Hey, Scripting Guy! Blog

Learn about Windows PowerShell

2012 Scripting Games Advanced Event 7: Search Windows Logs

The Scripting Guys 10 Apr 2012 1:01 AM 23

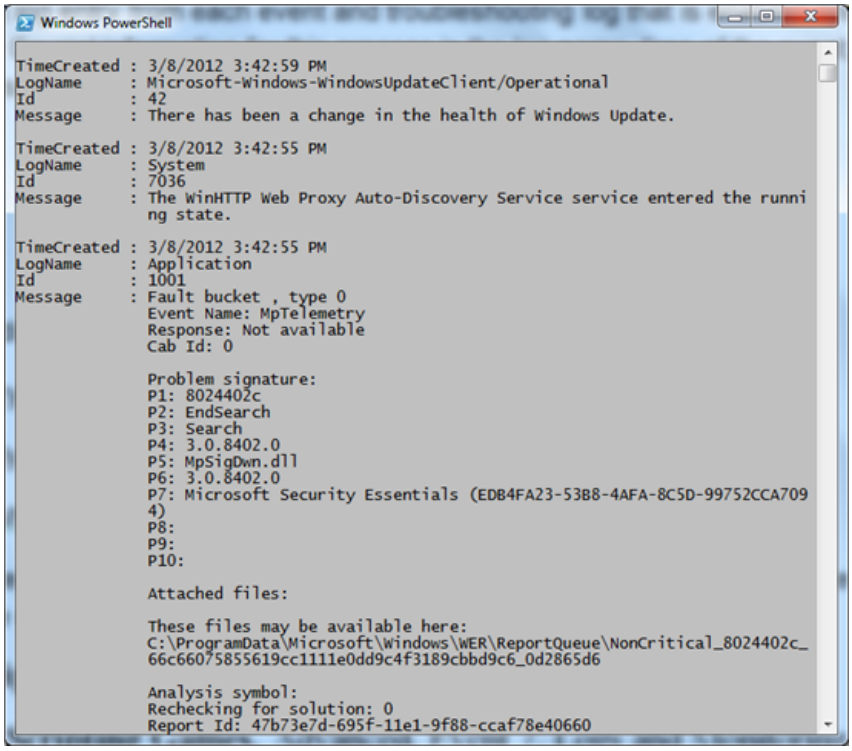
Summary: In Advanced Event 7, you are required to search all Windows logs for the most recent event.

About this event

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

Event scenario

You are troubleshooting a problem with your Windows 7 laptop, and you hope to find some clues to the recent performance issues by examining recent entries from various Windows logs. You have recently become aware that there are nearly 500 logs available in a standard Windows 7 installation, but you do not feel like manually searching through all of the logs by using the Event Viewer utility. You decide to use Windows PowerShell to come to the rescue. You want to write a command that will display the most recent one-event log entry from each event log and troubleshooting log that is enabled and has at least one entry in it. Crucial information for this process includes the log name, time of the event, the event ID, and the event message. An acceptable output is shown in the image that follows.



Design points

- Your code should not display any errors.
- Your code should query hidden logs if they are enabled and they contain at least one entry.
- You should display only the most recent entry from each log.
- The event log entries should be sorted so that the most recent entry appears first.
- You must display the following required properties: time of the event, the name of the log, number of the event ID, and the event details.

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, 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

Comments

IamMred 10 Apr 2012 2:47 PM

Please do NOT post answers to these questions here. The 2012 Scripting Games are still going on.

Roman Prosvetov 10 Apr 2012 2:54 PM

You are late Ed, I've read it! *evil laugh*

IamMred 10 Apr 2012 3:05 PM

@Roman Prosvetov Yes, but I deleted the answer because it was a bad script, and I did not want everyone copying it and getting a 1 :-)

Mikko K' 10 Apr 2012 3:08 PM

So hidden logs that are disabled, even if they contain entries, shouldn't be displayed, right?

IamMred 10 Apr 2012 3:17 PM

@Mikko K that is correct. If a hidden log is disabled it should not be displayed even it does have entries.

10 Apr 2012 5:11 PM

vNoob

What about logs that might need special access/rights to view?

IamMred 10 Apr 2012 5:15 PM

@VNoob you need to trap the error and display log name with "no access" in the output.

10 Apr 2012 5:48 PM

DamienCharbonnel

Hi,

When you ask for "a command that will display the most recent one-event log entry from each event log and troubleshooting log that is enabled and has at least one entry in it", in fact, you want the first information event of each log?

IamMred 10 Apr 2012 5:52 PM

@DamienCharbonnel I want the most recently written event log entry from each of the logs -- that is the one that is closest in time when the script runs.

10 Apr 2012 6:11 PM

DamienCharbonnel

Ok , thank you for your quick answer

10 Apr 2012 6:43 PM

Ryan Ries

I hope you have a fast computer for grading this one...

Bigteddy 10 Apr 2012 8:57 PM

Ed, can you confirm that you want errors trapped and reported, if a log is inaccessible? This is not what you stated in the original outline. You said "Do not display errors". This seems like an additional requirement.

IamMred 10 Apr 2012 9:03 PM

@Bigteddy, I do not want to display raw errors, but they should be trapped, and something friendly like logname not accessible should be displayed instead.

10 Apr 2012 10:51 PM

vNoob

What about logs that are enabled but don't have any log entries? Should those be included?

K Schulte 10 Apr 2012 11:58 PM

HI Ed,

I seem to be the only one here, who hadn't ever heard of "hidden" logs.

Even Google (or Bing) don't do much better :-(

If I once will get to know them ,,, is it right, that we should display ONLY these logs?

The description of the event let me think, that we should query ALL logs.

Design point 2 ... is it: ONLY "Hidden?" logs ???

Klaus

1 2