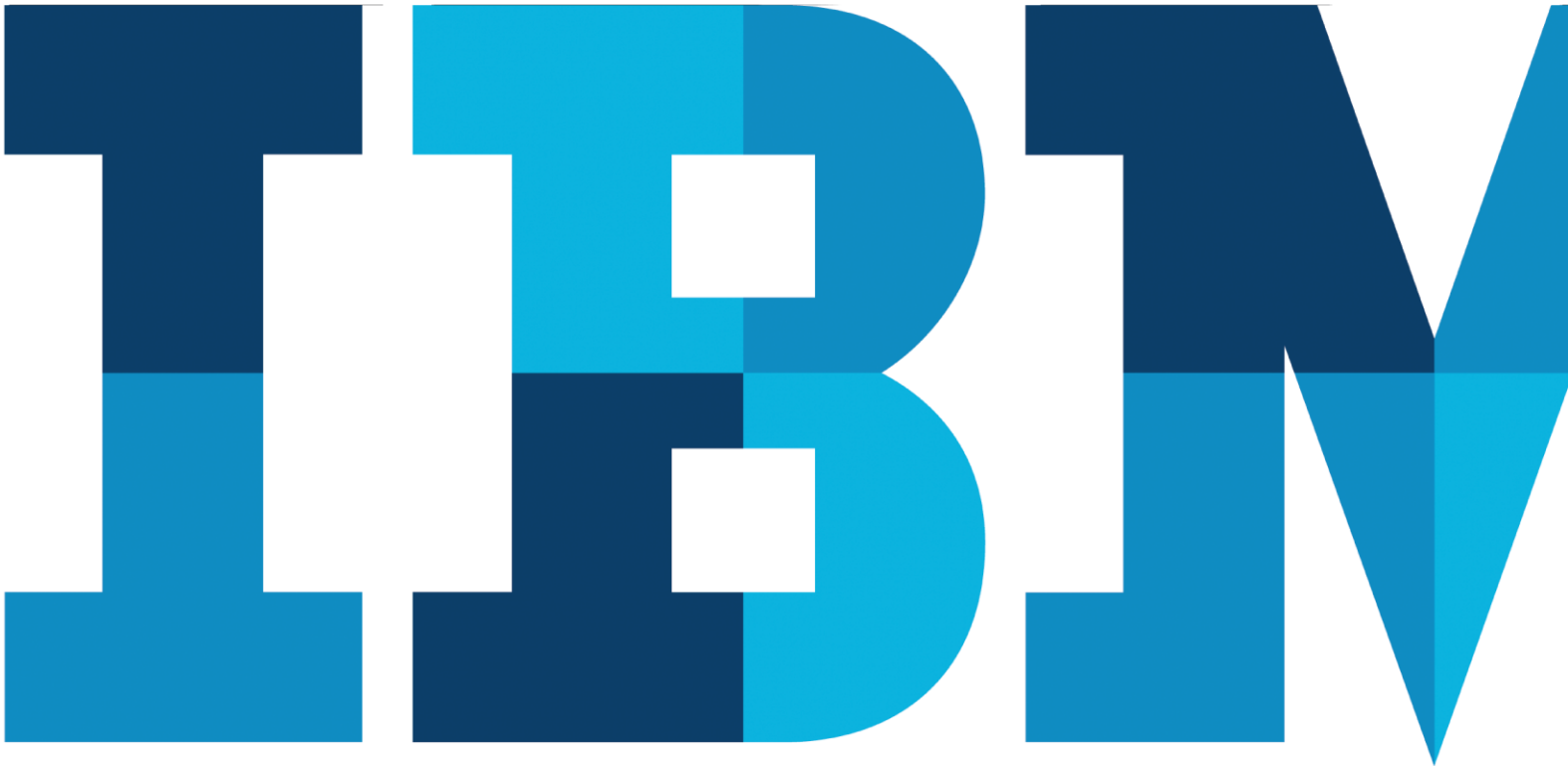
IBM InfoSphere Guardium
選用功能



目錄

InfoSphere Guardium 概觀

InfoSphere Guardium 可提供簡單但功能強大的解決方案，以保護整個應用程式和資料庫基礎架構，包括：

- 即時資料庫活動監視 (DAM)，可主動找出未獲授權或可疑的活動，防止特許使用者進行攻擊和封鎖未獲授權存取。
- 稽核與法規遵循解決方案，可自動化及簡化 PCI DSS、SOX、SAS70、ISO 27001/2、NIST 800-53 和資料隱私權規定的相關驗證活動。
- 變更控制解決方案，可防止未獲授權的資料庫、專用權及配置變更。
- 漏洞管理解決方案，可找出並解決資料庫漏洞，例如遺漏的修補程式、配置不當的專用權和預設帳戶。
- 詐欺防禦解決方案可提供應用程式層的監視，以識別應用程式使用者（SAP、PeopleSoft、Oracle EBS、Cognos 等）的未獲授權活動。
- 資料庫洩漏防禦解決方案，可找出機密資料並遏止資料中心入侵活動。

目前全球有超過 400 名客戶安裝此解決方案，包括 5 大全球銀行、 前 6 大保險公司中的 4 家、 頂尖政府機構、 前 3 大零售商中的 2 家、 20 家全球一流電信業者、 2 家全球最受歡迎的飲料品牌、 知名的 PC 業者、 前 3 大汽車製造商之一、 前 3 大航太公司之一，以及商業智慧軟體的領導供應商。 InfoSphere Guardium 是第一家解決核心資料安全漏洞的公司，可爲業界提供可調式企業平台，即時保護資料庫並自動化整個法規遵循審核程序。

此解決方案簡介將提供 InfoSphere Guardium 的多種選用功能概觀。如需 InfoSphere Guardium 核心解決方案的完整概觀，請參閱 InfoSphere Guardium 手冊。

Guardium 是 IBM InfoSphere 整合平台的一部分，此整合平台可定義、整合、保護及管理系統的可靠資訊。InfoSphere Platform 可根據共用中介資料與模式的核心整合，提供可靠資訊的所有基礎建置區塊，包括資料整合、資料倉儲、主要資料管理，以及資訊控管。此模組化產品可讓您隨時啓用，並將 InfoSphere 軟體建置區塊與其他供應商的元件混合搭配使用，或選擇同時部署多個建置區塊，以提高速度和價值。InfoSphere Platform 可爲資訊密集的專案提供企業級基礎，以簡化難題並爲企業快速提供可靠資訊，進而達到最佳效能、可調整性、可靠性及加速功能。

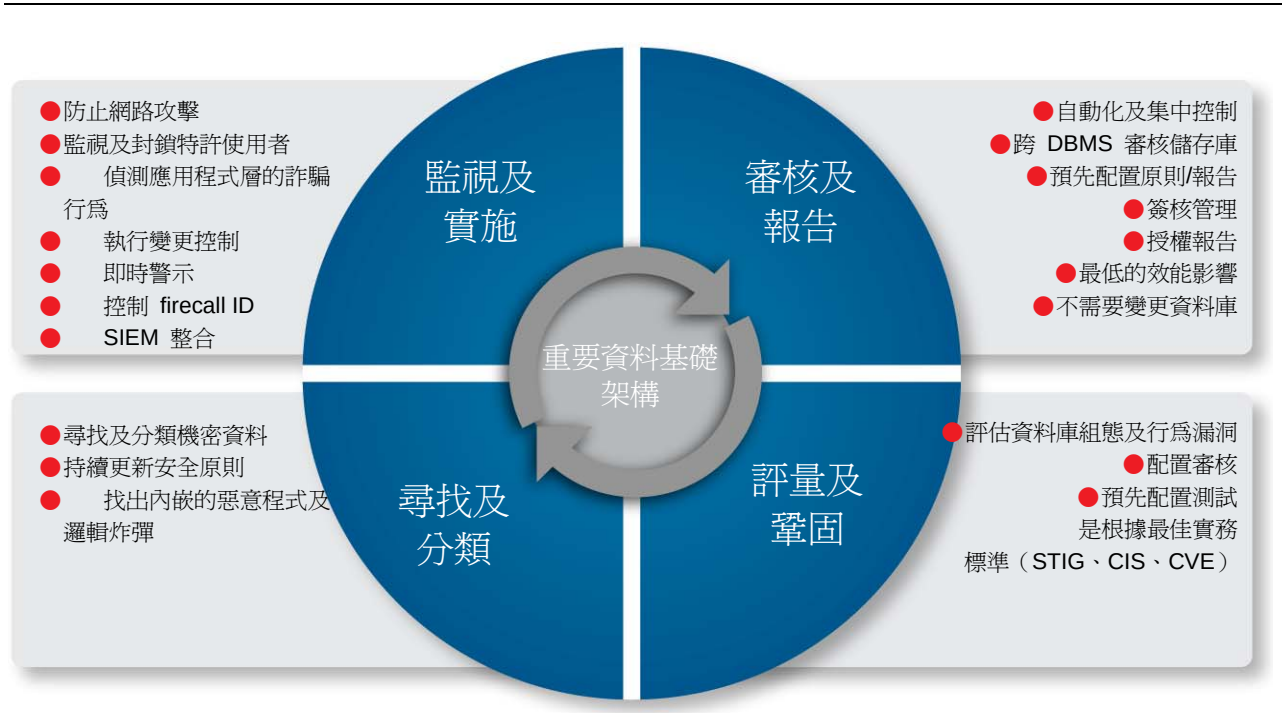


圖 1 ：InfoSphere Guardium 以單一統一主控台和後端資料儲存庫爲基礎，提供一系列整合模組，以管理整個資料庫安全及法規遵循生命週期。

Advanced Compliance Workflow Automation

自動化監督程序，以降低營運成本

- 可集中和自動化企業層面的監督程序，包括報告產生、分發、電子簽核和呈報
- 可指定獨特的工作流程步驟、動作和使用者組合，輕鬆建立自訂程序
- 以報表行項目爲基礎自動執行監督程序，發揮最佳的程序效率，而不影響安全
- 可確保監督小組成員只能看到本身職責相關的資料和工作
- 可使用即時的集中化程序管理工具，改善程序效率
- 可將程序結果與法規遵循和鑑識所需的精細審核資料，一起存放在安全的集中儲存庫中

管理企業層面的監督程序

隨著法規要求越來越多，以及對資料安全和隱私權的重視，組織已部署各種程序來審查定期排程的監視活動結果，並且深入調查及補救違反控管原則的事件。例如，組織可能要每天審查事件報告，每週定期執行和審查資料庫漏洞評量和資料庫探索程序。

多數企業都有數百、甚至成千上萬的資料庫，這些資料庫是由安全和 IT 團隊等部門所管理及監督。因此，可能是按照部門、地區、系統功能及其他因素分別管理。這種複雜的管理方式通常會直接影響監督程序；而不同的監督程序都有各自的審查步驟、行動和參與者。

手動程序會增加營運成本和審核異常

一般上，組織會手動管理本身的監督程序，使用電子郵件及試算表等工具來記錄事件、分發資訊給相關人員，以進行調查、取得補救活動和記錄備註。由於程序種類繁多且複雜，以致營運成本高，而且會經常發生程序中斷所引起的審核異常。加上監督資訊的儲存格式各異，有時還存放在不同的實體位置，擷取鑑識所需的歷程結果也變得十分困難。

自動化監督程序，以改善營運效率

Advanced Compliance Workflow Automation 模組可自動化整個安全和法規遵循工作流程，不必進行手動作業，還可即時完成監督活動。容易使用的圖形使用者介面可建立各種程序，以滿足相關作業和個人的獨特需求。只要透過下列幾個簡單步驟，即可建立新程序：

1. 建立由個別事件狀態和動作組成的自訂工作流程（請參見圖 2）。
2. 將一或多個個人或角色指派給要執行的動作。這些動作可選擇要求電子簽核。允許平行動作，以支援因不同準則而細分動作的程序（例如，不同 DBMS 產生的異常審查可能會由不同人簽核）。
3. 建立及排程審核程序，定期自動執行工作流程（請參見圖 3）。
4. 將任何作業組合加入各審核程序。例如，每週使用相同工作流程執行和審查的數個報告，可指派給相同審核作業。支援多種審核作業，包括審查自動產生的漏洞評量結果、資產探索、資料分類、配置審核及資料庫活動監視報告。

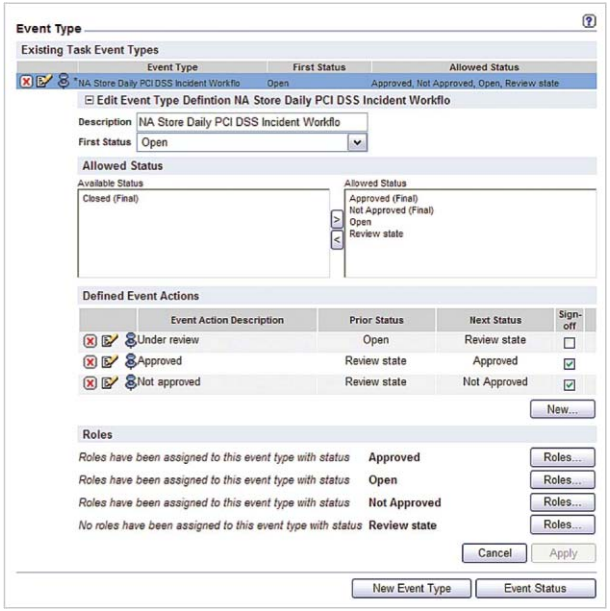


圖 2 ：InfoSphere Guardium 的 Advanced Compliance Workflow Automation 模組可讓使用者輕鬆建立工作流程，透過簡單的圖形使用者介面，指定適當的動作、事件狀態和角色組合，以自訂本身的獨特程序。

