This lab is designed to provide hands-on experience in managing user accounts within Active Directory. Utilizing tools such as Active Directory Administrative Center, Active Directory Users and Computers, and PowerShell, participants will gain practical skills in user account management. The lab aims to enhance understanding and proficiency in these essential administrative tasks, ensuring that users can effectively manage and maintain Active Directory environments.

Lab 4 - Managing User Accounts

420-636-AB-Network Installation and Administration II

Teacher: Antoine Tohme
Student: Monica Perez Mata
Student id : 2498056

Table of Contents

1 Lab 4 - Managing User Accounts

1.1 Objective

This lab is designed to help you practice **managing user accounts** in Active Directory using **Active Directory Administrative Center**, Active **Directory Users and Computers** and **PowerShell**.

You will perform tasks related to **user creation, movement, enabling/disabling accounts, locking/unlocking users, and configuring roaming profiles**.

1.2 Lab Requirements

- Domain Name: **vlabs1.com**
- **Servers**:
  - **DC101** (Windows Server 2022, Primary DC for vlabs.com)
  - **SRV01** (Windows Server 2025 - domain-joined) → ***Roaming profiles will be configured here.***
- **Client Machine:**
  - **Client1** (Windows 11 - domain-joined).

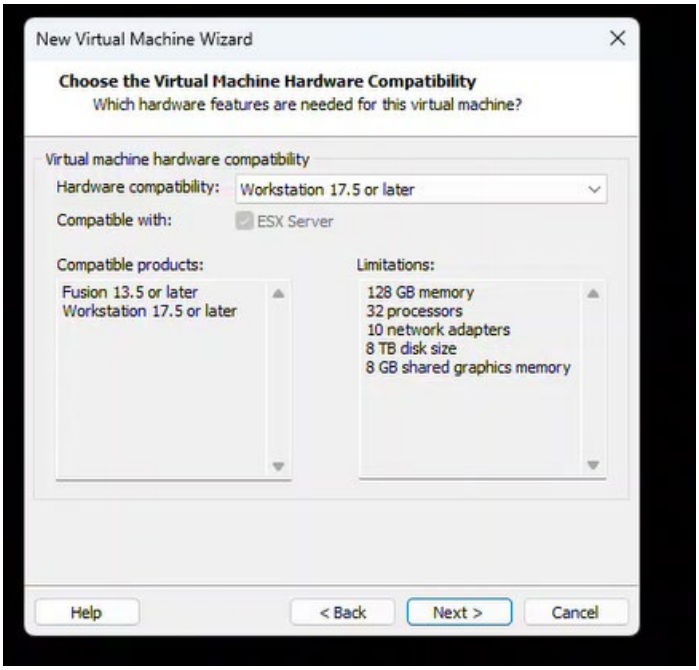
NOTE - Lab 4 is based on Lab 3

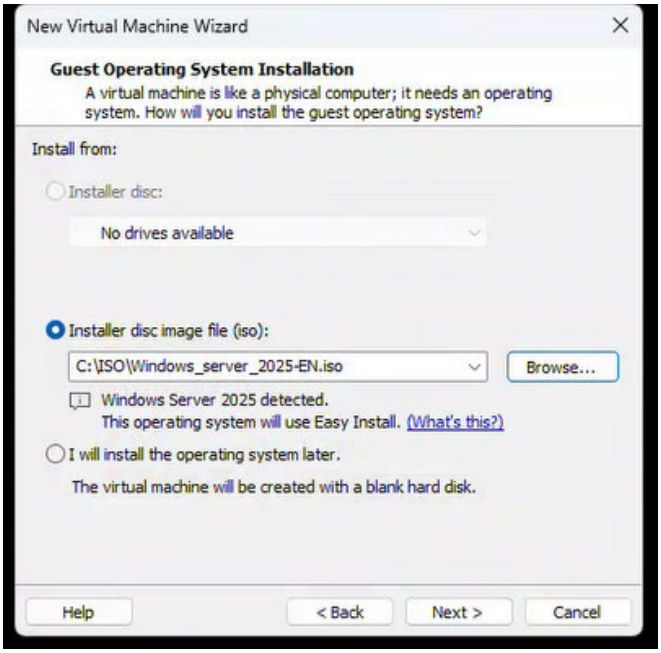
2 Task 1: Install a Windows File Server 2025

Requirements

- OS: **Windows Server 2025 Standard Edition (Desktop Experience)**
- Serail number: **HMP2Y-T9NJ2-Q8MH6-2VGM9-CDQMB**
- Name**: SRV01** – *Where 01 is your remote computer number*
- Specs**: 2 vCPU, 4 GB RAM, 60 GB HDD**
- Network**: LAN Segment: LAN1**
    - Assign a static IP: **192.168. 1.10/24**
    - Set DNS Server: **192.168.1.1**
- Join this server to the **vlabs1.com** domain.

2.1 Create new VM



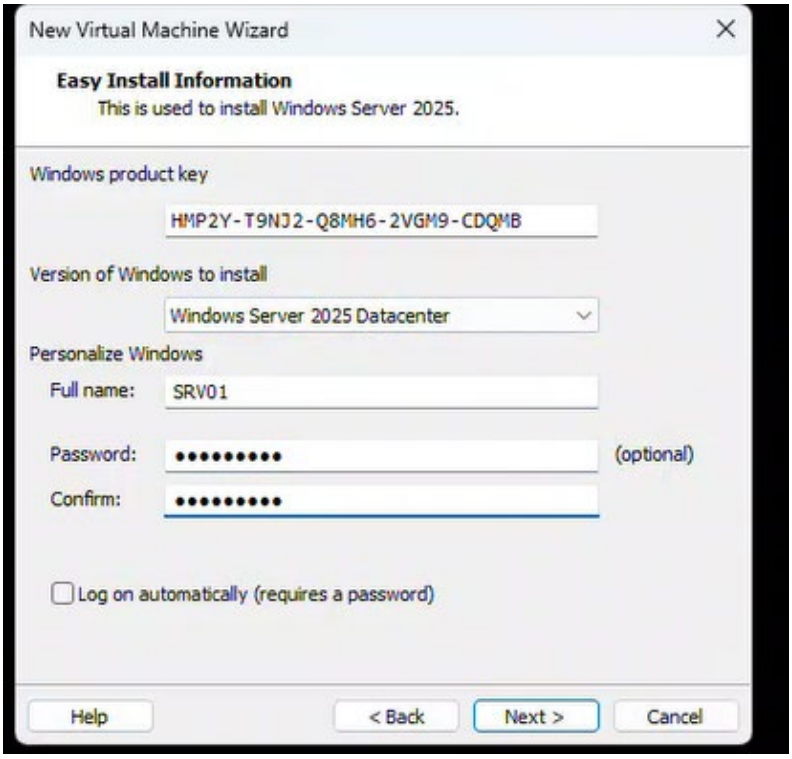


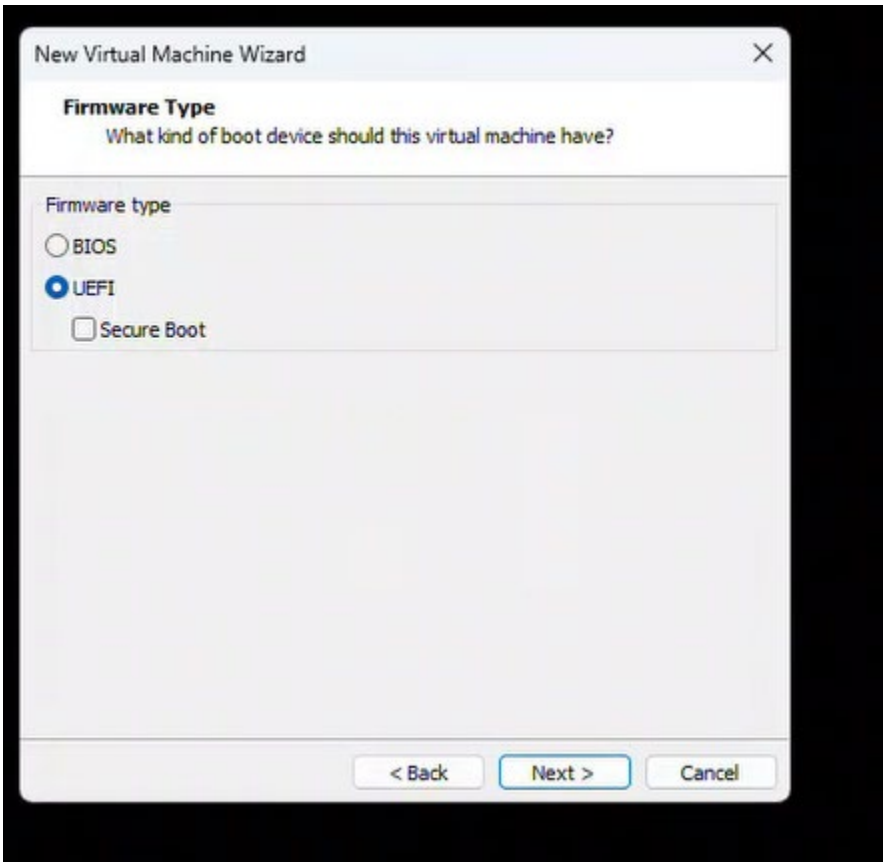
- Serail number: **HMP2Y-T9NJ2-Q8MH6-2VGM9-CDQMB**
- Name**: SRV01** – *Where 01 is your remote computer number*
- Specs**: 2 vCPU, 4 GB RAM, 60 GB HDD**

Network**: LAN Segment: LAN1** Assign a static IP: **192.168. 1.10/24**

Set DNS Server: **192.168.1.1**

Join this server to the **vlabs1.com** domain

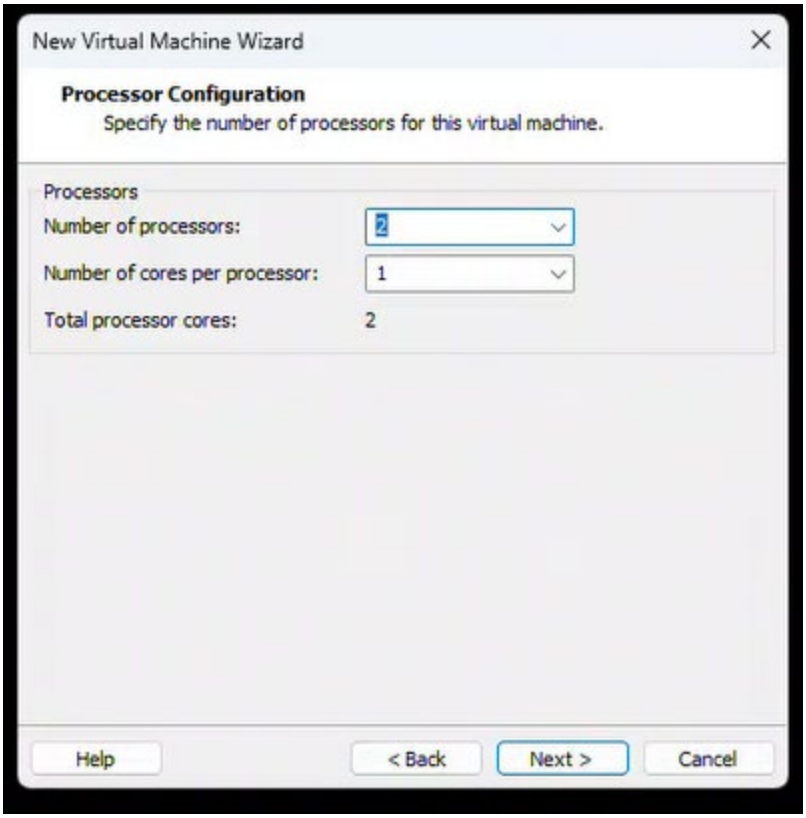


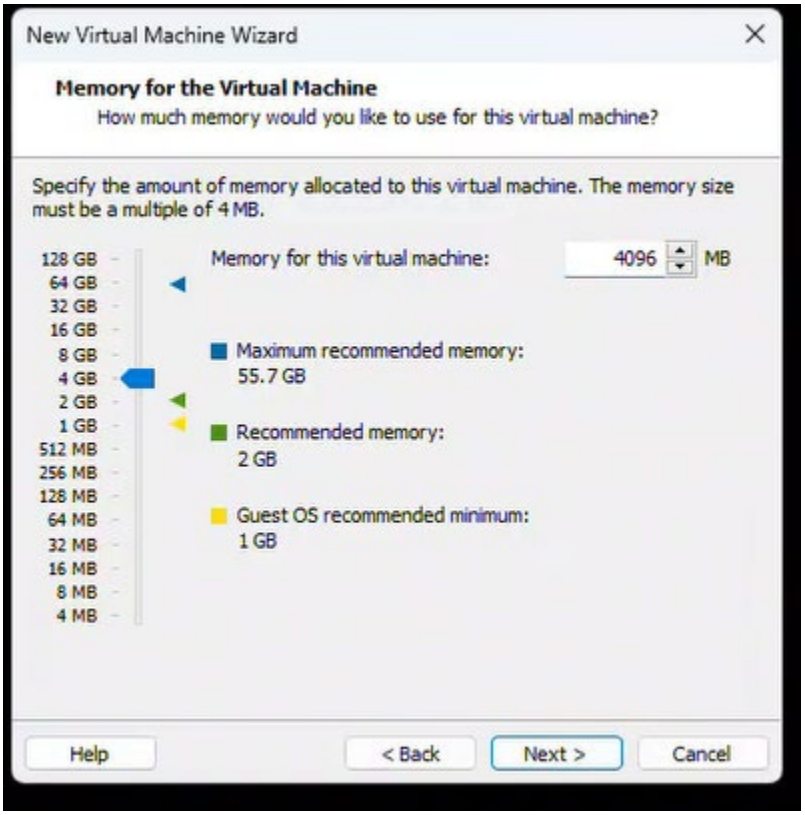


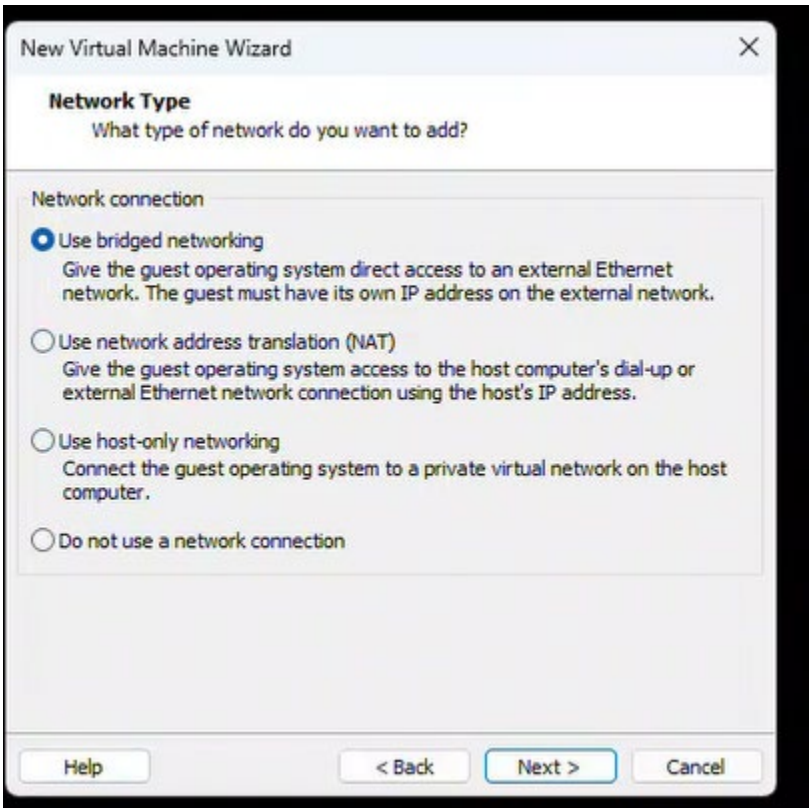
Specs**: 2 vCPU, 4 GB RAM, 60 GB HDD**

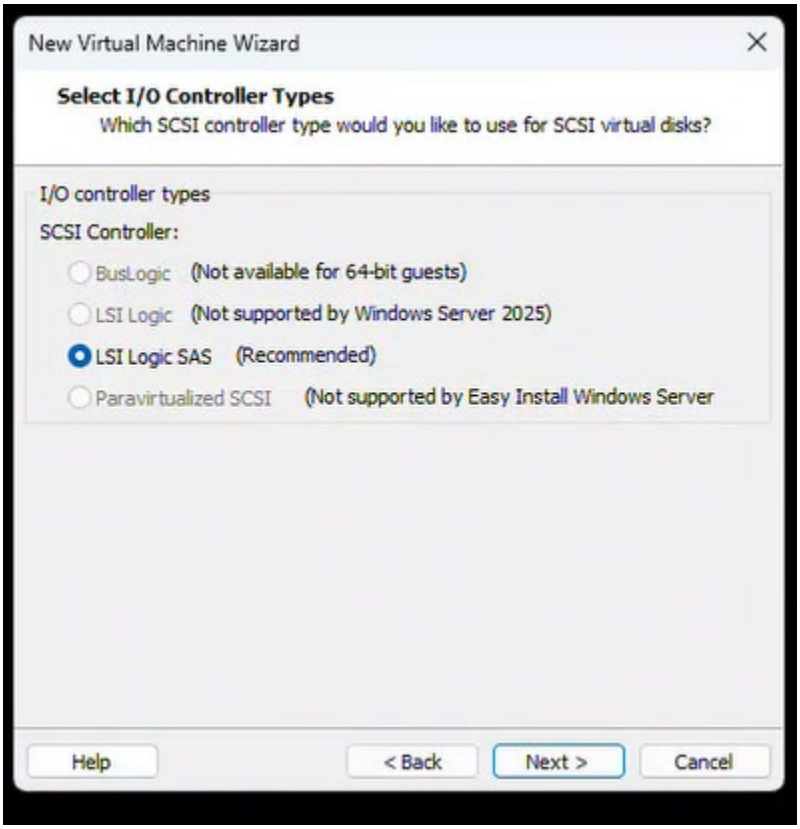
Network**: LAN Segment: LAN1** Assign a static IP: **192.168. 1.10/24**

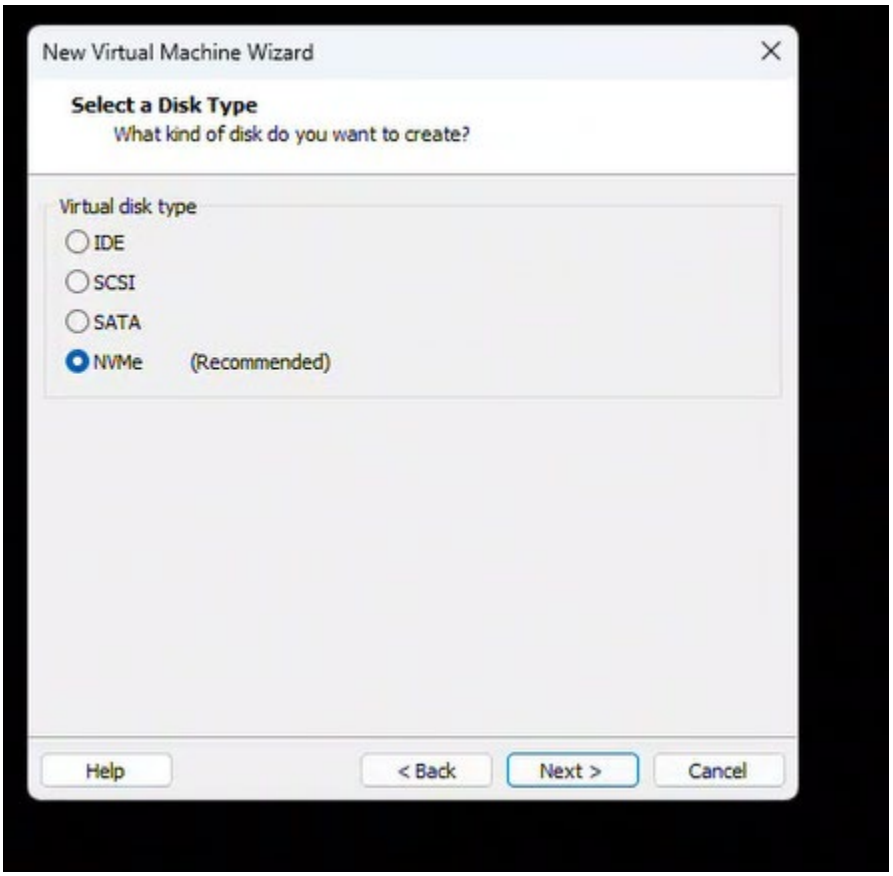
Set DNS Server: **192.168.1.1**

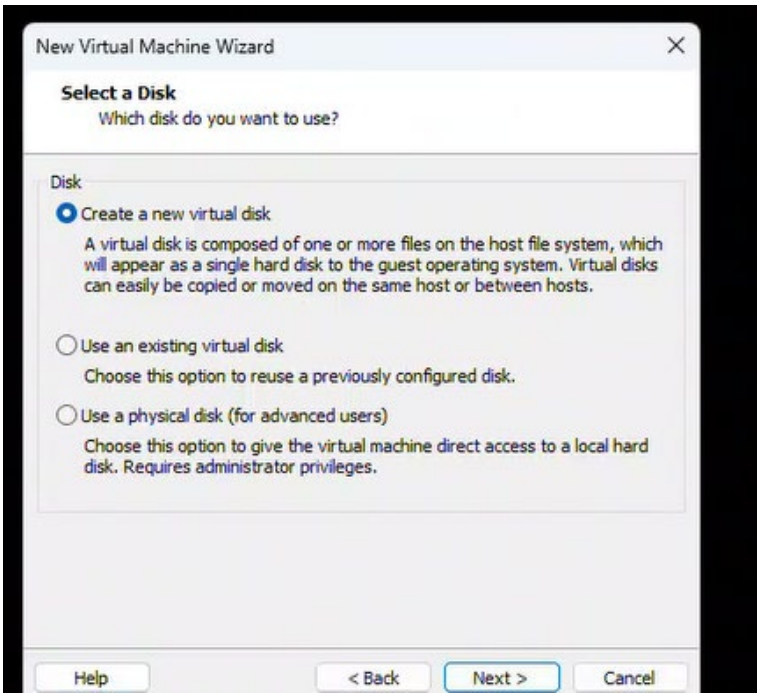

New Virtual Machine Wizard
Processor Configuration
Specify the number of processors for this virtual machine.
Processors
Number of processors:
2
Number of cores per processor:
1
Total processor cores:
2
Help
< Back
Next >
Cancel

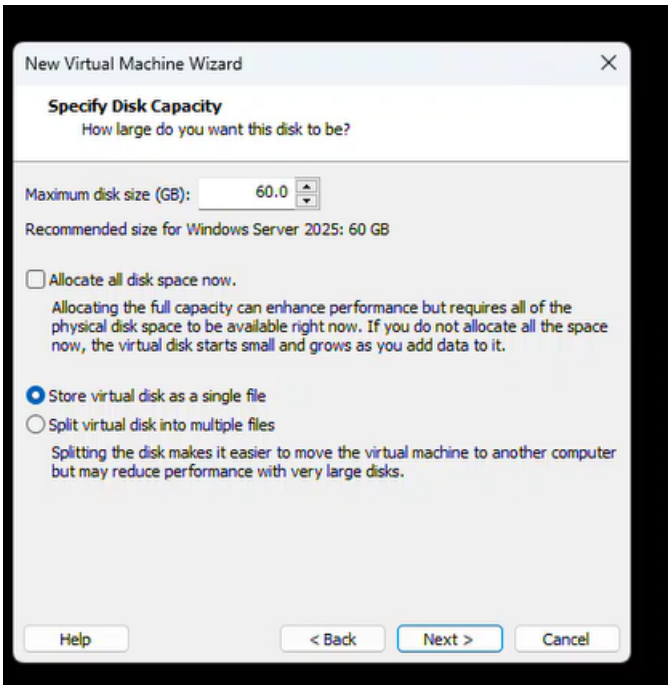

New Virtual Machine Wizard
Memory for the Virtual Machine
How much memory would you like to use for this virtual machine?
Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.
128 GB
64 GB
32 GB
16 GB
8 GB
4 GB
2 GB
1 GB
512 MB
256 MB
128 MB
64 MB
32 MB
16 MB
8 MB
4 MB
Memory for this virtual machine:
4096
MB
Maximum recommended memory:
55.7 GB
Recommended memory:
2 GB
Guest OS recommended minimum:
1 GB
Help
< Back
Next >
Cancel


New Virtual Machine Wizard
Network Type
What type of network do you want to add?
Network connection
Use bridged networking
Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.
Use network address translation (NAT)
Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.
Use host-only networking
Connect the guest operating system to a private virtual network on the host computer.
Do not use a network connection
Help
< Back
Next >
Cancel

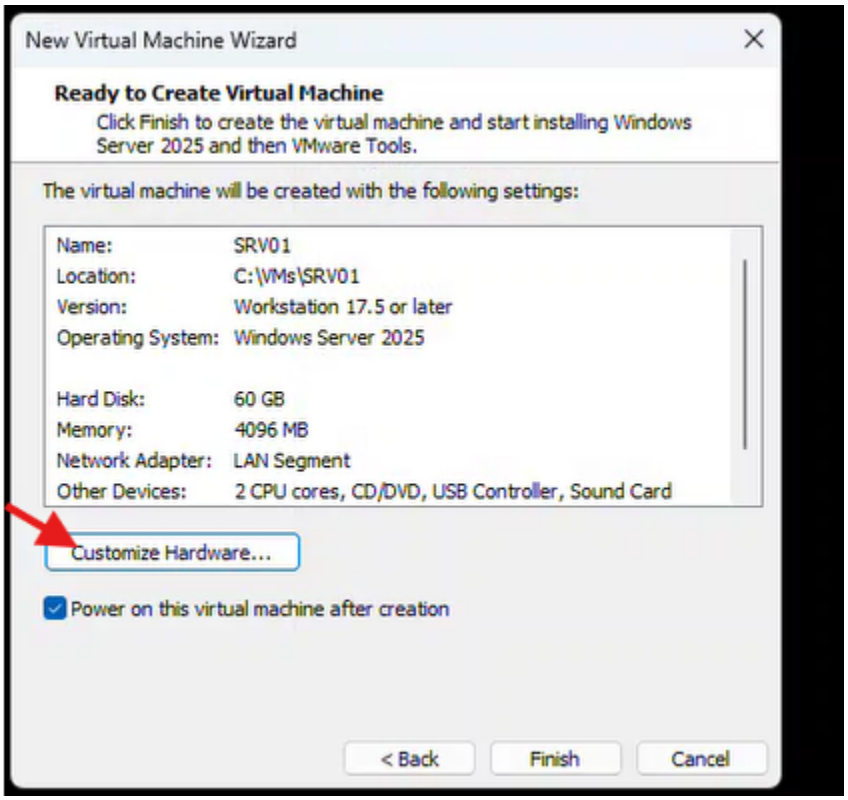

New Virtual Machine Wizard
Select I/O Controller Types
Which SCSI controller type would you like to use for SCSI virtual disks?
I/O controller types
SCSI Controller:
BusLogic (Not available for 64-bit guests)
LSI Logic (Not supported by Windows Server 2025)
LSI Logic SAS (Recommended)
Paravirtualized SCSI (Not supported by Easy Install Windows Server
Help
< Back
Next >
Cancel

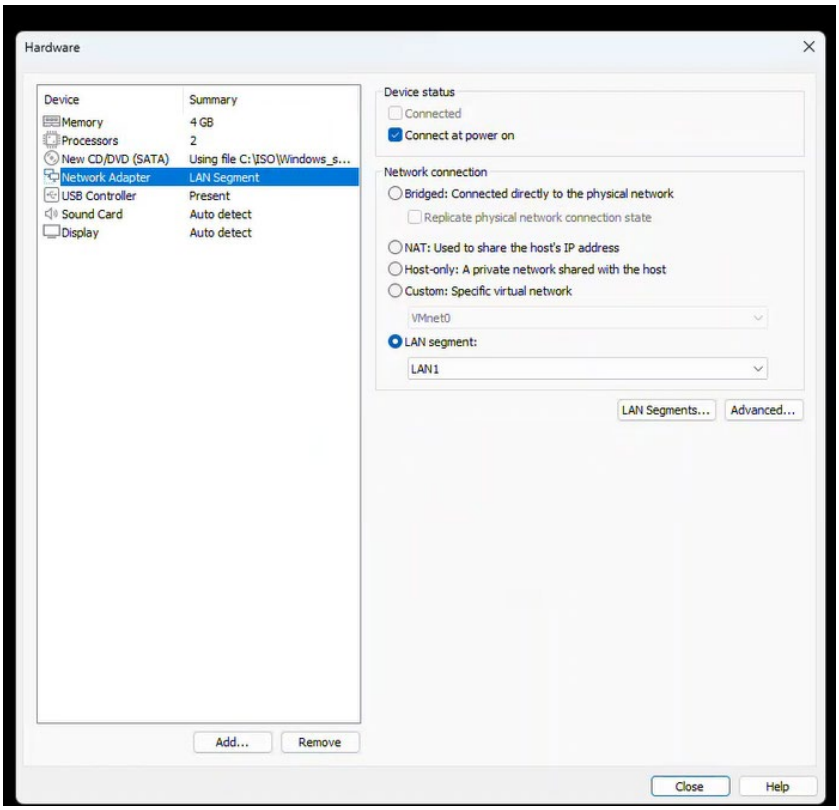

New Virtual Machine Wizard
Select a Disk Type
What kind of disk do you want to create?
Virtual disk type
IDE
SCSI
SATA
NVMe (Recommended)
Help
< Back
Next >
Cancel

