

The Ultimate Education Destination ORLANDO 2023

Managing Active Directory with PowerShell

Jeff Hicks Learning Architect

Level: Intermediate











Cybersecurity & Ransomware uve

PS C:\> whoami

- Veteran IT Pro
- Microsoft MVP
- Author
- Teacher
- https://jdhitsolutions.github.io







Why PowerShell

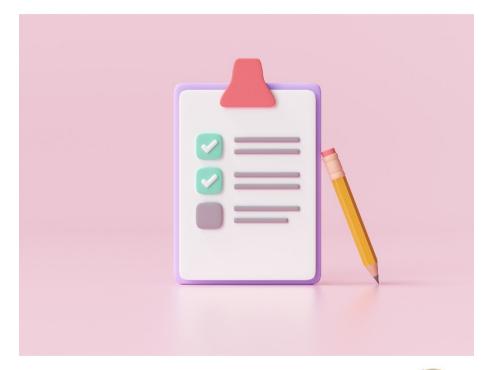
- Available everywhere
 - Install PowerShell 7
- Manage from your desktop
- Consistency
- Efficiency
- Scalability
 - Manage at Scale





Requirements

- PowerShell
- RSAT ActiveDirectory tools
 - Local AD infrastructure
 - Run from your desktop
 - NO RDP!
- Permissions
- DNSServer module
 - Out of scope today





PS C:\> Get-WindowsCapability -name rsat.ActiveDirectory* -online

Name : Rsat.ActiveDirectory.DS-LDS.Tools~~~0.0.1.0

State : Installed

DisplayName : RSAT: Active Directory Domain Services and Lightweight Directory Services Tools

Description : Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS)

Tools include snap-ins and command-line tools for remotely managing AD DS and AD LDS on Windows Server.

DownloadSize : 5230259 InstallSize : 34704398

Remote Server Administration Tools

Ships with Windows 10/11



Get-WindowsCapability -name rsat.ActiveDirectory* -online |
Add-WindowsCapability -online



```
Count Name
                                Group
                                {Add-ADCentralAccessPolicyMember, Add-ADComputerServiceAccount, Add-ADDomainControll...
   7 Add
    2 Clear
                                {Clear-ADAccountExpiration. Clear-ADClaimTransformLink}
    2 Disable
                                {Disable-ADAccount, Disable-ADOptionalFeature}
    2 Enable
                                {Enable-ADAccount, Enable-ADOptionalFeature}
                                {Get-ADAccountAuthorizationGroup, Get-ADAccountResultantPasswordReplicationPolicy, G...
  43 Get
    1 Grant
                                {Grant-ADAuthenticationPolicySiloAccess}
                                {Install-ADServiceAccount}
    1 Install
    3 Move
                                {Move-ADDirectorvServer, Move-ADDirectorvServerOperationMasterRole, Move-ADObject}
   20 New
                                {New-ADAuthenticationPolicy, New-ADAuthenticationPolicySilo, New-ADCentralAccessPoli...
                                {Remove-ADAuthenticationPolicy, Remove-ADAuthenticationPolicySilo, Remove-ADCentralA...
   26 Remove
                                {Rename-ADObject}
    1 Rename
    1 Reset
                                {Reset-ADServiceAccountPassword}
    1 Restore
                                {Restore-ADObject}
                                {Revoke-ADAuthenticationPolicySiloAccess}
    1 Revoke
    1 Search
                                {Search-ADAccount}
                                {Set-ADAccountAuthenticationPolicySilo, Set-ADAccountControl, Set-ADAccountExpiratio...
   30 Set
                                {Show-ADAuthenticationPolicyExpression}
    1 Show
    1 Sync
                                {Sync-ADObject}
                                {Test-ADServiceAccount}
    1 Test
    1 Uninstall
                                {Uninstall-ADServiceAccount}
    1 Unlock
                                {Unlock-ADAccount}
PS C:\> Get-Command -module ActiveDirectory | Measure-Object | Select-Object Count
Count
```

PS C:\> Get-Command -module ActiveDirectory | Group Verb

147

PSDrive

 Navigate AD as a drive

```
PS AD:\DC=Company,DC=Pri> dir
Name
                      ObiectClass
                                           DistinguishedName
Accounting
                      organizationalUnit
                                           OU=Accounting, DC=Company, DC=Pri
                                           CN=Builtin, DC=Company, DC=Pri
Builtin
                      builtinDomain
                                           CN=Computers, DC=Company, DC=Pri
Computers
                      container
Dev
                      organizationalUnit
                                           OU=Dev, DC=Company, DC=Pri
                                           OU=Domain Controllers, DC=Company, DC=Pri
Domain Controllers
                     organizationalUnit
Employees
                      organizationalUnit
                                           OU=Employees, DC=Company, DC=Pri
                                           CN=ForeignSecurityPrincipals,DC=Company,DC=Pri
ForeignSecurityPr... container
                      infrastructureUpdate CN=Infrastructure, DC=Company, DC=Pri
Infrastructure
                      organizationalUnit
                                           OU=IT, DC=Company, DC=Pri
JEA_Operators
                                           OU=JEA_Operators, DC=Company, DC=Pri
                      organizationalUnit
Keys
                      container
                                           CN=Keys, DC=Company, DC=Pri
LostAndFound
                      lostAndFound
                                           CN=LostAndFound.DC=Company.DC=Pri
                                           CN=Managed Service Accounts, DC=Company, DC=Pri
Managed Service A... container
Marketing
                      organizationalUnit
                                           OU=Marketing, DC=Company, DC=Pri
NTDS Ouotas
                      msDS-OuotaContainer CN=NTDS Ouotas.DC=Company.DC=Pri
Program Data
                      container
                                           CN=Program Data,DC=Company,DC=Pri
Sales
                      organizationalUnit
                                           OU=Sales.DC=Company.DC=Pri
Servers
                      organizationalUnit
                                           OU=Servers, DC=Company, DC=Pri
Svstem
                      container
                                           CN=System, DC=Company, DC=Pri
                     msTPM-Information... CN=TPM Devices, DC=Company, DC=Pri
TPM Devices
Users
                      container
                                           CN=Users, DC=Company, DC=Pri
PS AD:\DC=Company,DC=Pri> get-item '//Rootdse/CN=Administrator,CN=Users,DC=Company,DC=Pri'
Name
                      ObjectClass
                                           DistinguishedName
Administrator
                                           CN=Administrator, CN=Users, DC=Company, DC=Pri
                      user
PS AD:\DC=Company,DC=Pri>
```



Show Me



Session Survey

- Your feedback is very important to us
- Please take a moment to complete the session survey found in the mobile app
- Use the QR code or search for "Converge360 Events" in your app store
- Find this session on the Agenda tab
- Click "Session Evaluation"
- Thank you!



Questions

