瞭解聯結器讀取的視窗事件/事件ID

目錄

簡介

本文檔介紹聯結器預設讀取的視窗事件/事件ID。

概觀

Umbrella Virtual Appliance(VA)在技術上只能看到它從哪個源IP地址接收DNS查詢。為了使使用者與DNS請求相關聯，VA與聯結器配合工作，這導致發生使用者到IP的對映。

聯結器從域控制器上的安全事件日誌中讀取具有特定事件ID的事件。然後分析這些事件，並將使用者名稱和源IP地址傳送到VA，VA隨後在該源IP和使用者之間建立對映。

如果域控制器未稽核這些事件，將無法正確執行VA對映過程。這篇文章精確地概述了聯結器在預設情況下監視的事件ID型別。

事件ID	說明
4624	事件4624記錄每次成功登入本地電腦的嘗試，無論登入型別、使用者位置或帳戶型別如何。
528	只要帳戶登入到本地電腦，就會記錄事件528，網路登入事件除外。無論用於登入的帳戶是本地SAM帳戶還是域帳戶，都會記錄事件528。
540	當網路中其他位置的使用者連線到此電腦上的伺服器服務提供的資源（如共用資料夾）時，將記錄事件540。
4768	此事件僅在域控制器上記錄，並且同時記錄此事件的成功和失敗例項。
4769	Windows將此事件ID用於成功和失敗的服務票證請求。

如果聯結器無法從域控制器的安全事件日誌中直接讀取事件，您可以向Umbrella索取支援票證，請求將此更改為WMI訂閱。在WMI訂閱的情況下，聯結器訂閱上面列出的所有事件。此外，聯結器還會預訂具有下面所述的EventID的註銷事件。請注意，預設情況下，聯結器不從安全事件日誌中讀取

這些註銷事件。

事件ID	說明
538	無論使用者是從網路連線、互動式登入還是其他登入型別註銷，都會記錄事件538(有關登入型別的圖表，請參閱事件528)。
4647	此事件表示登入會話的結束，並可使用登入ID關聯回登入事件4624。
4634	此事件也表示登入會話的結束，並可使用登入ID關聯回登入事件4624。

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）。