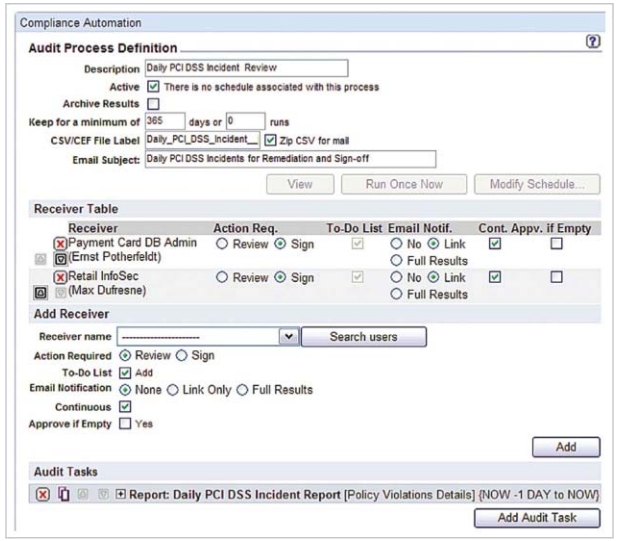


圖 3 ：工作流程可自動按照排程開始實施，以確保持續執行並追蹤重複發生的作業，如每日事件審查和漏洞評量。

透過精細的工作流程控制，提高安全性

執行工作流程時，系統會使用自動電子郵件通知和 InfoSphere Guardium 網頁介面的「待辦事項」(To-Do) 清單更新項目，通知動作負責人必須執行的特定動作。所有必要動作都可以透過網頁安全執行，包括審查結果、進行核准、提出意見及動作升級。

動作是根據行項目執行，因此可完成快速又全面的審查，並確保程序不會因爲需要調查的個別行項目而受阻。例如，工作人員收到的每日 PCI DSS 異常報告有五個事件，其中四件是已經解決的問題所造成的。此時，即可快速將這四行項目標示爲已審查並核准；而第五項則會在事件完成調查及解決後才核准。在工作流程中，這四個核准項目會立即繼續下一步；然後才執行第五項。您也可以行項目的方式，加入說明已採取補救措施的註解。

爲了達到最佳安全性及支援職權分立原則，參與工作流程的每個人只可看到本身職責相關的資訊。指派的職責分爲兩種。一種是工作流程相關職責，如上所述。負責人只能看到透過工作流程定義指派給他們的動作相關資訊。

另一種是核心 InfoSphere Guardium 系統內建的存取控制機制相關職責，該系統可讓管理員將特定資料庫或系統的職責（或角色）指派給個人及其各級管理層。以下簡單範例可說明此功能的好處。假設某工作流程的目的是審查定期 Database Vulnerability Assessment 結果，流程的第一步是讓 DBA 群組審查測試結果。授與 DBA 群組成員 Martha 所有財務資料庫的 InfoSphere Guardium 權限，Martha 只能查看財務資料庫的相關測試結果，而僅有付款卡資料庫權限的 Patrick 則只能查看相關結果。InfoSphere Guardium 可定義包含平行動作的有效工作流程，而不影響安全性或讓使用者接收太多與職責不相關的資訊。

透過企業層面的管理提高可靠性

工作流程管理者可即時檢視各審核工作的企業狀態，包括根據負責人、目前的動作狀態及備註檢視所需動作。這個功能強大的介面可提供必要資訊，以有效管理異質資料庫基礎架構與分散團隊的監督程序、提高可靠性並減少審核異常。

審核程序結果會與審核資料一起儲存在 InfoSphere Guardium 的安全儲存庫中，讓組織輕鬆提供審核者確實的審核追蹤，證明公司有持續執行所有必要工作。準確的保存功能可自動且安全地保存儲存庫，以支援最嚴格的記錄保存要求，亦可根據審核者或鑑識調查的要求進行還原。

InfoSphere Guardium 的 Advanced Compliance Workflow Automation 可讓組織自動化並精簡法規遵循程序，以降低營運成本和簡化順利通過審核的準備工作，即使是營運需求獨特的複雜環境也適用。

Database Vulnerability Assessment

根據最佳實務的詳盡自動化測試

- 掃描指定的資料庫群組
- 檢查是否有一般漏洞，如遺漏的修補程式、低保護性密碼、配置不當的專用權和預設供應商帳戶
- 隨附由網路安全中心 (Center for Internet Security, CIS) 和美國國防部 (DoD) 根據最佳實務開發的數百個預先配置測試
- 可產生安全性能報告卡，並建議加強資料庫安全性的具體行動計畫
- 大型環境的簡化部署，可透過指令碼介面自動載入多個資料來源（DB 名稱、類型、伺服器 IP、連接埠、角色）並連結至評量

改善資料庫安全和法規遵循

定期執行資料庫環境的安全評量，是保護資料庫基礎架構、遵守法規及通過審核的最佳方法之一。

安全評量會評估資料庫環境的安全強度，並與業界最佳實務比較。這些深度評估作業會檢視修補程式層級及資料庫配置，以突顯環境漏洞；如此一來，您便可快速補救問題及防止重要企業資料受到內外部威脅。

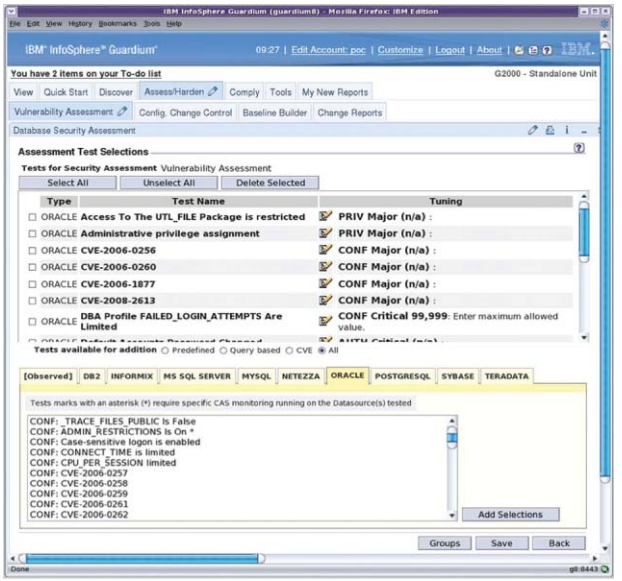


圖 4 ：InfoSphere Guardium 的 Database Vulnerability Assessment 模組會掃描您的資料庫基礎架構，查看是否有遺漏的修補程式、配置不當的專用權及其他漏洞。其中包含隨附數百個預先配置測試的最佳實務庫，還可提供補救漏洞的建議，包括與外部資源相關聯的識別碼（如 CVE）。您也可以建立自訂測試及監督程序。

根據 CIS 和 DoD 最佳實務的預先配置測試

InfoSphere Guardium 的 Database Vulnerability Assessment (VA) 模組會掃描資料庫基礎架構，查看是否有漏洞，並使用即時及歷程資料，提供安全狀況的後續評估。

InfoSphere Guardium VA 隨附根據業界最佳實務的預先配置測試庫（請參見圖 4）。這些最佳實務包括 Computer Internet Security (CIS) 指標和美國國防部制定的資料庫安全技術實作手冊 (Database Security Technical Implementation Guide, STIG)。這些測試會檢查是否有一般漏洞，如遺漏的修補程式、低保護性密碼、配置不當的專用權、預設帳戶，以及各 DBMS 平台的獨特漏洞。

InfoSphere Guardium 的 Knowledge Base Service 每季會定期更新這些測試。您也可以定義自訂測試（請參見圖 5），並排程包含掃描、分發報告、電子簽核及呈報的自動化審核工作。

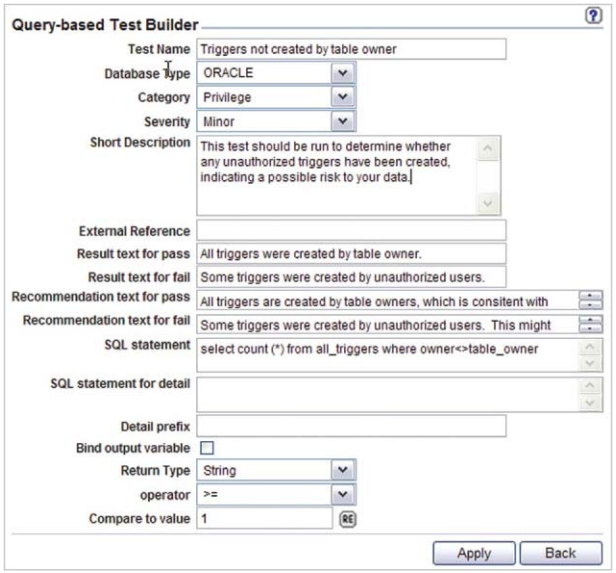


圖 5 ：表單型測試建置器可輕鬆建立使用 SQL 查詢的自訂測試。您也可以使用 OS 指令碼和 Java 類別建立自訂測試。

除了使用往下探查功能產生詳細報告（請參見圖 6），評量模組還會針對各漏洞建議具體行動計畫，協助您加強安全性。例如，如果專用權有問題，系統會通知您應該撤消哪一個專用權，以符合最佳實務。測試結果還包括參考資料，如與外部資源相關的 CVE 識別碼。

補救有漏洞的系統之後，組織必須確保只可以進行授權的變更。一旦建立安全的配置基準線後，InfoSphere Guardium 的 Configuration Audit System (CAS) 便可監視系統是否有變更。

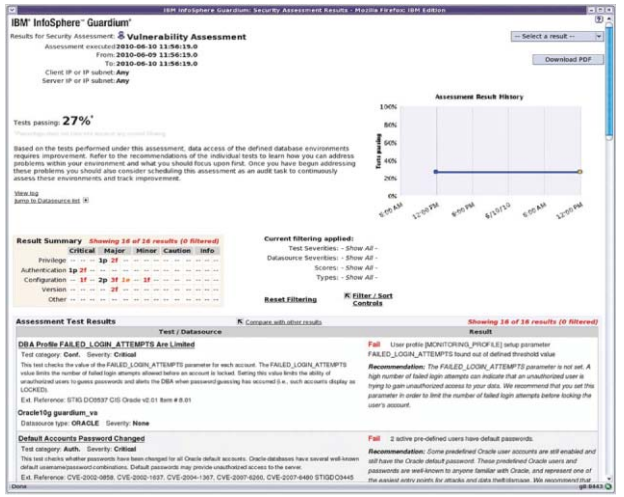


圖 6 ：InfoSphere Guardium 的 Database Vulnerability Assessment 模組可產生讓您瞭解整體安全狀況的摘要結果，以及包含具體改善建議的詳細逐層分析。

廣泛多元的精細測試

評量分爲幾大類：

- **專用權：**檢查物件建立與使用權限、授與 DBA 和使用者的專用權，以及系統層次權限。
- **鑑別：**驗證密碼原則、預設供應商帳戶、沒有空密碼、遠端登入參數等。
- **配置：**檢查特定平台的變數，如 DBA 基本資料的登入失敗次數上限 (Oracle)、不允許更新系統表格 (MS-SQL) 並確保已定義 SYSADM_GROUP (DB2)。
- **版本：**驗證適當版本號碼和修補程式層級。
- **行爲：**這些測試會利用 InfoSphere Guardium 的即時活動監視功能，找出受監視行爲的漏洞，如下班時間登入太多次、登入失敗、執行特許指令，以及共用特許認證。
- **檔案許可權：**檢查重要物件（如資料庫起始位置目錄）、配置檔（如 sqlnet.ora），以及登錄或環境變數的許可權。

多種評量技術不影響執行時間或效能

InfoSphere Guardium VA 是業界獨一無二的產品，結合三種重要的偵測方法，可針對各種漏洞和威脅提供詳盡的保護：

- **掃描：**系統會使用經過認證的方式（唯讀）存取資料庫，以評量資料庫漏洞。
- **代理程式型掃描：**各資料庫伺服器所安裝的輕量型代理程式可找出遠端無法判斷的漏洞，如重要 OS 和資料庫配置檔與指令碼（需要 CAS）的檔案許可權。
- **被動網路監視：**系統會即時觀察所有資料庫交易，如過多的資料庫錯誤（表示可能受到 SQL 資料隱碼攻擊）、共用管理帳戶和服務 ID 的使用情形，或預設供應商帳戶的使用情形，以找出漏洞。

最重要的是，InfoSphere Guardium 的漏洞評量可提供完整的平台保護（請參見圖 7），而不影響效能或重要系統的穩定性。系統不會模仿駭客進行入侵攻擊而導致系統當機，也不使用可能會產生額外支出的傳統資料庫日誌或原生審核功能。

資料庫支援
Oracle
Microsoft SQL Server 2000、2005、2008
IBM DB2（LUW 和 z/OS）
IBM Informix
Sybase
Oracle MySQL
Teradata
PostgreSQL
Netezza

圖 7 ：InfoSphere Guardium 可提供鞏固整個資料庫基礎架構的簡單方法，以便所有主要 DBMS 平台都可使用 Vulnerability Assessment 功能。

不僅是簡單的報告功能，還可因應整個漏洞管理生命週期

InfoSphere Guardium 的 Database Vulnerability Assessment 模組已緊密整合平台中的其他模組，可讓您透過單一統一的 Web 主控台、後端資料儲存庫和工作流程自動化系統，管理整個資料庫的安全和法規遵循生命週期。

