CNT 4603: System Administration
Spring 2012

Scripting – Windows PowerShell – Part 1

Instructor: Dr. Mark Llewellyn
markl@cs.ucf.edu
HEC 236, 4078-823-2790

Department of Electrical Engineering and Computer Science
Computer Science Division
University of Central Florida
A **shell** is software that provides a customized interface designed for executing commands or scripts. (The term originated from OS nomenclature where the outer layer of a layered architecture OS was the interface between the user and the kernel of the OS.)

Most OS shells generally fall into one of two categories: command-line and graphical. Command-line shells provide a command-line interface (CLI) to the OS, while graphical shells provide a graphical user interface (GUI).

In either category the primary purpose of the shell is to invoke or “launch” other programs. In most modern environments, shells frequently have additional capabilities such as viewing the contents of directories.
Scripting – Windows PowerShell

• Windows PowerShell is a command-line interface (CLI).

• Two important features of PowerShell are scripts and cmdlets.

• A **script** is a file of commands that is run when you execute or invoke the script.

• A **cmdlet** (short for command-let, its pronounced like the long version) is a specialized (lightweight – they are technically instances of .NET Framework classes and are not stand-alone executables) command for completing common tasks in the PowerShell environment.

• There are about 130 built-in cmdlets already defined in PowerShell and you can also define (create) your own custom cmdlets as well as import third-party cmdlets.
Scripting – Windows PowerShell

• Windows PowerShell is particularly well suited for situations in which there are multiple servers and it is more efficient to manage them using a consistent set of scripts.

• It is also ideal for managing servers with the Application Server role installed in situations where the applications need to be configured the same way and regular updates are applied.

• Windows Server 2008 comes with PowerShell and it can be installed via the Server Manager (it also comes with Windows 7) and it can be easily downloaded into older server versions.
Some of the more common server administration tasks that can easily be handled through PowerShell include:

- Managing files and folders (directories).
- Managing network tasks.
- Managing fixed and removable storage devices.
- Configuring printing services.
- Managing software applications and updates.
- Managing Terminal Services.
- Managing server services and features.
- Managing Web server services
- Working with the system registry.
Scripting – Windows PowerShell

• PowerShell is not installed by default in Server 2008 (although it should be in Server 2008 R2 editions).

• To install PowerShell from the Server Manager:
  – Scroll down to the Features Summary.
  – Click Add Features.
  – Under Features, scroll to find Windows PowerShell and check its box.
  – Click Next and then click Install.
  – Click Close.
  – Close the Server Manager.

• The next few screen shots step you through this simple process.
Click Here
1. Check the Windows PowerShell checkbox.
2. Then click Next.
To install the following roles, role services, or features, click Install.

1 informational message below

- This server might need to be restarted after the installation completes.

Windows PowerShell

Click Install
Click Close after successful installation
Back in Server Manager, the new feature lists under the installed features on this server.
Once you’ve installed PowerShell on the server, you’re reading to take advantage of some of the cmdlets.

With PowerShell installed, you should be able to find it on the server under the Start menu, click All Programs, click Accessories, Click Windows PowerShell, and Windows PowerShell should be there (see the next page).

Note: there will also be a Windows PowerShell ISE, which is the Integrated Scripting Environment. We’ll look at this later.

Once you click on Windows PowerShell, you should see a screen like the one shown on page 14.
You’ll find PowerShell under the Accessories list from the Start, All Programs listing.
This is the default appearance with the window maximized. To change this setting see pages 43-44.
PS C:\users\Administrator> _
To view the files in the current folder (the default folder will be the Users/Administrator folder), one page of files at a time, enter the command:

```
dir | more
```

Press Enter after typing in the command (pressing the spacebar will give you the next page if there is one – probably not on our servers, since we don’t have much out there yet).

What you’re doing here is executing the directory command and piping its output through to the more command which displays input one page at a time.

The next page shows the execution of this command on one of my virtual servers.
PS C:\users\Administrator> dir | more

Directory: C:\users\Administrator

Mode LastWriteTime Length Name
------ ------------- ------ --------
    dr-- 10/3/2011 10:13 AM    5        .grasp_settings
    dr-- 11/16/2011 4:41 PM    0        .idlerc
    dr-- 3/15/2012 11:28 AM    0        .m2
    dr-- 9/21/2011 5:02 PM    0        Contacts
    dr-- 2/22/2012 2:15 PM    0        Desktop
    dr-- 3/1/2012 8:21 AM    0        Documents
    dr-- 2/22/2012 2:16 PM    0        Downloads
    dr-- 9/21/2011 5:02 PM    0        Favorites
    dr-- 9/21/2011 5:02 PM    0        Links
    dr-- 9/21/2011 5:02 PM    0        Music
    dr-- 11/16/2011 12:15 PM    0        MyScripts
    dr-- 9/21/2011 5:02 PM    0        Pictures
    dr-- 11/16/2011 4:30 PM    0        Python Scripts
    dr-- 9/21/2011 5:02 PM    0        Saved Games
    dr-- 9/21/2011 5:02 PM    0        Searches
    dr-- 9/21/2011 5:02 PM    0        Videos
    dr-- 9/21/2011 5:02 PM    0        workspace

