N-Cloud 6.0
DATA SHEET

Next Generation IT Operation Platform

Integrate Network Management, Flow Analysis and Log Reporting

2020/03/26

N-Cloud 是一個全新的 Log 分析管理平台中心，可應用於政府行政單位、大 型企業、跨國企業、教育市網中心、電信加值雲端服務單位等機構。針對有 Log 管理需求者，N-Cloud 提供了統一的服務平台，管理者可輕鬆的對企業內所有 Log 進行有效保存與分析應用，落實 Log 資料管理，並且透過快速整合 判斷，協助強化網路資安問題，同時滿足個資法規與產業需求。

N-Cloud 同時引入階層式的分權管理概念，可以分別為企業內的每個分公司 或部門建立單位群組，群組內的成員僅能看到所管轄的資料，因此，每個單 位群組，就像擁有獨立的 Log 管理平台；而總公司的管理人員則以全域角度 (Global) 查看全公司的 Log，隨時掌握全網的資安狀況。

■ 軟體功能

- 不分廠牌和設備，支援各式 Syslog 資料的蒐集。
- 提供系統狀態查詢，使用者可以查詢運行版號、CPU 使用率、記憶體使用率、Syslog / Flow 資料接受量。
- 提供 Flow 收集的能力，如 Netflow v5/v9/v10、sFlow、 Jflow、IPFIX 等。
- 支援中文 Web(HTTP/HTTPS) 操作介面，使用者權限可依使用需求調整。
- 提 供 CLI (Command Line Interface)， 可 透過 Console 或 SSH 連線進行系統操作。
- 支援 IPv6 環境，同時也適用於 IPv4 與 IPv6 雙軌運行的環境。
- 支援 SNMP v1/v2c/v3 監控網路設備，系統可呈現出特定內網 IP 所在的 Switch 位置。
- 支援繪製設備樹狀圖，能將設備按照從屬關係排列成根目錄、子目錄關聯順序，並可以收合展開。當設備出現異常時上層目錄夾也會同步顯示異常燈號。
- 支 援 採 用 SNMP 監 控 設 備 狀 態， 包 括 CPU/Memory 使用率、介面流量訊息、ICMP 等，並可以設定告警值及送出告警。
- 監控設備的 CPU、Memory 使用量圖形支援 Drill Down 點擊功能，Drill Down 後轉跳 TopN 報表關聯 Syslog/Flow，自動排出用量排行。
- 並且監控功能支援自訂 OID/MIB，監控所需項目狀態。
- 支援繪製拓樸圖，圖形自動繪製並以顏色呈現介面負載。
- 可輸入多筆查詢條件進行邏輯運算 (or/not)，條件包括事件關鍵字、IP、嚴重等級等各項參數，輸入條件數無限制。
- 提供 IP 網段名稱解析對應功能，在事件及報表中呈現 IP 及網段名稱
- 提供 Port 名稱解析功能，管理者可以自行定義Port 的名稱對應 (如：Port 80 等於 Http)。
- 內建 Flow 分析與統計功能，能自動繪製流量 (Packet/Byte) 並產生用量 Top N 表。
- 具備 Flow 異常流量智能分析功能，即時分析異常流量 (DDoS、Host Scan、Port Scan 等)。
- 系統可下達阻擋特定 IP 指令到網路與資安設備進行聯防 (註：非所有設備都支援此項功能)。
- 系統提供自動阻擋的聯防機置，可自行定義自動聯防的條件。
- 根據 Syslog/Flow 歷史用量自動學習建立 Base Line，能即時分析出發生異常突增的事件或 IP，並送出告警。
- 支援報表 Drill Down 深入查閱行為。
- 內建圓餅、長條、曲線圖等多種圖型式樣，可依需求客製化報表。
- 提供流量圖形呈現 Max/Avg/PCT 95 數值。
- 可以自行訂製事件呈現的欄位和事件 PDF 輸出的欄位。
- 支援製作中文報表，中文 PDF 的輸出。
- 自訂 PDF 輸出的 LOGO 和版面。
- 提供 Windows AD 解析功能，可以將事件的 IP 解析出使用者名稱。
- 支援各類主機的使用者登入登出的稽核日誌報表：Linux、Windows server 2003 / 2008 / 2012 / 2016 等。
- 提供異常登入行為偵測與告警。
- 支援各類資料庫的使用者登入登出的稽核日誌報表：Oracle、MSSQL、MySQL 等。
- 支援 Windows 檔案分享的稽核日誌報表。
- 支援資料庫備份與回復功能。
- 提供資料庫儲存天數預測功能。
- 支援 Syslog 原始的 Raw data 備份。
- 提供使用者自定動態 Dashboard，即時呈現告警現況及事件統計等資訊。

- 支援 Access Control List，限制可執行管理的 IP 白名單。
- 完整的記錄使用者操作歷程，並提供 PDF 格式的輸出。
- 提供 Open Interface，使用者可通透 Open Interface 取得事件資訊。
- 彈性的告警通報設定，可以依不同的報表或告警種類指定不同的郵件群組。
- 獨創最新壓縮的儲存技術，使用符合國際公認推薦密碼模組 FIPS 140-2 SHA-256 和 DES-256 的加密原則，確保資料的完整性和不可否認性，其壓縮比高達 10 倍，大幅度提升儲存空間利用率。
- 提供 CPU、風扇和硬碟狀態監控，主動通知管理者異常告警。
- 支援 SNMP Trap，硬體異常可以即時告警。
- 支援高可用度 (HA) 架構，確保系統運作不中斷。
- 內建事件模組，使用者可隨時查詢 Syslog、Flow 的事件內容明細。
- 內建 Top N 模組，使用者可隨時訂製、查詢 Top N的排行。
- 內建監控報表，使用者可以依據不同條件，訂製自己的監控條件，當異常發生時則立即通知管理者。
- 階層式管理，各自獨立運作，各自擁有獨立的 Reporting 分析功能
- 離線報表支援群組化功能。
- 支援多樣的即時輸出格式：PDF、XML、CSV 等。

階層分權管理機制

N-Cloud 的階層式管理，滿足了企業分權管理的需求。例如，可以將管理階層群組定義如下：總公司、分公司、分公司的部門等 (如圖1 所示)。台中分公司所管轄的設備，其他分公司的管理者是無權查看的，但總公司的管理者，則擁有查閱分公司設備訊息的權限。N-Cloud 的階層式管理提供了靈活的階層管理架構，可滿足大型企業管理需求。

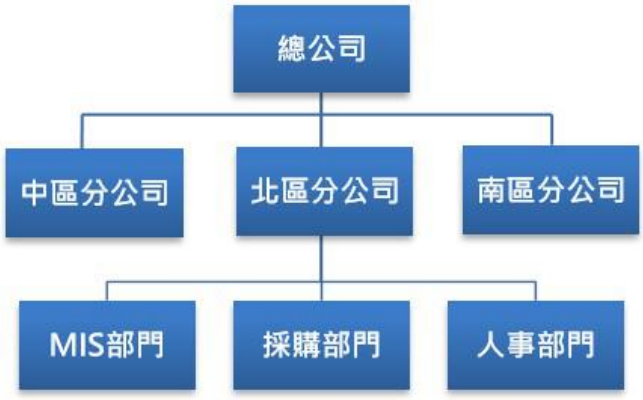


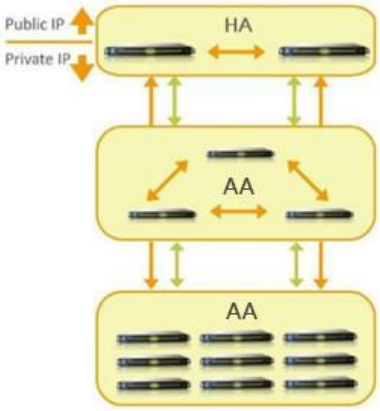
圖 1

各種資料的集中管理中心

N-Cloud 支援橫跨網路 (Router、Switch)、資安 (Firewall、 IDP/IPS、Web Cache Appliance、WAF、UTM)、伺服器、資料庫、大型主機等設備的Syslog 資料收集。N-Cloud可蒐集分析不同廠牌或設備的Syslog及不同格式的流量資訊，如 Netflow、jFlow、sFlow 等。系統會將所有的資料做關聯分析，供管理者平行比對，輕鬆查看全網的資安危機分析、Top N 排行、稽核報表、流量管理、歷史趨勢分析、即時阻擋異常攻擊等資訊。

支援高可用度 (HA) 架構

搭配 N-Cloud 專屬的 N-LB (Load Balancer)，可達成多部 N-Center/N-Receiver 互為備援 (如圖 2所示)，提供 24 小時不中斷的資料收取保證，為企業提供符合個資法規的最佳工具。



N-Load Balancer
提供負載平衡和主機異常偵測。

N-Center
提供客戶報表及資料分析服務。

N-Receiver
提供資料收集儲存和運算。

圖 2

靈活彈性的 N-Cloud 架構

N-Cloud 在建構時有三個主要元件：

(一) N-Load Balancer：

負責負載平衡及主機狀態偵測。

(二) N-Center：

負責處理使用者的查詢工作及資料交叉分析。

(三) N-Receiver：

負責分析 Log 資料。此架構具備高度擴展性，可以依據使用者需求，因應未來資料量與使用者個數的成長預估，進行適當的調配，不用擔心當收容的資料大幅增加時，會發生無法擴充的問題。

建置中大型的 N-Cloud 服務平台，即可提供數百個使用者同時上線及查詢，並允許建立上千個領域。依教育市網中心為例，市網中心建置一 N-Cloud 服務平台，即可同時提供數百所中學使用N-Cloud 服務，而不需要親自至各所學校進行 Log 服務建置的動作。由於所有中學都使用相同的服務平台，因此在問題的交流與溝通上，亦彰顯得簡單和清楚。

可依客戶需求規劃

- 支援多人線上使用者，可達百人以上
- 支援 Log 使用單位群組，可達上千個單位
- Syslog 接收能力高達 100,000EPS 以上
- Flow 接收能力高達 100,000EPS 以上
- 可同時蒐集 1000 部以上的 Syslog 設備
- 可依需求，規劃儲存資料的筆數和資料保存時間
- 可自 N-Reporter 6.0 升級架構為 N-Cloud 6.0

同時輸入多筆查詢條件 進行邏輯運算與製作報表

在維運的歷程中，資料查詢是占系統大部份的執行時間。當接收的 Syslog/Flow Data 越來越多時，能夠支援彈性的搜尋條件輸入與快速的查詢結果呈現是使用者對報表工具的基本要求。

N-Cloud 提供智慧型的查詢功能，搭配邏輯運算概念能夠讓使用者完成各式各樣要求下的查詢工作。

事件呈現及可輸入的參數選項

- 根據 Syslog 查詢或是根據 Flow 查詢
- 設備
- 設備的介面
- 時間
- 事件關鍵字
- 使用者名稱
- 來源 / 目的 IP(支援 CIDR 與不連續區段)
- 來源 / 目的 Port
- 來源 / 目的國家
- Packet/Byte 大小
- 事件嚴重等級
- 事件處置動作 (Block、Permit 等)
- Packet/Byte 用量大小
- Policy ID
- AS Number

所謂的邏輯運算指的是多個查詢條件間以聯集 (Or) 和排除 (Not) 概念所建立的關聯性結果。舉例來說：若要查詢多個事件關鍵字，可以在輸入關鍵字之間用聯集 (Or)；若是希望排除某些特定的關鍵字不要呈現於報表之中，則使用排除 (Not) 指令。

N-Cloud 不僅支援「事件關鍵字」的邏輯運算，使用者亦可針對「IP」選項進行邏輯運算，或是同時進行跨不同選項間的邏輯運算。以下說明幾個操作範例。

Event Keyword

P2P+Streaming:

表示欲同時查找含有 P2P 或是 Streaming 關鍵字的所有事件。

P2P+Streaming!BT:

表示欲同時查找含有 P2P 或是 Streaming 關鍵字的所有事件，但是需要排除 BT。

[IP]

192.168.1.0/24+192.168.2.0/24

表示欲同時查找這兩個網段的所有事件。

192.168.1.0/24+

192.168.2.0/24!192.168.1.100-200

表示欲同時查找這兩個網段的所有事件，但是過濾掉 192.168.1.100-200 這個區段的事件。

事件搜尋條件可以依據實際需求輸入多筆條件，N-Partner《Smart DB》同樣給予 N-Cloud 快速查詢事件的能力，讓邏輯運算機制不會因執行大量條件比對而延遲搜尋結果的呈現。

Flow模組進行流量分析

Flow (如：Netflow/sFlow) 資料在網管工作中經常扮演用量分析的重要角色，IT 管理者藉由 Flow 資料了解哪個 IP 或是哪個 組織單位用量最多；哪種 Protocol (ex：Port 80、Port 21) 佔去最多的頻寬資源等訊息。

Flow 模組可滿足上述 IT 管理者對於 Flow 分析的需求，諸如： 用量 Top N 分析與 Drill Down 進階查詢；針對特定對象長期繪 製流量圖；查詢特定 IP 或是組織單位的流量使用紀錄等。

