DDoS 防护 AAD

用户指南

文档版本 05

发布日期 2024-03-19

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 DDoS 原生基础防护操作指南

1.1 使用概览

DDoS原生基础防护的使用概览如**使用概览**所示。

表 1-1 使用概览

子流程	说明
设置防护策略	为公网IP设置流量清洗阈值。详细操作请参见**设置防护策略**。
开启告警通知	为Anti-DDoS开启告警通知后，当公网IP受到DDoS攻击时用户会收到提醒消息。详细操作请参见**开启Anti-DDoS告警通知**。
设置事件告警通知	通过云监控服务，对防护的弹性公网IP启用事件监控，当出现清洗、封堵、解封等事件时进行告警。详细操作请参见**设置事件告警通知**。
查看监控报表	查看单个公网IP的监控详情，包括当前防护状态、当前防护配置参数、24小时的流量情况、24小时的异常事件等。详细操作请参见**查看Anti-DDoS监控报表**。
查看拦截报告	查看用户所有公网IP地址的防护统计信息，包括清洗次数、清洗流量，以及公网IP被攻击次数Top10和共拦截攻击次数。详细操作请参见**查看Anti-DDoS拦截报告**。

1.2 设置防护策略

Anti-DDoS为华为云上的公网IP资源自动开启DDoS攻击防护，即Anti-DDoS对华为云上购买的EIP自动开启DDoS攻击防护。

Anti-DDoS防护策略支持以下两种设置方法：

- 设置默认防护策略

  默认防护策略作为系统初始策略，对所有新购买的公网IP生效。策略默认的“流量清洗阈值”为120Mbps，支持修改。

- 手动设置防护策略

  手动为公网IP设置特定的防护策略，支持批量操作和单个操作。手动设置了防护策略的公网IP将不再使用默认防护策略。

设置默认防护策略

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 选择“公网IP”页签，单击“设置默认防护策略”。

步骤4 根据实际设置“流量清洗阈值”，如图1-1所示。

图 1-1 配置默认防护策略

表 1-2 参数说明

参数	说明
流量清洗阈值	Anti-DDoS检测到IP的入流量超过该阈值时，触发流量清洗。 “流量清洗阈值”可按照实际业务流量进行设置，建议设置为与所购买带宽最接近的数值，但不超过购买带宽。 “默认防护”为“120Mbps”，“手动设置”支持更多档位。 **说明** • 当实际业务流量触发流量清洗阈值时，Anti-DDoS仅拦截攻击流量；当实际业务流量未触发流量清洗阈值时，无论是否为攻击流量，都不会进行拦截。 • 请按照实际业务访问流量选择参数。建议选择与所购买带宽最接近的数值，但不超过购买带宽。

步骤5 单击“确定”，完成默认防护策略的设置。

说明

默认防护策略设置完成后，新购买的公网IP均按照默认防护策略启动防护。

----结束

手动设置防护策略

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在“公网IP”页签，根据实际选择设置方法。

- 为多个公网IP设置防护策略：勾选多个公网IP后，单击页面上方“防护设置”。

图 1-2 批量设置防护策略

- 为单个公网IP设置防护策略：在需要设置防护策略的公网IP所在行，单击“防护设置”。

图 1-3 单个公网 IP 设置防护策略

步骤4 根据实际设置“流量清洗阈值”。

图 1-4 设置防护策略

表 1-3 参数说明

参数	说明
流量清洗阈值	Anti-DDoS检测到IP的入流量超过该阈值时，触发流量清洗。 “流量清洗阈值”可按照实际业务流量进行设置，建议设置为与所购买带宽最接近的数值，但不超过购买带宽。 “默认防护”为“120Mbps”，“手动设置”支持更多档位。 **说明** • 当实际业务流量触发流量清洗阈值时，Anti-DDoS仅拦截攻击流量；当实际业务流量未触发流量清洗阈值时，无论是否为攻击流量，都不会进行拦截。 • 请按照实际业务访问流量选择参数。建议选择与所购买带宽最接近的数值，但不超过购买带宽。

步骤5 单击“确定”，完成设置。

----结束

1.3 查看 Anti-DDoS 公网 IP

操作场景

该任务指导用户查看公网IP。

须知

- 购买了公网IP后，自动开启Anti-DDoS“默认防护”。开启Anti-DDoS防护后，即可对开启防护的IP地址提供DDoS攻击保护。
- 开启Anti-DDoS防护后，不允许关闭。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 选择“公网IP”页签，查看公网IP，参数说明如表1-4所示。

图 1-5 查看公网 IP

说明

- 支持防护IPv4和IPv6环境下发起的流量攻击。
- 全部开启防护：单击“全部开启防护”，为当前区域下所有未开启防护的公网IP开启Anti-DDoS防护。
- 开启Anti-DDoS“默认防护”后，当检测到报文总流量达到120Mbps时， 触发流量清洗功能。如果需要配置Anti-DDoS的防护策略，可以修改防护参数，详细操作请参见**设置防护策略**。
- Anti-DDoS最高提供500Mbps的DDoS攻击防护。系统会对超过黑洞阈值的受攻击公网IP进行黑洞处理，正常访问流量会丢弃；对于可能会遭受超过500Mbps流量攻击的应用，建议您购买华为云DDoS高防服务，提升防护能力。
- 在“所有防护状态”搜索框中选择防护状态，“公网IP”界面将只显示对应状态的公网IP。

表 1-4 参数说明

参数名称	说明
公网IP	Anti-DDoS防护的公网IP地址。 **说明** 如果公网IP已开启Anti-DDoS防护，单击公网IP，可以跳转至该公网IP的“监控报表”页面。
防护状态	公网IP的防护状态，包括： • 正常 • 设置中 • 未开启 • 清洗中 • 黑洞中
资产类型	• EIP：弹性公网IP。 • ELB：弹性负载均衡。 • NetInterFace • VPN：虚拟专用网络。 • NAT：NAT网关。 • VIP：高可用虚拟IP。 • CCI：云容器实例。 • SubEni
防护设置	当前公网IP的流量清洗阈值。
企业项目	当前公网IP所属的企业项目。

----结束

1.4 开启 Anti-DDoS 告警通知

操作场景

为Anti-DDoS开启告警通知后，当公网IP受到DDoS攻击时用户会收到提醒消息（通知方式由用户设置）。否则，无论DDoS攻击流量多大，用户都只能登录管理控制台自行查看，无法收到报警信息。

前提条件

登录账号已购买公网IP。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 选择“告警通知”页签，设置告警通知，相关参数说明如表1-5所示。

图 1-6 设置告警通知

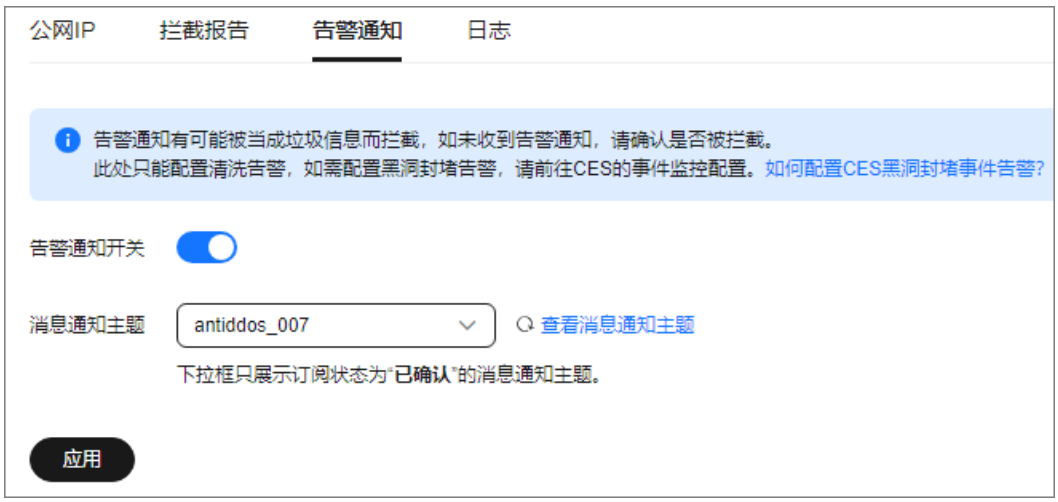


表 1-5 设置告警通知

参数名称	说明
告警通知开关	开启或关闭告警通知，说明如下： •  ：开启状态。 •  ：关闭状态。

参数名称	说明
消息通知主题	可以选择使用已有的主题，或者单击“查看消息通知主题”创建新的主题。 更多关于主题的信息，请参见《消息通知服务用户指南》。

步骤4 单击“应用”，开启告警通知。

----结束

1.5 设置事件告警通知

操作场景

通过云监控服务，对防护的弹性公网IP启用事件监控，当出现清洗、封堵、解封等事件时进行告警，方便您及时了解DDoS原生基础防护的防护情况。

开启事件告警通知后，出现相关事件时，即可在云监控服务的事件监控页面查看事件详情。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上方的，选择“管理与监管 > 云监控服务”。

步骤4 根据实际选择方式。

- 方法一：在左侧导航树，单击“事件监控”，进入“事件监控”页面。
- 方法二：在左侧导航树，选择“告警 > 告警规则”，进入“告警规则”页面。

步骤5 在页面右上方，单击“创建告警规则”，进入“创建告警规则”页面。

步骤6 参考表1-6配置告警参数。

图 1-7 告警参数

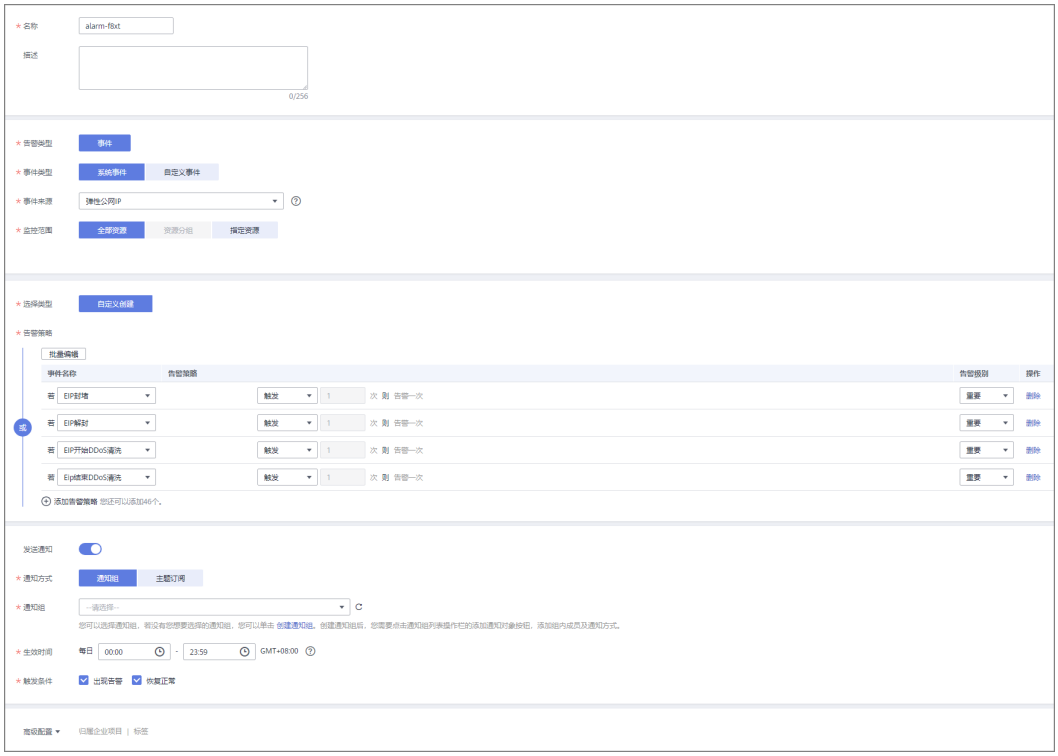


表 1-6 参数说明

参数	说明
名称	系统会随机产生一个名称，您也可以进行修改。
描述	告警规则描述。
告警类型	选择“事件”。
事件类型	选择“系统事件”。
事件来源	选择“弹性公网IP”。
监控范围	告警规则适用的资源范围，根据需要选择。
选择类型	默认为“自定义创建”。
告警策略	推荐选择“EIP封堵”、“EIP解封”、“EIP开始DDoS清洗”、“EIP结束DDoS清洗”。 当流量大于10000kps时，系统会在开始清洗和结束清洗各发送一次告警通知；流量小于10000kps不会发送告警通知。
通知方式	选择“通知组”或“主题订阅”。
通知组	选择所需的通知组。
通知对象	选择所需的主题订阅。
生效时间	根据实际选择。

参数	说明
触发条件	选择“出现告警”、“恢复正常”。

步骤7 根据实际需要，选择是否发送通知。

说明

告警消息由消息通知服务SMN发送，可能产生少量费用。

表 1-7 通知参数

参数	说明
发送通知	配置是否发送邮件、短信、HTTP和HTTPS通知用户。
通知方式	根据需要可选择通知组或主题订阅两种方式。
通知组	通知方式为通知组时生效，根据实际选择。
通知对象	通知方式为主题订阅时生效，根据实际选择。
生效时间	该告警规则仅在生效时间内发送通知消息。
触发条件	根据实际选择。

步骤8 单击“立即创建”，在弹出的窗口中单击“确定”，告警通知创建成功。

----结束

1.6 配置 Anti-DDoS 日志

操作场景

启用Anti-DDoS防护功能后，您可以将攻击日志记录到云日志服务（Log Tank Service，简称LTS）中，通过LTS记录的Anti-DDoS日志数据，快速高效地进行实时决策分析、设备运维管理以及业务趋势分析。

前提条件

已开通云日志服务。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 选择“日志”页签，开启日志  ，并选择日志组和日志流，相关参数说明如表1-8所示。

图 1-8 配置日志

表 1-8 日志配置参数

参数	参数说明
选择日志组	选择已创建的日志组，或者单击“查看日志组”，跳转到LTS管理控制台创建新的日志组。
记录攻击日志	选择已创建的日志流，或者单击“查看日志流”，跳转到LTS管理控制台创建新的日志流。 攻击日志记录每一个攻击告警信息，包括攻击类型、防护的IP等信息。

步骤4 单击“确定”，日志配置成功。

您可以在LTS管理控制台查看Anti-DDoS的防护日志。

----结束

日志字段说明

本章节介绍了AntiDDoS日志包含的日志字段。

表 1-9 全量日志字段说明

字段	说明
logType	日志类型。默认为“ip_attack_sum”，攻击日志。
deviceType	上报日志的设备类型。默认为“CLEAN”，清洗设备。
inKbps	入流量（单位：kbps）。
maxPps	入流量峰值（单位：pps）。
dropPps	丢弃的流量均值（单位：pps）。

字段	说明
maxAttackInBps	攻击流量峰值时刻的入流量值（单位：bps）。
currentConn	当前连接数。
zoneIP	防护的IP。
logTime	日志产生的时间。
attackType	攻击类型，对应的攻击类型请参考**表1-10**。
inPps	入流量（单位：pps）。
maxKbps	入流量峰值（单位：kbps）。
dropKbps	丢弃的流量均值（单位：kbps）。
startTime	攻击开始时间。
endTime	攻击结束时间，为空时则表示攻击还未结束。
maxAttackInConn	攻击流量峰值时刻的连接数。
newConn	新建连接数。

表 1-10 攻击类型说明

数值	攻击类型
0-9	自定义服务攻击
10	Syn Flood攻击
11	Ack Flood攻击
12	SynAck Flood攻击
13	Fin/Rst Flood攻击
14	并发连接数超过阈值
15	新建连接数超过阈值
16	TCP分片报文攻击
17	TCP分片BandWidth limit攻击
18	TCP BandWidth limit攻击
19	UDP flood攻击
20	UDP分片攻击
21	UDP分片BandWidth limit攻击
22	UDP BandWidth limit攻击

数值	攻击类型
23	ICMP BandWidth limit攻击
24	Other BandWidth limit攻击
25	总流量限流
26	HTTPS Flood攻击
27	HTTP Flood攻击
28	保留
29	DNS Query Flood攻击
30	DNS Reply Flood攻击
31	Sip Flood攻击
32	黑名单丢弃
33	HTTP URL行为异常
34	TCP分片abnormal丢弃流量
35	TCP abnormal丢弃流量
36	UDP分片abnormal丢弃流量
37	UDP abnormal丢弃流量
38	ICMP abnormal攻击
39	Other abnormal攻击
40	Connection Flood攻击
41	域名劫持攻击
42	DNS投毒攻击报文
43	DNS反射攻击
44	超大DNS报文攻击
45	DNS源请求速率异常
46	DNS源回应速率异常
47	DNS域名请求速率异常
48	DNS域名回应包速率异常
49	DNS请求报文TTL异常
50	DNS报文格式异常
51	DNS Cache匹配丢弃攻击
52	端口扫描攻击

数值	攻击类型
53	TCP Abnormal攻击(tcp 报文标记位异常)
54	BGP攻击
55	UDP关联防范异常
56	DNS NO such Name异常
57	Other 指纹攻击
58	防护对象限流攻击
59	HTTP慢速攻击
60	恶意软件防范
61	域名阻断
62	FILTER过滤
63	Web攻击抓包
64	SIP源限速攻击

1.7 设置标签

标签由标签键和标签值组成，用于标识云资源。当您拥有相同类型的许多云资源时，可以使用标签按各种维度（例如用途、所有者或环境）对云资源进行分类。DDoS原生基础防护支持为防护的公网IP配置标签，方便管理。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 单击“公网IP”页签。

步骤4 在需要设置标签的公网IP所在行，单击“设置标签”。

图 1-9 设置标签

步骤5 在标签添加页面，单击“添加标签”。

步骤6 选择“标签键”和“标签值”。

- 手动设置标签：手动输入标签键和标签值。
- 选择已有标签：选择已有的标签。

图 1-10 添加标签

说明

如您的组织已经设定本服务的相关标签策略，则需按照标签策略规则为资源添加标签。标签如果不符合标签策略的规则，则可能会导致标签添加失败，请联系组织管理员了解标签策略详情。

步骤7 单击“确定”。

----结束

1.8 查看 Anti-DDoS 监控报表

操作场景

用户可以查看单个公网IP的监控详情，包括当前防护状态、当前防护配置参数、24小时的流量情况、24小时的异常事件等。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 选择“公网IP”页签，在待查看监控报表的公网IP地址所在行，单击“查看监控报表”。

图 1-11 查看监控报表

步骤4 在“监控报表”页面，可以查看该公网IP报表的详细指标，如图1-12和图1-13所示。

- 可查看包括当前防护状态、当前防护配置参数、24小时流量情况、24小时异常事件等信息。
- 24小时防护流量数据图，以5分钟一个数据点描绘的流量图，主要包括以下方面：
  - 流量图展示所选云服务器的流量情况，包括服务器的正常入流量以及攻击流量。
  - 报文速率图展示所选云服务器的报文速率情况，包括正常入报文速率以及攻击报文速率。
- 近1天内攻击事件记录表：近1天内云服务器的DDoS事件记录，包括清洗事件和黑洞事件。

图 1-12 查看流量监控报表

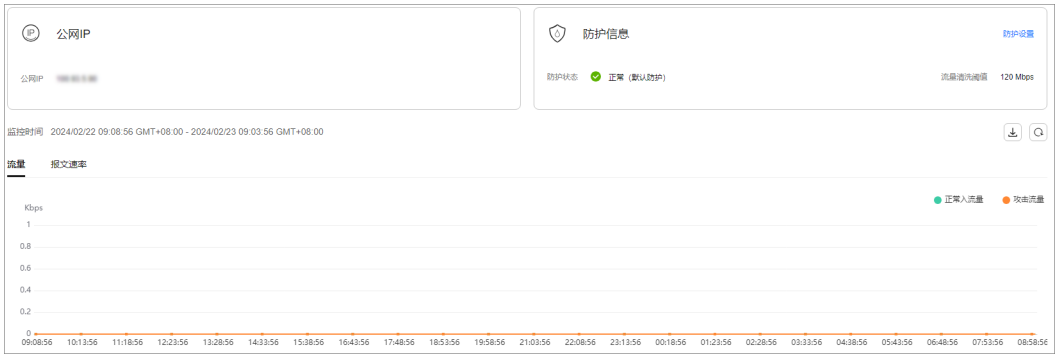
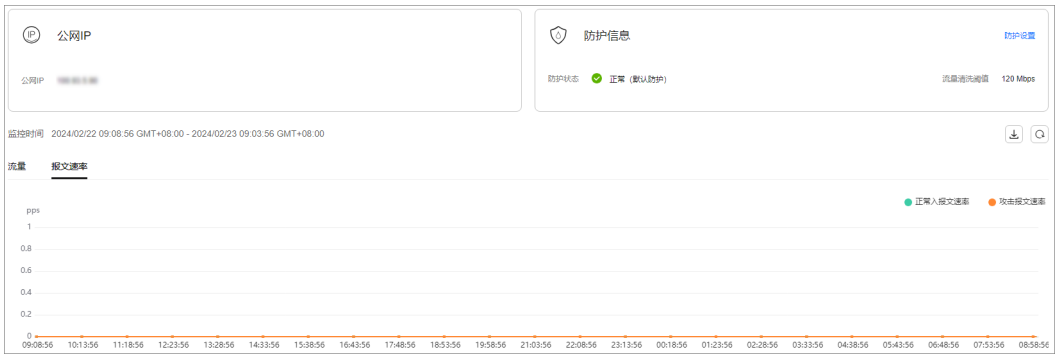


图 1-13 查看报文速率



说明

单击  ，可以将监控报表下载到本地，查看公网IP报表的详细指标信息。

----结束

1.9 查看 Anti-DDoS 拦截报告

操作场景

查看用户所有公网IP地址的防护统计信息，包括清洗次数、清洗流量，以及公网IP被攻击次数Top10和共拦截攻击次数。

操作步骤

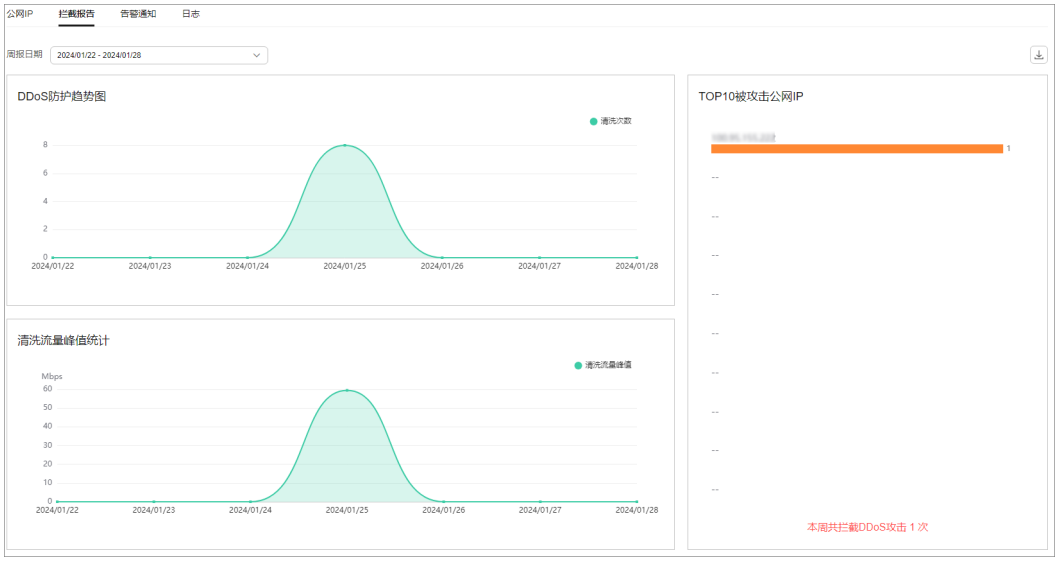
步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 选择“拦截报告”页签，可以查看用户所有公网IP地址的防护统计信息，如图1-14所示。

可通过选择“周报日期”来查看固定日期内的安全报告，查看时间范围为一周，支持查询前四周统计数据，包括清洗次数、清洗流量，以及公网IP被攻击次数Top10和共拦截攻击次数。

图 1-14 查看拦截报告



说明

单击  ，可以将拦截报表下载到本地，查看固定日期内的防护统计信息。

----结束

1.10 审计

1.10.1 云审计服务支持的 Anti-DDoS 操作列表

云审计服务（Cloud Trace Service，CTS）记录了Anti-DDoS相关的操作事件，方便用户日后的查询、审计和回溯，具体请参见云审计服务用户指南。

云审计服务支持的Anti-DDoS操作列表如**表1-11**所示。

表 1-11 CTS 支持的 Anti-DDoS 操作列表

操作名称	事件名称
开启Anti-DDoS防护	OPEN_ANTIDDOS
修改Anti-DDoS防护配置	UPDATE_ANTIDDOS
设置LTS全量日志配置	UPDATE_LTS_CONFIG
批量添加/编辑TMS资源标签	UPDATE_RESOURCE_TAGS
批量删除TMS资源标签	DELETE_RESOURCE_TAGS
更新租户的告警提醒配置情况	UPDATE_ALERT_CONFIG
修改流量清洗阈值默认档位	UPDATE_DEFAULT_CONFIG
删除流量清洗阈值默认档位	DELETE_DEFAULT_CONFIG

1.10.2 查看云审计日志

开启了云审计服务后，系统开始记录Anti-DDoS资源的操作。云审计服务管理控制台保存最近7天的操作记录。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左侧的 ☰，选择“管理与监管 > 云审计服务”，进入云审计服务信息页面。

步骤3 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤4 在下拉框中选择“云服务”，输入“Anti-DDoS”，按“Enter”。

步骤5 在查询结果中单击事件名称，查看事件详情。

事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：

- 事件名称、资源名称、资源ID、事件ID：需要输入某个具体的名称或ID。
  - 资源名称：当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。
  - 资源ID：当该资源类型无资源ID或资源创建失败时，该字段为空。
- 云服务、资源类型：在下拉框中选择对应的云服务名称或资源类型。

- 操作用户：在下拉框中选择一个或多个具体的操作用户。
- 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
  - normal：表示操作成功。
  - warning：表示操作失败。
  - incident：表示比操作失败更严重的情况，如引起其他故障等。
- 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近1周内任意时间段的操作事件。

----结束

1.11 权限管理

1.11.1 创建用户并授权使用 Anti-DDoS

如果您需要对您所拥有的Anti-DDoS进行精细的权限管理，）您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用Anti-DDoS资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将Anti-DDoS资源委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用Anti-DDoS服务的其它功能。

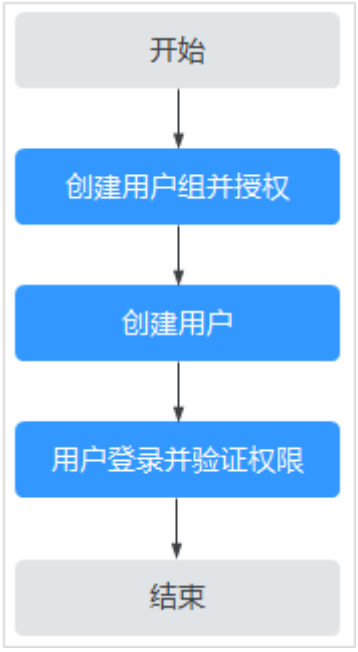
本章节为您介绍对用户授权的方法，操作流程如**图1-15**所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的Anti-DDoS权限，并结合实际需求进行选择，Anti-DDoS支持的系统权限，请参见：**Anti-DDoS系统权限**。如果您需要对除Anti-DDoS之外的其它服务授权，IAM支持服务的所有权限请参见**系统权限**。

示例流程

图 1-15 给用户授权服务权限流程



1. **创建用户组并授权**。

   在IAM控制台创建用户组，并授予Anti-DDoS服务的管理员权限“Anti-DDoS Administrator”。

2. **创建用户并加入用户组**。

   在IAM控制台创建用户，并将其加入**1**中创建的用户组。

3. **用户登录**并验证权限。

   新创建的用户登录控制台，切换至授权区域，验证权限：

   单击页面左上方的 ☰，选择除Anti-DDoS服务外的任一服务，如果提示权限不足，表示“Anti-DDoS Administrator”已生效。

1.11.2 Anti-DDoS 自定义策略

如果系统预置的Anti-DDoS权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参见**Anti-DDoS权限及授权项**。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的Anti-DDoS自定义策略样例。

Anti-DDoS 自定义策略样例

- 示例1：授权用户查询Anti-DDoS默认防护策略

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "anti-ddos:defaultDefensePolicy:get"
                        ]
        }
    ]
}
```

1.11.3 Anti-DDoS 权限及授权项

如果您需要对您所拥有的Anti-DDoS进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，IAM），如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用Anti-DDoS的其它功能。

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为**角色**和**策略**。角色以服务为粒度，是IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。策略授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。

- 权限：允许或拒绝某项操作。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。

权限	授权项	依赖关系说明
查询Anti-DDoS默认防护策略	anti-ddos:defaultDefensePolicy:get	-
配置Anti-DDoS默认防护策略	anti-ddos:defaultDefensePolicy:create	-
删除Anti-DDoS默认防护策略	anti-ddos:defaultDefensePolicy:delete	-
查询Anti-DDoS配置可选范围	anti-ddos:optionalDefensePolicy:list	-

权限	授权项	依赖关系说明
查询Anti-DDoS服务	anti-ddos:ip:getDefensePolicy	vpc:publicIps:list
更新Anti-DDoS服务	anti-ddos:ip:updateDefensePolicy	-
开通Anti-DDoS服务	anti-ddos:ip:enableDefensePolicy	-
查询周防护统计情况	anti-ddos:ip:getWeeklyReport	-
查询指定EIP防护流量	anti-ddos:ip:getDailyTrafficReport	-
查询指定EIP异常事件	anti-ddos:ip:getDailyEventReport	-
查询指定EIP防护状态	anti-ddos:ip:getDefenseStatus	-
查询EIP防护状态列表	anti-ddos:ip:listDefenseStatuses	-
查询Anti-DDoS任务	anti-ddos:task:list	-
查询告警配置信息	anti-ddos:alertConfig:get	smn:topic:list
更新告警配置信息	anti-ddos:alertConfig:update	-
查询云日志服务配置	anti-ddos:logConfig:get	-
更新云日志服务配置	anti-ddos:logConfig:update	-
查询配额	anti-ddos:quota:list	-
查询资源标签列表	anti-ddos:ip:listTagsForResource	-
批量添加标签	anti-ddos:ip:tagResource	-
批量删除标签	anti-ddos:ip:untagResource	-

2 DDoS 原生高级防护操作指南

2.1 使用概览

开通DDoS原生高级防护，将华为云公网IP资源绑定到实例后，DDoS原生高级防护提供的安全能力就可以直接加载到云服务。

DDoS原生高级防护的使用概览如**表2-1**所示。

表 2-1 使用概览

子流程	说明
购买DDoS原生高级防护实例	详细操作请参见**购买实例**。
配置防护策略	DDoS原生高级防护提供了丰富全面的防护规则，您可以根据业务需求配置相应的防护策略。详细操作请参见**添加防护策略**。
添加防护对象	将华为云上的公网IP资源添加为防护对象，才能为公网IP资源开启DDoS原生高级防护。详细操作请参见**添加防护对象**。
开启告警通知	开启告警通知后，当IP遭受DDoS攻击时，您可以第一时间接收告警通知。详细操作请参见**设置告警通知**。
查看数据报表	可查看到昨天、今天、3天范围内的访问与攻击统计次数等信息。详细操作请参见**查看数据报表**。
管理实例	开通续费、升级规格、配置标签等常用实例管理操作。详细操作请参见**管理实例**。
设置事件告警通知	通过云监控服务，对防护的弹性公网IP启用事件监控，当出现清洗、封堵、解封等事件时进行告警。详细操作请参见**设置事件告警通知**。

2.2 购买实例

在使用DDoS原生高级防护前，您需要购买DDoS原生高级防护实例。购买成功后，DDoS原生高级防护立即生效。

DDoS原生高级防护支持DDoS原生防护-全力防基础版、DDoS原生防护-全力防高级版两种服务版本，请您根据业务需求，购买对应版本。有关DDoS原生高级防护各版本详细的功能规格介绍，请参见**功能特性和业务规格**。

前提条件

购买DDoS原生防护前，已成功申请开通服务版本。

说明

进入“购买DDoS防护”界面，“实例类型”选择“DDoS原生防护”后，在界面右下角单击“立即申请”，按界面提示信息，申请开通。

规格限制

DDoS原生防护-全力防高级版只能防护专属EIP。您可以**提交工单**联系DDoS防护团队开通专属EIP购买权限。

约束限制

请确认购买实例的账号同时具有“CNAD FullAccess”和“BSS Administrator”角色，或者该账号具有“Tenant Administrator”角色。

购买 DDoS 原生防护-全力防基础版

步骤1 **登录管理控制台**。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在界面右上角，单击“购买DDoS防护”，进入“购买DDoS防护”页面。

步骤4 “实例类型”选择“DDoS原生防护”。

步骤5 “防护规格”选择“全力防基础版”。

步骤6 设置规格参数，如**图2-1**所示，相关参数说明如**表2-2**所示。

图 2-1 设置 DDoS 原生防护-全力防基础版防护规格

表 2-2 DDoS 原生防护-全力防基础版规格参数说明

参数	说明
资源所在地	选择防护资源所在的区域。 **须知** DDoS原生防护实例只能防护相同区域的云资源，不能跨Region防护。例如，华东-上海一的云原生防护实例只能防护华东一上海一的云资源。
防护IP数	取值范围为50～500，且防护IP数必须设置为5的倍数。
业务带宽	业务带宽是高防机房清洗后回源给源站的业务流量带宽。

步骤7 设置“实例名称”，选择“购买时长”和“购买数量”后，在界面右下角单击“立即购买”。

- 购买时长：可以选择3个月、6个月或1年。
- 购买数量：选择购买的实例个数。

说明

勾选“自动续费”后，当服务期满时，系统会自动按照购买周期进行续费。

步骤8 在“订单详情”页面，如果您确认订单无误，单击“去支付”。

步骤9 在“购买DDoS防护”的支付界面，单击“确认付款”，完成订单支付。

付款成功后，系统跳转至DDoS防护实例列表界面。当实例状态为“正常”时，说明实例创建成功。

----结束

购买 DDoS 原生防护-全力防高级版

说明

购买DDoS原生防护-全力防高级版前请确认已知晓全力防高级版只能防护专属EIP。

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在界面右上角，单击“购买DDoS防护”，进入“购买DDoS防护”页面。

步骤4 “实例类型”选择“DDoS原生防护”。

步骤5 “防护规格”选择“全力防高级版”。

步骤6 设置规格参数，相关参数说明如表2-3所示。

图 2-2 设置 DDoS 原生防护-全力防高级版防护规格

表 2-3 DDoS 原生防护-全力防高级版规格参数说明

参数	说明
资源所在地	选择防护资源所在的区域。 **须知** DDoS原生防护实例只能防护相同区域的云资源，不能跨Region防护。例如，华东-上海一的云原生防护实例只能防护华东一上海一的云资源。
防护IP数	取值范围为50～500，且防护IP数必须设置为5的倍数。

参数	说明
业务带宽	业务带宽是高防机房清洗后回源给源站的业务流量带宽。 取值范围：100M~40,000M

步骤7 设置“实例名称”，选择“购买时长”和“购买数量”后，在界面右下角单击“立即购买”。

- 购买时长：可以选择3个月、6个月或1年。
- 购买数量：选择购买的实例个数。

说明

勾选“自动续费”后，当服务期满时，系统会自动按照购买周期进行续费。

步骤8 在“订单详情”页面，如果您确认订单无误，单击“去支付”。

步骤9 在“购买DDoS防护”的支付界面，单击“确认付款”，完成订单支付。

付款成功后，系统跳转至DDoS防护实例列表界面。当实例状态为“正常”时，说明实例创建成功。

----结束

2.3 添加防护策略

2.3.1 配置清洗阈值

当IP遭受的DDoS攻击带宽超过配置的清洗阈值时，触发DDoS原生高级防护对攻击流量进行清洗，保障您的业务可用。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 防护策略”，进入DDoS原生高级防护“防护策略”页面。

步骤4 在防护策略列表的左上方，单击“创建策略”。

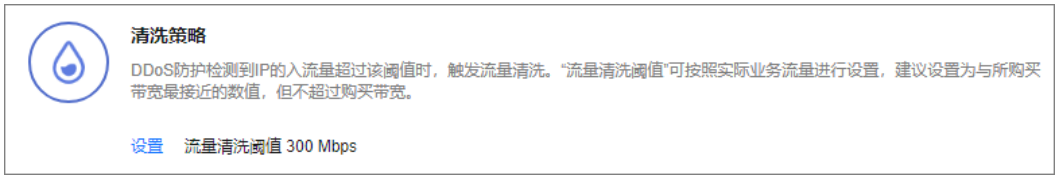
步骤5 在弹出的“创建策略”对话框中，设置“策略名称”并选择所属实例后，单击“确定”。

图 2-3 创建策略

步骤6 在目标防护策略所在行的“操作”列中，单击“配置策略”。

步骤7 在“清洗策略”配置框中，单击“设置”，如图2-4所示。

图 2-4 清洗策略配置框



步骤8 在弹出的“清洗策略设置”对话框中，设置流量清洗阈值，如图2-5所示。

图 2-5 设置流量清洗阈值

步骤9 单击“确定”。

----结束

2.3.2 水印防护

2.3.2.1 配置水印防护

通过在业务端共享水印算法和关键字，客户端发出的报文都镶嵌入水印特征，能有效抵御四层CC攻击。

约束条件

一个水印最多可以配置两条关键字。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 防护策略”，进入DDoS原生高级防护“防护策略”页面。

步骤4 在防护策略列表的左上方，单击“创建策略”。

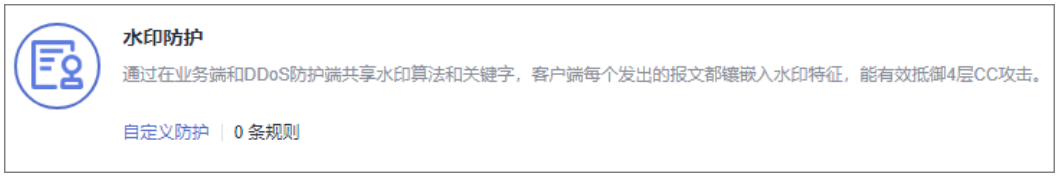
步骤5 在弹出的“创建策略”对话框中，设置“策略名称”并选择所属实例后，单击“确定”。

图 2-6 创建策略

步骤6 在目标防护策略所在行的“操作”列中，单击“配置策略”。

步骤7 在“水印防护”配置框中，单击“自定义防护”。

图 2-7 水印防护配置框



步骤8 在弹出的“水印防护设置”页面中，单击“新建水印”。

步骤9 在“新建水印”对话框中，设置水印参数。

图 2-8 新建水印

表 2-4 水印参数说明

参数	说明
水印名称	输入水印名称。
协议	当前仅支持UDP协议。
关键字	输入关键字，最多可输入两个关键字。
端口范围	支持的端口范围为1~65535。

步骤10 单击“确定”，水印添加成功。

说明

如您需要详细的水印配置指导，请参考**水印防护配置指导**章节。

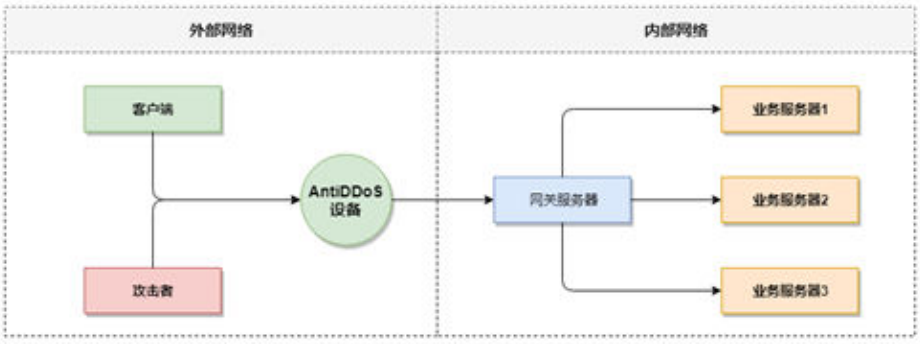
----结束

2.3.2.2 水印防护配置指导

2.3.2.2.1 基本原理

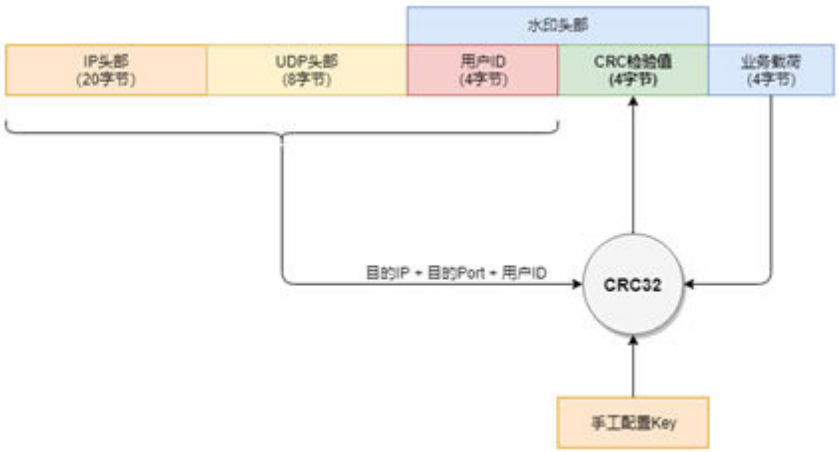
通常UDP Flood的防御方式有两种，一种是动态指纹学习，一种是UDP限流，前者可能会将正常的业务载荷学习成攻击指纹，容易造成误杀，后者会将正常流量和攻击流量一起进行阻断，影响您的正常业务使用。

图 2-9 设备防护原理图



如图2-10所示，华为云解决方案通过在UDP报文中增加水印头部信息，用以标识正常的业务报文，线下AntiDDoS设备在接收到UDP报文后，通过检查UDP水印的正确性，可以高效准确放行正常的业务报文，阻断攻击报文。

图 2-10 水印解决方案



客户端和AntiDDoS设备需要使用相同的信息结构和计算规则，其中计算规则是指计算水印值的哈希因子和哈希算法，在本方案中，哈希因子使用了目的IP、目的端口、用户标识和水印关键字，哈希算法使用CRC32。

2.3.2.2.2 开发示例

本节主要以C语言进行示例，指导**客户端开发人员**如何在客户端实现UDP水印的计算和添加，开发人员可以根据实现开发平台进行代码调整。

计算 CRC 哈希值代码示例

注意

本章节的CRC算法使用CRC-32-IEEE 802.3。

- 初始化CRC表：

```
unsigned int g_szCRCTable[256];
void CRC32TableInit(void)
```

```
{
    unsigned int c;
    int n, k;
    for (n = 0; n < 256; n++) {
        c = (unsigned int)n;
        for (k = 0; k < 8; k++) {
            if (c & 1) {
                c = 0xedb88320 ^ (c >> 1);
            }
            else {
                c = c >> 1;
            }
        }
        g_szCRCTable[n] = c;
    }
}
```

- 计算CRC哈希值的接口，其中第一个参数crc默认使用0即可。

```
unsigned int CRC32Hash(unsigned int crc, unsigned char* buf, int len)
{
    unsigned int c = crc ^ 0xFFFFFFFF;
    int n;
    for (n = 0; n < len; n++) {
        c = g_szCRCTable[(c ^ buf[n]) & 0xFF] ^ (c >> 8);
    }
    return c ^ 0xFFFFFFFF;
}
```

计算报文的水印值示例代码

计算水印信息结构如图2-11所示。

图 2-11 计算水印信息结构图

- 水印数据结构定义如下代码所示

```
typedef struct {
    unsigned int   userId;    /* 用户标识ID */
    unsigned int   payload;   /* 业务载荷 */
    unsigned short destPort;  /* 业务目的端口 */
    unsigned short rsv;       /* 保留字段，2字节填充 */
    unsigned int   destIp;    /* 业务目的IP */
    unsigned int   key;       /* 水印关键字 */
} UdpWatermarkInfo;
```

⚠ 注意

- 字节序需要使用网络序。
- 业务载荷不满4字节的，使用0进行填充。

- 计算CRC哈希值可以使用CPU硬件加速接口进行替换，以提升处理性能。

```
unsigned int UdpFloodWatermarkHashGet(unsigned int userId, unsigned int payload, unsigned short
destPort, unsigned int destIp, unsigned int key)
{
    UdpWatermarkInfo stWaterInfo;

    stWaterInfo.destIp   = destIp;
```

```
    stWaterInfo.destPort = destPort;
    stWaterInfo.userId   = userId;
    stWaterInfo.payload  = payload;
    stWaterInfo.key      = key;
    stWaterInfo.rsv      = 0;

