How to install and use Procmon on Linux, an open source tool just released by Microsoft

Procmon is a system utility that helps users easily track system calls (system calls), access the Registry and file activity related to processes running in the operating system.

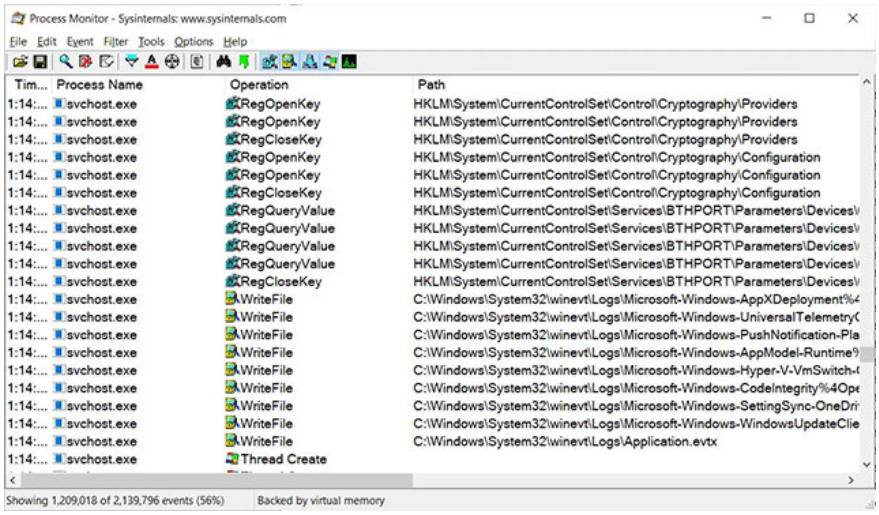
After a long time of planning with many delays, Microsoft has finally officially released the popular utility Sysiternals Procmon Linux version so that users can track the activities of running processes right on the operating system. on this open source.

Procmon on Linux

What is procmon?

Perhaps many Windows users are no stranger to this tool. Procmon is a system utility that helps users easily track system calls (system calls), access the Registry and file activity related to processes running in the operating system.

Tracking these processes allows users to early diagnose problems that may occur on the system, such as application conflicts, excessive resource usage, or even malware infection.



Procmon for Windows

The launch of the open source Procmon tool for Linux plays an important role, giving Linux users an additional tool to help track processes running on systems similar to Windows, as can be seen. in the demo below:

Procmon demo on Linux

How to install and build Procmon on Linux

System requirements

1. Operating system: Ubuntu 18.04 LTS with kernel> = 4.18 and kernel = 5.3.
2. cmake> = 3.13 (build-time only)
3. libsqlite3-dev> = 3.22 (build-time only)

Install Procmon

Sign up for Microsoft key and feed:

```
wget -q https://packages.microsoft.com/config/ubuntu/$(lsb_release -rs)/packages
```

Then use the following command to install Procmon:

```
sudo apt-get update sudo apt-get install procmon
```

Build Procmon from source

Install dependency:

```
sudo apt-get -y install bison build-essential flex git libedit-dev libllvm6.0 ll
```

Build and install BCC:

```
git clone --branch tag_v0.10.0 https://github.com/iovisor/bcc.git mkdir bcc/build
```

Build Procmon:

```
git clone https://github.com/Microsoft/Procmon-for-Linux cd Procmon-for-Linux mk
```

Build package Procmon:

The distribution packages for Procmon on Linux are built using cpack. To build the deb package for Procmon on Ubuntu you just need to run:

```
cd build cpack .
```

How to use Procmon

When using Procmon on Linux, users can specify the process ID they want to track or specific system calls with the following arguments:

```
Usage: procmon [TÙY CH?N]
```

There are OPTIONS including:

1. **-h / - help:** Print this help screen
2. **-p / - pids:** Separate the process id list with commas for monitoring
3. **-e / - events:** Separate a list of system calls with a comma for monitoring
4. **-c / - collect [PATHWAY]:** Option to start Procmon in non-terminal mode
5. **-f / - file** PATHWAY **:** Open the trace file Procmon

For example, to monitor processes with id 738 and 2657, enter the following command:

```
sudo procmon -p 738,2657
```

To monitor PID 738 and list all read / write calls, use the following command.

```
sudo procmon -p 738 -e read,write
```

For more information about using Procmon in Linux, you can refer to the GitHub website of this project HERE: