ALIBABA CLOUD

阿里云

Web应用防火墙

API参考（2019-09-10）

文档版本：20220520

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.API概览

本文汇总了Web应用防火墙（WAF）服务所有可调用的API。

实例信息

API	描述
DescribeInstanceInfo	查询已购买的WAF实例的基本信息，例如实例ID、实例的类型和状态等。
DescribeInstanceSpecInfo	查询已购买的WAF实例的规格信息。
DeleteInstance	释放已开通的按量付费WAF实例或者已到期的包年包月WAF实例。

域名配置

API	描述
DescribeDomainNames	查询所有已添加到WAF防护的域名名称列表。 **说明** 该接口只能一次性返回所有域名。推荐您调用DescribeDomainList接口进行分页查询。
DescribeDomainList	分页查询已添加到WAF防护的域名名称列表。 **说明** 该接口支持按条件查询及分页返回结果。对于域名数量较多的场景，推荐您调用该接口。
DescribeDomain	查询WAF实例中已添加的域名配置信息。
CreateDomain	添加域名配置信息，将您的域名接入WAF实例进行防护。
ModifyDomain	修改指定的域名配置信息。
DeleteDomain	删除指定的域名配置信息。
DescribeCertificates	查询指定域名关联的已有证书，即已在SSL证书服务中进行管理的证书。
DescribeCertMatchStatus	查询域名配置中上传的证书和私钥信息是否匹配。
CreateCertificate	为已添加的域名配置上传证书及私钥信息。
CreateCertificateByCertificateId	根据证书ID为指定的域名配置上传证书。
DescribeDomainBasicConfigs	查询已添加的域名配置的防护设置状态。
DescribeDomainAdvanceConfigs	查询已添加的域名配置的详细信息。

防护配置

API	描述
ModifyDomainIpv6Status	为域名配置开启或关闭IPv6安全防护功能。
DescribeProtectionModuleStatus	查询指定的WAF防护功能模块（包括Web入侵防护、数据安全、高级防护、Bot管理、访问控制或限流等模块）的开关状态。
ModifyProtectionModuleStatus	为域名配置开启或关闭WAF防护功能模块（包括Web入侵防护、数据安全、高级防护、Bot管理、访问控制或限流等模块）。
DescribeProtectionModuleMode	查询域名配置中各WAF防护功能模块（包括规则防护引擎、深度学习引擎、CC安全防护、数据风控、主动防御等模块）当前采用的防护模式。
ModifyProtectionModuleMode	修改指定的WAF防护功能模块（包括规则防护引擎、深度学习引擎、CC安全防护、数据风控、主动防御等模块）的防护模式。
DescribeProtectionModuleRules	查询指定的WAF防护功能模块（包括Web入侵防护、数据安全、Bot管理、访问控制或限流、网站白名单等模块）的规则配置记录。
CreateProtectionModuleRule	在指定的WAF防护功能模块（包括Web入侵防护、数据安全、Bot管理、访问控制或限流、网站白名单等模块）中创建规则配置。
ModifyProtectionModuleRule	修改指定的WAF防护功能模块（包括Web入侵防护、数据安全、高级防护、Bot管理、访问控制或限流、白名单等模块）的配置规则。
ModifyProtectionRuleStatus	为域名配置开启或关闭WAF防护功能模块（包括网站防篡改、合法爬虫、爬虫威胁情报、自定义防护策略、网站白名单等模块）中已创建的规则。
DescribeDomainRuleGroup	查询域名配置当前使用的规则防护引擎的防护规则组ID。
SetDomainRuleGroup	为域名配置选择规则防护引擎使用的防护规则组（除系统默认的三种防护规则组外，也可以选择自定义规则组）。
ModifyProtectionRuleCacheStatus	更新指定的网站防篡改规则所防护页面的缓存。
DeleteProtectionModuleRule	删除指定的防护模块下已创建的规则配置。
DescribeProtectionModuleCodeConfig	查询WAF地域级IP黑名单中支持配置的地域代码。

日志管理

API	描述
ModifyLogServiceStatus	为域名配置开启或关闭日志采集功能。
ModifyLogRetrievalStatus	为域名配置开启或关闭日志检索功能。
DescribeLogServiceStatus	查询已接入WAF进行防护的域名的日志采集状态（是否开启了日志采集）。

系统管理

API	描述
DescribeWafSourceIpSegment	查询WAF防护集群使用的回源IP网段。

资源相关接口

API	描述
MoveResourceGroup	将一个WAF资源转移到其他资源组。

2.调用方式

Web应用防火墙接口调用是向WAF API的服务端地址发送HTTP GET请求，并按照接口说明在请求中加入相应请求参数，调用后系统会返回处理结果。请求及返回结果都使用UTF-8字符集编码。

请求结构

Web应用防火墙的API是RPC风格，您可以通过发送HTTP GET请求调用WAF API。

其请求结构如下：

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

其中：

- Endpoint：根据WAF实例所属的地域选择适合的API服务接入地址。
  - 中国内地：wafopenapi.cn-hangzhou.aliyuncs.com
  - 非中国内地：wafopenapi.ap-southeast-1.aliyuncs.com
- Action：要执行的操作，如使用DescribeDomainNames查询已添加的域名名称列表。
- Version：要使用的API版本，WAF的API版本是*2019-09-10*。
- Parameters：请求参数，每个参数之间用“&”分隔。

  请求参数由公共请求参数和API自定义参数组成。公共参数中包含API版本号、身份验证等信息，详情请参见公共参数。

下面是一个调用DescribeDomainNames接口查询指定WAF实例中已添加的域名名称列表的示例：

> **说明** 为了便于用户查看，本文档中的示例都做了格式化处理。

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&Region=cn
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Format=xml
&Version=2019-09-10
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2012-06-01T12:00:00Z
...
```

API授权

为了确保您的账号安全，建议您使用子账号的身份凭证调用API。如果您使用RAM账号调用WAF API，您需要为该RAM账号创建、附加相应的授权策略。

API签名

WAF服务会对每个API请求进行身份验证，无论使用HTTP还是HTTPS协议提交请求，都需要在请求中包含签名（Signature）信息。

WAF通过使用AccessKey ID和AccessKey Secret进行对称加密的方法来验证请求的发送者身份。AccessKey是为阿里云账号和RAM用户发布的一种身份凭证（类似于用户的登录密码），其中AccessKey ID用于标识访问者的身份，AccessKey Secret是用于加密签名字符串和服务器端验证签名字符串的密钥，必须严格保密。

RPC API需按如下格式在请求中增加签名（Signature）：

```
https://endpoint/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&Signature=CT9X0VtwR86fNWSn
sc6v8YGOjuE%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
```

以DescribeDomainNames为例，假设AccessKey ID是 `testid` ，AccessKey Secret是 `testsecret` ，则签名前的请求URL如下：

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&Region=cn
&InstanceId=waf_elasticity-cn-0xldbqtm005
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2019-09-10
&SignatureVersion=1.0
```

完成以下步骤计算签名：

1. 使用请求参数创建待签名字符串：

   ```
   GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeDomainNames&Region%3Dcn&InstanceId%3Dwaf_
   elasticity-cn-0xldbqtm005&Format%3DXML&SignatureMethod%3DHMAC-SHA1&SignatureNonce%3D3ee
   8c1b8-83d3-44af-a94f-4e0ad82fd6cf&SignatureVersion%3D1.0&TimeStamp%3D2016-02-23T12%253A
   46%253A24Z&Version%3D2019-09-10
   ```

2. 计算待签名的HMAC的值。

   在AccessKey Secret后添加一个“&”作为计算HMAC值的key。本示例中的key为 `testsecret&` 。

   ```
   CT9X0VtwR86fNWSnsc6v8YGOjuE=
   ```

3. 将签名加到请求参数中：

   ```
   https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
   &Region=cn
   &InstanceId=waf_elasticity-cn-0xldbqtm005
   &TimeStamp=2016-02-23T12:46:24Z
   &Format=XML
   &AccessKeyId=testid
   &SignatureMethod=HMAC-SHA1
   &SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
   &Version=2019-09-10
   &SignatureVersion=1.0
   &Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D
   ```

3.公共参数

本文介绍每个接口都需要使用的请求参数和返回数据。

公共请求参数

名称	类型	是否必须	描述
Format	String	否	返回消息的格式。取值： • *JSON*（默认） • *XML*
Version	String	是	API版本号，使用YYYY-MM-DD日期格式。取值： *2019-09-10*
AccessKeyId	String	是	访问服务使用的密钥ID。
Signature	String	是	签名结果串。
SignatureMethod	String	是	签名方式，取值： *HMAC-SHA1*
Timestamp	String	是	请求的时间戳，为日期格式。使用UTC时间，按照 ISO 8601标准，格式为YYYY-MM-DDThh:mm:ssZ。 例如，北京时间2013年1月10日20点0分0秒，表示为2013-01-10T12:00:00Z。
SignatureVersion	String	是	签名算法版本，取值： *1.0*
SignatureNonce	String	是	唯一随机数，用于防止网络重放攻击。 在不同请求间要使用不同的随机数值。
ResourceOwnerAccount	String	否	本次API请求访问到的资源拥有者账号，即登录用户名。

示例

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&InstanceId=waf-cn-zz11sr5****
&Timestamp=2014-05-19T10%3A33%3A56Z
&Format=xml
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=NwDAxvLU6tFE0DVb
&Version=2019-09-10
&SignatureVersion=1.0
&Signature=Signature
```

公共返回数据

API返回结果采用统一格式，返回2xx HTTP状态码表示调用成功，返回4xx或5xx HTTP状态码表示调用失败。每次接口调用，无论成功与否，系统都会返回一个唯一识别码RequestId，用于标识本次请求。

调用成功返回的数据格式有XML和JSON两种。您可以在发送请求时指定返回的数据格式，默认为XML格式。

正常返回数据示例：

- XML格式

```
<?xml version="1.0" encoding="utf-8"?>
    <!--结果的根结点-->
    <接口名称+Response>
        <--返回请求标签-->
        <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
        <!--返回结果数据-->
    </接口名称+Response>
```

- JSON格式

```
{
    "RequestId":"4C467B38-3910-447D-87BC-AC049166F216",
    /*返回结果数据*/
    }
```

4.实例信息

4.1. DescribeInstanceInfo

调用DescribeInstanceInfo查询当前阿里云账号下WAF实例的详情。

使用说明

本接口用于查询当前阿里云账号下WAF实例的详情，例如，实例的ID、版本、状态、到期时间等。

QPS限制

本接口的单用户QPS限制为50次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstanceInfo	要执行的操作。取值：**DescribeInstanceInfo**。
InstanceId	String	否	waf-cn-tl32ast****	要查询的WAF实例的ID。 不设置该参数表示查询所有WAF实例的信息。
ResourceGroupId	String	否	rg-atstuj3rtop****	WAF实例在资源管理服务中所属的资源组ID。不设置该参数表示默认资源组。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	本次请求的ID。
InstanceInfo	Object		WAF实例的详情。

名称	类型	示例值	描述
Status	Integer	1	WAF实例是否过期。取值： • **0**：表示已过期。 • **1**：表示未过期。 **说明** PayType为0（表示未开通WAF实例）时，不返回该参数。
EndDate	Long	1512921600	WAF实例的到期时间。使用时间戳表示，单位：秒。 **说明** PayType为0（表示未开通WAF实例）时，不返回该参数。
Version	String	version_3	WAF实例的版本。取值： • **version_3**：表示中国内地高级版。 • **version_4**：表示中国内地企业版。 • **version_5**：表示中国内地旗舰版。 • **version_exclusive_cluster**：表示中国内地虚拟独享集群版。 • **version_hybrid_cloud_standard**：表示中国内地混合云WAF版。 • **version_pro_asia**：表示海外地区高级版。 • **version_business_asia**：表示海外地区企业版。 • **version_enterprise_asia**：表示海外地区旗舰版。 • **version_exclusive_cluster_asia**：表示海外地区虚拟独享集群版。 • **version_hybrid_cloud_standard_asia**：表示海外地区混合云WAF版。 • **version_elastic_bill**：表示按量计费版。 • **version_elastic_bill_new**：表示按量计费2.0版。 如果返回的version参数值不在上述列表中，请确认您使用的是阿里云中国站云账号。 **说明** PayType为0（表示未开通WAF实例）时，不返回该参数。

名称	类型	示例值	描述
RemainDay	Integer	1	试用版WAF实例的剩余可用天数。 **说明** 只有当Trial为1（表示已开通试用版WAF实例）时，才返回该参数。
Region	String	cn	WAF实例的地域。取值： • **cn**：表示中国内地。 • **cn-hongkong**：表示海外地区。 **说明** PayType为0（表示未开通WAF实例）时，不返回该参数。
PayType	Integer	1	WAF实例的开通状态。取值： • **0**：表示当前阿里云账号未开通WAF实例。 • **1**：表示当前阿里云账号已开通WAF包年包月实例。 • **2**：表示当前阿里云账号已开通WAF按量计费实例。
InDebt	Integer	1	WAF实例是否存在欠费。取值： • **0**：表示已欠费。 • **1**：表示未欠费。 **说明** PayType为0（表示未开通WAF实例）时，不返回该参数。
InstanceId	String	waf-cn-tl32ast****	WAF实例的ID。 **说明** PayType为0（表示未开通WAF实例）时，不返回该参数。

名称	类型	示例值	描述
SubscriptionType	String	Subscription	WAF实例的计费方式。取值： • **Subscription**：表示包年包月。 • **PayAsYouGo**：表示按量计费。 **说明** PayType为0（表示未开通WAF实例）时，不返回该参数。
Trial	Integer	1	当前阿里云账号是否开通了试用版WAF实例。取值： • **0**：表示否。 • **1**：表示是。 **说明** 只有当前阿里云账号已开通试用版WAF实例时，才会返回该参数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeInstanceInfo
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeInstanceInfoResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <InstanceInfo>
        <Status>1</Status>
        <EndDate>1512921600</EndDate>
        <Version>version_3</Version>
        <Region>cn</Region>
        <PayType>1</PayType>
        <InDebt>1</InDebt>
        <InstanceId>waf-cn-tl32ast****</InstanceId>
        <SubscriptionType>Subscription</SubscriptionType>
    </InstanceInfo>
</DescribeInstanceInfoResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "D7861F61-5B61-46CE-A47C-6B19160D5EB0",
  "InstanceInfo" : {
    "Status" : 1,
    "EndDate" : 1512921600,
    "Version" : "version_3",
    "Region" : "cn",
    "PayType" : 1,
    "InDebt" : 1,
    "InstanceId" : "waf-cn-tl32ast****",
    "SubscriptionType" : "Subscription"
  }
}
```

错误码

访问错误中心查看更多错误码。

4.2. DescribeInstanceSpecInfo

调用DescribeInstanceSpecInfo查询WAF实例的规格信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstanceSpecInfo	要执行的操作。取值：**DescribeInstanceSpecInfo**。
InstanceId	String	否	waf-cn-st2225l****	要查询的WAF实例的ID。 **说明** 您可以调用DescribeInstanceInfo查询当前WAF实例的ID。
ResourceGroupId	String	否	rg-atstuj3rtop****	WAF实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。 关于资源组的更多信息，请参见创建资源组。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	E906513E-F6B5-495E-98DC-7BA888671D76	本次请求的ID。
InstanceId	String	waf-cn-st2225l****	WAF实例ID。
Version	String	version_hybrid_cloud_standard	WAF实例的版本。取值： • **version_3**：表示中国内地高级版。 • **version_4**：表示中国内地企业版。 • **version_5**：表示中国内地旗舰版。 • **version_exclusive_cluster**：表示中国内地虚拟独享集群版。 • **version_hybrid_cloud_standard**：表示中国内地混合云WAF版。 • **version_pro_asia**：表示海外地区高级版。 • **version_business_asia**：表示海外地区企业版。 • **version_enterprise_asia**：表示海外地区旗舰版。 • **version_exclusive_cluster_asia**：表示海外地区虚拟独享集群版。 • **version_hybrid_cloud_standard_asia**：表示海外地区混合云WAF版。 • **version_elastic_bill**：表示按量计费版。 • **version_elastic_bill_new**：表示按量计费2.0版。 如果返回的version参数值不在上述列表中，请确认您使用的是阿里云中国站云账号。
InstanceSpecInfos	Array of InstanceSpecInfo		WAF实例的规格信息，以**Code**与**Value**的数组形式返回实例的各项规格信息。其中，**Code**表示规格代码，**Value**表示对应的规格值。
			WAF实例规格的代码。取值： • **100**：表示是否支持HTTPS业务防护。 • **101**：表示日常业务流量阈值。 • **102**：表示CC攻击防护阈值。 • **103**：表示支持接入防护的域名总数。

名称	类型	示例值	描述
Code	String	113	• 104：表示是否支持泛域名。 • 105：表示支持配置的自定义防护策略（ACL访问控制）规则的数量。 • 106：表示域名回源IP的数量。 • 107：表示是否支持云外房机。 • 108：表示是否支持自定义高级Web访问控制功能。 • 109：表示是否支持非标准端口。 • 110：表示是否支持扫描防护功能。 • 111：表示是否支持数据风控。 • 112：表示支持配置的数据风控记录数。 • 113：表示支持接入防护的主域名数（一级域名）。 • 114：表示正常业务带宽阈值。 • 115：表示绑定的域名包的数量。 • 116：表示是否支持添加不同阿里云账号下的ECS IP作为源站服务器IP。 • 117：表示是否支持添加虚拟主机IP作为源站服务器IP。 • 118：表示支持配置的数据风控规则场景的数量。 • 119：表示是否支持语义分析引擎功能。 • 12：表示是否支持业务流量分析功能。 • 120：表示接入域名是否需要判断备案。 • 121：表示是否支持配置自定义防护策略（CC攻击防护）规则。 • 122：表示支持配置的自定义防护策略（CC攻击防护）规则的数量。 • 123：表示是否支持地域级IP黑名单功能。 • 124：表示是否支持网站防篡改功能。 • 125：表示支持配置的自定义防篡改防护规则的数量。 • 126：表示是否支持收集日志功能。 • 127：表示支持添加的非标端口数。 • 128：表示支持添加的HTTP协议端口。 • 129：表示支持添加的HTTPS协议端口。 • 13：表示是否支持切换CC安全防护的模式。 • 130：表示是否支持黑客画像功能。 • 131：表示是否支持防敏感信息泄露功能。 • 132：表示支持配置的防敏感信息泄露规则的数量。 • 133：表示自定义防护策略及白名单策略中支持使用的条件字段。 • 134：表示绑定的独享IP的数量。 • 135：表示是否支持数据大屏功能。 • 136：表示支持的数据大屏数量。

名称	类型	示例值	描述
			• 137：表示是否支持深度学习引擎功能。 • 138：表示是否支持全量日志功能。 • 139：表示全量日志的存储时长。 • 14：表示是否支持查看CC攻击日志详情。 • 140：表示全量日志的最大存储容量。 • 141：表示是否支持告警设置功能。 • 142：表示全量日志的存储空间可清空次数。 • 143：表示是否支持自定义防护规则组功能。 • 144：表示支持配置的自定义规则组的数量。 • 145：表示是否支持使用防护模块通用网关代理。 • 146：表示是否支持使用防护模块通用规则代理。 • 147：表示是否支持安全专家服务平台。 • 148：表示是否支持试用。 • 149：表示是否支持使用透明代理模式。 • 150：表示是否支持IPv6。 • 151：表示是否支持主动防御功能。 • 152：表示支持配置的主动防护规则的数量。 • 153：表示是否支持HTTP 2.0业务防护。 • 154：表示是否支持域名配置功能。 • 155：表示是否支持资产识别功能。 • 156：表示是否具有预发测试规格。 • 157：表示是否支持使用虚拟独立集群。 • 158：表示虚拟独立集群支持的端口数量。 • 159：表示是否支持账号安全功能。 • 160：表示账号安全防护的接口数量。 • 162：表示支持添加的白名单规则的数量。 • 163：表示自定义防护规则的数量。 • 164：表示IP黑名单规则的数量。 • 167：表示是否支持自定义扫描防护配置。 • 168：表示全局负载均衡（GSLB）防护域名的数量。 • 169：表示是否支持智能负载均衡。 • 171：表示是否支持App防护功能。 • 172：表示App防护的规则数量。 • 173：表示是否支持典型爬虫行为识别功能。 • 176：表示是否支持合法爬虫功能。 • 177：表示是否支持爬虫威胁情报功能。 • 181：表示透明接入支持添加的引流配置（对应一个具体的实例IP+端口）的数量。 • 193：表示是否支持自定义TLS安全策略。 • 194：表示是否支持自定义TLS安全策略的高级设置。 • 196：表示透明接入是否支持接入任意接口。

名称	类型	示例值	描述
			• 199：表示是否支持IPv6回源。 • 200：表示是否支持防爬场景化配置。 • 201：表示防爬场景化配置的数量。
Value	String	300	WAF实例规格代码对应的值。布尔型规格（是否……）的取值包括：**true**（表示是）|**false**（表示否）。
ExpireTime	Long	1677168000000	WAF实例的到期时间。格式为毫秒级时间戳。 **说明** 对于按量计费实例，返回的值表示试用版的到期时间。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeInstanceSpecInfo
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeInstanceSpecInfoResponse>
   <InstanceSpecInfos>
      <Value>true</Value>
      <Code>190</Code>
   </InstanceSpecInfos>
   <InstanceSpecInfos>
      <Value>true</Value>
      <Code>191</Code>
   </InstanceSpecInfos>
   <InstanceSpecInfos>
      <Value>true</Value>
      <Code>192</Code>
   </InstanceSpecInfos>
   <InstanceSpecInfos>
      <Value>true</Value>
      <Code>193</Code>
   </InstanceSpecInfos>
   <InstanceSpecInfos>
      <Value>true</Value>
      <Code>194</Code>
   </InstanceSpecInfos>
   <InstanceSpecInfos>
      <Value>true</Value>
      <Code>195</Code>
   </InstanceSpecInfos>
   <InstanceSpecInfos>
      <Value>true</Value>
```

```
    <Code>196</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>true</Value>
    <Code>197</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>true</Value>
    <Code>110</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>true</Value>
    <Code>198</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>true</Value>
    <Code>111</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>true</Value>
    <Code>199</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>20</Value>
    <Code>112</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>300</Value>
    <Code>113</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>20</Value>
    <Code>114</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>100</Value>
    <Code>115</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>true</Value>
    <Code>116</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>false</Value>
    <Code>117</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>0,1,2,3</Value>
    <Code>118</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>false</Value>
    <Code>119</Code>
</InstanceSpecInfos>
```

```
    <InstanceSpecInfos>
      <Value>true</Value>
      <Code>12</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>true</Value>
      <Code>13</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>true</Value>
      <Code>14</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>true</Value>
      <Code>120</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>true</Value>
      <Code>121</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>50</Value>
      <Code>122</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>true</Value>
      <Code>123</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>true</Value>
      <Code>124</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>300</Value>
      <Code>125</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>true</Value>
      <Code>126</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>50</Value>
      <Code>127</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>80,81,82,83,84,88,800,808,3333,5000,5222,6001,6666,7000,7001,7002,7003,7004,70
05,7006,7009,7010,7011,7012,7013,7014,7015,7016,7018,7019,7020,7021,7022,7023,7024,7025,702
6,7070,7081,7082,7083,7088,7097,7777,8000,8001,8002,8003,8009,8020,8021,8022,8025,8026,8080
,8081,8082,8083,8084,8085,8086,8087,8088,8089,8090,8091,8181,8800,8888,8889,8999,9000,9001,
9002,9080,9200,9999,10000,10001,10080,12601,86,9021,9023,9027,9037,9081,9082,9201,9205,9207
,9208,9209,9210,9211,9212,9213,48800,87,97,7510,8686,9180,9916,9918,9919,9928,9929,9939,337
02,89,1000,1090,3501,3601,7800,8008,8077,8078,8106,8334,8336,9003,9898,9908,28080</Value>
      <Code>128</Code>
    </InstanceSpecInfos>
```

```
    <InstanceSpecInfos>
       <Value>443,4443,5443,6443,7443,8443,9443,8553,8663,9553,9663,18980</Value>
       <Code>129</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>true</Value>
       <Code>130</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>true</Value>
       <Code>131</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>50</Value>
       <Code>132</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>IP,URL,Referer,User-Agent,Params,Query_Arg,Cookie,Content-Type,X-Forwarded-For
,Content-Length,Post-Body,Http-Method,Header,URLPath</Value>
       <Code>133</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>2</Value>
       <Code>134</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>true</Value>
       <Code>135</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>all</Value>
       <Code>136</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>true</Value>
       <Code>137</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>true</Value>
       <Code>138</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>30</Value>
       <Code>139</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>3</Value>
       <Code>140</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>true</Value>
       <Code>141</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
```

```
      <Value>3</Value>
      <Code>142</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>true</Value>
      <Code>143</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>50</Value>
      <Code>144</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>true</Value>
      <Code>145</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>true</Value>
      <Code>146</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>true</Value>
      <Code>147</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>false</Value>
      <Code>148</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>true</Value>
      <Code>149</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>true</Value>
      <Code>150</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>true</Value>
      <Code>151</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>200</Value>
      <Code>152</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>true</Value>
      <Code>153</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>true</Value>
      <Code>154</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
      <Value>true</Value>
      <Code>155</Code>
    </InstanceSpecInfos>
```

```
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>true</Value>
       <Code>156</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>true</Value>
       <Code>157</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>50</Value>
       <Code>158</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>true</Value>
       <Code>159</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>3</Value>
       <Code>160</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>wafnext</Value>
       <Code>161</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>200</Value>
       <Code>162</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>200</Value>
       <Code>163</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>200</Value>
       <Code>164</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>false</Value>
       <Code>165</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>IP,Session,Param,Cookie,Header</Value>
       <Code>166</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>true</Value>
       <Code>167</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>true</Value>
       <Code>200</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
       <Value>1</Value>
```

```
    <Code>168</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>50</Value>
    <Code>201</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>true</Value>
    <Code>169</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>true</Value>
    <Code>202</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>false</Value>
    <Code>203</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>100</Value>
    <Code>204</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>50</Value>
    <Code>205</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>true</Value>
    <Code>170</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>true</Value>
    <Code>171</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>50</Value>
    <Code>172</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>true</Value>
    <Code>173</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>5</Value>
    <Code>174</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>500</Value>
    <Code>175</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
    <Value>true</Value>
    <Code>176</Code>
</InstanceSpecInfos>
```

```
<InstanceSpecInfos>
   <Value>true</Value>
   <Code>177</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
   <Value>custom</Value>
   <Code>178</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
   <Value>true</Value>
   <Code>179</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
   <Value>true</Value>
   <Code>180</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
   <Value>50</Value>
   <Code>181</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
   <Value>false</Value>
   <Code>182</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
   <Value>true</Value>
   <Code>183</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
   <Value>true</Value>
   <Code>184</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
   <Value>false</Value>
   <Code>185</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
   <Value>true</Value>
   <Code>186</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
   <Value>true</Value>
   <Code>187</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
   <Value>true</Value>
   <Code>100</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
   <Value>true</Value>
   <Code>188</Code>
</InstanceSpecInfos>
<InstanceSpecInfos>
   <Value>5000</Value>
```

```
      <Code>101</Code>
   </InstanceSpecInfos>
   <InstanceSpecInfos>
      <Value>true</Value>
      <Code>189</Code>
   </InstanceSpecInfos>
   <InstanceSpecInfos>
      <Value>500000</Value>
      <Code>102</Code>
   </InstanceSpecInfos>
   <InstanceSpecInfos>
      <Value>1200</Value>
      <Code>103</Code>
   </InstanceSpecInfos>
   <InstanceSpecInfos>
      <Value>true</Value>
      <Code>104</Code>
   </InstanceSpecInfos>
   <InstanceSpecInfos>
      <Value>200</Value>
      <Code>105</Code>
   </InstanceSpecInfos>
   <InstanceSpecInfos>
      <Value>20</Value>
      <Code>106</Code>
   </InstanceSpecInfos>
   <InstanceSpecInfos>
      <Value>true</Value>
      <Code>107</Code>
   </InstanceSpecInfos>
   <InstanceSpecInfos>
      <Value>true</Value>
      <Code>108</Code>
   </InstanceSpecInfos>
   <InstanceSpecInfos>
      <Value>true</Value>
      <Code>109</Code>
   </InstanceSpecInfos>
   <RequestId>E906513E-F6B5-495E-98DC-7BA888671D76</RequestId>
   <InstanceId>waf-cn-st2225l****</InstanceId>
   <Version>version_hybrid_cloud_standard</Version>
   <ExpireTime>1677168000000</ExpireTime>
</DescribeInstanceSpecInfoResponse>
```

`JSON` 格式

```
{
 "InstanceSpecInfos": [
  {
   "Value": "true",
   "Code": "190"
  },
  {
   "Value": "true",
```

```
 "Code": "191"
},
{
 "Value": "true",
 "Code": "192"
},
{
 "Value": "true",
 "Code": "193"
},
{
 "Value": "true",
 "Code": "194"
},
{
 "Value": "true",
 "Code": "195"
},
{
 "Value": "true",
 "Code": "196"
},
{
 "Value": "true",
 "Code": "197"
},
{
 "Value": "true",
 "Code": "110"
},
{
 "Value": "true",
 "Code": "198"
},
{
 "Value": "true",
 "Code": "111"
},
{
 "Value": "true",
 "Code": "199"
},
{
 "Value": "20",
 "Code": "112"
},
{
 "Value": "300",
 "Code": "113"
},
{
 "Value": "20",
 "Code": "114"
},
```

```
{
 "Value": "100",
 "Code": "115"
},
{
 "Value": "true",
 "Code": "116"
},
{
 "Value": "false",
 "Code": "117"
},
{
 "Value": "0,1,2,3",
 "Code": "118"
},
{
 "Value": "false",
 "Code": "119"
},
{
 "Value": "true",
 "Code": "12"
},
{
 "Value": "true",
 "Code": "13"
},
{
 "Value": "true",
 "Code": "14"
},
{
 "Value": "true",
 "Code": "120"
},
{
 "Value": "true",
 "Code": "121"
},
{
 "Value": "50",
 "Code": "122"
},
{
 "Value": "true",
 "Code": "123"
},
{
 "Value": "true",
 "Code": "124"
},
{
 "Value": "300",
```

```
    "Code": "125"
   },
   {
    "Value": "true",
    "Code": "126"
   },
   {
    "Value": "50",
    "Code": "127"
   },
   {
    "Value": "80,81,82,83,84,88,800,808,3333,5000,5222,6001,6666,7000,7001,7002,7003,7004,70
05,7006,7009,7010,7011,7012,7013,7014,7015,7016,7018,7019,7020,7021,7022,7023,7024,7025,702
6,7070,7081,7082,7083,7088,7097,7777,8000,8001,8002,8003,8009,8020,8021,8022,8025,8026,8080
,8081,8082,8083,8084,8085,8086,8087,8088,8089,8090,8091,8181,8800,8888,8889,8999,9000,9001,
9002,9080,9200,9999,10000,10001,10080,12601,86,9021,9023,9027,9037,9081,9082,9201,9205,9207
,9208,9209,9210,9211,9212,9213,48800,87,97,7510,8686,9180,9916,9918,9919,9928,9929,9939,337
02,89,1000,1090,3501,3601,7800,8008,8077,8078,8106,8334,8336,9003,9898,9908,28080",
    "Code": "128"
   },
   {
    "Value": "443,4443,5443,6443,7443,8443,9443,8553,8663,9553,9663,18980",
    "Code": "129"
   },
   {
    "Value": "true",
    "Code": "130"
   },
   {
    "Value": "true",
    "Code": "131"
   },
   {
    "Value": "50",
    "Code": "132"
   },
   {
    "Value": "IP,URL,Referer,User-Agent,Params,Query_Arg,Cookie,Content-Type,X-Forwarded-For
,Content-Length,Post-Body,Http-Method,Header,URLPath",
    "Code": "133"
   },
   {
    "Value": "2",
    "Code": "134"
   },
   {
    "Value": "true",
    "Code": "135"
   },
   {
    "Value": "all",
    "Code": "136"
   },
   {
```

```
 "Value": "true",
 "Code": "137"
},
{
 "Value": "true",
 "Code": "138"
},
{
 "Value": "30",
 "Code": "139"
},
{
 "Value": "3",
 "Code": "140"
},
{
 "Value": "true",
 "Code": "141"
},
{
 "Value": "3",
 "Code": "142"
},
{
 "Value": "true",
 "Code": "143"
},
{
 "Value": "50",
 "Code": "144"
},
{
 "Value": "true",
 "Code": "145"
},
{
 "Value": "true",
 "Code": "146"
},
{
 "Value": "true",
 "Code": "147"
},
{
 "Value": "false",
 "Code": "148"
},
{
 "Value": "true",
 "Code": "149"
},
{
 "Value": "true",
 "Code": "150"
}
```

```
},
{
 "Value": "true",
 "Code": "151"
},
{
 "Value": "200",
 "Code": "152"
},
{
 "Value": "true",
 "Code": "153"
},
{
 "Value": "true",
 "Code": "154"
},
{
 "Value": "true",
 "Code": "155"
},
{
 "Value": "true",
 "Code": "156"
},
{
 "Value": "true",
 "Code": "157"
},
{
 "Value": "50",
 "Code": "158"
},
{
 "Value": "true",
 "Code": "159"
},
{
 "Value": "3",
 "Code": "160"
},
{
 "Value": "wafnext",
 "Code": "161"
},
{
 "Value": "200",
 "Code": "162"
},
{
 "Value": "200",
 "Code": "163"
},
{
 "Value": "200",
```

```
 "Code": "164"
},
{
 "Value": "false",
 "Code": "165"
},
{
 "Value": "IP,Session,Param,Cookie,Header",
 "Code": "166"
},
{
 "Value": "true",
 "Code": "167"
},
{
 "Value": "true",
 "Code": "200"
},
{
 "Value": "1",
 "Code": "168"
},
{
 "Value": "50",
 "Code": "201"
},
{
 "Value": "true",
 "Code": "169"
},
{
 "Value": "true",
 "Code": "202"
},
{
 "Value": "false",
 "Code": "203"
},
{
 "Value": "100",
 "Code": "204"
},
{
 "Value": "50",
 "Code": "205"
},
{
 "Value": "true",
 "Code": "170"
},
{
 "Value": "true",
 "Code": "171"
},
```

```
{
 "Value": "50",
 "Code": "172"
},
{
 "Value": "true",
 "Code": "173"
},
{
 "Value": "5",
 "Code": "174"
},
{
 "Value": "500",
 "Code": "175"
},
{
 "Value": "true",
 "Code": "176"
},
{
 "Value": "true",
 "Code": "177"
},
{
 "Value": "custom",
 "Code": "178"
},
{
 "Value": "true",
 "Code": "179"
},
{
 "Value": "true",
 "Code": "180"
},
{
 "Value": "50",
 "Code": "181"
},
{
 "Value": "false",
 "Code": "182"
},
{
 "Value": "true",
 "Code": "183"
},
{
 "Value": "true",
 "Code": "184"
},
{
 "Value": "false",
```

```
 "Code": "185"
},
{
 "Value": "true",
 "Code": "186"
},
{
 "Value": "true",
 "Code": "187"
},
{
 "Value": "true",
 "Code": "100"
},
{
 "Value": "true",
 "Code": "188"
},
{
 "Value": "5000",
 "Code": "101"
},
{
 "Value": "true",
 "Code": "189"
},
{
 "Value": "500000",
 "Code": "102"
},
{
 "Value": "1200",
 "Code": "103"
},
{
 "Value": "true",
 "Code": "104"
},
{
 "Value": "200",
 "Code": "105"
},
{
 "Value": "20",
 "Code": "106"
},
{
 "Value": "true",
 "Code": "107"
},
{
 "Value": "true",
 "Code": "108"
},
```

```
    {
     "Value": "true",
     "Code": "109"
    }
  ],
  "RequestId": "E906513E-F6B5-495E-98DC-7BA888671D76",
  "InstanceId": "waf-cn-st22251****",
  "Version": "version_hybrid_cloud_standard",
  "ExpireTime": "1677168000000"
}
```


错误码

访问错误中心查看更多错误码。

4.3. DeleteInstance

调用DeleteInstance释放Web应用防火墙（WAF）按量付费实例或者到期的包年包月实例。

释放实例后，实例的相关数据将全部丢失且不可恢复，请谨慎操作。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteInstance	系统规定参数。 取值：DeleteInstance。
InstanceId	String	是	waf_elasticity-cn-0xldbqt****	WAF实例ID。
ResourceGroupId	String	否	rg-atstuj3rtop****	相关的资源组ID。 默认为空，表示属于默认资源组。

返回数据

名称	类型	示例值	描述
RequestId	String	F35F45B0-5D6B-4238-BE02-A62D0760E840	阿里云为此次API调用请求生成的唯一标识符。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteInstance
&InstanceId=waf_elasticity-cn-0xldbqt****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DeleteInstanceResponse>
  <RequestId>F35F45B0-5D6B-4238-BE02-A62D0760E840</RequestId>
</DeleteInstanceResponse>
```

`JSON` 格式

```
{"RequestId":"F35F45B0-5D6B-4238-BE02-A62D0760E840"}
```

错误码

访问错误中心查看更多错误码。

5.域名配置

5.1. DescribeDomainList

调用DescribeDomainList分页查询已添加到WAF防护的域名列表。

> **说明** DescribeDomainNames接口也可以用于查询已添加到WAF防护的所有域名，但是不支持分页查询（即只能一次性返回所有域名）。对于域名数量较多的场景，推荐您调用该接口进行分页查询（分页显示结果并支持按条件查询）。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainList	要执行的操作。取值：**DescribeDomainList**。
InstanceId	String	是	waf-cn-7pp26f1****	WAF实例的ID。 > **说明** 您可以调用DescribeInstanceInfo，查看当前WAF实例的ID。
ResourceGroupId	String	否	rg-acfm2pz25js****	WAF实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。 关于资源组的更多信息，请参见创建资源组。
DomainName	String	否	example.com	要查询的域名名称。 您可以设置该参数，模糊查询某个域名是否已接入WAF防护。
DomainNames.N	RepeatList	否	example.com	要查询的域名列表。 您可以设置该参数，模糊查询多个域名是否已接入WAF防护。

名称	类型	是否必选	示例值	描述
PageNumber	Integer	否	1	分页查询时，返回第几页数据。默认值为**1**，表示返回第1页数据。
PageSize	Integer	否	10	分页查询时，每页包含多少条结果。默认值为**10**，表示每页包含10条结果。
IsSub	Integer	否	0	要查询的域名类型。取值： • **0**（默认）：表示查询所有域名（包含具体域名和泛域名）。 • **1**：表示仅查询具体域名。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
DomainNames	List	["www.example.com","test.example.com"]	查询到的域名列表。
RequestId	String	592E866F-6C05-4E7C-81DE-B4D8E86B91EF	本次请求的ID。
TotalCount	Integer	2	查询到的域名的数量。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainList
&InstanceId=waf-cn-7pp26f1****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDomainListResponse>
    <TotalCount>2</TotalCount>
    <RequestId>592E866F-6C05-4E7C-81DE-B4D8E86B91EF</RequestId>
    <DomainNames>www.example.com</DomainNames>
    <DomainNames>test.example.com</DomainNames>
</DescribeDomainListResponse>
```

`JSON` 格式

```
{
  "TotalCount": 2,
  "RequestId": "592E866F-6C05-4E7C-81DE-B4D8E86B91EF",
  "DomainNames": [
    "www.example.com",
    "test.example.com"
  ]
}
```

错误码

访问错误中心查看更多错误码。

5.2. DescribeDomainNames

调用DescribeDomainNames接口获取指定WAF实例中已添加的域名名称列表。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainNames	要执行的操作。取值：**DescribeDomainNames**。
InstanceId	String	是	waf_elasticity-cn-0xldbqt****	WAF实例ID。 **说明** 您可以通过调用DescribeInstanceInfo接口查看当前WAF实例ID。
ResourceGroupId	String	否	rg-atstuj3rtop****	域名在资源管理产品中所属的资源组ID。默认为空，即属于默认资源组。

返回数据

名称	类型	示例值	描述
DomainNames	List	["1.example.com","2.example.com","3.example.com"]	已添加的域名名称列表。
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	请求ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainNames
&InstanceId=waf_elasticity-cn-0xldbqt****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDomainNamesResponse>
   <DomainNames>1.example.com</DomainNames>
   <DomainNames>2.example.com</DomainNames>
   <DomainNames>3.example.com</DomainNames>
   <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</DescribeDomainNamesResponse>
```

`JSON` 格式

```
{
    "DomainNames": [
        "1.example.com",
        "2.example.com",
        "3.example.com"
    ],
    "RequestId": "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

5.3. DescribeDomain

调用DescribeDomain查询已添加到WAF防护的域名的配置信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomain	要执行的动作。取值：**DescribeDomain**。
Domain	String	是	www.example.com	要查询的域名名称。 **说明** 您可以调用DescribeDomainNames查询所有已添加到WAF防护的域名。
InstanceId	String	是	waf-cn-7pp26f1****	WAF实例的ID。 **说明** 您可以调用DescribeInstanceInfo查询当前WAF实例的ID。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	D827FCFE-90A7-4330-9326-D33C8B4C7726	本次请求的ID。
Domain	Struct		域名的配置信息。
AccessHeaderMode	Integer	1	WAF获取客户端真实IP的方式。取值： • **0**：表示WAF读取请求头中X-Forwarded-For（XFF）字段的第一个值作为客户端IP。 • **1**：表示WAF读取请求头中由您设置的自定义字段值作为客户端IP。 **说明** 仅当IsAccessProduct取值为1（表示WAF前有其他七层代理服务）时，返回该参数。

名称	类型	示例值	描述
AccessHeaders	List	["X-Client-IP"]	用于获取客户端IP的自定义字段列表。 **说明** 仅当AccessHeaderMode取值为1（表示WAF读取请求头中由您设置的自定义字段值作为客户端IP）时，返回该参数。
AccessType	String	waf-cloud-dns	域名接入方式。取值： • **waf-cloud-dns**：表示CNAME接入。 • **waf-cloud-native**：表示透明接入。
CloudNativeInstances	Array of CloudNativeInstances		透明接入的配置列表。 **说明** 仅当AccessType取值为waf-cloud-native（表示域名使用透明接入方式接入WAF）时，返回该参数。
CloudNativeProductName	String	ALB	云产品实例的类型。取值： • **SLB**：表示传统型负载均衡CLB（原SLB）实例。 • **ECS**：表示云服务器ECS实例。 • **ALB**：表示应用型负载均衡ALB实例。
IPAddressList	String	["39.XX.XX.197"]	云产品实例的公网IP地址列表。
InstanceId	String	alb-s65nua68wdedsp****	云产品实例的ID。
ProtocolPortConfigs	Array of ProtocolPortConfigs		协议及端口配置列表。
Ports	String	[80]	端口列表。
Protocol	String	http	协议类型。取值： • **http**：表示HTTP协议。 • **https**：表示HTTPS协议。

名称	类型	示例值	描述
RedirectionTypeName	String	ALB	引流端口的类型。取值： • **SLB-L4**：表示从传统型负载均衡CLB（原SLB）实例的四层监听端口引流到WAF进行防护。 • **SLB-L7**：表示从传统型负载均衡CLB（原SLB）实例的七层监听端口引流到WAF进行防护。 • **ECS**：表示从云服务器ECS实例的监听端口引流到WAF进行防护。 • **ALB**：表示从应用型负载均衡ALB实例的HTTP、HTTPS监听端口引流到WAF进行防护。
ClusterType	Integer	0	WAF实例对应的集群类型。取值： • **0**：表示物理集群。 • **1**：表示虚拟集群，即WAF独享集群。 **说明** 仅当AccessType取值为**waf-cloud-dns**（表示域名使用CNAME接入方式接入WAF）时，返回该参数。
Cname	String	kdmqyi3ck7xogegxpiyfpb0fj21mgkxn.****.com	WAF为域名分配的CNAME地址。 **说明** 仅当AccessType取值为**waf-cloud-dns**（表示域名使用CNAME接入方式接入WAF）时，返回该参数。
ConnectionTime	Integer	5	WAF集群的连接超时时长。单位：秒。 **说明** 仅当AccessType取值为**waf-cloud-dns**（表示域名使用CNAME接入方式接入WAF）时，返回该参数。
Http2Port	List	[443,8443]	HTTP 2.0端口列表。 **说明** 仅当AccessType取值为**waf-cloud-dns**（表示域名使用CNAME接入方式接入WAF）且**HttpsPort**取值不为空（表示域名使用HTTPS协议）时，返回该参数。

名称	类型	示例值	描述
HttpPort	List	[80]	HTTP端口列表。 **说明** 仅当AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式接入WAF）时，返回该参数。
HttpToUserIp	Integer	0	是否开启了HTTP回源功能。取值： • **0**：表示未开启。 • **1**：表示已开启。 **说明** 仅当AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式接入WAF）且HttpsPort取值不为空（表示域名使用HTTPS协议）时，返回该参数。
HttpsPort	List	[443,8443]	HTTPS端口列表。 **说明** 仅当AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式接入WAF）时，返回该参数。
HttpsRedirect	Integer	0	是否开启了HTTPS强制跳转。取值： • **0**：表示未开启。 • **1**：表示已开启。 **说明** 仅当AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式接入WAF）且HttpsPort取值不为空（表示域名使用HTTPS协议）时，返回该参数。

名称	类型	示例值	描述
IpFollowStatus	Integer	1	是否开启了IPv4/IPv6回源协议跟随。取值： • **0**：表示未开启。 • **1**：表示已开启。 **说明** 仅当AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式接入WAF）时，返回该参数。
IsAccessProduct	Integer	1	域名在WAF前是否配置有其他七层代理（例如高防、CDN等），即客户端访问流量到WAF前是否有经过其他七层代理转发。取值： • **0**：表示否。 • **1**：表示是。
LoadBalancing	Integer	2	回源时采用的负载均衡算法。取值： • **0**：表示IP Hash算法。 • **1**：表示轮询算法。 • **2**：表示Least Time算法。 **说明** 仅当AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式接入WAF）时，返回该参数。
LogHeaders	Array of LogHeader		域名的流量标记字段和值，用于标记经过WAF处理的流量。 **说明** 仅当域名开启了流量标记功能时，返回该参数。
k	String	ALIWAF-TAG	流量标记字段的名称。
v	String	Yes	流量标记字段的值。
ReadTime	Integer	120	WAF集群的读连接超时时长。单位：秒。 **说明** 仅当AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式接入WAF）时，返回该参数。

名称	类型	示例值	描述
ResourceGroupId	String	rg-acfm2mkrunv****	WAF实例所属资源组ID。
SniHost	String	waf.example.com	SNI扩展字段的自定义值。取值为空表示未自定义SNI值，默认使用请求头中**Host**字段的值作为SNI扩展字段的值。 **说明** 仅在SniStatus取值为1（表示开启SNI回源）时，返回该参数。
SniStatus	Integer	1	是否开启了回源SNI。回源SNI表示WAF转发客户端请求到源站服务器，在与源站进行TLS握手时，通过SNI扩展字段（Server Name Indicator extension）指定要访问的主机，并与该主机建立HTTPS连接。取值： • **0**：表示未开启。 • **1**：表示已开启。 **说明** 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）且HttpsPort取值不为空（表示域名使用HTTPS协议）时，返回该参数。
SourceIps	List	["39.XX.XX.197"]	源站服务器地址。 **说明** 仅当AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式接入WAF）时，返回该参数。
Version	Long	40	当前域名配置的版本。
WriteTime	Integer	120	WAF集群的写连接超时时长。单位：秒。 **说明** 仅当AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式接入WAF）时，返回该参数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomain
&Domain=www.example.com
&InstanceId=waf-cn-7pp26f1****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeDomainResponse>
   <RequestId>D827FCFE-90A7-4330-9326-D33C8B4C7726</RequestId>
   <Domain>
      <HttpToUserIp>0</HttpToUserIp>
      <HttpPort>80</HttpPort>
      <IsAccessProduct>1</IsAccessProduct>
      <AccessHeaderMode>1</AccessHeaderMode>
      <ResourceGroupId>rg-acfm2mkrunv****</ResourceGroupId>
      <AccessHeaders>X-Client-IP</AccessHeaders>
      <ReadTime>120</ReadTime>
      <SourceIps>39.XX.XX.197</SourceIps>
      <IpFollowStatus>1</IpFollowStatus>
      <ClusterType>0</ClusterType>
      <LoadBalancing>2</LoadBalancing>
      <Cname>kdmqyi3ck7xogegxpiyfpb0fj21mgkxn.****.com</Cname>
      <LogHeaders>
         <v>Yes</v>
         <k>ALIWAF-TAG</k>
      </LogHeaders>
      <WriteTime>120</WriteTime>
      <Http2Port>443</Http2Port>
      <Http2Port>8443</Http2Port>
      <Version>40</Version>
      <HttpsRedirect>0</HttpsRedirect>
      <ConnectionTime>5</ConnectionTime>
      <AccessType>waf-cloud-dns</AccessType>
      <HttpsPort>443</HttpsPort>
      <HttpsPort>8443</HttpsPort>
   </Domain>
</DescribeDomainResponse>
```

`JSON` 格式

```
{
  "RequestId": "D827FCFE-90A7-4330-9326-D33C8B4C7726",
  "Domain": {
    "HttpToUserIp": 0,
    "HttpPort": [
      80
    ],
    "IsAccessProduct": 1,
    "AccessHeaderMode": 1,
    "ResourceGroupId": "rg-acfm2mkrunv****",
    "AccessHeaders": [
      "X-Client-IP"
    ],
    "ReadTime": 120,
    "SourceIps": [
      "39.XX.XX.197"
    ],
    "IpFollowStatus": 1,
    "ClusterType": 0,
    "LoadBalancing": 2,
    "Cname": "kdmqyi3ck7xogegxpiyfpb0fj21mgkxn.****.com",
    "LogHeaders": [
      {
        "v": "Yes",
        "k": "ALIWAF-TAG"
      }
    ],
    "WriteTime": 120,
    "Http2Port": [
      443,
      8443
    ],
    "Version": 40,
    "HttpsRedirect": 0,
    "ConnectionTime": 5,
    "AccessType": "waf-cloud-dns",
    "HttpsPort": [
      443,
      8443
    ]
  }
}
```


错误码

访问错误中心查看更多错误码。

5.4. CreateDomain

调用CreateDomain添加域名配置信息，将您的域名接入WAF实例进行防护。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateDomain	要执行的操作。取值：**CreateDomain**。
InstanceId	String	是	waf-cn-7pp26f1****	WAF实例的ID。 **说明** 您可以调用DescribeInstanceInfo查询当前WAF实例的ID。
Domain	String	是	www.example.com	要添加到WAF防护的域名。
IsAccessProduct	Integer	是	0	域名在WAF前是否配置有七层代理（例如高防、CDN等），即客户端访问流量到WAF前是否有经过其他七层代理转发。取值： • **0**：表示否。 • **1**：表示是。
AccessHeaderMode	Integer	否	0	WAF获取客户端真实IP的方式。取值： • **0**（默认）：表示WAF读取请求头中X-Forwarded-For（XFF）字段的第一个值作为客户端IP。 • **1**：表示WAF读取请求头中由您设置的自定义字段值作为客户端IP。 **说明** 仅在IsAccessProduct取值为1（表示WAF前有其他七层代理服务）时，需要设置该参数。

名称	类型	是否必选	示例值	描述
AccessHeaders	String	否	["X-Client-IP"]	设置用于获取客户端IP的自定义字段列表，使用 `["header1","header2",……]` 格式表示。 **说明** 仅在AccessHeaderMode取值为1（表示WAF读取请求头中由您设置的自定义字段值作为客户端IP）时，需要设置该参数。
LogHeaders	String	否	[{"k":"ALIWAF-TAG","v":"Yes"}]	域名的流量标记字段和值，用于标记经过WAF处理的流量。 该参数值的格式为 `[{"k":"_key_","v":"_value_"}]`。其中，`_key_` 表示所指定的自定义请求头部字段，`_value_` 表示为该字段设定的值。 通过指定自定义请求头部字段和对应的值，当域名的访问流量经过WAF时，WAF自动在请求头部中添加所设定的自定义字段值作为流量标记，便于后端服务统计相关信息。 **说明** 如果请求中已存在该自定义头部字段，系统将用所设定的流量标记值覆盖请求中该自定义字段的值。
ResourceGroupId	String	否	rg-atstuj3rtop****	WAF实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。 关于资源组的更多信息，请参见创建资源组。
AccessType	String	否	waf-cloud-dns	域名接入方式。取值： - **waf-cloud-dns**（默认）：表示CNAME接入。 - **waf-cloud-native**：表示透明接入。

名称	类型	是否必选	示例值	描述
HttpPort	String	否	[80]	HTTP协议端口列表，使用 `[port1,port2,……]` 格式表示。 **说明** 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）时，需要设置该参数。设置该参数表示域名使用HTTP协议。HttpPort与HttpsPort不允许同时为空。
HttpsPort	String	否	[443]	HTTPS协议端口列表，使用 `[port1,port2,……]` 格式表示。 **说明** 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）时，需要设置该参数。设置该参数表示域名使用HTTPS协议。HttpPort与HttpsPort不允许同时为空。
HttpsRedirect	Integer	否	0	是否开启HTTPS强制跳转。开启强制跳转后，客户端的HTTP请求将被强制跳转成HTTPS请求，默认跳转端口为443。取值： • 0（默认）：表示关闭。 • 1：表示开启。 **说明** 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）且HttpsPort取值不为空（表示域名使用HTTPS协议）时，需要设置该参数。
Http2Port	String	否	[443]	HTTP 2.0协议端口列表，使用 `[port1,port2,……]` 格式表示。 **说明** 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）且HttpsPort取值不为空（表示域名使用HTTPS协议）时，需要设置该参数。

名称	类型	是否必选	示例值	描述
HttpToUserIp	Integer	否	0	是否开启HTTP回源。开启HTTP回源后，HTTPS访问请求将通过HTTP协议转发回源站，默认回源端口为80。取值： • 0（默认）：表示关闭。 • 1：表示开启。 说明 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）且HttpsPort取值不为空（表示域名使用HTTPS协议）时，需要设置该参数。
IpFollowStatus	Integer	否	1	源站服务器地址同时包含IPv4和IPv6地址时，是否开启IPv4/IPv6回源协议跟随。开启回源协议跟随后，WAF将来自IPv4地址的请求转发到IPv4源站、将来自IPv6地址的请求转发到IPv6源站。取值： • 0（默认）：表示关闭。 • 1：表示开启。 说明 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）时，需要设置该参数。
SourceIps	String	否	["39.XX.XX.197"]	域名对应的源站服务器IP或服务器回源域名。您只能选择设置源站服务器IP或服务器回源域名中的一种： • 设置源站服务器IP时，使用 `["ip1","ip2",……]` 格式表示。最多支持添加20个IP。 • 设置服务器回源域名时，使用 `["domain"]` 格式表示。只能填写1个域名地址。 说明 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）时，需要设置该参数。

名称	类型	是否必选	示例值	描述
LoadBalancing	Integer	否	0	回源时采用的负载均衡算法。取值： • 0：表示IP Hash算法。 • 1：表示轮询算法。 • 2：表示Least Time算法。 说明 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）时，需要设置该参数。
ClusterType	Integer	否	0	WAF防护集群类型。取值： • 0（默认）：表示物理集群。 • 1：表示虚拟集群，即WAF独享集群。 说明 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）时，需要设置该参数。
ConnectionTime	Integer	否	5	WAF独享集群的连接超时时长。单位：秒。 说明 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）且ClusterType取值为1（表示域名使用WAF独享集群）时，需要设置该参数。
ReadTime	Integer	否	120	WAF独享集群的读连接超时时长。单位：秒。 说明 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）且ClusterType取值为1（表示域名使用WAF独享集群）时，需要设置该参数。

名称	类型	是否必选	示例值	描述
WriteTime	Integer	否	120	WAF独享集群的写连接超时时长。单位：秒。 **说明** 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）且ClusterType取值为1（表示域名使用WAF独享集群）时，需要设置该参数。

