ALIBABA CLOUD

阿里云

DDoS防护

DDoS原生防护用户指南

文档版本：20220708

阿里云

法律声明

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

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

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

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

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

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

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

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

目录

1.流量安全总览

流量安全总览能够帮助您处理网络资产受到的网络流量攻击（以下简称流量攻击）事件，及全面了解网络资产的安全防御状态和安全评估、资产受攻击趋势、热点资产分布等信息。本文介绍了查询流量安全总览数据的方法和相关数据的说明。

查询流量安全总览

1. 登录流量安全产品控制台。
2. 在**总览**页面，查询流量安全总览数据。

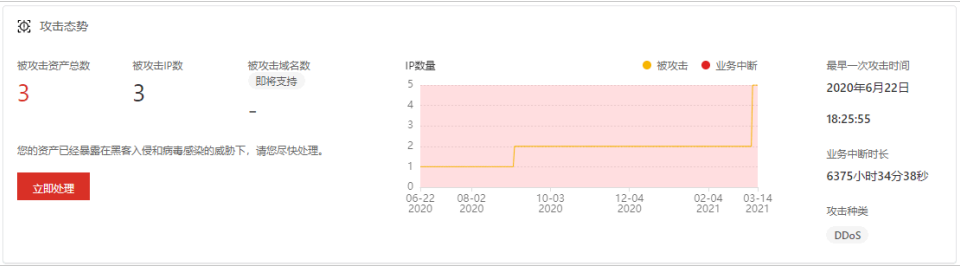
下表描述了流量安全总览页面支持查询的数据及说明。

名称	用途	支持的操作	详细说明

名称	用途	支持的操作	详细说明
攻击态势（图示①）	帮助您了解网络资产（目前仅支持公网IP资产）遭受流量攻击的整体状况，及处理导致业务中断的攻击威胁。	对于被攻击的资产，您可以通过**立即处理**入口，获取相关的应急操作建议和防御部署方案。	攻击态势数据说明
安全防御（图示②）	帮助您了解网络资产的安全防护状态和安全加固建议。	如果网络资产存在安全风险，建议您根据建议执行安全加固，提升安全防御水平。	安全防御数据说明
攻击分析（图示③）	帮助您分析网络资产上近一年内发生的网络攻击的整体趋势，便于您评估业务的受攻击风险和安全防护需求。	支持切换查询时间范围和攻击数据类型。	攻击分析数据说明
热点资产（图示④）	帮助您分析近一年内受攻击次数最多的网络资产排行，便于您识别关键资产。	暂无。	热点资产数据说明
行业风险透视（图示⑤）	帮助您分析业务所在行业在近半年内发生的网络攻击事件数量的趋势，了解行业安全态势。	支持设置您的业务所在行业，关注对应行业的安全风险。	行业风险透视数据说明
流量安全相关资料（图示⑥）	提供了流量安全领域的最新资讯，帮助您了解前沿动态。	支持查看您感兴趣的资讯的具体内容。	流量安全相关资料

攻击态势数据说明

攻击态势展示了您的网络资产（目前仅支持公网IP资产）遭受网络攻击的整体状况，具体包含以下信息：**被攻击资产总数**、**被攻击IP数**、**最早一次攻击时间**、（攻击导致的）**业务中断时长**、**攻击类型**等。



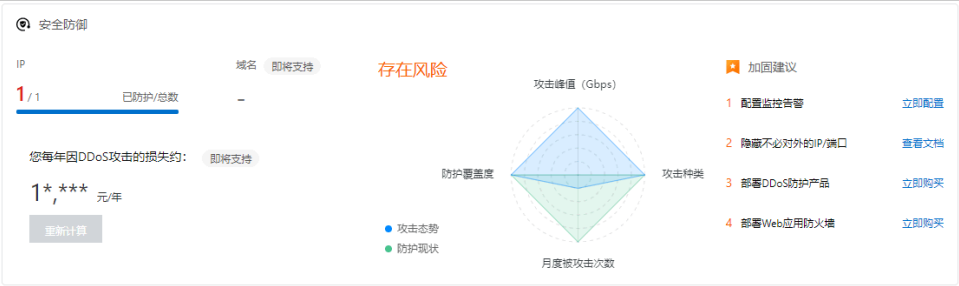
如果存在已经导致业务中断的攻击威胁，您可以单击**立即处理**，查询攻击信息和相关的**应急操作**及**部署防御方案**。具体说明如下：

- **应急操作**可以帮助您快速恢复业务，但是不能防止业务再次被攻击，且应急操作一般存在使用限制（例如，可以使用的次数有限、效果有限等）。
- **部署防御方案**提供了针对该类型攻击的有效解决方案，通过部署安全服务，达到减少或杜绝业务被攻击导致中断的情形。

例如，对于业务遭受DDoS攻击导致中断的情形，您可以在**立即处理**页面，通过**应急操作**，将被攻击IP从黑洞中恢复出来；也可以通过**部署防御方案**，为业务部署DDoS高防（新BGP）、DDoS原生防护服务，提升业务对抗DDoS攻击的防御能力。关于具体方案的介绍及如何开通，请参见**立即处理**页面的说明。

安全防御数据说明

安全防御展示了您的网络资产的安全防护状态（例如，已防护资产在所有资产中的占比、业务安全评估等）和相关的安全**加固建议**，帮助您了解业务网络安全的薄弱环节并获取提升安全防御能力的措施。



如果您的业务安全评估结果为**存在风险**（如上图所示），建议您根据**加固建议**区域提供的相关建议，执行安全加固措施，提升业务的安全防御水平。

攻击分析数据说明

攻击分析展示了您的网络资产上近一年内发生的网络攻击的整体趋势，帮助您评估业务的受攻击风险和安全防护需求。

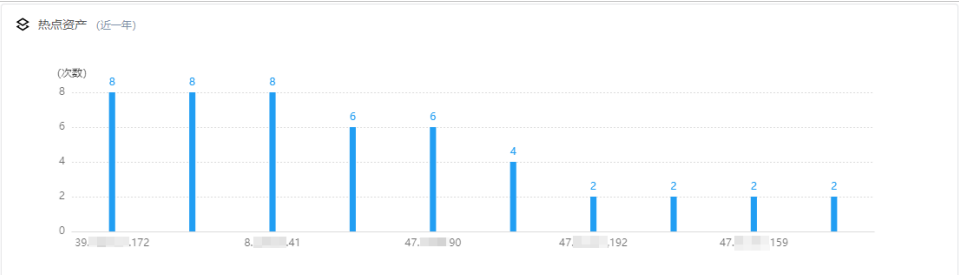
目前支持查询的数据包括：

- **攻击趋势（IP）**：针对IP资产的流量攻击的基本信息，具体包括流量**清洗次数**、**黑洞次数**、**清洗IP数**、**黑洞IP数**。
- **攻击峰值（IP）**：针对IP资产的流量攻击的攻击峰值变化趋势。
- **攻击时长（IP）**：针对IP资产的流量攻击的攻击持续时长变化趋势。

您可以通过单击该区域右上角的时间选择按钮，选择查询时间，具体包括**近1周**、**近1月**、**近3月**、**近1年**。

热点资产数据说明

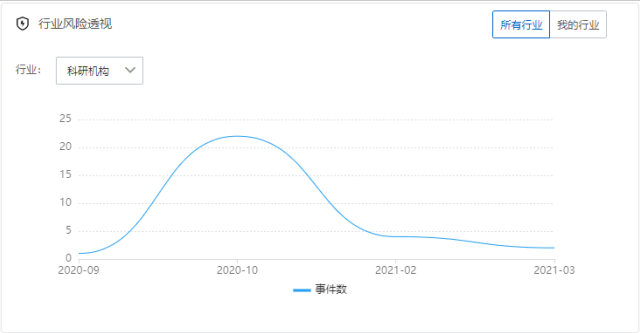
热点资产展示了近一年内您的网络资产中受攻击次数最多的资产排行，帮助您识别关键资产。



建议您对受攻击次数最多的资产部署完善的安全加固方案。更多信息，请参见DDoS攻击缓解最佳实践。

行业风险透视数据说明

行业风险透视展示了近半年内不同行业内发生的网络攻击事件数量的变化趋势，帮助您了解业务所在行业的整体安全态势。



您可以通过单击该区域右上角的**所有行业**、**我的行业**，选择要查询的数据类型。具体说明如下：

- 在**所有行业**下，您可以通过**行业**下拉列表，选择您关注的行业（例如，科研机构、汽车制造、游戏等），查询该行业在近半年内发生的网络攻击事件数量。
- 在**我的行业**下，您可以设置您的业务所在行业，查询业务所在行业在近半年内发生的网络攻击事件数量。

流量安全相关资料

流量安全相关资料展示了流量安全领域近期发布的相关资讯的链接，帮助您了解流量安全防护领域的背景信息和前沿动态。

您可以单击感兴趣的链接，查看具体内容。

2.资产中心

DDoS原生防护基础版默认开启，免费为您账号下的阿里云云产品提供不超过5 Gbps流量的DDoS攻击防护能力。本文介绍了如何查询您的阿里云账号下公网IP资产的DDoS防护信息以及如何为指定资产提升DDoS防护能力。

操作步骤

1. 登录流量安全产品控制台。
2. 在左侧导航栏，单击**资产中心**。
3. 在**资产中心**页面，您可以查看DDoS攻击防护说明或公网IP资产的DDoS防护信息。
   - 查看DDoS攻击防护说明：
     - 单击**默认基础防护阈值**，查看不同地域下资产的默认DDoS防护能力，即支持防御的DDoS攻击带宽。
     - 单击**黑洞**，查看阿里云黑洞策略。
     - 单击**DDoS原生防护**，前往DDoS原生防护**实例管理**页面，您可以根据需要开通DDoS原生防护实例。具体操作，请参见购买DDoS原生防护企业版实例。
   - 查看公网IP资产的DDoS防护信息：
     a. 单击需要查看的云产品页面，例如ECS。
     b. 在资产列表查看公网IP资产的DDoS防护信息。

信息类型	说明
IP/备注	资产的公网IP地址。 单击公网IP，可以跳转到**实例详情**页，您可以查看公网IP资产的流量趋势，以及发生事件的详细信息。
状态	公网IP资产的DDoS安全状态。 ■ **正常** ■ **清洗中**：您可以手动取消流量清洗，具体操作，请参见取消流量清洗。 ■ **黑洞中**：您可以查看黑洞事件记录，具体操作，请参见查看IP进入黑洞的时间和原因。
防护能力	公网IP资产的DDoS攻击防护能力，即可以防御的最大攻击带宽。 如果攻击带宽超过了当前实例的防护能力，则实例会进入黑洞。您可以参照步骤为指定实例提升DDoS防护能力。
清洗阈值	触发流量清洗的最小访问带宽，包括流量（Mbps）和报文数量（PPS）。更多信息，请参见设置流量清洗阈值。

4. 为指定公网IP资产提升DDoS防护能力。

   如果DDoS原生防护基础版提供的DDoS攻击防护能力不能满足您的业务需求，您可以根据攻击防御场景，选择DDoS原生防护企业版或DDoS高防。具体信息，请参见选型参考。

   - 开通DDoS原生防护企业版

以给ECS类型的公网IP资产开启原生防护为例，其他类型的公网IP资产操作类似：

a. 在**ECS**页签选中要操作的公网IP，单击列表下方的**添加原生防护**。

b. 在**DDoS原生防护列表**页面，选择要应用的原生防护实例，单击**操作**列下的**添加**并完成**确认**。

> **说明** 如果您未开通DDoS原生防护实例，请先前往购买页购买。具体操作，请参见购买DDoS原生防护企业版实例。

- 开通DDoS高防

  您可以在左侧导航栏，单击**网络安全**下的**DDoS高防（新BGP）**或者**DDoS高防（国际）**，直达对应的产品控制台。关于DDoS高防的相关配置，请参见快速入门。

3.流量安全管理器

流量安全管理器向您展示阿里云流量安全防护解决方案的整体架构和您的网络资产的防护状态，帮助您分析业务流量安全防护的薄弱环节，及了解对应的解决方案。本文介绍了流量安全管理器的使用方法。

背景信息

您可以通过流量安全管理器，查看当前阿里云账号保有的公网IP资产的数量和被攻击的资产数量，以及阿里云提供的不同安全防护产品的开通状态。

操作步骤

1. 登录流量安全产品控制台。
2. 在左侧导航栏，单击**流量安全管理器**。
3. 在**流量安全管理器**页面，您可以单击右上角的**开始探索**体验流量安全管理器DEMO，也可以单击**申请内测**查看真实的业务数据。
   - **开始探索**

     流量安全管理器DEMO将引导您查看**资产安全总览**、**流量类型总览**、**被攻击资产**、**攻击源**、**攻击事件**等信息。

     > **注意** DEMO中的数据非真实数据，仅供参考。

   - **申请内测**

     如果您需要通过流量安全管理器查看真实的业务数据，可以单击页面右上角的**申请内测**，并在**流量安全管理器内测申请**页面提交申请。

     阿里云工程师在收到您的申请后，将通过您提交的联系方式联系您，与您确认内测相关事宜。内测申请经审核通过后，您将可以在**流量安全管理器**页面查看真实的业务数据。

4.购买DDoS原生防护企业版实例

本文介绍了购买DDoS原生防护企业版实例的操作方法。

背景信息

DDoS原生防护提供基础版和企业版套餐。具体说明如下：

- 基础版：默认为阿里云公网IP资产免费开启，无需购买。提供不超过5 Gbps的DDoS基础防护能力。
- 企业版：购买后开启，支持防护阿里云公网IP资产。提供不改变IP地址的DDoS共享全力防护能力。

  全力防护指阿里云根据当前机房网络的整体水位，尽可能帮助您防御DDoS攻击。随着阿里云网络能力的不断提升，全力防护的防护能力也会相应提升，而不需要您额外付出升级成本。

  关于DDoS原生防护的详细计费说明，请参见DDoS原生防护计费方式。

> **说明** 如果您需要防护的资产是EIP，您也可以在EIP购买页上直接开通DDoS防护（增强）功能。相关操作，请参见申请EIP。关于开通DDoS防护（增强）功能的费用信息，请参见按量付费。

前提条件

- 您需要购买DDoS原生防护企业版的阿里云账号已完成实名认证。
- 支持防护的云产品为ECS、SLB、EIP（含NAT）、轻量服务器、WAF。

操作步骤

1. 访问DDoS原生防护购买页面。
2. 配置如下购买项，完成DDoS原生防护企业版实例的购买。

配置项	说明
商品类型	选择**DDoS原生防护**。
防护套餐	默认已选择**企业版**。不支持修改。
防护次数	默认已选择**不限次**。不支持修改。
IP协议	原生防护实例支持防护的IP协议类型。可选项：**IPv4**、**IPv6**。
资源所在地域	原生防护实例的地域。 **注意** ○ DDoS原生防护实例的地域必须与需要防护的阿里云公网IP资产地域一致。 ○ 目前仅支持在原生防护购买页购买中国内地地域的实例。如果您需要购买海外和港澳台地域的原生防护企业版实例，请提交工单或者联系销售人员。

配置项	说明
业务带宽	要防护业务的正常业务规模（以网络带宽来衡量）。 关于业务规模的估算方法，请参见DDoS原生防护企业版实例规格。
保护IP数量	要防护的IP的总个数。最小规格为100个公网IP。如果您需要防护更多IP，可以增大该规格。
防护分析	提供防护流量的全量日志分析和报表功能。可选项：**开启**、**关闭**。 **说明** 该功能正在公测中（公测期间免费）。开启防护分析功能后，您可以在控制台左侧导航栏看到防护分析模块。
资源组	资源组是当前阿里云账号下一组相关的资源，用于对资源组内成员、权限和资源进行独立管理。您可以选择已创建的资源组或新建资源组。 更多信息，请参见创建资源组。
购买数量	要购买的原生防护实例的总数。
购买时长	要购买的原生防护实例的有效期。可以根据需要选择是否开启**到期自动续费**。

3. 单击**立即购买**并完成支付。

   您可以访问**实例管理**页面，查看已购买的实例并将要防护的公网IP资产添加为实例的防护对象。具体操作，请参见添加防护对象。

5.业务监控

业务监控页面为您展示了DDoS原生防护实例上的业务防护数据（例如，被防护资产的流量趋势、DDoS攻击事件记录等），帮助您随时掌握业务的安全状态。本文介绍了查询业务监控数据的方法和相关数据的说明。

