain：不包含 equal：等于 nequal：不等于 lless：长度小于 lequal：长度等于 lgreat：长度大于 regular：正则匹配

params	访问请求的URL地址中的参数部分，通常指URL中”?”后面的部分。例如，
	`www.abc.com/index.html?action=login`
	中的
	`action=login`
	就是参数部分。
		contain：包含
		ncontain：不包含
		equal：等于
		nequal：不等于
		lless：长度小于
		lequal：长度等于
		lgreat：长度大于

匹配字段（field）	描述	适用的逻辑符（match_method）
cookie	访问请求中的Cookie信息。	contain：包含 ncontain：不包含 equal：等于 nequal：不等于 lless：长度小于 lequal：长度等于 lgreat：长度大于 nexist：不存在
content-type	访问请求指定的响应HTTP内容类型，即MIME类型信息。	contain：包含 ncontain：不包含 equal：等于 nequal：不等于 lless：长度小于 lequal：长度等于 lgreat：长度大于
x-forwarded-for	访问请求的客户端真实IP。X-Forwarded-For（XFF）用来识别通过HTTP代理或负载均衡方式转发的访问请求的客户端最原始的IP地址的HTTP请求头字段，只有通过HTTP代理或者负载均衡服务器转发的访问请求才会包含该项。	contain：包含 ncontain：不包含 equal：等于 nequal：不等于 lless：长度小于 lequal：长度等于 lgreat：长度大于 nexist：不存在 regular：正则匹配
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

匹配字段（field）	描述	适用的逻辑符（match_method）
post-body	访问请求的内容信息。	contain：包含 ncontain：不包含 equal：等于 nequal：不等于 regular：正则匹配
http-method	访问请求的方法，如GET、POST等。	equal：等于 nequal：不等于
header	访问请求的头部信息，用于自定义HTTP头部字段。	contain：包含 ncontain：不包含 equal：等于 nequal：不等于 lless：长度小于 lequal：长度等于 lgreat：长度大于 nexist：不存在

返回数据

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

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyWebPreciseAccessRule
&Domain=www.aliyun.com
&Rules=[{"action":"block","name":"testrule","condition":[{"field":"uri","match_method":"contain","content":"/test/123"}]}]
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

JSON 格式

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

错误码

访问错误中心查看更多错误码。

11.18. DeleteWebPreciseAccessRule

调用DeleteWebPreciseAccessRule删除网站业务精确访问控制规则。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteWebPreciseAccessRule	要执行的操作。取值：DeleteWebPreciseAccessRule
Domain	String	是	www.aliyun.com	网站业务的域名。 说明 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。
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

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=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。

11.19. ModifyWebAreaBlockSwitch

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

调试

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

请求参数

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

Config	String	是	{"RegionblockEnable": 1}	区域封禁（针对域名）的开关状态，使用JSON格式的字符串表述，具体结构如下。
				• RegionblockEnable：Integer类型，必选，区域封禁（针对域名）的开关状态。取值：
				  ○ 1：开启
				  ○ 0：关闭

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

返回数据

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

示例

请求示例

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

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

访问错误中心查看更多错误码。

11.20. DescribeWebAreaBlockConfigs

调用DescribeWebAreaBlockConfigs查询网站业务区域封禁（针对域名）的配置信息。

调试

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

请求参数

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

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
AreaBlockConfigs	Array		区域封禁（针对域名）的配置信息。
Domain	String	www.aliyun.com	网站域名。
RegionList	Array		封禁地区信息。
Block	Integer	0	封禁状态。取值： • 0：未封禁 • 1：已封禁
Region	String	CN-SHANGHAI	地区。
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。

示例

请求示例

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

正常返回示例

`XML` 格式

```
<DescribeWebAreaBlockConfigsResponse>
```

```
<AreaBlockConfigs>
<RegionList>
<Block>1</Block>
<Region>CN-YUNNAN</Region>
</RegionList>
<RegionList>
<Block>0</Block>
<Region>CN-HEILONGJIANG</Region>
</RegionList>
<RegionList>
<Block>0</Block>
<Region>OVERSEAS-ANTARCTICA</Region>
</RegionList>
<RegionList>
<Block>1</Block>
<Region>OVERSEAS-EUROPE</Region>
</RegionList>
<RegionList>
<Block>0</Block>
<Region>CN-BEIJING</Region>
</RegionList>
<RegionList>
<Block>0</Block>
<Region>CN-HENAN</Region>
</RegionList>
<RegionList>
<Block>0</Block>
<Region>CN-HUNAN</Region>
</RegionList>
<RegionList>
<Block>0</Block>
<Region>CN-FUJIAN</Region>
</RegionList>
<RegionList>
<Block>0</Block>
<Region>CN-JIANGSU</Region>
</RegionList>
<RegionList>
<Block>0</Block>
<Region>CN-ZHEJIANG</Region>
</RegionList>
```

```
<RegionList>
<Block>0</Block>
<Region>CN-HAINAN</Region>
</RegionList>
<RegionList>
<Block>0</Block>
<Region>CN-TIBET</Region>
</RegionList>
<RegionList>
<Block>0</Block>
<Region>CN-INNERMONGOLIA</Region>
</RegionList>
<RegionList>
<Block>0</Block>
<Region>CN-NINGXIA</Region>
</RegionList>
<RegionList>
<Block>0</Block>
<Region>CN-SHAANXI</Region>
</RegionList>
<RegionList>
<Block>0</Block>
<Region>CN-GUANGDONG</Region>
</RegionList>
<RegionList>
<Block>0</Block>
<Region>CN-QINGHAI</Region>
</RegionList>
<RegionList>
<Block>0</Block>
<Region>OVERSEAS-NAMERICA</Region>
</RegionList>
<RegionList>
<Block>0</Block>
<Region>OVERSEAS-SAMERICA</Region>
</RegionList>
<RegionList>
<Block>0</Block>
<Region>CN-SHANGHAI</Region>
</RegionList>
<RegionList>
```

```
<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。

11.21. ModifyWebAreaBlock

调用ModifyWebAreaBlock设置网站业务区域封禁（针对域名）的封禁地区。

调试

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

请求参数

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

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。
Regions.N	RepeatList	否	CN-SHANGHAI	要封禁的区域列表。不传入表示取消区域封禁（针对域名）。取值： 中国地区 • CN-SHANGHAI：上海市 • CN-YUNNAN：云南省 • CN-INNERMONGOLIA：内蒙古自治区 • CN-BEIJING：北京市 • CN-TAIWAN：台湾省 • CN-JILIN：吉林省 • CN-SICHUAN：四川省 • CN-TIANJIN：天津省 • CN-NINGXIA：宁夏回族自制区 • CN-ANHUI：安徽省 • CN-SHANDONG：山东省 • CN-SHAANXI：陕西省 • CN-SHANXI：山西省 • CN-GUANGDONG：广东省 • CN-GUANGXI：广西壮族自治区 • CN-XINJIANG：新疆维吾尔自治区 • CN-JIANGSU：江苏省 • CN-JIANGXI：江西省 • CN-HEBEI：河北省 • CN-HENAN：河南省 • CN-ZHEJIANG：浙江省 • CN-HAINAN：海南省

名称	类型	是否必选	示例值	描述
				• CN-HUBEI：湖北省 • CN-HUNAN：湖南省 • CN-MACAU：澳门特别行政区 • CN-GANSU：甘肃省 • CN-FUJIAN：福建省 • CN-TIBET：西藏自治区 • CN-GUIZHOU：贵州省 • CN-LIAONING：辽宁省 • CN-CHONGQING：重庆市 • CN-QINGHAI：青海省 • CN-HONGKONG：香港特别行政区 • CN-HEILONGJIANG：黑龙江省 海外地区 • OVERSEAS-ASIA：亚洲（中国除外） • OVERSEAS-EUROPE：欧洲 • OVERSEAS-NAMERICA：北美洲 • OVERSEAS-SAMERICA：南美洲 • OVERSEAS-AFRICA：非洲 • OVERSEAS-OCEANIA：大洋洲 • OVERSEAS-ANTARCTICA：南极洲

返回数据

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

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyWebAreaBlock
&Domain=www.aliyun.com
&Regions.1=CN-SHANGHAI
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

JSON 格式

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

错误码

访问错误中心查看更多错误码。

12.非网站业务防护策略

12.1. DescribePortAutoCcStatus

调用DescribePortAutoCcStatus查询非网站业务AI智能防护的配置信息。

调试

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

请求参数

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

返回数据

名称	类型	示例值	描述
PortAutoCcStatus	Array		非网站业务AI智能防护的配置信息。
Mode	String	normal	AI智能防护的模式。取值： • normal：正常 • loose：宽松 • strict：严格

名称	类型	示例值	描述
Switch	String	on	AI智能防护的开关状态。取值： • on：开启 • off：关闭
WebMode	String	normal	80和443端口的防护模式。取值： • normal：正常 • loose：宽松 • strict：严格
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。

12.2. ModifyPortAutoCcStatus

调用ModifyPortAutoCcStatus设置非网站业务AI智能防护。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyPortAutoCcStatus	要执行的操作。取值：ModifyPortAutoCcStatus
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
Mode	String	是	normal	非网站业务AI智能防护的模式。取值： • normal：正常 • loose：宽松 • strict：严格

名称	类型	是否必选	示例值	描述
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。

12.3. DescribeNetworkRuleAttributes

调用DescribeNetworkRuleAttributes查询非网站业务端口转发规则的防护配置，包括会话保持和DDoS防护策略。

调试

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

请求参数

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

返回数据

名称	类型	示例值	描述
NetworkRuleAttributes	Array		非网站业务端口转发规则的防护配置，包括会话保持和DDoS防护策略。
Config	Struct		端口转发规则的防护配置。
Cc	Struct		源连接频繁超限控制策略。

名称	类型	示例值	描述
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。
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。

名称	类型	示例值	描述
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。

名称	类型	示例值	描述
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。
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。

12.4. ModifyNetworkRuleAttribute

调用ModifyNetworkRuleAttribute编辑端口转发规则的会话保持设置。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyNetworkRuleAttribute	要执行的操作。取值：ModifyNetworkRuleAttribute
Config	String	是	{"PersistenceTimeout":900}	端口转发规则的会话保持设置。使用JSON格式的字符串表述，具体结构描述如下。 • PersistenceTimeout：Integer类型，必选，会话保持的超时时间。取值范围：30~3600，单位：秒。默认为0，表示关闭。
ForwardProtocol	String	是	tcp	转发协议。取值： • tcp • udp
FrontendPort	Integer	是	8080	转发端口。
InstanceId	String	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务

返回数据

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

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyNetworkRuleAttribute
&Config={"PersistenceTimeout":900}
&ForwardProtocol=tcp
&FrontendPort=8080
&InstanceId=ddoscoo-cn-mp91j1ao****
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

访问错误中心查看更多错误码。

13.定制场景策略

13.1. DescribeSceneDefensePolicies

调用DescribeSceneDefensePolicies查询定制场景策略的详细信息。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeSceneDefensePolicies	要执行的操作。取值：DescribeSceneDefensePolicies
Template	String	否	promotion	策略模板。取值： • promotion：重大活动 • bypass：全量转发
Status	String	否	1	策略生效状态。取值： • 0：禁用 • 1：等待生效 • 2：生效中 • 3：过期
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
Policies	Array		定制场景策略的详细信息。

名称	类型	示例值	描述
Done	Integer	1	策略执行状态。取值： • 1：未执行或执行完成 • 0：执行中 • -1：执行失败
EndTime	Long	1586016000000	生效结束时间。时间戳格式，单位：毫秒。
Name	String	testpolicy	策略名称。
ObjectCount	Integer	1	防护对象数量。
PolicyId	String	321a-fd31-df51-****	策略ID。
RuntimePolicies	Array		策略运行规则。
NewValue	String	{"cc_rule_enable": false }	策略生效时的防护规则。 PolicyType为1时，取值：{"cc_rule_enable": false }，表示禁用频率控制。 PolicyType为2时，取值：{"ai_rule_enable": 0}，表示禁用AI智能防护。
PolicyType	Integer	1	策略生效时触发的防护功能变更类型。取值： • 1：频率控制 • 2：AI智能防护
Status	Integer	3	策略运行状态。取值： • 0：未下发或策略恢复成功 • 1：正在生效中（策略生效） • 2：正在恢复中（策略恢复） • 3：策略生效成功 • 4：策略生效失败 • 5：策略恢复失败 • 6：策略对应对象的配置不存在（可能已删除）

名称	类型	示例值	描述
oldValue	String	{"cc_rule_enable": true}	策略生效前的防护规则。 PolicyType为1时，取值：{"cc_rule_enable": true}，表示启用了频率控制。 PolicyType为2时，取值：{"ai_rule_enable": 1}，表示启用了AI智能防护。
StartTime	Long	1585670400000	生效开始时间。时间戳格式，单位：毫秒。
Status	Integer	1	策略生效状态。取值： • 0：禁用 • 1：等待生效 • 2：生效中 • 3：过期
Template	String	promotion	策略模板。取值： • promotion：重大活动 • bypass：全量转发
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	本次请求的ID。
Success	Boolean	true	是否成功调用、取值： • true：是 • false：否

示例

请求示例

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

正常返回示例

`XML` 格式