這項整合不僅可提供企業簡單的漏洞報告功能，還能應付整個端對端漏洞管理程序，如評量和規避商業風險、排定補救活動的優先順序，以及簡化法規遵循報告和監督程序。特別是，InfoSphere Guardium 還可讓您快速達到以下目標：

- **找出資料庫漏洞：**未修正和配置不當的資料庫會導致龐大風險。InfoSphere Guardium VA 已納入根據業界最佳實務的大量評量測試庫，以找出漏洞。季度 Knowledge Base Service 也可確定評量測試保持最新狀態。
- **透過即時控制保護未修正的系統：**有漏洞的系統可能要花 3-6 個月時間修正。InfoSphere Guardium 即可透過活動監視、簽章型原則和預防控制，保護資料庫直到修正爲止。原則和基準設定也能防止發生應用程式漏洞，如 SQL 資料隱碼攻擊和緩衝區溢位。例如，您可警示及/或封鎖非業務單位應用程式針對未修正程序發出的呼叫（可能是攻擊）。
- **根據商業風險排定補救活動的優先順序：**InfoSphere Guardium 的分類器模組可找出並分類企業資料庫中的機密資料，如信用卡號，而其基準設定功能則可分析受觀察行爲，以瞭解業務單位應用程式如何及何時存取有漏洞的資料庫。由於多數組織沒有足夠資源可同時修正全部有漏洞的系統，所以風險評量是排定補救活動優先順序的關鍵。
- **加強資料庫安全：**使用評量測試所提供的建議修復有漏洞的系統後，InfoSphere Guardium 的 CAS 會確保只有在授權的情況下才能變更資料庫，以加強配置安全。
- **記錄及精簡法規遵循：**審核者要確定公司會即時追蹤並解決事件。有了 InfoSphere Guardium 的事件管理和 Compliance Workflow Automation（請參見圖 8），您便可自動化報告分發、電子簽核與呈報，同時追蹤有漏洞系統的補救進度。

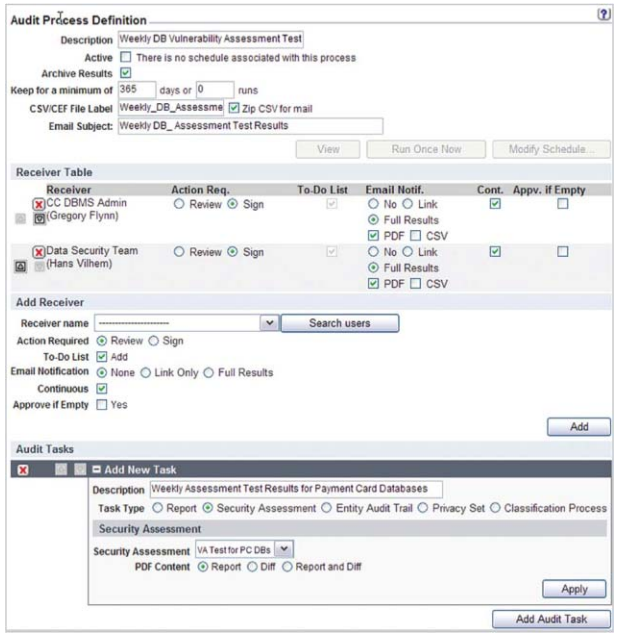


圖 8 ：審核者需要證據顯示組織有定義完善的程序，以保護重要資料。InfoSphere Guardium 的工作流程自動化模組可讓您定義自訂審核工作 (Audit Task)，自動執行排程的漏洞評量及報告分發、簽核與呈報。

Database Protection Knowledge Base

更新重複出現的內容，發揮最佳的保護和法規遵循功能

- 利用資料庫漏洞的最新資訊、最佳實務原則及企業應用程式中的機密表格，主動更新 InfoSphere Guardium 系統
- 將有安全風險的資料庫物件與套件最新資訊匯入漏洞物件群組，自動更新相關防禦原則
- 找出一般企業應用程式（如 SAP、Oracle EBS）中所需保護的機密表格，如包含 PCI DSS 或財務 (SOX) 資訊的表格，不需要花數小時維護人力
- 更新 InfoSphere Guardium 龐大的預先定義資料庫漏洞評量測試庫，以免承受最新威脅的風險
- 維護大量群組，以找出有安全和法規遵循需求的資料庫和應用程式物件，進而制定更準確原則

在快速變遷環境下保護機密資料的挑戰

各產業的組織都使用資料庫來儲存最寶貴的資訊，並搭配企業應用程式執行重要業務工作。因此，通常會部署資料庫保護和法規遵循解決方案，如 IBM 的 InfoSphere Guardium。

若要發揮 InfoSphere Guardium 的最佳保護功能，應定期更新群組、原則、測試及其他可配置參數，以因應不斷變化的資料庫基礎架構和相關威脅。例如，漏洞測試應該反映最新的攻擊和修補程式層級，而原則也應該包含機密和有漏洞物件的最新清單。

雖然管理員可透過手動方式輕鬆更改 InfoSphere Guardium 的可配置參數以說明相關變更，但通常缺乏執行所需的專業知識或時間。若要彙整綜合性的漏洞資訊，則需要受保護系統的技術知識，以及研究並整合業界攻擊資訊的能力。另一個困難則是隨時掌握各資料庫系統及一般企業中企業應用程式的變更。各有其專屬架構、說明文件和發行排程。然而，如果無法隨時反映這些參數的最新變更，可能會導致嚴重的安全和法規遵循漏洞。

善用 IBM 的專業知識和員工，達到最佳的保護和法規遵循

IBM InfoSphere Guardium Database Protection Knowledge Base 是一項年度服務，可爲用戶端提供支援資料庫和應用程式的相關最新內容（Guardium 消耗品格式），以達到最佳的保護和法規遵循。提供的內容包括：

- 軟體修補程式層級
- 版本等級
- 漏洞物件
- 機密物件（如含有 SOX、PII 或 PCI 資料的表格）
- 漏洞評量測試和識別碼
- 儲存程序
- 管理程式
- 指令、錯誤和使用者角色。

系統會使用廣泛的來源以找出此資訊，包括 IBM 內部研究、與其他供應商的關係，以及跨產業合作計畫，如 CVE。這些資訊經過彙整、封裝後會納入適當的 Guardium 元素（如漏洞測試、群組等），測試後便傳送到 InfoSphere Guardium 用戶端。

容易管理

Knowledge Base 通常會根據 DBMS 供應商的季度發佈排程，每季發佈相關更新。然而，視目前環境和風險分析而定，將有所例外。

只要按一下滑鼠即可輕鬆套用更新（請參見圖 9）。InfoSphere Guardium 內建的智慧型更新程序可提供特定使用者自訂作業。如果使用者新增了物件，系統會在更新過程中識別該動作並加以保留。例如，如果企業應用程式已經過自訂，則可能新增物件至相關 PCI 群組，以確保反映該自訂作業。在下一次更新時，InfoSphere Guardium 就會在更新過程中確認已新增並保留該物件。

圖 9 ：只要按一下滑鼠，即可將 Database Protection Knowledge Base 服務定期提供的最新漏洞、審核及最佳實務庫納入 InfoSphere Guardium。

IBM 可提供立即納入 InfoSphere Guardium 的最新內容，不必手動更新內容，因此可將管理成本降至最低；同時，還確保原則和測試反映企業基礎架構和威脅狀態的最新資訊，以發揮最大的系統資料保護和法規遵循效益。

異質環境的詳細保護

InfoSphere Guardium Database Protection Knowledge Base 更新可爲所有主要平台提供內容（請參見圖 10），因此可輕鬆確定防禦原則是最新的，甚至是在多數組織常見的異質環境。系統會針對各平台提供多樣化的內容（如上所述），以實現廣泛用途，包括：

- **進行測試，以避免多數最新資料庫漏洞 1[1]：**更新後的 Vulnerability Assessment (VA) 測試可確保，最佳安全實務及各種法規遵循規定所要求的定期排程 VA 掃描可偵測資料庫基礎架構中各平台的最新漏洞（含遺漏的修補程式）。
- **法規遵循驗證：**PCI DSS 和 SOX 等法規會要求企業實施控管，以免未獲授權的機密資料變更及存取。SAP 和 Oracle EBS 的更新最佳實務審核庫也可透過 InfoSphere Guardium 輕鬆執行，不需要花數小時研究這些應用程式，以找出機密表格。
- **保護漏洞物件（虛擬修正）：**在多數組織中，從公布資料庫修補程式到安裝修補程式之間通常有明顯延誤。因此，如果組織希望將這段時間的風險降至最低，則可使用漏洞物件群組的更新資料輕鬆執行原則，以警示或封鎖非預期的漏洞物件存取，直到可以安裝修補程式爲止。

1 需要 Vulnerability Assessment 模組

有了 InfoSphere Guardium 的 Database Protection Knowledge Base 即可實現多種不同用途，包括使用機密儲存程序時發出警示，以及追蹤特定錯誤種類（可能是不當活動）。透過提供包含重要安全和法規遵循用途的相關群組最新資訊，InfoSphere Guardium 還可開發功能強大的控管機制，但不增加營運支出。

資料庫支援
Oracle
Microsoft SQL Server 2000、2005、2008
IBM DB2（LUW 和 z/OS）
IBM Informix
Sybase
Oracle MySQL
Teradata
PostgreSQL
Netezza

圖 10 ：InfoSphere Guardium Database Protection Knowledge Base 可提供廣泛的更新內容，包括所有主要資料庫平台的漏洞測試、機密物件、漏洞物件和最新修補程式資訊。

Data-Level Access Control

適用於異質 DBMS 環境的簡化預防控制

- 可防止特許使用者檢視或變更機密資料、建立新使用者帳戶或提升專用權
- 完全不影響應用程式層次的資料流量
- 可支援 IT 委外及相關成本節約，而且不增加風險
- 可針對 SOX、PCI、Basel II、資料隱私權規定，實施職權分立原則
- 可透過一組適用於異質 DBMS 基礎架構的精細存取原則，簡化安全和法規遵循
- 可利用集中且自動化的控管機制取代手動程序，加強作業效率

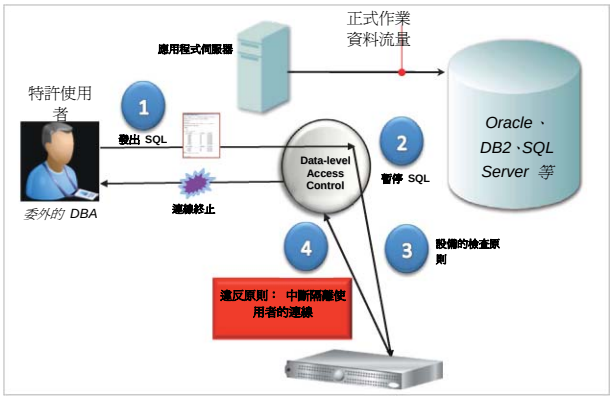
變更控制需求

「Gartner 預測，2008 年的金融危機將促使法規要求更嚴格。因此，不能再忽視風險管理和法規遵循問題。」[1]

對許多組織來說，除了管理風險、防止內部威脅及因應法規需求之外，以較少資源完成更多工作也越來越重要。

角色型存取和其他內建 DBMS 控制可防止終端使用者存取機密資料，但無法禁止可自由存取所有 SQL 指令和資料庫物件的特許使用者進行未獲授權存取。

資料庫活動監視 (DAM) 等較新技術可提供多一層的保護，在偵測到異常活動或違反存取原則（包括特許使用者違規）時，產生詳細的審核追蹤和即時安全警示。



角色及相關原則	DDL	DML	SELECT	CREATE/ALTER USER
PeopleSoft DBA	允許	允許	封鎖	封鎖
存取其他綱目的 DBA	封鎖	封鎖	封鎖	封鎖
使用 DBA 綱目的 DBA（sys、V$ 表格、調整）	封鎖	允許	允許	允許或封鎖
抄寫及備份	允許	允許	允許	封鎖
開發人員	封鎖	封鎖	封鎖	封鎖

圖 11 ：InfoSphere Guardium Data-Level Access Control 可透過一組精細原則簡化企業安全性，針對多個 DBMS 平台實施職權分立原則，而且不必中斷應用程式存取或變更資料庫配置。這是防止特許使用者（如 DBA、開發人員、委外人員及其他進階使用者）檢視或變更機密資料的唯一跨 DBMS 技術。InfoSphere Guardium Data-Level Access Control 可監視所有資料庫連線，包括特許使用者透過非 TCP 連線（Oracle BEQ、SHM、TLI、IPC 等）的本端存取。

儘管 DAM 是深入防禦策略的重要元素，但通常僅限於提供偵測控制，而非預防控制，因爲光是監視並不能執行安全原則，也無法防止未獲授權動作的發生。

即時預防控制；完全不影響 IT 基礎架構

InfoSphere Guardium Data-Level Access Control 是使用精細安全原則（請參見圖 12）執行的輕量主機型軟體代理程式（請參見圖 11），可提供自動化的即時控制，防止特許使用者執行未獲授權的動作，如：

