Use PowerShell to create EventLog

In the following article, I will show you how to use PowerShell to create log records on the system, namely the Write-EventLog cmdlet command. The basic syntax of this command takes the form ...

TipsMake.com - In the following article, we will introduce and show you how to use PowerShell to create log records on the system, specifically the cmdlet Write-EventLog . The basic syntax of this command is in the form of:

PS C:> help Write-EventLog

Note that when using this cmdlet, you must declare the log file name, source, event id and corresponding message. Very similar to the **EVENTCREATE.EXE** command tool, but users cannot use non-standard or similar sources. Instead, they must first create specifications or data sources. And one of the easiest ways to find data sources is to use **Windows Management Instrumentation** (WMI).

PS C:> $ log = Get-WmiObject win32_nteventlogfile -filter "filename = 'system'"
PS C:> $ log.Sources
System
ACPI
adp94xx
adpahci
adpu320
.

If one of the above sources seems appropriate, please record it as a record as follows:

PS C:> write-event System -source Server -eventid 12345 -message "I am a custom event log message"

The default entry type is **Information** , users can create **eventID** separately and change, edit at any time:

PS C:> get-eventlog system -newest 1 |Format-list EventID, EntryType, Source, Message
EventID: 12345
EntryType: Information
Source: Server
Message: The description for Event ID '12345' in Source 'Server' cannot be
tìm th?y. Máy ?nh c?c b? không có có ph?n m?m c?n thi?t
thông tin ho?c t?p tin DLL t?p tin ?? hi?n th? thông báo, ho?c b?n
có th? không có quy?n ?? truy c?p thêm. The following inform
là ph?n c?a ph?n c?a s? ki?n:

Suppose that if you want to search for any event ID or message, you will get a small error like this:

```
PS C:> get-eventlog system -newest 1 -message "* custom event *"
Index Time EntryType Source InstanceID Message
----- ---- --------- ------ ---------- -------
1512222 Jan 25 10:05 Information Server 12345 The des .
```

Not really perfect, but still functioning properly. While theoretically we can register with new data sources, and can also create new records by using the **cmdlet New-Eventlog** command. Usually this cmdlet is applied to developers, programming a fixed event log model. In the following example, we will create a log in custom format, and initialize a number of different data sources.

```
PS C:> new-eventlog -LogName PSLogging -Source ADSI, WMI, Test, Other
```

Check what was created:

```
PS C:> $ log = Get-WmiObject win32_NTEventlogfile -filter "filename = 'PSLogging'"
PS C:> $ log | fl
FileSize: 69632
LogfileName: PSLogging
Name: C: WindowsSystem32WinevtLogsPSLogging.evtx
NumberOfRecords: 0
```

That's a completely new log file, followed by a check of the data source - source:

```
PS C:> $ log.sources
PSLogging
ADSI
Other
Ki?m TRA
WMI
```

And finally, enter any data here:

```
PS C:> Write-EventLog PSLogging -Source Test -eventID 1000 -Message "I am the first entry"
```

Besides, we can use any event ID, or create them at will:

```
PS C:> get-eventlog PSLogging |format-list
Index: 14
EntryType: Information
InstanceId: 1000
Message: I am m?c nh?p ??u vào
Category: (1)
CategoryNumber: 1
ReplacementStrings: {I am the first entry}
Source: Test
TimeGenerated: 1/25/2012 10:45:47 AM
TimeWritten: 1/25/2012 10:45:47 AM
UserName:
```

At this step, Windows will no longer 'care' for the event ID. If you want to add any other data source, you only need to re-use the cmdlet **New-Eventlog:**

PS C:> New-EventLog PSLogging -source Scripting

And our new source here:

PS C:> Get-WmiObject win32_NTEventlogfile -filter "filename = 'PSLogging'" |Select -expand Sources
PSLogging
ADSI
Other
Scripting
Ki?m TRA
WMI

The cmdlet **New-Eventlog** command has the parameter **-computername** , so it's much easier to create any new eventlog on the entire Desktop or server - where we want to monitor and manage the log. Good luck!