TWAREN 大數據整合資料平台

陳品瑄　梁明章　陳俊傑
財團法人國家實驗研究院高速網路與計算中心
{hsuan,liangmc,jjchen}@narlabs.org.tw

摘要

為了滿足越來越複雜的網路行為，也因此在 IT 方面投入更多的設備資源，以建立更複雜的網路架構，來符合使用者的需求。但是當建立新的架構和設備時，數據資料也正在以驚人速度增加中，所面對的更困難的挑戰是如何從巨量數據(Big Data)中整合多樣性的資料、分析及解讀並取得當中之線索、趨勢以及戰略價值，以維持系統的正常運作，提高網路服務的品質? 本整合平台利用 Logstash[1]蒐集多種不同來源的日誌、警訊資料及搭配 Elasticsearch[2]巨量資料搜尋建置符合所需查詢分析平台(ILTAS , Intelligent Log and Trap Analysis System)。存取台灣高品質學術研究網路（TaiWan Advanced Research and Education Network，TWAREN）[3]混合型網路（ Hybrid Network）架構上的多種資料來源，提供平台資料搜尋、視覺化數據分析及資料匯出。針對巨量數據中的 SNMP Trap、Syslog 事件紀錄提供整合性即時資料查詢，及透過關聯性事件分類，快速提供使用者所需綜合性資料，進行可視覺化的數據瀏覽及分析，進而從中萃取出有價值的資訊，提升維運績效，降低風險，提供新一代維運方式。

關鍵詞：Big Data、TWAREN、Elasticsearch、Logstash、SNMP Trap、Syslog。

1. 前言

運用大數據分析來確保高效率且穩健的運作，儼然已成為趨勢。網路服務中斷的根本原因，其實就藏在每天累積的海量日誌資料、事件紀錄中。因此透過收集不同的資料、解讀設備日誌資料與分析的方式掌握網路狀況發生異常狀況時，釐清眾多導致的可能發生異常狀況。分析相關因素的的紀錄檔案內容來確認異常原因並解決問題，才能清楚掌握網路事件及網路現況並關聯相關事件。當網路發生異常或是網路訊號中斷時，透過單一資料來源，往往無法釐清問題原因和影響範圍，不同的網路設備所提供的資料各有專長，也都有不足之處。整合得當將有助於一線網管人員窺知網路活動的全貌。即時提供整合性、跨領域的資料，有助於一線人員查看和診斷故障問題進行綜合性判斷，以明白其問題脈絡和障礙影響範圍。

ElasticSearch 沒有權限管理，使用者認證功能。因此，任何人都可以隨意讀寫 ElasticSearch 的 API 並獲取數據資料。因此 Elastic 公司為 ElasticSearch 開發的一個商業安全插件(plugins) Shield。Shield 是一款商業產品，提供 30 天免費試用。因此，藉由本平台單一入口，使用者可以使用 ElasticSearch 來完成其內容搜尋與資料處理分析的工作。透過直覺化易操作使用介面，將下轄網路裡的 SNMP Trap 與 Syslog 資料集中，提供使用者獲取整合性資料及數據分析視覺化呈現。

2. 相關議題

2.1 ELK(Elasticsearch、Logstash、Kibana)

ELK(Elasticsearch、Logstash、Kibana)是目前 Apache.org 所開發的搜集大資料的架構。

1. Elasticsearch 分散式搜尋系統，提供搜集、分析、儲存數據三大功能；是一套開放 REST 和 JAVA API 等結構提供高效率搜索功能，構建於 Apache Lucene 搜尋引擎庫之上。
2. Logstash 是一個用來搜集、分析、過濾日誌的工具。提供了各式各樣的日誌收集及輸出的 Plugin，任何類型的日誌幾乎都有支援，包括系統日誌、錯誤日誌和自定義應用程式日誌。可以從許多來源接收日誌，並且能夠以多種方式輸出數據。
3. Kibana 是一個基於 Web 的圖形介面，沒有權限管理，使用者認證功能。可以用於搜索、分析，及視覺化呈現儲存在 Elasticsearch Index(索引)中的日誌數據。可以利用 Elasticsearch 的 REST 接口來檢索數據，使用者可以創造個人化數據的視覺化儀表板，或是可以以特殊的方式查詢和過濾數據。

2.2 測試範例

Logstash 主要可分為輸入資料(input)、處理資料(filter)、輸出資料(Output)，以圖1 Logstash 設定檔為例，input 使用 stdin 方式，也就是接受畫面上的輸入，Output 則是使用 Elasticsearch 輸出到 host

```
input{
  stdin{}
}

filter
{
 }

output {
        stdout { codec => rubydebug }
        elasticsearch {
                hosts => ["192.168.3.95:9200"]
                index => "logstash-test-%{+YYYY.MM.d
        }
}
```

圖1 Logstash 測試

執行設定檔後輸入測試訊息後，在 kibana 中建立一個 logstash-test-* Index Pattern，就可以在 kibana 上看到剛剛輸入的測試訊息如圖2所示

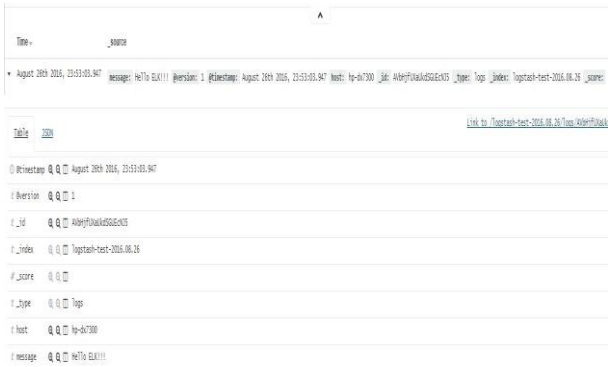

圖2 測試結果

3. 系統建置與實作

3.1 系統架構

將 TWAREN 網路環境中的設備 ，包括網路設備 (Router/Switch/ROADM/ASR..等)、伺服器，逐一設定 SNMP Trap 與 Syslog 輸出。系統架構如圖3所示，使用 Logstash 接收與處理網路設備在異常發生時送出的 Trap 及設備的 syslog。透過 Logstash 導入各種資料收集模組，取得各網路設備中的詳細使用記錄，進行過濾和格式化（轉成 JSON 格式），然後傳給 Elasticsearch 進行儲存、建構搜尋索引。

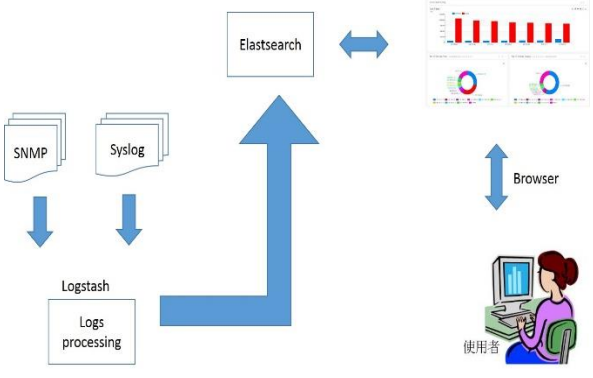

圖3 系統架構

3.2 資料過濾(Data Filter)

利用 Logstash 來作為前置處理器以分析來源，收集不同的資料，剖析日誌、設定格式分析轉換成各種資料欄位。將各種不同結構的資料進行結構化，輸出至 Elasticsearch 使用。Syslog 方式將事件日誌(Event)做為分析或是稽核備查之用已經非常普及，包括網路設備、安全設備、伺服器(OS、Application)都已能支援 Syslog。然而，Syslog 丟出的設定並不相同，日誌的格式也都不一樣，因此，接收端需要能夠辨識剖析不同型態的日誌，並且過濾處理，才能做後續分析。因此，將 Syslog 原始訊息如圖4，過濾解析後轉成結構化資料如圖5。

```
<190>731354: RP/0/RP0/CPU0:Aug 26 22:36:07.558 : devc-vty[187]: %MGBL-TTY-6-CONNECTION_DENY_ACL_ERROR :
Connection denied by ACL mismatch. Source Add 179.222.93.27. Dest Add 211.73.76.145. Source Port 58256. Dest port 23. Acl
acl_10_vty.
```

