Grafana 實作網路管理視覺化監控告警系統

林孟璋
國家實驗研究院國家高速網路與計算中心
kent@narlabs.org.tw

摘要

視覺化系統是一種趨勢，是資訊系統的明日之星，以網管資料為基底，結合了時間序列資料庫，透過資料轉換程式，將即時資料轉成時間序列的資料，並且打造了網管監控儀表版，於儀表版加入告警機制，透過設定監控標的的閥值，作為即時告警的依據。相信，資料不僅僅是冷冰冰的放在機器硬碟上，儘管網管監控標的是如此的多樣且複雜，視覺化監控系統也可使資料更有意義的呈現與操作使用。

關鍵詞：網路管理、視覺化、Grafana、時間序列資料庫。

1. 前言

隨著視覺化系統在最近這幾年風起雲湧，網路管理系統上也漸漸嗅到這方面的趨勢，TWAREN 100G 骨幹網路自上線服務以來，網路監控系統有著良好的維運品質，也進一步的想以視覺化資料方式，打造網路監控的儀表版，讓工程師與終端使用者有此更直覺的瀏覽介面，知悉哪裡出現障礙，作為除錯的參考，因此我們導入了開放原始碼的系統，將網路管理的監控資料，以視覺化的方式呈現。

TWAREN 100G 網管的資料已儲存於 MariaDB[1]資料庫多年，目前網管監控系統，以此資料作為分析的來源，以每五分鐘的監控數據加以儲存，多年來累計了不少重要資料，透過 MariaDB 轉化成 InfluxDB[2]的方式，以 InfluxDB 為資料來源加以呈現，並透過 Grafana 設定監控標的的閥值的方式，制定告警依據，設定 Grafana 管理介面中的通知頻道(Notification Channel)方式，透過多元化的告警方式，只要監控標的超過閥值，即可即時告警通知，以利維運二線人員及早收到訊息，做後續告警處置。

1.1 Grafana 簡介

Grafana 是一個開放源碼的監控視覺化工具，是由 Grafana Lab 所經營的一個完美儀表板開發系統，可以整合不同的資料來源，例如時下使用最常使用的 ElasticSearch、OpenTSDB、InfluxDB、MySQL 等，幾乎包含了所有關聯式資料庫與大數據資料庫。

由於 Grafana 強調了儀表板的豐富畫面，推出了所謂的插件(Plugins)擴充功能，讓想要開發更多元化的儀表板，可透過安裝插件來完成，開發者有想要完成特殊的面板，可以前往 Grafana Labs 的插件網址(https://grafana.com/grafana/plugins/)，搜尋是否有支援您要的插件，也因如此，使用 Grafana 一直備受開發者的關注，因此有了論壇[3]的成立，讓開發者一起共享開發上經驗與交流。

例如最近因疫情數據的展示，世界地圖疫情儀表版的使用備受注目，Grafana 就可以透過安裝插件的方式取得，透過尋找 Worldmap Panel 可以找到插件的詳細安裝資訊，以此插件進行開發，開發完成以圖1畫面呈現。

回歸主題，我們的主題是以 Grafana 開發視覺化監控系統，重要的議題是資料來源，TWAREN 網管資料與時序列(Time-series) 息息相關，在呈現各個不同的監控標的同時，都會伴隨著時間，來代表目前這個時間點的監控標的值，以往監控資料儲存於 MariaDB 資料庫，即以時間與值的方式儲存，本篇技術報告會提及 MaraiDB 與 InfluxDB 資料轉換的技術，作為最後 Grafana 存取 InfluxDB 來達成最終目的。

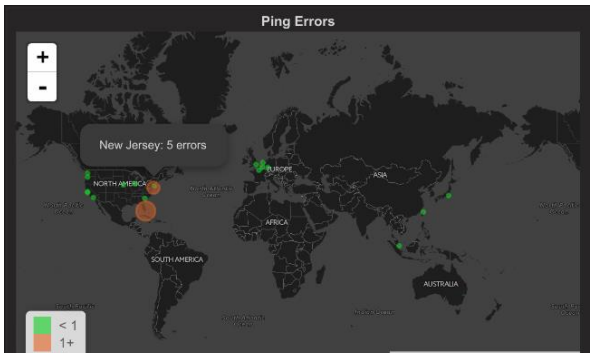

圖 1.Grafana 地圖顯示

1.2 時間序列資料庫-InfluxDB

隨著物連網在最近這幾年的風起雲湧，帶有大量時間戳(Timestamp)資料儲存與處理上日漸受到重視，InfluxDB 也因此躍上時間序列資料庫(Time-Series Database)的排行榜首，簡單來說，時間序列資料庫有著帶有時間欄位的特異性，透過時間欄位做精確且快速的查詢或儲存動作。且 InfluxDB 有著與關連式資料庫極為相似的語法，使得之前接觸關連式資料庫的開發人員可以順利接手管理。以下介紹 InfluxDB 與關連式資料庫對應的相關名詞，如表1。

