ALIBABA CLOUD

Alibaba Cloud

Web应用防火墙

API Reference (2019-09-10)

Document Version: 20220520

Alibaba Cloud

Legal disclaimer

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

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

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

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

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

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

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

Document conventions

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

Table of Contents

1.List of operations by function

The following tables list API operations available for use in Web Application Firewall (WAF).

Instance management

Operation	Description
DescribeInstanceInfo	Queries the basic information about the WAF instance that you purchase. The information includes the ID, type, and status of the WAF instance.
DescribeInstanceSpecInfo	Queries the specification information about the WAF instance that you purchase.
DeleteInstance	Releases a subscription WAF instance that expires.

Domain name configurations

Operation	Description
DescribeDomainNames	Queries all the domain names that are added to WAF. **Note** This operation returns all the domain names at a time. We recommend that you call the DescribeDomainList operation, which returns domain names by page.
DescribeDomainList	Queries the domain names that are added to WAF by page. **Note** This operation allows you to specify different conditions for the query and returns query results by page. If you want to query a large number of domain names, we recommend that you call the operation.
DescribeDomain	Queries the configuration of a specific domain name that is added to WAF.
CreateDomain	Adds a domain name to WAF.
ModifyDomain	Modifies the configuration of a specific domain name.
DeleteDomain	Removes a domain name from WAF.
DescribeCertificates	Queries the certificates that are associated with a specific domain name. The certificates are managed by SSL Certificates Service.
DescribeCertMatchStatus	Checks whether the certificate and the private key that you upload for a specific domain name match each other.

Operation	Description
CreateCertificate	Uploads the certificate and private key for a domain name that is added to WAF.
CreateCertificateByCertificateId	Uploads the certificate for a specific domain name based on the certificate ID.
DescribeDomainBasicConfigs	Queries the protection status of a domain name that is added to WAF.
DescribeDomainAdvanceConfigs	Queries the configuration details of a domain name that is added to WAF.

Protection configurations

Operation	Description
ModifyDomainIpv6Status	Enables or disables IPv6 traffic protection for a domain name.
DescribeProtectionModuleStatus	Queries whether a specific WAF protection module is enabled. The WAF protection modules include web intrusion prevention, data security, advanced protection, bot management, and access control or throttling.
ModifyProtectionModuleStatus	Enables or disables a specific WAF protection module. The WAF protection modules include web intrusion prevention, data security, advanced protection, bot management, and access control or throttling.
DescribeProtectionModuleMode	Queries the protection mode of a specific WAF protection module. The WAF protection modules include the Protection Rules Engine, Big Data Deep Learning Engine, HTTP flood protection, data risk control, and proactive defense.
ModifyProtectionModuleMode	Modifies the protection mode of a specific WAF protection module. The WAF protection modules include the Protection Rules Engine, Big Data Deep Learning Engine, HTTP flood protection, data risk control, and proactive defense.
DescribeProtectionModuleRules	Queries the rules that are created for a specific WAF protection module. The WAF protection modules include web intrusion prevention, data security, bot management, access control or throttling, and website whitelist.
CreateProtectionModuleRule	Creates rules for a specific WAF protection module. The WAF protection modules include web intrusion prevention, data security, bot management, access control or throttling, and whitelist.
ModifyProtectionModuleRule	Modifies the rules that are created for a specific WAF protection module. The WAF protection modules include web intrusion prevention, data security, advanced protection, bot management, access control or throttling, and website whitelist.

Operation	Description
ModifyProtectionRuleStatus	Enables or disables the rules that are created for a specific WAF protection module. The WAF protection modules include website tamper-proofing, allowed crawlers, bot threat intelligence, custom protection policy, and website whitelist.
DescribeDomainRuleGroup	Queries the ID of the protection rule group that is provided by the Protection Rules Engine for a specific domain name.
SetDomainRuleGroup	Configures the protection rule group that is provided by the Protection Rules Engine for a specific domain name. The system provides three default protection rule groups. You can also select a custom protection rule group.
ModifyProtectionRuleCacheStatus	Updates the cached pages of a domain name that is protected by a specific website tamper-proofing rule.
DeleteProtectionModuleRule	Deletes the rule that is created for a specific WAF protection module
DescribeProtectionModuleCodeConfig	Queries the codes of regions that can be configured in the WAF region blacklist.

Log management

Operation	Description
ModifyLogServiceStatus	Enables or disables the log collection feature for a domain name.
ModifyLogRetrievalStatus	Enables or disables the log retrieval feature for a domain name.
DescribeLogServiceStatus	Queries whether the log collection feature is enabled for the domain names that are added to WAF.

System management

Operation	Description
DescribeWafSourceIpSegment	Queries the back-to-origin CIDR blocks that are used by the WAF protection cluster.

2.Request method

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

Request syntax

WAF API operations use the RPC protocol. You can call WAF API operations by sending HTTP GET requests.

The request syntax is as follows:

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

In the request:

- Endpoint: the endpoint of the WAF API varies with the region.
  - Mainland China: wafopenapi.cn-hangzhou.aliyuncs.com
  - Outside mainland China: wafopenapi.ap-southeast-1.aliyuncs.com
- Action: the operation that you want to perform. For example, to obtain a list of the domains added to WAF, you must set the Action parameter to DescribeDomainNames.
- Version: the version of the API to be used. The current WAF API version is *2019-09-10*.
- Parameters: the request parameters for the operation. Separate multiple parameters with ampersands (&).

  Request parameters include both common parameters and operation-specific parameters. Common parameters include the API version and authentication information. For more information, see Common parameters.

The following example demonstrates how to call the DescribeDomainNames operation to obtain a list of the domains added to WAF.

> **Note** To improve readability, the API request is displayed in the following format.

```
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 authorization

To ensure the security of your account, we recommend that you call the WAF API as a RAM user. To call the WAF API as a RAM user, you must create an account for the RAM user and grant the account required permissions.

Signature method

You must sign all API requests to ensure security. WAF uses the request signature to verify the identity of the API caller.

WAF implements symmetric encryption with an AccessKey pair to verify the identity of the request sender. An AccessKey pair is an identity credential issued to Alibaba Cloud accounts and RAM users that is similar to a logon username and password. An AccessKey pair consists of an AccessKey ID and an AccessKey secret. The AccessKey ID is used to verify the identity of the user, while the AccessKey secret is used to encrypt and verify the signature string. You must keep your AccessKey secret strictly confidential.

You must add the signature to the Cloud Firewall API request in the following format:

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

Take the DescribeDomainNames operation as an example. If the AccessKey ID is `testid` and the AccessKey secret is `testsecret`, the original request URL is as follows:

```
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
```

Perform the following operations to calculate the signature:

1. Use the request parameters to compose a string-to-sign.

   ```
   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. Calculate the HMAC value of the string-to-sign.

   Add an ampersand (&) to the end of the AccessKey secret, and use the result as the key to calculate the HMAC value. In this example, the key is `testsecret&`.

   ```
   CT9X0VtwR86fNWSnsc6v8YGOjuE=
   ```

3. Add the signature to the request parameters:

```
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.Common parameters

This topic describes the parameters that are common to all API requests and responses.

Common request parameters

Parameter	Type	Required	Description
Format	String	No	The response format. Valid values: • *JSON* (default) • *XML*
Version	String	Yes	The version number of the API. Specify the version number in the YYYY-MM-DD format. Set the value to *2019-09-10*.
AccessKeyId	String	Yes	The AccessKey ID provided to you by Alibaba Cloud.
Signature	String	Yes	The signature string of the current request.
SignatureMethod	String	Yes	The encryption method of the signature string. Set the value to *HMAC-SHA1*.
Timestamp	String	Yes	The timestamp of the request. Specify the time in the ISO 8601 standard in the YYYY-MM-DDThh:mm:ssZ format. The time must be in UTC. For example, use 2013-01-10T12:00:00Z to indicate January 10, 2013, 20:00:00 (UTC+8).
SignatureVersion	String	Yes	The version of the signature encryption algorithm. Set the value to *1.0*.
SignatureNonce	String	Yes	A unique, random number used to prevent replay attacks. You must use different numbers for different requests.
ResourceOwnerAccount	String	No	The Alibaba Cloud account to which the resource you want to access belongs.

Example

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&Region=cn
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Timestamp=2014-05-19T10%3A33%3A56Z
&Format=xml
&AccessKeyId=testid
&SignatureMethod=Hmac-SHA1
&SignatureNonce=NwDAxvLU6tFE0DVb
&Version=2019-09-10
&SignatureVersion=1.0
&Signature=Signature
```

Common response parameters

API responses use the HTTP response format where a 2xx status code indicates a successful call and a 4xx or 5xx status code indicates a failed call. Every response returns a unique RequestID regardless of whether the call is successful.

Responses can be returned in either the JSON or XML format. You can specify the response format in the request. The default response format is XML.

Sample success responses

- XML format

```
<?xml version="1.0" encoding="utf-8"?>
    <!--Result Root Node-->
    <Interface Name+Response>
        <!--Return Request Tag-->
        <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
        <!--Return Result Data-->
    </Interface Name+Response>
```

- JSON format

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

4.Instance information

4.1. DescribeInstanceInfo

Queries the information about the Web Application Firewall (WAF) instance within your Alibaba Cloud account.

Usage notes

You can call the DescribeInstanceInfo operation to query the information about the WAF instance within your Alibaba Cloud account. The information includes the ID, version, status, and expiration time of the instance.

Limits

You can call this operation up to 50 times per second per account. If the number of the calls per second exceeds the limit, throttling is triggered. As a result, your business may be affected. We recommend that you take note of the limit when you call this operation.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeInstanceInfo	The operation that you want to perform. Set the value to **DescribeInstanceInfo**.
InstanceId	String	No	waf-cn-tl32ast****	The ID of the WAF instance. If you do not specify this parameter, the information about all WAF instances is returned.
ResourceGroupId	String	No	rg-atstuj3rtop****	The ID of the resource group to which the WAF instance belongs in Resource Management. If you do not specify this parameter, the WAF instance belongs to the default resource group.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the **"Examples"** section of this topic.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
InstanceInfo	Object		The information about the WAF instance.
Status	Integer	1	Indicates whether the WAF instance expires. Valid values: • **0**: The instance expires. • **1**: The instance does not expire. **Note** If the value of **PayType** is **0**, this parameter is not returned. The value 0 indicates that no WAF instance is purchased.
EndDate	Long	1512921600	The expiration time of the WAF instance. This value is a UNIX timestamp. Unit: seconds. **Note** If the value of **PayType** is **0**, this parameter is not returned. The value 0 indicates that no WAF instance is purchased.

Parameter	Type	Example	Description
Version	String	version_3	The edition of the WAF instance. Valid values: • **version_pro_china**: a WAF Pro instance in the Chinese mainland • **version_business_china**: a WAF Business instance in the Chinese mainland • **version_enterprise_china**: a WAF Enterprise instance in the Chinese mainland • **version_exclusive_china**: a WAF instance that uses an exclusive cluster in the Chinese mainland • **version_hybrid_cloud_standard_china**: a Hybrid Cloud WAF instance in the Chinese mainland • **version_pro**: a WAF Pro instance outside the Chinese mainland • **version_business**: a WAF Business instance outside the Chinese mainland • **version_enterprise**: a WAF Enterprise instance outside the Chinese mainland • **version_exclusive**: a WAF instance that uses an exclusive cluster outside the Chinese mainland • **version_hybrid_cloud_standard**: a Hybrid Cloud WAF instance outside the Chinese mainland The preceding list contains all the editions of WAF instances within accounts that are created at the International site. If the returned version is not in the list, check whether your account is created at the International site. **Note** If the value of **PayType** is **0**, this parameter is not returned. The value 0 indicates that no WAF instance is purchased.

Parameter	Type	Example	Description
RemainDay	Integer	1	The number of remaining days before the trial period of the WAF instance ends. **Note** This parameter is returned only if the value of **Trial** is **1**. The value 1 indicates that the free trial of a WAF instance is activated.
Region	String	cn	The region in which the WAF instance resides. Valid values: • **cn**: the Chinese mainland • **cn-hongkong**: outside the Chinese mainland **Note** If the value of **PayType** is **0**, this parameter is not returned. The value 0 indicates that no WAF instance is purchased.
PayType	Integer	1	The activation status of WAF. Valid values: • **0**: No WAF instance is purchased within the Alibaba Cloud account. • **1**: A subscription WAF instance is purchased within the Alibaba Cloud account.
InDebt	Integer	1	Indicates whether the WAF instance has overdue payments. Valid values: • **0**: The instance has overdue payments. • **1**: The instance do not have overdue payments. **Note** If the value of **PayType** is **0**, this parameter is not returned. The value 0 indicates that no WAF instance is purchased.

Parameter	Type	Example	Description
InstanceId	String	waf-cn-tl32ast****	The ID of the WAF instance. **Note** If the value of **PayType** is **0**, this parameter is not returned. The value 0 indicates that no WAF instance is purchased.
SubscriptionType	String	Subscription	The billing method of the WAF instance: The value is fixed as **Subscription**. **Note** If the value of **PayType** is **0**, this parameter is not returned. The value 0 indicates that no WAF instance is purchased.
Trial	Integer	1	Indicates whether the free trial of a WAF instance is activated within the Alibaba Cloud account. Valid values: • **0**: no • **1**: yes **Note** This parameter is returned only if the free trial of a WAF instance is activated within the Alibaba Cloud account.

Examples

Sample requests

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

Sample success responses

`XML` format

```
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` format

```
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"
  }
}
```

Error codes

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

4.2. DescribeInstanceSpecInfo

Queries the specifications of a Web Application Firewall (WAF) instance.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeInstanceSpecInfo	The operation that you want to perform. Set the value to **DescribeInstanceSpecInfo**.
InstanceId	String	No	waf-cn-st2225l****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
ResourceGroupId	String	No	rg-atstuj3rtop****	The ID of the resource group to which the WAF instance belongs in Resource Management. This parameter is empty by default, which indicates that the WAF instance belongs to the default resource group. For more information about resource groups, see Create a resource group.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the **"Examples"** section of this topic.

Response parameters

Parameter	Type	Example	Description
RequestId	String	E906513E-F6B5-495E-98DC-7BA888671D76	The ID of the request.
InstanceId	String	waf-cn-st2225l****	The ID of the WAF instance.

Parameter	Type	Example	Description
Version	String	version_hybrid_cloud_standard	The edition of the WAF instance. Valid values: • **version_pro_china**: a Pro instance in mainland China • **version_business_china**: a Business instance in mainland China • **version_enterprise_china**: an Enterprise instance in mainland China • **version_exclusive_china**: an instance in an exclusive cluster and in mainland China • **version_hybrid_cloud_standard_china**: a Hybrid Cloud WAF instance in mainland China • **version_pro**: a Pro instance in regions outside mainland China • **version_business**: a Business instance in regions outside mainland China • **version_enterprise**: an Enterprise instance in regions outside mainland China • **version_exclusive**: an instance in an exclusive cluster and in regions outside mainland China • **version_hybrid_cloud_standard**: a Hybrid Cloud WAF instance in regions outside mainland China The preceding list contains all the editions of WAF instances for accounts created at the International site. If the returned version is not in the list, check whether your account is created at the International site.
InstanceSpecInfos	Array of InstanceSpecInfo		An array that consists of the specifications of the WAF instance. Each element in the array is a struct that contains the **Code** and **Value** fields. **Code** indicates the specification code, and **Value** indicates the specification value.
			The specification code of the WAF instance. Valid values: • **100**: indicates whether the WAF instance can protect HTTPS services. • **101**: indicates the maximum QPS. • **102**: indicates the request rate that triggers HTTP flood protection. • **103**: indicates the maximum number of

Parameter	Type	Example	Description
			domain names that the WAF instance can protect. • **104**: indicates whether wildcard domain names are supported. • **105**: indicates the maximum number of custom protection policies (ACL rules) that can be configured. • **106**: indicates the maximum number of back-to-origin IP addresses that can be configured. • **107**: indicates whether the WAF instance can protect external servers. • **108**: indicates whether the custom protection policy feature is supported. • **109**: indicates whether non-standard ports are supported. • **110**: indicates whether the scan protection feature is supported. • **111**: indicates whether the data risk control feature is supported. • **112**: indicates the maximum number of URLs that can be protected by data risk control. • **113**: indicates the maximum number of second-level domain names that can be added to the WAF instance. • **114**: indicates the maximum bandwidth of normal traffic that can pass through the WAF instance. • **115**: indicates the number of purchased extra domain packages. • **116**: indicates whether the IP addresses of ECS instances from different Alibaba Cloud accounts can be added as the IP addresses of origin servers. • **117**: indicates whether the IP address of a Cloud Web Hosting instance can be added as the IP address of the origin server. • **118**: indicates the maximum number of rules for data risk control that can be configured. • **119**: indicates whether the semantic analysis engine is supported. • **12**: indicates whether the traffic analysis feature is supported. • **120**: indicates whether the ICP filing of a domain name is obtained. • **121**: indicates whether custom protection policies can be configured to defend against HTTP flood attacks.

Parameter	Type	Example	Description
Code	String	113	• 122: indicates the maximum number of custom protection policies that can be configured to defend against HTTP flood attacks. • 123: indicates whether the region blacklist feature is supported. • 124: indicates whether the website tamper-proofing feature is supported. • 125: indicates the maximum number of custom website tamper-proofing rules that can be configured. • 126: indicates whether the log collection feature is supported. • 127: indicates the maximum number of non-standard ports that can be added to the WAF instance. • 128: indicates the HTTP ports that can be added to the WAF instance. • 129: indicates the HTTPS ports that can be added to the WAF instance. • 13: indicates whether the work mode of the HTTP flood protection feature can be changed. • 130: indicates whether the attacker profiling feature is supported. • 131: indicates whether the data leakage prevention feature is supported. • 132: indicates the maximum number of rules for data leakage prevention that can be configured. • 133: indicates the condition fields that are supported by the custom protection policy and whitelist features. • 134: indicates the number of purchased exclusive IP addresses. • 135: indicates whether the data visualization feature is supported. • 136: indicates the maximum number of data dashboards that are supported. • 137: indicates whether Big Data Deep Learning Engine is supported. • 138: indicates whether the log search feature is supported. • 139: indicates the maximum period during which logs can be stored. • 14: indicates whether the logs of HTTP flood attacks can be viewed. • 140: indicates the maximum capacity that can be used to store logs. • 141: indicates whether the alert settings

Parameter	Type	Example	Description
			feature is supported. • **142**: indicates the maximum number of times that the log storage can be cleared. • **143**: indicates whether custom rule groups are supported. • **144**: indicates the maximum number of custom rule groups that can be configured. • **145**: indicates whether the general gateway proxy developed by Alibaba Cloud is supported. • **146**: indicates whether the general rule proxy developed by Alibaba Cloud is supported. • **147**: indicates whether the security expert service is supported. • **148**: indicates whether the free trial of the WAF instance is available. • **149**: indicates whether the transparent proxy mode is supported. • **150**: indicates whether IPv6 addresses can be configured for origin servers. • **151**: indicates whether the positive security model is supported. • **152**: indicates the maximum number of rules that can be generated for the positive security model. • **153**: indicates whether the WAF instance can protect HTTP/2 services. • **154**: indicates whether the website configuration feature is supported. • **155**: indicates whether the asset discovery feature is supported. • **156**: indicates whether specifications are provided for the staging environment. • **157**: indicates whether exclusive clusters are supported. • **158**: indicates the maximum number of ports that are supported by an exclusive cluster. • **159**: indicates whether the account security feature is supported. • **160**: indicates the maximum number of APIs that can be protected by the account security feature. • **162**: indicates the maximum number of whitelist rules that can be created. • **163**: indicates the maximum number of custom protection policies that can be configured.

Parameter	Type	Example	Description
			• **164**: indicates the maximum number of IP address blacklist rules that can be configured. • **167**: indicates whether custom scan protection is supported. • **168**: indicates the maximum number of domain names that can be protected when Global Server Load Balancer (GSLB) is deployed. • **169**: indicates whether intelligent load balancing is supported. • **171**: indicates whether the app protection feature is supported. • **172**: indicates the maximum number of app protection rules that can be configured. • **173**: indicates whether the typical bot behavior identification feature is supported. • **176**: indicates whether the allowed crawlers feature is supported. • **177**: indicates whether the bot threat intelligence feature is supported. • **181**: indicates the maximum number of traffic redirection configuration items that are supported in transparent proxy mode. A configuration item consists of the IP address of a specific cloud service instance and ports. • **193**: indicates whether custom TLS security policies are supported. • **194**: indicates whether the advanced settings for custom TLS security policies are supported. • **196**: indicates whether the transparent proxy mode supports all ports. • **199**: indicates whether the WAF instance can forward requests over IPv6. • **200**: indicates whether scenario-specific configuration is supported. • **201**: indicates the maximum number of bot mitigation scenarios that are supported.
Value	String	300	The specification value of the WAF instance. Data type: Boolean. Valid values: **true** and **false**.

Parameter	Type	Example	Description
ExpireTime	Long	1677168000000	The UNIX timestamp when the WAF instance expires. Unit: milliseconds. **Note** If the WAF instance is billed on a pay-as-you-go basis, this parameter indicates the time when the trial period ends.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<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>80,81,82,83,84,88,800,808,3333,5000,5222,6001,6666,7000,7001,7002,7003,7004,7005,7006,7009,7010,7011,7012,7013,7014,7015,7016,7018,7019,7020,7021,7022,7023,7024,7025,7026,7070,7081,7082,7083,7088,7097,7777,8000,8001,8002,8003,8009,8020,8021,8022,8025,8026,8080,8081,8082,8083,8084,8085,8086,8087,8088,8089,8090,8091,8181,8800,8888,8889,8999,9000,9001,9002,9080,9200,9999,10000,10001,10080,12601,86,9021,9023,9027,9037,9081,9082,9201,9205,9207,9208,9209,9210,9211,9212,9213,48800,87,97,7510,8686,9180,9916,9918,9919,9928,9929,9939,33702,89,1000,1090,3501,3601,7800,8008,8077,8078,8106,8334,8336,9003,9898,9908,28080</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-Forward
ed-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>
```

```
        <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>
            <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` format

```
{
    "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": "80,81,82,83,84,88,800,808,3333,5000,5222,6001,6666,7000,7001,7002,7003,7004,7005,7006,7009,7010,7011,7012,7013,7014,7015,7016,7018,7019,7020,7021,7022,7023,7024,7025,7026,7070,7081,7082,7083,7088,7097,7777,8000,8001,8002,8003,8009,8020,8021,8022,8025,8026,8080,8081,8082,8083,8084,8085,8086,8087,8088,8089,8090,8091,8181,8800,8888,8889,8999,9000,9001,9002,9080,9200,9999,10000,10001,10080,12601,86,9021,9023,9027,9037,9081,9082,9201,9205,9207,9208,9209,9210,9211,9212,9213,48800,87,97,7510,8686,9180,9916,9918,9919,9928,9929,9939,33702,89,1000,1090,3501,3601,7800,8008,8077,8078,8106,8334,8336,9003,9898,9908,28080",
            "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-st2225l****",
    "Version": "version_hybrid_cloud_standard",
    "ExpireTime": "1677168000000"
}
```

Error codes

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

4.3. DeleteInstance

Releases expired subscription WAF instances.

After the instances are released, the data related to the instances is deleted and cannot be recovered. Proceed with caution.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteInstance	The operation that you want to perform. Set the value to DeleteInstance.
InstanceId	String	Yes	waf_elasticity-cn-0xldbqt****	The ID of the WAF instance.
ResourceGroupId	String	No	rg-atstuj3rtop****	The ID of the resource group to which the instance belongs. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

Response parameters

Parameter	Type	Example	Description
RequestId	String	F35F45B0-5D6B-4238-BE02-A62D0760E840	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DeleteInstance
&InstanceId=waf_elasticity-cn-0xldbqt****
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

5.Domain configurations

5.1. DescribeDomainList

Queries the domain names that are added to Web Application Firewall (WAF) by page.

> **Note** You can also call the DescribeDomainNames operation to query the domain names that are added to WAF. However, this operation does not support the paged query, and all domain names are returned on one page. If you want to query a large number of domain names, we recommend that you call the DescribeDomainList operation. This operation allows you to specify different conditions for the query and returns query results by page.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeDomainList	The operation that you want to perform. Set the value to **DescribeDomainList**.
InstanceId	String	Yes	waf-cn-7pp26f1****	The ID of the WAF instance. > **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
ResourceGroupId	String	No	rg-acfm2pz25js****	The ID of the resource group to which the WAF instance belongs in Resource Management. This parameter is empty by default, which indicates that the WAF instance belongs to the default resource group. For more information about resource groups, see Create a resource group.

Parameter	Type	Required	Example	Description
DomainName	String	No	example.com	The domain name to query. You can specify this parameter to check whether a domain name is added to WAF. Fuzzy match is supported.
DomainNames.N	RepeatList	No	example.com	Domain name N to query. You can specify this parameter to check whether multiple domain names are added to WAF. Fuzzy match is supported.
PageNumber	Integer	No	1	The number of the page to return. Pages start from page 1. Default value: **1**.
PageSize	Integer	No	10	The number of entries to return on each page. Default value: **10**.
IsSub	Integer	No	0	The type of domain name to query. Valid values: • **0**: all domain names, including both exact match domain names and wildcard domain names. This is the default value. • **1**: exact match domain names.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the **"Examples"** section of this topic.

Response parameters

Parameter	Type	Example	Description
DomainNames	List	["www.example.com","test.example.com"]	The domain names that are returned.
RequestId	String	592E866F-6C05-4E7C-81DE-B4D8E86B91EF	The ID of the request.

Parameter	Type	Example	Description
TotalCount	Integer	2	The number of domain names that are returned.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeDomainList
&InstanceId=waf-cn-7pp26f1****
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

5.2. DescribeDomainNames

Queries the domain names that are added to a specific WAF instance.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeDomainNames	The operation that you want to perform. Set the value to **DescribeDomainNames**.
InstanceId	String	Yes	waf_elasticity-cn-0xldbqt****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
ResourceGroupId	String	No	rg-atstuj3rtop****	The ID of the resource group to which the domain name belongs in Resource Management. This parameter is empty by default, indicating that the domain name belongs to the default resource group.

Response parameters

Parameter	Type	Example	Description
DomainNames	List	["1.example.com","2.example.com","3.example.com"]	An array that consists of the domain names that are added to the WAF instance.
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeDomainNames
&InstanceId=waf_elasticity-cn-0xldbqt****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<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` format

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

Error codes

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

5.3. DescribeDomain

Queries the configurations of a domain name that is added to Web Application Firewall (WAF).

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeDomain	The operation that you want to perform. Set this parameter to **DescribeDomain**.
Domain	String	Yes	www.example.com	The domain name that you want to query. **Note** You can call the DescribeDomainNames operation to query the domain names that are added to WAF.
InstanceId	String	Yes	waf-cn-7pp26f1****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the **Examples** section of this topic.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D827FCFE-90A7-4330-9326-D33C8B4C7726	The ID of the request.
Domain	Struct		The configurations of the domain name.
AccessHeaderMode	Integer	1	The method that WAF uses to obtain the actual IP address of a client. Valid values: • **0**: WAF reads the first value of the X-Forwarded-For (XFF) header field as the actual IP address of the client. • **1**: WAF reads the value of a custom header field as the actual IP address of the client. **Note** This parameter is returned only when the **IsAccessProduct** parameter is set to **1**. The value 1 indicates that a Layer 7 proxy is deployed in front of WAF.
AccessHeaders	List	["X-Client-IP"]	The custom header field that is used to obtain the actual IP address of a client. **Note** This parameter is returned only when the **AccessHeaderMode** parameter is set to **1**. The value 1 indicates that WAF reads the value of the custom header field as the actual IP address of a client.
AccessType	String	waf-cloud-dns	The mode that is used to add the domain name. Valid values: • **waf-cloud-dns**: CNAME record mode • **waf-cloud-native**: transparent proxy mode

Parameter	Type	Example	Description
CloudNativeInstances	Array of CloudNativeInstances		The list of configurations that are added in transparent proxy mode. **Note** This parameter is returned only when the **AccessType** parameter is set to **waf-cloud-native**.
CloudNativeProductName	String	ALB	The type of cloud service instance. Valid values: • **SLB**: Classic Load Balancer (CLB) instance, originally called Server Load Balancer (SLB) instance • **ECS**: Elastic Compute Service (ECS) instance • **ALB**: Application Load Balancer (ALB) instance
IPAddressList	String	["39.XX.XX.197"]	The public IP addresses of the cloud service instances.
InstanceId	String	alb-s65nua68wdedsp****	The ID of the cloud service instance.
ProtocolPortConfigs	Array of ProtocolPortConfigs		The protocol and port configurations.
Ports	String	[80]	The ports.
Protocol	String	http	The protocol. Valid values: • **http**: HTTP • **https**: HTTPS

Parameter	Type	Example	Description
RedirectionTypeName	String	ALB	The type of traffic redirection port. Valid values: • **SLB-L4**: Traffic on the Layer 4 listening ports of the CLB instance is redirected to WAF. • **SLB-L7**: Traffic on the Layer 7 listening ports of the CLB instance is redirected to WAF. • **ECS**: Traffic on the listening ports of the ECS instance is redirected to WAF. • **ALB**: Traffic on the HTTP and HTTPS listening ports of the ALB instance is redirected to WAF.
ClusterType	Integer	0	The type of WAF protection cluster. Valid values: • **0**: shared cluster • **1**: exclusive cluster **Note** This parameter is returned only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.
Cname	String	kdmqyi3ck7xogegxpiyfpb0fj21mgkxn.****.com	The CNAME assigned by WAF. **Note** This parameter is returned only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.
ConnectionTime	Integer	5	The timeout period for connections of WAF clusters. Unit: seconds. **Note** This parameter is returned only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.

Parameter	Type	Example	Description
Http2Port	List	[443,8443]	The HTTP/2 ports. **Note** This parameter is returned only when the value of the **AccessType** parameter is set to **waf-cloud-dns** and the **HttpsPort** parameter is not empty. If the HttpsPort parameter is not empty, your website uses HTTPS.
HttpPort	List	[80]	The HTTP ports. **Note** This parameter is returned only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.
HttpToUserIp	Integer	0	Indicates whether the feature of redirecting HTTPS requests to HTTP requests is enabled. Valid values: • **0**: The feature is disabled. • **1**: The feature is enabled. **Note** This parameter is returned only when the value of the **AccessType** parameter is set to **waf-cloud-dns** and the **HttpsPort** parameter is not empty. If the HttpsPort parameter is not empty, your website uses HTTPS.
HttpsPort	List	[443,8443]	The HTTPS ports. **Note** This parameter is returned only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.

Parameter	Type	Example	Description
HttpsRedirect	Integer	0	Indicates whether the feature of redirecting HTTP requests to HTTPS requests is enabled. Valid values: • **0**: The feature is disabled. • **1**: The feature is enabled. **Note** This parameter is returned only when the value of the **AccessType** parameter is set to **waf-cloud-dns** and the **HttpsPort** parameter is not empty. If the HttpsPort parameter is not empty, your website uses HTTPS.
IpFollowStatus	Integer	1	Indicates whether the feature of forwarding requests to the origin servers that use the IP address type specified in the requests is enabled. Valid values: • **0**: The feature is disabled. • **1**: The feature is enabled. **Note** This parameter is returned only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.
IsAccessProduct	Integer	1	Indicates whether a Layer 7 proxy is configured, which is used to filter inbound traffic before the traffic is sent to the WAF instance. The supported Layer 7 proxies include Anti-DDoS Pro, Anti-DDoS Premium, and Alibaba Cloud CDN. Valid values: • **0**: A Layer 7 proxy is not configured. • **1**: A Layer 7 proxy is configured.

Parameter	Type	Example	Description
LoadBalancing	Integer	2	The load balancing algorithm that is used when WAF forwards requests to the origin server. Valid values: • **0**: IP hash • **1**: Round-robin • **2**: least time **Note** This parameter is returned only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.
LogHeaders	Array of LogHeader		The key-value pair that is used to mark the requests that pass through the WAF instance. **Note** This parameter is returned only when the traffic marking feature is enabled for the domain name.
k	String	ALIWAF-TAG	The name of the custom header field.
v	String	Yes	The value of the custom header field.
ReadTime	Integer	120	The timeout period for read connections of WAF clusters. Unit: seconds. **Note** This parameter is returned only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.
ResourceGroupId	String	rg-acfm2mkrunv****	The ID of the resource group to which the WAF instance belongs.

Parameter	Type	Example	Description
SniHost	String	waf.example.com	The value of the custom Server Name Indication (SNI) field. If the parameter is left empty, the value of the **Host** field in the request header is automatically used as the value of the SNI field. **Note** This parameter is returned only when the value of the **SniStatus** parameter is set to **1**.
SniStatus	Integer	1	Indicates whether origin SNI is enabled. Origin Server Name Indication (SNI) specifies the domain name to which an HTTPS connection needs to be established at the start of the TLS handshaking process when WAF forwards requests to the origin server. Valid values: • **0**: Origin SNI is disabled. • **1**: Origin SNI is enabled. **Note** This parameter is returned only when the value of the **AccessType** parameter is set to **waf-cloud-dns** and the **HttpsPort** parameter is not empty. If the HttpsPort parameter is not empty, your website uses HTTPS.
SourceIps	List	["39.XX.XX.197"]	The IP address of the origin server. **Note** This parameter is returned only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.
Version	Long	40	The version of the domain name configuration.
WriteTime	Integer	120	The timeout period for write connections of WAF clusters. Unit: seconds. **Note** This parameter is returned only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeDomain
&Domain=www.example.com
&InstanceId=waf-cn-7pp26f1****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<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` format

