Recopilar Crashdumps de procesos en Windows para procesos Sfc

Contenido

Introducción

Este documento describe cómo recopilar crashdumps de proceso en Windows para el proceso sfc.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conector de terminal seguro de Cisco
- Ventanas del símbolo del sistema

Componentes utilizados

Este documento no se limita a las versiones de software y hardware. 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.

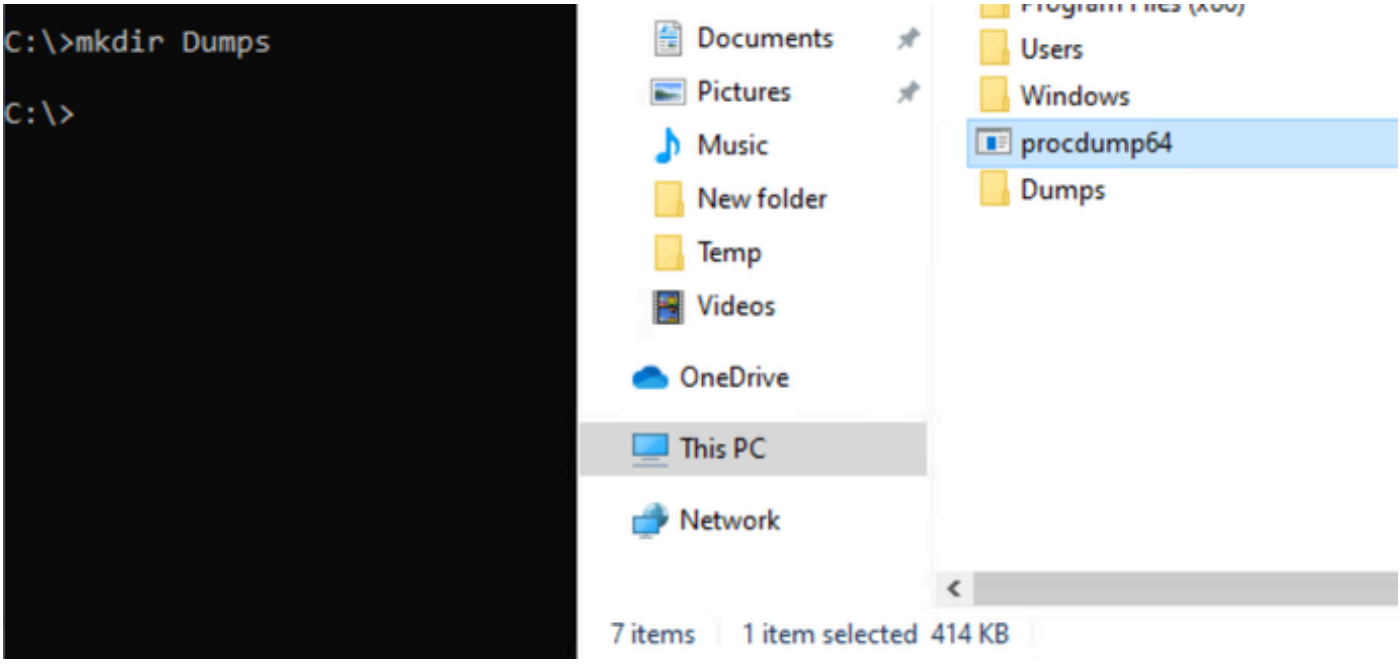
Problema

- La aplicación de punto final de Cisco Secure puede pasar a un estado deshabilitado o desconectado debido a la caída del proceso de sfc.exe, que podría estar relacionada con el cierre inesperado de Windows o cualquier otra actividad en Windows.
- Windows activa una herramienta de depuración configurada en los valores del Registro de AeDebug. Cualquier programa puede ser seleccionado de antemano como la herramienta a utilizar en esta situación. El programa elegido se conoce como el depurador postmortem.

