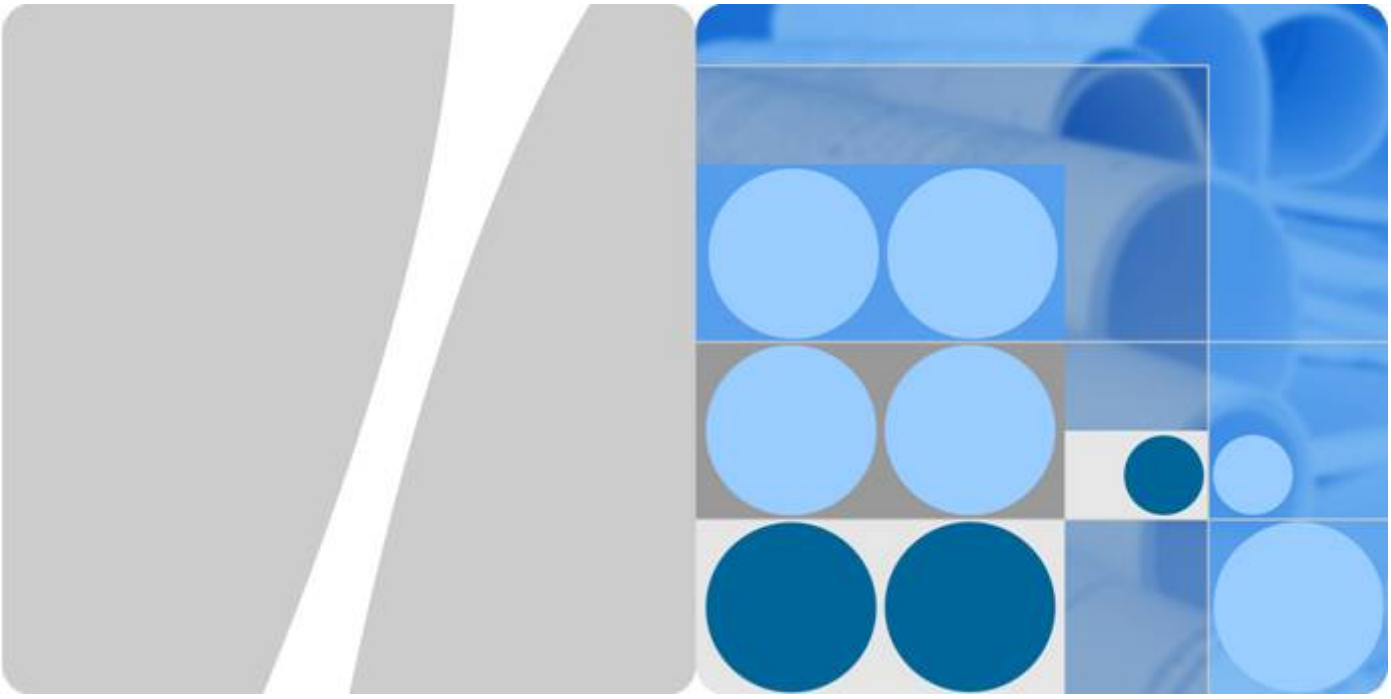


Anti-DDoS

API Reference

Issue 05

Date 2019-11-28

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Copyright © Huawei Technologies Co., Ltd. 2019. 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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://e.huawei.com

Contents

1 Before You Start....1

2 API Overview....2

3 Calling APIs....4

3.1 Making an API Request....4

3.2 Authentication....6

4 Calling APIs....8

4.1 Making an API Request....8

4.2 Examples....10

5 APIs of Anti-DDoS....12

5.1 Querying Optional Anti-DDoS Defense Policies....12

5.2 Enabling Anti-DDoS....16

5.3 Disabling Anti-DDoS....18

5.4 Querying Configured Anti-DDoS Defense Policies....19

5.5 Updating Anti-DDoS Defense Policies....20

5.6 Querying Anti-DDoS Tasks....22

5.7 Querying the List of Defense Statuses of EIPs....23

5.8 Querying the Defense Status of a Specified EIP....26

5.9 Querying the Traffic of a Specified EIP....27

5.10 Querying Events of a Specified EIP....28

5.11 Querying Weekly Defense Statistics....30

6 Querying the Alarm Configuration....34

6.1 Querying Alarm Configuration....34

7 Common Parameters....36

7.1 Error Codes....36

A Appendix....38

A.1 Common Returned Values....38

A.2 Obtaining a Project ID....39

B Change History....40

 Copyright © Huawei Technologies Co., Ltd.

