Hey, Scripting Guy! Blog

Learn about Windows PowerShell

2012 Scripting Games Beginner Event 9: Search the Event Log

The Scripting Guys 12 Apr 2012 1:01 AM 23

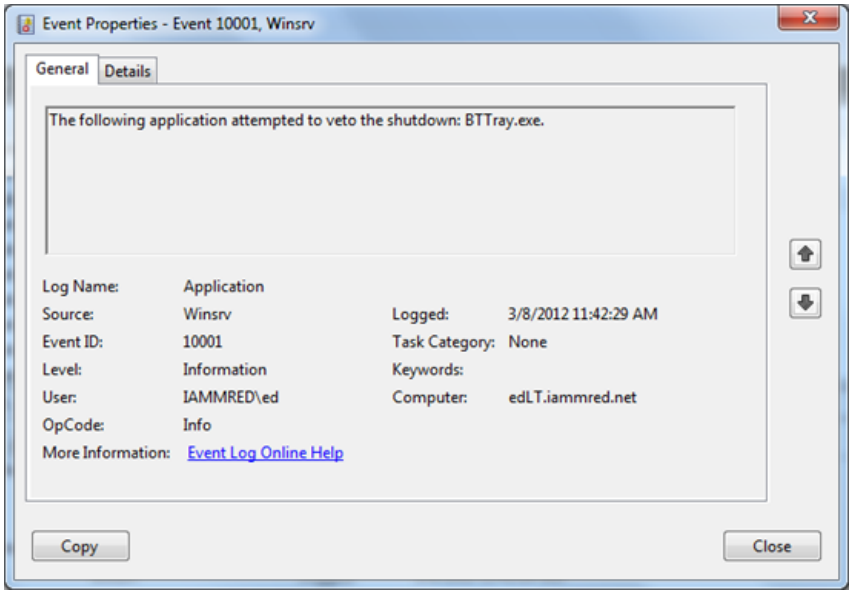
Summary: In Beginner Event 9, you are required to search the event log for specific entries.

About this event

Division	Beginner
Date of Event	4/12/2012 12:01 AM
Due Date	4/19/2012 12:01 AM

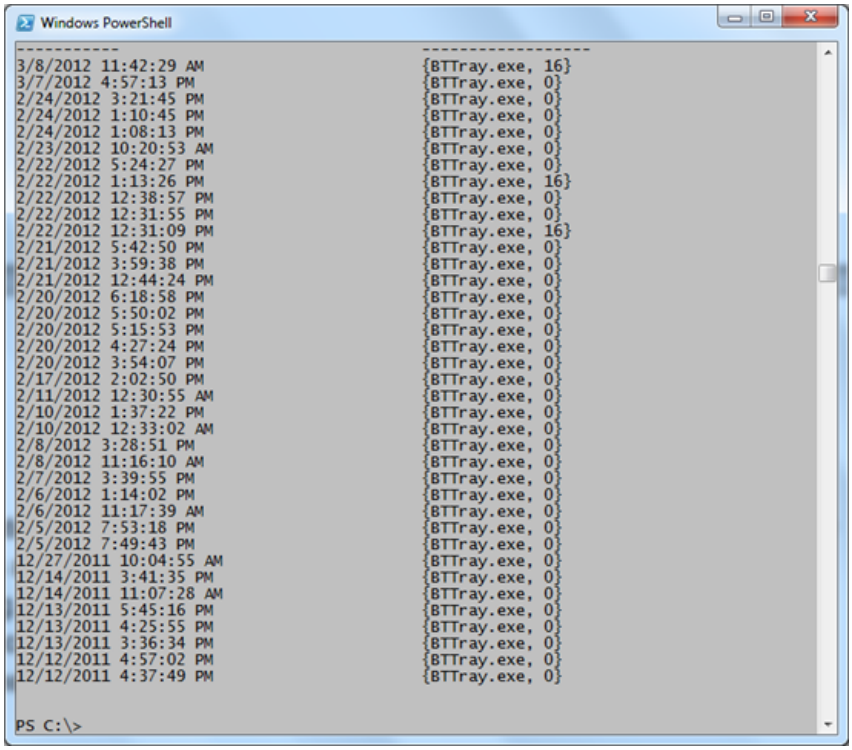
Event scenario

You are trying to troubleshoot shutdown issues on your laptop. It appears to hang for few seconds before it begins the shutdown process. You were looking through the application event log, and you noticed an event log entry that states that the BTTray.exe application attempted to veto the shutdown (how rude). A sample event log entry is shown in the image that follows.



