Cisco Secure Endpoint Linux-connector

Inhoud

Inleiding

De Cisco Secure Endpoint Linux-connector kan u op de hoogte stellen van een optie die door fouten wordt verhoogd wanneer deze een toestand detecteert die de juiste werking van de connector beïnvloedt. Op dezelfde manier communiceert een Fault Cleared-event dat de conditie niet langer aanwezig is.

Secure Endpoint Linux Connector - functietabel

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

ID fout	Beschrijving	Probleemoplossing/oplossing
5	Scan de servicetechnicus niet beschikbaar	De connector heeft geen gebruiker gemaakt om het proces voor het scanne bestanden uit te voeren. De connector werkt hieraan door de basisgebruike gebruiken om een bestandsscan uit te voeren. Dit wijkt af van het beoogde ontwerp en wordt niet verwacht. Als de `cisco-amp-scan-svc` De gebruiker of groep is verwijderd of de configur van de gebruiker en de groep is gewijzigd. Als u de connector opnieuw installeert, worden de gebruiker en de groep opnieuw gecreëerd met de benodigde configuratie. Er zijn aanvullende gegevens beschikbaar in */var/log/cisco/ampdaemon.log*. Als de klant het maken van gebruikersgroepen beperkt via de instellingen in **/etc/login.defs** moet dit bestand tijdelijk worden gewijzigd terwijl het installatieprogramma uitgevoerd wordt om de gebruiker en de groep te kunn maken. Dit kan gedaan worden om **gebruikersgroepen_enab** van nee in ja t veranderen.
6	Scanservice vaak opnieuw starten	Deze fout kan worden opgevoerd in Linux-connectors 1.15.1 en nieuwer als ander programma de adressering van een van de connector wijzigt (d.w.z. /opt/cisco of een kindfolder). Om dit te verzachten, moet de veranderde fold toestemming terug naar default (d.w.z. 0755), ervoor zorgen dat geen toekomstige programma's de /opt/cisco-directory (of enige kindergidsen) wij en de verbindingsdienst opnieuw opstarten. Het bestandsscanproces van de connector kwam op herhaalde fouten en d connector is opnieuw begonnen in een poging de storing op te heffen. Het i mogelijk dat een of meer bestanden op het systeem ervoor zorgen dat het scanalgoritme verandert wanneer het gescand wordt. De connector gaat ve met scans 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 de gebruiker nog meer moet ing

		en dat de capaciteit van de connector om scans uit te voeren wordt aangeta Zie */var/log/cisco/ampdaemon.log* en */var/log/cisco/ampscansvc.log* voor m informatie.
7	Scanservice is niet gestart	Het bestandsscanproces van de connector is niet gestart en de connector is opnieuw gestart in een poging de storing op te heffen. De functionaliteit voo scannen van bestanden is uitgeschakeld als deze fout is verhoogd. Deze fout kan worden geactiveerd als een fout wordt aangetroffen bij het la van een nieuw geïnstalleerd virus definitiebestanden (.cvd-bestanden). De connector voert een aantal integriteit- en stabiliteitscontroles uit voordat er nieuwe .cvd-bestanden worden geactiveerd om deze storing te voorkomen. het opnieuw opstarten verwijdert de connector alle ongeldige .cvd-bestande zodat de connector kan worden hervat. Als deze fout niet wordt gewist wanneer de connector opnieuw wordt gestar dit een indicatie dat de gebruiker nog meer moet ingrijpen. Als deze fout op optreedt met elke .cvd-update dan is dit een indicatie dat een ongeldig .cvd-bestand niet correct wordt gedetecteerd door de controles van de .cvd-bestandsintegriteit van de connector. Deze fout kan in de Linux-connectors worden veroorzaakt als de machine n actief is op het beschikbare geheugen en de scannerservice niet kan starter Raadpleeg de "Secure Endpoint (voorheen AMP voor endpoints)" voor de minimale systeemvereisten voor Linux. Zie */var/log/cisco/ampdaemon.log* en */var/log/cisco/ampscansvc.log* voor m informatie.
8	Realtime systeemmonitor is niet gestart	de kernel module die realtime controle van de bestandsactiviteit verschaft i geladen en het verbindingsbeleid heeft "Monitor File Copies and Moves" ingeschakeld. Deze bewakingsfuncties zijn niet beschikbaar in de connecto terwijl deze fout is verhoogd. Deze fout is groter wanneer de Secure Endpoi connector niet in staat is de onderliggende kernelmodule te laden die nodig voor de controle van de bestandsactiviteit. UEFI Secure Boot moet op het systeem zijn uitgeschakeld. Indien Secure Boot is uitgeschakeld, kan deze fout worden veroorzaakt doo onverenigbaarheid tussen de ampavt- of amfsm-kernelmodule die wordt gel met de Secure Endpoint-connector en de systeemkernel of andere derdeke modules die op het systeem zijn geïnstalleerd. Bekijk deze fout door*/var/log/berichten* voor meer informatie te bekijken of schakelt de bestandsbewaking in de beleidsinstellingen van de connector uit. Deze fout kan ook worden veroorzaakt bij het gebruik van een kernelversie niet door de connector wordt ondersteund. In dit geval kan deze worden gel door een aangepaste amfsm-kernelmodule te maken voor de huidige actiev systeemkern. (Van toepassing op de Linux-aansluitversies 1.16.0 en nieuwer) Zie voor meer informatie over het bouwen van aangepaste kernelmodules: Bouwen aan Cisco Secure Endpoint Linux-kabelmodules
9	Realtime netwerkmonitor is niet gestart	De kernelmodule die realtime netwerkactiviteitsbewaking biedt werd niet ge en het verbindingsbeleid heeft "ApparaatFlow Correlatie inschakelen" ingeschakeld. Deze bewakingsfunctie is niet beschikbaar in de connector te deze fout is verhoogd. Deze fout is groter wanneer de Secure Endpoint-connector niet in staat is de onderliggende kernelmodule te laden die nodig

