Collecter les Crashdumps de processus sous Windows pour le processus Sfc

Table des matières

Introduction

Ce document décrit comment collecter les crashdumps de processus sur Windows pour le processus sfc.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connecteur Cisco Secure Endpoint
- Fenêtres Invite de commandes

Composants utilisés

Ce document n'est pas limité aux versions logicielles et matérielles. The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

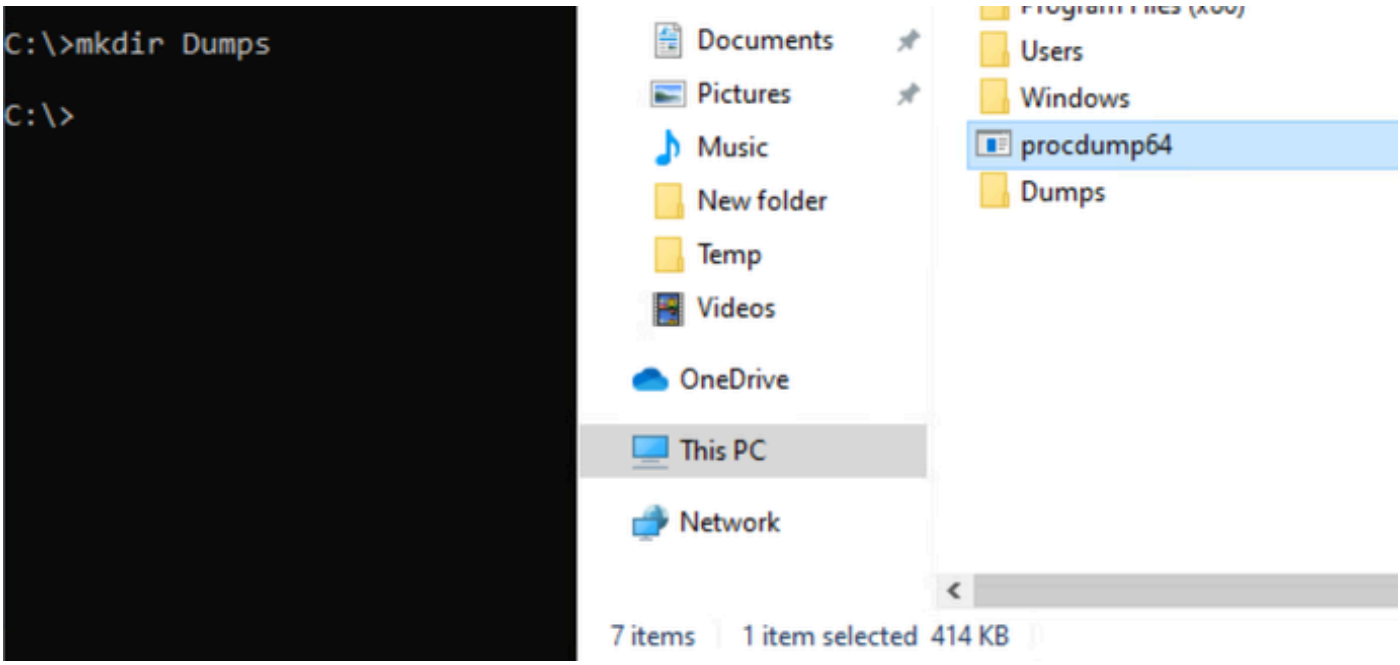
Problème

- L'application Cisco Secure Endpoint peut passer à l'état désactivé ou déconnecté en raison d'une panne du processus de sfc.exe, qui peut être liée à un arrêt inattendu de Windows ou à toute autre activité sur Windows.
- Windows active un outil de débogage configuré dans les valeurs de Registre AeDebug. N'importe quel programme peut être sélectionné à l'avance comme outil à utiliser dans cette situation. Le programme choisi est appelé débogueur post-mortem.

