

# Re: WMI/COM and ExecNotificationQueryAsync for Win32\_NTLogEvent

---

*Source:*

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.networks/2006-02/msg00446>

---

- *From:* roger\_man <[rogerman@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:rogerman@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 22 Feb 2006 10:41:27 -0800
- 

I have run some more testing, and it turns out the error I am getting is in fact a access denied error. So it seems that I need to set up security and permissions to correctly access the windows NT event log. I see in the VB examples these lines of code:

```
Set objWMI = GetObject("winmgmts:" _
& "{impersonationLevel=impersonate}!\" _
& strComputer & "\root\cimv2")
Set colLoggedEvents = objWMI.ExecQuery _
("Select * from Win32_NTLogEvent Where Logfile = 'System'")
```

What is the corresponding C++/COM version of this? I can't seem to find the correct incantation in COM land to get the system log notifications through an asynchronous query handler?

Thanks so much,

"roger\_man" wrote:

Thanks, yes, I have looked at those, but none of them have any examples specifically for Win32\_NTLogEvent. I think it might either be a security thing or a WQL query issue, since when I call ExecNotificationQueryAsync, I get an error message which does not map to any of the standard error messages one can get from this call. I am using an unsecured apartment for security, could that be an issue?

Thanks,

"Scherbina Vladimir" wrote:

Hello, roger\_man.

"roger\_man" <[rogerman@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:rogerman@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message

Re: WMI/COM and ExecNotificationQueryAsync for Win32\_NTLogEvent

news:COBB7E48-1E78-453D-947C-7E9112926B98@xxxxxxxxxxxxxxxxxxxx

Hi,

I am trying to create an application that uses WMI to listen for Win32\_NTLogEvent messages from the local machine through a asynchronous listener via ExecNotificationQueryAsync in a C++/COM environment, and I'm not having a whole lot of luck. I am finding examples to do this with Visual Basic, but somehow they do not translate into C++/COM very well.

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmisdk/wmi/wmi\\_c\\_application\\_c](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmisdk/wmi/wmi_c_application_c)

–  
this list of c++ examples will be usefull for you.

Particularly, I am having trouble creating the WQL query in the function:

```
hresult = pSvc->ExecNotificationQueryAsync(
    _bstr_t("WQL"),
    _bstr_t("SELECT * "
"FROM __InstanceCreationEvent WITHIN 1 "
"WHERE TargetInstance ISA 'Win32_NTLogEvent'"),
    WBEM_FLAG_SEND_STATUS,
    NULL,
    pStubSink);
```

Something along these lines, but for some reason I am not able to connect to this event. I know I have to have security permissions in order to receive these events (which I beleive I do), but is there something wrong with my WQL query that is keeping me from connecting to and listening to NT log events?  
What else could I be doing wrong with this approach?

Thank you so much for any and all assistance,

Re: WMI/COM and ExecNotificationQueryAsync for Win32\_NTLogEvent

—  
Vladimir