Web 应用防火墙

接口参考

文档版本 02

发布日期 2022-12-28

华为云计算技术有限公司

商标声明


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

注意

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

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

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 使用前必读

1.1 概述

Web应用防火墙（Web Application Firewall，WAF），通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。

您可以使用本文档提供API对WAF进行相关操作，如查询、更改防护域名等。支持的全部操作请参见**API概览**。

在调用WAF API之前，请确保已经充分了解WAF相关概念，详细信息请参见《Web应用防火墙用户指南》的“产品简介”章节。

1.2 调用说明

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

1.3 终端节点

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

1.4 约束与限制

详细的约束限制请参见具体API的说明。

1.5 基本概念

- 区域（Region）

  从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属

Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。

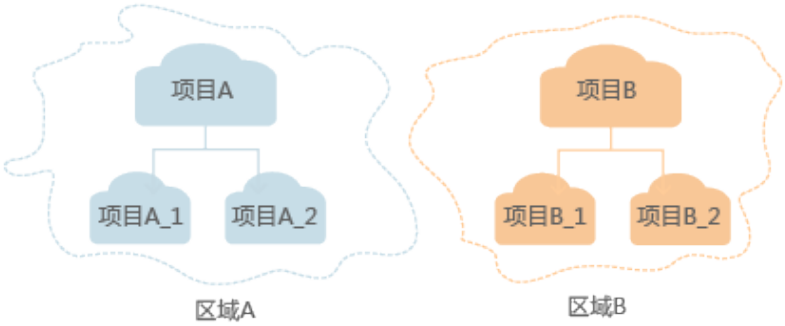
- 可用区（AZ，Availability Zone）

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

- 项目

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

图 1-1 项目隔离模型



2 API 概览

通过使用WAF提供的接口，您可以完整的使用WAF的所有功能。

类型	说明
用户资源配额	获取套餐信息和已添加资源数量接口。
WAF防护域名	防护域名API接口，包括查询、创建防护域名等接口。
证书管理	证书管理API接口，包括上传、查询证书等接口。
防护状态与域名接入	修改防护状态和域名接入接口。
防护策略	防护策略API接口，包括查询、创建防护策略等接口。
黑白名单	IP黑白名单API接口，包括查询、创建IP黑白名单等接口。
CC规则	CC规则API接口，包括查询、创建CC规则等接口。
精准防护规则	精准访问防护规则API接口，包括查询、创建精准访问防护规则等接口。
隐私屏蔽规则	隐私屏蔽规则API接口，包括查询、创建隐私屏蔽规则等接口。
网页防篡改规则	网页防篡改规则API接口，包括查询、创建网页防篡改规则等接口。
误报屏蔽规则	误报屏蔽规则API接口，包括查询、创建误报屏蔽规则等接口。
事件日志查询	查询事件日志API接口，包括查询攻击事件日志、事件类型分布等接口。
告警通知配置	查询和更新告警配置信息接口。
获取选项信息	查询告警通知中事件类型选项信息，以及获取真实源IP的HTTP请求头的选项信息。
对接Cloud Eye	查询对接Cloud Eye的实例名称和状态。

3 如何调用 API

3.1 构造请求

本节介绍如何构造REST API的请求，并以调用IAM服务的获取用户Token说明如何调用API，该API获取用户的Token，Token可以用于调用其他API时鉴权。

请求 URI

请求URI由如下部分组成。

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

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

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

说明

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

请求方法

HTTP请求方法（也称为操作或动词），它告诉服务你正在请求什么类型的操作。

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

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

```
POST https://{{endpoint}}/v3/auth/tokens
```

请求消息头

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

如下公共消息头需要添加到请求中。

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

  说明

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

  AK/SK认证的详细说明请参见**AK/SK认证**。

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

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

请求消息体

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

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

对于获取用户Token接口，您可以从接口的请求部分看到所需的请求参数及参数说明。将消息体加入后的请求如下所示，加粗的斜体字段需要根据实际值填写，其中***username***为用户名，***domainname***为用户所属的账号名称，*********为用户登录密码，***xxxxxxxxxxxxxxxxx***为project的名称，如“eu-west-0”，您可以从**地区和终端节点**获取，对应地区和终端节点页面的“区域”字段的值。

说明

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

```
POST https://{{endpoint}}/v3/auth/tokens
Content-Type: application/json
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "********",
                    "domain": {
                        "name": "domainname"
                    }
                }
            }
        },
        "scope": {
            "project": {
                "name": "xxxxxxxxxxxxxxxxxx"
            }
        }
    }
}
```

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

3.2 认证鉴权

调用接口有如下两种认证方式，您可以选择其中一种进行认证鉴权。

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

Token 认证

说明

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

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

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

```
{
    "auth": {
        "identity": {
```

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

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

```
POST https://{{endpoint}}/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

AK/SK 认证

说明

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

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

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

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

须知

签名SDK只提供签名功能，与服务提供的SDK不同，使用时请注意。

3.3 返回结果

状态码

请求发送以后，您会收到响应，包含状态码、响应消息头和消息体。

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

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

响应消息头

对应请求消息头，响应同样也有消息头，如“Content-type”。

对于获取用户Token接口，返回如图3-1所示的消息头，其中“x-subject-token”就是需要获取的用户Token。有了Token之后，您就可以使用Token认证调用其他API。

图 3-1 获取用户 Token 响应消息头

响应消息体（可选）

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

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

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

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

```
{
    "error": {
        "message": "The request you have made requires authentication.",
        "title": "Unauthorized"
    }
}
```


其中，error_code表示错误码，error_msg表示错误描述信息。

4 API 说明

4.1 云模式

4.1.1 用户资源配额

4.1.1.1 获取套餐信息

功能介绍

获取某个用户的套餐信息。

URI

- URI格式
  GET /v1/{project_id}/waf/bundle
- 参数说明

  表 4-1 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-2 响应参数说明

名称	参数类型	说明
type	Integer	版本信息。
name	String	套餐名称。
options	表3	套餐防护策略开关可开启范围。
rule	表4	套餐防护策略中规则条数限制。
host	表5	套餐防护策略中规则域名限制。
other	表6	套餐中的其他限制。

表 4-3 options

名称	参数类型	说明
webattack	Boolean	套餐防护策略开关，Web攻击是否可以开启。 ● true：表示可以开启。 ● false：表示不能开启。
common	Boolean	套餐防护策略开关，Web攻击的常规攻击检测是否可以开启。 ● true：表示可以开启。 ● false：表示不能开启。
crawler	Boolean	套餐防护策略开关，Web攻击的爬虫检测主开关是否可以开启。 ● true：表示可以开启。 ● false：表示不能开启。 **说明** 当crawler开关关闭时，crawler开关的所有子开关功能将无效。
crawler_engine	Boolean	套餐防护策略开关，Web攻击的爬虫检测搜索引擎是否可以开启。 ● true：表示可以开启。 ● false：表示不能开启。
crawler_scanner	Boolean	套餐防护策略开关，Web攻击的爬虫检测扫描器是否可以开启。 ● true：表示可以开启。 ● false：表示不能开启。

名称	参数类型	说明
crawler_script	Boolean	套餐防护策略开关，Web攻击的爬虫检测脚本工具是否可以开启。 ● true：表示可以开启。 ● false：表示不能开启。
crawler_other	Boolean	套餐防护策略开关，Web攻击的爬虫检测其他爬虫是否可以开启。 ● true：表示可以开启。 ● false：表示不能开启。
webshell	Boolean	套餐防护策略开关，Web攻击的Webshell是否可以开启。 ● true：表示可以开启。 ● false：表示不能开启。
cc	Boolean	套餐防护策略开关，Web攻击的CC防护是否可以开启。 ● true：表示可以开启。 ● false：表示不能开启。
custom	Boolean	套餐防护策略开关，Web攻击的精准防护是否可以开启。 ● true：表示可以开启。 ● false：表示不能开启。
whiteblackip	Boolean	套餐防护策略开关，Web攻击的IP黑白名单是否可以开启。 ● true：表示可以开启。 ● false：表示不能开启。
privacy	Boolean	套餐防护策略开关，Web攻击的隐私屏蔽是否可以开启。 ● true：表示可以开启。 ● false：表示不能开启。
Ignore	Boolean	套餐防护策略开关，Web攻击的误报屏蔽是否可以开启。 ● true：表示可以开启。 ● false：表示不能开启。
antitamper	Boolean	套餐防护策略开关，Web攻击的网页防篡改是否可以开启。 ● true：表示可以开启。 ● false：表示不能开启。

名称	参数类型	说明
full_detection	Boolean	套餐防护策略开关，精准防护的全检测模式是否可以开启。 ● true：全检测。当用户的请求符合精准防护中的拦截条件时，不会立即拦截，WAF会继续执行其他防护的检测，待其他防护的检测完成后进行拦截。 ● false：短路检测。当用户的请求符合精准防护中的拦截条件时，便立刻终止检测，进行拦截。
log_download	Boolean	套餐防护策略开关，日志下载是否可用。 ● true：表示可用。 ● false：表示不可用。

表 4-4 rule

名称	参数类型	说明
antitamper	Integer	可设置的网页防篡改规则的总条数。最大值为100。
cc	Integer	可设置的CC规则的总条数。最大值为100。
custom	Integer	可设置的精准防护规则的总条数。最大值为100。
ignore	Integer	可设置的误报屏蔽规则的总条数。最大值为1000。
privacy	Integer	可设置的隐私屏蔽规则的总条数。最大值为1000。
whiteblackip	Integer	可设置的IP黑白名单的总条数。最大值为100。

说明

用户可以联系管理员，申请增大表4-4中的最大值配额。

表 4-5 host

名称	参数类型	说明
wildcard	Boolean	是否支持泛域名。 ● true：表示支持泛域名。 ● false：表示不支持泛域名。
ports	表7	支持端口的范围。
protocol	表8	对外协议。
server	Integer	支持的后端服务器数量。最大取值为30。
host	Integer	支持的子域名数量。最大取值为100。
domain	Integer	支持的域名数量。最大取值为100。
cert_num	Integer	支持的证书数量。最大取值为100。
policy_apply_to	Boolean	是否支持一个策略对应多个域名。 ● true：表示支持一个策略对应多个域名。 ● false：表示不支持一个策略对应多个域名。
policy_num	Integer	支持的策略数量。最大数量为5000。

表 4-6 other

名称	参数类型	说明
default_cc	Integer	防护策略中默认CC规则的最大的请求次数。

表 4-7 ports

名称	参数类型	说明
http	Array	支持的HTTP端口列表。
https	Array	支持的HTTPS端口列表。
max_num	Integer	支持端口的个数。

名称	参数类型	说明
none_standard	Boolean	是否支持非标准端口。 ● true：支持非标准端口。 ● false：不支持非标准端口。

表 4-8 protocol

名称	参数类型	说明
http	Boolean	是否支持http协议。 ● true：表示支持http协议。 ● false：表示不支持http协议。
https	Boolean	是否支持https协议。 ● true：表示支持https协议。 ● false：表示不支持https协议。
http_https	Boolean	是否同时支持http和https协议。 ● true：表示同时支持http和https协议。 ● false：表示同时不支持http和https协议。

示例

如下以获取套餐信息为例。

响应样例

```
{
  "type": 1,
  "name": "Basic",
  "options": {
    "webattack": true,
    "common": true,
    "crawler": true,
    "webshell": false,
    "cc": false,
    "custom": false,
    "whiteblackip": true,

    "privacy": true,
    "ignore": true,
    "antitamper": false,
"log_download": true,
  },
  "rule": {
    "cc": 0,
    "custom": 0,
    "whiteblackip": 10,
```

```
    "privacy": 10,
    "ignore": 1000,
"antitamper": 0,
  },
  "host": {
    "wildcard": false,
    "protocol": {
      "http": true,
      "https": false,
      "http_https": false
    },
    "ports": {
      "none_standard": false,
      "http": [],
      "https": [],
      "max_num": 0
    },
    "domain": 1,
    "host": 10,
    "server": 10,
    "route": false
  },
  "other": {
      "default_cc": 25000
    }
}
```


状态码

表4-9描述的是API返回的正常状态码。

表 4-9 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.1.2 获取已添加的资源数量

功能介绍

获取某个用户已添加的资源数量。

URI

- URI格式
  GET /v1/{project_id}/waf/bundle/usage/{resource_type}
- 参数说明

表 4-10 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
resource_type	是	String	资源类型，取值范围为：“instance”，“policy”，“certificate”。

请求消息

请求参数

无

响应消息

响应参数

表 4-11 响应参数说明

名称	参数类型	说明
count	Integer	已经创建资源数量。

示例

如下以获取已创建的证书数量，返回记录条数为“2”为例。

响应样例

```
{
  "count": 2
}
```

状态码

表4-12描述的是API返回的正常状态码。

表 4-12 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.2 WAF 防护域名

4.1.2.1 查询防护域名列表

功能介绍

查询防护域名列表。

URI

- URI格式

  GET /v1/{project_id}/waf/instance?offset={offset}&limit={limit}&hostname={hostname}&policyname={policyname}

- 参数说明

  表 4-13 Path 参数

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
offset	否	Long	指定返回的页数，取值范围为：[0, 65535]，默认值为0。
limit	否	Long	指定查询返回每页记录的最大条数，取值范围为：(0, 50]，默认值为10。当limit=-1时，将返回offset=0，limit=65535的数据。
hostname	否	String	防护域名。
policyname	否	String	防护策略的名称。

请求消息

请求参数

无

响应消息

响应参数

表 4-14 响应参数说明

名称	参数类型	说明
total	Integer	返回的域名总数。
items	表3	返回的防护域名对象列表。

表 4-15 items

名称	参数类型	说明
id	String	防护域名的ID。
hostname	String	返回的防护域名。
cname	String	生成的CNAME值。 例如：efec1196267b41c399f2980ea4048517.waf.cloud.com
txt_code	String	TXT记录，当“proxy”为“true”时，才会返回该值。
sub_domain	String	子域名，当“proxy”为“true”时，才会返回该值。
policy_id	String	policy的ID。
protect_status	Integer	防护状态。 ● “-1”：表示bypass。 ● “0”：表示关闭。 ● “1”：表示开启。
access_status	Integer	接入状态。 ● “0”：表示未接入。 ● “1”：表示已接入。
proxy	Boolean	是否使用代理。 ● true：表示使用了代理。 ● false：表示没有使用代理。
timestamp	Long	创建防护域名的时间。

示例

如下以查询防护域名列表，返回记录条数为“2”为例。

响应样例

```
{
   "total": 2,
   "items": [
      {
        "id": "388a7789d55b41d1918b3088a8f1e7f3",
        "hostname": "www.a.com",
        "cname": "3249d21e5eb34d21be12fdc817fcb67d.waf.cloud.com",
        "txt_code": "3249d21e5eb34d21be12fdc817fcb67d",
        "sub_domain": "3249d21e5eb34d21be12fdc817fcb67d.www.a.com",
        "policy_id": "xxxxxxxxxxxxx",
        "protect_status": 0,
        "access_status": 0,
        "proxy": true,
        "timestamp": 1499817600
      },
```

```
    {
      "id": "296a7710d55b41d1918b3036a8f1e7e5",
      "hostname": "www.b.com",
      "cname": "efec1196267b41c399f2980ea4048517.waf.cloud.com",
      "policy_id": "xxxxxxxxxxxxxx",
      "protect_status": 1,
      "access_status": 1,
      "proxy": false,
      "timestamp": 1499817612
    }
  ]
}
```

状态码

表4-16描述的是API返回的正常状态码。

表 4-16 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见**状态码**。

4.1.2.2 创建防护域名

功能介绍

创建防护域名。

URI

- URI格式
  POST /v1/{project_id}/waf/instance
- 参数说明

  表 4-17 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。

请求消息

请求参数

表 4-18 请求参数说明

名称	是否必选	参数类型	说明
hostname	是	String	创建的防护域名的名称。 例如：www.example.com或者*.example.com
certificate_id	否	String	证书ID，当“client_protocol”为“HTTPS”时，需要设置该参数。
server	是	Array	源站信息列表，包含“client_protocol”、“server_protocol”、“address”、“port”四个字段。 ● “client_protocol”：客户端协议类型。包括HTTP、HTTPS两种协议类型，例如：HTTPS。 ● “server_protocol”：服务器协议类型，WAF转发客户端请求的协议。包括HTTP、HTTPS两种协议类型，例如：HTTP。 ● “address”：客户端访问的网站服务器的公网IP地址或者域名。 ● “port”：客户端访问的网站服务器的端口号，取值为(0,65535)，例如：8080。
proxy	是	Boolean	是否使用代理。 ● true：表示使用了代理。 ● false：表示没有使用代理。
sip_header_name	否	String	获取真实源IP的http请求头的类别。当“proxy”为“true”时，才需要传该字段。 取值范围为：“default”，“cloudflare”，“akamai”，“custom”。

名称	是否必选	参数类型	说明
sip_header_list	否	Array	获取真实源IP的http请求头。当“proxy”为“true”时，才需要传该字段。 ● 当“sip_header_name”为“default”时，“sip_header_list”为["X-Forwarded-For"]； ● 当“sip_header_name”为“cloudflare”时，“sip_header_list”为["CF-Connecting-IP", "X-Forwarded-For"]； ● 当“sip_header_name”为“akamai”时，“sip_header_list”为["True-Client-IP"]； ● 当“sip_header_name”为“custom”时，用户可以自定义。

响应消息

响应参数

表 4-19 响应参数说明

名称	参数类型	说明
id	String	实例ID。
hostname	String	创建的防护域名。
cname	String	CNAME的值。例如：efec1196267b41c399f2980ea4048517.waf.cloud.com。
txt_code	String	TXT记录。当“proxy”为“true”时，才会返回“txt_code”。
sub_domain	String	子域名。当“proxy”为“true”时，才返回“sub_domain”。
policy_id	String	policy的ID。
protect_status	Integer	防护状态。 ● “-1”：表示bypass。 ● “0”：表示关闭。 ● “1”：表示开启。

名称	参数类型	说明
access_status	Integer	接入状态。 ● “0”：表示未接。 ● “1”：表示已接入。
proxy	Boolean	是否使用代理。 ● true：表示使用了代理。 ● false：表示没有使用代理。
protocol	String	返回的客户端协议类型，包含“HTTP”、“HTTPS”和“HTTP,HTTPS”。
certificate_id	String	证书ID， 当“client_protocol”为“HTTPS”时，需要设置该参数。
server	Array	源站信息列表，包含“client_protocol”、“server_protocol”、“address”、“port”四个字段。
sip_header_name	String	获取真实源IP的http请求头的类别。当“proxy”为“true”时，才会返回该值。 取值范围为：“default”，“cloudflare”，“akamai”，“custom”。
sip_header_list	Array	获取真实源IP的http请求头。当“proxy”为“true”时，才会返回该值。 ● 当“sip_header_name”为“default”时，“sip_header_list”为["X-Forwarded-For"]； ● 当“sip_header_name”为“cloudflare”时，“sip_header_list”为["CF-Connecting-IP", "X-Forwarded-For"]； ● 当“sip_header_name”为“akamai”时，“sip_header_list”为["True-Client-IP"]； ● 当“sip_header_name”为“custom”时，用户可以自定义。
timestamp	Long	创建防护域名的时间。

示例

如下以创建域名www.b.com为例。

- 请求样例

```
{
 "hostname": "www.b.com",
 "certificate_id": "07fb6809a89241fca86ac6f69e34963d",
 "server": [
    {"client_protocol": "HTTPS", "server_protocol": "HTTP", "address": "X.X.X.X", "port": "8080"},
    {"client_protocol": "HTTP", "server_protocol": "HTTP", "address": "X.X.X.X", "port": "80"}
 ],
```

```
  "proxy": true,
  "sip_header_name": "default",
  "sip_header_list": ["X-Forwarded-For"]
}
```

- 响应样例

```
{
        "id": "388a7789d55b41d1918b3088a8f1e7f3",
        "hostname": "www.b.com",
        "cname": "3249d21e5eb34d21be12fdc817fcb67d.waf.cloud.com",
        "txt_code": "3249d21e5eb34d21be12fdc817fcb67d",
        "sub_domain": "3249d21e5eb34d21be12fdc817fcb67d.www.b.com",
        "policy_id": "xxxxxxxxxxxxx",
        "certificate_id": "xxxxxxxxxxxxxxxxxx",
        "protect_status": 0,
        "access_status": 0,
        "protocol": "HTTP,HTTPS",
        "server": [
          {"client_protocol": "HTTPS", "server_protocol":"HTTP", "address":"X.X.X.X", "port":443},
          {"client_protocol": "HTTP", "server_protocol":"HTTP", "address":"X.X.X.X", "port":80}
        ],
        "proxy": true,
        "sip_header_name": "default",
        "sip_header_list": ["X-Forwarded-For"],
        "timestamp": 1499817600


}
```

状态码

表4-20描述的是API返回的正常状态码。

表 4-20 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.2.3 查询防护域名

功能介绍

查询某个防护域名的详细信息。

URI

- URI格式
  GET /v1/{project_id}/waf/instance/{instance_id}
- 参数说明

表 4-21 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
instance_id	是	String	防护实例ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-22 响应参数说明

名称	参数类型	说明
id	String	防护实例的ID。
hostname	String	域名。
cname	String	CNAME的值，例如：efec1196267b41c399f2980ea4048517.waf.cloud.com。
txt_code	String	TXT记录。当“proxy”为“true”时，才会返回“txt_code”。
sub_domain	String	子域名。当“proxy”为“true”时，才返回“sub_domain”。
policy_id	String	policy的ID。
protect_status	Integer	防护状态。 ● “0”：表示关闭。 ● “1”：表示开启。 ● “-1”：表示bypass。
access_status	Integer	接入状态。 ● “0”：表示未接入。 ● “1”：表示已接入。
protocol	String	协议类型，取值范围为：“HTTP”，“HTTPS”和“HTTP,HTTPS”。
certificate_id	String	证书ID，只有当“client_protocol”为“HTTPS”时，才会返回该值。

名称	参数类型	说明
server	Array	源站信息列表，包含“client_protocol”、“server_protocol”、“address”、“port”四个字段。 ● “client_protocol”：客户端协议类型。包括HTTP、HTTPS两种协议类型，例如：HTTPS。 ● “server_protocol”：服务器协议类型，WAF转发客户端请求的协议。包括HTTP、HTTPS两种协议类型，例如：HTTP。 ● “address”：客户端访问的网站服务器的公网IP地址或域名。 ● “port”：客户端访问的网站服务器的端口号，取值为(0, 65535)，例如：8080。
proxy	Boolean	是否使用代理。 ● false：表示没有使用代理。 ● true：表示使用了代理。
sip_header_name	String	获取真实源IP的http请求头的类别。当“proxy”为“true”时，才会返回该值。 取值范围为：“default”，“cloudflare”，“akamai”，“custom”。
sip_header_list	Array	获取真实源IP的http请求头。当“proxy”为“true”时，才会返回该值。 ● 当“sip_header_name”为“default”时，“sip_header_list”为["X-Forwarded-For"]； ● 当“sip_header_name”为“cloudflare”时，“sip_header_list”为["CF-Connecting-IP", "X-Forwarded-For"]； ● 当“sip_header_name”为“akamai”时，“sip_header_list”为["True-Client-IP"]； ● 当“sip_header_name”为“custom”时，用户可以自定义。
timestamp	Long	创建防护域名的时间。
block_page	**BlockPage** object	告警页面配置

表 4-23 BlockPage

参数	参数类型	描述
template	String	模板名称

参数	参数类型	描述
custom_page	CustomPage object	自定义告警页面
redirect_url	String	页面URL

表 4-24 CustomPage

参数	参数类型	描述
status_code	String	返回状态码
content_type	String	“自定义”告警页面内容类型，可选择text/html、text/xml和application/json三种类型
content	String	根据选择的“content_type”配置对应的页面内容。

示例

如下以查询防护域名www.a.com为例。

响应样例

```
{
        "id": "388a7789d55b41d1918b3088a8f1e7f3",
        "hostname": "www.a.com",

        "cname": "3249d21e5eb34d21be12fdc817fcb67d.waf.cloud.com",
        "txt_code": "3249d21e5eb34d21be12fdc817fcb67d",
        "sub_domain": "3249d21e5eb34d21be12fdc817fcb67d.www.a.com",
        "policy_id": "xxxxxxxxxxxxxx",
        "certificate_id": "xxxxxxxxxxxxxxxxxxx",
        "protect_status": 0,
        "access_status": 0,
        "protocol": "HTTP,HTTPS",

        "server": [
          {"client_protocol": "HTTPS", "server_protocol":"HTTP", "address":"X.X.X.X.", "port":443},
          {"client_protocol": "HTTP", "server_protocol":"HTTP", "address":"X.X.X.X", "port":80}
        ],
       "proxy": true,
       "sip_header_name": "default",
       "sip_header_list": ["X-Forwarded-For"],
       "timestamp": 1499817600
       "block_page" : {
       "template" : "default"
        },


}
```

状态码

表4-25描述的是API返回的正常状态码。

表 4-25 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见**状态码**。

4.1.2.4 更改防护域名的配置

功能介绍

更改某个防护域名的基本配置。

URI

- URI格式
  PUT /v1/{project_id}/waf/instance/{instance_id}
- 参数说明

  表 4-26 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
instance_id	是	String	防护实例的ID。

请求消息

请求参数

表 4-27 请求参数说明

名称	是否必选	参数类型	说明
certificate_id	否	String	证书ID， 当“client_protocol”为“HTTP”时，不需要设置此参数。

名称	是否必选	参数类型	说明
server	否	Array	源站信息列表，包含“client_protocol”、“server_protocol”、“address”、“port”四个字段。 ● “client_protocol”：客户端协议类型。包括HTTP、HTTPS两种协议类型，例如：HTTPS。 ● “server_protocol”：服务器协议类型，WAF转发客户端请求的协议。包括HTTP、HTTPS两种协议类型，例如：HTTP。 ● “address”：客户端访问的网站服务器的公网IP地址或者域名。 ● “port”：客户端访问的网站服务器的端口号，取值为(0, 65535)，例如：8080。
proxy	否	Boolean	是否使用代理。 ● false：表示没有使用代理。 ● true：表示使用了代理。
sip_header_name	否	String	获取真实源IP的http请求头的类别。当“proxy”为“true”时，才需要传该字段。 取值范围为：“default”，“cloudflare”，“akamai”，“custom”。

名称	是否必选	参数类型	说明
sip_header_list	否	Array	获取真实源IP的http请求头。当“proxy”为“true”时，才需要传该字段。 ● 当“sip_header_name”为“default”时，“sip_header_list”为["X-Forwarded-For"]； ● 当“sip_header_name”为“cloudflare”时，“sip_header_list”为["CF-Connecting-IP", "X-Forwarded-For"]； ● 当“sip_header_name”为“akamai”时，“sip_header_list”为["True-Client-IP"]； ● 当“sip_header_name”为“custom”时，用户可以自定义。

响应消息

响应参数

表 4-28 响应参数说明

名称	参数类型	说明
id	String	域名ID。
hostname	String	创建的防护域名。
cname	String	CNAME的值，例如：efec1196267b41c399f2980ea4048517.waf.cloud.com。
txt_code	String	TXT记录。当“proxy”为“true”时，才会返回“txt_code”。
sub_domain	String	子域名。当“proxy”为“true”时，才返回“sub_domain”。
policy_id	String	policy的ID。
protect_status	Integer	防护状态。 ● “0”：表示防护状态处于“关闭”状态。 ● “1”：表示防护状态处于“开启”状态。 ● “-1”：表示bypass。

名称	参数类型	说明
access_status	Integer	接入状态。 ● “0”：表示未接入。 ● “1”：表示已接入。
protocol	Integer	协议类型，取值范围为“HTTP”，“HTTPS”和“HTTP,HTTPS”。
certificate_id	String	证书ID，只有当“protocol”为“HTTPS”时，才会返回该值。
server	Array	源站IP列表，包含“client_protocol”、“server_protocol”、“address”、“port”四个字段。
proxy	Boolean	是否使用代理。 ● false：表示没有使用代理。 ● true：表示使用了代理。
sip_header_name	String	获取真实源IP的http请求头的类别。当“proxy”为“true”时，才会返回该值。 取值范围为：“default”，“cloudflare”，“akamai”，“custom”。
sip_header_list	Array	获取真实源IP的http请求头。当“proxy”为“true”时，才会返回该值。 ● 当“sip_header_name”为“default”时，“sip_header_list”为["X-Forwarded-For"]； ● 当“sip_header_name”为“cloudflare”时，“sip_header_list”为["CF-Connecting-IP", "X-Forwarded-For"]； ● 当“sip_header_name”为“akamai”时，“sip_header_list”为["True-Client-IP"]； ● 当“sip_header_name”为“custom”时，用户可以自定义。
timestamp	Long	创建防护域名的时间。

示例

如下以更改域名www.a.com的配置为例。

- 请求样例

```
{
  "certificate_id": "07fb6809a89241fca86ac6f69e34963d",
  "server": [
     {"client_protocol": "HTTPS","server_protocol": "HTTP", "address": "X.X.X.X","port": "8080"},
     {"client_protocol": "HTTP", "server_protocol": "HTTP", "address": "X.X.X.X", "port": "80"}
  ],
  "proxy": true,
```

```
  "sip_header_name": "default",
  "sip_header_list": ["X-Forwarded-For"]


}
```

- 响应样例

```
{
        "id": "388a7789d55b41d1918b3088a8f1e7f3",
        "hostname": "www.a.com",

        "cname": "3249d21e5eb34d21be12fdc817fcb67d.wafcloud.com",
        "txt_code": "3249d21e5eb34d21be12fdc817fcb67d",
        "sub_domain": "3249d21e5eb34d21be12fdc817fcb67d.www.a.com",
        "policy_id": "xxxxxxxxxxxxx",
        "certificate_id": "xxxxxxxxxxxxxxxxxxx",
        "protect_status": 0,
        "access_status": 0,
        "protocol": "HTTP,HTTPS",

        "server": [
          {"client_protocol": "HTTPS", "server_protocol":"HTTP", "address":"X.X.X.X", "port":443},
          {"client_protocol": "HTTP", "server_protocol":"HTTP", "address":"X.X.X.X", "port":80}
        ],
       "proxy": true,
       "sip_header_name": "default",
        "sip_header_list": ["X-Forwarded-For"],
       "timestamp": 1499817600


}
```

状态码

表4-29描述的是API返回的正常状态码。

表 4-29 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.2.5 删除防护域名

功能介绍

删除某个防护域名。

须知

删除域名会依赖一些组件，比如DNS，这些组件可能会导致域名删除不成功。

URI

- URI格式
  DELETE /v1/{project_id}/waf/instance/{instance_id}?keepPolicy={keepPolicy}
- 参数说明

表 4-30 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
instance_id	是	String	实例/域名的ID。
keepPolicy	否	Boolean	删除防护域名时，是否需要保留策略。 • “keepPolicy”默认为“false”，删除策略。 • “keepPolicy”为“true”时，保留策略。

请求消息

请求参数

无

响应消息

响应参数

无

状态码

表4-31描述的是API返回的正常状态码。

表 4-31 状态码

状态码	编码	状态说明
204	No Content	服务器成功处理了请求，没有返回任何内容。

异常状态码，请参见状态码。

4.1.3 证书管理

4.1.3.1 获取证书列表

功能介绍

获取某个用户的证书列表。

URI

- URI格式
  GET /v1/{project_id}/waf/certificate?offset={offset}&limit={limit}
- 参数说明

  表 4-32 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
offset	否	Long	指定返回的页数，取值范围为：[0, 65535]，默认值为0。
limit	否	Long	指定查询返回每页记录的最大条数，取值范围为：(0, 50]，默认值为10。当limit=-1时，将返回offset=0，limit=65535的数据。

请求消息

请求参数

无

响应消息

响应参数

表 4-33 响应参数说明

名称	参数类型	说明
total	Integer	获得证书的总数。
items	表3	证书对象列表。

表 4-34 items

名称	参数类型	说明
id	String	证书的ID。
name	String	证书名称。
expireTime	Long	证书的到期时间
timestamp	Long	创建证书的时间。

示例

如下以获取证书列表，返回记录条数为“2”为例。

响应样例

```
{
  "total": 2,
   "items": [
      {
        "id": "388a7789d55b41d1918b3088a8f1e7f3",
        "name": "cert_a",
        "timestamp": 1544756441859,
        "expireTime": 1545978662373
      }, {
        "id": "388a7789d55b41d1918b3088a8f1e7f4",
        "name": "cert_b",
        "timestamp": 1544756441859,
        "expireTime": 1545978662356
      }]
}
```

状态码

表4-35描述的是API返回的正常状态码。

表 4-35 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.3.2 上传证书

功能介绍

上传新证书。

URI

- URI格式
  POST /v1/{project_id}/waf/certificate

- 参数说明

  表 4-36 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。

请求消息

请求参数

表 4-37 请求参数说明

名称	是否必选	参数类型	说明
name	是	String	证书的名称。最大长度为256字符。只支持以数字、字母、下划线或中划线命名。
content	是	String	证书的内容。 **说明** • 获得的证书文件参考样例为： -----BEGIN CERTIFICATE----- MIIDezCCAmOgAwIBAgIJAMJcdOLsrN3iMA0GCSqGSIb3DQEBCwUAMFQxCzAJBgNV ... 8qh1Vpk2FXoadOVze2fQFLBkkB7LPExj8Nrf76CJEA== -----END CERTIFICATE----- • 上传证书时，默认用“\n”将每行的内容连在一起，再上传，例如： -----BEGIN CERTIFICATE-----“\n” MIIDezCCAmOgAwIBAgIJAMJcdOLsrN3iMA0GCSqGSIb3DQEBCwUAMFQxCzAJBgNV“\n”...“\n” 8qh1Vpk2FXoadOVze2fQFLBkkB7LPExj8Nrf76CJEA==“\n”-----END CERTIFICATE-----

名称	是否必选	参数类型	说明
key	是	String	证书的私钥。 **说明** • 获得的证书秘钥参考样例为： -----BEGIN RSA PRIVATE KEY----- MIIEowIBAAKCAQEAsj2QPAwXYcPDH0mvf6Jbej6RGgYlb4EFMS85BjKrKNPOTqZf ... 4j0RY9DeUgSLdy625BBmew2it9l/NynIScG4Ow6w8Bu4iBANGv94 -----END RSA PRIVATE KEY----- • 上传证书秘钥时，默认用“\n”将每行的内容连在一起，再上传，例如： ----BEGIN RSA PRIVATE KEY----“\n” MIIEowIBAAKCAQEAsj2QPAwXYcPDH0mvf6Jbej6RGgYlb4EFMS85BjKrKNPOTqZf“\n”...“\n” 4j0RY9DeUgSLdy625BBmew2it9l/NynIScG4Ow6w8Bu4iBANGv94 “\n”-----END RSA PRIVATE KEY-----

响应消息

响应参数

表 4-38 响应参数说明

名称	参数类型	说明
id	String	证书的ID。
name	String	证书的名称。
expireTime	Long	证书的到期时间。
timestamp	Long	创建证书的时间。

示例

如下以上传证书名为“cert_a”的证书为例。

- 请求样例

```
{
 "name": "cert_a",
 "content": "-----BEGIN CERTIFICATE-----
\nMIIDezCCAmOgAwIBAgIJAMJcdOLsrN3iMA0GCSqGSIb3DQEBCwUAMFQxCzAJBgNV
\n...\n8qh1Vpk2FXoadOVze2fQFLBkkB7LPExj8Nrf76CJEA==\n-----END CERTIFICATE-----",
 "key": "----BEGIN RSA PRIVATE KEY----
\nMIIEowIBAAKCAQEAsj2QPAwXYcPDH0mvf6Jbej6RGgYlb4EFMS85BjKrKNPOTqZf
\n...\n4j0RY9DeUgSLdy625BBmew2it9l/NynIScG4Ow6w8Bu4iBANGv94\n-----END RSA PRIVATE
KEY-----"
}
```

- 响应样例

```
{
    "id": "388a7789d55b41d1918b3088a8f1e7f3",
    "name": "cert_b",
    "expireTime": 1565467166765,
    "timestamp": 1545467166765
}
```

状态码

表4-39描述的是API返回的正常状态码。

表 4-39 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.3.3 查询单个证书

功能介绍

查询单个证书的详细信息。

URI

- URI格式

  GET /v1/{project_id}/waf/certificate/{certificate_id}

- 参数说明

  表 4-40 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
certificate_id	是	String	需要查询的证书的ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-41 响应参数说明

名称	参数类型	说明
id	String	证书的ID。
name	String	证书的名称。
expireTime	Long	证书的到期时间。
timestamp	Long	创建证书的时间。

示例

如下以查询证书"cert_b"为例。

响应样例

```
{
    "id": "388a7789d55b41d1918b3088a8f1e7f3",
    "name": "cert_b",
    "timestamp": 1545467166765,
    "expireTime": 1555467166765
}
```

状态码

表4-42描述的是API返回的正常状态码。

表 4-42 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.3.4 修改证书名称

功能介绍

修改证书名称。

URI

- URI格式
  PUT /v1/{project_id}/waf/certificate/{certificate_id}
- 参数说明

表 4-43 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
certificate_id	是	String	需要修改的证书ID。

请求消息

请求参数

表 4-44 请求参数说明

名称	是否必选	参数类型	说明
name	是	String	证书的名称。最大长度为256字符。只支持以数字、字母、下划线或中划线命名。

响应消息

响应参数

表 4-45 响应参数说明

名称	参数类型	说明
id	String	证书的ID。
name	String	证书的名称。
expireTime	Long	证书的到期时间。
timestamp	Long	创建证书的时间。

示例

如下以上传证书名为“cert_a”的证书为例。

- 请求样例

```
{
 "name": "cert_b"
}
```

- 响应样例

```
{
    "id": "388a7789d55b41d1918b3088a8f1e7f3",
    "name": "cert_b",
    "expireTime": 1565467166765,
    "timestamp": 1545467166765
}
```

状态码

表4-46描述的是API返回的正常状态码。

表 4-46 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.3.5 删除证书

功能介绍

删除没有被域名使用的单个证书。

URI

- URI格式
  DELETE /v1/{project_id}/waf/certificate/{certificate_id}
- 参数说明

  表 4-47 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
certificate_id	是	String	需要删除的证书的ID。

请求消息

请求参数

无

响应消息

响应参数

无

状态码

表4-48描述的是API返回的正常状态码。

表 4-48 状态码

状态码	编码	状态说明
204	No Content	服务器成功处理了请求，没有返回任何内容。

异常状态码，请参见**状态码**。

4.1.3.6 查询证书对应的域名

功能介绍

查询某一个证书对应的防护域名。

URI

- URI格式
  GET /v1/{project_id}/waf/certificate/{certificate_id}/host
- 参数说明

  表 4-49 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
certificate_id	是	String	证书ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-50 响应参数说明

名称	参数类型	说明
hostname	Array	域名列表。

示例

如下以获取证书列表为例。

响应样例

```
{
   "hostname": ["www.a.com","www.b.com"]
}
```

状态码

表4-51描述的是API返回的正常状态码。

表 4-51 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.4 防护状态与域名接入

4.1.4.1 修改防护状态

功能介绍

修改防护状态。

URI

- URI格式
  PUT /v1/{project_id}/waf/instance/{instance_id}/protect_status
- 参数说明

  表 4-52 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
instance_id	是	String	防护实例的ID。

请求消息

请求参数

表 4-53 请求参数说明

名称	是否必选	参数类型	说明
protect_status	是	Integer	域名的防护状态。 ● “1”：开启防护。 ● “0”：关闭防护。 ● “-1”：Bypass（客户的请求直接到达服务器，不再经过WAF）。

响应消息

响应参数

表 4-54 响应参数说明

名称	是否必选	参数类型	说明
protect_status	是	Integer	域名的防护状态。 ● “1”：开启防护。 ● “0”：关闭防护。 ● “-1”：Bypass（客户的请求直接到达服务器，不再经过WAF）。

示例

如下以修改防护状态为“开启”为例。

- 请求样例

```
{
    "protect_status": 1
}
```

- 响应样例

```
{
    "protect_status": 1
}
```

状态码

表4-55描述的是API返回的正常状态码。

表 4-55 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.4.2 域名接入

功能介绍

接入域名。

URI

- URI格式
  PUT /v1/{project_id}/waf/instance/{instance_id}/access_status
- 参数说明

  表 4-56 Path 参数说明

名称	是否必选	参数类型	说明
projecte_id	是	String	用户操作的项目ID。
instance_id	是	String	防护实例ID。

请求消息

请求参数

表 4-57 请求参数说明

名称	是否必选	参数类型	说明
access_status	是	Integer	域名接入状态。 “1”：已接入域名。

响应消息

响应参数

表 4-58 响应参数说明

名称	是否必选	参数类型	说明
access_status	是	Integer	域名接入状态。 ● “1”：已接入域名。 ● “0”：未接入域名。

名称	是否必选	参数类型	说明
protect_status	是	Integer	域名的防护状态。 ● “1”：开启防护。 ● “0”：关闭防护。 ● “-1”：Bypass（客户的请求直接到达服务器，不再经过WAF）。

示例

如下以域名状态为“1”为例。

- 请求样例

```
{
 "access_status": 1
}
```

- 响应样例

  接入成功

```
{
  "access_status": 1,
  "protect_status": 1
}
```

  接入失败

```
{
 "access_status": 0,
 "protect_status": 0
}
```

状态码

表4-59描述的是API返回的正常状态码。

表 4-59 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.5 防护策略

4.1.5.1 查询所有防护策略

功能介绍

查询防护策略列表。

URI

- URI格式

  GET /v1/{project_id}/waf/policy?policyname={policyname}&offset={offset}&limit={limit}

- 参数说明

  表 4-60 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policyname	否	String	策略名称。GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip?offset={offset}&limit={limit}
offset	否	Long	指定返回的页数，取值范围为：[0, 65535]，默认值为0。
limit	否	Long	指定查询返回每页记录的最大条数，取值范围为：(0, 10]，默认值为10。

请求消息

请求参数

无

响应消息

响应参数

表 4-61 响应参数说明

名称	参数类型	说明
total	Integer	防护策略总数。
items	表3	防护策略对象列表。

表 4-62 items

名称	参数类型	说明
id	String	实例ID。
name	String	防护策略名称。

名称	参数类型	说明
options	表4	防护规则是否开启。
action	表5	Web基础防护中的防护动作。 ● “block”：拦截并且记录。 ● “log”：仅记录不拦截。
level	Integer	防护等级。 ● “1”：表示低。 不检测header中的XSS攻击和CMDI攻击，当发现防护规则拦截了您的正常业务时，可调整防护等级为“1”，“1”防护下对业务的误报率降低，但漏报率可能会增高，例如：wget、curl等检测。 ● “2”：表示中。 默认情况下，选择“2”，根据文件的敏感程度区分，中危检测有远程文件包含、第三方软件漏洞、Webshell、cp、ftp。 ● “3”：表示高。 当您需要更严格的防护等级时，建议选择“3”，而“3”防护下对业务的误报率可能会增高，但漏报率降低，例如nc、nmap、kill等。
full_detection	Boolean	精准防护中的检测模式。 ● true：全检测。当用户的请求符合精准防护中的拦截条件时，不会立即拦截，WAF会继续执行其他防护的检测，待其他防护的检测完成后进行拦截。 ● false：短路检测。当用户的请求符合精准防护中的拦截条件时，便立刻终止检测，进行拦截。
hosts	Array	防护域名的ID。
timestamp	Long	创建策略的时间。

表 4-63 options

名称	参数类型	说明
webattack	Boolean	Web攻击是否开启。 ● true：表示开启。 ● false：表示关闭。

名称	参数类型	说明
common	Boolean	Web攻击的常规攻击检测是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler	Boolean	Web攻击的爬虫检测是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler_engine	Boolean	Web攻击的搜索引擎是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler_scanner	Boolean	Web攻击的扫描器是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler_script	Boolean	Web攻击的脚本工具是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler_other	Boolean	Web攻击的其他爬虫是否开启。 ● true：表示开启。 ● false：表示关闭。
webshell	Boolean	Web攻击的Webshell是否开启。 ● true：表示开启。 ● false：表示关闭。
cc	Boolean	Web攻击的CC防护是否开启。 ● true：表示开启。 ● false：表示关闭。
custom	Boolean	Web攻击的精准访问防护是否开启。 ● true：表示开启。 ● false：表示关闭。

名称	参数类型	说明
whiteblackip	Boolean	Web攻击的IP黑白名单是否开启。 ● true：表示开启。 ● false：表示关闭。
privacy	Boolean	Web攻击的隐私屏蔽是否开启。 ● true：表示开启。 ● false：表示关闭。
Ignore	Boolean	Web攻击的误报屏蔽是否开启。 ● true：表示开启。 ● false：表示关闭。
antitamper	Boolean	Web攻击的网页防篡改是否开启。 ● true：表示开启。 ● false：表示关闭。

表 4-64 action

名称	参数类型	说明
category	String	Web基础防护中防护动作的类型。 ● “block”：拦截。 ● “log”：仅记录不拦截。

示例

如下以查询所有防护策略，返回记录条数为“2”为例。

响应样例

```
{
   "total": 2,
   "items": [
      {
        "id": "xxxxxxxxxxxxxxxxxxxxxxxx",
        "name": "policy_1",
        "action": {
            "category ": "block"
         },
         "options": {
            "webattack": true,
            "common": true,
            "crawler": true,
            "crawler_engine": true,
            "crawler_scanner": true,
```

```
            "crawler_script": true,
            "crawler_other": true,
            "webshell": true,
            "cc": true,
            "custom": true,
            "whiteblackip": true,
            "ignore": true,
            "privacy": true,
            "antitamper": true
          },
          "level": 1,
          "full_detection": false,
          "hosts": ["1111111111111111", "2222222222222222"],
          "timestamp": 1499817612
        }, {
          "id": "xxxxxxxxxxxxxxxxxxxxxxxx",
          "name": "policy_2",
          "action": {
              "category": "block"
          },
          "options": {
              "webattack": true,
              "common": true,
              "crawler": true,
              "crawler_engine": true,
              "crawler_scanner": true,
              "crawler_script": true,
              "crawler_other": true,
              "webshell": true,
              "cc": true,
              "custom": true,
              "whiteblackip": true,
              "ignore": true,
              "privacy": true,
              "antitamper": true
          },
          "level": 1,
          "full_detection": false,
          "hosts": ["1111111111111111", "2222222222222222"],
          "timestamp": 1499817612
        }
    ]
}
```


状态码

表4-65描述的是API返回的正常状态码。

表 4-65 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.5.2 创建防护策略

功能介绍

创建防护策略。

URI

- URI格式
  POST /v1/{project_id}/waf/policy
- 参数说明

表 4-66 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。

请求消息

请求参数

表 4-67 请求参数说明

名称	是否必选	参数类型	说明
name	是	String	防护策略名称。最大长度为256字符。只支持以数字、字母、下划线或中划线命名。

响应消息

响应参数

表 4-68 响应参数说明

名称	参数类型	说明
id	String	防护实例的ID。
name	String	防护策略名称。
options	表4	防护规则是否开启。
action	表5	Web基础防护中的防护动作，默认为“log”模式。 ● “block”：拦截并记录。 ● “log”：仅记录不拦截。
level	Integer	防护等级。 ● “1”：表示低。 ● “2”：表示中。 ● “3”：表示高。
full_detection	Boolean	精准防护中的检测模式。

名称	参数类型	说明
hosts	Array	防护域名的ID。
timestamp	Long	创建防护策略的时间。

表 4-69 options

名称	参数类型	说明
webattack	Boolean	Web攻击是否开启，默认为开启状态。 ● true：表示开启。 ● false：表示关闭。
common	Boolean	Web攻击的常规攻击检测是否开启，默认为开启状态。 ● true：表示开启。 ● false：表示关闭。
crawler	Boolean	Web攻击的爬虫检测是否开启，默认为开启状态。 ● true：表示开启。 ● false：表示关闭。
crawler_engine	Boolean	Web攻击的搜索引擎是否开启，默认为关闭状态。 ● true：表示开启。 ● false：表示关闭。
crawler_scanner	Boolean	Web攻击的扫描器是否开启，默认为开启状态。 ● true：表示开启。 ● false：表示关闭。
crawler_script	Boolean	Web攻击的脚本工具是否开启，默认为关闭状态。 ● true：表示开启。 ● false：表示关闭。
crawler_other	Boolean	Web攻击的其他爬虫是否开启，默认为关闭状态。 ● true：表示开启。 ● false：表示关闭。

名称	参数类型	说明
webshell	Boolean	Web攻击的Webshell是否开启，默认为关闭状态。 ● true：表示开启。 ● false：表示关闭。
cc	Boolean	Web攻击的CC防护是否开启，默认为开启状态。 ● true：表示开启。 ● false：表示关闭。
custom	Boolean	Web攻击的精准访问防护是否开启，默认为开启状态。 ● true：表示开启。 ● false：表示关闭。
whiteblackip	Boolean	Web攻击的IP黑白名单是否开启，默认为开启状态。 ● true：表示开启。 ● false：表示关闭。
privacy	Boolean	Web攻击的隐私屏蔽是否开启，默认为开启状态。 ● true：表示开启。 ● false：表示关闭。
Ignore	Boolean	Web攻击的误报屏蔽是否开启，默认为开启状态。 ● true：表示开启。 ● false：表示关闭。
antitamper	Boolean	Web攻击的网页防篡改是否开启，默认为开启状态。 ● true：表示开启。 ● false：表示关闭。

表 4-70 action

名称	参数类型	说明
category	String	Web基础防护中防护动作的类型，默认为“log”模式。 ● “block”：拦截。 ● “log”：仅记录不拦截。

示例

如下以创建防护策略“policy_1”为例。

- 请求样例

```
{
  "name": "policy_1"
}
```

- 响应样例

```
{
        "id": "xxxxxxxxxxxxxxxxxxxxxxxx",
        "name": "policy_1",
        "action": {
            "category": "block"
         },
         "options": {
            "webattack": true,
            "common": true,
            "crawler": true,
            "crawler_engine": true,
            "crawler_scanner": true,
            "crawler_script": true,
            "crawler_other": true,
            "webshell": true,
            "cc": true,
            "custom": true,
            "whiteblackip": true,
            "ignore": true,
            "privacy": true,
            "antitamper": true
          },
         "level": 1,
         "full_detection": false,
         "hosts": [],
         "timestamp": 1499817612
}
```

状态码

表4-71描述的是API返回的正常状态码。

表 4-71 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.5.3 查询单个防护策略

功能介绍

查询防护策略的详细信息。

URI

- URI格式

GET /v1/{project_id}/waf/policy/{policy_id}

- 参数说明

表 4-72 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	需要查询的策略ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-73 响应参数说明

名称	参数类型	说明
id	String	防护实例的ID。
name	String	防护策略名称。
action	表3	策略规则命中后操作对象。 • “block”：拦截。 • “log”：仅记录不拦截。
options	表4	攻击防护类型开关对象。
level	Integer	防护等级。 • “1”：表示低。 • “2”：表示中。 • “3”：表示高。
full_detection	Boolean	精准防护中的检测模式。 • true：全检测。当用户的请求符合精准防护中的拦截条件时，不会立即拦截，WAF会继续执行其他防护的检测，待其他防护的检测完成后进行拦截。 • false：短路检测。当用户的请求符合精准防护中的拦截条件时，便立刻终止检测，进行拦截。

名称	参数类型	说明
hosts	Array	防护域名的ID。
timestamp	Long	创建策略的时间。

表 4-74 action

名称	参数类型	说明
category	String	操作类型。 ● “block”： 拦截。 ● “log”： 仅记录不拦截。

表 4-75 options

名称	参数类型	说明
webattack	Boolean	Web攻击是否开启。 ● true：表示开启。 ● false：表示关闭。
common	Boolean	Web攻击的常规攻击检测是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler	Boolean	Web攻击的爬虫检测是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler_engine	Boolean	Web攻击的搜索引擎是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler_scanner	Boolean	Web攻击的扫描器是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler_script	Boolean	Web攻击的脚本工具是否开启。 ● true：表示开启。 ● false：表示关闭。

名称	参数类型	说明
crawler_other	Boolean	Web攻击的其他爬虫是否开启。 ● true：表示开启。 ● false：表示关闭。
webshell	Boolean	Web攻击的Webshell是否开启。 ● true：表示开启。 ● false：表示关闭。
cc	Boolean	Web攻击的CC防护是否开启。 ● true：表示开启。 ● false：表示关闭。
custom	Boolean	Web攻击的精准访问防护是否开启。 ● true：表示开启。 ● false：表示关闭。
whiteblackip	Boolean	Web攻击的IP黑白名单是否开启。 ● true：表示开启。 ● false：表示关闭。
privacy	Boolean	Web攻击的隐私屏蔽是否开启。 ● true：表示开启。 ● false：表示关闭。
Ignore	Boolean	Web攻击的误报屏蔽是否开启。 ● true：表示开启。 ● false：表示关闭。
antitamper	Boolean	Web攻击的网页防篡改是否开启。 ● true：表示开启。 ● false：表示关闭。

示例

如下以查询防护策略“policy_2”为例。

响应样例

```
{
    "id": "xxxxxxxxxxxxxxxxxxxxxxxxx",
```

```
        "name": "policy_2",
        "action": {
            "category": "block"
        },
        "options": {
            "webattack": true,
            "common": true,
            "crawler": true,
            "crawler_engine": true,
            "crawler_scanner": true,
            "crawler_script": true,
            "crawler_other": true,
            "webshell": true,
            "cc": true,
            "custom": true,
            "whiteblackip": true,
            "ignore": true,
            "privacy": true,
            "antitamper": true
        },
        "level": 1,
        "full_detection": false,
        "hosts": ["1111111111111111", "2222222222222222"],
        "timestamp": 1499817612
}
```

状态码

表4-76描述的是API返回的正常状态码。

表 4-76 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.5.4 防护域名应用防护策略

功能介绍

防护域名应用防护策略。

URI

- URI格式
  PUT /v1/{project_id}/waf/policy/{policy_id}/hosts
- 参数说明

  表 4-77 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。

名称	是否必选	参数类型	说明
policy_id	是	String	策略ID。

请求消息

请求参数

表 4-78 请求参数说明

名称	是否必选	参数类型	说明
hosts	是	List	防护域名的ID。

响应消息

响应参数

表 4-79 响应参数说明

名称	参数类型	说明
id	String	策略ID。
name	String	策略名称。
action	表4	Policy规则命中后操作对象。 ● “block”：拦截。 ● “log”：仅记录不拦截。
options	表5	攻击防护类型开关对象。
level	Integer	防护等级。 ● “1”：表示低。 ● “2”：表示中。 ● “3”：表示高。
full_detection	Boolean	精准防护中的检测模式。 ● true：全检测。当用户的请求符合精准防护中的拦截条件时，不会立即拦截，WAF会继续执行其他防护的检测，待其他防护的检测完成后进行拦截。 ● false：短路检测。当用户的请求符合精准防护中的拦截条件时，便立刻终止检测，进行拦截。

名称	参数类型	说明
hosts	Array	防护域名的ID。
timestamp	Long	创建策略的时间。

表 4-80 action

名称	参数类型	说明
category	String	操作类型。 ● “block”： 拦截。 ● “log”： 仅记录不拦截。

表 4-81 options

名称	参数类型	说明
webattack	Boolean	Web攻击是否开启。 ● true：表示开启。 ● false：表示关闭。
common	Boolean	Web攻击的常规攻击检测是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler	Boolean	Web攻击的爬虫检测是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler_engine	Boolean	Web攻击的搜索引擎是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler_scanner	Boolean	Web攻击的扫描器是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler_script	Boolean	Web攻击的脚本工具是否开启。 ● true：表示开启。 ● false：表示关闭。

名称	参数类型	说明
crawler_other	Boolean	Web攻击的其他爬虫是否开启。 ● true：表示开启。 ● false：表示关闭。
webshell	Boolean	Web攻击的Webshell是否开启。 ● true：表示开启。 ● false：表示关闭。
cc	Boolean	Web攻击的CC防护是否开启。 ● true：表示开启。 ● false：表示关闭。
custom	Boolean	Web攻击的精准访问防护是否开启。 ● true：表示开启。 ● false：表示关闭。
whiteblackip	Boolean	Web攻击的IP黑白名单是否开启。 ● true：表示开启。 ● false：表示关闭。
privacy	Boolean	Web攻击的隐私屏蔽是否开启。 ● true：表示开启。 ● false：表示关闭。
Ignore	Boolean	Web攻击的误报屏蔽是否开启。 ● true：表示开启。 ● false：表示关闭。
antitamper	Boolean	Web攻击的网页防篡改是否开启。 ● true：表示开启。 ● false：表示关闭。

示例

如下将防护域名ID为“de06e61829494691b51979b9a03d5dcb"和"563972cc974b43848c73ed1a86268136”的域名应用防护策略“policy_2”为例。

- 请求样例

```
{
  "hosts": [
```

```
    "de06e61829494691b51979b9a03d5dcb",
    "563972cc974b43848c73ed1a86268136"
  ]
}
```

- 响应样例

```
{
        "id": "xxxxxxxxxxxxxxxxxxxxxxxx",
        "name": "policy_2",
        "action": {
            "category": "block"
         },
         "options": {
            "webattack": true,
            "common": true,
            "crawler": true,
            "crawler_engine": true,
            "crawler_scanner": true,
            "crawler_script": true,
            "crawler_other": true,
            "webshell": true,
            "cc": true,
            "custom": true,
            "whiteblackip": true,
            "ignore": true,
            "privacy": true,
            "antitamper": true
          },
         "level": 1,
         "full_detection": false,
         "hosts": ["de06e61829494691b51979b9a03d5dcb", "563972cc974b43848c73ed1a86268136"],
         "timestamp": 1499817612
}
```

状态码

表4-82描述的是API返回的正常状态码。

表 4-82 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.5.5 更新防护策略

功能介绍

部分更新防护策略。

URI

- URI格式

  PUT /v1/{project_id}/waf/policy/{policy_id}

- 参数说明

表 4-83 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。

请求消息

请求参数

表 4-84 请求参数说明

名称	是否必选	参数类型	说明
name	否	String	策略名称。
action	否	表3	Policy规则命中后操作对象。 ● “block”： 拦截。 ● “log”： 仅记录不拦截。
options	否	表4	攻击防护类型开关对象。
level	否	Integer	防护等级。 ● “1”： 表示低。 ● “2”： 表示中。 ● “3”： 表示高。
full_detection	否	Boolean	精准防护中的检测模式。 ● true：全检测。当用户的请求符合精准防护中的拦截条件时，不会立即拦截，WAF会继续执行其他防护的检测，待其他防护的检测完成后进行拦截。 ● false：短路检测。当用户的请求符合精准防护中的拦截条件时，便立刻终止检测，进行拦截。

表 4-85 action

名称	是否必选	参数类型	说明
category	是	String	操作类型。 ● “block”： 拦截。 ● “log”： 仅记录不拦截。

表 4-86 options

名称	是否必选	参数类型	说明
webattack	否	Boolean	Web攻击是否开启。 ● true：表示开启。 ● false：表示关闭。
common	否	Boolean	Web攻击的常规攻击检测是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler	否	Boolean	Web攻击的爬虫检测是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler_engine	否	Boolean	Web攻击的搜索引擎是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler_scanner	否	Boolean	Web攻击的扫描器是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler_script	否	Boolean	Web攻击的脚本工具是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler_other	否	Boolean	Web攻击的其他爬虫是否开启。 ● true：表示开启。 ● false：表示关闭。
webshell	否	Boolean	Web攻击的Webshell是否开启。 ● true：表示开启。 ● false：表示关闭。
cc	否	Boolean	Web攻击的CC防护是否开启。 ● true：表示开启。 ● false：表示关闭。

名称	是否必选	参数类型	说明
custom	否	Boolean	Web攻击的精准访问防护是否开启。 ● true：表示开启。 ● false：表示关闭。
whiteblackip	否	Boolean	Web攻击的IP黑白名单是否开启。 ● true：表示开启。 ● false：表示关闭。
privacy	否	Boolean	Web攻击的隐私屏蔽是否开启。 ● true：表示开启。 ● false：表示关闭。
Ignore	否	Boolean	Web攻击的误报屏蔽是否开启。 ● true：表示开启。 ● false：表示关闭。
antitamper	否	Boolean	Web攻击的网页防篡改是否开启。 ● true：表示开启。 ● false：表示关闭。

响应消息

响应参数

表 4-87 响应参数说明

名称	参数类型	说明
id	String	实例ID。
name	String	防护策略的名称。
options	表9	攻击防护类型开关对象。
action	表6	Web基础防护中的防护动作。 ● “block”：拦截。 ● “log”：仅记录不拦截。

名称	参数类型	说明
level	Integer	防护等级。 ● “1”：表示低。 ● “2”：表示中。 ● “3”：表示高。
full_detection	Boolean	精准防护中的检测模式。 ● true：全检测。当用户的请求符合精准防护中的拦截条件时，不会立即拦截，WAF会继续执行其他防护的检测，待其他防护的检测完成后进行拦截。 ● false：短路检测。当用户的请求符合精准防护中的拦截条件时，便立刻终止检测，进行拦截。
hosts	Array	防护域名的ID。
timestamp	Long	创建策略的时间。

表 4-88 action

名称	参数类型	说明
category	String	操作类型。 ● “block”：拦截。 ● “log”：仅记录不拦截。

表 4-89 options

名称	参数类型	说明
webattack	Boolean	Web攻击是否开启。 ● true：表示开启。 ● false：表示关闭。
common	Boolean	Web攻击的常规攻击检测是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler	Boolean	Web攻击的爬虫检测是否开启。 ● true：表示开启。 ● false：表示关闭。

名称	参数类型	说明
crawler_engine	Boolean	Web攻击的搜索引擎是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler_scanner	Boolean	Web攻击的扫描器是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler_script	Boolean	Web攻击的脚本工具是否开启。 ● true：表示开启。 ● false：表示关闭。
crawler_other	Boolean	Web攻击的其他爬虫是否开启。 ● true：表示开启。 ● false：表示关闭。
webshell	Boolean	Web攻击的Webshell是否开启。 ● true：表示开启。 ● false：表示关闭。
cc	Boolean	Web攻击的CC防护是否开启。 ● true：表示开启。 ● false：表示关闭。
custom	Boolean	Web攻击的精准访问防护是否开启。 ● true：表示开启。 ● false：表示关闭。
whiteblackip	Boolean	Web攻击的IP黑白名单是否开启。 ● true：表示开启。 ● false：表示关闭。
privacy	Boolean	Web攻击的隐私屏蔽是否开启。 ● true：表示开启。 ● false：表示关闭。

名称	参数类型	说明
Ignore	Boolean	Web攻击的误报屏蔽是否开启。 ● true：表示开启。 ● false：表示关闭。
antitamper	Boolean	Web攻击的网页防篡改是否开启。 ● true：表示开启。 ● false：表示关闭。

示例

如下以更新防护策略“policy_1”为例。

- 请求样例

```
{
        "name": "policy_1",
        "action": {
            "category": "block"
         },
         "options": {
            "webattack": true,
            "common": true,
            "crawler": true,
            "crawler_engine": true,
            "crawler_scanner": true,
            "crawler_script": true,
            "crawler_other": true,
            "webshell": true,
            "cc": true,
            "custom": true,
            "whiteblackip": true,
            "ignore": true,
            "privacy": true,
            "antitamper": true
          },
         "level": 1,
         "full_detection": false
}
```

- 响应样例

```
{
        "id": "xxxxxxxxxxxxxxxxxxxxxxxx",
        "name": "policy_1",
        "action": {
            "category": "block"
         },
         "options": {
            "webattack": true,
            "common": true,
            "crawler": true,
            "crawler_engine": true,
            "crawler_scanner": true,
            "crawler_script": true,
            "crawler_other": true,
            "webshell": true,
            "cc": true,
            "custom": true,
            "whiteblackip": true,
```

```
            "ignore": true,
            "privacy": true,
            "antitamper": true
        },
        "level": 1,
        "full_detection": false,
        "hosts": [],
        "timestamp": 1499817612
}
```

状态码

表4-90描述的是API返回的正常状态码。

表 4-90 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.5.6 删除防护策略

功能介绍

删除某个防护策略。

URI

- URI格式
  DELETE /v1/{project_id}/waf/policy/{policy_id}
- 参数说明

  表 4-91 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	防护策略ID。

请求消息

请求参数

无

响应消息

响应参数

无

状态码

表4-92描述的是API返回的正常状态码。

表 4-92 状态码

状态码	编码	状态说明
204	No Content	服务器成功处理了请求，没有返回任何内容。

异常状态码，请参见状态码。

4.1.6 黑白名单

4.1.6.1 查询 IP 黑白名单列表

功能介绍

查询IP黑白名单列表。

URI

- URI格式

  GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip?offset={offset}&limit={limit}

- 参数说明

  表 4-93 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID
offset	否	Long	指定返回的页数，取值范围为：[0, 65535]，默认值为0。
limit	否	Long	指定查询返回每页记录的最大条数，取值范围为：(0, 50]，默认值为10。

请求消息

请求参数

无

响应消息

响应参数

表 4-94 响应参数说明

名称	参数类型	说明
total	Integer	规则总数量。
items	表3	IP黑白名单对象列表。

表 4-95 items

名称	参数类型	说明
id	String	IP黑白名单规则的ID。
policy_id	String	IP黑白名单规则的策略ID。
addr	String	公网IP地址，例如：X.X.0.125、子网X.X.6.0/24。
white	Integer	设置的IP地址类型。 • “1”：白（放行）。 • “0”：黑（拦截）。
timestamp	Long	创建IP黑白名单的时间。

示例

如下以查询IP黑白名单列表，返回记录条数为“2”为例。

响应样例

```
{
  "total": 2,
  "items": [{
      "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
      "policy_id": "ertr45c0f96784ec8abd8ba61a98064ef",
      "addr": "X.X.0.125",
      "white": 1,
      "timestamp": 1499817600
    }, {
      "id": "44d887434169475794b2717438f7fa78",
      "policy_id": "ertr45c0f96784ec8abd8ba61a98064ef",
      "addr": "X.X.0.125",
      "white": 0,
      "timestamp": 1499817601
    }
  ]
}
```

状态码

表4-96描述的是API返回的正常状态码。

表 4-96 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见**状态码**。

4.1.6.2 创建 IP 黑白名单

功能介绍

创建IP黑白名单。

URI

- URI格式
  POST /v1/{project_id}/waf/policy/{policy_id}/whiteblackip
- 参数说明

  表 4-97 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。

请求消息

请求参数

表 4-98 请求参数说明

名称	是否必选	参数类型	说明
addr	是	String	公网IP地址，例如：X.X.0.125、子网X.X.6.0/24。
white	否	Integer	设置的IP地址类型。 ● “1”：白（放行）。 ● “0”：黑（拦截）。 如果没有white字段表示黑IP，与white=0 效果相同。

响应消息

响应参数

表 4-99 响应参数说明

名称	参数类型	说明
id	String	IP黑白名单规则的ID。
policy_id	String	策略ID。
addr	String	公网IP地址，例如：X.X.0.125、子网X.X.6.0/24。
white	Integer	设置的IP地址类型。 ● “1”：白（放行）。 ● “0”：黑（拦截）。 如果没有white字段表示黑IP，与white=0 效果相同。
timestamp	Long	创建IP黑白名单的时间。

示例

如下以创建IP白名单“X.X.0.125”为例。

- 请求样例

```
{
    "addr": "X.X.0.125",
    "white": 1
}
```

- 响应样例

```
{
  "id": "44d887434169475794b2717438f7fa78",
  "policy_id": "ertr45c0f96784ec8abd8ba61a98064ef",
  "addr": "X.X.0.125",
  "white": 1,
  "timestamp": 1499817600
}
```

状态码

表4-100描述的是API返回的正常状态码。

表 4-100 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.6.3 删除 IP 黑白名单

功能介绍

删除IP黑白名单。

URI

- URI格式

  DELETE /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{whiteblackip_rule_id}

- 参数说明

  表 4-101 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
whiteblackip_rule_id	是	String	黑白IP名单的规则ID。

请求消息

请求消息

无

响应消息

响应参数

无

状态码

表4-102描述的是API返回的正常状态码。

表 4-102 状态码

状态码	编码	状态说明
204	No Content	服务器成功处理了请求，没有返回任何内容。

异常状态码，请参见状态码。

4.1.6.4 查询 IP 黑白名单

功能介绍

查询IP黑白名单的详细信息。

URI

- URI格式

  GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{whiteblackip_rule_id}

- 参数说明

  表 4-103 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
whiteblackip_rule_id	是	String	黑白IP名单的规则ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-104 响应参数说明

名称	参数类型	说明
id	String	IP黑白名单的规则ID。
policy_id	String	策略ID。
addr	String	公网IP地址，例如：X.X.0.125、X.X.6.0/24。
white	Integer	设置的IP地址类型。 ● “1”：白（放行）。 ● “0”：黑（拦截）。
timestamp	Long	创建IP黑白名单的时间。

示例

如下以查询IP白名单“X.X.0.125”为例。

响应样例

```
{
  "id": "44d887434169475794b2717438f7fa78",
  "policy_id": "ertr45c0f96784ec8abd8ba61a98064ef",
  "addr": "X.X.0.125",
  "white": 0,
  "timestamp": 1499817600
}
```

状态码

表4-105描述的是API返回的正常状态码。

表 4-105 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.6.5 更新 IP 黑白名单

功能介绍

更新某个IP黑白名单。

URI

- URI格式

  PUT /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{whiteblackip_rule_id}

- 参数说明

  表 4-106 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
whiteblackip_rule_id	是	String	黑白IP名单的规则ID。

请求消息

请求参数

表 4-107 请求参数说明

名称	是否必选	参数类型	说明
addr	是	String	公网IP地址，例如：X.X.0.125、子网X.X.6.0/24。
white	否	Integer	设置的IP地址类型。 ● “1”：白（放行）。 ● “0”：黑（拦截）。

响应消息

响应参数

表 4-108 响应参数说明

名称	参数类型	说明
id	String	IP黑白名单的规则ID。
policy_id	String	策略ID。
addr	String	IP地址，例如：X.X.0.125、子网X.X.6.0/24。
white	Integer	设置的IP地址类型。 ● “1”：白（放行）。 ● “0”：黑（拦截）。 如果没有white字段表示黑IP，与white=0 效果相同。
timestamp	Long	创建IP黑白名单的时间。

示例

如下以更新IP黑名单“X.X.0.125”为例。

- 请求样例

```
{
 "addr": "X.X.0.125",
 "white": 1
}
```

- 响应样例

```
{
  "id": "44d887434169475794b2717438f7fa78",
  "policy_id": "ertr45c0f96784ec8abd8ba61a98064ef",
  "addr": "X.X.0.125",
  "white": 1,
  "timestamp": 1499817600
}
```

状态码

表4-109描述的是API返回的正常状态码。

表 4-109 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.7 CC 规则

4.1.7.1 查询 CC 规则列表

功能介绍

查询某个策略下所有的CC规则列表。

URI

- URI格式
  GET /v1/{project_id}/waf/policy/{policy_id}/cc?offset={offset}&limit={limit}
- 参数说明

  表 4-110 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
offset	否	Long	指定返回的页数，取值范围为：[0, 65535]，默认值为0。
limit	否	Long	指定查询返回每页记录的最大条数，取值范围为：(0, 50]，默认值为10。

请求消息

请求参数

无

响应消息

响应参数

表 4-111 响应参数说明

名称	参数类型	说明
total	Integer	该策略下CC防护规则总数量。
items	表3	CC规则对象列表。

表 4-112 items

名称	参数类型	说明
id	String	CC规则ID。
policy_id	String	CC防护策略的策略ID。
path	String	规则应用的URL链接，不包含域名。 ● 前缀匹配：以*结尾代表以该路径为前缀。 例如，需要防护的路径为“/admin/test.php”或“/adminabc”，则路径可以填写为“/admin*”。 ● 完全匹配：需要防护的路径需要与此处填写的路径完全相等。 如果防护路径为“/admin”，该规则必须填写为“/admin”。
limit_num	Integer	单个用户的周期内请求次数（单用户限速）。
limit_period	Integer	限速周期。
lock_time	Integer	锁定时长。取值范围为[0秒, 2^{32}秒)
tag_type	String	防护模式。 ● “ip”：IP限速，根据IP区分单个Web访问者。 ● “cookie”：用户限速，根据Cookie键值区分单个Web访问者。 ● “other”：根据Referer（自定义请求访问的来源）字段区分单个Web访问者。

名称	参数类型	说明
tag_index	String	当“tag_type”为cookie时，该参数表示cookie name。
tag_condition	表4	Referer（自定义请求访问的来源）字段，当“tag_type”为“other”时，会返回该字段。
action	表5	请求次数限制到达后采取的动作。
timestamp	Long	创建CC规则的时间。
default	Boolean	是否为默认CC规则。 • true：表示该规则是默认的CC规则，创建域名时默认创建的CC规则。 • false：表示该规则不是默认的CC规则，用户自己创建的CC规则。

表 4-113 tag_condition

名称	参数类型	说明
category	String	类别，取值为“Referer”。
contents	List	category的内容，例如“http://www.example.com”。

表 4-114 action

名称	参数类型	说明
category	String	动作类型。 • “block”：阻断。 • “captcha”：人机验证，阻断后用户需要输入正确的验证码，恢复正确的访问页面。 默认为“block”。
detail	表6	动作详情，“detail”为“null”时表示默认阻断页面。

表 4-115 detail

名称	参数类型	说明
response	表7	返回页面。

表 4-116 response

名称	参数类型	说明
content_type	String	返回页面的内容类型。 固定值为“application/json”、“text/html”、“text/xml”。
content	String	返回页面的内容。

示例

以查询CC规则列表，返回记录条数为“2”为例。

响应样例

```
{
  "total": 2,
  "items": [{
     "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
     "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
     "path": "/abc1",
     "limit_num": 10,
     "limit_period": 60,
     "lock_time": 10,
     "tag_type": "cookie",
     "tag_index": "sesssionid",
     "action": {
       "category": "block",
       "detail": {
         "response": {
             "content_type": "application/json",
             "content": "{\"error\":\"forbidden\"}"
         }
       }
     },
     "timestamp": 1499817600,
     "default": true
   }, {
     "id": "3d7bea768b10480984f98c6b69d43d0f",
     "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
     "path": "/efgh",
     "limit_num": 10,
     "limit_period": 60,
     "lock_time": 5,
     "tag_type": "other",
     "tag_condition":{
        "category": "referer",
       "contents": ["http://www.example.com"]
     }
     "action": {
       "category": "block",
     },
     "timestamp": 1499817600,
```

```
    "default": true
  }
 ]
}
```

状态码

表4-117描述的是API返回的正常状态码。

表 4-117 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.7.2 创建 CC 规则

功能介绍

创建CC规则。

URI

- URI格式
  POST /v1/{project_id}/waf/policy/{policy_id}/cc
- 参数说明

  表 4-118 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。

请求消息

请求参数

表 4-119 请求参数说明

名称	是否必选	参数类型	说明
path	是	String	规则应用的URL链接，不包含域名。 ● 前缀匹配：以*结尾代表以该路径为前缀。例如，需要防护的路径为“/admin/test.php”或“/adminabc”，则路径可以填写为“/admin*”。 ● 完全匹配：需要防护的路径需要与此处填写的路径完全相等。如果防护路径为“/admin”，该规则必须填写为“/admin”。
limit_num	否	Integer	单个用户的周期内请求次数（单用户限速）。取值范围为(0次, 2^{32}次)，默认是1
limit_period	否	Integer	限速周期。取值范围为(0, 2^{32}秒)，默认是1
lock_time	否	Integer	锁定时长。取值范围为[0秒, 2^{32}秒)
tag_type	是	String	防护模式。 ● “ip”：IP限速，根据IP区分单个Web访问者。 ● “cookie”：用户限速，根据Cookie键值区分单个Web访问者。 ● “other”：根据Referer（自定义请求访问的来源）字段区分单个Web访问者。
tag_index	否	String	当“tag_type”为“cookie”时，该参数表示cookie name。
tag_condition	否	表3	Referer（自定义请求访问的来源）字段，当“tag_type”为“other”时，需要传该字段。

名称	是否必选	参数类型	说明
action	是	表4	请求次数限制到达后采取的动作。

表 4-120 tag_condition

名称	是否必选	参数类型	说明
category	是	String	类别。取值为“Referer”。 当传tag_condition字段时，需要传该字段。
contents	是	List	category的内容。 格式为：http://www.example.com/path。 当传tag_condition字段时，需要传该字段。目前该字段只接受单个值，不要写入多个参数。

表 4-121 action

名称	是否必选	参数类型	说明
category	是	String	动作类型。 ● “block”：阻断。 ● “captcha”：人机验证，阻断后用户需要输入正确的验证码，恢复正确的访问页面。 默认为“block”。 当“tag_type”为“other”时，只能取值“block”。
detail	否	表5	动作详情，detail为null时表示默认阻断页面。 当“category”为“captcha”时，不能传此字段。 当“category”为“block”时，需要传此字段。

表 4-122 detail

名称	是否必选	参数类型	说明
response	是	表6	返回页面。

表 4-123 response

名称	是否必选	参数类型	说明
content_type	是	String	返回页面的内容类型。 固定值为“application/json”、“text/html”、“text/xml”。 默认值为“application/json”。
content	是	String	返回页面的内容。

响应消息

响应参数

表 4-124 响应参数说明

名称	参数类型	说明
id	String	CC规则ID。
policy_id	String	策略ID。
path	String	规则应用的URL链接。
limit_num	Integer	单个用户的请求次数。
limit_period	Integer	限速周期。
lock_time	Integer	锁定时间。取值范围为[0秒, 2^{32}秒）
tag_type	String	防护模式。 • “ip”：IP限速，根据IP区分单个Web访问者。 • “cookie”：用户限速，根据Cookie键值区分单个Web访问者。 • “other”：根据Referer（自定义请求访问的来源）字段区分单个Web访问者。

名称	参数类型	说明
tag_index	String	当“tag_type”为“cookie”时，该参数表示cookie name。
tag_condition	表8	Referer（自定义请求访问的来源）字段，当“tag_type”为“other”时，会返回该字段。
action	表9	请求次数到达限制后采取的动作。
timestamp	Long	创建CC规则的时间。
default	Boolean	是否为默认CC规则。 • true：表示该规则是默认的CC规则，创建域名时默认创建的CC规则。 • false：表示该规则不是默认的CC规则，用户自己创建的CC规则。

表 4-125 tag_condition

名称	参数类型	说明
category	String	类别。取值为“Referer”。
contents	List	category的内容。

表 4-126 action

名称	参数类型	说明
category	String	动作类型。 • “block”：阻断。 • “captcha”：人机验证，阻断后用户需要输入正确的验证码，恢复正确的访问页面。 默认为“block”。 当“tag_type”为“other”时，只能取值block。
detail	表10	动作详情，“detail”为“null”时，表示默认阻断页面。

表 4-127 detail

名称	参数类型	说明
response	表11	返回页面。

表 4-128 response

名称	参数类型	说明
content_type	String	返回页面的内容类型。 固定值为“application/json”、“text/html”、“text/xml”。
content	String	返回页面的内容。

示例

如下以创建一条CC规则为例。

- 请求样例

```
{
    "path": "/abc1",
    "limit_num": 10,
    "limit_period": 60,
    "lock_time": 10,
    "tag_type": "cookie",
    "tag_index": "sesssionid",
    "action": {
      "category": "block",
      "detail": {
        "response": {
            "content_type": "application/json",
            "content": "{\"error\":\"forbidden\"}"
        }
      }
    }
}
```

- 响应样例

```
{
    "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
    "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
    "path": "/abc1",
    "limit_num": 10,
    "limit_period": 60,
    "lock_time": 10,
    "tag_type": "cookie",
    "tag_index": "sesssionid",
    "action": {
      "category": "block",
      "detail": {
        "response": {
            "content_type": "application/json",
            "content": "{\"error\":\"forbidden\"}"
        }
      }
    },
    "timestamp": 1499817600,
```

```
    "default": false
}
```

状态码

表4-129描述的是API返回的正常状态码。

表 4-129 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.7.3 删除 CC 规则

功能介绍

删除CC规则。

URI

- URI格式
  DELETE /v1/{project_id}/waf/policy/{policy_id}/cc/{ccrule_id}
- 参数说明

  表 4-130 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
ccrule_id	是	String	CC规则的ID。

请求消息

请求参数

无

响应消息

响应参数

无

状态码

表4-131描述的是API返回的正常状态码。

表 4-131 状态码

状态码	编码	状态说明
204	No Content	服务器成功处理了请求，没有返回任何内容。

异常状态码，请参见状态码。

4.1.7.4 查询 CC 规则

功能介绍

查询CC规则的详细信息。

URI

- URI格式
  GET /v1/{project_id}/waf/policy/{policy_id}/cc/{ccrule_id}
- 参数说明

  表 4-132 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
ccrule_id	是	String	CC规则的ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-133 响应参数说明

名称	参数类型	说明
id	String	CC规则的ID。

名称	参数类型	说明
policy_id	String	策略ID。
path	String	规则应用的URL链接， 不包含域名。
limit_num	Integer	单个用户的周期内请求次数（单用户限速）。
limit_period	Integer	限速周期。
lock_time	Integer	锁定时长。取值范围为[0秒, 2^{32}秒)。
tag_type	String	防护模式。 • “ip”：IP限速，根据IP区分单个Web访问者。 • “cookie”：用户限速，根据Cookie键值区分单个Web访问者。 • “other”：根据Referer（自定义请求访问的来源）字段区分单个Web访问者。
tag_index	String	当“tag_type”为“cookie”时，该参数表示cookie name。
tag_condition	表3	Referer（自定义请求访问的来源）字段，当“tag_type”为“other”时，会返回该字段。
action	表4	请求次数到达限制后采取的动作。
timestamp	Long	创建CC规则的时间。
default	Boolean	是否为默认CC规则。 • true：表示该规则是默认的CC规则，创建域名时默认创建的CC规则。 • false：表示该规则不是默认的CC规则，用户自己创建的CC规则。

表 4-134 tag_condition

名称	参数类型	说明
category	String	类别。取值为“Referer”。
contents	List	category的内容。

表 4-135 action

名称	参数类型	说明
category	String	动作类型。 ● “block”：阻断。 ● “captcha”：人机验证，阻断后用户需要输入正确的验证码，恢复正确的访问页面。 默认为“block”。 当“tag_type”为“other”时，只能取值“block”。
detail	表5	动作详情，“detail”为“null”时表示默认阻断页面。

表 4-136 detail

名称	参数类型	说明
response	表6	返回页面。

表 4-137 response

名称	参数类型	说明
content_type	String	返回页面的内容类型。 固定值为“application/json”、“text/html”、“text/xml”。
content	String	返回页面的内容。

示例

如下以查询一条CC规则为例。

- 响应样例

```
{
  "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
  "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
  "path": "/abc1",
  "limit_num": 10,
  "limit_period": 60,
  "lock_time": "",
  "tag_type": "cookie",
  "tag_index": "sesssionid",
  "action": {
    "category": "block",
    "detail": {
```

```
    "response": {
      "content_type": "application/json",
      "content": "{\"error\":\"forbidden\"}"
    }
   }
 },
 "timestamp": 1499817600,
  "default": false
}
```

状态码

表4-138描述的是API返回的正常状态码。

表 4-138 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.7.5 更新 CC 规则

功能介绍

更新某个CC规则。

URI

- URI格式
  PUT /v1/{project_id}/waf/policy/{policy_id}/cc/{ccrule_id}
- 参数说明

  表 4-139 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
ccrule_id	是	String	CC规则的ID。

请求消息

请求参数

表 4-140 请求参数说明

名称	是否必选	参数类型	说明
path	是	String	规则应用的URL链接，不包含域名。
limit_num	是	Integer	单个用户的周期内请求次数（单用户限速）。取值范围为(0次, 2^{32}次)
limit_period	是	Integer	限速周期。取值范围为(0秒, 2^{32}秒)
lock_time	否	Integer	锁定时长。取值范围为[0秒, 2^{32}秒)
tag_type	是	String	防护模式。 • “ip”：IP限速，根据IP区分单个Web访问者。 • “cookie”：用户限速，根据Cookie键值区分单个Web访问者。 • “other”：根据Referer（自定义请求访问的来源）字段区分单个Web访问者。
tag_index	否	String	当“tag_type”为“cookie”时，该参数表示cookie name。
tag_condition	否	表3	Referer（自定义请求访问的来源）字段，当“tag_type”为“other”时，需要传该字段。
action	是	表4	请求次数到达限制后采取的动作。

表 4-141 tag_condition

名称	是否必选	参数类型	说明
category	是	String	类别。取值为“Referer”。 当传tag_condition字段时，需要传该字段。

名称	是否必选	参数类型	说明
contents	是	List	category的内容。 格式为：http://www.example.com/path。 当传tag_condition字段时，需要传该字段。目前该字段只接受单个值，不要写入多个参数。

表 4-142 action

名称	是否必选	参数类型	说明
category	是	String	动作类型。 ● “block”：阻断。 ● “captcha”：人机验证，阻断后用户需要输入正确的验证码，恢复正确的访问页面。 默认为“block”。 当“tag_type”为“other”时，只能取值“block”。
detail	否	表5	动作详情，“detail”为“null”时表示默认阻断页面。 当“category”为“captcha”时，不能传此字段。 当“category”为“block”时，需要传此字段。

表 4-143 detail

名称	是否必选	参数类型	说明
response	是	表6	返回页面。

表 4-144 response

名称	是否必选	参数类型	说明
content_type	是	String	返回页面的内容类型。 固定值为“application/json”、“text/html”、“text/xml”。 默认值为“application/json”。
content	是	String	返回页面的内容。

GET /v1/{project_id}/waf/policy/{policy_id}/custom?offset={offset}&limit={limit}

响应消息

响应参数

表 4-145 响应参数说明

名称	参数类型	说明
id	String	CC规则的ID。
policy_id	String	策略ID。
path	String	规则应用的URL链接，不包含域名。
limit_num	Integer	单个用户的周期内请求次数（单用户限速）。
limit_period	Integer	限速周期。
lock_time	Integer	锁定时长。取值范围为[0秒, 2^{32}秒)
tag_type	String	标记对象类型，固定值cookie、ip、other。
tag_index	String	当“tag_type”为“cookie”时，index表示cookie name。
tag_condition	表8	当“tag_type”为“other”时，该字段才有意义。
action	表9	请求次数到达限制后采取的动作。
timestamp	Long	创建CC规则的时间。

名称	参数类型	说明
default	Boolean	是否为默认CC规则。 • true：表示该规则是默认的CC规则，创建域名时默认创建的CC规则。 • false：表示该规则不是默认的CC规则，用户自己创建的CC规则。

表 4-146 tag_condition

名称	参数类型	说明
category	String	类别。取值为“Referer”。
contents	List	category的内容。

表 4-147 action

名称	参数类型	说明
category	String	动作类型。 • “block”：阻断。 • “captcha”：人机验证，阻断后用户需要输入正确的验证码，恢复正确的访问页面。 默认为“block”。 当“tag_type”为“other”时，只能取值“block”。
detail	表10	动作详情，“detai”l为“null”时表示默认阻断页面。

表 4-148 detail

名称	是否必选	参数类型	说明
response	是	表11	返回页面。

表 4-149 response

名称	参数类型	说明
content_type	String	返回页面的内容类型。 固定值为“application/json”、“text/html”、“text/xml”。
content	String	返回页面的内容。

示例

如下以更新一条CC规则为例。

- 请求样例

