网络检测与响应

产品介绍

文档版本 01

发布日期 2025-12-04

华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 2025。 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


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

 版权所有 © 华为云计算技术有限公司

1 什么是网络检测与响应服务

网络检测与响应（Network Detection and Response，简称NDR）是基于华为多年攻防经验，运用特征规则、大数据分析、AI模型和威胁情报等技术，对企业网络流量进行实时检测、捕获、解码、审计，发现企业网络和系统中存在的安全风险和威胁，及时开展威胁响应处置，保障云资产安全。

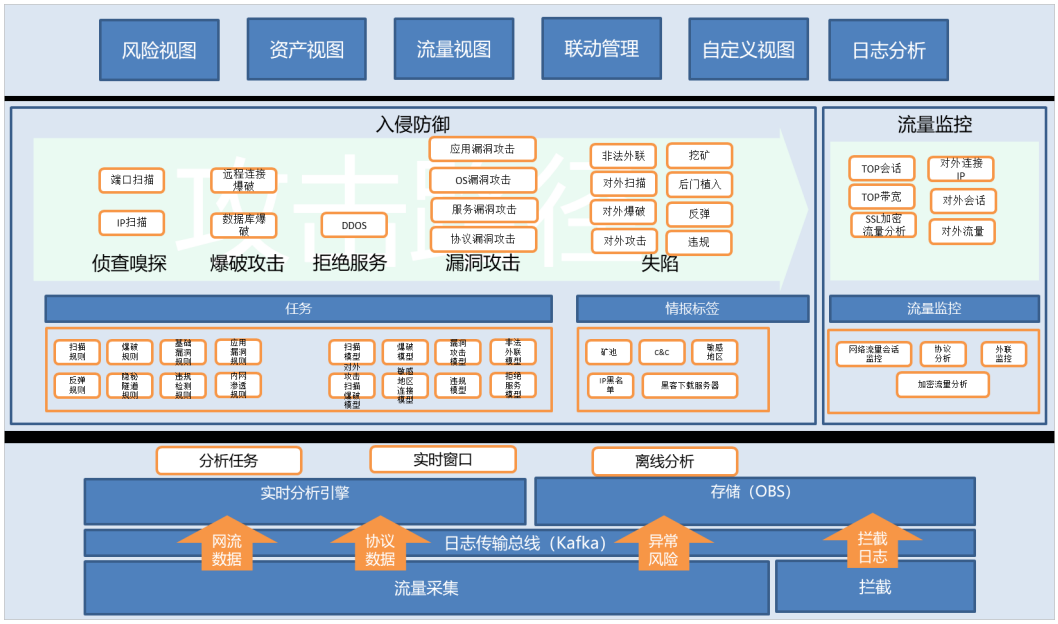
产品架构

NDR系统共分为三层，分别是平台层、业务层和应用层。

- **平台层**：提供东西向+南北向的流量采集能力，提供日志传输总线、阻断拦截、实施分析和数据存储的能力，是流量安全分析的基础底座
- **业务层**：NDR的核心任务是对流量型威胁进行入侵检测和流量监控。入侵防御方面，可实现对嗅探行为、爆破攻击和漏洞利用等威胁检测，依赖规则特征、威胁情报和检测模型；流量监控方面，可对云平台和租户的流量进行汇总统计，含五元组信息和字节报文数统计等，辅助安全业务人员分析流量异常和威胁研判
- **应用层**：结合业务层的分析数据，为安全业务人员提供可视化能力，包含风险视图报表，日志查询分析系，威胁研判处置等功能，最终实现威胁的响应及处置。

版权所有 © 华为云计算技术有限公司

图 1-1 产品架构



版权所有 © 华为云计算技术有限公司

2 产品优势

多场景防御

预置多种检测和拦截模型，轻松应对多种攻击场景。

- **暴力破解**：21（FTP）、22（SSH）、1433/3306（MySQL）、3389（RDP）等
- **扫描**：扫描工具、漏洞扫描
- **恶意程序**：非法挖矿
- **异常协议**：异常报文
- **注入**：SQL注入、命令注入
- **数据泄露**：敏感信息泄露、任意文件读取、目录遍历
- **漏洞利用**：缓冲区溢出、提权绕过、代码执行
- **网站攻击**：XSS跨站脚本、SSRF/CSRF请求伪造
- **后门**：后门木马、WebShell

全日志审计

提供丰富的日志，精准定位每一次攻击事件，让危险无处可藏。

- 攻击事件日志
- 流量日志
- 审计日志

高精度拦截

基于深度流检测（Deep Flow Inspection，DFI）技术，对关键网络区域南北向的底层网络流量数据包（包括带宽、网络协议、基于网段的业务、网络异常流量、应用服务异常等）进行采集和分析，检测准确度达99%，有效避免误报。

多协议解析

支持多种应用协议的解析，全面提升解析能力，NDR支持的协议如下：

- Telnet
- SMTP

 版权所有 © 华为云计算技术有限公司

- DHCP
- FTP
- MySQL
- IMAP
- SSH
- SMB
- DNS
- RDP
- HTTP
- TLS
- MSSQL

 版权所有 © 华为云计算技术有限公司

3 应用场景

拦截恶意攻击

通过分析7层协议（包括HTTP/MySQL等交互协议），对满足一些恶意特征的请求进行检测，并产生响应告警。通过安全运营手段进一步确认之后，通过IP黑名单的方式进行阻断和拦截，避免黑客利用云主机的漏洞和脆弱性实施攻击。NDR支持拦截的恶意攻击类型包括但不限于以下类型：

- 目录遍历攻击
- 信息泄露攻击
- WebShell、后门木马攻击
- SQL注入攻击
- 文件包含、文件上传攻击
- 绕过、提权攻击
- 跨站脚本、请求伪造攻击
- 代码执行攻击
- Web管理平台爆破（phpmyadmin、wordpress）

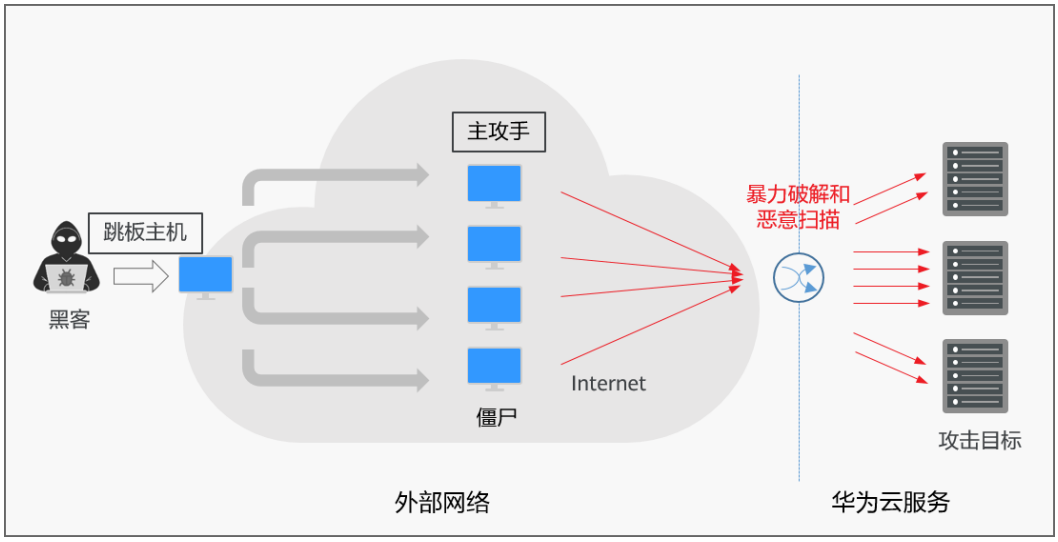
阻断暴力破解和恶意扫描

通过网络流量分析，在时间维度上针对包含暴力破解和恶意扫描特征的请求进行检测，并产生告警。通过安全运营手段进一步确认之后，通过IP黑名单的方式进行阻断和拦截。

当云主机被黑客暴力破解后，主机即成为“僵尸/肉鸡”，黑客通常会通过跳板机来控制僵尸主机进行二次暴力破解和恶意扫描，企图扩大被控制主机的数量。其原理如图3-1所示。

 版权所有 © 华为云计算技术有限公司

图 3-1 云主机暴力破解和恶意扫描



- 暴力破解

  NDR支持对FTP、SSH、RDP协议的暴力破解检测和拦截；并对数据库，包括MS-SQL、MySQL的恶意访问进行检测和拦截；同时针对常见Web管理后台的暴力破解进行检测，包括phpmyadmin、wordpress。

- 恶意扫描

  NDR支持对常见扫描工具、漏洞扫描进行检测：如nmap扫描、zmap扫描、RPC漏洞扫描、CLDAP反射扫描，发现并记录风险事件。

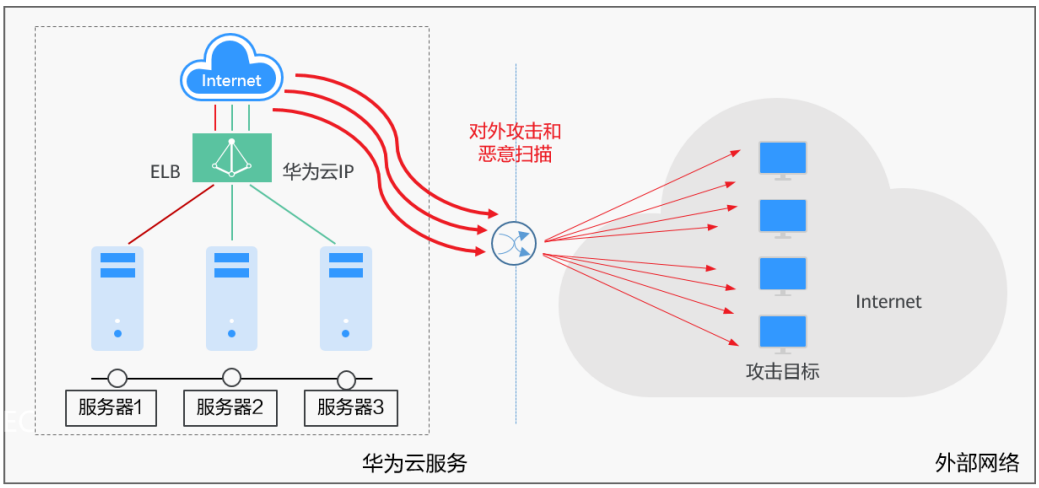
拦截主机对外攻击

黑客通过上传木马后门去控制僵尸主机，并通过僵尸主机对外发动攻击（如暴力破解、恶意扫描、DDoS攻击），让企业无法溯源到真实的攻击源信息。

其原理如图3-2所示。

NDR支持对被控制主机对外的攻击行为进行检测和拦截。

图 3-2 云主机被控制后对外发起攻击



版权所有 © 华为云计算技术有限公司

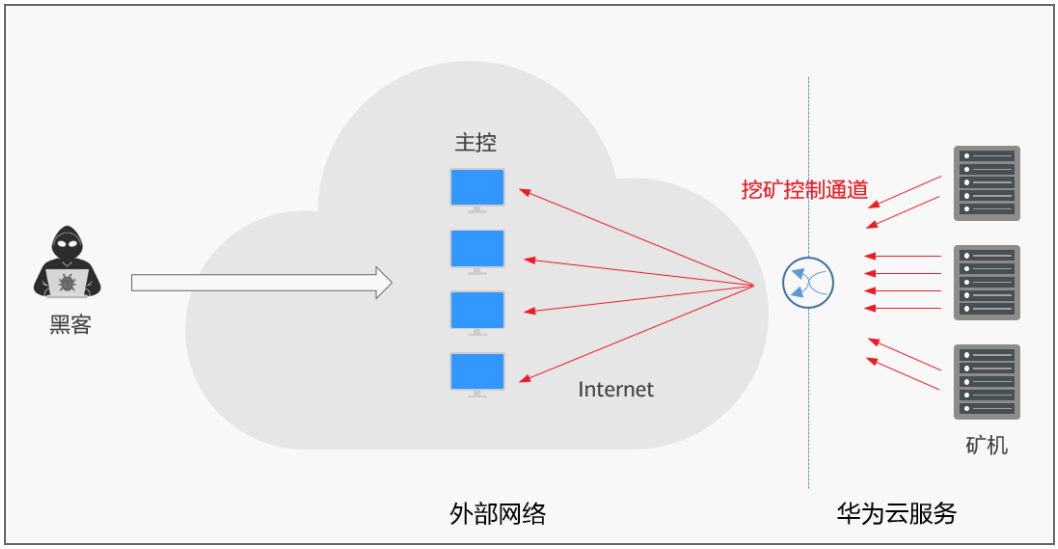
阻断主机挖矿

挖矿是指使用大算力或海量服务器挖掘虚拟货币的通俗说法。因为有利可图，黑客通过控制主机来进行挖矿，期间会占用大量CPU、带宽等资源，影响正常业务运行的同时造成巨大的资源浪费。