1 Before You Start

This document describes the application programming interfaces (APIs) of Anti-DDoS and their syntax, parameters, and examples. You can search for information you need according to **Table 1-1**.

Table 1-1 Document overview

Chapter	Description
API Overview	Learning about the list of Anti-DDoS APIs
Preparing the Environment	Preparations before using the APIs
Using APIs	Representational State Transfer (REST) message bodies, calling methods, and examples
APIs of Anti-DDoS Querying the Alarm Configuration	API calling description
Common Parameters	Common parameters

 Copyright © Huawei Technologies Co., Ltd.

2 API Overview

The following table describes the APIs provided by Anti-DDoS.

Table 2-1 APIs

API	Description
Querying Optional Anti-DDoS Defense Policies	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.
Enabling Anti-DDoS	This asynchronous API allows you to enable the Anti-DDoS traffic cleaning defense.
Disabling Anti-DDoS	This asynchronous API allows you to disable the Anti-DDoS traffic cleaning defense.
Querying Configured Anti-DDoS Defense Policies	This API enables you to query configured Anti-DDoS defense policies. You can query the policy of a specified EIP.
Updating Anti-DDoS Defense Policies	This API enables you to update the Anti-DDoS defense policy of a specified EIP.
Querying Anti-DDoS Tasks	This API enables you to query the execution status of a specified Anti-DDoS configuration task.
Querying the List of Defense Statuses of EIPs	This API enables you to query the defense statuses of all EIPs, regardless whether an EIP has been bound to an Elastic Cloud Server (ECS) or not.
Querying the Defense Status of a Specified EIP	This API allows you to query the defense status of a specified EIP.
Querying the Traffic of a Specified EIP	This API allows you to query the traffic of a specified EIP in the last 24 hours. Traffic is detected in five-minute intervals.
Querying Events of a Specified EIP	This API allows you to query events of a specified EIP in the last 24 hours. Events include cleaning and black hole events, and the query delay is within five minutes.

 Copyright © Huawei Technologies Co., Ltd.

API	Description
Querying Weekly Defense Statistics	This API allows you to query weekly defense statistics about all your EIPs, including the number of intercepted DDoS attacks, number of attacks, and ranking by the number of attacks.
Querying Alarm Configuration	This API allows you to query alarm configuration, such as whether a certain type of alarms will be received, and whether alarms are received through SMS messages or emails.

Copyright © Huawei Technologies Co., Ltd.

3 Calling APIs

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 the administrator**Regions and Endpoints**.

- **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.

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.

 Copyright © Huawei Technologies Co., Ltd.

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, and the request is as follows:

```
POST https://{{endpoint}}/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.

  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://{{endpoint}}/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.

 Copyright © Huawei Technologies Co., Ltd.

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. Replace ***username***, ***domainname***, ******** (login password), and ***xxxxxxxxxxxxxxxxx*** (project name, for example, eu-west-0) with the actual values. Obtain a project name from the administratorthe **Region** field in **Regions and Endpoints**.

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://{{endpoint}}/v3/auth/tokens
Content-Type: application/json

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

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.

Copyright © Huawei Technologies Co., Ltd.

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.

In **Making an API Request**, the process of calling the API used to obtain a user token is described. 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:

```
POST https://{{endpoint}}/v3/auth/projects
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.

Copyright © Huawei Technologies Co., Ltd.

4 Calling APIs

4.1 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 the administrator**Regions and Endpoints**.

- **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.

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.

 Copyright © Huawei Technologies Co., Ltd.

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://{{endpoint}}/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.

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://{{endpoint}}/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. Replace ***username***, ***domainname***, ******** (login password), and ***xxxxxxxxxxxxxxxxx*** (project name) with the actual values. Obtain a project name, from the administrator**Regions and Endpoints**.

For details about how to obtain the project ID, see **Obtaining a Project ID**.

 Copyright © Huawei Technologies Co., Ltd.

> **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://{{endpoint}}/v3/auth/tokens
Content-Type: application/json

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

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.

4.2 Examples

This section uses updating Anti-DDoS defense policies as an example to show how to use the Anti-DDoS APIs. Updating the Anti-DDoS defense policies involves two steps.

1. Use the token authentication to obtain the user token, which will be put into the request header for authentication in a subsequent request.
2. Call the API for updating Anti-DDoS defense policies.

Prerequisites

- You have obtained the project ID. For details, see **Obtaining a Project ID**.
- You have obtained the endpoints of IAM and Anti-DDoS. For details, see **Regions and Endpoints**.
- You have obtained the ID of the EIP to be updated.

Updating Anti-DDoS Defense Policies

The following values are merely examples and you need to replace them based on actual situations:

Copyright © Huawei Technologies Co., Ltd.

- IAM endpoint: **iam_endpoint**
- Anti-DDoS endpoint: **antiddos_endpoint**
- Project ID: **67641fe6886f43fcb78edbbf0ad0b99f**
- EIP ID: **ee0c854e-082f-499e-b7d8-1b42c22781af**

You need to perform the following steps to update Anti-DDoS defense policies.

1. Before calling other APIs, obtain the token and set it as an environment variable.

```
curl -H "Content-Type:application/json" https://{iam_endpoint}/v3/auth/tokens
-X POST -d '{     "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "testname",
                    "domain": {
                        "name": "testname"
                    },
                    "password": "Password"
                }
            }
        },
        "scope": {
            "project": {
                "name": "cn-north-1"
            }
        }
    }
}' -v -k
```

   In the response header, the value of **X-Subject-Token** is **token**.

```
X-Subject-
Token:MIIDkgYJKoZIhvcNAQcCoIIDgzCCA38CAQExDTALBglghkgBZQMEAgEwgXXXXX...
```

   Run the following command to set the token as an environment variable for future use:

```
export Token={X-Subject-Token}
```

   X-Subject-Token is the token obtained in the preceding step.

```
export X-Auth-
Token=MIIDkgYJKoZIhvcNAQcCoIIDgzCCA38CAQExDTALBglghkgBZQMEAgEwgXXXXX...
```

2. Call the API for updating Anti-DDoS defense policies.

```
curl -X POST -H 'Content-Type:application/json;charset=utf-8' -H "X-Auth-
Token:$Token" -d '{
    "enable_L7":false,
    "traffic_pos_id":2,
    "http_request_pos_id":1,
    "cleaning_access_pos_id":1,
    "app_type_id":1
}' https://{antiddos_endpoint}/v1/67641fe6886f43fcb78edbbf0ad0b99f/antiddos/
ee0c854e-082f-499e-b7d8-1b42c22781af -v -k
```

   If status code **200** is returned, the job is successfully created.

 Copyright © Huawei Technologies Co., Ltd.

5 APIs of Anti-DDoS

5.1 Querying Optional Anti-DDoS Defense Policies

Function

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	A user's ID

Request

- Request example

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

Response

- Element description

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

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
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

- Response example

```
{
  "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
    },
    {
```

 Copyright © Huawei Technologies Co., Ltd.

```
      "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,
      "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
    },
    {
```


 Copyright © Huawei Technologies Co., Ltd.

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


 Copyright © Huawei Technologies Co., Ltd.

```
  ],
  "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.

Returned Value

See **Common Returned Values**.

5.2 Enabling Anti-DDoS

Function

This asynchronous API allows you to enable the Anti-DDoS traffic cleaning defense. Successfully invoking this API only means that the service node has received the enabling request. You need to use the task querying API to check the task execution status. For details about the task querying API, see **Querying Anti-DDoS Tasks**.

URI

- URI format

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

- Parameter description

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
project_id	Yes	String	A user's ID
floating_ip_id	Yes	String	ID corresponding to the EIP of a user

Request

- Parameter description

Parameter	Mandatory	Type	Description
enable_L7	No	Boolean	Whether to enable L7 defense
traffic_pos_id	Yes	Integer	Position ID of traffic. The value ranges from 1 to 9.
http_request_pos_id	Yes	Integer	Position ID of number of HTTP requests. The value ranges from 1 to 15.
cleaning_access_pos_id	Yes	Integer	Position ID of access limit during cleaning. The value ranges from 1 to 8.
app_type_id	No	Integer	Application type ID. Possible values: ● 0 ● 1

- Request example

