DDoS Mitigation

API Reference

Issue 02

Date 2021-04-19



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2021. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Before You Start 1
1.1 Overview 1
1.2 API Calling 1
1.3 Endpoints 1
1.4 Notes and Constraints 1
1.5 Concepts 2
2 API Overview 4
3 API Calling 5
3.1 Making an API Request 5
3.2 Authentication 8
3.3 Response 9
4 Cloud Native Anti-DDoS Basic APIs 11
4.1 Task Controller 11
4.1.1 Querying Anti-DDoS Tasks 11
4.2 Anti-DDoS Controller 13
4.2.1 Querying the List of Defense Statuses of EIPs 13
4.2.2 Querying Optional Anti-DDoS Defense Policies 15
4.2.3 Querying Weekly Defense Statistics 20
4.2.4 Querying Configured Anti-DDoS Defense Policies 23
4.2.5 Updating Anti-DDoS Defense Policies 25
4.2.6 Querying the Traffic of a Specified EIP 27
4.2.7 Querying Events of a Specified EIP 30
4.2.8 Querying Configured Anti-DDoS Defense Policies 32
4.3 Alert Controller 34
4.3.1 Querying alert config 34
4.3.2 Configuring alert config 36
4.4 Default Anti-DDoS Controller 39
4.4.1 Configuring the Default Protection Policy for Newly Purchased Public IP Addresses 39
4.4.2 Querying the Default Protection Policy Configured for the Newly Purchased Public IP Addresses 41
4.4.3 Deleting the Default Anti-DDoS Policy Configured for Newly Purchased Public IP Addresses 43
5 Application Examples of Cloud Native Anti-DDoS Basic APIs 45
5.1 Example 1: Updating Defense Policy for an IP Address 45

 Copyright © Huawei Technologies Co., Ltd.

5.2 Example 2: Configuring the Default Protection Policy....49

A Appendix....52

A.1 HTTP Status Codes of Cloud Native Anti-DDoS Basic....52

A.2 Error Codes....53

A.3 Obtaining a Project ID....54

B Historical APIs of Cloud Native Anti-DDoS Basic....56

B.1 Querying Optional Anti-DDoS Defense Policies....56

B.2 Querying Anti-DDoS Tasks....60

C Change History....63

 Copyright © Huawei Technologies Co., Ltd.

1 Before You Start

1.1 Overview

HUAWEI CLOUD provides multiple security solutions to defend against DDoS attacks. You can select an appropriate one based on your service requirements. HUAWEI CLOUD Anti-DDoS Service (ADS) includes CNAD Basic (Anti-DDoS), CNAD Pro, and AAD.

Cloud Native Anti-DDoS Basic (Anti-DDoS), Anti-DDoS for short, protects public IP addresses against Layer 4 to Layer 7 distributed denial of service (DDoS) attacks and sends alarms immediately when detecting an attack. In addition, Anti-DDoS improves the bandwidth utilization to further safeguard user services.

This document describes how to use application programming interfaces (APIs) to perform operations to Anti-DDoS, such as querying or updating Anti-DDoS protection policy. For details about all supported operations, see **API Overview**.

Before calling Anti-DDoS APIs, ensure that you are familiar with Anti-DDoS concepts. For details, see section "Service Overview" of the *Anti-DDoS User Guide*.

1.2 API Calling

Anti-DDoS provides Representational State Transfer (REST) APIs, allowing you to use HTTPS requests to call them. For details, see **API Calling**.

1.3 Endpoints

An endpoint is the **request address** for calling an API. Endpoints vary depending on services and regions. For the endpoints of all services, see **Regions and Endpoints**.

1.4 Notes and Constraints

For details about the constraints, see the API description.

 Copyright © Huawei Technologies Co., Ltd.

1.5 Concepts

- Account

  An account is created upon successful registration. The account has full access permissions for all of its cloud services and resources. It can be used to reset user passwords and grant user permissions. The account is a payment entity and should not be used to perform routine management. For security purposes, create IAM users and grant them permissions for routine management.

- User

  An IAM user is created by an account in IAM to use cloud services. Each IAM user has its own identity credentials (password and access keys).

  An IAM user can view the account ID and user ID on the **My Credentials** page of the management console. The domain name, username, and password will be required for API authentication.

- Region

  Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.

  For details, see **Region and AZ**.

- Availability Zone (AZ)

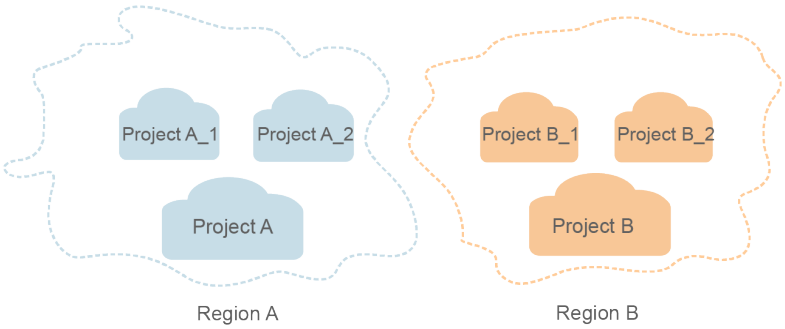
  An AZ comprises one or multiple physical data centers equipped with independent ventilation, fire, water, and electricity facilities. Compute, network, storage, and other resources in an AZ are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to support cross-AZ high-availability systems.

- Project

  Projects group and isolate resources (including compute, storage, and network resources) across physical regions. A default project is provided for each region, and subprojects can be created under each default project. Users can be granted permissions to access all resources in a specific project. For more refined access control, create subprojects under a project and create resources in the subprojects. Users can then be assigned permissions to access only specific resources in the subprojects.

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-1 Project isolation model



 Copyright © Huawei Technologies Co., Ltd.

2 API Overview

You can use all functions of Anti-DDoS through its APIs.

Type	Description
APIs of Anti-DDoS	Anti-DDoS APIs, including the APIs for querying and updating the Anti-DDoS defense policies.
Alarm Reminding APIs	Alarm reminding APIs, including the API for querying alarm configuration information

 Copyright © Huawei Technologies Co., Ltd.

3 API Calling

3.1 Making an API Request

This section describes the structure of a REST API request, and uses the IAM API for **obtaining a user token** as an example to demonstrate how to call an API. The obtained token can then be used to authenticate the calling of other APIs.

Request URI

A request URI is in the following format:

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

Although a request URI is included in the request header, most programming languages or frameworks require the request URI to be transmitted separately.

- **URI-scheme**:

  Protocol used to transmit requests. All APIs use HTTPS.

- **Endpoint**:

  Domain name or IP address of the server bearing the REST service. The endpoint varies between services in different regions. It can be obtained from **Regions and Endpoints**.

  For example, the endpoint of IAM in the **CN North-Beijing1** region is **iam.cn-north-1.myhuaweicloud.com**.

- **resource-path**:

  Access path of an API for performing a specified operation. Obtain the path from the URI of an API. For example, the **resource-path** of the API used to obtain a user token is **/v3/auth/tokens**.

- **query-string**:

  Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of "Parameter name=Parameter value". For example, **?limit=10** indicates that a maximum of 10 data records will be displayed.

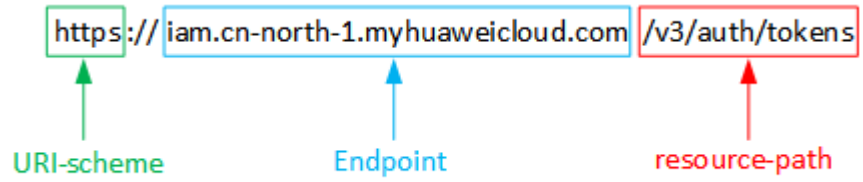
For example, to obtain an IAM token in the **CN North-Beijing1** region, obtain the endpoint of IAM (**iam.cn-north-1.myhuaweicloud.com**) for this region and the

 Copyright © Huawei Technologies Co., Ltd.

resource-path (**/v3/auth/tokens**) in the URI of the API used to **obtain a user token**. Then, construct the URI as follows:

```
https://iam.cn-north-1.myhuaweicloud.com/v3/auth/tokens
```

Figure 3-1 Example URI



NOTE

To simplify the URI display in this document, each API is provided only with a **resource-path** and a request method. The **URI-scheme** of all APIs is **HTTPS**, and the endpoints of all APIs in the same region are identical.

Request Methods

The HTTP protocol defines the following request methods that can be used to send a request to the server:

- **GET**: requests the server to return specified resources.
- **PUT**: requests the server to update specified resources.
- **POST**: requests the server to add resources or perform special operations.
- **DELETE**: requests the server to delete specified resources, for example, an object.
- **HEAD**: same as GET except that the server must return only the response header.
- **PATCH**: requests the server to update partial content of a specified resource. If the resource does not exist, a new resource will be created.

For example, in the case of the API used to **obtain a user token**, the request method is POST. The request is as follows:

```
POST https://iam.cn-north-1.myhuaweicloud.com/v3/auth/tokens
```

Request Header

You can also add additional header fields to a request, such as the fields required by a specified URI or HTTP method. For example, to request for the authentication information, add **Content-Type**, which specifies the request body type.

Common request header fields are as follows:

- **Content-Type**: specifies the request body type or format. This field is mandatory and its default value is **application/json**. Other values of this field will be provided for specific APIs if any.
- **X-Auth-Token**: specifies a user token only for token-based API authentication. The user token is a response to the API used to **obtain a user token**. This API is the only one that does not require authentication.

Copyright © Huawei Technologies Co., Ltd.

> **NOTE**
>
> In addition to supporting token-based authentication, APIs also support authentication using access key ID/secret access key (AK/SK). During AK/SK-based authentication, an SDK is used to sign the request, and the **Authorization** (signature information) and **X-Sdk-Date** (time when the request is sent) header fields are automatically added to the request.
>
> For more information, see **AK/SK-based Authentication**.

The API used to **obtain a user token** does not require authentication. Therefore, only the **Content-Type** field needs to be added to requests for calling the API. An example of such requests is as follows:

```
POST https://iam.cn-north-1.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json
```

Request Body

The body of a request is often sent in a structured format as specified in the **Content-Type** header field. The request body transfers content except the request header.

The request body varies between APIs. Some APIs do not require the request body, such as the APIs requested using the GET and DELETE methods.

In the case of the API used to **obtain a user token**, the request parameters and parameter description can be obtained from the API request. The following provides an example request with a body included. Set ***username*** to the name of a user, ***domainname*** to the name of the account that the user belongs to, ********* to the user's login password, and ***xxxxxxxxxxxxxxxxx*** to the project name, such as **cn-north-1**. You can learn more information about projects from **Regions and Endpoints**. Check the value of the **Region** column.

> **NOTE**
>
> The **scope** parameter specifies where a token takes effect. You can set **scope** to an account or a project under an account. In the following example, the token takes effect only for the resources in a specified project. For more information about this API, see **Obtaining a User Token**.

```
POST https://iam.cn-north-1.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json

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

 Copyright © Huawei Technologies Co., Ltd.

```
    }
  }
}
```

If all data required for the API request is available, you can send the request to call the API through **curl**, **Postman**, or coding. In the response to the API used to obtain a user token, **x-subject-token** is the desired user token. This token can then be used to authenticate the calling of other APIs.

3.2 Authentication

Requests for calling an API can be authenticated using either of the following methods:

- Token-based authentication: Requests are authenticated using a token.
- AK/SK-based authentication: Requests are authenticated by encrypting the request body using an AK/SK pair. This method is recommended because it provides higher security than token-based authentication.

Token-based Authentication

NOTE

The validity period of a token is 24 hours. When using a token for authentication, cache it to prevent frequently calling the IAM API used to obtain a user token.

A token specifies temporary permissions in a computer system. During API authentication using a token, the token is added to requests to get permissions for calling the API.

The token can be obtained by calling the required API. For more information, see **Obtaining a User Token**. A project-level token is required for calling this API, that is, **auth.scope** must be set to **project** in the request body. Example:

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

After a token is obtained, the **X-Auth-Token** header field must be added to requests to specify the token when calling other APIs. For example, if the token is **ABCDEFJ....**, **X-Auth-Token: ABCDEFJ....** can be added to a request as follows:

 Copyright © Huawei Technologies Co., Ltd.

```
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

AK/SK-based Authentication

NOTE

AK/SK-based authentication supports API requests with a body not larger than 12 MB. For API requests with a larger body, token-based authentication is recommended.

In AK/SK-based authentication, AK/SK is used to sign requests and the signature is then added to the requests for authentication.

- AK: access key ID, which is a unique identifier used in conjunction with a secret access key to sign requests cryptographically.
- SK: secret access key used in conjunction with an AK to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

In AK/SK-based authentication, you can use an AK/SK to sign requests based on the signature algorithm or use the signing SDK to sign requests. For details about how to sign requests and use the signing SDK, see **API Signature Guide**.

NOTICE

The signing SDK is only used for signing requests and is different from the SDKs provided by services.

3.3 Response

Status Code

After sending a request, you will receive a response, including a status code, response header, and response body.

A status code is a group of digits, ranging from 1xx to 5xx. It indicates the status of a request. For more information, see **HTTP Status Codes of Cloud Native Anti-DDoS Basic**.

For example, if status code **201** is returned for calling the API used to **obtain a user token**, the request is successful.

Response Header

Similar to a request, a response also has a header, for example, **Content-Type**.

The following shows the response header for the API to **obtain a user token**, in which **x-subject-token** is the desired user token. This token can then be used to authenticate the calling of other APIs.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-2 Header fields of the response to the request for obtaining a user token



(Optional) Response Body

The body of a response is often returned in structured format as specified in the **Content-Type** header field. The response body transfers content except the response header.

The following shows part of the response body for the API to **obtain a user token**. For the sake of space, only part of the content is displayed here.

```
{
    "token": {
        "expires_at": "2019-02-13T06:52:13.855000Z",
        "methods": [
            "password"
        ],
        "catalog": [
            {
                "endpoints": [
                    {
                        "region_id": "xxxxxxxx",
.....
```

If an error occurs during API calling, an error code and a message will be displayed. The following shows an error response body.

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

In the response body, **error_code** is an error code, and **error_msg** provides information about the error.

 Copyright © Huawei Technologies Co., Ltd.

4 Cloud Native Anti-DDoS Basic APIs

4.1 Task Controller

4.1.1 Querying Anti-DDoS Tasks

Function

Querying Anti-DDoS Tasks

Debugging

You can use **API Explorer** to debug this API.

URI

GET /v2/{project_id}/query-task-status

Table 4-1 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	poject id Minimum: **32** Maximum: **64**

Table 4-2 Query parameters

Parameter	Mandatory	Type	Description
task_id	Yes	String	Task ID (nonnegative integer) character string

 Copyright © Huawei Technologies Co., Ltd.

Request Parameters

Table 4-3 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	token Minimum: **32** Maximum: **2097152**
Content-Type	Yes	String	Default: **application/json;charset=utf8**

Response Parameters

Status code: 200

Table 4-4 Response body parameters

Parameter	Type	Description
task_status	String	Status of a task
task_msg	String	Additional information about a task

Example Requests

None

Example Responses

Status code: 200

OK

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

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

Copyright © Huawei Technologies Co., Ltd.

4.2 Anti-DDoS Controller

4.2.1 Querying the List of Defense Statuses of EIPs

Function

Querying the List of Defense Statuses of EIPs

Debugging

You can use **API Explorer** to debug this API.