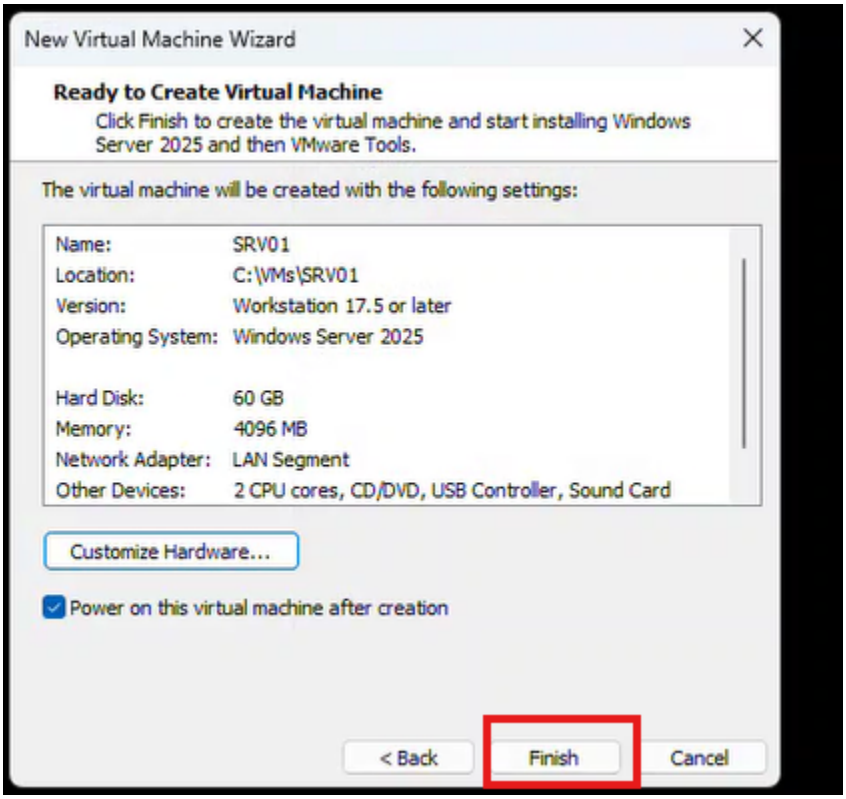

New Virtual Machine Wizard
Select a Disk
Which disk do you want to use?
Disk
Create a new virtual disk
A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.
Use an existing virtual disk
Choose this option to reuse a previously configured disk.
Use a physical disk (for advanced users)
Choose this option to give the virtual machine direct access to a local hard disk. Requires administrator privileges.
Help
< Back
Next >
Cancel


New Virtual Machine Wizard
Specify Disk Capacity
How large do you want this disk to be?
Maximum disk size (GB):
60.0
Recommended size for Windows Server 2025: 60 GB
Allocate all disk space now.
Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.
Store virtual disk as a single file
Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Help
< Back
Next >
Cancel

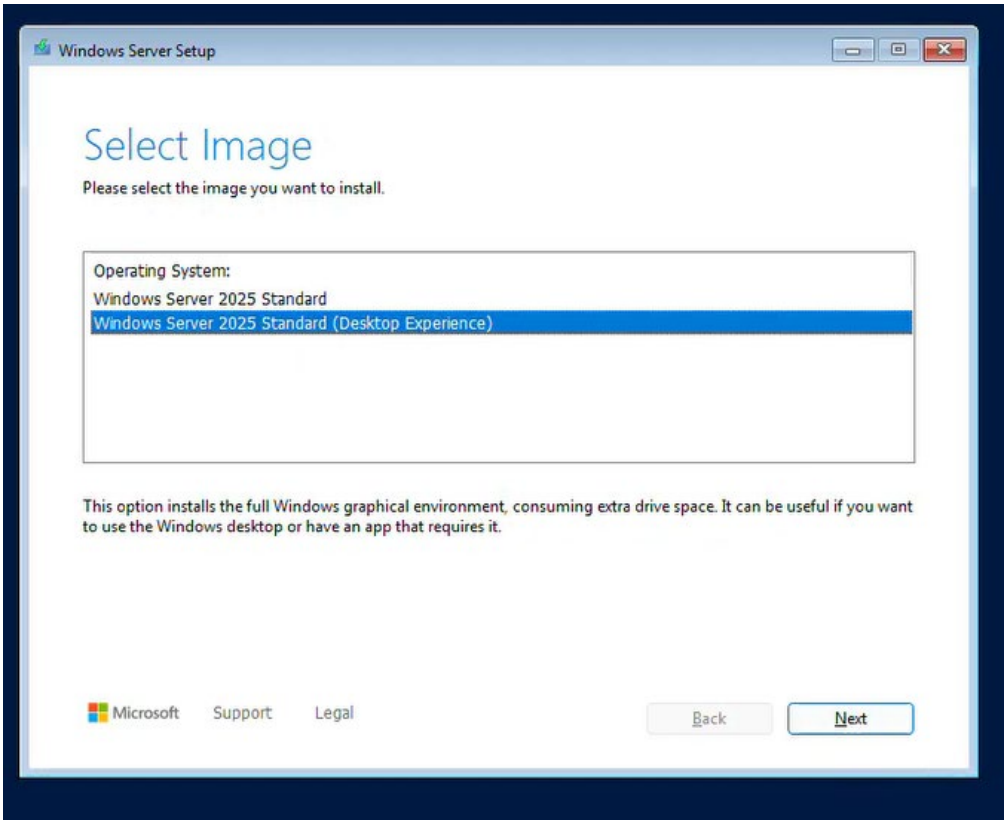

New Virtual Machine Wizard
Specify Disk File
Where would you like to store the disk file?
Disk file
One 60 GB disk file will be created using this file name.
SRV01.vmdk
Browse...
Help
< Back
Next >
Cancel

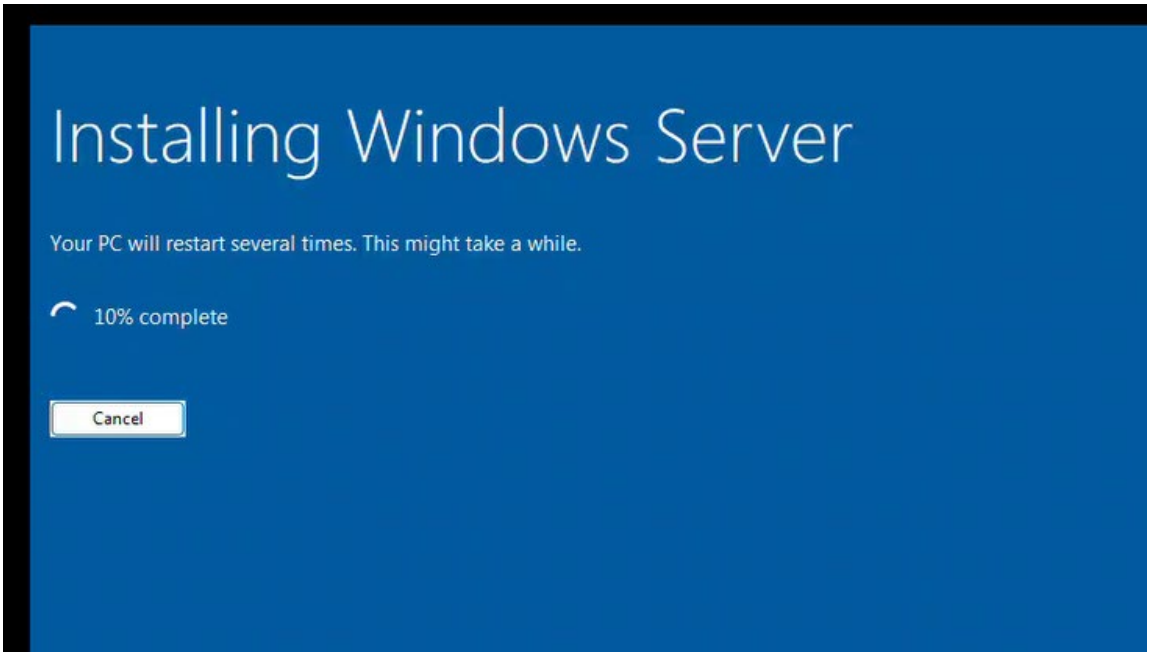

New Virtual Machine Wizard
Ready to Create Virtual Machine
Click Finish to create the virtual machine and start installing Windows Server 2025 and then VMware Tools.
The virtual machine will be created with the following settings:
Name: SRV01
Location: C:\VMs\SRV01
Version: Workstation 17.5 or later
Operating System: Windows Server 2025
Hard Disk: 60 GB
Memory: 4096 MB
Network Adapter: LAN Segment
Other Devices: 2 CPU cores, CD/DVD, USB Controller, Sound Card
Customize Hardware...
Power on this virtual machine after creation
< Back
Finish
Cancel


Hardware
Device
Summary
Memory
4 GB
Processors
2
New CD/DVD (SATA)
Using file C:\ISO\Windows_s...
Network Adapter
LAN Segment
USB Controller
Present
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
LAN1
LAN Segments...
Advanced...
Add...
Remove
Close
Help

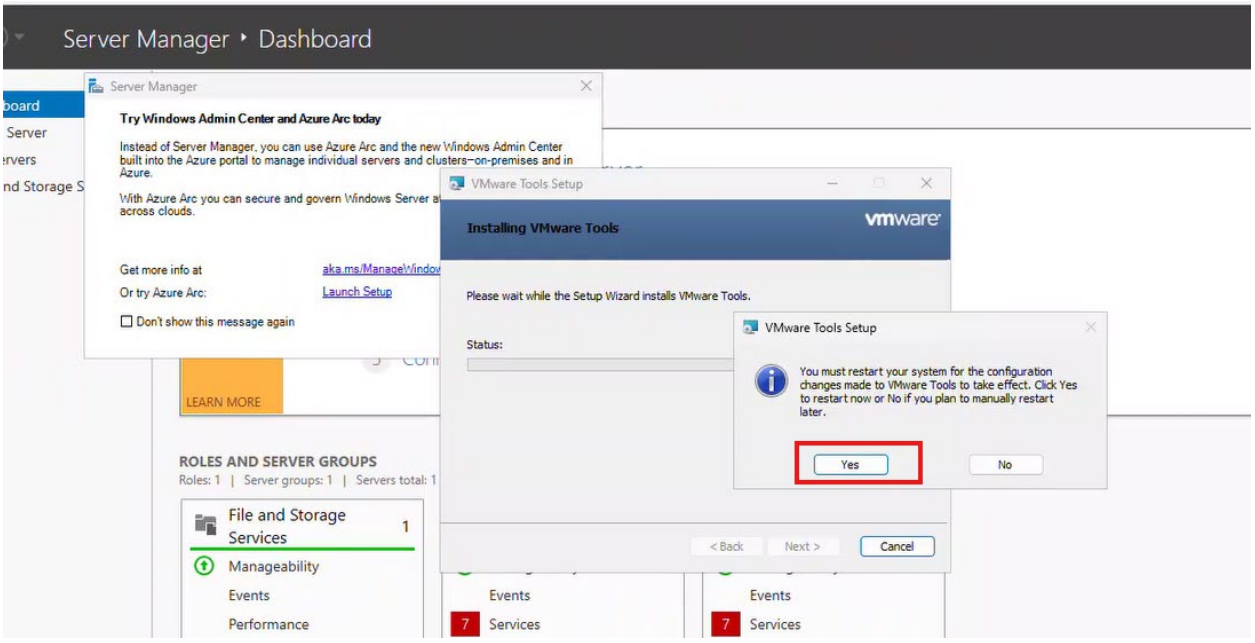


2.2 Windows Install



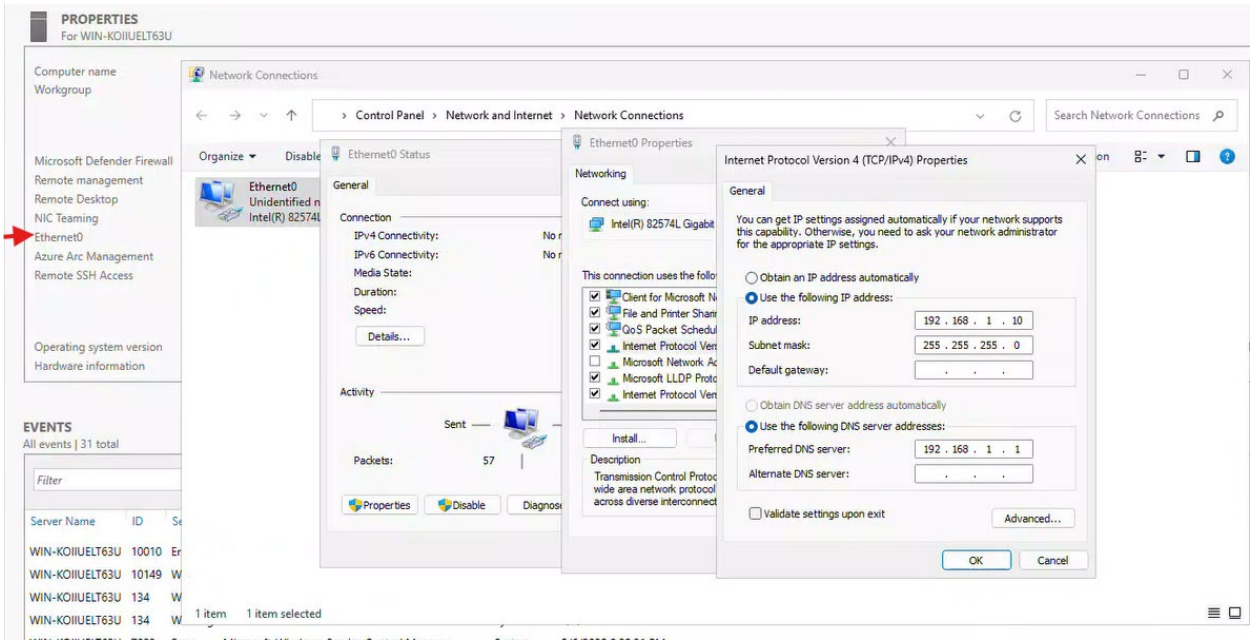


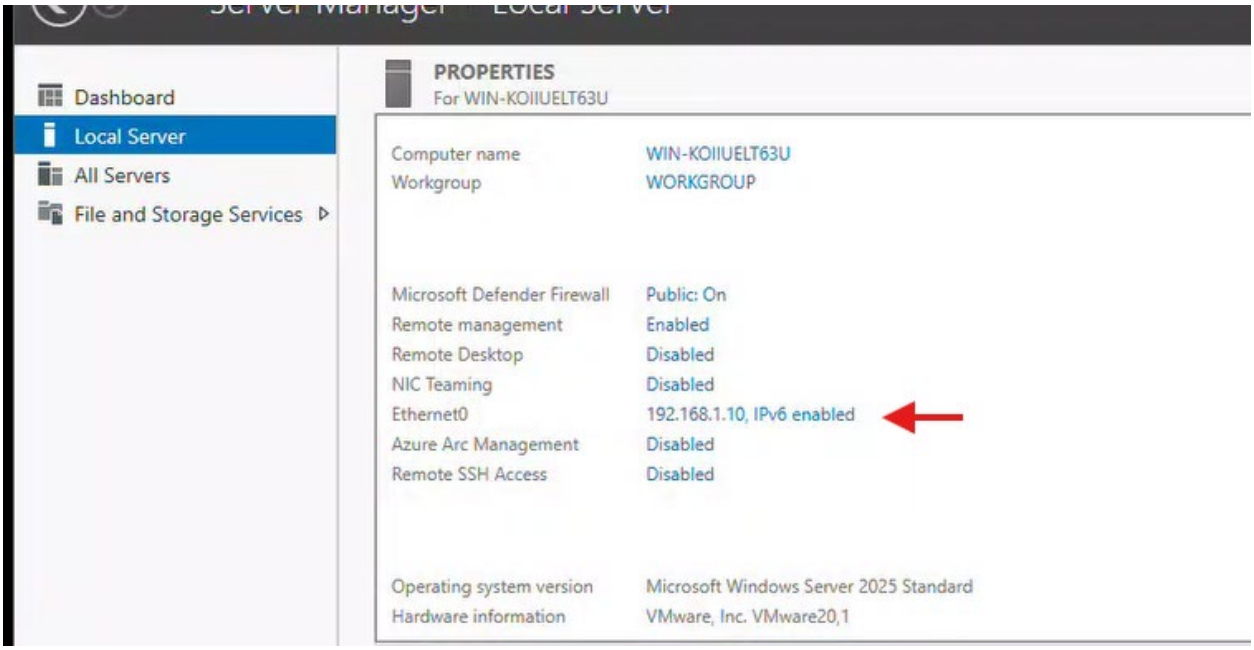
After instlling windows and VMWare tools, a restart is issued



2.3 Set IP address

- Assign a static IP: 192.168. 1.10/24
- Set DNS Server: 192.168.1.1



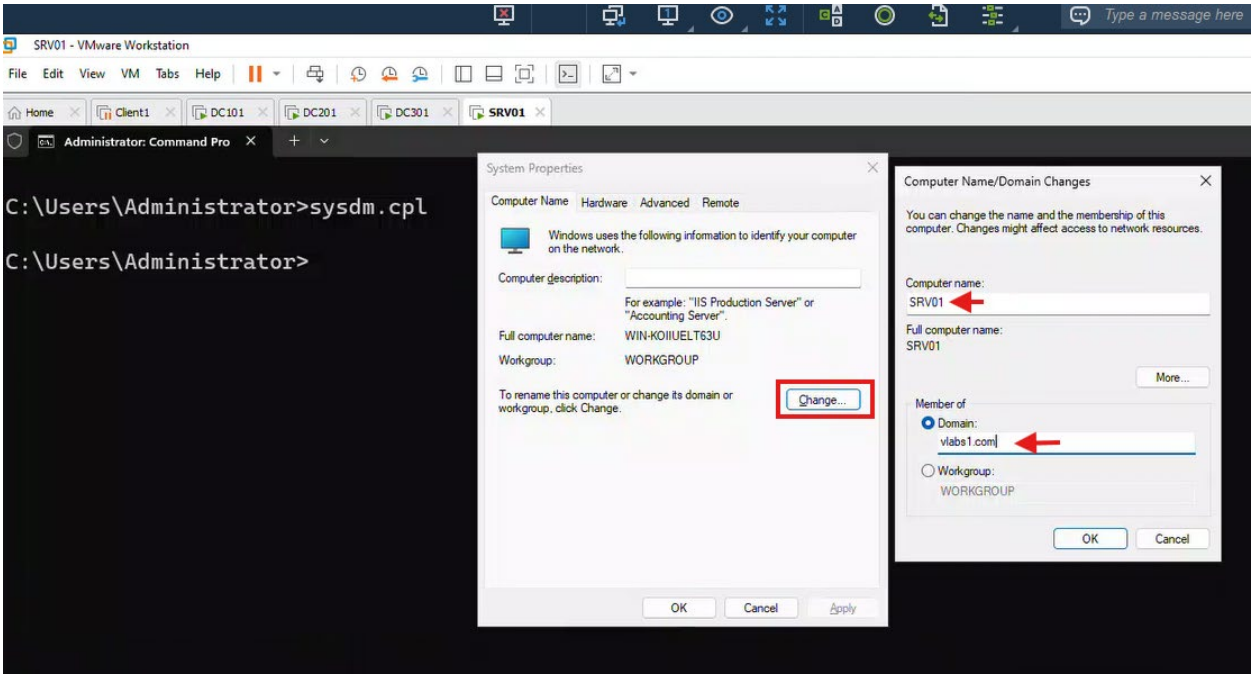


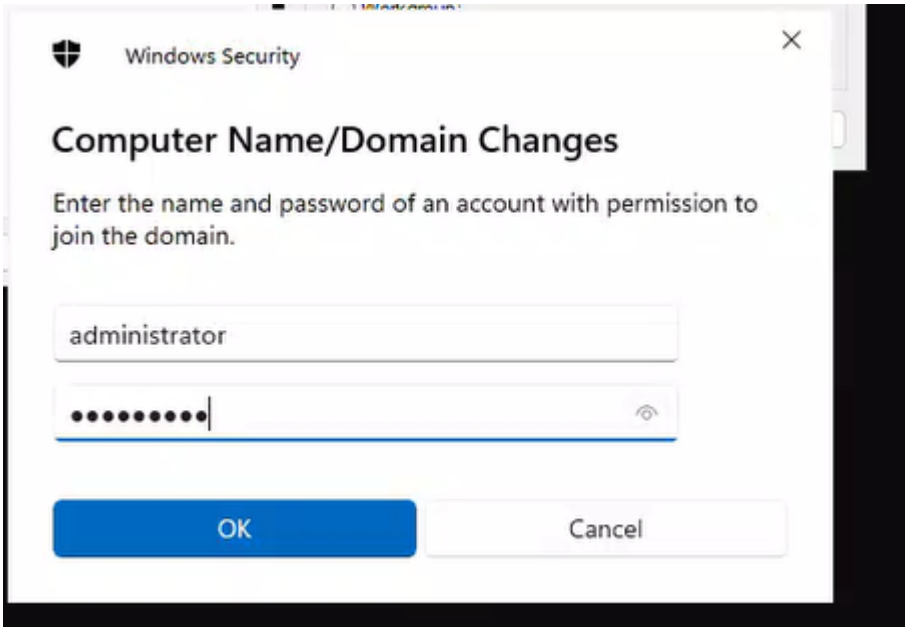
2.4 Join this server to the vlabs1.com domain

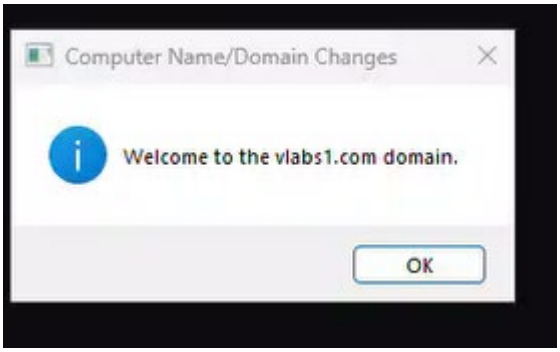
On client

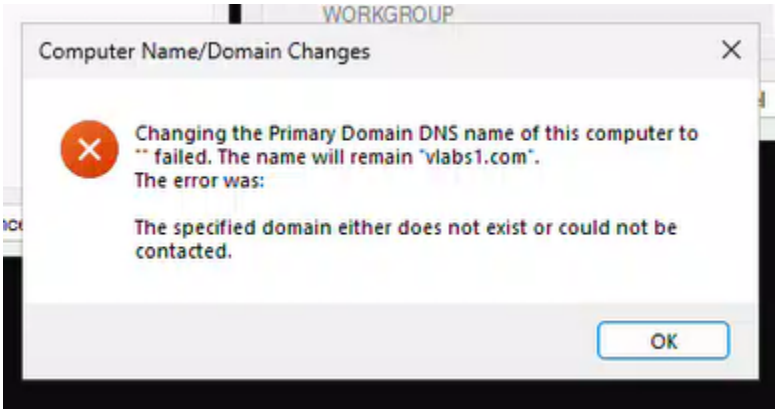
Open command prompt and type **sysdm.cpl** on command prompt for client

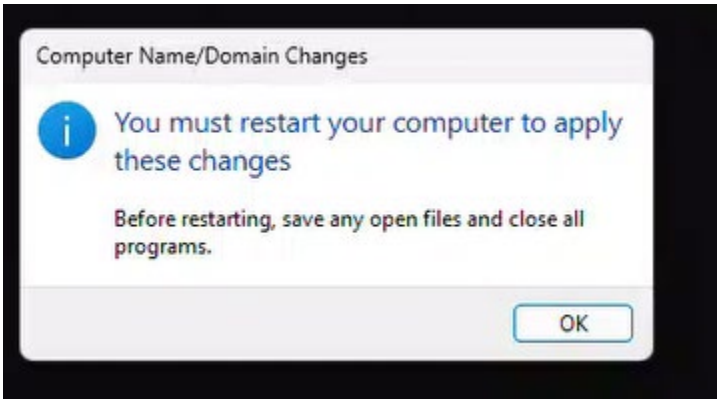
Select change and assign domain

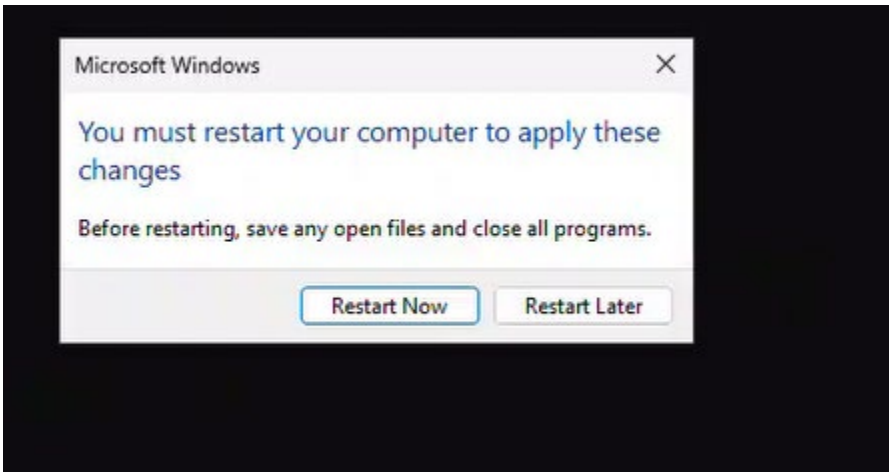

SRV01 - VMware Workstation
File Edit View VM Tabs Help
Home
Client1
DC101
DC201
DC301
SRV01
Administrator: Command Pro
C:\Users\Administrator>sysdm.cpl
C:\Users\Administrator>
System Properties
Computer Name
Hardware
Advanced
Remote
Windows uses the following information to identify your computer on the network.
Computer description:
For example: "IIS Production Server" or "Accounting Server".
Full computer name:
WIN-KOIIUELT63U
Workgroup:
WORKGROUP
To rename this computer or change its domain or workgroup, click Change.
Change...
OK
Cancel
Apply
Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.
Computer name:
SRV01
Full computer name:
SRV01
More...
Member of
Domain:
vlabs1.com
Workgroup:
WORKGROUP
OK
Cancel


Windows Security
Computer Name/Domain Changes
Enter the name and password of an account with permission to join the domain.
administrator
OK
Cancel





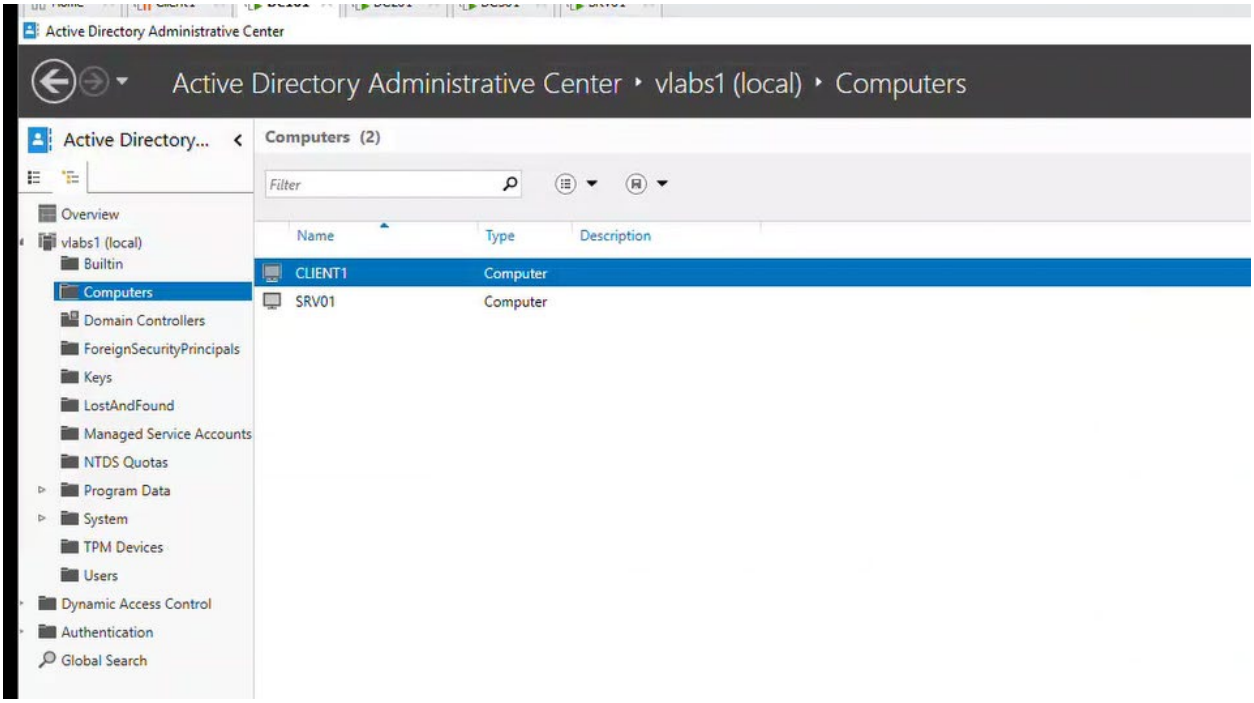


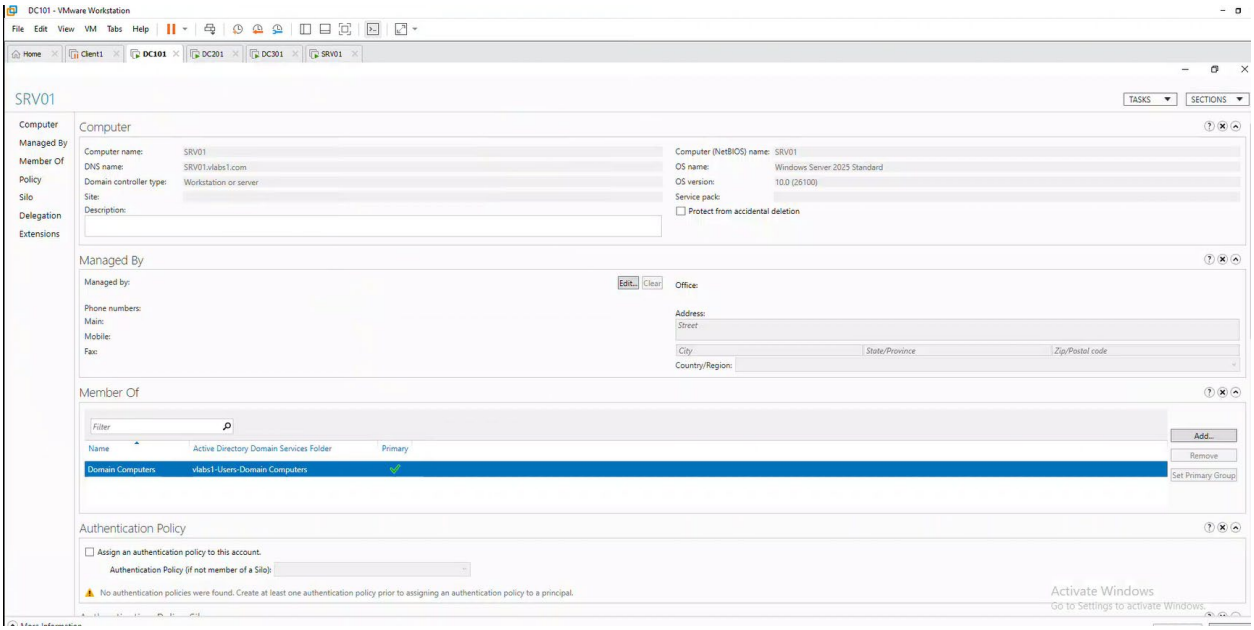


Computer will restart

Server DC 101

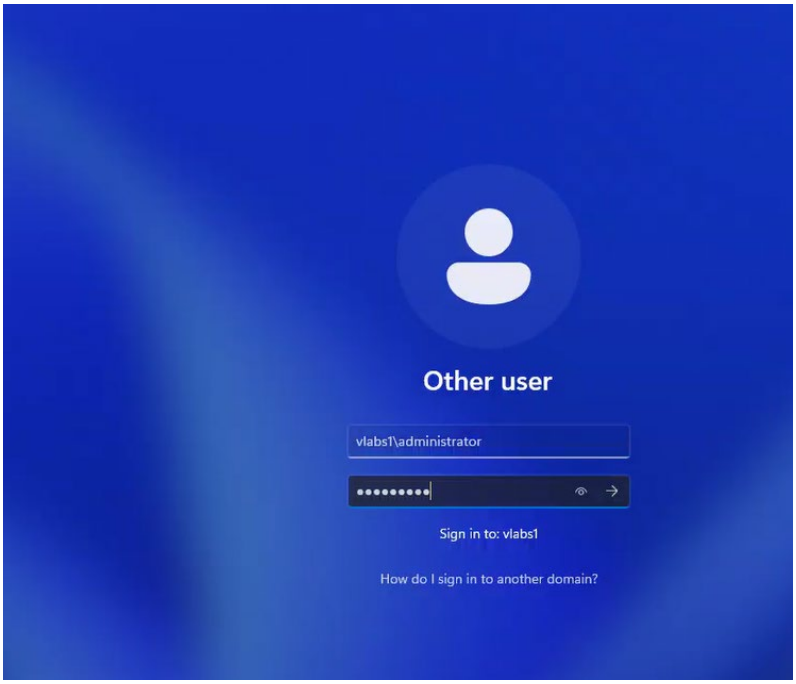
Go to server and verify in Active directory Administrative Center the computer ahs been added



