

Re: Default Registry Permissions

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2006-10/msg00147.html>

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
 - *Date:* Thu, 19 Oct 2006 08:20:23 -0700
-

Well, I am pretty stumped.

I doubt that the SAFER (software restriction policy) settings have any bearing on your issue of the ACL'ing of and in software\classes

If there is a setting to determine the default ACL for new subkeys somewhere in Windows (as shipped) I have never noticed it anywhere.

What I do not get is how your reg perms got that way to start with, and so, whether what did that is still operative (hooked event of create subkey).

Roger

"G. Stoynev" <gstoynev@xxxxxxxxxx> wrote in message
news:1161269257.853401.308040@xx

Straight to your questions:

How are you determining it is Everyone Full on your clean install ?

It's Everyone: Full now, not on the clean install. And the clean install is probably irrelevant.

What are the permissions you are seeing?

As a container,
HKEY_LOCAL_MACHINE\SOFTWARE\Classes allows "Everyone – Full Control" – that's the only setting, in addition to "Allow inheritable permissions to propagate to this object"

My class however, after registering my DLL using regsvr32,
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\myDLL.myClass allows only SYSTEM and the Administrators group "Special Permissions – Full Control"

Do you have any idea, what Windows security mechanism is responsible

Re: Default Registry Permissions

for determining what permissions are assigned to the myDLL.myClass key.

It's not the container's ACL.

As far as I can tell, it's not a local security policy. The only remotely related setting that I've found so far are under the Local Security Settings snap-in:

Security Settings\Software restriction policies\Enforcement ("All software except libraries" and "All users")

and

Security Settings\Software restriction policies\Additional Rules\%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot% ("Unrestricted")

Security Settings\Software restriction policies\Additional Rules\%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%*.exe ("Unrestricted")

Security Settings\Software restriction policies\Additional Rules\%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot\System32*.exe ("Unrestricted")

Security Settings\Software restriction policies\Additional Rules\%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir% ("Unrestricted")

Under Security Settings\Software restriction policies\Security Levels, "Unrestricted" is the default one; "Disallowed" is also defined as "Software will not run, regardless of the access rights of the user."

I've confirmed these settings by running "Resultant Set of Policy" on the login I use as well as on the "computer policy settings only".

Note that in no snap-in any policy showed as defined under "... \Security Settings\Registry

I haven't been able to run "Security Configuration and Analysis" on my "C:\windows\security\Database\secedit.sdb". I use NTBackup to copy the file to a temp folder and get "Error while opening the file". (I use NTBackup because regular "Copy" comes back with "File in use by another program" error.

Thanks.

(you can use my profile email to speed up communication – I can also send snapshots that way.)

Roger Abell [MVP] wrote:

"G. Stoynev" <gstoynev@xxxxxxxx> wrote in message
news:1161206786.232071.150850@xx

Thank you for your reply. My comments are below.

Re: Default Registry Permissions

Roger Abell [MVP] wrote:

Your registry seems to have been changed as what you state to be the ACL on HKLM\Software\Classes is not what is set by default, at least with a clean install (I am not sure what you would see on a machine upgraded to W2k3 or R2 from earlier versions with a history of upgrade clear back to NT 4)

Can't comment on that as I didn't take a note what the ACL looked like freshly installed. But it's a clean 2003 install and R2 immediately after that.

default ACL'ing runs:

System Full Key+Subkeys
Administrators Full Key+Subkeys
Users Read Key+Subkeys
Creator Owner Full Subkeys
Power Users Special Key+Subkeys
(where PU exists; Special = Full less Create link, Write DAC, Write Owner)

How are you determining it is Everyone Full on your clean install ?

It is my understanding that just using regsvr32 would add the reg entries allowing them to have an initial ACL as determined from the ACL on their parents. This is apparently not happening for you, but you do not indicate use of an installer that might be adjusting the ACL after regsvr32 runs.

No installer involved. I run regsvr32 and immediately after that I check the permissions.

Re: Default Registry Permissions

What are the permissions you are seeing?

PS

SP1 for W2k3 R2 has not come out

Control Panel->System displays exactly the following string:

Microsoft Windows Server 2003 R2

Standard Edition

Service Pack 1

Well, I guess you cannot believe that interface then.

(Note that W2k3 R2 initial release was in lock-step with W2k3 Sp1)