昕力資訊 企業級 Log 監控管理平台

digiLogs

digiLogs - 企業級 Log 監控管理平台

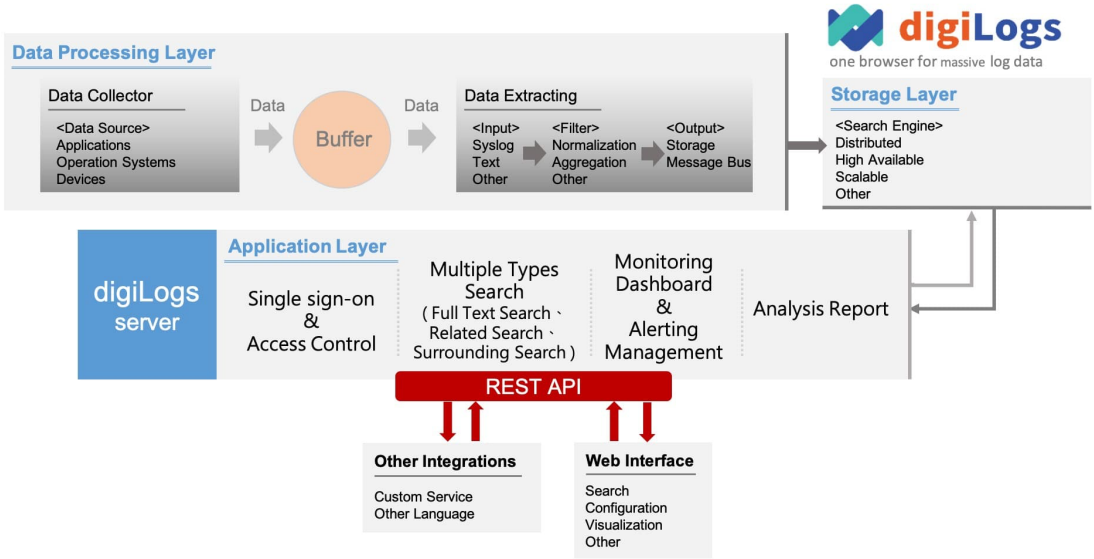
一個瀏覽器、管理海量 Log

- 一個瀏覽器，集中管理海量 Log，解決逐一尋找瑣碎 Log 訊息的不便
- 一次整合多台系統資料運作記錄，快速精確的查詢以了解系統問題來源
- 以冷資料技術儲存大量歷史 Log，節省硬體資源並提高運作效能
- 一目瞭然的視覺化多元分析統計報表可滿足企業管理需求

digiLogs 系統功能模組

- 登入整合: 整合企業 AD、LDAP、OAuth 及 SSO 等系統，降低使用阻礙
- 權限控管: 滿足企業權限管理需求，確保不同層級的使用權限
- Log 檢索: 動態欄位查詢、全文檢索與上下文關聯性查詢，Log 管理更容易
- 監控告警: 監控系統及 Log 實際運作狀況，並可於異常時即時進行告警通知
- 交易路徑: 瞭解 Log 在各系統別、交易別及主機的路徑分析及平均交易時間
- 分析報表: 各式 Log 數據統計分析報表，清晰呈現 Log 現況

digiLogs 系統架構



(1) 資料處理層
- 各設備透過 digiLogs 設置的資料收集器 (Agent) 傳送 Log 至資料緩衝區 (Buffer) 後，資料會依序被解析及聚合；再將資料以 document 的格式存放於 No-SQL 的 database。

(2) 資料儲存層
- 依不同業務單位各自定義資料集有效優化儲存空間之查詢效能。
- 為確保效能不受資料量影響，系統以「時間」為單位，將資料以不同的形式儲存。系統會自動將舊資料 (預設為 1 個月以上) 定義為「睡眠資料」，digiLogs 不會在內存中維護這些資料的數據結構，所以可以有效釋放系統資源，當「睡眠資料」有被查詢的需求，digiLogs 會將其重新激活，並可在一分鐘內提供服務；而歷史資料 (預設 6 個月以上) 將以「snapshot」的方式壓縮儲存於文件系統中，確保日誌儲存年限符合法規需求。

(3) 資料應用層
- 使用者可應用解析後的 Log，包含全文檢索、關鍵字查詢、報表分析、系統監控與即時告警，協助使用者了解 Log 狀況。
- digiLogs 同時也可監控系統健康狀況，包含預設與自定義項目，當超過系統閥值時，系統的預設機制會發動告警，通知相關人員，讓人員可以即時掌握系統狀況。

digiLogs 即時告警

1. 監控項目
   - 預設項目 (CPU High, Heap High, Disk High, DB Connection Fail)
   - 自訂關鍵字項目
2. 發送告警
   - 設定 Alert API 介接
   - 告警透過 Email, Line, SMS

digiLogs 支援多元解析格式

三層式架構：input、filter、output，每層都有相對應的 plugin 來使用

1. Input: 決定資料來源(file、mongo、http、...等)
   - 已支援 40 多種 input: eventLog、http、jdbc、Log4j、redis、kafka、cassandra、mongodb
2. filter: 用來對每一個 event 做一些進階處理(時間處理、字串擷取、...等)
   - 有許多 filter 可以組織解析器: aggregate、date、geoip、json、xml
   - 已有 40 多種預設 format 解析器: AIX、Log4j、eventLog、sysLog、snmp、jmx
3. output: 來決定最後要將 event 輸出至哪裡(console、Elasticsearch、...等)
   - 已支援 40 多種 output: csv、email、http、mongo、kafka、redis

昕力資訊 企業級 Log 監控管理平台

digiLogs

digiLogs 系統基本規格

作業系統：Linux (RedHat、CentOS 7.6+)、
Windows Server 2012+

容器軟體：Docker CE 18.06.1 +

語言環境：Open JDK 1.8

項目	Server	台數	CPU	RAM	HDD	Network
1	資料萃取 / Admin server	2	4 Core	32GB	100GB	1GBit
2	資料庫叢集	3	4 Core	32GB	依實際評估	1GBit