Managing and troubleshooting Active Directory using cmd and PowerShell

Version 22.9

Ahmed Abdelwahed
Microsoft MCT
ahmed@abdelwahed.me

Table of Contents

Get all installed features 3
Install AD DS Role using PowerShell 3
Install **abdelwahed.me** Domain using PowerShell 3
Get Active Directory (AD) Domain and Forest functional level 3
Get and transfer FSMO Roles 3
Check replication status and summary 3
Show which DCclient authenticate from 3
Create OUs, Groups, Users and add users to groups using cmd (Batch) 4
Get users in abc OU and change all users password 5
Export Active Directory Users information using PowerShell 5
Get last login date for all users 5
Get user last password changes 6
Get and disable inactive users (doesn't login 6 months ago) using PowerShell 6
Find and remove computers that not login 8 weeks ago using cmd 6
Find and remove disabled computers using cmd 6
Find and remove users that not login 8 weeks ago using cmd 6
Find and remove disabled users using cmd 6
disable the inactive computers/users using cmd 6
Count all enabled users 6
Convert security group to Distribution using cmd 6
Convert Distribution to security group using cmd 6
Reset default domain policy 6
Set IPv4 as preferred 6
Solve The trust relationship between this workstation and the domain failed 7
Resolve incorrect time with Windows Domain Controller 7
Open different AD Administrative Tools using cmd or PS 7

Managing and troubleshooting Active Directory using cmd and PowerShell

This Lab help system admins to configure and manage Active Directory daily tasks through command line and PowerShell in a fast and easy way.

Note: in this lab the domain name is **abdelwahed.me**

Get all installed features

```
Get-WindowsFeature | where installed
```

Install AD DS Role using PowerShell

```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
```

Install abdelwahed.me Domain using PowerShell

```
Install-ADDSDomainController –NoGlobalCatalog:$true –CreateDnsDelegation:$false –Credential (Get-Credential) –CriticalReplicationOnly:$false –DatabasePath “C:\Windows\NTDS” –DomainName “abdelwahed.me” –InstallDns:$false –LogPath “C:\Windows\NTDS” –NoRebootonMepletion:$false –SiteName “Default-First-Site-Name” –SysvolPath “C:\Windows\SYSVOL” –Force:$true
```

Get Active Directory (AD) Domain and Forest functional level

```
(Get-ADForest).ForestMode
```

```
(Get-ADDomain).DomainMode
```

Get and transfer FSMO Roles

```
NetDOM /query FSMO
```

```
Move-ADDirectoryServerOperationMasterRole -Identity "DC1" -OperationMasterRole SchemaMaster,RIDMaster,InfrastructureMaster,DomainNamingMaster,PDCEmulator
```

Also you can force this operation in case of FSMO Role server down

```
Move-ADDirectoryServerOperationMasterRole -Identity "Target-DC" -OperationMasterRole 0,1,2,3,4 -Force
```

Check replication status and summary

```
Dcdiag
```

```
Dcdiagrepadmin /replsum
```

```
repadmin /showreps
```

Show which DCclient authenticate from

```
nltest /dsgetdc:abdelwahed.me
```

Create OUs, Groups, Users and add users to groups using cmd (Batch)

Save the following lines in one batch file (.bat)

```
dsadd ou "ou=IT,dc=abdelwahed,dc=me"
dsadd ou "ou=HR,dc=abdelwahed,dc=me"
dsadd ou "ou=Sales,dc=abdelwahed,dc=me"
dsadd ou "ou=Markting,dc=abdelwahed,dc=me"
dsadd ou "ou=QA,dc=abdelwahed,dc=me"
dsadd group "cn=IT_Gr,ou=IT,dc=abdelwahed,dc=me"
dsadd group "cn=HR_Gr,ou=HR,dc=abdelwahed,dc=me"
dsadd group "cn=Sales_Gr,ou=Sales,dc=abdelwahed,dc=me"
dsadd group "cn=Markting_Gr,ou=Markting,dc=abdelwahed,dc=me"
dsadd group "cn=QA_Gr,ou=QA,dc=abdelwahed,dc=me"
dsadd user "cn=IT01,ou=IT,dc=abdelwahed,dc=me" - dept IT -pwd Yat@2015
dsadd user "cn=IT02,ou=IT,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=IT03,ou=IT,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=IT04,ou=IT,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=IT05,ou=IT,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=HR01,ou=HR,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=HR02,ou=HR,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=HR03,ou=HR,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=HR04,ou=HR,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=HR05,ou=HR,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=Sales01,ou=Sales,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=Sales02,ou=Sales,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=Sales03,ou=Sales,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=Sales04,ou=Sales,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=Sales05,ou=Sales,dc=abdelwahed,dc=me" -pwd Yat@2015
```

```
dsadd user "cn=Markting01,ou=Markting,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=Markting02,ou=Markting,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=Markting03,ou=Markting,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=Markting04,ou=Markting,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=Markting05,ou=Markting,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=QA01,ou=QA,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=QA02,ou=QA,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=QA03,ou=QA,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=QA04,ou=QA,dc=abdelwahed,dc=me" -pwd Yat@2015
dsadd user "cn=QA05,ou=QA,dc=abdelwahed,dc=me" -pwd Yat@2015
dsquery user ou=IT,dc=abdelwahed,dc=me |dsmod group cn=IT_Gr,ou=hr,dc=abdelwahed,dc=me -addmbr
dsquery user ou=HR,dc=abdelwahed,dc=me |dsmod group cn=HR_Gr,ou=hr,dc=abdelwahed,dc=me -addmbr
dsquery user ou=Sales,dc=abdelwahed,dc=me |dsmod group cn=Sales_Gr,ou=hr,dc=abdelwahed,dc=me -addmbr
dsquery user ou=Markting,dc=abdelwahed,dc=me |dsmod group cn=Markting_Gr,ou=hr,dc=abdelwahed,dc=me -addmbr
dsquery user ou=QA,dc=abdelwahed,dc=me |dsmod group cn=QA_Gr,ou=hr,dc=abdelwahed,dc=me -addmbr
```

Get users in abc OU and change all users password

1-Using cmd

```
dsquery user “ou=abc,dc=abdelwahed,dc=me” -limit 0 | dsmod user -pwd Learn@2022
```

2-Using PowerShell

```
Get-ADUser -SearchBase "ou=students,dc= abdelwahed,dc=me" | Set-ADAccountPassword -Reset -NewPassword
(ConvertTo-SecureString -AsPlainText "Learn@2022" -Force)
```

Export Active Directory Users information using PowerShell

```
Get-ADUser -Filter * -Properties GivenName,Surname,Title,Department,City,AccountExpirationDate | Export-csv c:\Ad.csv
Get-ADUser -Filter *| Export-csv c:/users.csv
Get-ADUser -searchbase "ou=abc,dc=abdelwahed,dc=me" -Filter *| Export-csv c:/users.csv
```

Get last login date for all users

```
get-aduser -f * -pr lastlogondate|sort -property lastlogondate|ft samaccountname,lastlogondate -auto
```

Managing and troubleshooting Active Directory using cmd and PowerShell

---

Get user last password changes

```
Get-ADUser -Identity a.abdelwahed -Properties * -Server ruh-dc05 | Select PasswordLastSet
```

Get and disable inactive users (doesn't login 6 months ago) using PowerShell

```
search-adaccount -accountinactive -usersonly -timespan "180" | Disable-ADAccount
```

Find and remove computers that not login 8 weeks ago using cmd

```
dsquery computer -inactive 8 -limit 0 | dsrm -noprompt
```

Find and remove disabled computers using cmd

```
dsquery computer –disabled | dsrm -noprompt
```

Find and remove users that not login 8 weeks ago using cmd

```
dsquery user -inactive 8 -limit 0 | dsrm -noprompt
```

Find and remove disabled users using cmd

```
dsquery user –disabled | dsrm -noprompt
```

disable the inactive computers/users using cmd

```
dsquery computer -inactive 7 | dsmod computer –disabled yes
```

Count all enabled users

```
(Get-ADUser -Filter *|where {$_.enabled -eq "True"}).count
```

Convert security group to Distribution using cmd

```
dsmod group cn=it,ou=it,dc=abdelwahed,dc=me -secgrp no
```

Convert Distribution to security group using cmd

```
dsmod group cn=it,ou=it,dc=abdelwahed,dc=me -secgrp yes
```

Reset default domain policy

```
 DCGPOFIX /target:dc

DCGPOFIX /target:domain

DCGPOFIX /target:both
```

Set IPv4 as preferred

```
netsh interface ipv6 set prefixpolicy ::ffff:0:0/96 50 0
```

Solve The trust relationship between this workstation and the domain failed

- Winows Server

```
netdom resetpwd /s:dc.abdelwahed.me /ud:dn\administrator /pd:*
```

- Windows Client

```
$credential = Get-Credential
```

```
Reset-ComputerMachinePassword -server dc.abdelwahed.me -credential $credential
```

- in case not work download following link

Windows Management Framework 4.0

Resolve incorrect time with Windows Domain Controller

- Domain Side (PowerShell)

```
net stop w32time
```

```
w32tm /config /syncfromflags:manual /manualpeerlist:"0.asia.pool.ntp.org, 1.asia.pool.ntp.org, 2.asia.pool.ntp.org"
```

```
w32tm /config /reliable:yes
```

```
net start w32time
```

```
w32tm /query /configuration
```

- Client Side (cmd as admin)

```
w32tm /resync
```

Open different AD Administrative Tools using cmd or PS

AD Domains and Trusts

```
domain.msc
```

AD Sites and Services

```
dssite.msc
```

AD Users and Meputers

```
dsa.msc
```

ADSI Edit

```
adsiedit.msc
```

Certification Authority Management

```
certsrv.msc
```

Device Manager
devmgmt.msc

DHCP Managment
dhcpmgmt.msc

Disk Manager
diskmgmt.msc

Distributed File System
dfsgui.msc

DNS Managment
dnsmgmt.msc

Event Viewer
eventvwr.msc

Local Group Policy Editor
gpedit.msc

Local Security Settings Manager
secpol.msc

Local Users and Groups Manager
lusrmgr.msc

Network Load balancing
nlbmgr.exe

Performance Montior
perfmon.msc

Routing and Remote Access Manager
rrasmgmt.msc

Schema management
schmmgmt.msc

Services Management
services.msc

Shared Folders

fsmgmt.msc