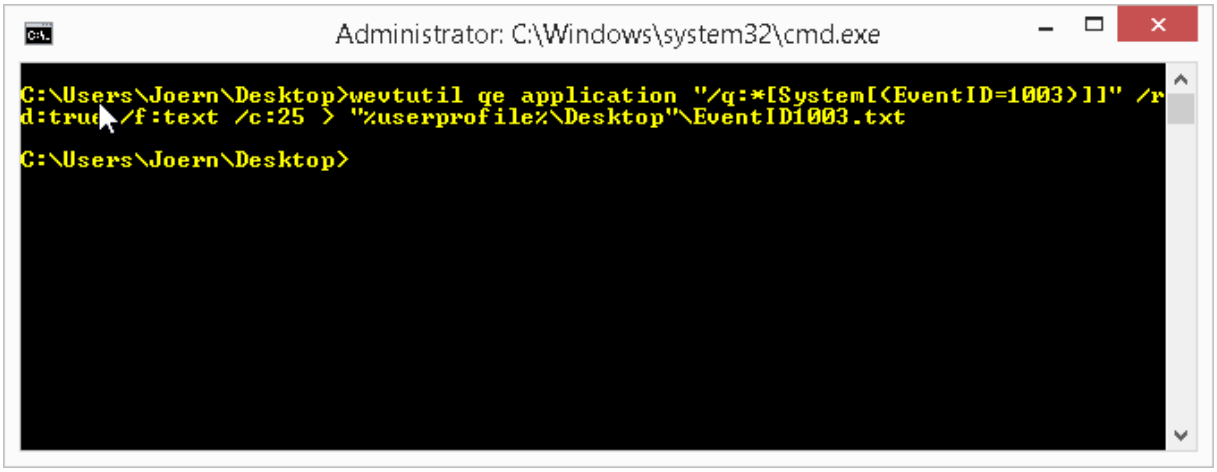
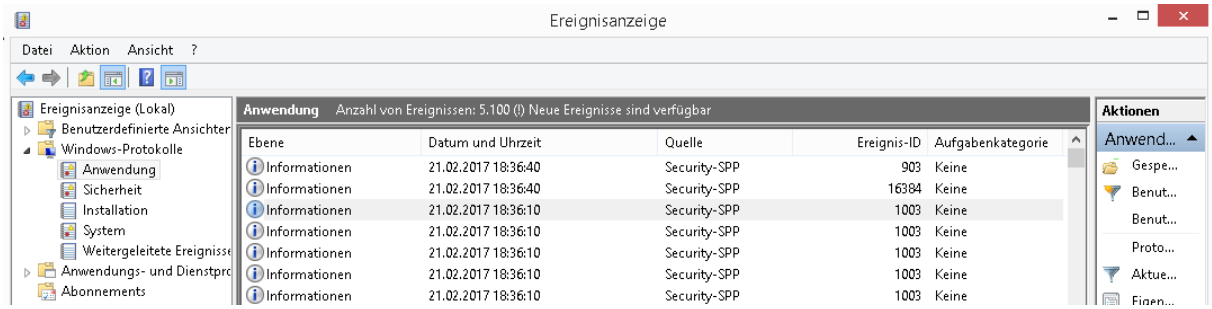
Windows - Event Log filtern (parsen)

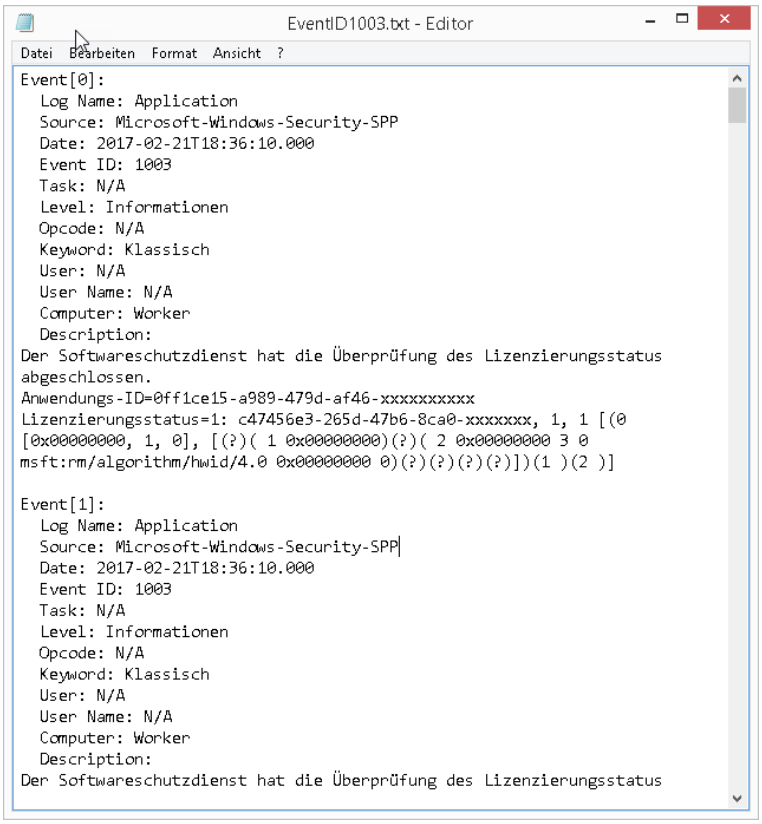
Mit diesem Befehl können wir Events aus dem Application-Log nach einer belieben ID und Anzahl filtern.

```
wevtutil qe application "/q:*[System[(EventID=1003)]]" /rd:true /f:text /c:25 > "%userprofile%\Desktop"\EventID1003.txt
```





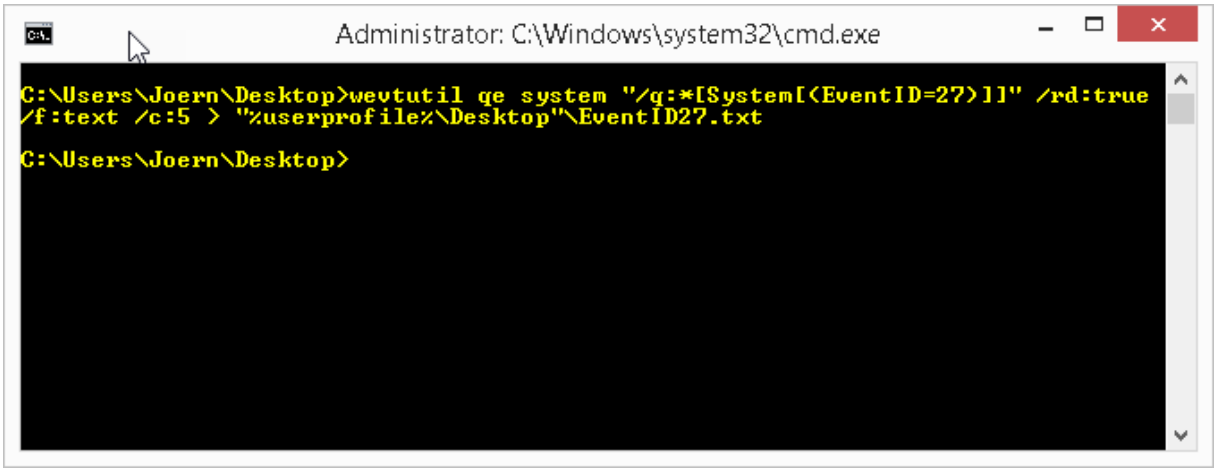
Log:

