Microsoft brings Sysmon tools to Linux

Microsoft has just released the Linux version of the very popular Sysmon system monitoring tool on Windows. Sysmon will allow Linux Admins to monitor devices to detect dangerous and unusual activities.

Sysmon (aka System Monitor) is a tool in Microsoft's SysInternals toolkit. Its function is to monitor the system for malicious activities and then log all detected behavior into system log files.

Sysmon is extremely flexible allowing Admins to create custom configuration files to monitor specific system events. From there, the Admin will easily detect dangerous activities on the system.

Sysmon for Linux will be released as an open source project on GitHub. Linux users will have to compile the program themselves and make sure they have all the required dependencies. Instructions for compiling the program are provided on the project's GitHub page here.

It should be noted that to compile Sysmon you must first install the SysinternalsEBP project.

After Sysmon is compiled, you can view the help file by entering the command: sudo ./sysmon -h. To use the program, you must first accept the permission agreement for the user by entering the command: sudo ./sysmon -accepteula.

You can then run Sysmon with or without the configuration file using one of the following commands:

No configuration file:

1. sudo ./sysmon -i

There is an image level file:

1. sudo ./sysmon -i CONFIG_FILE

To create your own Sysmon configuration file, you need to use the ./sysmon -s command to view the current instance's configuration graph and see what commands are available. To learn more about creating a Sysmon configuration file, please refer to the official Microsoft documentation here.

After starting Sysmon will start logging events to the file /var/log/syslog. So, if you don't configure it to restrict what is logged, you will find your log file size increasing.

Hope you have a "happy" time with Microsoft's new tool for Linux.