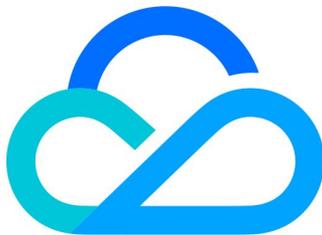


NDR 网络威胁检测系统

常见问题



腾讯云

【 版权声明 】

©2013–2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或 95716。

常见问题

最近更新时间：2025-04-14 15:18:42

NDR 网络威胁检测系统可以进行防护拦截吗？

NDR 网络威胁检测系统在订阅阻断服务后，支持旁路阻断功能，能够基于告警或 IP 地址阻断攻击流量。该系统配备了自动熔断机制，防止误拦截，同时支持开放API，实现在小流量场景下的“检测-响应”闭环。

软件化部署时，如何计算存储资源？

在默认日志存储策略下，NDR 网络威胁检测系统解析网络流量并存储全流量日志，将会占用较大的存储资源，按经验值，1Gbps流量每90天需要消耗15TB磁盘存储空间，若考虑数据高可用，磁盘空间将同步成倍增加，例如 ES 日志1副本，将消耗30TB磁盘存储空间。

NDR 网络威胁检测系统支持哪几种部署模式？

NDR 网络威胁检测系统支持单机部署与分布式部署两种模式。

- 小流量场景可使用单机部署模式，即流量采集与解析、沙箱分析系统、数据分析平台将在一台服务器上完成。
- 大流量场景推荐使用分布式部署模式，数据平台分析采用分布式架构，支持平行扩容，同时支持接入多个沙箱分析与流量采集探针。在分布式部署模式下，沙箱分析系统及流量采集探针也都具备平行扩容能力。

NDR 网络威胁检测系统支持东西向流量采集吗？

与 NDR 网络威胁检测系统探针部署的位置相关，若将汇聚层流量镜像到NDR网络威胁检测系统界探针，NDR网络威胁检测系统即能感知东西向流量。

NDR 网络威胁检测系统支持隔离网环境吗？

支持，NDR 网络威胁检测系统支持离线包升级，可以在隔离网中正常工作。

NDR 网络威胁检测系统安装部署需要多长时间？

NDR 网络威胁检测系统支持一键化简易部署，用户只需要将流量镜像到 NDR 网络威胁检测系统探针，NDR 网络威胁检测系统即能对网络流量进行分析感知，无需做复杂配置。