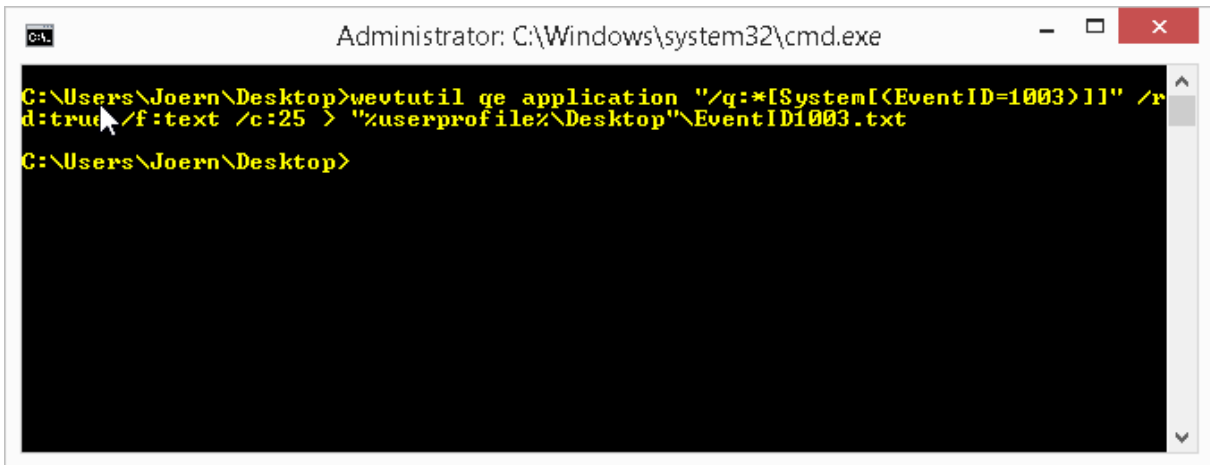


Windows - Event Log filtern (parsen)

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

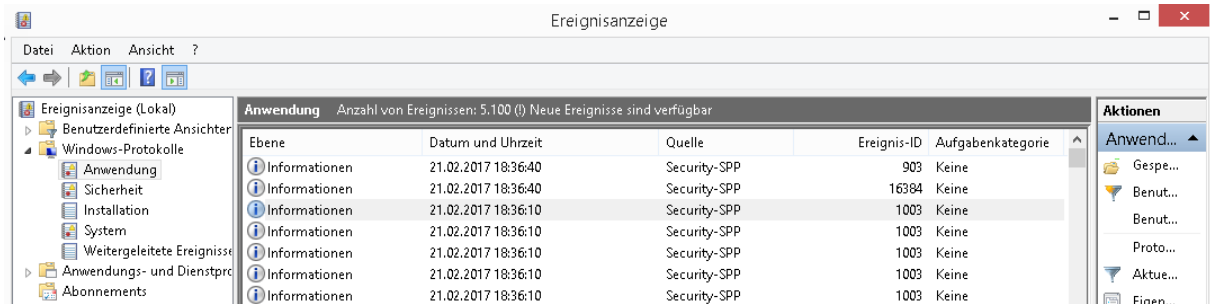
```
wevtutil qe application "/q:*[System[(EventID=1003)]]" /rd:true /f:text /c:25 > "%userprofile%\Desktop"\EventID1003.txt
```



```
Administrator: C:\Windows\system32\cmd.exe

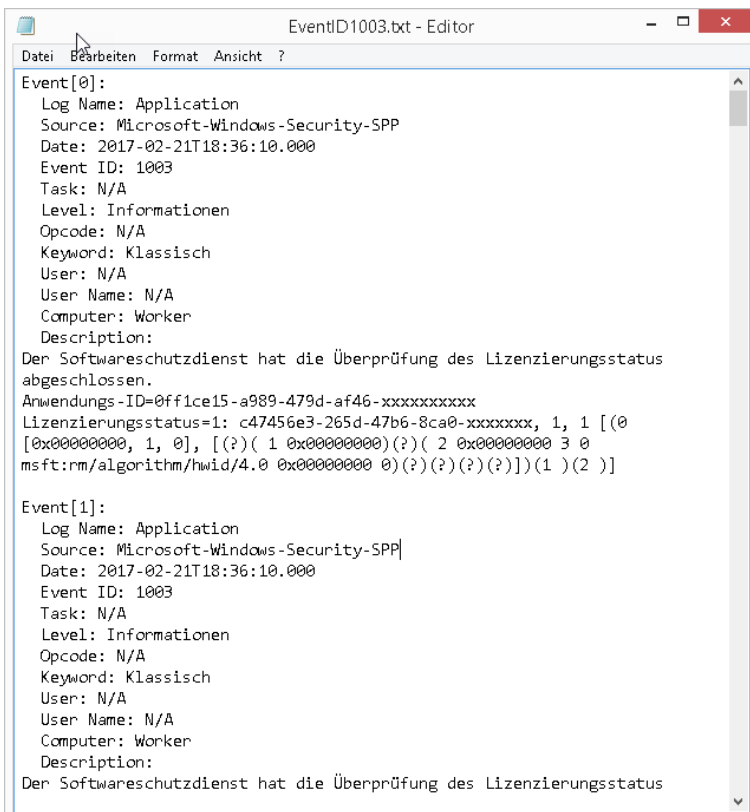
C:\Users\Joern\Desktop>wevtutil qe application "/q:*[System[(EventID=1003)]]" /rd:true /f:text /c:25 > "%userprofile%\Desktop"\EventID1003.txt

C:\Users\Joern\Desktop>
```



