How can I figure out which user modified a file?

devblogs.microsoft.com/oldnewthing/20130418-00

April 18, 2013

Raymond Chen

The `GetFileTime` function will tell you *when* a file was last modified, but it won't tell you who did it. Neither will `FindFirstFile`, `GetFileAttributes`, or `ReadDirectory-ChangesW`, or `FileSystemWatcher`.

None of these the file system functions will tell you which user modified a file because the file system doesn't keep track of which user modified a file. But there is somebody who *does* keep track: The security event log.

To generate an event into the security event log when a file is modified, you first need to enable auditing on the system. In the *Local Security Policy* administrative tool, go to *Local Policies*, and then double-click *Audit Policy*. (These steps haven't changed since Windows 2000; the only thing is that the Administrative Tools folder moves around a bit.) Under *Audit Object Access*, say that you want an audit raised when access is successfully granted by checking *Success (An audited security access attempt that succeeds)*.

Once auditing is enabled, you can then mark the files that you want to track modifications to. On the *Security* tab of each file you are interested in, go to the *Auditing* page, and select *Add* to add the user you want to audit. If you want to audit all accesses, then you can choose *Everyone*; if you are only interested in auditing a specific user or users in specific groups, you can enter the user or group.

After specifying whose access you want to monitor, you can select what actions should generate security events. In this case, you want to check the *Successful* box next to *Create files / write data*. This means "Generate a security event when the user requests and obtains permission to create a file (if this object is a directory) or write data (if this object is a file)."

If you want to monitor an entire directory, you can set the audit on the directory itself and specify that the audit should apply to objects within the directory as well.

After you've set up your audits, you can view the results in *Event Viewer*.

This technique of using auditing to track who is generating modifications also works for registry keys: Under the *Edit* menu, select *Permissions*.

Exercise: You're trying to debug a problem where a file gets deleted mysteriously, and you're not sure which program is doing it. How can you use this technique to log an event when that specific file gets deleted?

Raymond Chen

Follow