對安全終端Linux聯結器故障進行故障排除

目錄

簡介

本文檔描述Cisco Secure Endpoint Linux聯結器用來通知您影響其正常運行的條件的故障。

背景資訊

當思科安全終端Linux聯結器檢測到影響聯結器正常工作的條件時，會通過故障引發事件發出通知。同樣，「已清除故障」事件通知不再存在該條件。

安全終結點Linux聯結器故障表

該表描述了故障及其關聯的診斷步驟。

故障ID	說明	疑難排解/解決方案
5	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。聯結器使用根使用者執行檔案掃描作為解決方法。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，然後您可以重新安裝聯結器，以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 /var/log/cisco/ampdaemon.log. 如果通過/etc/login.defs 中的設定限制使用者組的建立，則必須在安裝程式運行時臨時更改此檔案以允許建立使用者和組。為此，請將usergroups_enab從no更改為yes。 如果另一個程式修改了聯結器的一個目錄許可權（即/opt/cisco或子目錄），則在Linux聯結器1.15.1和更新版本中可能會引發此故障。要緩解此問題，必須將更改的目錄許可權重新設定為預設值（即0755），確保將來的程式不會修改/opt/cisco目錄（或任何子目錄），然後重新啟動聯結器服務。
6	掃描服務頻繁重	聯結器檔案掃描進程遇到重複的故障，聯結器已重新啟動以嘗試清除該故障

	新啟動	。系統上的一個或多個檔案可能會在掃描時導致掃描演算法崩潰。該聯結器以盡力掃描的方式繼續。 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預，並且聯結器執行掃描的能力已降低。 如需詳細資訊，請參閱/var/log/cisco/ampdaemon.log 和 /var/log/cisco/ampscansvc.log。
7	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。引發此故障時，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，則可能會觸發此故障。聯結器在啟用新的.cvd檔案以防止此故障之前，會執行許多完整性和穩定性檢查。重新啟動時，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。如果每次進行.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無效的.cvd檔案。 如果電腦的可用記憶體不足，並且掃描程式服務無法啟動，則在Linux聯結器中可以觸發此故障。有關Linux上的最低系統要求，請參閱《安全終端（前身為面向終端的AMP）使用手冊》。 如需詳細資訊，請參閱/var/log/cisco/ampdaemon.log 和 /var/log/cisco/ampscansvc.log。
8	即時檔案系統監視無法啟動	未載入提供即時檔案系統活動監視的核心模組，並且聯結器策略已啟用「監視檔案複製和移動」。出現此故障時，聯結器中的這些監視功能不可用。當安全終結點聯結器無法載入檔案系統活動監視所需的底層核心模組時，將引發此故障。 必須在系統上禁用UEFI安全引導。 如果禁用安全引導，則此故障可能是由隨安全終端聯結器提供的ampavflt或ampfsm核心模組與系統上安裝的系統核心或其他第三方核心模組之間的不相容造成的。檢視/var/log/messages以瞭解詳細資訊。 當運行聯結器不支援的核心版本時，也可能導致該故障。在這種情況下，可以通過為當前運行的系統核心構建自定義ampfsm核心模組來清除此漏洞。（適用於Linux聯結器版本1.16.0及更新版本。）有關構建自定義核心模組的更多資訊，請參閱：構建Cisco安全終端Linux聯結器核心模組
9	無法啟動即時網路監控	未載入提供即時網路活動監視的核心模組，並且聯結器策略已啟用「啟用裝置流關聯」。出現此故障時，此監控功能在聯結器中不可用。 當安全終結

		點聯結器無法載入檔案系統活動監視所需的底層核心模組時，將引發此故障。 必須在系統上禁用UEFI安全引導。 如果禁用安全引導，則此故障可能是由隨安全終端聯結器提供的ampavflt或ampfsm核心模組與系統上安裝的系統核心或其他第三方核心模組之間的不相容造成的。檢視/var/log/messages以瞭解詳細資訊。 當運行聯結器不支援的核心版本時，也可能導致該故障。在這種情況下，可以通過為當前運行的系統核心構建自定義ampfsm核心模組來清除此漏洞。（適用於Linux聯結器版本1.16.0及更新版本。）有關構建自定義核心模組的更多資訊，請參閱：構建Cisco安全終端Linux聯結器核心模組
11	缺少所需的核心級包	安全端點聯結器使用eBPF模組監控檔案系統、進程和網路活動。聯結器需要系統上具有某些可用軟體包來載入和運行這些eBPF模組。若要解決此故障，請按照如下所述安裝Linux發行版所需的程式包，然後重新啟動聯結器。 對於基於Red Hat的分發，當缺少核心級軟體包時引發此故障。安裝核心級軟體包並重新啟動聯結器。（僅適用於Linux聯結器版本1.13.0及更新版本。） 對於Oracle Linux UEK 6及更高版本，當核心級級別時，會引發此故障缺少包。安裝核心級程式包，然後重新啟動聯結器。（僅適用於Linux聯結器版本1.18.0及更新版本。） 對於基於Debian的分發，當缺少linux-headers包時，將引發此故障。安裝linux-headers程式包，然後重新啟動聯結器。（適用於Linux聯結器版本1.15.0及更新版本。） 有關詳情，請參閱：Linux核心級故障
16	不相容的核心	當前運行的核心與當前運行的聯結器不相容，並且聯結器策略已啟用「監視檔案複製和移動」或「啟用裝置流關聯」。 將核心降級到支援的版本，或將聯結器升級到支援此核心的較新版本。 有關支援的核心版本的詳細資訊，請參見：Cisco安全終端Linux聯結器OS相容性
18	聯結器事件監視超載	當由於系統事件數目過多而導致聯結器承受重負載時，會引發此故障。系統保護是有限的，並且聯結器會監控較小的一組系統關鍵事件，直到整體系統活動減少。 此故障可能是惡意系統活動或系統中非常活躍的應用程式的指示。

		如果活動應用程式是良性的且受使用者信任，則可以將其新增到進程排除集中，以減少聯結器上的監視負載。此操作可能足以清除故障。 如果沒有良性進程導致負載過重，則需要執行一些調查來確定活動增加是否由惡意進程引起。 如果聯結器在短時間內承受過載，則此故障可能會自行消除。 如果經常出現此故障，則不會存在會導致負載過重的良性進程，並且不會發現惡意進程，則需要重新調配系統來處理負載過重的進程。
19	SELinux策略缺失或禁用	當系統上的Secure Enterprise Linux(SELinux)策略阻止聯結器監視系統活動時，將引發此故障。如果已啟用SELinux且處於強制模式，則Connector在SELinux策略中需要此規則： `allow unconded_service_t self:bpf { map_create map_read map_write prog_load prog_run };` 在基於Red Hat的系統（包括RHEL 7和Oracle Linux 7）上，此規則在預設的SELinux策略中不存在。在安裝或升級期間，聯結器會嘗試通過安裝名為SELinux策略模組來新增此規則 `cisco-secure-bpf`.如果 `cisco-secure-bpf` 無法安裝和載入，或已被禁用，則會引發故障。 要解決故障，請確保安裝了系統軟體包policycoreutils-python。重新安裝或升級聯結器以觸發`cisco-secure-bpf`的安裝，或者手動將該規則新增到現有的SELinux策略並重新啟動聯結器。 有關修改SELinux策略以解決此故障的更多詳細說明，請參閱SELinux策略故障。

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）。