對Umbrella中的活動搜尋報告中缺少的Active Directory使用者進行故障排除

目錄

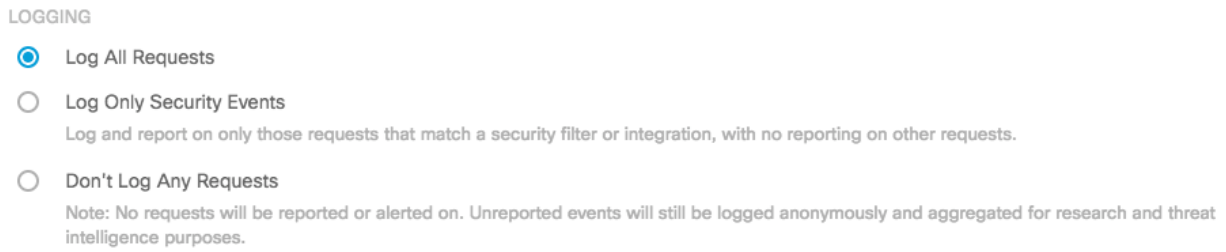
簡介

本檔案介紹Cisco Umbrella中的「Activity Search Report」。活動搜尋報告是一個近乎即時的報告，其中包含您的使用者正在執行的所有DNS查詢。如果您已設定Cisco Umbrella Active Directory(AD)整合，您可能會看到您的AD使用者正在填充「活動搜尋」中的「身份」列。但是，有時使用者會從「身份」列中丟失。

解析

如果您認為您應該直接在「活動搜尋」的「身份」列中看到AD使用者，但是沒有看到他們，或者看到了一些AD使用者，但沒有達到您預期的數量，請注意以下幾點：

1. 站點和Active Directory
   - 檢查所有AD元件，確保沒有報告的錯誤或問題。如果您在任一元件上看到任何灰色、橙色或紅色狀態指示燈，獲取這些詳細資訊並開啟支援票證(umbrella-support@cisco.com)。
     - 來自受影響的使用者（未顯示在「活動搜尋」中的使用者）的診斷測試
     - 虛擬裝置(VA)控制檯的螢幕截圖，其中擴展了所有錯誤消息
     - AD聯結器稽核日誌
2. 日誌記錄設定
   - 在每個策略的Advanced Settings中，底部有一個關於記錄量的部分。您可以將其設定為：
     - 記錄所有請求
     - 僅記錄安全事件
     - 不記錄任何請求
   - 如果您的策略當前設定為「僅記錄安全事件」，則可以解釋為什麼您看到的查詢沒有達到期望的數量，或者某些使用者根本沒有結果。



3. 正確的策略優先順序
    - 如果您的策略應用於網路標識的策略在策略清單中高於您的AD使用者策略，則網路標識策略可能會應用。這又意味著，在「活動搜尋」中，您將看到網路作為報告身份。請同時檢視思科有關最佳實踐和原則優先順序的文檔。

原因

Activity Search從何處獲得「身份」？

當DNS查詢進入Umbrella時，假設您的AD整合按預期工作，此資訊將在查詢中傳遞：

- 內部IP地址
- AD身份雜湊（使用者、主機或兩者）
- 輸出IP
- 正在查詢的域

AD身份雜湊由虛擬裝置新增到查詢中，虛擬裝置會傳遞該資訊以及來自AD聯結器的登入事件的相應內部IP地址。

然後，Cisco Umbrella使用此資訊查詢組織並確定應用哪個策略。如果您沒有專門針對您的AD使用者的策略，但您的網路或站點有相應的策略，則Cisco Umbrella會使用該身份應用該策略。這表示當在「活動搜尋」中報告查詢、標識和響應時，將報告觸發策略的標識。其他資訊仍在請求中標籤，因此您仍然可以搜尋AD用戶，獲取將網路報告為「標識」的活動。此外，如果將「活動搜尋」資料匯出到CSV檔案，則會顯示與查詢關聯的所有身份資訊。

其他資訊

如果您仍然沒有看到任何AD使用者，請諮詢支援(umbrella-support@cisco.com)，並附上診斷測試結果和任何AD聯結器稽核日誌。

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）。