

ALIBABA CLOUD

Alibaba Cloud

云防火墙
API参考

文档版本：20220602

 阿里云

法律声明

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

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

通用约定

格式	说明	样例
 危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 警告 重启操作将导致业务中断，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击 确定 。
Courier字体	命令或代码。	执行 <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	09
3.公共参数	11
4.访问控制API	13
4.1. AddControlPolicy	13
4.2. DescribeControlPolicy	21
4.3. DescribeDomainResolve	30
4.4. DescribePolicyPriorUsed	32
4.5. ModifyControlPolicy	34
4.6. ModifyControlPolicyPosition	38
4.7. DeleteControlPolicy	40
4.8. 严格模式	42
4.8.1. DescribePolicyAdvancedConfig	42
4.8.2. ModifyPolicyAdvancedConfig	43
4.9. VPC边界防火墙	45
4.9.1. CreateVpcFirewallControlPolicy	45
4.9.2. DescribeVpcFirewallControlPolicy	49
4.9.3. DescribeVpcFirewallPolicyPriorUsed	56
4.9.4. DescribeVpcFirewallAclGroupList	58
4.9.5. ModifyVpcFirewallControlPolicy	61
4.9.6. ModifyVpcFirewallControlPolicyPosition	65
4.9.7. ResetVpcFirewallRuleHitCount	67
4.9.8. DeleteVpcFirewallControlPolicy	69
4.9.9. CreateVpcFirewallConfigure	70
4.9.10. DescribeVpcFirewallDetail	73
4.9.11. DescribeVpcFirewallList	79

4.9.12. DeleteVpcFirewallConfigure	86
4.9.13. ModifyVpcFirewallConfigure	88
4.9.14. ModifyVpcFirewallSwitchStatus	91
4.9.15. BatchCopyVpcFirewallControlPolicy	93
4.9.16. CreateVpcFirewallCenConfigure	95
4.9.17. DeleteVpcFirewallCenConfigure	97
4.9.18. DescribeVpcFirewallCenList	99
4.9.19. DescribeVpcFirewallCenDetail	106
4.9.20. ModifyVpcFirewallCenConfigure	111
4.9.21. ModifyVpcFirewallCenSwitchStatus	113
4.9.22. DescribeVpcFirewallDefaultIPSConfig	115
4.9.23. ModifyVpcFirewallDefaultIPSConfig	117
5.地址簿API	120
5.1. AddAddressBook	120
5.2. DeleteAddressBook	123
5.3. ModifyAddressBook	124
5.4. DescribeAddressBook	127
6.多账号管控	132
6.1. ModifyInstanceMemberAttributes	132
6.2. DescribeInstanceMembers	133
6.3. DeleteInstanceMembers	136
6.4. AddInstanceMembers	137

1.API概览

本文汇总了云防火墙服务所有可调用的API。

防火墙开关

API	描述
DescribeAssetList	获取云防火墙防护的资产信息。
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	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	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。
CreateVpcFirewallConfigure	创建VPC边界防火墙（防护通过高速通道连接的两个VPC之间的流量）。
DescribeVpcFirewallDetail	查询指定VPC边界防火墙（防护通过高速通道连接的两个VPC之间的流量）的详细信息。
DescribeVpcFirewallList	分页查询VPC边界防火墙（防护通过高速通道连接的两个VPC之间的流量）的信息。
DeleteVpcFirewallConfigure	删除指定VPC边界防火墙（防护通过高速通道连接的两个VPC之间流量）。
ModifyVpcFirewallConfigure	修改指定VPC边界防火墙（防护通过高速通道连接的两个VPC之间的流量）的配置信息。
ModifyVpcFirewallSwitchStatus	修改指定VPC边界防火墙（防护通过高速通道连接的两个VPC之间的流量）的开关状态。
BatchCopyVpcFirewallControlPolicy	从源VPC边界防火墙策略组拷贝所有策略到目标VPC边界防火墙策略组。
CreateVpcFirewallCenConfigure	创建VPC边界防火墙（防护云企业网内的网络实例和指定VPC之间的互访流量）。
DeleteVpcFirewallCenConfigure	删除指定VPC边界防火墙（防护云企业网内的网络实例和指定VPC之间的互访流量）。
DescribeVpcFirewallCenList	分页查询VPC边界防火墙（防护云企业网内的网络实例和指定VPC之间的互访流量）的信息。
DescribeVpcFirewallCenDetail	查询指定VPC边界防火墙（防护云企业网内的网络实例和指定VPC之间的互访流量）的详细信息。
ModifyVpcFirewallCenConfigure	修改指定VPC边界防火墙（防护云企业网内的网络实例和指定VPC之间的互访流量）的配置信息。
ModifyVpcFirewallCenSwitchStatus	修改指定VPC边界防火墙（防护云企业网内的网络实例和指定VPC之间的互访流量）的开关状态。
DescribeVpcFirewallDefaultIPSConfig	获取指定VPC边界防火墙的入侵防御配置信息。
ModifyVpcFirewallDefaultIPSConfig	修改指定VPC边界防火墙的入侵防御配置信息。

地址簿

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。

多账号管控

API	描述
ModifyInstanceMemberAttributes	更新云防火墙成员账号信息。
DescribeInstanceMembers	获取云防火墙成员账号信息。
DeleteInstanceMembers	删除云防火墙成员账号。
AddInstanceMembers	添加云防火墙成员账号。

攻击防护

API	描述
DescribeRiskEventGroup	获取入侵防御事件的详细数据。

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=CT9X0VtwR86fNWSn
sc6v8YGOjuE%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：Singapore。
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请求访问到的资源拥有者账户，即登录用户名。

示例

```
https://cloudfw.Singapore.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接口，添加访问控制策略。

使用说明

您可以使用本接口创建一条对经过云防火墙流量放行、拒绝或观察的策略。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	AddControlPolicy	系统规定参数。取值： AddControlPolicy 。
SourceIp	String	否	192.0.XX.XX	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（默认）：中文en：英文
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	否	ANY	<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_No_Cert • 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
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。
Destination	String	是	192.0.XX.XX/24	<p>访问控制策略中的目的地址段。</p> <p>取值：</p> <ul style="list-style-type: none"> 当DestinationType为net时，Destination为目的的CIDR。 例如：1.2.XX.XX/24 当DestinationType为group时，Destination为目的的地址簿名称。 例如：db_group 当DestinationType为domain时，Destination为目的的域名。 例如：*.aliyuncs.com 当DestinationType为location时，Destination为目的的区域。 例如：["BJ11", "ZB"]
DestinationType	String	是	net	<p>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地址） group：目的地址簿 domain：目的域名 location：目的区域

名称	类型	是否必选	示例值	描述
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
Proto	String	是	ANY	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	192.0.XX.XX/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：1.1.XX.XX/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
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。
DestPortType	String	否	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	是否必选	示例值	描述
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。  说明 DestPortType设置为group时，您需要设置目的端口地址簿名称。
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
IpVersion	String	否	6	支持的IP地址版本。 取值： <ul style="list-style-type: none">• 4：表示IPv4地址• 6：表示IPv6地址

名称	类型	是否必选	示例值	描述
ApplicationNameList.N	String	否	["ANY"]	<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_No_Cert • 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，ApplicationNameList支持选择以上所有应用类型，使用 ["HTTP", "HTTPS",] 格式表示；Proto为UDP、ICMP或ANY协议类型时，ApplicationNameList仅支持选择ANY。当ApplicationNameList和ApplicationName同时传值时，以ApplicationNameList为准。</p>

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
- 中国台湾: TW
- 中国香港特别行政区: HK
- 中国澳门特别行政区: 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。

名称	类型	示例值	描述
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
&SourceIp=192.0.XX.XX
&Lang=zh
&AclAction=accept
&ApplicationName=ANY
&Description=放行流量
&DestPort=80
&Destination=192.0.XX.XX/24
&DestinationType=net
&Direction=in
&Proto=ANY
&Source=192.0.XX.XX/24
&SourceType=net
&NewOrder=1
&DestPortType=port
&DestPortGroup=my_port_group
&Release=true
&IpVersion=6
&ApplicationNameList=["\\\"ANY\\\""]
&公共请求参数

```

正常返回示例

XML 格式

```

HTTP/1.1 200 OK
Content-Type:application/xml
<AddControlPolicyResponse>
  <AclUuid>00281255-d220-4db1-8f4f-c4df221ad84c</AclUuid>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
</AddControlPolicyResponse>

```

JSON 格式

```

HTTP/1.1 200 OK
Content-Type:application/json
{
  "AclUuid" : "00281255-d220-4db1-8f4f-c4df221ad84c",
  "RequestId" : "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}

```

4.2. DescribeControlPolicy

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

使用说明

本接口一般用于分页查询访问控制策略的信息。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeControlPolicy	系统规定参数。取值： DescribeControlPolicy 。
SourceIp	String	否	192.0.XX.XX	访问源的IP地址。
Lang	String	否	zh	接收消息的语言类型。取值： <ul style="list-style-type: none">zh（默认）：中文en：英文
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。
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。

名称	类型	是否必选	示例值	描述
Source	String	否	192.0.XX.XX	<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 <code>net</code> 时，访问源为IP/CIDR地址。例如：10.0.1.0/24。 当SourceType为 <code>group</code> 时，访问源为源地址簿名称。例如：<code>db_group</code>为空（表示查询所有访问控制源）。 当SourceType为 <code>location</code> 时，访问源为源区域。例如：北京或 <code>beijing</code>（支持使用中文或英文进行查询）。 <p> 说明 不设置该参数表示查询所有类型的访问源。</p>
Destination	String	否	192.0.XX.XX	<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 <code>net</code> 时，目的地址为IP/CIDR地址。例如：10.0.3.0/24。 当DestinationType为 <code>domain</code> 时，目的地址为域名。例如：<code>aliyun</code>。 当DestinationType为 <code>group</code> 时，目的地址为地址簿的名称。例如：<code>db_group</code>。 当DestinationType为 <code>location</code> 时，目的地址为目的区域。例如：北京或 <code>beijing</code>（支持使用中文或英文进行查询）。 <p> 说明 不设置该参数表示查询所有类型的目的地址。</p>
Description	String	否	test	<p>访问控制策略的描述信息。支持模糊查询。</p> <p> 说明 不设置该参数表示查询所有策略的描述信息。</p>

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（表示所有协议类型） <p> 说明 不设置该参数表示查询所有协议类型。</p>
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 <p> 说明 不设置该参数表示查询所有的动作类型。</p>
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-c4df221a****	访问控制策略的唯一标识ID。
IpVersion	String	否	6	支持的IP地址版本。取值： <ul style="list-style-type: none"> 4（默认）：代表IPv4地址 6：代表IPv6地址

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。

名称	类型	示例值	描述
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2****	结果的请求ID。
TotalCount	String	100	访问控制策略的总数量。
Policys	Array of Datatem		访问控制策略的信息。
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
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。
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
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（表示所有应用类型）
HitTimes	Long	100	访问控制策略的命中次数。

名称	类型	示例值	描述
Description	String	test	访问控制策略的描述信息。
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。
DnsResultTime	Long	1579261141	DNS解析的时间戳。使用秒级时间戳格式表示。
DnsResult	String	192.0.XX.XX,192.0.XX.XX	DNS解析结果。
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
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。

名称	类型	示例值	描述
Destination	String	192.0.XX.XX/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：192.0.XX.XX/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"]。
HitLastTime	Long	1579261141	最新命中时间戳。使用秒级时间戳格式表示。
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。
AclUuid	String	00281255-d220-4db1-8f4f-c4df221a****	访问控制策略的唯一标识ID。
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
Source	String	192.0.XX.XX/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：192.0.XX.XX/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"]。
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

名称	类型	示例值	描述
DestPort	String	80	访问控制策略中访问流量的目的端口。
IpVersion	Integer	6	支持的IP地址版本。 取值： <ul style="list-style-type: none"> • 4：代表IPv4地址 • 6：代表IPv6地址
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
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
ApplicationId	String	10***	访问控制策略中设置访问流量的应用ID。
DestinationGroupCidrs	Array of String	["192.0.XX.XX/24", "192.0.XX.XX/32"]	访问控制策略中的目的地址簿中的网段列表。
DestPortGroupPorts	Array of String	[80,443]	目的端口地址簿中包含的端口列表。
SourceGroupCidrs	Array of String	["192.0.XX.XX/24", "192.0.XX.XX/32"]	访问控制策略中的源地址簿中的网段列表。
ApplicationNameList	Array of String	HTTP, HTTPS	应用名称，支持多选。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeControlPolicy
&SourceIp=192.0.XX.XX
&Lang=zh
&Direction=in
&CurrentPage=1
&PageSize=10
&Source=192.0.XX.XX
&Destination=192.0.XX.XX
&Description=test
&Proto=TCP
&AclAction=accept
&Release=true
&AclUuid=00281255-d220-4db1-8f4f-c4df221a****
&IpVersion=6
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeControlPolicyResponse>
  <PageNo>1</PageNo>
  <PageSize>10</PageSize>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2****</RequestId>
  <TotalCount>100</TotalCount>
  <Policys>
    <Direction>in</Direction>
    <Order>1</Order>
    <SourceType>net</SourceType>
    <ApplicationName>HTTP</ApplicationName>
    <HitTimes>100</HitTimes>
    <Description>test</Description>
    <SourceGroupType>ip</SourceGroupType>
    <DnsResultTime>1579261141</DnsResultTime>
    <DnsResult>192.0.XX.XX,192.0.XX.XX</DnsResult>
    <Proto>TCP</Proto>
    <DestinationGroupType>ip</DestinationGroupType>
    <Destination>192.0.XX.XX/24</Destination>
    <HitLastTime>1579261141</HitLastTime>
    <DestPortGroup>my_port_group</DestPortGroup>
    <AclUuid>00281255-d220-4db1-8f4f-c4df221a****</AclUuid>
    <DestPortType>port</DestPortType>
    <Source>192.0.XX.XX/24</Source>
    <DestinationType>net</DestinationType>
    <DestPort>80</DestPort>
    <IpVersion>6</IpVersion>
    <AclAction>accept</AclAction>
    <Release>true</Release>
    <ApplicationId>10***</ApplicationId>
    <DestinationGroupCidrs>["192.0.XX.XX/24", "192.0.XX.XX/32"]</DestinationGroupCidrs>
    <DestPortGroupPorts>[80,443]</DestPortGroupPorts>
    <SourceGroupCidrs>["192.0.XX.XX/24", "192.0.XX.XX/32"]</SourceGroupCidrs>
    <ApplicationNameList>HTTP, HTTPS</ApplicationNameList>
  </Policys>
</DescribeControlPolicyResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "PageNo" : "1",
  "PageSize" : "10",
  "RequestId" : "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2****",
  "TotalCount" : "100",
  "Policys" : [ {
    "Direction" : "in",
    "Order" : 1,
    "SourceType" : "net",
    "ApplicationName" : "HTTP",
    "HitTimes" : 100,
    "Description" : "test",
    "SourceGroupType" : "ip",
    "DnsResultTime" : 1579261141,
    "DnsResult" : "192.0.XX.XX,192.0.XX.XX",
    "Proto" : "TCP",
    "DestinationGroupType" : "ip",
    "Destination" : "192.0.XX.XX/24",
    "HitLastTime" : 1579261141,
    "DestPortGroup" : "my_port_group",
    "AclUuid" : "00281255-d220-4db1-8f4f-c4df221a****",
    "DestPortType" : "port",
    "Source" : "192.0.XX.XX/24",
    "DestinationType" : "net",
    "DestPort" : "80",
    "IpVersion" : 6,
    "AclAction" : "accept",
    "Release" : "true",
    "ApplicationId" : "10****",
    "DestinationGroupCidrs" : [ "[\"192.0.XX.XX/24\", \"192.0.XX.XX/32\"]" ],
    "DestPortGroupPorts" : [ "[80,443]" ],
    "SourceGroupCidrs" : [ "[\"192.0.XX.XX/24\", \"192.0.XX.XX/32\"]" ],
    "ApplicationNameList" : [ "HTTP, HTTPS" ]
  } ]
}
```

4.3. DescribeDomainResolve

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

使用说明

本接口一般用于获取域名DNS的解析结果。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。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeDomainResolve	系统规定参数。取值： DescribeDomainResolve 。
SourceIp	String	否	192.0.XX.XX	访问者源IP地址。
Lang	String	否	zh	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
Domain	String	是	www.aliyundoc.com	待解析的域名地址。
IpVersion	String	否	6	云防火墙防护的资产的IP版本。 取值： <ul style="list-style-type: none"> 4（默认）：IPV4 6：IPV6

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	Object		域名解析结果。
IpAddrs	String	11.1.X.X,12.1.X.X	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。单位：秒。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainResolve
&SourceIp=192.0.XX.XX
&Lang=zh
&Domain=www.aliyundoc.com
&IpVersion=6
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeDomainResolveResponse>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
  <ResolveResult>
    <IpAddrs>11.1.X.X,12.1.X.X</IpAddrs>
    <UpdateTime>1579091739</UpdateTime>
  </ResolveResult>
</DescribeDomainResolveResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D",
  "ResolveResult" : {
    "IpAddrs" : "11.1.X.X,12.1.X.X",
    "UpdateTime" : 1579091739
  }
}
```

4.4. DescribePolicyPriorUsed

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

使用说明

本接口一般用于查询外对内流量或内对外流量访问控制策略优先级生效范围。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	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	192.0.XX.XX	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（默认）：中文 en：英文
IpVersion	String	否	6	云防火墙防护的资产的IP版本。 取值： <ul style="list-style-type: none"> 4（默认）：IPv4 6：IPv6

返回数据

名称	类型	示例值	描述
End	Integer	150	您已创建的访问控制策略的最低优先级。 <div style="background-color: #e6f2ff; padding: 5px; margin-top: 5px;"> ? 说明 -1表示最低优先级。 </div>
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	结果的请求ID。
Start	Integer	1	您已创建的访问控制策略的最高优先级。 <div style="background-color: #e6f2ff; padding: 5px; margin-top: 5px;"> ? 说明 0表示最高优先级。 </div>

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
}
```

4.5. ModifyControlPolicy

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

使用说明

本接口一般用于修改流量通过云防火墙方式为放行、拒绝或观察的访问控制策略的配置信息。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyControlPolicy	系统规定参数。取值： ModifyControlPolicy 。
SourceIp	String	否	192.0.XX.XX	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（默认）：中文 en：英文
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
ApplicationName	String	是	HTTP	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： <ul style="list-style-type: none"> ANY HTTP HTTPS MySQL SMTP SMTPS RDP VNC SSH Redis MQTT MongoDB Memcache SSL <div style="border: 1px solid #ccc; 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>
Description	String	是	test	安全访问控制策略的描述信息。
DestPort	String	否	80	安全访问控制策略中流量访问的目的端口。

名称	类型	是否必选	示例值	描述
Destination	String	是	192.0.XX.XX/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="border: 1px solid #ccc; 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	192.0.XX.XX/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"]
AclUuid	String	是	00281255-d220-4db1-8f4f-c4df221ad84c	安全访问控制策略的唯一标识ID。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <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> </div>
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
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。
Release	String	否	true	安全访问控制策略的状态。取值： <ul style="list-style-type: none"> true：策略开启状态 false：策略关闭状态
MessageType	String	否	FTP	协议中消息报文分类。
ApplicationName List.N	String	否	HTTP,HTTPS	应用名称，支持多选。

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
&SourceIp=192.0.XX.XX
&Lang=zh
&AclAction=accept
&ApplicationName=HTTP
&Description=test
&DestPort=80
&Destination=192.0.XX.XX/24
&DestinationType=net
&Direction=in
&Proto=TCP
&Source=192.0.XX.XX/24
&AclUuid=00281255-d220-4db1-8f4f-c4df221ad84c
&SourceType=net
&DestPortType=port
&DestPortGroup=my_port_group
&Release=true
&MessageType=FTP
&ApplicationNameList=["HTTP,HTTPS"]
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyControlPolicyResponse>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
</ModifyControlPolicyResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}
```

4.6. ModifyControlPolicyPosition

调用ModifyControlPolicyPosition接口，修改互联网边界防火墙IPv4访问控制策略（表示访问控制策略中的访问源IP、目的IP使用IPv4格式）的优先级。

使用说明

本接口一般用于修改互联网边界防火墙IPv4访问控制策略的优先级。暂不支持以调用接口的方式修改互联网边界防火墙IPv6访问控制策略的优先级。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyControlPolicyPosition	系统规定参数。取值： ModifyControlPolicyPosition 。
Direction	String	是	in	互联网边界防火墙IPv4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。
NewOrder	String	是	1	<p>为互联网边界防火墙IPv4访问控制策略设置一个新的优先级。</p> <p>优先级使用数字表示，输入数字1表示优先级最高，数字越大优先级越低。</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin: 5px 0;"> <p> 说明 新的优先级数字不能超出您已创建的互联网边界防火墙IPv4策略优先级的范围，否则会导致调用该接口时出错。</p> </div> <p>建议您在调用该接口前，先调用DescribePolicyPriorUsed查询互联网边界防火墙指定流量方向的IPv4策略优先级范围。</p>
OldOrder	String	是	5	要修改的互联网边界防火墙IPv4访问控制策略当前的优先级。
SourceIp	String	否	192.0.XX.XX	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（默认）：中文。en：英文。

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

调用API的请求格式，请参见本文[示例](#)中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125EEB1	本次请求的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

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

JSON 格式

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

4.7. DeleteControlPolicy

调用DeleteControlPolicy接口删除访问控制策略。

使用说明

本接口一般用于删除流量方向为外对内或内对外的访问控制策略。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	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	192.0.XX.XX	流量的源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（默认）：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"
}
```

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。

使用说明

本接口一般用于查询访问控制策略严格模式的开启状态。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribePolicyAdvancedConfig	要执行的操作。 取值： DescribePolicyAdvancedConfig 。
SourceIp	String	否	192.0.XX.XX	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（默认）：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"
}
```

4.8.2. ModifyPolicyAdvancedConfig

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

使用说明

本接口一般用于开启或关闭访问控制策略严格模式。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	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	192.0.XX.XX	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（默认）：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"
}
```

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。

使用说明

本接口一般用于为指定VPC边界防火墙策略组添加访问控制策略。VPC边界防火墙防护通过云企业网连接的两个VPC之间的流量或防护通过高速通道连接的两个VPC之间的流量时，使用不同的访问控制策略。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateVpcFirewallControlPolicy	系统规定参数。取值： CreateVpcFirewallControlPolicy 。
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（默认）：中文 en：英文
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

名称	类型	是否必选	示例值	描述
ApplicationName	String	是	HTTP	<p>VPC边界防火墙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 • 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。
DestPort	String	否	80	<p>VPC边界防火墙访问控制策略中流量访问的目的端口。</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p>? 说明</p> <p>当DestPortType为 <code>port</code> 时，设置该参数。</p> </div>
Destination	String	是	10.2.XX.XX/24	<p>VPC边界防火墙访问控制策略中流量访问的目的地址。取值：</p> <ul style="list-style-type: none"> • 当DestinationType为 <code>net</code> 时，Destination为目的CIDR地址。 • 当DestinationType为 <code>group</code> 时，Destination为目的地址簿名称。 • 当DestinationType为 <code>domain</code> 时，Destination为目的域名。

名称	类型	是否必选	示例值	描述
DestinationType	String	是	net	VPC边界防火墙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
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边界防火墙防护通过云企业网连接的两个VPC之间的流量时，策略组ID使用云企业网实例ID。 当VPC边界防火墙防护通过高速通道连接的两个VPC之间的流量时，策略组ID使用VPC边界防火墙实例ID。 <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>
Proto	String	是	TCP	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： <ul style="list-style-type: none"> ANY（不确定具体协议类型时可设置为ANY） TCP UDP ICMP
Source	String	是	10.2.XX.XX/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。 当SourceType为group时，Source为源地址簿名称。
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

名称	类型	是否必选	示例值	描述
NewOrder	String	是	1	VPC边界防火墙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。
DestPortType	String	否	port	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
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; margin-top: 10px;"> <p>? 说明 当DestPortType为 <code>group</code> 时，设置该参数。</p> </div>
MemberUid	String	否	258039427902*** *	当前阿里云账号的成员账号UID。
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

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
&Lang=zh
&AclAction=accept
&ApplicationName=HTTP
&Description=test
&DestPort=80
&Destination=10.2.XX.XX/24
&DestinationType=net
&VpcFirewallId=vfw-a42bbb7b887148c9****
&Proto=TCP
&Source=10.2.XX.XX/24
&SourceType=net
&NewOrder=1
&DestPortType=port
&DestPortGroup=my_port_group
&MemberUid=258039427902****
&Release=true
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<CreateVpcFirewallControlPolicyResponse>
  <AclUuid>00281255-d220-4db1-8f4f-c4df221ad84c</AclUuid>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
</CreateVpcFirewallControlPolicyResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "AclUuid" : "00281255-d220-4db1-8f4f-c4df221ad84c",
  "RequestId" : "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}
```

4.9.2. DescribeVpcFirewallControlPolicy

调用DescribeVpcFirewallControlPolicy接口，查询指定的VPC边界防火墙的所有访问控制策略信息。

使用说明

本接口一般用于查询VPC边界防火墙的访问控制策略。VPC边界防火墙防护通过云企业网连接的两个VPC之间的流量或防护通过高速通道连接的两个VPC之间的流量时，使用不同的访问控制策略。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeVpcFirewallControlPolicy	系统规定参数。取值： DescribeVpcFirewallControlPolicy 。
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（默认）：中文 en：英文
VpcFirewallId	String	是	vfw-a42bbb7b887148c9****	VPC边界防火墙的实例ID。取值： <ul style="list-style-type: none"> 当VPC边界防火墙防护通过云企业网连接的两个VPC之间的流量时，策略组ID使用云企业网实例ID。 当VPC边界防火墙防护通过高速通道连接的两个VPC之间的流量时，策略组ID使用VPC边界防火墙实例ID。 <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>
CurrentPage	String	是	1	分页查询时，设置当前页的页码。
PageSize	String	是	10	分页查询时，设置每页包含VPC边界防火墙的访问控制策略数量。 可设置值最大为50。
Source	String	否	192.0.XX.XX/24	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。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p> 说明 Source可以是单个CIDR地址或地址簿名称。</p> </div>

名称	类型	是否必选	示例值	描述
Destination	String	否	192.0.XX.XX/24	VPC边界防火墙访问控制策略中的目的地址。支持模糊查询。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p>? 说明 Destination可以是单个CIDR地址或域名，也可以是地址簿名称。</p> </div>
Description	String	否	test	VPC边界防火墙访问控制策略的描述信息。支持模糊查询。
Proto	String	否	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（查询所有协议类型） <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p>? 说明 不设置该参数表示查询所有协议类型。</p> </div>
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 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p>? 说明 不设置该参数表示查询所有动作。</p> </div>
MemberUid	String	否	258039427902*** *	当前阿里云账号的成员账号UID。
AclUuid	String	否	4037fbf7-3e39-4634-92a4-d0155247****	VPC边界防火墙访问控制策略的唯一标识ID。
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

返回数据

名称	类型	示例值	描述
TotalCount	String	20	VPC边界防火墙访问控制策略的总数量。
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	本次请求的ID。
Policys	Array of DataItem		VPC边界防火墙访问控制策略的信息。
Destination	String	192.0.XX.XX/24	VPC边界防火墙访问控制策略中的目的地址。取值： <ul style="list-style-type: none"> 当DestinationType为 <code>net</code> 时，Destination为目的CIDR地址。 当DestinationType为 <code>domain</code> 时，Destination为目的域名。 当DestinationType为 <code>group</code> 时，Destination为目的地址簿名称。
Order	Integer	1	VPC边界防火墙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，表示优先级越高。
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。
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"> <code>net</code>：源CIDR地址 <code>group</code>：源地址簿

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）
AclUuid	String	4037fbf7-3e39-4634-92a4-d0155247****	VPC边界防火墙访问控制策略的唯一标识ID。
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：单个端口 • group：端口地址簿
Source	String	192.0.XX.XX/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。 • 当SourceType为 group 时，Source为地址簿名称。
DestinationType	String	net	VPC边界防火墙访问控制策略中目的地址的类型。取值： <ul style="list-style-type: none"> • net：目的CIDR地址 • group：目的地址簿 • domain：目的域名
HitTimes	Integer	100	VPC边界防火墙访问控制策略的命中次数。

名称	类型	示例值	描述
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。
Description	String	test	VPC边界防火墙访问控制策略的描述信息。
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
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。
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）
DestinationGroupCidrs	Array of String	["192.0.XX.XX/24", "192.0.XX.XX/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。
DestPortGroupPorts	Array of String	[80,443]	VPC边界防火墙访问控制策略中目的端口地址簿中包含的端口列表。
SourceGroupCidrs	Array of String	["192.0.XX.XX/24", "198.51.XX.XX/32"]	VPC边界防火墙访问控制策略中，源地址簿中的网段列表。
MemberUid	String	258039427902****	当前阿里云账号的成员账号UID。
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

示例

请求示例

```

http(s)://[Endpoint]/?Action=DescribeVpcFirewallControlPolicy
&Lang=zh
&VpcFirewallId=vfw-a42bbb7b887148c9****
&CurrentPage=1
&PageSize=10
&Source=192.0.XX.XX/24
&Destination=192.0.XX.XX/24
&Description=test
&Proto=TCP
&AclAction=accept
&MemberUid=258039427902****
&AclUuid=4037fbf7-3e39-4634-92a4-d0155247****
&Release=true
&公共请求参数

```

正常返回示例

XML 格式

```

HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeVpcFirewallControlPolicyResponse>
  <TotalCount>20</TotalCount>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
  <Policys>
    <Destination>192.0.XX.XX/24</Destination>
    <Order>1</Order>
    <DestPortGroup>my_port_group</DestPortGroup>
    <SourceType>net</SourceType>
    <ApplicationName>HTTP</ApplicationName>
    <AclUuid>4037fbf7-3e39-4634-92a4-d0155247****</AclUuid>
    <DestPortType>port</DestPortType>
    <Source>192.0.XX.XX/24</Source>
    <DestinationType>net</DestinationType>
    <HitTimes>100</HitTimes>
    <DestPort>80</DestPort>
    <Description>test</Description>
    <AclAction>accept</AclAction>
    <ApplicationId>10**</ApplicationId>
    <Proto>TCP</Proto>
    <DestinationGroupCidrs>["192.0.XX.XX/24", "192.0.XX.XX/32"]</DestinationGroupCidrs>
    <DestPortGroupPorts>[80,443]</DestPortGroupPorts>
    <SourceGroupCidrs>["192.0.XX.XX/24", "198.51.XX.XX/32"]</SourceGroupCidrs>
    <MemberUid>258039427902****</MemberUid>
    <Release>true</Release>
  </Policys>
</DescribeVpcFirewallControlPolicyResponse>

```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "TotalCount" : "20",
  "RequestId" : "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D",
  "Policys" : [ {
    "Destination" : "192.0.XX.XX/24",
    "Order" : 1,
    "DestPortGroup" : "my_port_group",
    "SourceType" : "net",
    "ApplicationName" : "HTTP",
    "AclUuid" : "4037fbf7-3e39-4634-92a4-d0155247****",
    "DestPortType" : "port",
    "Source" : "192.0.XX.XX/24",
    "DestinationType" : "net",
    "HitTimes" : 100,
    "DestPort" : "80",
    "Description" : "test",
    "AclAction" : "accept",
    "ApplicationId" : "10**",
    "Proto" : "TCP",
    "DestinationGroupCidrs" : [ "[\"192.0.XX.XX/24\", \"192.0.XX.XX/32\"]" ],
    "DestPortGroupPorts" : [ "[80,443]" ],
    "SourceGroupCidrs" : [ "[\"192.0.XX.XX/24\", \"198.51.XX.XX/32\"]" ],
    "MemberUid" : "258039427902****",
    "Release" : "true"
  } ]
}
```

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。

使用说明

本接口一般用于查询指定VPC防火墙策略组访问控制策略优先级生效范围。

QPS限制

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

调试

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

请求参数

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

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 。
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（默认）：中文 en：英文
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****

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。
Start	Integer	1	访问控制策略生效的优先级最高值。
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	结果的请求ID。

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

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeVpcFirewallPolicyPriorUsedResponse>
<RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
<Start>1</Start>
<End>150</End>
</DescribeVpcFirewallPolicyPriorUsedResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D",
  "Start" : 1,
  "End" : 150
}
```

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。

使用说明

本接口一般用于查询VPC防火墙所有访问控制策略组信息。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeVpcFirewallAclGroupList	系统规定参数。取值： DescribeVpcFirewallAclGroupList 。
Lang	String	否	zh	接收消息的语言类型。 <ul style="list-style-type: none">zh（默认）：中文en：英文

名称	类型	是否必选	示例值	描述
FirewallConfigure Status	String	否	configured	VPC防火墙的配置状态。 <ul style="list-style-type: none"> not configured：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
TotalCount	Integer	1	VPC防火墙访问控制策略组的总数量。
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	结果的请求ID。
AclGroupList	Array of Data		VPC防火墙访问控制策略组的信息。
AclGroupId	String	vfw-a42bbb7b887148c9***	VPC边界防火墙的访问控制策略组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-erw0g12b5jbw**** 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	示例值	描述
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。
MemberUid	String	258039427902****	当前阿里云账号的成员账号UID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeVpcFirewallAclGroupList
&Lang=zh
&FirewallConfigureStatus=configured
&CurrentPage=1
&PageSize=10
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeVpcFirewallAclGroupListResponse>
  <TotalCount>1</TotalCount>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
  <AclGroupList>
    <AclGroupId>vfw-a42bbb7b887148c9****</AclGroupId>
    <AclGroupName>group_test</AclGroupName>
    <MemberUid>258039427902****</MemberUid>
  </AclGroupList>
</DescribeVpcFirewallAclGroupListResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "TotalCount" : 1,
  "RequestId" : "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D",
  "AclGroupList" : [ {
    "AclGroupId" : "vfw-a42bbb7b887148c9****",
    "AclGroupName" : "group_test",
    "MemberUid" : "258039427902****"
  } ]
}
```

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。

使用说明

本接口一般用于修改指定VPC防火墙策略组的访问控制策略的配置信息。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。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyVpcFirewallControlPolicy	系统规定参数。取值： ModifyVpcFirewallControlPolicy 。
Lang	String	否	zh	接收消息的语言类型。 取值： <ul style="list-style-type: none">zh：（默认）中文en：英文
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

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。
DestPort	String	否	80	访问控制策略中访问流量的目的端口。
Destination	String	是	10.2.X.X/XX	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

名称	类型	是否必选	示例值	描述
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
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****
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.X.X/XX	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
AclUuid	String	是	00281255-d220-4db1-8f4f-c4df221a****	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
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
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。
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

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
&Lang=zh
&AclAction=accept
&ApplicationName=HTTP
&Description=test
&DestPort=80
&Destination=10.2.X.X/XX
&DestinationType=net
&VpcFirewallId=vfw-a42bbb7b887148c9****
&Proto=TCP
&Source=10.2.X.X/XX
&AclUuid=00281255-d220-4db1-8f4f-c4df221a****
&SourceType=net
&DestPortType=port
&DestPortGroup=my_port_group
&Release=true
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyVpcFirewallControlPolicyResponse>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
</ModifyVpcFirewallControlPolicyResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}
```

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。

使用说明

本接口一般用于修改指定VPC防火墙策略组访问控制策略的优先级。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyVpcFirewallControlPolicyPosition	系统规定参数。取值： ModifyVpcFirewallControlPolicyPosition 。
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（默认）：中文 en：英文
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-ervw0g12b5jw**** 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****
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。

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

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyVpcFirewallControlPolicyPositionResponse>
<RequestId>850A84D6-0DE4-4797-A1E8-00090125EEB1</RequestId>
</ModifyVpcFirewallControlPolicyPositionResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "850A84D6-0DE4-4797-A1E8-00090125EEB1"
}
```

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。

使用说明

本接口一般用于将指定的VPC防火墙策略组访问控制策略的命中计数清零。

QPS限制

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

调试

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

请求参数

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

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（默认）：中文 en：英文
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。

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

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ResetVpcFirewallRuleHitCountResponse>
<RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
</ResetVpcFirewallRuleHitCountResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}
```

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。

使用说明

本接口一般用于删除指定VPC防火墙策略组的访问控制策略。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。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteVpcFirewallControlPolicy	系统规定参数。取值： DeleteVpcFirewallControlPolicy 。
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
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。
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-erw0g12b5jbw**** 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-a42bbb7b887148c91****

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

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DeleteVpcFirewallControlPolicyResponse>
<RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
</DeleteVpcFirewallControlPolicyResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}
```

4.9.9. CreateVpcFirewallConfigure

调用CreateVpcFirewallConfigure接口，创建VPC边界防火墙（防护通过高速通道连接的两个VPC之间的流量）。

使用说明

本接口一般用于创建VPC边界防火墙。该VPC边界防火墙是防护通过高速通道连接的两个VPC之间的流量。该VPC边界防火墙不支持防护VPC跨地域、跨账号以及VPC与VBR间的互访流量。更多信息，请参见[VPC边界防火墙限制说明](#)。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateVpcFirewallConfigure	系统规定参数。取值： CreateVpcFirewallConfigure 。
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（默认）：中文。 en：英文。
VpcFirewallName	String	是	测试用实例	VPC边界防火墙的实例名称。
LocalVpcId	String	是	vpc-8vbwbo90rq0anm6t****	本端VPC的实例ID。
LocalVpcRegion	String	是	cn-hangzhou	本端VPC所属地域ID。 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> ? 说明 关于云防火墙支持地域的详细信息，请参见支持的地域。 </div>
PeerVpcId	String	是	vpc-wb8vbo90rq0anm6t****	对端VPC的实例ID。
PeerVpcRegion	String	是	cn-shanghai	对端VPC所属地域ID。 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> ? 说明 关于云防火墙支持地域的详细信息，请参见支持的地域。 </div>
FirewallSwitch	String	是	open	设置VPC边界防火墙创建后的开启状态。取值： <ul style="list-style-type: none"> open（默认）：创建VPC边界防火墙后自动开启防护。 close：创建VPC边界防火墙后不自动开启防护。您可以调用接口 ModifyVpcFirewallSwitchStatus 开启防护。

名称	类型	是否必选	示例值	描述
LocalVpcCidrTableList	String	是	<pre>[{"RouteTableId": "vtb-1234", "RouteEntryList": [{"DestinationCidr": "192.168.XX.XX/24", "NextHopInstanceId": "vrt-m5eb5me6c3l5sezae****"}]}, {"RouteTableId": "vtb-1235", "RouteEntryList": [{"DestinationCidr": "192.168.XX.XX/24", "NextHopInstanceId": "vrt-m5eb5me6c3l5sezae****"}]}]</pre>	<p>本端VPC的网段列表，以JSON格式表示，具体包含以下参数：</p> <ul style="list-style-type: none"> RouteTableId：表示本端VPC的路由表ID。 RouteEntryList：该参数使用JSON格式，包含DestinationCidr（表示本端VPC的目标网段）和NextHopInstanceId（表示本端VPC的下一跳实例ID）。
PeerVpcCidrTableList	String	是	<pre>[{"RouteTableId": "vtb-1234", "RouteEntryList": [{"DestinationCidr": "192.168.XX.XX/24", "NextHopInstanceId": "vrt-m5eb5me6c3l5sezae****"}]}, {"RouteTableId": "vtb-1235", "RouteEntryList": [{"DestinationCidr": "192.168.XX.XX/24", "NextHopInstanceId": "vrt-m5eb5me6c3l5sezae****"}]}]</pre>	<p>对端VPC的网段列表，以JSON格式表示，具体包含以下参数：</p> <ul style="list-style-type: none"> RouteTableId：表示对端VPC的路由表ID。 RouteEntryList：该参数使用JSON格式，包含DestinationCidr（表示对端VPC的目标网段）和NextHopInstanceId（表示对端VPC的下一跳实例ID）。
MemberUid	String	否	258039427902****	阿里云成员账号的UID。

返回数据

名称	类型	示例值	描述
VpcFirewallId	String	vfw-m5e7dbc4y****	VPC边界防火墙实例ID。

名称	类型	示例值	描述
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125h4j6	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateVpcFirewallConfigure
&Lang=zh
&VpcFirewallName=测试用实例
&LocalVpcId=vpc-8vbwbo90rq0anm6t****
&LocalVpcRegion=cn-hangzhou
&PeerVpcId=vpc-wb8vbo90rq0anm6t****
&PeerVpcRegion=cn-shanghai
&FirewallSwitch=open
&LocalVpcCidrTableList=[{"RouteTableId":"vtb-1234","RouteEntryList":[{"DestinationCidr":"192.168.XX.XX/24","NextHopInstanceId":"vrt-m5eb5me6c3l5sezae****"}]},{"RouteTableId":"vtb-1235","RouteEntryList":[{"DestinationCidr":"192.168.XX.XX/24","NextHopInstanceId":"vrt-m5eb5me6c3l5sezae****"}]}]
&PeerVpcCidrTableList=[{"RouteTableId":"vtb-1234","RouteEntryList":[{"DestinationCidr":"192.168.XX.XX/24","NextHopInstanceId":"vrt-m5eb5me6c3l5sezae****"}]},{"RouteTableId":"vtb-1235","RouteEntryList":[{"DestinationCidr":"192.168.XX.XX/24","NextHopInstanceId":"vrt-m5eb5me6c3l5sezae****"}]}]
&MemberUid=258039427902****
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<CreateVpcFirewallConfigureResponse>
  <VpcFirewallId>vfw-m5e7dbc4y****</VpcFirewallId>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125h4j6</RequestId>
</CreateVpcFirewallConfigureResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "VpcFirewallId" : "vfw-m5e7dbc4y****",
  "RequestId" : "850A84D6-0DE4-4797-A1E8-00090125h4j6"
}
```

4.9.10. DescribeVpcFirewallDetail

调用DescribeVpcFirewallDetail接口，查询VPC边界防火墙（防护通过高速通道连接的两个VPC之间的流量）的详细信息。

使用说明

本接口用于获取VPC边界防火墙的详细信息。该VPC边界防火墙是防护通过高速通道连接的两个VPC之间的流量。

调用本接口前，必须已经调用CreateVpcFirewallConfigure接口创建了VPC边界防火墙。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeVpcFirewallDetail	系统规定参数。取值： DescribeVpcFirewallDetail 。
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（默认）：中文。 en：英文。
VpcFirewallId	String	是	vfw-m5e7dbc4y****	VPC边界防火墙的实例ID。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 5px;"> <p> 说明 您可以调用DescribeVpcFirewallList接口查询VPC边界防火墙的实例ID。</p> </div>
LocalVpcId	String	否	vpc-8vbwbo90rq0anm6t****	本端VPC的实例ID。
PeerVpcId	String	否	vpc-90rq0anm6t8vbwbo****	对端VPC的实例ID。