```
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
}
```

Response

- Element description

Name	Type	Description
error_code	String	Internal error code
error_description	String	Internal error description

 Copyright © Huawei Technologies Co., Ltd.

Name	Type	Description
task_id	String	ID of a task. This ID can be used to query the status of the task. This field is reserved for use in task auditing later. It is temporarily unused.

- Response example

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

Returned Value

See **Common Returned Values**.

5.3 Disabling Anti-DDoS

Function

This asynchronous API allows you to disable the Anti-DDoS traffic cleaning defense. Successfully invoking this API only means that the service node has received the disabling request. You need to use the task querying API to check the task execution status. For details about the task querying API, see **Querying Anti-DDoS Tasks**.

URI

- URI format

  DELETE /v1/{project_id}/antiddos/{floating_ip_id}

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	A user's ID
floating_ip_id	Yes	String	ID corresponding to the EIP of a user

Request

- Request example

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

Response

- Element description

 Copyright © Huawei Technologies Co., Ltd.

Name	Type	Description
error_code	String	Internal error code
error_description	String	Internal error description
task_id	String	ID of a task. This ID can be used to query the status of the task. This field is reserved for use in task auditing later. It is temporarily unused.

- Response example

```
{
   "error_code": "10000000",
   "error_description": "Task has been received and is being processed.",
   "task_id": "d90dc577-abd2-4be0-b2cf-cb8f5f67ddb0"
}
```

Returned Value

See **Common Returned Values**.

5.4 Querying Configured Anti-DDoS Defense Policies

Function

This API enables you to query configured Anti-DDoS defense policies. You can query the policy of a specified EIP.

URI

- URI format

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

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	A user's ID
floating_ip_id	Yes	String	ID corresponding to the EIP of a user

Request

- Request example

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

Response

- Element description

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
enable_L7	Yes	Boolean	Whether L7 defense has been enabled
traffic_pos_id	Yes	Integer	Position ID of traffic. The value ranges from 1 to 9.
http_request_pos_id	Yes	Integer	Position ID of number of HTTP requests. The value ranges from 1 to 15.
cleaning_access_pos_id	Yes	Integer	Position ID of access limit during cleaning. The value ranges from 1 to 8.
app_type_id	Yes	Integer	Application type ID. Possible values: ● 0 ● 1

- Response example

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

Returned Value

See **Common Returned Values**.

5.5 Updating Anti-DDoS Defense Policies

Function

This API enables you to update the Anti-DDoS defense policy of a specified EIP. Successfully invoking this API only means that the service node has received the update request. You need to use the task querying API to check the task execution status. For details about the task querying API, see **Querying Anti-DDoS Tasks**.

URI

- URI format

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

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	A user's ID

Copyright © Huawei Technologies Co., Ltd.

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

Request

- Parameter description

Parameter	Mandatory	Type	Description
enable_L7	No	Boolean	Whether to enable L7 defense
traffic_pos_id	Yes	Integer	Position ID of traffic. The value ranges from 1 to 9.
http_request_pos_id	Yes	Integer	Position ID of number of HTTP requests. The value ranges from 1 to 15.
cleaning_access_pos_id	Yes	Integer	Position ID of access limit during cleaning. The value ranges from 1 to 8.
app_type_id	No	Integer	Application type ID. Possible values: ● 0 ● 1

- Request example

```
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
}
```

Response

- Element description

Name	Type	Description
error_code	String	Internal error code
error_description	String	Internal error description
task_id	String	ID of a task. This ID can be used to query the status of the task. This field is reserved for use in task auditing later. It is temporarily unused.

 Copyright © Huawei Technologies Co., Ltd.

- Response example

