



次世代資料庫活動監控系統 DAM+

dataisec 智安數據科技股份有限公司

1. 引言

在數位化時代，企業依賴資料庫來存儲與管理關鍵數據，涵蓋客戶資訊、財務數據、營運數據等多方面敏感信息。然而，隨著資料量的快速成長，資料庫的安全性與合規性成為企業不可忽視的重要議題。資料庫活動監控系統不僅要能夠幫助企業監控資料庫的存取與變更，還要能確保符合相關法規，如個人資料保護法（個資法）及各項資訊安全法規標準。特別是面對日益嚴峻的資訊安全威脅與複雜的法規環境下，傳統的稽核監控系統無法準確識別前端使用者，也無法追蹤資料的異動軌跡，因此無法滿足法規要求。本公司累積多年經驗，創新研發次世代資料庫活動監控系統 DAM+，採用微服務架構，實現模組化設計，讓每個服務都能獨立開發、安裝部署和升級，提高系統靈活性、可維護性和可擴展性。採用分布式叢集架構部署，支持 NonStop Active-Active 模式，滿足高可用要求，保障監控稽核服務不中斷。支持客戶可以按需橫向擴展，保障投資。創新研發 Smart Agent 可以準確識別前端使用者身分，追蹤前端使用者資料庫活動，並且支援追蹤資料異動前、異動後數據，真正符合個資法人、事、時、地、物 5W 要求。

2. 產品特色

■ 高可擴展性和靈活性

DAM+ 的設計具有高度可擴展性和靈活性，能夠輕鬆適應不斷成長的資料庫規模和不斷變化的需求。無論您的資料庫環境如何發展，DAM+ 都能提供可靠的稽核和安全保障。



■ 監控稽核服務不中斷

採用模組化設計，以分布式叢集架構部署，支持 Active-Active 模式，滿足高可用要求，如有設備發生故障或其他原因造成失效，系統將自動切換，保障監控稽核服務不中斷。

■ 前端使用者追蹤

可以追蹤前端 Web 使用者行為，明確責任歸屬，提高稽核正確性，並精準定位和簡化安全事件的調查。支持 .NET 和 Java 應用平台。

■ 即時分析與可視化

提供即時的日誌分析與可視化報表，幫助管理人員快速掌握系統狀態，做出即時的決策。支持多維度的數據分析，提升企業的數據洞察能力。

■ 強大安全性

採用多樣安全防護措施，包括資料加密、存取控制和自我監控，確保稽核資料的安全性。這些防護措施可以有效防止未經授權的稽核資料存取、修改或刪除等安全威脅。

■ 符合法規

符合個資法、資訊安全管理體系 ISMS 標準 ISO 27001, 27011 規範，金融法規例如: SOX, BASEL II/III, COBIT, GLBA, PCI-DSS 等、醫療業 HIPAA 等重要法規要求。

3. DAM+ 核心技術

■ 微服務架構

採用微服務架構，實現模組化設計，讓每個服務都能獨立開發、部署和升級，提高系統靈活性、可維護性和可擴展性。容器化和自動化部署

■ Nonstop 分布式叢集部署

創新使用分布式叢集架構部署，支持 AA 模式，滿足高可用要求，如有設備發生故障或失效，系統將自動切換，保障監控稽核服務不中斷。

■ NoSQL 分析引擎

分布式 NoSQL 分析引擎，實現即時日誌分析、靈活查詢、可視化儀表板，具備高可用性和可靠性。



■ 機器學習引擎

採用機器學習引擎，透過分析資料庫行為模式，建立異常偵測模型，提升資料安全性和預測性風險評估能力。

■ 分散式流處理技術

採用分散式流處理技術，高速接收解析後資料，實現即時流處理。

■ 前端使用者追蹤(Smart Agent for APU)

自研前端使用者追蹤技術可以準確識別前端用戶身分，並準確關連追蹤使用者在資料庫的存取行為。精準識別使用者名稱並正確關連執行 SQL 語句，不遺漏，提供有效證據，釐清責任，符合法規要求。

■ 資料異動軌跡查詢

自研資料異動軌跡追蹤技術，準確紀錄資料的新增、修改、刪除行為，可以識別資料異動前、異動後的數據。

4. 產品功能

■ 支援主流資料庫，支援監控以下資料庫活動軌跡紀錄，包括：

- Oracle, Microsoft SQL Server, DB2, Informix, MySQL, PostgreSQL, Sybase, MongoDB 等資料庫。

■ 前端使用者追蹤(Smart Agent for APU)，前端使用者身分追蹤，支援以下應用伺服器平台，包括：

- .NET 平台：.NET framework, .NET core
- Java 平台：Tomcat, WebLogic, WebSphere, JBOSS, ...等。

■ DAM+ 支援安裝於 LINUX 作業系統，包括：RHEL, CentOS, Ubuntu, ...等。

■ 提供異常偵測模型，透過使用者行為分析與機器學習，建立異常行為偵測模型，自動辨識異常行為，預測潛在風險，主動防禦。

■ 支援資料異動軌跡查詢，可以明確識別資料刪除、修改前的數據，以及識別新增、刪除、修改後的數據。



- 圖形化管理工具
 - 提供 Web-Based 圖形化集中管理工具，支持 HTTPS 通訊協定，支援繁體中文及英文顯示頁面。
 - 提供管理網頁登入帳號、密碼以及密碼安全強度設定。
 - 提供角色權限管理，根據登入人員角色權限不同顯示不同功能選單。
- 提供自定義儀表板，使用者可以按身分職責需要定義儀表板顯示圖表內容，選擇需要關注的圖表，視覺化管理追蹤整體資安情況。可以按照不同角色身分職責，自定義關注不同圖表信息。
- 提供報表與圖表方式查詢，使用者可以查詢所有稽核紀錄，也可以輸入搜尋條件查詢，並支援以 csv, pdf, html 文件格式下載資料。
- 提供設定告警發送機制，支援透過 Email, SNMP, Syslog 方式發送告警通知，並附上觸發告警事件詳細活動紀錄。
- 提供資料集和條件集設置功能，彙總歸集稽核紀錄資料，方便設定異常行為觸發條件。
- 提供事件簽核功能，透過事件管理與簽核功能，可以追蹤告警事件處理情形，確定事件處理完成，減少資安事件發生。
- 提供稽核報表與告警，支援符合個資法、資訊安全管理體系 ISMS 標準 ISO 27001, 27011 規範，金融法規例如: 沙賓法案 SOX, 巴賽爾協定 BASEL II/III, COBIT, GLBA, PCI-DSS 等，以及醫療業 HIPAA 等法規要求，協助企業滿足法規要求。