Sammeln von Prozess-Absturzsicherungen auf Windows für SFC-Prozess

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Process Crashdumps unter Windows für den SFC-Prozess gesammelt werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Endpoint Connector
- Eingabeaufforderungsfenster

Verwendete Komponenten

Dieses Dokument ist nicht auf Software- und Hardwareversionen beschränkt. Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Problem

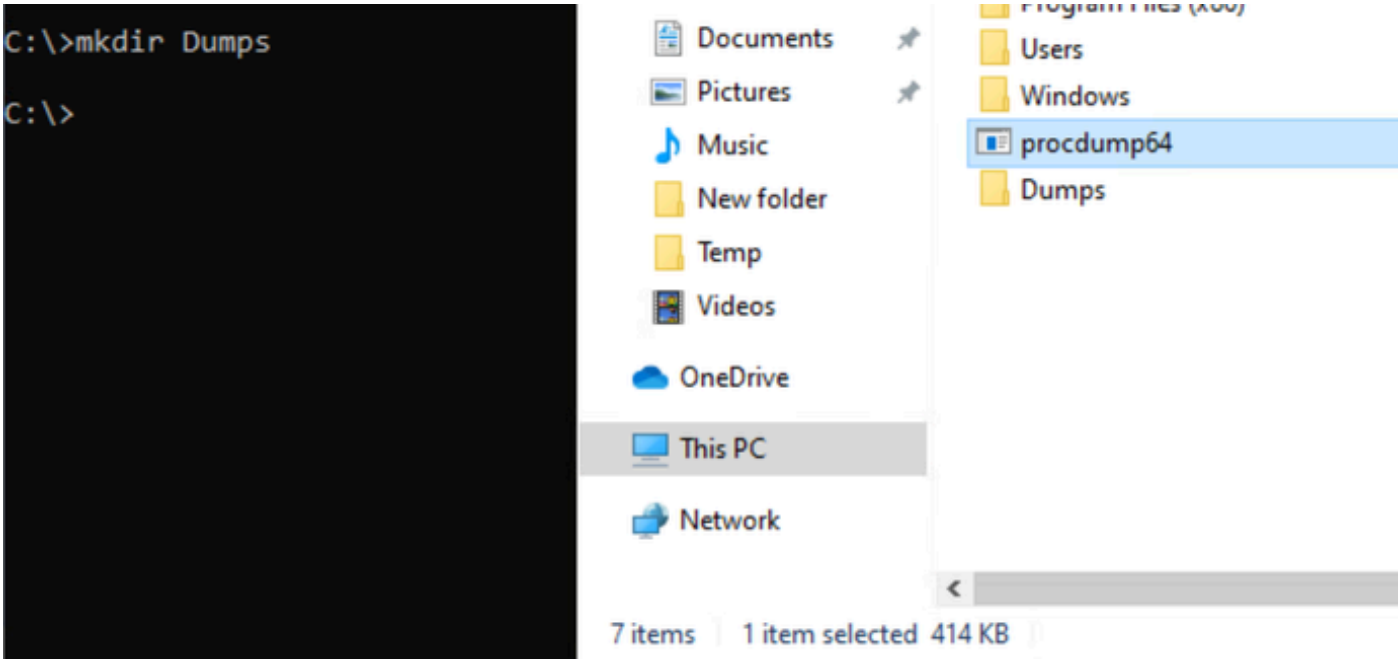
- Die Anwendung für sichere Endgeräte von Cisco kann aufgrund eines Prozessabsturzes von sfc.exe in den Status "Deaktiviert" oder "Getrennt" wechseln. Dies kann mit einem unerwarteten Herunterfahren von Windows oder anderen Aktivitäten auf Windows zusammenhängen.
- Windows aktiviert ein Debugtool, das in den AeDebug-Registrierungswerten konfiguriert ist. Jedes Programm kann im Voraus als Werkzeug für diese Situation ausgewählt werden. Das

ausgewählte Programm wird als Postmortem-Debugger bezeichnet.

