

SfcプロセスのWindowsでのプロセスのクラッシュダンプの収集

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題](#)

[解決方法](#)

はじめに

このドキュメントでは、SFCプロセスのWindowsでプロセスのクラッシュダンプを収集する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Endpointコネクタ
- コマンドプロンプトウィンドウ

使用するコンポーネント

このドキュメントは、ソフトウェアとハードウェアのバージョンに限定されるものではありません。このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

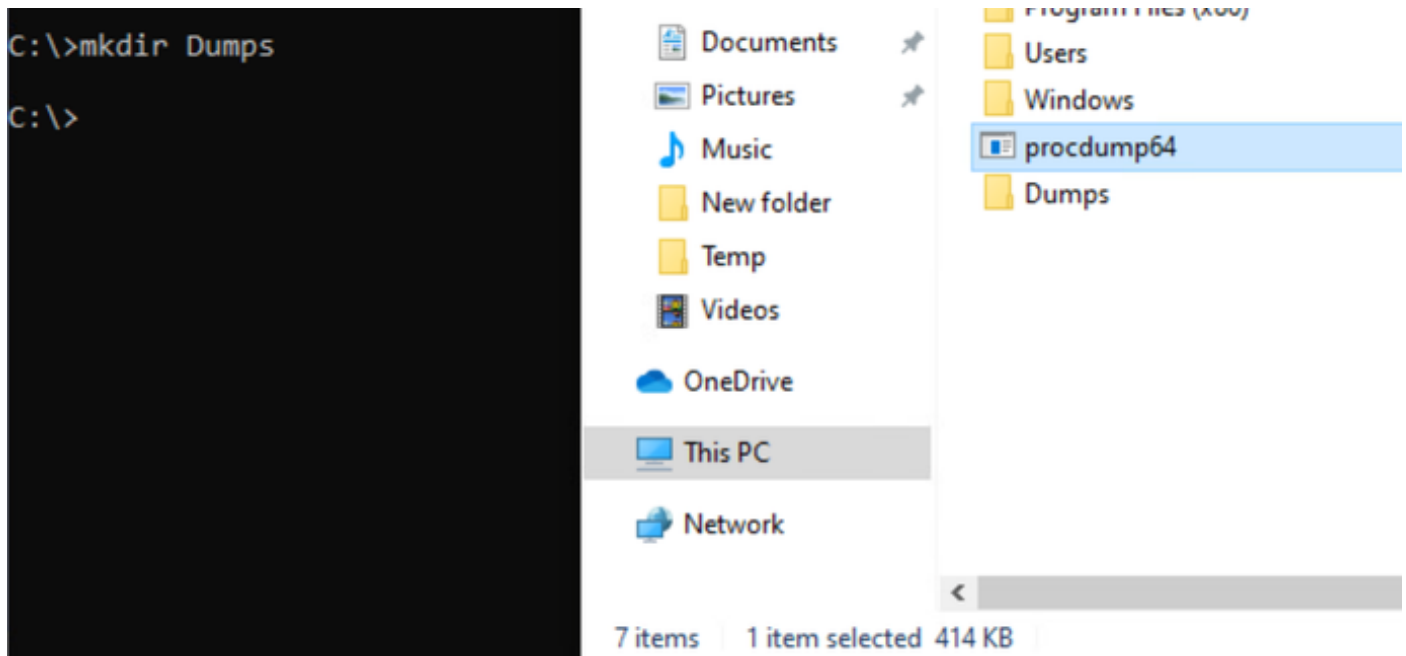
問題

- sfc.exeのプロセスのクラッシュにより、Cisco Secureエンドポイントアプリケーションが無効または切断された状態になる場合があります。これは、予期しないwindowsのシャットダウンや、windows上のその他のアクティビティに関連している可能性があります。
- Windowsは、AeDebugレジストリ値に設定されているデバッグツールをアクティブにします。この状況で使用するツールとして、任意のプログラムを事前に選択できます。選択したプログラムは、事後デバッガと呼ばれます。