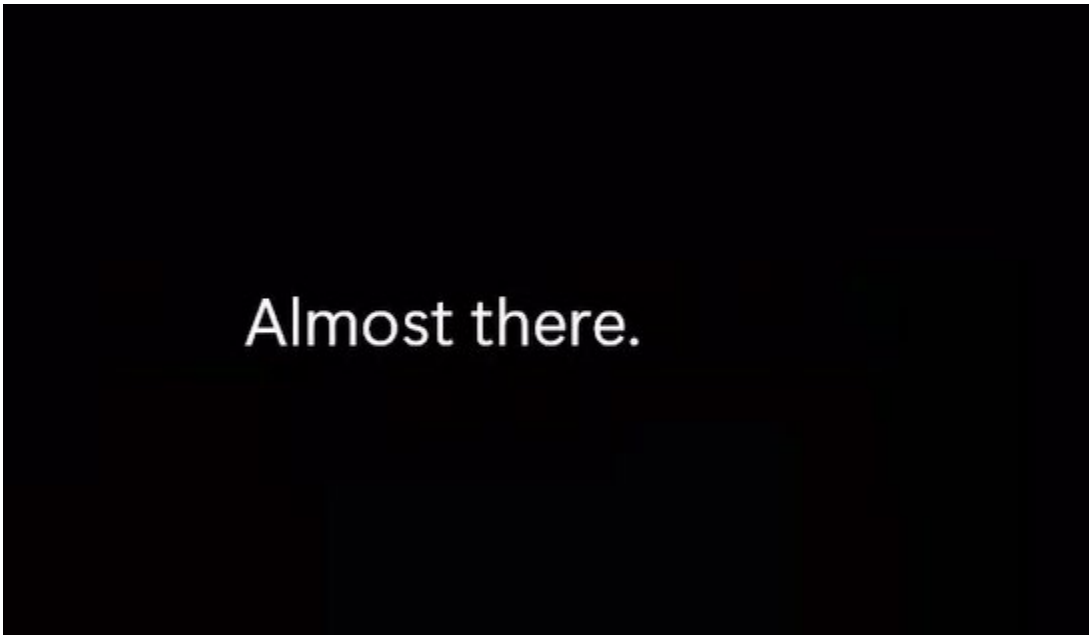


2.4.1 Login with the domain **administrator** to test it

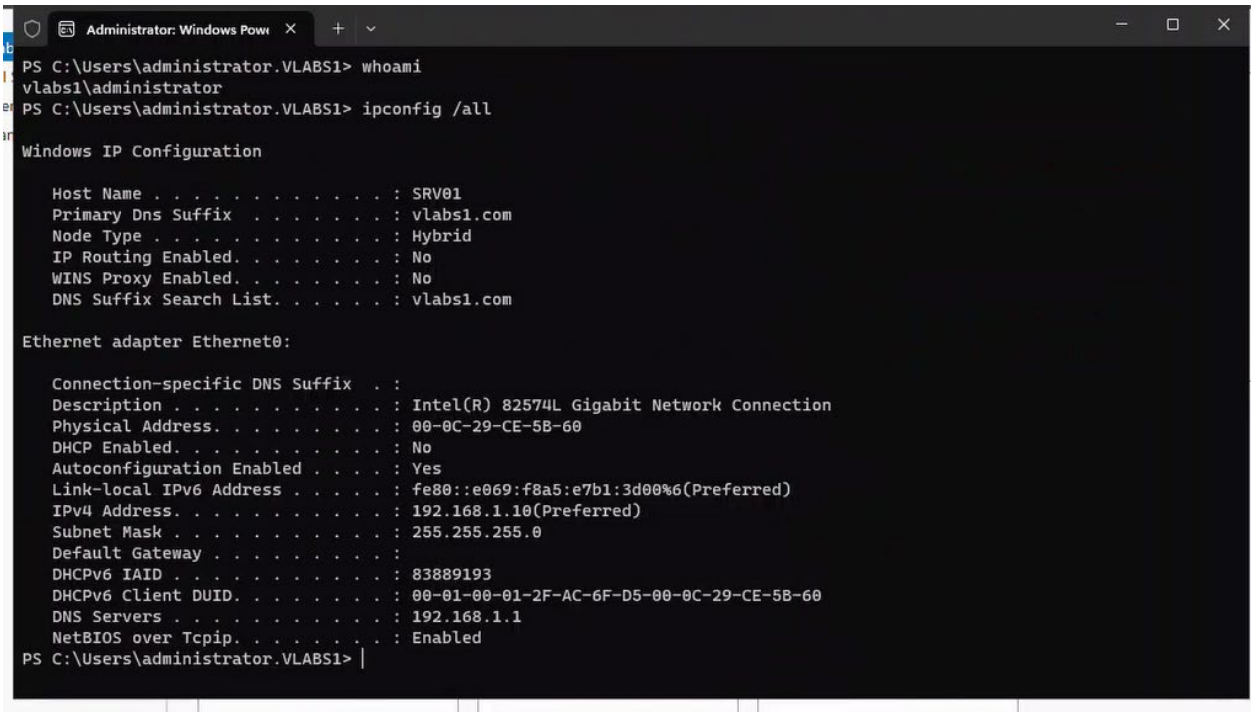
From client login as administrator



Wait



Verify connection


Administrator: Windows Powe
PS C:\Users\administrator.VLABS1> whoami
vlabs1\administrator
PS C:\Users\administrator.VLABS1> ipconfig /all
Windows IP Configuration
Host Name . . . . . : SRV01
Primary Dns Suffix . . . . . : vlabs1.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : vlabs1.com
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-CE-5B-60
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::e069:f8a5:e7b1:3d00%6(Preferred)
IPv4 Address. . . . . : 192.168.1.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 83889193
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-AC-6F-D5-00-0C-29-CE-5B-60
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
PS C:\Users\administrator.VLABS1>

3 Task 2: Create Organizational Units (OUs) and Users

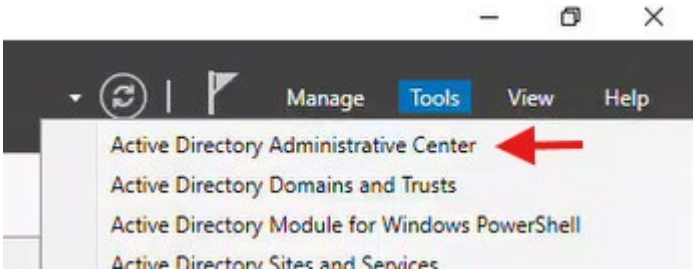
1. Create the following **OUs** using the **Active Directory Administrative Center**
    - **HR OU** and **IT OU**
2. Create the following **users** in the **HR OU** using the **Active Directory Administrative Center**
    - **Sophie Lambert (s.lambert)**
    - **Liam Dupont (l.dupont)**
    - **Emma Morel (e.morel)**
3. Create the following users in the **IT OU** using **PowerShell**:
    - **Lucas Bernard (l.bernard)**
    - **Thomas Aviles (t.aviles)**
    - **Chloe Girard (c.girard)** ***(This user should be disabled during creation).***

3.1 Create OUs using the Active Directory Administrative Center

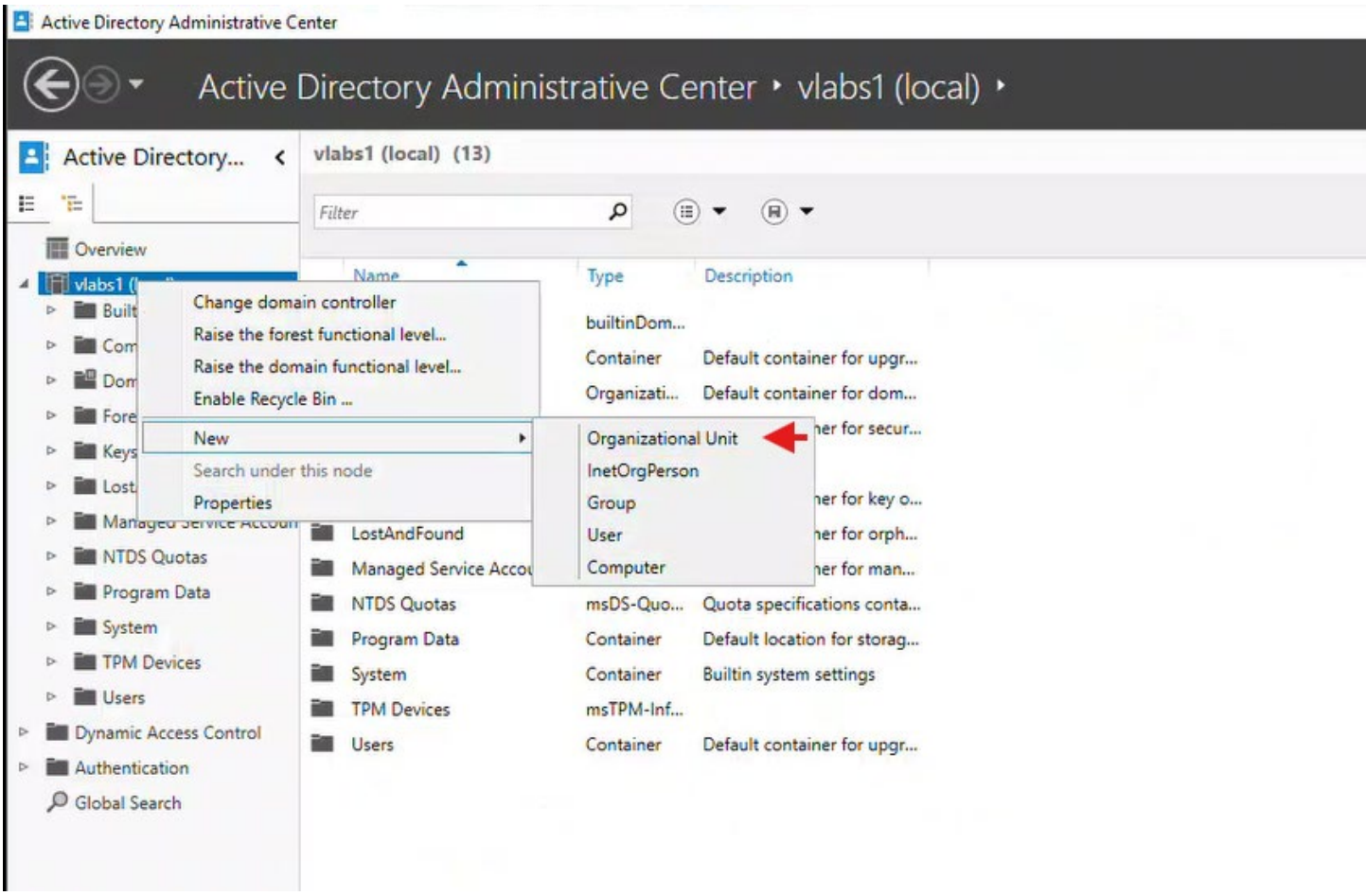
Create the following OUs using the Active Directory Administrative Center

- HR OU and IT OU

1. Open Active Directory Administrative Center.

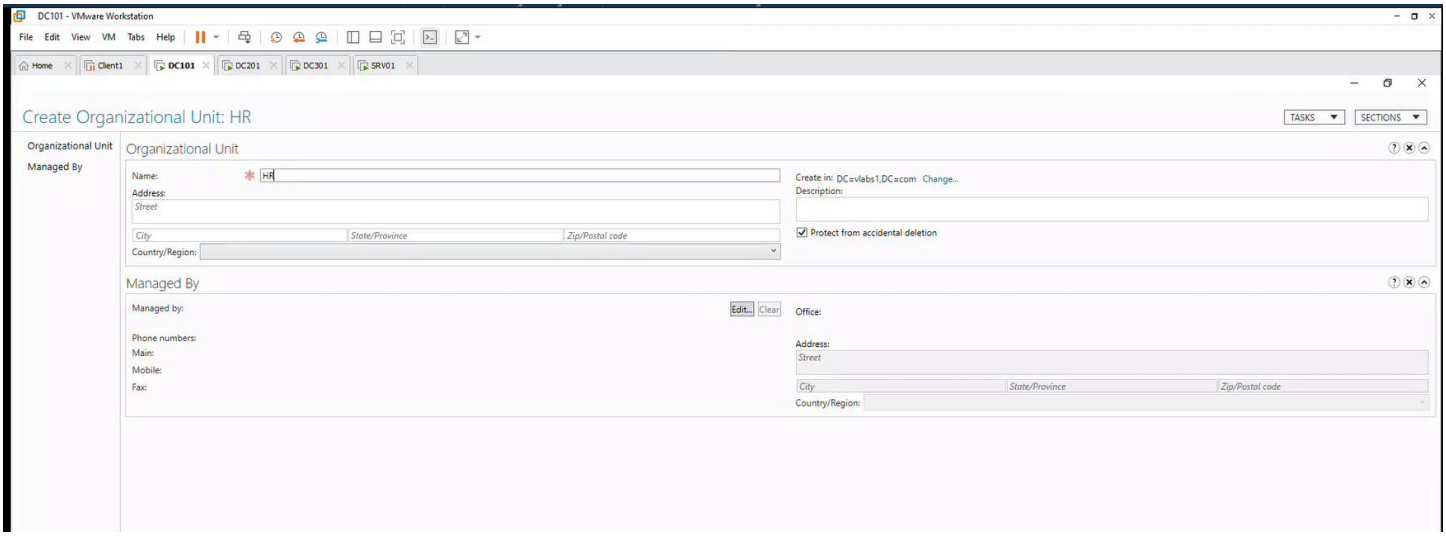


2. Navigate to your domain → Click New → Organizational Unit.

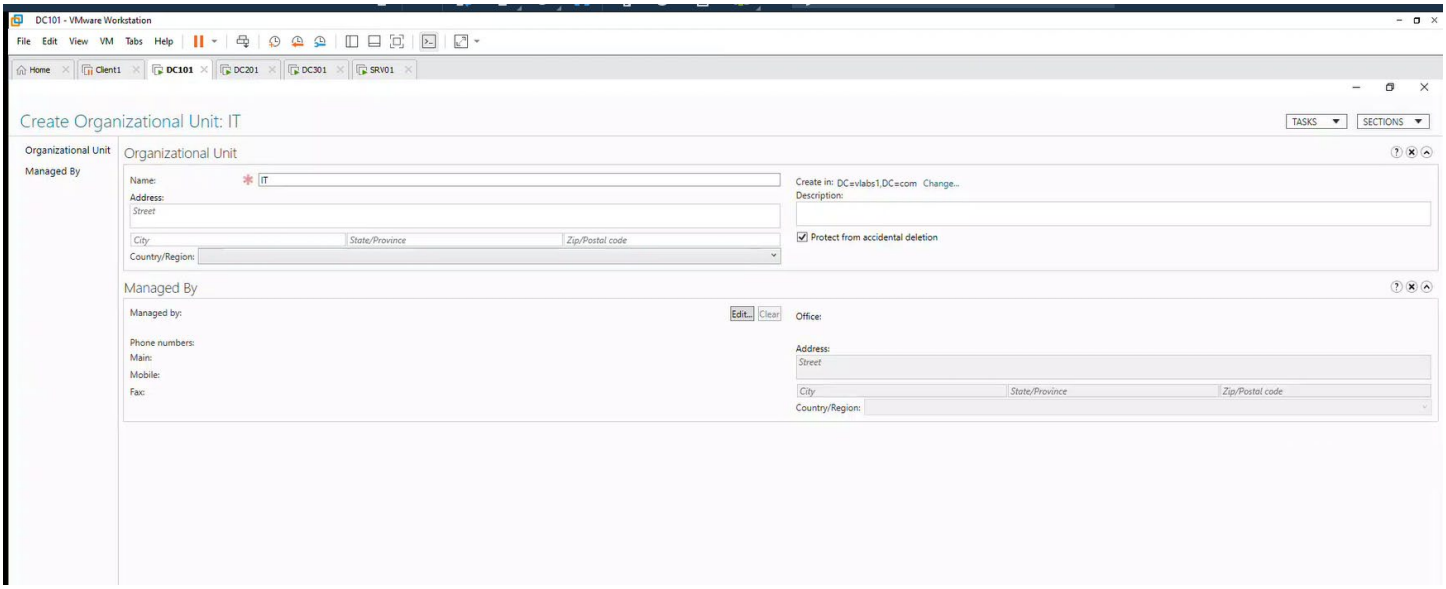


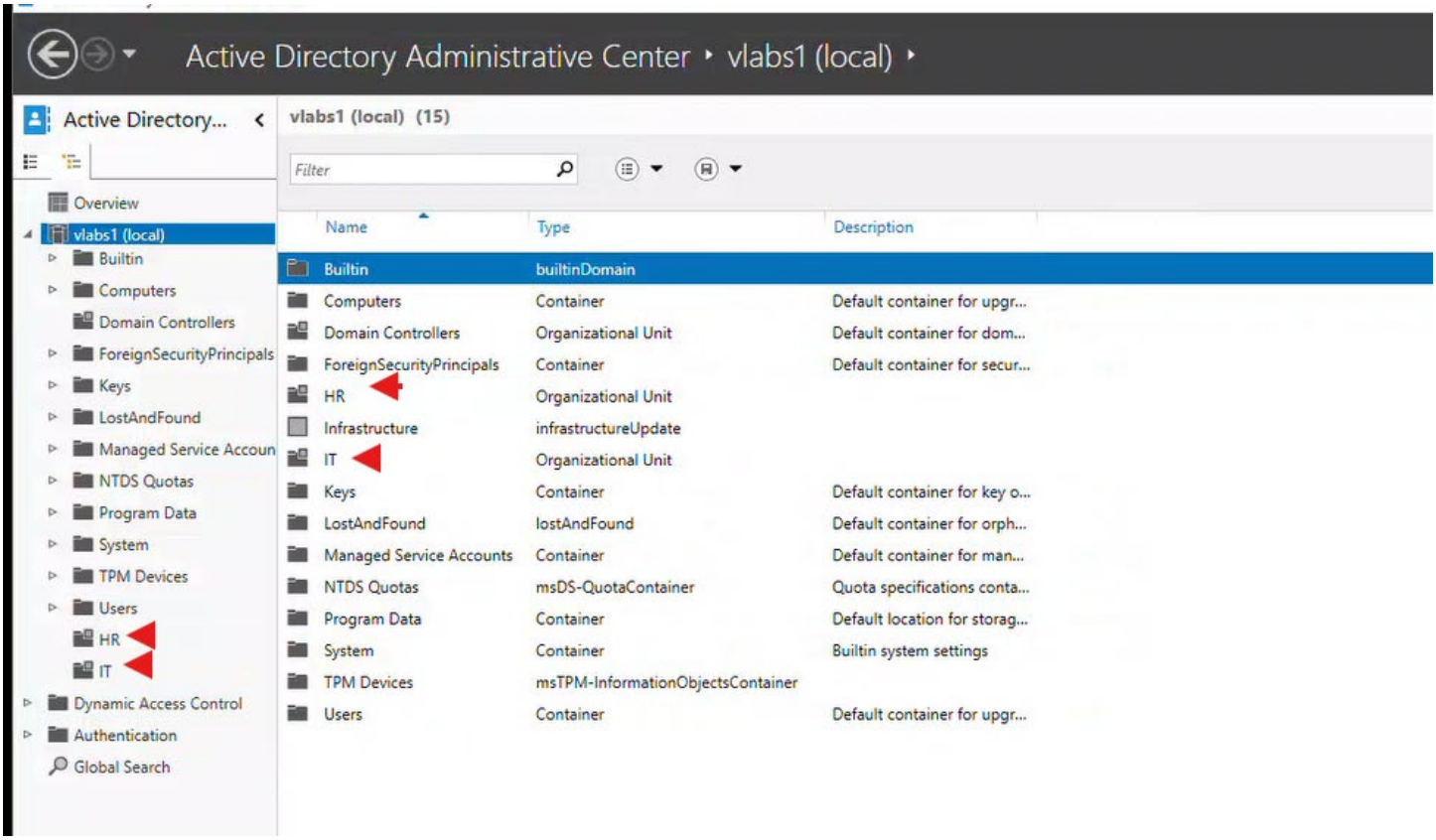
3. Create:

- HR OU (`OU=HR,DC=vlabs1,DC=com`)



- IT OU (`OU=IT,DC=vlabs1,DC=com`)



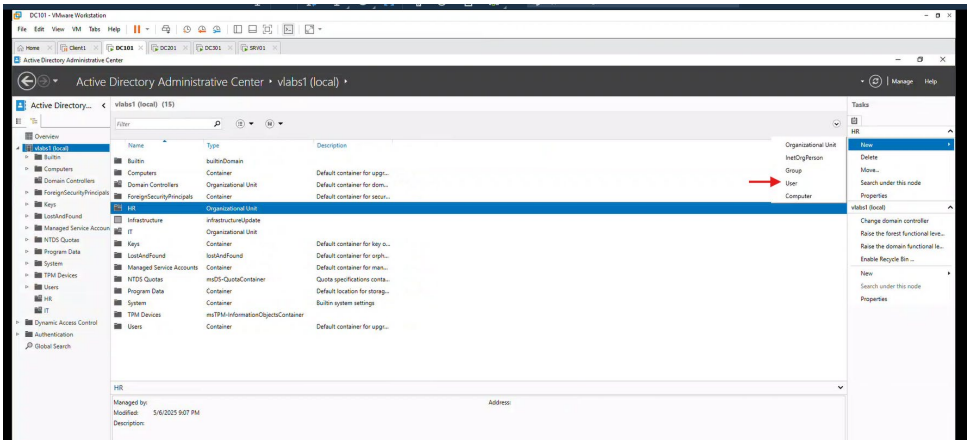


3.2 Create Users in HR OU Using ADAC

Create the following users in the HR OU using the Active Directory Administrative Center

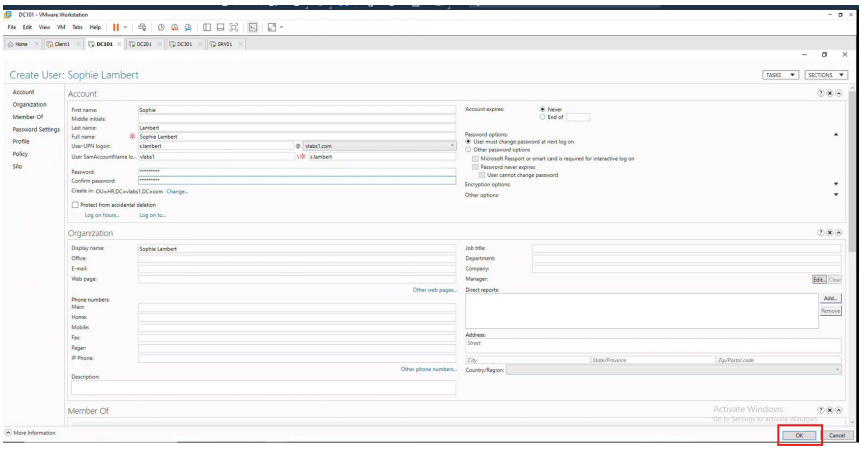
- Sophie Lambert (s.lambert)
- Liam Dupont (l.dupont)
- Emma Morel (e.morel)

1. In Active Directory Administrative Center, navigate to HR OU.

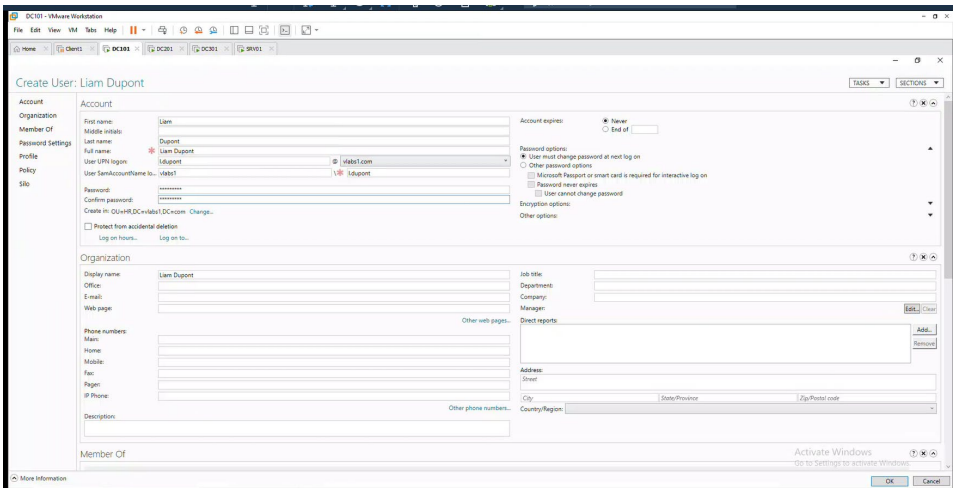


2. Click New → User and enter information
3. Set passwords and enable "User must change password at next logon" if required.
4. 4. Click OK to create users.

