阿里云
DDoS基础防护

API参考

文档版本：20190429

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
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能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，恢复业务所需时间约10分钟。
	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。	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。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 调用方式

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

请求结构

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

其请求结构如下：

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

其中：

- Endpoint：DDoS高防IP API的服务接入地址为ddospro.cn-hangzhou.aliyuncs.com。
- Action：要执行的操作，如使用DescribeInstancePage，查询高防Ip的实例信息。
- Version：要使用的API版本，DDoS高防IP的API版本是2017-07-25。
- Parameters：请求参数，每个参数之间用“&”分隔。
- 请求参数由公共请求参数和API自定义参数组成。公共参数中包含API版本号、身份验证等信息，详情参见公共参数。

下面是一个调用DescribeInstancePage接口查询高防Ip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://ddospro.cn-hangzhou.aliyuncs.com/?Action=DescribeInstancePage
&Region=cn
&InstanceId=ddospro-cn-XXXX1
&Format=xml
&Version=2017-07-25
&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高防IP API，您需要为该RAM账号创建、附加相应的授权策略。

API签名

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

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

RPC API需按如下格式在请求中增加签名（Signature）：

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

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

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DescribeInstancePage
&Region=cn
&InstanceId=ddospro-cn-XXXX1
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2017-07-25
&SignatureVersion=1.0
```

完成以下步骤计算签名：

1. 使用请求参数创建待签名字符串：

   ```
   GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeDomainNames&Region
   %3Dcn&InstanceId%3Dwaf_elasticity-cn-0xldbqtm005&Format%3DXML&
   SignatureMethod%3DHMAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-
   a94f-4e0ad82fd6cf&SignatureVersion%3D1.0&TimeStamp%3D2016-02-23T12%
   253A46%253A24Z&Version%3D2018-01-17
   ```

2. 计算待签名的HMAC的值。

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

   ```
   CT9X0VtwR86fNWSnsc6v8YGOjuE=
   ```

3. 将签名加到请求参数中：

   ```
   https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DescribeIn
   stancePage
   &Region=cn
   &InstanceId=ddospro-cn-XXXX1
   ```

```
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2017-07-25
&SignatureVersion=1.0
&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D
```

2 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
Region	String	是	DDoS高防IP实例所在的地域。取值：cn-hangzhou（表示中国大陆地区）。
Format	String	否	返回消息的格式。取值： · JSON（默认） · XML
Version	String	是	API版本号，使用YYYY-MM-DD日期格式。取值：2017-07-25。
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://ddospro.cn-hangzhou.aliyuncs.com/?Action=DescribeInstancePage
&Region=cn
&InstanceId=ddospro-cn-XXXX1
&Timestamp=2014-05-19T10%3A33%3A56Z
&Format=xml
&AccessKeyId=testid
&SignatureMethod=Hmac-SHA1
&SignatureNonce=NwDAxvLU6tFE0DVb
&Version=2017-07-25
```

```
&SignatureVersion=1.0
&Signature=Signature
```

公共返回参数

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

每次接口调用，无论成功与否，系统都会返回一个唯一识别码RequestId。

- XML格式

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

- JSON格式

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

3 报表

3.1 DescribeDdosAttackTypeChart

调用DescribeDdosAttackTypeChart接口查询高防IP的攻击类型概览图表。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDdosAttackTypeChart	要执行的操作。取值：DescribeDdosAttackTypeChart。
EndTime	Long	是	1536891600	查询结束时间戳，单位为毫秒。
Ip	String	是	1.1.1.1	要查询的高防实例IP。
StartTime	Long	是	1536893404	查询开始时间戳，单位为毫秒。

返回参数

名称	类型	示例值	描述
AttckCount	Integer	6	攻击种类个数。
AttckType	String	udp-flood	攻击种类，取值： · tcp-flood · udp-flood · icmp-flood · finrst-flood
DropCount	Integer	405322	清洗包大小，单位为Kbps。
DropType	String	udp	清洗的攻击种类。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DescribeDdosAttackTy
peChart
&StartTime=1536891600
&EndTime=1536893404
&Ip=1.1.1.1
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDdosAttackTypeChartResponse>
  <AttackCount>6</AttackCount>
  <AttackType>udp-flood</AttackType>
  <DropCount>405322</DropCount>
  <DropType>udp</DropType>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</DescribeDdosAttackTypeChartResponse>
```

`JSON` 格式

```
{
 "AttackType":"udp-flood",
 "DropType":"udp",
 "DropCount":405322,
 "AttackCount":6,
 "RequestId":"C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

查看本产品错误码

3.2 DescribeDdosPeakFlow

调用DescribeDdosPeakFlow接口查询高防IP的攻击峰值。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDdosPeakFlow	要执行的操作。取值：DescribeDdosPeakFlow。
Ip	String	是	1.1.1.1	要查询的高防实例IP。
EndTime	Long	否	1536893404	查询结束时间戳，单位为毫秒。
StartTime	Long	否	1536891600	查询开始时间戳，单位为毫秒。

返回参数

名称	类型	示例值	描述
PeakFlow	String	8.36	攻击峰值，单位为G。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DescribeDdosPeakFlow
&StartTime=1536891600
&EndTime=1536893404
&Ip=1.1.1.1
&公共请求参数
```

正常返回示例

`XML` 格式

```
<DescribeDdosPeakFlowResponse>
  <PeakFlow>8.36</PeakFlow>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</DescribeDdosPeakFlowResponse>
```

`JSON` 格式

```
{
 "RequestId":"C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
 "PeakFlow":"8.36"
}
```

错误码

查看本产品错误码

3.3 DescribeDdosFlowProportionDiagram

调用DescribeDdosFlowProportionDiagram接口查询高防IP的攻击比例图表。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDdosFlowProportionDiagram	要执行的操作。取值：DescribeDdosFlowProportionDiagram。
EndTime	Long	是	1536893404	查询结束时间戳，单位为毫秒。时间跨度不能超过30天。
Ip	String	是	1.1.1.1	要查询的高防实例IP。
StartTime	Long	是	1536891600	查询开始时间戳，单位为毫秒。

返回参数

名称	类型	示例值	描述
DropBps	Integer	27729882	攻击流量大小，单位为Bps。
DropPps	Integer	3264010	攻击数据包个数。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
TotalBps	Integer	27854138	总流量大小，单位Bps。
TotalPps	Integer	3374169	总数据包个数。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DescribeDdosFlowProp
ortionDiagram
&StartTime=1536891600
&EndTime=1536893404
&Ip=1.1.1.1
&公共请求参数
```

正常返回示例

`XML` **格式**

```
<DescribeDdosFlowProportionDiagramResponse>
  <DropBps>27729882</DropBps>
  <DropPps>3264010</DropPps>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <TotalBps>27854138</TotalBps>
  <TotalPps>3374169</TotalPps>
</DescribeDdosFlowProportionDiagramResponse>
```

`JSON` **格式**

```
{
 "DropBps":27729882,
 "TotalBps":27854138,
 "RequestId":"C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
 "TotalPps":3374169,
 "DropPps":3264010
}
```

错误码

查看本产品错误码

3.4 DescribeDdosAttackEvents

调用DescribeDdosAttackEvents接口查询高防IP的攻击事件。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDdosAttackEvents	要执行的操作。取值：DescribeDdosAttackEvents。
CurrentPage	Integer	是	1	分页页号，最小值为1。

名称	类型	是否必选	示例值	描述
EndTime	Long	是	1536893404	查询结束时间戳，单位为毫秒。时间跨度不能超过30天。
Ip	String	是	1.1.1.1	要查询的高防实例IP。
PageSize	Integer	是	10	分页大小，最大值为20。
StartTime	Long	是	1536891600	查询开始时间戳，单位为毫秒。

返回参数

名称	类型	示例值	描述
Data			攻击事件信息，包括事件总数和事件列表。
└EventList			攻击事件列表。
└AttackType	String	syn-flood	攻击类型，取值： · tcp-flood · udp-flood · icmp-flood · finrst-flood
└EndTime	Long	1535019587000	攻击结束时间戳，单位为毫秒。
└Result	Integer	1	事件结果，取值： · 0：清洗中 · 1：清洗成功 · 3：黑洞结束
└StartTime	Long	1535018684000	攻击开始时间戳，单位为毫秒。
└TotalCount	Integer	4	事件总数。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DescribeDdosAttackEv
ents
&StartTime=1536891600
&EndTime=1536893404
&Ip=1.1.1.1
```

```
&CurrentPage=1
&PageSize=10
&公共请求参数
```

正常返回示例

`XML` **格式**

```
<DescribeDdosAttackEventsResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <Data>
    <TotalCount>4</TotalCount>
    <EventList>
      <EndTime>1535019587000</EndTime>
      <StartTime>1535018684000</StartTime>
      <AttackType>syn-flood</AttackType>
      <Result>1</Result>
    </EventList>
  </Data>
</DescribeDdosAttackEventsResponse>
```

`JSON` **格式**

```
{
 "Data":{
  "EventList":[
   {
    "Result":1,
    "AttackType":"syn-flood",
    "EndTime":1535019587000,
    "StartTime":1535018684000
   }
  ],
  "TotalCount":4
 },
 "RequestId":"C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

查看本产品错误码

3.5 DescribeDdosAttackEventSourceIps

调用DescribeDdosAttackEventSourceIps接口查询高防IP攻击事件的源攻击IP列表。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDdosAttackEventSourceIps	要执行的操作。取值：DescribeDdosAttackEventSourceIps。
CurrentPage	Integer	是	1	分页页号，最小值为1。
EndTime	Long	是	1536893404	查询结束时间戳，单位为毫秒。时间跨度不能超过30天。
Ip	String	是	1.1.1.1	要查询的高防实例IP。
PageSize	Integer	是	10	分页大小，最大值为20。
StartTime	Long	是	1536891600	查询开始时间戳，单位为毫秒。

返回参数

名称	类型	示例值	描述
Data			攻击源IP信息，包括总数和列表。
└IpList			攻击源IP列表。
└City	String	中国-辽宁省-大连市	攻击来源城市。
└InBps	Integer	65798144	攻击流量大小，单位Bps。
└SourceIp	String	2.2.2.2	攻击源IP。
└TotalCount	Integer	55	事件总数。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DescribeDdosAttackEventSourceIps
&StartTime=1536891600
&EndTime=1536893404
&Ip=1.1.1.1
&CurrentPage=1
&PageSize=10
&公共请求参数
```

正常返回示例

XML 格式

```
<DescribeDdosAttackEventSourceIpsResponse>
  <Data>
    <IpList>
      <element>
        <City>中国-辽宁省-大连市</City>
        <InBps>65798144</InBps>
        <SourceIp>2.2.2.2</SourceIp>
      </element>
    </IpList>
    <TotalCount>55</TotalCount>
  </Data>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</DescribeDdosAttackEventSourceIpsResponse>
```

JSON 格式

```
{
 "Data":{
  "TotalCount":55,
  "IpList":[
   {
    "City":"中国-辽宁省-大连市",
    "SourceIp":"2.2.2.2",
    "InBps":65798144
   }
  ]
 },
 "RequestId":"C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

查看本产品错误码

3.6 DescribeCcEvents

调用DescribeCcEvents接口查询用户域名的CC攻击事件。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

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

名称	类型	是否必选	示例值	描述
Domain	String	否	www.aliyun.com	要查询的域名。
EndTime	Long	否	1534921519	查询结束时间戳，单位为秒。时间跨度不能超过30天。
PageNo	Integer	否	1	分页页号，最小值为1。
PageSize	Integer	否	10	分页大小，最大值为20。
StartTime	Long	否	1536891600	查询开始时间戳，单位为秒。

返回参数

名称	类型	示例值	描述
EventList			攻击事件列表。
└AttackFinished	Boolean	true	攻击是否结束。
└BlockedCount	Integer	1041	攻击被阻断次数。
└Domain	String	www.aliyun.com	域名。
└Duration	Integer	3	攻击持续时长，单位小时
└EndTime	String	2018-08-23 10:29:00	攻击结束时间。
└MaxQps	Integer	274	峰值QPS。
└StartTime	String	2018-08-23 10:26:00	攻击开始时间。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
Total	Integer	3	攻击事件总数。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DescribeCcEvents
&StartTime=1536891600
&EndTime=1534921519
&Domain=www.aliyun.com
```

```
&PageNo=1
&PageSize=10
&公共请求参数
```

正常返回示例

`XML` **格式**

```
<DescribeCcEventsResponse>
  <EventList>
    <element>
      <AttackFinished>true</AttackFinished>
      <BlockedCount>1041</BlockedCount>
      <Domain>www.aliyun.com</Domain>
      <Duration>3</Duration>
      <EndTime>2018-08-23 10:29:00</EndTime>
      <MaxQps>274</MaxQps>
      <StartTime>2018-08-23 10:26:00</StartTime>
    </element>
  </EventList>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <Total>3</Total>
</DescribeCcEventsResponse>
```

`JSON` **格式**

```
{
 "EventList":[
  {
   "BlockedCount":1041,
   "Domain":"www.aliyun.com",
   "Duration":3,
   "MaxQps":274,
   "EndTime":"2018-08-23 10:29:00",
   "StartTime":"2018-08-23 10:26:00",
   "AttackFinished":true
  }
 ],
 "RequestId":"C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
 "Total":3
}
```

错误码

查看本产品错误码

3.7 DescribeBizFlow

调用DescribeBizFlow接口查询高防IP上的业务流量信息，包括入方向和出方向流量。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeBizFlow	要执行的操作。取值：DescribeBizFlow。
EndTime	Long	是	1536498197	查询结束时间戳，单位为秒。
Ip	String	是	1.1.1.1	要查询的高防IP。
StartTime	Long	是	1536496397	查询开始时间戳，单位为秒。

返回参数

名称	类型	示例值	描述
Data			流量查询结果。  说明: 您可以根据该结果进行图表绘制。
└InKbps		[1,1,1,1,1,1]	入流量查询结果列表，每个数据为该时间点上的入流量大小，单位为Kbps。  说明: 该数据对应的时间点可以根据TimeScope信息进行计算。
└OutKbps		[1,1,1,1,1,1]	出流量查询结果列表，每个数据为该时间点上的出流量大小，单位为Kbps。  说明: 该数据对应的时间点可以根据TimeScope信息进行计算。
└TimeScope			时间范围信息。
└Interval	Integer	60	流量点列表中相邻两个点的时间差，单位为秒。
└StartTime	Long	1536496397	查询开始时间戳，单位为秒。
RequestId	String	C8B26B44-0189-443E-9816-D951F59623A9	本次请求的ID。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DescribeBizFlow
&EndTime=1536498197
&Ip=1.1.1.1
&StartTime=1536496397
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeBizFlowResponse>
  <Data>
    <InKbps>
      <element>0</element>
      <element>1</element>
      <element>1</element>
      <element>0</element>
      <element>0</element>
      <element>1</element>
      <element>1</element>
      <element>0</element>
      <element>1</element>
      <element>4</element>
      <element>0</element>
      <element>1</element>
      <element>1</element>
      <element>0</element>
      <element>1</element>
      <element>2</element>
      <element>0</element>
      <element>1</element>
      <element>1</element>
      <element>1</element>
      <element>0</element>
      <element>0</element>
      <element>1</element>
      <element>0</element>
      <element>1</element>
      <element>0</element>
      <element>1</element>
      <element>0</element>
      <element>0</element>
      <element>2</element>
      <element>0</element>
    </InKbps>
    <OutKbps>
      <element>0</element>
      <element>0</element>
      <element>0</element>
      <element>0</element>
      <element>0</element>
      <element>0</element>
      <element>0</element>
      <element>0</element>
      <element>0</element>
      <element>0</element>
```

```
        <element>0</element>
        <element>0</element>
        <element>0</element>
        <element>0</element>
        <element>0</element>
        <element>0</element>
        <element>0</element>
        <element>0</element>
        <element>0</element>
        <element>0</element>
        <element>0</element>
        <element>0</element>
        <element>0</element>
        <element>0</element>
        <element>0</element>
        <element>0</element>
        <element>0</element>
        <element>0</element>
        <element>0</element>
        <element>0</element>
      </OutKbps>
      <TimeScope>
        <Interval>60</Interval>
        <StartTime>1536496380</StartTime>
      </TimeScope>
    </Data>
    <requestId>C8B26B44-0189-443E-9816-D951F59623A9</requestId>
</DescribeBizFlowResponse>
```

