Powershell 3 Lab Chapter 10

**1. Display a table of processes that includes only the process names, IDs, and whether or not they’re responding to Windows (the Responding property has that information). Have the table take up as little horizontal room as possible, but don’t allow any information to be truncated.**

PS> Get-Process | Format-Table -Property ProcessName, Id, Responding -Autosize

ProcessName Id Responding

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

ApplicationFrameHost 4456 True

audiodg 4468 True

conhost 700 True

csrss 584 True

csrss 644 True

dllhost 2836 True

dllhost 2976 True

dwm 964 True

explorer 3884 True

Idle 0 True

lsass 768 True

msdtc 2216 True

MsMpEng 2000 True

...

**2. Display a table of processes that includes the process names and IDs. Also include columns for virtual and physical memory usage, expressing those values in megabytes (MB).**

PS> get-process | format-table -Property ProcessName, Id, @{n='Virtual Memory (MB)'; e={$\_.VirtualMemorySize64 / 1MB -as [int]}}, @{n='Physical Memory (MB)'; e={$\_.PagedMemorySize64 / 1MB -as [int]}}

ProcessName Id Virtual Memory (MB) Physical Memory (MB)

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

ApplicationFrameHost 4456 2097291 7

conhost 700 2097259 6

csrss 584 2097200 1

csrss 644 2097288 1

dllhost 2836 2097257 3

dllhost 2976 2097204 3

dwm 964 2097363 44

explorer 3884 2097587 26

Idle 0 0 0

lsass 768 2097200 5

msdtc 2216 2097197 2

MsMpEng 2000 2097610 109

NisSrv 2360 2097204 5

OneDrive 4744 122 4

powershell 2332 2097837 236

RuntimeBroker 3684 2097314 14

SearchIndexer 1740 2097311 26

...

**3. Use Get-EventLog to display a list of available event logs. (Hint: you’ll need to read the help to learn the correct parameter to accomplish that.) Format the output as a table that includes, in this order, the log display name and the retention period. The column headers must be “LogName” and “RetDays.”**

PS> Get-EventLog -List | Format-Table -Property @{n='LogName'; e={$\_.LogDisplayName}}, @{n='RetDays'; e={$\_.MinimumRetentionDays}}

LogName RetDays

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

Application 0

Hardware Events 0

Internet Explorer 7

Key Management Service 0

Security 0

System 0

ThinPrint Diagnostics 0

Windows PowerShell 0

**4. Display a list of services so that a separate table is displayed for services that are started and services that are stopped. Services that are started should be displayed first. (Hint: you’ll use a -groupBy parameter).**

PS> Get-Service | Sort-Object -Property Status -Descending | Format-Table -GroupBy Status

Status: Running

Status Name DisplayName

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

Running MSDTC Distributed Transaction Coordinator

Running NcbService Network Connection Broker

Running Netlogon Netlogon

Running LSM Local Session Manager

Running VMTools VMware Tools

Running MpsSvc Windows Firewall

Running nsi Network Store Interface Service

Running VGAuthService VMware Alias Manager and Ticket Ser...

Running PcaSvc Program Compatibility Assistant Ser...

Running Netman Network Connections

...

Status: Stopped

Status Name DisplayName

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

Stopped TermService Remote Desktop Services

Stopped TapiSrv Telephony

Stopped wbengine Block Level Backup Engine Service

Stopped TabletInputService Touch Keyboard and Handwriting Pane...

Stopped WpnService Windows Push Notifications Service

Stopped WPDBusEnum Portable Device Enumerator Service

Stopped TPAutoConnSvc TP AutoConnect Service

Stopped WalletService WalletService

Stopped VSS Volume Shadow Copy

Stopped TieringEngineSe... Storage Tiers Management

...