URI

GET /v1/{project_id}/antiddos

Table 4-5 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	poject id Minimum: **32** Maximum: **64**

Table 4-6 Query parameters

Parameter	Mandatory	Type	Description
status	No	String	status
limit	No	String	Maximum number of returned results. The value ranges from 1 to 100.
offset	No	String	Offset. The value ranges from 0 to 2147483647.
ip	No	String	IP address. Both IPv4 and IPv6 addresses are supported. For example, if you enter ?ip=192.168, the defense status of EIPs corresponding to 192.168.111.1 and 10.192.168.8 is returned.

 Copyright © Huawei Technologies Co., Ltd.

Request Parameters

Table 4-7 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	token Minimum: **32** Maximum: **2097152**
Content-Type	Yes	String	Default: **application/json;charset=utf8**

Response Parameters

Status code: 200

Table 4-8 Response body parameters

Parameter	Type	Description
total	Integer	total count
ddosStatus	Array of **DDosStatus** objects	Anti-DDoS status

Table 4-9 DDosStatus

Parameter	Type	Description
floating_ip_id	String	ID of an EIP
floating_ip_address	String	IP address. Both IPv4 and IPv6 addresses are supported. For example, if you enter ?ip=192.168, the defense status of EIPs corresponding to 192.168.111.1 and 10.192.168.8 is returned.
network_type	String	EIP type. The value can be: EIP: EIP that is bound or not bound with ECS. ELB: EIP that is bound with ELB.
status	String	Defense status
blackhole_endtime	Long	The end time of blackhole
protect_type	String	Protect type

Copyright © Huawei Technologies Co., Ltd.

Parameter	Type	Description
traffic_threshold	Long	Threshold of traffic
http_threshold	Long	Threshold of http traffic

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "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
  } ]
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.2.2 Querying Optional Anti-DDoS Defense Policies

Function

Querying Optional Anti-DDoS Defense Policies

Debugging

You can use **API Explorer** to debug this API.

Copyright © Huawei Technologies Co., Ltd.

URI

GET /v2/{project_id}/antiddos/query-config-list

Table 4-10 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	poject id Minimum: **32** Maximum: **64**

Request Parameters

Table 4-11 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	token Minimum: **32** Maximum: **2097152**
Content-Type	Yes	String	Default: **application/json;charset=utf8**

Response Parameters

Status code: 200

Table 4-12 Response body parameters

Parameter	Type	Description
traffic_limited_list	Array of **TriggerBpsDict** objects	List of traffic limits
http_limited_list	Array of **TriggerQpsDict** objects	List of HTTP limits
connection_limited_list	Array of **CleanLimitDict** objects	List of limits of numbers of connections
extend_ddos_config	Array of **ExtendDDoSSet** objects	List of extend ddos limits

Copyright © Huawei Technologies Co., Ltd.

Table 4-13 TriggerBpsDict

Parameter	Type	Description
traffic_pos_id	Long	Position ID of traffic
traffic_per_second	Long	Threshold of traffic per second (Mbit/s)
packet_per_second	Long	Threshold of number of packets per second

Table 4-14 TriggerQpsDict

Parameter	Type	Description
http_request_pos_id	Long	Position ID of number of HTTP requests
http_packet_per_second	Long	Threshold of number of HTTP requests per second

Table 4-15 CleanLimitDict

Parameter	Type	Description
cleaning_access_pos_id	Long	Position ID of access limit during cleaning
new_connection_limited	Long	Number of new connections of a source IP address
total_connection_limited	Long	Total number of connections of a source IP address

Table 4-16 ExtendDDoSSet

Parameter	Type	Description
SetID	Long	Position ID of config
new_connection_limited	Long	List of limits of numbers of connections
total_connection_limited	Long	List of limits of numbers of total connections
http_packet_per_second	Long	Threshold of number of HTTP requests per second

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Type	Description
traffic_per_second	Long	Threshold of traffic per second (Mbit/s)
packet_per_second	Long	Threshold of number of packets per second

Example Requests

None

Example Responses

Status code: 200

OK


```
{
  "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
  }, {
    "traffic_pos_id" : 3,
    "traffic_per_second" : 50,
    "packet_per_second" : 10000
  }, {
    "traffic_pos_id" : 4,
    "traffic_per_second" : 70,
    "packet_per_second" : 15000
  }, {
    "traffic_pos_id" : 5,
    "traffic_per_second" : 100,
    "packet_per_second" : 20000
  }, {
    "traffic_pos_id" : 6,
    "traffic_per_second" : 150,
    "packet_per_second" : 25000
  }, {
    "traffic_pos_id" : 7,
    "traffic_per_second" : 200,
    "packet_per_second" : 35000
  }, {
    "traffic_pos_id" : 8,
    "traffic_per_second" : 250,
    "packet_per_second" : 50000
  }, {
    "traffic_pos_id" : 9,
    "traffic_per_second" : 300,
    "packet_per_second" : 70000
  }, {
    "traffic_pos_id" : 88,
    "traffic_per_second" : 1000,
    "packet_per_second" : 300000
  } ],
  "http_limited_list" : [ {
    "http_request_pos_id" : 1,
    "http_packet_per_second" : 100
```


 Copyright © Huawei Technologies Co., Ltd.

```
}, {
  "http_request_pos_id" : 2,
  "http_packet_per_second" : 150
}, {
  "http_request_pos_id" : 3,
  "http_packet_per_second" : 240
}, {
  "http_request_pos_id" : 4,
  "http_packet_per_second" : 350
}, {
  "http_request_pos_id" : 5,
  "http_packet_per_second" : 480
}, {
  "http_request_pos_id" : 6,
  "http_packet_per_second" : 550
}, {
  "http_request_pos_id" : 7,
  "http_packet_per_second" : 700
}, {
  "http_request_pos_id" : 8,
  "http_packet_per_second" : 850
}, {
  "http_request_pos_id" : 9,
  "http_packet_per_second" : 1000
}, {
  "http_request_pos_id" : 10,
  "http_packet_per_second" : 1500
}, {
  "http_request_pos_id" : 11,
  "http_packet_per_second" : 2000
}, {
  "http_request_pos_id" : 12,
  "http_packet_per_second" : 3000
}, {
  "http_request_pos_id" : 13,
  "http_packet_per_second" : 5000
}, {
  "http_request_pos_id" : 14,
  "http_packet_per_second" : 10000
}, {
  "http_request_pos_id" : 15,
  "http_packet_per_second" : 20000
} ],
"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
}, {
  "cleaning_access_pos_id" : 3,
  "new_connection_limited" : 30,
  "total_connection_limited" : 200
}, {
  "cleaning_access_pos_id" : 4,
  "new_connection_limited" : 40,
  "total_connection_limited" : 250
}, {
  "cleaning_access_pos_id" : 5,
  "new_connection_limited" : 50,
  "total_connection_limited" : 300
}, {
  "cleaning_access_pos_id" : 6,
  "new_connection_limited" : 60,
  "total_connection_limited" : 500
}, {
  "cleaning_access_pos_id" : 7,
```


 Copyright © Huawei Technologies Co., Ltd.

```
    "new_connection_limited" : 70,
    "total_connection_limited" : 600
  }, {
    "cleaning_access_pos_id" : 8,
    "new_connection_limited" : 80,
    "total_connection_limited" : 700
  } ],
  "extend_ddos_config" : [ ]
}
```


Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.2.3 Querying Weekly Defense Statistics

Function

Querying Weekly Defense Statistics

Debugging

You can use **API Explorer** to debug this API.

URI

GET /v1/{project_id}/antiddos/weekly

Table 4-17 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	poject id Minimum: **32** Maximum: **64**

Table 4-18 Query parameters

Parameter	Mandatory	Type	Description
period_start_date	No	String	Start date of a seven-day period

 Copyright © Huawei Technologies Co., Ltd.

