Raccogli dettagli arresto anomalo del processo in Windows per processo Sfc

Sommario

Introduzione

In questo documento viene descritto come raccogliere i dettagli arresto anomalo del processo in Windows per il processo sfc.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Endpoint Connector
- Finestre del prompt dei comandi

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware. Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

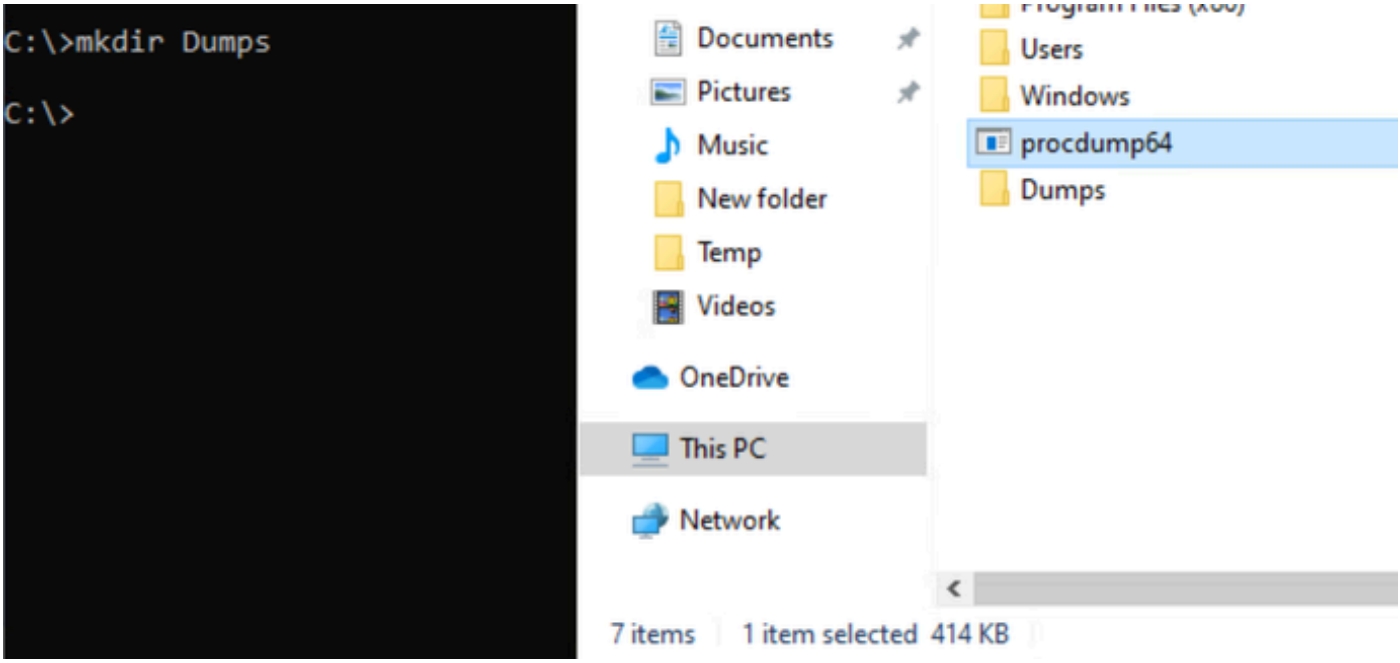
- L'applicazione Cisco Secure Endpoint può passare a uno stato disabilitato o disconnesso a causa di un arresto anomalo del processo di sfc.exe, che potrebbe essere correlato a un arresto imprevisto di Windows o a qualsiasi altra attività in Windows.
- Windows attiva uno strumento di debug configurato nei valori del Registro di sistema AeDebug. Qualsiasi programma può essere selezionato in anticipo come strumento da utilizzare in questa situazione. Il programma scelto viene indicato come debugger post-

mortem.

