

ALIBABA CLOUD

阿里云

DDoS防护
DDoS原生防护

文档版本：20201117

 阿里云

法律声明

阿里云提醒您在使用或阅读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 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录


1.2017-11-20版本	06
1.1. API概览	06
1.2. 调用方式	06
1.3. 公共参数	08
1.4. 代播实例	10
1.4.1. DescribeOnDemandInstance	10
1.4.2. ModifyOnDemaondDefenseStatus	13
1.4.3. DescribeTopTraffic	15
2.2018-07-20版本	18
2.1. API概览	18
2.2. 调用方式	19
2.3. 公共参数	21
2.4. 防护	23
2.4.1. AddIp	23
2.4.2. Deletelp	25
2.4.3. DeleteBlackhole	26
2.5. 实例	27
2.5.1. DescribeRegions	28
2.5.2. DescribeInstanceList	31
2.5.3. DescribeInstanceSpecs	35
2.5.4. DescribeExcpetionCount	38
2.5.5. DescribePackIpList	40
2.5.6. ModifyRemark	42
2.5.7. CheckGrant	44
2.6. 流量包	45
2.6.1. DescribeResourcePackInstances	45

2.6.2. DescribeResourcePackStatistics	48
2.6.3. DescribeResourcePackUsage	50
2.6.4. DescribePackPaidTraffic	52
2.7. 图表日志	55
2.7.1. DescribeDdosEvent	55
2.7.2. DescribeOpEntities	58
2.7.3. DescribeTraffic	61
2.7.4. DescribeOnDemandDdosEvent	64
2.8. 标签	67
2.8.1. ListTagKeys	67
2.8.2. ListTagResources	71
2.8.3. TagResources	75
2.8.4. UntagResources	76
2.9. 代播防护	78
2.9.1. DescribeOnDemandInstanceStatus	78
2.9.2. SetInstanceModeOnDemand	82
2.9.3. CreateSchedruleOnDemand	84
2.9.4. QuerySchedruleOnDemand	87
2.9.5. ConfigSchedruleOnDemand	91
2.9.6. DeleteSchedruleOnDemand	94

1.2017-11-20版本

1.1. API概览

本文汇总了DDoS原生防护（防护包）服务的所有可调用的2017-11-20版本的API，具体接口信息请参见相关文档。

 **注意** DDoS原生防护（防护包）的API接口目前仅对DDoS原生防护企业版实例开放。在使用以下接口前，请确认您已经开通了DDoS原生防护企业版实例。更多信息，请参见[开通DDoS原生防护企业版](#)。

代播实例

代播实例可以防护海外线下IDC服务器或云上资产通过网段实现DDoS原生防护。更多信息，请参见[资产中心](#)。

接口	描述
DescribeOnDemandInstance	查询代播实例信息。
ModifyOnDemandDefenseStatus	修改代播实例的防护状态。
DescribeTopTraffic	查询指定时间段内，代播实例上牵引流量最大的前N个IP信息。

1.2. 调用方式

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

请求结构

DDoS原生防护的API是RPC风格，您可以通过发送HTTP GET请求调用DDoS原生防护API。请求结构如下：

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

参数释义：

- Endpoint：DDoS原生防护API的服务接入地址。

Endpoint	支持的地域
----------	-------

Endpoint	支持的地域
ddosbgp.aliyuncs.com	<ul style="list-style-type: none"> ○ 中国内地 <ul style="list-style-type: none"> ■ 华东1（杭州）：cn-hangzhou ■ 华东2（上海）：cn-shanghai ■ 华北1（青岛）：cn-qingdao ■ 华北2（北京）：cn-beijing ■ 华北3（张家口）：cn-zhangjiakou ■ 华北5（呼和浩特）：cn-huhehaote ■ 华北6（乌兰察布）：cn-wulanchabu ■ 华南1（深圳）：cn-shenzhen ■ 华南2（河源）：cn-heyuan ■ 西南1（成都）：cn-chengdu ○ 海外地区 <ul style="list-style-type: none"> ■ 英国（伦敦）：eu-west-1 ■ 德国（法兰克福）：eu-central-1 ■ 日本（东京）：ap-northeast-1 ■ 澳大利亚（悉尼）：ap-southeast-2 ■ 马来西亚（吉隆坡）：ap-southeast-3 ■ 印度尼西亚（雅加达）：ap-southeast-5 ■ 印度（孟买）：ap-south-1 ■ 阿联酋（迪拜）：me-east-1 ■ 俄罗斯（莫斯科）：rus-west-1
ddosbgp.cn-hongkong.aliyuncs.com	中国香港：cn-hongkong
ddosbgp.ap-southeast-1.aliyuncs.com	新加坡：ap-southeast-1
ddosbgp.us-west-1.aliyuncs.com	美国（硅谷）：us-west-1
ddosbgp.us-east-1.aliyuncs.com	美国（弗吉尼亚）：us-east-1

- Action：要执行的操作。例如使用DescribeInstanceList 查询DDoS原生防护的实例信息。
- Version：要使用的API版本，该目录下DDoS原生防护API的版本是2017-11-20。
- Parameters：请求参数。多个参数之间用“&”连接。

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

下面是一个调用DescribeInstanceList 接口查询DDoS原生防护实例信息的示例：

 **说明** 为了便于您查看，本文档中的示例都做了格式化处理。

```
https://ddosbgp.aliyuncs.com/?Action=DescribeOnDemandInstance
&DdosRegionId=cn-hangzhou
&InstanceId=ddosbgp-cn-xxx
&Format=xml
&Version=2017-11-20
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2012-06-01T12:00:00Z
```

API授权

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

API签名

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

RPC API需按如下格式在请求中增加签名（Signature）：

```
https://endpoint/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&Signature=CT9X0VtwR86fNWSnsc
6v8YGOjuE%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
```

1.3. 公共参数

公共请求参数是每个接口都需要使用到的请求参数。

公共请求参数

名称	类型	是否必需	描述
----	----	------	----

名称	类型	是否必需	描述
DdosRegionId	String	是	DDoS防护包实例所在的地域。取值： <ul style="list-style-type: none"> cn-hangzhou cn-shanghai cn-qingdao cn-beijing cn-zhangjiakou cn-huhehaote cn-shenzhen cn-hongkong us-west-1
Format	String	否	返回消息的格式。取值： <ul style="list-style-type: none"> JSON（默认） XML
Version	String	是	API版本号，使用YYYY-MM-DD日期格式。取值：2017-11-20。
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，格式为YYYY-MM-DDThh:mm:ssZ。 例如，北京时间2013年1月10日20点0分0秒，表示为2013-01-10T12:00:00Z。
SignatureVersion	String	是	签名算法版本，取值：1。
SignatureNonce	String	是	唯一随机数，用于防止网络重放攻击。在不同请求间要使用不同的随机数值。
ResourceOwnerAccount	String	否	本次API请求访问到的资源所有者账户，即登录用户名。

示例

```
https://ddosbgp.aliyuncs.com/?Action=DescribeOnDemandInstance
&DdosRegionId=cn-hangzhou
&InstanceId=ddosbgp-cn-xxx
&Format=xml
&Version=2017-11-20
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2012-06-01T12:00:00Z
```

公共返回参数

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

每次接口调用，无论成功与否，系统都会返回一个唯一识别码RequestId。

- XML格式

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


- JSON格式

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

1.4. 代播实例

1.4.1. DescribeOnDemandInstance

调用DescribeOnDemandInstance查询代播实例的详细信息。

 **说明** 代播实例可以防护海外云下IDC服务器或在云上按照网段去实现DDoS防护，目前仅支持联系销售人员购买。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeOnDemandInstance	要执行的操作。取值： DescribeOnDemandInstance 。
PageNo	Integer	是	1	列表的页码，默认值为1。
PageSize	Integer	是	10	分页查询时每页的行数，最大值为50，默认值为10。
RegionId	String	否	cn-zhangjiakou	代播实例的地域ID。 <div style="border: 1px solid #ccc; padding: 5px; background-color: #e6f2ff;"> ? 说明 您可以调用DescribeRegions查询DDoS原生防护支持的所有地域信息。 </div>

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

调用API的请求格式，请参见本文[示例](#)中的请求示例。

返回数据

名称	类型	示例值	描述
Instances	Array of Instance		代播实例的详情。
DefenseStatus	String	Defense	代播实例的防护状态。取值： <ul style="list-style-type: none"> Defense：代播防护已开启，代播IP为资产流量提供牵引和防护。 UnDefense：代播防护已关闭。
Instanceid	String	ddosbgp-cn-z2q1qzxb****	代播实例的ID。
Ipnet	List	47.***.***.0/24	代播实例的IP网段。
RegionId	String	cn-zhangjiakou	代播实例的地域ID。

名称	类型	示例值	描述
Remark	String	123	代播实例的备注信息。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
Total	String	1	代播实例的总数。

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribeOnDemandInstanceResponse>
  <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
  <Total>1</Total>
  <Instances>
    <InstanceId>ddosbgp-cn-z2q1qzxb****</InstanceId>
    <Ipnet>47.***.***.0/24</Ipnet>
    <Remark>123</Remark>
    <RegionId>cn-zhangjiakou</RegionId>
    <DefenseStatus>Defense</DefenseStatus>
  </Instances>
</DescribeOnDemandInstanceResponse>
```

JSON 格式

```
{
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
  "Total": "1",
  "Instances": [
    {
      "InstanceId": "ddosbgp-cn-z2q1qzxb****",
      "Ipnet": [
        "47.***.***.0/24"
      ],
      "Remark": "123",
      "RegionId": "cn-zhangjiakou",
      "DefenseStatus": "Defense"
    }
  ]
}
```

错误码

访问[错误中心](#)查看更多错误码。

1.4.2. ModifyOnDemaondDefenseStatus

调用ModifyOnDemaondDefenseStatus修改代播实例的防护状态。

 **说明** DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

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

请求参数

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

名称	类型	是否必选	示例值	描述
DdosRegionId	String	是	cn-hangzhou	代播实例的地域ID。  说明 您可以调用 DescribeRegions 查询所有地域信息。
DefenseStatus	String	是	Defense	设置代播实例的防护状态，可选值： <ul style="list-style-type: none"> • Defense：开启牵引 • UnDefense：关闭牵引
InstanceId	String	是	ddosbgp-xxx	要操作的代播实例的ID。

返回数据

名称	类型	示例值	描述
RequestId	String	4C467B38-3910-447D-87BC-AC049166F216	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyOnDemaondDefenseStatus
&DdosRegionId=cn-hangzhou
&DefenseStatus=Defense
&InstanceId=ddosbgp-xxx
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ModifyOnDemaondDefenseStatusResponse>
  <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
</ModifyOnDemaondDefenseStatusResponse>
```

JSON 格式

```
{
  "RequestId":"4C467B38-3910-447D-87BC-AC049166F216"
}
```

错误码

访问[错误中心](#)查看更多错误码。

1.4.3. DescribeTopTraffic

调用DescribeTopTraffic查询指定时间段内，代播实例上牵引流量最大的前N个IP信息。

 **说明** DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeTopTraffic	要执行的操作。取值： DescribeTopTraffic 。
EndTime	String	是	1563445054	指定查询结束时间，秒级时间戳。
InstanceId	String	是	ddosbgp-xxx	要查询的代播实例的ID。
StartTime	String	是	1560853054	指定查询开始时间，秒级时间戳。
Ipnet	String	否	1.1.1.0/24	要查询的代播实例的IP网段。
Rn	Integer	否	1	指定查询牵引流量最大的前几个IP。默认为1，即查询牵引流量最大的IP。
PageNo	Integer	否	1	列表的页码，默认值为1。
PageSize	Integer	否	10	分页查询时每页的行数，最大值为50，默认值为10。

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

返回数据

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
Total	Long	1	返回结果的总数。
TrafficList	Array		牵引流量信息。
Pps	Integer	100000	牵引总数据包数，单位：pps。
Bps	Integer	2919212	牵引总流量大小，单位：Kbps。
AttackBps	Integer	0	攻击流量大小，单位：Kbps。
AttackPps	Integer	0	攻击数据包数，单位：pps。
Ip	String	1.1.1.1	代播IP地址。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeTopTraffic
&EndTime=1563445054
&InstanceId=ddosbgp-xxx
&StartTime=1560853054
&<公共请求参数>
```

正常返回示例

XML 格式


```
<DescribeTopTrafficResponse>
  <code>200</code>
  <requestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</requestId>
  <success>>true</success>
  <data>
    <Pps>100000</Pps>
    <Bps>2919212</Bps>
    <Ip>1.1.1.1</Ip>
    <AttackBps>0</AttackBps>
    <AttackPps>0</AttackPps>
  </data>
</DescribeTopTrafficResponse>
```

JSON 格式

```
{
  "code": 200,
  "Total": "1",
  "requestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
  "success": true,
  "data": {
    "Pps": 100000,
    "Bps": 2919212,
    "Ip": "1.1.1.1",
    "AttackBps": 0,
    "AttackPps": 0
  }
}
```


错误码

访问[错误中心](#)查看更多错误码。

2.2018-07-20版本

2.1. API概览

本文汇总了DDoS原生防护（防护包）服务的所有可调用的2018-07-20版本的API，具体接口信息请参见相关文档。

 **注意** DDoS原生防护（防护包）的API接口目前仅对DDoS原生防护企业版实例开放。在使用以下接口前，请确认您已经开通了DDoS原生防护企业版实例。更多信息，请参见[开通DDoS原生防护企业版](#)。


防护设置

接口	描述
AddIps	为DDoS原生防护实例添加防护对象IP。
DeleteIps	将被防护IP从原生防护实例中移除，取消防护。
DeleteBlackhole	为被防护IP解除黑洞状态。

实例

接口	描述
DescribeRegions	查询DDoS原生防护服务支持的地域信息。
DescribeInstanceList	查询原生防护实例的详细信息。
DescribeInstanceSpecs	查询原生防护实例的规格信息。
DescribeExceptionCount	查询异常原生防护实例的信息。
DescribePackIpsList	查询原生防护实例的防护IP列表信息。
ModifyRemark	修改DDoS原生防护实例的备注。
CheckGrant	检查DDoS原生防护服务的授权状态，即是否授权DDoS原生防护查询您的ECS服务器信息。

抗D流量包

 **说明** 从2019年12月起，DDoS原生防护（防护包）新购和续费按照业务规模预付费，未到期实例免除抗D流量包费用。更多信息，请参见[DDoS原生防护计费方式](#)。

接口	描述
DescribeResourcePacks	查询抗D流量包的详细信息。

接口	描述
DescribeResourcePackStatistics	查询抗D流量包的统计信息。
DescribeResourcePackUsage	查询抗D流量包的使用明细。
DescribePackPaidTraffic	查询付费流量明细。

图表日志

接口	描述
DescribeDdosEvent	查询指定原生防护实例上的DDoS事件。
DescribeOpEntities	查询用户的操作日志。
DescribeTraffic	查询指定原生防护实例上的流量信息。
DescribeOnDemandDdosEvent	查询DDoS防护代播实例上的DDoS事件。

标签

接口	描述
ListTagKeys	查询所有标签。
TagResources	为指定原生防护实例绑定标签。
UntagResources	移除指定原生防护实例的标签。
ListTagResources	查询原生防护实例和标签的对应关系。

代播防护

2.2. 调用方式

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

请求结构

DDoS原生防护API是RPC风格，您可以通过发送HTTP GET请求调用DDoS原生防护API。其请求结构如下：

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

参数释义：


- Endpoint：DDoS原生防护API的服务接入地址。

Endpoint	支持的地域
ddosbgp.aliyuncs.com	<ul style="list-style-type: none"> ○ 中国内地 <ul style="list-style-type: none"> ■ 华东1（杭州）：cn-hangzhou ■ 华东2（上海）：cn-shanghai ■ 华北1（青岛）：cn-qingdao ■ 华北2（北京）：cn-beijing ■ 华北3（张家口）：cn-zhangjiakou ■ 华北5（呼和浩特）：cn-huhehaote ■ 华北6（乌兰察布）：cn-wulanchabu ■ 华南1（深圳）：cn-shenzhen ■ 华南2（河源）：cn-heyuan ■ 西南1（成都）：cn-chengdu ○ 海外地区 <ul style="list-style-type: none"> ■ 英国（伦敦）：eu-west-1 ■ 德国（法兰克福）：eu-central-1 ■ 日本（东京）：ap-northeast-1 ■ 澳大利亚（悉尼）：ap-southeast-2 ■ 马来西亚（吉隆坡）：ap-southeast-3 ■ 印度尼西亚（雅加达）：ap-southeast-5 ■ 印度（孟买）：ap-south-1 ■ 阿联酋（迪拜）：me-east-1 ■ 俄罗斯（莫斯科）：rus-west-1
ddosbgp.cn-hongkong.aliyuncs.com	中国香港：cn-hongkong
ddosbgp.ap-southeast-1.aliyuncs.com	新加坡：ap-southeast-1
ddosbgp.us-west-1.aliyuncs.com	美国（硅谷）：us-west-1
ddosbgp.us-east-1.aliyuncs.com	美国（弗吉尼亚）：us-east-1

- Action: 要执行的操作。例如使用DescribeInstanceList 查询DDoS原生防护的实例信息。
- Version: 要使用的API版本。当前目录下DDoS原生防护API的版本是2018-07-20。
- Parameters: 请求参数，多个参数之间用“&”连接。

请求参数由公共请求参数和API自定义参数组成。公共参数中包含API版本号、身份验证等信息，详情参见[公共参数](#)。

下面是一个调用DescribeInstanceList 接口查询DDoS原生防护实例信息的示例：

 **说明** 为了便于您查看，本文档中的示例都做了格式化处理。

```
https://ddosbgp.aliyuncs.com/?Action=DescribeInstanceList
&DdosRegionId=cn-hangzhou
&InstanceId=ddosbgp-cn-xxx
&Format=xml
&Version=2018-07-20
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2012-06-01T12:00:00Z
```

API授权

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

API签名

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

RPC API需按如下格式在请求中增加签名（Signature）：

```
https://endpoint/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&Signature=CT9X0VtwR86fNWSnsc
6v8YGOjuE%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
```

2.3. 公共参数

公共请求参数是每个接口都需要使用到的请求参数。

公共请求参数

名称	类型	是否必需	描述
----	----	------	----

名称	类型	是否必需	描述
DdosRegionId	String	是	DDoS防护包实例所在的地域。取值： <ul style="list-style-type: none"> cn-hangzhou cn-shanghai cn-qingdao cn-beijing cn-zhangjiakou cn-huhehaote cn-shenzhen cn-hongkong us-west-1
Format	String	否	返回消息的格式。取值： <ul style="list-style-type: none"> JSON（默认） XML
Version	String	是	API版本号，使用YYYY-MM-DD日期格式。取值：2018-07-20。
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，格式为YYYY-MM-DDThh:mm:ssZ。 例如，北京时间2013年1月10日20点0分0秒，表示为2013-01-10T12:00:00Z。
SignatureVersion	String	是	签名算法版本，取值：1。
SignatureNonce	String	是	唯一随机数，用于防止网络重放攻击。在不同请求间要使用不同的随机数值。
ResourceOwnerAccount	String	否	本次API请求访问到的资源拥有者账户，即登录用户名。

示例

```
https://ddosbgp.aliyuncs.com/?Action=DescribeInstanceList
&DdosRegionId=cn-hangzhou
&InstanceId=ddosbgp-cn-xxx
&Format=xml
&Version=2018-07-20
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2012-06-01T12:00:00Z
```

公共返回参数

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

每次接口调用，无论成功与否，系统都会返回一个唯一识别码RequestId。

- XML格式

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

- JSON格式

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

2.4. 防护

2.4.1. AddIp

调用AddIp接口为DDoS防护包添加防护对象IP。

 **说明** DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	AddIp	系统规定参数。取值： AddIp 。
InstanceId	String	是	ddosbgp-cn-12345678	要操作的防护包实例ID。
IpList	String	是	[{"ip":"1.1.1.1"}, {"ip":"2.2.2.2"}]	添加到防护包进行防护的IP，支持添加过个IP。
ResourceGroupId	String	否	test	资源组ID。
ResourceRegionId	String	否	cn-hangzhou	地域ID。

返回数据

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

示例

请求示例

```
http(s)://[Endpoint]/?Action=AddIp
&InstanceId=ddosbgp-cn-12345678
&IpList=[{"ip":"1.1.1.1"}, {"ip":"2.2.2.2"}]
&<公共请求参数>
```

正常返回示例

XML 格式

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


JSON 格式

```
{
  "RequestId":"4C467B38-3910-447D-87BC-AC049166F216"
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.4.2. DeleteIp

调用DeleteIp接口将被防护IP从防护包中移除，取消防护。

 说明 DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteIp	要执行的操作，取值： DeleteIp 。
InstanceId	String	是	ddosbgp-cn-xxx	要操作的防护包ID。
IpList	String	是	[{"ip":"1.1.1.1"}, {"ip":"2.2.2.2"}]	要从防护包中移除的被防护IP，支持填写多个IP。
ResourceGroupId	String	否	xx	资源组ID。
ResourceRegionId	String	否	cn-hangzhou	地域ID。

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=DeleteIp
&InstanceId=ddosbgp-cn-xxx
&IpList=1.1.1.1,2.2.2.2
&<公共请求参数>
```

正常返回示例

XML 格式

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

JSON 格式

```
{
  "RequestId": "4C467B38-3910-447D-87BC-AC049166F216"
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.4.3. DeleteBlackhole

调用DeleteBlackhole接口为被防护IP解除黑洞状态。

 说明 DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteBlackhole	系统规定参数。取值： DeleteBlackhole 。
InstanceId	String	是	ddosbgp-cn-xxx	要操作的防护包实例ID。

名称	类型	是否必选	示例值	描述
Ip	String	是	1.1.1.1	要解除黑洞状态的被防护IP。
ResourceGroupId	String	否	xx	资源组ID。
ResourceRegionId	String	否	cn-hangzhou	地域ID。

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=DeleteBlackhole
&InstanceId=ddosbgp-cn-xxx
&Ip=1.1.1.1
&<公共请求参数>
```

正常返回示例

XML 格式

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

JSON 格式

```
{
  "RequestId": "4C467B38-3910-447D-87BC-AC049166F216"
}
```


错误码

访问[错误中心](#)查看更多错误码。

2.5. 实例

2.5.1. DescribeRegions

调用DescribeRegions接口查看支持DDoS防护包服务的地域信息。

 **说明** DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeRegions	要执行的操作，取值： DescribeRegions 。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
Code	String	true	响应状态码。
Regions	Array		防护包支持的地域信息。
RegionEnName	String	shanghai	地域英文名称。
RegionId	String	cn-shanghai	地域ID。
RegionName	String	上海	地域中文名称。
RequestId	String	C3D66E07-41BF-41B7-A4BF-83A9E08E1C09	本次请求的ID。
Success	Boolean	true	是否成功调用请求。

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribeRegionsResponse>
  <RequestId>C3D66E07-41BF-41B7-A4BF-83A9E08E1C09</RequestId>
  <Regions>
    <Region>
      <RegionId>cn-shenzhen</RegionId>
    </Region>
    <Region>
      <RegionId>cn-qingdao</RegionId>
    </Region>
    <Region>
      <RegionId>cn-beijing</RegionId>
    </Region>
    <Region>
      <RegionId>cn-shanghai</RegionId>
    </Region>
    <Region>
      <RegionId>cn-hongkong</RegionId>
    </Region>
    <Region>
      <RegionId>cn-huhehaote</RegionId>
    </Region>
    <Region>
      <RegionId>cn-zhangjiakou</RegionId>
    </Region>
    <Region>
      <RegionId>us-west-1</RegionId>
    </Region>
    <Region>
      <RegionId>cn-hangzhou</RegionId>
    </Region>
  </Regions>
  <Success>>true</Success>
  <Code>200</Code>
</DescribeRegionsResponse>
```

JSON 格式


```
{
  "RequestId":"9C48E43E-58A6-4A08-A858-4C9BB9631870",
  "Regions":[
    {
      "RegionId":"cn-shenzhen"
    },
    {
      "RegionId":"cn-qingdao"
    },
    {
      "RegionId":"cn-beijing"
    },
    {
      "RegionId":"cn-shanghai"
    },
    {
      "RegionId":"cn-hongkong"
    },
    {
      "RegionId":"cn-huhehaote"
    },
    {
      "RegionId":"cn-zhangjiakou"
    },
    {
      "RegionId":"us-west-1"
    },
    {
      "RegionId":"cn-hangzhou"
    }
  ],
  "Success":true,
  "Code":"200"
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.5.2. DescribeInstanceList

调用DescribeInstanceList接口查询防护包实例的详细信息。

 **说明** DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstanceList	要执行的操作，取值： DescribeInstanceList 。
PageNo	Integer	是	1	列表的页码，默认值为1。
PageSize	Integer	是	10	分页查询时每页的行数，最大值为50，默认值为10。
ResourceGroupId	String	否	test	资源组ID。
InstanceIdsList	String	否	['ddosbgp-cn-xx','ddosbpg-cn-xxx']	指定要查询的防护包实例ID，多个ID间用逗号分隔。以JSON数组串格式传入，例如， <code>['ddosbgp-cn-xx','ddosbpg-cn-xxx']</code> 。  说明 若不传入该参数，则返回所有防护包信息。
Remark	String	否	test	指定要查询的防护包实例的备注。  说明 若不传入该参数，则返回所有防护包信息。
DdosRegionId	String	否	cn-hangzhou	实例所在地区ID。

名称	类型	是否必选	示例值	描述
IpVersion	String	否	IPv4	<p>指定要查询的防护包实例的防护IP类型，取值：</p> <p>? 说明 若不传入该参数，则返回所有防护包信息。</p> <ul style="list-style-type: none"> • IPv4 • IPv6
InstanceType	String	否	0	<p>指定要查询的防护包实例的类型，取值：</p> <p>? 说明 若不传入该参数，则返回所有防护包信息。</p> <ul style="list-style-type: none"> • 0：专业版 • 1：企业版
Ip	String	否	1.1.1.1	<p>指定要查询的防护包实例的防护对象IP。</p> <p>? 说明 若不传入该参数，则返回所有防护包信息。</p>
Orderby	String	否	expireTime	<p>排序字段，取值：expireTime（到期时间）。</p>
Orderdire	String	否	asc	<p>排序方向，取值：</p> <ul style="list-style-type: none"> • desc：倒序 • asc：顺序
Tag.N.Key	String	否	test	<p>标签的Key值。若有多个标签，依次传入Tag.1.Key、Tag.2.Key、Tag.3.Key ...</p>
Tag.N.Value	String	否	test	<p>标签的Value值。若有多个标签，依次传入Tag.1.Value、Tag.2.Value、Tag.3.Value ...</p>

返回数据

名称	类型	示例值	描述
InstanceList	Array		防护包实例的详细信息。

名称	类型	示例值	描述
AutoRenewal	Boolean	false	是否开启自动续费。
BlackholdingCount	String	0	防护包中正在黑洞中的IP数量。
ExpireTime	Long	1560009600000	防护包的到期时间。
GmtCreate	Long	1554708159000	防护包的创建时间。
InstanceId	String	ddosbgp-cn-xx	防护包实例ID。
InstanceType	String	1	防护包实例的类型，取值： <ul style="list-style-type: none"> 0：专业版 1：企业版
IpType	String	IPv4	防护包的防护IP类型，取值： <ul style="list-style-type: none"> IPv4 IPv6
Product	String	SLB	防护对象的产品类型，取值： <ul style="list-style-type: none"> ECS SLB EIP WAF
Remark	String	test	防护包的备注。
Status	String	1	实例状态，取值： <ul style="list-style-type: none"> 1：正常 2：过期 3：释放
RequestId	String	C3F7E6AE-43B2-4730-B6A3-FD17552B8F65	本次请求的ID。

名称	类型	示例值	描述
Total	Long	1	返回结果的总数。

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribeInstanceListResponse>
  <RequestId>5DE4D6B1-8D6D-4AC3-84AF-5EE0A4C2778E</RequestId>
  <InstanceList>
    <Instance>
      <Status>1</Status>
      <AutoRenewal>true</AutoRenewal>
      <IpType>IPv4</IpType>
      <ExpireTime>1560009600000</ExpireTime>
      <InstanceId>ddosbgp-cn-xx</InstanceId>
      <GmtCreate>1554708159000</GmtCreate>
      <Remark>test</Remark>
      <BlackholdingCount>0</BlackholdingCount>
    </Instance>
  </InstanceList>
  <Total>1</Total>
</DescribeInstanceListResponse>
```

JSON 格式

```
{
  "RequestId": "C3F7E6AE-43B2-4730-B6A3-FD17552B8F65",
  "InstanceList": [
    {
      "Status": "1",
      "AutoRenewal": true,
      "IpType": "IPv4",
      "ExpireTime": 1560009600000,
      "InstanceId": "ddosbgp-cn-xx",
      "GmtCreate": 1554708159000,
      "Remark": "test",
      "BlackholdingCount": 0
    }
  ],
  "Total": 1
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.5.3. DescribeInstanceSpecs

调用DescribeInstanceSpecs接口查询防护包的规格信息。

 **说明** DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK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 。
InstanceIdList	String	是	["ddosbgp-cn-x1","ddosbgp-cn-x2"]	要查询的防护包实例ID，多个ID间以逗号分隔。以JSON字符串格式传入，例如，" ddosbgp-cn-x1 "," ddosbgp-cn-x2 "。

名称	类型	是否必选	示例值	描述
DdosRegionId	String	否	cn-hangzhou	实例所在地区ID。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
InstanceSpecs			防护包实例的规格信息。
AvailableDeleteBlackholeCount	String	100	可用的解除黑洞次数。
InstanceId	String	ddosbgp-cn-x1	防护包实例ID。
PackConfig			防护包实例的配置信息。
BindIpCount	Integer	0	已添加的防护IP数量。
IpAdvanceThre	Integer	101	被防护IP的弹性防护阈值，单位为Gb。
IpBasicThre	Integer	20	被防护IP的基础防护阈值，单位为Gb。
IpSpec	Integer	100	可添加IP的数量。
PackAdvThre	Integer	100	防护包的弹性防护带宽，单位为Gb。
PackBasicThre	Integer	20	防护包的基础防护带宽，单位为Gb。
Region	String	cn-hangzhou	防护包实例的区域。
RequestId	String	CEB7F4F5-1DA8-41ED-A9C4-E0F0033E9E1F	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeInstanceSpecs
&InstanceIdList=["ddosbgp-cn-x1","ddosbgp-cn-x2"]
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeInstanceSpecsResponse>
  <InstanceSpecs>
    <InstanceSpec>
      <Region>cn-hangzhou</Region>
      <InstanceId>ddosbgp-cn-x1</InstanceId>
      <AvailableDeleteBlackholeCount>100</AvailableDeleteBlackholeCount>
      <PackConfig>
        <IpBasicThre>20</IpBasicThre>
        <BindIpCount>0</BindIpCount>
        <PackBasicThre>20</PackBasicThre>
        <IpAdvanceThre>101</IpAdvanceThre>
        <IpSpec>100</IpSpec>
        <PackAdvThre>101</PackAdvThre>
      </PackConfig>
    </InstanceSpec>
  </InstanceSpecs>
  <RequestId>CEB7F4F5-1DA8-41ED-A9C4-E0F0033E9E1F</RequestId>
</DescribeInstanceSpecsResponse>
```

JSON 格式


```
{
  "InstanceSpecs":[
    {
      "Region":"cn-hangzhou",
      "AvailableDeleteBlackholeCount":100,
      "InstanceId":"ddosbgp-cn-x1",
      "PackConfig":{
        "IpBasicThre":20,
        "BindIpCount":0,
        "PackBasicThre":20,
        "IpAdvanceThre":100,
        "PackAdvThre":101,
        "IpSpec":100
      }
    }
  ],
  "RequestId":"D8D786F2-2008-4280-B9AB-8E6C4E8C2A16"
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.5.4. DescribeExcpetionCount

调用DescribeExcpetionCount接口查询防护包异常信息。

 说明 DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeExcpetionCount	要执行的操作，取值： DescribeExcpetionCount 。
DdosRegionId	String	是	cn-hangzhou	实例所在地区ID。

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

返回数据

名称	类型	示例值	描述
ExceptionIpCount	Integer	0	异常IP的数量，如被防护的ECS IP、SLB IP等。
ExpireTimeCount	Integer	1	7天内即将到期的实例数量。
RequestId	String	A3EEE55F-3B9F-4765-8C03-1A1A904F3451	本次请求的ID。

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribeExcpetionCountResponse>
  <ExpireTimeCount>1</ExpireTimeCount>
  <RequestId>58609615-FCF9-41DF-8B25-0D5C8DAB92BA</RequestId>
  <ExceptionIpCount>0</ExceptionIpCount>
</DescribeExcpetionCountResponse>
```

