Monitor what killed diawp.exe in Windows

Last updated by | Veena Pachauri | Mar 8, 2023 at 11:10 PM PST

Contents

- TSG Contact
- About Gflags
- Known limitation
- Configure Windows process exit monitoring
- Enable dump collection
- Remove Windows process exit monitoring

TSG Contact

davizen

About Gflags

https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/gflags

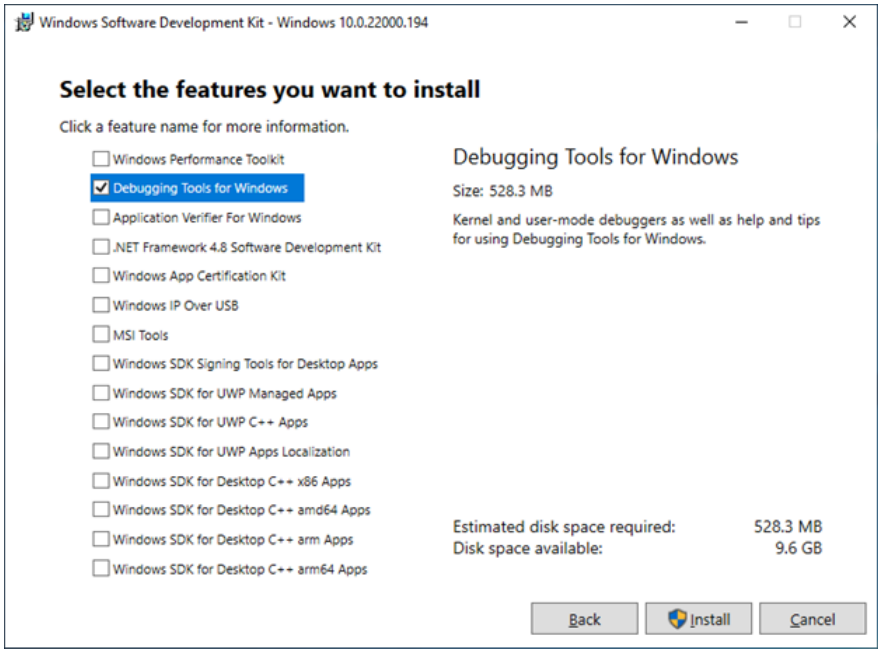
Known limitation

The monitoring feature does not detect normal process termination that happens when the last thread of the process exits. The monitoring feature does not detect process termination that is initiated by kernel-mode code.

Configure Windows process exit monitoring

1. Download the Windows SDK from https://developer.microsoft.com/en-us/windows/downloads/windows-sdk/

2. Install below features:



Windows Software Development Kit - Windows 10.0.22000.194

Select the features you want to install

Click a feature name for more information.

- □ Windows Performance Toolkit
- ☑ Debugging Tools for Windows
- □ Application Verifier For Windows
- □ .NET Framework 4.8 Software Development Kit
- □ Windows App Certification Kit
- □ Windows IP Over USB
- □ MSI Tools
- □ Windows SDK Signing Tools for Desktop Apps
- □ Windows SDK for UWP Managed Apps
- □ Windows SDK for UWP C++ Apps
- □ Windows SDK for UWP Apps Localization
- □ Windows SDK for Desktop C++ x86 Apps
- □ Windows SDK for Desktop C++ amd64 Apps
- □ Windows SDK for Desktop C++ arm Apps
- □ Windows SDK for Desktop C++ arm64 Apps

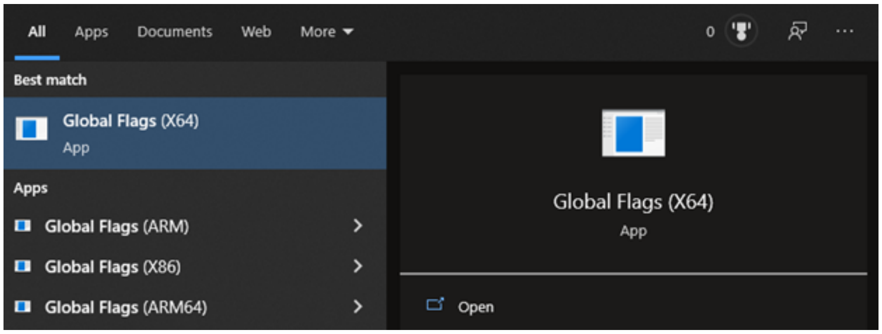
Debugging Tools for Windows

Size: 528.3 MB

Kernel and user-mode debuggers as well as help and tips for using Debugging Tools for Windows.

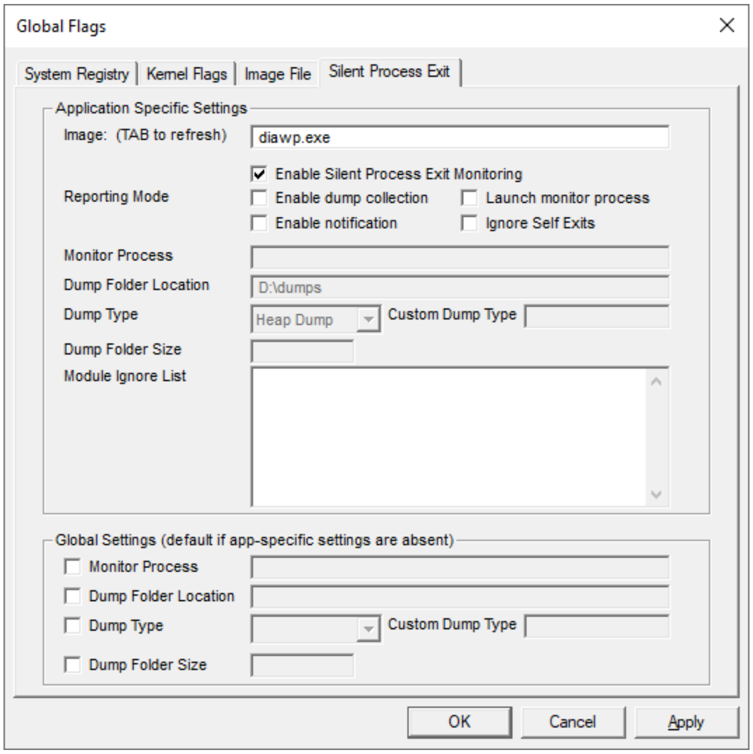
Estimated disk space required: 528.3 MB
Disk space available: 9.6 GB

3. Launch gflags.exe from the installation directory or start menu. It requires admin privileges to open so be sure to be administrator on the computer where you are launching this.



4. Follow the below instructions to configure Windows process exit monitoring.

- Launch gflags.exe from Windows Debugging tool kit installation directory
- Switch to “Silent Process Exit” tab
- Type the name of the process that you want to monitor. For example, diawp.exe
- Press tab and check the box “Enable silent process exit monitoring”
- Click OK to complete



Application Specific Settings

Image: (TAB to refresh) diawp.exe

☑ Enable Silent Process Exit Monitoring

Reporting Mode ☐ Enable dump collection ☐ Launch monitor process

☐ Enable notification ☐ Ignore Self Exits

Monitor Process

Dump Folder Location D:\dumps

Dump Type Heap Dump Custom Dump Type

Dump Folder Size

Module Ignore List

Global Settings (default if app-specific settings are absent)