前提条件

已购买DDoS原生防护实例且为实例添加了防护对象。

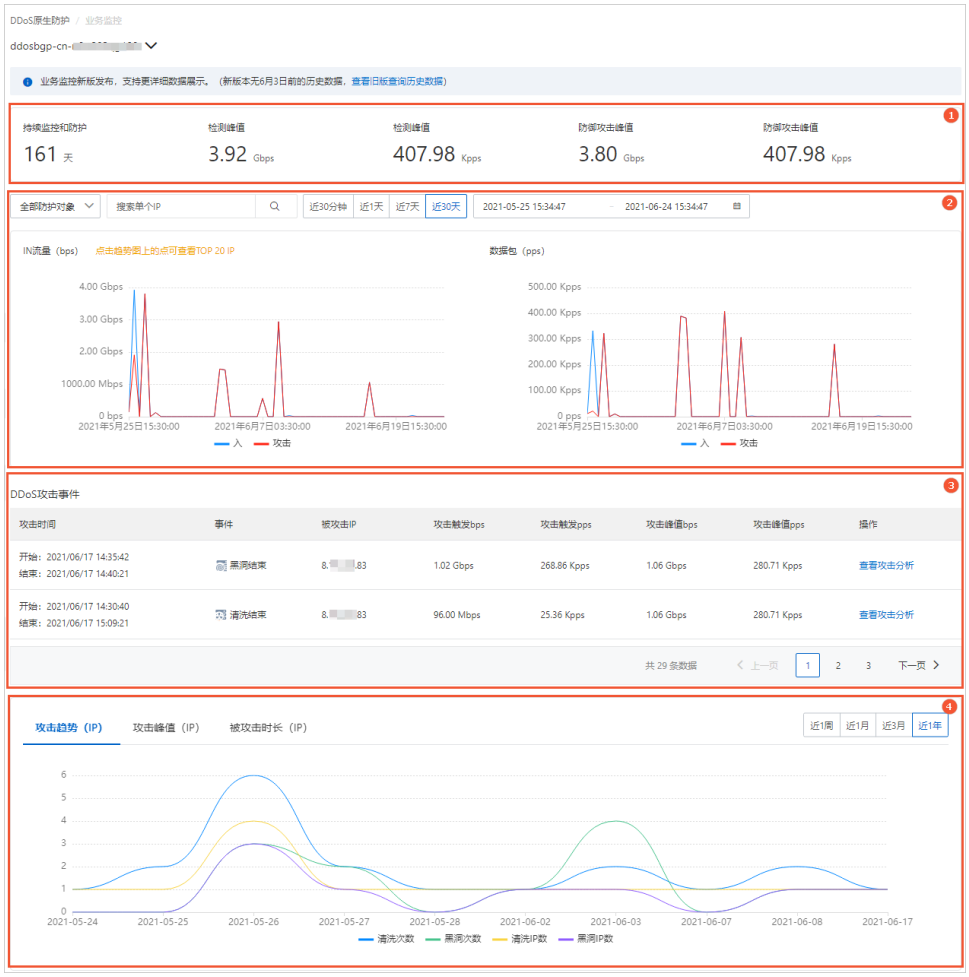
相关操作，请参见购买DDoS原生防护企业版实例、添加防护对象。

背景信息

业务监控页面仅支持查询2021年06月03日及以后的数据。如果您需要查询该日期前的历史数据，请参见查看安全报表。

查询业务监控数据

1. 登录流量安全产品控制台。
2. 在左侧导航栏，选择**网络安全 > DDoS原生防护 > 业务监控**。
3. 在顶部菜单栏左上角处，选择实例所在资源组和地域。
4. 在页面左上角，选择要查询的DDoS原生防护实例。
5. 查看DDoS原生防护实例的业务监控数据。



下表描述了业务监控页面支持查询的数据及说明。

类型	用途	支持的操作	详细说明
业务统计数据（图示①）	帮助您了解DDoS原生防护实例的历史防护峰值数据，包括持续监控和防护的天数、检测到的全部流量峰值（bps、pps）和防御的攻击流量峰值（bps、pps）。	无。	业务统计数据说明
业务流量趋势（图示②）	帮助您了解受DDoS原生防护实例保护的公网IP资产的入方向业务流量的变化趋势，包含宽带速率（bps）变化趋势和数据包转发率（pps）变化趋势。	设置防护对象、时间范围，查询相关的数据。	业务流量趋势数据说明
DDoS攻击事件（图示③）	帮助您了解针对DDoS原生防护实例的攻击事件（包含清洗事件、黑洞事件）信息，并支持及对事件进行分析和处理。	○ 设置防护对象、时间范围，查询相关的数据。 ○ 针对某个DDoS攻击事件记录：提前解除清洗、下载抓包、查看攻击分析。	DDoS攻击事件数据说明
攻击趋势分析图（图示④）	帮助您分析DDoS原生防护实例上近一年内发生的网络攻击的整体趋势，便于您评估业务的受攻击风险和安全防护需求。	设置时间范围，查询相关的数据。	攻击趋势分析数据说明

业务统计数据说明

该区域展示了以下统计数据：

- **持续监控和防护**：表示当前DDoS原生防护实例已经为您服务的天数。
- **检测峰值**：表示在DDoS原生防护实例为您服务期间，实例上检测到的全部业务流量的峰值数据，包括宽带速率（单位：bps）和数据包转发率（单位：pps）。
- **防御攻击峰值**：表示在DDoS原生防护实例为您服务期间，实例清洗过的攻击流量的峰值数据，包括宽带速率（单位：bps）和数据包转发率（单位：pps）。

业务流量趋势数据说明

该区域包含以下图表：

- **IN流量（bps）**趋势图：表示指定防护对象（IP）入方向总流量、攻击流量的宽带速率（单位：bps）变化趋势。
- **数据包（pps）**趋势图：表示指定防护对象（IP）入方向总数据包、攻击数据包的包转发率（单位：pps）变化趋势。

您可以在该区域上方设置以下查询参数：

- 防护对象：支持从下拉列表中选择**全部防护对象**、某个防护对象（IP），查询对应防护对象的数据。

  选择**全部防护对象**时，您可以在趋势图上单击某个点，查询在该时间点的流量数据中占比最大的TOP 20防护对象（IP）。
- 时间范围：支持直接单击**近30分钟**、**近1天**、**近7天**、**近30天**，或者自定义时间范围，查询对应时间范围的数据。

自定义查询时间范围时，最多允许查询最近30天内的数据。

DDoS攻击事件数据说明

攻击事件记录表记录了DDoS原生防护实例上发生的所有攻击事件。每条攻击事件记录包含以下信息：**攻击时间**、**事件**状态、**被攻击IP**、**攻击触发bps**、**攻击触发pps**、**攻击峰值bps**、**攻击峰值pps**。

攻击事件记录支持以下操作：

- **提前解除清洗**：仅适用于进行中的流量清洗事件。如果您确认当前业务流量突增与攻击无关（例如由于业务大促导致流量突增），可以通过该操作提前解除流量清洗。
- **下载抓包**：表示下载针对该攻击事件的抓包文件。您可以将获取的抓包文件作为证据，用于向网监报案。
- **查看攻击分析**：表示查看针对该攻击事件的详细攻击分析数据。关于攻击分析数据的更多介绍，请参见攻击分析。

您可以在业务流量趋势区域上方设置以下查询参数：防护对象、时间范围，从攻击事件记录表中筛选攻击事件。

攻击趋势分析数据说明

攻击趋势分析展示了DDoS原生防护实例上近一年内发生的网络攻击的整体趋势，具体包括以下图表：

- **攻击趋势（IP）**：表示DDoS原生防护实例所受攻击的次数（包括**清洗次数**、**黑洞次数**、**清洗IP数**、**黑洞IP数**）的变化趋势。
- **攻击峰值（IP）**：表示DDoS原生防护实例所受攻击的流量峰值（单位：bps）的变化趋势。
- **被攻击时长（IP）**：表示DDoS原生防护实例所受攻击的持续时长（包括**小于10分钟**、**10~30分钟**、**30~120分钟**、**2~10小时**、**大于10小时**）的变化趋势。

您可以在该区域的右上角设置查询时间范围。支持直接单击**近1周**、**近1月**、**近3月**、**近1年**，查询对应时间范围的数据。

6.攻击分析

您将云上公网IP资产添加到DDoS原生防护实例进行防护后，可以通过攻击分析页面查询资产上发生的DDoS攻击事件记录和详情，了解攻击防护的具体信息。本文介绍了使用攻击分析页面的方法。

前提条件

- 已购买DDoS原生防护企业版实例。

  相关操作，请参见购买DDoS原生防护企业版实例。

- 已将要防护的云上公网IP资产添加为DDoS原生防护企业版实例的防护对象。

  相关操作，请参见添加防护对象。

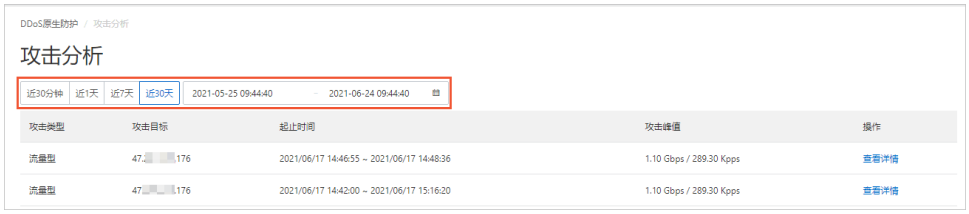
背景信息

DDoS原生防护的**攻击分析**页面向您展示流量型DDoS攻击事件的记录和详情。您可以通过**攻击分析**页面查询历史攻击事件的攻击目标、起止时间、攻击峰值等信息。**攻击分析**页面还支持查看攻击事件详情，帮助您了解攻击来源IP、攻击类型分布、攻击来源地区分布等信息，实现攻击防护流程的透明化，提升防护分析体验。

操作步骤

1. 登录流量安全产品控制台。
2. 在左侧导航栏，选择**网络安全 > DDoS原生防护 > 攻击分析**。
3. 在**攻击分析**页面，选择查询时间范围，查询相关的攻击记录。

   支持快速查询**近30分钟**、**近1天**、**近7天**、**近30天**的攻击事件，也可以自定义查询时间范围。自定义查询时间范围时，最多允许查询最近30天内的攻击事件。

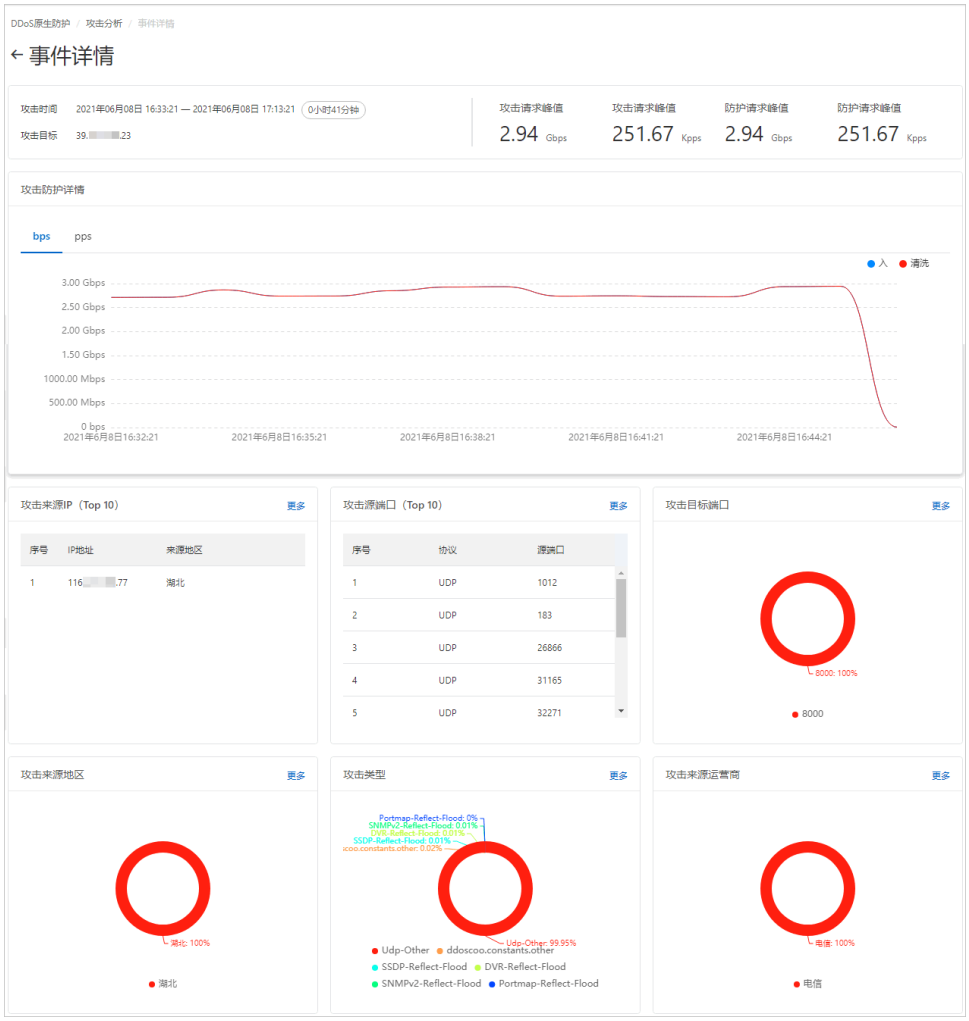
   

   攻击分析页面展示了DDoS原生防护实例保护的所有公网IP资产（包含不同地域的资产）上发生的流量型DDoS攻击事件记录。每条攻击事件记录包含以下信息：

   - **攻击类型**：目前仅支持**流量型**。
   - **攻击目标**：表示被攻击的公网IP资产。
   - **起止时间**：表示本次攻击的开始时间和结束时间。
   - **攻击峰值**：包含攻击流量的带宽峰值（单位：bps）和攻击报文的包转发率峰值（单位：pps）。

4. 查看攻击事件详情。

   您可以单击某个攻击事件记录后的**查看详情**，前往**事件详情**页面（如下图所示），查看事件详情并执行相关操作。



事件详情页面包含以下内容：

- 页面上方展示了**攻击时间**、**攻击目标**、**攻击请求峰值**和**防护请求峰值**信息。

  攻击请求峰值表示原生防护实例检测到的攻击带宽的峰值（单位：bps）和攻击报文的包转发率峰值（单位：pps），**防护请求峰值**表示经原生防护实例清洗的攻击带宽的峰值（单位：bps）和攻击报文的包转发率峰值（单位：pps）。

- **攻击防护详情**：展示了攻击期间，入方向流量和清洗流量的带宽变化趋势图（单位：bps）、入方向报文和清洗报文的包转发率变化趋势图（单位：pps）。
- **攻击来源IP（Top 10）**：展示了请求来源IP地址列表和对应的来源地区。列表显示Top 10请求来源IP，单击**更多**可以查看Top 100请求来源IP的信息。

  > **说明** 该数据包含攻击请求和正常业务请求。

- **攻击源端口（Top 10）**：展示了请求来源端口及对应的协议列表。列表显示Top 10源端口，单击**更多**可以查看Top 100源端口的信息。

  > **说明** 该数据包含攻击请求和正常业务请求。

- **攻击目标端口**：展示了请求目标端口的分布图，单击**更多**可以查看不同目标端口的请求占比数据。

> **说明** 该数据包含攻击请求和正常业务请求。

- **攻击来源地区**：展示了攻击流量的来源地区分布图，单击**更多**可以查看不同来源地区的请求占比数据。
- **攻击类型**：展示了攻击流量的类型分布图，单击**更多**可以查看不同攻击类型的请求占比数据。
- **攻击来源运营商**：展示了攻击流量的来源运营商分布图，单击**更多**可以查看不同运营商的请求占比数据。

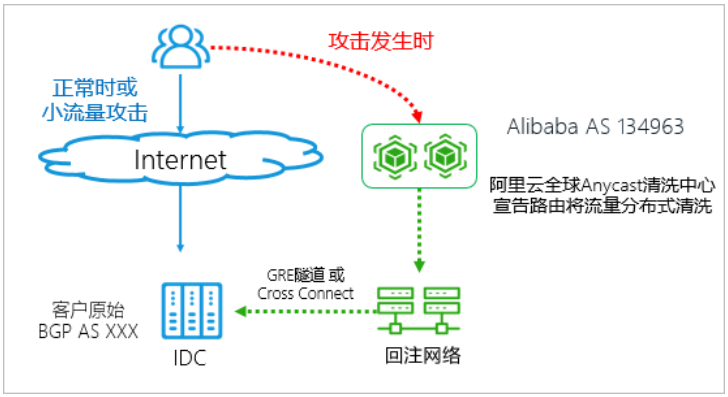
7.IDC代播防护

7.1. 开启云下IDC代播防护

购买DDoS原生防护代播实例后，您可以在云下IDC（Internet Data Center）服务器遇到DDoS攻击时手动开启代播防护，将业务流量重定向到阿里云全球Anycast清洗中心进行异常流量清洗。攻击结束后您可以手动关闭代播防护，保障业务无额外延迟。本文介绍了如何为云外IDC服务器开启及关闭代播防护。

应用场景

代播防护适用于为海外及港澳台区域的云外IDC服务器提供阿里云的DDoS防护，防护过程不需要改变原有业务IP地址和网络架构。下图描述了DDoS原生防护代播模式的防护架构。



前提条件

您已经购买了DDoS原生防护代播实例。

> **说明** 代播实例可以防护海外和港澳台区域的云下IDC服务器，目前仅支持联系销售人员购买。

操作步骤

1. 登录流量安全产品控制台。
2. 在左侧导航栏，单击**资产中心**。
3. 在顶部菜单栏左上角处，选择资产所在地域。
4. 在**资产中心**页面，单击**其他**页签。

   其他列表罗列了您已经购买的当前地域下DDoS原生防护代播实例的IP地址。如果您没有购买过代播实例或者代播实例不在当前地域，则**其他**列表为空。
5. 定位到要操作的代播实例，单击操作列下的**开启牵引**，并在弹出的对话框中单击**确认**。
   成功开启代播防护后，代播实例的**状态**变更为**牵引防护中**，表示被防护资产的流量已经获得DDoS防护。

   如果您希望停止防护，则可以单击**暂停牵引**。

   > **说明** 暂停牵引后，代播实例将不再为被防护资产的流量提供DDoS防护服务。

相关操作

代播防护也支持自动启动模式，可以根据IDC服务器的NetFlow信息和您设置的规则，自动开启或关闭代播防护。开启自动启动模式的具体操作，请参见开启自动启动模式。

相关API

- ModifyOnDemaondDefenseStatus

7.2. 开启自动启动模式

购买DDoS原生防护代播实例后，您可以设置代播防护的启动模式。默认情况下，您需要在IDC服务器遇到DDoS攻击时手动开启代播防护；您也可以开启自动启动模式，当从互联网访问IDC的网络带宽或者报文数量连续多次超过阈值时，自动开启代播防护。

前提条件

- 已经购买了DDoS原生防护代播实例。

  > **说明** 代播实例可以防护海外和港澳台区域的云下IDC服务器，目前仅支持联系销售人员购买。

- 如果您要防护非阿里云资产（例如，云下IDC服务器），在开启自动启动模式前，您必须先向阿里云转发服务器的NetFlow信息。关于具体的配置方法，请提交工单进行咨询。

操作步骤

1. 登录流量安全产品控制台。
2. 在左侧导航栏，单击**资产中心**。
3. 在顶部菜单栏左上角处，选择资产所在地域。
4. 在**资产中心**页面，单击**其他**页签。

   其他列表罗列了您已经购买的当前地域下DDoS原生防护代播实例的IP地址。如果您没有购买过代播实例或者代播实例不在当前地域，则**其他**列表为空。
5. 定位到要操作的代播实例，选择**操作**列下的**更多 > 设置自动启动**。
6. 在**启动设置模式**页面，完成以下配置。

参数	说明
启动模式	代播防护的启动模式。可选值： ○ **手动开启**（默认）：您需要在IDC服务器遇到DDoS攻击时，手动开启代播防护，并在攻击结束后，手动关闭代播防护。 选择该模式后，您无需配置其他参数。 ○ **自动（NetFlow）模式**：如果从互联网访问IDC的网络带宽或者报文数量连续多次超过您设置的阈值，将自动开启代播防护。 选择该模式后，您还需要配置代播防护的自动启动规则和停止方式等参数。 **注意** 开启**自动（NetFlow）模式**前，请确保您已经向阿里云转发服务器的NetFlow信息。
Bps阈值	入方向带宽阈值。单位：Mbps。最小值：100。
pps阈值	入方向报文数阈值。单位：Kpps。最小值：10。
连续	从互联网访问IDC的网络带宽或者报文数量连续超过阈值多少次时，将自动开启代播防护。
停止方式	代播防护开启后，停止代播防护的方式。可选值： ○ **手动停止**（默认）：您需要在攻击停止后，手动停止代播防护。 ○ **自动停止**：攻击停止后，自动在您指定的时间停止代播防护。 选择该方式后，您还需要配置以下参数： ■ **时区**：选择您的IDC服务器所在的时区。使用格林威治时间表示，格式：`GMT-hh:mm`。例如，`GMT-08:00`表示东八区。 ■ **自动停止时间**：自动停止代播防护的时间。使用24小时制表示，格式：`hh:mm`。 建议您将该时间设置为业务低峰期。当阿里云DDoS防护检测到攻击停止后，会在您设置的时间自动停止代播防护。

7. 单击**确定**。
   成功开启自动启动模式后，如果从互联网访问IDC的网络带宽或者报文数量连续多次超过您设置的阈值，将会自动开启代播防护。您可以在**资产中心**页面的**其他**页签下查看代播实例的防护状态。更多信息，请参见开启代播防护。

相关API

- SetInstanceModeOnDemand：设置代播实例的调度模式。
- CreateSchedruleOnDemand：为代播实例创建一条调度规则。
- QuerySchedruleOnDemand：查询代播实例的调度规则。
- ConfigSchedruleOnDemand：修改代播实例的调度规则。
- DeleteSchedruleOnDemand：删除代播实例的调度规则。

8.清洗设置

8.1. 设置流量清洗阈值

当您的公网IP资产的业务流量超过正常流量基线时，DDoS防护会对攻击流量进行清洗，并尽可能保障您的业务可用。本文介绍了设置流量清洗阈值的方法。

背景信息

DDoS原生防护在清洗判定中采用了AI智能分析的方法。您可以根据正常业务流量基线，设置一个清洗阈值；DDoS原生防护能够基于阿里云的大数据能力，自学习您的业务流量基线，并结合算法识别异常攻击。

只有当AI智能分析检测到DDoS攻击且请求流量达到您设置的清洗阈值时，DDoS防护才会触发流量清洗，避免了使用固定阈值可能导致的误清洗（例如，正常业务上涨波动超出固定清洗阈值，引起误清洗）。

操作步骤

1. 登录流量安全产品控制台。
2. 在左侧导航栏，单击**资产中心**。
3. 在顶部菜单栏左上角处，选择资产所在地域。
4. 单击需要操作的云产品页面，例如ECS。

   > **说明** **其他**页签目前适用于原生防护的代播防护设置，不支持清洗设置。关于代播防护的更多信息，请参见开启云下IDC代播防护。

5. 在IP资产列表中，单击要操作的IP。
6. 在**实例详情**页面，单击**清洗设置**。
7. 在**清洗设置**面板，为当前目标实例设置**清洗阈值**并单击**确定**。

   支持以下方式：

   - **系统默认**：DDoS原生防护服务根据云服务器的流量负载自动调整清洗阈值。
   - **手动设置**：由您设置**流量**和**报文数量**的清洗阈值。

     > **说明** 当DDoS检测到攻击时，如果流量或者报文数量其中之一达到阈值，就会触发流量清洗。

     清洗阈值手动设置建议：

     - 清洗阈值需要略高于实际访问值。阈值如果设置过高，起不到防御效果；如果设置过低，DDoS原生防护触发流量清洗可能会影响正常的访问。
     - 如果清洗影响了正常的请求，请适当调高清洗阈值。
     - 网站进行推广或促销活动时，建议您适当调高清洗阈值。

8.2. 取消流量清洗

当服务器遭受流量攻击时，监控系统自动检测到攻击，并为服务器清洗异常流量。对于处于异常状态（清洗中）的公网IP资产，您可以手动取消流量清洗。本文介绍了手动取消流量清洗的方法。

背景信息

清洗是指对进入服务器的数据流量进行实时监控，及时发现包括DDoS攻击在内的异常流量。在不影响正常业务的前提下，清洗掉异常流量，将可疑流量从原始网络路径中重定向到净化产品上进行恶意流量的识别和剥离，还原出的合法流量回注到原网络中转发给目标系统。

> **说明** 阿里云账号一天之内只能手动取消流量清洗三次。

操作步骤

1. 登录流量安全产品控制台。
2. 在左侧导航栏，单击**资产中心**。
3. 在顶部菜单栏左上角处，选择资产所在地域。
4. 单击需要操作的云产品页面，例如ECS。

   > **说明** **其他**页签目前适用于原生防护的代播防护设置，不支持清洗设置。关于代播防护的更多信息，请参见开启云下IDC代播防护。

5. 在IP资产列表中，单击要操作的IP（**状态**为**清洗中**）。
6. 在**实例详情**页，找到进行中的清洗事件（**事件**为**清洗**且**结束时间**为空），单击其操作列下的**取消清洗**。

   > **说明** 如果当前没有进行中的清洗事件，则**取消清洗**操作不会出现。

后续步骤

取消流量清洗后，建议您根据当前业务需要（例如活动或大促期间业务访问量增大）适当调高清洗阈值，避免再次触发流量清洗。更多信息，请参见设置流量清洗阈值。

> **说明** 最大清洗阈值和云产品实例的规格绑定。如果可配置的最大清洗阈值无法满足您的需求，建议您升级云产品规格。

8.3. 云产品规格与清洗阈值

阿里云免费为您提供基础DDoS防护能力，帮助您缓解面向公网开放的云产品所遭受的DDoS攻击。当云产品公网IP的网络流量超过设置的清洗阈值时，DDoS基础防护服务将自动对该IP的流量进行清洗，尽可能地保障您的正常业务免受DDoS攻击影响。

关于流量清洗的详细说明，请参见流量清洗、黑洞与阈值。

其中，各云产品所支持设置的最大清洗阈值取决于各云产品实例的规格。在您创建或变更云服务器ECS、负载均衡SLB、NAT网关实例时，系统将自动计算当前实例规格所对应的最大清洗阈值。

> **说明** 各云产品实例的实际黑洞阈值将综合最大清洗阈值、安全信誉等因素进行计算。

- 关于云服务器ECS实例的最大清洗阈值的具体计算方式，请参见云服务器ECS DDoS基础防护。
- 关于负载均衡SLB实例的最大清洗阈值的具体计算方式，请参见负载均衡SLB DDoS基础防护。
- 关于NAT网关实例的最大清洗阈值的具体计算方式，请参见NAT网关 DDoS基础防护。

> **说明** 弹性公网IP（EIP）的最大清洗阈值的计算方式与NAT网关相同。

8.4. 云服务器压力测试指引

DDoS原生防护基础版（DDoS基础防护）服务免费为云服务器提供DDoS攻击防御能力。默认情况下，当云服务器的网络带宽超过180 Mbps、每秒30,000个报文数、每秒480个HTTP请求中的任何一项（根据实际实例规格可能有所不同）阿里云将自动启动DDoS防御服务对流量进行清洗。

因此，您在对云服务器进行压力测试前，需要在DDoS防护产品管理控制台调整目标云服务器实例的DDoS防护阈值。具体操作请参见设置流量清洗阈值。

> **说明** 强烈建议您每分钟的压力测试增长速度不要超过100倍，否则仍可能触发流量清洗。

9.实例管理

9.1. 添加防护对象

开通DDoS原生防护企业版实例后，您只需将要防护的公网IP资产添加为DDoS原生防护的防护对象，即可为云资源开启DDoS原生防护。本文介绍了为实例添加防护对象的方法。

前提条件

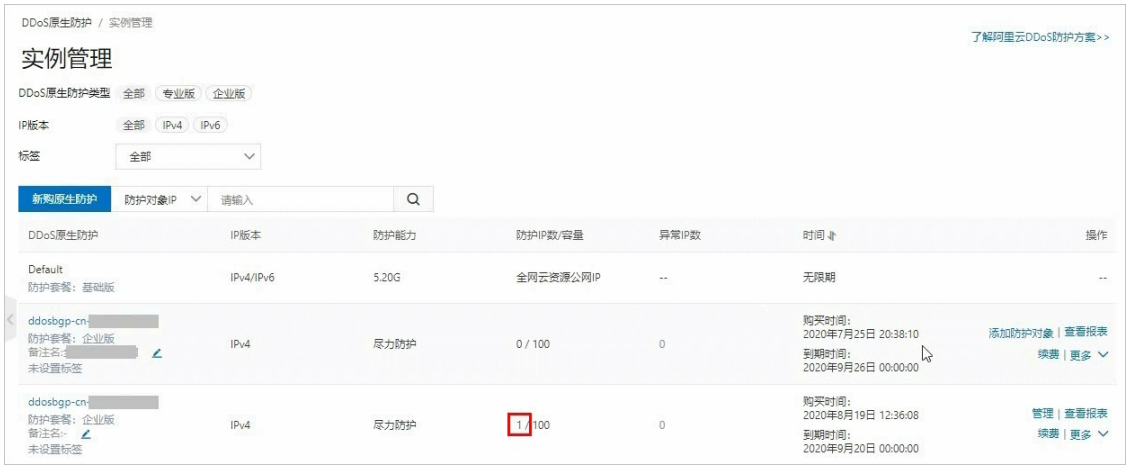
已开通DDoS原生防护企业版实例。更多信息，请参见购买DDoS原生防护企业版实例。

> **说明** DDoS原生防护企业版实例的地域必须与要添加的防护对象的地域一致。

操作步骤

1. 登录流量安全产品控制台。
2. 在左侧导航栏，选择**网络安全 > DDoS原生防护 > 实例管理**。
3. 在顶部菜单栏左上角处，选择实例所在资源组和地域。
4. 在**实例管理**页面，找到目标原生防护企业版实例，单击**操作**列下的**添加防护对象**。

   > **说明** 只有在当前实例未添加任何防护IP时，操作列才会出现**添加防护对象**。如果当前实例下已添加过防护IP，您可以单击实例**操作**列下的**管理**，并在**实例详情**页面单击**添加防护对象**。



5. 如果您是第一次使用DDoS原生防护实例，请根据页面提示完成云产品授权，授权DDoS原生防护实例访问您的其他云产品。
6. 在**添加防护对象**对话框，输入您需要防护的云产品的IP，并单击**确认**。

   > **说明**
   > - 输入的IP地址必须和原生防护企业版实例在相同地域，且必须为当前阿里云账号保有的云资源的IP地址。
   > - 多个IP间以英文逗号（,）分隔。

   完成防护配置后，DDoS原生防护实例将直接为已添加的防护对象IP提供DDoS防护能力。

相关操作

- 查看安全报表
- 解除黑洞
- 添加防护IP时，企业版实例的防护IP容量已占满该怎么办？
- 添加防护IP时收到“IP不属于你”的错误提示该怎么办？

9.2. 查看安全报表

为DDoS原生防护实例配置完防护IP后，您可以查看原生防护实例的总流量信息、单个IP的流量信息和DDoS攻击事件记录。

操作步骤

1. 登录流量安全产品控制台。
2. 在左侧导航栏，选择**网络安全 > DDoS原生防护 > 实例管理**。
3. 在顶部菜单栏左上角处，选择实例所在资源组和地域。
4. 在**实例管理**页面，定位到要操作的原生防护实例，单击其**操作**列下的**查看监控**，跳转至**业务监控**页面。
5. 在**业务监控**页面，选择要查询的防护对象和时间范围，查看防护对象的网络流量趋势（入方向流量和接收的数据包数）及DDoS攻击事件记录。

> **说明** 支持查询近30天的数据。

9.3. 查看操作日志

DDoS原生防护为您提供您实例的操作日志，便于您追溯原生防护实例的配置变更情况。

操作步骤

1. 登录流量安全产品控制台。
2. 在左侧导航栏，选择**网络安全 > DDoS原生防护 > 实例管理**。
3. 在顶部菜单栏左上角处，选择实例所在资源组和地域。
4. 在**实例管理**页面，定位到要操作的原生防护实例，单击其**操作**列下的**操作日志**。
5. 在**操作日志**页签下，查询该实例的配置变更日志。

   您可以设置要查询的时间范围，查看指定时间范围内，该DDoS原生防护实例的操作日志，包括操作时间、操作日志详情。

> **说明** 支持查看最近30天内的操作日志。

9.4. 升级实例规格

如果您购买的DDoS原生防护企业版实例的规格（例如业务带宽和防护IP数量）不能满足实际业务需要，您可以升级当前实例的规格。本文介绍了升级DDoS原生防护企业版实例规格的具体操作。

前提条件

已开通DDoS原生防护企业版实例。更多信息，请参见购买DDoS原生防护企业版实例。

背景信息

通过升级实例规格，您可以提升DDoS原生防护企业版实例的**业务规模**、**保护IP数量**。关于规格参数的详细说明，请参见DDoS原生防护企业版实例参数描述。

> **说明** DDoS原生防护基础版（DDoS基础防护）实例不支持升级实例规格的操作。如果您使用的是原生防护基础版，并且基础版默认提供的5 Gbps防护带宽无法满足您的需求，您可以开通DDoS原生防护企业版实例。更多信息，请参见购买DDoS原生防护企业版实例。

操作步骤

1. 登录DDoS防护产品控制台。
2. 在左侧导航栏，单击**DDoS原生防护 > 实例管理**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**实例管理**页面，定位到要操作的实例，选择**操作**列下的**更多 > 升配**。
5. 在**变配**面板，根据需要调整当前实例的规格。
6. 选中**服务协议**并单击**立即购买**。
7. 完成支付。

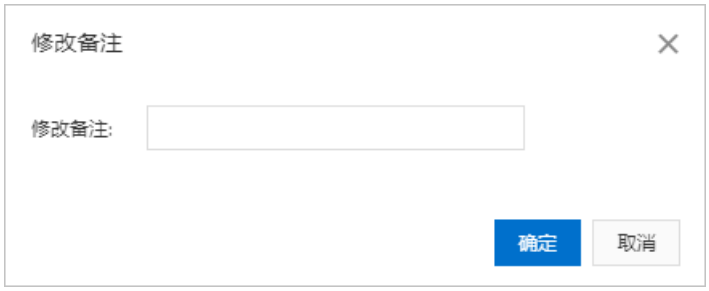
9.5. 设置实例的备注名称

DDoS原生防护（防护包）实例支持设置备注名称。当拥有多个DDoS原生防护实例时，您可以根据原生防护实例的使用对象、场景、范围等设置备注名称，用于区分不同用途的原生防护实例，并可通过备注名称快速辨识和管理您的原生防护实例。

操作步骤

1. 登录流量安全产品控制台。
2. 在左侧导航栏，选择**网络安全 > DDoS原生防护 > 实例管理**。
3. 在顶部菜单栏左上角处，选择实例所在资源组和地域。
4. 在**实例管理**页面，定位到要操作的实例，单击**备注名**后的编辑图标。

5. 在**修改备注**对话框，输入原生防护实例的备注名称，并单击**确认**。



执行结果

设置成功后，备注名称将显示在DDoS原生防护实例ID下方。您也可以按照上述步骤随时修改DDoS原生防护实例的备注名称，根据业务需要灵活地调整备注名称。

10.防护配置（公测）

10.1. 近源压制

云资产IP添加原生防护后，您可以通过开启近源压制，直接丢弃跨境业务流量，提升DDoS防护效果。该功能适用于业务本身不存在跨境流量的场景。

前提条件

- 已购买原生防护企业版实例。

  更多信息，请参见购买DDoS原生防护企业版实例。

  > **说明** 目前防护配置功能在免费公测，已购买原生防护企业版实例的用户可以提交工单申请开通防护配置功能。

- 云资产IP已经添加原生防护。

  更多信息，请参见添加防护对象。

背景信息

近源压制指对中国内地、海外及港澳台之间的跨境流量实行主动封禁，在指定的封禁时长内直接丢弃所有跨境业务流量。

- 跨境流量：
  - 如果云资产的地域是中国内地，开启近源压制将封禁所有来自海外及港澳台地区的流量。
  - 如果云资产的地域是海外及港澳台，开启近源压制将封禁所有来自中国内地的流量。
- 封禁时长：支持设置为30分钟~1天。
- 使用限制：每个DDoS原生防护实例每月默认拥有10次触发流量封禁的额度。

