排除Umbrella Insights AD整合故障不檢測使用者流量

目錄

簡介

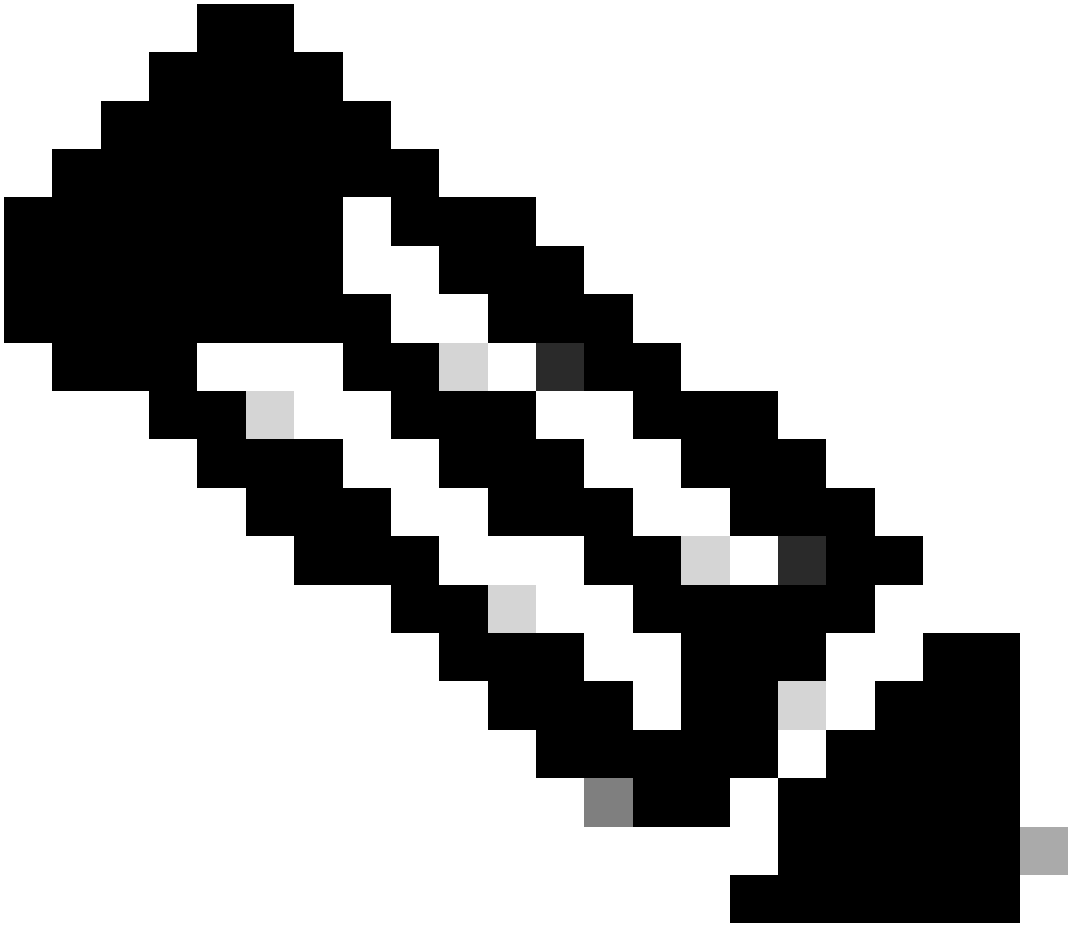
本文說明如何對不檢測使用者流量的Umbrella Insights AD整合進行故障排除。

概觀

您已安裝Umbrella Insights、設定聯結器和虛擬裝置，並註冊了域控制器。 所有元件都顯示為綠色，並在儀表板的`deployments -> Sites and Active Directory`下工作。但是，您已經配置了一個策略來使用AD使用者或組對象，但是您仍然沒有看到儀表板或策略中報告的使用者活動被正確應用。

您還可能注意到OpenDNSAuditClient.log檔案中的此條目重複

'上次接收事件時間為1970-01-01 00:00:00'



附註：日誌檔案位於C:\Program Files(x86)\OpenDNS\OpenDNS Connector\<VERSION>\
VERSION =聯結器服務的實際安裝版本，如v1.1.22

