在Windows上為Sfc進程收集進程崩潰轉儲

目錄

簡介

本文檔介紹如何在Windows上為sfc進程收集進程崩潰轉儲。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全終端聯結器
- 命令提示視窗

使用的元件集

本檔案所述內容不限於軟體和硬體版本。本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

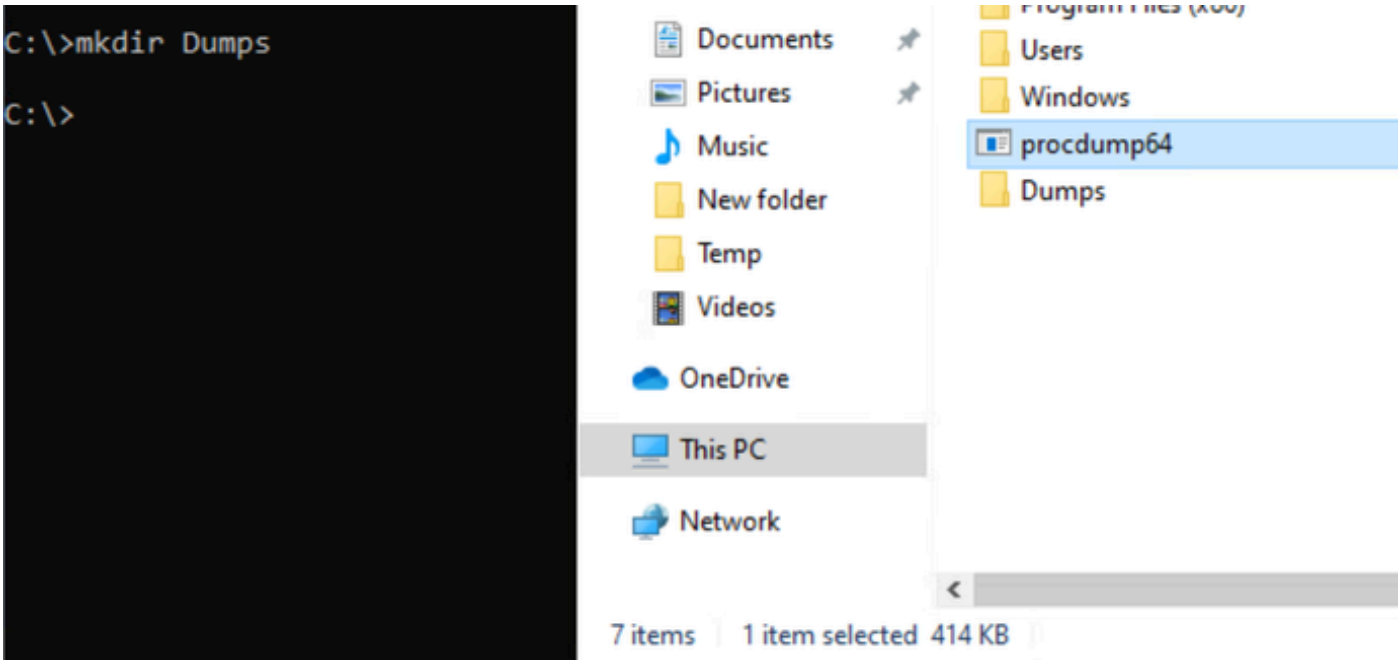
問題

- 由於sfc.exe進程崩潰，思科安全終結點應用程式可能進入禁用或斷開連線狀態，這可能與Windows上的意外關閉或其他活動有關。
- Windows啟用在AeDebug登錄檔值中配置的調試工具。任何程式都可以事先選擇作為在這種情況下使用的工具。所選程式稱為死後的調試程式。

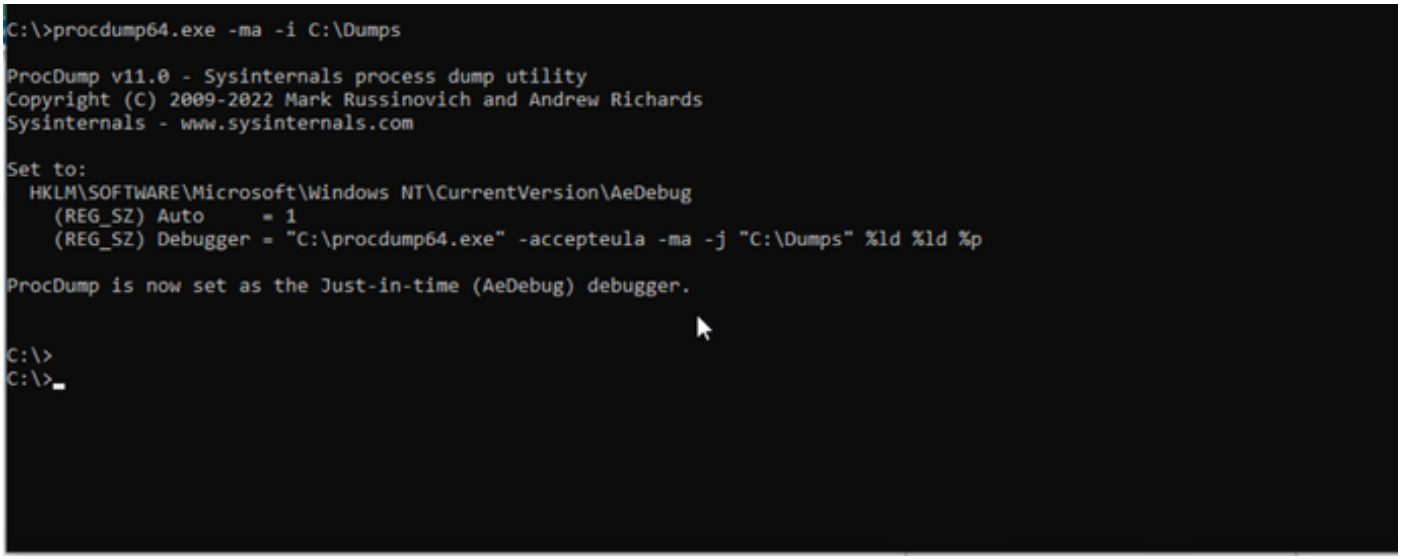
解決方案

從sysinternals套件下載Procdump作為(AeDebug)事後偵錯程式。

在c驅動器中提取Procdump，然後為crashdump集合建立Dumps資料夾，如下所示：



將Procdump設定為AeDebugger:



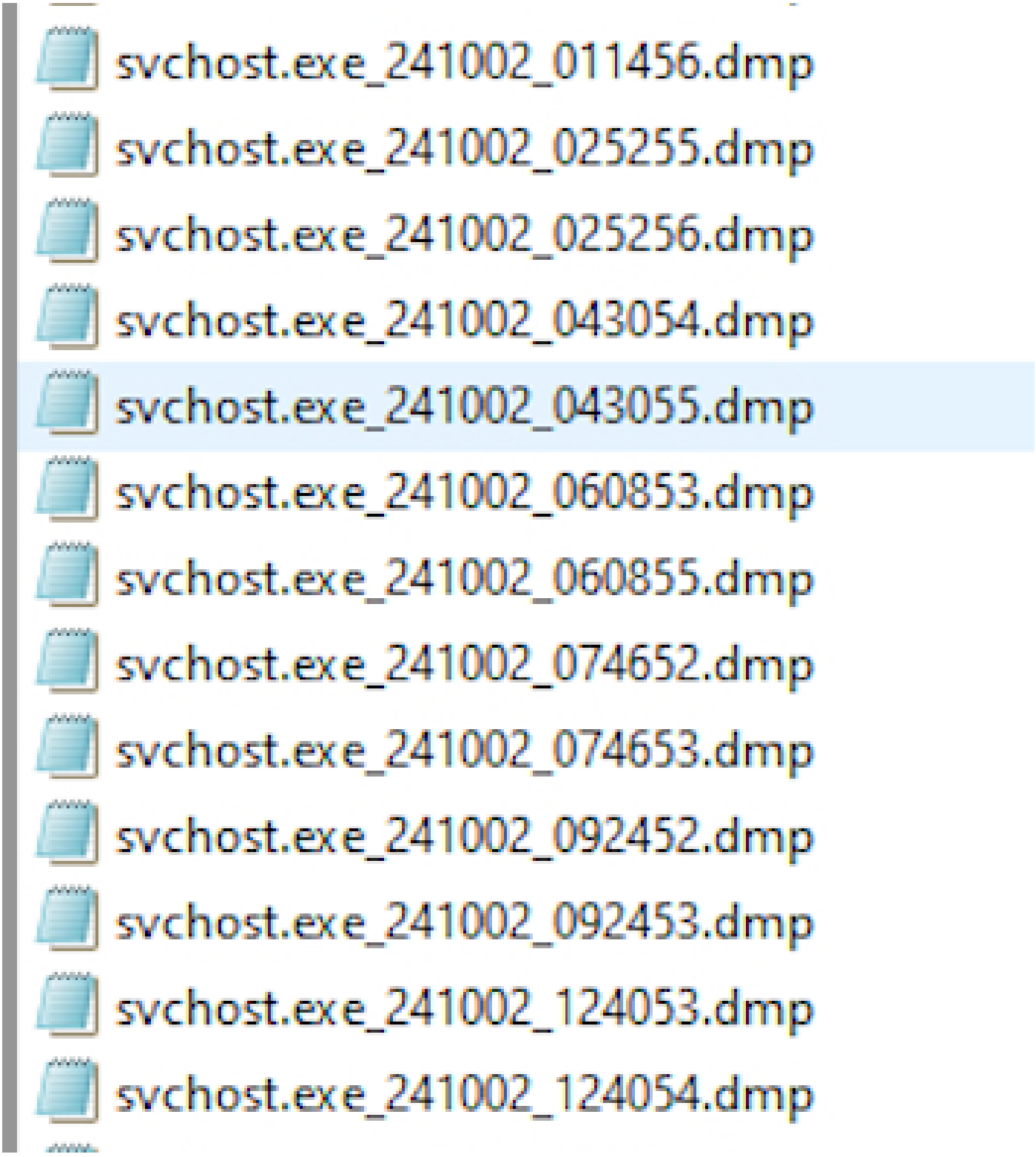
使用方法:

- 以管理員身份啟動CMD。
- 轉到解壓縮過程轉儲工具的目錄。
- 命令示例： procdump64.exe -ma <PID |進程名稱>或procdump64.exe -ma -i C:\Dumps

sfc.exe示例：

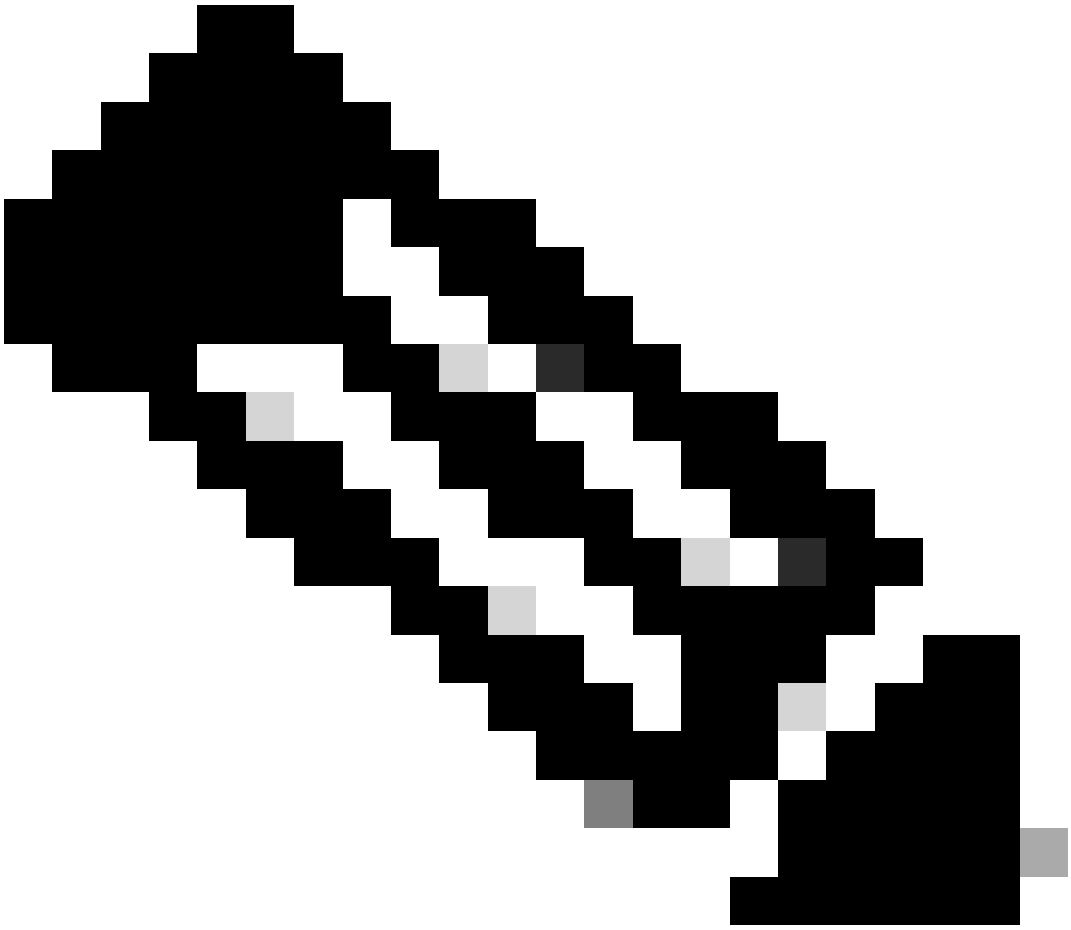
procdump64.exe -accepteula -ma -e -x c:\install %ProgramFiles%\Cisco\AMP\8.2.3.30119\sfc.exe