JSON 格式

```
{
 "Data":{
  "InKbps":[
   0,
   1,
   1,
   0,
   0,
   1,
   1,
   0,
   1,
   4,
   0,
   1,
   1,
   0,
   1,
   2,
   0,
   1,
   1,
   1,
   0,
   0,
   1,
   0,
   1,
   0,
   1,
   0,
```

```
    0,
    2,
    0
   ],
   "TimeScope":{
    "Interval":60,
    "StartTime":1536496380
   },
   "OutKbps":[
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0
   ]
  },
  "requestId":"C8B26B44-0189-443E-9816-D951F59623A9"
}
```


错误码

查看本产品错误码

4 网站功能

4.1 DescribeDomainConfigPage

调用DescribeDomainConfigPage接口分页查询用户的网站配置列表。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainConfigPage	要执行的操作。取值：DescribeDomainConfigPage。
PageNo	Integer	是	1	分页页号，最小值为1。
PageSize	Integer	是	5	分页大小，最大值为5。
Domain	String	否	www.aliyun.com	要查询的域名。支持模糊查询。

返回参数

名称	类型	示例值	描述
ConfigList			网站配置列表。
└Cname	String	xxxxxx.alicloudddos.com	高防Cname值。
└Domain	String	www.aliyun.com	被防护的域名。
└Instances			与域名配置关联的高防实例信息。
└InstanceId	String	ddosbag-xxxx-xxxx	高防实例ID。
└InstanceRemark	String	高防实例1	高防IP的实例备注。
└Rules			转发规则。

名称	类型	示例值	描述
└Ip	String	1.1.1.1	高防实例IP。
└Line	String	CT	线路，取值： · MT：移动 · CT：电信 · CUT：联通 · BGP：BGP
└ProxyTypeList		["https", "http"]	转发协议列表，取值： · http · https · websocket · websockets
└RealServers		["2.2.2.2", "3.3.3.3"]	源站列表。
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
Total	Integer	10	配置总数。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainConfigPage
&Domain=www.aliyun.com
&PageNo=1
&PageSize=10
&公共请求参数
```

正常返回示例

`XML` 格式

```
<DescribeDomainConfigPageResponse>
  <ConfigList>
    <element>
      <Cname>xxxxxxxxxxxxx.alicloudddos.com</Cname>
      <Domain>www.aliyun.com</Domain>
      <Instances>
        <element>
          <InstanceId>ddosBag-cn-XXXXX</InstanceId>
          <Rules>
            <element>
              <Ip>3.3.3.3</Ip>
```

```
              <Line>CUT</Line>
              <ProxyTypeList>
                <element>http</element>
                <element>https</element>
              </ProxyTypeList>
              <RealServers>
                <element>1.1.1.1</element>
                <element>2.2.2.2</element>
              </RealServers>
            </element>
          </Rules>
        </element>
      </Instances>
    </element>
  </ConfigList>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <Total>6</Total>
</DescribeDomainConfigPageResponse>
```

JSON 格式

```
{
 "RequestId":"C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
 "ConfigList":[
  {
   "Cname":"xxxxxxxxxxxxx.alicloudddos.com",
   "Domain":"www.aliyun.com",
   "Instances":[
    {
     "InstanceId":"ddosBag-cn-XXXXX",
     "Rules":[
      {
       "Ip":"3.3.3.3",
       "ProxyTypeList":[
        "http",
        "https"
       ],
       "RealServers":[
        "1.1.1.1",
        "2.2.2.2"
       ],
       "Line":"CUT"
      }
     ]
    }
   ]
  }
 ],
 "Total":6
}
```

错误码

查看本产品错误码

4.2 DescribeDomainSecurityConfig

调用DescribeDomainSecurityConfig接口查询用户域名的安全防护配置。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainSecurityConfig	要执行的操作。取值：DescribeDomainSecurityConfig。
Domain	String	否	www.aliyun.com	要查询的域名。

返回参数

名称	类型	示例值	描述
BlackList	String	1.1.1.1,2.2.2.2	黑名单列表。
CcInfo			CC防护配置信息。
└ CcCustomRuleCount	Integer	10	CC自定义规则总数。
└ CcCustomRuleEnable	Boolean	true	CC自定义规则功能开关。
└CcSwitch	Boolean	true	CC攻击防护功能开关。
└ CcTemplate	String	danger	CC防护模式，取值： · default：正常 · gf_under_attack：攻击紧急 · gf_sos_verify：严格 · gf_sos_enhance：非常严格
CnameEnable	Boolean	true	Cname开关。
CnameMode	Integer	1	调度模式，取值： · 0：优先级方式 · 1：负载均衡方式

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
WhiteList	String	1.1.1.1,2.2.2.2	白名单列表。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainSecurityConfig
&Domain=www.aliyun.com
&公共请求参数
```

正常返回示例

`XML` 格式

```
<DescribeDomainSecurityConfigResponse>
  <BlackList>1.1.1.1,2.2.2.2</BlackList>
  <CcInfo>
    <CcCustomRuleCount>10</CcCustomRuleCount>
    <CcCustomRuleEnable>true</CcCustomRuleEnable>
    <CcSwitch>true</CcSwitch>
    <CcTemplate>danger</CcTemplate>
  </CcInfo>
  <CnameEnable>true</CnameEnable>
  <CnameMode>0</CnameMode>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <WhiteList>1.1.1.1,2.2.2.2</WhiteList>
</DescribeDomainSecurityConfigResponse>
```

`JSON` 格式

```
{
 "CcInfo":{
  "CcSwitch":true,
  "CcCustomRuleCount":10,
  "CcTemplate":"danger",
  "CcCustomRuleEnable":true
 },
 "CnameMode":0,
 "BlackList":"1.1.1.1,2.2.2.2",
 "CnameEnable":true,
 "RequestId":"C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
 "WhiteList":"1.1.1.1,2.2.2.2"
}
```

错误码

查看本产品错误码

4.3 ListCcCustomedRule

调用ListCcCustomedRule接口查询用户的自定义CC规则。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ListCcCustomedRule	要执行的操作。取值：ListCcCustomedRule。
CurrentPage	Integer	否	1	分页页号，最小值为1。
Domain	String	否	ww.aliyun.com	要查询的域名。
PageSize	Integer	否	10	分页大小，最大值为10。

返回参数

名称	类型	示例值	描述
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	本次请求的ID。
RuleList			自定义CC规则列表。
└BlockingTime	Integer	60	阻断时间，单位为秒，取值范围：60~86,400。
└BlockingType	String	captcha	阻断类型，取值： · captcha：人机识别 · close：封禁
└Interval	Integer	5	检测时长，单位为秒，取值范围：5~10,800。
└MatchingRule	String	prefix	匹配规则，取值： · prefix：前缀模式 · match：完全匹配

名称	类型	示例值	描述
└Name	String	customedCcRule1	自定CC规则名称。 说明: 您可以通过该名称找到对应规则，并进行修改、删除操作。
└Uri	String	/a/b/c	防护路径。
└VisitCount	Integer	200	允许的单一IP访问次数，取值范围：2~2,000。
TotalCount	Integer	10	规则总数。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=ListCcCustomedRule
&Domain=www.aliyun.com
&CurrentPage=1
&PageSize=10
&公共请求参数
```

正常返回示例

`XML` 格式

