Hey, Scripting Guy! Blog

Learn about Windows PowerShell

2012 Scripting Games Advanced Event 5: List Errors

The Scripting Guys 6 Apr 2012 1:01 AM 16

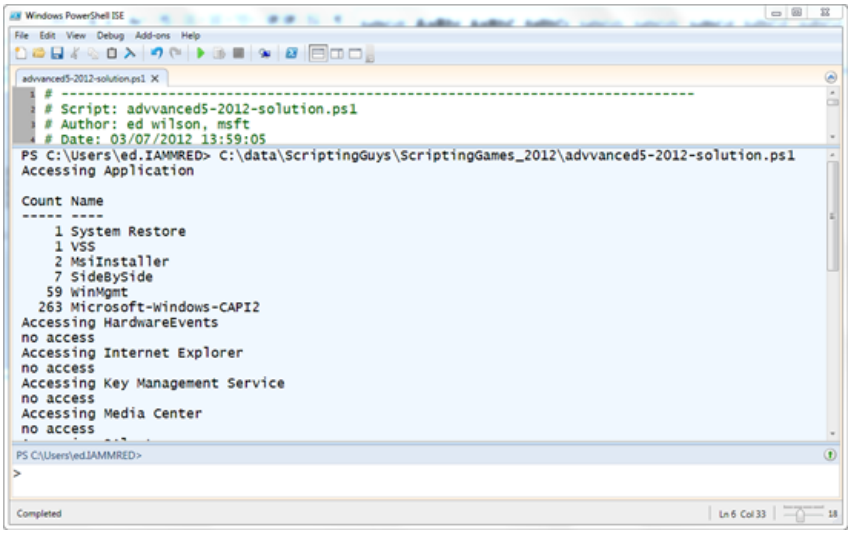
Summary: In Advanced Event 5, you will produce a report that lists the number of errors from all the traditional logs on a particular server.

About this event

Division	Advanced
Date of Event	4/6/2012 12:01 AM
Due Date	4/13/2012 12:01 AM

Event scenario

You are an analyst on the server team of a medium-sized organization. You are studying the performance and reliability of various servers on the network, and you decide to produce a report that lists the number of errors from all the traditional logs on a particular server. The code you use should be capable of running against a local computer or against an arbitrary number of remote computers. An acceptable output is shown here.



Design points

- You will use impersonation for all remote connections, so you do not need to be able to supply credentials.
- You should not display errors due to permissions or due to no events matching your filter.

- You should not make changes to the users' environment. If you do, you should change them back at the end of the script. Modification to the users' environment following script completion will cost you points.
- Your script should run without prompting against the local computer.
- Your output should be organized such that the largest source of errors appears at the top of the output.

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

Roman Prosvetov 6 Apr 2012 1:16 PM

If the script is executed with multiple computers, we need to get help for them, individually or together?

6 Apr 2012 2:56 PM

Cameron Wilson

"Traditional Logs" - Is that all event log types or traditional only being limited to "Application, Security, and System"? Thx.

6 Apr 2012 3:58 PM

Cameron Wilson

Disregard my last. I see from the screen shot that we're doing all logs.

IamMred 6 Apr 2012 6:07 PM

@Prosvetov Roman There are no design requirements about displaying help (comment based help) but I think you are talking about what does the display look like when the script runs against a remote computer. THe answer is you would want a separate section for each computer. So you do not want to total ALL errors from ALL computers into a single list. That information would not be too useful unless you were limiting to a specific event ID.

IamMred 6 Apr 2012 6:09 PM

@Cameron Wilson yes, the event calls for gathering information from all traditional event logs (System, Application, Security, as well as other traditionally formatted logs.) This event does not target the newer ETW type of logs.

K Schulte 6 Apr 2012 9:20 PM

Hi Ed,

you know, I'm germam ... and I don't understand english speaking people ... sometimes ...

If I look at your last design point:

Your output should be organized such that the largest source of errors appears at the top of the output.

and at your acceptable output image, where "1" - "System Restore" is the top source of error ...

I'm a little bit irritated ... but maybe because we have a differently ordered number system here :-)))

(Sorry4that, Ed ... but you know: I can't let a good joke go without mentioning ... *sss* :-)

Klaus

K Schulte 6 Apr 2012 11:17 PM

Hi Ed,

an a little bit more serious question:

Should the output be aggregated over all servers in one table with (or even without?) the servername?

Or should we produce one table per server?

Klaus.

IamMred 7 Apr 2012 1:37 AM

@K_Schulte you do not need to aggregate the output. You can do one table per server.

---

7 Apr 2012 11:44 PM

Scott Heath

The image seems to contradict the statement "Your output should be organized such that the largest source of errors appears at the top of the output."

Can you please clarify?

---

8 Apr 2012 12:11 AM

Scott Heath

Also confusing to me is that you say we should not display access or no matching event errors, but it looks like you have displayed a "friendly" error message for "no access". Can you explain any further?

IamMred 8 Apr 2012 1:01 AM

@Scott Heath you are correct. My sample I wrote for this event is a 4 point script because it does not properly organize the errors. It is an acceptible output, but not a perfect output. Good catch. I actually changed the requirements, adding the sorting, after I wrote the sample (because I thought it was too easy) and after I did the screen shot.

IamMred 8 Apr 2012 1:03 AM

@Scott Heath Friendly errors are permissible, even encouraged. What I do not want are the raw red messages that clutter the output. Thanks for the question and for giving me a chance to clarify this.

---

10 Apr 2012 2:33 PM

Albert Fortes

Hi!

I'm going crazy with the design point that talks about the "users' environment". I don't underestand that. It's at variable level? registry level? files? session?

Thanks in advance.

IamMred 10 Apr 2012 2:45 PM

@Albert Fortes It could be. For example, a user PowerShell ISE may be set so that the working directory is C:\ if you call set-location and change the working drive to HKLM: and do not change it back to C:\ at the end of the script then you have altered the scripting environment. It could lead to disasterous problems with the next script. If you change the $erroractionpreference variable to "stop" and do not change it back to "continue" it can cause problems for the user. Basically, if you change anything during the script, and you do not set it back you will lose at least one point here.

---

10 Apr 2012 7:08 PM

Joel

I'm looking for 2 points of clarification.

1) Should the errors be ranked per log or per computer, i.e. Server1/Log1 5,4,3,2,1 Server1/Log2 5,4,3,2,1. Or all logs per computer, i.e. Server1/Logs 10,8,6,4,2?

2) Is it the expectation that this will need to be run against computers singularly, i.e. execute against computer A, then execute against computer B. Or in a mass fashion, i.e. execute against computer a,computer b,computer c

---

1 2