



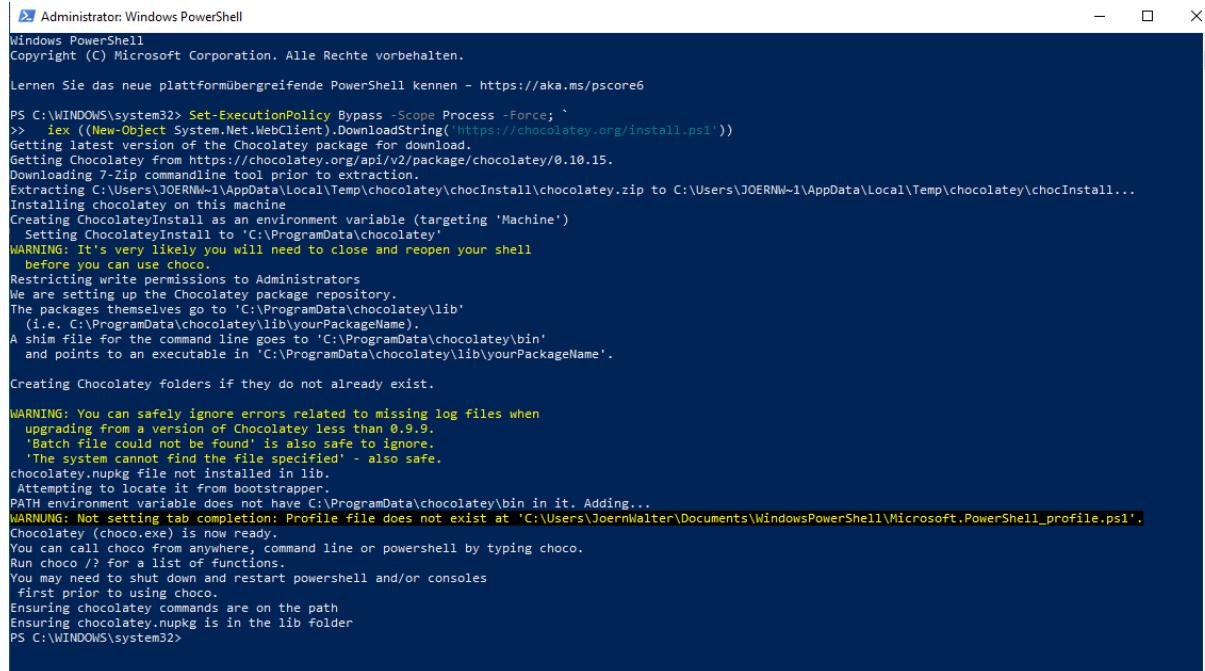
DNS-Abfragen protokollieren

Sysmon (System Monitor) ist ein zeitgleich ein Systemdienst und Treiber, der nach der Installation immer aktiv bleibt. Sysmon überwacht alle Systemaktivitäten und schreibt diese ins Windows Ereignisprotokoll.

Neuinstallation von Sysmon

```
Set-ExecutionPolicy Bypass -Scope Process -Force; `
```

```
Invoke-Expression ((New-Object
System.Net.WebClient).DownloadString('https://chocolatey.org/install.ps1'))
```



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

Lernen Sie das neue plattformübergreifende PowerShell kennen - https://aka.ms/pscore6

