N-Reporter 7

DATASHEET

Next Generation IT Operation Platform

Integrate Network Management, Flow Analysis and Log Reporting

2025/04/16

现今网络设备、服务器与安全产品大多具备Syslog 或 Flow 流量数据的输出功能。对 IT 人员来说，Syslog Data 提供了事件详情的描述信息，而 Flow Record 则是了解网络用量的最佳帮手。

N-Partner 公司采用多项创新开发技术所生产的 N-Reporter 除了提供对Syslog/Flow 数据的收集、储存、实时分析、查询与报表制作等功能之外，其更大的特点是可以执行 Syslog 与 Flow 间的关联性分析 (Correlation)，将来自 Flow 的L3/L4 Packet/Byte 数据与来自Syslog 的L7事件内容完美结合，让IT 管理者完全掌握网络的使用细节。N-Reporter 堪称业界效能最优、功能最强大、操作最简单的 Syslog 与 Flow 报表 + 整合分析平台 (Reporter + Analyzer)。

■ 软件功能

- 不分厂牌和设备，支持各式 Syslog 资料的搜集。
- 提供系统状态查询，用户可以查询运行版号、CPU 使用率、内存使用率、Syslog / Flow 数据接收量。
- 提供 Flow 收集的能力，如 Netflow v5/v9/v10、sFlow v4/v5、JFlow 等，或以防火墙 Traffic Log 进行使用分析。
- 支持中文/英文/日文 Web(HTTP/HTTPS) 操作接口，用户权力可依使用需求调整。
- 提供 CLI (Command Line Interface)，可透过 Console 或 SSH联机进行系统操作。使用Web即可基本网络设定：IP Address、Gateway、DNS、Static Route 与 NTP Server，可以重新启动(reboot)与关机(shutdown)，并支持Setup page，可以reset password与reset系统回复出厂值。
- 支持 IPv6 环境，同时也适用于 IPv4 与 IPv6 双轨运行的环境。
- 支持 SNMP v1/v2c/v3 监控网络设备，系统可呈现出特定内网 IP 所在的 Switch 位置。
- 支持绘制设备树状图，能将设备按照从属关系排列成根目录、子目录关联顺序，并可以收合展开。当设备出现异常时上层目录夹也会同步显示异常灯号并发出告警声警示。
- 支持采用 SNMP监控设备状态，包括 CPU/Memory 使用率、接口(Interface)流量讯息、Broadcast/Error讯息、ICMP 等，并可以设定告警值及送出告警。
- 监控设备的CPU、Memory 使用量图形支持 Drill Down点击功能，Drill Down 后转跳 TOP N 报表关联 Syslog/Flow，自动排出用量排行。并且监控功能支持自定义 OID，监控所需项目状态。
- 支持绘制拓朴图，图形自动绘制并以颜色呈现接口负载。
- 可输入多笔查询条件进行逻辑运算 (or/not)，条件包括事件关键词、IP、严重等级等各项参数，输入条件数无限制。
- 提供 IP 网段名称解析对应功能，在事件及报表中呈现 IP 及网段名称。
- 提供Port名称解析对应功能，管理者可以自行定义 Port 的名称对应 (如：Port 80 等于 HTTP)。
- 内建 Flow 分析与统计功能，能自动绘制流量图 (Packet/Byte) 并产生用量 TOP N 表。
- 提供以服务/部门/分行等为单位的封包大小 (64/128/256/512 Bytes)分时图。
- 支持IP地理位置信息(国家类别)、知名服务(如 Google/Facebook/Line等) 、可疑 Domain/IP 数据库，可进行日志及流量的比对功能，提供部门组织或IP的流量关联图，并拥有自动更新数据库机制。
- 可透过Syslog协议接收日志(Log)并内建正规化(Normalization)功能，可将日志里的日期、事件名称、严重等级、IP地址、用户名称、Packet/Byte传送量等信息分别呈现在同一表格的不同字段中。
- 内建实时Flow分析与统计功能，依据流量来源和目的IP区段、主机、用户名称、应用埠号 、协议、网络接口、流量输出设备、MAC地址、国别、封包大小分布等监控参数做成TOP N排序报表或实时流量(Packet/Byte)线形图，并允许自定义阀值，超过阀值主动发出告警。
- 具备 Flow 异常流量智能分析功能，实时分析异常流量 (DDoS、Host Scan、Port Scan、Flooding、Burst Session 等)。
- 系统可下达阻挡特定 IP 指令到网络与资安设备进行联防 (注：非所有设备都支持此项功能)。
- 系统提供自动阻挡的联防机置，可自行定义自动联防的条件。

