ALIBABA CLOUD

Alibaba Cloud

Anti-DDoS

API Refrence for Anti-DDoS Origin

Document Version: 20200826

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.API reference (2017-11-20)

1.1. List of operations by function

The following table lists API operations available for use in Anti-DDoS Origin. For more information, see related documentation.

> **Notice** The API operations of Anti-DDoS Origin are available only for Anti-DDoS Origin Enterprise instances. Before you call the following operations, make sure that you have purchased an Anti-DDoS Origin Enterprise instance. For more information, see 开通DDoS原生防护企业版.

On-demand instance management

On-demand instances protect servers in on-premises data centers outside China and cloud assets based on CIDR blocks. For more information, see Assets.

Operation	Description
DescribeOnDemandInstance	Queries the information about on-demand instances.
ModifyOnDemaondDefenseStatus	Modifies the protection status of an on-demand instance.
DescribeTopTraffic	Queries the top N IP addresses that reroute the most traffic among on-demand instances in a specific period.

1.2. Make API requests

To send an Anti-DDoS Origin API request, you must send an HTTP GET request to the Anti-DDoS Origin endpoint. You must add the request parameters that correspond to the API operation being called. After you call the API operation, the system returns a response. The request and response are encoded in UTF-8.

Request structure

Anti-DDoS Origin API operations use the RPC protocol. You can call Anti-DDoS Origin API operations by sending HTTP GET requests. The request syntax is as follows:

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

Parameters:

- Endpoint: the endpoint of the Anti-DDoS Origin API.

Endpoint	Supported region

Endpoint	Supported region
ddosbgp.aliyuncs.com	○ Regions in mainland China ■ China (Hangzhou): cn-hangzhou ■ China (Shanghai): cn-shanghai ■ China (Qingdao): cn-qingdao ■ China (Beijing): cn-beijing ■ China (Zhangjiakou-Beijing Winter Olympics): cn-zhangjiakou ■ China (Hohhot): cn-huhehaote ■ China (Ulanqab): cn-wulanchabu ■ China (Shenzhen): cn-shenzhen ■ China (Heyuan): cn-heyuan ■ China (Chengdu): cn-chengdu ○ Regions outside China ■ UK (London): eu-west-1 ■ Germany (Frankfurt): eu-central-1 ■ Japan (Tokyo): ap-northeast-1 ■ Australia (Sydney): ap-southeast-2 ■ Malaysia (Kuala Lumpur): ap-southeast-3 ■ Indonesia (Jakarta): ap-southeast-5 ■ India (Mumbai): ap-south-1 ■ UAE (Dubai): me-east-1 ■ Russia (Moscow): rus-west-1
ddosbgp.cn-hongkong.aliyuncs.com	China (Hong Kong): cn-hongkong
ddosbgp.ap-southeast-1.aliyuncs.com	Singapore (Singapore): ap-southeast-1
ddosbgp.us-west-1.aliyuncs.com	US (Silicon Valley): us-west-1
ddosbgp.us-east-1.aliyuncs.com	US (Virginia): us-east-1

- Action: the name of the operation being performed. For example, to query Anti-DDoS Origin instances, you must set the Action parameter to **DescribeInstanceList**.
- Version: the version number of the API. Set the value to **2017-11-20**.
- Parameters: the request parameters for the operation. Separate multiple parameters with ampersands (&).

  Request parameters include both common parameters and operation-specific parameters. Common parameters contain information such as the version number of the API and identity authentication. For more information, see Common parameters.

The following example demonstrates how to call the **DescribeInstanceList** operation in Anti-DDoS Origin:

Note To improve readability, the API request is displayed in the following format:

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

Authorization

To ensure the security of your account, we recommend that you use a RAM user to call Anti-DDoS Origin API operations. Before you use a RAM user to call Anti-DDoS Origin API operations, you must create and attach permission policies to the RAM user.

API signature

You must sign all API requests to ensure security. Alibaba Cloud uses the request signature to verify the identity of the API caller, regardless of an HTTP request or an HTTPS request.

You must add the signature to the Anti-DDoS Origin API request in the following format:

```
https://endpoint/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&Signature=CT9X0VtwR86fNW
Snsc6v8YGOjuE%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
```

1.3. Common parameters

Common request parameters must be included in all Anti-DDoS Origin API requests.

Sample common parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
DdosRegionId	String	Yes	The region of the DDoS Origin service. Valid values: • *cn-hangzhou* • *cn-shanghai* • *cn-qingdao* • *cn-beijing* • *cn-zhangjiakou* • *cn-huhehaote* • *cn-shenzhen* • *cn-hongkong* • *us-west-1*
Format	String	No	The format in which to return the response. Valid values: • *JSON* (default) • *XML*
Version	String	Yes	The version number of the API, in the format of YYYY-MM-DD. Set the value to *2017-11-20*.
AccessKeyId	String	Yes	The AccessKey ID provided to you by Alibaba Cloud.
Signature	String	Yes	The signature string of the current request.
SignatureMethod	String	Yes	The encryption method of the signature string. Set the value to *HMAC-SHA1*.
Timestamp	String	Yes	The timestamp of the request. Specify the time in the ISO 8601 standard in the *YYYY-MM-DDThh:mm:ssZ* format. The time must be in UTC. For example, *2013-01-10T12:00:00Z* indicates January 10, 2013, 20:00:00 (UTC+8).
SignatureVersion	String	Yes	The version of the signature encryption algorithm. Set the value to *1*.
SignatureNonce	String	Yes	A unique, random number used to prevent replay attacks. You must use different numbers for different requests.
ResourceOwnerAccount	String	No	The name of the account that owns the resource that you want to access by using this API request.

Examples

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

Common response parameters

API responses use the HTTP response format where a 2xx status code indicates a successful call and a 4xx or 5xx status code indicates a failed call. Response data can be returned in either the JSON or XML format. You can specify the response format in the request. The default response format is XML.

Every response returns a unique RequestId regardless of whether the call is successful.