```
<ListCcCustomedRuleResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <RuleList>
    <Rule>
      <element>
        <BlockingTime>7380</BlockingTime>
        <BlockingType>close</BlockingType>
        <Interval>123</Interval>
        <MatchingRule>match</MatchingRule>
        <Name>testttt</Name>
        <Uri>/a/a/a</Uri>
        <VisitCount>123</VisitCount>
      </element>
    </Rule>
  </RuleList>
  <TotalCount>3</TotalCount>
</ListCcCustomedRuleResponse>
```

`JSON` 格式

```
{
 "RuleList":{
  "Rule":[
   {
    "Name":"testttt",
    "BlockingType":"close",
```

```
      "VisitCount":123,
      "Interval":123,
      "BlockingTime":7380,
      "Uri":"/a/a/a",
      "MatchingRule":"match"
    }
   ]
  },
  "TotalCount":3,
  "RequestId":"C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```


错误码

查看本产品错误码

4.4 CreateDomain

调用CreateDomain接口创建网站防护规则。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateDomain	要执行的操作。取值：CreateDomain。
Domain	String	是	www.aliyun.com	添加要防护的域名。
ProxyType.N	RepeatLis	是	http	转发类型，取值： · http · https · websocket · websockets 说明： 若有多个类型，依次传入ProxyType.1、ProxyType.2、ProxyType.3

名称	类型	是否必选	示例值	描述
RealServer.N	RepeatList	是	1.1.1.1	源站列表。  说明: 若有多个源站，依次传入RealServer.1、RealServer.2、RealServer.
Type	String	是	IP	选择回源类型，取值： · IP：回源到Ip · DOMAIN：回源到域名
CcEnable	Boolean	否	true	是否开启CC攻击防护功能。
Ips.N	RepeatList	否	1.1.1.1	防护解析到的高防IP列表，最多支持6个IP。  说明: 若有多个高防IP，依次传入Ips.1、Ips.2、Ips.3 ...

返回参数

名称	类型	示例值	描述
RequestId	String	C8B26B44-0189-443E-9816-D951F59623A9	本次请求的ID。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=CreateDomain
&Domain=www.aliyun.com
&Ips=["1.1.1.1","2.2.2.2"]
&RealServer=["1.1.1.1","2.2.2.2"]
&Type=IP
&CcEnable=true
&ProxyType=["http","https"]
&公共请求参数
```

正常返回示例

XML 格式

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

```
</CreateDomainResponse>
```

JSON 格式

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

错误码

查看本产品错误码

4.5 DeleteDomain

调用DeleteDomain接口删除网站防护规则。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteDomain	要执行的操作。取值：DeleteDomain。
Domain	String	是	www.aliyun.com	要移除的域名。

返回参数

名称	类型	示例值	描述
RequestId	String	C8B26B44-0189-443E-9816-D951F59623A9	本次请求的ID。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DeleteDomain
&Domain=www.aliyun.com
&公共请求参数
```

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

查看本产品错误码

4.6 CreateTransmitLine

调用CreateTransmitLine接口添加网站防护转发线路。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateTransmitLine	要执行的操作。取值：CreateTransmitLine。
Domain	String	否	www.aliyun.com	要操作的域名。
Ips.N	RepeatList	否	1.1.1.1	高防IP列表。 说明: 若有多个列表，依次传入Ips.1、Ips.2、Ips.3 ...
RealServers.N	RepeatList	否	2.2.2.2	源站列表。 说明: 若有多个源站，依次传入RealServer.1、RealServer.2、RealServer.

名称	类型	是否必选	示例值	描述
Type	String	否	IP	回源类型，取值： · IP：回源到Ip · DOMAIN：回源到域名

返回参数

名称	类型	示例值	描述
RequestId	String	C8B26B44-0189-443E-9816-D951F59623A9	本次请求的ID。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=CreateTransmitLine
&Domain=www.aliyun.com
&Ips=["1.1.1.1","2.2.2.2"]
&RealServer=["1.1.1.1","2.2.2.2"]
&Type=IP
&公共请求参数
```

正常返回示例

XML 格式

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

JSON 格式

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

错误码

查看本产品错误码

4.7 ModifyTransmitLine

调用ModifyTransmitLine接口修改网站防护转发线路。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyTransmitLine	要执行的操作。取值：ModifyTransmitLine。
Domain	String	否	www.aliyun.com	要操作的域名。
Ips.N	RepeatList	否	1.1.1.1	高防IP列表。 说明: 若有多个高防IP，依次传入Ips.1、Ips.2、Ips.3 ...

返回参数

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

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=ModifyTransmitLine
&Domain=www.aliyun.com
&Ips=["1.1.1.1","2.2.2.2"]
&公共请求参数
```

正常返回示例

`XML` 格式

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

`JSON` 格式

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

```
}
```

错误码

查看本产品错误码

4.8 DeleteTransmitLine

调用DeleteTransmitLine接口删除网站防护转发线路。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteTransmitLine	要执行的操作。取值：DeleteTransmitLine。
Domain	String	否	www.aliyun.com	要操作的域名。
Line	String	否	CUT	要删除的线路，取值： · BGP：bgp线路 · CT：电信 · CUT：联通 · MT：移动

返回参数

名称	类型	示例值	描述
RequestId	String	C8B26B44-0189-443E-9816-D951F59623A9	本次请求的ID。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DeleteTransmitLine
&Domain=www.aliyun.com
&Line=BGP
```

```
&公共请求参数
```

正常返回示例

`XML` **格式**

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

`JSON` **格式**

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

错误码

查看本产品错误码

4.9 ModifyIpCnameStatus

调用ModifyIpCnameStatus接口修改网站防护中高防IP的Cname解析状态。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyIpCnameStatus	要执行的操作。取值：ModifyIpCnameStatus。
Domain	String	否	www.aliyun.com	要操作的域名。
Enable	Boolean	否	true	是否开启Cname解析。
Ip	String	否	1.1.1.1	要操作的高防IP。

返回参数

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

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=ModifyIpCnameStatus
&Domain=www.aliyun.com
&Ip=1.1.1.1
&Enable=true
&公共请求参数
```

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

查看本产品错误码

4.10 ModifyRealServers

调用ModifyRealServers接口修改网站防护配置中线路对应的源站。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyRealServers	要执行的操作。取值：ModifyRealServers。
Domain	String	否	www.aliyun.com	要操作的域名。
Line	String	否	CUT	要操作的线路，取值： · BGP：BGP线路 · CT：电信 · CUT：联通 · MT：移动
RealServers.N	RepeatList	否	1.1.1.1	源站列表。 说明： 若有多个源站，依次传入RealServer.1、RealServer.2、RealServer.
Type	String	否	IP	回源类型，取值： · IP：回源到Ip · DOMAIN：回源到域名

返回参数

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

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=ModifyRealServers
&Domain=www.aliyun.com
&Line=BGP
&Type=IP
&RealServers=["1.1.1.1","2.2.2.2"]
&公共请求参数
```

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

查看本产品错误码

4.11 ConfigSwitchPriority

调用ConfigSwitchPriority接口修改网站防护中高防IP的调度优先级。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
`Action`	String	是	ConfigSwitchPriority	要执行的操作。取值：ConfigSwitchPriority。
`Domain`	String	是	www.aliyun.com	要操作的域名。
`Config.N.Ip`	String	否	1.1.1.1	高防实例IP。 说明: 多值时依次传入Config.1.Ip、Config.2.Ip、Config.3.Ip ...
`Config.N.Priority`	Integer	否	30	优先级大小，取值：1~999。取值越小优先级越高。 说明: 多值时依次传入Config.1.Priority、Config.2.Priority、Co

返回参数

名称	类型	示例值	描述
RequestId	String	C8B26B44-0189-443E-9816-D951F59623A9	本次请求的ID。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=ConfigSwitchPriority
&Domain=www.aliyun.com
&Config=[{"ip":"1.1.1.1","priority":50}]
&公共请求参数
```

