Anti-DDoS 流量清洗

API 参考

文档版本 02

发布日期 2024-06-30

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 使用前必读

1.1 概述

Anti-DDoS流量清洗服务（以下简称Anti-DDoS）为公网IP提供四到七层的DDoS攻击防护和攻击实时告警通知。同时，Anti-DDoS可以提升用户带宽利用率，确保用户业务稳定运行。

Anti-DDoS通过对互联网访问公网IP的业务流量进行实时监测，及时发现异常DDoS攻击流量。在不影响正常业务的前提下，根据用户配置的防护策略，清洗掉攻击流量。同时，Anti-DDoS为用户生成监控报表，清晰展示网络流量的安全状况。

您可以使用本文档提供API对Anti-DDoS进行相关操作，如查询、更新Anti-DDoS服务等。支持的全部操作请参见**API概览**。

在调用Anti-DDoS API之前，请确保已经充分了解Anti-DDoS相关概念，详细信息请参见《Anti-DDoS流量清洗用户指南》的“产品介绍”章节。

1.2 调用说明

Anti-DDoS提供了REST（Representational State Transfer）风格API，支持您通过HTTPS请求调用，调用方法请参见**如何调用API**。

1.3 终端节点

终端节点（Endpoint）即调用API的**请求地址**，不同服务不同区域的终端节点不同，您可以从**地区和终端节点**中查询所有服务的终端节点。

1.4 约束与限制

详细的约束限制请参见具体API的说明。

1.5 基本概念

- 区域（Region）

从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。

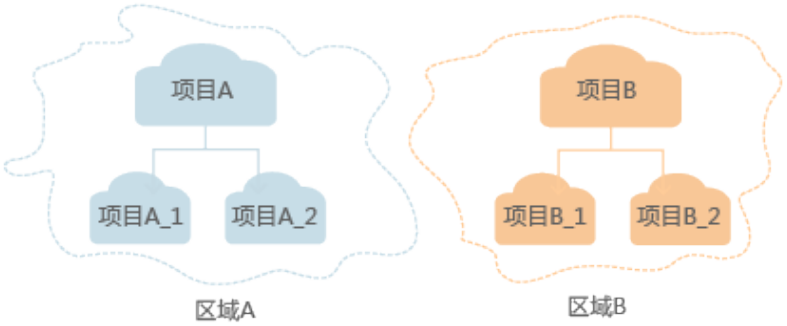
- 可用区（AZ，Availability Zone）

  一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

- 项目

  区域默认对应一个项目，这个项目由系统预置，用来隔离物理区域间的资源（计算资源、存储资源和网络资源），以默认项目为单位进行授权，用户可以访问您账号中该区域的所有资源。如果您希望进行更加精细的权限控制，可以在区域默认的项目中创建子项目，并在子项目中创建资源，然后以子项目为单位进行授权，使得用户仅能访问特定子项目中资源，使得资源的权限控制更加精确。

  图 1-1 项目隔离模型



- 企业项目

  企业项目是项目的升级版，针对企业不同项目间资源的分组和管理，是逻辑隔离。企业项目中可以包含多个区域的资源，且项目中的资源可以迁入迁出。

  关于企业项目ID的获取及企业项目特性的详细信息，请参见**企业项目管理**。

2 API 概览

通过使用Anti-DDoS提供的接口，您可以完整的使用Anti-DDoS的所有功能。

类型	说明
DDoS防护管理	开通和更新Anti-DDoS服务，查询Anti-DDoS服务、EIP防护状态、防护统计情况、防护流量、异常事件等接口。
DDoS任务管理	查询Anti-DDoS任务接口。
DDoS告警配置管理	查询和更新告警配置信息接口。

3 如何调用 API

3.1 构造请求

本节介绍REST API请求的组成，以调用**获取用户Token**接口说明如何调用API，该API获取用户的Token，Token是用户的访问令牌，承载身份与权限信息，Token可以用于调用其他API时鉴权。

请求 URI

请求URI由如下部分组成。

{URI-scheme} :// {Endpoint} / {resource-path} ? {query-string}

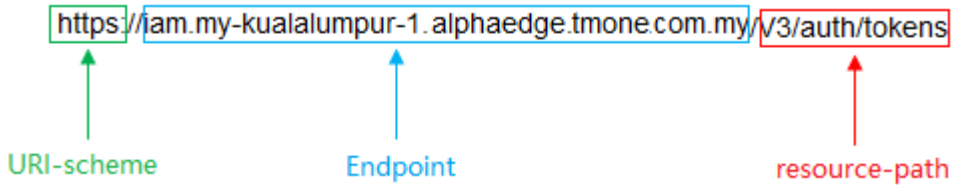
尽管请求URI包含在请求消息头中，但大多数语言或框架都要求您从请求消息中单独传递它，所以在此单独强调。

