輕鬆落實資料庫存取軌跡

完整紀錄非法及高權使用者的存取行為

撰稿：叡揚資訊 資訊安全事業處

資料庫稽核的重要性

自個資法實施後，除了擴大適用範圍到所有產業外，企業須面臨高額的罰金與刑事責任。資料庫內包含員工、個人資料與企業核心資料，對於敏感性資料的查詢、新增、修改、刪除，都必須連接到資料庫進行工作，非法使用者進入資料庫的行為，一直是資料庫人員最大的挑戰，對資料庫使用者活動狀況並進行管控相當重要，如 SQL Injection 的攻擊手法最為常見，資料庫中的個人機敏資料將全數公開，故選擇一套最符合公司的工具，將是目前優先需要考量的工作，本次將介紹資料庫稽核工具，並以實例展示資料庫活動狀況監控。

傳統資料庫稽核工作面臨的挑戰

1. 資料庫管理人員對於資訊安全觀念不足
2. 使用資料庫稽核工作是否會影響目前資料庫效能
3. 資料庫內建稽核機制管理檢視不易
4. 欠缺集中統一管理報表顯示

採用資料庫內建稽核機制的困難

1. 公司使用資料庫種類多 - Oracle、SQL Server、Sybase、MySQL
2. 資料庫管理人員需同時管理多個資料庫
3. 不同資料庫種類稽核機制設定管理方式不同且複雜
4. 資料庫效能影響程度無標準

市面上多款資料庫稽核工具選擇條件

1. 資料庫規模、數量、種類，例如某公司有 5-10 個資料庫管控需求
2. 是否需要開啟資料庫內建稽核機制 (效能考量)
3. 能否提供證據保全的「公正」及「不可否認」性
4. 選擇軟體式 / 硬體式解決方案

輕鬆落實資料庫存取軌跡 -Fortinet FortiDB 資料庫稽核工具介紹

FortiDB 為從小到大規模的企業提供了快速實施，易於管理，且有效成本控制資料庫的安全性和法規遵從解決方案。漏洞掃瞄，監控和資料庫稽核活動，並生成合法規之報告。直觀的來自 Web Browser 的界面，配置便捷，最大限度地減少資料庫管理員和 IT 人員的管理負擔。

● 多種資料收集方式：

FortiDB 提供多種資料收集方式，包含 TCP/IP Sniffer、Native Audit、Net Agent，協助提供不同的環境建置、部署容易，為資料庫提供簡易的管理介面，中央管理介面檢視環境資訊 DashBoard 儀表版，Web Browser 介面管理，企業架構中只需有一台 FortiDB 即可完成全部資料庫稽核工作，並可監控本地端資料庫及遠端資料庫，同時支援網路監聽模式及代理程式解決方案，適用於雲端虛擬化資料庫及非虛擬化資料庫。

● 弱點評估 (Vulnerability Assessment)：

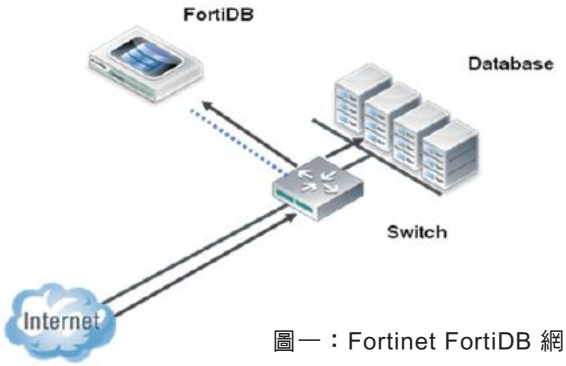
可掃描資料庫及作業系統存在之安全性弱點，例如資料庫參數值設定過大、過小，資料庫使用者密碼未設定及使用預設密碼等，皆可掃描出並提供資料庫安全保護之依據，並依照 Critical、Major、Minor、Cautionary、Information 呈現弱點分類及提供安全建議改善作法。

● 資料庫活動狀況監控 (DB Activity Monitoring)：

可記錄使用者連線資料庫存取之動作，例 SQL 語法 Select、Insert、Update、Delete、Drop、Alter、Create、Grant 等之指令，提供管理人員檢視是否有非法使用者存取資料庫的使用者活動特徵 – Activity Profiling，提供稽核功能的 Activity Auditing 檢視使用者存取資料庫行為，產生相符 SOC、PCI 法規之報表。

Fortinet FortiDB 網路監聽模式

TCP/IP Sniffer 的運作方式，在 Internet 到 Database 資料庫的網路連線中，利用 Switch Sniffer 將封包複製於 FortiDB 進行稽核工作。



圖一：Fortinet FortiDB 網路監聽模式運作圖

Fortinet FortiDB 實際使用案例一

使用者 pepa 連線到 SQL Server Database 對表格查詢 Select 資料

記錄使用者登入登出資料庫時間及所執行過的軌跡

圖二：Fortinet FortiDB 使用案例一

Fortinet FortiDB 實際使用案例二

使用者 pepa 連線到 SQL Server Database 執行正常操作

條件設為執行 DDL (Create、Alter、Drop) 語法則發送通知警示訊息管理者

圖三：Fortinet FortiDB 使用案例二

關於 Fortinet

Fortinet 為 UTM 解決方案全球領導者與網路安全領導供應商。Fortinet 產品與線上安全服務能提供全方位、整合與高效能的防護，不僅能抵禦不斷變化的安全威脅，並可同時簡化資訊安全架構。