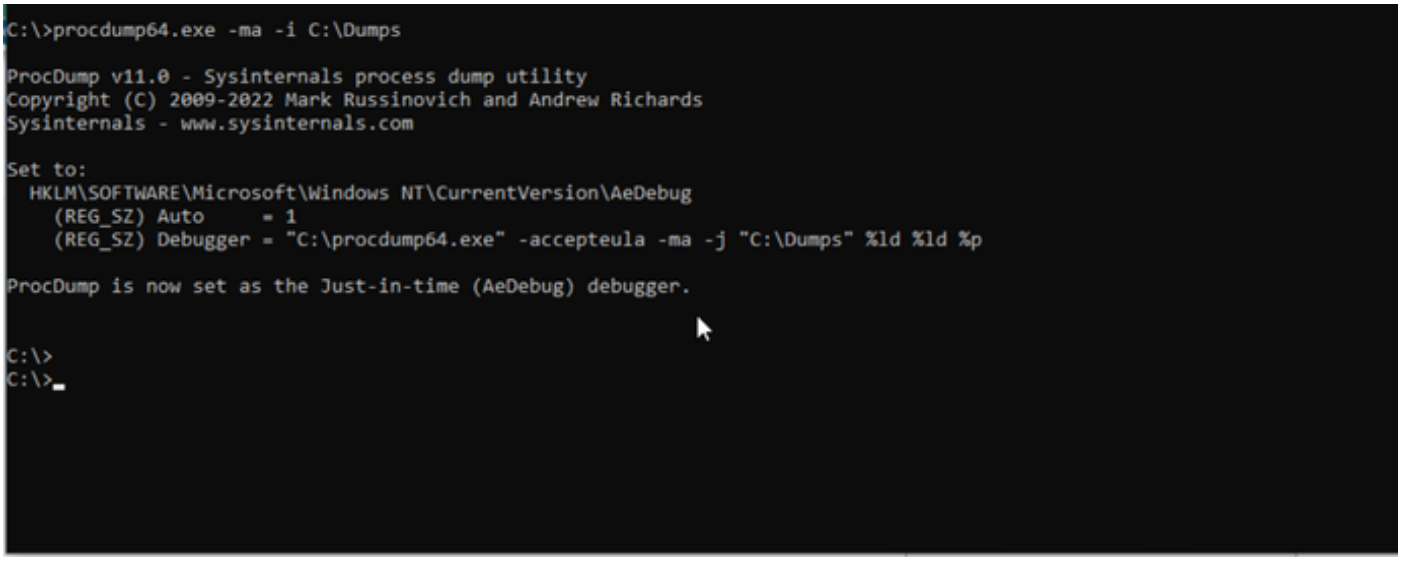
Soluzione

Scaricare Procdump come debugger post-mortem (AeDebug) dalla suite sysinternals.

Estrarre Procdump nell'unità c e creare la cartella Dump per la raccolta di dettagli arresto anomalo come mostrato:



Impostare Procdump come AeDebugger:



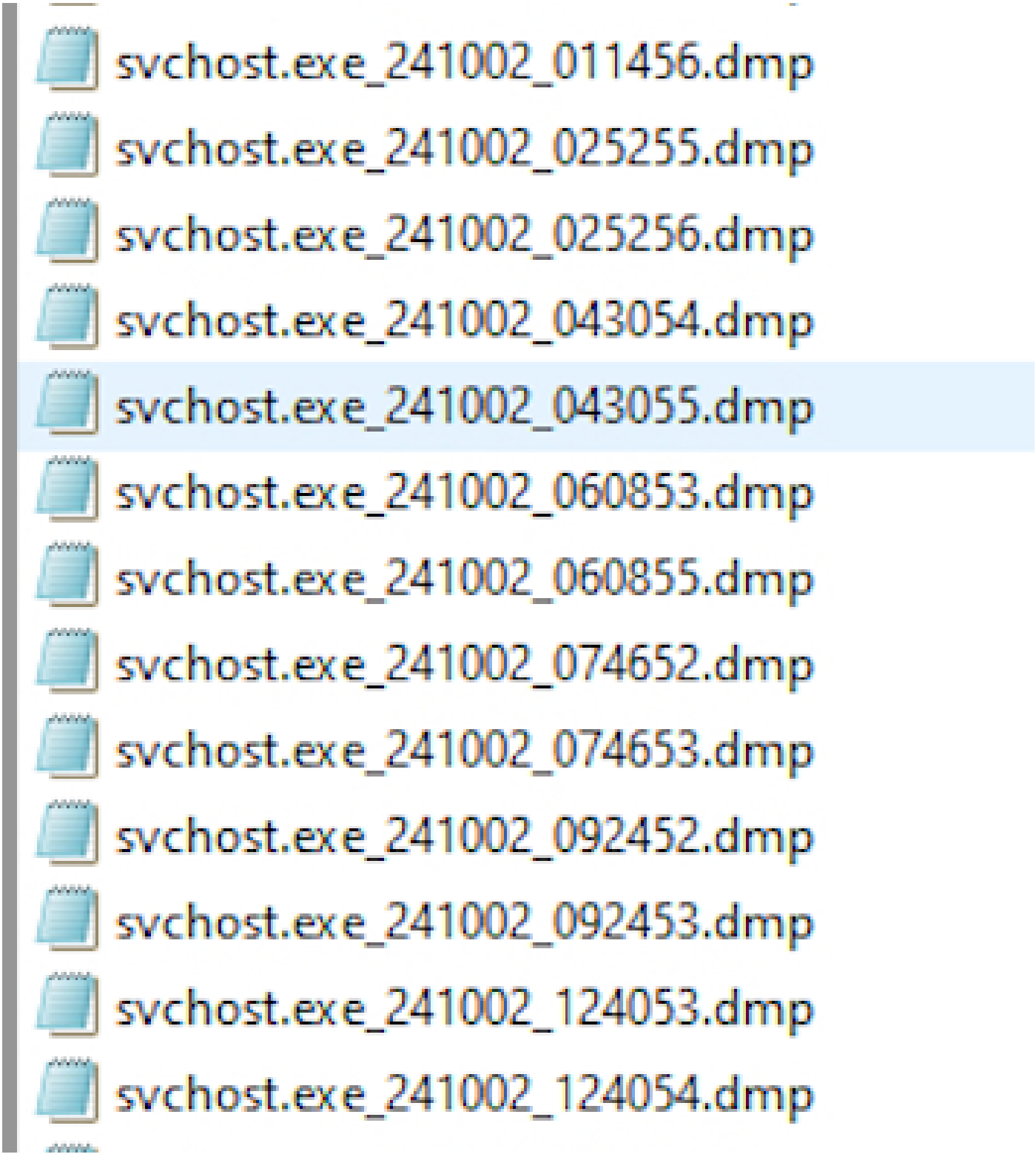
Modalità d'uso:

- Avviare CMD come amministratore.
- Passare alla directory in cui è stato decompresso lo strumento procdump.
- Esempio di comando: procdump64.exe -ma <PID | Nome processo> o procdump64.exe -ma -i C:\Dumps

Esempio per sfc.exe:

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

I dump di arresto anomalo del sistema vengono salvati nella cartella Dump come illustrato. Raccogli e condividilo per l'analisi:



Per disinstallare procdump utilizzare: procdump64.exe -u

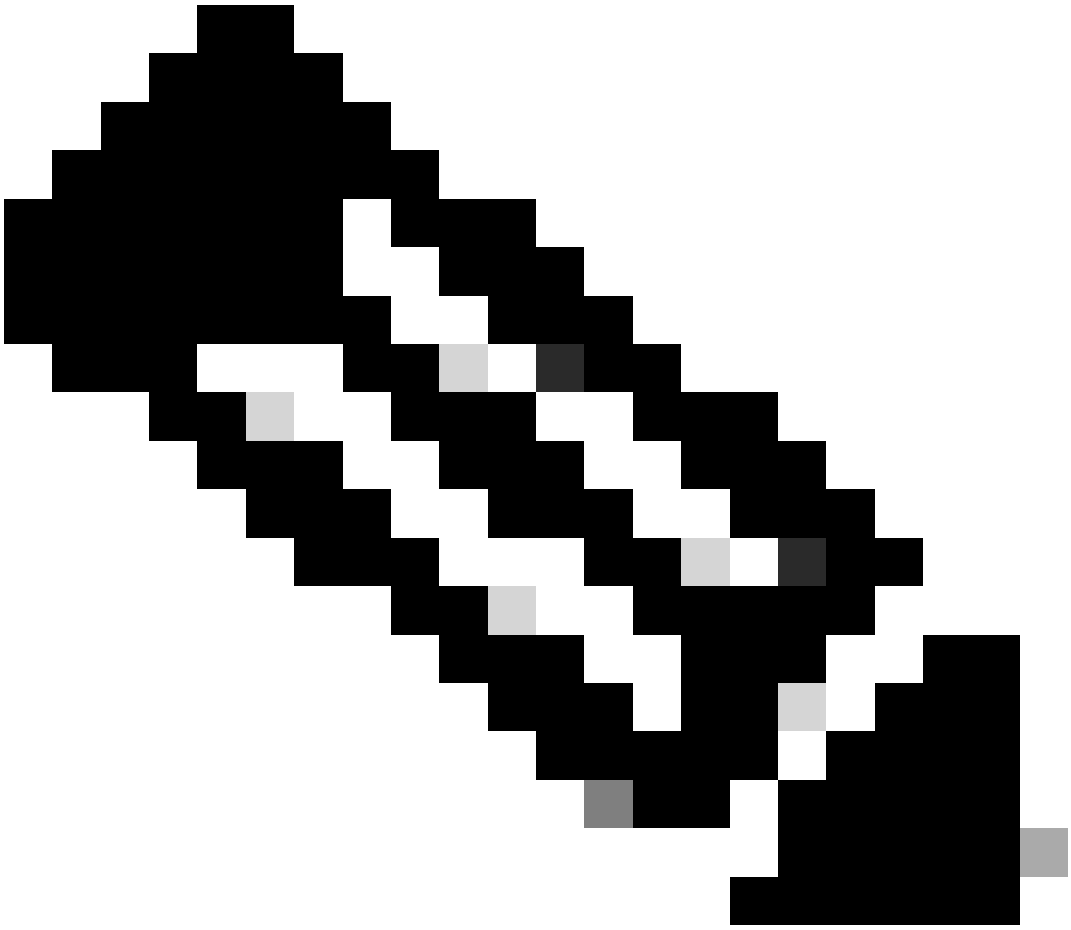
```
C:\>
C:\>procdump64.exe -u

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:\>_
```