Anwendung	Anzahl von Ereignissen: 5.100 (0) Neue Ereignisse sind verfügbar			
Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	21.02.2017 18:36:40	Security-SPP	903	Keine
Informationen	21.02.2017 18:36:40	Security-SPP	16384	Keine
Informationen	21.02.2017 18:36:10	Security-SPP	1003	Keine
Informationen	21.02.2017 18:36:10	Security-SPP	1003	Keine
Informationen	21.02.2017 18:36:10	Security-SPP	1003	Keine
Informationen	21.02.2017 18:36:10	Security-SPP	1003	Keine
Informationen	21.02.2017 18:36:10	Security-SPP	1003	Keine
Informationen	21.02.2017 18:36:10	Security-SPP	1003	Keine

Log:



```
EventID1003.txt - Editor

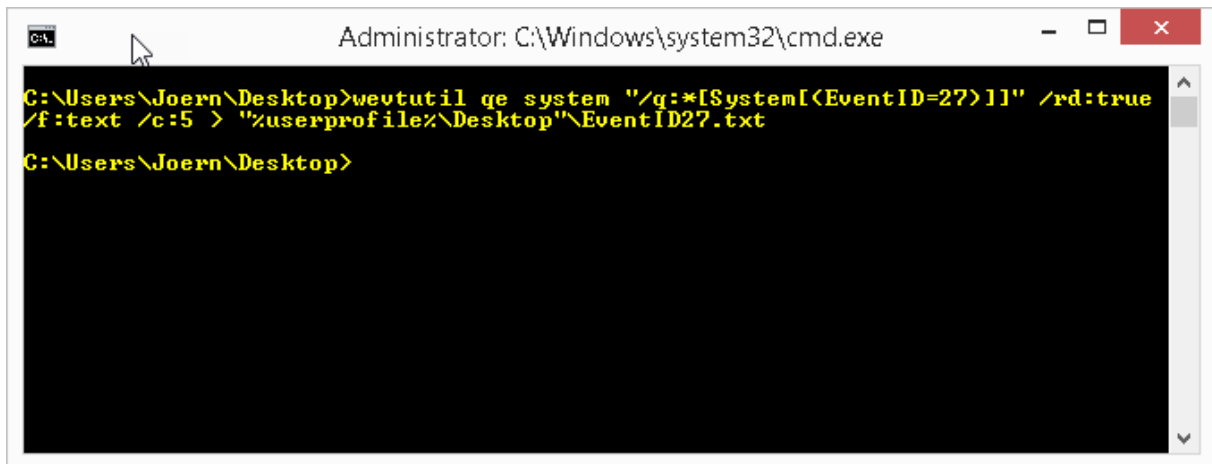
Event[0]:
  Log Name: Application
  Source: Microsoft-Windows-Security-SPP
  Date: 2017-02-21T18:36:10.000
  Event ID: 1003
  Task: N/A
  Level: Informationen
  Opcode: N/A
  Keyword: Klassisch
  User: N/A
  User Name: N/A
  Computer: Worker
  Description:
  Der Softwareschutzdienst hat die Überprüfung des Lizenzierungsstatus abgeschlossen.
  Anwendungs-ID=0ff1ce15-a989-479d-af46-xxxxxxxxxxx
  Lizenzierungsstatus=1: c47456e3-265d-47b6-8ca0-xxxxxxx, 1, 1 [(0 [0x00000000, 1, 0], [(?)( 1 0x00000000)(?)( 2 0x00000000 3 0 msft:rm/algorithm/hwid/4.0 0x00000000 0)(?)(?)(?)(?))(1 )(2 )]

Event[1]:
  Log Name: Application
  Source: Microsoft-Windows-Security-SPP
  Date: 2017-02-21T18:36:10.000
  Event ID: 1003
  Task: N/A
  Level: Informationen
  Opcode: N/A
  Keyword: Klassisch
  User: N/A
  User Name: N/A
  Computer: Worker
  Description:
  Der Softwareschutzdienst hat die Überprüfung des Lizenzierungsstatus
```

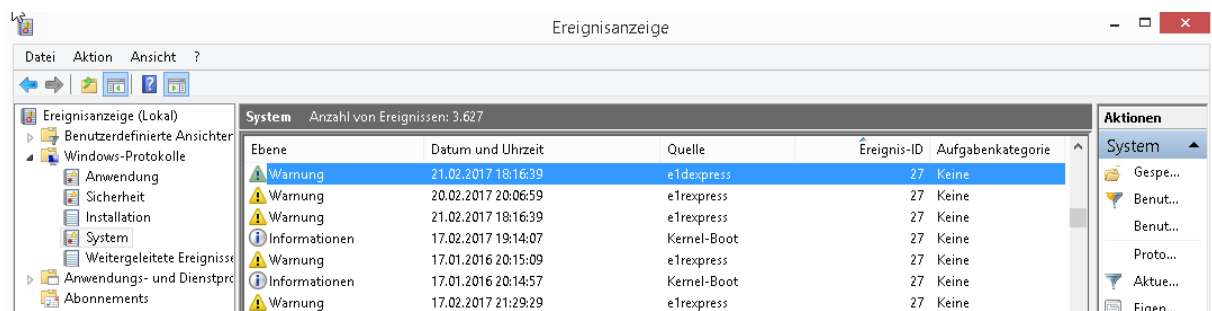
Windows - Event Log filtern (parsen)

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

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

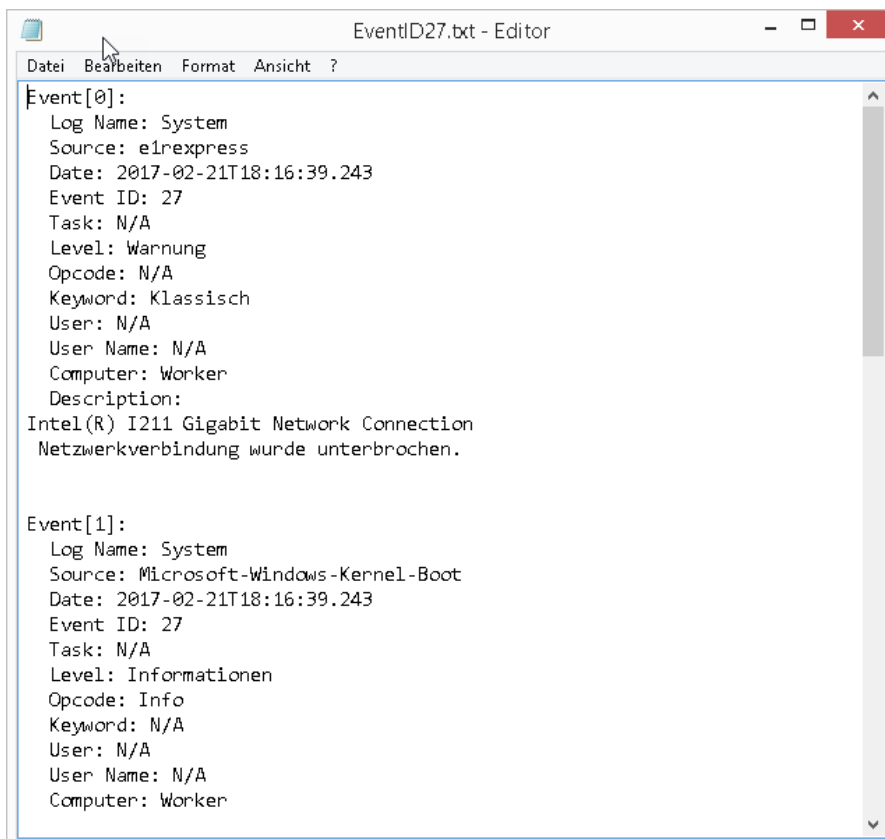


```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Joern\Desktop>wevtutil ql system "/q:*[System[(EventID=27)]]" /rd:true
/f:text /c:5 > "%userprofile%\Desktop"\EventID27.txt
C:\Users\Joern\Desktop>
```



Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Warnung	21.02.2017 18:16:39	e1nexpress	27	Keine
Warnung	20.02.2017 20:06:59	e1nexpress	27	Keine
Warnung	21.02.2017 18:16:39	e1nexpress	27	Keine
Informationen	17.02.2017 19:14:07	Kernel-Boot	27	Keine
Warnung	17.01.2016 20:15:09	e1nexpress	27	Keine
Informationen	17.01.2016 20:14:57	Kernel-Boot	27	Keine
Warnung	17.02.2017 21:29:29	e1nexpress	27	Keine

Log:

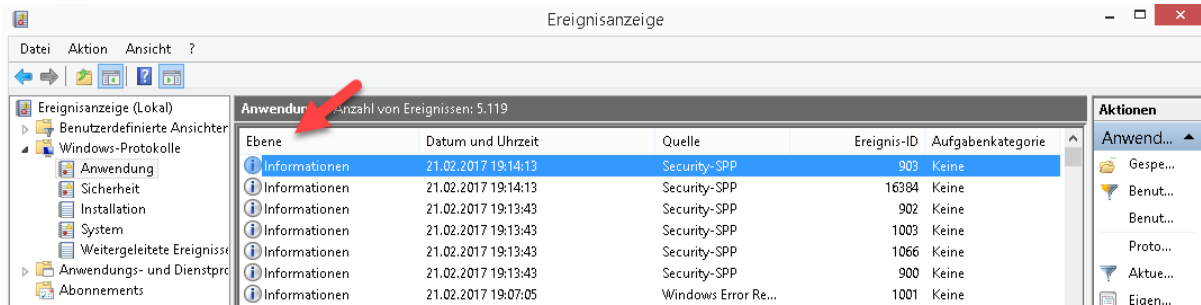


```
Event[0]:
  Log Name: System
  Source: e1nexpress
  Date: 2017-02-21T18:16:39.243
  Event ID: 27
  Task: N/A
  Level: Warnung
  Opcode: N/A
  Keyword: Klassisch
  User: N/A
  User Name: N/A
  Computer: Worker
  Description:
  Intel(R) I211 Gigabit Network Connection
  Netzwerkverbindung wurde unterbrochen.

Event[1]:
  Log Name: System
  Source: Microsoft-Windows-Kernel-Boot
  Date: 2017-02-21T18:16:39.243
  Event ID: 27
  Task: N/A
  Level: Informationen
  Opcode: Info
  Keyword: N/A
  User: N/A
  User Name: N/A
  Computer: Worker
```

Windows - Event Log filtern (parsen)

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



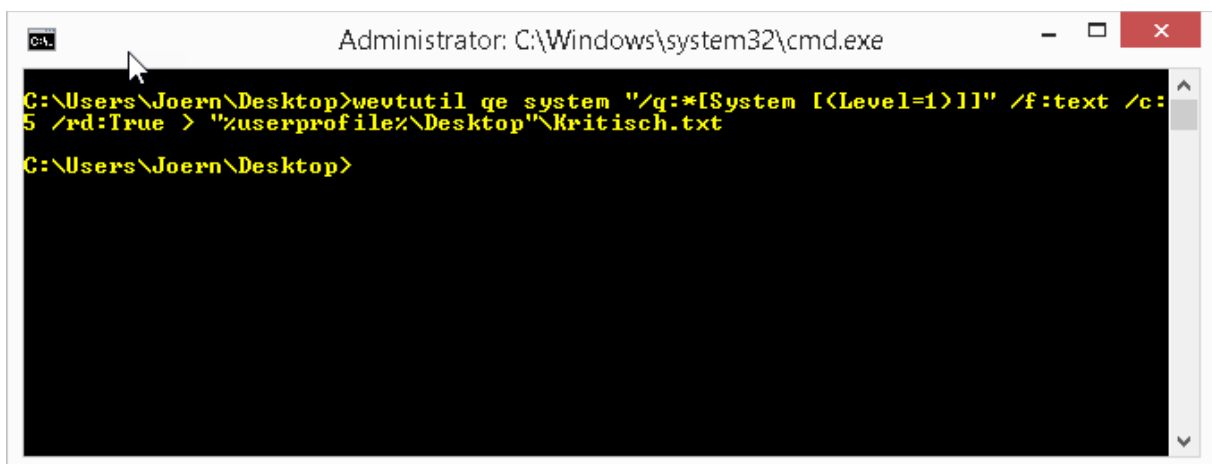
Level 1 = Kritisch Level 2 = Fehler Level 3 = Warnung Level 4 = Information