```
{
  "path": "/abc1",
  "limit_num": 10,
  "limit_period": 60,
  "lock_time": "",
  "tag_type": "cookie",
  "tag_index": "sesssionid",
  "action": {
    "category": "block",
    "detail": {
      "response": {
        "content_type": "application/json",
        "content": "{\'error\':\'forbidden\}"
      }
    }
  }
}
```

- 响应样例

```
{
  "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
  "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
  "path": "/abc1",
  "limit_num": 10,
  "limit_period": 60,
  "lock_time": "",
  "tag_type": "cookie",
  "tag_index": "sesssionid",
  "action": {
    "category": "block",
    "detail": {
      "response": {
        "content_type": "application/json",
        "content": "{\"error\":\"forbidden\"}"
      }
    }
  },
  "timestamp": 1499817600,
   "default": false
}
```

状态码

表4-150描述的是API返回的正常状态码。

表 4-150 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见**状态码**。

4.1.8 精准防护规则

4.1.8.1 查询精准防护规则列表

功能介绍

查询某个策略下所有的精准防护规则列表。

URI

- URI格式

  GET /v1/{project_id}/waf/policy/{policy_id}/custom?offset={offset}&limit={limit}

- 参数说明

  表 4-151 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
offset	否	Long	指定返回的页数，取值范围为：[0, 65535]，默认值为0。
limit	否	Long	指定查询返回每页记录的最大条数，取值范围为：(0, 50]，默认值为10。

请求消息

请求参数

无

响应消息

响应参数

表 4-152 响应参数说明

名称	参数类型	说明
total	Integer	该策略下设置的精准防护规则总数量。
items	表3	精准防护规则的对象列表。

表 4-153 items

名称	参数类型	说明
id	String	精准防护规则的ID。
policy_id	String	防护策略ID。
name	String	精准防护规则的名称。
conditions	List of 表4	匹配条件列表。匹配条件必须同时满足。
action	表5	精准防护规则命中后操作对象。
time	Boolean	精准防护规则的生效时间。 • “false”：表示该规则立即生效。 • “true”：表示自定义生效时间。
start	Long	精准防护规则生效的起始时间。当time=true，才会返回该参数。
end	Long	精准防护规则生效的终止时间。当time=true，才会返回该参数。
priority	Integer	执行该规则的优先级，值越小，优先级越高，值相同时，规则创建时间早，优先级越高。取值范围：0到65535。
timestamp	Long	创建精准访问防护规则的时间。

表 4-154 conditions

名称	参数类型	说明
category	String	条件类型。固定值path、user-agent、ip、params、cookie、referer、header。

名称	参数类型	说明
index	String	• 当“category”为“cookie”时，index表示cookie name。 • 当“category”为“params”时，index表示param name。 • 当“category”为“header”时，index表示header中的选项。
logic	String	“contain”，“not_contain”“equal”，“not_equal”，“prefix”，“not_prefix”，“suffix”，“not_suffix”分别代表包含、不包含、等于、不等于、前缀为、前缀不为、后缀为、后缀不为。 当条件类型“category”为ip时，“logic”只能为“equal”或者“not_equal”。
contents	List	条件匹配的内容。

表 4-155 action

名称	参数类型	说明
category	String	操作类型。 • “block”：拦截。 • “pass”：放行。

示例

如下以查询精准防护规则列表，返回记录条数为"2" 为例。

响应样例

```
{
  "total": 2,
  "items": [{
      "id": "7374ad99c6c448e9a9ca35cb46660a39",
      "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
      "name":  "rule1",
      "time": true,
      "start": 1499817600,
      "end": 1567817600,
      "conditions": [{
          "category": "path",
          "contents": ["/login"],
          "logic": "containi"
        },{
```

```
        "category": "ip",
         "logic": "equal",
         "contents": ["X.X.1.1"]
       }
     ],
     "action": {
       "category": "block"
     },

    "priority": 1,
    "timestamp": 1499817600
   }, {
     "id": "7374ad99c6c448e9a9ca35cb46660a39",
     "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
     "name":  "rule2",
     "time": false,
     "conditions": [{
         "category": "path",
         "contents": ["/login"],
         "logic": "contain"
       },{
         "category": "ip",
         "logic": "equal",
         "contents": ["X.X.1.1"]
       }
     ],
     "action": {
       "category": "block"
     },

    "priority": 1,
    "timestamp": 1499817600
   }
 ]
}
```


状态码

表4-156描述的是API返回的正常状态码。

表 4-156 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.8.2 创建精准防护规则

功能介绍

创建精准防护规则。

URI

- URI格式
  POST /v1/{project_id}/waf/policy/{policy_id}/custom

- 参数说明

表 4-157 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。

请求消息

请求参数

表 4-158 请求参数说明

名称	是否必选	参数类型	说明
name	是	String	自定义规则的名称。最大长度为256字符。只支持以数字、字母、下划线或中划线命名。
time	否	Boolean	精准防护规则生效时间。 ● “false”：表示该规则立即生效。 ● “true”：表示自定义生效时间。
start	否	Long	精准防护规则生效的起始时间。当time=true时，起始时间和终止时间必须有一个非空。
end	否	Long	精准防护规则生效的终止时间。当time=true时，起始时间和终止时间必须有一个非空。
conditions	是	List of 表3	匹配条件列表。
action	是	表4	精准防护规则命中后操作对象。
priority	否	Integer	执行该规则的优先级，值越小，优先级越高，值相同时，规则创建时间早，优先级越高。取值范围：0到65535。

表 4-159 conditions

名称	是否必选	参数类型	说明
category	是	String	条件类型。固定值path、user-agent、ip、params、cookie、referer、header。
index	否	String	• 当“category”为“cookie”时，index表示cookie name。 • 当“category”为“params”时，index表示param name。 • 当“category”为“header”时，index表示header中的选项。
logic	是	String	“contain”，“not_contain”“equal”，“not_equal”，“prefix”，“not_prefix”，“suffix”，“not_suffix”分别代表包含、不包含、等于、不等于、前缀为、前缀不为、后缀为、后缀不为。 当条件类型“category”为ip时，“logic”只能为“equal”或者“not_equal”。
contents	是	List	条件匹配的内容。目前该字段只接受一个值，不要写入多个参数。

表 4-160 action

名称	是否必选	参数类型	说明
category	是	String	操作类型。 • “block”： 拦截。 • “pass”： 放行。

响应消息

响应参数

表 4-161 响应参数说明

名称	参数类型	说明
id	String	精准防护规则的ID。
policy_id	String	精准防护规则的策略ID。
name	String	精准防护规则的名称。
conditions	List of 表6	精准防护规则的匹配条件列表。
action	表7	精准防护规则命中后操作对象。
priority	Integer	执行该规则的优先级，值越小，优先级越高，值相同时，规则创建时间早，优先级越高。取值范围：0到65535。
time	Boolean	精准防护规则的生效时间。 • “false”：表示该规则立即生效。 • “true”：表示自定义生效时间。
start	Long	精准防护规则生效的起始时间。
end	Long	精准防护规则生效的终止时间。
timestamp	Long	创建精准访问防护规则的时间。

表 4-162 conditions

名称	参数类型	说明
category	String	条件类型。固定值path、user-agent、ip、params、cookie、referer、header。
index	String	• 当“category”为“cookie”时，index表示cookie name。 • 当“category”为“params”时，index表示param name。 • 当“category”为“header”时，index表示header中的选项。

名称	参数类型	说明
logic	String	“contain”，“not_contain”“equal”,“not_equal”，“prefix”，“not_prefix”，“suffix”，“not_suffix”分别代表包含、不包含、等于、不等于、前缀为、前缀不为、后缀为、后缀不为。 当条件类型“category”为ip时，“logic”只能为“equal”或者“not_equal”。
contents	List	条件匹配的内容。

表 4-163 action

名称	参数类型	说明
category	String	操作类型。 ● “block”： 拦截。 ● “pass”： 放行。

示例

如下以创建一条名为“rule1”的精准防护规则为例。

- 请求样例

```
{
    "name":  "rule1",
    "time": true,
    "start": 1499817600,
    "end": 1567817600,
    "conditions": [{
        "category": "path",
        "contents": ["/login"],
        "logic": "contain"
      },{
        "category": "ip",
         "logic": "equal",
         "contents": ["X.X.1.1"]
      }
    ],
    "action": {
      "category": "block"
    },
   "priority": 10
}
```

- 响应样例

```
{
    "id": "7374ad99c6c448e9a9ca35cb46660a39",
    "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
    "name":  "rule1",
    "time": true,
    "start": 1499817600,
```

```
    "end": 1567817600,
    "conditions": [{
        "category": "path",
        "contents": ["/login"],
        "logic": "contain"
      },{
        "category": "ip",
         "logic": "equal",
         "contents": ["X.X.1.1"]
      }
    ],
    "action": {
      "category": "block"
    },

   "priority": 10,
   "timestamp": 1499817600
}
```

状态码

表4-164描述的是API返回的正常状态码。

表 4-164 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.8.3 删除精准防护规则

功能介绍

删除精准防护规则。

URI

- URI格式
  DELETE /v1/{project_id}/waf/policy/{policy_id}/custom/{custom_rule_id}
- 参数说明

表 4-165 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
custom_rule_id	是	String	精准防护规则的ID。

请求消息

请求参数

无

响应消息

响应参数

无

状态码

表4-166描述的是API返回的正常状态码。

表 4-166 状态码

状态码	编码	状态说明
204	No Content	服务器成功处理了请求，没有返回任何内容。

异常状态码，请参见状态码。

4.1.8.4 查询某个自定义规则

功能介绍

查询自定义规则的详细信息。

URI

- URI格式
  GET /v1/{project_id}/waf/policy/{policy_id}/custom/{custom_rule_id}
- 参数说明

  表 4-167 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
custom_rule_id	是	String	自定义精准防护规则的ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-168 响应参数说明

名称	参数类型	说明
id	String	精准防护规则的ID。
policy_id	String	策略ID。
name	String	精准防护规则名称。
time	Boolean	精准防护规则生效时间。 • “false”：表示该规则立即生效。 • “true”：表示自定义生效时间。
start	Long	精准防护规则生效的起始时间。
end	Long	精准防护规则生效的终止时间。
conditions	List of 表3	匹配条件列表。
action	表4	精准防护规则命中后操作对象。
priority	Integer	执行该规则的优先级，值越小，优先级越高，值相同时，规则创建时间早，优先级越高。取值范围：0到65535。
timestamp	Long	创建精准访问防护规则的时间。

表 4-169 conditions

名称	参数类型	说明
category	String	条件类型。固定值path、user-agent、ip、params、cookie、referer、header。

名称	参数类型	说明
index	String	• 当“category”为“cookie”时，index表示cookie name。 • 当“category”为“params”时，index表示param name。 • 当“category”为“header”时，index表示header中的选项。
logic	String	“contain”，“not_contain”“equal”，“not_equal”，“prefix”，“not_prefix”，“suffix”，“not_suffix”分别代表包含、不包含、等于、不等于、前缀为、前缀不为、后缀为、后缀不为。 当条件类型“category”为“ip”时，“logic”只能为“equal”或者“not_equal”。
contents	List	条件匹配的内容。

表 4-170 action

名称	参数类型	说明
category	String	操作类型。 • “block”： 拦截。 • “pass”： 放行。

示例

如下以查询id 为“7374ad99c6c448e9a9ca35cb46660a39”的自定义规则为例。

响应样例

```
{
    "id": "7374ad99c6c448e9a9ca35cb46660a39",
    "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
    "name": "rule1",
    "time": true,
    "start": 1499817600,
    "end": 1567817600,
    "conditions": [{
        "category ": "path",
        "contents": ["/login"],
        "logic": "contain"
      },{
        "category": "ip",
```

```
        "logic": "equal",
        "contents": ["X.X.1.1"]
      }, {
        "category": "referer",
        "logic": "prefix",
        "contents": ["https://www.waf.com/xxx"]
      }, {
        "category": "user-agent",
        "logic": "contain",
        "contents": ["Mozilla/5.0"]
      }, {
        "category": "cookie",
        "index": "SID",
        "logic": 3,
        "contents": ["234SDFASR4R32412FSR325S"]
      }, {
        "category": "header",
        "index": "x-language",
        "logic": "equal",
        "contents": ["en-us"]
      }, {
        "category": "params",
        "index": "name",
        "logic": "equal",
        "contents": ["abc"]
      }
    ],
    "action": {
      "category": "block"
    },
    "priority": 10,
    "timestamp": 1499817600
}
```

状态码

表4-171描述的是API返回的正常状态码。

表 4-171 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.8.5 更新精准防护规则

功能介绍

更新某个精准防护规则。

URI

- URI格式
  PUT /v1/{project_id}/waf/policy/{policy_id}/custom/{custom_rule_id}
- 参数说明

表 4-172 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
custom_rule_id	是	String	精准防护规则的ID。

请求消息

请求参数

表 4-173 请求参数说明

名称	是否必选	参数类型	说明
name	是	String	精准防护规则的名称。
time	否	Boolean	精准防护规则生效时间。 • “false”：表示该规则立即生效。 • “true”：表示自定义生效时间。
start	否	Long	精准防护规则生效的起始时间。当time=true时，起始时间和终止时间必须有一个非空。
end	否	Long	精准防护规则生效的终止时间。当time=true时，起始时间和终止时间必须有一个非空。
conditions	是	List of 表3	匹配条件列表。
action	是	表4	精准防护规则命中后操作对象。
priority	否	Integer	优先级。取值范围为“0-65535”。默认值50。值越小，优先级越高。

表 4-174 conditions

名称	是否必选	参数类型	说明
category	是	String	条件类型。固定值path、user-agent、ip、params、cookie、referer、header。

名称	是否必选	参数类型	说明
index	否	String	• 当“category”为“cookie”时，index表示cookie name。 • 当“category”为“params”时，index表示param name。 • 当“category”为“header”时，index表示header中的选项。
logic	是	String	“contain”，“not_contain”“equal”，“not_equal”，“prefix”，“not_prefix”，“suffix”，“not_suffix”分别代表包含、不包含、等于、不等于、前缀为、前缀不为、后缀为、后缀不为。 当条件类型“category”为ip时，“logic”只能为“equal”或者“not_equal”。
contents	是	List	条件匹配的内容。目前该字段只接受一个值，不要写入多个参数。

表 4-175 action

名称	是否必选	参数类型	说明
category	是	String	操作类型。 • “block”： 拦截。 • “pass”： 放行。

响应消息

响应参数

表 4-176 响应参数说明

名称	参数类型	说明
id	String	精准防护规则的ID。
policy_id	String	策略ID。

名称	参数类型	说明
name	String	精准防护规则名称。
time	Boolean	精准防护规则生效时间。 • “false”：表示该规则立即生效。 • “true”：表示自定义生效时间。
start	Long	精准防护规则生效的起始时间。
end	Long	精准防护规则生效的终止时间。
conditions	List of 表6	匹配条件列表。
action	表7	精准防护规则命中后操作对象。
priority	Integer	执行该规则的优先级，值越小，优先级越高，值相同时，规则创建时间早，优先级越高。取值范围：0到65535。
timestamp	Long	创建精准访问防护规则的时间。

表 4-177 conditions

名称	参数类型	说明
category	String	条件类型。固定值path、user-agent、ip、params、cookie、referer、header。
index	String	• 当“category”为“cookie”时，index表示cookie name。 • 当“category”为“params”时，index表示param name。 • 当“category”为“header”时，index表示header中的选项。

名称	参数类型	说明
logic	String	“contain”，“not_contain”“equal”,“not_equal”，“prefix”，“not_prefix”，“suffix”，“not_suffix”分别代表包含、不包含、等于、不等于、前缀为、前缀不为、后缀为、后缀不为。 当条件类型“category”为ip时，“logic”只能为“equal”或者“not_equal”。
contents	List	条件匹配的内容。

表 4-178 action

名称	参数类型	说明
category	String	操作类型。 ● “block”： 拦截。 ● “pass”： 放行。

示例

如下以更新精准防护规则“rule1”为例。

- 请求样例

```
{
    "name":  "rule1",
    "time": true,
    "start": 1499817600,
    "end": 1567817600,
    "conditions": [{
        "category": "path",
        "contents": ["/login"],
        "logic": "contain"
      },{
        "category": "ip",
         "logic": "equal",
         "contents": ["X.X.1.1"]
      }
    ],
    "action": {
      "category": "block"
    },
   "priority": 10
}
```

- 响应样例

```
{
    "id": "7374ad99c6c448e9a9ca35cb46660a39",
    "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
    "name":  "rule1",
    "time": true,
    "start": 1499817600,
```

```
    "end": 1567817600,
    "conditions": [{
        "category": "path",
        "contents": ["/login"],
        "logic": "contain"
      },{
        "category": "ip",
         "logic": "equal",
         "contents": ["X.X.1.1"]
      }
    ],
    "action": {
      "category": "block"
    },

   "priority": 10,
   "timestamp": 1499817600
}
```

状态码

表4-179描述的是API返回的正常状态码。

表 4-179 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.9 隐私屏蔽规则

4.1.9.1 查询隐私屏蔽规则列表

功能介绍

查询某个策略下所有的隐私屏蔽规则列表。

URI

- URI格式

  GET /v1/{project_id}/waf/policy/{policy_id}/privacy?offset={offset}&limit={limit}

- 参数说明

  表 4-180 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。

名称	是否必选	参数类型	说明
offset	否	Long	指定返回的页数，取值范围为：[0, 65535]，默认值为0。
limit	否	Long	指定查询返回每页记录的最大条数，取值范围为：(0, 50]，默认值为10。

请求消息

请求参数

无

响应消息

响应参数

表 4-181 响应参数说明

名称	参数类型	说明
total	Integer	规则总数量。
items	表3	隐私屏蔽规则对象列表。

表 4-182 items

名称	参数类型	说明
id	String	隐私屏蔽规则ID。
policy_id	String	策略ID。
path	String	隐私屏蔽规则应用的URL（默认完全匹配）。
category	String	屏蔽字段，取值范围是：params，header。
index	String	屏蔽字段名。
timestamp	Long	创建隐私屏蔽规则的时间。

示例

如下以查询隐私屏蔽规则列表，返回记录条数为“2”为例。

响应样例

```
{
  "total": 2,
  "items": [{
      "id": "e1c0e55865544d1f8c95cf71df108c6b",
      "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
      "path": "/login",
      "category": "params",
      "index": "password",
      "timestamp": 123243414132
    }, {
      "id": "d947d31c3e794b70a25e5e2057997f8e",
      "policy_id": "yuc0e55865544d1f8c95cf71df108c89",
      "path": "/register",
      "category": "header",
      "index": "x-auth-token",
      "timestamp": 1343243243123
    }
  ]
}
```

状态码

表4-183描述的是API返回的正常状态码。

表 4-183 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.9.2 创建隐私屏蔽规则

功能介绍

创建隐私屏蔽规则。

URI

- URI格式

  POST /v1/{project_id}/waf/policy/{policy_id}/privacy

- 参数说明

  表 4-184 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。

请求消息

请求参数

表 4-185 请求参数说明

名称	是否必选	参数类型	说明
path	是	String	隐私屏蔽规则应用的URL（默认完全匹配）。
category	是	String	屏蔽类别。固定值为params，header。
index	是	String	屏蔽字段名。

响应消息

响应参数

表 4-186 响应参数说明

名称	参数类型	说明
id	String	隐私屏蔽规则ID。
policy_id	String	策略ID。
path	String	隐私屏蔽规则应用的URL（默认完全匹配）。
category	String	屏蔽字段，取值范围是：params，header。
index	String	屏蔽字段名。
timestamp	Long	创建隐私屏蔽规则的时间。

示例

如下以创建隐私屏蔽规则为例。

- 请求样例

```
{
  "path": "/login",
  "category": "params",
  "index": "name"
}
```

- 响应样例

```
{
    "id": "e1c0e55865544d1f8c95cf71df108c6b",
    "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
    "path": "/login",
    "category":"params",
    "index": "name",
```

```
    "timestamp": 123243414132
}
```

状态码

表4-187描述的是API返回的正常状态码。

表 4-187 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.9.3 删除隐私屏蔽规则

功能介绍

删除隐私屏蔽规则。

URI

- URI格式
  DELETE /v1/{project_id}/waf/policy/{policy_id}/privacy/{privacy_rule_id}
- 参数说明

  表 4-188 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
privacy_rule_id	是	String	隐私屏蔽规则ID。

请求消息

请求参数

无

响应消息

响应参数

无

状态码

表4-189描述的是API返回的正常状态码。

表 4-189 状态码

状态码	编码	状态说明
204	No Content	服务器成功处理了请求，没有返回任何内容。

异常状态码，请参见状态码。

4.1.9.4 查询隐私屏蔽规则

功能介绍

查询隐私屏蔽规则的详细信息。

URI

- URI格式
  GET /v1/{project_id}/waf/policy/{policy_id}/privacy/{privacy_rule_id}
- 参数说明

  表 4-190 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
privacy_rule_id	是	String	隐私屏蔽规则的ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-191 响应参数说明

名称	参数类型	说明
id	String	隐私屏蔽规则ID。

名称	参数类型	说明
policy_id	String	策略ID。
path	String	隐私屏蔽规则应用的URL（默认完全匹配）。
category	String	屏蔽字段，取值范围是：params，header。
index	String	屏蔽字段名。
timestamp	Long	创建隐私屏蔽规则的时间。

示例

如下以查询id为“e1c0e55865544d1f8c95cf71df108c6b”的隐私屏蔽规则为例。

响应样例

```
{
  "id": "e1c0e55865544d1f8c95cf71df108c6b",
  "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
  "path": "/login",
  "category": "params",
  "index": "password",
  "timestamp": 12324435345
}
```

状态码

表4-192描述的是API返回的正常状态码。

表 4-192 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.9.5 更新隐私屏蔽规则

功能介绍

更新某个隐私屏蔽规则。

URI

- URI格式
  PUT /v1/{project_id}/waf/policy/{policy_id}/privacy/{privacy_rule_id}
- 参数说明

表 4-193 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
privacy_rule_id	是	String	隐私屏蔽规则的ID。

请求消息

请求参数

表 4-194 请求参数说明

名称	是否必选	参数类型	说明
path	是	String	隐私屏蔽规则应用的URL（默认完全匹配）。
category	是	String	屏蔽字段，取值范围是：params，header。
index	是	String	屏蔽字段名。

响应消息

响应参数

表 4-195 响应参数说明

名称	参数类型	说明
id	String	隐私屏蔽规则ID。
policy_id	String	策略ID。
path	String	隐私屏蔽应用的URL（默认完全匹配）。
category	String	屏蔽字段，取值范围是：params，header。
index	String	屏蔽字段名。
timestamp	Long	创建隐私屏蔽规则的时间。

示例

如下以更新隐私屏蔽规则为例。

- 请求样例

```
{
  "path": "/login",
  "category": "params",
  "index": "password"
}
```

- 响应样例

```
{
  "id": "e1c0e55865544d1f8c95cf71df108c6b",
  "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
  "path": "/login",
  "category": "params",
  "index": "password",
  "timestamp": 123434534543
}
```

状态码

表4-196描述的是API返回的正常状态码。

表 4-196 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.10 网页防篡改规则

4.1.10.1 查询网页防篡改规则列表

功能介绍

查询某个策略下所有的网页防篡改规则列表。

URI

- URI格式

  GET /v1/{project_id}/waf/policy/{policy_id}/antitamper?offset={offset}&&limit={limit}

- 参数说明

表 4-197 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。

名称	是否必选	参数类型	说明
offset	否	Long	指定返回的页数，取值范围为：[0, 65535]，默认值为0。
limit	否	Long	指定查询返回每页记录的最大条数，取值范围为：(0, 50]，默认值为10。

请求消息

请求参数

无

响应消息

响应参数

表 4-198 响应参数说明

名称	参数类型	说明
total	Integer	该策略下防篡改规则的总条数。
items	表3	网页防篡改对象列表。

表 4-199 items

名称	参数类型	说明
id	String	网页防篡改规则ID。
policy_id	String	网页防篡改规则的策略ID。
hostname	String	防护域名。
path	String	防篡改的URL链接，不包含域名。
timestamp	Long	缓存的更新时间。

示例

如下以查询网页防篡改规则列表，返回记录条数为“2”为例。

响应样例

```
{
  "total": 2,
  "items": [{
      "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
```

```
    "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
    "hostname": "www.aaa.com",
    "path": "/a",
    "timestamp": 1499817600
  }, {
    "id": "44d887434169475794b2717438f7fa78",
    "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
    "hostname": "www.bbb.com",
    "path": "/b",
    "timestamp": 1499817600
  }
 ]
}
```


状态码

表4-200描述的是API返回的正常状态码。

表 4-200 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.10.2 创建网页防篡改规则

功能介绍

创建网页防篡改规则。

URI

- URI格式

  POST /v1/{project_id}/waf/policy/{policy_id}/antitamper
- 参数说明

  表 4-201 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	防护策略ID。

请求消息

请求参数

表 4-202 请求参数说明

名称	是否必选	参数类型	说明
hostname	是	String	防护域名。
path	是	String	防篡改的URL，不包含域名。

响应消息

响应参数

表 4-203 响应参数说明

名称	参数类型	说明
id	String	网页防篡改规则ID。
policy_id	String	防护策略ID。
hostname	String	防护域名。
path	String	防篡改的URL链接，不包含域名。
timestamp	Long	缓存的更新时间。

示例

如下以为域名“www.abc.com”创建网页防篡改规则为例。

- 请求样例

```
{
  "hostname": "www.abc.com",
  "path": "/a"
}
```

- 响应样例

```
{
    "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
    "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
    "hostname": "www.abc.com",
    "path": "/a",
    "timestamp": 1499817600
}
```

状态码

表4-204描述的是API返回的正常状态码。

表 4-204 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见**状态码**。

4.1.10.3 删除网页防篡改规则

功能介绍

删除网页防篡改规则。

URI

- URI格式

  DELETE /v1/{project_id}/waf/policy/{policy_id}/antitamper/{antitamper_rule_id}

- 参数说明

  表 4-205 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	防护策略ID。
antitamper_rule_id	是	String	网页防篡改规则的ID。

请求消息

请求参数

无

响应消息

响应参数

无

状态码

表4-206描述的是API返回的正常状态码。

表 4-206 状态码

状态码	编码	状态说明
204	No Content	服务器成功处理了请求，没有返回任何内容。

异常状态码，请参见**状态码**。

4.1.10.4 查询某个网页防篡改规则

功能介绍

查询网页防篡改规则的详细信息。

URI

- URI格式
  GET /v1/{project_id}/waf/policy/{policy_id}/antitamper/{antitamper_rule_id}
- 参数说明

  表 4-207 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
antitamper_rule_id	是	String	网页防篡改规则的ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-208 响应参数说明

名称	参数类型	说明
id	String	网页防篡改规则ID。
policy_id	String	策略ID。
hostname	String	防护域名。
path	String	防篡改的URL链接，不包含域名。
timestamp	Long	缓存的更新时间。

示例

如下以查询id为“3a9b5c0f96784ec8abd8ba61a98064ef”的网页防篡改规则为例。

响应样例

```
{
    "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
    "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
    "hostname": "www.aaa.com",
    "path": "/a",
    "timestamp": 1499817600
}
```

状态码

表4-209描述的是API返回的正常状态码。

表 4-209 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.10.5 刷新网页防篡改规则的缓存

功能介绍

若防篡改的网页内容有修改，需要WAF重新缓存网页内容，可刷新某个网页防篡改规则中的缓存。

URI

- URI格式

  POST /v1/{project_id}/waf/policy/{policy_id}/antitamper/{antitamper_rule_id}/cache

- 参数说明

  表 4-210 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
antitamper_rule_id	是	String	网页防篡改规则的ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-211 响应参数说明

名称	参数类型	说明
id	String	网页防篡改规则ID。
policy_id	String	策略ID。
hostname	String	防护域名。
path	String	防篡改的URL链接，不包含域名。
timestamp	Long	缓存的更新时间。

示例

如下以刷新缓存为例。

响应样例

```
{
    "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
    "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
    "hostname": "www.aaa.com",
    "path": "/a",
    "timestamp": 1499817600
}
```

状态码

表4-212描述的是API返回的正常状态码。

表 4-212 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.11 误报屏蔽规则

4.1.11.1 查询误报屏蔽规则列表

功能介绍

查询某个策略下所有的误报屏蔽规则列表。

URI

- URI格式

  GET /v1/{project_id}/waf/policy/{policy_id}/ignore?path={path}&offset={offset}&limit={limit}

- 参数说明

  表 4-213 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
path	否	String	误报路径。
offset	否	Long	指定返回的页数，取值范围为：[0, 65535]，默认值为0。
limit	否	Long	指定查询返回每页记录的最大条数，取值范围为：(0, 50]，默认值为10。

请求消息

请求参数

无

响应消息

响应参数

表 4-214 响应参数说明

名称	参数类型	说明
total	Integer	Policy的总数量。
items	表3	误报屏蔽规则对象列表。

表 4-215 items

名称	参数类型	说明
id	String	误报屏蔽规则ID。
policy_id	String	策略ID。

名称	参数类型	说明
path	String	误报路径，完整的URL链接，不包含域名。
event_id	String	防护事件的ID。
event_type	String	事件类型。
rule	String	屏蔽的规则ID，由6位数字组成，不能为空。
timestamp	Long	创建误报屏蔽规则的时间。

示例

如下以查询误报屏蔽规则列表，返回记录条数为“2”为例。

响应样例

```
{
  "total": 2,
  "items": [{
      "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
      "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
      "event_id": "02d3ac3cd99f440daf8d38e03cf0e2a6",
      "event_type": "xss",
      "rule": "100001",
      "timestamp": 1499817600,
      "path": "/a"
    }, {
      "id": "44d887434169475794b2717438f7fa78",
      "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
      "event_id": "f8c74b656a9d4d329dbcefe0969cc427",
      "event_type": "sqli",
      "rule": "100002",
      "timestamp": 1499817600,
      "path": "/a"
    }
  ]
}
```

状态码

表4-216描述的是API返回的正常状态码。

表 4-216 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.11.2 创建误报屏蔽规则

功能介绍

创建误报屏蔽。

URI

- URI格式
  POST /v1/{project_id}/waf/policy/{policy_id}/ignore
- 参数说明

  表 4-217 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。

请求消息

请求参数

表 4-218 请求参数说明

名称	是否必选	参数类型	说明
path	是	String	误报路径，完整的URL链接，不包含域名。
event_id	是	String	防护事件的ID。 “防护事件”列表中事件类型为非“自定义规则”的误报攻击事件所对应的事件ID。可单击该攻击事件所在行的“误报处理”获取事件ID。

响应消息

响应参数

表 4-219 响应参数说明

名称	参数类型	说明
id	String	误报屏蔽规则ID。
policy_id	String	策略ID。

名称	参数类型	说明
path	String	误报路径，完整的URL链接，不包含域名。
event_id	String	防护事件的ID。
event_type	String	事件类型。
timestamp	Long	创建误报屏蔽规则的时间。
rule	String	屏蔽的规则ID，由6位数字组成，不能为空。

示例

如下以创建一条误报屏蔽规则“100001”为例。

- 请求样例

```
{
  "path": "/a",
  "event_id": "3737fb122f2140f39292f597ad3b7e9a"

}
```

- 响应样例

```
{
  "id": "6cdc116040d444f6b3e1bf1dd629f1d0",
  "policy_id": "44d887434169475794b2717438f7fa78",
  "path": "/a",
  "event_id": "3737fb122f2140f39292f597ad3b7e9a",
  "event_type": "xss",
  "rule": "100001",
  "timestamp": 1499817600
}
```

状态码

表4-220描述的是API返回的正常状态码。

表 4-220 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.11.3 删除误报屏蔽规则

功能介绍

删除误报屏蔽规则。

URI

- URI格式
  DELETE /v1/{project_id}/waf/policy/{policy_id}/ignore/{ignore_rule_id}
- 参数说明

  表 4-221 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
ignore_rule_id	是	String	误报屏蔽规则的ID。

请求消息

请求参数

无

响应消息

响应参数

无

状态码

表4-222描述的是API返回的正常状态码。

表 4-222 状态码

状态码	编码	状态说明
204	No Content	服务器成功处理了请求，没有返回任何内容。

异常状态码，请参见状态码。

4.1.11.4 查询误报屏蔽规则

功能介绍

查询误报屏蔽规则的详细信息。

URI

- URI格式
  GET /v1/{project_id}/waf/policy/{policy_id}/ignore/{ignore_id}

- 参数说明

  表 4-223 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
ignore_id	是	String	误报屏蔽规则的ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-224 响应参数说明

名称	参数类型	说明
id	String	误报屏蔽规则ID。
policy_id	String	策略ID。
path	String	误报路径，完整的URL链接，不包含域名。
event_id	String	防护事件的ID。
event_type	String	事件类型。
timestamp	Long	创建误报屏蔽规则的时间。
rule	String	屏蔽的规则ID，由6位数字组成，不能为空。

示例

- 响应样例

```
{
  "id": "6cdc116040d444f6b3e1bf1dd629f1d0",
  "policy_id": "44d887434169475794b2717438f7fa78",
  "path": "/a",
  "event_id": "3737fb122f2140f39292f597ad3b7e9a",
  "event_type": "xss",
  "rule": "100001",
  "timestamp": 1499817600
}
```

状态码

表4-225描述的是API返回的正常状态码。

表 4-225 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.11.5 更新误报屏蔽规则

功能介绍

更新误报屏蔽规则。

URI

- URI格式
  PUT /v1/{project_id}/waf/policy/{policy_id}/ignore/{ignore_id}
- 参数说明

  表 4-226 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
policy_id	是	String	策略ID。
ignore_id	是	String	误报屏蔽规则的ID。

请求消息

请求参数

表 4-227 请求参数说明

名称	是否必选	参数类型	说明
path	否	String	误报路径，完整的URL链接，不包含域名。

名称	是否必选	参数类型	说明
event_id	否	String	防护事件的ID。 “防护事件”列表中事件类型为非“自定义规则”的误报攻击事件所对应的ID。可单击该攻击事件所在行的“误报处理”获取事件ID。

响应消息

响应参数

表 4-228 响应参数说明

名称	参数类型	说明
id	String	误报屏蔽规则ID。
policy_id	String	策略ID。
path	String	误报路径，完整的URL链接，不包含域名。
event_id	String	防护事件的ID。
event_type	String	事件类型。
timestamp	Long	创建误报屏蔽规则的时间。
rule	String	屏蔽的规则ID，由6位数字组成，不能为空。

示例

- 请求样例

```
{
  "path": "/a",
  "event_id": "3737fb122f2140f39292f597ad3b7e9a"
}
```

- 响应样例

```
{
  "id": "6cdc116040d444f6b3e1bf1dd629f1d0",
  "policy_id": "44d887434169475794b2717438f7fa78",
  "path": "/a",
  "event_id": "3737fb122f2140f39292f597ad3b7e9a",
  "event_type": "xss",
  "rule": "100001",
  "timestamp": 1499817600
}
```

状态码

表4-229描述的是API返回的正常状态码。

表 4-229 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见**状态码**。

4.1.12 事件日志查询

4.1.12.1 查询攻击事件日志

功能介绍

查询事件详情列表。

URI

- URI格式

  GET /v1/{project_id}/waf/event?from={from}&to={to}&hosts={hostname}&attacks={attack}&sips={sip}&offset={offset}&limit={limit}

  说明

  样例如下：

  GET /v1/3ac26c59e15a4a11bb680a103a29ddb6/waf/event/attack/type?from=1543976973635&to=1563976973635&hosts=3211757cafa3437aae24d760022e79ba&hosts=93029844064b43739b51ca63036fbc4b&hosts=34fe5f5c60ef4e43a9975296765d1217

- 参数说明

  表 4-230 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
from	是	Long	开始时间UTC miliseconds。例如，from的值为“1548172800000”。
to	是	Long	结束时间UTC miliseconds。例如，to的值为“1548431999000”。
hosts	否	Array	防护域名的ID。
attacks	否	Array	攻击类型列表。例如，attacks=sqli&attacks=xss。

名称	是否必选	参数类型	说明
sips	否	Array	攻击源IP。例如，sips=X.X.12.23&sips=X.X.20.85。
nsips	否	Array	排除的攻击源IP。例如，nsips=X.X.12.1&nsips=X.X.20.2。
offset	否	Long	指定返回的页数，取值范围为：[0, 65535)，默认值为0。
limit	否	Long	指定查询返回每页记录的最大条数，取值范围为：(0, 50]，默认值为10。
marker	否	String	事件ID，取值为上一页数据的最后一条记录的ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-231 响应参数说明

名称	参数类型	说明
total	Integer	日志事件的总数量。
items	表3	攻击事件日志对象列表

表 4-232 items

名称	参数类型	说明
id	String	攻击事件ID。
time	Integer	攻击事件时间（Milliseconds since Unix Epoch）。
policy_id	String	策略ID。
sip	String	攻击源的IP。
host	String	被攻击的域名。

名称	参数类型	说明
host_id	String	域名ID。
url	String	攻击的URL链接，不包含域名。
attack	String	攻击类型。 ● “cc”代表CC攻击。 ● “cmdi”代表命令注入。 ● “custom”代表精准防护。 ● “illegal”代表非法请求。 ● “sqli”代表SQL注入。 ● “lfi”代表本地文件包含。 ● "robot"代表恶意爬虫。 ● “antitamper”代表网页防篡改。 ● “rfi”代表远程文件包含。 ● “vuln”代表其他类型攻击。 ● “xss”代表xss攻击。 ● “whiteblackip”代表IP黑白名单。 ● “webshell”代表网站木马。
rule	String	命中的规则ID，由6位数字组成。
payload	String	命中的载荷。
action	String	防护动作。 ● “Block”： 拦截。 ● “Log only”： 仅记录不拦截。 ● “Allow”： 放行。 ● “Verification code”： 验证码验证。 ● “Filter”： 过滤。 ● “Mismatch”： 不匹配。
payload_location	String	攻击发生在请求报文的位置。取值范围为：body、url、params、header。
request_line	String	攻击请求的方法。
headers	Object	攻击请求头部。
cookie	String	cookie。

名称	参数类型	说明
body	String	攻击请求的请求体。

示例

如下以查询攻击事件日志，返回记录条数为“2”为例。

响应样例


```
{
  "total": 2,
  "items": [
    {
      "id": "0000-0000-0000-13-56ef71f5745764348192f844658dd144",
      "time": 1499817600,
      "policy_id": "xxx",
      "sip": "X.X.1.1",
      "host": "a.com",
      "host_id": "123",
      "url": "/login",
      "attack": "sqli",
      "rule": "20001",
      "payload": "1 or 1=1",
      "action": "block",
      "payload_location": "params",
      "request_line": "GET / ",
      "headers": {
        "Connection": "keep-alive",
        "User-Agent": "curl"
      },
      "cookie": "sid=123; uid=456",
      "body": "user=admin&pass=abc123"
    },
    {
      "id": "0000-0000-0000-13-56ef71f5745764348192f844658dd144",
      "time": 1499817600,
      "host": "a.com",
      "host_id": "a",
      "policy_id": "xxx",
      "sip": "X.X.1.2",
      "url": "/login",
      "attack": "sqli",
      "rule": "20001",
      "payload": "1 or 1=1",
      "action": "log",
      "payload_location": "params",
      "request_line": "GET / ",
      "headers": {
        "Connection": "keep-alive",
        "User-Agent": "curl"
      },
      "cookie": "sid=123; uid=456",
      "body": "user=admin&pass=abc123"
    }
  ]
}
```


状态码

表4-233描述的是API返回的正常状态码。

表 4-233 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见**状态码**。

4.1.12.2 根据 ID 查询攻击事件日志

功能介绍

通过ID来查询攻击事件日志。

URI

- URI格式
  GET /v1/{project_id}/waf/event/{event_id}
- 参数说明

  表 4-234 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
event_id	是	String	事件ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-235 响应参数说明

名称	参数类型	说明
id	String	攻击事件ID。
time	Integer	攻击事件时间（Milliseconds since Unix Epoch）。
policy_id	String	策略ID。
sip	String	攻击源的IP。

名称	参数类型	说明
host	String	被攻击的域名。
host_id	String	域名的ID。
url	String	攻击的URL链接，不包含域名。
attack	String	攻击类型。
rule	String	命中的规则ID。
payload	String	命中的载荷。
action	String	防护动作。 ● “Block”：拦截。 ● “Log only”：仅记录不拦截。 ● “Allow”：放行。 ● “Verification code”：验证码验证。 ● “Filter”：过滤。 ● “Mismatch”：不匹配。
payload_location	String	攻击发生在请求报文的位置。取值范围为：body、url、params、header。
request_line	String	攻击请求的方法。
headers	Object	攻击请求头部。
cookie	String	cookie。
body	String	攻击请求的请求体。

示例

如下以根据id“0000-0000-0000-13-56ef71f5745764348192f844658dd144”查询攻击事件日志为例。

响应样例

