

# N-CLOUD

## DATA SHEET

new log analysis and log management tool

---



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、電信增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 Flow 收集的能力，如 Netflow V5；Netflow V9、sFlow、Jflow、IPFIX 等。
- ▶ 支援 IPv6 的 Syslog 資料分析，IPv6 流量分析。
- ▶ 支援 SNMP 設備的監控。
- ▶ 階層式管理，各自獨立運作，各自擁有獨立的 Reporting 分析功能。
- ▶ 支援中文 Web 操作介面，使用者權限可分為管理者與一般使用者。
- ▶ 支援製作中文報表，中文 PDF 的輸出。
- ▶ 可以自行訂製事件呈現的欄位和事件 PDF 輸出的欄位。
- ▶ 自訂 PDF 輸出的 LOGO 和版面。
- ▶ 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 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。
- ▶ 內建 Offline 模組，使用者可以自行訂製離線報表 (Daily、Weekly、Monthly Report)。
- ▶ 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。
- ▶ 提供名稱解析功能，管理者可以自行定義網段名稱對應 (如：192.168.1.0/24 等於人事部門)。
- ▶ 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 Web)。
- ▶ 支援多樣的即時輸出格式：PDF、XML、CSV 等。
- ▶ 告警通報設定模組，管理者可以設定不同的 E-Mail 群組，針對不同的告警發生，各自寄送到不同的 E-Mail 群組。
- ▶ 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。
- ▶ 提供資料壓縮技術，其壓縮比高達 8 倍，大幅度提升儲存空間利用率。
- ▶ 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 SHA-256 和 DES-256 的加密原則，確保資料的完整性和不可否認性。
- ▶ 支援高可用度 (HA) 架構，確保系統運作不中斷。
- ▶ 提供 CLI (Command Line Interface)，可透過 Console 或 SSH 連線進行系統操作。

## 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 接收能力最高達 100,000EPS 以上
- ▶ Flow 接收能力最高達 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
- ▶ 內建 Action 模組，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)

## 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。不分廠牌或設備的 Syslog，N-Cloud 均可蒐集分析，並且還可同時接收 Netflow、jFlow、sFlow 等流量資訊。管理者可以將所有的資料，進行平行比對，輕鬆查看全網的資安危機分析、Top N 排行、稽核查詢報表、流量管理、歷史趨勢分析、即時阻擋異常攻擊等資訊。

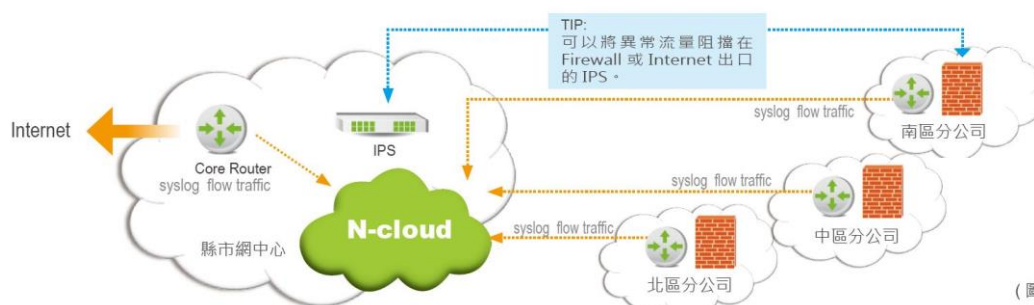
## 靈活彈性的 N-Cloud 架構

N-Cloud 在建構時有兩個主要元件：

(一) **N-Center**：負責處理使用者的查詢工作及資料交叉分析。

(二) **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。

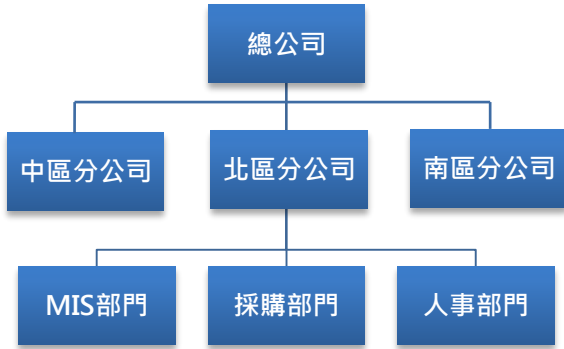
建置中大型的 N-Cloud 服務平台，即可提供數百個使用者同時上線及查詢，並允許建立上千個領域。依教育市網中心為例 (如圖 1 所示)，市網中心建置一 N-Cloud 服務平台，即可同時提供數百所中學使用 N-Cloud 服務，而不需要親自至各所學校進行 Log 服務建置的動作。由於所有中學都使用相同的服務平台，因此在問題的交流與溝通上，亦彰顯得簡單和清楚。



(圖 1)

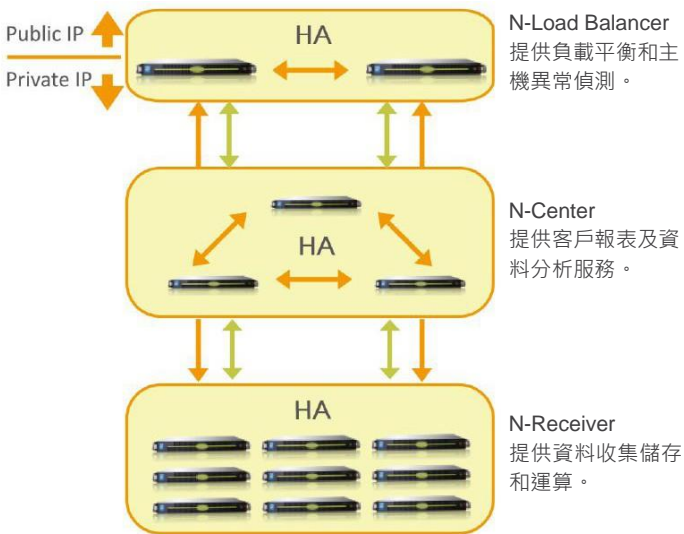
## 階層分權管理機制

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 2 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。



## 支援高可用性 (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 3 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。



## 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。

## 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)
- ▶ Policy ID
- ▶ Session ID

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。

## 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-Reporter 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 (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、Memory 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 / Memory 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。



▲ SNMP 監控設備

## 內建人工智慧，根據歷史紀錄

### 自動產出趨勢分析報表

N-Reporter 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-Reporter 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。

<http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html#2416>  
<http://csrc.nist.gov/groups/STM/cavp/documents/shs/shaval.htm#2073>



採購與銷售合作：[sales@npartnertech.com](mailto:sales@npartnertech.com)

技術諮詢：[support@npartnertech.com](mailto:support@npartnertech.com)

TEL: +886-4-23752865

FAX: +886-4-23757458