

## Windows 7 - brisanje logova



Svima su poznati logovi na operativnim sustavima Unix i Linux. I Windowsi imaju sustav za bilježenje sistemskih događaja, nazvan "Event log". Doduše, zapisi u Windowsu XP su malo "siromašni" i nečitki. No, počevši od Viste Microsoft je drastično promijenio i poboljšao shemu zapisa u Event log, te omogućio aplikacijama bolji i precizniji zapis kako bi omogućio kvalitetnije otklanjanje problema.

Administratorima je olakšano filtriranje logova po nekoliko kriterija, kao i definiranje korisnički definiranih pogleda ("Custom Views") za više logova.

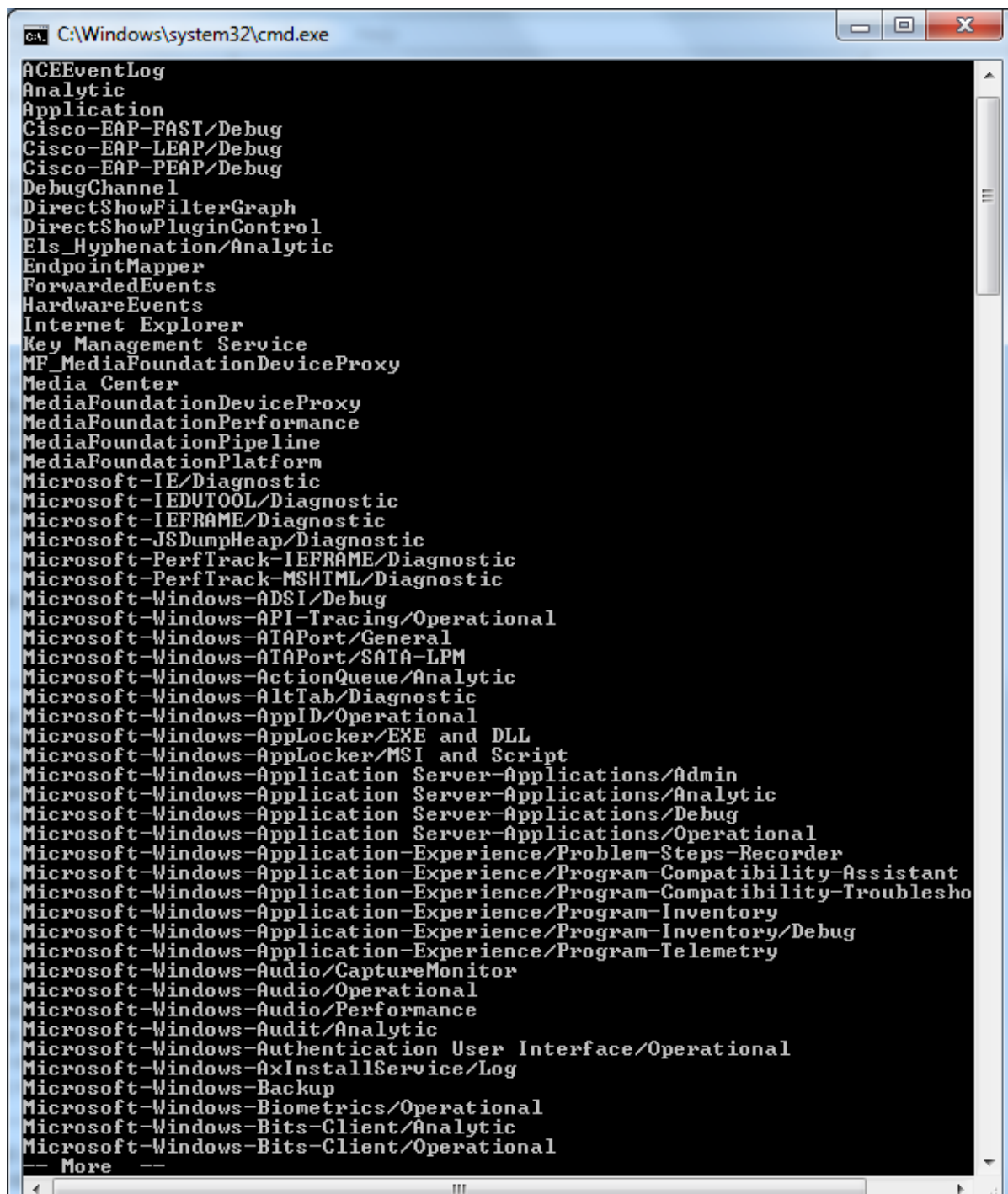
Kako je Event log redizajniran, izdan je i novi alat za upravljanje Event log zapisima. Taj alat je nazvan **wevtutil**. On omogućuje upravljanje nad svakim dijelom zapisa u Event logu.

