

Diving Deeper into PowerShell

Matt Elliott – Developer Advocate

Mike Preston – Developer Advocate



Jaap Brasser

Tweets

 jaap_brasser

Codes

 jaapbrasser

Works

Dev Advocate @ Rubrik

Does

Blogger, Speaker, Tech Enthusiast

Likes

Cloud Automation & Quokkas



Get Well Soon, Jaap!

Matt Elliott

Tweets



NetworkBrouhaha

Codes



shamsway

Works

Developer Advocate @ Rubrik

Does

Coding, Learning, Parenting

Likes

Tech, Getting Outdoors, Live Music



Mike Preston

Tweets

 mwpreston

Codes

 mwpreston

Works

Developer Advocate @ Rubrik

Does

Coding, Writing, Talking

Likes

Maple Syrup and Hockey



Agenda

What is PowerShell

PowerShell Security


PowerShell in the Cloud

Q&A

What is PowerShell

What is PowerShell

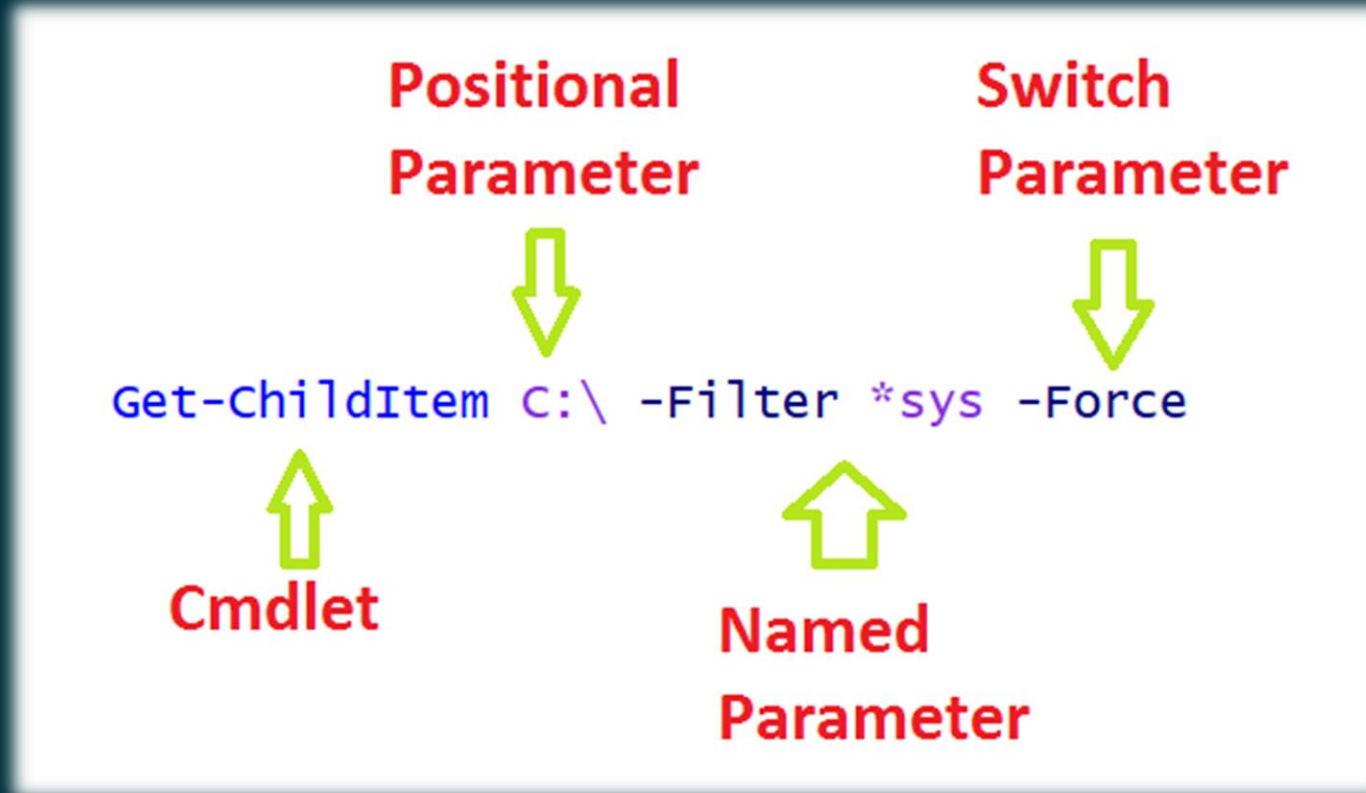
- Microsoft Automation Language
- Available on Windows by default
- Shell
- Open Source
- Cross Platform



Why
PowerShell
???

P O W E R S H E L L

PowerShell Language



PowerShell Security

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-Pmerr
PersistentMemory-ScmBi
PersistentMemory-Virtua
Policy-based QoS
PowerShell
Admin
Operational
PowerShell-DesiredStateC
PrimaryNetworkIcon
PrintBRM
PrintService
PriResources-Deploymen
Program-Compatibility-I
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 (Mitr...	4104	Execute a Remote ...
Warning	6/28/2018 11:45:35 AM	PowerShell (Mitr...	4104	Execute a Remote ...
Information	6/28/2018 11:45:32 AM	PowerShell (Mitr...	4103	Executing Pipeline
Information	6/28/2018 11:45:32 AM	PowerShell (Mitr...	4103	Executing Pipeline
Warning	6/28/2018 11:45:32 AM	PowerShell (Mitr...	4104	Execute a Remote ...
Information	6/28/2018 11:45:30 AM	PowerShell (Mitr...	40962	PowerShell Conso...
Information	6/28/2018 11:45:30 AM	PowerShell (Mitr...	53504	PowerShell Name...
Information	6/28/2018 11:45:29 AM	PowerShell (Mitr...	40961	PowerShell Conso...
Information	6/28/2018 11:45:28 AM	PowerShell (Mitr...	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 ($SpsEditor -is [Microsoft.PowerShell.EditorServices.Extensions.EditorObject]) {  
    [Microsoft.PowerShell.EditorServices.VSCode.ComponentRegistration]::Register($SpsEditor.Components)  
}  
else {  
    Write-Verbose 'SpsEditor 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

Group Policy

Just Enough Administration (JEA)



Secrets Management

- Export-CliXml
 - Encrypt credential objects
 - Store within files on the local filesystem
 - Accessible to specific user on specific computer
 - Windows specific (Data Protection API)
- Dev release of SecretsManagement Module
 - Create and store secrets in vaults
 - Default Built-In Vault included
 - Store string, bytes, credentials, hashtables, etc



Demo: PowerShell Security



Demo Summary

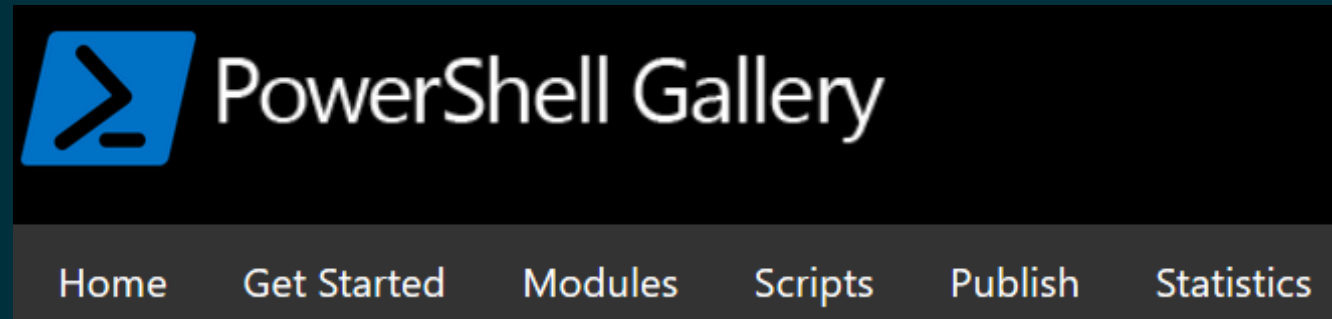
Store password securely

Connect to a remote system

JEA demonstration

PowerShell in the Cloud

PowerShell Gallery



- Install Modules from PowerShell
- Curated and Secured
- Best-practices enforced

Cloud Shell



Requirements



Azure
Subscription



Browser,
Extension, App



Storage
Account



Shell skills

Browser Support



Chrome



Edge



Firefox



Safari



IE

CloudDrive in Cloud Shell

Command

`clouddrive mount` :Mount an Azure file share to Cloud Shell.

Mount enables mounting and associating an Azure file share to Cloud Shell. Cloud Shell will automatically attach this file share on each session.

Cloud Shell persists files with both methods below:

1. Create a disk image of your \$HOME directory to persist files within. This disk image is saved in your specified file share as 'acc_jcjbrass' in the path `///<storageaccount>.file.storage.windows.net/<fileshare>/.cloudconsole`.
2. Mount specified file share as 'clouddrive' in \$HOME for file sharing. `/home/jcjbrasser/clouddrive` maps to `///<storageaccount>.file.storage`.

Arguments

<code>-s</code>	<code>--subscription id</code>	[Required]:Subscription ID or name.
<code>-g</code>	<code>--resource-group group</code>	[Required]:Resource group name.
<code>-n</code>	<code>--storage-account name</code>	[Required]:Storage account name.
<code>-f</code>	<code>--file-share name</code>	[Required]:File share name.
<code>-d</code>	<code>--disk-size size</code>	Disk size in GB. (default 5)
<code>-F</code>	<code>--force</code>	Skip warning prompts.
<code>-?</code>	<code>-h</code> <code>--help</code>	Shows this usage text.

Cloud Shell machines exist in the following regions:

Area	Region
Americas	East US, South Central US, West US
Europe	North Europe, West Europe
Asia Pacific	India Central, Southeast Asia

Demo: PowerShell in the Cloud



Demo Summary

Find and Install modules

Using PowerShell modules to manage
Cloud services

Azure Cloud Shell



Build the Future of Cloud Data Management



Software Development Kits

 Go >


 PowerShell >


 Python >

[VIEW ALL SDKS](#)



Tooling Integrations

 Ansible >


 VMware vRealize >


 Monitor Rubrik with Splunk >


[VIEW ALL INTEGRATIONS](#)



Use Cases

 Roxie, Rubrik's Intelligent Personal As... >

 Backup Validation with PowerShell >

 Provision and Protect with vRealize >

[VIEW ALL USE CASES](#)

Q&A - Discussion