N-Cloud 7

DATASHEET

Next Generation IT Operation Platform

Integrate Network Management, Flow Analysis and Log Reporting

2025/04/09

N-Cloud 是一个全新的Syslog 分析管理平台中心，可应用于政府行政单位、大型企业、跨国企业、教育市网中心、 电信加值云端服务单位等机构。针对有 Syslog 管理需求者，N-Cloud 提供了统一的服务平台，管理者可轻松对企业内 所有 Syslog 进行有效保存与分析应用，落实 Syslog 资料管理，并且透过快速整合 判断，协助强化网路安全问题，同时满足 行业需求和相关法规。

N-Cloud 同时引入阶层式的分权管理概念，可以分别为企业内的每个分公司 或部门建立单位群组，群组内的成员仅 能看到所管辖的资料，因此，每个单位群组，就像拥有独立的Syslog 管理平台；而总公司的管理人员则以全局角度(Global)查 看全公司的 Syslog，随时掌握全网的安全状况。

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 数据接受量。
- 提供 Flow 收集的能力，如 Netflow v5/v9/v10、sFlow、 Jflow、IPFIX 等。
- 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。提供基本网络设定：IP Address、Gateway、DNS、Static Route ，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。
- 支援采用SNMP 监控设备状态，包括 CPU/ Memory 使用率、接口流量讯息、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 TopN 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/MIB，监控所需项目状态。
- 支持绘制拓扑图，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 名称解析功能，管理者可以自行定义 Port 的名称对应 (如：Port 80 等于 Http)。
- 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，提供部门或组织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 与 MAC 指令到网络与资安设备如防火墙与交换器，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。
- 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，中文 PDF 的输出。
- 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。
- 完整的记录用户操作审计，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。
- 独创最新压缩的储存技术，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 排序的每一结果可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。
- 阶层式管理，各自独立运作，各自拥有独立的 Reporting 分析功能。
- 支持高可用度 (HA) 架构，确保系统运作不中断。

阶层分权管理机制

N-Cloud 的阶层式管理，满足了企业分权管理的需求。例如，可以将管理阶层群组定义如下：总公司、分公司、分公司的部门等 (如图1 所示)。台中分公司所管辖的设备，其他分公司的管理者是无权查看的，但总公司的管理者，则拥有查阅分公司设备讯息的权限。

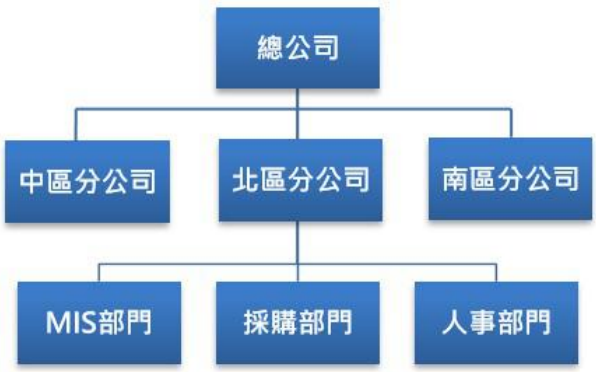


图 1

N-Cloud 的阶层式管理提供了灵活的阶层管理架构，可满足大型企业管理需求。

各种资料的集中管理中心

N-Cloud 支持横跨网络 (Router、Switch)、资安 (Firewall、 IDP/IPS、Web Cache Appliance、WAF、UTM)、 服务器、数据库、大型主机等设备的 Syslog 数据收集。N-Cloud 可搜集分析不同厂牌或设备的 Syslog 及不同格式的流量信息，如 Netflow、jFlow、sFlow 等。系统会将所有的数据做关联分析，供管理者平行比对，轻松查看全网的资安危机分析、Top N 排行、稽核报表、流量管理、历史趋势分析、实时阻挡异常攻击等信息。

