

ALIBABA CLOUD

Alibaba Cloud

云防火墙
API参考

文档版本：20201026

 阿里云

法律声明

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

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

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

目录

1.API概览	06
2.调用方式	08
3.公共参数	10
4.访问控制API	12
4.1. AddControlPolicy	12
4.2. DescribeControlPolicy	19
4.3. DescribeDomainResolve	28
4.4. DescribePolicyPriorUsed	29
4.5. ModifyControlPolicy	31
4.6. ModifyControlPolicyPosition	35
4.7. DeleteControlPolicy	37
4.8. 严格模式	38
4.8.1. DescribePolicyAdvancedConfig	39
4.8.2. ModifyPolicyAdvancedConfig	40
4.9. VPC边界防火墙	41
4.9.1. CreateVpcFirewallControlPolicy	41
4.9.2. DescribeVpcFirewallControlPolicy	46
4.9.3. DescribeVpcFirewallPolicyPriorUsed	54
4.9.4. DescribeVpcFirewallAclGroupList	56
4.9.5. ModifyVpcFirewallControlPolicy	59
4.9.6. ModifyVpcFirewallControlPolicyPosition	63
4.9.7. ResetVpcFirewallRuleHitCount	64
4.9.8. DeleteVpcFirewallControlPolicy	66
5.地址簿API	69
5.1. AddAddressBook	69
5.2. DeleteAddressBook	71

5.3. ModifyAddressBook	73
5.4. DescribeAddressBook	75

1.API概览

本文列举了云防火墙提供的所有API接口，方便您查询使用。

防火墙开关API

API	描述
PutEnableFwSwitch	为指定资产开启防火墙开关。
PutDisableFwSwitch	为指定资产关闭防火墙开关。
PutEnableAllFwSwitch	为所有资产开启防火墙开关。
PutDisableAllFwSwitch	为所有资产关闭防火墙开关。

访问控制API

API	描述
AddControlPolicy	添加访问控制策略。
DescribeControlPolicy	获取所有访问控制策略信息。
DescribeDomainResolve	获取域名DNS的解析结果。
DescribePolicyPriorUsed	查询访问控制策略优先级生效范围。
ModifyControlPolicy	修改安全访问控制策略的配置信息。
ModifyControlPolicyPosition	修改访问控制策略的优先级。
DeleteControlPolicy	删除访问控制策略。
DescribePolicyAdvancedConfig	查询访问控制策略严格模式的开启状态。
ModifyPolicyAdvancedConfig	开启或关闭访问控制策略严格模式。

VPC边界防火墙API

API	描述
CreateVpcFirewallControlPolicy	为指定VPC防火墙策略组添加访问控制策略。
DescribeVpcFirewallControlPolicy	查询指定的VPC边界防火墙所有的访问控制策略信息。
DescribeVpcFirewallPolicyPriorUsed	查询指定VPC防火墙策略组访问控制策略优先级生效范围。
DescribeVpcFirewallAclGroupList	获取VPC防火墙所有访问控制策略组信息。

API	描述
ModifyVpcFirewallControlPolicy	修改指定VPC防火墙策略组的访问控制策略的配置信息。
ModifyVpcFirewallControlPolicyPosition	修改指定VPC防火墙策略组访问控制策略的优先级。
ResetVpcFirewallRuleHitCount	将指定的VPC防火墙策略组访问控制策略的命中计数清零。
DeleteVpcFirewallControlPolicy	删除指定VPC防火墙策略组的访问控制策略。

地址簿API

API	描述
AddAddressBook	添加安全访问控制地址簿，包括IP地址簿、ECS标签地址簿、端口地址簿和域名地址簿。
DescribeAddressBook	查询安全访问控制地址簿的详细信息。
ModifyAddressBook	修改安全访问控制的地址簿。
DeleteAddressBook	删除安全访问控制的地址簿。

2. 调用方式

您可以通过发送HTTP GET请求调用云防火墙的API，并按照接口说明在请求中加入相应的请求参数。调用接口后系统会返回处理结果。请求和返回结果都使用UTF-8字符集进行编码。

请求结构

云防火墙系统的API是RPC风格，您可以通过发送HTTP GET请求调用云防火墙的API。

其请求结构如下：

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

其中：

- **Endpoint**：云防火墙API的服务接入地址为cloudfw.cn-hangzhou.aliyuncs.com。
- **Action**：要执行的操作，如使用AddControlPolicy接口添加访问控制策略。
- **Version**：要使用的API版本，云防火墙的API版本是2017-12-07。
- **Parameters**：请求参数，每个参数之间用“&”分隔。

请求参数由公共请求参数和API自定义参数组成。公共参数中包含API版本号、身份验证等信息，详细内容参见[公共参数](#)。

下面是一个调用AddControlPolicy接口添加访问控制策略的示例：

 **说明** 为了便于用户查看，本文档中的示例都做了格式化处理。

```
http(s)://cloudfw.cn-hangzhou.aliyuncs.com/?Action=AddControlPolicy
&Format=xml
&Version=2017-12-07
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2012-06-01T12:00:00Z
...
```

API签名

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

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

RPC API需按如下格式在请求中增加签名（Signature）：


```
https://endpoint/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
```

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

```
https://cloudfw.cn-hangzhou.aliyuncs.com/?Action=AddControlPolicy
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2017-12-07
&SignatureVersion=1.0
```

完成以下步骤计算签名：

1. 使用请求参数创建待签名字符串：

```
GET&%2F&AccessKeyId%3Dtestid&Action%3DAddControlPolicy&Format%3DXML&SignatureMethod%3DHMAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&SignatureVersion%3D1.0&TimeStamp%3D2016-02-23T12%253A46%253A24Z&Version%3D2018-12-03
```

2. 计算待签名的HMAC的值。

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

```
CT9X0VtwR86fNWSnsc6v8YGOjuE=
```

3. 将签名加到请求参数中：

```
https://cloudfw.cn-hangzhou.aliyuncs.com/?Action=AddControlPolicy
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2017-12-07
&SignatureVersion=1.0
&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D
```

 **说明** 阿里云提供了多种语言的SDK及第三方SDK，可以免去您对签名算法进行编码的麻烦。更多阿里云SDK信息请参见[阿里云开发工具包（SDK）](#)。

3. 公共参数

本文档介绍API接口使用的公共请求参数。

公共请求参数

参数名称	类型	是否必须	描述
Region	String	是	云防火墙实例所在区域的取值：cn-hangzhou（表示中国内地地区）。
Format	String	否	返回消息的格式。取值： <ul style="list-style-type: none"> JSON（默认） XML
Version	String	是	API版本号，使用YYYY-MM-DD日期格式。取值：2017-12-07。
AccessKeyId	String	是	访问服务使用的密钥ID。
Signature	String	是	签名结果串。
SignatureMethod	String	是	签名方式，取值：HMAC-SHA1。
Timestamp	String	是	请求的时间戳，为日期格式。使用UTC时间按照ISO8601标准，格式为YYYY-MM-DDThh:mm:ssZ。例如，北京时间2013年1月10日20点0分0秒，表示为2013-01-10T12:00:00Z。
SignatureVersion	String	是	签名算法版本，目前版本是1.0。
SignatureNonce	String	是	唯一随机数，用于防止网络重放攻击。在不同请求间要使用不同的随机数值。
ResourceOwnerAccount	String	否	本次API请求访问到的资源所有者账户，即登录用户名。

示例

```
https://cloudfw.cn-hangzhou.aliyuncs.com/?Action=AddControlPolicy
&BizId=13688
&Region=cn
&Format=xml
&Version=2017-12-07
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2012-06-01T12:00:00Z
```

公共返回参数

API返回结果采用统一格式，返回2xx HTTP状态码代表调用成功；返回4xx或5xx HTTP状态码代表调用失败。

调用成功返回的数据格式有XML和JSON两种，可以在发送请求时指定返回的数据格式，默认为JSON格式。每次接口调用，无论成功与否，系统都会返回一个唯一识别码RequestId。

- XML格式

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

- JSON格式

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

4. 访问控制API

4.1. AddControlPolicy

调用AddControlPolicy添加访问控制策略。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	AddControlPolicy	要执行的操作。 取值：AddControlPolicy。
AclAction	String	是	accept	访问控制策略中设置的流量通过云防火墙的方式。取值： <ul style="list-style-type: none">accept：放行drop：拒绝log：观察

名称	类型	是否必选	示例值	描述
ApplicationName	String	是	HTTP	<p>访问控制策略支持的应用类型。取值：</p> <ul style="list-style-type: none"> • FTP • HTTP • HTTPS • Memcache • MongoDB • MQTT • MySQL • RDP • Redis • SMTP • SMTPS • SSH • SSL • VNC • ANY（表示所有类型的应用） <p> 说明 支持的应用类型取值与协议类型（Proto）取值存在依赖关系。Proto为TCP协议时，ApplicationName支持选择以上所有应用类型中的任意一种；Proto为UDP、ICMP或ANY协议类型时，ApplicationName仅支持选择ANY。</p>
Description	String	是	放行所有TCP流量。	访问控制策略的描述信息。

