- (https://adsecurity.org/?feed=rss2)

Beyond Domain Admins – Domain Controller & AD Administration (https://adsecurity.org/?p=3700)

Securing Microsoft Active Directory Federation Server (ADFS) (https://adsecurity.org/?p=3782)

Aug 11 2017

Gathering AD Data with the Active Directory PowerShell Module

- By Sean Metcalf (https://adsecurity.org/?author=2) in PowerShell (https://adsecurity.org/?cat=7), Technical Reference (https://adsecurity.org/?cat=2)

Microsoft provided several Active Directory PowerShell cmdlets with Windows Server 2008 R2 (and newer) which greatly simplify tasks which previously required putting together lengthy lines of code involving ADSI.

On a Windows client, install the Remote Sever Administration Tools (RSAT) (https://www.microsoft.com/en-us/download/details.aspx?id=45520) and ensure the Active Directory PowerShell module is installed.

On a Windows server (2008 R2 or newer), run the following commands in a PowerShell console (as an Adminsitrator):

Import-Module ServerManager ; Add-WindowsFeature RSAT-AD-PowerShell

Here's my (poor) ADSI example:

```
$UserID = "JoeUser"
$root = [ADSI]''
$searcher = new-object System.DirectoryServices.DirectorySearcher($root)
$searcher.filter = "(&(objectClass=user)(sAMAccountName= $UserID))"
$user = $searcher.findall()
$user
```

Here's the same thing with the AD PowerShell cmdlet:

Import-module ActiveDirectory
$UserID = "JoeUser"
*Get-ADUser $UserID –property **

Note that with PowerShell version 3 and newer, you don't need to run the first line since Powershell will identify the necessary module and auto load it.

Once you have the Active Directory PowerShell module loaded, you can do cool stuff like browse AD like a file system

```
PS C:\Users\LukeSkywalker> import-module activedirectory
PS C:\Users\LukeSkywalker> dir ad:

Name                ObjectClass          DistinguishedName
----                -----------          -----------------
lab                 domainDNS            DC=lab,DC=adsecurity,DC=org
Configuration       configuration        CN=Configuration,DC=lab,DC=adsecurity,DC=org
Schema              dMD                  CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC=org
DomainDnsZones      domainDNS            DC=DomainDnsZones,DC=lab,DC=adsecurity,DC=org
ForestDnsZones      domainDNS            DC=ForestDnsZones,DC=lab,DC=adsecurity,DC=org


PS C:\Users\LukeSkywalker> set-location ad:
PS AD:\> set-location "dc=lab,dc=adsecurity,dc=org"
PS AD:\dc=lab,dc=adsecurity,dc=org> dir

Name                ObjectClass          DistinguishedName
----                -----------          -----------------
Admin Groups        organizationalUnit   OU=Admin Groups,DC=lab,DC=adsecurity,DC=org
Builtin             builtinDomain        CN=Builtin,DC=lab,DC=adsecurity,DC=org
Computers           container            CN=Computers,DC=lab,DC=adsecurity,DC=org
CorpOU              organizationalUnit   OU=CorpOU,DC=lab,DC=adsecurity,DC=org
Domain Controllers  organizationalUnit   OU=Domain Controllers,DC=lab,DC=adsecurity,DC=org
Domain Management   organizationalUnit   OU=Domain Management,DC=lab,DC=adsecurity,DC=org
ForeignSecurityPr... container            CN=ForeignSecurityPrincipals,DC=lab,DC=adsecurity,DC=org
Infrastructure      infrastructureUpdate CN=Infrastructure,DC=lab,DC=adsecurity,DC=org
LostAndFound        lostAndFound         CN=LostAndFound,DC=lab,DC=adsecurity,DC=org
Managed Service A... container            CN=Managed Service Accounts,DC=lab,DC=adsecurity,DC=org
                                         CN=NTDS Quotas,DC=lab,DC=adsecurity,DC=org
Program Data        container            CN=Program Data,DC=lab,DC=adsecurity,DC=org
Service Accounts    organizationalUnit   OU=Service Accounts,DC=lab,DC=adsecurity,DC=org
System              container            CN=System,DC=lab,DC=adsecurity,DC=org
                                         CN=TPM Devices,DC=lab,DC=adsecurity,DC=org
Users               container            CN=Users,DC=lab,DC=adsecurity,DC=org


PS AD:\dc=lab,dc=adsecurity,dc=org>
```

Finding Useful Commands (Cmdlets):

Discover available PowerShell modules: **Get-Module -ListAvailable**

Discover cmdlets in a PowerShell module: **Get-Command -module ActiveDirectory**

PowerShell AD Module Cmdlets:

- Windows Server 2008 R2: 76 cmdlets
- Windows Server 2012: 135 cmdlets
- Windows Server 2012 R2: 147 cmdlets
- Windows Server 2016: 147 cmdlets

```
(Get-Command -module ActiveDirectory).count
```

Finding Active Directory Flexible Master Single Operation (FSMO) Roles:

Active Directory Module:

- ```
  (Get-ADForest).SchemaMaster
  ```
- ```
  (Get-ADForest).DomainNamingMaster
  ```

- ```
  (Get-ADDomain).InfrastructureMaster
  ```
- ```
  (Get-ADDomain).PDCEmulator
  ```
- ```
  (Get-ADDomain).RIDMaster
  ```

.NET Calls:

- ```
  ([System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest()).SchemaRoleOwner
  ```
- ```
  ([System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest()).NamingRoleOwner
  ```
- ```
  ([System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()).InfrastructureRoleOw
  ```
- ```
  ([System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()).PdcRoleOwner
  ```
- ```
  ([System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()).RidRoleOwner
  ```

Active Directory PowerShell Module Cmdlet Examples:

Get-RootDSE gets information about the LDAP server (the Domain Controller) and displays it. There's some interesting information in the results like what OS the DC is running.

```
PS C:\Windows\system32> get-adrootdse


configurationNamingContext    : CN=Configuration,DC=lab,DC=adsecurity,DC=org
currentTime                   : 1/18/2015 9:07:52 PM
defaultNamingContext          : DC=lab,DC=adsecurity,DC=org
dnsHostName                   : ADSDC05.lab.adsecurity.org
domainControllerFunctionality : Windows2012R2
domainFunctionality           : Windows2003Domain
dsServiceName                 : CN=NTDS Settings,CN=ADSDC05,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=lab,DC
                                =adsecurity,DC=org
forestFunctionality           : Windows2003Forest
highestCommittedUSN           : 110986
isGlobalCatalogReady          : {TRUE}
isSynchronized                : {TRUE}
ldapServiceName               : lab.adsecurity.org:adsdc05$@LAB.ADSECURITY.ORG
namingContexts                : {DC=lab,DC=adsecurity,DC=org, CN=Configuration,DC=lab,DC=adsecurity,DC=org,
                                CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC=org,
                                DC=DomainDnsZones,DC=lab,DC=adsecurity,DC=org...}
rootDomainNamingContext       : DC=lab,DC=adsecurity,DC=org
schemaNamingContext           : CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC=org
serverName                    : CN=ADSDC05,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=lab,DC=adsecurity,DC=or
                                g
subschemaSubentry             : CN=Aggregate,CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC=org
supportedCapabilities         : {1.2.840.113556.1.4.800 (LDAP_CAP_ACTIVE_DIRECTORY_OID), 1.2.840.113556.1.4.1670
                                (LDAP_CAP_ACTIVE_DIRECTORY_V51_OID), 1.2.840.113556.1.4.1791
                                (LDAP_CAP_ACTIVE_DIRECTORY_LDAP_INTEG_OID), 1.2.840.113556.1.4.1935
                                (LDAP_CAP_ACTIVE_DIRECTORY_V61_OID)...}
supportedControl              : {1.2.840.113556.1.4.319 (LDAP_PAGED_RESULT_OID_STRING), 1.2.840.113556.1.4.801
                                (LDAP_SERVER_SD_FLAGS_OID), 1.2.840.113556.1.4.473 (LDAP_SERVER_SORT_OID), 1.2.840.113556.1.4.528
                                (LDAP_SERVER_NOTIFICATION_OID)...}
supportedLDAPPolicies         : {MaxPoolThreads, MaxPercentDirSyncRequests, MaxDatagramRecv, MaxReceiveBuffer...}
supportedLDAPVersion          : {3, 2}
supportedSASLMechanisms       : {GSSAPI, GSS-SPNEGO, EXTERNAL, DIGEST-MD5}
```

Get-ADForest provides information about the Active Directory forest the computer you run the command is in.

```
PS C:\Windows\system32> get-adforest


ApplicationPartitions : {DC=DomainDnsZones,DC=lab,DC=adsecurity,DC=org, DC=ForestDnsZones,DC=lab,DC=adsecurity,DC=org}
CrossForestReferences : {}
DomainNamingMaster    : ADSDC01.lab.adsecurity.org
Domains               : {lab.adsecurity.org}
ForestMode            : Windows2003Forest
GlobalCatalogs        : {ADSDC01.lab.adsecurity.org, ADSDC02.lab.adsecurity.org, ADSDC04.lab.adsecurity.org,
                        ADSDC05.lab.adsecurity.org}
Name                  : lab.adsecurity.org
PartitionsContainer   : CN=Partitions,CN=Configuration,DC=lab,DC=adsecurity,DC=org
RootDomain            : lab.adsecurity.org
SchemaMaster          : ADSDC01.lab.adsecurity.org
Sites                 : {Default-First-Site-Name}
SPNSuffixes           : {}
UPNSuffixes           : {}
```