```
{
    "id": "0000-0000-0000-13-56ef71f5745764348192f844658dd144",
     "time": 1499817600,
     "policy_id": "xxx",
     "sip": "X.X.1.1",
     "host": "a.com",
     "host_id": "123",
     "url": "/login",
     "attack": "sqli",
     "rule": "20001",
     "payload": "1 or 1=1",
     "action": "block",
     "payload_location": "params",
     "request_line": "GET / ",
```

```
  "headers": {
    "Connection": "keep-alive",
    "User-Agent": "curl"
  },
  "cookie": "sid=123; uid=456",
  "body": "user=admin&pass=abc123"
}
```

状态码

表4-236描述的是API返回的正常状态码。

表 4-236 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.12.3 查询事件类型分布

功能介绍

查询事件分布类型。

URI

- URI格式

  GET /v1/{project_id}/waf/event/attack/type?
  from={from}&to={to}&hosts={hostids}

  说明

  样例如下：

  GET /v1/3ac26c59e15a4a11bb680a103a29ddb6/waf/event/attack/type?
  from=1543976973635&to=1563976973635&hosts=3211757cafa3437aae24d760022e79ba&hosts=93029844064b43739b51ca63036fbc4b&hosts=34fe5f5c60ef4e43a9975296765d1217

- 参数说明

  表 4-237 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
from	是	Long	开始时间UTC miliseconds。例如，from的值为“1548172800000”。

名称	是否必选	参数类型	说明
to	是	Long	结束时间UTC miliseconds。例如，to的值为“1548431999000”。
hosts	否	Array	防护域名的ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-238 响应参数说明

名称	参数类型	说明
xss	Integer	时间区间内xss攻击的数量。
sqli	Integer	时间区间内sqli攻击的数量。
cmdi	Integer	时间区间内cmdi攻击的数量。
cc	Integer	时间区间内cc攻击的数量。
custom	Integer	时间区间内对自定义规则攻击的数量。
illegal	Integer	时间区间内非法请求的数量。
lfi	Integer	时间区间内lfi攻击的数量。
robot	Integer	恶时间区间内恶意爬虫的数量。
antitamper	Integer	时间区间内网页篡改攻击的数量。
rfi	Integer	时间区间内rfi攻击的数量。
vuln	Integer	时间区间内其他攻击的数量。

名称	参数类型	说明
whiteblackip	Integer	时间区间内黑白名单的数量。
webshell	Integer	时间区间内webshell攻击的数量。

示例

如下以查询事件类型分布为例。

响应样例

```
{
    "xss": 150,
    "sqli": 321,
    "cmdi": 120,
    "robot": 10,
    "whiteblackip": 30,
    "custom": 50,
    "cc": 60,
    "illegal": 10
}
```

状态码

表4-239描述的是API返回的正常状态码。

表 4-239 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.12.4 查询请求/攻击数量统计

功能介绍

查询请求/攻击数量统计。

URI

- URI格式

  GET /v1/{project_id}/waf/event/timeline?
  from={from}&to={to}&timezone={timezone}&hosts={hostids}

说明

样例如下：

GET /v1/3ac26c59e15a4a11bb680a103a29ddb6/waf/event/attack/type?from=1543976973635&to=1563976973635&hosts=3211757cafa3437aae24d760022e79ba&hosts=93029844064b43739b51ca63036fbc4b&hosts=34fe5f5c60ef4e43a9975296765d1217

- 参数说明

表 4-240 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
from	是	Long	开始时间UTC miliseconds。例如，from的值为“1548172800000”。
to	是	Long	结束时间UTC miliseconds。例如，to的值为“1548431999000”。
timezone	否	String	时区，例如伦敦的时区是“+00:00”。默认是“+00:00”。
hosts	否	Array	防护域名的ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-241 响应参数说明

名称	参数类型	说明
requests	List of 表3	请求个数列表。
attacks	List of 表4	攻击次数列表。

表 4-242 requests

名称	参数类型	说明
time	Integer	统计终止时间点（Milliseconds since Unix Epoch）。
num	Integer	统计计数。

表 4-243 attacks

名称	参数类型	说明
time	Integer	统计终止时间点（Milliseconds since Unix Epoch）。
num	Integer	统计计数。

示例

如图以查询请求/攻击数量统计为例。

响应样例

```
{
  "requests": [
        {"time": 1499817600, "num": 123400},
        {"time": 1499817601, "num": 123401},
        {"time": 1499817602, "num": 123402}
  ],
  "attacks": [
        {"time": 1499817600, "num": 1234},
        {"time": 1499817601, "num": 1235},
        {"time": 1499817602, "num": 1236}
  ]
}
```

状态码

表4-244描述的是API返回的正常状态码。

表 4-244 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.12.5 查询攻击数量

功能介绍

查询攻击数量。

URI

- URI格式

  GET /v1/{project_id}/waf/event/attack/num?
  from={from}&to={to}&hosts={hostids}

  说明

  样例如下：

  GET /v1/3ac26c59e15a4a11bb680a103a29ddb6/waf/event/attack/type?
  from=1543976973635&to=1563976973635&hosts=3211757cafa3437aae24d760022e79ba&hosts=93029844064b43739b51ca63036fbc4b&hosts=34fe5f5c60ef4e43a9975296765d1217

- 参数说明

  表 4-245 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
from	是	String	开始时间UTC miliseconds。例如，from的值为“1548172800000”。
to	是	String	结束时间UTC miliseconds。例如，to的值为“1548431999000”。
hosts	否	Array	防护域名的ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-246 响应参数说明

名称	参数类型	说明
attack_num	Integer	攻击数量。

示例

如下以查询攻击数量为例。

响应样例

```
{
  "attack_num":  150
}
```

状态码

表4-247描述的是API返回的正常状态码。

表 4-247 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.12.6 查询攻击源 IP TOPN

功能介绍

查询攻击源IP TopN。

URI

- URI格式

  GET /v1/{project_id}/waf/event/attack/source?top={top}&from={from}&to={to}&hosts={hostids}

  说明

  样例如下：

  GET /v1/3ac26c59e15a4a11bb680a103a29ddb6/waf/event/attack/type?from=1543976973635&to=1563976973635&hosts=3211757cafa3437aae24d760022e79ba&hosts=93029844064b43739b51ca63036fbc4b&hosts=34fe5f5c60ef4e43a9975296765d1217

- 参数说明

  表 4-248 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
top	否	Integer	指定查询攻击量排名，默认值为5。

名称	是否必选	参数类型	说明
from	是	Long	开始时间UTC miliseconds。例如，from的值为“1548172800000”。
to	是	Long	结束时间UTC miliseconds。例如，to的值为“1548431999000”。
hosts	否	Array	防护域名的ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-249 响应参数说明

名称	参数类型	说明
total	Integer	攻击源IP的总数量。
items	表3	对象数组。

表 4-250 items

名称	参数类型	说明
ip	String	攻击源IP地址。
num	Integer	攻击源IP的攻击次数。

示例

如下以查询攻击源IP TOP5为例。

响应样例

```
{
  "total": 4,
  "items": [
    {"ip": "X.X.1.1", "num": 1000},
    {"ip": "X.X.1.2", "num": 1000},
    {"ip": "X.X.1.3", "num": 1000},
    {"ip": "X.X.1.4", "num": 1000}
  ]
}
```

状态码

表4-251描述的是API返回的正常状态码。

表 4-251 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.12.7 查询攻击源 IP 的个数

功能介绍

查询攻击源IP的个数。

URI

- URI格式

  GET /v1/{project_id}/waf/event/attack/source/num?from={from}&to={to}&hosts={hostids}

  说明

  样例如下：

  GET /v1/3ac26c59e15a4a11bb680a103a29ddb6/waf/event/attack/type?from=1543976973635&to=1563976973635&hosts=3211757cafa3437aae24d760022e79ba&hosts=93029844064b43739b51ca63036fbc4b&hosts=34fe5f5c60ef4e43a9975296765d1217

- 参数说明

  表 4-252 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
from	是	Long	开始时间UTC miliseconds。例如，from的值为“1548172800000”。
to	是	Long	结束时间UTC miliseconds。例如，to的值为“1548431999000”。
hosts	否	Array	防护域名的ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-253 响应参数说明

名称	参数类型	说明
sip	Integer	攻击源IP个数。

示例

如下以查询攻击源IP的个数为例。

响应样例

```
{
  "sip":  50
}
```

状态码

表4-254描述的是API返回的正常状态码。

表 4-254 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.12.8 查询请求 QPS

功能介绍

查询每秒多少请求。

URI

- URI格式

  GET /v1/{project_id}/waf/event/request/peak?from={from}&to={to}&hosts={hostids}

说明

样例如下：

GET /v1/3ac26c59e15a4a11bb680a103a29ddb6/waf/event/attack/type?from=1543976973635&to=1563976973635&hosts=3211757cafa3437aae24d760022e79ba&hosts=93029844064b43739b51ca63036fbc4b&hosts=34fe5f5c60ef4e43a9975296765d1217

- 参数说明

表 4-255 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
from	是	Long	开始时间UTC miliseconds。例如，from的值为“1548172800000”。
to	是	Long	结束时间UTC miliseconds。例如，to的值为“1548431999000”。
hosts	否	Array	防护域名的ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-256 响应参数说明

名称	参数类型	说明
qps	Integer	所有请求的每秒请求数。

示例

如下以查询请求QPS为例。

响应样例

```
{
"qps": 800
}
```

状态码

表4-257描述的是API返回的正常状态码。

表 4-257 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见**状态码**。

4.1.12.9 查询攻击日志文件列表

功能介绍

查询攻击日志下载列表。

URI

- URI格式
  GET /v1/{project_id}/waf/event/dump?offset={offset}&limit={limit}
- 参数说明

  表 4-258 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
offset	否	Long	指定返回的页数，取值范围为：[0, 65535]，默认值为0。
limit	否	Long	指定查询返回每页记录的最大条数，取值范围为：(0, 50]，默认值为10。

请求消息

请求参数

无

响应消息

响应参数

表 4-259 响应参数说明

名称	参数类型	说明
total	Integer	日志文件的总数量。

名称	参数类型	说明
items	表3	日志文件对象列表。

表 4-260 items

名称	参数类型	说明
id	String	日志文件的ID。
filename	String	日志文件的名称。
total	Integer	日志文件中的事件数量。
url	String	日志文件下载的地址。
timestamp	Long	生成日志文件的时间。

示例

如下以查询攻击日志列表，返回记录条数为“2”为例。

响应样例

```
{
  "total": 2,
  "items": [{
      "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
      "filename": "",
      "total": "100",
      "url": "https://obs_server/obs-waf-log/-2019-01-15-xxxxxxxxxx.csv?
AWSAccessKeyId=XXXXXXXXXXXX&Expires=1547632&Signature=nC7ipaGzLQs",
      "timestamp": 1499817600
    }, {
      "id": "44d887434169475794b2717438f7fa78",
      "filename": "W-2019-01-14.csv",
      "total": "200",
      "url": "https://obs_server/obs-waf-log/-2019-01-14-xxxxxxxxxx.csv?
AWSAccessKeyId=XXXXXXXXXXXX&Expires=1547632&Signature=nC7ipaGzLQs",
      "timestamp": 1499817601
    }
  ]
}
```

4.1.13 告警通知配置

只能查看、修改当前租户已订阅的告警项。

4.1.13.1 查询告警通知配置

功能介绍

查询告警通知配置。

URI

- URI格式
  GET /v1/{project_id}/waf/config/alert
- 参数说明

  表 4-261 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-262 响应参数说明

名称	参数类型	说明
id	String	告警配置的唯一标识。
enabled	Boolean	是否发送告警通知。 ● true：发送告警通知。 ● false：不发送告警通知。
topic_urn	String	发送到哪个告警通知的SMN群组。
sendfreq	Integer	发送告警的最低时间限制，单位是“分钟”，最小取值为5，固定取值5、15、30、60。
times	Integer	固定时间内告警的次数，小于这个次数则不发送告警通知。取值大于等于1。

名称	参数类型	说明
threat	List<String>	事件类型列表。 ● “all”代表全部。 ● “cc”代表CC攻击。 ● “cmdi”代表命令注入。 ● “custom”代表精准防护。 ● “illegal”代表非法请求。 ● “sqli”代表SQL注入。 ● “lfi”代表本地文件包含。 ● "robot"代表恶意爬虫。 ● “antitamper”代表网页防篡改。 ● “rfi”代表远程文件包含。 ● “vuln”代表其他类型攻击。 ● “xss”代表xss攻击。 ● “whiteblackip”代表IP黑白名单。 ● “webshell”代表网站木马。
locale	String	语言配置，只支持zh-cn简体中文、en-us美式英文，默认是en-us。

示例

如下以查询告警通知配置为例。

响应样例

```
{
    "id": "37b4bbe8a562453aa0163a96e6b71dd6",
    "enabled": true,
    "topic_urn": "urn:smn:eude:fca6f667ac5f4d9798d1641dfd38106b:wbtest",
    "sendfreq": 5,
    "times": 200,
    "threat": ["xss", "sqli", "cmdi"],
    "locale": "en-us"
}
```

状态码

表4-263描述的是API返回的正常状态码。

表 4-263 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.1.13.2 更新告警通知配置

功能介绍

更新告警通知配置。

URI

- URI格式
  PUT /v1/{project_id}/waf/config/alert/{alertconfig_id}
- 参数说明

表 4-264 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
alertconfig_id	是	String	需要更新的告警通知配置ID。请参考**查询告警通知配置**查询告警通知配置ID。

请求消息

请求参数

表 4-265 请求参数说明

名称	是否必选	参数类型	说明
enabled	是	Boolean	是否发送告警通知。 • true：发送告警通知。 • false：不发送告警通知。
topic_urn	是	String	发送到哪个告警通知群组。 **说明** 选择的告警通知群组必须为有效的群组，即已经在SMN里完成了订阅信息配置的主题群组。
sendfreq	是	Integer	发送告警的最低时间限制，单位是“分钟”，最小取值为5，固定取值5、15、30、60。
times	是	Integer	固定时间内告警的次数，小于这个次数则不发送告警通知。取值大于等于1。

名称	是否必选	参数类型	说明
threat	是	List<String>	事件类型列表。 ● “all”代表全部。 ● “cc”代表CC攻击。 ● “cmdi”代表命令注入。 ● “custom”代表精准防护。 ● “illegal”代表非法请求。 ● “sqli”代表SQL注入。 ● “lfi”代表本地文件包含。 ● “robot”代表恶意爬虫。 ● “antitamper”代表网页防篡改。 ● “rfi”代表远程文件包含。 ● “vuln”代表其他类型攻击。 ● “xss”代表xss攻击。 ● “whiteblackip”代表IP黑白名单。 ● “webshell”代表网站木马。
locale	否	String	语言配置，只支持zh-cn简体中文、en-us美式英文，默认是en-us。

响应消息

响应参数

表 4-266 响应参数说明

名称	参数类型	说明
id	String	告警配置的唯一标识。
enabled	Boolean	是否发送告警通知。 ● true：发送告警通知。 ● false：不发送告警通知。
topic_urn	String	自定义选择的告警通知群组，用户通过该群组设置的电话或者邮箱地址接收告警通知。
sendfreq	Integer	发送告警的最低时间限制，单位是“分钟”，最小取值为5，固定取值5、15、30、60。
times	Integer	固定时间内告警的次数，小于这个次数则不发送告警通知。取值大于等于1。

名称	参数类型	说明
threat	List<String>	事件类型列表。 • “all”代表全部。 • “cc”代表CC攻击。 • “cmdi”代表命令注入。 • “custom”代表精准防护。 • “illegal”代表非法请求。 • “sqli”代表SQL注入。 • “lfi”代表本地文件包含。 • “robot”代表恶意爬虫。 • “antiTamper”代表网页防篡改。 • “rfi”代表远程文件包含。 • “vuln”代表其他类型攻击。 • “xss”代表xss攻击。 • “whiteblackip”代表IP黑白名单。 • “webshell”代表网站木马。
locale	String	语言配置，只支持zh-cn简体中文、en-us美式英文，默认是en-us。

示例

如下以更新告警通知配置为例。

- 请求样例

```
{
    "enabled": true,
    "topic_urn": "urn:smn:eude:fca6f667ac5f4d9798d1641dfd38106b:wbtest",
    "sendfreq": 5,
    "times": 200,
    "threat": ["xss", "sqli", "cmdi"]
}
```

- 响应样例

```
{
    "id": "37b4bbe8a562453aa0163a96e6b71dd6",
    "enabled": true,
    "topic_urn": "urn:smn:eude:fca6f667ac5f4d9798d1641dfd38106b:wbtest",
    "sendfreq": 5,
    "times": 200,
    "threat": ["xss", "sqli", "cmdi"],
    "locale": "en-us"
}
```

状态码

表4-267描述的是API返回的正常状态码。

表 4-267 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见**状态码**。

4.1.14 获取选项信息

4.1.14.1 查询告警通知中事件类型选项的详细信息

功能介绍

查询告警通知中事件类型选项的详细信息。

URI

- URI格式
  GET /v1/{project_id}/waf/map/threat?lang={lang}
- 参数说明

  表 4-268 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
lang	否	String	语言类型，zh-cn代表中文，en-us代表英文，默认是英文。

请求消息

请求参数

无

响应消息

响应参数

表 4-269 响应参数说明

名称	参数类型	说明
threats	List	对应的选项。
locale	**表3**	对应的名称。

表 4-270 locale

名称	参数类型	说明
xss	String	跨站脚本攻击。
sqli	String	SQL注入攻击。
cmdi	String	命令注入攻击。
cc	String	CC攻击。
custom	String	精准防护。
illegal	String	非法请求。
lfi	String	本地文件包含。
robot	String	恶意爬虫。
antitamper	String	网页防篡改。
rfi	String	远程文件包含。
vuln	String	其他类型攻击。
whiteblackip	String	IP黑白名单。
webshell	String	网站木马。

示例

如下以查询告警通知中事件类型选择的详细信息为例。

响应样例

```
{
  "threats": ["xss", "sqli", "cmdi"],
  "locale": {
      "xss":  "Cross Site Scripting",
      "sqli": "SQL Injection",
      "cmdi": "Command Injection"
   }
}
```

状态码

表4-271描述的是API返回的正常状态码。

表 4-271 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见**状态码**。

4.1.14.2 查询获取真实源 IP 的 HTTP 请求头的选项信息

功能介绍

查询获取真实源IP的HTTP请求头的选项信息。

URI

- URI格式
  GET /v1/{project_id}/waf/map/sipheader?lang={lang}
- 参数说明

表 4-272 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
lang	否	String	语言类型，zh-cn代表中文，en-us代表英文，默认是英文。

请求消息

请求参数

无

响应消息

响应参数

表 4-273 响应参数说明

名称	参数类型	说明
sipheadermap	**表3**	对应的选项。
locale	**表4**	对应的名称。

表 4-274 sipheadermap

名称	参数类型	说明
default	Array	默认获取真实源IP的HTTP请求头。

名称	参数类型	说明
cloudflare	Array	CloudFlare获取真实源IP的HTTP请求头。
akamai	Array	Akamai获取真实源IP的HTTP请求头。
custom	Array	自定义获取真实源IP的HTTP请求头。

表 4-275 locale

名称	参数类型	说明
default	String	默认。
cloudflare	String	CloudFlare。
akamai	String	Akamai。
custom	String	自定义。

示例

如下以查询获取真实源IP的HTTP请求头为例。

响应样例

```
{
  "sipheadermap": {
      "default": ["X-Forwarded-For"],
      "cloudflare": ["CF-Connecting-IP", "X-Forwarded-For"],
      "akamai": ["True-Client-IP"],
      "custom": []
  },
  "locale": {
       "default": "Default",
       "cloudflare": "CloudFlare",
       "akamai": "Akamai",
       "custom": "Custom"
   }
}
```

状态码

表4-276描述的是API返回的正常状态码。

表 4-276 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见**状态码**。

4.1.15 对接 Cloud Eye

4.1.15.1 查询实例名称和状态

功能介绍

查询对接Cloud Eye的实例名称和状态。

URI

- URI格式
  GET /v1/{project_id}/waf/instance/{instance_id}/metrics
- 参数说明

  表 4-277 Path 参数说明

名称	是否必选	参数类型	说明
project_id	是	String	用户操作的项目ID。
instance_id	是	String	实例ID。

请求消息

请求参数

无

响应消息

响应参数

表 4-278 响应参数说明

名称	参数类型	说明
waf_instance_id	String	指标维度的标识符。
name	String	资源实例名称。
status	String	资源实例状态。

示例

如下以查询实例名称和状态为例。

响应样例

```
{
    "waf_instance_id": "dhbvhdfbvdhbasdkjvfhwoow",
    "name": "www.test.com",
    "status": "enable"
}
```

状态码

表4-279描述的是API返回的正常状态码。

表 4-279 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。

异常状态码，请参见状态码。

4.2 独享模式

4.2.1 独享实例管理

4.2.1.1 查询 WAF 独享引擎列表

功能介绍

查询WAF独享引擎列表

URI

GET /v1/{project_id}/premium-waf/instance

表 4-280 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID

表 4-281 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id
page	否	Integer	分页查询参数，默认值为1
pagesize	否	Integer	分页查询参数，每页包含多少条记录，默认值为10
instancename	否	String	模糊查询，独享引擎名称

请求参数

表 4-282 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-283 响应 Body 参数

参数	参数类型	描述
total	Integer	独享引擎实例数量
purchased	Boolean	是否曾经购买过独享引擎
items	Array of **ListInstance** objects	详细的独享引擎信息列表

表 4-284 ListInstance

参数	参数类型	描述
id	String	独享引擎实例ID
instancename	String	独享引擎实例名称
region	String	独享引擎实例Region ID
zone	String	可用区ID
arch	String	CPU架构
cpu_flavor	String	ECS规格
vpc_id	String	独享引擎实例所在VPC ID
subnet_id	String	独享引擎实例所在VPC的子网ID
service_ip	String	独享引擎实例的业务面IP
security_group_ids	Array of strings	独享引擎绑定的安全组
status	Integer	独享引擎计费状态 ● 0：正常计费 ● 1：冻结,资源和数据会保留，但租户无法再正常使用云服务 ● 2：终止，资源和数据将清除
run_status	Integer	独享引擎运行状态 ● 0：创建中 ● 1：运行中 ● 2：删除中 ● 3：已删除 ● 4：创建失败 ● 5：已冻结 ● 6：异常 ● 7：更新中 ● 8：更新失败
access_status	Integer	独享引擎接入状态（0：未接入，1：已接入）
upgradable	Integer	独享引擎是否可升级（0：不可升级，1：可升级）
cloudServiceType	String	云服务代码。 仅作为标记，用户可忽略。
resourceType	String	云服务资源类型，仅作为标记，用户可忽略。

参数	参数类型	描述
resourceSpecCode	String	云服务资源代码。仅作为标记，用户可忽略。
specification	String	独享引擎ECS规格，如"8vCPUs | 16GB"
hosts	Array of IdHostnameEntry objects	独享引擎防护的域名
serverId	String	独享引擎ECS ID
create_time	Long	引擎实例创建时间
instance_name	String	独享引擎实例名称

表 4-285 IdHostnameEntry

参数	参数类型	描述
id	String	防护域名ID
hostname	String	防护域名

状态码： 400

表 4-286 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-287 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-288 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{endpoint}/v1/{project_id}/premium-waf/instance
```

响应示例

状态码： 200

独享引擎信息列表

```
{
  "purchased" : true,
  "total" : 1,
  "items" : [ {
    "id" : "0619871acb764d48a112695e8f7cbb10",
    "region" : "region-01-7",
    "zone" : "region-01-7a",
    "specification" : "8vCPUs | 16GB",
    "arch" : "x86",
    "upgradable" : 0,
    "status" : 0,
    "serverId" : "477353dc-8687-4bf4-b45b-1d7fee74fa63",
    "cloudServiceType" : "hws.service.type.waf",
    "resourceType" : "hws.resource.type.waf.instance",
    "resourceSpecCode" : "waf.instance.enterprise",
    "vpc_id" : "13718074-a3f9-408d-82aa-3c41ef55e589",
    "subnet_id" : "74d1b5a6-c7eb-4e9a-8372-181212552fcc",
    "service_ip" : "192.168.10.68",
    "security_group_ids" : [ "34287bdb-7aba-471a-b041-27427f1af76a" ],
    "cpu_flavor" : "Si2.2xlarge.2",
    "run_status" : 2,
    "access_status" : 1,
    "hosts" : [ {
      "id" : "c3be17bbe3a641c7a1ded6019c377402",
      "hostname" : "demo.www.com"
    } ],
    "instance_name" : "0412elb"
  } ]
}
```

状态码

状态码	描述
200	独享引擎信息列表
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.1.2 创建 WAF 独享引擎实例

功能介绍

创建WAF独享引擎实例

URI

POST /v1/{project_id}/premium-waf/instance

表 4-289 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID

表 4-290 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-291 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

表 4-292 请求 Body 参数

参数	是否必选	参数类型	描述
chargemode	否	Integer	收费模式，当前仅支持按需收费（30）
region	是	String	需要创建独享引擎的局点
available_zone	是	String	需要创建独享引擎的可用区
arch	是	String	独享引擎CPU架构，例如：x86与arm
instancename	是	String	独享引擎名称前缀
specification	是	String	独享引擎版本规格 • 企业版：waf.instance.enterprise • 专业版：waf.instance.professional
cpu_flavor	是	String	独享引擎ECS规格，实例规格。具体支持的规格以waf控制台上支持的规格为准。
vpc_id	是	String	独享引擎所在VPC的ID
subnet_id	是	String	独享引擎所在VPC内的子网ID
security_group	是	Array of strings	独享引擎需要绑定的安全组ID
count	是	Integer	申请的独享引擎数量
res_tenant	是	Boolean	是否为资源租户类 • true: 资源租户类

响应参数

状态码： 200

表 4-293 响应 Body 参数

参数	参数类型	描述
instances	Array of **instanceInfo** objects	instances

表 4-294 instanceInfo

参数	参数类型	描述
id	String	引擎实例ID
name	String	引擎实例名称

状态码： 400

表 4-295 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-296 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-297 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
POST https://{endpoint}/v1/{project_id}/premium-waf/instance

{
  "chargemode" : 30,
  "region" : "region-01-4",
  "available_zone" : "region-01-4a",
  "arch" : "x86",
  "instancename" : "demo",
  "specification" : "waf.instance.enterprise",
  "cpu_flavor" : "c3ne.2xlarge.2",
```

```
  "vpc_id" : "d7b6a5ff-6c53-4cd4-9d57-f20ee8753056",
  "subnet_id" : "e59ccd18-7e15-4588-b689-04b856f4e78b",
  "security_group" : [ "09b156a2-f0f0-41fd-9891-60e594601cfd" ],
  "count" : 1,
  "res_tenant" : true
}
```

响应示例

状态码： 200

独享引擎信息

```
{
  "instances" : [ {
    "id" : "50a6b6c9bdb643f9a8038976fc58ad02",
    "name" : "demo-6wvl"
  } ]
}
```

状态码

状态码	描述
200	独享引擎信息
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.1.3 查询 WAF 独享引擎信息

功能介绍

查询WAF独享引擎信息

URI

GET /v1/{project_id}/premium-waf/instance/{instance_id}

表 4-298 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID
instance_id	是	String	独享引擎ID（通过调用WAF的ListInstance接口获取所有独享引擎信息查询独享引擎ID）

表 4-299 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-300 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-301 响应 Body 参数

参数	参数类型	描述
id	String	独享引擎实例ID
instancename	String	独享引擎实例名称
region	String	独享引擎实例Region ID
zone	String	可用区ID
arch	String	CPU架构
cpu_flavor	String	ECS规格
vpc_id	String	独享引擎实例所在VPC ID
subnet_id	String	独享引擎实例所在VPC的子网ID
service_ip	String	独享引擎实例的业务面IP
security_group_ids	Array of strings	独享引擎绑定的安全组

参数	参数类型	描述
status	Integer	独享引擎计费状态 ● 0：正常计费 ● 1：冻结,资源和数据会保留，但租户无法再正常使用云服务 ● 2：终止，资源和数据将清除
run_status	Integer	独享引擎运行状态 ● 0：创建中 ● 1：运行中 ● 2：删除中 ● 3：已删除 ● 4：创建失败 ● 5：已冻结 ● 6：异常 ● 7：更新中 ● 8：更新失败
access_status	Integer	独享引擎接入状态（0：未接入，1：已接入）
upgradable	Integer	独享引擎是否可升级（0：不可升级，1：可升级）
cloudServiceType	String	云服务代码。 仅作为标记，用户可忽略。
resourceType	String	云服务资源类型，仅作为标记，用户可忽略。
resourceSpecCode	String	云服务资源代码。仅作为标记，用户可忽略。
specification	String	独享引擎ECS规格，如"8vCPUs | 16GB"
serverId	String	独享引擎ECS ID
create_time	Long	引擎实例创建时间

状态码： 400

表 4-302 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-303 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-304 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{endpoint}/v1/{project_id}/premium-waf/instance/{instance_id}
```

响应示例

状态码： 200

请求成功

```
{
  "id" : "0619871acb764d48a112695e8f7cbb10",
  "region" : "region-01-7",
  "zone" : "region-01-7a",
  "specification" : "8vCPUs | 16GB",
  "arch" : "x86",
  "upgradable" : 0,
  "status" : 0,
  "serverId" : "477353dc-8687-4bf4-b45b-1d7fee74fa63",
  "cloudServiceType" : "hws.service.type.waf",
  "resourceType" : "hws.resource.type.waf.instance",
  "resourceSpecCode" : "waf.instance.enterprise",
  "vpc_id" : "13718074-a3f9-408d-82aa-3c41ef55e589",
  "subnet_id" : "74d1b5a6-c7eb-4e9a-8372-181212552fcc",
  "service_ip" : "192.168.10.68",
  "security_group_ids" : [ "34287bdb-7aba-471a-b041-27427f1af76a" ],
  "cpu_flavor" : "Si2.2xlarge.2",
  "run_status" : 2,
  "access_status" : 1,
  "instancename" : "0412elb",
  "create_time" : 1649217360674
}
```

状态码

状态码	描述
200	请求成功
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.1.4 重命名 WAF 独享引擎

功能介绍

重命名WAF独享引擎

URI

PUT /v1/{project_id}/premium-waf/instance/{instance_id}

表 4-305 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID
instance_id	是	String	独享引擎ID（通过调用WAF的ListInstance接口获取所有独享引擎信息查询独享引擎ID）

表 4-306 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-307 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

表 4-308 请求 Body 参数

参数	是否必选	参数类型	描述
instancename	是	String	独享引擎新名称

响应参数

状态码： 200

表 4-309 响应 Body 参数

参数	参数类型	描述
id	String	独享引擎实例ID
instancename	String	独享引擎实例名称
region	String	独享引擎实例Region ID
zone	String	可用区ID
arch	String	CPU架构
cpu_flavor	String	ECS规格
vpc_id	String	独享引擎实例所在VPC ID
subnet_id	String	独享引擎实例所在VPC的子网ID
service_ip	String	独享引擎实例的业务面IP
security_group_ids	Array of strings	独享引擎绑定的安全组

参数	参数类型	描述
status	Integer	独享引擎计费状态 ● 0：正常计费 ● 1：冻结,资源和数据会保留，但租户无法再正常使用云服务 ● 2：终止，资源和数据将清除
run_status	Integer	独享引擎运行状态 ● 0：创建中 ● 1：运行中 ● 2：删除中 ● 3：已删除 ● 4：创建失败 ● 5：已冻结 ● 6：异常 ● 7：更新中 ● 8：更新失败
access_status	Integer	独享引擎接入状态（0：未接入，1：已接入）
upgradable	Integer	独享引擎是否可升级（0：不可升级，1：可升级）
cloudServiceType	String	云服务代码。 仅作为标记，用户可忽略。
resourceType	String	云服务资源类型，仅作为标记，用户可忽略。
resourceSpecCode	String	云服务资源代码。仅作为标记，用户可忽略。
specification	String	独享引擎ECS规格，如"8vCPUs | 16GB"
serverId	String	独享引擎ECS ID
create_time	Long	引擎实例创建时间

状态码： 400

表 4-310 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-311 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-312 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
PUT https://{endpoint}/v1/{project_id}/premium-waf/instance/{instance_id}

{
  "instancename" : "0412elb"
}
```

响应示例

状态码： 200

请求成功

```
{
  "id" : "0619871acb764d48a112695e8f7cbb10",
  "region" : "region-01-7",
  "zone" : "region-01-7a",
  "specification" : "8vCPUs | 16GB",
  "arch" : "x86",
  "upgradable" : 0,
  "status" : 0,
  "serverId" : "477353dc-8687-4bf4-b45b-1d7fee74fa63",
  "cloudServiceType" : "hws.service.type.waf",
  "resourceType" : "hws.resource.type.waf.instance",
  "resourceSpecCode" : "waf.instance.enterprise",
  "vpc_id" : "13718074-a3f9-408d-82aa-3c41ef55e589",
  "subnet_id" : "74d1b5a6-c7eb-4e9a-8372-181212552fcc",
  "service_ip" : "192.168.10.68",
  "security_group_ids" : [ "34287bdb-7aba-471a-b041-27427f1af76a" ],
  "cpu_flavor" : "Si2.2xlarge.2",
  "run_status" : 2,
  "access_status" : 1,
  "instancename" : "0412elb"
}
```

状态码

状态码	描述
200	请求成功
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.1.5 删除 WAF 独享引擎信息

功能介绍

删除WAF独享引擎信息

URI

DELETE /v1/{project_id}/premium-waf/instance/{instance_id}

表 4-313 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID
instance_id	是	String	独享引擎ID（通过调用WAF的ListInstance接口获取所有独享引擎信息查询独享引擎ID）

表 4-314 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-315 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-316 响应 Body 参数

参数	参数类型	描述
id	String	独享引擎实例ID
instancename	String	独享引擎实例名称
region	String	独享引擎实例Region ID
zone	String	可用区ID
arch	String	CPU架构
cpu_flavor	String	ECS规格
vpc_id	String	独享引擎实例所在VPC ID
subnet_id	String	独享引擎实例所在VPC的子网ID
service_ip	String	独享引擎实例的业务面IP
security_group_ids	Array of strings	独享引擎绑定的安全组
status	Integer	独享引擎计费状态 ● 0：正常计费 ● 1：冻结,资源和数据会保留，但租户无法再正常使用云服务 ● 2：终止，资源和数据将清除

参数	参数类型	描述
run_status	Integer	独享引擎运行状态 ● 0：创建中 ● 1：运行中 ● 2：删除中 ● 3：已删除 ● 4：创建失败 ● 5：已冻结 ● 6：异常 ● 7：更新中 ● 8：更新失败
access_status	Integer	独享引擎接入状态（0：未接入，1：已接入）
upgradable	Integer	独享引擎是否可升级（0：不可升级，1：可升级）
cloudServiceType	String	云服务代码。 仅作为标记，用户可忽略。
resourceType	String	云服务资源类型，仅作为标记，用户可忽略。
resourceSpecCode	String	云服务资源代码。仅作为标记，用户可忽略。
specification	String	独享引擎ECS规格，如"8vCPUs | 16GB"
serverId	String	独享引擎ECS ID
create_time	Long	引擎实例创建时间

状态码： 400

表 4-317 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-318 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-319 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
DELETE https://{endpoint}z/v1/{project_id}/premium-waf/instance/{instance_id}
```

响应示例

状态码： 200

请求成功

```
{
  "id" : "0619871acb764d48a112695e8f7cbb10",
  "region" : "region-01-7",
  "zone" : "region-01-7a",
  "specification" : "8vCPUs | 16GB",
  "arch" : "x86",
  "upgradable" : 0,
  "status" : 0,
  "serverId" : "477353dc-8687-4bf4-b45b-1d7fee74fa63",
  "cloudServiceType" : "hws.service.type.waf",
  "resourceType" : "hws.resource.type.waf.instance",
  "resourceSpecCode" : "waf.instance.enterprise",
  "vpc_id" : "13718074-a3f9-408d-82aa-3c41ef55e589",
  "subnet_id" : "74d1b5a6-c7eb-4e9a-8372-181212552fcc",
  "service_ip" : "192.168.10.68",
  "security_group_ids" : [ "34287bdb-7aba-471a-b041-27427f1af76a" ],
  "cpu_flavor" : "Si2.2xlarge.2",
  "run_status" : 2,
  "access_status" : 1,
  "instancename" : "0412elb"
}
```

状态码

状态码	描述
200	请求成功

状态码	描述
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.2 WAF 防护域名

4.2.2.1 创建独享模式域名

功能介绍

创建独享模式域名

URI

POST /v1/{project_id}/premium-waf/host

表 4-320 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id

表 4-321 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-322 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。

表 4-323 请求 Body 参数

参数	是否必选	参数类型	描述
certificateid	否	String	证书id，通过查询证书列表接口（ListCertificates）接口获取证书id • 对外协议为HTTP时不需要填写 • 对外协议HTTPS时为必填参数
certificatename	否	String	证书名 • 对外协议为HTTP时不需要填写 • 对外协议HTTPS时为必填参数
hostname	是	String	创建的防护域名的名称。例如：www.example.com或者*.example.com
proxy	是	Boolean	是否使用代理。 • true：表示使用了代理； • false：表示没有使用代理
policyid	否	String	防护域名初始绑定的策略ID，可以通过策略名称调用查询防护策略列表（ListPolicy）接口查询到对应的策略id
server	是	Array of **PremiumWafServer** objects	源站信息列表

参数	是否必选	参数类型	描述
access_progress	否	Array of Access_progress objects	冗余参数，仅用于前端使用

表 4-324 PremiumWafServer

参数	是否必选	参数类型	描述
front_protocol	是	String	客户端请求访问源站服务器的协议 枚举值： • **HTTP** • **HTTPS**
back_protocol	是	String	WAF转发客户端请求到源站服务器的协议 枚举值： • **HTTP** • **HTTPS**
address	是	String	客户端访问的源站服务器的公网IP地址或者域名
port	是	Integer	客户端访问的网站服务器的端口号，取值为(0, 65535)，例如：8080
type	是	String	源站地址为ipv4或ipv6 枚举值： • **ipv4** • **ipv6**
vpc_id	是	String	虚拟私有云id，通过以下步骤获取VPC id： • 1.找到独享引擎所在的虚拟私有云名称，VPC\子网这一列就是VPC的名称：登录WAF的控制台->单击系统管理->独享引擎->VPC\子网 • 2.登录虚拟私有云 VPC控制台->虚拟私有云->单击虚拟私有云的名称->基本信息的ID

表 4-325 Access_progress

参数	是否必选	参数类型	描述
step	否	Integer	步骤
status	否	Integer	状态

响应参数

状态码： 200

表 4-326 响应 Body 参数

参数	参数类型	描述
id	String	创建的防护域名id
policyid	String	防护策略id
hostname	String	创建的防护域名
domainid	String	租户id
projectid	String	用户操作的项目id
protocol	String	http协议
protect_status	Integer	域名防护状态： ● -1：bypass，该域名的请求直接到达其后端服务器，不再经过WAF ● 0：暂停防护，WAF只转发该域名的请求，不做攻击检测 ● 1：开启防护，WAF根据您配置的策略进行攻击检测
access_status	Integer	接入状态。 ● “0”：表示未接入 ● “1”：表示已接入
web_tag	String	网站名称
proxy	Boolean	是否使用代理。 ● true：表示使用了代理 ● false：表示没有使用代理
server	Array of **PremiumWafServer** objects	源站信息列表
flag	**Flag** object	特殊标识，用于前端使用

参数	参数类型	描述
block_page	**BlockPage** object	告警页面
extend	Map<String,String>	可扩展属性

表 4-327 PremiumWafServer

参数	参数类型	描述
front_protocol	String	客户端请求访问源站服务器的协议 枚举值： • **HTTP** • **HTTPS**
back_protocol	String	WAF转发客户端请求到源站服务器的协议 枚举值： • **HTTP** • **HTTPS**
address	String	客户端访问的源站服务器的公网IP地址或者域名
port	Integer	客户端访问的网站服务器的端口号，取值为(0,65535)，例如：8080
type	String	源站地址为ipv4或ipv6 枚举值： • **ipv4** • **ipv6**
vpc_id	String	虚拟私有云id，通过以下步骤获取VPC id： • 1.找到独享引擎所在的虚拟私有云名称，VPC\子网这一列就是VPC的名称：登录WAF的控制台->单击系统管理->独享引擎->VPC\子网 • 2.登录虚拟私有云 VPC控制台->虚拟私有云->单击虚拟私有云的名称->基本信息的ID

表 4-328 Flag

参数	参数类型	描述
pci_3ds	String	是否通过pci_3ds标准认证。 ● true：通过pci_3ds标准认证 ● false：未通过pci_3ds标准认证 枚举值： ● **true** ● **false**
pci_dss	String	是否通过pci_dss标准认证。 ● true：通过pci_dss标准认证 ● false：未通过pci_dss标准认证 枚举值： ● **true** ● **false**
cname	String	域名使用老的cname还是新的cname ● old：代表域名使用老的cname ● new：代表域名使用新的cname 枚举值： ● **old** ● **new**
is_dual_az	String	WAF是否支持多可用区容灾 ● true：WAF支持多可用区容灾 ● false：WAF不支持多可用区容灾 枚举值： ● **true** ● **false**

表 4-329 BlockPage

参数	参数类型	描述
template	String	模板名称
custom_page	**CustomPage** object	自定义告警页面
redirect_url	String	重定向URL

表 4-330 CustomPage

参数	参数类型	描述
status_code	String	返回状态码
content_type	String	页面内容类型
content	String	页面内容

状态码： 400

表 4-331 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-332 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-333 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
POST https://{Endpoint}/v1/{project_id}/premium-waf/host?enterprise_project_id=0

{
  "hostname" : "www.demo.com",
  "server" : [ {
    "front_protocol" : "HTTP",
    "back_protocol" : "HTTP",
    "vpc_id" : "cf6dbace-b36a-4d51-ae04-52a3319ae247",
```

```
    "type" : "ipv4",
    "address" : "x.x.x.x",
    "port" : 80
  } ],
  "proxy" : false,
  "description" : ""
}
```

响应示例

状态码： 200

ok