- **URI-scheme**：
  表示用于传输请求的协议，当前所有API均采用**HTTPS**协议。
- **Endpoint**：
  指定承载REST服务端点的服务器域名或IP，不同服务不同区域的Endpoint不同，您可以从**地区和终端节点**获取。
  例如IAM服务在“**my-kualalumpur-1**”区域的Endpoint为“**iam.my-kualalumpur-1.alphaedge.tmone.com.my**”。
- **resource-path**：
  资源路径，也即API访问路径。从具体API的URI模块获取，例如“获取用户Token”API的resource-path为“/v3/auth/tokens”。
- **query-string**：
  查询参数，是可选部分，并不是每个API都有查询参数。查询参数前面需要带一个“？”，形式为“参数名=参数取值”，例如“limit=10”，表示查询不超过10条数据。

例如您需要获取IAM在“my-kualalumpur-1”区域的Token，则需使用“my-kualalumpur-1”区域的Endpoint（iam.my-kualalumpur-1.alphaedge.tmone.com.my），并在**地区和终端节点**的URI部分找到resource-path（/v3/auth/tokens），拼接起来如下所示。

```
https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens
```

图 3-1 URI 示意图



说明

为查看方便，在每个具体API的URI部分，只给出resource-path部分，并将请求方法写在一起。这是因为URI-scheme都是HTTPS，同一个服务的Endpoint在同一个区域也相同，所以简洁起见将这两部分省略。

请求方法

HTTP请求方法（也称为操作或动词），它告诉服务你正在请求什么类型的操作。

- **GET**：请求服务器返回指定资源。
- **PUT**：请求服务器更新指定资源。
- **POST**：请求服务器新增资源或执行特殊操作。
- **DELETE**：请求服务器删除指定资源，如删除对象等。
- **HEAD**：请求服务器资源头部。
- **PATCH**：请求服务器更新资源的部分内容。当资源不存在的时候，PATCH可能会去创建一个新的资源。

在**获取用户Token**的URI部分，您可以看到其请求方法为“POST”，则其请求为：

```
POST https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens
```

请求消息头

附加请求头字段，如指定的URI和HTTP方法所要求的字段。例如定义消息体类型的请求头“Content-Type”，请求鉴权信息等。

如下公共消息头需要添加到请求中。

- **Content-Type**：消息体的类型（格式），必选，默认取值为“application/json”，有其他取值时会在具体接口中专门说明。
- **X-Auth-Token**：用户Token，可选，当使用Token方式认证时，必须填充该字段。用户Token也就是调用**获取用户Token**接口的响应值，该接口是唯一不需要认证的接口。

  说明

  API同时支持使用AK/SK认证，AK/SK认证是使用SDK对请求进行签名，签名过程会自动往请求中添加Authorization（签名认证信息）和X-Sdk-Date（请求发送的时间）请求头。

  AK/SK认证的详细说明请参见**AK/SK认证**。

对于**获取用户Token**接口，由于不需要认证，所以只添加“Content-Type”即可，添加消息头后的请求如下所示。

```
POST https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens
Content-Type: application/json
```

请求消息体

请求消息体通常以结构化格式发出，与请求消息头中Content-type对应，传递除请求消息头之外的内容。若请求消息体中参数支持中文，则中文字符必须为UTF-8编码。

每个接口的请求消息体内容不同，也并不是每个接口都需要有请求消息体（或者说消息体为空），GET、DELETE操作类型的接口就不需要消息体，消息体具体内容需要根据具体接口而定。

对于**获取用户Token**接口，您可以从接口的请求部分看到所需的请求参数及参数说明。将消息体加入后的请求如下所示，加粗的斜体字段需要根据实际值填写，其中***username***为用户名，***domainname***为用户所属的账号名称，*********为用户登录密码，***xxxxxxxxxxxxxxxxxx***为project的名称，您可以从获取。

说明

scope参数定义了Token的作用域，下面示例中获取的Token仅能访问project下的资源。您还可以设置Token作用域为某个账号下所有资源或账号的某个project下的资源，详细定义请参见**获取用户Token**。

```
POST https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens
Content-Type: application/json
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "********",
                    "domain": {
                        "name": "domainname"
                    }
                }
            }
        },
        "scope": {
            "project": {
                "name": "xxxxxxxxxxxxxxxxxx"
            }
        }
    }
}
```

到这里为止这个请求需要的内容就具备齐全了，您可以使用**curl**、**Postman**或直接编写代码等方式发送请求调用API。对于获取用户Token接口，返回的响应消息头中“x-subject-token”就是需要获取的用户Token。有了Token之后，您就可以使用Token认证调用其他API。

3.2 认证鉴权

调用接口有如下两种认证方式，您可以选择其中一种进行认证鉴权。

- Token认证：通过Token认证调用请求。
- AK/SK认证：通过AK（Access Key ID）/SK（Secret Access Key）加密调用请求。推荐使用AK/SK认证，其安全性比Token认证要高。

Token 认证

> **说明**
>
> Token的有效期为24小时，需要使用一个Token鉴权时，可以先缓存起来，避免频繁调用。

Token在计算机系统中代表令牌（临时）的意思，拥有Token就代表拥有某种权限。Token认证就是在调用API的时候将Token加到请求消息头，从而通过身份认证，获得操作API的权限。

Token可通过调用**获取用户Token**接口获取，调用本服务API需要project级别的Token，即调用**获取用户Token**接口时，请求body中auth.scope的取值需要选择project，如下所示。

```
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "********",
                    "domain": {
                        "name": "domainname"
                    }
                }
            }
        },
        "scope": {
            "project": {
                "name": "xxxxxxxx"
            }
        }
    }
}
```

获取Token后，再调用其他接口时，您需要在请求消息头中添加“X-Auth-Token”，其值即为Token。例如Token值为“ABCDEFJ....”，则调用接口时将“X-Auth-Token: ABCDEFJ....”加到请求消息头即可，如下所示。

```
POST https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

AK/SK 认证

> **说明**
>
> AK/SK签名认证方式仅支持消息体大小12MB以内，12MB以上的请求请使用Token认证。

AK/SK认证就是使用AK/SK对请求进行签名，在请求时将签名信息添加到消息头，从而通过身份认证。

- AK(Access Key ID)：访问密钥ID。与私有访问密钥关联的唯一标识符；访问密钥ID和私有访问密钥一起使用，对请求进行加密签名。
- SK(Secret Access Key)：与访问密钥ID结合使用的密钥，对请求进行加密签名，可标识发送方，并防止请求被修改。

使用AK/SK认证时，您可以基于签名算法使用AK/SK对请求进行签名，也可以使用专门的签名SDK对请求进行签名。详细的签名方法和SDK使用方法请参见**API签名指南**。

须知

签名SDK只提供签名功能，与服务提供的SDK不同，使用时请注意。

3.3 返回结果

状态码

请求发送以后，您会收到响应，包含状态码、响应消息头和消息体。

状态码是一组从1xx到5xx的数字代码，状态码表示了请求响应的状态，完整的状态码列表请参见**状态码**。

对于**获取用户Token**接口，如果调用后返回状态码为“201”，则表示请求成功。

响应消息头

对应请求消息头，响应同样也有消息头，如“Content-type”。

对于**获取用户Token**接口，返回如**图3-2**所示的消息头，其中“x-subject-token”就是需要获取的用户Token。有了Token之后，您就可以使用Token认证调用其他API。

图 3-2 获取用户 Token 响应消息头

响应消息体（可选）

响应消息体通常以结构化格式返回，与响应消息头中Content-type对应，传递除响应消息头之外的内容。

对于**获取用户Token**接口，返回如下消息体。为篇幅起见，这里只展示部分内容。

```
{
    "token": {
        "expires_at": "2019-02-13T06:52:13.855000Z",
```

```
        "methods": [
            "password"
        ],
        "catalog": [
            {
                "endpoints": [
                    {
                        "region_id": "xxxxxxxx",
.....
```

当接口调用出错时，会返回错误码及错误信息说明，错误响应的Body体格式如下所示。

```
{
    "error_msg": "The format of message is error",
    "error_code": "AS.0001"
}
```

其中，error_code表示错误码，error_msg表示错误描述信息。

4 API

4.1 DDoS 防护管理

4.1.1 查询 EIP 防护状态列表

功能介绍

查询用户所有EIP的Anti-DDoS防护状态信息，用户的EIP无论是否绑定到云服务器，都可以进行查询。

URI

- URI格式

  GET /v1/{project_id}/antiddos

  说明

  可以在URI后面用“?”和“&”添加不同的查询条件组合，请参考请求样例。

- 参数说明

参数	是否必选	类型	说明
project_id	是	String	项目ID。

请求消息

表 4-1 请求参数

参数	是否必选	类型	说明
status	否	String	可选范围： ● normal：表示正常。 ● configging：表示设置中。 ● notConfig：表示未设置。 ● packetcleaning：表示清洗。 ● packetdropping：表示黑洞。 不带此参数默认所有列表，以neutron查询到的顺序为准。
limit	否	Integer	返回结果个数限制，取值范围：1~100。
offset	否	Integer	偏移量，取值范围：0~2147483647。
ip	否	String	IP地址，支持IPv4格式和IPv6格式输入，支持部分查询。例如“?ip=192.168”，会返回192.168.111.1和10.192.168.8所对应的EIP防护状态。

响应消息

- 要素说明

名称	类型	说明
total	Integer	弹性IP总数。
ddosStatus	列表数据结构	防护状态列表。

- ddosStatus字段数据结构说明

参数	类型	说明
floating_ip_address	String	浮动IP地址。
floating_ip_id	String	EIP的ID。
network_type	String	EIP所属类型，可选范围： ● EIP：未绑定到ECS的EIP或绑定到ECS的EIP。 ● ELB：绑定到ELB的EIP。

参数	类型	说明
status	String	防护状态，可选范围： • normal：表示正常。 • configging：表示设置中。 • notConfig：表示未设置。 • packetcleaning：表示清洗。 • packetdropping：表示黑洞。
blackhole_endtime	Integer	黑洞结束时间。
protect_type	String	防护类型。
traffic_threshold	Integer	流量阈值。
http_threshold	Integer	http流量阈值。

示例

- 请求示例
```
GET /v1/67641fe6886f43fcb78edbbf0ad0b99f/antiddos?status=packetdropping
```
- 响应示例
```
{
   "total": 1,
   "ddosStatus": [
      {
         "floating_ip_id": "18e6ace5-eb36-4196-a15e-1e000c24e026",
         "floating_ip_address": "139.9.116.167",
         "network_type": "EIP",
         "status": "normal",
         "blackhole_endtime": 0,
         "protect_type": "default",
         "traffic_threshold": 99,
         "http_threshold": 0
      }
   ]
}
```

返回值

请参考**状态码**。

4.1.2 查询 Anti-DDoS 配置可选范围

功能介绍

查询系统支持的Anti-DDoS防护策略配置的可选范围，用户根据范围列表选择适合自己业务的防护策略进行Anti-DDoS流量清洗。

URI

- URI格式
  GET /v1/{project_id}/antiddos/query_config_list
- 参数说明

参数	是否必选	类型	说明
project_id	是	String	项目ID。

请求消息

请求参数

无

响应消息

- 要素说明

参数	类型	说明
traffic_limited_list	列表数据结构	流量限制列表。
http_limited_list	列表数据结构	HTTP限制列表。
connection_limited_list	列表数据结构	连接数限制列表。

- traffic_limited_list字段数据结构说明

参数	类型	说明
traffic_pos_id	Integer	流量分段ID。
traffic_per_second	Integer	每秒流量（Mbit/s）阈值。
packet_per_second	Integer	每秒报文数（个/s）阈值。

- http_limited_list字段数据结构说明

参数	类型	说明
http_request_pos_id	Integer	HTTP请求数分段ID。
http_packet_per_second	Integer	每秒HTTP请求数（个/s）阈值。

- connection_limited_list字段数据结构说明

参数	类型	说明
cleaning_access_pos_id	Integer	清洗时访问限制分段ID。
new_connection_limited	Integer	单一源IP新建连接个数。

参数	类型	说明
total_connection_limited	Integer	单一源IP连接数总个数。

示例

- 请求示例