表1.InfluxDB 與關聯式資料庫對應關係

InfluxDB 名詞	關連式資料庫名詞
Database	資料庫
Measurement	資料表，就是 Table
Points	表裡面的一行資料，就是 Rows(行)

其中以 Point 由時間戳(Time)、標籤(Tag)與欄(Field)組合而成。詳細說明，列於表2

表2.InfluxDB 欄位與關連式資料庫對應關係

InfluxDB 欄位屬性	關連式資料庫名詞
Time	每筆數據紀錄的時間，以時間戳記儲存，類似關連式資料庫的主鍵(key)
Tag	各種有索引（index）的屬性
Field	記錄資料的欄位，數據資料。

2. 系統架構

2.1 與非視覺化軟體不同之處

相信網路管理工程師都有聽過 MRTG 這套流量數據呈現的套裝軟體，同樣是透過 SNMP(Simple Network Management Protocol)收集網路設備資訊，並加以圖形化呈現，但也存在著網路管理上的幾個缺點。

1.資料聚集(Data Aggregation)的問題

當以長時間區間查詢流量數據時，因展示過多的資料，圖形因此會被壓縮，無法明確顯示當時的流量數據，且使用者在圖形上點選欲觀看的時間點流量時，無法呈現當時流量。Grafana 可藉由使用者互動方式，以游標指到欲觀看的時間點，即可顯示當時流量數據，例如圖2，同一時間點，Grafana 與 MRTG 的比較，很明顯的看到，Grafana 可以透過互動的方式得知在某個時間點的流量為何，但 MRTG 約略僅可看到當天的縮圖。

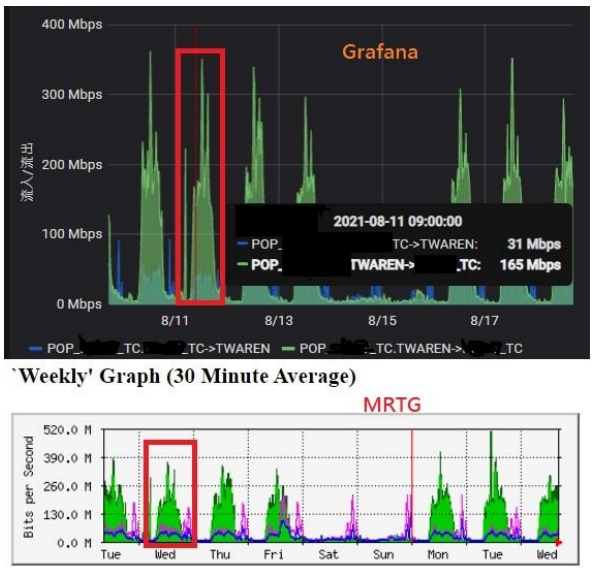

圖 2.Grafana 與 MRTG 比較

2.被動的告警通知機制

當有事件發生時，網路流量是第一個呈現的參考依據，然而傳統的 MRTG 軟體僅能被動的讓管理者登入網站察看過往流量，對於現今網管工程師已不符實際需求，工程師不應該時時刻刻盯著畫面監看網頁，我們著重的是即時的通報機制。透過主動的通知頻道，監控系統異常狀況可以馬上收到，以利障礙排除。

2.2 視覺化系統資料架構

以 Grafana 作為視覺化資料呈現的平台，加上網管資料以每五分鐘寫進資料庫，InfluxDB 更能以時間序列資料庫的優勢儲存這些資料。此章節針對這些資料如何處理流程與架構加以說明，最後目的是供 Grafana 繪圖之用，來達成建構網管視覺化之目的。整個流程架構圖如圖3，因此從路由器等設備獲取到的資料已經儲存於 MariaDB 資料庫，之後會開發轉換程式將其剖析進 InfluxDB。