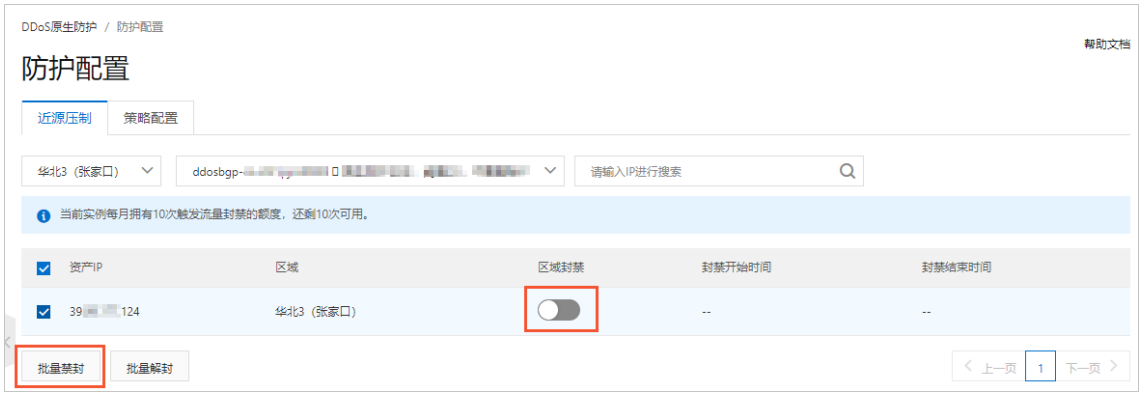
  如果当月额度已经用完，您可以提交工单联系售后支持。

近源压制生效期间支持随时手动解除。

开启近源压制

1. 登录流量安全产品控制台。
2. 在左侧导航栏，选择**网络安全 > DDoS原生防护 > 防护配置**。
3. 在**近源压制**页签下，选择DDoS原生防护实例所在地域和要操作的实例。
4. 在当前实例的防护对象列表中，定位到要操作的资产IP，开启近源压制。

   支持以下两种开启方式：
   - 为一个资产IP单独开启近源压制：开启资产IP对应的**区域封禁**开关。
   - 为多个资产IP批量开启近源压制：选中要操作的资产IP，单击**批量禁封**。



5. 在**设置封禁时长**对话框，设置流量封禁的持续时长，并单击**确定**。

   可选时长范围：30分钟~1天。

   > **说明** 封禁时长设置生效后不支持修改。如果您需要修改封禁时长，必须先解除已生效的近源压制再重新开启近源压制。

   完成上述设置后，资产IP的**区域封禁**状态将变更为开启，近源压制立即生效。您可以在资产列表中查看**封禁开始时间**和**封禁结束时间**。

   等待已设置的封禁时长结束后，流量封禁将自动取消，资产IP的**区域封禁**状态将变更为关闭。

手动解除近源压制

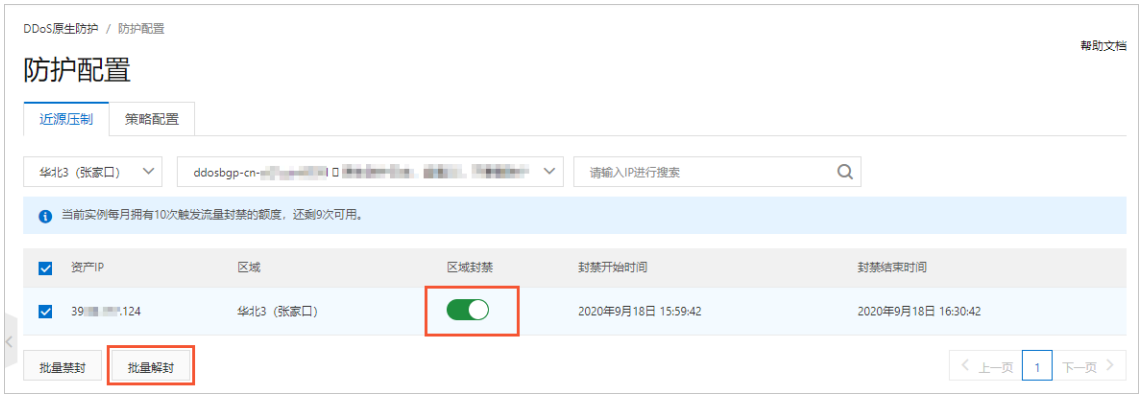
近源压制生效期间，如果您想提前结束近源压制，则可以手动解除近源压制。

> **说明** 近源压制生效期间不支持为云资产关闭原生防护，您必须先手动解除近源压制才能为云资产关闭原生防护。

1. 登录流量安全产品控制台。
2. 在左侧导航栏，选择**网络安全 > DDoS原生防护 > 防护配置**。
3. 在**近源压制**页签下，选择DDoS原生防护实例所在地域和要操作的实例。
4. 在当前实例的防护对象列表中，定位到要操作的资产IP，解除近源压制。

   支持以下两种解除方式：

   - 为一个资产IP单独解除近源压制：关闭资产IP对应的**区域封禁**开关。
   - 为多个资产IP批量解除近源压制：选中要操作的资产IP，单击**批量解封**。



5. 在**确认**对话框，单击**确认**。

完成上述设置后，资产IP的**区域封禁**状态将变更为关闭，流量封禁立即解除。

10.2. 策略配置

云资产IP添加原生防护后，您可以根据自身业务特征和需求配置防护策略，放行或丢弃包含指定特征的业务流量，提升DDoS防护效果。

前提条件

- 已创建原生防护企业版实例。相关操作，请参见购买DDoS原生防护企业版实例。

  > **说明** 目前防护配置功能在免费公测，已购买原生防护企业版实例的用户可以提交工单开通防护配置功能。

- 云资产IP已经添加原生防护。相关操作，请参见添加防护对象。

配置流程

首次使用策略配置功能时，推荐您参照以下流程进行操作：

1. 新建一个策略模板。
2. 为策略模板设置生效资产，即在哪些资产上应用当前策略模板。
3. 为策略模板配置具体的防护策略。已配置的防护策略将在上一步设置的资产上生效。

   下表描述了支持配置的防护策略。

策略名称	说明	配置方法

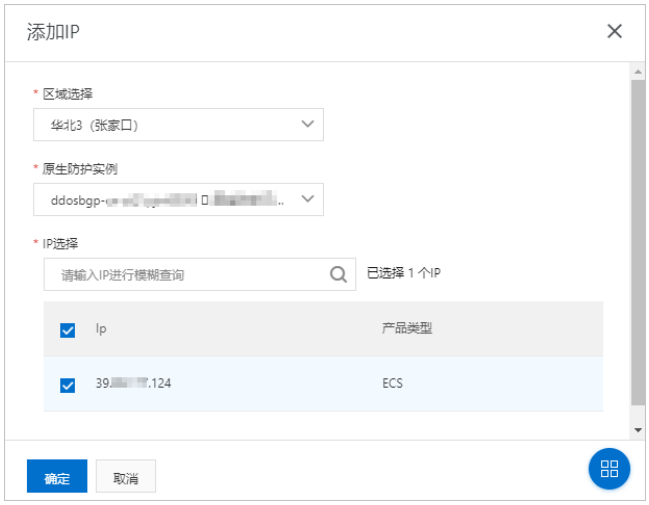
策略名称	说明	配置方法
ICMP协议禁用	在流量清洗时直接丢弃ICMP协议流量，可以过滤ICMP攻击，并减少服务器被探测的风险。	通过单击**状态**开关，开启或关闭**ICMP协议禁用**。开启该策略后，ICMP协议流量将被直接丢弃。 **说明** ICMP协议禁用对白名单中IP也会生效，即开启该策略后，来自白名单IP的ICMP协议流量也会被丢弃。 具体操作，请参见配置ICMP协议禁用策略。
源端口封禁	针对UDP或TCP协议+源或目的端口设置过滤规则，直接丢弃来自指定协议及对应端口的流量，可以用于过滤UDP反射攻击。	需要配置规则，指定要封禁的协议及对应端口。规则生效后，禁用协议+端口的请求流量将被直接丢弃。 具体操作，请参见配置源端口封禁规则。
黑白名单	针对源IP设置过滤或放行规则，直接丢弃或放行指定源IP的流量。	需要配置黑名单、白名单，分别指定黑名单IP、白名单IP。配置生效后，黑名单IP的请求流量将被直接丢弃，白名单IP的请求流量将被直接放行。 具体操作，请参见配置黑白名单。
指纹过滤	在流量清洗时，对数据包中指定位置的内容进行特征匹配，根据匹配结果设置过滤、放行或限速规则。	需要配置规则，指定要检测的数据包特征。匹配中特征的请求将触发规则对应的动作，例如通过、丢弃或限速。 具体操作，请参见配置指纹过滤特征。

操作步骤

1. 登录流量安全产品控制台。
2. 在左侧导航栏，选择**网络安全 > DDoS原生防护 > 防护配置**。
3. 单击**策略配置**页签。
4. 选择或新建一个策略模板。
   - 如果您已经创建过策略模板，在左侧**策略模板**列表单击要操作的策略模板。
   - 如果您从未创建过策略模板，参照以下步骤创建一个策略模板：
     a. 在左侧**策略模板**列表上方，单击**添加策略**。
     b. 在**添加**对话框，输入**策略名**，并单击**确定**。

     成功创建策略模板后，新建的策略模板将被默认选中。
5. 添加生效资产。
   i. 在右侧**生效资产列表**区域，单击**添加IP**。

ii. 在**添加IP**面板，选择要应用当前策略模板的资产IP。



参数	说明
区域选择	资产IP所在地域。
原生防护实例	资产IP关联的原生防护实例。
IP选择	资产IP。 **说明** 一个资产IP只允许关联一个策略模板。如果资产IP已经关联了其他策略模板，则不允许添加到当前策略模板。

iii. 单击**确定**。

成功添加生效资产后，资产IP的流量将受当前策略模板中防护策略的约束。新建的策略模板默认未开启任何防护策略，您需要进一步配置具体的防护策略，才能实现特定的防护效果。

您可以在**生效资产列表**中**移出**已有资产。

6. （可选）配置**ICMP协议禁用**策略。

您可以参照以下步骤开启、关闭**ICMP协议禁用**策略：

i. 在**ICMP协议禁用**区域，单击**状态**开关。

ii. 在**确认**对话框，单击**确定**。

7. （可选）配置**源端口封禁**规则。

您可以参照以下步骤配置源端口封禁规则：

i. 在**源端口封禁**区域，单击**设置**。

ii. 在**禁用端口**面板，单击**添加端口**。

> **说明** 最多支持添加8条端口规则。

iii. 在**新增禁用端口**面板，完成以下规则配置。

参数	说明
协议	要封禁的协议类型。可选值：**TCP**、**UDP**。
端口类型	要封禁的端口类型。可选值：**源端口**、**目的端口**。
开始端口 — 结束端口	要封禁的端口范围。可选范围：1~65535。 **说明** 同一协议下相同类型端口的范围不允许重合。
匹配后动作	匹配中协议及对应端口后，对流量执行的操作。取值固定为**丢弃**。

关于源端口封禁规则的推荐配置，请参见源端口封禁推荐配置。

iv. 单击**确定**。
成功添加端口封禁规则后，规则自动生效，禁用协议+端口的请求流量将被直接丢弃。您可以在**禁用端口**列表中管理已有规则，例如**编辑**、**删除**规则。

8. （可选）配置黑白名单。

您可以参照以下步骤配置黑白名单：

i. 在**黑白名单**区域，单击**设置**。

ii. 在**黑白名单库**面板，单击**添加黑白名单**。

iii. 在**添加黑白名单**面板，完成黑白名单配置。

最多允许添加10,000个黑名单IP和10,000个白名单IP，多个IP间需要使用空格或者换行符进行分隔。

iv. 单击**确定**。

成功添加黑白名单后，黑白名单设置自动生效，黑名单IP的请求流量将被直接丢弃，白名单IP的请求流量将被直接放行。您可以在**黑白名单库**管理已有黑名单IP、白名单IP，例如**删除**已添加的IP或者**清空黑名单**、**清空白名单**。

9. （可选）配置指纹过滤特征。

您可以参照以下步骤配置指纹过滤特征：

i. 在**指纹过滤**区域，单击**设置**。

ii. 在**指纹过滤特征**面板，单击**添加特征**。

> **说明** 最多允许添加8条指纹特征规则。

iii. 在**新增指纹过滤特征**面板，完成以下规则配置。

参数	说明
协议	协议类型。可选值：**TCP**、**UDP**。
开始源端口 — 结束源端口	源端口范围。可选范围：1~65535。
开始目的端口 — 结束目的端口	目的端口范围。可选范围：1~65535。
最小包长 — 最大包长	IP数据包的长度范围。可选范围：1~1500，单位：Byte。
偏移量	UDP或TCP头部后数据体（payload）的偏移量，可选范围：0~1500，单位：Byte。 偏移量为0时，从数据体的第一字节开始匹配。
检测载荷	要匹配的数据体（payload）内容，需要输入以0x开头的十六进制字符串。
匹配后动作	匹配中特征后，对流量执行的操作。可选值：**通过**、**丢弃**、**源IP限速**、**session限速**。 选择**源IP限速**、**session限速**后，必须设置**限速值**。**限速值**取值范围：1~100000。

iv. 单击**确定**。
成功添加指纹过滤特征后，指纹过滤自动生效，匹配中特征的请求将触发规则对应的动作。您可以在**指纹过滤特征**列表中管理已有特征，例如**编辑**、**删除**特征，或者对特征排序。

> **说明** 特征排序仅为了方便您管理现有规则，不会对规则生效有任何影响。

源端口封禁推荐配置

配置自定义源端口封禁规则时，建议您根据业务场景选择以下推荐配置，提升防护效果：

- 如果生效资产中只有TCP业务（无UDP业务），建议您封禁全部UDP源端口。
  具体的端口规则配置如下图所示。

- 如果生效资产中存在UDP业务，建议您封禁常见的UDP反射源端口，包括1~52、54~161、389、1900、11211。
  具体的端口规则配置如下图所示。

11.防护分析（公测）

11.1. 开启防护分析

DDoS原生防护支持防护分析功能，该功能目前处于公测阶段，支持免费开通使用。您可以通过防护分析功能查询和分析DDoS原生防护实例的防护日志、查看内置的防护报表。本文介绍了为原生防护实例开启防护分析的方法。

前提条件

已购买DDoS原生防护企业版实例，且实例地域属于中国内地。

更多信息，请参见购买DDoS原生防护企业版实例。

操作步骤

1. 登录流量安全产品控制台。
2. 在左侧导航栏，选择**网络安全 > DDoS原生防护 > 防护分析Beta**。
3. 在顶部菜单栏左上角处，选择实例所在资源组和地域。
4. （可选）首次使用防护分析时，您需要参照以下步骤完成RAM授权。如果您已经完成过授权，请跳过该步骤。
   i. 单击**立即授权**。

   ii. 在**云资源访问授权**页面，单击**同意授权**。

   iii. 授权成功后，返回**防护分析Beta**页面并手动刷新页面。
5. 在**防护分析Beta**页面上方，选择DDoS原生防护实例，并单击**立即升级**。

6. 在**变配**页面，选择开启**防护分析（公测）**功能。

7. 选中**服务协议**（表示您已阅读并同意协议内容），并单击**立即购买**。
8. 完成支付。

> **说明** 防护分析公测期间支持免费开通。

完成支付后，防护分析的状态默认为暂停，需要您手动开启。

9. 返回**防护分析Beta**页面，单击**立即开启**。
当前实例的防护分析状态更新为开启后，原生防护将自动采集当前实例的防护日志（存储在阿里云日志服务中），并向您提供查询分析和报表功能。您可以通过设置状态开关，开启、关闭当前实例的防护分析功能。