- 根据Syslog/Flow历史用量自动学习建立 Base Line，能实时分析出发生异常突增的事件或 IP，并送出告警。
- 支持报表 Drill Down 深入查阅行为。
- 内建圆饼、长条、曲线图等多种图型式样，可依需求客制化报表。
- 提供流量图形呈现 Max/Avg/PCT 95 数值。
- 可以自行订制事件呈现的字段和事件 PDF 输出的字段。
- 支持制作中文报表与输出中文 PDF 。
- 自定义 PDF 输出的 Logo和版面。
- 提供 Windows AD 解析功能，可以将事件的 IP 解析出使用者名称。
- 支持各类主机的用户登入注销的稽核日志报表：Linux、Windows Server 2003/2008/2012/2016 等。
- 提供异常登入行为侦测与告警。
- 支持各类数据库的用户登入注销的稽核日志报表：Oracle、MSSQL、MySQL 等。
- 支持 Windows 档案分享的稽核日志报表。
- 内建动态 仪表盘 能呈现实时事件内容、告警现况及事件统计等信息，并可根据需求自行定义与调整 仪表盘 内容、格框大小与画面排列方式，提供各种时间区段(一小时/一天/一周)事件统计报表、流量图与系统状态。
- 支持 Access Control List，限制可执行管理的 IP 白名单。
- 支持 Syslog 原始的 Raw data 备份。
- 完整记录用户操作历程，并提供 PDF 格式的输出。
- 提供 Open Interface，用户可透过Open Interface 取得事件信息。
- 弹性的告警通报设定，可以依不同的报表或告警种类指定不同的邮件群组。
- 提供 CPU、风扇和硬盘状态监控，主动通知管理者异常告警。
- 支持 SNMP Trap，硬件异常可以实时告警。
- 支持 SNMP Agent，可提供系统运行状况。
- 独创最新的压缩储存技术，使用符合国际公认推荐 FIPS 104-3 密码模块 並使用 SHA3-256 、SHA3-512 、 AES-CTR 與 AES-GCM 的加密原则，确保数据的完整性和不可否认性，其压缩比高达 10 倍，大幅度提升储存空间利用率。
- 系统可以与原厂保持联机，自动下载最新版本的软件。
- 支持 WMI 方式取得 Windows Server 日志。
- 支持2D/3D全球视觉的攻击动态实时呈现。
- 统计 1 千万笔 Syslog Data 的 TOP 1,000 报表仅需 48 秒；搜寻 1 亿笔 Flow 数据内的特定 IP 仅耗时250 秒。
- Syslog 接收能力最高达 10,000 EPS 以上，最高等级的 Flow 模块接收能力最高达每秒 20,000 笔Flow Records。
- 支持使用 ICMP 对监控节点做不间断的节点可用度(Availability)以及网络质量(Run Trip Time, RTT)的监控。
- 提供趋势预测(Prediction)功能，可针对纳管网络设备与服务器的 CPU/Memory/Disk 使用率，以及线路带宽/质量量测值，提供短期及长期的未来走势预测线型可视图。
- 自动关联IP所在的Switch/Interface信息，并可回溯查询历史对应纪录。
- 系统提供APP，可于行动装置查阅实时状态与障碍通知。
- 提供两层式 TOP N 报表功能，针对第一层TOP N 排序的每一结果再次设定新的统计加总条件后产出第二层 TOP N 报表。两层 TOP N 报表所设定的统计加总条件可以不同，如第一层是 IP 流量排行而第二层是事件排行。

- 内建 Top N 模块，用户可随时订制、查询 Top N 统计报表，并且可以选定时间统计区间、事件关键词、来源/目的 IP、来源/目的 Port、设备、图表型态等参数，制作出时报、日报、周报、月报、季报、半年报与年报等各种报表。
- 内建事件模块，用户可随时查询 Syslog、Flow 的事件内容明细。
- 提供数据库储存天数预测功能。
- 支持数据库备份与回复功能。
- 系统具备自动学习功能，根据 Syslog/Flow 历史用量(例如过去一小时、过去数天) 透过演算方式自动学习建立 Base Line，能实时分析出发生异常突增的事件或 IP，并以趋势图型态呈现突增发生的准确时间点，发送告警。无须人工设定阀值(Threshold)，系统自动建立合理的动态阀值。
- 内建监控报表，用户可以依据不同条件，订制自己的监控条件，当异常发生时则立即通知管理者。
- 离线报表支持群组化功能。
- 支持多样的实时输出格式：PDF、XML、CSV 等。