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

查看本产品错误码

4.12 ModifyDomainProxy

调用ModifyDomainProxy接口修改网站防护的转发协议。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyDomainProxy	要执行的操作。取值：ModifyDomainProxy。
Domain	String	是	www.aliyun.com	要操作的域名。
ProxyType.N	RepeatList	是	https	转发协议类型，取值： · http · https · websocket · websockets  说明： 若有多个协议类型，依次传入ProxyType.1、ProxyType.2、ProxyType.3

返回参数

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

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=ModifyDomainProxy
&Domain=www.aliyun.com
&ProxyType=["http","https"]
&公共请求参数
```

正常返回示例

`XML` 格式

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

`JSON` 格式

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

```
}
```

错误码

查看本产品错误码

4.13 ModifyDomainBlackWhiteList

调用ModifyDomainBlackWhiteList接口修改网站安全防护的黑白名单。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyDomainBlackWhiteList	要执行的操作。取值：ModifyDomainBlackWhiteList。
Domain	String	是	www.aliyun.com	要操作的域名。
Black.N	RepeatList	否	2.2.2.2/24	传入黑名单IP或IP段列表。 说明： 若传入空列表，则表示清空黑名单。多值时依次传入Black.1、Black.2、Black.3 ...
White.N	RepeatList	否	1.1.1.1/24	传入白名单IP或IP段列表。 说明： 若传入空列表，则表示清空白名单。多值时依次传入White.1、White.2、White.3 ...

返回参数

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

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=ModifyDomainBlackWhiteList
&Domain=www.aliyun.com
&Black.1=2.2.2.2/24
&White.1=1.1.1.1/24
&公共请求参数
```

正常返回示例

`XML` **格式**

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

`JSON` **格式**

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

错误码

查看本产品错误码

4.14 ModifyCcStatus

调用ModifyCcStatus接口启用或禁用网站安全CC攻击防护功能。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyCcStatus	要执行的操作。取值：ModifyCcStatus。
Domain	String	是	www.aliyun.com	要操作的域名。
Enable	Boolean	是	true	设置CC攻击防护开关状态。

返回参数

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

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=ModifyCcStatus
&Domain=www.aliyun.com
&Enable=true
&公共请求参数
```

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

查看本产品错误码

4.15 ModifyCcTemplate

调用ModifyCcTemplate接口修改网站安全防护CC防护模式。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyCcTemplate	要执行的操作。取值：ModifyCcTemplate。
Domain	String	是	www.aliyun.com	要操作的域名。
Mode	Integer	是	0	设置CC防护模式，取值： · 0：正常 · 1：攻击紧急 · 2：严格 · 3：超级严格

返回参数

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

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=ModifyCcTemplate
&Domain=www.aliyun.com
&Mode=0
&公共请求参数
```

正常返回示例

XML 格式

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

```
</ModifyCcTemplateResponse>
```

JSON 格式

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

错误码

查看本产品错误码

4.16 ModifyCcCustomStatus

调用ModifyCcCustomStatus接口启用或禁用网站安全防护CC自定义规则。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyCcCustomStatus	要执行的操作。取值：ModifyCcCustomStatus。
Domain	String	是	www.aliyun.com	要操作的域名。
Enable	Boolean	是	true	是否启用CC自定义规则。

返回参数

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

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=ModifyCcCustomStatus
&Domain=www.aliyun.com
&Enable=true
```

```
&公共请求参数
```

正常返回示例

`XML` **格式**

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

`JSON` **格式**

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

错误码

查看本产品错误码

4.17 CreateCcCustomedRule

调用CreateCcCustomedRule接口创建网站安全防护CC自定义规则。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateCcCustomedRule	要执行的操作。取值：CreateCcCustomedRule。
BlockingTime	Integer	是	60	设置阻断时间，单位为秒，取值范围：60~86,400。
BlockingType	String	是	captcha	选择阻断类型，取值： · captcha：人机识别 · close：封禁
Domain	String	是	www.aliyun.com	要操作的域名。
Interval	Integer	是	5	设置检测时长，单位为秒，取值范围：5~10,800。

名称	类型	是否必选	示例值	描述
MatchingRule	String	是	prefix	选择匹配规则，取值： · prefix：前缀模式 · match：完全匹配
Name	String	是	customeCcRule1	设置规则名称。
Uri	String	是	/a/b/c	设置防护路径。
VisitCount	Integer	是	2	允许单一IP的访问次数，取值范围：2~2,000。

返回参数

名称	类型	示例值	描述
RequestId	String	C8B26B44-0189-443E-9816-D951F59623A9	本次请求的ID。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=CreateCcCustomedRule
&Domain=www.aliyun.com
&Name=testCcRule1
&Uri=/a/b/c
&MatchingRule=prefix
&Interval=100
&BlockingType=captcha
&BlockingTime=100
&VisitCount=100
&公共请求参数
```

正常返回示例

`XML` **格式**

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

`JSON` **格式**

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

错误码

查看本产品错误码

4.18 UpdateCcCustomedRule

调用UpdateCcCustomedRule接口修改网站安全防护CC自定义规则。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	UpdateCcCustomedRule	要执行的操作。取值：UpdateCcCustomedRule。
BlockingTime	Integer	是	100	设置阻断时间，单位为秒，取值范围：60~86,400。
BlockingType	String	是	captcha	选择阻断类型，取值： · captcha：人机识别 · close：封禁
Domain	String	是	www.aliyun.com	要操作的域名。
Interval	Integer	是	100	设置检测时长，单位为秒，取值范围：5~10,800。
MatchingRule	String	是	prefix	选择匹配规则，取值： · prefix：前缀模式 · match：完全匹配
Name	String	是	testCcRule1	设置规则名称。
Uri	String	是	/a/b/c	设置防护路径。
VisitCount	Integer	是	100	允许单一IP的访问次数，取值范围：2~2,000。

返回参数

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

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=UpdateCcCustomedRule
&Domain=www.aliyun.com
&Name=testCcRule1
&Uri=/a/b/c
&MatchingRule=prefix
&Interval=100
&BlockingType=captcha
&BlockingTime=100
&VisitCount=100
&公共请求参数
```

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

查看本产品错误码

4.19 DeleteCcCustomedRule

调用DeleteCcCustomedRule接口删除网站安全防护CC自定义规则。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteCcCustomedRule	要执行的操作。取值：DeleteCcCustomedRule。
Domain	String	是	www.aliyun.com	要操作的域名。
Name	String	是	customedCcRule1	要删除的规则的名称。

返回参数

名称	类型	示例值	描述
RequestId	String	C8B26B44-0189-443E-9816-D951F59623A9	本次请求的ID。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DeleteCcCustomedRule
&Domain=www.aliyun.com
&Name=testCcRule1
&公共请求参数
```

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

查看本产品错误码

4.20 DescribeBackSourceCidr

调用DescribeBackSourceCidr接口查询高防回源网段地址。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

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。
Line	String	否	bgp	要查询的线路类型。取值： · unicom：中国联通 · telecom：中国电信 · mobile：中国移动 · bgp：BGP线路
Region	String	否	hangzhou	要查询的地区。取值： 说明: 当Line传入bgp时必需。 · hangzhou：杭州 · beijing：北京 · shenzhen：深圳

返回参数

名称	类型	示例值	描述
CidrList		["180.97.165.0/24", "180.97.166.0/24"]	高防回源网段列表，结构描述如下： · Cidr，List类型，高防回源网段列表。
RequestId	String	C8B26B44-0189-443E-9816-D951F59623A9	本次请求的ID。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DescribeBackSourceCi
dr
&Line=telecom
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeBackSourceCidrResponse>
  <CidrList>
    <Cidr>
      <element>180.97.165.0/24</element>
      <element>180.97.166.0/24</element>
    </Cidr>
  </CidrList>
  <requestId>480AC85F-2B2A-49A4-A2DA-BF98AA96E8D6</requestId>
</DescribeBackSourceCidrResponse>
```

JSON 格式

