阿里云
DDoS高防IP

DDoS防护包

文档版本：20191223

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. **阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，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
	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。	 **禁止:** 重置操作将丢失用户配置数据。
	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。
	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。
	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。	执行`cd /d C:/window`命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{}或者{a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

法律声明..... I
通用约定..... I
1 产品简介..... 1
1.1 什么是DDoS防护包..... 1
1.2 应用场景..... 2
2 产品定价..... 5
2.1 计费方式..... 5
3 快速入门..... 8
3.1 购买DDoS防护包..... 8
3.2 为遭受攻击的IP开通DDoS防护包..... 9
4 用户指南..... 11
4.1 添加防护对象IP..... 11
4.2 设置DDoS防护包实例的备注名称..... 12
4.3 查看安全报表..... 13
4.4 解除黑洞..... 14
4.5 管理抗D流量包..... 15
4.6 查看操作日志..... 16
4.7 DDoS防护包升级DDoS高防IP..... 17
5 最佳实践..... 19
5.1 DDoS防护包黑洞自动解除最佳实践..... 19
5.2 DDoS原生防护（防护包）+高防组合使用方案..... 22
6 API参考..... 36
6.1 API概览..... 36
6.2 调用方式..... 37
6.3 公共参数..... 39
6.4 防护..... 41
6.4.1 AddIp..... 41
6.4.2 DeleteIp..... 42
6.4.3 DeleteBlackhole..... 43
6.5 实例..... 45
6.5.1 DescribeRegions..... 45
6.5.2 DescribeInstanceList..... 47
6.5.3 DescribeInstanceSpecs..... 51
6.5.4 DescribeExcpetionCount..... 54
6.5.5 DescribePackIpList..... 55
6.5.6 ModifyRemark..... 58
6.5.7 CheckGrant..... 59
6.6 流量包..... 61
6.6.1 DescribeResourcePackInstances..... 61

6.6.2 DescribeResourcePackStatistics....63
6.6.3 DescribeResourcePackUsage....65
6.6.4 DescribePackPaidTraffic....67
6.7 图表日志....70
6.7.1 DescribeDdosEvent....70
6.7.2 DescribeOpEntities....72
6.7.3 DescribeTraffic....75
6.8 ListTagKeys....78
7 常见问题....81
7.1 DDoS防护包常见问题....81
7.2 防护包添加防护IP时收到“IP不属于你”的错误提示....82
8 相关协议....84
8.1 DDoS防护包服务条款....84

1 产品简介

1.1 什么是DDoS防护包

DDoS防护包是一款针对云上ECS、SLB、Web应用防火墙、EIP等云产品直接提升DDoS防御能力的安全产品。相比于DDoS高防，DDoS防护包可以直接把防御能力加载到云产品上，不需要更换IP，也没有四层端口、七层域名数等限制。同时，DDoS防护包部署简易，购买后只需要绑定需要防护的云产品的IP地址即可使用，几分钟内生效。

优势

DDoS防护包具有以下优势。

- **即刻购买，即刻生效。最短一分钟内即可完成DDoS防护包的部署，直接把防御能力加载到云产品，免去部署和切换IP的烦恼。**
- **具备弹性防护能力，遭受大规模攻击时调用当前地域阿里云最大DDoS防护能力提供全力防护。**
- **采用阿里云BGP带宽，覆盖电信、联通、移动、教育网、长城宽带等不同的运营商，只需要一个IP，即可实现多个不同运营商的极速访问。**
- **海量清洗带宽，满足活动大促、活动上线、重要业务的安全稳定性保障需求。**
- **支持多个IP共享防护能力，满足多个IP地址都需要提升防御带宽的需求。**

使用限制

DDoS防护包目前仅支持华东1（杭州）、华东2（上海）、华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、华南1（深圳）地域。

计费方式

DDoS防护包的实际费用包括保底防护带宽费用和弹性防护流量费用。

- **保底防护带宽费用：根据DDoS防护包的规格，一次性支付DDoS防护包的保底带宽费用。关于如何购买DDoS防护包，请参见*购买DDoS防护包*。**
- **弹性防护流量费用：根据DDoS防护包实例全部入方向流量计算弹性防护流量费用。需要通过您额外购买的抗D流量包，抵扣DDoS防护包实际产生的弹性防护流量。**

弹性防护能力（抗D流量包）

如果您的DDoS防护包需要具备弹性防护能力，您可以通过购买抗D流量包来抵扣您的DDoS防护包所产生的弹性防护流量费用。

说明:

购买DDoS防护包时，您将获得包含一定流量的抗D流量包供您免费使用（企业版防护包实例赠送30 TB弹性防护流量）。因此，您可以安心为您的DDoS防护包开启弹性防护功能。

弹性防护流量计费区间

DDoS防护包的弹性流量计费周期为五分钟，即每五分钟根据企业版防护包实例的全部入方向流量计算弹性防护流量费用，并消耗抗D流量包中的流量。

弹性防护流量计算示例

在一个弹性防护流量计费周期（五分钟）内，您的企业版DDoS防护包实例入方向的带宽为100Mbps（无论是否遭受攻击），则该计费周期内的弹性防护总流量为3.75GB = 300[秒，计费周期] * 0.1[Gbps，入方向带宽] * /8[单位转换]。因此，在该弹性防护流量计费周期内，您的抗D流量包需要被扣除3.75GB的流量。

您可根据实际日常流量计算可能产生的弹性防护流量，选购所需的抗D流量包规格。关于如何购买抗D流量包，请参见购买抗D流量包。

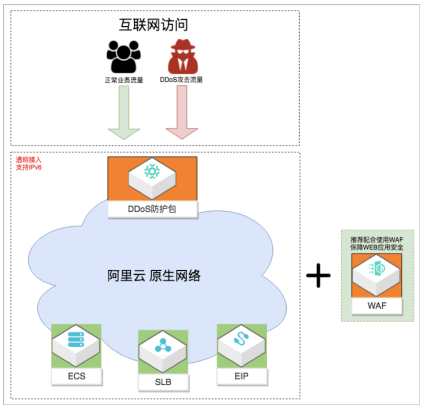
1.2 应用场景

DDoS防护包主要提供针对三层四层流量型攻击的防护。当流量超出DDoS防护包的默认清洗阈值后，自动触发流量清洗，实现DDoS攻击防护。

概述

DDoS防护包适用于部署在阿里云上的业务，能够满足业务规模大、对网络质量要求高的客户。此类型客户虽然遭受DDoS攻击风险较低，但是一旦遭受DDoS攻击导致业务中断或受损，将会带来巨大的商业损失。阿里云DDoS防护包可在最小接入成本的情况下提升DDoS防护能力，降低DDoS攻击对业务带来的潜在风险。具体地，DDoS防护包应用于以下场景：

- **资源部署在阿里云上。**
- **需要保护的公网IP数量多。**
- **业务带宽或QPS较大。**
- **具有IPv6访问流量的防护需求。**



DDoS攻击类型

下表描述了DDoS防护包适合防御的DDoS攻击类型。

攻击类型	是否适用	最佳防御配置
SSDP、NTP、Memcached等反射型攻击	是	推荐使用DDoS防护包 > SLB > ECS的部署方式，通过负载均衡（SLB）丢弃未监听协议和端口的流量，获得更好的防护效果。
UDP Flood攻击	是	推荐使用DDoS防护包 > SLB > ECS的部署方式，通过负载均衡（SLB）丢弃未监听协议和端口的流量，获得更好的防护效果。
SYN Flood攻击（大包攻击）	是	推荐使用DDoS防护包 > SLB > ECS的部署方式，通过负载均衡（SLB）丢弃未监听协议和端口的流量，获得更好的防护效果。
SYN Flood攻击（小包攻击）	效果一般	推荐使用高防IP服务进行防护。
连接数攻击	否	推荐使用高防IP服务或游戏盾服务。
CC攻击	否	推荐使用“DDoS防护包+WAF”的部署方式，由Web应用防火墙（WAF）防御CC攻击、DDoS防护包防御流量攻击，获得更好的防护效果。
Web攻击	否	推荐使用“DDoS防护包+WAF”的部署方式，由Web应用防火墙（WAF）防御诸如SQL注入等Web应用攻击、DDoS防护包防御流量攻击，获得更好的防护效果。

业务场景

下表描述了DDoS防护包适用的业务场景。

业务类型	是否适用	最佳防御配置
网站类业务	是	推荐使用DDoS防护包 > SLB > ECS的部署方式，通过负载均衡（SLB）丢弃未监听协议和端口的流量，获得更好的防护效果。 如果网站需要防护CC攻击和Web攻击，推荐使用“DDoS防护包+WAF”的部署方式，由Web应用防火墙（WAF）防御CC攻击和Web攻击、DDoS防护包防御流量攻击。
游戏类业务	否	推荐使用游戏盾服务进行防护。
UDP服务类业务	否	推荐使用高防IP服务或游戏盾服务进行防护。
App应用类业务	是	推荐使用DDoS防护包 > SLB > ECS的部署方式，通过负载均衡（SLB）丢弃未监听协议和端口的流量，获得更好的防护效果。

2 产品定价

2.1 计费方式

DDoS原生防护企业版按照包年包月（预付费）方式计费。在使用包年包月资源前，您必须创建一个DDoS原生防护企业版实例。DDoS原生防护企业版实例的包年单价由要防护的云资源的业务规模和接入保护的IP数量决定。您只需选择与自身业务规模匹配的实例规格并完成一次性付费，即可享用DDoS原生防护企业版服务。

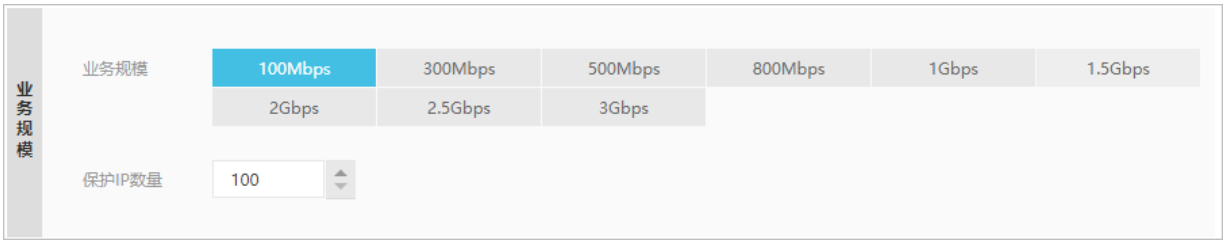
注意:

本文所述计费方式自2019年10月1日起生效。如果在此之前您已使用“保底防护带宽+弹性防护流量”的旧版计费方式开通DDoS原生防护（防护包）企业版实例，请参见*DDoS*原生防护计费方式调整说明。

DDoS原生防护企业版实例规格

DDoS原生防护企业版实例默认提供20G的保底防护带宽和全力防护的弹性防护能力。全力防护指根据当前机房网络和整体水位，尽可能对攻击进行防护，并且随着阿里云网络能力的不断提升，全力防护也会提升防护能力，不需要您额外付出升级成本。

DDoS原生防护企业版实例仅支持按年开通服务，订购时长包括1年、2年、3年。在创建包年包月DDoS原生防护企业版实例时，单个实例的包年单价由您选择的业务规模和保护IP数量决定。



- 业务规模：指被防护业务的正常业务规模，以带宽来衡量，in/out取按月95最大值，可选规格：
  100Mbps、300Mbps、500Mbps、800Mbps、1Gbps、1.5Gbps、2Gbps、2.5Gbps、3Gbps。

  您可以按照以下方式估算业务规模（业务带宽）：

  以5分钟为粒度采样，采集入方向和出方向的流量并计算入方向和出方向在5分钟内的平均带宽值，取入方向和出方向中较大的值作为采样点的带宽值。月底将所有的采样点按峰值从高到低排序，去掉5%的最高峰值采样点，以第95%个最高峰作为95计费点带宽。

  下图是计费点带宽的示意图，以一个月30天为例。

  如果实际业务带宽超过已购买的原生防护企业版实例的业务规模，会有什么影响?

  原生防护企业版允许业务流量短期峰值超过购买的业务规模规格，但是如果一个月累计36小时超过规格，则全力防护会失效，仅保留20G防护能力，正常业务带宽不会受到限制。
- 保护IP数量：要使用DDoS原生防护实例保护的所有IP的数量，默认是100个，可选规格：100~255。

计费规则

下表描述了不同实例规格的具体计费规则。

计费项	计费规则
基础月单价	固定为40,100元/月。
业务规模	每100Mbps业务带宽的包月单价为6,700元。 说明: 默认100Mbps业务规模起售。若业务规模超过3Gbps，请联系我们定制。
保护IP数量	超过100时计费，每增加一个IP，其包月单价为200元。

计费示例

假设您要开通DDoS原生防护企业版实例，并选择1Gbps的业务规模，且保护IP数量为120个，则该实例的包年单价为：1,333,200（元）=（40,100 [基础月单价] + 6,700 [每100Mbps月单价] * 10 + 200 [每个增加IP的月单价] *20 [增加IP的数量]）*12 [月数]。

不支持退款说明

DDoS原生防护（防护包）实例不支持五天无理由退款。

DDoS原生防护计费方式调整说明

自2019年10月1日起，DDoS原生防护（防护包）采用新版计费方式，即“按业务规模一次性计费”，详见*DDoS*原生防护企业版实例规格。

说明:
关于旧版计费方式的更多信息，请参见*#unique_10*。

- **新购DDoS原生防护（防护包）实例不再支持通过“保底防护带宽+弹性防护流量”的旧版计费方式下单。**
- **已经通过“保底防护带宽+弹性防护流量”的旧版计费方式开通的实例，不再收取抗D流量包费用。**
- **已经通过“保底防护带宽+弹性防护流量”的旧版计费方式开通的实例，支持继续按照旧方式续费到2020年3月31。在此之后将逐步停止旧方式续费，需要切换新计费方式，您可以提交工单联系我们协助。**

相比于“保底防护带宽+弹性防护流量”的旧版计费方式，新版计费方式具备以下优势：

- **业务带宽比流量消耗大小更容易评估，便于企业客户快速评估防御成本。**
- **新方式一次性计算总费用，更适合企业客户申请预算。**
- **老方式弹性防护流量计费包含攻击和正常流量，新方式业务带宽不会算入攻击，成本更可控。**

新方式（按业务带宽计费）和旧方式（按弹性防护流量计费）间产生的实际费用基本一致。

假设您要防护的业务带宽平均是100Mbps，若按旧方式计算，则弹性防护流量费用=100Mpbs * 2678400 [秒，按31天计算一个月的总秒数] / 1000 [单位转换] * 0.2 [元/GB，抗D包流量单价] = 6,696元；使用新方式计算，则按每100Mbps业务带宽每月一次性计费为6,700元。

联系我们

您可以通过工单或联系商务经理定制指定规格的DDoS原生防护（防护包）。

3 快速入门

3.1 购买DDoS防护包

您可以参考以下操作步骤，购买DDoS防护包：

操作步骤

1. **登录阿里云*DDoS*防护包购买页面。**

2. **选择地域。**

> **说明:**
> **DDoS防护包实例的地域必须与需要绑定的防护对象（例如，ECS、SLB等云产品）所在的地域一致。**

3. **选择需要防护的IP类型：IPV6或者IPV4。**

> **说明:**

一个防护包实例只能对一种访问流量类型提供防护，不支持同时防护IPv6和IPv4两种类型的访问流量。如果您需要防护不同类型访问流量，请购买两个防护包实例并选择不同的IP类型。

4. 选择购买数量及购买时长。
5. 单击立即购买，完成支付。

说明:

关于DDoS防护包的详细计费说明，请参见*DDoS*防护包计费方式。

3.2 为遭受攻击的IP开通DDoS防护包

阿里云默认为您购买的所有具备公网IP的产品（ECS云服务器、SLB负载均衡、EIP弹性公网IP、Web应用防火墙）提供DDoS基础防护服务。当这些产品的公网IP遭受超过默认防护能力的DDoS攻击时，您可以立即付费开通DDoS防护包，利用该公网IP所在地域的最大DDoS攻击防护能力防护攻击，保障您的业务免受攻击影响。