Get-ADDomain provides information about the current domain you are in.

```
PS C:\Windows\system32> Get-ADDomain


AllowedDNSSuffixes               : {}
ChildDomains                     : {}
ComputersContainer               : CN=Computers,DC=lab,DC=adsecurity,DC=org
DeletedObjectsContainer          : CN=Deleted Objects,DC=lab,DC=adsecurity,DC=org
DistinguishedName                : DC=lab,DC=adsecurity,DC=org
DNSRoot                          : lab.adsecurity.org
DomainControllersContainer       : OU=Domain Controllers,DC=lab,DC=adsecurity,DC=org
DomainMode                       : Windows2003Domain
DomainSID                        : S-1-5-21-1473643419-774954089-2222329127
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=lab,DC=adsecurity,DC=org
Forest                           : lab.adsecurity.org
InfrastructureMaster             : ADSDC01.lab.adsecurity.org
LastLogonReplicationInterval     :
LinkedGroupPolicyObjects         : {cn={ABDBA081-F312-4F2A-9F95-143800450BB8},cn=policies,cn=system,DC=lab,DC=adsecurity,DC=org,
                                   cn={19DB3FB7-0098-4F85-8E24-B03050C686DE},cn=policies,cn=system,DC=lab,DC=adsecurity,DC=org,
                                   CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=lab,DC=adsecurity,DC=org}
LostAndFoundContainer            : CN=LostAndFound,DC=lab,DC=adsecurity,DC=org
ManagedBy                        :
Name                             : lab
NetBIOSName                      : ADSECLAB
ObjectClass                      : domainDNS
ObjectGUID                       : f6d46828-b721-463d-9696-3b3714e2676a
ParentDomain                     :
PDCEmulator                      : ADSDC01.lab.adsecurity.org
QuotasContainer                  : CN=NTDS Quotas,DC=lab,DC=adsecurity,DC=org
ReadOnlyReplicaDirectoryServers  : {}
ReplicaDirectoryServers          : {ADSDC01.lab.adsecurity.org, ADSDC02.lab.adsecurity.org, ADSDC04.lab.adsecurity.org,
                                   ADSDC05.lab.adsecurity.org}
RIDMaster                        : ADSDC02.lab.adsecurity.org
SubordinateReferences            : {DC=ForestDnsZones,DC=lab,DC=adsecurity,DC=org, DC=DomainDnsZones,DC=lab,DC=adsecurity,DC=org,
                                   CN=Configuration,DC=lab,DC=adsecurity,DC=org}
SystemsContainer                 : CN=System,DC=lab,DC=adsecurity,DC=org
UsersContainer                   : CN=Users,DC=lab,DC=adsecurity,DC=org
```

Get-ADDomainController provides computer information specific to Domain Controllers. This cmdlet makes it easy to find all DCs in a specific site or running an OS version.

```
PS C:\Windows\system32> Get-ADDomainController



ComputerObjectDN           : CN=ADSDC05,OU=Domain Controllers,DC=lab,DC=adsecurity,DC=org
DefaultPartition           : DC=lab,DC=adsecurity,DC=org
Domain                     : lab.adsecurity.org
Enabled                    : True
Forest                     : lab.adsecurity.org
HostName                   : ADSDC05.lab.adsecurity.org
InvocationId               : 2df64259-f56d-4e61-acde-3b67548a0977
IPv4Address                : 172.16.11.15
IPv6Address                :
IsGlobalCatalog            : True
IsReadOnly                 : False
LdapPort                   : 389
Name                       : ADSDC05
NTDSSettingsObjectDN       : CN=NTDS Settings,CN=ADSDC05,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=lab,DC=adse
                             curity,DC=org
OperatingSystem            : Windows Server 2012 R2 Datacenter
OperatingSystemHotfix      :
OperatingSystemServicePack :
OperatingSystemVersion     : 6.3 (9600)
OperationMasterRoles       : {}
Partitions                 : {DC=ForestDnsZones,DC=lab,DC=adsecurity,DC=org, DC=DomainDnsZones,DC=lab,DC=adsecurity,DC=org,
                             CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC=org, CN=Configuration,DC=lab,DC=adsecurity,DC=org...}
ServerObjectDN             : CN=ADSDC05,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=lab,DC=adsecurity,DC=org
ServerObjectGuid           : d68af971-b5af-4a32-9531-7f61f95e15cf
Site                       : Default-First-Site-Name
SslPort                    : 636
```

Get-ADComputer provides most of what you would want to know about a computer object in AD.
*Run with "-Prop *" to show all standard properties.*

```
PS C:\Windows\system32> get-adcomputer adsdc05



DistinguishedName : CN=ADSDC05,OU=Domain Controllers,DC=lab,DC=adsecurity,DC=org
DNSHostName       : ADSDC05.lab.adsecurity.org
Enabled           : True
Name              : ADSDC05
ObjectClass       : computer
ObjectGUID        : 72b0c16d-a1b6-4f31-bd36-901744a699ec
SamAccountName    : ADSDC05$
SID               : S-1-5-21-1473643419-774954089-2222329127-1602
UserPrincipalName :
```

Get-ADUser provides most of what you want to know about an AD user.
*Run with "-Prop *" to show all standard properties.*

```
PS C:\Windows\system32> get-aduser "hansolo"



DistinguishedName : CN=Han Solo,CN=Users,DC=lab,DC=adsecurity,DC=org
Enabled           : True
GivenName         : Han
Name              : Han Solo
ObjectClass       : user
ObjectGUID        : 8239fdc4-f82a-4346-a6bb-fac16b4b7bbf
SamAccountName    : HanSolo
SID               : S-1-5-21-1473643419-774954089-2222329127-1107
Surname           : Solo
UserPrincipalName : HanSolo@lab.adsecurity.org
```

Get-ADGroup provides information about an AD group. Find all security groups by running:
Get-ADGroup -Filter {GroupCategory -eq 'Security}

```
PS C:\Windows\system32> get-adgroup "Administrators"



DistinguishedName : CN=Administrators,CN=Builtin,DC=lab,DC=adsecurity,DC=org
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Administrators
ObjectClass       : group
ObjectGUID        : db5e60b4-9e61-4712-a518-ce7d06a9db24
SamAccountName    : Administrators
SID               : S-1-5-32-544
```

Get-ADGroupMember enumerates and returns the group members. Use the Recursive parameter to include all members of nested groups.
Get-ADGroupMember 'Administrators' -Recursive

```
PS C:\Windows\system32> get-adgroupmember "Administrators"



distinguishedName : CN=svc-SQLReporting,OU=Service Accounts,DC=lab,DC=adsecurity,DC=org
name              : svc-SQLReporting
objectClass       : user
objectGUID        : d85ccfa7-bec2-43a8-bf3e-cbf7760b90bc
SamAccountName    : svc-SQLReporting
SID               : S-1-5-21-1473643419-774954089-2222329127-1609

distinguishedName : CN=admin,OU=Domain Management,DC=lab,DC=adsecurity,DC=org
name              : admin
objectClass       : user
objectGUID        : f608ef24-72b8-4013-9dda-03008d6fd56a
SamAccountName    : admin
SID               : S-1-5-21-1473643419-774954089-2222329127-1000

distinguishedName : CN=Domain Admins,CN=Users,DC=lab,DC=adsecurity,DC=org
name              : Domain Admins
objectClass       : group
objectGUID        : 66bbe7dd-1a23-4df1-9904-4ea276cdf303
SamAccountName    : Domain Admins
SID               : S-1-5-21-1473643419-774954089-2222329127-512

distinguishedName : CN=Enterprise Admins,CN=Users,DC=lab,DC=adsecurity,DC=org
name              : Enterprise Admins
objectClass       : group
objectGUID        : 833a5827-5d7c-44a7-b5a6-b1b5f6f1d4b1
SamAccountName    : Enterprise Admins
SID               : S-1-5-21-1473643419-774954089-2222329127-519

distinguishedName : CN=Administrator,OU=Domain Management,DC=lab,DC=adsecurity,DC=org
name              : Administrator
objectClass       : user
objectGUID        : bc70c1fd-9513-40d9-9e29-264cface3fcf
SamAccountName    : Administrator
SID               : S-1-5-21-1473643419-774954089-2222329127-500
```

These cmdlets are useful to identify situations that previously required purchasing a product or custom scripting.

The following examples find inactive (stale) computers and users – accounts that haven't changed their passwords in the last 10 days. Note that this is a lab example. For real-world checks, change this to 60 to 90 days for computers and 180 – 365 days for users.

Find inactive computers.

```
PS C:\Windows\system32> $InactiveDate = (get-date).AddDays(-10)
Get-ADComputer -filter {(LastLogonDate -le $InactiveDate) -AND (PasswordLastSet -le $InactiveDate)} -property Name,IPv4Address,`
LastLogonDate,PasswordLastSet,Description,Created,DNSHostName


Created           : 12/7/2014 12:13:35 PM
Description       :
DistinguishedName : CN=ADSWKWIN8,CN=Computers,DC=lab,DC=adsecurity,DC=org
DNSHostName       : ADSWKWin8.lab.adsecurity.org
Enabled           : True
IPv4Address       : 172.16.11.202
LastLogonDate     : 1/6/2015 2:31:23 PM
Name              : ADSWKWIN8
ObjectClass       : computer
ObjectGUID        : ff423c3c-842c-41a2-ba02-0d035364a249
PasswordLastSet   : 1/7/2015 10:58:35 AM
SamAccountName    : ADSWKWIN8$
SID               : S-1-5-21-1473643419-774954089-2222329127-1109
UserPrincipalName :
```

Find inactive users.

```
PS C:\Windows\system32> $InactiveDate = (get-date).AddDays(-15)
Get-ADUser -filter {(LastLogonDate -le $InactiveDate) -AND (PasswordLastSet -le $InactiveDate)} -property SAMAccountName,DisplayName,`
LastLogonDate,PasswordLastSet,Description,Created,UserPrincipalName



Created           : 12/28/2014 7:15:49 PM
Description       :
DisplayName       : svc-SQLAgent01
DistinguishedName : CN=svc-SQLAgent01,OU=Service Accounts,DC=lab,DC=adsecurity,DC=org
Enabled           : True
GivenName         :
LastLogonDate     : 12/28/2014 7:18:02 PM
Name              : svc-SQLAgent01
ObjectClass       : user
ObjectGUID        : eba3c611-6ea6-46bc-b68c-c8f28685e7f5
PasswordLastSet   : 1/3/2015 1:42:01 PM
SamAccountName    : svc-SQLAgent01
SID               : S-1-5-21-1473643419-774954089-2222329127-1606
Surname           :
UserPrincipalName : svc-SQLAgent01@lab.adsecurity.org

Created           : 12/28/2014 7:16:23 PM
Description       :
DisplayName       : svc-SQLDBEngine01
DistinguishedName : CN=svc-SQLDBEngine01,OU=Service Accounts,DC=lab,DC=adsecurity,DC=org
Enabled           : True
GivenName         :
LastLogonDate     : 12/28/2014 7:18:02 PM
Name              : svc-SQLDBEngine01
ObjectClass       : user
ObjectGUID        : 9f05af08-4f2c-4e95-8064-ad7a690ee495
PasswordLastSet   : 1/3/2015 1:43:26 PM
SamAccountName    : svc-SQLDBEngine01
SID               : S-1-5-21-1473643419-774954089-2222329127-1607
Surname           :
UserPrincipalName : svc-SQLDBEngine01@lab.adsecurity.org
```

