为Windows上的sfc.exe配置进程崩溃转储集合

目录

简介

先决条件

问题

- 下载并准备环境
- 自动收集
- 卸载自动调试器
- 手动收集

崩溃转储文件夹压缩

- 使用CLI（命令行界面）
- 使用GUI（图形用户界面）

简介

本文档介绍如何为sfc.exe进程收集Windows上的故障转储。

环境

平台：Windows终结点

产品:思科安全终端连接器

工具:Windows命令提示符；Microsoft Sysinternals ProcDump(procdump64.exe)

假定知识:

- 思科安全终端连接器
- Windows命令提示符

本文档不限于软件和硬件版本。本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。在现用网络中使用任何命令之前，先检查其潜在影响。

原因

- sfc.exe崩溃可能会使思科安全终端应用程序处于禁用或断开连接状态。
- Windows可以调用通过AeDebug注册表值配置的事后调试器；可以将ProcDump注册为调试器，以捕获崩溃转储。

问题

- 如果sfc.exe崩溃，思科安全终端可以进入禁用或断开连接状态。出现意外的Windows关闭或其他Windows活动后可能会出现这种情况。
- Windows激活在AeDebug(Application Error Debug)注册表值中配置的调试工具。在此场景中，可以预先选择一个程序作为要使用的工具，这称为死后调试程序。

分辨率

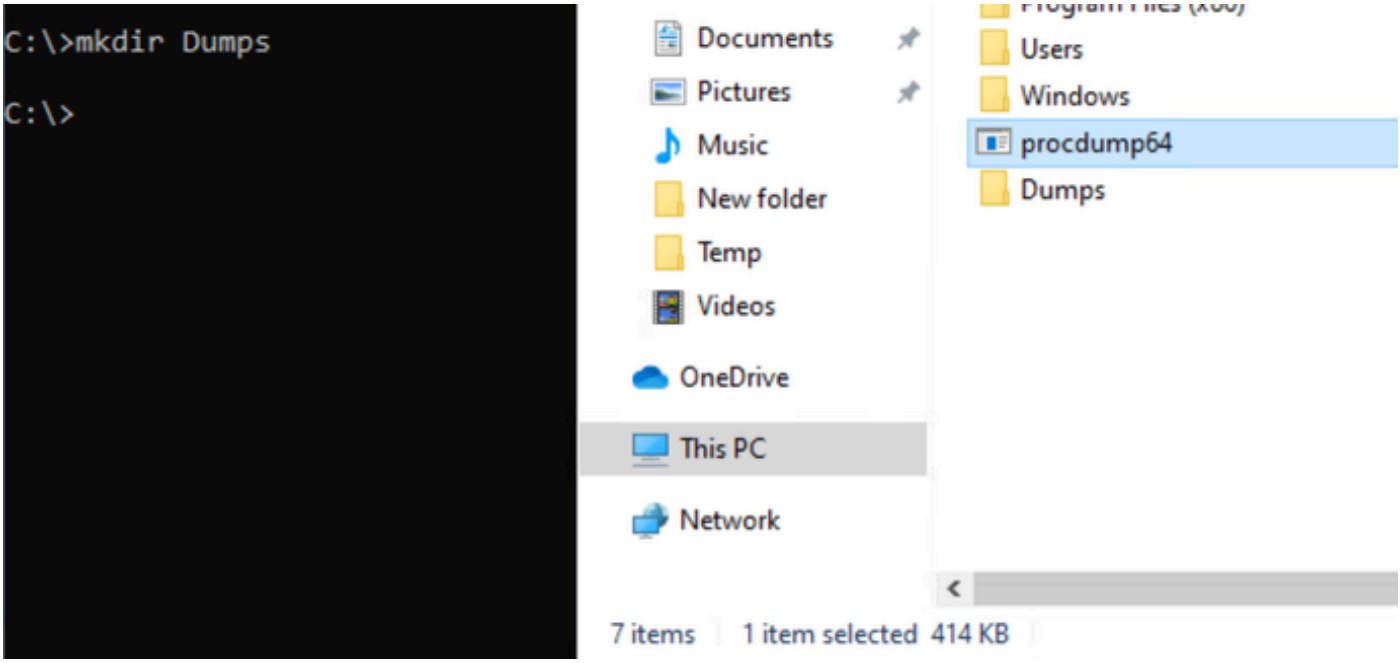
开始使用前

1. 确认对Windows终结点的管理访问。
2. 确认C:\Dumps存在（或可以创建），并且运行ProcDump的帐户具有对文件夹的写访问权限。
3. 确定是需要自动收集（事后调试器注册）还是手动收集（按需转储）。

