WMI and WMIC

Table of Contents

WMI & WMIC................................................................................................................................. 2
WMI -1 ............................................................................................................................................ 3
WMI -2 ............................................................................................................................................ 4
WMI -3 ............................................................................................................................................ 5
WMI Browsers -1 ............................................................................................................................ 6
WMI Browsers -2 ............................................................................................................................ 7
WMIC -1 .......................................................................................................................................... 8
WMIC -2 .......................................................................................................................................... 9
WMIC Aliases -1 ............................................................................................................................ 10
WMIC Aliases -2 ............................................................................................................................ 11
WMIC Examples -1 ........................................................................................................................ 12
WMIC Examples -2 ........................................................................................................................ 13
WMIC Examples -3 ........................................................................................................................ 14
Notices .......................................................................................................................................... 15
WMI & WMIC

WMI (Windows Management Instrumentation) provides a management and information sharing infrastructure for Windows machine.

- Can be accessed directly through Powershell, VBScript and programming languages like C/C++ and Visual Basic

WMIC (WMI Command) extends WMI through a command-line interface and BATCH files.

Available on Windows 2000 and later

**043 Okay, WMI and WMIC, the Windows Management Instrumentation and Instrumentation Command. They give you lots of functionality. Very powerful management and information-sharing infrastructure for the Windows operating system. It can be directly accessed using PowerShell, VBScript, programming languages like C++ and Visual Basic. And the WMIC extends that WMI so you can access all that stuff through the command line interface, and of course that makes it possible for you to use that in your batch scripts. This has been available since Windows 2000 and the modern Windows as well.
Sampling of what it can provide

- Start/Stop/View processes on a remote computer
- Reboot a computer remotely
- Query Users and Groups on the local or remote computer
- Query the resources on the local or remote computer
  - Hard drives/file systems
  - OS settings
  - Services
  - Shares
  - Registry settings
  - Event logs

**044 Not unlike the net commands, this has the ability to start, stop and look at processes. This happens to be able to do it on remote computers as well. You can reboot computers remotely. You can look into the user and user groups, either locally or remotely, and you can be looking at the resources such as hard drives, the OS settings. Registry settings are pretty important and pretty powerful as well. Even event logs, like the security event logs, can be accessed through the WMI console.**
Think of WMI as a SQL server, but with live information of the Windows machine.

Query them with SQL like statements.

The root contains namespaces that contain classes.

The default namespace is root\cimv2.
- Contains Win32 Classes – Hardware and OS info

Applications can create additional namespaces to provide information through the WMI service.

**045 So think of WMI as sort of a database holding information, not unlike a SQL server but with live information, current information, about that particular Windows machine, and you can query them with SQL-like statements. So the root of this database, if you will, contains namespaces and they hold certain classes. The default namespace, probably the most important is the root\cimv2. It contains the Win32 classes, which have a lot of information about the hardware and operating system information.
Applications can create additional namespaces within this, and then you can also access that through WMI Console or through the command.

Each Class contains Instances, which have Properties and Methods.

Win32_UserAccount as an example
  • Instances are the individual user accounts on the system.
  • Each user account has Properties and Methods that can be performed on it.
    – Properties: Name, Domain, Description, SID, and more
    – Methods: Rename – the only action that can be performed on this particular Instance

Use a WMI Browser to view them all.
  • Microsoft’s WMI Administrative tools

**046 So each class contains instances and each instance has properties and methods, similar to some programming languages--object-oriented programming languages that use that construct where they have objects and each object has a property and a method, but in this case they call them instances.

So Win32 user account, for example. The instances of the individual user
accounts on the system, and each of the accounts has properties and methods that you can access that with so that the properties here-- name, domain, description, etcetera-- and in this case there’s only one method-- it’s a rename-- that can be used on this particular instance.

There are WMI browsers, and there’s Microsoft’s WMI Administrative Tools.

**WMI Browsers -1**

**Use a WMI Browser software to view them all**

Microsoft’s WMI Administrative tools (CIM Studio)


**047** There, and that’s kind of what it looks like, and this lets you access lots and lots of information. So if you’re an administrator, this would be a very, very powerful tool
for you to use, and the GUI is obviously a bonus. It makes it a little easier to see exactly what you're dealing with.

**048 Here's another browser, WMI Explored by Advanced Network Software. So there's a few different browsers out there that you can take advantage of depending on what you like and what your need might be in accessing this data.**
Uses *aliases* to act as a friendly interface to the names space

- *Aliases* provide simple commands to replace complicated namespaces and queries.
- No knowledge of programming languages required
- Can also bypass aliases and access namespace directly
- Stored in root\cli namespace under the class MSFT_CliAlias
- Output results to text, XML, HTML, CSV (Comma Separated)

**049 So WMIC uses aliases to kind of act as an interface to the namespaces. It’s not quite as-- I don’t want to say complicated, but complex as dealing with like the cimv2 and that sort of thing. They provide some simple commands to replace the complicated stuff, and then there’s no real need of knowing anything to do with programming languages in order to access the aliases. You can also bypass the aliases and access namespaces directly. And then you can make the output anything from text, XML, and then of course comma-separated or HTML. And these aliases are stored
in the root/cli, command line interface, namespace under the Microsoft_CLI alias class.