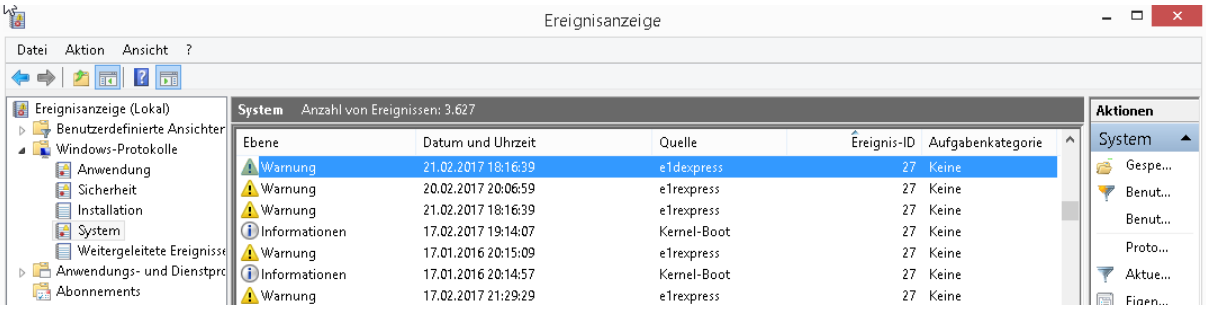


Windows - Event Log filtern (parsen)

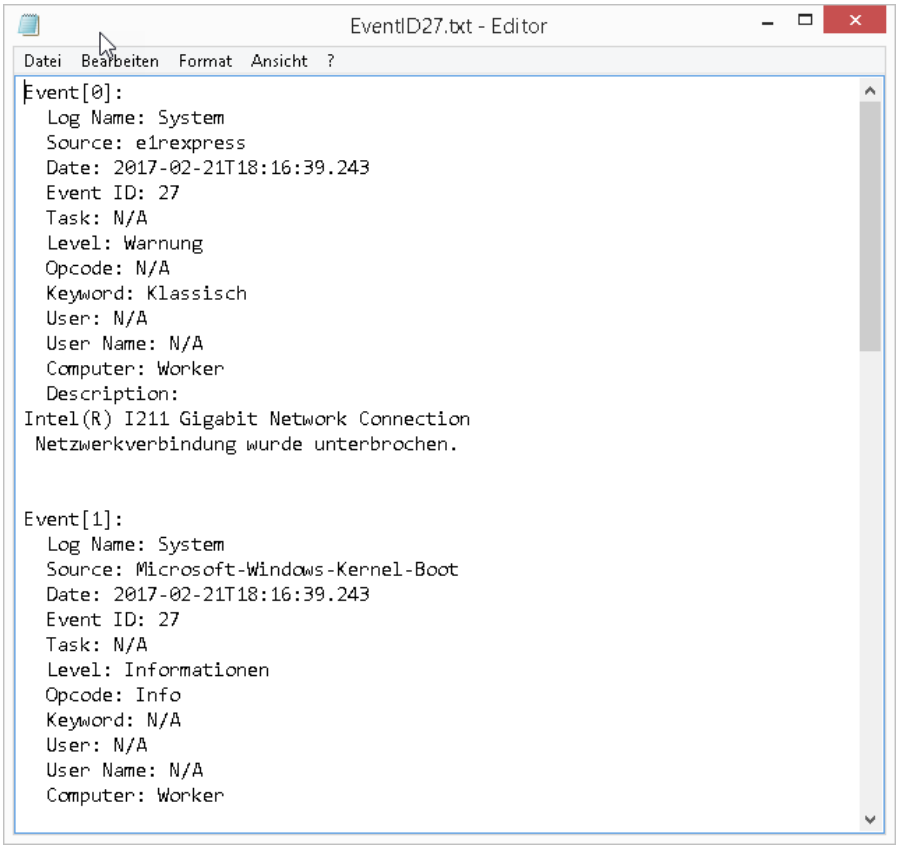
Gerne auch das Event 27 aus dem System-Log und zwar nur die letzten 5

wevtutil qe system "/q:*[System[(EventID=27)]]" /rd:true /f:text /c:5 > "%userprofile%\Desktop"\EventID27.txt



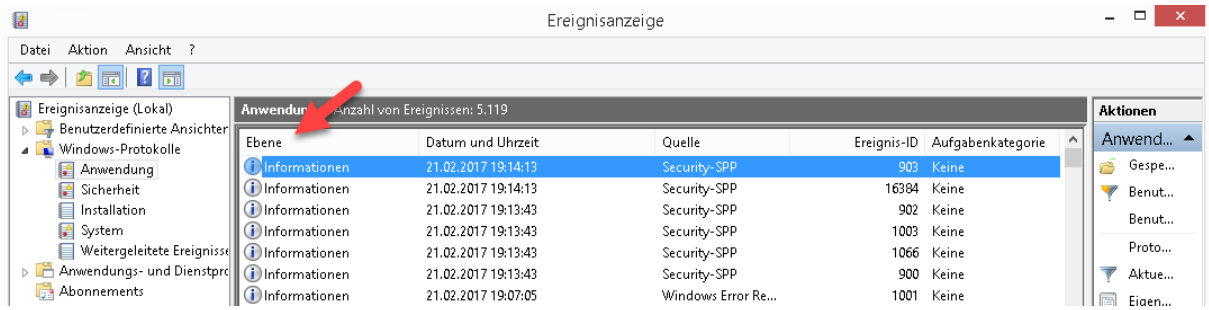


Log:



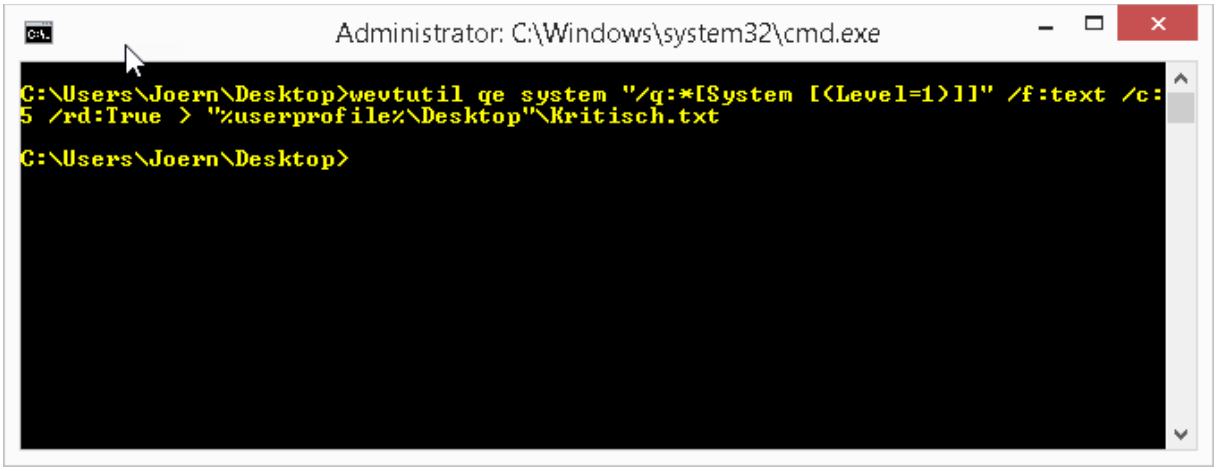
Windows - Event Log filtern (parsen)

Das Ganze kann man sich aber auch nach Ebenen anzeigen bzw. exportieren lassen:

