

## WMI Event Cmdlet Examples:

To Get list of network shares

```
Get-WmiObject -ComputerName . -Namespace root\cimv2 -Class Win32_Share
```

To Get list of GPOs applied to local system

```
Get-WmiObject -ComputerName . -Namespace root\rsop\computer - Class RSOP_GPO
```

WQL Query for all network adapters

```
Get-WmiObject -Query "select * from win32_networkadapter"
```

When a process (Notepad) starts

Register-WmiEvent

```
-Query "select * from _InstanceCreationEvent within 5 where  
TargetInstance ISA 'Win32_Process' and TargetInstance.Name = 'notepad.exe'"  
  
-Action { Write-Host -Object {"Process started" +  
$Event.SourceArgs.NewEvent.TargetInstance.Name} };
```

Disk free space drops below threshold

Register-WmiEvent

```
-Query "select * from _InstanceModificationEvent within 5 where  
TargetInstance ISA 'Win32_LogicalDisk' and TargetInstance.FreeSpace < 1000000000000"  
  
-Action { Write-Host -Object {"Free space dropped to {0} on drive{1}"  
-f $Event.SourceArgs.NewEvent.TargetInstance.FreeSpace,  
$Event.SourceArgs.NewEvent.TargetInstance.DeviceID} };
```

When a user logs on/off

Register-WmiEvent

```
-Query "select * from _InstanceCreationEvent within 5  
where TargetInstance ISA 'Win32_UserProfile' and  
TargetInstance.Loaded <> PreviousInstance.Loaded"  
  
-Action { Write-Host -Object "User logged on or off";
```

New Print job created

Register-WmiEvent

```
-Query "select * from _InstanceCreationEvent within 5  
where TargetInstance ISA 'Win32_PrintJob'"  
  
-Action { Write-Host -Object "New print job created";
```

\*\*\*\*\*

remotely starting notepad.exe on a remote computer.:

\$cred = get-credential

```
$process = Get-WmiObject -Query "SELECT * FROM Meta_Class WHERE __Class = 'Win32_Process'" -  
namespace "root\cimv2" -computername 'DESKTOP-SRRBF5O' -credential $cred $process.Create(  
"notepad.exe" )
```

\*\*\*\*\*

```
SELECT * FROM Win32_Service WHERE Started=0 AND StartMode="Auto"
```

```
select * from Win32_ComputerSystem
```

```
Select name, version from Win32_Bios
```

```
SELECT ThreadCount FROM Win32_Process WHERE ThreadCount>10
```

```
Get-WmiObject -Computer 127.0.0.1 -Namespace "root/cimv2" -Query "SELECT * FROM Win32_VolumeChangeEvent"
```

```
Get-WmiObject -Computer 127.0.0.1 -Namespace "root/cimv2" -Query "SELECT * FROM Win32_Service WHERE Started=0 AND StartMode='Auto'"
```

```
Get-WmiObject -Computer 127.0.0.1 -Namespace "root/cimv2" -Query "SELECT * FROM Win32_Service WHERE Started=0"
```

```
Get-wmiobject win32_computersystem
```

```
Get-WmiObject -Computer 127.0.0.1 -Namespace "root/cimv2" -Query "select * from Win32_ComputerSystem"
```

```
Get-WmiObject -Computer 127.0.0.1 -Namespace "root/cimv2" -Query "Select name, version from Win32_Bios"
```

```
Get-WmiObject -Computer 127.0.0.1 -Namespace "root/cimv2" -Query "SELECT * FROM Win32_ComputerSystem WHERE TotalPhysicalMemory < 2147483648"
```

```
Get-WmiObject -Computer 127.0.0.1 -Namespace "root/cimv2" -Query "SELECT ThreadCount FROM Win32_Process WHERE ThreadCount>10"
```