CloudNativeInstances	String	否	[{"ProtocolPortConfigs":[{"Ports":[80],"Protocol":"http"}],"RedirectionTypeName":"ALB","InstanceId":"alb-s65nua68wdedsp****","IPAddressList":["182.XX.XX.113"],"CloudNativeProductName":"ALB"}]	透明接入的服务器及端口配置列表。使用JSON数组转化的字符串格式表示。JSON数组中的每个元素是一个结构体，包含以下字段：
				• **ProtocolPortConfigs**：JSON Array类型 | 必选 | 表示协议及端口配置列表。JSON数组中的每个元素是一个结构体，包含以下字段：
				  ○ **Ports**：Array类型 | 必选 | 表示端口列表，格式为 `[port1,port2,……]`。
				  ○ **Protocol**：String类型 | 必选 | 表示协议类型。取值：**http**、**https**。
				• **CloudNativeProductName**：String类型 | 必选 | 表示云产品实例的类型。取值：**ECS**、**SLB**、**ALB**。
				• **RedirectionTypeName**：String类型 | 必选 | 表示引流端口的类型。取值：**ECS**（表示ECS端口）、**SLB-L4**（表示SLB四层端口）、**SLB-L7**（表示SLB七层端口）、**ALB**（表示ALB端口）。
				• **InstanceId**：String类型 | 必选 | 表示云产品实例的ID。
				• **IPAddressList**：Array类型 | 必选 | 表示云产品实例的公网IP列表。格式为 `["ip1","ip2",……]`。
				说明 仅在AccessType为waf-cloud-native（表示域名使用透明接入方式）时，需要设置该参数。

名称	类型	是否必选	示例值	描述
SniStatus	Integer	否	1	设置是否开启回源SNI。回源SNI表示WAF转发客户端请求到源站服务器，在与源站进行TLS握手时，通过SNI扩展字段（Server Name Indicator extension）指定要访问的主机，并与该主机建立HTTPS连接。如果您的源站服务器有多个虚拟主机（对应不同域名），则您需要开启回源SNI。取值： • 0：表示关闭。 • 1：表示开启。 中国内地WAF实例默认关闭SNI回源；海外地区WAF实例默认开启SNI回源。 说明 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）且HttpsPort取值不为空（表示域名使用HTTPS协议）时，需要设置该参数。
SniHost	String	否	waf.example.com	自定义SNI扩展字段的值。如果不设置该参数，则默认使用请求头中Host字段的值作为SNI扩展字段的值。 一般情况无需自定义SNI，除非您的业务有特殊配置要求，希望WAF在回源请求中使用与实际请求Host不一致的SNI（即此处设置的自定义SNI）。 说明 仅在SniStatus取值为1（表示开启SNI回源）时，需要设置该参数。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述

名称	类型	示例值	描述
Cname	String	mmspx7qhfvnfzggheh1g2wnbhog66vcv.****.com	WAF为域名分配的CNAME地址。 **说明** 仅当域名使用CNAME接入方式（请求参数AccessType取值为waf-cloud-dns）时，返回该参数。
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateDomain
&InstanceId=waf-cn-7pp26f1****
&Domain=www.example.com
&IsAccessProduct=0
&HttpPort=[\"80\"]
&SourceIps=[\"39.XX.XX.197\"]
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<CreateDomainResponse>
   <Cname>mmspx7qhfvnfzggheh1g2wnbhog66vcv.****.com</Cname>
   <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</CreateDomainResponse>
```

`JSON` 格式

```
{
 "Cname": "mmspx7qhfvnfzggheh1g2wnbhog66vcv.****.com",
 "RequestId": "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

5.5. ModifyDomain

调用ModifyDomain修改已创建的域名配置。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyDomain	要执行的操作。取值：**ModifyDomain**。
Domain	String	是	www.example.com	要操作的域名。 **说明** 您可以调用DescribeDomainNames查询所有已添加到WAF防护的域名。
InstanceId	String	是	waf-cn-7pp26f1****	WAF实例的ID。 **说明** 您可以调用DescribeInstanceInfo查询当前WAF实例的ID。
IsAccessProduct	Integer	是	0	域名在WAF前是否配置有七层代理（例如高防、CDN等），即客户端访问流量到WAF前是否有经过其他七层代理转发。取值： • **0**：表示否。 • **1**：表示是。

名称	类型	是否必选	示例值	描述
SourceIps	String	否	["39.XX.XX.197"]	域名对应的源站服务器IP或服务器回源域名。您只能选择设置源站服务器IP或服务器回源域名中的一种： • 设置源站服务器IP时，使用 `["ip1","ip2",……]` 格式表示。最多支持添加20个IP。 • 设置服务器回源域名时，使用 `["domain"]` 格式表示。只能填写1个域名地址。 **说明** 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）时，需要设置该参数。
LoadBalancing	Integer	否	0	回源时采用的负载均衡算法。取值： • **0**：表示IP Hash算法。 • **1**：表示轮询算法。 • **2**：表示Least Time算法。 **说明** 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）时，需要设置该参数。
HttpPort	String	否	[80]	HTTP协议端口列表，使用 `[port1,port2,……]` 格式表示。 **说明** 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）时，需要设置该参数。设置该参数表示域名使用HTTP协议。HttpPort与HttpsPort不允许同时为空。

名称	类型	是否必选	示例值	描述
HttpsPort	String	否	[443]	HTTPS协议端口列表，使用 `[port1,port2,……]` 格式表示。 **说明** 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）时，需要设置该参数。设置该参数表示域名使用HTTPS协议。HttpPort与HttpsPort不允许同时为空。
Http2Port	String	否	[443]	HTTP 2.0协议端口列表，使用 `[port1,port2,……]` 格式表示。 **说明** 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）且HttpsPort取值不为空（表示域名使用HTTPS协议）时，需要设置该参数。
HttpsRedirect	Integer	否	0	是否开启HTTPS强制跳转。开启强制跳转后，客户端的HTTP请求将被强制跳转成HTTPS请求，默认跳转端口为443。取值： • 0（默认）：表示关闭。 • 1：表示开启。 **说明** 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）且HttpsPort取值不为空（表示域名使用HTTPS协议）时，需要设置该参数。
HttpToUserIp	Integer	否	0	是否开启HTTP回源。开启HTTP回源后，HTTPS访问请求将通过HTTP协议转发回源站，默认回源端口为80。取值： • 0（默认）：表示关闭。 • 1：表示开启。 **说明** 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）且HttpsPort取值不为空（表示域名使用HTTPS协议）时，需要设置该参数。

名称	类型	是否必选	示例值	描述
AccessHeaderMode	Integer	否	0	WAF获取客户端真实IP的方式。取值： • 0（默认）：表示WAF读取请求头中X-Forwarded-For（XFF）字段的第一个值作为客户端IP。 • 1：表示WAF读取请求头中由您设置的自定义字段值作为客户端IP。 **说明** 仅在IsAccessProduct取值为1（表示WAF前有其他七层代理服务）时，需要设置该参数。
AccessHeaders	String	否	["X-Client-IP"]	设置用于获取客户端IP的自定义字段列表，使用 `["header1","header2",……]` 格式表示。 **说明** 仅在AccessHeaderMode取值为1（表示WAF读取请求头中由您设置的自定义字段值作为客户端IP）时，需要设置该参数。
LogHeaders	String	否	[{"k":"ALIWAF-TAG","v":"Yes"}]	域名的流量标记字段和值，用于标记经过WAF处理的流量。 该参数值的格式为 `[{"k":"_key_","v":"_value_"}]`。其中，`_key_` 表示所指定的自定义请求头部字段，`_value_` 表示为该字段设定的值。 通过指定自定义请求头部字段和对应的值，当域名的访问流量经过WAF时，WAF自动在请求头部中添加所设定的自定义字段值作为流量标记，便于后端服务统计相关信息。 **说明** 如果请求中已存在该自定义头部字段，系统将用所设定的流量标记值覆盖请求中该自定义字段的值。

名称	类型	是否必选	示例值	描述
ClusterType	Integer	否	0	WAF防护集群类型。取值： • 0（默认）：表示物理集群。 • 1：表示虚拟集群，即WAF独享集群。 说明 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）时，需要设置该参数。
ConnectionTime	Integer	否	5	WAF独享集群的连接超时时长。单位：秒。 说明 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）且ClusterType取值为1（表示使用WAF独享集群）时，需要设置该参数。
ReadTime	Integer	否	120	WAF独享集群的读连接超时时长。单位：秒。 说明 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）且ClusterType取值为1（表示使用WAF独享集群）时，需要设置该参数。
WriteTime	Integer	否	120	WAF独享集群的写连接超时时长。单位：秒。 说明 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）且ClusterType取值为1（表示使用WAF独享集群）时，需要设置该参数。
AccessType	String	否	waf-cloud-dns	域名接入方式。取值： • waf-cloud-dns（默认）：表示CNAME接入。 • waf-cloud-native：表示透明接入。

名称	类型	是否必选	示例值	描述

CloudNativeInstances	String	否	[{"ProtocolPortConfigs":[{"Ports":[80],"Protocol":"http"}],"RedirectionTypeName":"ALB","InstanceId":"alb-s65nua68wdedsp****","IPAddressList":["182.XX.XX.113"],"CloudNativeProductName":"ALB"}]	透明接入的服务器及端口配置列表。使用JSON数组转化的字符串格式表示。JSON数组中的每个元素是一个结构体，包含以下字段：
				• **ProtocolPortConfigs**：JSON Array类型 | 必选 | 表示协议及端口配置列表。JSON数组中的每个元素是一个结构体，包含以下字段：
				  ○ **Ports**：Array类型 | 必选 | 表示端口列表，格式为 `[port1,port2,……]`。
				  ○ **Protocol**：String类型 | 必选 | 表示协议类型。取值：**http**、**https**。
				• **CloudNativeProductName**：String类型 | 必选 | 表示云产品实例的类型。取值：**ECS**、**SLB**、**ALB**。
				• **RedirectionTypeName**：String类型 | 必选 | 表示引流端口的类型。取值：**ECS**（表示ECS端口）、**SLB-L4**（表示SLB四层端口）、**SLB-L7**（表示SLB七层端口）、**ALB**（表示ALB端口）。
				• **InstanceId**：String类型 | 必选 | 表示云产品实例的ID。
				• **IPAddressList**：Array类型 | 必选 | 表示云产品实例的公网IP列表。格式为 `["ip1","ip2",……]`。
				说明 仅在AccessType取值为**waf-cloud-native**（表示域名使用透明接入方式）时，需要设置该参数。

IpFollowStatus	Integer	否	0	源站服务器地址同时包含IPv4和IPv6地址时，是否开启IPv4/IPv6回源协议跟随。开启回源协议跟随后，WAF将来自IPv4地址的请求转发到IPv4源站、将来自IPv6地址的请求转发到IPv6源站。取值： • **0**（默认）：表示关闭。 • **1**：表示开启。 **说明** 仅在AccessType取值为**waf-cloud-dns**（表示域名使用CNAME接入方式）时，需要设置该参数。

名称	类型	是否必选	示例值	描述
SniStatus	Integer	否	1	设置是否开启回源SNI。回源SNI表示WAF转发客户端请求到源站服务器，在与源站进行TLS握手时，通过SNI扩展字段（Server Name Indicator extension）指定要访问的主机，并与该主机建立HTTPS连接。如果您的源站服务器有多个虚拟主机（对应不同域名），则您需要开启回源SNI。取值： • 0：表示关闭。 • 1：表示开启。 中国内地WAF实例默认关闭SNI回源；海外地区WAF实例默认开启SNI回源。 说明 仅在AccessType取值为waf-cloud-dns（表示域名使用CNAME接入方式）且HttpsPort取值不为空（表示域名使用HTTPS协议）时，需要设置该参数。
SniHost	String	否	waf.example.com	自定义SNI扩展字段的值。如果不设置该参数，则默认使用请求头中Host字段的值作为SNI扩展字段的值。 一般情况无需自定义SNI，除非您的业务有特殊配置要求，希望WAF在回源请求中使用与实际请求Host不一致的SNI（即此处设置的自定义SNI）。 说明 仅在SniStatus取值为1（表示开启SNI回源）时，需要设置该参数。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyDomain
&InstanceId=waf-cn-7pp26f1****
&Domain=www.example.com
&IsAccessProduct=0
&HttpPort=[\"80\"]
&SourceIps=[\"39.XX.XX.197\"]
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<ModifyDomainResponse>
   <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</ModifyDomainResponse>
```

`JSON` 格式

```
{
    "RequestId": "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

5.6. DeleteDomain

调用DeleteDomain接口删除指定域名配置信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteDomain	要执行的操作。取值：**DeleteDomain**。
Domain	String	是	www.example.com	已接入WAF的域名名称。
InstanceId	String	是	waf_elasticity-cn-0xldbqt****	WAF实例ID。 **说明** 您可以通过调用DescribeInstanceInfo接口查看当前WAF实例ID。

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	请求ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteDomain
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqt****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DeleteDomainResponse>
   <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</DeleteDomainResponse>
```

`JSON` 格式

```
{
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

5.7. DescribeCertificates

调用DescribeCertificates查询域名关联的SSL证书列表。

使用说明

本接口用于查询域名关联的SSL证书列表（通过阿里云SSL证书服务购买、已上传到SSL证书服务进行托管），例如，证书的ID、名称、关联的域名、SAN（Subject Alternative Name）扩展属性等。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeCertificates	要执行的操作。取值：**DescribeCertificates**。
InstanceId	String	是	waf-cn-zz11sr5****	WAF实例的ID。 **说明** 您可以调用DescribeInstanceInfo获取当前WAF实例的ID。
Domain	String	否	www.aliyundoc.com	要查询关联SSL证书的域名。 不设置该参数表示查询所有域名关联的SSL证书。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	ECF65091-3704-55D5-BC88-EC208B0E238C	本次请求的ID。
Certificates	Array of Certificate		域名关联的SSL证书信息。
IsUsing	Boolean	false	是否是该域名当前所使用的证书。取值： • **true**：表示是。 • **false**：表示否。
CertificateName	String	*.aliyundoc.com	证书名称。
CertificateId	Long	2329260	证书ID。
CommonName	String	*.aliyundoc.com	证书绑定的域名。
Sans	Array of String	*.aliyundoc.com	证书绑定的其他域名。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeCertificates
&InstanceId=waf-cn-zz11sr5****
&Domain=www.aliyundoc.com
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeCertificatesResponse>
    <RequestId>ECF65091-3704-55D5-BC88-EC208B0E238C</RequestId>
    <Certificates>
        <IsUsing>false</IsUsing>
        <CertificateName>*.aliyundoc.com</CertificateName>
        <CertificateId>2329260</CertificateId>
        <CommonName>*.aliyundoc.com</CommonName>
        <Sans>*.aliyundoc.com</Sans>
    </Certificates>
</DescribeCertificatesResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "ECF65091-3704-55D5-BC88-EC208B0E238C",
  "Certificates" : [ {
    "IsUsing" : false,
    "CertificateName" : "*.aliyundoc.com",
    "CertificateId" : 2329260,
    "CommonName" : "*.aliyundoc.com",
    "Sans" : [ "*.aliyundoc.com" ]
  } ]
}
```

错误码

访问错误中心查看更多错误码。

5.8. DescribeCertMatchStatus

调用DescribeCertMatchStatus接口检查指定域名配置上传的证书和私钥信息是否匹配。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeCertMatchStatus	要执行的操作。取值：**DescribeCertMatchStatus**。
Certificate	String	是	-----BEGIN CERTIFICATE----- 62EcYPWd2Oy1vs6MTXcJSfN9Z7rZ9fmxWr2BFN2XbahgnsSXM48ixZJ4krc+1M+j2kcubVpsE2cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOkjgvhlqt9vc65Cgb4mL+n5+DV9uOyTZTW/MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvIAqYxXZ7wRwWWmv4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg== -----END CERTIFICATE-----	证书文件内容。
Domain	String	是	www.example.com	已接入WAF的域名名称。
InstanceId	String	是	waf_elasticity-cn-0xldbqt****	WAF实例ID。 **说明** 您可以通过调用DescribeInstanceInfo接口查看当前WAF实例ID。

名称	类型	是否必选	示例值	描述
PrivateKey	String	是	-----BEGIN RSA PRIVATE KEY----- DADTPZoOHd9WtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThLyvsmLQKBgQCr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJaiygoIYoaMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04RtKadOw== -----END RSA PRIVATE KEY-----	私钥文件内容。

返回数据

名称	类型	示例值	描述
MatchStatus	Boolean	false	证书与私钥内容是否匹配。
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	请求ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeCertMatchStatus
&Certificate=-----BEGIN CERTIFICATE----- 62EcYPWd2Oy1vs6MTXcJSfN9Z7rZ9fmxWr2BFN2XbahgnsSXM48ixZJ4krc+1M+j2kcubVpsE2cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOkjgvhlqt9vc65Cgb4mL+n5+DV9uOyTZTW/MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvIAqYxXZ7wRwWWmv4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg== -----END CERTIFICATE-----
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqt****
&PrivateKey=-----BEGIN RSA PRIVATE KEY----- DADTPZoOHd9WtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThLyvsmLQKBgQCr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJaiygoIYoaMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04RtKadOw== -----END RSA PRIVATE KEY-----
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeCertMatchStatusResponse>
   <MatchStatus>false</MatchStatus>
   <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</DescribeCertMatchStatusResponse>
```

`JSON` 格式

```
{
    "MatchStatus": false,
    "RequestId": "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

5.9. CreateCertificate

调用CreateCertificate接口为已添加的域名配置记录上传证书及私钥信息。

> **说明** 您也可以调用该接口为指定域名配置更新已上传的证书及私钥信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateCertificate	要执行的操作。取值：**CreateCertificate**。
CertificateName	String	是	CertName	证书名称。
Domain	String	是	www.example.com	已接入WAF的域名名称。
InstanceId	String	是	waf_elasticity-cn-0xldbqt****	WAF实例ID。 **说明** 您可以通过调用DescribeInstanceInfo接口查看当前WAF实例ID。

名称	类型	是否必选	示例值	描述
PrivateKey	String	是	-----BEGIN RSA PRIVATE KEY----- DADTPZoOHd9WtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThLyvsmLQKBgQCr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJaiygoIYoaMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04RtKadOw== -----END RSA PRIVATE KEY-----	证书对应的私钥文件内容。
Certificate	String	否	-----BEGIN CERTIFICATE----- 62EcYPWd2Oy1vs6MTXcJSfN9Z7rZ9fmxWr2BFN2XbahgnsSXM48ixZJ4krc+1M+j2kcubVpsE2cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOkjgvhlqt9vc65Cgb4mL+n5+DV9uOyTZTW/MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvlAqYxXZ7wRwWWmv4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg== -----END CERTIFICATE-----	证书文件内容。
HttpsCertId	Long	否	123456	证书ID。

返回数据

名称	类型	示例值	描述
CertificateId	Long	2329260	系统自动生成的证书记录ID。
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	请求ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateCertificate
&CertificateName=CertName
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqt****
&PrivateKey=-----BEGIN RSA PRIVATE KEY----- DADTPZoOHd9WtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZ
L7Jt8zSDGM9sTMThLyvsmLQKBgQCr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBc
QJaiygoIYoaMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF
8bv5UK5G04RtKadOw== -----END RSA PRIVATE KEY-----
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<CreateCertificateResponse>
   <CertificateId>2329260</CertificateId>
   <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</CreateCertificateResponse>
```

`JSON` 格式

```
{
    "CertificateId": "2329260",
    "RequestId": "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

5.10. CreateCertificateByCertificateId

调用CreateCertificateByCertificateId，根据证书ID为指定域名添加SSL证书。

使用说明

本接口用于通过证书ID，为指定域名添加SSL证书。

调用本接口前，您可以调用DescribeCertificates查询域名关联的所有SSL证书的ID。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateCertificateByCertificateId	要执行的操作。取值：**CreateCertificateByCertificateId**。
Domain	String	是	www.aliyundoc.com	要添加SSL证书的域名。 **说明** 您可以调用DescribeDomainList查询所有已接入WAF防护的域名。
CertificateId	Long	否	3384669	要添加的证书的ID。 **说明** 您可以调用DescribeCertificates查询域名关联的所有SSL证书的ID。
InstanceId	String	是	waf-cn-zz11sr5****	WAF实例的ID。 **说明** 您可以调用DescribeInstanceInfo查询当前WAF实例的ID。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
CertificateId	Long	3384669	已添加的证书的ID。

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateCertificateByCertificateId
&Domain=www.aliyundoc.com
&CertificateId=3384669
&InstanceId=waf-cn-zz11sr5****
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<CreateCertificateByCertificateIdResponse>
    <CertificateId>3384669</CertificateId>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</CreateCertificateByCertificateIdResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "CertificateId" : 3384669,
  "RequestId" : "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

5.11. DescribeDomainBasicConfigs

调用DescribeDomainBasicConfigs查询已接入WAF防护的网站域名的基本配置。

使用说明

本接口用于分页查询已接入WAF防护的网站域名的基本配置（以下简称域名配置），例如，域名配置的状态、默认防护模块（包括规则防护引擎、CC安全防护、自定义防护策略）的状态和模式等。

QPS限制

本接口的单用户QPS限制为50次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainBasicConfigs	要执行的操作。取值：**DescribeDomainBasicConfigs**。
InstanceId	String	是	waf-cn-tl32ast****	WAF实例的ID。 **说明** 您可以调用DescribeInstanceInfo查询当前WAF实例的ID。
DomainKey	String	否	aliyundoc	设置域名关键字，查询包含指定关键字的域名配置。 不设置该参数表示查询所有域名配置。
AccessType	String	否	waf-cloud-dns	设置域名接入模式，查询使用指定方式接入WAF防护的域名配置。取值： • **waf-cloud-dns**：表示CNAME接入。 • **waf-cloud-native**：表示透明接入。 不设置该参数表示查询所有域名配置。
CloudNativeProductId	Integer	否	0	设置源站类型，查询在透明接入方式下通过指定源站类型接入WAF防护的域名配置。取值： • **0**：表示云服务器ECS实例。 • **1**：表示传统型负载均衡CLB实例。 • **2**：表示应用型负载均衡ALB实例。 不设置该参数表示查询所有域名配置。
PageNumber	Integer	否	1	分页查询时，设置当前页面的页码。默认值为1。

名称	类型	是否必选	示例值	描述
PageSize	Integer	否	10	分页查询时，设置每页包含域名配置的数量。默认值为**10**。
ResourceGroupId	String	否	rg-acfm2pz25js****	网站域名在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
TotalCount	Integer	1	查询到的域名配置的总数量。
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	本次请求的ID。
DomainConfigs	Array of DomainConfig		域名配置详情列表。
Status	Integer	1	域名配置的状态。取值： • **0**：表示无效（已删除）。 • **1**：表示有效（创建成功）。 • **10**：表示创建中。 • **11**：表示创建失败。 • **20**：表示删除中。
Domain	String	www.aliyundoc.com	域名。
Owner	String	WAF	域名配置的来源。取值固定为**WAF**，表示通过Web应用防火墙服务添加。
CcMode	Integer	0	CC安全防护功能的模式。取值： • **0**：表示**防护**模式。 • **1**：表示**防护-紧急**模式。

名称	类型	示例值	描述
CcStatus	Integer	1	CC安全防护功能的状态。取值： • **0**：表示关闭。 • **1**：表示开启。
AccessType	String	waf-cloud-dns	域名接入模式。取值： • **waf-cloud-dns**：表示CNAME接入。 • **waf-cloud-native**：表示透明接入。
Version	Long	0	当前配置的版本号。
AclStatus	Integer	1	自定义防护策略功能的状态。取值： • **0**：表示关闭。 • **1**：表示开启。
WafStatus	Integer	1	规则防护引擎功能的状态。取值： • **0**：表示关闭。 • **1**：表示开启。
WafMode	Integer	0	规则防护引擎功能的模式。取值： • **0**：表示**拦截**模式。 • **1**：表示**告警**模式。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainBasicConfigs
&InstanceId=waf-cn-tl32ast****
&PageNumber=1
&PageSize=10
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeDomainBasicConfigsResponse>
    <TotalCount>1</TotalCount>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <DomainConfigs>
        <Status>1</Status>
        <Domain>www.aliyundoc.com</Domain>
        <Owner>WAF</Owner>
        <CcMode>0</CcMode>
        <CcStatus>1</CcStatus>
        <Version>0</Version>
        <AclStatus>1</AclStatus>
        <WafStatus>1</WafStatus>
        <WafMode>0</WafMode>
    </DomainConfigs>
</DescribeDomainBasicConfigsResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "TotalCount" : 1,
  "RequestId" : "D7861F61-5B61-46CE-A47C-6B19160D5EB0",
  "DomainConfigs" : [ {
    "Status" : 1,
    "Domain" : "www.aliyundoc.com",
    "Owner" : "WAF",
    "CcMode" : 0,
    "CcStatus" : 1,
    "Version" : 0,
    "AclStatus" : 1,
    "WafStatus" : 1,
    "WafMode" : 0
  } ]
}
```

错误码

访问错误中心查看更多错误码。

5.12. DescribeDomainAdvanceConfigs

调用DescribeDomainAdvanceConfigs查询已添加到WAF防护的域名的详细配置。

使用说明

本接口用于查询已添加到WAF防护的域名的详细配置，例如，CNAME地址、源站服务器地址、HTTP和HTTPS端口列表等。

QPS限制

本接口的单用户QPS限制为50次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainAdvanceConfigs	要执行的操作。取值：**DescribeDomainAdvanceConfigs**。
InstanceId	String	是	waf-cn-2r427ng****	WAF实例的ID。 **说明** 您可以调用DescribeInstanceInfo查询当前WAF实例的ID。
DomainList	String	是	www.aliyundoc.com	要查询配置详情的域名。支持同时设置多个域名，多个域名间使用半角逗号（,）分隔。 **说明** 您可以调用DescribeDomainList查询所有已接入WAF防护的域名。
ResourceGroupId	String	否	rg-atstuj3rtop****	网站域名在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	本次请求的ID。
DomainConfigs	Array of DomainConfig		域名的详细配置信息。

名称	类型	示例值	描述
Domain	String	www.aliyundoc.com	域名。
Profile	Object		域名配置。
Http2Port	Array of Integer	443	HTTP 2.0端口。
Ipv6Status	Integer	1	是否开启IPv6安全防护。取值： • **0**：表示关闭。 • **1**：表示开启。
HttpPort	Array of Integer	80	HTTP端口。
GSLBStatus	String	on	是否启用智能负载均衡。取值： • **off**：表示否。 • **on**：表示是。
Rs	Array of String	38.XX.XX.42	源站服务器地址。
VipServiceStatus	Integer	0	当前使用的WAF实例IP（或WAF虚拟集群IP）的服务状态。取值： • **0**：表示正常。 • **1**：表示正在进行流量清洗。 • **2**：表示处于黑洞状态。
ClusterType	Integer	0	WAF实例的集群类别。取值： • **0**（默认）：表示物理集群。 • **1**：表示虚拟集群，即WAF独享集群。
ExclusiveVipStatus	Integer	0	是否使用独享IP。取值： • **0**：表示否。 • **1**：表示是。
Cname	String	****dsbpkt75zeiok5mta2j5l7hggcrm.****.com	WAF实例为该域名配置分配的CNAME地址。