返回数据

名称	类型	示例值	描述
----	----	-----	----

名称	类型	示例值	描述
ConnectType	String	expressconnect	VPC边界防火墙的互通类型。取值： expressconnect ，表示高速通道。
VpcFirewallId	String	vfw-m5e7dbc4y****	VPC边界防火墙实例ID。
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125g4d2	本次请求的ID。
Bandwidth	Integer	2	高速通道的带宽规格。单位：Mbps。
VpcFirewallName	String	测试防火墙	VPC边界防火墙的实例名称。
FirewallSwitchStatus	String	opened	VPC边界防火墙的状态。取值： <ul style="list-style-type: none"> opened：已开启。 closed：已关闭。 notconfigured：表示暂未配置VPC边界防火墙。 configured：表示已配置VPC边界防火墙。
LocalVpc	Object		本端VPC的详细信息。
VpcId	String	vpc-8vbwbo90rq0anm6t****	本端VPC的实例ID。
VpcName	String	测试用实例	本端VPC的实例名称。
RegionNo	String	cn-hangzhou	本端VPC所属地域ID。
EniPrivateIpAddress	String	192.168.XX.XX	本端VPC中弹性网卡私网IP。
RouterInterfaceId	String	vrt-m5eb5me6c3l5sezae****	本端VPC中路由器接口ID。
EniId	String	eni-8vbhfosfqv2rff42****	本端VPC中弹性网卡的实例ID。

名称	类型	示例值	描述
VpcCidrTableList	Array of cidrTable		本端VPC的网段列表信息。
RouteTableId	String	vtb-1234	本端VPC的路由表ID。
RouteEntryList	Array of routeEntry		本端VPC的路由条目列表。
NextHopInstanceId	String	vrt-m5eb5me6c3l5sezae****	本端VPC中的下一跳实例ID。
DestinationCidr	String	192.168.XX.XX/24	本端VPC的目标网段。
PeerVpc	Object		对端VPC的详细信息。
VpcId	String	vpc-90rq0anm6t8vbwbo****	对端VPC的实例ID。
VpcName	String	测试vpc2	对端VPC的实例名称。
RegionNo	String	cn-hangzhou	对端VPC所属地域ID。
EniPrivateIpAddress	String	192.168.XX.XX	对端VPC中弹性网卡私网IP。
RouterInterfaceId	String	vrt-m5eb5me6c3l5sezae****	对端VPC中路由器接口ID。
EniId	String	eni-8vbhfosfqv2rff42***	对端VPC中弹性网卡的实例ID。
VpcCidrTableList	Array of cidrTable		对端VPC的网段列表信息。
RouteTableId	String	vtb-1256	对端VPC的路由表ID。
RouteEntryList	Array of routeEntry		对端VPC路由条目列表信息。
NextHopInstanceId	String	vrt-m5eb5me6c3l5sezae****	对端VPC中的下一跳实例ID。

名称	类型	示例值	描述
DestinationCidr	String	192.168.XX.XX/24	对端VPC的目标网段。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeVpcFirewallDetail
&Lang=zh
&VpcFirewallId=vfw-m5e7dbc4y****
&LocalVpcId=vpc-8vbwbo90rq0anm6t****
&PeerVpcId=vpc-90rq0anm6t8vbwbo****
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type: application/xml
<DescribeVpcFirewallDetailResponse>
  <ConnectType>expressconnect</ConnectType>
  <VpcFirewallId>vfw-m5e7dbc4y****</VpcFirewallId>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125g4d2</RequestId>
  <Bandwidth>2</Bandwidth>
  <VpcFirewallName>测试防火墙</VpcFirewallName>
  <FirewallSwitchStatus>opened</FirewallSwitchStatus>
  <LocalVpc>
    <VpcId>vpc-8vbwbo90rq0anm6t****</VpcId>
    <VpcName>测试用实例</VpcName>
    <RegionNo>cn-hangzhou</RegionNo>
    <EniPrivateIpAddress>192.168.XX.XX</EniPrivateIpAddress>
    <RouterInterfaceId>vrt-m5eb5me6c3l5sezae****</RouterInterfaceId>
    <EniId>eni-8vbhfosfqv2rff42****</EniId>
    <VpcCidrTableList>
      <RouteTableId>vtb-1234</RouteTableId>
      <RouteEntryList>
        <NextHopInstanceId>vrt-m5eb5me6c3l5sezae****</NextHopInstanceId>
        <DestinationCidr>192.168.XX.XX/24</DestinationCidr>
      </RouteEntryList>
    </VpcCidrTableList>
  </LocalVpc>
  <PeerVpc>
    <VpcId>vpc-90rq0anm6t8vbwbo****</VpcId>
    <VpcName>测试vpc2</VpcName>
    <RegionNo>cn-hangzhou</RegionNo>
    <EniPrivateIpAddress>192.168.XX.XX</EniPrivateIpAddress>
    <RouterInterfaceId>vrt-m5eb5me6c3l5sezae****</RouterInterfaceId>
    <EniId>eni-8vbhfosfqv2rff42****</EniId>
    <VpcCidrTableList>
      <RouteTableId>vtb-1256</RouteTableId>
      <RouteEntryList>
        <NextHopInstanceId>vrt-m5eb5me6c3l5sezae****</NextHopInstanceId>
        <DestinationCidr>192.168.XX.XX/24</DestinationCidr>
      </RouteEntryList>
    </VpcCidrTableList>
  </PeerVpc>
</DescribeVpcFirewallDetailResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "ConnectType" : "expressconnect",
  "VpcFirewallId" : "vfw-m5e7dbc4y****",
  "RequestId" : "850A84D6-0DE4-4797-A1E8-00090125g4d2",
  "Bandwidth" : 2,
  "VpcFirewallName" : "测试防火墙",
  "FirewallSwitchStatus" : "opened",
  "LocalVpc" : {
    "VpcId" : "vpc-8vbwbo90rq0anm6t****",
    "VpcName" : "测试用实例",
    "RegionNo" : "cn-hangzhou",
    "EniPrivateIpAddress" : "192.168.XX.XX",
    "RouterInterfaceId" : "vrt-m5eb5me6c3l5sezae****",
    "EniId" : "eni-8vbhfosfqv2rff42****",
    "VpcCidrTableList" : [ {
      "RouteTableId" : "vtb-1234",
      "RouteEntryList" : [ {
        "NextHopInstanceId" : "vrt-m5eb5me6c3l5sezae****",
        "DestinationCidr" : "192.168.XX.XX/24"
      } ]
    } ]
  },
  "PeerVpc" : {
    "VpcId" : "vpc-90rq0anm6t8vbwbo****",
    "VpcName" : "测试vpc2",
    "RegionNo" : "cn-hangzhou",
    "EniPrivateIpAddress" : "192.168.XX.XX",
    "RouterInterfaceId" : "vrt-m5eb5me6c3l5sezae****",
    "EniId" : "eni-8vbhfosfqv2rff42****",
    "VpcCidrTableList" : [ {
      "RouteTableId" : "vtb-1256",
      "RouteEntryList" : [ {
        "NextHopInstanceId" : "vrt-m5eb5me6c3l5sezae****",
        "DestinationCidr" : "192.168.XX.XX/24"
      } ]
    } ]
  }
}
```

4.9.11. DescribeVpcFirewallList

调用DescribeVpcFirewallList接口，查询VPC边界防火墙（防护通过高速通道连接的两个VPC之间的流量）的信息。

使用说明

本接口一般用于分页查询VPC边界防火墙的信息。该VPC边界防火墙是防护通过高速通道连接两个VPC之间的流量。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeVpcFirewallList	系统规定参数。取值： DescribeVpcFirewallList 。
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（默认）：中文。 en：英文。
RegionNo	String	否	cn-hangzhou	VPC所在的地域ID。 ? 说明 关于云防火墙支持地域的详细信息，请参见支持的地域。
VpcId	String	否	vpc-8vbwbo90rq0anm6t****	VPC实例ID。
FirewallSwitchStatus	String	否	opened	VPC边界防火墙的状态。取值： <ul style="list-style-type: none"> opened：已开启。 closed：已关闭。 not configured：表示暂未配置VPC边界防火墙。 configured：表示已配置VPC边界防火墙。 ? 说明 不设置该参数表示查询所有状态的VPC边界防火墙。
VpcFirewallId	String	否	vfw-m5e7dbc4y****	VPC边界防火墙的实例ID。
VpcFirewallName	String	否	测试环境防火墙	VPC边界防火墙的实例名称。

名称	类型	是否必选	示例值	描述
CurrentPage	String	否	1	分页查询时，设置当前页面的页码。 默认值为1，表示返回第1页数据。
PageSize	String	否	10	分页查询时，设置每页包含VPC边界防火墙的数量。 默认值为10，表示每页包含10条结果。最大值为50。
MemberUid	String	否	258039427902**** *	当前阿里云账号的成员账号UID。

返回数据

名称	类型	示例值	描述
TotalCount	Integer	10	VPC边界防火墙的总数量。
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125k8g2	本次请求的ID。
VpcFirewalls	Array of Data		VPC边界防火墙的详细信息。
ConnectType	String	expressconnect	VPC边界防火墙的互通类型。取值： expressconnect ，表示高速通道。
VpcFirewallId	String	vfw-m5e7dbc4y****	VPC边界防火墙的实例ID。
RegionStatus	String	enable	地域开放状态。取值： <ul style="list-style-type: none"> enable：已开放，表示该地域允许配置VPC边界防火墙。 disable：未开放，表示该地域不允许配置VPC边界防火墙。
Bandwidth	Integer	2	高速通道的带宽规格。单位：Mbps。
VpcFirewallName	String	测试防火墙	VPC边界防火墙的实例名称。

名称	类型	示例值	描述
FirewallSwitchStatus	String	opened	VPC边界防火墙开关的状态。取值： <ul style="list-style-type: none"> opened：已开启。 closed：已关闭。 not configured：表示暂未配置VPC边界防火墙。
LocalVpc	Object		本端VPC的详细信息。
VpcName	String	测试用实例	本端VPC的实例名称。
VpcId	String	vpc-8vbwbo90rq0anm6t****	本端VPC的实例ID。
AuthorizationStatus	String	authorized	本端VPC的授权状态。取值：authorized，表示已授权。
OwnerId	Long	158039427902****	本端VPC所属阿里云账号的UID。
RegionNo	String	cn-hangzhou	本端VPC所属地域ID。
VpcCidrTableList	Array of cidrTable		本端VPC的网段列表信息。
RouteTableId	String	vtb-1234	本端VPC的路由表ID。
RouteEntryList	Array of routeEntry		本端VPC的路由条目列表。
NextHopInstanceId	String	vrt-m5eb5me6c3l5sezae****	本端VPC的下一跳实例ID。
DestinationCidr	String	192.168.XX.XX/24	本端VPC的目标网段。
PeerVpc	Object		对端VPC的详细信息。
VpcName	String	测试vpc2	对端VPC的实例名称。

名称	类型	示例值	描述
VpcId	String	vpc-8vbwbo90rq0anm6t****	对端VPC的实例ID。
AuthorizationStatus	String	authorized	对端VPC的授权状态。取值： authorized ，表示已授权。
OwnerId	Long	158039427902****	对端VPC所属的阿里云账号的UID。
RegionNo	String	cn-hangzhou	对端VPC所属地域ID。
VpcCidrTableList	Array of cidrTable		对端VPC网段列表信息。
RouteTableId	String	vtb-1256	对端VPC的路由表ID。
RouteEntryList	Array of routeEntry		对端VPC路由条目列表信息。
NextHopInstanceId	String	vrt-m5eb5me6c3l5seaze****	对端VPC的下一跳实例ID。
DestinationCidr	String	192.168.XX.XX/24	对端VPC的目标网段。
IpsConfig	Object		IPS配置信息。
BasicRules	Integer	1	基础规则开关。取值： • 1：开启状态。 • 0：关闭状态。
EnableAllPatch	Integer	1	虚拟补丁开关。取值： • 1：开启状态。 • 0：关闭状态。
RunMode	Integer	0	IPS防御模式。取值： • 1：拦截模式。 • 0：观察模式。
MemberUid	String	258039427902****	阿里云成员账号的UID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeVpcFirewallList
&Lang=zh
&RegionNo=cn-hangzhou
&VpcId=vpc-8vbwbo90rq0anm6t****
&FirewallSwitchStatus=opened
&VpcFirewallId=vfw-m5e7dbc4y****
&VpcFirewallName=测试环境防火墙
&CurrentPage=1
&PageSize=10
&MemberUid=258039427902****
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeVpcFirewallListResponse>
  <TotalCount>10</TotalCount>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125k8g2</RequestId>
  <VpcFirewalls>
    <ConnectType>expressconnect</ConnectType>
    <VpcFirewallId>vfw-m5e7dbc4y****</VpcFirewallId>
    <RegionStatus>enable</RegionStatus>
    <Bandwidth>2</Bandwidth>
    <VpcFirewallName>测试防火墙</VpcFirewallName>
    <FirewallSwitchStatus>opened</FirewallSwitchStatus>
    <LocalVpc>
      <VpcName>测试用实例</VpcName>
      <VpcId>vpc-8vbwbo90rq0anm6t****</VpcId>
      <AuthorizationStatus>authorized</AuthorizationStatus>
      <RegionNo>cn-hangzhou</RegionNo>
      <VpcCidrTableList>
        <RouteTableId>vtb-1234</RouteTableId>
        <RouteEntryList>
          <NextHopInstanceId>vrt-m5eb5me6c3l5sezae****</NextHopInstanceId>
          <DestinationCidr>192.168.XX.XX/24</DestinationCidr>
        </RouteEntryList>
      </VpcCidrTableList>
    </LocalVpc>
    <PeerVpc>
      <VpcName>测试vpc2</VpcName>
      <VpcId>vpc-8vbwbo90rq0anm6t****</VpcId>
      <AuthorizationStatus>authorized</AuthorizationStatus>
      <RegionNo>cn-hangzhou</RegionNo>
      <VpcCidrTableList>
        <RouteTableId>vtb-1256</RouteTableId>
        <RouteEntryList>
          <NextHopInstanceId>vrt-m5eb5me6c3l5sezae****</NextHopInstanceId>
          <DestinationCidr>192.168.XX.XX/24</DestinationCidr>
        </RouteEntryList>
      </VpcCidrTableList>
    </PeerVpc>
    <IpsConfig>
      <BasicRules>1</BasicRules>
      <EnableAllPatch>1</EnableAllPatch>
      <RunMode>0</RunMode>
    </IpsConfig>
    <MemberUid>258039427902****</MemberUid>
  </VpcFirewalls>
</DescribeVpcFirewallListResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "TotalCount" : 10,
  "RequestId" : "850A84D6-0DE4-4797-A1E8-00090125k8g2",
  "VpcFirewalls" : [ {
    "ConnectType" : "expressconnect",
    "VpcFirewallId" : "vfw-m5e7dbc4y****",
    "RegionStatus" : "enable",
    "Bandwidth" : 2,
    "VpcFirewallName" : "测试防火墙",
    "FirewallSwitchStatus" : "opened",
    "LocalVpc" : {
      "VpcName" : "测试用实例",
      "VpcId" : "vpc-8vbwbo90rq0anm6t****",
      "AuthorizationStatus" : "authorized",
      "RegionNo" : "cn-hangzhou",
      "VpcCidrTableList" : [ {
        "RouteTableId" : "vtb-1234",
        "RouteEntryList" : [ {
          "NextHopInstanceId" : "vrt-m5eb5me6c3l5sezae****",
          "DestinationCidr" : "192.168.XX.XX/24"
        } ]
      } ]
    },
    "PeerVpc" : {
      "VpcName" : "测试vpc2",
      "VpcId" : "vpc-8vbwbo90rq0anm6t****",
      "AuthorizationStatus" : "authorized",
      "RegionNo" : "cn-hangzhou",
      "VpcCidrTableList" : [ {
        "RouteTableId" : "vtb-1256",
        "RouteEntryList" : [ {
          "NextHopInstanceId" : "vrt-m5eb5me6c3l5sezae****",
          "DestinationCidr" : "192.168.XX.XX/24"
        } ]
      } ]
    },
    "IpsConfig" : {
      "BasicRules" : 1,
      "EnableAllPatch" : 1,
      "RunMode" : 0
    },
    "MemberUid" : "258039427902****"
  } ]
}
```