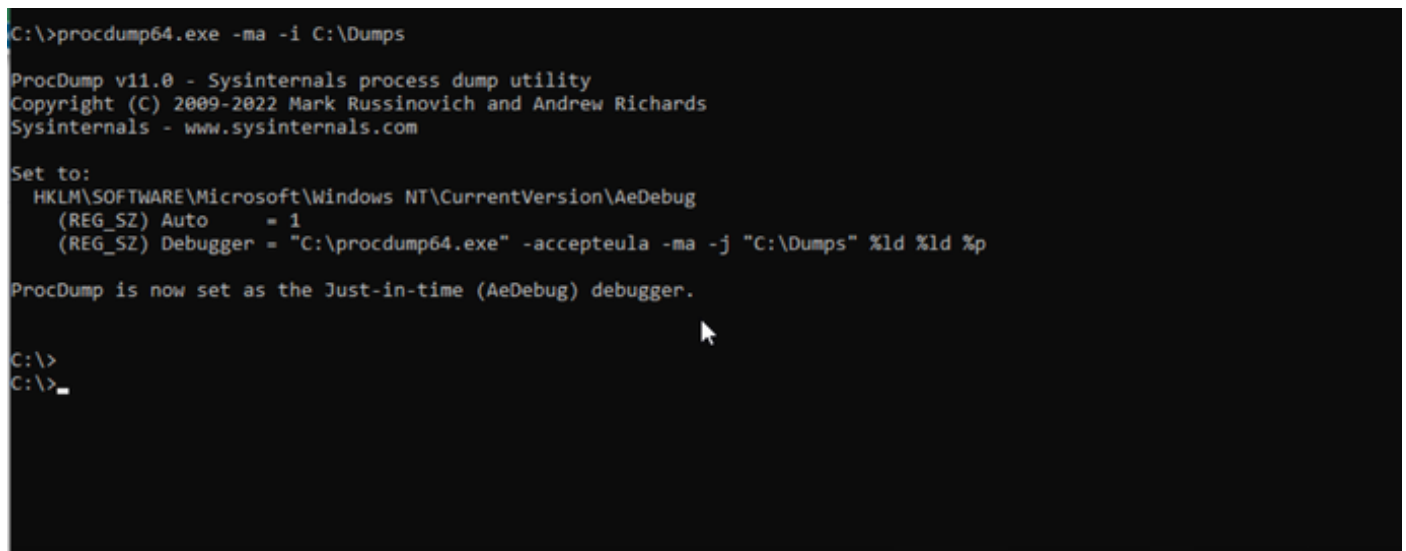
解決方法

sysinternals suiteから[Procdumpを\(AeDebug\)postmortemデバッガ](#)としてダウンロードします。

cドライブにProcdumpを抽出し、次に示すようにクラッシュダンプ収集用のDumpsフォルダを作成します。



ProcdumpをAeDebuggerとして設定します。



使用方法:

- 管理者としてCMDを起動します。
- procdumpツールを展開したディレクトリに移動します。

- コマンド例 : procdump64.exe -ma <PID | Process Name> または procdump64.exe -ma -i C:\Dumps

sfc.exeの例 :

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

次に示すように、クラッシュダンプがDumpsフォルダに保存されます。分析のために収集して共有します。

 svchost.exe_241002_011456.dmp svchost.exe_241002_025255.dmp svchost.exe_241002_025256.dmp svchost.exe_241002_043054.dmp svchost.exe_241002_043055.dmp svchost.exe_241002_060853.dmp svchost.exe_241002_060855.dmp svchost.exe_241002_074652.dmp svchost.exe_241002_074653.dmp svchost.exe_241002_092452.dmp svchost.exe_241002_092453.dmp svchost.exe_241002_124053.dmp svchost.exe_241002_124054.dmp