名称	类型	示例值	描述
CertStatus	Integer	1	证书状态（即HTTPS协议状态）。取值： • **0**：表示异常，例如，未上传证书、上传的证书无效。 • **1**：表示正常，已上传证书且证书有效。
HttpsPort	Array of Integer	443	HTTPS端口。
ResolvedType	Integer	0	CNAME解析记录类型。取值： • **-1**：表示指向源站服务器。 • **0**：表示指向WAF实例IP。 • **1**：表示指向WAF虚拟集群IP。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainAdvanceConfigs
&InstanceId=waf-cn-2r427ng****
&DomainList=www.aliyundoc.com
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeDomainAdvanceConfigsResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <DomainConfigs>
        <Domain>www.aliyundoc.com</Domain>
        <Profile>
            <Http2Port>443</Http2Port>
            <Ipv6Status>1</Ipv6Status>
            <HttpPort>80</HttpPort>
            <GSLBStatus>on</GSLBStatus>
            <Rs>38.XX.XX.42</Rs>
            <VipServiceStatus>0</VipServiceStatus>
            <ClusterType>0</ClusterType>
            <ExclusiveVipStatus>0</ExclusiveVipStatus>
            <Cname>****dsbpkt75zeiok5mta2j5l7hggcrm.****.com</Cname>
            <CertStatus>1</CertStatus>
            <HttpsPort>443</HttpsPort>
            <ResolvedType>0</ResolvedType>
        </Profile>
    </DomainConfigs>
</DescribeDomainAdvanceConfigsResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "D7861F61-5B61-46CE-A47C-6B19160D5EB0",
  "DomainConfigs" : [ {
    "Domain" : "www.aliyundoc.com",
    "Profile" : {
      "Http2Port" : [ 443 ],
      "Ipv6Status" : 1,
      "HttpPort" : [ 80 ],
      "GSLBStatus" : "on",
      "Rs" : [ "38.XX.XX.42" ],
      "VipServiceStatus" : 0,
      "ClusterType" : 0,
      "ExclusiveVipStatus" : 0,
      "Cname" : "****dsbpkt75zeiok5mta2j5l7hggcrm.****.com",
      "CertStatus" : 1,
      "HttpsPort" : [ 443 ],
      "ResolvedType" : 0
    }
  } ]
}
```

错误码

访问错误中心查看更多错误码。

6.防护配置

6.1. ModifyDomainIpv6Status

调用ModifyDomainIpv6Status接口开启或关闭指定域名配置的IPv6安全防护功能。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyDomainIpv6Status	要执行的操作。取值：**ModifyDomainIpv6Status**。
Domain	String	是	www.example.com	已添加的域名名称。
Enabled	String	是	0	是否启用IPv6安全防护，取值： • **0**：关闭 • **1**：开启
InstanceId	String	是	waf-cn-mp9153****	WAF实例ID。 **说明** 您可以通过调用DescribeInstanceInfo接口查看当前WAF实例ID。

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	请求ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyDomainIpv6Status
&Domain=www.example.com
&Enabled=0
&InstanceId=waf-cn-mp9153****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<ModifyDomainIpv6StatusResponse>
   <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</ModifyDomainIpv6StatusResponse>
```

`JSON` 格式

```
{
    "RequestId": "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

6.2. DescribeProtectionModuleStatus

调用DescribeProtectionModuleStatus查询指定的WAF防护功能模块的启用状态。

使用说明

本接口用于查询指定的WAF防护功能模块的启用状态。您可以通过设置**DefenseType**参数值指定要查询的某个防护功能模块。具体参数值的含义，请参见请求参数**DefenseType**的描述。

QPS限制

本接口的单用户QPS限制为50次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeProtectionModuleStatus	要执行的操作。取值：**DescribeProtectionModuleStatus**。

名称	类型	是否必选	示例值	描述
Domain	String	是	www.aliyundoc.com	要查询的网站域名。 **说明** 您可以调用DescribeDomainList查询所有已接入WAF防护的域名。
DefenseType	String	是	waf	要查询的WAF防护功能模块。取值： • **waf**：表示规则防护引擎。 • **dld**：表示深度学习引擎。 • **tamperproof**：表示网站防篡改。 • **dlp**：表示防敏感信息泄漏。 • **normalized**：表示主动防御。 • **bot_crawler**：表示合法爬虫。 • **bot_intelligence**：表示爬虫威胁情报。 • **antifraud**：表示数据风控。 • **bot_algorithm**：表示智能算法。 • **bot_wxbb**：表示App防护。 • **bot_wxbb_pkg**：表示App防护中的版本防护。 • **ac_cc**：表示CC安全防护。 • **ac_blacklist**：表示IP黑名单。 • **ac_highfreq**：表示扫描防护中的高频Web攻击封禁。 • **ac_dirscan**：表示扫描防护中的目录遍历防护。 • **ac_scantools**：表示扫描防护中的扫描工具封禁。 • **ac_collaborative**：表示扫描防护中的协同防御。 • **ac_custom**：表示自定义防护策略。 **说明** 只支持设置一个功能模块。
InstanceId	String	是	waf-cn-zz11sr5****	要查询的WAF实例的ID。 **说明** 您可以调用DescribeInstanceInfo查询当前WAF实例的ID。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
ModuleStatus	Integer	1	防护功能模块的启用状态。取值： • **0**：表示功能模块已关闭。 • **1**：表示功能模块已开启。
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeProtectionModuleStatus
&Domain=www.aliyundoc.com
&DefenseType=waf
&InstanceId=waf-cn-zz11sr5****
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeProtectionModuleStatusResponse>
    <ModuleStatus>1</ModuleStatus>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</DescribeProtectionModuleStatusResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "ModuleStatus" : 1,
  "RequestId" : "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

6.3. ModifyProtectionModuleStatus

调用ModifyProtectionModuleStatus开启或关闭指定的WAF防护功能模块。

使用说明

本接口用于开启或关闭指定的WAF防护功能模块。

您可以通过设置**DefenseType**参数值指定要操作的某个防护功能模块。具体参数值的含义，请参见请求参数**DefenseType**的描述。

QPS限制

本接口的单用户QPS限制为20次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyProtectionModuleStatus	要执行的操作。取值：**ModifyProtectionModuleStatus**。
Domain	String	是	www.aliyundoc.com	要操作的网站域名。 **说明** 您可以调用DescribeDomainList查询所有已接入WAF防护的域名。

名称	类型	是否必选	示例值	描述
DefenseType	String	是	waf	要操作的WAF防护功能模块。取值： • waf：表示规则防护引擎。 • dld：表示深度学习引擎。 • tamperproof：表示网站防篡改。 • dlp：表示防敏感信息泄漏。 • normalized：表示主动防御。 • bot_crawler：表示合法爬虫。 • bot_intelligence：表示爬虫威胁情报。 • antifraud：表示数据风控。 • bot_algorithm：表示智能算法。 • bot_wxbb：表示App防护。 • bot_wxbb_pkg：表示App防护中的版本防护。 • ac_cc：表示CC安全防护。 • ac_blacklist：表示IP黑名单。 • ac_highfreq：表示扫描防护中的高频Web攻击封禁。 • ac_dirscan：表示扫描防护中的目录遍历防护。 • ac_scantools：表示扫描防护中的扫描工具封禁。 • ac_collaborative：表示扫描防护中的协同防御。 • ac_custom：表示自定义防护策略。 **说明** 只支持设置一个功能模块。
ModuleStatus	Integer	是	1	设置防护功能模块的开关状态。取值： • 0：表示关闭功能模块。 • 1：表示开启功能模块。
InstanceId	String	是	waf-cn-zz11sr5****	要操作的WAF实例的ID。 **说明** 您可以调用DescribeInstanceInfo查询当前WAF实例的ID。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyProtectionModuleStatus
&Domain=www.aliyundoc.com
&DefenseType=waf
&ModuleStatus=1
&InstanceId=waf-cn-zz11sr5****
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyProtectionModuleStatusResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</ModifyProtectionModuleStatusResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

6.4. DescribeProtectionModuleMode

调用DescribeProtectionModuleMode查询网站防护配置中，指定防护模块（包括规则防护引擎、深度学习引擎、CC安全防护、数据风控、主动防御）当前使用的防护模式。

使用说明

本接口用于查询网站防护配置中，指定防护模块（包括规则防护引擎、深度学习引擎、CC安全防护、数据风控、主动防御）当前使用的防护模式。

您可以通过设置DefenseType参数值指定要查询的防护模块。具体参数值的含义，请参见请求参数DefenseType的描述。

调用本接口前，您必须已经调用CreateDomain创建了网站接入配置，将网站域名接入WAF防护。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeProtectionModuleMode	要执行的操作。取值：**DescribeProtectionModuleMode**。
Domain	String	是	www.aliyundoc.com	要查询的网站域名。 **说明** 网站域名必须已经接入WAF防护。您可以调用DescribeDomainList查询所有已接入WAF防护的网站域名。
DefenseType	String	是	waf	要查询其模式的防护模块。取值： • **waf**：表示规则防护引擎。 • **dld**：表示深度学习引擎。 • **ac_cc**：表示CC安全防护。 • **antifraud**：表示数据风控。 • **normalized**：表示主动防御。
InstanceId	String	是	waf-cn-tl32ast****	WAF实例的ID。 **说明** 您可以调用DescribeInstanceInfo查询当前WAF实例的ID。
ResourceGroupId	String	否	rg-atstuj3rtop****	网站域名在资源管理服务中所属的资源组ID。不设置该参数表示默认资源组。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
LearnStatus	Integer	3	主动防御模块的学习状态。取值：【待补充】 **说明** 只有当请求参数DefenseType为normalized（表示查询主动防御模块）时，才会返回该参数。
RequestId	String	DE14845A-F46F-59BE-B8F7-6ED7A787D213	本次请求的ID。

Mode	Integer	0	防护模块当前使用的防护模式。根据请求参数DefenseType不同，该参数的取值和含义不同，具体说明如下：
			• DefenseType为waf（表示查询规则防护引擎），Mode取值：
			  ○ 0：表示拦截模式。
			  ○ 1：表示告警模式。
			• DefenseType为dld（表示查询深度学习引擎），Mode取值：
			  ○ 0：表示告警模式。
			  ○ 1：表示拦截模式。
			• DefenseType为ac_cc（表示查询CC安全防护模块），Mode取值：
			  ○ 0：表示防护模式。
			  ○ 1：表示防护-紧急模式。
			• DefenseType为antifraud（表示查询数据风控模块），Mode取值：
			  ○ 0：表示告警模式。
			  ○ 1：表示拦截模式。
			  ○ 2：表示强拦截模式。
			• DefenseType为normalized（表示查询主动防御模块），Mode取值：
			  ○ 0：表示告警模式。
			  ○ 1：表示拦截模式。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeProtectionModuleMode
&Domain=www.aliyundoc.com
&DefenseType=waf
&InstanceId=waf-cn-tl32ast****
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeProtectionModuleModeResponse>
    <LearnStatus>3</LearnStatus>
    <RequestId>DE14845A-F46F-59BE-B8F7-6ED7A787D213</RequestId>
    <Mode>0</Mode>
</DescribeProtectionModuleModeResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "LearnStatus" : 3,
  "RequestId" : "DE14845A-F46F-59BE-B8F7-6ED7A787D213",
  "Mode" : 0
}
```

错误码

访问错误中心查看更多错误码。

6.5. ModifyProtectionModuleMode

调用ModifyProtectionModuleMode接口修改指定WAF防护功能模块（包括正则防护引擎、大数据深度学习引擎、CC安全防护、数据风控、主动防御等模块）中的防护模式。

您可以通过设置DefenseType参数值指定防护功能模块。具体参数值的含义，请参见请求参数DefenseType的描述。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyProtectionModuleMode	要执行的操作。取值：**ModifyProtectionModuleMode**。
DefenseType	String	是	waf	防护功能模块，取值： • **waf**：正则防护引擎 • **dld**：大数据深度学习引擎 • **ac_cc**：CC安全防护 • **antifraud**：数据风控 • **normalized**：主动防御
Domain	String	是	www.example.com	已添加的域名名称。
InstanceId	String	是	waf_elasticity-cn-0xldbqt****	WAF实例ID。 **说明** 您可以通过调用DescribeInstanceInfo接口查看当前WAF实例ID。

名称	类型	是否必选	示例值	描述
Mode	Integer	是	0	防护模式。 说明 根据所指定的防护模块（DefenseType）不同，防护模式（Mode）值的含义有所不同。 • 正则防护引擎（waf） ○ 0：表示拦截模式。 ○ 1：表示告警模式。 • 大数据深度学习引擎（dld） ○ 0：表示告警模式。 ○ 1：表示拦截模式。 • CC安全防护（ac_cc） ○ 0：表示防护模式。 ○ 1：表示防护-紧急模式。 • 数据风控（antifraud） ○ 0：表示告警模式。 ○ 1：表示拦截模式。 ○ 2：表示强拦截模式。 • 主动防御（normalized） ○ 1：表示拦截模式。 ○ 0：表示告警模式。

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	请求ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyProtectionModuleMode
&DefenseType=waf
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqt****
&Mode=0
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<ModifyProtectionModuleModeResponse>
   <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</ModifyProtectionModuleModeResponse>
```

`JSON` 格式

```
{
    "RequestId": "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

6.6. DescribeProtectionModuleRules

调用DescribeProtectionModuleRules查询指定WAF防护功能模块（包括Web入侵防护、数据安全、Bot管理、访问控制或限流、网站白名单等模块）的规则配置记录。

使用说明

本接口用于分页查询指定WAF防护功能模块（包括Web入侵防护、数据安全、Bot管理、访问控制或限流、网站白名单等模块）的规则配置记录。

您可以通过设置**DefenseType**参数值指定防护功能模块配置。具体参数值的含义，请参见请求参数**DefenseType**的描述。

QPS限制

本接口的单用户QPS限制为50次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeProtectionModuleRules	要执行的操作。取值：**DescribeProtectionModuleRules**。
PageSize	Integer	否	10	分页查询时，设置每页返回规则的数量。默认值为**10**。
PageNumber	Integer	否	1	分页查询时，设置当前页面的页面。默认值为1。

名称	类型	是否必选	示例值	描述
Domain	String	否	www.aliyundoc.com	要查询的域名。具体说明如下： • DefenseType取值为ng_account以外的值（即查询除账户安全规则配置以外的其他网站防护配置）时，必须设置该参数。 说明 您可以调用DescribeDomainList查询所有已添加到WAF防护的域名。 • DefenseType取值是ng_account（即查询账户安全规则配置）时，不要设置该参数，否则会返回错误信息。

名称	类型	是否必选	示例值	描述
DefenseType	String	是	ac_highfreq	要查询的防护功能配置的类型。取值： • waf-codec：表示查询规则防护引擎解码设置。 • tamperproof：表示查询网站防篡改规则配置。 • dlp：表示查询防敏感信息泄漏规则配置。 • ng_account：表示查询账户安全规则配置。 • bot_crawler：表示查询合法爬虫规则配置。 • bot_intelligence：表示查询爬虫威胁情报规则配置。 • antifraud：表示查询数据风控防护请求配置。 • antifraud_js：表示查询数据风控JS插入页面配置。 • bot_algorithm：表示查询智能算法规则配置。 • bot_wxbb_pkg：表示查询App防护的版本防护规则。 • bot_wxbb：表示查询App防护的路径防护规则。 • ac_blacklist：表示查询IP黑名单规则配置。 • ac_highfreq：表示查询高频Web攻击IP自动封禁规则配置。 • ac_dirscan：表示查询目录扫描防护规则配置。 • ac_custom：表示查询自定义防护策略规则配置。 • whitelist：表示查询白名单规则配置。
				设置规则的过滤和排序，以JSON格式字符串表达，具体包含以下参数： **说明** 该参数必须使用Base64编码格式，请按照以下参数说明构造JSON格式字符串后将其转换为Base64编码格式。 • filter：JSON格式字符串 | 可选 | 过滤条件。以JSON字符串格式描述，具体包含以下参数：

名称	类型	是否必选	示例值	描述
Query	String	否	e2ZpbHRlcjp7InJ1bGVJZCI6NDI3NTV9LG9yZGVyQnk6ImdtdF9tb2RpZmllZCIsZGVzYzp0cnVlfQ==	○ **nameId**：String类型 | 可选 | 查询规则ID等于该参数值或规则名称中包含该参数值的规则。 ○ **scene**：String类型 | 可选 | 设置要查询的防护模块，取值与**DefenseType**参数相同。 ○ **enabled**：Boolean类型 | 可选 | 设置要查询的规则状态，取值： ■ **false**：表示已禁用。 ■ **true**：表示已启用。 ○ **status**：Integer类型 | 可选 | 设置要查询的规则状态，与**enabled**参数含义相同，取值： ■ **0**：表示已禁用。 ■ **1**：表示已启用。 ○ **ruleId**：Integer类型 | 可选 | 设置要查询的规则ID。 ○ **ruleIdList**：Array类型 | 可选 | 设置要查询的规则ID列表，多个规则ID间用半角逗号（,）分隔。 ○ **sceneList**：Array类型 | 可选 | 设置要查询的防护模块列表，取值与**DefenseType**参数相同，多个防护模块间用半角逗号（,）分隔。 ○ **originList**：Array类型 | 可选 | 设置规则来源，取值为**system**（表示系统自动生成）和**custom**（表示自定义创建），设置多个规则来源时用半角逗号（,）分隔。 ○ **tag**：String类型 | 可选 | 当设置的查询防护模块为白名单（**whitelist**）时，可通过设置该参数查询不检测指定模块的白名单规则。**tag**参数的取值和含义可参考返回参数中白名单规则配置中的描述。 ○ **origin**：String类型 | 可选 | 当设置的查询防护模块为白名单（**whitelist**）时，可通过设置该参数查询WAF智能规则托管功能自动添加的白名单规则。取值固定为**ai**。不设置该参数表示查询所有白名单规则（包括您手动添加的规则和智能规则托管功能自动添加的规则）。

名称	类型	是否必选	示例值	描述
				○ **category**：String类型 | 可选 | 当设置的查询防护模块为白名单（**whitelist**）时，可通过设置该参数查询指定白名单分类，取值： ■ **waf**：表示网站白名单。 ■ **ws**：表示Web入侵防护白名单。 ■ **ac**：表示访问控制/限流白名单。 ■ **ds**：表示数据安全白名单。 • **orderBy**：String类型 | 可选 | 排序字段，取值： ○ **action**：表示规则处置动作，该参数值仅在查询自定义防护策略规则时有效。 ○ **gmt_modified**（默认）：表示最后一次修改时间。 ○ **name**：表示规则名称。 ○ **status**：表示规则状态。 • **desc**：Boolean类型 | 可选 | 是否倒序排列，取值： ○ **false**：表示正序排列。 ○ **true**（默认）：表示倒序排列。
Lang	String	否	zh	设置规则名称的语言属性，取值： • **zh**：表示规则名称为中文。 • **en**：表示规则名称为英文。 • **ja**：表示规则名称为日文。
InstanceId	String	是	waf_elasticity-cn-0xldbqt****	WAF实例的ID。 **说明** 您可以调用DescribeInstanceInfo查询当前WAF实例的ID。
ResourceGroupId	String	否	rg-acfm2pz25js****	WAF实例在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
TotalCount	Integer	1	查询到的规则配置的总数量。
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	本次请求的ID。
Rules	Array of Rule		规则配置信息，包含规则ID、创建时间、状态等。
Status	Long	1	规则状态。取值： • **0**：表示已禁用。 • **1**：表示已启用。
Time	Long	1570700044	规则创建时间。使用时间戳表示，单位：秒。
Content	Map		规则配置内容，以一系列参数构造的JSON格式转化成字符串。 **说明** 根据所指定的防护功能模块配置（DefenseType）不同，具体涉及的参数有所不同。详细信息，请参见Content参数具体说明。
Version	Long	2	当前规则配置的版本号。
RuleId	Long	42755	规则ID。

Content参数具体说明

- 规则防护引擎解码设置（**waf-codec**）对应的JSON字符串中包含以下参数：
  - **codecList**：String类型 | 必选 | 启用的解码配置项。
  - **示例**

```
{
    "codecList":["url","base64"]
}
```

- 网站防篡改规则配置（**tamperproof**）对应的JSON字符串中包含以下参数：
  - **uri**：String类型 | 必选 | 所需防护的具体URL。
  - **name**：String类型 | 必选 | 规则名称。

- status：Integer类型 | 可选 | 规则的防护状态：
  - 0（默认）：表示不生效。
  - 1：表示生效。
- 示例

```
{
    "name":"example",
    "uri":"http://www.example.com/example",
    "status":1
}
```

- 防敏感信息泄露规则配置（dlp）对应的JSON字符串中包含以下参数：
  - name：String类型 | 必选 | 规则名称。
  - conditions：Array类型 | 必选 | 以JSON字符串格式描述匹配条件，支持设置最多两条匹配条件且条件间的关系为并且。其中包含以下具体参数：
    - key：匹配项。
      - 0：表示防护的URL。
      - 10：表示敏感信息。
      - 11：表示响应码。
    - operation：匹配逻辑，取值固定为1，表示包含。
    - value：以JSON字符串描述匹配条件值，支持设置多个条件值。其中包含以下具体参数：
      - v：仅适用于匹配项（key）为URL（0）或响应码（11）的场景。
        - URL：当 `"key":0` 时，参数值为URL地址。
        - 响应码：当 `"key":11` ，参数取值包括400、401、402、403、404、405-499、500、501、502、503、504、505-599。
      - k：仅适用于匹配项（key）为敏感信息（10）的场景，取值：
        - 100：表示身份证。
        - 101：表示信用卡。
        - 102：表示电话号码。
        - 103：表示默认敏感词。
  - action：匹配动作。
    - 3：表示告警。
    - 10：表示敏感信息过滤，该动作仅适用于包含敏感信息（ `"key":10` ）的匹配条件场景。
    - 11：表示返回系统内置拦截页面，该动作仅适用于包含响应码（ `"key":11` ）的匹配条件场景。

- 示例

```
  {
 "name":"example",
 "conditions":[{"key":11,"operation":1,"value":[{"v":401}]},{"key":"0","operation":1,"v
alue":[{"v":"www.example.com"}]}],
 "action":3
  }
```

- 账户安全规则配置（ng_account）对应的JSON字符串中包含以下参数：
  - domain：String类型 | 必选 | 防护的域名。
  - method：String类型 | 必选 | 检测的请求方式，包括POST、GET、PUT、DELETE。支持设定多个请求方式，以英文逗号“,”分隔。
  - url_path：String类型 | 必选 | 检测接口，以URL路径表示，必须以正斜杠（/）开头。
  - account_left：String类型 | 必选 | 账号参数名。
  - password_left：String类型 | 可选 | 密码参数名。
  - action：String类型 | 必选 | 防护动作，取值：
    - monitor：表示预警。
    - block：表示拦截。
  - 示例

```
    {
        "domain":"www.example.com",
        "method":"GET,POST",
        "url_path":"/example",
        "account_left":"aaa",
        "action":"monitor"
    }
```

- 合法爬虫规则配置（bot_crawler）对应的JSON字符串中包含以下参数：
  - Status：Integer类型 | 必选 | 是否启用，取值：
    - 0：表示禁用。
    - 1：表示启用。
  - Version：Integer类型 | 必选 | 规则版本号。
  - Content：String类型 | 必选 | 规则详细信息，以JSON字符串格式进行描述，具体包含以下参数：
    - name：String类型 | 必选 | 规则名称。
    - conditions：Array类型 | 可选 | 防护路径条件。在合法爬虫规则配置中固定为空，表示全路径。
    - expressions：Array类型 | 必选 | 规则条件表达式，以更易读的方式表示所有规则条件信息。
    - bypassTags：String类型 | 必选 | 不检测的模块。在合法爬虫规则配置中固定为antibot，表示Bot管理模块。
    - tags：Array类型 | 必选 | 规则所属防护功能模块。在合法爬虫规则配置中固定为 `["antibot"]`，表示Bot管理模块。
  - RuleId：Integer类型 | 必选 | 规则ID。

- **Time**：String类型 | 必选 | 规则最新修改时间，以秒级时间戳格式表示。
- **示例**

```
    {
        "Status":0,
        "Version":1,
        "Content":{
            "name":"百度蜘蛛白名单",
            "conditions":[],
            "expressions":["remote_addr inl 'ioc.210d077a-cf34-49ad-a9b3-0aa48095c595'
&& uri =^ '/'"],
            "bypassTags":"antibot",
            "tags":["antibot"]
        },
 "RuleId":20384,
 "Time":1585818161
    }
```

- 爬虫威胁情报规则配置（**bot_intelligence**）对应的JSON字符串中包含以下参数：
  - **Status**：Integer类型 | 必选 | 是否启用，取值：
    - 0：表示禁用。
    - 1：表示启用。
  - **Version**：Integer类型 | 必选 | 规则版本号。
  - **Content**：String类型 | 必选 | 规则详细信息，以JSON字符串格式进行描述，具体包含以下参数：
    - **name**：String类型 | 必选 | 规则名称。
    - **action**：String类型 | 必选 | 处置动作，取值：
      - **monitor**：表示观察。
      - **captcha**：表示滑块。
      - **captcha_strict**：表示严格滑块。
      - **js**：表示JavaScript校验。
      - **block**：表示阻断。
    - **urlList**：Array类型 | 必选 | 防护路径，最多指定十个防护路径。以JSON字符串方式表示，具体包含以下参数：
      - **mode**：String类型 | 必选 | 匹配方式，与路径关键字（**url**）参数结合指定防护路径。可选值：**eq**（精准匹配）、**prefix-match**（前缀匹配）、**regex**（正则匹配）。
      - **url**：String类型 | 必选 | 路径关键字，必须以正斜杠（/）开头。
    - **keyType**：String类型 | 必选 | 情报库类型，包含IP库（**ip**）、指纹库（**ua**）两种类型。
  - **RuleId**：Integer类型 | 必选 | 规则ID。
  - **Time**：String类型 | 必选 | 规则最新修改时间，以秒级时间戳格式表示。

- 示例

```
    {
        "Status":1,
        "Version":1,
        "Content":{
            "name":"IDC IP库-腾讯云",
            "action":"captcha_strict",
            "urlList":[{"mode":"prefix-match","url":"/indexa"}, {"mode":"regex","url":"
/"},{"mode":"eq","url":"/"}],
            "keyType":"ip"
        },
        "RuleId":922777,
        "Time":1585907112
    }
```

- 数据风控防护请求规则配置（antifraud）对应的JSON字符串中包含以下参数：
  - uri：String类型 | 必选 | 具体的防护请求URL。
  - 示例

```
    {
        "uri": "http://1.example.com/example"
    }
```

- 数据风控JS插入页面配置（antifraud_js）对应的JSON字符串中包含以下参数：
  - uri：String类型 | 必选 | 需要插入数据风控JS页面的URL，系统将为所指定的URL路径下的所有页面插入数据风控JS。
  - 示例

```
    {
        "uri": "/example/example"
    }
```

- 智能算法规则配置（bot_algorithm）对应的JSON字符串中包含以下参数：
  - Status：Integer类型 | 必选 | 是否启用，取值：
    - 0：表示禁用。
    - 1：表示启用。
  - Version：Integer类型 | 必选 | 规则版本号。
  - Content：String类型 | 必选 | 规则详细信息，以JSON字符串格式进行描述，具体包含以下参数：
    - name：String类型 | 必选 | 规则名称。
    - timeInterval：Integer类型 | 必选 | 检测周期，可选值：30、60、120、300、600，单位秒。

- action：String类型 | 必选 | 处置动作，取值：
  - monitor：表示观察。
  - captcha：表示滑块。
  - js：表示JavaScript校验。
  - block：表示阻断。选择阻断作为处置动作时，必须设置阻断时长（blocktime）参数。
- blocktime：Integer类型 | 可选 | 阻断时长，单位分钟，取值范围：1~600。
- algorithmName：String类型 | 必选 | 算法名称，取值：
  - RR：表示专项资源爬虫识别算法。
  - PR：表示定向路径爬虫识别算法。
  - DPR： 表示参数轮询爬虫识别算法。
  - SR：表示动态IP爬虫识别算法。
  - IND：表示代理设备爬虫识别算法。
  - Periodicity：表示周期性爬虫识别算法。
- config：String类型 | 必选 | 算法配置信息，以JSON字符串格式表示。算法配置信息中的具体子参数与所选择的算法名称（algorithmName）相关。
  - 专项资源爬虫识别算法（RR）对应的配置信息应包含以下子参数：
    - resourceType：Integer类型 | 可选 | 请求的资源类型，取值：
      - 1：表示动态资源类型。
      - 2：表示静态资源类型。
      - -1：表示自定义资源类型。选择自定义资源组时，需要再设置extensions参数，以字符串格式指定具体的资源后缀名，多个后缀名间以英文逗号“,”分隔，例如 `css,jpg,xls` 。
    - minRequestCountPerIp：Integer类型 | 必选 | 检测周期中检测IP的范围，大于等于一定访问请求数量的IP才会被检测。通过该参数指定访问请求数量的最小值，取值范围：5~10000。
    - minRatio：Float类型 | 必选 | 风险判定条件，即IP访问请求中访问指定资源类型的占比阈值，超过阈值后判定为风险，取值范围：0.01~1。
  - 定向路径爬虫识别算法（PR）对应的配置信息应包含以下子参数：
    - keyPathConfiguration：Array类型 | 可选 | 请求的路径信息，支持指定最多10条路径，只在使用定向路径爬虫识别算法时需设置该子参数。以JSON字符串格式表示，具体包含以下参数：
      - method：String类型 | 必选 | 请求方法，可选值：POST、GET、PUT、DELETE、HEAD、OPTIONS。
      - url：String类型 | 必选 | 请求路径关键字，必须以正斜杠（/）开头。
      - matchType：String类型 | 必选 | 匹配方式，与请求路径关键字（url）参数结合指定请求路径。可选值：all（精准匹配）、prefix（前缀匹配）、regex（正则匹配）。
    - minRequestCountPerIp：Integer类型 | 必选 | 检测周期中检测IP的范围，大于等于一定访问请求数量的IP才会被检测。通过该参数指定访问请求数量的最小值，取值范围：5~10000。
    - minRatio：Float类型 | 必选 | 风险判定条件，即IP访问请求中访问指定路径的占比阈值（对应定向路径爬虫识别算法），超过阈值后判定为风险，取值范围：0.01~1。

