

Re: NTFS Effective Permissions?

Source: <http://www.tech-archive.net/Archive/Scripting/microsoft.public.scripting.wsh/2004-12/0465.html>

From: Al Dunbar [MS-MVP] (alan-no-drub-spam_at_hotmail.com)

Date: 12/30/04

Date: Wed, 29 Dec 2004 21:05:45 -0700

"Gerry Hickman" <gerry666uk@yahoo.co.uk> wrote in message
news:OL2NXRf7EHA.2452@TK2MSFTNGP14.phx.gbl...

> *Hi,*

>

> > *For example, I often see NTFS objects whose security settings as
displayed*

> > *in the GUI are identical, while a script that uses ADsSecurity.dll to*

> > *display the detailed security settings shows that they are not the same.*

I

> > *assume that this has something to do with how permissions were inherited
by*

> > *the objects and/or how they were created.*

>

> *Can you clarify? If you go into the "Advanced" tab of the GUI, are you*

> *saying it's not the same as what you see when using a script? Do you*

> *have any such folder on your computer where you can test this? When you*

> *run CACLS on such a folder, does it agree with the GUI, or with your
script?*

OK, there are two profile folders on my XP system, Jon and Al. Obviously,
these are permitted differentially to two different accounts, so I will
focus on the permissions that are extended to "SYSTEM". In the advanced
security settings tab, each folder shows the following for SYSTEM:

type = allow

name = SYSTEM

permission = full control

inherited from = <not inherited>

apply to = this folder, subfolders and files

Same so far. If I click the respective "Edit..." buttons, they show a check
in every "allow" box. Still the same, identical, in fact.

I then run a vbscript (you'll have to trust me on this a little bit), and it
shows two entries for SYSTEM on the Jon folder, but only one on the Al
folder. Below is (and also attached) is the complete output from this
script:

microsoft.public.scripting.wsh: Re: NTFS Effective Permissions?

```
C:\Documents and Settings\Jon
no. flags aceflgs acetype accessmask trustee
1 0 0 0 001F01FF MYPC\Jon
2 0 0 0 001F01FF NT AUTHORITY\SYSTEM
3 0 0 0 001F01FF BUILTIN\Administrators
4 0 11 0 10000000 MYPC\Jon
5 0 11 0 10000000 NT AUTHORITY\SYSTEM
6 0 11 0 10000000 BUILTIN\Administrators
C:\Documents and Settings\Al
no. flags aceflgs acetype accessmask trustee
1 0 3 0 001F01FF BUILTIN\Administrators
2 0 3 0 001F01FF MYPC\Al
3 0 3 0 001F01FF NT AUTHORITY\SYSTEM
```

Sure, they both seem to give FULL