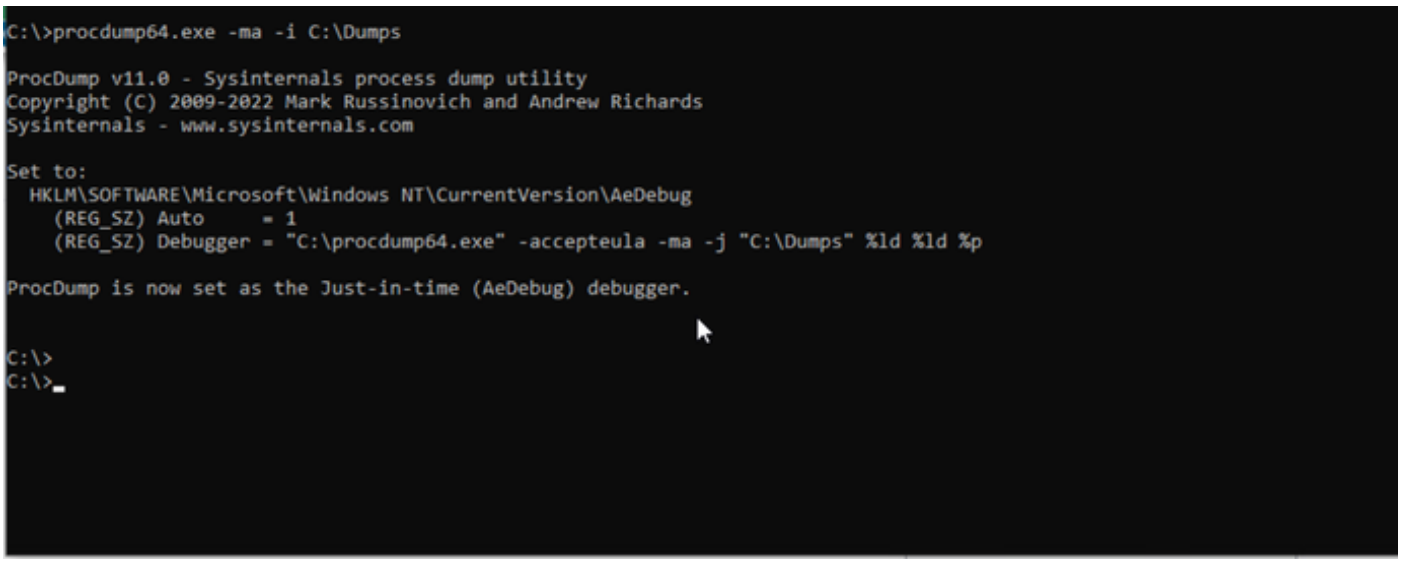
Solution

Téléchargez [Procdump en tant que débogueur post-mortem (AeDebug)] depuis la suite sysinternals.

Extrayez Procdump dans le lecteur c et créez le dossier Dumps pour la collection crashdump comme indiqué :



Définir Procdump comme AeDebugger :



Marche à suivre:

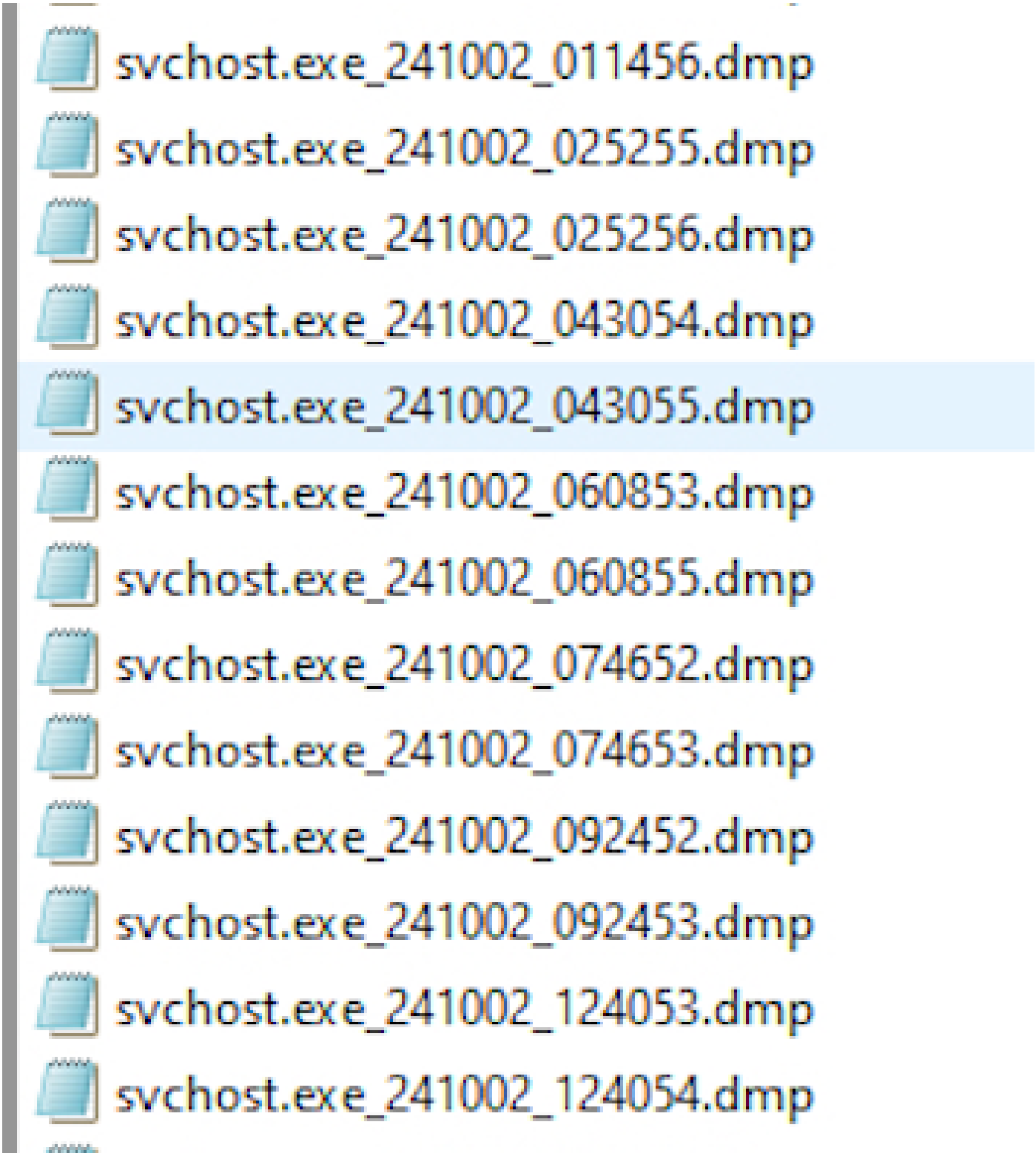
- Lancez CMD en tant qu'administrateur.

- Accédez au répertoire dans lequel vous avez décompressé l'outil procdump.
- Exemple de commande : procdump64.exe -ma <PID | Nom du processus> ou procdump64.exe -ma -i C:\Dumps

Exemple pour sfc.exe :