JSON 格式

```
{
  "RequestId": "A3EEE55F-3B9F-4765-8C03-1A1A904F3451",
  "ExpireTimeCount": 1,
  "ExceptionIpCount": 0
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.5.5. DescribePackIpList


调用DescribePackIpList接口查询防护包的防护IP列表信息。

 **说明** DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribePackIpList	要执行的操作，取值： DescribePackIpList 。
DdosRegionId	String	是	cn-hangzhou	实例所在地区ID。
InstanceId	String	是	ddosbgp-cn-x1	要查询的防护包实例ID。
PageNo	Integer	是	1	列表的页码，默认值为1。
PageSize	Integer	是	10	分页查询时每页的行数，最大值为50，默认值为10。
Ip	String	否	1.1.1.1	要查询的防护对象IP，设置后只返回指定IP的信息。
ProductName	String	否	ECS	要查询的防护对象IP的归属产品类型，取值： <div data-bbox="976 1626 1362 1697" style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin: 5px 0;">  说明 设置后只返回指定产品的防护IP信息。 </div> <ul style="list-style-type: none"> • ECS • SLB • EIP • WAF
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
Code	String	200	响应状态码。
IpList			防护IP列表。
Ip	String	1.1.1.1	被防护IP。
Product	String	ECS	IP的归属产品，取值： <ul style="list-style-type: none"> • ECS • SLB • EIP • WAF
Remark	String	test	归属产品备注，比如ECS实例的备注。
Status	String	normal	IP的状态，取值： <ul style="list-style-type: none"> • normal：正常 • hole_begin：黑洞中
RequestId	String	B479FE9B-F0EB-423B-81E5-ECE2167BCF40	本次请求的ID。
Success	Boolean	true	是否成功调用请求。
Total	Integer	1	返回结果的数量。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePackIpList
&DdosRegionId=cn-hangzhou
&InstanceId=ddosbgp-cn-x1
&PageNo=1
&PageSize=10
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribePackIpListResponse>
  <RequestId>8584D3B6-BB3C-441E-B1D6-E154ED25C032</RequestId>
  <IpList>
    <Ipitem>
      <Status>normal</Status>
      <Ip>1.1.1.1</Ip>
      <Product>ECS</Product>
      <Remark>test</Remark>
    </Ipitem>
  </IpList>
  <Success>true</Success>
  <Code>200</Code>
  <Total>1</Total>
</DescribePackIpListResponse>
```

JSON 格式

```
{
  "RequestId":"B479FE9B-F0EB-423B-81E5-ECE2167BCF40",
  "IpList":[
    {
      "Ip":"1.1.1.1",
      "Status":"normal",
      "Product":"ECS",
      "Remark":"test"
    }
  ],
  "Success":true,
  "Code":"200",
  "Total":1
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.5.6. ModifyRemark

调用ModifyRemark接口修改DDoS防护包的备注。

 说明 DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyRemark	要执行的操作，取值： ModifyRemark 。
InstanceId	String	是	ddosbgp-cn-xxx	要操作的防护包实例ID。
Remark	String	是	test	要添加的备注内容。
ResourceGroupId	String	否	test	资源组ID。
ResourceRegionId	String	否	cn-hangzhou	资源组地区ID。

返回数据

名称	类型	示例值	描述
RequestId	String	4C467B38-3910-447D-87BC-AC049166F216	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyRemark
&InstanceId=ddosbgp-cn-xxx
&Remark=test
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ModifyRemarkResponse>
  <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
</ModifyRemarkResponse>
```

JSON 格式

```
{
  "RequestId":"4C467B38-3910-447D-87BC-AC049166F216"
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.5.7. CheckGrant

调用CheckGrant接口检查防护包服务的授权状态，即是否授权防护包查询您的ECS服务器信息。

 说明 DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CheckGrant	要执行的操作，取值： CheckGrant 。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	E76E316C-697F-42D8-883A-D99864D2E77F	本次请求的ID。

名称	类型	示例值	描述
Status	Integer	1	授权状态，取值： <ul style="list-style-type: none"> 1：已授权DDoS防护包查询您的ECS服务器信息 0：未授权DDoS防护包查询您的ECS服务器信息

示例

请求示例

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

正常返回示例

XML 格式

```
<CheckGrantResponse>
  <RequestId>E76E316C-697F-42D8-883A-D99864D2E77F</RequestId>
  <Status>1</Status>
</CheckGrantResponse>
```

JSON 格式

```
{
  "Status":1,
  "RequestId":"E76E316C-697F-42D8-883A-D99864D2E77F"
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.6. 流量包

2.6.1. DescribeResourcePackInstances

调用DescribeResourcePackInstances接口查询抗D流量包信息。

 **说明** DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeResourcePacksInstances	要执行的操作，取值： DescribeResourcePacksInstances 。
CurrentPage	Integer	是	1	列表的页码，默认值为1。
PageSize	Integer	是	10	分页查询时每页显示的行数，最大值为50，默认值为10。
ResourceGroupId	String	否	xx	资源组ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
RequestId	String	40B322C3-464E-477F-B137-46E64349F0E9	本次请求的ID。
ResourcePacks	Array		抗D流量包信息。
CurrCapacity	Long	0	可用防护流量，单位为Byte。
EndTime	Long	1649433600000	失效时间。
InitCapacity	Long	1000000000000000	初始防护流量，单位为Byte。
ResourcePacksId	String	DDOSFLOWBAG-cn-o4012thf1000b5	抗D流量包ID。
StartTime	Long	1554708226000	生效时间。

名称	类型	示例值	描述
Status	String	valid	流量包的状态，取值： <ul style="list-style-type: none"> closed：失效 valid：有效
TotalCount	Integer	1	返回结果的总数。

示例

请求示例

```
https://ddosbgp.aliyuncs.com/?Action=DescribeResourcePackInstances
&CurrentPage=1
&PageSize=10
&公共请求参数
```

正常返回示例

XML 格式

```
<DescribeResourcePackInstancesResponse>
  <TotalCount>1</TotalCount>
  <ResourcePacks>
    <ResourcePack>
      <Status>valid</Status>
      <ResourcePackId>DDOSFLOWBAG-cn-xx</ResourcePackId>
      <InitCapacity>10000000000000</InitCapacity>
      <EndTime>1649433600000</EndTime>
      <StartTime>1554708226000</StartTime>
      <CurrCapacity>0</CurrCapacity>
    </ResourcePack>
  </ResourcePacks>
  <RequestId>40B322C3-464E-477F-B137-46E64349F0E9</RequestId>
</DescribeResourcePackInstancesResponse>
```

JSON 格式

```
{
  "TotalCount":1,
  "ResourcePacks":[
    {
      "Status":"valid",
      "ResourcePackId":"DDOSFLOWBAG-cn-o4012thfl000b5",
      "InitCapacity":10000000000000,
      "EndTime":1649433600000,
      "StartTime":1554708226000,
      "CurrCapacity":0
    }
  ],
  "RequestId":"40B322C3-464E-477F-B137-46E64349F0E9"
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.6.2. DescribeResourcePackStatistics

调用DescribeResourcePackStatistics接口查询抗D流量包的统计信息。

 **说明** DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeResourcePackStatistics	要执行的操作，取值： DescribeResourcePackStatistics 。
DdosRegionId	String	否	cn-hangzhou	实例所在地区ID。
InstanceId	String	否	ddosbgp-cn-x1	要查询的防护包实例ID。
ResourceGroupId	String	否	xx	资源组ID。

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

返回数据

名称	类型	示例值	描述
AvailablePackNum	Integer	8	可用流量包数量。
RequestId	String	A2D6D5FB-FA07-41A8-B093-A2B7B26E72F2	本次请求的ID。
TotalCurrCapacity	Long	20831250000000	总可用防护流量，单位为Byte。
TotalInitCapacity	Long	4270000000000000	总初始防护流量，单位为Byte。
TotalUsedCapacity	Long	52854390000000	总消耗防护流量，单位为Byte。

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribeResourcePackStatisticsResponse>
  <TotalInitCapacity>4270000000000000</TotalInitCapacity>
  <TotalUsedCapacity>52854390000000</TotalUsedCapacity>
  <TotalCurrCapacity>20831250000000</TotalCurrCapacity>
  <RequestId>A2D6D5FB-FA07-41A8-B093-A2B7B26E72F2</RequestId>
  <AvailablePackNum>8</AvailablePackNum>
</DescribeResourcePackStatisticsResponse>
```

JSON 格式


```
{
  "TotalInitCapacity":42700000000000,
  "TotalUsedCapacity":5285439000000,
  "RequestId":"A2D6D5FB-FA07-41A8-B093-A2B7B26E72F2",
  "TotalCurrCapacity":20831250000000,
  "AvailablePackNum":8
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.6.3. DescribeResourcePackUsage

调用DescribeResourcePackUsage接口查询抗D流量包的使用明细。

 **说明** DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeResourcePackUsage	要执行的操作，取值： DescribeResourcePackUsage 。
EndTime	Long	是	1557909844	查询结束时间，秒级时间戳。所设置的查询时间区间不能超过30天。
StartTime	Long	是	1557305044	查询开始时间，秒级时间戳。所设置的查询时间区间不能超过30天。
InstanceId	String	否	ddosbgp-cn-x1	要查询的防护包实例ID。
ResourceGroupId	String	否	xx	资源组ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
EndTime	Long	1557910800	统计结束时间，秒级时间戳。
Interval	Long	3600	统计时间间隔，单位为秒。
PackUsages	Array		已用防护流量明细。
Time	Long	1557471600	时间。
Traffic	Float	153.064	流量，单位为Gb。
RequestId	String	38F3D5EF-42BA-4533-81EB-AEAD068B5E02	本次请求的ID。
StartTime	Long	1557302400	统计起始时间，秒级时间戳。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeResourcePackUsage
&EndTime=1557909844
&StartTime=1557305044
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeResourcePackUsageResponse>
  <Interval>3600</Interval>
  <PackUsages>
    <PackUsage>
      <Time>1557471600</Time>
      <Traffic>153.064</Traffic>
    </PackUsage>
  </PackUsages>
  <RequestId>38F3D5EF-42BA-4533-81EB-AEAD068B5E02</RequestId>
  <EndTime>1557910800</EndTime>
  <StartTime>1557302400</StartTime>
</DescribeResourcePackUsageResponse>
```

