I set the same ACL with the GUI and with icacls, yet the results are different

devblogs.microsoft.com/oldnewthing/20191118-00

November 18, 2019

Raymond Chen

A customer found that if they used the GUI and the `icacls` program to deny Delete permission to a folder, the results were different, even though the resulting ACLs are the same.

Create a user, say, *Bob*, and create a folder, say, `C:\test`.

With the GUI

- Right-click the folder and select *Properties*.
- Go the *Security* tab, click *Advanced*.
- Click the *Add* button to add a new ACE.
- Select *Bob* as the Principal.
- Set the *Type* to *Deny*.
- Click *Show advanced permissions*.
- Check *Delete* and uncheck everything else.
- Click *OK* a bunch of times to save the changes.

With `icacls`

> From a command prompt, type `icacls C:\test /deny Bob:D`

If you followed the GUI steps, then Bob can open the directory in Explorer. On the other hand, if you followed the `icacls` steps, then Bob cannot open the directory in Explorer.

In both cases, running `icacls` to view the permissions report the same results:

```
C:\> icacls c:\test
test THISPC\Bob:(DENY)(D)
     BUILTIN\Administrators:(I)(OI)(CI)(F)
     NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
     BUILTIN\Users:(I)(OI)(CI)(RX)
     NT AUTHORITY\Authenticated Users:(I)(M)
     NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(IO)(M)
```

How is it possible that the permissions are identical, yet the results are different depending on *how* you set the permissions?

The problem is that your tools are lying to you. The Deny ACE on the directory is not what `icacls` reports.

If you change the security with the GUI, then the Deny ACE is `0x00010000` = `DELETE`. But if you change it with the `icacls` program, then the Deny ACE is is `0x00110000` = `DELETE | SYNCHRONIZE`.

So the `icacls` program is lying when it says that it denied Delete (D) permission. It actually denied both Delete and Synchronize.

And then on top of that, the `icacls` program is lying when it says that the actual ACE is a Deny D. It's hiding the denied `SYNCHRONIZE` access.

And it's that denied `SYNCHRONIZE` access which is the difference. Explorer cannot open a folder where `SYNCHRONIZE` is denied. (And the command prompt cannot `chdir` into such a directory either.)

I'm guessing that the `icacls` is doing this extra work as a courtesy, but it also makes diagnosing problems more difficult.

Raymond Chen

Follow