软硬件的完美结合

N-Partner 公司 RD 团队多年来专注于巨量数据的高效率收集、储存以及分析领域，运用自行开发的数据库优化技术：命名为 N-Partner《Smart DB》，可将数据搜寻与统计排序所需要的时间缩减至最短。经过实际环境的验证，N-Reporter 统计 1 千万笔 Syslog Data 制作成 TOP 1,000 报表仅需花费 48 秒钟；而在 1 亿笔 Flow Records 中要找寻一个或是多个特定 IP 则仅需耗时 250 秒。

除了能够拥有高速与稳定的处理效能之外，提供简易的维修程序亦是产品以 Appliance 架构问世的主要考虑。保固期间内若硬件损坏，N-Partner 公司将以整机 RMA 方式处理，免去除错时间的浪费。

同时输入多笔查询条件 进行逻辑运算与制作报表

在维运的历程中，数据查询是大部分时间里所需执行的工作。当接收的 Syslog/Flow 数据越来越多时，能够支持弹性的搜寻条件输入与快速的查询结果呈现是用户对报表工具的基本要求。

N-Reporter 提供智能型的查询功能，搭配逻辑运算概念能够让用户完成各式各样要求下的查询工作。

事件呈现字段及可输入的过滤参数选项

根据 Syslog或是Flow查询
设备 (支持单一设备或跨设备查询)
设备的接口
时间
事件关键词
使用者名称
来源/目的 IP(支持 CIDR 与不连续区段)
来源/目的 Port
来源/目的国家
事件严重等级
事件类型 (Security、Traffic、Audit、Web 等)
事件处置动作 (Block、Permit 等)
Packet/Byte 用量大小
Policy ID
AS Number

所谓的逻辑运算指的是多个查询条件间以联集 (Or) 和排除 (Not) 概念所建立的关联性结果。举例来说：在「事件关键词」的条件中采用联集 (Or) 可以查询多个关键词相关事件，或用排除 (Not) 过滤掉不想查看的事件。

N-Reporter 不仅支持「事件关键词」的逻辑运算，用户亦可针对「IP」选项进行逻辑运算。以下说明几个操作范例：

事件关键词

P2P+Streaming

表示欲同时查找含有 P2P 或是 Streaming关键词的所有事件。

P2P+Streaming! BT

表示欲同时查找含有 P2P 或是 Streaming 关键词的所有事件，但是需要排除 BT。

IP

192.168.1.0/24+192.168.2.0/24

表示欲同时查找这两个网段的所有事件。

192.168.1.0/24+192.168.2.0/24
!192.168.1.100-192.168.1.200

表示欲同时查找这两个网段的所有事件，但是过滤掉 192.168.1.100-192.168.1.200 这个区段的事件。

事件搜寻条件可以依据实际需求输入，没有上限；N-Partner《Smart DB》同样给予 N-Reporter 快速查询事件的能力，让逻辑运算机制不会因执行大量条件比对而延迟搜寻结果的呈现。

Flow 模块进行用量分析

Flow(ex：Netflow/sFlow)数据在网管工作中经常扮演用量分析的重要角色，IT 管理者藉由 Flow 数据了解哪个 IP 或是哪个组织单位用量最多；哪种 Protocol (ex：Port 80、Port 21) 占去最多的带宽资源等讯息。

N-Reporter 加装 Flow 模块后可满足上述 IT 管理者对于 Flow 分析的需求，诸如：每日用量排行、针对特定对象长期绘制流量图、查询特定 IP 或是组织单位的流量使用纪录等。

