Fallos del conector Mac de Cisco Secure Endpoint

Contenido

Introducción

El conector puede notificarle de un evento de llenado de fallas cuando detecta una condición que afecta al correcto funcionamiento del conector. De manera similar, un evento Fault Cleared comunica que la condición ya no está presente.

Tabla de fallas del conector

En la tabla siguiente se describen los errores y los pasos de diagnóstico correspondientes.

ID de falla	Texto del portal	Terminal Descripción	Resolución/resolución de problemas
1	Módulo de núcleo no autorizado	Extensión del sistema no autorizada	Se ha bloqueado la ejecución de la extensión del sistema del conector. Abra Security and Privacy System Preferences y apruebe la extensión. Alternativamente, las extensiones del sistema se pueden aprobar de forma re mediante un perfil de gestión de dispositivos móviles (MDM).
2	Discordancia de la versión	Discordancia de la versión de extensión del sistema	El software de conector instalado está dañado. Vuelva a instalar el conector. Nota: Al ejecutar las versiones 1.14.0 y posteriores del conector Mac, es posib que se borren algunas ocurrencias de este error reiniciando el ordenador.
3	Acceso al disco no concedido	Acceso completo al disco no concedido	El conector no puede tener acceso a los archivos de usuario para la exploraci Abra Security and Privacy System Preferences y conceda acceso completo al al servicio AMP. Para las versiones de Mac Connector anteriores a 1.14.0, este proceso se denomina */opt/cisco/amp/ampdaemon*. Para Mac Connector versiones 1.14.0 y posteriores, las dos aplicaciones sigui requieren acceso completo al disco en función de la versión de macOS: • *AMP para terminales Servicio* (necesario para todas las versiones de mac • *Extensión de seguridad AMP* (se necesita en macOS 10.15.5 y posterior) Para las versiones 1.14.1 y posteriores del conector Mac, las dos aplicaciones siguientes requieren acceso completo al disco en función de la versión de mac • *AMP para terminales Servicio* (necesario para todas las versiones de mac • *Extensión de seguridad AMP* (se necesita en macOS 11 y posterior) En esta nota técnica encontrará detalles adicionales.
4	Módulo de	No se pudo cargar la	Para las versiones del conector Mac anteriores a 1.14.0 o cuando se ejecuta e macOS 10.14 o 10.15, este error indica que la extensión del sistema del cone

	núcleo no cargado	extensión del sistema; reinstalación del conector	es la versión correcta y se ha aprobado para su ejecución, pero aún no se ha podido cargar. Revise */Library/Logs/Cisco/ampdaemon.log* para obtener más detalles. La desinstalación y reinstalación del conector también puede solucion este error.
5	El usuario del servicio de análisis no está disponible	El usuario del servicio de análisis no está disponible	El conector no pudo crear un usuario para ejecutar el proceso de escaneo de archivos. El conector funciona en torno a esto utilizando el usuario raíz para re el escaneo de archivos. Esto se aparta del diseño previsto y no se espera. Si `cisco-amp-scan-svc` se ha eliminado el usuario o el grupo o se ha cambiado l configuración del usuario y del grupo, al volver a instalar el conector se volverá crear el usuario y el grupo con la configuración necesaria. Los detalles adicion están disponibles en */Library/Logs/Cisco/ampdaemon.log*.
6	Reiniciar el servicio con frecuencia	Reiniciar el servicio con frecuencia	El proceso de escaneo de archivos del conector encontró fallas repetidas y el conector se ha reiniciado en un intento de borrar la falla. Es posible que uno o archivos del sistema provoquen que el algoritmo de escaneo se desmorone cu se analiza. El conector continúa con las exploraciones con el mejor esfuerzo. Si este fallo no se borra automáticamente en los 10 minutos siguientes al inici conector, esto indica que se requiere una mayor intervención del usuario y se degradará la capacidad del conector para realizar exploraciones. Revisión */Library/Logs/Cisco/ampdaemon.log* y */Library/Logs/Cisco/ampscans* para obtener detalles.
7	Error al iniciar el servicio de análisis	Error al iniciar el servicio de análisis	No se pudo iniciar el proceso de escaneo de archivos del conector y éste se h reiniciado en un intento de borrar la falla. La funcionalidad de escaneo de arch se inhabilita mientras se provoca este error. Esta falla se puede activar si se produce un error al cargar un archivo de defin de virus recientemente instalado (archivos .cvd). El conector realiza una serie comprobaciones de integridad y estabilidad antes de activar nuevos archivos para evitar este error. Al reiniciar el conector, se quitarán los archivos .cvd no válidos para que el conector pueda reanudarse. Si no se borra este error cuando se reinicia el conector, esto indica que se req una intervención adicional del usuario. Si esta falla se repite con cada actualiz .cvd, esto indica que las comprobaciones de integridad del archivo .cvd del conector no detectan correctamente un archivo .cvd no válido. Revisión */Library/Logs/Cisco/ampdaemon.log* y */Library/Logs/Cisco/ampscans* para obtener detalles.
10	Reinicio necesario para cargar el módulo	Reinicio necesario para cargar las extensiones del sistema	Reinicie el sistema. Para las versiones 1.11.1 y 1.14.0 del conector Mac, este error se puede prov si las extensiones del sistema no pueden cargarse. En este caso, este error se puede borrar reinstalando el conector. Tenga en cuenta que Mac Connector 1.14.1 y posteriores pueden provocar es error si hay demasiadas extensiones del sistema de filtro de contenido de red instaladas en el sistema. Consulte la guía de fallos 13 a continuación para obt más detalles si el reinicio del ordenador no elimina este error.

	kernel o la extensión del sistema		
12	Filtro de red no permitido	Filtro de red no permitido	La función "Habilitar correlación de flujo de dispositivos" de la política requiere filtro de red. Para eliminar este error, permita que "AMP para terminales Servi filtre el contenido de la red en el terminal. Se puede acceder al cuadro de diálogo macOS para permitir el filtro de red haciendo clic en el error activo que se muestra en el menú Agente y siguiendo instrucciones proporcionadas. Los detalles adicionales, incluidos los parámetros de perfil MDM para la autorización remota de filtros de red, están disponibles en esta nota técnica.
13	Demasiadas extensiones del sistema de filtrado de contenido de red	Demasiadas extensiones del sistema de filtrado de contenido de red	Para Mac Connector 1.14.0, este error se provoca frecuentemente debido a u error de macOS al iniciar la extensión del sistema de filtrado de contenido de r Al reiniciar el ordenador, se borrará este error. La función "Habilitar correlación de flujo de dispositivos" de la política requiere uso de un filtro de contenido de red macOS de grado de firewall. MacOS limita número de filtros de contenido de red que se pueden ejecutar. Si se produce este error y no se borra reiniciando el equipo, desinstale los filtr contenido de red de grado firewall que ya no sean necesarios y reinicie el con
14	Demasiadas extensiones del sistema de seguridad de terminales	Demasiadas extensiones del sistema de seguridad de terminales	MacOS limita el número de extensiones del sistema de seguridad de terminale que se pueden ejecutar. El conector Mac requiere una de estas extensiones d sistema de seguridad de terminales para las funciones 'Monitor File Copies an Moves' y 'Monitor Process Execution' de la política . Para eliminar este error, desinstale las extensiones del sistema de seguridad d terminal que ya no sean necesarias y reinicie el conector.
15	La extensión del sistema requiere acceso completo al disco	La extensión del sistema requiere acceso completo al disco	Las Extensiones del sistema macOS del conector Mac no pueden acceder a lo archivos de usuario para la exploración. Abra Security & Privacy System Preferences y conceda acceso completo al disco a la *AMP Security Extension* En esta nota técnica se incluyen detalles adicionales, como la configuración d perfil MDM para la autorización remota de acceso completo al disco con extensiones del sistema. Tenga en cuenta que un error en macOS 11.0.0 puede hacer que la configura completa de acceso al disco se borre espontáneamente en un reinicio después que se haya concedido. Este bug ha sido corregido en macOS 11.0.1.
17	No se ha concedido acceso al	No se ha concedido acceso al	Orbital requiere acceso completo al disco para acceder a los archivos y directo protegidos para las consultas. Abra Security & Privacy System Preferences y conceda acceso completo al disco a *Cisco Orbital*.

ido
acceso
al disco
disco completo
comple orbital
to
orbital