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
<!—Result Root Node--> <Interface Name+Response> <!—Return Request Tag--> <RequestId>4C467
B38-3910-447D-87BC-AC049166F216</RequestId>
<!—Return Result Data--> </Interface Name+Response>
```

- JSON format

```
{
"RequestId":"4C467B38-3910-447D-87BC-AC049166F216",
/*Return result data*/ }
```

1.4. On-demand instances

1.4.1. DescribeOnDemandInstance

Queries the information of an on-demand instance.

> Note Anti-DDoS Origin API operations are available only for Anti-DDoS Origin Enterprise users.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeOnDemandInstance	The operation that you want to perform. Set the value to **DescribeOnDemandInstance**.
PageNo	Integer	Yes	1	The number of the page to return. Default value: **1**.
PageSize	Integer	Yes	10	The number of entries to return on each page. Maximum value: **50**. Default value: **10**.
DdosRegionId	String	No	cn-hangzhou	The ID of the region that you want to query. **Note** You can call the DescribeRegions operation to query the most recent region list.

Response parameters

Parameter	Type	Example	Description
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	The ID of the request.
Total	String	1	The total number of on-demand instances.
Instances	Array		Information of on-demand instances.
InstanceId	String	ddosbgp-xxx	The ID of the instance.
Remark	String	123	The remark of the on-demand instance.
DefenseStatus	String	Defense	The protection status of the on-demand instance. Valid values: • **Defense**: rerouting enabled • **UnDefense**: rerouting disabled
Ipnet	List	1.1.1.0/24	The CIDR block of the on-demand instance.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeOnDemandInstance
&PageNo=1 &PageSize=10 &<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeOnDemandInstanceResponse>
<code>200</code>
<data>
<DefenseStatus>Defense</DefenseStatus>
<InstanceId>ddosbgp-xxx</InstanceId>
<Ipnet>
<element>1.1.1.0/24</element>
</Ipnet>
<Remark>123</Remark>
</data>
<Total>1</Total>
<requestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</requestId>
<success>true</success>
</DescribeOnDemandInstanceResponse>
```

`JSON` format

```
{
"code": 200,
"requestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
"Total":"1",
"success": true,
"data": {
"InstanceId":"ddosbgp-xxx",
"Ipnet": ["1.1.1.0/24"],
"Remark": "123",
"DefenseStatus": "Defense" }
}
```

Error codes

For a list of error codes, visit the API Error Center.

1.4.2. ModifyOnDemaondDefenseStatus

Modifies the protection status of an on-demand instance.

> **Note** Anti-DDoS Origin API operations are available only for Anti-DDoS Origin Enterprise users.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyOnDemaondDefenseStatus	The operation that you want to perform. Set the value to **ModifyOnDemaondDefenseStatus**.
DdosRegionId	String	Yes	cn-hangzhou	The region ID of the on-demand instance. Note You can call the DescribeRegions operation to query the most recent region list.
DefenseStatus	String	Yes	Defense	The protection status of the on-demand instance. Valid values: • **Defense**: enables rerouting. • **UnDefense**: disables rerouting.
InstanceId	String	Yes	ddosbgp-xxx	The ID of an on-demand instance.

Response parameters

Parameter	Type	Example	Description
RequestId	String	4C467B38-3910-447D-87BC-AC049166F216	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=ModifyOnDemaondDefenseStatus
&DdosRegionId=cn-hangzhou
&DefenseStatus=Defense
&InstanceId=ddosbgp-xxx
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

For a list of error codes, visit the API Error Center.

1.4.3. DescribeTopTraffic

Queries the top N IP addresses that reroute the most traffic among on-demand instances in a specific period.

> **Note** Anti-DDoS Origin API operations are available only for Anti-DDoS Origin Enterprise users.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeTopTraffic	The operation that you want to perform. Set the value to **DescribeTopTraffic**.
EndTime	String	Yes	1563445054	The end of the time range to query. Unit: seconds.
InstanceId	String	Yes	ddosbgp-xxx	The ID of the on-demand instance.
StartTime	String	Yes	1560853054	The beginning of the time range to query. Unit: seconds.
Ipnet	String	No	1.1.1.0/24	The CIDR block of the on-demand instance.
Rn	Integer	No	1	The number of IP addresses that you want to query. Default value: 1 (to query the IP address that reroutes the most traffic).
PageNo	Integer	No	1	The number of the page to return. Default value: 1.
PageSize	Integer	No	10	The number of entries to return on each page. Maximum value:50. Default value: 10.
ResourceGroupId	String	No	test	The ID of the resource group.

Response parameters

Parameter	Type	Example	Description
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	The ID of the request.
Total	Long	1	The total number of entries returned.
TrafficList	Array		Information of rerouted traffic.
Pps	Integer	100000	The total number of rerouted data packets. Unit: pps.
Bps	Integer	2919212	The total size of the rerouted traffic. Unit: Kbit/s.
AttackBps	Integer	0	The size of attack traffic. Unit: Kbit/s.
AttackPps	Integer	0	The number of attack data packets. Unit: pps.
Ip	String	1.1.1.1	The IP address of the on-demand instance.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeTopTraffic
&EndTime=1563445054
&InstanceId=ddosbgp-xxx
&StartTime=1560853054
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

For a list of error codes, visit the API Error Center.

2.API reference (2018-07-20)

2.1. List of operations by function

The following tables list API operations available for use in Anti-DDoS Origin. For more information, see related documentation.

> **Notice** The API operations of Anti-DDoS Origin are available only for Anti-DDoS Origin Enterprise instances. Before you call the following operations, make sure that you have purchased an Anti-DDoS Origin Enterprise instance. For more information, see 开通DDoS原生防护企业版.

Protection setting management

Operation	Description
AddIp	Adds IP addresses to an Anti-DDoS Origin instance.
DeleteIp	Removes IP addresses from an Anti-DDoS Origin instance to cancel protection.
DeleteBlackhole	Disables blackhole filtering for a protected IP address.

Instance management

Operation	Description
DescribeRegions	Queries regions where Anti-DDoS Origin is available.
DescribeInstanceList	Queries the details of Anti-DDoS Origin instances.
DescribeInstanceSpecs	Queries the specifications of Anti-DDoS Origin instances.
DescribeExcpetionCount	Queries the exceptions of an Anti-DDoS Origin instance.
DescribePackIpList	Queries IP addresses that are protected by an Anti-DDoS Origin instance.
ModifyRemark	Modifies the remarks about an Anti-DDoS Origin instance.
CheckGrant	Checks whether Anti-DDoS Origin is authorized to query information about your Elastic Compute Service (ECS) instances.

Log management

Operation	Description
DescribeDdosEvent	Queries the DDoS events on a specified Anti-DDoS Origin instance.
DescribeOpEntities	Queries operations logs.
DescribeTraffic	Queries the traffic that flows through a specified Anti-DDoS Origin instance.
DescribeOnDemandDdosEvent	Queries the DDoS events on an Anti-DDoS Origin on-demand instance.

Tag management

Operation	Description
ListTagKeys	Queries all tags.
TagResources	Binds tags to a specified Anti-DDoS Origin instance.
UntagResources	Unbinds tags from a specified Anti-DDoS Origin instance.
ListTagResources	Queries Anti-DDoS Origin instances that are bound with tags.

2.2. Make API requests

To send an Anti-DDoS Origin API request, you must send an HTTP GET request to the Anti-DDoS Origin endpoint. You must add the request parameters that correspond to the API operation being called. After you call the API operation, the system returns a response. The request and response are encoded in UTF-8.

Request structure

Anti-DDoS Origin API operations use the RPC protocol. You can call Anti-DDoS Origin API operations by sending HTTP GET requests. The request syntax is as follows:

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

Parameters:

- Endpoint: the endpoint of the Anti-DDoS Origin API.

