Anti-DDoS 流量清洗

API 参考

发布日期　2024-02-21

目 录

1 API

1.1 API 接口

1.1.1 查询配置可选范围

功能介绍

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

URI

- URI格式
- 参数说明

参数	是否必选	类型	说明
project_id	是	String	用户的ID

请求消息

请求参数

无

响应消息

- 要素说明

参数	是否必选	类型	说明
traffic_limited_list	是	列表数据结构	流量限制列表
http_limited_list	是	列表数据结构	HTTP限制列表

参数	是否必选	类型	说明
connection_limited_list	是	列表数据结构	连接数限制列表

- traffic_limited_list字段数据结构说明

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

- http_limited_list字段数据结构说明

参数	是否必选	类型	说明
http_request_pos_id	是	Integer	HTTP请求数分段ID
http_packet_per_second	是	Integer	每秒HTTP请求数（个/s）阈值

- connection_limited_list字段数据结构说明

参数	是否必选	类型	说明
cleaning_access_pos_id	是	Integer	清洗时访问限制分段ID
new_connection_limited	是	Integer	单一源IP新建连接个数
total_connection_limited	是	Integer	单一源IP连接数总个数

示例

- 请求示例
- 响应样例

```
{
  "traffic_limited_list": [
    {
      "traffic_pos_id": 1,
      "traffic_per_second": 10,
      "packet_per_second": 2000
    },
    {
      "traffic_pos_id": 2,
      "traffic_per_second": 30,
      "packet_per_second": 6000
    },
    {
      "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
  },
  {
    "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
  }
],
```

```
"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
  }
 ]
}
```


说明

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

返回值

请参考**状态码**。

1.1.2 开通服务

功能介绍

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

URI

- URI格式

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

- 参数说明

参数	是否必选	类型	说明
project_id	是	String	用户的ID

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

请求消息

表 1-1 请求参数

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

响应消息

表 1-2 响应参数

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

示例

- 请求示例

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

- 响应示例

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

返回值

请参考**状态码**。

1.1.3 查询服务

功能介绍

查询配置的防护策略，用户可以查询指定EIP的防护策略。

URI

- URI格式

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

- 参数说明

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

请求消息

请求参数

无

响应消息

表 1-3 响应参数

参数	是否必选	类型	说明
enable_L7	是	Boolean	是否开启L7层防护
traffic_pos_id	是	Integer	流量分段ID，取值范围1～9或取值99
http_request_pos_id	是	Integer	HTTP请求数分段ID，取值范围：1～15
cleaning_access_pos_id	是	Integer	清洗时访问限制分段ID，取值范围：1～8或取值99

参数	是否必选	类型	说明
app_type_id	是	Integer	应用类型ID，可选取值： • 0 • 1

示例

- 请求示例
  ```
  GET /v1/67641fe6886f43fcb78edbbf0ad0b99f/antiddos/1df977c2-fdc6-4483-bc1c-ba46829f57b8
  ```
- 响应示例
  ```
  {
    "enable_L7": true,
    "traffic_pos_id": 1,
    "http_request_pos_id": 1,
    "cleaning_access_pos_id": 1,
    "app_type_id": 1
  }
  ```

返回值

请参考**状态码**。

1.1.4 更新服务

功能介绍

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

URI

- URI格式

  PUT /v1/{project_id}/antiddos/{floating_ip_id}
- 参数说明

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

请求示例

表 1-4 请求参数

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

响应消息

表 1-5 响应参数

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

示例

- 请求示例

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

- 响应示例

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

返回值

请参考状态码。

1.1.5 查询任务

功能介绍

用户查询指定的防护配置任务，得到任务当前执行的状态。

URI

- URI格式

  说明

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

- 参数说明

参数	是否必选	类型	说明
project_id	是	String	用户的ID

请求消息

表 1-6 请求参数

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

响应消息

- 要素说明

名称	类型	说明
task_status	String	任务状态，有以下几种： • success • failed • waiting • running • preprocess • ready
task_msg	String	任务的附加信息

示例

- 响应示例

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

返回值

请参考**状态码**。

1.1.6 查询 EIP 防护状态列表

功能介绍

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

URI

- URI格式

  GET /v1/{project_id}/antiddos

  说明

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

- 参数说明

参数	是否必选	类型	说明
project_id	是	String	用户的ID

请求消息

表 1-7 请求参数

参数	是否必选	类型	说明
status	否	String	可选范围： • normal：表示正常 • configging：表示设置中 • notConfig：表示未设置 • packetcleaning：表示清洗 • packetdropping：表示黑洞 不带此参数默认所有列表，以neutron查询到的顺序为准。
limit	否	Integer	返回结果个数限制，取值范围：1~100

参数	是否必选	类型	说明
offset	否	Integer	偏移量，取值范围：0~2147483647
ip	否	String	IP地址，支持IPv4格式和IPv6格式输入，支持部分查询。例如“?ip=192.168”，会返回192.168.111.1和10.192.168.8所对应的EIP防护状态。

响应消息

- 要素说明

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

- ddosStatus字段数据结构说明

参数	是否必选	类型	说明
floating_ip_address	是	String	浮动IP地址
floating_ip_id	是	String	EIP的ID
network_type	是	String	EIP所属类型，可选范围： • EIP：未绑定到ECS的EIP或绑定到ECS的EIP • ELB：绑定到ELB的EIP
status	是	String	防护状态，可选范围： • normal：表示正常 • configging：表示设置中 • notConfig：表示未设置 • packetcleaning：表示清洗 • packetdropping：表示黑洞

示例

- 请求示例

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

- 响应示例

```
{
  "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"
    }
  ]
}
```


返回值

请参考**状态码**。

1.1.7 查询指定 EIP 防护状态

功能介绍

查询指定EIP的防护状态。

URI

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

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

请求消息

请求参数

无

响应消息

- 要素说明

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

示例

- 请求示例

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

- 响应示例

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

返回值

请参考**状态码**。

1.1.8 查询指定 EIP 防护流量

功能介绍

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

URI

- URI格式

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

- 参数说明

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

请求消息

请求参数

无

响应

- 要素说明

名称	参数类型	说明
data	数据结构	24小时内的流量数据

- data字段数据结构说明

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

示例

- 请求示例

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

- 响应示例

```
{"data": [
    {
    "period_start": 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
  }]
}
```

返回值

请参考状态码。

1.1.9 查询指定 EIP 异常事件

功能介绍

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

URI

- URI格式

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

  说明

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

- 参数说明

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

请求消息

表 1-8 请求参数

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

响应消息

- 要素说明

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

- logs字段数据结构说明

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

示例

- 请求示例

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

- 响应示例

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

返回值

请参考**状态码**。

1.1.10 查询周防护统计情况

功能介绍

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

URI

- URI格式

  GET /v1/{project_id}/antiddos/weekly

  说明

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

- 参数说明

参数	是否必选	类型	说明
project_id	是	String	用户的ID

请求消息

表 1-9 请求参数

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

响应消息

- 要素说明

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

- weekdata字段数据结构说明

参数	是否必选	类型	说明
ddos_intercept_times	是	Integer	DDoS拦截次数
ddos_blackhole_times	是	Integer	DDoS黑洞次数

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

- top10字段数据结构说明

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

示例

- 请求示例

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

- 响应示例

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

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


返回值

请参考**状态码**。

1.2 告警提醒 API 接口

1.2.1 查询告警配置信息

功能介绍

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

URI

- URI格式

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

- 参数说明

参数	是否必选	类型	说明
project_id	是	String	用户的ID

请求消息

请求参数

无

响应消息

- 要素说明

参数	是否必选	类型	说明
warn_config	是	列表数据结构	告警配置信息
topic_urn	是	String	告警群组的唯一标识
display_name	是	String	告警群组描述

- warn_config字段数据结构说明

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

示例

- 请求示例

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

- 响应示例

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

说明

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

返回值

请参考状态码。

1.2.2 更新告警配置信息

功能介绍

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

URI

- URI格式

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

- 参数说明

参数	是否必选	类型	说明
project_id	是	String	用户的ID。

请求消息

- 要素说明

参数	是否必选	类型	说明
warn_config	是	列表数据结构	告警配置信息。
topic_urn	是	String	告警群组的唯一标识。
display_name	是	String	告警群组描述。

- warn_config字段数据结构说明

参数	是否必选	类型	说明
antiDDoS	是	Boolean	DDoS攻击
bruce_force	否	Boolean	暴力破解（系统登录，FTP，DB）
remote_login	否	Boolean	异地登录提醒
weak_password	否	Boolean	弱口令（系统，数据库）

参数	是否必选	类型	说明
high_privilege	否	Boolean	数据库进程权限过高
back_doors	否	Boolean	网页后门
waf	否	Boolean	保留字段

说明

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

示例

请求示例

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

返回值

请参考**状态码**。

A 附录

A.1 状态码

- 正常

返回值	说明
200	请求成功。

- 异常

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

状态码	编码	说明
502	Bad Gateway	请求未完成，服务器从上游服务器收到一个无效的响应。
503	Service Unavailable	请求未完成，系统暂时异常。
504	Gateway Timeout	网关超时。

A.2 Anti-DDoS 错误码

状态码	错误码	错误信息	描述	处理措施
200	Anti-DDoS.0	Succeeded	成功	无需处理
200	Anti-DDoS.10000000	The task has been received and is being handled	任务已接收，正在处理	无需处理
400	Anti-DDoS.10000001	Enter a valid request message	请求消息格式非法	检查参数
400	Anti-DDoS.10001008	An incorrect task ID is used	不正确的任务ID	检查参数
400	Anti-DDoS.10001010	Invalid time	时间非法	检查参数
401	Anti-DDoS.10000004	Public test service denied	公测服务被拒绝	申请公测
403	Anti-DDoS.10000002	Failed to authenticate the token in the request	请求所带的Token认证失败	重新申请Token
403	Anti-DDoS.10000009	The account is restricted	账户受限	申请权限
403	Anti-DDoS.10000010	The account is frozen	账户冻结	申请解冻
403	Anti-DDoS.10000012	Unknown user type	未知用户类型	申请权限

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

B 修订记录

发布日期	修改说明
2020-09-30	第一次正式发布。