Recuperar archivos en cuarentena por un terminal seguro

Contenido

Introducción

Este documento describe cómo restaurar archivos que fueron puestos en cuarentena por el conector de Secure Endpoint desde la consola de Secure Endpoint.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- consola de Cisco Secure Endpoint

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Secure Endpoint Console v5.4.2025030619

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

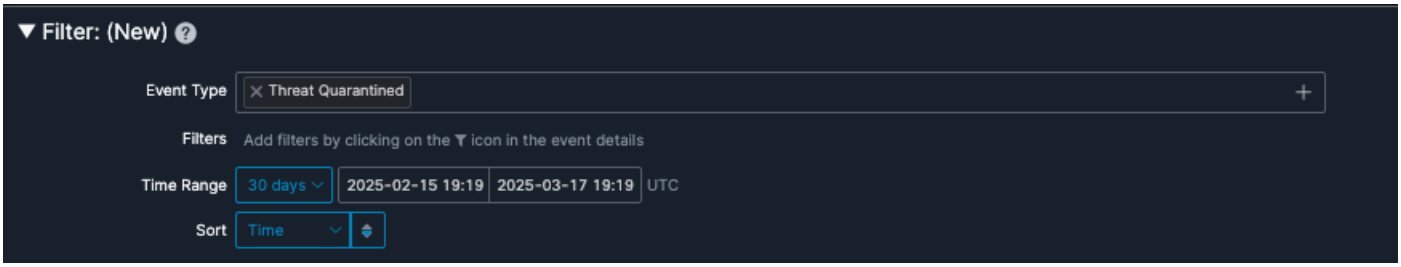
Problema

Los archivos puestos en cuarentena por el conector de Secure Endpoint (SE) se pueden recuperar para el análisis de archivos, el envío de falsos positivos o la restauración cuando se sabe que el archivo es seguro. Los administradores pueden realizar esta acción directamente desde Secure Endpoint Console.

Solución

1. Acceda a la página Eventos de la consola de SE.

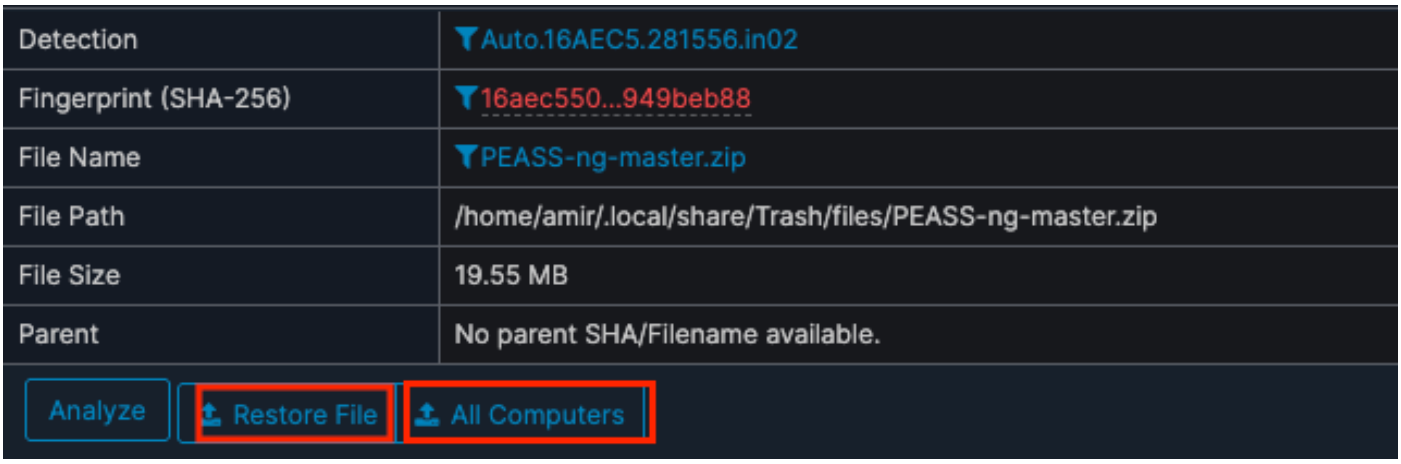
2. Filtre los eventos para mostrar todas las cuarentenas correctas seleccionando el filtro Tipo de evento = Amenaza en cuarentena.



Tipo de evento de amenaza en cuarentena

3. Identifique el evento de detección asociado al archivo que necesita restaurar.

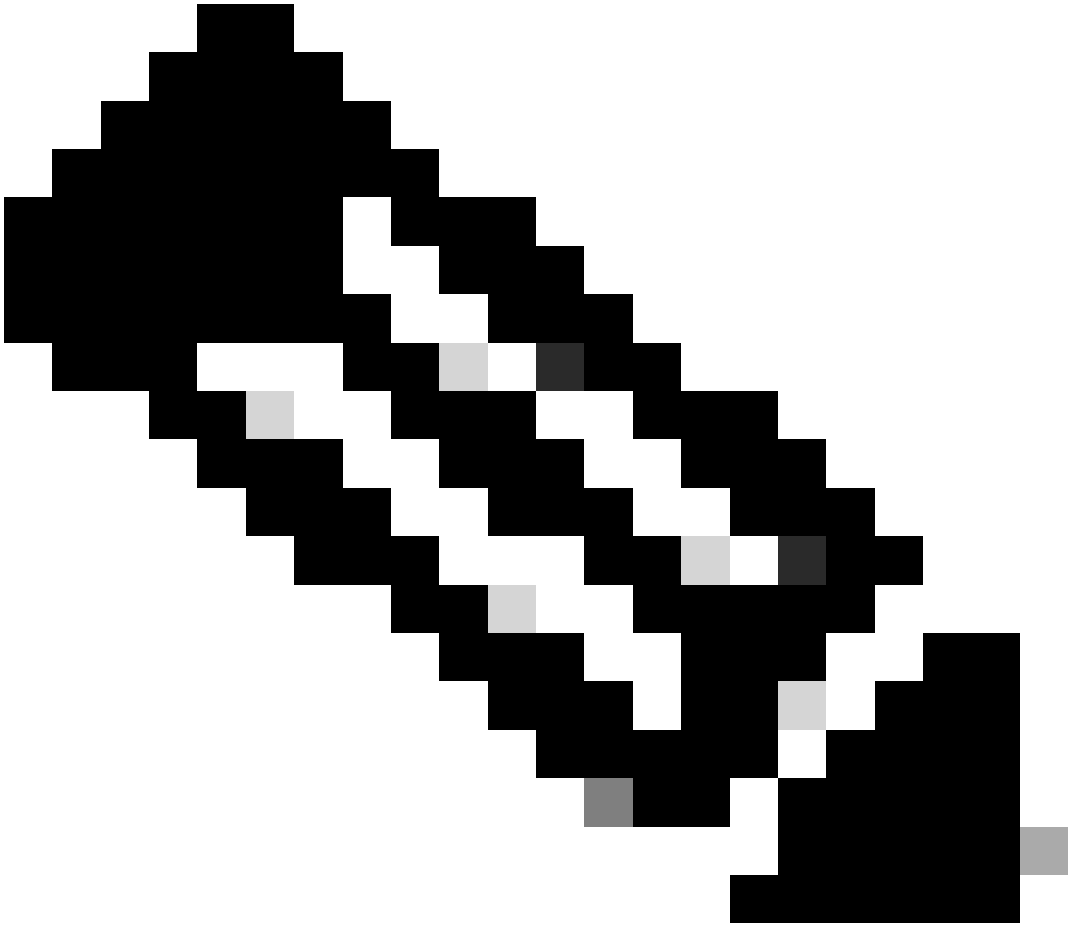
4. Expanda los detalles del evento para acceder a la opción Restaurar archivo. Al seleccionar Restaurar archivo se restaura el archivo en el equipo afectado. Al seleccionar Todos los equipos, se restaura el archivo en todos los equipos en los que se puso en cuarentena.



Restaurar opciones de archivo

5. El intervalo de latidos es la frecuencia con la que el conector llama a casa para comprobar si el administrador puede restaurar algún archivo. Los archivos se restauran una vez que los equipos afectados están en línea o se produce el siguiente intervalo de latidos.

6. Si el archivo es de confianza, agréguelo a una Lista de permitidos para evitar que se ponga en cuarentena de nuevo.



Nota: Los archivos permanecen en cuarentena durante 30 días o cuando la carpeta de cuarentena alcanza los 100 MB y se depuran los archivos más antiguos. Los archivos en cuarentena ya no se pueden restaurar después de su depuración.