```
<DescribeSceneDefensePoliciesResponse>
<Policies>
<PolicyId>321a-fd31-df51-****</PolicyId>
<Name>testpolicy</Name>
<Template>promotion</Template>
<StartTime>1585670400000</StartTime>
<EndTime>1586016000000</EndTime>
<Status>1</Status>
<ObjectCount>1</ObjectCount>
<Done>1</Done>
<RuntimePolicies>
<Status>4</Status>
<PolicyType>1</PolicyType>
<NewValue>
<cc_rule_enable>false</cc_rule_enable>
</NewValue>
<oldValue>
<cc_rule_enable>true</cc_rule_enable>
</oldValue>
</RuntimePolicies>
<RuntimePolicies>
<Status>3</Status>
<PolicyType>2</PolicyType>
<NewValue>
<ai_rule_enable>0</ai_rule_enable>
</NewValue>
<oldValue>
<ai_rule_enable>1</ai_rule_enable>
</oldValue>
</RuntimePolicies>
</Policies>
<Success>true</Success>
<RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
</DescribeSceneDefensePoliciesResponse>
```

`JSON` 格式

```
{
"Policies": [
{
"PolicyId": "321a-fd31-df51-****",
"Name": "testpolicy",
"Template": "promotion",
"StartTime": 1585670400000,
"EndTime": 1586016000000,
"Status": 1,
"ObjectCount": 1,
"Done": 1,
"RuntimePolicies": [
{
"Status": 4,
"PolicyType": 1,
"NewValue": {
"cc_rule_enable": false
},
"oldValue": {
"cc_rule_enable": true
}
},
{
"Status": 3,
"PolicyType": 2,
"NewValue": {
"ai_rule_enable": 0
},
"oldValue": {
"ai_rule_enable": 1
}
}
]
}
],
"Success": true,
"RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D"
}
```


错误码

访问错误中心查看更多错误码。

13.2. CreateSceneDefensePolicy

调用CreateSceneDefensePolicy创建定制场景策略。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateSceneDefensePolicy	要执行的操作。取值：CreateSceneDefensePolicy
EndTime	Long	是	1586016000000	生效结束时间。时间戳格式，单位：毫秒。
Name	String	是	testpolicy	策略名称。
StartTime	Long	是	1585670400000	生效开始时间。时间戳格式，单位：毫秒。
Template	String	是	promotion	策略模板。取值： • promotion：重大活动 • bypass：全量转发
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	本次请求的ID。

名称	类型	示例值	描述
Success	Boolean	true	是否成功创建策略。取值： • true：是 • false：否

示例

请求示例

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

正常返回示例

`XML` 格式

```
<CreateSceneDefensePolicyResponse>
<RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
<Success>true</Success>
</CreateSceneDefensePolicyResponse>
```

`JSON` 格式

```
{
"RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
"Success": true
}
```

错误码

访问错误中心查看更多错误码。

13.3. ModifySceneDefensePolicy

调用ModifySceneDefensePolicy编辑定制场景策略。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifySceneDefensePolicy	要执行的操作。取值：ModifySceneDefensePolicy
EndTime	Long	是	1586016000000	生效结束时间。时间戳格式，单位：毫秒。
Name	String	是	testpolicy	策略名称。
PolicyId	String	是	321a-fd31-df51-****	要编辑的策略ID。 说明 您可以调用DescribeSceneDefensePolicies查询所有策略ID。
StartTime	Long	是	1585670400000	生效开始时间。时间戳格式，单位：毫秒。
Template	String	是	promotion	策略模板。取值： • promotion：重大活动 • bypass：全量转发
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	本次请求的ID。
Success	Boolean	true	是否成功调用。取值： • true：是 • false：否

示例

请求示例

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

正常返回示例

`XML` 格式

```
<ModifySceneDefensePolicyResponse>
<RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
<Success>true</Success>
</ModifySceneDefensePolicyResponse>
```

`JSON` 格式

```
{
"RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
"Success":true
}
```

错误码

访问错误中心查看更多错误码。

13.4. 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

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteSceneDefensePolicy	要执行的操作。取值：DeleteSceneDefensePolicy
PolicyId	String	是	321a-fd31-df51-****	要删除的策略ID。 说明 您可以调用DescribeSceneDefensePolicies查询所有策略ID。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	本次请求的ID。
Success	Boolean	true	是否成功调用。取值： • true：是 • false：否

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteSceneDefensePolicy
&PolicyId=321a-fd31-df51-****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DeleteSceneDefensePolicyResponse>
<RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
<Success>true</Success>
</DeleteSceneDefensePolicyResponse>
```

JSON 格式

```
{
"RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
"Success":true
}
```

错误码

访问错误中心查看更多错误码。

13.5. DescribeSceneDefenseObjects

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeSceneDefenseObjects	要执行的操作。取值：DescribeSceneDefenseObjects
PolicyId	String	是	321a-fd31-df51-****	要查询的策略ID。 说明 您可以调用DescribeSceneDefensePolicies查询所有策略ID。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
Objects	Array		防护对象信息。
Domain	String	www.aliyun.com	域名。
PolicyId	String	321a-fd31-df51-****	策略ID。
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	本次请求的ID。
Success	Boolean	true	是否成功调用。取值： • true：是 • false：否

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeSceneDefenseObjects
&PolicyId=321a-fd31-df51-****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeSceneDefenseObjectsResponse>
<Objects>
<PolicyId>321a-fd31-df51-****</PolicyId>
<Domain>www.aliyun.com</Domain>
</Objects>
<Success>true</Success>
<RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
</DescribeSceneDefenseObjectsResponse>
```

`JSON` 格式

```
{
"Objects": [
{
"PolicyId": "321a-fd31-df51-****",
"Domain": "www.aliyun.com"
}
],
"Success": true,
"RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D"
}
```


错误码

访问错误中心查看更多错误码。

13.6. AttachSceneDefenseObject

调用AttachSceneDefenseObject为定制场景策略添加防护对象。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	AttachSceneDefenseObject	要执行的操作。取值：AttachSceneDefenseObject
Objects	String	是	www.aliyun.com	要添加的防护对象。多个对象间使用英文逗号（,）分隔。
ObjectType	String	是	Domain	对象类型。取值：Domain，表示域名。
PolicyId	String	是	321a-fd31-df51-****	策略ID。 说明 您可以调用DescribeSceneDefensePolicies查询所有策略ID。

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

返回数据

名称	类型	示例值	描述
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	本次请求的ID。
Success	Boolean	true	是否成功调用。取值： • true：是 • false：否

示例

请求示例

```
http(s)://[Endpoint]/?Action=AttachSceneDefenseObject
&Objects=www.aliyun.com
&ObjectType=Domain
&PolicyId=321a-fd31-df51-****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<AttachSceneDefenseObjectResponse>
<RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
<Success>true</Success>
</AttachSceneDefenseObjectResponse>
```

`JSON` 格式

