系統日誌分析與告警服務

計通中心為協助校內單位預防資安異常狀況及保存系統日誌(事件紀錄)問題，規劃「系統日誌分析與告警」服務。本服務為建立一持續收集資訊系統產生的紀錄，以自建規則進行資料分析後，自動產生異常狀態通知信，及時通知管理人員進行處理的資安檢測系統。另，系統收集的資料會保留六個月以上(依系統資源狀況進行調整)，用於申請端的系統資料因故被刪除時，提供另一份系統日誌資料進行分析使用。此服務系統已完成建置，於108年6月正式上線。

功能

目前本服務接受 2 種格式資料：

1. MS Windows 平台的事件紀錄的收集分析服務，自動通知有關“帳號異常”、“特定資料匣\檔案異動”等異常狀態。
2. Syslog 格式的記錄收集服務，自動通知“登錄異常”或依申請者需求客制化的“異常狀態”。

監控的異常狀態種類說明

- 帳號異常：帳號登入錯誤、帳號新增、帳號刪除…等
- 檔案異動：資料匣與檔案的建立與刪除等，此項種類需啟用 Window 系統的物件存取稽核原則，會耗用較大量的系統資源進行事件紀錄，因此僅提供限制特定資料匣監控，避免系統資源加快耗盡。註：此監控非預設提供項目。欲使用該監控功能，作業系統須另外啟用檔案稽核功能，並設定目標檔案或資料匣。
- MSSQL 帳號異常
- (將陸續新增異常監控規則，例如：本機防火牆異動…等)

服務申請注意事項

1. 本服務須由單位網管透過 email 向服務聯絡人提出申請。
2. MS Windows 系統的事件紀錄匯出，需安裝一**服務應用程式(Agent)**，藉由此程式將 Windows 的事件紀錄發送至本服務系統，會耗用些許系統資源。
3. 可能需調整既有的防火牆規則，允許與本服務之間的通訊連線。
4. 如需由本組提供相關日誌資料，目前僅能提供 CSV 格式。
5. 申請 syslog 格式的記錄收集分析服務時，因各設備所產生的syslog資料欄位並不相同，需經過格式解析後，才能用於本分析服務。因本服務所儲存的資料已非原始的 syslog 資料，無法提供申請單位要求該格式的日誌資料。

其他

1. 因系統資源限制，本服務目前可接受申請的系統或設備以行政、教學單位的公用服務系統 MS Windows 作業系統）及 Cisco 網路交換器資料為主。
2. 於 Linux OS 平台上，已有 logwatch Fail2ban 等軟體能提供自動化的 log 分析與阻擋異常登入的

功能，建議 linux OS 平台管理人員可參考使用。

服務聯絡人：網路系統組 施先生，校內分機 31134，郵件信箱yucshih @ mx.nthu.edu.tw

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/security:log_collection

Last update: **2020/06/18 10:07**