PS C:\users\Administrator> _
Scripting – Windows PowerShell

• To get a listing of the services currently running on your server, enter the command `get-service`, at the command prompt. A partial listing of the output of this cmdlet is shown on page 19.

• To view a listing of all the currently defined cmdlets, enter the command `get-command | more`, at the command prompt. Here you will see the cmdlets one screen at a time, so press the spacebar to advance to the next screen. Simply repeat this until you’ve seen all the pages, or alternatively, press `q`, to quite and exit back to the command line if you don’t want to view all the pages. This command is illustrated on page 20.
<table>
<thead>
<tr>
<th>Status</th>
<th>Name</th>
<th>DisplayName</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running</td>
<td>AeLookupSvc</td>
<td>Application Experience</td>
</tr>
<tr>
<td>Stopped</td>
<td>ALG</td>
<td>Application Layer Gateway Service</td>
</tr>
<tr>
<td>Stopped</td>
<td>Apache2.2</td>
<td>Apache2.2</td>
</tr>
<tr>
<td>Stopped</td>
<td>AppInfo</td>
<td>Application Information</td>
</tr>
<tr>
<td>Stopped</td>
<td>AppMgmt</td>
<td>Application Management</td>
</tr>
<tr>
<td>Stopped</td>
<td>AudioEndpointBuilder</td>
<td>Windows Audio Endpoint Builder</td>
</tr>
<tr>
<td>Stopped</td>
<td>AudioSrv</td>
<td>Windows Audio</td>
</tr>
<tr>
<td>Running</td>
<td>BFE</td>
<td>Base Filtering Engine</td>
</tr>
<tr>
<td>Running</td>
<td>BITS</td>
<td>Background Intelligent Transfer Server</td>
</tr>
<tr>
<td>Stopped</td>
<td>Browser</td>
<td>Computer Browser</td>
</tr>
<tr>
<td>Stopped</td>
<td>CertPropSvc</td>
<td>Certificate Propagation</td>
</tr>
<tr>
<td>Stopped</td>
<td>clr_optimization2</td>
<td>Microsoft .NET Framework NGEN v2.0</td>
</tr>
<tr>
<td>Stopped</td>
<td>clr_optimization3</td>
<td>Microsoft .NET Framework NGEN v4.0</td>
</tr>
<tr>
<td>Running</td>
<td>COMSysApp</td>
<td>COM+ System Application</td>
</tr>
<tr>
<td>Running</td>
<td>CryptSvc</td>
<td>Cryptographic Services</td>
</tr>
<tr>
<td>Stopped</td>
<td>CscService</td>
<td>Offline Files</td>
</tr>
<tr>
<td>Running</td>
<td>DcomLaunch</td>
<td>DCOM Server Process Launcher</td>
</tr>
<tr>
<td>Running</td>
<td>Dhcp</td>
<td>DHCP Client</td>
</tr>
<tr>
<td>Running</td>
<td>DnsCache</td>
<td>DNS Client</td>
</tr>
<tr>
<td>Stopped</td>
<td>dot3svc</td>
<td>Wired AutoConfig</td>
</tr>
<tr>
<td>Running</td>
<td>Dps</td>
<td>Diagnostic Policy Service</td>
</tr>
<tr>
<td>Stopped</td>
<td>EapHost</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>Running</td>
<td>EventLog</td>
<td>Windows Event Log</td>
</tr>
<tr>
<td>Running</td>
<td>EventSystem</td>
<td>COM+ Event System</td>
</tr>
<tr>
<td>Stopped</td>
<td>FCRegSvc</td>
<td>Microsoft Fibre Channel Platform Re...</td>
</tr>
<tr>
<td>Stopped</td>
<td>fdHost</td>
<td>Function Discovery Provider Host</td>
</tr>
<tr>
<td>Running</td>
<td>FDResPub</td>
<td>Function Discovery Resource Publicati...</td>
</tr>
<tr>
<td>Running</td>
<td>FontCache</td>
<td>Windows Font Cache Service</td>
</tr>
<tr>
<td>Stopped</td>
<td>FontCache3.0.0.0</td>
<td>Windows Presentation Foundation Font...</td>
</tr>
<tr>
<td>Running</td>
<td>gpSvc</td>
<td>Group Policy Client</td>
</tr>
<tr>
<td>Stopped</td>
<td>hidsvc</td>
<td>Human Interface Device Access</td>
</tr>
<tr>
<td>Stopped</td>
<td>hkmsvc</td>
<td>Health Key and Certificate Management</td>
</tr>
<tr>
<td>Stopped</td>
<td>idsvc</td>
<td>Windows CardSpace</td>
</tr>
<tr>
<td>Running</td>
<td>IKEEXT</td>
<td>IKE and AuthIP IPsec Keying Modules</td>
</tr>
<tr>
<td>Stopped</td>
<td>IPBusEnum</td>
<td>PnP-X IP Bus Enumerator</td>
</tr>
<tr>
<td>Running</td>
<td>iplpsvc</td>
<td>IP Helper</td>
</tr>
<tr>
<td>Stopped</td>
<td>KeyIso</td>
<td>CMG Key Isolation</td>
</tr>
<tr>
<td>Running</td>
<td>KtmRm</td>
<td>KtmRm for Distributed Transaction C...</td>
</tr>
<tr>
<td>Running</td>
<td>LanmanServer</td>
<td>Server</td>
</tr>
<tr>
<td>Running</td>
<td>LanmanWorkstation</td>
<td>Workstation</td>
</tr>
</tbody>
</table>
PS C:\Users\Administrator> get-command | more
Scripting – Windows PowerShell

• One big plus of PowerShell is consistency. With many shells, the commands can vary in complexity; however, given the object-oriented nature of PowerShell, most cmdlets are fairly basic in their usage and are highly consistent.

• The power comes is using combinations of cmdlets.

• The cmdlets naming convention is for the first part to be a verb (for example, get-, format-, out-, or set-) that dictates what the cmdlet does (such as get information, format information, direct information, or set information).

• The next part is a noun, which specifies what is being acted on.
Everything is based around this verb-noun pair; for example, `get-process w*` retrieves information about processes whose names start with the letter w, as shown below.

![PowerShell get-process example](image)
Although the output, as shown on the previous page, is tabular, this is not how the data is returned in PowerShell. It’s referenced in its .NET object format, but the default display format is a table.

You can easily output in other formats, such as a list by piping the output of the `get-process` cmdlet to the `format-list` cmdlet.
• Probably the greatest cmdlet (as well as the best verb-noun combination) that you’ll ever use is `get-help`.

• On its own, `get-help` gives you just basic information, but it can show you the names of other cmdlets, so you can detailed help on them.

• For example, `get-help format-*` will list all the cmdlets starting with `format-` to help you see the options available to you.
```bash
PS C:\users\Administrator> get-help format-*
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Category</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format-List</td>
<td>Cmdlet</td>
<td>Formats the output as a list of properties in which each property appears.</td>
</tr>
<tr>
<td>Format-Custom</td>
<td>Cmdlet</td>
<td>Uses a customized view to format the output.</td>
</tr>
<tr>
<td>Format-Table</td>
<td>Cmdlet</td>
<td>Formats the output as a table.</td>
</tr>
<tr>
<td>Format-Wide</td>
<td>Cmdlet</td>
<td>Formats objects as a wide table that displays only one property of each object.</td>
</tr>
</tbody>
</table>
In addition to getting detailed help about a cmdlet, use the `get-help` command with the name of the cmdlet followed by `-detailed` to get all available help.

Add `-full` to just view a portion of the help, or add `-examples` to have examples of use listed for you.

Note that when the `-detailed` option is selected, the examples are also listed.

The following screen shots illustrate these cases. Note that the detailed case requires several pages of output and I only show the first one here. The same is often true for full and examples.
get-help format-list -detailed

NAME
Format-List

SYNOPSIS
Formats the output as a list of properties in which each property appears on a new line.

SYNTAX

DESCRIPTION
The Format-List cmdlet formats the output of a command as a list of properties in which each property is displayed on a separate line. You can use Format-List to format and display all or selected properties of an object as a list.

Because more space is available for each item in a list than in a table, Windows PowerShell displays more properties of the object in the list, and the property values are less likely to be truncated.

PARAMETERS
-DisplayError [%SwitchParameter%]
Displays errors at the command line.

-Expand <string>
Formats the collection object, as well as the objects in the collection. This parameter is designed to for objects that support the ICollection (%System.Collections%) interface. The default value is EnumOnly.

Valid values are:
-- EnumOnly: Displays the properties of the objects in the collection.
-- CoreOnly: Displays the properties of the collection object.
-- Both: Displays the properties of the collection object and the properties of objects in the collection.

-Force [%SwitchParameter%]
Directs the cmdlet to display all of the error information. Use with the DisplayError or ShowError parameter. By default, when an error object is written to the error or display streams, only some of the error information is displayed.

-GroupBy <Object>
Formats the output in groups based on a shared property or value. Enter an expression or a property of the object.
get-help format-list -examples

NAME
Format-List

SYNOPSIS
Formats the output as a list of properties in which each property appears on a new line.

------------------------ EXAMPLE 1 ------------------------

C:\PS>get-service | format-list

Description

This command formats information about services on the computer as a list. By default, the services are formatted as a table. The Get-Service cmdlet gets objects representing the services on the computer. The pipeline operator passes the results through the pipeline to Format-List. Then, the Format-List cmdlet formats the service information in a list and sends it to the default output cmdlet for display.

