Das Microsoft Tool wevtutil einsetzen

Wer über die Kommandozeile mal schnell ein Ereignis auslesen möchte geht wie folgt vor.

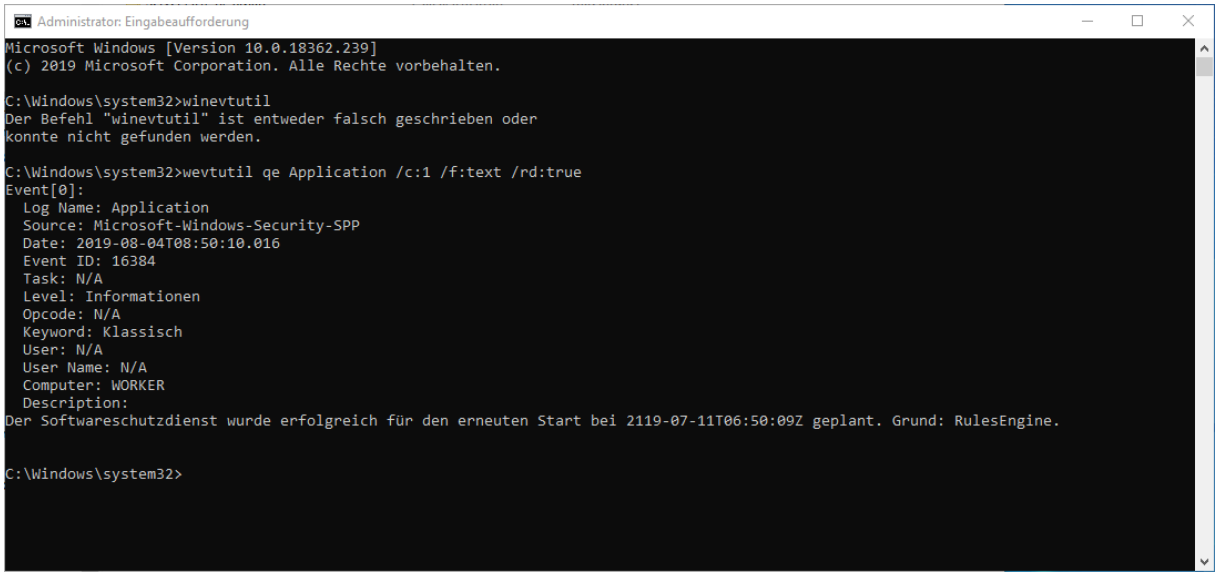
Hier einige Beispiele für den Umgang mit dem Tool wevutil.exe.

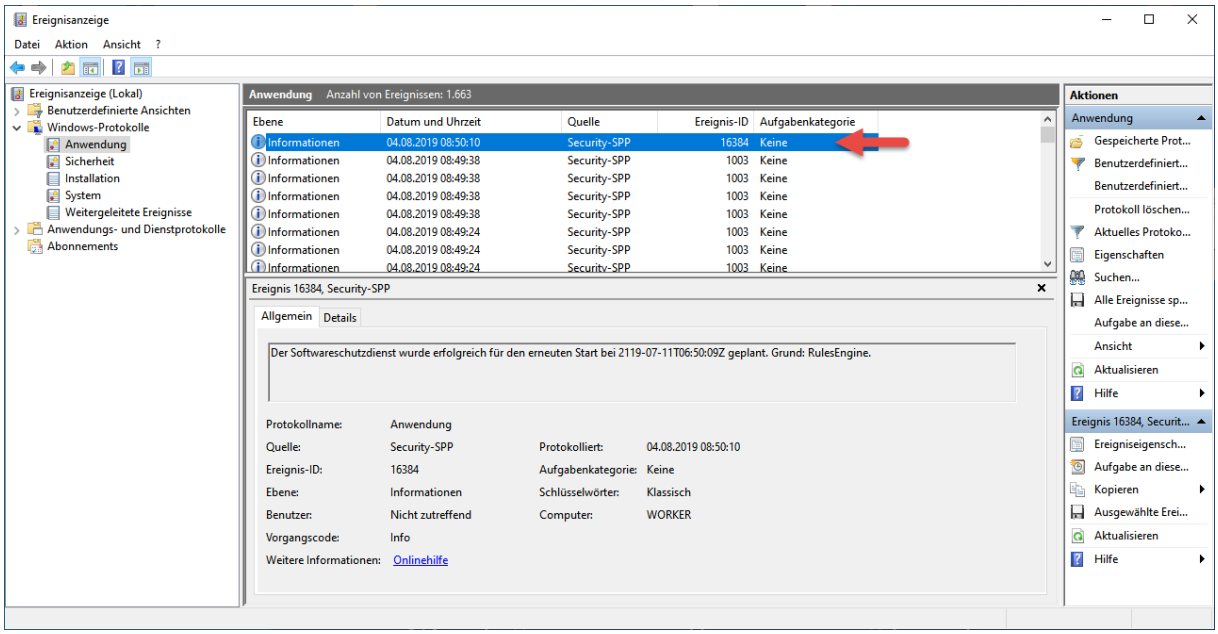
Eine Erklärung zu den gängigen Parametern:

/f: formatiert die Ausgabe in Text
/e: aktiviert oder deaktiviert ein Protokoll über true oder false
qe liest Ereignisse aus
/rd: bestimmt die Richtung der Ereignisse. True sind die neusten und False die älteren
epl exportiert Logs

Liest den letzten Eintrag aus Anwendungen aus und gibt diesen als Text aus.

wevtutil qe Application /c:1 /f:text /rd:true

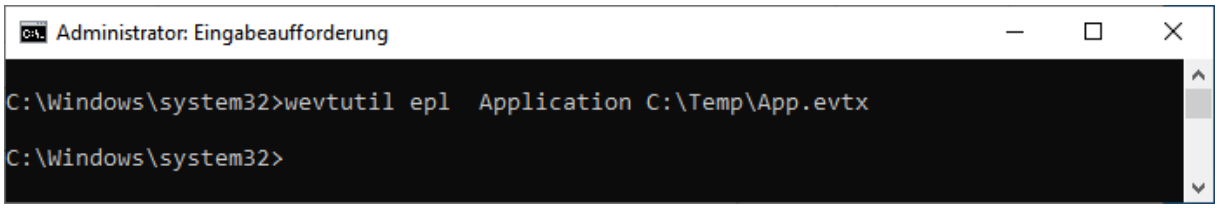


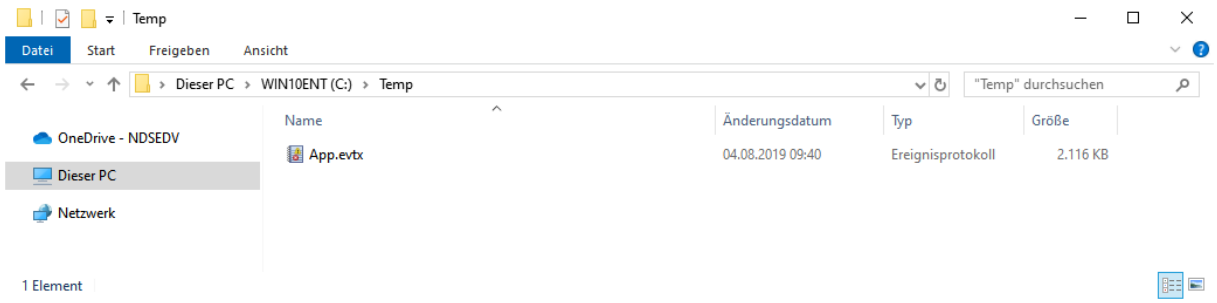


Das Microsoft Tool wevtutil einsetzen

Exportiert alle Ereignisse aus Anwendungen

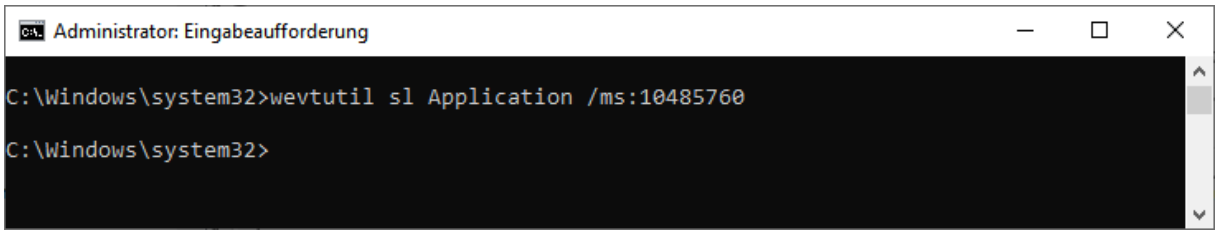
wevtutil epl Application C:\Temp\App.evtx

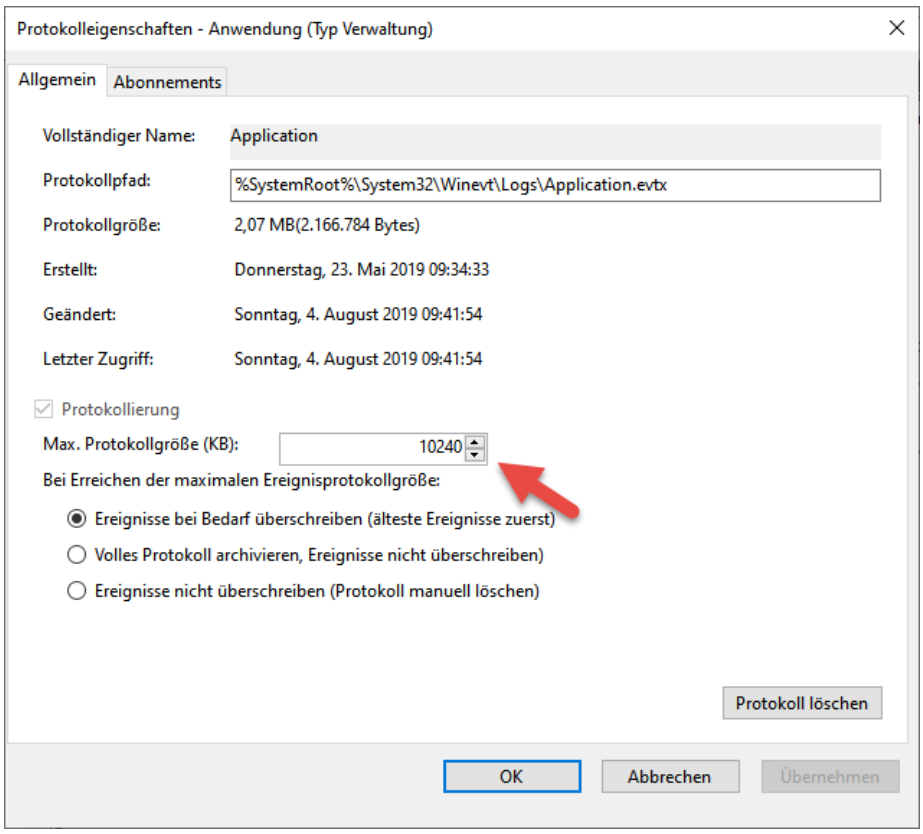




Setzt die maximale Größe für Anwendungen auf 10 MB fest.