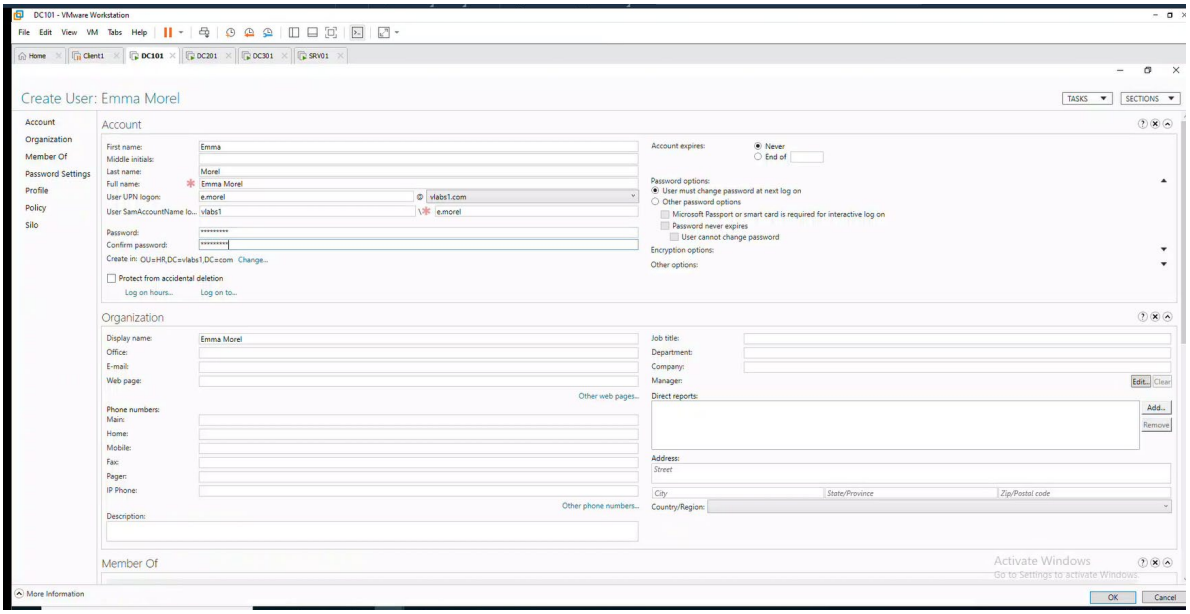
- `Name: Sophie Lambert | s.lambert`



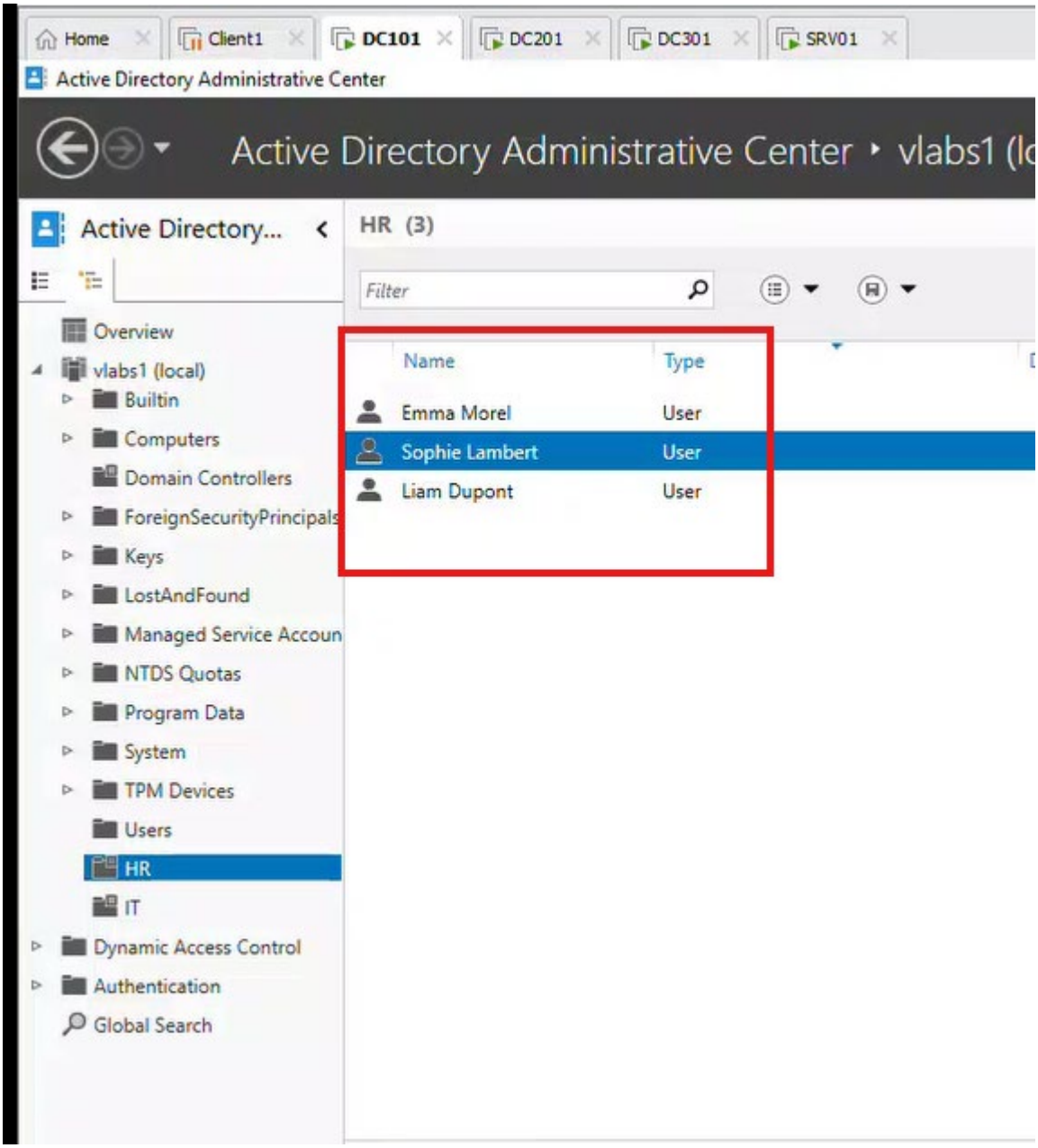
- `Name: Liam Dupont | l.dupont`



- `Name: Emma Morel | e.morel`



5. See created users under HR



3.3 Create Users in IT OU Using PowerShell

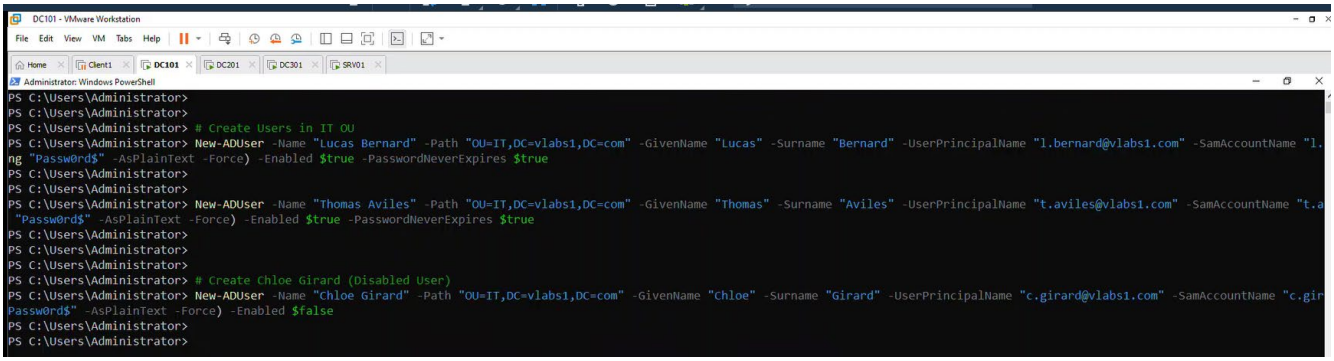
Create the following users in the **IT OU** using **PowerShell**:

- **Lucas Bernard (l.bernard)**
- **Thomas Aviles (t.aviles)**
- **Chloe Girard (c.girard)** ***(This user should be disabled during creation).***

```
# Create Users in IT OU
New-ADUser -Name "Lucas Bernard" -Path "OU=IT,DC=vlabs1,DC=com" -GivenName "Lucas" -Surname "Bernard" -UserPrincipalName "l.bernard@vlabs1.com" -SamAccountName "l.bernard" -AccountPassword (ConvertTo-SecureString "Passw0rd$" -AsPlainText -Force) -Enabled $true -PasswordNeverExpires $true
```

New-ADUser -Name "Thomas Aviles" -Path "OU=IT,DC=vlabs1,DC=com" -GivenName "Thomas" -Surname "Aviles" -UserPrincipalName "t.aviles@vlabs1.com" -SamAccountName "t.aviles" -AccountPassword (ConvertTo-SecureString "Passw0rd$" -AsPlainText -Force) -Enabled $true -PasswordNeverExpires $true

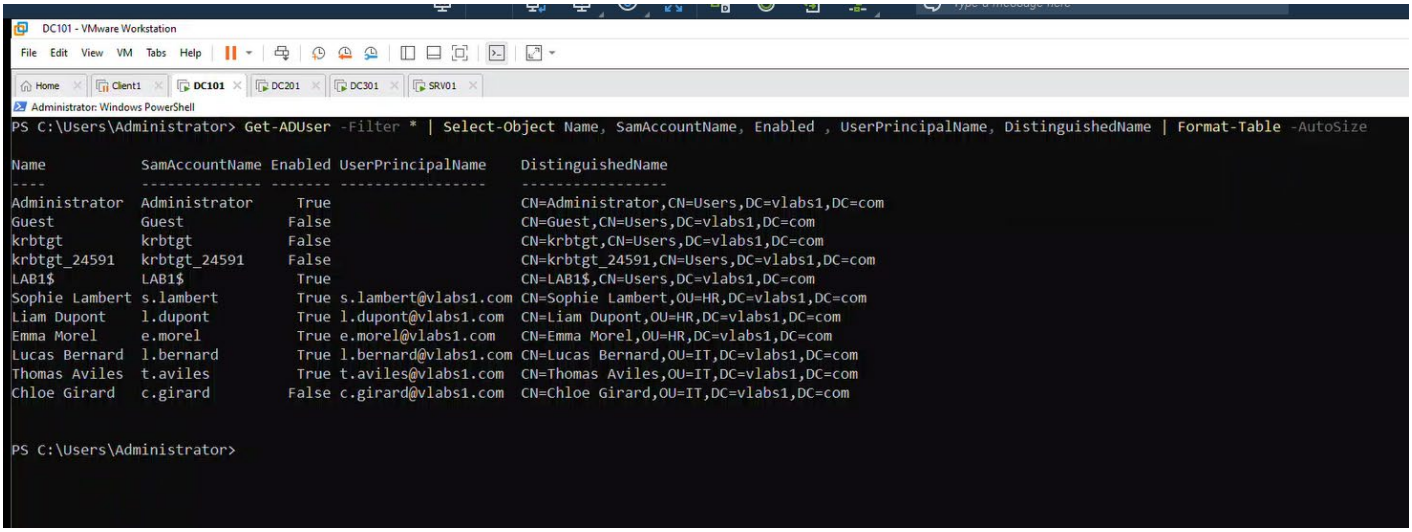
 # Create Chloe Girard (Disabled User)
New-ADUser -Name "Chloe Girard" -Path "OU=IT,DC=vlabs1,DC=com" -GivenName "Chloe" -Surname "Girard" -UserPrincipalName "c.girard@vlabs1.com" -SamAccountName "c.girard" -AccountPassword (ConvertTo-SecureString "Passw0rd$" -AsPlainText -Force) -Enabled $false



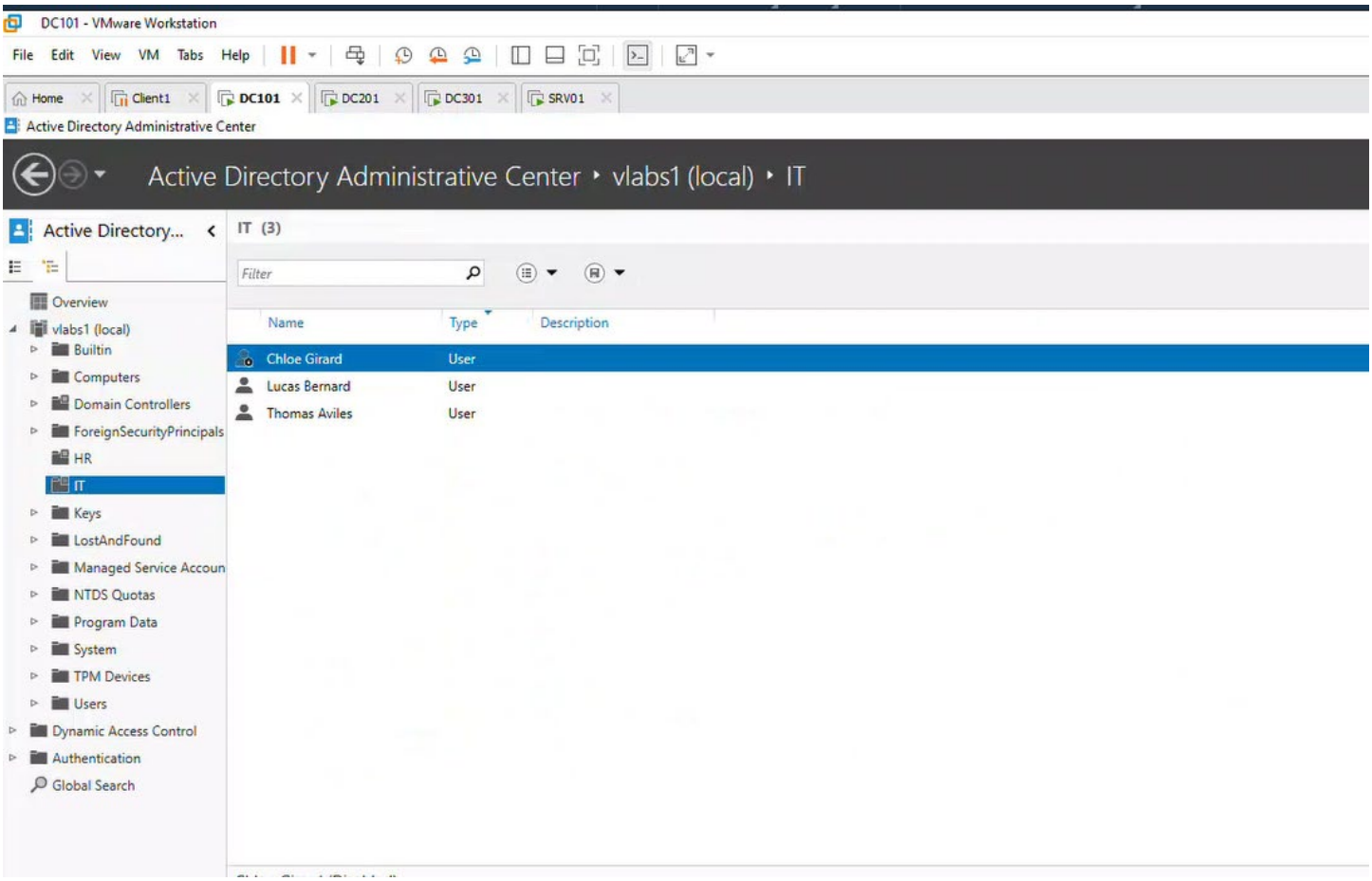
3.3.1 Verify users were created

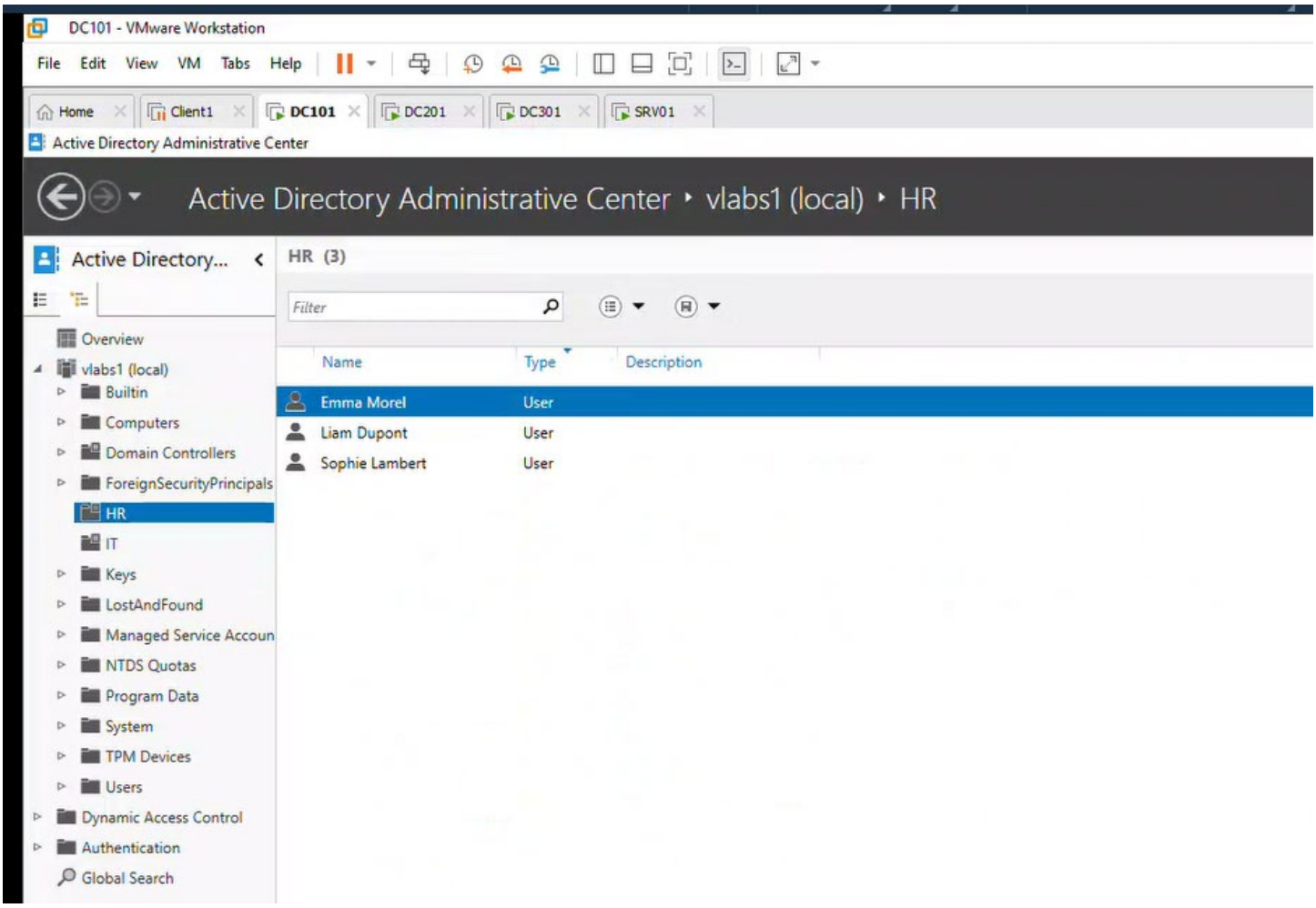
3.3.1.1 Powershell

Get-ADUser -Filter * | Select-Object Name, SamAccountName, Enabled , UserPrincipalName, DistinguishedName | Format-Table -AutoSize



3.3.1.2 Active Directory Administrative Center



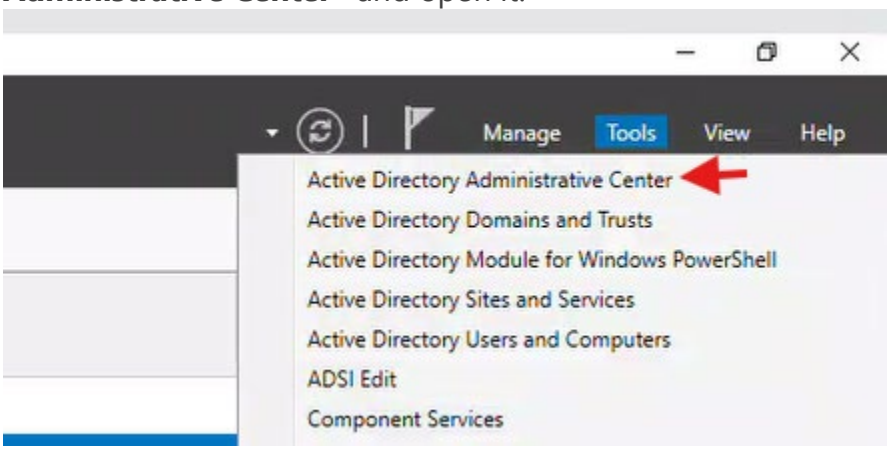

DC101 - VMware Workstation
File Edit View VM Tabs Help
Home
Client1
DC101
DC201
DC301
SRV01
Active Directory Administrative Center
Active Directory Administrative Center ‣ vlabs1 (local) ‣ HR
Active Directory...
HR (3)
Filter
Overview
vlabs1 (local)
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
HR
IT
Keys
LostAndFound
Managed Service Accoun
NTDS Quotas
Program Data
System
TPM Devices
Users
Dynamic Access Control
Authentication
Global Search
Name
Type
Description
Emma Morel
User
Liam Dupont
User
Sophie Lambert
User

4 Task 3: Delete Users

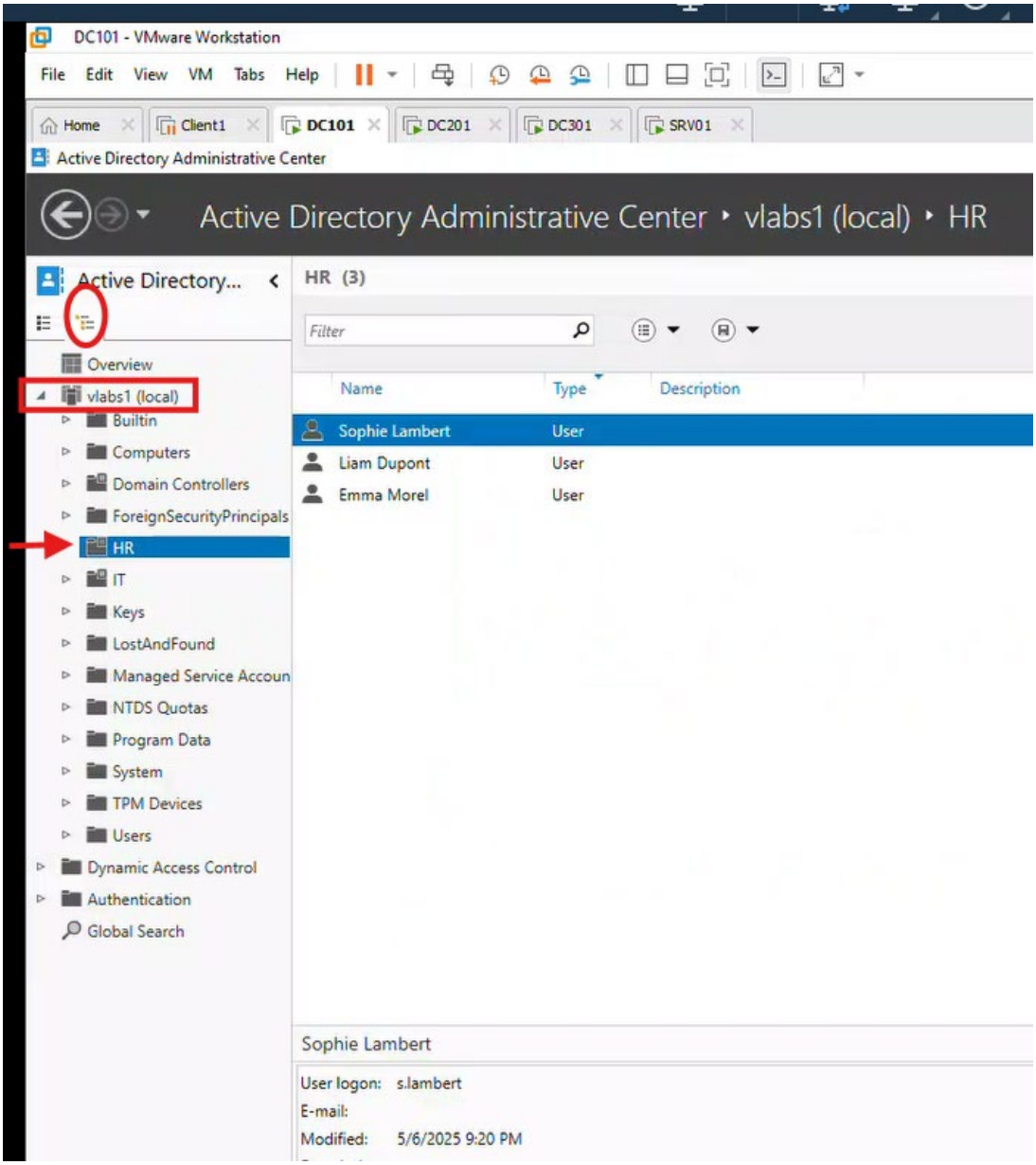
4.1 Delete user account using Active Directory Administrative Center

Delete the user account **Liam Dupont** using **Active Directory Administrative Center**

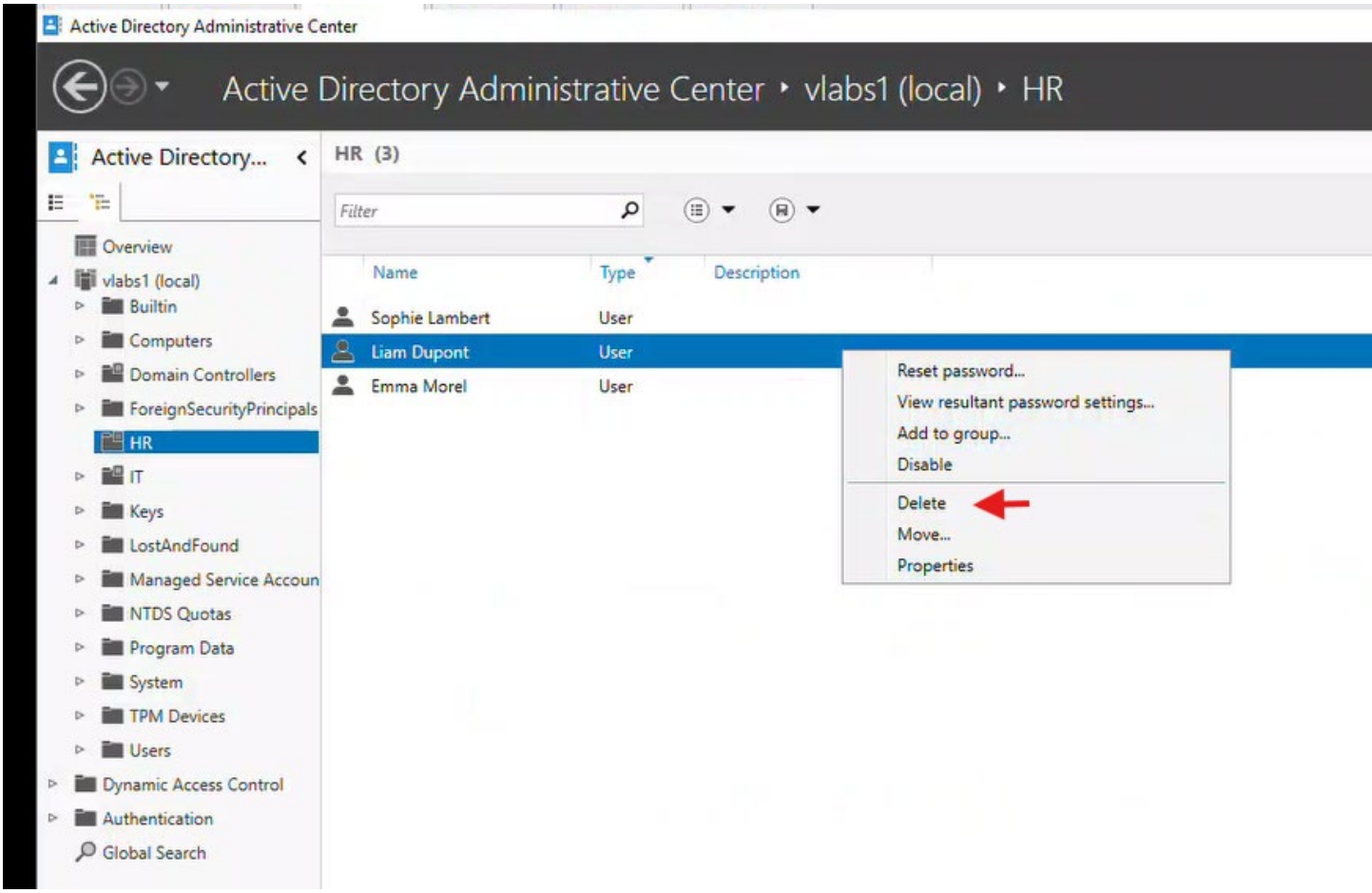
1. **Open Active Directory Administrative Center**
    - On **DC101** server manager, click **Tools** and search for **"Active Directory Administrative Center"** and open it.



2. **Navigate to the HR OU**
    - In the left pane, expand your domain (**vlabs1.com**).
    - Locate and click on the **HR** Organizational Unit (OU).

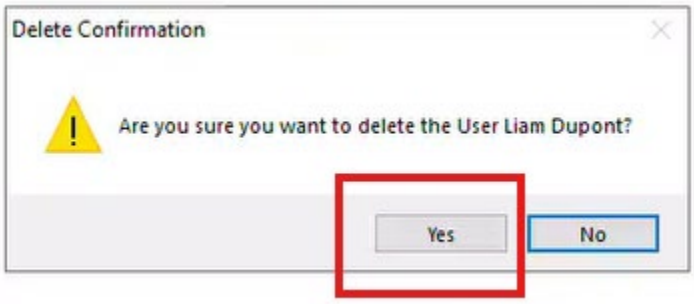


3. **Find and Select Liam Dupont**
    - In the center pane, locate the user **"Liam Dupont"** (or **l.dupont** in the username column).
    - Right-click on the user and select **Delete**.

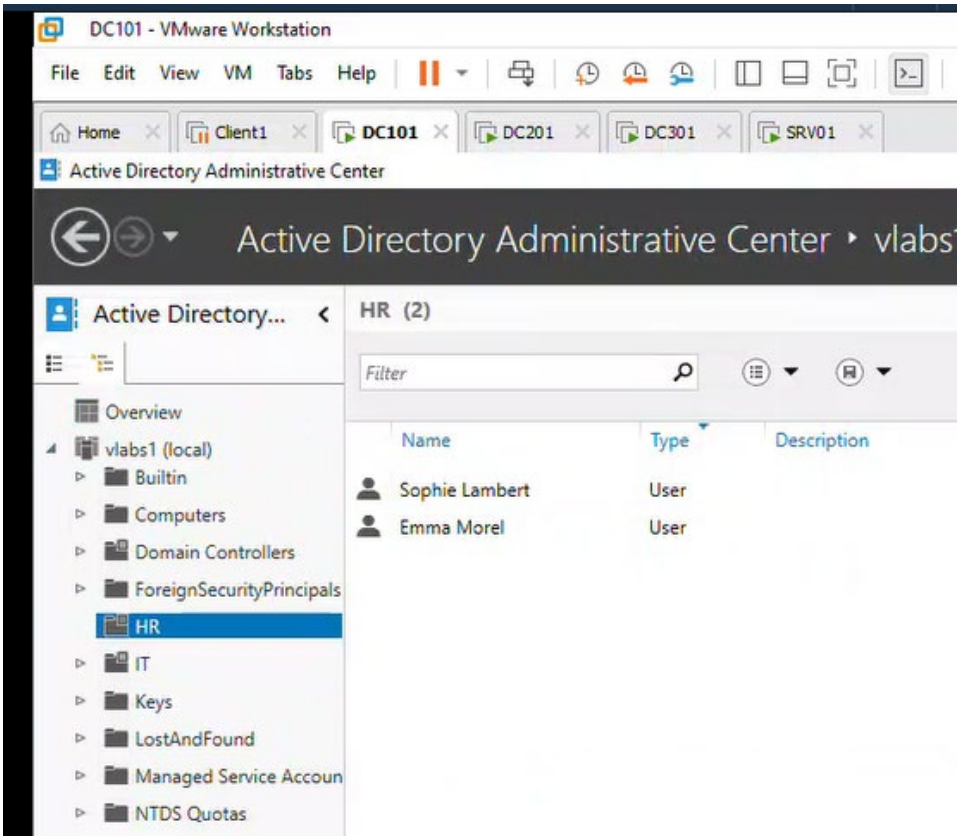


4. **Confirm Deletion**
    - A confirmation prompt will appear:

      "Are you sure you want to delete the user Liam Dupont?"
    - Click **Yes** to permanently delete the user.



5. See user does not appear anymore



4.2 Delete user account using PowerShell

Delete the user account **Thomas Aviles** using **PowerShell**.

