Change Auditor for Active Directory

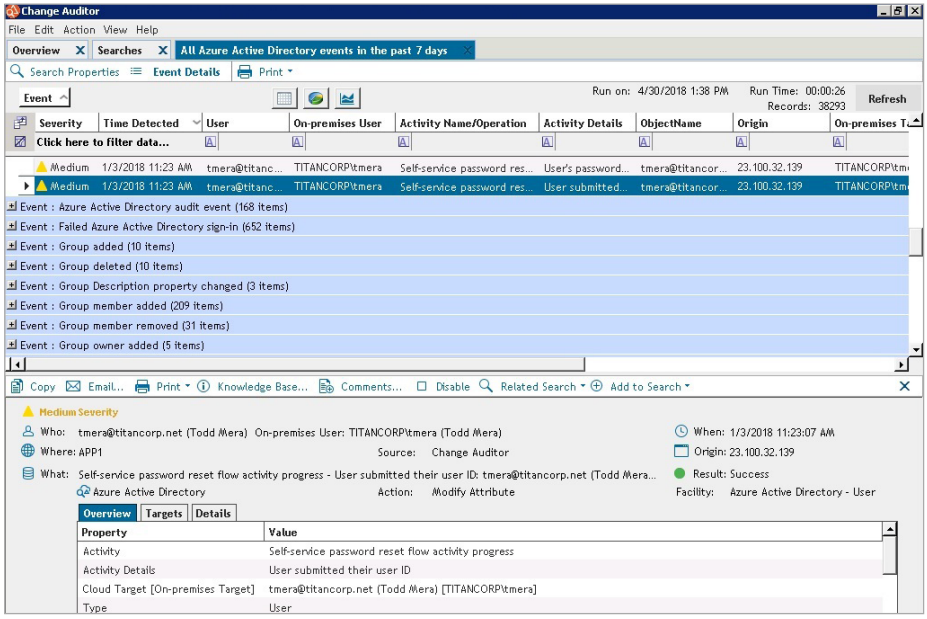
Active Directory 和 Azure Active Directory 適用的即時稽核

Microsoft Active Directory (AD) 是關鍵任務網路基礎架構的核心。AD 若出現問題，可能導致無預警且代價高昂的服務中斷事件，以及會傷及業務的網路停機時間，更別提嚴重的安全資料外洩與違反重要政府規範 (例如 SOX、PCI、HIPAA、GDPR 等) 帶來的巨額損失。AD 和 Azure AD 發生重大變更時，企業組織必須即時收到通知。

Quest® Change Auditor for Active Directory 可在單一主控台中追蹤所有重要組態變更並加以整合，進而提高 AD 和 Azure AD 的安全性和控制力。對於會影響您內部部署及雲端環境的相關變更，Change Auditor 可加以追蹤、稽核、回報和警示，省下啓用原生稽核功能的成本。藉由 Change Auditor for AD，您可以得知各項變更的人員、內容、時間、位置和原始工作站，以及任何相關事件的詳細資訊，包括變更前後的值，以及具有關聯的內部部署和雲端身分。您也可以加入註解，說明做出特定變更的原因，以配合稽核規定。藉由 Change Auditor for AD，您可以快速又有效率地稽核所有重大變更，以確保您珍貴的資料和資源安全無虞。

稽核所有重大變更

取得豐富可自訂的稽核和報告功能，瞭解所有 AD 和 Azure AD 的重大變更，包括對群組原則物件 (GPO)、網域命名系統 (DNS)、伺服器組態、巢狀群組等其他項



透過 Change Auditor for Active Directory，您可以按時間順序掌握各項變更的人員、內容、時間、位置和原始工作站資訊，包括具有關聯的內部部署和雲端身分。