wevtutil sl Application /ms:10485760



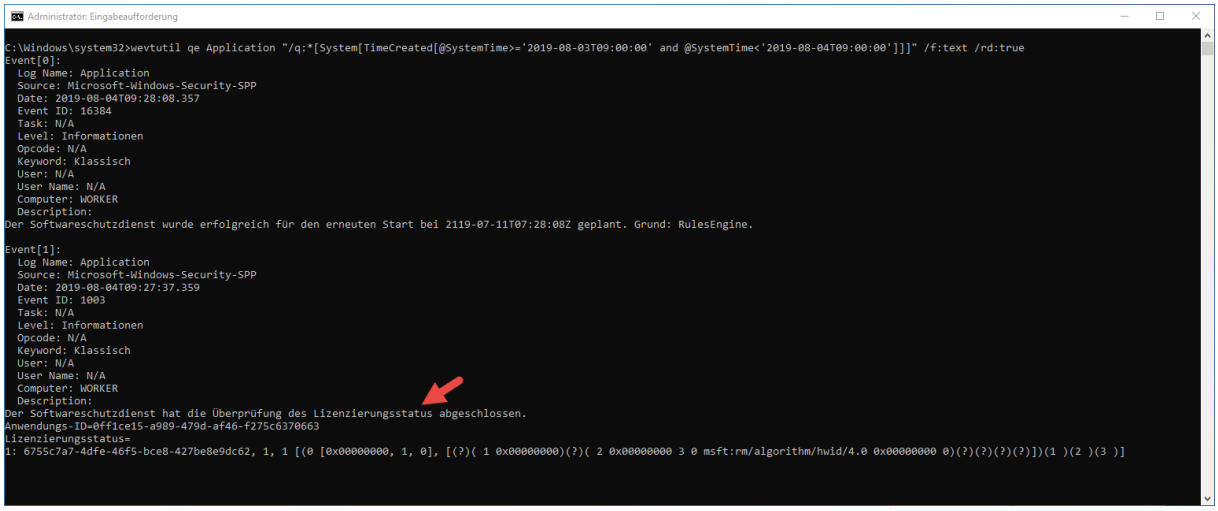


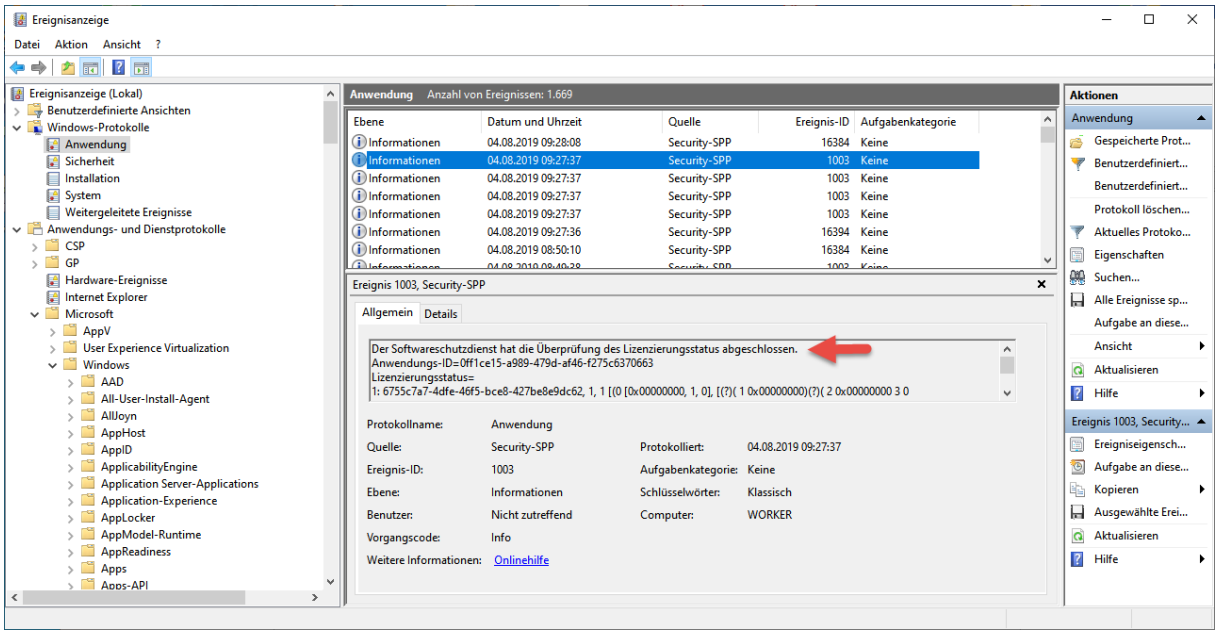
Erstellt von Jörn Walter **02.08.2019**

Das Microsoft Tool wevtutil einsetzen

Gibt die Ereignisse der letzten 24 Stunden aus, die neusten zuerst.

wevtutil qe Application "/q:*[System[TimeCreated[@SystemTime>='2019-08-03T09:00:00' and @SystemTime<'2019-08-04T09:00:00']]]" /f:text /rd:true