- 針對機密表格執行查詢
- 變更機密資料值
- 在變更視窗以外新增或刪除重要表格（綱目變更）
- 建立新使用者帳戶及變更專用權

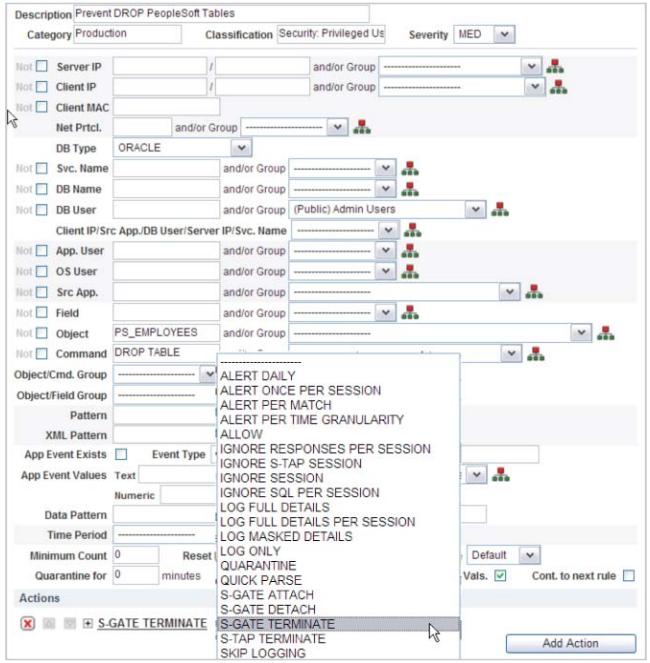
InfoSphere Guardium Data-Level Access Control 是非入侵式工具，不需要在資料庫內新增功能。因此，可以在不中斷 Oracle E-Business Suite、PeopleSoft、Siebel、SAP、Business Objects 和內部應用程式等重要業務應用程式的情況下，快速實作。

優於資料庫常駐控制之處

InfoSphere Guardium Data-Level Access Control 可提供優於資料庫常駐控制的強大功能，包括：

- **跨平台支援：**InfoSphere Guardium Data-Level Access Control 可讓組織定義一套適用於所有應用程式和資料庫基礎架構的存取原則，不僅是控制單一特定 DBMS 平台或版本的存取。由於 InfoSphere Guardium Data-Level Access Control 是在資料庫以外執行，所以可支援所有主要 DBMS 平台：Oracle、Microsoft SQL Server、IBM DB2、IBM Informix、Sybase、Oracle MySQL、Teradata、Netezza 及 PostgreSQL。

- **非 DBA 亦可輕鬆使用：**資料庫常駐控制需要 DBA 進行管理，因而產生職權分立的問題。InfoSphere Guardium Data-Level Access Control 卻可由 IT 安全、法規遵循或風險小組管理，因爲此工具使用可透過下拉功能表自訂的簡單英文原則，不需要資料庫指令和結構的相關知識。此外，InfoSphere Guardium Data-Level Access Control 使用加強的 Linux 網路設備來管理存取原則，防止特許使用者停用或變更原則，進一步鞏固職權分立。




```
[oracle~]$ sqlplus hr@ora10
SQL*Plus: Release 10.2.0.4.0 - Production on Tue Nov 25 14:16:13 2008
Copyright (c) 1982, 2007, Oracle.  All Rights Reserved.

Connected to: Oracle Database 10g Enterprise Edition Release 10.2.0.4.0
 - Production

SQL> SELECT * FROM PS_EMPLOYEES;

  ID FIRSTNAME            LASTNAME             STATUS
---- -------------------- -------------------- --------
 100 Robert               McBride              ACTIVE
 101 Linda                Jones                ACTIVE

SQL> DROP TABLE PS_EMPLOYEES;
DROP TABLE PS_EMPLOYEES
*
ERROR at line 1:
ORA-03113: end-of-file on communication channel

SQL> SELECT * FROM PS_EMPLOYEES;
ERROR:
ORA-03114: not connected to ORACLE
```

圖 12 ：InfoSphere Guardium 平台可支援精細的判斷原則，主動找出違規行爲（而非探索式地尋找錯誤）。這些原則是以特定階段作業屬性爲根據，如用戶端 IP 位址、MAC 位址、來源應用程式、DB 使用者、OS 使用者、應用程式使用者、當日時間、SQL 指令及表格名稱，且通常是使用預定群組來定義，以簡化後續管理。一旦違反原則，即可觸發多種原則動作，如即時警示（SMTP、SNMP、Syslog、CEF）、使用者隔離和終止連線（如上所示）。

- **原則強制執行及審核的單一解決方案：**爲了遵循法規，必須儲存所有特許使用者的完整動作審核追蹤，以記錄法規遵循情況和輔助鑑識調查。DBMS 供應商通常會提供精細的審核程序及審核儲存庫，作爲獨立附加程式。InfoSphere Guardium 在單一解決方案中提供了原則強制執行和精細審核，進一步降低成本和複雜性。
- **檢查查詢結果，不僅是送入查詢的原則：**資料庫常駐控管機制只能控制針對特定物件執行特定 SQL 指令。而 InfoSphere Guardium Data-Level Access Control 則還可檢查查詢結果（請參見圖 13）。例如，此工具可終止異常指令碼或應用程式嘗試從資料庫擷取 PII 的連線，或在調查時加以隔離，但允許有效應用程式擷取相同的 PII 資料。
- **全天候實施：**有些資料庫常駐控管機制必須關閉，才能進行備份和修正等例行維護作業。特許使用者可在這些維護期間，利用停用的控管機制來執行未獲授權的動作。InfoSphere Guardium Data-Level Access Control 不必停用資料庫內的特定特許帳戶，因此可全天候實施存取原則。

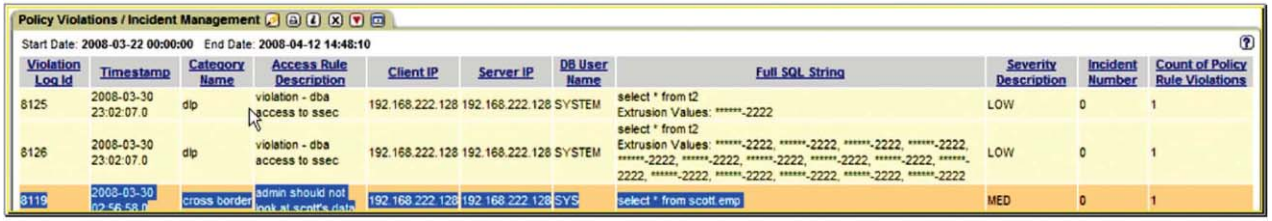


圖 13 ：外洩原則會檢查傳回資料（而非送入的 SQL 指令），以尋找類似 16 位數信用卡號碼或 9 位數社會保險號碼的數值模式。 輸出資料通常會先加以遮罩，再存入 InfoSphere Guardium 設備，作爲審核追蹤（如以上顯示的星號）。 您可定義原則動作（稱爲「S-TAP TERMINATE」）在偵測到查詢結果中的機密資料時終止連線，以免資料外洩（通常是幾十筆記錄）。 相形之下，「S-GATE TERMINATE」甚至可在 DBMS 針對特定資料庫物件執行 SQL 指令之前，便終止連線。

InfoSphere Guardium 主機型軟體探測器的延伸套件

Data-Level Access Control 是 InfoSphere Guardium 輕量主機型探測器 S-TAP™ (software tap) 的延伸套件。S-TAP 是業界獨一無二的非入侵式軟體探測器，可在資料庫伺服器的 OS 層次監視網路串流，包括特許使用者的網路存取和本端存取（透過共用記憶體、具名管道、Oracle Bequeath 等）。

S-TAP 會將所有資料流量轉送到個別 InfoSphere Guardium 設備，進行原則評估、分析、報告和安全的審核追蹤線上儲存，因此可將對伺服器的效能影響降至最低。

已經使用 S-TAP 的客戶可輕鬆升級到 InfoSphere Guardium Data-Level Access Control，以非常精細的方式開始實施存取控制，但不影響應用程式環境。

1 Gartner 發表的「Managing IT Risks During Cost-Cutting Periods」，Mark Nicolett、Paul Proctor、French Caldwell，2008 年 10 月 22 日。

Entitlement Reports

簡化異質資料庫環境中的使用者權限管理

- 可提供簡單的方式，以彙整及瞭解整個資料庫基礎架構的授權資訊
- 立即支援適用於所有主要作業系統的八大供應商資料庫平台
- 預先定義的報告，因應一般所需檢視
- 可充分整合其他 InfoSphere Guardium 模組，包括 Compliance Workflow Automation，以降低營運成本
- 減少手動處理的人力、提高資料安全性，並簡化是否遵循 SOX、PCI DSS 及資料隱私權等重要法規的驗證程序

管理資料庫使用者權限的難題

近年來，組織始終難以應付資料庫資訊的快速成長。其中一個難題就是執行有效的資料保護措施。一般而言，資料庫管理員 (DBA) 主要是依賴 DBMS 的原生授權功能來保護資料；根據使用者的工作需求，授與使用者最少的物件和系統專用權（授權）。基於可用的專用權十分廣泛、使用者帳戶和物件越來越多，加上管理階層式角色的複雜性，此作業需要龐大的人力資源。

然而，商業環境的改變也導致使用者授權管理越來越困難。靈活的組織比以往更需要經常變更角色和職責。而企業購併亦產生許多分散各地的不同供應商資料庫基礎架構，以致 DBA 必須應付各種供應商授權模式及大量不同系統。因此，保障資料庫專用權，以免不當使用機密物件和系統權限的工作變得十分困難。這不僅是資料保護問題，也是法規遵循問題。

審核者在驗證主要法規的遵循情況時，需要定期審查（有時亦稱資料庫使用者權限認證報告），以確保公司有根據人員、職責及實際使用情形的異動，定期調整使用者授權。

資料庫支援
Oracle
Microsoft SQL Server 2000、2005、2008
IBM DB2
IBM Informix
Sybase
Oracle MySQL
Teradata
PostgreSQL
Netezza

圖 14 ：InfoSphere Guardium Entitlement Reports 可提供簡單的方法，以收集並掌握異質資料庫基礎架構的使用者權限資訊。

自動化並集中授權資訊的收集

InfoSphere Guardium Entitlement Reports 可提供簡單的方法，以彙整並掌握整個組織的資料庫授權。您也可以配置選用軟體模組，依排程掃描基礎架構中的所有選定資料庫，自動收集使用者權限資訊，包括透過角色和群組會員資格授與的權限。如此一來，便不需要花時間檢查各資料庫，也不必逐一查看階層式角色（授與角色的角色），即可完全掌握授權情形。此外，還可透過定期且有系統的方式收集此資訊，不需要使用珍貴的技術資源，便能提供即時的精確資訊，以加強安全狀況、滿足審核者的要求並降低營運成本。

廣泛的預先配置報告

Entitlement Reports 選項可搭配各種常用 DBMS 的授權系統（請參見圖 14），以便透過有限且認證的唯讀存取權，擷取、瞭解和呈現從異質環境收集的資訊。[1] 各種預先定義報告（請參見圖 15 和 16）可提供不同的授權資料檢視方法，以便企業組織快速、輕鬆找出安全風險，如不當暴露的物件、權限過多的使用者及未獲授權的管理動作。大量預先定義報告的範例如下：

- 有系統專用權的帳戶
- 所有系統和管理專用權；按使用者和角色顯示
- 使用者的物件專用權
- 有 PUBLIC 存取權的所有物件
- 物件的使用者專用權
- 授與使用者與角色的角色
- 專用權授與和撤消
- 程序的執行專用權

ORA Accnts with BECOME USER

Start Date: **2010-07-02 11:50:00** End Date: **2010-07-09 11:50:00**
Aliases: **ON**

Grantee	Privilege	Admin Option	Datasource Name
BANKAPP	BECOME USER	NO	OCEAN ORACLE DB
JBROWN	BECOME USER	YES	OCEAN ORACLE DB
DBA	BECOME USER	YES	OCEAN ORACLE DB

圖 15 ：有了 InfoSphere Guardium Entitlement Reports，即可輕鬆找出擁有不當權限的使用者。在此報告中，JBROWN 擁有功能強大的 Oracle「BECOME USER」系統專用權，如果遭濫用，則可存取未獲授權的資訊或攻擊重要應用程式。

mssql2005/8 Accnt Of db_owner db_securityadmin Role

Start Date: **2010-07-02 15:13:14** End Date: **2010-07-09 15:13:14**
Aliases: **OFF**

Granted_Role	Grantee	SqlGuard Timestamp	Datasource Name	DB Name
db_owner	dbo	2010-07-09 15:02:12.0	MS SQL SVR PRIMARY 1433	financial
db_owner	dbo	2010-07-09 15:02:12.0	MS SQL SVR PRIMARY 1433	tempdb
db_owner	JBrown	2010-07-09 15:02:12.0	MS SQL SVR PRIMARY 1433	financial
db_securityadmin	JBrown	2010-07-09 15:02:12.0	MS SQL SVR PRIMARY 1433	financial

圖 16 ：InfoSphere Guardium 可彙整並顯示八大 DBMS 平台的授權資訊，如 SQL Server、Oracle 及 DB2。藉此簡化尋找不當授與角色的程序，如授與 JBrown 財務資料庫的 db_owner 和 db_security 管理角色。

1 透過需要有限（唯讀）專用權的 IBM 隨附指令碼登入資料庫，以收集授權資訊； 客戶可檢查此指令碼，判斷該專用權是否符合企業原則。

自動化安全和法規遵循的驗證活動

從資料庫基礎架構收集的所有授權資訊會與其他資料庫審核資訊，一起存放在 InfoSphere Guardium 的安全防竄改儲存庫中，以便 Report Builder、Policy Builder 和 Compliance Workflow Automation 應用程式等所有系統模組使用。只要使用直覺式的拖放介面，便可輕鬆建置自訂報告，以顯示預先定義報告沒有提供的特定視圖。Compliance Workflow Automation 還可自動產生需要定期審查的報告，然後分發給相關監督小組。此外，可以電子方式擷取備註、呈報及核准，然後存放在儲存庫中，供審核者使用。