**WMIC -2**

**WMIC -2**

Can be used as an interactive shell by typing `wmic` without any options.

For Batch files and single use, run it with options.

- `wmic [options] command`

Use with `/?` to show all possible options and aliases.

- Easiest way to see all aliases available – very helpful!
- **Alias /?** For usage help on the alias specified

```
C:\Data\nic useraccount /?
USERACCOUNT - User account management.
MINT: HELP for Alias usage.
   (<List> (WMIObject) | <List> (path where) | <List> <path where> | [germ of
   <List>].
   USAGE:
   USERACCOUNT ASSOC [{format specifier}]
   USERACCOUNT CALL [{method name} [{actual param list}]]
   USERACCOUNT CREATE [{assign list}]
   USERACCOUNT DELETE
   USERACCOUNT GSET [{property list} [{set switches}]
   USERACCOUNT GGET [{assign list}]
   USERACCOUNT GSET [{assign list}]

**050 WMIC can be used as an interactive shell just by typing "WMIC" on the command line. For batch files and single use, you can run it with options, and then option is optional, and then a command with it. Uses slash question mark just like the others to bring up the options that are available. In this case, WMIC user account slash question mark gives you the alias usage and the format for the instance and then the properties and the things you can use.**```
So if you'd like help on aliases in particular, you can do alias slash question mark.

**WMIC Aliases -1**

**WMIC Aliases -1**

Most useful aliases
- COMPUTERSYSTEM – Computer system management
- DISKDRIVE – Physical disk drive management
- GROUP – Group account management
- LOGON – LOGON sessions
- NICCONFIG – Network adapter management
- NTDOMAIN – NT Domain management
- NTEVENT – Entries in the NT Event Log
- PARTITION – Management of disk partitions

**051 And here's a list of some of the most useful aliases. If you need to access computer system management, you can use Computer System. Group Account Management, just the word Group. So they simplified it a little bit. NIC config, Network Interface Card config, will let you know the network adapter information. And domain management, you'd use NT Domain, and if you have to deal with disk partitions, you just use the alias Partition.**
WMIC Aliases -2

More useful aliases
- PRINTER – Printer device management
- PRINTJOB – Print job management
- PROCESS – Process Management
- QFE – Quick Fix Engineering (Hot Fixes & Service Packs)
- REGISTRY – Computer system registry management
- SERVICE – Service application management
- SHARE – Shared resource management
- STARTUP – Management of commands that run at logon
- VOLUME – Local storage volume management

Remember to use `wmic alias /?` for details.

**052 And here's a few more useful ones. Print jobs. If you're going to deal with processes, you can use Process as an alias. Pretty powerful. If you know anything about Windows you know that registry is a very, very important part of Windows, so you can access the registry with the Registry alias, and services in the share, and then, again, if you do the WMIC alias slash question mark, for more of the details.
wmic useraccount list
  • Provide a list of the accounts on the local machine, add brief or full to customize details
wmic /output:users.html useraccount list /format:hform
  • Output the list of users in HTML table format, replace hform with csv or htable for other formats
wmic /node:"machinename" useraccount list
  • List of accounts on a remote computer

**053 So WMIC kind of uses a construct of item and then a verb. So in this case, user account list, and it provides you a list of the accounts on the local machine. This one you can actually take the brief version or the less detailed version, or you can do the full version. And if you use the slash format, in this case hform, you can output lists using HTML table format, if you use the htable, and you can also do CSV, so you can adjust the format output as you need to in case you want to use it as an input to another command, or for other information.
So wmic /node: "machinename" useraccount-- this will give you the list of accounts on a remote computer. So again, very powerful for administration. So you see a lot of the comparisons to like the net commands, and even net shell.

**WMIC Examples -2**

wmic /node:"machinename" nicconfig
  • Provide a list of the adapters on the local machine
wmic /node:"machinename" computersystem get username
  • Determine user currently logged in remotely

**054 So on this one it'll give you the list of adapters on a local machine. You used a /node and put your host name in the machine name area, and you can determine currently logged-on individuals by using the /node machine name and then the computer system get username.**
WMIC Examples -3

wmic process where name="cmd.exe" delete
  • Kills a process
wmic /node:"machinename" nicconfig where Index=1
call EnableStatic ("192.168.20.20"),
("255.255.255.0")
  • Remotely change the IP to a static IP, Index is the Interface #, can be retrieved with
wmic /node:"machinename" nicconfig where
IPEnabled='true'
  • Display IPEnabled interfaces

**055 So this is the part where you can kind of see the power, because obviously if you can delete a running process within a system, that's a pretty powerful thing. So in this case, the WMIC process where-- and that's where you kind of see the similarity in like SQL or S-Q-L, if you've ever used SQL-- process where name equals cmd.exe, and you delete that, so you can shut that process down.

And then on the next line it uses the nicconfig where index equals one call EnableStatic, so you're changing an IP to a static IP and you're actually assigning it right here in this-- in one
line on the command line. And you can enable an interface also using the nicconfig portion of WMIC.

Notices

© 2015 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.