```
{
"RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
"Success":true
}
```

错误码

访问错误中心查看更多错误码。

13.7. 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。
Success	Boolean	true	是否成功调用。取值： • true：是 • false：否

示例

请求示例

```
http(s)://[Endpoint]/?Action=DetachSceneDefenseObject
&Objects=www.aliyun.com
&PolicyId=321a-fd31-df51-****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DetachSceneDefenseObjectResponse>
<RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
<Success>true</Success>
</DetachSceneDefenseObjectResponse>
```

`JSON` 格式

```
{
"RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
"Success":true
}
```

错误码

访问错误中心查看更多错误码。

13.8. EnableSceneDefensePolicy

调用EnableSceneDefensePolicy启用定制场景策略。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	EnableSceneDefensePolicy	要执行的操作。取值：EnableSceneDefensePolicy
PolicyId	String	是	321a-fd31-df51-****	要启用的策略ID。 说明 您可以调用DescribeSceneDefensePolicies查询所有策略ID。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	本次请求的ID。
Success	Boolean	true	是否成功调用。取值： • true：是 • false：否

示例

请求示例

```
http(s)://[Endpoint]/?Action=EnableSceneDefensePolicy
&PolicyId=321a-fd31-df51-****
&<公共请求参数>
```

正常返回示例

XML 格式

```
<EnableSceneDefensePolicyResponse>
<RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
<Success>true</Success>
</EnableSceneDefensePolicyResponse>
```

JSON 格式

```
{
"RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
"Success":true
}
```

错误码

访问错误中心查看更多错误码。

13.9. 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。

14.静态页面缓存

14.1. ModifyWebCacheSwitch

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyWebCacheSwitch	要执行的操作。取值：ModifyWebCacheSwitch
Domain	String	是	www.aliyun.com	网站业务的域名。 说明 域名必须已配置网站业务转发规则且关联了增强功能套餐的DDoS高防实例。您可以调用DescribeDomains查询所有域名。
Enable	Integer	是	1	静态页面缓存的开关状态。取值： • 1：开启 • 0：关闭
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

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

示例

请求示例

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

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

访问错误中心查看更多错误码。

14.2. ModifyWebCacheMode

调用ModifyWebCacheMode设置网站业务静态页面缓存的缓存模式。

调试

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

请求参数

名称	类型	是否必选	示例值	描述

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyWebCacheMode	要执行的操作。取值：ModifyWebCacheMode
Domain	String	是	www.aliyun.com	网站业务的域名。 说明 域名必须已配置网站业务转发规则且关联了增强功能套餐的DDoS高防实例。您可以调用DescribeDomains查询所有域名。
Mode	String	是	standard	静态页面缓存的模式。取值： • standard：标准模式 • aggressive：强力模式 • bypass：不缓存
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

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

示例

请求示例

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

正常返回示例

XML 格式

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

JSON 格式

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

错误码

访问错误中心查看更多错误码。

14.3. ModifyWebCacheCustomRule

调用ModifyWebCacheCustomRule设置网站业务静态页面缓存的自定义规则。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyWebCacheCustomRule	要执行的操作。取值：ModifyWebCacheCustomRule
Domain	String	是	www.aliyun.com	网站业务的域名。 说明 域名必须已配置网站业务转发规则且关联了增强功能套餐的DDoS高防实例。您可以调用DescribeDomains查询所有域名。

名称	类型	是否必选	示例值	描述

Rules	String	是	[{"Name": "test","Uri": "/a","Mode": "standard","CacheTtl": 3600}]	静态页面缓存的自定义规则信息，使用JSON格式的字符串表述，具体结构如下。
				• Name：String类型，必选，规则名称。
				• Uri：String类型，必选，缓存页面的路径。
				• Mode：String类型，必选，缓存模式。取值：
				  ○ standard：标准模式
				  ○ aggressive：强力模式
				  ○ bypass：不缓存
				• CacheTtl：Integer类型，必选，页面缓存的过期时间。单位：秒。

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

返回数据

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

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyWebCacheCustomRule
&Domain=www.aliyun.com
&Rules=[{"Name": "test","Uri": "/a","Mode": "standard","CacheTtl": 3600}]
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

JSON 格式

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

错误码

访问错误中心查看更多错误码。

14.4. DeleteWebCacheCustomRule

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteWebCacheCustomRule	要执行的操作。取值：DeleteWebCacheCustomRule
Domain	String	是	www.aliyun.com	网站业务的域名。 说明 域名必须已配置网站业务转发规则且关联了增强功能套餐的DDoS高防实例。您可以调用DescribeDomains查询所有域名。
RuleNames.N	RepeatList	是	test	要删除的规则的名称。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务

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=DeleteWebCacheCustomRule
&Domain=www.aliyun.com
&RuleNames.1=test
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

访问错误中心查看更多错误码。

14.5. DescribeWebCacheConfigs

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

调试

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

请求参数

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

返回数据

名称	类型	示例值	描述
DomainCacheConfigs	Array		静态页面缓存的配置信息。
CustomRules	Array		自定义规则信息。
CacheTtl	Long	86400	页面缓存的过期时间。单位：秒。
Mode	String	standard	缓存模式。取值： • **standard**：标准模式 • **aggressive**：强力模式 • **bypass**：不缓存
Name	String	c1	规则名称。

名称	类型	示例值	描述
Uri	String	/blog/	缓存页面的路径。
Domain	String	www.aliyun.com	网站域名。
Enable	Integer	1	开关状态。取值： • 1：开启 • 0：关闭
Mode	String	bypass	缓存模式。取值： • standard：标准模式 • aggressive：强力模式 • bypass：不缓存
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。

示例

请求示例

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

正常返回示例

`XML` 格式

```
<DescribeWebCacheConfigsResponse>
<RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
<DomainCacheConfigs>
<Domain>www.aliyun.com</Domain>
<Enable>1</Enable>
<Mode>bypass</Mode>
<CustomRules>
<Name>c1</Name>
<Uri>/blog/</Uri>
<Mode>standard</Mode>
<CacheTtl>86400</CacheTtl>
</CustomRules>
</DomainCacheConfigs>
</DescribeWebCacheConfigsResponse>
```

JSON 格式

```
{
"RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
"DomainCacheConfigs": [
{
"Domain": "www.aliyun.com",
"Enable": 1,
"Mode": "bypass",
"CustomRules": [
{
"Name": "c1",
"Uri": "/blog/",
"Mode": "standard",
"CacheTtl": 86400
}
]
}
]
}
```

错误码

访问错误中心查看更多错误码。

15.监控报表

15.1. DescribeDDoSEvents

调用DescribeDDoSEvents查询针对DDoS高防实例的攻击事件。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDDoSEvents	要执行的操作。取值：DescribeDDoSEvents
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
PageNumber	Integer	是	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写1。
PageSize	Integer	是	10	页面显示的记录数量。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

名称	类型	是否必选	示例值	描述
EndTime	Long	否	1583683200	查询结束时间。时间戳格式，单位：秒。 说明 必须为整点分钟。

返回数据

名称	类型	示例值	描述
DDoSEvents	Array		DDoS攻击事件列表。
Bps	Long	0	攻击流量带宽大小。单位：bps。
EndTime	Long	1583933330	攻击结束时间。时间戳格式，单位：秒。
EventType	String	blackhole	攻击事件类型。取值： • defense：清洗事件 • blackhole：黑洞事件
Ip	String	203.***.***.132	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。

名称	类型	示例值	描述
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。

15.2. DescribePortFlowList

调用DescribePortFlowList查询DDoS高防实例的流量数据列表。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribePortFlowList	要执行的操作。取值：DescribePortFlowList
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 说明 必须为整点分钟。

名称	类型	是否必选	示例值	描述
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
Interval	Integer	是	1000	返回数据的步长，单位为秒，即每隔多少秒返回一个结果。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	null	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
PortFlowList	Array		流量数据。
AttackBps	Long	0	攻击带宽，单位：bps。
AttackPps	Long	0	攻击包转发率，单位：pps。
InBps	Long	2176000	入方向带宽，单位：bps。
InPps	Long	2934	入方向包转发率，单位：pps。

名称	类型	示例值	描述
Index	Long	0	返回数据的索引号。
OutBps	Long	4389	出方向带宽，单位：bps。
OutPps	Long	5	出方向包转发率，单位：pps。
Region	String	cn	访问流量来源地区。取值： • cn：中国内地 • alb-ap-northeast-1-gf-x：日本 • alb-ap-southeast-gf-x：新加坡 • alb-cn-hongkong-gf-x：中国香港 • alb-eu-central-1-gf-x：德国 • alb-us-west-1-gf-x：美国西部 说明 cn以外的取值只有在DDoS高防（国际）服务（RegionId为ap-southeast-1）中提供。
Time	Long	1582992000	统计时间。时间戳格式，单位：秒。
RequestId	String	FFC77501-BDF8-4BC8-9BF5-B295FBC3189B	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePortFlowList
&EndTime=1583683200
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&Interval=1000
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribePortFlowListResponse>
<RequestId>FFC77501-BDF8-4BC8-9BF5-B295FBC3189B</RequestId>
<PortFlowList>
<OutPps>5</OutPps>
<OutBps>4389</OutBps>
<InBps>2176000</InBps>
<InPps>2934</InPps>
<Region>cn</Region>
<Index>0</Index>
<AttackBps>0</AttackBps>
<AttackPps>0</AttackPps>
<Time>1582992000</Time>
</PortFlowList>
<PortFlowList>
<OutPps>5</OutPps>
<OutBps>4155</OutBps>
<InBps>4648000</InBps>
<InPps>6268</InPps>
<Region>cn</Region>
<Index>1</Index>
<AttackBps>0</AttackBps>
<AttackPps>0</AttackPps>
<Time>1582993000</Time>
</PortFlowList>
</DescribePortFlowListResponse>
```

