中文型錄

Active Directory Change Tracker

Active Directory 的異動稽核、追踪與分析

概覽

* 無 Agent代理程式安裝。 在您的桌上電腦上工作。 安裝與設定該工具只需幾分鐘。

* 追踪與稽核整個企業對 Active Directory 所做的所有異動。 追踪對關鍵 OU 與 GPO 的異動。

* 分析並確定異動的完整性（是否由正確的人員進行了正確的異動）。

* 可使用或不使用 Active Directory 的原身稽核 native auditing功能追踪異動。

* 高效率的資料蒐集。 每次執行期間僅蒐集增量異動資料。

** 捕獲並維護對 Active Directory 與 GPO 的所有重要異動的異動歷史記錄。*

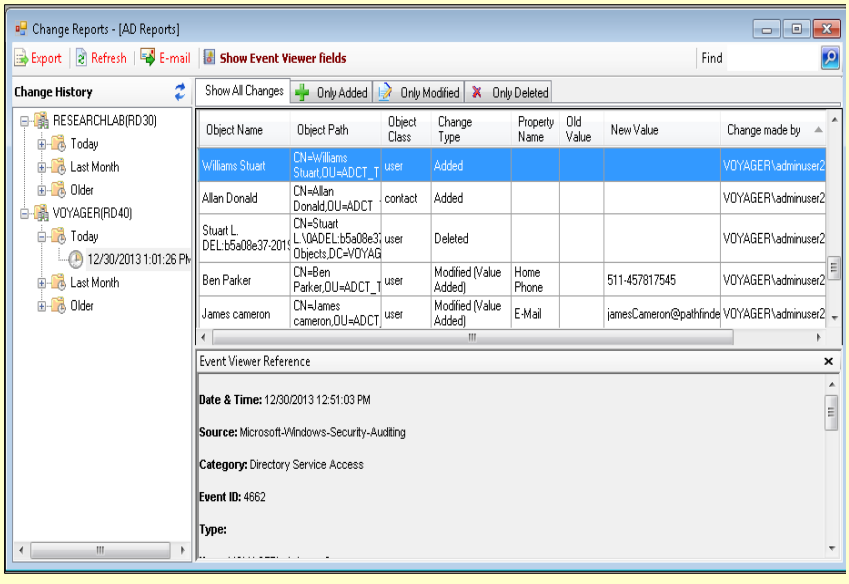
你為什麼需要它?

Active Directory 是組織企業網路的支柱。 Active Directory (AD) 的龐大規模與壓倒性的複雜性使其管理變得複雜。 異動追踪Change Tracking與管理已成為法規遵循、法規與內部管理需求的必要條件。 必須採取此類措施來解決有關 Active Directory 的共享與安全性的重要問題。

Active Directory Change Tracker (ADCT) 是 Vyapin 的解決方案，可幫助您追踪與稽核對 Active Directory 的所有異動。

它可以在有或沒有啟動 AD 的原身稽核native auditing的情況下工作。 即使沒有 AD 的原身稽核，您仍然可以使用我們解決方案的增量異動資料蒐集功能來追踪對 AD 的異動； 記錄 - 發生了什麼變化以及在哪裡。 如果您決定將 ADCT 與您的原身 AD 稽核一起使用，它會成為一個更強大的解決方案，首先偵測來自您所有網域控制器的特定異動，並僅提取那些包含指示異動者與異動時間所需資訊的相關記錄。

此外，您還可以儲存整個事件日誌記錄以及異動，以供將來參考。 ADCT 是追踪與維護對 Active Directory 所做的所有異動的長期歷史記錄以及用作預警工具的有效方法。



