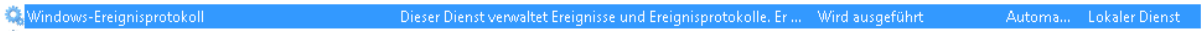
Windows - Event Log Dienst startet nicht

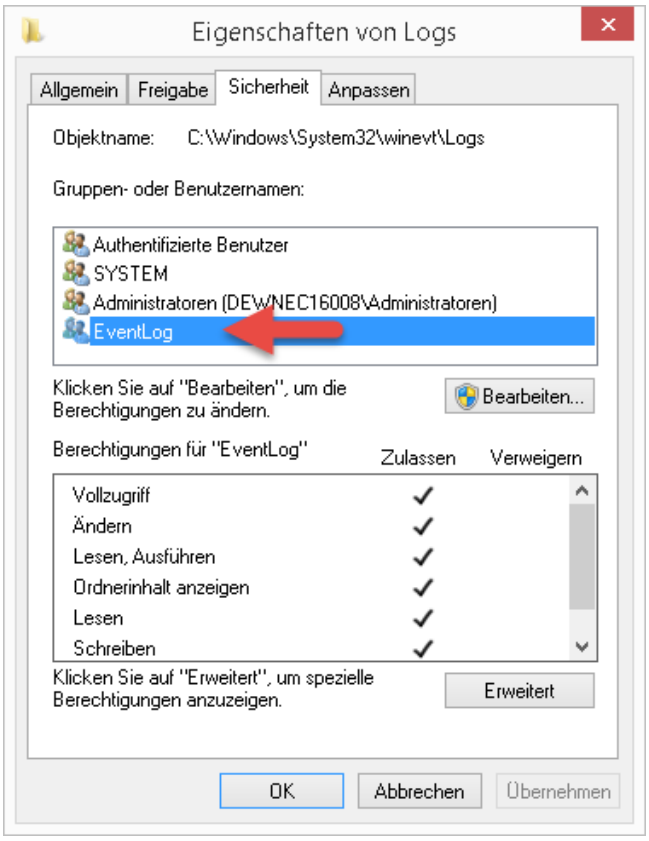
Das Windows-Ereignisprotokoll lässt sich nicht starten.



Das kann darin liegen, das durch Microsoft Security Patches vor 2 Wochen der

- NT SERVICE\EventLog oder SYSTEM

  User aus dem Ordner %SystemRoot%\System32\winevt\logs entfernt wurde.



User Hinzufügen und den Dienst durchstarten.

Wenn das nicht zum Erfolg führen sollte, dann fügen wir den LOCAL SERVICE oder/und NETWORK SERVICE und starten den Dienst noch einmal durch.

Als letzten Mittel übertragen wir die ACLs von einer funktionierenden Maschine auf die Problembüchse. Dazu wechseln wir in die CMD und navigieren zum Pfad %SystemRoot%\SYSTEM32

icacls winevt* /save aclexport /T

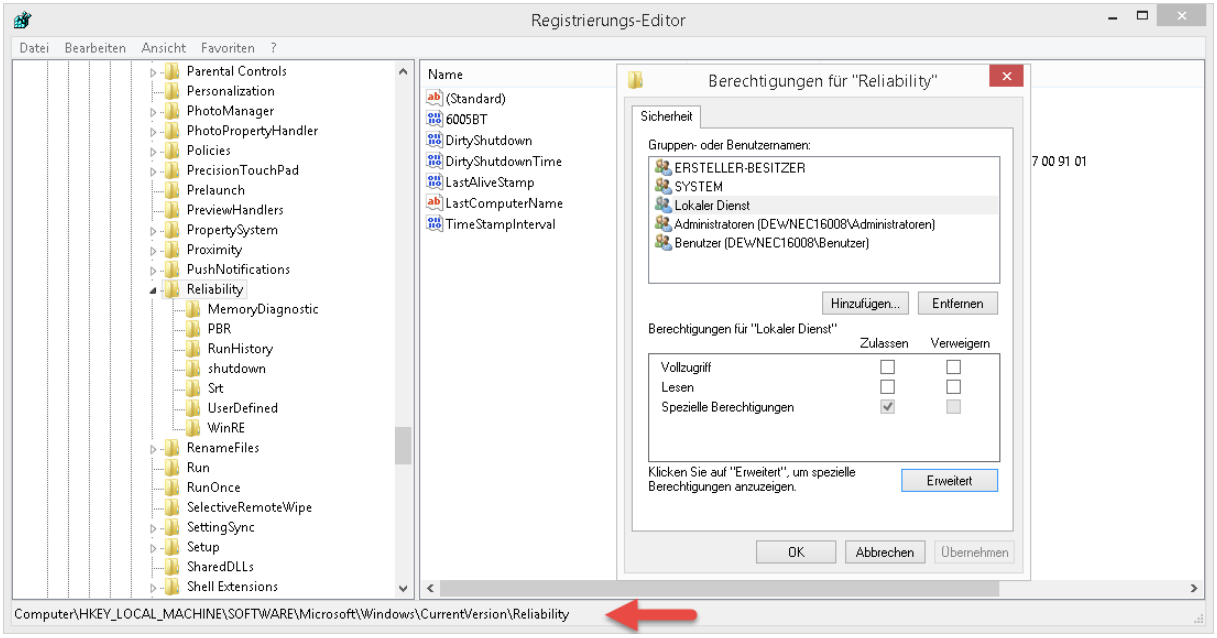
icacls winevt\ /restore aclexport

Erstellt von Jörn Walter – 31.01.2017

Windows - Event Log Dienst startet nicht

Öffnen die Registry und prüfen die Berechtigungen auf diesem Pfad:

HKLM\Software\Microsoft\Windows\CurrentVersion\Reliability



Die Default Berechtigungen sollten wie folgt aussehen:

- CREATOR OWNER - Full control
- SYSTEM - Full control
- LOCAL SERVICE - Query Value, Set Value, Create Subkey, Notify and Delete
- Administrators - Full control
- Users – Read

Erstellt von Jörn Walter – 31.01.2017