

## Re: Can't get something basic to work (WMI)

*Source:* <http://www.tech-archive.net/Archive/VC/microsoft.public.vc.language/2004-04/0741.html>

---

*From:* Ivan Brugiolo [MSFT] ([ivanbrug\\_at\\_online.microsoft.com](mailto:ivanbrug_at_online.microsoft.com))

*Date:* 04/18/04

Date: Sun, 18 Apr 2004 11:32:43 -0700

This has nothing to do with DCOM, but with the security packages in the SSPI infrastructure, of which DCOM, like RPC and the very same rdbss.sys / srv.sys (where the SMB/CIFS protocols are implemented) are just plain clients.

the NTLM Authentication Package does not allow delegation, while Kerberos does. This is the only essence of the problem. Attempting to delegate impersonated credentials from NTLM will end up in the usage of the Null-Session, that is on average forbidden in many well administered networks.

Delegation is a feature of networks with a W2K or greater authenticaiton infrastructure provided by Active Directory.

The process created by WIn32\_Process.Create on the remote machine will NOT be created under the LocalSystem account.

If will be created under the account making the call.

It will be created in the "Service-0x0-3e7\$" WindowsStation, that is not the "Winsta0" windowstation.

This makes the process to appear invisible.

One more thing about the net-use commands is the fact that the shares are "local" to a logon session (in WinXP and above), and thus they are designed to not contaminate each other.

--

This posting is provided "AS IS" with no warranties, and confers no rights.

Use of any included script samples are subject to the terms specified at

<http://www.microsoft.com/info/copyright.htm>

"Manfred Braun" <aa@bb.cc> wrote in message

news:eECbuRVJEHA.2904@TK2MSFTNGP09.phx.gbl...

> Hi,

>

> just a note from a person, which will never understand DCOM in all details,

> but ....

>

> The process, you create, is running on the remote box under the

> <LocalSystem> account, which has no network access rights. The credentials

> specified, are only used to check, if the calling user [which requests the

> creation of the remote process] is allowed to do this. You could write a

> small cmd or vbs, which simply waits for, say a minute, and then go to the

> taskmanager of this machine and you'll see the process running.

Re: Can't get something basic to work (WMI)

microsoft.public.vc.language: Re: Can't get something basic to work (WMI)

>  
> As an administrator, I found this behavior always very annoying and there  
> seem to be no simple way in the MS world to solve this problem.  
> Additionally, you are not able to display something on the screen for the  
> same reason.  
>  
> What helps:  
>  
> Create two separate components, I've done that for experimental purposes  
> only, so, please don't ask for the code, it is too muddy to become  
> published. One component to display a message on the screen, one to do a  
> network connection. Install this components, I've created them in script  
> [.wsc], on the remote box. In the component management, configure the  
> component, which displays the message, to run under the interactive user.  
> Configure the second component to run under a well-known admin account,  
> which you are able to control. Write a script, which instantiates the  
> network-component and store this script onto the remote box. Execute this  
> script with your remote connection via WMI and it will work. Additionally,  
> this way you can start a second script, which instantiates the  
> display-component and shows some message to the logged-on user, if any.  
>  
> You can do all this things locally and export the components via  
> component-services as MSI files. This MSI files in turn can be installed  
> remotely via WMI.  
>  
> Hope, this leads you into the right direction.  
>  
> Best regards,  
> Manfred Braun  
>  
> (Private)  
> Mannheim  
> Germany  
>  
> mailto:\_manfred.braun@manfbraun.de  
> (Remove the anti-spam-underscore to mail me!)  
>  
> "Rob Bolton" <nospam@nospam.com> wrote in message  
> news:eeujDvTJEHA.2412@TK2MSFTNGP12.phx.gbl...  
> > Thanks very much. I just started learning WMI so haven't studied  
scripting  
> > yet. Will spend some time deciphering this and try again. BTW (for my  
own  
> > information), is this the generally recommended way of doing it? I  
> followed  
> > the (fairly short C++) example at the following link which appears to be  
> > more mainstream (I could be wrong):  
> >  
> >  
<http://www.codeguru.com/Cpp/W-P/system/processesmodules/article.php/c2831/>  
> >  
> > BTW, please feel free to get technical if required (I'm experienced).  
> > Thanks.  
> >  
> > "Jiachuan Wang [MSFT]" <jiaawang@online.microsoft.com> wrote in message  
> > news:%23S7mxDKJEHA.2572@TK2MSFTNGP12.phx.gbl...  
> > > try the following script.  
> > >  
> > >  
> > > Function ProcessCreate(Server, cmd)  
> > >  
> > > Dim process, processid, nRet

microsoft.public.vc.language: Re: Can't get something basic to work (WMI)

```
> > >
> > >
> > >
> > >         If Server = "" THEN
> > >
> > >                 SET process =
> > >
> > >
>
GetObject("WinMgmts:{impersonationLevel=impersonate}!/root/cimv2:Win32_Proce
> > > ss")
> > >
> > >         ELSE
> > >
> > >                 SET process =
> > > GetObject("WinMgmts:{impersonationLevel=impersonate}!/" & Server &
> > > "/root/cimv2:Win32_Process")
> > >
> > >         End IF
> > >
> > >         nRet = process.Create(cmd, null, null, processid)
> > >
> > >         If (nRet <> 0) Then WScript.Quit nRet
> > >
> > >         SET process = Nothing
> > >
> > > End Function
> > >
> > >
> > > If WScript.Arguments.Count <> 2 Then
> > >
> > >         WScript.Echo "Usage: cscript " & WScript.ScriptName & "
> server
> > > command"
> > >
> > >         WScript.Quit 1
> > >
> > > End If
> > >
> > >
> > > On Error Resume Next
> > >
> > > ProcessCreate WScript.Arguments(0), WScript.Arguments(1)
> > >
> > > If Err Then
> > >
> > >         WScript.Quit Err.Number
> > >
> > > Else
> > >
> > >         WScript.Quit 0
> > >
> > > End If
> > >
> > >
> > > --
> > > This posting is provided "AS IS" with no warranties, and confers no
> > > rights.
> > >
> > >
```