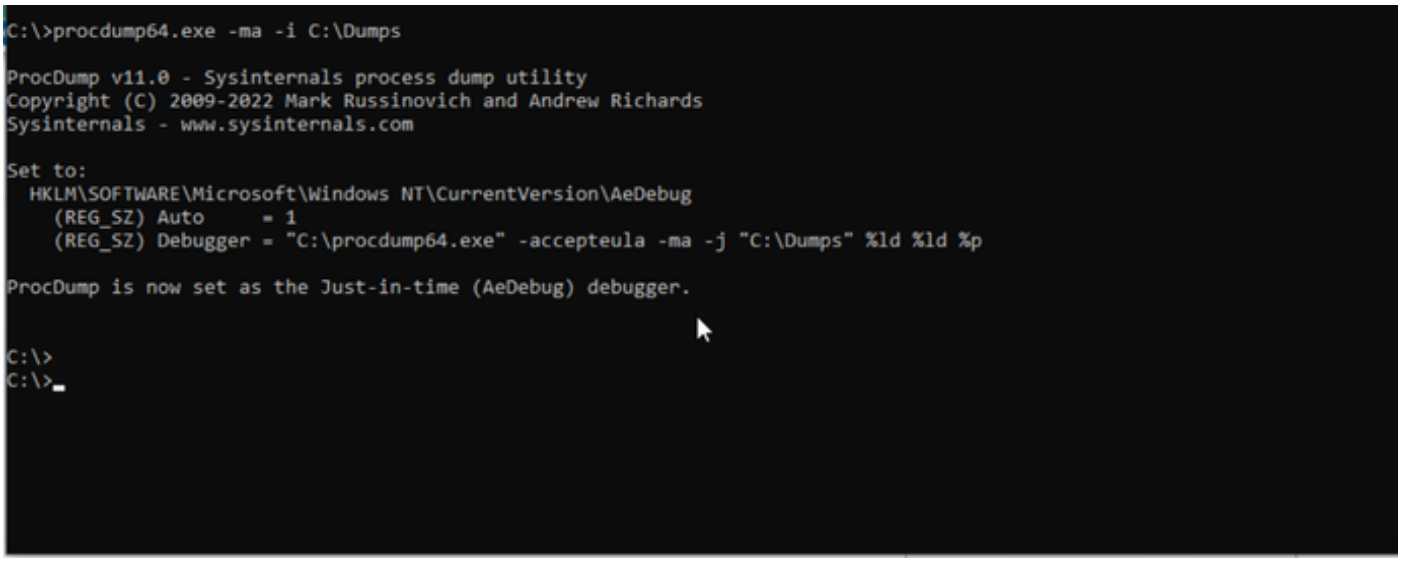
Solución

Descargue [Procdump como el depurador postmortem (AeDebug)] de sysinternals suite.

Extraiga Procdump en la unidad c y cree la carpeta Dumps para la colección crashdump como se muestra:



Establezca Procdump como AeDebugger:



Cómo usarla:

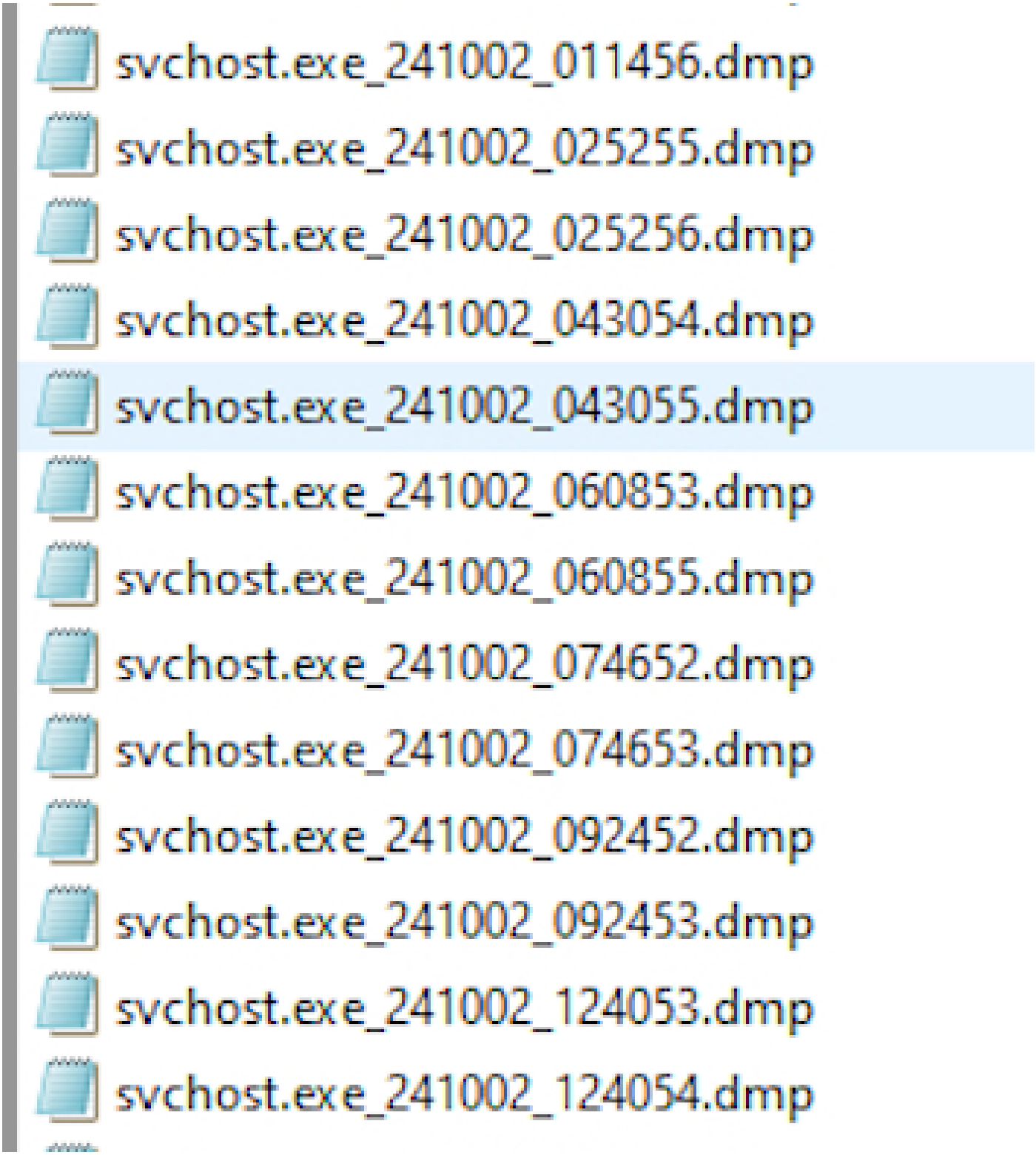
- Inicie CMD como administrador.
- Cambie al directorio donde desempaquetó procdump tool.

- Ejemplo de comando: procdump64.exe -ma <PID | Process Name> o procdump64.exe -ma -i C:\Dumps

Ejemplo de sfc.exe:

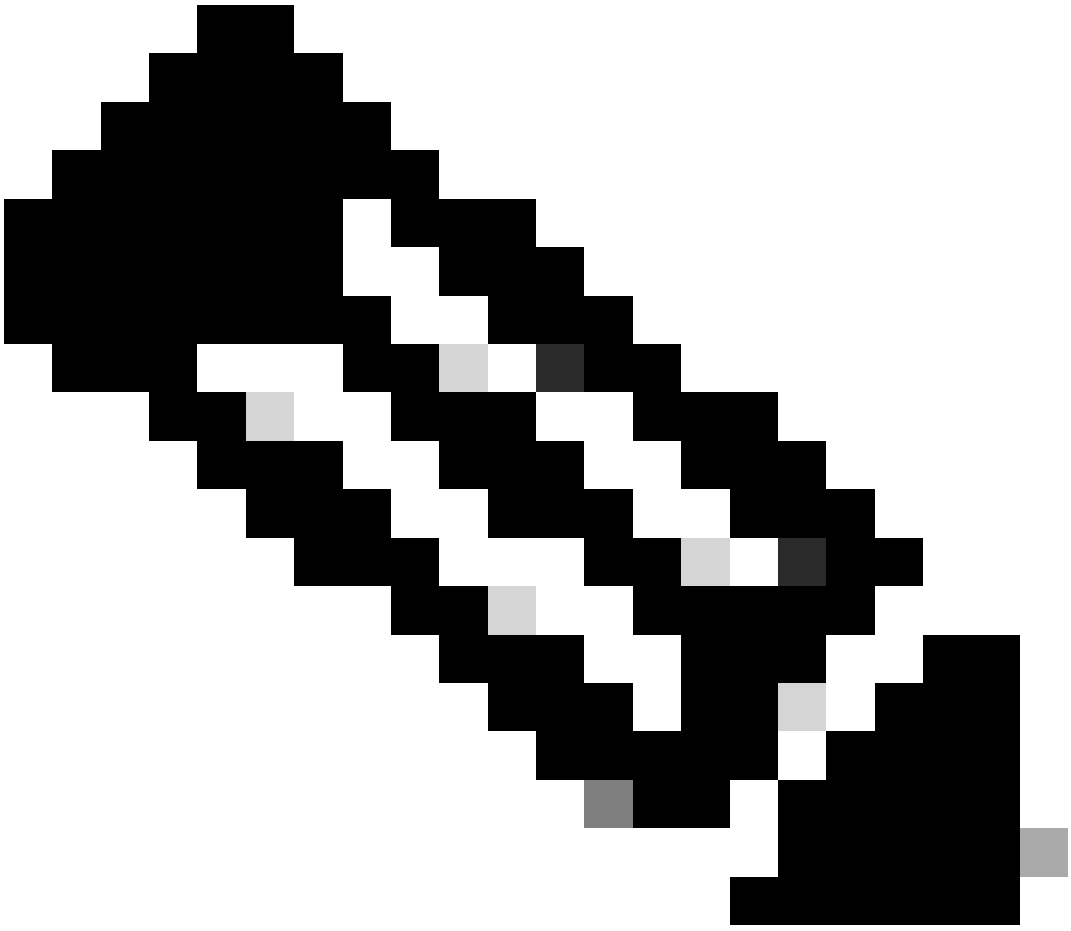
procdump64.exe -accept-ma -e -x c:\install %ProgramFiles%\Cisco\AMP\8.2.3.30119\sfc.exe

Guarda los crashdumps en la carpeta Dumps como se muestra. Recopile y comparta la información para su análisis:



Para desinstalar procdump, utilice: procdump64.exe -u

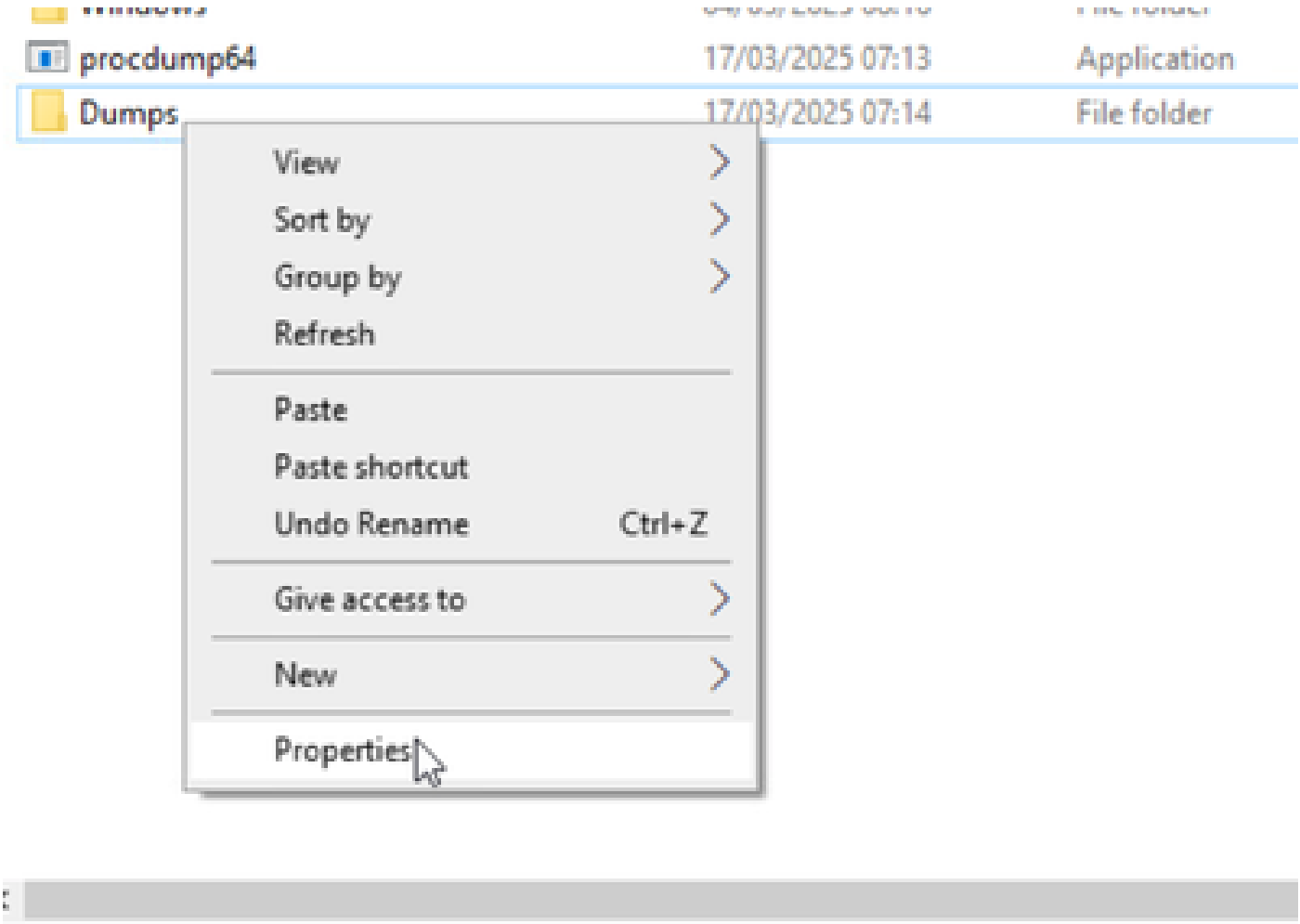
```
C:\>
C:\>procdump64.exe -u

ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

Reset to:
  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug
    (REG_SZ) Auto     = <deleted>
    (REG_SZ) Debugger = <deleted>

ProcDump is no longer the Just-in-time (AeDebug) debugger.


C:\>_
```

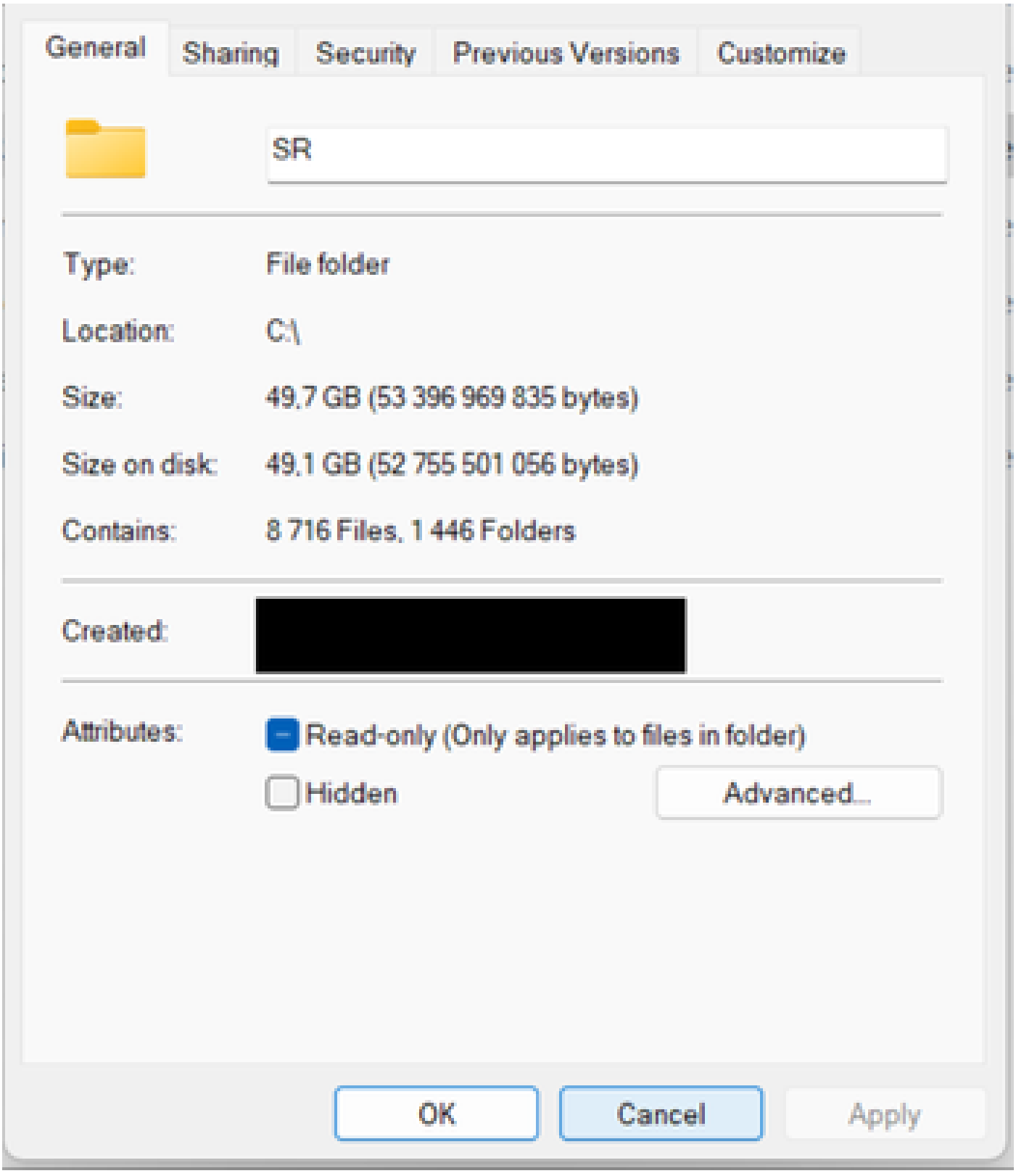


Nota: Los volcados de memoria pueden consumir gran espacio en el disco y procdump puede detenerse una vez que se realiza la recolección.

