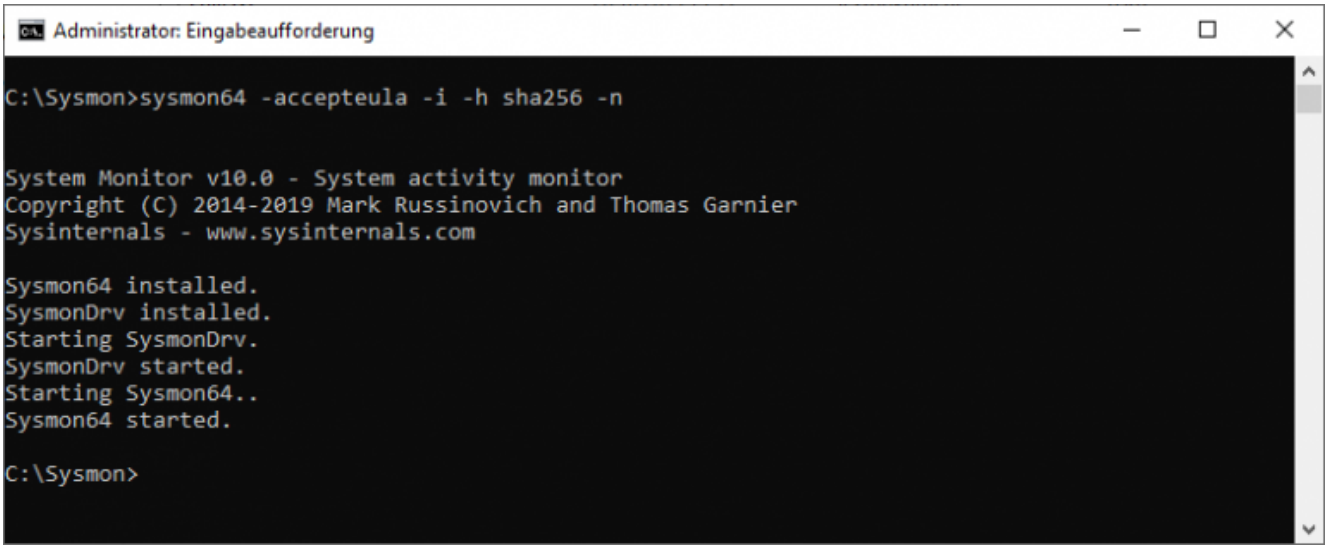


Sysinternals Sysmon jetzt mit einer DNS Query Protokollierung

Sysinternals – Sysmon mit DNS Protokollierung

Die neue Ereignis-ID für DNS-Abfragen lautet 22. Sobald ein Prozess eine DNS-Abfrage ausführt, wird dieses als Ereignis ins LOG geschrieben, egal ob das Ergebnis positiv oder negativ ist.

Download Sysmon

https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Download aller Tools

https://live.sysinternals.com/

```
Get-WinEvent -FilterHashtable @{logname="Microsoft-Windows-Sysmon/Operational";id=3;} | Where {$_.message -like "*172.18.32.10*" -and $_.message -like "*DestinationPort: 80*"} | Select-Object -Property message -First
```

```
1 | Format-List
```

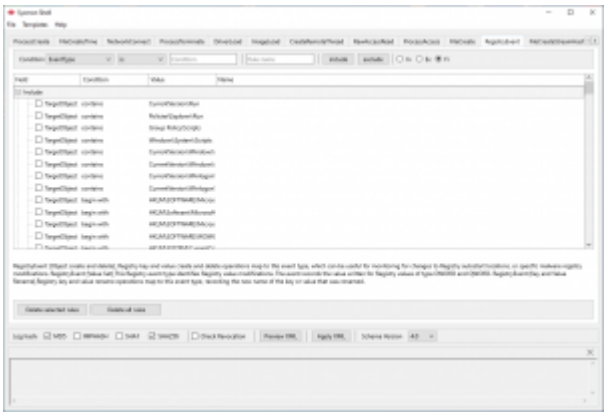
```
Get-WinEvent -FilterHashtable @{logname="Microsoft-Windows-Sysmon/Operational";id=3;} | Where {$_.message -like "*172.18.32.10*" -and $_.message -like "*DestinationPort: 443*"} | Select-Object -Property message -First 1 | Format-List
```

```
Get-WinEvent -FilterHashtable @{logname="Microsoft-Windows-Sysmon/Operational";id=22;} | Format-List
```

Sysmon Search Event

Sysmon Tools

Die Sysmon Shell ein Tool zur Erstellung von Konfigurations-Templates und vieles mehr.



Sysmon View, ein Offline Tool zur grafischen Auswertung der Events. Es unterstützt bei der Verfolgung und Visualisierung von Sysmon-Protokollen, indem verschiedene Sysmon-Ereignisse logisch gruppiert und miteinander in Beziehung gesetzt werden.

[Download Sysmon Tools]