Solución de problemas de Secure Endpoint Linux Connector Faults

Contenido

[Introducción](#)
[Antecedentes](#)
[Tabla de fallas del conector de Secure Endpoint Linux](#)

Introducción

Este documento describe fallas que el conector de Cisco Secure Endpoint Linux utiliza para notificarle de condiciones que afectan su correcto funcionamiento.

Antecedentes

El conector de Cisco Secure Endpoint Linux notifica con un evento Fault Raised cuando detecta una condición que afecta el correcto funcionamiento del conector. De manera similar, un evento Fault Cleared comunica que la condición ya no está presente.

Tabla de fallas del conector de Secure Endpoint Linux

En la tabla se describen los fallos y los pasos de diagnóstico asociados.

ID de fallo	Descripción	Resolución/resolución de problemas
5	Usuario del servicio de digitalización no disponible	El conector no pudo crear un usuario para ejecutar el proceso de análisis de archivos. El conector utiliza el usuario raíz para realizar análisis de archivos como solución alternativa. Esto se desvía del diseño previsto y no se espera. Si `cisco-amp-scan-svc` se ha eliminado el usuario o el grupo, o se ha cambiado la configuración del usuario y el grupo, puede volver a instalar el conector para volver a crear el usuario y el grupo con las configuraciones necesarias. Encontrará más información en /var/log/cisco/ampdaemon.log. Si la creación del grupo de usuarios está restringida a través de la configuración de /etc/login.defs, este archivo debe cambiarse

		temporalmente mientras el instalador se está ejecutando para permitir que se creen el usuario y el grupo. Para ello, cambie userggroups_enab de no a yes. Este fallo puede producirse en los conectores Linux 1.15.1 y posteriores si otro programa ha modificado uno de los permisos de directorio del conector (es decir, /opt/cisco o un directorio secundario). Para aliviar esto, el permiso de directorio cambiado debe ser establecido de nuevo en el valor predeterminado (por ejemplo, 0755), asegúrese de que ningún programa futuro modifique el directorio /opt/cisco (o cualquier directorio secundario) y reinicie el servicio de conector.
6	El servicio de análisis se reinicia con frecuencia	El proceso de análisis de archivos de conector encontró errores repetidos y el conector se reinició en un intento de borrar el error. Es posible que uno o más archivos del sistema provoquen que el algoritmo de escaneo falle cuando se escanea. El conector continúa escaneando en el mejor de los casos. Si este fallo no se elimina automáticamente en los 10 minutos siguientes al inicio del conector, esto indica que se requiere una intervención adicional del usuario y que la capacidad del conector para realizar análisis se ha degradado. Consulte /var/log/cisco/ampdaemon.log y /var/log/cisco/ampscansvc.log para obtener más información.
7	Error al iniciar el servicio de análisis	El proceso de análisis de archivos del conector no se pudo iniciar y el conector se ha reiniciado en un intento de borrar el error. La funcionalidad de análisis de archivos está deshabilitada mientras se provoca este error. Este error puede desencadenarse si se produce un error al cargar los archivos de definición de virus recién instalados (archivos .cvd). El conector realiza una serie de comprobaciones de integridad y estabilidad antes de activar nuevos archivos .cvd para evitar este error. Al reiniciar, el conector quita los archivos .cvd no válidos para que el conector pueda reanudarse. Si este error no se borra cuando se reinicia el conector, esto es una indicación de que se requiere la intervención del usuario. Si este error se repite con cada actualización .cvd, esto indica que las comprobaciones de integridad del archivo .cvd del conector no detectan correctamente un archivo .cvd no válido. Este error se puede activar en los conectores de Linux si el equipo se

		está quedando sin memoria disponible y el servicio de escáner no puede iniciarse. Consulte la "Guía del usuario de Secure Endpoint (anteriormente AMP para terminales)" para conocer los requisitos mínimos del sistema en Linux. Consulte /var/log/cisco/ampdaemon.log y /var/log/cisco/ampscansvc.log para obtener más información.
8	Error al iniciar el monitor del sistema de archivos en tiempo real	El módulo del núcleo que proporciona monitoreo de actividad del sistema de archivos en tiempo real no se cargó y la política del conector tiene habilitada la opción "Monitorear copias y movimientos de archivos". Estas funciones de supervisión no están disponibles en el conector mientras se produce este fallo. Este fallo se genera cuando el conector Secure Endpoint no puede cargar el módulo del núcleo subyacente necesario para la supervisión de la actividad del sistema de archivos. El arranque seguro UEFI debe estar desactivado en el sistema. Si Secure Boot está inhabilitado, esta falla puede ser causada por una incompatibilidad entre el módulo de kernel ampavflt o ampfsm proporcionado con el conector Secure Endpoint y el kernel del sistema u otros módulos de kernel de terceros instalados en el sistema. Revise /var/log/messages para obtener detalles o inhabilite la supervisión de archivos en la configuración de directivas del conector para borrar este error. La falla también puede ser causada cuando se ejecuta una versión del núcleo que no es soportada por el conector. En este caso, se puede borrar construyendo un módulo de kernel ampfsm personalizado para el kernel del sistema actual en ejecución. (Aplicable a las versiones 1.16.0 y posteriores del conector Linux). Para obtener más información sobre cómo crear módulos de kernel personalizados, consulte: Building Cisco Secure Endpoint Linux Connector Kernel Modules
9	Error al iniciar el monitor de red en tiempo real	El módulo del kernel que proporciona monitoreo de actividad de red en tiempo real no se cargó y la política del conector tiene habilitada la opción "Habilitar correlación de flujo de dispositivos". Esta función de supervisión no está disponible en el conector mientras se produce este fallo. Este fallo se genera cuando el conector Secure Endpoint no puede cargar el módulo del núcleo subyacente necesario para la supervisión de la actividad del sistema de archivos. El arranque seguro UEFI debe estar desactivado en el sistema.