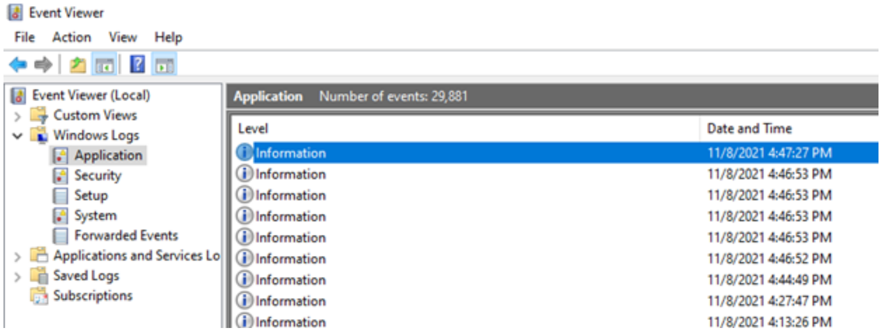
☐ Monitor Process

☐ Dump Folder Location

☐ Dump Type Custom Dump Type

☐ Dump Folder Size

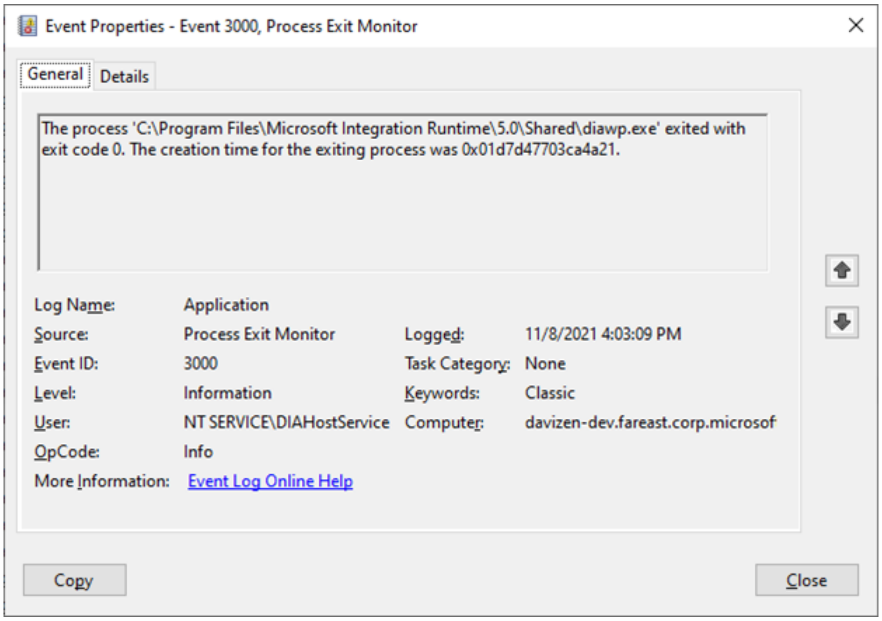
- Log is shown in Event Viewer -> Windows Logs -> Application



Application Number of events: 29,881

Level	Date and Time
Information	11/8/2021 4:47:27 PM
Information	11/8/2021 4:46:53 PM
Information	11/8/2021 4:46:53 PM
Information	11/8/2021 4:46:53 PM
Information	11/8/2021 4:46:53 PM
Information	11/8/2021 4:46:52 PM
Information	11/8/2021 4:44:49 PM
Information	11/8/2021 4:27:47 PM
Information	11/8/2021 4:13:26 PM

- Restart SHIR to close diawp.exe gracefully and we can see below event log in Application event log with event ID 3000 from source “Process Exit Monitor”