背景信息

DDoS防护包企业版提供全力防护的弹性防护能力。当遭受攻击时，自动调度该企业版DDoS防护包实例所在地域的阿里云最大DDoS防护能力提供全力防护。

DDoS防护包的弹性防护将消耗抗D流量包中的流量，不会产生任何后付费。在您购买DDoS防护包实例时，您将获赠包含一定流量的抗D流量包用于抵扣DDoS防护包所消耗的弹性防护流量。当抗D流量包中的流量耗尽后，DDoS防护包实例的弹性阈值将自动下调为保底防护带宽的20G，您需要单独购买抗*D*流量包后重新恢复DDoS防护包的弹性防护能力。

准备工作

在购买开通DDoS防护包前，您应确认以下信息：

- 遭受攻击的IP地址。
- 遭受攻击的IP所在地域。

说明:

目前，DDoS防护包尚未在所有地域开通，因此您需要确认遭受攻击的IP所在的地域已开通DDoS防护包服务。关于DDoS防护包支持的地域信息，请参见什么是*DDoS*防护包。

- 遭受的攻击流量类型（IPv4或IPv6）。

操作步骤

1. 登录阿里云*DDoS*防护包购买页面。

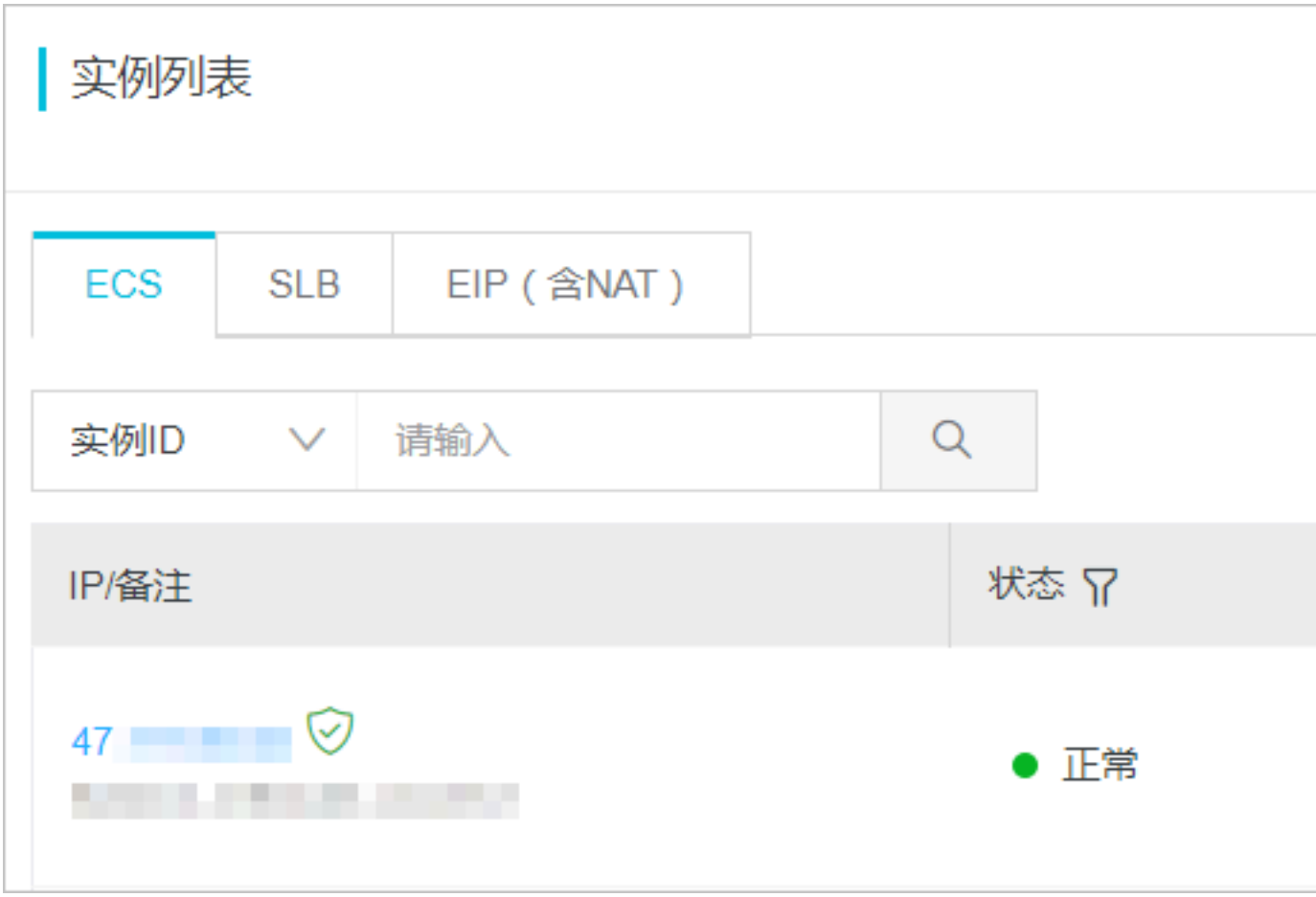
2. 参见购买DDoS防护包，购买DDoS防护包实例。

> **说明:**
> 您所选择的DDoS防护包的地域应与您需要防护的ECS、SLB、EIP等产品实例所在的地域一致。

3. 购买DDoS防护包实例并完成支付后，登录云盾DDoS防护管理控制台。
4. 定位到防护包 > 实例 页面，参见添加防护对象IP将需要防护的IP添加至已购买的DDoS防护包实例中进行防护。

预期结果

防护IP添加成功后，该IP即可享受所绑定的DDoS防护包实例的防护能力。在云盾DDoS防护管理控制台的基础防护 > 实例页面，您可以查看到该IP的防护阈值已经提升为所绑定的DDoS防护包实例的防护能力。



4 用户指南

4.1 添加防护对象IP

成功购买DDoS防护包后，参考以下操作步骤将需要防护的IP添加至DDoS防护包进行防护。

操作步骤

1. **登录云盾DDoS防护管理控制台。**
2. **定位到防护包 > 实例页面，选择您已购买的DDoS防护包。**

说明:

在防护包列表中可以查看已购买的DDoS防护包的规格、IP版本、到期时间等信息。

3. **单击添加防护对象。**

说明:

如果您是第一次使用DDoS防护包，您需要授权DDoS防护包防护您的其它云产品对象。

4. **在添加防护对象对话框，添加您想要防护的IP。**

说明:

DDoS防护包企业版实例支持添加最多100个防护IP。

5. 单击确定完成防护配置。根据您的防护包实例类型，防护包将直接为您所添加的防护对象IP提供DDoS防护能力。

在防护包实例中添加防护IP时，如果收到IP不属于你的错误提示，请参见添加防护对象IP报错问题。

4.2 设置DDoS防护包实例的备注名称

您可以为已购买的DDoS防护包实例设置备注名称。当拥有多个DDoS防护包实例时，您可以通过设置备注名称快速辨识和管理您的防护包实例。

背景信息

您可以根据防护包实例的使用对象、场景、范围等设置备注名称，帮助您有效区分不同用途的防护包实例。参考以下操作步骤，为您的防护包实例设置备注名称。

操作步骤

1. 登录云盾DDoS防护管理控制台。
2. 定位到防护包 > 实例页面，选择防护包实例所在的地域。

3. 选择您想要设置备注名称的防护包实例，单击编辑防护包实例备注名按钮。

4. 输入防护包实例备注名称，单击确定。

> **说明:**
> 备注名称长度为2-50个字符，只允许输入字母、汉字、数字或下划线（_）。

预期结果

设置成功后，备注名称将显示在DDoS防护包实例ID下方。

您也可以按照上述步骤随时修改DDoS防护包实例的备注名称，根据业务需要灵活调整备注名称。

4.3 查看安全报表

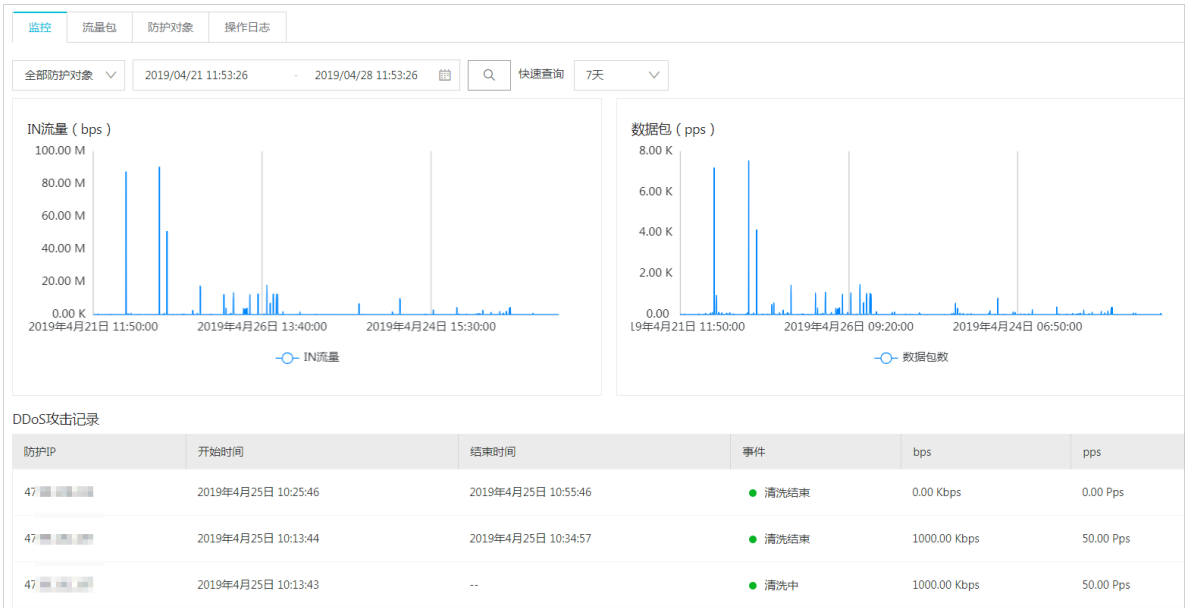
为您的防护包配置完防护IP后，您可以参考以下操作步骤查看该防护包的总流量信息、单个IP的流量信息和DDoS攻击事件记录。

操作步骤

1. 登录云盾DDoS防护管理控制台。
2. 定位到防护包 > 实例页面，选择防护包实例所在的地域。
3. 在防护包实例列表中，选择防护包实例，单击查看报表前往该防护包详情的监控页签。
4. 在防护包详情的监控页签前，查看该防护包的网络流量趋势（入方向流量和接收的数据包数）及DDoS攻击事件记录。

> **说明:**

您可以通过报表上方的过滤条件查看指定防护对象和时间范围（仅支持查看最近7天内的流量信息和事件记录）。



4.4 解除黑洞

DDoS防护包为已防护的IP提供黑洞解除功能，即您可以自行对某个处于黑洞状态的防护对象IP进行黑洞解除操作。

背景信息

购买DDoS防护包企业版的用户将获赠100次黑洞解除机会；且在您已购买的DDoS防护包的服务周期内，每月初将自动重置该防护包实例的黑洞解除次数。

说明:

上月未使用的剩余黑洞解除次数将不会累计至下月。

由于黑洞解除涉及阿里云后台系统的风控管理策略，解除黑洞操作可能失败（解除失败时不会扣减您的剩余黑洞解除次数）。如果出现未能成功解除的情况，请您耐心等待一段时间后再次尝试。

强烈建议您在执行黑洞解除操作前查看平台自动解封时间，如果您可以接受该自动解封时间，请您耐心等待。

操作步骤

1. **登录云盾*DDoS*防护管理控制台。**
2. **定位到防护包 > 实例页面，选择防护包实例所在的地区。**

3. 在防护包实例的操作栏中，单击解除黑洞前往该实例详情的防护对象页签。

> **说明：**
> 当该防护包实例所防护的IP被黑洞时，在异常IP数栏中将显示异常IP数。同时，在操作栏中出现解除黑洞。您也可以单击管理前往实例的详情页面，选择防护对象页签。

4. 在防护包详情的防护对象页签，选择处于黑洞中状态的防护对象，单击解除黑洞。

5. 在解决黑洞对话框中，查看剩余黑洞解除次数，单击确认。

> **说明：**
> 如果黑洞解除失败，您将收到失败提示信息，请耐心等待一段时间后再尝试；如果未收到提示信息，则表示黑洞状态已成功解除。

4.5 管理抗D流量包

购买抗D流量包后，您可以在防护包实例详情的流量包页签，查看当前可用流量包数量、可用流量、历史消耗流量等信息。

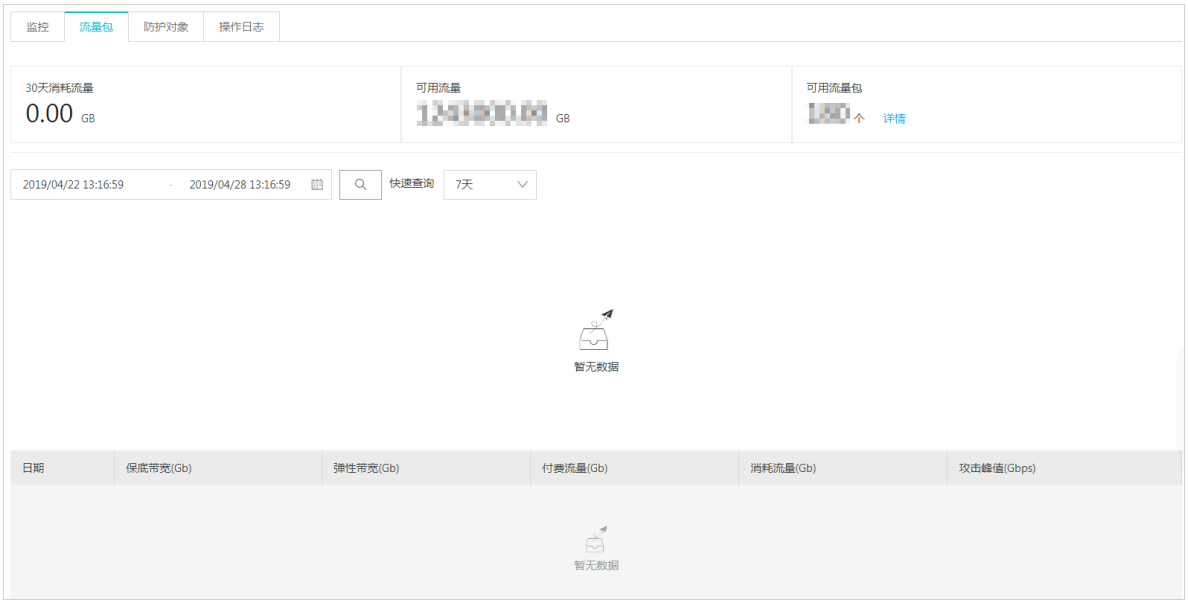
操作步骤

1. 登录云盾DDoS防护管理控制台。
2. 定位到防护包 > 实例页面，选择任意防护包实例，单击更多下拉菜单选择流量包消耗前往流量包页签，查看您所拥有的抗D流量包的相关信息和历史消耗记录。

   在流量包页签，您可以设置查询时间范围，查看该时间段内详细的历史流量消耗情况。

> **说明：**

支持查看最近7天内的流量消耗情况。



3. **单击可用流量包数量区块中的详情可前往抗D流量包详情页面，查看您拥有的所有抗D流量包详情信息，包括规格、剩余可用流量、失效时间等信息。**

4.6 查看操作日志

在云盾DDoS防护管理控制台，您可以查看DDoS防护包的相关操作日志，便于您追溯DDoS防护包的配置变更情况。

操作步骤

1. **登录云盾*DDoS*防护管理控制台。**
2. **定位到防护包 > 实例页面，选择防护包实例所在的地域。**
3. **在防护包实例列表中，选择防护包实例，单击管理前往实例详情页面。**
4. **在操作日志页签，设置查询时间范围，单击查询按钮。**

说明:

支持查看最近7天内的防护包操作日志。

5. 查看指定时间范围内该DDoS防护包的操作日志，包括操作时间、操作日志详情。

4.7 DDoS防护包升级DDoS高防IP

鉴于DDoS防护包产品的架构限制，在某些特定情况下，DDoS防护包提供的安全防护能力可能无法完全满足您的DDoS防护需求。如果DDoS防护包已无法满足您的安全防护需求，建议您切换至DDoS高防IP服务提升安全防护能力。

背景信息

关于DDoS防护包适用的安全防护场景，请参见*DDoS*防护包适用场景。

如果您已购买DDoS防护包实例，在实际使用过程中遇到以下问题，可以将已购买的DDoS防护包升级为DDoS高防IP服务：

- 遭受的DDoS攻击持续时间较长，因此大量消耗抗D流量包的防护流量导致防御成本较高。
- 防护的业务遭受CC攻击，而对此类攻击DDoS防护包无法防御。
- 其他特殊情况，需要您具体说明。

说明:
对于您已购买的DDoS防护包实例，我们将为您退回余款。

操作步骤

1. 通过您的专属服务钉钉群联系服务人员，说明详细情况。

   如果您尚未加入专属服务钉钉群，使用钉钉扫描下方二维码。

> 说明:
> 如果在DDoS防护包升级DDoS高防IP服务过程中遇到任何问题，请通过您的专属钉钉服务群联系服务人员。

2. 服务人员将根据您的实际情况判断是否满足升级条件。
3. 待服务人员确认满足升级条件后，将为您处理已购买的DDoS防护包实例的退款事宜。系统将根据您所购买的DDoS防护包实例的规格及剩余服务时长为您退回余款。

> 说明:
> 如果您的账号中有未消耗完的抗D流量包，系统也将一并退回余款。

4. 购买DDoS高防IP实例，将您的业务切换至所DDoS高防IP实例进行防护。

5 最佳实践

5.1 DDoS防护包黑洞自动解除最佳实践

添加至DDoS防护包的防护列表的业务IP遭受瞬时超大流量DDoS攻击时仍可能被黑洞，需要对被黑洞的IP快速执行黑洞解除操作恢复业务，保障业务稳定性。针对这一场景，企业版DDoS防护包提供黑洞自动化响应和快速解除的解决方案。

前提条件

DDoS防护包黑洞自动化响应和快速解除解决方案需要调用DDoS防护包的API接口，因此该解决方案仅支持企业版DDoS防护包实例。在部署黑洞自动解除方案前，确认您的业务IP已添加至企业版DDoS防护包实例进行防护。

背景信息

DDoS防护包提供黑洞解除功能，而手动解除黑洞可能存在延迟和不确定性。如果您的业务对于稳定性和连续性有较高的要求，您可以通过以下方案实现黑洞自动化响应和快速解除：

1. 通过云监控的事件告警功能监控DDoS防护包实例的黑洞事件。
2. 通过自定义消息的消费机制，调用DDoS防护包的黑洞解除API接口（#unique_24）自动解除被黑洞的业务IP。

> **说明:**
> 只有已添加为DDoS防护包实例的防护对象IP触发黑洞策略时，才会触发云监控的黑洞事件报警的消息推送。对于不在DDoS防护包实例的防护对象列表中的IP触发的黑洞事件将不会被推送。
>
> 由于黑洞解除涉及阿里云后台系统的风控管理策略，解除黑洞操作可能失败（解除失败时不会扣减您的剩余黑洞解除次数）。如果出现未能成功解除的情况，请您耐心等待一段时间后再次尝试。
>
> 强烈建议您在执行黑洞解除操作前查看平台自动解封时间，如果您可以接受该自动解封时间，请您耐心等待。

通过类似的方法，您还可以实现当DDoS攻击事件发生时自动调用云解析的API接口将相关域名的DNS解析切换至DDoS高防实例等。

操作步骤

1. 登录云监控控制台，定位到事件监控 > 报警规则页面。

2. 单击创建事件报警，为DDoS防护包创建黑洞事件报警。

3. 在所创建的事件报警中，根据您想要使用的消息消费机制，选择事件报警消息的推送渠道，单击确定。

   云监控支持多种渠道供您实现事件消息的消费：

   - 消息服务队列
   - 函数计算
   - URL回调
   - 日志服务

事件报警创建完成后，当DDoS防护包实例中已防护的IP被黑洞时，云监控将自动报警并将以下消息实时推送至您所选择的消费渠道。

消息示例

```
{
    "action": "add", //动作。其中，add表示事件开始；del表示事件结束。
    "bps": 0, //触发事件的流量bps，单位：Mbps。
```

```
    "pps": 0, //触发事件的包速率，单位：pps。
    "instanceId": "ddosbgp-cn-78v17******", //DDoS防护包实例ID。
    "ip": "47.*.*.*", //发生事件的IP。
    "regionId": "cn-hangzhou", //DDoS防护包实例所在的地域。
    "time": 1564104493000, //触发事件的时间，时间格式为毫秒时间戳。
    "type": "blackhole"  //事件类型。其中，defense表示清洗事件；blackhole
表示黑洞事件。
}
```

4. 定义消息消费机制，对事件消息进行处理并结合*#unique_24* API接口实现黑洞自动解除。

5.2 DDoS原生防护（防护包）+高防组合使用方案

通过组合使用DDoS原生防护和DDoS高防，您可以在尽量保证正常业务流畅体验的前提下，为其部署强力的DDoS防护。组合使用方案通过DDoS高防流量调度器的防护调度规则实现。本文介绍了组合使用方案的配置方法。

背景信息

DDoS原生防护（企业版）是一款针对阿里云ECS、SLB、EIP、Web应用防火墙等云产品直接提升DDoS攻击防御能力的安全产品。DDoS原生防护的主要好处是可以直接把防御能力加载到云产品上，不需要更换IP，也没有四层端口、七层域名数等限制。DDoS原生防护部署简单，即刻购买，即刻生效，同时具备弹性防护能力，遭受大规模攻击时调用当前地域阿里云最大DDoS防护能力提供全力防护。

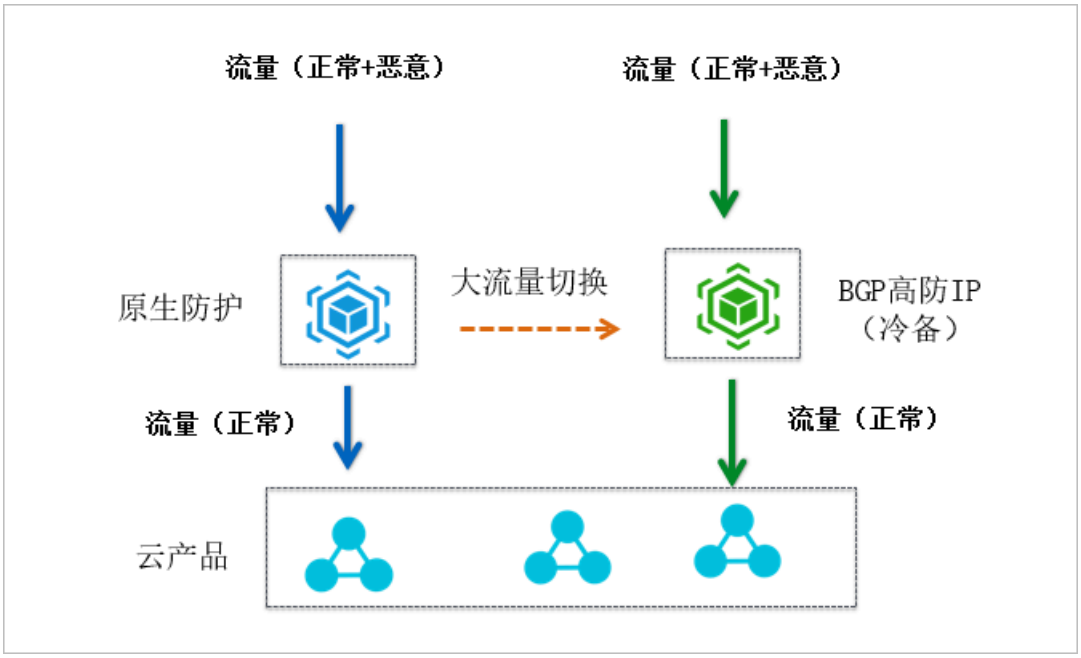
DDoS高防（新BGP）服务采用中国大陆地域独有的T级八线BGP带宽资源，防护带宽最大达到1.5T，可防御超大流量DDoS攻击。DDoS高防采用DNS解析牵引的模式接入，拥有中国大陆地域最优质的BGP带宽资源，BGP线路覆盖电信、联通、移动、教育等运营商线路，平均访问时延仅20ms左右。

DDoS高防流量调度器允许您设置DDoS高防与DDoS原生防护之间的联动规则，实现日常使用原生防护防御DDoS攻击，仅在被大流量攻击的时候，切换到DDoS高防进行防御。

方案概述

DDoS原生防护和DDoS高防的组合方案允许您同时享受到DDoS原生防护和DDoS高防的优势，例如DDoS原生防护的费用可控、全资产防护、透明部署无延迟，和DDoS高防的超大攻击流量防护。

在DDoS原生防护和DDoS高防的组合方案中，您可以开通DDoS原生防护企业版，保护单地域100个IP，应用尽力防护模式（防御防护能力一般不低于100~300Gbps，具体防护能力和所在区域有关）；在DDoS原生防护的基础上，增加一组DDoS高防，冷备防御200G以上的大流量攻击。配置防护调度规则后，将业务接入高防流量调度器，在原生防护触发黑洞时自动切换DDoS高防IP。组合使用方案中，业务带宽收费计入原生防护，高防只收取保底带宽费。



DDoS原生防护和DDoS高防的组合方案具备以下特性：

- **原生防护企业版提供多区域、账号级DDoS防护，无需更改IP，无需改变业务架构，无延迟增加。**
- **原生防护提供200Gbps防护能力，更大流量自动切换到Tbps级别的高防防御。**
- **黑洞触发自动切换，通过DNS调度完成切换，最短1-3分钟切换完成，最长5-10分钟全国切换完成。**
- **专线回源，不受云产品黑洞影响。**

方案对比

方案	防护配置	业务延时	防护效果
DDoS原生防护	保底20Gbps，弹性尽力防护（200Gbps）	正常无业务延时	攻击带宽20~200Gbps间抵扣抗D流量，200Gbps以上黑洞
DDoS高防	保底30Gbps，弹性300Gbps	存在业务延时（约20ms）	攻击带宽30~300Gbps间弹性后付费，300Gbps以上黑洞

方案	防护配置	业务延时	防护效果
DDoS原生防护+DDoS高防	保底20Gbps，弹性300Gbps	正常无业务延时，被攻击时延时约20ms	攻击带宽20~200Gbps间抵扣抗D流量，200~300Gbps间弹性后付费，300Gbps以上黑洞

部署组合方案后，业务默认解析在SLB/ECS/WAF，开启原生防护企业版，此时不增加延迟；攻击过大，流量包触发黑洞时，高防调度器调度到DDoS高防IP，使用高防IP防护大流量的攻击；攻击停止，流量回切到SLB/ECS/WAF，使用原生防护防护。

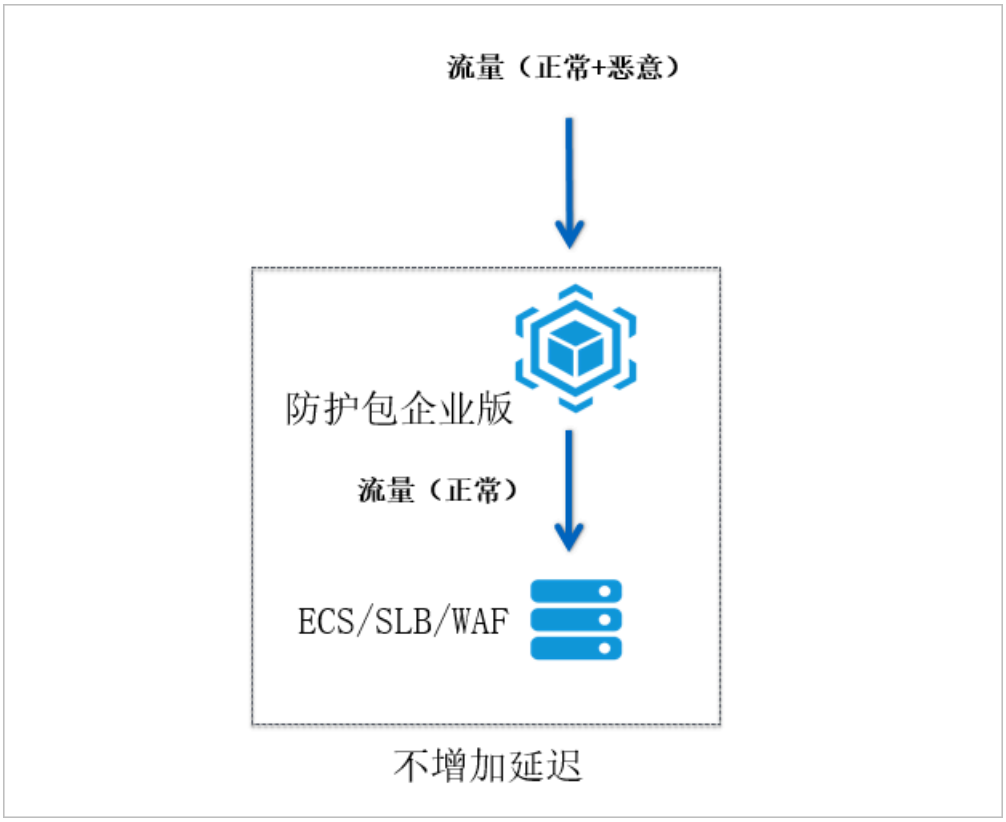
- 触发切换后，受国内ldns影响，最多5~10分钟可以完成全国切换。
- 切换到DDoS高防时，黑洞阈值受高防的最大防护能力限制。开通实例时可以配置30Gbps保底+300Gbps弹性，但您可以通过工单联系我们升级到1T甚至更高。
- 切换到高防之后，即使攻击停止也不会马上回切。流量调度器支持设置切换延迟时间，默认是120分钟（2小时），目的是防止回切后被持续攻击触发频繁切换，出现震荡，导致业务始终在切换状态。

开通和配置DDoS原生防护

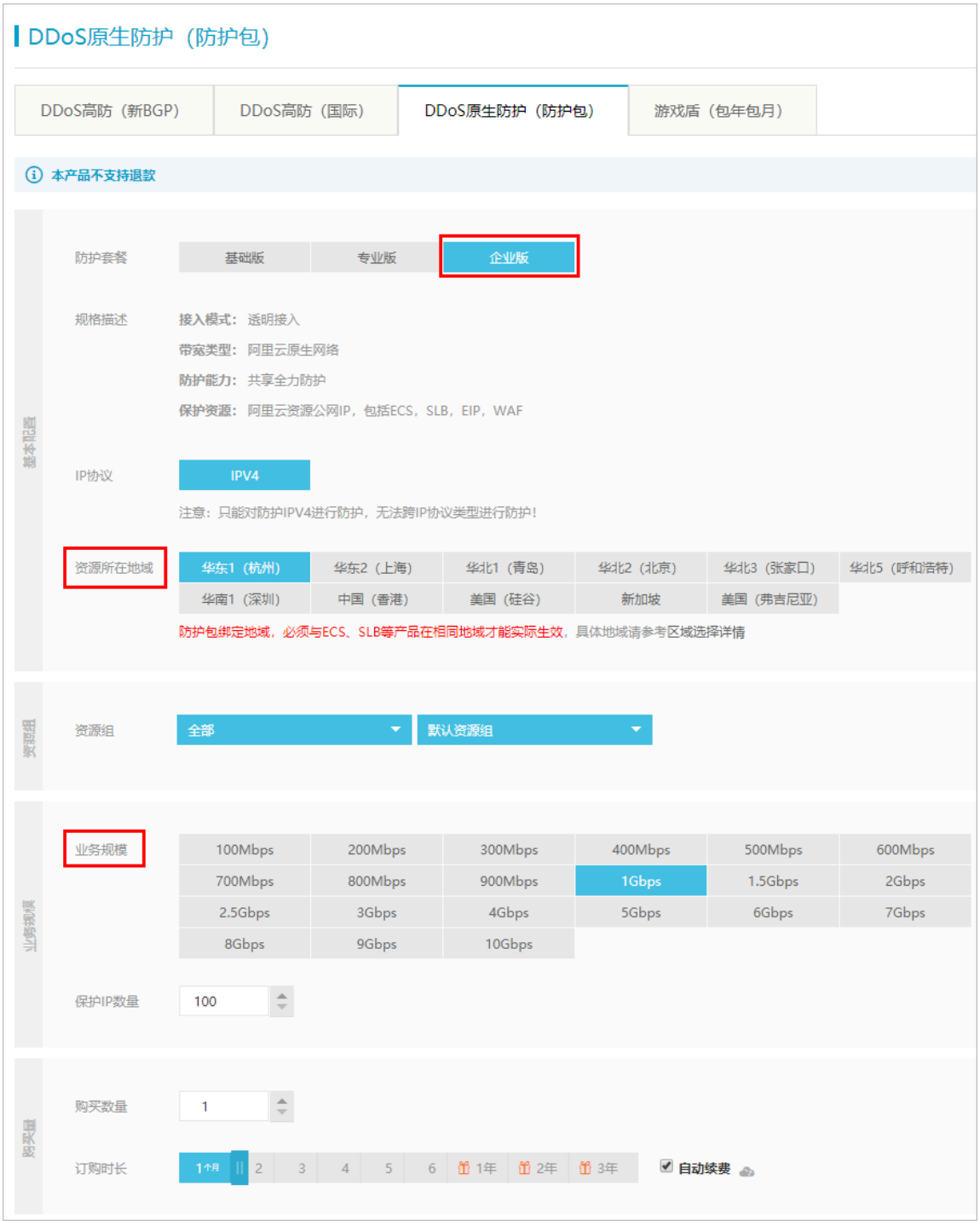
开通DDoS原生防护（防护包）企业版实例，并添加同地域阿里云资源（ECS、SLB、EIP、WAF）作为防护对象。

注意:

- 如果采用公网SLB、ECS、EIP、NAT对外服务，需要注意对应产品的网络规格满足业务正常流量需要，并在对应产品控制台查看清洗限流阈值能否满足业务需求。
- 大促前，需要提前报备，协商正常流量峰值，防止误触发清洗或限流保护，对业务产生影响。


流量（正常+恶意）
防护包企业版
流量（正常）
ECS/SLB/WAF
不增加延迟

1. 开通DDoS原生防护企业版。若已开通，请跳过此步骤。
   a) 登录云盾DDoS基础防护控制台。
   b) 在防护包 > 实例页面，单击新购防护包。
   c) 在DDoS原生防护（防护包）购买页面，完成防护包实例配置，并单击立即购买。防护包的配置描述如下。
      - 防护套餐：企业版
      - 资源所在地域：要防护的阿里云资源的地域
      - 业务规模：要防护的业务的正常网络带宽



说明：

更多信息，请参见*购买DDoS防护包*。

d) 确认订单并完成支付。

成功开通DDoS原生防护企业版实例。

2. 为DDoS原生防护添加防护对象。

a) 登录云盾DDoS基础防护控制台。

b) 在防护包 > 实例页面，定位到企业版防护包，单击其操作列下的添加防护对象。

c) 在添加防护对象对话框中，输入要防护的业务的源站IP地址，并单击确定。

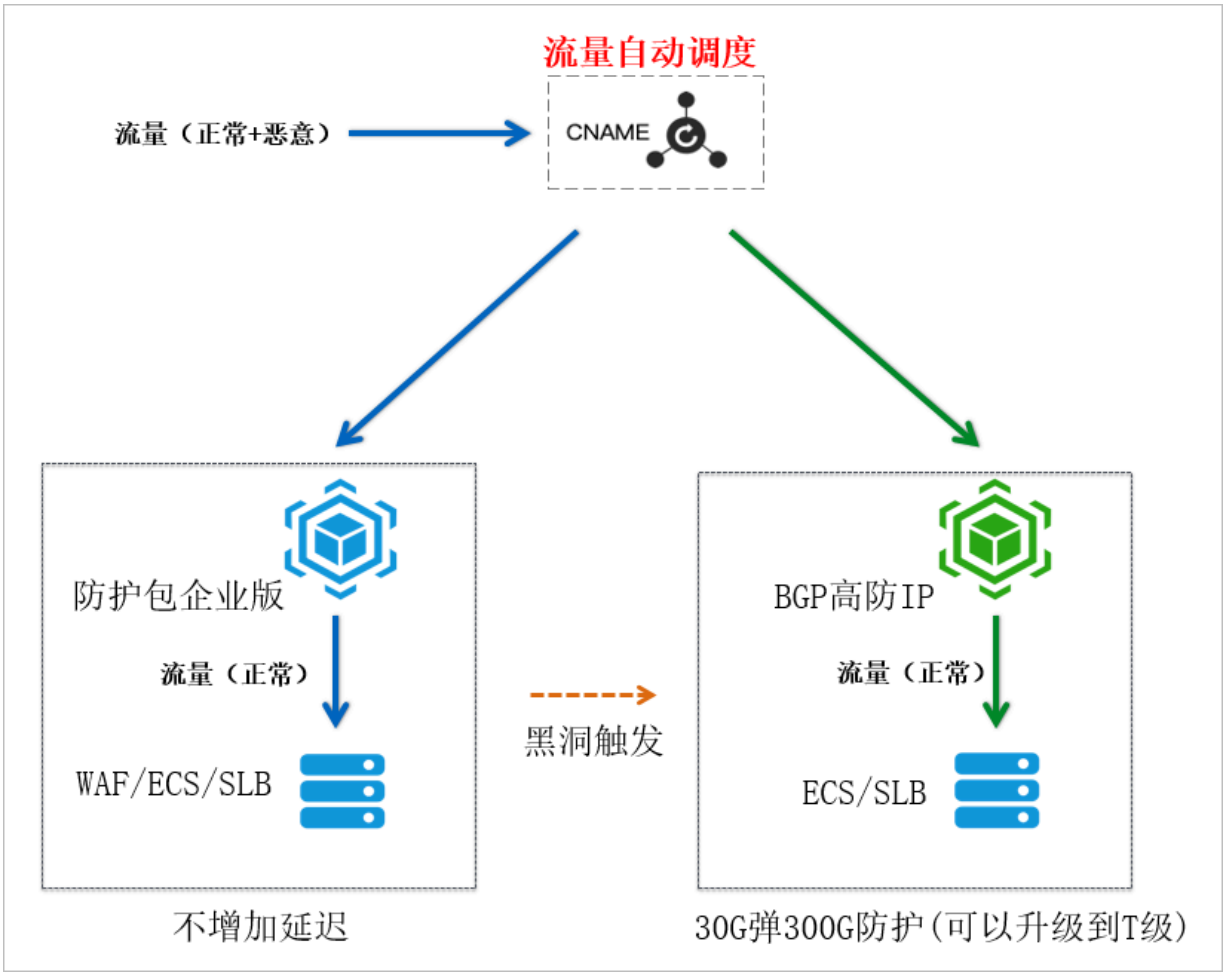
说明:

更多信息，请参见添加防护对象IP。

成功添加防护对象。

配置DDoS高防和流量调度器

开通DDoS高防（新BGP）专业版，添加业务转发规则，并通过流量调度器配置防护调度规则。完成规则配置后，将业务解析到流量调度器的Cname地址。


流量自动调度
流量（正常+恶意）
CNAME
防护包企业版
流量（正常）
WAF/ECS/SLB
黑洞触发
BGP高防IP
流量（正常）
ECS/SLB
不增加延迟
30G弹300G防护(可以升级到T级)

1. 开通DDoS高防专业版。若已开通，请跳过此步骤。

   a) 登录*DDoS*高防（新*BGP*）控制台。

   b) 在管理 > 实例列表页面，单击新购实例。

   c) 在DDoS高防（新BGP）购买页面，完成高防实例的配置，并单击立即购买。高防实例的配置描述如下。

      - 防护套餐：专业版
      - 保底防护带宽：30Gb
      - 弹性防护带宽：300Gb
      - 业务带宽：要防护的业务的正常网络带宽


DDoS高防（新BGP）
新BGP高防IP
DDoS高防（国际）
游戏盾（包年包月）
本产品不支持退款。业务服务器在中国大陆，推荐购买新BGP高防，使用新BGP高防，域名必须经过ICP备案，未备案域名将无法正常访问。业务服务器在海外，推
基本配置
防护套餐
专业版
基础规格
接入模式： DNS解析牵引
资源预留： 1个独享 IP
带宽类型： 多线BGP
防护能力： 保底防护（预付费）+ 弹性防护（按量后付费）
保底防护带宽
30Gb
60Gb
100Gb
300Gb
400Gb
500Gb
600Gb
此部分为保底带宽，预付费。计费详情
弹性防护带宽
30Gb
40Gb
50Gb
60Gb
70Gb
80Gb
100Gb
150Gb
200Gb
300Gb
弹性防护带宽为最高防护带宽，如果弹性防护带宽值跟保底防护带宽值设置一样，则不会产生后付费且最高防护带宽为保底防护带宽值，如果弹性带宽值设置高于保底带宽值，则超过保底带宽值但不大于弹性带宽值的攻击仍然可以进行有效防护，但会根据超出保底带宽的部分产生后付费。请参考产品价格详情
业务带宽
2500M
5000M
1000 M
当您购买的套餐规格里的业务带宽不够用时，可能会丢包或者影响业务，在这种情况下请及时升级业务带宽。
资源组
资源组
全部
默认资源组
高级配置
功能套餐
标准功能
增强功能
防护域名数
50
防护域名数是本实例可添加的HTTP/HTTPS域名数量，每10个域名配置限制支持1个一级域名（站点）
举例：3个域名 www.abc.com; *.abc.com; www.xyz.com，对应2个站点 abc.com和xyz.com
单实例最多可选购200个域名（20个站点）申请接入更多域名 >>
业务QPS
3000
业务QPS是无攻击状态下本实例最大可容纳HTTP/S的并发请求速率。如果正常业务QPS需要更高，请通过工单联系客服进行定制
防护端口数
50
购买量
购买数量
1
购买时长
1个月
2个月
3个月
4个月
5个月
6个月
1年
2年
自动续费

说明:

更多信息，请参见*#unique_28*。

d) 确认订单并完成支付。

成功开通DDoS高防（新BGP）专业版。

2. 为业务添加网站配置。

a) 登录*DDoS*高防（新*BGP*）控制台。

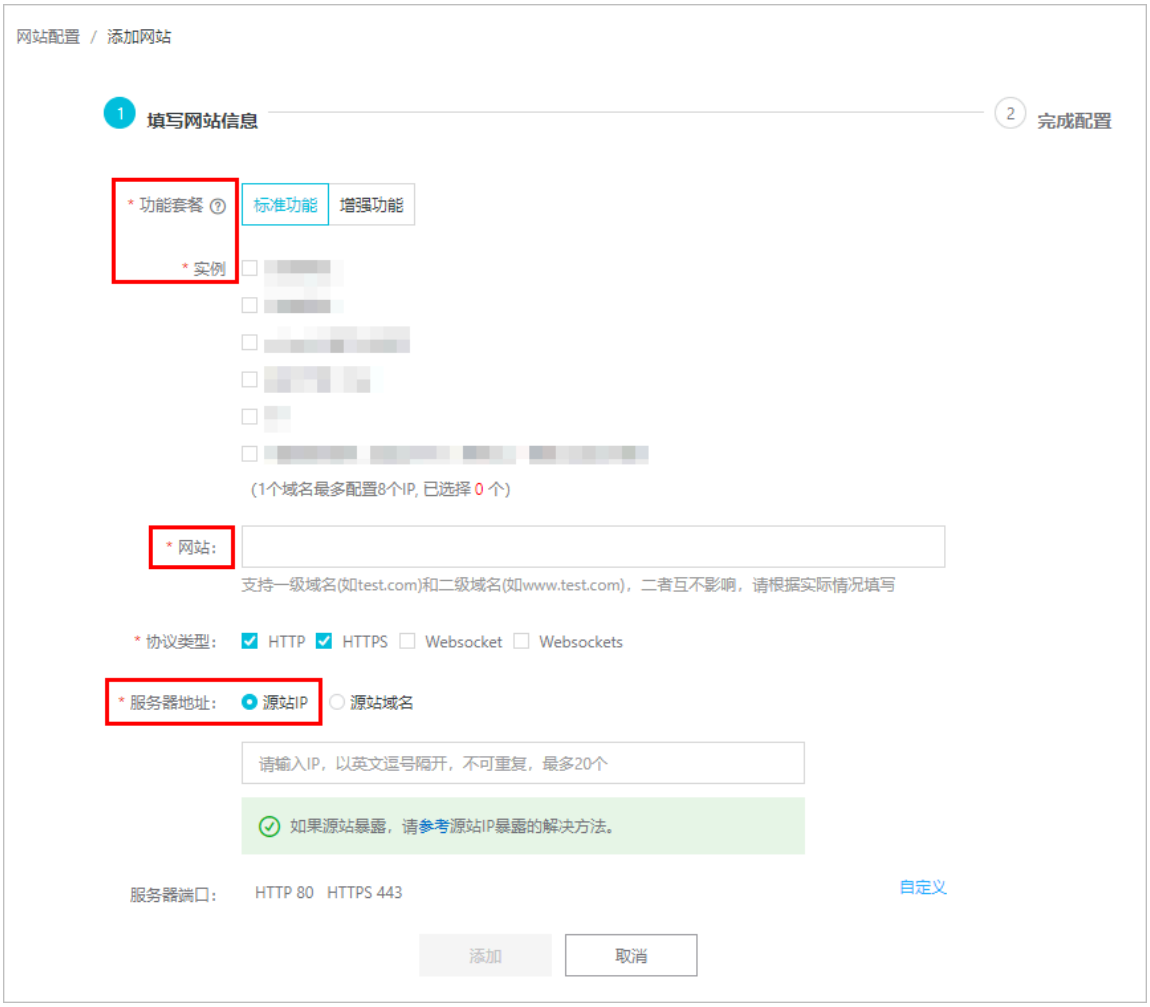
b) 在管理 > 网站配置页面，单击添加网站。

c) 在填写网站信息任务中，完成要防护的业务的转发配置，并单击添加。转发配置的描述如下。

- 功能套餐和实例：要使用的高防实例
- 网站：填写网站域名
- 服务器地址：选择并填写源站IP

说明:

更多信息，请参见添加网站配置。



成功添加网站业务转发配置。

说明:

添加网站配置后，无需按照页面提示修改DNS解析。

3. 使用流量调度器，为业务添加防护调度规则。

a) 登录*DDoS*高防（新*BGP*）控制台。

b) 前往管理 > 流量调度器页面，在防护调度页签下，单击添加规则。

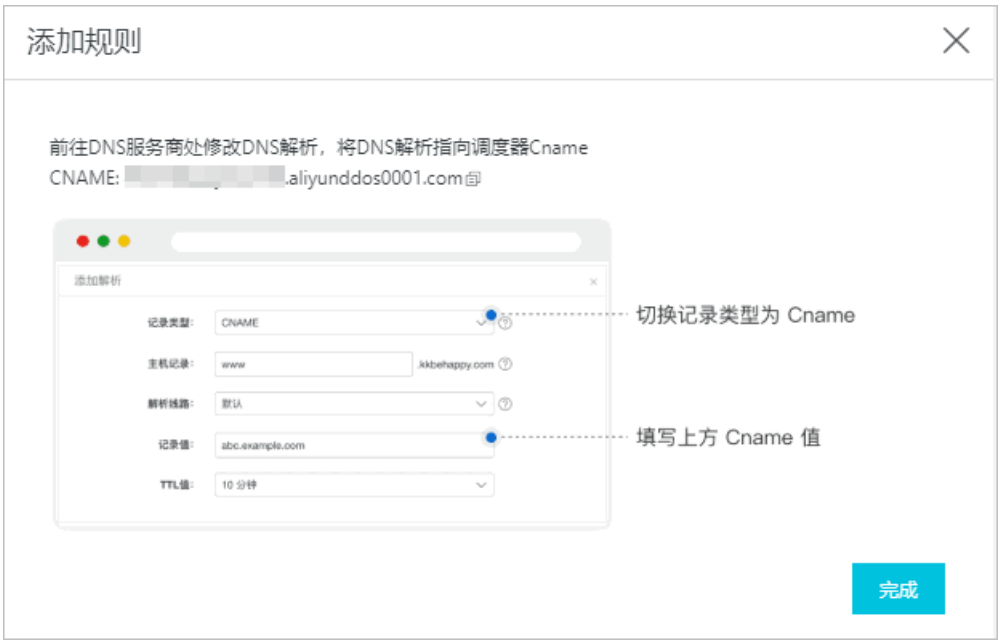
c) 在添加规则侧边页，完成阶梯防护规则的配置，并单击下一步。阶梯防护规则的配置描述如下。

- 联动场景：阶梯防护
- 高防IP：选择在网站配置中使用的高防实例
- 云资源：选择业务的源站IP

说明：

更多信息，请参见*#unique_30*。

成功添加调度规则，获得调度器Cname地址。



4. **更新业务域名解析，使能DDoS高防流量调度规则。前往域名DNS服务商处修改DNS解析，应用CNAME解析，并将解析指向流量调度器Cname地址。**

6 API参考

6.1 API概览

本文汇总了DDoS防护包服务的所有可调用API，具体接口信息请参见相关文档。

> **注意:**
> **DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。**

防护设置相关接口

接口	描述
#unique_33	为DDoS防护包添加防护对象IP。
#unique_34	将被防护IP从防护包中移除，取消防护。
#unique_24	为被防护IP解除黑洞状态。

防护包实例相关接口

接口	描述
#unique_35	查看DDoS防护包服务支持的地域信息。
#unique_36	查询防护包实例的详细信息。
#unique_37	查询防护包实例的规格信息。
#unique_38	查询异常防护包实例的信息。
#unique_39	查询防护包实例的防护IP列表信息。
#unique_40	修改DDoS防护包的备注。
#unique_41	检查防护包服务的授权状态，即是否授权防护包查询您的ECS服务器信息。

抗D流量包相关接口

接口	描述
#unique_42	查询抗D流量包的详细信息。
#unique_43	查询抗D流量包的统计信息。
#unique_44	查询抗D流量包的使用明细。
#unique_45	查询付费流量明细。

图表日志相关接口

接口	描述
#unique_46	查询指定防护包上的DDoS事件。
#unique_47	查询用户的操作日志。
#unique_48	查询指定防护包上的流量信息。

6.2 调用方式

DDoS防护包接口调用是向DDoS防护包的API的服务端地址发送HTTP GET请求，并按照接口说明在请求中加入相应请求参数，调用后系统会返回处理结果。请求及返回结果都使用UTF-8字符集进行编码。

请求结构

DDoS防护包的API是RPC风格，您可以通过发送HTTP GET请求调用DDoS防护包 API。

其请求结构如下：

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

其中：

- `Endpoint`：**DDoS防护包 API的服务接入地址为：**
  - `ddosbgp.aliyuncs.com`

    支持以下地域：

    - **cn-hangzhou**
    - **cn-shanghai**
    - **cn-qingdao**
    - **cn-beijing**
    - **cn-zhangjiakou**
    - **cn-huhehaote**
    - **cn-shenzhen**
  - `ddosbgp.cn-hongkong.aliyuncs.com`：**支持cn-hongkong地域**
  - `ddosbgp.us-west-1.aliyuncs.com`：**支持us-west-1地域**
- `Action`：**要执行的操作，如使用**`DescribeInstanceList`**，查询DDoS防护包的实例信息。**
- `Version`：**要使用的API版本，DDoS防护包的API版本是**`2018-07-20`。

- Parameters：请求参数，多个参数之间用“&”连接。

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

下面是一个调用DescribeInstanceList接口查询DDoS防护包实例信息的示例：

说明：

为了便于您查看，本文档中的示例都做了格式化处理。

```
https://ddosbgp.aliyuncs.com/?Action=DescribeInstanceList
&DdosRegionId=cn-hangzhou
&InstanceId=ddosbgp-cn-xxx
&Format=xml
&Version=2018-07-20
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2012-06-01T12:00:00Z
```

API授权

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

API签名

DDoS防护包服务会对每个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。

RPC API需按如下格式在请求中增加签名（Signature）：

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

6.3 公共参数

公共请求参数是每个接口都需要使用到的请求参数。

公共请求参数

名称	类型	是否必需	描述
DdosRegionId	String	是	DDoS防护包实例所在的地域。取值： · cn-hangzhou · cn-shanghai · cn-qingdao · cn-beijing · cn-zhangjiakou · cn-huhehaote · cn-shenzhen · cn-hongkong · us-west-1
Format	String	否	返回消息的格式。取值： · JSON（默认） · XML
Version	String	是	API版本号，使用YYYY-MM-DD日期格式。取值：2018-07-20。
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，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。

名称	类型	是否必需	描述
SignatureVersion	String	是	签名算法版本，取值：1。
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://ddosbgp.aliyuncs.com/?Action=DescribeInstanceList
&DdosRegionId=cn-hangzhou
&InstanceId=ddosbgp-cn-xxx
&Format=xml
&Version=2018-07-20
&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XML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*/
```

```
    }
```

6.4 防护

6.4.1 AddIp

调用AddIp接口为DDoS防护包添加防护对象IP。

说明:

DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

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	AddIp	系统规定参数。取值：AddIp。
InstanceId	String	是	ddosbgp-cn-12345678	要操作的防护包实例ID。
IpList	String	是	[{"ip":"1.1.1.1"},{"ip":"2.2.2.2"}]	添加到防护包进行防护的IP，支持添加过个IP。
ResourceGroupId	String	否	test	资源组ID。
ResourceRegionId	String	否	cn-hangzhou	地域ID。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	请求ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=AddIp
&InstanceId=ddosbgp-cn-12345678
&IpList=[{"ip":"1.1.1.1"},{"ip":"2.2.2.2"}]
&<公共请求参数>
```

正常返回示例

`XML` **格式**

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

`JSON` **格式**

```
{
 "RequestId":"4C467B38-3910-447D-87BC-AC049166F216"
}
```

错误码

访问错误中心查看更多错误码。

6.4.2 DeleteIp

调用DeleteIp接口将被防护IP从防护包中移除，取消防护。

说明:

DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

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	DeleteIp	要执行的操作，取值：DeleteIp。
InstanceId	String	是	ddosbgp-cn-xxx	要操作的防护包ID。
IpList	String	是	[{"ip":"1.1.1.1"},{"ip":"2.2.2.2"}]	要从防护包中移除的被防护IP，支持填写多个IP。
ResourceGroupId	String	否	xx	资源组ID。

名称	类型	是否必选	示例值	描述
ResourceRegionId	String	否	cn-hangzhou	地域ID。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteIp
&InstanceId=ddosbgp-cn-xxx
&IpList=1.1.1.1,2.2.2.2
&<公共请求参数>
```

正常返回示例

`XML` **格式**

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

`JSON` **格式**

```
{
 "RequestId":"4C467B38-3910-447D-87BC-AC049166F216"
}
```

错误码

访问错误中心查看更多错误码。

6.4.3 DeleteBlackhole

调用DeleteBlackhole接口为被防护IP解除黑洞状态。

说明:

DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

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	DeleteBlackhole	系统规定参数。取值：DeleteBlackhole。
InstanceId	String	是	ddosbgp-cn-xxx	要操作的防护包实例ID。
Ip	String	是	1.1.1.1	要解除黑洞状态的被防护IP。
ResourceGroupId	String	否	xx	资源组ID。
ResourceRegionId	String	否	cn-hangzhou	地域ID。

返回数据

名称	类型	示例值	描述
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteBlackhole
&InstanceId=ddosbgp-cn-xxx
&Ip=1.1.1.1
&<公共请求参数>
```

正常返回示例

XML 格式

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

```
</DeleteBlackholeResponse>
```

JSON 格式

```
{
 "RequestId":"4C467B38-3910-447D-87BC-AC049166F216"
}
```

错误码

访问错误中心查看更多错误码。

6.5 实例

6.5.1 DescribeRegions

调用DescribeRegions接口查看支持DDoS防护包服务的地域信息。

说明:
DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

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	DescribeRegions	要执行的操作，取值：DescribeRegions。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
Code	String	true	响应状态码。
Regions	Array		防护包支持的地域信息。
RegionEnName	String	shanghai	地域英文名称。

名称	类型	示例值	描述
RegionId	String	cn-shanghai	地域ID。
RegionName	String	上海	地域中文名称。
RequestId	String	C3D66E07-41BF-41B7-A4BF-83A9E08E1C09	本次请求的ID。
Success	Boolean	true	是否成功调用请求。

示例

请求示例

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

正常返回示例

`XML` **格式**

```
<DescribeRegionsResponse>
      <RequestId>C3D66E07-41BF-41B7-A4BF-83A9E08E1C09</RequestId>
      <Regions>
            <Region>
                  <RegionId>cn-shenzhen</RegionId>
            </Region>
            <Region>
                  <RegionId>cn-qingdao</RegionId>
            </Region>
            <Region>
                  <RegionId>cn-beijing</RegionId>
            </Region>
            <Region>
                  <RegionId>cn-shanghai</RegionId>
            </Region>
            <Region>
                  <RegionId>cn-hongkong</RegionId>
            </Region>
            <Region>
                  <RegionId>cn-huhehaote</RegionId>
            </Region>
            <Region>
                  <RegionId>cn-zhangjiakou</RegionId>
            </Region>
            <Region>
                  <RegionId>us-west-1</RegionId>
            </Region>
            <Region>
                  <RegionId>cn-hangzhou</RegionId>
            </Region>
      </Regions>
      <Success>true</Success>
```

```
    <Code>200</Code>
</DescribeRegionsResponse>
```

JSON 格式

```
{
 "RequestId":"9C48E43E-58A6-4A08-A858-4C9BB9631870",
 "Regions":[
  {
   "RegionId":"cn-shenzhen"
  },
  {
   "RegionId":"cn-qingdao"
  },
  {
   "RegionId":"cn-beijing"
  },
  {
   "RegionId":"cn-shanghai"
  },
  {
   "RegionId":"cn-hongkong"
  },
  {
   "RegionId":"cn-huhehaote"
  },
  {
   "RegionId":"cn-zhangjiakou"
  },
  {
   "RegionId":"us-west-1"
  },
  {
   "RegionId":"cn-hangzhou"
  }
 ],
 "Success":true,
 "Code":"200"
}
```

错误码

访问错误中心查看更多错误码。

6.5.2 DescribeInstanceList

调用DescribeInstanceList接口查询防护包实例的详细信息。

说明:

DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

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	DescribeInstanceList	要执行的操作，取值：DescribeInstanceList。
PageNo	Integer	是	1	列表的页码，默认值为1。
PageSize	Integer	是	10	分页查询时每页的行数，最大值为50，默认值为10。
DdosRegionId	String	否	cn-hangzhou	实例所在地区ID。
InstanceIdList	String	否	['ddosbgp-cn-xx','ddosbpg-cn-xxx']	指定要查询的防护包实例ID，多个ID间用逗号分隔。以JSON数组串格式传入，例如，\'ddosbgp-cn-xx','ddosbpg-cn-xxx'。  说明: 若不传入该参数，则返回所有防护包信息。
InstanceType	String	否	0	指定要查询的防护包实例的类型，取值：  说明: 若不传入该参数，则返回所有防护包信息。 · 0：专业版 · 1：企业版
Ip	String	否	1.1.1.1	指定要查询的防护包实例的防护对象IP。  说明: 若不传入该参数，则返回所有防护包信息。

名称	类型	是否必选	示例值	描述
IpVersion	String	否	IPv4	指定要查询的防护包实例的防护IP类型，取值： 说明: 若不传入该参数，则返回所有防护包信息。 · IPv4 · IPv6
Orderby	String	否	expireTime	排序字段，取值：expireTime（到期时间）。
Orderdire	String	否	asc	排序方向，取值： · desc：倒序 · asc：顺序
Remark	String	否	test	指定要查询的防护包实例的备注。 说明: 若不传入该参数，则返回所有防护包信息。
ResourceGroupId	String	否	test	资源组ID。
Tag.N.Key	String	否	test	标签的Key值。若有多个标签，依次传入Tag.1.Key、Tag.2.Key、Tag.3.Key ...
Tag.N.Value	String	否	test	标签的Value值。若有多个标签，依次传入Tag.1.Value、Tag.2.Value、Tag.3.Value ...

返回数据

名称	类型	示例值	描述
InstanceList			防护包实例的详细信息。

名称	类型	示例值	描述
AutoRenewal	Boolean	false	是否开启自动续费。
BlackholdingCount	String	0	防护包中正在黑洞中的IP数量。
ExpireTime	Long	1560009600000	防护包的到期时间。
GmtCreate	Long	1554708159000	防护包的创建时间。
InstanceId	String	ddosbgp-cn-xx	防护包实例ID。
IpType	String	IPv4	防护包的防护IP类型。
Remark	String	test	防护包的备注。
Status	String	1	实例状态，取值： · 1：正常 · 2：过期 · 3：释放
RequestId	String	C3F7E6AE-43B2-4730-B6A3-FD17552B8F65	本次请求的ID。
Total	Long	1	返回结果的总数。

示例

请求示例

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

正常返回示例

`XML` **格式**

```
<DescribeInstanceListResponse>
     <RequestId>5DE4D6B1-8D6D-4AC3-84AF-5EE0A4C2778E</RequestId>
     <InstanceList>
           <Instance>
                 <Status>1</Status>
                 <AutoRenewal>true</AutoRenewal>
```

```
                <IpType>IPv4</IpType>
                <ExpireTime>1560009600000</ExpireTime>
                <InstanceId>ddosbgp-cn-xx</InstanceId>
                <GmtCreate>1554708159000</GmtCreate>
                <Remark>test</Remark>
                <BlackholdingCount>0</BlackholdingCount>
            </Instance>
        </InstanceList>
        <Total>1</Total>
</DescribeInstanceListResponse>
```

JSON 格式

```
{
 "RequestId":"C3F7E6AE-43B2-4730-B6A3-FD17552B8F65",
 "Total":1,
 "InstanceList":[
  {
   "Status":"1",
   "AutoRenewal":true,
   "IpType":"IPv4",
   "ExpireTime":1560009600000,
   "InstanceId":"ddosbgp-cn-xx",
   "Remark":"test",
   "GmtCreate":1554708159000,
   "BlackholdingCount":0
  }
 ]
}
```

错误码

访问错误中心查看更多错误码。

6.5.3 DescribeInstanceSpecs

调用DescribeInstanceSpecs接口查询防护包的规格信息。

说明:

DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

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	DescribeInstanceSpecs	要执行的操作，取值：DescribeInstanceSpecs。

名称	类型	是否必选	示例值	描述
InstanceIdList	String	是	["ddosbgp-cn-x1","ddosbgp-cn-x2"]	要查询的防护包实例ID，多个ID间以逗号分隔。以JSON字符串格式传入，例如，\"ddosbgp-cn-x1","ddosbgp-cn-x2"。
DdosRegionId	String	否	cn-hangzhou	实例所在地区ID。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
InstanceSpecs			防护包实例的规格信息。
AvailableDeleteBlackholeCount	String	100	可用的解除黑洞次数。
InstanceId	String	ddosbgp-cn-x1	防护包实例ID。
PackConfig			防护包实例的配置信息。
BindIpCount	Integer	0	已添加的防护IP数量。
IpAdvanceThre	Integer	101	被防护IP的弹性防护阈值，单位为Gb。
IpBasicThre	Integer	20	被防护IP的基础防护阈值，单位为Gb。
IpSpec	Integer	100	可添加IP的数量。
PackAdvThre	Integer	100	防护包的弹性防护带宽，单位为Gb。
PackBasicThre	Integer	20	防护包的基础防护带宽，单位为Gb。
Region	String	cn-hangzhou	防护包实例的区域。

