Windows 7 - brisanje logova

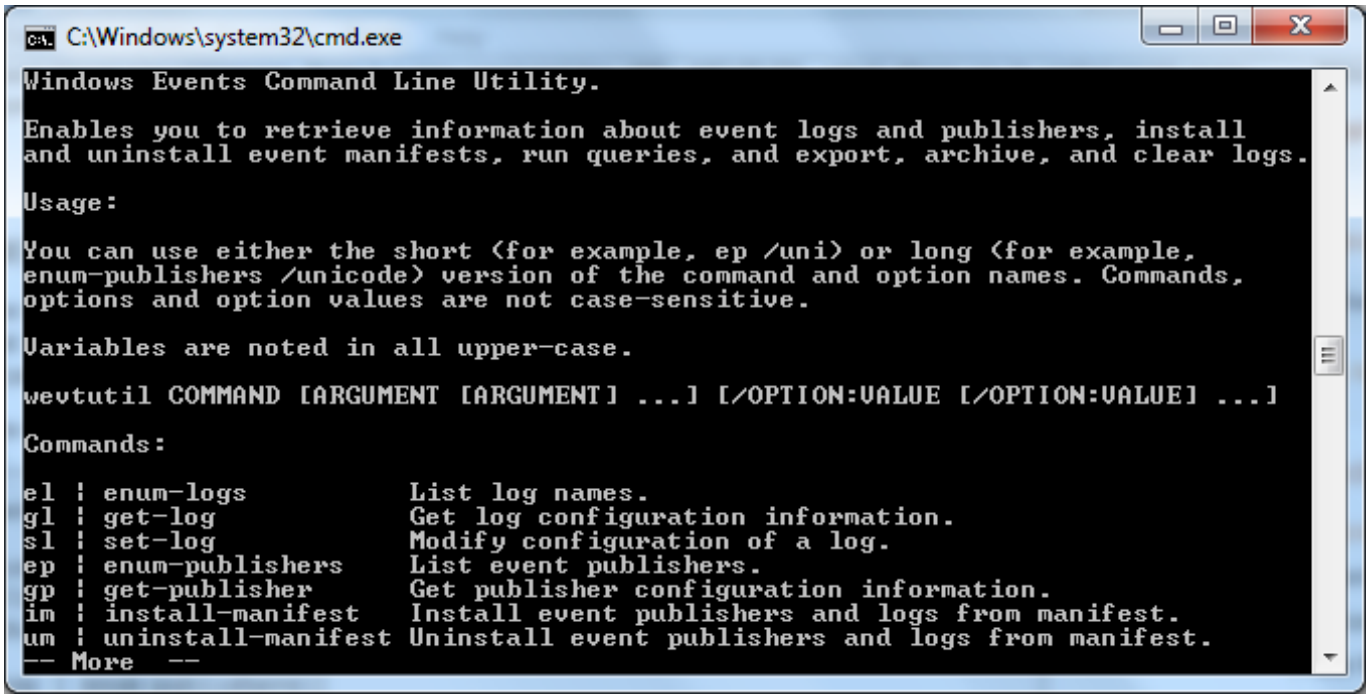
Svima su poznati logovi na operativnim sustavima Unix i Linux. I Windowsi imaju sustav za bilježenje sistemskih događaja, nazvan "Event log". Doduše, zapisi u Windowsu XP su malo "siromašni" i nečitki. No, počevši od Viste Microsoft je drastično promijenio i poboljšao shemu zapisa u Event log, te omogućio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