支持高可用度 (HA) 架构

搭配 N-Cloud 专属的 N-LB (Load Balancer) ，可达成多部 N-Center/N-Receiver 互为备援 (如图 2所示)，提供 24 小时不中断的数据收取保证， N-Cloud 没有限制接收 Syslog 与 Flow 的来源设备数量，也无限制接收日志/流量的笔数限制，可接收之日志EPS 数至少达10,000 EPS(Event per Second)，为企业提供符合个资法规的最佳工具。

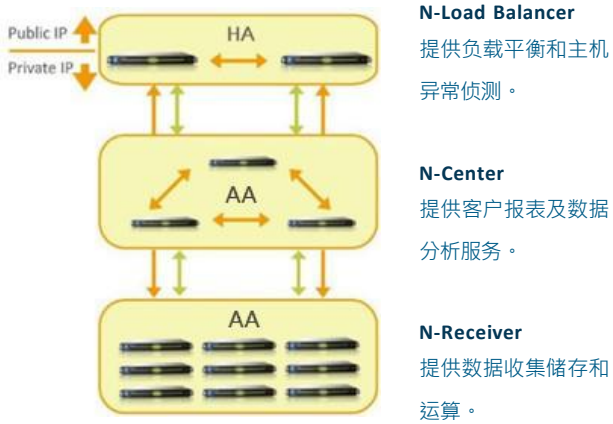


图 2

灵活弹性的 N-Cloud 架构

N-Cloud 在建构时有三个主要组件：

(一) N-Load Balancer：

负责负载平衡及主机状态侦测。

(二) N-Center：

负责处理用户的查询工作及资料交叉分析。

(三) N-Receiver：

负责保存及分析运算Log数据。

此架构具备高度扩展性，可以依据使用者需求，因应未来数据量与用户个数的成长预估，进行适当的调配，不用担心当收容的数据大幅增加时， 会发生无法扩充的问题。

建置中大型的 N-Cloud 服务平台，即可提供数百个使用者同时上线及查询，并允许建立上千个领域。依教育市网中心为例，市网中心建置一 N-Cloud 服务平台，即可同时提供数百所中学使用N-Cloud 服务，而不需要亲自至各所学校进行 Log 服务建置的动作。由于所有中学都使用相同的服务平台，因此在问题的交流与沟通上，亦彰显得简单和清楚。

可依客户需求规划

- 支持多人在线使用者，可达百人以上
- 支持 Log 使用单位群组，可达上千个单位
- Syslog 接收能力高达 100,000EPS 以上
- Flow 接收能力高达 100,000EPS 以上
- 接收 Syslog/Flow 的来源设备数无限制
- 可依需求，规划储存数据的笔数和数据保存时间
- 可自 N-Reporter 6 升级架构为 N-Cloud 6

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，数据查询是占系统大部份的运行时间。当接收的 Syslog/Flow Data 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-Cloud 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。

事件呈现及可输入的参数选项

- 根据 Syslog 查询或是根据 Flow 查询
- 设备
- 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
- Packet/Byte 大小
- 事件严重等级
- 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：若要查询多个事件关键词，可以在输入关键词之间用联集(Or) ；若是希望排除某些特定的关键词不要呈现于报表之中，则使用排除 (Not) 指令。

N-Cloud 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，或是同时进行跨不同选项间的逻辑运算。以下说明几个操作范例。

Event Keyword

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!192.168.1.100-200

表示欲同时查找这两个网段的所有事件，但是过滤掉 192.168.1.100-200 这个区段的事件。

事件搜寻条件可以依据实际需求输入多笔条件，N-Partner《Smart DB》同样给予 N-Cloud 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 模块进行使用分析

Flow (如：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。

Flow 模块可满足上述 IT 管理者对于 Flow 分析的需求，诸如： 用量 Top N 分析与 Drill Down 进阶查询；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。

Flow 模块除了支持 Netflow v5/v9；sFlow v4/v5；J-Flow 等格式之外，亦可扩充运用于没有 Flow 设备但有防火墙建置的环境中。由于大多数的防火墙都支持 Syslog功能，可将流经的网络联机讯息封装成 Syslog Data 后输出，因此企业也可以利用防火墙的 Syslog 信息进行流量的分析。