轉換程式的資料來源為 MariaDB 資料庫，目的為 InfluxDB。我們系統不直接將設備的監控標的儲存於 InfluxDB 原因在於，儲存於 MariaDB 資料庫的資料已經作為整合式監控平台所使用，並不僅僅只提供給視覺化呈現，且關連式資料庫在用於呈現視覺化資料時，針對資料庫做較消耗資源的查詢，對於呈現速度上有嚴重的延遲現象，且 InfluxDB 在呈現視覺化，特別是 Grafana 的介面呈現上，更勝於關連資料庫。也因此有轉換程式的存在必要性。

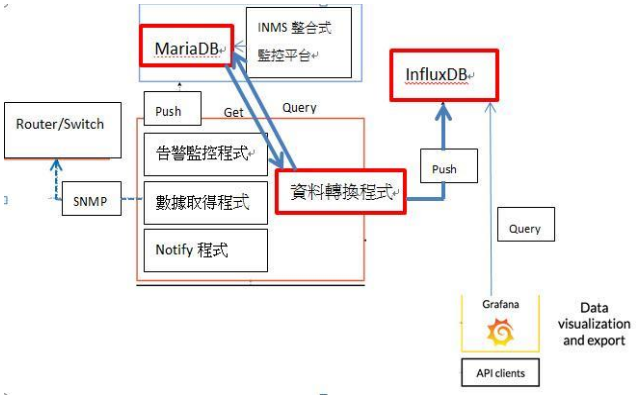

圖 3.監控資料流與架構

2.3 資料轉換軟體

工欲善其事必先利其器，有鑑於 InfluxDB 是以時間序列來儲存的資料庫，其設計方式與架構與關連式資料庫不同，例如以傳統關連式資料庫而言，搜尋資料方式是建立索引(Index)方式來加速資料的搜尋，最終以檔案來做為索引的儲存方式，

但磁碟上仍有其 I/O 上的瓶頸，然而 InfluxDB 卻是將索引（Tags）儲存在記憶體中，藉以加速查詢速度，但在資料一直增加的情況下，記憶體耗盡就是我們需要注意的議題。鑑於網管資料持續寫入，與日後記憶體耗盡導致系統崩潰的情況，設計不以寫入標籤的方式，直接透過欄位(Fields)儲存資料。鑑於 InfluxDB 需做歷史資料的轉換，我們透過 Influxdata 提供的 influxdb-php[4]這套軟體，處理 MariaDB 與 InlfuxDB 之間的的資料庫轉移作業。以下就是流量資料轉移的程式細節，依照處理資料的幾個流程說明，程式碼如圖4。

1. 載入連結 MariaDB 與 InfluxDB 資料庫所需的函示庫，並且宣告需要用到的變數。例如我們 InfluxDB 主機為'192.168.3.73'、連接的埠號(Port)為8086、寫進資料表為' interface_traffic' 這些都是建立連結 InfluxDB 資料庫的最主要資訊。完成連結之後產生一個連接物件，若資訊有誤會拋出錯誤。
2. 依照不同的電路編號，剖析進我們想要的資料庫，因此設計 InfluxDB 資料庫變數為$wr_measurement，之後繪製 Grafana 圖表會選用這些資料表當作資料來源（Data Sources）
3. 讀出 MariaDB 的資料，透過一個陣列變數儲存流進/流出的資料。
4. 儲存進 InfluxDB 的前置作業。設計資料表時，不需要表的值(measurement's value)與設計標籤（tags），所以這兩個我們以 null 與 $emptyArray 來代替。之後產生一個點（Points,等同於關連式資料庫的 Rows），最後透過 writePoints 方法寫進 InfluxDB。完成轉換作業。

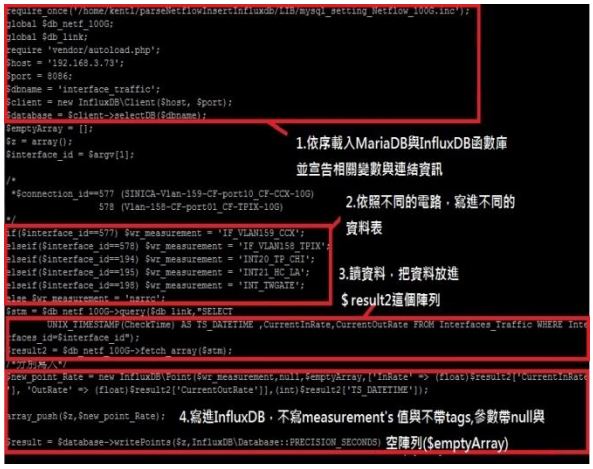

圖 4.資料轉換程式碼

3. 設計

設計 Grafana 的網管告警系統有兩個最主要方針，先透過介面建立一個儀表版(Dashboard)，儀表版有多個面板(Panels)，每個面板都可以自訂連結資料來源。也因如此，如果每個儀表版建立多個面板，都來自於不同來源，我們在設計初期，需要將資料來源設定好，再接下去設計圖表想要怎麼呈現，所以，設計流程是有其先後關係。