Enumerate Domain Trusts

```
PS C:\Windows\system32> $DomainDNS = [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain().Name
[array]$ADDomainTrusts = Get-ADObject -Filter {ObjectClass -eq "trustedDomain"} -Properties *
[int]$ADDomainTrustsCount = $ADDomainTrusts.Count

Write-Output "Discovered $ADDomainTrustsCount Trust(s) in $DomainDNS `r"
$ADDomainTrusts | select Name,Created,flatName,instanceType,trustAttributes,trustDirection,securityIdentifier | format-table -auto
Discovered 1 Trust(s) in lab.adsecurity.org

Name            Created            flatName instanceType trustAttributes trustDirection securityIdentifier
----            -------            -------- ------------ --------------- -------------- -----------------
rd.adsecurity.org 1/11/2015 5:09:45 PM ADSECRD            4               8              2 S-1-5-21-3834807805-851291830-904607491
```

Get AD site information.

Note that the Windows 2012 module includes cmdlet for sites (Get-ADReplicationSite (https://technet.microsoft.com/en-us/library/hh852269(v=wps.630).aspx)*).

```
PS C:\Windows\system32> $ADSites = [System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest().Sites
[int]$ADSitesCount = $ADSites.Count
Write-Output "There are $ADSitesCount AD Sites `r"

$ADSites | select-object Name,Domains,Subnets,AdjacentSites,SiteLinks | format-table -AutoSize

There are 1 AD Sites

Name                  Domains             Subnets AdjacentSites SiteLinks
----                  -------             ------- ------------- ---------
Default-First-Site-Name {lab.adsecurity.org} {}      {}            {DEFAULTIPSITELINK}
```

Backup domain GPOs

Note this requires that the Group Policy PowerShell module is installed, which is separate from the Active Directory module.

```
PS C:\Users\Administrator.ADSECMLAB> Backup-GPO -All -Domain "mlab.adsecurity.org" -Path "C:\GPOBackup"


DisplayName     : Default Domain Policy
GpoId           : 31b2f340-016d-11d2-945f-00c04fb984f9
Id              : f64bc902-e7d0-45f5-a702-ac610cf04a4b
BackupDirectory : C:\GPOBackup
CreationTime    : 1/27/2015 8:30:42 PM
DomainName      : mlab.adsecurity.org
Comment         :

DisplayName     : Default Domain Controllers Policy
GpoId           : 6ac1786c-016f-11d2-945f-00c04fb984f9
Id              : 33ddea3b-c539-4b2c-bfe5-2e080f47dea0
BackupDirectory : C:\GPOBackup
CreationTime    : 1/27/2015 8:30:47 PM
DomainName      : mlab.adsecurity.org
Comment         :
```

Find AD Kerberos Service Accounts

```
PS C:\Windows\system32> Get-ADUser -filter {ServicePrincipalName -like "*"} -property serviceprincipalname



DistinguishedName    : CN=krbtgt,CN=Users,DC=lab,DC=adsecurity,DC=org
Enabled              : False
GivenName            :
Name                 : krbtgt
ObjectClass          : user
ObjectGUID           : 6fd9529f-0805-4f3c-bb4d-29ad2ac377ef
SamAccountName       : krbtgt
serviceprincipalname : {kadmin/changepw}
SID                  : S-1-5-21-1473643419-774954089-2222329127-502
Surname              :
UserPrincipalName    :

DistinguishedName    : CN=svc-SQLAgent01,OU=Service Accounts,DC=lab,DC=adsecurity,DC=org
Enabled              : True
GivenName            :
Name                 : svc-SQLAgent01
ObjectClass          : user
ObjectGUID           : eba3c611-6ea6-46bc-b68c-c8f28685e7f5
SamAccountName       : svc-SQLAgent01
serviceprincipalname : {MSSQLSvc/ADSAPPSQL03.lab.adsecurity.org:1433,
                       MSSQLSvc/ADSAPPSQL02.lab.adsecurity.org:1433,
                       MSSQLSvc/ADSAPPSQL01.lab.adsecurity.org:1433}
SID                  : S-1-5-21-1473643419-774954089-2222329127-1606
Surname              :
UserPrincipalName    : svc-SQLAgent01@lab.adsecurity.org

DistinguishedName    : CN=svc-MSSQLServer01,OU=Service Accounts,DC=lab,DC=adsecurity,DC=org
Enabled              : True
GivenName            :
Name                 : svc-MSSQLServer01
ObjectClass          : user
ObjectGUID           : 2260906f-6985-404b-b6ea-fbed5d573bff
SamAccountName       : svc-MSSQLServer01
serviceprincipalname : {MSSQLSvc/adsmswin2k8r2:1433, MSSQLSvc/adsmswin2k8r2.lab.adsecurity.org:1433}
SID                  : S-1-5-21-1473643419-774954089-2222329127-1613
Surname              :
UserPrincipalName    : svc-MSSQLServer01@lab.adsecurity.org
```

