BIG DATA ENGINE

This Platform Realizes Data Visualization And Rapid Analysis.

HIGHLIGHTS

- 全方位整合環境資訊，提高企業效能。
- 即時發現並解決問題，降低時間及人力成本。
- 縱深視覺化資訊呈現，一手掌握全面訊息。
- 大數據歷史軌跡分析，風險判斷無往不利。
- 高彈性環境整合能力，效能、安全面面俱到。

簡單好用的分析系統

Twister5公司專注於網路行為及安全分析已有多年經驗，並同時專研於數據收集及分析系統的應用及優化，此次提供一套易於使用及導入的大數據分析引擎系統(BIG DATA ENGINE；BDE)，該系統具備簡易的操作環境，卻同時提供完整的視覺化呈現能力， 利於企業於日誌/事件的保存、稽核，資訊安全分析、潛在風險發掘及預防，並有效整合環境數據以帶來效能提供之價值。

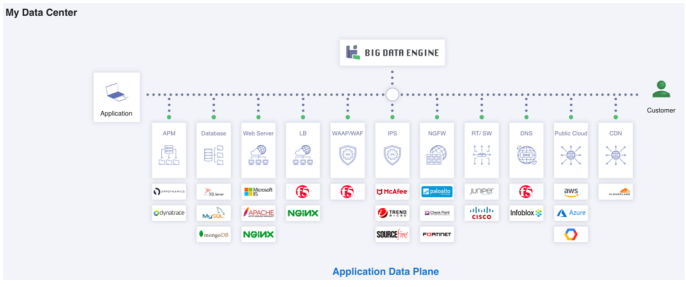
BDE主要收集數據來源基於環境設備及系統，訊息大致上分為網路日誌(Syslog)及系統事件訊息(Event) 。簡易的面向，大數據引擎(BDE)可以接收並讀取以上訊息，並加以整理同時即時呈現出來，所以使用者或管理人員可以即時的利用大數據引擎(BDE)得知目前資訊環境所面臨或遇到的事件，再由問題著手，如此便可大幅降低維運所消耗的時間，同時提升運維效益。

此外，提供中文管理介面更能貼近使用者的應用思維，用戶無需學習複雜且不友善的介面及邏輯，搭配淺顯易懂的說明，可達成安裝即上手之效益。

系統及環境維運分析

在資訊環境中，最容易發生的工作事項就是故障排除，而且通常終端用戶所提出來的問題都不具體或是方向性極為廣闊，如此一來都會造成維運人員的極大負擔，亦造成時間成本的大量流逝。然而，透過大數據引擎(BDE)，管理者或維運人員可以快速的從各項設備中取得所需要的資訊，再利用關聯式的資訊對應方式，找到問題源進行處理。所以當環境中的設備，已然將大量的日誌(Syslog)及事件(Event)發送給大數據引擎(BDE)時，管理者可以即時知到設備上的政策觸發以及系統的服務運作情況。

我們可以搭配日誌(Syslog)及事件(Event)的訊息，充份的提供相對應關聯的可能性，如此便能清楚的分析日誌及事件間的對應關係，亦能從時間軌跡的應用方式，來了解此狀態是否為常態或是非常態，管理者或維運人員將可利用此訊息判斷環境異常的來源點跟可能性原因，更將大幅縮短問提查找的時間消耗，以達到企業或環境維運的最佳效益。



資訊收集

大數據引擎(BDE)是一套專為大量數據資訊所產生的日誌管理解決方案，可收集各種型態的日誌，舉凡能成為文字格式的資料型態，皆能接收並加以解析，成立正規化資料庫以提供快速、準確及龐大的系統日誌呈現與追蹤，並統合各種日誌資料類型之搜尋、分析、警示與報表產製能力，快速產製異常行為稽核報告與法規遵循報告，可讓企業以高效能、低成本的方式達成日誌長期保存與資安符規之目標。