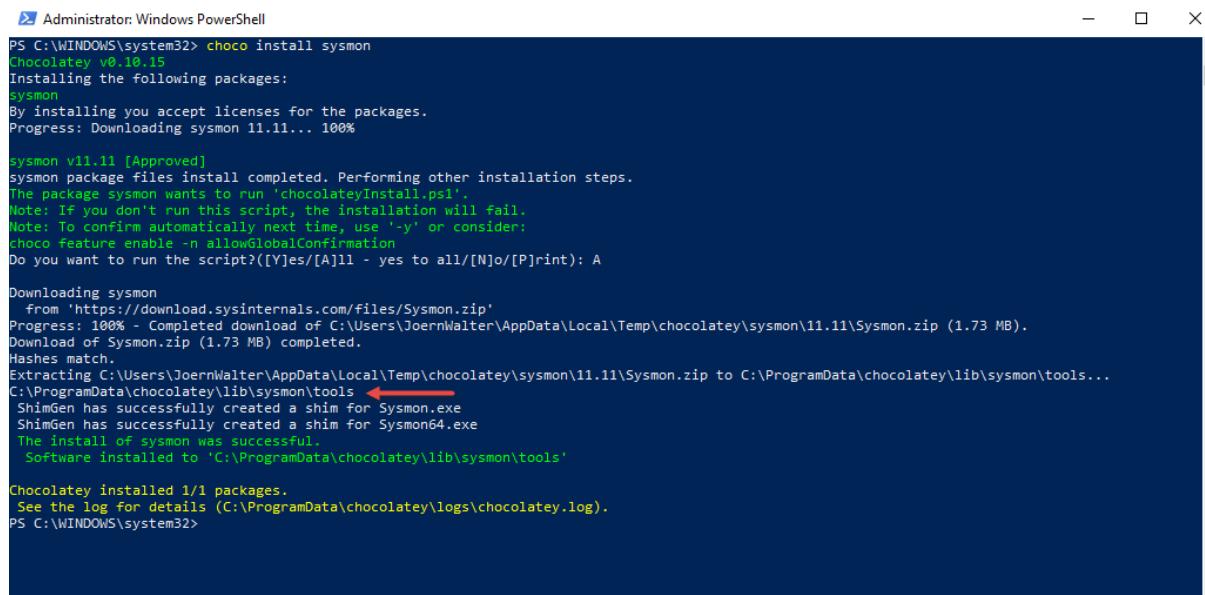
PS C:\WINDOWS\system32> Set-ExecutionPolicy Bypass -Scope Process -Force; `>> iex ((New-Object System.Net.WebClient).DownloadString('https://chocolatey.org/install.ps1'))Getting latest Version of the Chocolatey package for download.
Getting Chocolatey from https://chocolatey.org/api/v2/package/chocolatey/0.10.15.
Downloading 7-Zip commandline tool prior to extraction.
Extracting C:\Users\JOERNW~1\AppData\Local\Temp\chocolatey\chocInstall\chocolatey.zip to C:\Users\JOERNW~1\AppData\Local\Temp\chocolatey\chocInstall...
Installing chocolatey on this machine
Creating ChocolateyInstall as an environment variable (targeting 'Machine')
  Setting ChocolateyInstall to 'C:\ProgramData\chocolatey'
WARNING: It's very likely you will need to close and reopen your shell
  before you can use choco.
Restricting write permissions to Administrators
We are setting up the Chocolatey package repository.
The packages themselves go to 'C:\ProgramData\chocolatey\lib'
  (i.e. C:\ProgramData\chocolatey\lib\yourPackageName).
A shim file for the command line goes to 'C:\ProgramData\chocolatey\bin'
  and points to an executable in 'C:\ProgramData\chocolatey\lib\yourPackageName'.

Creating Chocolatey folders if they do not already exist.

WARNING: You can safely ignore errors related to missing log files when
  upgrading from a version of Chocolatey less than 0.9.9.
  'Batch file could not be found' is also safe to ignore.
  'The system cannot find the file specified' - also safe.
chocolatey.nupkg file not installed in lib.
Attempting to locate it from bootstrapper.
PATH environment variable does not have C:\ProgramData\chocolatey\bin in it. Adding...
WARNING: Not setting tab completion: Profile file does not exist at 'C:\Users\JOERNWALTER\Documents\WindowsPowerShell\Microsoft.PowerShell_profile.ps1'.
Chocolatey (choco.exe) is now ready.
You can call choco from anywhere, command line or powershell by typing choco.
Run choco /? for a list of functions.
You may need to shut down and restart powershell and/or consoles
  first prior to using choco.
Ensuring chocolatey commands are on the path
Ensuring chocolatey.nupkg is in the lib folder
PS C:\WINDOWS\system32>
```

```
choco search sysmon
choco install sysmon
```

Sysmon wurde heruntergeladen und ist bereit zur Nutzung.



