brainlink

YOU RUN YOUR BUSINESS, LEAVE THE IT TO US!

The Secret About Windows Logging That Microsoft Doesn't Want You To Know



Configuring your Windows devices so that they collect informative logs will allow you to gain actionable and understandable intel about the performance of your system - but only if you know how to do it.

In past blogs, we've covered how vital a comprehensive log is in ensuring you have accurate and useful information about the performance and security of your systems - but just how does logging work when it comes to Windows?

In Windows, logging allows you to monitor events related to users accessing, modifying, and deleting sensitive files and folders on your network. A wide range of events can be audited in Windows, all of which fall in into several different categories:

- Account log-on events – these are instances of a user logging on to or logging off from another computer in which this computer is used to validate the account, as well as which domain controller authenticated the user. You can also track log-on events involving a specific server.
- Account management – these are instances of account management tasks being performed on a computer, such as password changes, user account, group modifications, etc.
- Directory service access – these are instances of a user accessing an Active Directory object with its own specified system access control list (SACL).
- Object access – these are events of a user accessing an object -- files, folders, registry keys, printers, etc. -- with its own specified SACL.
- Policy change – these are instances of a change to user rights assignment policies, audit policies, or trust policies.
- Privilege use – these are instances of a user exercising a user right.
- Process tracking – detailed tracking information for instances including program activation, process exit, handle duplication, indirect object access, etc.
- System events – these are instances of a user restarting or shutting down the computer, as well as when an event occurs that has an effect on either the system security or the security log.

There are some caveats though - each category also includes several different event types that may be triggered, and may be enabled for the auditing of successful of failed events. This is useful because it will allow you to track when a user attempted to perform a task or access an object, regardless of whether they were successful or not. By enabling any of these audit categories, Windows will then write messages to the event log whenever an audited event occurs.

That said, here's the big secret - Windows' auditing capabilities pale in comparison to other available options. The reality is that, when enabled, auditing will provide you with an overwhelming amount of information, little of which you will be able to make use of. That's why it's worth checking out other options.

Sysmon from Sysinternals, for example, is a highly capable Host-level tool for event tracking that will help you detect advanced threats that enter into your network. As compared to Antivirus/ HIDS solutions, Sysmon offers deep monitoring of system activity, logging high-confidence indicators of advanced attacks.

Sysmon can monitor the following events on your Windows systems:

- Process creation
- Process termination
- Network connections
- File creation timestamps changes
- Driver/image loading
- Create remote threads
- Raw disk access
- Process memory access

While some of these events can be collected through the previously mentioned Windows auditing capability, you would still gather a lot of useless information, without getting the actionable details offered through Sysmon.

Sysmon can track key events that you need in order to trace attacker activity and increase host visibility, including:

Event Class	Event IDs	Rate	Author's Recommendation	Importance
Process Create	1	Low-Medium	Log these events	Detect initial infection and malware child processes. Hashes captured by the Sysmon driver can be investigated using VirusTotal.com
Process Terminate	2	Low-Medium	Log these events (for forensic investigations)	Useful for forensic investigations. May be correlated with process creation events
Drive Load	6	Low		Detect device drivers loading
Image Load	7	High	Log these events (for forensic investigations)	Detect DLL injection, unsinged DLL loading
File Creation Time Changed	2	Medium-High	Log these events	Detect anti-forensic activity (timestamp changed to cover tracks)
Network Connection	3	High	Log these events (use filtering)	Identify network activity, connection to malware C&C servers, connection to ransomware server to download encryption keys
CreateRemoteThread	8	Low-Medium	Log these events	Detect code injections used by malware Credential theft tools also use this technique to inject their code into the LSASS process
RawAccessRead	9	Low	Log these events	Detect dropping off SAM or NTDS.DIT from compromised hosts

However, keep in mind that Sysmon doesn't offer anything in terms of analysis - you can use other tools to visualize and investigate the raw events, but you'd have to handle it yourself...

Unless you choose to partner with Brainlink.

The Brainlink team knows how important logging is, and we're ready to help you set up a comprehensive and simple Windows logging system at your business.

Our BrainSENSE logging solution is perfectly suited to integrate with your Windows systems to deliver actionable this data in easy-to-use and read dashboards that are customizable and tailored specifically to your business.

Start harnessing real information about your network for the good of your business by reaching out to us at (347) 460-2238 or raj@brainlink.com for more information about our logging solution, BrainSENSE, and what it will do for your business.