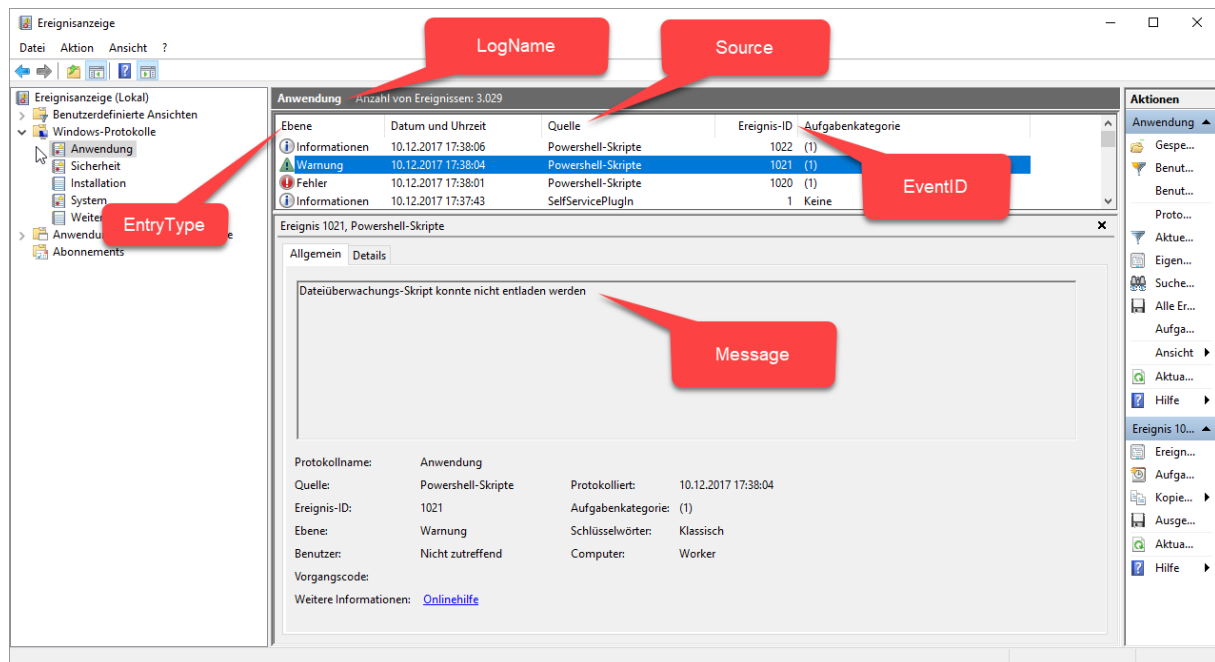




Eigenes Event-Log erstellen

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

Eine Veranschaulichung der Ereignisanzeige:



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  
TimeGenerated,Message -wrap  
Get-WinEvent -FilterHashtable @{LogName="Application";ID=1020}
```

Source wieder löschen:

```
Remove-EventLog -Source "Powershell-Skripte"
```



Eigenes Event-Log erstellen

Das Ergebnis etwas näher betrachtet:

The screenshot shows the Windows Event Viewer interface. At the top, it displays 'Anwendung' and 'Anzahl von Ereignissen: 3.029 (1) Neue Ereignisse sind verfügbar'. Below this is a table of events. The first four rows are highlighted with a red box:

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)

Below the table, the details for 'Ereignis 1023, Powershell-Skripte' are shown. The 'Allgemein' tab is active, displaying the message: 'Dateiüberwachungs-Skript wurde beendet'. Below this, the following metadata is provided:

Protokollname: Anwendung
Quelle: Powershell-Skripte Protokolliert: 10.12.2017 17:38:09
Ereignis-ID: 1023 Aufgabenkategorie: (1)
Ebene: Informationen Schlüsselwörter: Klassisch
Benutzer: Nicht zutreffend Computer: Worker
Vorgangscod:

Weitere Informationen: [Onlinehilfe](#)