Installing Sysmon in windows

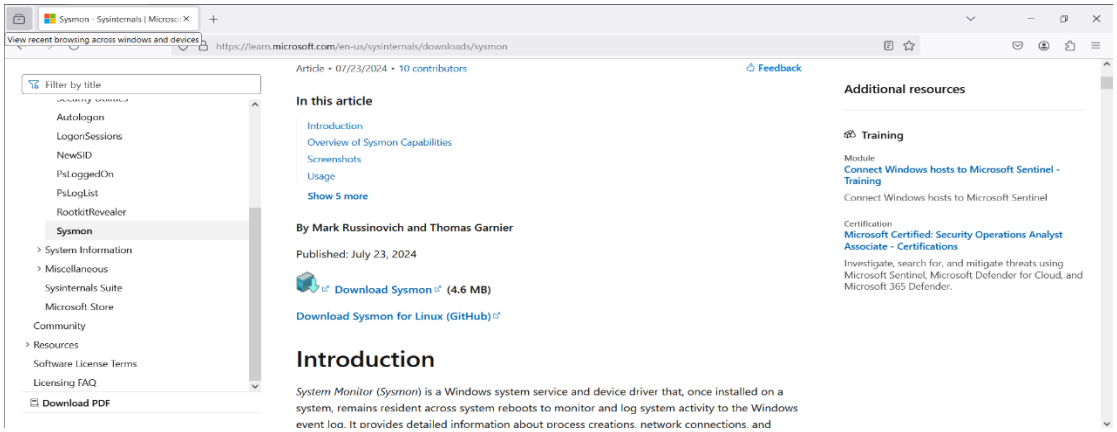
Overview:-

Sysmon (System Monitor) is a powerful tool created by Microsoft. Once installed, Sysmon remains resident across system reboots to monitor and log system activity. By collecting these events, it becomes easier to monitor and analyze the system using any SIEM software or tools.

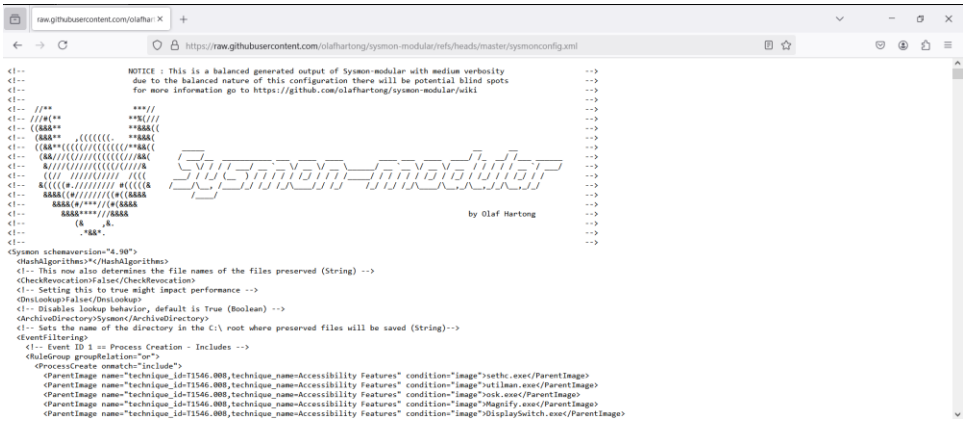
This documentation details the steps to install Sysmon on a Windows 10 computer, whether it's a standalone computer or a virtual machine hosted on any virtualization software.

Steps 1:- Download Necessary Files

1. Open a browser on the system where you want to install Sysmon, and search for "Sysmon".
2. Visit the first link provided by Microsoft



