


spiceworks
ALL ACCESS

Automate Everything with PowerShell

Jaap Brasser
 @Jaap_Brasser

#AllAccessIT



jaapbrasser.com/about

- Works at Rubrik
- PowerShell Conference EU/Asia
- Dutch PowerShell User Group
- Speaker / Blogger / Tech Enthusiast



Agenda

What is PowerShell

PowerShell Infrastructure

PowerShell Security

PowerShell Cloud

PowerShell Serverless



Why PowerShell ???

P O W E R S H E L L

A wide-angle photograph of a Norwegian fjord. The water is a deep blue, reflecting the sky and the surrounding mountains. On the right, a red and white ferry boat is moving across the water, leaving a white wake. The mountains are steep and rugged, with some snow-capped peaks in the distance. The sky is a clear, vibrant blue with a few wispy white clouds. The overall scene is peaceful and majestic.

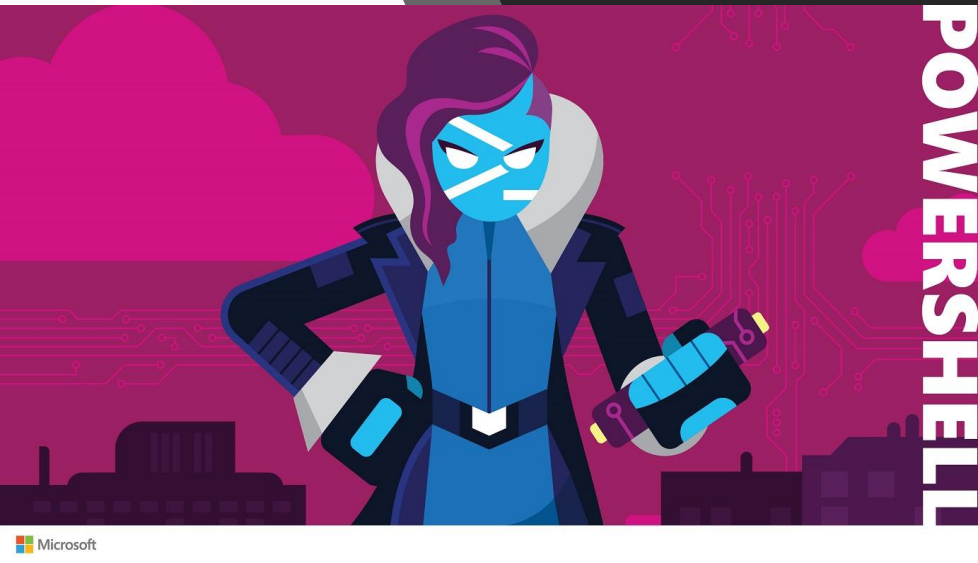
New Start

Worth it?

HOW LONG CAN YOU WORK ON MAKING A ROUTINE TASK MORE EFFICIENT BEFORE YOU'RE SPENDING MORE TIME THAN YOU SAVE?
(ACROSS FIVE YEARS)

		HOW OFTEN YOU DO THE TASK					
		50/DAY	5/DAY	DAILY	WEEKLY	MONTHLY	YEARLY
HOW MUCH TIME YOU SHAVE OFF	1 SECOND	1 DAY	2 HOURS	30 MINUTES	4 MINUTES	1 MINUTE	5 SECONDS
	5 SECONDS	5 DAYS	12 HOURS	2 HOURS	21 MINUTES	5 MINUTES	25 SECONDS
	30 SECONDS	4 WEEKS	3 DAYS	12 HOURS	2 HOURS	30 MINUTES	2 MINUTES
	1 MINUTE	8 WEEKS	6 DAYS	1 DAY	4 HOURS	1 HOUR	5 MINUTES
	5 MINUTES	9 MONTHS	4 WEEKS	6 DAYS	21 HOURS	5 HOURS	25 MINUTES
	30 MINUTES		6 MONTHS	5 WEEKS	5 DAYS	1 DAY	2 HOURS
	1 HOUR		10 MONTHS	2 MONTHS	10 DAYS	2 DAYS	5 HOURS
	6 HOURS				2 MONTHS	2 WEEKS	1 DAY
	1 DAY					8 WEEKS	5 DAYS

What is PowerShell



- Development started in 2001
- First released in 2006
- Was initially codenamed Monad
- It is written: **P**ower**S**hell
- Currently at version 6

Components of PowerShell



Windows PowerShell

Learn about the PowerShell scripting language.



Desired State Configuration

Use PowerShell to manage system and enforce configurations.



Just Enough Administration

Secure management in PowerShell by limiting permissions to only what is needed.



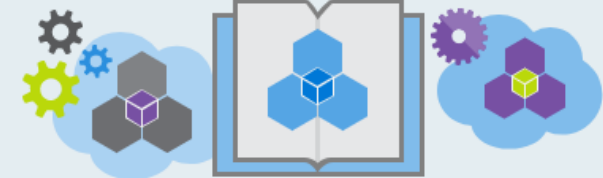
PowerShell Gallery

The central repository for PowerShell scripts and modules.



Azure PowerShell

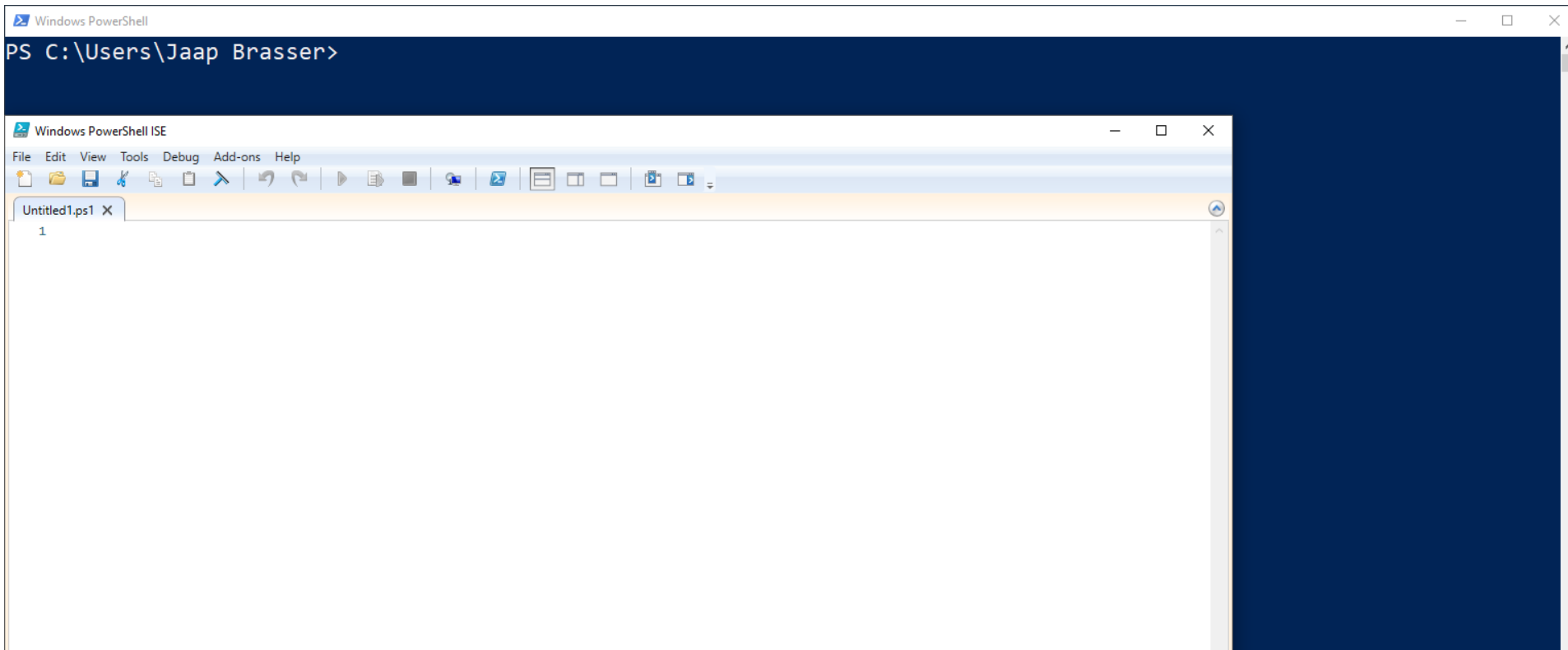
Manage your Azure deployments using PowerShell.



Modules

See the reference documentation for numerous PowerShell modules.