Endpoint	Supported region

Endpoint	Supported region
ddosbgp.aliyuncs.com	○ Regions in mainland China ■ China (Hangzhou): cn-hangzhou ■ China (Shanghai): cn-shanghai ■ China (Qingdao): cn-qingdao ■ China (Beijing): cn-beijing ■ China (Zhangjiakou-Beijing Winter Olympics): cn-zhangjiakou ■ China (Hohhot): cn-huhehaote ■ China (Ulanqab): cn-wulanchabu ■ China (Shenzhen): cn-shenzhen ■ China (Heyuan): cn-heyuan ■ China (Chengdu): cn-chengdu ○ Regions outside China ■ UK (London): eu-west-1 ■ Germany (Frankfurt): eu-central-1 ■ Japan (Tokyo): ap-northeast-1 ■ Australia (Sydney): ap-southeast-2 ■ Malaysia (Kuala Lumpur): ap-southeast-3 ■ Indonesia (Jakarta): ap-southeast-5 ■ India (Mumbai): ap-south-1 ■ UAE (Dubai): me-east-1 ■ Russia (Moscow): rus-west-1
ddosbgp.cn-hongkong.aliyuncs.com	China (Hong Kong): cn-hongkong
ddosbgp.ap-southeast-1.aliyuncs.com	Singapore (Singapore): ap-southeast-1
ddosbgp.us-west-1.aliyuncs.com	US (Silicon Valley): us-west-1
ddosbgp.us-east-1.aliyuncs.com	US (Virginia): us-east-1

- Action: the name of the operation being performed. For example, to query Anti-DDoS Origin instances, you must set the Action parameter to **DescribeInstanceList**.
- Version: the version number of the API. Set the value to **2018-07-20**.
- Parameters: the request parameters for the operation. Separate multiple parameters with ampersands (&).

  Request parameters include both common parameters and operation-specific parameters. Common request parameters include information, such as API version number and authentication information. For more information, see Common parameters.

The following example demonstrates how to call the DescribeInstanceList operation in Anti-DDoS Origin:

Note To improve readability, the API request is displayed in the following format:

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

Authorization

To ensure the security of your account, we recommend that you use a RAM user to call Anti-DDoS Origin API operations. Before you use a RAM user to call Anti-DDoS Origin API operations, you must create and attach permission policies to the RAM user.

Request signatures

You must sign all API requests to ensure security. Alibaba Cloud uses the request signature to verify the identity of the API caller, regardless of whether an HTTP or HTTPS request is used.

You must add the signature to the Anti-DDoS Origin API request in the following format:

```
https://endpoint/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&Signature=CT9X0VtwR86fNW
Snsc6v8YGOjuE%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
```

2.3. Common parameters

Common request parameters must be included in all API operations of the anti-DDoS protection package.

Common request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
DdosRegionId	String	Yes	The region of the protection package. Valid values: • *cn-hangzhou* • *cn-shanghai* • *cn-qingdao* • *cn-beijing* • *cn-zhangjiakou* • *cn-huhehaote* • *cn-shenzhen* • *cn-hongkong* • *us-west-1*
Format	String	No	The format of the response. Valid values: • *JSON* (default) • *XML*
Version	String	Yes	The version number of the API, in the format of YYYY-MM-DD. Example: *2018-07-20*.
AccessKeyId	String	Yes	The AccessKey ID provided to you by Alibaba Cloud.
Signature	String	Yes	The signature string of the current request.
SignatureMethod	String	Yes	The encryption algorithm of the signature string. Set the value to *HMAC-SHA1*.
Timestamp	String	Yes	The timestamp of the request. Specify the time in the ISO 8601 standard in the *yyyy-MM-ddTHH:mm:ssZ* format. The time must be in UTC. For example, *2013-01-10T12:00:00Z* indicates January 10, 2013, 20:00:00 (UTC+8).
SignatureVersion	String	Yes	The version of the signature encryption algorithm. Set the value to *1*.
SignatureNonce	String	Yes	A unique and randomly generated number used to prevent replay attacks. Users must use different numbers for different requests.
ResourceOwnerAccount	String	No	The name of the account that owns the resource to be accessed through this API request.

Examples

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

Common response parameters

API responses use the HTTP response format where a status code of 2XX indicates a successful call and a status code of 4XX or 5XX indicates a failed call. Response data can be returned in either the JSON or XML format. You can specify the response format when you are making the request. The default response format is XML.

Every response has a unique RequestId regardless of whether the call was successful or not.

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
<!—Result root node-->
<Operation name+Response>
<!—Return request tag-->
<RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
<!—Return result data-->
</Operation name+Response>
```

- JSON format

```
{
"RequestId":"4C467B38-3910-447D-87BC-AC049166F216",
/*Return result data*/
}
```

2.4. Protection

2.4.1. AddIp

Adds IP addresses to an Anti-DDoS Origin Enterprise instance.

Note Anti-DDoS Origin API operations are available for only Anti-DDoS Origin Enterprise users.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	AddIp	The operation that you want to perform. Set the value to **AddIp**.
InstanceId	String	Yes	ddosbgp-cn-12345678	The ID of the Anti-DDoS Origin Enterprise instance.
IpList	String	Yes	[{"ip":"1.1.1.1"},{"ip":"2.2.2.2"}]	The list of IP addresses that you want to add. You can specify multiple IP addresses.
ResourceGroupId	String	No	test	The ID of the resource group.
ResourceRegionId	String	No	cn-hangzhou	The ID of the region where the resource group resides.

Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=AddIp
&InstanceId=ddosbgp-cn-12345678
&IpList=[{"ip":"1.1.1.1"},{"ip":"2.2.2.2"}]
& <Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

For a list of error codes, visit the API Error Center.

2.4.2. DeleteIp

Removes IP addresses from an Anti-DDoS Origin Enterprise instance to remove protection.

> Note Anti-DDoS Origin API operations are available for only Anti-DDoS Origin Enterprise users.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteIp	The operation that you want to perform. Set the value to **DeleteIp**.
InstanceId	String	Yes	ddosbgp-cn-xxx	The ID of the Anti-DDoS Origin Enterprise instance.
IpList	String	Yes	[{"ip":"1.1.1.1"},{"ip":"2.2.2.2"}]	The list of IP addresses that you want to remove. You can specify multiple IP addresses.
ResourceGroupId	String	No	xx	The ID of the resource group.
ResourceRegionId	String	No	cn-hangzhou	The ID of the region where the resource group resides.

Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DeleteIp
&InstanceId=ddosbgp-cn-xxx
&IpList=1.1.1.1,2.2.2.2
& <Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

For a list of error codes, visit the API Error Center.

2.4.3. DeleteBlackhole

Deactivates a black hole for the IP address of a protection target.

> **Note** Anti-DDoS Origin API operations are available for only Anti-DDoS Origin Enterprise users.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteBlackhole	The operation that you want to perform. Set the value to **DeleteBlackhole**.
InstanceId	String	Yes	ddosbgp-cn-xxx	The ID of the Anti-DDoS Origin Enterprise instance.
Ip	String	Yes	1.1.1.1	The IP address for which you want to deactivate a black hole.
ResourceGroupId	String	No	xx	The ID of the resource group.
ResourceRegionId	String	No	cn-hangzhou	The ID of the region where the resource group resides.

Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DeleteBlackhole
&InstanceId=ddosbgp-cn-xxx
&Ip=1.1.1.1
& <Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

For a list of error codes, visit the API Error Center.

2.5. Instances

2.5.1. DescribeRegions

Views the regions that support Anti-DDoS Origin Enterprise.

> **Note** Anti-DDoS Origin API operations are available for only Anti-DDoS Origin Enterprise users.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeRegions	The operation that you want to perform. Set the value to **DescribeRegions**.
ResourceGroupId	String	No	xx	The ID of the resource group.

Response parameters

Parameter	Type	Example	Description
Code	String	true	The response status code.
Regions	Array		The list of supported regions where you can activate Anti-DDoS Origin Enterprise.
RegionEnName	String	shanghai	The English name of each region.
RegionId	String	cn-shanghai	The ID of each region.
RegionName	String	[DO NOT TRANSLATE]	The Chinese name of each region.
RequestId	String	C3D66E07-41BF-41B7-A4BF-83A9E08E1C09	The ID of the request.
Success	Boolean	true	Indicates whether the API operation is successfully called.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeRegions
& <Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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


Error codes

For a list of error codes, visit the API Error Center.

2.5.2. DescribeInstanceList

Queries the details of Anti-DDoS Origin Enterprise instances.

> Note Anti-DDoS Origin API operations are available for only Anti-DDoS Origin Enterprise users.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeInstanceList	The operation that you want to perform. Set the value to **DescribeInstanceList**.
PageNo	Integer	Yes	1	The number of the page to return. Default value: **1**.
PageSize	Integer	Yes	10	The number of entries to return on each page. Valid values: 1 to **50**. Default value: **10**.
ResourceGroupId	String	No	test	The ID of the resource group to query.
InstanceIdList	String	No	['ddosbgp-cn-xx','ddosbpg-cn-xxx']	The IDs of Anti-DDoS instances to query. If you want to query multiple instances, separate the IDs with commas (,). The parameter must be passed to the API operation in the JSON format, for example, `['ddosbgp-cn-xx','ddosbpg-cn-xxx']`. > Note If the parameter is empty, the details of all Anti-DDoS Origin Enterprise instances are returned.

Parameter	Type	Required	Example	Description
Remark	String	No	test	The alias of the Anti-DDoS Origin Enterprise instance. Note If the parameter is empty, the details of all Anti-DDoS Origin Enterprise instances are returned.
DdosRegionId	String	No	cn-hangzhou	The ID of the region where the Anti-DDoS Origin Enterprise instance resides.
IpVersion	String	No	IPv4	The IP version. Valid values: Note If the parameter is empty, the details of all Anti-DDoS Origin Enterprise instances are returned. • IPv4 • IPv6
InstanceType	String	No	0	The protection plan. Valid values: Note If the parameter is empty, the details of all Anti-DDoS Origin Enterprise instances are returned. • 0: Pro edition • 1: Enterprise edition
Ip	String	No	1.1.1.1	The IP address of the protection target that is protected by the Anti-DDoS Origin Enterprise instance. Note If the parameter is empty, the details of all Anti-DDoS Origin Enterprise instances are returned.

Parameter	Type	Required	Example	Description
Orderby	String	No	expireTime	The key by which you want to sort the entries. Valid value: **expireTime**, which specifies the expiration time.
Orderdire	String	No	asc	The order in which you want to sort the entries. Valid values: • **desc**: specifies the descending order • **asc**: specifies the ascending order
Tag.N.Key	String	No	test	The key of each tag. The N is a digit that starts from 1. If multiple tags exist, the keys are passed to the API operation in sequence, for example, Tag.1.Key, Tag.2.Key, and Tag.3.Key.
Tag.N.Value	String	No	test	The key of each tag. The N is a digit that starts from 1. If multiple tags exist, the values are passed to the API operation in sequence, for example, Tag.1.Value, Tag.2.Value, and Tag.3.Value.

Response parameters

Parameter	Type	Example	Description
InstanceList	Array		The list of Anti-DDoS Origin Enterprise instances and the details of each instance.
AutoRenewal	Boolean	false	Indicates whether auto-renewal is enabled for the Anti-DDoS Origin Enterprise instance.
BlackholdingCount	String	0	The number of IP addresses that are in the blackholing state.
ExpireTime	Long	1560009600000	The expiration time of the Anti-DDoS Origin Enterprise instance.

Parameter	Type	Example	Description
GmtCreate	Long	1554708159000	The creation time of the Anti-DDoS Origin Enterprise instance.
InstanceId	String	ddosbgp-cn-xx	The ID of an Anti-DDoS Origin Enterprise instance.
InstanceType	String	1	The protection plan. Valid values: • 0: Pro edition • 1: Enterprise edition
IpType	String	IPv4	The IP version. Valid values: • IPv4 • IPv6
Product	String	SLB	The type of service to be protected. Valid values: • ECS • SLB • EIP • WAF
Remark	String	test	The alias of the Anti-DDoS Origin Enterprise instance.
Status	String	1	The status of the Anti-DDoS Origin Enterprise instance. Valid values: • 1: indicates that the Anti-DDoS Origin Enterprise instance is in the normal state. • 2: indicates that the Anti-DDoS Origin Enterprise instance has expired. • 3: indicates that the Anti-DDoS Origin Enterprise instance is released.
RequestId	String	C3F7E6AE-43B2-4730-B6A3-FD17552B8F65	The ID of the request.
Total	Long	1	The total number of entries returned.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeInstanceList
&PageNo=1
&PageSize=10
&<Common request parameters>
```

Sample success response

`XML` format

```
<DescribeInstanceListResponse>
<RequestId>C3F7E6AE-43B2-4730-B6A3-FD17552B8F65</RequestId>
<InstanceList>
<Instance>
<Status>1</Status>
<AutoRenewal>true</AutoRenewal>
<IpType>IPv4</IpType>
<ExpireTime>1560009600000</ExpireTime>
<InstanceId>ddosbgp-cn-xx</InstanceId>
<GmtCreate>1554708159000</GmtCreate>
<Remark>test</Remark>
<BlackholdingCount>0</BlackholdingCount>
</Instance>
</InstanceList>
<Total>1</Total>
</DescribeInstanceListResponse>
```

`JSON` format

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


Error codes

For a list of error codes, visit the API Error Center.

2.5.3. DescribeInstanceSpecs

Queries the specifications of Anti-DDoS Origin Enterprise instances.