    return CRC32Hash(0, (UCHAR *)&stWaterInfo, sizeof(stWaterInfo));
}
```

填充报文 UDP 水印

将计算出的CRC哈希值，按图2-12结构填充到报文中，然后发送出去。

图 2-12 填充报文 UDP 水印

2.3.3 配置 IP 黑白名单

通过配置IP黑名单或IP白名单来封禁或者放行访问DDoS防护的源IP，从而限制访问您业务资源的用户。

规格限制

每条规则最多可以添加200条黑/白名单IP。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 防护策略”，进入DDoS原生高级防护“防护策略”页面。

步骤4 在防护策略列表的左上方，单击“创建策略”。

步骤5 在弹出的“创建策略”对话框中，设置“策略名称”并选择所属实例后，单击“确定”。

图 2-13 创建策略

步骤6 在目标防护策略所在行的“操作”列中，单击“配置策略”。

步骤7 在“IP黑白名单”配置框中，单击“自定义防护”，如图2-14所示。

图 2-14 IP 黑白名单配置框

步骤8 在弹出的“IP黑白名单设置”页面中，选择“黑名单”或“白名单”页签后，单击“添加”。

图 2-15 添加 IP

步骤9 在弹出的对话框中，输入黑名单IP/IP段（需要拦截的IP）或白名单IP/IP段（需要放行的IP）后，单击“确定”，如图2-16和图2-17所示。

图 2-16 添加黑名单 IP

图 2-17 添加白名单 IP

----结束

相关操作

- 选择“黑名单”页签，单击操作列的“删除”或批量勾选要删除的黑名单，在列表左上方单击“删除”，被删除的黑名单IP，设备将不再拦截其访问流量。
- 选择“白名单”页签，单击操作列的“删除”或批量勾选要删除的白名单，在列表左上方单击“删除”，被删除的白名单IP，设备将不再直接放行其访问流量。

2.3.4 配置端口封禁

您根据端口封禁规则，封禁访问DDoS原生高级防护的源流量。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 防护策略”，进入DDoS原生高级防护“防护策略”页面。

步骤4 在防护策略列表的左上方，单击“创建策略”。

步骤5 在弹出的“创建策略”对话框中，设置“策略名称”并选择所属实例后，单击“确定”。

图 2-18 创建策略

步骤6 在目标防护策略所在行的“操作”列中，单击“配置策略”。

步骤7 在“端口封禁”配置框中，单击“自定义防护”。

图 2-19 端口封禁配置框

步骤8 在弹出的“端口封禁设置”对话框中，单击“新建端口ACL”。

步骤9 在弹出的对话框中，设置端口ACL。

图 2-20 新建端口 ACL

表 2-5 端口 ACL 参数说明

参数	说明
端口规则名称	输入规则名称。
协议	设置封禁端口的协议。支持TCP、UDP。
端口类型	设置封禁端口的类型。
开始端口-结束端口	设置封禁端口的范围。
匹配后动作值	封禁端口匹配后的防护动作。

步骤10 单击“确定”。

----结束

后续处理

- 在目标端口所在行“操作”列，单击“删除”可以删除封禁端口规则。
- 在目标端口所在行“操作”列，单击“编辑”可以修改封禁端口规则信息。

2.3.5 配置协议封禁

根据协议类型一键封禁访问DDoS防护的源流量，支持封禁UDP/TCP/ICMP协议。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 防护策略”，进入DDoS原生高级防护“防护策略”页面。

步骤4 在防护策略列表的左上方，单击“创建策略”。

步骤5 在弹出的“创建策略”对话框中，设置“策略名称”并选择所属实例后，单击“确定”。

图 2-21 创建策略

步骤6 在目标防护策略所在行的“操作”列中，单击“配置策略”。

步骤7 在“协议封禁”配置框中，单击“设置”，如图2-22所示。

图 2-22 协议封禁配置框

步骤8 在弹出的“协议封禁设置”对话框中，选择开启或关闭封禁的协议，单击“确定”。

图 2-23 设置协议封禁

-  ：开启封禁，可以阻止UDP/TCP/ICMP协议流量访问。
-  ：关闭封禁，允许UDP/TCP/ICMP协议流量访问。

----结束

2.3.6 配置指纹过滤

您可以通过配置指纹过滤防护规则，对数据包中指定位置的内容进行特征匹配，根据匹配结果设置丢弃或限速规则。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 防护策略”，进入DDoS原生高级防护“防护策略”页面。

步骤4 在防护策略列表的左上方，单击“创建策略”。

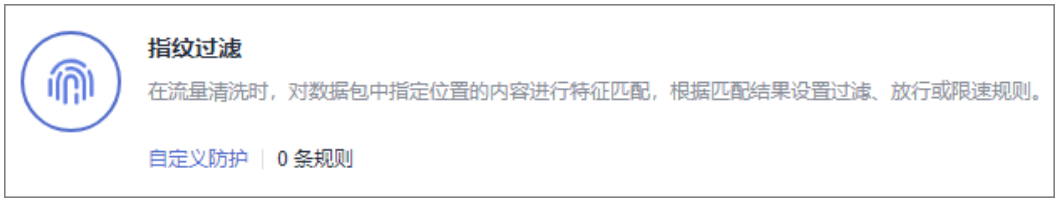
步骤5 在弹出的“创建策略”对话框中，设置“策略名称”并选择所属实例后，单击“确定”。

图 2-24 创建策略

步骤6 在目标防护策略所在行的“操作”列中，单击“配置策略”。

步骤7 在“指纹过滤”配置框中，单击“自定义防护”。

图 2-25 指纹过滤配置框



步骤8 在弹出的“指纹过滤设置”对话框中，单击“新建指纹”。

步骤9 在弹出的对话框中，设置指纹参数。

图 2-26 新建指纹

表 2-6 指纹参数说明

参数	说明
指纹名称	输入指纹规则名称。
协议	设置指纹的协议。
开始源端口-结束源端口	设置指纹源端口的范围。
开始目的端口-结束目的端口	设置指纹目的端口的范围。
匹配后动作值-限速值	设置匹配指纹规后的动作以及限速值，可以选择“丢弃”或“放行”动作。
检测载荷	设置检测载荷的十六进制值。
偏移量	设置指纹的偏移量。
检查深度	“检测载荷”为“1234afee”，“偏移量”为“20”，“检查深度”为“8”时，当数据区的第21个字节到第32个字节的内容匹配“1234afee”时，则认为此报文命中指纹。其中32=20+4（指纹长度）+8（检查深度）。

步骤10 单击“确定”。

----结束

后续处理

- 在目标端口所在行“操作”列，单击“删除”可以删除指纹过滤规则。
- 在目标端口所在行“操作”列，单击“编辑”可以修改指纹过滤规则的信息。

2.3.7 配置连接防护

须知

连接防护功能目前还处于公测阶段，仅DDoS原生高级防护-全力防高级版的华北地区支持该功能，如果您需要此项功能请提交工单开通。

如果同一个源站IP短时间内频繁发起大量异常连接状态的报文时，您可以通过配置连接防护，将该源站IP纳入黑名单中进行封禁惩罚，等封禁结束后可恢复访问。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 防护策略”，进入DDoS原生高级防护“防护策略”页面。

步骤4 在防护策略列表的左上方，单击“创建策略”。

步骤5 在弹出的“创建策略”对话框中，设置“策略名称”并选择所属实例后，单击“确定”。

图 2-27 创建策略

步骤6 在目标防护策略所在行的“操作”列中，单击“配置策略”。

步骤7 在“连接防护”配置框中，单击“设置”。

图 2-28 连接防护配置框

步骤8 开启“TCP连接耗尽攻击防御”，在弹出的对话框中，设置连接防护参数。

图 2-29 连接防护设置

表 2-7 连接防护设置参数说明

参数	说明
目的IP地址并发连接数检查	当目的IP地址的TCP并发连接数大于“连接数阈值”时，启动针对TCP连接耗尽攻击的防御。防御启动后，开始对源IP地址进行检查。设置范围：1-80000000。
目的IP地址新建连接速率检查	当目的IP地址每秒新增加的TCP连接数大于“连接速率阈值”时，启动针对TCP连接耗尽攻击的防御。防御启动后，开始对源IP地址进行检查。设置范围：1-10000000。
源IP地址新建连接速率检查	源IP地址新建连接速率检查：当针对TCP连接耗尽攻击的防御启动后，如果某个源IP地址在“检查周期”内发起的TCP连接数大于“连接数阈值”，则将该源IP地址作为攻击源上报ATIC管理中心。设置范围范围：连接数，1-80000000；时间周期，1-60（s）。
源IP地址连接数检查	当针对TCP连接耗尽攻击的防御启动后，如果某个源IP地址的TCP并发连接数大于“连接数阈值”值，则将该源IP地址作为攻击源上报ATIC管理中心。设置范围：1-80000000。

步骤9 单击“确定”。

----结束

2.3.8 配置区域封禁

您可以配置区域封禁，禁止一些地区的流量访问您的服务。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 防护策略”，进入DDoS原生高级防护“防护策略”页面。

步骤4 在防护策略列表的左上方，单击“创建策略”。

步骤5 在弹出的“创建策略”对话框中，设置“策略名称”并选择所属实例后，单击“确定”。

图 2-30 创建策略

步骤6 在目标防护策略所在行的“操作”列中，单击“配置策略”。

步骤7 在“区域封禁”配置框中，单击“设置”。

图 2-31 区域封禁设置

步骤8 在弹出的对话框中勾选需要封禁的区域。

图 2-32 选择封禁区域

说明

当前DDoS原生高级防护仅支持“海外地区”封禁。

步骤9 单击“确定”，完成区域封禁设置。

----结束

2.4 添加防护对象

开通DDoS原生高级防护后，您需要将华为云上的公网IP资源添加为防护对象，才能为公网IP资源开启DDoS原生高级防护。

前提条件

已成功购买DDoS原生高级防护实例。

约束条件

- 添加的防护对象（例如ECS、ELB、WAF、EIP等）IP资源所在区域与购买的DDoS原生高级防护实例区域相同。
- DDoS原生高级防护-全力防高级版只能防护专属EIP，专属EIP只能绑定到全力防高级版实例上。

操作步骤

步骤1 登录管理控制台。

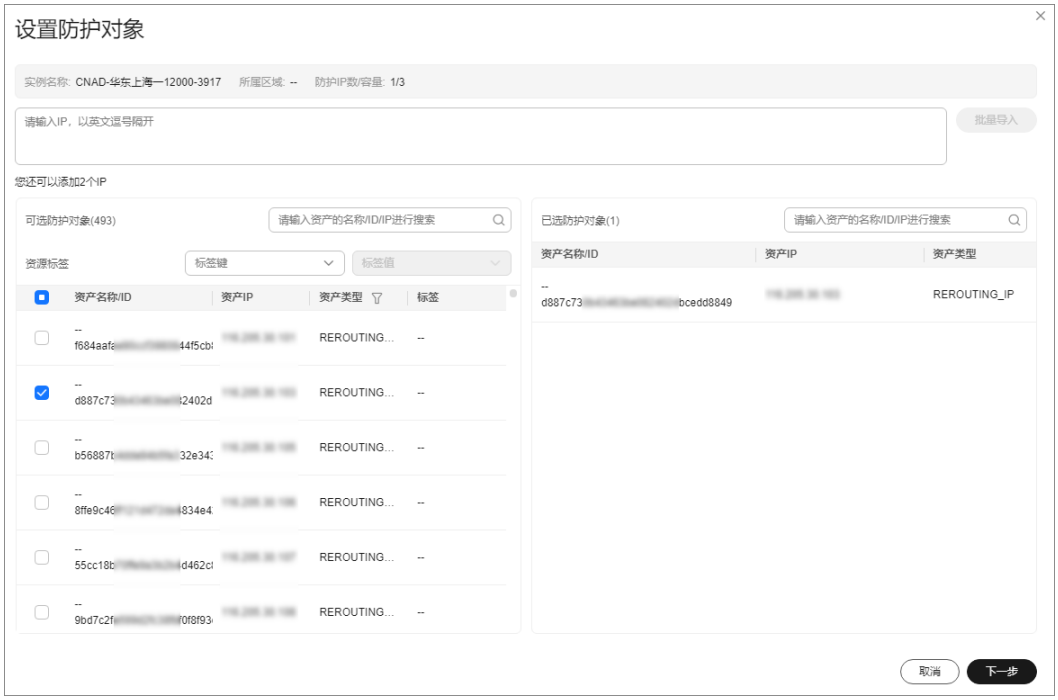
步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 实例列表”，进入DDoS原生高级防护“实例列表”页面。

步骤4 在目标实例所在框的右上方，单击“设置防护对象”。

步骤5 在弹出的“设置防护对象”对话框中，勾选需要防护的IP后，单击“下一步”。

图 2-33 设置防护对象



说明

- “可选防护对象”中为未添加到DDoS原生高级防护的IP。
- 支持批量导入防护IP。

步骤6 确认防护对象的设置，并且在下方选择IP防护策略，单击“确定”完成防护对象的设置。

图 2-34 确认防护对象设置

说明

防护策略的设置详见**添加防护策略**。

----结束

相关操作

- 您可以在实例区域框中，在“防护IP数”行后单击“查看”，查看当前实例的防护对象。

- 如果IP资源不需要DDoS原生高级防护进行防护，可以移除该IP。有关移除防护对象的详细操作，请参见**管理防护对象**。
- **配置标签**：在目标防护对象所在行的“标签”列中，单击。输入标签名称后，单击“确定”。

2.5 设置告警通知

开启告警通知后，当IP遭受DDoS攻击时，您将接收到告警通知信息（接收消息方式由您设置）。

前提条件

已成功购买DDoS原生高级防护实例。

约束条件

- 消息通知服务为付费服务，价格详情请参见**SMN价格详情**。
- 只支持显示和DDoS原生高级防护同一区域的通知主题。

操作步骤

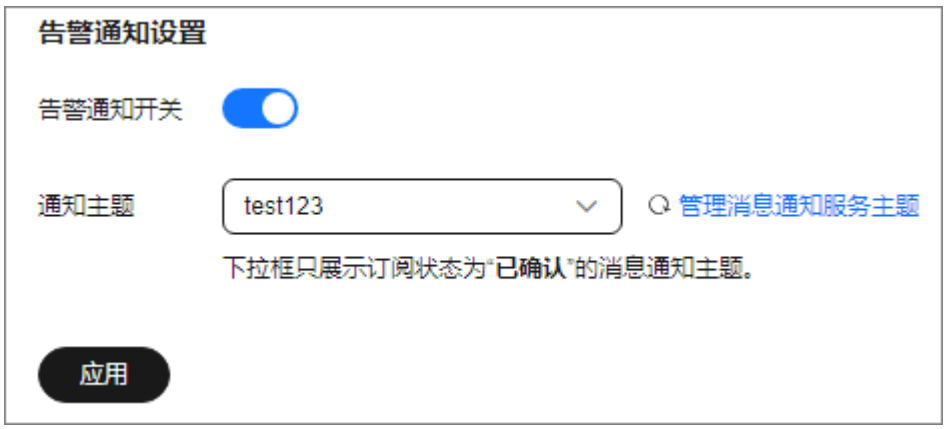
步骤1 **登录管理控制台**。

步骤2 在页面上方选择“区域”后，单击页面左上方的，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 告警通知”，进入“告警通知设置”页面。

步骤4 在“告警通知设置”页面，开启告警通知，即将告警通知开关设置为。

图 2-35 “告警通知设置”对话框



在“通知主题”下拉列表选择已创建的主题或者单击“管理消息通知服务主题”创建新的主题，用于配置接收告警通知的终端。

单击“管理消息通知服务主题”创建新主题的操作步骤如下：

1. 参见**创建主题**创建一个主题。
2. 参见**添加订阅**配置接收告警通知的手机号码、邮件地址等终端，即为创建的主题添加一个或多个订阅。

更多关于主题和订阅的信息，请参见《消息通知服务用户指南》。

步骤5 单击“应用”，告警通知设置完成。

----结束

相关操作

如需关闭告警通知，在**图2-35**中，关闭告警通知，即将告警通知开关设置为  。

2.6 防护日志管理

2.6.1 查看数据报表

DDoS原生高级防护从流量趋势和报文速率两个维度展示正常流量和攻击流量信息，您可以通过查看正常流量和攻击流量的信息，了解当前网络安全状态。

在“数据报表”页面，您可以查看实例的攻击源、接收流量、攻击流量，以及DDoS防护趋势图、清洗流量峰值、攻击类型分布、TOP10被攻击IP等信息。

前提条件

已添加防护对象并配置防护策略。

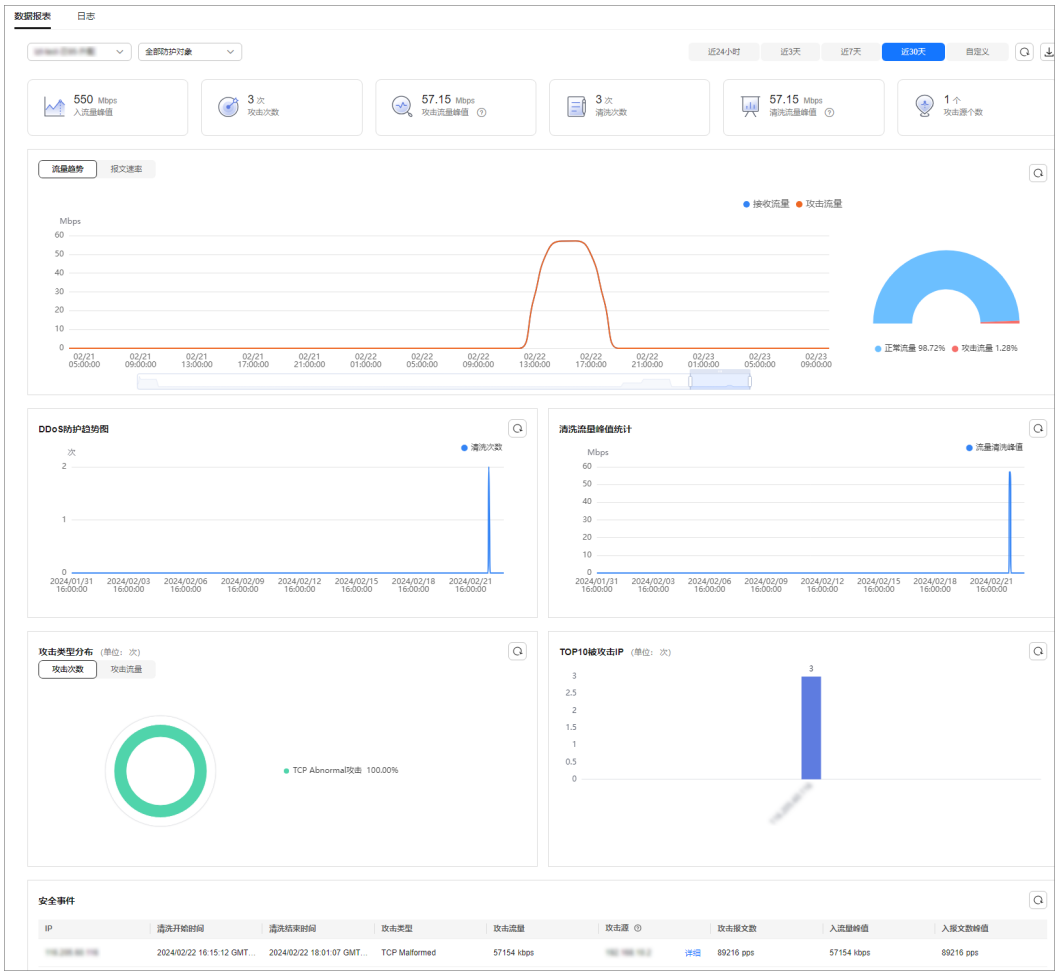
操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面上方选择“区域”后，单击页面左上方的，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 数据报表”，进入DDoS原生高级防护“数据报表”页面。

图 2-36 数据报表页面

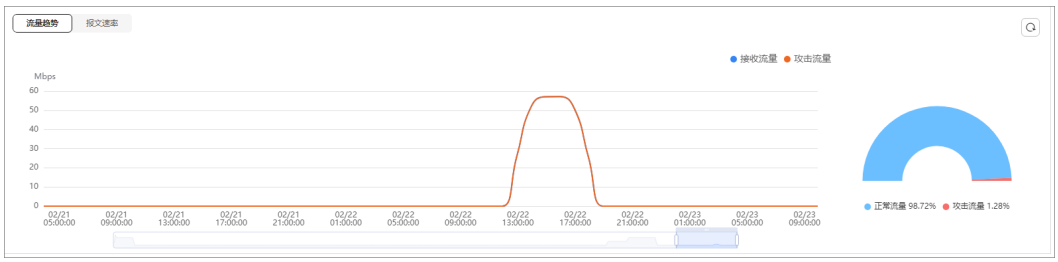


说明

- 单击攻击源IP后的“详细”，可以查看完整的攻击源IP列表。
- 攻击中的事件，单击“查看动态黑名单”，可以查看攻击中的黑名单列表。
- 进行中的攻击事件可能不展示攻击源。
- 一些只包含部分攻击类型的攻击事件不含攻击源。
- 攻击源随机采样，不是全量的攻击源信息。

步骤4 选择“流量趋势”页签，查看流量趋势防护信息。

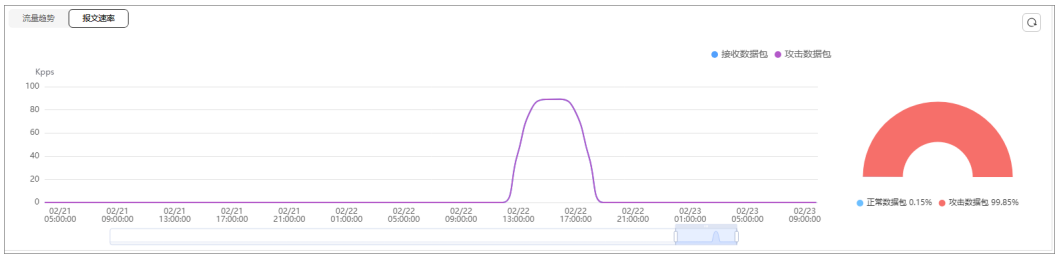
图 2-37 查看流量趋势防护信息



在界面右上角单击，可以将防护日志下载到本地。

步骤5 选择“报文速率”页签，查看报文速率详细信息。

图 2-38 报文速率



在界面右上角单击，可以将防护日志下载到本地。

----结束

2.7 管理实例

2.7.1 查看实例信息

开通DDoS原生高级防护后，您可以查看实例信息。

前提条件

已成功购买DDoS原生高级防护实例。

操作步骤

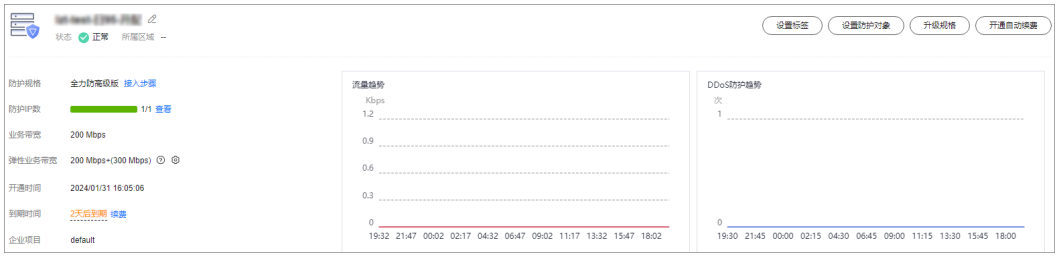
步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 实例列表”，进入DDoS原生高级防护“实例列表”页面。

步骤4 查看实例信息。

图 2-39 实例页面



----结束

2.7.2 配置实例标签

标签由标签键和标签值组成，用于标识云资源。当您拥有相同类型的许多云资源时，可以使用标签按各种维度（例如用途、所有者或环境）对云资源进行分类。DDoS实例支持配置标签，方便管理实例。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 实例列表”，进入“实例列表”页面。

步骤4 在目标实例所在行，单击“设置标签”。

图 2-40 设置标签

步骤5 在标签添加页面，单击“添加标签”。

步骤6 选择“标签键”和“标签值”。

- 手动设置标签：手动输入标签键和标签值。
- 选择已有标签：选择已有的标签。

图 2-41 添加标签

说明

如您的组织已经设定本服务的相关标签策略，则需按照标签策略规则为资源添加标签。标签如果不符合标签策略的规则，则可能会导致标签添加失败，请联系组织管理员了解标签策略详情。

步骤7 单击“确定”。

----结束

2.8 管理防护对象

2.8.1 查看防护对象信息

添加防护对象后，您可以查看防护对象详细信息。

前提条件

已添加防护对象。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 防护对象”，进入“防护对象”页面。

图 2-42 防护对象

步骤4 查看防护对象信息，相关参数说明如表2-8所示。

表 2-8 防护对象相关参数说明

参数	说明
防护IP	CNAD防护的IP资源。
标签	防护IP设置的标签信息。
状态	防护IP的防护状态。 • 正常 • 策略下发中
防护策略	防护IP所配置的防护策略。
所属区域	防护IP所在的区域。
所属实例	防护IP所在的实例。
操作	• 单击“查看报表”，跳转到数据报表页面，查看防护数据信息。 • 防护IP未配置防护策略时，单击设置策略，可以为防护IP选择防护策略。

----结束

2.8.2 为防护对象设置防护策略

您需要为添加的防护对象选择防护策略，防护对象才能使用DDoS原生高级防护策略，抵御DDoS攻击。

前提条件

- 已创建防护策略并配置防护策略。
- 已添加防护对象。
- 防护对象未配置防护策略。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

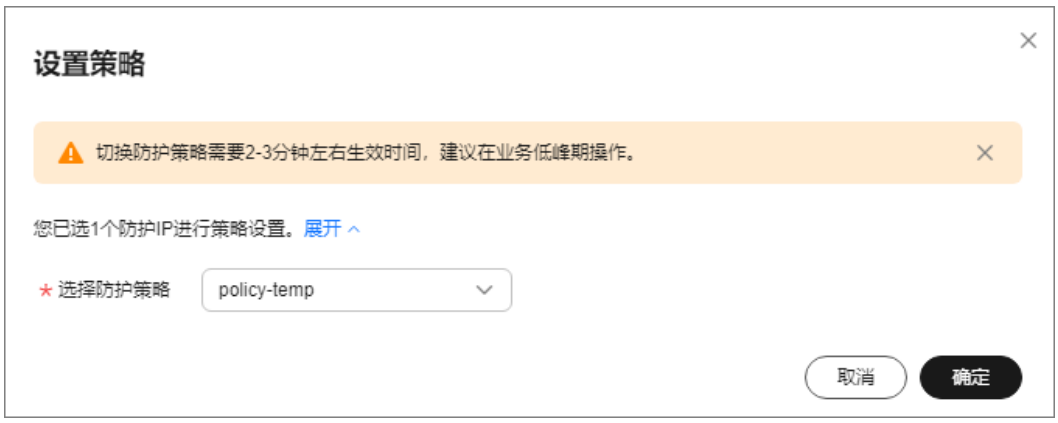
步骤3 在左侧导航栏选择“DDoS原生高级防护 > 防护对象”，进入“防护对象”页面。

图 2-43 防护对象

步骤4 在目标防护对象所在行的“操作”列中，单击“设置策略”。

步骤5 在弹出的对话框中，选择防护策略后，单击“确定”，如图2-44所示。

图 2-44 设置策略



说明

单击“展开”，可以查看防护IP的详细信息。

----结束

批量设置防护策略

勾选需要设置防护策略的防护对象，在列表左上角单击“设置策略”，根据提示选择防护策略，单击“确定”。

说明

批量设置方法只能用于同一实例下的多个防护对象。

2.8.3 移除防护对象

当防护对象不需要DDoS原生高级防护时，可以移除防护对象。

须知

绑定在DDoS原生高级防护-全力防基础版上的EIP，在移除后自动纳入DDoS原生基础防护中防护，防护能力不高于5Gbps。

绑定在DDoS原生高级防护-全力防高级版上的专属EIP，在移除后专属EIP会被拉黑，不可再被互联网访问。请谨慎选择后再移除防护对象。

前提条件

已添加防护对象。

操作步骤

步骤1 登录管理控制台。

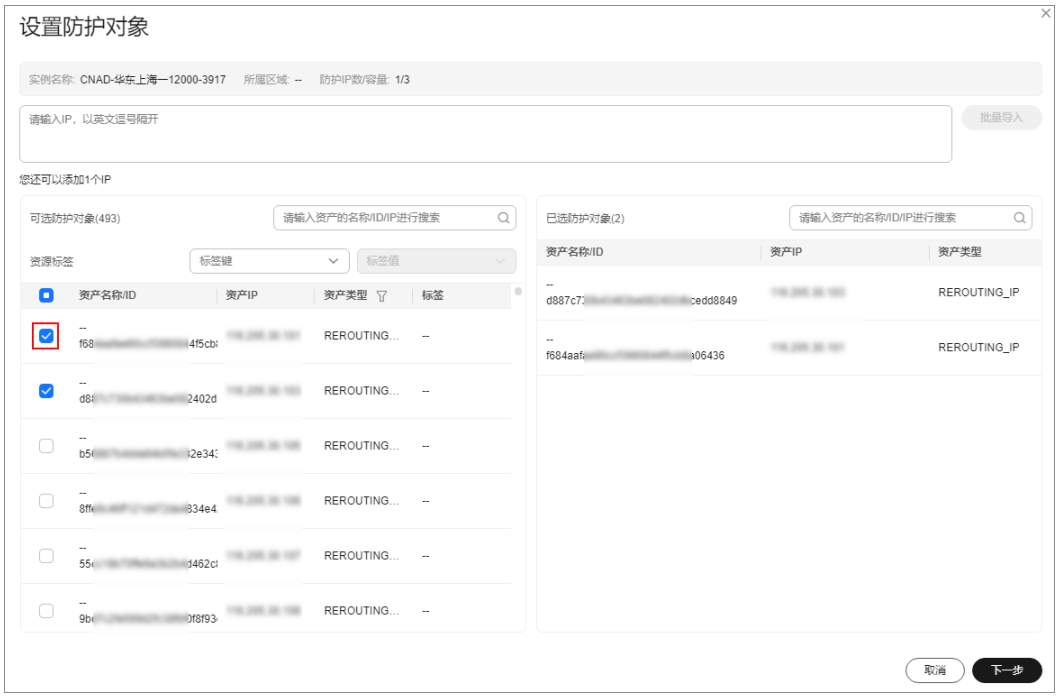
步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS原生高级防护 > 实例列表”，进入DDoS原生高级防护“实例列表”页面。

步骤4 找到需要移除防护对象的实例，单击“设置防护对象”。

步骤5 在弹出的对话框中，取消勾选需要移除的防护对象，单击“下一步”。

图 2-45 移除防护对象



步骤6 确认移除的防护对象，单击“确定”，完成移除防护对象。

图 2-46 确认移除防护对象

----结束

批量移除防护对象

您可以批量勾选需要移除的防护对象后，在防护对象列表左上方，单击“移除”，批量移除防护对象。

2.9 权限管理

2.9.1 创建用户并授权使用 CNAD

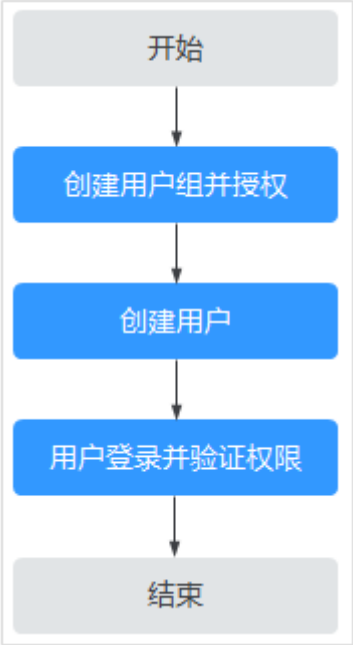
如果您需要对您所拥有的CNAD进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用CNAD资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将CNAD资源委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用CNAD服务的其它功能。

示例流程

图 2-47 给用户授权服务权限流程



1. **创建用户组并授权**

   在IAM控制台创建用户组，并授予DDoS原生高级防护权限“CNAD FullAccess”。

2. **创建用户并加入用户组**

   在IAM控制台创建用户，并将其加入**1**中创建的用户组。

3. **用户登录**并验证权限

   新创建的用户登录控制台，切换至授权区域，验证权限：

   在页面左上方的 ☰，选择除DDoS原生高级防护外（假设当前策略仅包含“CNAD FullAccess”）的任一服务，如果提示权限不足，表示“CNAD FullAccess”已生效。

2.9.2 CNAD 自定义策略

如果系统预置的CNAD权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参见**CNAD权限及授权项**。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的CNAD自定义策略样例。

CNAD 自定义策略样例

- 示例1：授权用户查询防护IP列表

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cnad:protectedIpDropList:list"
                        ]
        }
    ]
}
```

