Fouten in Secure Endpoint Linux-connector oplossen

Inhoud

Inleiding

Dit document beschrijft fouten die de Cisco Secure Endpoint Linux-connector gebruikt om u op de hoogte te stellen van voorwaarden die het correct functioneren van de connector beïnvloeden.

Achtergrondinformatie

De Cisco Secure Endpoint Linux-connector waarschuwt bij een fout-verhoogde gebeurtenis wanneer hij een voorwaarde detecteert die de juiste werking van de connector beïnvloedt. Op dezelfde manier communiceert een gebeurtenis met de foutmelding dat de aandoening niet langer aanwezig is.

Fouttabel voor Secure Endpoint Linux Connector

In de tabel worden fouten en de bijbehorende diagnostische stappen beschreven.

Fout-ID	**Beschrijving**	**Probleemoplossing/oplossing**
5	Scannen naar gebruiker niet beschikbaar	De connector is er niet in geslaagd een gebruiker te maken om de bestandsscanprocedure uit te voeren. De connector gebruikt de hoofdgebruiker om bestanden te scannen als tijdelijke oplossing. Dit wijkt af van het beoogde ontwerp en wordt niet verwacht. Indien de `Cisco Cisco-amp-scan-svc` de gebruiker of groep is verwijderd, of de configuratie van de gebruiker en groep is gewijzigd, dan kunt u de connector opnieuw installeren om de gebruiker en groep opnieuw te maken met de benodigde configuraties. Aanvullende informatie is beschikbaar in */var/log/cisco/ampdaemon.log*. Als de gebruikersgroep alleen kan worden gemaakt via de instellingen in **/etc/login.defs**, moet dit bestand tijdelijk worden gewijzigd terwijl het installatieprogramma wordt uitgevoerd, zodat de gebruiker en de groep kunnen worden gemaakt. Om dit te doen, verander **usergroups_enab** van nee in ja. Deze fout kan worden verhoogd in Linux-connectors 1.15.1 en nieuwer als een ander programma een van de directory-permissies van

		de connector heeft gewijzigd (dat is /opt/cisco of een child directory). Om dit te verhelpen, moet de gewijzigde directory toestemming worden teruggezet naar standaard (d.w.z. 0755), ervoor zorgen dat geen toekomstige programma's de /opt/cisco directory (of een onderliggende directory) wijzigen, en de connector service opnieuw starten.
6	Scanservice wordt vaak opnieuw gestart	Het scanproces van het verbindingsbestand heeft herhaaldelijk fouten aangetroffen en de connector is opnieuw gestart in een poging om de fout te verhelpen. Het is mogelijk dat een of meer bestanden op het systeem ervoor zorgen dat de scanalgoritme crasht wanneer het gescand wordt. De connector gaat verder met scannen op basis van de best mogelijke inspanning. Als deze fout niet automatisch wordt gewist binnen 10 minuten nadat de connector is gestart, is dit een indicatie dat verdere tussenkomst van de gebruiker vereist is en is de capaciteit van de connector om scans uit te voeren minder groot. Surf naar */var/log/cisco/ampdaemon.log* en */var/log/cisco/ampscansvc.log* voor meer informatie.
7	Scanservice is niet gestart	Het scanproces van het bestand van de connector is niet gestart en de connector is opnieuw gestart in een poging om de fout te verhelpen. De functionaliteit voor het scannen van bestanden is uitgeschakeld terwijl deze fout wordt veroorzaakt. Deze fout kan worden geactiveerd als er een fout wordt aangetroffen tijdens het laden van een nieuw geïnstalleerd virus definitie bestanden (.cvd bestanden). De -connector voert een aantal integriteits- en stabiliteitscontroles uit voordat nieuwe .cvd-bestanden worden geactiveerd om deze storing te voorkomen. Bij het opnieuw opstarten, verwijdert de connector alle ongeldige .cvd-bestanden zodat de connector kan hervatten. Als deze fout niet wordt gewist wanneer de connector opnieuw wordt opgestart, is dit een indicatie dat verdere tussenkomst van de gebruiker vereist is. Als deze fout zich herhaalt bij elke .cvd update dan is dit een indicatie dat een ongeldig .cvd bestand niet goed wordt gedetecteerd door de .cvd bestandsintegriteitscontroles van de connector. Deze fout kan worden geactiveerd in Linux-connectors als de machine bijna geen beschikbaar geheugen heeft en de scannerservice niet kan starten. Raadpleeg de "Secure Endpoint (voorheen AMP for Endpoints)"-gebruikershandleiding voor de minimale systeemvereisten op Linux. Surf naar */var/log/cisco/ampdaemon.log* en */var/log/cisco/ampscansvc.log* voor meer informatie.
8	Realtime	â€‹De kernel module die realtime bestandssysteem activiteit

	bestandssysteemmonitor is niet gestart	monitoring biedt is niet geladen en het connector beleid heeft "Monitor File Copies and Moves" ingeschakeld. Deze controlefuncties zijn niet beschikbaar in de connector terwijl deze fout wordt opgeheven. Deze fout wordt veroorzaakt wanneer de Secure Endpoint connector niet in staat is om de onderliggende kernel module te laden die nodig is voor bestandssysteem activiteit monitoring. UEFI Secure Boot moet op het systeem zijn uitgeschakeld. Als Secure Boot is uitgeschakeld, kan deze fout worden veroorzaakt door een incompatibiliteit tussen de ampavflt- of ampfsm-kernelmodule die is voorzien van de Secure Endpoint-connector en de systeemkernel of andere kernel-modules van derden die op het systeem zijn geïnstalleerd. Bekijk */var/log/*message voor meer informatie of schakel bestandbewaking uit in de instellingen van het verbindingsbeleid om deze fout uit te schakelen. De fout kan ook worden veroorzaakt bij het uitvoeren van een kernel versie die niet wordt ondersteund door de connector. In dit geval kan het worden gezuiverd door het bouwen van een aangepaste ampfsm kernel module voor de huidige lopende systeem kernel. (Van toepassing op Linux-connectorversies 1.16.0 en nieuwer.) Voor meer informatie over het bouwen van aangepaste kernelmodules raadpleegt u: Building Cisco Secure Endpoint Linux Connector Kernel Modules
9	Realtime netwerkmonitor kan niet worden gestart	De kernel module die real-time netwerkactiviteit bewaking biedt is niet geladen en het connector beleid heeft "Enable Device Flow Correlatie" ingeschakeld. Deze controlefunctie is niet beschikbaar in de connector terwijl deze fout wordt opgeheven. Deze fout wordt veroorzaakt wanneer de Secure Endpoint connector niet in staat is om de onderliggende kernel module te laden die nodig is voor bestandssysteem activiteit monitoring. UEFI Secure Boot moet op het systeem zijn uitgeschakeld. Als Secure Boot is uitgeschakeld, kan deze fout worden veroorzaakt door een incompatibiliteit tussen de ampavflt- of ampfsm-kernelmodule die is voorzien van de Secure Endpoint-connector en de systeemkernel of andere kernel-modules van derden die op het systeem zijn geïnstalleerd. Bekijk */var/log/*message voor meer informatie of schakel bestandbewaking uit in de instellingen van het verbindingsbeleid om deze fout uit te schakelen. De fout kan ook worden veroorzaakt bij het uitvoeren van een kernel versie die niet wordt ondersteund door de connector. In dit geval kan het worden gezuiverd door het bouwen van een aangepaste ampfsm kernel module voor de huidige lopende systeem kernel. (Van toepassing op Linux-connectorversies 1.16.0 en nieuwer.) Voor meer informatie over het bouwen van aangepaste kernelmodules raadpleegt u: Building Cisco Secure Endpoint Linux Connector Kernel Modules
11	Vereiste kernel-devel	Voor Red Hat gebaseerde distributies ontbreekt het kernel-devel

	pakket ontbreekt	pakket dat vereist is voor realtime bestandssysteem en netwerkactiviteit bewaking en het connectorbeleid heeft "Monitor File Copies and Moves" of "Enable Device Flow Correlatie" ingeschakeld. Deze fout wordt veroorzaakt wanneer de Secure Endpoint connector niet in staat is de onderliggende eBPF-module te compileren en laden die vereist is voor bestandssysteem activiteitsbewaking. Installeer het kernel-devel pakket voor de momenteel lopende kernel en start de connector opnieuw, of schakel deze functies uit in het beleid om deze fout te verwijderen. (Alleen van toepassing op Linux-connectorversies 1.13.0 en nieuwer.) Voor Oracle Linux UEK 6 en nieuwer is voor deze functies het kernel-uek-devel pakket vereist. Installeer het kernel-uek-devel pakket voor de momenteel lopende kernel en start de connector opnieuw, of schakel deze functies uit in het beleid om deze fout te verwijderen. (Alleen van toepassing op Linux-connectorversies 1.18.0 en nieuwer.) Voor op Debian gebaseerde distributies is het pakket linux-headers vereist voor deze functies. Installeer het linux-headers pakket voor de momenteel actieve kernel en start de connector opnieuw, of schakel deze functies uit in het beleid om deze fout te wissen. (Van toepassing op Linux-connectorversies 1.15.0 en nieuwer.) Zie voor meer informatie: Linux Kernel-Devel-fout
16	Incompatibele kernel	De momenteel actieve kernel is niet compatibel met de momenteel actieve connector en het aansluitbeleid heeft "Monitor File Copies and Moves" of "Enable Device Flow Correlatie" ingeschakeld. Downgrade de kernel naar een ondersteunde versie of upgrade de connector naar een nieuwere versie die deze kernel ondersteunt. Zie voor meer informatie over ondersteunde kernelversies: Compatibiliteit met Cisco Secure Endpoint Linux Connector
18	Connector-gebeurtenisbewaking is overbelast	Deze fout wordt opgeheven wanneer de connector onder zware belasting staat als gevolg van overweldigende gebeurtenissen in het getalsysteem. De systeembescherming is beperkt en de connector bewaakt een kleinere reeks systeemkritische gebeurtenissen totdat de totale systeemactiviteit is verminderd. Deze fout kan een indicatie zijn van kwaadaardige systeemactiviteit of van zeer actieve toepassingen op het systeem. Als een actieve toepassing benigne is en door de gebruiker wordt vertrouwd, dan kan deze worden toegevoegd aan een uitsluiting van het proces die is ingesteld om de controlebelasting op de connector te verminderen. Deze actie kan genoeg zijn om de fout weg te nemen.

		Als geen goedaardige processen zware belasting veroorzaken, dan is enig onderzoek vereist om te bepalen of de verhoogde activiteit toe te schrijven is aan een kwaadaardig proces. Als de connector kortstondig zwaar belast is, is het mogelijk dat deze fout vanzelf kan verdwijnen. Als deze fout vaak wordt verhoogd, zijn er geen goedaardige processen die zware lading veroorzaken, en geen kwaadaardige processen werden ontdekt, dan moet het systeem worden herprovisioneerd om zwaardere ladingen te behandelen.
19	SELinux-beleid ontbreekt of is uitgeschakeld	Deze fout wordt veroorzaakt wanneer het beleid van Secure Enterprise Linux (SELinux) op het systeem de Connector verhindert de systeemactiviteit te controleren. Als SELinux is ingeschakeld en in de afdwingingsmodus staat, vereist de Connector deze regel in het SELinux-beleid: `toestaan unconfined_service_t self:bpf { map_creative map_read_write prog_load prog_run};` Op Red Hat-gebaseerde systemen, waaronder RHEL 7 en Oracle Linux 7, is deze regel niet aanwezig in het standaard SELinux-beleid. Tijdens een installatie of upgrade probeert de Connector deze regel toe te voegen via de installatie van een SELinux Policy Module met de naam `Cisco Cisco-Secure-BPF`. Indien `Cisco Cisco-Secure-BPF` installatie en lading mislukt, of is uitgeschakeld, wordt de fout hersteld. Om de fout op te lossen, installeer of upgrade de Connector om de installatie van cisco-secure-bpf te starten, of voeg de regel handmatig toe aan het bestaande SELinux-beleid en start de Connector opnieuw. Zie SELinux Policy Fault voor meer informatie over het wijzigen van het SELinux Policy om deze fout op te lossen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.