WELCOME TO TECH | IMMERSION

Track: Active Directory Cmdlets

Presenter: Brian McCann

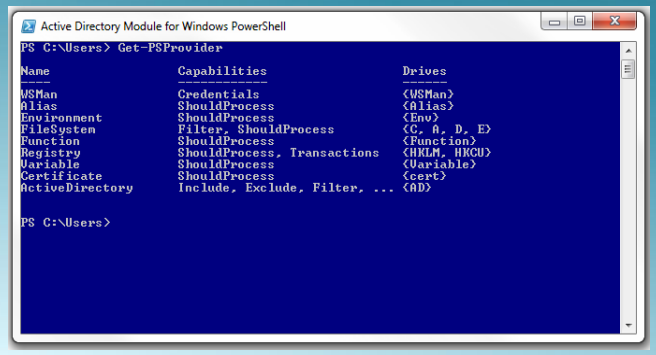
Global Platforms Engineer - Brian@Intel.com

PowerShell Advantages

- Consistent vocabulary and syntax
  - Verbs – Add, New, Get, Set, Remove, Clear…
  - Nouns – ADObject, ADUser, ADComputer, ADDomain, ADGroup, …
- Easily discovered
  - No need to find, install, or learn other tools, utilities or commands
- Flexible output
  - Output from one cmdlet easily consumed by another
- Leverage .Net Framework
  - All the capabilities of .Net Framework
- Common automation platform
  - End-to-End manageability of AD with other roles such as Exchange, Group Policy
- 76 Cmdlets for managing Active Directory
  - get-command *-ad*

Windows PowerShell – AD Module

Active Directory Module in Windows Server 2008 R2



- A Windows PowerShell module
- Manage AD domains and Lightweight Directory Services (LDS) configuration sets
- AD Database Mounting Tool instance

New Functionality

- Active Directory module provider
- Active Directory module cmdlets
- Windows PowerShell Integrated Scripting Environment (ISE)
- Out-GridView cmdlet
- Performance counters

Special Considerations

- Only installs on Windows Server 2008 R2
- At least one Windows Server 2008 R2 domain controller or LDS configuration set
- Windows 7 and Report Server Administration Tools (RSAT)

Active Directory Name Spaces

- Active Directory Users & Computers dumbs it down
- We need to know the real names
  - Active Directory Hierarchical structure
  - LDAP Distinguished Name (DN) – *CN=John Doe,OU=Sales,DC=DomainName,DC=com*
  - LDAP Relative Distinguished Name (RDN) – *John Doe*
  - Common Name (CN) – *John Doe*
  - Canonical Name – *DC=com/DC=DomainName/OU=Sales/CN=John Doe*
  - User Principal Name (UPN) – *John.Doe@DomainName.com*
  - Down level Name (SAM Account) – *DomainName\jdoe -or- jdoe*

Where to Start?

- Make sure your environment supports AD Cmdlets
- Start with a purpose and goal
- Account Management
- Directory Management
- Forest/Domain Management

Active Directory Cmdlets Requirements

- Server 2008 R2 Domain Controller or Lightweight Directory Services

Or

- Active Directory Management Gateway Service
  - Supported on Server 2003 SP2
  - Server 2003 R2 SP2
  - Server 2008 and above
  - Domain and Forest functional levels do not matter
  - DotNet 3.5 SP1
  - Server 2003 SP2 hotfix
  - Server 2003 SP2 and R2 SP2 hotfix
  - Server 2008 hotfix
  - Windows 7 Clients need RSAT
- Much easier if you have Server 2008 R2 DCs!!! ☺

How does PowerShell make my life easier?

- Common automation platform
- Easy to create and understand scripts
- Great documentation!!!
- A great open community that thrives on sharing ideas

Active Directory Cmdlets Getting Started

- Open PowerShell and type
  - import-module ActiveDirectory
- Now what is available
  - get-command -module ActiveDirectory | Select Name | Format-Wide
- How do we get the AD Cmdlets every time we open PowerShell?
  - Add it to your Windows PowerShell profile
  - Open the Active Directory PowerShell executable

Active Directory Account Management

Using AD Cmdlets for day to day tasks

- Search-ADAccount
- Disable-ADAccount
- Enable-ADAccount
- Unlock-ADAccount

ADAccount = Users, Computers & Service Accounts

Account Management One Liners

Find Disabled Accounts

- Search-ADAccount -AccountDisabled | FT Name,ObjectClass -A

Find Locked Accounts

- Search-ADAccount -LockedOut | FT Name,ObjectClass -A

Find Passwords that never expire

Search-ADAccount -PasswordNeverExpires | FT Name,ObjectClass -A

Account Management One Liners

Find Inactive Accounts

- Search-ADAccount -AccountInactive -TimeSpan 90.00:00:00 | FT Name,Obj

Find Expired Accounts

- Search-ADAccount -AccountExpired | FT Name,ObjectClass -A

Active Directory Account Management (cont)