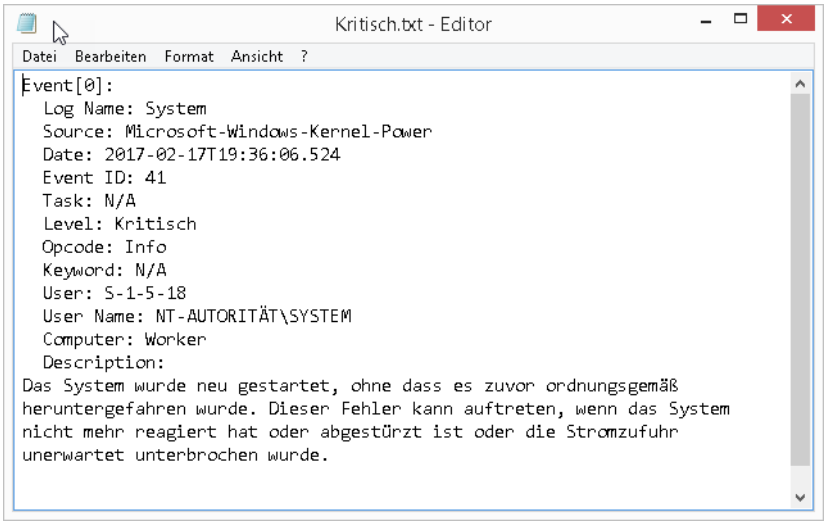


Level 1 = Kritisch Level 2 = Fehler Level 3 = Warnung Level 4 = Information

```
wevtutil qe system "/q:*[System [(Level=1)]]" /f:text /c:5 /rd:True > "%userprofile%\Desktop"\Kritisch.txt

wevtutil qe system "/q:*[System [(Level=2)]]" /f:text /c:5 /rd:True > "%userprofile%\Desktop"\Fehler.txt

wevtutil qe system "/q:*[System [(Level=3)]]" /f:text /c:5 /rd:True > "%userprofile%\Desktop"\Warnung.txt

wevtutil qe system "/q:*[System [(Level=4)]]" /f:text /c:5 /rd:True > "%userprofile%\Desktop"\Information.txt
```



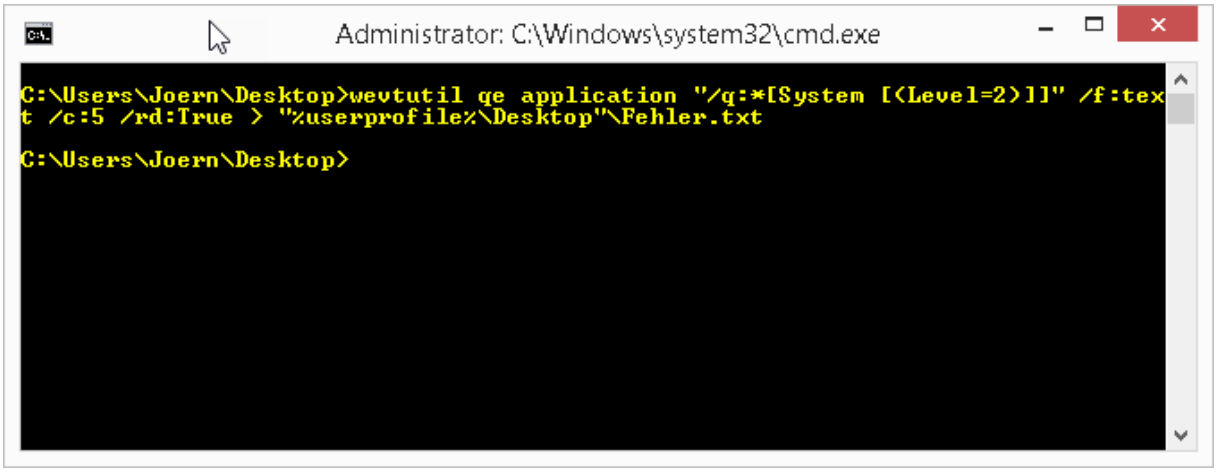
Log:



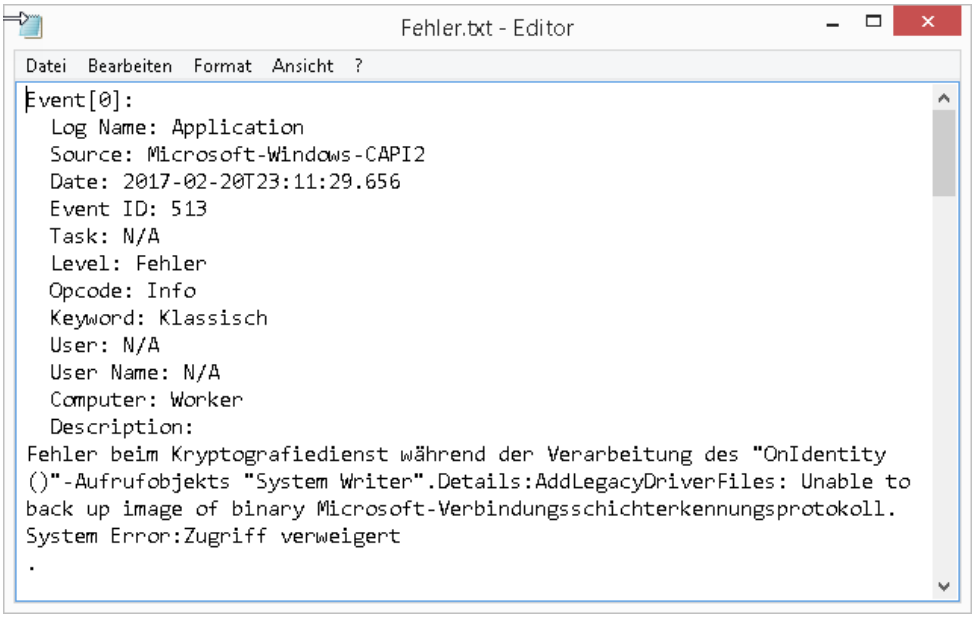
Windows - Event Log filtern (parsen)

