Configurer la collecte de vidage sur incident du processus pour sfc.exe sous Windows

Table des matières

- Introduction
- Conditions préalables
- Problème
  - Télécharger et préparer l'environnement
  - Collecte automatique
  - Désinstaller le débogueur automatique
  - Collecte manuelle
- Compression du dossier de vidage sur incident
  - Utiliser CLI (Command Line Interface)
  - Utiliser l'interface utilisateur graphique

Introduction

Ce document décrit comment collecter des vidages sur incident sous Windows pour le processus sfc.exe.

Environnement

Plate-forme : Terminal Windows

Produit : Connecteur Cisco Secure Endpoint

Outils: Invite de commandes Windows ; Microsoft Sysinternals ProcDump (procdump64.exe)

Connaissances supposées :

- Connecteur Cisco Secure Endpoint
- Invite de commandes Windows

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. Examiner l’impact potentiel d’une commande avant de l’utiliser sur un réseau actif.

Motif

- Les pannes sfc.exe peuvent entraîner la désactivation ou la déconnexion de l'application Cisco Secure Endpoint.
- Windows peut appeler un débogueur post-mortem configuré via les valeurs de registre AeDebug ; ProcDump peut être enregistré en tant que débogueur pour capturer les vidages de panne.

Problème

- Cisco Secure Endpoint peut passer à l'état désactivé ou déconnecté si sfc.exe tombe en panne. Cela peut se produire après un arrêt inattendu de Windows ou une autre activité Windows.
- Windows active un outil de débogage configuré dans les valeurs de registre AeDebug (Application Error Debug). Dans ce scénario, un programme peut être présélectionné en tant qu'outil à utiliser, appelé débogueur post-mortem.

Résolution

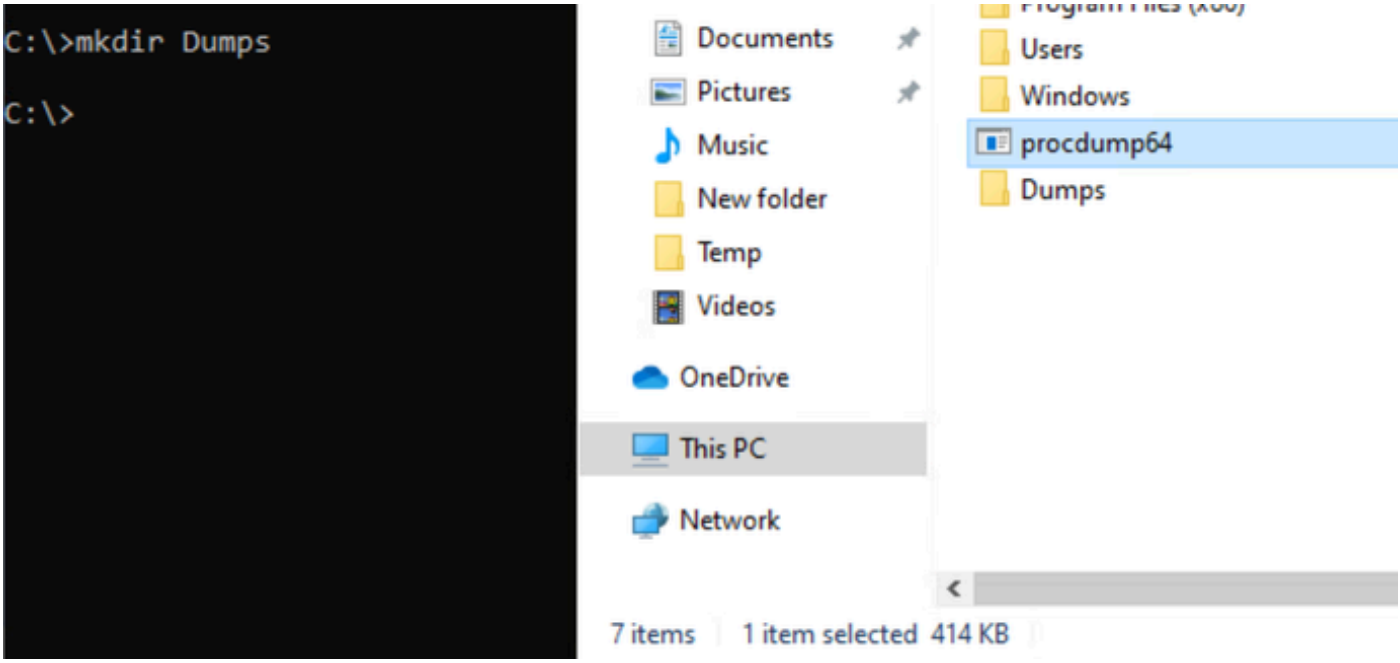
Avant de commencer

1. Confirmez l'accès administratif sur le terminal Windows.
2. Vérifiez que C:\Dumps existe (ou peut être créé) et que le compte exécutant ProcDump a un accès en écriture au dossier.
3. Décidez si la collecte automatique (enregistrement du débogueur post mortem) ou manuelle (vidage à la demande) est requise.

Télécharger et préparer l'environnement

1. Téléchargez Procdump (à utiliser comme débogueur post-mortem AeDebug) à partir de Sysinternals Suite.

2. Extrayez procdump64.exe vers le lecteur C : et créer le dossier Dumps pour la collecte de vidage sur incident.

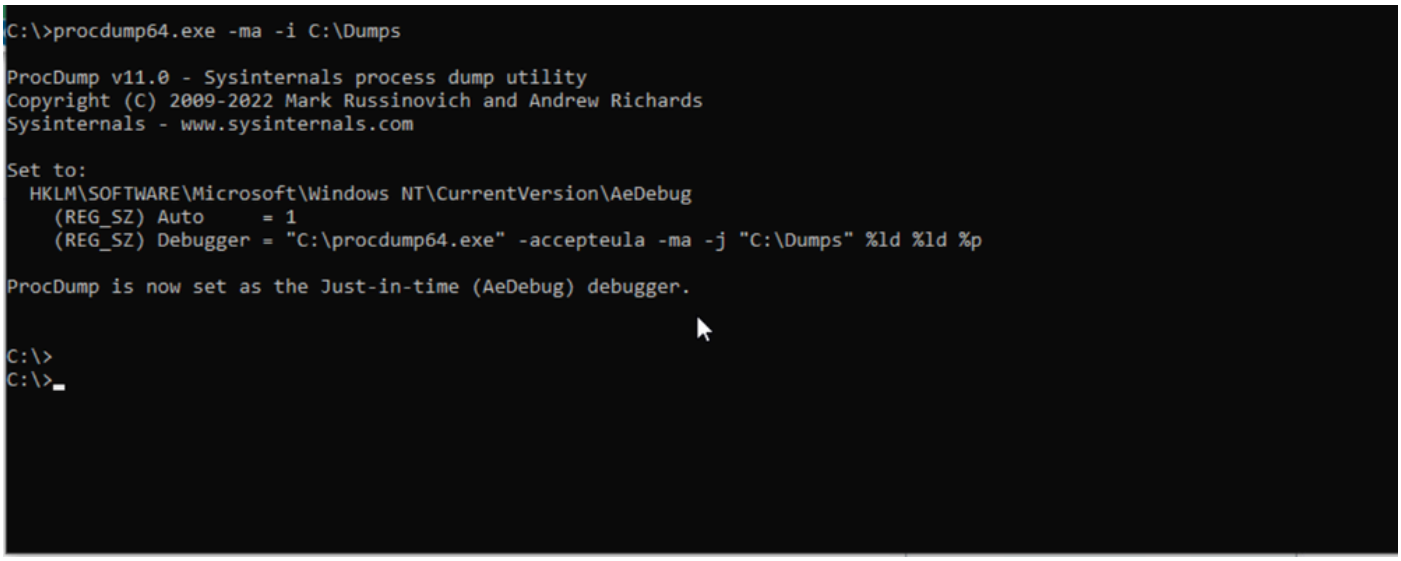


Remarque : ProcDump (procdump64.exe) prend en charge deux méthodes de collecte de vidage : collecte automatique (enregistrez ProcDump comme débogueur post-mortem et spécifiez un dossier de sortie) et collecte manuelle (déclenchez une vidange pour un ID ou un nom de processus spécifique).

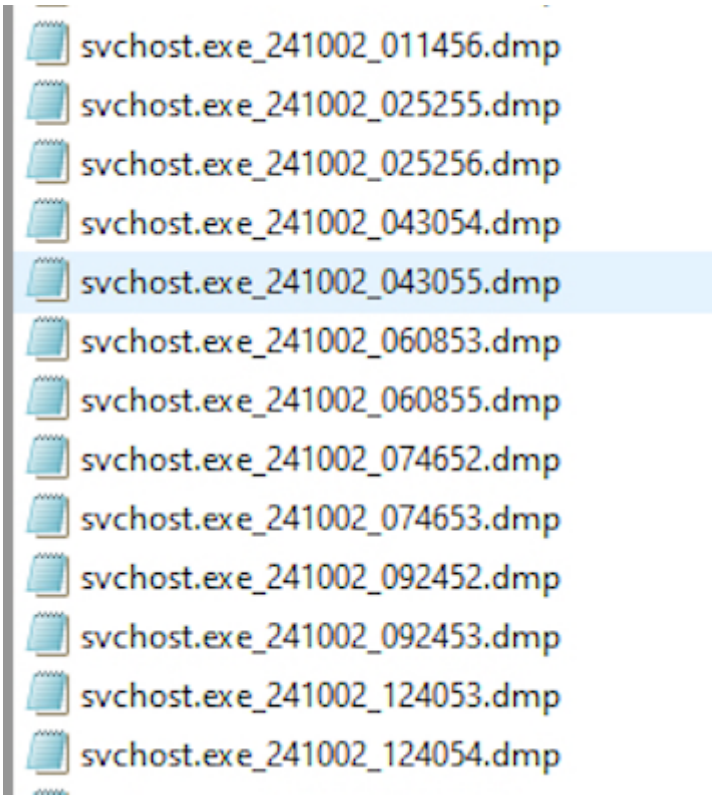
Collecte automatique

1. Définissez procdump64.exe comme débogueur automatique dans la configuration du Registre de débogage post-mortem Windows (AeDebug) avec cette commande. Lorsqu'un programme tombe en panne, ProcDump enregistre le vidage sur incident dans le dossier spécifié.

```
procdump64.exe -ma -i C:\Dumps
```



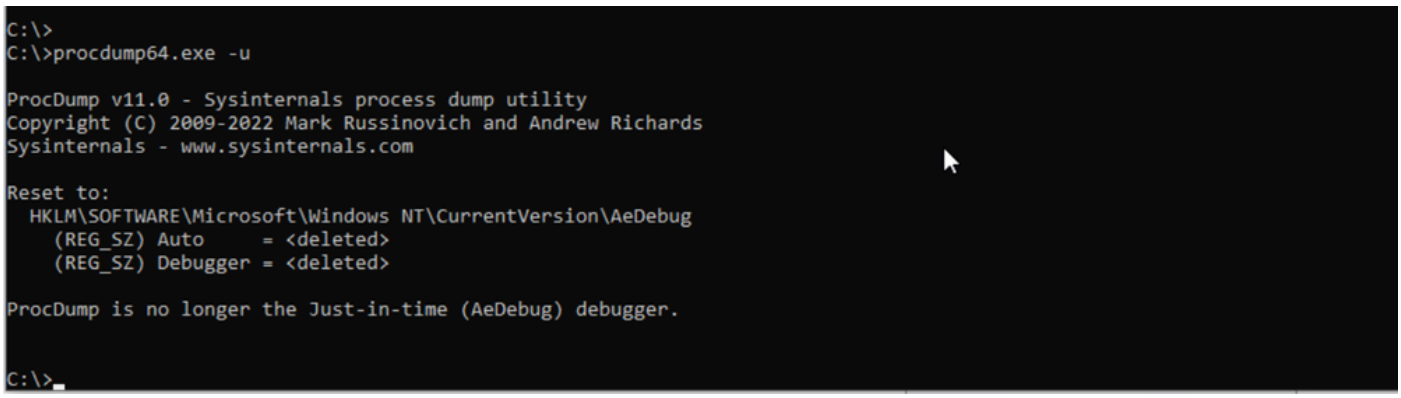
2. Accédez au dossier C:\Dumps. Compressez-le et partagez-le pour analyse.