Request Parameters

Table 4-19 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	token Minimum: **32** Maximum: **2097152**
Content-Type	Yes	String	Default: **application/json;charset=utf8**

Response Parameters

Status code: 200

Table 4-20 Response body parameters

Parameter	Type	Description
ddos_intercept_times	Integer	Number of DDoS attacks blocked in a week
weekdata	Array of **WeeklyCount** objects	Number of attacks in a week
top10	Array of **WeeklyTop10** objects	Top 10 attacked IP addresses

Table 4-21 WeeklyCount

Parameter	Type	Description
ddos_intercept_times	Integer	Number of DDoS attacks blocked
ddos_blackhole_times	Integer	Number of DDoS black holes
max_attack_bps	Integer	Maximum attack traffic
max_attack_conns	Integer	Maximum number of attack connections
period_start_date	Long	Start date

Copyright © Huawei Technologies Co., Ltd.

Table 4-22 WeeklyTop10

Parameter	Type	Description
floating_ip_address	String	EIP
times	Integer	Number of DDoS attacks intercepted, including cleaning operations and black holes

Example Requests

None

Example Responses

Status code: 200

OK


```
{
  "ddos_intercept_times" : 0,
  "weekdata" : [ {
    "ddos_intercept_times" : 0,
    "ddos_blackhole_times" : 0,
    "max_attack_bps" : 0,
    "max_attack_conns" : 0,
    "period_start_date" : 1605496722606
  }, {
    "ddos_intercept_times" : 0,
    "ddos_blackhole_times" : 0,
    "max_attack_bps" : 0,
    "max_attack_conns" : 0,
    "period_start_date" : 1605583122606
  }, {
    "ddos_intercept_times" : 0,
    "ddos_blackhole_times" : 0,
    "max_attack_bps" : 0,
    "max_attack_conns" : 0,
    "period_start_date" : 1605669522606
  }, {
    "ddos_intercept_times" : 0,
    "ddos_blackhole_times" : 0,
    "max_attack_bps" : 0,
    "max_attack_conns" : 0,
    "period_start_date" : 1605755922606
  }, {
    "ddos_intercept_times" : 0,
    "ddos_blackhole_times" : 0,
    "max_attack_bps" : 0,
    "max_attack_conns" : 0,
    "period_start_date" : 1605842322606
  }, {
    "ddos_intercept_times" : 0,
    "ddos_blackhole_times" : 0,
    "max_attack_bps" : 0,
    "max_attack_conns" : 0,
    "period_start_date" : 1605928722606
  }, {
    "ddos_intercept_times" : 0,
    "ddos_blackhole_times" : 0,
    "max_attack_bps" : 0,
    "max_attack_conns" : 0,
```


 Copyright © Huawei Technologies Co., Ltd.

```
    "period_start_date" : 1606015122606
  } ],
  "top10" : [ ]
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.2.4 Querying Configured Anti-DDoS Defense Policies

Function

Querying Configured Anti-DDoS Defense Policies

Debugging

You can use **API Explorer** to debug this API.

URI

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

Table 4-23 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	poject id Minimum: **32** Maximum: **64**
floating_ip_id	Yes	String	ID corresponding to the EIP of a user

Table 4-24 Query parameters

Parameter	Mandatory	Type	Description
ip	No	String	IP address.

Copyright © Huawei Technologies Co., Ltd.

Request Parameters

Table 4-25 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	token Minimum: **32** Maximum: **2097152**
Content-Type	Yes	String	Default: **application/json;charset=utf8**

Response Parameters

Status code: 200

Table 4-26 Response body parameters

Parameter	Type	Description
enable_L7	Boolean	Whether L7 defense has been enabled
traffic_pos_id	Long	Position ID of traffic. The value ranges from 1 to 9 and 33 to 36.
http_request_pos_id	Long	Position ID of number of HTTP requests. The value ranges from 1 to 15 and 33 to 36.
cleaning_access_pos_id	Long	Position ID of access limit during cleaning. The value ranges from 1 to 8 and 33 to 36.
app_type_id	Long	Application type ID.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "enable_L7" : false,
  "traffic_pos_id" : 8,
  "http_request_pos_id" : 8,
  "cleaning_access_pos_id" : 8,
  "app_type_id" : 1
}
```

 Copyright © Huawei Technologies Co., Ltd.

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.2.5 Updating Anti-DDoS Defense Policies

Function

Updating Anti-DDoS Defense Policies

Debugging

You can use **API Explorer** to debug this API.

URI

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

Table 4-27 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	poject id Minimum: **32** Maximum: **64**
floating_ip_id	Yes	String	ID corresponding to the EIP of a user

Table 4-28 Query parameters

Parameter	Mandatory	Type	Description
ip	No	String	ip

Copyright © Huawei Technologies Co., Ltd.

Request Parameters

Table 4-29 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	token Minimum: **32** Maximum: **2097152**
Content-Type	Yes	String	Default: **application/json;charset=utf8**

Table 4-30 Request body parameters

Parameter	Mandatory	Type	Description
app_type_id	Yes	Integer	Application type ID.
cleaning_access_pos_id	Yes	Integer	Position ID of access limit during cleaning. The value ranges from 1 to 8 and 33 to 36.
enable_L7	Yes	Boolean	Whether L7 defense has been enabled
http_request_pos_id	Yes	Integer	Position ID of number of HTTP requests. The value ranges from 1 to 15 and 33 to 36.
traffic_pos_id	Yes	Integer	Position ID of traffic. The value ranges from 1 to 9 and 33 to 36.

Response Parameters

Status code: 200

Table 4-31 Response body parameters

Parameter	Type	Description
error_code	String	Internal error code
error_msg	String	Internal error description
task_id	String	ID of a task.

Copyright © Huawei Technologies Co., Ltd.

Example Requests

```
{
  "app_type_id" : 0,
  "cleaning_access_pos_id" : 8,
  "enable_L7" : false,
  "http_request_pos_id" : 1,
  "traffic_pos_id" : 1
}
```