Oder nur den Events über den Level Fehler aus dem Application Log.

wevtutil qe application "/q:*[System [(Level=2)]]" /f:text /c:5 /rd:True > "%userprofile%\Desktop"\Fehler.txt



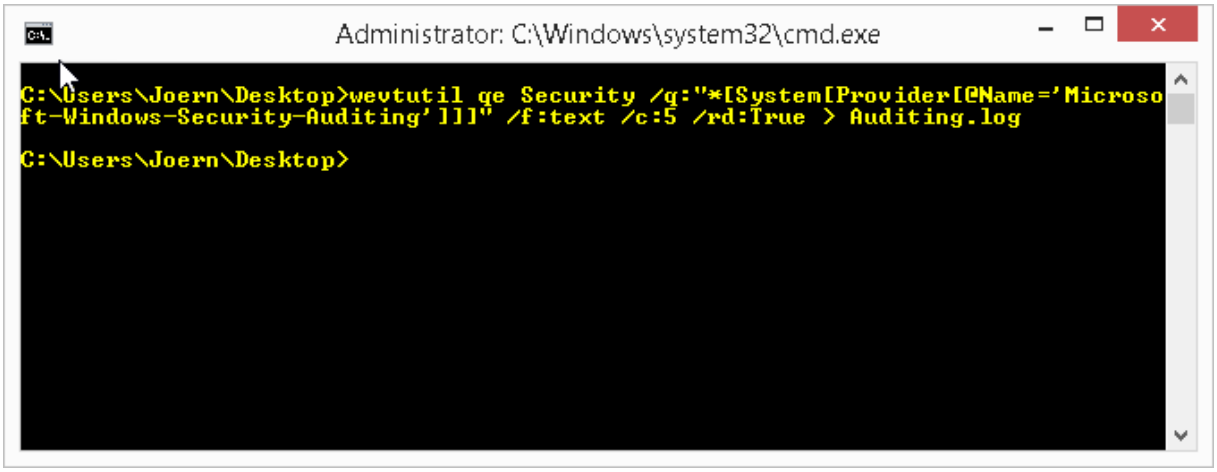
Log:

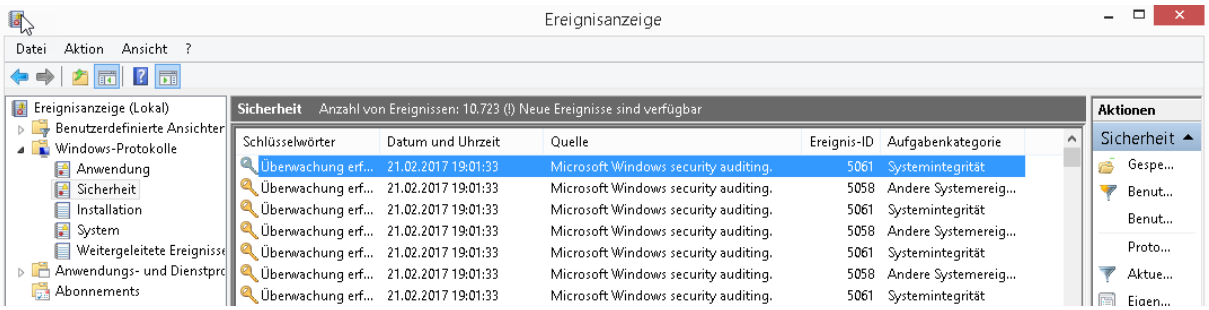


Windows - Event Log filtern (parsen)

