

Wmic-Beispiele

Auflistung der vorhandenen Treiber

```
wmic sysdriver get name
```

Auflistung der vorhandenen Treiber: zeigt, dass "list instance" in diesem Fall gleichbedeutend ist mit "get name":

```
wmic sysdriver list instance
```

Mit dem Windows-Installer installierte Produkte auflisten:

```
wmic product get
```

Software-Features auflisten (detaillierter als "Product"):

```
wmic softwarefeature get
```

Software-Elemente auflisten (detaillierter als "Softwarefeature"):

```
wmic softwareelement get
```

Hotfixes und Updates auflisten mit dem Alias "QFE"

```
wmic qfe list
```

Drei Eigenschaften des Alias "Logicaldisk" auswählen:

```
wmic logicaldisk get name,volumename,filesystem
```

Auflistung einiger Eigenschaften der aktuellen Prozesse mit vordefiniertem "list brief" im Ergebnis ähnlich dem Taskmanager:

```
wmic process list brief
```

Mit "Get" manuell ausgewählte Eigenschaften der aktuellen Prozesse - wieder ähnlich dem Taskmanager und identisch mit "list brief":

```
wmic process get ThreadCount,HandleCount,Name, Priority,ProcessId,WorkingSetSize
```

Vier wesentliche Eigenschaften der Systemdienste anzeigen:

```
Wmic service get caption, name, startmode, state
```

"Get" und "Get /Value": Breites Tabellenformat und simple Auflistung mit /Value, hier am Beispiel der User-Konten:

```
wmic useraccount get  
wmic useraccount get /value
```

Alle Eigenschaften der Klasse "Win32_OperatingSystem" (=Alias "os") in HTML-Ausgabe umleiten (OS.HTM anschließend per Doppelklick laden):

```
wmic os get /format:hform > os.HTM
```

Alle Eigenschaften der Klasse "Win32_OperatingSystem" (=Alias "os") und HTML-Ausgabe - wie letzter Befehl, nur mit anderer Syntax:

```
wmic /output:os.HTM os get /format:hform
```

Drei Eigenschaften der Systemtreiber mit HTML-Ausgabe; Die Sortierung nach einer bestimmten Spalte mit "Sortby" funktioniert nur mit dem breiten HTable-Format:

```
wmic sysdriver get name,pathname,startmode  
/format:htable:"sortby=StartMode" > drv.htm
```

Drei Eigenschaften der Systemtreiber, wieder mit Sortierung, hier aber mit dem simplen CMD-Filter Sort.EXE:

```
wmic sysdriver get name,pathname,startmode | sort /+63
```

Wmic-Ausgabe in die Zwischenablage leiten (hier Bios-Informationen):

```
wmic /output:clipboard bios list full
```

Instanzen von "LogicalDisk" auf Festplatten (Typ 3) einschränken:

```
wmic logicaldisk where "drivetype=3" get  
name,freespace,SystemName,FileSystem,Size,VolumeSerialNumber
```

Set-Befehl für Registry-Größe:

```
wmic registry set proposedsize=20
```

Create-Befehl für eine globale Systemvariable (mit dem Namen 'ZB', Wert '1'):

```
wmic environment create name="ZB", username="<SYSTEM>",variablevalue= "1"
```

Methode des Alias "Logicaldisk", um automatisches Checkdisk zu deaktivieren:

```
wmic logicaldisk call ExcludeFromAutochk "E:"
```

Methode des Alias "Process", um einen neuen Task zu erstellen:

```
wmic process call create "notepad.exe"
```

Beispiel für die Fähigkeit der "Create"-Methode des Alias "Process", ausführbaren Code eines NTFS-Streams zu laden. Das Beispiel geht der Kürze halber davon aus, dass sich Calc.EXE im aktuellen Verzeichnis befindet:

```
type calc.exe > dummy.txt:calc  
wmic process call create "dummy.txt:calc"
```

Einfacher Where-Filter: Aus allen Instanzen des Alias "Process" wird/werden jene/r mit dem Namen "iexplore.exe" ausgefiltert und mit der "Terminate"-Methode beendet:

```
wmic process where "name='iexplore.exe'" call terminate
```

