

Managing the Registry With Windows PowerShell

Jeffery Hicks
SAPIEN Technologies, Inc.

Pre-requisites for this presentation:

1) Basic PowerShell

Level: Intermediate

Agenda

- Registry PSDrive Provider
- Remote Registry with WMI
- Remote Registry with .NET
- Demos and Samples will be available later at blog.sapien.com
- *You may want to load slides from the conference CD for review*



- Some time set aside for some hands on work
 - not full blown labs
- Work together
- Open up your copy of the slide deck
- Use books, online resources, cmdlet help, Magic 8 Ball, Ouiji boards or telepathy

Danger Disclaimer

- This is the registry we're mucking around with so all the usual disclaimers, warnings, caveats and precautions apply.
- "You break it, you bought it"

Registry PSDrive

- Included by default with PowerShell (HKLM and HKCU)
- Navigate local registry as if it were a drive
- Use filesystem commands (with some limitations)
- Use Get-ItemProperty to retrieve values

```
PS C:\> get-itemproperty -path  
HKLM:\SOFTWARE\Microsoft\PowerShell\1  
\PowerShellEngine
```

- Navigating the registry

- List all services under
HKLM\System\CurrentControlSet
- Bonus: List name only
- List all items configured to run under
HKLM\software\microsoft\windows\currentver
sion\run

Creating Keys and Values

- Use mkdir (or New-Item) to create a new registry entry
- Use New-ItemProperty to create a registry value
 - Use -PropertyType to specify String, ExpandString, Binary, DWord, MultiString, QWord
- Use Set-ItemProperty to modify value

Removing Keys and Values

- Use DEL (remove-item)
- Use Remove-ItemProperty

- Making stuff up....



- Create an entry under HKCU using your account name (bonus if you can avoid hard coding)
- Create an entry for your computername and populate it with the actual computername
- Create an entry called data and give it a value
- Modify data with a new value
- Delete everything

WMI and the Registry

- Does NOT use Get-WMIObject
- Use the StdRegProv (provider) to connect to remote systems
- Alternate Credentials more complicated
- Not very quick

- \$HKLM=2147483650
- \$HKCU=2147483649
- \$HKCR=2147483648
- \$HKEY_USERS=2147483651

[WMIClass]\$Reg =

"\\computername\root\default:StdRegProv"

Enumerate Keys

```
$software=$reg.EnumKey($HKLM,"Software")  
$software | foreach {$_.snames}
```


Enumerate Values

```
$regpath="SOFTWARE\Microsoft\Windows\Current  
Version\Run"
```

```
$values=$reg.EnumValues($HKLM,$RegPath)
```

```
$values | foreach {$_.sNames}
```

What About Data?

- You need to call the appropriate method to read the data for a given registry value
 - GetBinaryValue()
 - GetDWORDValue()
 - GetExpandedStringValue()
 - GetMultiStringValue()
 - GetQWORDValue()
 - GetStringValue()

```
$regpath="SOFTWARE\Microsoft\Windows\  
CurrentVersion\Run"
```

```
$value="Windows Defender"
```

```
$reg.GetStringValue($HKLM,$regpath,$value).sValue
```

Discover Data Type

```
for ($i=0;$i -lt $values.snames.count;$i++) {  
    $values.snames[$i]+"="+$values.Types[$i]  
}
```

Windows Defender=2

IgfxTray=1

HotKeysCmds=1

Persistence=1

SigmatelSysTrayApp=1

- 1 = String
- 2 = ExpandedString
- 3 = Binary
- 4 = Dword
- 7 = MultiString

Create a Key

#create a single key

```
$reg.CreateKey($HKCU, "MyStuff")
```

#create a hierarchy

```
$reg.CreateKey($HKCU, "MyStuff\Key1\Key2")
```


Writing Values

- SetValue()
- SetBinaryValue()
- SetDWORDValue()
- SetExpandedStringValue()
- SetMultiStringValue()
- SetQWORDValue()
- SetSecurityDescriptor()
- SetStringValue()

Example

```
#create a string value
```

```
$reg.SetStringValue($HKCU,"MyStuff\Key1",  
    "SampleKey","I am a string")
```

```
#create a dword
```

```
$reg.SetDWORDValue($HKCU,"MyStuff\Key1",  
    "Sample Dword",1024)
```