You decide to search the application log for other event log entries from this source to determine how often this particular application is attempting to veto the shutdown, and to see if there are other applications doing the same thing. You write a quick one-line Windows PowerShell command that displays the date of the occurrence and the application name. An

acceptable output is shown in the image that follows (the column headings are hidden because part of the problem is finding the properties to display).



Design points

- Your command should be as efficient as possible; therefore, you want to limit the entries that are returned from the event log to only those that match the particular scenario. For hints on the filter to use, study the event log entry (the first image).
- Keep in mind that what appears in a graphical tool is not always what you need to use in your filter.
- Be careful with the number of entries returned from the application log—make your filter as efficient as possible. You will lose points for inefficient queries.
- Because you are troubleshooting your computer, this is not a long involved script, but a “one liner.” Do not get carried away writing a complex script—complexity will cost you points.

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

12 Apr 2012 10:29 AM

Timo Skupin

Hi Ed,

i'm a little bit confused on this one. Should we query just this application (BTTray.exe) or any application that causes this problem?

Thanks

Best regards from Germany =)

SdeDot 12 Apr 2012 3:32 PM

So I dont have any of these events generated on my systems, so anybody have any suggestions on how to work this script without having the specific events to work with?

12 Apr 2012 4:11 PM

Srikanth

I can connect to http://2012sg.poshcode.org/, but am unable to login to submit the script. Is anyone else facing this issue?

12 Apr 2012 4:26 PM

VincentVH

@Srikanth Yep, I can't login either. It has been like that for at least 6 hours.

12 Apr 2012 4:59 PM

Leon

Yip, same here, Can't log on to submit :-(

12 Apr 2012 5:01 PM

jlsuperman

@Srikanth @VincentVH me too me too...

12 Apr 2012 5:04 PM

DavidW

@SdeDot Try to restart with notepad running. Make sure to hit cancel when it asks to save and also when it asks to force quit.

12 Apr 2012 5:08 PM

MarcW

SdeDot, there are a lot of computers that wont have BTTray.exe running or causing errors because they dont come with bluetooth. The understanding i have is to write a script to filter out a specific process.

IamMred 12 Apr 2012 5:48 PM

@Timo Skupin You look for any application causing the problem. I simply used BTTray.exe as an example to clarify what I wanted.

IamMred 12 Apr 2012 5:49 PM

@SdeDOT open the Event log and look for something that IS causing an error. BTTray.exe is Blue Tooth tray, if your computer does not have bluetooth you will NOT find this particular process.

IamMred 12 Apr 2012 5:51 PM

@Srikanth try again in a little while. There are authentication issues at the hosting service.

IamMred 12 Apr 2012 5:52 PM

@MarcW exactly.

@DavidW this is a good suggestion.

SdeDot 12 Apr 2012 5:54 PM

Thanks for your comments DavidW and MarcW.

DavidW: Im not understanding specifically what you are saying. I think you are saying if I walk through the steps you outlined, I will generate Event ID 10001 records, correct?

MarcW: Yes, my understanding is as yours to write a 'filtering' script, however not being able to use Powersell commands against live data is somewhat limiting. If there is no data to test against, Im not sure the cmdlets/properties Im querying against are correct.

12 Apr 2012 6:17 PM

DavidW

@SdeDot Yes, if you follow my steps, it will create the same type of alert. Just one more thing to add to it though. Make sure to type something into notepad before rebooting the machine. If you don't, notepad will close without prompting.

SdeDot 12 Apr 2012 6:59 PM

DavidW: Bingo! Based on your instructions, EventID 10001 records were generated in the App Event Log, so thanks for the help. Hopefully now I have what I need to assemble this script.

---

1 2