```
GET /v1/67641fe6886f43fcb78edbbf0ad0b99f/antiddos/query_config_list
```

- 响应样例

```
{
    "traffic_limited_list": [
        {
            "traffic_pos_id": 1,
            "traffic_per_second": 10,
            "packet_per_second": 2000
        },
        {
            "traffic_pos_id": 2,
            "traffic_per_second": 30,
            "packet_per_second": 6000
        },
    ],
    "http_limited_list": [
        {
            "http_request_pos_id": 1,
            "http_packet_per_second": 100
        },
        {
            "http_request_pos_id": 2,
            "http_packet_per_second": 150
        },
    ],
    "connection_limited_list": [
        {
            "cleaning_access_pos_id": 1,
            "new_connection_limited": 10,
            "total_connection_limited": 30
        },
        {
            "cleaning_access_pos_id": 2,
            "new_connection_limited": 20,
            "total_connection_limited": 100
        },
    ],
    "extend_ddos_config": []
}
```

说明

“extend_ddos_config”字段显示用户根据实际需求设置的Anti-DDoS防护策略信息。

返回值

请参考**状态码**。

4.1.3 查询周防护统计情况

功能介绍

查询用户所有Anti-DDoS防护周统计情况，包括一周内DDoS拦截次数和攻击次数、以及按照被攻击次数进行的排名信息等统计数据。系统支持当前时间之前四周的周统计数据查询，超过这个时间的请求是查询不到统计数据的。

URI

- URI格式

  GET /v1/{project_id}/antiddos/weekly

  说明

  可以在URI后面用“?”和“&”添加不同的查询条件组合，请参考请求样例。

- 参数说明

参数	是否必选	类型	说明
project_id	是	String	项目ID。

请求消息

表 4-2 请求参数

参数	是否必选	类型	说明
period_start_date	否	String	每周的起始时间。

响应消息

- 要素说明

名称	类型	说明
ddos_intercept_times	Integer	一周内DDoS拦截次数。
weekdata	数据结构	一周的攻击次数统计数据。
top10	数据结构	被攻击次数排名前10的IP地址。

- weekdata字段数据结构说明

参数	类型	说明
ddos_intercept_times	Integer	DDoS拦截次数。
ddos_blackhole_times	Integer	DDoS黑洞次数。

参数	类型	说明
max_attack_bps	Integer	最大攻击流量。
max_attack_conns	Integer	最大攻击连接数。
period_start_date	Long integer	开始时间。

- top10字段数据结构说明

参数	类型	说明
floating_ip_address	String	弹性IP地址。
times	Integer	DDoS拦截次数，包括清洗和黑洞。

示例

- 请求示例

```
GET /v1/67641fe6886f43fcb78edbbf0ad0b99f/antiddos/weekly?
period_start_date=1006510306
```

- 响应示例

```
{
  "ddos_intercept_times": 23,
  "weekdata": [
    {
      "ddos_intercept_times": 0,
      "ddos_blackhole_times": 0,
      "max_attack_bps": 0,
      "max_attack_conns": 0,
      "period_start_date": 1474214461651
    },
    {
      "ddos_intercept_times": 0,
      "ddos_blackhole_times": 0,
      "max_attack_bps": 0,
      "max_attack_conns": 0,
      "period_start_date": 1474300861651
    },
    {
      "ddos_intercept_times": 0,
      "ddos_blackhole_times": 0,
      "max_attack_bps": 0,
      "max_attack_conns": 0,
      "period_start_date": 1474387261651
    },
    {
      "ddos_intercept_times": 0,
      "ddos_blackhole_times": 0,
      "max_attack_bps": 0,
      "max_attack_conns": 0,
      "period_start_date": 1474473661651
    },
    {
      "ddos_intercept_times": 0,
      "ddos_blackhole_times": 0,
      "max_attack_bps": 0,
      "max_attack_conns": 0,
      "period_start_date": 1474560061651
    },
    {
```

```
        "ddos_intercept_times": 2,
        "ddos_blackhole_times": 0,
        "max_attack_bps": 16375,
        "max_attack_conns": 0,
        "period_start_date": 1474646461651
      },
      {
        "ddos_intercept_times": 1,
        "ddos_blackhole_times": 0,
        "max_attack_bps": 0,
        "max_attack_conns": 0,
        "period_start_date": 1474732861651
      }
    ],
    "top10": [
      {
        "floating_ip_address": "192.168.44.69",
        "times": 23
      }
    ]
}
```


返回值

请参考**状态码**。

4.1.4 查询 Anti-DDoS 服务

功能介绍

查询配置的Anti-DDoS防护策略，用户可以查询指定EIP的Anti-DDoS防护策略。

URI

- URI格式

  GET /v1/{project_id}/antiddos/{floating_ip_id}

- 参数说明

参数	是否必选	类型	说明
project_id	是	String	项目ID。
floating_ip_id	是	String	用户EIP对应的ID。

请求消息

表 4-3 请求参数

参数	是否必选	类型	说明
ip	否	String	用户EIP。

响应消息

表 4-4 响应参数

参数	类型	说明
enable_L7	Boolean	是否开启L7层防护。 ● true：开启L7层防护。 ● false：不开启L7层防护。
traffic_pos_id	Integer	流量分段ID，取值范围1～9或取值99。
http_request_pos_id	Integer	HTTP请求数分段ID，取值范围：1～15。
cleaning_access_pos_id	Integer	清洗时访问限制分段ID，取值范围：1～8或取值99。
app_type_id	Integer	应用类型ID，可选取值： ● 0 ● 1

示例

- 请求示例

```
GET /v1/67641fe6886f43fcb78edbbf0ad0b99f/antiddos/1df977c2-fdc6-4483-bc1c-ba46829f57b8
```

- 响应示例

```
{
  "enable_L7": true,
  "traffic_pos_id": 1,
  "http_request_pos_id": 1,
  "cleaning_access_pos_id": 1,
  "app_type_id": 1
}
```

返回值

请参考**状态码**。

4.1.5 开通 Anti-DDoS 服务

功能介绍

用户开通Anti-DDoS流量清洗防护。作为异步接口，调用成功，只是说明服务节点收到了开通请求，开通是否成功需要通过任务查询接口查询该任务的执行状态，具体请参考**查询Anti-DDoS任务**。

URI

- URI格式

  POST /v1/{project_id}/antiddos/{floating_ip_id}

- 参数说明

参数	是否必选	类型	说明
project_id	是	String	用户的ID
floating_ip_id	是	String	用户EIP对应的ID

请求消息

表 4-5 请求参数

参数	是否必选	类型	说明
enable_L7	否	Boolean	是否开启L7层防护
traffic_pos_id	是	Integer	流量分段ID，取值范围：1～9
http_request_pos_id	是	Integer	HTTP请求数分段ID，取值范围：1～15
cleaning_access_pos_id	是	Integer	清洗时访问限制分段ID，取值范围：1～8
app_type_id	否	Integer	应用类型ID，可选取值： ● 0 ● 1

响应消息

表 4-6 响应参数

名称	类型	说明
error_code	String	内部错误码
error_description	String	内部错误描述
task_id	String	任务ID，后续可根据该ID查询本任务状态。 本字段为后续的任务审计扩展，暂时不需要，先保留。

示例

- 请求示例

```
POST /v1/67641fe6886f43fcb78edbbf0ad0b99f/antiddos/1df977c2-fdc6-4483-bc1c-ba46829f57b8
{
   "enable_L7":true,
```

```
    "traffic_pos_id":1,
    "http_request_pos_id":1,
    "cleaning_access_pos_id":1,
    "app_type_id":1
}
```

- 响应示例

