Microsoft

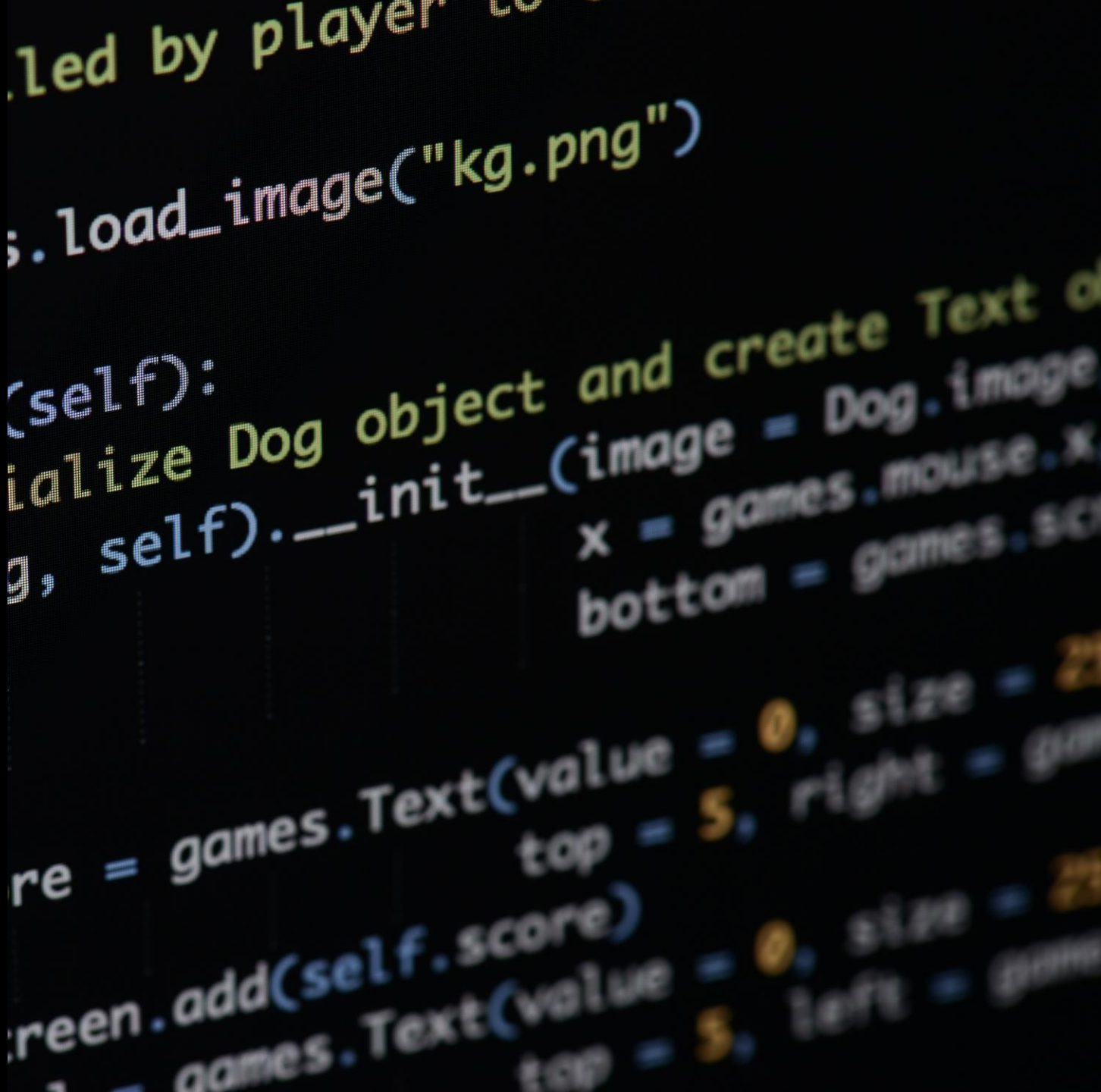
System Management Fundamentals

PowerShell 简介

Intro to PowerShell

Apr 2021

Microsoft Reactor | Ryan Chung

