瞭解安全終結點中的更新事件以進行組刪除

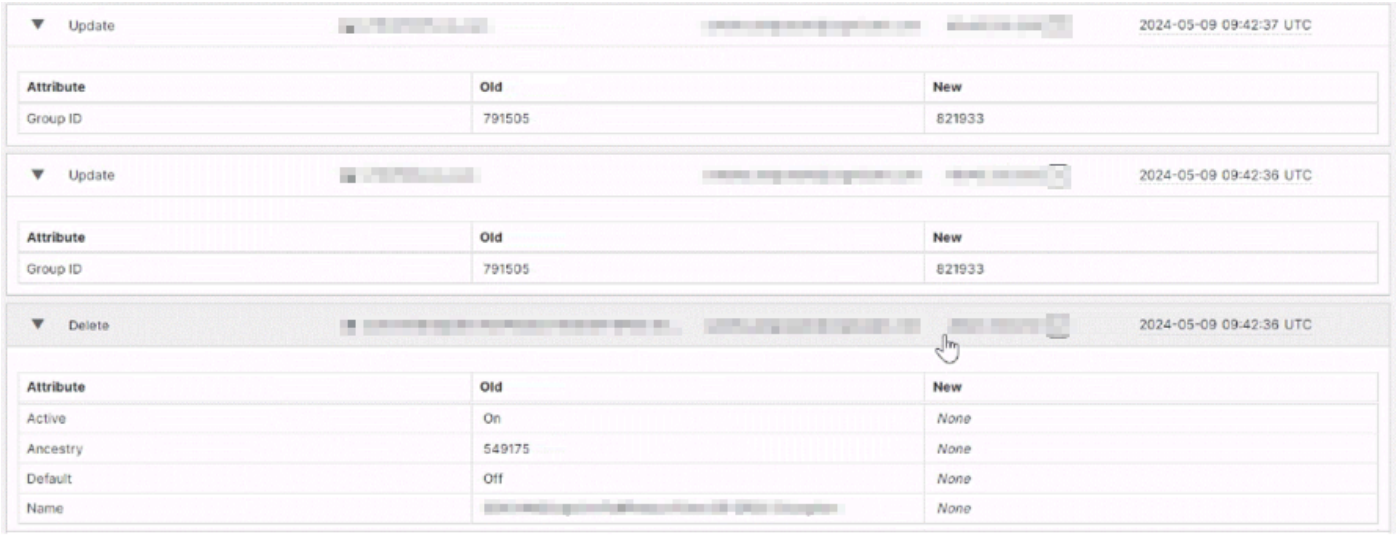
目錄

簡介

本文檔介紹當刪除空組時，安全終端稽核日誌如何記錄更新和刪除事件。

問題

此影象中的更新事件顯示電腦或工作站的新組ID，即使這些工作站在AMP控制檯電腦頁面上不可見。這些更新事件與登入以執行刪除的使用者電子郵件相關聯，這可能導致客戶端對發生的事情感到困惑。在某些情況下，刪除空組後可生成30-40個更新事件。



解決方案

這是預期行為。在刪除空組期間，在稽核日誌更新事件中看到的電腦或電腦主機名屬於以前屬於這些組，但現在處於非活動狀態的裝置。這些機器在停用90天後自動從控制檯移除，但它們仍然是後端組的一部分。

刪除組後，這些非活動電腦將移至預設組，從而觸發更新事件。遺憾的是，由於這些電腦處於非活動狀態，因此它們不會顯示在控制檯中，這就是在電腦下搜尋時無法找到它們的原因。

要獲取仍然分配到組的非活動電腦的完整清單，您需要聯絡TAC，因為無法通過安全終端門戶檢索此資訊。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。