```
{
  "error_code": "10000000",
  "error_description": "Task has been received and is being processed.",
  "task_id": "94e17e18-5b2c-40c6-a218-8ec5134e32a5"
}
```

返回值

请参考**状态码**。

4.1.6 更新 Anti-DDoS 服务

功能介绍

更新指定EIP的Anti-DDoS防护策略配置。调用成功，只是说明服务节点收到了关闭更新配置请求，操作是否成功需要通过任务查询接口查询该任务的执行状态，具体请参考**查询Anti-DDoS任务**。

URI

- URI格式

  PUT /v1/{project_id}/antiddos/{floating_ip_id}

- 参数说明

参数	是否必选	类型	说明
project_id	是	String	项目ID。
floating_ip_id	是	String	用户EIP对应的ID。

请求参数

表 4-7 请求参数

参数	是否必选	类型	说明
enable_L7	否	Boolean	是否开启L7层防护。 • true：开启L7层防护。 • false：不开启L7层防护。
traffic_pos_id	是	Integer	流量分段ID，取值范围：1～9或取值99。
http_request_pos_id	是	Integer	HTTP请求数分段ID，取值范围：1～15。

参数	是否必选	类型	说明
cleaning_access_pos_id	是	Integer	清洗时访问限制分段ID，取值范围：1～8或取值99。
app_type_id	否	Integer	应用类型ID，可选取值： • 0 • 1

响应消息

表 4-8 响应参数

名称	类型	说明
error_code	String	内部错误码。
error_msg	String	内部错误描述。
task_id	String	任务ID，后续可根据该ID查询本任务状态。 本字段为后续的任务审计扩展，暂时不需要，先保留。

示例

- 请求示例

```
PUT /v1/67641fe6886f43fcb78edbbf0ad0b99f/antiddos/ee0c854e-082f-499e-b7d8-1b42c22781af
{
    "enable_L7":false,
    "traffic_pos_id":2,
    "http_request_pos_id":1,
    "cleaning_access_pos_id":1,
    "app_type_id":1
}
```

- 响应示例

```
{
  "error_code": "10000000",
  "error_msg": "The task has been received and is being handled",
  "task_id": "4a4fefe7-34a1-40e2-a87c-16932af3ac4a"
}
```

返回值

请参考**状态码**。

4.1.7 查询指定 EIP 防护流量

功能介绍

查询指定EIP在过去24小时之内的防护流量信息，流量的间隔时间单位为5分钟。

URI

- URI格式
  GET /v1/{project_id}/antiddos/{floating_ip_id}/daily
- 参数说明

参数	是否必选	类型	说明
project_id	是	String	项目ID。
floating_ip_id	是	String	用户EIP对应的ID。

请求消息

表 4-9 请求参数

参数	是否必选	类型	说明
ip	否	String	用户EIP。

响应

- 要素说明

名称	参数类型	说明
data	数据结构	24小时内的流量数据。

- data字段数据结构说明

参数	类型	说明
period_start	Long integer	开始时间
bps_in	Integer	入流量（bit/s）
bps_attack	Integer	攻击流量（bit/s）
total_bps	Integer	总流量
pps_in	Integer	入报文速率（个/s）
pps_attack	Integer	攻击文速率（个/s）
total_pps	Integer	总报文速率

示例

- 请求示例
  ```
  GET /v1/67641fe6886f43fcb78edbbf0ad0b99f/antiddos/1df977c2-fdc6-4483-bc1c-ba46829f57b8/daily
  ```

- 响应示例

```
{
   "data": [
      {
         "period_start": 1606188642720,
         "bps_in": 0,
         "bps_attack": 0,
         "total_bps": 0,
         "pps_in": 0,
         "pps_attack": 0,
         "total_pps": 0
      }
   ]
}
```

返回值

请参考**状态码**。

4.1.8 查询指定 EIP 异常事件

功能介绍

查询指定EIP在过去24小时之内的异常事件信息，异常事件包括清洗事件和黑洞事件，查询延迟在5分钟之内。

URI

- URI格式

  GET /v1/{project_id}/antiddos/{floating_ip_id}/logs

  说明

  可以在URI后面用“?”和“&”添加不同的查询条件组合，请参考请求样例。

- 参数说明

参数	是否必选	类型	说明
project_id	是	String	项目ID。
floating_ip_id	是	String	用户EIP对应的ID。

请求消息

表 4-10 请求参数

参数	是否必选	类型	说明
limit	否	Integer	返回结果个数限制，此次查询返回数量最大值，取值范围：1～100，与offset配合使用。 若“limit”与“offset”均不携带则返回所有主机列表。
offset	否	Integer	偏移量，“limit”携带时此字段有效。
sort_dir	否	String	可选范围： ● desc：表示时间降序。 ● asc：表示时间升序。 默认值为“desc”。
ip	否	String	用户EIP。

响应消息

- 要素说明

名称	参数类型	说明
total	Integer	弹性IP总数
logs	数据结构	异常事件列表

- logs字段数据结构说明

参数	类型	说明
start_time	Long integer	开始时间。
end_time	Long integer	结束时间。
status	Integer	防护状态，可选范围： ● 1：表示清洗。 ● 2：表示黑洞。
trigger_bps	Integer	触发时流量。
trigger_pps	Integer	触发时报文速率。
trigger_http_pps	Integer	触发时HTTP请求速率。

示例

- 请求示例

```
GET /v1/67641fe6886f43fcb78edbbf0ad0b99f/antiddos/1df977c2-fdc6-4483-bc1c-ba46829f57b8/logs
```

- 响应示例

