Microsoft®

tech·ed

North America | 2011

MAY 16-19, 2011

ATLANTA

Microsoft tech·ed North America 2011

MAY 16-19, 2011 | ATLANTA

Managing the Registry with Windows PowerShell 2.0

Jeffery Hicks
Principal Consultant
JDH Information Technology Solutions

Agenda

- PowerShell Registry Provider
- Using the .NET Framework
- Using Windows Management Instrumentation

Demos and scripts will be available from
http://jdhitsolutions.com/blog

Introducing the Registry Provider

- Provides an abstraction layer for cmdlets
- Only works locally
- Defaults to HKLM and HCKU but we can add more

```
PS C:\> get-psprovider registry

Name     Capabilities                    Drives
----     ------------                    ------
Registry ShouldProcess, Transactions {HKLM, HKCU}
```

Navigating the Registry PSDrive

- Change to the “drive”

```
PS C:\> cd hklm:
```

- Use file system commands like CD and DIR.

```
PS HKLM:\> dir
```

- You can use New-PSDrive to create a new “drive”

```
New-PSDrive –name CurrentControl –PSProvider
Registry –Root HKLM:System\CurrentControlSet
```

Navigating the Registry PSDrive

demo

Modifying the Registry

- Use the Item cmdlets to get and set keys

```
get-item "hklm:software\microsoft\windows
nt\currentversion“
```

- Use the ItemProperty cmdlets to get and set values

```
get-itemproperty "hklm:software\microsoft\windows
nt\currentversion"
```

Modifying the Registry

- Use New-Item to create a new registry key
- Use New-itemProperty to create a new registry value
  - String
  - ExpandString
  - Binary
  - Dword
  - MultiString
  - QWord
- Use Set-ItemProperty to modify (or create) a registry value

Modifying the Registry

- Clear-Item deletes all values and leaves it empty
- Remove-Item deletes everything
- Clear-ItemProperty clears a registry value and leaves it empty
- Remove-ItemProperty deletes it

Modifying the Registry PSDrive

demo

Using Transactions

- Transactions allow for an “all or none” approach
- Use the Start-Transaction cmdlet to begin
- The –UseTransaction parameter adds the command to the transaction
- If no errors use Complete-Transaction
- Use Undo-Transaction to roll changes back

Transactions and the Registry PSDrive

demo

Security

- Use the ACL cmdlets
  - Get-ACL
  - Set-ACL
- Modifying is not a trivial task
- Nothing wrong with using a CLI tool like subinacl.exe

Registry Security and Permissions

Remote Management

- Anything you can do locally you can do remotely using a remote command
- Requires PowerShell 2.0 at both ends
- Requires PowerShell remoting to be enabled

```
PS C:\> invoke-command {get-itemproperty -path
"hklm:software\microsoft\windows
nt\currentversion" | Select Product*,CSDVersion}
-computername serenity,quark
```

