# Hey, Scripting Guy! Blog

Learn about Windows PowerShell

## 2012 Scripting Games Advanced Event 3: Create a Log that Updates

The Scripting Guys 4 Apr 2012 1:01 AM 15


**Summary**: Advanced Event 3 of the 2012 Scripting Games challenges you to create a log file that appends each time a person logs on to the network.

**About this event**

| | |
|---|---|
| Division | Advanced |
| Date of Event | 4/4/2012 12:01 AM |
| Due Date | 4/11/2012 12:01 AM |

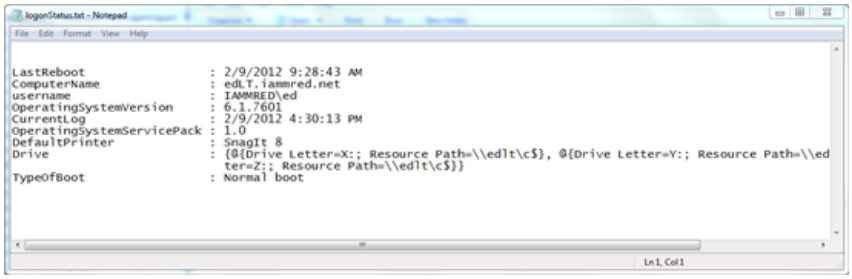
### Event scenario

You are “the scripting guy” at your small single location business. As a matter of fact, you are also “the Exchange Server guy,” “The AD guy,” and “The WSUS guy.” In short, you seem to do it all. The IT department consists of the CIO, you, and a Help Desk person. All servers are running Windows Server 2008 R2, and all workstations (except the IT department) are running Windows 7 Enterprise edition. About half of the workstations are running a 32-bit operating system, and the other half are running a 64-bit operating system. All of the workstations are running the 32-bit version of Microsoft Office 2010. The IT department staff (you, the Help Desk person, and the CIO) are running a beta version of Windows 8 on your client computers with a beta version of Office 2012.

Your boss, (aka, the CIO) has decided that she would like the Help Desk person to have a log that updates each time a person logs on to the network. The log, named *logonstatus.txt* should be stored in a folder off the root named *logonlog*. This file should append (the latest entries will be at the bottom of the log file) each time the user logs on. Therefore, if a user logs on to the computer 12 times in one day, there will be 12 entries in the log. Here is a list of things the CIO has mandated MUST be in the log file:

1. The user name in *domainname/username* format, for example: Microsoft/EdWilson
2. The computer name in *hostname.domainname* format, for example: Mred.Microsoft.Com
3. Operating system version
4. Service Pack level
5. All mapped drives and path to mapped resources
6. The default printer
7. The last reboot of the computer
8. The type of boot up (for example, safemode or normal)

The image shown here illustrates an acceptable output for the file.




## Design points

- For the purpose of this exercise, we are looking for a specific file name in a specific location.
- The file must append. Do not overwrite the file on each log on or you will lose a point. The history aspect of the file is important to the scenario.
- You must include all eight pieces of information in the file. If you miss information, you will lose points.
- Neatness counts. The information presented must be accurate and easy to read by humans. Therefore, outputting as a .csv, .tsv, or .xml file will not gain extra points. In fact, because they are not very humanly readable, you will lose points for such output. The idea here is that a Help Desk person will open the file and read it.

## 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

4 Apr 2012 9:20 AM

**Jason Stangroome**

Some clarifications:

1. "The log, named logonstatus.txt should be stored in a folder off the root named logonlog" - Is the log intended to be saved at this location on the computer that is being logged on to, or is the log to be saved at this location on a central management computer which will contain the log on history from all the computers on the network combined?

2. "a log that updates each time a person logs on to the network" - How is the script expected to be triggered? Will it be deployed as a logon script for all users or will it be run on a scheduled interval and look for recent logon activity or should the script somehow register itself to be notified when a remote computer is logged on to?

Regards,

Jason

---

**K Schulte** 4 Apr 2012 9:30 AM

Hi Ed,

even though I still have no idea to get some of the information pieces together ...

this seems to be another (maybe hard but) manageable task to do!

What I haven't understood exactly is:

"a folder off the root" ( an "english -> german" translation problem :-)

Does it just mean: "a subfolder of any root drive"?

And the other thing, that is more technical:

What does the login process have to do with the desired output?

Better: Have we got to deal with any part of the login process at all?

Or is it just our task to write to the logfile.

If you were like me, I would write a script to fullfill the tasks and call it from a login script (if present) as part of the login process ...

Klaus.