Example Responses

Status code: 200

OK

```
{
  "error_code" : "10000000",
  "error_msg" : "The task has been received and is being handled",
  "task_id" : "59385d2a-6266-4d3a-9122-a228c530f557"
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.2.6 Querying the Traffic of a Specified EIP

Function

Querying the Traffic of a Specified EIP

Debugging

You can use **API Explorer** to debug this API.

URI

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

Table 4-32 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	poject id Minimum: **32** Maximum: **64**

Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
floating_ip_id	Yes	String	ID corresponding to the EIP of a user

Table 4-33 Query parameters

Parameter	Mandatory	Type	Description
ip	No	String	IP address. Both IPv4 and IPv6 addresses are supported. For example, if you enter ?ip=192.168, the defense status of EIPs corresponding to 192.168.111.1 and 10.192.168.8 is returned.

Request Parameters

Table 4-34 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	token Minimum: **32** Maximum: **2097152**
Content-Type	Yes	String	Default: **application/json;charset=utf8**

Response Parameters

Status code: 200

Table 4-35 Response body parameters

Parameter	Type	Description
data	Array of **DailyData** objects	Traffic in the last 24 hours

Copyright © Huawei Technologies Co., Ltd.

Table 4-36 DailyData

Parameter	Type	Description
period_start	Long	Start time
bps_in	Integer	Inbound traffic (bit/s)
bps_attack	Long	Attack traffic (bit/s)
total_bps	Long	Total traffic
pps_in	Long	Inbound packet rate (number of packets per second)
pps_attack	Long	Attack packet rate (number of packets per second)
total_pps	Long	Total packet rate

Example Requests

None

Example Responses

Status code: 200

OK

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

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

 Copyright © Huawei Technologies Co., Ltd.

4.2.7 Querying Events of a Specified EIP

Function

Querying Events of a Specified EIP

Debugging

You can use **API Explorer** to debug this API.

URI

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

Table 4-37 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	poject id Minimum: **32** Maximum: **64**
floating_ip_id	Yes	String	ID corresponding to the EIP of a user

Table 4-38 Query parameters

Parameter	Mandatory	Type	Description
sort_dir	No	String	Possible values: desc: indicates that query results are given and sorted by time in descending order. asc: indicates that query results are given and sorted by time in ascending order.
limit	No	String	Limit of number of returned results or the maximum number of returned results of a query.
offset	No	String	Offset. This parameter is valid only when used together with the limit parameter.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
ip	No	String	IP address. Both IPv4 and IPv6 addresses are supported. For example, if you enter ?ip=192.168, the defense status of EIPs corresponding to 192.168.111.1 and 10.192.168.8 is returned.

Request Parameters

Table 4-39 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	token Minimum: **32** Maximum: **2097152**
Content-Type	Yes	String	Default: **application/json;charset=utf8**

Response Parameters

Status code: 200

Table 4-40 Response body parameters

Parameter	Type	Description
total	Long	Total number of EIPs
logs	Array of **DailyLog** objects	List of events

Table 4-41 DailyLog

Parameter	Type	Description
start_time	Long	Start time
end_time	Long	End time
status	Integer	Defense status
trigger_bps	Integer	Traffic at the triggering point

Copyright © Huawei Technologies Co., Ltd.

Parameter	Type	Description
trigger_pps	Integer	Packet rate at the triggering point
trigger_http_pps	Integer	HTTP request rate at the triggering point

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "total" : 0,
  "logs" : [ ]
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.2.8 Querying Configured Anti-DDoS Defense Policies

Function

Querying Configured Anti-DDoS Defense Policies

Debugging

You can use **API Explorer** to debug this API.

URI

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

 Copyright © Huawei Technologies Co., Ltd.

Table 4-42 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	poject id Minimum: **32** Maximum: **64**
floating_ip_id	Yes	String	ID corresponding to the EIP of a user

Table 4-43 Query parameters

Parameter	Mandatory	Type	Description
ip	No	String	IP address. Both IPv4 and IPv6 addresses are supported. For example, if you enter ?ip=192.168, the defense status of EIPs corresponding to 192.168.111.1 and 10.192.168.8 is returned.

Request Parameters

Table 4-44 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	token Minimum: **32** Maximum: **2097152**
Content-Type	Yes	String	Default: **application/json;charset=utf8**

Response Parameters

Status code: 200

Table 4-45 Response body parameters

Parameter	Type	Description
status	String	Ddos status

Copyright © Huawei Technologies Co., Ltd.

Example Requests

None

Example Responses

Status code: 200

OK

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

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3 Alert Controller

4.3.1 Querying alert config

Function

Querying alert config

Debugging

You can use **API Explorer** to debug this API.

URI

GET /v2/{project_id}/warnalert/alertconfig/query

Table 4-46 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	poject id Minimum: **32** Maximum: **64**

Copyright © Huawei Technologies Co., Ltd.

Request Parameters

Table 4-47 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	token Minimum: **32** Maximum: **2097152**
Content-Type	Yes	String	Default: **application/json;charset=utf8**

Response Parameters

Status code: 200

Table 4-48 Response body parameters

Parameter	Type	Description
topic_urn	String	ID of an alarm group
display_name	String	display name of alert config
warn_config	**warn_config** object	warn config

Table 4-49 warn_config

Parameter	Type	Description
antiDDoS	Boolean	DDoS attacks
back_doors	Boolean	Webshells
bruce_force	Boolean	Brute force cracking (system logins, FTP, and DB)
high_privilege	Boolean	Overly high rights of a database process
remote_login	Boolean	Alarms about remote logins
send_frequency	Integer	Possible values:0: indicates that alarms are sent once a day.1: indicates that alarms are sent once every half hour.This parameter is mandatory for the Host Intrusion Detection (HID) service.
waf	Boolean	Reserved

Copyright © Huawei Technologies Co., Ltd.

Parameter	Type	Description
weak_password	Boolean	Weak passwords (system and database)

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "warn_config" : {
    "antiDDoS" : false,
    "bruce_force" : false,
    "remote_login" : false,
    "weak_password" : false,
    "high_privilege" : false,
    "back_doors" : false,
    "waf" : false,
    "send_frequency" : 0
  },
  "topic_urn" : null,
  "display_name" : null
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.3.2 Configuring alert config

Function

Configuring alert config

Debugging

You can use **API Explorer** to debug this API.

Copyright © Huawei Technologies Co., Ltd.

URI

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

Table 4-50 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	poject id Minimum: **32** Maximum: **64**

Request Parameters

Table 4-51 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	token Minimum: **32** Maximum: **2097152**
Content-Type	Yes	String	Default: **application/json;charset=utf8**

Table 4-52 Request body parameters

Parameter	Mandatory	Type	Description
display_name	Yes	String	display name of alert config
topic_urn	Yes	String	topic urn
warn_config	Yes	**warn_config** object	warn config

Table 4-53 warn_config

Parameter	Mandatory	Type	Description
antiDDoS	No	Boolean	DDoS attacks
back_doors	No	Boolean	Webshells
bruce_force	No	Boolean	Brute force cracking (system logins, FTP, and DB)

Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
high_privilege	No	Boolean	Overly high rights of a database process
remote_login	No	Boolean	Alarms about remote logins
send_frequency	No	Integer	Possible values:0: indicates that alarms are sent once a day.1: indicates that alarms are sent once every half hour.This parameter is mandatory for the Host Intrusion Detection (HID) service.
waf	No	Boolean	Reserved
weak_password	No	Boolean	Weak passwords (system and database)

Response Parameters

Status code: 200

Table 4-54 Response body parameters

Parameter	Type	Description
error_code	String	Internal error code
error_msg	String	Internal error description

Example Requests

```
{
  "display_name" : "",
  "topic_urn" : "8",
  "enable_L7" : false,
  "warn_config" : {
    "antiDDoS" : false,
    "back_doors" : false,
    "bruce_force" : false,
    "high_privilege" : false,
    "remote_login" : false,
    "send_frequency" : 10,
    "waf" : false,
    "weak_password" : false
  }
}
```

Example Responses

Status code: 200

OK

Copyright © Huawei Technologies Co., Ltd.

```
{
  "error_code" : "10000000",
  "error_msg" : "Ok",
  "task_id" : ""
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.4 Default Anti-DDoS Controller

4.4.1 Configuring the Default Protection Policy for Newly Purchased Public IP Addresses

Function

This API enables you to configure the default protection policy. After a protection policy is configured, it applies to the newly purchased public IP addresses.

Debugging

You can use **API Explorer** to debug this API.

URI

POST /v1/{project_id}/antiddos/default-config

Table 4-55 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	poject id Minimum: **32** Maximum: **64**

Copyright © Huawei Technologies Co., Ltd.

Request Parameters

Table 4-56 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	token Minimum: **32** Maximum: **2097152**
Content-Type	Yes	String	Default: **application/json;charset=utf8**

Table 4-57 Request body parameters

Parameter	Mandatory	Type	Description
enable_L7	Yes	Boolean	Whether L7 defense has been enabled
traffic_pos_id	Yes	Long	Position ID of traffic. The value ranges from 1 to 9 and 33 to 36.
http_request_pos_id	Yes	Long	Position ID of number of HTTP requests. The value ranges from 1 to 15 and 33 to 36.
cleaning_access_pos_id	Yes	Long	Position ID of access limit during cleaning. The value ranges from 1 to 8 and 33 to 36.
app_type_id	Yes	Long	Application type ID.

Response Parameters

Status code: 200

Table 4-58 Response body parameters

Parameter	Type	Description
error_code	String	Internal error code
error_msg	String	Internal error description

Example Requests

None

 Copyright © Huawei Technologies Co., Ltd.

