

RE: Verifying if ntfs files/folders rights are inherited or not...

RE: Verifying if ntfs files/folders rights are inherited or not...

Source:

<http://www.tech-archive.net/Archive/Scripting/microsoft.public.scripting.vbscript/2006-12/msg00678.html>

- *From:* Claude Lachapelle <ClaudeLachapelle@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 22 Dec 2006 10:52:00 -0800
-

Even when rights are inherited, sometimes I got 3 instead of 19??? When I RE-APPLY the same security (remove the inherit from parent flag from the explorer GUI, and reset it to inherit again), now I got 19...

What I understand (correct me if I'm wrong), it is probably related to the fact that those directories or files are coming from an NTFS of NT 4.0 , where inheritance was not impleted, and explorer GUI of Windows 2003 "interpret" SAME SECURITY Of PARENT WHEN NT 4.0 NTFS = INHERIT FROM PARENT?

Does this is how it is made???

Thanks.

"Claude Lachapelle" wrote:

Hi!

I'm currently working on a vbscript that will allow me to identify files or folders where inheritance have been removed or altered with explicit ntfs security.

The problem is, I don't know how to manipulate the ace flags to know if the rights are inherited or not:

AceFlags Data type: uint32
Access type: Read/write

OBJECT_INHERIT_ACE 0x1 (1) Non-container child objects inherit the ACE as an effective ACE. For child objects that are containers, the ACE is inherited as an inherit-only ACE unless the NO_PROPAGATE_INHERIT_ACE bit flag is also set.

CONTAINER_INHERIT_ACE 0x2 (2) Child objects that are containers, such as directories, inherit the ACE as an effective ACE. The inherited ACE is inheritable unless the NO_PROPAGATE_INHERIT_ACE bit flag is also set.

NO_PROPAGATE_INHERIT_ACE 0x4 (4) If the ACE is inherited by a child object,

RE: Verifying if ntfs files/folders rights are inherited or not...

the system clears the OBJECT_INHERIT_ACE and CONTAINER_INHERIT_ACE flags in the inherited ACE. This prevents the ACE from being inherited by subsequent generations of objects.

INHERIT_ONLY_ACE 0x8 (8) Indicates an inherit-only ACE which does not control access to the object to which it is attached. If this flag is not set, the ACE is an effective ACE which controls access to the object to which it is attached.

Both effective and inherit-only ACEs can be inherited depending on the state of the other inheritance flags.

INHERITED_ACE 0x10 (16) The system sets this bit when it propagates an inherited ACE to a child object.

Here is my code:

```
Set wmiFileSecSetting = GetObject(
"winmgmts:Win32_LogicalFileSecuritySetting." & "path=" & strFolderName &
"" )
```

```
' Obtain the existing security descriptor for folder
RetVal = wmiFileSecSetting.GetSecurityDescriptor(wmiSecurityDescriptor)
```

```
If Err <> 0 Then
WScript.Echo "GetSecurityDescriptor failed" & VBCRLF & Err.Number &
VBCRLF & Err.Description
WScript.Quit
End If
```

```
' Retrieve the content of Win32_SecurityDescriptor DACL property.
' The DACL is an array of Win32_ACE objects.
DACL = wmiSecurityDescriptor.DACL
```

```
' Obtain the trustee for each access control entry (ACE)
For each wmiAce in DACL
```

```
' Get Win32_Trustee object from ACE
Set Trustee = wmiAce.Trustee
```

```
wscript.echo Trustee.Domain & "\" & Trustee.Name
wscript.echo wmiAce.AceFlags
Next
```

When I'm reading the wmiAce.AceFlags, I get 0, 3, 19 values... what does that mean???

Thanks.

Claude Lachapelle
Systems Administrator, MCSE

RE: Verifying if ntfs files/folders rights are inherited or not...