4.9.12. DeleteVpcFirewallConfigure

调用DeleteVpcFirewallConfigure接口，删除VPC边界防火墙（防护通过高速通道连接的两个VPC之间流量）。

使用说明

本接口一般用于删除VPC边界防火墙。该VPC边界防火墙是防护通过高速通道连接的两个VPC之间流量。调用本接口前，必须已经调用 [CreateVpcFirewallConfigure](#) 接口创建了VPC边界防火墙。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteVpcFirewallConfigure	系统规定参数。取值： DeleteVpcFirewallConfigure 。
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（默认）：中文。 en：英文。
MemberUid	String	否	258039427902****	当前阿里云账号的成员账号UID。
VpcFirewallIdList.N	String	是	vfw-m5e7dbc4y****	VPC边界防火墙的实例ID。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 5px;"> <p>? 说明 您可以通过调用 DescribeVpcFirewallList 接口查询VPC边界防火墙的实例ID。</p> </div>

返回数据

名称	类型	示例值	描述
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125k6j3	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteVpcFirewallConfigure
&Lang=zh
&VpcFirewallIdList=["vfw-m5e7dbc4y****"]
&MemberUid=258039427902****
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DeleteVpcFirewallConfigureResponse>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125k6j3</RequestId>
</DeleteVpcFirewallConfigureResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "850A84D6-0DE4-4797-A1E8-00090125k6j3"
}
```

4.9.13. ModifyVpcFirewallConfigure

调用ModifyVpcFirewallConfigure接口，修改VPC边界防火墙（防护通过高速通道连接的两个VPC之间的流量）的配置信息。

使用说明

本接口一般用于修改VPC边界防火墙的配置信息。该VPC边界防火墙是防护通过高速通道连接的两个VPC之间的流量。

调用本接口前，必须已经调用CreateVpcFirewallConfigure接口创建了VPC边界防火墙。

QPS限制

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

调试

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

请求参数

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

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyVpcFirewallConfigure	系统规定参数。取值： ModifyVpcFirewallConfigure 。
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（默认）：中文。 en：英文。
VpcFirewallId	String	是	vfw-m5e7dbc4y****	VPC边界防火墙的实例ID。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p> 说明 您可以调用 DescribeVpcFirewallList 接口查询 VPC边界防火墙的实例ID。</p> </div>
VpcFirewallName	String	是	测试环境防火墙	VPC边界防火墙的实例名称。
LocalVpcCidrTableList	String	是	<pre>[{"RouteTableId": "vtb-1234", "RouteEntryList": [{"DestinationCidr": "192.168.XX.XX/24", "NextHopInstanceId": "vrt-m5eb5me6c3l5sezae****"}]}, {"RouteTableId": "vtb-1235", "RouteEntryList": [{"DestinationCidr": "192.168.XX.XX/24", "NextHopInstanceId": "vrt-m5eb5me6c3l5sezae****"}]}</pre>	本端VPC的网段信息，以JSON格式表示，具体包含以下参数： <ul style="list-style-type: none"> RouteTableId：表示本端VPC的路由表ID。 RouteEntryList：该参数使用JSON格式，包含DestinationCidr（表示本端VPC的目标网段）和NextHopInstanceId（表示本端VPC的下一跳实例ID）。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p> 说明 您可以调用 DescribeVpcFirewallDetail 接口查询VPC边界防火墙的本端VPC网段信息。</p> </div>

名称	类型	是否必选	示例值	描述
PeerVpcCidrTableList	String	是	<pre> [{"RouteTableId": "vtb- 1234","RouteEntryList": [{"DestinationCidr": "192.168.XX.XX/24","NextHopInstanceld": "vrt-m5eb5me6c3l5sezae****"}], {"RouteTableId": "vtb- 1235","RouteEntryList": [{"DestinationCidr": "192.168.XX.XX/24","NextHopInstanceld": "vrt-m5eb5me6c3l5sezae****"}]}] </pre>	<p>对端VPC的网段信息，以JSON格式表示，具体包含以下参数：</p> <ul style="list-style-type: none"> RouteTableId：表示对端VPC的路由表ID。 RouteEntryList：该参数使用JSON格式，包含DestinationCidr（表示对端VPC的目标网段）和NextHopInstanceld（表示对端VPC的下一跳实例ID）。 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> 说明 您可以调用 DescribeVpcFirewallDetail 接口查询VPC边界防火墙的对端VPC网段信息。</p> </div>
MemberUid	String	否	258039427902****	当前阿里云账号的成员账号UID。

返回数据

名称	类型	示例值	描述
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125k6f8	本次请求的ID。

示例

请求示例

```

http(s)://[Endpoint]/?Action=ModifyVpcFirewallConfigure
&Lang=zh
&VpcFirewallId=vfw-m5e7dbc4y****
&VpcFirewallName=测试环境防火墙
&LocalVpcCidrTableList=[{"RouteTableId":"vtb-1234","RouteEntryList":[{"DestinationCidr":"192.168.XX.XX/24","NextHopInstanceId":"vrt-m5eb5me6c3l5sezae****"}]},{"RouteTableId":"vtb-1235","RouteEntryList":[{"DestinationCidr":"192.168.XX.XX/24","NextHopInstanceId":"vrt-m5eb5me6c3l5sezae****"}]}]
&PeerVpcCidrTableList=[{"RouteTableId":"vtb-1234","RouteEntryList":[{"DestinationCidr":"192.168.XX.XX/24","NextHopInstanceId":"vrt-m5eb5me6c3l5sezae****"}]},{"RouteTableId":"vtb-1235","RouteEntryList":[{"DestinationCidr":"192.168.XX.XX/24","NextHopInstanceId":"vrt-m5eb5me6c3l5sezae****"}]}]
&MemberUid=258039427902****
&公共请求参数

```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyVpcFirewallConfigureResponse>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125k6f8</RequestId>
</ModifyVpcFirewallConfigureResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "850A84D6-0DE4-4797-A1E8-00090125k6f8"
}
```

4.9.14. ModifyVpcFirewallSwitchStatus

调用ModifyVpcFirewallSwitchStatus接口，修改VPC边界防火墙（防护通过高速通道连接的两个VPC之间的流量）的开关状态。

使用说明

本接口一般用于修改VPC边界防火墙的开关状态。该VPC边界防火墙是防护通过高速通道连接的两个VPC之间的流量。打开VPC边界防火墙的开关后，高速通道连接的两个VPC之间的互访流量会受VPC边界防火墙防护。关闭VPC边界防火墙的开关后，VPC边界防火墙不再防护通过高速通道连接的两个VPC之间的互访流量。

调用本接口前，必须已经调用CreateVpcFirewallConfigure接口创建了VPC边界防火墙。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyVpcFirewallSwitchStatus	系统规定参数。取值： ModifyVpcFirewallSwitchStatus 。
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（默认）：中文。 en：英文。

名称	类型	是否必选	示例值	描述
VpcFirewallId	String	是	vfw-m5e7dbc4y****	VPC边界防火墙的实例ID。 说明 您可以通过调用DescribeVpcFirewallList接口查询VPC边界防火墙的实例ID。
FirewallSwitch	String	是	open	设置VPC边界防火墙的开关状态。取值： <ul style="list-style-type: none"> open：开启。 close：关闭。
MemberUid	String	否	258039427902****	当前阿里云账号的成员账号UID。

返回数据

名称	类型	示例值	描述
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125afj2	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyVpcFirewallSwitchStatus
&Lang=zh
&VpcFirewallId=vfw-m5e7dbc4y****
&FirewallSwitch=open
&MemberUid=258039427902****
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyVpcFirewallSwitchStatusResponse>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125afj2</RequestId>
</ModifyVpcFirewallSwitchStatusResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "850A84D6-0DE4-4797-A1E8-00090125afj2"
}
```

4.9.15. BatchCopyVpcFirewallControlPolicy

调用BatchCopyVpcFirewallControlPolicy接口，从源VPC边界防火墙策略组拷贝所有策略到目标VPC边界防火墙策略组。

使用说明

本接口一般用于从一个VPC边界防火墙策略组拷贝所有策略到目标VPC边界防火墙策略组。

进行该操作之前，建议您先进行策略备份。关于策略备份的详细信息，请参见[策略备份](#)。

该操作完成后，目标VPC边界防火墙策略组内的策略会完全替换成源VPC边界防火墙策略组内的策略。

源VPC边界防火墙策略组和目标VPC边界防火墙策略组必须属于同一个阿里云账号。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	BatchCopyVpcFirewallControlPolicy	系统规定参数。取值：BatchCopyVpcFirewallControlPolicy。
SourceIps	String	否	192.0.XX.XX	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（默认）：中文。 en：英文。

名称	类型	是否必选	示例值	描述
SourceVpcFirewallId	String	是	vfw-a42bbb7b887148c9****	<p>该操作的源VPC边界防火墙的访问控制策略组ID。取值：</p> <ul style="list-style-type: none"> VPC边界防火墙防护云企业网内的网络实例（网络实例包含VPC、VBR和CCN）和指定VPC之间的互访流量时，策略组ID使用云企业网实例ID。 VPC边界防火墙防护通过高速通道连接的两个VPC之间的流量时，策略组ID使用VPC边界防火墙实例ID。 <p> 说明 您可以通过调用DescribeVpcFirewallAclGroupList接口获取该ID。</p>
TargetVpcFirewallId	String	是	vfw-e37d3a04cf79446a****	<p>该操作的目标VPC边界防火墙的访问控制策略组ID。取值：</p> <ul style="list-style-type: none"> VPC边界防火墙防护云企业网内的网络实例（网络实例包含VPC、VBR和CCN）和指定VPC之间的互访流量时，策略组ID使用云企业网实例ID。 VPC边界防火墙防护通过高速通道连接的两个VPC之间的流量时，策略组ID使用VPC边界防火墙实例ID。 <p> 说明 您可以通过调用DescribeVpcFirewallAclGroupList接口获取该ID。</p>

返回数据

名称	类型	示例值	描述
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125k6j3	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=BatchCopyVpcFirewallControlPolicy
&SourceIp=192.0.XX.XX
&Lang=zh
&SourceVpcFirewallId=vfw-a42bbb7b887148c9****
&TargetVpcFirewallId=vfw-e37d3a04cf79446a****
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<BatchCopyVpcFirewallControlPolicyResponse>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125k6j3</RequestId>
</BatchCopyVpcFirewallControlPolicyResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "850A84D6-0DE4-4797-A1E8-00090125k6j3"
}
```

4.9.16. CreateVpcFirewallCenConfigure

调用CreateVpcFirewallCenConfigure接口，创建VPC边界防火墙（防护云企业网内的网络实例和指定VPC之间的互访流量）。

使用说明

本接口一般用于为云企业网内的VPC实例创建VPC边界防火墙。该VPC边界防火墙可以防护云企业网内的网络实例（网络实例包含VPC、VBR和CCN）和指定VPC之间的互访流量，不支持防护VBR与VBR、CCN与CCN、VBR与CCN之间的互访流量。更多信息，请参见[VPC边界防火墙限制说明](#)。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	CreateVpcFirewallCenConfigure	系统规定参数。取值： CreateVpcFirewallCenConfigure 。
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（默认）：中文。 en：英文。

名称	类型	是否必选	示例值	描述
VpcFirewallName	String	是	测试用实例	VPC边界防火墙的实例名称。
NetworkInstanceId	String	是	vpc-bp10zlfhxh6j0232w****	创建VPC边界防火墙的VPC实例ID。
VpcRegion	String	是	cn-hangzhou	创建VPC边界防火墙的VPC所属地域ID。  说明 关于云防火墙支持地域的详细信息，请参见 支持的地域 。
FirewallSwitch	String	是	open	设置VPC边界防火墙的开关状态。取值： <ul style="list-style-type: none"> open（默认）：创建VPC边界防火墙后自动开启防护。 close：创建VPC边界防火墙后不自动开启防护。您可以调用接口 ModifyVpcFirewallCenSwitchStatus 开启防护。
CenId	String	是	cen-x5jayxou71ad73***	云企业网实例ID。
MemberUid	String	否	258039427902***	当前阿里云账号的成员账号UID。