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

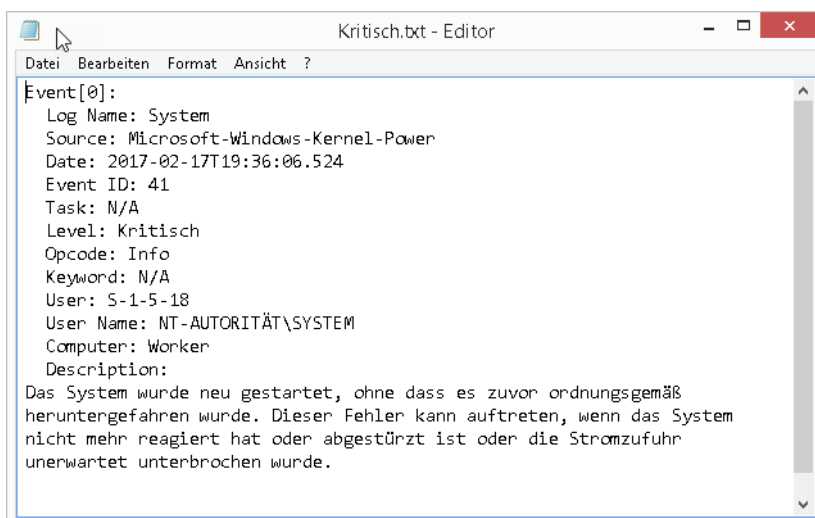
```
wevtutil qe system "/q:*[System [(Level=2)]]" /f:text /c:5 /rd:True > "%userprofile%\Desktop"\Fehler.txt
```

```
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
```



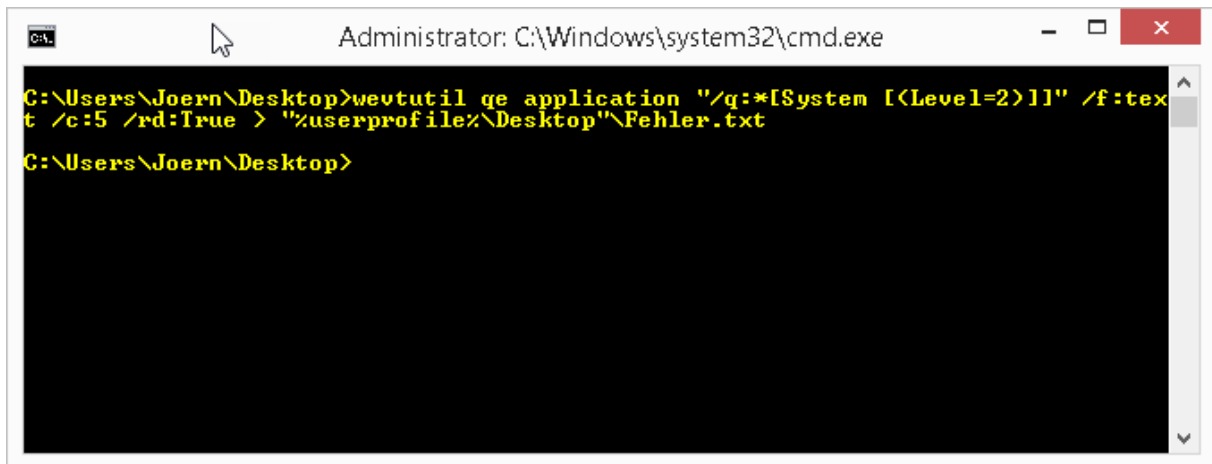
Log:



Windows - Event Log filtern (parsen)

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

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

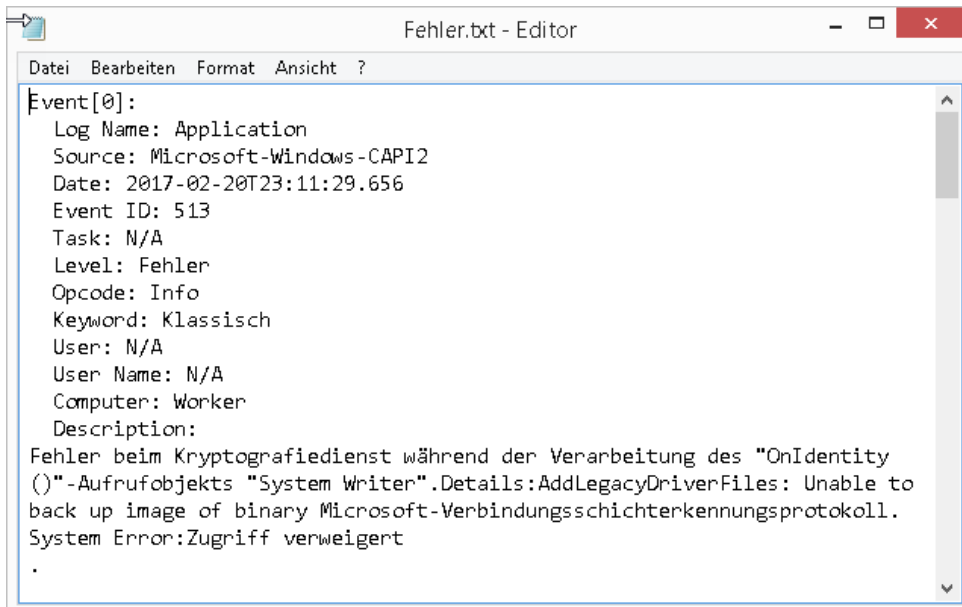


```
Administrator: C:\Windows\system32\cmd.exe

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

C:\Users\Joern\Desktop>
```