Flow 模組除了支援 Netflow v5/v9；sFlow v4/v5；J-Flow 等格式之外，亦可擴充運用於沒有 Flow 設備但有防火牆建置的環境中。由於大多數的防火牆都支援 Syslog功能，可將流經的網路連線訊息封裝成 Syslog Data 後輸出，因此企業也可以利用防火牆的 Syslog 資訊進行流量的分析。

豐富多樣的即時線上報表

N-Cloud 的即時線上報表系統支援動態顯示報表內容與統計圖型。使用者可依據喜好選擇適合的圖型樣式，包括：圓餅圖、長條圖、曲線圖等。報表功能同樣支援邏輯運算概念 (Or/Not)，使用者可根據各種實際的狀況邏輯結合多個過濾參數，讓報表產生的結果更貼近使用者的真實所需。例如：伺服器遭受嚴重攻擊事件日報表；員工使用社群網站與串流影音的流量周報表；資料庫存取記錄月統計等。

自訂分時報表，並提供異常監控功能

管理者可使用過濾條件來定義各式的分時報表，方便長期觀 察事件或是流量的變化。透過關鍵字的設定，可觀察特定事件的 分時變化；例如監看「Telnet/SSH Login Fail」數量來偵測是否 有帳密猜測、監看半夜連線某主機次數及流量來偵測是否異常、「Port 445」連線及流量監控來偵測是否感染蠕蟲等。 分時報表 同時也支援門檻值 (Threshold) 的設定。如此只要事件次數暴增， 或者發生流量異常時，系統將主動寄發告警郵件通知管理者。

加裝 Flow 模組的分時報表，可以在同一個分時報表畫面裡， 同步繪製事件、bps、pps 和 session 的曲線圖方便使用者進行交叉比對分析。

離線報表定期寄送

定期自動產生統計報表讓使用者無需每日手動執行報表製作與輸出的工作。N-Cloud 將根據報表儲存功能中使用者所定義的報表製作參數，寄送統計報表到指定的電子郵件帳號。

報表製作參數包括

- 事件等級
- 工作時段 (每日工時區間)
- 工作日 (星期日至星期六的選項)
- 報表型態 (時報、日報、週報、半月報、月報、季報、半年報 與年報)
- 定期寄送時間
- 指定的報表收件者
- 報表格式 (HTML、PDF、 XML、CSV)

支援SNMP監控設備

透過 SNMP 監控，可以定期取得設備的 CPU 、M emory 和介面流量資訊，並且提供清晰圖示供管理者查看。此外，也可以讓管理者自行設定監控的門檻值。例如在 CPU / M emory 上升至 80% 或介面流量超大時，觸發告警且透過郵件通知管理者。

使用樹狀圖，依階層式的方式，呈現 SNMP 設備管理的狀況。並且提供圖示，讓管理者清楚知道設備目前的

情況。例如 : 設備異常，會有紅火警示，且上層同時也會有驚嘆號圖示告訴管理者，在管理的區域下有設備異常。

內建人工智慧，根據歷史紀錄自動產出趨勢分析報表

N-Cloud 內建的人工智慧科技能根據蒐集到的Syslog/Flow 歷史資料自動找出發生次數、Packet 數或Byte 數異常突增的事件或 IP，並將發生異常突增的內容主動寄發通知郵件給 IT 管理者以利於第一時間處置網路中的的異常狀況。藉由 Behavior Based 偵測與分析功能，使用者無需猜測與預設合理的門檻值，即可充分掌握網路環境裡值得注意的變化，讓維運工作顯得更輕鬆容易。

N-Cloud 不僅是功能強大的事件查詢與報表製作系統，更是一部能真正做到趨勢分析的 Analyzer。

Action 模組執行聯合防禦

使用者可以運用這些有用的分析結果進行更進階的管理處置作為。透過 Action 模組，IT 管理者就能夠視影響網路的嚴重程 度準確地執行更進一步的管制作為 (通常是阻擋這個 IP 繼續連網)，讓網路立即恢復正常運作。

N-Cloud Action 模組，能允許使用者直接在 Web 管理介面上下達 IP 封鎖指令，可將 IP 封鎖指令下達至位於Internet 入口處的網路或是資安設備 (註：非所有廠牌均支援)，進行第一時間的防禦。

