N-Reporter/N-Cloud
Release Note 7.0.04X

(支援7.0.04X之后的所有版本)

2026/05/28

目录

■ 更新重大项目

项目名称	项 目 描述
[Kernel版本] 建议版本搭配	为确保产品使用正常，请采用 7.0.04X 版本 Firmware (下载)，搭配最新的 Kernel 版本(下载)。 ※建议使用 N-Partner Kernel 20260514091823 或更新的版本，以确保功能正常运作。
[N-Robot] UI UX 优化与 AI 功能	此次改版以用户互动为核心，重新设计了视觉层级、操作流程与互动回馈，让系统更易于理解与操作。 ※搭配N-AI模组，N-Robot提供自然语言问答、智慧报表关键洞察，以及多变环境下推荐最佳配置等功能。
[SLA] 功能新增与优化	SLA 新增了设备监控统计表与「PM Port (RTT)」功能，强化网络效能监控，协助即时发现异常，提升服务稳定性与可用性。优化的内容包括改用仪表图显示用量状态，并在报表生成上采用非同步处理，提升使用者体验
[Dashboard] 功能新增与优化	Dashboard新增动画效果，并支持多种SLA监控、程序监控，并优化了关联页面的跳查功能。自定义总览报表提供让用户导入Dashboard元件，提高了设定自由度与使用体验。

■ 新增功能及修正列表

项 目 名 称	项 目 描 述
[License] PM、ICMP、SNMP 资源类型，授权机制优化	使用者在导入 License 时，会判断目前 License 支持哪些功能模组，以及各模组可使用的授权数量；若设备实际使用的资源，超过 License 允许的数量，或该 License 未授权支持该模组，系统会自动停用（关闭）该设备上使用该资源的功能。
[UI] 伺服器稽核 Global 新增领域选项	1. 稽核报表 / 伺服器稽核的 Global 领域新增领域选项。 2. 稽核报表 / 伺服器稽核 / 主机登入稽核的 Global 领域新增领域选项。
[数据库备份] 支持SFTP	后台 「系统管理 / 数据库管理」数据库备份与数据库回复，新增 SFTP 方式做备份还原。
[FTP] 备份功能优化	备份失败时，Log 会显示是哪一份档案出问题。
[告警转 Syslog] 内容新增设备 IP	设备告警转 Syslog 新增设备 IP (dev_ip) 至 Ext11 字段。
[UI] 接口优化: 设备管理 > 批次设定	将设定项目从过滤条件移出，放置于工具列的第一位置，便于使用者操作且辨识目前的设定项目。
[UI] 加入 N-Probe 操作历程	在 N-Cloud / N-Reporter 上可看到 N-Probe 的操作纪录。
[Parser] User Defined Parser 的 keyword 处理优化	「设备管理 / 自定义资料格式」 修正 Tag Value Pair 类型：测试样本标签中，有重复字串或包含逗号时，优化显示与正规化结果。
[UI] User Defined Parser 导出导入	新增「设备管理 / 自定义资料格式」导入与导出功能。
[Action] 字段新增	「报表 / 智慧联防 / 自动执行脚本」联防参数新增 audit_user 供脚本使用。
[UI] 设备告警绘图显示告警时间线	设备告警图标示出告警发生的时间轴，方便进行对照和检视。
[UI] SMTP 设定操作优化	1. 未设定SMTP Server 时加上提醒。 2. 领域管理新增领域视窗调整。

[PM] Web 监控资讯优化	Web 监控目标为 FQDN 时，要记录当下 Polling IP，在浏览与通报信件中显示 IP 资讯。
[PM] Port Polling 新增 RTT 资讯	[效能监控]新增 Port 监控提供 Round Trip Time 资讯。
[PM] ICMP 群组调整及路径图	1. ICMP 监控的群组功能调整。 2. ICMP 监控列表拆分为独立监控和群组监控。 3. ICMP 群组浏览提供 MTR 图形和以监控设备为单位的流量图。 4. 停用 Web 监控和 Port 监控的群组相关功能。
[PM] Web 效能监控设定调整	优化 Web 监控「阈值」与「敏感度」的操作方式与说明。
[PM] PM 群组改为标签功能	加入效能监控标签功能。
[PM] 支持IPv6	效能监控新增支持IPV6目标监控。
[情资] 情资比对新增进阶比对功能	情资比对新增进阶比对功能，情资类型可以多选, 信赖评分可以选择分数区间。
[设备档备份] TFTP 支持 VR 选项	Extreme EXOS设备设定档备份支持带入VR (Virtual Routing) 。
[DPI] 事件、TopN、Filter	事件、TopN、Filter TopN 支持 Flow 输出 Deep Packet Inspection (DPI) 资讯。
[DPI] 新增类别资讯	事件、TopN、Filter TopN、IP 轨迹查询条件，支持Flow 输出 Deep Packet Inspection (DPI) 的类别资讯。
[设备] 单机设备 Raw Data 下载机制优化	N-Reporter 设备下载 Raw Data 改成与 N-Cloud 一致：1. 可直接下载，不需先另存档案。 2. 设备需要先勾选 Raw Data 保留。
[名称解析流量异常告警] 各领域事件数量总览	Global的名称解析流量异常告警加上领域告警数统计及快捷点选查询。 ※Global 专属功能
[报表] 输出(CSV)显示国家名称	事件及TopN输出(CSV)，来源及目的区域字段值呈现变更为国家代号(国家名称)。