```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> choco install sysmon
Chocolatey v0.10.15
Installing the following packages:
  sysmon
By installing you accept licenses for the packages.
Progress: Downloading sysmon 11.11... 100%
sysmon v11.11 [Approved]
sysmon package files install completed. Performing other installation steps.
The package sysmon wants to run 'chocolateyInstall.ps1'.
Note: If you don't run this script, the installation will fail.
Note: To confirm automatically next time, use '-y' or consider:
  choco feature enable -n allowGlobalConfirmation
Do you want to run the script?(Y)es/[A]ll - yes to all/[N]o/[P]rint): A

Downloading sysmon
  from 'https://download.sysinternals.com/files/Sysmon.zip'
Progress: 100% - Completed download of C:\Users\JOERNWALTER\AppData\Local\Temp\chocolatey\sysmon\11.11\Sysmon.zip (1.73 MB).
Download of Sysmon.zip (1.73 MB) completed.
Hashes match.
Extracting C:\Users\JOERNWALTER\AppData\Local\Temp\chocolatey\sysmon\11.11\Sysmon.zip to C:\ProgramData\chocolatey\lib\sysmon\tools...
C:\ProgramData\chocolatey\lib\sysmon\tools
  ShimGen has successfully created a shim for Sysmon.exe
  ShimGen has successfully created a shim for Sysmon64.exe
  The install of sysmon was successful.
  Software installed to 'C:\ProgramData\chocolatey\lib\sysmon\tools'

Chocolatey installed 1/1 packages.
See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).
PS C:\WINDOWS\system32>
```

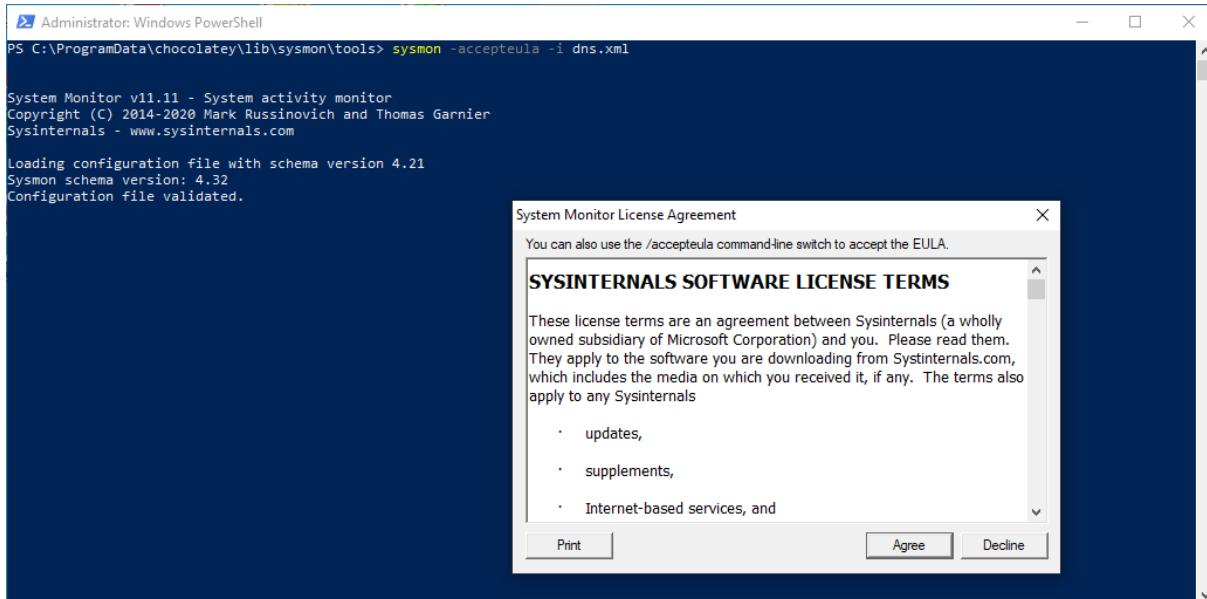
Alternativ kann man Sysmon auch von Microsoft direkt herunterladen.



DNS-Abfragen protokollieren

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

Wechseln in den Installationspfad „**C:\ProgramData\chocolatey\lib\sysmon\tools**“ und installieren SYSMON nun mit einer voreingestellten Konfigurationsdatei, die nur DNS-Abfragen ins Protokoll schreibt.