Sam alat **wevtutil** dolazi sa mnoštvom parametara i prekidača i njegova uporaba zahtjeva strogo pridržavanje komandne sintakse koja obuhvaća, osim parametara i prekidača, razmake, dvotočke i navodnike.

Samu sintaksu te koji se prekidači koriste najbrže ćete dobiti direktno preko konzole. Nakon što startate Command Prompt u prozoru upišite "wevtutil /?"

Primjerice, ukoliko želimo ispis svih naziva logova, koristit ćemo parametar "el" (s razmakom)

```
wevtutil el
```

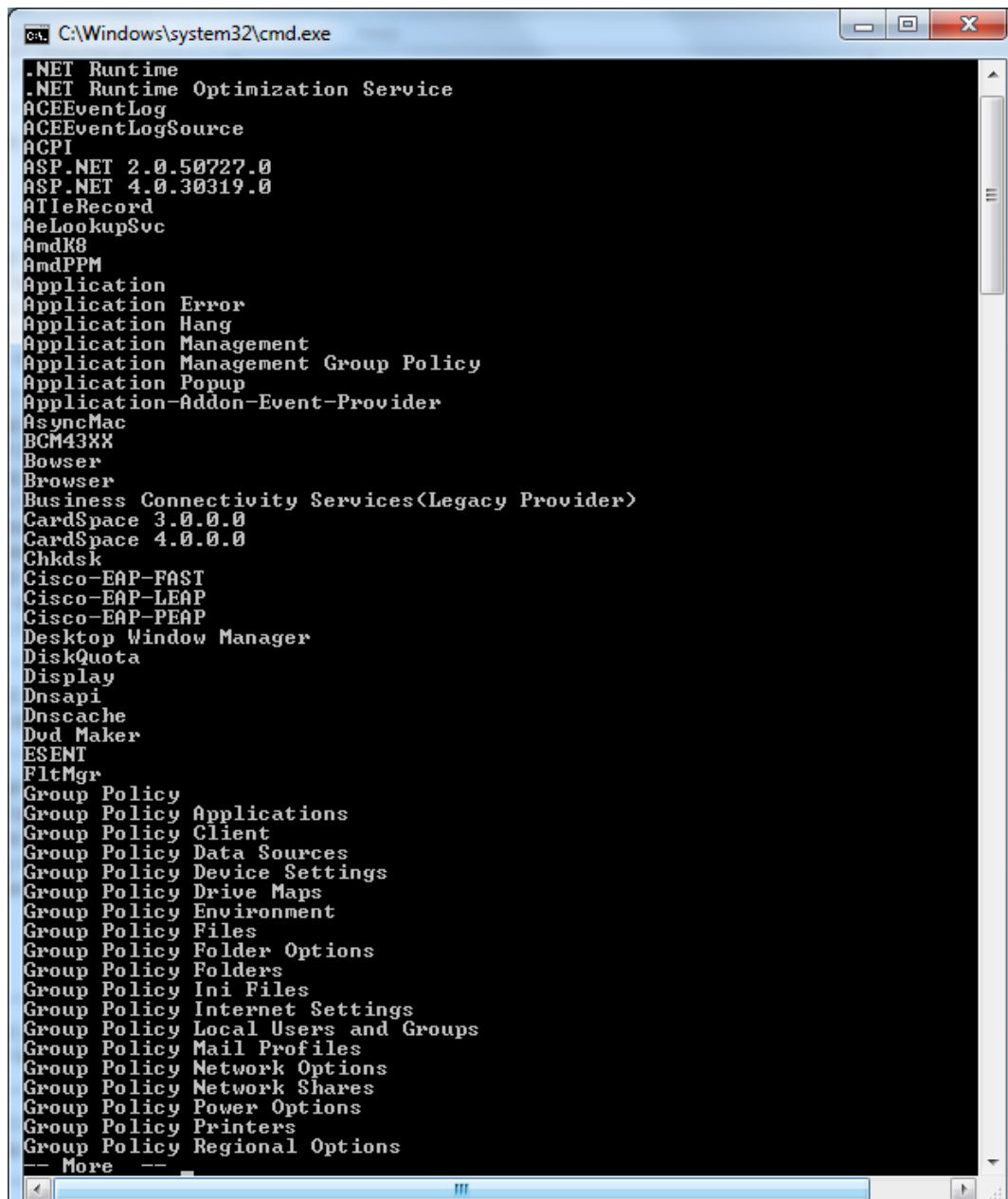


```
C:\Windows\system32\cmd.exe

ACEEventLog
Analytic
Application
Cisco-EAP-FAST/Debug
Cisco-EAP-LEAP/Debug
Cisco-EAP-PEAP/Debug
DebugChannel
DirectShowFilterGraph
DirectShowPluginControl
Els_Hyphenation/Analytic
EndpointMapper
ForwardedEvents
HardwareEvents
Internet Explorer
Key Management Service
MF_MediaFoundationDeviceProxy
Media Center
MediaFoundationDeviceProxy
MediaFoundationPerformance
MediaFoundationPipeline
MediaFoundationPlatform
Microsoft-IE/Diagnostic
Microsoft-IEDUTOTool/Diagnostic
Microsoft-IEFRAME/Diagnostic
Microsoft-JSDumpHeap/Diagnostic
Microsoft-PerfTrack-IEFRAME/Diagnostic
Microsoft-PerfTrack-MSHTML/Diagnostic
Microsoft-Windows-ADSI/Debug
Microsoft-Windows-API-Tracing/Operational
Microsoft-Windows-ATAPort/General
Microsoft-Windows-ATAPort/SATA-LPM
Microsoft-Windows-ActionQueue/Analytic
