

Oefening 4:

ACTIVE DIRECTORY BEHEER

1. Aanmaken van een Organizational Unit structuur

De Organizational Unit structuur van een domein wordt gebruikt voor 3 redenen:

- Gemakkelijk objecten terugvinden in de dikwijls grote Active Directory structuur.
- Toepassen van Group Policies op een OU.
- Delegeren van administratieve controle over een OU

Vooraf deze laatste 2 redenen zijn meestal doorslaggevend voor de OU-structuur van een bedrijf.

In het fictieve bedrijf dat we in deze cursus gebruiken is volgende bedrijfsstructuur te vinden:

- Ontwikkeling
- Boekhouding dat bestaat uit 2 delen:
 - Inkomsten
 - Uitgaven
- Marketing
- IT
- HR dat bestaat uit 2 delen:
 - Aanwerving
 - Personeelsdienst

Aangezien we in de toekomst Group Policies zullen instellen die van departement tot departement zullen verschillen, kunnen we best deze structuur aanmaken aan de hand van OU's. Open dus de Administrative Tool "Active Directory Users and Computers" en maak hierin bovenstaande structuur aan met behulp van OU's.

2. Aanmaken van user accounts

Om de OU structuur die je hierboven hebt aangemaakt te vullen met realistische accounts, maken we de volgende gebruikers aan, telkens met paswoord 'Student1', en de eigenschap 'User must change password at next logon' uitgevinkt:

- In departement ontwikkeling
 - Gebruiker An Verstraete met als logon-name an
 - Gebruiker Jos Peeters met als logon-name jos
- In departement boekhouding
 - Gebruiker Marc Hanno met als logon-name marc
 - Vul als Job Title via de properties in: Financieel directeur
 - Gebruiker Anita Haemers met als logon-name anita
 - Maak deze gebruiker aan in het subdepartement Inkomsten
 - Gebruiker Peter Delaet met als logon-name peter
 - Maak deze gebruiker aan in het subdepartement Uitgaven
- In departement marketing

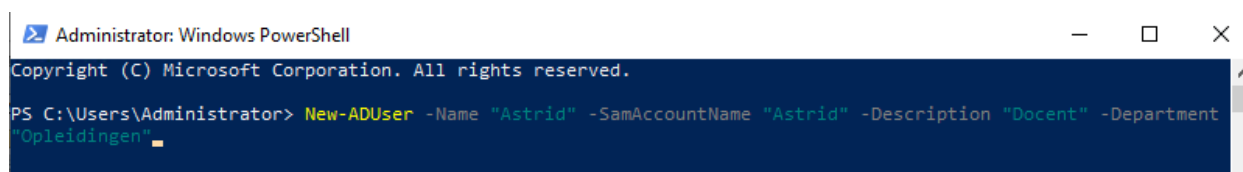
- Gebruiker Mia Vandekastele met als logon-name mia
- In departement IT
 - Gebruiker Hans Vandepoel met als logon-name hans
- In departement HR
 - Gebruiker Sharon Smith met als logon-name sharon
 - Maak deze gebruiker aan in het subdepartement Aanwerving
 - Gebruiker Ali El Haddouchi met logon-name ali
 - Maak deze gebruiker aan in het subdepartement Personeelsdienst

3. Aanmaken van user accounts via een csv-bestand

Omdat er heel wat nieuwe mensen werden aangenomen binnen het departement Human Resources, willen we het aanmaken van nieuwe gebruikers graag gaan automatiseren. Om meerdere gebruikers tegelijk toe te voegen in Active Directory, maken we best gebruik van een script. Aan de hand van een comma-separated-value bestand kunnen we ineens vele gebruikers in Active Directory aanmaken. Het .csv-bestand is te vinden via de EhB-fileserver (zie het bestand "Server OS - Logingegevens en locaties").

1. Open Powershell (of Visual Studio Code) en laadt vervolgens de AD module in via de cmdlet
Import-Module ActiveDirectory
2. Zorg ervoor dat het toegelaten is om scripts uit te voeren.