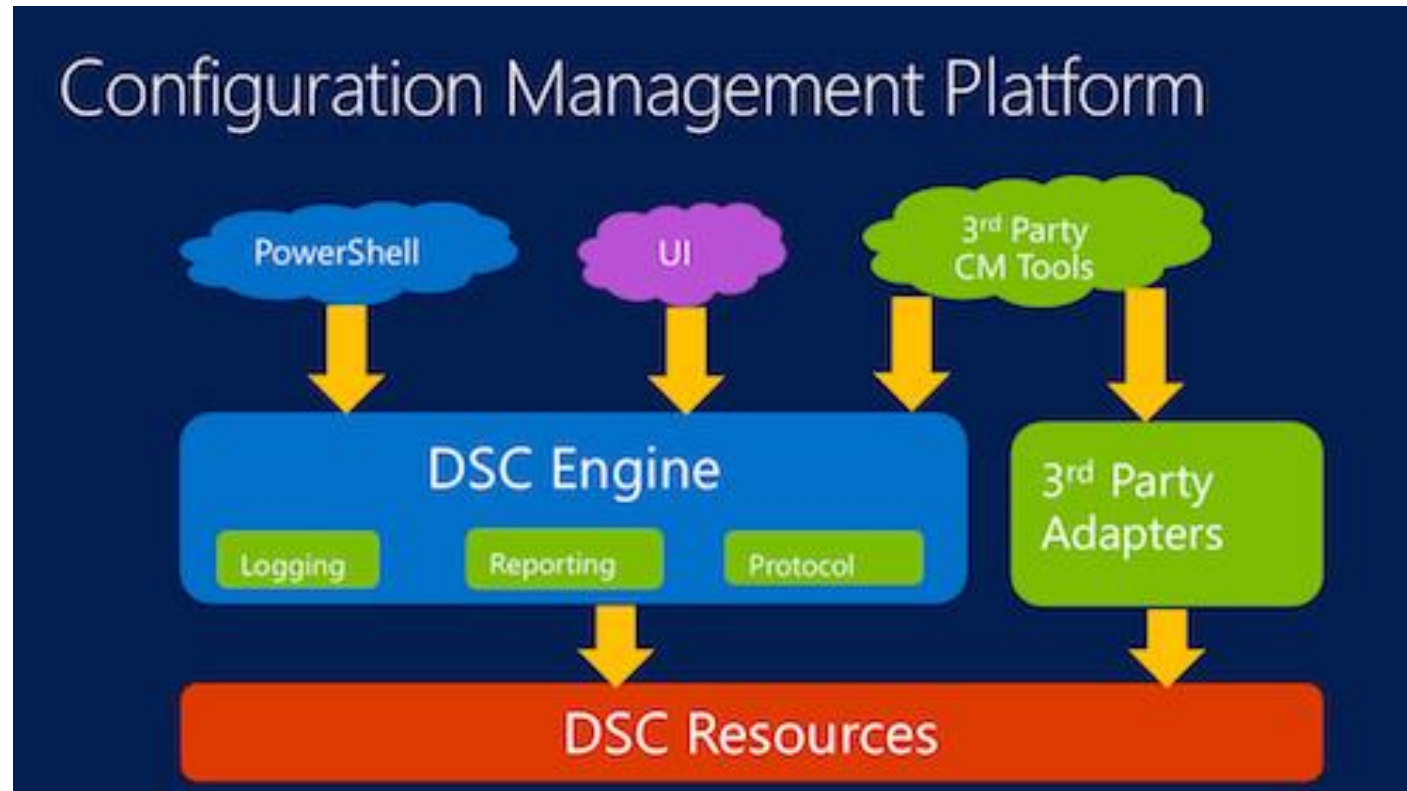
Windows PowerShell



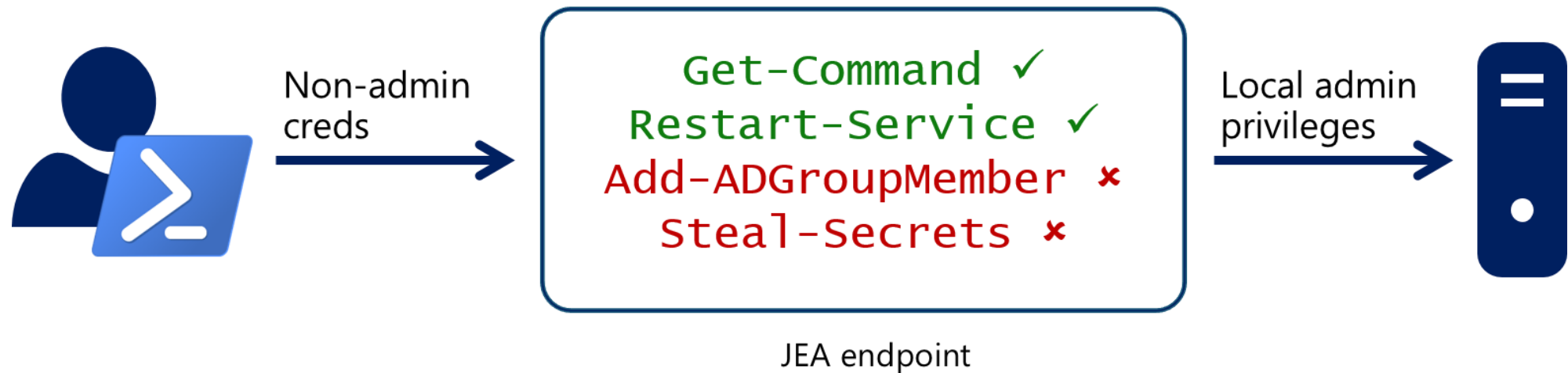
Windows PowerShell versions

PowerShell Version	Release Date	Default Windows Versions	Available Windows Versions
PowerShell 1.0	November 2006	Windows Server 2008 (*)	Windows XP SP2 Windows XP SP3 Windows Server 2003 SP1 Windows Server 2003 SP2 Windows Server 2003 R2 Windows Vista Windows Vista SP2
PowerShell 2.0	October 2009	Windows 7 Windows Server 2008 R2 (**)	Windows XP SP3 Windows Server 2003 SP2 Windows Vista SP1 Windows Vista SP2 Windows Server 2008 SP1 Windows Server 2008 SP2
PowerShell 3.0	September 2012	Windows 8 Windows Server 2012	Windows 7 SP1 Windows Server 2008 SP2 Windows Server 2008 R2 SP1
PowerShell 4.0	October 2013	Windows 8.1 Windows Server 2012 R2	Windows 7 SP1 Windows Server 2008 R2 SP1 Windows Server 2012
PowerShell 5.0	July 2015	Windows 10	Windows 8.1 Windows Server 2012 R2
PowerShell 5.1	July 2016	Windows 10	Windows 8.1 Windows Server 2012 R2

Desired State Configuration



Just Enough Administration (JEA)