詳細Vyapin Software產品資料請洽 商丞科技 02-2914-8001

概覽

* 通過使用本機 Active Directory 稽核從事件日誌中捕獲稽核記錄，並將它們與該工具結合以產生有關誰在何時進行異動的報告。

* 在 SQL 資料庫中建立與維護異動歷史記錄以及事件日誌稽核記錄。 幫助您儲存數年的異動資料，用於法規遵循與監管目的。

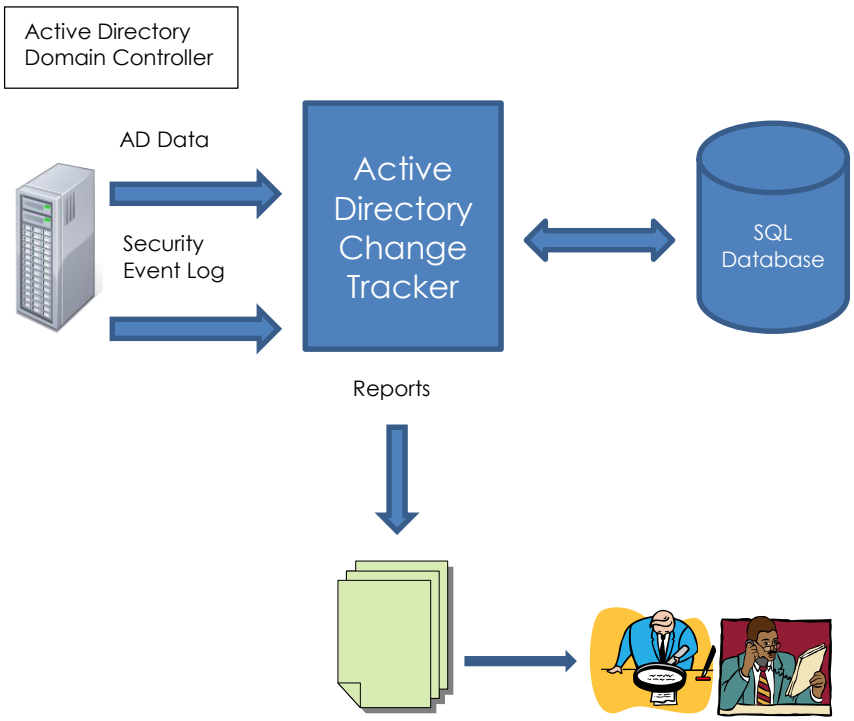
* 可選擇只追踪重要的容器 containers、OU 與事件 Event ID。 或者追踪指定日期範圍、網域、異動類型的事件報告並建立複雜的過濾條件。

* 使用強大的搜索條件搜索整個異動歷史記錄——搜索特定用使用者Users、群組、OU、物件屬性Object property等的新增、刪除與修改。

* 安排您的報告，以便在偵測到異動後立即通過電子郵件通知選擇的用戶群組。

它是如何運作的?

ADCT 是一種企業級監控解決方案，可追踪、分析與報告所有發生變化的 AD 事件。 該服務代理安裝在伺服器中，有助於追踪多項異動。 通常使用此服務監控的一些事件是 – 用戶登錄與登出 User login & logout、終端服務活動Terminal Service activities、密碼異動Password changes、群組與安全策略異動 Group and Security Policy changes、對各種 AD 物件所做的異動（如其建立、修改、刪除）、網域級別異動 、網域控制器角色的變化等。可以建立一組事件 ID 來專門監視這些變化。 這有助於將 ADCT 的稽核能力集中在這些重要的事件集上。 因此，ADCT 有助於建立更好、更高效執行的 Active Directory。



自由文本搜索過濾器可幫助您在關鍵字的幫助下分析任何預定義搜索條件的所有過去更改。 例如，您可能會搜索您的AD中最近一個月內所有的物件刪除。

靈活的報告功能允許您將需要的報告匯出Export到選定的郵箱或資料夾，或者簡單地將其存放在資料庫中以供需要時參考。您可以選擇以 HTML/CSV/XLSX檔案格式發送這些報告。

VYAPIN

詳細Vyapin Software產品資料請洽 商丞科技 02-2914-8001