Hey, Scripting Guy! Blog

Learn about Windows PowerShell

The 2011 Scripting Games Advanced Event 3: Use PowerShell to Query Classic Event and ETL Diagnostic Logs

ScriptingGuy1 6 Apr 2011 1:15 AM 8

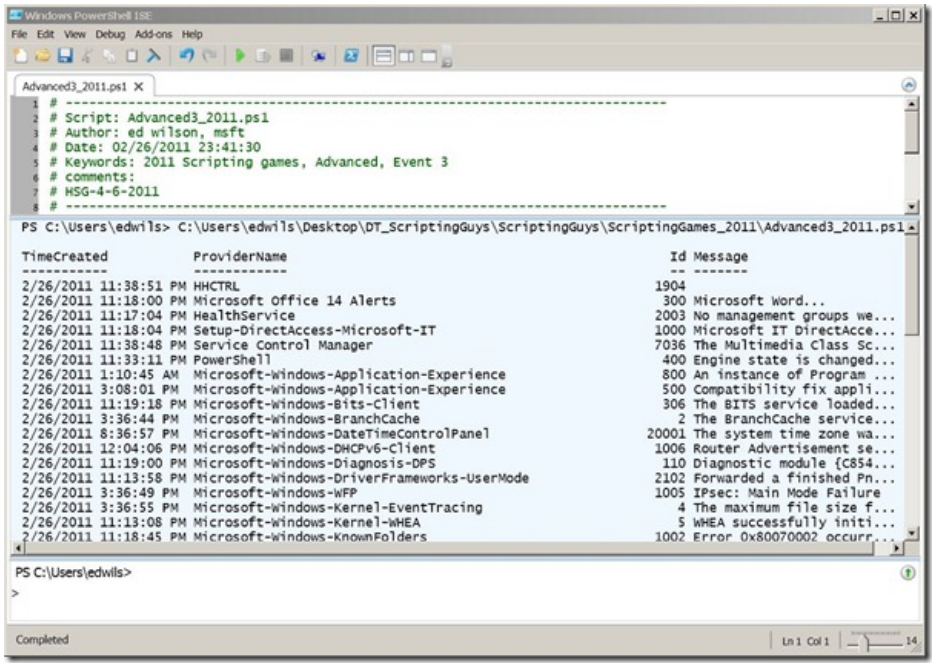
Summary: Advanced Event 3 of the 2011 Scripting Games uses Windows PowerShell to query class event and ETL diagnostic logs.

About this event

Division	Advanced
Date of Event	4/6/2011 12:15 AM
Due Date	4/13/2011 12:15 AM

Event scenario

You are in charge of server monitoring at a medium-sized company that consists of three geographically dispersed sites and 50 servers. The servers are running a combination of Windows Server 2008 R2 and Windows Server 2008. You want to query all classic event logs and the ETL diagnostic logs that are enabled and have had data written during the date in which the report is run. No matter when the report runs, it should return the most recent event written in the log, but only if the event occurred during the date in which the report runs. Your report should include the following information: The date and time that the event occurred, the name of the event provider, the event ID, and the message that is associated with that event. Remember, you only want to return the most recent event from each classic event log and ETL log that is enabled, and has had events written during the day in which the report runs. Output like that shown in the following image would meet the requirements of this scenario.



Design points

- For the purposes of this scenario, the script must only run locally. However, additional points are granted for configuring the script to run against remote machines.
- Additional points for querying Active Directory Domain Services (AD DS) for server names
- Additional points for reusable code
- Additional points for returning the name of the log that contained the event
- Additional points for allowing the user to select the number, severity, eventID, and other information when running the script or when calling the function

2011 Scripting Games links

2011 Scripting Games: All Links on One Page

Submit your scripts on PoshCode

Support our Sponsors!

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

6 Apr 2011 11:54 AM

Andrew

Anyone else having difficulties with the poshcode site?

6 Apr 2011 12:20 PM

André

Yes, a logon isn't possible at the moment

IamMred 6 Apr 2011 3:21 PM

@Andrew @Andre Poshcode is back up now

6 Apr 2011 5:04 PM

Jacques

The scenario says "it should return the most recent event written in the log", however the output provided as an example shows a long list of events generated the same day (2/26/2011). Some of them are even coming from the same provider "Microsoft-Windows-Application-Experience".

How exactly are we supposed to filter the events then? Would that be all events that were written the same day as the report is run? Thanks for clarifying.

6 Apr 2011 6:14 PM

marcadamcarter

@Jacques (!my interpretation!) filter/display only events that occur on the same 'day' as when the report is run.

"it should return the most recent event written in the log, but only if the event occurred during the date in which the report runs"

6 Apr 2011 6:34 PM

John

Can't upload script. Error message "A potentially dangerous Request.Form value was detected from the client (SourceCode="...-filename <string>]

advanced...").

6 Apr 2011 8:17 PM

Jacques

@marcadamcarter : yes, that is my interpretation too. In that case the scenario should say "the most recent events" instead of "the most recent event". I will stick to my interpretation then. :)

hassan sayed issa20014 4 Aug 2014 8:39 PM

thank you