- 参数轮询爬虫识别算法（DPR）对应的配置信息应包含以下子参数：
  - method：String类型 | 必选 | 请求方法，可选值：POST、GET、PUT、DELETE、HEAD、OPTIONS。
  - urlPattern：String类型 | 必选 | 关键参数路径，必须以正斜杠（/）开头。用{}表示关键参数，配置多个{}时将拼接这些参数作为关键参数。例如，`/company/{}/{}/{}/user.php?uid={}`。
  - minRequestCountPerIp：Integer类型 | 必选 | 检测周期中检测IP的范围，大于等于一定访问请求数量的IP才会被检测。通过该参数指定访问请求数量的最小值，取值范围：5~10000。
  - minRatio：Float类型 | 必选 | 风险判定条件，即IP访问请求中不同关键参数值的计数占比阈值，超过阈值后判定为风险，取值范围：0.01~1。
- 动态IP爬虫识别算法（SR）对应的配置信息应包含以下子参数：
  - maxRequestCountPerSrSession：Integer类型 | 必选 | 通过设定每个会话中存在的最小请求次数定义异常会话，即单个会话中的请求次数小于该值即判定为异常会话。取值范围：1~8。
  - minSrSessionCountPerIp：Integer类型 | 必选 | 风险判定条件，即IP访问请求中存在的异常会话数量阈值，单个IP访问请求中的异常会话次数超过该值后判定为风险。取值范围：5~300。
- 代理设备爬虫识别算法（IND）对应的配置信息应包含以下子参数：
  - minIpCount：Integer类型 | 必选 | 恶意设备判定条件，即设备使用WIFI关联的IP变换个数阈值，超过该阈值后判定为风险，取值范围：5~500。
  - keyPathConfiguration：Array类型 | 可选 | 检测路径信息，支持指定最多10条路径。以JSON字符串格式表示，具体包含以下参数：
    - method：String类型 | 必选 | 请求方法，可选值：POST、GET、PUT、DELETE、HEAD、OPTIONS。
    - url：String类型 | 必选 | 检测路径关键字，必须以正斜杠（/）开头。
    - matchType：String类型 | 必选 | 匹配方式，与检测路径关键字（url）参数结合指定请求路径。可选值：all（精准匹配）、prefix（前缀匹配）、regex（正则匹配）。
- 周期性爬虫识别算法（Periodicity）对应的配置信息应包含以下子参数：
  - minRequestCountPerIp：Integer类型 | 必选 | 检测周期中检测IP的范围，大于等于一定访问请求数量的IP才会被检测。通过该参数指定访问请求数量的最小值，取值范围：5~10000。
  - level：Integer类型 | 必选 | 风险判定等级，即访问IP的周期性特征的明显程度，取值：
    - 0：表示明显。
    - 1：表示中等。
    - 2：表示较弱。

- RuleId：Integer类型 | 必选 | 规则ID。
- Time：String类型 | 必选 | 规则最新修改时间，以秒级时间戳格式表示。

- **示例**

```
    {
        "Status":1,
        "Version":1,
        "Content":{
            "name":"动态IP",
            "timeInterval":60,
            "action":"warn",
            "algorithmName":"IND",
            "config":{"minIpCount":5,"keyPathConfiguration":[{"method":"GET","matchType
":"prefix","url":"/index"}]}
        },
        "RuleId":940180,
        "Time":1585832957
    }
```

- App防护的版本防护规则配置（**bot_wxbb_pkg**）对应的JSON字符串中包含以下参数：
  - **Version**：Integer类型 | 必选 | 规则版本号。
  - **Content**：String类型 | 必选 | 规则详细信息，以JSON字符串格式进行描述，具体包含以下参数：
    - **name**：String类型 | 必选 | 规则名称。
    - **action**：String类型 | 必选 | 处置动作，取值：
      - **test**：表示观察。
      - **close**：表示阻断。
    - **nameList**：Array类型 | 必选 | 合法版本信息，最多指定五条规则。以JSON字符串方式表示，具体包含以下参数：
      - **name**：String类型 | 必选 | 合法包名称。
      - **signList**：Array类型 | 必选 | 对应的包签名，最多包含15个，以半角逗号（,）分隔。
  - **RuleId**：Integer类型 | 必选 | 规则ID。
  - **Time**：String类型 | 必选 | 规则最新修改时间，以秒级时间戳格式表示。
  - **示例**

```
    {
        "Version":0,
        "Content":{
            "nameList":[{"signList":["xxxxxx","xxxxx","xxxx","xx"],"name":"apk-xxxx"}],
            "name":"test",
            "action":"close"
        },
        "RuleId":271,
        "Time":1585836143
    }
```

- App防护的路径防护规则配置（**bot_wxbb**）对应的JSON字符串中包含以下参数：
  - **Version**：Integer类型 | 必选 | 规则版本号。

- Content：String类型 | 必选 | 规则详细信息，以JSON字符串格式进行描述，具体包含以下参数：
  - name：String类型 | 必选 | 规则名称。
  - uri：String类型 | 必选 | 防护路径，必须以正斜杠（/）开头。
  - matchType：String类型 | 必选 | 匹配方式。可选值：all（精准匹配）、prefix（前缀匹配）、regex（正则匹配）。
  - arg：String类型 | 必选 | 参数包含，与匹配方式（matchType）参数结合指定防护路径配置。
  - action：String类型 | 必选 | 处置动作，取值：
    - test：表示观察。
    - close：表示阻断。
  - wxbbVmpFieldType：Integer类型 | 可选 | 自定义加签字段类型。如果规则中未设置自定义加签字段，则不返回该参数。取值：
    - 0：表示header。
    - 1：表示参数。
    - 2：表示cookie。
  - wxbbVmpFieldValue：String类型 | 可选 | 自定义加签字段值。如果规则中未设置自定义加签字段，则不返回该参数。
  - blockInvalidSign：Boolean类型 | 必选 | 是否对非法签名执行处置动作。
  - blockProxy：Boolean类型 | 必选 | 是否对代理执行处置动作。
  - blockSimulator：Boolean类型 | 必选 | 是否对模拟器执行处置动作。
- RuleId：Integer类型 | 必选 | 规则ID。
- Time：String类型 | 必选 | 规则最新修改时间，以秒级时间戳格式表示。
- 示例

```
{
    "Version":6,
    "Content":{
        "blockInvalidSign":true,
        "wxbbVmpFieldValue":"test",
        "blockSimulator":true,
        "matchType":"all",
        "arg":"test",
        "name":"test",
        "action":"close",
        "blockProxy":true,
        "uri":"/index",
        "wxbbVmpFieldType":1
    },
    "RuleId":2585,
    "Time":1586241849
}
```

- IP黑名单规则配置（ac_blacklist）对应的JSON字符串中包含以下参数：
  - empty：Boolean类型 | 必选 | 黑名单是否为空。
  - remoteAddr：Array类型 | 必选 | 黑名单中的IP。

- **area**：String类型 | 必选 | 以JSON格式字符串表示区域封禁规则，包含国家编码（countryCodes）、区域编码（regionCodes）、是否放行（not）具体参数。由于API接口中以编码形式返回封禁国家和区域，建议您在控制台中查看具体的封禁国家和区域。
- **示例**

```
{
    "empty":false,
    "remoteAddr":["1.XX.XX.1","12.XX.XX.2"]
}
```

- 高频Web攻击IP自动封禁规则配置（**ac_highfreq**）对应的JSON字符串中包含以下参数：
  - **interval**：Integer类型 | 必选 | 检测时间范围，单位秒，取值范围：5~1800。
  - **ttl**：Integer类型 | 必选 | 封禁IP时长，单位秒，取值范围：60~86400。
  - **count**：Integer类型 | 必选 | Web攻击次数阈值，检测时间范围内攻击次数超过该值，触发封禁。取值范围：2~50000。
  - **示例**

```
{
 "interval":60,
 "ttl":300,
 "count":60
 }
```

- 目录扫描防护规则配置（**ac_dirscan**）对应的JSON字符串中包含以下参数：
  - **interval**：Integer类型 | 必选 | 检测时间范围，单位秒，取值范围：5~1800。
  - **ttl**：Integer类型 | 必选 | 封禁IP时长，单位秒。
  - **count**：Integer类型 | 必选 | 访问次数阈值，取值范围：2~50000。
  - **weight**：Float类型 | 必选 | 404响应码占比阈值（百分比），取值范围：`(0,1]`。
  - **uriNum**：Integer类型 | 必选 | 扫描目录数量阈值，取值范围：2~50000。
  - **示例**

```
{
 "interval":10,
 "ttl":1800,
 "count":50,
 "weight":0.7,
    "uriNum":20
}
```

- 自定义防护策略规则配置（**ac_custom**），通过其对应JSON字符串中的**scene**参数来设置ACL访问控制规则和CC攻击防护规则。
  - 自定义ACL访问控制规则（**scene**参数值为**custom_acl**）对应的JSON字符串中包含以下参数：
    - **name**：String类型 | 必选 | 规则名称。
    - **scene**：String类型 | 必选 | 防护类型。设置ACL访问控制规则时，取值固定为**custom_acl**。

- action：String类型 | 必选 | 处置动作，取值：
  - monitor：表示观察。
  - captcha：表示滑块。
  - captcha_strict：表示严格滑块。
  - js：表示JS验证。
  - block：表示阻断。
- conditions：Array类型 | 必选 | 匹配条件，以JSON字符串格式进行描述，具体包含以下参数：
  - key：匹配字段，取值：URL、IP、Referer、User-Agent、Params、Cookie、Content-Type、Content-Length、X-Forwarded-For、Post-Body、Http-Method、Header、URLPath。
  - opCode：逻辑符，取值：
    - 11：表示等于。
    - 10：表示不等于。
    - 41：表示等于多值之一。
    - 50：表示不等于任一值。
    - 1：表示包含。
    - 0：表示不包含。
    - 51：表示包含多值之一。
    - 52：表示不包含任一值。
    - 82：表示存在。
    - 2：表示不存在。
    - 21：表示长度等于。
    - 22：表示长度大于。
    - 20：表示长度小于。
    - 60：表示正则不匹配。
    - 61：表示正则匹配。
    - 72：表示前缀匹配。
    - 81：表示后缀匹配。
    - 80：表示内容为空。
  - values：匹配内容。根据需要设置相应的内容，以String类型表示。
  - contain：同样表示规则条件的逻辑符，取值与opCode参数相同。
  - opValue：逻辑符的简写含义，您可以参考opCode参数取值说明了解详细信息。
  - pattern：同样表示逻辑符的简写含义，取值与opValue参数相同。
- expressions：Array类型 | 必选 | 规则条件表达式，以更易读的方式表示所有规则条件信息。

- **示例**

```
        {
            "name":"test2",
            "action":"monitor",
            "conditions":[{"contain":1,"values":"login","pattern":"contain","opCode":
1,"opValue":"contain","key":"URL"}],
            "expressions":["request_uri contains 'login' "],
            "scene":"custom_acl"
        }
```

- 自定义CC攻击防护规则（scene参数值为custom_cc）对应的JSON字符串中包含以下参数：
  - **name**：String类型 | 必选 | 规则名称。
  - **scene**：String类型 | 必选 | 防护类型。设置CC攻击防护规则时，取值固定为custom_cc。
  - **conditions**：Array类型 | 必选 | 匹配条件，以JSON字符串格式进行描述，具体包含以下参数：
    - **key**：匹配字段，取值：URL、IP、Referer、User-Agent、Params、Cookie、Content-Type、Content-Length、X-Forwarded-For、Post-Body、Http-Method、Header、URLPath。
    - **opCode**：逻辑符，取值：
      - **11**：表示等于。
      - **10**：表示不等于。
      - **41**：表示等于多值之一。
      - **50**：表示不等于任一值。
      - **1**：表示包含。
      - **0**：表示不包含。
      - **51**：表示包含多值之一。
      - **52**：表示不包含任一值。
      - **82**：表示存在。
      - **2**：表示不存在。
      - **21**：表示长度等于。
      - **22**：表示长度大于。
      - **20**：表示长度小于。
      - **60**：表示正则不匹配。
      - **61**：表示正则匹配。
      - **72**：表示前缀匹配。
      - **81**：表示后缀匹配。
      - **80**：表示内容为空。
    - **values**：匹配内容。根据需要设置相应的内容，以String类型表示。
    - **contain**：同样表示规则条件的逻辑符，取值与opCode参数相同。
    - **opValue**：逻辑符的简写含义，您可以参考opCode参数取值说明了解详细信息。
    - **pattern**：同样表示逻辑符的简写含义，取值与opValue参数相同。
  - **expressions**：Array类型 | 必选 | 规则条件表达式，以更易读的方式表示所有规则条件信息。

- action：String类型 | 必选 | 处置动作，取值：
  - monitor：表示观察。
  - captcha：表示滑块。
  - captcha_strict：表示严格滑块。
  - js：表示JS验证。
  - block：表示阻断。
- ratelimit：JSON格式 | 必选 | 频率设置。以JSON字符串格式进行描述，具体包含以下参数：
  - target：String类型 | 必选 | 统计对象类型，取值：
    - remote_addr：表示IP。
    - cookie.acw_tc：表示Session。
    - queryarg：表示自定义参数。选择自定义参数时，必须在subkey参数中设置需要统计的自定义参数名称。
    - cookie：表示自定义cookie。选择自定义cookie时，您必须在subkey参数中设置需要统计的cookie内容。
    - header：表示自定义header。选择自定义header时，您必须在subkey参数中设置需要统计的header内容。
  - subkey：String类型 | 可选 | 当target参数值为cookie、header或queryarg时，您必须在subkey参数中设置对应的信息。
  - interval：Integer类型 | 必选 | 统计时长（单位：秒），即访问次数的统计周期，与阈值（threshold）参数配合。
  - threshold：Integer类型 | 必选 | 在检测时长内，允许单个统计对象访问被防护地址的次数阈值。
  - status：JSON格式 | 可选 | 响应码频率设置。以JSON字符串格式进行描述，具体包含以下参数：
    - code：Integer类型 | 必选 | 指定响应码。
    - count：Integer类型 | 可选 | 出现次数阈值，即表示当指定的响应码出现次数超过该阈值时命中防护规则，取值范围：1~999999999。count参数与ratio参数两者选其一，不可同时配置。
    - ratio：Integer类型 | 可选 | 出现比例阈值（百分比），即表示当指定的响应码出现比例超过该阈值时命中防护规则，取值范围：1~100。count参数与ratio参数两者选其一，不可同时配置。
  - scope：String类型 | 必选 | 生效范围，取值：
    - rule：表示当前特征匹配范围内。
    - domain：表示当前规则作用的域名范围内。
  - ttl：Integer类型 | 必选 | 处置动作的生效时长，单位：秒，取值范围：60~86400。

■ **示例**

```
        {
            "name":"CC防护",
            "conditions":[{"contain":1,"values":"login","pattern":"contain","opCode
":1,"opValue":"contain","key":"URL"}],
            "expressions":["request_uri contains 'login' "],
            "action":"block",
            "scene":"custom_cc",
            "ratelimit":{
                "target": "remote_addr",
                "interval": 300,
                "threshold": 2000,
                "status": {
                    "code": 404,
                    "count": 200
                },
                "scope": "rule",
                "ttl": 1800
            }
        }
```

- 白名单规则配置（whitelist）对应的JSON字符串中包含以下参数：
  - **name**：String类型 | 必选 | 规则名称。
  - **tags**：Array类型 | 必选 | 不检测模块，可设置多个模块，取值：
    - **waf**：表示网站白名单。
    - **cc**：表示系统CC防护。
    - **customrule**：表示自定义规则。
    - **blacklist**：表示IP黑名单。
    - **antiscan**：表示扫描防护。
    - **regular**：表示规则防护引擎。
    - **deeplearning**：表示深度学习引擎。
    - **antifraud**：表示数据风控。
    - **dlp**：表示防敏感信息泄露。
    - **tamperproof**：表示网站防篡改。
    - **bot_intelligence**：表示爬虫威胁情报。
    - **bot_algorithm**：表示智能算法。
    - **bot_wxbb**：表示App防护。
  - **bypassTags**：String类型 | 必选 | 不检测的模块列表。
  - **origin**：String类型 | 可选 | 白名单规则的来源。取值固定为**ai**，表示白名单规则由WAF智能规则托管功能自动添加。不返回该参数表示白名单规则包括您手动添加的规则和智能规则托管功能自动添加的规则。

- conditions：Array类型 | 必选 | 匹配条件，以JSON字符串格式进行描述，具体包含以下参数：
  - key：匹配字段，取值：URL、IP、Referer、User-Agent、Params、Cookie、Content-Type、Content-Length、X-Forwarded-For、Post-Body、Http-Method、Header、URLPath。
  - opCode：逻辑符，取值：
    - 11：表示等于。
    - 10：表示不等于。
    - 41：表示等于多值之一。
    - 50：表示不等于任一值。
    - 1：表示包含。
    - 0：表示不包含。
    - 51：表示包含多值之一。
    - 52：表示不包含任一值。
    - 82：表示存在。
    - 2：表示不存在。
    - 21：表示长度等于。
    - 22：表示长度大于。
    - 20：表示长度小于。
    - 60：表示正则不匹配。
    - 61：表示正则匹配。
    - 72：表示前缀匹配。
    - 81：表示后缀匹配。
    - 80：表示内容为空。
  - values：匹配内容。根据需要设置相应的内容，以String类型表示。
  - contain：同样表示规则条件的逻辑符，取值与opCode参数相同。
  - opValue：逻辑符的简写含义，您可以参考opCode参数取值说明了解详细信息。
  - pattern：同样表示逻辑符的简写含义，取值与opValue参数相同。
- expressions：Array类型 | 必选 | 规则条件表达式，以更易读的方式表示所有规则条件信息。
- 示例

```
    {
        "name": "test",
        "tags": ["cc","customrule"],
        "bypassTags":"antifraud,dlp,tamperproof",
        "conditions":[{"contain":1,"values":"login","pattern":"contain","opCode":1,"opV
alue":"contain","key":"URL"}],
        "expressions":["request_uri contains 'login' "]
   }
```

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeProtectionModuleRules
&InstanceId=waf_elasticity-cn-0xldbqt****
&Domain=www.example.com
&DefenseType=ac_highfreq
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<?xml version="1.0" encoding="UTF-8" ?>
<DescribeProtectionModuleRulesResponse>
 <TotalCount>1</TotalCount>
 <Rules>
  <Version>2</Version>
  <Status>1</Status>
  <Content>
   <count>60</count>
   <interval>60</interval>
   <ttl>300</ttl>
  </Content>
  <RuleId>42755</RuleId>
  <Time>1570700044</Time>
 </Rules>
 <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</DescribeProtectionModuleRulesResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "TotalCount" : 1,
  "Rules" : [ {
    "Version" : 2,
    "Status" : 1,
    "Content" : {
      "count" : 60,
      "interval" : 60,
      "ttl" : 300
    },
    "RuleId" : 42755,
    "Time" : 1570700044
  } ],
  "RequestId" : "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

6.7. CreateProtectionModuleRule

调用CreateProtectionModuleRule，在指定的WAF防护功能模块（包括Web入侵防护、数据安全、高级防护、Bot管理、访问控制或限流等模块）中创建规则配置。

使用说明

本接口用于在指定的WAF防护功能模块（包括Web入侵防护、数据安全、高级防护、Bot管理、访问控制或限流等模块）中创建规则配置。您可以通过设置**DefenseType**参数值指定防护功能模块配置。具体参数值的含义，请参见请求参数**DefenseType**的描述。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateProtectionModuleRule	要执行的操作。取值：**CreateProtectionModuleRule**。
Domain	String	是	www.example.com	要添加防护规则配置的域名。 **说明** 您可以调用DescribeDomainNames查询所有已添加到WAF进行防护的域名。

名称	类型	是否必选	示例值	描述
DefenseType	String	是	ac_custom	要配置的防护功能模块。取值： • **waf-codec**：表示规则防护引擎解码设置。 • **tamperproof**：表示网站防篡改规则配置。 • **dlp**：表示防敏感信息泄漏规则配置。 • **ng_account**：表示账户安全规则配置。 • **antifraud**：表示数据风控防护请求配置。 • **antifraud_js**：表示数据风控JS插入页面配置。 • **bot_algorithm**：表示Bot管理的智能算法规则。 • **bot_wxbb_pkg**：表示App防护的版本防护规则。 • **bot_wxbb**：表示App防护的路径防护规则。 • **ac_custom**：表示自定义防护策略规则配置。 • **whitelist**：表示白名单规则配置。
Rule	String	是	{"action":"monitor","name":"test","scene":"custom_acl","conditions":[{"opCode":1,"key":"URL","values":"/example"}]}	规则配置内容，以一系列参数构造的JSON格式转化成字符串。 **说明** 根据所指定的防护功能模块配置（DefenseType）不同，具体涉及的参数有所不同。详细信息，请参见Rule参数具体说明。
InstanceId	String	是	waf-cn-0xldbqt****	WAF实例ID。 **说明** 您可以调用DescribeInstanceInfo查询当前WAF实例的ID。

Rule参数具体说明

- 规则防护引擎解码设置（**waf-codec**）对应的JSON字符串中包含以下参数：
  - **codecList**：Array类型 | 必选 | 启用的解码配置项。您可在Web应用防火墙控制台中查看该参数支持填写的参数值。

- 示例

```
{
    "codecList":["url","base64"]
}
```

- 网站防篡改规则配置（tamperproof）对应的JSON字符串中包含以下参数：
  - uri：String类型 | 必选 | 所需防护的具体URL。
  - name：String类型 | 必选 | 规则名称。
  - 示例

```
{
    "name":"example",
    "uri":"http://www.aliyundoc.com/example"
}
```

- 防敏感信息泄露规则配置（dlp）对应的JSON字符串中包含以下参数：
  - name：String类型 | 必选 | 规则名称。
  - conditions：Array类型 | 必选 | 以JSON字符串格式描述匹配条件，支持设置最多两条匹配条件且条件间的关系为并且。其中包含以下具体参数：
    - key：匹配项。取值：
      - 0：表示防护的URL。
      - 10：表示敏感信息。
      - 11：表示响应码。

        > 说明 您无法在conditions参数中同时为响应码（11）和敏感信息（10）设置匹配条件。

    - operation：匹配逻辑。取值固定为1，表示包含。
    - value：以JSON字符串描述匹配条件值，支持填写多个条件值。其中包含以下具体参数：
      - v：仅适用于匹配项（key）为URL（0）或响应码（11）的场景。
        - URL：当 `"key":0` 时，参数值为URL地址。
        - 响应码：当 `"key":11` ，参数取值范围包括400、401、402、403、404、405-499、500、501、502、503、504、505-599。
      - k：仅适用于匹配项（key）为敏感信息（10）的场景。取值范围：
        - 100：表示身份证。
        - 101：表示信用卡。
        - 102：表示电话号码。
        - 103：表示默认敏感词。

- action：匹配动作。取值：
  - 3：表示告警。
  - 10：表示敏感信息过滤，该动作仅适用于包含敏感信息（ `"key":10` ）的匹配条件场景。
  - 11：表示返回系统内置拦截页面，该动作仅适用于包含响应码（ `"key":11` ）的匹配条件场景。
- 示例

```
  {
 "name":"example",
 "conditions":[{"key":11,"operation":1,"value":[{"v":401}]},{"key":"0","operation":1,"v
alue":[{"v":"www.aliyundoc.com"}]}],
 "action":3
  }
```

- 账户安全规则配置（ng_account ）对应的JSON字符串中包含以下参数：
  - url_path：String类型 | 必选 | 检测接口，以URL路径表示，必须以正斜线（/）开头。
  - method：String类型 | 必选 | 检测的请求方式，包括POST、GET、PUT、DELETE。支持设定多个请求方式，以英文逗号（,）分隔。
  - account_left：String类型 | 必选 | 账号参数名。
  - password_left：String类型 | 可选 | 密码参数名。
  - action：String类型 | 必选 | 防护动作。取值：
    - monitor：表示预警。
    - block：表示拦截。
  - 示例

```
    {
        "url_path":"/example",
        "method":"POST,GET,PUT,DELETE",
        "account_left":"aaa",
        "password_left:"123",
        "action":"monitor"
    }
```

- 数据风控防护请求配置（antifraud）对应的JSON字符串中包含以下参数：
  - uri：String类型 | 必选 | 具体的防护请求URL。
  - 示例

```
    {
        "uri": "http://1.example.com/example"
    }
```

- 数据风控JS插入页面配置（antifraud_js）对应的JSON字符串中包含以下参数：
  - uri：String类型 | 必选 | 需要插入数据风控JS页面的URL，系统将为所指定的URL路径下的所有页面插入数据风控JS，必须以正斜线（/）开头。

- **示例**

```
{
    "uri": "/example/example"
}
```

- Bot管理的智能算法规则配置（**bot_algorithm**）对应的JSON字符串中包含以下参数：
  - **name**：String类型 | 必选 | 规则名称。
  - **algorithmName**：String类型 | 必选 | 算法名称。取值：
    - **RR**：表示专项资源爬虫识别算法。
    - **PR**：表示定向路径爬虫识别算法。
    - **DPR**：表示参数轮询爬虫识别算法。
    - **SR**：表示动态IP爬虫识别算法。
    - **IND**：表示代理设备爬虫识别算法。
    - **Periodicity**：表示周期性爬虫识别算法。
  - **timeInterval**：Integer类型 | 必选 | 检测周期。取值：30、60、120、300、600，单位：秒。
  - **action**：String类型 | 必选 | 处置动作。取值：
    - **monitor**：表示观察。
    - **captcha**：表示滑块。
    - **js**：表示JavaScript校验。
    - **block**：表示阻断。选择阻断作为处置动作时，必须传入阻断时长（**blocktime**）参数。
  - **blocktime**：Integer类型 | 可选 | 阻断时长。单位：分钟。取值范围：1~600。
  - **config**：String类型 | 必选 | 算法配置信息，以JSON字符串格式表示。算法配置信息中的具体子参数与所选择的算法名称（**algorithmName**）相关。
    - 专项资源爬虫识别算法（**RR**）对应的配置信息应包含以下子参数：
      - **resourceType**：Integer类型 | 可选 | 请求的资源类型。取值：
        - **1**：表示动态资源类型。
        - **2**：表示静态资源类型。
        - **-1**：表示自定义资源类型。选择自定义资源组时，需要再传入**extensions**参数，以字符串格式指定具体的资源后缀名，多个后缀名间以英文逗号（,）分隔，例如 `css,jpg,xls` 。
      - **minRequestCountPerIp**：Integer类型 | 必选 | 检测周期中检测IP的范围，大于等于一定访问请求数量的IP才会被检测。通过该参数指定访问请求数量的最小值。取值范围：5~10000。
      - **minRatio**：Float类型 | 必选 | 风险判定条件，即IP访问请求中访问指定资源类型的占比阈值（对应专项资源爬虫识别算法）或IP访问请求中访问指定路径的占比阈值（对应定向路径爬虫识别算法），超过阈值后判定为风险。取值范围：0.01~1。

