Why does saving a file in Notepad fire multiple FindFirstChangeNotification events?

devblogs.microsoft.com/oldnewthing/20140507-00

Raymond Chen

Many people have noticed that the `ReadDirectoryChangesW` and `FindFirstChange-Notification` functions (and therefore their BCL equivalent `FileSystemWatcher` and WinRT equivalent `StorageFolderQueryResult`) fire multiple `FILE_ACTION_MODIFIED` events when you save a file in Notepad. Why is that? Because multiple things were modified. Notepad opens the file for writing, writes the new data, calls `SetEndOfFile` to truncate any excess data (in case the new file is shorter than the old file), then closes the handle. Two things definitely changed, and a third thing might have changed.

- The file last-modified time definitely changed.
- The file size definitely changed.
- The file last-access time might have changed.

It's therefore not surprising that you got two events, possibly three. Remember the original design goals of the `ReadDirectoryChangesW` function: It's for letting an application cache a directory listing and update it incrementally. Given these design goals, filtering out redundant notifications in the kernel is not required aside from the performance benefits of reduced chatter. In theory, `ReadDirectoryChangesW` could report a spurious change every 5 seconds, and the target audience for the function would still function correctly (albeit suboptimally). Given this intended usage pattern, any consumer of `ReadDirectory-ChangesW` needs to accept that any notifications you receive encompass the minimum information you require in order to keep your cached directory information up to date, but it can contain *extra* information, too. If you want to respond only to actual changes, you need to compare the new file attributes against the old ones.

Bonus chatter: Actually, the two things that changed when Notepad set the file size are the allocation size and the file size (which you can think of as the physical and logical file sizes, respectively). Internally, this is done by two separate calls into the I/O manager, so it generates two change notifications.

Raymond Chen

Follow