PowerShell Gallery



#AllAccessIT

spiceworks
ALL ACCESS

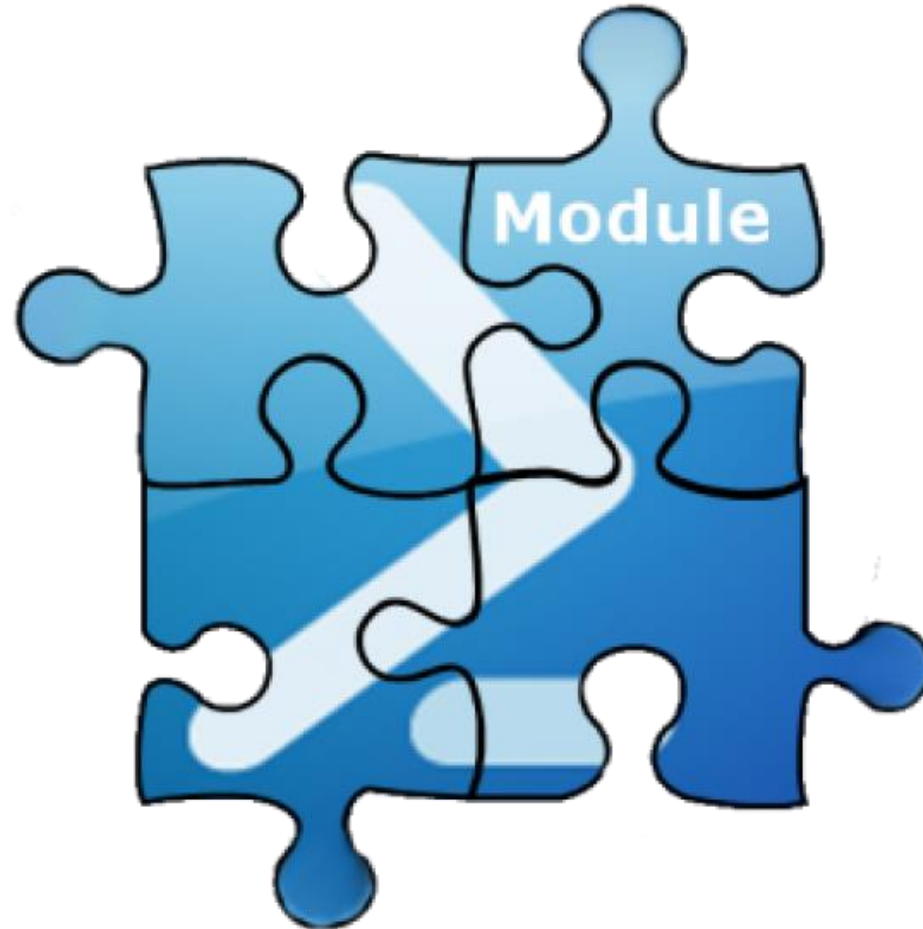
Azure PowerShell



PowerShell



PowerShell Modules



#AllAccessIT

spiceworks
ALL ACCESS



```
PS /> Get-Module -ListAvailable

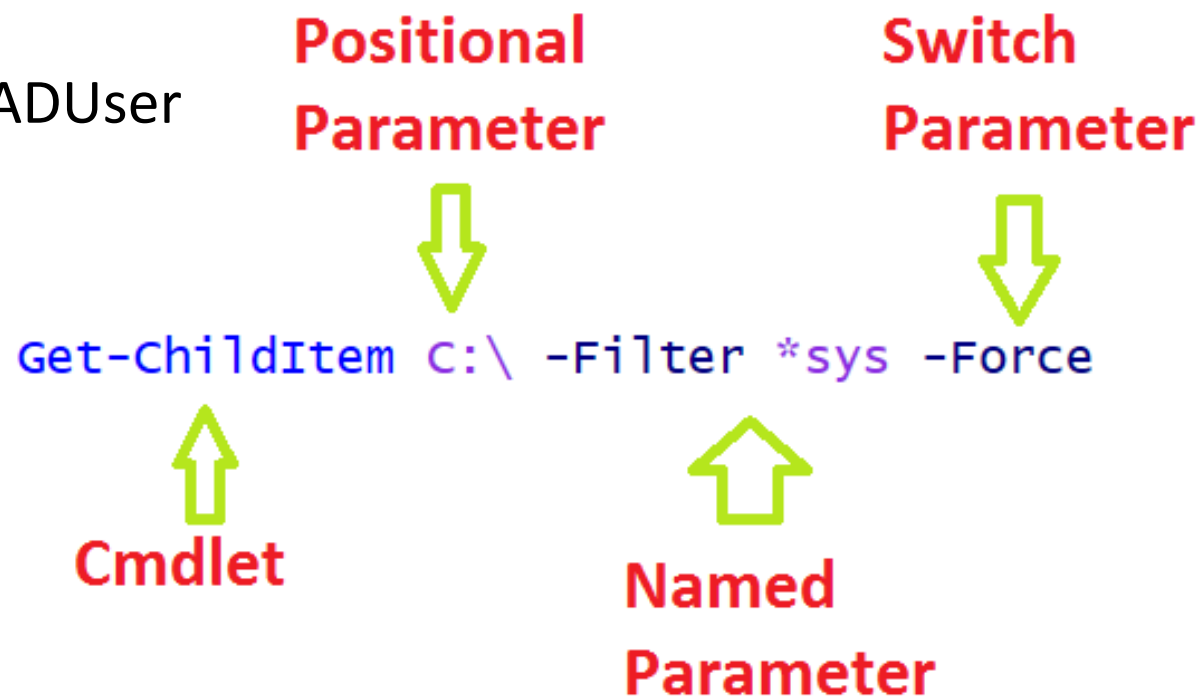
Directory: /opt/microsoft/powershell/6.0.0-beta.4/Modules

ModuleType Version Name ExportedCommands
-----
Script 0.0 Get-DiskSpace
Manifest 1.1.0.0 Microsoft.PowerShell.Archive {Compress-Archive, Expand-Archive}
Manifest 3.0.0.0 Microsoft.PowerShell.Host {Start-Transcript, Stop-Transcript}
Manifest 3.1.0.0 Microsoft.PowerShell.Management {Add-Content, Clear-Content, Clea...
Manifest 3.0.0.0 Microsoft.PowerShell.Security {Get-Credential, Get-ExecutionPol...
Manifest 3.1.0.0 Microsoft.PowerShell.Utility {Format-List, Format-Custom, For...
Script 1.1.4.0 PackageManagement {Find-Package, Get-Package, Get-P...
Script 3.3.9 Pester {Describe, Context, It, Should...}
Script 1.3.3.1 PowerShellGet {Install-Module, Find-Module, Sav...
Script 0.0 PSDesiredStateConfiguration {ThrowError, Get-PSMetaConfigocu...
Script 1.2 PSReadLine {Get-PSReadlineKeyHandler, Set-PS...
```

PowerShell, what else?

PowerShell Language

- Verb-Noun
 - Get-Help, Restart-Computer, Get-ADUser
- Cmdlets, Functions
- Parameters
- Arguments



Demo – PowerShell Basics

#AllAccessIT

spiceworks
ALL ACCESS

Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Jaap Brasser> **Get-Host**

Name	: ConsoleHost
Version	: 5.1.17134.137
InstanceId	: 5f155a42-2c53-4200-b1ac-5b67c3cbb388
UI	: System.Management.Automation.Internal.Host.InternalHostUserInterface
CurrentCulture	: en-US
CurrentUICulture	: en-US
PrivateData	: Microsoft.PowerShell.ConsoleHost+ConsoleColorProxy
DebuggerEnabled	: True
IsRunspacePushed	: False
Runspace	: System.Management.Automation.Runspace.LocalRunspace

PS C:\Users\Jaap Brasser> █



Version Information

CommandType	Name	Version	Source
Alias	Add-AdlAnalyticsDataSource	4.2.3	AzureRM.DataLakeAnalytics
Alias	Add-AdlAnalyticsFirewallRule	4.2.3	AzureRM.DataLakeAnalytics
Alias	Add-AdlStoreFirewallRule	5.2.0	AzureRM.DataLakeStore
Alias	Add-AdlStoreItemContent	5.2.0	AzureRM.DataLakeStore
Alias	Add-AdlStoreTrustedIdProvider	5.2.0	AzureRM.DataLakeStore
Alias	Add-AzureHDInsightConfigValues	5.1.2	Azure
Alias	Add-AzureHDInsightMetastore	5.1.2	Azure
Alias	Add-AzureHDInsightStorage	5.1.2	Azure
Alias	Add-AzureRmAccount	4.6.0	AzureRM.Profile
Alias	Add-AzureRmIoTHubEHCG	3.1.2	AzureRM.IoTHub
Alias	Add-ProvisionedAppxPackage	3.0	Dism
Alias	Add-ProvisioningPackage	3.0	Provisioning
Alias	Add-TrustedProvisioningCertificate	3.0	Provisioning
Alias	Add-WAPackEnvironment	5.1.2	Azure
Alias	Apply-WindowsUnattend	3.0	Dism
Alias	Begin-WebCommitDelay	1.0.0.0	WebAdministration
Alias	Confirm-SSLegacyVolumeContainerStatus	5.1.2	Azure
Alias	Disable-AzureRmHDInsightOMS	4.1.2	AzureRM.HDInsight
Alias	Disable-AzureStorageSoftDelete	4.2.1	Azure.Storage
Alias	Disable-PhysicalDiskIndication	2.0.0.0	Storage
Alias	Disable-StorageDiagnosticLog	2.0.0.0	Storage
Alias	Disable-WAPackWebsiteApplicationDiagnostic	5.1.2	Azure
Alias	Edit-ASRRRecoveryPlan	0.2.4	AzureRM.RecoveryServices.SiteRecovery
Alias	Edit-ASRRP	0.2.4	AzureRM.RecoveryServices.SiteRecovery
Alias	Enable-AdlStoreKeyVault	5.2.0	AzureRM.DataLakeStore
-- More --			

Available
commands


```
Windows PowerShell
PS C:\Users\Jaap Brasser> Get-Command * | Group-Object -Property CommandType

Count Name                                     Group
-----
580 Alias                                     {%, ?, ac, Add-AdlAnalyticsDataSource...}
1260 Function                                {A:, Add-BCDataCacheExtension, Add-BitLockerKeyProtector, Add-DaDatabaseIndex...}
3613 Cmdlet                                  {Add-AppvClientConnectionGroup, Add-AppvClientPackage, Add-AppvPublishingServer,...}
1 ExternalScript                             {Get-RemoteProgram.ps1}
725 Application                              {AgentService.exe, aitstatic.exe, alg.exe, AppHostRegistrationVerifier.exe...}


PS C:\Users\Jaap Brasser>
```

Commands - Grouped

```
PS C:\Users\Jaap Brasser> Get-Command * | Group-Object -Property CommandType | Sort Count
```

Count	Name	Group
-----	-----	-----
1	ExternalScript	{Get-RemoteProgram.ps1}
580	Alias	{%, ?, ac, Add-AdlAnalyticsDataSource...}
725	Application	{AgentService.exe, aitstatic.exe, alg.exe, AppHostRegistrationVerifier.exe...}
1260	Function	{A:, Add-BCDataCacheExtension, Add-BitLockerKeyProtector, Add-DaDatabaseIndex...}
3613	Cmdlet	{Add-AppvClientConnectionGroup, Add-AppvClientPackage, Add-AppvPublishingServer,...}

```
PS C:\Users\Jaap Brasser> █
```



Commands –
Grouped & Sorted

```
PS C:\Users\Jaap Brasser> Get-Help Get-WinEvent|more
```

NAME

Get-WinEvent

SYNOPSIS

Gets events from event logs and event tracing log files on local and remote computers.