后续步骤

- 查询防护日志
- 查看防护报表

11.2. 查询防护日志

开启防护分析后，您可以通过防护日志查询和分析DDoS原生防护实例上的清洗、黑洞和代播牵引事件信息。

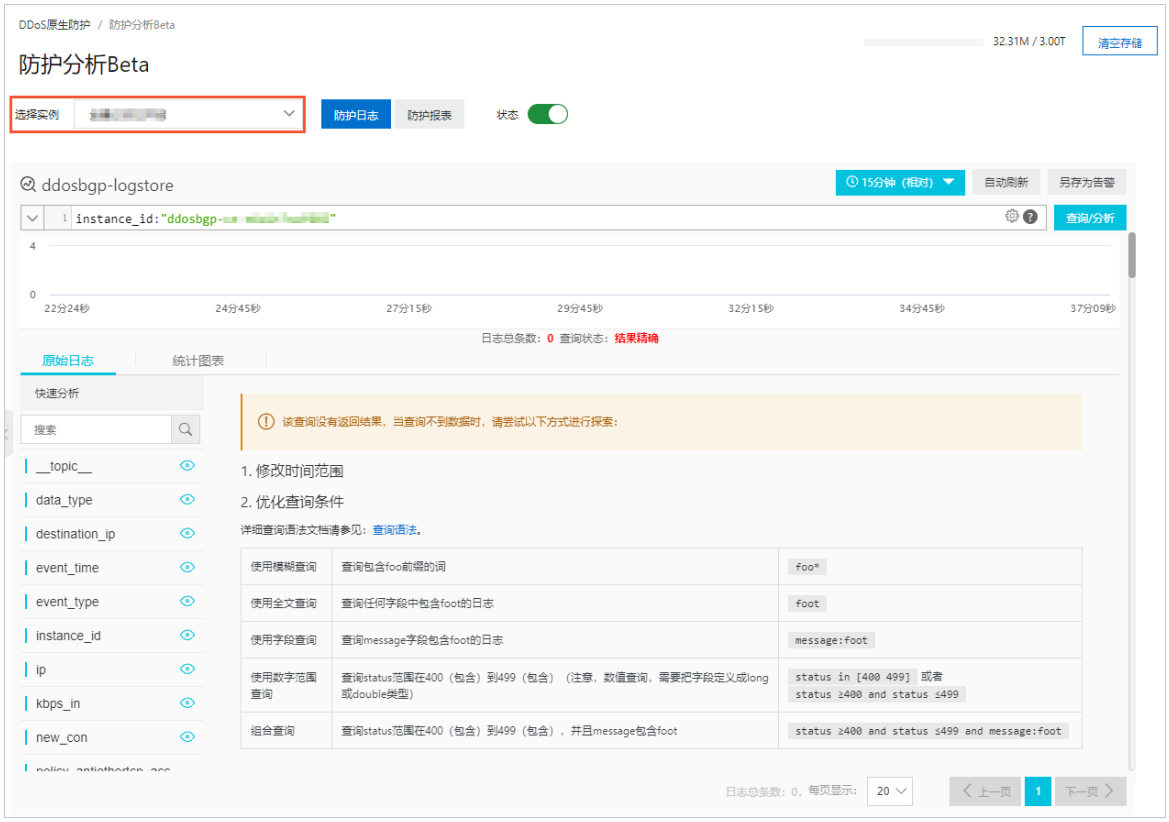
前提条件

已开启防护分析功能。更多信息，请参见开启防护分析。

查询分析日志

1. 登录流量安全产品控制台。
2. 在左侧导航栏，选择**网络安全 > DDoS原生防护 > 防护分析Beta**。
3. 在顶部菜单栏左上角处，选择实例所在资源组和地域。
4. 在**防护分析Beta**页面上方，选择DDoS原生防护实例。

> **说明** 实例的防护分析**状态**需要设置为开启，才能支持查询防护日志。关于如何开启防护分析，请参见开启防护分析。



5. 在输入框中输入查询分析语句。

   查询分析语句由查询语句和分析语句构成，格式为查询语句|分析语句，查询分析语句语法请参见查询语法、SQL分析语法。

   您还可以通过Data Explorer构建查询和分析语句。具体操作，请参见通过Data Explorer构建查询和分析语句。

6. 在页面右上角，单击**15分钟（相对）**，设置查询的时间范围。

   您可以选择相对时间、整点时间和自定义时间范围。

   > **说明** 查询结果相对于指定的时间范围来说，有1分钟以内的误差。

7. 单击**查询/分析**，查看查询分析结果。

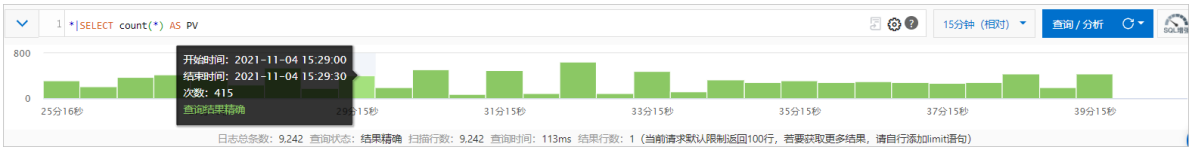
操作查询和分析结果

日志服务为您提供日志分布直方图、原始日志和统计图表形式的展示查询分析结果，并支持设置告警、快速查询等操作。

> **说明** 执行查询和分析语句后，默认只返回100条结果，您可以使用LIMIT语句控制返回结果数量。更多信息，请参见LIMIT子句。

- 日志分布直方图

日志分布直方图主要展示查询到的日志在时间上的分布。



- 鼠标指向绿色数据块时，可以查看该数据块代表的时间范围和日志命中次数。
- 单击绿色数据块，可以查看更细时间粒度的日志分布，同时在**原始日志**页签中同步展示指定时间范围内的查询结果。

- 原始日志

  在**原始日志**页签中展示当前查询结果，您可单击**表格**或**原始**查看日志并可执行如下操作。

  - 快速分析：用于快速分析某一字段在一段时间内的分布情况。更多信息，请参见快速分析。

    您还可以单击图标，选择显示Key或Key的别名，该别名可在创建索引时配置。例如host_name的别名为host，如果你选择显示别名，则在快速分析列表中显示host。

    > **说明** 当某字段没有别名时，您选择显示别名，在快速分析列表中仍显示字段名（Key）。

  - 上下文浏览：在**原始**页签中，单击目标日志中的图标，查看指定日志在原始文件中的上下文信息。更多信息，请参见上下文查询。

    > **说明** 上下文浏览功能仅支持Logtail采集到的日志数据。

  - LiveTail：在**原始**页签中，单击目标日志中的图标，实时监控日志内容，提取关键日志信息。更多信息，请参见LiveTail。

    > **说明** LiveTail功能仅支持Logtail采集到的日志数据。

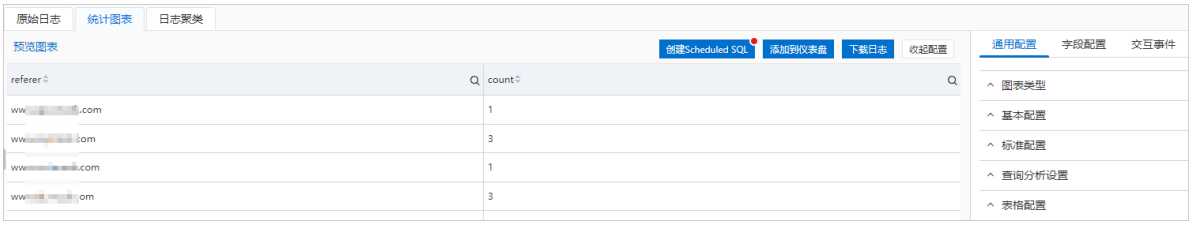
  - 设置Tag：在**原始**页签中，单击图标下的**Tag设置**，将次要的字段内容简化展示。

- 设置列：在**表格**页签中，单击图标下的**列设置**，设置表格中要展示的日志信息，其中列名称为字段名，内容为字段值。

- 设置JSON：在**表格**或**原始**页签中，单击图标下的**JSON设置**，设置JSON展开级别。
- 设置事件：在**表格**或**原始**页签中，单击图标下的**事件配置**，为原始日志设置事件。 更多信息，请参见事件配置。
- 下载日志：在**表格**或**原始**页签中，单击图标下载日志，支持选择下载范围和下载工具。更多信息，请参见下载日志。

- 统计图表

  执行查询分析语句后，您可以在**统计图表**页签中查看可视化的查询分析结果。



  - 查看查询分析结果：统计图表是日志服务根据查询与分析语句渲染出的结果。日志服务提供表格、线图、柱状图等多种图表类型。目前，统计图表包括Pro版本和普通版本。更多信息，请参见统计图表（Pro版本）概述、统计图表概述。
  - 添加图表到仪表盘：仪表盘是日志服务提供的实时数据分析大盘。单击**添加到仪表盘**，将查询分析结果以图表形式保存到仪表盘中。更多信息，请参见可视化概述。
  - 设置交互事件：交互事件是数据分析中不可缺少的功能之一，通过改变数据维度的层次、变换分析的粒度从而获取数据中更详尽的信息。更多信息，请参见交互事件。

- 日志聚类

  在**日志聚类**页签中，单击**开启日志聚类**，可实现在采集日志时将相似度高的日志聚合。更多信息，请参见日志聚类。

- 告警

  在查询分析页面上，选择**另存为告警 > 新版告警**，可为查询分析结果设置告警。更多信息，请参见快速设置日志告警。

- 快速查询

在查询分析页面上，单击**另存为快速查询**，将某一查询分析语句保存为快速查询。更多信息，请参见快速查询。

11.3. 查看防护报表

开启防护分析后，您可以通过防护报表查看DDoS原生清洗分析报表、DDoS原生防护事件报表。

前提条件

已开启防护分析。更多信息，请参见开启防护分析。

操作步骤

1. 登录流量安全产品控制台。
2. 在左侧导航栏，选择**网络安全 > DDoS原生防护 > 防护分析Beta**。
3. 在顶部菜单栏左上角处，选择实例所在资源组和地域。
4. 在**防护分析Beta**页面上方，选择DDoS原生防护实例，并单击**防护报表**。

   > **说明** 实例的防护分析**状态**需要设置为开启，才能支持查看防护报表。关于如何开启防护分析，请参见开启防护分析。

5. 在防护报表区域，选择要查看的报表类型页签：
   - **DDoS原生清洗分析报表**：展示入流量监控、入流量分布、入流量协议类型分布、包检查、SYN Cookie、源IP认证、首包丢弃、DIP限速、SIP限速、L7 Filter、L4 Filter、域名首包丢弃、域名认证、IP Domian限速、AntiTCP、AntiUDP、AntiOtherTCP等信息。
   - **DDoS原生防护事件报表**：展示DDoS事件趋势信息。
6. 在报表右上角，单击**时间选择**，设置查询的时间范围。

   您可以选择相对时间、整点时间和自定义时间范围。

   > **说明** 查询结果相对于指定的时间范围来说，有1分钟以内的误差。

7. 查看报表。

11.4. 日志字段说明

本文介绍了DDoS原生防护日志中包含的所有字段的说明。

DDoS原生防护的所有日志字段按照功能划分为以下类型：

- 事件类字段：表示与被防护资产上发生的清洗、黑洞、代播防护事件相关的字段，包含事件的时间、状态等信息。
- 流量检测类字段：表示与被防护资产上产生的流量数据相关的字段，例如，入方向流量的宽带速率、不同类型数据包的包转发率等。
- 流量清洗类字段：表示与流量清洗过程相关的字段，包含流量清洗过程中由不同防护策略丢弃、放行的流量数据。

事件类字段

名称	说明	取值示例
data_type	数据类型。取值： • Global_SC_Detection：表示从高防清洗中心流入的流量数据（代播模式中）。 • Global_SC_Mitigation：表示通过高防清洗中心清洗的流量数据（代播模式中）。 • Regional_SC_Detection：表示阿里云资产所在地域的入流量数据。 • Regional_SC_Mitigation：表示阿里云资产所在地域的清洗流量数据。 • event：表示攻击事件数据。	Regional_SC_Mitigation
event_time	事件发生时间。使用时间戳格式表示，单位：秒。	1624434027
event_type	事件类型。取值： • mitigation_begin：表示清洗事件开始。 • mitigation_ended：表示清洗事件结束。 • blackhole_begin：表示黑洞事件开始。 • blackhole_ended：表示黑洞事件结束。	mitigation_begin
instance_id	DDoS原生防护实例的ID。	ddosbgp-cn-n6w203qg****
ip	被防护的资产IP。	39.XX.XX.23
kbps_in	入方向流量宽带速率，单位：kbps。	1000
new_con	新建连接数量。	1000
pps_in	入方向数据包包转发率，单位：pps。	1000
qps	每秒查询数，单位：qps。	1000

名称	说明	取值示例
scrubbing_center	流量清洗中心所在地域。取值： • us_west：表示美国（弗吉尼亚）。 • us_east：表示美国（硅谷）。 • frankfurt：表示德国（法兰克福）。 • hk：表示中国（香港）。 • singapore：表示新加坡。 • malaysia：表示马来西亚（吉隆坡）。 • uk：表示英国（伦敦）。 • japan：表示日本（东京）。 • total_summary ：表示全部地域。 • assets_base_region：表示资产所在地域。	us_west
subnet	代播防护模式下，对应事件的网段。	1.XX.XX.1/24
user_id	阿里云账号ID。	170457416359****

流量检测类字段

名称	说明	取值示例
Ip	流量来源IP地址。	1.XX.XX.1
Time	流量检测日志的统计时间。使用时间戳格式表示，单位：秒。	1624434027
KbpsIn	在统计时间，入方向流量的宽带速率，单位：Kbps。	1000
KbpsOut	在统计时间，出方向流量的宽带速率，单位：Kbps。	1000
PpsIn	在统计时间，入方向全部数据包的包转发率，单位：pps。	1000
PpsOut	在统计时间，出方向全部数据包的包转发率，单位：pps。	1000
PpsInSyn	在统计时间，入方向SYN数据包的包转发率，单位：pps。	1000
PpsInSynack	在统计时间，入方向SYN-ACK数据包的包转发率，单位：pps。	1000
PpsInFin	在统计时间，入方向FIN、RST数据包的包转发率，单位：pps。	1000
PpsInHttpReq	在统计时间，同时满足以下特征的入方向TCP数据包的包转发率（单位：pps）： • 不是SYN、SYN-ACK、FIN、RST数据包。 • 目的端口为：80、3128、8080、8088。 • 包含payload，且http_payload的前4个字节为：GET 、PUT 、HEAD、POST 。	1000

名称	说明	取值示例
PpsInHttpResp	在统计时间，同时满足以下特征的入方向TCP数据包的包转发率（单位：pps）： • 不是SYN、SYN-ACK、FIN、RST数据包。 • 目的端口为：80、3128、8080、8088。 • 包含payload，且http_payload的前4个字节为：HTTP。	1000
PpsInHttpFlags	在统计时间，入方向的TCP ACK数据包（即不是SYN、SYN-ACK、FIN、RST数据包）的包转发率，单位：pps。	1000
PpsInIcmp	在统计时间，入方向ICMP数据包的包转发率，单位：pps。	1000
PpsInDns	在统计时间，入方向DNS数据包（使用UDP协议，且源或目的端口为53）的包转发率，单位：pps。	1000
PpsInUdprisk	在统计时间，命中高危UDP源端口的数据包的包转发率，单位：pps。	1000
PpsInUdpunknown	在统计时间，除PpsInDns外的入方向UDP数据包（使用UDP协议，且源或目的端口不是53）的包转发率，单位：pps。	1000

流量清洗类字段

名称	说明	取值示例
instance_id	DDoS原生防护实例的ID。	ddosbgp-cn-v641is26****
time	流量清洗记录的统计时间。使用时间戳格式表示，单位：秒。	1624434027
destination_ip	目的IP。	123.XX.XX.169
port	目的端口。取值： • all（默认）：表示全部端口的数据。 • 具体端口：表示针对某个具体端口（例如80）的数据。	80
total_traffic_in_bps	进入清洗过程的所有类型数据包的总字节数，单位：Bps（Byte per second）。	8000
total_traffic_drop_bps	经流量清洗过程丢弃的所有类型数据包的总字节数，单位：Bps（Byte per second）。	800
total_traffic_in_pps	入方向所有类型数据包的包转发率，单位：pps。	1000
total_traffic_drop_pps	被丢弃的所有类型数据包的包转发率，单位：pps。	1000
pps_types_in_tcp_pps	入方向TCP数据包的包转发率，单位：pps。	100

名称	说明	取值示例
pps_types_in_udp_pps	入方向UDP数据包的包转发率，单位：pps。	1000
pps_types_in_icmp_pps	入方向ICMP数据包的包转发率，单位：pps。	1000
pps_types_in_syn_pps	入方向SYN数据包的包转发率，单位：pps。	1000
pps_types_in_ack_pps	入方向ACK数据包的包转发率，单位：pps。	1000
pps_types_in_synack_pps	入方向SYN-ACK数据包的包转发率，单位：pps。	1000
pps_types_in_finrst_pps	入方向FIN、RST数据包的包转发率，单位：pps。	1000
pps_types_in_dns_pps	入方向DNS数据包的包转发率，单位：pps。	1000
pps_types_drop_tcp_pps	被丢弃的TCP数据包的包转发率，单位：pps。	1000
pps_types_drop_udp_pps	被丢弃的UDP数据包的包转发率，单位：pps。	1000
pps_types_drop_icmp_pps	被丢弃的ICMP数据包的包转发率，单位：pps。	1100
pps_types_drop_syn_pps	被丢弃的SYN数据包的包转发率，单位：pps。	1000
pps_types_drop_ack_pps	被丢弃的ACK数据包的包转发率，单位：pps。	1000
pps_types_drop_synack_pps	被丢弃的SYN-ACK数据包的包转发率，单位：pps。	1000
pps_types_finrst	被丢弃的FIN-RST数据包的包转发率，单位：pps。	1000
pps_types_dns	被丢弃的DNS数据包的包转发率，单位：pps。	1000
policy_packet_checking_acct_pps	由包检查策略（默认）放行的数据包的包转发率，单位：pps。	1000
policy_packet_checking_drop_pps	由包检查策略（默认）丢弃的数据包的包转发率，单位：pps。	1000
policy_dns_retransmission_authentication_drop_pps	由域名首包丢弃策略（默认）丢弃的数据包的包转发率，单位：pps。	1000

