Module 6

WMI

Overview

Remoting

*.cdxml

Events

1

Overview

Windows Management Instrumentation is a core Windows management technology.

- **WMI Components**
  - WMI Classes
  - WMI Methods
  - WMI Instances

```
Get-WmiObject -List
Get-WmiObject Win32_Service

Get-WmiObject -Query '*WQL*'

Invoke-WmiObject
```

- **Cmdlets**
  - *-Wmi*
    - Since PowerShell 1.0
  - *-CIM*
    - Since PowerShell 3.0

```
Get-CimClass
Get-CimClass -Class -Namespace

Get-CimInstance -Class|-Query

Invoke-CimMethod -InputObject
```


2

Remoting

How to work with different scopes for variables in scripts with functions

- ***-WMI* and -Computername**
  - DCOM is used
  - Allow on Firewall DCOM
  - Compatible to Windows 7 and PowerShell 2.0
- **CIMSessions**
  - WSMan is used; DCOM optional
  - Allow on Firewall HTTP/HTTPS
  - Sessions can be reused

DIST IT SERVICES & TRAINING

3

WQL

- **WMI Query Language (WQL)**
  - about_WQL

```
Select Properties From ClassName Where Property Operator Value

Select * From Win32_Service
Select Name,ProcessID,HandleCount From Win32_Process
Select * From Win32_LogicalDisk Where DeviceID="C:"
```


DIST IT SERVICES & TRAINING

4

Lab

- **How many physical memory has your machine?**

```
(Get-CimInstance Win32_ComputerSystem).TotalPhysicalMemory
```

- **When was the machine turned on?**

```
(Get-CimInstance Win32_OperatingSystem).LastBootUpTime
```

- **List all running services with Name, State and StartMode.**

```
Get-CimInstance Win32_Service | Where-Object { $_.State -eq "Running" } |
   Format-Table Name, State, StartMode
```

- **How much free space on drive c:?**

```
$Drive = Get-CimInstance Win32_LogicalDisk | Where-Object { $_.DeviceID -eq "c:" }
$Drive.Freespace / 1MB
```


DIST IT SERVICES & TRAINING

5

Object over WMI

- **Module for WMI Class**
  - Also properties and methods
- ***.cdxml**
  - Loaded as module
  - Module type CIM
  - Brings one or more functions with parameters
- **Purpose**
  - Quick access WMI *instances* without using *-wmi* or *-cim*
  - even though filtering is possible
  - Quick access WMI *methods* without using *-wmi* or *-cim*

DIST IT SERVICES & TRAINING

6

Events

Which kinds of events are there?

- **WMI events are notifications of changes in WMI Data Model**
- **Requirements**
  - Filter
    - What should be monitored?
  - Consumer
    - What should be executed in case of event?
  - Binding
    - Between filter and consumer

DIST IT SERVICES & TRAINING

7

WMI Events Filter

What is a WMI event filter?

- **A filter is a definition of what should be monitored**
- **Filters use event classes**
  - Intrinsic event classes
  - Extrinsic event classes
- **Intrinsic Events**
  - “An event that WMI provides, which is a notification of a change in the standard WMI data model. For example, the creation of a new instance of Win32_Process is an __InstanceCreationEvent type of intrinsic event.” [1]
- **Extrinsic Events**
  - An event notification from a provider by using a specific class. “For example, the Event Log Provider defines the event class Win32_NTLogEvent.” [2]

[1] https://msdn.microsoft.com/en-us/library/aa390809(v=vs.85).aspx#wmi.gloss_intrinsic_event
[2] https://msdn.microsoft.com/en-us/library/aa390797(v=vs.85).aspx#wmi.gloss_extrinsic_event

DIST IT SERVICES & TRAINING

8

What is a Consumer

What are event consumers?

- **Consumer**
  - A consumer is executed when an event occurred.
- **Temporary Consumer**
  - "… is a WMI client application that receives a WMI event." [1]
  - For example: Register-WMIEvent –Query … –Sourceidentifier … –Action … Action is a scriptblock and the consumer.
- **Permanent Consumer**
  - "A permanent consumer is a COM object that can receive a WMI event at all times. A permanent event consumer uses a set of persistent objects and filters to capture a WMI event." [1]
  - Examples: CommandLineEventConsumer, LogFileEventConsumer, SMTPEventConsumer, NTEventLogEventConsumer

 [1] https://msdn.microsoft.com/en-us/library/aa393013(v=vs.85).aspx

DIST IT SERVICES & TRAINING

9

What is Binding?

- **Binding is the link between a filter and a consumer**
- **Binding is done automatically with temporary consumer**
  - PowerShell
- **Binding is done manually with permanent consumer**

DIST IT SERVICES & TRAINING

10

Intrinsic Event Classes

How work with intrinsic event classes

- **Extrinsic event classes**
  - Get-CimClass –ClassName Win32_*Event
  - Get-CimClass –ClassName Win32_*Trace

```
Select * From Win32_DeviceChangeEvent
```

- **Intrinsic event classes**
  - __InstanceCreationEvent
  - __InstanceModificationEvent
  - __InstanceDeletionEvent

```
Select * From __InstanceCreationEvent Within 5 Where TargetInstance ISA Win32_Printer
Select * From __InstanceDeletionEvent Within 5 `
   Where targetinstance ISA Win32_Printer and TargetInstance.Name = "Xerox ABC"
```


Demo Temporary Consumer

How to register a WMI event

```
$FilterQuery = 'Select * From __InstanceModificationEvent WithIn 5
                Where TargetInstance ISA "Win32_Service" and TargetInstance.Name="bits" '

Register-WMIEvent -Query $FilterQuery -SourceIdentifier myEvents

Wait-Event …
Get-Event …
```

Do You Have Any Questions?