JSON 格式


```
{
  "Interval":3600,
  "PackUsages":[
    {
      "Time":1557471600,
      "Traffic":153.064
    }
  ],
  "RequestId":"38F3D5EF-42BA-4533-81EB-AEAD068B5E02",
  "EndTime":1557910800,
  "StartTime":1557302400
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.6.4. DescribePackPaidTraffic

调用DescribePackPaidTraffic接口查询付费流量明细。

 **说明** DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribePackPaidTraffic	要执行的操作，取值： DescribePackPaidTraffic 。
CurrentPage	Integer	是	1	列表的页码，默认值为1。
EndTime	Long	是	1557908337870	查询结束时间，秒级时间戳。所设置的查询时间区间不能超过30天。
PageSize	Integer	是	10	分页查询时每页的行数，最大值为50，默认值为10。
StartTime	Long	是	1557303537870	查询开始时间，秒级时间戳。所设置的查询时间区间不能超过30天。
InstanceId	String	否	ddosbgp-cn-x1	要查询的防护包实例ID。
ResourceGroupId	String	否	xx	资源组ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
PackPaidTraffic	Array		付费流量明细。
BaseBandwidth	Integer	20	基础防护带宽，单位为Gb。
ElasticBandwidth	Integer	100	弹性防护带宽，单位为Gb。
InstanceId	String	ddosbgp-cn-x1	防护包实例ID。
MaxAttack	Float	49.998	攻击流量峰值，单位为Gbps。
PaidCapacity	Float	615.166	付费流量大小，单位为Gb。

名称	类型	示例值	描述
StartTime	Long	1557809400000	统计时间。
TotalCapacity	Float	1302.666	总防护流量，单位为Gb。
RequestId	String	070363B7-BB66-43B8-9A2C-9E4B83284FC5	本次请求的ID。
TotalCount	Integer	1	返回结果的数量。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePackPaidTraffic
&CurrentPage=1
&EndTime=1557908337870
&PageSize=10
&StartTime=1557303537870
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribePackPaidTrafficResponse>
  <TotalCount>1</TotalCount>
  <RequestId>070363B7-BB66-43B8-9A2C-9E4B83284FC5</RequestId>
  <PackPaidTraffics>
    <PackPaidTraffic>
      <PaidCapacity>615.166</PaidCapacity>
      <MaxAttack>49.998</MaxAttack>
      <InstanceId>ddosbgp-cn-x1</InstanceId>
      <TotalCapacity>1302.666</TotalCapacity>
      <ElasticBandwidth>100</ElasticBandwidth>
      <BaseBandwidth>20</BaseBandwidth>
      <StartTime>1557809400000</StartTime>
    </PackPaidTraffic>
  </PackPaidTraffics>
</DescribePackPaidTrafficResponse>
```

JSON 格式

```
{
  "TotalCount":1,
  "RequestId":"070363B7-BB66-43B8-9A2C-9E4B83284FC5",
  "PackPaidTraffics":[
    {
      "PaidCapacity":615.166,
      "InstanceId":"ddosbgp-cn-x1",
      "MaxAttack":49.998,
      "TotalCapacity":1302.666,
      "ElasticBandwidth":100,
      "StartTime":1557809400000,
      "BaseBandwidth":20
    }
  ]
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.7. 图表日志

2.7.1. DescribeDdosEvent

调用DescribeDdosEvent接口查看指定防护包上的DDoS事件。

 说明 DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDdosEvent	要执行的操作，取值： DescribeDdosEvent 。
EndTime	Integer	是	1557909844	查询结束时间，秒级时间戳。

名称	类型	是否必选	示例值	描述
Instanceid	String	是	ddosbgp-cn-x1	要查询的防护包实例ID。
PageNo	Integer	是	1	列表的页码，默认值为1。
PageSize	Integer	是	10	分页查询时每页的行数，最大值为50，默认值为10。
StartTime	Integer	是	1557305044	查询开始时间，秒级时间戳。
Ip	String	否	1.1.1.1	要查询的防护对象IP。
ResourceGroupId	String	否	test	资源组ID。
ResourceRegionId	String	否	cn-hangzhou	资源组地区ID。

返回数据

名称	类型	示例值	描述
Events			DDoS事件信息。
EndTime	Integer	1557891306	攻击结束时间，秒级时间戳。
Ip	String	1.1.1.1	被攻击的IP。
Mbps	Integer	110000	攻击流量大小，单位为Mbps。
Pps	Integer	0	攻击报文数量，单位为pps
StartTime	Integer	1557889506	攻击开始时间，秒级时间戳。
Status	String	defense_end	事件状态，取值： <ul style="list-style-type: none"> hole_begin：黑洞中 hole_end：黑洞结束 defense_begin：清洗中 defense_end：清洗结束

名称	类型	示例值	描述
RequestId	String	6A507DC8-F657-4C13-84E2-D1D1B9400753	本次请求的ID。
Total	Long	8	DDoS事件总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDdosEvent
&EndTime=1557909844
&InstanceId=ddosbgp-cn-x1
&PageNo=1
&PageSize=10
&StartTime=1557305044
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeDdosEventResponse>
  <RequestId>6A507DC8-F657-4C13-84E2-D1D1B9400753</RequestId>
  <Events>
    <Event>
      <Pps>0</Pps>
      <Status>defense_end</Status>
      <Ip>1.1.1.1</Ip>
      <Mbps>110000</Mbps>
      <EndTime>1557891306</EndTime>
      <StartTime>1557889506</StartTime>
    </Event>
  </Events>
  <Total>1</Total>
</DescribeDdosEventResponse>
```

JSON 格式

```
{
  "RequestId":"6A507DC8-F657-4C13-84E2-D1D1B9400753",
  "Events":[
    {
      "Pps":0,
      "Ip":"1.1.1.1",
      "Status":"defense_end",
      "Mbps":110000,
      "EndTime":1557891306,
      "StartTime":1557889506
    }
  ],
  "Total":8
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.7.2. DescribeOpEntities

调用DescribeOpEntities接口查询用户的操作日志。

 **说明** DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK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 。
CurrentPage	Integer	是	1	列表的页码，默认值为1。
EndTime	Long	是	1557906714012	查询结束时间，毫秒级时间戳。
PageSize	Integer	是	10	分页查询时每页的行数，最大值为50，默认值为10。

名称	类型	是否必选	示例值	描述
StartTime	Long	是	1555314714011	查询开始时间，毫秒级时间戳。
InstanceId	String	否	ddosbgp-cn-x1	要查询的防护包实例ID。
OrderBy	String	否	opdate	排序字段，取值： opdate （操作时间）。
OrderDir	String	否	ASC	排序方向，取值： <ul style="list-style-type: none"> • ASC：正序 • DESC：倒序
ResourceGroupId	String	否	test	资源组ID。
ResourceRegionId	String	否	cn-hangzhou	资源组地区ID。

返回数据

名称	类型	示例值	描述
OpEntities	Array		操作日志信息。
EntityObject	String	ddosbgp-cn-o4013qftb006	操作对象，即防护包实例。
EntityType	Integer	1	操作对象类型，取值： 1 （实例）。
GmtCreate	Long	1557821673000	日志创建时间。
OpAccount	String	system	操作账号，取值： system （系统）。
OpAction	Integer	8	操作类型，取值： <ul style="list-style-type: none"> • 3：添加IP • 4：解绑IP • 5：实例降级 • 6：解除黑洞 • 7：重置解除黑洞次数 • 8：恢复弹性

名称	类型	示例值	描述
OpDesc	String	{\"entity\": {\"baseBandwidth\": :20,\"elasticBandwidth\":101}}	操作说明。
RequestId	String	52C8ECB0-0B1A- 4E66-A31C- B6A855120E82	本次请求的ID。
TotalCount	Integer	1	返回结果的数量。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeOpEntities
&CurrentPage=1
&EndTime=1557906714012
&PageSize=10
&StartTime=1555314714011
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeOpEntitiesResponse>
  <TotalCount>1</TotalCount>
  <OpEntities>
    <OpEntity>
      <OpAccount>system</OpAccount>
      <OpDesc>{\"entity\":{\"baseBandwidth\":20,\"elasticBandwidth\":101}}</OpDesc>
      <EntityObject>ddosbgp-cn-o4013qftb006</EntityObject>
      <EntityType>1</EntityType>
      <GmtCreate>1557821673000</GmtCreate>
      <OpAction>8</OpAction>
    </OpEntity>
  </OpEntities>
  <RequestId>52C8ECB0-0B1A-4E66-A31C-B6A855120E82</RequestId>
</DescribeOpEntitiesResponse>
```

JSON 格式

```
{
  "TotalCount":1,
  "OpEntities":[
    {
      "OpAccount":"system",
      "OpDesc":{"entity":{"baseBandwidth":20,"elasticBandwidth":101}},
      "EntityObject":"ddosbgp-cn-o4013qftb006",
      "EntityType":1,
      "GmtCreate":1557821673000,
      "OpAction":8
    }
  ],
  "RequestId":"52C8ECB0-0B1A-4E66-A31C-B6A855120E82"
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.7.3. DescribeTraffic

调用DescribeTraffic接口查看指定防护包上的流量情况。

 **说明** DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeTraffic	要执行的操作，取值： DescribeTraffic 。
EndTime	Integer	是	1563445054	查询结束时间，秒级时间戳。
Interval	Integer	是	1000	流量统计的时间间隔区间（单位：秒）。
StartTime	Integer	是	1560853054	查询开始时间，秒级时间戳。

名称	类型	是否必选	示例值	描述
Instanceid	String	否	ddosbgp-cn-*****	要查询的防护包实例ID。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; border-radius: 5px;"> ? 说明 Instanceid与Ip两者必须要至少指定其中一个参数。 </div>
Ip	String	否	1.1.1.1	要查询的防护对象IP。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; border-radius: 5px;"> ? 说明 Instanceid与Ip两者必须要至少指定其中一个参数。 </div>
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
FlowList	Array		流量信息。
FlowType	String	max	显示流量类型： <ul style="list-style-type: none"> • avg：区间平均值 • max：区间峰值
Kbps	Integer	8	流量大小（单位：Kbps）。
Name	String	73765106-54e7-11e9-aab0-d89d67182200	流量信息记录ID。
Pps	Integer	9	数据包数（单位：pps）。
Time	Integer	1560857000	流量信息时间戳。
RequestId	String	6A507DC8-F657-4C13-84E2-D1D1B9400753	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]?Action=DescribeTraffic
&EndTime=1563445054
&Interval=1000
&StartTime=1560853054
&InstanceId=ddosbgp-cn-*****
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeTraffic>
  <RequestId>6A507DC8-F657-4C13-84E2-D1D1B9400753</RequestId>
  <FlowList>
    <Name>73765106-54e7-11e9-aab0-d89d67182200</Name>
    <Pps>25</Pps>
    <Time>1560855000</Time>
    <FlowType>max</FlowType>
    <Kbps>17</Kbps>
  </FlowList>
  <FlowList>
    <Name>73765106-54e7-11e9-aab0-d89d67182200</Name>
    <Pps>9</Pps>
    <Time>1560857000</Time>
    <FlowType>max</FlowType>
    <Kbps>8</Kbps>
  </FlowList>
</DescribeTraffic>
```

