PowerShell Conference Asia

Jason and Jaap PowerShell tips

Jason Yoder & Jaap Brasser
@JasonYoder_MCT @jaap_brasser

#psconfasia

About_jason

- MCSE since Windows NT 4.0
- Bachelors degree in Computer Science
- Microsoft Certified Trainer
- SAPIEN Technologies PowerShell MVP
- Technical Reviewer for Microsoft's official PowerShell training
- Author of Advanced Windows PowerShell Scripting video training

@ JasonYoder_MCT

About_jaap

- Dutch PowerShell User Group
- Blogging
  - PowerShell Magazine
  - JaapBrasser.com
- Slack
- Reddit
- GitHub
- PowerShell Gallery
- TechNet Forums/Gallery

@Jaap_Brasser

PowerShell Conference Asia

Download the Code

http://tinyurl.com/hwkq7h4

Get-ADGroupMemberDate

- Uses the repadmin command to get information about users added to groups
- Can be used to determine historical group membership
- Can be used to identify malicious use of administrative groups

Script is available on TechNet

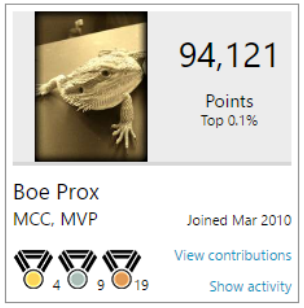
Download Windows Server 2012

Quick access

My contributions (15)

Upload a contribution

Browse script requests



More from Boe Prox

Get product keys of local and remote systems

★★★★★ (108)

Find the time a user was add/removed from a group

This function allows you to look at an Active Directory group's metadata using repadmin to determine who was added or removed from a group and the time this modification occurred. Also listed are number of times that this type of modification has taken place with a specific gro

Download Get-ADGroupMemberDate.ps1

My rating	★★★★★	Updated	5/22/2013
Downloaded	5,338 times	License	TechNet terms of use
Favorites	Add to favorites	Share it:	
Category	Active Directory		
Sub category	Groups		
Tags	Active Directory, Powershell, replication, repadmin		

Report abuse to Microsoft

Description | Q and A (3)

This function allows you to look at an Active Directory group's metadata using repadmin to determine who was added or removed from a group and the time this modification occurred. Also listed are number of times that this type of modification has taken place with a specific group member. Note that the ABSENT state (user removed from group) is only visible for as long as the Tombstone Lifetime (TSL) is configured for the domain. Once the date has reached the TSL, it is will be garbage collected and will no longer appear in the report.

Related blog post: http://learn-powershell.net/2013/05/21/find-when-a-user-was-added-or-removed-to-a-domain-group-using-powershell-and-repadmin/

Demo – Get-ADGroupMemberDate

```
PS C:\Users\JaapBrasser> $Files = Get-ChildItem -Path C:\Windows\ -Recurse
Get-ChildItem : Access to the path 'C:\Windows\appcompat\Programs' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\appcompat\Programs:String) [Get-ChildItem], UnauthorizedAc
   cessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\CSC' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\CSC:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\InfusedApps' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\InfusedApps:String) [Get-ChildItem], UnauthorizedAccessExc
   eption
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\LiveKernelReports' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\LiveKernelReports:String) [Get-ChildItem], UnauthorizedAcc
   essException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```

Demo Summary

- Showed historical view of users added and removed from a group
- Added and removed a domain admin to a group
- Viewed the results
- Showed how this information is gathered by repadmin

Posting message to Slack using PowerShell

- Slack is a communication tool
- Join psconfasia.slack.com
- Slack can be used to combine information from multiple sources
- Create automated reports

What is Slack

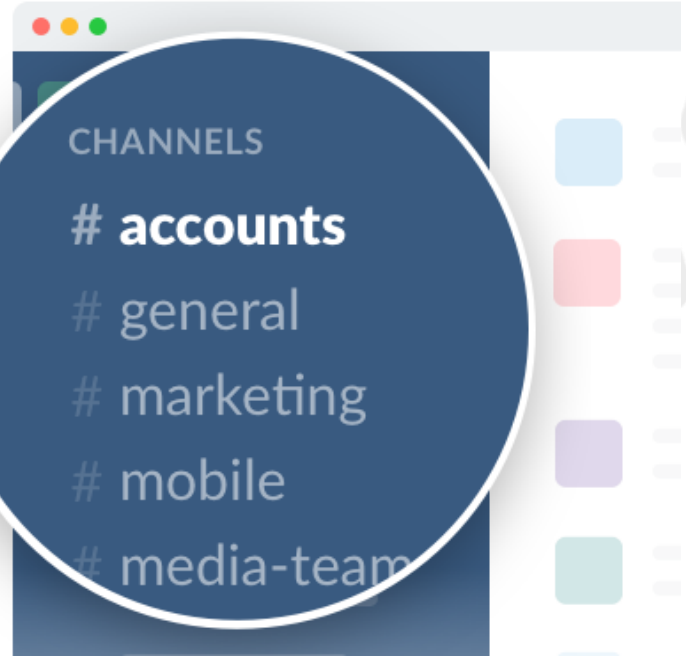
Team communication for the 21st century.

Channels

Organize your team conversations in open channels. Make a channel for a project, a topic, a team, or anything—everyone has a transparent view of all that's going on.

Private Channels

For sensitive information, create private channels and invite a few team members. No one else can see or join your private channels.



Demo – Slack and PowerShell

```
PS C:\Users\JaapBrasser> $Files = Get-ChildItem -Path C:\Windows\ -Recurse
Get-ChildItem : Access to the path 'C:\Windows\appcompat\Programs' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\appcompat\Programs:String) [Get-ChildItem], UnauthorizedAc
   cessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\CSC' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\CSC:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\InfusedApps' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\InfusedApps:String) [Get-ChildItem], UnauthorizedAccessExc
   eption
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\LiveKernelReports' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\LiveKernelReports:String) [Get-ChildItem], UnauthorizedAcc
   essException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```

Demo Summary

- How to setup a webhook in Slack
- Showed how to write custom messages using JSON
- How to request an API token
- How to install and use the PSSlack module

Getting folder size using PowerShell

- Getting folder size in PowerShell
- Use different methods of getting this information
- Disadvantage of using full objects

Demo – Getting folder size using PowerShell

```
PS C:\Users\JaapBrasser> $Files = Get-ChildItem -Path C:\Windows\ -Recurse
Get-ChildItem : Access to the path 'C:\Windows\appcompat\Programs' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\appcompat\Programs:String) [Get-ChildItem], UnauthorizedAc
   cessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\CSC' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\CSC:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\InfusedApps' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\InfusedApps:String) [Get-ChildItem], UnauthorizedAccessExc
   eption
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\LiveKernelReports' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\LiveKernelReports:String) [Get-ChildItem], UnauthorizedAcc
   essException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```

Demo Summary

- Showed three different methods of gathering folder sizes:
  - Get-ChildItem
  - The old dir command
  - Robocopy
- Showed the performance difference

Accessing Active Directory

- There are two type accelerators available in PowerShell
  - [adsi]
  - [adsisearcher]
- Does not require the Active Directory module
- Allows you to query Active Directory from any machine
- Default permissions in Active Directory allows any user to query

Demo – Query Active Directory using [adsisearcher]

```
PS C:\Users\JaapBrasser> $Files = Get-ChildItem -Path C:\Windows\ -Recurse
Get-ChildItem : Access to the path 'C:\Windows\appcompat\Programs' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\appcompat\Programs:String) [Get-ChildItem], UnauthorizedAc
   cessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\CSC' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\CSC:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\InfusedApps' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\InfusedApps:String) [Get-ChildItem], UnauthorizedAccessExc
   eption
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\LiveKernelReports' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\LiveKernelReports:String) [Get-ChildItem], UnauthorizedAcc
   essException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```

Demo Summary

- Used [adsisearcher] to query for user accounts
- Disabled a user account
- Get all user accounts in an Organization Unit
- Show how to enumerate a collection
- Changed a user password
- Enumerate users that has password does not expire flag set

Executing PowerShell from outside of PowerShell

- PowerShell can be started by calling powershell.exe
- There are two parameters available
  - File
  - Command
- There are some limitations to using the –File parameter

Demo – Execute PowerShell

```
PS C:\Users\JaapBrasser> $Files = Get-ChildItem -Path C:\Windows\ -Recurse
Get-ChildItem : Access to the path 'C:\Windows\appcompat\Programs' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\appcompat\Programs:String) [Get-ChildItem], UnauthorizedAc
   cessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\CSC' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\CSC:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\InfusedApps' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\InfusedApps:String) [Get-ChildItem], UnauthorizedAccessExc
   eption
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\LiveKernelReports' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\LiveKernelReports:String) [Get-ChildItem], UnauthorizedAcc
   essException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```

Demo Summary

- File can be used for simple scripts and functions does not support arrays
- Command allows you to specify the PowerShell code that should be executed
- How to execute PowerShell 32bit or PowerShell 64bit

Creating loops in PowerShell

- Show some common mistakes found in PowerShell samples found online
- How to create PowerShell custom objects
- How to optimize object creation and loops

Demo – Execute PowerShell

```
PS C:\Users\JaapBrasser> $Files = Get-ChildItem -Path C:\Windows\ -Recurse
Get-ChildItem : Access to the path 'C:\Windows\appcompat\Programs' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\appcompat\Programs:String) [Get-ChildItem], UnauthorizedAc
   cessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\CSC' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\CSC:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\InfusedApps' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\InfusedApps:String) [Get-ChildItem], UnauthorizedAccessExc
   eption
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand

Get-ChildItem : Access to the path 'C:\Windows\LiveKernelReports' is denied.
At line:1 char:10
+ $Files = Get-ChildItem -Path C:\Windows\ -Recurse
+          ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Windows\LiveKernelReports:String) [Get-ChildItem], UnauthorizedAcc
   essException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```

Demo Summary

- File can be used for simple scripts and functions does not support arrays
- Command allows you to specify the PowerShell code that should be executed
- How to execute PowerShell 32bit or PowerShell 64bit

Additional topics open for discussion

- Convert word document to pdf
- Check compression of zip file
- Check open folders in Explorer
- Change a drive letter
- Copy untitled tabs to clipboard
- Create simple GUI messagebox
- List non-administrative shares
- Rename a local/mapped disk
- Create GUI OpenFileDialog
- Query MSDN from PowerShell
- Test local credentials
- List AD attributes in use

Don’t Forget!

- Fill in your survey – it’s how we do better!
- Don’t lose your badge! You need it for the Social Events
- Grab the Speakers for a chat – they all have time for you!
- Let everyone know what they are missing on Social Media

  #PowerShell

  #PSConfAsia

  Tweets (preferably with Pictures) win Prizes!!!!

Photos of Marina Bay Credit: Sebastian Szumigalski