Désinstaller le débogueur automatique

1. Pour désinstaller procdump64.exe, utilisez cette commande.

```
procdump64.exe -u
```



Collecte manuelle

1. Utilisez cette commande pour créer un vidage à la demande.

```
procdump64.exe -accepteula -ma -e -x c:\Dumps <PID | Process Name>
```

Exemple pour sfc.exe.

```
procdump64.exe -accepteula -ma -e -x c:\Dumps "%ProgramFiles%\Cisco\AMP\8.6.1.30582\sfc.exe"
```

2. Accédez au dossier C:\Dumps. Compressez-le et partagez-le pour analyse.

Compression du dossier de vidage sur incident

Les vidages en cas de panne peuvent occuper une quantité importante d'espace disque. Il est donc important d'arrêter procdump une fois la collecte terminée. Vous pouvez également utiliser la solution de contournement pour compresser la taille du dossier.

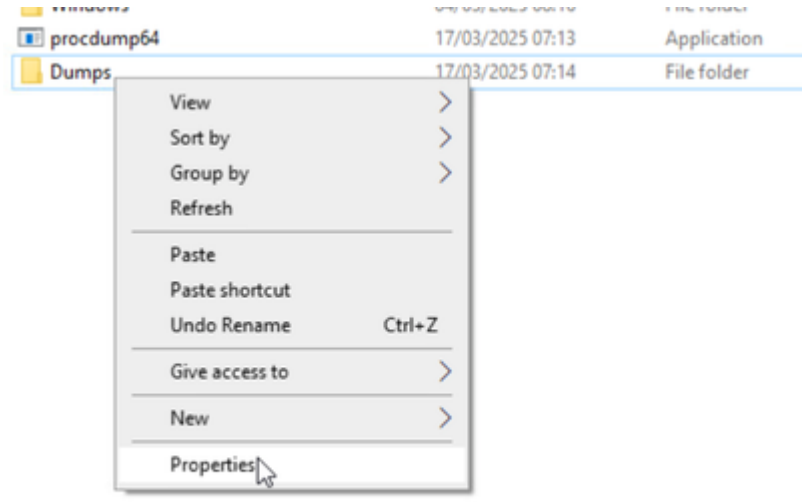
Utiliser CLI (Command Line Interface)

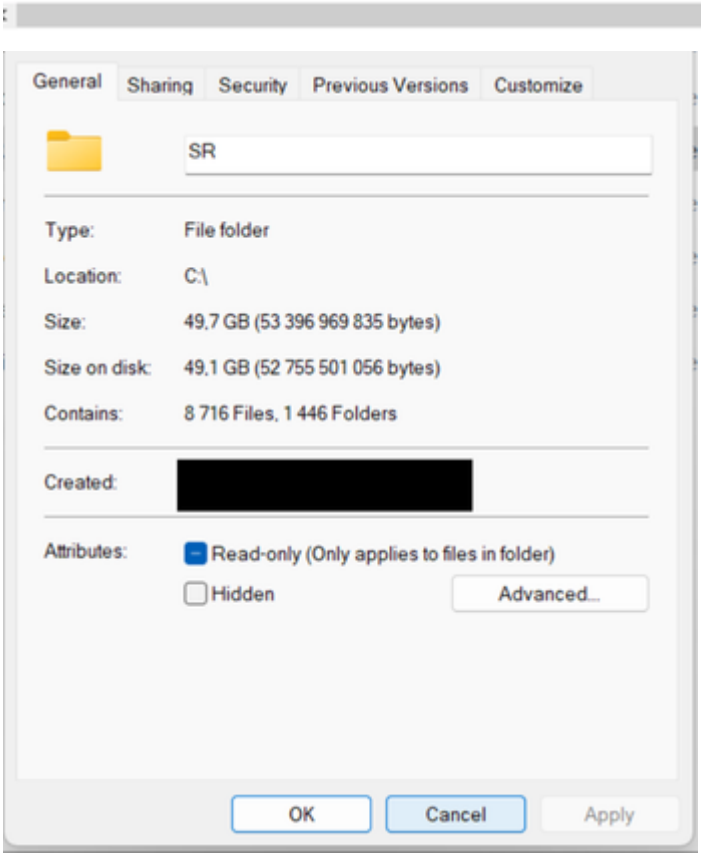
Utilisez cette commande dans l'invite de commandes pour activer la compression.

```
compact /c /s:c:\Dumps
```

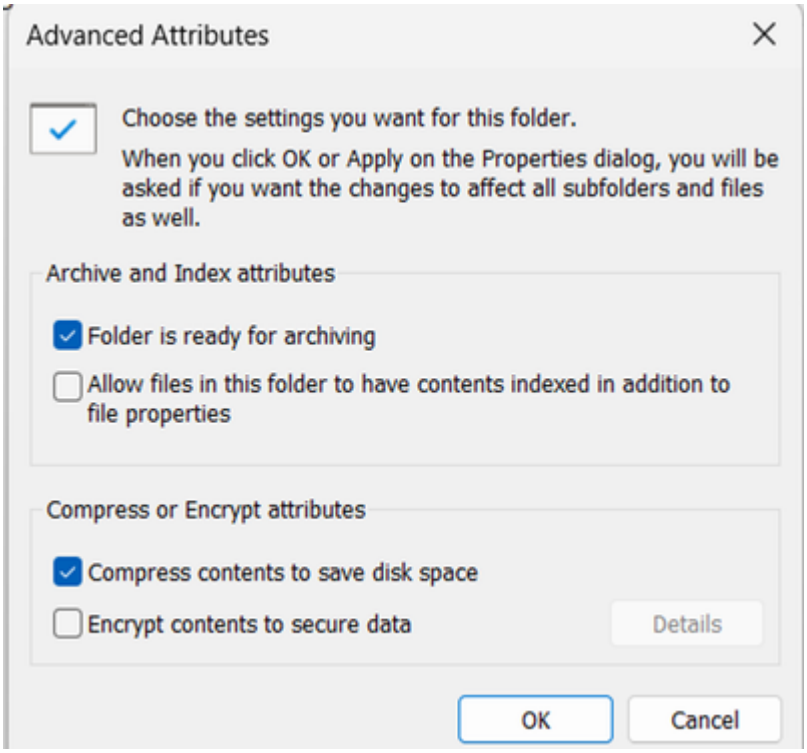
Utiliser l'interface utilisateur graphique

1. Accédez à Propriétés pour le dossier Dumps et vérifiez la taille d'origine du dossier sur le disque.

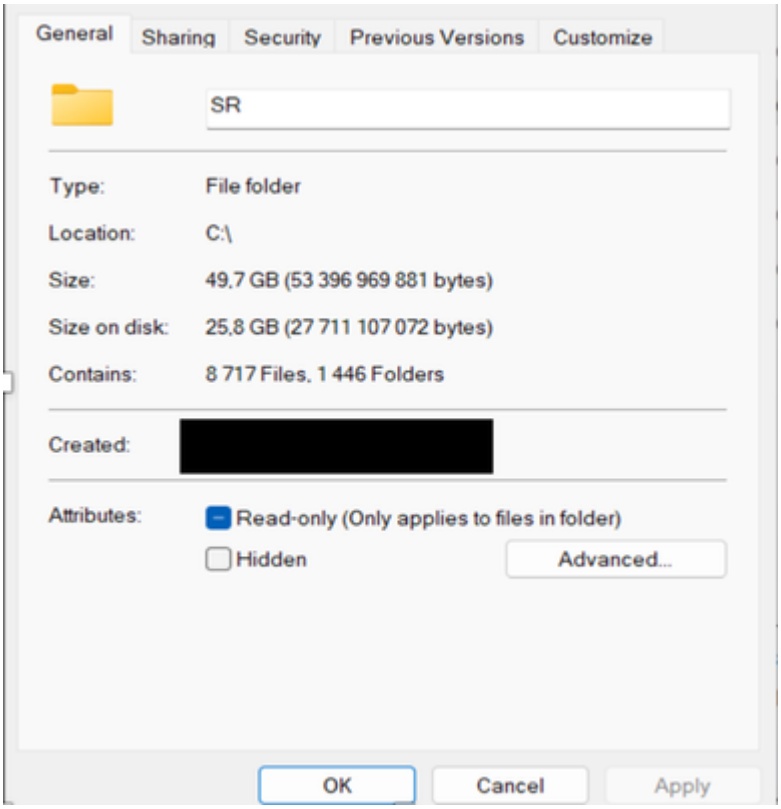




2. Dans Propriétés, cliquez sur Avancé, sélectionnez Compresser le contenu pour économiser de l'espace disque, puis cliquez sur OK pour appliquer la modification. Ce processus peut prendre plusieurs minutes.



3. En fin de compte, vous pouvez observer que la taille du dossier a considérablement réduit, atteignant presque la moitié de sa taille d'origine.



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.