```
{
  "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
    ]
  }
}
```


Error codes

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

5.4. CreateDomain

Adds a domain name to a Web Application Firewall (WAF) instance.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateDomain	The operation that you want to perform. Set the value to **CreateDomain**.
InstanceId	String	Yes	waf-cn-7pp26f1****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
Domain	String	Yes	www.example.com	The domain name that you want to add to WAF.
IsAccessProduct	Integer	Yes	0	Specifies whether to deploy a Layer 7 proxy, which is used to filter inbound traffic before the traffic reaches the WAF instance. The supported Layer 7 proxies include Anti-DDoS Pro, Anti-DDoS Premium, and Alibaba Cloud CDN. Valid values: • **0**: does not configure a Layer 7 proxy • **1**: configures a Layer 7 proxy

Parameter	Type	Required	Example	Description
AccessHeaderMode	Integer	No	0	The method that WAF uses to obtain the actual IP address of a client. Valid values: • **0**: WAF reads the first value of the X-Forwarded-For (XFF) header field as the actual IP address of the client. This is the default value. • **1**: WAF reads the value of a custom header field as the actual IP address of the client. **Note** You need to specify the parameter only when the **IsAccessProduct** parameter is set to **1**.
AccessHeaders	String	No	["X-Client-IP"]	The custom header fields that are used to obtain the actual IP address of a client. Specify the value in the `["header1","header2",...]` format. **Note** You need to specify the parameter only when the **AccessHeaderMode** parameter is set to **1**.

Parameter	Type	Required	Example	Description
LogHeaders	String	No	[{"k":"ALIWAF-TAG","v":"Yes"}]	The key-value pair that is used to mark the requests that pass through the WAF instance. Specify the key-value pair in the `[{"k":"_key_","v":"_value_"}]` format. `_key_` indicates the specified custom header field in a request. `_value_` indicates the value of the field. WAF automatically adds the key-value pair to the headers of requests. This way, the requests that pass through WAF are identified. **Note** If requests contain the custom header field, WAF overwrites the original value of the field with the specified value.
ResourceGroupId	String	No	rg-atstuj3rtop****	The ID of the resource group to which the WAF instance belongs in Resource Management. This parameter is empty by default, which indicates that the WAF instance belongs to the default resource group. For more information about resource groups, see Create a resource group.
AccessType	String	No	waf-cloud-dns	The mode that is used to add the domain name. Valid values: • **waf-cloud-dns**: CNAME record mode. This is the default value. • **waf-cloud-native**: transparent proxy mode.

Parameter	Type	Required	Example	Description
HttpPort	String	No	[80]	The HTTP ports. Specify the value in the `["port1","port2",...]` format. **Note** You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns**. If you specify this parameter, your website uses HTTP. You must specify at least one of the **HttpPort** and **HttpsPort** parameters.
HttpsPort	String	No	[443]	The HTTPS ports. Specify the value in the `["port1","port2",...]` format. **Note** You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns**. If you specify this parameter, your website uses HTTPS. You must specify at least one of the **HttpPort** and **HttpsPort** parameters.

Parameter	Type	Required	Example	Description
HttpsRedirect	Integer	No	0	Specifies whether to enable the feature of redirecting HTTP requests to HTTPS requests. If you enable the feature, HTTP requests are redirected to HTTPS requests on port 443, which is used by default. Valid values: • **0**: disables the feature. This is the default value. • **1**: enables the feature. **Note** You need to specify this parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns** and the **HttpsPort** parameter is not empty. If the HttpsPort parameter is not empty, your website uses HTTPS.
Http2Port	String	No	[443]	The HTTP/2 ports. Specify the value in the `["port1","port2",...]` format. **Note** You need to specify this parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns** and the **HttpsPort** parameter is not empty. If the HttpsPort parameter is not empty, your website uses HTTPS.

Parameter	Type	Required	Example	Description
HttpToUserIp	Integer	No	0	Specifies whether to enable the feature of redirecting HTTPS requests to HTTP requests. If you enable the feature, HTTPS requests are redirected to HTTP requests on port 80, which is used by default. Valid values: • **0**: disables the feature. This is the default value. • **1**: enables the feature. **Note** You need to specify this parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns** and the **HttpsPort** parameter is not empty. If the HttpsPort parameter is not empty, your website uses HTTPS.
IpFollowStatus	Integer	No	1	Specifies whether to enable the feature of forwarding requests to origin servers that use the IP address type specified in the requests. If you enable the feature, WAF forwards requests from IPv4 addresses to origin servers that use IPv4 addresses and requests from IPv6 addresses to origin servers that use IPv6 addresses. Valid values: • **0**: disables the feature. This is the default value. • **1**: enables the feature. **Note** You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.

Parameter	Type	Required	Example	Description
SourceIps	String	No	["39.XX.XX.197"]	The address type of the origin server. The address can be an IP address or a domain name. You can specify only one type of address. • If you use the IP address type, specify the value in the `["ip1","ip2",...]` format. You can add up to 20 IP addresses. • If you use the domain name type, specify the value in the `["domain"]` format. You can enter only one domain name. **Note** You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.
LoadBalancing	Integer	No	0	The load balancing algorithm that is used when WAF forwards requests to the origin server. Valid values: • **0**: IP hash • **1**: round-robin • **2**: least time **Note** You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.
ClusterType	Integer	No	0	The type of WAF protection cluster. Valid values: • **0**: shared cluster. This is the default value. • **1**: exclusive cluster. **Note** You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.

Parameter	Type	Required	Example	Description
ConnectionTime	Integer	No	5	The timeout period for connections of WAF exclusive clusters. Unit: seconds. **Note** You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns** and the value of the **ClusterType** parameter is set to **1**.
ReadTime	Integer	No	120	The timeout period for read connections of WAF exclusive clusters. Unit: seconds. **Note** You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns** and the value of the **ClusterType** parameter is set to **1**.
WriteTime	Integer	No	120	The timeout period for write connections of WAF exclusive clusters. Unit: seconds. **Note** You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns** and the value of the **ClusterType** parameter is set to **1**.

Parameter	Type	Required	Example	Description

CloudNativeInstances	String	No	[{"ProtocolPortConfigs":[{"Ports":[80],"Protocol":"http"}],"RedirectionTypeName":"ALB","InstanceId":"alb-s65nua68wdedsp****","IPAddressList":["182.XX.XX.113"],"CloudNativeProductName":"ALB"}]	The list of server and port configurations for the transparent proxy mode. The value is a string that consists of JSON arrays. Each element in a JSON array is a JSON struct that contains the following fields:
				• **ProtocolPortConfigs**: the list of protocol and port configurations. This field is required. Data type: array. Each element in a JSON array is a JSON struct that contains the following fields:
				  ◦ **Ports**: the list of ports. This field is required. Data type: array. The value is in the `[port1,port2,……]` format.
				  ◦ **Protocol**: the protocol. This field is required. Data type: string. Valid values: **http** and **https**.
				• **CloudNativeProductName**: the type of cloud service instance. This field is required. Data type: string. Valid values: **ECS**, **SLB**, and **ALB**.
				• **RedirectionTypeName**: the type of traffic redirection port. This field is required. Data type: string. Valid values: **ECS**, **SLB-L4**, **SLB-L7**, and **ALB**.
				• **InstanceId**: the ID of the cloud service instance. This field is required. Data type: string.
				• **IPAddressList**: the list of public IP addresses of the cloud service instance. This field is required. Data type: array. The value is in the `["ip1","ip2",...]` format.
				Note You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-native**.

Parameter	Type	Required	Example	Description
SniStatus	Integer	No	1	Specifies whether to enable origin SNI. Origin Server Name Indication (SNI) specifies the domain name to which an HTTPS connection needs to be established at the start of the TLS handshaking process when WAF forwards requests to the origin server. If the origin server hosts multiple domain names, you must enable this feature. Valid values: • **0**: disables origin SNI. • **1**: enables origin SNI. By default, origin SNI is disabled for WAF instances in mainland China and enabled for WAF instances outside mainland China. **Note** You need to specify this parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns** and the **HttpsPort** parameter is not empty. If the HttpsPort parameter is not empty, your website uses HTTPS.
SniHost	String	No	waf.example.com	The value of the custom SNI field. If this parameter is not specified, the value of the **Host** field in the request header is automatically used as the value of the SNI field. If you want WAF to use an SNI field whose value is different from the value of the Host field, you can specify a custom value for the SNI field. **Note** You need to specify this parameter only when the value of the **SniStatus** parameter is set to **1**.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the **Examples** section of this topic.

Response parameters

Parameter	Type	Example	Description
Cname	String	mmspx7qhfvnfzggheh1g2wnbhog66vcv.****.com	The CNAME assigned by WAF. **Note** This parameter is returned only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

5.5. ModifyDomain

Modifies the configurations of a domain name.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyDomain	The operation that you want to perform. Set the value to **ModifyDomain**.
Domain	String	Yes	www.example.com	The domain name whose configurations you want to modify. **Note** You can call the DescribeDomainNames operation to query the domain names that are added to Web Application Firewall (WAF).
InstanceId	String	Yes	waf-cn-7pp26f1****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
IsAccessProduct	Integer	Yes	0	Specifies whether to deploy a Layer 7 proxy, which is used to filter inbound traffic before the traffic reaches the WAF instance. The supported Layer 7 proxies include Anti-DDoS Pro, Anti-DDoS Premium, and Alibaba Cloud CDN. Valid values: • **0**: does not configure a Layer 7 proxy • **1**: configures a Layer 7 proxy

Parameter	Type	Required	Example	Description
SourceIps	String	No	["39.XX.XX.197"]	The address type of the origin server. The address can be an IP address or a domain name. You can specify only one type of address. • If you use the IP address type, specify the value in the `["ip1","ip2",...]` format. You can add up to 20 IP addresses. • If you use the domain name type, specify the value in the `["domain"]` format. You can enter only one domain name. **Note** You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.
LoadBalancing	Integer	No	0	The load balancing algorithm that is used when WAF forwards requests to the origin server. Valid values: • **0**: IP hash • **1**: round-robin • **2**: least time **Note** You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.
HttpPort	String	No	[80]	The HTTP ports. Specify the value in the `["port1","port2",...]` format. **Note** You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns**. If you specify this parameter, your website uses HTTP. You must specify at least one of the **HttpPort** and **HttpsPort** parameters.

Parameter	Type	Required	Example	Description
HttpsPort	String	No	[443]	The HTTPS ports. Specify the value in the `["port1","port2",...]` format. **Note** You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns**. If you specify this parameter, your website uses HTTPS. You must specify at least one of the **HttpPort** and **HttpsPort** parameters.
Http2Port	String	No	[443]	The HTTP/2 ports. Specify the value in the `["port1","port2",...]` format. **Note** You need to specify this parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns** and the **HttpsPort** parameter is not empty. If the HttpsPort parameter is not empty, your website uses HTTPS.
HttpsRedirect	Integer	No	0	Specifies whether to enable the feature of redirecting HTTP requests to HTTPS requests. If you enable the feature, HTTP requests are redirected to HTTPS requests on port 443, which is used by default. Valid values: • **0**: disables the feature. This is the default value. • **1**: enables the feature. **Note** You need to specify this parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns** and the **HttpsPort** parameter is not empty. If the HttpsPort parameter is not empty, your website uses HTTPS.

Parameter	Type	Required	Example	Description
HttpToUserIp	Integer	No	0	Specifies whether to enable the feature of redirecting HTTPS requests to HTTP requests. If you enable the feature, HTTPS requests are redirected to HTTP requests on port 80, which is used by default. Valid values: • **0**: disables the feature. This is the default value. • **1**: enables the feature. **Note** You need to specify this parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns** and the **HttpsPort** parameter is not empty. If the HttpsPort parameter is not empty, your website uses HTTPS.
AccessHeaderMode	Integer	No	0	The method that WAF uses to obtain the actual IP address of a client. Valid values: • **0**: WAF reads the first value of the X-Forwarded-For (XFF) header field as the actual IP address of the client. This is the default value. • **1**: WAF reads the value of a custom header field as the actual IP address of the client. **Note** You need to specify the parameter only when the **IsAccessProduct** parameter is set to **1**.

Parameter	Type	Required	Example	Description
AccessHeaders	String	No	["X-Client-IP"]	The custom header fields that are used to obtain the actual IP address of a client. Specify the value in the `["header1","header2",...]` format. **Note** You need to specify the parameter only when the **AccessHeaderMode** parameter is set to **1**.
LogHeaders	String	No	[{"k":"ALIWAF-TAG","v":"Yes"}]	The key-value pair that is used to mark the requests that pass through the WAF instance. Specify the key-value pair in the `[{"k":"_key_","v":"_value_"}]` format. `_key_` specifies a header field in a custom request. `_value_` specifies the value of the field. WAF automatically adds the key-value pair to the headers of requests. This way, the requests that pass through WAF are identified. **Note** If requests contain the custom header field, WAF overwrites the original value of the field with the specified value.
ClusterType	Integer	No	0	The type of WAF protection cluster. Valid values: • **0**: shared cluster. This is the default value. • **1**: exclusive cluster. **Note** You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.

Parameter	Type	Required	Example	Description
ConnectionTime	Integer	No	5	The timeout period for connections of WAF exclusive clusters. Unit: seconds. **Note** You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns** and the value of the **ClusterType** parameter is set to **1**.
ReadTime	Integer	No	120	The timeout period for read connections of WAF exclusive clusters. Unit: seconds. **Note** You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns** and the value of the **ClusterType** parameter is set to **1**.
WriteTime	Integer	No	120	The timeout period for write connections of WAF exclusive clusters. Unit: seconds. **Note** You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns** and the value of the **ClusterType** parameter is set to **1**.
AccessType	String	No	waf-cloud-dns	The mode that is used to add the domain name. Valid values: • **waf-cloud-dns**: CNAME record mode. This is the default value. • **waf-cloud-native**: transparent proxy mode.

Parameter	Type	Required	Example	Description

CloudNativeInstances	String	No	[{"ProtocolPortConfigs":[{"Ports":[80],"Protocol":"http"}],"RedirectionTypeName":"ALB","InstanceId":"alb-s65nua68wdedsp****","IPAddressList":["182.XX.XX.113"],"CloudNativeProductName":"ALB"}]	The list of server and port configurations for the transparent proxy mode. The value is a string that consists of JSON arrays. Each element in a JSON array is a JSON struct that contains the following fields:
				• **ProtocolPortConfigs**: the list of protocol and port configurations. This field is required. Data type: array. Each element in a JSON array is a JSON struct that contains the following fields:
				  ○ **Ports**: the list of ports. This field is required. Data type: array. The value is in the `[port1,port2,……]` format.
				  ○ **Protocol**: the protocol. This field is required. Data type: string. Valid values: **http** and **https**.
				• **CloudNativeProductName**: the type of the cloud service instance. This field is required. Data type: string. Valid values: **ECS**, **SLB**, and **ALB**.
				• **RedirectionTypeName**: the type of traffic redirection port. This field is required. Data type: string. Valid values: **ECS**, **SLB-L4**, **SLB-L7**, and **ALB**.
				• **InstanceId**: the ID of the cloud service instance. This field is required. Data type: string.
				• **IPAddressList**: the list of public IP addresses of the cloud service instance. This field is required. Data type: array. The value is in the `["ip1","ip2",...]` format.
				Note You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-native**.

Parameter	Type	Required	Example	Description
IpFollowStatus	Integer	No	0	Specifies whether to enable the feature of forwarding requests to the origin servers that use the IP address type specified in the requests. If you enable the feature, WAF forwards requests from IPv4 addresses to origin servers that use IPv4 addresses and requests from IPv6 addresses to origin servers that use IPv6 addresses. Valid values: • **0**: disables the feature. This is the default value. • **1**: enables the feature. **Note** You need to specify the parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns**.
SniStatus	Integer	No	1	Specifies whether to enable origin SNI. Origin Server Name Indication (SNI) specifies the domain name to which an HTTPS connection needs to be established at the start of the TLS handshaking process when WAF forwards requests to the origin server. If the origin server hosts multiple domain names, you must enable this feature. Valid values: • **0**: disables origin SNI. • **1**: enables origin SNI. By default, origin SNI is disabled for WAF instances in mainland China and enabled for WAF instances outside mainland China. **Note** You need to specify this parameter only when the value of the **AccessType** parameter is set to **waf-cloud-dns** and the **HttpsPort** parameter is not empty. If the HttpsPort parameter is not empty, your website uses HTTPS.

Parameter	Type	Required	Example	Description
SniHost	String	No	waf.example.com	The value of the custom SNI field. If this parameter is not specified, the value of the **Host** field in the request header is automatically used as the value of the SNI field. If you want WAF to use an SNI field whose value is different from the value of the Host field, you can specify a custom value for the SNI field. **Note** This parameter needs to be set only when the value of the **SniStatus** parameter is set to **1**.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the **Examples** section of this topic.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

5.6. DeleteDomain

Deletes a specific domain name.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteDomain	The operation that you want to perform. Set the value to **DeleteDomain**.
Domain	String	Yes	www.example.com	The domain name that is added to WAF.
InstanceId	String	Yes	waf_elasticity-cn-0xldbqt****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DeleteDomain
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqt****
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

5.7. DescribeCertificates

Queries the SSL certificate that is bound to a specific domain name.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeCertificates	The operation that you want to perform. Set the value to **DescribeCertificates**.
Domain	String	Yes	www.example.com	The domain name that is added to WAF.

Parameter	Type	Required	Example	Description
InstanceId	String	Yes	waf_elasticity-cn-0xldbqt****	The ID of the WAF instance. Note You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.

Response parameters

Parameter	Type	Example	Description
Certificates	Array		The information about the SSL certificate that is bound to the domain name.
CertificateId	Long	2329260	The ID of the SSL certificate.
CertificateName	String	CertName	The name of the SSL certificate.
CommonName	String	*.example.com	The domain name to which the SSL certificate is bound.
IsUsing	Boolean	false	Indicates whether the SSL certificate is being used by the domain name.
Sans	List	["*.example.com"]	An array that consists of domain names that are protected by WAF and bound to the SSL certificate.
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeCertificates
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqt****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<?xml version="1.0" encoding="UTF-8" ?>
<DescribeCertificatesResponse>
    <Certificates>
        <Sans>*.example.com</Sans>
        <CertificateId>2329260</CertificateId>
        <CertificateName>CertName</CertificateName>
        <IsUsing>true</IsUsing>
        <CommonName>*.example.com</CommonName>
    </Certificates>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</requestId>
</DescribeCertificatesResponse>
```

`JSON` format

```
{
    "Certificates": [
        {
            "Sans": [
                "*.example.com"
            ],
            "CertificateId": 2329260,
            "CertificateName": "CertName",
            "IsUsing": true,
            "CommonName": "*.example.com"
        }
    ],
    "RequestId": "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes

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

5.8. DescribeCertMatchStatus

Checks whether the certificate of a specific domain name matches the private key.

Debugging

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

Request parameters

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

Parameter	Type	Required	Example	Description
Certificate	String	Yes	-----BEGIN CERTIFICATE----- 62EcYPWd2Oy1vs 6MTXcJSfN9Z7rZ 9fmxWr2BFN2Xb ahgnsSXM48ixZJ4 krc+1M+j2kcubVp sE2cgHdj4v8H6jU z9Ji4mr7vMNS6d Xv8PUkl/qoDeNG CNdyTS5NIL5ir+g 92cL8IGOkjgvhlqt 9vc65Cgb4mL+n5 +DV9uOyTZTW/M ojmlgfUekC2xiXa 54nxJf17Y1TADGS byJbsC0Q9nIrHsPl 8YKkvRWvlAqYxX Z7wRwWWmv4T MxFhWRiNY7yZIo 2ZUhl02SIDNggIE eg== -----END CERTIFICATE-----	The content of the certificate.
Domain	String	Yes	www.example.com	The domain name that is added to WAF.
InstanceId	String	Yes	waf_elasticity-cn-0xldbqt****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.

Parameter	Type	Required	Example	Description
PrivateKey	String	Yes	-----BEGIN RSA PRIVATE KEY----- DADTPZoOHd9WtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThLyvsmLQKBgQCr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJaiygoIYoaMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04RtKadOw== -----END RSA PRIVATE KEY-----	The content of the private key.

Response parameters

Parameter	Type	Example	Description
MatchStatus	Boolean	false	Indicates whether the certificate matches the private key.
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
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-----
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

5.9. CreateCertificate

Uploads a certificate and a private key for a specific domain name.

> **Note** You can also call this operation to update the certificate and private key that are uploaded for a specific domain name.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateCertificate	The operation that you want to perform. Set the value to **CreateCertificate**.
CertificateName	String	Yes	CertName	The name of the certificate.
Domain	String	Yes	www.example.com	The domain name that is added to WAF.

Parameter	Type	Required	Example	Description
InstanceId	String	Yes	waf_elasticity-cn-0xldbqt****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
PrivateKey	String	Yes	-----BEGIN RSA PRIVATE KEY----- DADTPZoOHd9WtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThLyvsmLQKBgQCr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJaiggoIYoaMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04RtKadOw== -----END RSA PRIVATE KEY-----	The private key that corresponds to the certificate.

Parameter	Type	Required	Example	Description
Certificate	String	No	-----BEGIN CERTIFICATE----- 62EcYPWd2Oy1vs 6MTXcJSfN9Z7rZ 9fmxWr2BFN2Xb ahgnsSXM48ixZJ4 krc+1M+j2kcubVp sE2cgHdj4v8H6jU z9Ji4mr7vMNS6d Xv8PUkl/qoDeNG CNdyTS5NIL5ir+g 92cL8IGOkjgvhlqt 9vc65Cgb4mL+n5 +DV9uOyTZTW/M ojmlgfUekC2xiXa 54nxJf17Y1TADGS byJbsC0Q9nIrHsPl 8YKkvRWvlAqYxX Z7wRwWWmv4T MxFhWRiNY7yZIo 2ZUhl02SIDNggIE eg== -----END CERTIFICATE-----	The content of the certificate.
HttpsCertId	Long	No	123456	The ID of the certificate.

Response parameters

Parameter	Type	Example	Description
CertificateId	Long	2329260	The ID of the certificate record. This ID is automatically generated by WAF.
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
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-----
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

5.10. CreateCertificateByCertificateId

Uploads a certificate for a specific domain name based on the certificate ID.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateCertificateByCertificateId	The operation that you want to perform. Set the value to **CreateCertificateByCertificateId**.
Domain	String	Yes	www.example.com	The domain name that is added to WAF.
InstanceId	String	Yes	waf_elasticity-cn-0xldbqt****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
CertificateId	Long	No	3384669	The ID of the certificate.

Response parameters

Parameter	Type	Example	Description
CertificateId	Long	3384669	The ID of the certificate.
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CreateCertificateByCertificateId
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqt****
&CertificatedId=3384669
&<Common request parameters>
```

Sample success responses

`XML` format

```
<CreateCertificateByCertificateIdResponse>
   <CertificateId>3384669</CertificateId>
   <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</CreateCertificateByCertificateIdResponse>
```

`JSON` format

```
{
    "CertificateId": "3384669",
    "RequestId": "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes

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

5.11. DescribeDomainBasicConfigs

Queries the protection settings of the domain names that are protected by Web Application Firewall (WAF).

Usage notes

You can call the DescribeDomainBasicConfigs operation to perform a paged query for the protection settings of the domain names that are protected by WAF. The settings include the status of the protection settings for each domain name, and the status and mode of each protection module. The protection modules include the protection rules engine, HTTP flood protection, and custom protection policy.

Limits

You can call this operation up to 50 times per second per account. If the number of the calls per second exceeds the limit, throttling is triggered. As a result, your business may be affected. We recommend that you take note of the limit when you call this operation.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeDomainBasicConfigs	The operation that you want to perform. Set the value to **DescribeDomainBasicConfigs**.
InstanceId	String	Yes	waf-cn-tl32ast****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
DomainKey	String	No	aliyundoc	The keyword of the domain names. WAF returns the protection settings of the domain names that contain the keyword. If you do not specify this parameter, the protection settings of all domain names are returned.

Parameter	Type	Required	Example	Description
AccessType	String	No	waf-cloud-dns	The access mode of the domain names. WAF returns the protection settings of the domain names that are added to WAF in the specified mode. Valid values: • **waf-cloud-dns**: CNAME record mode • **waf-cloud-native**: transparent proxy mode If you do not specify this parameter, the protection settings of all domain names are returned.
CloudNativeProductId	Integer	No	0	The type of the origin server. WAF returns the protection settings of the domain names that are added to WAF in transparent proxy mode and are configured with the specified type of origin server. Valid values: • **0**: an Elastic Compute Service (ECS) instance. • **1**: a Classic Load Balancer (CLB) instance. • **2**: an Application Load Balancer (ALB) instance. If you do not specify this parameter, the protection settings of all domain names are returned.
PageNumber	Integer	No	1	The number of the page to return. Default value: **1**.
PageSize	Integer	No	10	The number of entries to return on each page. Default value: **10**.
ResourceGroupId	String	No	rg-acfm2pz25js****	The ID of the resource group to which the domain name belongs in Resource Management. If you do not specify this parameter, the domain name belongs to the default resource group.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the **"Examples"** section of this topic.

Response parameters

Parameter	Type	Example	Description
TotalCount	Integer	1	The total number of entries returned.
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
DomainConfigs	Array of DomainConfig		The protection settings of the domain name.
Status	Integer	1	The status of the protection settings for the domain name. Valid values: • **0**: invalid or deleted • **1**: valid or created • **10**: creating • **11**: creation failed • **20**: deleting
Domain	String	www.aliyundoc.com	The domain name.
Owner	String	WAF	The source of the protection settings for the domain name. The value is fixed as **WAF**, which indicates that the protection settings are created in WAF.
CcMode	Integer	0	The mode of the HTTP flood protection module. Valid values: • **0**: the **protection** mode • **1**: the **protection-emergency** mode
CcStatus	Integer	1	The status of the HTTP flood protection module. Valid values: • **0**: disabled • **1**: enabled
AccessType	String	waf-cloud-dns	The access mode of the domain name. Valid values: • **waf-cloud-dns**: CNAME record mode • **waf-cloud-native**: transparent proxy mode

Parameter	Type	Example	Description
Version	Long	0	The version of the protection settings.
AclStatus	Integer	1	The status of the custom protection policy module. Valid values: • **0**: disabled • **1**: enabled
WafStatus	Integer	1	The status of the protection rules engine module. Valid values: • **0**: disabled • **1**: enabled
WafMode	Integer	0	The mode of the protection rules engine module. Valid values: • **0**: the **block** mode • **1**: the **warn** mode

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeDomainBasicConfigs
&InstanceId=waf-cn-tl32ast****
&PageNumber=1
&PageSize=10
&Common request parameters
```

Sample success responses

`XML` format

```
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` format

```
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
  } ]
}
```

Error codes

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

5.12. DescribeDomainAdvanceConfigs

Queries the details about the configurations of the domain names that are protected by Web Application Firewall (WAF).

Description

You can call the DescribeDomainAdvanceConfigs operation to query the details about the configurations of the domain names that are protected by WAF. The details include the CNAMEs, origin server addresses, and HTTP and HTTPS ports.

Limits

You can call this operation up to 50 times per second per account. If the number of the calls per second exceeds the limit, throttling is triggered. As a result, your business may be affected. We recommend that you take note of the limit when you call this operation.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeDomainAdvanceConfigs	The operation that you want to perform. Set the value to **DescribeDomainAdvanceConfigs**.
InstanceId	String	Yes	waf-cn-2r427ng****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
DomainList	String	Yes	www.aliyundoc.com	The domain name for which you want to query the details about the configurations. If you enter multiple domain names, separate the domain names with commas (,). **Note** You can call the DescribeDomainList operation to query all domain names that are protected by WAF.
ResourceGroupId	String	No	rg-atstuj3rtop****	The ID of the resource group to which the domain name belongs in Resource Management. If you do not specify this parameter, the domain name belongs to the default resource group.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the **"Examples"** section of this topic.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
DomainConfigs	Array of DomainConfig		The details about the configurations of the domain name.
Domain	String	www.aliyundoc.com	The domain name.
Profile	Object		The configurations of the domain name.
Http2Port	Array of Integer	443	The HTTP/2 port.
Ipv6Status	Integer	1	Indicates whether protection against malicious IPv6 traffic is enabled. Valid values: • **0**: The protection is disabled. • **1**: The protection is enabled.
HttpPort	Array of Integer	80	The HTTP port.
GSLBStatus	String	on	Indicates whether intelligent load balancing is enabled. Valid values: • **off** • **on**
Rs	Array of String	38.XX.XX.42	The address of the origin server.
VipServiceStatus	Integer	0	The service status of the IP address of the WAF instance or the exclusive WAF cluster. Valid values: • **0**: The traffic to the IP address is normal. • **1**: The traffic to the IP address is being scrubbed. • **2**: The traffic to the IP address is undergoing blackhole filtering.

Parameter	Type	Example	Description
ClusterType	Integer	0	The type of the WAF cluster. Valid values: • **0**: shared cluster. This is the default value. • **1**: exclusive cluster.
ExclusiveVipStatus	Integer	0	Indicates whether an exclusive WAF IP address is used. Valid values: • **0**: no • **1**: yes
Cname	String	****dsbpkt75zeiok5mta2j5l7hggcrm.****.com	The CNAME that the WAF instance assigns for the domain name.
CertStatus	Integer	1	Indicates the status of the certificate that is configured for the domain name. This parameter is returned only when the domain name supports HTTPS. Valid values: • **0**: abnormal. For example, no certificate is uploaded, or the uploaded certificate is invalid. • **1**: normal. For example, a certificate is uploaded, and the certificate is valid.
HttpsPort	Array of Integer	443	The HTTPS port.
ResolvedType	Integer	0	The IP address to which the CNAME is resolved. Valid values: • **-1**: the IP address of the origin server. • **0**: the IP address of the WAF instance. • **1**: the IP address of the exclusive WAF cluster.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeDomainAdvanceConfigs
&InstanceId=waf-cn-2r427ng****
&DomainList=www.aliyundoc.com
&Common request parameters
```

Sample success responses

`XML` format

```
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` format

```
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
    }
  } ]
}
```

Error codes

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

6.Protection configuration

6.1. ModifyDomainIpv6Status

Enables or disables protection for a specific domain name against malicious IPv6 traffic.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyDomainIpv6Status	The operation that you want to perform. Set the value to **ModifyDomainIpv6Status**.
Domain	String	Yes	www.example.com	The domain name that is added to WAF.
Enabled	String	Yes	0	Specifies whether to enable protection against malicious IPv6 traffic. Valid values: • **0**: disables protection against malicious IPv6 traffic • **1**: enables protection against malicious IPv6 traffic
InstanceId	String	Yes	waf-cn-mp9153****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyDomainIpv6Status
&Domain=www.example.com
&Enabled=0
&InstanceId=waf-cn-mp9153****
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

6.2. DescribeProtectionModuleStatus

Queries the status of a specific protection module of Web Application Firewall (WAF).

You can set the **DefenseType** parameter to specify the protection module. For more information about the value of this parameter, see the description of the **DefenseType** parameter in the "Request parameters" section of this topic.

Debugging

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

Request parameters

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

Parameter	Type	Required	Example	Description
DefenseType	String	Yes	waf	The WAF protection module that you want to query. Valid values: • **waf**: Protection Rules Engine • **dld**: Big Data Deep Learning Engine • **tamperproof**: Website Tamper-proofing • **dlp**: Data Leakage Prevention • **normalized**: Positive Security Model • **bot_crawler**: Allowed Crawlers • **bot_intelligence**: Bot Threat Intelligence • **antifraud**: Data Risk Control • **bot_algorithm**: Intelligent Algorithm • **bot_wxbb**: App Protection • **bot_wxbb_pkg**: Version Protection for App Protection • **cc**: HTTP Flood Protection • **blacklist**: Blacklists • **ac_highfrep**: Blocking IPs Initiating High-frequency Web Attacks • **ac_dirscan**: Directory Traversal Prevention • **ac_scantool**: Scanning Tool Blocking • **ac_collaborative**: Collaborative Defense • **ac_custom**: Custom Protection Policy You can specify only one protection module.
Domain	String	Yes	www.example.com	The domain name of the website that you want to query. **Note** You must specify a domain name that is added to WAF for protection. You can call the DescribeDomainNames operation to query the domain names that are added to WAF for protection.

Parameter	Type	Required	Example	Description
InstanceId	String	Yes	waf_elasticity-cn-0xldbqt****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.

Response parameters

Parameter	Type	Example	Description
ModuleStatus	Integer	1	Indicates whether the protection module is enabled. Valid values: • **0**: disabled • **1**: enabled
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeProtectionModuleStatus
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqt****
&DefenseType=waf
&<Common request parameters>
```

Sample success responses

`XML` format

```
<ModifyProtectionRuleCacheStatusResponse>
   <ModuleStatus>1</ModuleStatus>
   <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</ModifyProtectionRuleCacheStatusResponse>
```

`JSON` format

```
{"RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0","ModuleStatus":"1"}
```

Error codes

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

6.3. ModifyProtectionModuleStatus

Enables or disables a protection module of Web Application Firewall (WAF).