------------------------ EXAMPLE 2 ------------------------

C:\PS>$a = get-childitem $pshome\*.ps1xml

Description

These commands display information about the PS1XML files in the Windows PowerShell directory as a list. The first command gets the objects representing the files and stores them in the $a variable. The second command uses Format-List to format information about objects stored in $a. This command uses the InputObject parameter to pass the objects to Format-List, which then sends the formatted output to the default output cmdlet for display.

------------------------ EXAMPLE 3 ------------------------

C:\PS>get-process | format-list -property name, basepriority, priorityclass

Description
We’ve already seen the cmdlet `get-command`. If you want to see all the commands that begin with a certain verb, such as `get`, issue the command `get-command -verb get`.

The output of this command is shown on the next page, but you might want to experiment a bit and try out some other options. For example, try listing all of the commands that use the verbs `add` or `new`. 
Now that you’ve have some basic familiarity with PowerShell, let’s do something more useful with it… let’s try starting and stopping a process.

- What you might want to do before going any further is first run the `get-help *-process` to list all the available commands that deal with a process. You should discover that there are five of these cmdlets.

What we’re going to do over the next few pages is start Notepad as a process running on our server and then use it and then stop the process. This will be illustrated by a sequence of screen shots from the server illustrating what is happening.

First off, we’ll see a screen shot of the current processes on the server. Notice that its alphabetically listed and Notepad is not running (Notepad++ is on my server).
Currently running processes do not include Notepad.
Enter the command: `start notepad` on the command line and press enter. Notepad immediately launches.
Reissue the command `get-process` and notice that now Notepad is listed.

Notice too in the tool tray that you can still see Notepad is there.
Notice on the previous screen shot that the id process id of the Notepad process was 3680. This is used in this version of the stop-process command to identify the process to be stopped.

Reissue the command get-process and notice that now Notepad is no longer listed.

Notice too in the tool tray that Notepad is no longer there.
You can also do a fair amount of customization of the PowerShell interface.

A common system administrator technique is to place scripts in a folder on a server that is frequently backed up. Thus, you might want PowerShell to open up in this default directory.

To illustrate doing this, let’s create a subdirectory in the C:\Users\Administrators folder named MyScripts. Then we’ll configure PowerShell to open in this folder.

To make some of these repetitive steps easier to accomplish, I also created a short-cut to PowerShell and put it on the start menu.
To set-up the default folder for PowerShell to open in, right click the short-cut to PowerShell and select Properties.

Locate the ShortCut tab on the Properties dialog box and in the Start in: text box enter the path to the new directory “C:\Users\Administrator\MyScripts”, then click OK.

Restart PowerShell and you should now see the new default directory loaded.
C:\users\Administrator\MyScripts> _
You can also change the text size and the screen foreground and background colors and many other features including hot-keys and so on in PowerShell.

The next part simply shows you how to reset the text size and the screen colors to customize your PowerShell environment.

Again going through the desktop shortcut to PowerShell, right-click on the short cut and select Properties. Locate the Font tab on the Properties dialog box and reset the Window size to 8x8 (the default is 8x12), then click OK.

Restart PowerShell and you should now see the new default screen size and font size for the window.
PS C:\users\Administrator\MyScripts> _
To change the screen colors for PowerShell, repeat the process but select the Colors tab.

Again going through the desktop shortcut to PowerShell, right click on the short cut and select Properties. Locate the Colors tab on the Properties dialog box and reset the colors to your liking, then click OK.

Restart PowerShell and you should now see the new colors appear.
Windows PowerShell

Copyright © 2009 Microsoft Corporation. All rights reserved.

PS C:\users\Administrator\MyScripts> _