名称	类型	是否必选	示例值	描述
Destination	String	是	1.2.3.4/24	访问控制策略中的目的地址。取值： <ul style="list-style-type: none"> 当DestinationType为net时，Destination为目的CIDR。 例如：1.2.3.4/24 当DestinationType为group时，Destination为目的地址簿名称。 例如：db_group 当DestinationType为domain时，Destination为目的域名。 例如：*.aliyuncs.com 当DestinationType为location时，Destination为目的区域。 例如：["BJ11", "ZB"]
DestinationType	String	是	net	访问控制策略中的目的地址类型。取值： <ul style="list-style-type: none"> net：目的网段（CIDR地址） group：目的地址簿 domain：目的域名 location：目的区域
Direction	String	是	in	访问控制策略的流量方向。取值： <ul style="list-style-type: none"> in：外对内流量访问控制 out：内对外流量访问控制
NewOrder	String	是	-1	访问控制策略生效的优先级。优先级数字从1开始顺序递增，优先级数字越小，优先级越高。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> ? 说明 - 1表示优先级最低。 </div>

名称	类型	是否必选	示例值	描述
Proto	String	是	TCP	访问控制策略中流量访问的协议类型。取值： <ul style="list-style-type: none"> • ANY（任何协议） • TCP • UDP • ICMP
Source	String	是	1.2.3.0/24	访问控制策略中的源地址。取值： <ul style="list-style-type: none"> • 当SourceType为net时，Source为源CIDR地址。 例如：1.2.3.0/24 • 当SourceType为group时，Source为源地址簿名称。 例如：db_group • 当SourceType为location时，Source为源区域。 例如["BJ11", "ZB"]
SourceType	String	是	net	访问控制策略中的源地址类型。取值： <ul style="list-style-type: none"> • net：源网段（CIDR） • group：源地址簿 • location：源区域
SourceIp	String	否	1.2.3.5	访问者源IP地址。
Lang	String	否	zh	请求和接收消息的语言类型。取值： <ul style="list-style-type: none"> • zh：中文 • en：英文

名称	类型	是否必选	示例值	描述
DestPort	String	否	80	<p>访问控制策略中流量访问的目的端口。取值：</p> <ul style="list-style-type: none"> 当协议类型为ICMP时，DestPort取值为空。 <p>? 说明 协议类型为ICMP时，不支持对目的端口进行访问控制。</p> <ul style="list-style-type: none"> 当协议类型为TCP、UDP或ANY时，并且目的端口类型（DestPortType）为group时，DestPort取值为空。 <p>? 说明 访问控制策略目的端口类型选择group（目的端口地址簿）时，您无需设置具体的目的端口号。需要该访问控制策略管控的所有端口会包含在目的端口地址簿中。</p> <ul style="list-style-type: none"> 当协议类型为TCP、UDP或ANY时，并且目的端口类型（DestPortType）为port时，DestPort取值为目的端口号。
DestPortType	String	否	port	<p>访问控制策略中流量访问的目的端口类型。</p> <p>取值：</p> <ul style="list-style-type: none"> port：端口 group：端口地址簿
DestPortGroup	String	否	my_port_group	<p>访问控制策略中访问流量的目的端口地址簿名称。</p> <p>? 说明 DestPortType设置为group时，您需要设置目的端口地址簿名称。</p>
Release	String	否	true	<p>访问控制策略的启用状态。策略创建后默认启用该策略。取值：</p> <ul style="list-style-type: none"> true：启用访问控制策略 false：不启用访问控制策略

地区编号如下：

- 中国：ZD
- 北京市：BJ11

- 天津市: TJ12
- 河北省: HB13
- 山西省: SX14
- 辽宁省: LN21
- 吉林省: JL22
- 上海市: SH31
- 江苏省: JS32
- 浙江省: ZJ33
- 安徽省: AH34
- 福建省: FJ35
- 江西省: JX36
- 山东省: SD37
- 河南省: HN41
- 湖北省: HB42
- 湖南省: HN43
- 广东省: GD44
- 海南省: HN46
- 重庆市: CQ50
- 四川省: SC51
- 贵州省: GZ52
- 云南省: YN53
- 陕西省: SX61
- 甘肃省: GS62
- 青海省: QH63
- 黑龙江省: HLJ23
- 西藏自治区: XZ54
- 广西壮族自治区: GX45
- 内蒙古自治区: NMG15
- 宁夏回族自治区: NX64
- 新疆维吾尔自治区: XJ65
- 台湾省: TW
- 香港特别行政区: HK
- 澳门特别行政区: MO
- 海外: ZB
- 亚洲 (中国内地除外): ZC
- 欧洲: EU
- 非洲: AF
- 北美洲: NA
- 南美洲: LA
- 大洋洲: OA

- 南极洲：AQ

返回数据

名称	类型	示例值	描述
AclUuid	String	00281255-d220-4db1-8f4f-c4df221ad84c	互联网边界防火墙访问控制策略的唯一标识ID。
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	返回结果的请求ID。

示例

请求示例

```

http(s)://[Endpoint]/?Action=AddControlPolicy
&AclAction=accept
&ApplicationName=ANY
&Description=demo_rule_1
&Destination=1.2.3.4/24
&DestinationType=net
&Direction=in
&NewOrder=-1
&Proto=TCP
&Source=1.2.3.0/24
&SourceType=net
&<公共请求参数>

```

正常返回示例

XML 格式

```

<AddControlPolicyResponse>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
  <AclUuid>00281255-d220-4db1-8f4f-c4df221ad84c</AclUuid>
</AddControlPolicyResponse>

```

JSON 格式

```

{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D",
  "AclUuid": "00281255-d220-4db1-8f4f-c4df221ad84c"
}

```

错误码

访问[错误中心](#)查看更多错误码。

4.2. DescribeControlPolicy


调用DescribeControlPolicy接口获取所有访问控制策略的信息。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeControlPolicy	需要执行的操作。 取值：DescribeControlPolicy。
CurrentPage	String	是	1	分页查询时，显示的当前页的页码。 默认值为1。
Direction	String	是	in	访问控制策略控制的流量方向。取值： <ul style="list-style-type: none"> in：外对内方向的流量访问控制。 out：内对外方向的流量访问控制。
PageSize	String	是	10	分页查询时，显示的每页数据的最大条数。 可设置值最大为50。
SourceIp	String	否	1.2.3.4	访问源的IP地址。
Lang	String	否	zh	请求和接收消息的语言类型。取值： <ul style="list-style-type: none"> zh：中文 en：英文

名称	类型	是否必选	示例值	描述
Source	String	否	1.2.3.5	<p>访问控制策略中的访问源地址。支持使用模糊查询的方式进行查询。SourceType（源类型）不同，访问源地址的取值也不同。</p> <ul style="list-style-type: none"> 当SourceType为 net 时，访问源为IP/CIDR地址。例如：10.0.1.0/24。 当SourceType为 group 时，访问源为源地址簿名称。例如：db_group为空（表示查询所有访问控制源）。 当SourceType为 location 时，访问源为源区域。例如：北京或beijing（支持使用中文或英文进行查询）。 当SourceType为空 时，表示查询所有类型的访问源。
Destination	String	否	1.2.3.0	<p>访问控制策略中的目的地址。支持模糊查询。DestinationType（目的类型）不同，目的地址的取值也不同。</p> <ul style="list-style-type: none"> 当DestinationType为 net 时，目的地址为IP/CIDR地址。例如：10.0.3.0/24。 当DestinationType为 domain 时，目的地址为域名。例如：aliyun。 当DestinationType为 group 时，目的地址为地址簿的名称。例如：db_group。 当DestinationType为 location 时，目的地址为目的区域。例如：北京或beijing（支持使用中文或英文进行查询）。 当DestinationType为空 时，表示查询所有类型的目的地址。
Description	String	否	test	<p>访问控制策略的描述信息。支持模糊查询。</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p> 说明 为空表示查询所有策略的描述信息。</p> </div>


名称	类型	是否必选	示例值	描述
Proto	String	否	TCP	访问控制策略中访问流量的协议类型。取值： <ul style="list-style-type: none"> • TCP • UDP • ICMP • ANY（表示所有类型的协议） • 为空（表示所有类型的协议）
AclAction	String	否	accept	访问控制策略中设置的流量通过云防火墙的方式（动作）。取值： <ul style="list-style-type: none"> • accept：放行 • drop：拒绝 • log：观察 • 为空：所有的动作类型
Release	String	否	true	访问控制策略的启用状态。策略创建后默认启用该策略。取值： <ul style="list-style-type: none"> • true：启用访问控制策略 • false：不启用访问控制策略
AclUuid	String	否	00281255-d220-4db1-8f4f-c4df221ad84c	访问控制策略的唯一标识ID。

返回数据

名称	类型	示例值	描述
PageNo	String	1	分页查询时，显示的当前页的页码。
PageSize	String	10	分页查询时，显示的每页数据的最大条数。
Policys	Array		访问控制策略的信息。
AclAction	String	accept	访问控制策略中设置的流量通过云防火墙的方式（动作）。取值： <ul style="list-style-type: none"> • accept：放行 • drop：拒绝 • log：观察

名称	类型	示例值	描述
AclUuid	String	00281255-d220-4db1-8f4f-c4df221ad84c	访问控制策略的唯一标识ID。
ApplicationId	String	10***	访问控制策略中设置访问流量的应用ID。
ApplicationName	String	HTTP	访问控制策略支持的应用类型。取值： <ul style="list-style-type: none"> FTP HTTP HTTPS Memcache MongoDB MQTT MySQL RDP Redis SMTP SMTPS SSH SSL VNC ANY（表示所有类型的应用）
Description	String	test	访问控制策略的描述信息。
DestPort	String	80	访问控制策略中访问流量的目的端口。
DestPortGroup	String	my_port_group	访问控制策略中流量访问的目的端口地址簿名称。
DestPortGroupPorts	List	[80,443]	目的端口地址簿中包含的端口列表。
DestPortType	String	port	访问控制策略中流量访问的目的端口类型。取值： <ul style="list-style-type: none"> port：端口 group：端口地址簿