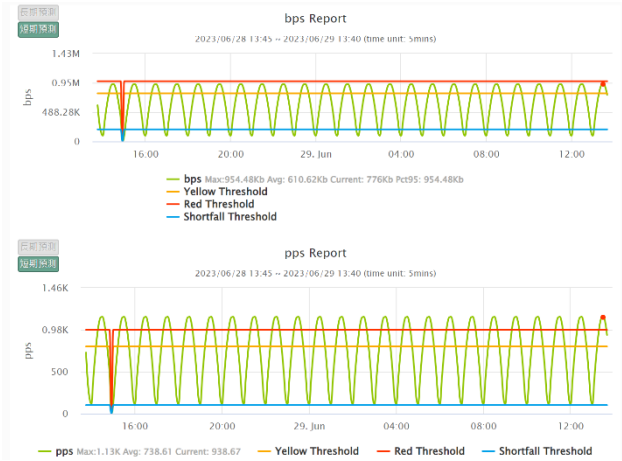
丰富多样的实时在线报表

N-Cloud 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。

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。



离线报表定期寄送

依据排程(Schedule)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-Cloud 将根据报表储存功能中用户所定义的报表制作参数，自动寄送统计报表到指定的电子邮件帐号。

报表制作参数包括

- 事件等级
- 工作时段 (每日工时区间)
- 工作日 (星期日至星期六的选项)
- 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
- 指定的报表收件者
- 报表格式 (HTML、PDF、 XML、CSV)

支持SNMP监控设备

透过 SNMP 监控，可以定期取得设备的 CPU 、Memory 和接口流量信息，并且提供清晰图标供管理者查看。此外，也可以让管理者自行设定监控的阀值。例如在 CPU / Memory 上升至 80% 或接口流量超大时，触发告警且透过邮件通知管理者。

使用树形图，依阶层式的方式，呈现 SNMP 设备管理的状况。并且提供图示，让管理者清楚知道设备目前的情况。例如：设备异常，会有红火警示，上层同时也会有惊叹号图示且将发出告警声告诉管理者，在管理的区域下有设备异常。

内建人工智能，根据历史纪录自动产出趋势分析报表

N-Cloud 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，

使用者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，让维运工作显得轻松容易。N-Cloud 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。

Action 模块执行联合防御

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作为。透过 Action 模块，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 (通常是阻挡这个 IP 继续连网)，让网络立即恢复正常运作。

N-Cloud Action 模块，能允许用户直接在 Web 管理接口上下达 IP 封锁指令，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 (注：非所有厂牌均支持)，进行第一时间的防御。

符合稽核规范

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 和 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

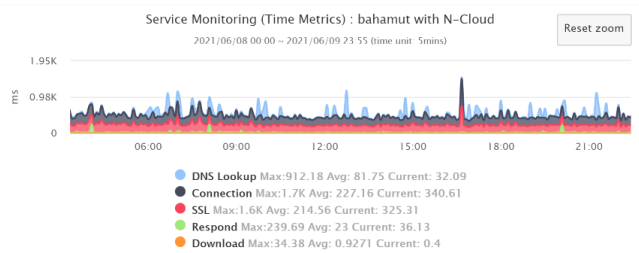
N-Probe/External Receiver 加值模块

除了 NetFlow 数据产出与 DNS 内容解析功能，N-Partner 旗下产品– N-Probe 亦提供以下加值功能，用户可依实际需求选购。

若用户的网络架构分散在不同地理位置的机房或是分支机构，各地透过 Internet/VPN 彼此连接，最佳操作建议是将 N-Probe 布署到各地并启动 External Receiver 模块功能，在本地采集SNMP/Flow/Syslog(含TCP与UDP协议Syslog)数据后加密压缩转发至N-Reporter/N-Cloud系统，同时保留原始来源IP，其压缩率达5倍，大幅降低Internet/VPN的带宽负载同时也强化了传输期间数据完整与安全性。External Receiver支持断线续传(Store and Forward)的功能，当连接的Internet/VPN线路发生中断障碍时，External Receiver会将SNMP/Flow/Syslog数据暂存，待联机恢复后完整重新转发至N-Reporter/N-Cloud系统。

