N-Reporter/N-Cloud
Release Note 7.0.04X

(支援7.0.04X之後的所有版本)

2026/05/28

目錄

■ 更新重大項目

項目名稱	項 目 描述
[Kernel版本] 建議版本搭配	為確保產品使用正常，請採用 7.0.04X 版本 Firmware (下載)，搭配最新的 Kernel 版本(下載)。 ※建議使用 N-Partner Kernel 20260514091823 或更新的版本，以確保功能正常運作。
[N-Robot] UI UX 優化與 AI 功能	此次改版以用戶互動為核心，重新設計了視覺層級、操作流程與互動回饋，讓系統更易於理解與操作。 ※搭配N-AI模組，N-Robot提供自然語言問答、智慧報表關鍵洞察，以及多變環境下推薦最佳配置等功能。
[SLA] 功能新增與優化	SLA 新增了設備監控統計表與「PM Port (RTT)」功能，強化網路效能監控，協助即時發現異常，提升服務穩定性與可用性。優化的內容包括改用儀表圖顯示用量狀態，並在報表生成上採用非同步處理，提升使用者體驗
[Dashboard] 功能新增與優化	Dashboard新增動畫效果，並支援多種SLA監控、程序監控，並優化了關聯頁面的跳查功能。自定義總覽報表提供讓用戶匯入Dashboard元件，提高了設定自由度與使用體驗。

■ 新增功能及修正列表

項目名稱	項目描述
[License] PM、ICMP、SNMP 資源類型，授權機制優化	使用者在匯入 License 時，會判斷目前 License 支援哪些功能模組，以及各模組可使用的授權數量；若設備實際使用的資源，超過 License 允許的數量，或該 License 未授權支援該模組，系統會自動停用（關閉）該設備上使用該資源的功能。
[UI] 伺服器稽核 Global 新增領域選項	1. 稽核報表 / 伺服器稽核的 Global 領域新增領域選項。 2. 稽核報表 / 伺服器稽核 / 主機登入稽核的 Global 領域新增領域選項。
[資料庫備份] 支援SFTP	後台 「系統管理 / 資料庫管理」資料庫備份與資料庫回復，新增 SFTP 方式做備份還原。
[FTP] 備份功能優化	備份失敗時，Log 會顯示是哪一份檔案出問題。
[告警轉 Syslog] 內容新增設備 IP	設備告警轉 Syslog 新增設備 IP (dev_ip) 至 Ext11 欄位。
[UI] 介面優化: 設備管理 > 批次設定	將設定項目從過濾條件移出，放置於工具列的第一位置，便於使用者操作且辨識目前的設定項目。
[UI] 加入 N-Probe 操作歷程	在 N-Cloud / N-Reporter 上可看到 N-Probe 的操作紀錄。
[Parser] User Defined Parser 的 keyword 處理優化	「設備管理 / 自定義資料格式」 修正 Tag Value Pair 類型：測試樣本標籤中，有重複字串或包含逗號時，優化顯示與正規化結果。
[UI] User Defined Parser 匯出匯入	新增「設備管理 / 自定義資料格式」匯入與匯出功能。
[Action] 欄位新增	「報表 / 智慧聯防 / 自動執行腳本」聯防參數新增 audit_user 供腳本使用。
[UI] 設備告警繪圖顯示告警時間線	設備告警圖標示出告警發生的時間軸，方便進行對照和檢視。