名称	类型	示例值	描述
Destination	String	1.2.3.4/24	访问控制策略中的目的地址。 DestinationType（目的类型）不同，目的地址的取值也不同。取值： <ul style="list-style-type: none"> 当DestinationType为net时，目的地址为IP/CIDR地址。例如：10.0.3.0/24。 当DestinationType为domain时，目的地址为域名。例如：aliyuncs.com。 当DestinationType为group时，目的地址为地址簿的名称。例如：db_group。 当DestinationType为location时，目的地址为区域名称（具体区域位置编码请参见AddControlPolicy）。例如：["BJ11", "ZB"]。
DestinationGroupCidrs	List	["1.2.3.0/24", "1.2.3.1/32"]	访问控制策略中的目的地址簿中的网段列表。
DestinationGroupType	String	ip	访问控制策略中的目的地址簿类型。取值： <ul style="list-style-type: none"> ip：IP地址簿，包含一个或多个IP地址段。 tag：ECS标签地址簿，包含一个或多个ECS标签下的IP地址。 domain：域名地址簿，包含一个或多个域名地址。 threat：威胁地址簿，包含一个或多个恶意IP或域名地址。 backsrc：回源地址簿，包含一个或多个DDoS防护实例或WAF实例的回源地址。
DestinationType	String	net	访问控制策略中的目的地址类型。取值： <ul style="list-style-type: none"> net：目的网段（CIDR） group：目的地址簿 domain：目的域名 location：目的区域
Direction	String	in	访问控制策略的流量方向。取值： <ul style="list-style-type: none"> in：外对内流量访问控制 out：内对外流量访问控制
DnsResult	String	1.1.1.1,2.2.2.2	DNS解析结果。
DnsResultTime	Long	1579261141	DNS解析的时间戳。

名称	类型	示例值	描述
HitTimes	Integer	100	访问控制策略的命中次数。
Order	Integer	1	访问控制策略生效的优先级。 优先级数字从1开始顺序递增，优先级数字越小，优先级越高。  说明 - 1表示优先级最低。
Proto	String	TCP	访问控制策略中流量访问的安全协议类型。取值： <ul style="list-style-type: none"> • ANY • TCP • UDP • ICMP
Release	String	true	访问控制策略的启用状态。策略创建后默认启用该策略。取值： <ul style="list-style-type: none"> • true：启用访问控制策略 • false：不启用访问控制策略
Source	String	1.2.3.0/24	访问控制策略中的访问源地址。取值： <ul style="list-style-type: none"> • 当SourceType为 net 时，访问源地址为CIDR地址。例如：10.0.1.0/24。 • 当SourceType为 group 时，访问源地址为源地址簿名称。例如：db_group。 • 当SourceType为 location 时，访问源地址为区域（具体区域位置编码请参见AddControlPolicy）。例如：["BJ11", "ZB"]。
SourceGroupCidrs	List	["10.0.0.0/24", "10.0.0.1/32"]	访问控制策略中的源地址簿中的网段列表。

名称	类型	示例值	描述
SourceGroupType	String	ip	访问控制策略中的源地址簿类型。取值： <ul style="list-style-type: none"> ip: IP地址簿，包含一个或多个IP地址段。 tag: ECS标签地址簿，包含一个或多个ECS标签下的IP地址。 domain: 域名地址簿，包含一个或多个域名地址。 threat: 威胁地址簿，包含一个或多个恶意IP或域名地址。 backsrc: 回源地址簿，包含一个或多个DDoS防护实例或WAF实例的回源地址。
SourceType	String	net	访问控制策略中的源地址类型。取值： <ul style="list-style-type: none"> net: 源网段（CIDR地址） group: 源地址簿 location: 源区域
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	结果的请求ID。
TotalCount	String	100	访问控制策略的总数量。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeControlPolicy
&CurrentPage=1
&Direction=in
&PageSize=10
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeControlPolicyResponse>
  <TotalCount>58</TotalCount>
  <PageNo>1</PageNo>
  <PageSize>10</PageSize>
  <RequestId>A08BC58F-A83D-43EB-BC31-2F0D723929CC</RequestId>
  <Policys>
    <ApplicationName>RDP</ApplicationName>
    <Description>11</Description>
    <HitTimes>0</HitTimes>
    <DestinationType>net</DestinationType>
    <SourceType>net</SourceType>
    <Proto>TCP</Proto>
    <Order>5</Order>
    <ApplicationId>27</ApplicationId>
    <Direction>in</Direction>
    <DestPortType>port</DestPortType>
    <Source>1.1.1.1/32</Source>
    <DestPort>1/1</DestPort>
    <AclAction>accept</AclAction>
    <AclUuid>53d82f0e-9bf1-4761-ab3b-a070b4811234</AclUuid>
    <Destination>1.1.1.1/32</Destination>
    <DnsResult>1.1.1.1,2.2.2.2</DnsResult>
    <DnsResultTime>1579261141</DnsResultTime>
  </Policys>
</DescribeControlPolicyResponse>
```

JSON 格式

```
{
  "TotalCount":58,
  "PageNo":1,
  "PageSize":10,
  "RequestId":"A08BC58F-A83D-43EB-BC31-2F0D723929CC",
  "Policys":[
    {
      "DestinationGroupCidrs":[

      ],
      "SourceGroupCidrs":[

      ],
      "ApplicationName":"RDP",
      "Description":"11",
      "HitTimes":0,
      "DestinationType":"net",
      "SourceType":"net",
      "Proto":"TCP",
      "Order":5,
      "ApplicationId":"27",
      "Direction":"in",
      "DestPortType":"port",
      "Source":"1.1.1.1/32",
      "DestPort":"1/1",
      "AclAction":"accept",
      "DestPortGroupPorts":[


      ],
      "AclUuid":"53d82f0e-9bf1-4761-ab3b-a070b4811234",
      "Destination":"1.1.1.1/32",
      "DnsResult": "1.1.1.1,2.2.2.2",
      "DnsResultTime": 1579261141
    }
  ]
}
```

错误码

访问[错误中心](#)查看更多错误码。

4.3. DescribeDomainResolve

调用DescribeDomainResolve接口获取域名DNS的解析结果。

 **说明** 当前仅支持从阿里云云解析DNS获取解析结果。要查询的域名必须使用云解析DNS，才能查询到其解析结果。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainResolve	要执行的操作。 取值： DescribeDomainResolve 。
Domain	String	是	www.aliyun.com	待解析的域名地址。
SourceIp	String	否	1.2.3.4	访问者源IP地址。
Lang	String	否	zh	请求和接收消息的语言类型。 取值包括： <ul style="list-style-type: none">zh: 中文en: 英文

返回数据

名称	类型	示例值	描述
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	结果的请求ID。
ResolveResult	Struct		域名解析结果。
IpAddrs	String	11.1.1.1,12.1.1.1	域名解析结果，多个IP地址用半角逗号(,)分隔。
UpdateTime	Long	1579091739	解析时间戳。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainResolve
&Domain=www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeDomainResolveResponse>
  <RequestId>412AF3C5-B225-4606-8323-A8924F796F16</RequestId>
  <ResolveResult>
    <IpAddrs>12.3.4,1.2.3.5,1.2.3.6</IpAddrs>
    <UpdateTime>1586765803</UpdateTime>
  </ResolveResult>
</DescribeDomainResolveResponse>
```

JSON 格式

```
{
  "RequestId": "412AF3C5-B225-4606-8323-A8924F796F16",
  "ResolveResult": {
    "IpAddrs": "12.3.4,1.2.3.5,1.2.3.6",
    "UpdateTime": 1586765803
  }
}
```

错误码

访问[错误中心](#)查看更多错误码。

4.4. DescribePolicyPriorUsed

调用DescribePolicyPriorUsed接口查询访问控制策略优先级生效范围。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribePolicyPriorUsed	系统规定参数。取值： DescribePolicyPriorUsed 。
Direction	String	是	in	访问控制策略的流量方向。 取值： <ul style="list-style-type: none"> in：外对内流量。 out：内对外流量。
SourceIp	String	否	1.2.3.4	访问者源IP地址。
Lang	String	否	zh	请求和接收消息的语言类型。 取值： <ul style="list-style-type: none"> zh：中文 en：英文

返回数据

名称	类型	示例值	描述
End	Integer	150	访问控制策略生效的最低优先级。
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	结果的请求ID。
Start	Integer	1	访问控制策略生效的最高优先级。

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribePolicyPriorUsedResponse>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
  <Start>1</Start>
  <End>150</End>
</DescribePolicyPriorUsedResponse>
```

JSON 格式

```
{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D",
  "Start": 1,
  "End": 150
}
```

错误码

访问[错误中心](#)查看更多错误码。

4.5. ModifyControlPolicy

调用ModifyControlPolicy接口修改安全访问控制策略的配置信息。


调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyControlPolicy	要执行的操作。取值： ModifyControlPolicy 。
AclAction	String	是	accept	安全访问控制策略中流量通过云防火墙的方式。取值： <ul style="list-style-type: none"> accept：放行 drop：拒绝 log：观察

名称	类型	是否必选	示例值	描述
AclUuid	String	是	00281255-d220-4db1-8f4f-c4df221ad84c	<p>安全访问控制策略的唯一标识ID。</p> <p> 说明 修改安全访问控制策略，需要提供该策略的唯一标识ID，该ID可调用DescribeControlPolicy接口获取。</p>
ApplicationName	String	是	HTTP	<p>安全访问控制策略支持的应用类型。支持的应用类型有以下几种：</p> <ul style="list-style-type: none"> • ANY • HTTP • HTTPS • MySQL • SMTP • SMTPS • RDP • VNC • SSH • Redis • MQTT • MongoDB • Memcache • SSL <p> 说明 ANY表示策略应用在所有类型的应用中。</p>
Description	String	是	test	安全访问控制策略的描述信息。

名称	类型	是否必选	示例值	描述
Destination	String	是	1.2.3.4/24	<p>安全访问控制策略中的目的地址。</p> <ul style="list-style-type: none"> 当DestinationType为net时，Destination为目的CIDR。例如：1.2.3.4/24 当DestinationType为group时，Destination为目的地址簿名称。例如：db_group 当DestinationType为domain时，Destination为目的域名。例如：*.aliyuncs.com 当DestinationType为location时，Destination为目的区域（具体区域位置编码见后文）。例如：["BJ11", "ZB"]
DestinationType	String	是	net	<p>安全访问控制策略中的目的地址类型。取值：</p> <ul style="list-style-type: none"> net：目的网段(CIDR) group：目的地址簿 domain：目的域名 location：目的区域
Direction	String	是	in	<p>安全访问控制策略的流量方向。取值：</p> <ul style="list-style-type: none"> in：外对内流量访问控制 out：内对外流量访问控制
Proto	String	是	TCP	<p>安全访问控制策略中流量访问的安全协议类型。支持的应用类型有以下几种：</p> <ul style="list-style-type: none"> ANY TCP UDP ICMP <div style="background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p> 说明 ANY表示策略应用在所有类型的应用中。</p> </div>

名称	类型	是否必选	示例值	描述
Source	String	是	1.2.3.0/24	安全访问控制策略中的源地址。 <ul style="list-style-type: none"> 当SourceType为net时，Source为源CIDR。例如：1.2.3.0/24 当SourceType为group时，Source为源地址簿名称。例如：db_group 当SourceType为location时，Source为源区域（具体区域位置编码见后文）。例如["BJ11", "ZB"]
SourceType	String	是	net	安全访问控制策略中的源地址类型。取值： <ul style="list-style-type: none"> net：源网段(CIDR) group：源地址簿 location：源区域
SourceIp	String	否	1.2.3.5	访问者源IP地址。
Lang	String	否	zh	请求和接收消息的语言类型。取值： <ul style="list-style-type: none"> zh：中文 en：英文
DestPort	String	否	80	安全访问控制策略中流量访问的目的端口。
DestPortType	String	否	port	安全访问控制策略中流量访问的目的端口类型。取值： <ul style="list-style-type: none"> port：端口 group：端口地址簿
DestPortGroup	String	否	my_port_group	安全访问控制策略中流量访问的目的端口地址簿名称。

返回数据

名称	类型	示例值	描述
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	结果的请求ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyControlPolicy
&AclAction=accept
&AclUuid=00281255-d220-4db1-8f4f-c4df221ad84c
&ApplicationName=HTTP
&Description=test
&Destination=1.2.3.4/24
&DestinationType=net
&Direction=in
&Proto=TCP
&Source=1.2.3.0/24
&SourceType=net
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ModifyControlPolicyResponse>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
</ModifyControlPolicyResponse>
```

JSON 格式

```
{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}
```

错误码

访问[错误中心](#)查看更多错误码。

4.6. ModifyControlPolicyPosition

调用ModifyControlPolicyPosition接口修改访问控制策略的优先级。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyControlPolicyPosition	系统规定参数。取值： ModifyControlPolicyPosition。
Direction	String	是	in	安全访问控制策略的流量方向。 <ul style="list-style-type: none"> in: 外对内流量访问控制 out: 内对外流量访问控制
NewOrder	String	是	1	修改后，访问控制策略生效的新优先级。
OldOrder	String	是	5	修改前，访问控制策略生效的旧优先级。
Lang	String	否	zh	请求和接收消息的语言类型。 <ul style="list-style-type: none"> zh: 中文 en: 英文
SourceIp	String	否	1.2.3.4	访问者源IP地址。

返回数据

名称	类型	示例值	描述
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125EEB1	结果的请求ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyControlPolicyPosition
&Direction=in
&NewOrder=1
&OldOrder=5
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ModifyControlPolicyPosition>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125EEB1</RequestId>
</ModifyControlPolicyPosition>
```

JSON 格式

```
{
  "RequestId": "850A84D6-0DE4-4797-A1E8-00090125EEB1"
}
```

错误码

访问[错误中心](#)查看更多错误码。

4.7. DeleteControlPolicy

调用DeleteControlPolicy接口删除访问控制策略。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteControlPolicy	系统规定参数。取值：DeleteControlPolicy。
AclUuid	String	是	00281255-d220-4db1-8f4f-c4df221ad84c	访问控制策略的唯一标识ID。 删除安全访问控制策略，需要提供该策略的唯一标识ID。您可调用DescribeControlPolicy接口获取该ID。
Direction	String	是	in	安全访问控制策略管控的流量方向。 取值： <ul style="list-style-type: none"> in：流量从外到内。 out：流量从内到外。
SourceIp	String	否	1.2.3.4	流量的源IP地址。

名称	类型	是否必选	示例值	描述
Lang	String	否	zh	请求和接收消息的语言类型。 取值： <ul style="list-style-type: none"> zh: 中文 en: 英文

返回数据

名称	类型	示例值	描述
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	结果的请求ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteControlPolicy
&AclUuid=00281255-d220-4db1-8f4f-c4df221ad84c
&Direction=in
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DeleteControlPolicyResponse>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
</DeleteControlPolicyResponse>
```

JSON 格式

```
{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}
```

错误码

访问[错误中心](#)查看更多错误码。

4.8. 严格模式

4.8.1. DescribePolicyAdvancedConfig

调用DescribePolicyAdvancedConfig查询访问控制策略严格模式的开启状态。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribePolicyAdvancedConfig	要执行的操作。 取值：DescribePolicyAdvancedConfig。
SourceIp	String	否	1.2.3.4	访问者源IP地址。
Lang	String	否	zh	请求和接收消息的语言类型。取值： <ul style="list-style-type: none"> zh：中文 en：英文

返回数据

名称	类型	示例值	描述
InternetSwitch	String	off	访问控制策略严格模式的开启状态。取值： <ul style="list-style-type: none"> on：严格模式已开启。 off：严格模式已关闭。
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125EEB1	返回结果的请求ID。

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribePolicyAdvancedConfigResponse>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125EEB1</RequestId>
  <InternetSwitch>off</InternetSwitch>
</DescribePolicyAdvancedConfigResponse>
```

JSON 格式

```
{
  "RequestId": "850A84D6-0DE4-4797-A1E8-00090125EEB1",
  "InternetSwitch": "off"
}
```

错误码

访问[错误中心](#)查看更多错误码。

4.8.2. ModifyPolicyAdvancedConfig

调用ModifyPolicyAdvancedConfig开启或关闭访问控制策略严格模式。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyPolicyAdvancedConfig	要执行的操作。 取值： ModifyPolicyAdvancedConfig 。
InternetSwitch	String	是	off	修改访问控制策略严格模式的开关状态。 取值： <ul style="list-style-type: none"> on：开启严格模式。 off：关闭严格模式。
SourceIp	String	否	1.2.3.4	访问者源IP地址。
Lang	String	否	zh	请求和接收消息的语言类型。取值： <ul style="list-style-type: none"> zh：中文 en：英文

返回数据

名称	类型	示例值	描述
RequestId	String	B2841452-CB8D-4F7D-B247-38E1CF7334F8	返回结果的请求ID。

示例

请求示例

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

正常返回示例

XML 格式

```
<ModifyPolicyAdvancedConfigResponse>
  <RequestId>B2841452-CB8D-4F7D-B247-38E1CF7334F8</RequestId>
</ModifyPolicyAdvancedConfigResponse>
```

JSON 格式

```
{
  "RequestId": "B2841452-CB8D-4F7D-B247-38E1CF7334F8"
}
```


错误码

访问[错误中心](#)查看更多错误码。

4.9. VPC边界防火墙

4.9.1. CreateVpcFirewallControlPolicy

调用CreateVpcFirewallControlPolicy接口为指定VPC防火墙策略组添加访问控制策略。


 **说明** 防护云企业网的VPC防火墙实例和防护高速通道的VPC防火墙实例使用不同的访问控制策略。



调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateVpcFirewallControlPolicy	需要执行的操作。 取值： CreateVpcFirewallControlPolicy 。
AclAction	String	是	accept	VPC边界防火墙访问控制策略中设置的流量通过云防火墙的方式（动作）。取值： <ul style="list-style-type: none"> • accept: 放行 • drop: 拒绝 • log: 观察
ApplicationName	String	是	HTTP	VPC边界防火墙访问控制策略支持的应用类型。取值： <ul style="list-style-type: none"> • FTP • HTTP • HTTPS • MySQL • SMTP • SMTPS • RDP • VNC • SSH • Redis • MQTT • MongoDB • Memcache • SSL • ANY（表示支持所有的应用类型）
Description	String	是	test	VPC边界防火墙访问控制策略的描述信息。

名称	类型	是否必选	示例值	描述
Destination	String	是	10.2.3.0/24	<p>VPC边界防火墙访问控制策略中流量访问的目的地址。</p> <p>取值：</p> <ul style="list-style-type: none"> 当DestinationType为 <code>net</code> 时，Destination为目的CIDR地址。 例如：10.2.3.0/24 当DestinationType为 <code>group</code> 时，Destination为目的地址簿名称。 例如：db_group 当DestinationType为 <code>domain</code> 时，Destination为目的域名。 例如：*.aliyuncs.com
DestinationType	String	是	net	<p>VPC边界防火墙访问控制策略中的目的地址类型。取值：</p> <ul style="list-style-type: none"> <code>net</code>：目的网段（CIDR） <code>group</code>：目的地址簿 <code>domain</code>：目的域名
NewOrder	String	是	-1	<p>VPC边界防火墙访问控制策略生效的优先级。</p> <p>优先级数字从1开始顺序递增，优先级数字越小，优先级越高。</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p> 说明 - 1表示优先级最低。</p> </div>
Proto	String	是	TCP	<p>VPC边界防火墙访问控制策略中流量访问的安全协议类型。取值：</p> <ul style="list-style-type: none"> <code>ANY</code>（不确定具体协议类型时可设置为ANY） <code>TCP</code> <code>UDP</code> <code>ICMP</code>

名称	类型	是否必选	示例值	描述
Source	String	是	10.2.3.0/24	VPC边界防火墙访问控制策略中的源地址。 <ul style="list-style-type: none"> 当SourceType为 net 时, Source为源CIDR。例如: 10.2.3.0/24。 当SourceType为 group 时, Source为源地址簿名称。例如: db_group。
SourceType	String	是	net	VPC边界防火墙访问控制策略中的源地址类型。取值: <ul style="list-style-type: none"> net: 源网段 (CIDR) group: 源地址簿
VpcFirewallId	String	是	vfw-a42bbb7b887148c9****	VPC边界防火墙访问控制策略组ID。 <ul style="list-style-type: none"> 当VPC边界防火墙防护云企业网时, 策略组ID使用云企业网实例ID。例如: cen-ervw5jbw1234****。 当VPC边界防火墙防护高速通道时, 策略组ID使用VPC边界防火墙实例ID。例如: vfw-a42bbb748c91234****。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p> 说明 您可以调用DescribeVpcFirewallAclGroupList接口获取该ID。</p> </div>
Lang	String	否	zh	请求和接收消息的语言类型。取值: <ul style="list-style-type: none"> zh: 中文 en: 英文
DestPort	String	否	80	VPC边界防火墙访问控制策略中流量访问的目的端口。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p> 说明 当DestPortType为 port 时, 设置该参数。</p> </div>
DestPortType	String	否	net	VPC边界防火墙访问控制策略中流量访问的目的端口类型。取值: <ul style="list-style-type: none"> port: 端口 group: 端口地址簿

名称	类型	是否必选	示例值	描述
DestPortGroup	String	否	my_port_group	VPC边界防火墙访问控制策略中流量访问的目的端口地址簿名称。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px;"> <p>? 说明</p> <p>当DestPortType为 <code>group</code> 时，设置该参数。</p> </div>

返回数据

名称	类型	示例值	描述
AclUuid	String	00281255-d220-4db1-8f4f-c4df221ad84c	安全访问控制策略的唯一标识ID。
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	返回结果的请求ID。

示例

请求示例

```

http(s)://[Endpoint]/?Action=CreateVpcFirewallControlPolicy
&VpcFirewallId=vfw-a42bbb7b887148c9****
&AclAction=accept
&ApplicationName=ANY
&Description=demo_rule_1
&Destination=10.2.3.0/24
&DestinationType=net
&NewOrder=-1
&Proto=TCP
&Source=10.2.3.0/24
&SourceType=net
&<公共请求参数>

```

正常返回示例

XML 格式

```
<CreateVpcFirewallControlPolicyResponse>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
  <AclUuid>00281255-d220-4db1-8f4f-c4d*****</AclUuid>
</CreateVpcFirewallControlPolicyResponse>
```

JSON 格式


```
{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D",
  "AclUuid": "00281255-d220-4db1-8f4f-c4d*****"
}
```

错误码

访问[错误中心](#)查看更多错误码。

4.9.2. DescribeVpcFirewallControlPolicy

调用DescribeVpcFirewallControlPolicy接口查询指定的VPC边界防火墙所有的访问控制策略信息。


 **说明** 防护每个云企业网的VPC防火墙实例和防护每个高速通道的VPC防火墙实例使用不同的访问控制策略。



调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeVpcFirewallControlPolicy	系统规定参数。 取值： DescribeVpcFirewallControlPolicy 。
CurrentPage	String	是	1	分页查询时，显示的当前页的页码。 默认值为1。
PageSize	String	是	10	分页查询时，显示的每页数据的最大条数。 可设置值最大为50。

名称	类型	是否必选	示例值	描述
VpcFirewallId	String	是	vfw-a42bbb7b887148c9****	<p>VPC边界防火墙的访问控制策略组ID。您可调用DescribeVpcFirewallAclGroupList接口获取该ID。</p> <p>取值：</p> <ul style="list-style-type: none"> VPC边界防火墙防护云企业网时，策略组ID使用云企业网实例ID。 例如：cen-ervw0g12b5jbw**** VPC边界防火墙防护高速通道时，策略组ID使用VPC边界防火墙实例ID。 例如：vfw-a42bbb7b887148c9****
Lang	String	否	zh	<p>请求和接收消息的语言类型。</p> <p>取值：</p> <ul style="list-style-type: none"> zh：中文 en：英文
Source	String	否	10.0.1.0/24	<p>VPC边界防火墙访问控制策略中的访问源地址。支持使用模糊查询。</p> <p>取值：</p> <ul style="list-style-type: none"> 当SourceType为 net 时，Source为访问源CIDR地址。 例如：10.0.1.0/24 当SourceType为 group 时，Source为源地址簿名称。 例如：db_group 为空：表示查询所有访问控制源。 <p> 说明 SourceType（即源类型）不同，访问源地址的取值也不同。</p>


名称	类型	是否必选	示例值	描述
Destination	String	否	10.0.3.0	<p>VPC边界防火墙访问控制策略中的目的地址。支持模糊查询。</p> <p>取值：</p> <ul style="list-style-type: none"> 当DestinationType为 net 时，Destination为目的CIDR地址。 例如：10.0.3.0/24 当DestinationType为 domain 时，Destination为目的域名。 例如：aliyun.com 当DestinationType为 group 时，Destination为目的地址簿名称。 例如：db_group 为空：查询所有访问控制策略的目的地址。 <p> 说明 DestinationType（即目的类型）不同，目的地址的取值也不同。</p>
Description	String	否	test	<p>VPC边界防火墙访问控制策略的描述信息。支持模糊查询。</p> <p> 说明 为空表示查询所有访问控制策略的描述信息。</p>
Proto	String	否	TCP	<p>VPC边界防火墙访问控制策略中访问流量的协议类型。</p> <p>取值：</p> <ul style="list-style-type: none"> TCP UDP ICMP 为空（查询所有协议类型） ANY（查询所有协议类型）

名称	类型	是否必选	示例值	描述
AclAction	String	否	accept	VPC边界防火墙访问控制策略中设置的访问流量通过云防火墙的方式（动作）。 取值： <ul style="list-style-type: none"> • accept: 放行 • drop: 拒绝 • log: 观察 • 为空: 查询所有动作类型的访问控制策略

返回数据

名称	类型	示例值	描述
Policys	Array		VPC边界防火墙访问控制策略的信息。
AclAction	String	accept	VPC边界防火墙访问控制策略中设置的访问流量通过云防火墙的方式（动作）。 取值： <ul style="list-style-type: none"> • accept: 放行 • drop: 拒绝 • log: 观察
AclUuid	String	00281255-d220-4db1-8f4f-c4df221a****	VPC边界防火墙访问控制策略的唯一标识ID。
ApplicationId	String	10**	VPC边界防火墙访问控制策略中设置访问流量的应用的ID。

名称	类型	示例值	描述
ApplicationName	String	HTTP	VPC边界防火墙访问控制策略支持的应用类型。 取值： <ul style="list-style-type: none"> • HTTP • HTTPS • MySQL • SMTP • SMTPS • RDP • VNC • SSH • Redis • MQTT • MongoDB • Memcache • SSL • ANY（表示查询访问控制策略所有的应用类型）
Description	String	test	VPC边界防火墙访问控制策略的描述信息。
DestPort	String	80	VPC边界防火墙访问控制策略中访问流量的目的端口。
DestPortGroup	String	my_port_group	VPC边界防火墙访问控制策略中访问流量的目的端口地址簿名称。
DestPortGroupPorts	List	[80,443]	目的端口地址簿中包含的端口列表。
DestPortType	String	port	VPC边界防火墙访问控制策略中访问流量的目的端口类型。 取值： <ul style="list-style-type: none"> • port：端口 • group：端口地址簿

名称	类型	示例值	描述
Destination	String	10.0.3.0/24	<p>VPC边界防火墙访问控制策略中的目的地址。</p> <p>取值：</p> <ul style="list-style-type: none"> 当DestinationType为 <code>net</code> 时，Destination为目的CIDR地址。 例如：10.0.3.0/24 当DestinationType为 <code>domain</code> 时，Destination为目的域名。 例如：aliyuncs.com 当DestinationType为 <code>group</code> 时，Destination为目的地址簿名称。 例如：db_group <p> 说明 DestinationType（即目的类型）不同，目的地址的取值也不同。</p>
DestinationGroupCidrs	List	["10.0.4.0/24", "10.0.0.1/32"]	VPC边界防火墙访问控制策略中目的地址簿中的网段列表。
DestinationType	String	net	<p>VPC边界防火墙访问控制策略中目的地址的类型。</p> <p>取值：</p> <ul style="list-style-type: none"> <code>net</code>：目的网段 <code>group</code>：目的地址簿 <code>domain</code>：目的域名
Direction	String	in	<p>VPC边界防火墙访问控制策略的流量方向。</p> <p>取值：</p> <ul style="list-style-type: none"> <code>in</code>：外对内访问流量 <code>out</code>：内对外访问流量
HitTimes	Integer	100	VPC边界防火墙访问控制策略的命中次数。
Order	Integer	1	<p>VPC边界防火墙访问控制策略生效的优先级。</p> <p>优先级数字从1开始顺序递增，优先级数字越小，表示优先级越高。-1表示优先级最低。</p>

名称	类型	示例值	描述
Proto	String	TCP	VPC边界防火墙访问控制策略中访问流量的协议类型。 取值： <ul style="list-style-type: none"> TCP UDP ICMP ANY（表示查询所有协议类型）
Source	String	10.0.6.0/24	VPC边界防火墙访问控制策略中的访问源地址。 取值： <ul style="list-style-type: none"> 当SourceType为 net 时，Source为访问源CIDR地址。 例如：10.0.6.0/24 当SourceType为 group 时，Source为源地址簿名称。 例如：db_group <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p>🔍 说明 SourceType（即源类型）不同，访问源地址的取值也不同。</p> </div>
SourceGroupCidrs	List	["10.0.6.0/24", "10.0.0.2/32"]	VPC边界防火墙访问控制策略中，源地址簿中的网段列表。
SourceType	String	net	VPC边界防火墙访问控制策略中源地址类型。 取值： <ul style="list-style-type: none"> net：源网段地址（CIDR） group：源地址簿
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	结果的请求ID。
TotalCount	String	20	VPC边界防火墙访问控制策略的总数量。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeVpcFirewallControlPolicy
&CurrentPage=1
&PageSize=10
&VpcFirewallId=vfw-a42bbb7b887148c9****
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeVpcFirewallControlPolicyResponse>
  <TotalCount>1</TotalCount>
  <PageNo>1</PageNo>
  <PageSize>10</PageSize>
  <RequestId>A08BC58F-A83D-43EB-BC31-2F0D723929CC</RequestId>
  <Policys>
    <ApplicationName>HTTP</ApplicationName>
    <Description>11</Description>
    <HitTimes>0</HitTimes>
    <DestinationType>net</DestinationType>
    <SourceType>net</SourceType>
    <Proto>TCP</Proto>
    <Order>5</Order>
    <ApplicationId>27</ApplicationId>
    <DestPortType>port</DestPortType>
    <Source>10.1.1.1/32</Source>
    <DestPort>80/80</DestPort>
    <AclAction>accept</AclAction>
    <AclUuid>53d82f0e-9bf1-4761-ab3b-a070b4811234</AclUuid>
    <Destination>10.2.1.1/32</Destination>
  </Policys>
</DescribeVpcFirewallControlPolicyResponse>
```

JSON 格式

```
{
  "TotalCount":1,
  "PageNo":1,
  "PageSize":10,
  "RequestId":"A08BC58F-A83D-43EB-BC31-2F0D723929CC",
  "Policys":[
    {
      "DestinationGroupCidrs":[

      ],
      "SourceGroupCidrs":[

      ],
      "ApplicationName":"HTTP",
      "Description":"11",
      "HitTimes":0,
      "DestinationType":"net",
      "SourceType":"net",
      "Proto":"TCP",
      "Order":5,
      "ApplicationId":"27",
      "DestPortType":"port",
      "Source":"10.1.1.1/32",
      "DestPort":"80/80",
      "AclAction":"accept",
      "DestPortGroupPorts":[

      ],
      "AclUuid":"53d82f0e-9bf1-4761-ab3b-a070b4811234",
      "Destination":"10.2.1.1/32"
    }
  ]
}
```

错误码

访问[错误中心](#)查看更多错误码。

4.9.3. DescribeVpcFirewallPolicyPriorUsed

调用DescribeVpcFirewallPolicyPriorUsed接口查询指定VPC防火墙策略组访问控制策略优先级生效范围。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeVpcFirewallPolicyPriorUsed	系统规定参数。 取值：DescribeVpcFirewallPolicyPriorUsed。
VpcFirewallId	String	是	vfw-a42bbb7b887148c9****	VPC边界防火墙的访问控制策略组ID。您可调用DescribeVpcFirewallAclGroupList接口获取该ID。 取值： <ul style="list-style-type: none"> VPC边界防火墙防护云企业网时，策略组ID使用云企业网实例ID。 例如cen-ervw0g12b5jbw**** VPC边界防火墙防护高速通道时，策略组ID使用VPC边界防火墙实例ID。 例如vfw-a42bbb7b887148c9****
Lang	String	否	zh	请求和接收消息的语言类型。 取值： <ul style="list-style-type: none"> zh：中文 en：英文

返回数据

名称	类型	示例值	描述
End	Integer	150	访问控制策略生效的优先级最低值。
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	结果的请求ID。
Start	Integer	1	访问控制策略生效的优先级最高值。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeVpcFirewallPolicyPriorUsed
&VpcFirewallId=vfw-a42bbb7b887148c9****
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeVpcFirewallPolicyPriorUsedResponse>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
  <Start>1</Start>
  <End>150</End>
</DescribeVpcFirewallPolicyPriorUsedResponse>
```

JSON 格式

```
{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D",
  "Start": 1,
  "End": 150
}
```

错误码

访问[错误中心](#)查看更多错误码。

4.9.4. DescribeVpcFirewallAclGroupList

调用DescribeVpcFirewallAclGroupList接口获取VPC防火墙所有访问控制策略组信息。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
----	----	------	-----	----

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeVpcFirewallAclGroupList	需要执行的操作。 取值： DescribeVpcFirewallAclGroupList 。
Lang	String	否	zh	请求和接收消息的语言类型。 <ul style="list-style-type: none"> zh: 中文 en: 英文
FirewallConfigureStatus	String	否	configured	VPC防火墙的配置状态。 <ul style="list-style-type: none"> notconfigured: VPC边界防火墙未配置（即未创建防火墙）。 configured: VPC边界防火墙已配置（即已创建了防火墙）。 不填表示查询所有VPC防火墙配置状态对应的策略组。
CurrentPage	String	否	1	分页查询时，显示的当前页的页码。 默认值为1。
PageSize	String	否	10	分页查询时，显示的每页数据的最大条数。 可设置值最大为50。

返回数据

名称	类型	示例值	描述
AclGroupList	Array		VPC防火墙访问控制策略组的信息。

名称	类型	示例值	描述
AclGroupId	String	vfw-a42bbb7b887148c9****	VPC边界防火墙的访问控制策略组ID。您可调用DescribeVpcFirewallAclGroupList接口获取该ID。 取值： <ul style="list-style-type: none"> VPC边界防火墙防护云企业网时，策略组ID使用云企业网实例ID。 例如：cen-ervw0g12b5jbw**** VPC边界防火墙防护高速通道时，策略组ID使用VPC边界防火墙实例ID。 例如：vfw-a42bbb7b887148c9****
AclGroupName	String	group_test	VPC边界防火墙的访问控制策略组名称。 <ul style="list-style-type: none"> VPC边界防火墙防护云企业网时，策略组名称使用云企业网名称。 VPC边界防火墙防护高速通道时，策略组名称使用VPC边界防火墙名称。
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	结果的请求ID。
TotalCount	Integer	1	VPC防火墙访问控制策略组的总数量。

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribeVpcFirewallAclGroupListResponse>
  <TotalCount>1</TotalCount>
  <AclGroupList>
    <AclGroupId>vfw-a42bbb7b887148c9****</AclGroupId>
    <AclGroupName>group_test</AclGroupName>
  </AclGroupList>
</DescribeVpcFirewallAclGroupListResponse>
```

JSON 格式


```
{"TotalCount":1,"AclGroupList":[{"AclGroupId":"vfw-a42bbb7b887148c9****","AclGroupName":"group_test"}]}
```

错误码

访问[错误中心](#)查看更多错误码。

4.9.5. ModifyVpcFirewallControlPolicy

调用ModifyControlPolicy接口修改指定VPC防火墙策略组的访问控制策略的配置信息。

 **说明** 防护每个云企业网的VPC防火墙实例和防护每个高速通道的VPC防火墙实例使用不同的访问控制策略。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyVpcFirewallControlPolicy	需要执行的操作。 取值： ModifyVpcFirewallControlPolicy 。
AclAction	String	是	accept	安全访问控制策略中访问流量通过云防火墙的方式（动作）。 取值： <ul style="list-style-type: none"> accept：放行 drop：拒绝 log：观察
AclUuid	String	是	00281255-d220-4db1-8f4f-c4df221ad84c	访问控制策略的唯一标识ID。 修改访问控制策略时，需要提供该策略的唯一标识ID。您可调用DescribeVpcFirewallControlPolicy接口获取该ID。

名称	类型	是否必选	示例值	描述
ApplicationName	String	是	HTTP	访问控制策略支持的应用类型。 取值： <ul style="list-style-type: none"> • ANY • FTP • HTTP • HTTPS • MySQL • SMTP • SMTPS • RDP • VNC • SSH • Redis • MQTT • MongoDB • Memcache • SSL • ANY（表示查询所有类型的应用）
Description	String	是	test	访问控制策略的描述信息。
Destination	String	是	10.2.3.0/24	访问控制策略中的目的地址。 <ul style="list-style-type: none"> • 当DestinationType为 net 时，Destination为目的CIDR地址。 例如：10.2.3.0/24 • 当DestinationType为 group 时，Destination为目的地址簿名称。 例如：db_group • 当DestinationType为 domain 时，Destination为目的域名。 例如：*.aliyuncs.com
DestinationType	String	是	net	访问控制策略中的目的地址类型。 取值： <ul style="list-style-type: none"> • net：目的网段（CIDR地址） • group：目的地址簿 • domain：目的域名

名称	类型	是否必选	示例值	描述
Proto	String	是	TCP	访问控制策略中流量访问的安全协议类型。 取值： <ul style="list-style-type: none"> ANY（表示查询所有协议类型） TCP UDP ICMP
Source	String	是	10.2.4.0/24	访问控制策略中的源地址。 取值： <ul style="list-style-type: none"> 当SourceType为 net 时，Source为源CIDR地址。 例如：10.2.4.0/24 当SourceType为 group 时，Source为源地址簿名称。 例如：db_group
SourceType	String	是	net	访问控制策略中的源地址类型。 取值： <ul style="list-style-type: none"> net：源网段（CIDR地址） group：源地址簿
VpcFirewallId	String	是	vfw-a42bbb7b887148c9****	VPC边界防火墙的ACL策略组ID。您可调用DescribeVpcFirewallAclGroupList接口获取该ID。 <ul style="list-style-type: none"> VPC边界防火墙防护云企业网时，策略组ID使用云企业网实例ID。 例如cen-ervw0g12b5jbw**** VPC边界防火墙防护高速通道时，策略组ID使用VPC边界防火墙实例ID。 例如vfw-a42bbb7b887148c9****
Lang	String	否	zh	请求和接收消息的语言类型。 取值： <ul style="list-style-type: none"> zh：中文 en：英文

名称	类型	是否必选	示例值	描述
DestPort	String	否	80	访问控制策略中访问流量的目的端口。
DestPortType	String	否	port	安全访问控制策略中访问流量的目的端口类型。 <ul style="list-style-type: none"> port: 端口 group: 端口地址簿
DestPortGroup	String	否	my_port_group	访问控制策略中访问流量的目的端口地址簿名称。

返回数据

名称	类型	示例值	描述
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	结果的请求ID。

示例

请求示例

```

http(s)://[Endpoint]/?Action=ModifyVpcFirewallControlPolicy
&VpcFirewallId=vfw-a42bbb7b887148c9****
&AclAction=accept
&AclUuid=00281255-d220-4db1-8f4f-c4df221ad84c
&ApplicationName=ANY
&Description=demo_rule_1
&Destination=10.2.3.0/24
&DestinationType=net
&Proto=TCP
&Source=10.2.4.0/24
&SourceType=net
&<公共请求参数>

```

正常返回示例

XML 格式

```

<ModifyVpcFirewallControlPolicyResponse>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
</ModifyVpcFirewallControlPolicyResponse>

```

JSON 格式

```
{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}
```

错误码

访问[错误中心](#)查看更多错误码。

4.9.6. ModifyVpcFirewallControlPolicyPosition

调用ModifyVpcFirewallControlPolicyPosition接口修改指定VPC防火墙策略组访问控制策略的优先级。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyVpcFirewallControlPolicyPosition	系统规定参数。 取值：ModifyVpcFirewallControlPolicyPosition。
NewOrder	String	是	1	访问控制策略优先级修改后，该策略的新优先级。
OldOrder	String	是	5	访问控制策略优先级修改前，该策略的原优先级。
VpcFirewallId	String	是	vfw-a42bbb7b887148c9****	VPC边界防火墙的访问控制策略组ID。您可调用DescribeVpcFirewallAclGroupList接口获取该ID。 取值： <ul style="list-style-type: none"> VPC边界防火墙防护云企业网时，策略组ID使用云企业网实例ID。 例如cen-ervw0g12b5jbw**** VPC边界防火墙防护高速通道时，策略组ID使用VPC边界防火墙实例ID。 例如vfw-a42bbb7b887148c9****

名称	类型	是否必选	示例值	描述
Lang	String	否	zh	请求和接收消息的语言类型。 取值： <ul style="list-style-type: none"> zh: 中文 en: 英文

返回数据

名称	类型	示例值	描述
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125EEB1	结果的请求ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyVpcFirewallControlPolicyPosition
&VpcFirewallId=vfw-a42bbb7b887148c9****
&NewOrder=1
&OldOrder=5
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ModifyVpcFirewallControlPolicyPositionResponse>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125EEB1</RequestId>
</ModifyVpcFirewallControlPolicyPositionResponse>
```

JSON 格式

```
{
  "RequestId": "850A84D6-0DE4-4797-A1E8-00090125EEB1"
}
```

错误码

访问[错误中心](#)查看更多错误码。

4.9.7. ResetVpcFirewallRuleHitCount

调用ResetVpcFirewallRuleHitCount接口，将指定的VPC防火墙策略组访问控制策略的命中计数清零。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ResetVpcFirewallRuleHitCount	系统规定的参数。 取值：ResetVpcFirewallRuleHitCount。
AclUuid	String	是	00281255-d220-4db1-8f4f-c4df221ad84c	访问控制策略的唯一标识ID。 删除访问控制策略时，需要提供该策略的唯一标识ID。您可调用DescribeVpcFirewallControlPolicy接口获取该ID。
Lang	String	否	zh	请求和接收消息的语言类型。 取值： <ul style="list-style-type: none"> zh：中文 en：英文

返回数据

名称	类型	示例值	描述
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	结果的请求ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ResetVpcFirewallRuleHitCount
&AclUuid=00281255-d220-4db1-8f4f-c4df221a1234
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ResetVpcFirewallRuleHitCountResponse>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
</ResetVpcFirewallRuleHitCountResponse>
```

JSON 格式


```
{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}
```

错误码

访问[错误中心](#)查看更多错误码。

4.9.8. DeleteVpcFirewallControlPolicy

调用DeleteVpcFirewallControlPolicy接口删除指定VPC防火墙策略组的访问控制策略。

 **说明** 防护每个云企业网的VPC防火墙实例和防护每个高速通道的VPC防火墙实例使用不同的访问控制策略。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteVpcFirewallControlPolicy	需要执行的操作。 取值：DeleteVpcFirewallControlPolicy。
AclUuid	String	是	00281255-d220-4db1-8f4f-c4df2214****	VPC边界防火墙访问控制策略的唯一标识ID。 删除安全访问控制策略时，需要提供该策略的唯一标识ID。您可调用DescribeVpcFirewallControlPolicy接口获取该ID。

名称	类型	是否必选	示例值	描述
VpcFirewallId	String	是	vfw-a42bbb7b887148c91****	VPC边界防火墙的访问控制策略组ID。您可调用DescribeVpcFirewallAclGroupList接口获取该ID。 取值： <ul style="list-style-type: none"> VPC边界防火墙防护云企业网时，策略组ID使用云企业网实例ID。 例如：cen-ervw0g12b5jbw**** VPC边界防火墙防护高速通道时，策略组ID使用VPC边界防火墙实例ID。 例如：vfw-a42bbb7b887148c9****
Lang	String	否	zh	请求和接收消息的语言类型。 <ul style="list-style-type: none"> zh：中文 en：英文

返回数据

名称	类型	示例值	描述
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	结果的请求ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteVpcFirewallControlPolicy
&VpcFirewallId=vfw-a42bbb7b887148c9****
&AclUuid=00281255-d220-4db1-8f4f-c4df221ad84c
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DeleteVpcFirewallControlPolicyResponse>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
</DeleteVpcFirewallControlPolicyResponse>
```

JSON 格式

```
{  
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"  
}
```

错误码

访问[错误中心](#)查看更多错误码。

5.地址簿API

5.1. AddAddressBook

调用AddAddressBook接口添加安全访问控制地址簿，包括IP地址簿、ECS标签地址簿、端口地址簿和域名地址簿。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	AddAddressBook	系统规定参数。取值：AddAddressBook。
Description	String	是	DEMO地址簿	地址簿的描述信息。
GroupName	String	是	demo_address_book	地址簿的名称。
GroupType	String	是	ip	地址簿的类型，可选值包括： <ul style="list-style-type: none"> ip：IP地址簿 domain：域名地址簿 port：端口地址簿 tag：ECS标签地址簿
AddressList	String	否	1.2.3.4/32, 1.2.3.0/24	地址簿的地址列表，多个地址间用英文逗号分隔。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p> 说明 当GroupType为ip、port或domain时必须设置。</p> </div> <ul style="list-style-type: none"> 当GroupType为ip时，地址列表中填写IP地址。例如：1.2.3.4/32, 1.2.3.0/24 当GroupType为port时，地址列表中填写端口或端口范围。例如：80, 100/200 当GroupType为domain时，地址列表中填写域名。例如： demo1.aliyun.com, demo2.aliyun.com

名称	类型	是否必选	示例值	描述
AutoAddTagEcs	String	否	1	是否自动添加新匹配标签的ECS公网IP到地址簿。 <ul style="list-style-type: none"> 1: 表示自动添加 0: 表示不自动添加
Lang	String	否	zh	请求和接收消息的语言类型。 <ul style="list-style-type: none"> zh: 中文 en: 英文
SourceIp	String	否	1.2.3.4	访问者源IP地址。
TagList.N.TagKey	String	否	key1	待匹配的ECS标签Key。
TagList.N.TagValue	String	否	value1	待匹配的ECS标签值。
TagRelation	String	否	and	待匹配的多个ECS标签间的关系。 <ul style="list-style-type: none"> and: 多个标签间为“与”关系，即同时匹配多个标签的ECS公网IP才会被加入地址簿。 or: 多个标签间为“或”关系，即只要匹配一个标签的ECS公网IP就会被加入地址簿。

返回数据

名称	类型	示例值	描述
GroupUuid	String	f04ac7ce-628b-4cb7-be61-310222b718e8	添加成功后返回的地址簿唯一标识ID。
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	结果的请求ID。

示例

请求示例