Microsoft-Windows-AltTab/Diagnostic
Microsoft-Windows-AppID/Operational
Microsoft-Windows-AppLocker/EXE and DLL
Microsoft-Windows-AppLocker/MSI and Script
Microsoft-Windows-Application Server-Applications/Admin
Microsoft-Windows-Application Server-Applications/Analytic
Microsoft-Windows-Application Server-Applications/Debug
Microsoft-Windows-Application Server-Applications/Operational
Microsoft-Windows-Application-Experience/Problem-Steps-Recorder
Microsoft-Windows-Application-Experience/Program-Compatibility-Assistant
Microsoft-Windows-Application-Experience/Program-Compatibility-Troubleshooter
Microsoft-Windows-Application-Experience/Program-Inventory
Microsoft-Windows-Application-Experience/Program-Inventory/Debug
Microsoft-Windows-Application-Experience/Program-Telemetry
Microsoft-Windows-Audio/CaptureMonitor
Microsoft-Windows-Audio/Operational
Microsoft-Windows-Audio/Performance
Microsoft-Windows-Audit/Analytic
Microsoft-Windows-Authentication User Interface/Operational
Microsoft-Windows-AxInstallService/Log
Microsoft-Windows-Backup
Microsoft-Windows-Biometrics/Operational
Microsoft-Windows-Bits-Client/Analytic
Microsoft-Windows-Bits-Client/Operational
-- More --
```

Ako želimo vidjeti ispis svih zapisa programskih komponenti koje mogu generirati logove, te ih potom proslijediti Event Vieweru, koristit ćemo parametar "ep"

```
wevtutil ep
```

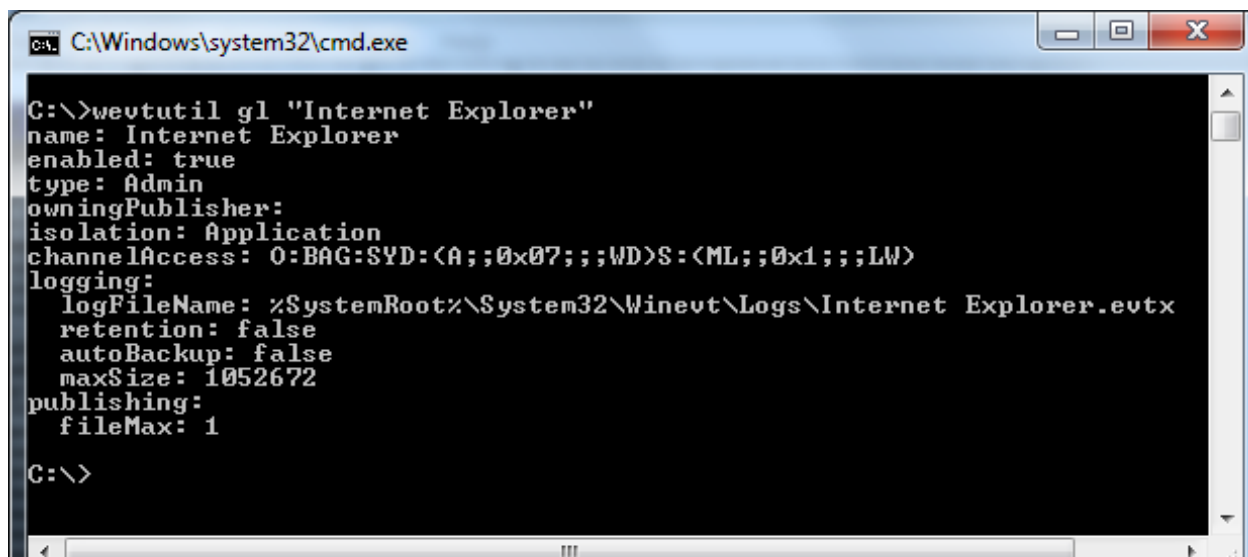


```
ca. C:\Windows\system32\cmd.exe
.NET Runtime
.NET Runtime Optimization Service
ACEEventLog
ACEEventLogSource
ACPI
ASP.NET 2.0.50727.0
ASP.NET 4.0.30319.0
ATIERecord
AeLookupSvc
AmdK8
AmdPPM
Application
Application Error
Application Hang
Application Management
Application Management Group Policy
Application Popup
Application-Addon-Event-Provider
AsyncMac
BCM43XX
Bowser
Browser
Business Connectivity Services(Legacy Provider)
CardSpace 3.0.0.0
CardSpace 4.0.0.0
Chkdsk
Cisco-EAP-FAST
Cisco-EAP-LEAP
Cisco-EAP-PEAP
Desktop Window Manager
DiskQuota
Display
Dnsapi
Dnscache
Dvd Maker
ESENT
FltMgr
Group Policy
Group Policy Applications
Group Policy Client
Group Policy Data Sources
Group Policy Device Settings
Group Policy Drive Maps
Group Policy Environment
Group Policy Files
Group Policy Folder Options
Group Policy Folders
Group Policy Ini Files
Group Policy Internet Settings
Group Policy Local Users and Groups
Group Policy Mail Profiles
Group Policy Network Options
Group Policy Network Shares
Group Policy Power Options
Group Policy Printers
Group Policy Regional Options
-- More --
```

Za dobivanje informacija o specifičnom log zapisu, poput toga da li je uključen, koja je vrsta zapisa (admin, operational, debug, staza, veličina) i slično, koristit ćemo parametar "**gl ime log zapisa**".

Kao primjer prikazat ćemo informacije o log zapisu Internet Explorera (u ovom primjeru koristit ćemo navodnike jer u nazivu postoji razmak):

```
wevtutil gl "Internet Explorer"
```



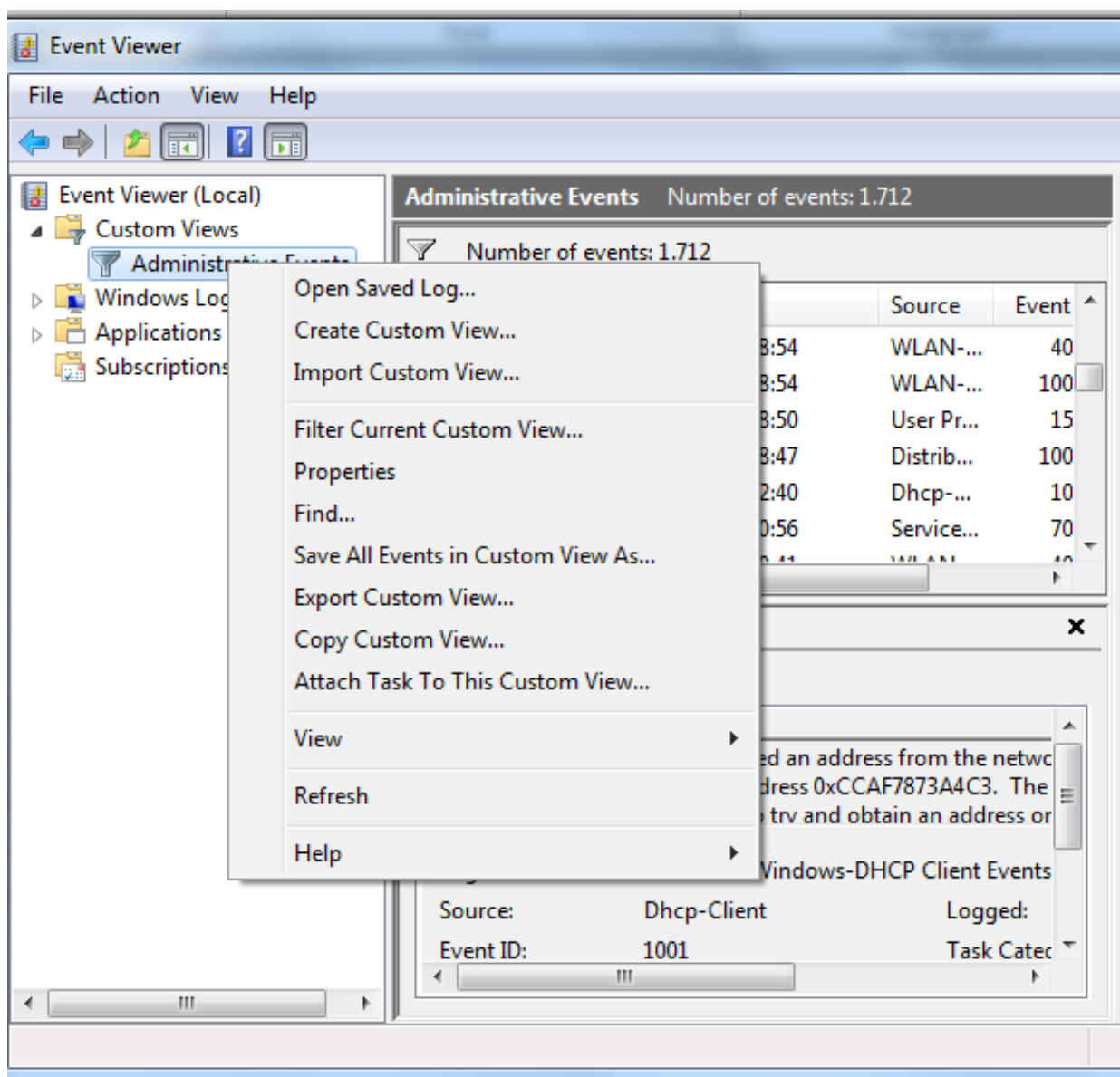
```
C:\Windows\system32\cmd.exe

C:\>wevtutil gl "Internet Explorer"
name: Internet Explorer
enabled: true
type: Admin
owningPublisher:
isolation: Application
channelAccess: 0:BAG:SYD:<A;;0x07;;;WD>S:<ML;;0x1;;;LW>
logging:
  logFileName: %SystemRoot%\System32\Winevt\Logs\Internet Explorer.evtx
  retention: false
  autoBackup: false
  maxSize: 1052672
publishing:
  fileMax: 1

C:\>
```

U primjera je vidljivo da je log uključen, tip zapisa je "Admin", možemo vidjeti punu stazu do zapisa i tako dalje.

