六、大數據日誌儲存模組

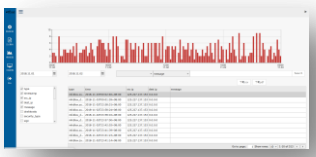
日誌大數據

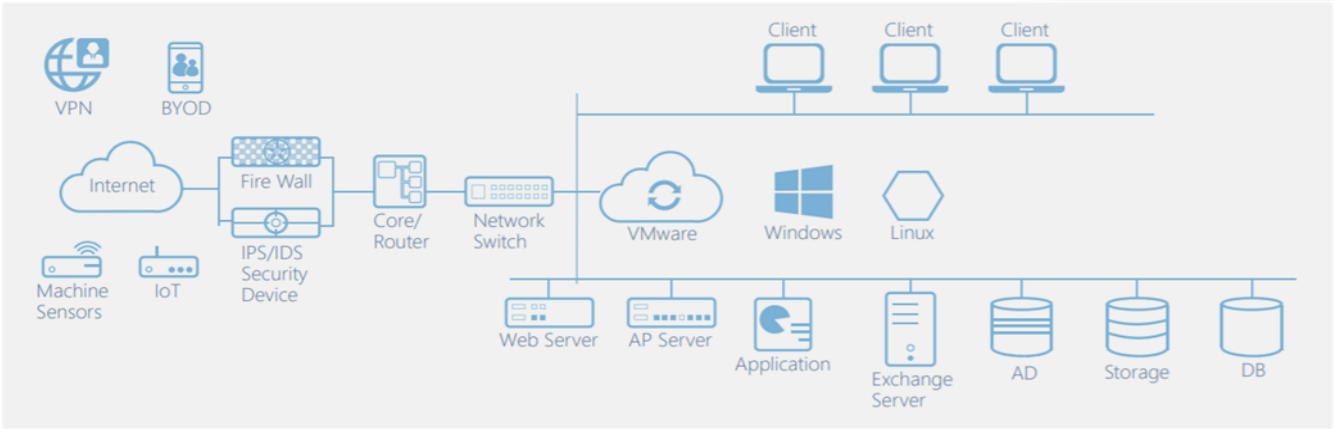
大數據運作第一步是進行數據格式的定義，智能型核心引擎內建NoSQL DB支援無格式數據日誌與網管數據儲存與查詢、MyReport 自定義查詢報表，是運行邊緣運算/大數據/機器學習整合智能維運不可或缺元素。

日誌儲存系統

配合系統與網路設備訊息格式定義，巨量格式化日誌儲存，LOGinsight授權包括：

- **日誌大數據** – syslog 大數據儲存, 延展性, 容錯設計
- **格式定義** –大數據運作第一步是進行數據格式的定義，系統內建支援無格式數據日誌與網管數據儲存與查詢、MyReport 自定義查詢報表。
- **日誌查詢** – 可選擇時間點如最近4小時或自訂義日期時間，另外亦可選擇條件欄位然後設定operator(包含, > < >= <=) 及符合的值進行查詢。
- **不可否認性** – 日誌儲存
- **報表視圖管理** – 趨勢圖, 統計分析圖, 營運報告





全方位的設備裝置支援

支援各種網路設備、安全性裝置及異質性平台的不同日誌記錄來源管理，包括：路由器／交換器、無線網路、防火牆、虛擬私有網路(VPN)、入侵偵測/防護系統(IDS/IPS)等網路設備日誌，Windows / Linux/Unix主機作業系統日誌及AD登入日誌，防毒應用程式、MS-SQL/ Oracle / MySQL資料庫、郵件app.及網頁應用程式。自訂格式與報表，簡化跨不同安全性及整體網路裝置的搜尋、資料關聯與分析報告，並可升級整合企業版本其他網路資安設備進行聯合防禦，提供手動及自動阻擋機制迅速隔離資安問題，協助IT 營運安全管理。

軟體定義資料格式及統計分析

雖然軟體以本文方式接收的系統或網路設備的原始日誌, 這些日誌可以原始方式儲存, 之外也仍然可加以定義, 以欄位的概念儲存。有了這些切割的欄位資訊, 系統即可以依據欄位進行排序與聚合產生管理員所期待的統計或分析的資訊, 甚至製作成視圖或報表, 使得這些日誌變成可供參考之可用資訊。

MyReport是系統提供的有用工具, 讓管理員可自行依據需求將原始資料客製化成統計分析之報表或視圖(chart), 它的過程包括: 數據來源定義、過濾條件定義、欄位選擇、統計運算、輸出定義。

大數據儲存, 延展性, 容錯設計

系統具備叢集佈署能力, 得以Active-Active獨立運作與異地備援支援整體系統的高可用性。各自的獨立系統亦具備延展性, 容錯管理設計, 可橫向擴展疊加硬體比例提升整體系統效能, 並具備N+1高可用性之容錯設計, 管理員可因為實體硬體的疊加同時提高系統運作的可用性。系統內建NoSQL資料庫自動化的記錄蒐集、儲存網路及系統設備等日誌, 可同時以傳統關聯式欄位的概念及全文關鍵字檢索複合方式, 快速與有效查詢與聚合儲存數據進行統計與分析。

不可否認性法規遵循

系統支援 Syslog 原始的 Raw Data 儲存及加密不可否認性之管理, SHA-1 雜湊演算法，每小時可產生數位簽章PKCS7 方式封裝, 自動蒐集分類、聚合、正規化、關聯分析、歸檔保存、稽核報表，符合法規要 求如：PCI DSS 3.0 以及 HIPAA、HITECH、NIST 日誌管理標準，確保日誌資料保存的完整性 (Log file integrity checking) 以及不可竄改性，符合個人資料保護法應用, 輕鬆完成 ISO 27001 ISMS 管理作業，減少人力作業時間成本，符合安全管理與成本效益。 。