Example Responses

Status code: 200

OK

```
{
  "error_code" : "10000000",
  "error_msg" : "Ok",
  "task_id" : ""
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.4.2 Querying the Default Protection Policy Configured for the Newly Purchased Public IP Addresses

Function

This API enables you to query the default protection policy configured for the newly purchased public IP addresses.

Debugging

You can use **API Explorer** to debug this API.

URI

GET /v1/{project_id}/antiddos/default-config

Table 4-59 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	poject id Minimum: **32** Maximum: **64**

Copyright © Huawei Technologies Co., Ltd.

Request Parameters

Table 4-60 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	token Minimum: **32** Maximum: **2097152**
Content-Type	Yes	String	Default: **application/json;charset=utf8**

Response Parameters

Status code: 200

Table 4-61 Response body parameters

Parameter	Type	Description
enable_L7	Boolean	Whether L7 defense has been enabled
traffic_pos_id	Long	Position ID of traffic. The value ranges from 1 to 9 and 33 to 36.
http_request_pos_id	Long	Position ID of number of HTTP requests. The value ranges from 1 to 15 and 33 to 36.
cleaning_access_pos_id	Long	Position ID of access limit during cleaning. The value ranges from 1 to 8 and 33 to 36.
app_type_id	Long	Application type ID.

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "app_type_id" : 1,
  "cleaning_access_pos_id" : 8,
  "enable_L7" : false,
  "http_request_pos_id" : 8,
  "traffic_pos_id" : 8
}
```


Copyright © Huawei Technologies Co., Ltd.

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

4.4.3 Deleting the Default Anti-DDoS Policy Configured for Newly Purchased Public IP Addresses

Function

This API enables you to delete the default protection policy configured for newly purchased public IP addresses.

Debugging

You can use **API Explorer** to debug this API.

URI

DELETE /v1/{project_id}/antiddos/default-config

Table 4-62 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	poject id Minimum: **32** Maximum: **64**

Request Parameters

Table 4-63 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	token Minimum: **32** Maximum: **2097152**
Content-Type	Yes	String	Default: **application/json;charset=utf8**

Copyright © Huawei Technologies Co., Ltd.

Response Parameters

Status code: 200

Table 4-64 Response body parameters

Parameter	Type	Description
error_code	String	Internal error code
error_msg	String	Internal error description

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "error_code" : "10000000",
  "error_msg" : "Ok",
  "task_id" : ""
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

Copyright © Huawei Technologies Co., Ltd.

5 Application Examples of Cloud Native Anti-DDoS Basic APIs

5.1 Example 1: Updating Defense Policy for an IP Address

Scenario

You can modify the defense policy configured for an IP address on the Anti-DDoS console or by calling the API.

Process:

1. Query the defense statuses of all IP addresses.
2. Query the optional Anti-DDoS defense policies.
3. Update the defense policy for an IP address.
4. Query the execution status of the defense policy updating task based on the task ID returned in **3**.

Involved APIs

The following APIs are required for updating the Anti-DDoS defense policy for an IP address:

- **Step 1** is used for querying the defense statuses of all IP addresses.
- **Step 2** is used for querying the optional Anti-DDoS defense policies.
- **Step 3** is used for updating the defense policy for an IP address.
- **Step 4** is used for querying the execution status of the defense policy updating task based on the task ID.

Procedure

Step 1 Query the defense statuses of all IP addresses.

- API information

 Copyright © Huawei Technologies Co., Ltd.

URI format: **GET /v1/{*project_id*}/antiddos**

For details, see section "Querying the List of Defense Statuses of EIPs".

- Example request

  GET: https://*{endpoint}*/v1/1858a4e1f99d4454bd6a539d5477f5de/antiddos

  Obtain *{endpoint}* from **Regions and Endpoints**.

  Body:

```
{
}
```

- Example response

```
{
"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
}
]
}
```

Step 2 Query the optional Anti-DDoS defense policies.

- API information

  URI format: **GET /v2/{*project_id*}/antiddos/query-config-list**

  For details, see section "Querying Optional Anti-DDoS Defense Policies".

- Example request

  GET: https://*{endpoint}*/v2/1858a4e1f99d4454bd6a539d5477f5de/antiddos/query-config-list

  Obtain *{endpoint}* from **Regions and Endpoints**.

  Body:

```
{
}
```

- Example response

```
{
"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
},
{
"traffic_pos_id": 3,
"traffic_per_second": 50,
"packet_per_second": 10000
},
{
"traffic_pos_id": 4,
"traffic_per_second": 70,
"packet_per_second": 15000
```


Copyright © Huawei Technologies Co., Ltd.

```
},
{
"traffic_pos_id": 5,
"traffic_per_second": 100,
"packet_per_second": 20000
},
{
"traffic_pos_id": 6,
"traffic_per_second": 150,
"packet_per_second": 25000
},
{
"traffic_pos_id": 7,
"traffic_per_second": 200,
"packet_per_second": 35000
},
{
"traffic_pos_id": 8,
"traffic_per_second": 250,
"packet_per_second": 50000
},
{
"traffic_pos_id": 9,
"traffic_per_second": 300,
"packet_per_second": 70000
},
{
"traffic_pos_id": 88,
"traffic_per_second": 1000,
"packet_per_second": 300000
}
],
"http_limited_list": [
{
"http_request_pos_id": 1,
"http_packet_per_second": 100
},
{
"http_request_pos_id": 2,
"http_packet_per_second": 150
},
{
"http_request_pos_id": 3,
"http_packet_per_second": 240
},
{
"http_request_pos_id": 4,
"http_packet_per_second": 350
},
{
"http_request_pos_id": 5,
"http_packet_per_second": 480
},
{
"http_request_pos_id": 6,
"http_packet_per_second": 550
},
{
"http_request_pos_id": 7,
"http_packet_per_second": 700
},
{
"http_request_pos_id": 8,
"http_packet_per_second": 850
},
{
"http_request_pos_id": 9,
"http_packet_per_second": 1000
},
```


 Copyright © Huawei Technologies Co., Ltd.

```
{
"http_request_pos_id": 10,
"http_packet_per_second": 1500
},
{
"http_request_pos_id": 11,
"http_packet_per_second": 2000
},
{
"http_request_pos_id": 12,
"http_packet_per_second": 3000
},
{
"http_request_pos_id": 13,
"http_packet_per_second": 5000
},
{
"http_request_pos_id": 14,
"http_packet_per_second": 10000
},
{
"http_request_pos_id": 15,
"http_packet_per_second": 20000
}
],
"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
},
{
"cleaning_access_pos_id": 3,
"new_connection_limited": 30,
"total_connection_limited": 200
},
{
"cleaning_access_pos_id": 4,
"new_connection_limited": 40,
"total_connection_limited": 250
},
{
"cleaning_access_pos_id": 5,
"new_connection_limited": 50,
"total_connection_limited": 300
},
{
"cleaning_access_pos_id": 6,
"new_connection_limited": 60,
"total_connection_limited": 500
},
{
"cleaning_access_pos_id": 7,
"new_connection_limited": 70,
"total_connection_limited": 600
},
{
"cleaning_access_pos_id": 8,
"new_connection_limited": 80,
"total_connection_limited": 700
}
],
"extend_ddos_config": []
}
```


 Copyright © Huawei Technologies Co., Ltd.

Step 3 Update the defense policy for an IP address.

- API information

  URI format: **PUT /v1/{*project_id*}/antiddos/{floating_ip_id}**

  For details, see section "Updating Anti-DDoS Defense Policies".

- Example request

  PUT: https://*{endpoint}*/v1/1858a4e1f99d4454bd6a539d5477f5de/antiddos/18e6ace5-eb36-4196-a15e-1e000c24e026

  Obtain *{endpoint}* from **Regions and Endpoints**.