- 定向路径爬虫识别算法（PR）对应的配置信息应包含以下子参数：
  - **keyPathConfiguration**：Array类型 | 可选 | 请求的路径信息，支持指定最多10条路径，只在使用定向路径爬虫识别算法时需传入该子参数。以JSON字符串格式表示，具体包含以下参数：
    - **method**：String类型 | 必选 | 请求方法。取值：**POST**、**GET**、**PUT**、**DELETE**、**HEAD**、**OPTIONS**。
    - **url**：String类型 | 必选 | 请求路径关键字，必须以正斜线（/）开头。
    - **matchType**：String类型 | 必选 | 匹配方式，与请求路径关键字（**url**）参数结合指定请求路径。取值：**all**（精准匹配）、**prefix**（前缀匹配）、**regex**（正则匹配）。
  - **minRequestCountPerIp**：Integer类型 | 必选 | 检测周期中检测IP的范围，大于等于一定访问请求数量的IP才会被检测。通过该参数指定访问请求数量的最小值。取值范围：5~10000。
  - **minRatio**：Float类型 | 必选 | 风险判定条件，即IP访问请求中访问指定资源类型的占比阈值（对应专项资源爬虫识别算法）或IP访问请求中访问指定路径的占比阈值（对应定向路径爬虫识别算法），超过阈值后判定为风险。取值范围：0.01~1。
- 参数轮询爬虫识别算法（DPR）对应的配置信息应包含以下子参数：
  - **method**：String类型 | 必选 | 请求方法。取值：**POST**、**GET**、**PUT**、**DELETE**、**HEAD**、**OPTIONS**。
  - **urlPattern**：String类型 | 必选 | 关键参数路径，必须以正斜线（/）开头。用{}表示关键参数，配置多个{}时将拼接这些参数作为关键参数。例如，`/company/{}/{}/{}/user.php?uid={}`。
  - **minRequestCountPerIp**：Integer类型 | 必选 | 检测周期中检测IP的范围，大于等于一定访问请求数量的IP才会被检测。通过该参数指定访问请求数量的最小值。取值范围：5~10000。
  - **minRatio**：Float类型 | 必选 | 风险判定条件，即IP访问请求中不同关键参数值的计数占比阈值，超过阈值后判定为风险。取值范围：0.01~1。
- 动态IP爬虫识别算法（SR）对应的配置信息应包含以下子参数：
  - **maxRequestCountPerSrSession**：Integer类型 | 必选 | 通过设定每个会话中存在的最小请求次数定义异常会话，即单个会话中的请求次数小于该值即判定为异常会话。取值范围：1~8。
  - **minSrSessionCountPerIp**：Integer类型 | 必选 | 风险判定条件，即IP访问请求中存在的异常会话数量阈值，单个IP访问请求中的异常会话次数超过该值后判定为风险。取值范围：5~300。
- 代理设备爬虫识别算法（IND）对应的配置信息应包含以下子参数：
  - **minIpCount**：Integer类型 | 必选 | 恶意设备判定条件，即设备使用WIFI关联的IP变换个数阈值，超过该阈值后判定为风险。取值范围：5~500。
  - **keyPathConfiguration**：Array类型 | 可选 | 检测路径信息，支持指定最多10条路径。以JSON字符串格式表示，具体包含以下参数：
    - **method**：String类型 | 必选 | 请求方法。取值：**POST**、**GET**、**PUT**、**DELETE**、**HEAD**、**OPTIONS**。
    - **url**：String类型 | 必选 | 检测路径关键字，必须以正斜线（/）开头。
    - **matchType**：String类型 | 必选 | 匹配方式，与检测路径关键字（**url**）参数结合指定请求路径。取值：**all**（精准匹配）、**prefix**（前缀匹配）、**regex**（正则匹配）。

- 周期性爬虫识别算法（Periodicity）对应的配置信息应包含以下子参数：
  - minRequestCountPerIp：Integer类型 | 必选 | 检测周期中检测IP的范围，大于等于一定访问请求数量的IP才会被检测。通过该参数指定访问请求数量的最小值。取值范围：5~10000。
  - level：Integer类型 | 必选 | 风险判定等级，即访问IP的周期性特征的明显程度。取值：
    - 0：表示明显。
    - 1：表示中等。
    - 2：表示较弱。

- 示例

```
    {
        "name":"代理设备爬虫识别",
        "algorithmName":"IND",
        "timeInterval":"60",
        "action":"monitor",
        "config":{
            "minIpCount":5,
            "keyPathConfiguration":[{"url":"/index","method":"GET","matchType":"prefix"
}]
        }
    }
```

- App防护的版本防护规则配置（bot_wxbb_pkg）对应的JSON字符串中包含以下参数：
  - name：String类型 | 必选 | 规则名称。
  - action：String类型 | 必选 | 处置动作。取值：
    - test：表示观察。
    - close：表示阻断。
  - nameList：Array类型 | 必选 | 合法版本信息，最多指定五条规则。以JSON字符串方式表示，具体包含以下参数：
    - name：String类型 | 必选 | 合法包名称。
    - signList：Array类型 | 必选 | 对应的包签名，最多填写15个，以英文逗号（,）分隔。
  - 示例

```
    {
        "name":"test",
        "action":"close",
        "nameList":[{
            "name":"apk-xxxx",
            "signList":["xxxxxx","xxxxx","xxxx","xx"]
        }]
    }
```

- App防护的路径防护规则配置（bot_wxbb）对应的JSON字符串中包含以下参数：
  - name：String类型 | 必选 | 规则名称。
  - uri：String类型 | 必选 | 防护路径，必须以正斜线（/）开头。

- matchType：String类型 | 必选 | 匹配方式。取值：all（精准匹配）、prefix（前缀匹配）、regex（正则匹配）。
- arg：String类型 | 必选 | 参数包含，与匹配方式（matchType）参数结合指定防护路径配置。
- action：String类型 | 必选 | 处置动作。取值：
  - test：表示观察。
  - close：表示阻断。
- hasTag：Boolean类型 | 必选 | 是否需要自定义加签字段。
  - true：表示是。选择需要自定义加签字段时，需传入wxbbVmpFieldType和wxbbVmpFieldValue参数指定加签字段的类型和对应值。
  - false：表示否。
- wxbbVmpFieldType：Integer类型 | 可选 | 自定义加签字段类型。当hasTag参数值为true时，必须传入参数。取值：
  - 0：表示header。
  - 1：表示参数。
  - 2：表示cookie。
- wxbbVmpFieldValue：String类型 | 可选 | 自定义加签字段值。当hasTag参数值为true时，必须传入参数。
- blockInvalidSign：Integer类型 | 必选 | 是否对非法签名执行处置动作，固定值1。路径防护规则的默认防护策略。
- blockProxy：Integer类型 | 可选 | 是否对代理执行处置动作，固定值1。如果无需对代理行为执行处置动作时无需传入该参数。
- blockSimulator：Integer类型 | 可选 | 是否对模拟器执行处置动作，固定值1。如果无需对模拟器行为执行处置动作时无需传入该参数。
- 示例

```
{
    "name":"test",
    "uri":"/index",
    "matchType":"all",
    "arg":"test",
    "action":"close",
    "hasTag":true,
    "wxbbVmpFieldType":2,
    "wxbbVmpFieldValue":"test",
    "blockInvalidSign":1,
    "blockProxy":1
}
```

- 自定义防护策略规则配置（ac_custom），通过其对应的JSON字符串中的scene参数来设置ACL访问控制规则和CC攻击防护规则。
  - 设置ACL访问控制规则（scene参数值为custom_acl），其对应的JSON字符串中包含以下参数：
    - name：String类型 | 必选 | 规则名称。
    - scene：String类型 | 必选 | 防护类型。设置ACL访问控制规则时。取值固定为custom_acl。

- action：String类型 | 必选 | 处置动作。取值：
  - monitor：表示观察。
  - captcha：表示滑块。
  - captcha_strict：表示严格滑块。
  - js：表示JS验证。
  - block：表示阻断。
- conditions：Array类型 | 必选 | 匹配条件，支持填写最多五个匹配条件。以JSON字符串格式进行描述，具体包含以下参数：
  - key：匹配字段。取值范围：URL、IP、Referer、User-Agent、Params、Cookie、Content-Type、Content-Length、X-Forwarded-For、Post-Body、Http-Method、Header、URLPath。
  - opCode：逻辑符。取值：

    > 说明 并不是每一个自定义规则的匹配字段（key）都能对应配置全部的逻辑符（opcode）。关于不同匹配字段支持使用的逻辑符，请以WAF控制台自定义规则中匹配字段和逻辑符的关联关系为准。

    - 11：表示等于。
    - 10：表示不等于。
    - 41：表示等于多值之一。
    - 50：表示不等于任一值。
    - 1：表示包含。
    - 0：表示不包含。
    - 51：表示包含多值之一。
    - 52：表示不包含任一值。
    - 82：表示存在。
    - 2：表示不存在。
    - 21：表示长度等于。
    - 22：表示长度大于。
    - 20：表示长度小于。
    - 60：表示正则不匹配。
    - 61：表示正则匹配。
    - 72：表示前缀匹配。
    - 81：表示后缀匹配。
    - 80：表示内容为空。
  - values：匹配内容。根据需要填写相应的内容，以String类型表示。

    > 说明 匹配条件参数中的逻辑符（opCode）、匹配内容（values）参数取值范围与所指定的匹配字段（key）相关。关于支持的匹配条件配置详细信息，请参见匹配条件字段说明。

- **示例**

```
{
    "action":"monitor",
    "name":"test",
    "scene":"custom_acl",
    "conditions":[{"opCode":1,"key":"URL","values":"/example"}]
}
```

- 设置CC攻击防护规则（**scene**参数值为**custom_cc**），对应的JSON字符串中包含以下参数：
  - **name**：String类型 | 必选 | 规则名称。
  - **scene**：String类型 | 必选 | 防护类型。设置CC攻击防护规则时，固定为**custom_cc**。

- conditions：Array类型 | 必选 | 匹配条件，支持填写最多五个匹配条件。以JSON字符串格式进行描述，具体包含以下参数：
  - key：匹配字段。取值范围：URL、IP、Referer、User-Agent、Params、Cookie、Content-Type、Content-Length、X-Forwarded-For、Post-Body、Http-Method、Header、URLPath。
  - opCode：逻辑符。取值：

    > 说明 并不是每一个自定义规则的匹配字段（key）都能对应配置全部的逻辑符（opcode）。关于不同匹配字段支持使用的逻辑符，请以WAF控制台自定义规则中匹配字段和逻辑符的关联关系为准。

    - 11：表示等于。
    - 10：表示不等于。
    - 41：表示等于多值之一。
    - 50：表示不等于任一值。
    - 1：表示包含。
    - 0：表示不包含。
    - 51：表示包含多值之一。
    - 52：表示不包含任一值。
    - 82：表示存在。
    - 2：表示不存在。
    - 21：表示长度等于。
    - 22：表示长度大于。
    - 20：表示长度小于。
    - 60：表示正则不匹配。
    - 61：表示正则匹配。
    - 72：表示前缀匹配。
    - 81：表示后缀匹配。
    - 80：表示内容为空。
  - values：匹配内容。根据需要填写相应的内容，以String类型表示。

    > 说明 匹配条件参数中的逻辑符（opCode）、匹配内容（values）参数取值范围与所指定的匹配字段（key）相关。

- action：String类型 | 必选 | 处置动作。取值：
  - monitor：表示观察。
  - captcha：表示滑块。
  - captcha_strict：表示严格滑块。
  - js：表示JS验证。
  - block：表示阻断。

- ratelimit：JSON格式 | 必选 | 频率设置。以JSON字符串格式进行描述，具体包含以下参数：
  - target：String类型 | 必选 | 统计对象类型。取值：
    - remote_addr：表示IP。
    - cookie.acw_tc：表示Session。
    - queryarg：表示自定义参数。选择自定义参数时，必须在subkey参数中填写需要统计的自定义参数名称。
    - cookie：表示自定义cookie。选择自定义cookie时，必选在subkey参数中填写需要统计的cookie内容。
    - header：表示自定义header。选择自定义header时，必选在subkey参数中填写需要统计的header内容。
  - subkey：String类型 | 可选 | 当target参数值为cookie、header或queryarg时，必选在subkey参数中填写对应的信息。
  - interval：Integer类型 | 必选 | 统计时长（单位：秒），即访问次数的统计周期，与阈值（threshold）参数配合。
  - threshold：Integer类型 | 必选 | 在检测时长内，允许单个统计对象访问被防护地址的次数阈值。
  - status：JSON格式 | 可选 | 响应码频率设置。以JSON字符串格式进行描述，具体包含以下参数：
    - code：Integer类型 | 必选 | 指定响应码。
    - count：Integer类型 | 可选 | 出现次数阈值，即表示当指定的响应码出现次数超过该阈值时命中防护规则。取值范围：1~999999999。count参数与ratio参数两者选其一，不可同时配置。
    - ratio：Integer类型 | 可选 | 出现比例阈值（百分比），即表示当指定的响应码出现比例超过该阈值时命中防护规则。取值范围：1~100。count参数与ratio参数两者选其一，不可同时配置。
  - scope：String类型 | 必选 | 生效范围。取值：
    - rule：表示当前特征匹配范围内。
    - domain：表示当前规则作用的域名范围内。
  - ttl：Integer类型 | 必选 | 处置动作的生效时长（单位：秒）。取值范围：60~86400。

- **示例**

```
{
    "name":"CC防护",
    "conditions":[{"opCode":1,"key":"URL","values":"/example"}],
    "action":"block",
    "scene":"custom_cc",
    "ratelimit":{
        "target": "remote_addr",
        "interval": 300,
        "threshold": 2000,
        "status": {
            "code": 404,
            "count": 200
        },
        "scope": "rule",
        "ttl": 1800
    }
}
```

- 网站白名单规则配置（whitelist）对应的JSON字符串中包含以下参数：
  - **name**：String类型 | 必选 | 规则名称。

- tags：Array类型 | 必选 | 不检测模块。不同类型的白名单规则支持设置的不检测模块（tags）不同，具体说明如下：

  > 说明 tags的取值只能包含具体白名单类型下罗列的取值。例如，tags取值不允许同时包含regular和cc，因为regular属于Web入侵防护白名单下的取值、cc属于访问控制/限流白名单下的取值。

  - 如需设置全局白名单，tags取值：
    - waf：表示不检测所有防护模块。
  - 如需设置Web入侵防护白名单，tags取值（可设置多个）：
    - regular：表示不检测规则防护引擎（包含所有防护规则）。
    - regular_rule：表示不检测规则防护引擎中的指定防护规则（如选择该取值，必须通过regularRules参数设置不检测的规则ID）。
    - regular_type：表示不检测规则防护引擎中指定类型的防护规则（如选择该取值，必须通过regularTypes参数设置不检测的规则类型）。
    - deeplearning：表示不检测深度学习引擎。
  - 如需设置访问控制/限流白名单，tags取值（可设置多个）：
    - cc：表示不检测CC安全防护模块。
    - customrule：表示不检测自定义防护策略。
    - blacklist：表示不检测IP黑名单模块。
    - antiscan：表示不检测扫描防护模块。
  - 如需设置数据安全白名单，tags取值（可设置多个）：
    - dlp：表示不检测防敏感信息泄露模块。
    - tamperproof：表示不检测网站防篡改模块。
    - account：表示不检测账户安全模块。
  - 如需设置Bot防护白名单，tags取值（可设置多个）：
    - bot_intelligence：表示不检测爬虫威胁情报模块。
    - bot_algorithm：表示不检测典型爬虫行为识别模块。
    - bot_wxbb：表示不检测App防护模块。
    - antifraud：表示不检测数据风控模块。
- regularRules：Array类型 | 可选 | 不检测的防护规则ID列表。如果tags参数的取值中包含regular_rule，必须填写该参数。您可以在WAF控制台的**防护规则组**页面，通过**新建规则组**，查询WAF包含的所有Web攻击防护规则，获取相关规则的ID。具体操作，请参见自定义防护规则组。

- regularTypes：Array类型 | 可选 | 不检测的防护规则类型列表。如果tags参数取值中包含regular_type，必须填写该参数。取值：
  - sqli：表示SQL注入。
  - xss：表示跨站脚本。
  - code_exec：表示代码执行。
  - lfilei：表示本地文件包含。
  - rfilei：表示远程文件包含。
  - webshell：表示WebShell。
  - vvip：表示定制的防护规则。
  - other：表示其他类型。

- conditions：Array类型 | 必选 | 匹配条件，支持填写最多五个匹配条件。以JSON字符串格式进行描述，具体包含以下参数：
  - key：匹配字段。取值范围：URL、IP、Referer、User-Agent、Params、Cookie、Content-Type、Content-Length、X-Forwarded-For、Post-Body、Http-Method、Header、URLPath。
  - opCode：逻辑符。取值：

    > 说明 并不是每一个自定义规则的匹配字段（key）都能对应配置全部的逻辑符（opcode）。关于不同匹配字段支持使用的逻辑符，请以WAF控制台自定义规则中匹配字段和逻辑符的关联关系为准。

    - 11：表示等于。
    - 10：表示不等于。
    - 41：表示等于多值之一。
    - 50：表示不等于任一值。
    - 1：表示包含或属于。
    - 0：表示不包含或不属于。
    - 51：表示包含多值之一。
    - 52：表示不包含任一值。
    - 82：表示存在。
    - 2：表示不存在。
    - 21：表示长度等于。
    - 22：表示长度大于。
    - 20：表示长度小于。
    - 60：表示正则不匹配。
    - 61：表示正则匹配。
    - 72：表示前缀匹配。
    - 81：表示后缀匹配。
    - 80：表示内容为空。
    - 30：表示值小于。
    - 31：表示值大于。
  - values：匹配内容。根据需要填写相应的内容，以String类型表示。

    > 说明 匹配条件参数中的逻辑符（opCode）、匹配内容（values）参数取值范围与所指定的匹配字段（key）相关。

- 示例

```
 {
     "name": "test",
     "tags": ["cc","customrule"],
     "conditions":[{"opCode":1,"key":"URL","values":"/example"}],
}
```

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateProtectionModuleRule
&Domain=www.example.com
&DefenseType=ac_custom
&Rule= {"action":"monitor","name":"test","scene":"custom_acl","conditions":[{"opCode":1,"ke
y":"URL","values":"/example"}]}
&InstanceId=waf-cn-0xldbqt****
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<CreateProtectionModuleRuleResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</CreateProtectionModuleRuleResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

6.8. ModifyProtectionModuleRule

调用ModifyProtectionModuleRule修改指定WAF防护功能模块（包括Web入侵防护、数据安全、高级防护、Bot管理、访问控制或限流、白名单等模块）中的规则配置。

使用说明

本接口用于修改指定WAF防护功能模块（包括Web入侵防护、数据安全、高级防护、Bot管理、访问控制或限流、白名单等模块）中的规则配置。您可以通过设置**DefenseType**参数值指定防护功能模块配置。具体参数值的含义，请参见请求参数**DefenseType**的描述。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyProtectionModuleRule	要执行的操作。取值：**ModifyProtectionModuleRule**。
Domain	String	是	www.example.com	要修改规则配置的域名。 **说明** 您可以调用DescribeDomainNames查询所有已添加到WAF进行防护的域名。

名称	类型	是否必选	示例值	描述
DefenseType	String	是	ac_custom	要修改的规则配置所属防护功能模块。取值： • **tamperproof**：表示配置网站防篡改规则。 • **dlp**：表示配置防敏感信息泄漏规则。 • **ng_account**：表示配置账户安全规则。 • **bot_intelligence**：表示配置爬虫威胁情报。 • **antifraud**：表示配置数据风控防护请求。 • **antifraud_js**：表示配置数据风控JS插入页面。 • **bot_algorithm**：表示配置Bot管理的智能算法规则。 • **bot_wxbb_pkg**：表示配置App防护的版本防护规则。 • **bot_wxbb**：表示配置App防护的路径防护规则。 • **ac_blacklist**：表示配置IP黑名单规则。 • **ac_highfreq**：表示配置高频Web攻击IP自动封禁规则。 • **ac_dirscan**：表示配置目录扫描防护规则。 • **ac_custom**：表示配置自定义防护策略规则。 • **whitelist**：表示配置白名单规则。
Rule	String	是	{"action":"monitor","name":"test","scene":"custom_acl","conditions":[{"opCode":1,"key":"URL","values":"/example"}]}	规则配置内容，以一系列参数构造的JSON格式转化成字符串。 **说明** 根据所指定的防护功能模块配置（DefenseType）不同，具体涉及的参数有所不同。详细信息，请参见Rule参数具体说明。
RuleId	Long	是	369998	要修改的规则配置对应的规则ID。 **说明** 您可以调用DescribeProtectionModuleRules查询所有已创建的规则的ID。

名称	类型	是否必选	示例值	描述
LockVersion	Long	是	2	要修改的规则配置的版本号。 **说明** 您可以调用DescribeProtectionModuleRules查询规则配置的版本号。
InstanceId	String	是	waf-cn-0xldbqt****	WAF实例ID。 **说明** 您可以通过调用DescribeInstanceInfo查询当前WAF实例ID。

Rule参数具体说明

- 网站防篡改规则配置（tamperproof）对应的JSON字符串中包含以下参数：
  - **uri**：String类型 | 必选 | 所需防护的具体URL。
  - **name**：String类型 | 必选 | 规则名称。
  - **status**：Integer类型 | 可选 | 规则的防护状态。取值：
    - 0（默认）：表示不生效。
    - 1：表示生效。
  - **示例**

```
{
    "name":"example",
    "uri":"http://www.example.com/example",
    "status":1
}
```

- 防敏感信息泄露规则配置（dlp）对应的JSON字符串中包含以下参数：
  - **name**：String类型 | 必选 | 规则名称。

- conditions：Array类型 | 必选 | 以JSON字符串格式描述匹配条件，支持设置最多两条匹配条件且条件间的关系为并且。其中包含以下具体参数：
  - key：匹配项。
    - 0：表示防护的URL。
    - 10：表示敏感信息。
    - 11：表示响应码。

      > 说明 您无法在conditions参数中同时为响应码（11）和敏感信息（10）设置匹配条件。

  - operation：匹配逻辑，取值固定为1，表示包含。
  - value：以JSON字符串描述匹配条件值，支持填写多个条件值。其中包含以下具体参数：
    - v：仅适用于匹配项（key）为URL（0）或响应码（11）的场景。
      - URL：当 `"key":0` 时，参数值为URL地址。
      - 响应码：当 `"key":11` ，参数取值包括400、401、402、403、404、405-499、500、501、502、503、504、505-599。
    - k：仅适用于匹配项（key）为敏感信息（10）的场景，取值：
      - 100：表示身份证。
      - 101：表示信用卡。
      - 102：表示电话号码。
      - 103：表示默认敏感词。
- action：匹配动作。
  - 3：表示告警。
  - 10：表示敏感信息过滤，该动作仅适用于包含敏感信息（ `"key":10` ）的匹配条件场景。
  - 11：表示返回系统内置拦截页面，该动作仅适用于包含响应码（ `"key":11` ）的匹配条件场景。
- 示例

```
  {
 "name":"example",
 "conditions":[{"key":11,"operation":1,"value":[{"v":401}]},{"key":"0","operation":1,"v
alue":[{"v":"www.example.com"}]}],
 "action":3
  }
```

- 账户安全规则配置（ng_account ）对应的JSON字符串中包含以下参数：
  - url_path：String类型 | 必选 | 检测接口，以URL路径表示，必须以“/”开头。
  - method：String类型 | 必选 | 检测的请求方式，包括POST、GET、PUT、DELETE。支持设定多个请求方式，以英文逗号（,）分隔。
  - account_left：String类型 | 必选 | 账号参数名。
  - password_left：String类型 | 可选 | 密码参数名。

- action：String类型 | 必选 | 防护动作。取值：
  - monitor：表示预警。
  - block：表示拦截。
- 示例

```
{
    "url_path":"/example",
    "method":"POST,GET,PUT,DELETE",
    "account_left":"aaa",
    "password_left:"123",
    "action":"monitor"
}
```

- Bot管理的爬虫威胁情报配置（bot_intelligence）对应的JSON字符串中包含以下参数：
  - name：String类型 | 必选 | 规则名称，必须与规则ID（RuleId）参数对应。
  - urlList：Array类型 | 必选 | 防护路径，最多指定10个防护路径。以JSON字符串方式表示，具体包含以下参数：
    - mode：String类型 | 必选 | 匹配方式，与路径关键字（url）参数结合指定防护路径。取值：eq（精准匹配）、prefix-match（前缀匹配）、regex（正则匹配）。
    - url：String类型 | 必选 | 路径关键字，必须以“/”开头。
  - action：String类型 | 必选 | 处置动作。取值：
    - monitor：表示观察。
    - captcha：表示滑块。
    - captcha_strict：表示严格滑块 。
    - js：表示JavaScript校验。
    - block：表示阻断。
  - status：Integer类型 | 必选 | 启用状态。取值：
    - 0：表示禁用。
    - 1：表示启用。
  - 示例

```
{
    "urlList":[
        {"mode":"prefix-match","url":"/indexa"},
        {"mode":"regex","url":"/"},
        {"mode":"eq","url":"/"}],
    "name":"IDC IP库-腾讯云",
    "action":"captcha_strict",
    "status":1
}
```

- Bot管理的智能算法规则配置（bot_algorithm）对应的JSON字符串中包含以下参数：
  - name：String类型 | 必选 | 规则名称。

- algorithmName：String类型 | 必选 | 算法名称。取值：
  - RR：表示专项资源爬虫识别算法。
  - PR：表示定向路径爬虫识别算法。
  - DPR：表示参数轮询爬虫识别算法。
  - SR：表示动态IP爬虫识别算法。
  - IND：表示代理设备爬虫识别算法。
  - Periodicity：表示周期性爬虫识别算法。
- timeInterval：Integer类型 | 必选 | 检测周期。单位：秒，取值：30、60、120、300、600。
- action：String类型 | 必选 | 处置动作。取值：
  - monitor：表示观察。
  - captcha：表示滑块。
  - js：表示JavaScript校验。
  - block：表示阻断。选择阻断作为处置动作时，必须传入阻断时长（blocktime）参数。
- blocktime：Integer类型 | 可选 | 阻断时长。单位：分钟，取值：1~600。
- config：String类型 | 必选 | 算法配置信息，以JSON字符串格式表示。算法配置信息中的具体子参数与所选择的算法名称（algorithmName）相关。
  - 专项资源爬虫识别算法（RR）对应的配置信息应包含以下子参数：
    - resourceType：Integer类型 | 可选 | 请求的资源类型。取值：
      - 1：表示动态资源类型。
      - 2：表示静态资源类型。
      - -1：表示自定义资源类型。选择自定义资源组时，需要再传入extensions参数，以字符串格式指定具体的资源后缀名，多个后缀名间以英文逗号（,）分隔，例如 `css,jpg,xls` 。
    - minRequestCountPerIp：Integer类型 | 必选 | 检测周期中检测IP的范围，大于等于一定访问请求数量的IP才会被检测。通过该参数指定访问请求数量的最小值。取值范围：5~10000。
    - minRatio：Float类型 | 必选 | 风险判定条件，即IP访问请求中访问指定资源类型的占比阈值，超过阈值后判定为风险。取值范围：0.01~1。
  - 定向路径爬虫识别算法（PR）对应的配置信息应包含以下子参数：
    - keyPathConfiguration：Array类型 | 可选 | 请求的路径信息，支持指定最多10条路径，只在使用定向路径爬虫识别算法时需传入该子参数。以JSON字符串格式表示。具体包含以下参数：
      - method：String类型 | 必选 | 请求方法。取值：POST、GET、PUT、DELETE、HEAD、OPTIONS。
      - url：String类型 | 必选 | 请求路径关键字，必须以“/”开头。
      - matchType：String类型 | 必选 | 匹配方式，与请求路径关键字（url）参数结合指定请求路径。取值：all（精准匹配）、prefix（前缀匹配）、regex（正则匹配）。
    - minRequestCountPerIp：Integer类型 | 必选 | 检测周期中检测IP的范围，大于等于一定访问请求数量的IP才会被检测。通过该参数指定访问请求数量的最小值。取值范围：5~10000。
    - minRatio：Float类型 | 必选 | 风险判定条件，即IP访问请求中访问指定路径的占比阈值，超过阈值后判定为风险。取值范围：0.01~1。

- 参数轮询爬虫识别算法（DPR）对应的配置信息应包含以下子参数：
  - method：String类型 | 必选 | 请求方法。取值：POST、GET、PUT、DELETE、HEAD、OPTIONS。
  - urlPattern：String类型 | 必选 | 关键参数路径，必须以“/”开头。用{}表示关键参数，配置多个{}时将拼接这些参数作为关键参数。例如，`/company/{}/{}/{}/user.php?uid={}`。
  - minRequestCountPerIp：Integer类型 | 必选 | 检测周期中检测IP的范围，大于等于一定访问请求数量的IP才会被检测。通过该参数指定访问请求数量的最小值。取值范围：5~10000。
  - minRatio：Float类型 | 必选 | 风险判定条件，即IP访问请求中不同关键参数值的计数占比阈值，超过阈值后判定为风险。取值范围：0.01~1。
- 动态IP爬虫识别算法（SR）对应的配置信息应包含以下子参数：
  - maxRequestCountPerSrSession：Integer类型 | 必选 | 通过设定每个会话中存在的最小请求次数定义异常会话，即单个会话中的请求次数小于该值即判定为异常会话。取值范围：1~8。
  - minSrSessionCountPerIp：Integer类型 | 必选 | 风险判定条件，即IP访问请求中存在的异常会话数量阈值，单个IP访问请求中的异常会话次数超过该值后判定为风险。取值范围：5~300。
- 代理设备爬虫识别算法（IND）对应的配置信息应包含以下子参数：
  - minIpCount：Integer类型 | 必选 | 恶意设备判定条件，即设备使用WIFI关联的IP变换个数阈值，超过该阈值后判定为风险。取值范围：5~500。
  - keyPathConfiguration：Array类型 | 可选 | 检测路径信息，支持指定最多10条路径。以JSON字符串格式表示，具体包含以下参数：
    - method：String类型 | 必选 | 请求方法。取值：POST、GET、PUT、DELETE、HEAD、OPTIONS。
    - url：String类型 | 必选 | 检测路径关键字，必须以“/”开头。
    - matchType：String类型 | 必选 | 匹配方式，与检测路径关键字（url）参数结合指定请求路径。取值：all（精准匹配）、prefix（前缀匹配）、regex（正则匹配）。
- 周期性爬虫识别算法（Periodicity）对应的配置信息应包含以下子参数：
  - minRequestCountPerIp：Integer类型 | 必选 | 检测周期中检测IP的范围，大于等于一定访问请求数量的IP才会被检测。通过该参数指定访问请求数量的最小值。取值范围：5~10000。
  - level：Integer类型 | 必选 | 风险判定等级，即访问IP的周期性特征的明显程度。取值：
    - 0：表示明显。
    - 1：表示中等。
    - 2：表示较弱。

- **示例**

```
    {
        "name":"代理设备爬虫识别",
        "algorithmName":"IND",
        "timeInterval":"60",
        "action":"warn",
        "config":{
            "minIpCount":5,
            "keyPathConfiguration":[{"url":"/index","method":"GET","matchType":"prefix"
}]
        }
    }
```

- App防护的版本防护规则配置（bot_wxbb_pkg）对应的JSON字符串中包含以下参数：
  - name：String类型 | 必选 | 规则名称。
  - action：String类型 | 必选 | 处置动作。取值：
    - test：表示观察。
    - close：表示阻断。
  - nameList：Array类型 | 必选 | 合法版本信息，最多指定五条规则。以JSON字符串方式表示，具体包含以下参数：
    - name：String类型 | 必选 | 合法包名称。
    - signList：Array类型 | 必选 | 对应的包签名，最多填写15个，以英文逗号（,）分隔。
  - 示例

```
{
    "name":"test",
    "action":"close",
    "nameList":[{
        "name":"apk-xxxx",
        "signList":["xxxxxx","xxxxx","xxxx","xx"]
    }]
}
```

- App防护的路径防护规则配置（bot_wxbb）对应的JSON字符串中包含以下参数：
  - name：String类型 | 必选 | 规则名称。
  - uri：String类型 | 必选 | 防护路径，必须以“/”开头。
  - matchType：String类型 | 必选 | 匹配方式。取值：all（精准匹配）、prefix（前缀匹配）、regex（正则匹配）。
  - arg：String类型 | 必选 | 参数包含，与匹配方式（matchType）参数结合指定防护路径配置。
  - action：String类型 | 必选 | 处置动作。取值：
    - test：表示观察。
    - close：表示阻断。
  - hasTag：Boolean类型 | 必选 | 是否需要自定义加签字段。
    - true：表示是。选择需要自定义加签字段时，需传入wxbbVmpFieldType和wxbbVmpFieldValue参数指定加签字段的类型和对应值。
    - false：表示否。
  - wxbbVmpFieldType：Integer类型 | 可选 | 自定义加签字段类型。当hasTag参数值为true时，必须传入参数。取值：
    - 0：表示header。
    - 1：表示参数。
    - 2：表示cookie。
  - wxbbVmpFieldValue：String类型 | 可选 | 自定义加签字段值。当hasTag参数值为true时，必须传入参数。
  - blockInvalidSign：Integer类型 | 必选 | 是否对非法签名执行处置动作，固定值1。路径防护规则的默认防护策略。

- **blockProxy**：Integer类型 | 可选 | 是否对代理执行处置动作，固定值**1**。如果无需对代理行为执行处置动作时无需传入该参数。
- **blockSimulator**：Integer类型 | 可选 | 是否对模拟器执行处置动作，固定值**1**。如果无需对模拟器行为执行处置动作时无需传入该参数。
- **示例**

```
{
    "name":"test",
    "uri":"/index",
    "matchType":"all",
    "arg":"test",
    "action":"close",
    "hasTag":true,
    "wxbbVmpFieldType":2,
    "wxbbVmpFieldValue":"test",
    "blockInvalidSign":1,
    "blockProxy":1
}
```

- 数据风控防护请求配置（**antifraud**）对应的JSON字符串中包含以下参数：
  - **uri**：String类型 | 必选 | 具体的防护请求URL。
  - **示例**

```
{
    "uri": "http://1.example.com/example"
}
```

- 数据风控JS插入页面配置（**antifraud_js**）对应的JSON字符串中包含以下参数：
  - **uri**：String类型 | 必选 | 需要插入数据风控JS页面的URL，系统将为所指定的URL路径下的所有页面插入数据风控JS，必须以“/”开头。
  - **示例**

```
{
    "uri": "/example/example"
}
```

- IP黑名单规则配置（**ac_blacklist**）对应的JSON字符串中包含以下参数：
  - **remoteAddr**：Array类型 | 可选 | 黑名单中的IP。支持填写IP和IP地址段。多个IP以英文逗号（,）分隔，最多可以添加200个。填写空值表示清空IP黑名单。
  - **area**：Array类型 | 可选 | 地域级IP黑名单中的地域。使用JSON数组转化的字符串格式表示，JSON数组中的每个元素是一个结构体，包含以下字段：
    - **countryCodes**：Array类型 | 必选 | 国家代码。只填写 `["CN"]` ，表示封禁中国境内地域，必须同时填写**regionCodes**；填写 `["CN"]` 以外内容，表示封禁中国境外地域，无需填写**regionCodes**。您可以调用DescribeProtectionModuleCodeConfig查询中国境内地域代码和中国境外地域代码。
    - **regionCodes**：Array类型 | 可选 | 中国境内地域代码。

- **示例**

```
{
    "remoteAddr": [
        "1.XX.XX.1",
        "2.XX.XX.2"
    ],
    "area": [
        {
            "countryCodes": [
                "CN"
            ],
            "regionCodes": [
                "310000",
                "530000"
            ]
        },
        {
            "countryCodes": [
                "AD",
                "AL"
            ]
        }
    ]
}
```

- 高频Web攻击IP自动封禁规则配置（**ac_highfreq**）对应的JSON字符串中包含以下参数：
  - **interval**：Integer类型 | 必选 | 检测时间范围。单位：秒，取值范围：5~1800。
  - **ttl**：Integer类型 | 必选 | 封禁IP时长。单位秒，取值范围：60~86400。
  - **count**：Integer类型 | 必选 | Web攻击次数阈值，检测时间范围内攻击次数超过该值，触发封禁。取值范围：2~50000。
  - **示例**

```
    {
     "interval":60,
     "ttl":300,
     "count":60
     }
```

- 目录扫描防护规则配置（**ac_dirscan**）对应的JSON字符串中包含以下参数：
  - **interval**：Integer类型 | 必选 | 检测时间范围。单位秒，取值范围：5~1800。
  - **ttl**：Integer类型 | 必选 | 封禁IP时长。单位秒，取值范围：60~86400。
  - **count**：Integer类型 | 必选 | 访问次数阈值。取值范围：2~50000。
  - **weight**：Float类型 | 必选 | 404响应码占比阈值（百分比）。取值范围：0~1。
  - **uriNum**：Integer类型 | 必选 | 扫描目录数量阈值。取值范围：2~50000。

- **示例**

```
{
 "interval":10,
 "ttl":1800,
 "count":50,
 "weight":0.7,
    "uriNum":20
}
```

- 自定义防护策略规则配置（ac_custom），通过其对应的JSON字符串中的scene参数来设置ACL访问控制规则和CC攻击防护规则。

- 设置ACL访问控制规则（scene参数值为custom_acl），其对应的JSON字符串中包含以下参数：
  - name：String类型 | 必选 | 规则名称。
  - scene：String类型 | 必选 | 防护类型。设置ACL访问控制规则时，取值固定为custom_acl。
  - action：String类型 | 必选 | 处置动作。取值：
    - monitor：表示观察。
    - captcha：表示滑块。
    - captcha_strict：表示严格滑块。
    - js：表示JS验证。
    - block：表示阻断。
  - conditions：Array类型 | 必选 | 匹配条件，最多支持填写5个匹配条件。以JSON字符串格式进行描述，具体包含以下参数：
    - key：匹配字段。取值：URL、IP、Referer、User-Agent、Params、Cookie、Content-Type、Content-Length、X-Forwarded-For、Post-Body、Http-Method、Header、URLPath。
    - opCode：逻辑符。取值：
      - 0：表示不包含、不属于。
      - 1：表示包含、属于。
      - 2：表示不存在。
      - 10：表示不等于。
      - 11：表示等于。
      - 20：表示长度小于。
      - 21：表示长度等于。
      - 22：表示长度大于。
      - 30：表示值小于。
      - 31：表示值等于。
      - 32：表示值大于。
    - values：匹配内容。根据需要填写相应的内容，以String类型表示。

      > 说明 匹配条件参数中的逻辑符（opCode）、匹配内容（values）参数取值范围与所指定的匹配字段（key）相关。关于支持的匹配条件配置详细信息，请参见匹配条件字段说明。

    - 示例

```
{
    "action":"monitor",
    "name":"test",
    "scene":"custom_acl",
 "conditions":[{"opCode":1,"key":"URL","values":"/example"}]
}
```

- 设置CC攻击防护规则（scene参数值为custom_cc），对应的JSON字符串中包含以下参数：
  - name：String类型 | 必选 | 规则名称。

- scene：String类型 | 必选 | 防护类型。设置CC攻击防护规则时，取值固定为custom_cc。
- conditions：Array类型 | 必选 | 匹配条件，最多支持填写5个匹配条件。以JSON字符串格式进行描述，具体包含以下参数：
  - key：匹配字段。取值：URL、IP、Referer、User-Agent、Params、Cookie、Content-Type、Content-Length、X-Forwarded-For、Post-Body、Http-Method、Header、URLPath。
  - opCode：逻辑符。取值：
    - 0：表示不包含、不属于。
    - 1：表示包含、属于。
    - 2：表示不存在。
    - 10：表示不等于。
    - 11：表示等于。
    - 20：表示长度小于。
    - 21：表示长度等于。
    - 22：表示长度大于。
    - 30：表示值小于。
    - 31：表示值等于。
    - 32：表示值大于。
  - values：匹配内容。根据需要填写相应的内容，以String类型表示。

    > 说明 匹配条件参数中的逻辑符（opCode）、匹配内容（values）参数取值范围与所指定的匹配字段（key）相关。

- action：String类型 | 必选 | 处置动作，取值：
  - monitor：表示观察。
  - captcha：表示滑块。
  - captcha_strict：表示严格滑块。
  - js：表示JS验证。
  - block：表示阻断。
- ratelimit：JSON格式 | 必选 | 频率设置。以JSON字符串格式进行描述，具体包含以下参数：
  - target：String类型 | 必选 | 统计对象类型，取值：
    - remote_addr：表示IP。
    - cookie.acw_tc：表示Session。
    - queryarg：表示自定义参数。选择自定义参数时，必须在subkey参数中填写需要统计的自定义参数名称。
    - cookie：表示自定义cookie。选择自定义cookie时，必选在subkey参数中填写需要统计的cookie内容。
    - header：表示自定义header。选择自定义header时，必选在subkey参数中填写需要统计的header内容。
  - subkey：String类型 | 可选 | 当target参数值为cookie、header或queryarg时，必选在subkey参数中填写对应的信息。

- interval：Integer类型 | 必选 | 统计时长（单位：秒），即访问次数的统计周期，与阈值（threshold）参数配合。
- threshold：Integer类型 | 必选 | 在检测时长内，允许单个统计对象访问被防护地址的次数阈值。
- status：JSON格式 | 可选 | 响应码频率设置。以JSON字符串格式进行描述，具体包含以下参数：
  - code：Integer类型 | 必选 | 指定响应码。
  - count：Integer类型 | 可选 | 出现次数阈值，即表示当指定的响应码出现次数超过该阈值时命中防护规则。取值范围：1~999999999。count参数与ratio参数两者选其一，不可同时配置。
  - ratio：Integer类型 | 可选 | 出现比例阈值（百分比），即表示当指定的响应码出现比例超过该阈值时命中防护规则。取值范围：1~100。count参数与ratio参数两者选其一，不可同时配置。
- scope：String类型 | 必选 | 生效范围，取值：
  - rule：表示当前特征匹配范围内。
  - domain：表示当前规则作用的域名范围内。
- ttl：Integer类型 | 必选 | 处置动作的生效时长。单位：秒，取值范围：60~86400。
- 示例

```
        {
            "name":"CC防护",
            "conditions":[{"opCode":1,"key":"URL","values":"/example"}],
            "action":"block",
            "scene":"custom_cc",
            "ratelimit":{
                "target": "remote_addr",
                "interval": 300,
                "threshold": 2000,
                "status": {
                    "code": 404,
                    "count": 200
                },
                "scope": "rule",
                "ttl": 1800
            }
    }
```

- 网站白名单规则配置（whitelist）对应的JSON字符串中包含以下参数：
  - name：String类型 | 必选 | 规则名称。

- tags：Array类型 | 必选 | 不检测模块。不同类型的白名单规则支持设置的不检测模块（tags）不同，具体说明如下：

  > 说明 tags的取值只能包含具体白名单类型下罗列的取值。例如，tags取值不允许同时包含regular和cc，因为regular属于Web入侵防护白名单下的取值、cc属于访问控制/限流白名单下的取值。

  - 如需设置全局白名单，tags取值：
    - waf：表示不检测所有防护模块。
  - 如需设置Web入侵防护白名单，tags取值（可设置多个）：
    - regular：表示不检测规则防护引擎（包含所有防护规则）。
    - regular_rule：表示不检测规则防护引擎中的指定防护规则（如选择该取值，必须通过regularRules参数设置不检测的规则ID）。
    - regular_type：表示不检测规则防护引擎中指定类型的防护规则（如选择该取值，必须通过regularTypes参数设置不检测的规则类型）。
    - deeplearning：表示不检测深度学习引擎。
  - 如需设置访问控制/限流白名单，tags取值（可设置多个）：
    - cc：表示不检测CC安全防护模块。
    - customrule：表示不检测自定义防护策略。
    - blacklist：表示不检测IP黑名单模块。
    - antiscan：表示不检测扫描防护模块。
  - 如需设置数据安全白名单，tags取值（可设置多个）：
    - dlp：表示不检测防敏感信息泄露模块。
    - tamperproof：表示不检测网站防篡改模块。
    - account：表示不检测账户安全模块。
  - 如需设置Bot防护白名单，tags取值（可设置多个）：
    - bot_intelligence：表示不检测爬虫威胁情报模块。
    - bot_algorithm：表示不检测典型爬虫行为识别模块。
    - bot_wxbb：表示不检测App防护模块。
    - antifraud：表示不检测数据风控模块。
- regularRules：Array类型 | 可选 | 不检测的防护规则ID列表。如果tags参数的取值中包含regular_rule，必须填写该参数。您可以在WAF控制台的**防护规则组**页面，通过**新建规则组**，查询WAF包含的所有Web攻击防护规则，获取相关规则的ID。具体操作，请参见自定义防护规则组。

- regularTypes：Array类型 | 可选 | 不检测的防护规则类型列表。如果tags参数取值中包含regular_type，必须填写该参数。取值：
  - sqli：表示SQL注入。
  - xss：表示跨站脚本。
  - code_exec：表示代码执行。
  - lfilei：表示本地文件包含。
  - rfilei：表示远程文件包含。
  - webshell：表示WebShell。
  - vvip：表示定制的防护规则。
  - other：表示其他类型。
- conditions：Array类型 | 必选 | 匹配条件，最多支持填写5个匹配条件。以JSON字符串格式进行描述，具体包含以下参数：
  - key：匹配字段。取值：URL、IP、Referer、User-Agent、Params、Cookie、Content-Type、Content-Length、X-Forwarded-For、Post-Body、Http-Method、Header、URLPath。
  - opCode：逻辑符，取值：
    - 0：表示不包含、不属于。
    - 1：表示包含、属于。
    - 2：表示不存在。
    - 10：表示不等于。
    - 11：表示等于。
    - 20：表示长度小于。
    - 21：表示长度等于。
    - 22：表示长度大于。
    - 30：表示值小于。
    - 31：表示值等于。
    - 32：表示值大于。
  - values：匹配内容。根据需要填写相应的内容，以String类型表示。

    > **说明** 匹配条件参数中的逻辑符（opCode）、匹配内容（values）参数取值范围与所指定的匹配字段（key）相关。

- 示例

```
 {
     "name": "test",
     "tags": ["cc","customrule"],
     "conditions":[{"opCode":1,"key":"URL","values":"/example"}],
}
```

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyProtectionModuleRule
&Domain=www.example.com
&DefenseType=ac_custom
&Rule= {"action":"monitor","name":"test","scene":"custom_acl","conditions":[{"opCode":1,"ke
y":"URL","values":"/example"}]}
&RuleId=369998
&LockVersion=2
&InstanceId=waf-cn-0xldbqt****
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyProtectionModuleRuleResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</ModifyProtectionModuleRuleResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

6.9. ModifyProtectionRuleStatus

调用ModifyProtectionRuleStatus接口启用或禁用指定域名配置的WAF防护功能模块（包括网站防篡改、合法爬虫、爬虫威胁情报、自定义防护策略、网站白名单等模块）中的指定规则。

您可以通过设置DefenseType参数值指定防护功能模块配置。具体参数值的含义，请参见请求参数DefenseType的描述。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyProtectionRuleStatus	要执行的操作。取值：**ModifyProtectionRuleStatus**。
DefenseType	String	是	tamperproof	防护功能模块，取值： • **tamperproof**：网站防篡改 • **bot_crawler**：合法爬虫中的合法搜索引擎白名单 • **bot_intelligence**：爬虫威胁情报 • **ac_custom**：自定义防护策略 • **whitelist**：网站白名单
Domain	String	是	www.example.com	已添加的域名名称。
InstanceId	String	是	waf_elasticity-cn-0xldbqt****	WAF实例ID。 **说明** 您可以通过调用DescribeInstanceInfo接口查看当前WAF实例ID。
LockVersion	Long	是	2	规则配置记录版本号。
RuleId	Long	是	42755	配置规则ID。 **说明** 调用DescribeProtectionModuleRules接口可以查询到所有规则ID。
RuleStatus	Integer	是	1	配置规则状态。取值： • **0**：禁用 • **1**：启用

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	请求ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyProtectionRuleStatus
&DefenseType=tamperproof
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqt****
&LockVersion=2
&RuleId=42755
&RuleStatus=1
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<ModifyProtectionRuleStatusResponse>
   <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</ModifyProtectionRuleStatusResponse>
```

`JSON` 格式

```
{
    "RequestId": "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

6.10. DescribeDomainRuleGroup

调用DescribeDomainRuleGroup查询域名绑定的防护规则组的ID及智能规则托管功能的启用状态。

使用说明

本接口用于查询规则防护引擎下，指定域名绑定的防护规则组的ID及智能规则托管功能的启用状态。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainRuleGroup	要执行的操作。取值：**DescribeDomainRuleGroup**。
Domain	String	是	www.aliyundoc.com	要查询的域名。 **说明** 您可以调用DescribeDomainList查询所有已接入WAF防护的域名。
InstanceId	String	是	waf-cn-tl32ast****	WAF实例的ID。 **说明** 您可以调用DescribeInstanceInfo查询当前WAF实例的ID。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RuleGroupId	Long	1012	域名绑定的防护规则组的ID。取值： • **1011**：表示WAF内置的严格规则组。 • **1012**：表示WAF内置的中等规则组。 • **1013**：表示WAF内置的宽松规则组。 其他取值表示您自定义的规则组的ID。
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	本次请求的ID。
WafAiStatus	Integer	1	智能规则托管功能的启用状态。取值： • **0**：表示关闭。 • **1**：表示开启。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainRuleGroup
&Domain=www.aliyundoc.com
&InstanceId=waf-cn-tl32ast****
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeDomainRuleGroupResponse>
    <RuleGroupId>1012</RuleGroupId>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <WafAiStatus>1</WafAiStatus>
</DescribeDomainRuleGroupResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RuleGroupId" : 1012,
  "RequestId" : "D7861F61-5B61-46CE-A47C-6B19160D5EB0",
  "WafAiStatus" : 1
}
```

错误码

访问错误中心查看更多错误码。

6.11. SetDomainRuleGroup

调用SetDomainRuleGroup为域名设置规则防护引擎的防护规则组及智能规则托管功能的启用状态。

使用说明

本接口用于为指定域名设置规则防护引擎的防护规则组及智能规则托管功能的启用状态。

设置防护规则组时，除了可以使用WAF内置的正常、严格和宽松防护规则组，您还可以选择自定义规则组。

> **注意** 目前暂不支持通过API创建自定义规则组。您必须先在Web应用防火墙控制台的**系统管理** > **防护规则组**页面，新建规则组并获得对应规则组ID后，才可以调用本接口，为域名应用自定义规则组。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	SetDomainRuleGroup	要执行的操作。取值：**SetDomainRuleGroup**。
Domains	String	是	["www.aliyundoc.com"]	要设置防护规则组的域名列表。使用数组转化的字符串格式表示。 支持同时设置多个域名，格式：`["<域名1>","<域名2>",……]`。 **说明** 您可以调用DescribeDomainList查询所有已接入WAF防护的域名。
RuleGroupId	Long	是	1012	为规则防护引擎设置要应用的防护规则组ID。取值： • **1011**：表示WAF内置的严格规则组。 • **1012**：表示WAF内置的中等规则组。 • **1013**：表示WAF内置的宽松规则组。 除了以上内置规则组外，您还可以设置自定义规则组的ID。 **说明** 您可以在Web应用防火墙控制台的**防护规则组**页面，获取自定义规则组的ID。
WafVersion	Long	否	1	为当前配置设置一个版本号（用于实现乐观锁控制）。
InstanceId	String	是	waf-cn-tl32ast****	WAF实例ID。 **说明** 您可以通过调用DescribeInstanceInfo接口查看当前WAF实例ID。
ResourceGroupId	String	否	rg-acfm2pz25js****	网站域名在资源管理服务中所属的资源组ID。 不设置该参数表示默认资源组。

名称	类型	是否必选	示例值	描述
WafAiStatus	Integer	否	1	设置智能规则托管功能的启用状态。取值： • 0：表示关闭。 • 1（默认）：表示开启。 智能规则托管表示由WAF智能学习历史业务流量的行为模式，识别可能对正常业务产生误拦截的防护规则，并通过自动设置Web入侵防护白名单，在特定业务防护场景下屏蔽对应防护规则。等误报风险消除后，再恢复使用被屏蔽的防护规则。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=SetDomainRuleGroup
&Domains=["www.aliyundoc.com"]
&RuleGroupId=1012
&InstanceId=waf-cn-tl32ast****
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<SetDomainRuleGroupResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</SetDomainRuleGroupResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

6.12. ModifyProtectionRuleCacheStatus

调用ModifyProtectionRuleCacheStatus接口更新指定网站防篡改规则所防护的页面的缓存。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyProtectionRuleCacheStatus	要执行的操作。取值：**ModifyProtectionRuleCacheStatus**。
Domain	String	是	www.example.com	已添加的域名名称。
RuleId	Long	是	42755	配置规则ID。 **说明** 调用DescribeProtectionModuleRules接口可以查询到所有规则ID。
DefenseType	String	是	tamperproof	防护功能模块。固定取值：**tamperproof**。
InstanceId	String	是	waf_elasticity-cn-0xldbqt****	WAF实例ID。 **说明** 您可以通过调用DescribeInstanceInfo接口查看当前WAF实例ID。

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	请求ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyProtectionRuleCacheStatus
&DefenseType=tamperproof
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqt****
&RuleId=42755
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<?xml version="1.0" encoding="UTF-8" ?>
<ModifyProtectionRuleCacheStatusResponse>
 <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</ModifyProtectionRuleCacheStatusResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

6.13. DeleteProtectionModuleRule

调用DeleteProtectionModuleRule删除指定防护模块中配置的规则。

使用说明

本接口用于删除指定防护模块中配置的规则。

QPS限制

本接口的单用户QPS限制为10次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteProtectionModuleRule	要执行的操作。取值：**DeleteProtectionModuleRule**。
Domain	String	是	www.aliyundoc.com	要删除防护规则的域名。 **说明** 您可以调用DescribeDomainList查询所有已接入WAF防护的域名。
DefenseType	String	是	ac_custom	要删除的防护规则所属防护功能模块。取值： • **waf-codec**：表示规则防护引擎解码设置。 • **tamperproof**：表示网站防篡改规则配置。 • **dlp**：表示防敏感信息泄漏规则配置。 • **ng_account**：表示账户安全规则配置。 • **antifraud**：表示数据风控防护请求配置。 • **antifraud_js**：表示数据风控JS插入页面配置。 • **bot_algorithm**：表示Bot管理的智能算法规则。 • **bot_wxbb_pkg**：表示App防护的版本防护规则。 • **bot_wxbb**：表示App防护的路径防护规则。 • **ac_custom**：表示自定义防护策略规则配置。 • **whitelist**：表示白名单规则配置。

名称	类型	是否必选	示例值	描述
RuleId	Long	是	42754	要删除的防护规则的ID。 **说明** 您可以调用DescribeProtectionModuleRules查询指定防护功能模块下的所有规则ID。
InstanceId	String	是	waf-cn-mp9153****	WAF实例的ID。 **说明** 您可以调用DescribeInstanceInfo查询当前WAF实例的ID。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	1557B42F-B889-460A-B17F-1DE5C5AD7FF2	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteProtectionModuleRule
&Domain=www.aliyundoc.com
&DefenseType=ac_custom
&RuleId=42754
&InstanceId=waf-cn-mp9153****
&公共请求参数
```

正常返回示例

`XML` 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DeleteProtectionModuleRuleResponse>
    <RequestId>1557B42F-B889-460A-B17F-1DE5C5AD7FF2</RequestId>
</DeleteProtectionModuleRuleResponse>
```

`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "1557B42F-B889-460A-B17F-1DE5C5AD7FF2"
}
```