名称	说明	取值示例
policy_dns_retransmission_authentication_acct_pps	由域名首包丢弃策略（默认）放行的数据包的包转发率，单位：pps。	100
policy_source_ip_authentication_succeed_pps	由源IP认证策略（默认）检查成功的数据包的包转发率，单位：pps。	1000
policy_source_ip_authentication_checked_pps	由源IP认证策略（默认）正在检查的数据包的包转发率，单位：pps。	1000
policy_source_ip_authentication_acct_pps	由源IP认证策略（默认）放行的数据包的包转发率，单位：pps。	1000
policy_source_ip_authentication_drop_pps	由源IP认证策略（默认）丢弃的数据包的包转发率，单位：pps。	1000
policy_source_ip_rate_limitation_drop_syn_pps	由源IP限速策略（默认）丢弃的SYN数据包的包转发率，单位：pps。	1000
policy_source_ip_rate_limitation_drop_con_max_pps	超过源IP并发连接限速策略（默认）规定的最大连接数而被丢弃的数据包的包转发率，单位：pps。	1000
policy_source_ip_rate_limitation_drop_con_rate_pps	超过源IP并发连接限速策略（默认）规定的连接速率而被丢弃的数据包的包转发率，单位：pps。	1000
policy_source_ip_rate_limitation_drop_udp_rate_pps	由源IP UDP限速策略（默认）丢弃的数据包的包转发率，单位：pps。	1000
policy_source_ip_rate_limitation_drop_tcpack_rate_pps	由源IP ACK限速策略（默认）丢弃的数据包的包转发率，单位：pps。	1000
policy_source_ip_rate_limitation_drop_tcpsynack_rate_pps	由源IP SYN-ACK限速策略（默认）丢弃的数据包的包转发率，单位：pps。	1000
policy_destination_ip_rate_limitation_drop_syn_rate	由目的IP限速策略（默认）丢弃的SYN数据包的包转发率，单位：pps。	1000
policy_destination_ip_rate_limitation_drop_udp_rate	由目的IP限速策略（默认）丢弃的UDP数据包的宽带速率，单位：pps。	1000

名称	说明	取值示例
policy_destination_ip_rate_limitation_drop_ack_rate	由目的IP限速策略（默认）丢弃的ACK数据包的宽带速率，单位：pps。	1000
policy_destination_ip_rate_limitation_drop_icmp_rate	由目的IP限速策略（默认）丢弃的ICMP数据包的宽带速率，单位：pps。	1000
policy_destination_ip_rate_limitation_drop_other_rate	由目的IP限速策略（默认）丢弃的其他类型（除UDP、ICMP、TCP-SYN、TCP-SYN-ACK、TCP-ACK外）数据包的包转发率，单位：pps。	1000
policy_destination_ip_rate_limitation_drop_synack_rate	由目的IP限速策略（默认）丢弃的SYN-ACK数据包的包转发率，单位：pps。	1000
policy_layer_4_filter_l4_filiter_drop_pps	由全部指纹过滤策略（在防护配置中自定义）丢弃的数据包的包转发率，单位：pps。	1000
policy_layer_4_filter_l4_filiter_acct_num	通过指纹过滤策略模块（在防护配置中自定义）放行的数据包的包转发率，单位：pps。	1000
policy_layer_4_filter_l4_filite_drop_rule_1_pps	由排序为1的指纹过滤策略（在防护配置中自定义）丢弃的数据包的包转发率，单位：pps。	1000
policy_layer_4_filter_l4_filite_drop_rule_2_pps	由排序为2的指纹过滤策略（在防护配置中自定义）丢弃的数据包的包转发率，单位：pps。	1000
policy_layer_4_filter_l4_filite_drop_rule_3_pps	由排序为3的指纹过滤策略（在防护配置中自定义）丢弃的数据包的包转发率，单位：pps。	1000
policy_layer_4_filter_l4_filite_drop_rule_4_pps	由排序为4的指纹过滤策略（在防护配置中自定义）丢弃的数据包的包转发率，单位：pps。	1000
policy_layer_4_filter_l4_filite_drop_rule_5_pps	由排序为5的指纹过滤策略（在防护配置中自定义）丢弃的数据包的包转发率，单位：pps。	1000
policy_layer_4_filter_l4_filite_drop_rule_6_pps	由排序为6的指纹过滤策略（在防护配置中自定义）丢弃的数据包的包转发率，单位：pps。	1000
policy_layer_4_filter_l4_filite_drop_rule_7_pps	由排序为7的指纹过滤策略（在防护配置中自定义）丢弃的数据包的包转发率，单位：pps。	1000

名称	说明	取值示例
policy_layer_4_filter_l4_filite_drop_rule_8_pps	由排序为8的指纹过滤策略（在防护配置中自定义）丢弃的数据包的包转发率，单位：pps。	1000
policy_dns_domain_authentication_succ_domain_pps	由域名认证策略（默认）检查成功的数据包的包转发率，单位：pps。	1000
policy_dns_domain_authentication_fail_domain_pps	由域名认证策略（默认）检查失败的数据包的包转发率，单位：pps。	1000
policy_dns_domain_authentication_drop_pps	由域名认证策略（默认）丢弃的全部数据包的包转发率，单位：pps。	1000
policy_dns_domain_authentication_acct_pps	由域名认证策略（默认）放行的全部数据包的包转发率，单位：pps。	1000
policy_syn_cookie_succ_check_pps	由SYN Cookie策略（默认）检查成功的数据包的包转发率，单位：pps。	1000
policy_syn_cookie_fail_check_pps	由SYN Cookie策略（默认）检查失败的数据包的包转发率，单位：pps。	1000
policy_syn_cookie_drop_pps	由SYN Cookie策略（默认）丢弃的数据包的包转发率，单位：pps。	1000
policy_syn_cookie_rebound_check_pps	由SYN Cookie策略（默认）进行反弹验证的数据包的包转发率，单位：pps。	1000
policy_syn_cookie_acct_pps	由SYN Cookie策略（默认）放行的数据包的包转发率，单位：pps。	1000
policy_udp_defense_drop_pps	由UDP防护策略（默认）丢弃的数据包的包转发率，单位：pps。	1000
policy_antiothertcp_drop_pps	由其他TCP防护策略（默认）丢弃的数据包的包转发率，单位：pps。	1000
policy_antiothertcp_acct_pps	由其他TCP防护策略（默认）放行的数据包的包转发率，单位：pps。	1000
policy_antitcp_drop_tcp_pps	由TCP防护策略（默认）丢弃的全部TCP数据包的包转发率，单位：pps。	1000
policy_antitcp_drop_ack_pps	由TCP防护策略（默认）丢弃的ACK数据包的包转发率，单位：pps。	1000

名称	说明	取值示例
policy_retransmission_authentication_acct_pps	由首包丢弃策略（默认）放行的数据包的包转发率，单位：pps。	1000
policy_retransmission_authentication_drop_pps	由首包丢弃策略（默认）丢弃的数据包的包转发率，单位：pps。	1000

12.黑洞策略

12.1. 查看黑洞时长

服务器遭受DDoS攻击触发黑洞后，其公网IP在一定时间内将无法被访问，只有等到黑洞时长过后才会恢复正常访问。不同地域资产的默认黑洞时长不同，且黑洞时长与资产遭受的攻击情况有关。您可以在DDoS防护控制台查看资产的黑洞时长。

背景信息

关于阿里云黑洞策略的详细介绍，请参见阿里云黑洞策略。

操作步骤

1. 登录流量安全产品控制台。
2. 在左侧导航栏，单击**资产中心**。
3. 在顶部菜单栏左上角处，选择资产所在地域。
4. 在**资产中心**页面上方，查看**DDoS攻击防护说明**。

   DDoS攻击防护说明中的**当前解除黑洞时间**表示当前地域下资产的黑洞时长。

12.2. 查看IP进入黑洞的时间和原因

当您的公网IP资产遭到的DDoS攻击流量超出对应的黑洞阈值后将进入黑洞，所有来自外部的流量都将被丢弃，相关的业务无法正常访问。本文介绍了发生黑洞事件后如何查询黑洞事件信息，例如IP进入黑洞的时间及所遭受的攻击流量。

背景信息

关于黑洞的具体说明，请参见阿里云黑洞策略。

不同地域下实例的黑洞触发阈值请参见下表。在下表中，✓表示支持，×表示不支持。

各地域黑洞触发阈值

地域	支持IPv4	支持IPv6	1核CPU规格ECS实例、轻量服务器实例	2核CPU规格ECS实例	4核以上CPU规格ECS实例	SLB、EIP（含NAT）、WAF实例
华东1（杭州）	✓	✓	500 Mbps	1 Gbps	5 Gbps	5 Gbps
华东2（上海）	✓	✓	500 Mbps	1 Gbps	2 Gbps	2 Gbps
华北1（青岛）	✓	×	500 Mbps	1 Gbps	5 Gbps	5 Gbps

地域	支持IPv4	支持IPv6	1核CPU规格ECS实例、轻量服务器实例	2核CPU规格ECS实例	4核以上CPU规格ECS实例	SLB、EIP（含NAT）、WAF实例
华北2（北京）	✓	✓	500 Mbps	1 Gbps	2 Gbps	2 Gbps
华北3（张家口）	✓	✓	500 Mbps	1 Gbps	2 Gbps	2 Gbps
华北5（呼和浩特）	✓	✓	500 Mbps	1 Gbps	2 Gbps	2 Gbps
华南1（深圳）	✓	✓	500 Mbps	1 Gbps	2 Gbps	2 Gbps
华南2（河源）	✓	✓	500 Mbps	1 Gbps	2 Gbps	2 Gbps
西南1（成都）	✓	×	500 Mbps	1 Gbps	2 Gbps	2 Gbps
中国香港	✓	✓	500 Mbps	500 Mbps	500 Mbps	500 Mbps
日本（东京）	✓	×	500 Mbps	500 Mbps	500 Mbps	500 Mbps
新加坡	✓	×	500 Mbps	500 Mbps	500 Mbps	500 Mbps
澳大利亚（悉尼）	✓	×	500 Mbps	500 Mbps	500 Mbps	500 Mbps
马来西亚（吉隆坡）	✓	×	500 Mbps	500 Mbps	500 Mbps	500 Mbps
印度尼西亚（雅加达）	✓	×	500 Mbps	500 Mbps	500 Mbps	500 Mbps
印度（孟买）	✓	×	500 Mbps	1 Gbps	1 Gbps	1 Gbps
韩国（首尔）	✓	×	500 Mbps	500 Mbps	500 Mbps	500 Mbps
德国（法兰克福）	✓	×	500 Mbps	500 Mbps	500 Mbps	500 Mbps
英国（伦敦）	✓	×	500 Mbps	500 Mbps	500 Mbps	500 Mbps
美国（硅谷）	✓	×	500 Mbps	1 Gbps	2 Gbps	2 Gbps
美国（弗吉尼亚）	✓	×	500 Mbps	500 Mbps	500 Mbps	500 Mbps

地域	支持IPv4	支持IPv6	1核CPU规格ECS实例、轻量服务器实例	2核CPU规格ECS实例	4核以上CPU规格ECS实例	SLB、EIP（含NAT）、WAF实例
阿联酋（迪拜）	✓	×	500 Mbps	500 Mbps	500 Mbps	500 Mbps

操作步骤

1. 登录流量安全产品控制台。
2. 在左侧导航栏，单击**资产中心**。
3. 在顶部菜单栏左上角处，选择资产所在地域。
4. 单击需要操作的云产品页面，例如**ECS**。
5. 在IP资产列表中，单击要操作的IP。
6. 在**实例详情**页，通过事件列表查看历史黑洞事件（**事件**为**黑洞**）的信息，并在流量图中查看黑洞事件发生时的攻击流量。

   黑洞事件中记录了黑洞的**开始时间**和**结束时间**。

   > **说明** 如果当前资产中未发生过黑洞或清洗事件，则事件列表中将无记录展示。

7. （可选）单击目标事件操作列下的**证据下载**，您可以下载针对该攻击事件的抓包文件作为证据，用于向网监报案。

12.3. 连接已被黑洞的服务器

本文介绍了在服务器进入黑洞时，通过阿里云同地域ECS服务器连接被黑洞服务器的方法。

背景信息

假如您的服务器遭受大流量攻击而进入黑洞，则所有来自外部的流量都会被丢弃，但是阿里云内部与该服务器同地域的云产品仍然能够正常连通该服务器。

因此，在您的服务器进入黑洞后，您可以使用阿里云内部的ECS云服务器连接该服务器。

操作步骤

1. 登录与被黑洞服务器同地域且可正常访问的ECS云服务器。

   > **说明** 该ECS云服务器需要与被黑洞的服务器可连通，属于同一个专有网络VPC环境，且连接不被安全组的相关访问控制规则所阻断。更多信息，请参见安全组概述。

2. 在ECS云服务器中，通过工具或命令连接黑洞状态的服务器。
   通过ECS云服务器成功连接该服务器后，您可以将处于黑洞状态的服务器上的文件转移至已登录的ECS云服务器，您也可以通过这种方式变更该服务器上的配置文件等。

12.4. 云虚拟主机DDoS防护黑洞阈值

云独享虚拟主机默认黑洞触发阈值如下（单位：bps）。

> **说明** 对于共享虚拟主机，由于多台共享虚拟主机会共享同一个IP，因此其黑洞阈值无法确定，但必定低于同地域独享虚拟主机的黑洞阈值。而且，如果有一台共享虚拟主机遭受大量DDoS攻击并触发黑洞机制，那么与它共享IP的其他虚拟主机都将无法访问。如果您的业务对安全性和稳定性有一定要求，建议购买独享虚拟主机或者ECS云服务器。

地区	独享虚拟主机
华东 1（杭州）	5G
华北 1（青岛）	5G
华南 1（深圳）	2G
华北 2（北京）	2G
华东 2（上海）	2G
中国香港	500M
美国	500M
新加坡	500M

默认的黑洞时长是2.5小时，黑洞期间不支持解封。实际黑洞时长视攻击情况而定，从30分钟到24小时不等。黑洞时长主要受以下因素影响：

- 攻击是否持续。如果攻击一直持续，黑洞时间会延长，黑洞时间从延长时刻开始重新计算。
- 攻击是否频繁，如果某用户是首次被攻击，黑洞时间会自动缩短；反之，频繁被攻击的用户被持续攻击的概率较大，黑洞时间会自动延长。

> **说明** 针对个别黑洞过于频繁的用户，阿里云保留延长黑洞时长和降低黑洞阈值的权利，具体黑洞阈值和黑洞时长以控制台显示为准。

如果您想获得更高的增量DDoS防护能力，购买DDoS高防IP服务，获得每天最高300G的独享DDos防护服务。

12.5. 解除黑洞

DDoS原生防护为已防护的IP提供黑洞解除功能，您可以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

购买原生防护企业版后，您将获赠每月100次黑洞解除次数。在您的DDoS原生防护实例有效期内，每月初该防护包实例的黑洞解除次数将自动重置为100。

> **说明** 如果当月的黑洞解除次数未及时用完，将会在月底自动清零，不会累计到下个月的黑洞解除次数中。

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，请您耐心等待平台自动解封。更多信息，请参见查看黑洞时长。

操作步骤

1. 登录流量安全产品控制台。
2. 在左侧导航栏，选择**网络安全 > DDoS原生防护 > 实例管理**。
3. 在顶部菜单栏左上角处，选择实例所在资源组和地域。
4. 在**实例管理**页面，定位到要操作的原生防护实例，单击**操作**列下的**解除黑洞**。

> **注意** 只有当原生防护实例下存在**异常IP**（即防护对象被黑洞）时，才支持**解除黑洞**操作。未发生黑洞时，控制台不会展示**解除黑洞**。

5. 在**防护对象**页签下，定位到处于**黑洞中**状态的防护对象，单击**操作**列下的**解除黑洞**。

6. 在**解除黑洞**对话框，查看剩余黑洞解除次数，并单击**确认**。

> **说明** 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）。

执行结果

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重新尝试。如果未收到提示信息，则表示黑洞状态已成功解除。

相关文档

- DeleteBlackhole

13.最佳实践

13.1. 设置DDoS攻击事件报警

本文介绍了设置DDoS原生防护黑洞、清洗事件报警通知的方法。通过为DDoS原生防护开启事件报警，您能够及时获知DDoS原生防护实例上的DDoS攻击事件，并在发生故障时第一时间发现问题，缩短故障处理时间，以便尽快恢复业务。

报警方式说明

DDoS原生防护目前支持以下报警方式：

- 消息中心报警

  消息中心是阿里云账号提供的消息通知服务，支持配置与阿里云服务相关的各类消息通知。您可以通过消息中心，开启**云盾安全信息通知**，使阿里云在您的资产上发生安全事件时，通过站内信、邮件、短信、语音等方式，向您指定的消息接收人发送报警通知。

- 云监控报警

  云监控（CloudMonitor） 是一项针对阿里云资源和互联网应用进行监控的服务。云监控支持监控DDoS原生防护实例上的DDoS攻击事件，具体包括：

  - 黑洞事件：表示DDoS攻击流量的峰值带宽超过了服务器的DDoS防御能力（即黑洞阈值），导致服务器IP进入黑洞。
  - 清洗事件：表示DDoS攻击流量超过清洗阈值，触发流量清洗。

  您可以通过云监控的报警服务功能，为DDoS原生防护设置事件报警规则，使云监控在DDoS原生防护实例上检测发现DDoS攻击事件时，通过短信、邮件、钉钉等方式向您指定的报警联系人发送报警通知，以便您在第一时间知晓攻击事件并及时进行处理。

- 日志分析服务报警

  DDoS原生防护企业版支持基于流量日志进行防护分析。您为企业版实例开启防护分析后，即可使DDoS原生防护采集防护对象的业务流量及防护日志，供您进行查询与分析。您可以在查询与分析日志的基础上，通过条件组合等方式对需要关注的业务指标自定义报警规则，使DDoS原生防护在业务指标异常时，及时向您发送报警。