  Body:

  ```
  {
  "app_type_id": 1,
  "cleaning_access_pos_id": 8,
  "enable_L7": false,
  "http_request_pos_id": 8,
  "traffic_pos_id": 8
  }
  ```

- Example response

  ```
  {
  "error_code": "10000000",
  "error_msg": "The task has been received and is being handled",
  "task_id": "59385d2a-6266-4d3a-9122-a228c530f557"
  }
  ```

Step 4 Query the execution status of the defense policy updating task based on the task ID returned in **Step 3**.

- API information

  URI format: **GET /v2/{*project_id*}/query-task-status**

  For details, see section "Querying Anti-DDoS Tasks".

- Example request

  GET: https://*{endpoint}*/v2/1858a4e1f99d4454bd6a539d5477f5de/query-task-status?task_id=59385d2a-6266-4d3a-9122-a228c530f557

  Obtain *{endpoint}* from **Regions and Endpoints**.

  Body:

  ```
  {
  }
  ```

- Example response

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

----End

5.2 Example 2: Configuring the Default Protection Policy

Scenario

You can configure the default protection policy for newly purchased IP addresses on the Anti-DDoS console or by call the API.

Copyright © Huawei Technologies Co., Ltd.

Process:

1. Query the default protection settings for the newly purchased IP addresses.
2. Configure the default protection policy for newly purchased IP addresses.

Involved APIs

The following APIs are required for configuring default protection policy for newly purchased IP addresses.

- **Step 1** is used to query default protection settings for the newly purchased IP addresses.
- **Step 2** is used to configure default protection policy for newly purchased IP addresses.

Procedure

Step 1 Query default protection settings for the newly purchased IP addresses.

- API information

  URI format: **GET /v1/{*project_id*}/antiddos/default-config**

  For details, see section "Querying the Default Protection Policy Configured for the Newly Purchased Public IP Addresses".

- Example request

  GET: https://*{endpoint}*/v1/1858a4e1f99d4454bd6a539d5477f5de/antiddos/default/config

  Obtain *{endpoint}* from **Regions and Endpoints**.

  Body:

  ```
  {
  }
  ```

- Example response

  ```
  {
  "app_type_id": 1,
  "cleaning_access_pos_id": 8,
  "enable_L7": false,
  "http_request_pos_id": 8,
  "traffic_pos_id": 8
  }
  ```

Step 2 Configure default protection policy for newly purchased IP addresses.

- API information

  URI format: **POST /v1/{*project_id*}/antiddos/default-config**

  For details, see section "Configuring the Default Protection Policy for Newly Purchased Public IP Addresses".

- Example request

  POST: https://*{endpoint}*/v1/1858a4e1f99d4454bd6a539d5477f5de/antiddos/default-config

  Obtain *{endpoint}* from **Regions and Endpoints**.

  Body:

  ```
  {
  "app_type_id": 1,
  "cleaning_access_pos_id": 8,
  "enable_L7": false,
  ```

 Copyright © Huawei Technologies Co., Ltd.

```
"http_request_pos_id": 8,
"traffic_pos_id": 8
}
```

- Example response

```
{
}
```

----End

 Copyright © Huawei Technologies Co., Ltd.

A Appendix

A.1 HTTP Status Codes of Cloud Native Anti-DDoS Basic

- Normal

Returned Value	Description
200	The request is successfully processed.

- Abnormal

Status Code	Status	Description
400	Bad Request	The server fails to process the request.
401	Unauthorized	The requested page requires a username and a password.
403	Forbidden	Access to the requested page is denied.
404	Not Found	The server fails to find the requested page.
405	Method Not Allowed	Method specified in the request is not allowed.
406	Not Acceptable	Response generated by the server is not acceptable to the client.
407	Proxy Authentication Required	Proxy authentication is required before the request is processed.
408	Request Timeout	A timeout error occurs because the request is not processed within the specified waiting period of the server.

 Copyright © Huawei Technologies Co., Ltd.

Status Code	Status	Description
409	Conflict	The request cannot be processed due to a conflict.
500	Internal Server Error	The request is not processed due to a server error.
501	Not Implemented	The request is not processed because the server does not support the requested function.
502	Bad Gateway	The request is not processed, and the server receives an invalid response from the upstream server.
503	Service Unavailable	The request is not processed due to a temporary system abnormality.
504	Gateway Timeout	A gateway timeout error occurs.

A.2 Error Codes

For more service error codes, see **API Error Center**.

Status Code	Error Codes	Error Message	Description	Solution
200	Anti-DDoS.0	Succeeded	Succeeded	No need to deal with it
200	Anti-DDoS.10000000	The task has been received and is being handled	The task has been received and is being handled	No need to deal with it
400	Anti-DDoS.10000001	Enter a valid request message	Enter a valid request message	Check the parameters
400	Anti-DDoS.10001008	An incorrect task ID is used	An incorrect task ID is used	Check the parameters
400	Anti-DDoS.10001010	Invalid time	Invalid time	Check the parameters
401	Anti-DDoS.10000004	Public test service denied	Public test service denied	Apply for public test

Copyright © Huawei Technologies Co., Ltd.

Status Code	Error Codes	Error Message	Description	Solution
403	Anti-DDoS.10000002	Failed to authenticate the token in the request	Failed to authenticate the token in the request	Re apply for token
403	Anti-DDoS.10000009	The account is restricted	The account is restricted	Apply for authority
403	Anti-DDoS.10000010	The account is frozen	The account is frozen	Apply for unfreeze
403	Anti-DDoS.10000012	Unknown user type	Unknown user type	Apply for authority
403	Anti-DDoS.10000016	VPC access failed or EIP is not exist	VPC access failed or EIP is not exist	Contact to administrator
403	Anti-DDoS.10000030	You have not been authenticated. Perform real-name authentication first.	You have not been authenticated. Perform real-name authentication first.	Real name authentication
403	Anti-DDoS.10001009	The operation permission is restricted	The operation permission is restricted	Apply for authority
403	Anti-DDoS.11000001	Access to the database is rejected	Access to the database is rejected	Contact to administrator
500	Anti-DDoS.11000000	Internal system exception. Contact technical support engineers	Internal system exception. Contact technical support engineers	Contact to administrator

A.3 Obtaining a Project ID

Obtaining a Project ID by Calling an API

You can obtain the project ID by calling the API used to **query project information based on the specified criteria**.

Copyright © Huawei Technologies Co., Ltd.

The API used to obtain a project ID is GET https://{Endpoint}/v3/projects. **{Endpoint}** is the IAM endpoint and can be obtained from **Regions and Endpoints**. For details about API authentication, see **Authentication**.

In the following example, **id** indicates the project ID.

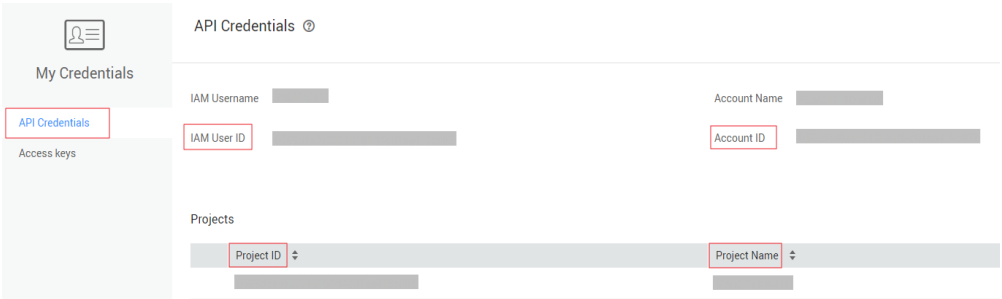
```
{
    "projects": [
        {
            "domain_id": "65382450e8f64ac0870cd180d14e684b",
            "is_domain": false,
            "parent_id": "65382450e8f64ac0870cd180d14e684b",
            "name": "xxxxxxxx",
            "description": "",
            "links": {
                "next": null,
                "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"
    }
}
```

Obtaining a Project ID from the Console

A project ID is required for some URLs when an API is called. To obtain a project ID, perform the following operations:

1. Log in to the management console.
2. Click the username and choose **Basic Information** from the drop-down list.
3. On the **Account Info** page, click **Manage** next to **Security Credentials**.
   On the **API Credentials** page, view project IDs in the project list.

