ESET Tech Center

Kennisbank > Diagnostics > Using Process Monitor to create log files

Using Process Monitor to create log files

Steef | ESET Nederland - 2021-07-19 - Reacties (0) - Diagnostics

lssue

After contacting ESET Technical Support, you may be asked to recreate your problem and provide us with the Process Monitor log files.

When are Process Monitor log files needed?

Process Monitor log files are typically required to diagnose issues that recede when ESET real-time protection is disabled.

Solution

- 1. Download Process Monitor from Microsoft Technet and save it to your Desktop.
- Extract ProcessMonitor.zip, double-click Procmon.exe and then click Yes at the prompt. Click Agree if you agree to the conditions in the End-User License Agreement.
- 3. In the main window, click **Filter** → **Enable Advanced Output**.

Process Monitor - Sysinternals: www.sysinternals.com					
File Edit Event Filte	r Tools Options He	p			
🛎 🖬 🍳 🐂	Enable Advanced Outpu	t	🌋 🗟 🔬 🞝	<u>A.</u>	
Time Process Na	Filter	Ctrl+L		Resul ^	
11:08: 둘 snagitedi	Reset Filter	Ctrl+R			
11:08: • dwm.exe 11:08: & Searchin	Load Filter	>		SUCCI SUCCI	
11:08: 🗖 dwm.exe	Save Filter		ARE\INTEL\IGFX\D3	D10NAME	
11:08: A SearchIn	Organize Filters			SUCCI	
11:08: • dwm.exe				DIONAME	
11:08: • ekm.exe	Drop Filtered Events		stem32\en-US\ntdll.d	I SUCCI	
11:08: 💶 ekm.exe	Highlight	Ctrl+H	stem32\en-US\ntdll.d	I SUCCI	
11:08: 📻 Explorer.	- ingrinightan		AClasses	SUCCI	
11:08: 💶 ekm.exe	2316 🛃 Query Standar	dlC:\Windows\Sy	stem32\en-US\ntdll.d	I SUCCI	
11:08: 📊 Explorer.EXE	4608 🌋 RegQueryKey	 HKCU\Software 	e\Classes	SUCCI	
11:08: 💶 ekm.exe	2316 🛃 ReadFile	C:\Windows\Sy	stem32\en-US\ntdll.d	I SUCCI	
11-08- Evolorer EXE	1602 🏘 Rea Ouenriker	 HKCH/Software 	\Claeeae	 Incri * 	
<				>	
Showing 65 737 of 221 756	events (29%)	Backed by virtual	memory	.:	

Figure 1-1

4. See the appropriate instructions below to gather the specific logs requested by

Gather process log files

1. Process Monitor begins recording logs as soon as you open it. Click the magnifying glass icon to stop recording logs.



Figure 2-1

1. Click the eraser icon to clear the current log files list.



Figure 2-2

- Click the magnifying glass icon to start capturing new log files and then reproduce your issue. After you reproduce your issue, click the magnifying glass again to stop recording logs.
- 2. Click the diskette icon to save your new log files. In the pop-up window, select **All** events and then select **Native Procesess Monitor Format (.PML)** option.



Figure 2-3

- Navigate to the **ProcessMonitor** folder where you saved the files, you may need to make hidden files visible to see this folder.
- Select the log files, right-click them and then select Send to → Compressed (zipped) folder from the context menu to create a .zip file.
- 3. If you have not already done so, <u>open a case</u> with ESET Technical Support before you submit your .zip file.
- 4. Attach the .zip file to an email reply to ESET Technical Support. A Technical Support representative will examine the log and respond as soon as possible with the recommended action based on their findings.

Gather boot log files

1. Click **Options** → **Enable Boot Logging**.

👌 Process Monitor - Sysinternals	www.sysinternals.com -	
File Edit Event Filter Tools	Options Help	
😅 🖬 🍳 🅦 🖾 🗢	Always on Top	
Time Process Name PID	Font	Result ^
11:37: Ssnagiteditor.exe 7264	Highlight Colors	JCCESS
11:37: SearchIndexer 5248	Configure Symbols	UCCESS
11:37: 🔏 Search Indexer 5248	Select Columns	JCCESS
11:37: Explorer.EXE 3028	Select Columns	JCCESS
11:37: Explorer.EXE 3028	History Depth	JUCESS
11:37: Explorer.EXE 3028	Profiling Events	JCCESS
11:37: 🙀 Explorer.EXE 3028		JCCESS
11:37: Texplorer.EXE 3028	Enable Boot Logging	JCCESS
11:37: Explorer.EXE 3028	Show Resolved Network Addresses Ctri-	+N UCCESS
11:37: • svchost.exe 372	Hey File Offsets and Lengths	JCCESS
11:37: 🙀 Explorer.EXE 3028		JCCESS 🗸
		>
Showing 34 563 485 of 44 238 255 ev	ents (78%) Backed by virtual memory	

Figure 3-1

 Select the check box next to Generate profiling events to enable it, set the frequency to Every second and then click OK.

Enable Boot Logging			
Process Monitor can generate thread profiling events that capture the state of all running applications at a regular interval.			
Generate thread profiling events			
Every second			
O Every 100 milliseconds			
OK Cancel			

Figure 3-2

 Restart your computer, reproduce your issue and then run **Process Monitor**. Click Yes at the prompt to save the boot log.





- Save the boot log as a Procmon Log (.PML) file and make a note of where it is saved.
- Navigate to the folder where you saved .PML file, you may need to <u>make hidden files</u> <u>visible</u> to see this folder.
- Select the log files, right-click them and then select Send to → Compressed (zipped) folder from the context menu to create a .zip file.
- 4. If you have not already done so, <u>open a case</u> with ESET Technical Support before you submit your .zip file.
- 5. Attach the .zip file to an email reply to ESET Technical Support. A Technical Support representative will examine the log and respond as soon as possible with the recommended action based on their findings.

Running ProcMon against a Remote Machine

Utilizing <u>psexec</u>, you can run ProcMon against a remote machine.

To start the trace on a remote computer run:

Psexec \\<hostname> /s /d procmon.exe /accepteula /quiet /backingfile
c:\hostname_trace.pml

Now, to stop the trace on the remote computer run:

Psexec \\<hostname> /s /d procmon.exe /accepteula /terminate

Finally, copy the log file to your remote machine for viewing:

xcopy \\<hostname>\c\$\hostname_trace.pml c:\TEMP

You can then view the log file in ProcMon locally by running:

Procmon /openlog c:\temp\hostname_trace.pml

Gerelateerde inhoud

- Create a full memory dump of a VMware virtual machine
- How do I generate a memory dump manually?
- How to create a Wireshark log
- <u>Run the Info_get.command on a Linux machine and send the logs to ESET Technical</u> <u>Support</u>

• How do I use ESET Log Collector?