		Si Secure Boot está inhabilitado, esta falla puede ser causada por una incompatibilidad entre el módulo de kernel ampavflt o ampfsm proporcionado con el conector Secure Endpoint y el kernel del sistema u otros módulos de kernel de terceros instalados en el sistema. Revise /var/log/messages para obtener detalles o inhabilite la supervisión de archivos en la configuración de directivas del conector para borrar este error. La falla también puede ser causada cuando se ejecuta una versión del núcleo que no es soportada por el conector. En este caso, se puede borrar construyendo un módulo de kernel ampfsm personalizado para el kernel del sistema actual en ejecución. (Aplicable a las versiones 1.16.0 y posteriores del conector Linux). Para obtener más información sobre cómo crear módulos de kernel personalizados, consulte: Building Cisco Secure Endpoint Linux Connector Kernel Modules
11	Falta el paquete kernel-devel requerido	Para las distribuciones basadas en Red Hat, falta el paquete de desarrollo de kernel necesario para el sistema de archivos en tiempo real y la supervisión de la actividad de red, y la política del conector tiene habilitada la opción "Supervisar copias y movimientos de archivos" o "Habilitar correlación de flujo de dispositivos". Este fallo se genera cuando el conector Secure Endpoint no puede compilar y cargar el módulo eBPF subyacente necesario para la supervisión de la actividad del sistema de archivos. Instale el paquete kernel-devel para el núcleo que se está ejecutando actualmente y reinicie el conector, o inhabilite estas funciones en la política para borrar este fallo. (Aplicable únicamente a las versiones 1.13.0 y posteriores del conector Linux). Para Oracle Linux UEK 6 y versiones posteriores, se requiere el paquete kernel-uek-devel para estas funciones. Instale el paquete kernel-uek-devel para el núcleo que se está ejecutando actualmente y reinicie el conector, o inhabilite estas funciones en la política para borrar esta falla. (Aplicable únicamente a las versiones 1.18.0 y posteriores del conector Linux). Para las distribuciones basadas en Debian, se requiere el paquete linux-header para estas funciones. Instale el paquete linux-encabezados para el núcleo que se está ejecutando actualmente y reinicie el conector, o inhabilite estas funciones en la política para borrar este fallo. (Aplicable a las versiones 1.15.0 y posteriores del conector Linux).

		Para obtener más información, visite: Falla de Linux Kernel-Devel
16	kernel incompatible	El núcleo que se está ejecutando actualmente no es compatible con el conector que se está ejecutando actualmente y la política del conector tiene habilitada la opción "Supervisar copias y movimientos de archivos" o "Habilitar correlación de flujo de dispositivos". Reduzca el núcleo a una versión compatible o actualice el conector a una versión más reciente que admita este núcleo. Para obtener más información sobre las versiones compatibles del núcleo, consulte: Compatibilidad de SO del conector de Cisco Secure Endpoint Linux
18	La supervisión de eventos del conector está sobrecargada	Este fallo se produce cuando el conector está sometido a una carga pesada debido a un número abrumador de eventos del sistema. La protección del sistema es limitada y el conector supervisa un conjunto menor de eventos críticos del sistema hasta que se reduce la actividad general del sistema. Este fallo podría ser un indicio de actividad maliciosa del sistema o de aplicaciones muy activas en el sistema. Si una aplicación activa es benigna y de confianza para el usuario, se puede agregar a un conjunto de exclusión de procesos para reducir la carga de supervisión en el conector. Esta acción puede ser suficiente para despejar la falla. Si ningún proceso benigno causa una carga pesada, se requiere alguna investigación para determinar si el aumento de la actividad se debe a un proceso malicioso. Si el conector se encuentra bajo períodos cortos de carga pesada, es posible que este fallo se pueda resolver por sí mismo. Si este fallo se produce con frecuencia, no hay procesos benignos que causen una carga pesada y no se han detectado procesos maliciosos, es necesario volver a aprovisionar el sistema para gestionar cargas más pesadas.
19	Falta la política SELinux o está inhabilitada	Este fallo se produce cuando la política de Secure Enterprise Linux (SELinux) del sistema impide que el conector supervise la actividad del sistema. Si SELinux está habilitado y en el modo de aplicación, el Conector requiere esta regla en la Política de SELinux: `allow unconfined_service_t self:bpf { map_create map_read map_write`

		`prog_load prog_run };` En los sistemas basados en Red Hat, incluyendo RHEL 7 y Oracle Linux 7, esta regla no está presente en la política de SELinux predeterminada. Durante una instalación o actualización, el conector intenta agregar esta regla a través de la instalación de un módulo de políticas de SELinux llamado `Cisco-Secure-BPF`. Si `Cisco-Secure-BPF` no se puede instalar y cargar, o está deshabilitado, se genera el error. Para resolver el error, asegúrese de que el paquete del sistema policcoreutils-python esté instalado. Reinstale o actualice el conector para activar la instalación de `cisco-secure-bpf`, o agregue manualmente la regla a la política de SELinux existente y reinicie el conector. Para obtener instrucciones más detalladas sobre la modificación de la Política de SELinux para resolver este fallo, vea Falla de la Política de SELinux.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).