由於VPN配置檔名稱長度限制，安全訪問VPN管理員重置斷開連線

目錄

問題

遠端訪問VPN使用者在活動會話期間Cisco Secure Access出現間歇性斷開連線。Cisco Secure Access(CSA)日誌將這些斷開連線事件記錄為管理員重置，儘管當時沒有計畫維護活動。在正常業務操作期間，斷開連線會影響遠端訪問使用者，在使用者主動連線到VPN服務時導致意外的會話終止。

斷連事件在遠端訪問日誌中顯示為管理員重置條目，通常表示管理干預或系統啟動的會話終止。但是，在報告的時限內，未對系統執行任何管理操作。

環境

- Cisco Secure Access(CSA) — 遠端訪問VPN服務
- 名稱長度超過46個字元的VPN配置檔案配置

解析

解決方法涉及實施一種解決方法，以解決導致Administrator Reset事件的VPN配置檔名稱長度限制：

即時解決方法

步驟 1:識別名稱超過46個字元的VPN配置檔案

檢視Cisco Secure Access控制面板中的所有現有VPN配置檔案配置，並確定名稱超過46個字元的所有配置檔案。

步驟 2:重新命名VPN配置檔案以符合字元限制

重新命名所有超過46個字元的VPN配置檔案，以確保其長度不超過46個字元。這可通過思科安全訪問管理介面完成。

步驟 3:監控斷開連線事件

實施VPN配置檔名稱更改後，監控遠端訪問日誌以驗證在正常操作期間不再發生管理員重置事件。

長期解決方案

正在開發永久修復程式以解決GUI限制，從而允許VPN配置檔名稱超過後端處理限制。此修復程式在使用者介面級別強制實施46個字元的限制，阻止建立名稱導致後端處理問題的VPN配置檔案。

開發團隊正致力於在GUI中實施適當的驗證，以在建立和修改期間限制VPN配置檔名稱長度，這可防止在未來的配置中出現此問題。

其他考量事項

在某些情況下，客戶端裝置上的Wi-Fi介面卡電源管理設定會導致連線問題。如果在實施VPN配置檔名稱長度修復後斷開仍然存在，請驗證受影響的客戶端裝置上是否禁用了Wi-Fi介面卡節能功能，因為這些設定可能會導致重新連線事件，這些事件在日誌中顯示為管理員重置條目。

原因

管理員重置事件的根本原因是思科安全訪問中的後端處理限制，其中VPN配置檔名稱超過46個字元

會導致會話管理期間出現系統錯誤。當後端系統遇到名稱長於此限制的VPN配置檔案時，會觸發管理員重置以終止受影響的會話作為保護措施。

之所以會出現此問題，是因為GUI介面允許使用者建立長度超過46個字元的VPN配置檔名稱，但後端處理系統具有嚴格的46個字元限制。後端處理較大字串長度時，會導致記錄管理員重置事件並強制斷開關聯VPN會話的連線。

相關內容

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）。