		voor de controle van de bestandsactiviteit. UEFI Secure Boot moet op het systeem zijn uitgeschakeld. Indien Secure Boot is uitgeschakeld, kan deze fout worden veroorzaakt doo onverenigbaarheid tussen de ampavt- of amfsm-kernelmodule die wordt ge met de Secure Endpoint-connector en de systeemkernel of andere derdeke modules die op het systeem zijn geïnstalleerd. Bekijk deze fout door*/var/log/berichten* voor meer informatie te bekijken of schakelt de bestandsbewaking in de beleidsinstellingen van de connector uit. Deze fout kan ook worden veroorzaakt bij het gebruik van een kernelversie niet door de connector wordt ondersteund. In dit geval kan deze worden ge door een aangepaste amfsm-kernelmodule te maken voor de huidige actiev systeemkern. (Van toepassing op de Linux-aansluitversies 1.16.0 en nieuwer) Zie voor meer informatie over het bouwen van aangepaste kernelmodules: Bouwen aan Cisco Secure Endpoint Linux-kabelmodules Voor Red Hat gebaseerde distributies is het kerneldevelpakket vereist voor realtime bestands systeem en netwerkactiviteitsbewaking niet aanwezig en verbindingsbeleid heeft ofwel "Monitor File Copies and Moves" of "Enable Devices Flow Correling inschakelen" ingeschakeld. Deze fout wordt groter wanneer de Secure Endpoint connector niet in staat is de onderliggende eB module samen te stellen en te laden die nodig is voor monitoring van de bestandsactiviteit. Installeer het knel-vel-pakket voor het momenteel actieve kastdroge en star connector opnieuw, of blokkeer deze functies in het beleid om deze fout te verwijderen. (Alleen van toepassing op de Linux-opdrachtversies 1.13.0 en nieuwer.)
11	Vereiste pakket voor wielafstellen ontbreekt	Voor Oracle Linux UEK 6 en nieuwer is het kernel-stap pakket vereist voor functies. Installeer het pakket met de kern uitlijning voor het momenteel draaiende kanaal en start de connector opnieuw, of blokkeer deze functies i beleid om deze fout te verwijderen. (Alleen van toepassing op de Linux-opdrachtversies 1.18.0 en nieuwer.) Voor distributies op basis van Debian is het linux-headerpakket vereist voor functies. Installeer het linux-headerpakket voor de huidige draaiende kern e start de connector opnieuw, of blokkeer deze functies in het beleid om deze te verwijderen. (Van toepassing op Linux-connectors versies 1.15.0 en nieu Zie voor meer informatie: Linux Kernel-Devel Fault
16	Oncompatibele kern	Het momenteel draaiende kanaal is niet compatibel met de momenteel actie connector en het verbindingsbeleid heeft "Monitor File Copies and Moves" o "Enable Devices Flow Correling" ingeschakeld. De kern naar een ondersteunde versie downloaden of de connector verbete naar een nieuwere versie die deze kern ondersteunt. Zie voor meer informatie over ondersteunde kleinere versies: Cisco Secure Endpoint Linux-compatibiliteit