



Eigenes Event-Log erstellen

In dieser Anleitung beschreibe ich kurz, wie man ein eigenes Event-Log erstellen kann.

Eine Veranschaulichung der Ereignisanzeige:

Ebene	Datum und Uhrzeit	Quelle	Event-ID	Aufgabenkategorie
Informationen	10.12.2017 17:38:06	Powershell-Skripte	1022 (1)	
Warnung	10.12.2017 17:38:04	Powershell-Skripte	1021 (1)	
Fehler	10.12.2017 17:38:01	Powershell-Skripte	1020 (1)	
Informationen	10.12.2017 17:37:43	SelfServicePlugin	1 Keine	

Ereignis 1021, Powershell-Skripte

Allgemein Details

Dateiüberwachungs-Skript konnte nicht entladen werden

Protokollname: Anwendung
Quelle: Powershell-Skripte
Ereignis-ID: 1021
Ebene: Warnung
Benutzer: Nicht zutreffend
Vorgangscode:
Weitere Informationen: [Onlinehilfe](#)

Mein Ziel ist es, das meine Powershell-Skripte je nach Bedarf, eine Nachricht in der Ereignisanzeige im Anwendungsprotokoll schreiben.

Anwendungsprotokolle z.B. sind

- Application
- Security
- Installation
- System

Mit diesen One-Linern erstellen wir eine neue Source im Bereich Application und hinterlassen dort Nachrichten mit individuellen Event-IDs.

```
# Der Windows Papst https://www.der-windows-papst.de
# Neue Source anlegen:
New-EventLog -LogName Application -Source "Powershell-Skripte"

# EventLog schreiben
Write-EventLog -LogName Application -Source "Powershell-Skripte" -EntryType Error -EventID 1020 -Message "Dateiüberwachungs-Skript konnte nicht gestartet werden"
Write-EventLog -LogName Application -Source "Powershell-Skripte" -EntryType Warning -EventID 1021 -Message "Dateiüberwachungs-Skript konnte nicht entladen werden"
Write-EventLog -LogName Application -Source "Powershell-Skripte" -EntryType Information -EventID 1022 -Message "Dateiüberwachungs-Skript wurde gestartet"
Write-EventLog -LogName Application -Source "Powershell-Skripte" -EntryType Information -EventID 1023 -Message "Dateiüberwachungs-Skript wurde beendet"

# EventLog auslesen
Get-EventLog -LogName Application -Newest 10 | Select-Object -Property Index, TimeGenerated, Timewritten, EventType, Source, CategoryNumber, Message
Get-Eventlog -LogName Application -Entrytype Information -After 09/12/2017 -Newest 5 | Where-Object Message -Like "Dateiüberwachungs*" | Format-Table
Get-WinEvent -FilterHashtable @{LogName="Application";ID=1020}

# Source wieder löschen:
Remove-EventLog -Source "Powershell-Skripte"
```



Eigenes Event-Log erstellen

Das Ergebnis etwas näher betrachtet:

Anwendung Anzahl von Ereignissen: 3.029 (!) Neue Ereignisse sind verfügbar

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	10.12.2017 17:38:09	Powershell-Skripte	1023 (1)	
Informationen	10.12.2017 17:38:06	Powershell-Skripte	1022 (1)	
Warnung	10.12.2017 17:38:04	Powershell-Skripte	1021 (1)	
Fehler	10.12.2017 17:38:01	Powershell-Skripte	1020 (1)	
Informationen	10.12.2017 17:37:43	SelfServicePlugin	1	Keine
Informationen	10.12.2017 17:37:22	Powershell-Skripte	1023 (1)	
Informationen	10.12.2017 17:37:20	Powershell-Skripte	1022 (1)	
Warnung	10.12.2017 17:37:19	Powershell-Skripte	1021 (1)	
Informationen	10.12.2017 17:36:43	SelfServicePlugin	1	Keine
Informationen	10.12.2017 17:27:55	Powershell-Skripte	1020 (1)	

Ereignis 1023, Powershell-Skripte

Allgemein Details

Dateiüberwachungs-Skript wurde beendet

Protokollname: Anwendung
Quelle: Powershell-Skripte
Ereignis-ID: 1023
Ebene: Informationen
Benutzer: Nicht zutreffend
Vorgangscode:
Weitere Informationen: [Onlinehilfe](#)