procmon

quinta-feira, 12 de dezembro de 2019

14:21

1. Download Process Monitor <https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>

2. Run procmon.exe

3. Go to Filter > Filter

Texto alternativo gerado por máquina:
Edit Event 
Process N 
aplorer 
aplorer 
aplorer 
svchost 
svchost 
svchost 
aplorer 
svchost 
MEMTA 
MELSC 
Process Monitor - S 
Filter Toals Options Help 
Enable Advanced Output 
Filter „ 
Reset Filter 
Load Filter 
Save Filter... 
Organize Filters... 
Drap Filtered Events 
Highlight.„ 
Ctrl*L 
Ctrl*R 
Ctrl* 

4. In Display entries matching these conditions, specify so that it matches the following:

- Result

- Is

- ACCESS DENIED

- Then: Include (see image below)

Texto alternativo gerado por máquina:
Process Monitor Filter 
Display entries matchinç these conditons: 
Remove 
Column 
Result 
Process N 
Process N 
Process N 
Process N 
Process N 
Value 
ACCESS DENIED 
Procexp exe 
Autorunsexe 
Procmon64exe 
Procexp 64 exe 
Include 
aclude 
aclude 

5. Click OK

6. Reproduce the issue/error;

7. At the very same time, look at the process monitor and scroll down to the bottom of the results to see the very last result. Take a note of the Process Name; OPeration; Path; Result/ and Detail.

Texto alternativo gerado por máquina:
File Edit Event Filter Toals Options Help 
Process Monitor 
Sysinternals: www.sysinternals.com 
Operation 
r: *CreateFlIe 
Path 
C:NProaram Files lx88ñPIeskNadminhhtdocsNnebconfia 
Result 
ACCESS DENIED 
Detail 
Desired Access: Read Atributes. Disaostion: Caen. Ootions: Caen Reaarse Point. Atributes: n,'a. ShareMode: 
Time of Day Process Name 
2984 
Showing 400 of 705 events (0.0%) 
Backecl byvirtual memory 

8. Click on the Process Name in question to see more details about it.

Texto alternativo gerado por máquina:
Event 
Prcu:ess 
Event Properties 
Stack 
13.12.2019 
File System 
Crea teFiIe 
C: Program Files config 
o.oooozgo 
Read Attribu tes 
Open 
Open Reparse Point 
Read, Write, Delete 
Operaton: 
PBth: 
Duration: 
Desir ed Access: 
Dispositon: 
Optons: 
Attributes: 
ShareMode: 
Alloca tionSi ze: 

9. In this example, the w3wp.exe process was failing to open the C:\Program Files (x86)\Plesk\admin\htdocs\web.config file. Because the Desired Access (Read Attributes) was not met.