You can set the **DefenseType** parameter to specify the protection module. For more information about the value of this parameter, see the description of the **DefenseType** parameter in the "Request parameters" section of this topic.

Debugging

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

Request parameters

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

Parameter	Type	Required	Example	Description
DefenseType	String	Yes	waf	The WAF protection module that you want to manage. Valid values: • **waf**: Protection Rules Engine • **dld**: Big Data Deep Learning Engine • **tamperproof**: Website Tamper-proofing • **dlp**: Data Leakage Prevention • **normalized**: Positive Security Model • **bot_crawler**: Allowed Crawlers • **bot_intelligence**: Bot Threat Intelligence • **antifraud**: Data Risk Control • **bot_algorithm**: Intelligent Algorithm • **bot_wxbb**: App Protection • **bot_wxbb_pkg**: Version Protection for App Protection **Note** If you enable the version protection module, you must call the CreateProtectionModuleRule operation to create a version protection rule. This rule specifies the allowed versions. • **cc**: HTTP Flood Protection • **blacklist**: Blacklists • **ac_highfrep**: Blocking IPs Initiating High-frequency Web Attacks • **ac_dirscan**: Directory Traversal Prevention • **ac_scantool**: Scanning Tool Blocking • **ac_collaborative**: Collaborative Defense • **ac_custom**: Custom Protection Policy You can specify only one protection module.

Parameter	Type	Required	Example	Description
Domain	String	Yes	www.example.com	The domain name of the website. **Note** You must specify a domain name that is added to WAF for protection. You can call the DescribeDomainNames operation to query the domain names that are added to WAF for protection.
InstanceId	String	Yes	waf_elasticity-cn-0xldbqt****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
ModuleStatus	Integer	Yes	1	Specifies whether to enable or disable the specified protection module. Valid values: • **0**: disables the protection module • **1**: enables the protection module

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyProtectionModuleStatus
&DefenseType=waf
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqt****
&ModuleStatus=1
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

6.4. DescribeProtectionModuleMode

Queries the protection mode of a protection module for a specific domain name. The protection modules include the RegEx Protection Engine, Big Data Deep Learning Engine, HTTP flood protection, data risk control, and positive security model.

You can set the **DefenseType** parameter to specify the protection module. For more information about the value of this parameter, see the description of the **DefenseType** parameter in the "Request parameters" section of this topic.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeProtectionModuleMode	The operation that you want to perform. Set the value to **DescribeProtectionModuleMode**.
DefenseType	String	Yes	waf	The protection module. Valid values: • **waf**: RegEx Protection Engine • **dld**: Big Data Deep Learning Engine • **cc**: HTTP Flood Protection • **antifraud**: Data Risk Control • **normalized**: Positive Security Model

Parameter	Type	Required	Example	Description
Domain	String	Yes	www.example.com	The domain name that is added to WAF.
InstanceId	String	Yes	waf_elasticity-cn-0xldbqt****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
ResourceGroupId	String	No	rg-atstuj3rtop****	The ID of the resource group to which the domain name belongs in Resource Management. This parameter is empty by default, indicating that the domain name belongs to the default resource group.

Response parameters

Parameter	Type	Example	Description

Parameter	Type	Example	Description

Mode	Integer	1	The protection mode of the specified protection module. Valid values:
			Note The value of the **Mode** parameter varies based on the value of the **DefenseType** parameter.
			• RegEx Protection Engine (The DefenseType parameter is set to **waf**.)
			  ◦ **0**: block mode
			  ◦ **1**: warn mode
			• Big Data Deep Learning Engine (The DefenseType parameter is set to **dld**.)
			  ◦ **0**: warn mode
			  ◦ **1**: block mode
			• HTTP flood protection (The DefenseType parameter is set to **ac_cc**.)
			  ◦ **0**: prevention mode
			  ◦ **1**: protection-emergency mode
			• Data risk control (The DefenseType parameter is set to **antifraud**.)
			  ◦ **0**: warn mode
			  ◦ **1**: block mode
			  ◦ **2**: strict interception mode
			• Positive security model (The DefenseType parameter is set to **normalized**.)
			  ◦ **0**: warn mode
			  ◦ **1**: block mode

RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeProtectionModuleMode
&DefenseType=waf
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqt****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeProtectionModuleModeResponse>
      <Mode>1</Mode>
      <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</DescribeProtectionModuleModeResponse>
```

`JSON` format

```
{
    "Mode": 1,
    "RequestId": "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes

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

6.5. ModifyProtectionModuleMode

Modifies the protection mode of a specific protection module of Web Application Firewall (WAF). The protection modules include the RegEx Protection Engine, Big Data Deep Learning Engine, HTTP flood protection, data risk control, and positive security model.

You can set the **DefenseType** parameter to specify the protection module. For more information about the value of this parameter, see the description of the **DefenseType** parameter in the "Request parameters" section of this topic.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyProtectionModuleMode	The operation that you want to perform. Set the value to **ModifyProtectionModuleMode**.
DefenseType	String	Yes	waf	The protection module. Valid values: • **waf**: RegEx Protection Engine • **dld**: Big Data Deep Learning Engine • **cc**: HTTP Flood Protection • **antifraud**: Data Risk Control • **normalized**: Positive Security Model

Parameter	Type	Required	Example	Description
Domain	String	Yes	www.example.com	The domain name that is added to WAF.
InstanceId	String	Yes	waf_elasticity-cn-0xldbqt****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.

Mode	Integer	Yes	0	The protection mode of the specified protection module. Valid values:
				Note The value of the **Mode** parameter varies based on the value of the **DefenseType** parameter.
				• RegEx Protection Engine (The DefenseType parameter is set to **waf**.)
				  ◦ **0**: block mode
				  ◦ **1**: warn mode
				• Big Data Deep Learning Engine (The DefenseType parameter is set to **dld**.)
				  ◦ **0**: warn mode
				  ◦ **1**: block mode
				• HTTP flood protection (The DefenseType parameter is set to **ac_cc**.)
				  ◦ **0**: prevention mode
				  ◦ **1**: protection-emergency mode
				• Data risk control (The DefenseType parameter is set to **antifraud**.)
				  ◦ **0**: warn mode
				  ◦ **1**: block mode
				  ◦ **2**: strict interception mode
				• Positive security model (The DefenseType parameter is set to **normalized**.)
				  ◦ **1**: block mode
				  ◦ **0**: warn mode

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

6.6. DescribeProtectionModuleRules

Queries the rules that are configured in a specific protection module of Web Application Firewalls (WAF), such as the web intrusion prevention, data security, bot management, access control or throttling, or website whitelist module.

Usage notes

You can call the DescribeProtectionModuleRules operation to perform a paged query of the rules that are configured in a specific WAF protection module. The protection modules include web intrusion prevention, data security, bot management, access control or throttling, and website whitelist.

You can set the **DefenseType** parameter to specify a protection module. For more information about the values of this parameter, see the description of the **DefenseType** parameter.

Limits

You can call this operation up to 50 times per second per account. If the number of the calls per second exceeds the limit, throttling is triggered. As a result, your business may be affected. We recommend that you take note of the limit when you call this operation.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeProtectionModuleRules	The operation that you want to perform. Set the value to **DescribeProtectionModuleRules**.
PageSize	Integer	No	10	The number of entries to return on each page. Default value: **10**.
PageNumber	Integer	No	1	The number of the page to return. Default value: **1**.
Domain	String	No	www.aliyundoc.com	The domain name that you want to query. • If you set the **DefenseType** parameter to a value other than **ng_account**, you must also specify this parameter. **Note** You can call the DescribeDomainList operation to query all the domain names that are protected by WAF. • If you set the **DefenseType** parameter to **ng_account**, leave this parameter unspecified. Otherwise, an error message is returned.

Parameter	Type	Required	Example	Description
DefenseType	String	Yes	ac_highfreq	The type of the protection feature whose rule you want to query. Valid values: • **waf-codec**: decoding configuration of the protection rules engine feature • **tamperproof**: website tamper-proofing • **dlp**: data leak prevention • **ng_account**: account security • **bot_crawler**: allowed crawlers • **bot_intelligence**: bot threat intelligence • **antifraud**: data risk control • **antifraud_js**: configuration of a web page into which a JavaScript plug-in is inserted for data risk control • **bot_algorithm**: intelligent algorithm • **bot_wxbb_pkg**: version protection for the app protection module • **bot_wxbb**: path protection for the app protection module • **ac_blacklist**: IP address blacklist • **ac_highfreq**: blocking configuration of IP addresses that initiate high-frequency web attacks • **ac_dirscan**: scan protection • **ac_custom**: custom protection policy • **whitelist**: website whitelist
				The methods that are used to filter and sort the rules. The value is a JSON string that contains the following parameters: **Note** The value of the Query parameter must be Base64-encoded. • **filter**: the filter conditions. This parameter is optional. Data type: JSON string. The value is a string that consists of a JSON struct. The JSON struct contains the following fields:

Parameter	Type	Required	Example	Description
				○ **nameId**: queries the rules whose IDs are the same as the value of this parameter or the rules whose names contain the parameter value. This parameter is optional. Data type: string. ○ **scene**: the protection module whose rule you want to query. The valid values of this parameter are the same as those of the **DefenseType** parameter. This parameter is optional. Data type: string. ○ **enabled**: specifies whether the rule is enabled. This parameter is optional. Data type: Boolean. Valid values: ■ **false**: disabled ■ **true**: enabled ○ **status**: the status of the rule. The meaning of this parameter is the same as that of the **enabled** parameter. This parameter is optional. Data type: integer. Valid values: ■ **0**: disabled ■ **1**: enabled ○ **ruleId**: the ID of the rule. This parameter is optional. Data type: integer. ○ **ruleIdList**: the list of rule IDs. Separate multiple rule IDs with commas (,). This parameter is optional. Data type: array. ○ **sceneList**: the list of protection modules. The valid values of this parameter are the same as those of the **DefenseType** parameter. Separate multiple protection modules with commas (,). This parameter is optional. Data type: array. ○ **originList**: the list of rule sources. Separate multiple rule sources with commas (,). This parameter is optional. Data type: array. Valid values: **system** (system-generated) and **custom** (user-customized).
Query	String	No	e2ZpbHRlcjp7InJ1bGVJZCI6NDI3NTV9LG9yZGVyQnk6ImdtdF9tb2RpZmllZCIsZGVzYzp0cn	

Parameter	Type	Required	Example	Description
			VlfQ==	○ **tag**: If you set the DefenseType parameter to **whitelist**, you can set this parameter to query the whitelist rules of specific modules that do not detect requests. This parameter is optional. Data type: string. For more information about **tag**, see the description of whitelist rules in the "Description of the Content parameter" section. ○ **origin**: If you set the DefenseType parameter to **whitelist**, you can set this parameter to query the whitelist rules that are automatically added by the intelligent rule hosting feature. This parameter is optional. Data type: string. Set the value to **ai**. If you do not set this parameter, all whitelist rules are queried, including the rules that you manually added and the rules that are automatically added by the intelligent rule hosting feature. ○ **category**: If you set the DefenseType parameter to **whitelist**, you can set this parameter to query a specific type of whitelist. This parameter is optional. Data type: string. Valid values: ■ **waf**: website whitelist ■ **ws**: whitelist for web intrusion prevention whitelist ■ **ac**: whitelist for access control/throttling ■ **ds**: data security whitelist • **orderBy**: the sorting method. This parameter is optional. Data type: string. Valid values: ○ **action**: the action that is performed after the rule is matched. This parameter takes effect only when you query the rules of the custom protection policy module. ○ **gmt_modified**: the time when the rule was last modified. This is the default value. ○ **name**: the name of the rule. ○ **status**: the status of the rule.

Parameter	Type	Required	Example	Description
				• **desc**: specifies whether the rule is sorted in descending order. This parameter is optional. Data type: Boolean. Valid values: ◦ **false**: ascending order. ◦ **true**: descending order. This is the default value.
Lang	String	No	zh	The language of the rule name. Valid values: • **zh**: Chinese • **en**: English • **ja**: Japanese
InstanceId	String	Yes	waf_elasticity-cn-0xldbqt****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
ResourceGroupId	String	No	rg-acfm2pz25js****	The ID of the resource group to which the WAF instance belongs in Resource Management. If you do not specify this parameter, the WAF instance belongs to the default resource group.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "**Examples**" section of this topic.

Response parameters

Parameter	Type	Example	Description
TotalCount	Integer	1	The total number of entries returned.
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Parameter	Type	Example	Description
Rules	Array of Rule		The configurations of the rule, including the rule ID, creation time, and status.
Status	Long	1	The status of the rule. Valid values: • **0**: disabled • **1**: enabled
Time	Long	1570700044	The time when the rule was created. This value is a UNIX timestamp. Unit: seconds.
Content	Map		The content of the rule. This value is a JSON string that contains multiple parameters. **Note** The parameters vary based on the value of the **DefenseType** parameter. For more information, see the **"Description of the Content parameter"** section.
Version	Long	2	The version of the rule.
RuleId	Long	42755	The ID of the rule.

Description of the Content parameter

- If the DefenseType parameter is set to **waf-codec**, the value of the Content parameter contains the following parameter:
  - **codecList**: the enabled decoding items. This parameter is required. Data type: string.
  - **Example**

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

- If the DefenseType parameter is set to **tamperproof**, the value of the Content parameter contains the following parameters:
  - **uri**: the URL that requires protection. Data type: string. This parameter is required. Data type: string.
  - **name**: the name of the rule. This parameter is required. Data type: string.

- **status**: the status of the rule. This parameter is optional. Data type: integer. Valid values:
  - **0**: disabled. This is the default value.
  - **1**: enabled.
- **Example**

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

- If the DefenseType parameter is set to **dlp**, the value of the Content parameter contains the following parameters:
  - **name**: the name of the rule. This parameter is required. Data type: string.
  - **conditions**: the matching conditions, which are formulated in a JSON string. You can specify a maximum of two conditions. The two conditions use a logical AND. This parameter is required. Data type: array. The JSON string contains the following parameters:
    - **key**: the matching item. Valid values:
      - **0**: URL
      - **10**: sensitive data
      - **11**: HTTP status code
    - **operation**: the matching logic. This value is fixed as **1**, which indicates the INCLUDES logical relation.
    - **value**: the matching value, which is formulated in a JSON string. You can specify multiple values. The JSON string contains the following parameters:
      - **v**: This parameter takes effect only when the **key** parameter is set to **0** or **11**.
        - URL: If the `key` parameter is set to 0, the value of the v parameter is a URL.
        - HTTP status code: If the `key` parameter is set to 11, the valid values of the v parameter are **400**,**401**,**402**,**403**,**404**,**405 to 499**,**500**,**501**,**502**,**503**,**504**, and **505 to 599**.
      - **k**: This parameter takes effect only when the **key** parameter is set to **10**. Valid values:
        - **100**: ID card numbers
        - **101**: credit card numbers
        - **102**: phone numbers
        - **103**: default sensitive words
  - **action**: the action that is performed after the rule is matched
    - **3**: generates alerts.
    - **10**: filters sensitive data. This action takes effect only when the `key` parameter is set to 10.
    - **11**: returns the built-in block page of the system. This action takes effect only when the `key` parameter is set to 11.

- Example

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

- If the DefenseType parameter is set to **ng_account**, the value of the Content parameter contains the following parameters:
  - **domain**: the domain name that is protected by WAF. This parameter is required. Data type: string.
  - **method**: the method of the requests. This parameter is required. Data type: string. Valid values: POST, GET, PUT, and DELETE. You can specify multiple request methods. Separate the request methods with commas (,).
  - **url_path**: the URL path in the requests that are detected. The path must start with a forward slash (/). This parameter is required. Data type: string.
  - **account_left**: the account. This parameter is required. Data type: string.
  - **password_left**: the password. This parameter is optional. Data type: string.
  - **action**: the action that is performed after the rule is matched. This parameter is required. Data type: string. Valid values:
    - **monitor**: generates alerts.
    - **block**: blocks requests.
  - Example

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

- If the DefenseType parameter is set to **bot_crawler**, the value of the Content parameter contains the following parameters:
  - **Status**: the status of the rule. This parameter is required. Data type: integer. Valid values:
    - 0: disabled
    - 1: enabled
  - **Version**: the version of the rule. This parameter is required. Data type: integer.

- **Content**: the details of the rule. This parameter is required. Data type: string. The value is a JSON string that contains the following parameters:
  - **name**: the name of the rule. This parameter is required. Data type: string.
  - **conditions**: the condition for URL paths that are protected. This parameter is optional. Data type: array. If the DefenseType parameter is set to bot_crawler, the value of the conditions parameter is fixed as empty, which indicates that all URL paths are protected.
  - **expressions**: the conditional expression of the rule. The expression represents all the conditions of the rule. This parameter is required. Data type: array.
  - **bypassTags**: the protection module that does not detect requests. This parameter is required. Data type: string. If the DefenseType parameter is set to bot_crawler, the value of the bypassTags parameter is fixed as **antibot**, which indicates the bot management module.
  - **tags**: the protection module to which the rule belongs. This parameter is required. Data type: array. If the DefenseType parameter is set to bot_crawler, the value of the tags parameter is fixed as `["antibot"]`, which indicates the bot management module.
- **RuleId**: the ID of the rule. This parameter is required. Data type: integer.
- **Time**: the UNIX timestamp of when the rule was last modified. Unit: seconds. This parameter is required. Data type: string.
- **Example**

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

- If the DefenseType parameter is set to **bot_intelligence**, the value of the Content parameter contains the following parameters:
  - **Status**: the status of the rule. This parameter is required. Data type: integer. Valid values:
    - 0: disabled
    - 1: enabled
  - **Version**: the version of the rule. This parameter is required. Data type: integer.

- **Content**: the details of the rule. This parameter is required. Data type: string. The value is a JSON string that contains the following parameters:
  - **name**: the name of the rule. This parameter is required. Data type: string.
  - **action**: the action that is performed after the rule is matched. This parameter is required. Data type: string. Valid values:
    - **monitor**: monitors requests.
    - **captcha**: performs slider CAPTCHA verification.
    - **captcha_strict**: performs strict slider CAPTCHA verification.
    - **js**: performs JavaScript verification.
    - **block**: blocks requests.
  - **urlList**: the URL path that requires protection. You can specify up to 10 URL paths. This parameter is required. Data type: array. The value is a JSON string that contains the following parameters:
    - **mode**: the matching method. This parameter is required. Data type: string. This parameter specifies a URL path in combination with the **url** parameter. Valid values: **eq** (exact match), **prefix-match** (prefix match), and **regex** (regular expression match).
    - **url**: the keyword of the URL path. The path must start with a forward slash (/). This parameter is required. Data type: string.
  - **keyType**: the type of the intelligence library. Valid values: **IP** (IP address library) and **ua** (fingerprint library).
- **RuleId**: the ID of the rule. This parameter is required. Data type: integer.
- **Time**: the UNIX timestamp of when the rule was last modified. Unit: seconds. This parameter is required. Data type: string.
- **Example**

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

- If the DefenseType parameter is set to **antifraud**, the value of the Content parameter contains the following parameters:
  - **uri**: the requested URL. This parameter is required. Data type: string.

