网络检测与响应

快速入门

文档版本 01

发布日期 2025-12-04

华为云计算技术有限公司

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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 安装 NDR 插件并开启加密流量检测.....1

1 安装 NDR 插件并开启加密流量检测

NDR支持对指定主机进行流量检测，检测到的攻击将被记录在攻击事件日志中。在加密流量检测场景下，业务之间的访问、传输、存储和交换等过程通常经过加密操作，NDR能够对加密后的服务器进程进行流量检测，从而进一步提升系统的安全性。

操作流程

本章节介绍如何配置NDR加密流量检测，流程如**图1-1**所示。

图 1-1 操作流程

操作步骤	说明
步骤一：准备主机	准备一台ECS主机并安装HSS服务Agent。
步骤二：购买NDR插件	购买NDR专业版插件，用于加密流量检测。
步骤三：开启加密流量检测	开启加密流量检测功能，用于检测加密流量的攻击特征。
步骤四：配置加密检测进程	配置需要开启加密流量检测的进程。
步骤五：查看检测结果	查看加密流量检测结果。

准备事项

1. 在使用服务之前，请先注册华为账号并开通华为云。具体操作详见**注册华为账号并开通华为云**和**实名认证**。

   如果您已开通华为云并进行实名认证，请忽略此步骤。
2. 请确保已为账号赋予相关权限。具体操作请参见**创建用户并授权使用NDR**。

> **说明**
>
> 如果用户已有符合要求的ECS服务器，可重复使用，无需再次创建。

步骤一：准备主机

用于加密流量检测的ECS服务器需要安装Agent，本文以购买一台ECS并免费试用1个月主机安全基础防护（默认安装了Agent）为例进行介绍。

> **说明**
>
> 如果用户已有符合要求的ECS服务器，可重复使用，无需再次创建。

步骤1 登录ECS服务控制台，进入**购买弹性云服务器**页面。

步骤2 在购买弹性云服务页面，设置购买参数。

表 1-1 购买参数设置

参数	示例	说明
区域	**华北-北京四**	请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。ECS购买后无法更换区域，请谨慎选择。
计费模式	**包年/包月**	该模式需先付费再使用，按照订单的购买周期进行结算。在购买之前，需确保账户余额充足。 更多信息，请参见**计费说明**。
可用区	**随机分配**	选择“随机分配”后，云平台会基于用户的UUID（Universally Unique Identifier）选择一个默认的可用区。ECS购买后无法更换可用区。
CPU架构	**x86计算**	弹性云服务器提供x86和鲲鹏架构的多种类型的实例规格。
实例筛选	**c6.xlarge.2**	请根据业务需要选择合适的规格。更多信息，请参见**规格清单**。
镜像	**公共镜像 > Huawei Cloud EulerOS 2.0 标准版 64位 (40 GiB)**	华为云提供的Linux类型公共镜像，该镜像免费。
开启安全防护	**勾选“开启完全防护”，并选择“基础防护”**	免费体验一个月企业主机安全基础版功能，提供口令检测、漏洞检测等功能。
其他参数	-	请根据实际情况设置。参数配置详情，请参见**快速购买和使用Linux ECS**。

步骤3 确认所有信息无误后，单击“立即购买”，在提示框中单击“同意并立即购买”，支付完成后，云服务器将自动创建，并默认开机。

云服务器状态为“运行中”后，将自动安装企业主机安全的Agent并开启“基础版”防护，这个过程预计需要20分钟左右。

----结束

步骤二：购买 NDR 插件

步骤1 **登录NDR控制台**。

步骤2 单击“购买网络检测与响应”。

图 1-2 开通服务

步骤3 根据实际配置服务参数。

表 1-2 参数说明

参数	示例	说明
区域	**华北-北京四**	选择需要检测流量的HSS主机所在区域。
计费模式	**包年/包月**	当前只支持包年/包月。
插件规格	**专业版**	• 基础版：支持检测未加密流量的攻击特征和全流量的流量记录，可扩容。 • 专业版：在基础版的基础上，支持检测加密流量的攻击特征，可扩容。
购买数量	**1**	需要购买的插件数量。
其他参数	-	请根据实际设置，参数说明请参考**购买NDR插件**。

步骤4 单击“下一步”。

步骤5 确认配置无误，单击“去支付”，根据提示完成购买。

----结束

步骤三：开启加密流量检测

步骤1 在左侧导航树中，选择“检测管理 > 检测策略”，进入“检测策略”页面。

步骤2 在目标服务器所在行，单击“安装”，选择需要安装的NDR插件。

图 1-3 安装插件

表 1-3 参数说明

参数	示例	说明
插件规格	**专业版**	选择已购买的专业版插件。
其他参数	-	请根据实际设置。

步骤3 确认配置无误，单击“确认”。

步骤4 勾选已安装插件的目标主机，单击“开启加密流量检测”按钮，开启加密流量检测。

步骤5 在弹窗中单击“确定”。

----结束

步骤四：配置加密检测进程

本文以检测加密系统默认进程为例，介绍如何配置加密检测进程。

步骤1 在目标服务器所在行，单击“加密进程配置”。

步骤2 在“系统内置”页签，打开“默认进程检测”的开关。

图 1-4 默认进程检测

步骤3 在弹窗中，单击“确定”。

----结束

步骤五：查看检测结果

步骤1 在左侧导航栏，选择“日志审计 > 日志分析 ”，进入“攻击事件日志”页面。

步骤2 在筛选框中选择需要查看的时间范围，“流量类型”选择“加密”，即可查看攻击检测结果。

图 1-5 检测结果

----结束

相关信息

- 关于流量检测策略的更多配置请参见**配置流量检测策略**。
- 如果您希望通过更多方式管理加密进程，请参见**管理加密进程**。