> **Note** Anti-DDoS Origin API operations are available for only Anti-DDoS Origin Enterprise users.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeInstanceSpecs	The operation that you want to perform. Set the value to **DescribeInstanceSpecs**.
InstanceIdList	String	Yes	["ddosbgp-cn-x1","ddosbgp-cn-x2"]	The IDs of Anti-DDoS instances to query. If you want to query multiple instances, separate the IDs with commas (,). The parameter must be passed to the API operation in the JSON format, for example, `["ddosbgp-cn-x1","ddosbgp-cn-x2"]`.
DdosRegionId	String	No	cn-hangzhou	The ID of the region where Anti-DDoS Origin Enterprise instances reside.
ResourceGroupId	String	No	test	The ID of the resource group.

Response parameters

Parameter	Type	Example	Description
InstanceSpecs			The list of Anti-DDoS Origin Enterprise instances and the specifications of each instance.
AvailableDeleteBlackholeCount	String	100	The number of times that you can deactivate a black hole.
InstanceId	String	ddosbgp-cn-x1	The ID of an Anti-DDoS Origin Enterprise instance.
PackConfig			The configuration information of the Anti-DDoS Origin Enterprise instance.
BindIpCount	Integer	0	The number of IP addresses that are protected by the Anti-DDoS Origin Enterprise instance.

Parameter	Type	Example	Description
IpAdvanceThre	Integer	101	The threshold of elastic protection for the specified IP addresses. Unit: Gbit/s.
IpBasicThre	Integer	20	The threshold of basic protection for the specified IP addresses. Unit: Gbit/s.
IpSpec	Integer	100	The maximum number of IP addresses that you can add to the Anti-DDoS Origin Enterprise instance.
PackAdvThre	Integer	100	The bandwidth of elastic protection. Unit: Gbit/s.
PackBasicThre	Integer	200	The bandwidth of basic protection. Unit: Gbit/s.
Region	String	cn-hangzhou	The ID of the region where the Anti-DDoS Origin Enterprise instance resides.
RequestId	String	CEB7F4F5-1DA8-41ED-A9C4-E0F0033E9E1F	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeInstanceSpecs
&InstanceIdList=["ddosbgp-cn-x1","ddosbgp-cn-x2"]
& <Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

For a list of error codes, visit the API Error Center.

2.5.4. DescribeExcpetionCount

Queries information about exceptions of an Anti-DDoS Origin Enterprise instance.

> Note Anti-DDoS Origin API operations are available for only Anti-DDoS Origin Enterprise users.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeExcpetionCount	The operation that you want to perform. Set the value to **DescribeExcpetionCount**.
DdosRegionId	String	Yes	cn-hangzhou	The ID of the region where the Anti-DDoS Origin Enterprise instance resides.
ResourceGroupId	String	No	test	The ID of the resource group.

Response parameters

Parameter	Type	Example	Description
ExceptionIpCount	Integer	0	The number of IP addresses that have exceptions. These IP addresses include the IP addresses of Elastic Compute Service (ECS) and Server Load Balancer (SLB) instances that are protected.
ExpireTimeCount	Integer	1	The number of instances that will expire within seven days.
RequestId	String	A3EEE55F-3B9F-4765-8C03-1A1A904F3451	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeExcpetionCount
&DdosRegionId=cn-hangzhou
& <Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

For a list of error codes, visit the API Error Center.

2.5.5. DescribePackIpList

Queries IP addresses that are protected by Anti-DDoS Origin Enterprise.

> Note Anti-DDoS Origin API operations are available for only Anti-DDoS Origin Enterprise users.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribePackIpList	The operation that you want to perform. Set the value to **DescribePackIpList**.
DdosRegionId	String	Yes	cn-hangzhou	The ID of the region where the Anti-DDoS Origin Enterprise instance resides.
InstanceId	String	Yes	ddosbgp-cn-x1	The ID of the Anti-DDoS Origin Enterprise instance.
PageNo	Integer	Yes	1	The number of the page to return. Default value: **1**.
PageSize	Integer	Yes	10	The number of entries to return on each page. Valid values: 1 to **50**. Default value: **10**.
Ip	String	No	1.1.1.1	The IP address of the protection target. Returns the details of only the protection target to which the specified IP address points.

Parameter	Type	Required	Example	Description
ProductName	String	No	ECS	The type of service that is under protection. Valid values: Note Returns the details of only the protection target to which the specified IP address points. • ECS • SLB • EIP • WAF
ResourceGroupId	String	No	test	The ID of the resource group.

Response parameters

Parameter	Type	Example	Description
Code	String	200	The response status code.
IpList			The list of IP addresses.
Ip	String	1.1.1.1	The IP address that is protected.
Product	String	ECS	The type of protection target to which the specified IP address points. Valid values: • ECS • SLB • EIP • WAF
Remark	String	test	The remarks about the protection target. For example, remarks about an ECS instance.

Parameter	Type	Example	Description
Status	String	normal	The status of the protection target. Valid values: • **normal**: indicates that the protection target is in the running state • **hole_begin**: indicates that the protection target is in the blackhole state
RequestId	String	B479FE9B-F0EB-423B-81E5-ECE2167BCF40	The ID of the request.
Success	Boolean	true	Indicates whether the API operation is successfully called.
Total	Integer	1	The total number of entries returned.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribePackIpList
&DdosRegionId=cn-hangzhou
&InstanceId=ddosbgp-cn-x1
&PageNo=1
&PageSize=10
& <Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

For a list of error codes, visit the API Error Center.

2.5.6. ModifyRemark

Modifies the alias of an Anti-DDoS Origin Enterprise instance.

Note Anti-DDoS Origin API operations are available for only Anti-DDoS Origin Enterprise users.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyRemark	The operation that you want to perform. Set the value to ModifyRemark.
InstanceId	String	Yes	ddosbgp-cn-xxx	The ID of the Anti-DDoS Origin Enterprise instance.
Remark	String	Yes	test	The alias that you want to add.
ResourceGroupId	String	No	test	The ID of the resource group.
ResourceRegionId	String	No	cn-hangzhou	The ID of the region where the resource group resides.

Response parameters

Parameter	Type	Example	Description
RequestId	String	4C467B38-3910-447D-87BC-AC049166F216	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=ModifyRemark
&InstanceId=ddosbgp-cn-xxx
&Remark=test
& <Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

For a list of error codes, visit the API Error Center.

2.5.7. CheckGrant

Checks whether Anti-DDoS Origin Enterprise is authorized to query information about Elastic Compute Service (ECS) instances.

> **Note** Anti-DDoS Origin API operations are available for only Anti-DDoS Origin Enterprise users.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CheckGrant	The operation that you want to perform. Set the value to **CheckGrant**.
ResourceGroupId	String	No	xx	The ID of the resource group.

Response parameters

Parameter	Type	Example	Description
RequestId	String	E76E316C-697F-42D8-883A-D99864D2E77F	The ID of the request.
Status	Integer	1	The authorization status. Valid values: • **1**: indicates that Anti-DDoS Origin Enterprise is authorized to query information about ECS instances • **0**: indicates that Anti-DDoS Origin Enterprise is not authorized to query information about ECS instances

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=CheckGrant
& <Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

For a list of error codes, visit the API Error Center.

2.6. Charts and logs

2.6.1. DescribeDdosEvent

Queries DDoS events of the specified Anti-DDoS Origin Enterprise instance.

> **Note** Anti-DDoS Origin API operations are available for only Anti-DDoS Origin Enterprise users.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeDdosEvent	The operation that you want to perform. Set the value to **DescribeDdosEvent**.
EndTime	Integer	Yes	1557909844	The timestamp that specifies the end of the time range to query. Unit: seconds. The timestamp follows the UNIX time format. It is the number of seconds that have elapsed since 00:00:00 Thursday, 1 January 1970.
InstanceId	String	Yes	ddosbgp-cn-x1	The ID of the Anti-DDoS Origin Enterprise instance.
PageNo	Integer	Yes	1	The number of the page to return. Default value: **1**.
PageSize	Integer	Yes	10	The number of entries to return on each page. Valid values: 1 to **50**. Default value: **10**.
StartTime	Integer	Yes	1557305044	The timestamp that specifies the beginning of the time range to query. Unit: seconds. The timestamp follows the UNIX time format. It is the number of seconds that have elapsed since 00:00:00 Thursday, 1 January 1970.
Ip	String	No	1.1.1.1	The IP address of the protection target.
ResourceGroupId	String	No	test	The ID of the resource group.
ResourceRegionId	String	No	cn-hangzhou	The ID of the region where the resource group resides.

Response parameters

Parameter	Type	Example	Description
Events			The list of DDoS events and the details of each event.
EndTime	Integer	1557891306	The timestamp that indicates the end time of the attack. Unit: seconds. The timestamp follows the UNIX time format. It is the number of seconds that have elapsed since 00:00:00 Thursday, 1 January 1970.
Ip	String	1.1.1.1	The IP address of the protection target that encounters the DDoS attack.
Mbps	Integer	110000	The throughput of the DDoS attack. Unit: Mbit/s.
Pps	Integer	0	The packet forwarding rate of the DDoS attack. Unit: packets per second (PPS).
StartTime	Integer	1557889506	The timestamp that indicates the start time of the attack. Unit: seconds. The timestamp follows the UNIX time format. It is the number of seconds that have elapsed since 00:00:00 Thursday, 1 January 1970.
Status	String	defense_end	The status of the event. Valid values: • **hole_begin**: indicates that the event is in the blackhole state. • **hole_end**: indicates that blackhole ends. • **defense_begin**: indicates that the event is in the cleaning state. • **defense_end**: indicates that cleaning ends.
RequestId	String	6A507DC8-F657-4C13-84E2-D1D1B9400753	The ID of the request.
Total	Long	8	The total number of DDoS events.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeDdosEvent
&EndTime=1557909844
&InstanceId=ddosbgp-cn-x1
&PageNo=1
&PageSize=10
&StartTime=1557305044
& <Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeDdosEventResponse>
<RequestId>6A507DC8-F657-4C13-84E2-D1D1B9400753</RequestId>
</Events>
<Event>
<qps>0</qps>
<Status>finished</Status>
<Ip>1.1.1.1</Ip>
<Mbps>110000</Mbps>
<EndTime>1542957514000</EndTime>
<StartTime>1542957499000</StartTime>
</Event>
</Events>
<Total>1</Total>
</DescribeDdosEventResponse>
```

`JSON` format