  关于如何配置日志服务告警，请参见快速设置日志告警。

下表从多个维度对比了不同报警方式，方便您根据需要进行选择。

对比项	消息中心报警	云监控报警	日志分析服务报警
支持的原生防护实例版本	企业版和基础版（即免费提供的DDoS基础防护）	仅企业版	仅企业版，且必须已开启防护分析功能
使用场景	通用告警，仅需要知晓被攻击	通用告警，通过简单过滤条件，过滤需要通知的重点事件	企业级告警，支持自定义组合条件、报警方式、通知方式、通知内容，并基于过滤条件生成统计报表
配置复杂度	简易	适中	复杂

对比项	消息中心报警	云监控报警	日志分析服务报警
灵活性	低 支持在事件开始、结束时告警	中 目前支持在事件开始、结束时告警	高 支持在事件开始、结束时告警，按流量阈值告警，多种条件组合告警
通知方式	• 站内信 • 短信 • 邮件 • 语音（仅在IP进入黑洞时支持）	• 短信 • 邮件 • 语音 • Webhook	• 短信 • 邮件 • 语音 • Webhook
可靠与实时性	可靠性极高，告警时差在5分钟以内	可靠性较高，告警时差为5~10分钟	可靠性较高，告警时差为5~10分钟

配置云监控报警（仅企业版实例）

如果您已购买DDoS原生防护企业版实例，请参照以下步骤，通过云监控配置DDoS攻击事件报警；如果您使用DDoS原生防护基础版，由于基础版暂不支持配置云监控告警，推荐您配置消息中心报警。

1. 登录云监控控制台。
2. （可选）创建报警联系人。如果已有联系人，请跳过此步骤。
   i. 在左侧导航栏，选择**报警服务 > 报警联系人**。
   ii. 在**报警联系人**页签，单击**新建联系人**。
   iii. 在**设置报警联系人**面板，填写联系人信息并完成滑块验证，单击**确认**。
3. （可选）创建报警联系组。如果已有联系人组，请跳过此步骤。

   > **说明** 报警通知的接收对象必须是联系人组，您可以在联系人组中添加一个或多个联系人。

   i. 在左侧导航栏，选择**报警服务 > 报警联系人**。
   ii. 在**报警联系组**页签，单击**新建联系组**。
   iii. 在**新建联系组**面板，设置**组名**，从**已有联系人**中选择并添加联系人到当前组，单击**确认**。
4. 在左侧导航栏，选择**报警服务 > 报警规则**。
5. 单击**事件报警**页签，然后单击**创建事件报警**。
6. 在**创建/修改事件报警**面板，完成以下事件报警配置，并单击**确定**。

类型	配置项	说明
基本信息	**报警规则名称**	为报警规则命名。
	事件类型	选择**系统事件**。
	产品类型	选择**DDoS原生防护**，表示DDoS原生防护企业版实例。

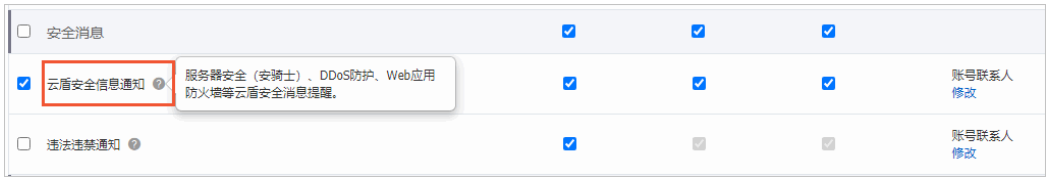
类型	配置项	说明
事件报警规则	事件类型	要通知的事件类型，可选项：**DDoS攻击**。
	事件等级	要通知的事件等级。可选项：**严重**、**警告**、**信息**。 注意 所有DDoS告警事件均为严重等级，该参数必须包含**严重**。
	事件名称	要通知的事件。可选项：**黑洞**、**清洗**。
	资源范围	选择**全部资源**。
报警方式	报警通知	选中**报警通知**，并设置**联系人组**和**通知方式**。 ○ 联系人组：选择一个已有联系人组。 ○ 通知方式：选择**Warning（短息+邮箱+钉钉机器人）**或者**Info（邮箱+钉钉机器人）**方式。 单击**添加操作**，可以设置多个联系人组和通知方式。
	消息服务队列	无需设置。
	函数计算	无需设置。
	URL回调	无需设置。
	日志服务	无需设置。

成功创建报警规则后，您可以在规则列表中查看新建的规则。新建的报警规则默认启用。当DDoS原生防护企业版实例上发生DDoS攻击事件（黑洞、清洗）时，阿里云将向报警通知联系人组中设置的联系人发送报警通知。

配置消息中心报警（基础版、企业版实例）

参照以下步骤，通过消息中心配置DDoS攻击事件报警。

1. 登录消息中心控制台。
2. 在左侧导航栏，选择**消息接收管理 > 基本接收管理**。
3. 在**基本接收管理**页面，选中**云盾安全信息通知**，并根据需要选择通知方式。



支持以下通知方式：

- **站内信**：表示将相关通知发送到阿里云控制台顶部菜单栏右上角的站内消息（单击

图标可以查看站内消息）。

- **邮箱**：表示以邮件方式，将相关通知发送到您设置的消息接收人的邮箱地址。
- **短信**：表示以短信方式，将相关通知发送到您设置的消息接收人的手机号码。

4. 单击**添加消息接收人**。
5. 在**修改消息接收人**对话框，设置**消息接收人**及其联系方式，并单击**保存**。
6. 开启语音报警通知。
   i. 在左侧导航栏，选择**消息接收管理 > 语音接收管理**。
   ii. 在**语音接收管理**页面，为**DDoS黑洞通知**开启**语音**消息通知。

   iii. 单击**DDoS黑洞通知**操作列下的**修改**。
   iv. 在**修改消息接收人**对话框，修改语音消息的**消息接收人**，并单击**保存**。

完成消息接收配置后，当您的DDoS原生防护实例上发生DDoS攻击事件时，阿里云会向您设置的消息接收人发送相关通知。

13.2. 为遭受攻击的IP开通DDoS原生防护

如果您的公网IP资产遭受的DDoS攻击超过阿里云提供的基础防护能力，您可以开通DDoS原生防护企业版，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原生防护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原生防护实例所在地域的阿里云最大DDoS防护能力提供全力防护。

前提条件

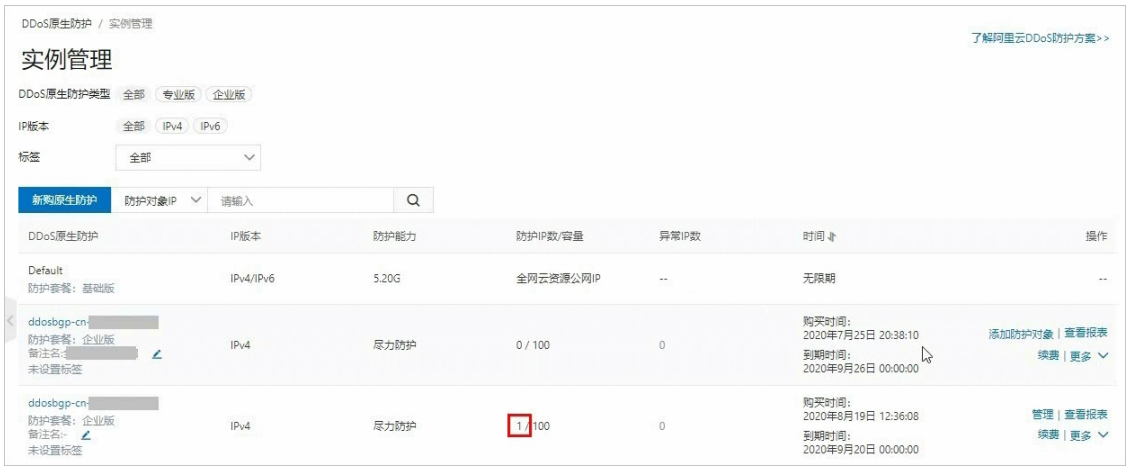
在开通DDoS原生防护企业版实例前，您应明确遭受攻击的IP地址及IP所在地域。

步骤一：购买DDoS原生防护企业版实例

步骤二：添加防护对象

1. 登录流量安全产品控制台。
2. 在左侧导航栏，选择**网络安全 > DDoS原生防护 > 实例管理**。
3. 在顶部菜单栏左上角处，选择实例所在资源组和地域。
4. 在**实例管理**页面，找到目标原生防护企业版实例，单击**操作**列下的**添加防护对象**。

> **说明** 只有在当前实例未添加任何防护IP时，操作列才会出现**添加防护对象**。如果当前实例下已添加过防护IP，您可以单击实例**操作**列下的**管理**，并在**实例详情**页面单击**添加防护对象**。



5. 如果您是第一次使用DDoS原生防护实例，请根据页面提示完成云产品授权，授权DDoS原生防护实例访问您的其他云产品。
6. 在**添加防护对象**对话框，输入您需要防护的云产品的IP，并单击**确认**。

> **说明**
> - 输入的IP地址必须和原生防护企业版实例在相同地域，且必须为当前阿里云账号保有的云资源的IP地址。
> - 多个IP间以英文逗号（,）分隔。

完成防护配置后，DDoS原生防护实例将直接为已添加的防护对象IP提供DDoS防护能力。

执行结果

防护IP添加成功后，您可以在**资产中心**页面，将鼠标放在该IP的**防护能力**上，即可查看绑定的DDoS原生防护实例的防护能力。

13.3. 升级使用DDoS高防服务

由于DDoS原生防护服务的架构限制，在某些特定情况下，DDoS原生防护企业版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原生防护企业版已无法满足您的安全防护需求，建议您升级使用DDoS高防服务，提升安全防护能力。

背景信息

关于DDoS原生防护适用的安全防护场景，请参见应用场景。

如果您已购买DDoS原生防护企业版实例，在实际使用过程中遇到以下问题，可以将已购买的DDoS原生防护企业版升级为DDoS高防服务：

- 遭受的DDoS攻击持续时间较长，且攻击流量较大。
- 防护的业务遭受CC攻击，而对此类攻击DDoS原生防护企业版无法防御。
- 其他特殊情况，需要您具体说明。

> **注意** DDoS原生防护企业版升级为DDoS高防服务时，对于您已购买的DDoS原生防护企业版实例，我们将为您退回余款。

如果单独使用DDoS原生防护企业版或者DDoS高防无法满足您的DDoS防护需求，推荐您组合使用DDoS原生防护企业版和DDoS高防服务。更多信息，请参见同时部署DDoS原生防护企业版和DDoS高防（新BGP）。

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，请使用钉钉加入DDoS高防产品问题咨询专家群聊（群号：31182544）。

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. 待服务人员确认您满足升级条件后，将为您处理已购买的DDoS原生防护实例的退款事宜。系统将根据您所购买的DDoS原生防护实例的规格及剩余服务时长为您退回余款。
4. 购买DDoS高防实例。

   具体操作，请参见购买DDoS高防实例。

5. 将您的业务接入到DDoS高防实例进行防护。

   关于网站类业务接入DDoS高防的操作，请参见步骤1：添加网站业务转发规则。

   关于非网站类业务接入DDoS高防的操作，请参见步骤1：添加端口转发规则。

13.4. 黑洞自动解除最佳实践

已经添加到DDoS原生防护企业版进行防护的业务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。针对该场景，DDoS原生防护企业版提供了黑洞自动化响应和快速解除的解决方案。

前提条件

黑洞自动化响应和快速解除解决方案需要调用DDoS原生防护企业版的API接口，目前该解决方案仅支持DDoS原生防护企业版实例。在部署黑洞自动解除方案前，请确认您的业务IP已添加至DDoS原生防护企业版实例进行防护。更多信息，请参见添加防护对象。

背景信息

DDoS原生防护企业版提供黑洞解除功能，您可以在DDoS原生防护控制台手动解除黑洞，具体操作，请参见解除黑洞。由于手动解除黑洞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原生防护企业版实例的黑洞事件。

   > **说明** 只有已添加为DDoS原生防护企业版实例的防护对象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原生防护企业版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。

2. 通过自定义消息的消费机制，调用DDoS原生防护企业版的黑洞解除API接口（DeleteBlackhole）自动解除被黑洞的业务IP。

通过类似方法，您还可以实现在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。
2. 在左侧导航栏，选择**报警服务 > 报警规则**。
3. 在**报警规则列表**页面，单击**事件报警**页签。
4. 单击**创建事件报警**，为DDoS原生防护企业版创建黑洞事件报警规则。
   - **产品类型**：选择**DDoS原生防护**。
   - **事件名称**：选择**黑洞**。