procdumpをアンインストールするには、procdump64.exe -uを使用します。

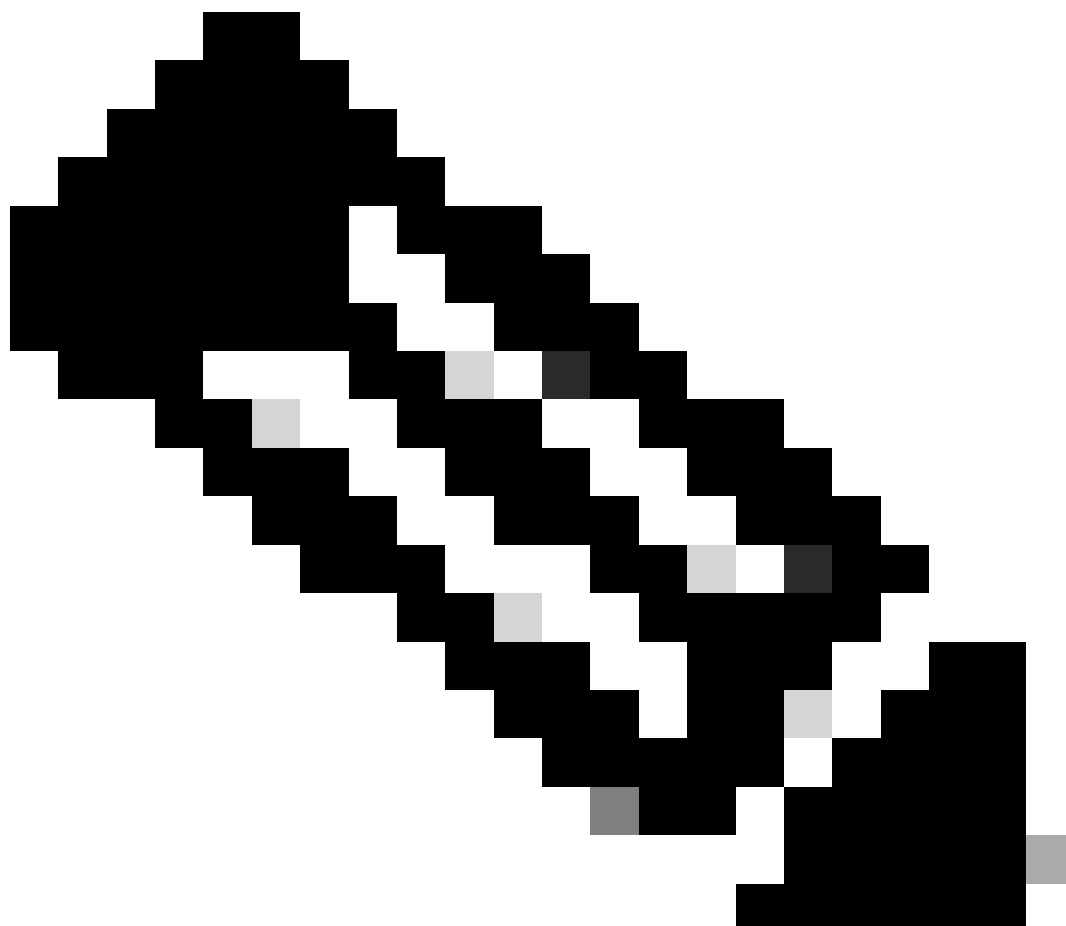
```
C:\>
C:\>procdump64.exe -u

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.

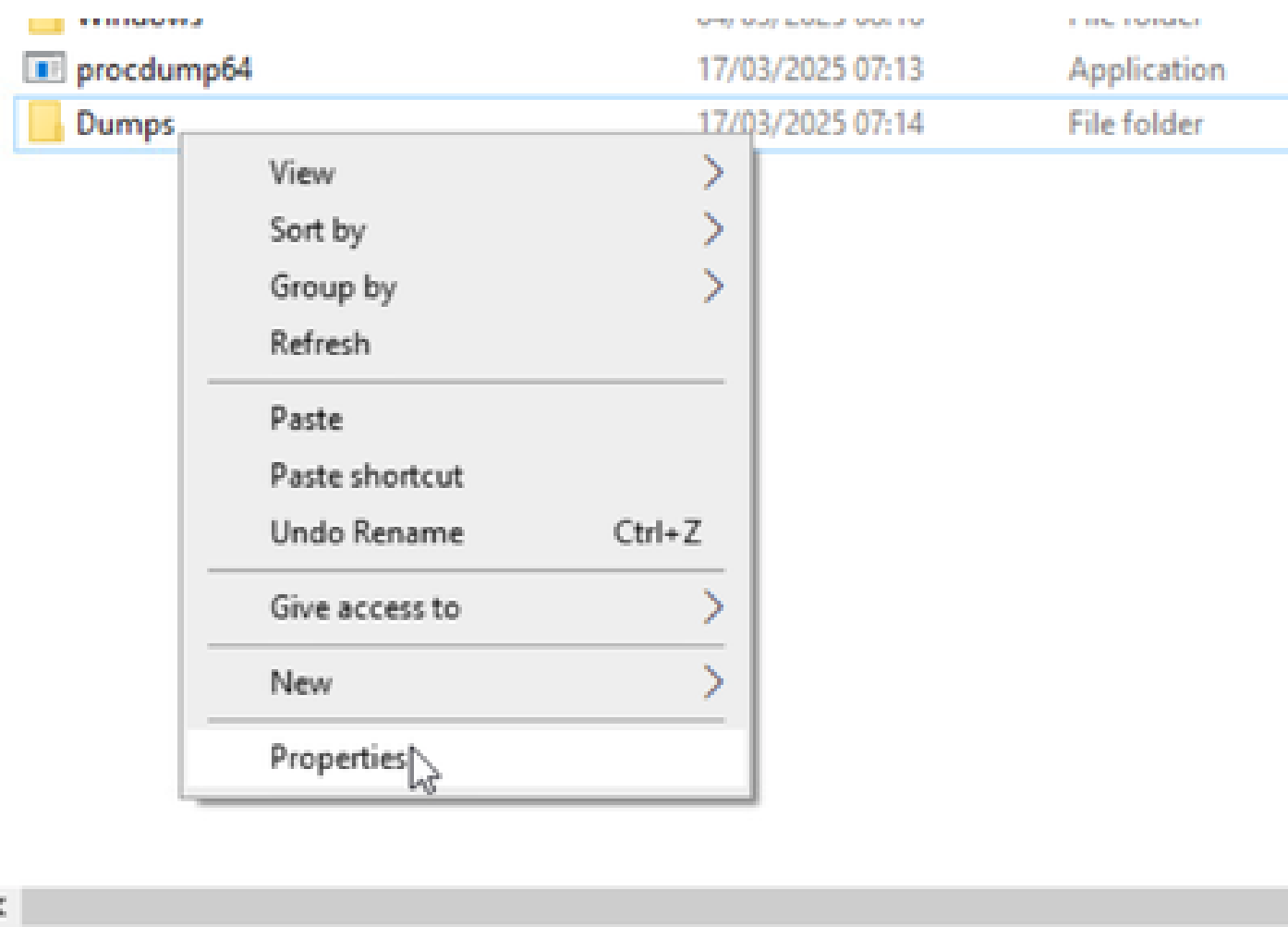
C:\>_
```

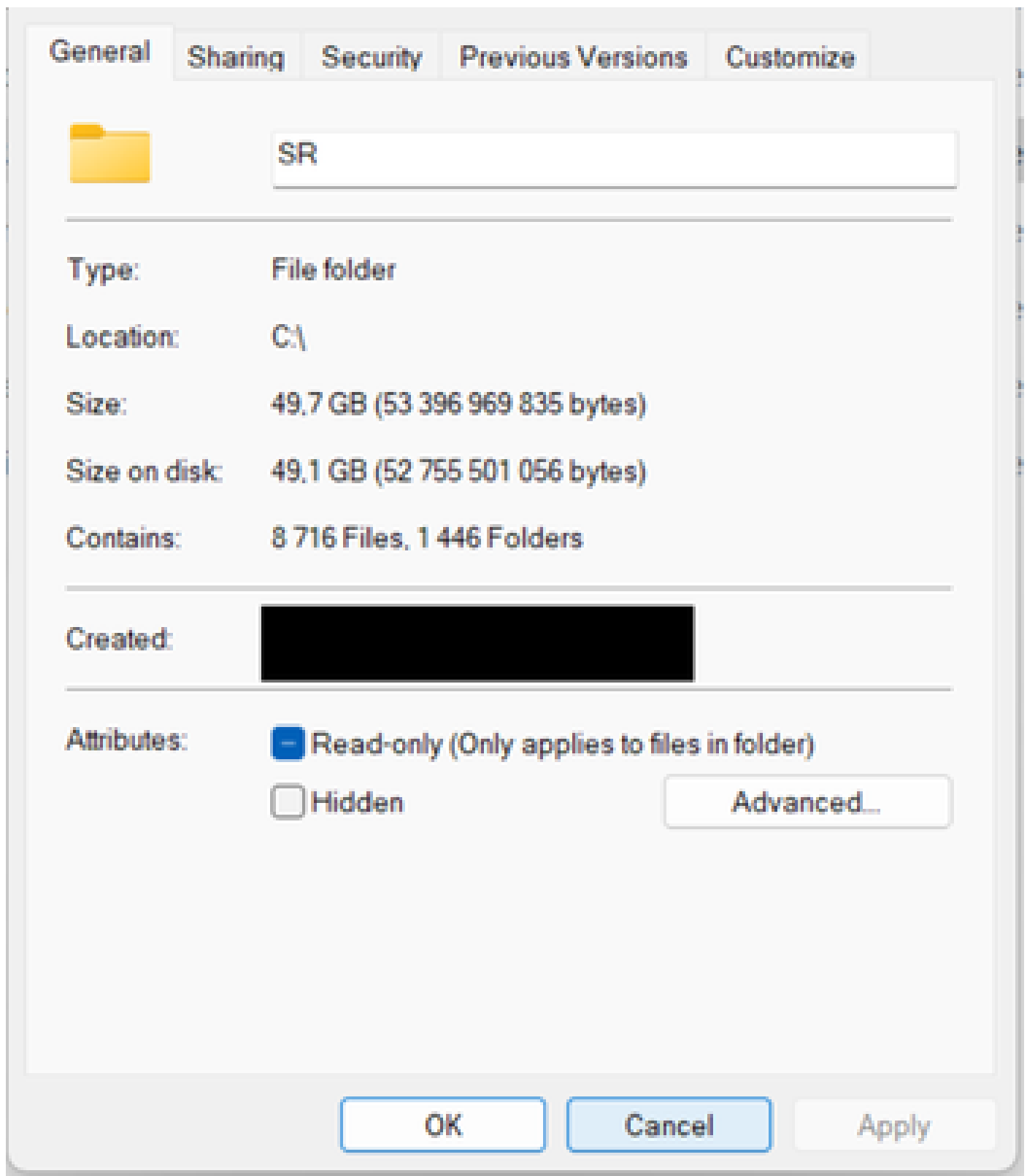


注：クラッシュダンプはディスク上の領域を大量に消費する可能性があり、収集が完了したらprocdumpを停止できます。

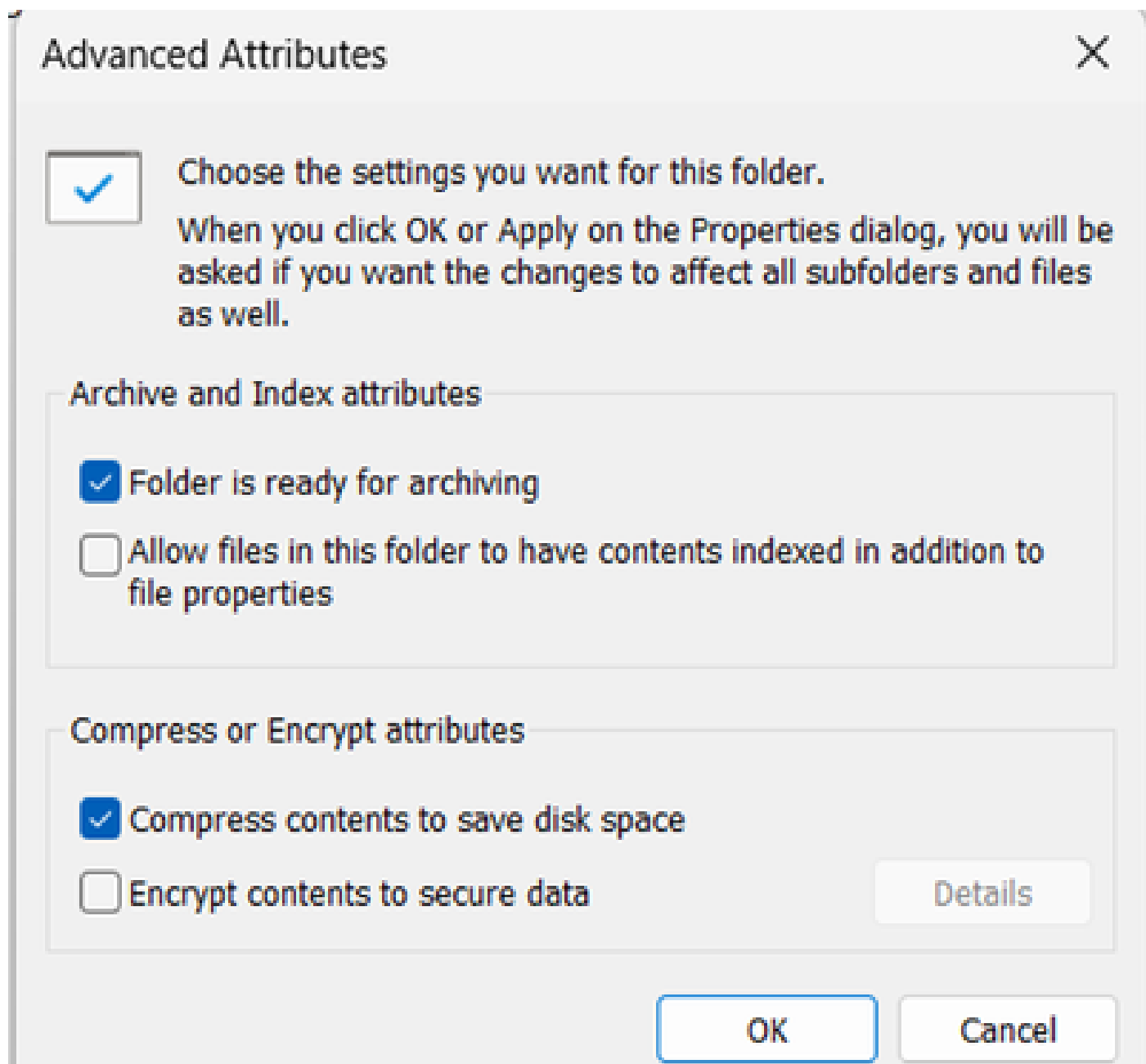
ただし、回避策を使用してフォルダのサイズを圧縮することもできます。