說明

發生這種情況的主要原因是可能未在您的Active Directory域中配置稽核登入事件。日誌消息表明聯結器自安裝後未看到一個單使用者事件。 目前，這不會在儀表板中生成錯誤。

解析

主要要做的是檢查AD組策略以查詢正確的稽核策略配置：

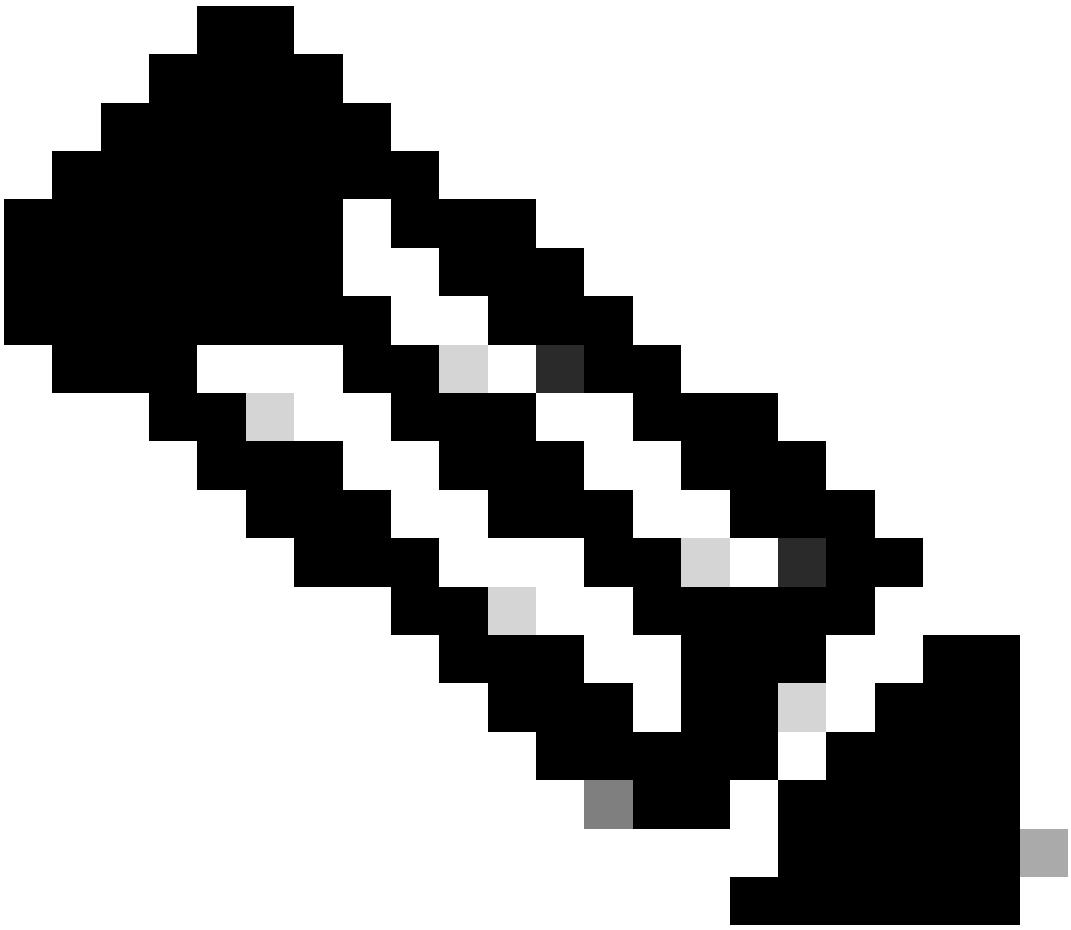
1. 在域控制器上，開啟管理工具中的組策略管理(Group Policy Management)面板，選擇適用於域控制器的策略（預設域控制器策略可能是候選策略）。

2. 按一下右鍵該策略，然後選擇編輯以啟動組策略管理編輯器。

3. 瀏覽到「Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy」資料夾，然後選擇Audit logon events以檢視其屬性。

4. 此策略必須用於稽核成功嘗試。

5. 運行gpupdate命令以應用策略。



附註：在某些情況下，「Default Domain Controllers and the Default Domain Policy」可能需要配置該設定。

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）。