[UI] SMTP 設定操作優化	1. 未設定SMTP Server 時加上提醒。 2. 領域管理新增領域視窗調整。
[PM] Web 監控資訊優化	Web 監控目標為 FQDN 時，要記錄當下 Polling IP，在瀏覽與通報信件中顯示 IP 資訊。
[PM] Port Polling 新增 RTT 資訊	[效能監控]新增 Port 監控提供 Round Trip Time 資訊。
[PM] ICMP 群組調整及路徑圖	1. ICMP 監控的群組功能調整。 2. ICMP 監控列表拆分為獨立監控和群組監控。 3. ICMP 群組瀏覽提供 MTR 圖形和以監控設備為單位的流量圖。 4. 停用 Web 監控和 Port 監控的群組相關功能。
[PM] Web 效能監控設定調整	優化 Web 監控「門檻值」與「敏感度」的操作方式與說明。
[PM] PM 群組改為標籤功能	加入效能監控標籤功能。
[PM] 支援IPv6	效能監控新增支援IPV6目標監控。
[情資] 情資比對新增進階比對功能	情資比對新增進階比對功能，情資類型可以多選, 信賴評分可以選擇分數區間。
[設備檔備份] TFTP 支援 VR 選項	Extreme EXOS設備設定檔備份支援帶入VR (Virtual Routing) 。
[DPI] 事件、TopN、Filter	事件、TopN、Filter TopN 支援 Flow 輸出 Deep Packet Inspection (DPI) 資訊。
[DPI] 新增類別資訊	事件、TopN、Filter TopN、IP 軌跡查詢條件，支援Flow 輸出 Deep Packet Inspection (DPI) 的類別資訊。
[設備] 單機設備 Raw Data 下載機制優化	N-Reporter 設備下載 Raw Data 改成與 N-Cloud 一致：1. 可直接下載，不需先另存檔案。 2. 設備需要先勾選 Raw Data 保留。

[名稱解析流量異常告警] 各領域事件數量總覽	Global的名稱解析流量異常告警加上領域告警數統計及快捷點選查詢。 ※Global 專屬功能
[報表] 輸出(CSV)顯示國家名稱	事件及TopN輸出(CSV)，來源及目的區域欄位值呈現變更為國家代號(國家名稱)。
[Kernel] Upgrade 流程優化	1. 新增強制結束更新按鈕。 2. 更新後若需要重開機會有推播警告。 ex: 5 分鐘後將重啟，1 分鐘內將重啟，30 秒內將重啟。 3. 重啟時，前後台 UI 畫面會顯示重啟畫面。
[登入] 多因子認證	增加登入 E-mail 雙重驗證功能。
[雲端日誌] 訊息優化	系統授權(License)不足時，紀錄至後台雲端系統日誌。
[雲端日誌] 分時轉發逾時	[後台] [雲端系統日誌] 新增分時監控 Syslog 條件轉發逾時紀錄。
[雲端日誌] SNMP Polling 逾時	若當日 SNMP 監控有逾時的情形，系統將記錄至後台「雲端系統日誌」。
[UI] 列表功能位置優化	列表繪圖瀏覽功能欄位移置操作欄位右側。
[UI] VMI 測試功能	「設備管理 / 設備資產樹狀圖」頁面，新增或編輯設備時，監控與告警 > 監控與連線測試，可對 WMI 設備進行 "設備連線測試"。
[UI] 批次設定過濾條件優化	「設備管理 / 批次設定」頁面，過濾條件選單加上 "附加條件": "暫停接收"、"設備維護中"、"設備共享"、"聯防設備" 等項目。
[UI] 憑證功能優化	「系統管理 / 網路參數設定 / 憑證管理」新增「產生 CSR 」功能。除了必填的主旨資訊如網址/網域外，用戶還可以選擇填寫組織、國家等資訊。生成的 CSR 檔案可用於申請正式憑證。

