Powershell 3 Lab Review 1

**1. Run a command that will display the newest 100 entries from the Application event log. Do not use Get-WinEvent.**

PS> Get-EventLog Application -Newest 100

Index Time EntryType Source InstanceID Message

----- ---- --------- ------ ---------- -------

1340 Nov 17 15:09 Information SecurityCenter 1 The Windo...

1339 Nov 17 15:07 Information Windows Search Se... 1073742827 The Windo...

1338 Nov 17 15:07 Information ESENT 326 SearchInd...

1337 Nov 17 15:07 Information Software Protecti... 3221233669 SLUI.exe ...

1336 Nov 17 15:07 Information ESENT 105 SearchInd...

1335 Nov 17 15:07 Information ESENT 102 SearchInd...

1334 Nov 17 15:07 Information Software Protecti... 1073750054 The rules...

...

**2. Write a command line that displays only the five top processes based on virtual memory (VM) usage.**

PS> Get-Process | Sort-Object VM -Descending | Select-Object -First 5

Handles NPM(K) PM(K) WS(K) VM(M) CPU(s) Id SI ProcessName

------- ------ ----- ----- ----- ------ -- -- -----------

643 48 43888 46556 ...13 3.86 3684 1 SearchUI

416 23 42276 51180 ...83 23.03 936 0 svchost

729 49 140848 162076 ...45 14.20 4564 1 powershell

616 59 101640 56556 ...70 34.70 1984 0 MsMpEng

1869 109 68268 85248 ...69 26.50 512 0 svchost

**3. Create a CSV file that contains all services, including only the service names and statuses. Have running services listed before stopped services.**

PS> Get-Service | Select-Object Name, Status | Sort-Object Status -Descending | Export-CSV "C:\Services.csv"

PS> Get-Content "C:\Services.csv"

#TYPE Selected.System.ServiceProcess.ServiceController

"Name","Status"

"W32Time","Running"

"VMware Physical Disk Helper Service","Running"

"FontCache","Running"

"Themes","Running"

...

"SNMPTRAP","Stopped"

"svsvc","Stopped"

"SmsRouter","Stopped"

"UI0Detect","Stopped"

"tzautoupdate","Stopped"

...

**4. Write a command line that changes the startup type of the BITS service to Manual.**

PS> Get-Service BITS | Select-Object StartType

StartType

---------

Automatic

PS> Set-Service BITS -StartupType Manual

PS> Get-Service BITS | Select-Object StartType

StartType

---------

Manual

**5. Display a list of all files named win\*.\* on your computer. Start in the C:\ folder. Note: you may need to experiment and use some new parameters of a cmdlet in order to complete this task.**

PS> Get-ChildItem "\" -Filter "win\*.\*" -Recurse

Directory: C:\

Mode LastWriteTime Length Name

---- ------------- ------ ----

d----- 17/11/2016 3:06 PM Windows

Directory: C:\Program Files

Mode LastWriteTime Length Name

---- ------------- ------ ----

d----- 3/11/2016 3:50 PM Windows Defender

d----- 3/11/2016 3:50 PM Windows Mail

d----- 3/11/2016 3:50 PM Windows Media Player

d----- 3/11/2016 3:50 PM Windows Multimedia Platform

d----- 30/10/2015 6:24 PM Windows NT

d----- 3/11/2016 3:50 PM Windows Photo Viewer

d----- 3/11/2016 3:50 PM Windows Portable Devices

d---s- 30/10/2015 6:24 PM WindowsPowerShell

Directory: C:\Program Files\Common Files\VMware\Drivers\vmci\sockets\bin

Mode LastWriteTime Length Name

---- ------------- ------ ----

d----- 5/09/2016 12:27 PM win32

d----- 5/09/2016 12:27 PM win64

...