SYNTAX

```
Get-WinEvent [[-LogName] <String[]>] [-ComputerName <String>] [-Credential <PSCredential>] [-FilterXPath  
<String>] [-Force] [-MaxEvents <Int64>] [-Oldest] [<CommonParameters>]
```

```
Get-WinEvent [-ListProvider] <String[]> [-ComputerName <String>] [-Credential <PSCredential>]  
[<CommonParameters>]
```

```
Get-WinEvent [-ProviderName] <String[]> [-ComputerName <String>] [-Credential <PSCredential>] [-FilterXPath  
<String>] [-Force] [-MaxEvents <Int64>] [-Oldest] [<CommonParameters>]
```

```
Get-WinEvent [-ListLog] <String[]> [-ComputerName <String>] [-Credential <PSCredential>] [-Force]  
[<CommonParameters>]
```

```
Get-WinEvent [-FilterHashtable] <Hashtable[]> [-ComputerName <String>] [-Credential <PSCredential>] [-Force]  
[-MaxEvents <Int64>] [-Oldest] [<CommonParameters>]
```

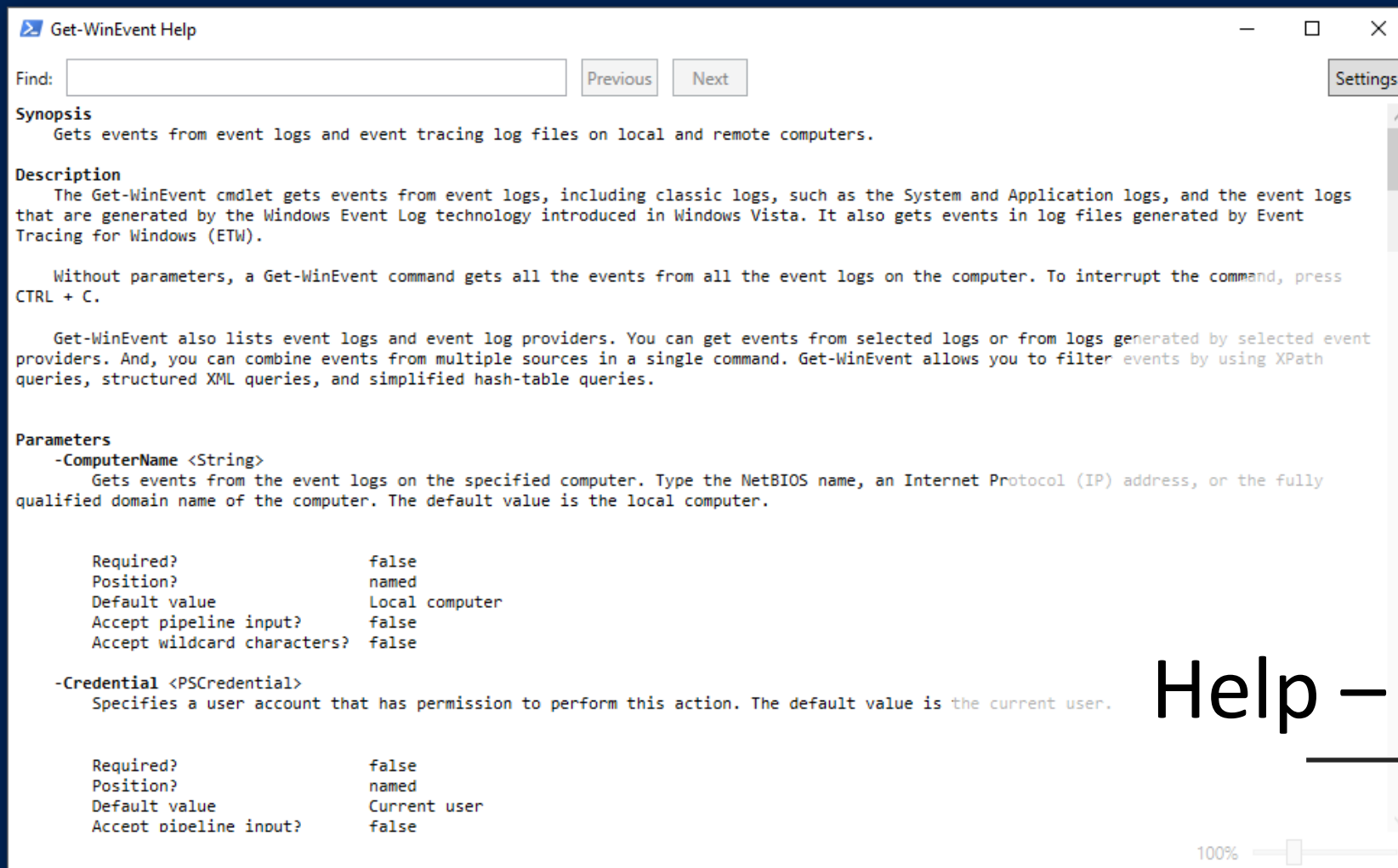
```
Get-WinEvent [-FilterXml] <XmlDocument> [-ComputerName <String>] [-Credential <PSCredential>] [-MaxEvents  
<Int64>] [-Oldest] [<CommonParameters>]
```

```
Get-WinEvent [-Path] <String[]> [-Credential <PSCredential>] [-FilterXPath <String>] [-MaxEvents <Int64>]
```

Help

```
PS C:\Users\Jaap Brasser> Get-Help Get-WinEvent -ShowWindow
```

```
PS C:\Users\Jaap Brasser>
```



Help – in GUI

```
PS C:\Users\Jaap Brasser> Show-Command Get-WinEvent
```

Get-WinEvent

Parameters for "Get-WinEvent":

ListLogSet	ListProviderSet	XmlQuerySet
GetLogSet	FileSet	GetProviderSet
		HashQuerySet

ComputerName:

Credential:

FilterXPath:

☐ Force

LogName:

MaxEvents:

☐ Oldest

Common Parameters

Run Copy Cancel

Show-Command


```
PS C:\Users\Jaap Brasser> Get-Process | more
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
-----	-----	-----	-----	-----	--	--	-----
241	15	6092	22980	0.52	2340	1	ApplicationFrameHost
157	8	1988	7420		13496	0	AppVShNotify
166	9	2292	9040	0.06	13508	1	AppVShNotify
206	12	9136	16136	5.63	16096	0	audiodg
391	11	2120	8316	0.02	888	1	chrome
286	23	25576	35812	0.34	1548	1	chrome
291	21	20424	31524	0.34	1968	1	chrome
142	11	1948	8880	0.03	2704	1	chrome
789	49	289324	280740	62.78	2976	1	chrome
281	21	19696	29748	0.22	3684	1	chrome
381	27	35596	52616	1.13	4900	1	chrome
320	28	51100	72652	5.48	5048	1	chrome
320	54	135256	157904	13.70	5748	1	chrome
368	28	35140	51216	1.47	5852	1	chrome
276	18	12876	21128	0.08	7080	1	chrome
338	50	121848	148244	63.14	7128	1	chrome
286	21	22032	33912	0.28	7188	1	chrome
314	22	22600	36392	0.23	8136	1	chrome
289	21	19532	29716	0.23	8308	1	chrome
289	21	19848	29972	0.22	8316	1	chrome
338	29	48752	69464	3.30	8532	1	chrome
302	26	40156	52620	0.73	8740	1	chrome
289	21	19672	29652	0.28	8948	1	chrome
309	27	46344	58244	1.11	9052	1	chrome
355	27	41440	57432	0.92	9124	1	chrome

Get-Process

```
PS C:\Users\Jaap Brasser> Get-Process | Out-GridView
```

```
PS C:\Users\Jaap Brasser> 
```

Get-Process Out-GridView							
Filter							
+ Add criteria ▼							
Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
241	15	6092	22980	0.52	2,340	1	ApplicationFrameHost
157	8	1988	7420		13,...	0	AppVShNotify
166	9	2292	9040	0.06	13,...	1	AppVShNotify
216	12	9868	16272	7.13	16,...	0	audiodg
391	11	2120	8316	0.02	888	1	chrome
286	23	25576	35812	0.34	1,548	1	chrome
291	21	20424	31512	0.34	1,968	1	chrome
142	11	1948	8880	0.03	2,704	1	chrome
789	49	289...	269...	62.78	2,976	1	chrome
281	21	19696	29748	0.22	3,684	1	chrome
381	27	35596	52632	1.13	4,900	1	chrome
320	28	51100	71992	5.48	5,048	1	chrome
317	53	135...	157...	13.72	5,748	1	chrome
368	28	35140	51216	1.47	5,852	1	chrome
276	18	12876	21136	0.08	7,080	1	chrome
338	50	121...	148...	63.17	7,128	1	chrome
286	21	22032	33912	0.28	7,188	1	chrome
314	22	22600	36380	0.23	8,136	1	chrome
289	21	19532	29624	0.23	8,308	1	chrome
289	21	19848	29852	0.22	8,316	1	chrome
338	29	48752	69484	3.30	8,532	1	chrome
302	26	40156	52680	0.73	8,740	1	chrome
289	21	19672	29640	0.28	8,948	1	chrome
309	27	46344	58244	1.11	9,052	1	chrome
355	27	41440	57580	0.92	9,124	1	chrome
291	21	19672	29932	0.41	10,...	1	chrome
373	37	68364	87584	7.09	10,...	1	chrome
3,220	86	183...	237...	163.09	12,...	1	chrome
370	28	33856	52068	1.63	12,...	1	chrome
339	50	127...	141...	6.30	12,...	1	chrome
288	22	21936	34696	0.41	13,...	1	chrome

Get-Process | Out-GridView

```
PS C:\Users\Jaap Brasser> Get-Process | Out-GridView -PassThru | kill -WhatIf
```

Get-Process | Out-GridView -PassThru | kill -WhatIf

powerpnt

+ Add criteria ▼

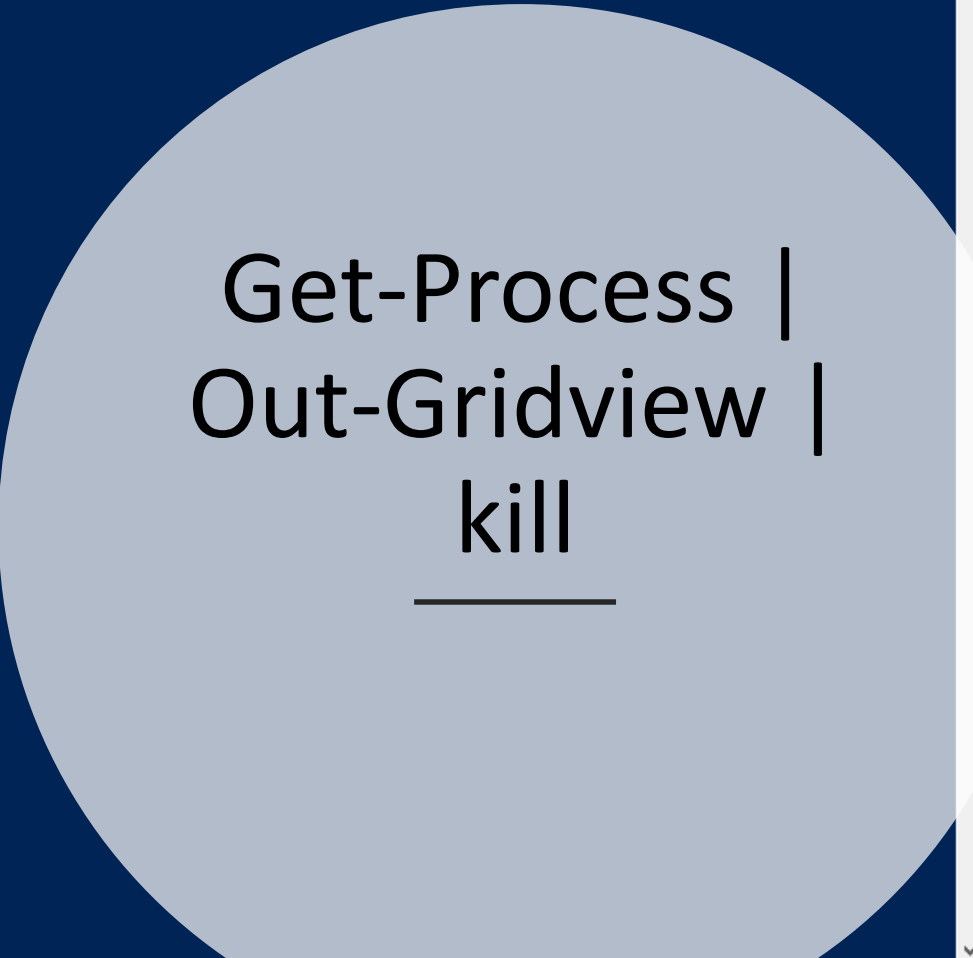
Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
1,922	95	257...	324...	536.20	2,240	1	POWERPNT

Get-Process |
Out-GridView |
kill

OK

Cancel

```
PS C:\Users\Jaap Brasser> Get-Process | Out-GridView
PS C:\Users\Jaap Brasser> Get-Process | Out-GridView -PassThru | kill -WhatIf
What if: Performing the operation "Stop-Process" on target "POWERPNT (2240)".
PS C:\Users\Jaap Brasser> █
```



Get-Process |
Out-GridView |
kill

Windows PowerShell

PS C:\Users\Jaap Brasser> Get-PSDrive

Name	Used (GB)	Free (GB)	Provider	Root	CurrentLocation
----	-----	-----	-----	----	-----
Alias			Alias		
C	221.77	16.17	FileSystem	C:\	Users\Jaap Brasser
Cert			Certificate	\	
Env			Environment		
Function			Function		
HKCU			Registry	HKEY_CURRENT_USER	
HKLM			Registry	HKEY_LOCAL_MACHINE	
Variable			Variable		
WSMan			WSMan		

PS C:\Users\Jaap Brasser>

PowerShell
Drives


```
PS C:\Users\Jaap Brasser> [math]::pow(2,10)  
1024  
PS C:\Users\Jaap Brasser> █
```



.Net methods

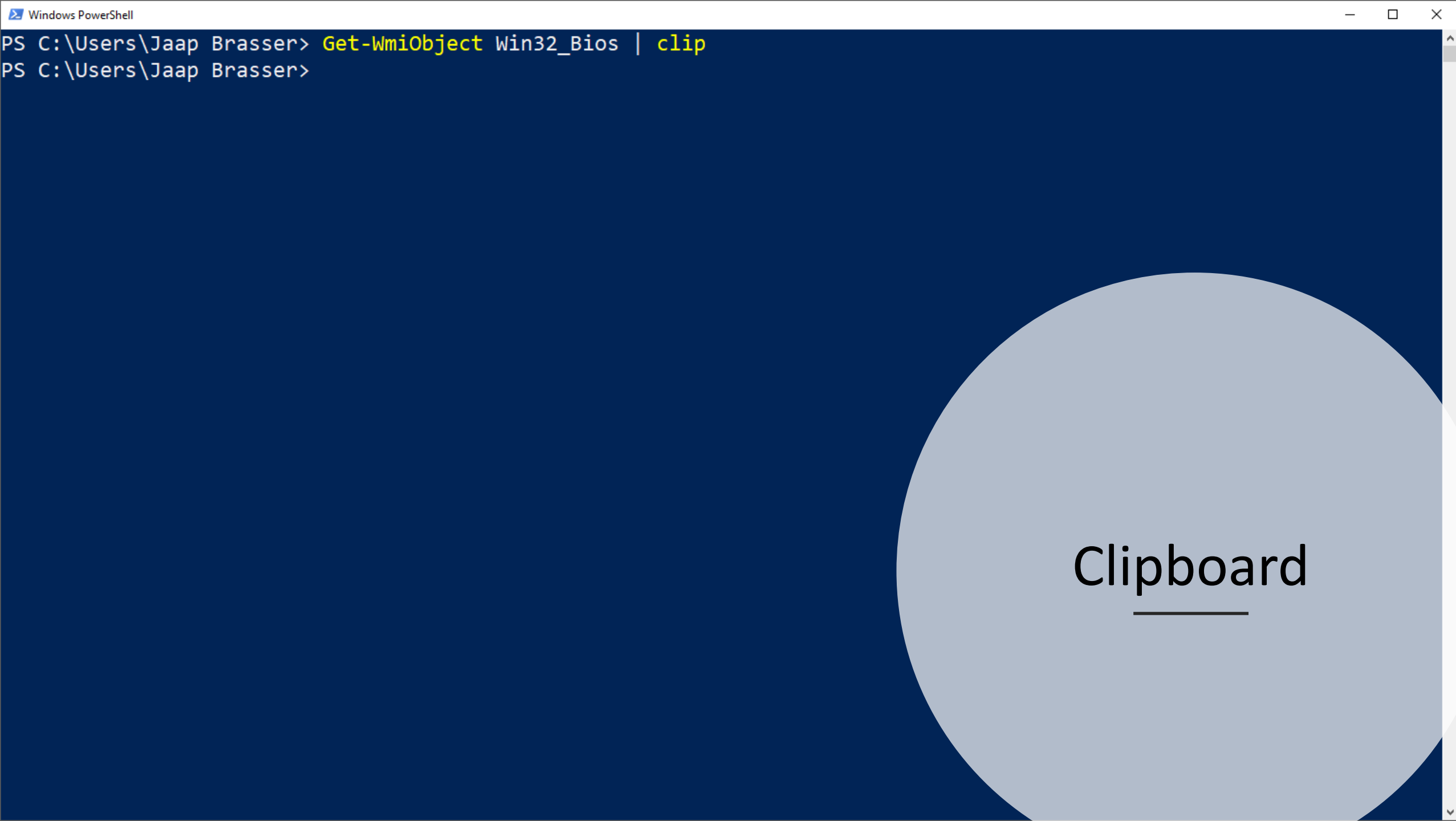
```
PS C:\Users\Jaap Brasser> Get-WmiObject Win32_Bios
```

```
SMBIOSBIOSVersion : XMAKB5R0P0200  
Manufacturer      : INSYDE Corp.  
Name               : InsydeH2O Version 05.12.09XMAKB5R0P0200  
SerialNumber       : 16771/00002140  
Version            : XMCC - 0
```

```
PS C:\Users\Jaap Brasser>
```



Wmi Query



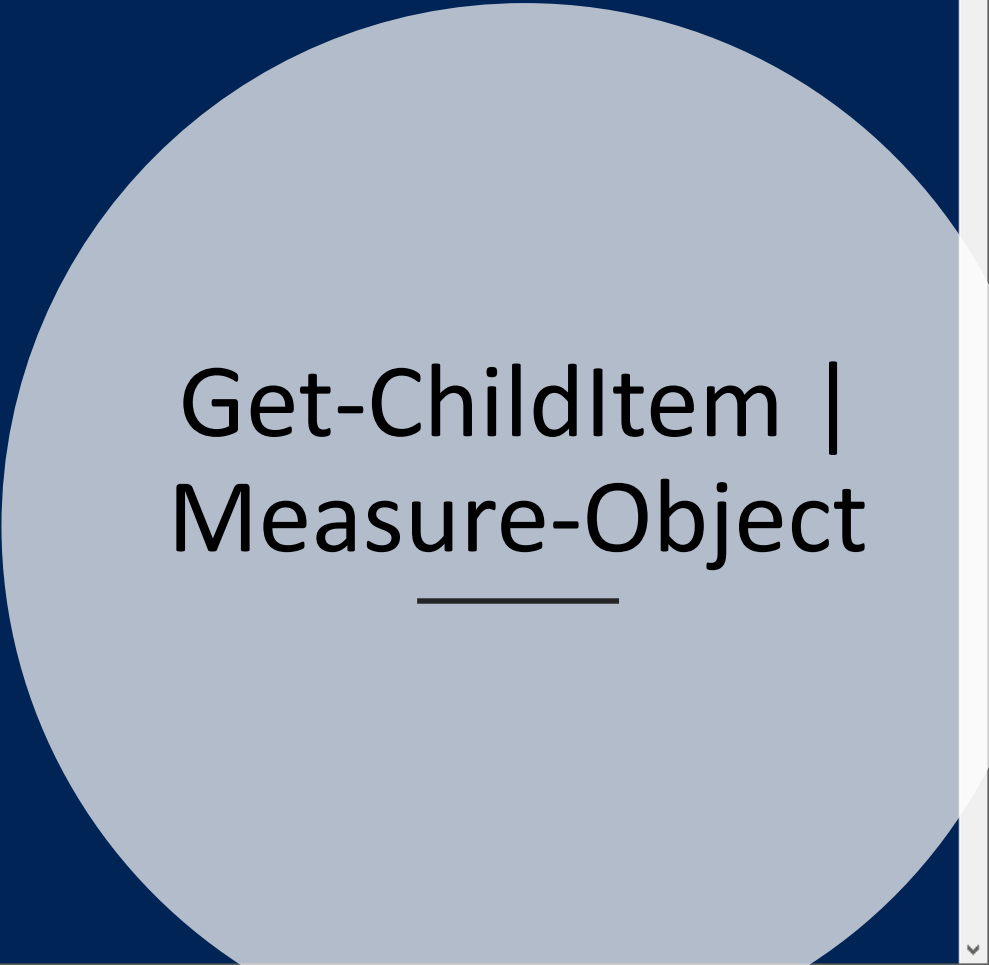
```
PS C:\Users\Jaap Brasser> Get-WmiObject Win32_Bios | clip
PS C:\Users\Jaap Brasser>
```

Clipboard

```
PS C:\Users\Jaap Brasser> Get-ChildItem *docx -Recurse -EA 0 | Measure-Object
```


```
Count      : 519  
Average    :  
Sum        :  
Maximum    :  
Minimum    :  
Property   :
```

```
PS C:\Users\Jaap Brasser> █
```



Get-ChildItem |
Measure-Object

```
PS C:\Users\Jaap Brasser\downloads> Get-ChildItem *exe | Set-Clipboard  
PS C:\Users\Jaap Brasser\downloads>
```



Get-ChildItem |
Set-Clipboard



Demo Summary

Get available commands

Get-Help

Show-Commands (GUI)

Manipulate output

Measure/Count and Group output

Writing scripts

No Aliases

Write help

No one-liners

Simple Code

Functions

Ask for help

powertheshell.co

Home of ISESteroids for Power

Windows PowerShell ISE

Loading...



Visual
Studio



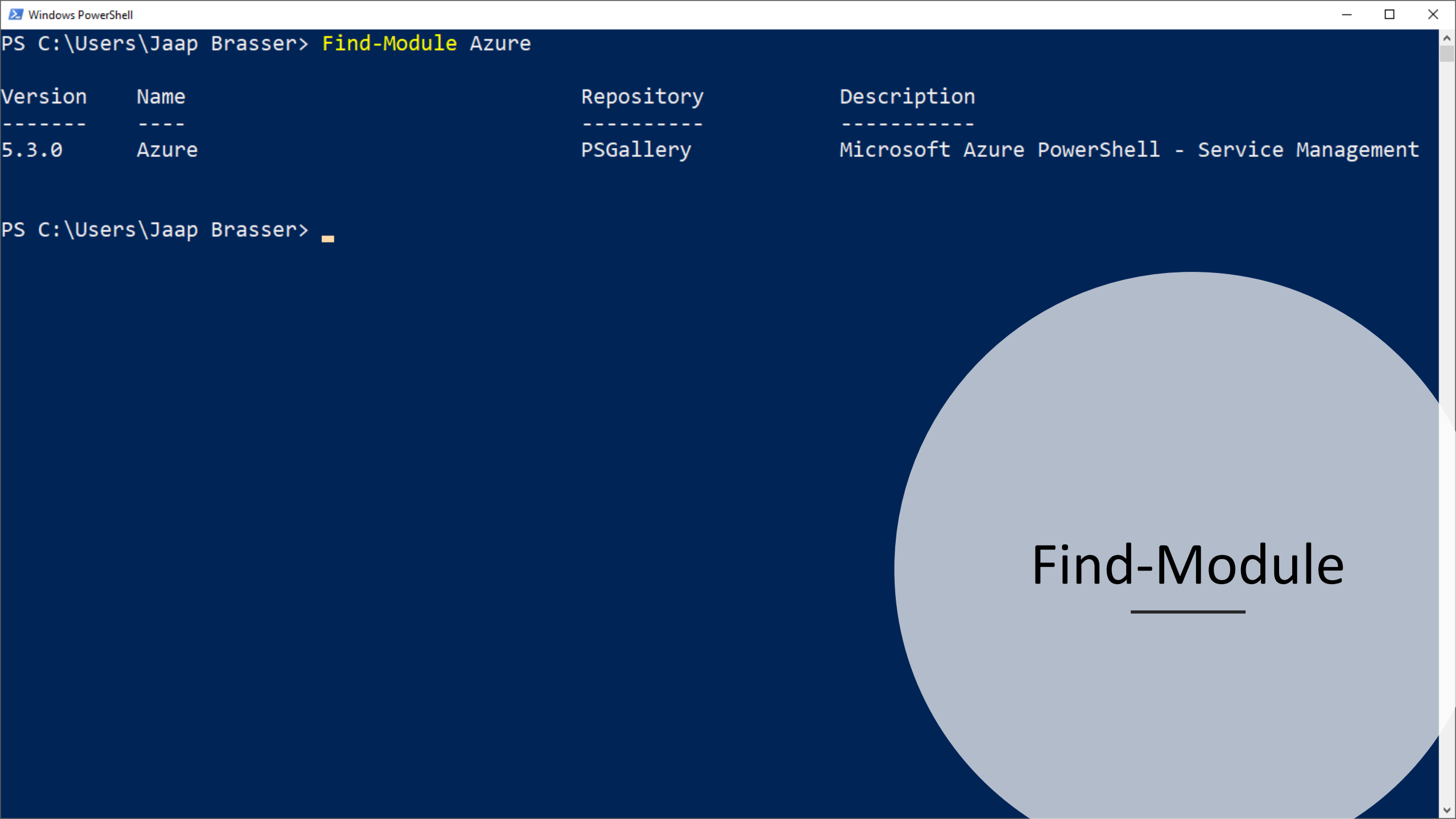
VS Code

Developing
PowerShell scripts

Demo – PowerShell Infra

#AllAccessIT

spiceworks
ALL ACCESS



PS C:\Users\Jaap Brasser> Find-Module Azure

Version	Name	Repository	Description
-----	----	-----	-----
5.3.0	Azure	PSGallery	Microsoft Azure PowerShell - Service Management

PS C:\Users\Jaap Brasser>

Find-Module

```
Windows PowerShell
PS C:\Users\Jaap Brasser> Find-Module Connect-Mstsc | Install-Module -Verbose -Force -Scope CurrentUser
VERBOSE: Repository details, Name = 'PSGallery', Location = 'https://www.powershellgallery.com/api/v2/'; IsTrusted = 'True'; IsRegistered = 'True'.
VERBOSE: Repository details, Name = 'PSGallery', Location = 'https://www.powershellgallery.com/api/v2/'; IsTrusted = 'True'; IsRegistered = 'True'.
VERBOSE: Performing the operation "Install-Module" on target "Version '1.2.5' of module 'Connect-Mstsc'".
VERBOSE: Repository details, Name = 'PSGallery', Location = 'https://www.powershellgallery.com/api/v2/'; IsTrusted = 'True'; IsRegistered = 'True'.
VERBOSE: Using the provider 'PowerShellGet' for searching packages.
VERBOSE: Using the specified source names : 'PSGallery'.
VERBOSE: Getting the provider object for the PackageManagement Provider 'NuGet'.
VERBOSE: The specified Location is 'https://www.powershellgallery.com/api/v2/' and PackageManagementProvider is 'NuGet'.
VERBOSE: Searching repository 'https://www.powershellgallery.com/api/v2/FindPackagesById()?id='Connect-Mstsc'' for '''.
VERBOSE: Total package yield:'1' for the specified package 'Connect-Mstsc'.
VERBOSE: Performing the operation "Install-Module" on target "Version '1.2.5' of module 'Connect-Mstsc'".
VERBOSE: The installation scope is specified to be 'CurrentUser'.
VERBOSE: The specified module will be installed in 'C:\Users\Jaap Brasser\Documents\WindowsPowerShell\Modules'.
VERBOSE: The specified Location is 'NuGet' and PackageManagementProvider is 'NuGet'.
VERBOSE: Downloading module 'Connect-Mstsc' with version '1.2.5' from the repository 'https://www.powershellgallery.com/api/v2/'.
VERBOSE: Searching repository 'https://www.powershellgallery.com/api/v2/FindPackagesById()?id='Connect-Mstsc'' for '''.
VERBOSE: InstallPackage' - name='Connect-Mstsc', version='1.2.5',destination='C:\Users\Jaap Brasser\AppData\Local\Temp\1991257908'
VERBOSE: DownloadPackage' - name='Connect-Mstsc', version='1.2.5',destination='C:\Users\Jaap Brasser\AppData\Local\Temp\1991257908\Connect-Mstsc\Connect-Mstsc.nupkg', uri='https://www.powershellgallery.com/api/v2/package/Connect-Mstsc/1.2.5'
```

Install-Module


```
PS C:\WINDOWS\system32> Get-RemoteProgram | Where-Object ProgramName -match 'Microsoft'
```

ProgramName	ComputerName
Microsoft Azure Compute Emulator - v2.9.5.3	??
Microsoft Office 365 ProPlus - en-us	??
Microsoft Office 365 ProPlus - nl-nl	??
Microsoft Azure Authoring Tools - v2.9.5.3	??
Microsoft SQL Server 2012 Native Client	??
Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219	??
Microsoft .NET Core Host FX Resolver - 2.0.7 (x64)	??
Microsoft Visual C++ 2012 x64 Additional Runtime - 11.0.61030	??
Microsoft Azure PowerShell - April 2018	??
Microsoft .NET Core Host - 2.0.7 (x64)	??
Microsoft .NET Core Runtime - 2.0.7 (x64)	??
Microsoft Visual Studio Installer	??
Microsoft Visual Studio Team Foundation Server 2017 RC Office Integration Language Pack (x64) - ENU	??
Microsoft .NET Core Host - 2.0.6 (x64)	??
Microsoft Web Deploy 4.0	??
Microsoft .NET Core SDK - 2.1.201 (x64)	??
Microsoft SQL Server 2016 LocalDB	??
Microsoft SQL Server 2012 Command Line Utilities	??
Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005	??
Microsoft ASP.NET Core 2.0.8 Runtime Package Store (x64)	??
Microsoft .NET Core SDK - 2.1.104 (x64)	??
Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005	??
Microsoft .NET Core Host FX Resolver - 2.0.6 (x64)	??
Microsoft Visual C++ 2017 x64 Minimum Runtime - 14.11.25325	??

Get-RemoteProgram


```
PS C:\WINDOWS\system32> Get-Counter -Counter "\Processor(_Total)\% Processor Time" -Continuous | Select -Exp CounterSamples
```

Path	InstanceName	CookedValue
-----	-----	-----
\\.\processor(_total)\% processor time _total		3.59148386134951
\\.\processor(_total)\% processor time _total		3.15483062183091
\\.\processor(_total)\% processor time _total		2.08138590447368
\\.\processor(_total)\% processor time _total		1.87270258536125
\\.\processor(_total)\% processor time _total		1.86304658452239
\\.\processor(_total)\% processor time _total		2.92538227953394
\\.\processor(_total)\% processor time _total		4.22625976408737
\\.\processor(_total)\% processor time _total		2.16541541098825
\\.\processor(_total)\% processor time _total		3.01727243308694
\\.\processor(_total)\% processor time _total		3.88363838379641
\\.\processor(_total)\% processor time _total		4.26516808889974

Get-Counter

```
PS C:\WINDOWS\system32> $Cred = Import-CliXml -Path C:\Temp\Dictator_Cred.xml
PS C:\WINDOWS\system32> Enter-Pssession -ComputerName 127.0.0.1 -Credential $Cred
[127.0.0.1]: PS C:\Users\Dictator\Documents> whoami
??\dictator
[127.0.0.1]: PS C:\Users\Dictator\Documents> exit
PS C:\WINDOWS\system32> whoami
??\jaap brasser
PS C:\WINDOWS\system32> █
```



Enter-PSSession

```
PS C:\WINDOWS\system32> Get-Content -Path C:\Temp\Dictator_Cred.xml -Tail 4
    <SS N="Password">01000000d08c9ddf0115d1118c7a00c04fc297eb010000003ef726f1ae993b448cceed271ae2b38500000000
020000000000106600000001000020000000e1a078b372affc21f1e090416accd1560d8efd0d3ebc9db038b7ded41c879469000000000e8
000000002000020000000075e5b64257f82e0978c64d2f6a7574ba20acabc9ec0c6ddd9155d6b3a3f8e12a200000006c219db1bd44ddb25
f7d0344f1f4501a42f2e080111b6f33ae6f5456e3767f74000000d0d818d93f2fcc6f90b86d956b365d8e8fe1d3a560a660052af3c7062
72a9ebd21414ca76cac289247f8c581db9b00a3f04664684532097a5978ca55a8fc89db</SS>
    </Props>
  </Obj>
</Objs>
PS C:\WINDOWS\system32>
```



Secure String

```
PS C:\WINDOWS\system32> Invoke-Command -ComputerName 127.0.0.1 -Credential $Cred {$PSVersionTable}
```

Name	Value
-----	-----
PSRemotingProtocolVersion	2.3
BuildVersion	10.0.17134.137
PSVersion	5.1.17134.137
PSCompatibleVersions	{1.0, 2.0, 3.0, 4.0...}
PSEdition	Desktop
CLRVersion	4.0.30319.42000
WSManStackVersion	3.0
SerializationVersion	1.1.0.1

```
PS C:\WINDOWS\system32> █
```

Invoke-Command



Demo Summary

Find and Install modules

Connect to a remote system

Store passwords securely

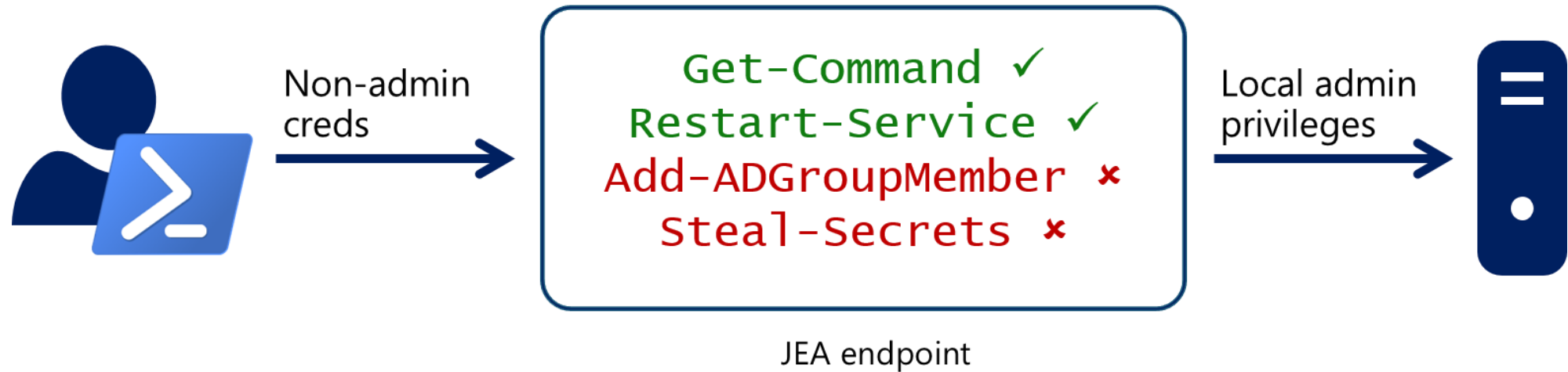
PowerShell Remoting



#AllAccessIT

spiceworks
ALL ACCESS

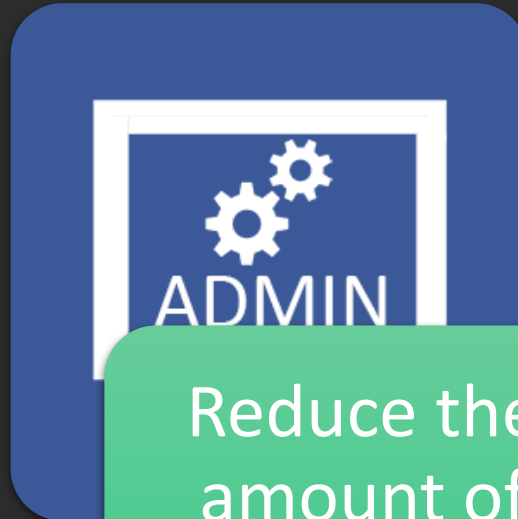
Just Enough Administration



Reasons for JEA



Secure
PowerShell
Access



Reduce the
amount of
people that
can do
„everything“



See what
users do on
the system

Demo – PowerShell Security

#AllAccessIT

spiceworks
ALL ACCESS

```
PS C:\Users\Jaap Brasser> Start-Transcript -Path C:\Temp\PowerShell.log
Transcript started, output file is C:\Temp\PowerShell.log
PS C:\Users\Jaap Brasser> 'This is logged'
This is logged
PS C:\Users\Jaap Brasser> Invoke-Item C:\Temp\PowerShell.log
PS C:\Users\Jaap Brasser>
```

```
PowerShell.log - Notepad
File Edit Format View Help
*****
Windows PowerShell transcript start
Start time: 20180628124918
Username: \Jaap Brasser
RunAs User: \Jaap Brasser
Configuration Name:
Machine: (Microsoft Windows NT 10.0.17134.0)
Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Process ID: 12920
PSVersion: 5.1.17134.137
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.137
BuildVersion: 10.0.17134.137
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
*****
Transcript started, output file is C:\Temp\PowerShell.log
PS C:\Users\Jaap Brasser> 'This is logged'|
This is logged
PS C:\Users\Jaap Brasser> Invoke-Item C:\Temp\PowerShell.log
```

Transcription Logging

```
PS C:\Users\Jaap Brasser> Get-PSReadlineOption | Select-Object HistorySavePath
```

```
HistorySavePath
```

```
-----
```

```
C:\Users\Jaap Brasser\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
```

```
PS C:\Users\Jaap Brasser>
```



Console Logging

Event Log

Event Viewer

File Action View Help

← → ↻ ?

OneBackup

OneX

OOBE-Machine-DUI

OtpCredentialProvider

PackageStateRoaming

ParentalControls

Partition

PerceptionRuntime

PerceptionSensorDataSer

PersistentMemory-INvdir

PersistentMemory-Nvdir

PersistentMemory-Nvdir

PersistentMemory-Pmem

PersistentMemory-ScmB

PersistentMemory-Virtua

Policy-based QoS

PowerShell

Admin

Operational

PowerShell-DesiredStateC

PrimaryNetworkIcon

PrintBRM

PrintService

PriResources-Deploymen

Program-Compatibility-A

Provisioning-Diagnostics

Proximity-Common

PushNotifications-Platfor

ReadyBoost

ReadyBoostDriver

ReFS

RemoteApp and Desktop

RemoteAssistance

RemoteDesktopServices-I

RemoteDesktopServices-I

RemoteDesktopServices-I

Operational Number of events: 5,835

Level	Date and Time	Source	Event ID	Task Category
Warning	6/28/2018 11:45:35 AM	PowerShell (Micr...	4104	Execute a Remote ...
Warning	6/28/2018 11:45:35 AM	PowerShell (Micr...	4104	Execute a Remote ...
Information	6/28/2018 11:45:32 AM	PowerShell (Micr...	4103	Executing Pipeline
Information	6/28/2018 11:45:32 AM	PowerShell (Micr...	4103	Executing Pipeline
Warning	6/28/2018 11:45:32 AM	PowerShell (Micr...	4104	Execute a Remote ...
Information	6/28/2018 11:45:30 AM	PowerShell (Micr...	40962	PowerShell Conso...
Information	6/28/2018 11:45:30 AM	PowerShell (Micr...	53504	PowerShell Name...
Information	6/28/2018 11:45:29 AM	PowerShell (Micr...	40961	PowerShell Conso...
Information	6/28/2018 11:45:28 AM	PowerShell (Micr...	40962	PowerShell Conso...

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General

Details

Creating Scriptblock text (1 of 1):

Copyright (c) Microsoft. All rights reserved.
Licensed under the MIT license. See LICENSE file in the project root for full license information.

if (\$SPSVersionTable.PSEdition -or \$SPSVersionTable.PSEdition -eq "Desktop") {
 Add-Type -Path "\$PSScriptRoot/bin/Desktop/Microsoft.PowerShell.EditorServices.VSCode.dll"
}
else {
 Add-Type -Path "\$PSScriptRoot/bin/Core/Microsoft.PowerShell.EditorServices.VSCode.dll"
}

if (\$psEditor -is [Microsoft.PowerShell.EditorServices.Extensions.EditorObject]) {
 [Microsoft.PowerShell.EditorServices.VSCode.ComponentRegistration]::Register(\$psEditor.Components)
}
else {
 Write-Verbose '\$psEditor object not found in the session, components will not be registered.'
}

Get-ChildItem -Path \$PSScriptRoot\Public*.ps1 -Recurse | ForEach-Object {

Log Name: Microsoft-Windows-PowerShell/Operational

Actions

Operational

Open Saved Log...

Create Custom View...

Import Custom View...

Clear Log...

Filter Current Log...

Properties

Disable Log

Find...

Save All Events As...

Attach a Task To this Log...

View

Refresh

Help

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

Event Properties

Attach Task To This Event...

Save Selected Events...

Copy

Refresh

Help



- RSS Feeds
- Search
- Security Center
- Shutdown Options
- Smart Card
- Software Protection Platform
- Sound Recorder
- Speech
- Store
- Sync your settings
- > Tablet PC
- Task Scheduler
- Text Input
- Windows Calendar
- Windows Color System
- Windows Customer Experienc
- > Windows Defender Antivirus
- Windows Defender Applicati
- > Windows Defender Exploit G
- > Windows Defender Security C
- > Windows Defender SmartScr
- > Windows Error Reporting
- Windows Game Recording ar
- > Windows Hello for Business
- Windows Ink Workspace
- Windows Installer
- Windows Logon Options
- Windows Media Digital Right
- Windows Media Player
- Windows Messenger
- Windows Mobility Center
- Windows PowerShell
- Windows Reliability Analysis
- > Windows Remote Managem
- Windows Remote Shell

Windows PowerShell

Select an item to view its description.

Setting	State	Comment
Turn on Module Logging	Not configured	No
Turn on PowerShell Script Block Logging	Not configured	No
Turn on Script Execution	Not configured	No
Turn on PowerShell Transcription	Not configured	No
Set the default source path for Update-Help	Not configured	No

Actions

Windows PowerShell

More Actions

Extended Standard

Group Policy



Demo Summary

Different types of logging


Transcription, Console, Event Log

Configured by GPO or registry settings

The future



Questions?

 @Jaap_Brasser

#AllAccessIT