- **Example**

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

- If the DefenseType parameter is set to **antifraud_js**, the value of the Content parameter contains the following parameters:
  - **uri**: the URL path of the web page into which the JavaScript plug-in for data risk control is inserted. The path must start with a forward slash (/). The system inserts the JavaScript plug-in into all the pages in the specified URL path. This parameter is required. Data type: string.
  - **Example**

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

- If the DefenseType parameter is set to **bot_algorithm**, the value of the Content parameter contains the following parameters:
  - **Status**: the status of the rule. This parameter is required. Data type: integer. Valid values:
    - 0: disabled
    - 1: enabled
  - **Version**: the version of the rule. This parameter is required. Data type: integer.
  - **Content**: the details of the rule. This parameter is required. Data type: string. The value is a JSON string that contains the following parameters:
    - **name**: the name of the rule. This parameter is required. Data type: string.
    - **timeInterval**: the interval of detection. This parameter is required. Data type: integer. Valid values: 30, 60, 120, 300, and 600. Unit: seconds.
    - **action**: the action that is performed after the rule is matched. This parameter is required. Data type: string. Valid values:
      - **monitor**: monitors requests.
      - **captcha**: performs slider CAPTCHA verification.
      - **js**: performs JavaScript verification.
      - **block**: blocks requests. If you set the parameter to block, you must also specify the **blocktime** parameter.
    - **blocktime**: the period during which requests are blocked. This parameter is optional. Data type: integer. Valid values: 1 to 600. Unit: minutes.

- **algorithmName**: the name of the algorithm. This parameter is required. Data type: string. Valid values:
  - **RR**: the algorithm that is used to identify specific resource crawlers
  - **PR**: the algorithm that is used to identify specific path crawlers
  - **DPR**: the algorithm that is used to identify parameter round-robin crawlers
  - **SR**: the algorithm that is used to identify dynamic IP address crawlers
  - **IND**: the algorithm that is used to identify proxy device crawlers
  - **Periodicity**: the algorithm that is used to identify periodic crawlers
- **config**: the configuration of the algorithm, which is formulated in a JSON string. This parameter is required. Data type: string. The parameters that are contained in the JSON string vary based on the value of the **algorithmName** parameter.
  - If you set the algorithmName parameter to **RR**, the value of the config parameter contains the following parameters:
    - **resourceType**: the type of the requested resource. This parameter is optional. Data type: integer. Valid values:
      - **1**: dynamic resources.
      - **2**: static resources.
      - **-1**: custom resources. In this case, you must also use the **extensions** parameter to specify resource suffixes in a string. Separate suffixes with commas (,). Example: `css,jpg,xls`.
    - **minRequestCountPerIp**: the minimum number of requests from an IP address. The system detects an IP address only when the number of requests from this IP address is greater than or equal to the value of this parameter. This parameter is required. Data type: integer. Valid values: 5 to 10000.
    - **minRatio**: the threshold for the proportion of requests that access specified types of resources to requests that are initiated from an IP address. This threshold is used to determine whether risks exist. If an actual proportion is greater than the threshold, risks exist. This parameter is required. Data type: float. Valid values: 0.01 to 1.

- If you set the algorithmName parameter to **PR**, the value of the config parameter contains the following parameters:
  - **keyPathConfiguration**: the requested URL path. You can specify a maximum of 10 URL paths. This parameter is required only when the algorithmName parameter is set to PR. This parameter is optional. Data type: array. This parameter is a JSON string that contains the following parameters:
    - **method**: the request method. This parameter is required. Data type: string. Valid values: **POST**, **GET**, **PUT**, **DELETE**, **HEAD**, and **OPTIONS**.
    - **url**: the keyword of the URL path. The path must start with a forward slash (/). This parameter is required. Data type: string.
    - **matchType**: the matching method. This parameter specifies a requested URL path in combination with the **url** parameter. This parameter is required. Data type: string. Valid values: **all** (exact match), **prefix** (prefix match), and **regex** (regular expression match).
  - **minRequestCountPerIp**: the minimum number of requests from an IP address. The system detects an IP address only when the number of requests from this IP address is greater than or equal to the value of this parameter. This parameter is required. Data type: integer. Valid values: 5 to 10000.
  - **minRatio**: the threshold for the proportion of requests that access specified URL paths to requests that are initiated from an IP address. This threshold is used to determine whether risks exist. If an actual proportion is greater than the threshold, risks exist. This parameter is required. Data type: float. Valid values: 0.01 to 1.
- If you set the algorithmName parameter to **DPR**, the value of the config parameter contains the following parameters:
  - **method**: the request method. This parameter is required. Data type: string. Valid values: **POST**, **GET**, **PUT**, **DELETE**, **HEAD**, and **OPTIONS**.
  - **urlPattern**: the path of key parameters. The path must start with a forward slash (/). This parameter is required. Data type: string. You can specify multiple key parameters and enclose each parameter with a pair of braces {}. Example: `/company/{}/{}/{}/user.php?uid={}`.
  - **minRequestCountPerIp**: the minimum number of requests from an IP address. The system detects an IP address only when the number of requests from this IP address is greater than or equal to the value of this parameter. This parameter is required. Data type: integer. Valid values: 5 to 10000.
  - **minRatio**: the threshold for the proportion of requests that use specified key parameters to requests that are initiated from an IP address. This threshold is used to determine whether risks exist. If an actual proportion is greater than the threshold, risks exist. This parameter is required. Data type: float. Valid values: 0.01 to 1.

- If you set the algorithmName parameter to **SR**, the value of the config parameter contains the following parameters:
  - **maxRequestCountPerSrSession**: the minimum number of requests in each session. If the number of requests in a single session is smaller than the value of this parameter, the session is considered abnormal. This parameter is required. Data type: integer. Valid values: 1 to 8.
  - **minSrSessionCountPerIp**: the threshold for the number of abnormal sessions in the requests that are initiated from an IP address. The threshold is used to determine whether risks exist. If an actual number is greater than the threshold, risks exist. This parameter is required. Data type: integer. Valid values: 5 to 300.
- If you set the algorithmName parameter to **IND**, the value of the config parameter contains the following parameters:
  - **minIpCount**: the threshold for the number of IP addresses that the Wi-Fi connected device accesses. This parameter specifies the condition that is used to determine malicious devices. If an actual number is greater than the threshold, risks exist. This parameter is required. Data type: integer. Valid values: 5 to 500.
  - **keyPathConfiguration**: the requested URL path. You can specify a maximum of 10 URL paths. This parameter is optional. Data type: array. This parameter is a JSON string that contains the following parameters:
    - **method**: the request method. This parameter is required. Data type: string. Valid values: **POST**, **GET**, **PUT**, **DELETE**, **HEAD**, and **OPTIONS**.
    - **url**: the keyword of the URL path. The path must start with a forward slash (/). This parameter is required. Data type: string.
    - **matchType**: the matching method. This parameter specifies a requested URL path in combination with the **url** parameter. This parameter is required. Data type: string. Valid values: **all** (exact match), **prefix** (prefix match), and **regex** (regular expression match).
- If you set the algorithmName parameter to **Periodicity**, the value of the config parameter contains the following parameters:
  - **minRequestCountPerIp**: the minimum number of requests from an IP address. The system detects an IP address only when the number of requests from this IP address is greater than or equal to the value of this parameter. This parameter is required. Data type: integer. Valid values: 5 to 10000.
  - **level**: the risk level, which is the extent of obviousness of periodic access from IP addresses. This parameter is required. Data type: integer. Valid values:
    - **0**: obvious
    - **1**: moderate
    - **2**: weak

- **RuleId**: the ID of the rule. This parameter is required. Data type: integer.
- **Time**: the UNIX timestamp of when the rule was last modified. Unit: seconds. This parameter is required. Data type: string.

- **Example**

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

- If the DefenseType parameter is set to **bot_wxbb_pkg**, the value of the Content parameter contains the following parameters:
  - **Version**: the version of the rule. This parameter is required. Data type: integer.
  - **Content**: the details of the rule. This parameter is required. Data type: string. The value is a JSON string that contains the following parameters:
    - **name**: the name of the rule. This parameter is required. Data type: string.
    - **action**: the action that is performed after the rule is matched. This parameter is required. Data type: string. Valid values:
      - **test**: monitors requests.
      - **close**: blocks requests.
    - **nameList**: the version information of valid package. You can specify the version information for a maximum of five valid packages. This parameter is required. Data type: array. The value is a JSON string that contains the following parameters:
      - **name**: the name of the valid package. This parameter is required. Data type: string.
      - **signList**: the signature for the package. You can specify a maximum of 15 signatures. Separate them with commas (,). This parameter is required. Data type: array.
  - **RuleId**: the ID of the rule. This parameter is required. Data type: integer.
  - **Time**: the UNIX timestamp of when the rule was last modified. Unit: seconds. This parameter is required. Data type: string.

- Example

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

- If the DefenseType parameter is set to **bot_wxbb**, the value of the Content parameter contains the following parameters:
  - **Version**: the version of the rule. This parameter is required. Data type: integer.
  - **Content**: the details of the rule. This parameter is required. Data type: string. The value is a JSON string that contains the following parameters:
    - **name**: the name of the rule. This parameter is required. Data type: string.
    - **uri**: the URL path that requires protection. The path must start with a forward slash (/). This parameter is required. Data type: string.
    - **matchType**: the matching method. This parameter is required. Data type: string. Valid values: **all** (exact match), **prefix** (prefix match), **regex** (regular expression match).
    - **arg**: the included parameters. This parameter specifies a URL path in combination with the **matchType** parameter. This parameter is required. Data type: string.
    - **action**: the action that is performed after the rule is matched. This parameter is required. Data type: string. Valid values:
      - **test**: monitors requests.
      - **close**: blocks requests.
    - **wxbbVmpFieldType**: the type of the signature field. This parameter is optional. Data type: integer. If no custom signature fields are added to the rule, this parameter is not returned. Valid values:
      - **0**: header
      - **1**: parameter
      - **2**: cookie
    - **wxbbVmpFieldValue**: the value of the signature field. This parameter is optional. Data type: string. If no custom signature fields are added to the rule, this parameter is not returned.
    - **blockInvalidSign**: specifies whether to take actions on an invalid signature. This parameter is required. Data type: Boolean.
    - **blockProxy**: specifies whether to take actions on a proxy. This parameter is required. Data type: Boolean.
    - **blockSimulator**: specifies whether to take actions on a simulator. This parameter is required. Data type: Boolean.
  - **RuleId**: the ID of the rule. This parameter is required. Data type: integer.

- **Time**: the UNIX timestamp of when the rule was last modified. Unit: seconds. This parameter is required. Data type: string.
- **Example**

```
{
    "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
}
```

- If the DefenseType parameter is set to **ac_blacklist**, the value of the Content parameter contains the following parameters:
  - **empty**: specifies whether the blacklist is empty. This parameter is required. Data type: Boolean.
  - **remoteAddr**: the IP addresses in the blacklist. This parameter is required. Data type: array.
  - **area**: the region blocking rule, which is formulated in a JSON string that contains the countryCodes, regionCodes, and not parameters. (The not parameter specifies whether to allow access.) This parameter is required. Data type: string. The blocked countries and regions are returned as codes. We recommend that you go to the console to view the blocked countries and regions.
  - **Example**

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

- If the DefenseType parameter is set to **ac_highfreq**, the value of the Content parameter contains the following parameters:
  - **interval**: the interval of detection. This parameter is required. Data type: integer. Valid values: 5 to 1800. Unit: seconds.
  - **ttl**: the period during which an IP address is blocked. Data type: integer. Valid values: 60 to 86400. Unit: seconds.
  - **count**: the threshold for the number of web attacks initiated from an IP address. If the number of attacks initiated from an IP address during the specified period is greater than the threshold, the IP address is blocked. This parameter is required. Data type: integer. Valid values: 2 to 50000.

- Example

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

- If the DefenseType parameter is set to **ac_dirscan**, the value of the Content parameter contains the following parameters:
  - **interval**: the interval of detection. This parameter is required. Data type: integer. Valid values: 5 to 1800. Unit: seconds.
  - **ttl**: the period during which an IP address is blocked. This parameter is required. Data type: integer. Unit: seconds.
  - **count**: the maximum number of requests allowed from an IP address. This parameter is required. Data type: integer. Valid values: 2 to 50000.
  - **weight**: the proportion of requests with HTTP 404 status codes to all requests. This parameter is required. Data type: float. Valid values: `(0,1]`.
  - **uriNum**: the maximum number of paths that can be scanned. This parameter is required. Data type: integer. Valid values: 2 to 50000.
  - Example

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

- If the DefenseType parameter is set to **ac_custom**, the value of the Content parameter varies based on the **scene** parameter.
  - If the **scene** parameter is set to **custom_acl** to configure an ACL rule, the value of the Content parameter contains the following parameters:
    - **name**: the name of the rule. This parameter is required. Data type: string.
    - **scene**: the type of the protection policy. This parameter is required. Data type: string. If an ACL rule is configured, the value of this parameter is fixed as **custom_acl**.
    - **action**: the action that is performed after the rule is matched. This parameter is required. Data type: string. Valid values:
      - **monitor**: monitors requests.
      - **captcha**: performs slider CAPTCHA verification.
      - **captcha_strict**: performs strict slider CAPTCHA verification.
      - **js**: performs JavaScript verification.
      - **block**: blocks requests.

- **conditions**: the matching condition. This parameter is required. Data type: array. The value is a JSON string that contains the following parameters:
  - **key**: the matching item. Valid values: **URL**, **IP**, **Referer**, **User-Agent**, **Params**, **Cookie**, **Content-Type**, **Content-Length**, **X-Forwarded-For**, **Post-Body**, **Http-Method**, **Header**, and **URLPath**.
  - **opCode**: the logical relation. Valid values:
    - **11**: equals
    - **10**: does not equal
    - **41**: equals one of multiple values
    - **50**: does not equal any value
    - **1**: includes
    - **0**: does not include
    - **51**: includes one of multiple values
    - **52**: does not include any value
    - **82**: exists
    - **2**: does not exist
    - **21**: length equal to
    - **22**: length greater than
    - **20**: length less than
    - **60**: does not match a regular expression
    - **61**: matches a regular expression
    - **72**: matches a prefix
    - **81**: matches a suffix
    - **80**: empty content
  - **values**: the matching value. You can specify this parameter based on your business requirements. Data type: string.
  - **contain**: the logical relation. The valid values of this parameter are the same as those of the **opCode** parameter.
  - **opValue**: the description of the abbreviated logical relation. For more information, see the description of the **opCode** parameter.
  - **pattern**: the description of the abbreviated logical relation. The valid values of this parameter are the same as those of the **opValue** parameter.
- **expressions**: the conditional expression of the rule. The expression represents all the conditions of the rule. This parameter is required. Data type: array.

- **Example**

```
        {
            "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"
        }
```

- If the **scene** parameter is set to **custom_cc** to configure an HTTP flood protection rule, the value of the Content parameter contains the following parameters:
  - **name**: the name of the rule. This parameter is required. Data type: string.
  - **scene**: the type of the protection policy. This parameter is required. Data type: string. If an HTTP flood protection rule is configured, the value of this parameter is fixed as **custom_cc**.

- **conditions**: the matching condition. This parameter is required. Data type: array. The value is a JSON string that contains the following parameters:
  - **key**: the matching item. Valid values: **URL**, **IP**, **Referer**, **User-Agent**, **Params**, **Cookie**, **Content-Type**, **Content-Length**, **X-Forwarded-For**, **Post-Body**, **Http-Method**, **Header**, and **URLPath**.
  - **opCode**: the logical relation. Valid values:
    - **11**: equals
    - **10**: does not equal
    - **41**: equals one of multiple values
    - **50**: does not equal any value
    - **1**: includes
    - **0**: does not include
    - **51**: includes one of multiple values
    - **52**: does not include any value
    - **82**: exists
    - **2**: does not exist
    - **21**: length equal to
    - **22**: length greater than
    - **20**: length less than
    - **60**: does not match a regular expression
    - **61**: matches a regular expression
    - **72**: matches a prefix
    - **81**: matches a suffix
    - **80**: empty content
  - **values**: the matching value. You can specify this parameter based on your business requirements. Data type: string.
  - **contain**: the logical relation. The valid values of this parameter are the same as those of the **opCode** parameter.
  - **opValue**: the description of the abbreviated logical relation. For more information, see the description of the **opCode** parameter.
  - **pattern**: the description of the abbreviated logical relation. The valid values of this parameter are the same as those of the **opValue** parameter.
- **expressions**: the conditional expression of the rule. The expression represents all the conditions of the rule. This parameter is required. Data type: array.
- **action**: the action that is performed after the rule is matched. This parameter is required. Data type: string. Valid values:
  - **monitor**: monitors requests.
  - **captcha**: performs slider CAPTCHA verification.
  - **captcha_strict**: performs strict slider CAPTCHA verification.
  - **js**: performs JavaScript verification.
  - **block**: blocks requests.

- **ratelimit**: the maximum rate of requests from an object. This parameter is required. Data type: JSON string. The value is a JSON string that contains the following parameters:
  - **target**: the type of the object from which the request rate is measured. This parameter is required. Data type: string. Valid values:
    - **remote_addr**: IP addresses.
    - **cookie.acw_tc**: sessions.
    - **queryarg**: custom parameters. If you choose to use custom parameters, you must specify the name of the custom parameter in the **subkey** parameter.
    - **cookie**: custom cookies. If you choose to use custom cookies, you must specify the cookie content in the **subkey** parameter.
    - **header**: custom headers. If you choose to use custom headers, you must specify the header content in the **subkey** parameter.
  - **subkey**: This parameter is required only when the **target** parameter is set to **cookie**, **header**, or **queryarg**. The **subkey** parameter is optional. Data type: string.
  - **interval**: the period for measuring the number of requests from the specified object. This parameter must be used together with the **threshold** parameter. This parameter is required. Data type: integer. Unit: seconds.
  - **threshold**: the maximum number of requests that are allowed from an individual object during the specified period. This parameter is required. Data type: integer.
  - **status**: the frequency of an HTTP status code. This parameter is optional. Data type: JSON string. The value is a JSON string that contains the following parameters:
    - **code**: the HTTP status code. This parameter is required. Data type: integer.
    - **count**: the threshold for the number of times that the specified HTTP status code is returned. The threshold is used to determine whether a rule is matched. If an actual number is greater than the threshold, the rule specified by the name parameter is matched. This parameter is optional. Data type: integer. Valid values: 1 to 999999999. You can set the **count** or **ratio** parameter. You cannot set both parameters at the same time.
    - **ratio**: the threshold for the percentage of times that the specified HTTP status code is returned. The threshold is used to determine whether a rule is matched. If an actual percentage is greater than the threshold, the rule specified by the name parameter is matched. This parameter is optional. Data type: integer. Valid values: 1 to 100. You can set the **count** or **ratio** parameter. You cannot set both parameters at the same time.
  - **scope**: the scope in which the settings take effect. This parameter is required. Data type: string. Valid values:
    - **rule**: the objects that match the specified conditions
    - **domain**: the domain names to which the rule is applied
  - **ttl**: the period during which the specified action is performed. This parameter is required. Data type: integer. Valid values: 60 to 86400. Unit: seconds.

- **Example**

```
        {
            "name":"HTTP flood protection rule",
            "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
            }
        }
```

- If the DefenseType parameter is set to **whitelist**, the value of the Content parameter contains the following parameters:
  - **name**: the name of the rule. This parameter is required. Data type: string.
  - **tags**: the protection module that skips detection. You can specify multiple modules. This parameter is required. Data type: array. Valid values:
    - **waf**: website whitelist
    - **cc**: HTTP flood protection
    - **customrule**: custom protection policy
    - **blacklist**: IP address blacklist
    - **antiscan**: scan protection
    - **regular**: protection rules engine
    - **deeplearning**: deep learning engine
    - **antifraud**: data risk control
    - **dlp**: data leak prevention
    - **tamperproof**: website tamper-proofing
    - **bot_intelligence**: bot threat intelligence
    - **bot_algorithm**: intelligent algorithm
    - **bot_wxbb**: app protection
  - **bypassTags**: the protection module that does not detect requests. This parameter is required. Data type: string.
  - **origin**: the source of the whitelist rule. This parameter is optional. Data type: string. The value is fixed as **ai**, which indicates that the whitelist rules are automatically added by the intelligent rule hosting feature. If the parameter is not returned, the whitelist rules include the rules that you manually added and the rules that are automatically added by the intelligent rule hosting feature.