External Receiver 可建置成 HA(Master/Slave)架构，提升可用度。再者，External Receiver 模块包含 SNMP 监控功能，负责本地端设备的 SNMP Polling 工作并取得 IP/MAC 及 MAC/Port 对应表，以协助网络管理。

N-Probe 亦提供效能监控(Performance Monitor, PM)模块，功能一是以 ICMP Ping 封包监测各量测点的网络等待时间(Round Trip Time, RTT)；功能二是仿真人们浏览网页服务(Web Service)的过程，N-Probe 会分别记录过程中几个阶段的响应时间(Response Time)：DNS 查询及响应、与 Web 服务器建立联机、SSL 传输、网页响应与内容下载，并将上述数据绘制成可视化分时图。为了可以更贴近使用者每个时刻的使用感受，信息管理人员可以将含 PM 模块的 N-Probe 布署在任何网络位置，例如办公室 OA 区、分公司里、外部电信承租的 IDC 机房里等等，让 N-Probe 从不同地点量测，N-Probe 会将收集到的延迟数据送到 N-Reporter/N-Cloud 智能维运平台绘制图形，供用户查看每个被监控点的网络质量，达成多点、多角度的持续性监控与分析。此外，搭配 N-Reporter/N-Cloud 的趋势预测功能，还能预测未来数小时到数个月的成长走势，在延迟变得严重之前收到预警，早一步处理。



1. DNS Query and Response
2. TCP Connection
3. SSL
4. Respond
5. First Page Download

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。

■ 硬件规格

	NP-CLD-BALANCER-CN	NP-CLD-RECEIVER-CN	NP-CLD-RECEIVER-H-CN	NP-CLD-CENTER-CN
CPU	Intel Xeon E-2334 Processor (8M Cache, 3.40GHz)	Intel Xeon E-2334 Processor (8M Cache, 3.40GHz)	Intel Xeon E-2334 Processor (8M Cache, 3.40GHz)	Intel Xeon E-2334 Processor (8M Cache, 3.40GHz)
Memory	32G DDR4 x 1	32G DDR4 x 2	32G DDR4 x 2	32G DDR4 x 2
Ethernet Controller	Dual Port GbE LAN	Dual Port GbE LAN	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	Integrated IPMI 2.0 and KVM with Dedicated LAN	Integrated IPMI 2.0 and KVM with Dedicated LAN
I/O Port	1 VGA, 1 COM	1 VGA, 1 COM	1 VGA, 1 COM	1 VGA, 1 COM
Power Supply	350W Platinum Level	350W Platinum Level	600W Platinum Level	350W Platinum Level
SSD	500GB	500GB	500GB	500GB
HDD	N/A	12TB (4x4T with RAID 5)	4x14T with RAID 5, up to 8x14T with RAID 6	8TB (3x4T with RAID 5)
RAID	N/A	Supports RAID 0, 1, 5, 6, 10, 50, and 60	Supports RAID 0, 1, 5, 6, 10, 50, and 60	Supports RAID 0, 1, 5, 6, 10, 50, and 60
AC Power	100v-240v, 4.2-1.8A, 50-60Hz	100v-240v, 4.2-1.8A, 50-60Hz	100v-240v, 7.5A, 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)	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)	10% to 85% (Non-condensing)	8% to 90% (Non-condensing)
尺寸	1U Rackmount, 19 Inch Standard Wide RackMount Industry Server	1U Rackmount, 19 Inch Standard Wide RackMount Industry Server	2U Rackmount, 19 Inch Standard Wide RackMount Industry Server	1U Rackmount, 19 Inch Standard Wide RackMount Industry Server
功能	内建专属 OS 与应用程序。提供连接、转送之负载平衡及 HA 功能。	内建专属 OS 与应用程序。提供收集数据之存储、查询、运算等功能。	内建专属 OS 与应用程序。提供收集数据之存储、查询、运算等功能。	内建专属 OS、数据库与应用程序。提供 N-Cloud 管理、网页操作接口、各项数据处理及告警等功能。