返回数据

名称	类型	示例值	描述
VpcFirewallId	String	vfw-m5e7dbc4y****	VPC边界防火墙的实例ID。
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125h4j6	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateVpcFirewallCenConfigure
&Lang=zh
&VpcFirewallName=测试用实例
&NetworkInstanceId=vpc-bp10z1lifxh6j0232w****
&VpcRegion=cn-hangzhou
&FirewallSwitch=open
&CenId=cen-x5jayxou71ad73****
&MemberUid=258039427902****
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<CreateVpcFirewallCenConfigureResponse>
  <VpcFirewallId>vfw-m5e7dbc4y****</VpcFirewallId>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125h4j6</RequestId>
</CreateVpcFirewallCenConfigureResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "VpcFirewallId" : "vfw-m5e7dbc4y****",
  "RequestId" : "850A84D6-0DE4-4797-A1E8-00090125h4j6"
}
```

4.9.17. DeleteVpcFirewallCenConfigure

调用DeleteVpcFirewallCenConfigure接口，删除VPC边界防火墙（防护云企业网内的网络实例和指定VPC之间的互访流量）。

使用说明

本接口一般用于删除VPC边界防火墙。该VPC边界防火墙是防护云企业网内的网络实例（网络实例包含VPC、VBR和CCN）和指定VPC之间的互访流量。

调用本接口前，必须已经调用CreateVpcFirewallCenConfigure接口创建了VPC边界防火墙。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteVpcFirewallCenConfigure	系统规定参数。取值： DeleteVpcFirewallCenConfigure 。
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（默认）：中文。 en：英文。
MemberUid	String	否	258039427902****	当前阿里云账号的成员账号UID。
VpcFirewallIdList.N	String	是	vfw-m5e7dbc4y****	VPC边界防火墙的实例ID。 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> 说明 您可以通过调用 DescribeVpcFirewallCenList 接口查询VPC边界防火墙的实例ID。</p> </div>

返回数据

名称	类型	示例值	描述
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125k6j3	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteVpcFirewallCenConfigure
&Lang=zh
&VpcFirewallIdList=["vfw-m5e7dbc4y****"]
&MemberUid=258039427902****
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DeleteVpcFirewallCenConfigureResponse>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125k6j3</RequestId>
</DeleteVpcFirewallCenConfigureResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "850A84D6-0DE4-4797-A1E8-00090125k6j3"
}
```

4.9.18. DescribeVpcFirewallCenList

调用DescribeVpcFirewallCenList接口，查询VPC边界防火墙（防护云企业网内的网络实例和指定VPC之间的互访流量）的信息。

使用说明

本接口一般用于查询VPC边界防火墙的信息。该VPC边界防火墙是防护云企业网内的网络实例（网络实例包含VPC、VBR和CCN）和指定VPC之间的互访流量。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeVpcFirewallCenList	系统规定参数。取值： DescribeVpcFirewallCenList 。
Lang	String	否	zh	接收消息的语言类型。取值： <ul style="list-style-type: none"> zh（默认）：中文。 en：英文。
RegionNo	String	否	cn-hangzhou	VPC所在的地域ID。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 5px;"> ? 说明 关于云防火墙支持地域的详细信息，请参见支持的地域。 </div>
NetworkInstanceId	String	否	vpc-8vbwbo90rq0anm6t****	网络实例ID。

名称	类型	是否必选	示例值	描述
FirewallSwitchStatus	String	否	opened	<p>VPC边界防火墙的状态。取值：</p> <ul style="list-style-type: none"> opened：已开启。 closed：已关闭。 not configured：表示暂未配置VPC边界防火墙。 configured：表示已配置VPC边界防火墙。 <p> 说明 不设置该参数表示查询所有状态的VPC边界防火墙。</p>
VpcFirewallId	String	否	vfw-m5e7dbc4y****	VPC边界防火墙的实例ID。
VpcFirewallName	String	否	测试环境防火墙	VPC边界防火墙的实例名称。
CenId	String	否	cen-x5jayou71ad73**	云企业网实例ID。
CurrentPage	String	否	1	分页查询时，设置当前页面的页码。 默认值为1，表示返回第1页数据。
PageSize	String	否	10	分页查询时，设置每页包含VPC边界防火墙的数量。 默认值为10，表示每页包含10条结果。最大值为50。
RouteMode	String	否	auto	<p>路由模式。取值：</p> <ul style="list-style-type: none"> auto：表示自动模式。 manual：表示手动模式。 <p> 说明 不设置该参数表示查询所有路由模式的VPC边界防火墙。</p>
MemberUid	String	否	258039427902****	当前阿里云账号的成员账号UID。

返回数据

名称	类型	示例值	描述
TotalCount	Integer	10	VPC边界防火墙的总数量。
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125k8g2	本次请求的ID。
VpcFirewalls	Array of Data		VPC边界防火墙的详细信息。
ConnectType	String	cen	VPC边界防火墙的互通类型。取值：cen，表示云企业网。
VpcFirewallId	String	vfw-m5e7dbc4y****	VPC边界防火墙的实例ID。
RegionStatus	String	enable	地域开放状态。取值： <ul style="list-style-type: none"> enable：已开放，表示该地域允许配置VPC边界防火墙。 disable：未开放，表示该地域不允许配置VPC边界防火墙。
CenId	String	cen-x5jayyou71ad73****	云企业网实例ID。
VpcFirewallName	String	测试防火墙	VPC边界防火墙的实例名称。
ResultCode	String	test	创建VPC边界防火墙的操作结果代码。取值： <ul style="list-style-type: none"> Unauthorized：表示存在未授权的网络实例，不允许创建VPC边界防火墙。 RegionDisable：表示网络实例所在的地域是VPC边界防火墙不支持的地域，不允许创建VPC边界防火墙。 OpsDisable：表示不允许创建VPC边界防火墙。 VbrNotSupport：表示云企业网中的VBR不支持创建VPC边界防火墙。 空字符串，表示该网络实例可以正常创建VPC边界防火墙。
CenName	String	测试云企业网	云企业网实例名称。

名称	类型	示例值	描述
FirewallSwitchStatus	String	opened	VPC边界防火墙开关的状态。取值： <ul style="list-style-type: none"> opened：已开启。 closed：已关闭。 notconfigured：表示暂未配置VPC边界防火墙。
LocalVpc	Object		VPC的详细信息。
VpcId	String	vpc-8vbwbo90rq0anm6t****	VPC的实例ID。
TransitRouterType	String	Basic	云企业网转发路由器（CEN-TR）的版本。取值： <ul style="list-style-type: none"> Basic：基础版。 Enterprise：企业版。
NetworkInstanceId	String	vpc-2zefk9fbn8j7v585g****	网络实例ID。
RouteMode	String	auto	路由模式。取值： <ul style="list-style-type: none"> auto：表示自动模式。 manual：表示手动模式。
RegionNo	String	cn-hangzhou	VPC所属地域ID。
AuthorizationStatus	String	authorized	VPC的授权状态。取值： authorized ，表示已授权。
ManualVSwitchId	String	vsw-zeq4o875u****	路由模式为手动模式时指定的vSwitch的ID。
OwnerId	Long	158039427902****	VPC所属阿里云账号的UID。
NetworkInstanceType	String	VPC	网络实例的类型。取值： <ul style="list-style-type: none"> VPC（Virtual Private Cloud）。 VBR（Virtual Border Router）。 CCN（Cloud Connect Network）。
VpcName	String	测试用实例	VPC的实例名称。

名称	类型	示例值	描述
SupportManualMode	String	0	路由模式是否支持手动模式。取值： <ul style="list-style-type: none"> 1：支持。 0：不支持。
NetworkInstanceName	String	测试业务VPC	网络实例的名称。
VpcCidrTableList	Array of cidrTable		VPC的网段列表信息。
RouteTableId	String	vtb-1234	VPC的路由表ID。
RouteEntryList	Array of routeEntry		VPC的路由条目列表。
NextHopInstanceId	String	vrt-m5eb5me6c3l5sezae****	VPC中的下一跳实例ID。
DestinationCidr	String	192.168.XX.XX/24	VPC的目标网段。
DefendCidrList	Array of String	10.0.XX.XX/24	VPC边界防火墙防护的网段。
IpsConfig	Object		IPS配置信息。
BasicRules	Integer	1	基础规则开关。取值： <ul style="list-style-type: none"> 1：开启状态。 0：关闭状态。
EnableAllPatch	Integer	1	虚拟补丁开关。取值： <ul style="list-style-type: none"> 1：开启状态。 0：关闭状态。
RunMode	Integer	0	IPS防御模式。取值： <ul style="list-style-type: none"> 1：拦截模式。 0：观察模式。
MemberUid	String	258039427902****	当前阿里云账号的成员账号UID。

名称	类型	示例值	描述
PrecheckStatus	String	failed	是否可以自动开墙。取值： <ul style="list-style-type: none"> passed：可以自动开墙。 failed：不可以自动开墙。 unknown：未知状态。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeVpcFirewallCenList
&Lang=zh
&RegionNo=cn-hangzhou
&NetworkInstanceId=vpc-8vbwo90rq0anm6t****
&FirewallSwitchStatus=opened
&VpcFirewallId=vfw-m5e7dbc4y****
&VpcFirewallName=测试环境防火墙
&CenId=cen-x5jayxou71ad73****
&CurrentPage=1
&PageSize=10
&RouteMode=auto
&MemberUid=258039427902****
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type: application/xml
<DescribeVpcFirewallCenListResponse>
  <TotalCount>10</TotalCount>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125k8g2</RequestId>
  <VpcFirewalls>
    <ConnectType>cen</ConnectType>
    <VpcFirewallId>vfw-m5e7dbc4y****</VpcFirewallId>
    <RegionStatus>enable</RegionStatus>
    <CenId>cen-x5jayxou7lad73****</CenId>
    <VpcFirewallName>测试防火墙</VpcFirewallName>
    <ResultCode>test</ResultCode>
    <CenName>测试云企业网</CenName>
    <FirewallSwitchStatus>opened</FirewallSwitchStatus>
    <LocalVpc>
      <VpcId>vpc-8vbwbo90rq0anm6t****</VpcId>
      <TransitRouterType>Basic</TransitRouterType>
      <NetworkInstanceId>vpc-2zefk9fbn8j7v585g****</NetworkInstanceId>
      <RouteMode>auto</RouteMode>
      <RegionNo>cn-hangzhou</RegionNo>
      <AuthorizationStatus>authorized</AuthorizationStatus>
      <ManualVSwitchId>vsw-zeq4o875u****</ManualVSwitchId>
      <NetworkInstanceType>VPC</NetworkInstanceType>
      <VpcName>测试用实例</VpcName>
      <SupportManualMode>0</SupportManualMode>
      <NetworkInstanceName>测试业务vpc</NetworkInstanceName>
      <VpcCidrTableList>
        <RouteTableId>vtb-1234</RouteTableId>
        <RouteEntryList>
          <NextHopInstanceId>vrt-m5eb5me6c3l5sezae****</NextHopInstanceId>
          <DestinationCidr>192.168.XX.XX/24</DestinationCidr>
        </RouteEntryList>
      </VpcCidrTableList>
      <DefendCidrList>10.0.XX.XX/24</DefendCidrList>
    </LocalVpc>
    <IpsConfig>
      <BasicRules>1</BasicRules>
      <EnableAllPatch>1</EnableAllPatch>
      <RunMode>0</RunMode>
    </IpsConfig>
    <MemberUid>258039427902****</MemberUid>
    <PrecheckStatus>failed</PrecheckStatus>
  </VpcFirewalls>
</DescribeVpcFirewallCenListResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "TotalCount" : 10,
  "RequestId" : "850A84D6-0DE4-4797-A1E8-00090125k8g2",
  "VpcFirewalls" : [ {
    "ConnectType" : "cen",
    "VpcFirewallId" : "vfw-m5e7dbc4y****",
    "RegionStatus" : "enable",
    "CenId" : "cen-x5jayxou71ad73****",
    "VpcFirewallName" : "测试防火墙",
    "ResultCode" : "test",
    "CenName" : "测试云企业网",
    "FirewallSwitchStatus" : "opened",
    "LocalVpc" : {
      "VpcId" : "vpc-8vbwbo90rq0anm6t****",
      "TransitRouterType" : "Basic",
      "NetworkInstanceId" : "vpc-2zefk9fbn8j7v585g****",
      "RouteMode" : "auto",
      "RegionNo" : "cn-hangzhou",
      "AuthorizationStatus" : "authorized",
      "ManualVSwitchId" : "vsw-zeq4o875u****",
      "NetworkInstanceType" : "VPC",
      "VpcName" : "测试用实例",
      "SupportManualMode" : "0",
      "NetworkInstanceName" : "测试业务vpc",
      "VpcCidrTableList" : [ {
        "RouteTableId" : "vtb-1234",
        "RouteEntryList" : [ {
          "NextHopInstanceId" : "vrt-m5eb5me6c3l5sezae****",
          "DestinationCidr" : "192.168.XX.XX/24"
        } ]
      } ]
    },
    "DefendCidrList" : [ "10.0.XX.XX/24" ]
  },
  "IpsConfig" : {
    "BasicRules" : 1,
    "EnableAllPatch" : 1,
    "RunMode" : 0
  },
  "MemberUid" : "258039427902****",
  "PrecheckStatus" : "failed"
} ]
}
```

4.9.19. DescribeVpcFirewallCenDetail

调用DescribeVpcFirewallCenDetail接口，查询VPC边界防火墙（防护云企业网内的网络实例和指定VPC之间的互访流量）的详细信息。

使用说明

本接口一般用于获取VPC边界防火墙的详细信息。该VPC边界防火墙是防护云企业网内的网络实例（网络实例包含VPC、VBR和CCN）和指定VPC之间的互访流量。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeVpcFirewallCenDetail	系统规定参数。取值： DescribeVpcFirewallCenDetail 。
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（默认）：中文。 en：英文。
VpcFirewallId	String	是	vfw-m5e7dbc4y****	VPC边界防火墙的实例ID。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 5px;"> <p> 说明 您可以调用DescribeVpcFirewallCenList接口查询VPC边界防火墙的实例ID。</p> </div>
NetworkInstanceId	String	否	vpc-2zefk9fbn8j7v585g****	创建VPC边界防火墙的VPC实例ID。

返回数据

名称	类型	示例值	描述
ConnectType	String	cen	VPC边界防火墙的互通类型。取值： cen ，表示云企业网。
VpcFirewallName	String	测试防火墙	VPC边界防火墙的实例名称。
VpcFirewallId	String	vfw-m5e7dbc4y****	VPC边界防火墙的实例ID。

名称	类型	示例值	描述
FirewallSwitchStatus	String	opened	VPC边界防火墙的开关状态。取值： <ul style="list-style-type: none"> opened：已开启。 closed：已关闭。 notconfigured：未配置。
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125g4d2	本次请求的ID。
LocalVpc	Object		VPC的详细信息。
VpcId	String	vpc-8vbwbo90rq0anm6t****	VPC的实例ID。
TransitRouterType	String	Basic	云企业网转发路由器（CEN-TR）的版本。取值： <ul style="list-style-type: none"> Basic：基础版。 Enterprise：企业版。
RouteMode	String	auto	路由模式。取值： <ul style="list-style-type: none"> auto：表示自动模式。 manual：表示手动模式。
NetworkInstanceId	String	vpc-2zefk9fbn8j7v585g****	创建VPC边界防火墙的VPC实例ID。
RegionNo	String	cn-hangzhou	VPC所属地域ID。
ManualVSwitchId	String	vsw-zeq4o875u****	路由模式为手动模式时指定的vSwitch的ID。
OwnerId	String	158039427902****	VPC所属阿里云账户的UID。
NetworkInstanceType	String	VPC	网络实例的类型。取值： VPC 。
VpcName	String	测试用实例	VPC的实例名称。
SupportManualMode	String	0	路由模式是否支持手动模式。取值： <ul style="list-style-type: none"> 1：支持。 0：不支持。

名称	类型	示例值	描述
TransitRouterId	String	tr-2zetwxskej633l3u1***	CEN-TR的实例ID。
AttachmentId	String	tr-attach-sxig7bye51fid5****	网络实例的连接ID。
NetworkInstanceName	String	测试业务vpc	网络实例的名称。
AttachmentName	String	本地测试	网络实例的连接名称
VpcCidrTableList	Array of cidrTable		VPC的网段列表信息。
RouteTableId	String	vtb-1234	VPC的路由表ID。
RouteEntryList	Array of routeEntry		VPC的路由条目列表。
NextHopInstanceId	String	vrt-m5eb5me6c3l5seaze****	VPC中的下一跳实例ID。
DestinationCidr	String	192.168.XX.XX/24	VPC的目标网段。
EniList	Array of eniInfo		弹性网卡列表。
EniId	String	eni-8vbhfosfqv2rff42****	VPC中弹性网卡的实例ID。
EniPrivateIpAddress	String	192.168.XX.XX	VPC中弹性网卡的私网IP。
DefendCidrList	Array of String	10.0.XX.XX/24	VPC边界防火墙防护的网段。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeVpcFirewallCenDetail
&Lang=zh
&VpcFirewallId=vfw-m5e7dbc4y****
&NetworkInstanceId=vpc-2zefk9fbn8j7v585g****
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeVpcFirewallCenDetailResponse>
  <ConnectType>cen</ConnectType>
  <VpcFirewallName>测试防火墙</VpcFirewallName>
  <VpcFirewallId>vfw-m5e7dbc4y****</VpcFirewallId>
  <FirewallSwitchStatus>opened</FirewallSwitchStatus>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125g4d2</RequestId>
  <LocalVpc>
    <VpcId>vpc-8vbwbo90rq0anm6t****</VpcId>
    <TransitRouterType>Basic</TransitRouterType>
    <RouteMode>auto</RouteMode>
    <NetworkInstanceId>vpc-2zefk9fbn8j7v585g****</NetworkInstanceId>
    <RegionNo>cn-hangzhou</RegionNo>
    <ManualVSwitchId>vsw-zeq4o875u****</ManualVSwitchId>
    <OwnerId>158039427902****</OwnerId>
    <NetworkInstanceType>VPC</NetworkInstanceType>
    <VpcName>测试用实例</VpcName>
    <SupportManualMode>0</SupportManualMode>
    <TransitRouterId>tr-2zetwxskej633l3u1****</TransitRouterId>
    <AttachmentId>tr-attach-sxig7bye51fid5****</AttachmentId>
    <NetworkInstanceName>测试业务vpc</NetworkInstanceName>
    <AttachmentName>本地测试</AttachmentName>
    <VpcCidrTableList>
      <RouteTableId>vtb-1234</RouteTableId>
      <RouteEntryList>
        <NextHopInstanceId>vrt-m5eb5me6c3l5sezae****</NextHopInstanceId>
        <DestinationCidr>192.168.XX.XX/24</DestinationCidr>
      </RouteEntryList>
    </VpcCidrTableList>
    <EniList>
      <EniId>eni-8vbhfosfqv2rff42****</EniId>
      <EniPrivateIpAddress>192.168.XX.XX</EniPrivateIpAddress>
    </EniList>
    <DefendCidrList>10.0.XX.XX/24</DefendCidrList>
  </LocalVpc>
</DescribeVpcFirewallCenDetailResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "ConnectType" : "cen",
  "VpcFirewallName" : "测试防火墙",
  "VpcFirewallId" : "vfw-m5e7dbc4y****",
  "FirewallSwitchStatus" : "opened",
  "RequestId" : "850A84D6-0DE4-4797-A1E8-00090125g4d2",
  "LocalVpc" : {
    "VpcId" : "vpc-8vbwbo90rq0anm6t****",
    "TransitRouterType" : "Basic",
    "RouteMode" : "auto",
    "NetworkInstanceId" : "vpc-2zefk9fbn8j7v585g****",
    "RegionNo" : "cn-hangzhou",
    "ManualVSwitchId" : "vsw-zeq4o875u****",
    "OwnerId" : "158039427902****",
    "NetworkInstanceType" : "VPC",
    "VpcName" : "测试用实例",
    "SupportManualMode" : "0",
    "TransitRouterId" : "tr-2zetwxskej633l3ul****",
    "AttachmentId" : "tr-attach-sxig7bye51fid5****",
    "NetworkInstanceName" : "测试业务vpc",
    "AttachmentName" : "本地测试",
    "VpcCidrTableList" : [ {
      "RouteTableId" : "vtb-1234",
      "RouteEntryList" : [ {
        "NextHopInstanceId" : "vrt-m5eb5me6c3l5sezae****",
        "DestinationCidr" : "192.168.XX.XX/24"
      } ]
    } ],
    "EniList" : [ {
      "EniId" : "eni-8vbhfosfqv2rff42****",
      "EniPrivateIpAddress" : "192.168.XX.XX"
    } ],
    "DefendCidrList" : [ "10.0.XX.XX/24" ]
  }
}
```

4.9.20. ModifyVpcFirewallCenConfigure

调用ModifyVpcFirewallCenConfigure接口，修改VPC边界防火墙（防护云企业网内的网络实例和指定VPC之间的互访流量）的配置信息。

使用说明

本接口一般用于修改VPC边界防火墙的配置信息。该VPC边界防火墙是防护云企业网内的网络实例（网络实例包含VPC、VBR和CCN）和指定VPC之间的互访流量。

调用本接口前，必须已经调用CreateVpcFirewallCenConfigure接口创建了VPC边界防火墙。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyVpcFirewallCenConfigure	系统规定参数。取值： ModifyVpcFirewallCenConfigure 。
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（默认）：中文。 en：英文。
VpcFirewallId	String	是	vfw-m5e7dbc4y****	VPC边界防火墙的实例ID。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 5px;"> ? 说明 您可以通过调用DescribeVpcFirewallCenList接口查询VPC边界防火墙的实例ID。 </div>
VpcFirewallName	String	是	测试用实例	VPC边界防火墙的实例名称。
MemberUid	String	否	258039427902*****	当前阿里云账号的成员账号UID。

返回数据

名称	类型	示例值	描述
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125k6f8	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyVpcFirewallCenConfigure
&Lang=zh
&VpcFirewallId=vfw-m5e7dbc4y****
&VpcFirewallName=测试用实例
&MemberUid=258039427902****
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyVpcFirewallCenConfigureResponse>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125k6f8</RequestId>
</ModifyVpcFirewallCenConfigureResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "850A84D6-0DE4-4797-A1E8-00090125k6f8"
}
```

4.9.21. ModifyVpcFirewallCenSwitchStatus

调用ModifyVpcFirewallCenSwitchStatus接口，修改VPC边界防火墙（防护云企业网内的网络实例和指定VPC之间的互访流量）的开关状态。

使用说明

本接口一般用于修改VPC边界防火墙的开关状态。该VPC边界防火墙是防护云企业网内的网络实例（网络实例包含VPC、VBR和CCN）和指定VPC之间的互访流量。打开VPC边界防火墙的开关后，云企业网内的网络实例和指定VPC之间的互访流量会受VPC边界防火墙防护。关闭VPC边界防火墙的开关后，VPC边界防火墙不再防护云企业网内的网络实例和指定VPC之间的互访流量。

调用本接口前，必须已经调用CreateVpcFirewallCenConfigure接口创建了VPC边界防火墙。

QPS限制

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

调试

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

请求参数

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

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（默认）：中文。 en：英文。
VpcFirewallId	String	是	vfw-m5e7dbc4y****	VPC边界防火墙的实例ID。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 5px;"> <p> 说明 您可以通过调用 DescribeVpcFirewallCenList 接口查询VPC边界防火墙的实例ID。</p> </div>
FirewallSwitch	String	是	open	设置VPC边界防火墙的开关状态。取值： <ul style="list-style-type: none"> open：开启。 close：关闭。
MemberUid	String	否	258039427902*** *	当前阿里云账号的成员账号UID。

返回数据

名称	类型	示例值	描述
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125afj2	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyVpcFirewallCenSwitchStatus
&Lang=zh
&VpcFirewallId=vfw-m5e7dbc4y****
&FirewallSwitch=open
&MemberUid=258039427902****
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyVpcFirewallCenSwitchStatusResponse>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125afj2</RequestId>
</ModifyVpcFirewallCenSwitchStatusResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "850A84D6-0DE4-4797-A1E8-00090125afj2"
}
```

4.9.22. DescribeVpcFirewallDefaultIPSConfig

调用DescribeVpcFirewallDefaultIPSConfig接口，获取指定VPC边界防火墙的入侵防御配置信息。

使用说明

本接口一般用于获取指定VPC边界防火墙的入侵防御配置信息。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeVpcFirewallDefaultIPSConfig	系统规定参数。取值： DescribeVpcFirewallDefaultIPSConfig 。
VpcFirewallId	String	是	vfw-m5e7dbc4y****	VPC边界防火墙的实例ID。取值： <ul style="list-style-type: none"> VPC边界防火墙防护云企业网内的网络实例（网络实例包含VPC、VBR和CCN）和指定VPC之间的互访流量时，实例ID使用云企业网实例ID。您可以通过调用DescribeVpcFirewallCenList接口，查询云企业网的实例ID。 VPC边界防火墙防护通过高速通道连接的两个VPC之间的流量时，实例ID使用VPC边界防火墙实例ID。您可以通过调用DescribeVpcFirewallList接口，查询VPC边界防火墙的实例ID。
MemberUid	String	否	258039427902*** *	当前阿里云账号的成员账号UID。

返回数据

名称	类型	示例值	描述
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125adf1	本次请求的ID。
RunMode	Integer	0	IPS防御模式。取值： <ul style="list-style-type: none"> 1：拦截模式。 0：观察模式。
EnableAllPatch	Integer	1	虚拟补丁开关。取值： <ul style="list-style-type: none"> 1：开。 0：关。
BasicRules	Integer	1	基础规则开关。取值： <ul style="list-style-type: none"> 1：开。 0：关。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeVpcFirewallDefaultIPsConfig
&VpcFirewallId=vfw-m5e7dbc4y****
&MemberUid=258039427902****
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeVpcFirewallDefaultIPsConfigResponse>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125adf1</RequestId>
  <RunMode>0</RunMode>
  <EnableAllPatch>1</EnableAllPatch>
  <BasicRules>1</BasicRules>
</DescribeVpcFirewallDefaultIPsConfigResponse>
```

JSON 格式

```

HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "850A84D6-0DE4-4797-A1E8-00090125adf1",
  "RunMode" : 0,
  "EnableAllPatch" : 1,
  "BasicRules" : 1
}

```

4.9.23. ModifyVpcFirewallDefaultIPConfig

调用ModifyVpcFirewallDefaultIPConfig接口，修改VPC边界防火墙的入侵防御配置信息。

使用说明

本接口一般用于修改VPC边界防火墙的入侵防御配置信息。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyVpcFirewallDefaultIPConfig	系统规定参数。取值： ModifyVpcFirewallDefaultIPConfig 。
SourceIp	String	否	192.0.XX.XX	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（默认）：中文。 en：英文。

名称	类型	是否必选	示例值	描述
VpcFirewallId	String	是	vfw-m5e7dbc4y****	VPC边界防火墙的实例ID。取值： <ul style="list-style-type: none"> VPC边界防火墙防护云企业网内的网络实例（网络实例包含VPC、VBR和CCN）和指定VPC之间的互访流量时，实例ID使用云企业网实例ID。您可以通过调用DescribeVpcFirewallCenList接口，查询云企业网的实例ID。 VPC边界防火墙防护通过高速通道连接的两个VPC之间的互访流量时，实例ID使用VPC边界防火墙实例ID。您可以通过调用DescribeVpcFirewallList接口，查询VPC边界防火墙的实例ID。
BasicRules	String	是	1	基础规则开关。取值： <ul style="list-style-type: none"> 1：开。 0：关。
EnableAllPatch	String	是	1	虚拟补丁开关。取值： <ul style="list-style-type: none"> 1：开。 0：关。
RunMode	String	是	0	IPS防御模式。取值： <ul style="list-style-type: none"> 1：拦截模式。 0：观察模式。
MemberUid	String	否	258039427902****	当前阿里云账号的成员账号UID。

返回数据

名称	类型	示例值	描述
RequestId	String	3B51B5BF-3C26-5009-ADAB-190E58DE4D6E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyVpcFirewallDefaultIPConfig
&SourceIp=192.0.XX.XX
&Lang=zh
&VpcFirewallId=vfw-m5e7dbc4y****
&BasicRules=1
&EnableAllPatch=1
&RunMode=0
&MemberUid=258039427902****
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyVpcFirewallDefaultIPConfigResponse>
  <RequestId>3B51B5BF-3C26-5009-ADAB-190E58DE4D6E</RequestId>
</ModifyVpcFirewallDefaultIPConfigResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "3B51B5BF-3C26-5009-ADAB-190E58DE4D6E"
}
```

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。

使用说明

本接口一般用于添加访问控制的IP地址簿、ECS标签地址簿、端口地址簿或域名地址簿。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	AddAddressBook	系统规定参数。取值： AddAddressBook 。
SourceIp	String	否	192.0.XX.XX	访问者源IP地址。
Lang	String	否	zh	接收消息的语言类型。 <ul style="list-style-type: none">zh（默认）：中文。en：英文。

名称	类型	是否必选	示例值	描述
AddressList	String	否	192.0.XX.XX/32, 192.0.XX.XX/24	<p>地址簿的地址列表，多个地址间用英文逗号分隔。</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin: 5px 0;"> <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：192.0.XX.XX/32，192.0.XX.XX/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：example.com，aliyundoc.com。
Description	String	是	sz-001	地址簿的描述信息。
GroupName	String	是	sz-001	地址簿的名称。
GroupType	String	是	ip	<p>地址簿的类型，可选值包括：</p> <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。
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。</p> <ul style="list-style-type: none"> 1：表示自动添加。 0（默认）：表示不自动添加。
TagRelation	String	否	and	<p>待匹配的多个ECS标签间的关系。</p> <ul style="list-style-type: none"> and（默认）：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.TagValue	String	否	1	待匹配的ECS标签值。