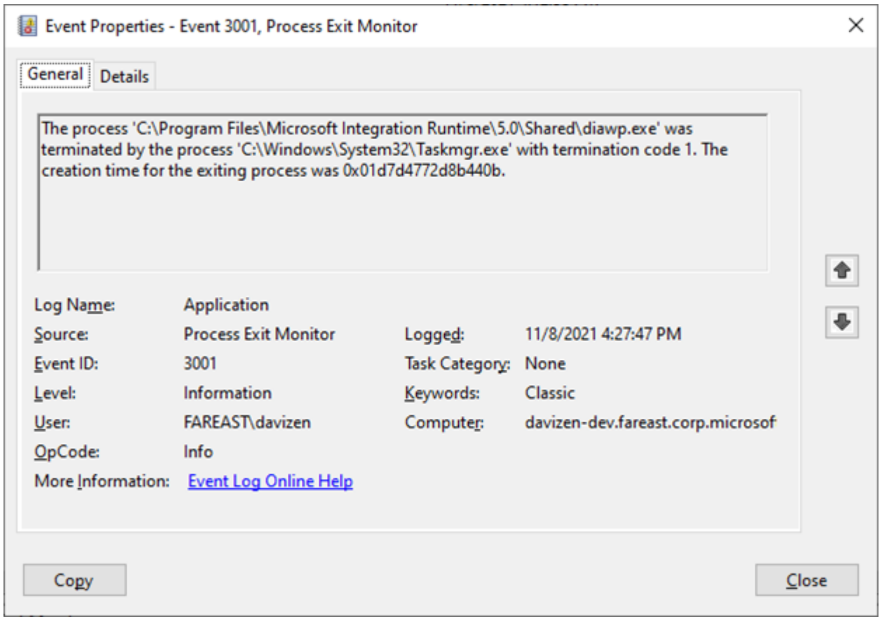


Event Properties - Event 3000, Process Exit Monitor

The process 'C:\Program Files\Microsoft Integration Runtime\5.0\Shared\diawp.exe' exited with exit code 0. The creation time for the exiting process was 0x01d7d47703ca4a21.

Log Name: Application
Source: Process Exit Monitor
Logged: 11/8/2021 4:03:09 PM
Event ID: 3000
Task Category: None
Level: Information
Keywords: Classic
User: NT SERVICE\DIAHostService
Computer: davizen-dev.fareast.corp.microsof
OpCode: Info
More Information: Event Log Online Help

- Kill diawp.exe via task manager. Now we can see a 3001 event ID in application log from the same source



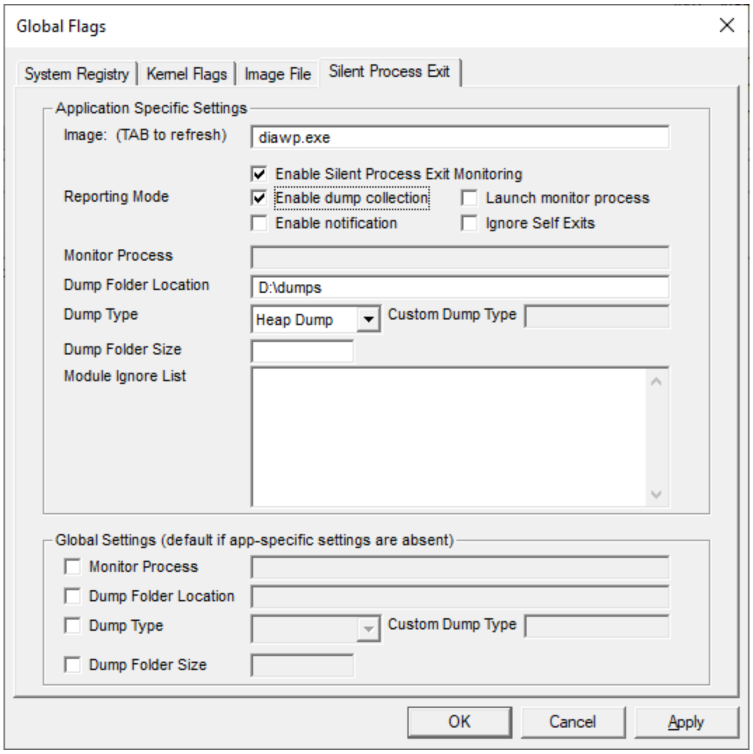
Event Properties - Event 3001, Process Exit Monitor

The process 'C:\Program Files\Microsoft Integration Runtime\5.0\Shared\diawp.exe' was terminated by the process 'C:\Windows\System32\Taskmgr.exe' with termination code 1. The creation time for the exiting process was 0x01d7d4772d8b440b.