当黑客控制多台主机后，即可在主机上部署挖矿脚本，此脚本通过专门的挖矿控制通道与黑客的控制端通讯。其原理如图3-3所示。

NDR支持对非法挖矿行为进行检测和拦截，有效防止因挖矿带来的资源浪费及业务中断。

图 3-3 主机被控制后挖矿



流量审计

NDR可以记录高危协议、中间件应用、黑客工具的访问日志，可以用于流量审计和分析。

版权所有 © 华为云计算技术有限公司

4 产品功能

本页面介绍了NDR服务支持的主要功能。关于各功能支持的地域（Region）信息，可通过控制台查询详情。

防御规则

NDR内置多种基础防御规则，能预防大规模威胁入侵，有效保护资产，提升系统安全性。有关更多信息请参阅**配置基础防御规则**。

流量检测

NDR支持对指定VPC内的ECS主机配置流量检测策略，开启检测策略后，检测到的攻击将会记录到攻击事件日志。

加密流量检测场景下，NDR支持开启内置进程加密，也支持用户对指定进程进行加密。

用户将服务器运行中的进程配置为加密进程后，NDR将对加密后的进程进行加密流量检测，进一步提高系统的安全性。有关更多信息请参阅**配置流量检测策略**。

日志管理

NDR提供攻击事件日志、流量日志和审计日志，全面记录攻击源和攻击目标的详细信息，帮助用户精准定位网络攻击。有关更多信息请参阅**查看日志**。

攻击告警

设置告警通知后，NDR可将触发的告警信息通过您设置的接收通知方式（例如邮件或短信）发送给您，您可以及时监测防护状态，迅速获得异常情况。有关更多信息请参阅**开启攻击事件告警通知**。

流量分析

通过“流量分析”页面，您可以查看特定时间内不同流量源头到NDR的访问流量详情。有关更多信息请参阅**查看流量访问详情**。

版权所有 © 华为云计算技术有限公司

安全分析

通过安全分析页面，您可以查看流量检测告警的信息、告警的趋势和分布、攻击者和受害IP分布以及TOP攻击类型、攻击者地理分布等信息。有关更多信息请参阅**查看安全分析信息**。

攻击趋势

NDR支持查看入方向、出方向及内部的TOP攻击类型排行、攻击类型分布等信息，帮助用户了解攻击趋势。有关更多信息请参阅**查看攻击趋势**。

ATT&CK 矩阵

NDR支持对发现的攻击进行ATT&CK模型分类展示，您可以快速查看指定时间段内使用某一类ATT&CK技术攻击的所有日志。有关更多信息请参阅**查看ATT&CK矩阵**。

攻击者画像

NDR支持对攻击者提供画像和溯源，可帮助用户查看攻击者地理分布、攻击源IP具体信息等。有关更多信息请参阅**管理攻击者画像**。

插件管理

NDR支持为主机安装插件包，安装插件包后，可以对主机进行加密流量检测。已购买的插件支持规格变更、更新等操作。有关更多信息请参阅**管理主机插件**。

版权所有 © 华为云计算技术有限公司

5 安全

5.1 责任共担

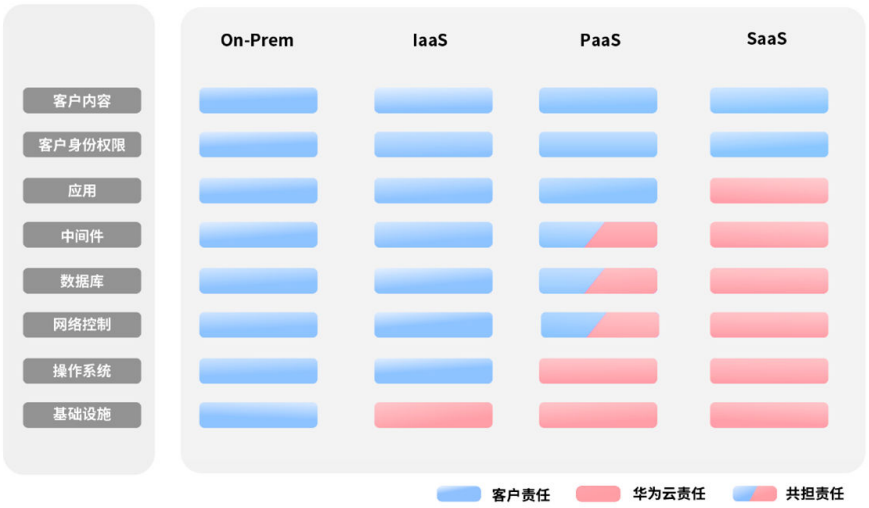
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