```
Administrator: Windows PowerShell
PS C:\ProgramData\chocolatey\lib\sysmon\tools> sysmon -accepteula -i dns.xml

System Monitor v11.11 - System activity monitor
Copyright (C) 2014-2020 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.21
Sysmon schema version: 4.32
Configuration file validated.

System Monitor License Agreement
You can also use the /accepteula command-line switch to accept the EULA.

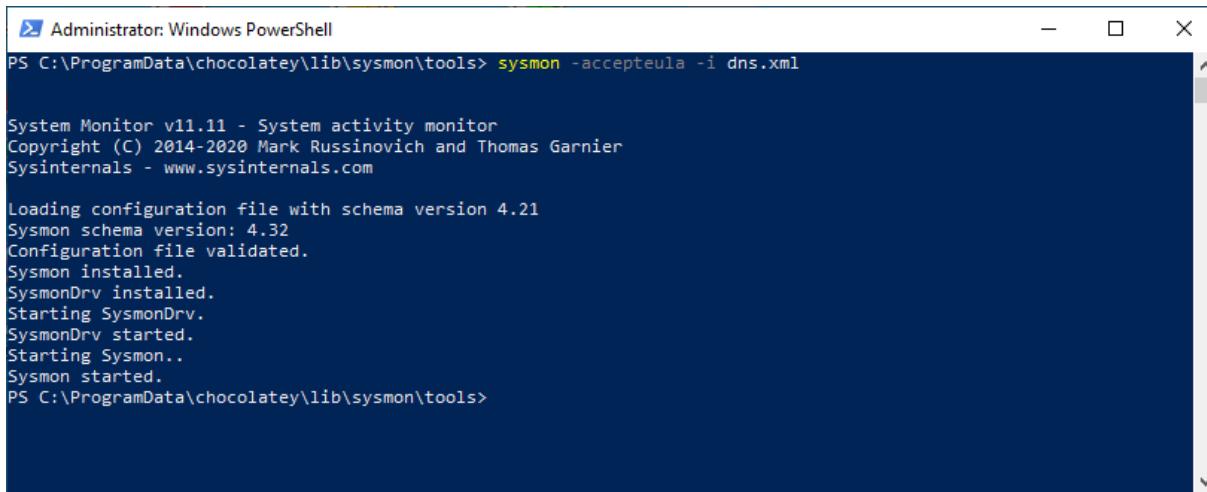
SYSINTERNALS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly
owned subsidiary of Microsoft Corporation) and you. Please read them.
They apply to the software you are downloading from Sysinternals.com,
which includes the media on which you received it, if any. The terms also
apply to any Sysinternals

    · updates,
    · supplements,
    · Internet-based services, and

Print Agree Decline
```

sysmon -accepteula -i dns.xml



```
Administrator: Windows PowerShell
PS C:\ProgramData\chocolatey\lib\sysmon\tools> sysmon -accepteula -i dns.xml

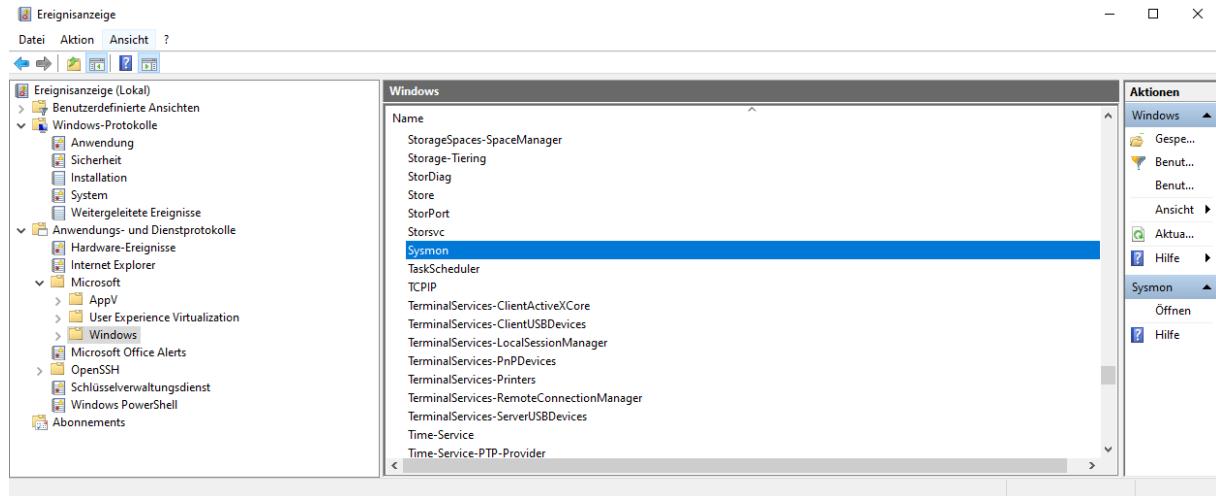
System Monitor v11.11 - System activity monitor
Copyright (C) 2014-2020 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.21
Sysmon schema version: 4.32
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
PS C:\ProgramData\chocolatey\lib\sysmon\tools>
```



DNS-Abfragen protokollieren

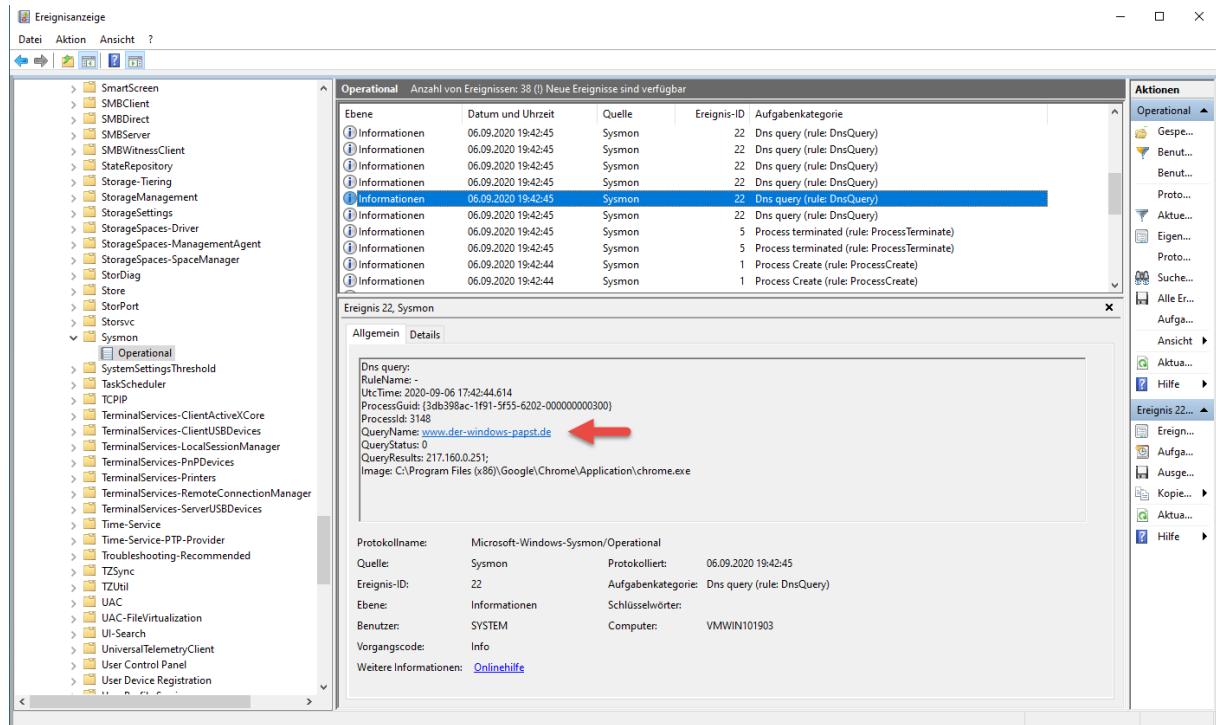
Nach der erfolgreichen Installation finden wir in der Ereignisanzeige nun den neuen Order Sysmon. Sysmon protokolliert ab sofort jede DNS-Abfrage.



Die Ereigniseinträge finden wir unter:

Anwendungen und Dienste / Microsoft / Windows / Sysmon / Operational

Öffne ich nun z.B. den Google Chrome und die Webseite „Der Windows Papst“ finden wir nun z.B. alle DNS-Abfragen rund um die Webseite <https://www.der-windows-papst.de>.





DNS-Abfragen protokollieren

Da ich auf meiner Hauptseite ein paar Verlinkungen habe (unten links), werden diese durch den Browser angefragt und aufgelöst.

4 Beispiele infolge...

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	06.09.2020 19:42:47	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:47	Sysmon	5	Process terminated (rule: ProcessTerminate)
Informationen	06.09.2020 19:42:46	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:46	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:46	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:46	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:45	Sysmon	5	Process terminated (rule: ProcessTerminate)
Informationen	06.09.2020 19:42:45	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:45	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:45	Sysmon	22	Dns query (rule: DnsQuery)



DNS-Abfragen protokollieren

Ereignisanzeige

Operational Anzahl von Ereignissen: 38 (0) Neue Ereignisse sind verfügbar

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	06.09.2020 19:42:47	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:47	Sysmon	22	Process terminated (rule: ProcessTerminate)
Informationen	06.09.2020 19:42:46	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:46	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:46	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:46	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:45	Sysmon	22	Process terminated (rule: ProcessTerminate)
Informationen	06.09.2020 19:42:45	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:45	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:45	Sysmon	22	Dns query (rule: DnsQuery)

Ereignis 22, Sysmon

Allgemein Details

Dns query:
RuleName: -
UtcTime: 2020-09-06 17:42:46.542
ProcessGuid: {3db398ac-1f91-5f55-6202-000000000300}
ProcessId: 3148
QueryName: www.blogspotamt.de (Red arrow)
QueryStatus: 0
QueryResults: 94.136.168.59;
Image: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

Protokollname: Microsoft-Windows-Sysmon/Operational
Quelle: Sysmon Protokolliert: 06.09.2020 19:42:47
Ereignis-ID: 22 Aufgabenkategorie: Dns query (rule: DnsQuery)
Ebene: Informationen Schlüsselwörter:
Benutzer: SYSTEM Computer: VMWIN101903
Vorgangscode: Info Weitere Informationen: [Onlinehilfe](#)

Aktionen

Operational ▾

- Gepe...
- Benut...
- Benut...
- Proto...
- Akte...
- Eigen...
- Proto...
- Suche...
- Alle Er...
- Aufga...
- Ansicht ▾
- Aktua...
- Hilfe ▾
- Ereignis 22... ▾
- Ereign...
- Aufga...
- Ause...
- Kopie...
- Aktua...
- Hilfe ▾

Ereignisanzeige

Operational Anzahl von Ereignissen: 38 (0) Neue Ereignisse sind verfügbar

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	06.09.2020 19:42:47	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:47	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:47	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:47	Sysmon	22	Process terminated (rule: ProcessTerminate)
Informationen	06.09.2020 19:42:47	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:46	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:46	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:45	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:45	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:45	Sysmon	22	Dns query (rule: DnsQuery)
Informationen	06.09.2020 19:42:45	Sysmon	22	Process terminated (rule: ProcessTerminate)

Ereignis 22, Sysmon

Allgemein Details

Dns query:
RuleName: -
UtcTime: 2020-09-06 17:42:46.543
ProcessGuid: {3db398ac-1f91-5f55-6202-000000000300}
ProcessId: 3148
QueryName: www.topblogs.de (Red arrow)
QueryStatus: 0
QueryResults: type: 5 topblogs.de,78.46.71.15;
Image: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