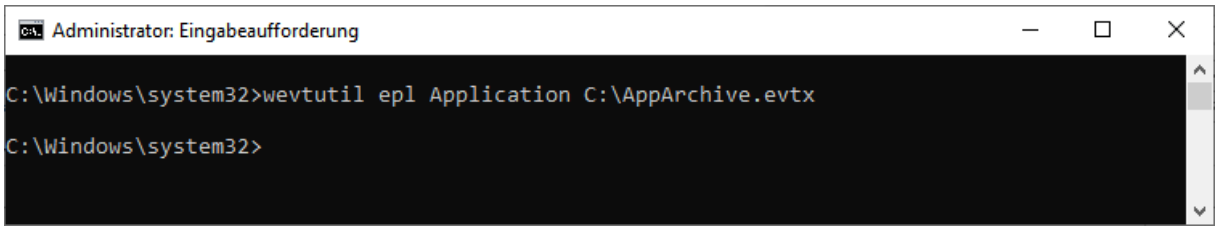


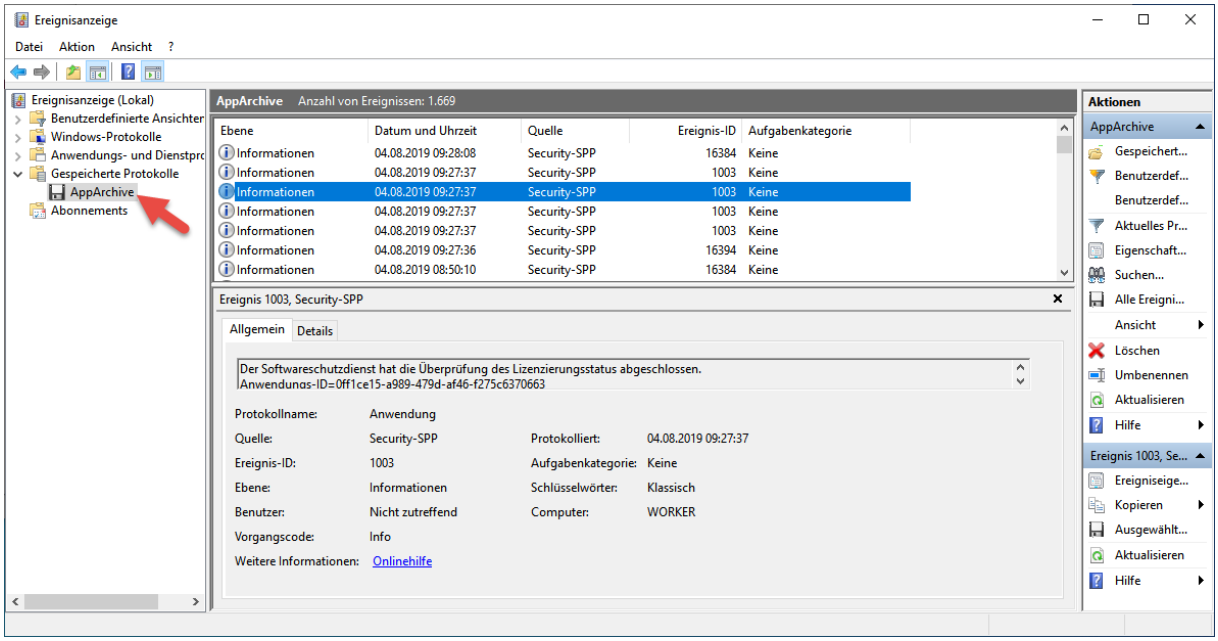


Das Microsoft Tool wevtutil einsetzen

Archiviert Ereignisse aus einem Ereignisprotokoll

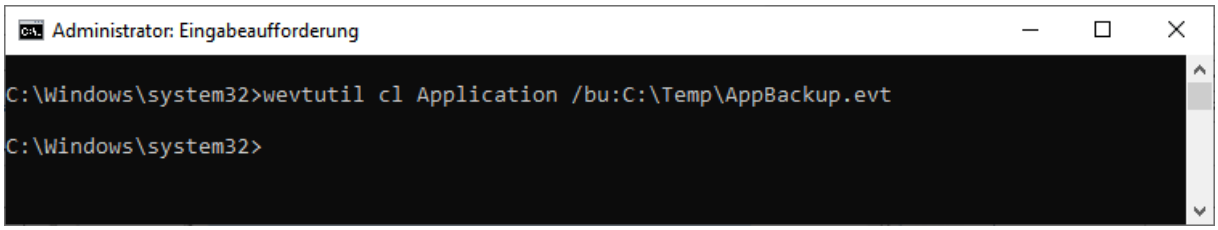
wevtutil epl Application C:\Temp\AppArchive.evtx