InfoSphere Guardium 的原則監視和實施功能也可利用 Entitlement Reports 模組取得的資訊。授權資訊可用於自動匯入原則群組等方面。一般使用案例是自動更新未獲授權使用者嘗試存取重要人物 (VIP) 記錄時產生警示的原則。

如果員工正在接受洩露 VIP 記錄調查，調查期間通常會撤消其存取權，下一次定期排程更新相關報告時，就會自動反映在「授權使用者」(Authorized Users) 群組中。如果員工嘗試存取 VIP 記錄，就會產生警示，並記錄該事件以便調查。

降低營運成本並改善資料保護

InfoSphere Guardium Entitlement Reports 可提供簡單的方法，彙整、瞭解及利用使用者權限資料，以發揮最佳的機密資料保護、降低營運成本並確保通過審核。如此一來，就不需要花時間手動收集和分析使用者權限資訊，也可以避免手動作業容易發生的錯誤，快速找出重要的安全漏洞，同時降低營運成本。整合法規遵循工作流程與原則管理可進一步降低營運成本，並且證明公司有實施主動控管，以滿足審核者的嚴格要求。

Configuration Audit System for Database Servers

偵測影響資料庫安全的配置變更

- 可追蹤資料庫引擎範圍之外、會影響資料庫環境安全性的所有變更
- 可補強 InfoSphere Guardium 的 Database Activity Monitoring 模組，以提供詳盡的資料庫監視
- 追蹤可能會影響資料庫安全狀況的資料庫配置檔和其他外部物件變更，如
  - 環境/登錄變數
  - 配置檔（如 SQLNET.ORA、NAMES.ORA）
  - Shell 指令碼
  - OS 檔案
  - Java 程式等執行檔
- 所有控管和風險管理實作必備的工具；
- 可執行不需要管理員介入的最佳安全實務

保護資料庫環境

多數資料庫環境變更都是透過資料庫引擎執行。而且多數資料庫類型是透過 DBA 或（資料庫的）安全管理員執行的特殊化 SQL 指令或儲存程序，進行控制和配置。

有了 InfoSphere Guardium 的資料庫活動監視功能，即可輕鬆保護這些活動，讓您監視並審核所有資料庫活動（包括特許使用者動作），以及執行存取控制原則，而不影響效能，也不需要靠 DBMS 常駐日誌或審核功能。

此外，InfoSphere Guardium 的 Vulnerability Assessment 產品可評量資料庫的安全強度並突顯必須解決的弱點，如配置不當的參數、預設帳戶、必須套用修補程式的漏洞，以及需撤消的專用權。

不過，資料庫是安裝在作業系統層次的程式，可利用作業系統服務。許多配置元素是在作業系統結構中，而不是在資料庫本身。

例如，檔案、登錄值和環境變數。其中許多檔案和數值控制某些最重要的資料庫安全環節。資料庫鑑別方法就是一個很好的例子。因此，幾乎所有資料庫平台的管理員都可以透過變更值（無論是否使用 SQL），變更資料庫鑑別使用者的方法。

如果管理員變更及使用不安全的鑑別方法，可能會導致嚴重的安全漏洞。因此，必須加以監視及警示。

InfoSphere Guardium 的 Configuration Audit System for Database Servers (CAS) 可在各種層次追蹤所有資料庫變更，並向集中的 Web 型主控台報告這些變更。如果使用 CAS，安全管理員即可確定，任何可能影響安全性的變更都無法略過資料庫的 SQL 引擎。

若搭配使用 InfoSphere Guardium 的 Database Activity Monitoring 功能，則可爲業界資料庫提供唯一的全方位監視、審核及控制解決方案。

CAS 的功能

CAS 是輕量型代理程式，可在資料庫實例所安裝的伺服器上執行。CAS 可監視各種結構的所有變更，包含檔案變更、擁有權與權限定義、登錄值、環境變數及資料庫結構。

CAS 會根據使用者定義的時段及是否有變更來輪詢這些結構，然後通知 InfoSphere Guardium 伺服器哪一個元素已變更、新值爲何（與舊值比較）等。

CAS 會利用定義監視項目的範本執行作業。InfoSphere Guardium 系統包括一組預先定義的範本，這些範本可定義監視 Oracle、DB2、Sybase、SQL Server、Informix、MySQL、Netezza、Teradata 或 PostgreSQL 環境（請參見圖 17）的最佳實務。使用者可選擇範本和主機，將這些範本部署到伺服器，其餘作業則交給 CAS。

部署後，CAS 會將此範本擴展至實際的實例元素。例如，最佳安全實務通常要求您確保資料庫執行檔未遭變更。資料庫安裝有數十個執行檔，駭客可使用任一檔案來攻擊環境。舉例來說，駭客可用執行一般工作且存有使用者名稱與密碼的檔案版本，取代其中一個執行檔以進行讀取。內外部審核都規定，不得變更這些檔案。

CAS 也可追蹤其他值。例如，SQL Server 允許使用 SSL 加密資料庫通訊。此值是在不同的 SQL Server 公用程式中設定。最後，此值會存入標準的 Windows 登錄中（請參見圖 18）。Windows 管理員可透過簡單的變更輕鬆關閉傳輸中的資料，沒有人會察覺。CAS 範本可監視這些值，進一步確保強大的資料庫安全性。

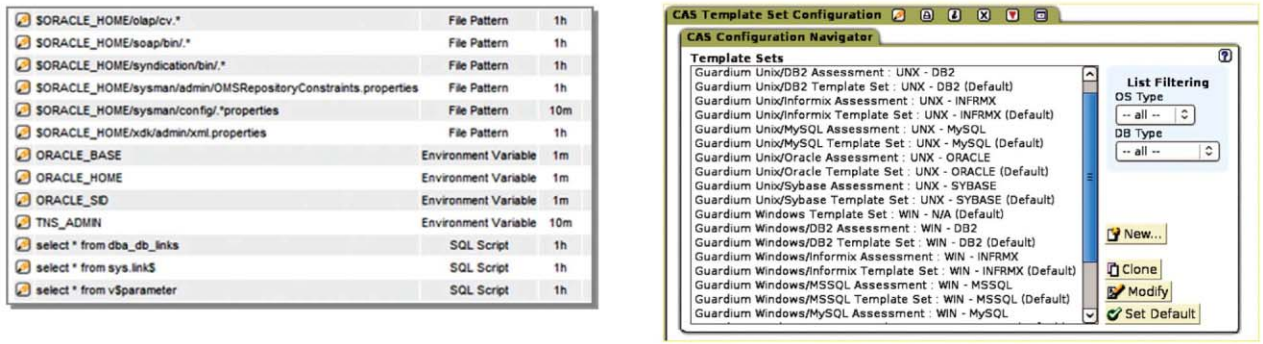


圖 17 ：InfoSphere Guardium 的 Configuration Audit System for Database Servers (CAS) 模組可追蹤可能會影響資料庫安全狀況的所有外部資料庫物件變更，如配置檔、環境與登錄變數、指令碼與執行檔。 爲了加速部署，CAS 還隨附最佳實務庫，其中有數百個預先配置的知識範本，適用於所有主要 OS 和 DBMS 組合。

除了檔案和登錄值變更，CAS 還可監視其他變更：

- 環境變數變更
- 檔案許可權變更。CAS 也可驗證檔案許可權的設定沒有超過特定限制
- 檔案所有權變更。CAS 也可驗證檔案所有權僅設定爲特定值
- 可查詢的任何資料庫元素變更
- 可查詢的任何作業系統值變更

CAS 可提供安全管理員能加以控制的其他參數。例如，雖然每個範本元素都有預設輪詢間隔，管理員還是可以設定不同的輪詢間隔（請參見圖 19）。管理員可指定 CAS 應如何判斷是否有變更。一個方法是使用時間戳記，另一方法則是使用 MD5 總和檢查值。後者需要運算較大量資料，但功能也較強大。

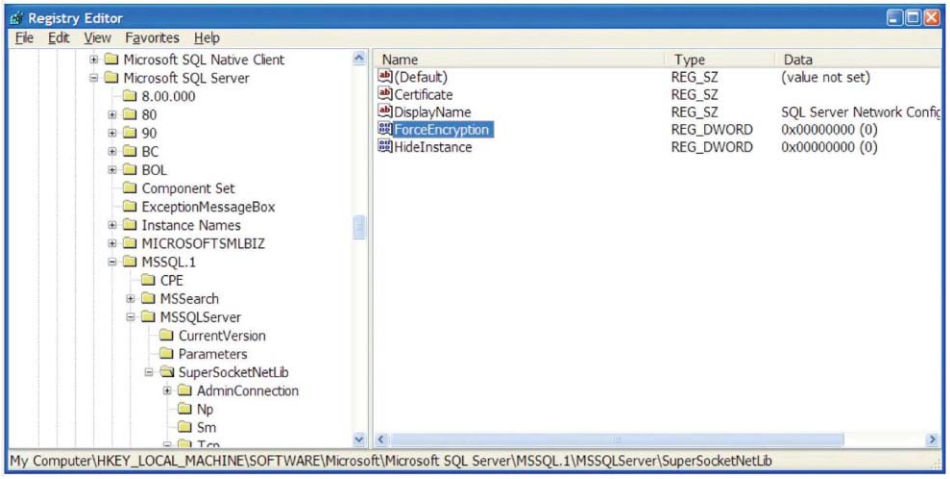


圖 18 ：CAS 可簡化追蹤重要登錄值的程序，如 SQL Server 的「強制通訊協定加密」登錄值。

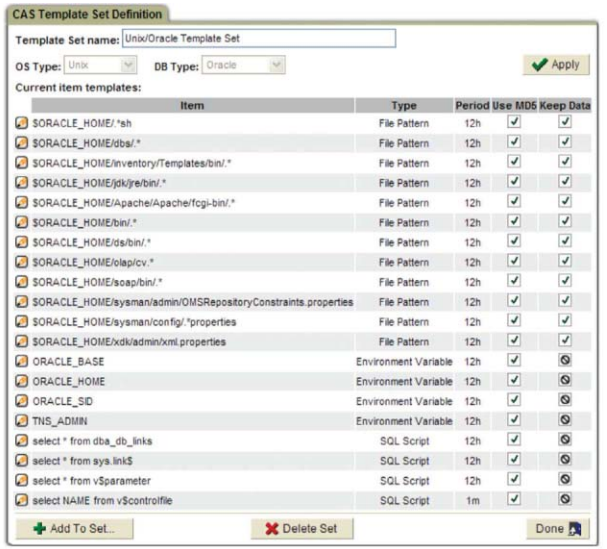


圖 19 ：CAS 可讓您定義追蹤變更的輪詢時間；是否使用 MD5 總和檢查追蹤變更（而非時間戳記）；以及 CAS 是否應該「保存資料」，以追蹤「之前的」值。

此外，每個元素可指定 CAS 是否應該只報告變更，還是也要顯示變更前後的值。如果是後者，提供的報告會顯示新舊值的差異（請參見圖 20）。

安裝及操作 CAS

CAS 可隨 S-TAP 一起安裝，或另行安裝。CAS 當作 Java 程式執行，所以需要在主機上安裝 Java 1.4 或更新版。Java 是安裝的必備項目，CAS 安裝程式會詢問 Java 的安裝位置。右表是 CAS 的儲存需求摘要。

自訂 CAS

除了預先建置的範本和追蹤元素，CAS 還可讓安全管理員建置必須追蹤的新目標。不僅僅是定義要監視的新檔案或元素。您可定義新資料庫指令碼和新作業系統指令碼，由 CAS 進行管理，而且可用來補強 CAS 提供的大量內建功能。

作業系統	所需磁碟空間
AIX	350MB
HP-UX	650MB
Linux	450MB
Solaris	400MB
Tru64	350MB
Windows	300MB

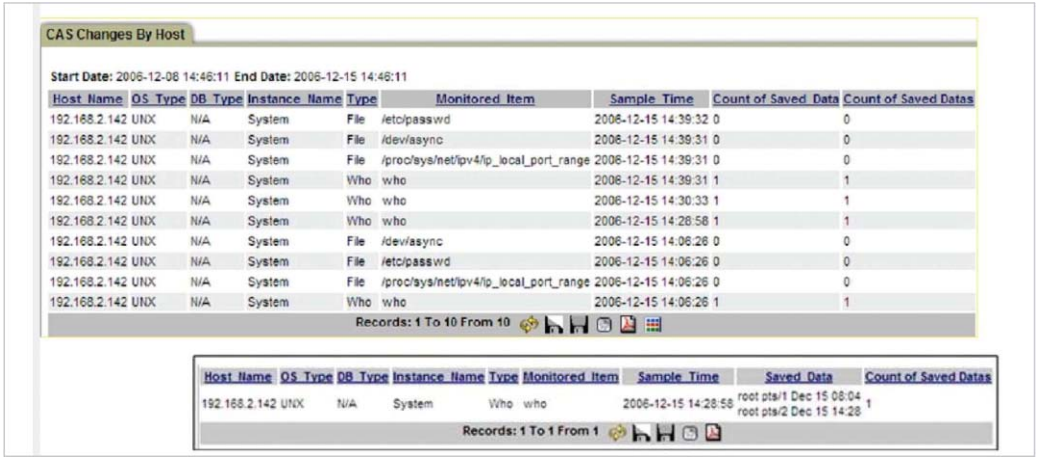


圖 20： CAS 可提供保留變更前後的值的選項（上述「Saved Data」）。

透過自動化簽核及呈報，記錄法規遵循情形

審核者要確定公司會即時追蹤並解決事件。有了 InfoSphere Guardium 事件管理和 Compliance Workflow Automation（請參見圖 21），您便可自動化報告分發、電子簽核、備註及呈報，同時追蹤變更事件的補救進度。

