The case of the volume label that doesn't change

devblogs.microsoft.com/oldnewthing/20161129-00

November 29, 2016

Raymond Chen

A customer liaison forwarded a problem from their customer: When the customer changed the volume label on a drive, the change is not reflected in Explorer. Explorer continues to show the old volume label.

A ProcMon trace revealed that `svchost.exe` running as `NT AUTHORITY\SYSTEM` attempted to open the root of the drive but got `STATUS_ACCESS_DENIED`. The access was coming from the shell hardware service at a point where it calls `GetVolumeInformation` to get the volume label.

Okay, that makes sense that the shell hardware service was trying to access the volume to read the volume label. After all, it was told that there was a change to the volume label, so it's going to the volume to see what the new label is. The question is why the shell hardware service, running as `SYSTEM`, got `STATUS_ACCESS_DENIED`.

I asked, "How did that happen? The `SYSTEM` account should have full access to the drive by default. Did the customer apply a custom ACL that revokes `SYSTEM` access? You'll find that a lot of things stop working when you revoke `SYSTEM` access."

The customer liaison wrote back, "Indeed, the customer did remove the `SYSTEM` account from the drive's permissions. I am not sure exactly what they were thinking when they revoked `SYSTEM` access. I need to ask them."

We didn't hear back from the customer, so maybe the customer was too embarrassed to explain why they revoked `SYSTEM` access to the drive.

Another case of a customer changing a security setting without really understanding why they did it, and then wondering why stuff stops working.

Raymond Chen

Follow