它將crashdump儲存在Dumps資料夾中，如下所示。收集並共用它進行分析：



要解除安裝procdump，請使用：procdump64.exe -u

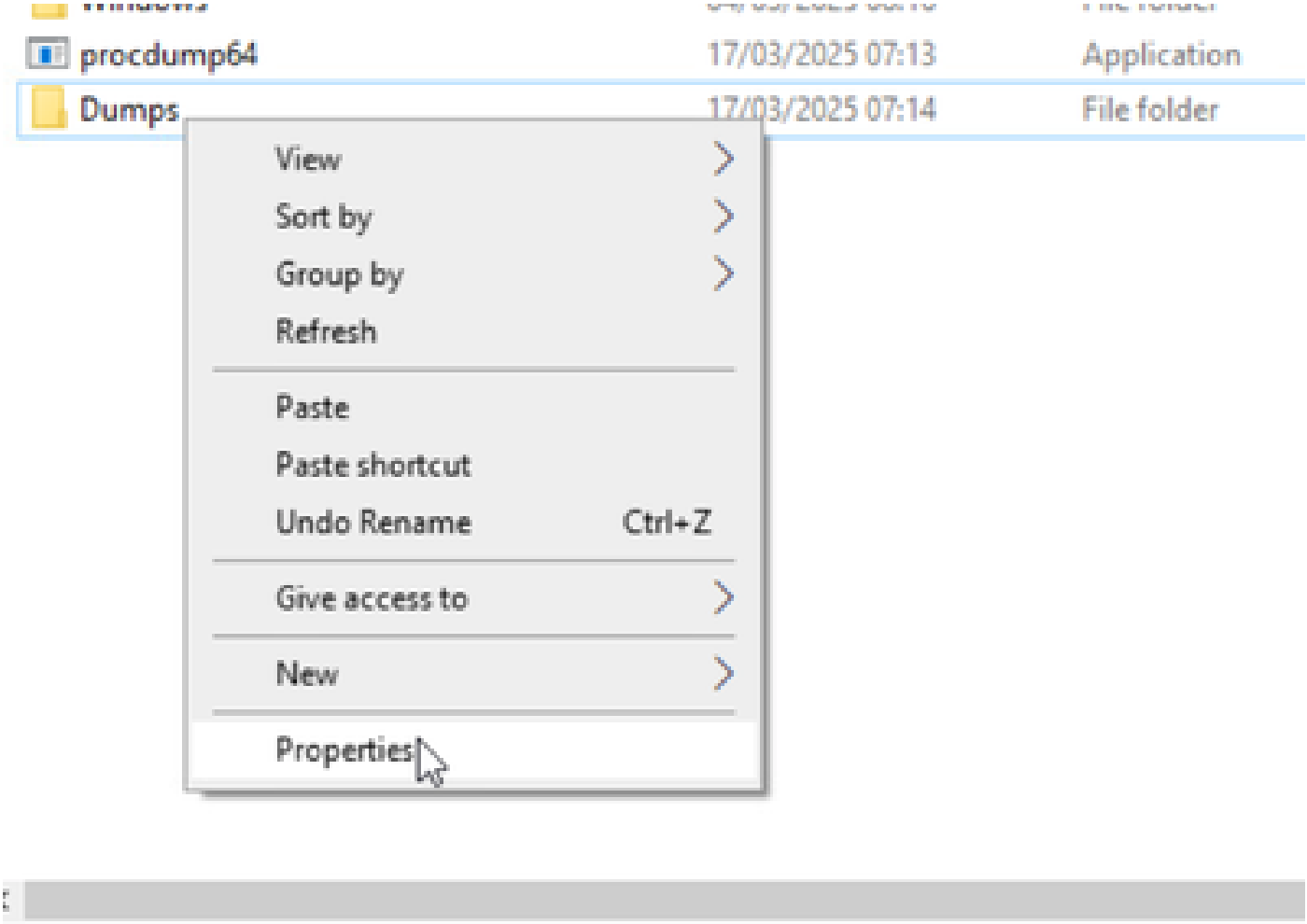
```
C:\>
C:\>procdump64.exe -u

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:\>_
```