[ATD] 指定flow設備計算ATD資料	可指定對特定設備或所有設備，進行 FLOW ATD 異常流量分析統計。
[操作歷程] 資訊呈現優化	後台操作歷程可以區分 N-Probe 指令的來源：是從 N-Cloud 更新，還是從 N-Probe 更新。
[黑名單] 新增FQDN派送	1.事件查詢支援FQDN (來源/目的主機,EXT8 ,EXT9) 加入黑名單。 2.自動執行腳本支援FQDN(來源/目的主機,EXT8 ,EXT9) 加入黑名單。
[設備資產樹狀圖] 新增告警通報設定 (預設)	設備資產樹狀圖可設定該領域的告警通報設定(預設)之通報原則，其設定結果與「系統管理 / 通報設定」頁面 >「告警通報設定」頁籤 >「設備異常告警」 類別的「預設」共通。
[設備資產樹狀圖] 設備狀態樹圖示優化	硬體狀態包含 Syslog (/Flow) no data 的告警，無資料時也會在樹狀圖設備後出現告警圖示。
[Offline center]效能優化	平均分配報表總數到不同 Center 寄信，降低總執行時間。
[TopN 報表] 批次修改資料格式	對已儲存的 TopN 報表，可批次修改資料格式：HTML, PDF, CSV, XML。
[TopN] 已儲存報表點擊動作優化	TopN 已儲存報表頁面，點擊報表名稱會帶入條件並執行查詢動作；勾選報表後點擊編輯則進入純編輯模式，不啟動查詢。
[情資資料庫] 新增來源	新增「預設情資資料庫」的情資來源 - MISP 納入 AbuseIPDB。
[SNMP] 網路拓樸 (Topology) Auto Discovery 支援可選監控設備	新增「監控設備」選項，能指定 N-Probe 做為網路拓樸的探索設備。基於效能考量，同一領域下同時只能由一拓樸執行 Auto-Discovery。
[UI] 密碼重置流程優化	密碼重置流程更新：密碼重置信件中的連結將於密碼成功重置後立即失效，以提升帳戶安全性。
[UI] 領域模擬權限控管	「系統管理 / 領域模擬」頁面權限為唯讀的帳號，在「領域模擬」

	列表時，僅列出唯讀權限的帳號。
[UI] 上傳功能優化	系統上傳檔案可能因檔案過大或用戶的網路環境和速度問題導致超時。超時會顯示警告，建議使用者檢查網路，改用 FTP 或其他方式上傳。
[IP 名稱解析] 功能優化	異常流量告警門檻值設定：新增功能 "不啟用" 與 調整功能 "手動設定" 可以部份啟用。
[SNMP] 設備告警功能優化	「系統管理 / 通報設定」的「告警通報設定」頁籤，設備異常告警類別在設定通報群組時，可分別設定紅色與黃色告警通報群組。
[黑名單] 記錄當下黑名單資訊	系統在 Syslog 與 Flow 中即時記錄黑名單資訊，提升可追溯性。事件/Top N/分時監控等功能頁面與相關報表，於「來源IP」或「目的IP」欄位標示黑名單資訊。
[偏好設定] 設備設定檔顯示優化	「系統管理 / 偏好設定」功能頁面，「設備管理 / 設備設定檔備份」自動備份功能，添加支援型號的提示。
[告警樣版] 自訂 OID 樣版功能優化	「設備管理 / 告警樣版」頁面，「自訂 OID 樣版」頁籤中加入 SNMP 測試後的測試結果下載功能。
[ATD] ATD效能優化	53 port 和 123 port 不列入 UDP Port Scan 計算。
[ATD] 黑名單/阻擋功能	ATD 異常流量即時分析列表，針對 IP 可以右鍵加入 IP 阻擋或黑名單功能。
[UI]後台使用者總表操作優化	擷取過濾條件中的領域，自動帶入新增使用者的領域選取中。
[檔案簽章] 功能頁面異動	將前台的檔案簽章相關功能移至後台「資料庫管理」功能頁面，方便使用管理。
[Receiver] Extend field 顯示優化	Extend field 內容長度256以上時，超過部分以「...」取代，並顯示提示資訊。