Einfacher Where-Filter: Von den Systemdiensten nur Eigenschaften der aktuell gestarteten Dienste auflisten:

```
wmic service where (state="running") get caption, name, startmode, state
```

Filter mit logischem "UND":

```
wmic datafile where "drive='c:' and extension='JPG' and filesize<10000"  
call delete
```

Beispiel für einfachen Filter (nur tatsächlich gestartete Treiber):

```
wmic sysdriver where "started=true" get name,pathname
```

Process-Methode mit "UND"-Filter:

```
wmic process where "name='explorer.exe' and workingsetsize>30000000" call terminate
```

Beispiel für eine-Methode, die zwingend (irgend) einen Filter voraussetzt:

```
wmic process where "status='ok'" call shutdown
```

Process-Filter mit dem "Like"-Operator:

```
wmic process where "name like '%explore%'" call terminate
```

Datafile-Filter mit dem "Like"-Operator (nur damit lassen sich alle Unterverzeichnisse beim Alias "Datafile" anprechen):

```
wmic datafile where "drive='d:' and path like '%backup%'" call compress
```

Methode "SetPriority":

```
wmic process where "name='winword.exe'" call setpriority 64
```

Einsatz weiterer Klassen jenseits der vordefinierten Aliase:

```
wmic path Win32_ServerConnection get computername,numberoffiles,username
```

```
wmic path Win32_Currenttime get /value
```

```
wmic path Win32_CodecFile get name,filename,description
```

"Get/List"-Schalter "/Every:<n>" (Aktion erfolgt alle <n> Sekunden):

```
wmic cpu get loadpercentage /every:3
```

```
wmic os get FreePhysicalMemory /every:30
```

```
wmic /append:connect.htm path win32_sessionconnection get /Format:hform  
/every:30
```

Komplexer Aufruf:

- Append-Ausgabe (Anhängen an bestehende Datei)

- Where-Filter

- Auswahl zweier Eigenschaften mit "Get"

- Wiederholen mit /Every

- Formatwahl HTML

```
wmic /append:"c:\wmic.htm" process where "WorkingSetSize > 20000000" get  
name,workingsetsize /every:10 /format:htable
```

Logon-Aufzeichnung:

```
wmic netlogin get name,numberoflogons
```

Direkte Wmic-Auswertung auf Batch-Ebene oder Kommandozeile:

```
for /F "delims== tokens=1" %n in ('wmic os get serialnumber') do set sn=%n
```

Umwandlung des Wmic-Outputs in Ascii (mit Type, Sort oder Find):

```
wmic nicconfig get /value | type > nic.txt
```

Autostart-Check (umfasst Autostart-Ordner und Registry-Schlüssel "Run"):

```
wmic startup get /value
```

Eigenschaften der Netzwerkkarte auslesen

```
wmic nicconfig where index=1 get /value
```

```
wmic nic get index,name
```

/Node: führt Wmic-Befehle auf anderen PCs aus. Die Syntax ab dem Alias (oder der "Path" angegebenen Klasse) ist identisch mit der lokalen Anwendung von Wmic:

```
wmic /node:<Rechner oder IP-Adresse> /user:<Benutzername>
```

```
/password:<Kennwort> <Befehl>
```

Shutdown-Varianten: Neustart

```
wmic os where "status='ok'" call reboot
```

Shutdown-Varianten: PC abschalten

```
wmic os where "status='ok'" call shutdown
```

Shutdown-Varianten: User abmelden

```
wmic os where "status='ok'" call Win32Shutdown 0
```

Shutdown-Varianten: Herunterfahren

```
wmic os where "status='ok'" call Win32Shutdown 1
```

Shutdown-Varianten: Neustart

```
wmic os where "status='ok'" call Win32Shutdown 2
```

Shutdown-Varianten: Herunterfahren erzwingen

```
wmic os where "status='ok'" call Win32Shutdown 4
```

Shutdown-Varianten: PC abschalten

```
wmic os where "status='ok'" call Win32Shutdown 8
```