APPLIED INCIDENT RESPONSE

WMIC Quick Reference

Version 20191223

Common WMIC Switches

Switch example	Description
`/Node:"System1","System2"`	Specifies the host, or comma-separated list of hosts, against which the command will run (`System1,System2` in this example).
`/Node:@filename.txt`	Specifies a file containing a list of hosts against which the command should be run, listed one per line (`filename.txt` in this example). The `@` sign indicates that a file will be provided.
`/failfast:on`	Reduces the amount of time `wmic` will wait on a response from a host. Useful when running against large numbers of systems, some of which may not be up and responding.
`/User:username`	An optional switch to specify an alternative username to be used as the credential for running the command against remote systems (`username` in this example).
`/Password`	An optional switch to specify the password to be used for the alternative username provided with the `/User` switch. This switch should never be used since it may expose the plaintext password if command-line auditing is in use. Instead, when this switch is omitted, the user is prompted for the password when the `/User` switch is used. This is the more secure approach.
`/Output:filename.txt`	Redirect the output to a file (`filename.txt` in this example). Standard shell redirects like `>` will also work.
`/Append:filename.txt`	Redirect the output to a file (`filename.txt` in this example) but append rather than overwrite if data already exists. Standard shell redirects like `>>` will also work.

APPLIED INCIDENT RESPONSE

WMIC Quick Reference

Version 20191223

Common WMIC aliases

Alias	Description
BASEBOARD	Information about the system main board
BIOS	The Basic/Input Output System
COMPUTERSYSTEM	Computer name, domain name, logged-in user, and hardware details of the system
ENVIRONMENT	Information about system environment variables
GROUP	Information about groups
LOGICALDISK	Information on volumes, including filesystem and free space
NICCONFIG	Information about network card, IP address
OS	Information about the installed OS, including version
PAGEFILE	Information about the system's pagefile
PROCESS	Information about running processes
PRODUCT	Information about software products installed
QFE	Information about Windows updates applied (stands for Quick Fix Engineering)
SERVICE	Information about services
SHARE	Information about network shares
STARTUP	Limited information about user startup items
USERACCOUNT	Information about configured user accounts

Common WQL `where` clause operators

Operator	Description
`=`	Equal to
`<`	Less than
`>`	Greater than
`<=`	Less than or equal to
`>=`	Greater than or equal to
`!= or <>`	Not equal to
`IS`	Valid only to compare a value to NULL
`IS NOT`	Valid only to compare a value to NULL
`LIKE`	Allows for pattern matching of a string

WMIC examples

Provide a brief listing of the environment variables on the local system and stores the results, formatted as a list, to a text file on a remote share on server1:

```
wmic environment list brief /format:list >
\\server1\BaselineData\Client2\environment.txt
```

Query a remote system called server1 to get the name, process ID, parent process ID, thread count, handle count, and command line used to start each process. Output the results to a file called processes.txt on the local system:

```
wmic /node:server1 /output:processes.txt process get name, processid,
parentprocessid, threadcount, handlecount, commandline
```

Delete all processes named s**cv**host.exe on the local system:

```
wmic process where name="scvhost.exe" delete
```

Display the name and executable path of any process running on the local system where “Download” is included in the path to the associated executable:

```
wmic process where (ExecutablePath LIKE "%Download%") get name,
executablepath
```

Display the name executable path, and parent process ID of any process running on the local system where “Windows” is not included in the path to the associated executable:

```
wmic process where (NOT ExecutablePath LIKE "%Windows%") get name,
executablepath, ParentProcessID
```

Enable PowerShell Remoting on a remote system called server1:

```
wmic /node:server1 process call create "winrm quickconfig"
```

Display the IP address, MAC address, Default Gateway and DNS host name for the local system:

```
wmic nicconfig get MACAddress, DefaultIPGateway, IPAddress,
DNSHostName
```

Display the shares hosted on a remote system called server1:

```
wmic /node:server1 share list brief
```

Exclude the default administrative shares from the above-mentioned list:

```
wmic /node:server1 share where (NOT Name LIKE "%$") list brief
```

Output the name, caption, state, start mode, and path to executable for services running on the remote system server1 to a CSV file called services.csv:

```
wmic /node:Server1 /user:administrator@company.demo service get Name,
Caption, State, StartMode, pathname /format:csv > services.csv
```

Display details of quick fix engineering patches applied to a list of systems. The list is stored one system per line in the Systems.txt file:

```
wmic /node:@Systems.txt qfe get csname, description, FixComments,
HotFixID, InstalledBy, InstalledOn, ServicePackInEffect
```

Example of using a `for` loop to perform multiple queries a list of systems (in Systems.txt), outputting the results for each system into a text file named for that system and the date in YYYMMDD format:

```
for /F %i in (Systems.txt) do @echo scanning %i & wmic /node:%i
/failfast:on process get name, processid, parentprocessid,
threadcount, handlecount >> %i%date:~-4,4%%date:~-7,2%%date:~-
10,2%.txt & wmic /node:%i /failfast:on environment list brief >>
%i%date:~-4,4%%date:~-7,2%%date:~-10,2%.txt & wmic /node:%i
/failfast:on nicconfig get MACAddress, DefaultIPGateway, IPAddress,
IPSubnet, DNSHostName, DNSDomain >> %i%date:~-4,4%%date:~-7,2%%date:~-
10,2%.txt & wmic /node:%i /failfast:on service get Name, Caption,
State, ServiceType, StartMode, pathname >> %i%date:~-4,4%%date:~-
7,2%%date:~-10,2%.txt & wmic /node:%i /failfast:on qfe get
description, FixComments, HotFixID, InstalledBy, InstalledOn,
ServicePackInEffect >> %i%date:~-4,4%%date:~-7,2%%date:~-10,2%.txt
```