



Anti-Money Laundering

洗錢防制系統-異常處理



Anson Lin



2021/9/14



Stark Technology Inc.

敦陽科技股份有限公司

Agenda

- 處理原則
- 常見錯誤
 - 名單匯入
 - SWIFT
 - 姓名檢核

■ 查看Log

- 事件檢視器
- AML資料庫紀錄：GCMAINDB..Logs table
- 相關應用程式紀錄
 - EXE：D:\PATRIOTOFFICER\PATRIOTOFFICER_FILES\EXE\Logs
 - Web Service：D:\Logs 或 D:\PATRIOTOFFICER
 - MSI：D:\Logs 或 C:\Program Files\GlobalVision Systems

■ 確認是否有環境異動

- 網路環境：防火牆異動、更換IP、網路異常等
- 作業系統：軟體(防毒)更新、windows Update等
- 人員異動：更換使用者帳號、密碼、群組、分行等

處理原則-事件檢視器

The screenshot displays the Windows Event Viewer interface. The left pane shows the navigation tree with 'Application' logs selected. The main pane shows a list of application errors, with the most recent one selected. The details pane for this event shows an exception of type 'NullReferenceException' from 'PatriotOfficer.MessageAutomation'.

事件檢視器 (本機)

- 自訂檢視
- Windows 記錄
 - 應用程式
 - 安全性
 - 安裝程式
 - 系統
 - Forwarded Events
- 應用程式及服務記錄檔
- 訂閱

應用程式 事件數目: 53,165

已篩選: 記錄: Application; 等級: 重大, 錯誤; 來源: 事件數目: 42,185

等級	日期和時間	來源	事件識別碼	工作類別
錯誤	2021/08/12 12:12:51	MSSQLServerOLA...	11	(289)
錯誤	2021/08/12 12:12:44	PATRIOT OFFICER	0	無
錯誤	2021/08/12 12:12:44	PATRIOT OFFICER	0	無
錯誤	2021/08/12 12:12:44	PATRIOT OFFICER	0	無
錯誤	2021/08/12 12:12:44	PATRIOT OFFICER...	0	無
錯誤	2021/08/12 12:12:44	PATRIOT OFFICER	0	無
錯誤	2021/08/12 12:12:39	PostgreSQL	0	無
錯誤	2021/08/12 12:12:39	PostgreSQL	0	無
錯誤	2021/08/12 12:12:39	PostgreSQL	0	無

事件 0, PATRIOT OFFICER

一般 詳細資料

Exception Type: NullReferenceException
Source: PatriotOfficer.MessageAutomation
Date: 2021年8月12日
Time: 下午 12:12:44
Message: 並未將物件參考設定為物件的執行個體

記錄檔名稱(M): 應用程式
來源(S): PATRIOT OFFICER 已記錄(D): 2021/08/12 12:12:44
事件識別碼(E): 0 工作類別(Y): 無
層級(L): 錯誤 關鍵字(K): 傳統
使用者(U): 不適用 電腦(R): TEST3-S00452
OpCode(O):
詳細資訊(I): [事件記錄檔線上說明](#)

動作

應用程式

- 開啟已儲存的記錄...
- 建立自訂檢視...
- 匯入自訂檢視...
- 清除記錄檔...
- 篩選目前的記錄...
- 清除篩選器
- 內容
- 尋找...
- 另存篩選記錄檔...
- 附加工作到此記錄檔中...
- 將篩選器儲存到自訂檢視...
- 檢視
- 重新整理
- 說明

事件 0, PATRIOT OFFICER

- 事件內容
- 附加工作到此事件...
- 複製
- 儲存選取的事件...
- 重新整理
- 說明

啟用 Windows
移至 [控制台] 中的 [系統] 以啟用 Windows。

■ GCMAINDB Logs資料表重要欄位

欄位名稱	欄位說明
DateTime	訊息日期時間
BankNo	銀行代號
Path	程式路徑
RawUrl	實體程式路徑
ExceptionType	例外類別
InternalMessage	內部訊息
ExceptionMessage	例外訊息
StackTrace	詳細訊息
Application	發生訊息應用程式
LogType	訊息類別