圖 21 ：審核者需要證據顯示組織有定義完善的程序，以保護重要資料。InfoSphere Guardium 的工作流程自動化模組可讓您定義自訂審核工作 (Audit Task)，自動執行排程的變更審核報告、報告分發、簽核與呈報。

Application End-User Identifier

監視應用程式使用者活動，即時偵測詐騙行為

- 可保護主要企業應用程式，防止發生詐騙、內外部攻擊、濫用專用權及資料洩漏
- 提報執行未獲授權作業的應用程式使用者認證，即便該使用者是使用一般服務帳戶存取資料庫
- 有別於其他系統使用無法進行審核及鑑識的統計抽樣及資料流量比對等近似方法，此工具會使用決定性方法積極找出應用程式使用者
- 可滿足審核者的要求，全面監視任何來源的所有機密性資訊存取
- 可降低營運成本，並簡化需滿足內外部審核規定的法規遵循程序，包括 SOX、PCI DSS、ISO 27001、NIST 800-53 和 SAS70

企業應用程式環境的安全和法規遵循

許多組織都使用企業應用程式來執行核心商業程序，以及管理大量重要業務和高度機密的資料。SAP、PeopleSoft 及 Oracle EBS 等應用程式所管理的資產就有財務資料、個人資料和客戶資料等。因此，許多法規遵循要求和審核都涉及企業應用程式管理的資料，要求 IT 安全部門必須確保這些資料的安全性。

InfoSphere Guardium Application End-User Identifier 可提供套裝解決方案，因應主要企業應用程式所管理資料的相關安全和法規遵循需求，不必變更現有商業程序或應用程式原始碼。

應用程式層的監視主要是爲了偵測透過企業應用程式進行的詐騙行爲。SOX、ISO 270001 、SAS 70 及 NIST 800-53 控制等資料控管法規通常會要求這個層次的監視。

保護多層企業應用程式

由於多層企業應用程式高度分散且目的是讓內部和客戶、供應商及合作夥伴等外部人員透過 Web 存取，所以最難維護安全。此外，這些多層企業應用程式通常會使用最佳化機制「連線儲存區」，遮罩資料庫交易層次的終端使用者身分。

連線儲存區會找出含有一般服務帳戶名稱的所有交易，因此，要將特定資料庫交易與特定應用程式終端使用者建立關聯就更加困難。尤其是使用只能根據資料庫登入帳戶，來監視並找出使用者的一般資料庫記載工具時。

由於企業應用程式資料儲存在關聯式資料庫中，所以也能透過直接資料庫連線（如透過 SQL *Plus 等開發工具）或應用程式本身存取。IBM 便提供了可因應這兩種存取方式的唯一綜合性解決方案。此方案可主動找出特定資料庫交易相關的應用程式使用者（請參見圖 22、26 和 27），以及找出特許使用者直接存取未獲授權物件的作業。例如，圖 24 中，使用者透過 SQL *Plus 執行 SELECT 資料，違反了使用者只能透過 Oracle 應用程式存取 EBS 資料的原則。此違規行爲會自動觸發指定動作。本案例的指定動作是終止 SQL *Plus 階段作業、記載違規行爲的詳細資料，並產生警示。

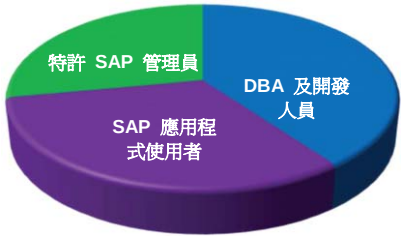
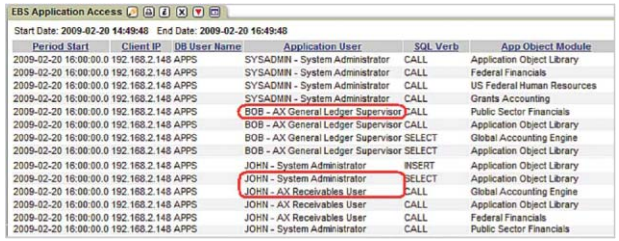


圖 23 ：InfoSphere Guardium 可保護企業應用程式環境，避免所有主要風險來源。



EBS Application Access

Start Date: 2009-02-20 14:49:48 End Date: 2009-02-20 16:49:48

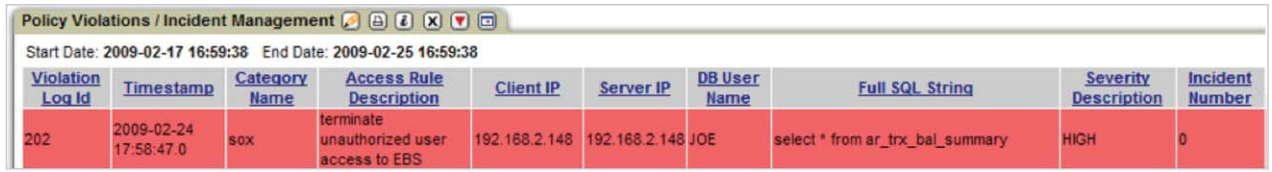
Period Start	Client IP	DB User Name	Application User	SQL Verb	App Object Module
2009-02-20 16:00:00.0	192.168.2.148	APPS	SYSADMIN - System Administrator	CALL	Application Object Library
2009-02-20 16:00:00.0	192.168.2.148	APPS	SYSADMIN - System Administrator	CALL	Federal Financials
2009-02-20 16:00:00.0	192.168.2.148	APPS	SYSADMIN - System Administrator	CALL	US Federal Human Resources
2009-02-20 16:00:00.0	192.168.2.148	APPS	SYSADMIN - System Administrator	CALL	Grants Accounting
2009-02-20 16:00:00.0	192.168.2.148	APPS	BOB - AX General Ledger Supervisor	CALL	Public Sector Financials
2009-02-20 16:00:00.0	192.168.2.148	APPS	BOB - AX General Ledger Supervisor	CALL	Application Object Library
2009-02-20 16:00:00.0	192.168.2.148	APPS	BOB - AX General Ledger Supervisor	SELECT	Global Accounting Engine
2009-02-20 16:00:00.0	192.168.2.148	APPS	BOB - AX General Ledger Supervisor	SELECT	Application Object Library
2009-02-20 16:00:00.0	192.168.2.148	APPS	JOHN - System Administrator	INSERT	Application Object Library
2009-02-20 16:00:00.0	192.168.2.148	APPS	JOHN - System Administrator	SELECT	Application Object Library
2009-02-20 16:00:00.0	192.168.2.148	APPS	JOHN - AX Receivables User	CALL	Global Accounting Engine
2009-02-20 16:00:00.0	192.168.2.148	APPS	JOHN - AX Receivables User	CALL	Application Object Library
2009-02-20 16:00:00.0	192.168.2.148	APPS	JOHN - AX Receivables User	CALL	Federal Financials
2009-02-20 16:00:00.0	192.168.2.148	APPS	JOHN - System Administrator	CALL	Public Sector Financials

圖 22 ：InfoSphere Guardium Application End-User Identifier 可協助 IT 安全部門快速找出違反企業原則的詐騙行爲和其他動作，如在企業應用程式環境中使用排存連線（注意，所有交易的 DB User Name 爲 APPS），進行未獲授權的機密資料變更。如果是 Oracle EBS 環境，在 EBS 定義職責後，也可以識別並利用指定給使用者的職責。在以上範例中，部門原則將 Bob 的工作 (AX General Ledger Supervisor) 指定爲監視活動之一，以簡化報告審查。我們也可以看到 John 有兩個身分；一個是 AX Receivables User，另一個是 System Administrator，說明可能有不當授權。

可擴展性企業安全平台

Application End-User Identifier 模組以 InfoSphere Guardium 領先業界的 Database Activity Monitoring (DAM) 和 Vulnerability Assessment (VA) 技術爲基礎，透過選定企業平台的特定應用程式原則、審核報告及追蹤群組，進一步鞏固這些核心模組。

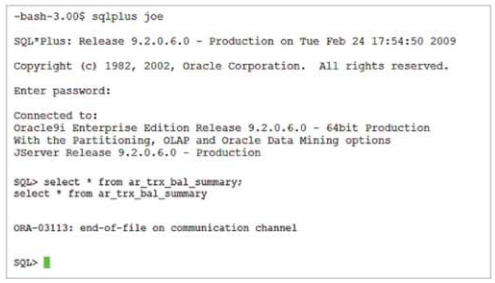
DAM 技術可即時監視所有資料庫存取，不必依賴原生資料庫日誌、不影響效能，也不需要進行資料庫變更。InfoSphere Guardium 的多層架構是業界獨一無二的解決方案，可從多個 DBMS 系統和位置，自動彙整並正規化審核資訊，將其納入單一的集中儲存庫。如此一來，便可加強企業層面的法規遵循報告、關聯、鑑識和進階資料庫導向分析。



Policy Violations / Incident Management

Start Date: 2009-02-17 16:59:38 End Date: 2009-02-25 16:59:38

Violation Log Id	Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description	Incident Number
202	2009-02-24 17:58:47.0	sox	terminate unauthorized user access to EBS	192.168.2.148	192.168.2.148	JOE	select * from ar_trx_bal_summary	HIGH	0



```
-bash-3.00$ sqlplus joe

SQL*Plus: Release 9.2.0.6.0 - Production on Tue Feb 24 17:54:50 2009

Copyright (c) 1982, 2002, Oracle Corporation.  All rights reserved.

Enter password:

Connected to:
Oracle9i Enterprise Edition Release 9.2.0.6.0 - 64bit Production
With the Partitioning, OLAP and Oracle Data Mining options
JServer Release 9.2.0.6.0 - Production

SQL> select * from ar_trx_bal_summary;
select * from ar_trx_bal_summary


ORA-03113: end-of-file on communication channel


SQL>
```

圖 24 ：可偵測使用 SQL *Plus 等工具規避 EBS 以直接存取資料的違規行爲，還可選擇加以封鎖（左）。 此工具還可記載詳細資料（上），然後透過工作流程自動化分派給相關人員進行調查。

其圖形 Web 主控台可提供原則、報告定義、法規遵循工作流程和裝置設定（如保存排程）的集中管理。只要新增在聯合模型中搭配使用的設備，即可輕鬆擴充此多層架構，以因應任何產量及審核原則組合。

InfoSphere Guardium 亦可提供 Vulnerability Assessment 模組，其中包含自動化測試的最佳實務庫，可找出各種漏洞，如遺漏的修補程式、配置不當的專用權、預設帳戶和低保護性密碼。爲了支援此模組，Knowledge Base 服務會定期提供漏洞測試更新，以及 SAP 和 Oracle EBS 的機密物件和預先配置群組。透過提供更新物件清單和群組，IBM 可簡化監視重要表格存取及變更的作業。

全方位的原則型監視及審核

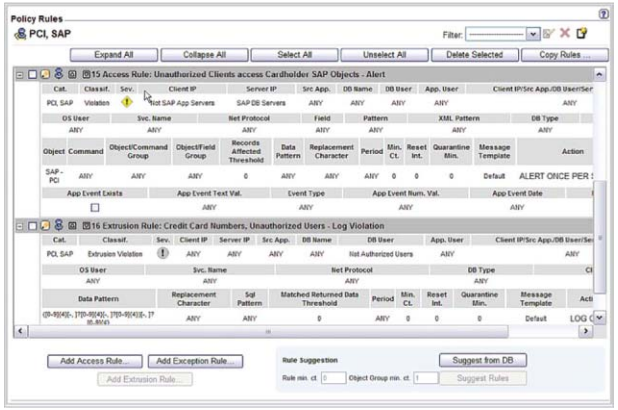


圖 25 ：InfoSphere Guardium 可提供 SAP 和 Oracle EBS 應用程式的精細預先配置原則，快速找出可疑或未獲授權的活動，如變更機密物件或多次登入失敗。Knowledge Base 服務會找出機密物件（可能需要深入研究才找得到），以快速部署自訂原則。此外，還可配置違反原則時執行的一系列動作，如即時 SNMP 警示。

InfoSphere Guardium 可提供：

- 內建針對 SOX 和 PCI 環境制定的預先配置報告（這些環境通常有企業應用程式）。
- 內建適用於 Oracle EBS 和 SAP 的 SOX 及 PCI DSS 原則（請參見圖 25）。
- 針對應用程式資料所儲存的基礎資料庫引擎，提供全方位的評量。
- 完整的活動和資料存取審核，顯示已執行的直接與間接活動，以及存取的資料。
- 使用者執行的活動審核追蹤，以顯示資料庫層次的存取和應用程式層次的使用者 ID（請參見圖 22、26 及 27）。審核記錄會顯示執行存取的使用者 ID 和用戶端主機。

廣泛的異質應用程式支援

InfoSphere Guardium 可支援所有主要應用程式和應用程式伺服器的應用程式層監視，不需要變更應用程式。這些應用程式包括：

- Oracle E-Business Suite
- SAP ERP 和 NetWeaver BW
- PeopleSoft
- Cognos
- Siebel
- Business Objects Web Intelligence