```
{
 "requestId":"480AC85F-2B2A-49A4-A2DA-BF98AA96E8D6",
 "CidrList":{
  "Cidr":[
   "180.97.165.0/24",
   "180.97.166.0/24"
  ]
 }
}
```

错误码

查看本产品错误码

5 非网站功能

5.1 DescribeDdosIpConfig

调用DescribeDdosIpConfig接口分页查询高防IP防护配置。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDdosIpConfig	要执行的操作。取值：DescribeDdosIpConfig。
Index	Integer	是	0	查询索引，从0开始。
PageSize	Integer	是	10	分页大小，最大值为10。
Ips.N	RepeatList	否	1.1.1.1	要查询的高防IP列表。若有多个IP，请依次传入Ips.1、Ips.2、Ips.3… 说明: 若不传入该参数，则返回所有实例的配置。

返回参数

名称	类型	示例值	描述
DataList			高防IP防护信息列表。
└Bandwidth	Integer	10000	基础带宽值。
└CleanStatus	Integer	0	高防实例IP的清洗状态，取值： · 0：正常 · 1：清洗中 · 2：黑洞中 · 3：延迟黑洞中

名称	类型	示例值	描述
└ ConfigDomainCount	Integer	0	已使用网站防护数。
└ConfigPortCount	Integer	0	已使用非网站防护数。
└ElasticBandwidth	Integer	10000	弹性带宽值。
└Ip	String	118.178.214.208	高防实例IP。
└LbId	String	133bd628-aa9f-11e8-bae4-2c9d1e2c4716-cn-hangzhou-dg-a01	高防IP策略修改标识，用于下发健康检查、会话保持、DDoS防护策略。
└Line	String	bgp	高防Ip线路，取值： · MT：移动 · CT：电信 · CUT：联通 · BGP：BGP
└Status	Integer	1	高防实例IP的当前状态，取值： · 0：创建中 · 1：正常 · 2：已过期
└TotalDefenseCount	Integer	0	历史防护攻击事件总数。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
Total	Integer	1	结果总数。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DescribeDdosIpConfig
&Ips.1=1.1.1.1
&Index=0
&PageSize=10
```

&公共请求参数

正常返回示例

XML 格式

```
<DescribeDdosIpConfigResponse>
  <DataList>
    <element>
      <Bandwidth>10000</Bandwidth>
      <CleanStatus>0</CleanStatus>
      <ConfigDomainCount>0</ConfigDomainCount>
      <ConfigPortCount>0</ConfigPortCount>
      <ElasticBandwidth>10000</ElasticBandwidth>
      <Ip>118.178.214.208</Ip>
      <LbId>133bd628-aa9f-11e8-bae4-2c9d1e2c4716-cn-hangzhou-dg-a01</
LbId>
      <Line>BGP</Line>
      <Status>1</Status>
      <TotalDefenseCount>0</TotalDefenseCount>
    </element>
  </DataList>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <Total>1</Total>
</DescribeDdosIpConfigResponse>
```

JSON 格式

```
{
 "RequestId":"C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
 "DataList":[
  {
   "Ip":"118.178.214.208",
   "Status":1,
   "TotalDefenseCount":0,
   "ConfigDomainCount":0,
   "CleanStatus":0,
   "ConfigPortCount":0,
   "ElasticBandwidth":10000,
   "LbId":"133bd628-aa9f-11e8-bae4-2c9d1e2c4716-cn-hangzhou-dg-a01",
   "Line":"BGP",
   "Bandwidth":10000
  }
 ],
 "Total":1
}
```

错误码

查看本产品错误码

5.2 DescribePortRulePage

调用DescribePortRulePage接口分页查询非网站转发规则。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribePortRulePage	要执行的操作。取值：DescribePortRulePage。
CurrentPage	Integer	否	1	分页页号，最小值为1。
Ip	String	否	1.1.1.1	要查询的高防实例IP。
PageSize	Integer	否	10	分页大小，最大值为10。

返回参数

名称	类型	示例值	描述
Count	Integer	3	转发规则总数。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
RuleList			转发规则列表。
└BackPort	Integer	233	源站端口。
└BackProtocol	String	tcp	源站端口转发协议。
└FrontPort	Integer	233	转发端口。
└FrontProtocol	String	tcp	转发端口转发协议。
└Ip	String	2.2.2.2	高防实例IP。
└LbId	String	xxxxxxx-xxxx-xxxx-xxxxxxxx	高防IP策略修改标识，用于下发健康检查、会话保持、DDoS防护策略。
└LvsType	String	poll	LVS转发规则，取值：poll（轮询模式）。
└RealServer	String	1.1.1.1	源站IP列表。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DescribePortRulePage
&Ip=1.1.1.1
&CurrentPage=1
&PageSize=10
&FrontPort=233
&公共请求参数
```

正常返回示例

XML 格式

```
<DescribePortRulePageResponse>
  <Count>3</Count>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <RuleList>
    <element>
      <BackPort>233</BackPort>
      <BackProtocol>tcp</BackProtocol>
      <FrontPort>233</FrontPort>
      <FrontProtocol>tcp</FrontProtocol>
      <Ip>2.2.2.2</Ip>
      <LbId>xxxxxxx-xxxx-xxxx-xxxxxxxx</LbId>
      <LvsType>poll</LvsType>
      <RealServer>1.1.1.1</RealServer>
    </element>
  </RuleList>
</DescribePortRulePageResponse>
```

JSON 格式

```
{
 "RuleList":[
  {
   "Ip":"2.2.2.2",
   "FrontPort":233,
   "RealServer":"1.1.1.1",
   "BackPort":233,
   "BackProtocol":"tcp",
   "LvsType":"poll",
   "LbId":"xxxxxxx-xxxx-xxxx-xxxxxxxx",
   "FrontProtocol":"tcp"
  }
 ],
 "Count":3,
 "RequestId":"C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

查看本产品错误码

5.3 CreatePortRule

调用CreatePortRule接口创建非网站转发规则。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreatePortRule	要执行的操作。取值：CreatePortRule。
BackPort	Integer	否	255	设置源站端口。
FrontPort	Integer	否	255	设置转发端口。
Ip	String	否	1.1.1.1	要操作的高防实例IP。
ProxyType	String	否	tcp	设置转发协议，取值： · tcp · udp
RealServerList	String	否	2.2.2.2,3.3.3.3	添加源站列表，以逗号分隔。

返回参数

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

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=CreatePortRule
&Ip=1.1.1.1
&FrontPort=255
&BackPort=255
&Protocol=tcp
&RealServerList=2.2.2.2,3.3.3.3
```

```
&公共请求参数
```

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

查看本产品错误码

5.4 UpdatePortRule

调用UpdatePortRule接口更新非网站转发规则。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	UpdatePortRule	要执行的操作。取值：UpdatePortRule。
FrontPort	Integer	是	255	设置转发端口。
Ip	String	是	1.1.1.1	要操作的高防实例IP。
RealServerList	String	是	2.2.2.2,3.3.3.3	添加源站列表，以逗号分隔。

返回参数

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

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=UpdatePortRule
&Ip=1.1.1.1
&FrontPort=255
&RealServerList=2.2.2.2,3.3.3.3
&公共请求参数
```

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

查看本产品错误码

5.5 DeletePortRule

调用DeletePortRule接口删除非网站转发规则。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeletePortRule	要执行的操作。取值：DeletePortRule。
FrontPort	Integer	是	255	要操作的转发端口。
Ip	String	是	1.1.1.1	要操作的高防实例IP。

