

DDoS 防护 AAD

最佳实践

文档版本 03
发布日期 2024-06-30



版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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云计算技术有限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，华为云计算技术有限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。

目录

1 设置 DDoS 攻击告警通知.....	1
2 连接已被黑洞的服务器.....	3
3 提升 DDoS 防护能力.....	5

1 设置 DDoS 攻击告警通知

操作场景

开启DDoS攻击告警通知，当公网IP受到DDoS攻击时用户会收到提醒消息（接收消息方式由您设置）。

前提条件

- 已购买消息通知服务。
- 登录账号已购买公网IP。

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](#)。
- 在开启告警通知前，建议您在“消息通知服务”已[创建主题](#)并[添加订阅](#)。

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1-1](#)所示。

图 1-1 设置告警通知

公网IP 拦截报告 **告警通知** 日志

i 告警通知有可能被当成垃圾信息而拦截，如未收到告警通知，请确认是否被拦截。
此处只能配置清洗告警，如需配置黑洞封堵告警，请前往CES的事件监控配置。[如何配置CES黑洞封堵事件告警？](#)

清洗流量告警阈值 Kbps

SMN告警通知开关

消息通知主题 [查看消息通知主题](#)

下拉框只展示订阅状态为“已确认”的消息通知主题。

应用

表 1-1 设置告警通知

参数名称	说明
清洗流量告警阈值	当清洗流量大小达到该阈值时，发送告警通知，请根据实际需要设置阈值大小。
SMN告警通知开关	开启或关闭告警通知，说明如下： <ul style="list-style-type: none"><input checked="" type="checkbox"/>：开启状态。<input type="checkbox"/>：关闭状态。
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

2 连接已被黑洞的服务器

操作场景

当服务器遭受大流量攻击时，Anti-DDoS将调用运营商黑洞，屏蔽该服务器的外网访问。对于黑洞的服务器，您可以通过弹性云服务器连接该服务器。

前提条件

- 登录账号已购买公网IP。
- 已获取弹性云服务器的登录账号与密码。
- 已获取被黑洞的服务器的登录账号与密码。

约束条件

弹性云服务器与被黑洞的服务器同地域且可正常访问。

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，选择区域或项目。

步骤3 单击页面左上方的，选择“计算 > 弹性云服务器”，进入弹性云服务器管理界面。

步骤4 登录与被黑洞的服务器同地域且可正常访问的弹性云服务器。

弹性云服务器提供多种登录方式，请根据需要选择登录方式。

- 登录Windows弹性云服务器的详细介绍，请参见[Windows弹性云服务器登录方式概述](#)。
- 登录Linux弹性云服务器的详细介绍，请参见[Linux弹性云服务器登录方式概述](#)。

步骤5 连接黑洞状态的服务器，连接方式说明如[表2-1](#)所示。

表 2-1 连接黑洞服务器说明

弹性云服务器的操作系统	黑洞服务器的操作系统	连接方式
Windows	Windows	使用mstsc方式登录黑洞状态的服务器。 1. 在弹性云服务器中输入“mstsc”，单击mstsc打开远程桌面连接工具。 2. 在“远程桌面连接”的对话框中，单击“选项”。 3. 输入待登录的云服务器的弹性公网IP和用户名，默认为“Administrator”。 4. 单击“确定”，根据提示输入密码，登录服务器。
	Linux	使用PuTTY、Xshell等远程登录工具登录服务器。
Linux	Windows	1. 安装远程连接工具（例如 rdesktop ）。 2. 执行以下命令，登录黑洞状态的服务器。 rdesktop -u 用户名 -p 密码 -g 分辨率 黑洞服务器绑定的弹性公网IP地址
	Linux	执行以下命令，登录黑洞状态的服务器。 ssh 黑洞服务器绑定的弹性公网IP

----结束

后续操作

通过弹性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弹性云服务器，您也可以通过这种方式变更该服务器上的配置文件等。

3 提升 DDoS 防护能力

华为云Anti-DDoS流量清洗服务提供最高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。

如果急需恢复业务，建议您购买华为云DDoS高防服务，提升DDoS防护能力。