Running Head: MICROSOFT EVENTS

Microsoft Events: The Trouble I’m In

Jered McClure

Walden University

Microsoft Events: The Trouble I’m In

When doing this assignment, I realized I had disabled event logging/viewing on my system as my machine is built for performance gaming. As such, I needed to re-enable the event logging services. However, this ended up being nowhere near as simple as one would imagine. This, in itself, is evidence of the usefulness of event logs.

Initially I thought it may have had something to do with my registry. Therefore, I opened command prompt and used the *sfc /scannow* command to check for any instabilities on my system. This came up clean. My next recourse was to run a full scan using Spybot Search & Destroy for any malicious software (Safer Networking Ltd., 2012). That is when I discovered several pieces of malware on my system which my Virus scanner (which doubles as a spyware scanner) McAfee did not pick up (McAfee, Inc, 2011). After removing these unwanted applications, I was able to get the event viewer to operate again.

Upon viewing the event logs on my system, I discovered I had a huge number of errors, but none were critical or seriously detrimental to my system. For instance, I had many errors related to Windows update. However, it seems Windows has been trying to update a version of Microsoft Office which I no longer have installed on my system. Another error had to do with a DHCP IP address not being assigned to one of my NICs. This was due to that particular NIC being disabled as I possess two on my machine.

The overall interface and user interaction is fairly straight forward. However, finding the actual auditing menu was not a straight answer. It is listed under the security logs in the Windows Logs directory. By renaming the “Windows Logs directory” to “Auditing,” and renaming “security” to “security audits,” accessing the event viewer console would be more user friendly.

As for what logs I would like to modify, none really. As stated previously, my system is built for performance. That being said, I will disable the even logging function of my machine after this as it does take up system CPU time and memory resources. However, in terms of corporate network security, I can see exactly how I would use the auditing function.

The Security logs allow the system admin to monitor who does what and when on a workstation. By having an audit of everyone who logs onto a machine, the administrator will know who was logged in when events occurred. This can help in diagnosing and resolving system issues down the road.

Management of such security tasks over large networks would become a pain without a tool to do so, however. Microsoft offers such a tool in the Windows Management Instrumentation application (Microsoft Corporation, 2012). This program allows a network admin, with the use of the C language (or Visual Basic), to develop security scripts which can be rolled out across an entire domain. This allows the administrator to write the security rights once, and then implement them multiple times for the entire network.

Overall, the event viewer WMI combination allows for administrative capabilities which are not available to the network administrator otherwise. The tools are robust and thorough in their auditing process. However, they are not truly meant for a home computer, or a computer which needs every bit of their system resources focused on other processes. That being said, if security is of paramount concern, not having the event logging feature turned on is wholly not recommended.

Reference

McAfee, Inc. (2011). *For Home.* Retrieved February 17, 2012, from McAfee: <http://home.mcafee.com/Default.aspx>

Microsoft Corporation. (2012). *Windows Management Instrumentation.* Retrieved February 17, 2012, from MSDN Library: <http://msdn.microsoft.com/en-us/library/aa394582%28VS.85%29.aspx>

Safer Networking Ltd. (2012). *Home.* Retrieved February 18, 2012, from Spybot Serach & Destroy: <http://www.safer-networking.org/en/index.html>