**6. Get a directory listing for C:\Program Files. Include all subfolders, and have the directory listing go into a text file named C:\Dir.txt (remember to use the > redirector, or the Out-File cmdlet).**

PS> Get-ChildItem "C:\Program Files" -Recurse | Out-File "C:\Dir.txt"

PS> Get-Content "C:\Dir.txt"

Directory: C:\Program Files

Mode LastWriteTime Length Name

---- ------------- ------ ----

d----- 3/11/2016 3:49 PM CMAK

d----- 5/09/2016 12:27 PM Common Files

d----- 3/11/2016 3:50 PM Internet Explorer

d----- 5/09/2016 12:27 PM VMware

d----- 3/11/2016 3:50 PM Windows Defender

d----- 3/11/2016 3:50 PM Windows Mail

d----- 3/11/2016 3:50 PM Windows Media Player

d----- 3/11/2016 3:50 PM Windows Multimedia Platform

d----- 30/10/2015 6:24 PM Windows NT

d----- 3/11/2016 3:50 PM Windows Photo Viewer

d----- 3/11/2016 3:50 PM Windows Portable Devices

d---s- 30/10/2015 6:24 PM WindowsPowerShell

Directory: C:\Program Files\CMAK

Mode LastWriteTime Length Name

---- ------------- ------ ----

d----- 3/11/2016 3:50 PM en-US

d----- 3/11/2016 3:49 PM Support

Directory: C:\Program Files\CMAK\en-US

Mode LastWriteTime Length Name

---- ------------- ------ ----

-a---l 3/11/2016 10:23 AM 84992 cmak.exe.mui

...

**7. Get a list of the most recent 20 entries from the Security event log, and convert the information to XML. Do not create a file on disk: have the XML display in the console window.**

**Note that the XML may display as a single top-level object, rather than as raw XML data—that’s fine. That’s just how PowerShell displays XML. You can pipe the XML object to Format-Custom to see it expanded out into an object hierarchy, if you like.**

PS> Get-EventLog Security -Newest 20 | ConvertTo-XML -As String

<?xml version="1.0"?>

<Objects>

<Object Type="System.Diagnostics.EventLogEntry">

<Property Name="EventID" Type="System.Int32">4634</Property>

<Property Name="MachineName" Type="System.String">Polonius.elsinore.local</Property>

<Property Name="Data" Type="System.Byte[]">System.Byte[]</Property>

<Property Name="Index" Type="System.Int32">10556</Property>

<Property Name="Category" Type="System.String">(12545)</Property>

<Property Name="CategoryNumber" Type="System.Int16">12545</Property>

<Property Name="EntryType" Type="System.Diagnostics.EventLogEntryType">SuccessAudit</Property>

...

**8. Get a list of services, and export the data to a CSV file named C:\services.csv.**

PS> Get-Service | Export-CSV "C:\services.csv"

PS> Get-Content "C:\services.csv"

#TYPE System.ServiceProcess.ServiceController

"Name","RequiredServices","CanPauseAndContinue","CanShutdown","CanStop","DisplayName","DependentServices","MachineName","ServiceName","ServicesDependedOn","ServiceHandle","Status","ServiceType","StartType","Site","Container"

"AJRouter","System.ServiceProcess.ServiceController[]","False","False","False","AllJoyn Router Service","System.ServiceProcess.ServiceController[]",".","AJRouter","System.ServiceProcess.ServiceController[]","SafeServiceHandle","Stopped","Win32ShareProcess","Manual",,

"ALG","System.ServiceProcess.ServiceController[]","False","False","False","Application Layer Gateway Service","System.ServiceProcess.ServiceController[]",".","ALG","System.ServiceProcess.ServiceController[]","SafeServiceHandle","Stopped","Win32OwnProcess","Manual",,

...

**9. Get a list of services. Keep only the services’ names, display names, and statuses, and send that information to an HTML file. Have the phrase “Installed Services” displayed in the HTML file before the table of service information.**

PS > Get-Service | Select-Object ServiceName, DisplayName, Status | ConvertTo-HTML -Title "Installed services"

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<title>Installed services</title>

</head><body>

<table>

<colgroup><col/><col/><col/></colgroup>

<tr><th>ServiceName</th><th>DisplayName</th><th>Status</th></tr>

<tr><td>AJRouter</td><td>AllJoyn Router Service</td><td>Stopped</td></tr>

<tr><td>ALG</td><td>Application Layer Gateway Service</td><td>Stopped</td></tr>

<tr><td>AppIDSvc</td><td>Application Identity</td><td>Stopped</td></tr>

<tr><td>Appinfo</td><td>Application Information</td><td>Running</td></tr>

...