Let op, de commando's zoals hieronder weergegeven zijn copy-paste klaar. Het is echter aan te raden deze manueel in te typen zodat je vertrouwd geraakt met de syntax. Doordat de commando's copy-paste moesten zijn in weergave, kan het zijn dat sommige commando's vreemd worden weergegeven, zoals hieronder. Het koppelteken "-" op het einde van de eerste regel moet eigenlijk voor "Departement" staan in de 2^{de} regel, zonder spatie. Dit geeft dan "-Departement". Of zoals het de bedoeling is in 1 lang commando:



Probeer nu zelf een gebruiker manueel aan te maken via Powershell.

```
New-ADUser -Name "Astrid" -SamAccountName "Astrid" -Description "Docent" -  
Department "Opleidingen"
```

Aangezien we niet hebben gespecificeerd in welke OU deze gebruiker dient aangemaakt te worden, zal deze in de default OU worden geplaatst, zijnde "Users".

Je kan dit ook iets uitgebreider doen, met meer parameters: (Let wel, je zal de naam van jouw_domeinnaam eerst moeten vervangen met jouw domeinnaam)

```
New-ADUser -Name "Astrid" -SamAccountName "astrid.decoester" -Description  
"Docent" -Department "Opleidingen" -Path "OU=sales, DC=[jouw_domeinnaam],  
DC=local" -Enabled $true -PasswordNotRequired $true
```

Bovenstaande commando maakt een user aan zonder paswoord in de OU sales. Merk ook op dat je 2 users kan aanmaken met dezelfde naam. Dit komt door de unieke SID's die aan elk AD-object wordt gekoppeld.

Wil je er nadien nog een paswoord aan toevoegen:

```
Get-ADUser astrid | Set-ADAccountPassword -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "Student1" -Force)
```

Haal het bestand nieuwegebruikers.csv af van de share zoals hierboven beschreven. Open het bestand en bekijk welke gebruikers je allemaal moet aanmaken. Bekijk de optionele velden. Probeer uit. Probeer nadien een aantal extra velden toe te voegen (bijvoorbeeld emailadres, enz). Verwijder wel eerst de users via AD Users en Computers of via PowerShell, want ze worden niet automatisch overschreven. (lees eerst de opdracht verder hieronder.)

Zorg ervoor dat de users uit het csv-bestand worden aangemaakt in de nieuwe (eerst manueel aangemaakte) OU 'csv-users' onder de root van uw Active Directory. Hiervoor zal je een parameter moeten aanpassen in 'Path'. Let wel, je zal de naam van jouw_domeinnaam eerst moeten vervangen met jouw domeinnaam. Let ook op het pad van het bestand nieuwegebruikers.csv.

```
Import-csv c:\nieuwegebruikers.csv | foreach {New-ADUser -SamAccountName $_.samaccountname -GivenName $_.givenname -Surname $_.surname -Name $_.name -DisplayName $_.Displayname -Path 'OU=Users,DC=[jouw_domeinnaam],DC=local' }
```

Uitvoeren van wijzigingen op grote groepen gebruikers

Er werd in een vergadering beslist dat voor elke gebruikersaccount van je domein het Company veld van elke gebruiker ingesteld moet worden op "Erasmushogeschool Brussel".

Aangezien het enorm tijdrovend zou zijn om dit manueel per gebruiker te gaan nakijken, maken we opnieuw gebruik van een script om dit meteen op alle gebruikers uit te voeren. Je kan dit ook toepassen door dit als .ps1 extensie op te slaan in de ingebouwde IDE van Powershell, of beter nog, gebruik te maken van Visual Studio Code met de Powershell extensie, de uitgelezen omgeving voor powershell scripting.

```
$ADUsers = Get-ADUser -Filter *  
  
foreach($ADUser in $ADUsers)  
{  
    $ADUser.company = "Erasmushogeschool Brussel"  
    Set-ADUser -Instance $ADUser  
}
```

4. Groepen & File Sharing

In ons bedrijf zullen de gebruikers toegang nodig hebben tot bepaalde resources: shares, printers, databases, ... Bouw zelf een groepsstructuur op volgens het AGDLP principe, om onderstaande structuur te verwezenlijken. Maak ALLE groepen aan in een nieuwe OU 'groepen' onder de root van je Active Directory domein. Lees eerst goed de hele tekst voor je aan de slag gaat.

Gebruik volgende naming convention:

- **Domain Local groups:** [naam_van_de_folder]-[afkorting_recht]
Bijvoorbeeld folderx-R, folderx-W, folderx-FC
- **Global groups:** gebruik de naam van het het profiel dat uw users gemeenschappelijk hebben
Bijvoorbeeld Marketing
- **Folders:** gebruik de exacte benamingen van de folders zoals beschreven in de opdracht

Belangrijk: wanneer het niet expliciet vermeld staat, zal een gebruiker geen rechten krijgen op een share. We gaan er dus van uit dat niemand op een share iets kan lezen of schrijven, tenzij anders vermeld.

