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

- 1 個瀏覽器，管理海量 Log　單一集中管理
- 全文檢索、關鍵字查詢 彈性搜尋查詢機制
- 可儲存大量歷史 Log　可匯出查詢
- 多元、客製化管理分析報表 充分符合企業管理需求

digiLogs 系統功能模組

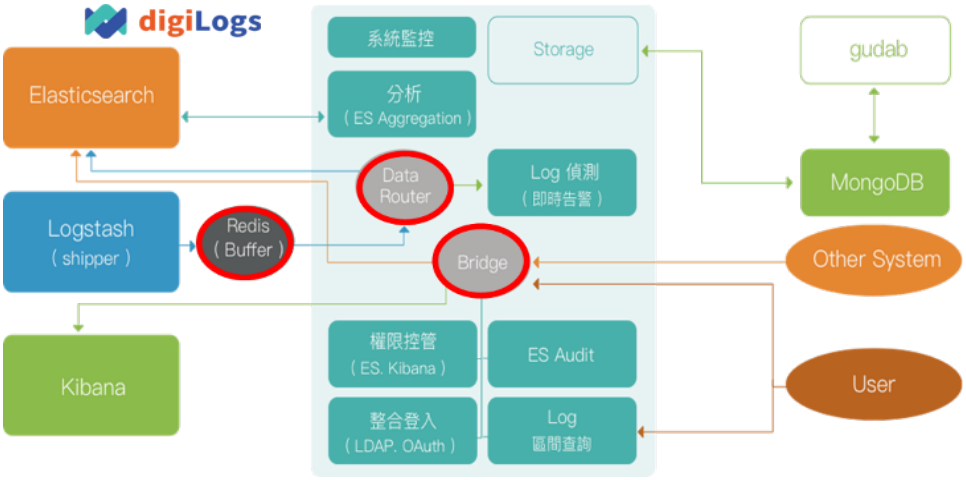
- 登入整合: LDAP, OAuth 等整合企業系統
- 權限控管: 整合企業權限管理需求
- Log 檢索: 全文檢索、彈性上下文關聯查詢
- 即時告警: Log 偵測第一時間進行告警
- 系統監控: 透過儀表板進行系統運行監控
- 分析報表: 各式統計分析報表

digiLogs 系統架構

1. 前端資料收集器透過 Logstash(shipper)傳送並解析 log 資料，digiLogs 會使用 Data Router 將資料存放於 Elasticsearch 上。
2. 使用者可以在 3-5 秒內看到 log 分析報表，包含全文檢索、關鍵字搜尋、使用報表分析、系統監控與即時告警，協助使用者了解 log 狀況。
3. 帳號管理預設為 Oauth 方式，系統也可結合現有認證機制，包含 AP/LDAP 等，藉以區分負責的管理人員，便於使用與設定。
4. 為確保效能不受資料量影響，系統會將歷史資料與交易資料區隔。存放於 Elasticsearch 上的資料，每日抄寫至 MongoDB 上，使用者可以在 ES 上查詢交易期間資料(預設為 1 個月)，超過交易時間資料，則於 MongoDB 上查詢。
5. 系統同時也監控健康狀況，包含預設與自定義項目，當超過系統閥值時，系統會發動告警機制，通知相關人員，確實掌握系統狀況。

昕力資訊 企業級 Log 監控管理平台

digiLogs



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
- input：決定資料來源(file、mongo、http、...等)
- filter：用來對每一個 event 做一些進階處理(時間處理、字串擷取、...等)
- output：來決定最後要將 event 輸出至哪裡(console、Elasticsearch、...等)
- 已支援 40 多種 input: eventlog、http、jdbc、log4j、redis、kafka
- 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: log4j、eventlog、syslog、snmp、jmx
- 已支援 40 多種 output: csv、email、http、mongo、kafka、redis

digiLogs 系統基本規格

作業系統：Linux (RedHat、CentOS 7.6+)、Windows 2016 Server+

容器(Docker)：18.06.1-ce+ (非必要)

CPU：4 核心以上

記憶體：16 GB 以上

磁碟空間：300 GB 以上