```
{
"RequestId":"6A507DC8-F657-4C13-84E2-D1D1B9400753",
"Events":[
{
"Pps":450,
"IP":"1.1.1.1",
"Status":"defense_end",
"Mbps":110000,
"EndTime":1557891306,
"StartTime":1557889506
}
],
"Total":1
}
```


Error codes.

For a list of error codes, visit the API Error Center.

2.6.2. DescribeOpEntities

Queries operations logs.

> Note Anti-DDoS Origin API operations are available for only Anti-DDoS Origin Enterprise users.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeOpEntities	The operation that you want to perform. Set the value to **DescribeOpEntities**.
CurrentPage	Integer	Yes	1	The number of the page to return. Default value: 1.

Parameter	Type	Required	Example	Description
EndTime	Long	Yes	1557906714012	The timestamp that specifies the end of the time range to query. Unit: seconds. The timestamp follows the UNIX time format. It is the number of seconds that have elapsed since 00:00:00 Thursday, 1 January 1970.
PageSize	Integer	Yes	10	The number of entries to return on each page. Valid values: 1 to **50**. Default value: **10**.
StartTime	Long	Yes	1555314714011	The timestamp that specifies the beginning of the time range to query. Unit: seconds. The timestamp follows the UNIX time format. It is the number of seconds that have elapsed since 00:00:00 Thursday, 1 January 1970.
InstanceId	String	No	ddosbgp-cn-x1	The ID of the Anti-DDoS Origin Enterprise instance.
OrderBy	String	No	opdate	The key by which you want to sort the entries. Valid values: **opdate**, which specifies the operation time.
OrderDir	String	No	ASC	The order in which you want to sort the entries. Valid values: • **ASC**: specifies the ascending order • **DESC**: specifies the descending order
ResourceGroupId	String	No	test	The ID of the resource group.
ResourceRegionId	String	No	cn-hangzhou	The ID of the region where the resource group resides.

Response parameters

Parameter	Type	Example	Description
OpEntities	Array		The list of operations logs and the details of each operations log.
EntityObject	String	ddosbgp-cn-o4013qftb006	The operation target, which is the ID of the Anti-DDoS Origin Enterprise instance.
EntityType	Integer	1	The type of the operation target. Valid value: 1, which indicates an instance.
GmtCreate	Long	1557821673000	The creation time of the log.
OpAccount	String	system	The account that is used to perform operations. Valid value: **system**, which indicates a predefined account that is owned by Anti-DDoS Origin Enterprise.
OpAction	Integer	8	The type of operation. Valid values: • 3: indicates an operation of adding an IP address. • 4: indicates an operation of unbinding an IP address. • 5: indicates an operation of downgrading an instance. • 6: indicates an operation of disabling a black hole. • 7: indicates an operation of resetting the number of times that you can deactivate a black hole. • 8: indicates an operation of restoring unlimited protection.
OpDesc	String	{\"entity\":{\"baseBandwidth\":20,\"elasticBandwidth\":101}}	The description of the operation.
RequestId	String	52C8ECB0-0B1A-4E66-A31C-B6A855120E82	The ID of the request.
TotalCount	Integer	1	The number of entries returned.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeOpEntities
&CurrentPage=1
&EndTime=1557906714012
&PageSize=10
&StartTime=1555314714011
& <Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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


Error codes

For a list of error codes, visit the API Error Center.

2.6.3. DescribeTraffic

Queries traffic statistics of an Anti-DDoS Origin Enterprise instance.

> **Note** Anti-DDoS Origin API operations are available for only Anti-DDoS Origin Enterprise users.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeTraffic	The operation that you want to perform. Set the value to **DescribeTraffic**.

Parameter	Type	Required	Example	Description
EndTime	Integer	Yes	1563445054	The timestamp that specifies the end of the time range to query. Unit: seconds. The timestamp follows the UNIX time format. It is the number of seconds that have elapsed since 00:00:00 Thursday, 1 January 1970.
Interval	Integer	Yes	1000	The interval between queries. Unit: seconds.
StartTime	Integer	Yes	1560853054	The timestamp that specifies the beginning of the time range to query. Unit: seconds. The timestamp follows the UNIX time format. It is the number of seconds that have elapsed since 00:00:00 Thursday, 1 January 1970.
InstanceId	String	No	ddosbgp-cn-*****	The ID of the Anti-DDoS Origin Enterprise instance. Note You must specify either the InstanceId or Ip parameter, or specify both parameters.
Ip	String	No	1.1.1.1	The IP address of the protection target. Note You must specify either the InstanceId or Ip parameter, or specify both parameters.
ResourceGroupId	String	No	test	The ID of the resource group.

Response parameters

Parameter	Type	Example	Description
FlowList	Array		The traffic statistics of each interval.
FlowType	String	max	The statistical aggregation method of the traffic statistics. Valid values: • **avg**: indicates the average traffic statistics within the specified time range. • **max**: indicates the maximum traffic statistics within the specified time range.
Kbps	Integer	8	The throughput of the instance. Unit: Kbit/s.
Name	String	73765106-54e7-11e9-aab0-d89d67182200	The ID of an entry that includes traffic statistics of the specified time range.
Pps	Integer	9	The packet forwarding rate of the instance. Unit: packets per second (PPS).
Time	Integer	1560857000	The timestamp that indicates the start time of the specified time range.
RequestId	String	6A507DC8-F657-4C13-84E2-D1D1B9400753	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeTraffic
&EndTime=1563445054
&Interval=1000
&StartTime=1560853054
&InstanceId=ddosbgp-cn-*****
& <Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

For a list of error codes, visit the API Error Center.

2.6.4. DescribeOnDemandDdosEvent

Call the DescribeOnDemandDdosEvent operation to query the DDoS events recorded for the IP address of the Anti-DDoS on-demand instance.

> **Note** Anti-DDoS Origin API operations are available for only Anti-DDoS Origin Enterprise users.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Prameter	Type	Required	Example	Description
Action	String	No	DescribeOnDemandDdosEvent	The operation that you want to perform. Set the value to **DescribeOnDemandDdosEvent**.
EndTime	Integer	Yes	1557909844	The timestamp that specifies the end of the time range to query. Unit: seconds. The timestamp follows the UNIX time format. It is the number of seconds that have elapsed since 00:00:00 Thursday, 1 January 1970.
InstanceId	String	No	ddosbgp-cn-x1	The ID of the on-demand instance to query.
PageNo	Integer	Yes	1	The number of the page to return. Default value: **1**.
PageSize	Integer	Yes	10	The number of entries to return on each page. The maximum value is **50**. The default value is **10**.

Prameter	Type	Required	Example	Description
StartTime	Integer	Yes	1557305044	The timestamp that specifies the beginning of the time range to query. Unit: seconds. The timestamp follows the UNIX time format. It is the number of seconds that have elapsed since 00:00:00 Thursday, 1 January 1970.
Ip	String	Yes	1.1.1.1	The IP address of the protection target.
ResourceGroupId	String	Yes	default	The ID of the resource group.
Region ID	String	Yes	cn-hangzhou	The ID of the region to query.

Response parameters

Parameter	Type	Sample response	Description
Events	Array		The list of DDoS events and the details of each event.
EndTime	Integer	1557891306	The timestamp that indicates the end time of the attack. Unit: seconds. The timestamp follows the UNIX time format. It is the number of seconds that have elapsed since 00:00:00 Thursday, 1 January 1970.
Ip	String	1.1.1.1	The IP address of the protection target that encounters the DDoS attack.
Mbps	Integer	110000	The throughput of the DDoS attack. Unit: Mbit/s.
Pps	Integer	0	The packet forwarding rate of the DDoS attack. Unit: packets per second (PPS).

Parameter	Type	Sample response	Description
StartTime	Integer	1557889506	The timestamp that indicates the start time of the attack. Unit: seconds. The timestamp follows the UNIX time format. It is the number of seconds that have elapsed since 00:00:00 Thursday, 1 January 1970.
Status	String	defense_end	The status of the event. Valid values: • **hole_begin** : indicates that the event is in the blackhole state. • **hole_end** : indicates that blackhole ends. • **defense_begin** : indicates that the event is in the cleaning state. • **defense_end** : indicates that cleaning ends.
RequestId	String	6A507DC8-F657-4C13-84E2-D1D1B9400753	The ID of the request.
Total	Long	8	The total number of DDoS events.

Samples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeOnDemandDdosEvent
&EndTime=1557909844
&InstanceId=ddosbgp-cn-x1
&PageNo=1
&PageSize=10
&StartTime=1557305044
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeOnDemandDdosEventResponse>
<RequestId>6A507DC8-F657-4C13-84E2-D1D1B9400753</RequestId>
</Events>
<Event>
<qps>0</qps>
<Status>finished</Status>
<Ip>1.1.1.1</Ip>
<Mbps>110000</Mbps>
<EndTime>1542957514000</EndTime>
<StartTime>1542957499000</StartTime>
</Event>
</Events>
<Total>1</Total>
</DescribeOnDemandDdosEventResponse>
```

`JSON` format

```
{
"RequestId":"6A507DC8-F657-4C13-84E2-D1D1B9400753",
"Events":[
{
"Pps":450,
"IP":"1.1.1.1",
"Status":"defense_end",
"Mbps":110000,
"EndTime":1557891306,
"StartTime":1557889506
}
],
"Total":1
}
```

Error codes

For a list of error codes, visit the API Error Center.

2.7. Tags

2.7.1. ListTagKeys

Queries all tags.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ListTagKeys	The operation that you want to perform. Set the value to **ListTagKeys**.
RegionId	String	Yes	cn-hangzhou	The region ID.
ResourceType	String	Yes	INSTANCE	The type of the resource. Valid value: **INSTANCE**.
PageSize	Integer	No	20	The number of entries to return on each page. Valid values: 1 to **50**. Default value: **10**.
CurrentPage	Integer	No	1	The number of the page to return. Pages start from page **1**. Default value: **1**.
ResourceGroupId	String	No	test	The ID of the resource group.

Response parameters

Parameter	Type	Example	Description
RequestId	String	97935DF1-0289-4AA2-9DD1-72377838B16B	The ID of the request.
CurrentPage	Integer	1	The page number of the returned page.
PageSize	Integer	20	The number of entries returned per page.
TotalCount	Integer	6	The total number of tags.
TagKeys	Array		The list of tags and the details of each tag.
TagKey	String	a	The key of each tag.
TagCount	Integer	1	The total number of tag values that correspond to each key.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=ListTagKeys
&RegionId=cn-hangzhou
&ResourceType=INSTANCE
&<Common request parameters>
```

Sample success responses

`JSON` format

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


`XML` format

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


Error codes

For a list of error codes, visit the API Error Center.

2.7.2. ListTagResources

Queries the tag details of Anti-DDoS Origin Enterprise instances.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ListTagResources	The operation that you want to perform. Set the value to **ListTagResources**.
RegionId	String	Yes	cn-hangzhou	The ID of the region where the Anti-DDoS Origin Enterprise instances reside.
ResourceType	String	Yes	INSTANCE	The type of the resource. Valid value: **INSTANCE**.
ResourceGroupId	String	No	test	The ID of the resource group.
ResourceId.N	RepeatList	No	ddosbgp-cn-v0h1fmwbc024	The IDs of Anti-DDoS Enterprise instances whose tags you want to query. Valid values of N: 1 to 50. You can specify a maximum of 50 instances at a time. Example: ResourceId.1, ResourceId.2, ..., ResourceId.50. **Note** You must specify either a **ResourceId** or a combination of a **Tag.N.Key** and a **Tag.N.Value**.
Tag.N.Key	String	No	testKey1	The key of each tag. Valid values of N: 1 to 20. You can specify a maximum of 20 tag keys at a time. For example, Tag.1.Key, Tag.2.Key, ..., and Tag.20.Key. **Note** You must specify either a **ResourceId** or a combination of a **Tag.N.Key** and a **Tag.N.Value**.

Parameter	Type	Required	Example	Description
Tag.N.Value	String	No	testValue1	The value of each tag. Valid values of N: 1 to 20. You can specify a maximum of 20 tag values at a time. For example, Tag.1.Value, Tag.2.Value, ..., and Tag.20.Value. **Note** You must specify either a **ResourceId** or a combination of a **Tag.N.Key** and a **Tag.N.Value**. You must specify the Tag.N.Key for each tag.
NextToken	String	No	RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCffomr	The token that is used to perform the next query. If the next query does not exist, you can leave the parameter empty.

Response parameters

Parameter	Type	Example	Description
RequestId	String	C3F7E6AE-43B2-4730-B6A3-FD17552B8F65	The ID of the request.
NextToken	String	RGuYpqDdKhzXb8C3.D1BwQgc1tMBsoxdGiEKHHUUCffomr	The token that is returned for the next query. If the next query does not exist, the parameter is not returned.
TagResources	Array		The list of Anti-DDoS Origin Enterprise instances and the tags that are attached to each instance.
ResourceType	String	INSTANCE	The type of the resource. Valid value: **INSTANCE**.
ResourceId	String	ddosbgp-cn-o4017n9q9004	The ID of each Anti-DDoS Origin Enterprise instance.
TagKey	String	testKey4	The key of each tag.
TagValue	String	testValue4	The value of each tag.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=ListTagResources
&RegionId=cn-hangzhou
&ResourceType=INSTANCE
&ResourceId.1=ddosbgp-cn-v0h1fmwbc024
&<Common request parameters>
```

Sample success responses

`JSON` format

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


`XML` format


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


Error codes

For a list of error codes, visit the API Error Center.

2.7.3. TagResources

Adds tags to Anti-DDoS Origin Enterprise instances.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	TagResources	The operation that you want to perform. Set the value to **TagResources**.
RegionId	String	Yes	cn-hangzhou	The ID of the region where the Anti-DDoS Origin Enterprise instances reside.
ResourceId.N	RepeatList	Yes	ddosbgp-cn-v0h1fmwbc024	The IDs of Anti-DDoS Origin Enterprise instances. Valid values of N: 1 to 50. You can specify a maximum of 50 instances at a time. For example, ResourceId.1, ResourceId.2, ..., and ResourceId.50.
ResourceType	String	Yes	INSTANCE	The type of the resource. Set the value to **INSTANCE**.
ResourceGroupId	String	No	test	The ID of the resource group.
Tag.N.Key	String	No	testKey1	The key of each tag. Valid values of N: 1 to 20. You can specify a maximum of 20 tag keys at a time. For example, Tag.1.Key, Tag.2.Key, ..., and Tag.20.Key.
Tag.N.Value	String	No	testValue1	The value of each tag. Valid values of N: 1 to 20. You can specify a maximum of 20 tag values at a time. For example, Tag.1.Value, Tag.2.Value, ..., and Tag.20.Value.

Response parameters

Parameter	Type	Example	Description
RequestId	String	7078CD1E-F609-47A4-9C39-B288CC27C686	The ID of the request.

Examples

Sample requests

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

Sample success responses

`JSON` format

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

`XML` format

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

Error code

For a list of error codes, visit the API Error Center.

2.7.4. UntagResources

Removes tags from Anti-DDoS Origin Enterprise instances.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	UntagResources	The operation that you want to perform. Set the value to **UntagResources**.
RegionId	String	Yes	cn-hangzhou	The ID of the region where the Anti-DDoS Origin Enterprise instances reside.
ResourceId.N	RepeatList	Yes	ddosbgp-cn-v0h1fmwbc024	The IDs of Anti-DDoS Origin Enterprise instances. Valid values of N: 1 to 50. You can specify a maximum of 50 instances at a time. For example, ResourceId.1, ResourceId.2, ..., and ResourceId.50.
ResourceType	String	Yes	INSTANCE	The type of the resource. Set the value to **INSTANCE**.
ResourceGroupId	String	No	test	The ID of the resource group.
TagKey.N	RepeatList	No	testKey1	The key of each tag. Valid values of N: 1 to 20. You can specify a maximum of 20 tag keys at a time. For example, Tag.1.Key, Tag.2.Key, ..., and Tag.20.Key.
All	Boolean	No	false	Specifies whether to remove all tags from the specified Anti-DDoS Origin Enterprise instances.

Response parameters

Parameter	Type	Example	Description
RequestId	String	F2D86AED-BA27-4584-BADC-B43BDA7EEBCA	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=UntagResources
&RegionId=cn-hangzhou
&ResourceId.1=ddosbgp-cn-v0h1fmwbc024
&ResourceType=INSTANCE
&TagKey.1=testKey1
&All=false
&<Common request parameters>
```

Sample success responses

`JSON` format

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

`XML` format

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

Error code

For a list of error codes, visit the API Error Center.