3.1 設定資料來源

Grafana 支援的資料來源非常廣泛，舉凡傳統的關連式資料庫，到最近流行的大數據資料庫、時間序列資料庫都列入其中。資料來源設定方法為，先進入 Grafana 管理介面中，設定(Configuration)/資料來源(Data Sources)這個頁籤中，裡面有個新增資料來源的按鈕，按下之後，選定要新增的資料來源為 InfluxDB，之後進入設定的主要內容畫面，如圖5，需填入的內容為。

1. 給資料來源命名。這邊我們取名為 InfluxDB，之後在建立視覺化儀表時，即可下拉選單，選用此資料來源
2. 透過 HTTP 連線 InfluxDB。填入我們之前資料移轉後的伺服器 IP 位址與埠號。例如'http://192.168.3.73:8086'。
3. 連線如需認證請勾選認證類別。如果僅是一般認證，例如帳號、密碼，請選基礎認證(Basic Auth)。
4. 之後填入 InfluxDB 細節部分。需要存取的 Database，就是之前我們移轉時指定的'interface_traffic'

圖 5.設定資料來源

3.2 面板視覺化設計

設計好資料來源之後進入設計面板階段，此階段最主要呈現面板的內容，包含需要存取資料庫名稱、資料表名稱、資料表欄位、資料是否要時間間格彙整（Group by time interval）等，這些設計需求最終才會呈現在面板上，但 Grafana 透過所

良好的呈現方式，一邊設定介面時一邊檢視成果，馬上可以知道哪裡出錯。設計步驟，如同設定資料來源時，進入 Grafana 管理介面，選定建立(Create)/儀表版(Dashboard)頁籤，並選定新增面板(Panels)，會得到以下畫面，如圖6，需選定填入的內容為。

1. 資料庫名稱。之前設定資料來源時，我們為新建的 InfluxDB 命名的名稱。
2. 選擇資料表。之前針對不同的電路線路，處理 MariaDB 並剖析進 InfluxDB 資料表的名稱(measurement's name)
3. 選擇欄位。以流量而言。我們於設計資料表時，有設計 InRate 與 OutRate 代表量個流量欄位。分別表示流進骨幹網路與流出骨幹網路的資料
4. 設定資料彙整時間間格。InfluxDB 可以儲存時間間格極小的資料，因次如果不聚集資料，會使圖表產生過於密集，因此透過設定時間間格(Time interval)方式，聚集化(Grouping)這些資料，才呈現，也因如此，原本資料最小單位小於設定的時間間格才有意義。

圖6.面板設計

3.3 閥值與告警管道設計

好的告警系統不僅是即時與正確的通知管理單位，更要是多元化的通知管道(Notification channels)。Grafana 支援多種通知管道，不僅僅是單純的電子郵件通知，也可以透過近期受歡迎的 webhook 把告警資訊透過 HTTP 協定，傳送到另個網頁系統，例如 Mattermost。

通知管道也是在管理介面中的告警(Altering)/通知(Notification channels)頁籤中找到，並切新增管道這按鈕，之後有通知管道類別供我們選擇，先為通知關到命名，以利之後選取。之後選擇 Email，並且在下方電子郵件欄位填入之後寄送的電子郵件，這邊可以填入多個收件者，以;作為區隔，事件發生時就可以讓多位收件者收到訊息。選擇與填入資訊如圖7。

