Cisco安全端點Mac聯結器故障

目錄

簡介

聯結器在檢測到影響聯結器正常工作的條件時，可能會通知您發生了故障引發事件。同樣，「已清除故障」事件通知不再存在該條件。

聯結器故障表

下表介紹了故障和相應的診斷步驟。

故障ID	門戶文本	終端說明	疑難排解/解決方案
1	核心模組未授權	未授權系統擴展	已阻止執行聯結器的系統擴展。 開啟安全和隱私系統首選項並批准擴展。 或者，可以使用流動裝置管理(MDM)配置檔案遠端批准系統擴展。
2	版本不匹配	系統擴展版本不匹配	安裝的聯結器軟體已損壞。重新安裝聯結器。 注意：運行Mac Connector 1.14.0版及更高版本時，重新啟動電腦可能會清除此的某些發生。
3	未授予磁碟訪問許可權	未授予完整磁碟訪問許可權	聯結器無法訪問要掃描的使用者檔案。開啟「安全和隱私系統首選項」(Securit Privacy System Preferences)並授予對AMP服務的全磁碟訪問許可權。 對於1.14.0之前的Mac聯結器版本，此過程名為*/opt/cisco/amp/ampdaemon*。 對於Mac Connector 1.14.0版及更高版本，以下兩個應用程式需要完全磁碟訪問體取決於macOS版本： • *AMP端點版 服務*（所有macOS版本都需要該服務） • *AMP安全擴展*（在macOS 10.15.5及更高版本上需要） 對於Mac Connector 1.14.1版及更高版本，以下兩個應用程式需要完全磁碟訪問體取決於macOS版本： • *AMP端點版 服務*（所有macOS版本都需要該服務） • *AMP安全擴展*（在macOS 11及更高版本上需要） 此技術說明中提供其他詳細資訊。
4	未載入核心模組	無法載入系統擴展；重新安裝聯結器	對於1.14.0之前的Mac Connector版本，或在macOS 10.14或10.15上運行時，此表示聯結器的系統擴展是正確的版本，已批准執行，但仍然無法載入。有關詳情參閱*/Library/Logs/Cisco/ampdaemon.log*。解除安裝並重新安裝聯結器也可能清故障。
5	掃描服務使用者不可用	掃描服務使用者不可用	聯結器無法建立使用者來運行檔案掃描進程。聯結器可通過使用root使用者執行掃描來解決此問題。這偏離了預期的設計並且是不預期的。 如果 `cisco-amp-scan-svc` 使用者或組已被刪除，或者使用者和組的配置已更改，安裝聯結器將重新建立具有必要配置的使用者和組。欲知更多詳情，請訪問*/Library/Logs/Cisco/ampdaemon.log*.

			聯結器的檔案掃描進程遇到反複故障，聯結器已重新啟動以嘗試清除故障。系統 一個或多個檔案可能導致掃描演算法在掃描時崩潰。聯結器繼續盡力掃描。
6	掃描服務頻繁重新啟動	掃描服務頻繁重新啟動	如果在聯結器啟動後10分鐘內沒有自動清除此故障，則表示需要進一步使用者干 ，並且聯結器的執行掃描能力將降低。 檢閱 */Library/Logs/Cisco/ampdaemon.log* 和 */Library/Logs/Cisco/ampscansvc.* 解詳細資訊。
7	無法啟動掃描服務	無法啟動掃描服務	聯結器的檔案掃描進程無法啟動，聯結器已重新啟動以嘗試清除故障。引發此故 ，檔案掃描功能被禁用。 如果在載入新安裝的病毒定義檔案（.cvd檔案）時遇到錯誤，則可能會觸發此故 在啟用新的.cvd檔案之前，聯結器會執行許多完整性和穩定性檢查以防止此故障 新啟動時，聯結器將刪除所有無效的.cvd檔案，以便聯結器可以恢復。 如果在重新啟動聯結器時未清除此故障，則表明需要進一步使用者干預。如果每 行.cvd更新時都重複此故障，則表明聯結器的.cvd檔案完整性檢查未正確檢測到 的.cvd檔案。 檢閱 */Library/Logs/Cisco/ampdaemon.log* 和 */Library/Logs/Cisco/ampscansvc.* 解詳細資訊。 重新啟動系統。
10	載入核心模組或系統擴展需要重新啟動	載入系統擴展需要重新啟動	對於Mac Connector 1.11.1和1.14.0版，如果系統擴展無法載入，可能會引發此 。在這種情況下，可以通過重新安裝聯結器來清除此故障。 請注意，如果系統上安裝了太多網路內容過濾器系統擴展，Mac Connector 1.1 更高版本可能會引發此故障。如果重新啟動電腦未清除此故障，請參閱以下故障 南以瞭解其他詳細資訊。 策略中的「啟用裝置流關聯」功能需要網路過濾器。若要清除此故障，請允許 終端的AMP服務」過濾終端上的網路內容。
12	不允許使用網路篩選器	不允許使用網路篩選器	通過按一下Agent選單中所列的活動故障並按照提供的指導，可以訪問允許網路 器的macOS對話方塊。 有關其他詳細資訊，包括用於遠端授權網路過濾器的MDM配置檔案設定，請參 技術筆記。
13	網路內容過濾器系統擴展太多	網路內容過濾器系統擴展太多	對於Mac Connector 1.14.0，在啟動網路內容過濾器系統擴展時由於macOS錯誤 常引發此故障。重新啟動電腦將清除此故障。 策略中的「啟用裝置流關聯」功能需要使用防火牆級別的macOS網路內容過濾器 MacOS 限制可以運行的網路內容過濾器的數量。 如果出現此故障，並且未通過重新啟動電腦來清除，解除安裝不再需要的防火牆 路內容過濾器並重新啟動聯結器。
14	終端安全系統擴展太多	Endpoint Security系統擴展太多	MacOS限制可以運行的Endpoint Security系統擴展的數量。Mac Connector要求 略中的「監視檔案複製和移動」和「監視進程執行」功能提供這些終端安全系統 名之一。 若要清除此故障，請解除安裝不再需要的終端安全系統擴展，然後重新啟動聯結
15	系統擴展需要完整磁	系統擴展需要完整磁碟訪問	Mac Connector的macOS系統擴展無法訪問要掃描的使用者檔案。開啟安全和隱 統首選項並授予對AMP安全擴展的*全磁碟訪問許可權*。

	碟訪問		本技術說明中提供了其他詳細資訊，包括用於通過系統擴展對全磁碟訪問進行遠權的MDM配置檔案設定。 請注意，macOS 11.0.0上的錯誤會導致在重新引導後自動清除全盤存取設定。誤已在macOS 11.0.1中修正。
17	未授予軌道全盤訪問	未授予軌道全盤訪問	**Orbital需要完全磁碟訪問，以訪問受保護的檔案和目錄以進行查詢。**開啟安全和系統首選項並授予對*Cisco* Orbital的完整磁*盤訪問許可權*。