[接收量] Syslog/Flow 記錄丟棄量	1. 前台「領域資訊」與後台「領域管理」頁面新增切換功能，可查看 Syslog 與 Flow 接收量超過 EPS 的次數及最大丟棄量。 2. 後台「系統管理」的 N-Probe 設備頁面新增切換功能，可查看該設備接收資料時超過 EPS 的次數及最大丟棄量。
[UI] 跳查 TopN 功能優化	分時監控 TopN 報表跳查 TopN 時，提供對映的排序依據組合。
[聯防記錄]功能優化	聯防記錄的查詢條件加上自動執行腳本選項。
[SNMP] 流量圖資訊優化	SNMP 相關流量圖(CPU, Memory, Interface, Disk, User defined OID)，查詢三天以上顯示最大值和最小值。
[Auto Action] 樣版參數擴充	「報表 / 智慧聯防 / 自動執行腳本」頁面，指令樣版新增參數：來源(/目的)名稱解析、來源(/目的)Port解析。
[Auto Action] 新增低量告警執行動作	「報表 / 智慧聯防 / 自動執行腳本」判定條件為分時監控報表時，可設定低量告警執行指令。
[Auto Action] 腳本參數擴充	指令樣板支援信賴評分、情資類型參數。
[黑名單] 支援 URL 方式匯入	新增黑名單的 URL 設定功能。
[網路拓樸] 列表增加備註欄位	網路拓樸列表加入備註欄位。
[網路拓樸] 編輯模式時增加格線功能	拓樸圖編輯模式顯示格線，方便設備定位。
[System] Receiver 低量/無資料告警	自動監控N-Receiver的Syslog封包或是Flow Record量。 - 若持續10分鐘以上無資料，觸發一次無資料告警。當資料量回復時，才重新啟動此監控。 - 相較於過去資料量處於低量，且持續10分鐘以上，則觸發一次低量告警，若已屬於無資料告警，則不觸發。當資料量回復正常時，才重新啟動此監控。

[事件查詢] 查詢條件擴充	事件查詢 Syslog 查詢條件新增 TCP Flags。
[通報設定] 郵件主旨設定優化	告警通報設定的郵件主旨可多選，並可調整前後順序。
[偏好設定] 登入啟用 E-Mail 驗證優化	啟用 E-mail 驗證前會先檢查：1. 已設定 SMTP Server，且前後台 Server 設定一致；2. E-mail 信箱可收取驗證碼。
[SNMP] 搜尋設備時可選監控設備	「設備管理 / 設備資產樹狀圖」頁面，批次新增設備可以選擇 N-Probe 作為監控設備進行掃描。
[離線報表寄送記錄] 功能優化	狀態文字修改、通報群組連動對應的領域，以提升用戶體驗。
[操作歷程] 新增「操作行為報表」	前台「系統管理 / 操作歷程」操作行為報表提供： 1. 頁面使用排行圖：統計(全部/單一帳號)頁面使用次數排行 2. 帳號使用時間圖：統計(全部/單一帳號)每個小時存取系統資料的次數 ※Global 專屬功能。
[設備樹狀圖] 搜尋功能變更	透過關鍵字搜尋設備名稱與 IP 時： 1. 左側樹狀圖只有領域(或資料夾) 符合關鍵字，右側設備列表會列全部設備。 2. 左側樹狀圖領域(或資料夾)與設備都符合關鍵字，右側設備列表僅保留有符合關鍵字的設備。
[設備樹狀圖] 告警圖示美化	告警圖示美化： 1. 設備(/效能)異常告警更好辨識。 2. 領域(與資料夾)底下若有告警，將告警總數標示於對應的圖示後面。
[設備細項設定] 新增介面過濾條件	用戶 IP 對應 MAC 功能頁籤，過濾條件添加介面名稱。