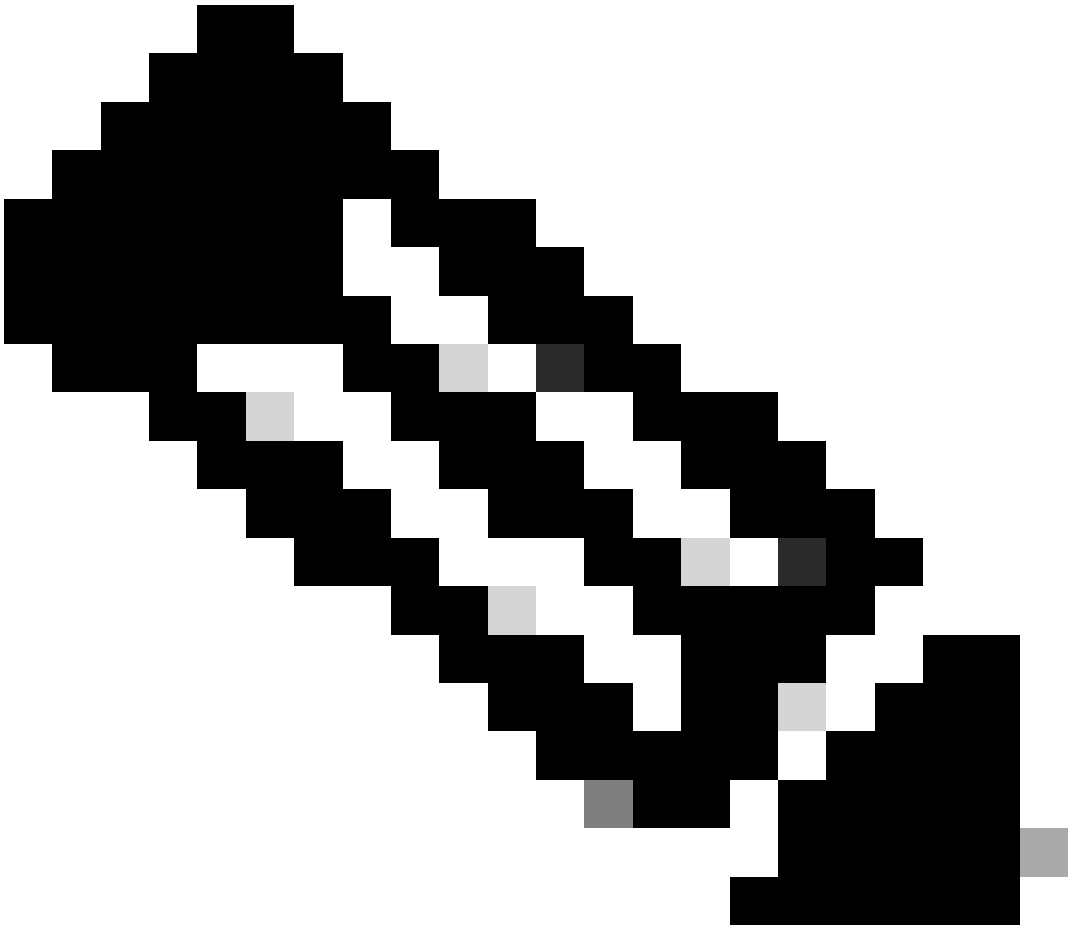
procdump64.exe -accepteula -ma -e -x c:\install %ProgramFiles%\Cisco\AMP\8.2.3.30119\sfc.exe

Il enregistre les dumps dans le dossier Dumps comme indiqué. Collectez et partagez-le pour analyse :