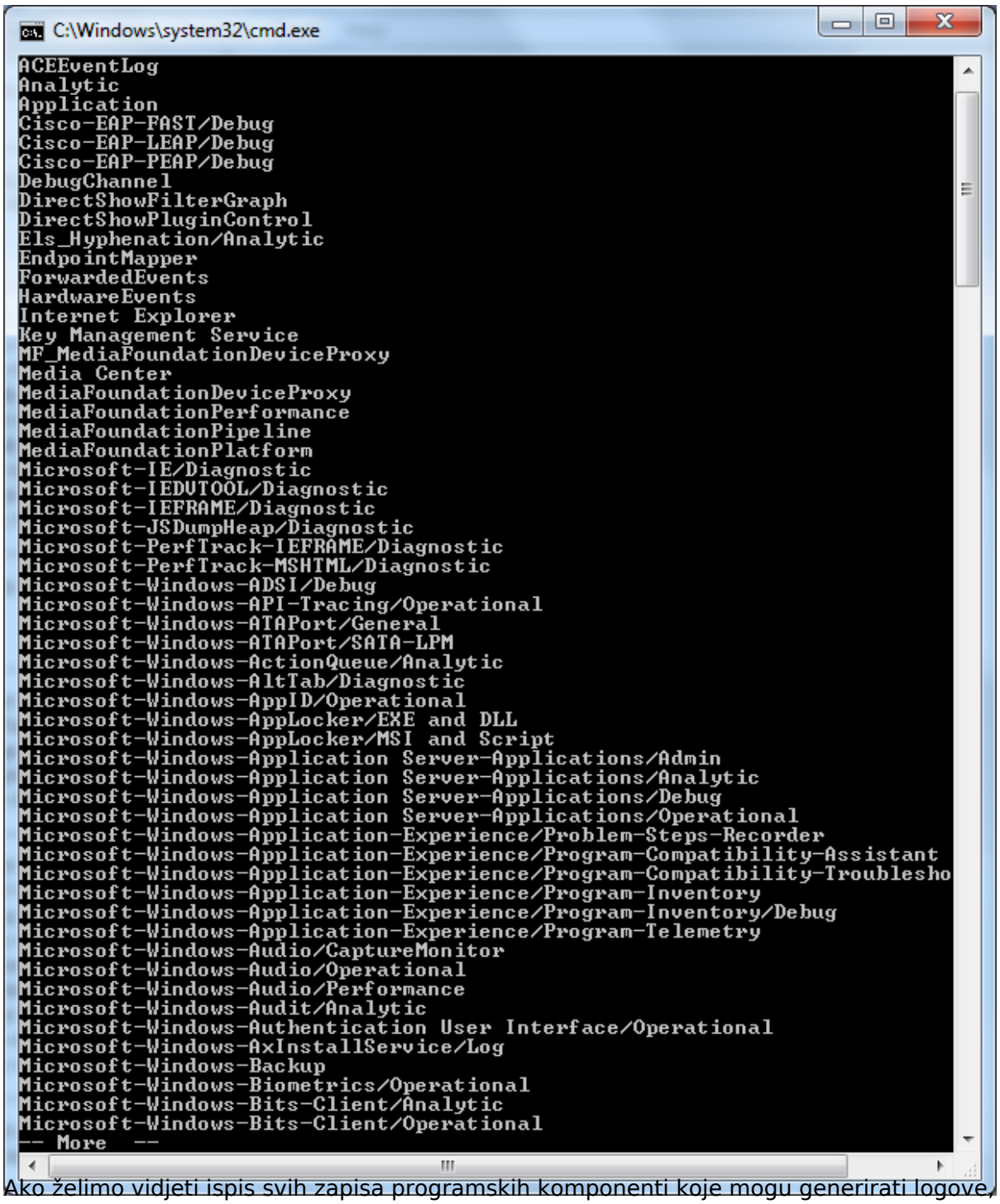
Sam alat **wevtutil** dolazi sa mnoštvom parametara i prekidača i njegova uporaba zahtjeva strogo pridržavanje komandne sintakse koja obuhvaća, osim parametara i prekidača, razmake, dvotočke i navodnike.