- 示例2：拒绝用户删除IP黑白名单规则

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循Deny优先。

  如果您给用户授予“CNAD FullAccess”的系统策略，但不希望用户拥有“CNAD FullAccess”中定义的删除IP黑白名单规则的权限（cnad:blackWhiteIpList:delete），您可以创建一条相同Action的自定义策略，并将自定义策略的Effect设置为“Deny”，然后同时将“CNAD FullAccess”和拒绝策略授予用户，根据Deny优先原则用户可以对CNAD执行除了删除IP黑白名单规则的所有操作。以下策略样例表示：拒绝用户删除IP黑白名单规则。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "cnad:blackWhiteIpList:delete"
            ]
        },
    ]
}
```

2.9.3 CNAD 权限及授权项

如果您需要对您所拥有的CNAD进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，IAM），如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用CNAD的其它功能。

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为**角色**和**策略**。角色以服务为粒度，是IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。策略授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。

- 权限：允许或拒绝某项操作。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。

权限	授权项	依赖关系说明
查询配额	cnad:quota:get	-
查询单个防护策略详情	cnad:policy:get	-
查询统计数据	cnad:countReport:get	-
查询资产安全状态	cnad:securityStatusReport:get	-
查询每周安全统计数据	cnad:weekStatisticsReport:get	-
创建告警通知	cnad:alarmConfig:create	如果授予用户告警通知权限，需要同时授予用户“cnad:alarmConfig:create”授权项和“中国-香港”的“SMN Administrator”权限。
删除告警通知	cnad:alarmConfig:delete	如果授予用户告警通知权限，需要同时授予用户“cnad:alarmConfig:delete”授权项和“中国-香港”的“SMN Administrator”权限。
查询告警通知	cnad:alarmConfig:get	如果授予用户告警通知权限，需要同时授予用户“cnad:alarmConfig:get”授权项和“中国-香港”的“SMN Administrator”权限。
更新实例	cnad:package:put	-

权限	授权项	依赖关系说明
绑定防护IP到实例	cnad:protectedIp:create	如果授予用户为CNAD实例绑定对象的权限，需要同时授予用户“cnad:protectedIp:create”授权项和实例所属区域的“vpc:publicIps:list”（查询弹性公网IP）授权项。 例如，用户在“中国-香港”购买了一个CNAD实例。如果授予用户为CNAD实例绑定对象的权限，则需要授予该用户“cnad:protectedIp:create”授权项和“中国-香港”的“vpc:publicIps:list”授权项，使该用户只能操作“中国-香港”实例上绑定的防护对象。
创建防护策略	cnad:policy:create	-
更新防护策略	cnad:policy:put	-
删除防护策略	cnad:policy:delete	-
绑定防护策略到防护IP	cnad:bindPolicy:create	-
移除防护IP的防护策略	cnad:unbindPolicy:create	-
创建IP黑白名单	cnad:blackWhiteIpList:create	-
删除IP黑白名单	cnad:blackWhiteIpList:delete	-
更新防护IP标签	cnad:ipTag:put	-
查询清洗范围	cnad:cleanScaleDropList:list	-
查询实例列表	cnad:packageDropList:list	-
查询防护策略列表	cnad:policyDropList:list	-
查询防护IP列表	cnad:protectedIpDropList:list	-
查询实例详情	cnad:package:list	-
查询防护策略详情	cnad:policy:list	-
查询防护IP列表	cnad:protectedIp:list	-
查询总流量数据	cnad:trafficTotalReport:list	-

权限	授权项	依赖关系说明
查询攻击流量	cnad:trafficAttackReport:list	-
查询总数据包	cnad:packetTotalReport:list	-
查询攻击数据包	cnad:packetAttackReport:list	-
查询DDoS防护趋势	cnad:cleanCountReport:list	-
查询清洗流量峰值统计数据	cnad:cleanKbpsReport:list	-
查询攻击类型分布	cnad:attackTypeReport:list	-
查询攻击事件	cnad:attackReport:list	-
查询Top10被攻击IP	cnad:attackTop:list	-
创建实例	cnad:package:create	如果授予用户购买CNAD权限，需要同时授予用户“cnad:package:create”授权项和所有区域以下BSS授权项： ● bss:order:update 操作订单权限 ● bss:contract:update 修改合同商务 ● bss:balance:view 查看账户 ● bss:order:pay 支付权限

2.10 监控

2.10.1 设置事件告警通知

操作场景

通过云监控服务，对防护的弹性公网IP启用事件监控，当出现清洗、封堵、解封等事件时进行告警，方便您及时了解DDoS原生高级防护的防护情况。

开启事件告警通知后，出现相关事件时，即可在云监控服务的事件监控页面查看事件详情。

说明

设置事件告警通知时，如果开启了“发送通知”，会使用消息通知服务（SMN）并产生相关费用。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上方的，选择“管理与监管 > 云监控服务”。

步骤4 根据实际选择方式。

- 方法一：在左侧导航树，单击“事件监控”，进入“事件监控”页面。
- 方法二：在左侧导航树，选择“告警 > 告警规则”，进入“告警规则”页面。

步骤5 在页面右上方，单击“创建告警规则”，进入“创建告警规则”页面。

步骤6 参考表2-9配置告警参数。

图 2-48 告警参数

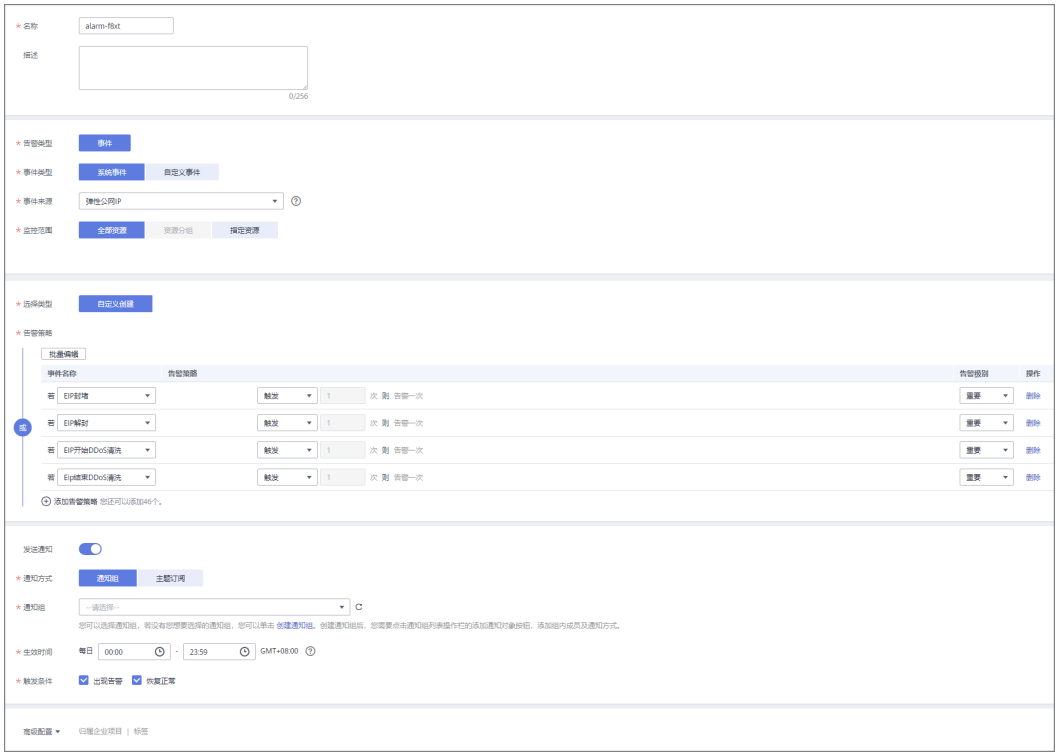


表 2-9 参数说明

参数	说明
名称	系统会随机产生一个名称，您也可以进行修改。
描述	告警规则描述。
告警类型	选择“事件”。
事件类型	选择“系统事件”。
事件来源	选择“弹性公网IP”。

参数	说明
监控范围	告警规则适用的资源范围，根据需要选择。
选择类型	默认为“自定义创建”。
告警策略	推荐选择“EIP封堵”、“EIP解封”、“EIP开始DDoS清洗”、“EIP结束DDoS清洗”。 当流量大于10000kps时，系统会在开始清洗和结束清洗各发送一次告警通知；流量小于10000kps不会发送告警通知。
通知方式	选择“通知组”或“主题订阅”。
通知组	选择所需的通知组。
通知对象	选择所需的主题订阅。
生效时间	根据实际选择。
触发条件	选择“出现告警”、“恢复正常”。

步骤7 根据实际需要，选择是否发送通知。

说明

告警消息由消息通知服务SMN发送，可能产生少量费用。

表 2-10 通知参数

参数	说明
发送通知	配置是否发送邮件、短信、HTTP和HTTPS通知用户。
通知方式	根据需要可选择通知组或主题订阅两种方式。
通知组	通知方式为通知组时生效，根据实际选择。
通知对象	通知方式为主题订阅时生效，根据实际选择。
生效时间	该告警规则仅在生效时间内发送通知消息。
触发条件	根据实际选择。

步骤8 单击“立即创建”，在弹出的窗口中单击“确定”，告警通知创建成功。

----结束

2.10.2 设置监控告警规则

通过设置DDoS告警规则，用户可自定义监控目标与通知策略，设置告警规则名称、监控对象、监控指标、告警阈值、监控周期和是否发送通知等参数，帮助您及时了解DDoS原生高级防护的防护状况，从而起到预警作用。

为多个实例或实例防护的IP设置监控告警请参考**批量设置监控告警规则**；为某个指定实例或实例防护的IP设置监控告警请参考**为单个指定资源设置监控告警规则**。

如果您需要自主定义更多的监控指标，可通过API请求上报至云监控服务，具体操作请参考**添加监控数据**和**监控指标说明**。

前提条件

已购买DDoS原生高级防护实例。

批量设置监控告警规则

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上方的，选择“管理与监管 > 云监控服务 ”。

步骤4 在左侧导航树栏，选择“告警 > 告警规则”，进入“告警规则”页面。

步骤5 在页面右上方，单击“创建告警规则”，进入“创建告警规则”界面。

步骤6 填写告警规则信息，如**图2-49**所示，填写规则如**表2-11**所示。

图 2-49 设置监控告警规则

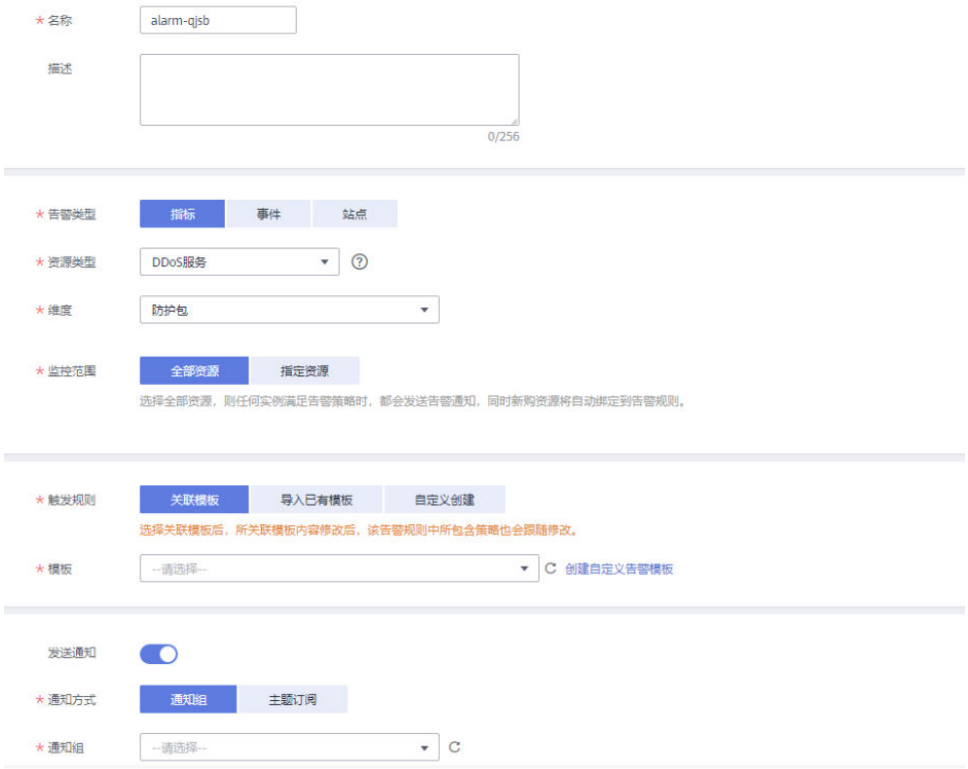


表 2-11 告警规则参数说明

参数名称	参数说明
名称	系统会随机产生一个名称，您也可以进行修改。

参数名称	参数说明
描述	告警规则描述。
告警类型	选择告警类型。
资源类型	在下拉列表框中选择“DDoS服务”。
维度	选择需要监控的资源维度。 ● 防护包：DDoS原生高级防护的实例维度。 ● 防护包-防护IP：实例防护的IP维度。
监控范围	告警规则适用的资源范围，可选择资源分组或指定资源。
触发规则	可选择“关联模板”、“导入已有模板”和“自定义创建”。 创建自定义模板的具体操作请参考**创建自定义告警模板**。 **说明** 选择关联模板后，所关联模板内容修改后，该告警规则中所包含策略也会跟随修改。
模板	选择关联或导入的模板。
发送通知	配置是否发送邮件、短信、HTTP和HTTPS通知用户。
通知方式	需要发送告警通知的对象，可选择云通知组或主题订阅。 ● 云账号联系人为注册账号时的手机和邮箱。 ● 主题是消息发布或客户端订阅通知的特定事件类型，如果此处没有需要的主题则需先创建主题并订阅该主题，该功能会调用消息通知服务（SMN），创建主题并添加订阅请参见**创建主题**、**添加订阅**。
通知组（通知方式选择通知组时生效）	选择需要通知的组织。
通知对象（通知方式选择主题订阅时生效）	选择需要通知的主题。
生效时间	该告警规则仅在生效时间内发送通知消息。
触发条件	可以选择“出现告警”、“恢复正常”两种状态，作为触发告警通知的条件。

步骤7 单击“立即创建”，在弹出的提示框中，单击“确定”， 告警规则创建成功。

----结束

为单个指定资源设置监控告警规则

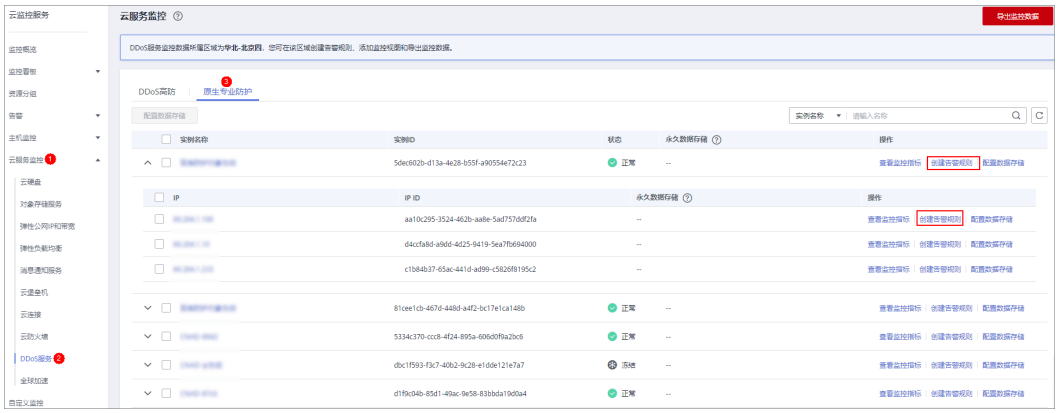
步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上方的，选择“管理与监管 > 云监控服务 ”。

步骤4 选择“云服务监控 > DDoS服务”，单击“原生专业防护”页签。

图 2-50 原生专业防护



步骤5 在需要监控的对象所在行，单击“创建告警规则”。

步骤6 填写告警规则信息，如图2-51所示，填写规则如表2-12所示。

图 2-51 设置监控告警规则

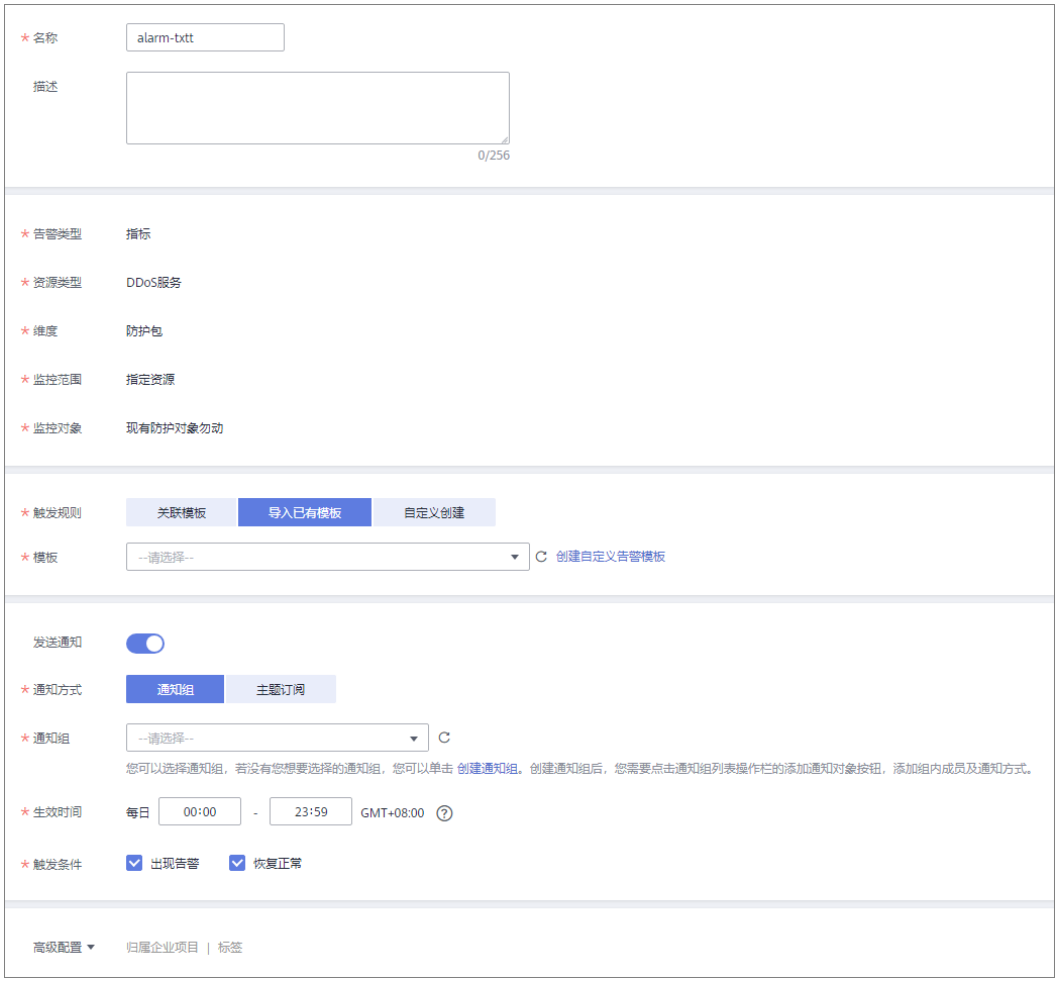


表 2-12 告警规则参数说明

参数名称	参数说明
名称	系统会随机产生一个名称，您也可以进行修改。
描述	告警规则描述。
告警类型	保持默认。
资源类型	保持默认。
维度	保持默认。
监控范围	保持默认。
监控对象	保持默认。

参数名称	参数说明
触发规则	可选择“关联模板”、“导入已有模板”和“自定义创建”。 创建自定义模板的具体操作请参考**创建自定义告警模板**。 **说明** 选择关联模板后，所关联模板内容修改后，该告警规则中所包含策略也会跟随修改。
模板	选择关联或导入的模板。
发送通知	配置是否发送邮件、短信、HTTP和HTTPS通知用户。
通知方式	需要发送告警通知的对象，可选择云通知组或主题订阅。 • 云账号联系人为注册账号时的手机和邮箱。 • 主题是消息发布或客户端订阅通知的特定事件类型，如果此处没有需要的主题则需先创建主题并订阅该主题，该功能会调用消息通知服务（SMN），创建主题并添加订阅请参见**创建主题**、**添加订阅**。
通知组（通知方式选择通知组时生效）	选择需要通知的组织。
通知对象（通知方式选择主题订阅时生效）	选择需要通知的主题。
生效时间	该告警规则仅在生效时间内发送通知消息。
触发条件	可以选择“出现告警”、“恢复正常”两种状态，作为触发告警通知的条件。

步骤7 单击“立即创建”，在弹出的提示框中，单击“确定”， 告警规则创建成功。

----结束

2.10.3 查看监控指标

您可以通过管理控制台，查看DDoS原生高级防护的相关指标，及时了解DDoS原生高级防护的防护状况，并通过指标设置防护策略。

前提条件

已在云监控页面设置监控告警规则。有关设置监控告警规则的详细操作，请参见**设置监控告警规则**。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上方的 ☰，选择“管理与监管 > 云监控服务 CES”。

步骤4 在左侧导航树栏，选择“云服务监控 > DDoS服务”，进入“云服务监控”页面。

步骤5 在需要查看的目标所在行，单击“查看监控指标”，查看对象的指标详情。

----结束

2.10.4 监控指标说明

功能说明

本节定义了DDoS原生高级防护上报云监控服务的监控指标的命名空间和监控指标列表，用户可以通过云监控服务提供管理控制台来检索DDoS原生高级防护产生的监控指标和告警信息。

命名空间

SYS.DDOS

说明

命名空间是对一组资源和对象的抽象整合。在同一个集群内可创建不同的命名空间，不同命名空间中的数据彼此隔离。使得它们既可以共享同一个集群的服务，也能够互不干扰。

监控指标

表 2-13 DDoS 原生高级防护服务支持的监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
ip_drop_rate	丢弃流量	IP丢弃流量带宽	≥0kb/s	DDoS原生高级防护	60秒
instance_drop_rate	丢弃流量	实例丢弃流量带宽	≥0kb/s	DDoS原生高级防护	60秒
ip_back_to_source_rate	回源带宽	IP回源流量带宽	≥0kb/s	DDoS原生高级防护	60秒
instance_back_to_source_rate	回源带宽	实例回源流量带宽	≥0kb/s	DDoS原生高级防护	60秒
ip_internet_in_rate	入流量	IP入流量带宽	≥0kb/s	DDoS原生高级防护	60秒
instance_internet_in_rate	入流量	实例入流量带宽	≥0kb/s	DDoS原生高级防护	60秒
ip_new_connection	新建连接	IP新建连接数	≥0count/s	DDoS原生高级防护	60秒

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
instance_new_connection	新建连接	实例新建连接数	≥0count/s	DDoS原生高级防护	60秒
ip_concurrent_connection	并发连接	IP并发连接数	≥0count/s	DDoS原生高级防护	60秒
instance_concurrent_connection	并发连接	实例并发连接数	≥0count/s	DDoS原生高级防护	60秒

维度

Key	Value
package	防护包
package_ip	防护包-防护IP

2.11 审计

2.11.1 云审计服务支持的 DDoS 防护操作列表

云审计服务（Cloud Trace Service，CTS）记录了DDoS防护相关的操作事件，方便用户日后的查询、审计和回溯，具体请参见**云审计服务用户指南**。

云审计服务支持的DDoS防护操作列表如**表2-14**所示。

表 2-14 云审计支持的 DDoS 防护操作列表

操作名称	资源类型	事件名称
更新告警通知配置	alarmConfig	updateAlarmConfig
删除告警通知配置	alarmConfig	deleteAlarmConfig
创建防护包	package	createPackage
更新防护包	package	updatePackage
绑定IP到防护包	package	bindIpToPackage
从防护包上解绑IP	package	unbindIpToPackage
删除防护包	package	DeletePackage
创建策略	policy	createPolicy

操作名称	资源类型	事件名称
更新策略	policy	updatePolicy
绑定IP到策略	policy	bindIpToPolicy
从策略中解绑IP	policy	unbindIpToPolicy
添加黑白名单	policy	addblackWhiteIpList
删除黑白名单	policy	deleteblackWhiteIpList
删除策略	policy	deletePolicy
配置全量日志的日志组和日志流	cnad	updateLogConfig
关闭全量日志的日志组和日志流	cnad	deleteLogConfig
给防护IP打标签	cnad	updateTagForIp

2.11.2 查看云审计日志

开启了云审计服务后，系统开始记录DDoS防护资源的操作。云审计服务管理控制台保存最近7天的操作记录。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左侧的 ☰，选择“管理与监管 > 云审计服务”，进入云审计服务信息页面。

步骤3 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤4 在下拉框中选择“云服务”，输入“CNAD”，按“Enter”。

步骤5 在查询结果中单击事件名称，查看事件详情。

事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：

- 事件名称、资源名称、资源ID、事件ID：需要输入某个具体的名称或ID。
  - 资源名称：当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。
  - 资源ID：当该资源类型无资源ID或资源创建失败时，该字段为空。
- 云服务、资源类型：在下拉框中选择对应的云服务名称或资源类型。
- 操作用户：在下拉框中选择一个或多个具体的操作用户。
- 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
  - normal：表示操作成功。

  - warning：表示操作失败。
  - incident：表示比操作失败更严重的情况，如引起其他故障等。
- 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近1周内任意时间段的操作事件。

----结束

3 DDoS 高防操作指南

3.1 使用概览

购买DDoS高防实例，业务接入DDoS高防后即可防护，通过丰富全面的防护规则帮助您防护海量DDoS攻击。

DDoS高防的使用概览如**使用概览**所示。

表 3-1 使用概览

子流程	说明
业务接入	请参见**域名网站类业务接入DDoS高防**。
配置防护策略	DDoS高防提供了丰富全面的防护规则，您可以根据业务需求配置相应的防护策略。详细操作请参见**配置防护策略**。
开启告警通知	开启告警通知后，当IP遭受DDoS攻击时，您可以第一时间接收告警通知。详细操作请参见**开启告警通知**。
实例管理	查看实例信息、升级防护带宽和业务带宽、修改弹性防护带宽等常用操作。详细操作请参见**实例管理**。
域名管理	查看域名信息、更新证书、修改解析线路、修改源站IP、修改域名业务配置等常用操作。详细操作请参见**域名管理**。
监控	设置监控指标告警，设置黑洞、调度和攻击事件告警，帮助您及时了解DDoS高防防护状况。详细操作请参见**监控**。
审计	记录了DDoS高防相关的操作事件，方便用户日后的查询、审计和回溯。详细操作请参见**审计**。

3.2 购买实例

3.2.1 购买 DDoS 高防实例

用户在使用DDoS高防前，需要购买高防实例。

须知

- DDoS高防购买后，不支持退款。
- DDoS高防实例到期≥30个自然日时，DDoS高防将停止转发业务流量，实例将被释放。如果您不需要继续使用DDoS高防，请务必在到期30个自然日之前，将业务流量从高防切换到源站服务器。

前提条件

请确认购买实例的账号同时具有“CAD Administrator”和“BSS Administrator”角色，或者该账号具有“Tenant Administrator”角色。

- BSS Administrator：费用中心、资源中心、账号中心的所有执行权限。项目级角色，在同项目中勾选。
- Tenant Administrator：除统一身份认证服务外，其他所有服务的所有执行权限。

规格限制

- 每个用户默认最多可以购买5个实例。如果配额不足，您可以**提交工单**申请扩大配额。
- 业务服务器在中国内地，推荐购买DDoS高防。使用DDoS高防，域名必须经过ICP备案，未备案域名将无法正常访问。
- 业务服务器在中国内地以外的地域，推荐购买DDoS高防国际版。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在界面右上角，单击“购买DDoS防护”，进入“购买DDoS防护”页面。

步骤4 在“购买DDoS防护”界面，“实例类型”选择“DDoS高防”。

步骤5 设置DDoS高防实例规格，如**图3-1**所示，相关参数说明如**表3-2**所示。

图 3-1 购买 DDoS 高防

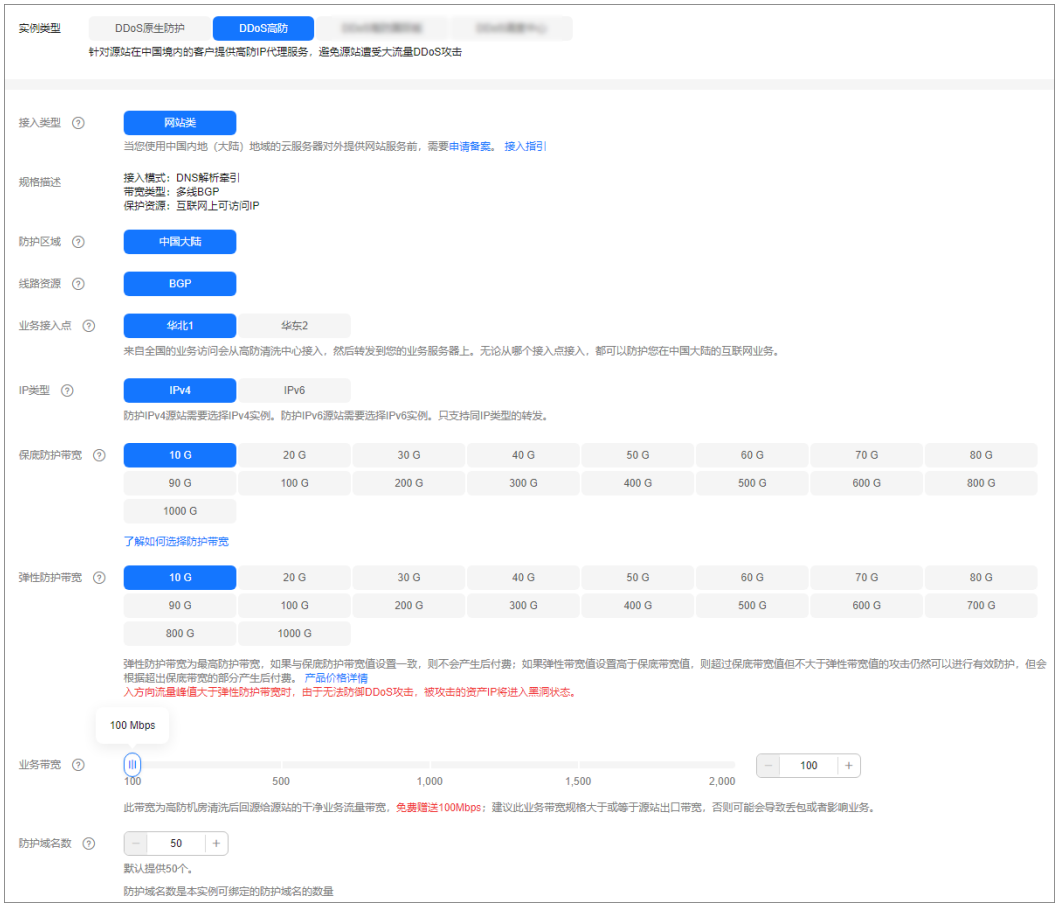


表 3-2 参数说明

参数	说明
接入类型	网站类：华为云通过智能算法为您选择最佳接入点，并且不再提供固定的高防IP。推荐使用“域名接入”的用户购买并使用。
防护区域	中国大陆：适用于业务服务器部署在中国大陆的场景。 业务服务器部署在其他地域的场景，推荐购买DDoS高防国际版。
线路资源	中国大陆：仅支持“BGP”。
业务接入点	中国大陆提供以下接入点，请根据您业务的地理位置自行选择： • 华北1：线路支持中国移动、中国电信、中国联通、北京教育网、鹏博士、河北广电、重庆广电。 • 华东2：支持中国移动、中国电信、中国联通。
IP类型	• IPv4：防护IPv4源站需要选择IPv4实例。 • IPv6：防护IPv6源站需要选择IPv6实例。

参数	说明
保底防护带宽	保底防护带宽是指用于防御攻击的保底带宽。如果攻击峰值小于等于客户购买的保底防护带宽，客户无需支付额外费用。 如果需要提升防护性能，可以设置“弹性防护带宽”。
弹性防护带宽	攻击峰值超过保底防护带宽时产生弹性防护费用，后扣费。 在购买高防实例后，可以根据业务实际情况，修改弹性防护带宽。 **说明** 弹性防护带宽不能小于保底防护带宽。如果用户选择的弹性防护带宽等于保底防护带宽，则弹性防护功能不生效。
防护域名数	（仅接入规则选择为：“网站类”时可选择）默认提供50个，可以付费增加，最多可支持200个。
业务带宽	高防实例的回源业务带宽，从高防实例转发回源站的干净流量带宽。业务带宽支持配置的范围为100Mbps～5000Mbps。 请您统计将要接入华为云DDoS高防实例的所有业务日常入方向和出方向总流量的峰值，您选择的最大业务带宽应大于这些业务的网络入、出方向总流量峰值中较大的值。 **注意** 如果您购买的实例业务带宽低于上述中的峰值流量大小，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。升级规格请参见**升级实例规格**。 假如，您有两个业务（业务A和业务B）需要接入DDoS高防服务，业务A正常业务流量峰值均不超过50 Mbps，业务B正常业务流量峰值均不超过70 Mbps，业务流量总和不超过120Mbps。在这种情况下，您只需要确保购买的实例的最大业务带宽大于120Mbps即可保证业务的正常运行。

步骤6 选择“购买时长”和“购买数量”，如**图3-2**所示，相关参数说明如**表3-3**所示。

图 3-2 选择购买时长和购买数量

表 3-3 购买参数说明

参数	说明	取值样例
实例名称	高防实例名称。 ● 名称长度小于等于32个字符。 ● 名称只能由中文字符、大小写英文字母、数字、下划线和中划线组成。	CAD-0001
企业项目	企业项目针对企业用户使用，只有开通了企业项目的客户，或者权限为企业主账号的客户才可见。如需使用该功能，请**开通企业管理功能**。企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。 **说明** ● “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。 ● 只有注册的华为云账号购买实例时，“企业项目”下拉列表中才可以选择到“default”。	-
购买时长	根据实际选择。	-
购买数量	选择购买的实例个数，每个用户默认最多可以购买5个实例。	1

说明

“自动续费”为可选项。勾选“自动续费”后，系统将在产品到期前自动续费。

步骤7 单击“立即购买”。

步骤8 在“订单详情”页面，如果您确认订单无误，单击“去支付”。

步骤9 在支付界面完成订单支付。

----结束

3.2.2 购买 DDoS 高防国际版实例

用户在使用DDoS高防前，需要购买高防实例。

须知

- DDoS高防购买后，不支持退款。
- DDoS高防实例到期≥30个自然日时，DDoS高防将停止转发业务流量，实例将被释放。如果您不需要继续使用DDoS高防，请务必在到期30个自然日之前，将业务流量从高防切换到源站服务器。

前提条件

请确认购买实例的账号同时具有“CAD Administrator”和“BSS Administrator”角色，或者该账号具有“Tenant Administrator”角色。

- BSS Administrator：费用中心、资源中心、账号中心的所有执行权限。项目级角色，在同项目中勾选。
- Tenant Administrator：除统一身份认证服务外，其他所有服务的所有执行权限。

规格限制

- 每个用户默认最多可以购买5个实例。如果配额不足，您可以提交工单申请扩大配额。
- 业务服务器在中国内地，推荐购买DDoS高防。使用DDoS高防，域名必须经过ICP备案，未备案域名将无法正常访问。
- 业务服务器在中国内地以外的地域，推荐购买DDoS高防国际版。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在界面右上角，单击“购买DDoS防护”，进入“购买DDoS防护”页面。

步骤4 在“购买DDoS防护”界面，“实例类型”选择“DDoS高防国际版”。

步骤5 设置DDoS高防实例规格，如图3-3所示，相关参数说明如表3-4所示。

图 3-3 购买 DDoS 高防国际版

表 3-4 参数说明

参数	说明
线路资源	“亚太”、“拉美”、“南非”、“欧洲”、“中东”。

参数	说明
IP个数	多个：为用户的每个业务系统单独提供高防IP，上限为所选规格内包含的防护域名与防护端口的总和。
保底防护带宽	50G：提供最高50Gbit/s防护。 无限防：提供无上限全力防护。
转发规则数	默认提供5个，最多可选50个。
防护域名数	默认提供5个，最多可选50个。
业务带宽	业务带宽指高防机房将清洗后的干净流量，转发给源站所占用的带宽。 • 业务带宽支持范围：10Mbps～5000Mbps。 • 高防机房在华为云外，建议购买的高防业务带宽规格大于或等于源站出口带宽。

步骤6 选择“购买时长”和“购买数量”，如图3-4所示，相关参数说明如表3-5所示。

图 3-4 选择购买时长和购买数量

表 3-5 购买参数说明

参数	说明	取值样例
实例名称	高防实例名称。 • 名称长度小于等于32个字符。 • 名称只能由中文字符、大小写英文字母、数字、下划线和中划线组成。	CAD-0001
购买时长	可以选择1个月～1年的时长。	1
购买数量	选择购买的实例个数，每个用户默认最多可以购买5个实例。	1

说明

“自动续费”为可选项。勾选“自动续费”后，系统将在产品到期前自动续费。

步骤7 单击“立即购买”。

步骤8 在“订单详情”页面，如果您确认订单无误，单击“去支付”。

步骤9 在支付界面完成订单支付。

----结束

3.3 业务接入

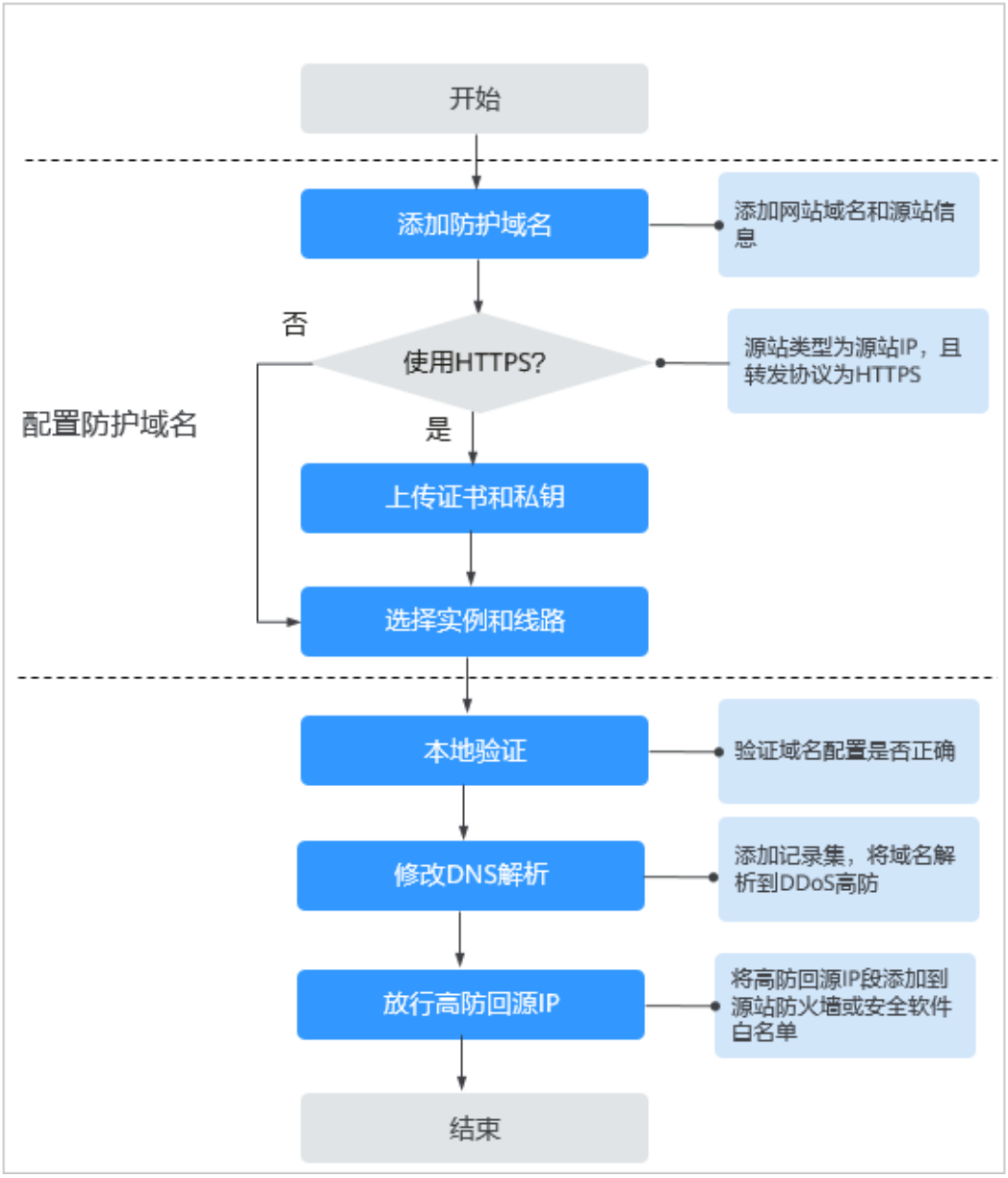
3.3.1 域名网站类业务接入 DDoS 高防

3.3.1.1 网站类业务接入流程

购买DDoS高防后，对于网站类业务，您需要通过CNAME解析方式接入DDoS高防，使所有的公网流量都引流至高防IP，进而隐藏源站。

网站类业务接入DDoS高防流程如图3-5所示。

图 3-5 网站类业务接入 DDoS 高防流程



3.3.1.2 步骤一：配置防护域名（网站类）

对于网站类业务，购买DDoS高防后，您需要将防护域名配置到DDoS高防，使业务通过CNAME解析的方式接入高防IP。

说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，在该企业项目下选择高防实例与线路。

前提条件

- 已成功购买高防实例。
- 防护域名已备案。

规格限制

每个用户最多可以接入50个域名，不支持批量添加防护域名。

约束条件

- “源站域名”当前仅支持配置为华为云WAF的CNAME。
- DDoS高防当前仅支持PEM格式证书。
- CNAME值是根据域名生成的，对于同一个域名，其CNAME值是一致的。
- DDoS高防支持Web Socket协议，且默认为开启状态。
- 一个域名可以选择多条线路（高防IP），选择多个高防IP时请确保各高防IP所配置的转发规则个数以及转发规则的转发协议、转发端口和业务类型保持一致。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-6 域名接入页

步骤4 在域名列表左上方，单击“添加域名”。

步骤5 在添加域名界面配置域名信息，如图3-7所示，相关参数说明如表3-6所示。

图 3-7 配置网站类域名信息

表 3-6 域名配置参数说明

参数名称	说明	示例
防护域名	用户的实际业务对外提供服务所使用的域名。 • 单域名：输入防护的单域名。例如：www.example.com。 • 泛域名 – 如果各子域名对应的服务器IP地址相同：输入防护的泛域名。例如：子域名a.example.com，b.example.com和c.example.com对应的服务器IP地址相同，可以直接添加泛域名*.example.com。 – 如果各子域名对应的服务器IP地址不相同：请将子域名按“单域名”方式逐条添加。	单域名：www.example.com 泛域名：*.example.com

参数名称	说明	示例
源站类型	待添加防护域名的源站的类型。 • 源站IP：真实服务器的公网IP地址，最多可输入20个IP地址，IP地址间以“,”分隔。 • 源站域名 当前仅支持华为云WAF CNAME。 • 转发协议 DDoS高防转发客户端（例如浏览器）请求的协议类型。包括“HTTP”、“HTTPS”两种协议类型。 • 源站端口 DDoS高防转发客户端请求到服务器的业务端口。 **须知** • 如果待添加域名与其它域名使用同一个高防IP（高防线路）与协议/端口，待添加域名和其它域名的“源站类型”必须保持一致，且注意： – 如果其他域名的“源站类型”为“源站IP”，请确保其它域名已开启Web攻击防护，详细操作请参考**开启WEB基础防护和CC防护**。 – 如果其他域名的“源站类型”为“源站域名”，请确保其它域名与待添加域名是在同一个WAF区域接入的WAF防护。 • 如果“源站类型”选择“源站域名”，请确保您的业务在接入WAF时选择了使用代理，否则接入高防后会导致业务不通。 • 华为云WAF接入DDoS高防后，如果后续您的业务需要拆除WAF防护，请首先把业务从DDoS高防拆除。	源站IP：XXX.XXX.1.1 转发协议：HTTP 源站端口：80
证书	“源站类型”选择“源站IP”且“转发协议”选择“HTTPS”时，需要上传证书。有关上传证书的详细操作，请参见**步骤6**。	-

步骤6 （可选）上传证书。

“源站类型”选择“源站IP”且“转发协议”选择“HTTPS”时，您需要导入证书。

您可以在“证书”下拉列表框中选择已有证书，或上传新证书。

上传新证书的操作步骤如下。

1. 单击“上传”，在弹出的“上传证书”对话框中，选择证书上传方式。
   – 手动上传：输入证书名称，粘贴证书和私钥文本内容，如**图3-8**所示，相关参数说明如**表3-7**所示。
   – 自动拉取：选择已签发的证书。

须知

建议证书名称长度不超过10个字符，且不包括特殊字符。

图 3-8 上传证书

说明

- 当前只支持TLS 1.0、TLS 1.1、TLS 1.2版本证书的上传。
- 当前仅支持PEM格式证书。
- 同一用户的证书名不可重复。

表 3-7 证书参数说明

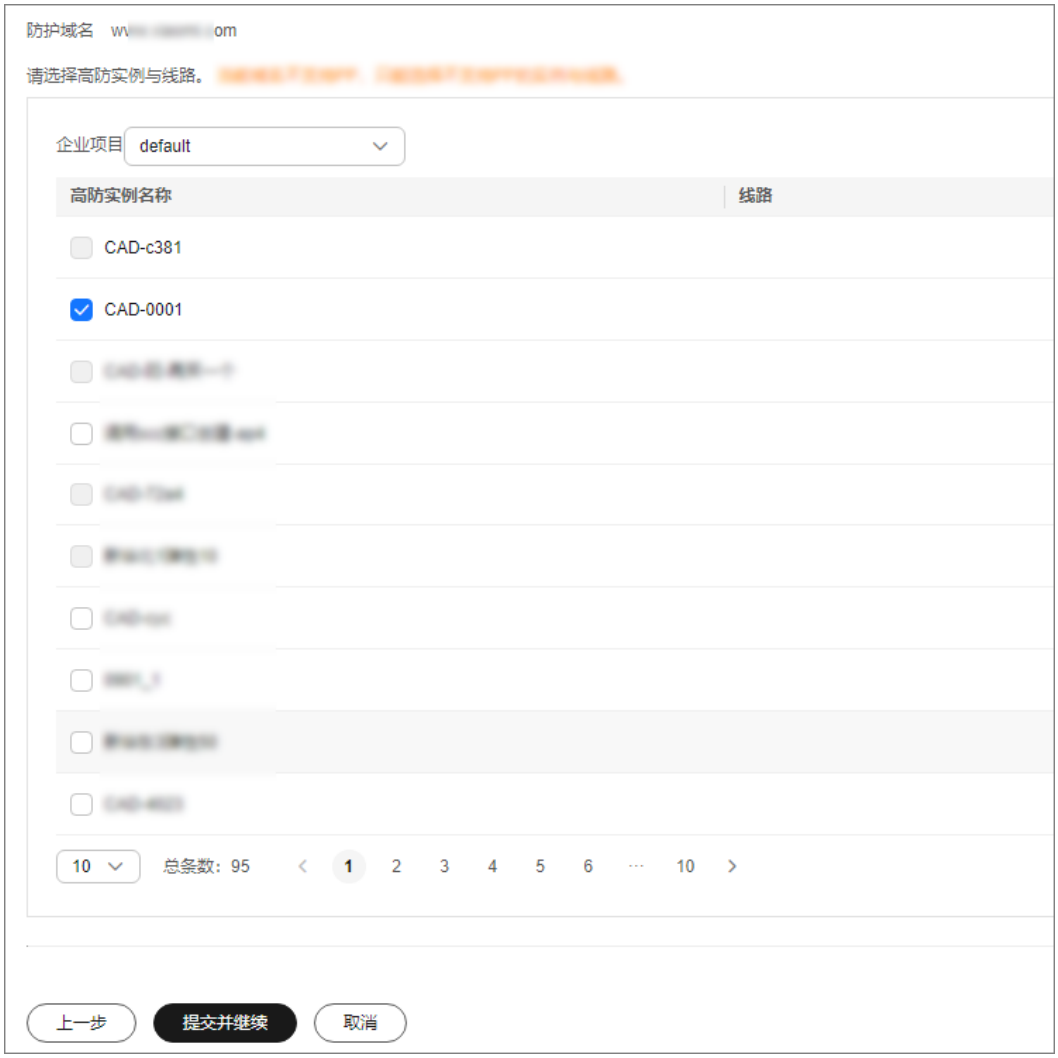
参数名称	说明
证书文件	- 证书输入格式如下： -----BEGIN CERTIFICATE----- MIIDljCCAv+gAwIBAgIJAMD2jG2tYGQ6MA0GCSqGSIb3DQEBBQUAMIGPMQswCQYD VQQGEwJDSDELMAkGA1UECBMCWkoxCzAJBgNVBAcTAkhaMQ8wDQYDVQQKEwZodWF3 ZWkxDzANBgNVBAsTBmh1YXdlaTEPMA0GA1UEAxMGaHVhd2VpMQ8wDQYDVQQpEwZz ZXJ2ZXIxIjAgBgkqhkiG9w0BCQEWE3p3YW5nd2VpZGtkQDE2My5jb20wHhcNMTUw MzE4MDMzNjU5WhcNMjUwMzE1MDMzNjU5WjCBjzELMAkGA1UEBhMCQ0gxCzAJBgNV BAgTAlpKMQswCQYDVQQHEwJIWjEPMA0GA1UEChMGaHVhda2VpMQ8wDQY..... -----END CERTIFICATE----- - 证书文件内容的复制方法： ▪ PEM格式证书：用文本编辑器直接打开进行复制。 ▪ 非PEM格式证书：先转换成PEM格式，再用文本编辑器直接打开进行复制。

参数名称	说明
私钥文件	私钥输入格式如下： -----BEGIN RSA PRIVATE KEY----- MIIDljCCAv+gAwIBAgIJAMD2jG2tYGQ6MA0GCSqGSIb3DQEBBQUAMIGPMQswCQYDVQQG EwJDSDELMAkGA1UECBMCWkoxCzAJBgNVBAcTAkhaMQ8wDQYDVQQKEwZodWF3ZWkxDzAN BgNVBAsTBmh1YXdlaTEPMA0GA1UEAxMGaHVhd2VpMQ8wDQYDVQQpEwZzZXJ2ZXIxIjAg BgkqhkiG9w0BCQEWE3poYW5nd2VpZGtkQDE2My5jb20wHhcNMTUwMzE4MDMzNjU5WhcN MjUwMzE1MDMzNjU5WjCBjzELMAkGA1UEBhMCQ0gxCzAJBgNVBAgTAlpKMQswCQYDVQQH EwJIWjEPMA0GA1UEChMGaHVhd2VpMQ8wDQYDVQQLEwZ -----END RSA PRIVATE KEY----- – 私钥文件内容的复制方法： ▪ PEM格式证书：用文本编辑器直接打开进行复制。 ▪ 非PEM格式证书：先转换成PEM格式，再用文本编辑器直接打开进行复制。

2. 单击“确定”。

步骤7 单击“下一步”，选择高防实例与线路，如图3-9所示。

图 3-9 选择高防实例与线路



须知

- 一个域名可以选择多条线路（高防IP），选择多个高防IP时请确保各高防IP所配置的转发规则个数以及转发规则的转发协议、转发端口和业务类型保持一致。

步骤8 单击“提交并继续”，弹出如图3-10所示界面。

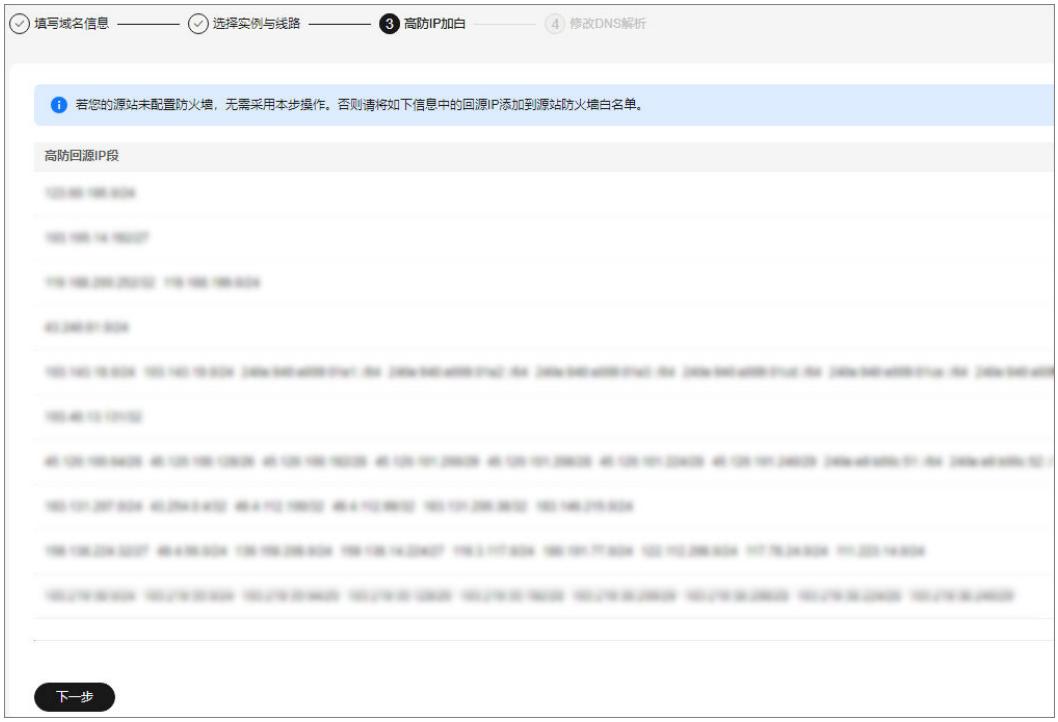
建议您单击“下一步”，跳过本步骤，后续参照**步骤四：修改DNS解析**完成DNS解析配置。

图 3-10 修改 DNS 解析

步骤9 单击“完成”，完成防护域名配置。

域名配置完成，系统跳转至“域名接入”界面，您可以在域名列表中查看添加的防护域名。

图 3-11 高防回源 IP 段



如果源站已配置防火墙或安装安全软件，请将高防回源IP地址段添加到源站的防火墙、ACL或者其他任何安全软件，即对回源IP段设置为放行，以确保高防的回源IP不受源站安全策略影响。有关放行回源IP的详细操作，请参见**步骤二：放行高防回源IP段**。

须知

DDoS高防会替换真实用户IP并且将客户业务的访问流量汇聚到高防回源IP。

- 在没有启用DDoS高防时：对于源站来说真实客户端的地址是非常分散的，且正常情况下每个源IP的请求量都不大。
- 在启用DDoS高防后：由于高防回源的IP段固定且有限，对于源站来说所有的请求都是来自高防回源IP段，因此分摊到每个回源IP上的请求量会增大很多（可能被误认为回源IP在对源站进行攻击）。此时，如果源站有其它防御DDoS的安全策略，很可能对回源IP进行拦截或者限速。例如，最常见的502错误。

----结束

后续处理

配置防护域名后，建议您本地验证域名参数配置正确，详细操作请参见**步骤三：本地验证（网站类）**。

相关操作

- 如果域名不需要解析到某个高防IP时，可以在该域名所在行的“实例和线路”列，单击“查看详情”。选择域名的高防IP，单击  ，将“域名解析”状态设置为  。

- 如果不需要防护某个域名时，可以在该域名所在行的“操作”列，单击“删除”，删除该域名。

3.3.1.3 步骤二：放行高防回源 IP 段

回源IP是DDoS高防用来代理客户端请求服务器时用的源IP，在服务器看来，接入DDoS高防后所有源IP都会变成DDoS高防的回源IP，以确保源站安全、稳定、可用。

如果源站已配置防火墙或安装安全软件，为了防止高防回源IP被源站拦截或限速，需要将高防回源IP段添加到源站的防火墙或其它防护软件的白名单中，即放行高防回源IP段，以确保高防的回源IP不受源站安全策略影响。

前提条件

防护域名已接入DDoS高防。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-12 域名接入页

步骤4 在域名列表左上角，单击“高防回源IP段”。

步骤5 在弹出的“高防回源IP段”对话框中，查看高防回源IP段信息，如图3-13所示。

图 3-13 查看高防回源 IP 段

步骤6 将高防回源IP段添加到源站的防火墙或其它防护软件的白名单中。

----结束

3.3.1.4 步骤三：本地验证（网站类）

将网站类业务添加到DDoS高防后，为了最大程度保证业务的稳定，建议在全面切换业务之前先进行本地的测试，验证域名配置正确。DDoS高防预期可以把发送到高防IP或高防CNAME的报文转发到源站（真实服务器）。

本章节以Telnet工具为例，介绍如何在本地验证网站类业务配置正确。

前提条件

防护域名已添加到DDoS高防。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-14 域名接入页

步骤4 在目标域名的“CNAME”列，单击 ，复制域名的CNAME值。

步骤5 打开Telnet，执行以下命令，测试已接入DDoS高防的源站IP是否能成功建立连接。

telnet *源站IP* 80

以源站IP对外开放的80端口为例。

- 如果可以连通，则说明Telnet公网地址在本机网络环境可用。
- 如果无法连通，则需要更换本地测试机网络环境，因为某些企业网有可能配置过内部网络限制。例如连接手机Wi-Fi热点以切换为运营商网络。

步骤6 执行以下命令，测试域名接入DDoS高防配置是否正确。

telnet *在目标域名的“CNAME”列，单击，复制域名的C...中的CNAME值* 80

- 如果可以连通，说明配置成功。
- 如果无法连通，请确认域名参数是否配置正确。

----结束

说明

如您需验证WAF基础防护是否正确开启，请参见：**WAF本地验证**。

3.3.1.5 步骤四：修改 DNS 解析

域名成功添加到DDoS高防后，您还需要到域名提供商处修改DNS解析，使域名接入DDoS高防，将所有的公网流量都引流至高防IP，进而隐藏源站。

DDoS高防支持A记录接入和CNAME接入两种方式，推荐使用CNAME接入。CNAME接入方式优势说明如下：

- CNAME接入更方便，用户只需在域名解析时（如华为云解析）修改一次解析配置即可生效。

- 当某条线路的高防出现异常时，使用CNAME解析，域名可自动切换到其他线路。
- 如果客户使用的是三线套餐，当某条线路被攻击导致黑洞时，使用CNAME解析，高防可自动解析到其他可用线路上，避免原来解析到该线路的业务受到影响，保证业务的可用性。

本章节以华为云的云解析服务为例说明修改DNS解析的操作步骤，具体的配置操作以业务实际情况为准。

前提条件

域名已经成功添加到DDoS高防。

约束条件

- 添加CNAME时，需要删除原DNS解析中的A记录，否则解析会产生冲突，无法添加CNAME解析（部分DNS解析服务提供商支持直接修改A记录为CNAME记录，此时修改不会有影响）。
- DNS配置需要等待一定时间才可以生效，您可通过一些在线测试工具测试域名的解析情况。

系统影响

DNS配置可能会影响当前业务，建议在业务较少时段配置。

CNAME 接入

获取防护域名的高防CNAME后，您需要将该CNAME值添加到在云解析服务的记录集中。

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-15 域名接入页

步骤4 在目标域名的“CNAME”列，单击 ，复制域名的CNAME值。

步骤5 单击页面左上方的 ☰，选择“网络 > 云解析服务 DNS”。

步骤6 参考**添加CNAME类型记录集**完成CNAME接入。

----结束

> **⚠ 注意**
>
> 如果您在**步骤三：本地验证（网站类）**中配置了hosts进行测试，请在本步骤后删除相关hosts配置，否则会造成防护异常。

A 记录接入

下面以电信线路套餐为例。

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“网络 > 云解析服务 DNS”。

步骤4 参考**添加A类型记录集**完成A记录接入。

----结束

3.4 配置防护策略

3.4.1 配置黑白名单

操作场景

DDoS高防服务支持对已接入防护的高防实例设置黑名单和白名单，以拦截或放行指定IP的访问请求。

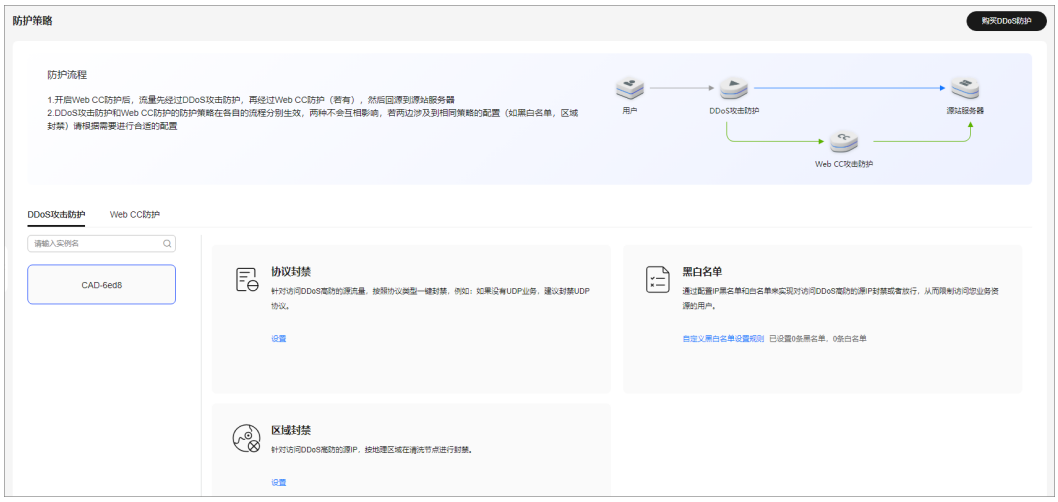
操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面上方选择“区域”后，单击页面左上方的，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 防护策略”，进入DDoS高防“防护策略”页面。

图 3-16 DDoS 高防防护策略页面



步骤4 选择需要配置黑名单或白名单的实例。

步骤5 配置黑白名单。

- 配置黑名单
  a. 在“黑白名单”配置框中，单击“自定义黑白名单设置规则”。
  b. 选择“黑名单”页签，单击“添加”。
  c. 在弹出的对话框中，输入需要进行拦截的IP或IP/掩码，如图3-17所示。

图 3-17 添加黑名单 IP

说明

每个实例可添加100个黑名单IP，黑名单中的IP会被拦截。

  d. 单击“确定”。

在“黑名单IP”界面，单击操作列的“删除”或选择要删除的黑名单执行“批量删除”，被删除的黑名单IP，设备将不再拦截其访问流量。

- 配置白名单
  a. 选择“白名单IP”页签，单击“添加”。
  b. 在弹出的对话框中，输入需要被放行的IP或IP/掩码，如图3-18所示。

图 3-18 添加白名单 IP

说明

每个实例可添加100个白名单IP，白名单中的IP会被放行。

  c. 单击“确定”。
  在“白名单IP”界面，单击操作列的“删除”或选择要删除的白名单执行“批量删除”，被删除的白名单IP，设备将不再直接放行其访问流量。

----结束

3.4.2 配置协议封禁

您可以通过UDP流量封禁功能，一键放行或阻止协议流量访问DDoS高防实例。

DDoS高防支持一键放行或阻止海外流量访问， 不支持对某个国家或地区配置流量封禁。

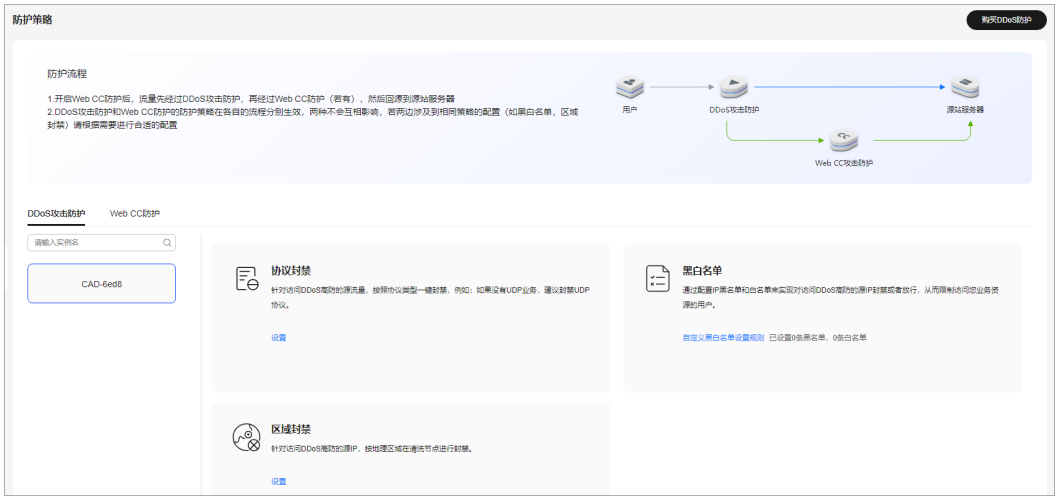
操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 防护策略”，进入DDoS高防“防护策略”页面。

图 3-19 DDoS 高防防护策略页面



步骤4 选择需要配置协议封禁的实例。

步骤5 在协议封禁配置框中单击“设置”。

步骤6 在弹出的对话框中选择需要配置协议封禁的路线，并且将开关调整至  ，打开协议禁用功能。

图 3-20 协议封禁设置

----结束

3.4.3 配置区域封禁

DDoS高防支持一键放行或阻止海外流量访问， 不支持对某个国家或地区配置流量封禁。

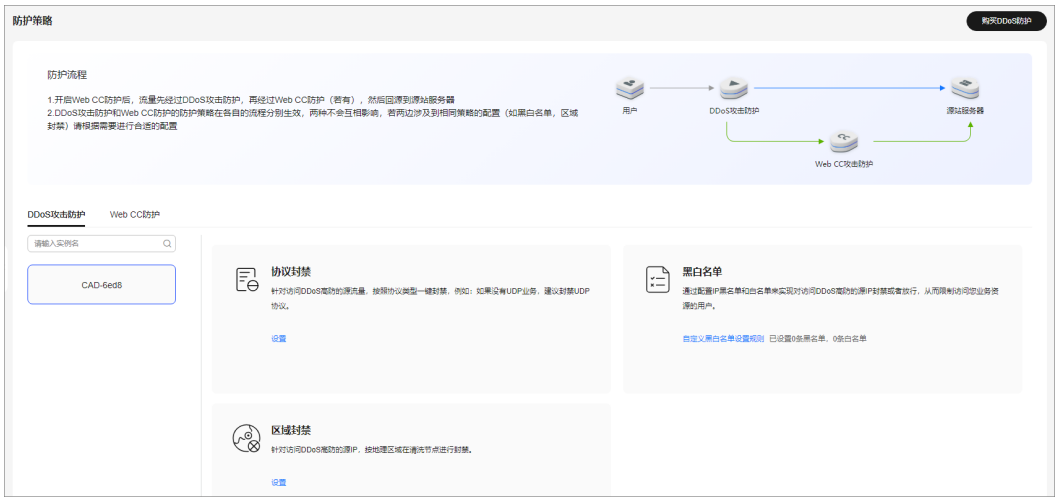
操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 防护策略”，进入DDoS高防“防护策略”页面。

图 3-21 DDoS 高防防护策略页面



步骤4 选择需要配置区域封禁的实例。

步骤5 在区域封禁配置框中单击“设置”。

步骤6 在弹出的对话框中，选择需要设置区域封禁的路线，并且勾选需要封禁的区域。

图 3-22 区域封禁设置

步骤7 单击“确定”，完成区域封禁设置。

----结束

3.4.4 配置 CC 攻击防护规则

3.4.4.1 设置频率控制规则

操作场景

您可以通过设置频率控制策略，限制单个IP/Cookie/Referer访问者对防护网站上源端的访问频率，同时支持策略限速、域名限速和URL限速，精准识别CC攻击以及有效缓解CC攻击。

前提条件

网站类业务已成功接入DDoS高防并开启“WEB基础防护”。

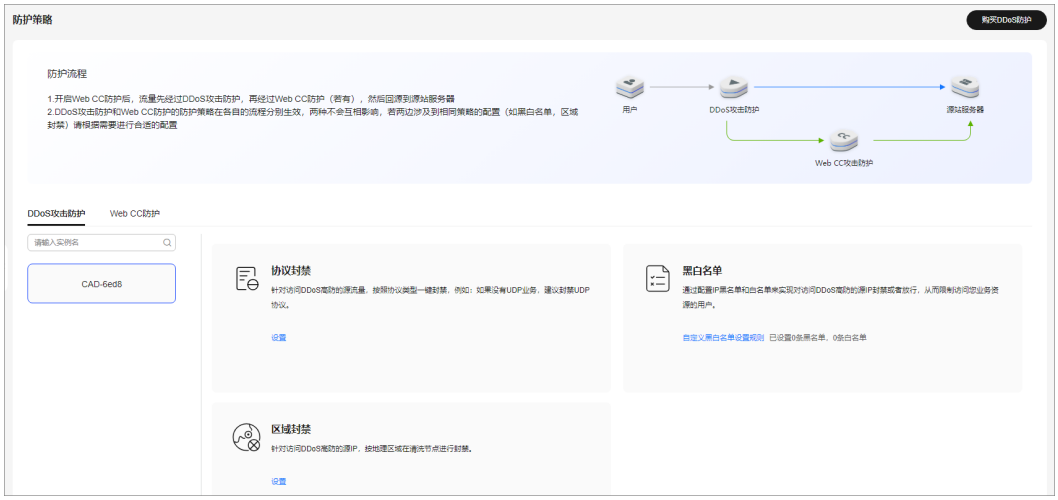
操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 防护策略”，进入DDoS高防“防护策略”页面。

图 3-23 DDoS 高防防护策略页面



步骤4 单击“Web CC防护”页签。

步骤5 选择需要防护的区域和对象后，在“频率控制”下方单击“自定义频率控制规则”。

图 3-24 频率控制

步骤6 单击“添加规则”。

步骤7 配置频率控制规则，如图3-25所示。

图 3-25 添加频率控制规则

表 3-8 参数说明

参数	说明
规则名称	自定义规则名称。

参数	说明
限速模式	● “源限速”：对源端限速，如某IP（或用户）的访问频率超过限速频率，就会对该IP（或用户）的访问限速。 – “IP限速”：根据IP区分单个Web访问者。 – “用户限速”：根据Cookie键值或者Header区分单个Web访问者。 – “其他”：根据Referer（自定义请求访问的来源）字段区分单个Web访问者。 **说明** 选择“其他”时，“Referer”对应的“内容”填写为包含域名的完整URL链接，仅支持前缀匹配和精准匹配的逻辑，“内容”里不能含有连续的多条斜线的配置，如“///admin”，WAF引擎会将“///”转为“/”。 例如：如果用户不希望访问者从“www.test.com”访问网站，则“Referer”对应的“内容”设置为“http://www.test.com”。 ● “目的限速”：对目的端限速。 – “策略限速”：当多个域名共用一个策略时，该策略下对应的所有域名请求次数合并限速(不区分访问IP)；泛域名防护场景时，该泛域名对应的所有子域名的请求次数合并限速(不区分访问IP)。 – “域名限速”：每个域名单独统计总请求次数，超过设定值则触发防护动作(不区分访问IP)。 – “URL限速”：每个URL请求单独统计请求次数，超过设定值则触发防护动作(不区分访问IP)。
域名聚合统计	“限速模式”选择“目的限速 > 策略限速”时，不需要配置此参数。 默认关闭，开启后，泛域名对应的所有子域名的请求次数合并限速(不区分访问IP)。例如，配置的泛域名为“*.a.com”，会将所有子域名（b.a.com，c.a.com等）的请求一起聚合统计。
用户标识	“限速模式”选择“源限速 > 用户限速”时，需要配置此参数： ● 选择“Cookie”时，设置Cookie字段名，即用户需要根据网站实际情况配置唯一可识别Web访问者的Cookie中的某属性变量名。用户标识的Cookie，不支持正则，必须完全匹配。例如：如果网站使用Cookie中的某个字段name唯一标识用户，那么可以用name字段来区分Web访问者。 ● 选择“Header”时，设置需要防护的自定义HTTP首部，即用户需要根据网站实际情况配置可识别Web访问者的HTTP首部。
限速条件	单击“添加”增加新的条件，至少配置一项条件，最多可添加30项条件，多个条件同时满足时，本条规则才生效。 ● “字段”：根据实际选择。 ● “子字段”：当“字段”选择IPv4、IPv6、Cookie、Header、Params时，请根据实际需求配置子字段。 ● “逻辑”：在下拉列表中选择需要的逻辑关系。 ● “内容”：输入或者选择条件匹配的内容。

参数	说明
限速频率	单个Web访问者在限速周期内可以正常访问的次数，如果超过该访问次数，Web应用防火墙服务将根据配置的“防护动作”来处理。 “全局计数”：根据不同的限速模式，将已经标识的请求在一个或多个WAF节点上的计数聚合。默认为每WAF节点单独计数，开启后本区域所有节点合并计数。“IP限速”不能满足针对某个用户进行限速，需要选择“用户限速”或“其他”的Referer限速，此时标识的请求可能会访问到不同的WAF节点，开启全局计数后，将请求访问的一个或多个WAF节点访问量聚合，达到全局统计的目的。
防护动作	当访问的请求频率超过“限速频率”时，可设置以下防护动作： ● “人机验证”：表示超过“限速频率”后弹出验证码，进行人机验证，完成验证后，请求将不受访问限制。人机验证目前支持英文。 ● “阻断”：表示超过“限速频率”将直接阻断。 ● “动态阻断”：上一个限速周期内，请求频率超过“限速频率”将被阻断，那么在下一个限速周期内，请求频率超过“放行频率”将被阻断。 ● “仅记录”：表示超过“限速频率”将只记录不阻断。
锁定验证	当“防护动作”选择“人机验证”时，需要配置该参数。 当人机验证未通过时，在设定时间内的访问都要进行验证。
放行频率	当“防护动作”选择“动态阻断”时，可配置放行频率。 如果在一个限速周期内，访问超过“限速频率”触发了拦截，那么，在下一个限速周期内，拦截阈值动态调整为“放行频率”。 “放行频率”需要小于等于“限速频率”。
生效时间	默认为“立即生效”。
阻断时长	当“防护动作”选择“阻断”时，可设置阻断后恢复正常访问页面的时间。
阻断页面	当“防护动作”选择“阻断”时，需要设置该参数，即当访问超过限速频率时，返回的错误页面。 ● 当选择“默认设置”时，返回的错误页面为系统默认的阻断页面。 ● 当选择“自定义”，返回错误信息由用户自定义。
页面类型	当“阻断页面”选择“自定义”时，可选择阻断页面的类型“application/json”、“text/html”或者“text/xml”。
页面内容	当“阻断页面”选择“自定义”时，可设置自定义返回的内容。

步骤8 单击“确定”。

----结束

后续操作

- 开启频率控制防护：在“Web CC防护”页面，将“频率控制”状态设置为 。
- 关闭频率控制防护：在“Web CC防护”页面，将“频率控制”状态设置为 。

3.4.5 开启 WEB 基础防护和 CC 防护

接入防护域名后，可以为域名开启WEB基础防护和CC防护。

前提条件

已成功接入防护域名。

约束条件

- WEB基础防护和CC防护仅对“网站类”业务类型且为源站类型为“源站IP”的转发规则生效。
- 开启“CC防护”前，需要先开启“WEB基础防护”。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-26 域名接入页

步骤4 将“WEB基础防护”和“CC防护”的状态设置为 ，开启WEB基础防护和CC防护。

说明

系统默认开启“流量攻击防护”。

----结束

3.5 开启告警通知

开启DDoS高防告警通知后，当出现以下情况时，您将接收到告警通知信息（接收消息方式由您设置）：

- IP遭受DDoS攻击。
- DDoS攻击峰值超过保底防护带宽而产生弹性计费。

如果您需要详细地监控服务各项指标，推荐您使用云监控服务设置监控告警规则和事件告警通知，具体操作请参考**监控**。

操作须知

- 消息通知服务为付费服务，价格详情请参见**SMN价格详情**。
- 在开启告警通知前，建议您先以管理员身份在“消息通知服务”中创建“消息主题”，详细操作请参见。
- 只支持显示和DDoS原生高级防护同一区域的通知主题。

前提条件

已成功购买并启用高防实例。

操作步骤

步骤1 **登录管理控制台**。

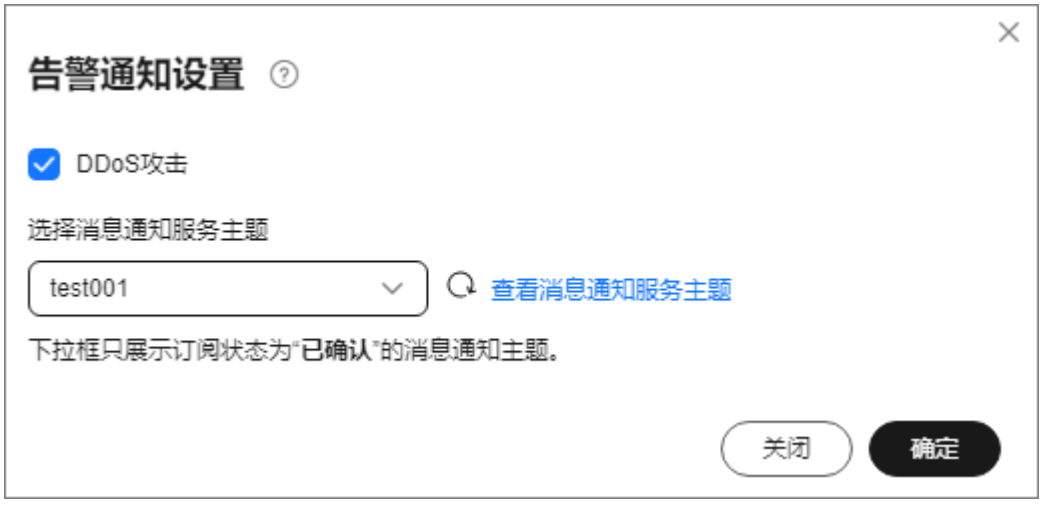
步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 实例列表”，进入“实例列表”页面。

步骤4 在实例列表右上角，单击“告警通知设置”。

步骤5 在弹出的“告警通知设置”对话框中，选中“DDoS攻击”。

图 3-27 “告警通知设置”对话框



单击下拉列表选择已创建的主题或者单击“查看消息通知服务主题”创建新的主题，用于配置接收告警通知的终端。

单击“查看主题”创建新主题的操作步骤如下：

1. 参见**创建主题**创建一个主题。

2. 配置接收告警通知的手机号码、邮件地址、函数、平台应用的终端、DMS或HTTP(S)终端，即为创建的主题添加一个或多个订阅，具体操作请参见**添加订阅**。
3. 确认订阅。添加订阅后，完成订阅确认。

更多关于主题和订阅的信息，请参见《消息通知服务用户指南》。

步骤6 单击“确定”，告警通知设置完成。

说明

如需关闭告警通知，在**图3-27**中，取消勾选“DDoS攻击”后，单击“确定”。

----结束

3.6 实例管理

3.6.1 查看实例信息

操作场景

该任务指导用户如何查看高防实例信息。

前提条件

已成功购买高防实例。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 实例列表”，进入“实例列表”页面。

步骤4 在实例列表界面，查看高防实例信息，相关参数说明如**表3-9**所示。

图 3-28 实例信息

表 3-9 实例参数说明

参数名称	说明
实例名称	• 高防实例的名称，单击名称右边的，可以更改实例名称。 • 高防实例到期的时间。 • 高防实例的业务宽带和宽带状态。 • 高防实例所属的企业项目。
业务带宽	实例的业务带宽。
弹性业务带宽	实例的弹性业务带宽。
防护区域	实例防护的区域范围。
线路信息	高防实例的线路和IP信息。
防护信息	高防实例的保底防护带宽、弹性防护带宽、防护端口数和防护域名数。 **说明** 如果需要调整弹性防护带宽，可以单击“编辑”，修改弹性防护带宽。
今日安全统计	高防实例统计最近24小时的防护信息，包括： • DDoS攻击峰值 • DDoS攻击次数

----结束

3.6.2 升级实例规格

操作场景

该任务指导用户如何变更高防实例的保底防护带宽、弹性防护带宽及业务带宽。

网站类接入的实例支持升级防护域名数，IP接入类的实例支持升级转发规则数。

说明

- 如果客户购买的是非BGP线路的三线实例（当前已不售卖），不提供升级规格功能，需要修改弹性带宽值请**提交工单**进行调整。
- 只有业务带宽和弹性防护带宽支持降低规格。
- 不支持升级时更换线路。
- 已到期的实例不支持升级。
- 已冻结的实例不支持升级。

前提条件

已拥有相关权限。

须知

请确认升级规格的账号同时具有“CAD Administrator”和“BSS Administrator”角色，或者该账号具有“Tenant Administrator”角色。

- BSS Administrator：费用中心、资源中心、账号中心的所有执行权限。项目级角色，在同项目中勾选。
- Tenant Administrator：除统一身份认证服务外，其他所有服务的所有执行权限。

费用说明

变更规格会引起费用的变化，详细的费用说明请参见**变更资源费用说明**。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 实例列表”，进入“实例列表”页面。

步骤4 在目标实例“实例名称”所在行，单击“变更规格”。

步骤5 在“DDoS高防变更规格”界面，调整实例规格。

图 3-29 调整规格

步骤6 单击“提交”，界面会判断选择的规格是否有变化，如果没有变化则弹出提示“规格无变化，无需升级”。否则跳转到下一步的确认界面。

步骤7 单击“去支付”，付款成功后，系统跳转至“支付成功”的界面。

----结束

3.6.3 修改弹性防护带宽

如果当前防护带宽不能满足业务实际需求，可以调整弹性防护带宽。

该任务指导用户如何修改高防实例的弹性防护带宽。

说明

- 弹性防护带宽的调整不涉及预付费。
- 如果客户购买的是非BGP线路的三线实例（当前已不售卖），不提供升级规格功能，需要修改弹性带宽值请**提交工单**进行调整。

前提条件

已成功购买高防实例。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 实例列表”，进入“实例列表”页面。

步骤4 在目标实例“实例名称”所在行，单击“变更规格”。

步骤5 在“DDoS高防变更规格”界面，调整弹性防护带宽。

图 3-30 调整规格

步骤6 单击“提交”，界面会判断选择的规格是否有变化，如果没有变化则弹出提示“规格无变化，无需升级”。否则跳转到下一步的确认界面。

步骤7 单击“去支付”，付款成功后，系统跳转至“支付成功”的界面。

----结束

3.6.4 开通自动续费

如果您购买实例时，开通了自动续费功能。当服务期满时，系统会自动按照购买的实例周期进行续费。您可以根据业务需求，选择开通自动续费功能。

说明

开通自动续费的资源可随时进行手动续费，手动续费成功后自动续费依然有效，系统将在资源新的到期时间前的第7天开始扣款。有关自动续费的详细介绍，请参见**续费规则说明**。

前提条件

已购买实例。

约束限制

请确认开通自动续费的账号同时具有“AAD FullAccess”和“BSS Administrator”角色，或者该账号具有“Tenant Administrator”角色。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 实例列表”，进入“实例列表”页面。

步骤4 在需要开通自动续费的实例所在行，单击“开通自动续费”，进入“开通自动续费”页面。

步骤5 在“开通自动续费”界面，选择“自动续费周期”和“自动续费次数”。

图 3-31 开通自动续费

步骤6 单击“开通”，按界面提示信息开通自动续费。

----结束

3.6.5 配置实例标签

标签由标签键和标签值组成，用于标识云资源。当您拥有相同类型的许多云资源时，可以使用标签按各种维度（例如用途、所有者或环境）对云资源进行分类。DDoS实例支持配置标签，方便管理实例。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 实例列表”，进入“实例列表”页面。

步骤4 在目标实例所在行，单击“标签”。

图 3-32 设置标签

步骤5 在标签添加页面，单击“添加标签”。

步骤6 选择“标签键”和“标签值”。

- 手动设置标签：手动输入标签键和标签值。
- 选择已有标签：选择已有的标签。

图 3-33 添加标签

说明

如您的组织已经设定本服务的相关标签策略，则需按照标签策略规则为资源添加标签。标签如果不符合标签策略的规则，则可能会导致标签添加失败，请联系组织管理员了解标签策略详情。

步骤7 单击“确定”。

----结束

3.7 域名管理

3.7.1 查看域名信息

操作场景

该任务指导用户如何查看域名信息。

前提条件

已成功接入防护域名。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-34 域名接入页

步骤4 查看域名信息。

表 3-10 参数说明

参数名称	说明
域名	防护的域名。
CNAME	• 域名通过CNAME解析的CNAME信息。 • 单击，可以复制“CNAME”。
实例与线路	• 域名的CNAME接入状态。 • 域名的实例线路信息，单击“查看详情”，可以查看域名配置的实例线路的详细信息。 • 开启“CNAME自动调度”，高防IP被黑洞时将自动进行DNS调度来保证业务的可用性。
源站IP/域名	填写的源站IP/域名。
业务类型	• 域名的业务类型。 • “HTTPS/WebSockets”证书的“更换”，单击“更换”，可以更新域名绑定的证书。详细操作，请参见更新证书。

参数名称	说明
安全防护	域名的流量攻击防护、WEB基础防护和CC防护开启状态。 • 对于配置了“源站IP”的“网站类”业务，用户可以为域名开启网站防护功能。 • 对于配置了“源站域名”的“网站类”业务，无需为域名开启网站防护功能。 • 对于“非网站类”业务，系统只提供默认开启的流量攻击防护。
企业项目	实例所属的企业项目。

----结束

3.7.2 更新证书

网站类业务接入DDoS高防，当“协议/端口”选择“HTTPS/WebSockets”且“源站类型”选择“源站IP”时，您需要上传证书（只支持TLS 1.0、TLS 1.1、TLS 1.2版本证书）使证书绑定到防护域名。

- 如果您购买的证书即将到期，为了不影响域名的使用，建议您在到期前重新购买证书，并在DDoS高防上同步更新域名绑定的证书。
- 如果您需要更新域名绑定证书的信息，可以在DDoS高防上为域名绑定新的证书。

须知

- 证书更新1分钟后生效，为避免影响业务，建议您在业务量较少的时段进行更新操作。
- 证书过期后，对源站的影响是覆灭性的，比主机崩溃和网站无法访问的影响还要大，建议您在证书到期前及时更新证书。
- 域名和证书需要一一对应，泛域名只能使用泛域名证书。如果您没有购买泛域名证书，只有单域名对应的证书，则只能在DDoS高防中按照单域名的方式逐条添加域名进行防护。

前提条件

网站类业务已成功接入DDoS高防。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-35 域名接入页

步骤4 在目标域名所在行的“业务类型”列，单击“更换”。

步骤5 在弹出的“更换证书”对话框中，上传新证书或者选择已有证书。

- 手动上传：输入证书名称，粘贴证书和私钥文本内容。当前仅支持PEM格式证书，非PEM格式的证书请参考**表3-11**转换。
- 自动拉取：选择已签发的证书。
- 选择已有证书：选择当前已使用的证书。

图 3-36 更换证书

表 3-11 证书转换命令

格式类型	转换方式
CER/CRT	将“cert.crt”证书文件直接重命名为“cert.pem”。
PFX	通过openssl工具进行转换。 提取私钥命令，以“cert.pfx”转换为“cert.key”为例。 **openssl pkcs12 -in cert.pfx -nocerts -out cert.key -nodes** 提取证书命令，以“cert.pfx”转换位“cert.pem”为例。 **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**

格式类型	转换方式
P7B	通过openssl工具进行转换。 1. 执行转换命令。**openssl pkcs7 -print_certs -in incertificat.p7b -out cert.cer** 2. 获取“cert.cer”文件中证书文件的内容。 3. 将证书内容保存为PEM格式。
DER	通过openssl工具进行转换。 1. 提取私钥命令，以“privatekey.der”转换为“privatekey.pem”为例。 **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** 2. 提取证书命令，以 “cert.cer”转换为“cert.pem”为例。 **openssl x509 -inform der -in cert.cer -out cert.pem**

说明

在Windows操作系统上执行openssl命令，请确保您已安装openssl工具。

步骤6 单击“确定”，证书更新完成。

----结束

3.7.3 修改域名的高防 IP 解析线路

操作场景

该任务指导客户进行如下操作：

- 关闭高防IP的域名解析功能。
- 新增域名的高防IP解析线路。
- 删除域名的高防IP解析线路。
- 导出域名的全量线路转发规则。

操作须知

修改域名的高防IP解析线路后约5分钟后生效。

前提条件

已成功接入防护域名。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-37 域名接入页

步骤4 在域名所在行的“实例与线路”列，单击“查看详情”。

步骤5 修改域名的高防IP解析线路，操作步骤如下：

- 关闭域名的高防IP解析线路。

  在线路详情页面，选择实例和线路后，将“域名解析”变更为  ，关闭该高防实例和线路下高防IP的域名解析功能。域名解析功能关闭后，用户仍然可以使用该高防IP的A记录方式。
- 新增域名的高防解析线路。
  a. 在线路详情页面，单击“新增实例线路”。
  b. 在“新增实例线路”对话框中，勾选新增的实例和线路，单击“确定”。
  c. 将“线路解析开关”变更为  ，开启新增的高防实例和线路下高防IP的域名解析功能。
- 删除域名的高防解析线路。
  a. 关闭待删除的高防IP的域名解析功能，详细步骤请参见**关闭域名解析**。
  b. 选择实例和线路，单击“删除线路”。
  c. 单击“确定”。
- 全量规则导出。

  在线路详情页面，单击“全量规则导出”，即可导出该域名的所有线路转发规则。

----结束

3.7.4 修改域名业务配置

操作场景

该任务指导用户如何修改网站类域名业务配置。

前提条件

已成功接入防护域名，且该防护域名的“业务类型”为“网站类”。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在页面上方选择“区域”后，单击页面左上方的，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-38 域名接入页

步骤4 在需要修改域名业务配置的域名所在行的“操作”列，单击“编辑”。

步骤5 在弹出的对话框“域名业务配置编辑”中，修改域名业务配置。

说明

- 如果要与其它域名复用同一个高防IP与端口，请确保其它域名与当前域名的“源站类型”相同。
- 如果要将域名的“源站类型”从“源站IP”改为“源站域名”时，请确保当前域名的“WEB基础防护”处于关闭状态。

图 3-39 修改域名业务配置

步骤6 单击“确定”。

----结束

3.7.5 删除域名

操作场景

当不需要防护某个域名时，可以删除该域名。

须知

删除域名前，用户需要确认DNS域名服务商处已将CNAME记录修改为CNAME对应的真实的IP地址。否则，直接删除域名将导致服务不可用。

前提条件

已成功接入防护域名。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-40 域名接入页

步骤4 在需要删除的域名所在行的“操作”列，单击“删除”。

步骤5 在弹出的对话框中，单击“确定”。

----结束

3.7.6 配置字段转发

DDoS高防支持为接入的域名配置字段转发，将添加的字段插入到header中转给源站。

前提条件

域名已接入DDoS高防。

约束限制

- 最多支持配置8个Key/Value值。
- 配置的Key值不能跟nginx原生字段重复。
- Value值可以自定义一个字符串，也可以配置为以$开头的变量。以$开头的变量仅支持配置如下字段：

```
$time_local
$request_id
$connection_requests
$tenant_id
$project_id
$remote_addr
$remote_port
$scheme
$request_method
$http_host
$origin_uri
$request_length
$ssl_server_name
$ssl_protocol
$ssl_curves
$ssl_session_reused
```

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-41 域名接入页

步骤4 在目标域名所在行的“高级配置”列，单击“编辑”。

步骤5 输入Key/Value值，单击“添加”。

图 3-42 配置字段

步骤6 单击“确认”。

----结束

3.7.7 修改 TLS 配置

DDoS高防支持修改HTTPS证书的TLS版本和加密套件。

前提条件

已上传证书。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 域名接入”，进入“域名接入”页面。

图 3-43 域名接入页

步骤4 在目标域名的“TLS配置”后，单击“编辑”。

步骤5 选择TLS版本和加密套件后，单击“确认”。

图 3-44 配置字段

----结束

3.8 防护日志管理

3.8.1 查看 DDoS 高防防护日志

操作场景

业务接入DDoS高防后，您可以通过查看高防实例线路的DDoS攻击防护日志和防护域名的CC攻击防护日志，了解当前业务的网络安全状态。

在“概览”页面，您可以查看以下防护日志信息：

- DDoS攻击防护

  可以查看高防实例线路的高防入流量峰值、攻击流量峰值和DDoS攻击次数信息，以及流量和报文两个维度的攻击类型分布、DDoS攻击事件、TOP5攻击类型流量清洗等信息。

- CC攻击防护

  可以查看防护域名请求与攻击次数、攻击类型分布、TOP5攻击源IP的次数等信息。

操作须知

- DDoS高防不支持下载防护日志数据。
- 在“概览”页面，您可以查看以下时间段的防护日志数据：
  - DDoS攻击防护

    可以查看指定高防实例和线路“24小时”、“近3天”、“近7天”、“近30天”和“自定义”的DDoS攻击防护数据，其中，“自定义”可以配置查看近90天的DDoS攻击防护数据。
  - CC攻击防护

    可以查看防护域名“昨天”、“今天”、“近3天”、“近7天”和“近30天”的CC攻击防护数据。

前提条件

已成功购买高防实例。

查看 DDoS 攻击防护日志

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 概览”，进入“概览”页面。

步骤4 单击“DDoS攻击防护”页签。

步骤5 选择待查看的实例名称、线路地址和历史时间段（24小时、近3天、近7天、近30天、自定义，其中，自定义可以查看90天内的防护日志），相关参数说明如表3-12所示。

图 3-45 DDoS 攻击防护

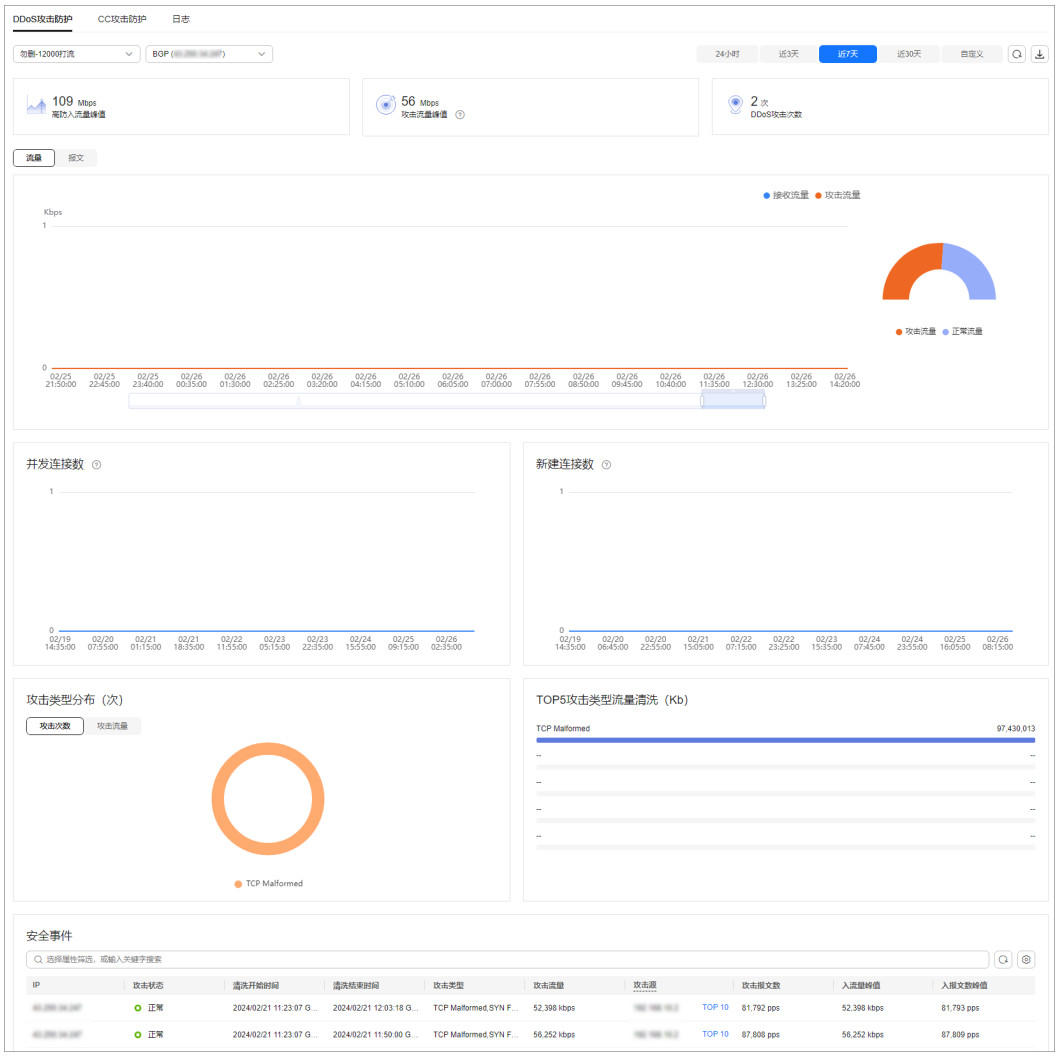


表 3-12 DDoS 攻击参数说明

参数	说明
高防入流量峰值	每秒访问指定实例指定IP的最高流量。
攻击流量峰值	每秒攻击指定实例指定IP的最高流量。
DDoS攻击次数	DDoS攻击指定实例指定IP的次数。
流量	查看接收流量和攻击流量趋势图。
报文	查看接收数据包和攻击数据包趋势图。
攻击类型分布	查看攻击事件类型。 • 单击“攻击次数”中的其中一个颜色区域，可查看指定域名被攻击的类型、攻击的次数、以及攻击占比。 • 单击“攻击流量”中的其中一个颜色区域，可查看指定域名被攻击的类型、攻击的流量、以及流量占比。

参数	说明
TOP5攻击类型流量清洗	TOP5攻击类型次数统计。
DDoS攻击事件	查看DDoS攻击事件。 ● 单击攻击源IP后的“详细”，可以查看完整的攻击源IP列表。 ● 攻击中的事件，单击“查看动态黑名单”，可以查看攻击中的黑名单列表。 **说明** 关于DDoS攻击事件报表中攻击源的字段，请您注意以下几点说明： ● 进行中的攻击事件可能不展示攻击源。 ● 一些只包含部分攻击类型的攻击事件不含攻击源。 ● 攻击源随机采样，不是全量的攻击源信息。

说明

在防护日志页面的流量或报文的图表中，不同的查询时间间隔对应的展示粒度不同，具体如下：

- 查询时间＜20分钟：展示粒度为1分钟。
- 20分钟＜查询时间＜40分钟：展示粒度为2分钟。
- 40分钟＜查询时间＜60分钟：展示粒度为3分钟。
- 1小时＜查询时间≤6小时：展示粒度为5分钟。
- 6小时＜查询时间≤24小时：展示粒度为10分钟。
- 1天＜查询时间≤7天：展示粒度为30分钟。
- 7天＜查询时间≤15天：展示粒度为1小时。
- 15天＜查询时间≤30天：展示粒度为14小时。

----结束

查看 CC 攻击防护日志

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS高防 > 概览”，进入“概览”页面。

步骤4 单击“CC攻击防护”页签。

步骤5 选择需要查看域名和时间范围，相关参数说明如表3-13所示。

表 3-13 CC 攻击防护参数说明

参数	说明
请求次数	访问者访问指定域名的总次数。 如果“全部域名”下拉列表中选择的是“全部域名”，则统计的是访问全部已开启WAF的域名的总次数。
请求峰值	每秒访问指定域名的最高次数。 如果“全部域名”下拉列表中选择的是“全部域名”，则统计的是每秒访问全部已开启WAF的域名的最高次数。
攻击次数	攻击指定域名的次数。
攻击源个数	攻击指定域名的攻击源个数。
次数统计（次）	• 请求次数：访问次数趋势图。 • 攻击次数：攻击次数趋势图。
攻击类型分布	查看攻击事件类型。 • 单击“攻击类型分布”中的其中一个颜色区域，可查看指定域名被攻击的类型、攻击的次数、以及攻击占比。 • 当不需要展示某种类型的攻击时，单击事件分布图右侧攻击类型对应的颜色方块，取消在事件分布圆环中的展示。
TOP5攻击源IP(次)	TOP5攻击源IP的攻击次数统计。

----结束

3.9 权限管理

3.9.1 创建用户并授权使用 AAD

如果您需要对您所拥有的AAD进行精细的权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用AAD资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将AAD资源委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用AAD服务的其它功能。

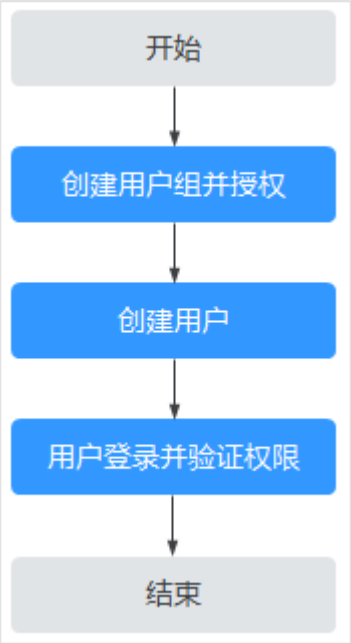
本章节为您介绍对用户授权的方法，操作流程如**图3-46**所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的AAD权限，并结合实际需求进行选择。

示例流程

图 3-46 给用户授权服务权限流程



1. **创建用户组并授权**
   在IAM控制台创建用户组，并授予DDoS高防服务权限“AAD FullAccess”。
2. **创建用户并加入用户组**
   在IAM控制台创建用户，并将其加入**1**中创建的用户组。
3. **用户登录**并验证权限
   新创建的用户登录控制台，验证权限：

   单击页面左上方的 ☰，选择除DDoS高防服务外（假设当前策略仅包含“AAD FullAccess”）的任一服务，如果提示权限不足，表示“AAD FullAccess”已生效。

3.9.2 AAD 自定义策略

如果系统预置的AAD权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参见**AAD权限及授权项**。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的AAD自定义策略样例。

AAD 自定义策略样例

- 示例1：授权用户查询防护策略

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aad:policy:get"
                        ]
        }
    ]
}
```