處理原則-相關應用程式紀錄

■ LOG分類

項目	路 徑	主機
EXE Log	D:\PATRIOTOFFICER\PATRIOTOFFICER_FILES\EXE\Logs	AP Server
IIS Log	C:\inetpub\logs\LogFiles	AP Server
		IN Server
MSI Log	C:\Program Files\GlobalVision Systems\應用程式\Logs C:\Logs D:\Logs	AP Server
		IN Server
		CDC Work Server

■ Log擷取

- 依據上述路徑找到Log記錄檔
- 依據錯誤發生時間點，確認是否有相關訊息
- 研判訊息內容或將訊息內容Email給敦陽科技PM、工程師，以便查看問題發生原因

常見錯誤-GVS名單匯入

■ 查看Logs

- 路徑D:\PATRIOTOFFICER\PATRIOTOFFICER_FILES\EXE\Logs (預設)
- 檔名DownloadComplianceList.log
- 檔名SCHED_BlacklistPreparation.log

■ 常見問題類型

- 名單晚到：檔案到檔時間比名單匯入排程時間晚
- 連線異常

常見錯誤-WC名單匯入

■ 查看Logs

- 路徑D:\PATRIOTOFFICER\PATRIOTOFFICER_FILES\EXE\Logs (預設)
- 檔名WC_ExtractList.log

■ 常見問題類型

- 名單晚到：檔案到檔時間比名單匯入排程時間晚
- 連線異常
- 記憶體滿了

常見錯誤-ETL匯入異常

■ 查看Logs

- 路徑D:\PATRIOT_OFFICER_ETL_FILES
- 檔名TriggerDataLoad.log

■ 常見問題類型

- 資料內容或資料型別錯誤(例如：數字欄位給字元資料、必填欄位為空等)
- 資料長度超過原廠提供的Spec定義
- 資料欄位數目不足(例如：資料錯誤導致斷行)

常見錯誤-SWIFT未回覆

■ 查看資料庫狀態

```
2 SELECT TOP 10 CREATEDDATE,Progress,Block4_UserReference,* FROM MESSAGEDATABASE..SWIFT_MTRAW A  
3 ORDER BY A.CREATEDDATE DESC
```

■ 狀態說明

- NEW : 新電文
- PARSER : 檢核電文
- SPLIT : 切割電文
- RELEASE1 : 未命中直接放行
- HOLD : 命中
- RELEASE2 : 人工審查後可放行
- REJECT : 人工審查後不可放行





■ 狀態未改變可能原因

- 一段時間內電文量超過AML系統可負荷數量
- AML SWIFT相關服務異常





SWIFT未回覆-服務重啟順序

- 若確認為SWIFT服務異常，則須申請權限重新啟動相關服務

- 開啟順序

 PATRIOT OFFICER Service Helper	4
 PATRIOT OFFICER SWIFT Database Service	1
 PATRIOT OFFICER SWIFT Name Splitter	2
 PATRIOT OFFICER SWIFT Parser	3

- 關閉順序

 PATRIOT OFFICER Service Helper	1
 PATRIOT OFFICER SWIFT Database Service	4
 PATRIOT OFFICER SWIFT Name Splitter	3
 PATRIOT OFFICER SWIFT Parser	2

■ 查看SWIFT程式Log

- 程式名稱
 - PATRIOT OFFICER Service Helper
 - PATRIOT OFFICER SWIFT Database Service
 - PATRIOT OFFICER SWIFT Processor
- Log路徑：C:\Program Files\GlobalVision Systems\AML應用程式\Logs(預設)

常見錯誤-NameCheck Web Service

■ 確認站台

- 確認IIS站台NameCheckService服務狀態為【已啟動】

■ 查看程式Log

- 程式名稱-PATRIOT OFFICER Detection Worker
 - Log路徑：D:\Logs\Worker
- 程式名稱-Namecheck Processor
 - Log路徑：D:\Logs\Namecheck

常見錯誤-批次姓名檢核

■ 確認服務狀態

- IIS站台FTP服務狀態為【已啟動】

■ 查看程式Log

- 程式名稱-PATRIOT OFFICER Detection Worker
 - Log路徑：D:\Logs\Worker
- 程式名稱-Namecheck Processor
 - Log路徑：D:\Logs\Namecheck

Q&A