- **New, Get, Set & Remove**
  - ADUser
  - ADGroup
  - ADComputer
  - ADServiceAccount
  - ADOrganizationalUnit
  - ADDomainController

Active Directory Account Management

Get User Info

- Get-ADUser -Identity ‘Administrator’

Additional info can be found

- -Properties *

Get Domain Controller Info

- Get-ADDomainController

Active Directory Account Management

Get Group Info

- Get-ADGroup -Identity “Administrators"

Get Group Membership

- Get-ADGroupMember -Identity “Administrators"

What is ADServiceAccount?

- It is a new type of Account that can be used for Services on a single system
- It is a hybrid account that is part User and part computer account
  - Password changes every 30days and are 240 characters
- Requirements:
  - Server 2008 R2 Schema
  - Server 2008 R2 or Windows 7 system

What is ADServiceAccount?

How to create an ADServiceAccount

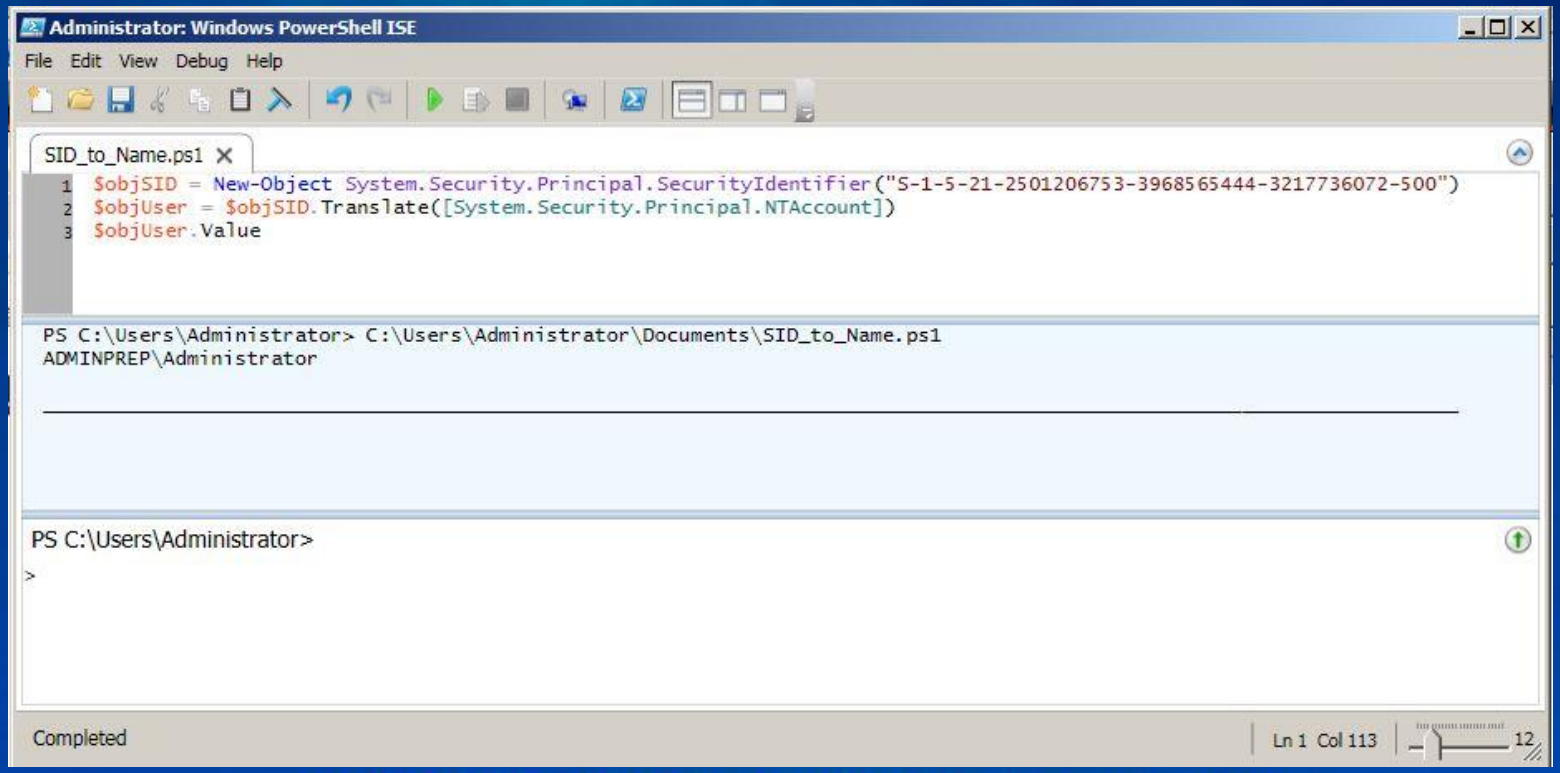
- New-ADServiceAccount SA-SQL01 -Enabled $true -Path “CN=Managed Service Accounts,DC=adminprep,DC=Local” -ServicePrincipalNames “MSSQLSVC/SQL01.adminprep.Local:1456″

Resolve a SID to Name

Who is S-1-5-21-2501206753-3968565444-3217736072-500

How about

S-1-5-21-2501206753-3968565444-3217736072-1000



Active Directory
Directory Management

- New, Get, Set & Remove
- Move, Rename & Restore
  - ADObject

Search Active Directory

```
Get-ADObject -Filter { CN -like "*bob*" }
```

Active Directory Site Management One Liners

List all your Active Directory Sites

- Get-ADObject -LDAPFilter "(objectClass=site)" -SearchBase 'CN=Configuration,DC=Adminprep,DC=local' -Properties CanonicalName | FT Name,CanonicalName –A

List all your Active Directory Subnets

- Get-ADObject -Filter 'ObjectClass -eq "site"' -SearchBase 'CN=Configuration,DC=AdminPrep,DC=local' -Properties siteObjectBL | foreach {$_.siteObjectBL}

Active Directory
Site Management Scripts

Scripts to get Site info:

- Get all Servers in a specified Active Directory site
- Get all Subnets in a specified Active Directory site
- Get a list of sites and their subnets

How do you like your Tombstone?

Tombstone Lifetime

- *(get-adobject "cn=Directory Service,cn=Windows NT,cn=Services,cn=Configuration,dc=AdminPrep,DC=Local" -properties "tombstonelifetime").tombstonelifetime*

Set Tombstone Object Lifetime

- Set-ADObject -Identity “CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=AdminPrep,DC=Local” –Partition “CN=Configuration,DC=AdminPrep,DC=Local” –Replace:@{“tombstoneLifetime” = 250}

Set Deleted Object Lifetime

- Set-ADObject -Identity “CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=AdminPrep,DC=Local” –Partition “CN=Configuration,DC=AdminPrep,DC=Local” –Replace:@{“msDS-DeletedObjectLifetime” = 250}

Active Directory Forest/Domain Management

- Functional Levels
- Password Policies
- FSMO Management
- Optional Features

Get Domain and Forest Info

Domain and Forest Configuration

- Get-ADForest adminprep.local
- Get-ADDomain adminprep.local

Raise Domain Functional Level

- Set-ADDomainMode –Identity adminprep.local –forestmode Windows2008R2Domain

Raise Forest Functional Level

- Set-ADForestMode –Identity adminprep.local –forestmode Windows2008R2Forest

Rollback Functional Levels

Server 2008 R2 PowerShell allows you to Revert functional levels

- Set-ADDomainMode –Identity adminprep.local –forestmode Windows2008Domain

Will not work if you enabled the Active Directory Recycle Bin

Will not work if you are currently in Server 2008 R2 FFL

Fine Grained Password Policies

Much easier than Windows Server 2008

- Get-adfinegrainedpasswordpolicy –filter *
- New-ADFineGrainedPasswordPolicy
- Add-ADFineGrainedPasswordPolicySubject

View which users have been applied a FGPP

- Get-ADFineGrainedPasswordPolicySubject –identity “group or user”

View Default Domain Password Policy

- Get-ADDefaultDomainPasswordPolicy

FSMO Management

FSMO Management

- *Move-ADDirectoryServerOperationMasterRole*
  - PDCEmulator
  - RIDMaster
  - InfrastructureMaster
  - SchemaMaster
  - DomainNamingMaster

Enabling AD Recycle Bin

Enable the Active Directory Recycle Bin:

Enable-ADOptionalFeature -Identity "CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service, CN=Windows NT,CN=Services, CN=Configuration, DC=AdminPrep,DC=Local" -Scope ForestorConfigurationSet -Target "AdminPrep.local“

Restore a deleted object:

get-adobject –inc –f {samaccountname –like “bri*"} | restore-adobject

Thank you.

http://blogs.msmvps.com/ad