[Kernel] Upgrade 流程优化	1. 新增强制结束更新按钮。 2. 更新后若需要重开机会有推播警告。 ex: 5 分钟后将重启，1 分钟内将重启，30 秒内将重启。 3. 重启时，前后台 UI 画面会显示重启画面。
[登入] 多因子认证	增加登入 E-mail 双重验证功能。
[云端日志] 讯息优化	系统授权(License)不足时，纪录至后台云端系统日志。
[云端日志] 分时转发逾时	[后台] [云端系统日志] 新增分时监控 Syslog 条件转发逾时纪录。
[云端日志] SNMP Polling 逾时	若当日 SNMP 监控有逾时的情形，系统将记录至后台「云端系统日志」。
[UI] 列表功能位置优化	列表绘图浏览功能字段移置操作字段右侧。
[UI] VMI 测试功能	「设备管理 / 设备资产树状图」页面，新增或编辑设备时，监控与告警 > 监控与连线测试，可对 WMI 设备进行 "设备连线测试"。
[UI] 批次设定过滤条件优化	「设备管理 / 批次设定」页面，过滤条件菜单加上 "附加条件": "暂停接收"、"设备维护中"、"设备共享"、"联防设备" 等项目。
[UI] 凭证功能优化	「系统管理 / 网络参数设定 / 凭证管理」新增「产生 CSR 」功能。除了必填的主旨资讯如网址/网域外，用户还可以选择填写组织、国家等资讯。生成的 CSR 档案可用于申请正式凭证。
[ATD] 指定flow设备计算ATD资料	可指定对特定设备或所有设备，进行 FLOW ATD 异常流量分析统计。
[操作历程] 资讯呈现优化	后台操作历程可以区分 N-Probe 指令的来源：是从 N-Cloud 更新，还是从 N-Probe 更新。
[黑名单] 新增FQDN派送	1.事件查询支持FQDN (来源/目的主机,EXT8 ,EXT9) 加入黑名单。 2.自动执行脚本支持FQDN(来源/目的主机,EXT8 ,EXT9) 加入黑名单。
[设备资产树状图] 新增告警通报设定 (缺省)	设备资产树状图可设定该领域的告警通报设定(缺省)之通报原则，其设定结果与「系统管理 / 通报设定」页面 >「告警通报设定」页

	签 >「设备异常告警」 类别的「缺省」共通。
[设备资产树状图] 设备状态树图示优化	硬体状态包含 Syslog (/Flow) no data 的告警，无资料时也会在树状图设备后出现告警图示。
[Offline center]效能优化	平均分配报表总数到不同 Center 寄信，降低总执行时间。
[TopN 报表] 批次修改资料格式	对已储存的 TopN 报表，可批次修改资料格式：HTML, PDF, CSV, XML。
[TopN] 已储存报表点击动作优化	TopN 已储存报表页面，点击报表名称会带入条件并执行查询动作；勾选报表后点击编辑则进入纯编辑模式，不启动查询。
[情资数据库] 新增来源	新增「缺省情资数据库」的情资来源 - MISP 纳入 AbuseIPDB。
[SNMP] 网络拓朴 (Topology) Auto Discovery 支持可选监控设备	新增「监控设备」选项，能指定 N-Probe 做为网络拓朴的探索设备。基于效能考量，同一领域下同时只能由一拓朴执行 Auto-Discovery。
[UI] 密码重置流程优化	密码重置流程更新：密码重置信件中的连结将于密码成功重置后立即失效，以提升帐户安全性。
[UI] 领域模拟权限控管	「系统管理 / 领域模拟」页面权限为唯读的帐号，在「领域模拟」列表时，仅列出唯读权限的帐号。
[UI] 上传功能优化	系统上传档案可能因档案过大或用户的网络环境和速度问题导致超时。超时会显示警告，建议使用者检查网络，改用 FTP 或其他方式上传。
[IP 名称解析] 功能优化	异常流量告警阈值设定：新增功能 "不启用" 与 调整功能 "手动设定 " 可以部份启用。
[SNMP] 设备告警功能优化	「系统管理 / 通报设定」的「告警通报设定」页签，设备异常告警类别在设定通报群组时，可分别设定红色与黄色告警通报群组。
[黑名单] 记录当下黑名单资讯	系统在 Syslog 与 Flow 中即时记录黑名单资讯，提升可追溯性。事件/Top N/分时监控等功能页面与相关报表，于「来源IP」或「目的IP」字段标示黑名单资讯。
[偏好设定] 设备设定档显示优化	「系统管理 / 偏好设定」功能页面，「设备管理 / 设备设定档备份」自动备份功能，添加支持型号的提示。

[告警模板] 自订 OID 模板功能优化	「设备管理 / 告警模板」页面，「自订 OID 模板」页签中加入 SNMP 测试后的测试结果下载功能。
[ATD] ATD效能优化	53 port 和 123 port 不列入 UDP Port Scan 计算。
[ATD] 黑名单/阻挡功能	ATD 异常流量即时分析列表，针对 IP 可以右键加入 IP 阻挡或黑名单功能。
[UI]后台使用者总表操作优化	撷取过滤条件中的领域，自动带入新增使用者的领域选取中。
[档案签章] 功能页面异动	将前台的档案签章相关功能移至后台「数据库管理」功能页面，方便使用管理。
[Receiver] Extend field 显示优化	Extend field 内容长度256以上时，超过部分以「...」取代，并显示提示资讯。
[接收量] Syslog/Flow 记录丢弃量	1. 前台「领域资讯」与后台「领域管理」页面新增切换功能，可查看 Syslog 与 Flow 接收量超过 EPS 的次数及最大丢弃量。 2. 后台「系统管理」的 N-Probe 设备页面新增切换功能，可查看该设备接收资料时超过 EPS 的次数及最大丢弃量。
[UI] 跳查 TopN 功能优化	分时监控 TopN 报表跳查 TopN 时，提供对映的排序依据组合。
[联防记录]功能优化	联防记录的查询条件加上自动执行脚本选项。
[SNMP] 流量图资讯优化	SNMP 相关流量图(CPU, Memory, Interface, Disk, User defined OID)，查询三天以上显示最大值和最小值。
[Auto Action] 模板参数扩充	「报表 / 智慧联防 / 自动执行脚本」页面，指令模板新增参数：来源(/目的)名称解析、来源(/目的)Port解析。
[Auto Action] 新增低量告警执行动作	「报表 / 智慧联防 / 自动执行脚本」判定条件为分时监控报表时，可设定低量告警执行指令。
[Auto Action] 脚本参数扩充	指令样板支持信赖评分、情资类型参数。
[黑名单] 支持 URL 方式导入	新增黑名单的 URL 设定功能。

[网络拓朴] 列表增加备注字段	网络拓朴列表加入备注字段。
[网络拓朴] 编辑模式时增加格线功能	拓朴图编辑模式显示格线，方便设备定位。
[System] Receiver 低量/无资料告警	自动监控N-Receiver的Syslog数据包或是Flow Record量。 - 若持续10分钟以上无资料，触发一次无资料告警。当资料量回复时，才重新启动此监控。 - 相较于过去资料量处于低量，且持续10分钟以上，则触发一次低量告警，若已属于无资料告警，则不触发。当资料量回复正常时，才重新启动此监控。
[事件查询] 查询条件扩充	事件查询 Syslog 查询条件新增 TCP Flags。
[通报设定] 邮件主旨设定优化	告警通报设定的邮件主旨可多选，并可调整前后顺序。
[偏好设定] 登入启用 E-Mail 验证优化	启用 E-mail 验证前会先检查：1. 已设定 SMTP Server，且前后台 Server 设定一致；2. E-mail 信箱可收取验证码。
[SNMP] 搜寻设备时可选监控设备	「设备管理 / 设备资产树状图」页面，批次新增设备可以选择 N-Probe 作为监控设备进行扫描。
[离线报表寄送记录] 功能优化	状态文字修改、通报群组连动对应的领域，以提升用户体验。
[操作历程] 新增「操作行为报表」	前台「系统管理 / 操作历程」操作行为报表提供： 1. 页面使用排行图：统计(全部/单一帐号)页面使用次数排行 2. 帐号使用时间图：统计(全部/单一帐号)每个小时存取系统资料的次数 ※Global 专属功能。
[设备树状图] 搜寻功能变更	透过关键字搜寻设备名称与 IP 时： 1. 左侧树状图只有领域(或资料夹) 符合关键字，右侧设备列表会列全部设备。 2. 左侧树状图领域(或资料夹)与设备都符合关键字，右侧设备列表仅保留有符合关键字的设备。

[设备树状图] 告警图示美化	告警图示美化： 1. 设备(/效能)异常告警更好辨识。 2. 领域(与资料夹)底下若有告警，将告警总数标示于对应的图示后面。
[设备细项设定] 新增接口过滤条件	用户 IP 对应 MAC 功能页签，过滤条件添加接口名称。
[UI] - 过滤禁用符号	限制用户输入禁用符号，避免影响字串的解析，导致系统出错。
[离线报表寄送记录] 手动寄送报表	后台「离线报表寄送记录」提供手动寄送离线报表。
[UX][列表页] 过滤条件优化	当滑鼠游标移动到功能列上的「过滤条件」按钮时，透过 Tooltip 显示目前设定的过滤条件。
[IP 名称解析] 内建网段重复时警语	新增或编辑「IP 名称解析」时，若与系统内建已知网段重复时，给予错误讯息:「此网段定义与系统内建规则重复」。
[系统管理] 系统效能分析功能优化	后台「系统管理」页面的「系统效能分析」功能，可即时进行主机系统分析，或「下载分析档案」后，将档案交付给 N-Partner 服务团队，进行离线研读分析。
[告警模板] User Defined OID 模板新增编辑规则变更	「设备管理 / 告警模板」页面，User Defined OID 模板需要先通过 SNMP 测试，得到结果为数值才能储存该模板。
[情资] 功能优化	「情资数据库」 功能调整与新增如下： 1. 在「事件 / 事件查询」页面新增「情资来源」字段。 2. 在「事件 / 事件查询」结果列表中，将查询时的比对更改为系统接收时符合情资数据库的「情资来源」、「情资类型」和「信赖评分」内容。。 3. 在「系统管理 / 偏好设定」页面，「事件字段」新增「情资来源」可选字段。
[Purge] 设备资料机制修改	在领域选取的资料接收设备的预估可用量尚未计算完成前，此领域的设备无法设定正规化资料保留天数。
[设备] 设备/PM 通知类灯号美化	设备与 PM 的通知类灯号变更为铃铛图示。