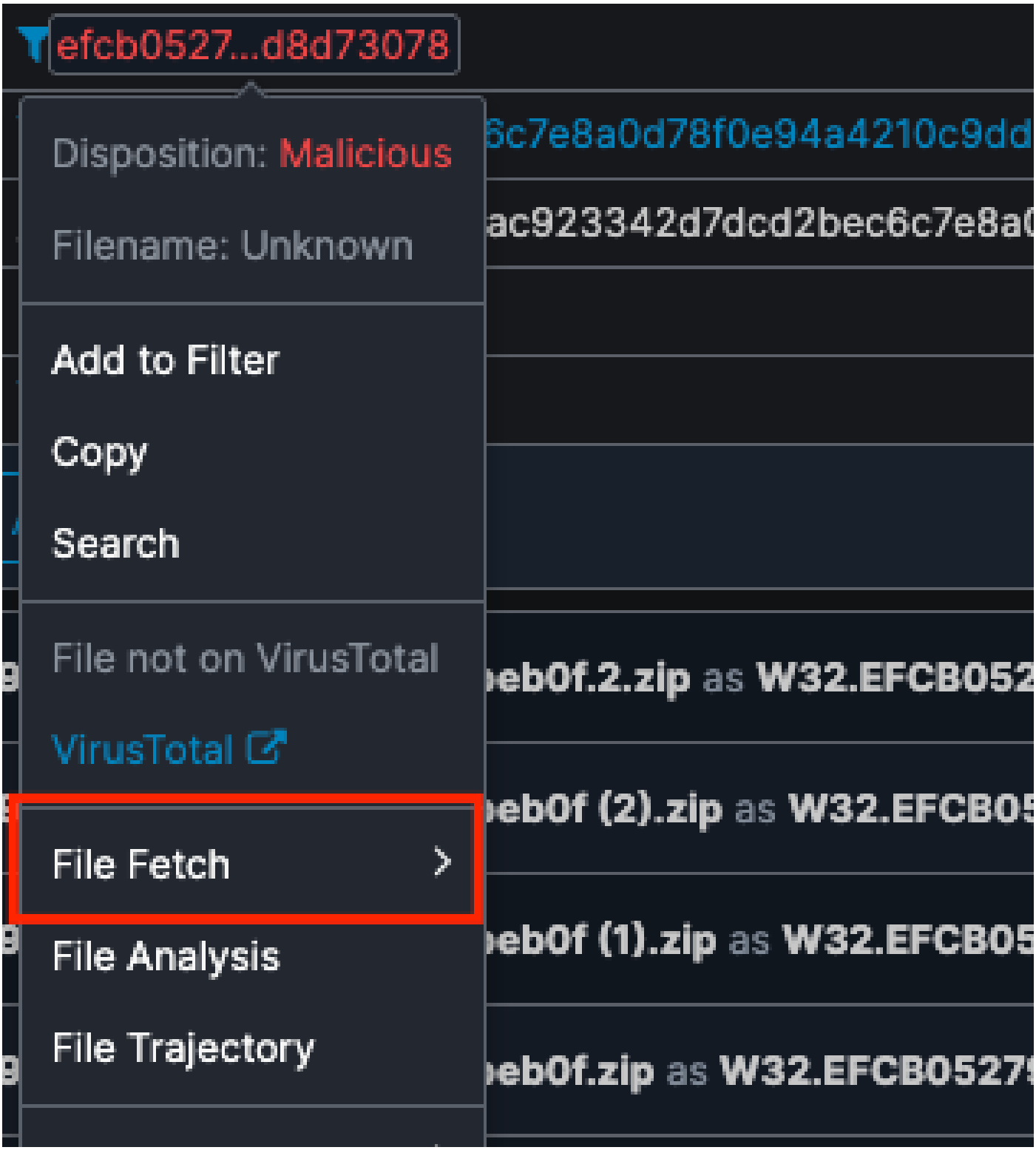
Si necesita simplemente descargar un archivo en cuarentena para el análisis de amenazas o envíos de falsos positivos sin restaurarlo a su entorno, puede utilizar la función File Fetch.

1. Acceda a la página Eventos de la consola de SE.

2. Filtre los eventos para mostrar todas las cuarentenas correctas seleccionando el filtro Tipo de evento = Amenaza en cuarentena.

3. Identifique el evento de detección asociado al archivo que necesita descargar.

4. Haga clic en el valor SHA-256 del archivo en cuarentena para mostrar la opción File Fetch.



Captura de archivos

Esto proporciona el estado de la búsqueda de archivos, la opción para iniciar la búsqueda y el acceso para ver el archivo en el Repositorio de archivos.

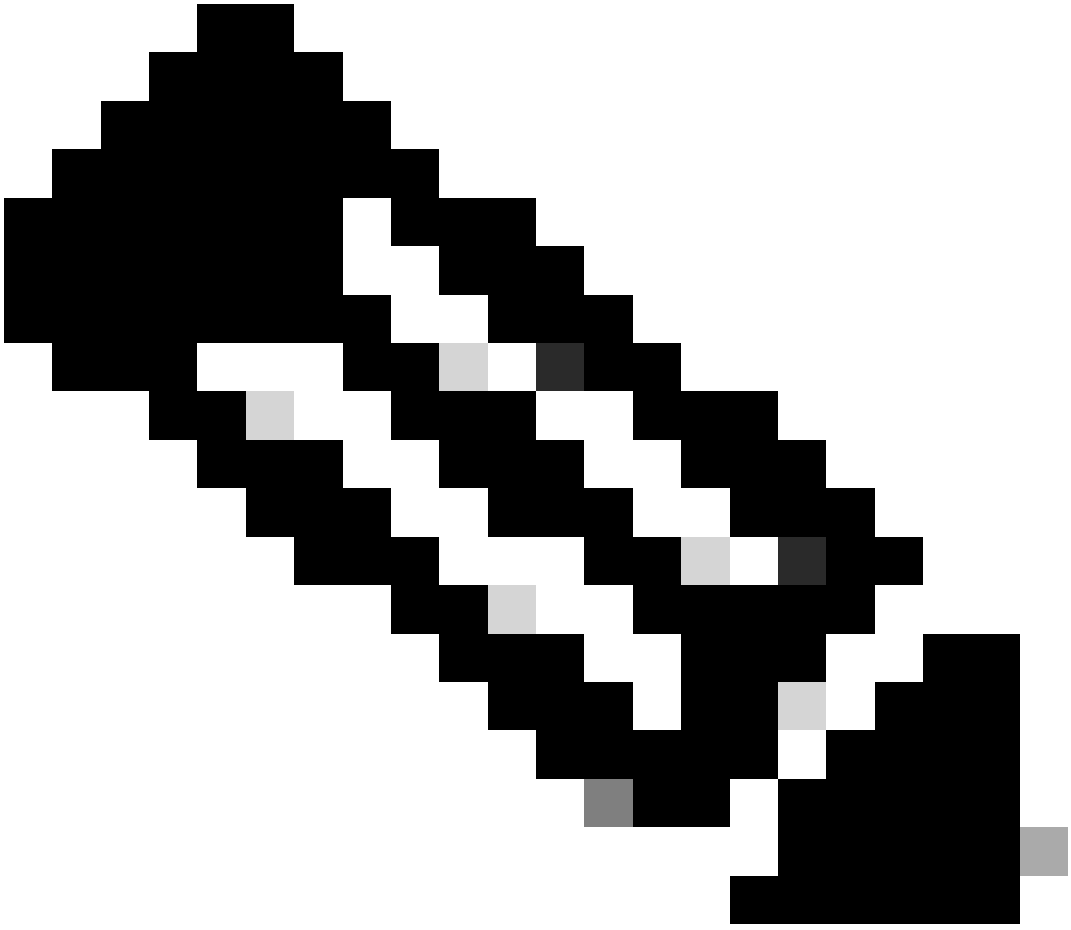
5. Pulse Recuperar Fichero, seleccione el Ordenador desde el que desea recuperar el fichero y confirme pulsando Recuperar.

6. Una vez cargado el archivo en el repositorio de archivos, se envía una notificación por correo electrónico.

7. Una vez que el archivo está disponible, puede ver el archivo y la opción para descargarlo en Analysis> File Repository.