```
{
   "error_code": "10000000",
   "error_description": "Task has been received and is being processed.",
   "task_id": "4a4fefe7-34a1-40e2-a87c-16932af3ac4a"
}
```

Returned Value

See **Common Returned Values**.

5.6 Querying Anti-DDoS Tasks

Function

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	A user's ID

Request

- Parameter description

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

- Request example

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

Response

- Element description

 Copyright © Huawei Technologies Co., Ltd.

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

- Response example

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

Returned Value

See **Common Returned Values**.

5.7 Querying the List of Defense Statuses of EIPs

Function

This API enables you to query the defense statuses of all EIPs, regardless whether an EIP has been bound to an Elastic Cloud Server (ECS) or not.

URI

- URI format

  GET /v1/{project_id}/antiddos

  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	A user's ID

Request

- Parameter description

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
status	No	String	Possible values: ● **normal**: indicates that the defense status is normal. ● **configging**: indicates that defense is being configured. ● **notConfig**: indicates that defense is not configured. ● **packetcleaning**: indicates that traffic cleaning is underway. ● **packetdropping**: indicates that traffic is discarded. If this parameter is not used, the defense statuses of all ECSs are displayed in the Neutron-queried order by default.
limit	No	Integer	Maximum number of returned results. The value ranges from 1 to 100.
offset	No	Integer	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.

- Request example

```
GET /v1/67641fe6886f43fcb78edbbf0ad0b99f/antiddos?
status=packetdropping
```

Response

- Element description

Name	Type	Description
total	Integer	Total number of EIPs
ddosStatus	List data structure	List of defense statuses

- Data structure description of **ddosStatus**

Parameter	Mandatory	Type	Description
floating_ip_address	Yes	String	Floating IP address
floating_ip_id	Yes	String	ID of an EIP

Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
network_type	Yes	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	Yes	String	Defense status, the possible value of which is one of the following: ● **normal**: indicates that the defense status is normal. ● **configging**: indicates that defense is being configured. ● **notConfig**: indicates that defense is not configured. ● **packetcleaning**: indicates that traffic cleaning is underway. ● **packetdropping**: indicates that traffic is discarded.

- Response example

```
{
   "total": 5,
   "ddosStatus": [
      {
         "floating_ip_id": "1867f954-fc11-4202-8247-6af2144867ea",
         "floating_ip_address": "192.168.42.221",
         "network_type": "EIP",
         "status": "notConfig"
      },
      {
         "floating_ip_id": "49c6af49-9ace-42e6-ab89-1eee1f4ac821",
         "floating_ip_address": "192.168.35.152",
         "network_type": "EIP",
         "status": "normal"
      },
      {
         "floating_ip_id": "7a8dc957-083b-499d-b7cf-6fa48f4880c5",
         "floating_ip_address": "192.168.42.222",
         "network_type": "EIP",
         "status": "notConfig"
      },
      {
         "floating_ip_id": "7c6676a0-b281-4163-9d0d-cb6485ae9860",
         "floating_ip_address": "192.168.44.69",
         "network_type": "EIP",
         "status": "normal"
      },
      {
         "floating_ip_id": "969c1d48-6a92-4ef1-b66c-b17c7e7d7ce7",
         "floating_ip_address": "192.168.47.192",
         "network_type": "EIP",
         "status": "notConfig"
      }
   ]
}
```

 Copyright © Huawei Technologies Co., Ltd.

Returned Value

See **Common Returned Values**.

5.8 Querying the Defense Status of a Specified EIP

Function

This API allows you to query the defense status of a specified EIP.

URI

- URI format

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

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	A user's ID
floating_ip_id	Yes	String	ID corresponding to the EIP of a user

Request

- Request example

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

Response

- Element description

Parameter	Mandatory	Type	Description
status	Yes	String	Defense status, the possible value of which is one of the following: ● **normal**: indicates that the defense status is normal. ● **configging**: indicates that defense is being configured. ● **notConfig**: indicates that defense is not configured. ● **packetcleaning**: indicates that traffic cleaning is underway. ● **packetdropping**: indicates that traffic is discarded.

- Response example

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


Copyright © Huawei Technologies Co., Ltd.

Returned Value

See **Common Returned Values**.

5.9 Querying the Traffic of a Specified EIP

Function

This API allows you to query the traffic of a specified EIP in the last 24 hours. Traffic is detected in five-minute intervals.

URI

- URI format

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

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	A user's ID
floating_ip_id	Yes	String	ID corresponding to the EIP of a user

Request

- Request example

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

Response

- Element description

Name	Type	Description
data	Data structure	Traffic in the last 24 hours

- Data structure description of **data**

Parameter	Mandatory	Type	Description
period_start	Yes	Long integer	Start time
bps_in	Yes	Integer	Ingress traffic (bit/s)
bps_attack	Yes	Integer	Attack traffic (bit/s)
total_bps	Yes	Integer	Total traffic

Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
pps_in	Yes	Integer	Inbound packet rate (number of packets per second)
pps_attack	Yes	Integer	Attack packet rate (number of packets per second)
total_pps	Yes	Integer	Total packet rate

- Response example

```
{"data": [
      {
      "period_start": 1472713370609,
      "bps_in": 0,
      "bps_attack": 0,
      "total_bps": 0,
      "pps_in": 0,
      "pps_attack": 0,
      "total_pps": 0
   },


   ...


      {
      "period_start": 1472713670609,
      "bps_in": 0,
      "bps_attack": 0,
      "total_bps": 0,
      "pps_in": 0,
      "pps_attack": 0,
      "total_pps": 0
   }]
}
```

Returned Value

See **Common Returned Values**.

5.10 Querying Events of a Specified EIP

Function

This API allows you to query events of a specified EIP in the last 24 hours. Events include cleaning and black hole events, and the query delay is within five minutes.

URI

- URI format

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

  NOTE

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

- Parameter description

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Mandatory	Type	Description
project_id	Yes	String	A user's ID
floating_ip_id	Yes	String	ID corresponding to the EIP of a user

Request

- Parameter description

Parameter	Mandatory	Type	Description
limit	No	Integer	Limit of number of returned results or the maximum number of returned results of a query. The value ranges from 1 to 100, and this parameter is used together with the **offset** parameter. If neither **limit** nor **offset** is used, query results of all ECSs are returned.
offset	No	Integer	Offset. This parameter is valid only when used together with the **limit** parameter.
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. The default value is **desc**.

- Request example

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

Response

- Element description

Name	Type	Description
total	Integer	Total number of EIPs
logs	Data structure	List of events

 Copyright © Huawei Technologies Co., Ltd.

- Data structure description of **logs**

Parameter	Mandatory	Type	Description
start_time	Yes	Long integer	Start time
end_time	Yes	Long integer	End time
status	Yes	Integer	Defense status, the possible value of which is one of the following: ● **1**: indicates that traffic cleaning is underway. ● **2**: indicates that traffic is discarded.
trigger_bps	Yes	Integer	Traffic at the triggering point
trigger_pps	Yes	Integer	Packet rate at the triggering point
trigger_http_pps	Yes	Integer	HTTP request rate at the triggering point

- Response example

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

Returned Value

See **Common Returned Values**.

5.11 Querying Weekly Defense Statistics

Function

This API allows you to query weekly defense statistics about all your EIPs, including the number of intercepted DDoS attacks, number of attacks, and ranking by the number of attacks. Currently, you can query weekly statistics up to four weeks before the current time. Data older than four weeks cannot be queried.

URI

- URI format

  GET /v1/{project_id}/antiddos/weekly

Copyright © Huawei Technologies Co., Ltd.

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	A user's ID

Request

- Parameter description

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

- Request example

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

Response

- Element description

Name	Type	Description
ddos_intercept_times	Integer	Number of DDoS attacks intercepted in a week
weekdata	Data structure	Number of attacks in a week
top10	Data structure	Top 10 attacked IP addresses

- Data structure description of **weekdata**

Parameter	Mandatory	Type	Description
ddos_intercept_times	Yes	Integer	Number of DDoS attacks intercepted
ddos_blackhole_times	Yes	Integer	Number of DDoS black holes
max_attack_bps	Yes	Integer	Maximum attack traffic
max_attack_conns	Yes	Integer	Maximum number of attack connections
period_start_date	Yes	Long integer	Start time

- Data structure description of **top10**

Copyright © Huawei Technologies Co., Ltd.

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

- Response example

```
{
   "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
```

 Copyright © Huawei Technologies Co., Ltd.

```
        }
    ]
}
```

Returned Value

See **Common Returned Values**.

 Copyright © Huawei Technologies Co., Ltd.

6 Querying the Alarm Configuration

6.1 Querying Alarm Configuration

Function

This API allows you to query alarm configuration, such as whether a certain type of alarms will be received, and whether alarms are received through SMS messages or emails.

URI

- URI format

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

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	A user's ID

Request

- Request example

```
GET /v2/67641fe6886f43fcb78edbbf0ad0b99f/warnalert/alertconfig/query
```

Response

- Element description

Parameter	Mandatory	Type	Description
warn_config	Yes	List data structure	Alarm configuration
topic_urn	Yes	String	ID of an alarm group
display_name	Yes	String	Description of an alarm group

 Copyright © Huawei Technologies Co., Ltd.

- Data structure description of **warn_config**

Parameter	Mandatory	Type	Description
antiDDoS	Yes	Boolean	DDoS attacks
bruce_force	No	Boolean	Brute force cracking (system logins, FTP, and DB)
remote_login	No	Boolean	Alarms about remote logins
weak_password	No	Boolean	Weak passwords (system and database)
high_privilege	No	Boolean	Overly high rights of a database process
back_doors	No	Boolean	Web page backdoors
waf	No	Boolean	Reserved

- Response example

```
{
   "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"
}
```

NOTE

SFTP is more secure than FTP. To secure data transmission, use SFTP to transfer files.

Returned Value

See **Common Returned Values**.

 Copyright © Huawei Technologies Co., Ltd.

7 Common Parameters

7.1 Error Codes

Table 7-1 Error codes

Code	Description
0	Success
10000000	The task has been received and is being processed.
10000001	The request message is in an invalid format.
10000002	In the request, the token has not been authenticated or the authentication fails.
10000003	The access to the authentication service (IAM) has been denied.
10000005	The network access has been denied.
10000006	The access to Neutron has been denied.
10000007	The access to Nova has been denied.
10000008	The service is not enabled.
10000009	The account is limited.
10000010	The account is frozen.
10000011	The account is abnormal.
10000012	The account is of an unknown type.
10000016	VPC cannot be accessed or the EIP does not exist.
10001001	The network access has been denied.
10001002	An invalid traffic triggering parameter is used.
10001003	An invalid HTTP request triggering parameter is used.

 Copyright © Huawei Technologies Co., Ltd.

Code	Description
10001004	An invalid cleaning limit parameter is used.
10001005	An invalid application type parameter is used.
10001006	The server is busy processing other requests, please try again later.
10001007	This operation is not allowed in the current status.
10001008	An incorrect task ID is used.
10001009	The operation rights are limited.
10001020	ID of the IP address is invalid.
10005001	An invalid sending frequency parameter is used.
10005002	The alarm configuration fails to be updated.
10005003	An update operation is being performed. Try again later.
10005004	Invalid **topic_urn**.
10005005	Invalid **display_name**.
10001010	The entered time range is invalid.
11000000	A system error occurs, please contact technical support engineers.
11000001	The access to the database has been denied.
11000002	The access to ATIC has been denied.
12100001	The specified ECS does not exist.

 Copyright © Huawei Technologies Co., Ltd.

A Appendix

A.1 Common Returned Values

- Normal

Returned Value	Description
200	The request is successfully processed.

- Abnormal

Returned Value	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.
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.

 Copyright © Huawei Technologies Co., Ltd.

Returned Value	Description
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 Obtaining a Project ID

1. Obtain the token.

   For details, see **Token-based Authentication**.

2. Obtain the project ID.

   The API for obtaining the project ID is **GET https://iam.eu-west-0.myhuaweicloud.com/v3/*projects***.

   Add **X-Auth-Token** to the request header, and set the value of **X-Auth-Token** to the token obtained in the preceding step.

   The following is an example response. **id** indicates the project ID.

```
{
    "links": {},
    "projects": [
        {
            "is_domain": ,
            "description": "",
            "links": {},
            "enabled": true,
            "id": "",   //Project ID
            "parent_id": "",
            "domain_id": "",
            "name": ""
        },
        ...
   ]
}
```


Copyright © Huawei Technologies Co., Ltd.

B Change History

Released On	Description
2019-11-28	This issue is the fifth official release. Adjusted the API architecture.
2018-12-24	This issue is the fourth official release, which incorporates the following changes: Modified the document based on the new template of the API reference.
2018-09-30	This issue is the third official release. Added "Querying All API Versions" and "Querying a Specified API Version".
2017-04-28	This issue is the second official release, which incorporates the following changes: ● Updated examples in "Querying Optional Anti-DDoS Defense Policies".
2017-01-06	This issue is the first official release.

 Copyright © Huawei Technologies Co., Ltd.