Opgelet: voor een goede manier van werken, zetten we de sharerechten voor “everyone” op “full control” op onze basis ‘C:\Shared’ folder, en stellen we de rechten in via NTFS-security (tabblad “security”).

Voor de C:\Shared folder is het een goed idee om alle gebruikers ook leesrechten te geven om de folder zelf, maar niet op de subfolders ervan. Hiervan kan je best alle (grote) global groups lid maken van een nieuwe global group “alle_gebruikers”, en deze dan lid maken van een domain local group Shared-R, die dan op zijn beurt Read&Execute permissies heeft op de Shared folder, maar niet op de subfolders ervan. Dit kan je instellen door in de Security ACL van deze folder op Advanced te klikken, en bij “Applies to” “This folder only” te selecteren. Indien je deze laatste instelling niet zou aanpassen, heb je alle gebruikers leesrechten gegeven op alle data van je bedrijf, wat uiteraard een zware fout is.

Voorzie volgende rechten op je file-server:

- Op dc1 staat onder “C:\Shared” een folder **informatica_docs**, waarop heel wat interessante documentatie over het netwerk wordt gedeeld. Enkel de gebruikers uit het departement IT krijgen lees- en schrijfrechten op deze share, al de andere gebruikers enkel leesrechten.
- Op dc1 staat onder “C:\Shared” een folder **ziekte_verlof**, waarop de gebruikers van personeelsdienst lees- en schrijfrechten hebben en waarop alle andere gebruikers leesrechten hebben.
- Op de dc1 staat onder “C:\Shared” een folder **finance_docs** waarop de gebruikers van de departementen inkomsten en uitgaven documenten kunnen afhalen (enkel lezen dus) die enkel door Marc Hanno (financieel directeur) op deze share gezet kunnen worden.
- Op dc1 staat onder “C:\Shared” een folder **finance_incoming** waarop de gebruikers van het departement inkomsten documenten kunnen delen rond binnenkomende bestellingen en betalingen.
- Op dc1 staat onder “C:\Shared” een folder **ontwikkeling** waarop de gebruikers van de afdeling ontwikkeling lees- en schrijfrechten hebben om hun recentste ontwikkelingen op te kunnen uitwisselen.

Voor het aanmaken van de shares voer je het volgende uit:

1. Ga naar dc1
2. Open Explorer
3. Maak een nieuwe map “Shared” aan onder de root van C:
4. Ga naar de properties van deze map
5. Ga naar het tabblad sharing, advanced sharing.
 - i. Kies share this folder en kies een sharenaam.
 - ii. Kies “Permissions” en geef Everyone een allow op *Full Control*.
6. Ga naar het tabblad security en configureer hier de gevraagde rechten.

Je kan ook een share aanmaken en beheren via de Server Manager, File Services, Share and Storage Management.

Indien je bestaande rechten niet kan verwijderen of wijzigen, dan staat inheritance aan. Je kan de rechten instellen via het security-tabblad. Klik eerst op Advanced, vervolgens op Disable Inheritance. Nadien kan je de keuze maken of je de overgeërfde rechten wil kopiëren (met bijgevolg de mogelijkheid om ze aan te passen) of verwijderen. Je zal dit moeten doen op C:\Shared enkel “CREATOR OWNER”, “SYSTEM” en “Administrators” behouden.

Bovenaan zie je Owner, de werkelijke eigenaar van het bestand of de map. Ownership kan je overnemen, bijvoorbeeld als admin.

Op het tabblad Effective Permissions kan je de effectieve permissies voor een bepaalde gebruiker nakijken. Op die manier ben je echt zeker van welke rechten die bepaalde gebruiker heeft. Dit kan ondermeer van pas komen als er rechten zijn ingesteld op verschillende groepen waarvan die specifieke gebruiker lid is.

Test je configuratie door aan te loggen met een gebruiker van een bepaalde groep op je client-computer en na te kijken of deze gebruiker de correcte rechten heeft op de folder, niet meer, niet minder. Indien je merkt dat je problemen blijft hebben, zet dan zelf een extra testconfiguratie verder op en test grondig tot je het volledig onder de knie hebt.