与传统的本地数据中心相比，云计算的运营方和使用方分离，提供了更好的灵活性和控制力，有效降低了客户的运营负担。正因如此，云的安全性无法由一方完全承担，云安全工作需要华为云与您共同努力，如图5-1所示。

- **华为云**：无论在任何云服务类别下，华为云都会承担基础设施的安全责任，包括安全性、合规性。该基础设施由华为云提供的物理数据中心（计算、存储、网络等）、虚拟化平台及云服务组成。在PaaS、SaaS场景下，华为云也会基于控制原则承担所提供服务或组件的安全配置、漏洞修复、安全防护和入侵检测等职责。
- **客户**：无论在任何云服务类别下，客户数据资产的所有权和控制权都不会转移。在未经授权的情况下，华为云承诺不触碰客户数据，客户的内容数据、身份和权限都需要客户自身看护，这包括确保云上内容的合法合规，使用安全的凭证（如强口令、多因子认证）并妥善管理，同时监控内容安全事件和账号异常行为并及时响应。

版权所有 © 华为云计算技术有限公司

图 5-1 华为云安全责任共担模型



云安全责任基于控制权，以可见、可用作为前提。在客户上云的过程中，资产（例如设备、硬件、软件、介质、虚拟机、操作系统、数据等）由客户完全控制向客户与华为云共同控制转变，这也就意味着客户需要承担的责任取决于客户所选取的云服务。如图5-1所示，客户可以基于自身的业务需求选择不同的云服务类别（例如IaaS、PaaS、SaaS）。不同的云服务类别中，每个组件的控制权不同，这也导致了华为云与客户的责任关系不同。

- 在On-prem场景下，由于客户享有对硬件、软件和数据等资产的全部控制权，因此客户应当对所有组件的安全性负责。
- 在IaaS场景下，客户控制着除基础设施外的所有组件，因此客户需要做好除基础设施外的所有组件的安全工作，例如应用自身的合法合规性、开发设计安全，以及相关组件（如中间件、数据库和操作系统）的漏洞修复、配置安全、安全防护方案等。
- 在PaaS场景下，客户除了对自身部署的应用负责，也要做好PaaS服务中间件、数据库、网络控制的安全配置和策略工作。
- 在SaaS场景下，客户对客户内容、账号和权限具有控制权，客户需要做好自身内容的保护以及合法合规、账号和权限的配置和保护等。

传统本地部署(On-Prem)：由客户在自有数据中心内部署和管理软件及IT基础设施，而非依赖于远程的云服务提供商；

基础设施即服务(IaaS)：由云服务提供商提供计算、网络、存储等基础设施服务，如**弹性云服务器 ECS**、**虚拟专用网络 VPN**、**对象存储服务 OBS**；

平台即服务(PaaS)：由云服务提供商提供应用程序开发和部署所需要的平台，客户无需维护底层基础设施，如**AI开发平台 ModelArts**、**云数据库 GaussDB**；

软件即服务 (SaaS)：由云服务提供商提供完整应用软件，客户直接应用软件而无需安装、维护应用软件及底层平台和基础设施，如**华为云会议 Meeting**。

5.2 身份认证与访问控制

NDR对接了统一身份认证服务（Identity and Access Management，IAM）服务。IAM权限是作用于云资源的，IAM权限定义了允许和拒绝的访问操作，以此实现云资源

版权所有 © 华为云计算技术有限公司

权限访问控制。通过IAM，可以将用户加入到一个用户组中，并用策略来控制他们对华为云资源的访问范围。

关于对NDR资源的访问权限，详细请参考**权限管理**。

5.3 数据保护技术

NDR通过如下数据保护手段和特性，保障NDR中的数据安全可靠。

数据保护手段	说明
静态数据保护	NDR通过敏感数据加密保证用户流量中敏感数据的安全性。
传输中的数据保护	微服务间管理数据传输进行加密，防止数据在传输过程中泄露或被篡改。用户的配置数据传输采用安全协议HTTPS，防止数据被窃取。
数据完整性校验	NDR进程启动时，配置数据从配置中心获取而非直接读取本地文件。
数据隔离机制	租户区与管理面隔离，租户的所有操作权限隔离，不同租户间的策略、日志等数据隔离。
数据销毁机制	考虑到残留数据导致的信息泄露问题，华为云根据客户等级设定了不同的保留期时长，保留期到期仍未续订或充值，存储在云服务中的数据将被删除，云服务资源将被释放。NDR对云服务自动感知并在保留期到期后释放资源。

5.4 审计与日志

云审计服务（Cloud Trace Service，以下简称CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

CTS可记录的NDR操作详见开通云审计服务中的“云审计服务支持的NDR操作列表”。用户开通云审计服务并创建和配置追踪器后，CTS开始记录操作事件用于审计，开通方法参见**CTS快速入门**。开通云审计服务后，可查看NDR的云审计日志，云审计服务保存最近7天的操作日志。

CTS支持配置关键操作通知。用户可将与NDR相关的高危敏感操作，作为关键操作加入到CTS的实时监控列表中进行监控跟踪。当用户使用NDR服务时，如果触发了监控列表中的关键操作，那么CTS会在记录操作日志的同时，向相关订阅者实时发送通知。

5.5 服务韧性

华为云数据中心按规则部署在全球各地，所有数据中心都处于正常运营状态，无一闲置。数据中心互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。为了减少由硬件故障、自然灾害或其他灾难带来的服务中断，华为云数据中心提供灾难恢复计划。

版权所有 © 华为云计算技术有限公司

当发生故障时，NDR的五级可靠性架构支持不同层级的可靠性，因此具有更高的可用性、容错性和可扩展性。

华为云NDR已面向全球用户服务，并在多个分区部署，同时NDR的所有管理面、引擎等组件均采用主备或集群方式部署。

5.6 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

版权所有 © 华为云计算技术有限公司

图 5-2 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 5-3 资源中心

 版权所有 © 华为云计算技术有限公司

合规资质证书

华为云安全服务提供了网络安全专用产品安全检测证书、软件著作权等证书，供用户下载和参考。具体请查看**合规资质证书**。

图 5-4 网络安全专用产品安全检测证书&软件著作权证书

版权所有 © 华为云计算技术有限公司

6 权限管理

如果您需要对华为云上创建的网络检测与响应（NDR）资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全地控制华为云资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并授权控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有NDR的使用权限，但是不希望他们拥有删除NDR资源等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用NDR，但是不允许删除NDR资源的权限，控制他们对NDR资源的使用范围。

如果华为账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用NDR服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。

关于IAM的详细介绍，请参见**IAM产品介绍**。

NDR 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

NDR部署时通过物理区域划分，为项目级服务，授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如华北-北京1）对应的项目（cn-north-1）中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问NDR时，需要先切换至授权区域。

如**表6-1**所示，包括了NDR的所有系统角色。由于云上各服务之间存在业务交互关系，NDR服务的角色依赖其他服务的角色实现功能。因此给用户授予NDR服务的角色时，需要同时授予依赖的角色，NDR服务的权限才能生效。

 版权所有 © 华为云计算技术有限公司

表 6-1 NDR 系统角色

策略名称	描述	依赖关系
NDR FullAccess	网络检测与响应服务所有权限	-
NDR ReadOnlyAccess	网络检测与响应服务只读权限	-
NDR AgencyAccess	网络检测与响应服务默认操作策略	-

版权所有 © 华为云计算技术有限公司

7 约束与限制

NDR 插件的资源使用限制

- NDR插件最多占用主机5%的CPU资源。
- NDR插件最多占用主机256MB物理内存，超出后插件会被卸载。
- NDR插件最多占用主机200MB磁盘空间，超出后插件会被卸载。
- NDR插件最多可同时打开200个文件或网络连接。

支持的服务器类型

- 弹性云服务器（Elastic Cloud Server，ECS）。
- 裸金属服务器（Bare Metal Server，BMS）。

安全组限制

安装插件的ECS，需要放通4789端口。

支持的操作系统

网络检测与响应服务当前支持的系统版本：

表 7-1 HCE 版本

操作系统版本	X86系统版本	Arm版本
HCE 2.0（64位）	√	√

表 7-2 EulerOS 版本

操作系统版本	X86系统版本	Arm版本
EulerOS 2.0（64位）	√	×

版权所有 © 华为云计算技术有限公司

操作系统版本	X86系统版本	Arm版本
EulerOS 2.2（64位）	√	×
EulerOS 2.3（64位）	√	×
EulerOS 2.5（64位）	√	×
EulerOS 2.7（64位）	√	×
EulerOS 2.8（64位）	√	√
EulerOS 2.9（64位）	√	√
EulerOS 2.10（64位）	√	√
EulerOS 2.11（64位）	√	√
EulerOS 2.12（64位）	√	√

表 7-3 CentOS 版本

操作系统版本	X86系统版本	Arm版本
CentOS 7.x（64位）	√	√
CentOS 8.x（64位）	√	√
CentOS 9.x（64位）	√	√

表 7-4 Ubuntu 版本

操作系统版本	X86系统版本	Arm版本
Ubuntu 16.04（64位）	√	×
Ubuntu 18.04（64位）	√	×

 版权所有 © 华为云计算技术有限公司

操作系统版本	X86系统版本	Arm版本
Ubuntu 20.04（64位）	√	√
Ubuntu 22.04（64位）	√	√
Ubuntu 24.04（64位）	√	√

版权所有 © 华为云计算技术有限公司

8 与其他云服务的关系

弹性云服务器

NDR为弹性云服务器（ECS主机）提供流量检测和分析功能，全面记录攻击源和攻击目标的详细信息，帮助用户精准定位网络攻击。

裸金属服务器

NDR为裸金属服务器提供流量检测和分析功能，全面记录攻击源和攻击目标的详细信息，帮助用户精准定位网络攻击。

弹性公网 IP

NDR需要ECS主机绑定弹性公网IP后，才能进行防护和检测。

企业主机安全 HSS

NDR支持为ECS主机和裸金属服务器提供流量检测功能，需要依赖HSS服务安装Agent并开启防护。

消息通知服务 SMN

NDR开启告警通知后，当网络攻击达到告警阈值时，告警信息会通过用户设置的接收通知方式发送给用户。

云审计服务 CTS

云审计服务（Cloud Trace Service，CTS）记录了NDR相关的操作事件，方便用户日后的查询、审计和回溯。

云日志服务 LTS

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NDR日志，可以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。

 版权所有 © 华为云计算技术有限公司

9 基本概念

检测插件

安装在业务主机上，可以对主机网卡流经的南北向和东西向流量，开展全流量威胁检测。

南北向流量

指业务主机网络与外部网络（如互联网）之间流入和流出的流量，NDR会对此类流量进行威胁检测。

东西向流量

指云环境内部业务主机之间，或者跨VPC之间传输的流量，NDR会对此类流量进行威胁检测。

加密流量检测

业务之间访问、传输、存储和交换等过程，经过了加密操作，保障数据安全。NDR可以对此类加密流量进行威胁检测。

威胁入侵防御

对网络流量进行收集、分析和监控，以发现潜在的威胁、入侵、恶意活动或异常行为。

横向移动

攻击者在攻陷一个系统后，在网络内部移动以扩大控制范围。

取证分析

在安全事件发生后，收集分析证据以确定攻击路径、范围和影响。

威胁特征库

特征库是网络安全中的一个关键组成部分，用于存储和管理网络安全事件中的特征数据。 这些特征涵盖了各种网络活动、攻击行为、异常模式等，为安全团队提供了强大的工具来检测、分析和应对威胁。

版权所有 © 华为云计算技术有限公司

威胁情报库

基于证据的知识，包括上下文、机制、标示、含义和能够执行的建议，这些知识与资产所面临已有的或酝酿中的威胁或危害相关，可用于资产相关主体对威胁或危害的响应或处理决策提供信息支持。

CVE 编号

CVE (Common Vulnerabilities and Exposures，通用漏洞披露) 是安全漏洞列表，列表中的每个条目都会有一个唯一的CVE编号。

威胁检测类型

NDR可对网络流量中的多种威胁进行检测，其中包括SQL注入、webshell、暴力破解、代码执行、恶意程序、反弹shell、黑客工具、缓冲区溢出、拒绝服务、跨站脚本、目录遍历、请求伪造、恶意扫描、恶意提权、挖矿行为、未授权访问、文件包含、信息泄露、异常连接和异常协议等。

 版权所有 © 华为云计算技术有限公司