Figure A-1 Viewing project IDs



 Copyright © Huawei Technologies Co., Ltd.

B Historical APIs of Cloud Native Anti-DDoS Basic

B.1 Querying Optional Anti-DDoS Defense Policies

NOTE

This API is a historical API and may not be maintained in the future. Please use the API in section "Querying Optional Anti-DDoS Defense Policies".

Functions

This API allows you to query optional Anti-DDoS defense policies. Based on your service, you can select a policy for Anti-DDoS traffic cleaning.

URI

- URI format

  GET /v1/{project_id}/antiddos/query_config_list

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID

Request

Example request

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

Response

- Parameter description

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
traffic_limited_list	Yes	List data structure	List of traffic limits
http_limited_list	Yes	List data structure	List of HTTP limits
connection_limited_list	Yes	List data structure	List of limits of numbers of connections

- Data structure description of **traffic_limited_list**

Parameter	Mandatory	Type	Description
traffic_pos_id	Yes	Integer	Position ID of traffic
traffic_per_second	Yes	Integer	Threshold of traffic per second (Mbit/s)
packet_per_second	Yes	Integer	Threshold of number of packets per second

- Data structure description of **http_limited_list**

Parameter	Mandatory	Type	Description
http_request_pos_id	Yes	Integer	Position ID of number of HTTP requests
http_packet_per_second	Yes	Integer	Threshold of number of HTTP requests per second

- Data structure description of **connection_limited_list**

Parameter	Mandatory	Type	Description
cleaning_access_pos_id	Yes	Integer	Position ID of access limit during cleaning
new_connection_limited	Yes	Integer	Number of new connections of a source IP address
total_connection_limited	Yes	Integer	Total number of connections of a source IP address

- Example response

```
{
  "traffic_limited_list": [
```

 Copyright © Huawei Technologies Co., Ltd.

```
  {
    "traffic_pos_id": 1,
    "traffic_per_second": 10,
    "packet_per_second": 2000
  },
  {
    "traffic_pos_id": 2,
    "traffic_per_second": 30,
    "packet_per_second": 6000
  },
  {
    "traffic_pos_id": 3,
    "traffic_per_second": 50,
    "packet_per_second": 10000
  },
  {
    "traffic_pos_id": 4,
    "traffic_per_second": 70,
    "packet_per_second": 15000
  },
  {
    "traffic_pos_id": 5,
    "traffic_per_second": 100,
    "packet_per_second": 20000
  },
  {
    "traffic_pos_id": 6,
    "traffic_per_second": 150,
    "packet_per_second": 25000
  },
  {
    "traffic_pos_id": 7,
    "traffic_per_second": 200,
    "packet_per_second": 35000
  },
  {
    "traffic_pos_id": 8,
    "traffic_per_second": 250,
    "packet_per_second": 50000
  },
  {
    "traffic_pos_id": 9,
    "traffic_per_second": 300,
    "packet_per_second": 70000
  }
 ],
 "http_limited_list": [
  {
    "http_request_pos_id": 1,
    "http_packet_per_second": 100
  },
  {
    "http_request_pos_id": 2,
    "http_packet_per_second": 150
  },
  {
    "http_request_pos_id": 3,
    "http_packet_per_second": 240
  },
  {
    "http_request_pos_id": 4,
    "http_packet_per_second": 350
  },
  {
    "http_request_pos_id": 5,
    "http_packet_per_second": 480
  },
  {
    "http_request_pos_id": 6,
```


 Copyright © Huawei Technologies Co., Ltd.

```
    "http_packet_per_second": 550
  },
  {
    "http_request_pos_id": 7,
    "http_packet_per_second": 700
  },
  {
    "http_request_pos_id": 8,
    "http_packet_per_second": 850
  },
  {
    "http_request_pos_id": 9,
    "http_packet_per_second": 1000
  },
  {
    "http_request_pos_id": 10,
    "http_packet_per_second": 1500
  },
  {
    "http_request_pos_id": 11,
    "http_packet_per_second": 2000
  },
  {
    "http_request_pos_id": 12,
    "http_packet_per_second": 3000
  },
  {
    "http_request_pos_id": 13,
    "http_packet_per_second": 5000
  },
  {
    "http_request_pos_id": 14,
    "http_packet_per_second": 10000
  },
  {
    "http_request_pos_id": 15,
    "http_packet_per_second": 20000
  }
],
"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
  },
  {
    "cleaning_access_pos_id": 3,
    "new_connection_limited": 30,
    "total_connection_limited": 200
  },
  {
    "cleaning_access_pos_id": 4,
    "new_connection_limited": 40,
    "total_connection_limited": 250
  },
  {
    "cleaning_access_pos_id": 5,
    "new_connection_limited": 50,
    "total_connection_limited": 300
  },
  {
    "cleaning_access_pos_id": 6,
    "new_connection_limited": 60,
    "total_connection_limited": 500
```


 Copyright © Huawei Technologies Co., Ltd.

```
  },
  {
    "cleaning_access_pos_id": 7,
    "new_connection_limited": 70,
    "total_connection_limited": 600
  },
  {
    "cleaning_access_pos_id": 8,
    "new_connection_limited": 80,
    "total_connection_limited": 700
  }
 ],
 "extend_ddos_config": [
  {
    "new_connection_limited": 80,
    "total_connection_limited": 700,
    "http_packet_per_second": 500000,
    "traffic_per_second": 1000,
    "packet_per_second": 200000,
    "setID": 33
  },
  {
    "new_connection_limited": 80,
    "total_connection_limited": 700,
    "http_packet_per_second": 500000,
    "traffic_per_second": 2000,
    "packet_per_second": 200000,
    "setID": 34
  },
  {
    "new_connection_limited": 80,
    "total_connection_limited": 700,
    "http_packet_per_second": 500000,
    "traffic_per_second": 5000,
    "packet_per_second": 400000,
    "setID": 35
  },
  {
    "new_connection_limited": 80,
    "total_connection_limited": 700,
    "http_packet_per_second": 0,
    "traffic_per_second": 0,
    "packet_per_second": 0,
    "setID": 36
  }
 ]
}
```


NOTE

The **extend_ddos_config** field displays information about Anti-DDoS defense policies set by users based on their needs.

Status Code

For details, see **HTTP Status Codes of Cloud Native Anti-DDoS Basic**.

B.2 Querying Anti-DDoS Tasks

NOTE

This API is a historical API and may not be maintained in the future. Please use the API in section "Querying Anti-DDoS Tasks".

 Copyright © Huawei Technologies Co., Ltd.

Functions

This API enables you to query the execution status of a specified Anti-DDoS configuration task.

URI

- URI format

  GET /v1/{project_id}/query_task_status

  NOTE

  You can use **?** and **&** behind the URI to add query conditions, as shown in the request example.

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	User ID

Request

- Parameter description

Parameter	Mandatory	Type	Description
task_id	Yes	String	Task ID (non-negative integer) character string

- Example request

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

Response

- Parameter description

Name	Type	Description
task_status	String	Status of a task, which can be one of the following: • success • failed • waiting • running • preprocess • ready
task_msg	String	Additional information about a task

- Example response

 Copyright © Huawei Technologies Co., Ltd.

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

Status Code

For details, see **HTTP Status Codes of Cloud Native Anti-DDoS Basic**.

 Copyright © Huawei Technologies Co., Ltd.

C Change History

Release Date	Description
2021-04-19	This issue is the second official release. Modified the section title.
2020-12-31	This issue is the first official release.

 Copyright © Huawei Technologies Co., Ltd.