Protokollname: Microsoft-Windows-Sysmon/Operational
Quelle: Sysmon Protokolliert: 06.09.2020 19:42:47
Ereignis-ID: 22 Aufgabenkategorie: Dns query (rule: DnsQuery)
Ebene: Informationen Schlüsselwörter:
Benutzer: SYSTEM Computer: VMWIN101903
Vorgangscode: Info Weitere Informationen: [Onlinehilfe](#)

Aktionen

Operational ▾

- Gepe...
- Benut...
- Benut...
- Proto...
- Akte...
- Eigen...
- Proto...
- Suche...
- Alle Er...
- Aufga...
- Ansicht ▾
- Aktua...
- Hilfe ▾
- Ereignis 22... ▾
- Ereign...
- Aufga...
- Ause...
- Kopie...
- Aktua...
- Hilfe ▾



DNS-Abfragen protokollieren

Klicke ich z.B. auf den Link von Hausarbeit, wird auch dieser versucht aufzulösen.

The screenshot shows the Windows Event Viewer with the 'Operational' log selected. A single event is listed: 'Informationen' (Information) on 06.09.2020 19:45:55 from 'Sysmon' (Event ID 22). The event details a 'Dns query (rule: DnsQuery)' for the URL 'hausarbeit-agentur.com'. A red arrow points to this URL in the event details pane. The event pane also shows the following properties: Protokollname: Microsoft-Windows-Sysmon/Operational; Quelle: Sysmon; Protokolliert: 06.09.2020 19:45:55; Aufgabenkategorie: Dns query (rule: DnsQuery); Ebene: Informationen; Benutzer: SYSTEM; Computer: VMWIN101903; Vorgangscode: Info; Weitere Informationen: [Onlinehilfe](#).

Auch die auf dem System laufenden Anwendungen und Aufgaben werden entsprechend ins Protokoll geschrieben.

The screenshot shows the Windows Event Viewer with the 'Operational' log selected. A single event is listed: 'Informationen' (Information) on 06.09.2020 19:46:15 from 'Sysmon' (Event ID 1). The event details a 'Process Create (rule: ProcessCreate)' for the process 'OfficeClickToRun.exe'. A red arrow points to the 'Process Create' section in the event details pane. The event pane also shows the following properties: Protokollname: Microsoft-Windows-Sysmon/Operational; Quelle: Sysmon; Protokolliert: 06.09.2020 19:46:15; Aufgabenkategorie: Process Create (rule: ProcessCreate); Ebene: Informationen; Benutzer: SYSTEM; Computer: VMWIN101903; Vorgangscode: Info; Weitere Informationen: [Onlinehilfe](#).

Wenn Sysmon bereits installiert ist, dann laden wir nur noch die DNS-Konfiguration.

sysmon.exe -c dns.xml