1- Dumpsフォルダのpropertiesに移動し、次に示すようにディスク上のフォルダのoriginal sizeを確認します (図1の矢印Aを参照) 。

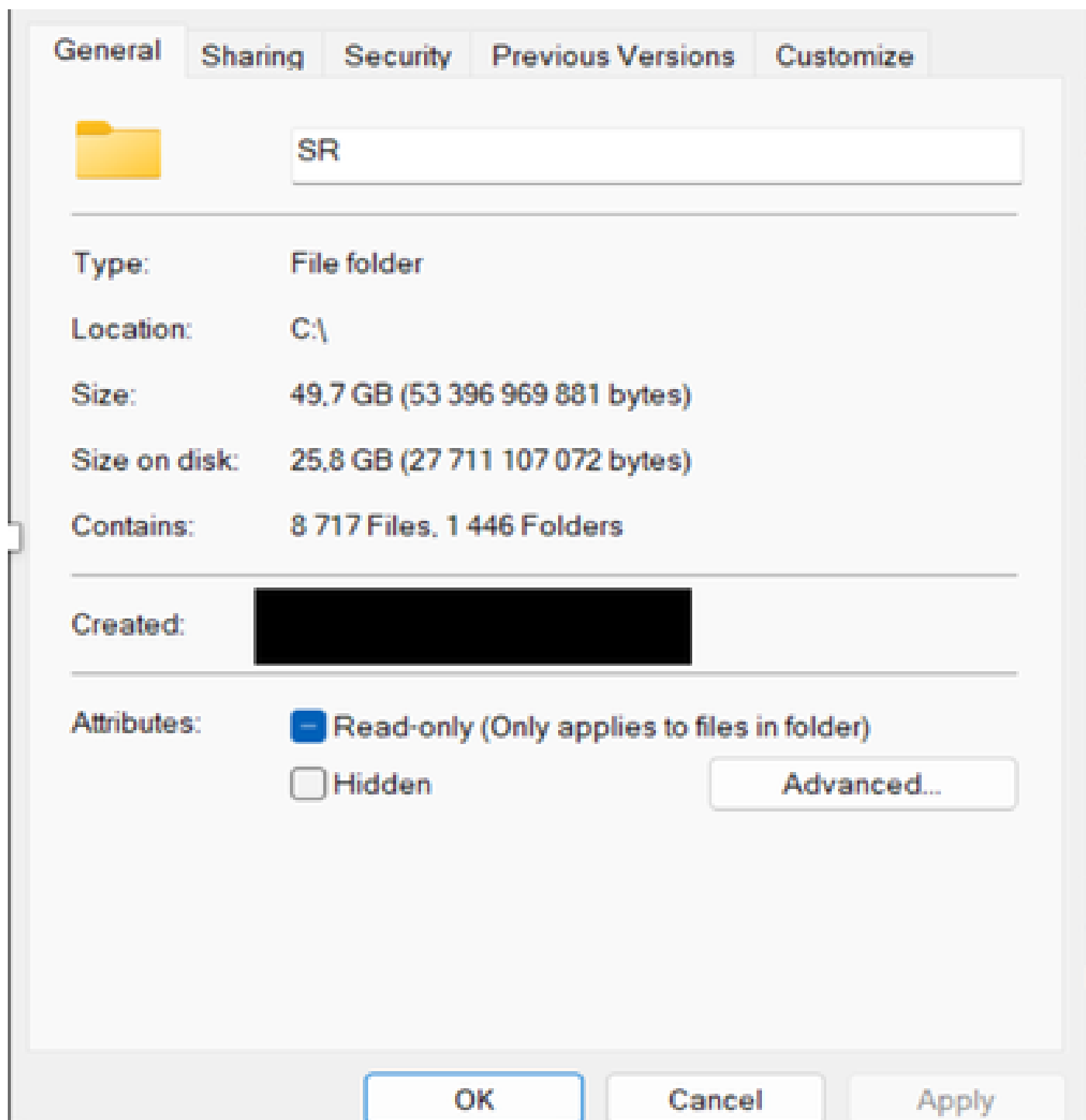




2- Advancedオプションに移動し、enable compressionを選択して適用します。これには数分かかります。



3 – 最後に、次のようにフォルダサイズが元のサイズのほぼ半分に縮小されることがわかります。



4 – コマンドプロンプトで次のコマンドを使用しても同じ結果が得られます。

コンパクト/c /s:c:\install

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。