對Umbrella聯結器阻止Active Directory服務帳戶進行故障排除

目錄

簡介

本文描述如何對Active Directory服務帳戶被Umbrella聯結器阻止的原因進行故障排除。

概觀

Umbrella聯結器服務將WMI連線到屬於同一Umbrella站點的任何已註冊域控制器(DC)的事件日誌，以便讀取登入事件資訊。 然後分析這些登入事件並將其上傳到位於同一Umbrella站點的所有虛擬裝置(VA)。然後VA為該使用者名稱/源IP地址建立臨時使用者到IP對映。有兩點值得注意：

- Umbrella Insights一次只能支援每個IP一個登入使用者
- 源IP最近處理的登入事件「wins」

由於所有登入事件都是相等的，聯結器有一個硬編碼清單，列出了忽略其事件的常見AD服務帳戶。 您可以檢視聯結器日誌檔案中提取的來自這些帳戶的登入事件。舉例來說：

已忽略列入黑名單的使用者的事件：OpenDNS_Connector

這樣做是為了防止服務帳戶（就像標準使用者在DC安全事件日誌中生成登入事件一樣）覆蓋實際登入使用者的使用者到IP對映。

在大型環境中，根據服務帳戶使用的進程/應用程式，他們每分鐘也會生成數千個登入事件。這也是聯結器的額外負載，它可能表現為使用者登入與正在應用的正確策略之間的延遲，或者表現為應用之後丟失的正確策略。

阻止的帳戶清單

- _vmware_user_
- 管理員
- 匿名
- 匿名登入
- ASPNET
- 本地服務

- McAfeeMVSUser
- MHConcontrol
- 網路服務
- netwrix
- OpenDNS_Connector
- peersyncsvc
- s-pcadmin
- SophosUpdateMgr
- SophosUpdMgr
- svc-altiris
- svc.iCreate

更多資訊

您還可以排除聯結器處理任何其他AD帳戶登入事件。有關說明，請參閱本文：

https://support.umbrella.com/hc/en-us/articles/231266088

此外，還有可從聯結器的AD同步中排除的AD組，執行AD同步是為了使用AD使用者、電腦和組的清單填充儀表板策略區域。您可以在以下位置找到此項：

https://support.umbrella.com/hc/en-us/articles/115005206526

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）。