符合稽核規範

使用符合國際公認推薦密碼模組 SHA-256 和 DES-256 的加密原則，確保資料的完整性和不可否認性。

https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=3002

■ 硬體功能

N-Loadbalance

- Intel CPU Xeon E3-1230 v6 L2-8M 3.5GHz series processor
- Intel C224 chipset
- 4x 3.5" Hot-swap SATA3 drive bays
- 16GB RAM DDR4 (supports to 64GB DDR4 ECC 2400MHz UDIMMs in 4 sockets)
- 1 PCI-E 3.0 x8 (in x16), 1 PCI-E 3.0 x8, and 1 PCI-E 2.0 x4 (in x8) slots
- Dual Gigabit Ethernet LAN ports (2 Intel® i210AT)
- Integrated IPMI 2.0 and KVM with Dedicated LAN
- I/O ports: 1x VGA, 2x COM(1 rear, 1 header), 6x USB 2.0
- 350W Gold Level Power Supply
- 4GB SATA DOM
- 100v-240v, 50-60Hz AC power, Operating Temperature: 0° C-50° C (32° F-122° F), Operating Relative Humidity: 8% to 90% (non-condensing)

N-Receiver

- Intel CPU Xeon E3-1230 v6 L2-8M 3.5GHz series processor
- Intel C224 chipset
- 4x 3.5" Hot-swap SATA3 drive bays
- 32GB RAM DDR4 (supports to 64GB DDR4 ECC 2400MHz UDIMMs in 4 sockets)
- 1 PCI-E 3.0 x8 (in x16), 1 PCI-E 3.0 x8, and 1 PCI-E 2.0 x4 (in x8) slots
- Dual Gigabit Ethernet LAN ports (2 Intel® i210AT)
- Integrated IPMI 2.0 and KVM with Dedicated LAN
- I/O ports: 1x VGA, 2x COM(1 rear, 1 header), 6x USB 2.0
- 350W Gold Level Power Supply
- 4GB SATA DOM
- 12TB HDD (4x4T with RAID5)

- RAID module(optional) support levels 0, 1 and 5, up to 12T storage space
- 100v-240v, 50-60Hz AC power, Operating Temperature: 0° C-50° C (32° F-122° F), Operating Relative Humidity: 8% to 90% (non-condensing)

N-Center

- Intel CPU Xeon E3-1230 v6 L2-8M 3.5GHz series processor
- Intel C224 chipset
- 4x 3.5" Hot-swap SATA3 drive bays
- 32GB RAM DDR4 (supports to 64GB DDR4 ECC 2400MHz UDIMMs in 4 sockets)
- 1 PCI-E 3.0 x8 (in x16), 1 PCI-E 3.0 x8, and 1 PCI-E 2.0 x4 (in x8) slots
- Dual Gigabit Ethernet LAN ports (2 Intel® i210AT)
- Integrated IPMI 2.0 and KVM with Dedicated LAN
- I/O ports: 1x VGA, 2x COM(1 rear, 1 header), 6x USB 2.0
- 350W Gold Level Power Supply
- 4GB SATA DOM
- 8TB HDD (3x4T with RAID5)
- RAID module(optional) support levels 0, 1 and 5, up to 12T storage space
- 100v-240v, 50-60Hz AC power, Operating Temperature: 0° C-50° C (32° F-122° F), Operating Relative Humidity: 8% to 90% (non-condensing)

產品料號	料號說明
NP-CLD-BALANCER-VM-TW	N-Balancer VM version. Do load balancing for N-Receiver and N-Center. Include 1 year MA.
NP-CLD-RECEIVER-VM-TW	N-Receiver VM version. Data receiver. Include 1 year MA.
NP-CLD-CENTER-VM-TW	N-Center VM version. Provide portal, reporting and analysis result. Include 20 domains license (max 120). Include 100 SNMP devices (max 1000) and 1 year MA.
NP-CLD-BALANCER-TW	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-TW	N-Receiver platform. Data receiver. Support up to 10,000 EPS. 4T HDD*4. Include 1 year MA.
NP-CLD-RECEIVER-H-TW	2U N-Receiver platform. Data receiver. Support up to 20,000 EPS. 14T HDD*4. Include 1 year MA.
NP-CLD-CENTER-TW	N-Center plarform. Provide portal, reporting and analysis result. Include 20 domains license (max 120). Include 100 SNMP devices (max 1000) and 1 year MA.
NP-CLD-E-REC-TW	External-Receiver platform. Collect and forward data. Include 1 year MA.
NP-CLD-VM-E-REC-TW	External-Receiver VM version. Collect and forward data. Include 1 year MA.

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