**10. Create a new alias, named D, which runs Get-ChildItem. Export just that alias to a file. Now, close the shell and open a new console window. Import that alias into the shell. Make sure you can run D and get a directory listing.**

PS C:\Windows\system32> New-Alias D Get-ChildItem

PS C:\Windows\system32> D

Directory: C:\Windows\system32

Mode LastWriteTime Length Name

---- ------------- ------ ----

d----- 31/10/2015 5:00 AM 0409

d----- 3/11/2016 3:50 PM AdvancedInstallers

d----- 30/10/2015 6:24 PM AppLocker

d----- 3/11/2016 3:50 PM appraiser

d----- 30/10/2015 6:24 PM ar-SA

...

PS> Export-Alias "C:\LabAlias"

PS> exit

PS> D

D : The term 'D' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.

...

PS> Import-Alias "C:\LabAlias" -Force

PS> D

Directory: C:\Windows\system32

Mode LastWriteTime Length Name

---- ------------- ------ ----

d----- 31/10/2015 5:00 AM 0409

d----- 3/11/2016 3:50 PM AdvancedInstallers

d----- 30/10/2015 6:24 PM AppLocker

d----- 3/11/2016 3:50 PM appraiser

d----- 30/10/2015 6:24 PM ar-SA

...

**11. Display a list of event logs that are available on your system.**

PS C:\Windows\system32> Get-EventLog -List

Max(K) Retain OverflowAction Entries Log

------ ------ -------------- ------- ---

20,480 0 OverwriteAsNeeded 1,417 Application

20,480 0 OverwriteAsNeeded 0 HardwareEvents

512 7 OverwriteOlder 0 Internet Explorer

20,480 0 OverwriteAsNeeded 0 Key Management Service

20,480 0 OverwriteAsNeeded 10,654 Security

20,480 0 OverwriteAsNeeded 1,608 System

512 0 OverwriteAsNeeded 0 ThinPrint Diagnostics

15,360 0 OverwriteAsNeeded 147 Windows PowerShell

**12. Run a command that will display the current directory that the shell is in.**

PS> Get-Location

Path

----

C:\Windows\system32

**13. Run a command that will display the most recent commands that you have run in the shell. Locate the command that you ran for task 11. Using two commands connected by a pipeline, rerun the command from task 11.**

PS> Get-History

Id CommandLine

-- -----------

1 get-help get-eventlog

2 Get-EventLog -List

3 get-help dir

4 get-help cd

5 get-command -noun location

6 Get-Location

7 get-command -noun history

PS> Get-History -Id 2 | Invoke-History

Get-EventLog -List

Max(K) Retain OverflowAction Entries Log

------ ------ -------------- ------- ---

20,480 0 OverwriteAsNeeded 1,434 Application

20,480 0 OverwriteAsNeeded 0 HardwareEvents

512 7 OverwriteOlder 0 Internet Explorer

20,480 0 OverwriteAsNeeded 0 Key Management Service

20,480 0 OverwriteAsNeeded 10,656 Security

20,480 0 OverwriteAsNeeded 1,608 System

512 0 OverwriteAsNeeded 0 ThinPrint Diagnostics

15,360 0 OverwriteAsNeeded 147 Windows PowerShell

**14. Run a command that modifies the Security event log to overwrite old events as needed.**

PS> Limit-EventLog Security -OverflowAction OverwriteAsNeeded

**15. Use the New-Item cmdlet to make a new directory named C:\Review. This is not the same as running Mkdir; the New-Item cmdlet will need to know what kind of new item you want to create. Read the help for the cmdlet.**

PS> New-Item "C:\Review" -ItemType "Directory"

Directory: C:\

Mode LastWriteTime Length Name

---- ------------- ------ ----

d----- 18/11/2016 2:13 PM Review

**16. Display the contents of this registry key:**

**HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders**

PS> Get-ChildItem "HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders"

**17. Find (but please do not run) cmdlets that can ...**

**Restart a computer**

Restart-Computer

**Shut down a computer**

Stop-Computer

**Remove a computer from a workgroup or domain**

Remove-Computer

**Restore a computer’s System Restore checkpoint**

Restore-Computer

**18. What command do you think could change a registry value? Hint: it’s the same noun as the cmdlet you found for task 16.**

Set-Item