

Re: 16-bit process

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.wmi/2004-03/0326.html>

From: AOUser (*rjgeers_at_hotmail.com*)

Date: 03/25/04

Date: 25 Mar 2004 01:20:30 -0800

Scott,

Thx for your input. Your method is more a workaround rather than a solution for my problem. I can't just kill the NTVDM process; other processes may use this process too.

And i want to be triggered on the drwatson process (or other unwanted 16-bit processes).

Let's make my need more clear.

The servers (amount: 50) i was talking about are located on different places around the country. Some (error) messages only appear on the server console.

I can't logon on each of these consoles to check whether there are console messages. One thing we found out is that most of these messages are drwatsons, explaining what was wrong.

To intercept these drwatsons (rather then to log on each of those servers to check the console status) a (tivoli resource)model was made to check the existance of predefined processes (or cpu intensive processes like some screensavers). THE 32-bit process are relatively simple to check. If it occurs, the operater wil get an event (kind of pop-up). I made the same model for unwanted services to start (some printerdrivers may hang up the system).

In this event (pop-up) i want to have an description or name of the unwanted process. In this scenario: "The process 'Drwatson.exe' has started on server nlab123". It is the Operater who must check this server and who must decide what to do with the process and the cause of the process. So just killing the process is not desirable.

I dont think i can use your query. The problem I see is that more processes can use ntvdm.exe and the thread number differs every time a 16-bit process is started.

One thing occupies my mind: In the taksmgr I can see the name of the 16-bit process within ntvdm.exe. But CIM/WMI doesnt show it anywhere. And using the process explorer (sysinternals) I can see the process NTVDM.exe with all the handles. The type of the handle is 'File' ('name' is path of the program) and will be displayed as soon as the process starts. When the process isnt on the system, the type and name disappears.

Is CIM/WMI only made for 32-bits processes? Am i looking for a needle, but it isnt it there at all?

"[MS] Scott McNairy" <scotmc@online.microsoft.com> wrote in message news:<4061d283\$1@news.microsoft.com>...

> *NTVDM.exe is the controlling process and the 16 bit application can be terminated (not sure if that is what you want to do) by terminating the NTVDM.exe process. If you are looking for the threads this query will help – 16 bit apps like DrWatson are single threaded, + the controlling process NTVDM.exe and WowExec.exe, not sure what that one does, it also plays a role in running a 16 bit application. Once you have your processHandle, you can issue this query to get the relevant threads.*

>
> *select * from win32_process where caption = "ntvdm.exe"*

> *then...*

> *select * from win32_thread where processHandle = "676"*

>
> *NTVDM.exe is an application that provides the environment for a 16-bit process to execute on a 32-bit platform like Windows XP.*

>
> --

> *[MS] Scott McNairy*

> *WMI Test Engineer*

> *This posting is provided "As Is" with no warranties, and confers no rights.*

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

> *<http://www.microsoft.com/info/cpyright.htm>*

>
> *"AOUser" <rjgeers@hotmail.com> wrote in message news:1ddab067.0403240703.3308192d@posting.google.com...*

> > *We monitor our w2k servers with Tivoli Monitoring. This product uses WMI/CIM for getting the data. I created a model to intercept unwanted 32-bit processes. But with WMI I cant get the 16-bit processes(f.i. drwatson.exe).*

> > *THE 16-bit processes are gathered with ntvdm.exe (this has its own process id), but they dont have their own process id's. HELP. Where do I find*

> > *those process/threads in WMI/CIM?*

> > *Thx in advance.*