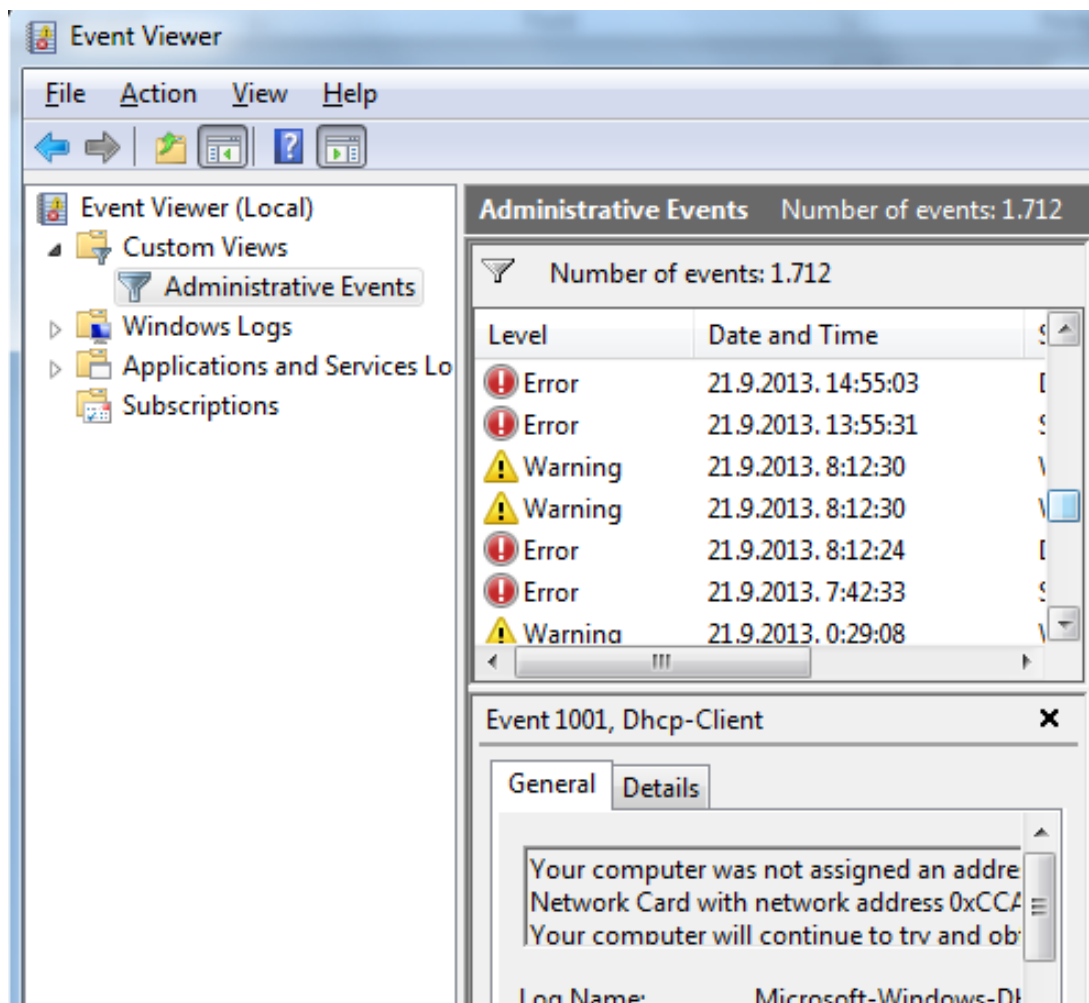
Naravno, pregled svih događaja i grešaka možemo vidjeti i putem Event Viewer konzole. Ono što je zanimljivo je da možemo primjetiti da u Custom views i pomoćnom izborniku nemamo opciju za brisanje Event log zapisa.



Ako želite imati "čistu" situaciju nakon otklanjanja problema tj. želite obrisati log zapise i lakše promatrati ponašanje problematičnog servisa nakon otklanjanje grešaka, možete se odlučiti na brisanje zapisa. Brisanje logova obavljate koristeći parametar "**cl**" (clear), dodajući tome naziv event loga. Primjerice, za brisanje logova Internet Explorera:

```
wevtutil cl "Internet Explorer"
```

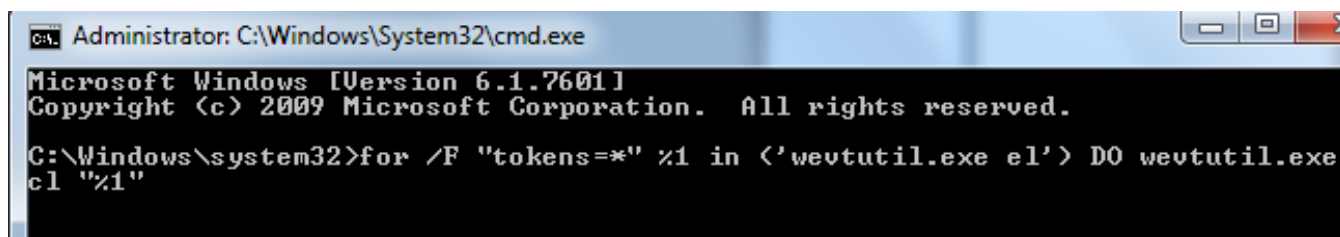
Ako želite obrisati sve log zapise, možete se poslužiti skriptom iz Command Prompta (koji je pokrenut kao administrator)

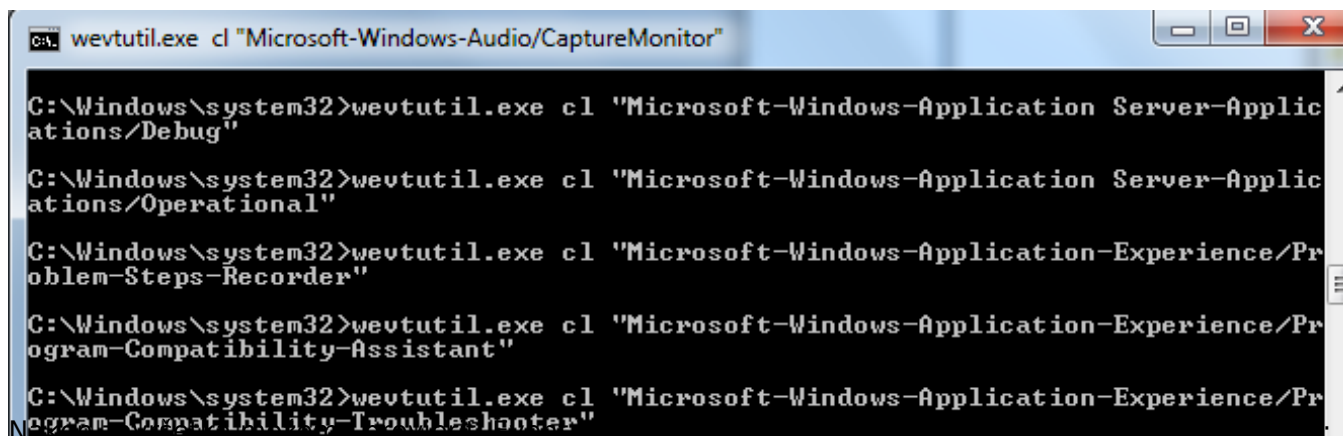


Slika prije brisanja zapisa.