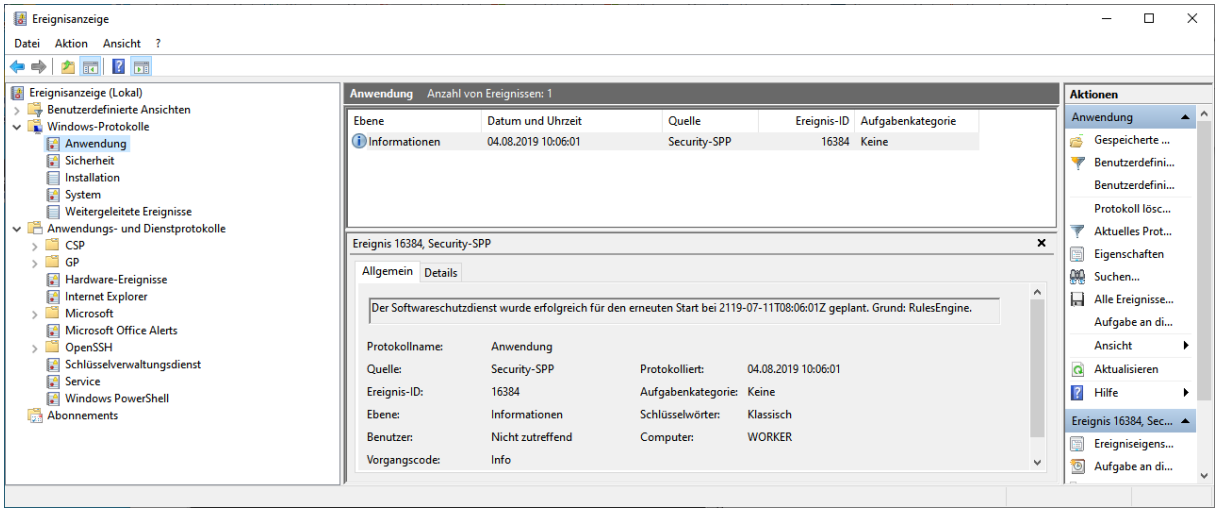


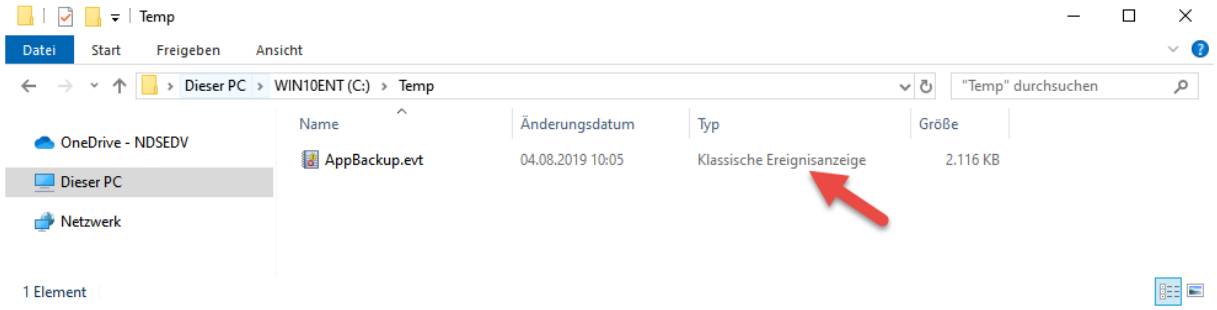
Protokoll löschen aber vorher sichern

wevtutil cl Application /bu:C:\Temp\AppBackup.evt oder evtx



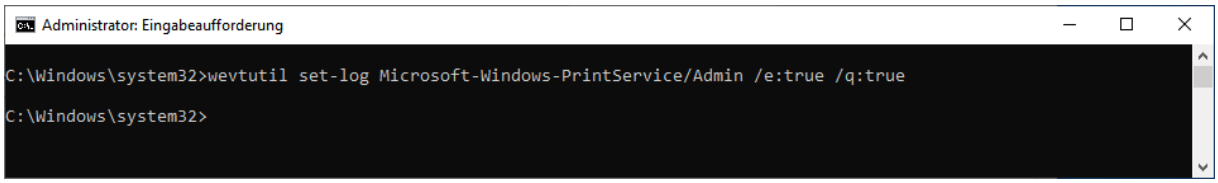
