由於端點安全狀態合規性問題，安全客戶端AnyConnect VPN訪問被拒絕

目錄

問題

多個使用者無法連線到AnyConnect VPN和零信任訪問(ZTA)，並收到錯誤消息「Login denied（登入被拒絕）」。您的環境不符合管理員定義的訪問條件。"

此問題與端點安全狀態合規性相關，其中端點安全代理要求報告為不匹配。使用者嘗試通過Cisco Secure Client連線時會遇到VPN和ZTA訪問拒絕。

狀態評估顯示，Trellix端點安全狀態在受影響的端點上失敗，阻止對VPN服務的成功身份驗證。

環境

- 思科安全使用者端（AnyConnect和零信任存取）
- Trellix端點安全代理版本5.8.4.505
- VPN狀態配置檔案：實施終端安全代理的KFIN_SECURE_VPN
- 安全狀態要求：終端安全代理正在運行，且更新在最近14天內
- 運行Trellix代理服務的Windows終結點
- 在終端上檢測到Umbrella代理進程

解析

通過解決Trellix端點安全代理狀態合規性問題解決了此問題。實施了在下一節中介紹的故障排除和

解決步驟。

步驟 1:驗證狀態配置檔案配置

檢視VPN狀態配置檔案以確認終端安全代理要求。KFIN_SECURE_VPN配置檔案強制終端安全代理必須在過去14天內運行和更新。

步驟 2:驗證Trellix端點安全狀態

檢查受影響端點上的Trellix端點安全代理的當前狀態：

```
Trellix Agent Service: masvc.exe
Version: 5.8.4.505
Install Location: C:\Program Files\McAfee\Agent\
Display Name: Trellix Agent
Publisher: Trellix
```

步驟 3:重新安裝Trellix端點安全

在受影響的終端上執行Trellix Endpoint Security的完整重新安裝：

1.完全解除安裝現有的Trellix Endpoint Security代理。

2.重新啟動系統。

3.按照組織標準安裝最新批准的Trellix代理版本。

4.確保代理在安裝後成功運行。

5.確認簽名/內容更新已成功完成。

步驟 4:為思科安全客戶端(ZTA)啟用TRACE日誌記錄

啟用詳細日誌記錄以捕獲狀態評估詳細資訊。

使用以下內容建立logconfig.json檔案：

```
{ "global": "DBG_TRACE" }
```

將檔案放在適當的目錄中：

- Windows:C:\ProgramData\Cisco\Cisco安全客戶端\ZTA
- macOS:/opt/cisco/secureclient/zta

建立檔案後重新啟動Cisco Secure Client/ZTA服務。

步驟 5:收集更新的DART捆綁包

實施更改後，收集新的DART捆綁包以驗證解決方案並確認正確的狀態合規性檢測。

原因

根本原因被確定為Trellix端點安全代理狀態合規性問題。VPN終端安全配置檔案要求終端安全代理在最近14天內運行並更新，但Trellix終端安全代理不符合這些合規性標準。狀態評估模組無法正確檢測或驗證終端安全代理狀態，導致VPN和ZTA連線的訪問被拒絕。此問題具體與Trellix代理配置有關，需要Trellix支援團隊進行干預以解決基礎代理合規性問題。

相關內容

- 收集詳細的ZTNA日誌以進行故障排除

- 思科技術支援與下載

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）。