VM 需求规格

	NP-CLD-BALANCER-VM-CN	NP-CLD-RECEIVER-VM-CN	NP-CLD-CENTER-VM-CN	NP-CLD-E-REC-VM-CN
CPU	E-2334 (8M Cache, 3.40GHz, 8 core)	E-2334 (8M Cache, 3.40GHz, 8 core)	E-2334 (8M Cache, 3.40GHz, 8 core)	E-2334 (8M Cache, 3.40GHz, 8 core)
Memory	32GB	64GB	64GB	32GB
HDD	128GB(System)	128GB(System)+ 500GB/1TB/2TB(Data)	128GB(System)+ 500GB/1TB/2TB(Data)	128GB(System)+ 500GB(Data)

VM 注意事项

1. VM 需求规格为最低运行需求，请依实际需求选择硬件规格。
2. 请准备一台 Server，安装 VMware ESXi 6.0 或以上的版本。
3. N-Cloud 运行时，若要达到最佳效能，需 8 Core 以上 CPU，N-Center 和 N-Receiver 虚拟机至少需要 64G 以上 的 RAM 内存空间，N-LB 虚拟机至少需要 32G 以上的 RAM 内存空间。
4. External Receiver 运行时，若要达到最佳效能，至少需要 32G RAM 内存空间。
5. 请准备一台 Windows 计算机，安装 VMware vSphere Client 或 VMware Web Client，用于管理 VMware Server。
6. 若环境中有 N-Probe/External Receiver，请准备 N-Reporter/N-Cloud 系统接收送来的 Flow 与 Syslog 流量。
7. N-Center VM 与 N-Receiver VM 提供 500G、1T、2T 版本供使用者选择；External Receiver VM 仅提供 500G 版本。

■ 产品料号

产品料号	料号说明
NP-CLD-BALANCER-VM-CN	N-Balancer VM version. Do load balancing for N-Receiver and N-Center. Include 1 year MA
NP-CLD-RECEIVER-VM-CN	N-Receiver VM version. Data receiver. Include 1 year MA
NP-CLD-CENTER-VM-CN	N-Center VM version. Provide portal, reporting and analysis result. Include 20 domains license (max up to 120 domains). Include 100 SNMP devices (max up to 1000) and 1 year MA
NP-CLD-BALANCER-CN	N-Balancer platform. Support up to 150,000 EPS. Do load balancing for N-Receiver and N-Center. Include 1 year MA
NP-CLD-RECEIVER-CN	N-Receiver platform. Data receiver. Support up to 10,000 EPS. 4T HDD*4. Include 1 year MA
NP-CLD-RECEIVER-H-CN	2U N-Receiver platform. Data receiver. Support up to 20,000 EPS. 14T HDD*4. Include 1 year MA
NP-CLD-CENTER-CN	N-Center platform. Provide portal, reporting and analysis result. Include 20 domains license (max up to 120 domains). Include 100 SNMP devices (max up to 1000) and 1 year MA
NP-CLD-E-REC-CN	External-Receiver platform. Collect and forward data. Include 1 year MA
NP-CLD-E-REC-VM-CN	External-Receiver VM version. Collect and forward data. Include 1 year MA
NP-CLD-CN-10Domains	Add 10 domains license for N-Center platform
NP-CLD-CN-100Domains	Add 100 domains license for N-Center platform
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-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-T	4 Hours Training coupon
NP-CN-PS-I	One-Day Professional Service
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