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
```



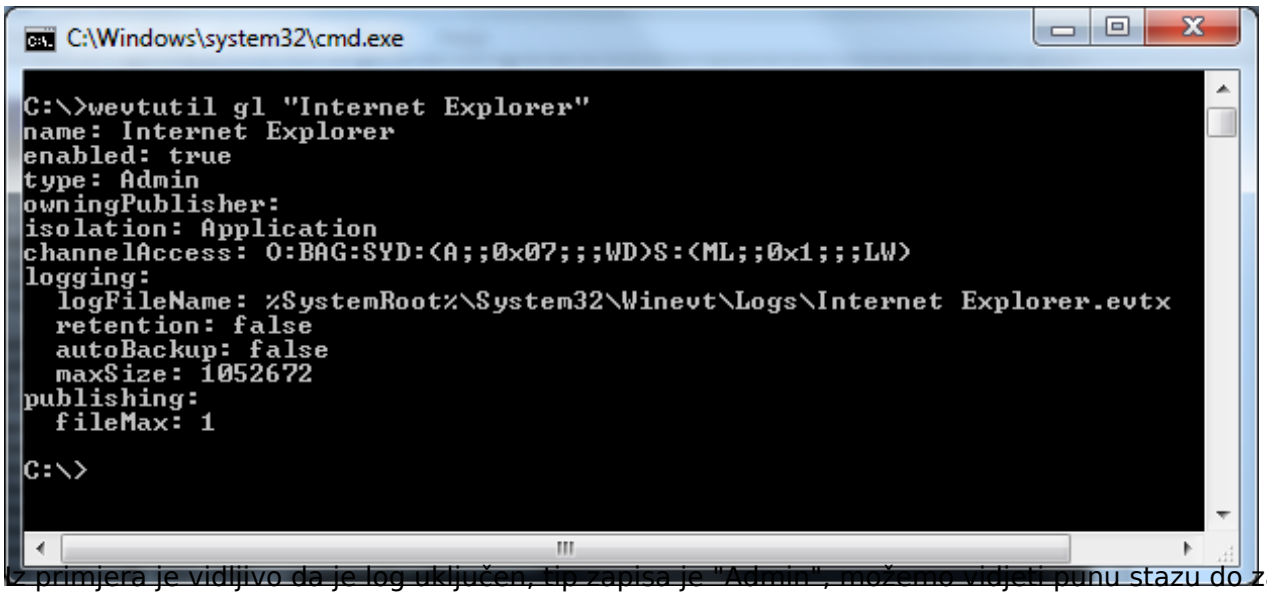
Ako želimo vidjeti ispis svih zapisa programskih komponenti koje mogu generirati logove, te ih potom proslijediti Event Vieweru, koristit ćemo parametar "ep"