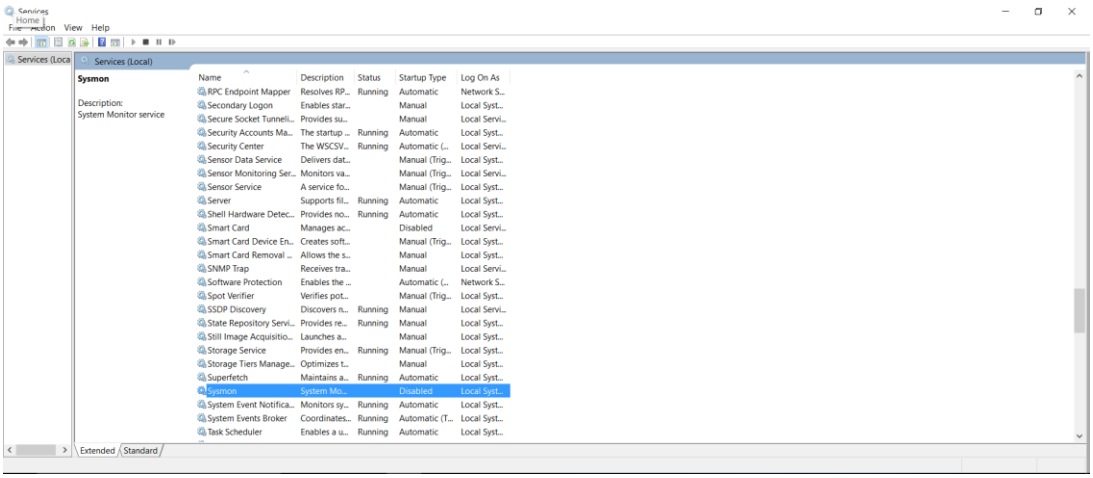
3. Click the "Download Sysmon" button to download a zip file.
4. Obtain a Sysmon config file from the following link: Sysmon Config.https://raw.githubusercontent.com/olafhartong/sysmon-modular/refs/heads/master/sysmonconfig.xml



5. Save this file as sysmonconfig.xml by right-clicking the page and selecting "Save As".

Steps 2:- Extract and Install Sysmon

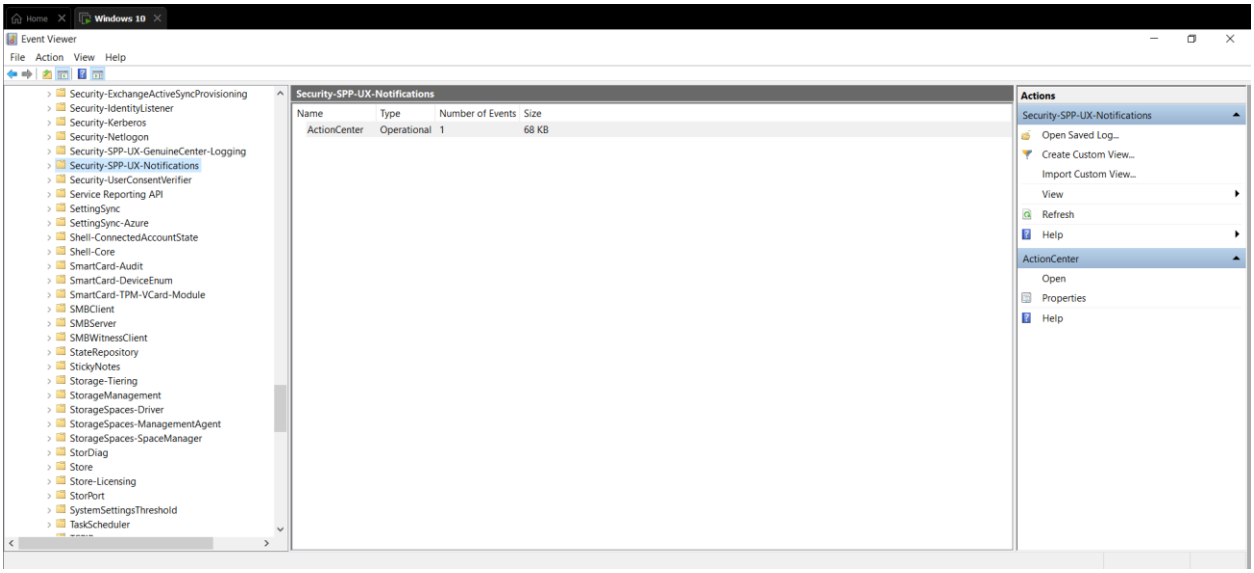
1. Extract the Sysmon.zip file by right-clicking on it and selecting "Extract All".
2. Check if Sysmon is already installed:
   Open "Services" on the system and look for a service named "Sysmon".



Now in my case I already have Sysmon service but see it has been disabled, I disabled for the sake of this documentation.

Now we will also check the event viewer for Sysmon.

Open "*Event Viewer*" from the Start menu, navigate to *Application and Service Logs > Microsoft > Windows > Sysmon*. If you don't find Sysmon, it means it's not installed.



Now you can see I don't have Sysmon install ' as I said earlier I have uninstalled for the sake of this documentation'.