[UI] Dashboard - CPU core table	新增元件:「其他」 > 「SNMP - 设备监控 > CPU」。
[UI]Dashboard 显示优化	已移除或停用报表会于 Dashboard 浏览画面上显示提示。
[UI] SLA 功能可以在Dashboard 显示	Dashboard增加支持：1. SLA - 统计表（表格）、2. SLA - SNMP（表格、曲线图）、3. SLA - Flow（曲线图）、4. SLA - ATD（表格）。
[Dashboard] 动态设计	新增 Dashboard 动画。
[Dashboard] 新增「动画开关」设定	「系统管理 / 偏好设定 / 报表」新增 Dashboard 页签，新增 Dashboard 动画效果开关。
[Dashboard] 新增程序告警监控	Dashboard 增加支持程序监控（曲线图/面积图）。
[Dashboard] 加入PM监控 - Web、ICMP	告警状态元件新增资料来源：效能告警监控。
[Dashboard] 设备数量显示元件跳查功能	Dashboard 的「设备健康度」跳转至「设备管理 / 设备资产树状图」时自动带入所选设备；「异常设备数」跳转后依「监控状态」排序。
[自定义总览报表] 导入指定 Dashboard 的元件	自定义总览报表新增时可导入 Dashboard 元件。
[N-Robot] UI UX 优化	此次改版以用户互动为核心，重新设计了视觉层级、操作流程与互动回馈，让系统更易于理解与操作。
[N-Robot] 导引说明	新增 Dashboard 的 「Dashboard 设定」「Dashboard列表说明」引导说明功能。 ※若搭配N-AI模组，此说明将会透过 N-Robot 以人工智能回答。
[N-Robot] 领域接收量爆量告警	新增领域的总流量自动监控，当发生爆量、低流量或无流量时发出N-Robot告警。 1. 总流量资讯包含：syslog接收量、flow接收流量(byte)、flow数据包量、flow记录数(record) 。 2. 爆量或低流量的标准由过去7周的领域总流量学习而来。 3. 低流量或无流量根据flow接收流量(byte)侦测。 4. 设定位于：系统管理 / 通报设定 / N-Robot > N-Robot 预警式告警

	通知 / 领域接收量。
[N-Robot] ATD Report 云端版	新增 ATD 异常流量即时分析 AI 报表功能。 ※搭配N-AI模组，N-Robot才有此功能。
[N-Robot] AI Report 异常登入/邮件告警	「智慧分析 / 统计分析 / 邮件异常告警」(/「异常登入行为分析」)，新增「AI报表」功能，由 LLM 分析指定时间段的资料，产生一份AI分析报表。 ※搭配N-AI模组，N-Robot 才有此功能。
[N-Robot] AI Report 联防记录/黑名单	「报表 / 智慧联防 / 联防记录」(/「黑名单」)，新增「AI报表」功能，由 LLM 分析指定时间段的资料，产生一份AI分析报表。 ※搭配N-AI模组，N-Robot 才有此功能。
[N-Robot] 互动式设定: 设备告警模板	1. 在设备资产树状图页面的编辑功能中，提供设备告警样板的推荐功能。 2. 在告警模板页面中，提供设备告警样板的阈值最佳化功能。 ※搭配N-AI模组，N-Robot 才有此功能。
[AI] 自定义总览报表提供完整与精简分析模式	「自定义总览报表」页面，编辑时用户可切换完整或精简模式，精简模式会隐藏报表内的「关联分析」内容。 ※搭配N-AI模组，设定时类型才能选「智慧总览报表」功能，才可切换模式。
[N-Robot] 提供撷图问答功能	用户可以透过截图贴上的方式让 N-Robot 帮忙分析图内数据，并以自然语言进行互动问答。 ※搭配N-AI模组，N-Robot 才有此功能。
[SLA] 自定义 Port	SLA 新增「PM Port (Round Trip Time，RTT)」项目，透过 Performance Monitoring 机制，量测关键 Port的网络往返延迟。此指标可强化网络效能监控，协助即时发现异常，提升服务稳定性与可用性。
[SLA] 设定及显示优化	1. 优化 SLA 设定与显示。 2. 清单页面优化显示各Node对应绘制的图形。 3. 设定页面优化各Node可独立设定需绘制的图形。 4. 报表页面优化各页签仅显示有设定对应绘制图型的Node。