[UI] - 過濾禁用符號	限制用戶輸入禁用符號，避免影響字串的解析，導致系統出錯。
[離線報表寄送記錄] 手動寄送報表	後台「離線報表寄送記錄」提供手動寄送離線報表。
[UX][列表頁] 過濾條件優化	當滑鼠游標移動到功能列上的「過濾條件」按鈕時，透過 Tooltip 顯示目前設定的過濾條件。
[IP 名稱解析] 內建網段重覆時警語	新增或編輯「IP 名稱解析」時，若與系統內建已知網段重複時，給予錯誤訊息:「此網段定義與系統內建規則重複」。
[系統管理] 系統效能分析功能優化	後台「系統管理」頁面的「系統效能分析」功能，可即時進行主機系統分析，或「下載分析檔案」後，將檔案交付給 N-Partner 服務團隊，進行離線研讀分析。
[告警樣版] User Defined OID 樣版新增編輯規則變更	「設備管理 / 告警樣版」頁面，User Defined OID 樣版需要先通過 SNMP 測試，得到結果為數值才能儲存該樣版。
[情資] 功能優化	「情資資料庫」 功能調整與新增如下： 1. 在「事件 / 事件查詢」頁面新增「情資來源」欄位。 2. 在「事件 / 事件查詢」結果列表中，將查詢時的比對更改為系統接收時符合情資資料庫的「情資來源」、「情資類型」和「信賴評分」內容。。 3. 在「系統管理 / 偏好設定」頁面，「事件欄位」新增「情資來源」可選欄位。
[Purge] 設備資料機制修改	在領域選取的資料接收設備的預估可用量尚未計算完成前，此領域的設備無法設定正規化資料保留天數。
[設備] 設備/PM 通知類燈號美化	設備與 PM 的通知類燈號變更為鈴鐺圖示。
[UI] Dashboard - CPU core table	新增元件:「其他」 > 「SNMP - 設備監控 > CPU」。
[UI]Dashboard 顯示優化	已移除或停用報表會於 Dashboard 瀏覽畫面上顯示提示。

[UI] SLA 功能可以在Dashboard 顯示	Dashboard增加支援：1. SLA - 統計表（表格）、2. SLA - SNMP（表格、曲線圖）、3. SLA - Flow（曲線圖）、4. SLA - ATD（表格）。
[Dashboard] 動態設計	新增 Dashboard 動畫。
[Dashboard] 新增「動畫開關」設定	「系統管理 / 偏好設定 / 報表」新增 Dashboard 頁籤，新增 Dashboard 動畫效果開關。
[Dashboard] 新增程序告警監控	Dashboard 增加支援程序監控（曲線圖/面積圖）。
[Dashboard] 加入PM監控 - Web、ICMP	告警狀態元件新增資料來源：效能告警監控。
[Dashboard] 設備數量顯示元件跳查功能	Dashboard 的「設備健康度」跳轉至「設備管理 / 設備資產樹狀圖」時自動帶入所選設備；「異常設備數」跳轉後依「監控狀態」排序。
[自定義總攬報表] 匯入指定 Dashboard 的元件	自定義總覽報表新增時可匯入 Dashboard 元件。
[N-Robot] UI UX 優化	此次改版以用戶互動為核心，重新設計了視覺層級、操作流程與互動回饋，讓系統更易於理解與操作。
[N-Robot] 導引說明	新增 Dashboard 的「Dashboard 設定」「Dashboard列表說明」引導說明功能。 ※若搭配N-AI模組，此說明將會透過 N-Robot 以人工智能回答。
[N-Robot] 領域接收量爆量告警	新增領域的總流量自動監控，當發生爆量、低流量或無流量時發出N-Robot告警。 1. 總流量資訊包含：syslog接收量、flow接收流量(byte)、flow封包量、flow記錄數(record) 。 2. 爆量或低流量的標準由過去7周的領域總流量學習而來。 3. 低流量或無流量根據flow接收流量(byte)偵測。 4. 設定位於：系統管理 / 通報設定 / N-Robot > N-Robot 預警式告警