1. Find the User's DistinguishedName

Get-ADUser -Identity "t.aviles" -Properties DistinguishedName | Select-Object DistinguishedName

2. Now, use the Remove-ADUser command with the full DN:

Remove-ADUser -Identity "CN=Thomas Aviles,OU=IT,DC=vlabs1,DC=com" -Confirm:$false

3. Verify Deletion

Check if the user no longer exists:

Get-ADUser -Filter "SamAccountName -eq 't.aviles'"

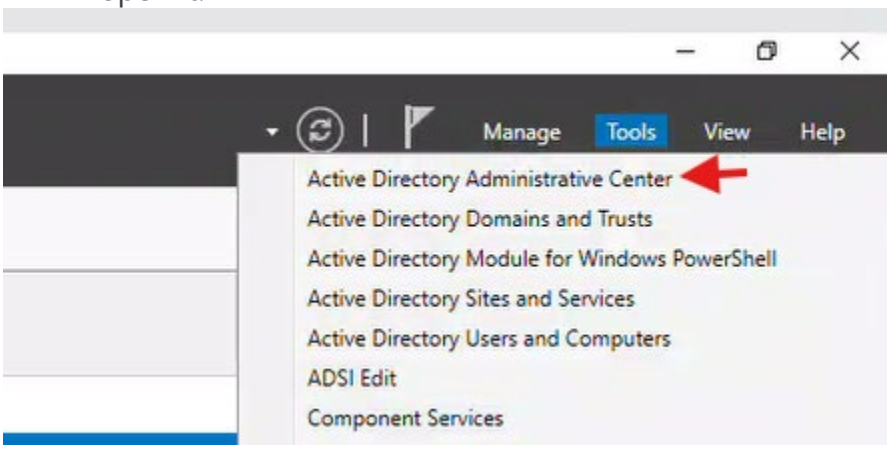
```
PS C:\Users\Administrator> Get-ADUser -Identity "t.aviles" -Properties DistinguishedName | Select-Object DistinguishedName

DistinguishedName
-----------------
CN=Thomas Aviles,OU=IT,DC=vlabs1,DC=com


PS C:\Users\Administrator> Remove-ADUser -Identity "CN=Thomas Aviles,OU=IT,DC=vlabs1,DC=com" -Confirm:$false
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADUser -Filter "SamAccountName -eq 't.aviles'"
PS C:\Users\Administrator>
```

5 Task 4: Move Users Between Organizational Units (OUs)

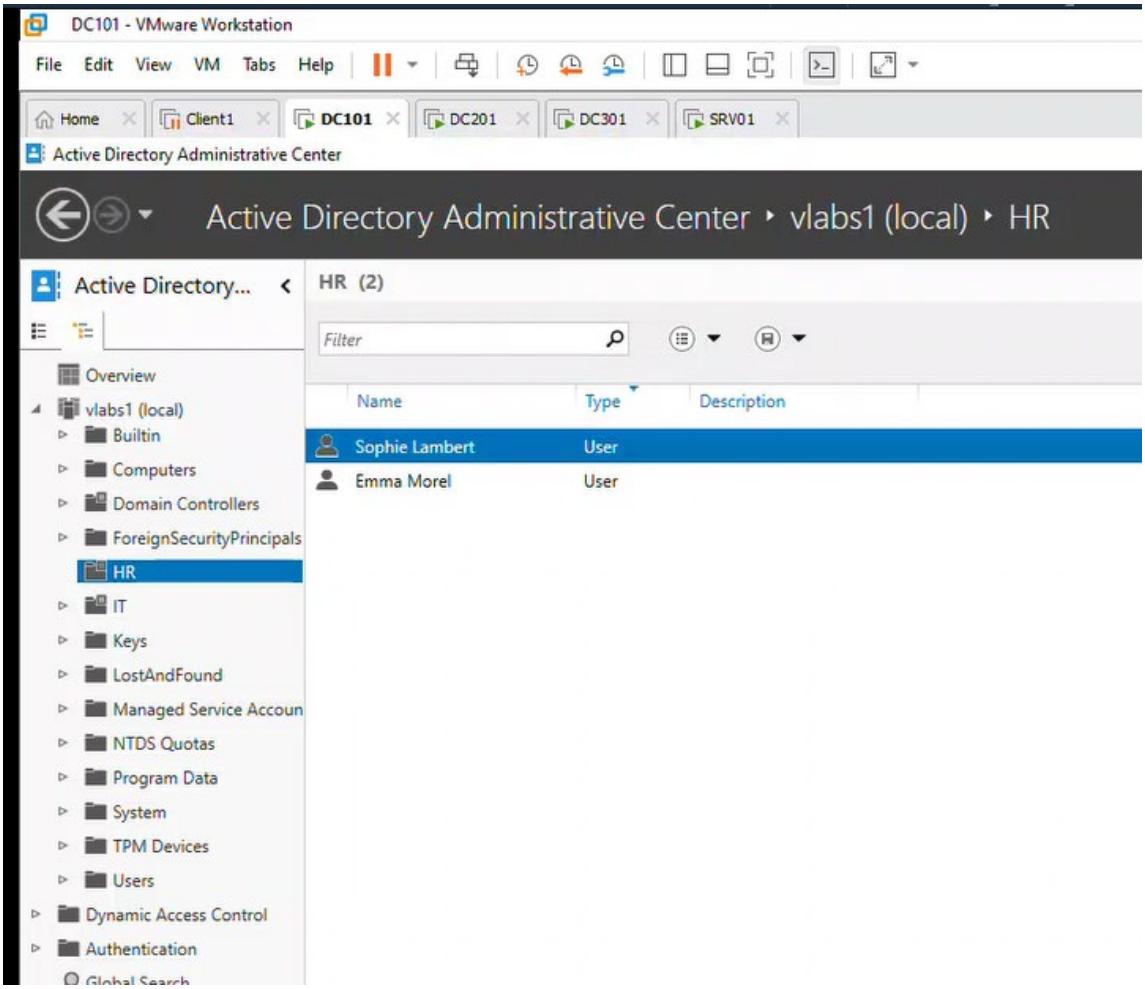
5.1 Move the user account using Active Directory Administrative Center

Move the user account Sophie Lambert to the IT OU using Active Directory Administrative Center

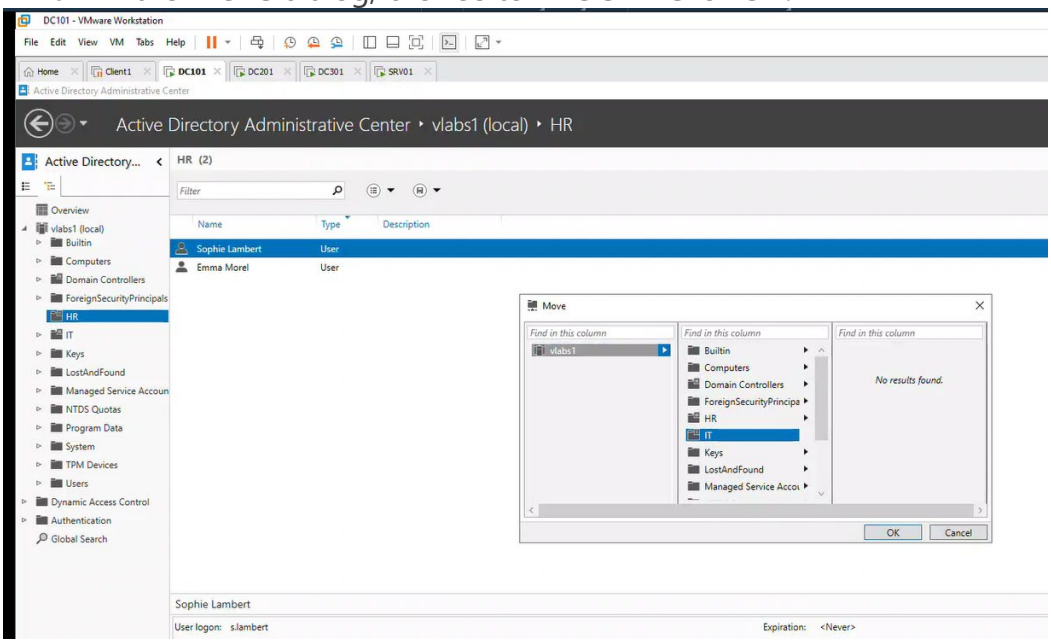
1. **Open Active Directory Administrative Center (ADAC)**
    - On **DC101**, click **Tools** → Search for **"Active Directory Administrative Center"** and open it.



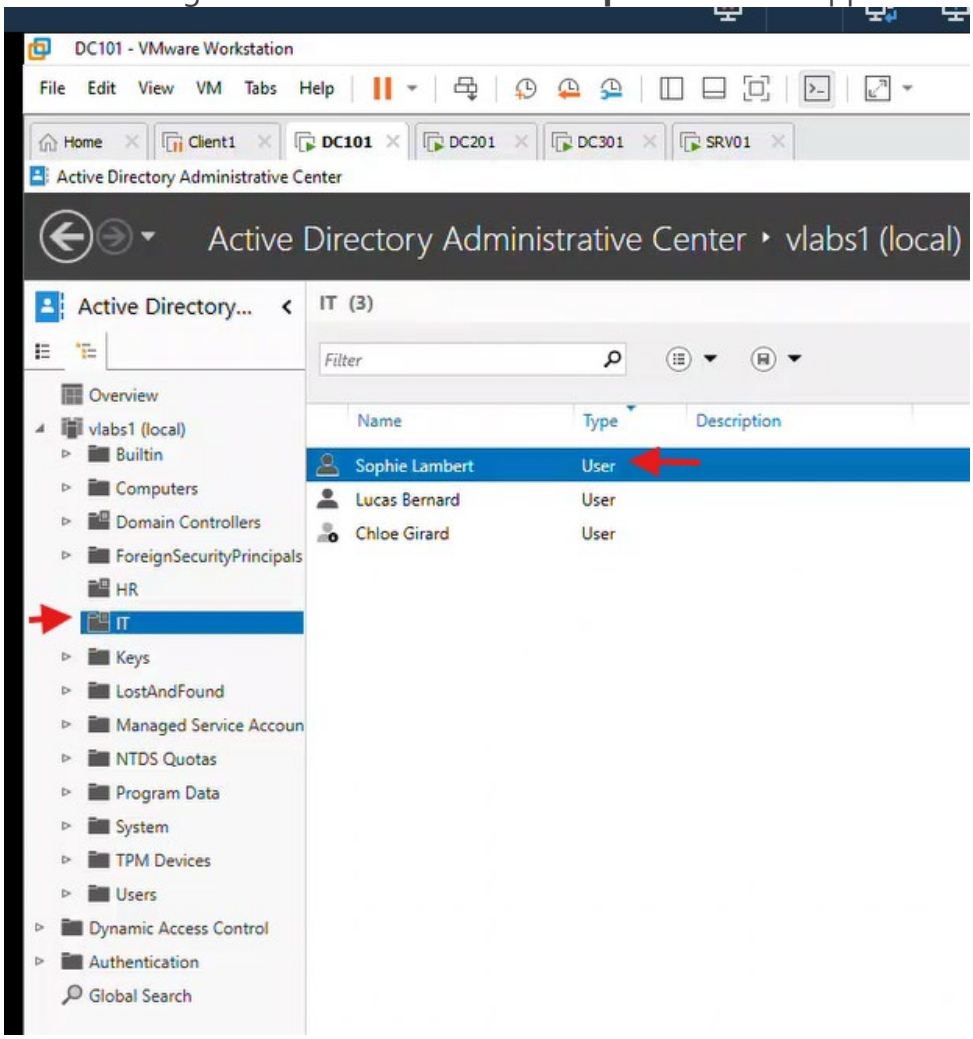
2. **Locate Sophie Lambert**
    - In the left pane, expand **vlabs1.com** → Navigate to the **HR** OU.
    - Find and select **Sophie Lambert** (or **s.lambert**).



3. **Move the User to the IT OU**
    - **Right-click** on **Sophie Lambert** → Select **Move...**
    - In the **Move** dialog, browse to **IT OU** → Click **OK**.



4. **Verify the Move**
    - Navigate to **IT OU** and confirm **Sophie Lambert** appears there.



5.2 Move the user account using PowerShell

Move the user account Lucas Bernard to the HR OU using PowerShell.

1. Find the User to be moved

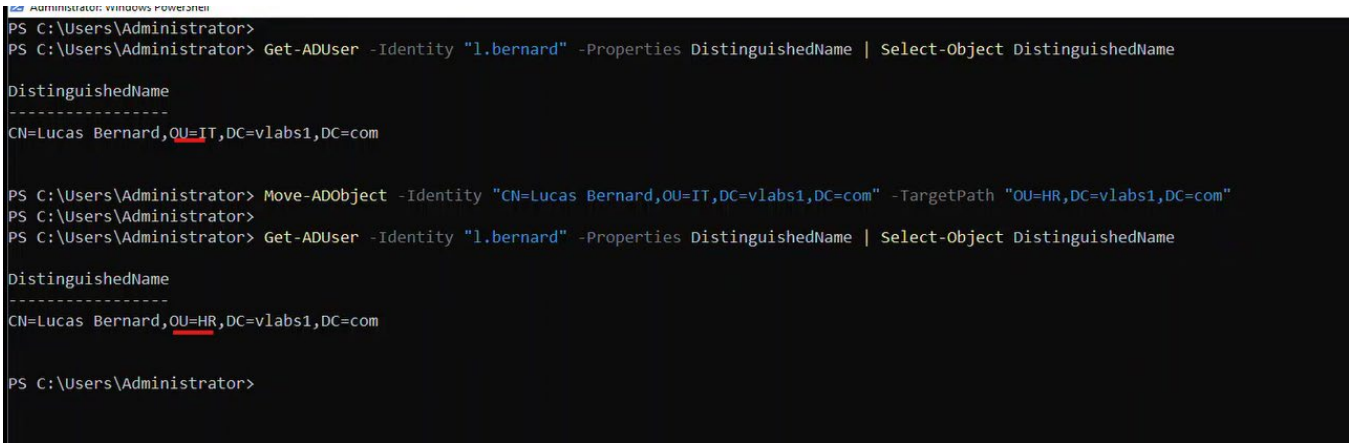
Get-ADUser -Identity "l.bernard" -Properties DistinguishedName | Select-Object DistinguishedName

2. Run the following command to move user

Move-ADObject -Identity "CN=Lucas Bernard,OU=IT,DC=vlabs1,DC=com" -TargetPath "OU=HR,DC=vlabs1,DC=com"

3. Find the moved User

Get-ADUser -Identity "l.bernard" -Properties DistinguishedName | Select-Object DistinguishedName



6 Task 5: Modify Users in IT OU

Assign the user account Sophie Lambert as Manager for all users in the IT OU using PowerShell.

1. First, we need to get Sophie Lambert's full distinguished name (DN):

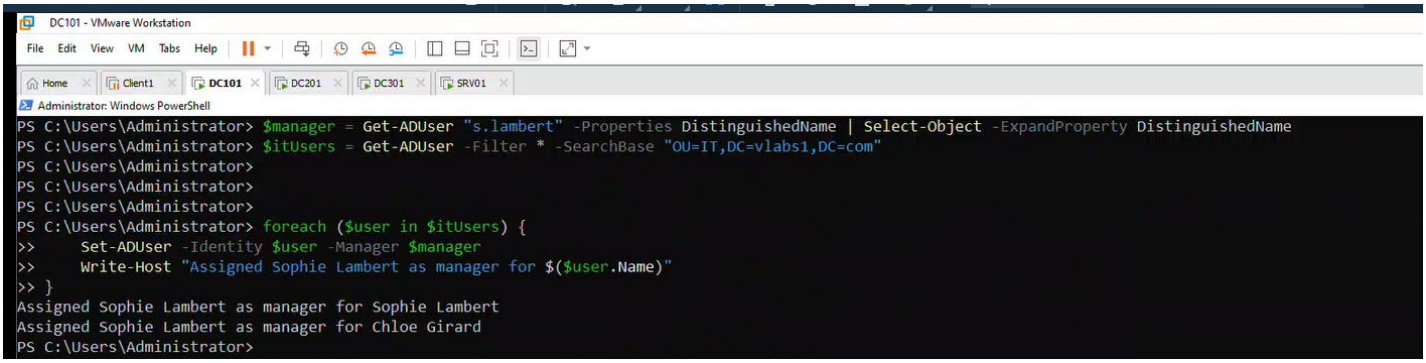
```
$manager = Get-ADUser "s.lambert" -Properties DistinguishedName | Select-Object -ExpandProperty DistinguishedName
```

2. Get All Users in the IT OU

```
$itUsers = Get-ADUser -Filter * -SearchBase "OU=IT,DC=vlabs1,DC=com"
```

3. Assign Sophie Lambert as Manager
   Loop through each user and assign Sophie Lambert as their manager:

```
foreach ($user in $itUsers) {
  Set-ADUser -Identity $user -Manager $manager
  Write-Host "Assigned Sophie Lambert as manager for $($user.Name)"
}
```



4. Verify the changes:

```
Get-ADUser -Filter * -SearchBase "OU=IT,DC=vlabs1,DC=com" -Properties Name,SamAccountName,Manager |    Select-Object Name, SamAccountName, @{Name="Manager";Expression={(Get-ADUser $_.Manager -ErrorAction SilentlyContinue).Name}} |
  Format-Table -AutoSize
```

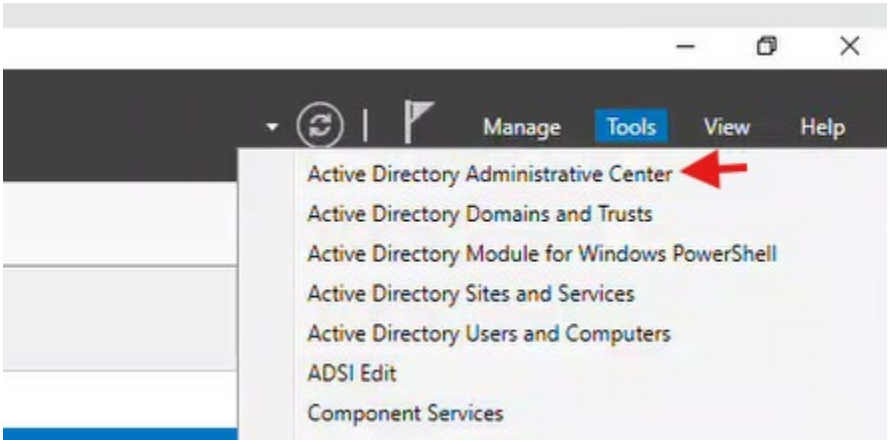
```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADUser -Filter * -SearchBase "OU=IT,DC=vlabs1,DC=com" -Properties Name,SamAccountName,Manager |     Select-Object Name, SamAccountName, @{Name="Manager";Expres
sion={(Get-ADUser $_.Manager -ErrorAction SilentlyContinue).Name}} | Format-Table -AutoSize

Name           SamAccountName Manager
----           -------------- -------
Sophie Lambert s.lambert      Sophie Lambert
Chloe Girard   c.girard       Sophie Lambert


PS C:\Users\Administrator>
```

7 Task 6: Enable and Disable User Accounts

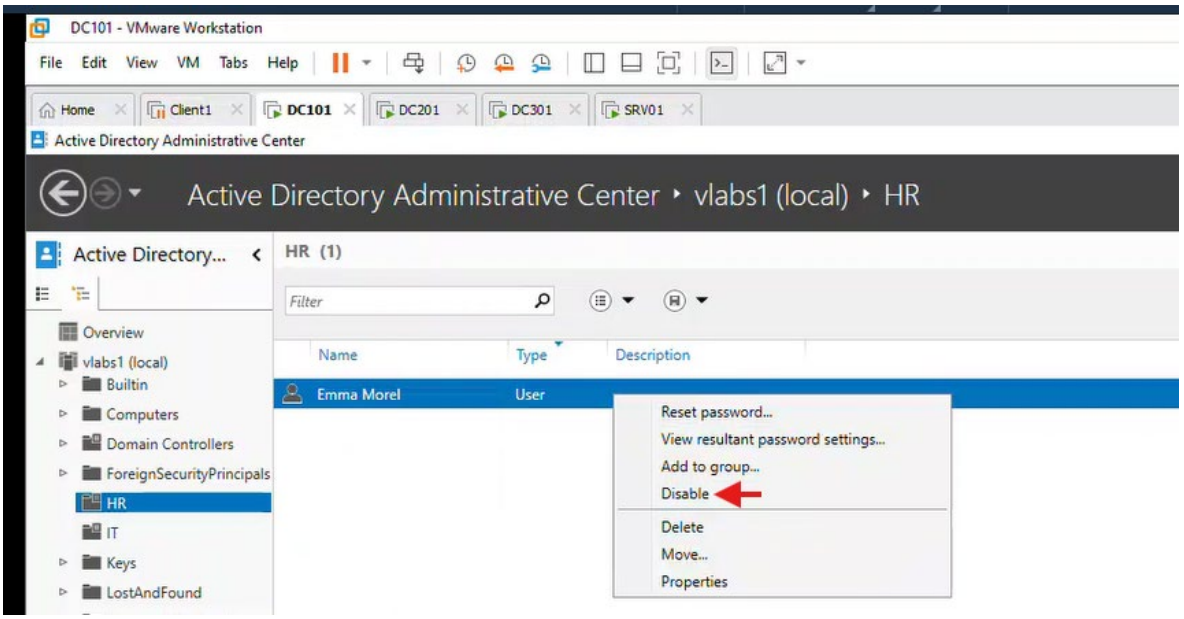
7.1 Disable user account using the Active Directory Administrative Center

Disable the user account **Emma Morel** using the **Active Directory Administrative Center.**

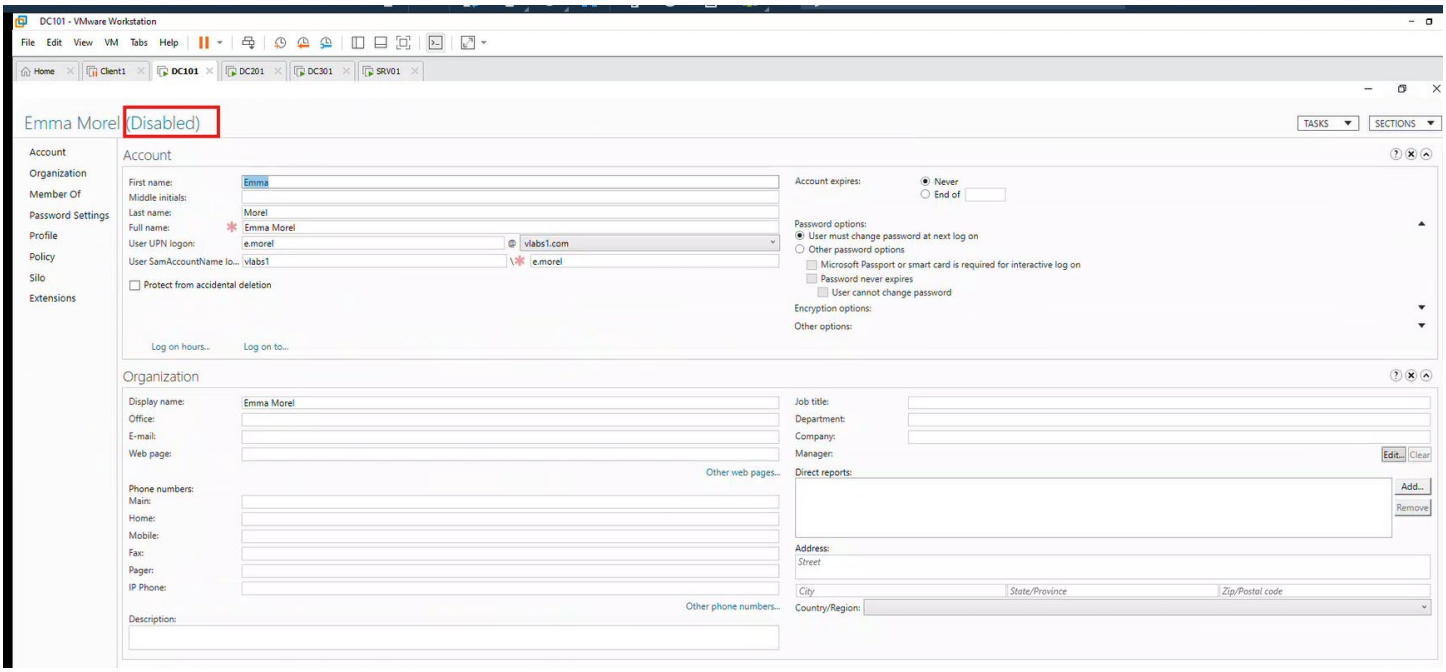
1. Open ADAC



2. Navigate to HR OU (vlabs1.com → HR).
3. Right-click Emma Morel → Select Disable.



4. Verify user is disabled



7.2 Enable the user account using PowerShell

Enable the user account **Chloe Girard** using **PowerShell**.

1. Check if **Chloe Girard** is currently disabled:

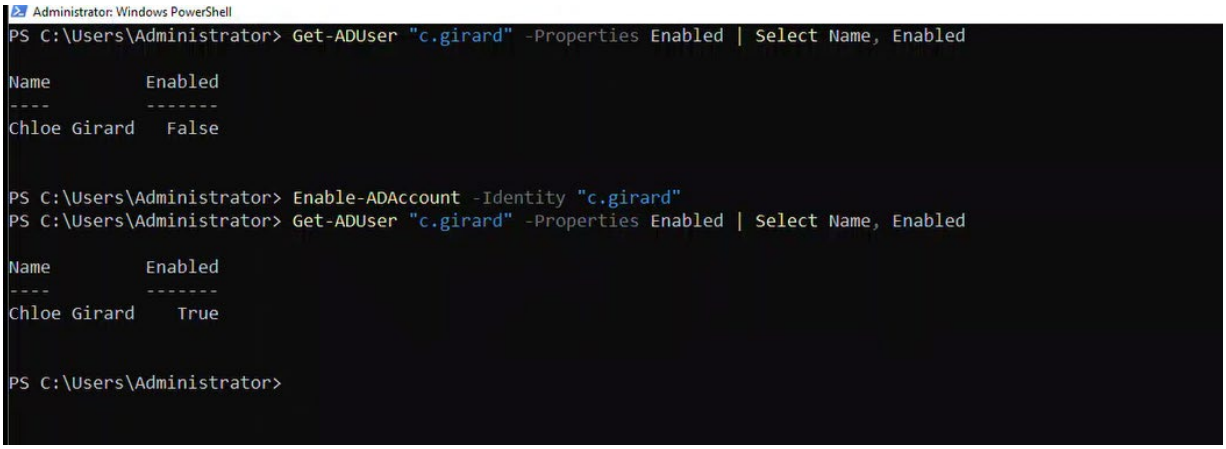
Get-ADUser "c.girard" -Properties Enabled | Select Name, Enabled

2. **Command to Enable the Account:**

Enable-ADAccount -Identity "c.girard"

3. **Post-Check (Verify Enabled Status)**

Get-ADUser "c.girard" -Properties Enabled | Select Name, Enabled



8 Task 7: Lock and Unlock Users

1. Find all locked-out users using **PowerShell**.

   Search-ADAccount -LockedOut -UsersOnly | Select-Object Name, SamAccountName, LastBadPasswordAttempt, LockedOut, DistinguishedName | Format-Table -AutoSize

   Get-ADUser -Filter {LockedOut -eq $true} -Properties LockedOut,LastBadPasswordAttempt | Select Name,SamAccountName,LockedOut,LastBadPasswordAttempt,DistinguishedName

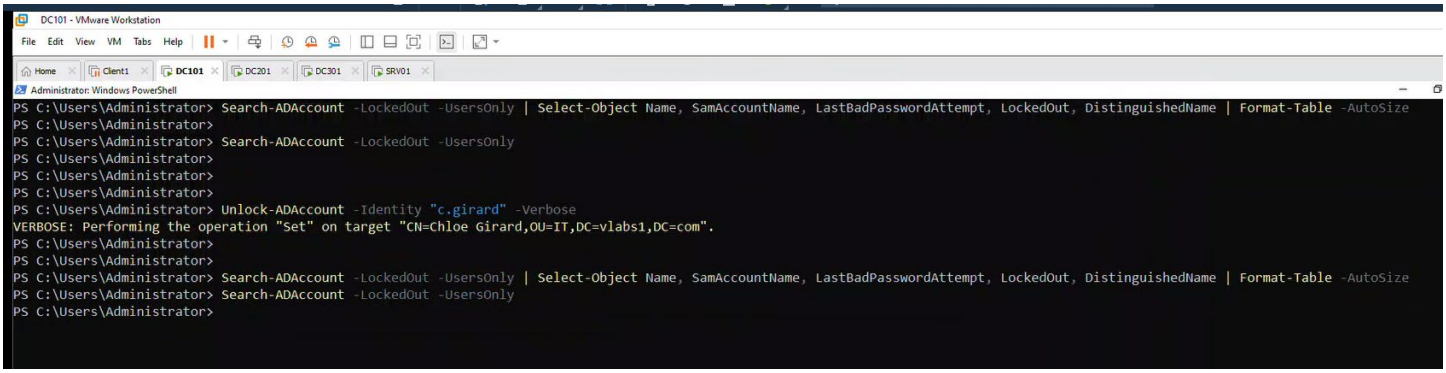
2. Try to unlock the user account **Chloe Girard** using **PowerShell.** *Note: His account is not locked. It is just to practice this command.*

   Unlock-ADAccount -Identity "c.girard" -Verbose

3. Find all locked-out users using **PowerShell**.

   Search-ADAccount -LockedOut -UsersOnly | Select-Object Name, SamAccountName, LastBadPasswordAttempt, LockedOut, DistinguishedName | Format-Table -AutoSize

   Get-ADUser -Filter {LockedOut -eq $true} -Properties LockedOut,LastBadPasswordAttempt | Select Name,SamAccountName,LockedOut,LastBadPasswordAttempt,DistinguishedName



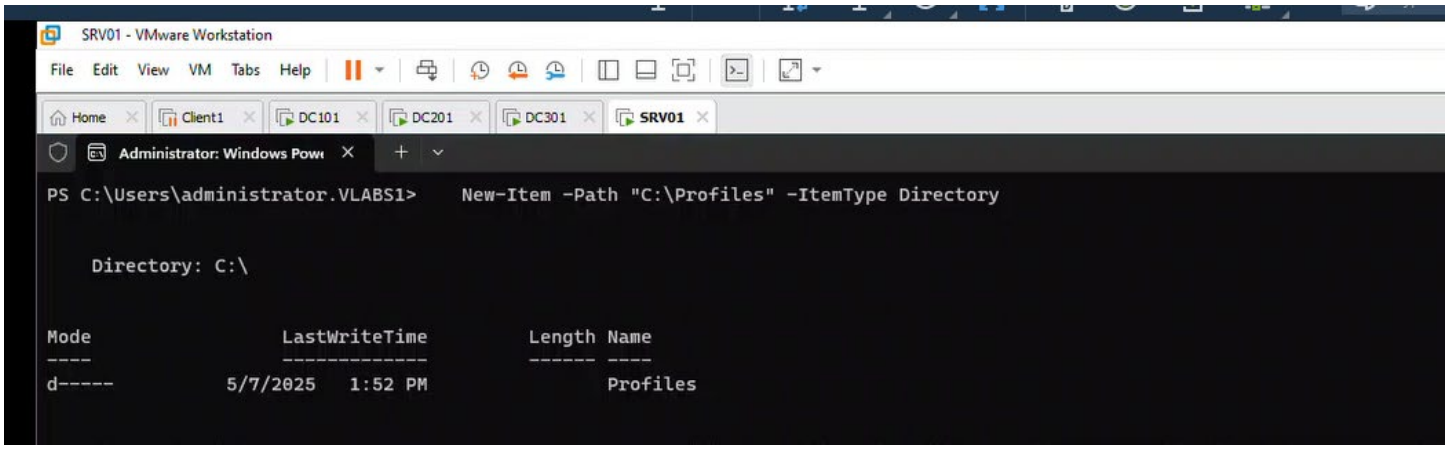
9 Task 8: Configure Roaming Profiles on SRV01

9.1 Create a shared folder **C:\Profiles** on **SRV01**.

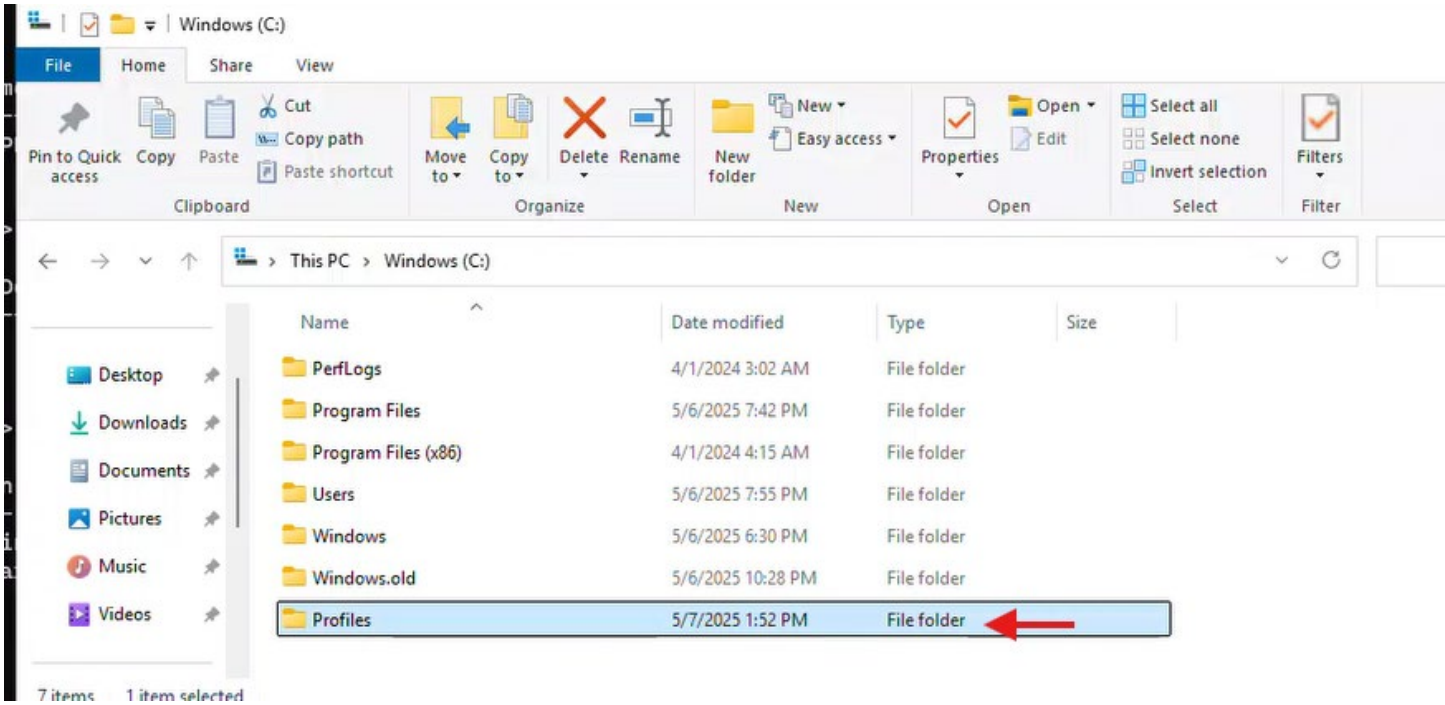
On SRV01 (Windows Server 2025):

1. Create the profiles folder:

   New-Item -Path "C:\Profiles" -ItemType Directory



2. Locate the Folder:



9.2 Share the folder with appropriate permissions

9.2.1 Create and share the profile on a File Server

New-SmbShare-Name "Profiles$" -Path "C:\Profiles" -FullAccess"Authenticated Users","Administrators" -ChangeAccess"Domain Users"

9.2.2 Verify folder permissions

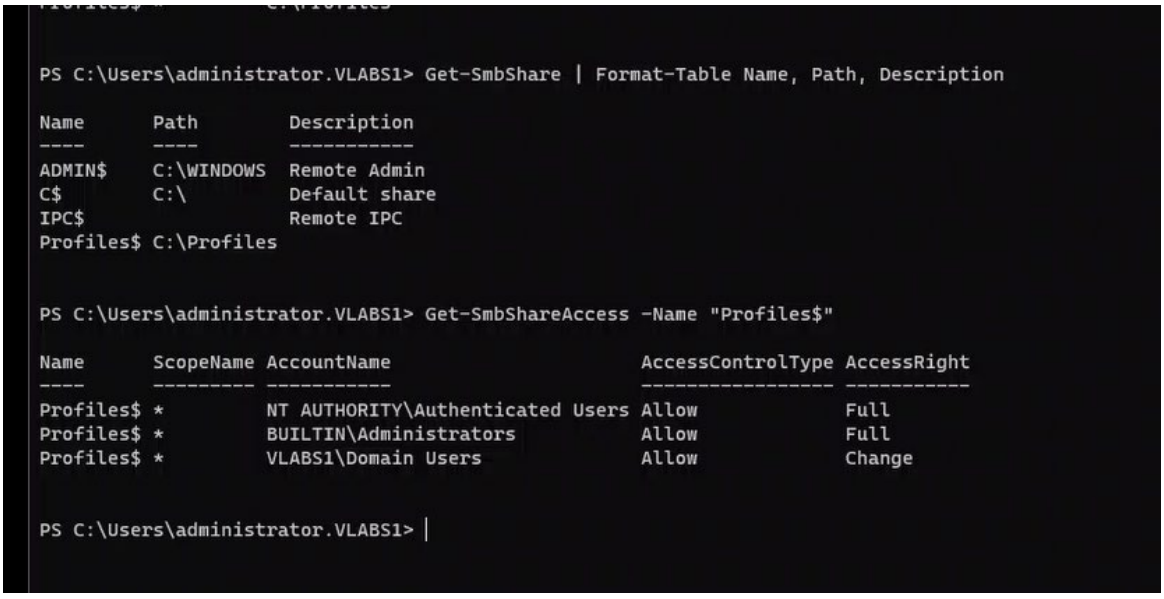
9.2.2.1 Via powershell

Check Existing SMB Shares

Get-SmbShare | Format-Table Name, Path, Description

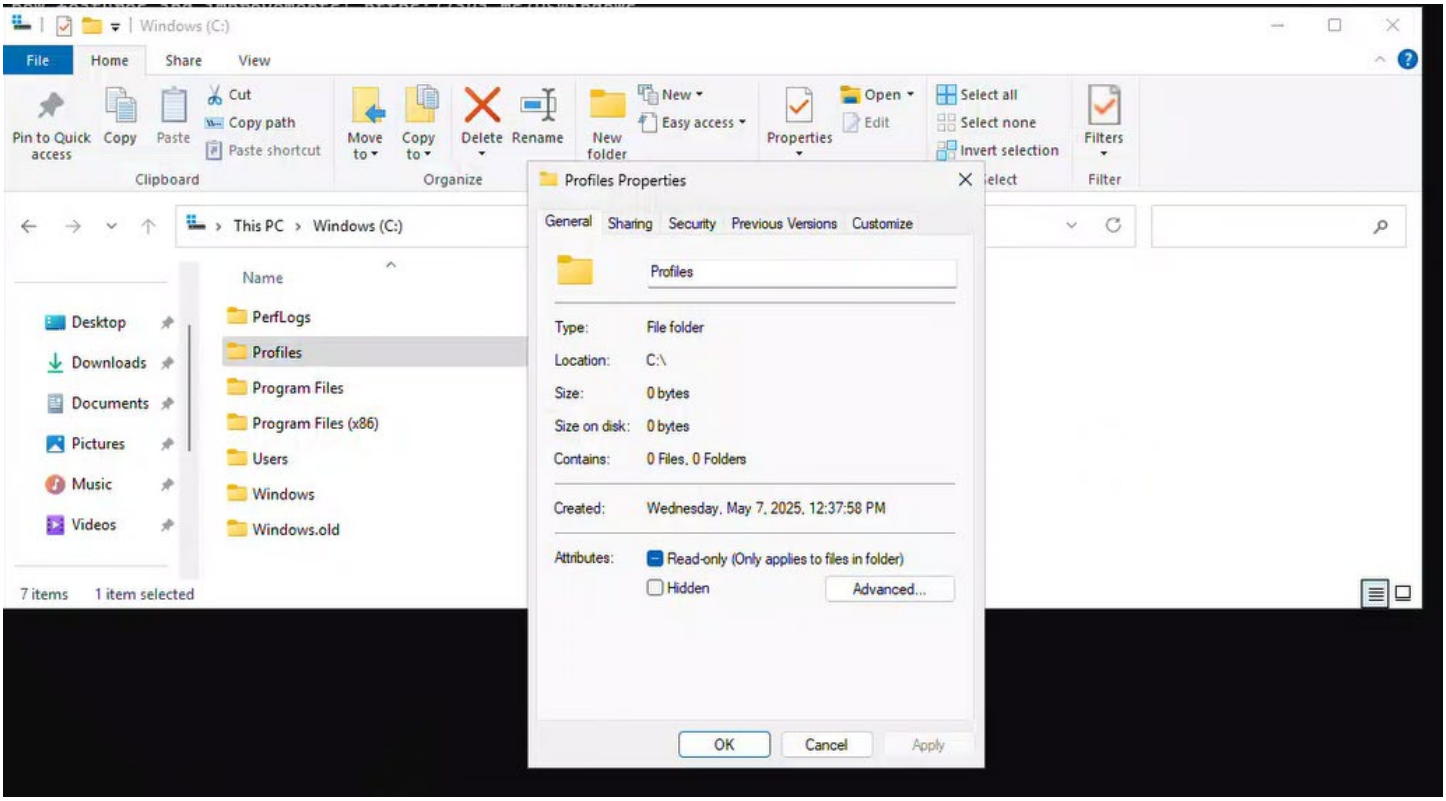
Verify permissions on the share

Get-SmbShareAccess -Name "Profiles$"



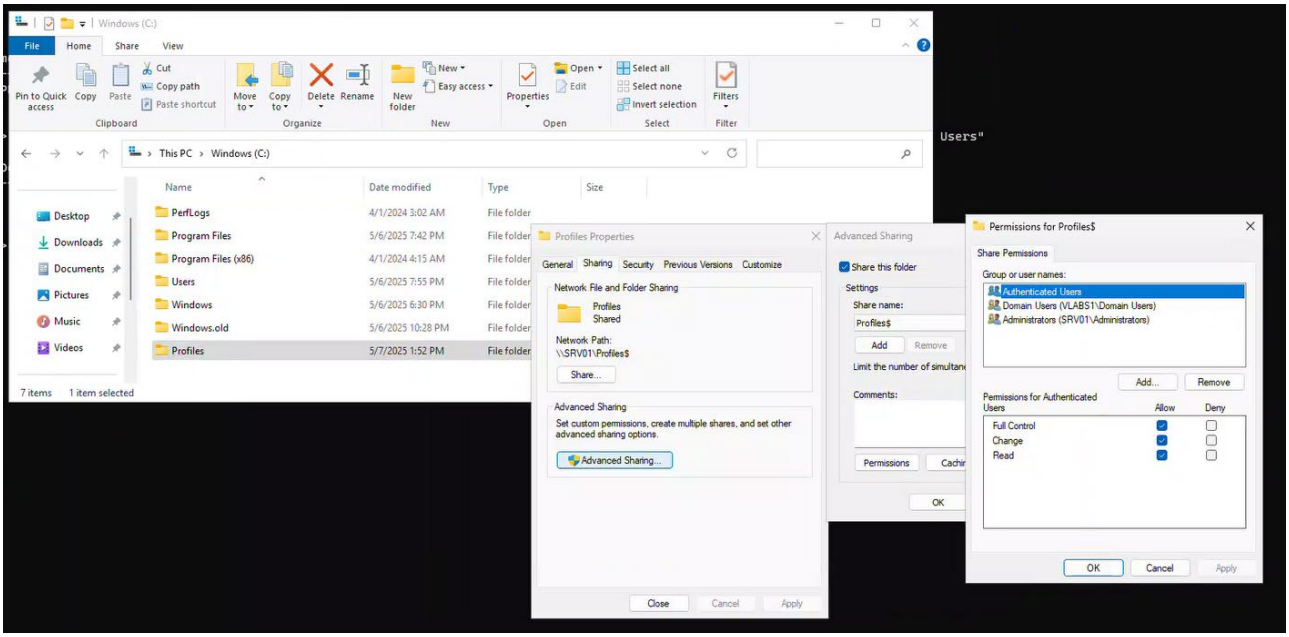
9.2.2.2 Via GUI

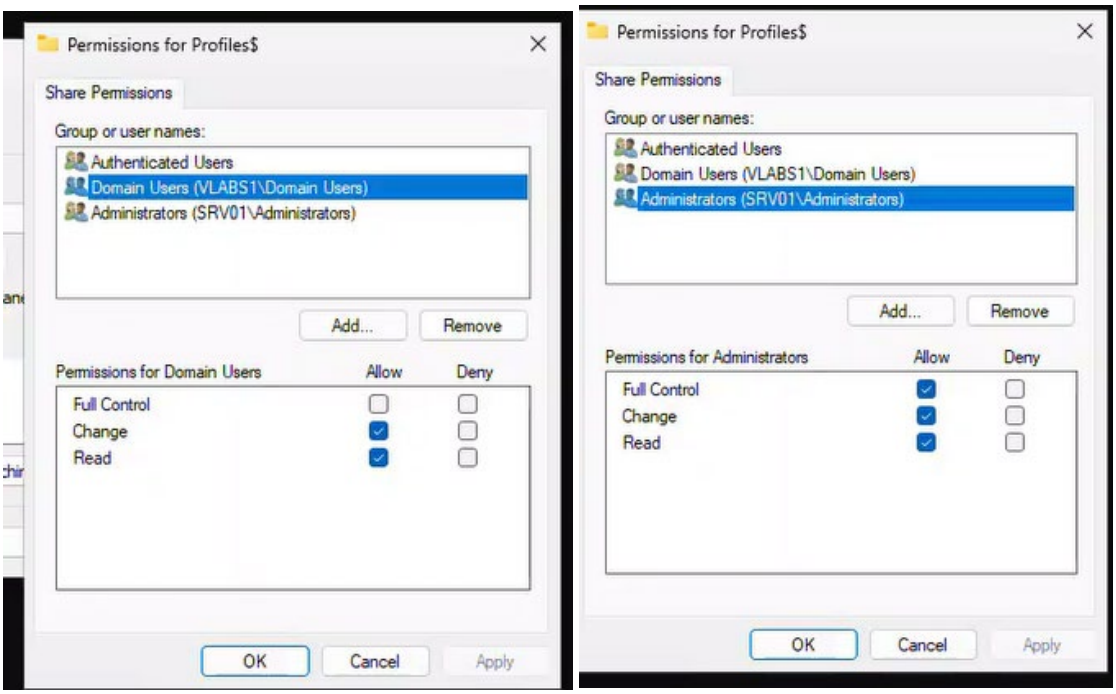
1. Right-click the folder → Properties.



2. Enable Sharing
   - Go to the Sharing tab → Click Advanced Sharing.

3. Click Permissions, see:
   - Authenticated Users → Full Control.
   - Domain Users → Change.
   - Administrators → Full Control.





9.3 Configure NTFS and share permissions for roaming profiles

9.3.1 Configure NTFS permissions for the Profiles folder

icacls "C:\Profiles" /grant "Authenticated Users:(OI)(CI)(M)" "Administrators:(OI)(CI)(F)" "SYSTEM:(OI)(CI)(F)"

```
>>
PS C:\Users\administrator.VLABS1> icacls "C:\Profiles" /grant "Authenticated Users:(OI)(CI)(M)" "Administrators:(OI)(CI)(F)" "SYSTEM:(OI)(CI)(F)"
processed file: C:\Profiles
Successfully processed 1 files; Failed processing 0 files
PS C:\Users\administrator.VLABS1>
```

This command:

1. Grants Modify permissions (M) to Authenticated Users with object inherit (OI) and container inherit (CI)

2. Grants Full control (F) to Administrators with inheritance

3. Grants Full control (F) to SYSTEM with inheritance

9.3.2 Verify

9.3.2.1 Powershell

icacls “C:\Profiles”

```
PS C:\Users\administrator.VLABS1>
PS C:\Users\administrator.VLABS1> icacls "C:\Profiles"
C:\Profiles BUILTIN\Administrators:(F)
            NT AUTHORITY\SYSTEM:(OI)(CI)(F)
            BUILTIN\Administrators:(OI)(CI)(F)
            NT AUTHORITY\Authenticated Users:(OI)(CI)(M)
            NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
            BUILTIN\Administrators:(I)(OI)(CI)(F)
            BUILTIN\Users:(I)(OI)(CI)(RX)
            BUILTIN\Users:(I)(CI)(AD)
            BUILTIN\Users:(I)(CI)(WD)
            CREATOR OWNER:(I)(OI)(CI)(IO)(F)

Successfully processed 1 files; Failed processing 0 files
PS C:\Users\administrator.VLABS1>
```

- F) = **Full Control**
- (M) = **Modify**
- (RX) = **Read & Execute**
- (AD) = **Append Data** (ability to add files but not modify existing ones)
- (WD) = **Write Data** (ability to create files)
- (OI) = **Object Inherit** (applies to files inside the folder)
- (CI) = **Container Inherit** (applies to subfolders)
- (I) = **Inherited** (this permission was inherited from a parent folder)
- (IO) = **Inherit Only** (applies only to child objects, not the folder itself)

Get-Acl "C:\Profiles" | Format-List

```
PS C:\Users\administrator.VLABS1> Get-Acl "C:\Profiles" | Format-List


Path   : Microsoft.PowerShell.Core\FileSystem::C:\Profiles
Owner  : BUILTIN\Administrators
Group  : VLABS1\Domain Users
Access : NT AUTHORITY\Authenticated Users Allow  Modify, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         BUILTIN\Users Allow  ReadAndExecute, Synchronize
         BUILTIN\Users Allow  AppendData
         BUILTIN\Users Allow  CreateFiles
         CREATOR OWNER Allow  268435456
Audit  :
Sddl   : O:BAG:DUD:AI(A;OICI;0x1301bf;;;AU)(A;OICI;FA;;;SY)(A;OICI;FA;;;BA)(A;OICIID;FA;;;SY)(A;OICIID;FA;;;BA)(A;OICIID;0x1200a9;;;BU)(A;CIID;LC;;;BU)(A;CIID;DC;;;BU)(A;OICIIOID;GA;;;CO)


PS C:\Users\administrator.VLABS1>
PS C:\Users\administrator.VLABS1>
```

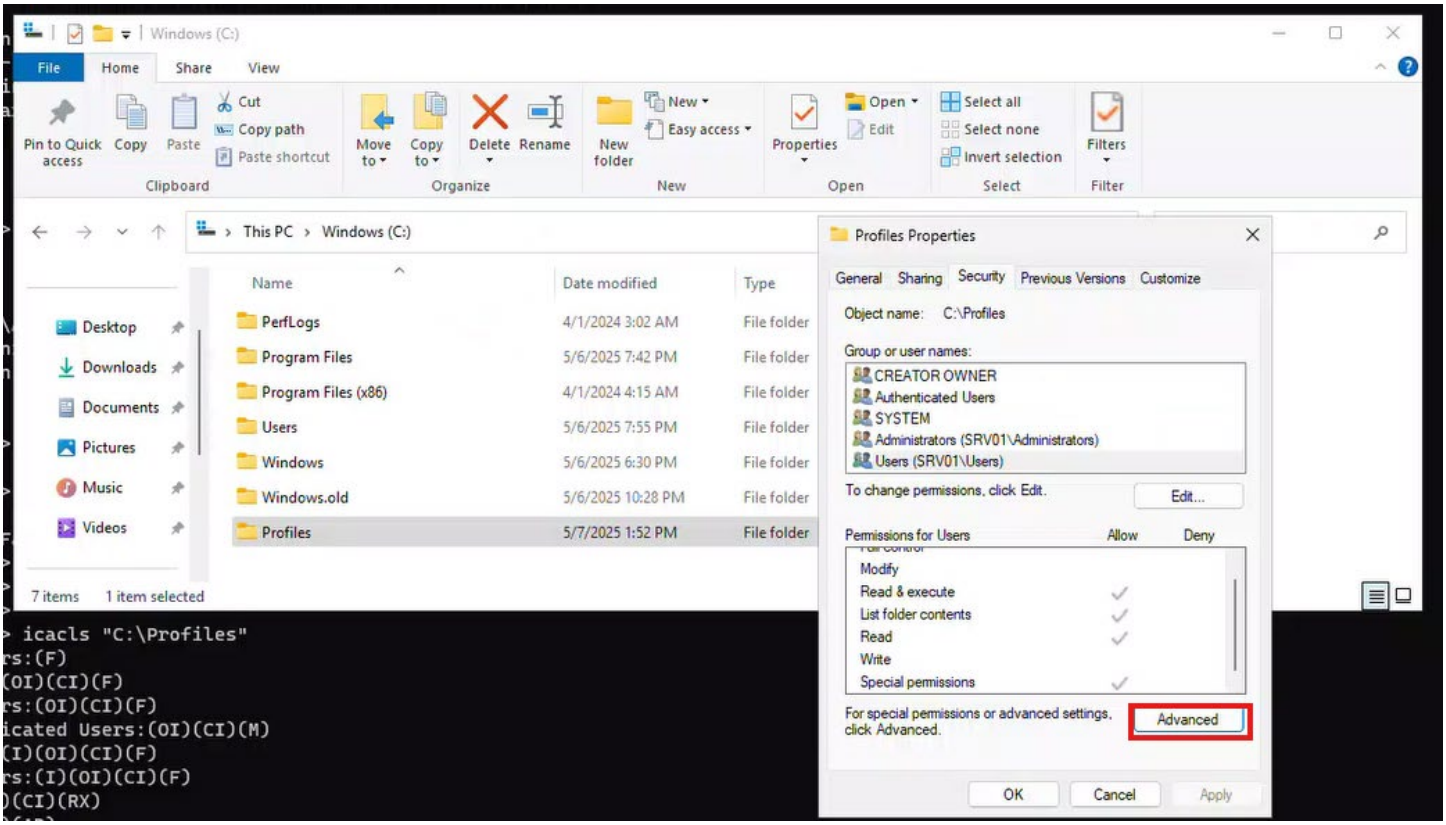
- **Owner**: BUILTIN\Administrators (who owns the folder).
- **Group**: VLABS1\Domain Users (the security group assigned to the folder).
- **Access Entries**:
  - Modify, Synchronize → **Authenticated Users**
  - FullControl → **SYSTEM & Administrators**
  - ReadAndExecute → **Domain Users**
  - AppendData → **Domain Users**

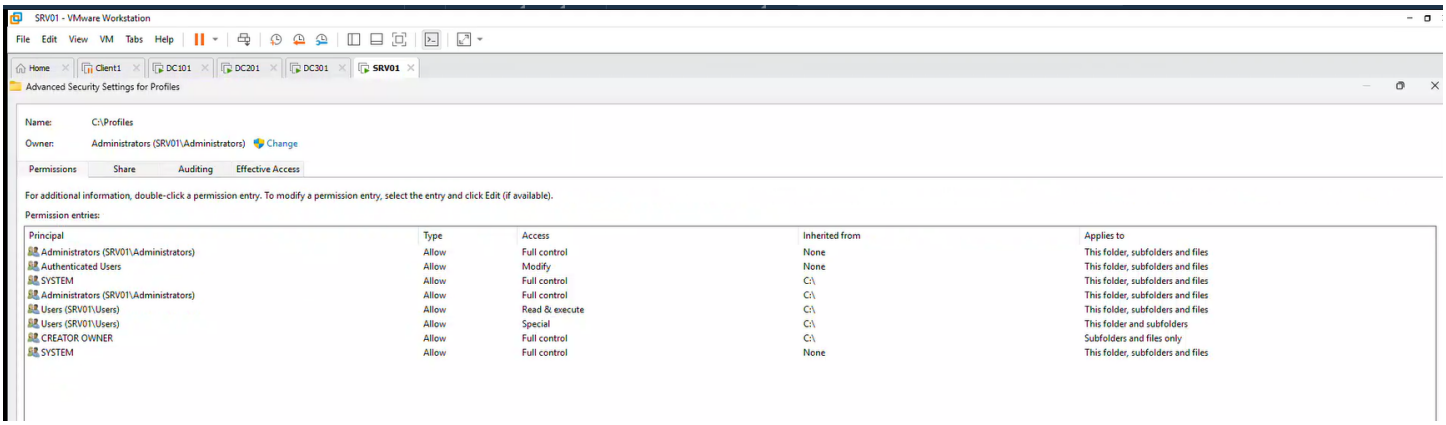
- CreateFiles → **Domain Users**
- 268435456 → **CREATOR OWNER** (Full Control in numeric form).

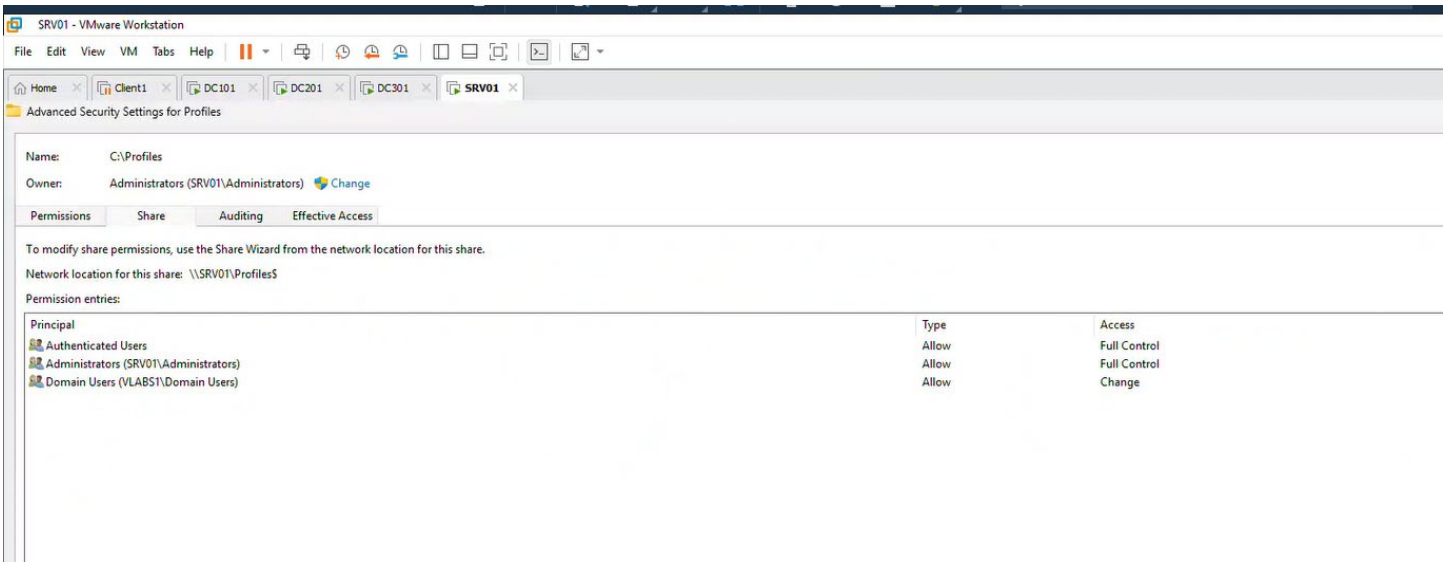
- **SDDL:** A security descriptor string (binary representation of permissions).

9.3.2.2 GUI

Right-click the folder → Properties -> Advanced -> Permissions / Share



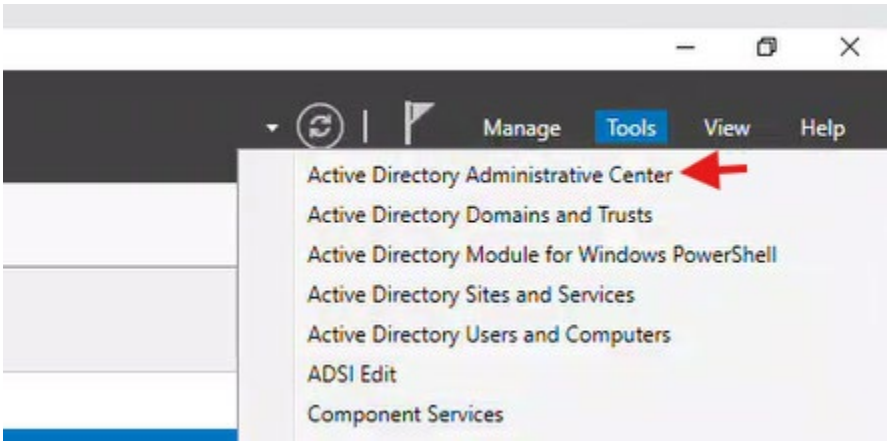




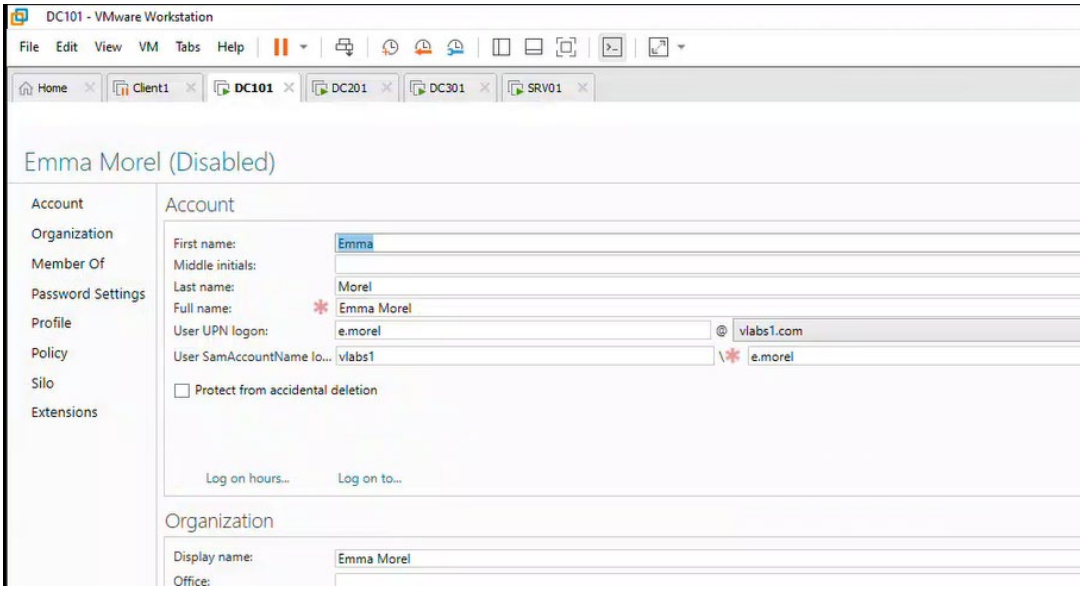
9.4 Assign a roaming profile path using the Active Directory Administrative Center.

9.4.1 Assign Roaming Profile for Emma Morel (AD Administrative Center)

1. Open ADAC



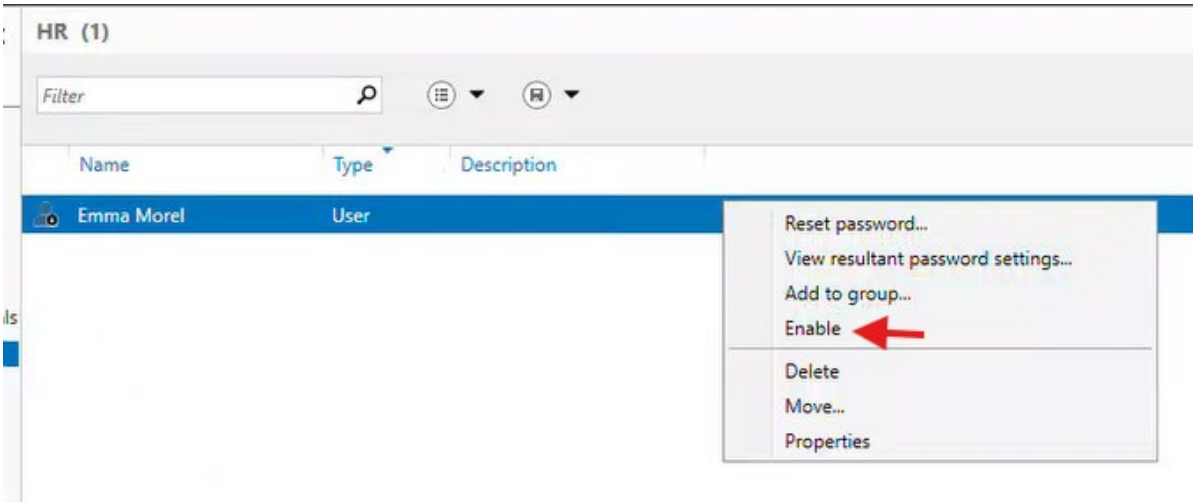
2. Navigate to HR OU (vlabs1.com → HR).
3. Right-click Emma Morel → Select Properties.



4. Set the Roaming Profile Path. Go to the Profile tab.
   Under Profile path, enter:

   \\SRV01\Profiles$\%username%

5. Click OK to save.
6. Since Emma Morel's account was disabled, enable it



7. Verify Account is Roaming profile

   Get-ADUser -Identity "e.morel" -Properties ProfilePath | Select-Object Name, ProfilePath

```
PS C:\Users\Administrator> Get-ADUser -Identity "e.morel" -Properties ProfilePath | Select-Object Name, ProfilePath

Name        ProfilePath
----        -----------
Emma Morel \\SRV01\Profiles$\%username%
```

9.5 Assign a roaming profile path for the user account **Lucas Bernard** using **PowerShell.**

1. Verify Lucas Bernard's SamAccountName

Since we need the exact username (SamAccountName), run:

Get-ADUser -Filter "Name -like 'Lucas*'" | Select-Object Name, SamAccountName

2. Assign the Roaming Profile Path

Use the confirmed SamAccountName to set the profile path:

Set-ADUser -Identity "l.bernard" -ProfilePath "\\SRV01\Profiles$\%username%"

3. Verify the Configuration

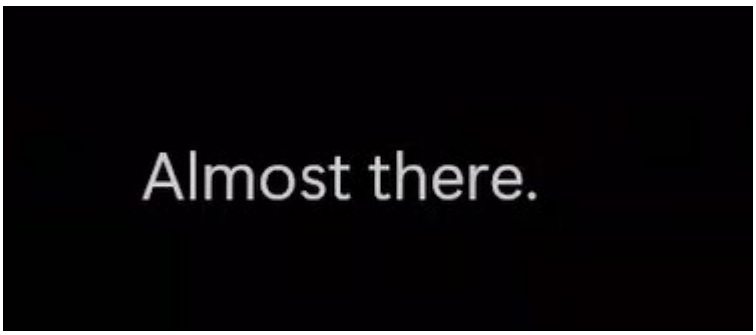
Check if the path was set correctly:

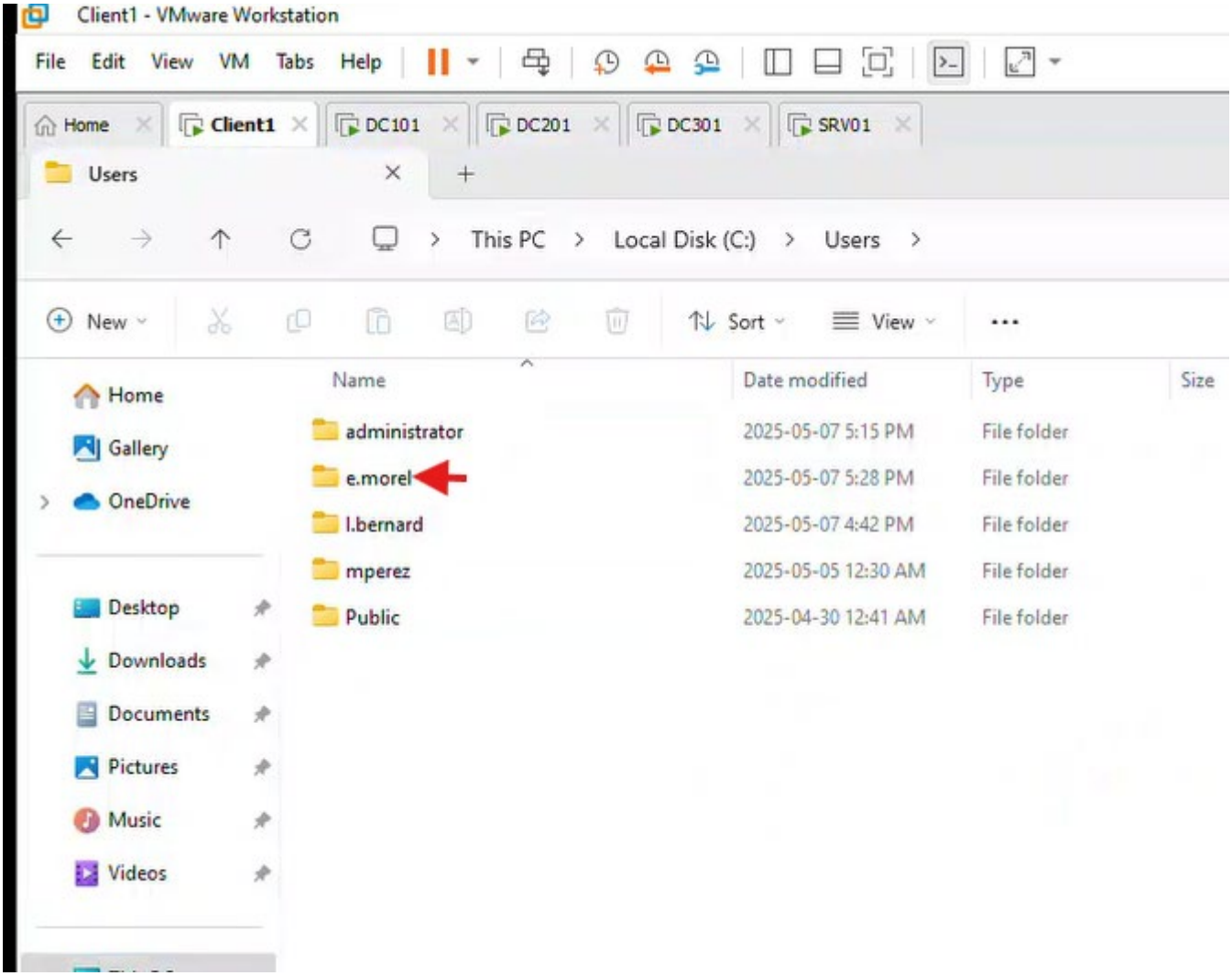
Get-ADUser -Identity "l.bernard" -Properties ProfilePath | Select-Object Name, ProfilePath

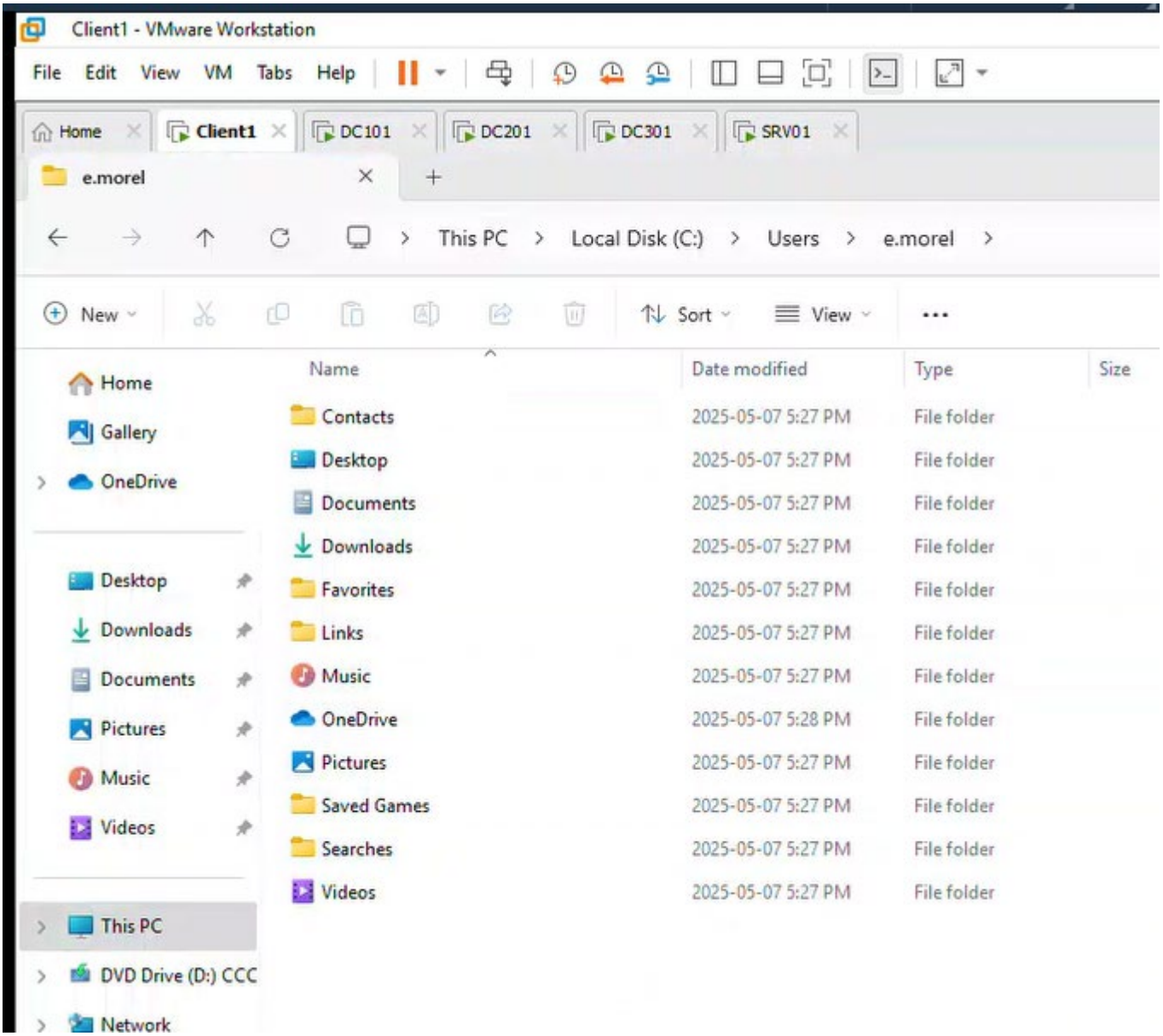
```
PS C:\Users\Administrator> Get-ADUser -Filter "Name -like 'Lucas*'" | Select-Object Name, SamAccountName

Name          SamAccountName
----          --------------
Lucas Bernard l.bernard


PS C:\Users\Administrator> Set-ADUser -Identity "l.bernard" -ProfilePath "\\SRV01\Profiles$\%username%"
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADUser -Identity "l.bernard" -Properties ProfilePath | Select-Object Name, ProfilePath

Name          ProfilePath
----          -----------
Lucas Bernard \\SRV01\Profiles$\%username%


PS C:\Users\Administrator>
```

9.6 Log in from **Client1** and verify the profile is stored in \\SRV01\Profiles$\%username%.

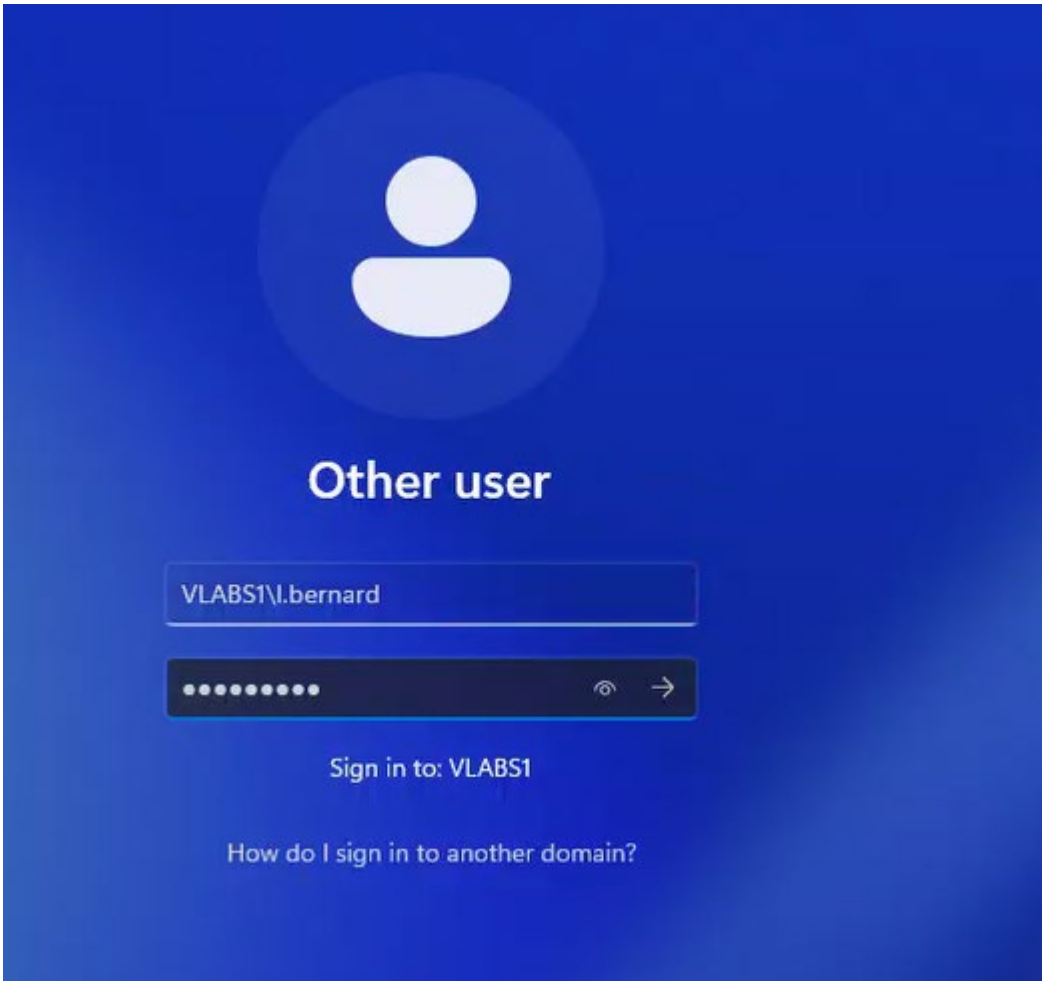
Emma



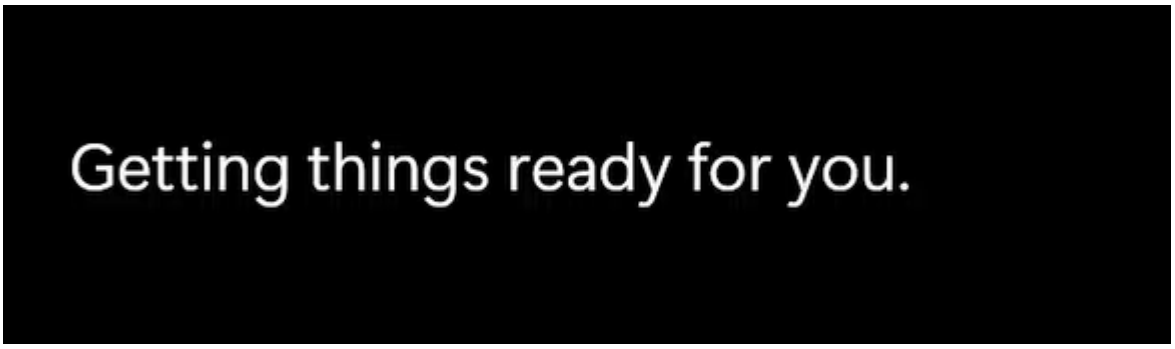

Client1 - VMware Workstation
File Edit View VM Tabs Help
Home
Client1
DC101
DC201
DC301
SRV01
Users
This PC
Local Disk (C:)
Users
New
Sort
View
Home
Gallery
OneDrive
Desktop
Downloads
Documents
Pictures
Music
Videos
Name
Date modified
Type
Size
administrator
2025-05-07 5:15 PM
File folder
e.morel
2025-05-07 5:28 PM
File folder
l.bernard
2025-05-07 4:42 PM
File folder
mperez
2025-05-05 12:30 AM
File folder
Public
2025-04-30 12:41 AM
File folder

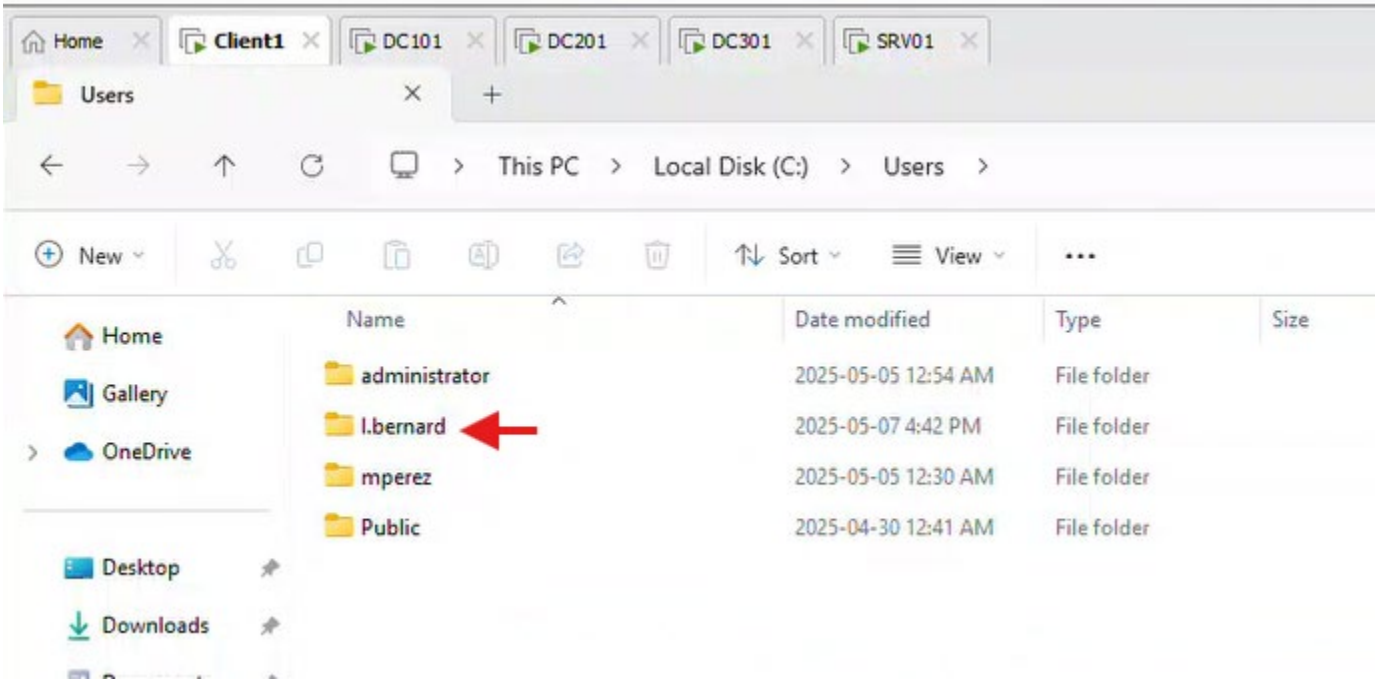

Client1 - VMware Workstation
File Edit View VM Tabs Help
Home Client1 DC101 DC201 DC301 SRV01
e.morel
This PC > Local Disk (C:) > Users > e.morel >
New Sort View
Home
Gallery
OneDrive
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
DVD Drive (D:) CCC
Network
Name Date modified Type Size
Contacts 2025-05-07 5:27 PM File folder
Desktop 2025-05-07 5:27 PM File folder
Documents 2025-05-07 5:27 PM File folder
Downloads 2025-05-07 5:27 PM File folder
Favorites 2025-05-07 5:27 PM File folder
Links 2025-05-07 5:27 PM File folder
Music 2025-05-07 5:27 PM File folder
OneDrive 2025-05-07 5:28 PM File folder
Pictures 2025-05-07 5:27 PM File folder
Saved Games 2025-05-07 5:27 PM File folder
Searches 2025-05-07 5:27 PM File folder
Videos 2025-05-07 5:27 PM File folder

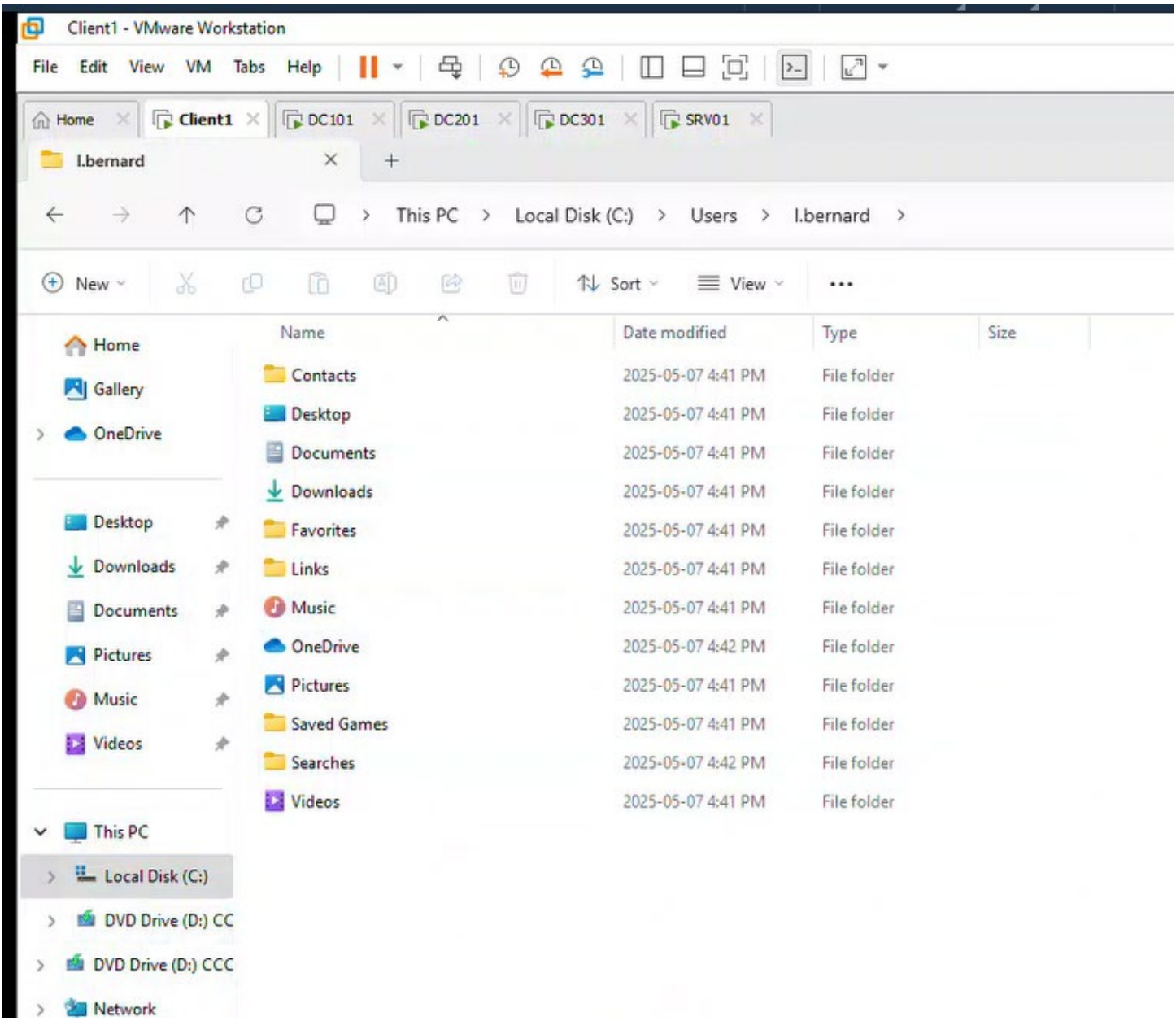
Lucas



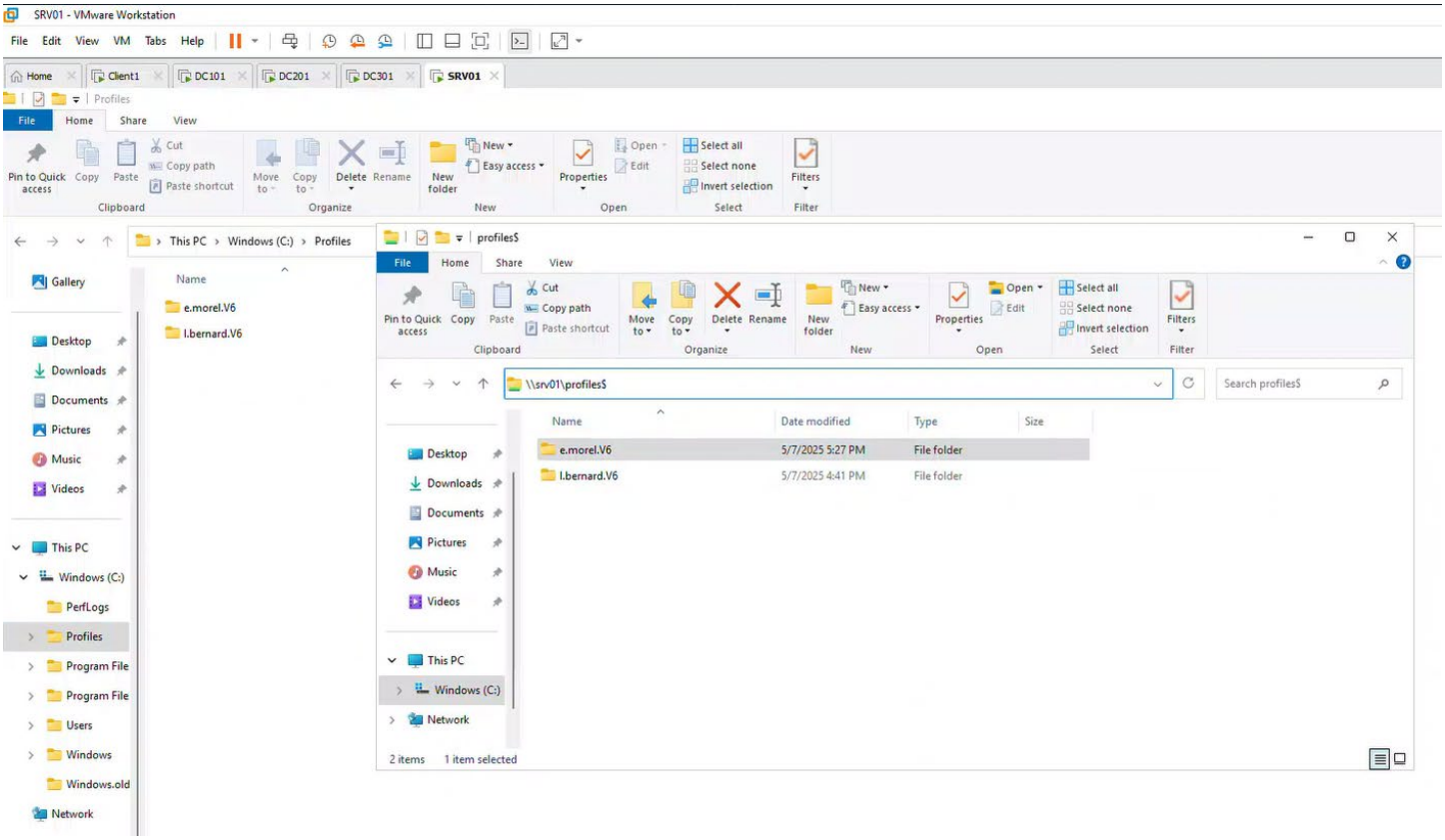
This will take time




Home
Client1
DC101
DC201
DC301
SRV01
Users
This PC
Local Disk (C:)
Users
New
Sort
View
Home
Gallery
OneDrive
Desktop
Downloads
Name
Date modified
Type
Size
administrator
2025-05-05 12:54 AM
File folder
l.bernard
2025-05-07 4:42 PM
File folder
mperez
2025-05-05 12:30 AM
File folder
Public
2025-04-30 12:41 AM
File folder



Verify profile is stored in \\SRV01\Profiles$\%username%.

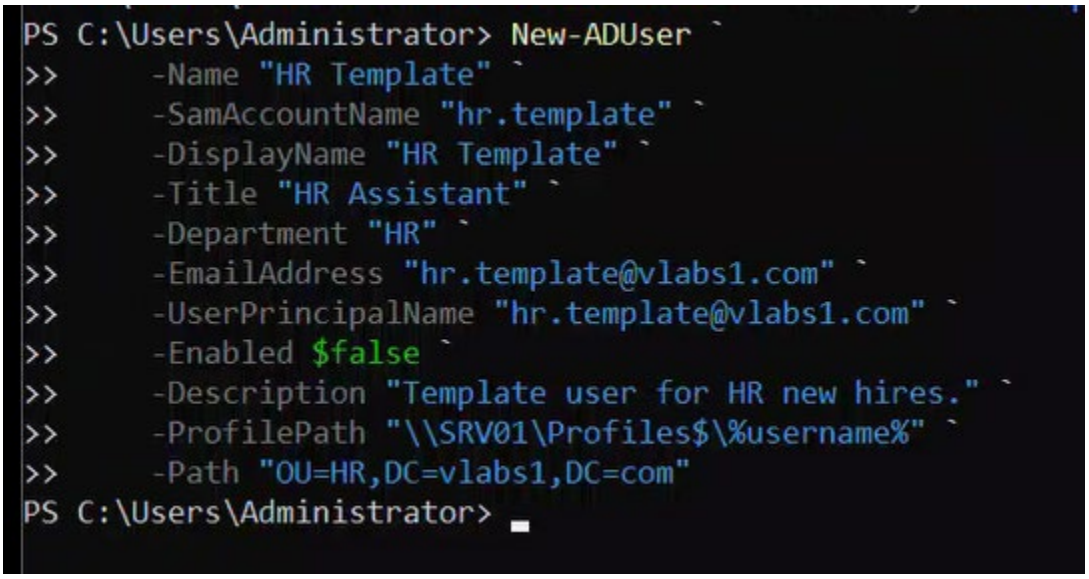

SRV01 - VMware Workstation
File Edit View VM Tabs Help
Home Client1 DC101 DC201 DC301 SRV01
Profiles
File Home Share View
Pin to Quick access Copy Paste Cut Copy path Paste shortcut
Clipboard
Move to Copy to Delete Rename
Organize
New folder New Easy access
New
Properties Open Edit
Open
Select all Select none Invert selection
Select
Filters
Filter
This PC › Windows (C:) › Profiles
Gallery
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
Windows (C:)
PerfLogs
Profiles
Program File
Program File
Users
Windows
Windows.old
Network
Name
e.morel.V6
l.bernard.V6
profiles$
File Home Share View
Pin to Quick access Copy Paste Cut Copy path Paste shortcut
Clipboard
Move to Copy to Delete Rename
Organize
New folder New Easy access
New
Properties Open Edit
Open
Select all Select none Invert selection
Select
Filters
Filter
\\srv01\profiles$
Search profiles$
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
Windows (C:)
Network
Name
Date modified
Type
Size
e.morel.V6
5/7/2025 5:27 PM
File folder
l.bernard.V6
5/7/2025 4:41 PM
File folder
2 items
1 item selected

10 Task 9: Create a Template User for HR

10.1 Create template

1. Create a template user for the **HR OU** with the following properties:
    - Full Name: **HR Template**
    - sAMAccountName: **hr.template**
    - Job Title: **HR Assistant**
    - Department: **HR**
    - Email: **hr.template@vlabs.com**
    - Account Status: **Disabled**
    - Description: **Template user for HR new hires.**
    - Profile: **\\SRVX\Profiles$\%username%**

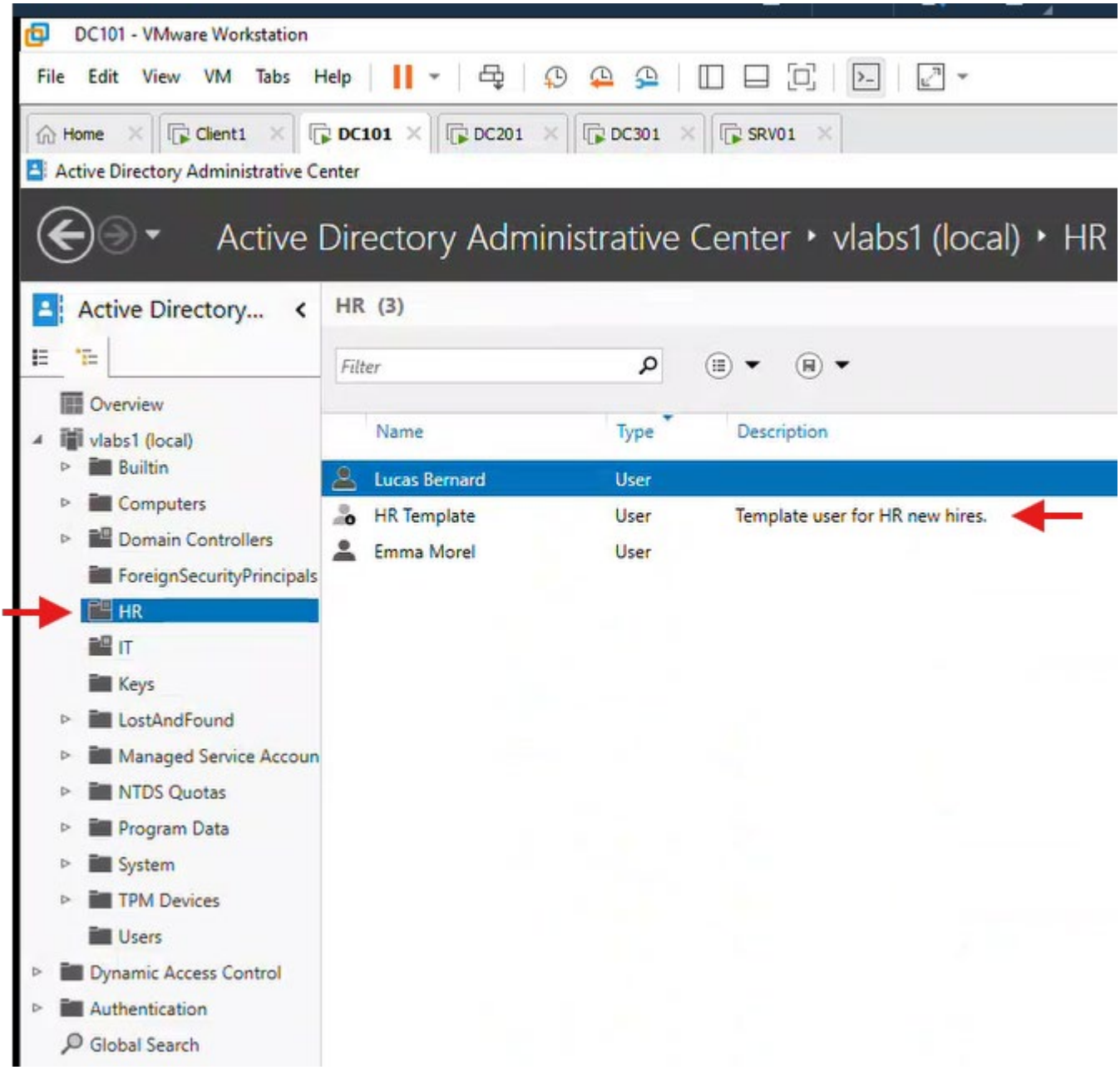
```
New-ADUser `
  -Name "HR Template" `
  -SamAccountName "hr.template" `
  -DisplayName "HR Template" `
  -Title "HR Assistant" `
  -Department "HR" `
  -EmailAddress "hr.template@vlabs1.com" `
  -UserPrincipalName "hr.template@vlabs1.com" `
  -Enabled $false `
  -Description "Template user for HR new hires." `
  -ProfilePath "\\SRV01\Profiles$\%username%" `
  -Path "OU=HR,DC=vlabs1,DC=com"
```

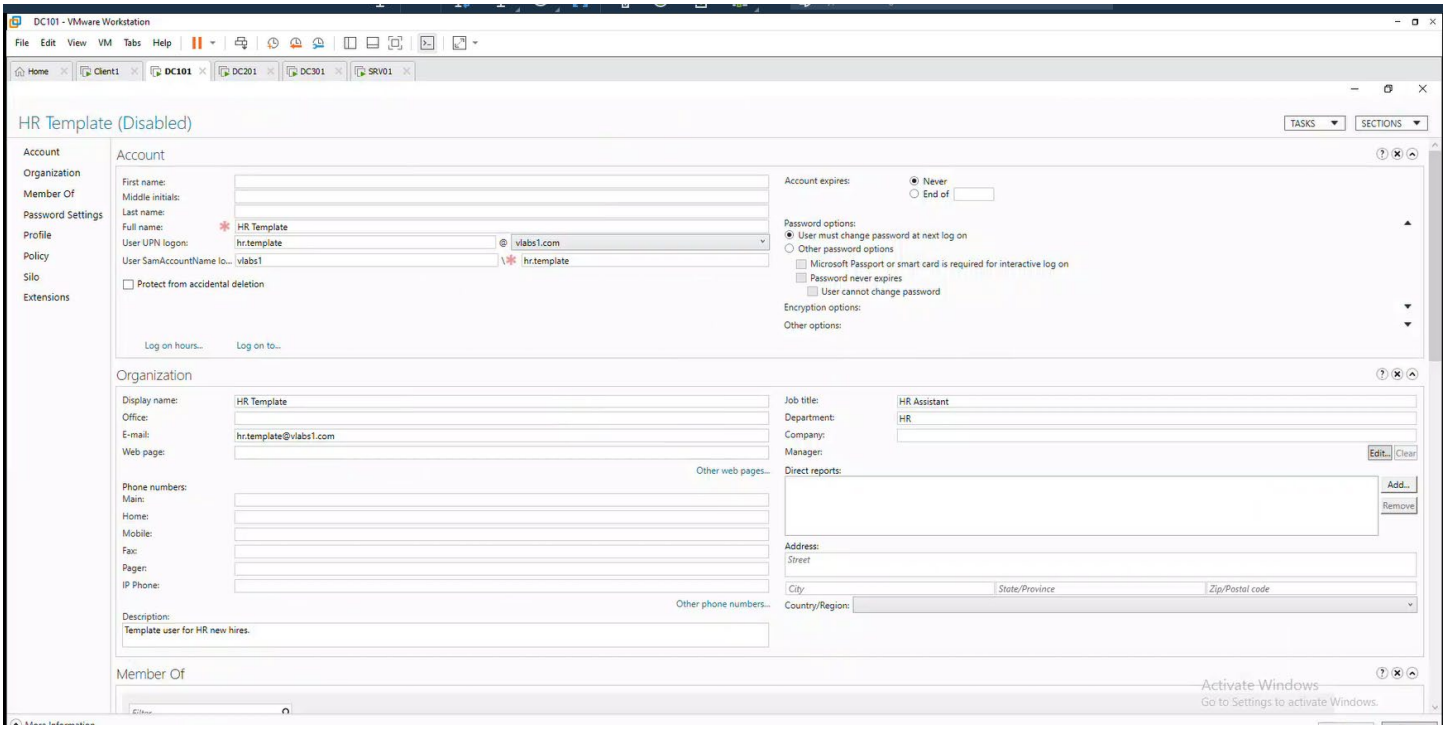


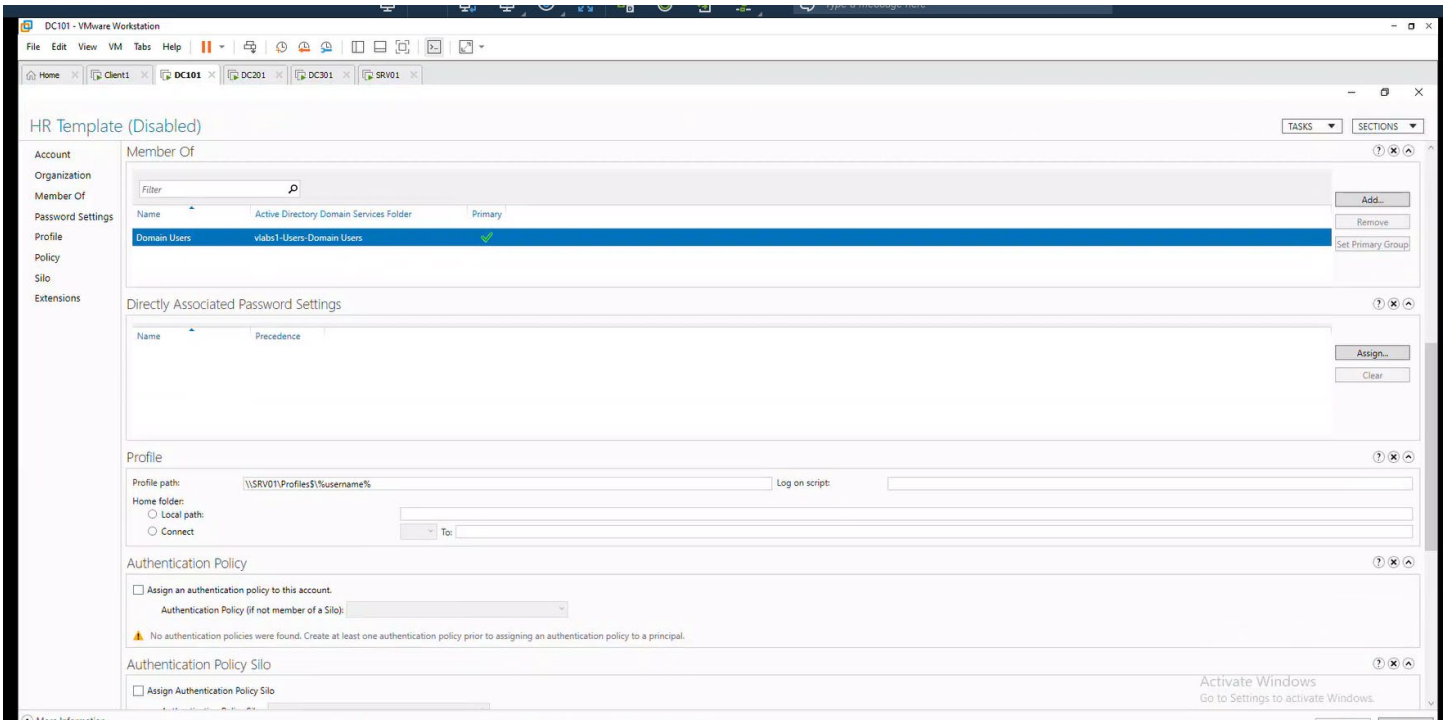
10.2 Verify Template

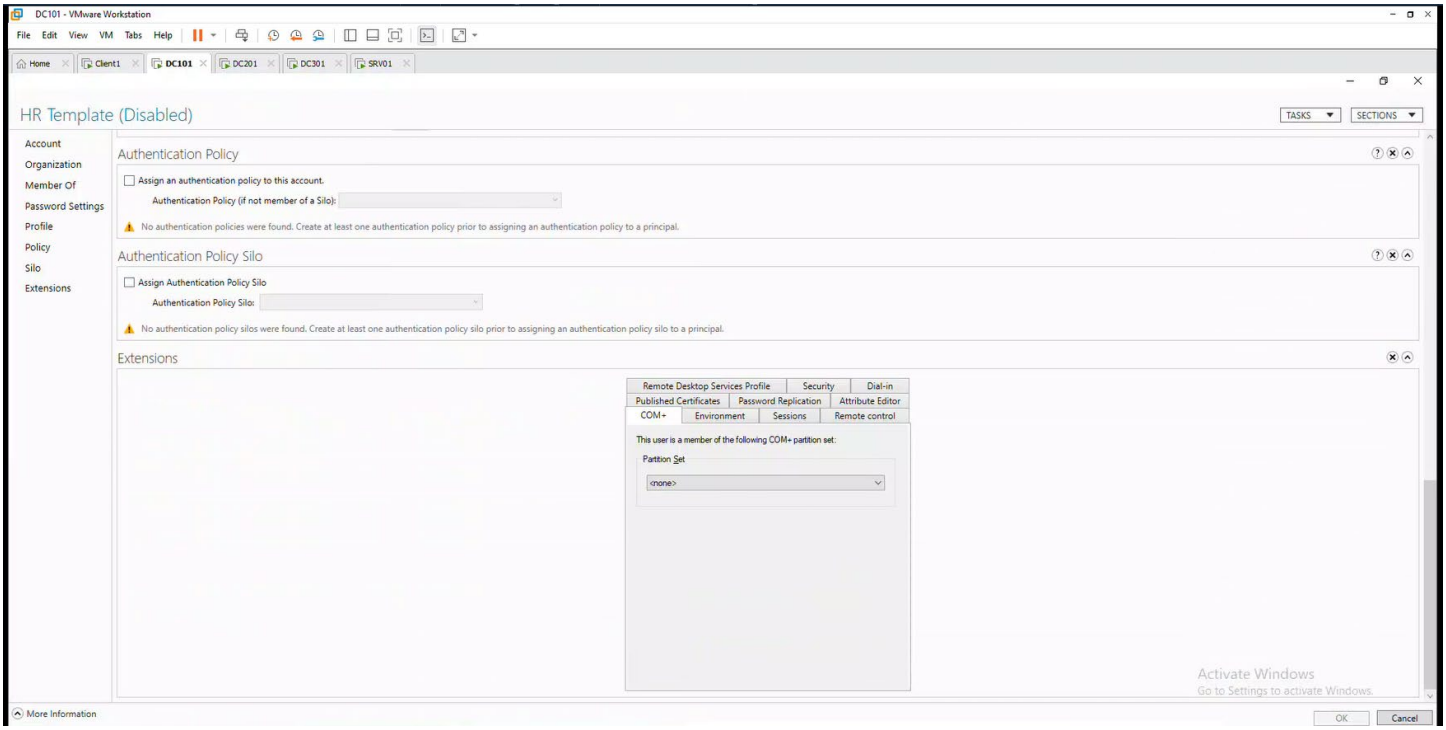
Get-ADUser -Identity "hr.template" -Properties * |
Select-Object Name,SamAccountName,Enabled,ProfilePath,EmailAddress,UserPrincipalName

```
PS C:\Users\Administrator> Get-ADUser -Identity "hr.template" -Properties * |
>>     Select-Object Name,SamAccountName,Enabled,ProfilePath,EmailAddress,UserPrincipalName


Name              : HR Template
SamAccountName    : hr.template
Enabled           : False
ProfilePath       : \\SRV01\Profiles$\%username%
EmailAddress      : hr.template@vlabs1.com
UserPrincipalName : hr.template@vlabs1.com



PS C:\Users\Administrator>
```


DC101 - VMware Workstation
File Edit View VM Tabs Help
Home
Client1
DC101
DC201
DC301
SRV01
Active Directory Administrative Center
Active Directory Administrative Center ‣ vlabs1 (local) ‣ HR
Active Directory...
Overview
vlabs1 (local)
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
HR
IT
Keys
LostAndFound
Managed Service Accoun
NTDS Quotas
Program Data
System
TPM Devices
Users
Dynamic Access Control
Authentication
Global Search
HR (3)
Filter
Name
Type
Description
Lucas Bernard
User
HR Template
User
Template user for HR new hires.
Emma Morel
User


DC101 - VMware Workstation
File Edit View VM Tabs Help
Home Client1 DC101 DC201 DC301 SRV01
HR Template (Disabled)
TASKS SECTIONS
Account
Organization
Member Of
Password Settings
Profile
Policy
Silo
Extensions
Account
First name:
Middle initials:
Last name:
Full name: HR Template
User UPN logon: hr.template @ vlabs1.com
User SamAccountName lo... vlabs1 \ hr.template
Protect from accidental deletion
Account expires: Never End of
Password options:
User must change password at next log on
Other password options
Microsoft Passport or smart card is required for interactive log on
Password never expires
User cannot change password
Encryption options:
Other options:
Log on hours... Log on to...
Organization
Display name: HR Template
Office:
E-mail: hr.template@vlabs1.com
Web page:
Other web pages...
Phone numbers:
Main:
Home:
Mobile:
Fax:
Pager:
IP Phone:
Other phone numbers...
Description: Template user for HR new hires.
Job title: HR Assistant
Department: HR
Company:
Manager:
Edit... Clear
Direct reports:
Add... Remove
Address:
Street
City State/Province Zip/Postal code
Country/Region:
Member Of
Activate Windows
Go to Settings to activate Windows.


DC101 - VMware Workstation
File Edit View VM Tabs Help
Home Client1 DC101 DC201 DC301 SRV01
HR Template (Disabled)
TASKS SECTIONS
Account
Organization
Member Of
Password Settings
Profile
Policy
Silo
Extensions
Member Of
Filter
Name Active Directory Domain Services Folder Primary
Domain Users vlabs1-Users-Domain Users
Add... Remove Set Primary Group
Directly Associated Password Settings
Name Precedence
Assign... Clear
Profile
Profile path: \\SRV01\Profiles$\%username%
Log on script:
Home folder:
Local path:
Connect To:
Authentication Policy
Assign an authentication policy to this account.
Authentication Policy (if not member of a Silo):
No authentication policies were found. Create at least one authentication policy prior to assigning an authentication policy to a principal.
Authentication Policy Silo
Assign Authentication Policy Silo
Activate Windows
Go to Settings to activate Windows.


DC101 - VMware Workstation
File Edit View VM Tabs Help
Home Client1 DC101 DC201 DC301 SRV01
HR Template (Disabled)
TASKS SECTIONS
Account
Organization
Member Of
Password Settings
Profile
Policy
Silo
Extensions
Authentication Policy
Assign an authentication policy to this account.
Authentication Policy (if not member of a Silo):
No authentication policies were found. Create at least one authentication policy prior to assigning an authentication policy to a principal.
Authentication Policy Silo
Assign Authentication Policy Silo
Authentication Policy Silo:
No authentication policy silos were found. Create at least one authentication policy silo prior to assigning an authentication policy silo to a principal.
Extensions
Remote Desktop Services Profile
Security
Dial-in
Published Certificates
Password Replication
Attribute Editor
COM+
Environment
Sessions
Remote control
This user is a member of the following COM+ partition set:
Partition Set
<none>
Activate Windows
Go to Settings to activate Windows.
More Information
OK
Cancel

11 Task 10: Verify New Users from DC201 (RODC Core Server)

Requirements:

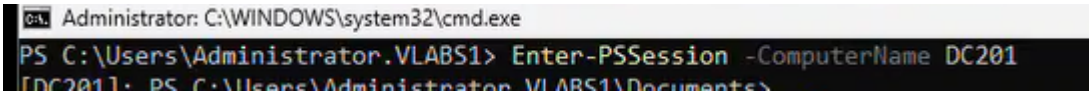
1. Use **PowerShell** on **DC201** to verify the newly created users exist and are replicated correctly in the **RODC**.
2. Ensure the users from **HR and IT OUs** are visible.
3. Confirm that disabled or deleted users are reflected on DC201.

To verify that users are properly replicated to your Read-Only Domain Controller (DC201), follow these steps:

11.1 Connect to DC201 and Verify Users

First, establish a PowerShell session with DC201:

Enter-PSSession -ComputerName DC201

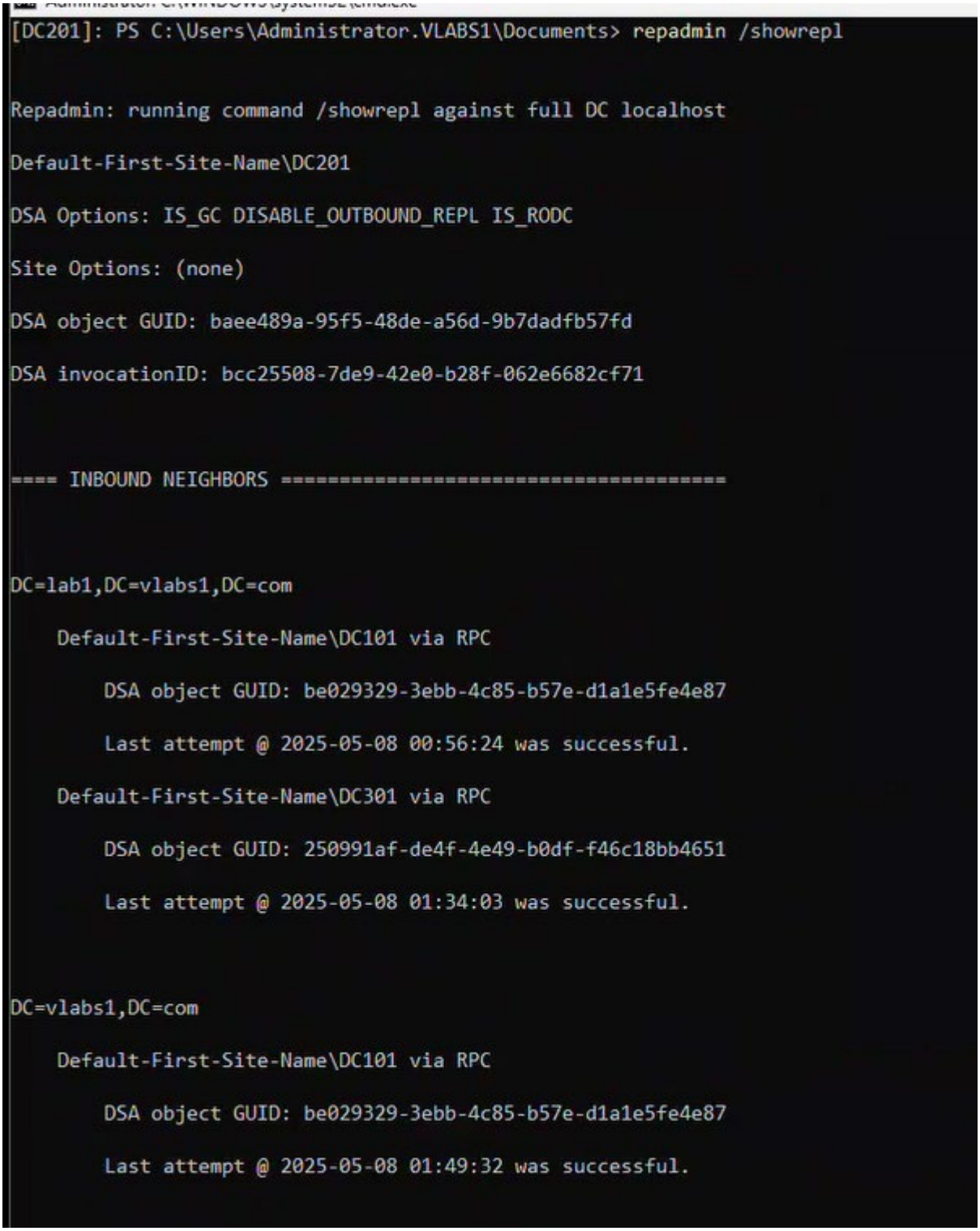


11.2 Check Replication Status

Verify that replication is working properly:

repadmin /showrepl

Note - Not all printout is shown



repadmin /replsummary

```
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> repadmin /replsummary
Replication Summary Start Time: 2025-05-08 01:49:50


Beginning data collection for replication summary, this may take awhile:

  ......



Source DSA          largest delta    fails/total %%   error

 DC101                      53m:26s    0 /   6    0

 DC301                      53m:26s    0 /   4    0



Destination DSA     largest delta    fails/total %%   error

 DC201                      53m:26s    0 /  10    0



Experienced the following operational errors trying to retrieve replication information:

         110 - DC101.vlabs1.com

         110 - DC301.lab1.vlabs1.com
```

11.3 Verify HR and IT Users Exist

For HR Users:

Get-ADUser -Filter * -SearchBase "OU=HR,DC=vlabs1,DC=com" -Server DC201 | Select-Object Name,SamAccountName,Enabled,DistinguishedName

```
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> Get-ADUser -Filter * -SearchBase "OU=HR,DC=vlabs1,DC=com" -Server DC201 | Select-Object Name,SamAccountName,Enabled,DistinguishedName

Name          SamAccountName Enabled DistinguishedName
----          -------------- ------- -----------------
Emma Morel    e.morel           True CN=Emma Morel,OU=HR,DC=vlabs1,DC=com
Lucas Bernard l.bernard         True CN=Lucas Bernard,OU=HR,DC=vlabs1,DC=com
HR Template   hr.template      False CN=HR Template,OU=HR,DC=vlabs1,DC=com
```

For IT Users:

Get-ADUser -Filter * -SearchBase "OU=IT,DC=vlabs1,DC=com" -Server DC201 | Select-Object Name,SamAccountName,Enabled,DistinguishedName

```
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> Get-ADUser -Filter * -SearchBase "OU=IT,DC=vlabs1,DC=com" -Server DC201 | Select-Object Name,SamAccountName,Enabled,DistinguishedName

Name           SamAccountName Enabled DistinguishedName
----           -------------- ------- -----------------
Sophie Lambert s.lambert         True CN=Sophie Lambert,OU=IT,DC=vlabs1,DC=com
Chloe Girard   c.girard          True CN=Chloe Girard,OU=IT,DC=vlabs1,DC=com
```

11.4 Verify Specific Template User

Check the HR template user specifically:

Get-ADUser -Identity "hr.template" -Server DC201 -Properties * | Select-Object Name,SamAccountName,Enabled,ProfilePath,WhenCreated

```
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> Get-ADUser -Identity "hr.template" -Server DC201 -Properties * | Select-Object Name,SamAccountName,Enabled,ProfilePath,WhenCreated


Name           : HR Template
SamAccountName : hr.template
Enabled        : False
ProfilePath    : \\SRV01\Profiles$\%username%
WhenCreated    : 5/8/2025 1:36:59 AM
```

11.5 Verify Disabled/Deleted Users

11.5.1 Check Disabled Users

Get-ADUser -Filter {Enabled -eq $false} -Server DC201 | Select-Object Name,SamAccountName,DistinguishedName

```
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> Get-ADUser -Filter {Enabled -eq $false} -Server DC201 | Select-Object Name,SamAccountName,DistinguishedName

Name         SamAccountName DistinguishedName
----         -------------- -----------------
Guest        Guest          CN=Guest,CN=Users,DC=vlabs1,DC=com
krbtgt       krbtgt         CN=krbtgt,CN=Users,DC=vlabs1,DC=com
krbtgt_24591 krbtgt_24591   CN=krbtgt_24591,CN=Users,DC=vlabs1,DC=com
HR Template  hr.template    CN=HR Template,OU=HR,DC=vlabs1,DC=com
```

11.5.2 Verify Deleted Users

Get-ADObject -Filter {isDeleted -eq $true} -IncludeDeletedObjects -Server DC201 | Select-Object Name,ObjectClass,Deleted

```
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> Get-ADObject -Filter {isDeleted -eq $true} -IncludeDeletedObjects -Server DC201 | Select-Object Name,ObjectClass,Deleted

Name                                                                ObjectClass Deleted
----                                                                ----------- -------
Deleted Objects                                                     container   True
gc...                                                               dnsNode     True
..Deleted-_msdcs.vlabs1.com...                                      dnsZone     True
be029329-3ebb-4c85-b57e-d1a1e5fe4e87...                             dnsNode     True
_ldap._tcp.pdc...                                                   dnsNode     True
_ldap._tcp.gc...                                                    dnsNode     True
_ldap._tcp.Default-First-Site-Name._sites.gc...                     dnsNode     True
_ldap._tcp.Default-First-Site-Name._sites.dc...                     dnsNode     True
_ldap._tcp.dc...                                                    dnsNode     True
_ldap._tcp.402b24e7-c605-4172-bb2c-f1356eab96a2.domains...          dnsNode     True
_kerberos._tcp.Default-First-Site-Name._sites.dc...                 dnsNode     True
_kerberos._tcp.dc...                                                dnsNode     True
@...                                                                dnsNode     True
ForestDnsZones...                                                   dnsNode     True
..Deleted-vlabs1.com...                                             dnsZone     True
DomainDnsZones...                                                   dnsNode     True
dc101...                                                            dnsNode     True
_msdcs...                                                           dnsNode     True
_ldap._tcp.ForestDnsZones...                                        dnsNode     True
_ldap._tcp.DomainDnsZones...                                        dnsNode     True
_ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones...         dnsNode     True
_ldap._tcp.Default-First-Site-Name._sites...                        dnsNode     True
_ldap._tcp...                                                       dnsNode     True
_kpasswd._udp...                                                    dnsNode     True
_kpasswd._tcp...                                                    dnsNode     True
_kerberos._udp...                                                   dnsNode     True
_kerberos._tcp.Default-First-Site-Name._sites...                    dnsNode     True
_kerberos._tcp...                                                   dnsNode     True
_gc._tcp.Default-First-Site-Name._sites...                          dnsNode     True
_gc._tcp...                                                         dnsNode     True
@...                                                                dnsNode     True
Liam Dupont...                                                      user        True
Thomas Aviles...                                                    user        True
HR Template...                                                      user        True
```