```
wevtutil  ep
```

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**".

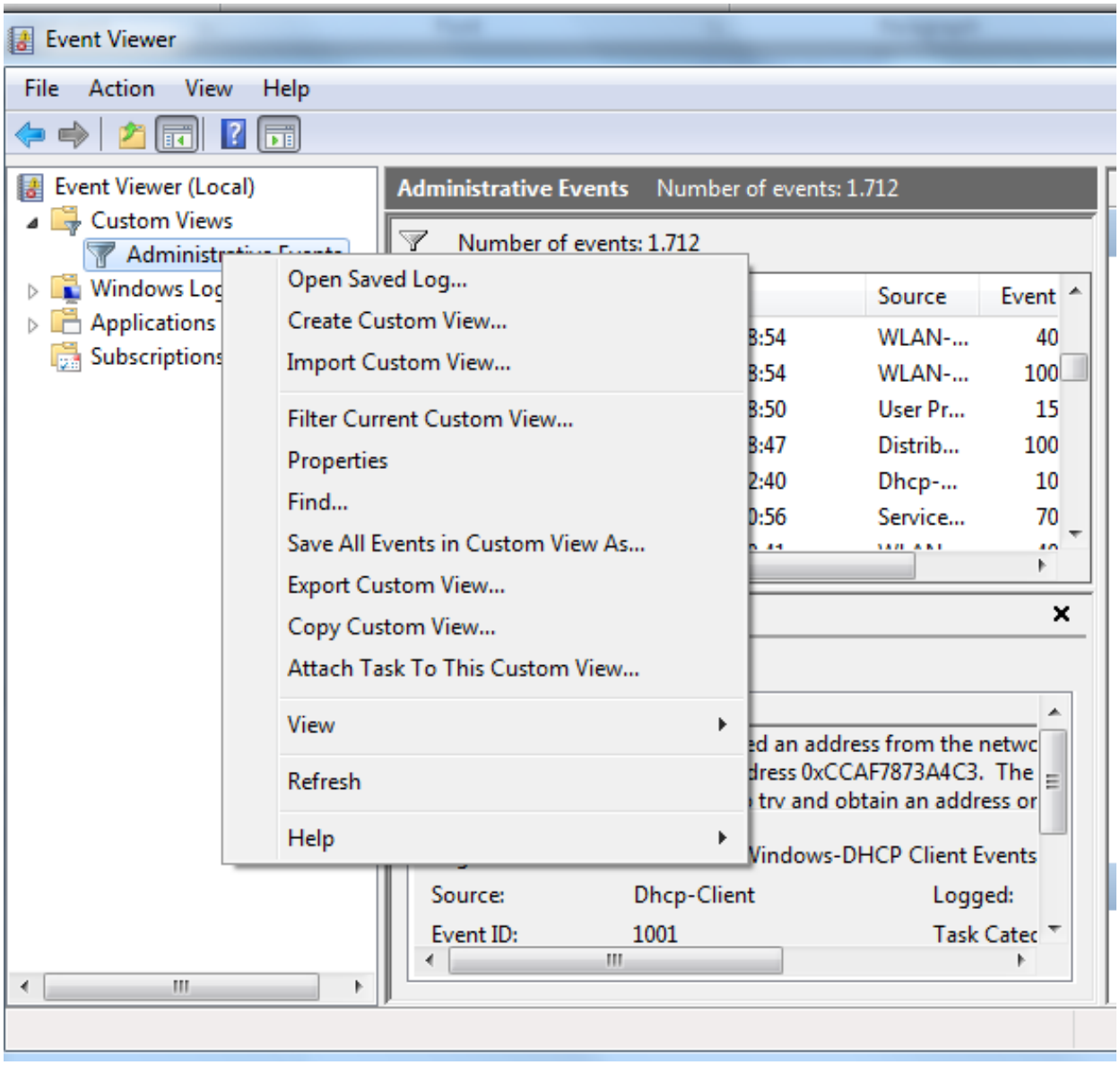
Kao primjer prikazat ćemo informacije o log zapisu Internet Explorera (u ovom primjeru koristit ćemo navodnike jer u nazivu postoji razmak):

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