	通知 / 領域接收量。
[N-Robot] ATD Report 雲端版	新增 ATD 異常流量即時分析 AI 報表功能。 ※搭配N-AI模組，N-Robot才有此功能。
[N-Robot] AI Report 異常登入/郵件告警	「智慧分析 / 統計分析 / 郵件異常告警」(/「異常登入行為分析」)，新增「AI報表」功能，由 LLM 分析指定時間段的資料，產生一份AI分析報表。 ※搭配N-AI模組，N-Robot 才有此功能。
[N-Robot] AI Report 聯防記錄/黑名單	「報表 / 智慧聯防 / 聯防記錄」 (/「黑名單」)，新增「AI報表」功能，由 LLM 分析指定時間段的資料，產生一份AI分析報表。 ※搭配N-AI模組，N-Robot 才有此功能。
[N-Robot] 互動式設定: 設備告警樣版	1. 在設備資產樹狀圖頁面的編輯功能中，提供設備告警樣板的推薦功能。 2. 在告警樣版頁面中，提供設備告警樣板的門檻值最佳化功能。 ※搭配N-AI模組，N-Robot 才有此功能。
[AI] 自定義總覽報表提供完整與精簡分析模式	「自定義總覽報表」頁面，編輯時用戶可切換完整或精簡模式，精簡模式會隱藏報表內的「關聯分析」內容。 ※搭配N-AI模組，設定時類型才能選「智慧總覽報表」功能，才可切換模式。
[N-Robot] 提供擷圖問答功能	用戶可以透過截圖貼上的方式讓 N-Robot 幫忙分析圖內數據，並以自然語言進行互動問答。 ※搭配N-AI模組，N-Robot 才有此功能。
[SLA] 自定義 Port	SLA 新增「PM Port (Round Trip Time，RTT)」項目，透過 Performance Monitoring 機制，量測關鍵 Port的網路往返延遲。此指標可強化網路效能監控，協助即時發現異常，提升服務穩定性與可用性。

[SLA] 設定及顯示優化	1. 優化 SLA 設定與顯示。 2. 清單頁面優化顯示各Node對應繪製的圖形。 3. 設定頁面優化各Node可獨立設定需繪製的圖形。 4. 報表頁面優化各頁籤僅顯示有設定對應繪製圖型的Node。 5. 設備類的圖形改為儀表圖(Gauge) 。 6. 離線報表添加對應調整，並優化報表生成流程，確保UI皆已繪製完成才產生報表。 7. 離線報表添加錯誤紀錄功能。
[SLA] Gauge Chart 門檻值顏色分區	改用 Gauge Chart 顯示 CPU、Memory 和磁碟分割區的用量圖，並在各設備頁面加載時顯示當前狀態，用量圖儀表區段的顏色根據設備告警樣板的門檻值呈現。
[SLA] 報表下載優化	服務級別協定 (SLA) 報表下載功能改採用非同步背景處理機制，透過將報表生成作業移至後端執行，在報表生成期間仍可繼續操作系統，無需等待報表完成，優化了使用者體驗。
[SLA] 新增設備群組監控功能	於SLA統計表頁籤新增設備監控統計表格；監控統計對象為有設定繪製統計表的設備，並統計該設備 CPU、Memory、Disk三項告警的次數。
[系統時間]校準功能優化	在 「系統管理 / 網路參數設定」，使用 NTP 校時要可選擇 NTP Server 或 ntpdate。 ※N-Reporter 才有此功能。
[偏好設定]白名單	在 「系統管理 / 偏好設定」，「白名單」頁籤新增「異常登入行為」分析功能, 符合白名單之IP不觸發告警。
[分時監控報表]功能優化	1. 新增檢查機制：刪除或停用分時監控報表前，系統會檢查該報表是否已被自動執行腳本採用，避免影響既有設定。 2. 告警通知改版優化：寄送郵件時不再附上大量事件資料，改為提供連結；使用者可點擊連結登入系統查看完整告警資訊。 3. 報表啟用/停用功能：可針對分時監控報表進行「停用」，系統

	將停止計算與資源消耗。
[優化]畫面、信件與報表	修改項目涵蓋 UI 畫面、告警信件、離線報表，統一描述字眼、排版、數值顯示與色系規範，提升整體一致性與可讀性。
[雲端日誌] 新增寄送逾時紀錄	告警/報表寄送逾時，記錄到後台雲端日誌，新增下列紀錄： 1. 告警信件超過三小時未寄出 2. 時報：超過當前小時未寄出；其他報表(日周月...等)：超過當日寄送時間六小時未寄出 3. 單筆報表執行時間超過30分鐘，每半小時記錄一次
[雲端日誌] 新增聯防逾時紀錄	每半點(30分時)判斷前一個小時有無聯防尚未執行，若有未執行情況則紀錄到後台雲端系統日誌。
[CLI]指令功能強化	1. 提供 np-vm poweroff 指令強制關掉 VM。 2. CLI 設定支援 IPv6/FQDN。
[報表] TopN 離線報表限制	新增「TopN 報表資源管理與顯示」功能： - 資源計算：僅設定「離線報表」的 TopN 報表會占用系統資源。 - 後台顯示：在「系統管理 / 系統管理列表 / 資源總覽」 中顯示 TopN 報表資源使用情況，方便管理者監控。 - 前台顯示：在「系統管理 / 領域資訊」 中顯示「TopN 報表數」欄位，提供用戶清楚掌握報表數量。 此次更新提升了資源使用透明度與管理效率，確保 TopN 報表的效能與可控性。
[自動聯防] 阻擋或執行失敗通知	自動執行腳本信件通報內容添加執行結果。
[TopN] 優化查詢排序功能	優化「TopN 查詢排序與流量分佈圖」功能： - 查詢時可指定排序數值，系統依選擇輸出 TopN 結果。 - 同步產生該排序依據的流量分佈圖，直觀呈現資料分布。

[Action] 效能改善	聯防效能改善：自動執行腳本若進行阻擋類行為，改為呼叫底層另一支程式負責，並且有執行筆數上限，以提高效能。
[設備] 介面過濾優化	事件、Top N、分時監控報表等功能頁面，過濾查詢加入介面編號顯示，以提升資訊呈現的完整性。
[情資比對] 功能優化	提高情資比對FQDN上限筆數到30萬。
[SNMP] 功能優化	SNMP Polling 得到的資訊：磁碟描述、介面描述(包含 Alias、名稱)與介面卡欄位，能顯示中文。
[分時告警] 效能優化	改善分時告警的延遲週期情形，優化分時告警效能。

■ 注意事項

- 在維護合約時效內，提供免費的韌體(Firmware)更新服務。
- N-Reporter 系統，將於此版本更新後，自動重新開機。並於開機後，重新啟動所有新的服務功能。
- 本產品已全面停止支援 IE 瀏覽器。為確保各項功能正常運作，請使用最新版 Chrome、Edge 或 Firefox。由於系統針對 Chromium 核心進行最佳化，建議優先使用 Chrome 或 Edge 瀏覽器，以享有最流暢的產品體驗。
- 此版本建議使用於 N-Partner Kernel 20260514091823 或之後的版本，以確保功能使用正常。

  若無使用BGP及SMB備份功能或是弱點掃描的需求，可暫不更新。若要進行kernel更新，請先判斷 eth0 MAC 需「小於」eth1 MAC，若遇到「大於」的狀況時，請聯繫TAC協助更新並重新申請License。

  欲檢查 kernel 版本，請於CLI中執行 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升級的詳細步驟，請參考「如何更新 N-Cloud / N-Reporter Firmware 與 Kernel」文件中的第5章「如何更新 Kernel」。
- 建議使用 NFS/SMB/FTP 定期備份 ，以避免因設備異常導致資料遺失。

■ 7.0.X 版升至 7.0.04X 版的更新方式

升級作業請依版本相容性順序執行：當目標版本為 7.0.04X 時，請分別下載 7.0.028 (下載) 與 7.0.04X (下載) 版本之Firmware，並先完成 7.0.028 版本的升級作業；確認系統已成功更新至 7.0.028 後，方可進一步升級至 7.0.04X 版。

使用者可透過 N-Reporter/N-Cloud 7.X 所提供之 UI 介面，進行 Firmware 與 Kernel 更新，請先以具備後台管理權限之帳號登入系統，並依下列方式完成更新作業。