名称	类型	是否必选	示例值	描述
TagList.N.TagKey	String	否	TXY	待匹配的ECS标签Key。

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

调用API的请求格式，请参见本文示例中的请求示例。

返回数据

名称	类型	示例值	描述
GroupUuid	String	f04ac7ce-628b-4cb7-be61-310222b7****	添加成功后返回的地址簿唯一标识ID。
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2****	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=AddAddressBook
&SourceIp=192.0.XX.XX
&Lang=zh
&AddressList=192.0.XX.XX/32, 192.0.XX.XX/24
&Description=sz-001
&GroupName=sz-001
&GroupType=ip
&AutoAddTagEcs=1
&TagRelation=and
&TagList=[{"TagValue":"1","TagKey":"TXY"}]
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<AddAddressBookResponse>
  <GroupUuid>f04ac7ce-628b-4cb7-be61-310222b7****</GroupUuid>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2****</RequestId>
</AddAddressBookResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "GroupUuid" : "f04ac7ce-628b-4cb7-be61-310222b7****",
  "RequestId" : "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2****"
}
```

5.2. DeleteAddressBook

调用DeleteAddressBook接口删除安全访问控制的地址簿。

使用说明

本接口一般用于删除访问控制中的地址簿。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteAddressBook	系统规定参数。取值： DeleteAddressBook 。
SourceIp	String	否	192.0.XX.XX	访问者源IP地址。
Lang	String	否	zh	请求和接收消息的语言类型。 <ul style="list-style-type: none">zh（默认）：中文en：英文
GroupUuid	String	是	0657ab9d-fe8b-4174-b2a6-6baf358e****	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。

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

调用API的请求格式，请参见本文示例中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125EEB1	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteAddressBook
&SourceIp=192.0.XX.XX
&Lang=zh
&GroupUuid=0657ab9d-fe8b-4174-b2a6-6baf358e****
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DeleteAddressBookResponse>
  <RequestId>850A84D6-0DE4-4797-A1E8-00090125EEB1</RequestId>
</DeleteAddressBookResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "850A84D6-0DE4-4797-A1E8-00090125EEB1"
}
```

5.3. ModifyAddressBook

调用ModifyAddressBook接口修改访问控制策略中设置的地址簿。

使用说明

本接口一般用于修改访问控制策略中设置的地址簿。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyAddressBook	系统规定参数。取值： ModifyAddressBook 。
SourceIp	String	否	192.0.XX.XX	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（默认）：中文 en：英文
AddressList	String	否	192.0.XX.XX/32, 192.0.XX.XX/24	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。 <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.XX.XX/32，1.2.XX.XX/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。
Description	String	是	bj-001	地址簿的描述信息。
GroupName	String	是	bj-001	地址簿的名称。
GroupUuid	String	是	0657ab9d-fe8b-4174-b2a6-6baf358e****	地址簿的唯一标识ID。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <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>
AutoAddTagEcs	String	否	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

名称	类型	是否必选	示例值	描述
TagRelation	String	否	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。
TagList.N.TagValue	String	否	1	待匹配的ECS标签值。
TagList.N.TagKey	String	否	TXY	待匹配的ECS标签Key。

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

调用API的请求格式，请参见本文[示例](#)中的请求示例。

返回数据

名称	类型	示例值	描述
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyAddressBook
&SourceIp=192.0.XX.XX
&Lang=zh
&AddressList=192.0.XX.XX/32,192.0.XX.XX/24
&Description=bj-001
&GroupName=bj-001
&GroupUuid=0657ab9d-fe8b-4174-b2a6-6baf358e****
&AutoAddTagEcs=1
&TagRelation=and
&TagList=[{"TagValue":"1","TagKey":"TXY"}]
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyAddressBookResponse>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
</ModifyAddressBookResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}
```

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。

使用说明

本接口一般用于查询访问控制策略地址簿的详细信息。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeAddressBook	系统规定参数。取值： DescribeAddressBook 。
SourceIp	String	否	192.0.XX.XX	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（默认）：中文。 en：英文。
CurrentPage	String	否	1	分页查询时，设置当前页面的页码。默认值为1，表示返回第1页数据。

名称	类型	是否必选	示例值	描述
PageSize	String	否	10	分页查询时，设置每页包含的地址簿的数量。 默认值为10，表示每页包含10条结果。最大值为50。
Query	String	否	192.0.XX.XX	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。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p>? 说明 不设置该参数表示查询IP地址簿和ECS标签地址簿。</p> </div>
ContainPort	String	否	80	查询包含指定端口的地址簿。仅当GroupType参数的值为port时，该参数才会作为本次查询的条件。

返回数据

名称	类型	示例值	描述
PageNo	String	1	当前页面的页码。
PageSize	String	10	每页包含的地址簿的数量。
RequestId	String	B36F150A-1E27-43AA-B72C-D2AC712F09DA	结果的请求ID。
TotalCount	String	100	地址簿的总数量。
Acls	Array of Acl		地址簿信息。
AddressListCount	Integer	2	地址簿中包含地址的个数。

名称	类型	示例值	描述
GroupUuid	String	f04ac7ce-628b-4cb7-be61-310222b7****	地址簿的唯一标识ID。
AutoAddTagEcs	Integer	1	是否自动添加新匹配标签的ECS（新购且完成标签设置的ECS或修改标签的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。
GroupName	String	demo_address_book	地址簿的名称。
ReferenceCount	Integer	3	地址簿被引用次数。
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。
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。
TagList	Array of TagListItem		地址簿支持自动添加的待匹配ECS标签信息。
TagValue	String	全部VALUE	待匹配的ECS标签值。
TagKey	String	company	待匹配的ECS标签Key。
AddressList	Array of String	["192.168.XX.XX/32", "192.168.XX.XX/32"]	地址簿的地址列表信息。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeAddressBook
&SourceIp=192.0.XX.XX
&Lang=zh
&CurrentPage=1
&PageSize=10
&Query=192.0.XX.XX
&GroupType=ip
&ContainPort=80
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeAddressBookResponse>
  <PageNo>1</PageNo>
  <PageSize>10</PageSize>
  <RequestId>B36F150A-1E27-43AA-B72C-D2AC712F09DA</RequestId>
  <TotalCount>100</TotalCount>
  <Acls>
    <AddressListCount>2</AddressListCount>
    <GroupUuid>f04ac7ce-628b-4cb7-be61-310222b7****</GroupUuid>
    <AutoAddTagEcs>1</AutoAddTagEcs>
    <Description>DEMO地址簿</Description>
    <GroupName>demo_address_book</GroupName>
    <ReferenceCount>3</ReferenceCount>
    <GroupType>ip</GroupType>
    <TagRelation>and</TagRelation>
    <TagList>
      <TagValue>全部VALUE</TagValue>
      <TagKey>company</TagKey>
    </TagList>
    <AddressList>[ "192.168.XX.XX/32", "192.168.XX.XX/32" ]</AddressList>
  </Acls>
</DescribeAddressBookResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "PageNo" : "1",
  "PageSize" : "10",
  "RequestId" : "B36F150A-1E27-43AA-B72C-D2AC712F09DA",
  "TotalCount" : "100",
  "Acls" : [ {
    "AddressListCount" : 2,
    "GroupUuid" : "f04ac7ce-628b-4cb7-be61-310222b7****",
    "AutoAddTagEcs" : 1,
    "Description" : "DEMO地址簿",
    "GroupName" : "demo_address_book",
    "ReferenceCount" : 3,
    "GroupType" : "ip",
    "TagRelation" : "and",
    "TagList" : [ {
      "TagValue" : "全部VALUE",
      "TagKey" : "company"
    } ],
    "AddressList" : [ "[ \"192.168.XX.XX/32\", \"192.168.XX.XX/32\" ]" ]
  } ]
}
```

6.多账号管控

6.1. ModifyInstanceMemberAttributes

调用ModifyInstanceMemberAttributes接口，更新云防火墙成员账号信息。

使用说明

本接口一般用于更新云防火墙成员账号信息。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	ModifyInstanceMemberAttributes	系统规定参数。取值： ModifyInstanceMemberAttributes 。
Members.N.MemberDesc	String	是	renewal	云防火墙成员账号的备注信息。
Members.N.MemberUid	Long	是	1234123412341234	云防火墙成员账号的UID。

返回数据

名称	类型	示例值	描述
RequestId	String	AB74E747-BA5C-492C-87DD-CEA67FCFFFE5	本次请求的ID。

示例

请求示例

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

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyInstanceMemberAttributesResponse>
<RequestId>AB74E747-BA5C-492C-87DD-CEA67FCFFFE5</RequestId>
</ModifyInstanceMemberAttributesResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "AB74E747-BA5C-492C-87DD-CEA67FCFFFE5"
}
```

6.2. DescribeInstanceMembers

调用DescribeInstanceMembers接口，获取云防火墙成员账号信息。

使用说明

本接口一般用于查询云防火墙成员账号信息。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeInstanceMembers	系统规定参数。取值： DescribeInstanceMembers 。
CurrentPage	String	否	1	分页查询时，返回第几页数据。默认值为1，表示返回第1页数据。
PageSize	String	否	20	分页查询时，每页包含多少条结果。默认值为20，表示每页包含20条结果。
MemberUid	String	否	258039427902*** *	云防火墙成员账号的UID。
MemberDisplayName	String	否	cloudfirewall_2	云防火墙成员账号的名称。

名称	类型	是否必选	示例值	描述
MemberDesc	String	否	renewal	云防火墙成员账号的备注信息，长度为1~256个字符。

返回数据

名称	类型	示例值	描述
RequestId	String	A531AE1A-FBA2-48B6-BAB8-84D02BD409EE	本次请求的ID。
PageInfo	Object		分页查询时的页面信息。
CurrentPage	Integer	1	本次查询第几页数据。
PageSize	Integer	20	本次查询每页包含多少条结果。
TotalCount	Integer	20	云防火墙成员账号的总数量。
Members	Array of Data		云防火墙成员账号的信息。
MemberDesc	String	renewal	云防火墙成员账号的备注信息。
MemberDisplayName	String	cloudfirewall_2	云防火墙成员账号的名称。
CreateTime	Integer	1615189819	云防火墙成员账号的加入时间。使用时间戳格式，单位：秒。
MemberUid	Long	258039427902****	云防火墙成员账号的UID。
MemberStatus	String	normal	云防火墙成员账号的状态。取值： <ul style="list-style-type: none"> normal：正常 deleting：删除中
ModifyTime	Integer	1615189819	云防火墙成员账号的最近修改时间。使用时间戳格式，单位：秒。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeInstanceMembers
&CurrentPage=1
&PageSize=20
&MemberUid=258039427902****
&MemberDisplayName=cloudfirewall_2
&MemberDesc=renewal
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeInstanceMembersResponse>
  <RequestId>A531AE1A-FBA2-48B6-BAB8-84D02BD409EE</RequestId>
  <PageInfo>
    <CurrentPage>1</CurrentPage>
    <PageSize>20</PageSize>
    <TotalCount>20</TotalCount>
  </PageInfo>
  <Members>
    <MemberDesc>renewal</MemberDesc>
    <MemberDisplayName>cloudfirewall_2</MemberDisplayName>
    <CreateTime>1615189819</CreateTime>
    <MemberStatus>normal</MemberStatus>
    <ModifyTime>1615189819</ModifyTime>
  </Members>
</DescribeInstanceMembersResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "A531AE1A-FBA2-48B6-BAB8-84D02BD409EE",
  "PageInfo" : {
    "CurrentPage" : 1,
    "PageSize" : 20,
    "TotalCount" : 20
  },
  "Members" : [ {
    "MemberDesc" : "renewal",
    "MemberDisplayName" : "cloudfirewall_2",
    "CreateTime" : 1615189819,
    "MemberStatus" : "normal",
    "ModifyTime" : 1615189819
  } ]
}
```

6.3. DeleteInstanceMembers

调用DeleteInstanceMembers接口，删除云防火墙成员账号。

使用说明

调用DeleteInstanceMembers接口一次最多可删除20个云防火墙成员账号，多个成员账号之间使用英文逗号(,)分隔。成员账号被删除后，云防火墙无法访问被删除成员账号的云资源，请谨慎操作。

删除前，调用DescribeInstanceMembers接口获取云防火墙成员账号信息。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DeleteInstanceMembers	系统规定参数。取值：DeleteInstanceMembers。
MemberUids.N	Long	是	258039427902*** *	云防火墙成员账号的UID列表。

返回数据

名称	类型	示例值	描述
RequestId	String	03E8AA70-0CC9-42EA-97AA-EA68377930B4	本次请求的ID。

示例

请求示例

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

正常返回示例

XML 格式

```

HTTP/1.1 200 OK
Content-Type:application/xml
<DeleteInstanceMembersResponse>
  <RequestId>03E8AA70-0CC9-42EA-97AA-EA68377930B4</RequestId>
</DeleteInstanceMembersResponse>

```

JSON 格式

```

HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "03E8AA70-0CC9-42EA-97AA-EA68377930B4"
}

```

6.4. AddInstanceMembers

调用AddInstanceMembers接口，添加云防火墙成员账号。

使用说明

本接口一般用于添加云防火墙成员账号。

QPS限制

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

调试

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

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	AddInstanceMembers	系统规定参数。取值：AddInstanceMembers。
Members.N.MemberDesc	String	否	renewal	云防火墙成员账号的备注信息，长度为1~256个字符。
Members.N.MemberUid	Long	是	258039427902*** *	云防火墙成员账号的UID。

返回数据

名称	类型	示例值	描述
----	----	-----	----

名称	类型	示例值	描述
RequestId	String	B40A54DF-C142-44F7-8441-B31C1EADB36E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=AddInstanceMembers
&Members=[{"MemberDesc":"renewal"}]
&公共请求参数
```

正常返回示例

XML 格式

```
HTTP/1.1 200 OK
Content-Type:application/xml
<AddInstanceMembersResponse>
  <RequestId>B40A54DF-C142-44F7-8441-B31C1EADB36E</RequestId>
</AddInstanceMembersResponse>
```

JSON 格式

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "B40A54DF-C142-44F7-8441-B31C1EADB36E"
}
```