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

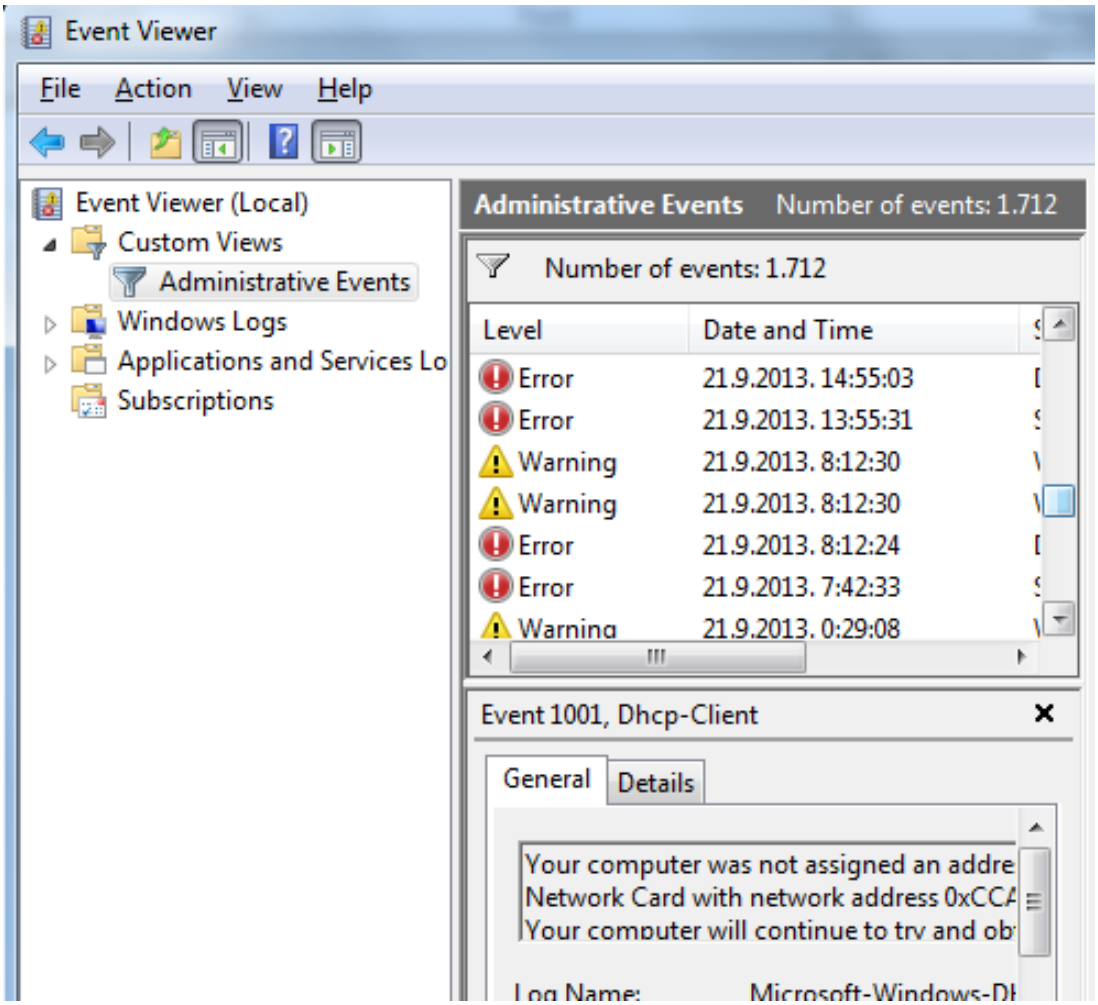
Naravno, pregled svih događaja i grešaka možemo vidjeti i putem Event Viewer konzole. Ono što je zanimljivo je da možemo primjetiti da u Custom views i pomoćnom izborniku nemamo opciju za brisanje Event log zapisa.



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"
```