- Firmware 更新
  - 線上更新
    - ✓ N-Reporter/N-Cloud 支援線上更新。
    - ✓ 請確定 N-Reporter/N-Cloud 可以連線到網際網路，且至少已設定一個 DNS Server。
    - ✓ 於「系統管理」頁面中，點選「系統更新」按鈕即可進行更新。
  - 離線更新
    - ✓ N-Reporter/N-Cloud 7.X 亦支援透過離線方式進行升級。
    - ✓ 於「系統管理」頁面中， 點選「上傳軟體更新檔」按鈕，選擇已下載的 ncloud-7.x.xxx.img 檔案，並點選 「匯入」 按鈕，即可開始上傳並執行更新。
- Kernel 更新

  請先下載7.0.X最新版 Kernel (下載)檔案，並完成後續更新作業。
  - N-Reporter/N-Cloud更新 Kernel

    於「系統管理」頁面中，點選下方「設備」，再切換至「Kernel 更新」 頁籤。點擊「排程更新」按鈕，

開啟「Kernel 更新」視窗後，選擇「手動上傳」，即可上傳 Kernel 檔案並執行更新。詳細步驟請參考「如何更新 N-Cloud / N-Reporter Firmware 與 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，請參閱文件「如何更新 N-Cloud / N-Reporter Firmware 與 Kernel」第2章，進行更新。

若您目前使用 6.1.18X 之後的版本，可參閱上述文件第3章，先更新至 6.X 最新版，再更新至 7.X 版，請依照下列步驟進行更新：

- Firmware 與 Kernel 更新

1. 下載最新6.1.18X版本 Firmware 檔案(下載)
2. 請以後台管理權限的帳號登入系統
3. 上傳檔案：於「系統管理」頁面點選「上傳軟體更新檔」，選擇第1步驟所下載的 ncloud-6.1.18x.img 檔案，並點擊「匯入」 按鈕開始上傳。請稍後約三分鐘，即可完成 Firmware 更新。
4. 升級至7版前，請先確認CPU型號；若CPU型號為E3 v3，則不建議升級至7版，請先聯繫您所購買之 N-Partner 產品經銷商/代理商，或聯繫本公司業務部門。
5. 若 CPU 非 E3 v3 型號，請參考上一小節「7.0.X 版升至 7.0.04X 版的更新方式」，繼續進行後續步驟。
6. 若您已更新至 6.X 最新版本，且暫不升級至7版，請完成 Kernel 更新，詳細步驟請參考「如何更新 N-Cloud / N-Reporter Firmware 與 Kernel」文件中第5章「如何更新 Kernel」。

註：6 版升級至 7 版前，請先以 CLI 指令 show hardware cpu 檢查 CPU 型號。

```
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#
```

上圖例 CPU 為 E3 v3 的型號，若有相關疑問，請聯繫經銷商/代理商，或洽詢本公司業務部門(sales@npartner.com)。

■ SNMP支援列表

► 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支援列表

► 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

■ 聯防支援列表—下達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)

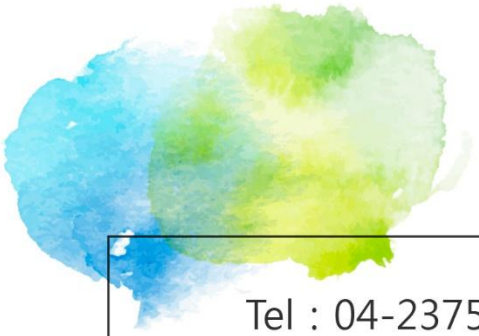
- ► **SNMP**
  - ✓ Aruba Controller、Aruba Controller 8.0
  - ✓ CheckPoint
  - ✓ F5 Networks
  - ✓ Fortigate
  - ✓ Paloalto
  - ✓ Ruckus AP
  - ✓ ZyXEL USG

■ 聯防支援列表—黑名單阻擋設備

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

技術文件下載

文件下載請至 http://www.npartner.com/



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