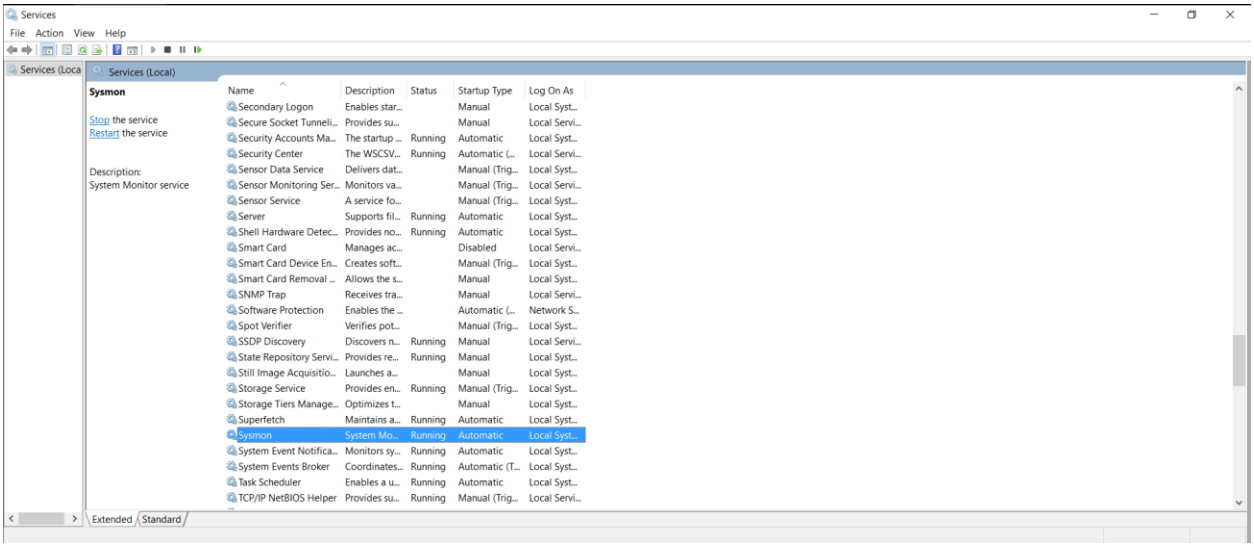
3. To install Sysmon using PowerShell:

- Copy the sysmonconfig.xml file you saved earlier to the extracted Sysmon folder.
- Open PowerShell with administrative privileges from the Start menu.
- Navigate to the folder where the Sysmon files are extracted.
- Run the command: ./Sysmon.exe -I sysmonconfig.xml

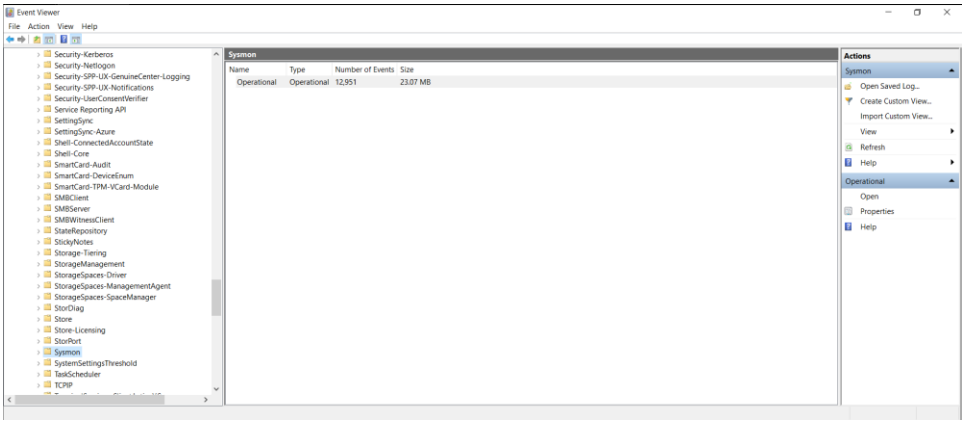
```
PS C:\Users\FOLusername\Downloads\Sysmon> .\Sysmon.exe -i sysmonconfig.xml

System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.90
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
```

Step 3:- Verify Sysmon Installation

1. Open "Services" to ensure the Sysmon service is running



2. Re-open "Event Viewer" as described in Step 2 and check for Sysmon events under Application and Service Logs > Microsoft > Windows > Sysmon.



Conclusion

This concludes the Sysmon installation guide. In upcoming documentation, I will demonstrate how to use Sysmon to monitor logs and then send these logs to SIEM solutions like Splunk or Wazuh. Stay tuned, and keep learning, living, and laughing!

Stay safe and happy.