Gerne auch nach der Kategorie Provider. In diesem Beispiel aus dem Bereich Auditing.

wevtutil qe Security /q:"*[System[Provider[@Name='Microsoft-Windows-Security-Auditing']]]" /f:text /c:5 /rd:True > Auditing.log

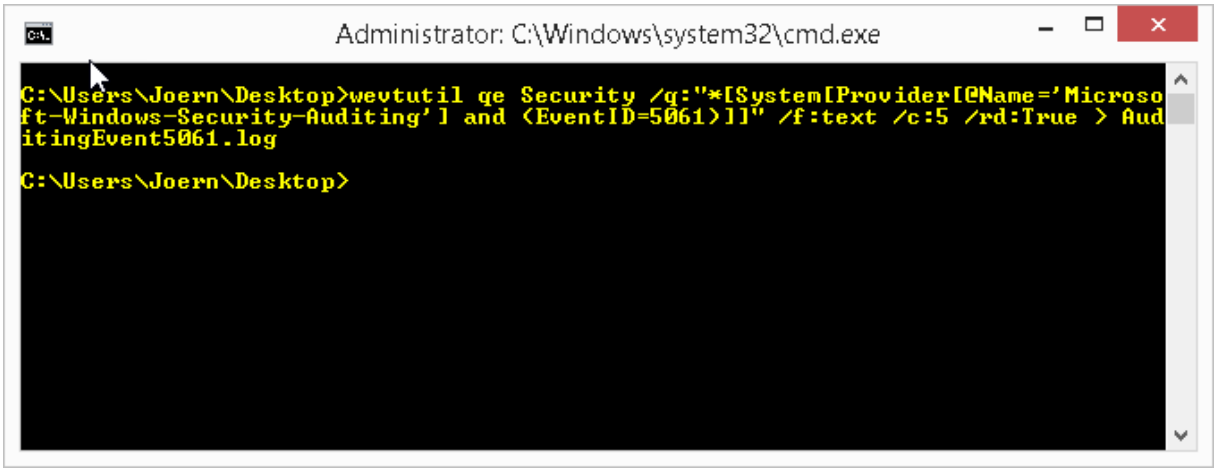


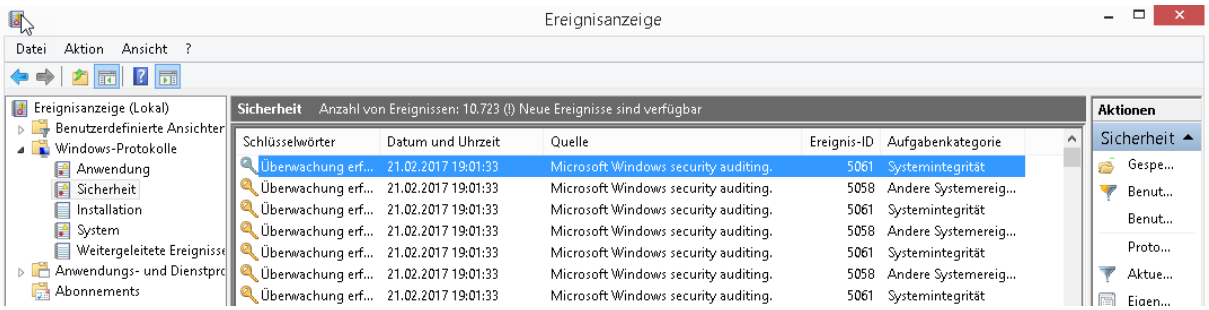


Windows - Event Log filtern (parsen)

Oder gefiltert nach der EventID5061:

wevtutil qe Security /q:"*[System[Provider[@Name='Microsoft-Windows-Security-Auditing'] and (EventID=5061)]]" /f:text /c:5 /rd:True > AuditingEvent5061.log





Log: