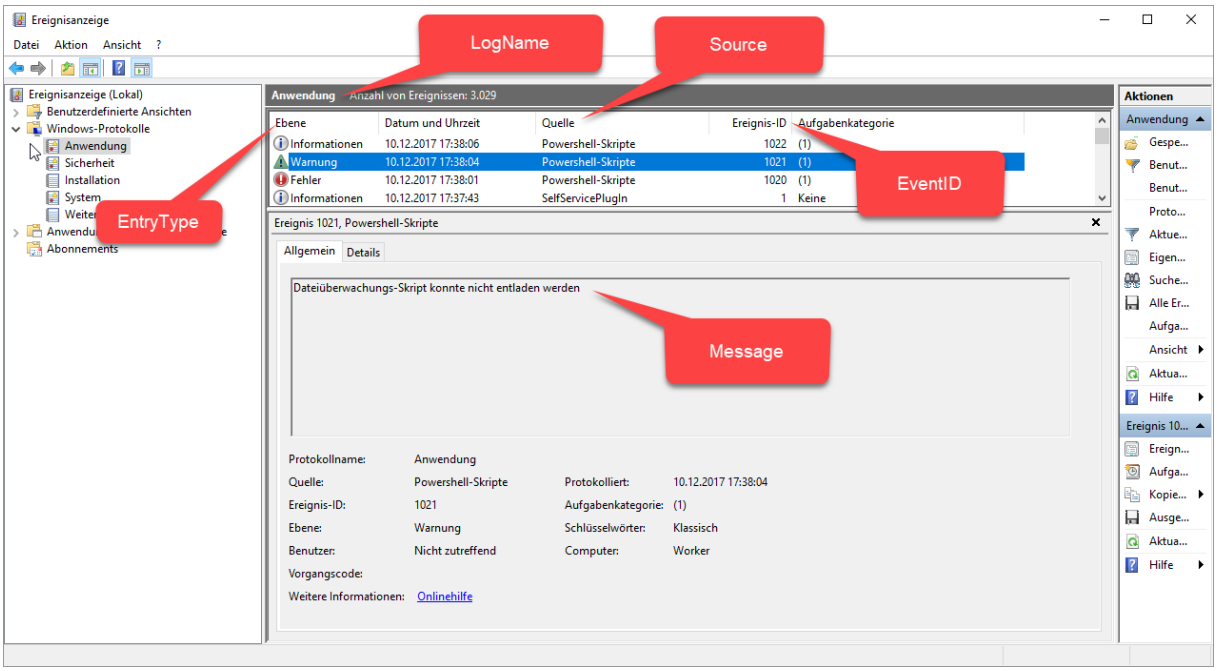
Eigenes Event-Log erstellen

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: