Dépannage des défaillances du connecteur Linux Secure Endpoint

Table des matières

[Introduction](#)
[Informations générales](#)
[Tableau des défaillances du connecteur Linux pour terminal sécurisé](#)

Introduction

Ce document décrit les erreurs que le connecteur Cisco Secure Endpoint Linux utilise pour vous avertir des conditions qui affectent son bon fonctionnement.

Informations générales

Le connecteur Cisco Secure Endpoint Linux envoie une notification avec un événement Fault Raised (Défaillance déclenchée) lorsqu'il détecte une condition qui affecte le bon fonctionnement du connecteur. De même, un événement Fault Cleared indique que la condition n'est plus présente.

Tableau des défaillances du connecteur Linux pour terminal sécurisé

Le tableau décrit les défaillances et les étapes de diagnostic associées.

ID de panne	Description	Dépannage/résolution
5	Utilisateur du service de numérisation non disponible	Le connecteur n'a pas pu créer d'utilisateur pour exécuter le processus d'analyse de fichier. Le connecteur utilise l'utilisateur racine pour effectuer des analyses de fichiers comme solution de contournement. Cela s'écarte de la conception prévue et n'est pas prévu. Si la `cisco-amp-scan-svc` l'utilisateur ou le groupe a été supprimé, ou la configuration de l'utilisateur et du groupe a été modifiée. Vous pouvez alors réinstaller le connecteur pour recréer l'utilisateur et le groupe avec les configurations nécessaires. Des détails supplémentaires sont disponibles dans

		/var/log/cisco/ampdaemon.log. Si la création du groupe d'utilisateurs est restreinte via les paramètres de /etc/login.defs, ce fichier doit être temporairement modifié pendant l'exécution du programme d'installation pour permettre la création de l'utilisateur et du groupe. Pour ce faire, changez usergroups_enab de no à yes. Cette erreur peut être déclenchée dans les connecteurs Linux 1.15.1 et versions ultérieures si un autre programme a modifié l'une des autorisations de répertoire du connecteur (c'est-à-dire /opt/cisco ou un répertoire enfant). Pour remédier à ce problème, l'autorisation de répertoire modifiée doit être rétablie sur la valeur par défaut (par exemple, 0755), assurez-vous qu'aucun programme futur ne modifie le répertoire /opt/cisco (ou tout répertoire enfant) et redémarrez le service de connecteur.
6	Redémarrage fréquent du service d'analyse	Le processus d'analyse des fichiers du connecteur a rencontré des échecs répétés et le connecteur a redémarré pour tenter d'effacer l'échec. Il est possible qu'un ou plusieurs fichiers du système provoquent le blocage de l'algorithme d'analyse lors de l'analyse. Le connecteur continue ses analyses au mieux de ses possibilités. Si ce défaut n'est pas automatiquement résolu dans les 10 minutes suivant le démarrage du connecteur, cela indique qu'une intervention supplémentaire de l'utilisateur est nécessaire et que la capacité du connecteur à effectuer des balayages est diminuée. Pour plus d'informations, consultez /var/log/cisco/ampdaemon.log et /var/log/cisco/ampscansvc.log.
7	Échec du démarrage du service d'analyse	Le processus d'analyse des fichiers du connecteur n'a pas pu démarrer et le connecteur a redémarré pour tenter de résoudre le problème. La fonctionnalité d'analyse des fichiers est désactivée lorsque cette erreur est déclenchée. Cet échec peut être déclenché si une erreur est rencontrée lors du chargement d'un fichier de définition de virus nouvellement installé (fichiers .cvd). Le connecteur effectue un certain nombre de contrôles d'intégrité et de stabilité avant d'activer de nouveaux fichiers .cvd pour empêcher cette défaillance. Au redémarrage, le connecteur supprime tous les fichiers .cvd non valides afin que le connecteur puisse reprendre. Si cette erreur n'est pas corrigée lors du redémarrage du connecteur, cela indique qu'une intervention supplémentaire de