	5. 设备类的图形改为仪表图(Gauge) 。 6. 离线报表添加对应调整，并优化报表生成流程，确保UI皆已绘制完成才产生报表。 7. 离线报表添加错误纪录功能。
[SLA] Gauge Chart 阈值颜色分区	改用 Gauge Chart 显示 CPU、Memory 和磁碟分割区的用量图，并在各设备页面加载时显示当前状态，用量图仪表区段的颜色根据设备告警样板的阈值呈现。
[SLA] 报表下载优化	服务级别协定 (SLA) 报表下载功能改采用非同步背景处理机制，透过将报表生成作业移至后端执行，在报表生成期间仍可继续操作系统，无需等待报表完成，优化了使用者体验。
[SLA] 新增设备群组监控功能	于SLA统计表页签新增设备监控统计表格；监控统计对象为有设定绘制统计表的设备，并统计该设备 CPU、Memory、Disk三项告警的次数。
[系统时间]校准功能优化	在 「系统管理 / 网络参数设定」，使用 NTP 校时要可选择 NTP Server 或 ntpdate。 ※N-Reporter 才有此功能。
[偏好设定]白名单	在 「系统管理 / 偏好设定」，「白名单」页签新增「异常登入行为」分析功能, 符合白名单之IP不触发告警。
[分时监控报表]功能优化	1. 新增检查机制：删除或停用分时监控报表前，系统会检查该报表是否已被自动执行脚本采用，避免影响既有设定。 2. 告警通知改版优化：寄送邮件时不再附上大量事件资料，改为提供连结；使用者可点击连结登入系统查看完整告警资讯。 3. 报表启用/停用功能：可针对分时监控报表进行「停用」，系统将停止计算与资源消耗。
[优化]画面、信件与报表	修改项目涵盖 UI 画面、告警信件、离线报表，统一描述字眼、排版、数值显示与色系规范，提升整体一致性与可读性。
[云端日志] 新增寄送逾时纪录	告警/报表寄送逾时，记录到后台云端日志，新增下列纪录： 1. 告警信件超过三小时未寄出 2. 时报：超过当前小时未寄出；其他报表(日周月...等)：超过当日寄送时间六小时未寄出 3. 单笔报表执行时间超过30分钟，每半小时记录一次

[云端日志] 新增联防逾时纪录	每半点(30分时)判断前一个小时有无联防尚未执行，若有未执行情况则纪录到后台云端系统日志。
[CLI]指令功能强化	1. 提供 np-vm poweroff 指令强制关掉 VM。 2. CLI 设定支持 IPv6/FQDN。
[报表] TopN 离线报表限制	新增「TopN 报表资源管理与显示」功能： - 资源计算：仅设定「离线报表」的 TopN 报表会占用系统资源。 - 后台显示：在「系统管理 / 系统管理列表 / 资源总览」 中显示 TopN 报表资源使用情况，方便管理者监控。 - 前台显示：在「系统管理 / 领域资讯」 中显示「TopN 报表数」字段，提供用户清楚掌握报表数量。 此次更新提升了资源使用透明度与管理效率，确保 TopN 报表的效能与可控性。
[自动联防] 阻挡或执行失败通知	自动执行脚本信件通报内容添加执行结果。
[TopN] 优化查询排序功能	优化「TopN 查询排序与流量分布图」功能： - 查询时可指定排序数值，系统依选择输出 TopN 结果。 - 同步产生该排序依据的流量分布图，直观呈现资料分布。
[Action] 效能改善	联防效能改善：自动执行脚本若进行阻挡类行为，改为呼叫底层另一支程序负责，并且有执行笔数上限，以提高效能。
[设备] 接口过滤优化	事件、Top N、分时监控报表等功能页面，过滤查询加入接口编号显示，以提升资讯呈现的完整性。
[情资比对] 功能优化	提高情资比对FQDN上限笔数到30万。
[SNMP] 功能优化	SNMP Polling 得到的资讯：磁碟描述、接口描述(包含 Alias、名称)与接口卡字段，能显示中文。
[分时告警] 效能优化	改善分时告警的延迟周期情形，优化分时告警效能。

■ 注意事项

- 在维护合约时效内，提供免费的韧体(Firmware)更新服务。
- N-Reporter 系统，将于此版本更新后，自动重新开机。并于开机后，重新启动所有新的服务功能。
- 本产品已全面停止支持 IE 浏览器。为确保各项功能正常运作，请使用最新版 Chrome、Edge 或 Firefox。由于系统针对 Chromium 核心进行最佳化，建议优先使用 Chrome 或 Edge 浏览器，以享有最流畅的产品体验。
- 此版本建议使用于 N-Partner Kernel 20260514091823 或之后的版本，以确保功能使用正常。
  若无使用BGP及SMB备份功能或是弱点扫描的需求，可暂不更新。若要进行kernel更新，请先判断 eth0 MAC 需「小于」eth1 MAC，若遇到「大于」的状况时，请联系TAC协助更新并重新申请License。
  欲检查 kernel 版本，请于CLI中执行 show version，即可看到NP Kernel version。

```
LB1# show version
Software version : 7.0.041 (20260518-1709)
NP Kernel version : 20260514091823
Serial number :
```

  Kernel升级的详细步骤，请参考「如何更新 N-Cloud / N-Reporter Firmware 与 Kernel」文件中的第5章「如何更新 Kernel」。
- 建议使用 NFS/SMB/FTP 定期备份，以避免因设备异常导致资料遗失。

■ 7.0.X 版升至 7.0.04X 版的更新方式

升级作业请依版本相容性顺序执行：当目标版本为 7.0.04X 时，请分别下载 7.0.028 (下载) 与 7.0.04X (下载) 版本之Firmware，并先完成 7.0.028 版本的升级作业；确认系统已成功更新至 7.0.028 后，方可进一步升级至 7.0.04X 版。

使用者可透过 N-Reporter/N-Cloud 7.X 所提供之 UI 接口，进行 Firmware 与 Kernel 更新，请先以具备后台管理权限之帐号登入系统，并依下列方式完成更新作业。

- Firmware 更新
  - 线上更新
    - ✓ N-Reporter/N-Cloud 支持线上更新。
    - ✓ 请确定 N-Reporter/N-Cloud 可以连线到网际网络，且至少已设定一个 DNS Server。
    - ✓ 于「系统管理」页面中，点选「系统更新」按钮即可进行更新。
  - 离线更新
    - ✓ N-Reporter/N-Cloud 7.X 亦支持透过离线方式进行升级。
    - ✓ 于「系统管理」页面中， 点选「上传软体更新档」按钮，选择已下载的 ncloud-7.x.xxx.img 档案，并点选 「导入」 按钮，即可开始上传并执行更新。
- Kernel 更新
  请先下载7.0.X最新版 Kernel (下载)档案，并完成后续更新作业。
  - N-Reporter/N-Cloud更新 Kernel

    于「系统管理」页面中，点选下方「设备」，再切换至「Kernel 更新」 页签。点击「排程更新」按钮，开启「Kernel 更新」视窗后，选择「手动上传」，即可上传 Kernel 档案并执行更新。详细步骤请参考「如何更新 N-Cloud / N-Reporter Firmware 与 Kernel」文件中的第5章「如何更新 Kernel」。

■ 6.1.18X 版升至 7.0.X 版的更新方式

若您原本使用的版本是N-Reporter/N-Cloud 6.1.18X之前的版本，请参阅文件「如何更新 N-Cloud / N-Reporter Firmware 与 Kernel」第2章，进行更新。

若您目前使用 6.1.18X 之后的版本，可参阅上述文件第3章，先更新至 6.X 最新版，再更新至 7.X 版，请依照下列

步骤进行更新：

- Firmware 与 Kernel 更新

1. 下载最新6.1.18X版本 Firmware 档案(下载)
2. 请以后台管理权限的帐号登入系统
3. 上传档案：于「系统管理」页面点选「上传软体更新档」，选择第1步骤所下载的 ncloud-6.1.18x.img 档案，并点击「导入」 按钮开始上传。请稍后约三分钟，即可完成 Firmware 更新。
4. 升级至7版前，请先确认CPU型号；若CPU型号为E3 v3，则不建议升级至7版，请先联系您所购买之 N-Partner 产品经销商/代理商，或联系本公司业务部门。
5. 若 CPU 非 E3 v3 型号，请参考上一小节「7.0.X 版升至 7.0.04X 版的更新方式」，继续进行后续步骤。
6. 若您已更新至 6.X 最新版本，且暂不升级至7版，请完成 Kernel 更新，详细步骤请参考「如何更新 N-Cloud / N-Reporter Firmware 与 Kernel」文件中第5章「如何更新 Kernel」。

注：6 版升级至 7 版前，请先以 CLI 指令 show hardware cpu 检查 CPU 型号。

```
LB1# show hardware cpu
CPU Model: Intel(R) Xeon(R) CPU E3-1231 v3 @ 3.40GHz, CPU Socket: 1, CPU Core: 4, CPU Thread: 8
LB1#
```

上图例 CPU 为 E3 v3 的型号，若有相关疑问，请联系经销商/代理商，或洽询本公司业务部门 (sales@npartner.com) 。

■ SNMP支持列表

► Switch / Router

- ✓ Alcatel
- ✓ Aruba 6300、Aruba Switch
- ✓ Brocade、Brocade VDX
- ✓ Cisco ASR、Cisco N9K、Cisco Nexus、Cisco Router、Cisco Switch
- ✓ D-Link、D-Link DGS 1000
- ✓ Dell Switch OS6
- ✓ Edgecore
- ✓ Extreme、Extreme EXOS
- ✓ FortiSwitch
- ✓ Foundry (Brocade)
- ✓ HP、HPE、HPE 1900、HPE S7500E
- ✓ Host Mib
- ✓ Huawei
- ✓ Juniper Switch
- ✓ MOXA
- ✓ Ruckus ICX
- ✓ Ruijie
- ✓ Standard Switch
- ✓ UCD-SNMP-MIB
- ✓ ZyXel Switch

► Application/DB/OS/Server

- ✓ Host Mib

► Firewall/IPS/Load Balancer/ NAC/UTM/WAF/Wireless

- ✓ A10
- ✓ Airwave
- ✓ Aruba Controller、Aruba Controller 8.0
- ✓ CheckPoint
- ✓ Cisco ASA (FirePOWER)、Cisco Controller WLC (2500,3500,5500)、Cisco Controller WLC(Cisco Catalyst 9800 Series Wireless Controllers)、Cisco FirePOWER
- ✓ F5 Networks
- ✓ Fortigate
- ✓ Host Mib
- ✓ Juniper SRX
- ✓ Paloalto
- ✓ Peplink