错误码

访问错误中心查看更多错误码。

6.14. DescribeProtectionModuleCodeConfig

调用DescribeProtectionModuleCodeConfig查询WAF地域级IP黑名单中支持配置的地域代码。

使用说明

本接口用于查询WAF地域级IP黑名单中支持配置的地域代码。【待补充：调用哪个接口设置IP黑名单】

QPS限制

本接口的单用户QPS限制为100次/秒。超过限制，API调用将会被限流，这可能影响您的业务，请合理调用。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeProtectionModuleCodeConfig	要执行的操作。取值：**DescribeProtectionModuleCodeConfig**。
CodeType	Integer	是	14	要查询的代码类型。取值固定为**14**，表示查询适用于WAF地域级IP黑名单配置的地域代码。
CodeValue	Integer	否	0	要查询的地域代码的类型。取值： • **0**：表示查询中国境内地域的代码。 • **1**：表示查询中国境外地域的代码。 不设置该参数表示查询所有类型。

名称	类型	是否必选	示例值	描述
InstanceId	String	是	waf-cn-tl32ast****	WAF实例的ID。 说明 您可以调用DescribeInstanceInfo查询当前WAF实例的ID。
ResourceGroupId	String	否	rg-acfm2pz25js****	网站域名在资源管理服务中所属的资源组ID。不设置该参数表示默认资源组。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
CodeConfigs	String	[{"code":0,"name":"310000,530000,150000,110000,TW_01,220000,510000,120000,640000,340000,370000,140000,440000,450000,650000,320000,360000,130000,410000,330000,460000,420000,430000,MO_01,620000,350000,540000,520000,210000,500000,610000,630000,HK_01,230000","env":"online"}]	地域代码的具体配置。使用JSON数组转化的字符串表示。JSON数组中的每个元素表示一种类型的地域代码，包含以下字段： • **code**：Integer类型 | 表示地域代码的类型。取值：**0**（表示中国境内地域代码）| **1**（表示中国境外地域代码）。 • **name**：String类型 | 表示该类型包含的所有地域代码。不同地域代码间使用半角逗号（,）分隔。关于地域代码的具体含义，请参见**返回数据**表格下方的说明。 • **env**：String类型 | 表示地域代码是否可用。取值：**online**（表示地域代码可用）| **offline**（表示地域代码不可用）。
RequestId	String	BE3911B8-9D96-5B39-8875-503BBC9DA4BF	本次请求的ID。

中国境内地域代码（`"code": 0`）含义说明

```
{
  "310000": "上海市",
  "610000": "陕西省",
  "360000": "江西省",
  "230000": "黑龙江省",
  "530000": "云南省",
  "140000": "山西省",
  "440000": "广东省",
  "320000": "江苏省",
  "110000": "北京市",
  "MO_01": "中国澳门",
  "620000": "甘肃省",
  "370000": "山东省",
  "150000": "内蒙古自治区",
  "450000": "广西壮族自治区",
  "410000": "河南省",
  "500000": "重庆市",
  "120000": "天津市",
  "630000": "青海省",
  "460000": "海南省",
  "640000": "宁夏回族自治区",
  "330000": "浙江省",
  "HK_01": "中国香港",
  "420000": "湖北省",
  "430000": "湖南省",
  "130000": "河北省",
  "510000": "四川省",
  "350000": "福建省",
  "210000": "辽宁省",
  "220000": "吉林省",
  "340000": "安徽省",
  "520000": "贵州省",
  "TW_01": "中国台湾"
}
```


中国境外地域代码（`"code": 1`）含义说明


```
{
  "KE": "肯尼亚",
  "KG": "吉尔吉斯斯坦",
  "KH": "柬埔寨",
  "KI": "基里巴斯",
  "KM": "科摩罗",
  "KN": "圣基茨和尼维斯联邦",
  "KP": "朝鲜",
  "KR": "韩国",
  "KW": "科威特",
  "KY": "开曼群岛",
  "KZ": "哈萨克斯坦",
  "LA": "老挝",
  "LB": "黎巴嫩",
  "LC": "圣卢西亚",
  "LI": "列支敦士登",
  "LK": "斯里兰卡",
```

```
"LR": "利比里亚",
"LS": "莱索托",
"LT": "立陶宛",
"LU": "卢森堡",
"LV": "拉脱维亚",
"LY": "利比亚",
"MA": "摩洛哥",
"MC": "摩纳哥",
"MD": "摩尔多瓦",
"ME": "黑山共和国",
"MF": "圣马丁",
"MG": "马达加斯加",
"MH": "马绍尔群岛",
"MK": "马其顿",
"ML": "马里",
"MM": "缅甸",
"MN": "蒙古",
"MP": "北马里亚纳群岛",
"MQ": "马提尼克岛",
"MR": "毛里塔尼亚",
"MS": "蒙塞拉特岛",
"MT": "马耳他",
"MU": "毛里求斯",
"MV": "马尔代夫",
"MW": "马拉维",
"MX": "墨西哥",
"MY": "马来西亚",
"MZ": "莫桑比克",
"NA": "纳米比亚",
"NC": "新喀里多尼亚",
"NE": "尼日尔",
"NF": "诺福克岛",
"NG": "尼日利亚",
"NI": "尼加拉瓜",
"NL": "荷兰",
"NO": "挪威",
"O1": "其它国家",
"NP": "尼泊尔",
"NR": "瑙鲁",
"NU": "纽埃岛",
"NZ": "新西兰",
"GA": "加蓬",
"GB": "英国",
"WS": "萨摩亚群岛",
"GD": "格林纳达",
"GE": "格鲁吉亚",
"GF": "法属圭亚那",
"GG": "根西岛",
"GH": "加纳",
"GI": "直布罗陀",
"GL": "格陵兰岛",
"GM": "冈比亚共和国",
"GN": "几内亚",
"GP": "瓜德罗普",
```

```
    "GQ": "赤道几内亚",
    "GR": "希腊",
    "GS": "南乔治亚岛和南桑威奇群岛",
    "GT": "危地马拉",
    "GU": "关岛",
    "GW": "几内亚比绍共和国",
    "GY": "圭亚那",
    "HM": "赫德岛和麦克唐纳群岛",
    "HN": "洪都拉斯",
    "HR": "克罗地亚",
    "HT": "海地",
    "YE": "也门",
    "HU": "匈牙利",
    "YT": "马约特岛",
    "ID": "印度尼西亚",
    "IE": "爱尔兰",
    "IL": "以色列",
    "IM": "马恩岛",
    "IN": "印度",
    "IO": "英属印度洋领地",
    "ZA": "南非",
    "IQ": "伊拉克共和国",
    "IR": "伊朗",
    "IS": "冰岛",
    "IT": "意大利",
    "ZM": "赞比亚",
    "JE": "泽西岛",
    "ZW": "津巴布韦",
    "JM": "牙买加",
    "JO": "约旦",
    "JP": "日本",
    "SI": "斯洛文尼亚",
    "SJ": "斯瓦尔巴和扬马延岛",
    "BY": "白俄罗斯",
    "SK": "斯洛伐克",
    "BZ": "伯利兹",
    "SL": "塞拉利昂",
    "SM": "圣马力诺",
    "SN": "塞内加尔",
    "SO": "索马里",
    "CA": "加拿大",
    "SR": "苏里南",
    "SS": "南苏丹",
    "CC": "科科斯（基林）群岛",
    "ST": "圣多美和普林西比",
    "CD": "刚果民主共和国",
    "CF": "中非共和国",
    "SV": "萨尔瓦多",
    "CG": "刚果",
    "CH": "瑞士",
    "SX": "荷属圣马丁",
    "SY": "阿拉伯叙利亚共和国",
    "CI": "科特迪瓦",
    "SZ": "斯威士兰",
```

```
"CK": "库克群岛",
"CL": "智利",
"CM": "喀麦隆",
"CN": "中华人民共和国",
"CO": "哥伦比亚",
"TC": "特克斯和凯科斯岛",
"CR": "哥斯达黎加",
"TD": "乍得",
"CU": "古巴",
"TF": "法属南部领地",
"CV": "佛得角",
"TG": "多哥",
"CW": "库拉索",
"TH": "泰国",
"CX": "澳大利亚圣诞岛",
"TJ": "塔吉克斯坦",
"CY": "塞浦路斯",
"CZ": "捷克共和国",
"TK": "托克劳群岛",
"TL": "东帝汶",
"TM": "土库曼斯坦",
"TN": "突尼斯",
"TO": "汤加",
"TR": "土耳其",
"TT": "特立尼达和多巴哥",
"DE": "德国",
"TV": "图瓦卢",
"DJ": "吉布提",
"TZ": "坦桑尼亚",
"DK": "丹麦",
"DM": "多米尼克国",
"DO": "多米尼加共和国",
"UA": "乌克兰",
"UG": "乌干达",
"DZ": "阿尔及利亚",
"UM": "美国本土外小岛屿",
"US": "美国",
"EC": "厄瓜多尔",
"EE": "爱沙尼亚",
"EG": "埃及",
"EH": "西撒哈拉",
"UY": "乌拉圭",
"UZ": "乌兹别克斯坦",
"VA": "梵蒂冈",
"VC": "圣文森特和格林纳丁斯",
"ER": "厄立特里亚",
"ES": "西班牙",
"VE": "委内瑞拉",
"ET": "埃塞俄比亚",
"EU": "欧洲",
"VG": "英属维尔京群岛",
"VI": "美属维尔京群岛",
"VN": "越南",
"VU": "瓦努阿图",
"FI": "芬兰"
```

```
  "FI": "芬兰",
  "FJ": "斐济",
  "FK": "马尔维纳斯群岛",
  "FM": "密克罗尼西亚联邦",
  "FO": "法罗群岛",
  "FR": "法国",
  "WF": "瓦利斯群岛和富图纳群岛",
  "OM": "阿曼",
  "PA": "巴拿马",
  "PE": "秘鲁",
  "PF": "法属波利尼西亚",
  "PG": "巴布亚新几内亚",
  "PH": "菲律宾",
  "PK": "巴基斯坦",
  "PL": "波兰",
  "PM": "圣皮埃尔和密克隆岛",
  "PN": "皮特凯恩群岛",
  "PR": "波多黎各",
  "PS": "巴勒斯坦",
  "PT": "葡萄牙",
  "PW": "帕劳",
  "PY": "巴拉圭",
  "QA": "卡塔尔",
  "A1": "匿名代理",
  "A2": "卫星传输",
  "AD": "安道尔",
  "AE": "阿拉伯联合酋长国",
  "AF": "阿富汗",
  "AG": "安提瓜和巴布达",
  "AI": "安圭拉",
  "AL": "阿尔巴尼亚",
  "AM": "亚美尼亚",
  "AO": "安哥拉",
  "AP": "亚太地区",
  "AQ": "南极洲",
  "AR": "阿根廷",
  "AS": "美属萨摩亚",
  "RE": "留尼旺岛",
  "AT": "奥地利",
  "AU": "澳大利亚",
  "AW": "阿鲁巴",
  "AX": "奥兰群岛",
  "AZ": "阿塞拜疆",
  "RO": "罗马尼亚",
  "BA": "波黑",
  "BB": "巴巴多斯",
  "RS": "塞尔维亚",
  "BD": "孟加拉共和国",
  "BE": "比利时",
  "RU": "俄罗斯",
  "BF": "布基纳法索",
  "RW": "卢旺达",
  "BG": "保加利亚",
  "BH": "巴林",
  "BI": "布隆迪共和国",
```

```
  "BJ": "贝宁",
  "BL": "圣巴泰勒米岛",
  "BM": "百慕大群岛",
  "BN": "文莱达鲁萨兰国",
  "BO": "玻利维亚",
  "SA": "沙特阿拉伯",
  "BQ": "博内尔、圣尤斯蒂休斯和萨巴",
  "SB": "所罗门群岛",
  "BR": "巴西",
  "SC": "塞舌尔",
  "SD": "苏丹",
  "BS": "巴哈马群岛",
  "SE": "瑞典",
  "BT": "不丹",
  "BV": "布韦岛",
  "SG": "新加坡",
  "SH": "圣赫勒拿岛",
  "BW": "博茨瓦纳"
}
```


示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeProtectionModuleCodeConfig
&CodeType=14
&CodeValue=0
&InstanceId=waf-cn-tl32ast****
&公共请求参数
```

正常返回示例

`XML` 格式


```
HTTP/1.1 200 OK
Content-Type:application/xml
<?xml version="1.0" encoding="UTF-8" ?>
<DescribeProtectionModuleCodeConfigResponse>
 <RequestId>BE3911B8-9D96-5B39-8875-503BBC9DA4BF</RequestId>
 <CodeConfigs>
  <code>0</code>
  <name>310000,530000,150000,110000,TW_01,220000,510000,120000,640000,340000,370000,140000,
440000,450000,650000,320000,360000,130000,410000,330000,460000,420000,430000,MO_01,620000,3
50000,540000,520000,210000,500000,610000,630000,HK_01,230000</name>
  <env>online</env>
 </CodeConfigs>
</DescribeProtectionModuleCodeConfigResponse>
```


`JSON` 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "BE3911B8-9D96-5B39-8875-503BBC9DA4BF",
  "CodeConfigs" : [ {
    "code" : 0,
    "name" : "310000,530000,150000,110000,TW_01,220000,510000,120000,640000,340000,370000,1
40000,440000,450000,650000,320000,360000,130000,410000,330000,460000,420000,430000,MO_01,62
0000,350000,540000,520000,210000,500000,610000,630000,HK_01,230000",
    "env" : "online"
  } ]
}
```

错误码

访问错误中心查看更多错误码。

7.日志管理

7.1. ModifyLogRetrievalStatus

调用ModifyLogRetrievalStatus为指定域名开启或关闭日志检索功能。

> **说明** 日志检索功能已经升级为WAF日志服务功能，更多信息，请参见WAF日志服务。该接口仅适用于保有日志检索功能的存量用户。如果您需要为域名开启或关闭WAF日志服务，请调用ModifyLogServiceStatus。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyLogRetrievalStatus	要执行的操作。取值：**ModifyLogRetrievalStatus**。
Domain	String	是	www.example.com	已添加的域名名称。 > **说明** 您可以调用DescribeDomainNames查询所有已经添加的域名。
Enabled	Integer	是	1	是否开启日志检索功能，取值： • **0**：表示关闭。 • **1**：表示开启。 > **说明** 只有为域名开启日志检索功能后，WAF才会记录该域名的访问请求日志。如果您关闭日志检索功能，则处于关闭状态期间的访问请求日志不会被记录；即使重新开启日志检索功能，您也无法查询到停用期间的访问请求日志。

名称	类型	是否必选	示例值	描述
InstanceId	String	是	waf_elasticity-cn-0xldbqt****	要操作的WAF实例ID。 说明 您可以调用DescribeInstanceInfo查询WAF实例的ID。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyLogRetrievalStatus
&Domain=www.example.com
&Enabled=1
&InstanceId=waf_elasticity-cn-0xldbqt****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<ModifyLogRetrievalStatusResponse>
   <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</ModifyLogRetrievalStatusResponse>
```

`JSON` 格式

```
{
    "RequestId": "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

7.2. ModifyLogServiceStatus

调用ModifyLogServiceStatus接口开启或关闭指定域名配置的日志采集功能。

为域名配置开启日志采集功能前请确认WAF实例已开通日志实时查询分析功能并且授权WAF将记录的日志分发到您专属的日志服务Logstore中。

更多详细信息，请参见日志实时查询分析。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyLogServiceStatus	要执行的操作。取值：**ModifyLogServiceStatus**。
Domain	String	是	www.example.com	已添加的域名名称。
Enabled	Integer	是	1	是否开启日志采集功能，取值： • **0**：关闭 • **1**：开启
InstanceId	String	是	waf_elasticity-cn-0xldbqt****	WAF实例ID。 您可以通过调用DescribeInstanceInfo接口查看当前WAF实例ID。

返回数据

名称	类型	示例值	描述
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	请求ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyLogServiceStatus
&Domain=www.example.com
&Enabled=1
&InstanceId=waf_elasticity-cn-0xldbqt****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<ModifyLogServiceStatusResponse>
   <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</ModifyLogServiceStatusResponse>
```

`JSON` 格式

```
{
    "RequestId": "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

错误码

访问错误中心查看更多错误码。

7.3. DescribeLogServiceStatus

调用DescribeLogServiceStatus查询已接入WAF进行防护的域名的日志采集状态（是否开启日志采集）。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeLogServiceStatus	要执行的操作。取值：**DescribeLogServiceStatus**。
InstanceId	String	是	waf-cn-zz11sr5****	WAF实例的ID。 **说明** 您可以调用DescribeInstanceInfo查询当前WAF实例的ID。
Region	String	否	cn	WAF实例的地域ID。默认为**cn**，表示中国内地；如果WAF实例的地域是海外地区，请填写**cn-hongkong**。 **说明** 您可以调用DescribeInstanceInfo查询当前WAF实例的地域ID。

名称	类型	是否必选	示例值	描述
ResourceGroupId	String	否	rg-acfm2pz25js****	WAF实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。 关于资源组的更多信息，请参见创建资源组。
PageNumber	Integer	否	1	列表的页码。默认值为**1**。
PageSize	Integer	否	10	分页查询时每页的行数。默认值为**10**。
DomainNames.N	RepeatList	否	www.aliyun.com	要查询的域名列表。一次最多允许查询10个域名。不填写该参数表示查询所有域名。 **说明** 您可以调用DescribeDomainNames查询所有已经接入当前WAF实例进行防护的域名。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
DomainStatus	Array of status		域名的日志采集状态（是否开启了日志采集）。
Domain	String	www.aliyun.com	域名名称。
SlsLogActive	Integer	1	该域名是否开启了日志采集。取值： • **1**：表示已开启。 • **0**：表示未开启。
RequestId	String	C2E97B3F-1623-4CDF-A7E2-FD9D4CF1027A	本次请求的ID。
TotalCount	Integer	1	返回结果的总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeLogServiceStatus
&InstanceId=waf-cn-zz11sr5****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeLogServiceStatusResponse>
   <RequestId>C2E97B3F-1623-4CDF-A7E2-FD9D4CF1027A</RequestId>
   <TotalCount>1</TotalCount>
   <DomainStatus>
      <Domain>www.aliyun.com</Domain>
      <SlsLogActive>1</SlsLogActive>
   </DomainStatus>
</DescribeLogServiceStatusResponse>
```

`JSON` 格式

```
{
    "RequestId": "C2E97B3F-1623-4CDF-A7E2-FD9D4CF1027A",
    "TotalCount": 1,
    "DomainStatus": [
        {
            "Domain": "www.aliyun.com",
            "SlsLogActive": 1
        }
    ]
}
```

错误码

访问错误中心查看更多错误码。

8.系统管理

8.1. DescribeWafSourceIpSegment

调用DescribeWafSourceIpSegment查询WAF防护集群使用的回源IP网段。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeWafSourceIpSegment	要执行的操作。取值：**DescribeWafSourceIpSegment**。
InstanceId	String	是	waf-cn-zz11sr5****	要查询的WAF实例的ID。 **说明** 您可以调用DescribeInstanceInfo查询当前WAF实例的ID。
ResourceGroupId	String	否	rg-acfm2pz25js****	WAF实例在资源管理服务中所属的资源组ID。默认为空，即属于默认资源组。 关于资源组的更多信息，请参见创建资源组。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
IpV6s	String	39.XXX.XXX.0/24,.....,2408:400a:XXXX:XXXX::/56	IPv6防护集群使用的WAF回源IP网段列表。
Ips	String	47.XXX.XXX.192/26,.....,47.XXX.XXX.0/24	IPv4防护集群使用的WAF回源IP网段列表。

名称	类型	示例值	描述
RequestId	String	AB2F5E31-EE96-4FD7-9560-45FF5D5377FF	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeWafSourceIpSegment
&InstanceId=waf-cn-zz11sr5****
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeWafSourceIpSegmentResponse>
   <RequestId>AB2F5E31-EE96-4FD7-9560-45FF5D5377FF</RequestId>
   <IpV6s>39.XXX.XXX.0/24,……,2408:400a:XXXX:XXXX::/56</IpV6s>
   <Ips>47.XXX.XXX.192/26,……,47.XXX.XXX.0/24</Ips>
</DescribeWafSourceIpSegmentResponse>
```

`JSON` 格式

```
{
 "RequestId": "AB2F5E31-EE96-4FD7-9560-45FF5D5377FF",
 "IpV6s": "39.XXX.XXX.0/24,……,2408:400a:XXXX:XXXX::/56",
 "Ips": "47.XXX.XXX.192/26,……,47.XXX.XXX.0/24"
}
```

错误码

访问错误中心查看更多错误码。

9.资源相关接口

9.1. MoveResourceGroup

调用MoveResourceGroup，将一个WAF资源转移到其他资源组。

使用说明

WAF资源表示已接入WAF防护的域名。资源组（Resource Group）是在阿里云账号下进行资源分组管理的一种机制。资源组帮助您解决单个云账号内多项目或多应用的资源分组，以及用户授权管理的复杂性问题。接入WAF防护的域名资源默认属于默认资源组。您可以将WAF的域名资源转移到您自定义的资源组中，实现资源分组管理。

您可以通过阿里云控制台创建资源组，相关操作，请参见创建资源组；或者通过调用资源管理服务的API创建资源组，具体接口说明，请参见CreateResourceGroup。

关于资源组的更多介绍，请参见什么是资源管理。

QPS限制

本接口无单用户QPS限制，请您根据实际需要合理调用。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	MoveResourceGroup	要执行的操作。取值：**MoveResourceGroup**。
RegionId	String	是	cn-hangzhou	WAF实例所属地域。取值： • **cn-hangzhou**：表示中国内地。 • **ap-southeast-1**：表示海外地区。
ResourceType	String	是	domain	WAF资源的类型。唯一取值：**domain**，表示WAF的资源类型仅为域名。

名称	类型	是否必选	示例值	描述
ResourceId	String	是	waf-cn-09k1rd5****~www.example.com	要操作的WAF资源的ID。 您将网站域名接入WAF防护后，则该域名表示一个WAF资源。WAF资源在资源管理服务中使用资源ID（ResourceId）作为其唯一标识，WAF资源ID的命名方式为：`<InstanceId>~<Domain>`。具体说明如下： • `<InstanceId>` 表示当前WAF实例的ID。您可以调用WAF API中的DescribeInstanceInfo接口，查询当前WAF实例的ID。 • `<Domain>` 表示已接入WAF实例防护的网站域名。您可以调用WAF API中的DescribeDomainList接口，查询所有已接入WAF实例防护的域名。 • `<InstanceId>` 和 `<Domain>` 之间使用 `~` 连接，即表示WAF域名资源的资源ID。
ResourceGroupId	String	是	rg-atstuj3rtop****	WAF资源要转入的资源组的ID。 您通过资源管理服务创建资源组后，资源管理服务会为资源组生成一个唯一标识，即资源组ID（ResourceGroupId）。 您可以在资源管理控制台的**资源组**页面，查询所有资源组ID；或者调用资源管理服务提供的ListResourceGroups接口，查询所有资源组ID。

调用API时，除了本文中该API的请求参数，还需加入阿里云API公共请求参数。公共请求参数的详细介绍，请参见公共参数。

调用API的请求格式，请参见本文**示例**中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次调用请求的ID，是由阿里云为该请求生成的唯一标识符，可用于排查和定位问题。

示例

请求示例

```
http(s)://[Endpoint]/?Action=MoveResourceGroup
&RegionId=cn-hangzhou
&ResourceType=domain
&ResourceId=waf-cn-09k1rd5****~www.example.com
&ResourceGroupId=rg-atstuj3rtop****
&<公共请求参数>
```

正常返回示例

`XML` 格式

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

`JSON` 格式

```
{
    "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

错误码

访问错误中心查看更多错误码。

10.错误码

您可以在错误代码表中查看所有的错误码，排查问题。

Error Code	Error Message	描述
RequestError	The system is unavailable. Please try again later.	您的请求错误，请重试。
ComboError	No package information is available.	无套餐信息。例如，UID、WAF实例ID信息设置错误。
DomainCountError	The number of domain names exceeds the limit. You can upgrade the domain package.	域名数限制。
HttpsSupportError	HTTPS is not supported.	不支持HTTPS。
OuterCloudSupportError	Servers outside Alibaba is not supported.	不支持云外主机。
DomainSourceIpCountError	The number of origin fetch addresses exceeds the limit.	回源IP个数限制。
DomainNotRegisterError	The specified domain name is not ICP filed.	域名未备案。
ExtensiveDomainSupportError	Wildcard domains is not supported.	不支持泛域名。
DomainHasAdded	The domain has been configured.	域名已经添加。
SourceIpNotYoursError	You are not the owner of this origin fetch address.	服务器IP不属于您。
HttpsCertFormatError	The certificate file is malformed.	HTTPS证书格式错误。
HttpsPrivateKeyFormatError	The private key of the certificate is malformed.	HTTPS密钥格式错误。
ErrorInSourceIps	The origin fetch address includes disallowed IP addresses or domains.	源站服务器地址中包含不能添加的IP、域名，请确认后再添加。
DomainNotExist	The specified domain does not exist.	域名不存在。
IsNonStandardPort	Non-standard ports are not supported.	不支持非标准端口。
InvalidDomainError	The domain is invalid.	无效域名。

Error Code	Error Message	描述
InvalidMainDomainError	The number of primary domains exceeds the limit. You can upgrade the domain package.	主域名个数限制。
NotSupportMainDomainError	The primary domain is not supported.	不支持该顶级域。
CertAndKeyNotMatch	The certificate file and private key do not match.	证书和密钥不匹配。
SourceIpSupportsVirtualIpError	This is an instance dedicated for shared virtual host. Only an IP of a virtual host can be added.	当前为共享虚拟主机定制版，只能添加万网虚拟主机的IP。
DomainAutoAccessError	The auto access of domain is being configured.	域名自动接入配置中。
DomainHttpPortError	An invalid HTTP port is specified.	HTTP端口不支持。
DomainHttpsPortError	An invalid HTTPS port is specified.	HTTPS端口不支持。
PortCountError	The number of ports exceeds the limit.	端口数量超出限制。
DomainBlackError	The domain has been listed in the blacklist.	域名已被加入黑名单。
AclRuleCountError	The number of access control rules exceeds the limit.	自定义防护策略（ACL访问控制）数量超出限制。
AclRuleSeniorError	You don't have permission to use senior access control rule.	不支持使用高级自定义防护策略（ACL访问控制）。
AclRuleDuplicateError	The access control rule name is invalid or a rule with the same name already exists.	自定义防护策略（ACL访问控制）名称错误。
AclRuleNotFound	The specified access control rule does not exist.	没有找到指定的自定义防护策略（ACL访问控制）。
ExtensiveDomainHasBeenUsedByOthers	Another user has used this wildcard domain in WAF.	泛域名已被其他阿里云用户使用。
AuthorizeCertFailed	There are some errors when the system checks your certificate.	验证证书失败。
CertServiceError	There are some errors in the certificate service.	证书服务错误。
CertNameExisted	The certificate name already exists.	证书名称已经存在。

Error Code	Error Message	描述
CertKeysIsEmpty	The private key of the certificate is required.	证书密钥为空。
CertKeyFormatError	The private key of the certificate is malformed.	证书密钥格式错误。
SaveCertFailed	There are some errors when the system save your certificate.	保存证书失败。
CertHasExisted	This certificate has already been uploaded. Do not upload it again.	证书已经存在。
CertHasExpired	The certificate has expired. Do not continue using this certificate.	证书已经到期。
CertKeyServerError	The certificate service is unavailable,Please try again later.	证书服务不可用。
ParamError	The parameters of your request are invalid.	参数错误。
CertIsNotMatchDomain	The certificate does not include this domain.	证书与域名不匹配。
CertNotExist	The certificate is not exist.	证书不存在。
CertHasDelInCA	The certificate is deleted in CA service.	证书在CA端已被删除。
NotOperateOtherCallerConfig	You are not authorized to perform other channel config.	不能操作其他渠道的配置。
DomainNotCloseInAntibot	The domain is still used in Anti-Bot service.	爬虫风险管理的防护功能未关闭。
AntibotServerError	Anti-bot service is unavailable.	爬虫风险管理不可用。
TaskNotFound	The specified task does not exist.	任务未找到。
TaskIsRejected	The task has been rejected.	任务被拒绝。
TaskStillRunning	The task is running.	任务仍在执行。
TaskTimeOut	The task is timeout.	任务超时。