

Wait, so does moving a file recalculate inherited permissions or doesn't it?

 devblogs.microsoft.com/oldnewthing/20130924-00

September 24, 2013



Raymond Chen

A customer had a question about whether moving a file recalculated inherited permissions. They found that on their Windows Server 2008 R2 machine, if they moved a file between directories with different inheritable ACEs, then the security descriptor is recalculated to match the destination folder, if they perform the move from the machine itself. The same thing happens if they go to a machine running Windows 7. However, if they repeat the experiment from a machine running Windows XP or Windows Server 2003, then the security descriptor is preserved across the move. The customer is confused. Why does the behavior change based on the version of Windows running on the *client*, even though the files themselves are kept on the same server? The explanation is given in a few places:

- [Knowledge Base article 310316](#) describes how Windows Explorer behaves on Windows XP and Windows Server 2003.
- [Knowledge Base article 2617058](#) describes how Windows Explorer behaves on Windows 7 and Windows Server 2008 R2.
- [An old article of mine](#) discusses the issue mostly at a file system level, but discusses the Explorer angle towards the end.

Even with these explanations, the customer remained confused. “Why does the permission depend on the operating system running on the client? The files are on the server, so regardless of the client operating system, it should be following the rules which apply to the server, right?” There are two different operations here. Suppose I told you, “When you buy clothes from the store, it will have the store sticker on it. You must remove the sticker yourself, and you should also wash the clothes before wearing it the first time, because the store puts powder in the bag to keep the clothes from getting moldy.” You then say, “That is not true. When I go to my closet to get clothes I recently bought from the store, the store stickers are already gone, and there is no powder.” That’s because you live with your parents, and your mother takes your clothes, removes the stickers, washes the clothes, and then hangs them up in your closet. The underlying file system “move” operation preserves the ACLs from the source. On the other hand, if you use Explorer to move the files, then you are not using the underlying file system “move” operation directly. Your mother is moving the files. And

when mother Explorer moves the files, she also *edits the ACLs* based on the nature of the source and destination folders, as described in the aforementioned Knowledge Base articles. Furthermore, different versions of mother Explorer *edit the ACLs in different ways*. That is why the behavior is dependent upon the client operating system. When you move the file from a client machine connected to the server, the client machine asks the server to move the files (which preserve the ACLs since that's what the low-level "move" operation does), and then the client machine *goes back in and edits the ACLs* in a client-specific way.

It is therefore the client operating system which controls how the ACL editing is performed, because it is the client operating system which is editing the ACLs.

Raymond Chen

Follow