名称	类型	示例值	描述
RequestId	String	CEB7F4F5-1DA8-41ED-A9C4-E0F0033E9E1F	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeInstanceSpecs
&InstanceIdList=["ddosbgp-cn-x1","ddosbgp-cn-x2"]
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeInstanceSpecsResponse>
     <InstanceSpecs>
           <InstanceSpec>
                 <Region>cn-hangzhou</Region>
                 <InstanceId>ddosbgp-cn-x1</InstanceId>
                 <AvailableDeleteBlackholeCount>100</AvailableD
eleteBlackholeCount>
                 <PackConfig>
                       <IpBasicThre>20</IpBasicThre>
                       <BindIpCount>0</BindIpCount>
                       <PackBasicThre>20</PackBasicThre>
                       <IpAdvanceThre>101</IpAdvanceThre>
                       <IpSpec>100</IpSpec>
                       <PackAdvThre>101</PackAdvThre>
                 </PackConfig>
           </InstanceSpec>
     </InstanceSpecs>
     <RequestId>CEB7F4F5-1DA8-41ED-A9C4-E0F0033E9E1F</RequestId>
</DescribeInstanceSpecsResponse>
```

`JSON` **格式**

```
{
 "InstanceSpecs":[
  {
   "Region":"cn-hangzhou",
   "AvailableDeleteBlackholeCount":100,
   "InstanceId":"ddosbgp-cn-x1",
   "PackConfig":{
    "IpBasicThre":20,
    "BindIpCount":0,
    "PackBasicThre":20,
    "IpAdvanceThre":100,
    "PackAdvThre":101,
    "IpSpec":100
   }
  }
 ],
 "RequestId":"D8D786F2-2008-4280-B9AB-8E6C4E8C2A16"
```

```
}
```

错误码

访问错误中心查看更多错误码。

6.5.4 DescribeExcpetionCount

调用DescribeExcpetionCount接口查询防护包异常信息。

说明:

DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

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	DescribeExcpetionCount	要执行的操作，取值：DescribeExcpetionCount。
DdosRegionId	String	是	cn-hangzhou	实例所在地区ID。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
ExceptionIpCount	Integer	0	异常IP的数量，如被防护的ECS IP、SLB IP等。
ExpireTimeCount	Integer	1	7天内即将到期的实例数量。
RequestId	String	A3EEE55F-3B9F-4765-8C03-1A1A904F3451	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeExcpetionCount
&DdosRegionId=cn-hangzhou
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeExcpetionCountResponse>
      <ExpireTimeCount>1</ExpireTimeCount>
      <RequestId>58609615-FCF9-41DF-8B25-0D5C8DAB92BA</RequestId>
      <ExceptionIpCount>0</ExceptionIpCount>
</DescribeExcpetionCountResponse>
```

`JSON` **格式**

```
{
 "RequestId":"A3EEE55F-3B9F-4765-8C03-1A1A904F3451",
 "ExpireTimeCount":1,
 "ExceptionIpCount":0
}
```

错误码

访问错误中心查看更多错误码。

6.5.5 DescribePackIpList

调用DescribePackIpList接口查询防护包的防护IP列表信息。

说明:

DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

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	DescribePackIpList	要执行的操作，取值：DescribePackIpList。

名称	类型	是否必选	示例值	描述
DdosRegionId	String	是	cn-hangzhou	实例所在地区ID。
InstanceId	String	是	ddosbgp-cn-x1	要查询的防护包实例ID。
PageNo	Integer	是	1	列表的页码，默认值为1。
PageSize	Integer	是	10	分页查询时每页的行数，最大值为50，默认值为10。
Ip	String	否	1.1.1.1	要查询的防护对象IP，设置后只返回指定IP的信息。
ProductName	String	否	ECS	要查询的防护对象IP的归属产品类型，取值： 说明: 设置后只返回指定产品的防护IP信息。 · ECS · SLB · EIP · WAF
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
Code	String	200	响应状态码。
IpList			防护IP列表。
Ip	String	1.1.1.1	被防护IP。

名称	类型	示例值	描述
Product	String	ECS	IP的归属产品，取值： · ECS · SLB · EIP · WAF
Remark	String	test	归属产品备注，比如ECS实例的备注。
Status	String	normal	IP的状态，取值： · normal：正常 · hole_begin：黑洞中
RequestId	String	B479FE9B-F0EB-423B-81E5-ECE2167BCF40	本次请求的ID。
Success	Boolean	true	是否成功调用请求。
Total	Integer	1	返回结果的数量。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePackIpList
&DdosRegionId=cn-hangzhou
&InstanceId=ddosbgp-cn-x1
&PageNo=1
&PageSize=10
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribePackIpListResponse>
     <RequestId>8584D3B6-BB3C-441E-B1D6-E154ED25C032</RequestId>
     <IpList>
           <Ipitem>
                 <Status>normal</Status>
                 <Ip>1.1.1.1</Ip>
                 <Product>ECS</Product>
                 <Remark>test</Remark>
           </Ipitem>
     </IpList>
     <Success>true</Success>
     <Code>200</Code>
```

```
    <Total>1</Total>
</DescribePackIpListResponse>
```

JSON 格式

```
{
 "RequestId":"B479FE9B-F0EB-423B-81E5-ECE2167BCF40",
 "IpList":[
  {
   "Ip":"1.1.1.1",
   "Status":"normal",
   "Product":"ECS",
   "Remark":"test"
  }
 ],
 "Success":true,
 "Code":"200",
 "Total":1
}
```

错误码

访问错误中心查看更多错误码。

6.5.6 ModifyRemark

调用ModifyRemark接口修改DDoS防护包的备注。

说明:

DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

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	ModifyRemark	要执行的操作，取值：ModifyRemark。
InstanceId	String	是	ddosbgp-cn-xxx	要操作的防护包实例ID。
Remark	String	是	test	要添加的备注内容。
ResourceGroupId	String	否	test	资源组ID。

名称	类型	是否必选	示例值	描述
ResourceRegionId	String	否	cn-hangzhou	资源组地区ID。

返回数据

名称	类型	示例值	描述
RequestId	String	4C467B38-3910-447D-87BC-AC049166F216	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ModifyRemark
&InstanceId=ddosbgp-cn-xxx
&Remark=test
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<ModifyRemarkResponse>
      <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
</ModifyRemarkResponse>
```

`JSON` **格式**

```
{
 "RequestId":"4C467B38-3910-447D-87BC-AC049166F216"
}
```

错误码

访问错误中心查看更多错误码。

6.5.7 CheckGrant

调用CheckGrant接口检查防护包服务的授权状态，即是否授权防护包查询您的ECS服务器信息。

说明:

DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

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	CheckGrant	要执行的操作，取值：CheckGrant。
ResourceGroupId	String	否	xx	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	E76E316C-697F-42D8-883A-D99864D2E77F	本次请求的ID。
Status	Integer	1	授权状态，取值： · 1：已授权DDoS防护包查询您的ECS服务器信息 · 0：未授权DDoS防护包查询您的ECS服务器信息

示例

请求示例

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

正常返回示例

XML 格式

```
<CheckGrantResponse>
      <RequestId>E76E316C-697F-42D8-883A-D99864D2E77F</RequestId>
      <Status>1</Status>
```

```
</CheckGrantResponse>
```

JSON 格式

```
{
 "Status":1,
 "RequestId":"E76E316C-697F-42D8-883A-D99864D2E77F"
}
```

错误码

访问错误中心查看更多错误码。

6.6 流量包

6.6.1 DescribeResourcePackInstances

调用DescribeResourcePackInstances接口查询抗D流量包信息。

说明:

DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

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	DescribeResourcePackInstances	要执行的操作，取值：DescribeResourcePackInstances。
CurrentPage	Integer	是	1	列表的页码，默认值为1。
PageSize	Integer	是	10	分页查询时每页显示的行数，最大值为50，默认值为10。
ResourceGroupId	String	否	xx	资源组ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
RequestId	String	40B322C3-464E-477F-B137-46E64349F0E9	本次请求的ID。
ResourcePacks	Array		抗D流量包信息。
CurrCapacity	Long	0	可用防护流量，单位为Byte。
EndTime	Long	1649433600000	失效时间。
InitCapacity	Long	100000000000000	初始防护流量，单位为Byte。
ResourcePackId	String	DDOSFLOWBAG-cn-o4012thfl000b5	抗D流量包ID。
StartTime	Long	1554708226000	生效时间。
Status	String	valid	流量包的状态，取值： · closed：失效 · valid：有效
TotalCount	Integer	1	返回结果的总数。

示例

请求示例

```
https://ddosbgp.aliyuncs.com/?Action=DescribeResourcePackInstances
&CurrentPage=1
&PageSize=10
&公共请求参数
```

正常返回示例

`XML` **格式**

```
<DescribeResourcePackInstancesResponse>
     <TotalCount>1</TotalCount>
     <ResourcePacks>
           <ResourcePack>
                 <Status>valid</Status>
                 <ResourcePackId>DDOSFLOWBAG-cn-xx</ResourcePackId>
```

```
                <InitCapacity>100000000000000</InitCapacity>
                <EndTime>1649433600000</EndTime>
                <StartTime>1554708226000</StartTime>
                <CurrCapacity>0</CurrCapacity>
            </ResourcePack>
        </ResourcePacks>
        <RequestId>40B322C3-464E-477F-B137-46E64349F0E9</RequestId>
</DescribeResourcePackInstancesResponse>
```

JSON 格式

```
{
 "TotalCount":1,
 "ResourcePacks":[
  {
   "Status":"valid",
   "ResourcePackId":"DDOSFLOWBAG-cn-o4012thfl000b5",
   "InitCapacity":100000000000000,
   "EndTime":1649433600000,
   "StartTime":1554708226000,
   "CurrCapacity":0
  }
 ],
 "RequestId":"40B322C3-464E-477F-B137-46E64349F0E9"
}
```

错误码

访问错误中心查看更多错误码。

6.6.2 DescribeResourcePackStatistics

调用DescribeResourcePackStatistics接口查询抗D流量包的统计信息。

说明:

DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

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	DescribeResourcePackStatistics	要执行的操作，取值：DescribeResourcePackStatistics。
DdosRegionId	String	否	cn-hangzhou	实例所在地区ID。

名称	类型	是否必选	示例值	描述
InstanceId	String	否	ddosbgp-cn-x1	要查询的防护包实例ID。
ResourceGroupId	String	否	xx	资源组ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
AvailablePackNum	Integer	8	可用流量包数量。
RequestId	String	A2D6D5FB-FA07-41A8-B093-A2B7B26E72F2	本次请求的ID。
TotalCurrCapacity	Long	20831250000000	总可用防护流量，单位为Byte。
TotalInitCapacity	Long	427000000000000	总初始防护流量，单位为Byte。
TotalUsedCapacity	Long	5285439000000	总消耗防护流量，单位为Byte。

示例

请求示例

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

正常返回示例

`XML` **格式**

```
<DescribeResourcePackStatisticsResponse>
     <TotalInitCapacity>427000000000000</TotalInitCapacity>
     <TotalUsedCapacity>5285439000000</TotalUsedCapacity>
     <TotalCurrCapacity>20831250000000</TotalCurrCapacity>
     <RequestId>A2D6D5FB-FA07-41A8-B093-A2B7B26E72F2</RequestId>
     <AvailablePackNum>8</AvailablePackNum>
```

```
</DescribeResourcePackStatisticsResponse>
```

JSON 格式

```
{
 "TotalInitCapacity":427000000000000,
 "TotalUsedCapacity":5285439000000,
 "RequestId":"A2D6D5FB-FA07-41A8-B093-A2B7B26E72F2",
 "TotalCurrCapacity":20831250000000,
 "AvailablePackNum":8
}
```

错误码

访问错误中心查看更多错误码。

6.6.3 DescribeResourcePackUsage

调用DescribeResourcePackUsage接口查询抗D流量包的使用明细。

说明:

DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

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	DescribeResourcePackUsage	要执行的操作，取值：DescribeResourcePackUsage。
EndTime	Long	是	1557909844	查询结束时间，秒级时间戳。所设置的查询时间区间不能超过30天。
StartTime	Long	是	1557305044	查询开始时间，秒级时间戳。所设置的查询时间区间不能超过30天。
InstanceId	String	否	ddosbgp-cn-x1	要查询的防护包实例ID。
ResourceGroupId	String	否	xx	资源组ID。

名称	类型	是否必选	示例值	描述
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
EndTime	Long	1557910800	统计结束时间，秒级时间戳。
Interval	Long	3600	统计时间间隔，单位为秒。
PackUsages	Array		已用防护流量明细。
Time	Long	1557471600	时间。
Traffic	Float	153.064	流量，单位为Gb。
RequestId	String	38F3D5EF-42BA-4533-81EB-AEAD068B5E02	本次请求的ID。
StartTime	Long	1557302400	统计起始时间，秒级时间戳。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeResourcePackUsage
&EndTime=1557909844
&StartTime=1557305044
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeResourcePackUsageResponse>
     <Interval>3600</Interval>
     <PackUsages>
           <PackUsage>
                 <Time>1557471600</Time>
                 <Traffic>153.064</Traffic>
           </PackUsage>
     </PackUsages>
     <RequestId>38F3D5EF-42BA-4533-81EB-AEAD068B5E02</RequestId>
     <EndTime>1557910800</EndTime>
```

```
    <StartTime>1557302400</StartTime>
</DescribeResourcePackUsageResponse>
```

JSON 格式

```
{
 "Interval":3600,
 "PackUsages":[
  {
   "Time":1557471600,
   "Traffic":153.064
  }
 ],
 "RequestId":"38F3D5EF-42BA-4533-81EB-AEAD068B5E02",
 "EndTime":1557910800,
 "StartTime":1557302400
}
```

错误码

访问错误中心查看更多错误码。

6.6.4 DescribePackPaidTraffic

调用DescribePackPaidTraffic接口查询付费流量明细。

说明:

DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

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	DescribePackPaidTraffic	要执行的操作，取值：DescribePackPaidTraffic。
CurrentPage	Integer	是	1	列表的页码，默认值为1。
EndTime	Long	是	1557908337870	查询结束时间，秒级时间戳。所设置的查询时间区间不能超过30天。
PageSize	Integer	是	10	分页查询时每页的行数，最大值为50，默认值为10。

名称	类型	是否必选	示例值	描述
StartTime	Long	是	1557303537870	查询开始时间，秒级时间戳。所设置的查询时间区间不能超过30天。
InstanceId	String	否	ddosbgp-cn-x1	要查询的防护包实例ID。
ResourceGroupId	String	否	xx	资源组ID。
SourceIp	String	否	1.1.1.1	请求源IP。无需填写，系统自动获取。

返回数据

名称	类型	示例值	描述
PackPaidTraffics	Array		付费流量明细。
BaseBandwidth	Integer	20	基础防护带宽，单位为Gb。
ElasticBandwidth	Integer	100	弹性防护带宽，单位为Gb。
InstanceId	String	ddosbgp-cn-x1	防护包实例ID。
MaxAttack	Float	49.998	攻击流量峰值，单位为Gbps。
PaidCapacity	Float	615.166	付费流量大小，单位为Gb。
StartTime	Long	1557809400000	统计时间。
TotalCapacity	Float	1302.666	总防护流量，单位为Gb。
RequestId	String	070363B7-BB66-43B8-9A2C-9E4B83284FC5	本次请求的ID。
TotalCount	Integer	1	返回结果的数量。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePackPaidTraffic
&CurrentPage=1
&EndTime=1557908337870
&PageSize=10
&StartTime=1557303537870
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribePackPaidTrafficResponse>
      <TotalCount>1</TotalCount>
      <RequestId>070363B7-BB66-43B8-9A2C-9E4B83284FC5</RequestId>
      <PackPaidTraffics>
            <PackPaidTraffic>
                  <PaidCapacity>615.166</PaidCapacity>
                  <MaxAttack>49.998</MaxAttack>
                  <InstanceId>ddosbgp-cn-x1</InstanceId>
                  <TotalCapacity>1302.666</TotalCapacity>
                  <ElasticBandwidth>100</ElasticBandwidth>
                  <BaseBandwidth>20</BaseBandwidth>
                  <StartTime>1557809400000</StartTime>
            </PackPaidTraffic>
      </PackPaidTraffics>
</DescribePackPaidTrafficResponse>
```