- **conditions**: the matching condition. This parameter is required. Data type: array. The value is a JSON string that contains the following parameters:
  - **key**: the matching item. Valid values: **URL**, **IP**, **Referer**, **User-Agent**, **Params**, **Cookie**, **Content-Type**, **Content-Length**, **X-Forwarded-For**, **Post-Body**, **Http-Method**, **Header**, and **URLPath**.
  - **opCode**: the logical relation. Valid values:
    - **11**: equals
    - **10**: does not equal
    - **41**: equals one of multiple values
    - **50**: does not equal any value
    - **1**: includes
    - **0**: does not include
    - **51**: includes one of multiple values
    - **52**: does not include any value
    - **82**: exists
    - **2**: does not exist
    - **21**: length equal to
    - **22**: length greater than
    - **20**: length less than
    - **60**: does not match a regular expression
    - **61**: matches a regular expression
    - **72**: matches a prefix
    - **81**: matches a suffix
    - **80**: empty content
  - **values**: the matching value. You can specify this parameter based on your business requirements. Data type: string.
  - **contain**: the logical relation. The valid values of this parameter are the same as those of the **opCode** parameter.
  - **opValue**: the description of the abbreviated logical relation. For more information, see the description of the **opCode** parameter.
  - **pattern**: the description of the abbreviated logical relation. The valid values of this parameter are the same as those of the **opValue** parameter.
- **expressions**: the conditional expression of the rule. The expression represents all the conditions of the rule. This parameter is required. Data type: array.

- **Example**

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

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeProtectionModuleRules
&InstanceId=waf_elasticity-cn-0xldbqt****
&Domain=www.example.com
&DefenseType=ac_highfreq
&<Common request parameters>
```

Sample success responses

`XML` format

```
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` format

```
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"
}
```

Error codes

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

6.7. ModifyProtectionModuleRule

Modifies a rule of a specific WAF protection module, such as the web intrusion prevention, data security, advanced protection, bot management, access control or throttling, or website whitelist module.

Usage notes

You can call the ModifyProtectionModuleRule operation to modify a rule of a specific WAF protection module. The protection modules include web intrusion prevention, data security, advanced protection, bot management, access control or throttling, and website whitelist. You can set the **DefenseType** parameter to specify the protection module. For more information about the values of this parameter, see the description of the **DefenseType** parameter.

QPS limits

You can call this operation up to 10 times per second per account. If the number of the calls per second exceeds the limit, throttling is triggered. As a result, your business may be affected. We recommend that you take note of the limit when you call this operation.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyProtectionModuleRule	The operation that you want to perform. Set the value to **ModifyProtectionModuleRule**
Domain	String	Yes	www.example.com	The domain name for which you want to modify the rule. **Note** You can call the DescribeDomainNames operation to query the domain names that are protected by WAF.
DefenseType	String	Yes	ac_custom	The protection module whose rules you want to modify. Valid values: • **tamperproof**: website tamper-proofing • **dlp**: data leak prevention • **ng_account**: account security • **bot_intelligence**: bot threat intelligence • **antifraud**: data risk control • **antifraud_js**: configuration of a webpage into which you want to insert a JavaScript plug-in for data risk control • **bot_algorithm**: intelligent algorithm for the bot management module • **bot_wxbb_pkg**: version protection for the app protection module • **bot_wxbb**: path protection for the app protection module • **ac_blacklist**: IP address blacklist • **ac_highfreq**: blocking configuration of IP addresses that initiate high-frequency web attacks • **ac_dirscan**: scan protection • **ac_custom**: custom protection policies • **whitelist**: website whitelist

Parameter	Type	Required	Example	Description
Rule	String	Yes	null	The configurations of the rule. The value is a string that consists of a JSON struct. The JSON struct contains multiple parameters. **Note** The parameters that are contained in the string vary based on the protection module, which is specified by the **DefenseType** parameter. For more information, see the "Description of the Rule parameter" section of this topic.
RuleId	Long	Yes	369998	The ID of the rule that you want to modify. **Note** You can call the DescribeProtectionModuleRules operation to query the IDs of existing rules.
LockVersion	Long	Yes	2	The version of the rule that you want to modify. **Note** You can call the DescribeProtectionModuleRules operation to query the versions of existing rules.
InstanceId	String	Yes	waf-cn-0xldbqt****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.

Description of the Rule parameter

- If the DefenseType parameter is set to **tamperproof**, the value of the Rule parameter consists of the following parameters:
  - **uri**: the URL that you want to protect. This parameter is required. Data type: string.
  - **name**: the name of the rule. This parameter is required. Data type: string.
  - **status**: the status of the rule. This parameter is optional. Data type: integer. Valid values:
    - **0**: disables the rule. This is the default value.
    - **1**: enables the rule.
  - **Example**

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

- If the DefenseType parameter is set to **dlp**, the value of the Rule parameter consists of the following parameters:
  - **name**: the name of the rule. This parameter is required. Data type: string.
  - **conditions**: the conditions based on which WAF searches for and protects sensitive data. You can specify a maximum of two conditions. The two conditions are specified as a JSON string and must be in an AND logical relation. This parameter is required. Data type: array. The JSON string consists of the following parameters:
    - **key**: the match item. Valid values:
      - **0**: URL
      - **10**: sensitive data
      - **11**: HTTP status code

      > **Note** You cannot specify HTTP status codes (**11**) and sensitive data (**10**) as the match items in the **conditions** parameter at the same time.

    - **operation**: the match logic. Set the value to **1**, which indicates the INCLUDES logical relation.
    - **value**: the match value, which is formulated in a JSON string. You can specify multiple values. The JSON string consists of the following parameters:
      - **v**: This parameter is valid only when the **key** parameter is set to **0** or **11**.
        - URL: If the `key` parameter is set to 0, the value of the v parameter is a URL.
        - HTTP status code: If the `key` parameter is set to 11, the valid values of the v parameter are **400**,**401**,**402**,**403**,**404**,**405 to 499**,**500**,**501**,**502**,**503**,**504**, and **505 to 599**.
      - **k**: This parameter is valid only when the **key** parameter is set to **10**. Valid values:
        - **100**: ID card numbers
        - **101**: credit card numbers
        - **102**: phone numbers
        - **103**: default sensitive words

- **action**: the action that is performed after the rule is matched
  - **3**: generates alerts.
  - **10**: filters sensitive data. This action is valid only when the `key` parameter is set to 10.
  - **11**: returns the built-in block page of the system. This action is valid only when the `key` parameter is set to 11.
- **Example**

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

- If the DefenseType parameter is set to **ng_account**, the value of the Rule parameter consists of the following parameters:
  - **url_path**: the URL path in the requests that are detected. The path must start with a forward slash (/). This parameter is required. Data type: string.
  - **method**: the method of the requests that are detected. This parameter is required. Data type: string. Valid values: POST, GET, PUT, and DELETE. You can specify multiple request methods. Separate the request methods with commas (,).
  - **account_left**: the account. This parameter is required. Data type: string.
  - **password_left**: the password. This parameter is optional. Data type: string.
  - **action**: the action that is performed after the rule is matched. This parameter is required. Data type: string. Valid values:
    - **monitor**: generates alerts.
    - **block**: blocks requests.
  - **Example**

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

- If the DefenseType parameter is set to **bot_intelligence**, the value of the Rule parameter consists of the following parameters:
  - **name**: the name of the rule, which must match the ID of the rule (**RuleId**). This parameter is required. Data type: string.

- **urlList**: the URL paths that you want to protect. You can specify a maximum of 10 protection URL paths. Data type: array. The value is a JSON string that consists of the following parameters:
  - **mode**: the match method. This parameter specifies a URL path in combination with the **url** parameter. This parameter is required. Data type: string. Valid values: **eq** (exact match), **prefix-match** (prefix match), and **regex** (regular expression match).
  - **url**: the keyword of the URL path. The path must start with a forward slash (/). This parameter is required. Data type: string.
- **action**: the action that is performed after the rule is matched. This parameter is required. Data type: string. Valid values:
  - **monitor**: monitors requests.
  - **captcha**: performs common slider CAPTCHA verification.
  - **captcha_strict**: performs strict slider CAPTCHA verification.
  - **js**: performs JavaScript verification.
  - **block**: blocks requests.
- **status**: the status of the rule. This parameter is required. Data type: integer. Valid values:
  - **0**: disables the rule.
  - **1**: enables the rule.
- **Example**

```
{
    "urlList":[
        {"mode":"prefix-match","url":"/indexa"},
        {"mode":"regex","url":"/"},
        {"mode":"eq","url":"/"}],
    "name":"IDC IP Address Library-Tencent Cloud",
    "action":"captcha_strict",
    "status":1
}
```

- If the DefenseType parameter is set to **bot_algorithm**, the value of the Rule parameter consists of the following parameters:
  - **name**: the name of the rule. This parameter is required. Data type: string.
  - **algorithmName**: the name of the algorithm. This parameter is required. Data type: string. Valid values:
    - **RR**: the algorithm that is used to identify special resource crawlers
    - **PR**: the algorithm that is used to identify specific path crawlers
    - **DPR**: the algorithm that is used to identify parameter round-robin crawlers
    - **SR**: the algorithm that is used to identify dynamic IP address crawlers
    - **IND**: the algorithm that is used to identify proxy device crawlers
    - **Periodicity**: the algorithm that is used to identify periodic crawlers
  - **timeInterval**: the interval of detection. This parameter is required. Data type: integer. Valid values: 30, 60, 120, 300, and 600. Unit: seconds.

- **action**: the action that is performed after the rule is matched. This parameter is required. Data type: string. Valid values:
  - **monitor**: monitors requests.
  - **captcha**: performs slider CAPTCHA verification.
  - **js**: performs JavaScript verification.
  - **block**: blocks requests. If you set the action parameter to block, you must also specify the **blocktime** parameter.
- **blocktime**: the period during which requests are blocked. This parameter is optional. Data type: integer. Valid values: 1 to 600. Unit: minutes.
- **config**: the configuration of the algorithm, which is formulated in a JSON string. This parameter is required. Data type: string. The parameters that are contained in the JSON string vary based on the value of the **algorithmName** parameter.
  - If you set the algorithmName parameter to **RR**, the value of the config parameter consists of the following parameters:
    - **resourceType**: the type of resource that is requested. This parameter is optional. Data type: integer. Valid values:
      - **1**: dynamic resources
      - **2**: static resources
      - **-1**: custom resources. In this case, you must also use the **extensions** parameter to specify resource suffixes in a string. Separate suffixes with commas (,). Example: `css,jpg,xls`
    - **minRequestCountPerIp**: the minimum number of requests from an IP address. WAF detects an IP address only when the number of requests from this IP address is greater than or equal to the value of this parameter. This parameter is required. Data type: integer. This parameter specifies the minimum number of access requests. Valid values: 5 to 10000.
    - **minRatio**: the threshold for the proportion of requests that access specified types of resources in requests that are initiated from an IP address. This threshold is used to determine whether risks exist. If an actual proportion is greater than the threshold, risks exist. This parameter is required. Data type: float. Valid values: 0.01 to 1.

- If you set the algorithmName parameter to **PR**, the value of the config parameter consists of the following parameters:
  - **keyPathConfiguration**: the requested URL paths. You can specify a maximum of 10 URL paths. This parameter is required only when the algorithmName parameter is set to PR. This parameter is optional. Data type: array. This parameter is a JSON string that consists of the following parameters:
    - **method**: the request method. This parameter is required. Data type: string. Valid values: **POST**, **GET**, **PUT**, **DELETE**, **HEAD**, and **OPTIONS**.
    - **url**: the keyword of the URL path. The path must start with a forward slash (/). This parameter is required. Data type: string.
    - **matchType**: the match method. This parameter specifies a requested URL path in combination with the **url** parameter. This parameter is required. Data type: string. Valid values: **all** (exact match), **prefix** (prefix match), and **regex** (regular expression match).
  - **minRequestCountPerIp**: the minimum number of requests from an IP address. WAF detects an IP address only when the number of requests from this IP address is greater than or equal to the value of this parameter. This parameter is required. Data type: integer. This parameter specifies the minimum number of access requests. Valid values: 5 to 10000.
  - **minRatio**: the threshold for the proportion of requests that access specified URL paths in requests that are initiated from an IP address. This threshold is used to determine whether risks exist. If an actual proportion is greater than the threshold, risks exist. This parameter is required. Data type: float. Valid values: 0.01 to 1.
- If you set the algorithmName parameter to **DPR**, the value of the config parameter consists of the following parameters:
  - **method**: the request method. This parameter is required. Data type: string. Valid values: **POST**, **GET**, **PUT**, **DELETE**, **HEAD**, and **OPTIONS**.
  - **urlPattern**: the path of key parameters. The path must start with a forward slash (/). This parameter is required. Data type: string. You can specify multiple key parameters and enclose each parameter with a pair of braces {}. Example: `/company/{}/{}/{}/user.php?uid={}`.
  - **minRequestCountPerIp**: the minimum number of requests from an IP address. WAF detects an IP address only when the number of requests from this IP address is greater than or equal to the value of this parameter. This parameter is required. Data type: integer. This parameter specifies the minimum number of access requests. Valid values: 5 to 10000.
  - **minRatio**: the threshold for the proportion of requests that use specified key parameters in requests that are initiated from an IP address. This threshold is used to determine whether risks exist. If an actual proportion is greater than the threshold, risks exist. This parameter is required. Data type: float. Valid values: 0.01 to 1.
- If you set the algorithmName parameter to **SR**, the value of the config parameter consists of the following parameters:
  - **maxRequestCountPerSrSession**: the minimum number of requests in each session. If the number of requests in a single session is smaller than the value of this parameter, the session is considered abnormal. This parameter is required. Data type: integer. Valid values: 1 to 8.
  - **minSrSessionCountPerIp**: the threshold for the number of abnormal sessions in the requests that are initiated from an IP address. The threshold is used to determine whether risks exist. If an actual number is greater than the threshold, risks exist. This parameter is required. Data type: integer. Valid values: 5 to 300.

- If you set the algorithmName parameter to **IND**, the value of the config parameter consists of the following parameters:
  - **minIpCount**: the threshold for the number of IP addresses that the Wi-Fi connected device accesses. This parameter specifies the condition that is used to identify malicious devices. If an actual number is greater than the threshold, risks exist. This parameter is required. Data type: integer. Valid values: 5 to 500.
  - **keyPathConfiguration**: the requested URL path. You can specify a maximum of 10 URL paths. This parameter is optional. Data type: array. This parameter is a JSON string that consists of the following parameters:
    - **method**: the request method. This parameter is required. Data type: string. Valid values: **POST**, **GET**, **PUT**, **DELETE**, **HEAD**, and **OPTIONS**.
    - **url**: the keyword of the URL path. The path must start with a forward slash (/). This parameter is required. Data type: string.
    - **matchType**: the match method. This parameter specifies a requested URL path in combination with the **url** parameter. This parameter is required. Data type: string. Valid values: **all** (exact match), **prefix** (prefix match), and **regex** (regular expression match).
- If you set the algorithmName parameter to **Periodicity**, the value of the config parameter consists of the following parameters:
  - **minRequestCountPerIp**: the minimum number of requests from an IP address. WAF detects an IP address only when the number of requests from this IP address is greater than or equal to the value of this parameter. This parameter is required. Data type: integer. This parameter specifies the minimum number of access requests. Valid values: 5 to 10000.
  - **level**: the risk level, which is the extent of obviousness of periodic access from IP addresses. This parameter is required. Data type: integer. Valid values:
    - **0**: obvious
    - **1**: moderate
    - **2**: weak

- **Example**

```
    {
        "name": "Crawler identification for proxy devices",
        "algorithmName":"IND",
        "timeInterval":"60",
        "action":"warn",
        "config":{
            "minIpCount":5,
            "keyPathConfiguration":[{"url":"/index","method":"GET","matchType":"prefix"
}]
        }
    }
```

- If the DefenseType parameter is set to **bot_wxbb_pkg**, the value of the Rule parameter consists of the following parameters:
  - **name**: the name of the rule. This parameter is required. Data type: string.

- **action**: the action that is performed after the rule is matched. This parameter is required. Data type: string. Valid values:
  - **test**: monitors requests.
  - **close**: blocks requests.
- **nameList**: the version information of valid packages. You can specify the version information for a maximum of five valid packages. This parameter is required. Data type: array. The value is a JSON string that consists of the following parameters:
  - **name**: the name of the valid package. This parameter is required. Data type: string.
  - **signList**: the signatures for the package. You can specify a maximum of 15 signatures. Separate them with commas (,). This parameter is required. Data type: array.
- **Example**

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

- If the DefenseType parameter is set to **bot_wxbb**, the value of the Rule parameter consists of the following parameters:
  - **name**: the name of the rule. This parameter is required. Data type: string.
  - **url**: the URL path that requires protection. The path must start with a forward slash (/). This parameter is required. Data type: string.
  - **matchType**: the match method. This parameter is required. Data type: string. Valid values: **all** (exact match), **prefix** (prefix match), **regex** (regular match).
  - **arg**: the included parameters. This parameter specifies a URL path in combination with the **matchType** parameter. This parameter is required. Data type: string.
  - **action**: the action that is performed after the rule is matched. This parameter is required. Data type: string. Valid values:
    - **test**: monitors requests.
    - **close**: blocks requests.
  - **hasTag**: specifies whether to add a custom signature field. This parameter s required. Data type: Boolean.
    - **true**: In this case, you must set the **wxbbVmpFieldType** and **wxbbVmpFieldValue** parameters to specify the type and value of the field.
    - **false**:

- **wxbbVmpFieldType**: the type of the signature field. This parameter is optional. Data type: integer. If you set the **hasTag** parameter to **true**, you must also specify this parameter. Valid values:
  - **0**: header
  - **1**: parameter
  - **2**: cookie
- **wxbbVmpFieldValue**: the value of the signature field. This parameter is optional. Data type: string. If you set the **hasTag** parameter to **true**, you must also specify this parameter.
- **blockInvalidSign**: specifies whether to take actions on an invalid signature. This parameter is required. Data type: integer. Set the value to **1**. The value 1 specifies that the default protection policy for path protection is enabled.
- **blockProxy**: specifies whether to take actions on a proxy. This parameter is optional. Data type: integer. Set the value to **1**. If you do not need to perform actions on the proxy, you can leave this parameter unspecified.
- **blockSimulator**: specifies whether to take actions on a simulator. This parameter is optional. Data type: integer. Set the value to **1**. If you do not need to perform actions on the simulator, you can leave this parameter unspecified.
- **Example**

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

- If the DefenseType parameter is set to **antifraud**, the value of the Rule parameter consists of the following parameters:
  - **uri**: the requested URL. This parameter is required. Data type: string.
  - **Example**

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

- If the DefenseType parameter is set to **antifraud_js**, the value of the Rule parameter consists of the following parameters:
  - **uri**: the URL path of the web page into which you want to insert the JavaScript plug-in for data risk control. The path must start with a forward slash (/). WAF inserts the JavaScript plug-in into all the web pages in the specified URL path. This parameter is required. Data type: string.

- Example

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

- If the DefenseType parameter is set to **ac_blacklist**, the value of the Rule parameter consists of the following parameters:
  - **remoteAddr**: the IP addresses in the blacklist. This parameter is optional. Data type: array. You can enter both IP addresses and CIDR blocks. Separate multiple IP addresses with commas (,). You can enter a maximum of 200 IP addresses. If you leave this parameter unspecified, WAF clears the blacklist.
  - **area**: the regions in the region-level IP address blacklist. This parameter is optional. Data type: array. This parameter is a string that consists of JSON arrays. Each element in a JSON array is a JSON struct that consists of the following fields:
    - **countryCodes**: the code of the country. This parameter is required. Data type: array. If you set this parameter to `["CN"]`, WAF blocks requests from administrative regions in China, and you must also specify the **regionCodes** parameter. If you set this parameter to a value other than `["CN"]`, WAF blocks requests from countries and areas outside China, and you do not need to specify the **regionCodes** parameter. You can call the DescribeProtectionModuleCodeConfig operation to query the codes of administrative regions inside China and the codes of countries and areas outside China.
    - **regionCodes**: the code of the administrative region inside China. This parameter is optional. Data type: array.
  - Example

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

- If the DefenseType parameter is set to **ac_highfreq**, the value of the Rule parameter consists of the following parameters:
  - **interval**: the interval of detection. This parameter is required. Data type: integer. Valid values: 5 to 1800. Unit: seconds.
  - **ttl**: the period during which an IP address is blocked. This parameter is required. Data type: integer. Valid values: 60 to 86400. Unit: seconds.
  - **count**: the threshold for the number of web attacks initiated from an IP address. If the number of attacks initiated from an IP address during the specified period is greater than the threshold, the IP address is blocked. This parameter is required. Data type: integer. Valid values: 2 to 50000.
  - **Example**

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

- If the DefenseType parameter is set to **ac_dirscan**, the value of the Rule parameter consists of the following parameters:
  - **interval**: the interval of detection. This parameter is required. Data type: integer. Valid values: 5 to 1800. Unit: seconds.
  - **ttl**: the period during which an IP address is blocked. This parameter is required. Data type: integer. Valid values: 60 to 86400. Unit: seconds.
  - **count**: the maximum number of requests allowed from an IP address. This parameter is required. Data type: integer. Valid values: 2 to 50000.
  - **weight**: the proportion of requests with HTTP 404 status codes in all requests. This parameter is required. Data type: float. Valid values: 0 to 1.
  - **uriNum**: the maximum number of paths that can be scanned. This parameter is required. Data type: integer. Valid values: 2 to 50000.
  - **Example**

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

- If the DefenseType parameter is set to **ac_custom**, the value of the Rule parameter varies based on the **scene** parameter.
  - To modify an ACL rule, set the **scene** parameter to **custom_acl**. The value of the Rule parameter consists of the following parameters:
    - **name**: the name of the rule. This parameter is required. Data type: string.
    - **scene**: the type of the protection policy. This parameter is required. Data type: string. If an ACL rule is configured, set the value to **custom_acl**.