返回参数

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

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DeletePortRule
&Ip=1.1.1.1
&FrontPort=255
&公共请求参数
```

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

查看本产品错误码

5.6 DescribeHealthCheckConfig

调用DescribeHealthCheckConfig接口查询非网站转发健康检查类配置。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeHealthCheckConfig	要执行的操作。取值：DescribeHealthCheckConfig。
Ip	String	是	1.1.1.1	要查询的高防IP。

返回参数

名称	类型	示例值	描述
Listeners			健康检查监听配置。
└BackPort	Integer	8080	源站端口。
└Check			健康检查配置信息。
└Domain	String	www.aliyun.com	（仅HTTP协议）域名。
└Down	Integer	7	不健康阈值。
└Interval	Integer	6	检查间隔。
└Port	Integer	8080	检查端口。
└Timeout	Integer	5	响应超时时间。
└Type	String	tcp	协议类型。
└Up	Integer	8	健康阈值。
└Uri	String	/login	（仅HTTP协议）检查路径。
└Config			DDoS防护策略。
└NoDataConn	String	off	虚假源开关。
└PayloadLength			包长度过滤，Min为最小值，Max为最大值。
└Max	Integer	6000	包长度最大值。

名称	类型	示例值	描述
└Min	Integer	0	包长度最小值。
└PersistenceTimeout	Integer	900	会话保持检查时间，单位为秒。
└Sla			目的新建、并发链接配置。
└Cps	Integer	125	源新建连接限速。
└CpsEnable	Integer	1	源新建连接限速开关，取值： · 0：关闭 · 1：打开
└MaxConn	Integer	1226	源并发连接限速。
└MaxConnEnable	Integer	1	源并发连接限速开关，取值： · 0：关闭 · 1：打开
└Slimit			源新建、并发链接配置。
└Cps	Integer	123	源新建连接限速。
└CpsEnable	Integer	1	源新建连接限速开关，取值： · 0：关闭 · 1：打开
└MaxConn	Integer	124	源并发连接限速。
└MaxConnEnable	Integer	1	源并发连接限速开关，取值： · 0：关闭 · 1：打开
└SynProxy	String	on	空连接开关。
└FrontendPort	Integer	8080	转发端口。
└Protocol	String	tcp	协议。
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DescribeHealthCheckC
onfig
&Ip=1.1.1.1
&公共请求参数
```

正常返回示例

`XML` **格式**

```
<DescribeHealthCheckConfigResponse>
  <Listeners>
    <element>
      <BackPort>8080</BackPort>
      <Check>
        <Down>7</Down>
        <Interval>6</Interval>
        <Port>8080</Port>
        <Timeout>5</Timeout>
        <Type>tcp</Type>
        <Up>8</Up>
      </Check>
      <Config>
        <NoDataConn>off</NoDataConn>
        <PayloadLength>
          <Max>6000</Max>
          <Min>0</Min>
        </PayloadLength>
        <PersistenceTimeout>900</PersistenceTimeout>
        <Sla>
          <Cps>125</Cps>
          <CpsEnable>1</CpsEnable>
          <MaxConn>1226</MaxConn>
          <MaxConnEnable>1</MaxConnEnable>
        </Sla>
        <Slimit>
          <Cps>123</Cps>
          <CpsEnable>1</CpsEnable>
          <MaxConn>124</MaxConn>
          <MaxConnEnable>1</MaxConnEnable>
        </Slimit>
        <SynProxy>on</SynProxy>
      </Config>
      <FrontendPort>8080</FrontendPort>
      <Protocol>tcp</Protocol>
    </element>
  </Listeners>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</DescribeHealthCheckConfigResponse>
```

`JSON` **格式**

```
{
 "Listeners":[
  {
   "Check":{
    "Down":7,
    "Port":8080,
    "Timeout":5,
    "Interval":6,
    "Up":8,
    "Type":"tcp"
```

```
    },
    "Config":{
     "PayloadLength":{
      "Max":6000,
      "Min":0
     },
     "SynProxy":"on",
     "Sla":{
      "MaxConnEnable":1,
      "MaxConn":1226,
      "Cps":125,
      "CpsEnable":1
     },
     "NoDataConn":"off",
     "Slimit":{
      "MaxConnEnable":1,
      "MaxConn":124,
      "Cps":123,
      "CpsEnable":1
     },
     "PersistenceTimeout":900
    },
    "FrontendPort":8080,
    "BackPort":8080,
    "Protocol":"tcp"
   }
  ],
  "RequestId":"C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```


错误码

查看本产品错误码

5.7 ModifyPersistenceTimeOut

调用ModifyPersistenceTimeOut接口配置会话保持时间。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

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

名称	类型	是否必选	示例值	描述
ConfigJson	String	是	{"persistence_timeout":400}	会话保持时间配置内容（JSON字符串格式），具体结构描述如下： · persistence_timeout，Integer类型，必选，设置会话保持时间，单位为秒，取值范围：30-3,600。 说明: 此处的参数名以小写开头。
FrontPort	Integer	是	255	转发端口。
Ip	String	是	1.1.1.1	要操作的高防实例IP。
LbId	String	否	xxxxxxx-xxxx-xxxx-xxxxxxxx	高防IP策略修改标识。

返回参数

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

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=ModifyPersistenceTimeOut
&Ip=1.1.1.1
&FrontPort=255
&ConfigJson={"persistence_timeout":400}
&LbId=xxxxxxx-xxxx-xxxx-xxxxxxxx
&公共请求参数
```

正常返回示例

XML 格式

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

```
</ModifyPersistenceTimeOutResponse>
```

JSON 格式

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

错误码

查看本产品错误码

5.8 ModifyHealthCheckConfig

调用ModifyHealthCheckConfig接口修改健康检查配置。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

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。

名称	类型	是否必选	示例值	描述
ConfigJson	String	是	{"check":{"interval":5,"port":255,"timeout":5,"type":"http","up":3,"down":3,"domain":"www.aliyun.com","uri":"/a/a/a"}}	健康检查配置内容（JSON字符串格式），具体结构描述如下： · check，Object类型，必选，健康检查内容配置，具体结构描述如下： 说明： 该参数名以小写开头。 - interval，Integer类型，必选，检查间隔。 - port，Integer类型，可选，检测端口。 说明： 协议为tcp或udp时必填。 - timeout，Integer类型，必选，响应超时时间。 - type，String类型，必选，协议类型，取值： ■ tcp ■ udp ■ http - up，Integer类型，必选，健康阈值。 - down，Integer类型，必选，不健康阈值。 - domain，String类型，可选，域名。 说明： 协议为http时可填，非必需。 - uri，String类型，可选，检查路径。 说明： 协议为http时必填。
FrontPort	Integer	是	255	转发端口。
Ip	String	是	1.1.1.1	要操作的高防实例IP。

名称	类型	是否必选	示例值	描述
LbId	String	否	xxxxxxx-xxxx-xxxx-xxxxxxxx	高防IP策略修改标识。

返回参数

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

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=ModifyHealthCheckConfig
&Ip=1.1.1.1
&FrontPort=255
&LbId=xxxxxxx-xxxx-xxxx-xxxxxxxx
&ConfigJson={"check":{"interval":5,"port":255,"timeout":5,"type":"http","up":3,"down":3,"domain":"www.aliyun.com","uri":"/a/a/a"}}
&公共请求参数
```

正常返回示例

`XML` **格式**

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

`JSON` **格式**

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

错误码

查看本产品错误码

5.9 ModifyDDoSProtectConfig

调用ModifyDDoSProtectConfig接口修改DDoS防护配置。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

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

名称	类型	是否必选	示例值	描述
ConfigJson	String	是	{"payload_len":{"min":0,"max":6000},"synproxy":"on","slimit":{"pps":0,"maxconn_enable":1,"bps":0,"maxconn":124,"cps":123,"cps_enable":1},"sla":{"pps":0,"maxconn_enable":1,"outbps":536870912,"cps":125,"maxconn":1226,"inbps":0,"cps_enable":1},"nodata_conn":"off"}	DDoS防护配置内容（JSON字符串格式），具体结构描述如下： · check，Object类型，必选，DDoS防护策略配置，具体结构描述如下： 说明: 该参数名以小写开头。 - PayloadLength，Object类型，包长度过滤，具体结构描述如下： ■ Min，Integer类型，必选，包长度最小值。 ■ Max，Integer类型，必选，包长度最大值。 - PersistenceTimeout，Integer类型，必选，会话保持检查时间，单位为秒。 - NoDataConn，String类型，必选，虚假源开关。 - SynProxy，String类型，必选，空连接开关。 - Sla，Object类型，必选，目的新建、并发链接配置，具体结构描述如下： ■ MaxConnEnable，Integer类型，必选，目的并发连接限速开关，取值： ■ 0：关闭 ■ 1：打开 ■ MaxConn，Integer类型，必选，目的并发连接限速。 ■ CpsEnable，Integer类型，必选，目的新建连接限速开关，取值： ■ 0：关闭 ■ 1：打开 ■ Cps，Integer类型，必选，目的新建连接限速。 - Slimit，Object类型，必选，源新建、并发链接配

名称	类型	是否必选	示例值	描述
FrontPort	Integer	是	255	转发端口。
Ip	String	是	1.1.1.1	要操作的高防实例IP。
LbId	String	否	xxxxxxx-xxxx-xxxx-xxxxxxxx	高防IP策略修改标识。

返回参数

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

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=ModifyHealthCheckCon
fig
&Ip=1.1.1.1
&FrontPort=255
&LbId=xxxxxxx-xxxx-xxxx-xxxxxxxx
&ConfigJson={"payload_len":{"min":0,"max":6000},"synproxy":"on","
slimit":{"pps":0,"maxconn_enable":1,"bps":0,"maxconn":124,"cps":123,"
cps_enable":1},"sla":{"pps":0,"maxconn_enable":1,"outbps":536870912,"
cps":125,"maxconn":1226,"inbps":0,"cps_enable":1},"nodata_conn":"off"}
&公共请求参数
```

正常返回示例

`XML` 格式

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

`JSON` 格式

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

错误码

查看本产品错误码

6 实例相关

6.1 DescribeInstancePage

调用DescribeInstancePage接口查询高防IP的实例信息。

调试

前往【*API Explorer*】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstancePage	要执行的操作。取值：DescribeInstancePage。
CurrentPage	Integer	否	1	分页页号，最小值为1。
InstanceId	String	否	ddosBag-cn-xxxxx	要查询的实例ID，优先级比InstanceIdList高。
InstanceIdList.N	RepeatList	否	ddosBag-cn-xxxxx	根据实例ID查询，传入要查询的高防实例ID。若有多个实例，依次传入InstanceIdList.1、InstanceIdList.2、InstanceIdList.3 ... 说明: 该参数不为空时，则优先根据传入的实例ID进行查询。
IpList.N	RepeatList	否	1.1.1.1	根据高防IP查询，传入要查询的高防IP。若有多个高防IP，依次传入IpList.1、IpList.2、IpList.3 ... 说明: 该参数优先级没有InstanceIdList高。若InstanceIdList为空，则根据传入的高防IP进行查询；否则，根据传入的InstanceIdList进行查询。

名称	类型	是否必选	示例值	描述
Line	String	否	CUT	要查询的线路，取值： · CUT：联通 · CT：电信
PageSize	Integer	否	10	分页大小，最大值为10。

返回参数

名称	类型	示例值	描述
InstanceList			实例信息列表。
└InstanceId	String	ddosBag-cn-xxxxx	高防实例ID。
└InstanceRemark	String	高防测试	高防实例备注。
└IpList			高防IP信息列表。
└BandWidth	Integer	10000	保底带宽值，单位为M。
└ElasticBandWidth	Integer	20000	弹性带宽值，单位为M。
└InstanceId	String	ddosBag-cn-xxxxx	高防IP地址，0表示未启用。
└Ip	String	1.1.1.1	高防实例的IP地址。
└Line	String	CUT	高防IP线路，取值： · CUT：联通 · CT：电信 · MT：移动 · BGP：BGP线路
└Status	Integer	1	高防实例状态，取值： · 0：创建中 · 1：正常 · 2：已过期
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。
Total	Integer	1	查询到的结果总数。

示例

请求示例

```
https://ddospro.cn-hangzhou.aliyuncs.com/?Action=DescribeInstancePage
&CurrentPage=1
&PageSize=10
&公共请求参数
```

正常返回示例

XML 格式

```
<DescribeInstancePageResponse>
  <InstanceList>
    <element>
      <InstanceId>ddosBag-cn-xxxxx</InstanceId>
      <InstanceRemark>高防测试</InstanceRemark>
      <IpList>
        <element>
          <BandWidth>10000</BandWidth>
          <ElasticBandWidth>20000</ElasticBandWidth>
          <InstanceId>ddosBag-cn-xxxxx</InstanceId>
          <Ip>1.1.1.1</Ip>
          <Line>CUT</Line>
          <Status>1</Status>
        </element>
      </IpList>
    </element>
  </InstanceList>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <Total>1</Total>
</DescribeInstancePageResponse>
```

JSON 格式

```
{
 "RequestId":"C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
 "InstanceList":[
  {
   "InstanceRemark":"高防测试",
   "InstanceId":"ddosBag-cn-xxxxx",
   "IpList":[
    {
     "Ip":"1.1.1.1",
     "Status":1,
     "BandWidth":10000,
     "ElasticBandWidth":20000,
     "InstanceId":"ddosBag-cn-xxxxx",
     "Line":"CUT"
    }
   ]
  }
 ],
 "Total":1
}
```

错误码

查看本产品错误码

7 API概览

本文档汇总了高防IP所有可调用的API，具体接口信息请参阅相关文档。

关于更多API资源，请访问*API Explorer*。

报表相关

API	描述
DescribeBizFlow	查询高防Ip上的业务流量信息，包括In方向和Out方向流量。
DescribeDdosAttackTypeChart	查询高防Ip的攻击类型概览图表。
DescribeDdosPeakFlow	查询高防Ip的攻击峰值。
DescribeDdosFlowProportionDiagram	查询高防Ip的攻击比例图表。
DescribeDdosAttackEvents	查询高防Ip的攻击事件。
DescribeDdosAttackEventSourceIps	查询高防Ip的攻击事件的源攻击IP列表。
DescribeCcEvents	查询用户域名的CC攻击事件。

网站功能

API	描述
DescribeBackSourceCidr	查询高防回源网段地址。
DescribeDomainConfigPage	分页查询用户的网站配置列表。
DescribeDomainSecurityConfig	查询用户域名的安全防护配置。
ListCcCustomedRule	查询用户的自定义CC规则。
CreateDomain	创建网站防护规则。
DeleteDomain	删除网站防护规则。
CreateTransmitLine	添加网站防护转发线路。
ModifyTransmitLine	修改网站防护转发线路。
DeleteTransmitLine	删除网站防护转发线路。
ModifyIpCnameStatus	修改网站防护中高防Ip Cname解析状态。
ModifyRealServers	修改网站防护配置中线路对应的源站。
ConfigSwitchPriority	修改网站防护中高防Ip的调度优先级。
ModifyDomainProxy	修改网站防护转发协议。

ModifyDomainBlackWhiteList	修改网站安全防护的黑白名单。
ModifyCcStatus	修改网站安全防护CC功能开关。
ModifyCcTemplate	修改网站安全防护CC防护模式。
ModifyCcCustomStatus	修改网站安全防护CC自定义规则开关。
CreateCcCustomedRule	创建网站安全防护CC自定义规则。
UpdateCcCustomedRule	修改网站安全防护CC自定义规则。
DeleteCcCustomedRule	删除网站安全防护CC自定义规则。

非网站功能

API	描述
DescribeDdosIpConfig	分页查询高防Ip防护配置。
DescribePortRulePage	分页查询非网站转发规则。
CreatePortRule	创建非网站转发规则。
UpdatePortRule	更新非网站转发规则。
DeletePortRule	删除非网站转发规则。
DescribeHealthCheckConfig	查询非网站转发健康检查类配置。
ModifyPersistenceTimeOut	配置会话保持时间。
ModifyHealthCheckConfig	修改健康检查配置。
ModifyDDoSProtectConfig	修改DDoS防护配置。

实例相关

API	描述
DescribeInstancePage	查询高防Ip的实例信息。