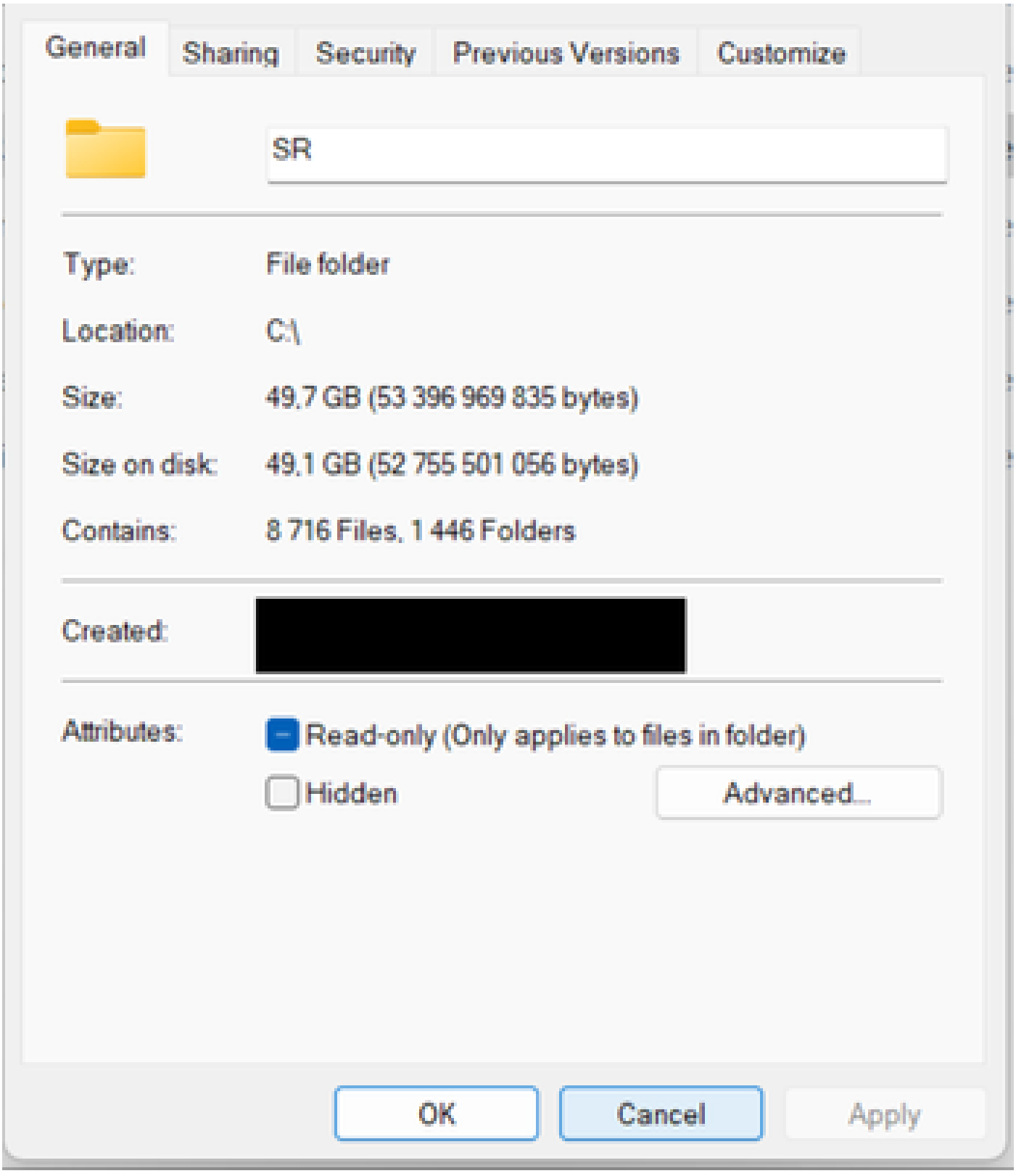


附註：故障轉儲可能會佔用磁碟上的大量空間，並且收集完成後可以停止轉儲。

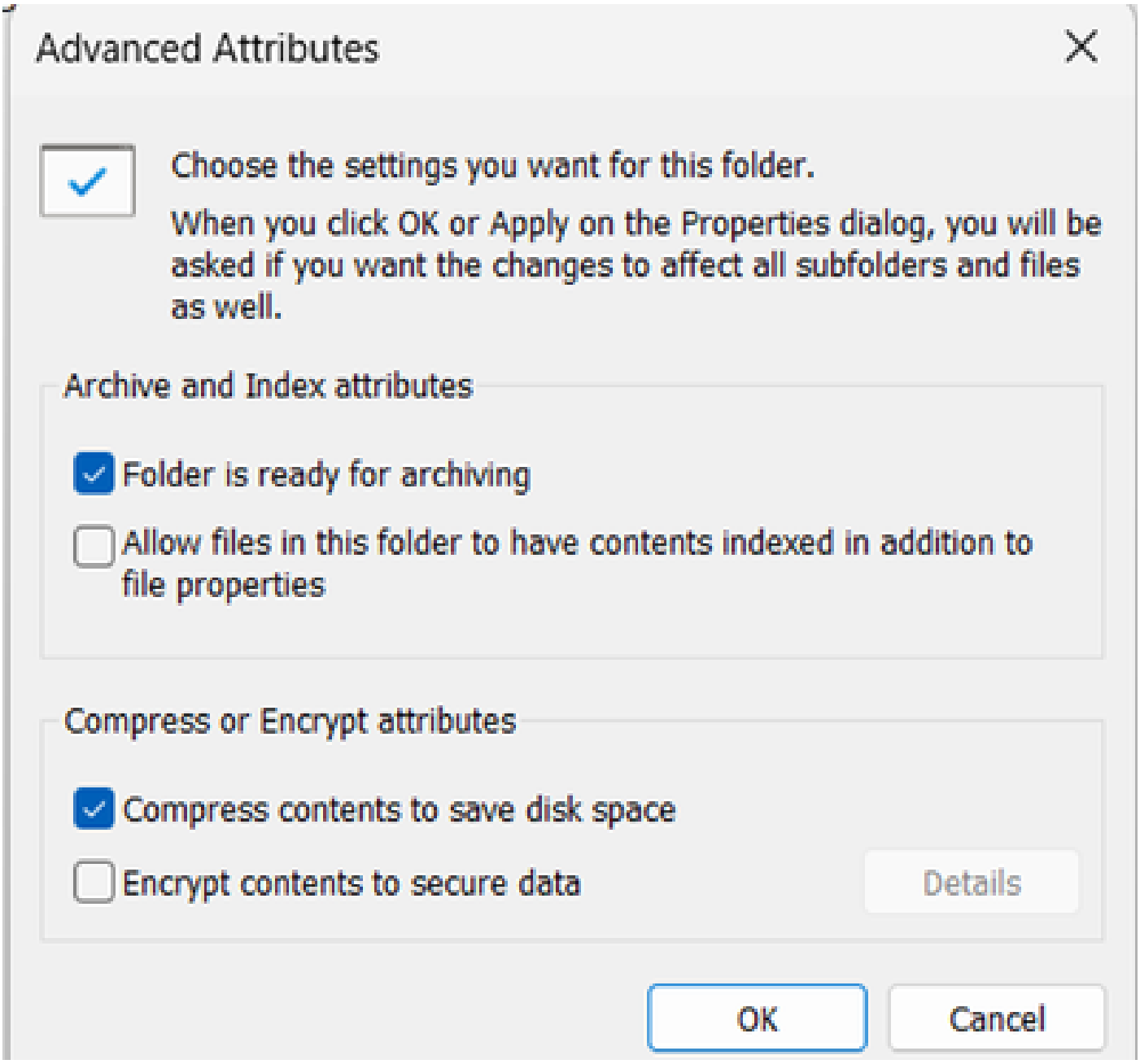
不過，也可以使用替代方法壓縮資料夾的大小：

1 — 導航到Dumps資料夾的屬性，然後檢查磁碟上資料夾的原始大小，如下所示：

