

# Hey, Scripting Guy! Blog

Learn about Windows PowerShell

## 2012 Scripting Games Beginner Event 7: Display a List of Enabled Logs

[The Scripting Guys](#)

10 Apr 2012 1:01 AM

[18](#)

### 2012 Scripting Games



*Join the fun and compete!*

**Summary:** In Beginner Event 7, you are required to display a list of all enabled logs on the computer that contain at least one entry.

### About this event

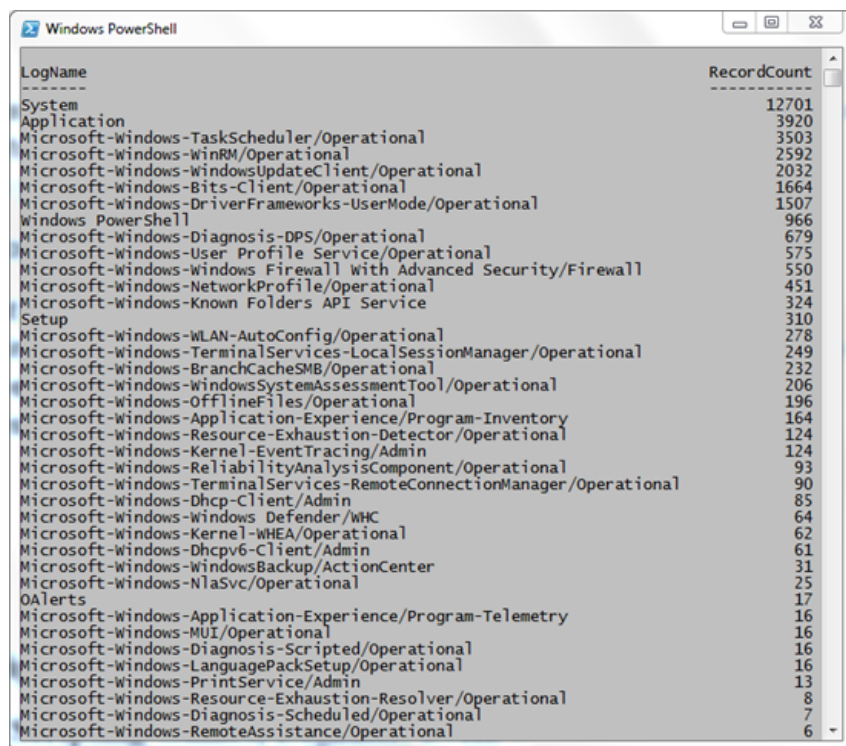
Division	Beginner
Date of Event	4/10/2012 12:01 AM
Due Date	4/17/2012 12:01 AM

### Event scenario

On a Windows 7 computer, nearly 500 logs provide auditing and troubleshooting capabilities. Many of these logs do not record any information unless an administrator enables them. You were recently discussing this information with your boss, and he asked a rather logical question:

"What logs actively record information on a Windows 7 computer at any given time?"

You were, of course, somewhat taken aback, and headed off to TechNet to find the answer. After about fifteen minutes of searching and clicking around, you were no closer to the answer than when you began. Your boss came over to you and suggested that you use Windows PowerShell to find the answer. The following image represents an acceptable type of output.



LogName	RecordCount
System	12701
Application	3920
Microsoft-Windows-TaskScheduler/Operational	3503
Microsoft-Windows-WinRM/Operational	2592
Microsoft-Windows-WindowsUpdateClient/Operational	2032
Microsoft-Windows-Bits-Client/Operational	1664
Microsoft-Windows-DriverFrameworks-UserMode/Operational	1507
Windows PowerShell	966
Microsoft-Windows-Diagnosis-DPS/Operational	679
Microsoft-Windows-User Profile Service/Operational	575
Microsoft-Windows-Windows Firewall With Advanced Security/Firewall	550
Microsoft-Windows-NetworkProfile/Operational	451
Microsoft-Windows-Known Folders API Service Setup	324
Microsoft-Windows-WLAN-AutoConfig/Operational	310
Microsoft-Windows-TerminalServices-LocalSessionManager/Operational	278
Microsoft-Windows-BranchCacheSMB/Operational	249
Microsoft-Windows-WindowsSystemAssessmentTool/Operational	232
Microsoft-Windows-OfflineFiles/Operational	206
Microsoft-Windows-Application-Experience/Program-Inventory	196
Microsoft-Windows-Resource-Exhaustion-Detector/Operational	164
Microsoft-Windows-Kernel-EventTracing/Admin	124
Microsoft-Windows-ReliabilityAnalysisComponent/Operational	124
Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational	93
Microsoft-Windows-Dhcp-Client/Admin	90
Microsoft-Windows-Windows Defender/WHC	85
Microsoft-Windows-Kernel-WHEA/Operational	64
Microsoft-Windows-Dhcpv6-Client/Admin	62
Microsoft-Windows-WindowsBackup/ActionCenter	61
Microsoft-Windows-NlaSvc/Operational	31
OALerts	25
Microsoft-Windows-Application-Experience/Program-Telemetry	17
Microsoft-Windows-MUI/Operational	16
Microsoft-Windows-Diagnosis-Scripted/Operational	16
Microsoft-Windows-LanguagePackSetup/Operational	16
Microsoft-Windows-PrintService/Admin	13
Microsoft-Windows-Resource-Exhaustion-Resolver/Operational	8
Microsoft-Windows-Diagnosis-Scheduled/Operational	7
Microsoft-Windows-RemoteAssistance/Operational	6

## Design points

- Your code should not display any errors when run.
- Your code should display all logs that have entries in them.
- Your code should display only logs that are enabled.
- Your code should display any enabled hidden logs that contain entries in them.
- You should display the complete log name, and the number of entries in the log.
- The number of entries in the logs should be displayed in descending order (the log with the most entries in it should appear on the first line of the output).
- You do not need to display a total count of the number of enabled logs that have entries.
- The requirements for this scenario can be met with a “one liner” (a one line logical command). Depending on the width of your Windows PowerShell console and the screen resolution, it may occupy more than one physical line).
- You do not need to write comment-based Help or accept command-line parameters (or anything like this). Your goal is simply to provide a bit of information to your boss—a “one liner” is perfectly acceptable.

## 2012 Scripting Games links

### 2012 Scripting Games: All Links on One Page

I invite you to follow me on [Twitter](#) and [Facebook](#). If you have any questions, send email to me at [scripter@microsoft.com](mailto:scripter@microsoft.com), or post your questions on the [Official Scripting Guys Forum](#). Good luck as you compete in this year's Scripting Games. We wish you well.

**Ed Wilson, Microsoft Scripting Guy**

Tweet

6

Share

1

Save this on Delicious

## Comments

**SoCalDavis**

10 Apr 2012 12:35 PM

This one was pretty fun. Just like all of the other events, I have learned something new every day!

**IamMred**

10 Apr 2012 2:47 PM

@SoCalDavis awesome! I am glad you are finding the events fun, and are learning something new each day!

10 Apr 2012 5:08 PM

**Tyson J. Hayes**

This event has been great, been rocking beginner and having a great time. Looking forward to seeing the posted solutions so I can use the ideas presented here for training opportunities for my team. Thanks for doing this!

11 Apr 2012 2:53 AM

**Dawn Villejoin**

Hmmm... Two of the design points have me over-thinking this. It's going to gnaw at me :) Good thing I have 7 days to think it over.

11 Apr 2012 5:21 PM

**ZoomZoomDude**

What permission level do we need to run the script? Can we assume that we're admins?

11 Apr 2012 6:06 PM

**IamMred**

@ZoomZoomDude you do not have to be an admin to run the script, but keep in mind the design requirements.

12 Apr 2012 11:33 AM

**Get-Exchange - sahal**

Hello Ed, Two question i have on this event:

- 1) Should the solution be capable of running on remote computer?
- 2) Should we hide all errors INCLUDING Terminating Erros?

Thanks for your feedback, this will help me submitt event 7

12 Apr 2012 5:43 PM

**brad**

by 'Your code should not display any errors when run' does this mean we need to add error handling or simple if you do it right there will be no errors to handle

12 Apr 2012 5:46 PM

**Daniel-D**

Regarding the following points (below), I see two possible ways to filter (Enabled AND Count > 0) vs (Enabled OR Count > 0). To me, the event scenario leans toward the first ("logs actively record"), but in order to display all logs with entries, the later would be needed. Does the "enabled only" design point take precedence over the "all logs with entries"? Mr Ed, would you clarify?

\* Your code should display all logs that have entries in them.

\* Your code should display only logs that are enabled.

Thanks!

12 Apr 2012 5:55 PM

**IamMred**

@Brad you probably want to add a bit of code to supress the errors. I am not looking for structured error handling, but just something so you get a clean output.

12 Apr 2012 5:59 PM

**IamMred**

@Daniel-D you want logs that are enabled AND have a record entry count that is greater than 0. If there is an enabled log with NO entries in it, then do not display that log.

12 Apr 2012 6:08 PM

**IamMred**

@Get-Exchange No, I am not checking for remote connectivity on this event. Do not return errors from the command.

12 Apr 2012 6:30 PM

**Daniel-D**

Thanks for your answer on my previous question. Have another one for you: Given the "one-liner" design point, are you implying that aliases are acceptable, or will points be deducted if aliases are used since you did not state that they are explicitly acceptable?

---

**IamMred**

12 Apr 2012 7:24 PM

@Daniel-D a onelinner is acceptable, and it is permissible to use aliases in the one linner. If you want to make DOUBLE SURE then include a comment with the "long version" of your command.

---

**Zak Humphries**

17 Apr 2012 10:23 AM

DOH!! Clicked submit and realized I had left a Measure-Object for debugging at the end of my line..... 1 star :(

---

**1** **2**