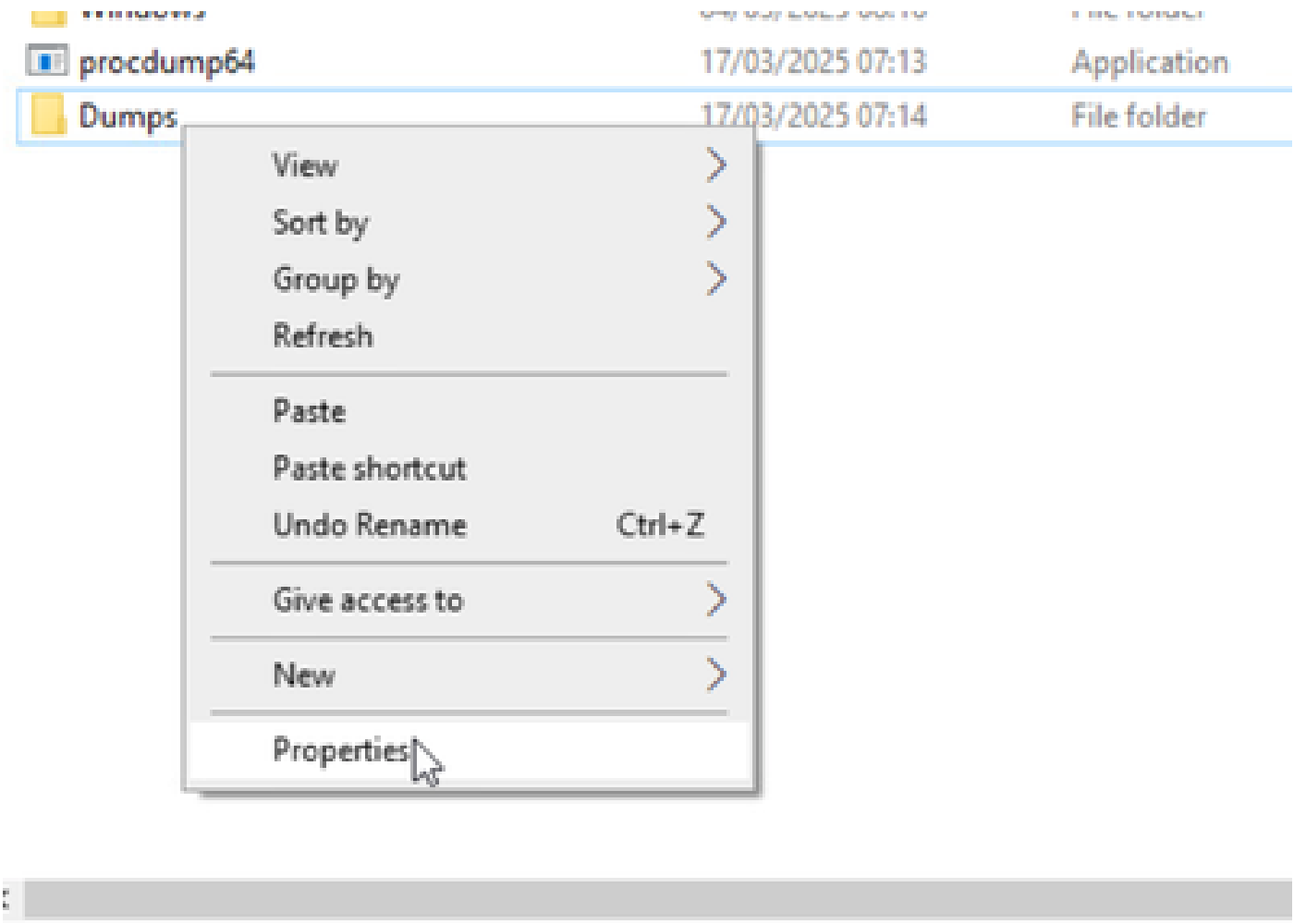


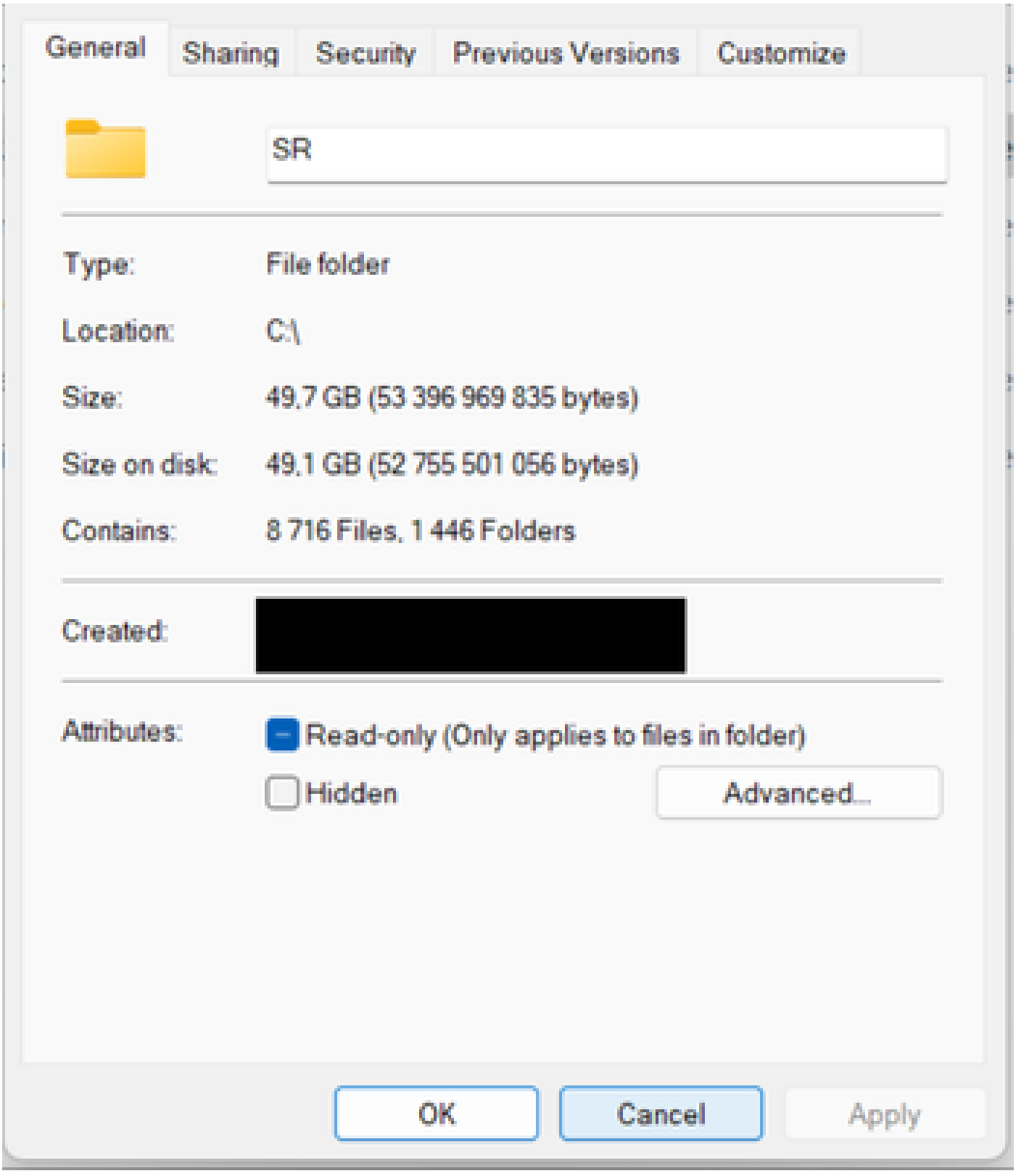
> Nota: I dump di arresto anomalo del sistema possono occupare molto spazio sul disco e al termine della raccolta è possibile arrestare procdump.

Sebbene sia possibile utilizzare la soluzione alternativa per comprimere le dimensioni della cartella:

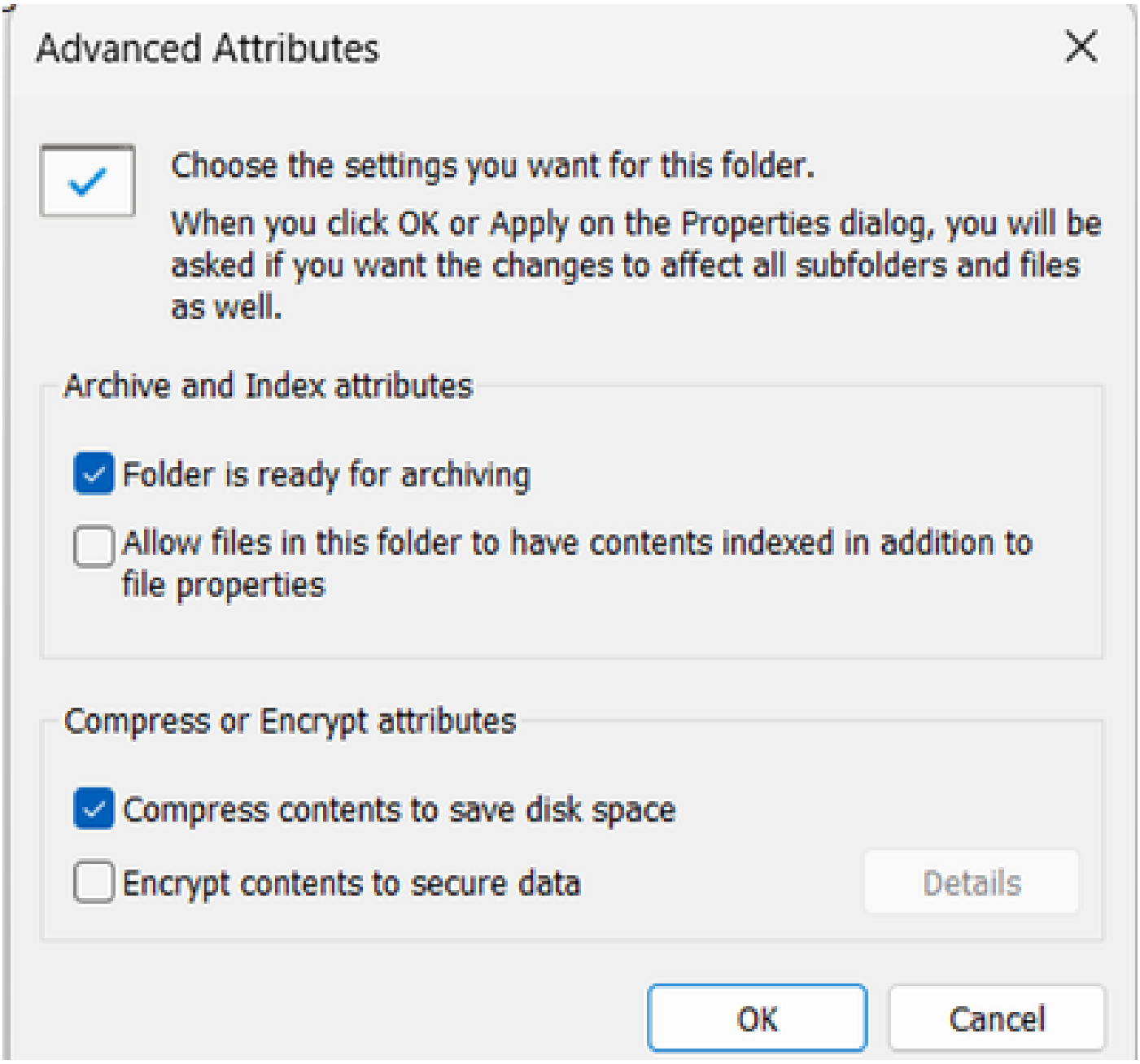
1- Passare alle proprietà della cartella Dump e controllare le dimensioni originali della cartella sul

disco come mostrato di seguito:

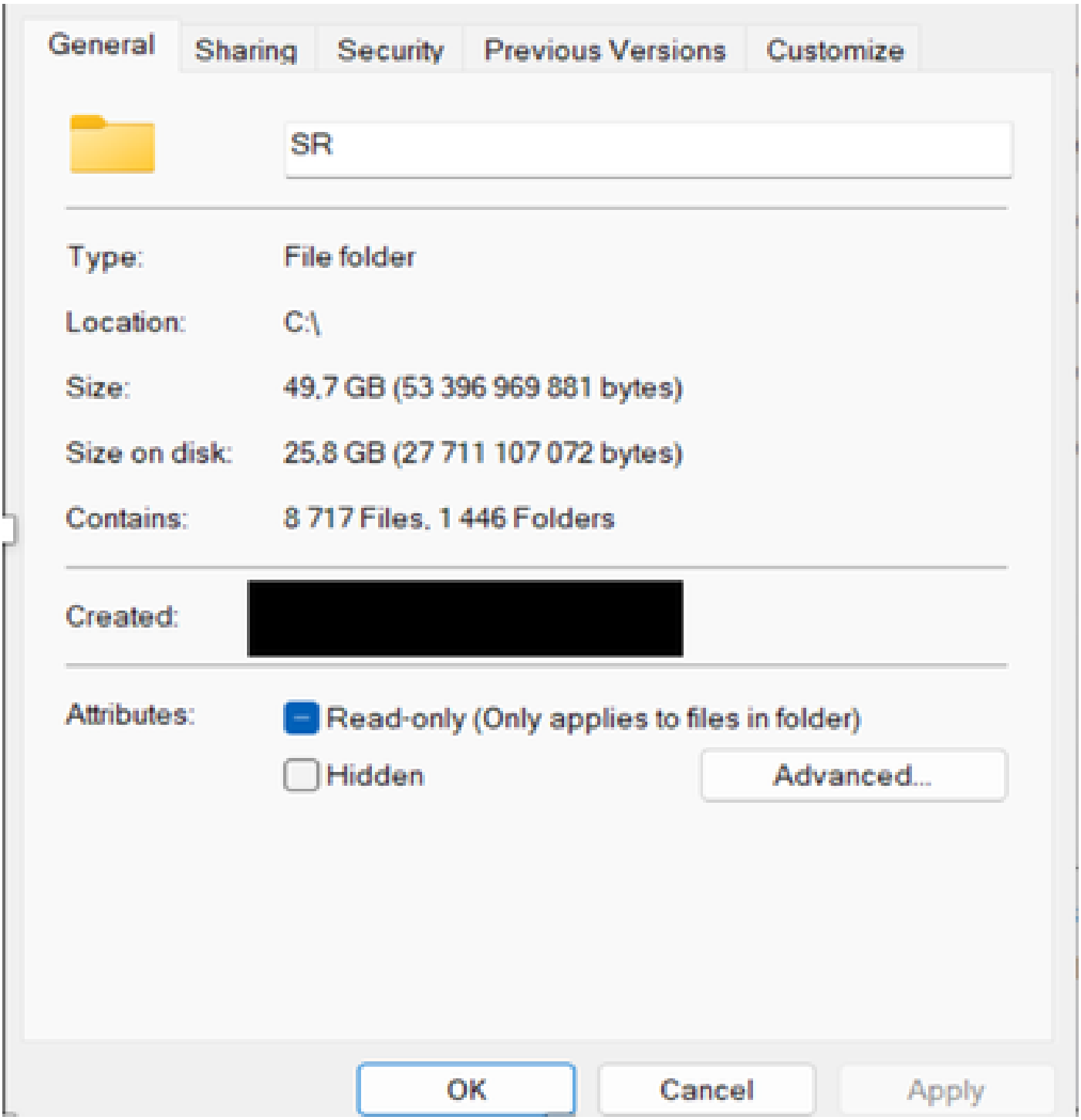




2- Passare all'opzione Advanced e abilitare la compressione e l'applicazione, operazione che richiede alcuni minuti:



3- Alla fine, è possibile vedere che le dimensioni della cartella si riducono a quasi la metà di quelle originali, come mostrato:



4- È possibile utilizzare questo comando anche al prompt dei comandi per ottenere lo stesso risultato:

compact /c /s:c:\installa

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).