Pour désinstaller procdump, utilisez : procdump64.exe -u

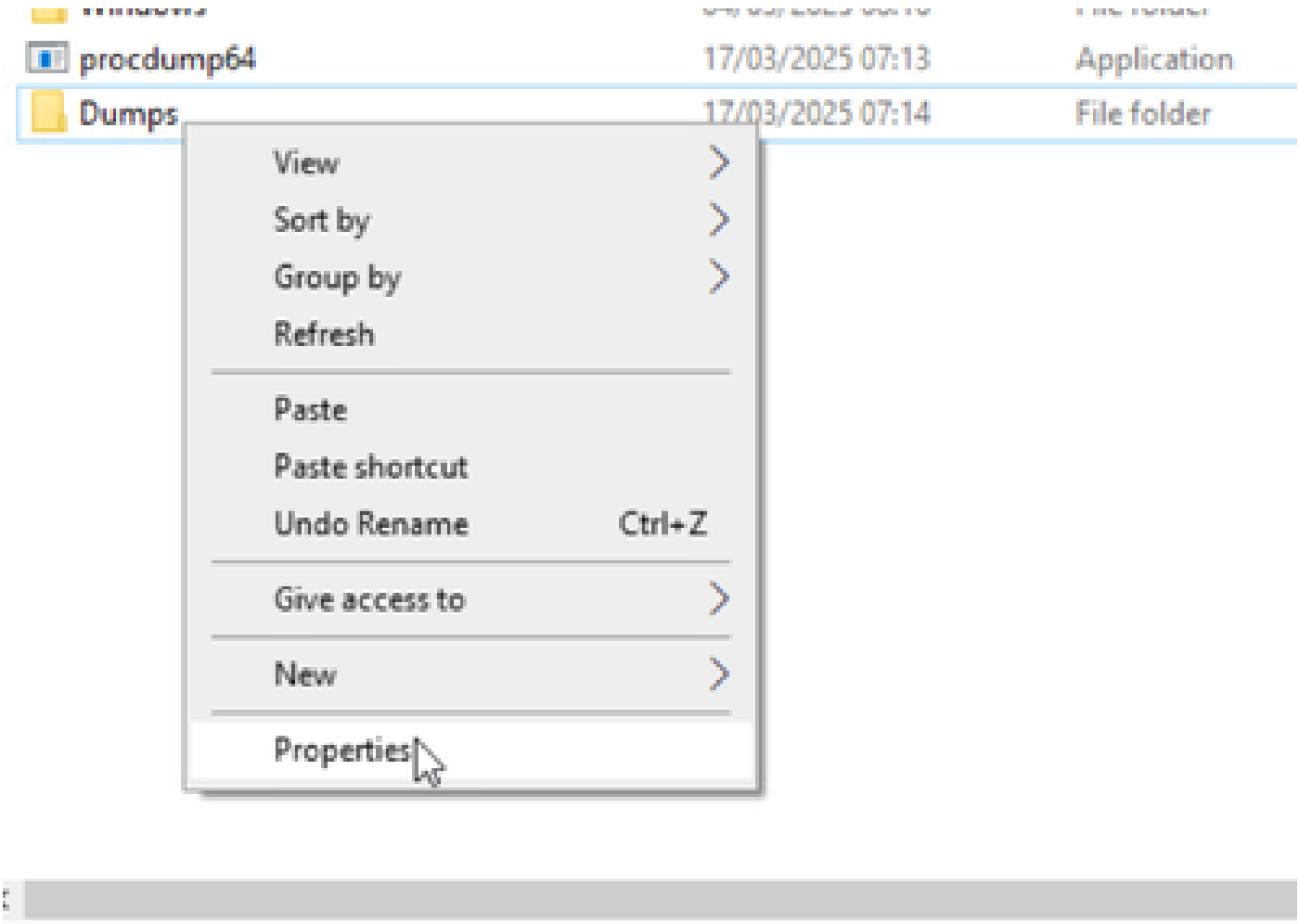
```
C:\>
C:\>procdump64.exe -u

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:\>_
```