Descargar archivo

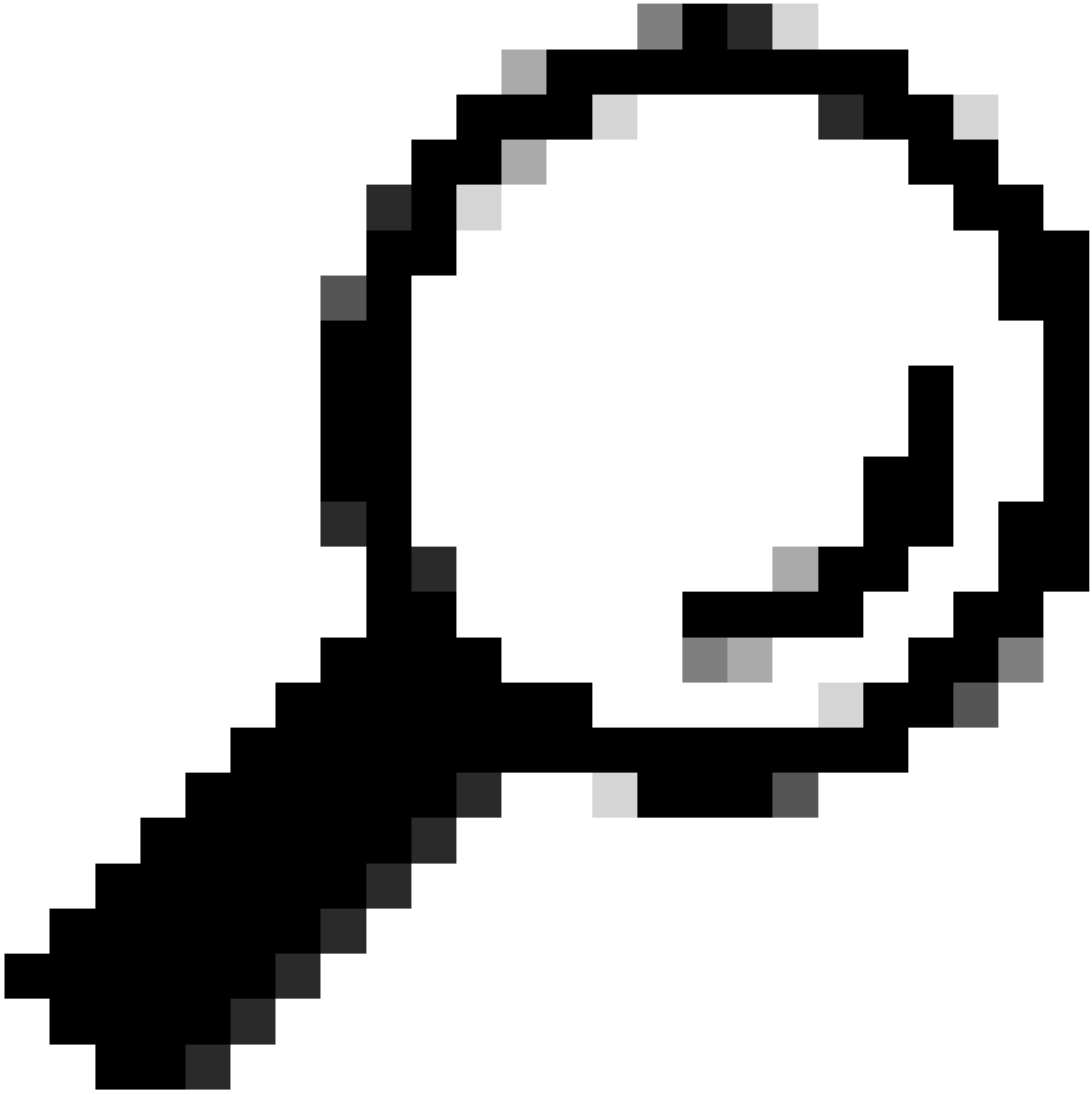
Todos los archivos descargados desde el Repositorio de archivos se comprimen y se protegen con contraseña.



Nota: Para que la recuperación de archivos funcione correctamente, se debe permitir el tráfico de red al servidor de recuperación de archivos adecuado en función de la región de la nube: Europa: rff.eu.amp.cisco.com Norteamérica: rff.amp.cisco.com Asia Pacífico, Japón y China: rff.apjc.amp.cisco.com. Además, asegúrese de que la Autenticación de dos factores (2FA) esté habilitada para la cuenta Administrador, ya que es necesaria para

---

iniciar correctamente una solicitud de recuperación de archivos.



Consejo: Puede filtrar eventos utilizando Event Type = Quarantined Restore Failed y Event Type = File Fetch Failed para identificar fallas y revisar las razones correspondientes para las operaciones Restore y File Fetch respectivamente.

Si no puede restaurar el archivo con los pasos descritos, póngase en contacto con el TAC de Cisco y proporcione el archivo .qrt ubicado en el directorio C:\Program Files\Cisco\AMP\Quarantine.

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).