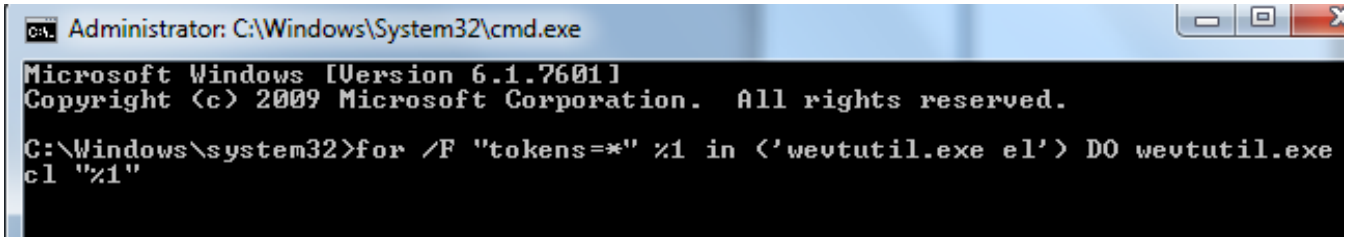
Ako želite obrisati sve log zapise, možete se poslužiti skriptom iz Command Prompta (koji je pokrenut kao administrator)

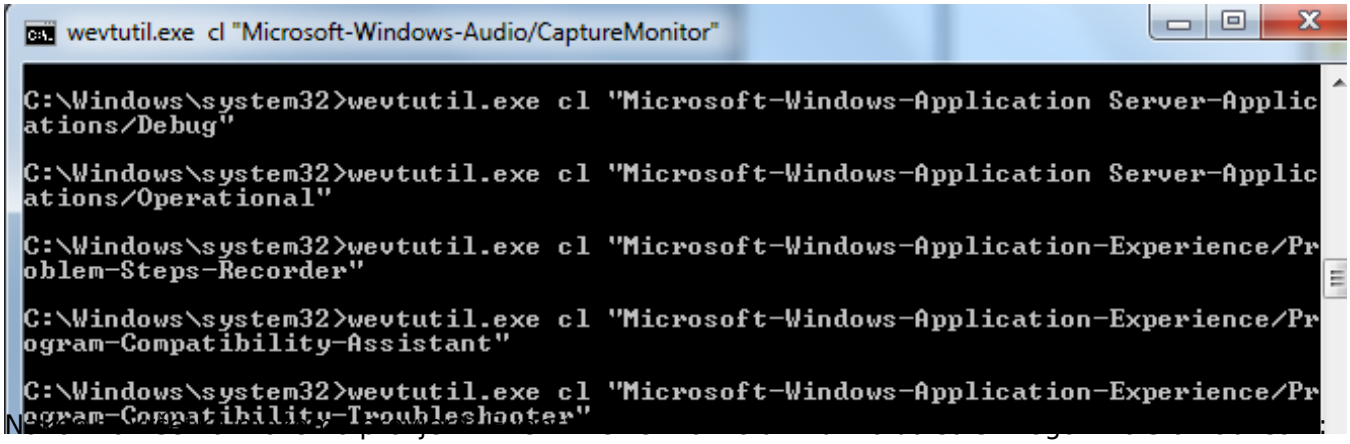


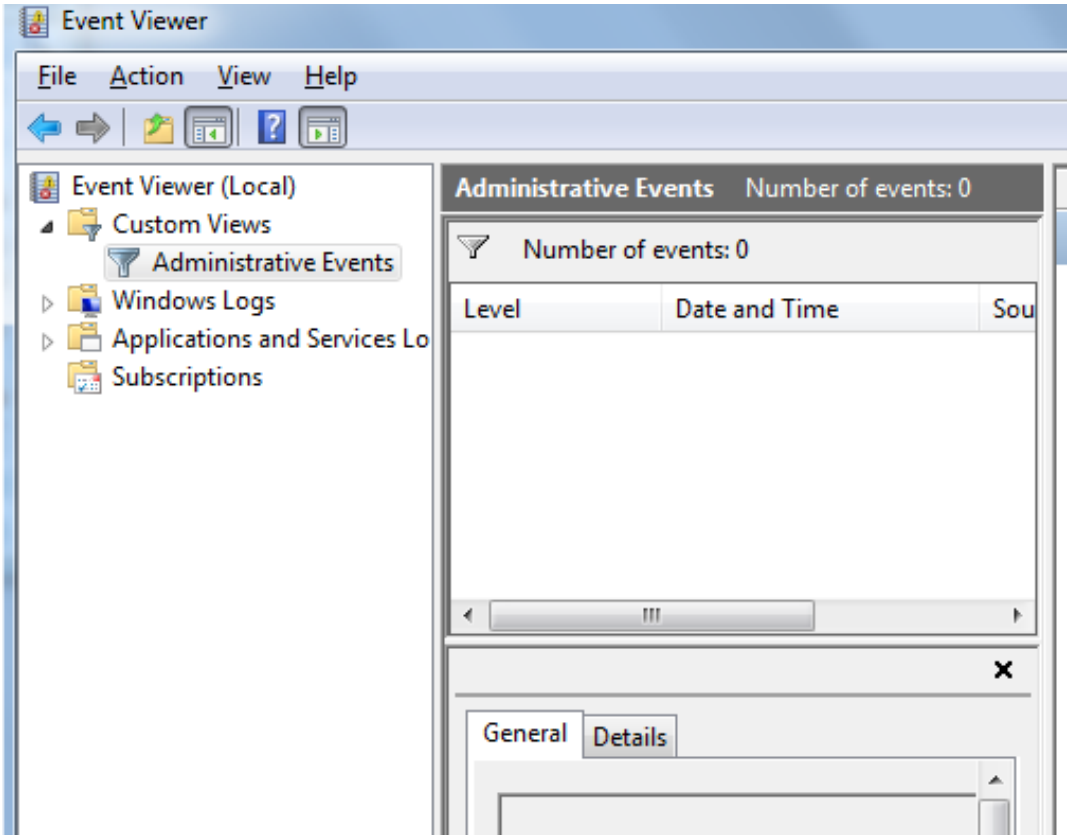
Slika prije brisanja zapisa.

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

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







Zdravko Rašić

sri, 2014-02-26 09:58 - Zdravko Rašić**Kuharice:** 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