Powershell 3 Lab Chapter 4

Alex Stock

**1. Display a list of running processes.**

PS > Get-Process

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

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

290 16 6720 21760 ...95 0.38 4284 1 ApplicationFrame

162 10 6012 10312 ...98 0.52 2044 0 audiodg

168 11 4900 14200 ...48 0.61 3964 1 conhost

345 13 1176 3380 ...04 0.67 584 0 csrss

243 16 1212 4696 ...02 2.77 668 1 csrss

214 13 3436 9668 ...06 0.28 2648 0 dllhost

330 25 47332 60200 ...66 6.16 96 1 dwm

...

**2. Display the 100 most recent entries from the Application event log.**

PS> Get-EventLog -LogName Application -Newest 100

Index Time EntryType Source

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

1759 Jun 09 12:50 Information Windows Error Rep...

1758 Jun 09 12:50 Information Windows Error Rep...

1757 Jun 09 12:50 Information Windows Error Rep...

1756 Jun 09 12:50 Information Windows Error Rep...

1755 Jun 09 12:50 Information Windows Error Rep...

...

**3. Display a list of all commands that are of the “cmdlet” type.**

PS> Get-Command -CommandType Cmdlet

CommandType Name Version Source

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

Cmdlet Add-AppxPackage 2.0.0.0 Appx

Cmdlet Add-AppxProvisionedPackage 3.0 Dism

Cmdlet Add-AppxVolume 2.0.0.0 Appx

Cmdlet Add-BitsFile 2.0.0.0 BitsTransfer

...

**4. Display a list of all aliases.**

PS> Get-Alias

CommandType Name Version Source

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

Alias % -> ForEach-Object

Alias ? -> Where-Object

Alias ac -> Add-Content

Alias asnp -> Add-PSSnapin

Alias cat -> Get-Content

...

**5. Make a new alias, so you can run d to get a directory listing.**

PS> New-Alias -Name d -Value Get-ChildItem

PS> d

Directory: C:\Windows\system32

Mode LastWriteTime Length Name

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

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

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

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

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

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

d----- 30/10/2015 6:24 PM bg-BG

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

...

**6. Display a list of services that begin with the letter M.**

PS> Get-Service -Name M\*

Status Name DisplayName

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

Stopped MapsBroker Downloaded Maps Manager

Running MpsSvc Windows Firewall

Running MSDTC Distributed Transaction Coordinator

Stopped MSiSCSI Microsoft iSCSI Initiator Service

Stopped msiserver Windows Installer

**7. Display a list of all Windows Firewall rules.**

PS C:\Windows\system32> Get-NetFirewallRule

Name : vm-monitoring-dcom

DisplayName : Virtual Machine Monitoring (DCOM-In)

Description : Allow DCOM traffic for remote Windows Management Instrumentation.

DisplayGroup : Virtual Machine Monitoring

Group : @icsvc.dll,-700

Enabled : False

Profile : Any

Platform : {}

Direction : Inbound

Action : Allow

EdgeTraversalPolicy : Block

LooseSourceMapping : False

LocalOnlyMapping : False

Owner :

PrimaryStatus : OK

Status : The rule was parsed successfully from the store. (65536)

EnforcementStatus : NotApplicable

PolicyStoreSource : PersistentStore

PolicyStoreSourceType : Local

Name : vm-monitoring-icmpv4

DisplayName : Virtual Machine Monitoring (Echo Request - ICMPv4-In)

Description : Echo Request messages are sent as ping requests to other nodes.

DisplayGroup : Virtual Machine Monitoring

Group : @icsvc.dll,-700

Enabled : False

Profile : Any

Platform : {}

Direction : Inbound

Action : Allow

EdgeTraversalPolicy : Block

LooseSourceMapping : False

LocalOnlyMapping : False

Owner :

PrimaryStatus : OK

Status : The rule was parsed successfully from the store. (65536)

EnforcementStatus : NotApplicable

PolicyStoreSource : PersistentStore

PolicyStoreSourceType : Local

...

**8. Display a list only of inbound Windows Firewall rules.**

PS> Get-NetFirewallRule -Direction Inbound

Name : vm-monitoring-dcom

DisplayName : Virtual Machine Monitoring (DCOM-In)

Description : Allow DCOM traffic for remote Windows Management Instrumentation.

DisplayGroup : Virtual Machine Monitoring

Group : @icsvc.dll,-700

Enabled : False

Profile : Any

Platform : {}

Direction : Inbound

Action : Allow

EdgeTraversalPolicy : Block

LooseSourceMapping : False

LocalOnlyMapping : False

Owner :

PrimaryStatus : OK

Status : The rule was parsed successfully from the store. (65536)

EnforcementStatus : NotApplicable

PolicyStoreSource : PersistentStore

PolicyStoreSourceType : Local

Name : vm-monitoring-icmpv4

DisplayName : Virtual Machine Monitoring (Echo Request - ICMPv4-In)

Description : Echo Request messages are sent as ping requests to other nodes.

DisplayGroup : Virtual Machine Monitoring

Group : @icsvc.dll,-700

Enabled : False

Profile : Any

Platform : {}

Direction : Inbound

Action : Allow

EdgeTraversalPolicy : Block

LooseSourceMapping : False

LocalOnlyMapping : False

Owner :

PrimaryStatus : OK

Status : The rule was parsed successfully from the store. (65536)

EnforcementStatus : NotApplicable

PolicyStoreSource : PersistentStore

PolicyStoreSourceType : Local

...