- **action**: the action that is performed after the rule is matched. This parameter is required. Data type: string. Valid values:
  - **monitor**: monitors requests.
  - **captcha**: performs common slider CAPTCHA verification.
  - **captcha_strict**: performs strict slider CAPTCHA verification.
  - **js**: performs JavaScript verification.
  - **block**: blocks requests.
- **conditions**: the match condition. You can specify a maximum of five match conditions. This parameter is required. Data type: array. The value is a JSON string that consists of the following parameters:
  - **key**: the match item. Value values **URL**, **IP**, **Referer**, **User-Agent**, **Params**, **Cookie**, **Content-Type**, **Content-Length**, **X-Forwarded-For**, **Post-Body**, **Http-Method**, **Header**, and **URLPath**.
  - **opCode**: the logical operator. Valid values:
    - **0**: does not include or does not belong to
    - **1**: includes or belongs to
    - **2**: does not exist
    - **10**: does not equal
    - **11**: equals
    - **20**: length less than
    - **21**: length equal to
    - **22**: length greater than
    - **30**: value less than
    - **31**: value equal to
    - **32**: value greater than
  - **values**: the match value. You can specify this parameter based on your business requirements. Data type: string.

    > **Note** The valid values of the **opCode** and **values** parameters in the match conditions vary based on the **key** parameter. For more information about match conditions, see Fields in match conditions.

  - **Example**

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

- To modify an HTTP flood protection rule, set the **scene** parameter to **custom_acl**. The value of the Rule parameter consists of the following parameters:
  - **name**: the name of the rule. This parameter is required. Data type: string.

- **scene**: the type of the protection policy. This parameter is required. Data type: string. If an HTTP flood protection rule is configured, set the value to **custom_cc**.
- **conditions**: the match condition. You can specify a maximum of five match conditions. This parameter is required. Data type: array. The value is a JSON string that consists of the following parameters:
  - **key**: the match item. Value values: **URL**, **IP**, **Referer**, **User-Agent**, **Params**, **Cookie**, **Content-Type**, **Content-Length**, **X-Forwarded-For**, **Post-Body**, **Http-Method**, **Header**, and **URLPath**.
  - **opCode**: the logical operator. Valid values:
    - **0**: does not include or does not belong to
    - **1**: includes or belongs to
    - **2**: does not exist
    - **10**: does not equal
    - **11**: equals
    - **20**: length less than
    - **21**: length equal to
    - **22**: length greater than
    - **30**: value less than
    - **31**: value equal to
    - **32**: value greater than
  - **values**: the match value. You can specify this parameter based on your business requirements. Data type: string.

    > **Note** The valid values of the **opCode** and **values** parameters in the match conditions vary based on the **key** parameter.

- **action**: the action that is performed after the rule is matched. This parameter is required. Data type: string. Valid values:
  - **monitor**: monitors requests.
  - **captcha**: performs slider CAPTCHA verification.
  - **captcha_strict**: performs strict slider CAPTCHA verification.
  - **js**: performs JavaScript verification.
  - **block**: blocks requests.
- **ratelimit**: the maximum rate of requests from an object. This parameter is required. Data type: JSON string. The value is a JSON string that consists of the following parameters:

- **target**: the type of the object from which the request rate is measured. This parameter is required. Data type: string. Valid values:
  - **remote_addr**: IP addresses.
  - **cookie.acw_tc**: sessions.
  - **queryarg**: custom parameters. If you use custom parameters, you must specify the name of the custom parameter in the **subkey** parameter.
  - **cookie**: custom cookies. If you use custom cookies, you must specify the cookie content in the **subkey** parameter.
  - **header**: custom headers. If you use custom headers, you must specify the header content in the **subkey** parameter.
- **subkey**: This parameter is required only when you set the **target** parameter to **cookie**, **header**, or **queryarg**. The **subkey** parameter is optional. Data type: string.
- **interval**: the period for measuring the number of requests from the specified object. This parameter must be used together with the **threshold** parameter. This parameter is required. Data type: integer. Unit: seconds.
- **threshold**: the maximum number of requests that are allowed from an individual object during the specified period. This parameter is required. Data type: integer.
- **status**: the frequency of an HTTP status code. This parameter is optional. Data type: JSON string. The value is a JSON string that consists of the following parameters:
  - **code**: the HTTP status code. This parameter is required. Data type: integer.
  - **count**: the threshold for the number of times that the specified HTTP status code is returned. The threshold is used to determine whether a rule is matched. If an actual number is greater than the threshold, the rule specified by the name parameter is matched. This parameter is optional. Data type: integer. Valid values: 1 to 999999999. You can set the **count** or **ratio** parameter. You cannot set both parameters at the same time.
  - **ratio**: the threshold for the percentage of times that the specified HTTP status code is returned. The threshold is used to determine whether a rule is matched. If an actual percentage is greater than the threshold, the rule specified by the name parameter is matched. This parameter is optional. Data type: integer. Valid values: 1 to 100. You can set the **count** or **ratio** parameter. You cannot set both parameters at the same time.
- **scope**: the scope in which the settings take effect. This parameter is required. Data type: string. Valid values:
  - **rule**: the objects that match the specified conditions
  - **domain**: the domain names to which the rule is applied
- **ttl**: the period during which the specified action is performed. This parameter is required. Data type: integer. Valid values: 60 to 86400. Unit: seconds.

- **Example**

```
        {
            "name":"HTTP flood protection rule",
            "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
            }
    }
```

- If the DefenseType parameter is set to **whitelist**, the value of the Rule parameter consists of the following parameters:
  - **name**: the name of the rule. This parameter is required. Data type: string.

- **tags**: the protection module that does not check requests. This parameter is required. Data type: array. The values of the **tags** parameter vary based on the types of the whitelist.

  > **Note** The values of the **tags** parameter can contain only the values that are listed in a specific whitelist. For example, the values of the **tags** parameter cannot contain both **regular** and **cc**. This is because **regular** belongs to the whitelist for the web intrusion prevention module and **cc** belongs to the whitelist for the access control or throttling module.

  - To configure the global whitelist, set the **tags** parameter to the following value:
    - **waf**: Requests bypass all protection modules.
  - To configure the whitelist for the web intrusion prevention module, set the **tags** parameter to one or more of the following values:
    - **regular**: Requests bypass the protection rules engine module. Requests bypass all protection rules.
    - **regular_rule**: Requests bypass specific rules of the protection rules engine module. If you set the tags parameter to the value, you must configure the **regularRules** parameter to specify the IDs of the rules.
    - **regular_type**: Requests bypass specific types of the rules of the protection rules engine module. If you set the tags parameter to the value, you must configure the **regularRules** parameter to specify the types of the rules.
    - **deeplearning**: Requests bypass the deep learning engine module.
  - To configure the whitelist for the access control or throttling module, set the **tags** parameter to one or more of the following values:
    - **cc**: Requests bypass the HTTP flood protection module.
    - **customrule**: Requests bypass custom protection policies.
    - **blacklist**: Requests bypass the IP address blacklist module.
    - **antiscan**: Requests bypass the scan protection module.
  - To configure the whitelist for the data security module, set the **tags** parameter to one or more of the following values:
    - **dlp**: Requests bypass the data leakage prevention module.
    - **tamperproof**: Requests bypass the website tamper-proofing module.
    - **account**: Requests bypass the account security module.
  - To configure the whitelist for the bot management module, set the **tags** parameter to one or more of the following values:
    - **bot_intelligence**: Requests bypass the bot threat intelligence module.
    - **bot_algorithm**: Requests bypass the typical bot behavior identification module.
    - **bot_wxbb**: Requests bypass the app protection module.
    - **antifraud**: Requests bypass the data risk control module.
- **antifraud**: Requests bypass the data risk control module. If the value of the **tags** parameter contains **regular_rule**, the regularRules parameter is required. You can view the IDs of the rules when you create a rule group. To create a rule group, go to the WAF console and click **Protection Rule Group**. On the page that appears, click **Create Rule Group**. For more information, see Customize protection rule groups.

- **regularTypes**: the types of the rules that skip detection. This parameter is optional. Data type: array. If the value of the **tags** parameter includes **regular_type**, the regularTypes parameter is required. Valid values:
  - **sqli**: SQL injection
  - **xss**: cross-site scripting
  - **code_exec**: code execution
  - **lfilei**: local file inclusion
  - **rfilei**: remote file inclusion
  - **webshell**: webshell
  - **vvip**: custom protection rules
  - **other**: other types
- **conditions**: the match condition. You can specify a maximum of five match conditions. This parameter is required. Data type: array. The value is a JSON string that consists of the following parameters:
  - **key**: the match item. Value values: **URL**, **IP**, **Referer**, **User-Agent**, **Params**, **Cookie**, **Content-Type**, **Content-Length**, **X-Forwarded-For**, **Post-Body**, **Http-Method**, **Header**, and **URLPath**.
  - **opCode**: the logical operator. Valid values:
    - **0**: does not include or does not belong to
    - **1**: includes or belongs to
    - **2**: does not exist
    - **10**: does not equal
    - **11**: equals
    - **20**: length less than
    - **21**: length equal to
    - **22**: length greater than
    - **30**: value less than
    - **31**: value equal to
    - **32**: value greater than
  - **values**: the match value. You can specify this parameter based on your business requirements. Data type: string.

    > **Note** The valid values of the **opCode** and **values** parameters in the match conditions vary based on the **key** parameter.

- **Example**

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

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the **"Examples"** section of this topic.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
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****
&Common request parameters
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

6.8. ModifyProtectionRuleStatus

Enables or disables a rule of a specific protection module for a domain name. The protection modules include the website tamper-proofing, allowed crawlers, bot threat intelligence, custom protection policy, and website whitelist.

You can set the **DefenseType** parameter to specify the protection module. For more information about the value, see the description of the **DefenseType** parameter in the "Request parameters" section of this topic.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyProtectionRuleStatus	The operation that you want to perform. Set the value to **ModifyProtectionRuleStatus**.
DefenseType	String	Yes	tamperproof	The protection module. Valid values: • **tamperproof**: Website Tamper-proofing • **bot_crawler**: Allowed Crawlers • **bot_intelligence**: Bot Threat Intelligence • **ac_custom**: Custom Protection Policy • **whitelist**: Website Whitelist
Domain	String	Yes	www.example.com	The domain name that is added to WAF.
InstanceId	String	Yes	waf_elasticity-cn-0xldbqt****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
LockVersion	Long	Yes	2	The version of the rule.

Parameter	Type	Required	Example	Description
RuleId	Long	Yes	42755	The ID of the rule. **Note** You can call the DescribeProtectionModuleRules operation to query the IDs of all rules.
RuleStatus	Integer	Yes	1	The status of the rule. Valid values: • **0**: disabled • **1**: enabled

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

6.9. DescribeDomainRuleGroup

Queries the ID of the protection rule group of the protection rules engine feature and the status of the intelligent rule hosting feature for a specific domain name.

Usage notes

You can call the DescribeDomainRuleGroup operation to query the ID of the protection rule group of the protection rules engine feature and the status of the intelligent rule hosting feature for a specific domain name.

Limits

You can call this operation up to 10 times per second per account. If the number of the calls per second exceeds the limit, throttling is triggered. As a result, your business may be affected. We recommend that you take note of the limit when you call this operation.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeDomainRuleGroup	The operation that you want to perform. Set the value to **DescribeDomainRuleGroup**.
Domain	String	Yes	www.aliyundoc.com	The domain name that you want to query. **Note** You can call the DescribeDomainList operation to query all domain names that are protected by Web Application Firewall (WAF).
InstanceId	String	Yes	waf-cn-tl32ast****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "**Examples**" section of this topic.

Response parameters

Parameter	Type	Example	Description
RuleGroupId	Long	1012	The ID of the protection rule group that is bound to the domain name. Valid values: • **1011**: the built-in strict rule group • **1012**: the built-in medium rule group • **1013**: the built-in loose rule group Other values indicate the ID of your custom rule group.
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
WafAiStatus	Integer	1	The status of the intelligent rule hosting feature. Valid values: • **0**: disabled • **1**: enabled

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeDomainRuleGroup
&Domain=www.aliyundoc.com
&InstanceId=waf-cn-tl32ast****
&Common request parameters
```

Sample success responses

`XML` format

```
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` format

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

Error codes

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

6.10. SetDomainRuleGroup

Configures a protection rule group of the protection rules engine feature and the status of the intelligent rule hosting feature for a specific domain name.

Usage notes

You can call the SetDomainRuleGroup operation to configure the protection rule group of the protection rules engine feature and the status of the intelligent rule hosting feature for a specific domain name.

When you configure a protection rule group, you can use the loose, medium, or strict protection rule group that is provided by Web Application Firewall (WAF). You can also use a custom protection rule group.

> **Notice** You cannot create a custom protection rule group by calling an API operation. To configure a custom protection rule group for a domain name, log on to the WAF console and choose **System Management** > **Protection Rule Group**. On the Protection Rule Group page, create a custom protection rule group and record its ID. Then, you can call the SetDomainRuleGroup operation to configure the custom protection rule group for the domain name.

Limits

You can call this operation up to 10 times per second per account. If the number of the calls per second exceeds the limit, throttling is triggered. As a result, your business may be affected. We recommend that you take note of the limit when you call this operation.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	SetDomainRuleGroup	The operation that you want to perform. Set the value to **SetDomainRuleGroup**.
Domains	String	Yes	["www.aliyundoc.com"]	The list of domain names for which you want to configure a protection rule group. The value is a string that consists of JSON arrays. You can specify multiple domain names in the `["<Domain name 1>","<Domain name 2>",...]` format. **Note** You can call the DescribeDomainList operation to query all domain names that are protected by WAF.
RuleGroupId	Long	Yes	1012	The ID of the protection rule group that is configured for the domain name. Valid values: • **1011**: the built-in strict rule group • **1012**: the built-in medium rule group • **1013**: the built-in loose rule group You can also configure the ID of a custom rule group. **Note** To obtain the ID of a custom rule group, log on to the WAF console and choose System Management > **Protection Rule Group**.
WafVersion	Long	No	1	The version number for the current configuration, which is used to implement optimistic locking.

Parameter	Type	Required	Example	Description
InstanceId	String	Yes	waf-cn-tl32ast****	The ID of the WAF instance. Note You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
ResourceGroupId	String	No	rg-acfm2pz25js****	The ID of the resource group to which the domain name belongs in Resource Management. If you do not specify this parameter, the WAF instance belongs to the default resource group.
WafAiStatus	Integer	No	1	The status of the intelligent rule hosting feature. Valid values: • 0: disabled • 1: enabled. This is the default value. The intelligent rule hosting feature automatically learns the patterns of historical network traffic, identifies protection rules that may block normal requests in specific scenarios, and then adds the protection rules to the whitelist for web intrusion prevention. After the risk of blocking normal requests is eliminated, the intelligent rule hosting feature removes the protection rules from the whitelist.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "**Examples**" section of this topic.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=SetDomainRuleGroup
&Domains=["www.aliyundoc.com"]
&RuleGroupId=1012
&InstanceId=waf-cn-tl32ast****
&Common request parameters
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

6.11. ModifyProtectionRuleCacheStatus

Updates the cached pages that are protected by a specific website tamper-proofing rule.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyProtectionRuleCacheStatus	The operation that you want to perform. Set the value to **ModifyProtectionRuleCacheStatus**.
DefenseType	String	Yes	tamperproof	The protection module. Set the value to **tamperproof**.

Parameter	Type	Required	Example	Description
Domain	String	Yes	www.example.com	The domain name that is added to WAF.
InstanceId	String	Yes	waf_elasticity-cn-0xldbqt****	The ID of the WAF instance. **Note** You can query the ID by calling DescribeInstanceInfo.
RuleId	Long	Yes	42755	The ID of the rule. **Note** You can query the ID of all protection rules by calling DescribeProtectionModuleRules.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

6.12. DeleteProtectionModuleRule

Deletes a rule from the protection configuration module.

Debugging

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

Request parameters

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

Parameter	Type	Required	Example	Description
DefenseType	String	Yes	ac_custom	Specifies the protection module configuration. Valid values: • **waf-codec**: configures RegEx Protection Engine decoding settings. • **tamperproof**: configures the website tamper-proofing rules. • **dlp**: configures the data leak prevention rules. • **ng_account**: configures account security rules. • **antifraud**: configures data risk control. • **antifraud_js**: configures the JavaScript plug-in for data risk control. • **bot_algorithm**: configures intelligent algorithm rules for bot management. • **bot_wxbb_pkg**: configures version protection rules for app protection. • **bot_wxbb**: configures path protection rules for app protection. • **ac_custom**: configures custom protection policies. • **whitelist**: configures the whitelist rules.
Domain	String	Yes	www.example.com	The domain name that is added to WAF.
InstanceId	String	Yes	waf-cn-mp9153****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
RuleId	Long	Yes	42754	The ID of the rule.

Response parameters

Parameter	Type	Example	Description
RequestId	String	1557B42F-B889-460A-B17F-1DE5C5AD7FF2	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<DeleteProtectionModuleRuleResponse>
  <RequestId>1557B42F-B889-460A-B17F-1DE5C5AD7FF2</RequestId>
</DeleteProtectionModuleRuleResponse>
```

`JSON` format

```
{
  "RequestId":"1557B42F-B889-460A-B17F-1DE5C5AD7FF2"
}
```

Error codes

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

6.13. DescribeProtectionModuleCodeConfig

Queries the codes of regions that can be configured in a region blacklist. These codes include the codes of administrative regions in China and the codes of countries and areas.

Debugging

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

Request parameters

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

Parameter	Type	Required	Example	Description
CodeType	Integer	Yes	14	The type of code that you want to query. Set the value to **14**, which indicates the codes of regions that can be configured in a region blacklist of WAF.
InstanceId	String	Yes	waf-cn-zz11sr5****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
CodeValue	Integer	No	0	The type of region code that you want to query. Valid values: • **0**: codes of administrative regions in China • **1**: codes of countries and areas **Note** If you do not specify this parameter, both types of regions are queried.
ResourceGroupId	String	No	rg-acfm2pz25js****	The ID of the resource group to which the WAF instance belongs in Resource Management. This parameter is empty by default, which indicates that the WAF instance belongs to the default resource group. For more information about resource groups, see Create a resource group.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the **Examples** section of this topic.

Response parameters

Parameter	Type	Example	Description

Parameter	Type	Example	Description
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"}]	The code configurations. The value is a string that consists of JSON arrays. Each element in a JSON array is a JSON struct that represents a region code of one type and includes the following fields: • **code**: the type of region code. Data type: integer. Valid values: **0** and **1**. The value 0 indicates the codes of administrative regions in China. The value 1 indicates the codes of countries and areas. • **name**: the configured region codes that belong to the specified type. Data type: string. If multiple region codes are returned, the region codes are separated by commas (,). For more information about region codes, see the descriptions that follows the **Response parameters** section. • **env**: indicates whether region codes are available. Data type: string. Valid values: **online** and **offline**. online indicates that region codes are available. offline indicates that region codes are unavailable.
RequestId	String	BE3911B8-9D96-5B39-8875-503BBC9DA4BF	The ID of the request.

Codes of administrative regions in China

```
{
  "310000": "Shanghai",
  "610000": "Shaanxi",
  "360000": "Jiangxi",
  "230000": "Heilongjiang",
  "530000": "Yunnan",
  "140000": "Shanxi",
  "440000": "Guangdong",
  "320000": "Jiangsu",
  "110000": "Beijing",
  "MO_01": "Macau (China)",
  "620000": "Gansu",
  "370000": "Shandong",
  "150000": "Nei Mongol",
  "450000": "Guangxi",
  "410000": "Henan",
  "500000": "Chongqing",
  "120000": "Tianjin",
  "630000": "Qinghai",
  "460000": "Hainan",
  "640000": "Ningxia",
  "330000": "Zhejiang",
  "HK_01": "Hong Kong (China)",
  "420000": "Hubei",
  "430000": "Hunan",
  "130000": "Hebei",
  "510000": "Sichuan",
  "350000": "Fujian",
  "210000": "Liaoning",
  "220000": "Jilin",
  "340000": "Anhui",
  "520000": "Guizhou",
  "TW_01": "Taiwan (China)",
}
```

Codes of countries and areas

```
{
  "KE": "Kenya",
  "KG": "Kyrgyzstan",
  "KH": "Kampuchea",
  "KI": "Kiribati",
  "KM": "Comoros",
  "KN": "Saint Kitts and Nevis",
  "KP": "Democratic People's Republic of Korea",
  "KR": "Republic of Korea",
  "KW": "Kuwait",
  "KY": "Cayman Islands",
  "KZ": "Kazakhstan",
  "LA": "Laos",
  "LB": "Lebanon",
  "LC": "Saint Lucia",
  "LI": "Liechtenstein",
```