JSON 格式

```
{
  "FlowList":[
    {
      "Pps":25,
      "Name":"73765106-54e7-11e9-aab0-d89d67182200",
      "Time":1560855000,
      "FlowType":"max",
      "Kbps":17
    },
    {
      "Pps":9,
      "Name":"73765106-54e7-11e9-aab0-d89d67182200",
      "Time":1560857000,
      "FlowType":"max",
      "Kbps":8
    }
  ],
  "RequestId":"6A507DC8-F657-4C13-84E2-D1D1B9400753"
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.7.4. DescribeOnDemandDdosEvent

调用DescribeOnDemandDdosEvent 查询DDoS防护代播IP上的DDoS事件记录。

 **说明** DDoS原生防护的API接口目前仅对DDoS原生防护企业版用户开放。

调试

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

请求参数

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

名称	类型	是否必选	示例值	描述
EndTime	Integer	是	1557909844	查询结束时间，秒级时间戳。
Instanceid	String	是	ddosbgp-cn-x1	要查询的代播实例ID。
PageNo	Integer	是	1	列表的页码，默认值为1。
PageSize	Integer	是	10	分页查询时每页的行数，最大值为50，默认值为10。
StartTime	Integer	是	1557305044	查询开始时间，秒级时间戳。
Ip	String	否	1.1.1.1	要查询的代播IP。
ResourceGroupId	String	否	default	DDoS防护代播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	要查询的代播实例的地域ID。

返回数据

名称	类型	示例值	描述
Events	Array		DDoS攻击事件信息。
EndTime	Integer	1557891306	攻击结束时间，秒级时间戳。
Ip	String	1.1.1.1	被攻击的IP。
Mbps	Integer	110000	攻击流量大小，单位：Mbps。
Pps	Integer	0	攻击报文数量，单位：pps。
StartTime	Integer	1557889506	攻击开始时间，秒级时间戳。

名称	类型	示例值	描述
Status	String	defense_end	事件状态，取值： <ul style="list-style-type: none">• hole_begin：黑洞中• hole_end：黑洞结束• defense_begin：清洗中• defense_end：清洗结束
RequestId	String	6A507DC8-F657-4C13-84E2-D1D1B9400753	本次请求的ID。
Total	Long	8	DDoS攻击事件总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeOnDemandDdosEvent
&EndTime=1557909844
&InstanceId=ddosbgp-cn-x1
&PageNo=1
&PageSize=10
&StartTime=1557305044
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeOnDemandDdosEventResponse>
  <RequestId>6A507DC8-F657-4C13-84E2-D1D1B9400753</RequestId>
  <Events>
    <Event>
      <Pps>0</Pps>
      <Status>defense_end</Status>
      <Ip>1.1.1.1</Ip>
      <Mbps>110000</Mbps>
      <EndTime>1557891306</EndTime>
      <StartTime>1557889506</StartTime>
    </Event>
  </Events>
  <Total>1</Total>
</DescribeOnDemandDdosEventResponse>
```

JSON 格式

```
{
  "RequestId": "6A507DC8-F657-4C13-84E2-D1D1B9400753",
  "Events": [
    {
      "Pps": 0,
      "Ip": "1.1.1.1",
      "Status": "defense_end",
      "Mbps": 110000,
      "EndTime": 1557891306,
      "StartTime": 1557889506
    }
  ],
  "Total": 1
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.8. 标签

2.8.1. ListTagKeys

调用ListTagKeys接口查询所有标签。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ListTagKeys	要执行的操作。取值： ListTagKeys 。
RegionId	String	是	cn-hangzhou	要查询的地域ID。
ResourceType	String	是	INSTANCE	资源类型，取值： INSTANCE 。
PageSize	Integer	否	20	分页查询时设置的每页行数，最大值为50，默认值为10。
CurrentPage	Integer	否	1	列表的页码，起始值为1，默认值为1。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	97935DF1-0289-4AA2-9DD1-72377838B16B	本次请求的ID。
CurrentPage	Integer	1	列表的页码。
PageSize	Integer	20	每页的行数。
TotalCount	Integer	6	标签的总数。
TagKeys	Array		标签信息。
TagKey	String	a	标签键。
TagCount	Integer	1	标签键下标签值的总数。

示例

请求示例

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

正常返回示例

JSON 格式

```
{
  "RequestId":"97935DF1-0289-4AA2-9DD1-72377838B16B",
  "TotalCount": 6,
  "PageSize": 20,
  "CurrentPage": 1,
  "TagKeys": [
    {
      "TagCount": 1,
      "TagKey": "a"
    },
    {
      "TagCount": 1,
      "TagKey": "testKey1"
    },
    {
      "TagCount": 1,
      "TagKey": "testKey2"
    },
    {
      "TagCount": 2,
      "TagKey": "testKey3"
    },
    {
      "TagCount": 1,
      "TagKey": "testKey4"
    },
    {
      "TagCount": 1,
      "TagKey": "x"
    }
  ]
}
```

XML 格式

```
<ListTagKeysResponse>
  <CurrentPage>1</CurrentPage>
  <PageSize>20</PageSize>
  <RequestId>97935DF1-0289-4AA2-9DD1-72377838B16B</RequestId>
  <TagKeys>
    <element>
      <TagCount>1</TagCount>
      <TagKey>a</TagKey>
    </element>
    <element>
      <TagCount>1</TagCount>
      <TagKey>testKey1</TagKey>
    </element>
    <element>
      <TagCount>1</TagCount>
      <TagKey>testKey2</TagKey>
    </element>
    <element>
      <TagCount>2</TagCount>
      <TagKey>testKey3</TagKey>
    </element>
    <element>
      <TagCount>1</TagCount>
      <TagKey>testKey4</TagKey>
    </element>
    <element>
      <TagCount>1</TagCount>
      <TagKey>x</TagKey>
    </element>
  </TagKeys>
  <TotalCount>6</TotalCount>
</ListTagKeysResponse>
```

错误码

访问[错误中心](#)查看更多错误码。

2.8.2. ListTagResources

调用ListTagResources接口查询资源（DDoS原生防护实例）和标签的对应关系。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ListTagResources	要执行的操作。取值： ListTagResources 。
RegionId	String	是	cn-hangzhou	原生防护实例的地域ID。
ResourceType	String	是	INSTANCE	资源类型，取值： INSTANCE 。
ResourceGroupId	String	否	test	资源组ID。
Resourceid.N	RepeatList	否	ddosbgp-cn-v0h1fmwbc024	<p>指定要查询的原生防护实例ID，查询实例的标签。n的取值范围为 [1, 50]，用于指定多个实例，最多50个。例如： Resourceid.1, Resourceid.2, ..., Resourceid.50。</p> <p> 说明 您必须指定Resourceid或者Tag.Key和Tag.Value组合。</p>
Tag.N.Key	String	否	testKey1	<p>指定要查询的标签键，查询标签下的实例。n的取值范围为 [1, 20]，用于指定多个标签键，最多20个。例如： Tag.1.Key, Tag.2.Key, ..., Tag.20.Key。</p> <p> 说明 您必须指定Resourceid或者Tag.Key和Tag.Value组合。</p>

名称	类型	是否必选	示例值	描述
Tag.N.Value	String	否	testValue1	<p>指定要查询的标签值，查询标签下的实例。n的取值范围为 [1, 20]，用于指定多个标签值，最多20个。例如： Tag.1.Value, Tag.2.Value, ..., Tag.20.Value。</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px;"> <p> 说明 您必须指定ResourceId或者Tag.Key和Tag.Value组合。指定标签值时，必须指定标签键；指定标签键后，标签值可以留空。</p> </div>
NextToken	String	否	RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCffomr	指定下一个查询开始的Token。如果没有下一个查询，请留空。

返回数据

名称	类型	示例值	描述
RequestId	String	C3F7E6AE-43B2-4730-B6A3-FD17552B8F65	本次请求的ID。
NextToken	String	RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCffomr	下一个查询开始的Token。没有下一个查询时空。
TagResources	Array		资源和标签的关系列表。
ResourceType	String	INSTANCE	资源类型，取值： INSTANCE 。
ResourceId	String	ddosbgp-cn-o4017n9q9004	原生防护实例ID。
TagKey	String	testKey4	标签键。
TagValue	String	testValue4	标签值。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ListTagResources
&RegionId=cn-hangzhou
&ResourceType=INSTANCE
&ResourceId.1=ddosbgp-cn-v0h1fmwbc024
&<公共请求参数>
```

正常返回示例

JSON 格式

```
{
  "RequestId": "C3F7E6AE-43B2-4730-B6A3-FD17552B8F65",
  "NextToken": "RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCffomr",
  "TagResources": {
    "TagResource": [
      {
        "ResourceId": "ddosbgp-cn-o4017n9q9004",
        "TagKey": "testKey4",
        "ResourceType": "INSTANCE",
        "TagValue": "testValue4"
      }
    ]
  }
}
```

XML 格式

```
<ListTagResourcesResponse>
  <NextToken>RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCffomr</NextToken>
  <RequestId>C3F7E6AE-43B2-4730-B6A3-FD17552B8F65</RequestId>
  <TagResources>
    <TagResource>
      <element>
        <ResourceId>ddosbgp-cn-o4017n9q9004</ResourceId>
        <ResourceType>INSTANCE</ResourceType>
        <TagKey>testKey4</TagKey>
        <TagValue>testValue4</TagValue>
      </element>
    </TagResource>
  </TagResources>
</ListTagResourcesResponse>
```

错误码

访问[错误中心](#)查看更多错误码。

2.8.3. TagResources

调用TagResources接口为指定资源（DDoS原生防护实例）绑定标签。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	TagResources	要执行的操作。取值： TagResources 。
RegionId	String	是	cn-hangzhou	原生防护实例的地域ID。
ResourceId.N	RepeatList	是	ddosbgp-cn-v0h1fmbwbc024	要操作的原生防护实例的ID。n的取值范围为 [1, 50]，用于指定多个实例，最多50个。例如：ResourceId.1, ResourceId.2, ..., ResourceId.50。
ResourceType	String	是	INSTANCE	资源的类型，取值： INSTANCE 。
ResourceGroupId	String	否	test	资源组ID。
Tag.N.Key	String	否	testKey1	要绑定的标签键。n的取值范围为 [1, 20]，用于指定多个标签键，最多20个。例如：Tag.1.Key, Tag.2.Key, ..., Tag.20.Key。
Tag.N.Value	String	否	testValue1	要绑定的标签值。n的取值范围为 [1, 20]，用于指定多个标签值，最多20个。例如：Tag.1.Value, Tag.2.Value, ..., Tag.20.Value。

返回数据

名称	类型	示例值	描述
----	----	-----	----

名称	类型	示例值	描述
RequestId	String	7078CD1E-F609-47A4-9C39-B288CC27C686	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=TagResources
&RegionId=cn-hangzhou
&ResourceId.1=ddosbgp-cn-v0h1fmwbc024
&ResourceType=INSTANCE
&Tag.1.Key=testKey.1
&Tag.1.Value=testValue1
&<公共请求参数>
```

正常返回示例

JSON 格式

```
{
  "requestId": "7078CD1E-F609-47A4-9C39-B288CC27C686"
}
```

XML 格式

```
<TagResourcesResponse>
  <requestId>7078CD1E-F609-47A4-9C39-B288CC27C686</requestId>
</TagResourcesResponse>
```

错误码

访问[错误中心](#)查看更多错误码。

2.8.4. UntagResources

调用UntagResources接口移除指定资源（DDoS原生防护实例）的标签。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	UntagResources	要执行的操作。取值： UntagResources 。
RegionId	String	是	cn-hangzhou	原生防护实例的地域ID。
ResourceId.N	RepeatList	是	ddosbgp-cn-v0h1fmwbc024	要操作的原生防护实例的ID。n的取值范围为 [1, 50]，用于指定多个实例，最多50个。例如：ResourceId.1, ResourceId.2, ..., ResourceId.50。
ResourceType	String	是	INSTANCE	资源类型，取值： INSTANCE 。
ResourceGroupId	String	否	test	资源组ID。
TagKey.N	RepeatList	否	testKey1	要移除的标签键。n的取值范围为 [1, 20]，用于指定多个标签键，最多20个。例如：Tag.1.Key, Tag.2.Key, ..., Tag.20.Key。
All	Boolean	否	false	是否移除实例上的所有标签。

返回数据

名称	类型	示例值	描述
RequestId	String	F2D86AED-BA27-4584-BADC-B43BDA7EEBCA	本次请求的ID。

示例

请求示例