Inventory Domain Controllers

Get-ADDomainController–filter * | `select hostname,IPv4Address,IsGlobalCatalog,IsReadOnly,OperatingSystem | `format-table -auto

```
hostname                      IPv4Address  IsGlobalCatalog IsReadOnly OperatingSystem
--------                      -----------  --------------- ---------- ---------------
adsmlabdc1.mlab.adsecurity.org 172.16.16.11           True      False Windows Server 2008 R2 Datacenter
adsmlabdc5.mlab.adsecurity.org 172.16.16.12           True      False Windows Server 2012 R2 Datacenter
```

Get-ADReplicationPartnerMetadata (Windows Server 2012 and newer)

```
Get-ADReplicationPartnerMetadata -Target "adsmlabdc1"


CompressChanges               : False
ConsecutiveReplicationFailures : 0
DisableScheduledSync          : False
IgnoreChangeNotifications     : False
IntersiteTransport            :
IntersiteTransportGuid        :
IntersiteTransportType        : IP
LastChangeUsn                 : 13042
LastReplicationAttempt        : 1/27/2015 9:14:54 PM
LastReplicationResult         : 0
LastReplicationSuccess        : 1/27/2015 9:14:54 PM
Partition                     : DC=mlab,DC=adsecurity,DC=org
PartitionGuid                 : e2e5fdb0-bd05-4c73-8ab8-c28d054a7a2b
Partner                       : CN=NTDS Settings,CN=ADSMLABDC5,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ml
                                ab,DC=adsecurity,DC=org
PartnerAddress                : 326cb425-1ae0-4e46-8a08-9b526cacfaeb._msdcs.mlab.adsecurity.org
PartnerGuid                   : 326cb425-1ae0-4e46-8a08-9b526cacfaeb
PartnerInvocationId           : 86bafa17-f779-4233-9028-f3b688b56bef
PartnerType                   : Inbound
ScheduledSync                 : True
Server                        : adsmlabdc1.mlab.adsecurity.org
SyncOnStartup                 : True
TwoWaySync                    : False
UsnFilter                     : 13042
Writable                      : True
```

Get-ADReplicationPartnerFailure provides information on DC replication failure status.

```
Get-ADReplicationFailure -Target "adsmlabdc1"


FailureCount     : 14
FailureType      : Connection
FirstFailureTime : 1/27/2015 6:32:05 PM
LastError        : 8524
Partner          : CN=NTDS Settings,CN=ADSMLABDC2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=mlab,DC=adsecuri
                   ty,DC=org
PartnerGuid      : 72a1a78e-c1b6-4d15-a066-c8e634220ab9
Server           : adsmlabdc1.mlab.adsecurity.org
```

Get-ADReplicationUptodatenessVectorTable tracks replication status between Domain Controllers.

```
PS C:\Users\Administrator.ADSECMLAB> Get-ADReplicationUpToDatenessVectorTable -Target "adsmlabdc1"


LastReplicationSuccess : 1/27/2015 9:14:54 PM
Partition              : DC=mlab,DC=adsecurity,DC=org
PartitionGuid          : e2e5fdb0-bd05-4c73-8ab8-c28d054a7a2b
Partner                : CN=NTDS Settings,CN=ADSMLABDC5,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=mlab,DC=ad
                         security,DC=org
PartnerInvocationId    : 86bafa17-f779-4233-9028-f3b688b56bef
Server                 : adsmlabdc1.mlab.adsecurity.org
UsnFilter              : 13042

LastReplicationSuccess : 1/27/2015 9:36:54 PM
Partition              : DC=mlab,DC=adsecurity,DC=org
PartitionGuid          : e2e5fdb0-bd05-4c73-8ab8-c28d054a7a2b
Partner                : CN=NTDS Settings,CN=ADSMLABDC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=mlab,DC=ad
                         security,DC=org
PartnerInvocationId    : 74a62edd-53bc-45e0-9ed4-cae49998cc9f
Server                 : adsmlabdc1.mlab.adsecurity.org
UsnFilter              : 21021
```

These examples and more are in these presentation slides: http://adsecurity.org/wp-content/uploads/2015/04/NoVaPowerShellUsersGroup2015-ActiveDirectoryPowerShell.pdf (https://adsecurity.org/wp-content/uploads/2015/04/NoVaPowerShellUsersGroup2015-ActiveDirectoryPowerShell.pdf)

(Visited 35,058 times, 7 visits today)

- Active Directory PowerShell Module (https://adsecurity.org/?tag=active-directory-powershell-module), Active Directory Trusts (https://adsecurity.org/?tag=active-directory-trusts), AD cmdlets (https://adsecurity.org/?tag=ad-cmdlets), AD PowerShell cmdlets (https://adsecurity.org/?tag=ad-powershell-cmdlets), Add-WindowsFeature RSAT-AD-PowerShell (https://adsecurity.org/?tag=add-windowsfeature-rsat-ad-powershell), ADSI (https://adsecurity.org/?tag=adsi), Backup domain GPOs (https://adsecurity.org/?tag=backup-domain-gpos), Enumerate Domain Trusts (https://adsecurity.org/?tag=enumerate-domain-trusts), Find AD Kerberos Service Accounts (https://adsecurity.org/?tag=find-ad-kerberos-service-accounts), Finding Active Directory Flexible Master Single Operation (FSMO) Roles (https://adsecurity.org/?tag=finding-active-directory-flexible-master-single-operation-fsmo-roles), Get AD site information. (https://adsecurity.org/?tag=get-ad-site-information), Get-ADComputer (https://adsecurity.org/?tag=get-adcomputer), Get-ADDomain (https://adsecurity.org/?tag=get-addomain), Get-ADDomainController (https://adsecurity.org/?tag=get-addomaincontroller), Get-ADForest (https://adsecurity.org/?tag=get-adforest), Get-ADGroup (https://adsecurity.org/?tag=get-adgroup), Get-ADGroupMember (https://adsecurity.org/?tag=get-adgroupmember), Get-ADReplicationPartnerFailure (https://adsecurity.org/?tag=get-adreplicationpartnerfailure), Get-ADReplicationPartnerMetadata (https://adsecurity.org/?tag=get-adreplicationpartnermetadata), Get-ADReplicationUptodatenessVectorTable (https://adsecurity.org/?tag=get-

adreplicationuptodatenessvectortable), Get-ADUser (https://adsecurity.org/?tag=get-aduser), Get-Command -module ActiveDirectory (https://adsecurity.org/?tag=get-command-module-activedirectory), Get-Module -ListAvailable (https://adsecurity.org/?tag=get-module-listavailable), Get-RootDSE (https://adsecurity.org/?tag=get-rootdse), Import-Module ServerManager (https://adsecurity.org/?tag=import-module-servermanager), Inventory Domain Controllers (https://adsecurity.org/?tag=inventory-domain-controllers), PowerShell (https://adsecurity.org/?tag=powershell), PowerShell Find inactive computers (https://adsecurity.org/?tag=powershell-find-inactive-computers), PowerShell Find inactive users (https://adsecurity.org/?tag=powershell-find-inactive-users)

(https://adsecurity.org/?author=2)

Sean Metcalf

I improve security for enterprises around the world working for TrimarcSecurity.com
Read the About page (top left) for information about me. :)
https://adsecurity.org/?page_id=8

(mailto:sean@adsecurity.org)

4 comments

Skip to comment form

1. Mitch Impey on August 11, 2017
   # (https://adsecurity.org/?p=3719#comment-13203)
   Hi Sean, I have benefited from your expertise for many years. Thanks very much !

2. SS on August 11, 2017
   # (https://adsecurity.org/?p=3719#comment-13204)
   Is there a way to prevent authenticated folks who are not authorized from running these commands?

   1. Sean Metcalf (https://ADSecurity.org) on August 14, 2017
      Author
      # (https://adsecurity.org/?p=3719#comment-13215)
      Not built-in and working to get these blocked would be non-trivial. Not that this is the same type of data that authenticated users can gather via LDAP.
      Check out the PowerShell module “PowerView”:

https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon (https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon)

2. 
   - Joonas on August 17, 2017
   - # (https://adsecurity.org/?p=3719#comment-13229)

   There is a way to prevent cmdlets or functions for PS remote session. Look at Securing Privileged Access document from Microsoft. From there look at Just enough admin and you find how to restrict PS usage

💬 Comments have been disabled.

Recent Posts

- Attacking Active Directory Group Managed Service Accounts (GMSAs) (https://adsecurity.org/?p=4367)
- From Azure AD to Active Directory (via Azure) – An Unanticipated Attack Path (https://adsecurity.org/?p=4277)
- What is Azure Active Directory? (https://adsecurity.org/?p=4211)
- Slides Posted for Black Hat USA 2019 Talk: Attacking & Defending the Microsoft Cloud (https://adsecurity.org/?p=4179)
- AD Reading: Windows Server 2019 Active Directory Features (https://adsecurity.org/?p=4187)

Trimarc Active Directory Security Services

Have concerns about your Active Directory environment? Trimarc helps enterprises improve their security posture. Find out how... (http://trimarcsecurity.com/security-services) TrimarcSecurity.com

Popular Posts

- Attack Methods for Gaining Domain Admin Rights in… (https://adsecurity.org/?p=2362)
- PowerShell Encoding & Decoding (Base64) (https://adsecurity.org/?p=478)
- Securing Domain Controllers to Improve Active… (https://adsecurity.org/?p=3377)
- Kerberos & KRBTGT: Active Directory's… (https://adsecurity.org/?p=483)
- Finding Passwords in SYSVOL & Exploiting Group… (https://adsecurity.org/?p=2288)
- Securing Windows Workstations: Developing a Secure Baseline (https://adsecurity.org/?p=3299)
- The Most Common Active Directory Security Issues and… (https://adsecurity.org/?p=1684)
- Building an Effective Active Directory Lab… (https://adsecurity.org/?p=2653)
- Microsoft Local Administrator Password Solution (LAPS) (https://adsecurity.org/?p=1790)
- Mimikatz DCSync Usage, Exploitation, and Detection (https://adsecurity.org/?p=1729)

Categories

- ActiveDirectorySecurity (https://adsecurity.org/?cat=565)
- Apple Security (https://adsecurity.org/?cat=55)
- Cloud Security (https://adsecurity.org/?cat=431)

- Continuing Education (https://adsecurity.org/?cat=17)
- Entertainment (https://adsecurity.org/?cat=396)
- Exploit (https://adsecurity.org/?cat=347)
- Hacking (https://adsecurity.org/?cat=1039)
- Hardware Security (https://adsecurity.org/?cat=168)
- Hypervisor Security (https://adsecurity.org/?cat=172)
- Linux/Unix Security (https://adsecurity.org/?cat=126)
- Malware (https://adsecurity.org/?cat=343)
- Microsoft Security (https://adsecurity.org/?cat=11)
- Mitigation (https://adsecurity.org/?cat=819)
- Network/System Security (https://adsecurity.org/?cat=48)
- PowerShell (https://adsecurity.org/?cat=7)
- RealWorld (https://adsecurity.org/?cat=698)
- Security (https://adsecurity.org/?cat=21)
- Security Conference Presentation/Video (https://adsecurity.org/?cat=234)
- Security Recommendation (https://adsecurity.org/?cat=1045)
- Technical Article (https://adsecurity.org/?cat=24)
- Technical Reading (https://adsecurity.org/?cat=4)
- Technical Reference (https://adsecurity.org/?cat=2)
- TheCloud (https://adsecurity.org/?cat=156)
- Vulnerability (https://adsecurity.org/?cat=930)

Tags

ActiveDirectory (https://adsecurity.org/?tag=activedirectory) Active Directory (https://adsecurity.org/?tag=active-directory) ActiveDirectoryAttack (https://adsecurity.org/?tag=activedirectoryattack) ActiveDirectorySecurity (https://adsecurity.org/?tag=activedirectorysecurity) Active Directory Security (https://adsecurity.org/?tag=active-directory-security) ADReading (https://adsecurity.org/?tag=adreading) ADSecurity (https://adsecurity.org/?tag=adsecurity) AD Security (https://adsecurity.org/?tag=ad-security) DCSync (https://adsecurity.org/?tag=dcsync) DEFCON (https://adsecurity.org/?tag=defcon) DomainController (https://adsecurity.org/?tag=domaincontroller) EMET5 (https://adsecurity.org/?tag=emet5) GoldenTicket (https://adsecurity.org/?tag=goldenticket) HyperV (https://adsecurity.org/?tag=hyperv) Invoke-Mimikatz (https://adsecurity.org/?tag=invoke-mimikatz) KB3011780 (https://adsecurity.org/?tag=kb3011780) KDC (https://adsecurity.org/?tag=kdc) Kerberos (https://adsecurity.org/?tag=kerberos) KerberosHacking (https://adsecurity.org/?tag=kerberoshacking) KRBTGT (https://adsecurity.org/?tag=krbtgt) LAPS (https://adsecurity.org/?tag=laps) LSASS (https://adsecurity.org/?tag=lsass) MCM (https://adsecurity.org/?tag=mcm) MicrosoftEMET (https://adsecurity.org/?tag=microsoftemet) MicrosoftWindows (https://adsecurity.org/?tag=microsoftwindows) mimikatz (https://adsecurity.org/?tag=mimikatz) MS14068 (https://adsecurity.org/?tag=ms14068) PassTheHash (https://adsecurity.org/?tag=passthehash) PowerShell (https://adsecurity.org/?tag=powershell)

PowerShellCode (https://adsecurity.org/?tag=powershellcode) PowerShellHacking (https://adsecurity.org/?tag=powershellhacking) PowerShellv5 (https://adsecurity.org/?tag=powershellv5) PowerSploit (https://adsecurity.org/?tag=powersploit) Presentation (https://adsecurity.org/?tag=presentation) Security (https://adsecurity.org/?tag=security) SIDHistory (https://adsecurity.org/?tag=sidhistory) SilverTicket (https://adsecurity.org/?tag=silverticket) SneakyADPersistence (https://adsecurity.org/?tag=sneakyadpersistence) SPN (https://adsecurity.org/?tag=spn) TGS (https://adsecurity.org/?tag=tgs) TGT (https://adsecurity.org/?tag=tgt) Windows10 (https://adsecurity.org/?tag=windows10) WindowsServer2008R2 (https://adsecurity.org/?tag=windowsserver2008r2) WindowsServer2012 (https://adsecurity.org/?tag=windowsserver2012) WindowsServer2012R2 (https://adsecurity.org/?tag=windowsserver2012r2)

Copyright

Content Disclaimer: This blog and its contents are provided "AS IS" with no warranties, and they confer no rights. Script samples are provided for informational purposes only and no guarantee is provided as to functionality or suitability. The views shared on this blog reflect those of the authors and do not represent the views of any companies mentioned.