```
"LK": "Sri Lanka",
"LR": "Liberia",
"LS": "Lesotho",
"LT": "Lithuania",
"LU": "Luxembourg",
"LV": "Latvia",
"LY": "Libya",
"MA": "Morocco",
"MC": "Monaco",
"MD": "Moldova",
"ME": "Montenegro",
"MF": "Saint Martin",
"MG": "Madagascar",
"MH": "Marshall Islands",
"MK": "Macedonia",
"ML": "Mali",
"MM": "Myanmar",
"MN": "Mongolia",
"MP": "Northern Mariana Islands",
"MQ": "Martinique",
"MR": "Mauritania",
"MS": "Montserrat",
"MT": "Malta",
"MU": "Mauritius",
"MV": "Maldives",
"MW": "Malawi",
"MX": "Mexico",
"MY": "Malaysia",
"MZ": "Mozambique",
"NA": "Namibia",
"NC": "New Caledonia",
"NE": "Niger",
"NF": "Norfolk Island",
"NG": "Nigeria",
"NI": "Nicaragua",
"NL": "Netherlands",
"NO": "Norway",
"O1": "Other countries",
"NP": "Nepal",
"NR": "Nauru",
"NU": "Niue",
"NZ": "New Zealand",
"GA": "Gabon",
"GB": "United Kingdom of Great Britain and Northern Ireland"
"WS": "Samoa",
"GD": "Grenada",
"GE": "Georgia",
"GF": "French Guiana",
"GG": "Guernsey",
"GH": "Ghana",
"GI": "Gibraltar",
"GL": "Greenland",
"GM": "The Gambia",
"GN": "Guinea",
```

```
    "GP": "Guadeloupe",
    "GQ": "Equatorial Guinea",
    "GR": "Greece",
    "GS": "South Georgia and the South Sandwich Islands",
    "GT": "Guatemala",
    "GU": "Guam",
    "GW": "Guinea-Bissau",
    "GY": "Guyana",
    "HM": "Heard Island and McDonald Islands",
    "HN": "Honduras",
    "HR": "Croatia",
    "HT": "Haiti",
    "YE": "Yemen",
    "HU": "Hungary",
    "YT": "Mayotte",
    "ID": "Indonesia",
    "IE": "Ireland",
    "IL": "Israel",
    "IM": "Isle of Man",
    "IN": "India",
    "IO": "British Indian Ocean Territory",
    "ZA": "South Africa",
    "IQ": "Iraq",
    "IR": "Iran",
    "IS": "Iceland",
    "IT": "Italy",
    "ZM": "Zambia",
    "JE": "Jersey",
    "ZW": "Zimbabwe",
    "JM": "Jamaica",
    "JO": "Jordan",
    "JP": "Japan",
    "SI": "Slovenia",
    "SJ": "Svalbard and Jan Mayen Islands",
    "BY": "Belarus",
    "SK": "Slovakia",
    "BZ": "Belize",
    "SL": "Sierra Leone",
    "SM": "San Marino",
    "SN": "Senegal",
    "SO": "Somalia",
    "CA": "Canada",
    "SR": "Suriname",
    "SS": "South Sudan",
    "CC": "Cocos (Keeling) Islands",
    "ST": "Sao Tome and Principe",
    "CD": "Democratic Republic of the Congo",
    "CF": "Central African Republic",
    "SV": "El Salvador",
    "CG": "Republic of the Congo",
    "CH": "Switzerland",
    "SX": "Sint Maarten",
    "SY": "Syrian Arab Republic",
    "CI": "Côte d'Ivoire",
```

```
    "SZ": "Eswatini",
    "CK": "Cook Islands",
    "CL": "Chile",
    "CM": "Cameroon",
    "CN": "China",
    "CO": "Colombia",
    "TC": "Turks and Caicos Islands",
    "CR": "Costa Rica",
    "TD": "Chad",
    "CU": "Cuba",
    "TF": "French Southern and Antarctic Lands",
    "CV": "Cape Verde",
    "TG": "Togo",
    "CW": "Curaçao",
    "TH": "Thailand",
    "CX": "Christmas Island",
    "TJ": "Tajikistan",
    "CY": "Cyprus",
    "CZ": "Czech Republic",
    "TK": "Tokelau",
    "TL": "East Timor",
    "TM": "Turkmenistan",
    "TN": "Tunisia",
    "TO": "Tonga",
    "TR": "Turkey",
    "TT": "Trinidad and Tobago",
    "DE": "Germany",
    "TV": "Tuvalu",
    "DJ": "Djibouti",
    "TZ": "Tanzania",
    "DK": "Denmark",
    "DM": "Dominica",
    "DO": "Dominican Republic",
    "UA": "Ukraine",
    "UG": "Uganda",
    "DZ": "Algeria",
    "UM": "United States Minor Outlying Islands",
    "US": "United States",
    "EC": "Ecuador",
    "EE": "Estonia",
    "EG": "Egypt",
    "EH": "Western Sahara",
    "UY": "Uruguay",
    "UZ": "Uzbekistan",
    "VA": "Vatican City",
    "VC": "Saint Vincent and the Grenadines",
    "ER": "Eritrea",
    "ES": "Spain",
    "VE": "Venezuela",
    "ET": "Ethiopia",
    "EU": "Europe",
    "VG": "British Virgin Islands",
    "VI": "United States Virgin Islands",
    "VN": "Vietnam",
    "VU": "Vanuatu"
```

```
"VU": "Vanuatu",
"FI": "Finland",
"FJ": "Fiji",
"FK": "Falkland Islands",
"FM": "Federated States of Micronesia",
"FO": "Faroe Islands",
"FR": "France",
"WF": "Wallis and Futuna",
"OM": "Oman",
"PA": "Panama",
"PE": "Peru",
"PF": "French Polynesia",
"PG": "Papua New Guinea",
"PH": "Philippines",
"PK": "Pakistan",
"PL": "Poland",
"PM": "Saint Pierre and Miquelon",
"PN": "Pitcairn Islands",
"PR": "Puerto Rico",
"PS": "Palestine",
"PT": "Portugal",
"PW": "Palau",
"PY": "Paraguay",
"QA": "Qatar",
"A1": "Anonymous proxy",
"A2": "Satellite transmission",
"AD": "Andorra",
"AE": "United Arab Emirates",
"AF": "Afghanistan",
"AG": "Antigua and Barbuda",
"AI": "Anguilla",
"AL": "Albania",
"AM": "Armenia",
"AO": "Angola",
"AP": " Asia-Pacific",
"AQ": "Antarctica",
"AR": "Argentina",
"AS": "American Samoa",
"RE": "Reunion",
"AT": "Austria",
"AU": "Australia",
"AW": "Aruba",
"AX": "Aland Islands",
"AZ": "Azerbaijan",
"RO": "Romania",
"BA": "Bosnia and Herzegovina",
"BB": "Barbados",
"RS": "Serbia",
"BD": "Bangladesh",
"BE": "Belgium",
"RU": "Russia",
"BF": "Burkina Faso",
"RW": "Rwanda",
"BG": "Bulgaria",
"BH": "Bahrain",
```

```
  "BI": "Burundi",
  "BJ": "Benin",
  "BL": "Saint Barthelemy",
  "BM": "Bermuda",
  "BN": "Brunei",
  "BO": "Bolivia",
  "SA": "Saudi Arabia",
  "BQ": "Caribbean Netherlands",
  "SB": "Solomon Islands",
  "BR": "Brazil",
  "SC": "Seychelles",
  "SD": "Sudan",
  "BS": "Bahamas",
  "SE": "Sweden",
  "BT": "Bhutan",
  "BV": "Bouvet Island",
  "SG": "Singapore",
  "SH": "Saint Helena",
  "BW": "Botswana"
}
```

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeProtectionModuleCodeConfig
&CodeType=14
&InstanceId=waf-cn-zz11sr5****
&CodeValue=0
&<Common request parameters>
```

Sample success responses

`XML` format

```
<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_01,620000,350000,540000,520000,210000,500000,610000,630000,HK_01,230000</name>
            <env>online</env>
      </CodeConfigs>
</DescribeProtectionModuleCodeConfigResponse>
```

`JSON` format

```
{
    "RequestId": "BE3911B8-9D96-5B39-8875-503BBC9DA4BF",
    "CodeConfigs": [
        {
            "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"
        }
    ]
}
```


Error codes

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

7.Log management

7.1. ModifyLogRetrievalStatus

Enables or disables the log retrieval feature for a specific domain name.

> **Note** The log retrieval feature of WAF records all the access requests to a domain name only after the feature is enabled for the domain name. If the feature is disabled, WAF does not record the access requests that are sent to the domain name. Even if you enable the feature later, you cannot query the access requests in the period when the feature was disabled.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyLogRetrievalStatus	The operation that you want to perform. Set the value to **ModifyLogRetrievalStatus**.
Domain	String	Yes	www.example.com	The domain name that is added to WAF.
Enabled	Integer	Yes	1	Specifies whether to enable log retrieval. Valid values: • **0**: disables log retrieval • **1**: enables log retrieval
InstanceId	String	Yes	waf_elasticity-cn-0xldbqt****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.

Response parameters

Parameter	Type	Example	Description

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyLogRetrievalStatus
&Domain=www.example.com
&Enabled=1
&InstanceId=waf_elasticity-cn-0xldbqt****
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

7.2. ModifyLogServiceStatus

Enables or disables the log collection feature for a specific domain name.

Before you enable log collection, make sure that real-time log analysis is enabled for the WAF instance, and WAF has the permission to save logs to the exclusive Logstore.

For more information, see Real-time log analysis.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyLogServiceStatus	The operation that you want to perform. Set the value to **ModifyLogServiceStatus**.
Domain	String	Yes	www.example.com	The domain name that is added to WAF.
Enabled	Integer	Yes	1	Specifies whether to enable log collection. Valid values: • **0**: disables log collection • **1**: enables log collection
InstanceId	String	Yes	waf_elasticity-cn-0xldbqt****	The ID of the WAF instance. You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyLogServiceStatus
&Domain=www.example.com
&Enabled=1
&InstanceId=waf_elasticity-cn-0xldbqt****
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

7.3. DescribeLogServiceStatus

Queries whether the log collection feature is enabled for the domain names that are added to a WAF instance.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeLogServiceStatus	The operation that you want to perform. Set the value to **DescribeLogServiceStatus**.
InstanceId	String	Yes	waf-cn-zz11sr5****	The ID of the WAF instance. **Note** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
Region	String	No	cn	The region ID of the WAF instance. Default value: **cn**, which indicates that the WAF instance resides in mainland China. If the WAF instance resides outside mainland China, set the value to **cn-hongkong**. **Note** You can call the DescribeInstanceInfo operation to query the region ID of the WAF instance.

Parameter	Type	Required	Example	Description
ResourceGroupId	String	No	rg-acfm2pz25js****	The ID of the resource group to which the WAF instance belongs in Resource Management. This parameter is empty by default, which indicates that the WAF instance belongs to the default resource group. For more information about resource groups, see Create a resource group.
PageNumber	Integer	No	1	The number of the page to return. Default value: **1**.
PageSize	Integer	No	10	The number of entries to return on each page. Default value: **10**.
DomainNames.N	RepeatList	No	www.aliyun.com	The domain names that you want to query. A maximum of 10 domain names can be queried at a time. If you do not specify this parameter, all domain names are queried. **Note** You can call the DescribeDomainNames operation to query all the domain names that are added to the WAF instance.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the **"Examples"** section of this topic.

Response parameters

Parameter	Type	Example	Description
DomainStatus	Array of status		Indicates whether the log collection feature is enabled.
Domain	String	www.aliyun.com	The domain name.

Parameter	Type	Example	Description
SlsLogActive	Integer	1	Indicates whether the log collection feature is enabled for the domain name. Valid values: • **1**: enabled • **0**: disabled
RequestId	String	C2E97B3F-1623-4CDF-A7E2-FD9D4CF1027A	The ID of the request.
TotalCount	Integer	1	The total number of entries returned.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeLogServiceStatus
&InstanceId=waf-cn-zz11sr5****
&<Common request parameters>
```

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

8.System management

8.1. DescribeWafSourceIpSegment

Queries the back-to-origin CIDR blocks that are used by a WAF instance.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeWafSourceIpSegment	The operation that you want to perform. Set the value to **DescribeWafSourceIpSegment**.
InstanceId	String	Yes	waf-cn-zz11sr5****	The ID of the WAF instance. Note You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
ResourceGroupId	String	No	rg-acfm2pz25js****	The ID of the resource group to which the WAF instance belongs in Resource Management. By default, no value is specified, indicating that the domain name belongs to the default resource group. For more information about resource groups, see Create a resource group.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the **"Examples"** section of this topic.

Response parameters

Parameter	Type	Example	Description
IpV6s	String	39.XXX.XXX.0/24,.....,2408:400a:XXXX:XXXX::/56	The back-to-origin IPv6 CIDR blocks that are used by the WAF instance.

Parameter	Type	Example	Description
Ips	String	47.XXX.XXX.192/26,.....,47.XXX.XXX.0/24	The back-to-origin IPv4 CIDR blocks that are used by the WAF instance.
RequestId	String	AB2F5E31-EE96-4FD7-9560-45FF5D5377FF	The ID of the request.

Examples

Sample request

```
http(s)://[Endpoint]/? Action=DescribeWafSourceIpSegment
&InstanceId=waf-cn-zz11sr5****
&<Common request parameters>
```

Sample responses

`XML` format

```
<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` format

```
{
    "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"
}
```

Error codes

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

9.Resource operations

9.1. MoveResourceGroup

Transfers WAF resources to another resource group.

Description

Web Application Firewall (WAF) resources are the domain names that are added to WAF. You can sort the resources that belong to your Alibaba Cloud account into various resource groups. This facilitates resource management among multiple projects or applications within your Alibaba Cloud account and simplifies permission management. By default, domain name resources that are added to WAF belong to the default resource group. To manage your resources, you can transfer the domain name resources to your custom resource group.

You can create a resource group in the Resource Management console. For more information, see Create a resource group. You can also create a resource group by calling the API of Resource Management. For more information, see CreateResourceGroup.

For more information about resource groups, see Resource management.

QPS limit

This operation does not have a queries per second (QPS) limit on a single user. You can call this operation based on your business requirements.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	MoveResourceGroup	The operation that you want to perform. Set the value to **MoveResourceGroup**.
RegionId	String	Yes	cn-hangzhou	The region where the WAF instance resides. Valid values: • **cn-hangzhou**: mainland China • **ap-southeast-1**: outside mainland China
ResourceType	String	Yes	domain	The type of the WAF resource. Set the value to **domain**, which indicates that the type of WAF resource can only be the domain name.

Parameter	Type	Required	Example	Description
ResourceId	String	Yes	waf-cn-09k1rd5****~www.example.com	The ID of the WAF resource that you want to use. After you add a domain name to WAF, the domain name indicates a WAF resource. A unique resource ID (ResourceId) is used in Resource Management to identify a WAF resource. The ID of a WAF resource is in the format of `<InstanceId>~<Domain>`. The following list describes the format: • `<InstanceId>` specifies the ID of the WAF instance. You can call the DescribeInstanceInfo operation to query the ID of the WAF instance. • `<Domain>` specifies the domain name that is added to WAF. You can call the DescribeDomainList operation to query all domain names that are added to WAF. • You can use a tilde `(~)` to connect `<InstanceId>` and `<Domain>`. This specifies the ID of the WAF domain name resource.
ResourceGroupId	String	Yes	rg-atstuj3rtop****	The ID of the resource group to which you want to transfer the domain name. After you create a resource group by using Resource Management, Resource Management generates an ID for the resource group (ResourceGroupId). On the **Resource Group** page of the Resource Management console, you can query the IDs of all resource groups. You can also call the ListResourceGroups operation to query the IDs of all resource groups.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the **"Examples"** section of this topic.

Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request. You can use the ID to locate and troubleshoot issues.

Examples

Sample requests

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

Sample success responses

`XML` format

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

`JSON` format

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

Error codes

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

10.Error codes

The following table lists all the error codes that the system may return when you call a WAF API.

Error code	Error message	Description
RequestError	The system is unavailable. Please try again later.	The error message returned because an internal error has occurred. Try again later.
ComboError	No package information is available.	The error message returned because no package information is available.
DomainCountError	The number of domain names exceeds the limit. You can upgrade the domain package.	The error message returned because the maximum number of domains has been reached.
HttpsSupportError	HTTPS is not supported.	The error message returned because HTTPS requests are not supported.
OuterCloudSupportError	Servers outside Alibaba is not supported.	The error message returned because external servers are not supported.
DomainSourceIpCountError	The number of origin fetch addresses exceeds the limit.	The error message returned because the maximum number of origin IP addresses has been reached.
DomainNotRegisterError	The specified domain name is not ICP filed.	The error message returned because the specified domain does not have an ICP license.
ExtensiveDomainSupportError	Wildcard domains is not supported.	The error message returned because wildcard domains are not supported.
DomainHasAdded	The domain has been configured.	The error message returned because the specified domain has already been added.
SourceIpNotYoursError	You are not the owner of this origin fetch address.	The error message returned because the specified origin IP address does not belong to the current user.
HttpsCertFormatError	The certificate file is malformed.	The error message returned because the HTTPS certificate format is invalid.

Error code	Error message	Description
HttpsPrivateKeyFormatError	The private key of the certificate is malformed.	The error message returned because the format of the SSL certificate private key is invalid.
ErrorInSourceIps	The origin fetch address includes disallowed IP addresses or domains.	The error message returned because some IP addresses or domains cannot be added as origins.
DomainNotExist	The specified domain does not exist.	The error message returned because the specified domain does not exist.
IsNonStandardPort	Non-standard ports are not supported.	The error message returned because WAF does not support non-standard ports.
InvalidDomainError	The domain is invalid.	The error message returned because the specified domain is invalid.
InvalidMainDomainError	The number of primary domains exceeds the limit. You can upgrade the domain package.	The error message returned because the maximum number of primary domains has been reached.
NotSupportMainDomainError	The primary domain is not supported.	The error message returned because the specified primary domain is invalid.
CertAndKeyNotMatch	The certificate file and private key do not match.	The error message returned because the specified certificate and private key do not match.
SourceIpSupportsVirtualIpError	This is an instance dedicated for shared virtual host. Only an IP of a virtual host can be added.	The error message returned because only the IP address of a Web Hosting instance can be added.
DomainAutoAccessError	The auto access of domain is being configured.	The error message returned because a domain is being automatically added to WAF.
DomainHttpPortError	An invalid HTTP port is specified.	The error message returned because HTTP ports are not supported.
DomainHttpsPortError	An invalid HTTPS port is specified.	The error message returned because HTTPS ports are not supported.

Error code	Error message	Description
PortCountError	The number of ports exceeds the limit.	The error message returned because the maximum number of ports has been reached.
DomainBlackError	The domain has been listed in the blacklist.	The error message returned because the specified domain has been blacklisted.
AclRuleCountError	The number of access control rules exceeds the limit.	The error message returned because the maximum number of HTTP ACL rules has been reached.
AclRuleSeniorError	You don't have permission to use senior access control rule.	The error message returned because the maximum number of advanced HTTP ACL rules has been reached.
AclRuleDuplicateError	The access control rule name is invalid or a rule with the same name already exists.	The error message returned because the specified HTTP ACL rule name is invalid.
AclRuleNotFound	The specified access control rule does not exist.	The error message returned because the specified rule does not exist.
ExtensiveDomainHasBeenUsedByOthers	Another user has used this wildcard domain in WAF.	The error message returned because the specified wildcard domain has already been used by another user.
AuthorizeCertFailed	There are some errors when the system checks your certificate.	The error message returned because the certificate verification failed.
CertServiceError	There are some errors in the certificate service.	The error message returned because a certificate error occurred.
CertNameExisted	The certificate name already exists.	The error message returned because the specified certificate name already exists.
CertKeysIsNotMatch	The certificate file and private key do not match.	The error message returned because the certificate and the private key do not match.
CertKeysIsEmpty	The private key of the certificate is required.	The error message returned because the certificate private key is not specified.
CertKeyFormatError	The private key of the certificate is malformed.	The error message returned because the certificate private key format is invalid.

Error code	Error message	Description
SaveCertFailed	There are some errors when the system save your certificate.	The error message returned because the system failed to save the certificate.
CertHasExisted	This certificate has already been uploaded. Do not upload it again.	The error message returned because the specified certificate already exists.
CertHasExpired	The certificate has expired. Do not continue using this certificate.	The error message returned because the specified certificate has expired.
CertKeyServerError	The certificate service is unavailable,Please try again later.	The error message returned because a certificate error occurred.
ParamError	The parameters of your request are invalid.	The error message returned because the parameters are invalid.
CertIsNotMatchDomain	The certificate does not include this domain.	The error message returned because the certificate and the domain do not match.
CertNotExist	The certificate is not exist.	The error message returned because the specified certificate does not exist.
CertHasDelInCA	The certificate is deleted in CA service.	The error message returned because the certificate has been deleted by the certificate authority.
NotOperateOtherCallerConfig	You are not authorized to perform other channel config.	The error message returned because you cannot manage a domain configuration record created by other services.
DomainNotCloseInAntibot	The domain is still used in Anti-Bot service.	The error message returned because the Anti-Bot Service protection feature is enabled.
AntibotServerError	Anti-bot service is unavailable.	The error message returned because Anti-Bot Service is unavailable.
TaskNotFound	The specified task does not exist.	The error message returned because the task does not exist.
TaskIsRejected	The task has been rejected.	The error message returned because the task has been rejected.

Error code	Error message	Description
TaskStillRunning	The task is running.	The error message returned because the task is still running.
TaskTimeOut	The task is timeout.	The error message returned because the task has timed out.