`JSON` **格式**

```
{
 "TotalCount":1,
 "RequestId":"070363B7-BB66-43B8-9A2C-9E4B83284FC5",
 "PackPaidTraffics":[
  {
   "PaidCapacity":615.166,
   "InstanceId":"ddosbgp-cn-x1",
   "MaxAttack":49.998,
   "TotalCapacity":1302.666,
   "ElasticBandwidth":100,
   "StartTime":1557809400000,
   "BaseBandwidth":20
  }
 ]
}
```

错误码

访问错误中心查看更多错误码。

6.7 图表日志

6.7.1 DescribeDdosEvent

调用DescribeDdosEvent接口查看指定防护包上的DDoS事件。

说明:

DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

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	DescribeDdosEvent	要执行的操作，取值：DescribeDdosEvent。
EndTime	Integer	是	1557909844	查询结束时间，秒级时间戳。
InstanceId	String	是	ddosbgp-cn-x1	要查询的防护包实例ID。
PageNo	Integer	是	1	列表的页码，默认值为1。
PageSize	Integer	是	10	分页查询时每页的行数，最大值为50，默认值为10。
StartTime	Integer	是	1557305044	查询开始时间，秒级时间戳。
Ip	String	否	1.1.1.1	要查询的防护对象IP。
ResourceGroupId	String	否	test	资源组ID。
ResourceRegionId	String	否	cn-hangzhou	资源组地区ID。

返回数据

名称	类型	示例值	描述
Events			DDoS事件信息。
EndTime	Integer	1557891306	攻击结束时间，秒级时间戳。
Ip	String	1.1.1.1	被攻击的IP。
Mbps	Integer	110000	攻击流量大小，单位为Mbps。
Pps	Integer	0	攻击报文数量，单位为pps
StartTime	Integer	1557889506	攻击开始时间，秒级时间戳。
Status	String	defense_end	事件状态，取值： · hole_begin：黑洞中 · hole_end：黑洞结束 · defense_begin：清洗中 · defense_end：清洗结束
RequestId	String	6A507DC8-F657-4C13-84E2-D1D1B9400753	本次请求的ID。
Total	Long	8	DDoS事件总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDdosEvent
&EndTime=1557909844
&InstanceId=ddosbgp-cn-x1
&PageNo=1
&PageSize=10
&StartTime=1557305044
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeDdosEventResponse>
     <RequestId>6A507DC8-F657-4C13-84E2-D1D1B9400753</RequestId>
     <Events>
```

```
            <Event>
                  <Pps>0</Pps>
                  <Status>defense_end</Status>
                  <Ip>1.1.1.1</Ip>
                  <Mbps>110000</Mbps>
                  <EndTime>1557891306</EndTime>
                  <StartTime>1557889506</StartTime>
            </Event>
      </Events>
      <Total>1</Total>
</DescribeDdosEventResponse>
```

JSON 格式

```
{
 "RequestId":"6A507DC8-F657-4C13-84E2-D1D1B9400753",
 "Events":[
  {
   "Pps":0,
   "Ip":"1.1.1.1",
   "Status":"defense_end",
   "Mbps":110000,
   "EndTime":1557891306,
   "StartTime":1557889506
  }
 ],
 "Total":8
}
```

错误码

访问错误中心查看更多错误码。

6.7.2 DescribeOpEntities

调用DescribeOpEntities接口查询用户的操作日志。

说明:

DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

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	DescribeOpEntities	要执行的操作，取值：DescribeOpEntities。
CurrentPage	Integer	是	1	列表的页码，默认值为1。

名称	类型	是否必选	示例值	描述
EndTime	Long	是	1557906714012	查询结束时间，毫秒级时间戳。
PageSize	Integer	是	10	分页查询时每页的行数，最大值为50，默认值为10。
StartTime	Long	是	1555314714011	查询开始时间，毫秒级时间戳。
InstanceId	String	否	ddosbgp-cn-x1	要查询的防护包实例ID。
OrderBy	String	否	opdate	排序字段，取值：opdate（操作时间）。
OrderDir	String	否	ASC	排序方向，取值： · ASC：正序 · DESC：倒序
ResourceGroupId	String	否	test	资源组ID。
ResourceRegionId	String	否	cn-hangzhou	资源组地区ID。

返回数据

名称	类型	示例值	描述
OpEntities	Array		操作日志信息。
EntityObject	String	ddosbgp-cn-o4013qftb006	操作对象，即防护包实例。
EntityType	Integer	1	操作对象类型，取值：1（实例）。
GmtCreate	Long	1557821673000	日志创建时间。
OpAccount	String	system	操作账号，取值：system（系统）。

名称	类型	示例值	描述
OpAction	Integer	8	操作类型，取值： · 3：添加IP · 4：解绑IP · 5：实例降级 · 6：解除黑洞 · 7：重置解除黑洞次数 · 8：恢复弹性
OpDesc	String	{\"entity\":{\"baseBandwidth\":20,\"elasticBandwidth\":101}}	操作说明。
RequestId	String	52C8ECB0-0B1A-4E66-A31C-B6A855120E82	本次请求的ID。
TotalCount	Integer	1	返回结果的数量。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeOpEntities
&CurrentPage=1
&EndTime=1557906714012
&PageSize=10
&StartTime=1555314714011
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeOpEntitiesResponse>
      <TotalCount>1</TotalCount>
      <OpEntities>
            <OpEntity>
                  <OpAccount>system</OpAccount>
                  <OpDesc>{"entity":{"baseBandwidth":20,"elasticBan
dwidth":101}}</OpDesc>
                  <EntityObject>ddosbgp-cn-o4013qftb006</EntityObject>
                  <EntityType>1</EntityType>
                  <GmtCreate>1557821673000</GmtCreate>
                  <OpAction>8</OpAction>
            </OpEntity>
      </OpEntities>
```

```
    <RequestId>52C8ECB0-0B1A-4E66-A31C-B6A855120E82</RequestId>
</DescribeOpEntitiesResponse>
```

JSON 格式

```
{
 "TotalCount":1,
 "OpEntities":[
  {
   "OpAccount":"system",
   "OpDesc":"{\"entity\":{\"baseBandwidth\":20,\"elasticBandwidth\":
101}}",
   "EntityObject":"ddosbgp-cn-o4013qftb006",
   "EntityType":1,
   "GmtCreate":1557821673000,
   "OpAction":8
  }
 ],
 "RequestId":"52C8ECB0-0B1A-4E66-A31C-B6A855120E82"
}
```

错误码

访问错误中心查看更多错误码。

6.7.3 DescribeTraffic

调用DescribeTraffic接口查看指定防护包上的流量情况。

说明:

DDoS防护包的API接口目前仅对企业版DDoS防护包用户开放。

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	DescribeTraffic	要执行的操作，取值：DescribeTraffic。
EndTime	Integer	是	1563445054	查询结束时间，秒级时间戳。
Interval	Integer	是	1000	流量统计的时间间隔区间（单位：秒）。
StartTime	Integer	是	1560853054	查询开始时间，秒级时间戳。

名称	类型	是否必选	示例值	描述
InstanceId	String	否	ddosbgp-cn-*****	要查询的防护包实例ID。 说明: InstanceId与Ip两者必须要至少指定其中一个参数。
Ip	String	否	1.1.1.1	要查询的防护对象IP。 说明: InstanceId与Ip两者必须要至少指定其中一个参数。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
FlowList	Array		流量信息。
FlowType	String	max	显示流量类型: · avg：区间平均值 · max：区间峰值
Kbps	Integer	8	流量大小（单位：Kbps）。
Name	String	73765106-54e7-11e9-aab0-d89d67182200	流量信息记录ID。
Pps	Integer	9	数据包数（单位：pps）。
Time	Integer	1560857000	流量信息时间戳。
RequestId	String	6A507DC8-F657-4C13-84E2-D1D1B9400753	本次请求的ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeTraffic
&EndTime=1563445054
&Interval=1000
&StartTime=1560853054
&InstanceId=ddosbgp-cn-*****
&<公共请求参数>
```

正常返回示例

`XML` **格式**

```
<DescribeTraffic>
   <RequestId>6A507DC8-F657-4C13-84E2-D1D1B9400753</RequestId>
   <FlowList>
      <Name>73765106-54e7-11e9-aab0-d89d67182200</Name>
      <Pps>25</Pps>
      <Time>1560855000</Time>
      <FlowType>max</FlowType>
      <Kbps>17</Kbps>
   </FlowList>
   <FlowList>
      <Name>73765106-54e7-11e9-aab0-d89d67182200</Name>
      <Pps>9</Pps>
      <Time>1560857000</Time>
      <FlowType>max</FlowType>
      <Kbps>8</Kbps>
   </FlowList>
</DescribeTraffic>
```

`JSON` **格式**

```
{
 "FlowList":[
  {
   "Pps":25,
   "Name":"73765106-54e7-11e9-aab0-d89d67182200",
   "Time":1560855000,
   "FlowType":"max",
   "Kbps":17
  },
  {
   "Pps":9,
   "Name":"73765106-54e7-11e9-aab0-d89d67182200",
   "Time":1560857000,
   "FlowType":"max",
   "Kbps":8
  }
 ],
 "RequestId":"6A507DC8-F657-4C13-84E2-D1D1B9400753"
}
```

错误码

访问错误中心查看更多错误码。

6.8 ListTagKeys

调用ListTagKeys接口查询所有标签。

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	ListTagKeys	要执行的操作。取值：ListTagKeys。
RegionId	String	是	cn-hangzhou	要查询的地域ID。
ResourceType	String	是	INSTANCE	资源类型，取值：INSTANCE。
PageSize	Integer	否	20	分页查询时设置的每页行数，最大值为50，默认值为10。
CurrentPage	Integer	否	1	列表的页码，起始值为1，默认值为1。
ResourceGroupId	String	否	test	资源组ID。

返回数据

名称	类型	示例值	描述
RequestId	String	97935DF1-0289-4AA2-9DD1-72377838B16B	本次请求的ID。
CurrentPage	Integer	1	列表的页码。
PageSize	Integer	20	每页的行数。
TotalCount	Integer	6	标签的总数。
TagKeys	Array		标签信息。

名称	类型	示例值	描述
TagKey	String	a	标签键。
TagCount	Integer	1	标签键下标签值的总数。

示例

请求示例

```
http(s)://[Endpoint]/?Action=ListTagKeys
&RegionId=cn-hangzhou
&ResourceType=INSTANCE
&<公共请求参数>
```

正常返回示例

`JSON` **格式**

```
{
 "RequestId":"97935DF1-0289-4AA2-9DD1-72377838B16B",
    "TotalCount": 6,
    "PageSize": 20,
    "CurrentPage": 1,
    "TagKeys": [
      {
        "TagCount": 1,
        "TagKey": "a"
      },
      {
        "TagCount": 1,
        "TagKey": "testKey1"
      },
      {
        "TagCount": 1,
        "TagKey": "testKey2"
      },
      {
        "TagCount": 2,
        "TagKey": "testKey3"
      },
      {
        "TagCount": 1,
        "TagKey": "testKey4"
      },
      {
        "TagCount": 1,
        "TagKey": "x"
      }
    ]
  }
```

`XML` **格式**

```
<ListTagKeysResponse>
     <CurrentPage>1</CurrentPage>
     <PageSize>20</PageSize>
```

