

Jul 9, 2010

Reading EventViewer from the Command-Line

Using wmic

The `wmic NTEVENT` command can be used to dump out the contents of EventViewer logs to the command-line. Here's an example: `wmic NTEVENT WHERE "LogFile='security' AND TimeGenerated > '20100709173000.000000-300'"`

The `TimeGenerated` is NOT epoch, but is a string in the form of `YYYYMMDDHHmmSS.uuuuuu-ZZZ` where:

Label	Meaning
Y	Year
M	Month
D	Day
H	Hour
m	Minute
S	Second
u	Microsecond
-	Literally, a -
Z	Timezone offset in minutes from UTC (not hours)

```
"LogFile='security' AND TimeGenerated > '20100709173000.000000-300'" GET  
TimeGenerated
```

And here's how to output as a CSV file: `wmic NTEVENT WHERE "LogFile='security' AND TimeGenerated > '20100709173000.000000-300'" GET TimeGenerated,User /format:csv`

See also:

- <http://technet.microsoft.com/en-us/library/cc784189%28WS.10%29.aspx>
- <http://xinn.org/misc-scripts/wmic.txt>

[WMITools.exe](#) can do a lot of this stuff, but practically locks up my system.

Using Microsoft Log Parser

Microsoft has a tool called [Log Parser](#) that can can also parse the event logs.

📁 #windows

📄 154 Words

📅 2010-07-09 15:46 +0000

← NEWER

OLDER →

[Hiding Teasers in Drupal](#)

[My .bashrc file for cygwin](#)