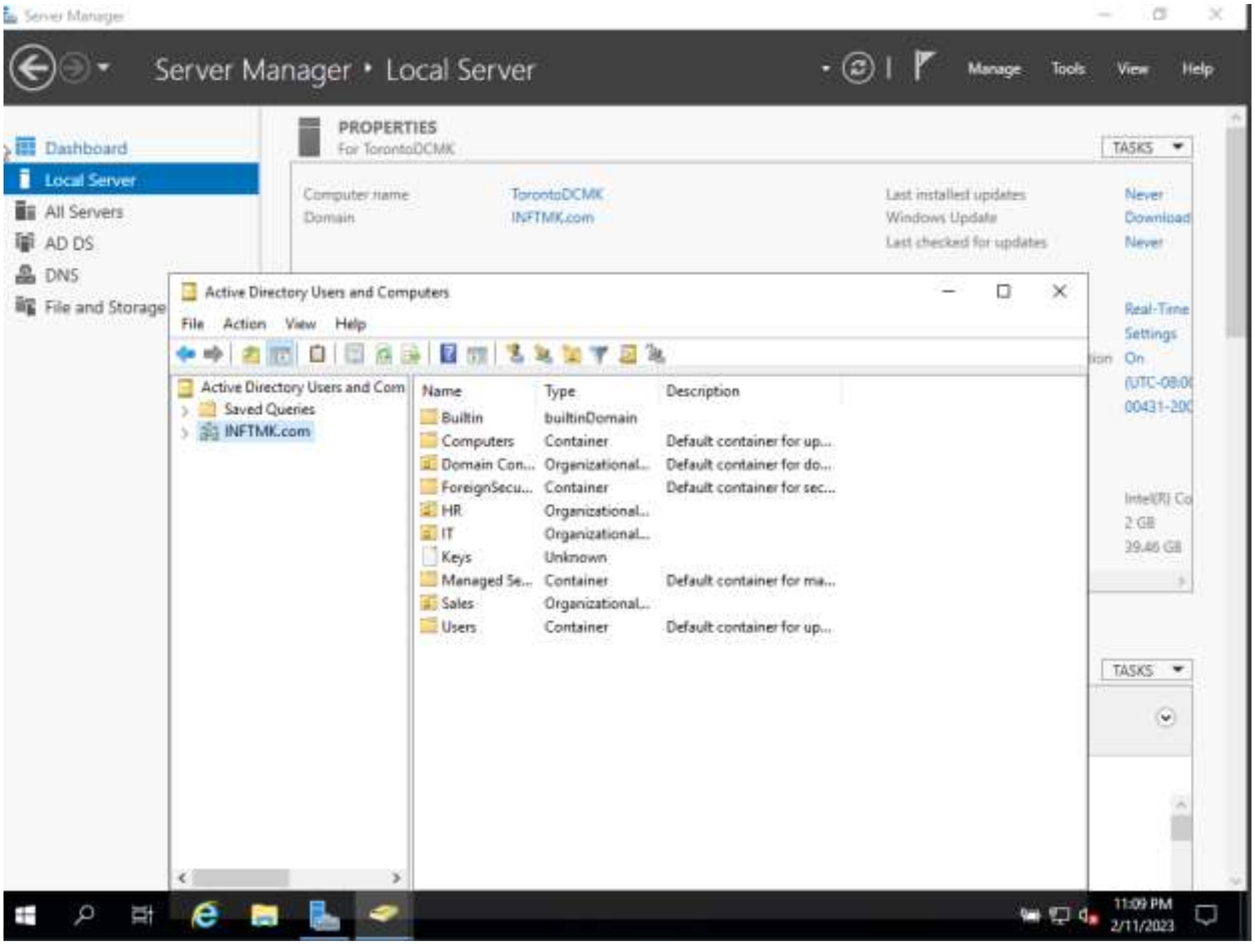
Use GUI for the following steps:

Part 1A: Creating and Managing Groups and OU's using GUI

On the **Toronto Domain Controller**

1. Log in as the **Domain Administrator** account
2. Open **Active Directory Users and Computers**
3. Create the following **OUs** directly under the Domain Object:
   - HR
   - Sales
   - IT

Take a screenshot of the OUs

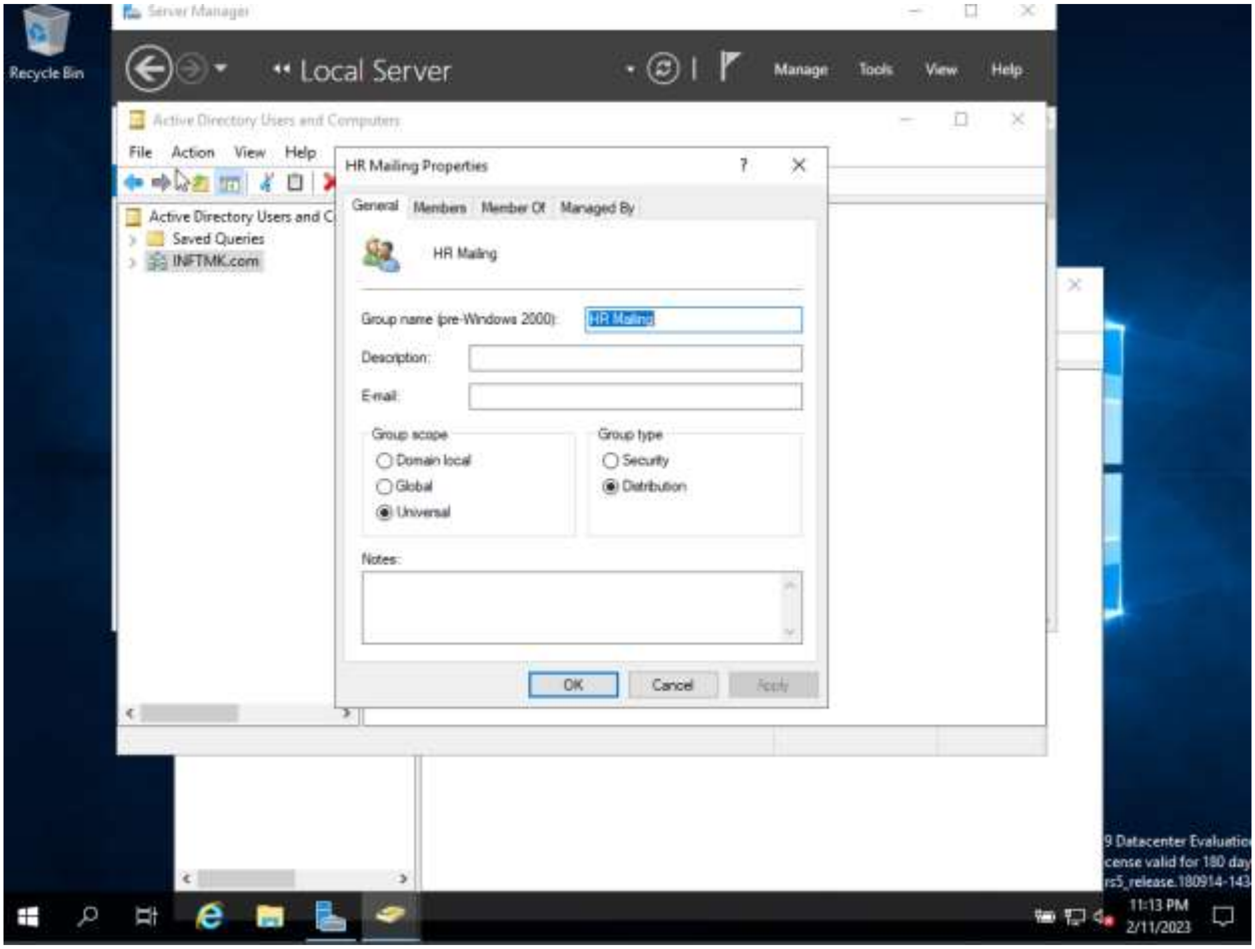


Computer name TorontoDCMK
Domain INFTMK.com
Last installed updates Never
Windows Update Download
Last checked for updates Never

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
HR	Organizational...	
IT	Organizational...	
Keys	Unknown	
Managed Se...	Container	Default container for ma...
Sales	Organizational...	
Users	Container	Default container for up...

4. Open the **Groups OU**
5. Create a **Distribution Group** named **HR Mailing** within the Groups OU
    - Scope: Universal
    - Type: Distribution
6. Right click the **HR Mailing** group and select *Properties*

Take a screenshot of the contents within the *General* tab before clicking "OK"



HR Mailing

Group name (pre-Windows 2000): HR Mailing

Description:

E-mail:

Group scope
○ Domain local
○ Global
● Universal

Group type
○ Security
● Distribution

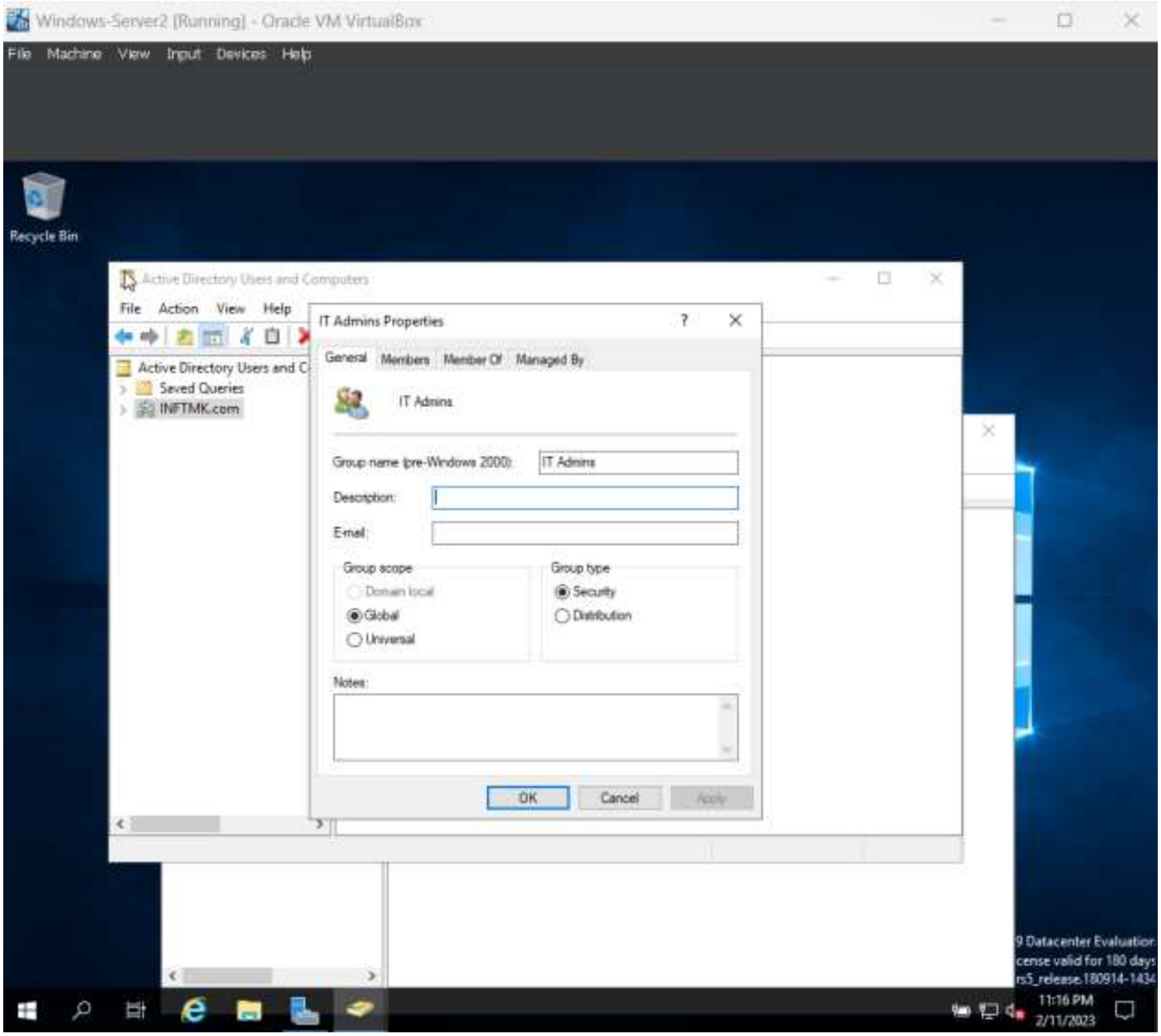
Notes:

7. Create a **Security Group** named **IT Admins** within the Groups OU
    - Scope: Global

- Type: Security

8. Right click the **IT OU** and select *Delegate Control*
    - Add the **IT Admins** group using the *Delegation of Control Wizard*
    - Delegate to following common tasks: *Create, delete, and manage user accounts*

Take a screenshot of the final *Delegation of Control Wizard* screen before clicking "Finish"


Windows-Server2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Active Directory Users and Computers
File Action View Help
Active Directory Users and C
Saved Queries
INFTMK.com
9 Datacenter Evaluation
cense valid for 180 days
rs5_release.180914-1434
11:16 PM
2/11/2023

IT Admins Properties

General | Members | Member Of | Managed By

IT Admins

Group name (pre-Windows 2000): IT Admins

Description:

E-mail:

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

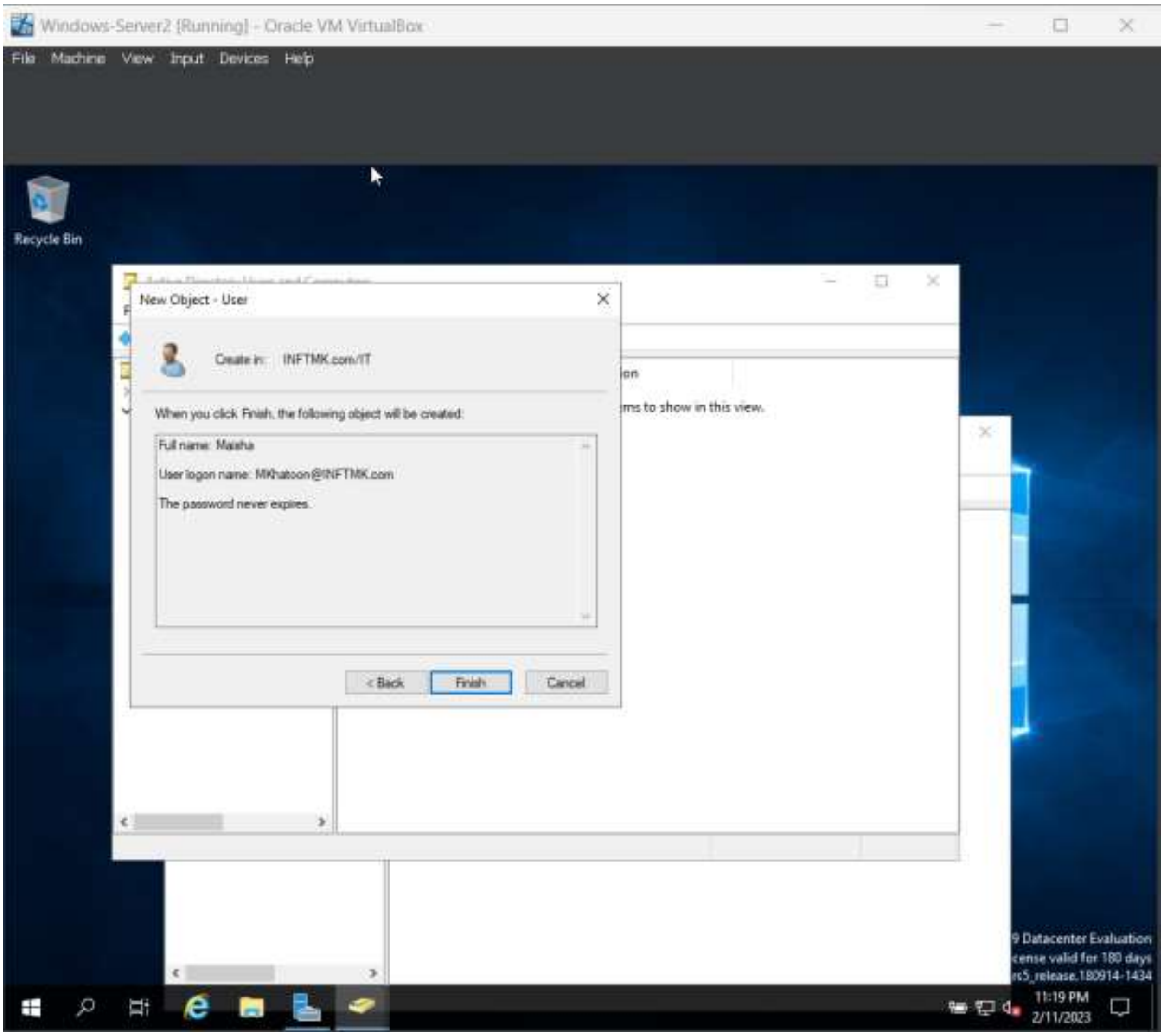
Notes:

OK | Cancel | Apply

9. Open the **IT OU** within Active Directory

- Create a new user account within the **IT OU**
    - Name: Your Name
    - User logon name: first initial last name
    - Uncheck: User must change password at next logon
    - Check: Password never expires

Take a screenshot of the New Object window before clicking “Finish”


Windows-Server2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
New Object - User

Create in: INFTMK.com/IT

When you click Finish, the following object will be created:

Full name: Maisha

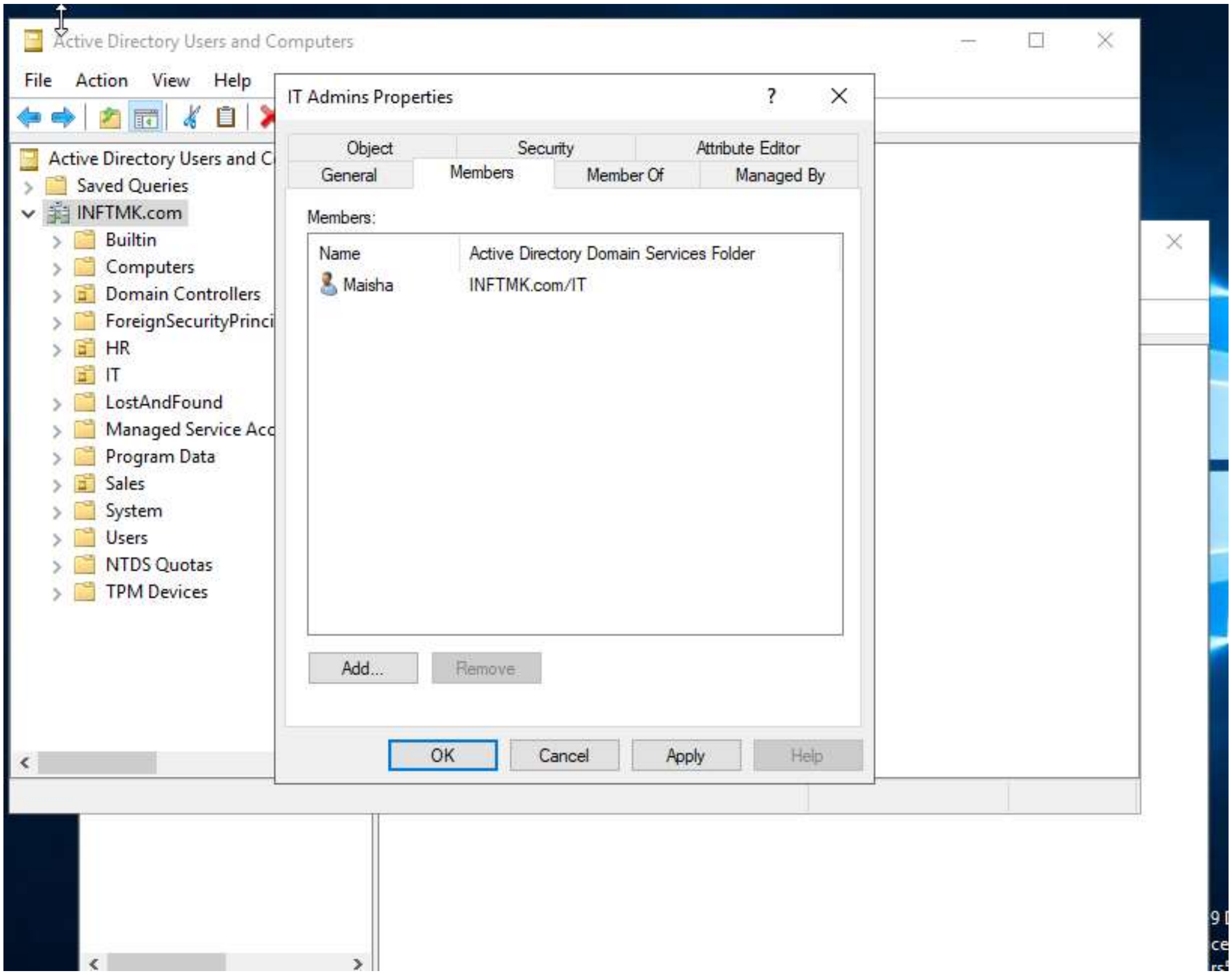
User logon name: MKhatoon@INFTMK.com

The password never expires.

*10.*Right click on the created user account and select *Properties*

- Select the *Attribute Editor* tab
- Select the *distinguisedName* attribute` security group
- Right click and select *Properties*
- Go to the *Members* tab
- Click *Add*
- Add your user account to the IT Admins security group

Take a screenshot of the Members tab and paste below before selecting "*OK*"



Members:

Name	Active Directory Domain Services Folder
Maisha	INFTMK.com/IT

Using Powershell for the following steps:

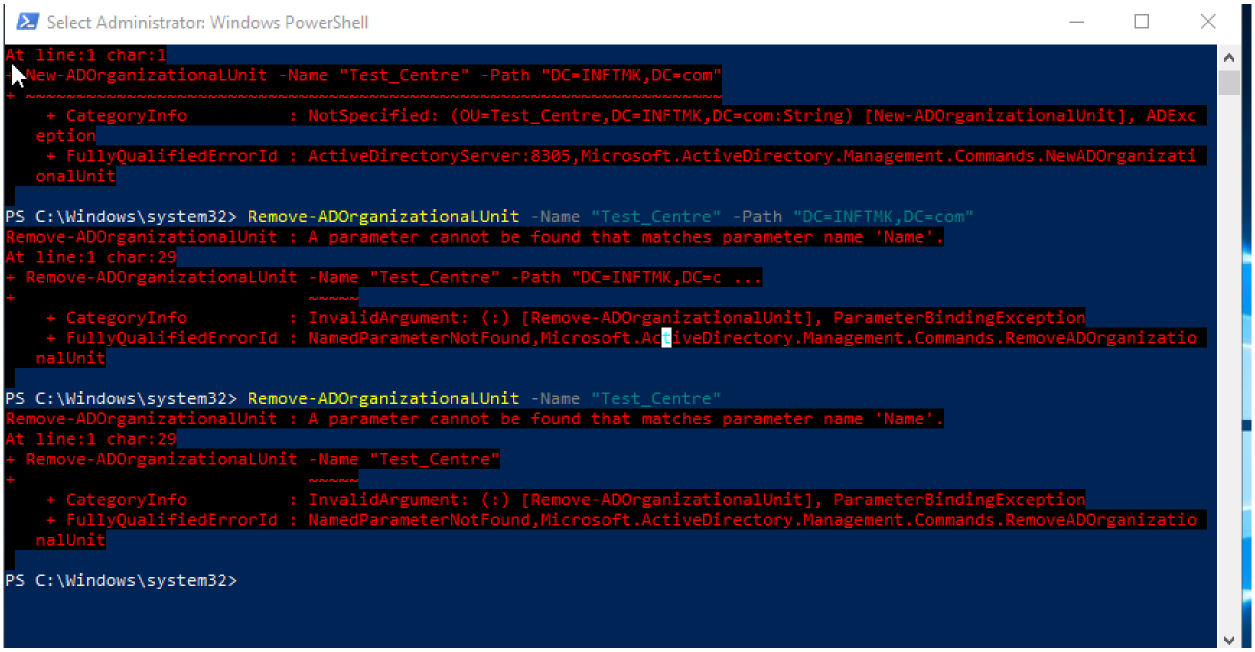
Part 1B: Creating and Managing Groups and OU’s using Powershell:

11. Create a OU called Test Centre.

On the **Toronto Domain Controller:**

- Open **PowerShell** as Administrator
- Type the following command: *New-ADOrganizationalUnit -Name "Test_Centre" -Path "DC=INFT1103,DC=com"*
- Open Active Directory Users and Computers

Take a screenshot of the output and paste it here



```
At line:1 char:1
+ New-ADOrganizationalUnit -Name "Test_Centre" -Path "DC=INFTMK,DC=com"
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (OU=Test_Centre,DC=INFTMK,DC=com:String) [New-ADOrganizationalUnit], ADExc
   eption
    + FullyQualifiedErrorId : ActiveDirectoryServer:8305,Microsoft.ActiveDirectory.Management.Commands.NewADOrganizati
   onalUnit

PS C:\Windows\system32> Remove-ADOrganizationalUnit -Name "Test_Centre" -Path "DC=INFTMK,DC=com"
Remove-ADOrganizationalUnit : A parameter cannot be found that matches parameter name 'Name'.
At line:1 char:29
+ Remove-ADOrganizationalUnit -Name "Test_Centre" -Path "DC=INFTMK,DC=c ...
+                             ~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Remove-ADOrganizationalUnit], ParameterBindingException
    + FullyQualifiedErrorId : NamedParameterNotFound,Microsoft.ActiveDirectory.Management.Commands.RemoveADOrganizatio
   nalUnit

PS C:\Windows\system32> Remove-ADOrganizationalUnit -Name "Test_Centre"
Remove-ADOrganizationalUnit : A parameter cannot be found that matches parameter name 'Name'.
At line:1 char:29
+ Remove-ADOrganizationalUnit -Name "Test_Centre"
+                             ~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Remove-ADOrganizationalUnit], ParameterBindingException
    + FullyQualifiedErrorId : NamedParameterNotFound,Microsoft.ActiveDirectory.Management.Commands.RemoveADOrganizatio
   nalUnit

PS C:\Windows\system32>
```

Here I faced some issues while writing the commands. That’s why I was unable to finish the rest of the questions.

12. Create a security group named :test_centre_admin”

On the **Toronto itDomain Controller:**

- Open **PowerShell** as Administrator

- Type the following command:
- *New-ADGroup -Name"test_centre_admin" -GroupScope Global -GroupCategory Security -Path “OU=Test_Centre,DC=inft1103,DC=com"*
- Open Active Directory Users and Computers

Take a screenshot of the output and paste it here

13. Delegation control for test_centre_admin

On the **Toronto Domain Controller:**

- Open **PowerShell** as Administrator
- Type the following command:
- *Add-ADPermission -Identity "OU=Test_Centre,DC=inft1103,DC=com" -User "test_centre_admin" -ExtendedRights "Create Child, Delete Child, Modify Permission"*

- Open Active Directory Users and Computers

Take a screenshot of the output and paste it here

The following steps are mixed with GUI and Powershell:

<u>Part 2: Service Accounts</u>

14.On the **Toronto DC**, create a KDS root key:

- Open **PowerShell** as Administrator
- type the following command: *Add-KDSRootKey -EffectiveTime ((Get-Date).AddHours(-10))*

Take a screenshot of the output and paste it here

15. Create a **Traditional Service Account:**

- Open Active Directory Users and Computers
- Create an **OU** below the Domain Object called **Service Accounts**
- Select the Service Accounts OU and create a **User account**
  - Name: backup service
  - User logon name: bu_service
  - Unchecked: User must change password at next logon
  - Checked: Password never expires
- Open PowerShell as Administrator
  - Type the following command: *Setspn –U –S backup/fileserver bu_service*

Take a screenshot of the response message before closing the PowerShell window

Part 3: Domain Password Policy

16. On the TorontoDC open **Group Policy Management**

a. Expand forest: INFT1103.com

b. Expand Domains

c. Expand INFT1103.com

d. Right click the Default Domain Policy and select *Edit*

e. Expand: *Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy*

f. Open *Maximum password age*

i. Uncheck: Define this policy setting

ii. Click OK

g. Open Minimum password length

iii. Password must be at least: 8 characters

iv. Click OK

Take a screenshot of the Password Policy Settings before closing the Group Policy Management Editor

Reflection:

So, which way do you prefer to use when managing Active Directory? Why? Do you see the advantages to using PowerShell? Please provide your answer below.

Ans: PowerShell is better for API and automation scripts. While the UI is good for day to day use for smaller task.