---

**K_Schulte** 4 Apr 2012 9:33 AM

OOOPSSS!!!

@Jason: Sorry, but I had the comment box open for some minutes and didn't notice that you asked for nearly the same details, I wanted to know :-)))

A great, but rare coincidence! ... Wellcome to the club *sss*

Klaus

---

**Nathan Linley** 4 Apr 2012 4:08 PM

Is a last reboot the time the machine last came online, or when it last shutdown?

---

4 Apr 2012 4:47 PM

**Justin Stokes**

Should we be assuming that the log version will always be 1.0? It's inclusion makes me think that a new log should be spawned at some point, but there is no mention. Just want to be sure that I'm not reading to much into that property.

---

**IamMred** 4 Apr 2012 5:43 PM

@Jason Stangroome Yes, the output file is named logonstatus.txt and it should be stored off the root in a file named logonlog. This log is stored on the local workstation, it is not going to be shipped to a central management station. You can assume that the script will be called from a logon script (logon.bat, logon.ps1, logon.cmd). But that your script will actually reside on the local workstation itself. Each time the user logs onto the network from the workstaion, the logon script runs, and in turn calls your script. You do not need to worry about scheduling the script.

---

**IamMred** 4 Apr 2012 5:47 PM

@K_Schulte yes, a folder off of any root drive. So my computer has windows installed on the C:\ drive, therefore I would create my C:\logonlog folder off of the C:\ drive. The logon process does not have anything to do with the desired output. I am just explaining how the script will be called later. No, you do not need to worry about the logon process because the script will be called from the network logon script. Exactly ... the script needs to fulfill all of the requirementsm, and it will be called from the login script as part of the login process.

---

**IamMred** 4 Apr 2012 5:49 PM

@Nathan Linley for this scenario, I am using last reboot time as the time the machine last came online ... not when it last shutdown.

---

**IamMred** 4 Apr 2012 5:50 PM

@Justin Stokes Yes, assume the log will always be 1.0. There is nothing in the scenario to indicate we will increment the log, or fork the output at anytime in the near future.

---

**LA Richards** 4 Apr 2012 8:03 PM

The event states that 8 pieces of information must be included. However, there are 9 bits of information present in the file. Should log in time be inferred? Is "Current Log" the header for the most recent login for the local machine?

---

**IamMred** 4 Apr 2012 8:30 PM

@LA Richards, yes the login time is inferred and should be included in the log file. Yes, "Current Log" is the heading for the most recent login to the local machine.

5 Apr 2012 3:08 AM

**Simon Wahlin**

Hi Ed,

If this script is running from the logon script it will run with user priviledges.

Can we assume that the user has access to create a folder and the logfile within it on the C-drive first time the script runs?

6 Apr 2012 5:25 AM

**scott_heath**

Are we really doing computer.domain name or computer.dnssuffix? For instance, my computer is in the somecompany.com domain, but my actual FQDN is computer.clients.somecompany.com.

**IamMred** 7 Apr 2012 6:27 PM

@Simon Wahlin Yes, you are correct. This is one reason I did not specifically want to say exactly how the script is run. It could be run from a logon script, it might also be assigned via Group Policy. I do not want rights to become an issue for this particular event -- There are enough things required to get the event correct, and I do not want it to be TOO difficult ... this is why I did not specify too many details around this aspect. You should assume that the user has access to create the folder and the logfile when the script runs the first time. I am not specifing C:\ because for people who dual boot (or triple boot) their systems, the root might not really be c:\. I specified off the root because I did not want you to have to worry with finding the user profile mydocuments folder -- in addition, storing logging information that may be collected at a later date in a user profile folder is a recipe for unnessary complexity. If you want, you can assume that the folder and the correct rights are assigned via a System Center package, and that the local user will therefore have right to create and to write to the file in that location. You should test to ensure that the folder does in fact exist. You might decide you then need to write to a different log file (maybe on a central share) that the folder and rights have not been created. However it helps you get the event straight in your mind. You might also add comments at the top of your submission that explain your reasoning.

**IamMred** 7 Apr 2012 6:36 PM

@Scott_heath You can use dns suffix if you wish. Or you can use the actual FQDN. It is up to you as to which information would be most useful. For example, I am may actually be in the northcarolina.northamerica.mycompany.com, but my dnssuffix may be mycompany.com. Now, you can choose which information would be best to use when attempting to locate the user and the computer later on. You may decide to use different pieces of information. IF you do, please add a note in a comment at the top of your script. I thought about having you record the UPN for the user instead of the NTLM type of login for the user, but that would have opened a different set of challenges and I did not want to overly complicate an already challenging event.