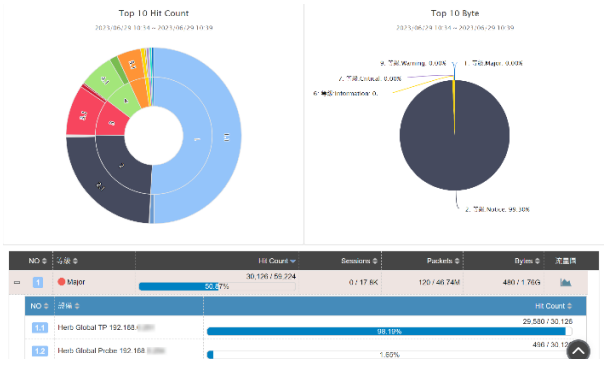
N-Reporter 的 Flow 模块除了支持路由器或交换器所送出的 Netflow/sFlow/Jflow 等格式之外，亦可在没有 Flow 设备的环境中，将防火墙送出的 Traffic Syslog 转换为 Flow 格式进行使用分析。N-Reporter 针对 Flow 数据的储存进行优化，可以大幅提升查询及报表运算效能。

Syslog 与 Flow 间的关联性整合运用

过去 IT 管理者需要分别建置 Syslog 储存系统与 Flow 分析机制作为辅助网管工作或是符合法规要求之用。但是独立运作的两套设备所提供的讯息都不是全面性的，导致 IT 管理者在执行网络维运与除错时只能往来两套系统反复查询数据后，再自行比对分析找出可能的关联性。

N-Reporter 能整合资安 Syslog 中的 L7 之用户行为数据与 Flow 的 L3/L4 流量信息，得到网络运作完整信息，让 IT管理者完全掌握管辖网络的使用细节。

例如当 IT 管理者从 Flow 的 TOP N 排行中发现某个 IP 或是单位传送了大量的封包，此时透过 N-Reporter 的关联性整合功能可以快速得知这个单位的网络使用行为是甚么内容：原来是 P2P 分享所产生巨量封包。反过来看：从第七层资安设备丢出的 Syslog 讯息中察觉到单位正遭受到 DDoS 攻击，藉由 N-Reporter 的关联性整合功能可以得到 DDoS 攻击流量图，并可以进一步追查攻击来源 IP 以进行防御，也可以得知 DDoS 对内部的影响范围。



丰富多样的实时在线报表

N-Reporter 的实时在线报表系统支持动态显示报表内容与统计图型。用户可依据喜好选择适合的图型样式，包括圆饼图、直方图、曲线图等。报表功能同样支持逻辑运算概念 (Or/Not)，使用者可根据各种实际的状况逻辑结合多个过滤参数，让报表产生的结果更贴近使用者的真实所需。例如：服务器遭受严重攻击事件日报表、员工使用社群网站与串流影音的流量周报表、数据库存取记录月统计等。

报表制作参数包括

事件关键词、来源及目的 IP、Port 、设备、图表型态等过滤条件及统计字段
工作时段(每日统计资料时段，如 8:00~18:00)
工作日(可限定只统计周一到周五)
报表型态(时报、日报、周报、半月报、月报、 季报、半年报与年报)
定期寄送时间
指定的报表收件群组
报表格式(HTML、PDF、 XML、CSV)

离线报表定期寄送

定期自动产生统计报表让用户无需每日手动执行报表制作与输出的工作。

N-Reporter 将根据用户所定义的报表制作参数，寄送统计报表到指定的电子邮件帐号。

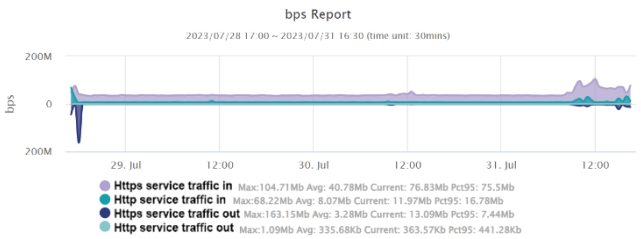
N-Reporter 针对各类主机及数据库系统，提供符合个资法需求的稽核 (Audit) 日周月报表，包含用户登入与注销、登入失败及帐密猜测等稽核日志报表。

自定义分时报表，并提供异常监控功能

管理者可使用过滤条件来定义各式的分时报表，方便长期观察事件或是流量的变化。透过关键词的设定，可观察特定事件的分时变化，例如监看「Telnet/SSH Login Fail」数量来侦测是否有帐密猜测、监看半夜联机某主机次数及流量来侦测是否异常、「Port 445」联机及流量监控来侦测是否感染蠕虫等。

分时报表同时也支持阀值(Threshold) 的设定。如此只要事件次数暴增， 或者发生流量异常时，系统将主动寄发告警邮件通知管理者。

加装 Flow 模块的分时报表，可以在同一个分时报表画面里， 同步绘制事件、bps、pps 和 session 的曲线图，方便用户进行交叉比对分析。



异常登入行为报表

分析全网的主机登入行为，一旦察觉异常登入行为立即通知管理者，提供针对主机的第二道安全防御，大幅减少黑客入侵成功率及所造成的危害。

智能稽核功能

帐号密码猜测
可疑 IP 登入成功
改变登入 IP

仪表盘：
動態即時呈現事件統計及告警現況

使用者可以依需求以最适用的方式，将系统运作现况、事件统计排行、实时趋势分析、异常告警等信息排列在专属的仪表板上，进行实时的监看。仪表盘 上所呈现的异常，也能直接以点选的方式到达该页面进一步处理，弹性的设定方式能让使用者建构出属于专属于自己环境内的资安战情中心。

Action 模块执行联合防御

N-Reporter 拥有优越的实时异常分析能力，使用者可以运用这些有用的分析结果进行更进阶的管理处置。搭配 Action 模块，可以快速锁定内网的异常 IP 发生在交换器的哪个接口上，IT 管理者就能够视影响网络的严重程度准确地执行更进一步的管制作为，让网络立即恢复正常运作。至于来自网外的攻击，则可将 IP 封锁指令下达至位于 Internet 入口处的网络或是资安设备，进行第一时间的防御。

用户也可以根据事件的关键词、定义自动阻挡的条件。系统即可主动分析定义的条件，一旦条件达到门坎值时，自动阻挡该异常的 IP 于联防的设备上。

N-Reporter 的 Action 模块搭配实时趋势分析功能是发掘并 阻挡 DDoS 攻击最有效的解决方案！

内建人工智能，根据历史纪录
自动产出趋势分析报表

N-Reporter 内建的人工智能科技能根据搜集到的 Syslog/Flow历史资料自动找出发生次数、Packet 数或 Byte 数异常突增的事件或 IP，并将发生异常突增的内容主动寄发通知邮件给 IT 管理者，以利于第一时间处置网络中的的异常状况。藉由 Behavior Based 侦测与分析

功能，用户无需猜测与预设合理的阀值，即可充分掌握网络环境里值得注意的变化，让维运工作显得更轻松容易。

N-Reporter 不仅是功能强大的事件查询与报表制作系统，更是一部能真正做到趋势分析的 Analyzer。

效能监控模块— 网络节点Ping监控

使用 ICMP 持续对监控的网络节点发出 Ping 测试，藉此了解网络节点是否正常运作并且量测与纪录其响应时间，分析网络质量良莠。根据授权数量，可以针对多个网络节点(IP)进行 Ping 量测，量测间距最短为一分钟一次，协助网络管理人员针对其选定的网络节点了解是否正常运作以及响应速度快慢(Response Time)，例如网络设备、重要的 IP Gateway、外网的IP节点等。透过自我学习功能，软件会自动发觉效能不佳的网络节点并发送告警。更大的特点是能够关联流量(Flow)以及日志(Log)数据分析出效能不佳的原因，让网管人员可以快速处理障碍、恢复网络质量。

效能监控模块— Web网站服务监控

模拟使用者开启浏览器观看网页的过程，持续对监控的 Web 网站进行浏览模拟，藉此了解 Web 网站是否正常运作并且量测与纪录浏览过程中各阶段的响应时间，分析 Web 网站服务质量良莠。根据授权数量，可以针对多个 Web 网站进行量测，量测间距最短为一分钟一次。协助网络管理人员针对其选定的 Web 网站了解从使用者端浏览这些 Web 服务是否正常以及响应速度快慢(Response Time)，包括自己架设的 Web 服务、放在云端的 Web 服务以及重要的公众 Web 服务等。整个过程的响应会记录成五个阶段：DNS、TCP Connection建立、SSL 加密通道、联机建立 Response 以及首页下载完成。透过自我学习功能，软件会自动发觉效能不佳的 Web 服务并发送告警，让网管人员可以快速处理障碍、恢复网络质量。

N-Partner 数据压缩模块

要做到全面的监控与分析，数据完整性至关重要。N-Reporter的数据压缩模块采用ZFS文件系统为基底，具备预防静态数据损毁的自我修复能力，会自动修复错误的区块，确保数据完整与正确。此外，ZFS可解决传统RAID的不稳定性，强化数据压缩能力，在N-Partner改良下，更可提升日志保存可靠度与系统运行效能。

全新 SNMP 树状拓墣设计

传统网管软件所使用的拓墣图功能在大型网络架构下相当不容易绘制，而实际使用上往往需要在好几个画面切换或是使用缩放功能才能定位到欲查阅的设备。有别于以往的星状拓墣，N-Reporter 使用全新树状结构设计，能将设备按照从属关系排列成根目录、子目录关联顺序，并可以收合展开，在一个画面中一目了然所有设备健康状态。当设备出现异常时，上层目录夹异常灯号同步显示，并发出告警声警示，协助使用者快速找出发生健康状态异常之设备。

简单易用的操作接口与管理功能

透过 Web 接口即可进行 N-Reporter 的操作与管理。此外，用户亦可以将 N-Reporter 数据库中的数据透过以下方式进行备份或是回复： FTP、NFS 、SMB。

Syslog 与 Flow 转发功能

使用者可以自行定义将接收到的 Syslog 与 Flow 资料保留原始来源IP转发至其他接收设备。

高弹性扩充机制

随着所管理设备日渐增多，当用户对于系统使用需求越来越高的时候，新一代 N-Reporter 保留超高弹性扩充机制，N-Reporter 可藉由扩充机制，将现有的 N-Reporter 变成私有云 N-Cloud 的一部份，提升储存空间及运算效能的同时，也将原始设定及数据保留，确保数据不掉失。

符合稽核规范

通过符合国际公认推荐 FIPS 104-3 密码模块，并使用 SHA3-256 、SHA3-512 、 AES-CTR 與 AES-GCM 的加密原则，确保数据的完整性和不可否认性。

https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?validation=39318

■ 硬件规格

	NP-RPT-K-CN	NP-RPT-D-CN
功能	All-in-One Appliance，内建专属 OS、数据库与应用程序	All-in-One Appliance，内建专属 OS、数据库与应用程序
尺寸	1U Rackmount, 19 Inch Standard Wide RackMount Industry Server	1U Rackmount, 19 Inch Standard Wide RackMount Industry Server
CPU	Intel Xeon E-2334 Processor (8M Cache, 3.40GHz)	Intel Xeon E-2334 Processor (8M Cache, 3.40GHz)
Memory	32G DDR4 x 2	32G DDR4 x 2
Ethernet Controller	Dual Port GbE LAN	Dual Port GbE LAN
IPMI	Integrated IPMI 2.0 and KVM with Dedicated LAN	Integrated IPMI 2.0 and KVM with Dedicated LAN
I/O Port	1 VGA, 1COM	1 VGA, 1 COM
Power Supply	350W Platinum Level	400W Platinum Level x 2
SSD	500GB	500GB
HDD	4TB, up to 12TB HDD (4x4T with RAID5)	4TB, up to 12TB HDD (4x4T with RAID5)
RAID Card	Supports RAID 0, 1, 5	Supports RAID 0, 1, 5
AC Power	100v-240v, 4.2-1.8A, 50-60Hz	100v-240v, 4.2-1.8A, 50-60Hz
Operating Temperature	0°C-50°C (32°F-122°F)	0°C-50°C (32°F-122°F)
Operating Relative Humidity	8% to 90% (Non-condensing)	8% to 90% (Non-condensing)

N-Reporter VM 建议规格

1. 请准备一台 Server，建议规格如下：

   ✓ CPU 建议 E-2334 (8M 高速缓存， 3.40 GHz) 以上。

   ✓ RAM 内存空間 80G 或以上。

   ✓ 硬盘空间可选择 500GB、1T 或 2T，请依实际需求决定。建议配置 2T 硬盘。

   ✓ 安装 VMware ESXi 6.0 或以上的版本。

   ✓ 安装 Windows Hyper-V 2016 或以上的版本。

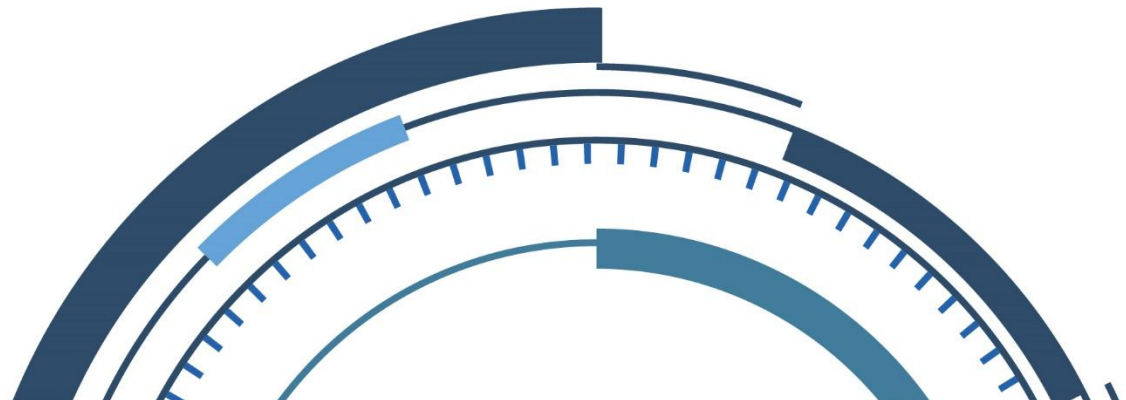
   ✓ 安装 KVM 4.2.0 或以上的版本。

2. N-Reporter 运行时，若要达到最佳效能，至少需要 CPU 3.4 GHZ, 8 Core、64G 内存空间。

3. 请准备一台 Windows 计算机，用于管理 VMware / Hyper-V / KVM Server。

产品料号

产品料号	料号说明
NP-RPT-VM-CN	Syslog collector, reporter and analyzer including 5 devices, 5 services license and 10 managed SNMP devices with 1 Year MA. VM Version
NP-RPT-K-CN	Syslog collector, reporter and analyzer including 5 devices, 5 services license and 10 managed SNMP devices with 1 Year MA
NP-RPT-D-CN	Syslog collector, reporter and analyzer including 10 devices license, 10 managed SNMP devices and dual power with 1 Year MA
NP-RPT-CN-5Dev	Add 5 devices license
NP-CN-20SNMP	Add 20 managed SNMP devices
NP-CN-50SNMP	Add 50 managed SNMP devices
NP-CN-200SNMP	Add 200 managed SNMP devices
NP-CN-500SNMP	Add 500 managed SNMP devices
NP-RPT-CN-Server-10	Server Module, 10 Services with username resolution feature
NP-RPT-CN-Server-50	Server Module, 50 Services with username resolution feature
NP-RPT-CN-Server-100	Server Module, 100 Services with username resolution feature
NP-RPT-CN-Server-200	Server Module, 200 Services with username resolution feature
NP-RPT-CN-Server-500	Server Module, 500 Services with username resolution feature
NP-RPT-CN-Flow-Lite	Flow Module Lite Version, 2000 records/per second, extra 4T HDD*1 (HDD For B/D/K model Only)
NP-RPT-CN-Flow-Plus	Flow Module Plus Version, 4000 records/per second, extra 4T HDD*1 (HDD For B/D/K model Only)
NP-RPT-CN-Flow-Adv	Flow Module Advance Version, 6000 records/per second, extra 4T HDD*2 (HDD For B/D/K model Only)
NP-RPT-CN-Flow-Pre	Flow Module Premium Version, 10,000 records/per second, extra 4T HDD*2 (HDD For B/D/K model Only)
NP-RPT-CN-Flow-Unl	Flow Module Unlimited Version, extra 4T HDD*2 (HDD For B/D/K model Only)
NP-CN-PM-100Ping	PM Module. Ping up to 100 nodes (IP Address)
NP-CN-PM-250Ping	PM Module. Ping up to 250 nodes (IP Address)
NP-CN-PM-1000Ping	PM Module. Ping up to 1000 nodes (IP Address)
NP-CN-PM-2500Ping	PM Module. Ping up to 2500 nodes (IP Address)
NP-CN-PM-20Web	PM Module. Do browse web site testing regularly. Support up to 20 web sites
NP-CN-PM-100Web	PM Module. Do browse web site testing regularly. Support up to 100 web sites

NP-RPT-CN-RAID-SM	RAID SofCNare Module and 4T HDD kit*1
NP-RPT-CN-HDD-4T-Kit	4T HDD*1
NP-CN-Ticket-G	Ticket System Module. Gold Version with 1 Year MA
NP-CN-Ticket-P	Ticket System Module. Premium Version with 1 Year MA
NP-CN-PS-I	One-Day Professional Service
NP-CN-PS-T	4 Hours Training coupon
NP-CN-PS-U	N-Reporter/N-Cloud Hardware Upgrade

Tel：+886-4-23752865　Fax：+886-4-23757458
业务咨询：sales@npartner.com
技术咨询：support@npartner.com