5. 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，并单击**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原生防护企业版实例中已防护的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", //事件状态。add表示事件开始，del表示事件结束。
    "bps": 0, //触发该事件的流量大小，单位：Mbps。
    "pps": 0, //触发该事件的包速率，单位：pps。
    "instanceId": "ddosbgp-cn-78v17******", //DDoS原生防护企业版实例ID。
    "ip": "47.*.*.*", //发生事件的IP。
    "regionId": "cn-hangzhou", //DDoS原生防护企业版实例所在的地域。
    "time": 1564104493000, //触发事件的时间，格式为毫秒时间戳。
    "type": "blackhole"  //事件类型。defense表示清洗事件，blackhole表示黑洞事件。
}
```

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

13.5. 同时部署DDoS原生防护企业版和DDoS高防（新BGP）

您可以同时部署DDoS原生防护企业版和DDoS高防（新BGP），通过DDoS高防流量调度器的阶梯防护联动规则，保证正常业务流畅体验的前提下增强DDoS防护能力。本文介绍了同时部署DDoS原生防护企业版和DDoS高防（新BGP）的配置方法。

背景信息

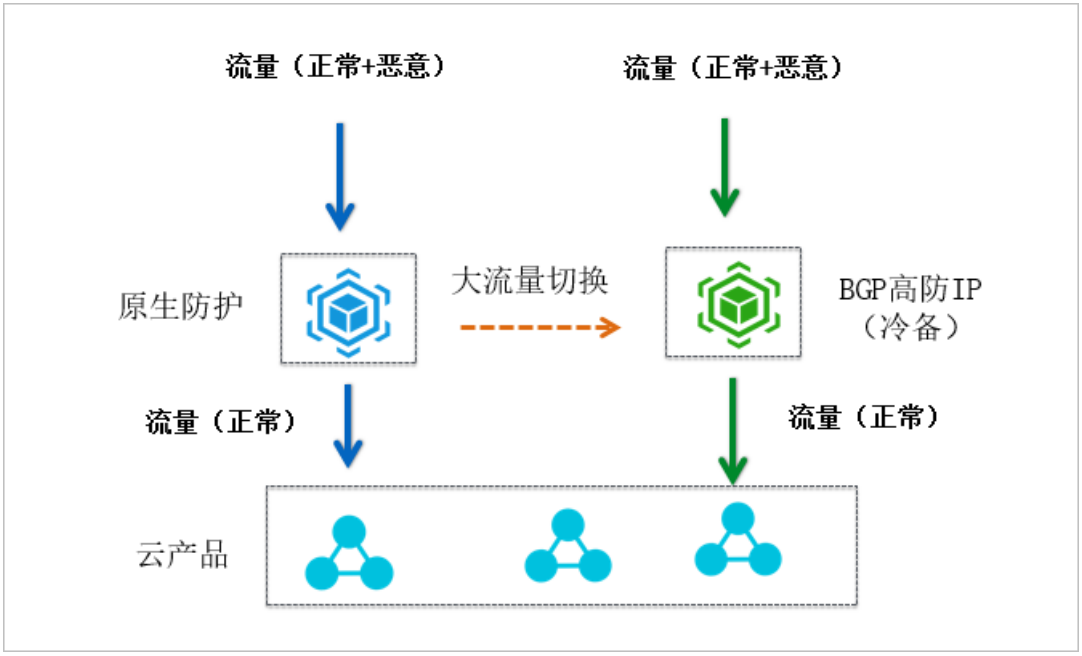
同时部署DDoS原生防护企业版和DDoS高防（新BGP），当DDoS攻击不超过原生防护企业版的防御能力时（防御能力具体和所在地域有关，一般不低于100~300 Gbps），业务流量默认解析到云产品，不增加业务延迟；当攻击过大触发黑洞时，高防流量调度器将流量切换到DDoS高防，防御大流量的攻击，此时存在约20 ms的业务延时；攻击停止后，根据流量调度器设置的切换延迟时间，等待一段时间后业务流量回切到云产品。

> **说明**
>
> - 黑洞触发后通过流量调度器自动完成网站业务流量的切换，中国内地的DNS解析更新约需5~10分钟，非中国内地约需1~3分钟。
> - 切换到DDoS高防（新BGP）后，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30 Gbps保底+300 Gbps弹性，您可以通过工单升级到1 Tbps甚至更高。
> - 切换到DDoS高防（新BGP）后，即使攻击停止也不会马上回切，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。流量调度器支持设置切换延迟时间，默认是120分钟（2小时）。

同时部署DDoS原生防护企业版和DDoS高防（新BGP）时，您可以同时享受两者的优势。例如DDoS原生防护企业版的费用可控、全资产防护、透明部署无延迟，和DDoS高防（新BGP）的超大攻击流量防护。

网络架构

具体架构如下图所示。



操作步骤

1. 开通DDoS原生防护企业版。

   具体操作，请参见购买DDoS原生防护企业版实例。

2. 将业务的源站IP地址添加为DDoS原生防护企业版的防护对象。

   具体操作，请参见添加防护对象。

3. 开通DDoS高防（新BGP）专业版。

   具体操作，请参见购买DDoS高防实例。

4. 添加网站配置接入DDoS高防。

   具体操作，请参见添加网站。

   > **说明** 成功添加网站业务转发配置后，无需按照页面提示修改DNS解析。

5. 使用流量调度器，为业务添加**阶梯防护**调度规则，将业务解析到流量调度器的Cname地址。

   具体操作，请参见阶梯防护。

   > **说明** 成功添加调度规则后，您可以在**通用联动**规则列表获取规则对应的流量调度器Cname地址。

6. 前往域名DNS服务商处修改域名的DNS解析，将解析指向流量调度器Cname地址。

   具体操作，请参见修改CNAME解析接入流量调度器。

13.6. DDoS原生防护和Web应用防火墙组合使用方案

本文介绍了为网站类业务同时部署DDoS原生防护和Web应用防火墙的配置方法。该方案适用于为网站业务同时防御四层DDoS攻击和七层Web攻击、CC攻击的场景。

前提条件

- 已创建ECS实例并部署了业务相关的应用，ECS实例拥有公网IP地址且网站有域名。

  > **说明** 如果网站用于在中国内地提供服务，则网站域名必须已经完成ICP备案，否则将不能接入中国内地的Web应用防火墙实例进行防护。更多信息，请参见ICP备案流程概述。

- 已开通DDoS原生防护企业版。更多信息，请参见购买DDoS原生防护企业版实例。

  > **说明** 您在购买原生防护企业版实例时，需要选择资源所在地域。该地域必须与ECS实例一致。

- 已开通Web应用防火墙。更多信息，请参见开通Web应用防火墙。

背景信息

为网站类业务开启DDoS原生防护企业版时，如果业务本身除了需要防御DDoS攻击，还需要防御Web攻击、CC攻击，建议您为网站同时开启Web应用防火墙，由Web应用防火墙帮助业务防御常见的Web攻击、CC攻击。关于Web应用防火墙（WAF）的详细介绍，请参见什么是Web应用防火墙。

同时使用DDoS原生防护和Web应用防火墙时，您需要先将网站业务接入Web应用防火墙进行防护，然后将WAF实例的IP地址添加为DDoS原生防护企业版实例的防护对象。完成上述部署后，所有业务流量先经过WAF进行安全清洗，攻击流量（包括DDoS攻击、Web攻击、CC攻击）被丢弃，只有正常的业务流量被转发到源站服务器。

操作步骤

1. 将网站接入Web应用防火墙进行防护。

   i. 登录Web应用防火墙控制台。

ii. 在顶部菜单栏，选择地域（**中国内地**、**海外地区**）。

Web应用防火墙将根据源站服务器的位置自动匹配最佳的服务地区。

iii. 在左侧导航栏，单击**资产中心 > 网站接入**。

iv. 单击**添加域名**。

Web应用防火墙支持**CNAME接入**和**透明接入**两种接入方式，其中CNAME接入分为域名一键接入（即自动操作）和手动添加网站，透明接入目前仅支持源站服务器部署在华北2（北京）地域的阿里云ECS实例。

本教程以CNAME接入-手动添加网站为例进行介绍。关于其他的接入方法，请参见CNAME接入-自动添加网站、透明接入。

v. （可选）在**域名一键接入**页面，单击**手动添加其他网站**。如果没有跳出**域名一键接入**页面，请忽略该步骤。

vi. 完成**添加域名**配置向导中的步骤1：**填写网站信息**，并单击**下一步**。

您需要填写以下网站信息：

- **域名**：网站的域名。
- **协议类型**：网站使用的协议类型。如果支持**HTTPS**，必须在添加域名后上传网站域名的HTTPS证书。更多信息，请参见上传HTTPS证书。
- **服务器地址**：选择**IP**类型并填写ECS实例的公网IP地址。
- **服务器端口**：选择协议类型后，自动匹配默认的服务端口。WAF也支持自定义非标准服务端口。更多信息，请参见WAF支持的端口。
- **WAF前是否有七层代理（高防/CDN等）**：选择**否**。

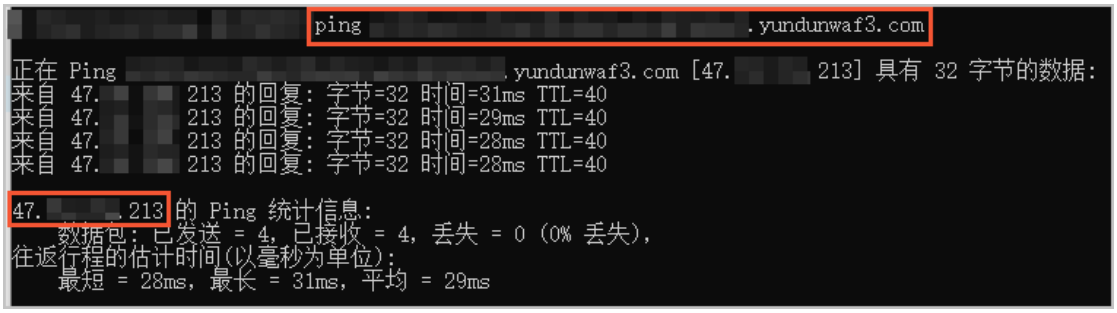
  您如果已在WAF前配置了其他的七层代理服务（例如DDoS高防、CDN等），那么客户端访问流量到WAF前会先经过其他七层代理转发。由于您使用的是DDoS原生防护，原生防护不属于七层代理服务，此处您选择否即可。

关于网站信息参数的更多说明，请参见网站信息参数说明。

vii. 单击**完成，返回网站列表**。

已添加的网站将获得一个CName地址，您可以在网站列表中获取网站域名的CName地址。

viii. 在本地计算机上执行ping命令，`ping 网站域名的CName地址`，获取您已购买的WAF实例的IP地址。



2. 在源站服务器上设置放行Web应用防火墙的回源IP段。

具体操作请参见放行WAF回源IP段。

3. 修改网站域名的DNS解析，将域名解析指向步骤1获得的WAF Cname地址。

具体操作请参见修改域名DNS。

修改域名解析后，网站的所有访问请求都会解析到Web应用防火墙进行安全清洗（过滤Web攻击、CC攻击），只有正常的业务流量被转发到源站服务器。

由于WAF实例本身不具备抵御大流量DDoS攻击的能力，业务遭受大流量DDoS攻击时会导致WAF实例性能受损，影响业务转发，所以需要为WAF实例开启原生防护企业版，提高业务的抗DDoS攻击能力。

4. 将WAF的IP地址添加为您已购买的DDoS原生防护企业版实例的防护对象，为WAF实例开启DDoS原生防护企业版防护。

   具体操作请参见添加防护对象。

   成功添加防护对象后，WAF实例将享有DDoS原生防护企业版实例的DDoS攻击全力防护能力，在业务遭受DDoS攻击时，自动触发流量清洗，防御DDoS攻击。

13.7. DDoS原生防护和负载均衡组合使用方案

本文介绍了为搭建在云服务器ECS上的网站类业务部署负载均衡，并开启DDoS原生防护企业版防护的配置方法。相比于直接为ECS源站服务器开启DDoS原生防护企业版防护，在源站前部署负载均衡后再开启DDoS原生防护，能够取得更好的防护效果。

前提条件

- 已创建ECS实例并部署业务相关应用。更多信息，请参见新手指引。
- 已开通DDoS原生防护企业版实例。更多信息，请参见购买DDoS原生防护企业版实例。

背景信息

使用DDoS原生防护企业版防护网站类业务时，推荐您为业务所在云服务器ECS实例部署负载均衡SLB并将负载均衡的服务地址添加为DDoS原生防护企业版的防护对象，实现通过SLB丢弃未监听协议和端口的流量并大幅提升源站的抗DDoS攻击能力。上述部署方式对防御不同类型的DDoS攻击（例如SSDP、NTP、Memcached等反射型攻击、UDP Flood攻击、SYN Flood大包攻击）有很好的效果。

本文将指导您为ECS源站服务器部署负载均衡并开启DDoS原生防护企业版防护。

> **说明** 如果您的源站服务器已经部署了负载均衡，则只需参见添加防护对象，将负载均衡的服务地址作为DDoS原生防护企业版的防护对象，即可为源站服务器开启DDoS原生防护企业版防护。

操作步骤

1. 创建一台公网负载均衡SLB实例。

   具体操作请参见创建和管理CLB实例。

   创建负载均衡实例时需要注意以下内容：

   - 由于负载均衡不支持跨地域部署，因此应选择与ECS实例相同的地域。
   - 由于DDoS原生防护仅支持防护公网IP资源，因此应选择公网实例类型。

   更多信息，请参见准备工作。

   成功创建负载均衡实例后，您可以在负载均衡SLB控制台的**实例管理**页面获取SLB实例的**服务地址**。

2. 配置负载均衡实例。

   具体操作请参见配置实例。

   配置负载均衡实例时需要注意以下内容：

   - 在选择**协议&监听**时，根据自身业务，只选择需要监听的协议（支持TCP、UDP、HTTP、HTTPS）和端口。未设置监听的协议和端口的流量将被直接丢弃，不会转发到后端ECS实例。
   - 在添加**后端服务器**时，选择添加已部署业务应用的ECS源站服务器。

   > **说明** 由于负载均衡SLB和后端ECS之间通过内网进行通信，所以在配置完负载均衡实例并测试负载均衡正常工作后，建议您关闭后端ECS实例的公网访问。

   成功配置负载均衡实例后，负载均衡实例将按照已有配置，将客户端的请求流量分发到后端ECS实例。

3. 修改域名DNS。
   - 如果您的业务是通过IP地址提供服务，您只需将步骤1获得的负载均衡实例的服务地址作为业务IP地址即可，可以跳过该步骤。
   - 如果您的业务是通过域名提供服务，您需要将域名的DNS解析指向步骤1获得的负载均衡实例的服务地址。具体操作请参见设置A记录域名解析。
4. 将负载均衡实例的服务地址添加为您已购买的DDoS原生防护企业版实例的防护对象，为负载均衡实例开启DDoS原生防护企业版防护。

   具体操作请参见添加防护对象。

   成功添加防护对象后，SLB源站服务器将享有DDoS原生防护企业版提供的DDoS攻击全力防护能力，在业务遭受DDoS攻击时，自动触发流量清洗。

13.8. DDoS原生防护代播模式攻击时自动启用配置

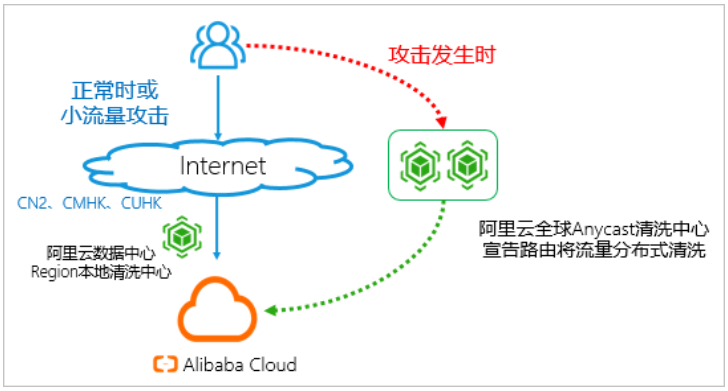
本文介绍了使用DDoS原生防护代播模式自动防御大流量DDoS攻击的最佳实践，适用于已经开通了DDoS原生防护代播模式的用户在阿里云IP资产受到攻击时，通过API接口自动启用DDoS原生防护代播模式的场景。

前提条件

- 已开通DDoS原生防护企业版实例。更多信息，请参见购买DDoS原生防护企业版实例。
- 已联系销售人员购买了DDoS原生防护代播版实例。
- 已在云监控服务中创建了报警联系人和联系人组。更多信息，请参见创建报警联系人或报警联系组。

背景信息

DDoS原生防护代播版可以为海外云下IDC、小型运营商、阿里云海外客户以及有自己BGP网络的客户提供阿里云的DDoS防护，且防护过程不需要改变原有业务IP地址和网络架构。下图描述了DDoS原生防护代播版的防护原理。



原理说明：

- 正常流量或小流量攻击：流量直接访问阿里云DDoS原生防护本地机房，无额外延迟增加，可以防御小流量攻击。
- 发生DDoS攻击时：清洗中心宣告路由，流量由全球清洗中心分布式清洗，延迟略有增加，但防护能力可以增加到Tbps级别。

本文将指导您使用云监控的报警功能设置报警规则，监控DDoS原生防护本地机房的DDoS攻击；如果发生DDoS攻击，通过API接口调用开启DDoS原生防护代播实例的牵引防护，并在攻击结束后，停止牵引防护。

> **说明** 本文中所有用到API请求参数示例的地方，全部使用 `<参数描述>` 表示，例如要求传入原生防护代播版实例ID的地方，表示为 `InstanceId=<yourOnDemandInstanceId>` 。
>
> 具体操作中，请使用真实的参数值替换 `<参数描述>` ，例如您需要联系销售人员获取您的原生防护代播实例的ID（InstanceId），并替换 `<yourOnDemandInstanceId>` 。

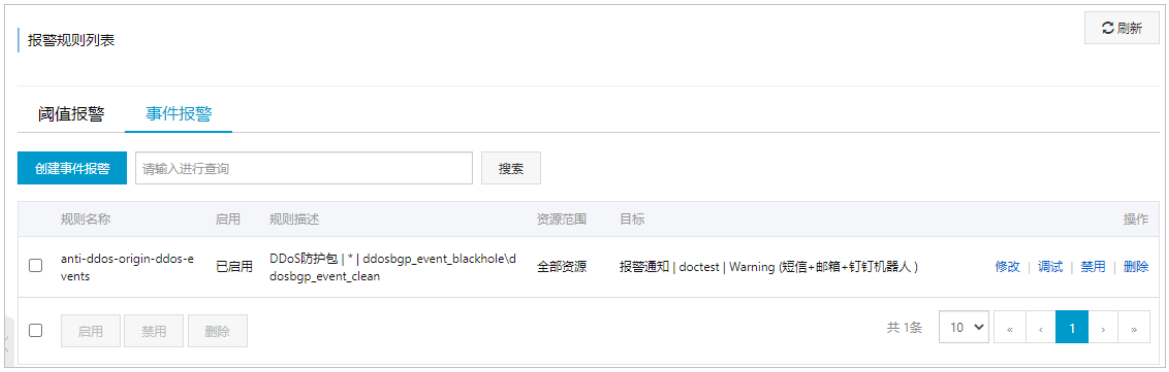
操作步骤

1. 通过云监控设置DDoS原生防护黑洞事件的报警通知，监控DDoS原生防护本地清洗中心的黑洞、清洗事件。
   i. 登录云监控控制台。
   ii. 在左侧导航栏，选择**报警服务 > 报警规则**。
   iii. 单击**事件报警**页签。
   iv. 单击**创建事件报警**。
   v. 在**创建/修改事件报警**页面，配置以下事件报警参数。

参数	说明
报警规则名称	为当前报警规则的命名。示例：原生防护DDoS攻击事件报警。
事件类型	选中**系统事件**。
产品类型	选择**DDoS防护包**。
事件等级	选择**全部级别**。
事件名称	选择**黑洞**和**清洗**。
资源范围	选择**全部资源**。
报警通知	选中**报警通知**，并选择要接收报警通知的报警**联系人组**和一种**通知方式**。

vi. 单击**确定**。

成功创建报警规则后，报警规则自动生效，一旦DDoS原生防护实例上发生DDoS攻击，报警规则中指定的联系人组会第一时间收到报警通知。您可以在**事件报警**规则列表中查看和管理报警规则。更多信息，请参见创建报警规则。



2. 发生DDoS攻击（即收到黑洞、清洗事件报警通知）时，调用ModifyOnDemaondDefenseStatus接口开启DDoS原生防护代播实例的流量牵引防护，将流量牵引至阿里云全球Anycast清洗中心。

   您需要传入以下请求参数：

   ```
   ?Action=ModifyOnDemaondDefenseStatus
   &DdosRegionId=<yourInstanceRegionId>
   &DefenseStatus=Defense
   &InstanceId=<yourOnDemandInstanceId>
   ```

3. （可选）解除DDoS原生防护企业版实例的黑洞状态。
   - 如果DDoS原生防护企业版实例未触发黑洞状态，请忽略该步骤。
   - 如果DDoS原生防护企业版实例处于黑洞状态，您可以在开启流量牵引防护约10秒以后，调用DeleteBlackhole接口解除DDoS原生防护企业版实例的黑洞状态。

     您需要传入以下请求参数：

     ```
     ?Action=DeleteBlackhole
     &InstanceId=<yourOnDemandInstanceId>
     &Ip=<yourOnDemandInstanceIp>
     ```

4. 调用DescribeTopTraffic接口查询DDoS攻击是否结束。

   您需要传入以下请求参数：

   ```
   ?Action=DescribeTopTraffic
   &Ipnet=<onDemandInstanceIpnetToQuery>
   &InstanceId=<yourOnDemandInstanceId>
   &StartTime=<startTimeToQuery>
   &EndTime=<endTimeToQuery>
   ```

   如果返回的AttackBps（攻击流量大小，单位：Kbps）小于300000，并持续30分钟以上，则表示DDoS攻击已经结束。

5. 确认DDoS攻击事件结束后，在业务低峰时段调用ModifyOnDemaondDefenseStatus接口停止DDoS原生防护代播实例的流量牵引防护。

   > **说明** 建议您在业务低峰时段调用停止牵引，这样可以减少流量切换带来的影响。

   您需要传入以下请求参数：

```
?Action=ModifyOnDemaondDefenseStatus
&DdosRegionId=<yourDdosRegionId>
&DefenseStatus=UnDefense
&InstanceId=<yourOnDemandInstanceId>
```