

Get quick info from a remote Windows machine with WMI and Powershell 2.0

This post is meant to offer some quick and easy ways to use Powershell and WMI for System Administrators. Many tools are available to find out attributes of machines on your network, but sometimes you need something quick, simple and direct. Below are some one-liners that I find useful.

WMI queries must be allowed on your systems, and you'll need Powershell 2.0 and administrative privileges.

If you're completely unfamiliar with Powershell, check out this page first:

<http://technet.microsoft.com/en-us/library/ee221100.aspx>

Example: Current logged on user

Long Version

```
Get-WmiObject win32_computersystem  
-Computer remote_computer | Select  
username
```

Slightly Shorter Version

```
gwmi win32_computersystem -comp
```

```
remote_computer | select username
```

What's Going On?

Get-WmiObject is querying the data in the **win32_computersystem** object. It queries the remote computer we specified by using the **-comp** tag, which can be either a machine name or IP address. Otherwise it would get results from the local machine. From the results of that query, we are displaying only the **username** value, which contains the name of the user that is currently logged on in the format *domain\username*. If no one is logged in, the result will be blank.

Other Useful WMI Queries

Try them for yourself! Just replace the values in the example with the values listed below.

WMI Object Name Value win32_OperatingSystem LastBootUpTime win32_OperatingSystem
Caption win32_OperatingSystem CSDVersion win32_LogicalDisk FreeSpace win32_LogicalDisk Size
win32_BIOS SerialNumber win32_ComputerSystem TotalPhysicalMemory

Of course there are many, many more...

Revision #3

Created 2010-04-02 20:43:23 UTC by Wilson, Jonathan

Updated 2010-04-02 23:46:21 UTC by Wilson, Jonathan