`JSON` 格式

```
{
"RequestId": "FFC77501-BDF8-4BC8-9BF5-B295FBC3189B",
"PortFlowList": [
{
"OutPps": 5,
"OutBps": 4389,
"InBps": 2176000,
"InPps": 2934,
"Region": "cn",
"Index": 0,
"AttackBps": 0,
"AttackPps": 0,
"Time": 1582992000
},
{
"OutPps": 5,
"OutBps": 4155,
"InBps": 4648000,
"InPps": 6268,
"Region": "cn",
"Index": 1,
"AttackBps": 0,
"AttackPps": 0,
"Time": 1582993000
}
]
}
```


错误码

访问错误中心查看更多错误码。

15.3. DescribePortConnsList

调用DescribePortConnsList查询DDoS高防实例的端口连接数列表。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribePortConnsList	要执行的操作。取值：DescribePortConnsList
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
Interval	Integer	是	1000	返回数据的步长，单位为秒，即每隔多少秒返回一个结果。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
Port	String	否	null	要查询的端口号。不传入表示查询所有端口。

返回数据

名称	类型	示例值	描述
ConnsList	Array		端口连接数据列表。

名称	类型	示例值	描述
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。

15.4. DescribePortConnsCount

调用DescribePortConnsCount查询DDoS高防实例的端口连接数统计信息。

调试

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

请求参数

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

名称	类型	是否必选	示例值	描述
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
Port	String	否	80	要查询的端口号。不传入该参数表示查询所有端口号。

返回数据

名称	类型	示例值	描述
ActConns	Long	159	活跃的连接数量。
Conns	Long	46340	并发连接数量。
Cps	Long	0	新建连接数量。
InActConns	Long	121	不活跃的连接数量。

名称	类型	示例值	描述
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。

15.5. DescribePortMaxConns

调用DescribePortMaxConns查询DDoS高防实例的端口连接峰值信息。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribePortMaxConns	要执行的操作。取值：DescribePortMaxConns。
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
PortMaxConns	Array		DDoS高防实例的端口连接峰值信息。
Cps	Long	100	最大每秒连接数。

名称	类型	示例值	描述
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。

15.6. DescribePortAttackMaxFlow

调用DescribePortAttackMaxFlow查询指定时间段内DDoS高防受到的攻击带宽和包速峰值。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribePortAttackMaxFlow	要执行的操作。取值：DescribePortAttackMaxFlow
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
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
Bps	Long	149559	攻击带宽峰值。单位：bps。
Pps	Long	23	攻击包速峰值。单位：pps。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePortAttackMaxFlow
&EndTime=1583683200
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribePortAttackMaxFlowResponse>
<RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
<Bps>149559</Bps>
<Pps>23</Pps>
</DescribePortAttackMaxFlowResponse>
```

JSON 格式

```
{
"RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
"Bps": 149559,
"Pps": 23
}
```

错误码

访问错误中心查看更多错误码。

15.7. DescribePortViewSourceCountries

调用DescribePortViewSourceCountries查询指定时间段内DDoS高防实例的请求来源国家分布。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribePortViewSourceCountries	要执行的操作。取值：DescribePortViewSourceCountries。
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
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
SourceCountrys	Array		DDoS高防实例的请求来源国家信息。
Count	Long	3390671	请求次数。
CountryId	String	cn	请求的来源国家或地域的代码。详见国家和地域代码说明。例如，cn表示中国，us表示美国。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePortViewSourceCountries
&EndTime=1583683200
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribePortViewSourceCountriesResponse>
<RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
<SourceCountrys>
<Count>3390671</Count>
<CountryId>cn</CountryId>
</SourceCountrys>
</DescribePortViewSourceCountriesResponse>
```

`JSON` 格式

```
{
"RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
"SourceCountrys": [
{
"Count": 3390671,
"CountryId": "cn"
}
]
}
```

错误码

访问错误中心查看更多错误码。

15.8. DescribePortViewSourceIsps

调用DescribePortViewSourceIsps查询指定时间段内DDoS高防实例的请求来源运营商分布。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribePortViewSourceIsps	要执行的操作。取值：DescribePortViewSourceIsps
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。不传入表示使用当前时间作为结束时间。 说明 必须为整点分钟。
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
Isps	Array		DDoS高防实例的请求来源运营商信息。
Count	Long	3390671	请求数量。
IspId	String	100017	运营商ID。详见返回参数表下的运营商代码说明，运营商ID对应表中的代码。

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

运营商代码

代码	运营商
100017	电信
100026	联通
100025	移动
100027	教育网
100020	铁通
1000143	鹏博士
100080	歌华
1000139	广电
100023	有线通
100063	方正宽带
1000337	皓宽网络
100021	世纪互联
1000333	华数传媒
100093	网宿

代码	运营商
1000401	腾讯
100099	百度
1000323	阿里云
100098	阿里巴巴

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePortViewSourceIsps
&EndTime=1583683200
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribePortViewSourceIspsResponse>
<RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
<Isps>
<Count>3390671</Count>
<IspId>100017</IspId>
</Isps>
</DescribePortViewSourceIspsResponse>
```

`JSON` 格式

```
{
"RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
"Isps": [
{
"Count": 3390671,
"IspId": "100017"
}
]
}
```


错误码

访问错误中心查看更多错误码。

15.9. DescribePortViewSourceProvinces

调用DescribePortViewSourceProvinces查询指定时间段内DDoS高防实例的请求来源（中国）省份分布。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribePortViewSourceProvinces	要执行的操作。取值：DescribePortViewSourceProvinces。
InstanceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 说明 必须为整点分钟。

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。
EndTime	Long	否	1583683200	查询结束时间。时间戳格式，单位：秒。不传入表示使用当前时间作为结束时间。 说明 必须为整点分钟。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
SourceProvinces	Array		DDoS高防实例的请求来源（中国）省份信息。
Count	Long	3390671	请求数量。
ProvinceId	String	440000	省份ID。详见中国和海外地区代码中的中国地区代码说明。例如，110000表示北京市，120000表示天津市。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePortViewSourceProvinces
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribePortViewSourceProvincesResponse>
<RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
<SourceProvinces>
<Count>3390671</Count>
<ProvinceId>440000</ProvinceId>
</SourceProvinces>
</DescribePortViewSourceProvincesResponse>
```

JSON 格式

```
{
"RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
"SourceProvinces": [
{
"Count": 3390671,
"ProvinceId": "440000"
}
]
}
```

错误码

访问错误中心查看更多错误码。

15.10. DescribeDomainAttackEvents

调用DescribeDomainAttackEvents查询针对网站业务的攻击事件。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainAttackEvents	要执行的操作。取值：DescribeDomainAttackEvents
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 说明 必须为整点分钟

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。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 说明 必须为整点分钟
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
Domain	String	否	www.aliyun.com	网站业务的域名。 说明 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

返回数据

名称	类型	示例值	描述
DomainAttackEvents	Array		网站业务DDoS攻击事件信息。
Domain	String	www.aliyun.com	被攻击域名。
EndTime	Long	1560320160	攻击结束时间。时间戳格式，单位：秒。
MaxQps	Long	1000	攻击峰值QPS。
StartTime	Long	1560312900	攻击开始时间。时间戳格式，单位：秒。

名称	类型	示例值	描述
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。

15.11. DescribeDomainQPSList

调用DescribeDomainQPSList查询网站业务的QPS统计信息。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainQPSList	要执行的操作。取值：DescribeDomainQPSList
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
Interval	Long	是	1000	返回数据的步长，单位为秒，即每隔多少秒返回一个结果。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 说明 必须为整点分钟。

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

返回数据

名称	类型	示例值	描述
DomainQPSList	Array		网站业务QPS统计信息。
AttackQps	Long	1	攻击QPS。
CacheHits	Long	0	缓存命中数。
Index	Long	0	返回数据的索引号。
MaxAttackQps	Long	37	攻击QPS峰值。
MaxNormalQps	Long	93	正常QPS峰值。
MaxQps	Long	130	总QPS峰值。
Time	Long	1582992000	统计时间。时间戳格式，单位：秒。

名称	类型	示例值	描述
TotalCount	Long	20008	总访问次数。
TotalQps	Long	1	总QPS。
RequestId	String	327F2ABB-104D-437A-AAB5-D633E29A8C51	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainQPSList
&Interval=1000
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDomainQPSListResponse>
<DomainQPSList>
<MaxAttackQps>37</MaxAttackQps>
<TotalQps>1</TotalQps>
<TotalCount>20008</TotalCount>
<MaxQps>130</MaxQps>
<MaxNormalQps>93</MaxNormalQps>
<AttackQps>1</AttackQps>
<Index>0</Index>
<Time>1582992000</Time>
<CacheHits>0</CacheHits>
</DomainQPSList>
<RequestId>327F2ABB-104D-437A-AAB5-D633E29A8C51</RequestId>
</DescribeDomainQPSListResponse>
```

`JSON` 格式

```
{
"DomainQPSList": [
{
"MaxAttackQps": 37,
"TotalQps": 1,
"TotalCount": 20008,
"MaxQps": 130,
"MaxNormalQps": 93,
"AttackQps": 1,
"Index": 0,
"Time": 1582992000,
"CacheHits": 0
}
],
"RequestId": "327F2ABB-104D-437A-AAB5-D633E29A8C51"
}
```


错误码

访问错误中心查看更多错误码。

15.12. DescribeDomainStatusCodeList

调用DescribeDomainStatusCodeList查询网站业务的响应状态码统计信息。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainStatusCodeList	要执行的操作。取值：DescribeDomainStatusCodeList
Interval	Long	是	1000	返回数据的步长，单位为秒，即每隔多少秒返回一个结果。
QueryType	String	是	gf	查询数据的来源。取值： • gf：高防响应 • upstrem：源站响应

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。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
EndTime	Long	否	1583683200	查询结束时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
Domain	String	否	www.aliyun.com	网站业务的域名。不传入表示查询所有域名的响应状态码统计信息。 说明 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

返回数据

名称	类型	示例值	描述
RequestId	String	3B63C0DD-8AC5-44B2-95D6-064CA9296B9C	本次请求的ID。
StatusCodeList	Array		响应状态码的统计信息。
Index	Integer	0	返回数据的索引号。
Status200	Long	15520	200状态码的统计值。

名称	类型	示例值	描述
Status2XX	Long	15520	2XX类状态码的统计值。
Status3XX	Long	0	3XX类状态码的统计值。
Status403	Long	0	403状态码的统计值。
Status404	Long	0	404状态码的统计值。
Status405	Long	0	405状态码的统计值。
Status4XX	Long	4486	4XX类状态码的统计值。
Status501	Long	0	501状态码的统计值。
Status502	Long	0	502状态码的统计值。
Status503	Long	0	503状态码的统计值。
Status504	Long	0	504状态码的统计值。
Status5XX	Long	0	5XX类状态码的统计值。
Time	Long	1582992000	统计时间。时间戳格式，单位：秒。

示例

请求示例

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

正常返回示例

`XML` 格式

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

`JSON` 格式

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


错误码

访问错误中心查看更多错误码。

15.13. DescribeDomainOverview

调用DescribeDomainOverview查询网站业务攻击总览，包括HTTP攻击峰值、HTTPS攻击峰值。

调试

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

请求参数

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

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。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
EndTime	Long	否	1583683200	查询结束时间。时间戳格式，单位：秒。不传入表示使用当前时间作为结束时间。 说明 必须为整点分钟。
Domain	String	否	www.aliyun.com	网站业务的域名。 说明 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

返回数据

名称	类型	示例值	描述
MaxHttp	Long	1000	HTTP攻击峰值。单位：qps。
MaxHttps	Long	1000	HTTPS攻击峰值。单位：qps。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainOverview
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDomainOverviewResponse>
<RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
<MaxHttps>1000</MaxHttps>
<MaxHttp>1000</MaxHttp>
</DescribeDomainOverviewResponse>
```

`JSON` 格式

```
{
"RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
"MaxHttps": 1000,
"MaxHttp": 1000
}
```

错误码

访问错误中心查看更多错误码。

15.14. DescribeDomainStatusCodeCount

调用DescribeDomainStatusCodeCount查询指定时间段内网站业务的各类响应状态码的统计信息。

调试

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

请求参数

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

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

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
Status200	Long	951159	查询时间段内200状态码的数量。
Status2XX	Long	951472	查询时间段内2XX类状态码的数量。
Status3XX	Long	133209	查询时间段内3XX状态码的数量。
Status403	Long	0	查询时间段内403状态码的数量。

名称	类型	示例值	描述
Status404	Long	897	查询时间段内404状态码的数量。
Status405	Long	0	查询时间段内405状态码的数量。
Status4XX	Long	5653	查询时间段内4XX状态码的数量。
Status501	Long	0	查询时间段内501状态码的数量。
Status502	Long	0	查询时间段内502状态码的数量。
Status503	Long	0	查询时间段内503状态码的数量。
Status504	Long	0	查询时间段内504状态码的数量。
Status5XX	Long	14	查询时间段内5XX状态码的数量。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainStatusCodeCount
&EndTime=1583683200
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDomainStatusCodeCountResponse>
<RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
<Status2XX>951472</Status2XX>
<Status200>951159</Status200>
<Status3XX>133209</Status3XX>
<Status4XX>5653</Status4XX>
<Status403>0</Status403>
<Status404>897</Status404>
<Status405>0</Status405>
<Status5XX>14</Status5XX>
<Status501>0</Status501>
<Status502>0</Status502>
<Status503>0</Status503>
<Status504>0</Status504>
</DescribeDomainStatusCodeCountResponse>
```

JSON 格式

```
{
"RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
"Status2XX": 951472,
"Status200": 951159,
"Status3XX": 133209,
"Status4XX": 5653,
"Status403": 0,
"Status404": 897,
"Status405": 0,
"Status5XX": 14,
"Status501": 0,
"Status502": 0,
"Status503": 0,
"Status504": 0
}
```

错误码

访问错误中心查看更多错误码。

15.15. DescribeDomainTopAttackList

调用DescribeDomainTopAttackList查询指定时间段内网站业务的QPS峰值数据，包括攻击QPS、总QPS。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainTopAttackList	要执行的操作。取值：DescribeDomainTopAttackList
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务

返回数据

名称	类型	示例值	描述
AttackList	Array		网站业务的QPS峰值数据。
Attack	Long	0	攻击QPS。单位：qps。
Count	Long	294	全部QPS，包含正常业务请求和攻击。单位：qps。
Domain	String	www.aliyun.com	网站域名。

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=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。

15.16. DescribeDomainViewSourceCountries

调用DescribeDomainViewSourceCountries查询指定时间段内网站业务的请求来源国家分布。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainViewSourceCountries	要执行的操作。取值：DescribeDomainViewSourceCountries。
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
Domain	String	否	www.aliyun.com	网站业务的域名。 说明 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
SourceCountrys	Array		网站业务的请求来源国家信息。
Count	Long	3390671	请求数量。
CountryId	String	cn	国家简称。详见中国和海外地区代码中的海外地区代码说明。例如，cn表示中国，us表示美国。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainViewSourceCountries
&EndTime=1583683200
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDomainViewSourceCountriesResponse>
<RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
<SourceCountries>
<Count>3390671</Count>
<CountryId>cn</CountryId>
</SourceCountries>
</DescribeDomainViewSourceCountriesResponse>
```

`JSON` 格式

```
{
"RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
"SourceCountries": [
{
"Count": 3390671,
"CountryId": "cn"
}
]
}
```


错误码

访问错误中心查看更多错误码。

15.17. DescribeDomainViewSourceProvinces

调用DescribeDomainViewSourceProvinces查询指定时间段内网站业务的请求来源（中国）省份分布。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainViewSourceProvinces	要执行的操作。取值：DescribeDomainViewSourceProvinces。
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

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

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
SourceProvinces	Array		网站业务的请求来源（中国）省份信息。
Count	Long	3390671	请求数量。
ProvinceId	String	440000	省份ID。详见中国和海外地区代码中的中国地区代码说明。例如，110000表示北京市，120000表示天津市。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainViewSourceProvinces
&EndTime=1583683200
&StartTime=1582992000
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeDomainViewSourceProvincesResponse>
<RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
<SourceProvinces>
<Count>3390671</Count>
<ProvinceId>440000</ProvinceId>
</SourceProvinces>
</DescribeDomainViewSourceProvincesResponse>
```

JSON 格式

```
{
"RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
"SourceProvinces": [
{
"Count": 3390671,
"ProvinceId": "440000"
}
]
}
```

错误码

访问错误中心查看更多错误码。

15.18. DescribeDomainViewTopCostTime

调用DescribeDomainViewTopCostTime查询指定时间段内网站业务的请求耗时最大的前N个URL。

调试

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

请求参数

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

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

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
UrlList	Array		请求耗时TOP URL列表。
CostTime	Float	3000	请求延时时长。单位：毫秒。
Domain	String	www.aliyun.com	网站域名。

名称	类型	示例值	描述
Url	String	Lw==	URL。使用BASE64加密表示。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainViewTopCostTime
&EndTime=1583683200
&StartTime=1582992000
&Top=5
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDomainViewTopCostTimeResponse>
<RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
<UrlList>
<CostTime>3000</CostTime>
<Domain>www.aliyun.com</Domain>
<Url>Lw==</Url>
</UrlList>
</DescribeDomainViewTopCostTimeResponse>
```

`JSON` 格式

```
{
"RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
"UrlList": [
{
"CostTime": 3000,
"Domain": "www.aliyun.com",
"Url": "Lw=="
}
]
}
```

错误码

访问错误中心查看更多错误码。

15.19. DescribeDomainViewTopUrl

调用DescribeDomainViewTopUrl查询指定时间段内网站业务访问量最大的前N个URL。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainViewTopUrl	要执行的操作。取值：DescribeDomainViewTopUrl
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
Top	Integer	是	5	返回URL的数量。取值：1~100。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
Domain	String	否	www.aliyun.com	网站业务的域名。 说明 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
UrlList	Array		网站业务的访问量TOP URL列表。
Count	Long	3390671	请求数量。
Domain	String	www.aliyun.com	网站域名。
Url	String	Lw==	URL。使用BASE64加密表示。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainViewTopUrl
&EndTime=1583683200
&StartTime=1582992000
&Top=5
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDomainViewTopUrlResponse>
<RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
<UrlList>
<Count>3390671</Count>
<Domain>www.aliyun.com</Domain>
<Url>Lw==</Url>
</UrlList>
</DescribeDomainViewTopUrlResponse>
```

`JSON` 格式

```
{
"RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
"UrlList": [
{
"Count": 3390671,
"Domain": "www.aliyun.com",
"Url": "Lw=="
}
]
}
```


错误码

访问错误中心查看更多错误码。

15.20. DescribeDomainQpsWithCache

调用DescribeDomainQpsWithCache查询网站业务的QPS数据列表，例如总QPS、由不同防护功能阻断的QPS、缓存命中数等。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainQpsWithCache	要执行的操作。取值：DescribeDomainQpsWithCache
EndTime	Long	是	1583683200	查询结束时间。时间戳格式，单位：秒。 说明 必须为整点分钟。
StartTime	Long	是	1582992000	查询开始时间。时间戳格式，单位：秒。 说明 必须为整点分钟。

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。
Domain	String	否	www.aliyun.com	网站业务的域名。 说明 域名必须已配置网站业务转发规则。您可以调用DescribeDomains查询所有域名。

返回数据

名称	类型	示例值	描述
Blocks	List	[20,30,20]	攻击QPS。
CacheHits	List	[0.3,0.4,0.5]	缓存命中率。使用小数表示，例如0.5表示缓存命中率是50%。
CcBlockQps	List	[1,0,0]	由频率控制阻断的QPS。
CcJsQps	List	[1,0,0]	由频率控制触发人机识别的QPS。
Interval	Integer	20384	返回数据的步长，单位为秒，即相邻两个数据的时间差。
IpBlockQps	List	[1,0,0]	由黑名单（针对域名）阻断的QPS。
PreciseBlocks	List	[1,0,0]	由精确访问控制阻断的QPS。
PreciseJsQps	List	[1,0,0]	由精确访问控制触发挑战的QPS。

名称	类型	示例值	描述
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
```

```
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。

16.全量日志分析

16.1. DescribeSlsOpenStatus

调用DescribeSlsOpenStatus查询阿里云日志服务SLS的开通状态。

调试

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

请求参数

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

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
SlsOpenStatus	Boolean	true	是否已开通日志服务。取值： • true：已开通 • false：未开通

示例

请求示例

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

正常返回示例

XML 格式

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

JSON 格式

```
{
"RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
"SlsOpenStatus": true
}
```

错误码

访问错误中心查看更多错误码。

16.2. DescribeSlsAuthStatus

调用DescribeSlsAuthStatus查询DDoS高防全量日志分析服务的授权状态，即是否授权DDoS高防访问日志服务。

调试

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

请求参数

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

返回数据

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

16.3. DescribeLogStoreExistStatus

调用DescribeLogStoreExistStatus查询是否已创建DDoS高防的日志库。

调试

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

请求参数

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

16.4. DescribeSlsLogstoreInfo

调用DescribeSlsLogstoreInfo查询DDoS高防的日志库信息，例如日志存储容量、日志存储时长等。

调试

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

请求参数

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

返回数据

名称	类型	示例值	描述
LogStore	String	ddoscoo-logstore	DDoS高防服务对接的日志库。
Project	String	ddoscoo-project-181071506993****-cn-hangzhou	DDoS高防服务对接的日志项目。
Quota	Long	3298534883328	可用的日志存储容量。单位：Byte。
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。

16.5. ModifyFullLogTtl

调用ModifyFullLogTtl编辑DDoS高防全量日志的存储时长。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	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。
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

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。

16.6. DescribeWebAccessLogDispatchStatus

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述

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

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
SlsConfigStatus	Array		域名的全量日志开关状态信息。
Domain	String	www.aliyun.com	域名。
Enable	Boolean	true	是否开启全量日志。取值： • true：已开启 • false：未开启
TotalCount	Integer	1	域名的总数。

示例

请求示例

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

正常返回示例

`XML` 格式

```
<?xml version="1.0" encoding="UTF-8" ?>
<DescribeWebAccessLogDispatchStatus>
<RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</requestId>
<TotalCount>1</TotalCount>
<SlsConfigStatus>
<Enable>true</Enable>
<Domain>www.aliyun.com</Domain>
</SlsConfigStatus>
</DescribeWebAccessLogDispatchStatus>
```

`JSON` 格式

```
{
"RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
"TotalCount": 1,
"SlsConfigStatus": [
{
"Enable": true,
"Domain": "www.aliyun.com"
}
]
}
```

错误码

访问错误中心查看更多错误码。

16.7. DescribeWebAccessLogStatus

调用DescribeWebAccessLogStatus查询单个网站业务的全量日志服务信息，例如开关状态、对接的日志项目、日志库。

调试

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

请求参数

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

16.8. EnableWebAccessLogConfig

调用EnableWebAccessLogConfig为网站业务开启全量日志分析。

调试

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

请求参数

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

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=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。

16.9. DisableWebAccessLogConfig

调用DisableWebAccessLogConfig为网站业务关闭全量日志分析。

调试

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

请求参数

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

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。

16.10. DescribeWebAccessLogEmptyCount

调用DescribeWebAccessLogEmptyCount查询可用的清空日志库的次数。

调试

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

请求参数

名称	类型	是否必选	示例值	描述

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。

16.11. EmptySlsLogstore

调用EmptySlsLogstore清空DDoS高防的日志库。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	EmptySlsLogstore	要执行的操作。取值：EmptySlsLogstore
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
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。

17.系统配置与日志

17.1. DescribeStsGrantStatus

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeStsGrantStatus	要执行的操作。取值：DescribeStsGrantStatus
Role	String	是	AliyunDDoSCOODefaultRole	要查询到角色名称。取值：AliyunDDoSCOODefaultRole，表示DDoS高防服务的默认角色。 说明 DDoS高防服务默认使用此角色来访问您在其他云产品中的资源。
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

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

名称	类型	示例值	描述
StsGrant	Struct		DDoS高防服务的授权状态。
Status	Integer	1	授权状态。取值： • 0：未授权 • 1：已授权

示例

请求示例

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

正常返回示例

`XML` 格式

```
<?xml version="1.0" encoding="UTF-8" ?>
<DescribeStsGrantStatus
<RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
<StsGrant>
<Status>1</Status>
</StsGrant>
</DescribeStsGrantStatus
```

`JSON` 格式

```
{
"RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
"StsGrant": {
"Status": 1
}
}
```

错误码

访问错误中心查看更多错误码。

17.2. DescribeBackSourceCidr

调用DescribeBackSourceCidr查询DDoS高防的回源IP网段。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeBackSourceCidr	要执行的操作。取值：DescribeBackSourceCidr
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
Line	String	否	coop-line-001	要查询的线路。

返回数据

名称	类型	示例值	描述
Cidrs	List	["47.***.***.0/25","47.***.***.128/25"]	DDoS高防的回源IP网段列表。
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。

示例

请求示例

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

正常返回示例

`XML` 格式

```
<DescribeBackSourceCidrResponse>
<RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
<Cidrs>47.***.***.0/25</Cidrs>
<Cidrs>47.***.***.128/25</Cidrs>
</DescribeBackSourceCidrResponse>
```

JSON 格式

```
{
"RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
"Cidrs": [
"47.***.***.0/25",
"47.***.***.128/25"
]
}
```

错误码

访问错误中心查看更多错误码。

17.3. DescribeOpEntities

调用DescribeOpEntities查询DDoS高防（新BGP）的操作日志。

> 说明 该接口仅适用于DDoS高防（新BGP）服务。

操作日志的类型包括：设置实例弹性防护规格、执行黑洞解封、设置近源流量压制、抵扣抗D包、更换ECS IP、清空全量日志等。

调试

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

请求参数

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

名称	类型	是否必选	示例值	描述
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。
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。

名称	类型	示例值	描述
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。 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：

名称	类型	示例值	描述
			• bandwidth：Integer类型，弹性防护带宽，单位：Gbps。
OpDesc	String	{"newEntity":{"actionMethod":"undo"}}	• 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。
RequestId	String	FB24D70C-71F5-4000-8CD8-22CDA0C53CD1	本次请求的ID。

名称	类型	示例值	描述
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。

17.4. DescribeDefenseRecords

调用DescribeDefenseRecords查询DDoS高防（国际）的高级防护日志。

> **说明** 该接口仅适用于DDoS高防（国际）服务。

调试

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

请求参数

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

名称	类型	是否必选	示例值	描述
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
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。

名称	类型	示例值	描述
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。

17.5. DescribeAsyncTasks

调用DescribeAsyncTasks查询异步导出任务的详细信息，例如任务ID、任务开始和结束时间、任务状态、任务参数、任务结果等。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeAsyncTasks	要执行的操作。取值：DescribeAsyncTasks
PageNumber	Integer	是	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写1。
PageSize	Integer	是	10	页面显示的记录数量。最大值：20
RegionId	String	否	cn-hangzhou	DDoS高防服务地域ID。取值： • cn-hangzhou：表示DDoS高防（新BGP）服务 • ap-southeast-1：表示DDoS高防（国际）服务
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
AsyncTasks	Array		异步导出任务的详细信息。
EndTime	Long	157927362000	任务结束时间。时间戳格式，单位：毫秒。
StartTime	Long	156927362000	任务开始时间。时间戳格式，单位：毫秒。
TaskId	Long	1	任务ID。
TaskParams	String	{"instanceId": "ddoscoo-cn-mp91j1ao****"}	任务参数。使用JSON格式的字符串表达。不同TaskType的任务参数不完全相同。 TaskType为1、3、4、5、6时，任务参数的结构如下。 • instanceId：String类型，DDoS高防实例的ID。 TaskType为2时，任务参数的结构如下。 • domain：String类型，网站业务的域名。

名称	类型	示例值	描述
TaskResult	String	{"instanceId": "ddoscoo-cn-mp91j1ao****","url": "https://****.oss-cn-beijing.aliyuncs.com/heap.bin?Expires=1584785140&OSSAccessKeyId=TMP.3KfzD82FyRJevJdEkRX6JEFHhbvRBBb75PZJnyJmksA2QkMm47xFAFDgMhEV8Nm6Vxr8xExMfiy9LsUFAcLcTBrN3rDu3v&Signature=Sj8BNcsxJLE8l5qm4cjNlDt8gv****"}	任务结果。使用JSON格式的字符串表达。不同TaskType的任务参数不完全相同。 TaskType为1、3、4、5、6时，任务参数的结构如下。 • instanceId：String类型，DDoS高防实例的ID。 • url：String类型，导出文件的OSS下载地址。 TaskType为2时，任务参数的结构如下。 • domain：String类型，网站业务的域名。 • url：String类型，导出文件的OSS下载地址。
TaskStatus	Integer	2	任务状态。取值： • 0：任务初始化 • 1：任务进行中 • 2：任务成功 • 3：任务失败
TaskType	Integer	5	任务类型。取值： • 1：四层导出任务，导出DDoS高防实例的端口转发规则 • 2：七层导出任务，导出网站业务转发规则 • 3：会话、健康检查导出任务，导出DDoS高防实例的会话、健康检查配置 • 4：DDoS防护策略导出任务，导出DDoS高防实例的DDoS防护策略配置 • 5：黑名单（针对目的IP）下载任务，导出针对DDoS高防实例的黑名单IP • 6：白名单（针对目的IP）下载任务，导出针对DDoS高防实例的白名单IP
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	本次请求的ID。
TotalCount	Integer	1	异步导出任务的总数。

示例

请求示例

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

正常返回示例

`XML` 格式

```
<DescribeAsyncTasksResponse>
<TotalCount>1</TotalCount>
<RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
<AsyncTasks>
<TaskId>1</TaskId>
<TaskType>5</TaskType>
<TaskStatus>2</TaskStatus>
<StartTime>156927362</StartTime>
<EndTime>157927362</EndTime>
<TaskParams>
<instanceId>ddoscoo-cn-mp91j1ao****</instanceId>
</TaskParams>
<TaskResult>
<instanceId>ddoscoo-cn-mp91j1ao****</instanceId>
<url>https://****.oss-cn-beijing.aliyuncs.com/heap.bin?Expires=1584785140&amp;OSSAccessKeyId=TM
P.3KfzD82FyRJevJdEkRX6JEFHhbvRBBb75PZJnyJmksA2QkMm47xFAFDgMhEV8Nm6Vxr8xExMfiy9LsUFAcLcT
BrN3rDu3v&amp;Signature=Sj8BNcsxJLE8l5qm4cjNlDt8gv****</url>
</TaskResult>
</AsyncTasks>
</DescribeAsyncTasksResponse>
```

`JSON` 格式

```
{
"TotalCount": 1,
"RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
"AsyncTasks": [
{
"TaskId": 1,
"TaskType": 5,
"TaskStatus": 2,
"StartTime": 156927362,
"EndTime": 157927362,
"TaskParams": {
"instanceId": "ddoscoo-cn-mp91j1ao****"
},
"TaskResult": {
"instanceId": "ddoscoo-cn-mp91j1ao****",
"url": "https://****.oss-cn-beijing.aliyuncs.com/heap.bin?Expires=1584785140&OSSAccessKeyId=TMP.3KfzD82FyRJevJdEkRX6JEFHhbvRBBb75PZJnyJmksA2QkMm47xFAFDgMhEV8Nm6Vxr8xExMfiy9LsUFAcLcTBrN3rDu3v&Signature=Sj8BNcsxJLE8l5qm4cjNlDt8gv****"
}
}
]
}
```


错误码

访问错误中心查看更多错误码。

17.6. CreateAsyncTask

调用CreateAsyncTask创建异步导出任务，例如导出网站业务转发规则、端口转发规则、会话保持和健康检查配置、DDoS防护策略、IP黑白名单。

调试

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

请求参数

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

名称	类型	是否必选	示例值	描述
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。

17.7. DeleteAsyncTask

调用DeleteAsyncTask删除异步导出任务。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteAsyncTask	要执行的操作。取值：DeleteAsyncTask
TaskId	Integer	是	1	要删除的任务ID。 说明 您可以调用DescribeAsyncTasks查询所有异步导出任务ID。

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=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。

18.标签

18.1. DescribeTagKeys

调用DescribeTagKeys查询所有标签键。

> 说明 仅DDoS高防（新BGP）服务支持标签功能。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeTagKeys	要执行的操作。取值：DescribeTagKeys。
RegionId	String	是	cn-hangzhou	DDoS高防服务地域ID。取值：cn-hangzhou，表示DDoS高防（新BGP）服务。
ResourceType	String	是	INSTANCE	资源类型。取值：INSTANCE，表示DDoS高防实例。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
PageSize	Integer	否	10	页面显示的记录数量。
PageNumber	Integer	否	1	分页查询请求时返回的页码。例如，查询第一页的返回结果，则填写1。

返回数据

名称	类型	示例值	描述
PageNumber	Integer	1	分页查询请求时返回的页码。
PageSize	Integer	10	页面显示的记录数量。

名称	类型	示例值	描述
RequestId	String	1B0D6FCD-ED11-46B7-9903-D5A45509EC11	本次请求的ID。
TagKeys	Array		标签键信息。
TagCount	Integer	6	标签键关联的资源总数。
TagKey	String	aa1	标签键。
TotalCount	Integer	3	标签键的总数。

示例

请求示例

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

正常返回示例

`XML` 格式

```
<DescribeTagKeysResponse>
<TotalCount>3</TotalCount>
<PageSize>10</PageSize>
<RequestId>1B0D6FCD-ED11-46B7-9903-D5A45509EC11</RequestId>
<PageNumber>1</PageNumber>
<TagKeys>
<TagCount>6</TagCount>
<TagKey>aa1</TagKey>
</TagKeys>
<TagKeys>
<TagCount>1</TagCount>
<TagKey>aa134</TagKey>
</TagKeys>
<TagKeys>
<TagCount>6</TagCount>
<TagKey>aa2</TagKey>
</TagKeys>
</DescribeTagKeysResponse>
```

`JSON` 格式

```
{
"TotalCount":3,
"PageSize":10,
"RequestId":"1B0D6FCD-ED11-46B7-9903-D5A45509EC11",
"PageNumber":1,
"TagKeys":[
{
"TagCount":6,
"TagKey":"aa1"
},
{
"TagCount":1,
"TagKey":"aa134"
},
{
"TagCount":6,
"TagKey":"aa2"
}
]
}
```


错误码

访问错误中心查看更多错误码。

18.2. DescribeTagResources

调用DescribeTagResources查询资源关联的标签信息。

> 说明 仅DDoS高防（新BGP）服务支持标签功能。

调试

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

请求参数

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

名称	类型	是否必选	示例值	描述
RegionId	String	是	cn-hangzhou	DDoS高防服务地域ID。取值：cn-hangzhou，表示DDoS高防（新BGP）服务。
ResourceType	String	是	INSTANCE	资源类型。取值：INSTANCE，表示DDoS高防实例。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
ResourceIds.N	RepeatList	否	ddoscoo-cn-mp91j1ao****	根据资源ID进行筛选，传入要查询的DDoS高防实例的ID。 说明 必须传入ResourceId或者Tag.N.Key和Tag.N.Value的组合。您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
Tags.N.Key	String	否	testkey	根据标签进行筛选，传入要查询的标签键（Key）。 说明 必须传入ResourceId或者Tag.N.Key和Tag.N.Value的组合。Tag.N.Key必须与Tags.N.Value成对存在。
Tags.N.Value	String	否	testvalue	根据标签进行筛选，传入要查询的标签值（Value）。 说明 必须传入ResourceId或者Tag.N.Key和Tag.N.Value的组合。Tag.N.Key必须与Tags.N.Value成对存在。
NextToken	String	否	RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCf****	传入下一个查询开始的Token。如果没有下一个查询，请留空。

返回数据

名称	类型	示例值	描述
NextToken	String	RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCf****	下一个查询开始的Token。没有下一个查询时为空。
RequestId	String	36E698F7-48A4-48D0-9554-0BB4BAAB99B3	本次请求的ID。
TagResources	Array		资源关联的标签信息。
TagResource			
ResourceId	String	ddoscoo-cn-mp91j1ao****	资源ID，具体指DDoS高防实例的ID。
ResourceType	String	INSTANCE	资源类型。取值：INSTANCE，表示DDoS高防实例。
TagKey	String	aa1	资源关联的标签键。
TagValue	String	aa1_1	资源关联的标签值。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeTagResources
&RegionId=cn-hangzhou
&ResourceType=INSTANCE
&ResourceIds.1=ddoscoo-cn-mp91mf6x****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeTagResources>
<NextToken>RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCf****</NextToken>
<RequestId>36E698F7-48A4-48D0-9554-0BB4BAAB99B3</RequestId>
<TagResources>
<ResourceId>ddoscoo-cn-mp91j1ao****</ResourceId>
<TagKey>aa1</TagKey>
<ResourceType>INSTANCE</ResourceType>
<TagValue>aa1_1</TagValue>
</TagResources>
</DescribeTagResources>
```

`JSON` 格式

```
{
"NextToken":"RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCf****",
"RequestId":"36E698F7-48A4-48D0-9554-0BB4BAAB99B3",
"TagResources":[
{
"ResourceId":"ddoscoo-cn-mp91j1ao****",
"TagKey":"aa1",
"ResourceType":"INSTANCE",
"TagValue":"aa1_1"
}
]
}
```

错误码

访问错误中心查看更多错误码。

18.3. CreateTagResources

调用CreateTagResources为资源关联标签。

> 说明 仅DDoS高防（新BGP）服务支持标签功能。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateTagResources	要执行的操作。取值：CreateTagResources。
RegionId	String	是	cn-hangzhou	DDoS高防服务地域ID。取值：cn-hangzhou，表示DDoS高防（新BGP）服务。
ResourceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	要操作的资源ID，具体指DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
ResourceType	String	是	INSTANCE	资源类型。取值：INSTANCE，表示DDoS高防实例。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
Tags.N.Key	String	否	testkey	要关联的标签键。
Tags.N.Value	String	否	testvalue	要关联的标签值。

返回数据

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

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateTagResources
&RegionId=cn-hangzhou
&ResourceIds.1=ddoscoo-cn-mp91j1ao****
&ResourceType=INSTANCE
&Tag.1.Key=testkey
&Tag.1.Value=testvalue
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

访问错误中心查看更多错误码。

18.4. DeleteTagResources

调用DeleteTagResources为资源移除标签。

> 说明 仅DDoS高防（新BGP）服务支持标签功能。

调试

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

请求参数

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

名称	类型	是否必选	示例值	描述
RegionId	String	是	cn-hangzhou	DDoS高防服务地域ID。取值：cn-hangzhou，表示DDoS高防（新BGP）服务。
ResourceIds.N	RepeatList	是	ddoscoo-cn-mp91j1ao****	要操作的资源ID，具体指DDoS高防实例的ID。 说明 您可以调用DescribeInstanceIds查询所有DDoS高防实例的ID信息。
ResourceType	String	是	INSTANCE	资源类型。取值：INSTANCE，表示DDoS高防实例。
ResourceGroupId	String	否	default	DDoS高防实例在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。
TagKey.N	RepeatList	否	testkey	要移除的标签键。
All	Boolean	否	false	是否移除资源上的所有标签。取值： • true：是 • false：否

返回数据

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

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteTagResources
&RegionId=cn-hangzhou
&ResourceIds.1=ddoscoo-cn-mp91j1ao****
&ResourceType=INSTANCE
&All=true
&<公共请求参数>
```

正常返回示例

XML 格式

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

JSON 格式

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

错误码

访问错误中心查看更多错误码。

19.错误码

本文介绍了DDoS高防API调用失败时返回的错误码及其含义。

错误码（Error Code）	描述
DomainNotExist	域名不存在。
DomainExist	域名属于别的用户。
WebRulePortDeny	端口已用于网站业务转发，禁止配置。
InvalidParameter.JSONError	JSON格式不正确。
ExceedFuncSpec	超过功能套餐规格。
ExceedNoStardardPort	无效的非标端口。
InvalidWebRule	无效的网站业务转发规则。
NetworkRuleExist	端口已配置转发规则。
NetworkRuleConflict	端口转发规则冲突。
ExceedWebRuleLimit	超过防护域名数规格。
ExceedNetworkRuleLimit	超过防护端口数规格。
InvalidDomain	无效的域名。
UnBlackholeLimit	超过解除封禁次数限制。
InvalidIp	无效的IP地址/地址段。
DomainOwnerError	域名属于别的用户。
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。

20.中国地区&国家和地域代码

本文介绍了在调用DDoS高防的基础设施防护策略-区域封禁和查询请求来源分布相关接口时用到的中国地区代码、国家和地域代码，方便您查询使用。

相关接口

本文描述的中国地区代码、国家和地域代码适用于在调用以下相关接口时查询使用。

类型	接口	使用场景
基础设施防护策略-区域封禁	ConfigNetworkRegionBlock	查询请求参数Config结构中的Countries和Provinces参数的取值。
	DescribeNetworkRegionBlock	查询返回参数Config结构中的Countries和Provinces参数的取值。
监控报表	DescribeDomainViewSourceCountries	查询返回参数CountryId对应的国家和地域名称。
	DescribeDomainViewSourceProvinces	查询返回参数ProvinceId对应的中国地区名称。
	DescribePortViewSourceCountries	查询返回参数CountryId对应的国家和地域名称。
	DescribePortViewSourceProvinces	查询返回参数ProvinceId对应的中国地区名称。

中国地区代码

① 适用于基础设施防护策略-区域封禁相关接口。

② 适用于监控报表相关接口。

名称	代码 ①	ProvinceId ②
北京市	11	110000
天津市	12	120000
河北省	13	130000
山西省	14	140000
内蒙古自治区	15	150000
辽宁省	21	210000
吉林省	22	220000
黑龙江省	23	230000
上海市	31	310000

名称	代码 ①	ProvinceId ②
江苏省	32	320000
浙江省	33	330000
安徽省	34	340000
福建省	35	350000
江西省	36	360000
山东省	37	370000
河南省	41	410000
湖北省	42	420000
湖南省	43	430000
广东省	44	440000
广西壮族自治区	45	450000
海南省	46	460000
重庆市	50	500000
四川省	51	510000
贵州省	52	520000
云南省	53	530000
西藏自治区	54	540000
陕西省	61	610000
甘肃省	62	620000
青海省	63	630000
宁夏回族自治区	64	640000
新疆维吾尔自治区	65	650000
香港特别行政区	81	810000
台湾省	71	710000
澳门特别行政区	82	820000

国家和地域代码

① 适用于基础设施防护策略-区域封禁相关接口。

② 适用于监控报表相关接口。

名称	代码 ①	CountryId ②
中国	1	CN
澳大利亚	2	AU
日本	3	JP
泰国	4	TH
印度	5	IN
美国	7	US
德国	8	DE
荷兰	9	NL
马来西亚	10	MY
安哥拉	11	AO
韩国	12	KR
新加坡	13	SG
柬埔寨	14	KH
菲律宾	16	PH
越南	17	VN
法国	18	FR
波兰	19	PL
西班牙	20	ES
俄罗斯	21	RU
瑞士	22	CH
英国	23	GB
意大利	24	IT
捷克	25	CZ
爱尔兰	26	IE

名称	代码 ①	CountryId ②
丹麦	27	DK
葡萄牙	28	PT
瑞典	29	SE
加纳	30	GH
土耳其	31	TR
喀麦隆	32	CM
南非	33	ZA
芬兰	34	FI
匈牙利	35	HU
阿联酋	36	AE
希腊	37	GR
巴西	38	BR
奥地利	39	AT
约旦	40	JO
比利时	41	BE
罗马尼亚	42	RO
卢森堡	43	LU
阿根廷	44	AR
乌干达	45	UG
亚美尼亚	46	AM
坦桑尼亚	47	TZ
布隆迪	48	BI
乌拉圭	49	UY
保加利亚	50	BG
乌克兰	51	UA
以色列	52	IL

名称	代码 ①	CountryId ②
卡塔尔	53	QA
伊拉克	54	IQ
立陶宛	55	LT
摩尔多瓦	56	MD
乌兹别克斯坦	57	UZ
斯洛伐克	58	SK
哈萨克斯坦	59	KZ
克罗地亚	60	HR
格鲁吉亚	61	GE
爱沙尼亚	62	EE
直布罗陀	63	GI
拉脱维亚	64	LV
挪威	65	NO
巴勒斯坦	66	PS
塞浦路斯	67	CY
沙特阿拉伯	68	SA
伊朗	69	IR
加拿大	70	CA
美属萨摩亚	71	AS
叙利亚	72	SY
科威特	73	KW
巴林	74	BH
黎巴嫩	75	LB
阿曼	76	OM
阿塞拜疆	77	AZ
赞比亚	78	ZM

名称	代码 ①	CountryId ②
津巴布韦	79	ZW
刚果民主共和国	80	CD
塞尔维亚	81	RS
冰岛	82	IS
斯洛文尼亚	83	SI
马其顿	84	MK
列支敦士登	85	LI
泽西岛	86	JE
波斯尼亚和黑塞哥维那（波黑）	87	BA
智利	88	CL
秘鲁	89	PE
吉尔吉斯斯坦	90	KG
留尼汪岛	91	RE
塔吉克斯坦	92	TJ
马恩岛	93	IM
根西岛	94	GG
马耳他	95	MT
利比亚	96	LY
也门	97	YE
白俄罗斯	98	BY
马约特	99	YT
瓜德罗普	100	GP
法属圣马丁	101	MF
马提尼克	102	MQ
圭亚那	103	GY
科索沃	104	XK

名称	代码 ①	CountryId ②
印度尼西亚	105	ID
北马里亚纳群岛	106	MP
多米尼加	107	DO
墨西哥	108	MX
关岛	109	GU
尼日利亚	110	NG
委内瑞拉	111	VE
波多黎各	112	PR
蒙古	113	MN
新西兰	114	NZ
孟加拉	115	BD
巴基斯坦	116	PK
巴布亚新几内亚	117	PG
特立尼达和多巴哥	118	TT
莱索托	119	LS
哥伦比亚	120	CO
哥斯达黎加	121	CR
厄瓜多尔	123	EC
斯里兰卡	124	LK
埃及	125	EG
英属维尔京群岛	126	VG
牙买加	127	JM
圣卢西亚	128	LC
开曼群岛	129	KY
格林纳达	130	GD
库拉索	131	CW

名称	代码 ①	CountryId ②
巴拿马	132	PA
巴巴多斯	133	BB
巴哈马	134	BS
尼泊尔	135	NP
托克劳	136	TK
马尔代夫	137	MV
阿富汗	138	AF
新喀里多尼亚	139	NC
斐济	140	FJ
瓦利斯和富图纳群岛	141	WF
阿尔巴尼亚	142	AL
圣马力诺	143	SM
黑山	144	ME
东帝汶	145	TL
摩纳哥	146	MC
几内亚	147	GN
缅甸	148	MM
格陵兰	149	GL
百慕大	150	BM
圣文森特和格林纳丁斯	151	VC
美属维尔京群岛	152	VI
苏里南	153	SR
圣巴泰勒米	154	BL
海地	155	HT
安提瓜和巴布达	156	AG
利比里亚	157	LR

名称	代码 ①	CountryId ②
肯尼亚	158	KE
博茨瓦纳	159	BW
莫桑比克	160	MZ
塞内加尔	161	SN
马达加斯加	162	MG
纳米比亚	163	NA
科特迪瓦	164	CI
苏丹	165	SD
马拉维	166	MW
加蓬	167	GA
马里	168	ML
贝宁	169	BJ
乍得	170	TD
佛得角	171	CV
卢旺达	172	RW
刚果共和国	173	CG
冈比亚	174	GM
毛里求斯	175	MU
阿尔及利亚	176	DZ
斯威士兰	177	SZ
布基纳法索	178	BF
塞拉利昂	179	SL
索马里	180	SO
尼日尔	181	NE
中非	182	CF
多哥	183	TG

名称	代码 ①	CountryId ②
南苏丹	184	SS
赤道几内亚	185	GQ
塞舌尔	186	SC
吉布提	187	DJ
摩洛哥	188	MA
毛里塔尼亚	189	MR
科摩罗	190	KM
英属印度洋领地	191	IO
突尼斯	192	TN
老挝	193	LA
文莱	194	BN
不丹	195	BT
瑙鲁	196	NR
瓦努阿图	197	VU
密克罗尼西亚联邦	198	FM
法属波利尼西亚	199	PF
汤加	200	TO
洪都拉斯	201	HN
玻利维亚	202	BO
萨尔瓦多	203	SV
危地马拉	204	GT
尼加拉瓜	205	NI
伯利兹	206	BZ
巴拉圭	207	PY
法属圭亚那	208	GF
安道尔	209	AD

名称	代码 ①	CountryId ②
法罗群岛	210	FO
纽埃	211	NU
基里巴斯	212	KI
马绍尔群岛	213	MH
帕劳	214	PW
萨摩亚	215	WS
所罗门群岛	216	SB
图瓦卢	217	TV
朝鲜	218	KP
梵蒂冈	219	VA
厄立特里亚	220	ER
埃塞俄比亚	221	ET
几内亚比绍	222	GW
圣多美和普林西比	223	ST
土库曼斯坦	224	TM
古巴	225	CU
多米尼克	226	DM
圣基茨和尼维斯	227	KN
阿鲁巴	228	AW
福克兰群岛	229	FK
特克斯和凯科斯群岛	230	TC
荷兰加勒比	231	BQ
荷属圣马丁	232	SX
蒙塞拉特岛	233	MS
安圭拉	234	AI
圣皮埃尔和密克隆群岛	235	PM

名称	代码 ①	CountryId ②
奥兰群岛	236	AX
诺福克岛	237	NF
南极洲	238	AQ
库克群岛	239	CK
圣诞岛	240	CX
欧洲其他	241	EU