優點：

- 只需幾分鐘即可完成安裝；可快速收集事件資訊，立即對 Windows 環境進行分析
- 從單一用戶端執行遍及整個企業，包括內部部署及雲端的稽核與法規遵循工作
- 根據使用者的行為模式主動偵測威脅
- 消除未知安全疑慮，透過追蹤所有事件以及與特定事件相關的變更，確保能夠持續存取應用程式、系統和使用者
- 向所有裝置發布即時警示，讓公司內外都能立即回應，在短時間內消除安全風險
- 預防擅自變更行為，並限制授權使用者的控制能力，利用此保護機制強化內部控制
- 允許主動排解帳戶鎖定問題，以提高可用性
- 不使用原生稽核方式來收集事件資訊，以降低對伺服器效能的影響，並省下儲存資源
- 簡化法規遵循工作，以配合企業與政府政策及法規規範，包括 GDPR、SOX、PCI DSS、HIPAA、FISMA 和 SAS 70 等
- 將資訊轉為深入解析的鑑識情報，供稽核人員和管理階層使用

「整體而言，Change Auditor 一直非常地好用。在我們評估過的其他所有產品中，沒有一個能夠提供相同等級的即時稽核與保護功能，不需針對所有的 Active Directory 變更啓用 Windows 稽核機制。」

Patrick Rohe
資深 IT 架構設計師
陶森大學

系統需求

如需系統需求的最新詳細清單，請造訪 quest.com/products/change-auditor-for-active-directory。

目的變更。不同於原生稽核，您可利用合併檢視瞭解所有內部部署、雲端和混合式 AD 變更活動，並透過深入的鑑識情報依時間順序瞭解上述活動在您 AD 和 Azure AD 環境中與其他事件的關聯。此外，透過主動警示功能，您可隨時保持警覺，在重大原則變更和安全漏洞產生時，隨處使用任何裝置來做出回應，降低與日常變更相關的風險。

追蹤使用者活動並防止未預期的變更

可針對使用者和管理員，追蹤其帳戶鎖定和存取重要登錄檔設定的活動，有助於加強整個企業的變更與控制原則。運用主動控制，從源頭預防發生重大變更、24 小時全年無休的警示、深入分析、復原先前數值和報告的能力，這些功能可讓您的 AD 和 Azure AD 環境免於遭受可疑的行爲和未經授權的存取，且隨時符合企業與政府的標準。

使用 CHANGE AUDITOR THREAT DETECTION 主動偵測威脅

透過分析異常活動來評斷組織中風險最高的使用者，並找出潛在威脅，以及減少誤判警示的干擾，進而簡化使用者威脅偵測作業。

將不相關的資料轉換爲具有意義的資訊，以提升安全性和法規遵循

追蹤重大變更，然後將原始資料轉譯爲具有意義的情報資料，協助保障您基礎架構的安全性和法規遵循性。Change Auditor for AD 可協助您掌握各項變更的人員、內容、時間、位置和原始工作站，以及任何相關事件詳細資訊，其中包括變更前後的值，讓您可以在有安全疑慮時快速做決策。您也可以藉助 Change Auditor 的高效能稽核引擎，讓稽核限制不再成爲您的羈絆。無需原生稽核記錄，您將可更快取得稽核結果並省下儲存成本。

整合式事件轉送

輕鬆與 SIEM 解決方案整合，將 Change Auditor 事件轉送至 Splunk、Micro Focus ArcSight 或 IBM QRadar。另外，Change Auditor 可整合 Quest® InTrust®，以 20:1 的壓縮率長期儲存事件及彙總原生或第三方記錄，進而降低 SIEM 轉送的儲存成本，並建立高度壓縮的記錄存放庫。

自動報告以配合企業與政府的規範

使用 Microsoft SQL Server Reporting Services 即時取得清楚、具有意義的安全性和法規遵循報告。利用內建的法規遵循資料庫和可自訂的報告，證明您符合政府標準規範 (例如：GDPR、SOX、HIPAA、PCI DSS、FISMA 和 SAS 70) 將變得易如反掌。

關於 QUEST

Quest 的宗旨是以簡單的解決方案解決複雜的問題。爲了達成此理念，我們堅持提供優異的產品和服務，並秉持簡單經營業務的整體目標。我們期望能爲您帶來兼顧效率與效益的技術，讓您和貴組織可以減少耗費在 IT 管理上的時間，進而投入更多時間發展業務創新。

DataSheet-ChangeAuditor4AD-US-KS-zh_TW-WL-33959