Log:



```
Fehler.txt - Editor

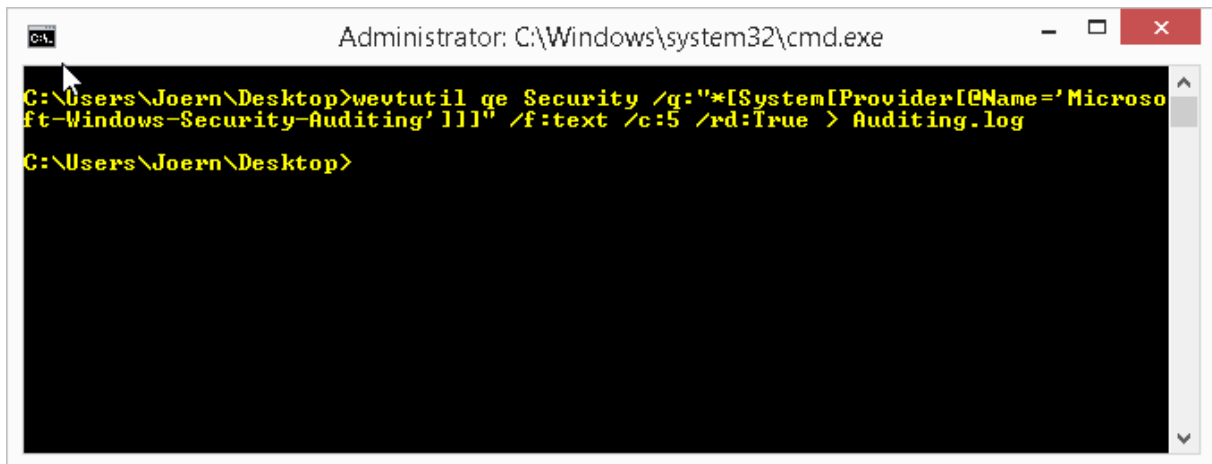
Datei Bearbeiten Format Ansicht ?

Event[0]:
  Log Name: Application
  Source: Microsoft-Windows-CAPI2
  Date: 2017-02-20T23:11:29.656
  Event ID: 513
  Task: N/A
  Level: Fehler
  Opcode: Info
  Keyword: Klassisch
  User: N/A
  User Name: N/A
  Computer: Worker
  Description:
  Fehler beim Kryptografiedienst während der Verarbeitung des "OnIdentity
  ()"-Aufrufobjekts "System Writer".Details:AddLegacyDriverFiles: Unable to
  back up image of binary Microsoft-Verbindungsschichterkennungprotokoll.
  System Error:Zugriff verweigert
  .
```

Windows - Event Log filtern (parsen)

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

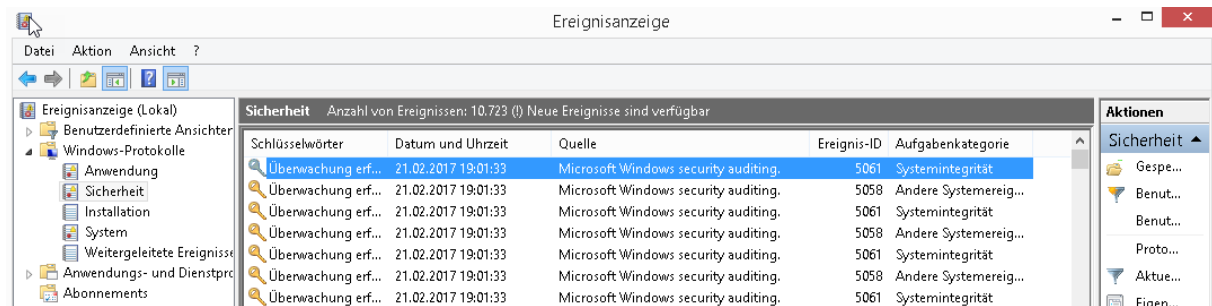
```
wevtutil qe Security /q:"*[System[Provider[@Name='Microsoft-Windows-Security-Auditing']]]" /f:text /c:5 /rd:True > Auditing.log
```



```
Administrator: C:\Windows\system32\cmd.exe

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

C:\Users\Joern\Desktop>
```