- ✓ Ruckus AP、Ruckus SmartZone、Ruckus ZoneDirector
- ✓ Sophos
- ✓ ZyXEL USG

► N-Cloud/N-Reporter/N-Probe

- ✓ Host Mib
- ✓ N-Partner

► Auto/ More/User Defined Format

- ✓ Generic Device
- ✓ Host Mib
- ✓ N-Partner

■ Syslog支持列表

► Switch / Router

- ✓ Aruba Switch
- ✓ Brocade Switch
- ✓ Cisco Nexus、Cisco Switch
- ✓ Dell Switch、Dell Switch OS 10
- ✓ Extreme Switch
- ✓ FortiSwitch
- ✓ Foundry Switch
- ✓ HP Switch、HPE Switch
- ✓ Huawei Switch
- ✓ Juniper Switch
- ✓ Ruckus ICX Switch
- ✓ User Defined Format
- ✓ ZyXEL Switch

► Application/DB/OS/Server

- ✓ AIX
- ✓ Apache
- ✓ ESXi、ESXi vCenter
- ✓ Exchange 2007、Exchange 2010、Exchange 2013
- ✓ IIS
- ✓ KH-OpenID、KH-KNTT
- ✓ Linux DHCP、Linux Radius、Linux Sendmail
- ✓ MS SQL、MS SQL (Common Event Format)
- ✓ MySQL
- ✓ Nginx
- ✓ OpenVPN
- ✓ Openfind Mail2000
- ✓ Oracle
- ✓ Postfix
- ✓ Postgrey
- ✓ PostgreSQL
- ✓ Squid
- ✓ SunOS
- ✓ UNIX DNS、UNIX FTP、UNIX/Linux/Solaris
- ✓ User Defined Format
- ✓ Windows、Windows (Raw)、Windows 2003 AD Server (WMI)、Windows 2003 Server (WMI)、

Windows 2008/2012 (WMI)、Windows 2008/2012 AD Server (WMI)、Windows AD、Windows AD (Raw)、Windows DHCP、Windows DNS

- ✓ Winoc
- ✓ ZDNS

► Firewall/IPS/Load Balancer/ NAC/UTM/WAF/Wireless

- ✓ A10 Load Balancer、A10 TPS、A10 Thunder
- ✓ AWS VPC Flow
- ✓ AboCom-UM
- ✓ AgileLink
- ✓ AndaPAM
- ✓ Arbor、Arbor (Common Event Format)
- ✓ Arcnet Traffic
- ✓ Array Networks
- ✓ Aruba、Aruba CX10000、Aruba Clearpass、Aruba Airwave
- ✓ AscenFlow
- ✓ AscenLink Traffic
- ✓ Astaro
- ✓ Axway APIM
- ✓ Barracuda Web Security Gateway
- ✓ Blue Coat、Blue Coat SG 6.6.5.2、Blue Coat SG 6.7.3.12
- ✓ Bluepunkt
- ✓ Broadweb Netkeeper
- ✓ CCU SSO
- ✓ Cellopoint
- ✓ CheckPoint、CheckPoint (Common Event Format)、CheckPoint CloudGuard WAF、Checkpoint 1500
- ✓ Cisco ACS、Cisco ASA、Cisco Firepower、Cisco Firepower (Common Event Format)、Cisco IPS 4240、Cisco ISE、Cisco Ironport Mail、Cisco Ironport WSA、Cisco WLC、Cisco WLC 17.9.5 above
- ✓ Citrix、Citrix (Common Event Format)、Citrix NetScaler
- ✓ Cloudflare
- ✓ Comodo
- ✓ Corero TopLayer
- ✓ CrowdStrike
- ✓ Cyberoam
- ✓ DP Tech DPX
- ✓ Decent DHCP
- ✓ Devecot
- ✓ Draytek
- ✓ ESET NOD32、ESET Protect

- ✓ Extreme Wireless
- ✓ F-Secure
- ✓ F5 ASM、F5 ASM (Common Event Format)、F5 BIG-IP、F5 LTM
- ✓ FiberLogic OptiQroute
- ✓ Forcepoint Email Security、Forcepoint NGFW、Forcepoint Sidewinder、Forcepoint Web Security、Forcepoint Web Security (Common Event Format)
- ✓ ForeScout
- ✓ FortiManager、FortiPAM、FortiWAN、FortiWeb、Fortinet
- ✓ GSI
- ✓ Guardix
- ✓ HP Wireless、HPE Access Controller、HPE Firewall、HPE IPS
- ✓ Hgiga
- ✓ Hillstone
- ✓ Huawei NGFW、Huawei USG Firewall
- ✓ IBM Proventia (ISS)
- ✓ IDExpert
- ✓ IDMART
- ✓ IXIA、IXIA (Common Event Format)
- ✓ Imperva、Imperva (Common Event Format)、Imperva Incapsula (Common Event Format)
- ✓ Infoblox
- ✓ Ironport ESA
- ✓ Jethro Qos
- ✓ Juniper ISG、Juniper NSM、Juniper Netscreen、Juniper PIC、Juniper SRX、Juniper SRX (Junos 12.0.3 above)、Juniper SRX (Junos 12.1x44 above)、Juniper SRX (Junos 12.3X48-D65.1 above)、Juniper SRX (Junos 15.1X49-D150 above)、Juniper SRX (Junos 15.1X49-D75.5)、Juniper SRX (Junos 19.4R3-S1.3 above)、Juniper SRX (Junos 20.2R3-S2.5 above)、Juniper SRX Structured、Juniper SSL VPN
- ✓ Kaspersky、Kaspersky BSD、Kaspersky KATA
- ✓ L7、L7 InstantCheck
- ✓ Legendsec NSG3000
- ✓ LinkProof
- ✓ McAfee IPS、McAfee NSP、McAfee Sidewinder
- ✓ MiWAF
- ✓ Mirapoint
- ✓ Motorola AP
- ✓ NetApp
- ✓ NetIQ
- ✓ Netskope (Common Event Format)
- ✓ Novell