Das Microsoft Tool wevtutil einsetzen

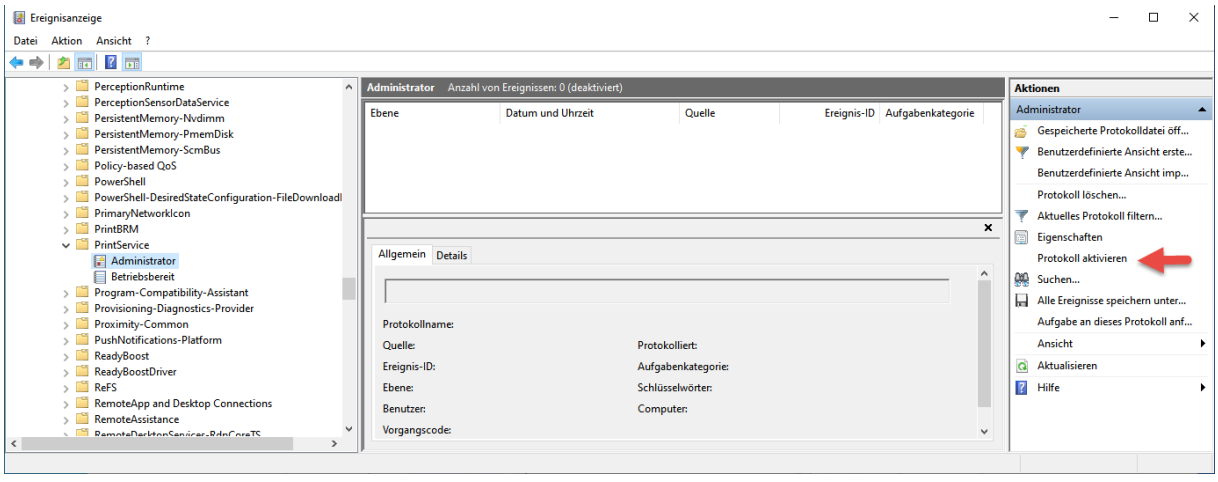




Ein Protokoll aktivieren

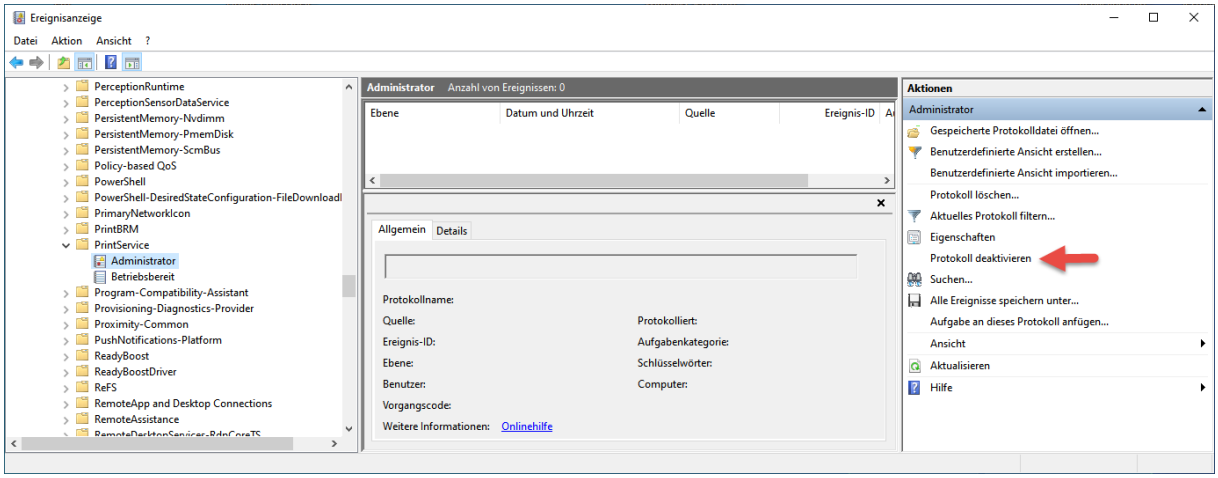
wevtutil set-log Microsoft-Windows-PrintService/Admin /e:true /q:true