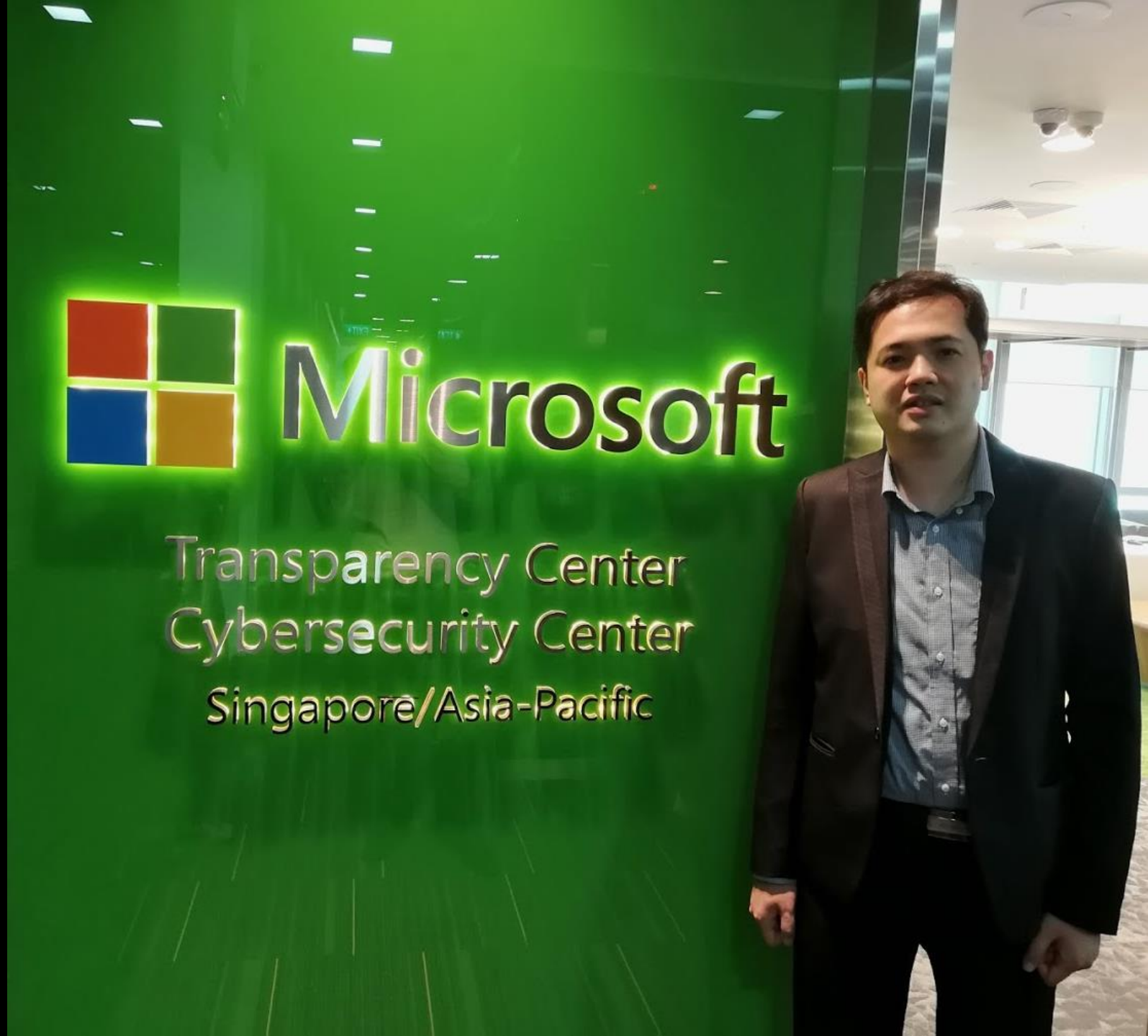


Microsoft

Ryan Chung

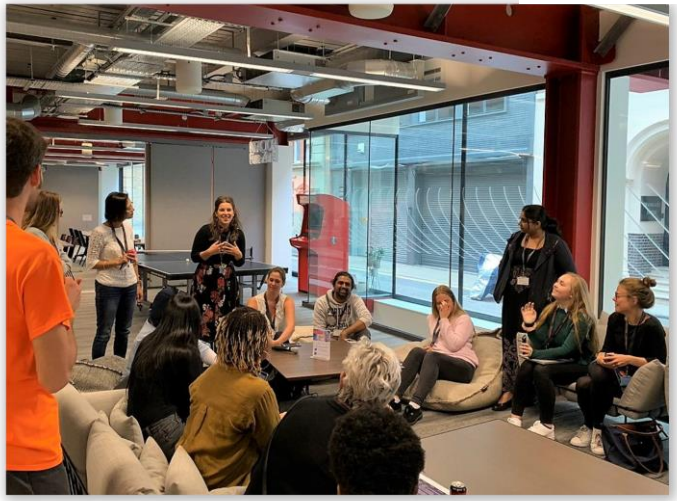
Instructor / DevelopIntelligence
Founder / MobileDev.TW

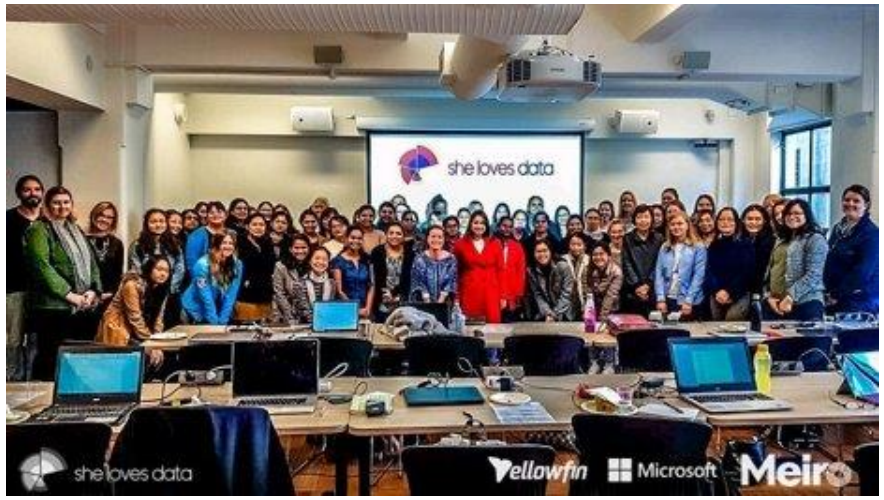
@ryanchung403 on WeChat
Ryan@MobileDev.TW

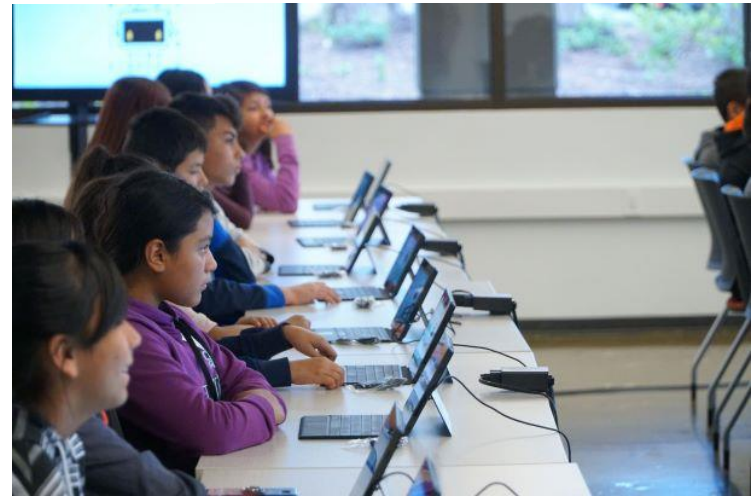


Microsoft

Reactor







developer.microsoft.com/reactor/

@MSFTReactor on Twitter

1000 XP

PowerShell 简介

58 分钟 • 模块 • 9 单元

★★★★½ 4.6 (302) 对其进行评级

初级 开发人员 学生 Visual Studio

了解 PowerShell 的基础知识。 此跨平台命令行 shell 和脚本语言是专为任务自动化和配置管理设计的。 你将了解一些基础知识，例如 PowerShell 的涵义、它的用途以及使用方法。

学习目标

完成此模块后，你将能够：

- 了解 PowerShell 的涵义及其用途。
- 了解 cmdlet
- 在管道中构造一系列 cmdlet。
- 对命令应用健全的筛选和格式设置原则。

先决条件

- 基本熟悉如何使用命令行 shell（如命令提示符或 Git Bash）
- 已安装 Visual Studio Code
- 能够安装 Visual Studio Code 扩展
- 如果不使用 Windows 操作系统，则能够在计算机上安装软件

书签 添加到集合

学习目标

- 了解PowerShell与其用途
- 使用Cmdlet
- 使用Cmdlet与管线
- 指令应用格式原则

PowerShell = 命令列介面 + Script 语言

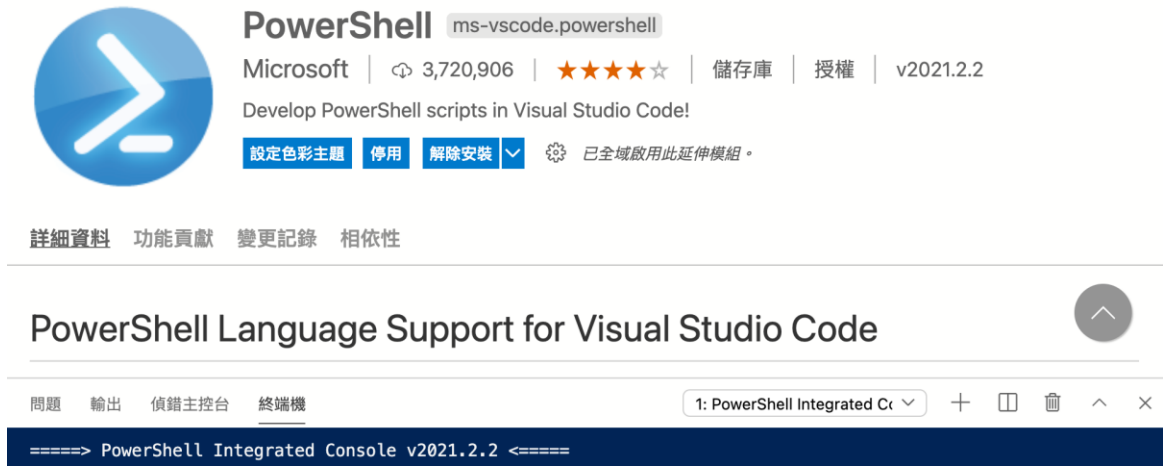
- 比图形介面快
- 任务自动化的好帮手(批次多行执行)
- 指令可重复利用

```
PowerShell 7.1.3
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.
```

安裝PowerShell

- Windows
  - 已內建
- Mac
  - brew install --cask powershell
- Visual Studio Code
  - 可安裝PowerShell Extension



Hello PowerShell!

- 开启PowerShell
  - Windows作业系统内建，直接搜寻Windows PowerShell
  - 其他作业系统可于终端机中使用pwsh指令开启
- 确认开启后，输入第一个指令$PSVersionTable
  - 显示版本资讯

单纯看版本号

- 指令：$PSVersionTable.PSVersion

```
Major  Minor  Patch  PreReleaseLabel BuildLabel
-----  -----  -----  --------------- ----------
7      1      3
```

Cmdlet

- 已编译的指令
- 动词-名词(怎么做-什么事)

查看可以做的动作

- 指令：Get-Verb

```
Verb        AliasPrefix Group           Description
----        ----------- -----           -----------
Add         a           Common          Adds a resource to a container, or attaches an …
Clear       cl          Common          Removes all the resources from a container but …
Close       cs          Common          Changes the state of a resource to make it inac…
Copy        cp          Common          Copies a resource to another name or to another…
Enter       et          Common          Specifies an action that allows the user to mov…
Exit        ex          Common          Sets the current environment or context to the …
Find        fd          Common          Looks for an object in a container that is unkn…
Format      f           Common          Arranges objects in a specified form or layout
Get         g           Common          Specifies an action that retrieves a resource
```

查看所有的指令(动词-名词)

- 指令：Get-Command

```
CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        cd..
Function        cd\
Function        Clear-Host
Function        Compress-Archive                                   1.2.5      Microsof…
Function        Configuration                                      2.0.5      PSDesire…
Function        Expand-Archive                                     1.2.5      Microsof…
Function        Find-Command                                       2.2.5      PowerShe…
Function        Find-DSCResource                                   2.2.5      PowerShe…
Function        Find-Module                                        2.2.5      PowerShe…
```

太多了，可使用筛选

- 范例指令：Get-Command –Noun J*
  - 列出所有名词为J开头的Cmdlet

```
CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Cmdlet          ConvertFrom-Json                                   7.0.0.0    Microsof…
Cmdlet          ConvertTo-Json                                     7.0.0.0    Microsof…
Cmdlet          Debug-Job                                          7.1.3.0    Microsof…
Cmdlet          Get-Job                                            7.1.3.0    Microsof…
Cmdlet          Receive-Job                                        7.1.3.0    Microsof…
Cmdlet          Remove-Job                                         7.1.3.0    Microsof…
Cmdlet          Start-Job                                          7.1.3.0    Microsof…
Cmdlet          Stop-Job                                           7.1.3.0    Microsof…
Cmdlet          Test-Json                                          7.0.0.0    Microsof…
Cmdlet          Wait-Job                                           7.1.3.0    Microsof…
```

太多了，可使用筛选

- 范例指令：Get-Command -Verb Get -Noun C*
  - 列出所有动词是Get、名词为C开头的Cmdlet

```
CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        Get-ClusteredScheduledTask                         1.0.0.0    ScheduledTasks
Function        Get-CredsFromCredentialProvider                    2.2.5      PowerShellGet
Cmdlet          Get-Certificate                                    1.0.0.0    PKI
Cmdlet          Get-CertificateAutoEnrollmentPolicy                1.0.0.0    PKI
Cmdlet          Get-CertificateEnrollmentPolicyServer              1.0.0.0    PKI
Cmdlet          Get-CertificateNotificationTask                    1.0.0.0    PKI
Cmdlet          Get-ChildItem                                      7.0.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-CimAssociatedInstance                          7.0.0.0    CimCmdlets
Cmdlet          Get-CimClass                                       7.0.0.0    CimCmdlets
Cmdlet          Get-CimInstance                                    7.0.0.0    CimCmdlets
Cmdlet          Get-CimSession                                     7.0.0.0    CimCmdlets
Cmdlet          Get-Clipboard                                      7.0.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-CmsMessage                                     7.0.0.0    Microsoft.PowerShell.Security
Cmdlet          Get-Command                                        7.1.3.0    Microsoft.PowerShell.Core
Cmdlet          Get-ComputerInfo                                   7.0.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-Content                                        7.0.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-Counter                                        7.0.0.0    Microsoft.PowerShell.Diagnostics
Cmdlet          Get-Credential                                     7.0.0.0    Microsoft.PowerShell.Security
Cmdlet          Get-Culture                                        7.0.0.0    Microsoft.PowerShell.Utility
```

开启协助系统

- 指令：Get-Help

```
TOPIC
    PowerShell Help System

SHORT DESCRIPTION
    Displays help about PowerShell cmdlets and concepts.

LONG DESCRIPTION
    PowerShell Help describes PowerShell cmdlets, functions, scripts, and
    modules, and explains concepts, including the elements of the PowerShell
    language.
```

单一指令细节查询

- 指令：Get-Help –Name Get-Content
  - 查询名为Get-Content的Cmdlet资讯

```
NAME
    Get-Content

SYNOPSIS
    Gets the content of the item at the specified location.


SYNTAX
    Get-Content [-Path] <System.String[]> [-ReadCount <System.Int64>]
    [-TotalCount <System.Int64>] [-Tail <System.Int32>] [-Filter
    <System.String>] [-Include <System.String[]>] [-Exclude <System.String[]>]
    [-Force] [-Credential <System.Management.Automation.PSCredential>]
    [-Delimiter <System.String>] [-Wait] [-Raw] [-Encoding {ASCII |
```

单一指令细节特定内容查询

- 指令：Get-Help Get-Content -Examples
  - 查看Get-Content的协助资讯中的示例

```
NAME
    Get-Content

SYNOPSIS
    Gets the content of the item at the specified location.


    ---------- Example 1: Get the content of a text file ----------

    1..100 | ForEach-Object { Add-Content -Path .\LineNumbers.txt -Value "This
    is line $_." }
    Get-Content -Path .\LineNumbers.txt

    This is Line 1
    This is Line 2
    ...
    This is line 99.
    This is line 100.
```

单一指令细节特定内容查询

- 指令：Get-Help Cmdlet_Name -XXX
  - Full
    - 标准版 + 参数、输入、输出
  - Detailed
    - 标准版 + 参数
  - Examples
    - 示例说明
  - Online
    - 开启该指令网页
  - Parameter
    - 需指定参数名称

查看目前正在这台主机上的执行程序

- 指令：Get-Process

```
NPM(K)    PM(M)      WS(M)     CPU(s)      Id  SI ProcessName
------    -----      -----     ------      --  -- -----------
     7     1.45       2.09       0.00   13244   0 aesm_service
    32    34.16      46.22       4.69   23216  16 ApplicationFrameHost
     8     1.53       1.76       0.00     148   0 AppVShNotify
     7     1.46       2.72       0.00    5620   0 ApsInsSvc
    18     4.16       3.20       0.00    8112   0 armsvc
    53    40.78      43.25     196.12   20872  16 atmgr
    16    15.65      19.84   1,774.72   21472   0 audiodg
    22     5.58       1.55       1.27   15088  16 avgnt
    75   214.80      51.00       0.00   19752   0 avguard
```

检视一个执行程序

- 指令：Get-Process ThisProcessName

```
PS                                Get-Process Calculator

 NPM(K)    PM(M)      WS(M)     CPU(s)      Id  SI ProcessName
 ------    -----      -----     ------      --  -- -----------
     28    21.61      47.66       0.48   14248  16 Calculator
```

检视一个执行程序的属性与方法

- 指令：Get-Process ThisProcessName | Get-Member

```
PS                             Get-Process Calculator | Get-Member

   TypeName: System.Diagnostics.Process

Name                           MemberType     Definition
----                           ----------     ----------
Handles                        AliasProperty  Handles = Handlecount
Name                           AliasProperty  Name = ProcessName
NPM                            AliasProperty  NPM = NonpagedSystemMemorySize64
PM                             AliasProperty  PM = PagedMemorySize64
SI                             AliasProperty  SI = SessionId
VM                             AliasProperty  VM = VirtualMemorySize64
WS                             AliasProperty  WS = WorkingSet64
```

检视一个执行程序的属性与方法，并照类型筛选

- 指令：Get-Process ThisProcessName | Get-Member -MemberType TypeName

```
PS                          Get-Process Calculator | Get-Member -MemberType Property

   TypeName: System.Diagnostics.Process

Name                        MemberType Definition
----                        ---------- ----------
BasePriority                Property   int BasePriority {get;}
Container                   Property   System.ComponentModel.IContainer Container {get;}
EnableRaisingEvents         Property   bool EnableRaisingEvents {get;set;}
ExitCode                    Property   int ExitCode {get;}
ExitTime                    Property   datetime ExitTime {get;}
Handle                      Property   System.IntPtr Handle {get;}
HandleCount                 Property   int HandleCount {get;}
HasExited                   Property   bool HasExited {get;}
Id                          Property   int Id {get;}
MachineName                 Property   string MachineName {get;}
MainModule                  Property   System.Diagnostics.ProcessModule MainModule {get;}
```

练习

- 列出名词是File开头相关的Cmdlet

练习

- 列出名词是File开头且**动词是Get**的Cmdlet

练习

- 取得Get-FileHash的指令介绍

练习

- 取得Get-FileHash的示例

练习

- 列出目前本地端正在运行的程序

练习

- 请只列出目前本地端正在运行的某一个程序

练习

- 请搭配管线，将该程序的属性、方法以及回传类型列出

再论管线 Pipeline

- 管线评估
- 建构辅助器
- 过滤与格式化

再论管线 Pipeline

- 管线评估
  - 什么样的管线输入值是合法的?
  - 参数处理的顺序
  - 如何提供数据
- 建构辅助器
- 过滤与格式化

管线评估 – 以 Get-Process为例

- 什么是 Get-Process
  - help Get-Process -Full

```
NAME
    Get-Process

SYNOPSIS
    Gets the processes that are running on the local computer.


SYNTAX
    Get-Process [[-Name] <System.String[]>] [-FileVersionInfo] [-Module] [<CommonParameters>]

    Get-Process [-FileVersionInfo] -Id <System.Int32[]> [-Module] [<CommonParameters>]

    Get-Process [-FileVersionInfo] -InputObject <System.Diagnostics.Process[]> [-Module] [<CommonParameters>]

    Get-Process -Id <System.Int32[]> -IncludeUserName [<CommonParameters>]

    Get-Process [[-Name] <System.String[]>] -IncludeUserName [<CommonParameters>]

    Get-Process -IncludeUserName -InputObject <System.Diagnostics.Process[]> [<CommonParameters>]
```

观察 PARAMETERS 与 INPUTS ，以下的共同点是？

- Parameters
  - Id <System.Int32[]>
  - InputObject <System.Diagnostics.Process[]>
  - Name <System.String[]>
- Inputs
  - System.Diagnostics.Process

观察 PARAMETERS 与 INPUTS，以下的共同点是：

- Parameters
  - Id <System.Int32[]>
    - Accept pipeline input? True (ByPropertyName)
  - InputObject <System.Diagnostics.Process[]>
    - Accept pipeline input? True (ByValue)
  - Name <System.String[]>
    - Accept pipeline input? True (ByPropertyName)
- Inputs
  - System.Diagnostics.Process
    - You can pipe a process object to this cmdlet.

管线如何确认输入值是否合法?

- By Value (by Type)
  - 例如，检查输入值是否像是System.Diagnostics.Process[]
- By Property Name
  - 如本例，是否为Name 或 Id

模拟管线测试

- 制造一个管线的输入
  - [pscustomobject]@{Name='wininit'} | Get-Process

```
PS                          [pscustomobject]@{Name='wininit'} | Get-Process

 NPM(K)    PM(M)      WS(M)     CPU(s)      Id  SI ProcessName
 ------    -----      -----     ------      --  -- -----------
     11     1.79       3.62       0.00    1592   0 wininit
```

管线辅助器

- 例：找到名称符合tccd的程序
  - Get-Process | Where-Object Name -eq wininit

```
PS                          Get-Process | Where-Object Name -eq wininit

 NPM(K)    PM(M)      WS(M)     CPU(s)      Id  SI ProcessName
 ------    -----      -----     ------      --  -- -----------
     11     1.79       3.62       0.00    1592   0 wininit
```

Operator

- eq 相等
- gt 大于
- lt 小于
- Match 是否吻合该正规表达式(Regular Expression)
  - 例：以World开头的程序
    - Get-Process | Where-Object Name -Match "^Se.*"

```
PS                      Get-Process | Where-Object Name -Match "^Se.*"

 NPM(K)    PM(M)      WS(M)     CPU(s)      Id  SI ProcessName
 ------    -----      -----     ------      --  -- -----------
    145   189.92     278.20      21.73   11752  16 SearchApp
     14     4.28      15.66       0.00    5436   0 SearchFilterHost
     87   236.38     174.61       0.00    9620   0 SearchIndexer
     10     1.95       8.29       0.02    4148  16 SearchProtocolHost
     14     2.94      15.27       0.00   22660   0 SearchProtocolHost
```

Filtering Left 尽快筛选，提升效率

- 哪一个比较好？为什么？

```
Get-Process | Select-Object Name | Where-Object Name -eq wininit
```

```
Get-Process | Where-Object Name -eq wininit | Select-Object Name
```

练习

- 抓出本地端主机，最吃CPU资源的前三个程序

```
Get-Process | Where-Object CPU -gt 100 | Sort-Object CPU -Descending | Select-Object -First 3
```

列出执行程序 -> 找到执行程序CPU值超过100的 -> 依CPU值从大排到小 -> 取出前3个

```
NPM(K)    PM(M)      WS(M)     CPU(s)      Id  SI ProcessName
------    -----      -----     ------      --  -- -----------
    16    15.62      19.82  1,873.73   21472   0 audiodg
   211   772.27     736.77  1,778.84    5096  16 Dropbox
    94   248.50     312.55    709.58   24364  16 chrome
```

练习

- 列出一个字串的属性与方法

```
"a string" | Get-Member
```

```
   TypeName: System.String

Name                 MemberType          Definition
----                 ----------          ----------
Clone                Method              System.Object Clone(), System.Object ICloneable.Clone()
CompareTo            Method              int CompareTo(System.Object value), int CompareTo(string st…
Contains             Method              bool Contains(string value), bool Contains(string value, Sy…
CopyTo               Method              void CopyTo(int sourceIndex, char[] destination, int destin…
EndsWith             Method              bool EndsWith(string value), bool EndsWith(string value, Sy…
EnumerateRunes       Method              System.Text.StringRuneEnumerator EnumerateRunes()
Equals               Method              bool Equals(System.Object obj), bool Equals(string value), …
GetEnumerator        Method              System.CharEnumerator GetEnumerator(), System.Collections.I…
```

练习

- 列出一个字串的属性与方法，并以格式化列表呈现

```
"a string" | Get-Member | Format-List
```

```
TypeName   : System.String
Name       : Clone
MemberType : Method
Definition : System.Object Clone(), System.Object ICloneable.Clone()

TypeName   : System.String
Name       : CompareTo
MemberType : Method
Definition : int CompareTo(System.Object value), int CompareTo(string strB), int
             IComparable.CompareTo(System.Object obj), int IComparable[string].CompareTo(string other)

TypeName   : System.String
Name       : Contains
MemberType : Method
Definition : bool Contains(string value), bool Contains(string value, System.StringComparison
             comparisonType), bool Contains(char value), bool Contains(char value,
             System.StringComparison comparisonType)
```

知识检查

1. 使用帮助系统时，哪个命令或函数对于查找有关命令的详细信息提供的体验最佳?

- ◯ `{your command} --help`
- ◯ `Get-Help {your command}`
- ◯ `help {your command}`

2. 哪一项表述最佳描述了“筛选左侧”原则?

- ◯ `Get-Process | Select-Object Name | Where-Object Name -eq name-of-process`
- ◯ `Get-Process | Where-Object Name -eq name-of-process | Select-Object name-of-process`
- ◯ `Get-Process -Name name-of-process | Select-Object Name`

3. 哪句话最佳描述了从命令查找返回类型?

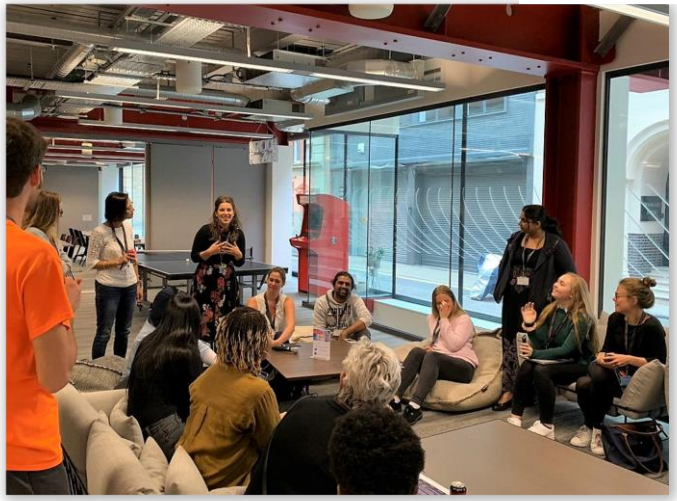
- ◯ `{command} --type`
- ◯ `{command} | Get-Member`
- ◯ `{command} | Get-Type`
- ◯ `{command} Get-Member`

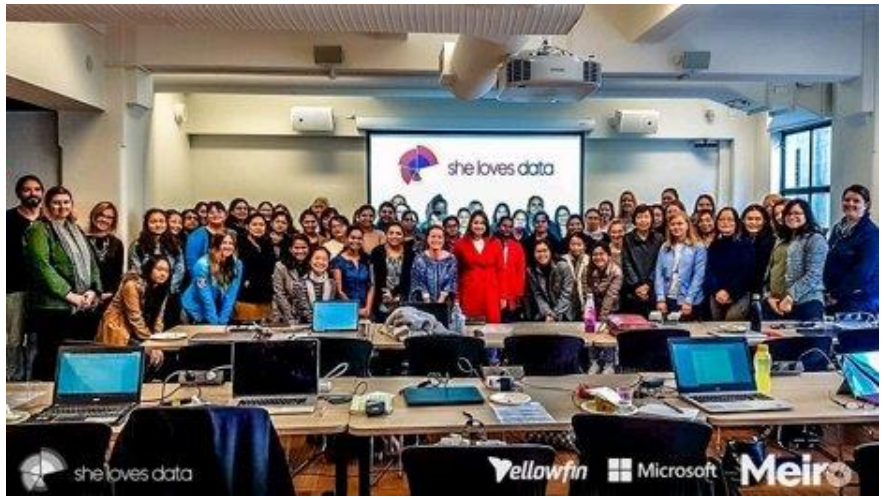
Summary

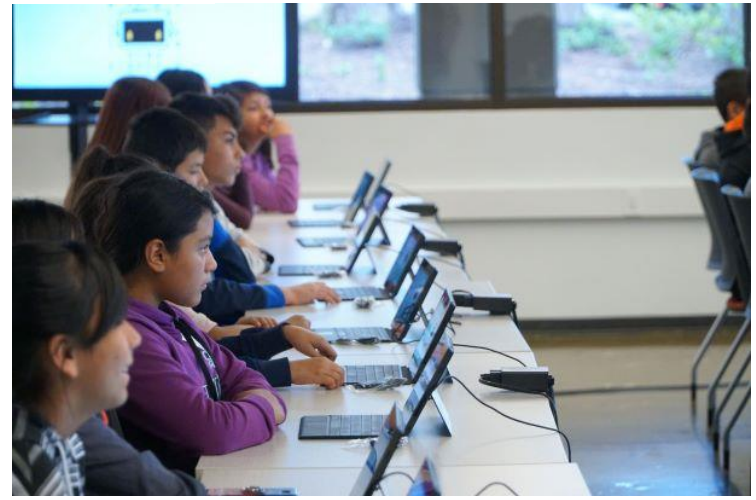
- Cmdlet的结构是由动词+名词所组成
- 善用管线(Pipeline, |)，将回传结果变成另一指令的输入
- Filtering Left, Formatting Right 先筛选、后格式化

Microsoft

Reactor







developer.microsoft.com/reactor/
@MSFTReactor on Twitter

Microsoft

议程结束
感谢聆听

请记得填写课程回馈问卷 (Event ID : XXXXX)
https://aka.ms/Reactor/Survey