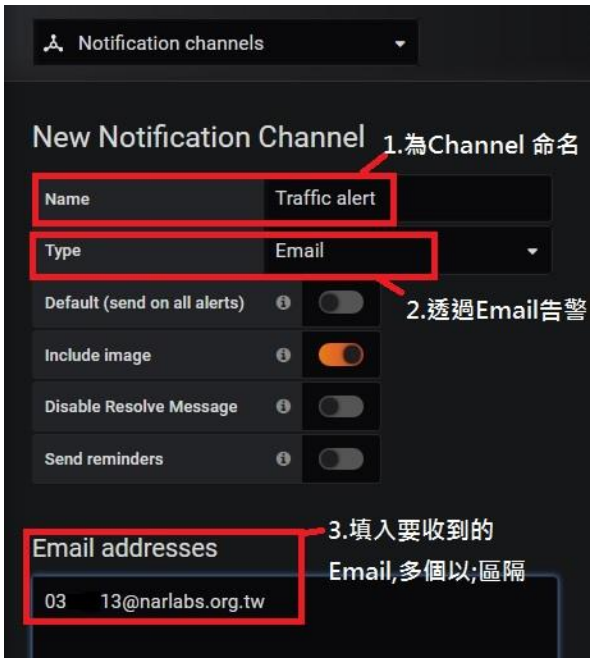

圖7.新增告警管道

透過建立好的告警管道，直接進入於之前的面板設計畫面，選擇最後一個帶有小鈴鐺的按鈕，出現提示告警(Alert)的符號，即是設定告警，並按下新增告警(Create Alert)，即可進入設定告警畫面，最主要需填

1. 為新增告警命名。不同的面板都有不同的告警條件，為了區別，為此命名此類的監控是針對哪些標的。此區塊的設定，也可以針對幾分鐘做一次告警偵測，以及針對持續突破閥值幾分鐘之後才發出告警，針對不想忽然突破閥值即刻告警非常有用。
2. 設定閥值。臨界閥值是告警的重要依據，可以透過資料庫的過往資料，來辨別是否發告警信件，例如針對流量閥值做了一個條件設定，當針對現在時刻起前15分鐘的平均值，超出600Mbps 閥值來作為告警，就可以寫成 *when avg() of query(A,15m,now) is above 600*。A 為當時面板設計時，建立查詢的編號，詳細如圖8。
3. 選擇告警給哪些人。透過設定好的告警管道，可以讓這些收件者受到訊息，並且於如下著名額外的資訊供參考。

圖8.告警閥值設定

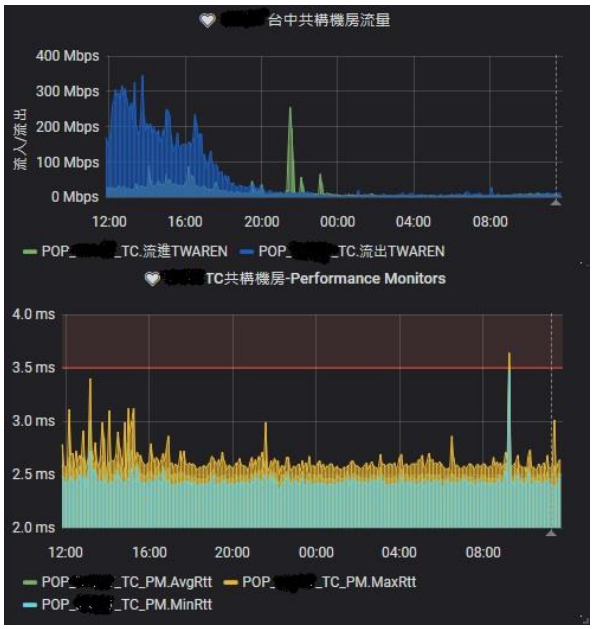

圖.9告警閥值設定

4. 告警實例與結論

設計網路管理監控告警系統最主要目的為，監控眾多的重要標的，讓維運人員可以即時知道目前網路哪裡出現明顯的問題，適時的迅速找出解決問題的方法，但又不造成維運人員緊盯監控螢幕累人的窘境，因此 Grafana 設計的告警系統可以彈性的將監控標的超出閥值與恢復正常狀態時予以提示，免於維運人員收到不必要的頻繁告警。

此外 Grafana 針對導入機器學習[5]，並予以預測有一定程度的探討，這方面的預測機制都是值得研究的議題。

4.1 告警實例

TWAREN 對連線單位的品質一直密切關注的議題，通常發生網路不順的情況，透過連上流量監控系統，觀察流量狀態以瞭解目前狀況，並探究造成原因，因此關注連線單位流量成為監控的重大指標之一，如果將流量記錄作成其中的面板，視其為主要的功能，一併將連線品質的資料納入其儀表版中，例如，利用 Ping 的回應結果，RTT(Round Trip Time)，將其量化，放置於同一個儀表版內，將是更好驗證紀錄。因此在設計連線單位監控儀表版時，可以不僅有一種監控，並且針對不同監控設定閥值，只要其中之一的標的異常，發出告警，來達到即時監控的功能。