```

http(s)://[Endpoint]/?Action=UntagResources
&RegionId=cn-hangzhou
&ResourceId.1=ddosbgp-cn-v0h1fmwbc024
&ResourceType=INSTANCE
&TagKey.1=testKey1
&All=false
&<公共请求参数>

```

正常返回示例

JSON 格式

```
{
  "requestId": "F2D86AED-BA27-4584-BADC-B43BDA7EEBCA"
}
```

XML 格式

```
<UntagResourcesResponse>
  <requestId>F2D86AED-BA27-4584-BADC-B43BDA7EEBCA</requestId>
</UntagResourcesResponse>
```

错误码

访问[错误中心](#)查看更多错误码。

2.9. 代播防护

2.9.1. DescribeOnDemandInstanceStatus

调用DescribeOnDemandInstanceStatus查询代播实例的详细信息。

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	DescribeOnDemandInstanceStatus	要执行的操作。取值： DescribeOnDemandInstanceStatus 。
InstanceList.N	RepeatList	是	ddosbgp-cn-z2q1qzxb****	要查询的代播实例的ID列表。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 5px;"> <p>? 说明 您可以调用DescribeOnDemandInstance查询所有代播实例的ID。</p> </div>

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-zhangjiakou	代播实例的地域ID。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px;"> <p> 说明 您可以调用 <code>DescribeRegions</code> 查询DDoS原生防护支持的所有地域信息。</p> </div>

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

调用API的请求格式，请参见本文[示例](#)中的请求示例。

返回数据

名称	类型	示例值	描述
Instances	Array of instance		代播实例的详细信息。
Declared	String	[{"region\":"oe24\" ,\"declared\":0}, {"region\":"oe26\" ,\"declared\":0}, {"region\":"oe28\" ,\"declared\":0}, {"region\":"oi39\" ,\"declared\":0}, {"region\":"us50\" ,\"declared\":0}, {"region\":"jp141\" ,\"declared\":0}]	海外IDC的路由宣告状态信息。以JSON数组格式转化成字符串表示，JSON数组中的每个结构体包含以下参数： <ul style="list-style-type: none"> region: String类型 海外IDC代码。关于IDC代码对应的地域信息，请参见该表格下方的海外IDC代码说明。 declared: String类型 该IDC是否宣告路由，取值：0（表示未宣告） 1（表示宣告）。
Desc	String	test	代播实例的描述。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px;"> <p> 说明 该参数仅在返回多个代播实例时才会返回。目前仅返回一个代播实例，该参数不会返回。</p> </div>
Instanceid	String	ddosbgp-cn-z2q1qzxb****	代播实例的ID。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px;"> <p> 说明 该参数仅在返回多个代播实例时才会返回。目前仅返回一个代播实例，该参数不会返回。</p> </div>

名称	类型	示例值	描述
Mode	String	netflow-auto	代播防护的启动模式。取值： <ul style="list-style-type: none"> manual：表示手动启动。 netflow-auto：表示通过NetFlow网络流量监测自动启动。
Net	String	47.***.***.0/24	代播网段。
RegisteredAs	String	0	自治系统AS (Autonomous System) 号码。目前取值固定为0，表示暂未启用。
Userid	String	171986973287****	阿里云账号ID。
RequestId	String	CC49FF51-612F-429B-AB1E-374B3F115396	本次请求的ID。

海外IDC代码

下表描述了不同海外地域部署的代播防护IDC的代码。

地域	IDC代码
美国（硅谷）	oe24、oe25、oc27、ot7
美国（弗吉尼亚）	us44-a、us44-b、us68、us50、us51
中国（香港）	meg、oe26、hk45、hk71
新加坡	oe28、og37、os30、sg94、sg52、sg113
澳大利亚（悉尼）	au49、au67、au57、au58
德国（法兰克福）	de46、de81、oe38、oi39
俄罗斯（莫斯科）	ol31、ru85、ru66
英国（伦敦）	gb82、gb83、gb33、gb124

地域	IDC代码
印度（孟买）	in74、in75、in73、in123
日本（东京）	jp59、jp42、jp43、jp138、jp141
马来西亚（吉隆坡）	my86、my87、my88、my115
印度尼西亚（雅加达）	id56、id55、id35、id90

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeOnDemandInstanceStatus
&InstanceIdList.1=ddosbgp-cn-z2q1qzxb****
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeOnDemandInstanceStatusResponse>
  <Instances>
    <UserId>171986973287****</UserId>
    <Mode>netflow-auto</Mode>
    <RegisteredAs>0</RegisteredAs>
    <Net>47.***.***.0/24</Net>
    <Declared>[{"region\":"oe24\","declared\":0},{"region\":"oe26\","declared\":0},{"region\":"oe28\","declared\":0},{"region\":"oi39\","declared\":0},{"region\":"us50\","declared\":0},{"region\":"jp141\","declared\":0}]</Declared>
  </Instances>
  <RequestId>CC49FF51-612F-429B-AB1E-374B3F115396</RequestId>
</DescribeOnDemandInstanceStatusResponse>
```

JSON 格式

```
{
  "Instances": [
    {
      "UserId": "171986973287****",
      "Mode": "netflow-auto",
      "RegisteredAs": "0",
      "Net": "47.***.***.0/24",
      "Declared": "[{\\"region\\":\\"oe24\\",\\"declared\\":0},{\\"region\\":\\"oe26\\",\\"declared\\":0},{\\"region\\":\\"oe28\\",\\"declared\\":0},{\\"region\\":\\"oi39\\",\\"declared\\":0},{\\"region\\":\\"us50\\",\\"declared\\":0},{\\"region\\":\\"jp141\\",\\"declared\\":0}]"
    }
  ],
  "RequestId": "CC49FF51-612F-429B-AB1E-374B3F115396"
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.9.2. SetInstanceModeOnDemand

调用SetInstanceModeOnDemand设置代播实例的调度模式。

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	SetInstanceModeOnDemand	要执行的操作。取值： SetInstanceModeOnDemand 。
InstanceList.N	RepeatList	是	ddosbgp-cn-z2q1qzxb****	要操作的代播实例的ID列表。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 5px;"> ? 说明 您可以调用DescribeOnDemandInstance查询所有代播实例的ID。 </div>
Mode	String	是	netflow-auto	设置代播实例的调度模式。取值： <ul style="list-style-type: none"> • manual：表示手动调度。 • netflow-auto：表示自动调度。

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-zhangjiakou	代播实例的地域ID。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px;"> <p> 说明 您可以调用 <code>DescribeRegions</code> 查询DDoS原生防护支持的所有地域信息。</p> </div>

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

调用API的请求格式，请参见本文[示例](#)中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	BD06F539-2FBE-450D-9391-7EFF787128F5	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=SetInstanceModeOnDemand
&InstanceIdList.1=ddosbgp-cn-z2q1qzxb****
&Mode=netflow-auto
&<公共请求参数>
```

正常返回示例

XML 格式

```
<SetInstanceModeOnDemandResponse>
  <RequestId>BD06F539-2FBE-450D-9391-7EFF787128F5</RequestId>
</SetInstanceModeOnDemandResponse>
```

JSON 格式

```
{
  "RequestId": "BD06F539-2FBE-450D-9391-7EFF787128F5"
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.9.3. CreateScheduleOnDemand

调用CreateScheduleOnDemand为代播实例创建一条调度规则。

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	CreateScheduleOnDemand	要执行的操作。取值： CreateScheduleOnDemand 。
Instanceid	String	是	ddosbgp-cn-z2q1qzxb****	要操作的代播实例的ID。 说明 您可以调用DescribeOnDemandInstance查询所有代播实例的ID。
RuleAction	String	是	declare	调度动作。取值固定为 declare ，表示宣告路由。
RuleConditionCnt	String	是	3	当代播实例的入方向带宽或者报文数量连续超过阈值多少次时，将触发调度规则并开启代播防护。 说明 带宽阈值通过RuleConditionMbps参数设置，报文数阈值通过RuleConditionKpps参数设置。
RuleConditionKpps	String	是	10	入方向报文数阈值，单位：Kpps。最小值： 10 。
RuleConditionMbps	String	是	100	入方向带宽阈值，单位：Mbps。最小值： 100 。

名称	类型	是否必选	示例值	描述
RuleName	String	是	ddosbgp-cn-z2q1qzxb****	<p>调度规则的名称。</p> <p>支持使用英文小写字母、数字、短划线 (-) 和下划线 (_), 不超过32个字符。建议您使用代播实例的ID作为调度规则名称, 例如, <code>ddosbgp-cn-z2q1qzxb****</code>。</p>
RuleSwitch	String	是	on	<p>调度规则的开关状态。取值:</p> <ul style="list-style-type: none"> <code>on</code>: 表示开启。 <code>off</code>: 表示关闭。
RuleUndoBeginTime	String	是	03:00	<p>自动停止调度的开始时间。使用24小时制表示, 格式: <code>hh:mm</code>。</p> <p>当系统检测到攻击停止后, 会在此处设置的时间开始停止代播防护。建议您将该时间设置为业务低峰期。</p> <p>说明 该参数仅在使用自动停止调度 (<code>RuleUndoMode</code> 设置为 <code>auto</code>) 时生效。</p>
RuleUndoMode	String	是	auto	<p>调度规则的停止方式。取值:</p> <ul style="list-style-type: none"> <code>auto</code>: 表示自动停止调度。 <code>manual</code>: 表示手动停止调度。
TimeZone	String	是	GMT-08:00	<p>自动停止调度时间对应的时区。使用格林威治时间表示, 格式: <code>GMT-hh:mm</code>。</p> <p>例如, <code>GMT-08:00</code> 表示东八区。</p> <p>说明 该参数仅在使用自动停止调度 (<code>RuleUndoMode</code> 设置为 <code>auto</code>) 时生效。</p>
RuleUndoEndTime	String	否	03:05	<p>自动停止调度的结束时间。使用24小时制表示, 格式: <code>hh:mm</code>。</p>

名称	类型	是否必选	示例值	描述
RegionId	String	否	cn-zhangjiakou	代播实例的地域ID。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px;"> <p> 说明 您可以调用 <code>DescribeRegions</code> 查询DDoS原生防护支持的所有地域信息。</p> </div>

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

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	BD06F539-2FBE-450D-9391-7EFF787128F5	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateSchedruleOnDemand
&InstanceId=ddosbgp-cn-z2q1qzxb****
&RuleAction=declare
&RuleConditionCnt=3
&RuleConditionKpps=10
&RuleConditionMbps=100
&RuleName=ddosbgp-cn-z2q1qzxb****
&RuleSwitch=on
&RuleUndoBeginTime=03:00
&RuleUndoMode=auto
&TimeZone=GMT-08:00
&<公共请求参数>
```