另外我們提供了非常容易閱讀的欄位格式介面，使用者或管理者可以直接將每項事件透過欄位解析後所呈現的值欄對應關係，一眼了解日誌或事件所代表及傳遞的訊息。

高彈性的日誌接收方式

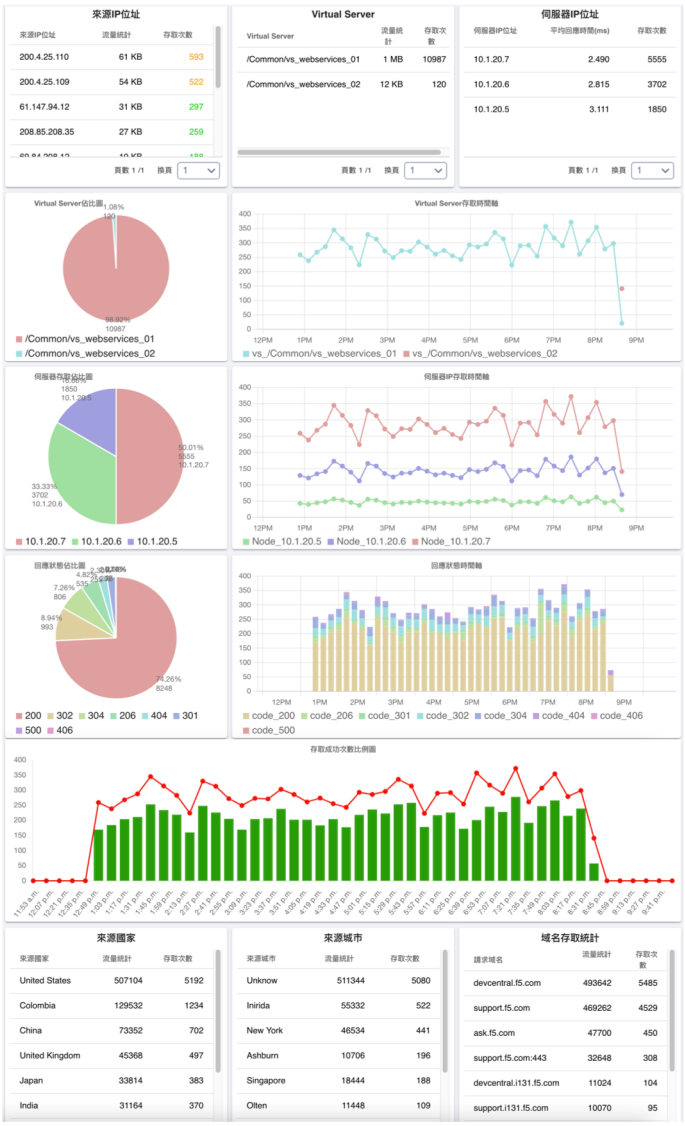
為因應現今企業不同的環境特性，大數據引擎能輕鬆的收集各種日誌，包含網路環境的Syslog。系統類別包含各類作業系統(如Windows、Linux)及其應用程式(如IIS、Exchange、DHCP、DNS、Apache)，另外資料庫(如MS SQL、My SQL、Oracle)與其他各種來源的日誌都可收集。

可視化面板

當收集大量的原始日誌(Raw Data)之後，我們可以利用可視化面板功能快速的呈現這些日誌所內含的真正意義，透過可視化的呈現，我們可以具體的顯示出包含依照時間、數量、關鍵字、特定欄位及指定設備的訊息及其變化。然而，被可視化後的訊息，才將會是大數據引擎所代來分析效益的第一步。

互動式即時報表

大數據引擎(BDE)所提供的即時報表可將已制定的可視化面板帶入報表中，藉此可快速的呈現所有相關的即時資訊，同時亦可在該報表追蹤對應的關鍵訊息，該報表提供互動式操作介面，當使用者想進一步追蹤特定訊息時，不需要透過搜尋引擎，可直接於統計圖表上點擊任何期望追蹤的訊息，即可帶入相對應的關聯資料。



即時關聯的分析應用

我們將可以透過關聯式的方式，帶出我們想要看的關係式狀態訊息。大數據引擎(BDE) 的關聯式應用相對其他廠家的應用方式更為簡單好用，使用者只要鎖定想要追蹤的訊息，即可直接將所有對應資訊於報表中呈現，透過一鍵代入式的操作概念，只要接收的訊息量足夠，必定能提供出利於分析的數據資訊。

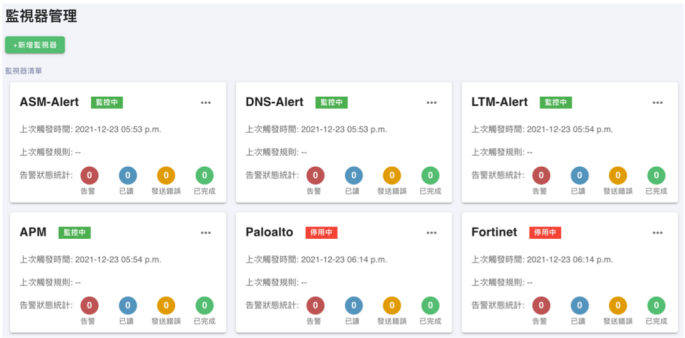
平行擴充能力

大數據引擎(BDE) 具備資料存儲擴充功能，利用集群(Cluster)技術，可以將資料儲存區進行極大限度的增長，使用者可以不用進行任何的設備汰換，僅需增加資料存儲模組即可完整儲存區的擴充。