實例1是以 TWAREN 的連線單位 M 台中共構機房為例，所提供的監控面板為，流量、RTT，如圖9所示。

其中，因為 RTT 的數據超出我們設定的閥值，3.5ms(millisecond)，同時也讓網管管理者同時注意到流量的監控數據，並因此發出異常告警到設定的信箱中。如圖10所示。

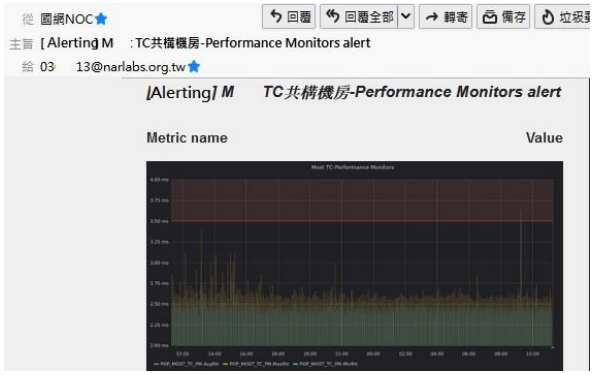

圖10.告警閥值設定

針對連線單位我們也加入監控，實例2為 TWAREN 連線單位，台灣大學，因其流量出現超出閥值的情況，但不久之後又恢復至閥值之下，透過 Grafana 告警機制，不僅可以收到告警與恢復狀況的告警信件，也可在其管理介面中得到告警與恢復的歷史記錄，這對於追蹤事件是一項利器。紀錄畫面如下圖11。

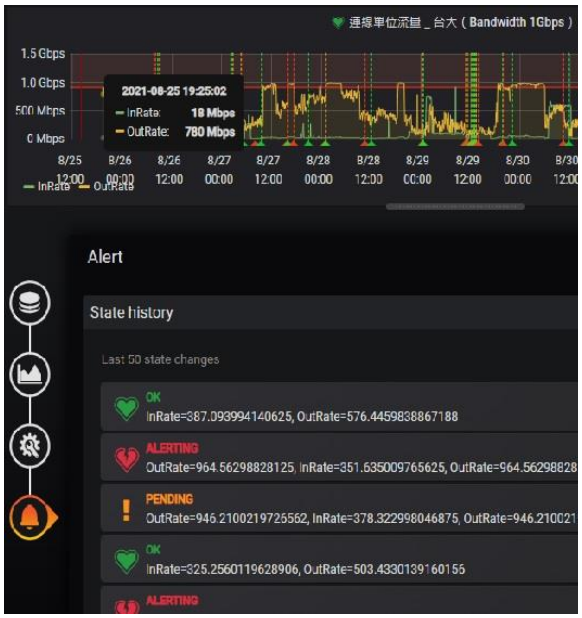

圖11.告警歷史記錄

4.2 結論

Grafana 不僅是一套視覺化呈現的軟體，更是監控資料狀態的告警監控軟體之一，開發者準備好要呈現與監控的資料，透過其介面設定，將想要呈現在使用者的畫面架構於儀表版上，觀看者容易瞭解資料想表達的意義，更賦予管理者好的監控功能，不需額外自行開發與刻劃美工圖案。Grafana 是一套平易近人的視覺化軟體，其刻畫好的儀表版甚至可以匯出/匯入的功能，易於使用者操作。

參考文獻

[1] MariaDB Foundation - MariaDB.org 。檢自 https://mariadb.org/ (Sep. 03, 2021)

[2] InfluxDB: Purpose-Built Open Source Time Series Database 。檢自 https://www.influxdata.com/ (Sep. 03, 2021)

[3] Grafana Labs Community Forums。檢自 https://community.grafana.com/ (Sep. 03, 2021)

[4] GitHub - influxdata/influxdb-php: influxdb-php: A PHP Client for InfluxDB, a time series database。檢自 https://github.com/influxdata/influxdb-php(Sep. 03, 2021)

[5] Configuring Machine Learning in Grafana to get predictions on system/web/applications KPIs。檢自 https://medium.com/@vova.sergeyev/configuring-machine-learning-in-grafana-to-get-predictions-on-system-web-applications-kpis-9c520eb595e9 (Nov. 03, 2021)