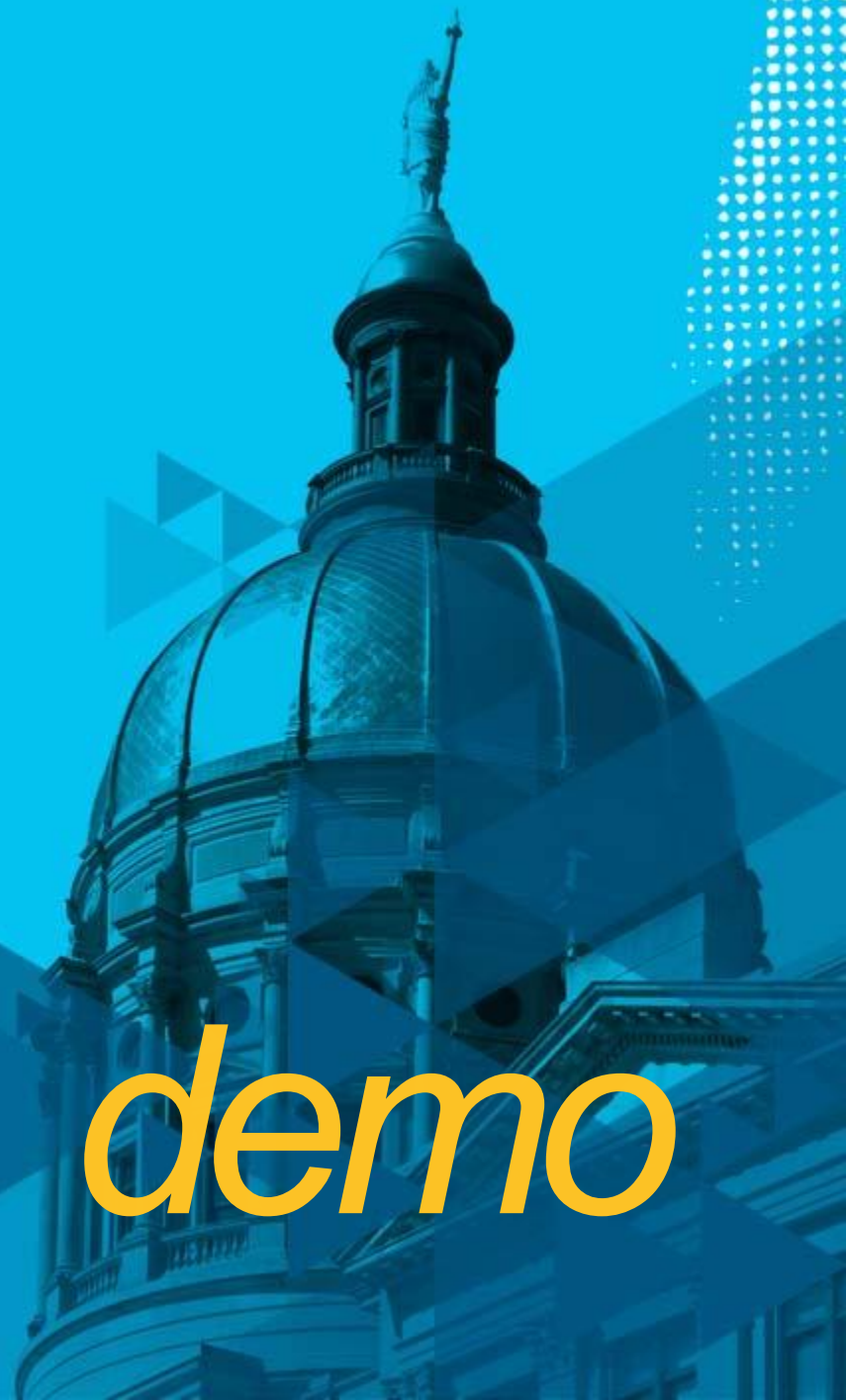
Using the .NET Framework

- An alternative for remote management if PowerShell remoting is not available
- Use the [Microsoft.Win32.RegistryKey] class
- Supports remote connections with current credentials

Managing the Registry with .NET

- OpenRemoteBaseKey(hive,computer)
  - LocalMachine
  - Users
  - ClassesRoot
  - CurrentUser
- Use CreateSubKey() and DeleteSubKey() to create/delete keys
- Use OpenSubKey and GetSubKeyNames to enumerate
- Use GetValue() and SetValue to modify values

Using the .NET Framework Registry classes



demo

Using WMI

- When all else fails use the WMI StdRegProv provider
- Expect poor performance
- Remote management requires firewall considerations
- Conceptually similar to .NET

WMI Steps

- $Reg = [WMIClass]"\\QUARK\root\default:StdRegProv"
- Access a hive by constant value
  - $HKLM=2147483650
  - $HKCU=2147483649
  - $HKCR=2147483648
  - $HKEY_USERS=2147483651
- Use different methods to return different values based on type, ie GetStringValue()

Using the WMI StdRegProvider

Recommendations

- Use cmdlets wherever possible
- Use the PSProvider and PowerShell remoting
- Use Transactions when modifying the registry
- Test thoroughly in a non-production environment

My Resources

- Windows PowerShell 2.0: TFM by Don Jones & Jeffery Hicks
- Windows PowerShell in Action by Bruce Payette
- Windows PowerShell Cookbook by Lee Holmes
- Remote Registry PowerShell Module
  - http://archive.msdn.microsoft.com/PSRemoteRegistry
- http://jdhitsolutions.com/blog

Questions & Answers

Resources

mytech·ed
Learn. Connect. Share.

Connect. Share. Discuss.

http://northamerica.msteched.com

Microsoft® tech·ed Online

Sessions On-Demand & Community

www.microsoft.com/teched

Microsoft® | Learning

Microsoft Certification & Training Resources

www.microsoft.com/learning

Microsoft® TechNet

Resources for IT Professionals

http://microsoft.com/technet

msdn®

Resources for Developers

http://microsoft.com/msdn

Microsoft®