

系統日誌分析與告警服務新增功能公告

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)，於108年建置「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。

新增可接收 Syslog 協定的日誌資料

即日起，本服務新增可接收 syslog 協定的系統日誌資料，並提供“登入異常”的自動化電子郵件通知。另，收集的資料會保留六個月以上(依系統資源狀況進行調整)，可用於申請單位自有的系統資料因故無法使用時，協助申請單位查詢相關記錄。

新增功能說明

1. 新增可接收 syslog 協定的日誌資料進行分析。
2. 目前以 Cisco 網路交換器的 syslog 資料的申請為主，提供發生“登入異常”時，自動發出電子郵件通知管理人員。
3. 可接受單位公共使用但非上述廠牌的基礎網路設備申請本服務。服務申請注意事項2

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. 單位網管請與服務聯絡人聯繫，進行資料解析新增格式作業。
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の日誌資料。

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_syslog

Last update: **2020/06/18 10:23**