```
{
  "total": 1,
  "logs": [
    {
      "start_time": 1473217200000,
      "end_time": 1473242400000,
      "status": 1,
      "trigger_bps": 51106,
      "trigger_pps": 2600,
      "trigger_http_pps": 3589
    }
  ]
}
```

返回值

请参考**状态码**。

4.1.9 查询指定 EIP 防护状态

功能介绍

查询指定EIP的Anti-DDoS防护状态。

URI

- URI格式

  GET /v1/{project_id}/antiddos/{floating_ip_id}/status

- 参数说明

参数	是否必选	类型	说明
project_id	是	String	项目ID。
floating_ip_id	是	String	用户EIP对应的ID。

请求消息

表 4-11 请求参数

参数	是否必选	类型	说明
ip	否	String	用户EIP。

响应消息

- 要素说明

参数	类型	说明
status	String	防护状态，可选范围： • normal：表示正常。 • configging：表示设置中。 • notConfig：表示未设置。 • packetcleaning：表示清洗。 • packetdropping：表示黑洞。

示例

- 请求示例

```
GET /v1/67641fe6886f43fcb78edbbf0ad0b99f/antiddos/1df977c2-fdc6-4483-bc1c-ba46829f57b8/status
```

- 响应示例

```
{
  "status": "normal"
}
```

返回值

请参考**状态码**。

4.2 DDoS 任务管理

4.2.1 查询 Anti-DDoS 任务

功能介绍

用户查询指定的Anti-DDoS防护配置任务，得到任务当前执行的状态。

URI

- URI格式

  GET /v1/{project_id}/query_task_status

  说明

  可以在URI后面用“?”和“&”添加不同的查询条件组合，请参考请求样例。

- 参数说明

参数	是否必选	类型	说明
project_id	是	String	项目ID。

请求消息

表 4-12 请求参数

参数	是否必选	类型	说明
task_id	是	String	任务ID（非负整数）的字符串。

响应消息

- 要素说明

名称	类型	说明
task_status	String	任务状态，有以下几种： ● success：运行成功。 ● failed：运行失败。 ● waiting：等待运行。 ● running：任务运行中。 ● preprocess：预处理中。 ● ready：任务准备中。
task_msg	String	任务的附加信息。

示例

- 请求示例

```
GET /v1/67641fe6886f43fcb78edbbf0ad0b99f/query_task_status?
task_id=4a4fefe7-34a1-40e2-a87c-16932af3ac4a
```

- 响应示例

```
{
  "task_status": "running",
  "task_msg": ""
}
```

返回值

请参考**状态码**。

4.3 告警配置管理

4.3.1 查询告警配置信息

功能介绍

查询用户配置信息，用户可以通过此接口查询是否接收某类告警，同时可以配置是手机短信还是电子邮件接收告警信息。

URI

- URI格式
  GET /v2/{project_id}/warnalert/alertconfig/query
- 参数说明

参数	是否必选	类型	说明
project_id	是	String	项目ID。

请求消息

无

响应消息

- 要素说明

参数	类型	说明
warn_config	列表数据结构	告警配置信息。
topic_urn	String	告警群组的唯一标识。
display_name	String	用于告警的SMN主题名称。

- warn_config字段数据结构说明

参数	类型	说明
antiDDoS	Boolean	DDoS攻击。
bruce_force	Boolean	暴力破解（系统登录，FTP，DB）。
remote_login	Boolean	异地登录提醒。
weak_password	Boolean	弱口令（系统，数据库）。
high_privilege	Boolean	数据库进程权限过高。
back_doors	Boolean	网页后门。
waf	Boolean	保留字段。
send_frequency	Integer	发送频率。 ● 0：表示每天一次。 ● 1：表示半小时一次。

示例

- 请求示例
  GET /v2/67641fe6886f43fcb78edbbf0ad0b99f/warnalert/alertconfig/query

- 响应示例

```
{
  "warn_config":    {
    "antiDDoS": true,
    "bruce_force": false,
    "remote_login": false,
    "weak_password": false,
    "high_privilege": false,
    "back_doors": false,
    "waf": false
  },
  "topic_urn": "urn:smn::67641fe6886f43fcb78edbbf0ad0b99f:test_soft",
  "display_name": "group_1"
}
```

说明

FTP是一种不安全的协议，为了保证数据传输的安全性，建议使用SFTP来代替FTP。

返回值

请参考状态码。

4.3.2 更新告警配置信息

功能介绍

更新用户配置信息，用户可以通过此接口更新是否接收某类告警，同时可以配置是手机短信还是电子邮件接收告警信息。

URI

- URI格式

  POST /v2/{project_id}/warnalert/alertconfig/update

- 参数说明

参数	是否必选	类型	说明
project_id	是	String	项目ID。

请求消息

- 要素说明

参数	是否必选	类型	说明
warn_config	是	列表数据结构	告警配置信息。
topic_urn	是	String	告警群组的唯一标识。
display_name	是	String	用于告警的SMN主题名称。

- warn_config字段数据结构说明

参数	是否必选	类型	说明
antiDDoS	否	Boolean	DDoS攻击。
bruce_force	否	Boolean	暴力破解（系统登录，FTP，DB）。
remote_login	否	Boolean	异地登录提醒。
weak_password	否	Boolean	弱口令（系统，数据库）。
high_privilege	否	Boolean	数据库进程权限过高。
back_doors	否	Boolean	网页后门。
waf	否	Boolean	保留字段。

说明

FTP是一种不安全的协议，为了保证数据传输的安全性，建议使用SFTP来代替FTP。

响应消息

参数	类型	说明
error_code	String	内部错误码
error_msg	String	内部错误描述
task_id	String	任务ID

示例

- 请求示例