#delete a value

```
$reg.DeleteValue($HKCU, "MyStuff\Key1",  
    "SampleKey")
```

#delete a key

```
$reg.Deletekey($HKCU, "MyStuff\Key1\Key2")
```

- You can't delete keys with subkeys

- Get-PowerShellInstall.ps1

- Get the registered owner and organization from HKLM\software\microsoft\windows nt\currentversion
- Change the value of registered owner

.NET and the Registry

- [Microsoft.Win32.RegistryKey]
- [Microsoft.Win32.RegistryHive]
- No good support for alternate credentials

Registry Hive Enums

- LocalMachine
- CurrentUser
- Users
- CurrentConfig

Connect to base key

```
$computer="chaos"
```

```
$regbase=[Microsoft.Win32.RegistryKey]::Open  
RemoteBaseKey("localmachine",$computer)
```

Open a Subkey

```
$key="software\microsoft\windows  
nt\currentversion"
```

```
$cv=$regbase.OpenSubKey($key,$True)
```

```
$cv.getSubkeynames()
```

```
$cv.GetValueNames()
```

```
$cv.GetValue("currentversion")
```

#create a registry sub key

```
$cv.CreateSubKey("foobar")
```

#or create a value

```
$cv.SetValue("conference", "Techmentor")
```

#or of a specific type

```
$cv.setvalue("home", "%userprofile%",  
"ExpandString")
```

- String, ExpandString, Binary, DWord, MultiString, QWord

#delete a value

```
$cv.DeleteValue("conference")
```

#delete a empty key

```
$cv.deletesubkey("foobar")
```

#delete a subtree

```
$cv.DeleteSubKeyTree("foobar")
```


- Demo-dotNetRegistry.ps1

- Create a key called Techmentor under HKCU
- Add values for your name, your birthday, and your age as a DWORD.
- Enumerate your new key
- Delete everything

Resources

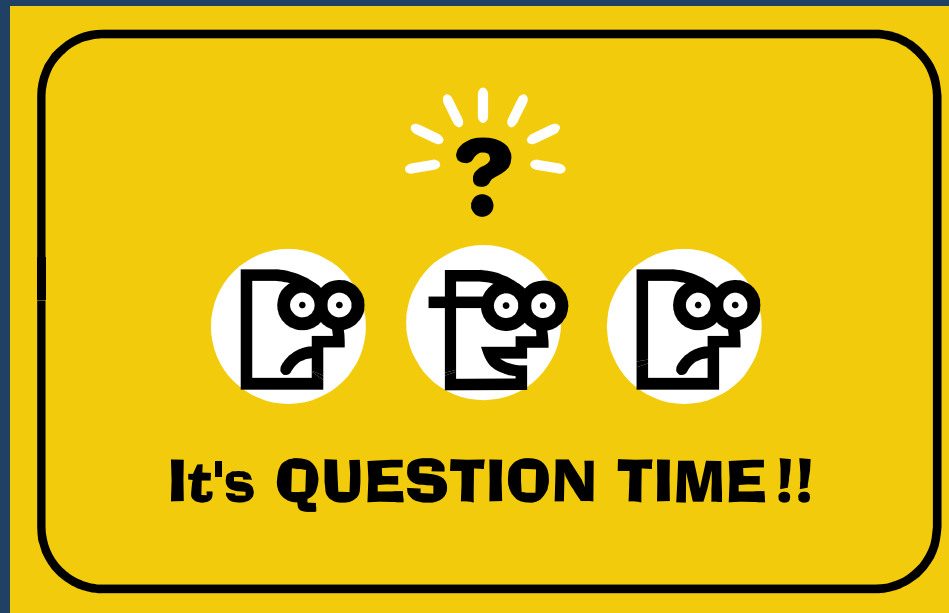
- blog.SAPIEN.com
- www.ScriptingAnswers.com
- www.PowerShellCommunity.org



Resources

- Windows PowerShell v1.0: TFM 2nd edition
- Windows PowerShell Cookbook (Lee Holmes)
- Windows PowerShell in Action (Bruce Payette)
- MSDN

Questions



Thank you

- jhicks@sapien.com
- Follow me at twitter.com/jeffhicks