```
{
  "id" : "51a5649e52d341a9bb802044950969dc",
  "hostname" : "www.demo.com",
  "protocol" : "HTTP",
  "server" : [ {
    "address" : "x.x.x.x",
    "port" : 80,
    "type" : "ipv4",
    "weight" : 1,
    "front_protocol" : "HTTP",
    "back_protocol" : "HTTP",
    "vpc_id" : "cf6dbace-b36a-4d51-ae04-52a3319ae247"
  } ],
  "proxy" : false,
  "locked" : 0,
  "timestamp" : 1650596007113,
  "flag" : {
    "pci_3ds" : "false",
    "pci_dss" : "false"
  },
  "description" : "",
  "policyid" : "1607df035bc847b582ce9c838c083b88",
  "projectid" : "550500b49078408682d0d4f7d923f3e1",
  "domainid" : "d4ecb00b031941ce9171b7bc3386883f",
  "enterprise_project_id" : "0",
  "protect_status" : 1,
  "access_status" : 0,
  "web_tag" : "",
  "access_progress" : [ ]
}
```

状态码

状态码	描述
200	ok
400	非法请求
401	Token无权限
500	服务器内部错误

错误码

请参见**错误码**。

4.2.2.2 查询独享模式域名列表

功能介绍

查询独享模式域名列表

URI

GET /v1/{project_id}/premium-waf/host

表 4-334 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id

表 4-335 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id
page	否	String	分页查询时，返回第几页数据。范围0-100000，默认值为1，表示返回第1页数据。 缺省值：**1**
pagesize	否	String	分页查询时，每页包含多少条结果。范围1-100，默认值为10，表示每页包含10条结果。 缺省值：**10**
hostname	否	String	防护域名
policyname	否	String	策略名称
protect_status	否	Integer	域名防护状态： ● -1：bypass，该域名的请求直接到达其后端服务器，不再经过WAF ● 0：暂停防护，WAF只转发该域名的请求，不做攻击检测 ● 1：开启防护，WAF根据您配置的策略进行攻击检测

请求参数

表 4-336 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。

响应参数

状态码： 200

表 4-337 响应 Body 参数

参数	参数类型	描述
total	Integer	全部防护域名的数量
items	Array of **SimplePremiumWafHost** objects	详细的防护域名信息

表 4-338 SimplePremiumWafHost

参数	参数类型	描述
id	String	域名id
hostname	String	域名
policyid	String	策略id
protect_status	Integer	域名防护状态： ● -1：bypass，该域名的请求直接到达其后端服务器，不再经过WAF ● 0：暂停防护，WAF只转发该域名的请求，不做攻击检测 ● 1：开启防护，WAF根据您配置的策略进行攻击检测

参数	参数类型	描述
access_status	Integer	接入状态。 • “0”：表示未接入 • “1”：表示已接入
flag	Map<String,String>	特殊标识，用于前端使用
mode	String	特殊模式独享引擎的标识（如elb）
block_page	**BlockPage** object	告警页面
traffic_mark	**TrafficMark** object	流量标识
extend	Map<String,String>	可扩展字段
circuit_breaker	**CircuitBreaker** object	熔断配置
timeout_config	**TimeoutConfig** object	超时配置
access_progress	Array of **Access_progress** objects	冗余参数，仅用于前端使用

表 4-339 BlockPage

参数	参数类型	描述
template	String	模板名称
custom_page	**CustomPage** object	自定义告警页面
redirect_url	String	重定向URL

表 4-340 CustomPage

参数	参数类型	描述
status_code	String	返回状态码
content_type	String	页面内容类型
content	String	页面内容

表 4-341 TrafficMark

参数	参数类型	描述
sip	Array of strings	惩罚ip
cookie	String	cookie
params	String	参数

表 4-342 CircuitBreaker

参数	参数类型	描述
switch	Boolean	熔断开关
dead_num	Integer	源站不可达数量阈值
dead_ratio	Number	源站不可达比例阈值
block_time	Integer	源站不可达熔断时间
superposition_num	Integer	熔断阈值叠加次数
suspend_num	Integer	连接数占用阈值
sus_block_time	Integer	连接数占用熔断时间

表 4-343 TimeoutConfig

参数	参数类型	描述
connect_timeout	Integer	WAF连接源站超时配置
send_timeout	Integer	WAF发送请求到源站超时配置
read_timeout	Integer	WAF接收源站响应超时配置

表 4-344 Access_progress

参数	参数类型	描述
step	Integer	步骤
status	Integer	状态

状态码： 400

表 4-345 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-346 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-347 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/premium-waf/host?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "total" : 1,
  "items" : [ {
    "id" : "ee896796e1a84f3f85865ae0853d8974",
    "hostname" : "www.demo.com",
    "extend" : { },
    "region" : "xx-xx-1",
    "flag" : {
      "pci_3ds" : "false",
      "pci_dss" : "false"
    },
    "description" : "",
    "policyid" : "df15d0eb84194950a8fdc615b6c012dc",
    "protect_status" : 1,
    "access_status" : 0,
    "hostid" : "ee896796e1a84f3f85865ae0853d8974"
```

```
 }]
}
```

状态码

状态码	描述
200	ok
400	非法请求
401	Token无权限
500	服务器内部错误

错误码

请参见**错误码**。

4.2.2.3 查看独享模式域名配置

功能介绍

查看独享模式域名配置

URI

GET /v1/{project_id}/premium-waf/host/{host_id}

表 4-348 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	租户操作的项目id
host_id	是	String	独享模式域名id

表 4-349 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-350 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。

响应参数

状态码： 200

表 4-351 响应 Body 参数

参数	参数类型	描述
id	String	域名id
policyid	String	防护域名初始绑定的策略ID，可以通过策略名称调用查询防护策略列表（ListPolicy）接口查询到对应的策略id
hostname	String	创建的独享模式防护域名
domainid	String	用户Domain ID
project_id	String	用户的project_id
access_code	String	cname前缀
protocol	String	http协议类型
server	Array of **PremiumWafServer** objects	源站信息
certificateid	String	证书id，通过查询证书列表接口（ListCertificates）接口获取证书id • 对外协议为HTTP时不需要填写 • 对外协议HTTPS时为必填参数
certificatename	String	证书名 • 对外协议为HTTP时不需要填写 • 对外协议HTTPS时为必填参数

参数	参数类型	描述
proxy	Boolean	是否开启了代理。 ● true：表示使用了代理； ● false：表示没有使用代理
locked	Integer	锁定状态 缺省值：**0**
protect_status	Integer	域名防护状态： ● -1：bypass，该域名的请求直接到达其后端服务器，不再经过WAF ● 0：暂停防护，WAF只转发该域名的请求，不做攻击检测 ● 1：开启防护，WAF根据您配置的策略进行攻击检测
access_status	Integer	接入状态。 ● “0”：表示未接入 ● “1”：表示已接入
web_tag	String	网站名称
timestamp	Long	创建防护域名的时间
flag	**Flag** object	特殊标识，用于前端使用
block_page	**BlockPage** object	告警页面
extend	Map<String,String>	可扩展属性
traffic_mark	**TrafficMark** object	流量标识
timeout_config	**TimeoutConfig** object	超时配置
access_progress	Array of **Access_progress** objects	冗余参数，仅用于前端使用

表 4-352 PremiumWafServer

参数	参数类型	描述
front_protocol	String	客户端请求访问源站服务器的协议 枚举值： ● **HTTP** ● **HTTPS**
back_protocol	String	WAF转发客户端请求到源站服务器的协议 枚举值： ● **HTTP** ● **HTTPS**
address	String	客户端访问的源站服务器的公网IP地址或者域名
port	Integer	客户端访问的网站服务器的端口号，取值为(0, 65535)，例如：8080
type	String	源站地址为ipv4或ipv6 枚举值： ● **ipv4** ● **ipv6**
vpc_id	String	虚拟私有云id，通过以下步骤获取VPC id： ● 1.找到独享引擎所在的虚拟私有云名称，VPC\子网这一列就是VPC的名称：登录WAF的控制台->单击系统管理->独享引擎->VPC\子网 ● 2.登录虚拟私有云 VPC控制台->虚拟私有云->单击虚拟私有云的名称->基本信息的ID

表 4-353 Flag

参数	参数类型	描述
pci_3ds	String	是否通过pci_3ds标准认证。 ● true：通过pci_3ds标准认证 ● false：未通过pci_3ds标准认证 枚举值： ● **true** ● **false**

参数	参数类型	描述
pci_dss	String	是否通过pci_dss标准认证。 ● true：通过pci_dss标准认证 ● false：未通过pci_dss标准认证 枚举值： ● **true** ● **false**
cname	String	域名使用老的cname还是新的cname ● old：代表域名使用老的cname ● new：代表域名使用新的cname 枚举值： ● **old** ● **new**
is_dual_az	String	WAF是否支持多可用区容灾 ● true：WAF支持多可用区容灾 ● false：WAF不支持多可用区容灾 枚举值： ● **true** ● **false**

表 4-354 BlockPage

参数	参数类型	描述
template	String	模板名称
custom_page	**CustomPage** object	自定义告警页面
redirect_url	String	重定向URL

表 4-355 CustomPage

参数	参数类型	描述
status_code	String	返回状态码
content_type	String	页面内容类型
content	String	页面内容

表 4-356 TrafficMark

参数	参数类型	描述
sip	Array of strings	惩罚ip
cookie	String	cookie
params	String	参数

表 4-357 TimeoutConfig

参数	参数类型	描述
connect_timeout	Integer	WAF连接源站超时配置
send_timeout	Integer	WAF发送请求到源站超时配置
read_timeout	Integer	WAF接收源站响应超时配置

表 4-358 Access_progress

参数	参数类型	描述
step	Integer	步骤
status	Integer	状态

状态码： 400

表 4-359 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-360 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码

参数	参数类型	描述
error_msg	String	错误信息

状态码： 500

表 4-361 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/premium-waf/host/{host_id}?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "id" : "ee896796e1a84f3f85865ae0853d8974",
  "hostname" : "www.demo.com",
  "protocol" : "HTTPS",
  "server" : [ {
    "address" : "1.2.3.4",
    "port" : 443,
    "type" : "ipv4",
    "weight" : 1,
    "front_protocol" : "HTTPS",
    "back_protocol" : "HTTPS",
    "vpc_id" : "ebfc553a-386d-4746-b0c2-18ff3f0e903d"
  } ],
  "proxy" : false,
  "locked" : 0,
  "timestamp" : 1650593801380,
  "flag" : {
    "pci_3ds" : "false",
    "pci_dss" : "false"
  },
  "description" : "",
  "policyid" : "df15d0eb84194950a8fdc615b6c012dc",
  "domainid" : "0ee78615ca08419f81f539d97c9ee353",
  "projectid" : "550500b49078408682d0d4f7d923f3e1",
  "protect_status" : 1,
  "access_status" : 0,
  "certificateid" : "360f992501a64de0a65c50a64d1ca7b3",
  "certificatename" : "certificatename75315",
  "web_tag" : "",
  "timeout_config" : {
    "connect_timeout" : 30,
    "read_timeout" : 180,
    "send_timout" : 180
  }
}
```

状态码

状态码	描述
200	ok
400	非法请求
401	Token无权限
500	服务器内部错误

错误码

请参见**错误码**。

4.2.2.4 修改独享模式域名配置

功能介绍

修改独享模式域名配置

URI

PUT /v1/{project_id}/premium-waf/host/{host_id}

表 4-362 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
host_id	是	String	独享模式域名id

表 4-363 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-364 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。

表 4-365 请求 Body 参数

参数	是否必选	参数类型	描述
proxy	否	Boolean	是否开启了代理。 • true：表示使用了代理； • false：表示没有使用代理
certificateid	否	String	https证书id，通过查询证书列表接口（ListCertificates）接口获取证书id
certificatename	否	String	https证书名称，通过查询证书列表接口（ListCertificates）接口获取证书id
locked	否	Integer	是否锁定
protect_status	否	Integer	域名防护状态： • -1：bypass，该域名的请求直接到达其后端服务器，不再经过WAF • 0：暂停防护，WAF只转发该域名的请求，不做攻击检测 • 1：开启防护，WAF根据您配置的策略进行攻击检测
access_status	否	Integer	接入状态。 • “0”：表示未接入 • “1”：表示已接入
timestamp	否	Integer	时间戳
block_page	否	**BlockPage** object	告警页面

参数	是否必选	参数类型	描述
traffic_mark	否	TrafficMark object	流量标识
flag	否	Map<String,String>	特殊标识，用于前端使用
extend	否	Map<String,String>	可扩展字段
circuit_breaker	否	CircuitBreaker object	熔断配置
timeout_config	否	TimeoutConfig object	超时配置

表 4-366 BlockPage

参数	是否必选	参数类型	描述
template	是	String	模板名称
custom_page	否	CustomPage object	自定义告警页面
redirect_url	否	String	重定向URL

表 4-367 CustomPage

参数	是否必选	参数类型	描述
status_code	是	String	返回状态码
content_type	是	String	页面内容类型
content	是	String	页面内容

表 4-368 TrafficMark

参数	是否必选	参数类型	描述
sip	否	Array of strings	惩罚ip
cookie	否	String	cookie
params	否	String	参数

表 4-369 CircuitBreaker

参数	是否必选	参数类型	描述
switch	否	Boolean	熔断开关
dead_num	否	Integer	源站不可达数量阈值
dead_ratio	否	Number	源站不可达比例阈值
block_time	否	Integer	源站不可达熔断时间
superposition_num	否	Integer	熔断阈值叠加次数
suspend_num	否	Integer	连接数占用阈值
sus_block_time	否	Integer	连接数占用熔断时间

表 4-370 TimeoutConfig

参数	是否必选	参数类型	描述
connect_timeout	否	Integer	WAF连接源站超时配置
send_timeout	否	Integer	WAF发送请求到源站超时配置
read_timeout	否	Integer	WAF接收源站响应超时配置

响应参数

状态码： 200

表 4-371 响应 Body 参数

参数	参数类型	描述
id	String	域名id
policyid	String	防护域名初始绑定的策略ID，可以通过策略名称调用查询防护策略列表（ListPolicy）接口查询到对应的策略id
hostname	String	创建的独享模式防护域名
domainid	String	用户Domain ID
project_id	String	用户的project_id
access_code	String	cname前缀
protocol	String	http协议类型

参数	参数类型	描述
server	Array of **PremiumWafServer** objects	源站信息
certificateid	String	证书id，通过查询证书列表接口（ListCertificates）接口获取证书id ● 对外协议为HTTP时不需要填写 ● 对外协议HTTPS时为必填参数
certificatename	String	证书名 ● 对外协议为HTTP时不需要填写 ● 对外协议HTTPS时为必填参数
proxy	Boolean	是否开启了代理。 ● true：表示使用了代理； ● false：表示没有使用代理
locked	Integer	锁定状态 缺省值：**0**
protect_status	Integer	域名防护状态： ● -1：bypass，该域名的请求直接到达其后端服务器，不再经过WAF ● 0：暂停防护，WAF只转发该域名的请求，不做攻击检测 ● 1：开启防护，WAF根据您配置的策略进行攻击检测
access_status	Integer	接入状态。 ● “0”：表示未接入 ● “1”：表示已接入
web_tag	String	网站名称
timestamp	Long	创建防护域名的时间
flag	**Flag** object	特殊标识，用于前端使用
block_page	**BlockPage** object	告警页面
extend	Map<String,String>	可扩展属性
traffic_mark	**TrafficMark** object	流量标识
timeout_config	**TimeoutConfig** object	超时配置

参数	参数类型	描述
access_progress	Array of **Access_progress** objects	冗余参数，仅用于前端使用

表 4-372 PremiumWafServer

参数	参数类型	描述
front_protocol	String	客户端请求访问源站服务器的协议 枚举值： • **HTTP** • **HTTPS**
back_protocol	String	WAF转发客户端请求到源站服务器的协议 枚举值： • **HTTP** • **HTTPS**
address	String	客户端访问的源站服务器的公网IP地址或者域名
port	Integer	客户端访问的网站服务器的端口号，取值为(0,65535)，例如：8080
type	String	源站地址为ipv4或ipv6 枚举值： • **ipv4** • **ipv6**
vpc_id	String	虚拟私有云id，通过以下步骤获取VPC id： • 1.找到独享引擎所在的虚拟私有云名称，VPC\子网这一列就是VPC的名称：登录WAF的控制台->单击系统管理->独享引擎->VPC\子网 • 2.登录虚拟私有云 VPC控制台->虚拟私有云->单击虚拟私有云的名称->基本信息的ID

表 4-373 Flag

参数	参数类型	描述
pci_3ds	String	是否通过pci_3ds标准认证。 ● true：通过pci_3ds标准认证 ● false：未通过pci_3ds标准认证 枚举值： ● **true** ● **false**
pci_dss	String	是否通过pci_dss标准认证。 ● true：通过pci_dss标准认证 ● false：未通过pci_dss标准认证 枚举值： ● **true** ● **false**
cname	String	域名使用老的cname还是新的cname ● old：代表域名使用老的cname ● new：代表域名使用新的cname 枚举值： ● **old** ● **new**
is_dual_az	String	WAF是否支持多可用区容灾 ● true：WAF支持多可用区容灾 ● false：WAF不支持多可用区容灾 枚举值： ● **true** ● **false**

表 4-374 BlockPage

参数	参数类型	描述
template	String	模板名称
custom_page	**CustomPage** object	自定义告警页面
redirect_url	String	重定向URL

表 4-375 CustomPage

参数	参数类型	描述
status_code	String	返回状态码
content_type	String	页面内容类型
content	String	页面内容

表 4-376 TrafficMark

参数	参数类型	描述
sip	Array of strings	惩罚ip
cookie	String	cookie
params	String	参数

表 4-377 TimeoutConfig

参数	参数类型	描述
connect_timeout	Integer	WAF连接源站超时配置
send_timeout	Integer	WAF发送请求到源站超时配置
read_timeout	Integer	WAF接收源站响应超时配置

表 4-378 Access_progress

参数	参数类型	描述
step	Integer	步骤
status	Integer	状态

状态码： 400

表 4-379 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-380 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-381 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
PUT https://{Endpoint}/v1/{project_id}/premium-waf/host/{host_id}?enterprise_project_id=0

{
  "proxy" : false
}
```

响应示例

状态码： 200

ok

```
{
  "id" : "27995fb98a2d4928a1e453e65ee8117a",
  "hostname" : "www.demo.com",
  "protocol" : "HTTP",
  "server" : [ {
    "address" : "192.168.0.209",
    "port" : 80,
    "type" : "ipv4",
    "weight" : 1,
    "front_protocol" : "HTTP",
    "back_protocol" : "HTTP",
    "vpc_id" : "cf6dbace-b36a-4d51-ae04-52a8459ae247"
  } ],
  "proxy" : false,
  "locked" : 0,
  "timestamp" : 1650590814885,
  "flag" : {
    "pci_3ds" : "false",
    "pci_dss" : "false"
  },
  "description" : "",
  "policyid" : "9555cda636ef4ca294dfe4b14bc94c47",
  "domainid" : "d4ecb00b031941ce9171b7bc3386883f",
  "projectid" : "05e33ecd328025dd2f7fc00696201fb4",
```

```
  "enterprise_project_id" : "0",
  "protect_status" : 1,
  "access_status" : 0,
  "web_tag" : ""
}
```

状态码

状态码	描述
200	ok
400	非法请求
401	Token无权限
500	服务器内部错误

错误码

请参见**错误码**。

4.2.2.5 删除独享模式域名

功能介绍

删除独享模式域名

URI

DELETE /v1/{project_id}/premium-waf/host/{host_id}

表 4-382 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
host_id	是	String	独享模式域名ID

表 4-383 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id
keepPolicy	否	Boolean	是否保留规则 缺省值：**false**

请求参数

表 4-384 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。

响应参数

状态码： 200

表 4-385 响应 Body 参数

参数	参数类型	描述
id	String	域名id
hostname	String	域名
policyid	String	策略id
region	String	区域id
protect_status	Integer	域名防护状态： ● -1：bypass，该域名的请求直接到达其后端服务器，不再经过WAF ● 0：暂停防护，WAF只转发该域名的请求，不做攻击检测 ● 1：开启防护，WAF根据您配置的策略进行攻击检测
access_status	Integer	接入状态。 ● “0”：表示未接入 ● “1”：表示已接入
flag	Map<String,String>	特殊标识，用于前端使用

状态码： 400

表 4-386 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-387 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-388 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
DELETE https://{Endpoint}/v1/{project_id}/premium-waf/host/{host_id}?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "id" : "ee896796e1a84f3f85865ae0853d8974",
  "hostname" : "www.demo.com",
  "region" : "xx-xx-1",
  "flag" : {
    "pci_3ds" : "false",
    "pci_dss" : "false"
  },
  "description" : "",
  "policyid" : "df15d0eb84194950a8fdc615b6c012dc",
  "protect_status" : 1,
  "access_status" : 0,
  "web_tag" : "",
  "hostid" : "ee896796e1a84f3f85865ae0853d8974"
}
```

状态码

状态码	描述
200	ok
400	非法请求
401	Token无权限
500	服务器内部错误

错误码

请参见**错误码**。

4.2.3 防护状态与域名接入

4.2.3.1 修改独享模式域名防护状态

功能介绍

修改独享模式域名防护状态

URI

PUT /v1/{project_id}/premium-waf/host/{host_id}/protect-status

表 4-389 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
host_id	是	String	独享模式域名ID

表 4-390 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-391 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。

表 4-392 请求 Body 参数

参数	是否必选	参数类型	描述
protect_status	是	Integer	域名防护状态： ● -1：bypass，该域名的请求直接到达其后端服务器，不再经过WAF ● 0：暂停防护，WAF只转发该域名的请求，不做攻击检测 ● 1：开启防护，WAF根据您配置的策略进行攻击检测

响应参数

状态码： 200

表 4-393 响应 Body 参数

参数	参数类型	描述
protect_status	Integer	域名防护状态： ● -1：bypass，该域名的请求直接到达其后端服务器，不再经过WAF ● 0：暂停防护，WAF只转发该域名的请求，不做攻击检测 ● 1：开启防护，WAF根据您配置的策略进行攻击检测

状态码： 400

表 4-394 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-395 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-396 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
PUT https://{Endpoint}/v1/{project_id}/premium-waf/host/{host_id}/protect-status?enterprise_project_id=0

{
  "protect_status" : 1
}
```

响应示例

状态码： 200

ok

```
{
  "protect_status" : 1
}
```

状态码

状态码	描述
200	ok

状态码	描述
400	非法请求
401	Token无权限
500	服务器内部错误

错误码

请参见**错误码**。

4.2.3.2 修改独享模式域名接入状态

功能介绍

修改独享模式域名接入状态

URI

PUT /v1/{project_id}/premium-waf/host/{host_id}/access_status

表 4-397 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
host_id	是	String	独享模式域名ID

请求参数

表 4-398 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。

表 4-399 请求 Body 参数

参数	是否必选	参数类型	描述
access_status	否	Integer	接入状态。 ● “0”：表示未接入 ● “1”：表示已接入
protect_status	否	Integer	域名防护状态： ● -1：bypass，该域名的请求直接到达其后端服务器，不再经过WAF ● 0：暂停防护，WAF只转发该域名的请求，不做攻击检测 ● 1：开启防护，WAF根据您配置的策略进行攻击检测

响应参数

状态码： 200

表 4-400 响应 Body 参数

参数	参数类型	描述
access_status	Integer	接入状态。 ● “0”：表示未接入 ● “1”：表示已接入

状态码： 400

表 4-401 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-402 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码

参数	参数类型	描述
error_msg	String	错误信息

状态码： 500

表 4-403 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
PUT https://{Endpoint}/v1/{project_id}/premium-waf/host/{host_id}/access_status

{
  "access_status" : 1
}
```

响应示例

状态码： 200

ok

```
{
  "access_status" : 1,
  "protect_status" : 1
}
```

状态码

状态码	描述
200	ok
400	非法请求
401	Token无权限
500	服务器内部错误

错误码

请参见**错误码**。

4.2.4 防护策略管理

4.2.4.1 查询防护策略列表

功能介绍

查询防护策略列表

URI

GET /v1/{project_id}/waf/policy

表 4-404 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id

表 4-405 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS)的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id
page	否	Integer	分页查询时，返回第几页数据。范围0-100000，默认值为1，表示返回第1页数据。 缺省值：**1**
pagesize	否	Integer	分页查询时，每页包含多少条结果。范围1-100，默认值为10，表示每页包含10条结果。 缺省值：**10**
name	否	String	防护策略名称

请求参数

表 4-406 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。

参数	是否必选	参数类型	描述
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-407 响应 Body 参数

参数	参数类型	描述
total	Integer	防护策略总数
items	Array of **PolicyResponse** objects	防护策略对象列表

表 4-408 PolicyResponse

参数	参数类型	描述
id	String	防护策略id
name	String	防护策略名
action	**PolicyAction** object	操作
options	**PolicyOption** object	选项
level	Integer	防护等级： • 1: 表示低，不检测header中的XSS攻击和CMDI攻击，当发现防护规则拦截了您的正常业务时，可调整防护等级为“1”，“1”防护下对业务的误报率降低，但漏报率可能会增高，例如：wget、curl等检测。 • 2：表示中，默认情况下，选择“2”，根据文件的敏感程度区分，中危检测有远程文件包含、第三方软件漏洞、Webshell、cp、ftp。 • 3：表示高，当您需要更严格的防护等级时，建议选择“3”，而“3”防护下对业务的误报率可能会增高，但漏报率降低，例如nc、nmap、kill等。

参数	参数类型	描述
full_detection	Boolean	精准防护中的检测模式： • true：全检测。当用户的请求符合精准防护中的拦截条件时，不会立即拦截，WAF会继续执行其他防护的检测，待其他防护的检测完成后进行拦截。 • false：短路检测。当用户的请求符合精准防护中的拦截条件时，便立刻终止检测，进行拦截。
bind_host	Array of **BindHost** objects	防护域名的信息
timestamp	Long	创建防护策略的时间
extend	Map<String,String>	扩展字段

表 4-409 PolicyAction

参数	参数类型	描述
category	String	防护等级： • log：仅记录 • block：拦截 枚举值： • **block** • **log**

表 4-410 PolicyOption

参数	参数类型	描述
webattack	Boolean	基础防护是否开启 枚举值： • **true** • **false**
common	Boolean	常规检测是否开启 枚举值： • **true** • **false**

参数	参数类型	描述
crawler	Boolean	反爬虫是否开启 枚举值： • **true** • **false**
crawler_engine	Boolean	搜索engine是否开启 枚举值： • **true** • **false**
crawler_scanner	Boolean	反爬虫检测是否开启 枚举值： • **true** • **false**
crawler_script	Boolean	脚本反爬虫是否开启 枚举值： • **true** • **false**
crawler_other	Boolean	其他爬虫是否开启 枚举值： • **true** • **false**
webshell	Boolean	Webshell检测是否开启 枚举值： • **true** • **false**
cc	Boolean	cc规则是否开启 枚举值： • **true** • **false**
custom	Boolean	精准防护是否开启 枚举值： • **true** • **false**

参数	参数类型	描述
whiteblackip	Boolean	黑白名单防护是否开启 枚举值： • **true** • **false**
geoip	Boolean	地理位置访问控制规则是否开启 枚举值： • **true** • **false**
ignore	Boolean	误报屏蔽是否开启 枚举值： • **true** • **false**
privacy	Boolean	隐私屏蔽是否开启 枚举值： • **true** • **false**
antitamper	Boolean	网页防篡改规则是否开启 枚举值： • **true** • **false**
antileakage	Boolean	防敏感信息泄露规则是否开启 枚举值： • **true** • **false**
bot_enable	Boolean	防网络机器人攻击是否开启 枚举值： • **true** • **false**

表 4-411 BindHost

参数	参数类型	描述
id	String	防护域名ID
hostname	String	防护域名

参数	参数类型	描述
waf_type	String	防护域名对应模式：cloud（云模式）/premium（独享模式）
mode	String	仅独享模式涉及特殊域名模式

状态码： 400

表 4-412 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-413 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-414 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/policy?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "total" : 1,
```

```
 "items" : [ {
   "id" : "41cba8aee2e94bcdbf57460874205494",
   "name" : "policy_2FHwFOKz",
   "level" : 2,
   "action" : {
     "category" : "log",
     "modulex_category" : "log"
   },
   "options" : {
     "webattack" : true,
     "common" : true,
     "crawler" : true,
     "crawler_engine" : false,
     "crawler_scanner" : true,
     "crawler_script" : false,
     "crawler_other" : false,
     "webshell" : false,
     "cc" : true,
     "custom" : true,
     "precise" : false,
     "whiteblackip" : true,
     "geoip" : true,
     "ignore" : true,
     "privacy" : true,
     "antitamper" : true,
     "anticrawler" : false,
     "antileakage" : false,
     "followed_action" : false,
     "bot_enable" : true
   },
   "hosts" : [ ],
   "extend" : { },
   "timestamp" : 1650527546218,
   "full_detection" : false,
   "bind_host" : [ ]
 } ]
}
```


状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.4.2 创建防护策略

功能介绍

创建防护策略

URI

POST /v1/{project_id}/waf/policy

表 4-415 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户的project_id

表 4-416 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS)的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-417 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

表 4-418 请求 Body 参数

参数	是否必选	参数类型	描述
name	是	String	防护策略名

响应参数

状态码： 200

表 4-419 响应 Body 参数

参数	参数类型	描述
id	String	防护策略id
name	String	防护策略名
action	**PolicyAction** object	操作
options	**PolicyOption** object	选项
level	Integer	防护等级： • 1: 表示低，不检测header中的XSS攻击和CMDI攻击，当发现防护规则拦截了您的正常业务时，可调整防护等级为“1”，“1”防护下对业务的误报率降低，但漏报率可能会增高，例如：wget、curl等检测。 • 2：表示中，默认情况下，选择“2”，根据文件的敏感程度区分，中危检测有远程文件包含、第三方软件漏洞、Webshell、cp、ftp。 • 3：表示高，当您需要更严格的防护等级时，建议选择“3”，而“3”防护下对业务的误报率可能会增高，但漏报率降低，例如nc、nmap、kill等。
full_detection	Boolean	精准防护中的检测模式： • true：全检测。当用户的请求符合精准防护中的拦截条件时，不会立即拦截，WAF会继续执行其他防护的检测，待其他防护的检测完成后进行拦截。 • false：短路检测。当用户的请求符合精准防护中的拦截条件时，便立刻终止检测，进行拦截。
bind_host	Array of **BindHost** objects	防护域名的信息
timestamp	Integer	创建防护策略的时间
extend	Map<String,String>	扩展字段

表 4-420 PolicyAction

参数	参数类型	描述
category	String	防护等级： ● log：仅记录 ● block：拦截 枚举值： ● **block** ● **log**

表 4-421 PolicyOption

参数	参数类型	描述
webattack	Boolean	基础防护是否开启 枚举值： ● **true** ● **false**
common	Boolean	常规检测是否开启 枚举值： ● **true** ● **false**
crawler	Boolean	反爬虫是否开启 枚举值： ● **true** ● **false**
crawler_engine	Boolean	搜索engine是否开启 枚举值： ● **true** ● **false**
crawler_scanner	Boolean	反爬虫检测是否开启 枚举值： ● **true** ● **false**
crawler_script	Boolean	脚本反爬虫是否开启 枚举值： ● **true** ● **false**

参数	参数类型	描述
crawler_other	Boolean	其他爬虫是否开启 枚举值： • **true** • **false**
webshell	Boolean	Webshell检测是否开启 枚举值： • **true** • **false**
cc	Boolean	cc规则是否开启 枚举值： • **true** • **false**
custom	Boolean	精准防护是否开启 枚举值： • **true** • **false**
whiteblackip	Boolean	黑白名单防护是否开启 枚举值： • **true** • **false**
geoip	Boolean	地理位置访问控制规则是否开启 枚举值： • **true** • **false**
ignore	Boolean	误报屏蔽是否开启 枚举值： • **true** • **false**
privacy	Boolean	隐私屏蔽是否开启 枚举值： • **true** • **false**

参数	参数类型	描述
antitamper	Boolean	网页防篡改规则是否开启 枚举值： • **true** • **false**
antileakage	Boolean	防敏感信息泄露规则是否开启 枚举值： • **true** • **false**
bot_enable	Boolean	防网络机器人攻击是否开启 枚举值： • **true** • **false**

表 4-422 BindHost

参数	参数类型	描述
id	String	防护域名ID
hostname	String	防护域名
waf_type	String	防护域名对应模式：cloud（云模式）/premium（独享模式）
mode	String	仅独享模式涉及特殊域名模式

状态码： 400

表 4-423 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-424 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 403

表 4-425 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-426 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
POST https://{Endpoint}/v1/{project_id}/waf/policy?enterprise_project_id=0

{
  "name" : "demo"
}
```

响应示例

状态码： 200

ok

```
{
  "id" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "level" : 2,
  "action" : {
    "category" : "log"
  },
  "options" : {
    "webattack" : true,
    "common" : true,
    "crawler" : true,
    "crawler_engine" : false,
```

```
    "crawler_scanner" : true,
    "crawler_script" : false,
    "crawler_other" : false,
    "webshell" : false,
    "cc" : true,
    "custom" : true,
    "precise" : false,
    "whiteblackip" : true,
    "geoip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "anticrawler" : false,
    "antileakage" : false,
    "followed_action" : false,
    "bot_enable" : true
  },
  "hosts" : [ ],
  "extend" : { },
  "timestamp" : 1650529538732,
  "full_detection" : false,
  "bind_host" : [ ]
}
```


状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
403	资源配额不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.4.3 根据 Id 查询防护策略

功能介绍

根据Id查询防护策略

URI

GET /v1/{project_id}/waf/policy/{policy_id}

表 4-427 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id

参数	是否必选	参数类型	描述
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id

表 4-428 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS)的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-429 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-430 响应 Body 参数

参数	参数类型	描述
id	String	防护策略id
name	String	防护策略名
action	**PolicyAction** object	操作
options	**PolicyOption** object	选项

参数	参数类型	描述
level	Integer	防护等级： ● 1: 表示低，不检测header中的XSS攻击和CMDI攻击，当发现防护规则拦截了您的正常业务时，可调整防护等级为“1”，“1”防护下对业务的误报率降低，但漏报率可能会增高，例如：wget、curl等检测。 ● 2：表示中，默认情况下，选择“2”，根据文件的敏感程度区分，中危检测有远程文件包含、第三方软件漏洞、Webshell、cp、ftp。 ● 3：表示高，当您需要更严格的防护等级时，建议选择“3”，而“3”防护下对业务的误报率可能会增高，但漏报率降低，例如nc、nmap、kill等。
full_detection	Boolean	精准防护中的检测模式： ● true：全检测。当用户的请求符合精准防护中的拦截条件时，不会立即拦截，WAF会继续执行其他防护的检测，待其他防护的检测完成后进行拦截。 ● false：短路检测。当用户的请求符合精准防护中的拦截条件时，便立刻终止检测，进行拦截。
bind_host	Array of **BindHost** objects	防护域名的信息
timestamp	Integer	创建防护策略的时间
extend	Map<String,String>	扩展字段

表 4-431 PolicyAction

参数	参数类型	描述
category	String	防护等级： ● log：仅记录 ● block：拦截 枚举值： ● **block** ● **log**

表 4-432 PolicyOption

参数	参数类型	描述
webattack	Boolean	基础防护是否开启 枚举值： • **true** • **false**
common	Boolean	常规检测是否开启 枚举值： • **true** • **false**
crawler	Boolean	反爬虫是否开启 枚举值： • **true** • **false**
crawler_engine	Boolean	搜索engine是否开启 枚举值： • **true** • **false**
crawler_scanner	Boolean	反爬虫检测是否开启 枚举值： • **true** • **false**
crawler_script	Boolean	脚本反爬虫是否开启 枚举值： • **true** • **false**
crawler_other	Boolean	其他爬虫是否开启 枚举值： • **true** • **false**
webshell	Boolean	Webshell检测是否开启 枚举值： • **true** • **false**

参数	参数类型	描述
cc	Boolean	cc规则是否开启 枚举值： • **true** • **false**
custom	Boolean	精准防护是否开启 枚举值： • **true** • **false**
whiteblackip	Boolean	黑白名单防护是否开启 枚举值： • **true** • **false**
geoip	Boolean	地理位置访问控制规则是否开启 枚举值： • **true** • **false**
ignore	Boolean	误报屏蔽是否开启 枚举值： • **true** • **false**
privacy	Boolean	隐私屏蔽是否开启 枚举值： • **true** • **false**
antitamper	Boolean	网页防篡改规则是否开启 枚举值： • **true** • **false**
antileakage	Boolean	防敏感信息泄露规则是否开启 枚举值： • **true** • **false**

参数	参数类型	描述
bot_enable	Boolean	防网络机器人攻击是否开启 枚举值： • **true** • **false**

表 4-433 BindHost

参数	参数类型	描述
id	String	防护域名ID
hostname	String	防护域名
waf_type	String	防护域名对应模式：cloud（云模式）/premium（独享模式）
mode	String	仅独享模式涉及特殊域名模式

状态码： 400

表 4-434 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-435 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-436 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "id" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "level" : 2,
  "action" : {
    "category" : "log",
    "modulex_category" : "log"
  },
  "options" : {
    "webattack" : true,
    "common" : true,
    "crawler" : true,
    "crawler_engine" : false,
    "crawler_scanner" : true,
    "crawler_script" : false,
    "crawler_other" : false,
    "webshell" : false,
    "cc" : true,
    "custom" : true,
    "precise" : false,
    "whiteblackip" : true,
    "geoip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "anticrawler" : false,
    "antileakage" : false,
    "followed_action" : false,
    "bot_enable" : true
  },
  "hosts" : [ ],
  "extend" : { },
  "timestamp" : 1650529538732,
  "full_detection" : false,
  "bind_host" : [ ],
  "share_info" : {
    "is_receiver" : false,
    "provider_display" : {
      "share_count" : 0,
      "accept_count" : 0,
      "process_status" : 0
    }
  }
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.4.4 更新防护策略

功能介绍

更新防护策略，请求体可只传需要更新的部分

URI

PATCH /v1/{project_id}/waf/policy/{policy_id}

表 4-437 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id

表 4-438 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-439 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

表 4-440 请求 Body 参数

参数	是否必选	参数类型	描述
name	否	String	防护策略名
action	否	**PolicyAction** object	操作
options	否	**PolicyOption** object	选项
level	否	Integer	防护等级： • 1: 表示低，不检测header中的XSS攻击和CMDI攻击，当发现防护规则拦截了您的正常业务时，可调整防护等级为“1”，“1”防护下对业务的误报率降低，但漏报率可能会增高，例如：wget、curl等检测。 • 2：表示中，默认情况下，选择“2”，根据文件的敏感程度区分，中危检测有远程文件包含、第三方软件漏洞、Webshell、cp、ftp。 • 3：表示高，当您需要更严格的防护等级时，建议选择“3”，而“3”防护下对业务的误报率可能会增高，但漏报率降低，例如nc、nmap、kill等。

参数	是否必选	参数类型	描述
full_detection	否	Boolean	精准防护中的检测模式： • true：全检测。当用户的请求符合精准防护中的拦截条件时，不会立即拦截，WAF会继续执行其他防护的检测，待其他防护的检测完成后进行拦截。 • false：短路检测。当用户的请求符合精准防护中的拦截条件时，便立刻终止检测，进行拦截。

表 4-441 PolicyAction

参数	是否必选	参数类型	描述
category	否	String	防护等级： • log：仅记录 • block：拦截 枚举值： • **block** • **log**

表 4-442 PolicyOption

参数	是否必选	参数类型	描述
webattack	否	Boolean	基础防护是否开启 枚举值： • **true** • **false**
common	否	Boolean	常规检测是否开启 枚举值： • **true** • **false**
crawler	否	Boolean	反爬虫是否开启 枚举值： • **true** • **false**

参数	是否必选	参数类型	描述
crawler_engine	否	Boolean	搜索engine是否开启 枚举值： • **true** • **false**
crawler_scanner	否	Boolean	反爬虫检测是否开启 枚举值： • **true** • **false**
crawler_script	否	Boolean	脚本反爬虫是否开启 枚举值： • **true** • **false**
crawler_other	否	Boolean	其他爬虫是否开启 枚举值： • **true** • **false**
webshell	否	Boolean	Webshell检测是否开启 枚举值： • **true** • **false**
cc	否	Boolean	cc规则是否开启 枚举值： • **true** • **false**
custom	否	Boolean	精准防护是否开启 枚举值： • **true** • **false**
whiteblackip	否	Boolean	黑白名单防护是否开启 枚举值： • **true** • **false**

参数	是否必选	参数类型	描述
geoip	否	Boolean	地理位置访问控制规则是否开启 枚举值： • **true** • **false**
ignore	否	Boolean	误报屏蔽是否开启 枚举值： • **true** • **false**
privacy	否	Boolean	隐私屏蔽是否开启 枚举值： • **true** • **false**
antitamper	否	Boolean	网页防篡改规则是否开启 枚举值： • **true** • **false**
antileakage	否	Boolean	防敏感信息泄露规则是否开启 枚举值： • **true** • **false**
bot_enable	否	Boolean	防网络机器人攻击是否开启 枚举值： • **true** • **false**

响应参数

状态码： 200

表 4-443 响应 Body 参数

参数	参数类型	描述
id	String	防护策略id
name	String	防护策略名
action	PolicyAction object	操作

参数	参数类型	描述
options	**PolicyOption** object	选项
level	Integer	防护等级： • 1: 表示低，不检测header中的XSS攻击和CMDI攻击，当发现防护规则拦截了您的正常业务时，可调整防护等级为“1”，“1”防护下对业务的误报率降低，但漏报率可能会增高，例如：wget、curl等检测。 • 2：表示中，默认情况下，选择“2”，根据文件的敏感程度区分，中危检测有远程文件包含、第三方软件漏洞、Webshell、cp、ftp。 • 3：表示高，当您需要更严格的防护等级时，建议选择“3”，而“3”防护下对业务的误报率可能会增高，但漏报率降低，例如nc、nmap、kill等。
full_detection	Boolean	精准防护中的检测模式： • true：全检测。当用户的请求符合精准防护中的拦截条件时，不会立即拦截，WAF会继续执行其他防护的检测，待其他防护的检测完成后进行拦截。 • false：短路检测。当用户的请求符合精准防护中的拦截条件时，便立刻终止检测，进行拦截。
bind_host	Array of **BindHost** objects	防护域名的信息
timestamp	Integer	创建防护策略的时间
extend	Map<String,String>	扩展字段

表 4-444 PolicyAction

参数	参数类型	描述
category	String	防护等级： • log：仅记录 • block：拦截 枚举值： • **block** • **log**

表 4-445 PolicyOption

参数	参数类型	描述
webattack	Boolean	基础防护是否开启 枚举值： • **true** • **false**
common	Boolean	常规检测是否开启 枚举值： • **true** • **false**
crawler	Boolean	反爬虫是否开启 枚举值： • **true** • **false**
crawler_engine	Boolean	搜索engine是否开启 枚举值： • **true** • **false**
crawler_scanner	Boolean	反爬虫检测是否开启 枚举值： • **true** • **false**
crawler_script	Boolean	脚本反爬虫是否开启 枚举值： • **true** • **false**
crawler_other	Boolean	其他爬虫是否开启 枚举值： • **true** • **false**
webshell	Boolean	Webshell检测是否开启 枚举值： • **true** • **false**

参数	参数类型	描述
cc	Boolean	cc规则是否开启 枚举值： • **true** • **false**
custom	Boolean	精准防护是否开启 枚举值： • **true** • **false**
whiteblackip	Boolean	黑白名单防护是否开启 枚举值： • **true** • **false**
geoip	Boolean	地理位置访问控制规则是否开启 枚举值： • **true** • **false**
ignore	Boolean	误报屏蔽是否开启 枚举值： • **true** • **false**
privacy	Boolean	隐私屏蔽是否开启 枚举值： • **true** • **false**
antitamper	Boolean	网页防篡改规则是否开启 枚举值： • **true** • **false**
antileakage	Boolean	防敏感信息泄露规则是否开启 枚举值： • **true** • **false**

参数	参数类型	描述
bot_enable	Boolean	防网络机器人攻击是否开启 枚举值： • **true** • **false**

表 4-446 BindHost

参数	参数类型	描述
id	String	防护域名ID
hostname	String	防护域名
waf_type	String	防护域名对应模式：cloud（云模式）/premium（独享模式）
mode	String	仅独享模式涉及特殊域名模式

状态码： 400

表 4-447 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-448 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-449 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
PATCH https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}?enterprise_project_id=0

{
  "options" : {
    "whiteblackip" : false
  }
}
```

响应示例

状态码： 200

ok

```
{
  "id" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "level" : 2,
  "action" : {
    "category" : "log"
  },
  "options" : {
    "webattack" : true,
    "common" : true,
    "crawler" : true,
    "crawler_engine" : false,
    "crawler_scanner" : true,
    "crawler_script" : false,
    "crawler_other" : false,
    "webshell" : false,
    "cc" : true,
    "custom" : true,
    "precise" : false,
    "whiteblackip" : false,
    "geoip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "anticrawler" : false,
    "antileakage" : false,
    "followed_action" : false,
    "bot_enable" : true
  },
  "hosts" : [ "c0268b883a854adc8a2cd352193b0e13" ],
  "timestamp" : 1650529538732,
  "full_detection" : false,
  "bind_host" : [ {
    "id" : "c0268b883a854adc8a2cd352193b0e13",
    "hostname" : "www.demo.com",
    "waf_type" : "cloud"
  } ],
  "share_info" : {
    "is_receiver" : false,
    "provider_display" : {
      "share_count" : 0,
```

```
    "accept_count" : 0,
    "process_status" : 0
  }
 }
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.4.5 删除防护策略

功能介绍

删除防护策略

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}

表 4-450 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id

表 4-451 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-452 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-453 响应 Body 参数

参数	参数类型	描述
id	String	防护策略id
name	String	防护策略名
action	**PolicyAction** object	操作
options	**PolicyOption** object	选项
level	Integer	防护等级： ● 1: 表示低，不检测header中的XSS攻击和CMDI攻击，当发现防护规则拦截了您的正常业务时，可调整防护等级为“1”，“1”防护下对业务的误报率降低，但漏报率可能会增高，例如：wget、curl等检测。 ● 2：表示中，默认情况下，选择“2”，根据文件的敏感程度区分，中危检测有远程文件包含、第三方软件漏洞、Webshell、cp、ftp。 ● 3：表示高，当您需要更严格的防护等级时，建议选择“3”，而“3”防护下对业务的误报率可能会增高，但漏报率降低，例如nc、nmap、kill等。

参数	参数类型	描述
full_detection	Boolean	精准防护中的检测模式： • true：全检测。当用户的请求符合精准防护中的拦截条件时，不会立即拦截，WAF会继续执行其他防护的检测，待其他防护的检测完成后进行拦截。 • false：短路检测。当用户的请求符合精准防护中的拦截条件时，便立刻终止检测，进行拦截。
bind_host	Array of **BindHost** objects	防护域名的信息
timestamp	Integer	创建防护策略的时间
extend	Map<String,String>	扩展字段

表 4-454 PolicyAction

参数	参数类型	描述
category	String	防护等级： • log：仅记录 • block：拦截 枚举值： • **block** • **log**

表 4-455 PolicyOption

参数	参数类型	描述
webattack	Boolean	基础防护是否开启 枚举值： • **true** • **false**
common	Boolean	常规检测是否开启 枚举值： • **true** • **false**

参数	参数类型	描述
crawler	Boolean	反爬虫是否开启 枚举值： • **true** • **false**
crawler_engine	Boolean	搜索engine是否开启 枚举值： • **true** • **false**
crawler_scanner	Boolean	反爬虫检测是否开启 枚举值： • **true** • **false**
crawler_script	Boolean	脚本反爬虫是否开启 枚举值： • **true** • **false**
crawler_other	Boolean	其他爬虫是否开启 枚举值： • **true** • **false**
webshell	Boolean	Webshell检测是否开启 枚举值： • **true** • **false**
cc	Boolean	cc规则是否开启 枚举值： • **true** • **false**
custom	Boolean	精准防护是否开启 枚举值： • **true** • **false**

参数	参数类型	描述
whiteblackip	Boolean	黑白名单防护是否开启 枚举值： • **true** • **false**
geoip	Boolean	地理位置访问控制规则是否开启 枚举值： • **true** • **false**
ignore	Boolean	误报屏蔽是否开启 枚举值： • **true** • **false**
privacy	Boolean	隐私屏蔽是否开启 枚举值： • **true** • **false**
antitamper	Boolean	网页防篡改规则是否开启 枚举值： • **true** • **false**
antileakage	Boolean	防敏感信息泄露规则是否开启 枚举值： • **true** • **false**
bot_enable	Boolean	防网络机器人攻击是否开启 枚举值： • **true** • **false**

表 4-456 BindHost

参数	参数类型	描述
id	String	防护域名ID
hostname	String	防护域名

参数	参数类型	描述
waf_type	String	防护域名对应模式：cloud（云模式）/premium（独享模式）
mode	String	仅独享模式涉及特殊域名模式

状态码： 400

表 4-457 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-458 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-459 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "id" : "62169e2fc4e64148b775ec01b24a1947",
```

```
  "name" : "demo",
  "level" : 2,
  "action" : {
    "category" : "log",
    "modulex_category" : "log"
  },
  "options" : {
    "webattack" : true,
    "common" : true,
    "crawler" : true,
    "crawler_engine" : false,
    "crawler_scanner" : true,
    "crawler_script" : false,
    "crawler_other" : false,
    "webshell" : false,
    "cc" : true,
    "custom" : true,
    "precise" : false,
    "whiteblackip" : true,
    "geoip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "anticrawler" : false,
    "antileakage" : false,
    "followed_action" : false,
    "bot_enable" : true
  },
  "hosts" : [ ],
  "extend" : { },
  "timestamp" : 1649316510603,
  "full_detection" : false,
  "bind_host" : [ ]
}
```


状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.5 黑白名单规则管理

4.2.5.1 查询黑白名单规则列表

功能介绍

查询黑白名单规则列表

URI

GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip

表 4-460 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id

表 4-461 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id
page	否	Integer	分页查询时，返回第几页数据。范围0-100000，默认值为1，表示返回第1页数据。 缺省值：**1**
pagesize	否	Integer	分页查询时，每页包含多少条结果。范围1-100，默认值为10，表示每页包含10条结果。 缺省值：**10**
name	否	String	黑白名单规则名称

请求参数

表 4-462 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-463 响应 Body 参数

参数	参数类型	描述
total	Integer	规则条数
items	Array of **WhiteBlackIpResponseBody** objects	规则

表 4-464 WhiteBlackIpResponseBody

参数	参数类型	描述
id	String	规则id
policyid	String	策略id
timestamp	Long	创建规则的时间戳
description	String	规则描述
status	Integer	规则状态，0：关闭，1：开启
addr	String	黑白名单
white	Integer	防护动作： • 0拦截 • 1放行 • 2仅记录

状态码： 400

表 4-465 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-466 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-467 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/whiteblackip?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "total" : 1,
  "items" : [ {
    "id" : "3c96caf769ca4f57814fcf4259ea89a1",
    "policyid" : "4dddfd44fc89453e9fd9cd6bfdc39db2",
    "policyname" : "hkhtest",
    "timestamp" : 1650362891844,
    "description" : "demo",
    "status" : 1,
    "addr" : "x.x.x.x",
    "white" : 0
  } ]
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.5.2 创建黑白名单规则

功能介绍

创建黑白名单规则

URI

POST /v1/{project_id}/waf/policy/{policy_id}/whiteblackip

表 4-468 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id

表 4-469 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS)的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-470 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

表 4-471 请求 Body 参数

参数	是否必选	参数类型	描述
name	是	String	规则名称只能由字母、数字、-、_和.组成，长度不能超过64个字符
addr	是	String	黑白名单ip地址，需要输入标准的ip地址或地址段，例如：10.123.120.66或10.123.120.0/16
description	否	String	黑白名单规则描述
white	是	Integer	防护动作： ● 0 拦截 ● 1 放行 ● 2 仅记录

响应参数

状态码： 200

表 4-472 响应 Body 参数

参数	参数类型	描述
id	String	规则id
policyid	String	策略id
addr	String	黑白名单ip地址，需要输入标准的ip地址或地址段，例如：10.123.120.66或10.123.120.0/16
white	Integer	防护动作： ● 0 拦截 ● 1 放行 ● 2 仅记录
timestamp	Long	创建规则的时间戳,13位毫秒时间戳

状态码： 400

表 4-473 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码

参数	参数类型	描述
error_msg	String	错误信息

状态码： 401

表 4-474 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-475 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/whiteblackip?enterprise_project_id=0

{
  "name" : "demo",
  "white" : 0,
  "description" : "demo",
  "addr" : "x.x.x.x"
}
```

响应示例

状态码： 200

ok

```
{
  "id" : "5d43af25404341058d5ab17b7ba78b56",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "timestamp" : 1650531872900,
  "description" : "demo",
  "status" : 1,
  "addr" : "x.x.x.x",
  "white" : 0,
  "size" : 1
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.5.3 查询黑白名单防护规则

功能介绍

根据Id查询黑白名单防护规则

URI

GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}

表 4-476 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	project_id
policy_id	是	String	policyid
rule_id	是	String	whiteblackIpRuleId

请求参数

表 4-477 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-478 响应 Body 参数

参数	参数类型	描述
id	String	规则id
policyid	String	策略id
addr	String	黑白名单地址
description	String	黑白名单规则描述
white	Integer	防护动作： • 0 拦截 • 1 放行 • 2 仅记录

状态码： 400

表 4-479 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-480 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-481 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码

参数	参数类型	描述
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}?enterprise_project_id=0
```

响应示例

无

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.5.4 更新黑白名单防护规则

功能介绍

更新黑白名单防护规则

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}

表 4-482 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id

参数	是否必选	参数类型	描述
rule_id	是	String	黑白名单规则ID（从查询黑白名单规则列表ListWhiteblackipRule接口获取）

表 4-483 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS)的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-484 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

表 4-485 请求 Body 参数

参数	是否必选	参数类型	描述
name	是	String	黑白名单规则名称
addr	是	String	黑白名单ip地址，需要输入标准的ip地址或地址段，例如：10.123.120.66或10.123.120.0/16
description	否	String	黑白名单规则描述

参数	是否必选	参数类型	描述
white	是	Integer	防护动作： • 0 拦截 • 1 放行 • 2 仅记录

响应参数

状态码： 200

表 4-486 响应 Body 参数

参数	参数类型	描述
id	String	规则id
policyid	String	策略id
addr	String	黑白名单地址
description	String	黑白名单规则描述
white	Integer	防护动作： • 0 拦截 • 1 放行 • 2 仅记录

状态码： 400

表 4-487 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-488 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码

参数	参数类型	描述
error_msg	String	错误信息

状态码： 500

表 4-489 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}?enterprise_project_id=0

{
  "name" : "demo",
  "white" : 0,
  "description" : "demo",
  "addr" : "10.1.1.2"
}
```

响应示例

状态码： 200

ok

```
{
  "id" : "5d43af25404341058d5ab17b7ba78b56",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "timestamp" : 1650531872900,
  "description" : "demo",
  "status" : 1,
  "addr" : "1.1.1.2",
  "white" : 0
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.5.5 删除黑白名单防护规则

功能介绍

删除黑白名单防护规则

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}

表 4-490 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id
rule_id	是	String	黑白名单规则id，从查询黑白名单规则列表接口获取

表 4-491 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-492 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。

参数	是否必选	参数类型	描述
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-493 响应 Body 参数

参数	参数类型	描述
id	String	黑白名单规则id
policyid	String	策略id
name	String	黑白名单规则名称
timestamp	Long	删除规则时间，13位毫秒时间戳
description	String	描述
status	Integer	规则状态，0：关闭，1：开启
addr	String	黑白名单ip地址，需要输入标准的ip地址或地址段，例如：10.123.120.66或10.123.120.0/16
white	Integer	防护动作： • 0 拦截 • 1 放行 • 2 仅记录

状态码： 400

表 4-494 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-495 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-496 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/whiteblackip?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "id" : "5d43af25404341058d5ab17b7ba78b56",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "timestamp" : 1650531872900,
  "description" : "demo",
  "status" : 1,
  "addr" : "10.1.1.2",
  "white" : 0
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.6 CC 规则管理

4.2.6.1 查询 CC 规则列表

功能介绍

查询CC规则列表

URI

GET /v1/{project_id}/waf/policy/{policy_id}/cc

表 4-497 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id

表 4-498 Query 参数

参数	是否必选	参数类型	描述
page	否	Integer	分页查询时，返回第几页数据。范围0-100000，默认值为1，表示返回第1页数据。 缺省值：**1**
pagesize	否	Integer	分页查询时，每页包含多少条结果。范围1-100，默认值为10，表示每页包含10条结果。 缺省值：**10**

请求参数

表 4-499 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。

参数	是否必选	参数类型	描述
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-500 响应 Body 参数

参数	参数类型	描述
total	Integer	该策略下CC防护规则总数量
items	Array of **CcrulesListInfo** objects	cc规则对象列表

表 4-501 CcrulesListInfo

参数	参数类型	描述
id	String	CC规则ID
policyid	String	CC防护策略的策略ID
url	String	规则应用的URL链接，不包含域名： • 前缀匹配：以*结尾代表以该路径为前缀。例如，需要防护的路径为“/admin/test.php”或“/adminabc”，则路径可以填写为“/admin*”。 • 完全匹配：需要防护的路径需要与此处填写的路径完全相等。如果防护路径为“/admin”，该规则必须填写为“/admin”。
limit_num	String	单个用户的周期内请求次数（单用户限速）
limit_period	String	限速周期。
lock_time	String	锁定时长。取值范围为[0秒, 2^32秒)

参数	参数类型	描述
tag_type	String	防护模式： ● “ip”：IP限速，根据IP区分单个Web访问者。 ● “cookie”：用户限速，根据Cookie键值区分单个Web访问者。 ● “other”：根据Referer（自定义请求访问的来源）字段区分单个Web访问者。
tag_index	String	防护模式标签，当“tag_type”为cookie时，该参数表示cookie name。
action	**action** object	请求次数限制到达后采取的动作
timestamp	Long	创建规则时间戳

表 4-502 action

参数	参数类型	描述
category	String	动作类型： ● “block”：阻断 ● “captcha”：人机验证，阻断后用户需要输入正确的验证码，恢复正确的访问页面。 ● 当“tag_type”为“other”时，只能取值“block”。
detail	String	动作详情，动作详情，detail为null时表示默认阻断页面。 ● 当“category”为“captcha”时，不能传此字段； ● “category”为“block”时，需要传此字段。

表 4-503 detail

参数	参数类型	描述
redirect_url	String	返回页面重定向的url
response	**response** object	返回页面

表 4-504 response

参数	参数类型	描述
content_type	String	内容类型，固定值为“application/json”、“text/html”、“text/xml”。
content	String	内容

状态码： 400

表 4-505 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-506 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-507 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/cc?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "total" : 1,
  "items" : [ {
    "aging_time" : 0,
    "description" : "",
    "id" : "a5f3fd28db564696b199228f0ac346b2",
    "limit_num" : 10,
    "limit_period" : 60,
    "lock_time" : 0,
    "mode" : 0,
    "policyid" : "1f016cde588646aca3fb19f277c44d03",
    "prefix" : false,
    "producer" : 1,
    "status" : 1,
    "tag_type" : "ip",
    "timestamp" : 1656494435686,
    "total_num" : 0,
    "unaggregation" : false,
    "url" : "/path"
  } ]
}
```


状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.6.2 创建 CC 规则

功能介绍

创建CC规则

URI

POST /v1/{project_id}/waf/policy/{policy_id}/cc

表 4-508 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id

请求参数

表 4-509 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

表 4-510 请求 Body 参数

参数	是否必选	参数类型	描述
description	否	String	规则描述
limit_num	否	Integer	限制频率次数 最小值：**0** 最大值：**10000**
limit_period	否	Integer	限制频率单位时间 最小值：**0** 最大值：**10000**
url	否	String	url 最小值：**0** 最大值：**10000**
mode	否	Integer	工作模式：（0标准，1高级），高级模式参数无法在同一个接口同一份文档中用描述，参考console页面构建参数 枚举值： • **0** • **1**
action	否	**action** object	请求次数限制到达后采取的动作

参数	是否必选	参数类型	描述
tag_type	否	String	防护模式： • “ip”：IP限速，根据IP区分单个Web访问者。 • “cookie”：用户限速，根据Cookie键值区分单个Web访问者。 • “other”：根据Referer（自定义请求访问的来源）字段区分单个Web访问者。 枚举值： • **ip** • **other** • **cookie**

表 4-511 action

参数	是否必选	参数类型	描述
category	否	String	防护动作

响应参数

状态码： 200

表 4-512 响应 Body 参数

参数	参数类型	描述
total	Integer	该策略下cc规则数量
items	Array of **CcrulesListInfo** objects	cc规则对象列表

表 4-513 CcrulesListInfo

参数	参数类型	描述
id	String	CC规则ID
policyid	String	CC防护策略的策略ID

参数	参数类型	描述
url	String	规则应用的URL链接，不包含域名： ● 前缀匹配：以*结尾代表以该路径为前缀。例如，需要防护的路径为“/admin/test.php”或“/adminabc”，则路径可以填写为“/admin*”。 ● 完全匹配：需要防护的路径需要与此处填写的路径完全相等。如果防护路径为“/admin”，该规则必须填写为“/admin”。
limit_num	String	单个用户的周期内请求次数（单用户限速）
limit_period	String	限速周期。
lock_time	String	锁定时长。取值范围为[0秒, 2^32秒)
tag_type	String	防护模式： ● “ip”：IP限速，根据IP区分单个Web访问者。 ● “cookie”：用户限速，根据Cookie键值区分单个Web访问者。 ● “other”：根据Referer（自定义请求访问的来源）字段区分单个Web访问者。
tag_index	String	防护模式标签，当“tag_type”为cookie时，该参数表示cookie name。
action	**action** object	请求次数限制到达后采取的动作
timestamp	Long	创建规则时间戳

表 4-514 action

参数	参数类型	描述
category	String	动作类型： ● “block”：阻断 ● “captcha”：人机验证，阻断后用户需要输入正确的验证码，恢复正确的访问页面。 ● 当“tag_type”为“other”时，只能取值“block”。
detail	String	动作详情，动作详情，detail为null时表示默认阻断页面。 ● 当“category”为“captcha”时，不能传此字段； ● “category”为“block”时，需要传此字段。

表 4-515 detail

参数	参数类型	描述
redirect_url	String	返回页面重定向的url
response	**response** object	返回页面

表 4-516 response

参数	参数类型	描述
content_type	String	内容类型，固定值为“application/json”、“text/html”、“text/xml”。
content	String	内容

状态码： 400

表 4-517 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-518 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-519 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/cc?enterprise_project_id=0

{
  "action" : {
    "category" : "captcha"
  },
  "description" : "",
  "limit_num" : 10,
  "limit_period" : 60,
  "mode" : 0,
  "tag_type" : "ip",
  "url" : "/path"
}
```

响应示例

状态码： 200

ok

```
{
  "aging_time" : 0,
  "description" : "",
  "id" : "a5f3fd28db564696b199228f0ac346b2",
  "limit_num" : 10,
  "limit_period" : 60,
  "lock_time" : 0,
  "mode" : 0,
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "prefix" : false,
  "producer" : 1,
  "status" : 1,
  "tag_type" : "ip",
  "timestamp" : 1656494435686,
  "total_num" : 0,
  "unaggregation" : false,
  "url" : "/path"
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.6.3 根据 Id 查询 CC 防护规则

功能介绍

根据Id查询CC护规则

URI

GET /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}

表 4-520 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id
rule_id	是	String	ccRuleId

请求参数

表 4-521 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-522 响应 Body 参数

参数	参数类型	描述
id	String	CC规则ID
policyid	String	CC防护策略的策略ID

参数	参数类型	描述
url	String	规则应用的URL链接，不包含域名： ● 前缀匹配：以*结尾代表以该路径为前缀。例如，需要防护的路径为“/admin/test.php”或“/adminabc”，则路径可以填写为“/admin*”。 ● 完全匹配：需要防护的路径需要与此处填写的路径完全相等。如果防护路径为“/admin”，该规则必须填写为“/admin”。
limit_num	String	单个用户的周期内请求次数（单用户限速）
limit_period	String	限速周期。
lock_time	String	锁定时长。取值范围为[0秒, 2^32秒)
tag_type	String	防护模式： ● “ip”：IP限速，根据IP区分单个Web访问者。 ● “cookie”：用户限速，根据Cookie键值区分单个Web访问者。 ● “other”：根据Referer（自定义请求访问的来源）字段区分单个Web访问者。
tag_index	String	防护模式标签，当“tag_type”为cookie时，该参数表示cookie name。
action	**action** object	请求次数限制到达后采取的动作
timestamp	Long	创建规则时间戳

表 4-523 action

参数	参数类型	描述
category	String	动作类型： ● “block”：阻断 ● “captcha”：人机验证，阻断后用户需要输入正确的验证码，恢复正确的访问页面。 ● 当“tag_type”为“other”时，只能取值“block”。
detail	String	动作详情，动作详情，detail为null时表示默认阻断页面。 ● 当“category”为“captcha”时，不能传此字段； ● “category”为“block”时，需要传此字段。

表 4-524 detail

参数	参数类型	描述
redirect_url	String	返回页面重定向的url
response	**response** object	返回页面

表 4-525 response

参数	参数类型	描述
content_type	String	内容类型，固定值为“application/json”、“text/html”、“text/xml”。
content	String	内容

状态码： 400

表 4-526 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-527 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-528 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "aging_time" : 0,
  "description" : "",
  "id" : "a5f3fd28db564696b199228f0ac346b2",
  "limit_num" : 10,
  "limit_period" : 60,
  "lock_time" : 0,
  "mode" : 0,
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "prefix" : false,
  "producer" : 1,
  "status" : 1,
  "tag_type" : "ip",
  "timestamp" : 1656494435686,
  "total_num" : 0,
  "unaggregation" : false,
  "url" : "/path"
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.6.4 更新 CC 防护规则

功能介绍

更新CC防护规则

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}

表 4-529 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	policyid
rule_id	是	String	ccRuleId

请求参数

表 4-530 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

表 4-531 请求 Body 参数

参数	是否必选	参数类型	描述
description	否	String	规则描述
limit_num	否	Integer	限制频率次数 最小值：**0** 最大值：**10000**
limit_period	否	Integer	限制频率单位时间 最小值：**0** 最大值：**10000**
url	否	String	url 最小值：**0** 最大值：**10000**
mode	否	Integer	工作模式：（0标准，1高级），高级模式参数无法在同一个接口同一份文档中用描述，参考console页面构建参数 枚举值： • **0** • **1**
action	否	**action** object	请求次数限制到达后采取的动作

参数	是否必选	参数类型	描述
tag_type	否	String	防护模式： • “ip”：IP限速，根据IP区分单个Web访问者。 • “cookie”：用户限速，根据Cookie键值区分单个Web访问者。 • “other”：根据Referer（自定义请求访问的来源）字段区分单个Web访问者。 枚举值： • **ip** • **other** • **cookie**

表 4-532 action

参数	是否必选	参数类型	描述
category	否	String	防护动作

响应参数

状态码： 200

表 4-533 响应 Body 参数

参数	参数类型	描述
id	String	CC规则ID
policyid	String	CC防护策略的策略ID
url	String	规则应用的URL链接，不包含域名： • 前缀匹配：以*结尾代表以该路径为前缀。例如，需要防护的路径为“/admin/test.php”或“/adminabc”，则路径可以填写为“/admin*”。 • 完全匹配：需要防护的路径需要与此处填写的路径完全相等。如果防护路径为“/admin”，该规则必须填写为“/admin”。
limit_num	String	单个用户的周期内请求次数（单用户限速）
limit_period	String	限速周期。

参数	参数类型	描述
lock_time	String	锁定时长。取值范围为[0秒, 2^32秒)
tag_type	String	防护模式： • “ip”：IP限速，根据IP区分单个Web访问者。 • “cookie”：用户限速，根据Cookie键值区分单个Web访问者。 • “other”：根据Referer（自定义请求访问的来源）字段区分单个Web访问者。
tag_index	String	防护模式标签，当“tag_type”为cookie时，该参数表示cookie name。
action	**action** object	请求次数限制到达后采取的动作

表 4-534 action

参数	参数类型	描述
category	String	动作类型： • “block”：阻断 • “captcha”：人机验证，阻断后用户需要输入正确的验证码，恢复正确的访问页面。 • 当“tag_type”为“other”时，只能取值“block”。
detail	String	动作详情，动作详情，detail为null时表示默认阻断页面。 • 当“category”为“captcha”时，不能传此字段； • “category”为“block”时，需要传此字段。

表 4-535 detail

参数	参数类型	描述
redirect_url	String	返回页面重定向的url
response	**response** object	返回页面

表 4-536 response

参数	参数类型	描述
content_type	String	内容类型，固定值为“application/json”、“text/html”、“text/xml”。
content	String	内容

状态码： 400

表 4-537 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-538 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-539 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}?enterprise_project_id=0

{
  "action" : {
    "category" : "captcha"
  },
  "description" : "",
  "limit_num" : 10,
  "limit_period" : 60,
```

```
  "mode" : 0,
  "tag_type" : "ip",
  "url" : "/path1"
}
```

响应示例

状态码： 200

ok

```
{
  "aging_time" : 0,
  "description" : "",
  "id" : "a5f3fd28db564696b199228f0ac346b2",
  "limit_num" : 10,
  "limit_period" : 60,
  "lock_time" : 0,
  "mode" : 0,
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "prefix" : false,
  "producer" : 1,
  "status" : 1,
  "tag_type" : "ip",
  "total_num" : 0,
  "unaggregation" : false,
  "url" : "/path1"
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.6.5 删除 CC 防护规则

功能介绍

删除CC防护规则

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}

表 4-540 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id
rule_id	是	String	ccRuleId

请求参数

表 4-541 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 400

表 4-542 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-543 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-544 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "aging_time" : 0,
  "description" : "",
  "id" : "a5f3fd28db564696b199228f0ac346b2",
  "limit_num" : 10,
  "limit_period" : 60,
  "lock_time" : 0,
  "mode" : 0,
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "prefix" : false,
  "producer" : 1,
  "status" : 1,
  "tag_type" : "ip",
  "timestamp" : 1656494435686,
  "total_num" : 0,
  "unaggregation" : false,
  "url" : "/path1"
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.7 精准防护规则管理

4.2.7.1 查询精准防护规则列表

功能介绍

查询精准防护规则列表

URI

GET /v1/{project_id}/waf/policy/{policy_id}/custom

表 4-545 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id

表 4-546 Query 参数

参数	是否必选	参数类型	描述
page	否	Integer	分页查询时，返回第几页数据。范围0-100000，默认值为1，表示返回第1页数据。 缺省值：**1**
pagesize	否	Integer	分页查询时，每页包含多少条结果。范围1-100，默认值为10，表示每页包含10条结果。 缺省值：**10**

请求参数

表 4-547 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-548 响应 Body 参数

参数	参数类型	描述
total	Integer	该策略下设置的精准防护规则总数量
items	Array of objects	精准防护规则的对象列表

表 4-549 CustomRuleBody

参数	参数类型	描述
id	String	精准防护规则的id
policyid	String	精准防护规则的策略id
conditions	Array of **conditions** objects	匹配条件列表，匹配条件必须同时满足。
action	**action** object	精准防护规则命中后操作对象
priority	Integer	执行该规则的优先级，值越小，优先级越高，值相同时，规则创建时间早，优先级越高。取值范围：0到1000。
timestamp	Long	创建精准防护规则的
start	Long	精准防护规则生效的起始时间戳（毫秒）。当time=true，才会返回该参数。
terminal	Long	精准防护规则生效的终止时间戳（毫秒）。当time=true，才会返回该参数。

表 4-550 conditions

参数	参数类型	描述
category	String	字段类型。固定值path、user-agent、ip、params、cookie、referer、header。

参数	参数类型	描述
index	String	该参数的含义为： ● 字段类型为ip且子字段为客户端ip时，不需要传index参数 ● 字段类型为ip且子字段类型为X-Forwarded-For时，index参数值为x-forwarded-for ● 字段类型为params、header、cookie并且子字段为自定义时，index的值为自定义子字段
check_all_indexes_logic	Integer	使用自定义子字段、字段类型为url或ip时不需要传check_all_indexes_logic参数，其它情况需要传该参数: ● 1：检查所有子字段 ● 2：检查任意子字段 ● null：使用自定义子字段
logic_operation	Integer	条件匹配逻辑，“contain”，“not_contain”，“equal”，“not_equal”，“prefix”，“not_prefix”，“suffix”，“not_suffix”分别代表包含、不包含、等于、不等于、前缀为、前缀不为、后缀为、后缀不为。 当条件类型“category”为ip时，“logic_operation”只能为“equal”或者“not_equal”
contents	Array of strings	条件匹配的内容

表 4-551 action

参数	参数类型	描述
category	String	操作类型。 ● “block”：拦截。 ● “pass”：放行。

状态码： 400

表 4-552 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-553 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-554 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/custom?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "items" : [ {
    "category" : "block",
    "action_mode" : false,
    "aging_time" : 0,
    "conditions" : [ {
      "category" : "header",
      "index" : "sdfsafsda",
      "logic_operation" : "exist"
    } ],
    "description" : "",
    "id" : "2a3caa2bc9814c09ad73d02e3485b4a4",
    "policyid" : "1f016cde588646aca3fb19f277c44d03",
    "priority" : 50,
    "producer" : 1,
    "status" : 1,
    "time" : false,
    "timestamp" : 1656495488880
  } ],
  "total" : 1
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.7.2 创建精准防护规则

功能介绍

创建精准防护规则

URI

POST /v1/{project_id}/waf/policy/{policy_id}/custom

表 4-555 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id

请求参数

表 4-556 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

表 4-557 请求 Body 参数

参数	是否必选	参数类型	描述
name	否	String	自定义规则的名称
time	否	Boolean	精准防护规则生效时间: • “false”：表示该规则立即生效。 • “true”：表示自定义生效时间。
start	否	Long	精准防护规则生效的起始时间戳（毫秒）。当time=true，才会返回该参数。
terminal	否	Long	精准防护规则生效的终止时间戳（毫秒）。当time=true，才会返回该参数。
conditions	否	Array of **CustomConditions** objects	匹配条件列表
action	否	**CustomAction** object	精准防护规则命中后操作对象
priority	否	Integer	执行该规则的优先级，值越小，优先级越高，值相同时，规则创建时间早，优先级越高。取值范围：0到1000。

表 4-558 CustomConditions

参数	是否必选	参数类型	描述
category	否	String	条件类型 固定值path、user-agent、ip、params、cookie、referer、header
index	否	String	当“category”为“cookie”时，index表示cookie。 • 当“category”为“params”时，index表示param。 当“category”为“header”时，index表示header中的选项
check_all_indexes_logic	否	Integer	取值范围：1,2；1 表示全部子字段，2 表示任意子字段

参数	是否必选	参数类型	描述
logic_operation	否	Integer	“contain”，“not_contain”，“equal”，“not_equal”，“prefix”，“not_prefix”，“suffix”，“not_suffix”分别代表包含、不包含、等于、不等于、前缀为、前缀不为、后缀为、后缀不为。当条件类型“category”为ip时，“logic_operation”只能为“equal”或者“not_equal”
contents	否	Array of strings	条件匹配的内容
value_list_id	否	String	引用表的id

表 4-559 CustomAction

参数	是否必选	参数类型	描述
category	否	String	操作类型。 • “block”：拦截。 • “pass”：放行。

响应参数

状态码： 200

表 4-560 响应 Body 参数

参数	参数类型	描述
id	String	精准防护规则的id
policyid	String	精准防护规则的策略id
conditions	Array of **conditions** objects	匹配条件列表，匹配条件必须同时满足。
action	**action** object	精准防护规则命中后操作对象
priority	Integer	执行该规则的优先级，值越小，优先级越高，值相同时，规则创建时间早，优先级越高。取值范围：0到1000。
timestamp	Long	创建精准防护规则的时间戳

参数	参数类型	描述
start	Long	精准防护规则生效的起始时间戳（毫秒）。当time=true，才会返回该参数。
terminal	Long	精准防护规则生效的终止时间戳（毫秒）。当time=true，才会返回该参数。

表 4-561 conditions

参数	参数类型	描述
category	String	条件类型。固定值path、user-agent、ip、params、cookie、referer、header。
index	String	当“category”为“cookie”时，index表示cookie。 ● 当“category”为“params”时，index表示param。 ● 当“category”为“header”时，index表示header中的选项
check_all_indexes_logic	Integer	取值范围：1,2；1 表示全部子字段，2 表示任意子字段
logic_operation	Integer	“contain”，“not_contain”，“equal”，“not_equal”，“prefix”，“not_prefix”，“suffix”，“not_suffix”分别代表包含、不包含、等于、不等于、前缀为、前缀不为、后缀为、后缀不为。当条件类型“category”为ip时，“logic_operation”只能为“equal”或者“not_equal”
contents	Array of strings	条件匹配的内容

表 4-562 action

参数	参数类型	描述
category	String	操作类型。 ● “block”：拦截。 ● “pass”：放行。

状态码： 400

表 4-563 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-564 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-565 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/custom?enterprise_project_id=0

{
  "description" : "",
  "action" : {
    "category" : "block"
  },
  "priority" : 50,
  "conditions" : [ {
    "category" : "header",
    "logic_operation" : "exist",
    "index" : "sdfsafsda"
  } ],
  "time" : false
}
```

响应示例

状态码： 200

ok

```
{
  "items" : [ {
```

```
  "action" : {
    "category" : "block"
  },
  "action_mode" : false,
  "aging_time" : 0,
  "conditions" : [ {
    "category" : "header",
    "index" : "sdfsafsda",
    "logic_operation" : "exist"
  } ],
  "description" : "",
  "id" : "2a3caa2bc9814c09ad73d02e3485b4a4",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "priority" : 50,
  "producer" : 1,
  "status" : 1,
  "time" : false,
  "timestamp" : 1656495488880
 } ]
}
```


状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.7.3 根据 Id 查询精准防护规则

功能介绍

根据Id查询精准防护规则

URI

GET /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}

表 4-566 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id

参数	是否必选	参数类型	描述
rule_id	是	String	customRuleId

请求参数

表 4-567 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-568 响应 Body 参数

参数	参数类型	描述
id	String	精准防护规则的id
policyid	String	精准防护规则的策略id
conditions	Array of **conditions** objects	匹配条件列表，匹配条件必须同时满足。
action	**action** object	精准防护规则命中后操作对象
priority	Integer	执行该规则的优先级，值越小，优先级越高，值相同时，规则创建时间早，优先级越高。取值范围：0到1000。
timestamp	Long	创建精准防护规则的
start	Long	精准防护规则生效的起始时间戳（毫秒）。当time=true，才会返回该参数。
terminal	Long	精准防护规则生效的终止时间戳（毫秒）。当time=true，才会返回该参数。

表 4-569 conditions

参数	参数类型	描述
category	String	条件类型。固定值path、user-agent、ip、params、cookie、referer、header。
index	String	当“category”为“cookie”时，index表示cookie。 ● 当“category”为“params”时，index表示param。 当“category”为“header”时，index表示header中的选项
check_all_indexes_logic	Integer	取值范围：1,2；1 表示全部子字段，2 表示任意子字段
logic_operation	Integer	“contain”，“not_contain”，“equal”，“not_equal”，“prefix”，“not_prefix”，“suffix”，“not_suffix”分别代表包含、不包含、等于、不等于、前缀为、前缀不为、后缀为、后缀不为。当条件类型“category”为ip时，“logic_operation”只能为“equal”或者“not_equal”
contents	Array of strings	条件匹配的内容

表 4-570 action

参数	参数类型	描述
category	String	操作类型。 ● “block”：拦截。 ● “pass”：放行。

状态码： 400

表 4-571 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-572 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-573 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "action" : {
    "category" : "block"
  },
  "action_mode" : false,
  "aging_time" : 0,
  "conditions" : [ {
    "category" : "header",
    "index" : "sdfsafsda",
    "logic_operation" : "exist"
  } ],
  "description" : "",
  "id" : "2a3caa2bc9814c09ad73d02e3485b4a4",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "priority" : 50,
  "producer" : 1,
  "status" : 1,
  "time" : false,
  "timestamp" : 1656495488880
}
```

状态码

状态码	描述
200	ok
400	请求失败

状态码	描述
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.7.4 更新精准防护规则

功能介绍

更新精准防护规则

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}

表 4-574 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id
rule_id	是	String	customRuleId

请求参数

表 4-575 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

表 4-576 请求 Body 参数

参数	是否必选	参数类型	描述
name	否	String	自定义规则的名称
time	否	Boolean	精准防护规则生效时间: • “false”：表示该规则立即生效。 -“true”：表示自定义生效时间。
start	否	Long	精准防护规则生效的起始时间戳（毫秒）。当time=true，才会返回该参数。
terminal	否	Long	精准防护规则生效的终止时间戳（毫秒）。当time=true，才会返回该参数。
conditions	否	Array of **CustomConditions** objects	匹配条件列表
action	否	**CustomAction** object	精准防护规则命中后操作对象
priority	否	Integer	执行该规则的优先级，值越小，优先级越高，值相同时，规则创建时间早，优先级越高。取值范围：0到1000。

表 4-577 CustomConditions

参数	是否必选	参数类型	描述
category	否	String	条件类型 固定值path、user-agent、ip、params、cookie、referer、header
index	否	String	当“category”为“cookie”时，index表示cookie。 • 当“category”为“params”时，index表示param。 当“category”为“header”时，index表示header中的选项
check_all_indexes_logic	否	Integer	取值范围：1,2；1 表示全部子字段，2 表示任意子字段

参数	是否必选	参数类型	描述
logic_operation	否	Integer	“contain”，“not_contain”，“equal”，“not_equal”，“prefix”，“not_prefix”，“suffix”，“not_suffix”分别代表包含、不包含、等于、不等于、前缀为、前缀不为、后缀为、后缀不为。当条件类型“category”为ip时，“logic_operation”只能为“equal”或者“not_equal”
contents	否	Array of strings	条件匹配的内容
value_list_id	否	String	引用表的id

表 4-578 CustomAction

参数	是否必选	参数类型	描述
category	否	String	操作类型。 • “block”：拦截。 • “pass”：放行。

响应参数

状态码： 200

表 4-579 响应 Body 参数

参数	参数类型	描述
id	String	精准防护规则的id
policyid	String	精准防护规则的策略id
conditions	Array of **conditions** objects	匹配条件列表，匹配条件必须同时满足。
action	**action** object	精准防护规则命中后操作对象
priority	Integer	执行该规则的优先级，值越小，优先级越高，值相同时，规则创建时间早，优先级越高。取值范围：0到1000。
timestamp	Long	创建精准防护规则的

参数	参数类型	描述
start	Long	精准防护规则生效的起始时间戳（毫秒）。当time=true，才会返回该参数。
terminal	Long	精准防护规则生效的终止时间戳（毫秒）。当time=true，才会返回该参数。

表 4-580 conditions

参数	参数类型	描述
category	String	条件类型。固定值path、user-agent、ip、params、cookie、referer、header。
index	String	当“category”为“cookie”时，index表示cookie。 ● 当“category”为“params”时，index表示param。 ● 当“category”为“header”时，index表示header中的选项
check_all_indexes_logic	Integer	取值范围：1,2；1 表示全部子字段，2 表示任意子字段
logic_operation	Integer	“contain”，“not_contain”，“equal”，“not_equal”，“prefix”，“not_prefix”，“suffix”，“not_suffix”分别代表包含、不包含、等于、不等于、前缀为、前缀不为、后缀为、后缀不为。当条件类型“category”为ip时，“logic_operation”只能为“equal”或者“not_equal”
contents	Array of strings	条件匹配的内容

表 4-581 action

参数	参数类型	描述
category	String	操作类型。 ● “block”：拦截。 ● “pass”：放行。

状态码： 400

表 4-582 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-583 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-584 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}?enterprise_project_id=0

{
  "description" : "",
  "action" : {
    "category" : "block"
  },
  "priority" : 50,
  "conditions" : [ {
    "category" : "header",
    "logic_operation" : "exist",
    "index" : "sdfsafsda1"
  } ],
  "time" : false
}
```

响应示例

状态码： 200

ok

```
{
  "action" : {
```

```
    "category" : "block"
  },
  "action_mode" : false,
  "aging_time" : 0,
  "conditions" : [ {
    "category" : "header",
    "index" : "sdfsafsda1",
    "logic_operation" : "exist"
  } ],
  "description" : "",
  "id" : "2a3caa2bc9814c09ad73d02e3485b4a4",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "priority" : 50,
  "producer" : 1,
  "status" : 1,
  "time" : false
}
```


状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.7.5 删除精准防护规则

功能介绍

删除精准防护规则

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}

表 4-585 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id
rule_id	是	String	customRuleId

请求参数

表 4-586 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 400

表 4-587 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-588 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-589 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}?enterprise_project_id=0
```

响应示例

状态码： 200

ok


```
{
  "action" : {
    "category" : "block"
  },
  "action_mode" : false,
  "aging_time" : 0,
  "conditions" : [ {
    "category" : "header",
    "index" : "sdfsafsda1",
    "logic_operation" : "exist"
  } ],
  "description" : "",
  "id" : "2a3caa2bc9814c09ad73d02e3485b4a4",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "priority" : 50,
  "producer" : 1,
  "status" : 1,
  "time" : false,
  "timestamp" : 1656495488880
}
```


状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.8 隐私屏蔽规则管理

4.2.8.1 查询隐私屏蔽规则列表

功能介绍

查询隐私屏蔽规则列表

URI

GET /v1/{project_id}/waf/policy/{policy_id}/privacy

表 4-590 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id

表 4-591 Query 参数

参数	是否必选	参数类型	描述
page	否	Integer	分页查询时，返回第几页数据。范围0-100000，默认值为1，表示返回第1页数据。
pagesize	否	Integer	分页查询时，每页包含多少条结果。范围1-100，默认值为10，表示每页包含10条结果。

请求参数

表 4-592 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-593 响应 Body 参数

参数	参数类型	描述
total	Integer	规则条数
items	Array of **PrivacyResponseBody** objects	规则

表 4-594 PrivacyResponseBody

参数	参数类型	描述
id	String	规则id
policyid	String	策略id
timestamp	Long	创建规则的时间，格式为13位毫秒时间戳
status	Integer	规则状态，0：关闭，1：开启
url	String	隐私屏蔽规则应用的url
category	String	屏蔽字段。 枚举值： • **params** • **cookie** • **header** • **form**
index	String	屏蔽字段名

状态码： 400

表 4-595 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-596 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-597 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/privacy?enterprise_project_id=0
```

响应示例

状态码： 200

OK

```
{
  "total" : 1,
  "items" : [ {
    "category" : "params",
    "description" : "",
    "id" : "41a5674e03a1470a90ac4761ec4657b4",
    "index" : "password",
    "policyid" : "1f016cde588646aca3fb19f277c44d03",
    "status" : 1,
    "timestamp" : 1656504425319,
    "url" : "/login"
  } ]
}
```

状态码

状态码	描述
200	OK
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.8.2 创建隐私屏蔽规则

功能介绍

创建隐私屏蔽规则

URI

POST /v1/{project_id}/waf/policy/{policy_id}/privacy

表 4-598 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id

请求参数

表 4-599 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

表 4-600 请求 Body 参数

参数	是否必选	参数类型	描述
url	是	String	隐私屏蔽规则防护的url，需要填写标准的url格式，例如/admin/xxx或者/admin/,*以*"'号结尾代表路径前缀
category	是	String	屏蔽字段 枚举值： • **params** • **cookie** • **header** • **form**
index	是	String	屏蔽字段名
description	否	String	规则描述

响应参数

状态码： 200

表 4-601 响应 Body 参数

参数	参数类型	描述
id	String	规则id
policyid	String	策略id
url	String	隐私屏蔽规则防护的url，需要填写标准的url格式，例如/admin/xxx或者/admin/,以'"'号结尾代表路径前缀
category	String	屏蔽字段 枚举值： • **params** • **cookie** • **header** • **form**
index	String	屏蔽字段名

状态码： 400

表 4-602 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-603 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-604 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/privacy?enterprise_project_id=0

{
  "url" : "/login",
  "category" : "params",
  "index" : "password",
  "description" : ""
}
```

响应示例

状态码： 200

OK

```
{
  "category" : "params",
  "description" : "",
  "id" : "41a5674e03a1470a90ac4761ec4657b4",
  "index" : "password",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "status" : 1,
  "timestamp" : 1656504425319,
  "url" : "/login"
}
```

状态码

状态码	描述
200	OK
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.8.3 根据 Id 查询隐私屏蔽防护规则

功能介绍

根据Id查询隐私屏蔽防护规则

URI

GET /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}

表 4-605 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id
rule_id	是	String	privacyRuleId

请求参数

表 4-606 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-607 响应 Body 参数

参数	参数类型	描述
id	String	规则id
policyid	String	策略id
url	String	隐私屏蔽规则防护的url，需要填写标准的url格式，例如/admin/xxx或者/admin/,以"'"号结尾代表路径前缀

参数	参数类型	描述
category	String	屏蔽字段 枚举值： • **params** • **cookie** • **header** • **form**
index	String	屏蔽字段名

状态码： 400

表 4-608 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-609 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-610 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "category" : "params",
  "description" : "",
  "id" : "41a5674e03a1470a90ac4761ec4657b4",
  "index" : "password",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "status" : 1,
  "timestamp" : 1656504425319,
  "url" : "/login"
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.8.4 更新隐私屏蔽防护规则

功能介绍

更新隐私屏蔽防护规则

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}

表 4-611 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id
rule_id	是	String	privacyRuleId

请求参数

表 4-612 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

表 4-613 请求 Body 参数

参数	是否必选	参数类型	描述
url	是	String	隐私屏蔽规则防护的url，需要填写标准的url格式，例如/admin/xxx或者/admin/,*以*'"号结尾代表路径前缀
category	是	String	屏蔽字段 枚举值： • **params** • **cookie** • **header** • **form**
index	是	String	屏蔽字段名
description	否	String	规则描述

响应参数

状态码： 200

表 4-614 响应 Body 参数

参数	参数类型	描述
id	String	规则id
policyid	String	策略id
url	String	隐私屏蔽规则防护的url，需要填写标准的url格式，例如/admin/xxx或者/admin/,*以*'"号结尾代表路径前缀

参数	参数类型	描述
category	String	屏蔽字段 枚举值： • **params** • **cookie** • **header** • **form**
index	String	屏蔽字段名

状态码： 400

表 4-615 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-616 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-617 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}?enterprise_project_id=0

{
```

```
  "url" : "/login",
  "category" : "header",
  "index" : "token",
  "description" : ""
}
```

响应示例

状态码： 200

ok

```
{
  "category" : "header",
  "description" : "",
  "id" : "41a5674e03a1470a90ac4761ec4657b4",
  "index" : "token",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "status" : 1,
  "timestamp" : 1656504425319,
  "url" : "/login"
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.8.5 删除隐私屏蔽防护规则

功能介绍

删除隐私屏蔽防护规则

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}

表 4-618 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id

参数	是否必选	参数类型	描述
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id
rule_id	是	String	privacyRuleId

请求参数

表 4-619 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 400

表 4-620 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-621 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-622 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "category" : "header",
  "description" : "",
  "id" : "41a5674e03a1470a90ac4761ec4657b4",
  "index" : "token",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "status" : 1,
  "timestamp" : 1656504425319,
  "url" : "/login"
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.9 网页防篡改规则管理

4.2.9.1 查询防篡改规则列表

功能介绍

查询防篡改规则列表

URI

GET /v1/{project_id}/waf/policy/{policy_id}/antitamper

表 4-623 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id

表 4-624 Query 参数

参数	是否必选	参数类型	描述
page	否	Integer	分页查询时，返回第几页数据。范围0-100000，默认值为1，表示返回第1页数据。 缺省值：**1**
pagesize	否	Integer	分页查询时，每页包含多少条结果。范围1-100，默认值为10，表示每页包含10条结果。 缺省值：**10**

请求参数

表 4-625 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-626 响应 Body 参数

参数	参数类型	描述
total	Integer	总条数
items	Array of **AntiTamperRuleResponseBody** objects	规则

表 4-627 AntiTamperRuleResponseBody

参数	参数类型	描述
id	String	规则id
policyid	String	策略id
timestamp	Long	时间戳(毫秒)
description	String	创建规则的描述
status	Integer	规则状态，0：关闭，1：开启
hostname	String	防篡改的URL链接，不包含域名。
url	String	防篡改的url

状态码： 400

表 4-628 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-629 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-630 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antitamper?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "total" : 1,
  "items" : [ {
    "description" : "",
    "hostname" : "www.domain.com",
    "id" : "0f59185b76c143f884d21cd0d88e6fa8",
    "policyid" : "1f016cde588646aca3fb19f277c44d03",
    "status" : 1,
    "timestamp" : 1656506256928,
    "url" : "/login"
  } ]
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.9.2 创建防篡改规则

功能介绍

创建防篡改规则

URI

POST /v1/{project_id}/waf/policy/{policy_id}/antitamper

表 4-631 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id

请求参数

表 4-632 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

表 4-633 请求 Body 参数

参数	是否必选	参数类型	描述
hostname	是	String	防护网站，查询云模式防护域名列表（ListHost）接口获取防护域名，响应体中的的hostname字段
url	是	String	防篡改规则防护的url，需要填写标准的url格式，例如/admin/xxx或者/admin/,以"'"号结尾代表路径前缀
description	否	String	规则描述

响应参数

状态码： 200

表 4-634 响应 Body 参数

参数	参数类型	描述
id	String	规则id
policyid	String	策略id
timestamp	Long	时间戳(毫秒)
hostname	String	防篡改的域名
url	String	防篡改的url，
description	String	创建规则的描述
status	Integer	规则状态，0：关闭，1：开启

状态码： 400

表 4-635 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-636 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-637 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antitamper?enterprise_project_id=0

{
  "hostname" : "www.domain.com",
  "url" : "/login",
  "description" : ""
}
```

响应示例

状态码： 200

ok

```
{
  "description" : "",
  "hostname" : "www.domain.com",
  "id" : "0f59185b76c143f884d21cd0d88e6fa8",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "status" : 1,
  "timestamp" : 1656506256928,
  "url" : "/login"
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.9.3 根据 Id 查询防篡改防护规则

功能介绍

根据Id查询防篡改防护规则

URI

GET /v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}

表 4-638 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id
rule_id	是	String	antitamperRuleId

请求参数

表 4-639 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-640 响应 Body 参数

参数	参数类型	描述
id	String	规则id
policyid	String	策略id
timestamp	Long	时间戳(毫秒)
hostname	String	防篡改的域名
url	String	防篡改的url，
description	String	创建规则的描述
status	Integer	规则状态，0：关闭，1：开启

状态码： 400

表 4-641 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-642 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-643 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "description" : "",
  "hostname" : "www.domain.com",
  "id" : "0f59185b76c143f884d21cd0d88e6fa8",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "status" : 1,
  "timestamp" : 1656506256928,
  "url" : "/login"
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.9.4 删除防篡改防护规则

功能介绍

删除防篡改防护规则

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}

表 4-644 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id
rule_id	是	String	antitamperRuleId

请求参数

表 4-645 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-646 响应 Body 参数

参数	参数类型	描述
id	String	规则id
policyid	String	策略id
timestamp	Long	时间戳(毫秒)
hostname	String	防篡改的域名
url	String	防篡改的url，
description	String	创建规则的描述
status	Integer	规则状态，0：关闭，1：开启

状态码： 400

表 4-647 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-648 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-649 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码

参数	参数类型	描述
error_msg	String	错误信息

请求示例

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}?
enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "description" : "",
  "hostname" : "www.domain.com",
  "id" : "0f59185b76c143f884d21cd0d88e6fa8",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "status" : 1,
  "timestamp" : 1656506256928,
  "url" : "/login"
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.9.5 某个网页防篡改规则更新缓存

功能介绍

若防篡改的网页内容有修改，需要WAF重新缓存网页内容，可刷新某个网页防篡改规则中的缓存

URI

POST /v1/{project_id}/waf/policy/{policy_id}/antitamper/{antitamperid}/refresh

表 4-650 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id
antitamperid	是	String	网页防篡改规则id

请求参数

表 4-651 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	租户token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-652 响应 Body 参数

参数	参数类型	描述
id	String	规则id
policyid	String	策略id
timestamp	Long	时间戳(毫秒)
hostname	String	防篡改的域名
url	String	防篡改的url
description	String	创建规则的描述
status	Integer	规则状态，0：关闭，1：开启

状态码： 400

表 4-653 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-654 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-655 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antitamper/{antitamperid}/refresh?
enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "description" : "",
  "hostname" : "www.domain.com",
  "id" : "0f59185b76c143f884d21cd0d88e6fa8",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "status" : 0,
  "timestamp" : 1656506256928,
  "url" : "/login"
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.10 误报屏蔽规则管理

4.2.10.1 查询误报屏蔽规则列表

功能介绍

查询误报屏蔽规则列表

URI

GET /v1/{project_id}/waf/policy/{policy_id}/ignore

表 4-656 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id

表 4-657 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS)的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

参数	是否必选	参数类型	描述
page	否	Integer	分页查询时，返回第几页数据。范围0-100000，默认值为1，表示返回第1页数据。 缺省值：**1**
pagesize	否	Integer	分页查询时，每页包含多少条结果。范围1-100，默认值为10，表示每页包含10条结果。 缺省值：**10**

请求参数

表 4-658 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-659 响应 Body 参数

参数	参数类型	描述
total	Integer	该策略下误报屏蔽规则数量
items	Array of **IgnoreRuleBody** objects	误报屏蔽规则对象列表

表 4-660 IgnoreRuleBody

参数	参数类型	描述
id	String	规则id
policyid	String	策略id
timestamp	Long	创建规则的时间戳(毫秒)

参数	参数类型	描述
description	String	规则描述
status	Integer	规则状态，0：关闭，1：开启
url	String	误报规则屏蔽路径，仅在mode为0的状态下有该字段
rule	String	屏蔽的内置规则id（内置规则id通常可以在Web应用防火墙控制台的防护策略->策略名称->Web基础防护->防护规则中查询，也可以在防护事件的事件详情中查询内置规则id）
mode	Integer	版本号，0代表v1旧版本，1代表v2新版本；mode为0时，不存在conditions字段，存在url和url_logic字段；mode为1时，不存在url和url_logic字段，存在conditions字段
url_logic	String	匹配逻辑支持: • equal：等于 • not_equal：不等于 • contain：包含 • not_contain：不包含 • prefix：前缀为 • not_prefix：前缀不为 • suffix：后缀为 • not_suffix：后缀不为 • regular_match：正则匹配 • regular_not_match：正则不匹配
conditions	Array of **Condition** objects	条件列表
domains	Array of strings	防护域名或防护网站

表 4-661 Condition

参数	参数类型	描述
category	String	字段类型，可选值有ip、url、params、cookie、header

参数	参数类型	描述
contents	Array of strings	内容,数组长度限制为1，内容格式根据字段类型变化，例如，字段类型为ip时，contents内容格式需为ip地址或ip地址段；字段类型为url时，contents内容格式需为标准url格式；字段类型为params,cookie,header时，内容的格式不做限制
logic_operation	String	匹配逻辑，匹配逻辑根据字段类型变化，字段类型为ip时，匹配逻辑支持（equal：等于，not_equal：不等于）；字段类型为url、header、params、cookie时，匹配逻辑支持（equal：等于，not_equal：不等于，contain：包含，not_contain：不包含，prefix：前缀为，not_prefix：前缀不为，suffix：后缀为，not_suffix：后缀不为，regular_match：正则匹配，regular_not_match：正则不匹配）
check_all_indexes_logic	Integer	字段类型为url或ip时不存在check_all_indexes_logic字段，其它情况下（1：检查所有子字段，2：检查任意子字段，null：使用自定义子字段）
index	String	字段类型为ip且子字段为客户端ip时，不存在index参数；子字段类型为X-Forwarded-For时，值为x-forwarded-for，字段类型为params、header、cookie并且子字段为自定义时，index的值为自定义子字段

状态码： 400

表 4-662 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-663 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-664 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/ignore?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "total" : 1,
  "items" : [ {
    "id" : "c20f67b3e1c040c0b0d8866e568ee8bf",
    "policyid" : "a75e96d8284c4c4f98ada7d391e8342c",
    "timestamp" : 1656507126528,
    "description" : "",
    "status" : 1,
    "rule" : "webshell",
    "mode" : 1,
    "conditions" : [ {
      "category" : "url",
      "contents" : [ "attack" ],
      "logic_operation" : "contain"
    } ],
    "domain" : [ "test3.th.com" ]
  } ]
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.10.2 创建误报屏蔽规则

功能介绍

创建误报屏蔽规则

URI

POST /v1/{project_id}/waf/policy/{policy_id}/ignore

表 4-665 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id

表 4-666 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务(EPS)的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-667 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

表 4-668 请求 Body 参数

参数	是否必选	参数类型	描述
domain	是	Array of strings	防护域名或防护网站，数组长度为0时，代表规则对全部域名或防护网站生效
conditions	是	Array of **CreateCondition** objects	条件列表
mode	是	Integer	固定值为1,代表v2版本误报屏蔽规则，v1版本仅用于兼容旧版本，不支持创建
rule	是	String	屏蔽的内置规则id（内置规则id通常可以在Web应用防火墙控制台的防护策略->策略名称->Web基础防护->防护规则中查询，也可以在防护事件的事件详情中看到查询规则id）
description	否	String	屏蔽规则描述

表 4-669 CreateCondition

参数	是否必选	参数类型	描述
category	是	String	字段类型，可选值有ip、url、params、cookie、header
contents	是	Array of strings	内容,数组长度限制为1，内容格式根据字段类型变化。例如，字段类型为ip时，contents内容格式需为ip地址或ip地址段；字段类型为url时，contents内容格式需为标准url格式；字段类型为params,cookie,header时，内容的格式不做限制

参数	是否必选	参数类型	描述
logic_operation	是	String	匹配逻辑，匹配逻辑根据字段类型变化，字段类型为ip时，匹配逻辑支持（equal：等于，not_equal：不等于），字段类型为url、header、params、cookie时，匹配逻辑支持（equal：等于，not_equal：不等于，contain：包含，not_contain：不包含，prefix：前缀为，not_prefix：前缀不为，suffix：后缀为，not_suffix：后缀不为，regular_match：正则匹配，regular_not_match：正则不匹配）
check_all_indexes_logic	否	Integer	使用自定义子字段、字段类型为url或ip时不需要传check_all_indexes_logic参数，其它情况下（1：检查所有子字段，2：检查任意子字段）
index	否	String	字段类型为ip且子字段为客户端ip时，不需要传index参数；子字段类型为X-Forwarded-For时，值为x-forwarded-for；字段类型为params、header、cookie并且子字段为自定义时，index的值为自定义子字段

响应参数

状态码： 200

表 4-670 响应 Body 参数

参数	参数类型	描述
id	String	规则id
policyid	String	策略id
timestamp	Long	创建规则的时间戳
description	String	规则描述
status	Integer	规则状态，0：关闭，1：开启

参数	参数类型	描述
rule	String	屏蔽的内置规则id（内置规则id通常可以在Web应用防火墙控制台的防护策略->策略名称->Web基础防护->防护规则中查询，也可以从防护事件的事件详情中查询内置规则id）
mode	Integer	版本号固定值为1,代表v2版本误报屏蔽规则，v1版本仅支持兼容旧版本，不支持创建
conditions	Array of **Condition** objects	条件列表
domain	Array of strings	防护域名或防护网站

表 4-671 Condition

参数	参数类型	描述
category	String	字段类型，可选值有ip、url、params、cookie、header
contents	Array of strings	内容,数组长度限制为1，内容格式根据字段类型变化，例如，字段类型为ip时，contents内容格式需为ip地址或ip地址段；字段类型为url时，contents内容格式需为标准url格式；字段类型为params,cookie,header时，内容的格式不做限制
logic_operation	String	匹配逻辑，匹配逻辑根据字段类型变化，字段类型为ip时，匹配逻辑支持（equal：等于，not_equal：不等于）；字段类型为url、header、params、cookie时，匹配逻辑支持（equal：等于，not_equal：不等于，contain：包含，not_contain：不包含，prefix：前缀为，not_prefix：前缀不为，suffix：后缀为，not_suffix：后缀不为，regular_match：正则匹配，regular_not_match：正则不匹配）
check_all_indexes_logic	Integer	字段类型为url或ip时不存在check_all_indexes_logic字段，其它情况下（1：检查所有子字段，2：检查任意子字段，null：使用自定义子字段）
index	String	字段类型为ip且子字段为客户端ip时，不存在index参数；子字段类型为X-Forwarded-For时，值为x-forwarded-for，字段类型为params、header、cookie并且子字段为自定义时，index的值为自定义子字段

状态码： 400

表 4-672 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-673 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-674 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/ignore?enterprise_project_id=0

{
  "domain" : [ "test3.th.com" ],
  "conditions" : [ {
    "category" : "url",
    "logic_operation" : "contain",
    "contents" : [ "attack" ],
    "index" : null
  } ],
  "mode" : 1,
  "description" : "",
  "rule" : "webshell"
}
```

响应示例

状态码： 200

OK

```
{
  "id" : "c20f67b3e1c040c0b0d8866e568ee8bf",
  "policyid" : "a75e96d8284c4c4f98ada7d391e8342c",
```

```
  "timestamp" : 1656507126528,
  "description" : "",
  "status" : 1,
  "rule" : "webshell",
  "mode" : 1,
  "conditions" : [ {
    "category" : "url",
    "contents" : [ "attack" ],
    "logic_operation" : "contain"
  } ],
  "domain" : [ "test3.th.com" ]
}
```

状态码

状态码	描述
200	OK
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.10.3 查询误报屏蔽防护规则

功能介绍

查询误报屏蔽防护规则

URI

GET /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}

表 4-675 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id
rule_id	是	String	ignoreRuleId

表 4-676 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS)的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-677 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-678 响应 Body 参数

参数	参数类型	描述
id	String	规则id
policyid	String	策略id
timestamp	Long	创建规则的时间戳
description	String	规则描述
status	Integer	规则状态，0：关闭，1：开启
rule	String	屏蔽的内置规则id（内置规则id通常可以在Web应用防火墙控制台的防护策略->策略名称->Web基础防护->防护规则中查询，也可以从防护事件的事件详情中查询内置规则id）
mode	Integer	版本号固定值为1,代表v2版本误报屏蔽规则，v1版本仅支持兼容旧版本，不支持创建
conditions	Array of **Condition** objects	条件列表

参数	参数类型	描述
domain	Array of strings	防护域名或防护网站

表 4-679 Condition

参数	参数类型	描述
category	String	字段类型，可选值有ip、url、params、cookie、header
contents	Array of strings	内容,数组长度限制为1，内容格式根据字段类型变化，例如，字段类型为ip时，contents内容格式需为ip地址或ip地址段；字段类型为url时，contents内容格式需为标准url格式；字段类型为params,cookie,header时，内容的格式不做限制
logic_operation	String	匹配逻辑，匹配逻辑根据字段类型变化，字段类型为ip时，匹配逻辑支持（equal：等于，not_equal：不等于）；字段类型为url、header、params、cookie时，匹配逻辑支持（equal：等于，not_equal：不等于，contain：包含，not_contain：不包含，prefix：前缀为，not_prefix：前缀不为，suffix：后缀为，not_suffix：后缀不为，regular_match：正则匹配，regular_not_match：正则不匹配）
check_all_indexes_logic	Integer	字段类型为url或ip时不存在check_all_indexes_logic字段，其它情况下（1：检查所有子字段，2：检查任意子字段，null：使用自定义子字段）
index	String	字段类型为ip且子字段为客户端ip时，不存在index参数；子字段类型为X-Forwarded-For时，值为x-forwarded-for，字段类型为params、header、cookie并且子字段为自定义时，index的值为自定义子字段

状态码： 400

表 4-680 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-681 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-682 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "id" : "c20f67b3e1c040c0b0d8866e568ee8bf",
  "policyid" : "a75e96d8284c4c4f98ada7d391e8342c",
  "timestamp" : 1656507126528,
  "description" : "",
  "status" : 1,
  "rule" : "webshell",
  "mode" : 1,
  "conditions" : [ {
    "category" : "url",
    "contents" : [ "attack" ],
    "logic_operation" : "contain"
  } ],
  "domain" : [ "test3.th.com" ]
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.10.4 更新误报屏蔽防护规则

功能介绍

更新误报屏蔽防护规则

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}

表 4-683 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id
rule_id	是	String	ignoreRuleId

表 4-684 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS)的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-685 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

表 4-686 请求 Body 参数

参数	是否必选	参数类型	描述
domain	是	Array of strings	防护域名或防护网站，数组长度为0时，代表规则对全部域名或防护网站生效
conditions	是	Array of **CreateCondition** objects	条件列表
mode	是	Integer	固定值为1,代表v2版本误报屏蔽规则，v1版本仅用于兼容旧版本，不支持创建
rule	是	String	屏蔽的内置规则id（内置规则id通常可以在Web应用防火墙控制台的防护策略->策略名称->Web基础防护->防护规则中查询，也可以在防护事件的事件详情中看到查询规则id）
description	否	String	屏蔽规则描述

表 4-687 CreateCondition

参数	是否必选	参数类型	描述
category	是	String	字段类型，可选值有ip、url、params、cookie、header
contents	是	Array of strings	内容,数组长度限制为1，内容格式根据字段类型变化。例如，字段类型为ip时，contents内容格式需为ip地址或ip地址段；字段类型为url时，contents内容格式需为标准url格式；字段类型为params,cookie,header时，内容的格式不做限制

参数	是否必选	参数类型	描述
logic_operation	是	String	匹配逻辑，匹配逻辑根据字段类型变化，字段类型为ip时，匹配逻辑支持（equal：等于，not_equal：不等于），字段类型为url、header、params、cookie时，匹配逻辑支持（equal：等于，not_equal：不等于，contain：包含，not_contain：不包含，prefix：前缀为，not_prefix：前缀不为，suffix：后缀为，not_suffix：后缀不为，regular_match：正则匹配，regular_not_match：正则不匹配）
check_all_indexes_logic	否	Integer	使用自定义子字段、字段类型为url或ip时不需要传check_all_indexes_logic参数，其它情况下（1：检查所有子字段，2：检查任意子字段）
index	否	String	字段类型为ip且子字段为客户端ip时，不需要传index参数；子字段类型为X-Forwarded-For时，值为x-forwarded-for；字段类型为params、header、cookie并且子字段为自定义时，index的值为自定义子字段

响应参数

状态码： 200

表 4-688 响应 Body 参数

参数	参数类型	描述
id	String	规则id
policyid	String	策略id
timestamp	Long	创建规则的时间戳
description	String	规则描述
status	Integer	规则状态，0：关闭，1：开启

参数	参数类型	描述
rule	String	屏蔽的内置规则id（内置规则id通常可以在Web应用防火墙控制台的防护策略->策略名称->Web基础防护->防护规则中查询，也可以从防护事件的事件详情中查询内置规则id）
mode	Integer	版本号固定值为1,代表v2版本误报屏蔽规则，v1版本仅支持兼容旧版本，不支持创建
conditions	Array of **Condition** objects	条件列表
domain	Array of strings	防护域名或防护网站

表 4-689 Condition

参数	参数类型	描述
category	String	字段类型，可选值有ip、url、params、cookie、header
contents	Array of strings	内容,数组长度限制为1，内容格式根据字段类型变化，例如，字段类型为ip时，contents内容格式需为ip地址或ip地址段；字段类型为url时，contents内容格式需为标准url格式；字段类型为params,cookie,header时，内容的格式不做限制
logic_operation	String	匹配逻辑，匹配逻辑根据字段类型变化，字段类型为ip时，匹配逻辑支持（equal：等于，not_equal：不等于）；字段类型为url、header、params、cookie时，匹配逻辑支持（equal：等于，not_equal：不等于，contain：包含，not_contain：不包含，prefix：前缀为，not_prefix：前缀不为，suffix：后缀为，not_suffix：后缀不为，regular_match：正则匹配，regular_not_match：正则不匹配）
check_all_indexes_logic	Integer	字段类型为url或ip时不存在check_all_indexes_logic字段，其它情况下（1：检查所有子字段，2：检查任意子字段，null：使用自定义子字段）
index	String	字段类型为ip且子字段为客户端ip时，不存在index参数；子字段类型为X-Forwarded-For时，值为x-forwarded-for，字段类型为params、header、cookie并且子字段为自定义时，index的值为自定义子字段

状态码： 400

表 4-690 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-691 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-692 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/ignore?enterprise_project_id=0

{
  "domain" : [ "test3.th.com" ],
  "conditions" : [ {
    "category" : "url",
    "logic_operation" : "contain",
    "contents" : [ "attack" ],
    "index" : null
  } ],
  "mode" : 1,
  "description" : "",
  "rule" : "vuln"
}
```

响应示例

状态码： 200

ok

```
{
  "id" : "c20f67b3e1c040c0b0d8866e568ee8bf",
  "policyid" : "a75e96d8284c4c4f98ada7d391e8342c",
```

```
  "timestamp" : 1656507126528,
  "description" : "",
  "status" : 1,
  "rule" : "vuln",
  "mode" : 1,
  "conditions" : [ {
    "category" : "url",
    "contents" : [ "attack" ],
    "logic_operation" : "contain"
  } ],
  "domain" : [ "test3.th.com" ]
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.10.5 删除误报屏蔽防护规则

功能介绍

删除误报屏蔽防护规则

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}

表 4-693 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
policy_id	是	String	防护策略id，您可以通过调用查询防护策略列表（ListPolicy）获取策略id
rule_id	是	String	ignoreRuleId

表 4-694 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS)的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-695 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	auth token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 400

表 4-696 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-697 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-698 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/ignore?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "id" : "c20f67b3e1c040c0b0d8866e568ee8bf",
  "policyid" : "a75e96d8284c4c4f98ada7d391e8342c",
  "timestamp" : 1656507126528,
  "description" : "",
  "status" : 1,
  "rule" : "vuln",
  "mode" : 1,
  "conditions" : [ {
    "category" : "url",
    "contents" : [ "attack" ],
    "logic_operation" : "contain"
  } ],
  "domain" : [ "test3.th.com" ]
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.11 安全总览

4.2.11.1 查询安全总览请求与攻击数量

功能介绍

查询安全总览请求与攻击数量。。需要注意的是，安全总览相关的接口，暂时不能支持任意时间的查询。只能支持 console上显示的 昨天，今天，3天，7天和30天 数据查询。

URI

GET /v1/{project_id}/waf/overviews/statistics

表 4-699 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id

表 4-700 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS)的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id
from	是	Long	起始时间(13位时间戳)，需要和to同时使用
to	是	Long	结束时间(13位时间戳),需要和from同时使用
hosts	否	String	域名id列表，通过查询云模式防护域名列表（ListHost）获取域名id或者通过独享模式域名列表（ListPremiumHost）获取域名id。默认不传，查询该项目下所有防护域名的top业务异常统计信息。当有需要传多个域名时，传参参考请求示例。
instances	否	String	要查询引擎实例列表

请求参数

表 4-701 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-702 响应 Body 参数

参数	参数类型	描述
[数组元素]	Array of **CountItem** objects	安全统计数据

表 4-703 CountItem

参数	参数类型	描述
key	String	类型
num	Integer	数量

状态码： 400

表 4-704 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-705 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 403

表 4-706 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-707 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/overviews/statistics?
enterprise_project_id=0&from=1650470400196&to=1650522936196&hosts=1bac09440a814aa98ed08302c580a48b&hosts=5a532f83a2fb476ba51ca1de7b1ebc43
```

响应示例

状态码： 200

ok

```
[ {
  "key" : "ACCESS",
  "num" : 1190
}, {
  "key" : "PRECISE",
  "num" : 0
}, {
  "key" : "CRAWLER",
  "num" : 10
}, {
  "key" : "WEB_ATTACK",
  "num" : 22
}, {
  "key" : "CC",
```

```
  "num" : 0
}, {
  "key" : "ATTACK",
  "num" : 32
} ]
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
403	资源配额不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.11.2 查询安全总览分类统计 TOP 信息

功能介绍

查询安全总览分类统计TOP信息，包含受攻击域名 、攻击源ip、受攻击URL、攻击来源区域、攻击事件分布。需要注意的是，安全总览相关的接口，暂时不能支持任意时间的查询。只能支持 console上显示的 昨天，今天，3天，7天和30天 数据查询。

URI

GET /v1/{project_id}/waf/overviews/classification

表 4-708 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id

表 4-709 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

参数	是否必选	参数类型	描述
from	是	Long	起始时间（13位毫秒时间戳），需要和to同时使用
to	是	Long	结束时间（13位毫秒时间戳），需要和from同时使用
top	否	Integer	要查询的前几的结果，最大值为10，默认值为5。
hosts	否	String	域名id列表，通过查询云模式防护域名列表（ListHost）获取域名id或者通过独享模式域名列表（ListPremiumHost）获取域名id。默认不传，查询该项目下所有防护域名的top业务异常统计信息。当有需要传多个域名时，传参参考请求示例。
instances	否	String	要查询引擎实例列表（仅独享或者ELB实例化模式涉及）

请求参数

表 4-710 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	租户 token
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-711 响应 Body 参数

参数	参数类型	描述
domain	**DomainClassificationItem** object	受攻击域名
attack_type	**AttackTypeClassificationItem** object	攻击事件分布

参数	参数类型	描述
ip	**IpClassificationItem** object	攻击源ip
url	**UrlClassificationItem** object	攻击url
geo	**GeoClassificationItem** object	攻击来源区域

表 4-712 DomainClassificationItem

参数	参数类型	描述
total	Integer	DomainItem的总数量
items	Array of **DomainItem** objects	DomainItem详细信息

表 4-713 DomainItem

参数	参数类型	描述
key	String	域名
num	Integer	数量
web_tag	String	网站名称

表 4-714 AttackTypeClassificationItem

参数	参数类型	描述
total	Integer	AttackTypeItem的总数量
items	Array of **AttackTypeItem** objects	AttackTypeItem详细信息

表 4-715 AttackTypeItem

参数	参数类型	描述
key	String	攻击事件类型

参数	参数类型	描述
num	Integer	数量

表 4-716 IpClassificationItem

参数	参数类型	描述
total	Integer	IpItem的总数量
items	Array of **IpItem** objects	IpItem详细信息

表 4-717 IpItem

参数	参数类型	描述
key	String	ip地址
num	Integer	数量

表 4-718 UrlClassificationItem

参数	参数类型	描述
total	Integer	UrlItem的总数量
items	Array of **UrlItem** objects	UrlItem详细信息

表 4-719 UrlItem

参数	参数类型	描述
key	String	路径
num	Integer	数量
host	String	域名

表 4-720 GeoClassificationItem

参数	参数类型	描述
total	Integer	GeoItem的总数量
items	Array of **GeoItem** objects	GeoItem详细信息

表 4-721 GeoItem

参数	参数类型	描述
key	String	攻击来源区域
num	Integer	数量

状态码： 400

表 4-722 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-723 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-724 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/overviews/classification?
enterprise_project_id=0&from=1652889600354&to=1655435681354&top=10&hosts=1bac09440a814aa98ed0
8302c580a48b&hosts=5a532f83a2fb476ba51ca1de7b1ebc43
```

响应示例

状态码： 200

请求成功

```
{
  "attack_type" : {
    "total" : 1,
    "items" : [ {
      "key" : "custom_custom",
      "num" : 2
    } ]
  },
  "domain" : {
    "total" : 2,
    "items" : [ {
      "key" : "www.whitelist.com",
      "num" : 2,
      "web_tag" : "www.whitelist.com"
    }, {
      "key" : "zbx002.apayaduo.cn",
      "num" : 2,
      "web_tag" : ""
    } ]
  },
  "geo" : {
    "total" : 1,
    "items" : [ {
      "key" : "10.142.4.15",
      "num" : 2
    } ]
  },
  "ip" : {
    "total" : 1,
    "items" : [ {
      "key" : "10.142.4.15",
      "num" : 2
    } ]
  },
  "url" : {
    "total" : 1,
    "items" : [ {
      "key" : "/attack",
      "num" : 2,
      "host" : "www.whitelist.com"
    } ]
  }
}
```

状态码

状态码	描述
200	请求成功
400	请求失败
401	token权限不足

状态码	描述
500	服务器内部错误

错误码

请参见**错误码**。

4.2.12 防护事件管理

4.2.12.1 查询攻击事件列表

功能介绍

查询攻击事件列表，该API暂时不支持查询全部防护事件，pagesize参数不可设为-1，由于性能原因，数据量越大消耗的内存越大，后端最多限制查询10000条数据，例如：自定义时间段内的数据超过了10000条，就无法查出page为101，pagesize为100之后的数据，需要调整时间区间，再进行查询

URI

GET /v1/{project_id}/waf/event

表 4-725 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id

表 4-726 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS)的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id
recent	否	String	查询日志的时间范围,(不能和from、to同时使用) 枚举值： • **yesterday** • **today** • **3days** • **1week** • **1month**

参数	是否必选	参数类型	描述
attacks	否	Array	攻击类型: ● vuln：其它攻击类型 ● sqli： sql注入攻击 ● lfi： 本地文件包含 ● cmdi：命令注入攻击 ● xss：XSS攻击 ● robot：恶意爬虫 ● rfi：远程文件包含 ● custom_custom：精准防护 ● cc: cc攻击 ● webshell：网站木马 ● custom_whiteblackip：黑白名单拦截 ● custom_geoip：地理访问控制拦截 ● antitamper：防篡改 ● anticrawler：反爬虫 ● leakage：网站信息防泄漏 ● illegal：非法请求
from	否	Long	起始时间(13位时间戳)，需要和to同时使用，不能和recent参数同时使用
to	否	Long	结束时间(13位时间戳)，需要和from同时使用，不能和recent参数同时使用
hosts	否	Array	域名id，从获取防护网站列表（ListHost）接口获取域名id
page	否	Integer	分页查询时，返回第几页数据。范围0-100000，默认值为1，表示返回第1页数据。
pagesize	否	Integer	分页查询时，每页包含多少条结果。范围1-100，默认值为10，表示每页包含10条结果。

请求参数

表 4-727 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-728 响应 Body 参数

参数	参数类型	描述
total	Integer	攻击事件数量
items	Array of **ListEventItems** objects	攻击事件详情

表 4-729 ListEventItems

参数	参数类型	描述
id	String	事件id
time	Long	次数
policyid	String	策略id
sip	String	源ip
host	String	域名
url	String	攻击的url链接

参数	参数类型	描述
attack	String	攻击类型: ● vuln：其它攻击类型 ● sqli： sql注入攻击 ● lfi： 本地文件包含 ● cmdi：命令注入攻击 ● xss：XSS攻击 ● robot：恶意爬虫 ● rfi：远程文件包含 ● custom_custom：精准防护 ● webshell：网站木马 ● custom_whiteblackip：黑白名单拦截 ● custom_geoip：地理访问控制拦截 ● antitamper：防篡改 ● anticrawler：反爬虫 ● leakage：网站信息防泄漏 ● illegal：非法请求
rule	String	命中的规则id
payload	String	命中的载荷
action	String	防护动作
request_line	String	请求方法和路径
headers	Object	http请求header
cookie	String	请求cookie
status	String	响应码状态
process_time	Integer	处理时长
region	String	地理位置
host_id	String	域名id
response_time	Long	响应时长
response_size	Integer	响应体大小
response_body	String	响应体
request_body	String	请求体

状态码： 400

表 4-730 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-731 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-732 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/event?
enterprise_project_id=0&page=1&pagesize=10&recent=today
```

响应示例

状态码： 200

ok

```
{
  "total" : 1,
  "items" : [ {
    "id" : "04-0000-0000-0000-21120220421152601-2f7a5ceb",
    "time" : 1650525961000,
    "policyid" : "25f1d179896e4e3d87ceac0598f48d00",
    "host" : "x.x.x.x:xxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "url" : "/osclass/oc-admin/index.php",
    "attack" : "lfi",
    "rule" : "040002",
    "payload" : " file=../../../../../../../../../etc/passwd",
    "payload_location" : "params",
    "sip" : "x.x.x.x",
    "action" : "block",
    "request_line" : "GET /osclass/oc-admin/index.php?
```

```
page=appearance&action=render&file=../../../../../../../../../etc/passwd",
    "headers" : {
      "accept-language" : "en",
      "ls-id" : "xxxxx-xxxxx-xxxx-xxxx-9c302cb7c54a",
      "host" : "x.x.x.x",
      "lb-id" : "2f5f15ce-08f4-4df0-9899-ec0cc1fcdc52",
      "accept-encoding" : "gzip",
      "accept" : "*/*",
      "user-agent" : "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
35.0.2309.372 Safari/537.36"
    },
    "cookie" : "HWWAFSESID=2a1d773f9199d40a53; HWWAFSESTIME=1650525961805",
    "status" : "418",
    "host_id" : "6fbe595e7b874dbbb1505da3e8579b54",
    "response_time" : 0,
    "response_size" : 3318,
    "response_body" : "",
    "process_time" : 2,
    "request_body" : "{}"
  } ]
}
```


状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.12.2 查询攻击事件详情

功能介绍

查询攻击事件详情

URI

GET /v1/{project_id}/waf/event/{eventid}

表 4-733 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
eventid	是	String	防护事件id,通过调用查询攻击事件列表(ListEvent)接口获取防护事件id

表 4-734 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS)的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-735 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-736 响应 Body 参数

参数	参数类型	描述
total	Integer	攻击事件数量
items	Array of **ShowEventItems** objects	攻击事件详情

表 4-737 ShowEventItems

参数	参数类型	描述
time	Long	攻击发生时的时间戳（毫秒）
policyid	String	策略id

参数	参数类型	描述
sip	String	源ip
host	String	域名
url	String	攻击的url链接
attack	String	攻击类型
rule	String	命中的规则id
action	String	防护动作
cookie	String	攻击请求的cookie
headers	Object	攻击请求的headers
host_id	String	被攻击的域名id
id	String	防护事件id
payload	String	恶意负载
payload_location	String	恶意负载位置
region	String	源ip地理位置
process_time	Integer	处理时长
request_line	String	攻击请求的请求行
response_size	Integer	返回大小（字节）
response_time	Long	响应时间（毫秒）
status	String	响应码
request_body	String	请求体

状态码： 400

表 4-738 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-739 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-740 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/event{event_id}?enterprise_project_id=0
```

响应示例

状态码： 200

ok

```
{
  "total" : 1,
  "items" : [ {
    "id" : "09-0000-0000-0000-12120220421093806-a60a6166",
    "time" : 1650505086000,
    "policyid" : "173ed802272a4b0798049d7edffeff03",
    "host" : "x.x.x.x:xxxxxx-xxx-xxx-xxx-xxxxxxxxx",
    "url" : "/mobile/DBconfigReader.jsp",
    "attack" : "vuln",
    "rule" : "091004",
    "payload" : " /mobile/dbconfigreader.jsp",
    "payload_location" : "uri",
    "sip" : "x.x.x.x",
    "action" : "block",
    "request_line" : "GET /mobile/DBconfigReader.jsp",
    "headers" : {
      "ls-id" : "c0d957e6-26a8-4f2e-8216-7fc9332a250f",
      "host" : "x.x.x.x:81",
      "lb-id" : "68d3c435-2607-45e0-a5e2-38980544dd45",
      "accept-encoding" : "gzip",
      "user-agent" : "Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 CSIRTx/2022"
    },
    "cookie" : "HWWAFSESID=2a0bf76a111c93926d; HWWAFSESTIME=1650505086260",
    "status" : "418",
    "region" : "Reserved IP",
    "host_id" : "e093a352fd3a4ddd994c585e2e1dda59",
    "response_time" : 0,
    "response_size" : 3318,
    "response_body" : "",
    "process_time" : 0,
    "request_body" : "{}"
```

```
  }]
}
```

状态码

状态码	描述
200	ok
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.13 证书管理

4.2.13.1 查询证书列表

功能介绍

查询证书列表

URI

GET /v1/{project_id}/waf/certificate

表 4-741 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id

表 4-742 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

参数	是否必选	参数类型	描述
page	否	Integer	分页查询时，返回第几页数据。范围0-100000，默认值为1，表示返回第1页数据。 缺省值：**1**
pagesize	否	Integer	分页查询时，每页包含多少条结果。范围1-100，默认值为10，表示每页包含10条结果。 缺省值：**10**
name	否	String	证书名称
host	否	Boolean	是否获取证书关联的域名，默认为false -true:获取已关联域名的证书 -false:获取未关联域名的证书 缺省值：**false**
exp_status	否	Integer	证书过期状态 ● 0：未过期 ● 1：已过期 ● 2：即将过期（证书将在一个月内过期）

请求参数

表 4-743 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-744 响应 Body 参数

参数	参数类型	描述
items	Array of **CertificateBody** objects	证书列表
total	Integer	证书总数

表 4-745 CertificateBody

参数	参数类型	描述
id	String	证书id
name	String	证书名
content	String	证书文件，PEM编码
key	String	证书私钥，PEM编码
expire_time	Long	证书过期时间戳
exp_status	Integer	证书过期状态，0-未过期，1-已过期，2-即将过期（一个月内即将过期）
timestamp	Long	证书上传时间戳
bind_host	Array of **BindHost** objects	证书关联的域名信息

表 4-746 BindHost

参数	参数类型	描述
id	String	防护域名ID
hostname	String	防护域名
waf_type	String	防护域名对应模式：cloud（云模式）/premium（独享模式）
mode	String	仅独享模式涉及特殊域名模式

状态码： 400

表 4-747 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-748 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-749 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/certificate?enterprise_project_id=0
```

响应示例

状态码： 200

OK

```
{
  "total" : 1,
  "items" : [ {
    "id" : "dc443ca4f29c4f7e8d4adaf485be317b",
    "name" : "demo",
    "timestamp" : 1643181401751,
    "expire_time" : 1650794100000,
    "bind_host" : [ ],
    "exp_status" : 2
  } ]
}
```

状态码

状态码	描述
200	OK
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.13.2 创建证书

功能介绍

创建证书

URI

POST /v1/{project_id}/waf/certificate

表 4-750 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id

表 4-751 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-752 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

表 4-753 请求 Body 参数

参数	是否必选	参数类型	描述
name	是	String	证书名称，证书名称只能由数字、字母、中划线、下划线和英文句点组成，长度不能超过64位字符
content	是	String	证书文件，仅支持PEM格式的证书和私钥文件，且文件中的换行符应以\n替换
key	是	String	证书私钥，仅支持PEM格式的证书和私钥文件，且文件中的换行符应以\n替换

响应参数

状态码： 200

表 4-754 响应 Body 参数

参数	参数类型	描述
id	String	证书ID
name	String	证书名
content	String	证书文件，PEM编码
key	String	证书私钥，PEM编码
expire_time	Long	证书过期时间戳

参数	参数类型	描述
exp_status	Integer	证书过期状态，0-未过期，1-已过期，2-即将过期
timestamp	Long	证书上传时间戳
bind_host	Array of **BindHost** objects	证书关联的域名信息

表 4-755 BindHost

参数	参数类型	描述
id	String	防护域名ID
hostname	String	防护域名
waf_type	String	防护域名对应模式：cloud（云模式）/premium（独享模式）
mode	String	仅独享模式涉及特殊域名模式

状态码： 400

表 4-756 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-757 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-758 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
POST https://{Endpoint}/v1/{project_id}/waf/certificate?enterprise_project_id=0

{
  "name" : "demo",
  "content" : "-----BEGIN CERTIFICATE-----
MIIDyzCCArOgAwIBAgIJAN5U0Z4Bh5ccMA0GCSqGSIb3DQEBCwUAMHwxCzAJBgNV
BAYTAlpIMRIwEAYDVQQIDAlHVUFOR0RPTkcxETAPBgNVBAcMCERPTkdHVUFOMQ0w
CwYDVQQKDARERUtFMQswCQYDVQQLDAJESzELMAkGA1UEAwwCT0QxHTAbBgkqhkiG
9w0BCQEWDk8IZC5odWF3ZWkuY29tMB4XDTIxMTExNTA4MTk0MVoXDTIyMTExNTA4
MTk0MVowfDELMAkGA1UEBhMCWkgxEjAQBgNVBAgMCUdVQU5HRE9ORzERMA8GA1UE
BwwIRE9OR0dVQU4xDTALBgNVBAoMBERFS0UxCzAJBgNVBAsMAkRLMQswCQYDVQQD
DAJPRDEdMBsGCSqGSIb3DQEJARYOTwhkLmh1YXdlaS5jb20wggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDcoLFK62//r0RHFyweYBj97S4NsJ8Qj0RG+Y02
OgwhQmRiNNjubJwP8Nqqyd86zr+fsSQxKBaBCosn1PcN2Pj2vPJD6NEk4I6VdOWr /
kFYMlOcimhSfW4wt6VakniOKIYGrCxxvQe1X2OyBxT+ocTLRgEIB8ZbvJyPNseg
feLEUuPYRpQ5kXLgJH2/3NwZFOgBHVv/b07l4fR+sWJMnIA2yIjSBQ0DEAOSusXo FQ/
WRbBRH7DrQmxGiXsq4VELEr9Nnc/Kywq+9pYi8L+mKeRL+lcMMbXC/3k6OfMB
tVTiwcmS1Mkr3iG03i8u6H7RSvRwyBz9G9sE+tmJZTPH6lYtAgMBAAGjUDBOMB0G
A1UdDgQWBBQprUUFXW+gIkpzXdrYlsWjfSahWjAfBgNVHSMEGDAWgBQprUUFXW+g
IkpzXdrYlsWjfSahWjAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQA2
603KozsQoIKeLvqDJlcAXwWRfNW8SvlaSJAulhHgneMt9bQgIL+3PJWA/iMniOhU o/
kVwkiUIcxw4t7RwP0hVms0OZw59MuqKd3oCSWkYO4vEHs3t40JDWnGDnmQ4sol
RkOWJwL4w8tnPe3qY9JSupjlsu6Y1hlvKtEfN2vEKFnsuMhidkUpUAJWodHhWBQH
wgIDo4/6yTnWZNGK8JDal86Dm5IchXea1EoYBJsHxiJb7HeWQlkre+MCYi1RHOin 4mIXTr0oT4/jWlgklSz6/
ZhGRq+7W7tIl7cvzCe+4XsVZIenAcYoNd/WLfo91PD4 yAsRXrOjW1so1Bj0BkDz -----END CERTIFICATE-----",
  "key" : "-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQDcoLFK62//r0RH FyweYBj97S4NsJ8Qj0RG
+Y02OgwhQmRiNNjubJwP8Nqqyd86zr+fsSQxKBaBCosn 1PcN2Pj2vPJD6NEk4I6VdOWr/
kFYMlOcimhSfW4wt6VakniOKIYGrCxxvQe1X2Oy BxT
+ocTLRgEIB8ZbvJyPNsegfeLEUuPYRpQ5kXLgJH2/3NwZFOgBHVv/b07l4fR+ sWJMnIA2yIjSBQ0DEAOSusXoFQ/
WRbBRH7DrQmxGiXsq4VELEr9Nnc/Kywq+9pYi 8L+mKeRL+lcMMbXC/
3k6OfMBtVTiwcmS1Mkr3iG03i8u6H7RSvRwyBz9G9sE+tmJ ZTPH6lYtAgMBAAECggEBAL+xZxm/QoqXT
+2stoqV2GEYaMFASpRqxlocjZMmEE/9 jZa+cBWIjHhVPsjRqYFBDcHEebu0JwlrjcjIAvgnIvnO5XgXm1A9Q
+WbscokmcX1 xCvpHgc+MDVn+uWdCd4KW5kEk4EnSsFN5iNSf+1VxNURN+gwSSp/0E+muwA5IISO G6HQ
+p6qs52JAitX5t/7ruKoHYXJxBnf7TUs7768qrh++KPKpPlq044qoYlcGO1n 4urPBHuNLy04GgGw
+vkaqjqOvZrNLVOMMaFWBxsDWBehgSSBQTj+f3NCxneGYtt8 3SCTZQI5nIkb+r/
M455EwKTSXuEsNHoIwx7L6GEPbQECgYEA8IxgK2fYykloICoh
TFJaRAvyjyKa2+Aza4qT9SGY9Y30VPClPjBB1vUu5M9KrFufzlv06nGEcHmpEwOe
8vbRu7nLAQTGYFi8VK63q8w6FlFdAyCG6Sx+BWCfWxJzXsZLAJTfklwi8HsOSlqh
6QNv0xbE2fLjXKf8MHvtrufip40CgYEA6sy87eDrkVgtq4ythAik3i1C5Z3v0fvx mTblG52Z21OyocNq3Tf/
b1ZwoIc1ik6cyBzY6z1bIrbSzArCqm0sb2iD+kJL81O0 /qqdXjBxZUkKiVAMNNp7xJGZHHFKWUxT2+UX/
tlyx4tT4dzrFIkdDXkcMmqfsRxd 1NEVaAaT8SECgYAoU7BPtpIun43YTpfUfr3pSIN6oZeKoxSbw9i4MNC
+4fSDRPC+ 80ImcmZRL7taF+Y7p0jxAOTuIkdJC8NbAiv5J9WzrwQ+5MF2BPB/2bYnRa6tNofH kZDy/
9bXYsl6qw2p5Ety8wVcgZTMvFMGiG/32IpZ65FYWEU8L5qSRwfFhQKBgQC9 ihjZTj/bTHtRiHZppzCvyYm/Igd
+Uwtsy0uXR1n0G1SQENgrTBD/J6AzdfJae6tE P0U8YIM5Oqxf2i/as9ay+IPRecMl4eSxz7jJWAGx6Yx/3AZ
+hAB1ZbNbqniCLYNk d0MvjwmA25ATO+ro4OZ7AdEpQbk3l9aG/WFyYBz9AQKBgQCucFPA1l5eslL8196V
WMr2Qo0tqzl7CGSoWQk2Sa2HZtZdfofXAaaqo+zvJ6RPHtJh0jgJtx536DVV3egI
37YrdQyJbCPZXQ3SPgqWCorUnXBwq/nxS06uwu6JBxUFc57ijmMU4fWYNrvkkmWb 7keAg/
r5Uy1joMAvBN1I6lB8pg== -----END PRIVATE KEY-----"
}
```

响应示例

状态码： 200

OK


```
{
  "id" : "6e2be127b79f4a418414952ad5d8c59f",
  "name" : "certificatename94319",
  "content" : "-----BEGIN CERTIFICATE-----\nMIIB
+TCCAaOgAwIBAgIUJP9I8OupQ77w0bGL2yWOQXreM4kwDQYJKoZIhvcNAQELBQAwUTELMAkGA1UEBhMC
QVUxEzARBgNVBAgMClNvbWUtU3RhdGUxDzANBgNVBAoMBkh1YXdlaTEcMBoGA1UEAwwTd2FmLmh1YXdl
aWNsb3VkLmNvbTAeFw0yMDA3MDkwNTQ2MDRaFw0yMDA4MDgwNTQ2MDRaMFExCzAJBgNVBAYTAkFV
MRMwEQYDVQQIDApTb21lLVN0YXRlMQ8wDQYDVQQKDAZIdWF3ZWkxHDAaBgNVBAMME3dhZi5odWF3Z
WljbG91ZC5jb20wXDANBgkqhkiG9w0BAQEFAANLADBIAkEA0UEbMzbvgOJTKrKcDUw9xjFqxM7BaQFM3SLs
QlmD5hkzygyL1ra
+cWajPJlTCxz9Ph6qldna2+OrIuTdvCcpjwIDAQABo1MwUTAdBgNVHQ4EFgQUE7ZQNcgl3lmryx1s5gy9mnC1rs
YwHwYDVR0jBBgwFoAUE7ZQNcgl3lmryx1s5gy9mnC1rsYwDwYDVR0TAQH/BAUwAwEB/
zANBgkqhkiG9w0BAQsFAANBAM5wGi88jYWLgOnGbae5hH3I9lMBKxGqv17Cbm1tjWuUogVINz86lqvCpuhzLv
D/vzJAqPIuDwqM8uvzjgRfZs8=\n-----END CERTIFICATE-----",
  "key" : "-----BEGIN RSA PRIVATE KEY-----
\nMIIBOQIBAAJBANFBGzM274DiUyqynA1MPcYxasTOwWkBTN0i7EJZg+YZM8oMi9a2vnFmozyZUwsc/
T4eqpXZ2tvjqyLk3bwnKY8CAwEAAQJBAI7LMPaH/HQk/b/bVmY0qsr
+me9nb9BqFLuqwzKbx0hSmWPOWFsd3rOFlSopyHqgYtAsPfvPumEdGbdnCyU8zAECIQD71768K1ejb
+ei2lqZqHaczqdUNQxMh54yot9F2yVWjwIhANS1Y1Jv89WEU/ZvvMS9a4638Msv2c4GGp08RtXNYn0BAiA0H4b
+cwoEbZjHf+HYg6Fo+uxu5TvSaw8287a6Qo0LyQIfVZSlYYWplT6oiX5rdLzBiap4N0gJWdsa2ihmV59LAQIgK8N
+j1daq63b0bJ9k4HruhQtpgxI6U9nFBemH4zTRYM=\n-----END RSA PRIVATE KEY-----",
  "timestamp" : 1650595334578,
  "expire_time" : 1596865564000
}
```


状态码

状态码	描述
200	OK
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.13.3 查询证书

功能介绍

查询证书

URI

GET /v1/{project_id}/waf/certificate/{certificate_id}

表 4-759 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
certificate_id	是	String	https证书id，您可以通过调用查询证书列表（ListCertificates）接口获取证书id

表 4-760 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-761 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-762 响应 Body 参数

参数	参数类型	描述
id	String	证书ID
name	String	证书名
content	String	证书文件，PEM编码

参数	参数类型	描述
key	String	证书私钥，PEM编码
expire_time	Long	证书过期时间戳
exp_status	Integer	证书过期状态，0-未过期，1-已过期，2-即将过期
timestamp	Long	证书上传时间戳
bind_host	Array of **BindHost** objects	证书关联的域名信息

表 4-763 BindHost

参数	参数类型	描述
id	String	防护域名ID
hostname	String	防护域名
waf_type	String	防护域名对应模式：cloud（云模式）/premium（独享模式）
mode	String	仅独享模式涉及特殊域名模式

状态码： 400

表 4-764 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-765 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-766 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/certificate/{certificate_id}?enterprise_project_id=0
```

响应示例

状态码： 200

OK

```
{
  "id" : "6e2be127b79f4a418414952ad5d8c59f",
  "name" : "certificatename94319",
  "content" : "-----BEGIN CERTIFICATE-----\nMIIB
+TCCAaOgAwIBAgIUJP9I8OupQ77w0bGL2yWOQXreM4kwDQYJKoZIhvcNAQELBQAwUTELMAkGA1UEBhMC
QVUxEzARBgNVBAgMClNvbWUtU3RhdGUxDzANBgNVBAoMBkh1YXdlaTEcMBoGA1UEAwwTd2FmLmh1YXdl
aWNsb3VkLmNvbTAeFw0yMDA3MDkwNTQ2MDRaFw0yMDA4MDgwNTQ2MDRaMFExCzAJBgNVBAYTAkFV
MRMwEQYDVQQIDApTb21lLVN0YXRlMQ8wDQYDVQQKDAZIdWF3ZWkxHDAaBgNVBAMME3dhZi5odWF3Z
WljbG91ZC5jb20wXDANBgkqhkiG9w0BAQEFAANLADBIAkEA0UEbMzbvgOJTKrKcDUw9xjFqxM7BaQFM3SLs
QlmD5hkzygyL1ra
+cWajPJlTCxz9Ph6qldna2+OrIuTdvCcpjwIDAQABo1MwUTAdBgNVHQ4EFgQUE7ZQNcgl3lmryx1s5gy9mnC1rs
YwHwYDVR0jBBgwFoAUE7ZQNcgl3lmryx1s5gy9mnC1rsYwDwYDVR0TAQH/BAUwAwEB/
zANBgkqhkiG9w0BAQsFAANBAM5wGi88jYWLgOnGbae5hH3I9lMBKxGqv17Cbm1tjWuUogVINz86lqvCpuhzLv
D/vzJAqPIuDwqM8uvzjgRfZs8=\n-----END CERTIFICATE-----",
  "key" : "-----BEGIN RSA PRIVATE KEY-----
\nMIIBOQIBAAJBANFBGzM274DiUyqynA1MPcYxasTOwWkBTN0i7EJZg+YZM8oMi9a2vnFmozyZUwsc/
T4eqpXZ2tvjqyLk3bwnKY8CAwEAAQJBAI7LMPaH/HQk/b/bVmY0qsr
+me9nb9BqFLuqwzKbx0hSmWPOWFsd3rOFlSopyHqgYtAsPfvPumEdGbdnCyU8zAEClQD71768K1ejb
+ei2lqZqHaczqdUNQxMh54yot9F2yVWjwIhANS1Y1Jv89WEU/ZvvMS9a4638Msv2c4GGp08RtXNYn0BAiA0H4b
+cwoEbZjHf+HYg6Fo+uxu5TvSaw8287a6Qo0LyQIfVZSlYYWplT6oiX5rdLzBiap4N0gJWdsa2ihmV59LAQIgK8N
+j1daq63b0bJ9k4HruhQtpgxI6U9nFBemH4zTRYM=\n-----END RSA PRIVATE KEY-----",
  "timestamp" : 1650595334578,
  "expire_time" : 1596865564000,
  "bind_host" : [ {
    "id" : "978b411657624c2db069cd5484195d1c",
    "hostname" : "www.demo.com",
    "waf_type" : "cloud"
  } ]
}
```

状态码

状态码	描述
200	OK
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.13.4 修改证书

功能介绍

修改证书

URI

PUT /v1/{project_id}/waf/certificate/{certificate_id}

表 4-767 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
certificate_id	是	String	https证书id，您可以通过调用查询证书列表（ListCertificates）接口获取证书id

表 4-768 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-769 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

表 4-770 请求 Body 参数

参数	是否必选	参数类型	描述
name	否	String	证书名称，证书名称只能由数字、字母、中划线、下划线和英文句点组成，长度不能超过64位字符

响应参数

状态码： 200

表 4-771 响应 Body 参数

参数	参数类型	描述
id	String	证书ID
name	String	证书名
expire_time	Long	证书过期时间戳
timestamp	Long	时间戳

状态码： 400

表 4-772 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-773 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-774 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
PUT https://{Endpoint}/v1/{project_id}/waf/certificate/{certificate_id}?enterprise_project_id=0

{
  "name" : "demo"
}
```

响应示例

状态码： 200

OK

```
{
  "id" : "360f992501a64de0a65c50a64d1ca7b3",
  "name" : "demo",
  "timestamp" : 1650593797892,
  "expire_time" : 1596865564000
}
```

状态码

状态码	描述
200	OK
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.13.5 删除证书

功能介绍

删除证书

URI

DELETE /v1/{project_id}/waf/certificate/{certificate_id}

表 4-775 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
certificate_id	是	String	https证书id，您可以通过调用查询证书列表（ListCertificates）接口获取证书id

表 4-776 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-777 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

响应参数

状态码： 200

表 4-778 响应 Body 参数

参数	参数类型	描述
id	String	证书ID
name	String	证书名
content	String	证书文件，PEM编码

参数	参数类型	描述
key	String	证书私钥，PEM编码
expire_time	Long	证书过期时间戳
exp_status	Integer	证书过期状态，0-未过期，1-已过期，2-即将过期
timestamp	Long	证书上传时间戳
bind_host	Array of **BindHost** objects	证书关联的域名信息

表 4-779 BindHost

参数	参数类型	描述
id	String	防护域名ID
hostname	String	防护域名
waf_type	String	防护域名对应模式：cloud（云模式）/premium（独享模式）
mode	String	仅独享模式涉及特殊域名模式

状态码： 400

表 4-780 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-781 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-782 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
DELETE https://{Endpoint}/v1/{project_id}/waf/certificate/{certificate_id}?enterprise_project_id=0
```

响应示例

状态码： 200

OK

```
{
  "id" : "e1d87ba2d88d4ee4a3b0c829e935e5e0",
  "name" : "certificatename29556",
  "timestamp" : 1650594410630,
  "expire_time" : 1596865564000
}
```

状态码

状态码	描述
200	OK
400	请求失败
401	token权限不足
500	服务器内部错误

错误码

请参见**错误码**。

4.2.13.6 绑定证书到域名

功能介绍

绑定证书到域名

URI

POST /v1/{project_id}/waf/certificate/{certificate_id}/apply-to-hosts

表 4-783 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	用户操作的项目id
certificate_id	是	String	https证书id，您可以通过调用查询证书列表（ListCertificates）接口获取证书id

表 4-784 Query 参数

参数	是否必选	参数类型	描述
enterprise_project_id	否	String	您可以通过调用企业项目管理服务（EPS）的查询企业项目列表接口（ListEnterpriseProject）查询企业项目id

请求参数

表 4-785 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	用户Token，通过调用IAM服务获取用户Token接口获取(响应消息头中X-Subject-Token的值)。
Content-Type	是	String	内容类型 缺省值：**application/json;charset=utf8**

表 4-786 请求 Body 参数

参数	是否必选	参数类型	描述
cloud_host_ids	否	Array of strings	云模式HTTPS域名id，通过查询云模式防护域名列表（ListHost）接口获取
premium_host_ids	否	Array of strings	独享模式HTTPS域名id，通过独享模式域名列表（ListPremiumHost）接口获取

响应参数

状态码： 200

表 4-787 响应 Body 参数

参数	参数类型	描述
id	String	证书id
name	String	证书名
timestamp	Long	时间戳
expire_time	Long	过期时间
bind_host	Array of **CertificateBundingHostBody** objects	绑定域名列表

表 4-788 CertificateBundingHostBody

参数	参数类型	描述
id	String	域名id
hostname	String	域名
waf_type	String	waf模式（分为云模式：cloud,独享模式：premium） 枚举值： • **cloud** • **premium**

状态码： 400

表 4-789 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 401

表 4-790 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

状态码： 500

表 4-791 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码
error_msg	String	错误信息

请求示例

```
GET https://{Endpoint}/v1/{project_id}/waf/certificate/{certificate_id}/apply-to-hosts?enterprise_project_id=0

{
  "cloud_host_ids" : [ "85e554189d494c0f97789e93531c9f90" ],
  "premium_host_ids" : [ "4e9e97c425fc463c8f374b90124e8392" ]
}
```

响应示例

状态码： 200

请求成功

```
{
  "id" : "3ac1402300374a63a05be68c641e92c8",
  "name" : "www.abc.com",
  "timestamp" : 1636343349139,
  "expire_time" : 1650794100000,
  "bind_host" : [ {
    "id" : "e350cf556da34adab1f017523d1c05ed",
    "hostname" : "www.demo.com",
    "waf_type" : "cloud",
    "bandwidth" : 0,
    "qps" : 0
  } ]
}
```

状态码

状态码	描述
200	请求成功
400	请求失败
401	token权限不足

状态码	描述
500	服务器内部错误

错误码

请参见**错误码**。

5 权限和授权项

5.1 权限及授权项说明

如果您需要对您所拥有的Web应用防火墙(Web Application Firewall，WAF)进行精细的权限管理，您可以使用统一身份认证服务(Identity and Acsess Management, IAM)，如果账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用WAF的其他功能。

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程成为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为角色和策略。角色以服务为粒度，是IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。策略以API接口为粒度进行权限拆分，授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

说明

如果您要允许或是禁止某个接口的操作权限，请使用策略。

账号具备所有接口的调用权限，如果使用账号下的IAM用户发起API请求时，该IAM用户必须具备调用该接口所需的权限，否则，API请求将调用失败。每个接口所需要的权限，与各个接口所对应的授权项相对应，只有发起请求的用户被授予授权项所对应的策略，该用户才能成功调用该接口。

5.2 支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。策略支持的操作与API相对应，授权项列表说明如下：

- 权限：允许或拒绝某项操作。
- 对应API接口：自定义策略实际调用的API接口。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。

- 依赖的授权项：部分Action存在对其他Action的依赖，需要将依赖的Action同时写入授权项，才能实现对应的权限功能。
- IAM项目(Project)/企业项目(Enterprise Project)：自定义策略的授权范围，包括IAM项目与企业项目。授权范围如果同时支持IAM项目和企业项目，表示此授权项对应的自定义策略，可以在IAM和企业管理两个服务中给用户组授权并生效。如果仅支持IAM项目，不支持企业项目，表示仅能在IAM中给用户组授权并生效，如果在企业管理中授权，则该自定义策略不生效。

说明

“√”表示支持，“x”表示暂不支持

权限	API	授权项	依赖项	IAM项目(Project)
查询WAF独享引擎信息	GET /v1/{project_id}/premium-waf/instance/{instance_id}	waf:premiumInstance:get	-	√
删除WAF独享引擎信息	DELETE /v1/{project_id}/premium-waf/instance/{instance_id}	waf:premiumInstance:delete	-	√
重命名WAF独享引擎	PUT /v1/{project_id}/premium-waf/instance/{instance_id}	waf:premiumInstance:put	-	√
创建WAF独享引擎实例	POST /v1/{project_id}/premium-waf/instance	waf:premiumInstance:create	-	√
查询WAF独享引擎列表	GET /v1/{project_id}/premium-waf/instance	waf:premiumInstance:list	-	√
创建独享模式域名	POST /v1/{project_id}/premium-waf/host	waf:instance:create	-	√
查询独享模式域名列表	GET /v1/{project_id}/premium-waf/host	waf:instance:list	-	√
修改独享模式域名配置	PUT /v1/{project_id}/premium-waf/host/{host_id}	waf:instance:put	-	√
查看独享模式域名配置	GET /v1/{project_id}/premium-waf/host/{host_id}	waf:instance:get	-	√

权限	API	授权项	依赖项	IAM项目(Project)
删除独享模式域名	DELETE /v1/{project_id}/premium-waf/host/{host_id}	waf:instance:delete	-	√
修改独享模式域名防护状态	PUT /v1/{project_id}/premium-waf/host/{host_id}/protect-status	waf:instance:put	-	√
修改独享模式域名接入状态	PUT /v1/{project_id}/premium-waf/host/{host_id}/access_status	waf:instance:put	-	√
查询防护策略列表	GET /v1/{project_id}/waf/policy	waf:policy:list	-	√
创建防护策略	POST /v1/{project_id}/waf/policy	waf:policy:create	-	√
根据Id查询防护策略	GET /v1/{project_id}/waf/policy/{policy_id}	waf:policy:get	-	√
更新防护策略	PATCH /v1/{project_id}/waf/policy/{policy_id}	waf:policy:put	-	√
删除防护策略	DELETE /v1/{project_id}/waf/policy/{policy_id}	waf:policy:delete	-	√
查询黑白名单规则列表	GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip	waf:whiteBlackIpRule:list	-	√
创建黑白名单规则	POST /v1/{project_id}/waf/policy/{policy_id}/whiteblackip	waf:whiteBlackIpRule:create	-	√
查询黑白名单防护规则	GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}	waf:whiteBlackIpRule:get	-	√

权限	API	授权项	依赖项	IAM项目(Project)
更新黑白名单防护规则	PUT /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}	waf:whiteBlackIpRule:put	-	√
删除黑白名单防护规则	DELETE /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}	waf:whiteBlackIpRule:delete	-	√
查询CC规则列表	GET /v1/{project_id}/waf/policy/{policy_id}/cc	waf:ccRule:list	-	√
创建CC规则	POST /v1/{project_id}/waf/policy/{policy_id}/cc	waf:ccRule:create	-	√
根据ID查询CC防护规则	GET /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}	waf:ccRule:get	-	√
更新CC防护规则	PUT /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}	waf:ccRule:put	-	√
删除CC防护规则	DELETE /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}	waf:ccRule:delete	-	√
查询精准防护规则列表	GET /v1/{project_id}/waf/policy/{policy_id}/custom	waf:preciseProtectionRule:list	-	√
创建精准防护规则	POST /v1/{project_id}/waf/policy/{policy_id}/custom	waf:preciseProtectionRule:create	-	√
根据Id 查询精准防护规则	GET /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}	waf:preciseProtectionRule:get	-	√

权限	API	授权项	依赖项	IAM项目(Project)
更新精准防护规则	PUT /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}	waf:preciseProtectionRule:put	-	√
删除精准防护规则	DELETE /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}	waf:preciseProtectionRule:delete	-	√
查询隐私屏蔽规则列表	GET /v1/{project_id}/waf/policy/{policy_id}/privacy	waf:privacyRule:list	-	√
创建隐私屏蔽规则	POST /v1/{project_id}/waf/policy/{policy_id}/privacy	waf:privacyRule:create	-	√
根据Id 查询隐私屏蔽防护规则	GET /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}	waf:privacyRule:get	-	√
更新隐私屏蔽防护规则	PUT /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}	waf:privacyRule:put	-	√
删除隐私屏蔽防护规则	DELETE /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}	waf:privacyRule:delete	-	√
查询防篡改规则列表	GET /v1/{project_id}/waf/policy/{policy_id}/antitamper	waf:antiTamperRule:list	-	√
创建防篡改规则	POST /v1/{project_id}/waf/policy/{policy_id}/antitamper	waf:antiTamperRule:create	-	√
根据Id 查询防篡改防护规则	GET /v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}	waf:antiTamperRule:get	-	√

权限	API	授权项	依赖项	IAM项目(Project)
删除防篡改防护规则	DELETE /v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}	waf:antiTamperRule:delete	-	√
某个网页防篡改规则更新缓存	POST /v1/{project_id}/waf/policy/{policy_id}/antitamper/{antitamperid}/refresh	waf:antiTamperRule:create	-	√
查询误报屏蔽规则列表	GET /v1/{project_id}/waf/policy/{policy_id}/ignore	waf:falseAlarmMaskRule:list	-	√
创建误报屏蔽规则	POST /v1/{project_id}/waf/policy/{policy_id}/ignore	waf:falseAlarmMaskRule:create	-	√
查询误报屏蔽防护规则	GET /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}	waf:falseAlarmMaskRule:get	-	√
更新误报屏蔽防护规则	PUT /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}	waf:falseAlarmMaskRule:put	-	√
删除误报屏蔽防护规则	DELETE /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}	waf:falseAlarmMaskRule:delete	-	√
查询证书列表	GET /v1/{project_id}/waf/certificate	waf:certificate:get	-	√
创建证书	POST /v1/{project_id}/waf/certificate	waf:certificate:create	-	√
查询证书	GET /v1/{project_id}/waf/certificate/{certificate_id}	waf:certificate:list	-	√

权限	API	授权项	依赖项	IAM项目(Project)
修改证书	PUT /v1/{project_id}/waf/certificate/{certificate_id}	waf:certificate:put	-	√
删除证书	DELETE /v1/{project_id}/waf/certificate/{certificate_id}	waf:certificate:delete	-	√
绑定证书到域名	POST /v1/{project_id}/waf/certificate/{certificate_id}/apply-to-hosts	waf:certificate:apply	-	√
查询安全总览请求与攻击数量	GET /v1/{project_id}/waf/overviews/statistics	waf:event:get	-	√
查询安全总览分类统计TOP信息	GET /v1/{project_id}/waf/overviews/classification	waf:event:get	-	√
查询攻击事件列表	GET /v1/{project_id}/waf/event	waf:event:get	-	√
查询攻击事件详情	GET /v1/{project_id}/waf/event/{eventid}	waf:event:get	-	√

A 附录

A.1 状态码

状态码	编码	状态说明
200	OK	客户端请求已处理成功。
204	No Content	服务器成功处理了请求，没有返回任何内容。
400	Bad Request	参数有误。
401	Unauthorized	认证失败。
403	Forbidden	无权限，拒绝访问。
404	Not Found	请求的资源不存在。
406	Not Acceptable	请求不可接受。
409	Conflict	请求资源冲突。
500	Internal Error	服务器内部异常。
503	Server Unavailable	服务不可用。

A.2 云模式错误码

功能介绍

公有云的扩展接口发生400、500等错误时，将返回自定义的错误信息，本章节介绍每个错误码的含义。

返回体格式

- HTTP状态码
  ```
  400
  ```

- 返回体样例

```
{
"error_code": "11000000",
"error_msg": "hx error."
}
```

错误码说明

错误码	说明
WAF.1001	非法请求
WAF.1002	非法的页码或者页面大小
WAF.1003	非法的ID
WAF.1004	非法的名称
WAF.1005	非法的路径
WAF.1006	非法的CC限速模式
WAF.1007	非法的CC用户标识
WAF.1008	非法的防护动作
WAF.1009	非法的CC规则
WAF.1012	非法的Referer
WAF.1013	非法类型
WAF.1014	非法逻辑
WAF.1015	非法子字段
WAF.1016	非法内容
WAF.1018	非法的精准防护规则
WAF.1019	非法的隐私屏蔽规则
WAF.1020	非法的User-Agent
WAF.1021	非法的IP
WAF.1022	非法的误报屏蔽规则
WAF.1023	非法数字
WAF.1025	非法时间
WAF.1029	非法的防护等级
WAF.1030	非法的优先级
WAF.1031	非法的攻击类型
WAF.1600	非法域名
WAF.1601	非法协议

错误码	说明
WAF.1602	非法的服务器地址
WAF.1603	非法的端口
WAF.1604	非法的防护状态或者接入状态
WAF.1605	非法的证书内容格式
WAF.1606	非法的证书私钥格式
WAF.2001	ID不匹配
WAF.2002	防护动作不能设置为阻断
WAF.2004	CC规则不能设置用户标识
WAF.2005	精准防护规则中条件列表为空
WAF.2006	精准防护规则中条件不能设置子字段
WAF.2007	精准防护规则中含有重复条件
WAF.2008	不支持泛域名
WAF.3001	资源未找到
WAF.3002	资源超出限制
WAF.3003	资源正在使用中
WAF.3004	系统繁忙
WAF.3005	域名已经存在
WAF.3006	规则名称已经存在
WAF.3007	规则冲突
WAF.3008	该规则已经存在
WAF.3010	防护策略已经绑定到该域名上了
WAF.4000	API未找到
WAF.4001	方法不允许
WAF.5000	内部错误
WAF.5001	数据访问失败
WAF.5002	HTTP请求失败
WAF.5003	ElasticSearch请求失败
WAF.6000	连接失败
WAF.6001	请求不接受
WAF.6002	返回数据读取失败

错误码	说明
WAF.6003	数据导出失败
WAF.6004	数据导入失败
WAF.7001	数据超出长度
WAF.9001	IAM认证失败
WAF.9002	未权限

A.3 错误码

状态码	错误码	错误信息	描述	处理措施
400	WAF.00011001	bad.request	非法请求	检查入参
400	WAF.00011002	url.param.illegal	URL格式不正确	检查url格式
400	WAF.00011003	request.body.illegal	请求Body格式错误：Body中的参数缺失、值非法	检查请求body
400	WAF.00011004	id.illegal	ID非法	检查ID
400	WAF.00011005	name.illegal	Name非法	检查name
400	WAF.00011006	host.illegal	域名非法	检查域名
400	WAF.00011007	port.illegal	端口非法	检查端口
400	WAF.00011007	ip.illegal	IP非法	检查IP地址
400	WAF.00011008	protect.status.illegal	防护状态非法	检查防护状态是否在枚举值范围
400	WAF.00011009	access.status.illegal	接入状态非法	检查接入状态是否在枚举值范围
400	WAF.00011010	offsetOrLimit.illegal	起始行或限制条数非法	检查起始行或者限制条数是否在范围内
400	WAF.00011011	pageOrPageSize.illegal	页码或每页条数非法	检查页码或者每页条数是否在范围内

状态码	错误码	错误信息	描述	处理措施
400	WAF.00011012	standard.violated	参数非法	检查参数
400	WAF.00011013	description.illegal	描述格式非法	检查描述格式
400	WAF.00011014	request.header.illegal	请求Header格式错误：Header中的参数缺失、值非法	检查header必填参数
400	WAF.00011014	website.not.register	网站未备案	备案网站
400	WAF.00011016	name.duplicate	名称重复	修改名称
400	WAF.00012001	invalid.token	token非法	检查token是否正确
400	WAF.00012002	invalid.project	project_id和token中的不一致	检查project_id和token的一致性
400	WAF.00012003	permission.denied	没有权限	给账户分配WAF所需权限
400	WAF.00012004	account.frozen	账号冻结	解除冻结
400	WAF.00012005	not.subscribe	未订阅	先订阅WAF服务
400	WAF.00012006	pdp.permission.denied	没有权限	检查账户的PDP权限
400	WAF.00012007	jwt.authentication.disabled	JWT认证关闭	开通JWT认证
400	WAF.00012008	jwt.authentication.invalid.token	JWT token非法	检查账号是否具有JWT权限
400	WAF.00012009	jwt.authentication.failed	JWT鉴权失败	先给账户授权
400	WAF.00012010	eps.all.not.support	所有企业项目下不支持写操作	开通企业项目的写权限
400	WAF.00013001	insufficient.quota	功能配额不足	购买功能配额升级包

状态码	错误码	错误信息	描述	处理措施
400	WAF.00013002	feature.not.support	功能不支持	无
400	WAF.00013003	port.not.support	端口不支持	通过ELB进行端口转换
400	WAF.00013004	protocol.not.support	协议不支持	通过ELB转换协议
400	WAF.00013005	wildcard.domain.not.support	泛域名不支持	使用具体的域名
400	WAF.00013006	ipv6.not.support	不支持IPV6	当前版本不支持IPV6
400	WAF.00013007	insufficient.tenant.quota	租户配额不足	购买配额升级包
400	WAF.00014001	resource.not.found	资源找不到	资源已删除或不存在
400	WAF.00014002	resource.already.exists	资源已存在	资源已存在
400	WAF.00014003	open.protect.failed	开启防护失败	检查域名防护状态
400	WAF.00014004	access.failed	接入WAF失败	修改DNS解析
400	WAF.00014005	bypass.failed	BypassWAF失败	检查防护状态后进行重试
400	WAF.00014006	proxy.config.error	代理配置错误	重新正确配置代理后重试
400	WAF.00014007	host.conflict	域名冲突	检查网站配置中是已存在域名
400	WAF.00014008	cert.inconsistent	相同的域名，但证书不一致	使用相同的证书
400	WAF.00014009	api.not.found	接口不存在	检查接口url
400	WAF.00014010	port.protocol.mismatch	端口和协议不匹配	选择匹配的协议和端口
400	WAF.00014011	host.blacklist	禁止添加该防护网站，域名被列入黑名单	无
400	WAF.00014012	insufficient.tenant.quota	租户配额不足	购买配额升级包

状态码	错误码	错误信息	描述	处理措施
400	WAF.00014013	exclusive.ip.config.error	独享IP配置错误	检查独享IP配置
400	WAF.00014014	exclusive.ip.config.error	独享IP配置错误	检查独享IP配置
400	WAF.00021002	url.param.illegal	url格式不正确	建议将请求体参数中url修改为标准的url后重新调试
400	WAF.00021003	request.body.illegal	请求体参数不正确	建议调试前根据文档检验入参
400	WAF.00021004	id.illegal	唯一标识符id格式不正确	建议按照文档中的正确说明获取ID
400	WAF.00021005	name.illegal	name参数格式不正确	检查name格式，只能由字母、数字、-、_和.组成,长度不能超过64个字符
400	WAF.00021006	host.illegal	域名格式不正确	域名只能由字母、数字、-、_和.组成,长度不能超过64个字符
400	WAF.00021007	protocol.illegal	后端协议格式不正确	后端协议只能配置为HTTP或HTTPS，且必须大写
400	WAF.00021008	port.illegal	源站端口格式不正确	检查配置的端口是否为空，目标端口是否在0-65535范围内
400	WAF.00021009	ip.illegal	ip格式不正确	建议检查ip格式是否为标准的ipv4或ipv6格式
400	WAF.00021010	server.address.illegal	服务器配置异常	检查服务器配置是否为空，数量是否在1-80范围内
400	WAF.00021012	path.illegal	规则配置中的url格式不正确	建议将请求体参数中url修改为标准的url后重新调试
400	WAF.00021013	cert.illegal	https证书已经过期	建议重新上传未过期的证书

状态码	错误码	错误信息	描述	处理措施
400	WAF.00021014	action.illegal	防护动作非法	建议根据文档中的枚举值配置防护动作
400	WAF.00021015	rule.status.illegal	规则状态非法	建议根据文档中的规则状态枚举值修改规则状态
400	WAF.00021016	description.illegal	描述异常	建议用标准的中英文语法描述
400	WAF.00021017	incorrect.rule.config	不正确的规则配置	建议根据帮助中心的文档配置防护规则
400	WAF.00021018	incorrect.reference.table.config	不正确的引用表配置	建议根据帮助中心的文档配置引用表
400	WAF.00021019	incorrect.route.config	不正确的线路配置	建议根据帮助中心的文档进行线路配置
400	WAF.00021020	offsetOrLimit.illegal	分页参数错误	建议根据帮助中心的文档填写分页参数
400	WAF.00021021	param.exceed.limit	参数超过限制	建议根据帮助中心的文档查看参数限制
400	WAF.00022002	resource.already.exists	资源已存在	建议在控制台查看所创建的资源是否已经存在
400	WAF.00022003	resource.is.being.used	资源正在使用中	先解除资源和使用者的关系，再删除资源
400	WAF.00022004	rule.conflict	规则冲突	检查目标规则是否和已有的规则发生冲突
403	WAF.00022005	insufficient.quota	资源不足	建议购买对应资源的升级包
404	WAF.00022001	resource.not.found	资源不存在	建议到控制台查看资源状态或求助技术支持
500	WAF.00010001	internal.error	内部错误	联系技术支持
500	WAF.00010002	system.busy	内部错误	联系技术支持

状态码	错误码	错误信息	描述	处理措施
500	WAF.00010003	cname.failed	创建或者修改CNAME失败	联系技术支持
500	WAF.00010004	cname.failed	获取OBS文件下载链接失败	联系技术支持
500	WAF.00020001	internal.error	服务内部异常	建议过五分钟后重试
500	WAF.00020002	system.busy	系统繁忙	建议过五分钟后重试

A.4 获取项目 ID

1. 获取Token。
   请参见**Token认证**。
2. 获取项目ID。
   获取项目ID的接口为“GET https://iam.eu-west-0.myhuaweicloud.com/v3/*projects*”。
   在请求消息头中增加“X-Auth-Token”，“X-Auth-Token”的取值为上一步获取的Token。
   响应示例如下，其中projects下的“id”即为项目ID。

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

A.5 字符集规范

- KEY字符集规范
  key不能为空，不能为空字符串。
  - 其他环境字符集要求：不能包含非打印字符ASCII(0-31) 以及“=”，“*”，“<”，“>”，“\”，“,”，“|”，“/”。
  - DT字符集要求：大小写字母，数字，中划线“-”，下划线“_”以及符号“@”。
- VALUE字符集规范
  value不能为空，但可以为空字符串。

- 其他环境字符集要求：不能包含非打印字符ASCII(0-31) 以及“=”，“*”，“<”，“>”，“\”，“,”，“|”，“/”。
- DT环境字符集要求：大小写字母，数字，中划线“-”，下划线“_”以及符号 “@”。

B 修订记录

发布日期	修改说明
2022-12-28	第二次正式发布。 增加“独享模式API”。
2021-07-14	第一次正式发布。