```
{
  "warn_config":    {
     "antiDDoS": true,
     "bruce_force": false,
     "remote_login": false,
     "weak_password": false,
     "high_privilege": false,
     "back_doors": false,
     "waf": false
  },
  "topic_urn": "urn:smn::67641fe6886f43fcb78edbbf0ad0b99f:test_soft",
  "display_name": "group_1"
}
```

- 响应示例

```
{
  "error_code" : "10000000",
```

```
  "error_msg" : "Ok",
  "task_id" : ""
}
```

返回值

请参考**状态码**。

A 状态码

- 正常

返回值	说明
200	请求成功。

- 异常

状态码	编码	说明
400	Bad Request	服务器未能处理请求。
401	Unauthorized	被请求的页面需要用户名和密码。
403	Forbidden	对被请求页面的访问被禁止。
404	Not Found	服务器无法找到被请求的页面。
405	Method Not Allowed	请求中指定的方法不被允许。
406	Not Acceptable	服务器生成的响应无法被客户端所接受。
407	Proxy Authentication Required	用户必须首先使用代理服务器进行验证，这样请求才会被处理。
408	Request Timeout	请求超出了服务器的等待时间。
409	Conflict	由于冲突，请求无法被完成。
500	Internal Server Error	请求未完成，服务异常。
501	Not Implemented	请求未完成，服务器不支持所请求的功能。
502	Bad Gateway	请求未完成，服务器从上游服务器收到一个无效的响应。
503	Service Unavailable	请求未完成，系统暂时异常。
504	Gateway Timeout	网关超时。

B Anti-DDoS 错误码

状态码	错误码	错误信息	描述	处理措施
200	Anti-DDoS.0	Succeeded	成功	无需处理
200	Anti-DDoS.10000000	The task has been received and is being handled	任务已接收，正在处理	无需处理
400	Anti-DDoS.10000001	Enter a valid request message	请求消息格式非法	检查参数
400	Anti-DDoS.10001008	An incorrect task ID is used	不正确的任务ID	检查参数
400	Anti-DDoS.10001010	Invalid time	时间非法	检查参数
401	Anti-DDoS.10000004	Public test service denied	公测服务被拒绝	申请公测
403	Anti-DDoS.10000002	Failed to authenticate the token in the request	请求所带的Token认证失败	重新申请Token
403	Anti-DDoS.10000009	The account is restricted	账户受限	申请权限
403	Anti-DDoS.10000010	The account is frozen	账户冻结	申请解冻

状态码	错误码	错误信息	描述	处理措施
403	Anti-DDoS.10000012	Unknown user type	未知用户类型	申请权限
403	Anti-DDoS.10000016	VPC access failed or EIP is not exist	访问VPC平台异常或EIP不存在	联系管理员
403	Anti-DDoS.10000030	You have not been authenticated. Perform real-name authentication first.	您尚未认证，请先进行实名认证。	实名认证
403	Anti-DDoS.10001009	The operation permission is restricted	操作权限受限	申请权限
403	Anti-DDoS.11000001	Access to the database is rejected	数据库访问被拒绝	联系管理员
500	Anti-DDoS.11000000	Internal system exception. Contact technical support engineers	系统内部异常，请联系技术支持人员	联系管理员

C 获取项目 ID

调用 API 获取项目 ID

获取项目ID的接口为“GET https://{Endpoint}/v3/projects”，其中{Endpoint}为IAM的终端节点，可以从**地区和终端节点**获取。接口的认证鉴权请参见**认证鉴权**。

响应示例如下，其中projects下的“id”即为项目ID。

```
{
    "projects": [
        {
            "domain_id": "65382450e8f64ac0870cd180d14e684b",
            "is_domain": false,
            "parent_id": "65382450e8f64ac0870cd180d14e684b",
            "name": "xxxxxxxx",
            "description": "",
            "links": {
                "next": null,
                "previous": null,
                "self": "https://www.example.com/v3/projects/a4a5d4098fb4474fa22cd05f897d6b99"
            },
            "id": "a4a5d4098fb4474fa22cd05f897d6b99",
            "enabled": true
        }
    ],
    "links": {
        "next": null,
        "previous": null,
        "self": "https://www.example.com/v3/projects"
    }
}
```

从控制台获取项目 ID

在调用接口的时候，部分URL中需要填入项目编号，所以需要获取到项目编号。项目编号获取步骤如下：

1. 登录管理控制台。
2. 单击用户名，在下拉列表中单击“我的凭证”。
   在“我的凭证”页面的项目列表中查看项目ID。

D 修订记录

发布日期	修改说明
2024-06-30	第二次正式发布。 ● 新增**开通Anti-DDoS服务**。 ● **API概览**优化描述。 ● **如何调用API**优化描述。 ● 优化大纲结构。
2020-09-30	第一次正式发布。