本系統支援在線擴充，可於運作狀態進行擴充動作，配合多方存取技術，集群成員愈多，愈可提升系統效能。

豐富且彈性的告警

人力監控的時代已然遠去，取而代之的是自動化應用，而其中最重要的即是自動通報機制，大數據引擎(BDE)提供了多元的告警運算元，同時可利用AND及OR等概念進行極豐富的告警配置，利用歷史軌跡的協助分析，即可掌握告警門檻及數值，配合Mail、Line Notify、 Telegram等不同的告警通報方式，以確保當問題及異常產生時，能即時通知到維運人員，以減少影響時長，進而提高企業運作效能。



維運分析

大數據引擎(BDE)可以搭配日誌(Syslog)及事件(Event)的訊息，充份的提供相對應關聯的可能性，如此便能清楚的分析流量及事件或日誌間的對應關係，亦能從時間軌跡的應用方式，來了解此狀態是否為常態或是非常態，管理者或維運人員將可利用此訊息判斷環境異常的來源點跟可能性原因，更將大幅縮短問提查找的時間消耗，以達到企業或環境維運的最佳效益。

軟體功能

- 系統軟體系統架構，可安裝於VM虛擬環境或實體主機。
- 無限制廠牌、設備、系統及API，Log皆可收集，僅限制容量空間，單一資料儲存載體支援1.5T(含)以上空間容量授權。
- 提供Web UI, HTTPS等連線管理。
- 具備閒置提醒及自動登出。
- 即時日誌查詢功能，可即時計算及呈現日誌量。
- 可依下拉式自動化選單進行多條件過濾。
- 客製化報表，可自由配置欄位與統計圖表。可製作區塊圖(Area)、柱狀圖(Bars)、線圖(Line)、圓餅圖(Pie)、計數器(Comparison)、座標地圖(Map)、及資料表(Data Table)等功能面版。
- 提供線上更新地圖資料庫。
- 可自由配置報表內的所有統計圖表。並呈現即時資料，報表內全統計圖表資訊可統一聯動。
- 統計圖表支援點擊即新增過濾器的友善操作。
- 日誌查詢及報表皆可調整顯示時間及資料更新頻率。
- 可透過Web UI對指定日誌檔進行關閉及刪除，同時系統能記錄每日的日誌大小。
- 內建系統環境追蹤，能顯示備援狀態、目前記憶體使用量及百分比、資料儲存空間使用量及百分比。
- 可自由指定日誌、欄位及時間區段，並製作條列式報表，報表格式支援CSV格式。
- 報表具分類功能，且同一報表支援多重分類設置。
- 具備排程報表功能，提供日誌及報表之寄送排程設定並支援日報、週報及月報排程。報表寄送可自由設置收件人郵件，且支援密件副本方式寄送。
- 報表排程信件內容可自由填寫，並顯示前10筆寄出紀錄。
- 具備多重登入權限管理控制系統，用戶可自由調整工作區、角色及使用者之權限配置，權限列表對應角色可配置功能(啟用/停用)、讀取寫入(讀/讀寫)。
- 日誌查詢、報表管理、告警系統、資料管理、權限管理可獨立配置於工作區中，不同工作區之資訊將不互通。
- 提供告警功能，告警能依各個日誌來進行告警配置，並提供多重條件配置。且可配置告警資料區間及重新告警間隔，時間單位可為分、時及天時間單位。告警通報機制須支援E-mail，LINE Notify，Telegram等。
- 提供告警歷史資料查詢。
- 報表寄送排程支援CSV及PDF格式輸出。

(以下為擴充功能)

- 提供日誌資料庫監控燈號，快速掌握狀態。
- 支援監控日誌資料庫CPU、記憶體、磁碟用量等。

系統結構

- 支援高可用性架構能力，日誌接收器支援HA高可用性架構，當單一接收器故障時不影響日誌接收，日誌儲存設備支援Cluster架構，可持續擴充資料存儲空間。

安裝環境需求

- VM虛擬環境或實體主機
- CPU：16 core
- 記憶體：64 GB
- 系統容量：50 GB
- 資料存儲容量：300 GB 以上