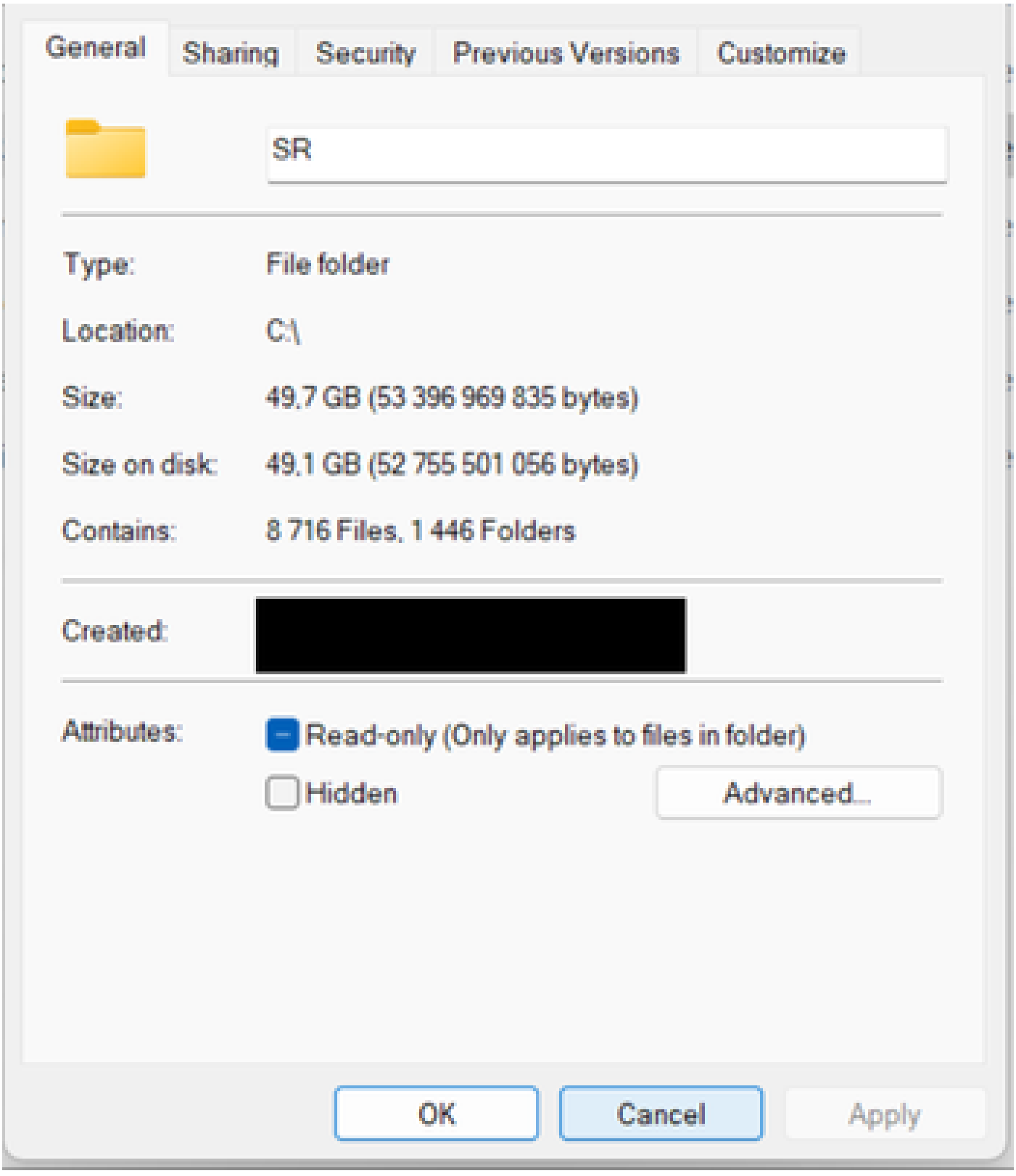


Remarque : Les vidages en cas de panne peuvent consommer un espace important sur le disque et procdump peut être arrêté une fois la collecte terminée.

