

MacOS休眠後安全客戶端ZTNA DNS解析和連線丟失

目錄

問題

在系統從睡眠或休眠模式恢復後，MacOS終端上的Cisco SecureClient ZTNA會遇到DNS解析失敗和ZTA連線丟失。此問題同時影響ZTNA IA（身份訪問）和ZTNA PA（專用訪問）功能。雖然基本IP連線仍可運作（對外部IP位址（例如8.8.8.8和208.67.222.222）的ICMP ping成功運作），但DNS名稱解析完全失敗，導致無法存取透過ZTNA設定的網際網路資源和私人資源。

觀察到的具體症狀包括：

- 使用nslookup命令時DNS查詢失敗(例如www.cisco.com的nslookup通過8.8.8.8和208.67.222.222不起作用)。
- ZTNA IA和ZTNA PA連線不可用。
- 在終端休眠和喚醒週期之後始終出現問題。
- 當裝置處於活動使用狀態時，問題也可能隨機發生。
- 終止ZTNA進程會導致立即重新啟動，但連線問題通常仍然存在。
- 只有完整的系統重新啟動才能恢復完整的DNS解析和ZTNA連線。

環境

- 作業系統：macOS（版本26.3已記錄案例）
- Cisco SecureClient:5.1.14.x版（5.1.16之前的受影響版本）
- ZTNA模組：同時使用身份訪問(IA)和專用訪問(PA)配置
- 網路監控：可以包括Sentinel One等第三方安全解決方案

- 其他安全軟體：可包括思科安全終端
- DNS伺服器：可通過ICMP訪問外部DNS伺服器(8.8.8.8、208.67.222.222)，但DNS解析失敗
- UMB模組：未使用

解析

此問題已通過思科工程部門提供的軟體修復程式解決。解決過程涉及以下各節中介紹的步驟。

步驟 1:問題識別與錯誤追蹤

思科工程部門發現這是已知缺陷，並將其記錄在Cisco錯誤ID CSCwt24392下，說明為「macOS:DNS停止使用ZTA SIA-all和NVM活動」。

步驟 2:診斷資料收集

收集此診斷資訊以支援工程分析：

- 來自受影響終端的DART (診斷和報告工具) 捆綁包。
- 封包擷取檔案 (ZTNA問題1.pcapng) 。
- 顯示連線故障的螢幕快照。
- 顯示問題重現的螢幕錄製。
- 顯示com.cisco.secureclient.zta.app.service和系統擴展進程行為的進程互動日誌。

步驟 3:工程修復程式開發

Cisco Engineering為CSCwt24392開發了一個目標修復程式，並將其包含在SecureClient版本5.1.16中。該修復程式專門解決ZTA SIA-all和NVM在休眠/休眠週期後，在macOS系統上處於活動狀態時發生的DNS解析故障。

步驟 4:軟體更新安裝

在受影響的macOS終端上安裝Cisco SecureClient 5.1.16版或更高版本。此版本包含DNS解析和ZTA連線問題的修補程式。

步驟 5:驗證測試

安裝SecureClient 5.1.16後，執行以下驗證步驟：

1. — 允許macOS終結點進入睡眠或休眠模式。
2. — 將系統從睡眠或休眠中喚醒。
3. — 使用nslookup命令測試DNS解析。
4. — 檢驗ZTNA IA和ZTNA PA與配置資源的連線。
5. — 確認網際網路訪問和私有資源訪問均能正常工作，而無需重新啟動系統。

早期版本的解決方法

對於無法立即升級到SecureClient 5.1.16的環境，可以使用以下臨時解決方法：

- 在每個睡眠/休眠週期後執行完整的系統重新引導以恢復DNS解析和ZTNA連線。
- 如果睡眠/休眠問題顯著影響工作效率，請考慮暫時從ZTNA註銷（請注意，這樣做會刪除ZTNA保護）。

原因

此問題的根本原因是低於5.1.16的Cisco SecureClient版本中的軟體缺陷，特別是被跟蹤為Cisco錯

誤ID CSCwt24392。當ZTA（零信任訪問）SIA-all（安全網際網路訪問）和NVM（網路可視性模組）元件在macOS系統上處於活動狀態時，會出現此缺陷。在睡眠或休眠和喚醒週期期間，這些元件無法正確恢復DNS解析功能，同時保持基本IP連線。這會導致ICMP流量(ping)正常運作，但DNS查詢失敗，從而有效地阻止對網際網路資源和受ZTNA保護的專用資源的訪問。該問題涉及com.cisco.secureclient.zta.app.service進程與系統狀態轉換期間系統擴展進程之間的不當互動。

相關內容

- 思科錯誤ID CSCwt24392 - macOS:DNS停止使用ZTA SIA-all和NVM活動
- [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）。