Ereignisanzeige

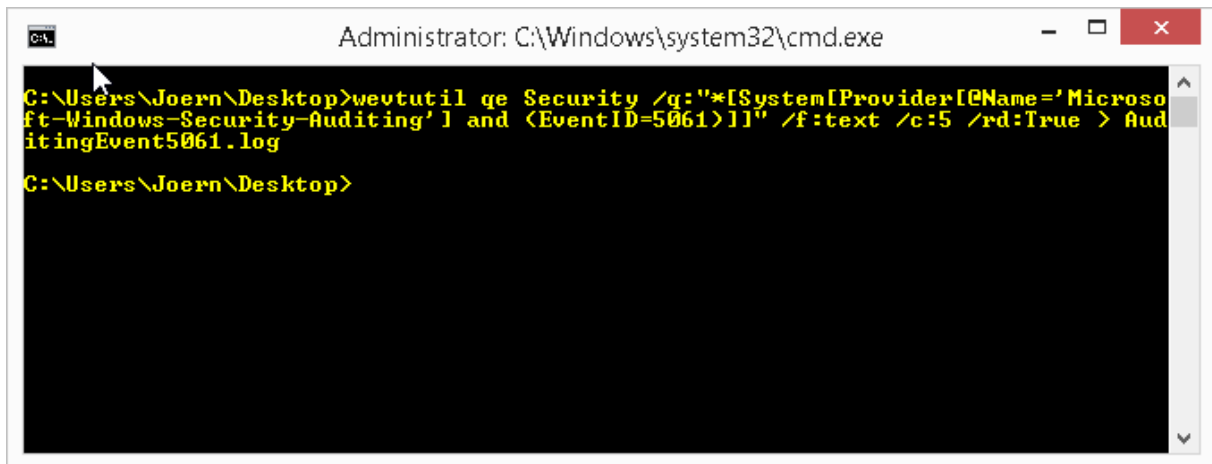
Sicherheit Anzahl von Ereignissen: 10.723 (1) Neue Ereignisse sind verfügbar

Schlüsselwörter	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Überwachung erf...	21.02.2017 19:01:33	Microsoft Windows security auditing.	5061	Systemintegrität
Überwachung erf...	21.02.2017 19:01:33	Microsoft Windows security auditing.	5058	Andere Systemereig...
Überwachung erf...	21.02.2017 19:01:33	Microsoft Windows security auditing.	5061	Systemintegrität
Überwachung erf...	21.02.2017 19:01:33	Microsoft Windows security auditing.	5058	Andere Systemereig...
Überwachung erf...	21.02.2017 19:01:33	Microsoft Windows security auditing.	5061	Systemintegrität
Überwachung erf...	21.02.2017 19:01:33	Microsoft Windows security auditing.	5058	Andere Systemereig...
Überwachung erf...	21.02.2017 19:01:33	Microsoft Windows security auditing.	5061	Systemintegrität

Windows - Event Log filtern (parsen)

Oder gefiltert nach der EventID5061:

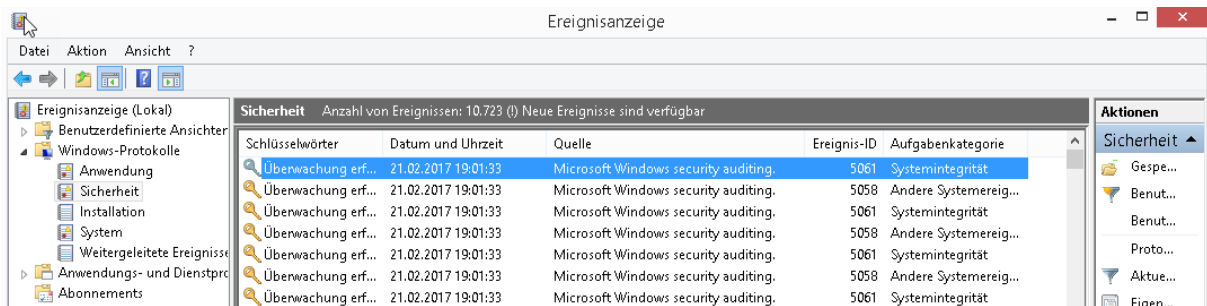
```
wevtutil qe Security /q:"*[System[Provider[@Name='Microsoft-Windows-Security-Auditing']] and (EventID=5061)]" /f:text /c:5 /rd:True > AuditingEvent5061.log
```



```
Administrator: C:\Windows\system32\cmd.exe

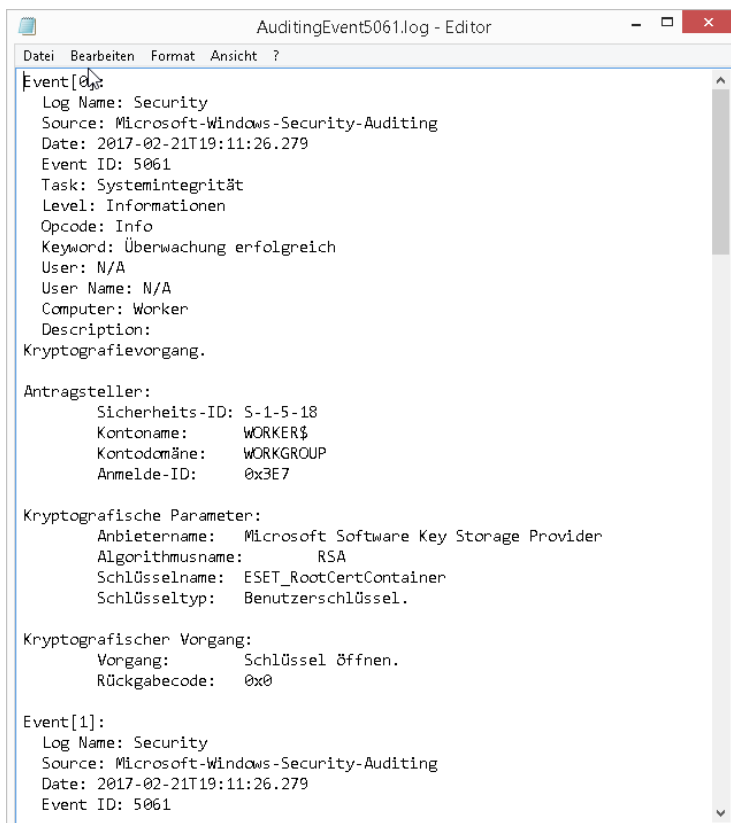
C:\Users\Joern\Desktop>wevtutil qe Security /q:"*[System[Provider[@Name='Microsoft-Windows-Security-Auditing']] and (EventID=5061)]" /f:text /c:5 /rd:True > AuditingEvent5061.log

C:\Users\Joern\Desktop>
```



Schlüsselwörter	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Überwachung erf...	21.02.2017 19:01:33	Microsoft Windows security auditing.	5061	Systemintegrität
Überwachung erf...	21.02.2017 19:01:33	Microsoft Windows security auditing.	5058	Andere Systemereig...
Überwachung erf...	21.02.2017 19:01:33	Microsoft Windows security auditing.	5061	Systemintegrität
Überwachung erf...	21.02.2017 19:01:33	Microsoft Windows security auditing.	5058	Andere Systemereig...
Überwachung erf...	21.02.2017 19:01:33	Microsoft Windows security auditing.	5061	Systemintegrität
Überwachung erf...	21.02.2017 19:01:33	Microsoft Windows security auditing.	5058	Andere Systemereig...
Überwachung erf...	21.02.2017 19:01:33	Microsoft Windows security auditing.	5061	Systemintegrität

Log:



```
AuditingEvent5061.log - Editor

Event[0]:
  Log Name: Security
  Source: Microsoft-Windows-Security-Auditing
  Date: 2017-02-21T19:11:26.279
  Event ID: 5061
  Task: Systemintegrität
  Level: Informationen
  Opcode: Info
  Keyword: Überwachung erfolgreich
  User: N/A
  User Name: N/A
  Computer: Worker
  Description:
  Kryptografievorgang.

  Antragsteller:
    Sicherheits-ID: S-1-5-18
    Kontoname: WORKER$
    Kontodomäne: WORKGROUP
    Anmelde-ID: 0x3E7

  Kryptografische Parameter:
    Anbietername: Microsoft Software Key Storage Provider
    Algorithmusname: RSA
    Schlüsselname: ESET_RootCertContainer
    Schlüsseltyp: Benutzerschlüssel.

  Kryptografischer Vorgang:
    Vorgang: Schlüssel öffnen.
    Rückgabecode: 0x0

Event[1]:
  Log Name: Security
  Source: Microsoft-Windows-Security-Auditing
  Date: 2017-02-21T19:11:26.279
  Event ID: 5061
```