下载并准备环境

1.从Sysinternals Suite下载Procdump（将用作AeDebug事后调试器）。

2.将procdump64.exe解压缩到C:驱动器并创建Dumps文件夹以进行故障转储收集。

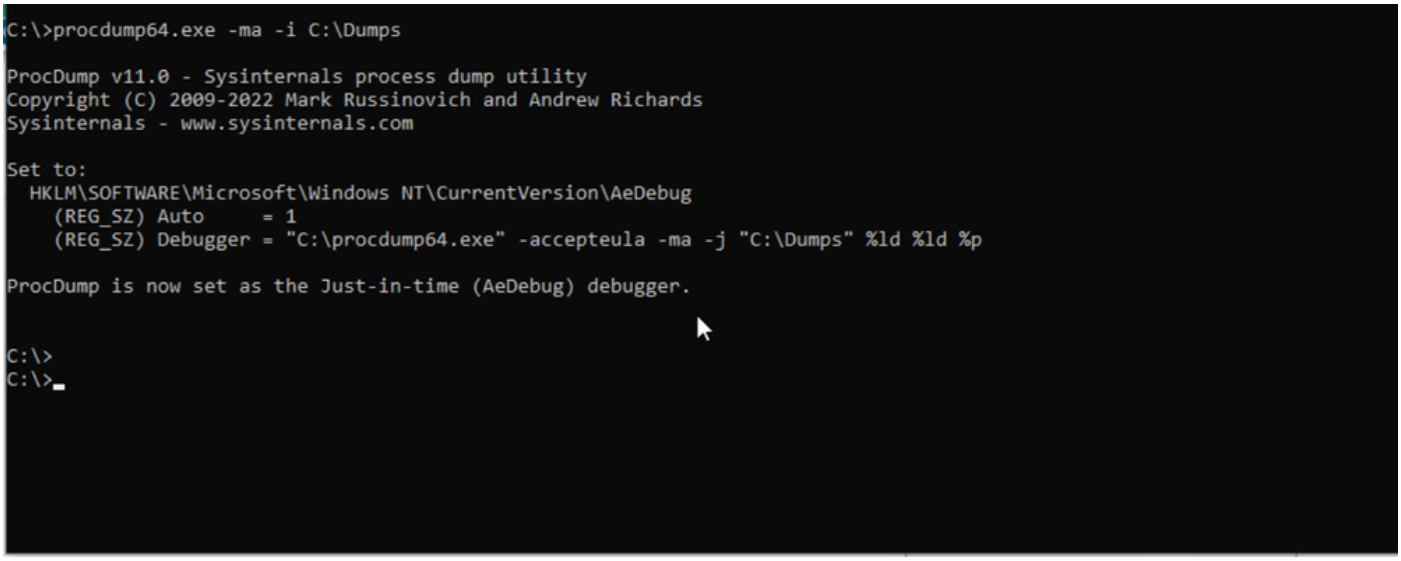


注意：ProcDump(procdump64.exe)支持两种转储收集方法：自动收集（将ProcDump注册为事后调试器并指定输出文件夹）和手动收集（为特定进程ID或进程名称触发转储）。

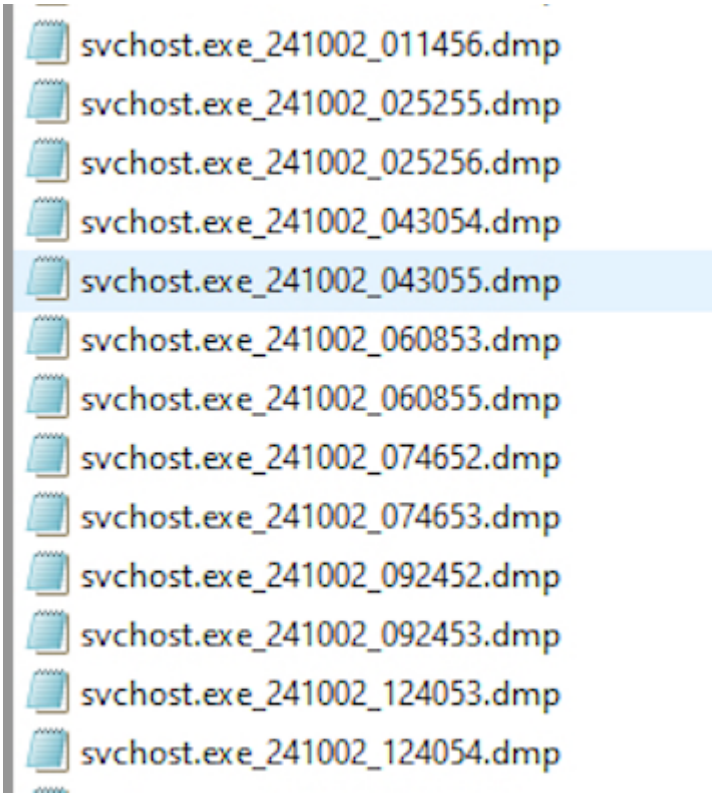
自动收集

1.使用此命令将procdump64.exe设置为Windows事后调试注册表配置(AeDebug)中的自动调试器。当程序崩溃时，ProcDump会将崩溃转储保存在指定的文件夹中。

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



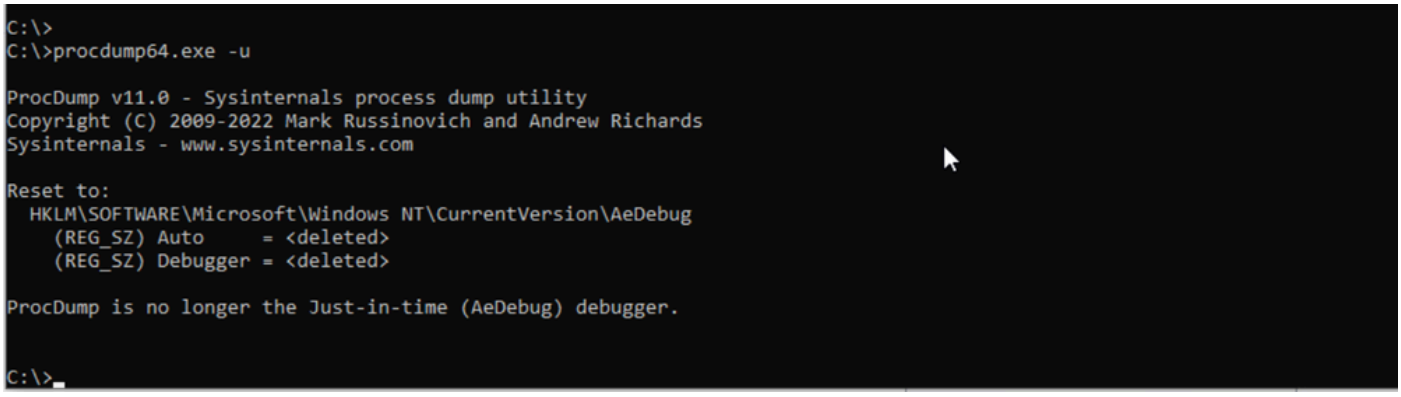
2.导航到C:\Dumps文件夹。压缩并共享以供分析。



卸载自动调试器

1.要卸载procdump64.exe，请使用此命令。

```
procdump64.exe -u
```



手动收集

1.使用此命令可按需创建转储。

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

sfc.exe的示例。

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

2.导航到C:\Dumps文件夹。压缩并共享以供分析。

崩溃转储文件夹压缩

故障转储可能会占用大量磁盘空间，因此收集完成后必须停止转储。还可以使用替代方法压缩文件夹的大小。

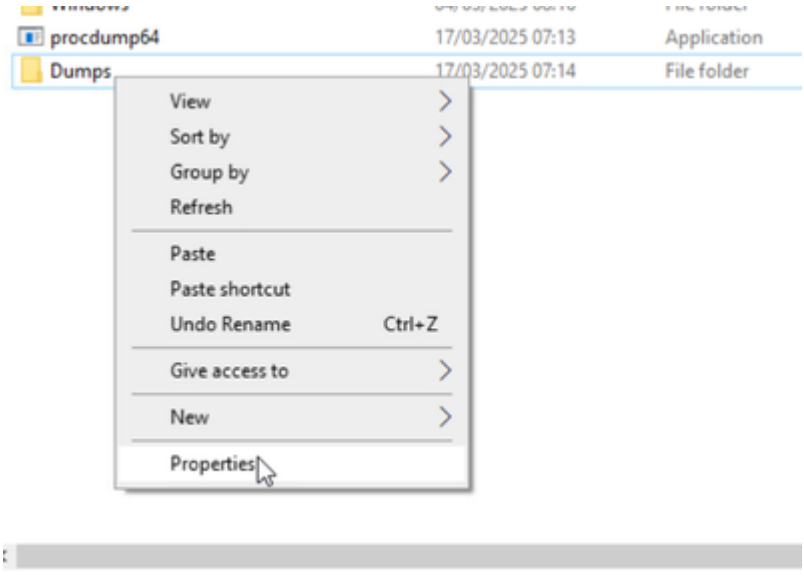
使用CLI（命令行界面）

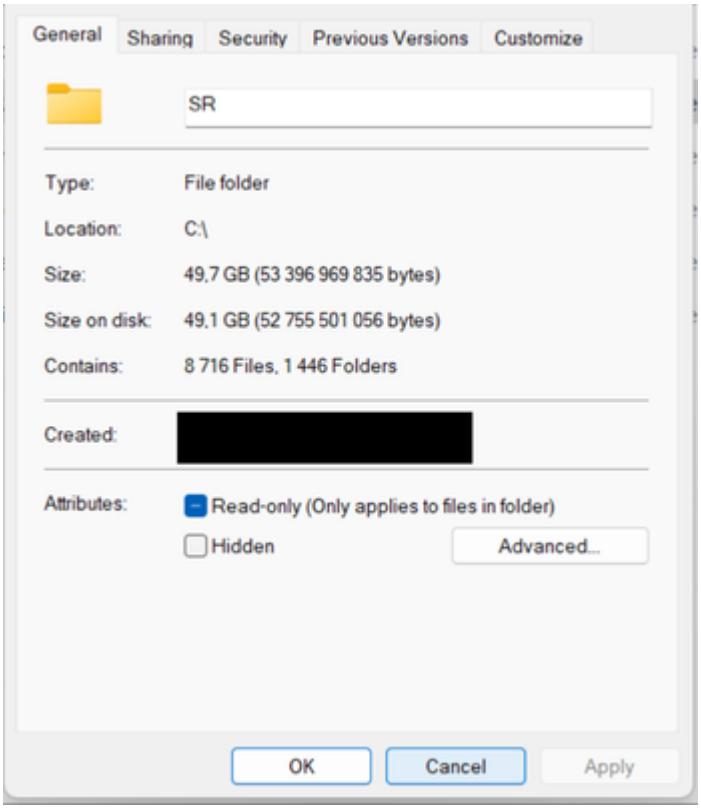
在命令提示符下使用此命令可启用压缩。

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