```

http(s)://[Endpoint]/?Action=AddAddressBook
&Description=DEMO地址簿
&GroupName=demo_address_book
&GroupType=ip
&AddressList=1.2.3.4/32,1.2.3.0/24
&<公共请求参数>

```

正常返回示例

XML 格式

```

<AddAddressBook>
  <RequestId>B2841452-CB8D-4F7D-B247-38E1CF7334F8</RequestId>
  <GroupUuid>0580bbd0-24cd-47ae-9e5a-f5a099251e32</GroupUuid>
</AddAddressBook>

```

JSON 格式

```

{
  "RequestId": "B2841452-CB8D-4F7D-B247-38E1CF7334F8",
  "GroupUuid": "0580bbd0-24cd-47ae-9e5a-f5a099251e32"
}

```

错误码

访问[错误中心](#)查看更多错误码。

5.2. DeleteAddressBook

调用DeleteAddressBook接口删除安全访问控制的地址簿。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteAddressBook	系统规定参数。取值：DeleteAddressBook。

名称	类型	是否必选	示例值	描述
GroupUuid	String	是	0657ab9d-fe8b-4174-b2a6-6baf358ea4ad	地址簿的唯一标识ID。 删除安全访问控制的地址簿，需要提供该地址簿的唯一标识ID，该ID可调用DescribeAddressBook接口获取。
Lang	String	否	zh	请求和接收消息的语言类型。 <ul style="list-style-type: none"> zh: 中文 en: 英文
SourceIp	String	否	1.2.3.4	访问者源IP地址。

返回数据

名称	类型	示例值	描述
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	结果的请求ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteAddressBook
&GroupUuid=0657ab9d-fe8b-4174-b2a6-6baf358ea4ad
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DeleteAddressBook>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125EEB1</RequestId>
</DeleteAddressBook>
```

JSON 格式

```
{
  "RequestId": "850A84D6-0DE4-4797-A1E8-00090125EEB1"
}
```

错误码

访问[错误中心](#)查看更多错误码。


5.3. ModifyAddressBook

调用ModifyAddressBook接口修改访问控制策略中设置的地址簿。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyAddressBook	要执行的操作。取值： ModifyAddressBook 。
Description	String	是	DEMO地址簿	地址簿的描述信息。
GroupName	String	是	demo_address_book	地址簿的名称。
GroupUuid	String	是	0657ab9d-fe8b-4174-b2a6-6baf358ea4ad	地址簿的唯一标识ID。 <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 5px;"> <p> 说明 修改访问控制策略中设置的地址簿信息，需要提供该地址簿的唯一标识ID，该ID可用DescribeAddressBook接口查询。</p> </div>
SourceIp	String	否	1.2.3.4	访问者源IP地址。
Lang	String	否	zh	请求和接收消息的语言类型。取值： <ul style="list-style-type: none"> • zh: 中文 • en: 英文

名称	类型	是否必选	示例值	描述
AddressList	String	否	1.1.1.1/32, 2.2.2.0/24	<p>地址簿中的地址列表，多个地址间用英文逗号分隔。当GroupType为ip、port或domain时，您必须配置此参数。</p> <ul style="list-style-type: none"> 当GroupType为ip时，地址列表中填写IP地址，例如： 1.2.3.4/32, 1.2.3.0/24。 当GroupType为port时，地址列表中填写端口或端口范围，例如： 80/80, 100/200。 当GroupType为domain时，地址列表中填写域名，例如： demo1.aliyun.com, demo2.aliyun.com。
AutoAddTagEcs	String	否	1	<p>是否自动添加新匹配标签的ECS公网IP到地址簿。取值：</p> <ul style="list-style-type: none"> 1：表示自动添加 0：表示不自动添加
TagRelation	String	否	and	<p>多个ECS标签间的关系。取值：</p> <ul style="list-style-type: none"> and：多个标签间为“与”关系，即同时匹配多个标签的ECS公网IP才会被加入地址簿。 or：多个标签间为“或”关系，即只要匹配一个标签的ECS公网IP就会被加入地址簿。
TagList.N.TagKey	String	否	key1	待匹配的ECS标签Key。
TagList.N.TagValue	String	否	value1	待匹配的ECS标签值。

返回数据

名称	类型	示例值	描述
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	结果的请求ID。

示例

请求示例

```

http(s)://[Endpoint]/?Action=ModifyAddressBook
&GroupUuid=0657ab9d-fe8b-4174-b2a6-6baf358ea4ad
&Description=DEMO地址簿
&GroupName=demo_address_book
&GroupType=ip
&AddressList=1.1.1.1/32,2.2.2.0/24
&<公共请求参数>

```

正常返回示例

XML 格式

```

<ModifyAddressBookResponse>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
</ModifyAddressBookResponse>

```

JSON 格式

```

{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}

```

错误码

访问[错误中心](#)查看更多错误码。

5.4. DescribeAddressBook

调用DescribeAddressBook接口查询云防火墙访问控制策略地址簿的详细信息。

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeAddressBook	要执行的操作。取值： DescribeAddressBook 。
SourceIp	String	否	1.2.3.4	访问者源IP地址。

名称	类型	是否必选	示例值	描述
Lang	String	否	zh	请求和接收消息的语言类型。取值： <ul style="list-style-type: none"> zh: 中文 en: 英文
CurrentPage	String	否	1	分页查询时的当前页的页码。默认值为1。
PageSize	String	否	50	分页查询时每页显示数据条数。可设置的最大值为50。
Query	String	否	1.2.3.0	搜索条件，输入待查询地址簿信息。
GroupType	String	否	ip	地址簿的类型。取值： <ul style="list-style-type: none"> ip: IP地址簿 domain: 域名地址簿 port: 端口地址簿 tag: ECS标签地址簿
ContainPort	String	否	80	查询包含指定端口的地址簿，仅当GroupType为port时有效。

返回数据

名称	类型	示例值	描述
Acls	Array		地址簿信息。
AddressList	List	["1.2.3.4/32", "0.0.0.0/0"]	地址簿的地址列表信息。
AddressListCount	Integer	2	地址簿中包含地址的个数。
AutoAddTagEcs	Integer	1	是否自动添加新匹配标签的ECS公网IP到地址簿。取值： <ul style="list-style-type: none"> 1: 表示自动添加 0: 表示不自动添加
Description	String	DEMO地址簿	地址簿的描述信息。

名称	类型	示例值	描述
Global	Integer	0	地址簿是否是全局地址簿。取值： <ul style="list-style-type: none"> 1: 是全局地址簿 0: 非全局地址簿
GroupName	String	demo_address_book	地址簿的名称。
GroupType	String	ip	地址簿的类型。取值： <ul style="list-style-type: none"> ip: IP地址簿 domain: 域名地址簿 port: 端口地址簿 tag: ECS标签地址簿
GroupUuid	String	f04ac7ce-628b-4cb7-be61-310222b718e8	地址簿的唯一标识ID。
ReferenceCount	Integer	3	地址簿被引用次数。
TagList	Array		地址簿支持自动添加的待匹配ECS标签信息。
TagKey	String	key1	待匹配的ECS标签Key。
TagValue	String	value1	待匹配的ECS标签值。
TagRelation	String	and	多个ECS标签间的关系。取值： <ul style="list-style-type: none"> and: 多个标签间为“与”关系，即同时匹配多个标签的ECS公网IP才会被加入地址簿。 or: 多个标签间为“或”关系，即只要匹配一个标签的ECS公网IP就会被加入地址簿。
PageNo	String	1	当前页的页码。
PageSize	String	10	每页显示数据条数。
RequestId	String	B36F150A-1E27-43AA-B72C-D2AC712F09DA	结果的请求ID。
TotalCount	String	100	地址簿的总数量。

示例

请求示例

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

正常返回示例

XML 格式

```
<DescribeAddressBookResponse>
  <TotalCount>123</TotalCount>
  <PageSiNo>1</PageSiNo>
  <PageSize>1</PageSize>
  <RequestId>B36F150A-1E27-43AA-B72C-D2AC712F09DA</RequestId>
  <Acls>
    <Description>9-3IP地址簿</Description>
    <GroupType>ip</GroupType>
    <AddressList>1.2.3.4/32</AddressList>
    <AddressList>0.0.0.0/0</AddressList>
    <GroupName>9-3IP地址簿</GroupName>
    <AutoAddTagEcs>0</AutoAddTagEcs>
    <TagValue></TagValue>
    <TagRelation></TagRelation>
    <ReferenceCount>0</ReferenceCount>
    <TagKey></TagKey>
    <AddressListCount>2</AddressListCount>
    <GroupUuid>a3c5e-018e-4c08-bea8-eafc95d1a54e</GroupUuid>
    <Global>0</Global>
  </Acls>
</DescribeAddressBookResponse>
```

JSON 格式

```
{
  "TotalCount":123,
  "PageSiNo": 1,
  "PageSize": 1,
  "RequestId":"B36F150A-1E27-43AA-B72C-D2AC712F09DA",
  "Acls":[
    {
      "Description":"9-3IP地址簿",
      "GroupType":"ip",
      "AddressList":[
        "1.2.3.4/32",
        "0.0.0.0/0"
      ],
      "GroupName":"9-3IP地址簿",
      "AutoAddTagEcs":0,
      "TagValue":"",
      "TagRelation":"",
      "TagList":[

      ],
      "ReferenceCount":0,
      "TagKey":"",
      "AddressListCount":2,
      "GroupUuid":"a3c5e-018e-4c08-bea8-eafc95d1a54e",
      "Global":0
    }
  ]
}
```

错误码

访问[错误中心](#)查看更多错误码。