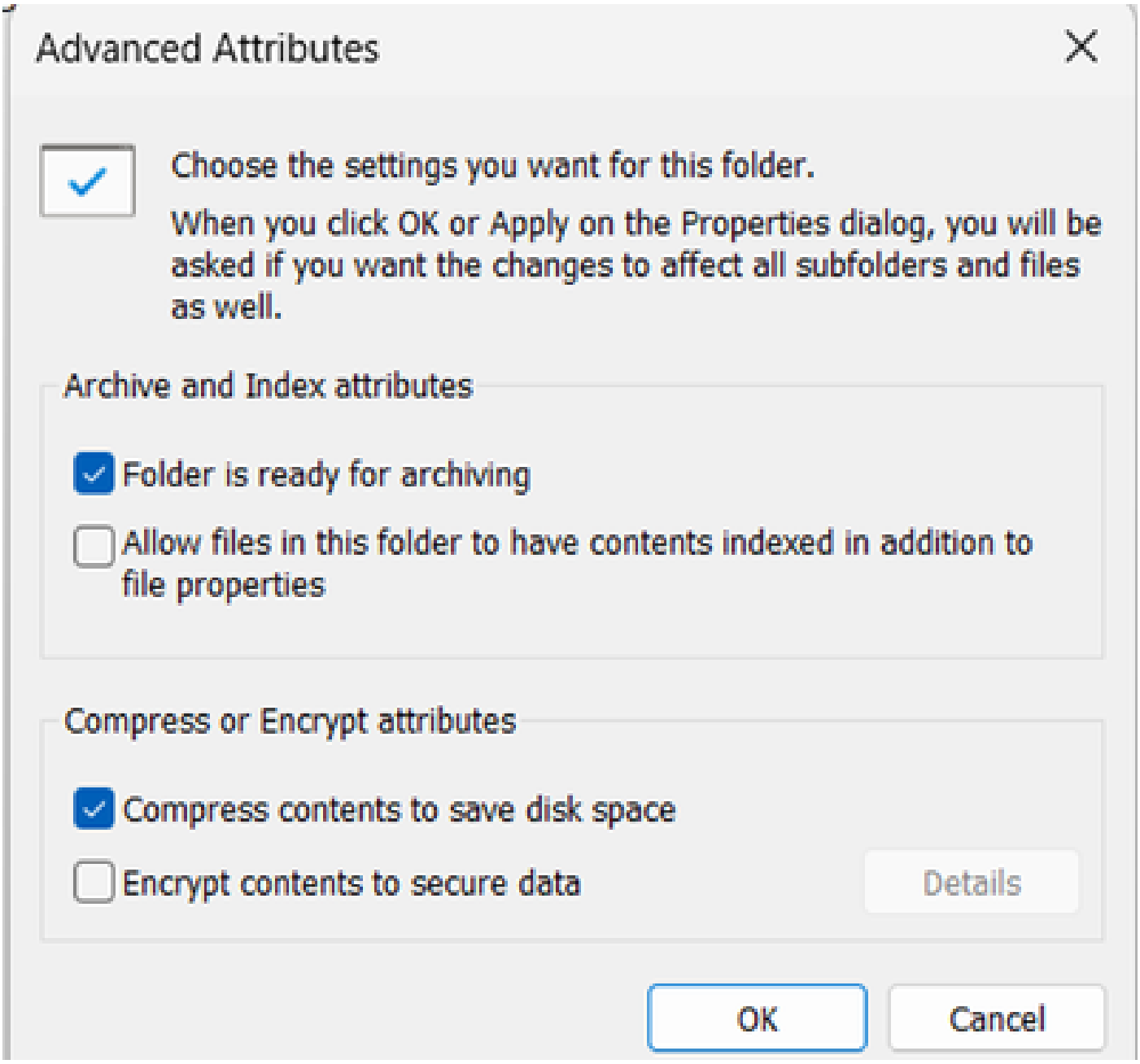
Aunque también puede utilizar la solución alternativa para comprimir el tamaño de la carpeta:

1- Navegue hasta propiedades de la carpeta Dumps y verifique el tamaño original de la carpeta en el disco como se muestra:

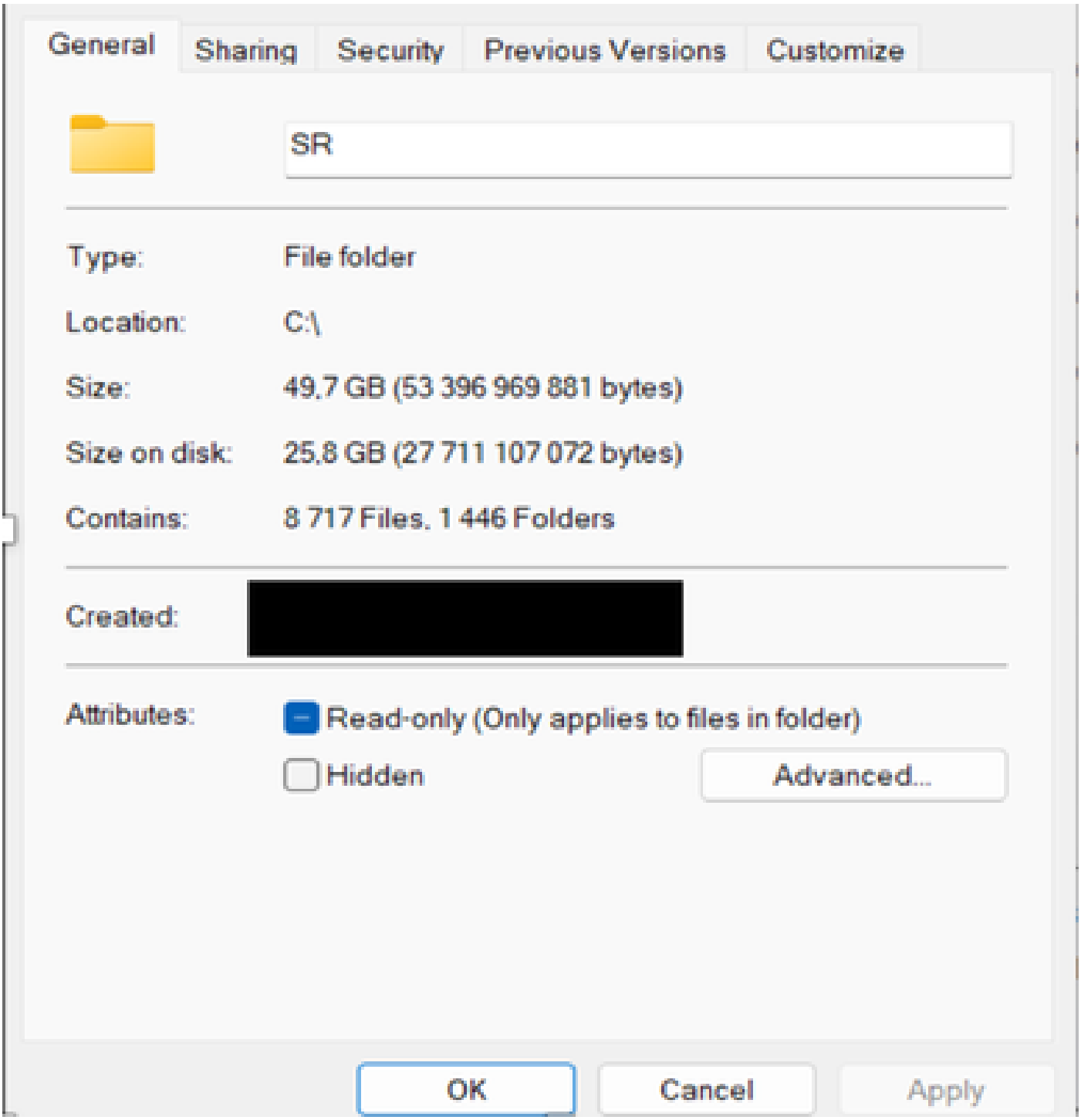




2- Navegue hasta la opción Advanced y habilite la compresión y aplique la que toma varios minutos:



3- Al final, puede ver que el tamaño de la carpeta se reduce a casi la mitad del tamaño original como se muestra:



4- También puede utilizar este comando en el símbolo del sistema para lograr lo mismo:

compact /c /s:c:\install

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).