InfoSphere Guardium 也可針對根據標準應用程式伺服器平台建置的自訂和套裝應用程式，找出應用程式使用者 ID，如：

- IBM WebSphere
- BEA WebLogic
- Oracle Application Server
- JBoss Enterprise Application Platform

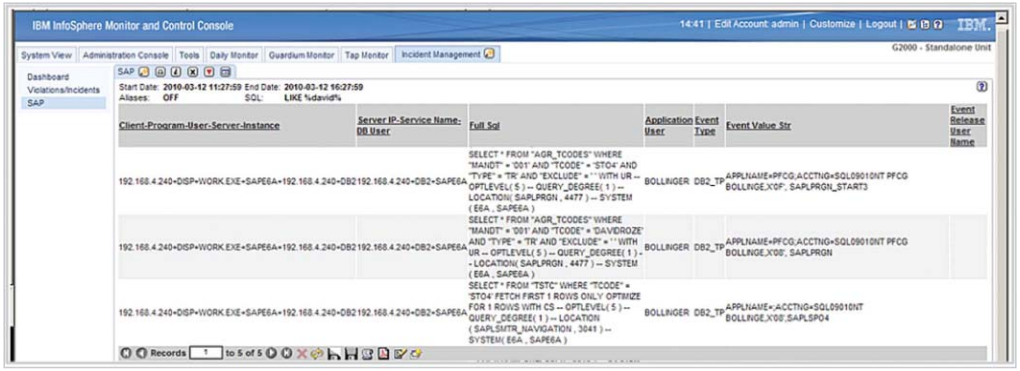


圖 26 ：InfoSphere Guardium Application End-User Identifier 可監視 SAP 及 DB2 與 Oracle 等資料庫環境之間的所有交易。

圖 27 ：End-User Identifier 模組可找出 PeopleSoft 排存連線環境中，特定交易（應用程式使用者）的相關使用者，依賴原生資料庫審核資訊的一般工具只能顯示通用識別碼 (SYSADM)。

Enterprise Integrator

整合資料，以加強作業及安全效率

- 輕鬆連到多個關聯式資料庫或文字檔以擷取資料，並將資料納入 InfoSphere Guardium 儲存庫，達到審核完整性
- 建立統一的審核報告，其中包括加強安全和提高作業有效性的外部資訊
- 匯入說明資訊，如對應使用者名稱的完整名稱和電話號碼，以精簡異常調查程序
- 整合角色及部門等資訊，以部署更精細的安全原則
- 整合 IBM iSeries 和 Progress 資料庫等環境的日誌資訊，以建立所有資料庫安全與法規遵循資料的單一管理點
- 善用現有 Tivoli 和 Centera 基礎架構，以簡化 InfoSphere Guardium 審核資料與作業結果的自動化保存作業

管理複雜且快速變遷的環境

資料庫安全和法規遵循的管理工作越來越困難。不僅是網路攻擊與日俱增，所管理的環境也變得十分複雜。

由於商業環境瞬息萬變，如合併、委外、工作人力調整及商業自動化加速等，導致無法即時取得資訊，以有效建立、管理安全原則並據此提出報告。各地區和部門的資料庫不斷激增，管理及授權資訊分散在不同系統中，人事及系統資料不斷改變，而且審核資訊的要求也越來越高。

企業通常會仰賴手動程序蒐集所需資料，以確保資料庫安全原則及報告包含精確且有意義的資料。有鑑於目前環境資源有限、所管理的環境複雜度及激增的工作量，組織致力尋求有效方法，以自動化資料庫安全和法規遵循作業。

自動化所有安全資料的取得、整合及保存

InfoSphere Guardium 的 Enterprise Integrator 是一套選用軟體模組，可簡化及自動化外部資料庫或文字檔的資料整合，然後納入 InfoSphere Guardium 儲存庫，還可利用現有企業儲存體基礎架構進行資料保存。此工具可有效利用新應用程式的廣泛功能，如自動化變更控制核對、改善程序和原則，將手動人力成本降至最低。

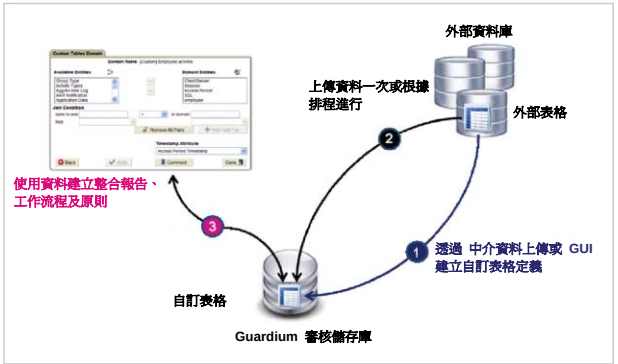


圖 28 ：Enterprise Integrator 可提供簡單的方法，整合外部來源的重要安全相關資訊。所提供的工具可自動或手動：1) 爲 InfoSphere Guardium Audit Repository 中的匯入資料建立自訂表格定義 2) 上傳外部來源的資料 3) 建立資料連結，以便所有 InfoSphere Guardium 工具有效使用匯入資料。

只要透過下列幾個簡單步驟，即可整合外部資訊（請參見圖 28）。首先，建立要儲存資料的自訂表格。您可提供 InfoSphere Guardium 從來源資料庫擷取中介資料所需的資訊來建立表格定義，或者使用特定 GUI 手動輸入表格定義。然後上傳目標資料，InfoSphere Guardium 還會提供工具以檢查綱目相容性並執行上傳後所需的 DML。您可一次全部上傳，或定期排程上傳，確保儲存庫與變更的主要資料來源同步，不需要人爲介入。

將資料儲存在儲存庫之後，即可有效利用所有 InfoSphere Guardium 原則、分析、報告和工作流程工具。例如，可匯入獨特環境（如 IBM iSeries）的日誌資訊，以便自動化報告、工作流程和簽核工具套用該資料，確保原則一致性並提高作業效率。上傳資料也可以連到儲存庫的現有資料。如此一來，即可將重要的說明資訊加入報告及原則（請參見圖 29），不需要手動查閱，同時可提供重要資料以找出特定原則違規情形。

自動化變更控制核對

多數組織都有正式的變更控制原則和程序，以控管正式作業資料庫的變更方法和時機。然而，由於變更管理應用程式和正式作業資料庫是不同系統，多數時候都無法偵測未獲授權的變更。少了強制執行機制，則無法有效實施變更控制原則。但一般可用的唯一方法是使用原生審核日誌進行手動核對，需要大量人力。

如果搭配使用 Enterprise Integrator 及核心 InfoSphere Guardium 系統，便可輕鬆實施變更控制原則，不需要大量人力。Enterprise Integrator 可擷取變更管理系統的核可變更要求，然後納入 InfoSphere Guardium 系統。商務系統（如 BMC 的 Remedy 及 HP 的 Peregrine）的要求包括商業層級的摘要說明。使用通行證 ID 將變更說明連到 InfoSphere Guardium 所觀察的實際變更，可自動化核對程序（請參見圖 30）。審查人員可輕鬆比較摘要說明及執行的 SQL 指令，以確保變更符合原則。

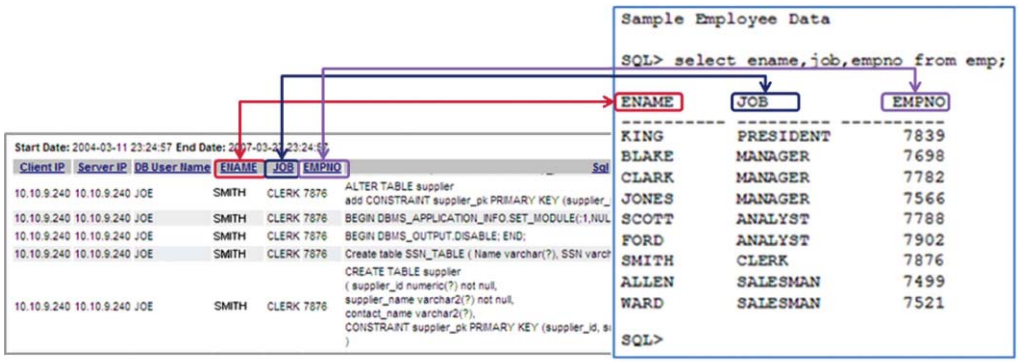


圖 29：Enterprise Integator 可讓使用者建立統一的審核報告，其中包括加強安全和提高作業效率的外部資訊。例如，可輕鬆整合遠端員工資料庫所儲存的真實員工姓名 (ENAME) 及編號 (EMPNO)，不需要手動研究特定 DB User Name 對應的員工，即可調查異常報告。匯入員工工作分類 (JOB) 的功能可找出不同活動，如更改資料庫表格的 CLERK。

工作流程自動化可確保所有變更已經過審查及核准，並且標示所有問題，以進行後續補救。一旦沒有使用通行證 ID、在授權變更期間以外或使用未獲授權使用者 ID 執行變更，系統就會自動偵測到。您可選擇做出各種回應，如發出即時警示或封鎖動作。

自動化變更控制核對作業可保護重要資料，並證明組織有主動控管，以滿足審核者的嚴格要求。

自動化原則資訊更新，避免安全漏洞

即使當初部署 InfoSphere Guardium 的目的是保護特定重要資產，但使用該系統一段時間後，企業通常會進行擴充，以保障企業的所有機密資料庫。隨著系統的擴大，群組的使用就變得很重要。群組是一組共用相同屬性的元素。使用群組可簡化原則和報告的制定與維護。例如，組織可能有 30 個分別儲存機密財務資料的獨立物件。您可定義包含所有成員的 SOX 群組，而不必建立分別指定所有物件的原則和報告。因此，用來監視及報告 SOX 物件存取情形的原則和報告就變得比較簡單。

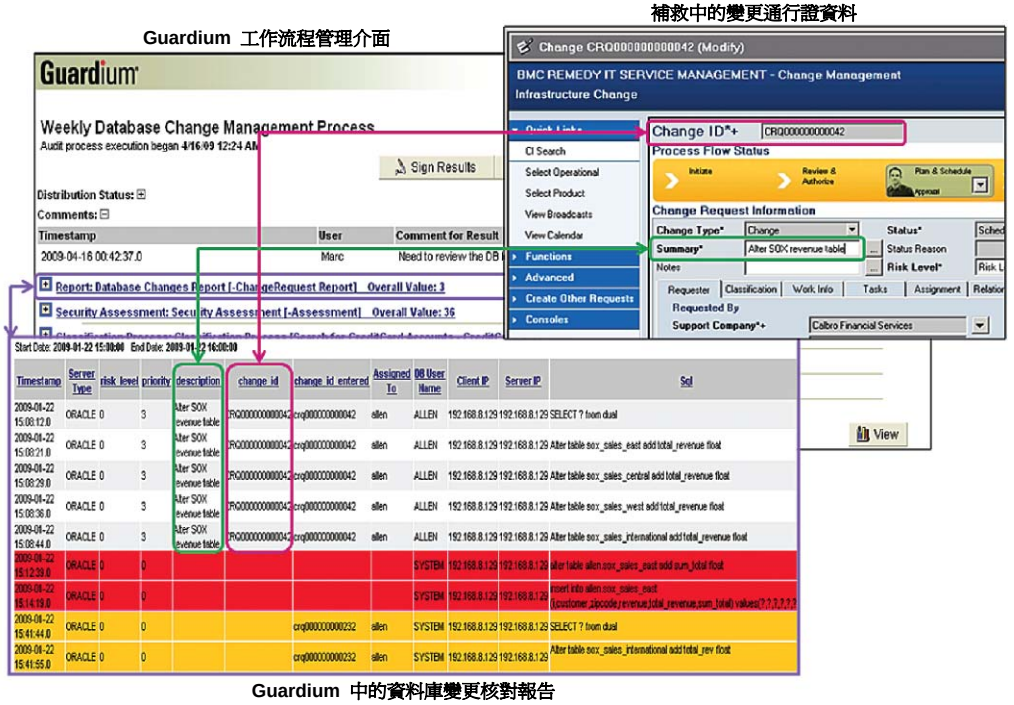


圖 30 ：Enterprise Integrator 可從自訂或商務系統（如 BMC 的 Remedy 或 HP 的 Peregrine）匯入變更管理資訊。在本範例中，使用 InfoSphere Guardium 的工作流程功能每週分發及管理的 Database Change Report，包含了 Change ID 和 Summary 說明。此報告已經過設計，以紅色突顯沒有通行證的實際變更。黃色的變更代表該變更輸入的變更號碼無效。顯示授權變更的 Remedy Summary 及實際執行的 SQL 指令可讓報告收件者確認所執行的變更皆爲授權變更。

Enterprise Integrator 支援	
資料來源	Oracle、DB2、Sybase、Microsoft SQL Server、Informix、mySQL、Teradata、Netezza 及 PostgreSQL 資料來源的立即可用支援
連線	HTTP、HTTPS、FTP、SAMBA 及 IBM iSeries 的立即可用支援，以連線至 CSV 文字檔資料來源

群組可用來簡化各種物件的管理作業，如伺服器類別（如包含 SOX、PCI、PII 資料的伺服器）及使用者（如特許使用者、可存取 SOX 物件的授權使用者，或負責審查伺服器群組異常的事業夥伴）。群組中的資料通常源自網路上的資料庫，而且在這些資料庫中進行維護。如果使用 Enterprise Integrator 擷取這類資料，然後移入群組，即可避免浪費人力和發生錯誤。更重要的是，只要排程 Enterprise Integrator 定期上傳，一旦物件變更（因爲職責變更、基礎架構變更等），就會自動更新群組成員資格，不需要更改 InfoSphere Guardium 群組或原則。如此一來，也可以減少工作，避免群組成員資格資料過時所發生的安全漏洞。