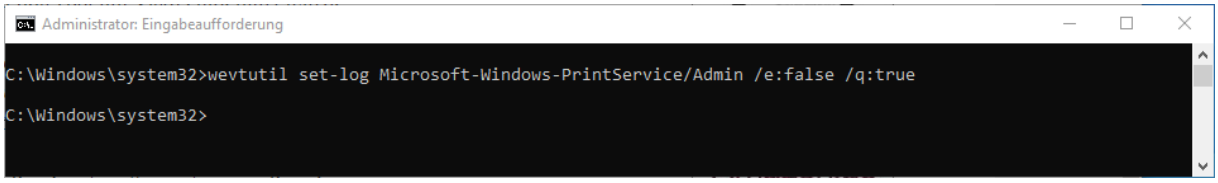
Erstellt von Jörn Walter **02.08.2019**

Das Microsoft Tool wevtutil einsetzen



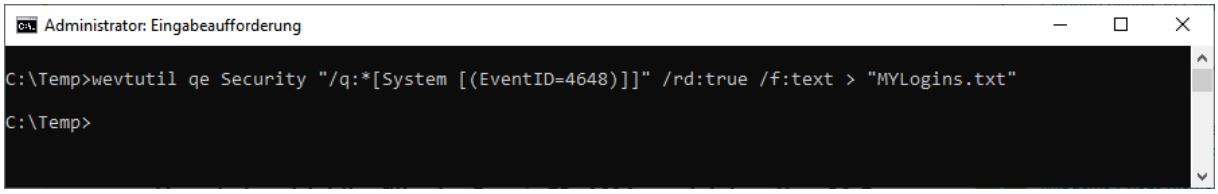
Ein Protokoll wieder deaktivieren

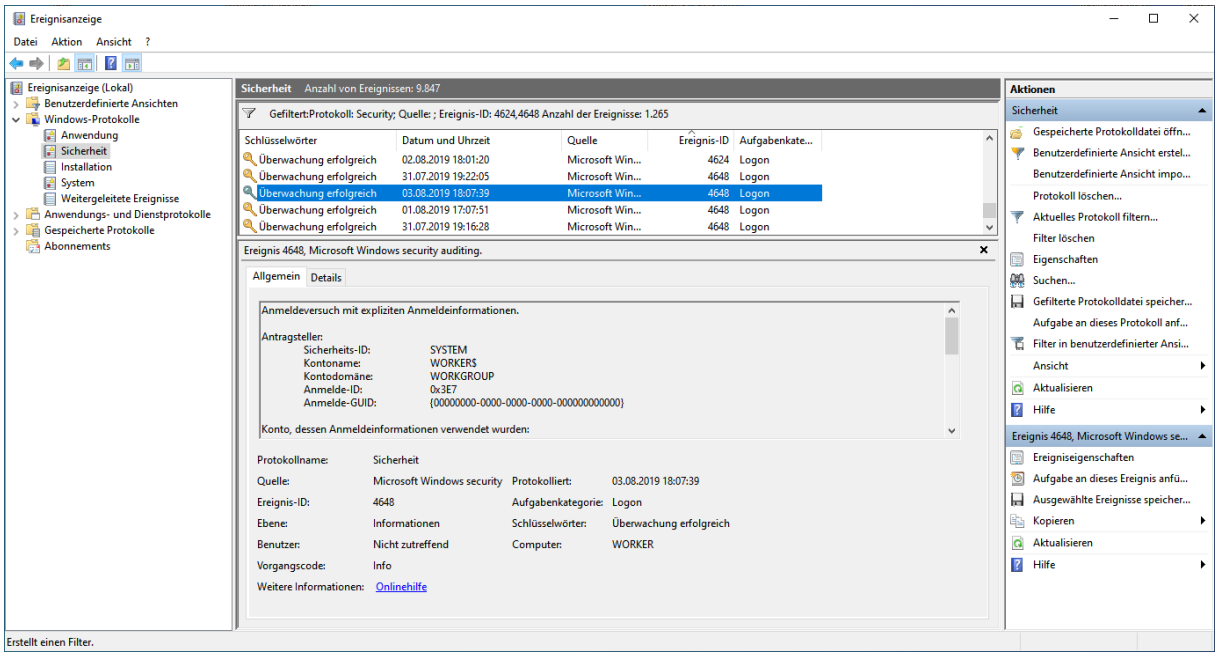
wevtutil set-log Microsoft-Windows-PrintService/Admin /e:false /q:true



Eine Abfrage nach einer ID filtern

wevtutil qe Security "/q:*[System [(EventID=4648)]]" /rd:true /f:text > "MYLogins.txt"
wevtutil qe Security "/q:*[System [(EventID=4624)]]" /rd:true /f:text > "MYLogins.txt"





Erstellt von Jörn Walter **02.08.2019**

Das Microsoft Tool wevtutil einsetzen

Abfrage

Die Basics:

- wevtutil el
  - gibt eine Liste aller Ereignisprotokolle aus
- wevtutil ep
  - gibt eine Liste aller Event-Publisher aus

Erstellt von Jörn Walter **02.08.2019**