		l'utilisateur est nécessaire. Si cette erreur se répète à chaque mise à jour .cvd, cela indique qu'un fichier .cvd non valide n'est pas correctement détecté par les contrôles d'intégrité du fichier .cvd du connecteur. Cette défaillance peut être déclenchée dans les connecteurs Linux si la mémoire disponible de l'ordinateur est insuffisante et que le service d'analyse ne peut pas démarrer. Consultez le « Guide de l'utilisateur de Secure Endpoint (anciennement AMP for Endpoints) » pour connaître la configuration système minimale requise sous Linux. Pour plus d'informations, consultez /var/log/cisco/ampdaemon.log et /var/log/cisco/ampscansvc.log.
8	Échec du démarrage du moniteur du système de fichiers en temps réel	Le module du noyau qui assure la surveillance en temps réel de l'activité du système de fichiers n'a pas été chargé et la stratégie de connecteur a activé « Surveiller les copies et les déplacements de fichiers ». Ces fonctions de surveillance ne sont pas disponibles dans le connecteur lorsque ce défaut est déclenché. Cette erreur est déclenchée lorsque le connecteur Secure Endpoint ne parvient pas à charger le module sous-jacent du noyau requis pour la surveillance de l'activité du système de fichiers. Le démarrage sécurisé UEFI doit être désactivé sur le système. Si le démarrage sécurisé est désactivé, cette erreur peut être causée par une incompatibilité entre le module noyau ampavflt ou ampfsm fourni avec le connecteur Secure Endpoint et le noyau du système ou d'autres modules de noyau tiers installés sur le système. Consultez /var/log/messages pour plus de détails ou désactivez la surveillance des fichiers dans les paramètres de stratégie de connecteur pour effacer cette erreur. La défaillance peut également être causée lors de l'exécution d'une version du noyau qui n'est pas prise en charge par le connecteur. Dans ce cas, il peut être effacé en construisant un module de noyau ampfsm personnalisé pour le noyau du système en cours d'exécution. (Applicable aux versions 1.16.0 et ultérieures du connecteur Linux.) Pour plus d'informations sur la construction de modules de noyau personnalisés, consultez : Construction de modules de noyau de connecteur Linux pour point d'extrémité sécurisé Cisco
9	Échec du démarrage du moniteur réseau	Le module du noyau qui assure la surveillance en temps réel de l'activité du réseau n'a pas été chargé et la stratégie de connecteur a

	en temps réel	activé l'option « Activer la corrélation de flux de périphérique ». Cette fonction de surveillance n'est pas disponible dans le connecteur lorsque cette erreur est déclenchée. Cette erreur est déclenchée lorsque le connecteur Secure Endpoint ne parvient pas à charger le module sous-jacent du noyau requis pour la surveillance de l'activité du système de fichiers. Le démarrage sécurisé UEFI doit être désactivé sur le système. Si le démarrage sécurisé est désactivé, cette erreur peut être causée par une incompatibilité entre le module noyau ampavflt ou ampfsm fourni avec le connecteur Secure Endpoint et le noyau du système ou d'autres modules de noyau tiers installés sur le système. Consultez /var/log/messages pour plus de détails ou désactivez la surveillance des fichiers dans les paramètres de stratégie de connecteur pour effacer cette erreur. La défaillance peut également être causée lors de l'exécution d'une version du noyau qui n'est pas prise en charge par le connecteur. Dans ce cas, il peut être effacé en construisant un module de noyau ampfsm personnalisé pour le noyau du système en cours d'exécution. (Applicable aux versions 1.16.0 et ultérieures du connecteur Linux.) Pour plus d'informations sur la construction de modules de noyau personnalisés, consultez : Construction de modules de noyau de connecteur Linux pour point d'extrémité sécurisé Cisco
11	Le package kernel-devel requis est manquant	Pour les distributions basées sur Red Hat, le package de développement du noyau requis pour la surveillance en temps réel du système de fichiers et de l'activité du réseau est manquant et la politique de connecteur a activé « Surveiller les copies et les déplacements de fichiers » ou « Activer la corrélation de flux de périphérique ». Cette erreur se produit lorsque le connecteur Secure Endpoint ne parvient pas à compiler et à charger le module eBPF sous-jacent requis pour la surveillance de l'activité du système de fichiers. Installez le paquet kernel-devel pour le noyau en cours d'exécution et redémarrez le connecteur, ou désactivez ces fonctionnalités dans la stratégie pour effacer cette erreur. (Applicable uniquement aux versions 1.13.0 et ultérieures du connecteur Linux.) Pour Oracle Linux UEK 6 et versions ultérieures, le package kernel-uek-devel est requis pour ces fonctions. Installez le paquet kernel-uek-devel pour le noyau en cours d'exécution et redémarrez le connecteur, ou désactivez ces fonctionnalités dans la stratégie pour

		effacer cette erreur. (Applicable uniquement aux versions 1.18.0 et ultérieures du connecteur Linux.) Pour les distributions basées sur Debian, le paquet linux-headers est requis pour ces fonctionnalités. Installez le paquet linux-headers pour le noyau en cours d'exécution et redémarrez le connecteur, ou désactivez ces fonctionnalités dans la stratégie pour effacer cette erreur. (Applicable aux versions 1.15.0 et ultérieures du connecteur Linux.) Pour plus d'informations, consultez : Défaillance du noyau Linux
16	Noyau incompatible	Le noyau en cours d'exécution n'est pas compatible avec le connecteur en cours d'exécution et la stratégie de connecteur a activé « Surveiller les copies et les déplacements de fichiers » ou « Activer la corrélation de flux de périphérique ». Rétrograder le noyau vers une version prise en charge ou mettre à niveau le connecteur vers une version plus récente prenant en charge ce noyau. Pour plus d'informations sur les versions du noyau prises en charge, voir : Compatibilité du système d'exploitation avec Cisco Secure Endpoint Linux Connector
18	La surveillance des événements du connecteur est surchargée	Cette erreur est déclenchée lorsque le connecteur est soumis à une charge importante en raison d'un nombre excessif d'événements système. La protection du système est limitée et le connecteur surveille un plus petit ensemble d'événements critiques du système jusqu'à ce que l'activité globale du système soit réduite. Cette erreur peut être une indication d'une activité malveillante du système ou d'applications très actives sur le système. Si une application active est bénigne et approuvée par l'utilisateur, elle peut être ajoutée à un jeu d'exclusions de processus pour réduire la charge de surveillance sur le connecteur. Cette action peut être suffisante pour effacer le défaut. Si aucun processus bénin ne provoque une charge importante, une enquête est nécessaire pour déterminer si l'activité accrue est due à un processus malveillant. Si le connecteur est sous de courtes périodes de charge lourde, alors il est possible que ce défaut peut se dissiper lui-même.

		Si cette erreur est fréquemment signalée, qu'aucun processus bénin n'entraîne une charge importante et qu'aucun processus malveillant n'a été détecté, le système doit être reconfiguré pour gérer les charges plus lourdes.
19	La stratégie SELinux est manquante ou désactivée	Cette erreur est déclenchée lorsque la politique Secure Enterprise Linux (SELinux) sur le système empêche le connecteur de surveiller l'activité du système. Si SELinux est activé et en mode d'application, le connecteur requiert cette règle dans la politique SELinux : `allow unrestricted_service_t self:bpf { map_create map_read map_write prog_load prog_run };` Sur les systèmes Red Hat, y compris RHEL 7 et Oracle Linux 7, cette règle n'est pas présente dans la politique SELinux par défaut. Au cours d'une installation ou d'une mise à niveau, le connecteur tente d'ajouter cette règle via l'installation d'un module de stratégie SELinux nommé `Cisco-Secure-BPF`. Si `Cisco-Secure-BPF` échoue lors de l'installation et du chargement, ou est désactivé, le problème est soulevé. Pour résoudre le problème, assurez-vous que le paquet system policy coreutils-python est installé. Réinstallez ou mettez à niveau le connecteur pour déclencher l'installation de `cisco-secure-bpf`, ou ajoutez manuellement la règle à la politique SELinux existante et redémarrez le connecteur. Pour plus d'instructions détaillées sur la modification de la politique SELinux pour résoudre cette erreur, consultez SELinux Policy Fault.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.