正常返回示例

XML 格式

```
<CreateSchedruleOnDemandResponse>
  <RequestId>BD06F539-2FBE-450D-9391-7EFF787128F5</RequestId>
</CreateSchedruleOnDemandResponse>
```

JSON 格式

```
{
  "RequestId": "BD06F539-2FBE-450D-9391-7EFF787128F5"
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.9.4. QuerySchedruleOnDemand

调用QuerySchedruleOnDemand查询代播实例的调度规则。

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	QuerySchedruleOnDemand	要执行的操作。取值： QuerySchedruleOnDemand 。
InstanceId	String	是	ddosbgp-cn-z2q1qzxb****	要查询的代播实例的ID。  说明 您可以调用 DescribeOnDemandInstance 查询所有代播实例的ID。
RegionId	String	否	cn-zhangjiakou	代播实例的地域ID。  说明 您可以调用 DescribeRegions 查询DDoS原生防护支持的所有地域信息。

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

调用API的请求格式，请参见本文示例中的请求示例。

返回数据

名称	类型	示例值	描述
InstanceId	String	ddosbgp-cn-z2q1qzxb****	代播实例的ID。
RequestId	String	4A8F9980-5ACB-497F-9F15-48E9D6B29028	本次请求的ID。
RuleConfig	Array of Config		调度规则的配置信息。
RuleAction	String	declare	调度动作。取值固定为 declare ，表示宣告路由。
RuleConditionCnt	String	3	当代播实例的入方向带宽或者报文数量连续超过阈值多少次时，将触发调度规则并开启代播防护。 说明 带宽阈值通过 RuleConditionMbps 参数设置，报文数阈值通过 RuleConditionKpps 参数设置。
RuleConditionKpps	String	10	入方向报文数阈值，单位：Kpps。最小值： 10 。
RuleConditionMbps	String	100	入方向带宽阈值，单位：Mbps。最小值： 100 。
RuleName	String	ddosbgp-cn-z2q1qzxb****	调度规则的名称。
RuleSwitch	String	on	调度规则的开关状态。取值： <ul style="list-style-type: none"> on：表示开启。 off：表示关闭。
RuleUndoBeginTime	String	03:00	自动停止调度的开始时间。使用24小时制表示，格式： hh:mm 。 当系统检测到攻击停止后，会在此处设置的时间开始停止代播防护。建议您将该时间设置为业务低峰期。 说明 该参数仅在使用自动停止调度（ RuleUndoMode 设置为 auto ）时生效。

名称	类型	示例值	描述
RuleUndoEndTime	String	03:05	自动停止调度的结束时间。使用24小时制表示，格式： hh:mm 。
RuleUndoMode	String	auto	调度规则的停止方式。取值： <ul style="list-style-type: none"> auto：表示自动停止调度。 manual：表示手动停止调度。
TimeZone	String	GMT-08:00	自动停止调度时间对应的时区。使用格林威治时间表示，格式： GMT-hh:mm 。 例如， GMT-08:00 表示东八区。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p>? 说明 该参数仅在使用自动停止调度（RuleUndoMode设置为auto）时生效。</p> </div>
RuleStatus	Array of Status		调度规则的状态信息。
Net	String	47.***.***.0/24	代播网段。
RuleScheduledStatus	String	unscheduled	调度状态。取值： <ul style="list-style-type: none"> scheduled：表示调度中。 unscheduled：表示不在调度中。
UserId	String	171986973287****	阿里云账号ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=QuerySchedruleOnDemand
&InstanceId=ddosbgp-cn-z2q1qzxb****
&<公共请求参数>
```

正常返回示例

XML 格式

```
<QuerySchedruleOnDemandResponse>
  <RequestId>4A8F9980-5ACB-497F-9F15-48E9D6B29028</RequestId>
  <Instanceld>ddosbgp-cn-z2q1qzxb****</Instanceld>
  <UserId>171986973287****</UserId>
  <RuleStatus>
    <RuleSchedStatus>unscheduled</RuleSchedStatus>
    <Net>47.***.***.0/24</Net>
  </RuleStatus>
  <RuleConfig>
    <RuleUndoEndTime>03:05</RuleUndoEndTime>
    <RuleSwitch>on</RuleSwitch>
    <TimeZone>GMT-08:00</TimeZone>
    <RuleConditionCnt>3</RuleConditionCnt>
    <RuleAction>declare</RuleAction>
    <RuleConditionMbps>100</RuleConditionMbps>
    <RuleConditionKpps>10</RuleConditionKpps>
    <RuleUndoMode>auto</RuleUndoMode>
    <RuleName>ddosbgp-cn-z2q1qzxb****</RuleName>
    <RuleUndoBeginTime>03:00</RuleUndoBeginTime>
  </RuleConfig>
</QuerySchedruleOnDemandResponse>
```

JSON 格式

```
{
  "RequestId": "4A8F9980-5ACB-497F-9F15-48E9D6B29028",
  "InstanceId": "ddosbgp-cn-z2q1qzxb****",
  "UserId": "171986973287****",
  "RuleStatus": [
    {
      "RuleSchedStatus": "unscheduled",
      "Net": "47.***.***.0/24"
    }
  ],
  "RuleConfig": [
    {
      "RuleUndoEndTime": "03:05",
      "RuleSwitch": "on",
      "TimeZone": "GMT-08:00",
      "RuleConditionCnt": "3",
      "RuleAction": "declare",
      "RuleConditionMbps": "100",
      "RuleConditionKpps": "10",
      "RuleUndoMode": "auto",
      "RuleName": "ddosbgp-cn-z2q1qzxb****",
      "RuleUndoBeginTime": "03:00"
    }
  ]
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.9.5. ConfigSchedruleOnDemand

调用ConfigSchedruleOnDemand修改代播实例的调度规则。

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
----	----	------	-----	----

名称	类型	是否必选	示例值	描述
Action	String	是	ConfigSchedruleOnDemand	要执行的操作。取值： ConfigSchedruleOnDemand 。
InstanceId	String	是	ddosbgp-cn-z2q1qzxb****	要操作的代播实例的ID。 说明 您可以调用 DescribeOnDemandInstance 查询所有代播实例的ID。
RuleAction	String	是	declare	调度动作。取值固定为 declare ，表示宣告路由。
RuleConditionCnt	String	是	3	当代播实例的入方向带宽或者报文数量连续超过阈值多少次时，将触发调度规则并开启代播防护。 说明 带宽阈值通过 RuleConditionMbps 参数设置，报文数阈值通过 RuleConditionKpps 参数设置。
RuleConditionKpps	String	是	10	入方向报文数阈值，单位：Kpps。最小值： 10 。
RuleConditionMbps	String	是	100	入方向带宽阈值，单位：Mbps。最小值： 100 。
RuleName	String	是	ddosbgp-cn-z2q1qzxb****	调度规则的名称。 支持使用英文小写字母、数字、短划线（-）和下划线（_），不超过32个字符。建议您使用代播实例的ID作为调度规则名称，例如， ddosbgp-cn-z2q1qzxb**** 。
RuleSwitch	String	是	on	调度规则的开关状态。取值： <ul style="list-style-type: none"> on：表示开启。 off：表示关闭。

名称	类型	是否必选	示例值	描述
RuleUndoBeginTime	String	是	03:00	<p>自动停止调度的开始时间。使用24小时制表示，格式：<code>hh:mm</code>。</p> <p>当系统检测到攻击停止后，会在此处设置的时间开始停止代播防护。建议您将该时间设置为业务低峰期。</p> <p>说明 该参数仅在使用自动停止调度（<code>RuleUndoMode</code>设置为<code>auto</code>）时生效。</p>
RuleUndoMode	String	是	manual	<p>调度规则的停止方式。取值：</p> <ul style="list-style-type: none"> <code>auto</code>：表示自动停止调度。 <code>manual</code>：表示手动停止调度。
TimeZone	String	是	GMT-08:00	<p>自动停止调度时间对应的时区。使用格林威治时间表示，格式：<code>GMT-hh:mm</code>。</p> <p>例如，<code>GMT-08:00</code>表示东八区。</p> <p>说明 该参数仅在使用自动停止调度（<code>RuleUndoMode</code>设置为<code>auto</code>）时生效。</p>
RuleUndoEndTime	String	否	03:05	<p>自动停止调度的结束时间。使用24小时制表示，格式：<code>hh:mm</code>。</p>
RegionId	String	否	cn-zhangjiakou	<p>代播实例的地域ID。</p> <p>说明 您可以调用<code>DescribeRegions</code>查询DDoS原生防护支持的所有地域信息。</p>

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

调用API的请求格式，请参见本文示例中的请求示例。

返回数据

名称	类型	示例值	描述
----	----	-----	----

名称	类型	示例值	描述
RequestId	String	BD06F539-2FBE-450D-9391-7EFF787128F5	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ConfigSchedruleOnDemand
&InstanceId=ddosbgp-cn-z2q1qzxb****
&RuleAction=declare
&RuleConditionCnt=3
&RuleConditionKpps=10
&RuleConditionMbps=100
&RuleName=ddosbgp-cn-z2q1qzxb****
&RuleSwitch=on
&RuleUndoBeginTime=03:00
&RuleUndoMode=manual
&TimeZone=GMT-08:00
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ConfigSchedruleOnDemandResponse>
  <RequestId>BD06F539-2FBE-450D-9391-7EFF787128F5</RequestId>
</ConfigSchedruleOnDemandResponse>
```

JSON 格式

```
{
  "RequestId": "BD06F539-2FBE-450D-9391-7EFF787128F5"
}
```

错误码

访问[错误中心](#)查看更多错误码。

2.9.6. DeleteSchedruleOnDemand

调用DeleteSchedruleOnDemand删除代播实例的调度规则。

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	DeleteSchedruleOnDemand	要执行的操作。取值： DeleteSchedruleOnDemand 。
Instanceid	String	是	ddosbgp-cn-z2q1qzxb****	要操作的代播实例的ID。 说明 您可以调用DescribeOnDemandInstance查询所有代播实例的ID。
RuleName	String	是	testrule	要删除的调度规则的名称。
RegionId	String	否	cn-zhangjiakou	代播实例的地域ID。 说明 您可以调用DescribeRegions查询DDoS原生防护支持的所有地域信息。

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

调用API的请求格式，请参见本文[示例](#)中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	BD06F539-2FBE-450D-9391-7EFF787128F5	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteSchedruleOnDemand
&Instanceid=ddosbgp-cn-z2q1qzxb****
&RuleName=testrule
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DeleteSchedruleOnDemandResponse>
  <RequestId>BD06F539-2FBE-450D-9391-7EFF787128F5</RequestId>
</DeleteSchedruleOnDemandResponse>
```

JSON 格式

```
{
  "RequestId": "BD06F539-2FBE-450D-9391-7EFF787128F5"
}
```

错误码

访问[错误中心](#)查看更多错误码。