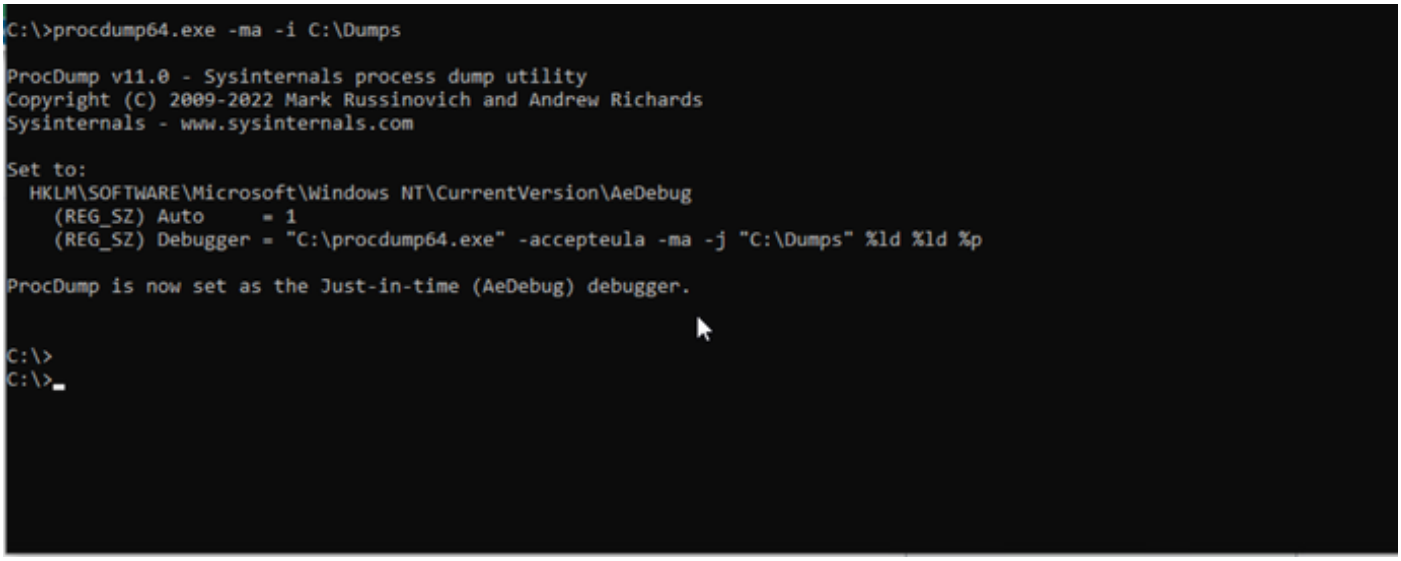
Lösung

Downloaden Sie Procdump als (AeDebug) Postmortem-Debugger aus der Systemintegrals-Suite.

Extrahieren Sie Procdump in Laufwerk C und erstellen Sie den Ordner Dumps für die Crashdump-Sammlung wie folgt:



Festlegen von Procdump als AeDebugger:



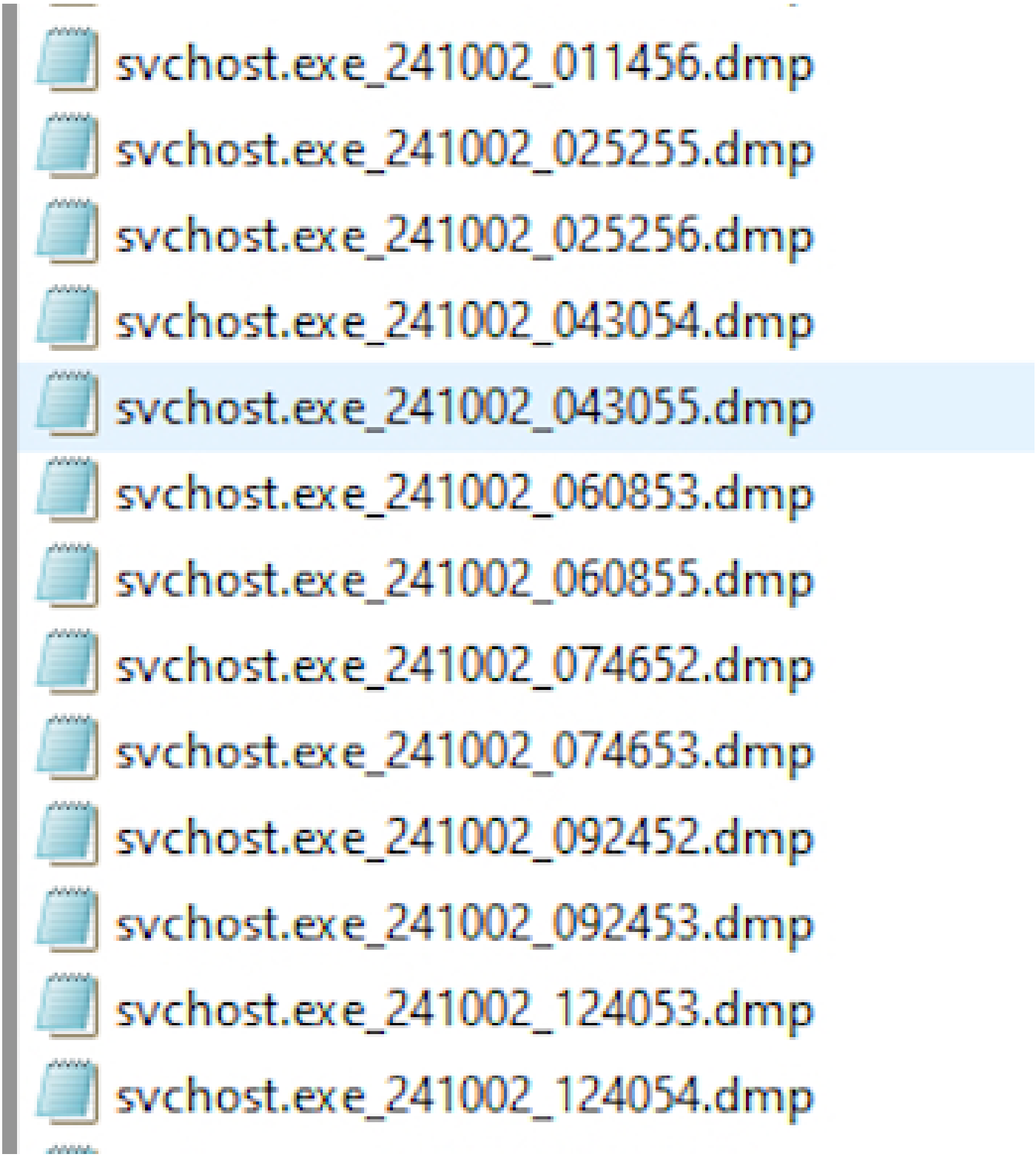
Nutzung:

- Starten Sie CMD als Administrator.
- Wechseln Sie in das Verzeichnis, in das Sie procdump entpackt haben.
- Befehlsbeispiel: procdump64.exe -ma <PID | Prozessname> oder procdump64.exe -ma -i C:\Dumps

Beispiel für sfc.exe:

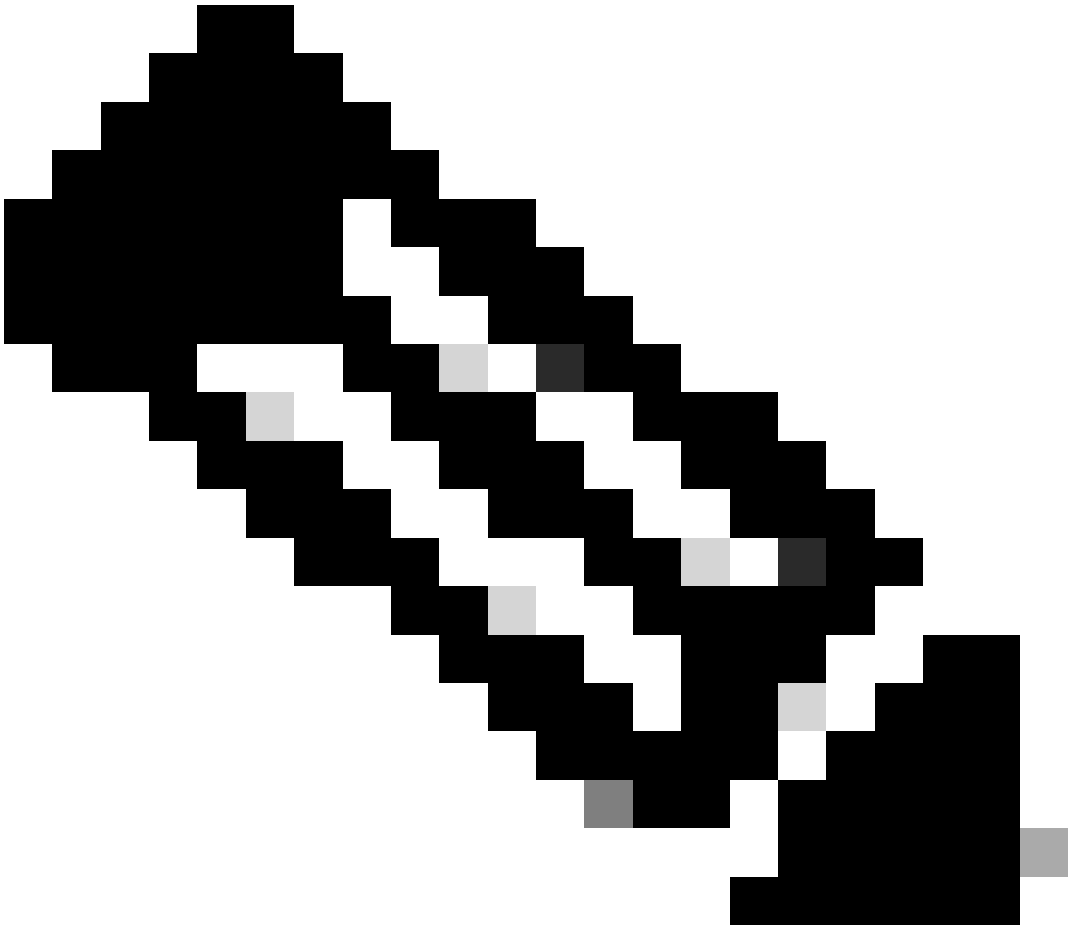
procdump64.exe -accept -ma -e -x c:\install %ProgramFiles%\Cisco\AMP\8.2.3.30119\sfc.exe

Es speichert die Abstürze im Dumps-Ordner wie abgebildet. Sammeln und zur Analyse freigeben:



So deinstallieren Sie procdump: procdump64.exe -u

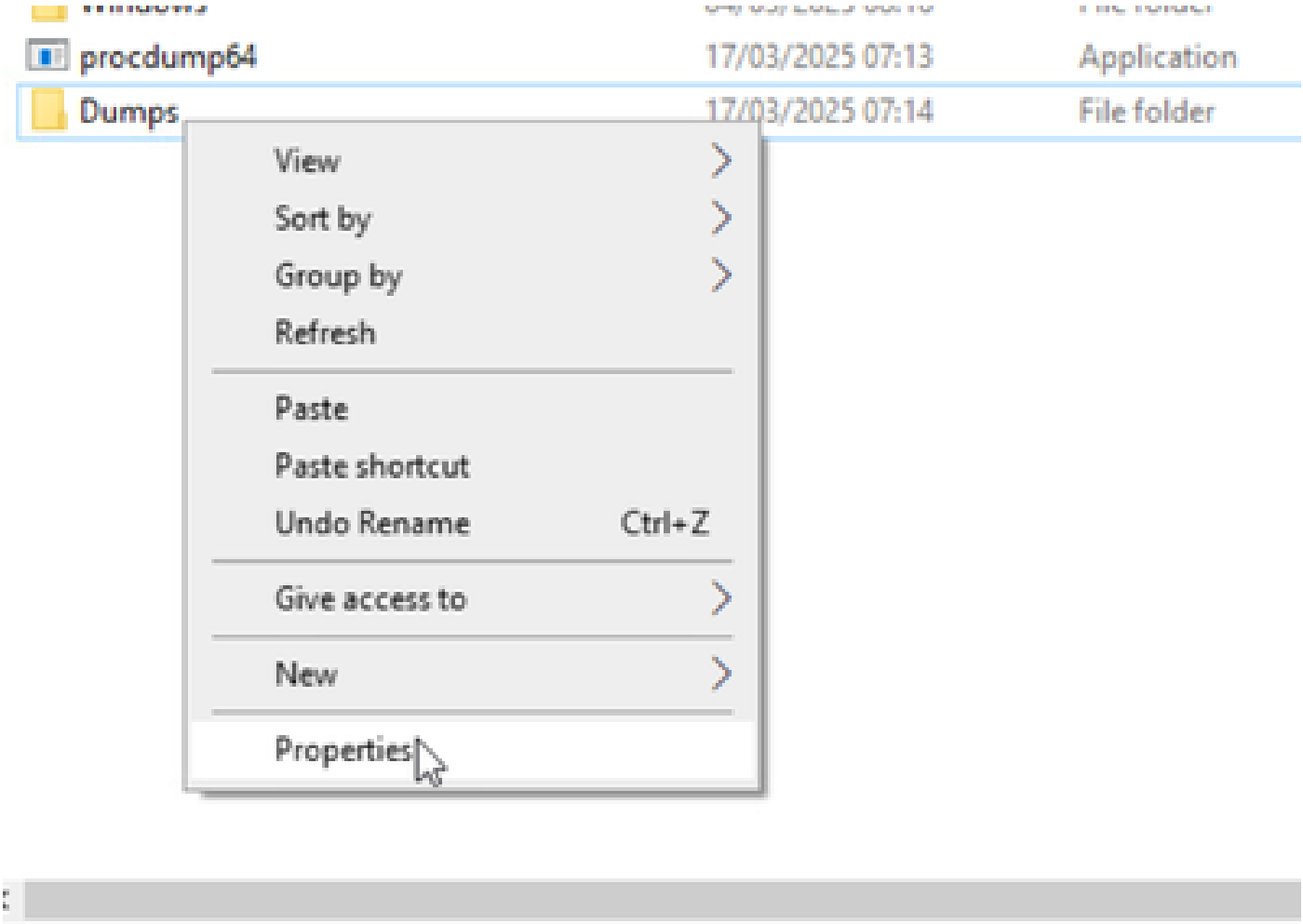
```
C:\>
C:\>procdump64.exe -u

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:\>_
```

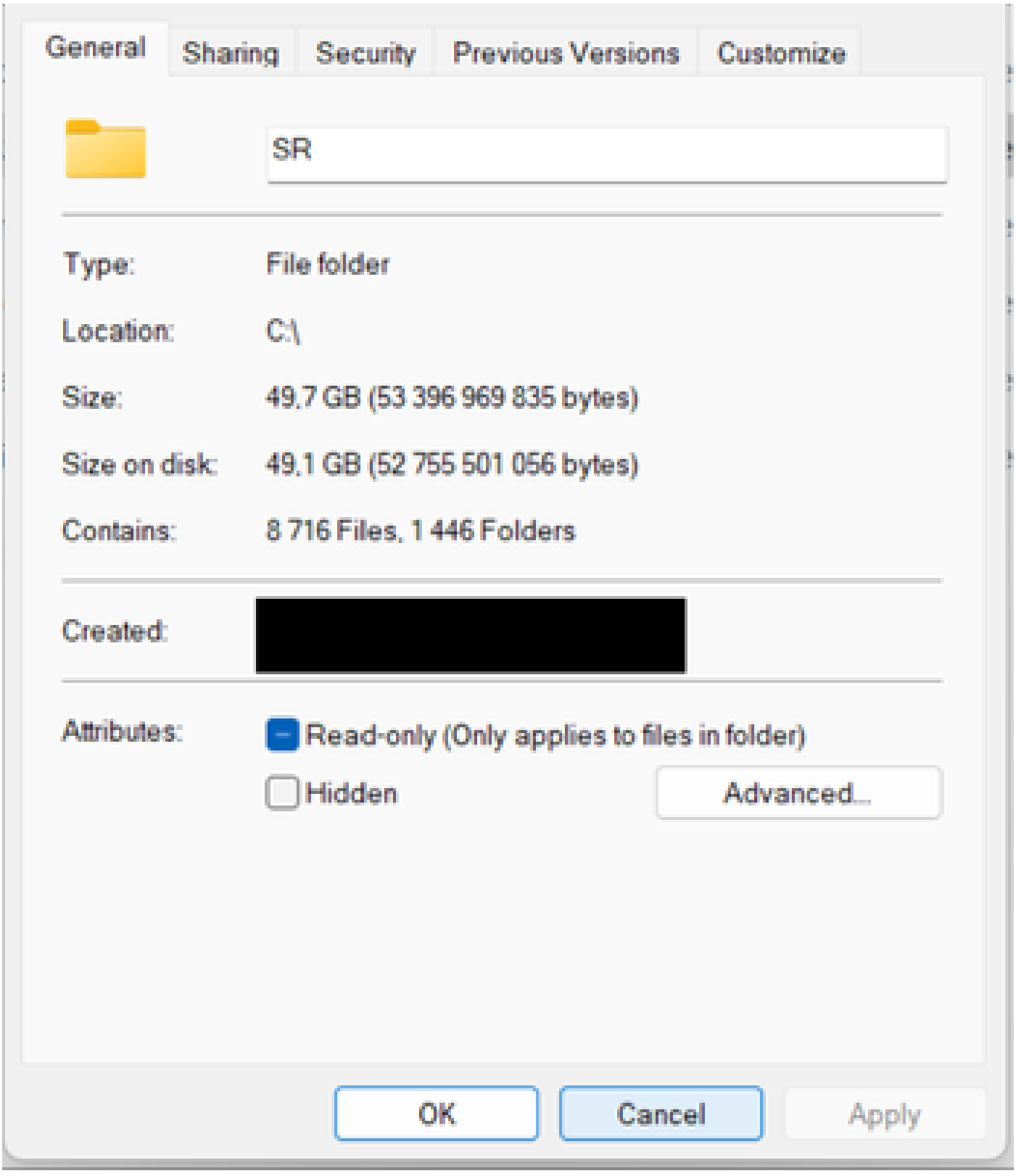


Anmerkung: Crash Dumps können großen Speicherplatz auf der Festplatte belegen, und procdump kann gestoppt werden, sobald die Sammlung abgeschlossen ist.

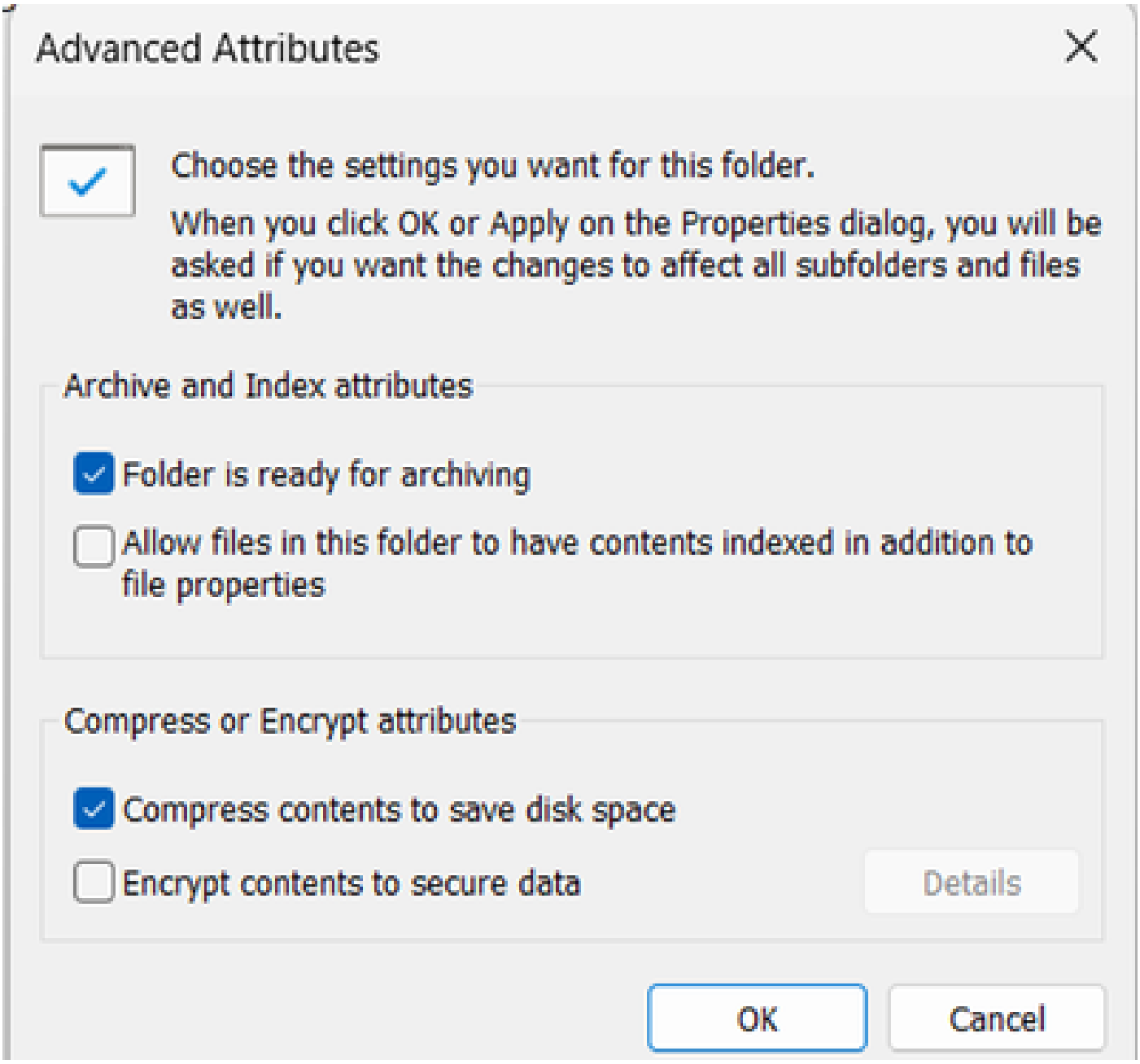
Sie können die Größe des Ordners jedoch auch mit der Problemumgehung komprimieren:

1- Navigieren Sie zu den Eigenschaften des Ordners Dumps und überprüfen Sie die Originalgröße des Ordners auf der Festplatte wie folgt:

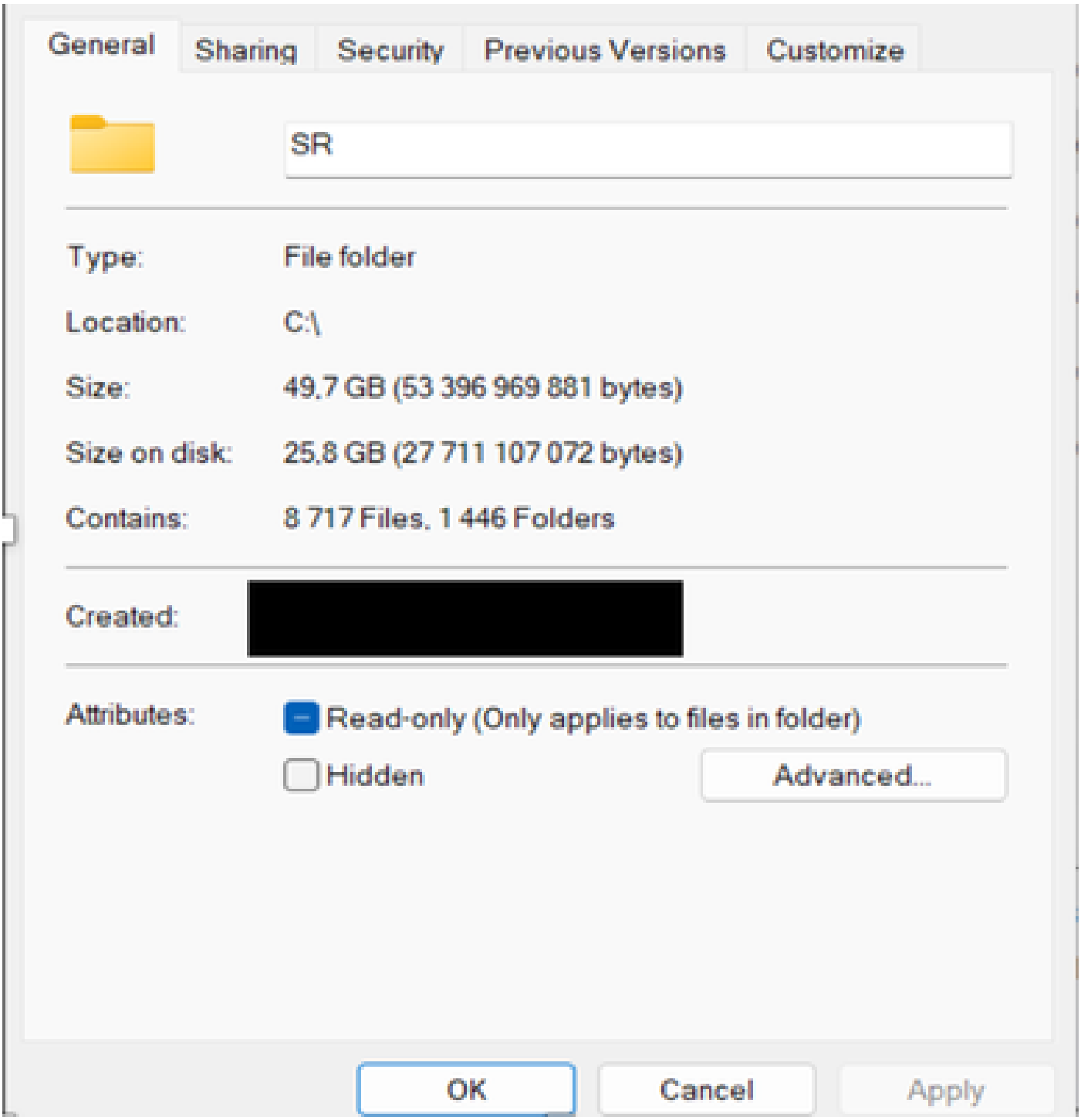




2 - Navigieren Sie zur Option Advanced und aktivieren Sie die Komprimierung und das Anwenden, was einige Minuten dauert:



3- Am Ende können Sie sehen, die Ordnergröße reduziert sich auf fast die Hälfte der ursprünglichen Größe wie gezeigt:



4- Sie können diesen Befehl auch an der Eingabeaufforderung verwenden, um dasselbe zu erreichen:

compact /c /s:c:\install

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.