- ✓ Nsfocus ADS-M
- ✓ OpenStack NCHC
- ✓ Openfind MailGate
- ✓ PacketX
- ✓ Paloalto、Paloalto (Common Event Format) 、Paloalto Cortex XDR、Paloalto Trap
- ✓ Panorama
- ✓ Peplink
- ✓ PfSense、Pfsense 2.5 dev
- ✓ Power admin File Sight Ultra
- ✓ Ivanti (Pulse Secure)
- ✓ QNAP
- ✓ RabbitMQ
- ✓ Radware APsolute、Radware Alteon、Radware AppWall、Radware DefensePro5、Radware DefensePro6、Radware DefensePro8、Radware DefensePro10
- ✓ Raw Data
- ✓ Ruckus、Ruckus Controller
- ✓ Ruijie AC
- ✓ SafeGuard (Common Event Format)
- ✓ Sangfor、Sangfor AC、Sangfor AF、Sangfor EDR
- ✓ SentinelOne (Common Event Format)
- ✓ ShareTech Mail Server、Sharetech
- ✓ Simple DNS
- ✓ Sire XDR
- ✓ Snort
- ✓ Socus
- ✓ SonicWALL
- ✓ Sophos、Sophos UTM
- ✓ Sourcefire
- ✓ Swift
- ✓ Symantec ATP、Symantec DLP、Symantec Message Gateway、Symantec ProxySG、Symantec SEP、Symantec SSLV
- ✓ Synology
- ✓ TOPSEC (天融信)
- ✓ TX One ODC
- ✓ Tipping Point、Tipping Point (Common Event Format)、Tipping Point NGFW、Tipping Point SMS
- ✓ Trend Micro (Common Event Format)、Trend Micro Apex Central、Trend Micro Apex Central (Common Event Format)、Trend Micro IWSVA、Trend Micro TMCM、Trend Micro Vision One (Common Event Format)
- ✓ UGuard

- ✓ UPAS、UPAS(Common Event Format)
- ✓ Uila
- ✓ User Defined Format
- ✓ VMware NSX、VMware VDI
- ✓ Venus Tech
- ✓ Vigor Firewall
- ✓ WatchGuard、Watchguard LEEF
- ✓ Websense DLP、Websense DLP (Common Event Format)
- ✓ ZyXEL USG、ZyXEL USG (Common Event Format)、ZyXEL WAC6500
- ✓ iSafer DNS

► N-Cloud/N-Reporter/N-Probe

- ✓ N-Partner
- ✓ User Defined Format

► Auto/ More/User Defined Format

- ✓ CCU Application
- ✓ CWB Mtsvc、CWB QappAccess、CWB QappPush
- ✓ MQTT
- ✓ N-Partner
- ✓ User Defined Format

■ 联防支持列表—下达CLI指令

◆ Switch/Router

► Syslog

- ✓ Aruba Switch
- ✓ Cisco Switch
- ✓ Dell Switch
- ✓ HPE Switch
- ✓ Huawei Switch

► SNMP

- ✓ Alcatel
- ✓ Aruba Switch
- ✓ Cisco Switch
- ✓ Dell Switch
- ✓ Extreme EXOS
- ✓ HPE、HP
- ✓ Huawei Switch、Huawei
- ✓ MOXA
- ✓ ZyXel Switch

◆ Firewall/IPS/Load Balancer/NAC/UTM/WAF/Wireless

► Syslog

- ✓ CheckPoint、CheckPoint (Common Event Format)
- ✓ F5 ASM、F5 ASM (Common Event Format)、F5 BIG-IP、F5 LTM
- ✓ Fortinet
- ✓ Paloalto、Paloalto (Common Event Format)

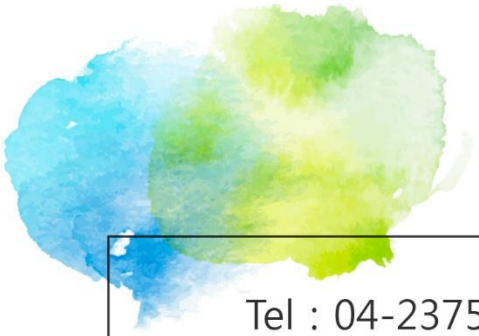
- ✓ TippingPoint
- ✓ ZyXEL USG、ZyXEL USG (Common Event Format)

- ► **SNMP**
  - ✓ Aruba Controller、Aruba Controller 8.0
  - ✓ CheckPoint
  - ✓ F5 Networks
  - ✓ Fortigate
  - ✓ Paloalto
  - ✓ Ruckus AP
  - ✓ ZyXEL USG

■ 联防支持列表—黑名单阻挡设备

- ► Fortigate
- ► PacketX
- ► Paloalto
- ► SDN
- ► TippingPoint SMS

技术文件下载
文件下载请至 http://www.npartner.com/



Tel：04-23752865　　Fax：04-23757458
業務詢問：sales@npartner.com
技術詢問：support@npartner.com