```
    <RequestId>97935DF1-0289-4AA2-9DD1-72377838B16B</RequestId>
    <TagKeys>
        <element>
            <TagCount>1</TagCount>
            <TagKey>a</TagKey>
        </element>
        <element>
            <TagCount>1</TagCount>
            <TagKey>testKey1</TagKey>
        </element>
        <element>
            <TagCount>1</TagCount>
            <TagKey>testKey2</TagKey>
        </element>
        <element>
            <TagCount>2</TagCount>
            <TagKey>testKey3</TagKey>
        </element>
        <element>
            <TagCount>1</TagCount>
            <TagKey>testKey4</TagKey>
        </element>
        <element>
            <TagCount>1</TagCount>
            <TagKey>x</TagKey>
        </element>
    </TagKeys>
    <TotalCount>6</TotalCount>
</ListTagKeysResponse>
```

错误码

访问错误中心查看更多错误码。

7 常见问题

7.1 DDoS防护包常见问题

本文介绍DDoS防护包使用中的一些常见问题。

问题1：DDoS防护包的弹性防护计费模式和DDoS高防IP的弹性防护计费模式有什么区别?

- **DDoS高防IP服务按照当日弹性带宽的流量峰值进行计费。**
- **DDoS防护包则按照实际产生的弹性带宽的防护流量的总和进行计费。**

问题 2：DDoS防护包的弹性防护费用如何计算?

DDoS防护包则按照实际产生的弹性带宽的防护流量的总和进行计费，按照每GB 0.2元计算弹性防护流量费用。

- **专业版：当遭受攻击且攻击流量超过保底防护带宽时，对超出保底防护带宽的入方向流量进行计费。**
- **企业版：无论是否遭受攻击，根据入方向的总流量进行计费。**

问题 3： DDoS防护包所防护的IP被黑洞了该怎么办?

防护包提供黑洞解除功能。您可以在DDoS防护管理控制台 > 防护包 > 实例页面，选择存在异常IP的防护包实例，单击解除黑洞前往该实例的防护对象页签，对处于黑洞状态的防护目标进行解除黑洞操作。

您还可以参考*DDoS*防护包黑洞自动解除最佳实践，实现已防护IP的黑洞自动化响应和快速解除。

问题 4： 如果DDoS防护包所防护的IP因遭受攻击而被黑洞，是否该部分攻击流量会被计费?

DDoS防护包的弹性防护流量的计费原则是针对超出保底防护带宽且小于等于弹性防护带宽的防护流量进行计费。被黑洞即意味着入方向的流量已超过所设置的弹性防护带宽，因此不在计费范围内。

说明:
仅针对因黑洞而防护失败的计费周期（五分钟）减免弹性防护流量费用。

问题 5： 当抗D流量包的剩余可用量为0时，弹性防护带宽为何要自动降低为保底防护带宽值？如果此时出现所防护的IP被黑洞的情况，应该如何应对?

由于DDoS防护包的弹性防护流量的计费模式为按照保底防护带宽和弹性防护带宽间的防护流量总和进行计费，并通过抗D流量包的预付费流量自动抵扣所消耗的弹性防护流量。为了避免因持续的

大流量攻击产生高额后付费账单，遵循“用户买多少用多少”的原则进行收费，当抗D流量包的剩余可用量为0时，DDoS防护包的弹性防护带宽将自动下降至保底防护带宽。

此时，如果DDoS防护包所防护的IP出现黑洞，您应该先购买一定量的抗D流量包，然后在DDoS防护管理控制台中升级DDoS防护包实例的弹性防护带宽，最后使用解除黑洞功能解除黑洞状态，通过弹性防护能力抵御攻击流量。

说明:

如果该DDoS防护包实例的解除黑洞的次数已用完，建议您耐心等待黑洞自动解除后再调整弹性防护带宽。

问题 6： 如果购买时选错了DDoS防护包实例的地域怎么办?

如果您想要防护的IP与所购买的DDoS防护包实例的地域不一致，请提交工单申请退款后重新购买新的DDoS防护包实例。

问题 7： DDoS防护包所防护的IP遭受大流量攻击直接被黑洞，但未消耗抗D流量包是什么原因?

如果您所防护的IP遭受的攻击流量在短时间内超出所设定的DDoS防护包的最大弹性防护带宽（例如，您的DDoS防护包的弹性防护带宽设置为30G，所防护的IP在一秒内遭受的攻击峰值即超过50G），则您的IP会直接被黑洞，且不产生任何弹性防护流量费用。

7.2 防护包添加防护IP时收到“IP不属于你”的错误提示

当您在为DDoS防护包设置防护对象IP时，收到IP不属于你的错误提示，请参考本章节处理问题。

问题描述

当您在为DDoS防护包设置防护对象IP时，收到IP不属于你的错误提示。

解决方案

按照以下步骤进行排查：

1. **检查您所输入的IP地址，确认输入的IP地址正确无误。**
2. **检查您想要添加的防护IP对应的云产品所属的地域，确认该地域与您所购买的DDoS防护包实例的所属地域一致。**
3. **如果该DDoS防护包是共享型防护包，检查您想要添加的防护IP所对应的云产品，确认所对应的云产品与您为该DDoS防护包实例所设置的防护对象（云产品）一致。**
4. **如果您想要添加的防护IP是WAF IP，检查该WAF实例的所属地域，确认DDoS防护包支持该地域。**

说明:

目前，DDoS防护包仅支持华东一（杭州）、华北二（北京）、华南一（深圳）、美西等地域的WAF IP。

8 相关协议

8.1 DDoS防护包服务条款

本服务条款是阿里云计算有限公司（以下简称“阿里云”）与您就DDoS防护包服务的相关事项所订立的有效合约。您通过盖章、网络页面点击确认或以其他方式选择接受本服务条款，或实际使用阿里云提供的DDoS防护包服务，即表示您与阿里云已达成协议并同意接受本服务条款的全部约定内容。如若双方盖章文本与网络页面点击确认或以其他方式选择接受之服务条款文本，存有不一致之处，以双方盖章文本为准。

在接受本服务条款之前，请您仔细阅读本服务条款的全部内容（特别是以粗体及/或下划线标注的内容）。如果您对本服务条款的条款有疑问的，请通过阿里云官网（www.aliyun.com） 公布的联系方式，进行询问，阿里云将向您解释条款内容。如果您不同意本服务条款的任意内容，或者无法准确理解阿里云对条款的解释，请不要进行后续操作。

1. 定义

1.1 本条款中的“您”是指：所有使用阿里云DDoS防护包服务的主体（包括但不限于个人、团队、公司、组织等），或称“用户”。

1.2 本条款中“服务”指：阿里云向您提供www.aliyun.com 网站上所展示的DDoS防护包服务以及相关的技术及网络支持服务。

1.3 DDoS: Distributed Denial of Service，即分布式拒绝服务攻击，在云端该攻击表现为，通过仿冒大量的正常服务请求来阻止用户访问其在云端数据、应用程序或网站。

1.4 防护带宽：在服务器遭受DDoS攻击时，服务器可以承受的攻击流量最大值。在攻击流量未超过防护带宽的情况下，用户的服务器可正常运行。

2. 服务费用

2.1 阿里云将在阿里云官网公布DDoS防护包服务的计费模式、价格体系等信息。具体计费规则请您查看www.aliyun.com上的页面公告，且按照页面公布的当时有效的计费模式与标准为准。包年包月服务不提前退订、以及您已使用了服务不支持退款。

2.2 DDoS防护包的费用由保底防护带宽费用和弹性防护流量费用两部分组成。保底防护带宽费用为按月预付费形式，在您付费之后，阿里云才开始为您提供服务；弹性防护流量费用：根据实际使用中超出保底防护带宽所产生的弹性防护流量计费。您需要通过购买预付费形式的抗D流量包，抵扣DDoS防护包所产生的弹性防护流量费用。

2.3 您应保持账户余额充足以确保服务的持续使用。阿里云保留在您未按照约定支付费用之前不向您提供服务和/或技术支持，或者终止服务和/或技术支持的权利，同时，阿里云保留对后付费服务中的欠费行为追究法律责任的权利。

2.4 服务期满双方愿意继续合作的，您应在服务期满前支付续费款项，以使服务得以继续进行。如续费时阿里云对产品体系、名称或价格进行调整的，双方同意按照届时有效的新的产品体系、名称或价格履行。

2.5 您理解并同意，阿里云有权根据经营情况，不定期的对DDoS防护包服务的产品体系、名称或价格、计费模式等进行调整。阿里云将尽合理范围内的最大努力，将前述调整及变化，通过官网公告、站内通知等方式提前告知您，或提前发送至您预留的联系方式。

2.6 阿里云有权根据其自身业务推广的需要不时推出优惠活动，您完全理解，所有的优惠活动以及业务推广服务都是阿里云提供的一次性特别优惠，优惠内容不包括赠送服务项目的修改、更新及维护费用，并且赠送服务项目不可折价冲抵服务价格。

3.权利义务

3.1 您的权利、义务

3.1.1 您同意遵守本服务条款以及服务展示页面的相关管理规范及流程。您了解上述协议及规范等的内容可能会不时变更。如本服务条款的任何内容发生变动，阿里云应通过提前30天在www.aliyun.com 的适当版面公告向您提示修改内容。如您不同意阿里云对本服务条款所做的修改，您有权停止使用阿里云的服务，此等情况下，阿里云应与您进行服务费结算（如有），并且您应将业务迁出。如您继续使用阿里云服务，则视为您接受阿里云对本服务条款相关条款所做的修改。

3.1.2 您应按照阿里云的页面提示及本服务条款的约定支付相应服务费用。

3.1.3 您承诺：

3.1.3.1 不利用本服务从事DDoS防护、DNS防护等防护售卖业务；

3.1.3.2 如果您利用DDoS防护包服务防护的网站或业务需要获得国家有关部门的许可或批准的，应获得该有关的许可或批准。包括但不限于以下内容：

- **如您网站提供非经营性互联网信息服务的，必须办理非经营性网站备案，并保证所提交的所有备案信息真实有效，在备案信息发生变化时及时在备案系统中提交更新信息；**
- **如您网站提供经营性互联网信息服务的，还应自行在当地通信管理部门取得经营性网站许可证；**
- **如您经营互联网游戏网站的，您应依法获得网络文化经营许可证；**
- **如您经营互联网视频网站的，您应依法获得信息网络传播视听节目许可证；**
- **若您从事新闻、出版、教育、医疗保健、药品和医疗器械等互联网信息服务，依照法律、行政法规以及国家有关规定须经有关主管部门审核同意，在申请经营许可或者履行备案手续前，应当依法经有关主管部门审核同意。**

- 您理解并认可，以上列举并不能穷尽您进行经营或非经营活动需要获得国家有关部门的许可或批准的全部类型，您应获得有关的许可或批准，并应符合国家及地方不时颁布相关法律法规之要求。

3.1.3.3 除阿里云明示许可外，不得修改、翻译、改编、出租、转许可、在信息网络上传播或转让阿里云提供的软件，也不得逆向工程、反编译或试图以其他方式发现阿里云提供的软件的源代码；

3.1.3.4 若阿里云的服务涉及第三方软件之许可使用的，您同意遵守相关的许可协议的约束；

3.1.3.5 您利用DDoS防护包服务进行防护的业务须为正常的商业、科研等符合国家法律规定的业务，不得用于从事任何非法业务，包括但不限于：

- 违反国家规定的政治宣传和/或新闻；
- 涉及国家秘密和/或安全；
- 封建迷信和/或淫秽、色情和/或教唆犯罪；
- 博彩有奖、赌博游戏、“私服”、“外挂”等非法互联网出版活动；
- 违反国家民族和宗教政策；
- 妨碍互联网运行安全；
- 侵害他人合法权益和/或其他有损于社会秩序、社会治安、公共道德的活动；
- 其他违反法律法规、部门规章或国家政策的内容。

3.1.3.6 不建立或利用有关设备、配置运行与所购服务无关的程序或进程，或者故意编写恶意代码导致大量占用阿里云云计算资源（如DDoS防护包服务、网络带宽、存储空间等）所组成的平台（以下简称“云平台”）中的服务器内存、CPU或者网络带宽资源，给阿里云云平台或者阿里云的其他用户的网络、服务器（包括但不限于本地及外地和国际的网络、服务器等）、产品/应用等带来严重的负荷，影响阿里云与国际互联网或者阿里云与特定网络、服务器及阿里云内部的通畅联系，或者导致阿里云云平台产品与服务或者阿里云的其他用户网站所在的服务器宕机、死机或者用户基于云平台的产品/应用不可访问等；

3.1.3.7 不进行任何破坏或试图破坏网络安全的行为（包括但不限于钓鱼，黑客，网络诈骗，网站或空间中含有或涉嫌散播：病毒、木马、恶意代码，及通过虚拟服务器对其他网站、服务器进行涉嫌攻击行为如扫描、嗅探、ARP欺骗、DDoS等）；

3.1.3.8 不进行任何改变或试图改变阿里云提供的系统配置或破坏系统安全的行为；

3.1.3.9 不利用阿里云提供的服务从事损害阿里云、阿里云的关联公司或阿里巴巴集团内包括但不限于阿里巴巴、淘宝、支付宝、阿里妈妈、阿里金融等（以下统称为阿里巴巴公司）各公司、网站合法权益之行为，前述损害阿里巴巴公司、网站合法权益的行为包括但不限于违反阿里巴巴公司公布的任何服务协议/条款、管理规范、交易规则等规范内容、破坏或试图破坏阿里巴巴公司公平交易环境或正常交易秩序等；

3.1.3.10 不从事其他违法、违规或违反阿里云服务条款的行为；

3.1.3.11 如阿里云发现您违反上述条款的约定，有权根据情况采取相应的处理措施，包括但不限于立即中止服务、终止服务等。如因您违反上述保证而给阿里云（包括阿里云关联公司）或阿里云合作伙伴造成损失的，您还应自行承担一切法律责任并赔偿损失；

3.1.3.12 如果第三方机构或个人对您提出质疑或投诉，阿里云将通知您，您有责任在规定时间内进行说明并出具证明材料，如您未能提供相反证据或您逾期未能反馈的，阿里云将采取包括但不限于立即中止服务或终止服务等处理措施。因您未及时更新联系方式或联系方式不正确而致使未能联系到您的，亦视为您逾期未能反馈；

3.1.3.13 阿里云依据第3.1.3.11条、第3.1.3.12条对您采取了中止服务、终止服务等措施而给您造成任何损失的，阿里云不承担任何责任。

3.1.4 您不应在阿里云服务或平台之上安装、使用盗版软件；您对自己行为（如自行安装的软件和进行的操作）所引起的结果承担全部责任。

3.1.5 您对自己存放在阿里云云平台上的数据以及进入和管理阿里云云平台上各类产品与服务的口令、密码的完整性和保密性负责。因您维护不当或保密不当或操作不当致使上述数据、口令、密码等丢失或泄漏所引起的一切损失和后果均由您自行承担。

3.1.6 您应向阿里云提交执行本服务条款的联系人和管理用户网络及云平台上各类产品与服务的人员名单和联系方式并提供必要的协助。如以上人员发生变动，您应自行将变动后的信息进行在线更新并及时通知阿里云。因您提供的人员的信息不真实、不准确、不完整，以及因以上人员的行为或不作为而产生的结果，均由您负责。

3.1.7 您了解阿里云无法保证其所提供的服务毫无瑕疵（如阿里云安全产品并不能保证您的硬件或软件的绝对安全），但阿里云承诺不断提升服务质量及服务水平。所以您同意：即使阿里云提供的服务存在瑕疵，但上述瑕疵是当时行业技术水平所无法避免的，其将不被视为阿里云违约。您同意和阿里云一同合作解决上述瑕疵问题。

3.1.8 您应依照相关操作指引进行操作。由您手动设置的部分及其产生的结果由您自行负责，请您自行把握风险并谨慎操作。

3.1.9您将在所选购的防护带宽范围内享受DDoS防护服务。如攻击流量有可能超过您所购买的防护带宽，您应及时升级至更高流量的防护带宽，否则您的服务器会由于被攻击导致业务中断。

3.2 阿里云的权利、义务

3.2.1 阿里云应按照本服务条款的约定及产品页面的服务标准，向您提供服务。

3.2.2 服务期限内，阿里云提供7×24小时的在线工单服务系统及售后服务电话，解答客户在使用中的问题。

3.2.3 阿里云将消除您非人为操作所出现的故障，但因您的原因和/或不可抗力以及非阿里云控制范围之内的事项除外。

3.2.4 阿里云提供本服务条款规定的技术支持，但不承担由于您的原因（包括但不限于代码质量，人为管理疏漏，自身安全管理等）造成的影响和损失。

4. 知识产权

4.1 您承认阿里云向您提供的任何资料、技术或技术支持、软件、服务等的知识产权均属于阿里云或第三方所有。除阿里云或第三方明示同意外，您无权复制、传播、转让、许可或提供他人使用上述资源，否则应承担相应的责任。

5. 保密条款

5.1 保密资料指由一方向另一方披露的所有技术及非技术信息（包括但不限于产品资料、产品计划、价格、财务及营销规划、业务战略、客户信息、客户数据、研发、软件硬件、API应用数据接口、技术说明、设计、特殊公式、特殊算法等）。

5.2 本服务条款任何一方同意对获悉的对方之上述保密资料予以保密，并严格限制接触上述保密信息的员工遵守本条之保密义务。除非国家机关依法强制要求或上述保密资料已经进入公有领域外，接受保密资料的一方不得对外披露。

5.3 本服务条款双方明确认可各自用户信息和业务数据等是各自的重要资产及重点保密信息。本服务条款双方同意尽最大的努力保护上述保密信息等不被披露。一旦发现有上述保密信息泄露事件，双方应合作采取一切合理措施避免或者减轻损害后果的产生。

5.4 本条款不因本服务条款的终止而失效。

6. 期限与终止

6.1 阿里云DDoS防护包服务自您开通服务之日起即可使用，至法律规定或本服务条款约定的终止情形出现之时终止。

6.2 发生下列情形，DDoS防护包服务终止：

6.2.1 双方协商一致终止；

6.2.2 由于您严重违反本服务条款（包括但不限于a.您未按照本服务条款的约定履行付款义务，及/或b.您严重违反本服务条款中所做的承诺，及/或c.您严重违反法律规定等），阿里云有权按本服务条款的相关约定单方面终止服务，并不退还您已经支付的费用；

6.2.3 阿里云由于自身经营政策的变动，提前通过提前30天发网站内公告、在网站内合适版面发通知或给您发站内通知、书面通知的方式，终止本服务条款项下的服务。

7. 违约责任

7.1 本服务条款任何一方违约均须依法承担违约责任。

7.2 如果因阿里云原因造成您连续72小时不能正常使用服务的，您可终止接受服务，但非阿里云控制之内的原因引起的除外。

7.3 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、特殊性的损害，包括您使用阿里云服务而遭受的利润损失承担责任（即使您已被告知该等损失的可能性）。

7.4 在任何情况下，阿里云对本服务条款所承担的违约赔偿责任总额不超过向您收取的该违约行为所对应的DDoS防护包服务之服务费总额。

8. 不可抗力

8.1 因不可抗力或者其他意外事件，使得本服务条款的履行不可能、不必要或者无意义的，遭受不可抗力、意外事件的一方不承担责任。

8.2 不可抗力、意外事件是指不能预见、不能克服并不能避免且对一方或双方当事人造成重大影响的客观事件，包括但不限于自然灾害如洪水、地震、瘟疫流行等以及社会事件如战争、动乱、政府行为、电信主干线路中断、黑客、网路堵塞、电信部门技术调整和政府管制等。

9. 法律适用及争议解决

9.1 本服务条款受中华人民共和国法律管辖。

9.2 在执行本服务条款过程中如发生纠纷，双方应及时协商解决。协商不成时，任何一方可直接向杭州市西湖区人民法院提起诉讼。

10. 附则

10.1 阿里云在www.aliyun.com 相关页面上的服务说明、价格说明和您确认同意的订购页面是本服务条款不可分割的一部分，如果阿里云在www.aliyun.com 相关页面上的服务说明、价格说明和您确认同意的订购页面与本服务条款有不一致之处，以本服务条款为准。

10.2 阿里云有权以提前30天在www.aliyun.com 上公布或给您发站内通知或书面通知的方式将本服务条款的权利义务全部或者部分转移给阿里云的关联公司。

10.3 如果任何条款在性质上或其他方面理应地在此协议终止时继续存在，那么应视为继续存在的条款，这些条款包括但不局限于保证条款、保密条款、知识产权条款、法律适用及争议解决条款。

10.4 本服务条款项下，阿里云对您的所有通知均可通过网页公告、网站内通知、电子邮件、手机短信或书面信函等任一方式进行；该等通知于发送之日即视为已送达收件人。