

資安利器 - Quest InTrust 簡介

一、資料稽核的重要性

近年來，無論是各國政府官方的統計、或民間具公信力之市調機構(如 Gartner, Forrester)所做的調查，都指出企業因內部、或外部不當存取資料而導致之資料外洩、毀損或遺失，其損失幅度年年攀升。而之前被認為最有能力管理並控制資料安全的專業人員(如 DBA)，反而被發現經由他們所造成的不當資料存取，高達整體的八成。因此，制定一套新的、且能有效稽核並審計資料的系統，好讓專業人員能據以找出所有對資料威脅的來源，進而設定安全的資料存取與防護機制，乃成了當前之急務。

目前已經制定出的、且廣為政府與大型機構所採用的安全規範規格大概有：PCI、SOX 等等。而根據這些規格所設計出來的專業資料庫稽核工具也愈來愈多，像是 Gardium、Indera、Lumingent、以及 Quest InTrust 等等。如何針對企業的需求挑選出最適當的稽核工具將會是資安人員或 DBA 們愈來愈重要的一項工作。

二、如何評估 Auditing 工具

通常在評估一個資料庫稽核工具時，會考量下列這三點：此工具如何取得稽核資料？此工具如何進行稽核工作？以及此工具如何儲存稽核資料？茲分述如下：

如何取得資料

很多工具傾向於直接套用資料庫系統本身一些現有的功能來取得所要稽核的資料。例如直接透過 Oracle 的 Log Miner 或結合 SQL Server 的 Trace 功能來捕捉重要的資料庫活動。若資料庫本身沒有提供上述類似的功能，則可能改用 Trigger 的方式來感應資料庫上所有實際發生的事件。

這樣做的好處是工具廠商不必花太多資源額外設計新功能，直接套用資料庫現有功能即可。如此一來無論是產品成本、或將來使用者的學習成本都得以降到最低。但缺點則是，由於混合了稽核系統與資料庫系統，DBA 因此可以隨時將部份功能停用或關閉，容易造成監控上的漏洞。有鑒於 DBA 的很多動作正是造成資料外洩的主因，任何會把 DBA 排除在稽核對象外的系統將來都會有嚴重的潛在危險。此外，別忘了以 Log Miner 為主的技術還有一個盲點，就是一些不會被 Log 的、或者 Read Only 的 SQL 活動是無法被偵測到的。另外，由於呼叫了資料庫系統的某些功能，因此額外加重了資料庫系統的負擔(尤以 Trigger 為最)，這對某些負載已經很重的 OLTP 系統來說，幾乎是無法承受的。

Aug 08 M-Power eNew

本篇文章版權為倍力資訊股份有限公司所有，未經書面同意，嚴禁複製、轉載

有鑒於此，很多的稽核工具廠商已經開始揚棄套用現成資料庫工具的方式，而改用獨立研發的技術來取得稽核資料。例如透過 Network Sniffer 的技術、或透過代理程式 Agent 的技術等等。而這其中又以 Agent 技術為佳。這是因為很多 Network Sniffer 技術會要求資料庫主機額外安裝許多核心層級(Kernel-Level)的 Driver，先不提安裝及移除不易，很多時候許多作業系統甚至根本就無法安裝這種 Driver，因此會有蠻嚴重的版本衝突問題。而就算安裝好了，目前很多 Network Sniffer 技術只能針對『Network』活動進行偵測，若是經由 Local 端存取資料庫，則會成爲此類工具無法感應的盲點。而 Agent 程式通常不牽涉到核心層級，只是簡單的透過一般應用程式安裝方式安裝，較無與作業系統版本衝突的問題。而且效能較佳、也比較沒有偵測上的盲點。

如何進行稽核

關於這一點，各家廠商實作的方式相當多樣。有的工具爲了減輕資料庫系統的負擔，因此採用了所謂表列法的方式來決定到底要監控、稽核哪些項目。目的就是想盡量降低對資料庫帶來的效能衝擊。此方法的缺點很顯而易見的就是潛在的危險相當大(誰敢保證威脅只出現在『表列』的項目中)。

另外，很多工具所謂的『稽核』，只是把蒐集監控到的資料以報表的方式呈現出來，讓使用者自行決定後續處理方式。若使用者沒有規劃出一套相當嚴謹的後續稽核機制與步驟的話，經常整個稽核流程到了看完報表這一步就結束了。因此所使用的工具是否提供一個包含從開始取得稽核資料、直到負責審計的人員確定稽核結果爲止的完整流程，將會是個很重要的評估點。

如何儲存稽核資料

假如千辛萬苦蒐集了一堆稽核資料，也走了很多後續的審計流程，卻最後才發現這些資料被人竄改，那就完全失去了稽核的意義。因此當今主流的稽核工具多半會強調自己用以儲存稽核資料的儲存方式是很強固的、是所謂 Temper-Proof 的，就是要讓使用者對所產生的稽核結果有信心。

可是一旦真的仔細觀察這些號稱『Temper-Proof』工具的儲存方式，還是有些叫人無法放心的地方，尤其是當它把稽核儲存在『資料庫』裡的時候。姑且不論我們正是因爲擔心資料庫遭到不當存取所以要稽核審計；何況 DBA 對資料庫還擁有完整的控制權，隨時可以對這些稽核資料做出異動。因此較佳的稽核工具，應該要擁有獨立的儲存系統、並且擁有強固的加密系統，這樣才能真的達到 Temper-Proof 的程度。

三、 Quest InTrust 的優缺點

Aug 08 M-Power eNew

本篇文章版權爲倍力資訊股份有限公司所有，未經書面同意，嚴禁複製、轉載

在看完上面所提的用來評估稽核工具的三大主要考量點後，我們來比對一下 Quest InTrust 是否能通過這三項評估：

- InTrustg 是透過獨立式 Agent 來取得並傳送稽核資料，效能較佳、也較無偵測上的盲點。
- InTrust 並非採取表列式方式去稽核資料，而是會把所有資料庫上所發生的事件與活動全部捕捉下來並儲存。使用者可透過內建 Profile 所提供的稽核規則、或自訂 Profile 的規則來針對這些資料進行審計動作，因此幾乎沒有什麼漏網之魚。而且所提供的是從取得資料到審計完畢一氣呵成的完整流程，配合的都是獨立於資料庫系統外的技術，因此能將 DBA 等資料庫管理員也納入審計範圍內，達到近乎無死角的完全稽核。
- InTrust 使用獨立於資料庫外的儲存系統(Repository)，並結合強固的加密機制，使得稽核資料遭到入侵或篡改的機率降到最低；稽核結果的正確性提升到最高。

但即使 Quest InTrust 在經過三大評估項目的檢視得到相當好的評價，還是有一些相對於其他產品較為不足的缺點：

- 由於 InTrust 幾乎都使用獨立研發的技術，較能擺脫與資料庫現有技術的混用，但也因此增加了產品成本。不可諱言的，此產品在與其他同類性產品比較時，會顯得價格稍微昂貴。
- 由於 InTrust 進入市場較晚，能支援的資料庫版本也相對較少，目前僅提供針對 Oracle 與 SQL Server 的版本，但對其他平台版本的支援(如 DB2, Sybase...)已列為後續開發的重點。

四、 Quest InTrust 未來發展藍圖

- 將支援更多資料庫平台 (DB2, Sybase...)
- 將支援更多作業系統平台 (HP/UX Itanium...)
- 將提供更多報表工具(Federal View, Policy Extension...)
- 將提供更豐富的稽核工具(Work Flow Tracking, Remedy Integration...)