Cisco Secure Endpoint Linux Connector-Fehler

Inhalt

[Einleitung](#)
[Fehlertabelle des sicheren Endpunkt-Linux-Connectors](#)

Einleitung

Der Cisco Secure Endpoint Linux-Connector kann Sie über ein Fault Raised-Ereignis informieren, wenn er eine Bedingung erkennt, die das ordnungsgemäße Funktionieren des Connectors beeinträchtigt. Ebenso teilt ein Fault Cleared-Ereignis mit, dass die Bedingung nicht mehr vorhanden ist.

Fehlertabelle des sicheren Endpunkt-Linux-Connectors

In der folgenden Tabelle werden Fehler und entsprechende Diagnoseschritte beschrieben.

Fehler-ID	Beschreibung	Problembehebung/Problembehebung
5	Service-Benutzer prüfen nicht verfügbar	Beim Anschluss konnte kein Benutzer erstellt werden, um den Dateiprüfvorg auszuführen. Der Connector umgeht dies, indem er den Root-Benutzer zum Durchführen eines Dateiprüfens verwendet. Dies unterscheidet sich vom beabsichtigten Design und ist nicht zu erwarten. Wenn `cisco-amp-scan-svc` Benutzer oder Gruppe wurde gelöscht, oder die Konfiguration des Benutzers und der Gruppe wurde geändert. Durch die Neuinstallation des Connectors werden Benutzer und Gruppe mit der erforderlichen Konfiguration neu erstellt. Weitere Informationen finden Sie u */var/log/cisco/ampdaemon.log*. Wenn der Kunde die Erstellung von Benutzergruppen über die Einstellunge **/etc/login.defs** einschränkt, muss diese Datei während der Ausführung des Installationsprogramms vorübergehend geändert werden, um das Erstellen Benutzers und der Gruppe zu ermöglichen. Dies kann durch das Ändern vo **usergroups_enab** von no in yes erfolgen.
6	Häufig Neustarten des Scan-Services	Dieser Fehler kann in Linux Connectors 1.15.1 und höher ausgelöst werden wenn ein anderes Programm eine der Verzeichnisberechtigungen des Connectors modifiziert hat (z.B. /opt/cisco oder ein untergeordnetes Verzeic Um dies zu verhindern, sollte die geänderte Verzeichnisberechtigung auf de Standardwert zurückgesetzt werden (d. h. 0755), stellen Sie sicher, dass ke zukünftigen Programme das Verzeichnis /opt/cisco (oder ein untergeordnete Verzeichnis) ändern, und starten Sie den Connector-Dienst neu. Beim Dateiprüfprozess des Connectors sind wiederholte Fehler aufgetreten der Connector wurde neu gestartet, um den Fehler zu beheben. Möglicherw verursacht eine oder mehrere Dateien im System einen Absturz des Scan-Algorithmus beim Scannen. Der Connector wird weiterhin bestmöglich gesc Wenn dieser Fehler nicht automatisch innerhalb von 10 Minuten nach dem des Steckverbinders behoben wird, ist dies ein Hinweis darauf, dass weitere

		Benutzereingriffe erforderlich sind und die Fähigkeit des Steckverbinders, Prüfungen durchzuführen, beeinträchtigt wird. Weitere Informationen finden Sie unter */var/log/cisco/ampdaemon.log* und */var/log/cisco/ampscansvc.log*.
7	Scan-Service konnte nicht gestartet werden	Der Dateiprüfprozess des Connectors konnte nicht gestartet werden, und de Connector wurde neu gestartet, um den Fehler zu beheben. Die Dateiprüfungsfunktion ist deaktiviert, während dieser Fehler ausgelöst wird. Dieser Fehler kann ausgelöst werden, wenn beim Laden einer neu installier Virendefinitionsdatei (.cvd-Dateien) ein Fehler auftritt. Der Connector führt v der Aktivierung neuer CSD-Dateien eine Reihe von Integritätsprüfungen und Stabilitätsprüfungen durch, um diesen Fehler zu verhindern. Beim Neustart werden alle ungültigen CSVD-Dateien vom Anschluss entfernt, sodass der Anschluss wieder aufgenommen werden kann. Wenn dieser Fehler beim Neustart des Connectors nicht behoben wird, ist d ein Hinweis darauf, dass weitere Benutzereingriffe erforderlich sind. Wenn s dieser Fehler mit jedem CVD-Update wiederholt, ist dies ein Hinweis darauf dass eine ungültige CSVD-Datei nicht richtig von den cvd-Dateiintegritätsprüfungen des Connectors erkannt wird. Dieser Fehler kann in Linux-Anschlüssen ausgelöst werden, wenn der Com mit wenig verfügbarem Speicher ausgeführt wird und der Scannerdienst nic starten kann. Informationen zu den Mindestsystemanforderungen für Linux Sie im Benutzerhandbuch für sichere Endgeräte (ehemals AMP für Endgerä Weitere Informationen finden Sie unter */var/log/cisco/ampdaemon.log* und */var/log/cisco/ampscansvc.log*.
8	Realtime-Dateisystemmonitor konnte nicht gestartet werden	Das Kernel-Modul, das eine Überwachung der Dateisystemaktivität in Echt bereitstellt, wurde nicht geladen, und die Connector-Richtlinie hat "Monitor F Copies and Moves" aktiviert. Diese Überwachungsfunktionen sind im Ansch nicht verfügbar, während der Fehler ausgelöst wird. Dieser Fehler wird ausg wenn der Secure Endpoint Connector das zugrunde liegende Kernelmodul, für die Überwachung der Dateisystemaktivität erforderlich ist, nicht laden ka UEFI Secure Boot muss im System deaktiviert sein. Wenn Secure Boot deaktiviert ist, kann dieser Fehler durch eine Inkompatib zwischen dem ampavflt- oder ampfsm-Kernelmodul mit dem Secure Endpoi Anschluss und dem System-Kernel oder anderen auf dem System installiert Kernelmodulen von Fremdherstellern verursacht werden. Lesen Sie Details *var/log/messages*, oder deaktivieren Sie die Dateiüberwachung in den Richtlinieneinstellungen des Connectors, um diesen Fehler zu beheben. Der Fehler kann auch bei der Ausführung einer Kernel-Version verursacht werden, die vom Connector nicht unterstützt wird. In diesem Fall wird es möglicherweise gelöscht, indem ein benutzerdefiniertes ampfsm-Kernelmod den aktuellen Kernel des laufenden Systems erstellt wird. (Gilt für Linux Connector Versionen 1.16.0 und höher.) Weitere Informationen zum Erstelle benutzerdefinierter Kernelmodule finden Sie unter: Erstellen von Cisco Secu Endpoint Linux Connector Kernel-Modulen
9	Realtime Network Monitor konnte nicht gestartet werden	Das Kernel-Modul, das eine Überwachung der Netzwerkaktivität in Echtzeit bereitstellt, wurde nicht geladen, und die Connector-Richtlinie hat "Enable D Flow Correlation" aktiviert. Diese Überwachungsfunktion ist im Anschluss ni verfügbar, während dieser Fehler ausgelöst wird. Dieser Fehler wird ausgel

11	Erforderliches Kernel-Devel-Paket fehlt	wenn der Secure Endpoint Connector das zugrunde liegende Kernelmodul, für die Überwachung der Dateisystemaktivität erforderlich ist, nicht laden ka UEFI Secure Boot muss im System deaktiviert sein. Wenn Secure Boot deaktiviert ist, kann dieser Fehler durch eine Inkompatib zwischen dem ampavflt- oder ampfsm-Kernelmodul mit dem Secure Endpoi Anschluss und dem System-Kernel oder anderen auf dem System installiert Kernelmodulen von Fremdherstellern verursacht werden. Lesen Sie Details *var/log/messages*, oder deaktivieren Sie die Dateiüberwachung in den Richtlinieneinstellungen des Connectors, um diesen Fehler zu beheben. Der Fehler kann auch bei der Ausführung einer Kernel-Version verursacht werden, die vom Connector nicht unterstützt wird. In diesem Fall wird es möglicherweise gelöscht, indem ein benutzerdefiniertes ampfsm-Kernelmod den aktuellen Kernel des laufenden Systems erstellt wird. (Gilt für Linux Connector Versionen 1.16.0 und höher.) Weitere Informationen zum Erstelle benutzerdefinierter Kernelmodule finden Sie unter: Erstellen von Cisco Secu Endpoint Linux Connector Kernel-Modulen Bei Red Hat-basierten Distributionen fehlt das Kernel-Devel-Paket, das für d Überwachung von Dateisystemen und Netzwerkaktivitäten in Echtzeit erforc ist, und die Connector-Richtlinie hat entweder "Monitor File Copies and Mov oder "Enable Device Flow Correlation" aktiviert. Dieser Fehler wird ausgelös wenn der Secure Endpoint Connector das zugrunde liegende eBPF-Modul, für die Überwachung der Dateisystemaktivität erforderlich ist, nicht kompilie und laden kann. Installieren Sie das Kernel-Devel-Paket für den derzeit laufenden Kernel un starten Sie den Connector neu, oder deaktivieren Sie diese Features in der Richtlinie, um diesen Fehler zu beheben. (Gilt nur für Linux Connector Vers 1.13.0 und höher.) Für Oracle Linux UEK 6 und höher ist das kernel-uek-devel-Paket für diese Funktionen erforderlich. Installieren Sie das kernel-uek-devel-Paket für den derzeit laufenden Kernel und starten Sie den Connector neu, oder deaktivie Sie diese Features in der Richtlinie, um diesen Fehler zu beheben. (Gilt nur Linux Connector Versionen 1.18.0 und höher.) Für Debian-basierte Distributionen ist das Linux-Header-Paket für diese Funktionen erforderlich. Installieren Sie das Linux-Headers-Paket für den ak laufenden Kernel und starten Sie den Connector neu, oder deaktivieren Sie Features in der Richtlinie, um diesen Fehler zu beheben. (Gilt für Linux Connector Versionen 1.15.0 und höher.) Weitere Informationen finden Sie unter: Linux Kernel-Devel-Fehler
16	Inkompatibler Kernel	Der aktuell ausgeführte Kernel ist nicht mit dem aktuell ausgeführten Conne kompatibel, und die Connector-Richtlinie hat entweder "Monitor File Copies Moves" (Kopien und Verschiebungen von Überwachungsdateien) oder "Ena Device Flow Correlation" (Gerätefluss-Korrelation aktivieren) aktiviert. Führen Sie ein Downgrade des Kernels auf eine unterstützte Version durch, aktualisieren Sie den Connector auf eine neuere Version, die diesen Kernel unterstützt. Ausführliche Informationen zu unterstützten Kernel-Versionen finden Sie unter: Kompatibilität des Cisco Secure Endpoint Linux Connector OS