- 示例2：拒绝用户删除IP黑白名单规则

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循Deny优先。

  如果您给用户授予“AAD FullAccess”的系统策略，但不希望用户拥有“AAD FullAccess”中定义的删除IP黑白名单规则的权限（aad:whiteBlackIpRule:delete），您可以创建一条相同Action的自定义策略，并将自定义策略的Effect设置为“Deny”，然后同时将“AAD FullAccess”和拒绝策略授予用户，根据Deny优先原则用户可以对AAD执行除了删除IP黑白名单规则的所有操作。以下策略样例表示：拒绝用户删除IP黑白名单规则。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "aad:whiteBlackIpRule:delete"
            ]
        },
    ]
}
```

3.9.3 AAD 权限及授权项

如果您需要对您所拥有的AAD进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，IAM），如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用AAD的其它功能。

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为**角色**和**策略**。角色以服务为粒度，是IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。策略授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。

- 权限：允许或拒绝某项操作。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。

权限	授权项
查询实例详情	aad:instance:get
查询实例列表	aad:instance:list
创建实例	aad:instance:create
修改实例	aad:instance:put
查询证书列表	aad:certificate:list
上传证书	aad:certificate:create
删除证书	aad:certificate:delete
获取域名详情	aad:domain:get
获取域名列表	aad:domain:list
添加域名	aad:domain:create
编辑域名	aad:domain:put
删除域名	aad:domain:delete
查询防护策略	aad:policy:get
查询开启防护策略的域名列表	aad:policy:list
创建防护策略	aad:policy:create
更新防护策略	aad:policy:put
删除防护策略	aad:policy:delete
创建黑白名单规则	aad:whiteBlackIpRule:create
删除黑白名单规则	aad:whiteBlackIpRule:delete
查询黑白名单规则列表	aad:whiteBlackIpRule:list
查询配额	aad:quotas:get
查询转发规则	aad:forwardingRule:get
导出转发规则	aad:forwardingRule:list
添加转发规则	aad:forwardingRule:create
修改转发规则	aad:forwardingRule:put
删除转发规则	aad:forwardingRule:delete
查看数据报表	aad:dashboard:get
查询告警通知	aad:alarmConfig:get

权限	授权项
创建告警通知	aad:alarmConfig:create

3.10 监控

3.10.1 设置事件告警通知

操作场景

通过云监控服务，对DDoS高防启用事件监控，当出现黑洞、调度、攻击等事件时进行告警，方便您及时了解DDoS高防的防护情况。

开启事件告警通知后，出现相关事件时，即可在云监控服务的事件监控页面查看事件详情。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上方的，选择“管理与监管 > 云监控服务”。

步骤4 根据实际选择方式。

- 方法一：在左侧导航树，单击“事件监控”，进入“事件监控”页面。
- 方法二：在左侧导航树，选择“告警 > 告警规则”，进入“告警规则”页面。

步骤5 在页面右上方，单击“创建告警规则”，进入“创建告警规则”页面。

步骤6 参考表3-14配置告警参数。

图 3-47 告警参数

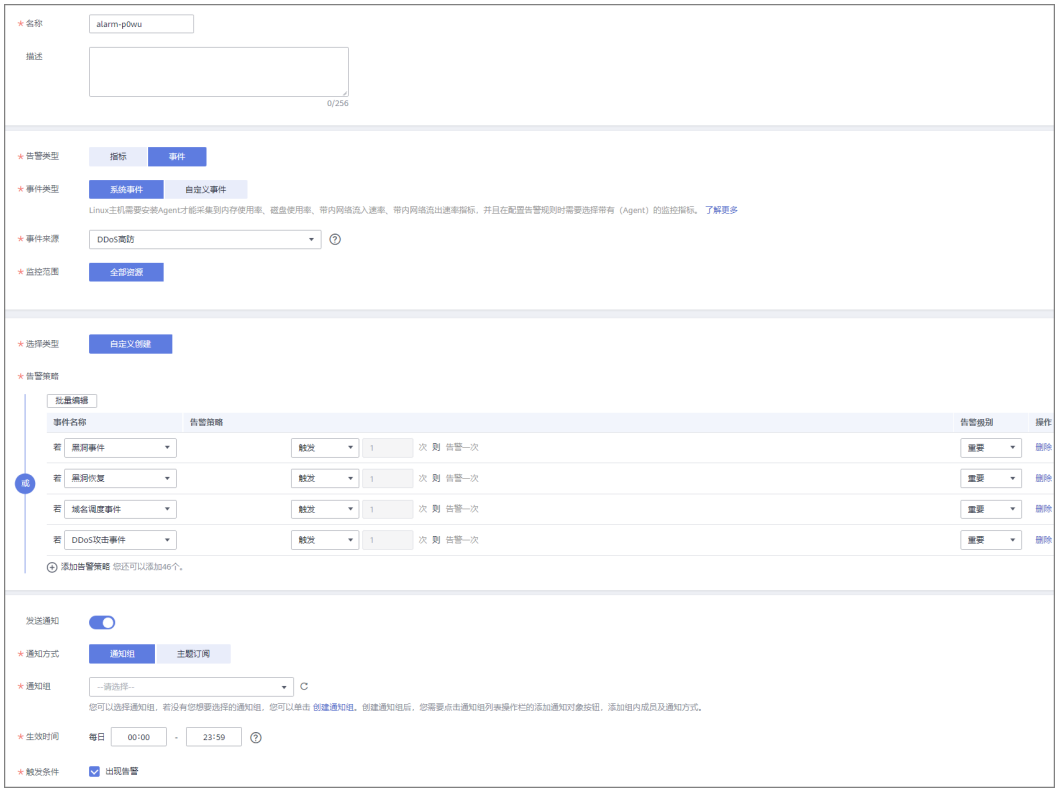


表 3-14 参数说明

参数	说明
名称	系统会随机产生一个名称，您也可以进行修改。
描述	告警规则描述。
告警类型	选择“事件”。
事件类型	选择“系统事件”。
事件来源	选择“DDoS高防”。
监控范围	选择“全部资源”。
选择类型	默认为“自定义创建”。
事件名称	推荐选择“黑洞事件”、“黑洞恢复”、“域名调度事件”、“DDoS攻击事件”。
触发方式	用户可根据该操作的严重程度选择触发或累计触发。
告警级别	根据告警的严重程度不同等级，可选择紧急、重要、次要、提示。

步骤7 根据实际需要，选择是否发送通知。

说明

告警消息由消息通知服务SMN发送，可能产生少量费用。

表 3-15 通知参数

参数	说明
发送通知	配置是否发送邮件、短信、HTTP和HTTPS通知用户。
通知方式	根据需要可选择通知组或主题订阅两种方式。
通知组	通知方式为通知组时生效，根据实际选择。
通知对象	通知方式为主题订阅时生效，根据实际选择。
生效时间	该告警规则仅在生效时间内发送通知消息。
触发条件	根据实际选择。

步骤8 单击“立即创建”，在弹出的窗口中单击“确定”，告警通知创建成功。

----结束

3.10.2 设置监控告警规则

通过设置DDoS告警规则，用户可自定义监控目标与通知策略，设置告警规则名称、监控对象、监控指标、告警阈值、监控周期和是否发送通知等参数，帮助您及时了解DDoS高防防护状况，从而起到预警作用。

为多个实例或实例防护的IP设置监控告警请参考**批量设置监控告警规则**；为某个指定实例或实例防护的IP设置监控告警请参考**为单个指定资源设置监控告警规则**。

如果您需要自主定义更多的监控指标，可通过API请求上报至云监控服务，具体操作请参考**添加监控数据**和**DDoS高防监控指标说明**。

前提条件

已购买DDoS高防实例。

批量设置监控告警规则

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上方的，选择“管理与监管 > 云监控服务 ”。

步骤4 在左侧导航树，选择“告警 > 告警规则”，进入“告警规则”页面。

步骤5 在页面右上方，单击“创建告警规则”，进入“创建告警规则”界面。

步骤6 填写告警规则信息，如**图 设置AAD监控告警规则**所示，填写规则如**表3-16**所示。

图 3-48 设置 AAD 监控告警规则

表 3-16 DDoS 高防告警规则参数说明

参数名称	参数说明
名称	系统会随机产生一个名称，您也可以进行修改。
描述	告警规则描述。
告警类型	选择告警类型。
资源类型	在下拉列表框中选择“DDoS服务”。
维度	选择需要监控的资源维度。 • 实例ID：DDoS高防实例维度。 • 实例ID-防护IP：DDoS高防实例防护的IP维度。
监控范围	告警规则适用的资源范围，可选择资源分组或指定资源。

参数名称	参数说明
触发规则	可选择“关联模板”、“导入已有模板”和“自定义创建”。创建自定义模板的具体操作请参考**创建自定义告警模板**。 **说明** 选择关联模板后，所关联模板内容修改后，该告警规则中所包含策略也会跟随修改。
模板	选择关联或导入的模板。
发送通知	配置是否发送邮件、短信、HTTP和HTTPS通知用户。
通知方式	需要发送告警通知的对象，可选择云通知组或主题订阅。 ● 云账号联系人为注册账号时的手机和邮箱。 ● 主题是消息发布或客户端订阅通知的特定事件类型，如果此处没有需要的主题则需先创建主题并订阅该主题，该功能会调用消息通知服务（SMN），创建主题并添加订阅请参见**创建主题**、**添加订阅**。
通知组（通知方式选择通知组时生效）	选择需要通知的组织。
通知对象（通知方式选择主题订阅时生效）	选择需要通知的主题。
生效时间	该告警规则仅在生效时间内发送通知消息。
触发条件	可以选择“出现告警”、“恢复正常”两种状态，作为触发告警通知的条件。

步骤7 单击“立即创建”，在弹出的提示框中，单击“确定”， 告警规则创建成功。

----结束

为单个指定资源设置监控告警规则

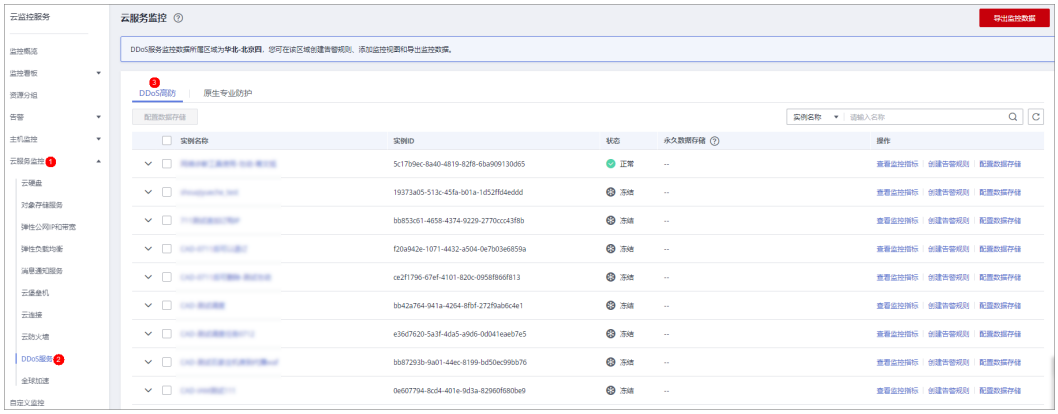
步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上方的，选择“管理与监管 > 云监控服务 ”。

步骤4 在左侧导航树，选择“云服务监控 > DDoS服务”，进入“DDoS高防”页面。

图 3-49 DDoS 高防



步骤5 在需要监控的对象所在行，单击“创建告警规则”。

图 3-50 选择监控对象

步骤6 填写告警规则信息，如**图 设置AAD监控告警规则**所示，填写规则如**表3-17**所示。

图 3-51 设置 AAD 监控告警规则

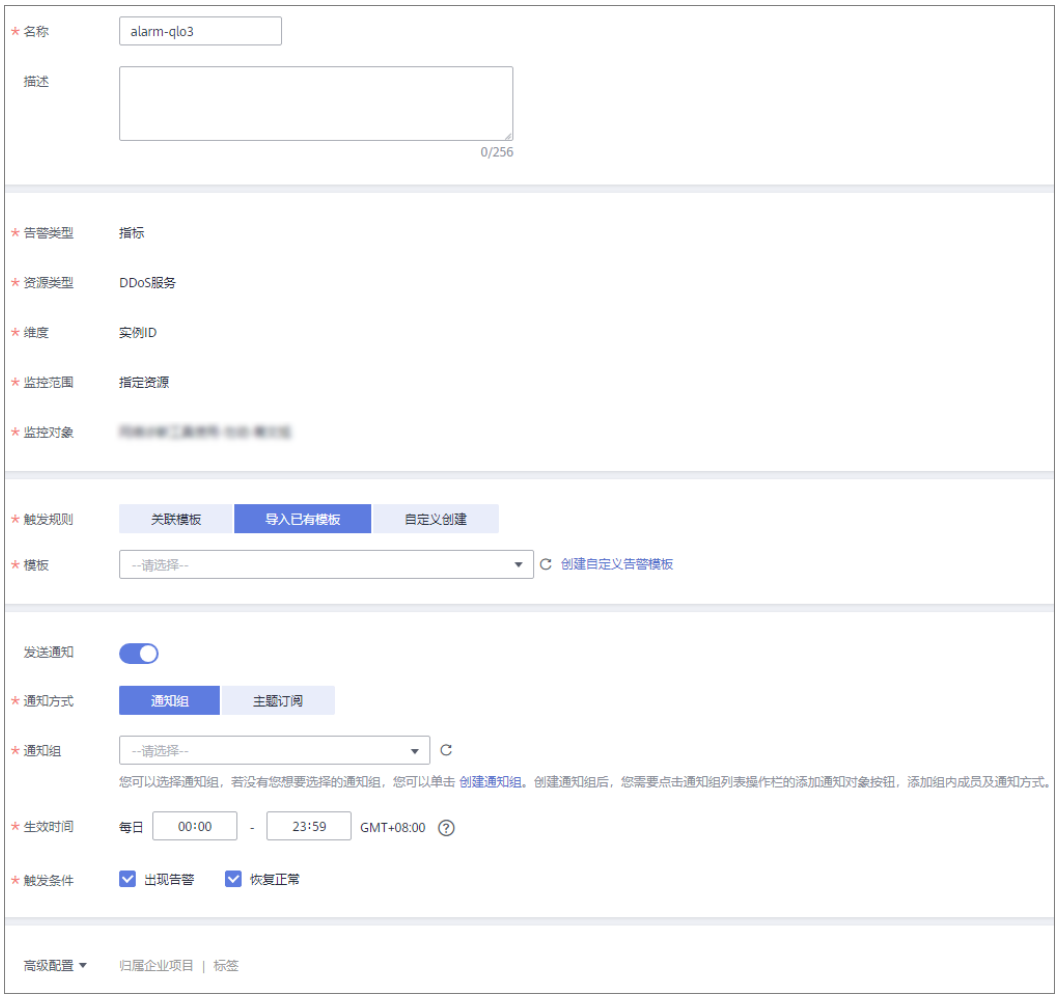


表 3-17 DDoS 高防告警规则参数说明

参数名称	参数说明
名称	系统会随机产生一个名称，您也可以进行修改。
描述	告警规则描述。
告警类型	保持默认。
资源类型	保持默认。
维度	保持默认。
监控范围	保持默认。
监控对象	保持默认。
触发规则	可选择“关联模板”、“导入已有模板”和“自定义创建”。创建自定义模板的具体操作请参考**创建自定义告警模板**。 **说明** 选择关联模板后，所关联模板内容修改后，该告警规则中所包含策略也会跟随修改。

参数名称	参数说明
模板	选择关联或导入的模板。
发送通知	配置是否发送邮件、短信、HTTP和HTTPS通知用户。
通知方式	需要发送告警通知的对象，可选择云通知组或主题订阅。 • 云账号联系人为注册账号时的手机和邮箱。 • 主题是消息发布或客户端订阅通知的特定事件类型，如果此处没有需要的主题则需先创建主题并订阅该主题，该功能会调用消息通知服务（SMN），创建主题并添加订阅请参见**创建主题**、**添加订阅**。
通知组（通知方式选择通知组时生效）	选择需要通知的组织。
通知对象（通知方式选择主题订阅时生效）	选择需要通知的主题。
生效时间	该告警规则仅在生效时间内发送通知消息。
触发条件	可以选择“出现告警”、“恢复正常”两种状态，作为触发告警通知的条件。

步骤7 单击“立即创建”，在弹出的提示框中，单击“确定”， 告警规则创建成功。

----结束

3.10.3 查看监控指标

您可以通过管理控制台，查看DDoS高防的相关指标，及时了解DDoS高防的防护状况，并通过指标设置防护策略。

前提条件

已在云监控页面设置监控告警规则。有关设置监控告警规则的详细操作，请参见**设置监控告警规则**。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 单击页面左上方的 ，选择“管理与监管 > 云监控服务 CES”。

步骤4 在左侧导航树栏，选择“云服务监控 > DDoS服务”，进入“云服务监控”页面。

步骤5 在需要查看的目标所在行，单击“查看监控指标”，查看对象的指标详情。

说明

在页面右上角单击“设置监控指标”，可以修改监控指标。

----结束

3.10.4 DDoS 高防监控指标说明

功能说明

本节定义了DDoS高防上报云监控服务的监控指标的命名空间和监控指标列表，用户可以通过云监控服务提供管理控制台来检索DDoS高防产生的监控指标和告警信息。

命名空间

SYS.DDOS

说明

命名空间是对一组资源和对象的抽象整合。在同一个集群内可创建不同的命名空间，不同命名空间中的数据彼此隔离。使得它们既可以共享同一个集群的服务，也能够互不干扰。

监控指标

表 3-18 DDoS 高防服务支持的监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
ip_drop_rate	丢弃流量	该指标为高防IP丢弃流量宽带	≥0kb/s	DDoS高防	5分钟
instance_drop_rate	丢弃流量	该指标为高防实例丢弃流量宽带	≥0kb/s	DDoS高防	5分钟
ip_back_to_source_rate	回源带宽	该指标为高防IP回源流量带宽	≥0kb/s	DDoS高防	5分钟
instance_back_to_source_rate	回源带宽	该指标为高防实例回源流量带宽	≥0kb/s	DDoS高防	5分钟
ip_internet_in_rate	入流量	该指标为高防IP入流量带宽	≥0kb/s	DDoS高防	5分钟
instance_internet_in_rate	入流量	该指标为高防实例入流量带宽	≥0kb/s	DDoS高防	5分钟
ip_new_connection	新建连接	该指标为高防IP新建连接数	≥0count/s	DDoS高防	5分钟
instance_new_connection	新建连接	该指标为高防实例新建连接数	≥0count/s	DDoS高防	5分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
ip_concurrent_connection	并发连接	该指标为高防IP并发连接数	≥0count/s	DDoS高防	5分钟
instance_concurrent_connection	并发连接	该指标为高防实例并发连接数	≥0count/s	DDoS高防	5分钟
ip_service_bandwidth_usage	业务带宽利用率	该指标为高防IP业务带宽利用率	≥0%	DDoS高防	5分钟
instance_service_bandwidth_usage	业务带宽利用率	该指标为高防实例业务带宽利用率	≥0%	DDoS高防	5分钟

维度

Key	Value
zone_ip	实例 - 防护IP
instance_id	实例ID

3.11 审计

3.11.1 云审计服务支持的 DDoS 高防相关操作

云审计服务（Cloud Trace Service，CTS）记录了DDoS高防相关的操作事件，方便用户日后的查询、审计和回溯，具体请参见**云审计服务用户指南**。

云审计服务支持的DDoS防护操作列表如**表3-19**所示。

表 3-19 云审计支持的 DDoS 高防操作列表

操作名称	资源类型	事件名称
新增域名	domainDns	domainDns
删除域名	deleteDomain	deleteDomain
购买	cadOpen	cadOpen
CNAME自动调度开关	cnameDispatchSwitch	cnameDispatchSwitch

操作名称	资源类型	事件名称
上传/修改证书	domainCert	domainCert
web基础防护开关和cc防护开关	domainSwitch	domainSwitch
编辑域名	domainConfigEdit	domainConfigEdit
添加转发规则	addProtocolRule	addProtocolRule
批量添加转发规则	importProtocolRule	importProtocolRule
批量删除转发规则	batchDelProtocolRule	batchDelProtocolRule
删除转发规则	deleteProtocolRule	deleteProtocolRule

3.11.2 查看云审计日志

开启了云审计服务后，系统开始记录DDoS防护资源的操作。云审计服务管理控制台保存最近7天的操作记录。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左侧的 ☰，选择“管理与监管 > 云审计服务”，进入云审计服务信息页面。

步骤3 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤4 在下拉框中选择“云服务”，输入“AAD”，按“Enter”。

步骤5 在查询结果中单击事件名称，查看事件详情。

事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：

- 事件名称、资源名称、资源ID、事件ID：需要输入某个具体的名称或ID。
  - 资源名称：当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。
  - 资源ID：当该资源类型无资源ID或资源创建失败时，该字段为空。
- 云服务、资源类型：在下拉框中选择对应的云服务名称或资源类型。
- 操作用户：在下拉框中选择一个或多个具体的操作用户。
- 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
  - normal：表示操作成功。
  - warning：表示操作失败。
  - incident：表示比操作失败更严重的情况，如引起其他故障等。

- 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近1周内任意时间段的操作事件。

----结束

4 DDoS 调度中心防护管理

4.1 购买 DDoS 调度中心防护

在使用DDoS调度中心防护前，您需要购买调度规则配额。购买成功后DDoS调度中心防护立即生效，您需要进一步配置DDoS阶梯调度策略。

操作步骤

购买DDoS调度中心防护

步骤1 登录管理控制台。

步骤2 在服务列表选择“安全与合规 > DDoS防护”，进入DDoS防护服务界面。

步骤3 在左侧导航栏选择“DDoS调度中心 > 阶梯调度”。

步骤4 单击界面右上角的“购买DDoS防护”。

- 规则数量：单个规则支持10个IP调度，购买多个规则可扩容IP调度总数。
- 购买时长：可选择1~3个月，6个月或1年。
- 自动续费：勾选后续可取消。

步骤5 确认规格无误后单击右下角“立即购买”，完成支付。

----结束

升级规格

如果您已购买DDoS调度中心防护，需要扩容规则，可通过升级规格购买规则数量。

步骤1 登录管理控制台。

步骤2 在服务列表选择“安全与合规 > DDoS防护”，进入DDoS防护服务界面。在左侧导航栏选择“DDoS调度中心 > 阶梯调度”。

步骤3 单击“升级规格”，如图4-1所示。在升级规格界面添加需要购买的规则数量，如图4-2所示。

图 4-1 升级规格

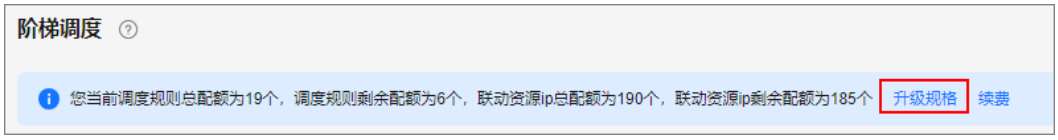


图 4-2 购买规则数

步骤4 单击右下角“提交”，完成支付。

----结束

续费

您的DDoS调度中心防护到期后，您可以申请续费。

步骤1 登录管理控制台。

步骤2 在服务列表选择“安全与合规 > DDoS防护”，进入DDoS防护服务界面。在左侧导航栏选择“DDoS调度中心 > 阶梯调度”。

步骤3 单击“续费”，如图4-3所示。根据需要选择续费时长和是否勾选“统一到期日”，如图4-4所示。

图 4-3 续费

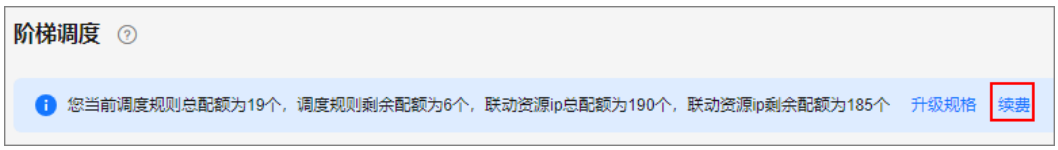


图 4-4 购买规格

说明

- 续费周期生效前进行变更，只能退订实例，不能退订续费周期。
- 续费资源不能享受5天无理由退订。

步骤4 单击右下角“提交”，完成支付。

----结束

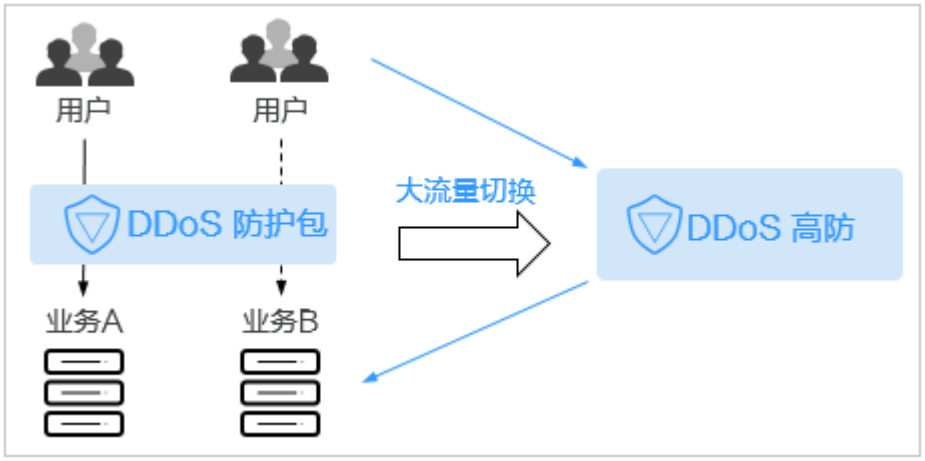
4.2 配置 DDoS 阶梯调度策略

购买DDoS原生防护-全力防基础版时选择开启联动防护后，通过配置DDoS阶梯调度策略，可以自动联动调度DDoS高防对DDoS原生防护-全力防基础版防护的云资源进行防护，防御海量攻击。

工作原理

DDoS原生高级防护自动联动调度DDoS高防的流程如图4-5所示。

图 4-5 联动调度流程图



前提条件

防护对象已接入DDoS高防。

约束条件

- DDoS高防仅支持对DDoS原生高级防护对象中的云资源进行联动防护。

- DDoS原生高防和DDoS高防需要配置不同的源站IP。
- DDoS调度中心暂不支持添加IPv6 IP。

有关配置源站IP的详细操作，请参见**步骤一：配置防护域名（网站类）**。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在服务列表选择“安全与合规 > DDoS防护”，进入DDoS防护服务界面。

步骤3 在左侧导航栏选择“DDoS调度中心 > 阶梯调度”。

步骤4 在阶梯调度列表框左上角，单击“添加规则”。

步骤5 在弹出的对话框中，设置调度规则参数，如**图4-6**所示，相关参数说明如**表4-1**所示。

图 4-6 添加调度规则

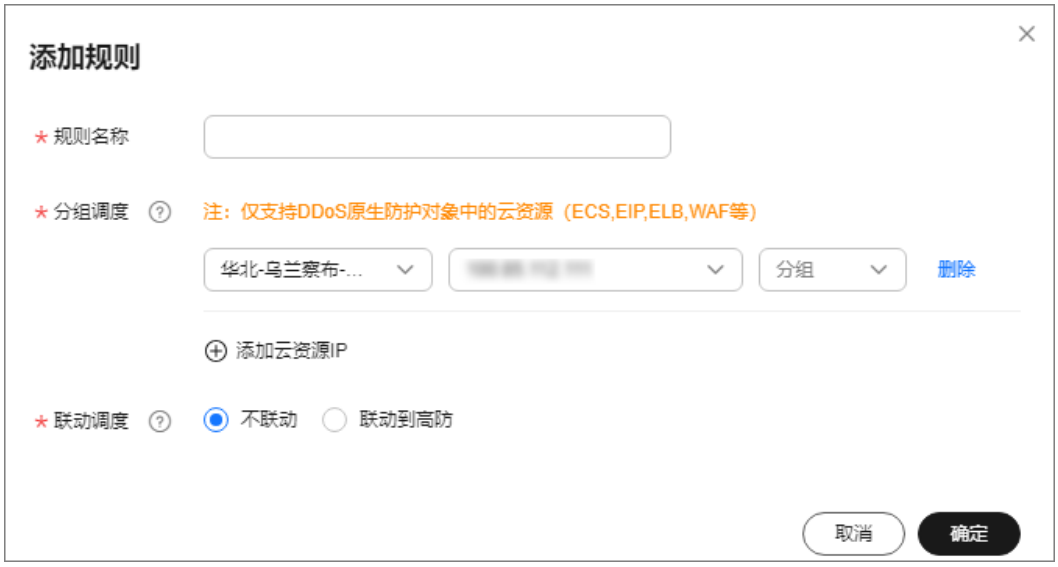


表 4-1 调度规则参数说明

参数	说明
规则名称	输入调度规则名称。 **说明** 一个规则可添加10个云资源IP，购买N个规则可添加的云资源IP总数为N*10个。

参数	说明
分组调度	填写局点、IP和调度分组。IP解析从1组开始依据分组进行。处于同一组的IP将同时发布解析。 默认分组：1。 **说明** • 当分组中存在被封禁的IP时，将跳过该IP对其他IP进行解析。 • 当前分组中所有IP被封堵后自动切换到下个分组，所有分组都无可用IP后进入联动调度。 • 仅支持DDoS原生防护对象中的云资源（ECS、EIP、ELB和WAF等）。
联动调度	• 不联动：只进行原生资源内的分组调度，不联动到高防DDoS防护。 • 联动到高防：调度到高防防护，需要提前购买并完成高防配置。

步骤6 单击“确定”完成配置。

----结束

相关操作

- 在目标调度规则所在行“操作”列，单击“删除”，可以删除该调度规则。
- 在目标调度规则所在行“操作”列，单击“查看详情”后，在弹出的页面中，可以查看调度规则的详细信息和添加的云资源信息。
  - 在基本信息后，单击，可以修改调度规则名称和是否联动调度。
  - 单击“添加资源”，在弹出的“添加联动资源”对话框中，修改、添加或删除云资源IP。
  - 在目标资源所在行的“操作”列，单击“删除”可以删除联动防护的云资源；或者勾选待删除的云资源后，在列表左上角单击“删除”，批量删除云资源。

4.3 开启阶梯调度告警通知

DDoS调度中心开启告警通知后，当防护IP发生以下事项时，您将接收到告警通知信息（接收消息方式由您设置）：

- 阶梯调度规则中的IP被封堵。
- 阶梯调度规则中的IP被解封。
- 某条阶梯调度规则中所有的IP被封堵后调度。
- 某条阶梯调度规则中所有的IP被封堵后，有一个IP被解封恢复调度。

前提条件

- 在开启告警通知前，建议您在“消息通知服务”中**创建主题**并**添加订阅**。
- 创建的主题需要订阅者确认，具体操作请参考**请求订阅**。

- 已成功配置DDoS阶梯调度策略。

操作步骤

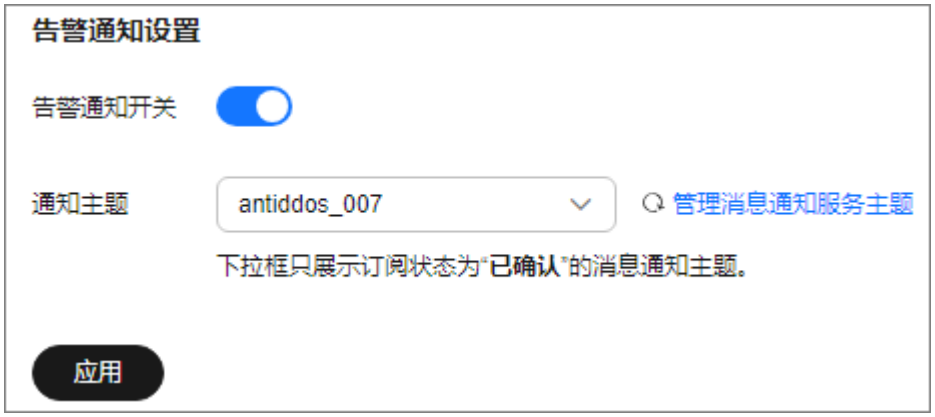
步骤1 登录管理控制台。

步骤2 在服务列表选择“安全与合规 > DDoS防护”，进入DDoS防护服务界面。在左侧导航栏选择“DDoS调度中心 > 告警通知”。

步骤3 在“告警通知”页面中，开启告警通知，即将告警通知开关设置为  。

步骤4 在“通知主题”下拉列表选择已创建的主题，如图4-7所示。

图 4-7 “告警通知设置”对话框



说明

- 只有订阅状态为“已确认”的主题才能显示在下拉框。
- 只有和DDoS调度中心相同区域的主题才能显示在下拉框。
- 消息通知服务为付费服务，价格详情请参见SMN价格详情。

步骤5 单击“应用”，告警通知设置完成。

----结束

相关操作

如需关闭告警通知，在图4-7中，关闭告警通知，即将告警通知开关设置为  。

4.4 配置 CDN 调度策略

开启CDN调度后，可自动联动调度DDoS高防对云资源进行防护。

前提条件

- 已购买和使用CDN服务。
- 已购买DDoS高防服务。

约束限制

您需要提交工单联系DDoS防护团队开通CDN调度功能权限。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面上方选择“区域”后，单击页面左上方的 ☰，选择“安全与合规 > DDoS防护 AAD”，进入“Anti-DDoS流量清洗”界面。

步骤3 在左侧导航栏选择“DDoS调度中心 > CDN调度”。

步骤4 在“CDN调度”页面中，单击上方的“添加规则”。

图 4-8 添加 CDN 调度规则

步骤5 在弹出的对话框中添加相关内容，具体填写规则见表4-2。

图 4-9 规则详情

表 4-2 规则填写详情

参数	说明
规则名称	输入CDN调度的自定义规则名称。

参数	说明
CDN域名	输入CDN域名（域名只能由字母、数字、-和.组成，且不能超过64个字符长度）。
服务范围	添加的CDN域名的服务范围，需和CDN页面上配置一致，支持“中国大陆”、“中国大陆境外”、“全球”。
CDN CNAME	输入CDN CNAME（只能由小写字母、数字和.组成，且不能超过128个字符长度）。
高防CNAME	输入高防CNAME（只能由小写字母、数字和.组成，且不能超过128个字符长度）。
切换条件	当访问QPS≥设置值时，触发调度。取值范围为100~10000。

步骤6 单击“确定”完成规则添加。

----结束

后续操作

- 编辑规则：在待编辑的规则所在行的“操作”列单击“编辑”，在弹出的对话框中修改相关参数。
- 删除规则：在待删除的规则所在行的“操作”列单击“删除”，在弹出的对话框中单击“确定”。

A 修订记录

发布日期	修改说明
2024-02-29	第四次正式发布。 ● 新增**配置字段转发**章节。 ● 新增**修改TLS配置**章节。 ● 下线“非域名类业务接入DDoS高防”章节。 ● 下线“转发规则管理”章节。 ● **查看数据报表**增加动态黑名单描述。 ● **查看DDoS高防防护日志**增加动态黑名单描述。 ● **查看防护对象信息**增加防护IP状态参数。
2023-09-30	第三次正式发布。 ● 新增**使用概览**章节。 ● 新增**使用概览**章节。
2022-04-27	第二次正式发布。 **购买实例**，更新购买参数。
2021-02-01	第一次正式发布。