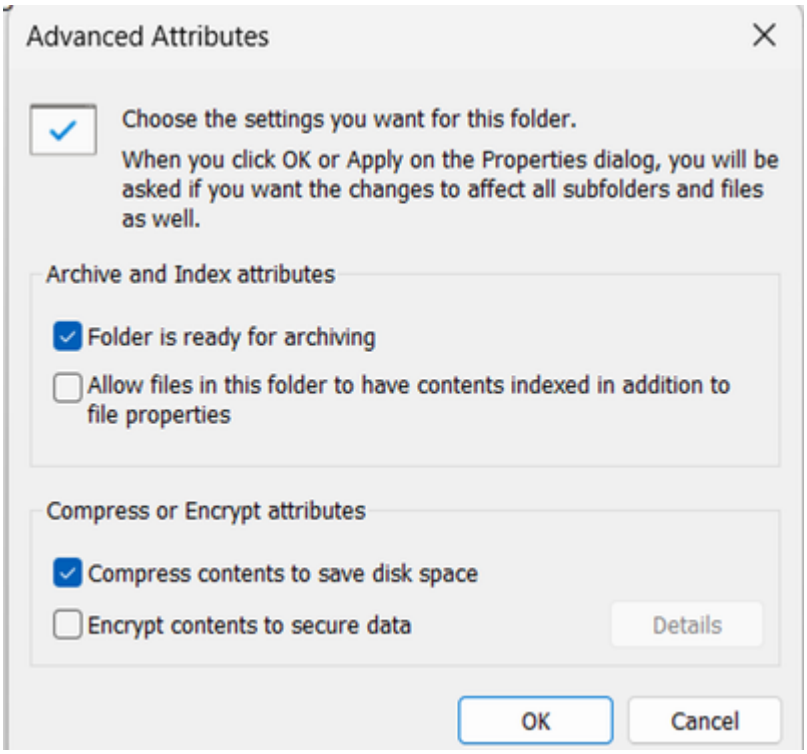
使用GUI（图形用户界面）

1.定位至转储文件夹的属性，然后检查磁盘上文件夹的原始大小。

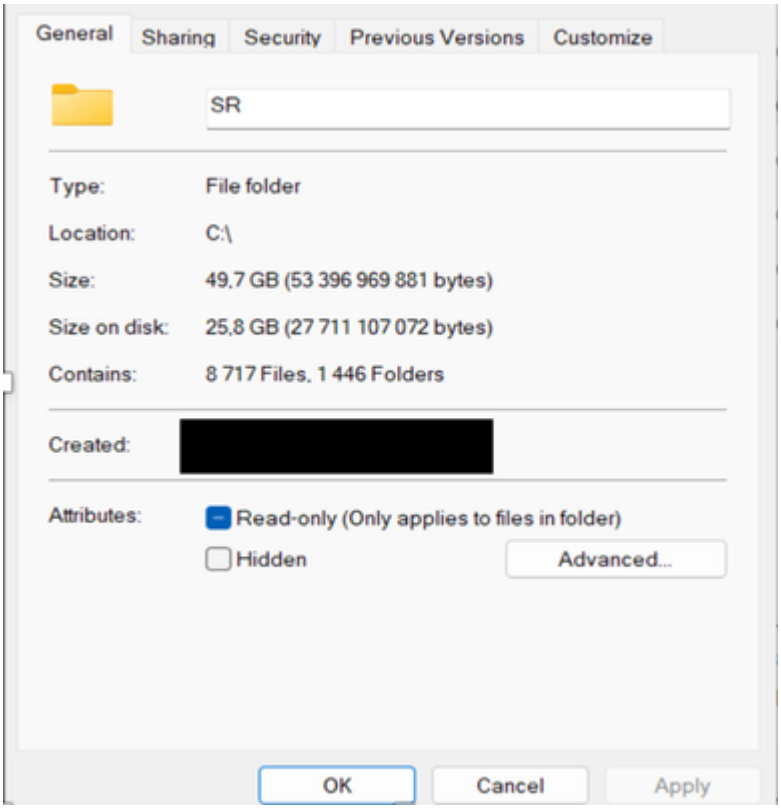




2.在属性中，单击高级，选择压缩内容以节省磁盘空间，然后单击确定以应用更改。此过程可能需要几分钟。



3.最后，您可以看到文件夹大小已显着减小，几乎达到其原始大小的一半。


General
Sharing
Security
Previous Versions
Customize
SR
Type:
File folder
Location:
C:\
Size:
49,7 GB (53 396 969 881 bytes)
Size on disk:
25,8 GB (27 711 107 072 bytes)
Contains:
8 717 Files, 1 446 Folders
Created:
Attributes:
Read-only (Only applies to files in folder)
Hidden
Advanced...
OK
Cancel
Apply

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。