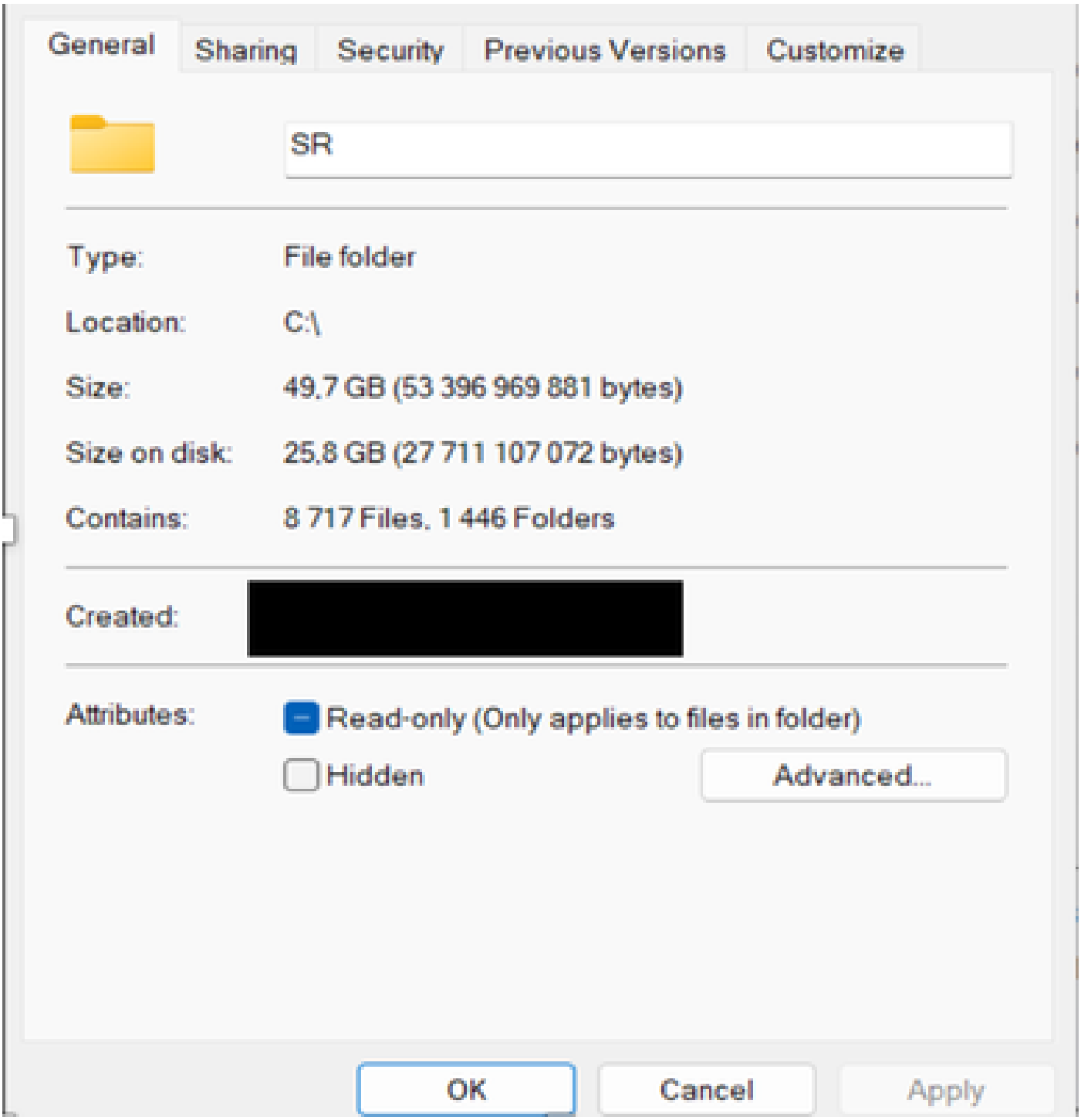

procdump64
17/03/2025 07:13
Application
Dumps
17/03/2025 07:14
File folder
View
Sort by
Group by
Refresh
Paste
Paste shortcut
Undo Rename
Ctrl+Z
Give access to
New
Properties



2 — 導航到Advanced選項，然後啟用compression並應用，此操作需要幾分鐘：



3 — 最後，您可以看到資料夾大小減少到原始大小的近一半，如下所示：



4 — 您也可以在命令提示符下使用此命令來實現相同目的：

精簡型/c /s:c:\install

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。