圖 4 Syslog 原始訊息

圖 5 Syslog 結構化資料

SNMP Trap 原始訊息是數值形式呈現(如圖6)，因此，將匯入廠商設備管理訊息資料庫(MIB)，透過 Logstash 轉換物件名稱的數值形式，將原始的訊息正規化呈現為可讀可分析的資料(如7所示)，並存入 Elasticsearch 。

```
#<SNMP::SNMPv2_Trap:0x35c7e228 @request_id=3243, @error_index=0, @error_status=0,
@source_ip="192.168.242.41", @varbind_list=[#<SNMP::VarBind:0x7b9965d5 @name=
[1.3.6.1.2.1.1.3.0], @value=#<SNMP::TimeTicks:0x533be780 @value=79170416>>, #
<SNMP::VarBind:0x59e7896d @name=[1.3.6.1.6.3.1.1.4.1.0], @value=[1.3.6.1.4.1.9.9.276.0.1]>, #
<SNMP::VarBind:0x7460198 @name=[1.3.6.1.2.1.2.2.1.1.436232192], @value=#
<SNMP::Integer:0x37416b68 @value=436232192>>, #<SNMP::VarBind:0x3b4a8de7 @name=
[1.3.6.1.2.1.2.2.1.7.436232192], @value=#<SNMP::Integer:0x5e03c702 @value=1>>, #
<SNMP::VarBind:0x69fe579b @name=[1.3.6.1.2.1.2.2.1.8.436232192], @value=#
<SNMP::Integer:0x55d86be7 @value=2>>, #<SNMP::VarBind:0x3a92f10e @name=
[1.3.6.1.2.1.31.1.1.1.1.436232192], @value="Ethernet1/7">, #<SNMP::VarBind:0x7a691a89
@name=[1.3.6.1.2.1.2.2.1.3.436232192], @value=#<SNMP::Integer:0x61b0c8d0 @value=6>>]>
```

圖 6 SNMP Trap 原始訊息

DISMAN-EVENT-MIB::sysUpTimeInstance	9 days 03:55:04.16
SNMPv2-MIB::snmpTrapOID	CISCO-IF-EXTENSION-MIB::cieLinkDown
IF-MIB::ifIndex.436232192	436232192
IF-MIB::ifAdminStatus.436232192	1
IF-MIB::ifOperStatus.436232192	2
IF-MIB::ifName.436232192	Ethernet1/7
IF-MIB::ifType.436232192	6

圖 7 SNMP Trap 結構化資料

3.3 資料搜尋

1. 全文檢索

本系統導入全文檢索搜尋引擎，可快速進行巨量資料搜尋，提供簡易即時查詢，方便使用者點擊搜尋。也可以使用關鍵字交叉查詢，並可設定搜尋期間、每頁顯示筆數篩選查詢範圍，節省搜尋時間。使用者可以根據關鍵字查詢方式輸入，系統將從訊息內容中，找到符合的內容，提供所需資料或是綜合性資料(如圖8)。

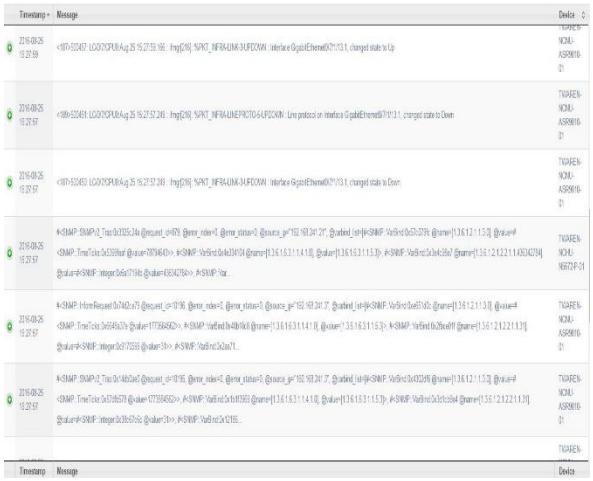

圖 8 down 事件搜尋範例

2. 分類檢索

本系統以常見的搜尋紀錄及故障重大事件，以關聯式分析，整合 trap 和 syslog，探勘出在 trap 警訊和 syslog 日誌間具有相關性的隱藏規則，進行分類，大致可分為下列類別:

1. BGP
2. OSPF
3. Link up/Down
4. 光網路訊號中斷

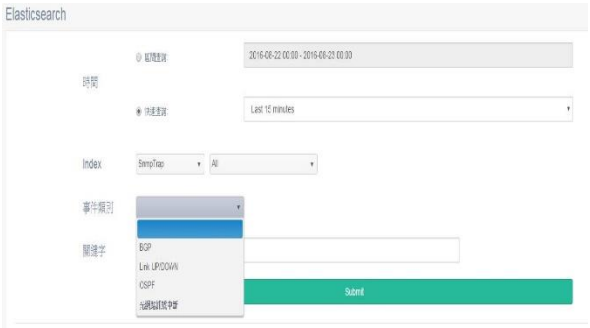

圖 9 搜尋介面

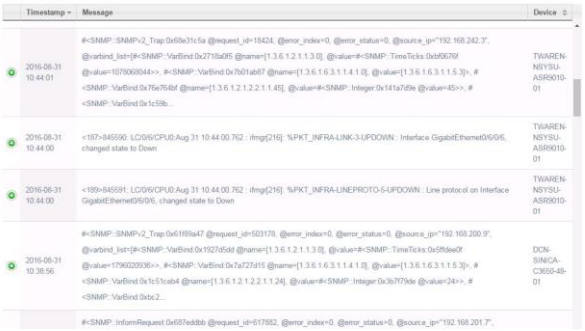

圖 10 Link up/down 事件整合資料

3.4 資料分析(Data Analysis)

資料是有價值的資源，巨量資料可能埋藏著前所未見的知識跟應用等著被我們挖掘發現；連結不同來源的資料並挖掘價值，而不再只是透過單一資料表分析。ILTAS 整合平台除了可提供即時資料查詢，同時提供資料彙整、即時分析異常設備。以視覺化儀表板清楚呈現綜合性資料，提供整體的資訊。

圖 11 ILTAS 綜合性即時資料分析

透過 ILTAS 整合平台系統分析功能，使用者可以自訂欲分析的資料區間及索引資料。SNMP Trap 以設備和 Trap OID 產生4種2階段彙整排序分析，透過此2階段彙整分析長期觀察或是即時分析，將有助於對未來 trap 事件分類及告警訊息嚴

重程度的過濾分析。以圖12 SNMP Trap 為例即時產生在15分鐘內的4種情境分析及2階段彙整排序分析過程如圖13所示:

1. Top Device & Top Trap : 根據查詢的期間分析出 top 10 設備, 再依據各個設備 drill down 彙整分析出發送最多的 trap
2. Top Device & Bottom Trap : 根據查詢的期間分析出 top 10 設備, 再依據各個設備, drill down 彙整分析出發送最少的 trap
3. Bottom Device & Top Trap : 根據查詢的期間分析出不常發送 trap 的設備, 再依據各個設備, drill down 彙整分析發送最多的 trap
4. Bottom Device & Bottom Trap : 根據查詢的期間分析出不常發送 trap 的設備, 再依據各個設備, drill down 彙整分析出發送最少的 trap

圖 12 SNMP Trap 即時資料分析

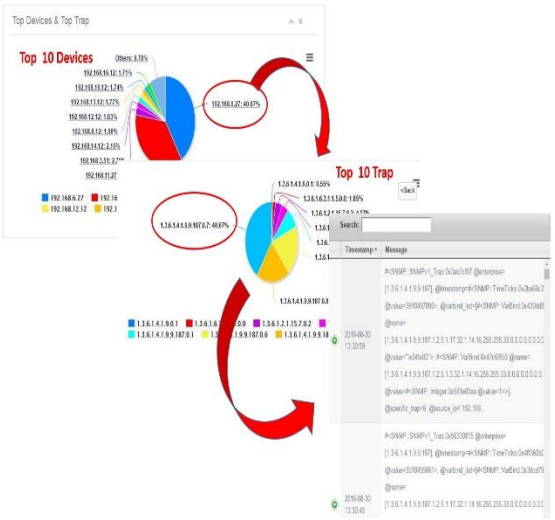

圖 13 SNMP Trap Drill Down 範例

Syslog 以 Program 和設備產生4種2階段彙整排序分析，以圖14 Syslog 為例即時產生在15分鐘內的4種情境分析:

1. Top programs & Top Devices: 根據查詢的期間分析出 top 10 syslog programs , 再依據各個 program, drill down 分析出 top 10 programs，主要是在那些設備中
2. Top programs & Bottom Devices: 根據查詢的期間分析出 top 10 programs, 再依據各個 program, drill down 分析出 top 10 programs，卻在那些設備中最少使用
3. Bottom programs & Top Devices: 根據查詢的期間分析出不常使用的 programs , 再依據各個 program, drill down 分析不常使用的 programs 中，主要是在那些設備中
4. Bottom programs & Bottom Devices: 根據查詢的期間分析出不常使用的 programs, 再依據各個 program, drill down 分析最少使用設備

圖 14 Syslog 即時資料分析

圖 15 Syslog Drill Down 範例

3.5 實作案例：

從 SNMP Trap 分析發現光纜出現異常狀況，Syslog 訊息告知 interface link down。
當光纜出現異常狀況，無法接收到對方所送出的光源，將影響到電路上的所有光通道服務，也將導致所連接 router 受到影響，發生告警。

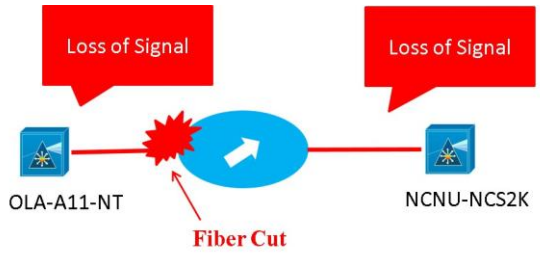

圖16 光纜異常狀況

整合平台收到光網路訊號中斷警訊，因此經由過濾分析由 Syslog 日誌，得知受到影響的 Router ，會有 interface link down 訊息。整合 SNMP Trap 和 Syslog 日誌，可以快速找到障礙發生點及釐清障礙影響範圍(如圖17)。

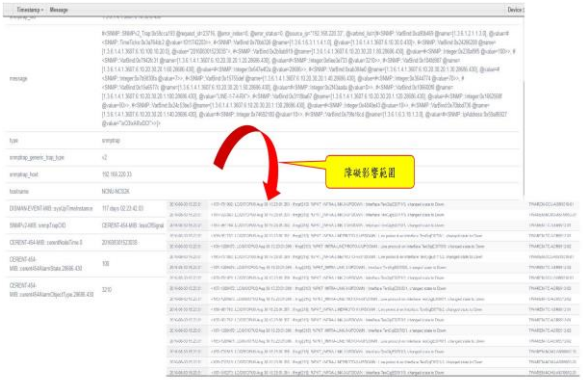

圖 17 分析案例

4. 結論與未來研究工作

巨量數據的運用已是未來主流，透過對巨量數據的蒐集、保存、分析和應用可以從中挖掘出未知的趨勢及有價值的 IT 資訊，提供新一代網路監控解決方案，呈現嶄新的視野。現今網路設備越來越多、越來越複雜，使用者在使用各式各樣的服務時，會在各個網路設備留下用記錄，網路設備發生問題時，同樣也會產生難以計數的告警訊息，在這樣的複合式記錄環境裡，需要透過資料收集系統進行彙整處理分析。本平台整合下轄網路設備裡的 SNMP 與 Syslog 資料集中蒐集、處理、分析，目的是為了可以完整呈現網路真實的使用現況，協助網路維運以及除錯，進而提供 一線人員未來執行 網路優化和擴充計畫時的確切可行方向，藉由本平台可以提供前端的頁面進行搜索和資料分析視覺化。透過全文檢索功能及事件分類分析，不僅可以提高診斷的效率，同時可以達到即時系統監測、網路安全、事件管理等功能。目前，我們仍持續針對大數據開發自動告警關聯分析。結合更多監控日誌數據資料，將告警(Alert)到報告(Reporting)以及記錄(Audit) 環節都緊密連結才能有效運用運算資源。

參考文獻

[1] Logstash, https://www.elastic.co/products/logstash
[2] Elasticsearch, https://www.elastic.co/products/elasticsearch
[3] TWAREN, TaiWan Advanced Research and Education Network. http://www.twaren.net/
[4] http://www.cisco.com/