自動化保存程序，以降低法規遵循成本

在多數組織中，法規遵循要求和內部原則都會規定，必須保存審核資料及審核工作結果等所有 InfoSphere Guardium 資料，以便進行報告及鑑識。爲了支援此需求，本解決方案已納入自動化保存與還原功能。Enterprise Integrator 隨附 Tivoli Storage Manager 及 EMC Centera 的立即可用連接器，透過 InfoSphere Guardium 的保存功能便可輕鬆使用這些主要企業保存解決方案。

使用者只需輸入配置資訊，如儲存區連線字串和密碼，InfoSphere Guardium 便可連接到這些系統。有了 Enterprise Integrator，使用者即可善用現有企業保存解決方案，不必開發自訂的整合器。

IBM InfoSphere Guardium for z/OS

使用實證的 z/OS 技術，達到完整的 DB2 審核透明度

- 可監視及審核 z/OS 上特許使用者、大型主機常駐應用程式和網路用戶端的所有資料庫活動
- 可詳細監視重要作業，如 SELECT、DDL、DML、存取授權與撤消
- 所有審核資料的分析、報告及儲存都是在資料庫以外的安全環境中執行
- 整合企業層面的 Guardium 架構，可提供大型主機和分散式資料庫環境適用的統一安全和法規遵循解決方案
- 可利用 IBM 的實證 z/OS 技術，發揮最佳可靠性和效率

DB2 的安全和法規遵循要求日趨嚴格

許多組織在大型主機資料庫中儲放了大量重要業務的機密資料。財務、人事及客戶記錄就是這些環境中的常見資訊。

因此，越來越嚴格的法規遵循通常也包含大型主機資料。此趨勢迫使組織實施新控制，以確保 DB2 資料安全，避免內外部使用者未獲授權存取及竄改，而且審核者可輕鬆取得詳細的審核追蹤，以驗證控制的有效性。

IBM InfoSphere Guardium 解決方案可提供簡單但功能強大的方法，以保護整個企業的重要資料。此方案可使用原則型快速偵測違反企業原則的異常活動，還可提供即時回應（如警示）、適當處理異常的可審核工作流程，及自動化報告功能，以簡化 SOX、PCI DSS 及資料隱私權等法規遵循的驗證程序。

InfoSphere Guardium for z/OS 可針對 z/OS 上的 DB2 提供這些功能。此解決方案可單獨用於大型主機環境，或者整合企業的其他 Guardium 資料庫安全和監視元件（請參見圖 31），以提供安全、集中的審核儲存庫及管理點。

避免一般解決方案的相關安全和成本問題

過去，組織一直希望能夠監視和保護 z/OS 上 DB2 機密資料，因此採用了根據記載公用程式（如追蹤或交易日誌）如所開發的自訂解決方案。然而，這些解決方案和其他以此爲基礎的方案都有許多限制，包括：

- 必須依賴大型主機資料庫管理員 (DBA) 進行管理，無法達到審核者的職權分立 (SOD) 原則
- 無法擷取審核者要求的所有重要活動（如使用 Logging 時的讀取作業，或使用 Trace 時的 SQL 陳述式）
- 缺乏精細分析和警示功能，以致無法立即偵測並遏制重要的未獲授權活動種類（如未獲授權更新使用者有權存取的資料）
- 需要大量有經驗的人力資源，才能維護自訂軟體，或分析報告以偵測違反原則情形

InfoSphere Guardium for z/OS 即可擺脫這些限制，同時提供重要的額外功能，如法規遵循工作流程自動化、報告及企業層面的資料庫安全和法規遵循情形視圖。

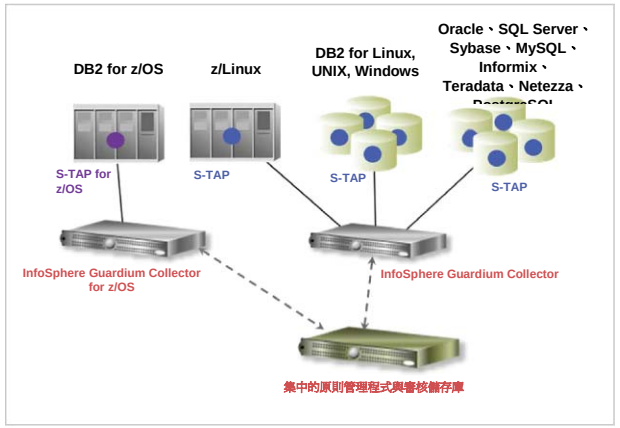


圖 31 ：Guardium 會使用輕量型軟體探測器 S-TAP for z/OS，擷取特許使用者、大型主機常駐應用程式和 z/OS 上的網路用戶端執行的金鑰資料庫活動。從單一主控台即可監視大型主機和分散式環境；此外，所有審核資料自動彙整並正規化後都會納入單一集中的儲存庫，以進行企業層面的法規遵循報告、分析及鑑識。

可調式企業層面資料庫安全和法規遵循平台

InfoSphere Guardium for z/OS 會使用輕量型軟體探測器 S-TAP for z/OS，擷取特許使用者、大型主機常駐應用程式和網路用戶端的所有資料庫活動，包括透過 JDBC 或 DB2 Connect 等服務連線的用戶端。實證的 IBM DB2/z 事件擷取技術能確保擷取所有重要作業，如 SELECT、DML、DDL 和存取授權，不必使用 DB2 Class 4 及 Class 5 審核追蹤資料。

S-TAP for z/OS 會將使用者定義審核原則所指定的資訊（請參見圖 32），傳送至 InfoSphere Guardium Collector for z/OS 設備。如此一來，大型主機就不需要一直增加儲存體或處理要求，網路資料流量有限，並且可安全儲存完整的審核追蹤。IBM Query Monitor 也可以共用 S-TAP 事件擷取技術，爲使用這兩種產品的用戶端進一步加強效能。

InfoSphere Guardium 的多層架構是業界獨一無二的解決方案（請參見圖 31），可彙整並正規化資料庫平台、應用程式及不同位置上的審核資訊，然後納入單一集中的儲存庫。如此一來，便可提供全方位的企業層面法規遵循報告、關聯、鑑識和資料庫導向分析。當初採用大型主機實作的使用者可輕鬆擴充，以支援任何資料庫與系統組合，只要加入聯合模型中搭配使用的適當 S-TAP、Collector 及 Aggregator 即可。

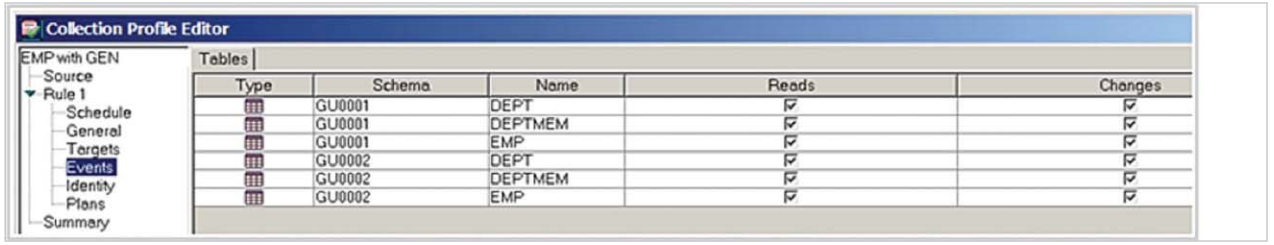
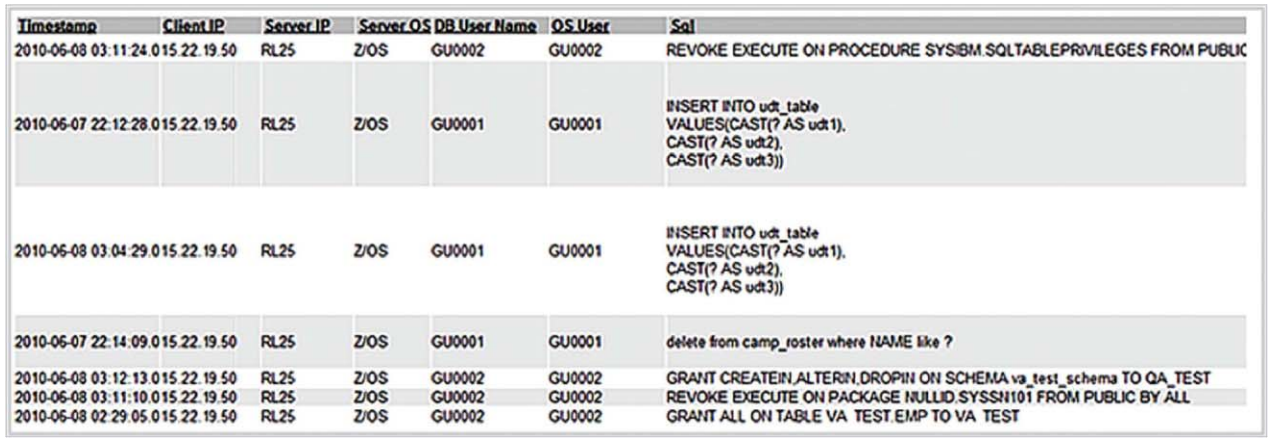


圖 32： 您可使用 Windows 型審核原則編輯器，輕鬆建置審核原則，以定義所需擷取的 DB2 交易。



Timestamp	Client IP	Server IP	Server OS	DB User Name	OS User	Sql
2010-06-08 03:11:24.0	15.22.19.50	RL25	Z/OS	GU0002	GU0002	REVOKE EXECUTE ON PROCEDURE SYSIBM.SQLTABLEPRIVILEGES FROM PUBLIC
2010-06-07 22:12:28.0	15.22.19.50	RL25	Z/OS	GU0001	GU0001	INSERT INTO udt_table VALUES(CAST(? AS udt1), CAST(? AS udt2), CAST(? AS udt3))
2010-06-08 03:04:29.0	15.22.19.50	RL25	Z/OS	GU0001	GU0001	INSERT INTO udt_table VALUES(CAST(? AS udt1), CAST(? AS udt2), CAST(? AS udt3))
2010-06-07 22:14:09.0	15.22.19.50	RL25	Z/OS	GU0001	GU0001	delete from camp_roster where NAME like ?
2010-06-08 03:12:13.0	15.22.19.50	RL25	Z/OS	GU0002	GU0002	GRANT CREATEIN,ALTERIN,DROPIN ON SCHEMA va_test_schema TO QA_TEST
2010-06-08 03:11:10.0	15.22.19.50	RL25	Z/OS	GU0002	GU0002	REVOKE EXECUTE ON PACKAGE NULLID.SYSSN101 FROM PUBLIC BY ALL
2010-06-08 02:29:05.0	15.22.19.50	RL25	Z/OS	GU0002	GU0002	GRANT ALL ON TABLE VA_TEST.EMP TO VA_TEST

圖 33：Guardium 可全面監視 z/OS 上的 DB2 資料使用情形，擷取包含重要細節的大型主機和網路存取（如 OS 使用者名稱）、用戶端 IP、資料庫使用者名稱和所執行的 SQL 陳述式。

自動化的原則型監視及審核，精簡法規遵循驗證

InfoSphere Guardium Web 主控台可集中管理警示、報告定義、法規遵循工作流程及設定（如保存排程），不需要 DBA 介入，因此可達到審核者要求的 SOD 並精簡法規遵循活動。可針對整個資料庫基礎架構執行廣泛的管理功能，包括：

- 使用特定環境的潛在風險指標，定義精細的存取原則，如資料物件、SQL 指令類型、使用者 ID、用戶端 IP 位址、OS 使用者名稱、來源應用程式或當日時間
- 自動建立供原則參考的正常活動基準，以偵測異常活動，如 SQL 資料隱碼攻擊
- 定義回應違反原則的動作，如產生警示及記載完整的事件詳細資料
- 自動化例行活動和事件回應的法規遵循工作流程，如簽核、提出意見及呈報等步驟
- 執行數百個立即可用的報告，如 SOX、PCI DSS 和資料隱私權法所需的報告，以及建立自訂報告

您可使用 InfoSphere Guardium 全面監視 DB2 環境，即時找出並應付未獲授權的活動，如資料竄改或駭客入侵。一旦自動化整個安全和法規遵循生命週期，便可降低人力成本，促進組織的溝通，以及簡化審核準備程序。

全方位的 IBM 環境支援

InfoSphere Guardium 解決方案可支援其他常用的 IBM 平台，包括：

- IBM DB2 for Linux, UNIX and Windows
- IBM Informix
- IBM DB2 for iSeries
- System z Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server for System z，可支援 IBM z/VM Hypervisor 中執行的所有主要 DBMS 平台（Oracle、MySQL 等）
- Cognos 8，InfoSphere Guardium 可透過應用程式層監視，找出詐欺及其他未獲授權活動。Guardium 也可支援其他企業應用程式，如專門爲 IBM WebSphere Application Server 及其他中介軟體平台開發的 SAP、PeopleSoft 和 SOA 應用程式。

IBM InfoSphere Guardium for z/OS	
支援的 DB2 版本	z/OS V7、V8 或 V9 專用的 DB2
支援的 z/OS 版本	z/OS V1.6 或更新版

110 台北市松仁路 7 號 3 樓
技術諮詢熱線：0800-000-700
台北市松仁路 7 號 3 樓

台灣印製
2010 年 5 月

InfoSphere®
軟體

IMB14083USEN-00