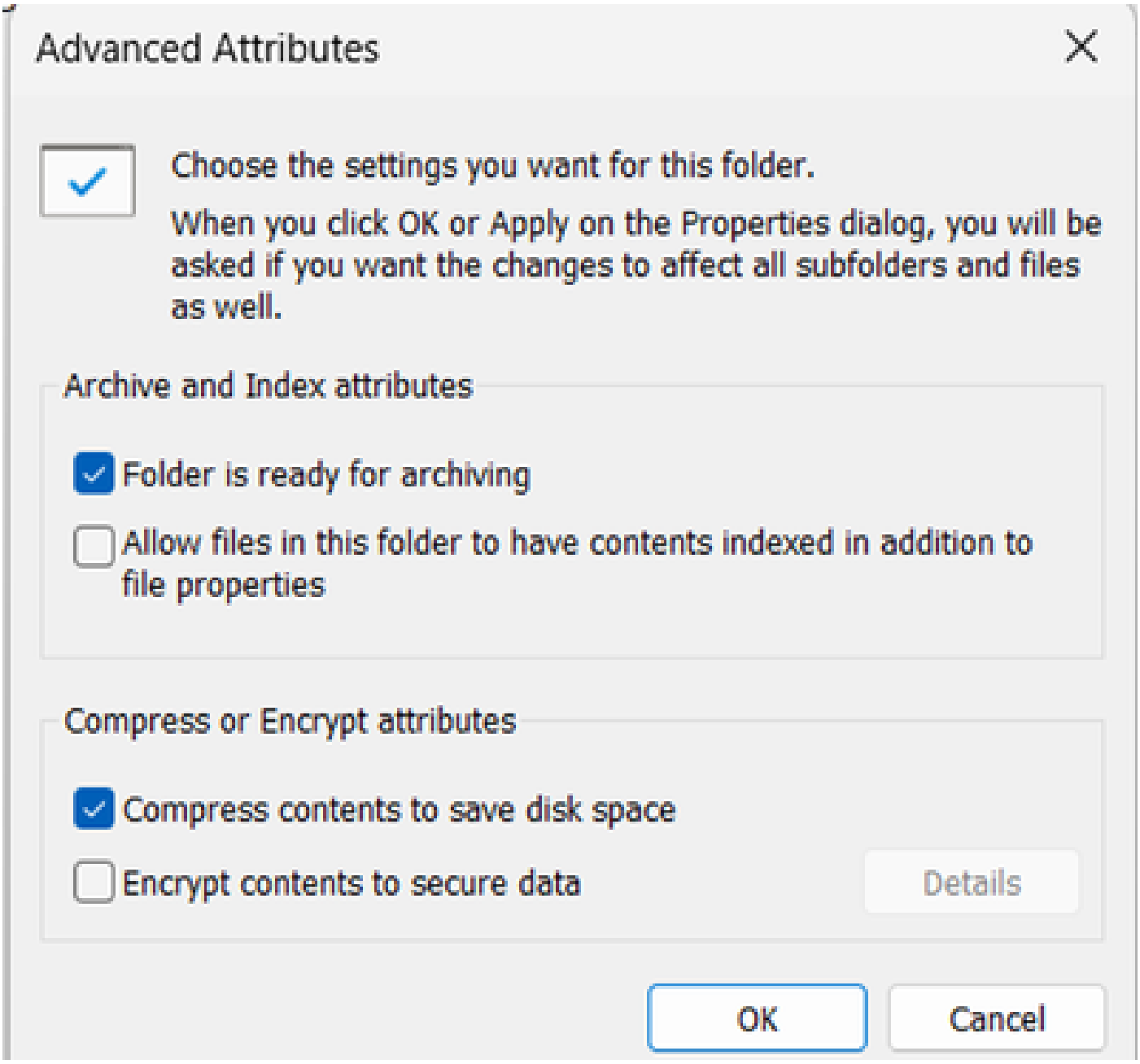
Bien que, vous pouvez également utiliser la solution de contournement pour compresser la taille du dossier :

1- Accédez aux propriétés du dossier Dumps et vérifiez la taille d'origine du dossier sur le disque comme indiqué :

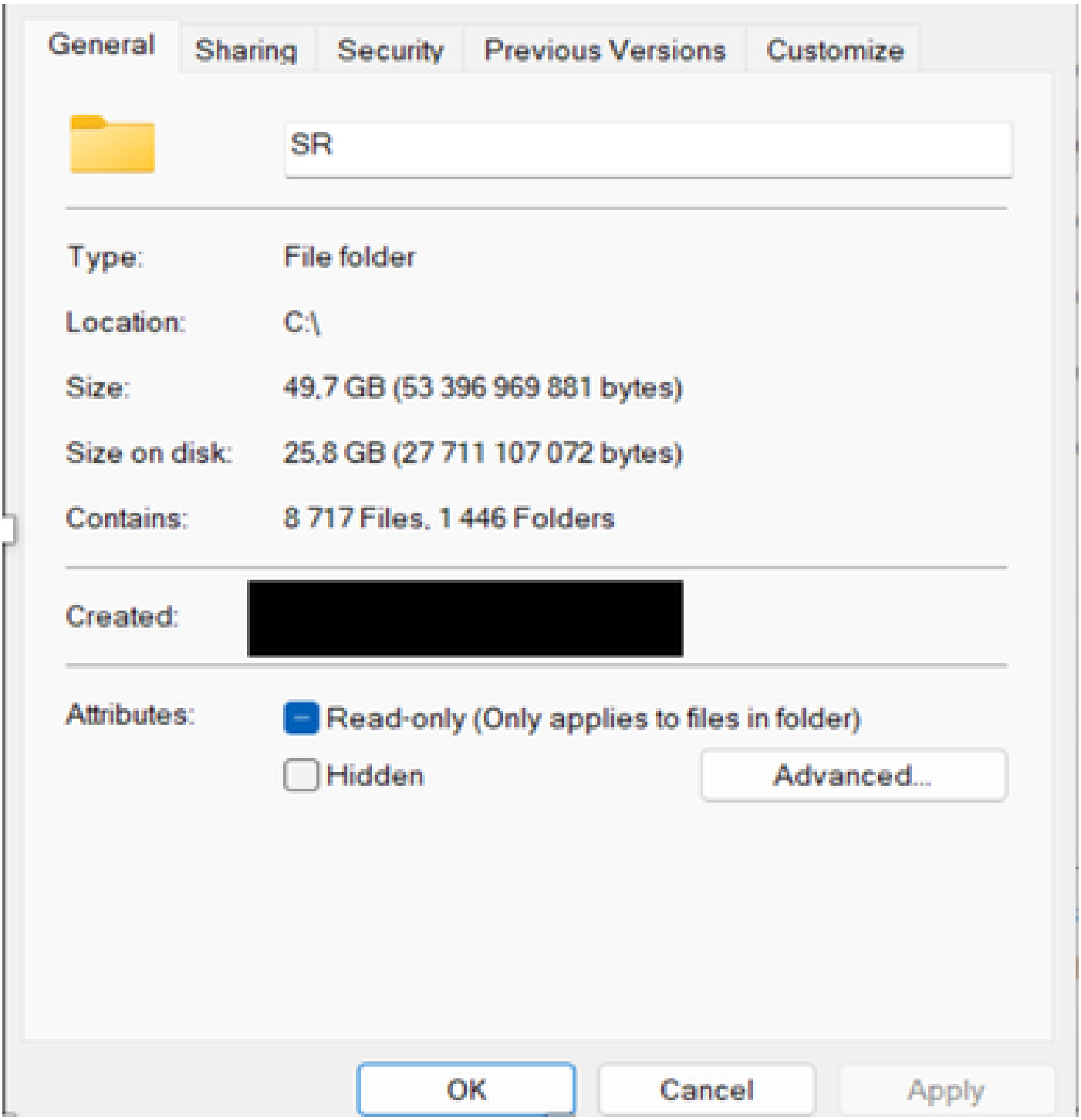




2- Accédez à l'option Advanced et activez la compression et appliquez ce qui prend plusieurs minutes :



3- À la fin, vous pouvez voir la taille du dossier réduit à près de la moitié de la taille d'origine comme indiqué :



4- Vous pouvez également utiliser cette commande sur l'invite de commande pour obtenir le même :

compact /c /s:c:\install

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.