Log Name: Application
Source: Process Exit Monitor
Logged: 11/8/2021 4:27:47 PM
Event ID: 3001
Task Category: None
Level: Information
Keywords: Classic
User: FAREAST\davizen
Computer: davizen-dev.fareast.corp.microsof
OpCode: Info
More Information: Event Log Online Help

Enable dump collection

1. Check the box “Enable dump collection”
2. Provide the folder at “Dump Folder Location”
3. Select the Dump Type: Heap Dump
4. Click OK to complete



Application Specific Settings

Image: (TAB to refresh) diawp.exe

☑ Enable Silent Process Exit Monitoring

Reporting Mode: ☑ Enable dump collection ☐ Launch monitor process ☐ Enable notification ☐ Ignore Self Exits

Monitor Process:

Dump Folder Location: D:\dumps

Dump Type: Heap Dump Custom Dump Type:

Dump Folder Size:

Module Ignore List:

Global Settings (default if app-specific settings are absent)

☐ Monitor Process

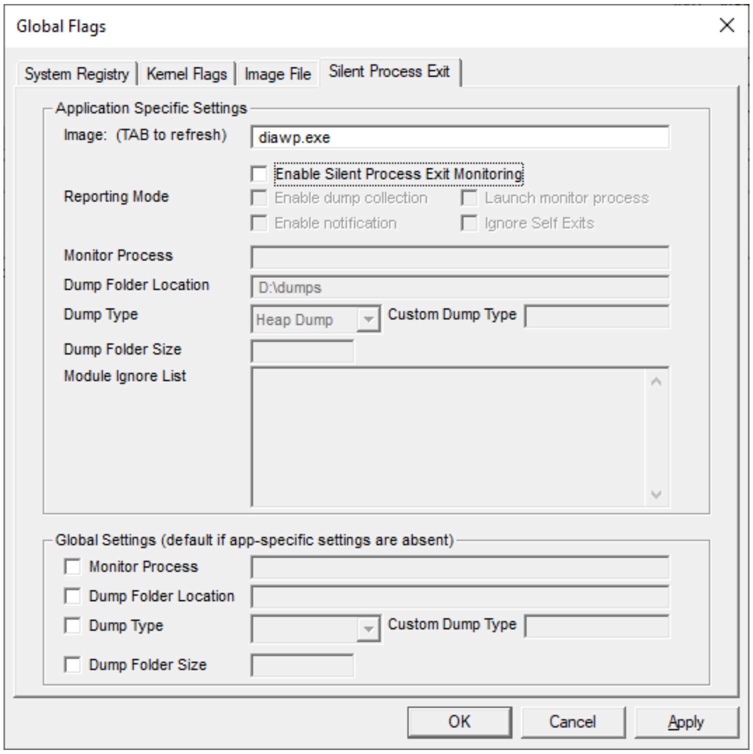
☐ Dump Folder Location

☐ Dump Type Custom Dump Type

☐ Dump Folder Size

Remove Windows process exit monitoring

1. Type the name of the process that you want to remove monitor. For example, diawp.exe
2. Uncheck the box “Enable silent process exit monitoring”
3. Click OK to complete



Application Specific Settings

Image: (TAB to refresh) diawp.exe

☐ Enable Silent Process Exit Monitoring

Reporting Mode: ☐ Enable dump collection ☐ Launch monitor process ☐ Enable notification ☐ Ignore Self Exits

Monitor Process:

Dump Folder Location: D:\dumps

Dump Type: Heap Dump Custom Dump Type:

Dump Folder Size:

Module Ignore List:

Global Settings (default if app-specific settings are absent)

☐ Monitor Process

☐ Dump Folder Location

☐ Dump Type Custom Dump Type

☐ Dump Folder Size