U Command Promptu upišite sljedeći *oneliner* (obratite pozornost na apostrofe!):

```
for /F "tokens=*" %1 in ('wevtutil.exe el') do wevtutil.exe cl %1
```





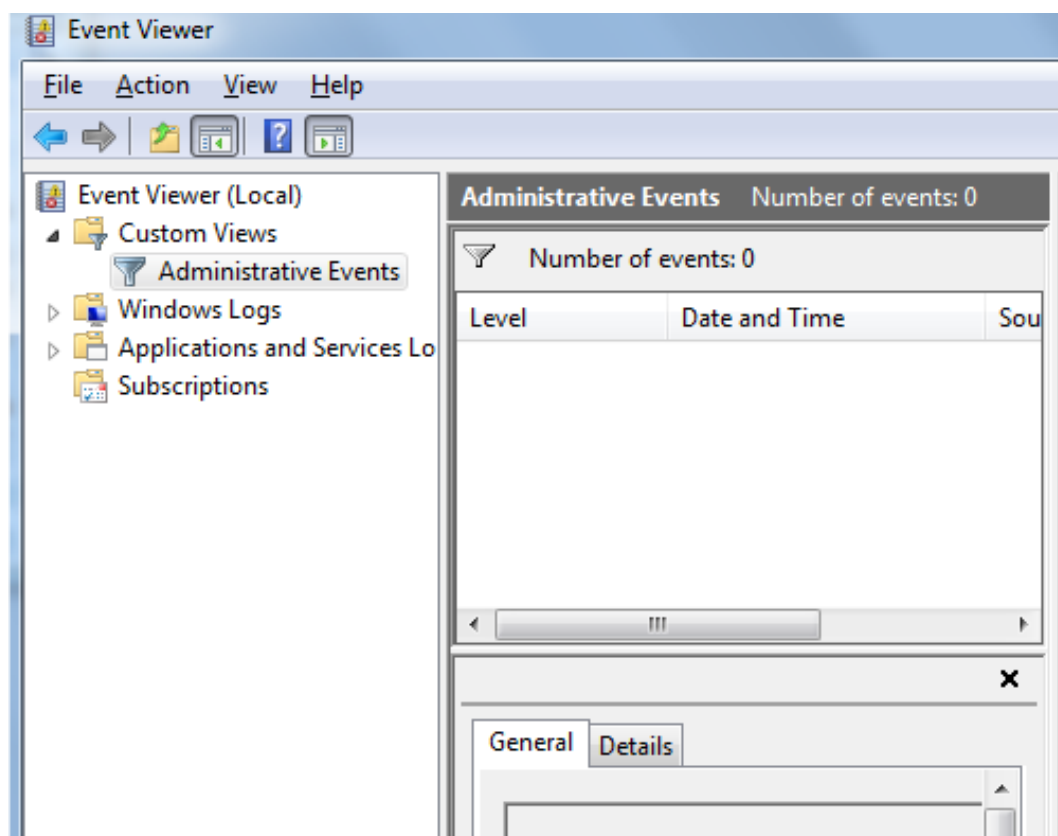
```
C:\Windows\system32>wevtutil.exe cl "Microsoft-Windows-Application Server-Applications/Debug"

C:\Windows\system32>wevtutil.exe cl "Microsoft-Windows-Application Server-Applications/Operational"

C:\Windows\system32>wevtutil.exe cl "Microsoft-Windows-Application-Experience/Problem-Steps-Recorder"

C:\Windows\system32>wevtutil.exe cl "Microsoft-Windows-Application-Experience/Program-Compatibility-Assistant"

C:\Windows\system32>wevtutil.exe cl "Microsoft-Windows-Application-Experience/Program-Compatibility-Troubleshooter"
```



Zdravko Rašić

sri, 2014-02-26 09:58 - Zdravko RašićKuharice: [Windows](#) [1]

**Kategorije:** [Operacijski sustavi](#) [2]

**Vote:** 5

Vaša ocjena: Nema Average: 5 (3 votes)

**Source URL:** <https://sysportal.carnet.hr/node/1359>

## Links

[1] <https://sysportal.carnet.hr/taxonomy/term/18>

[2] <https://sysportal.carnet.hr/taxonomy/term/26>