This lab will guide you through configuring and managing Active Directory (AD) domains, forests, and trusts. You will set up a multi-forest environment, configure DNS for communication, and establish trust relationships.

Lab Assignment 1 (Part I) - Managing AD Domains, Forests, and Trusts

420-636-AB-Network Installation and Administration II

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

Table of Contents

1 Lab Assignment Preparation

1.1 Task 1: Import Cisco Router VM

1. Download the **Cisco-Router.ova** file using the following link: **Cisco Router VM**
2. Import the **Cisco-Router** using the **Cisco-Router.ova** file**.**
3. **Before starting the router**, open the **VM settings** and make sure that:
   - **Network Adapter ➔ Bridged**
   - **Network Adapter 2 ➔ LAN1**
   - **Network Adapter 3 ➔ LAN2**
   - **Network Adapter 4 ➔ LAN3**
4. Start the **Cisco-Router** VM**.** Click **inside the VM** and **press any key** to continue. It will **take a couple of minutes to boot**. Just wait.

```
GRUB Loading stage2..
Press any key to continue.
```

5. Wait until it starts, type **show ip int br** to verify the IP address of the 4 NICs.

```
Cisco-Router#sh ip int br
Interface              IP-Address      OK? Method Status
GigabitEthernet1       192.168.25.50   YES manual up
GigabitEthernet2       192.168.35.50   YES manual up
GigabitEthernet3       192.168.45.50   YES manual up
GigabitEthernet0       192.168.2.184   YES DHCP   up
```

6. Verify the following:
   - **GigabitEthernet1** has an address **192.168.1.50 ➔ To Modify**
   - **GigabitEthernet2** has an address **192.168.35.50 ➔ Keep it as it is.**
   - **GigabitEthernet3** has an address **192.168.45.50 ➔ Keep it as it is.**
   - **GigabitEthernet 0** has a **Bridged** address **➔ Keep it as it is.**
7. You need to modify this IP address of **GigabitEthernet1** and use **192.168.*1*.50/24 (where 1 is your remote PC number).**

```
Cisco-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Cisco-Router(config)#int g1
Cisco-Router(config-if)#ip address 192.168.25.50 255.255.255.0
Cisco-Router(config-if)#end
Cisco-Router#wr
```

1.2 Task 2: Servers Configuration

1. Remove the card **NAT** from **Client1** ***(if it exists),*** just keep the **Lan Segment LAN1.**
2. Add the following Gateway IP on **DC101, DC201, DC301** and **Client1**:
   - Gateway: **192.168.1.50**

Note: Use this command to add the **Gateway** on **DC201:**

netsh interface ipv4 set address name="Ethernet0" static 192.168.1.2 255.255.255.0 192.168.1.50

3. **SRV01: *Windows* Server 2025 Core Desktop**
   - First, rename **SRV*01*** to **DC4*01*** and restart the VM.
   - Modify the **Network Adapter → LAN2**
   - Set IP **192.168.35.1/24**
   - Set **Primary DNS: 192.168.35.1**
   - Set **Gateway: 192.168.35.50**
   - Enable **ping** using the following command:

     netsh advfirewall firewall add rule name="Allow ICMPv4-In" protocol=icmpv4:8,any dir=in action=allow

4. **Test network connectivity**
   - Verify the **ping** between **DC101, DC201, DC301, DC401,** and **Client1**

2 Lab Assignment 1 (Part I) - Managing AD Domains, Forests, and Trusts

2.1 Lab Overview

This lab will guide you through **configuring and managing Active Directory (AD) domains, forests, and trusts**. You will set up a **multi-forest environment**, configure DNS for communication, and establish trust relationships.

2.2 Topology

2.3 Lab Requirements

- **DC101 (Windows Server 2022)**: PDC for vlabsXX.com
- **DC201 (Windows Server 2025):** RODC Core for vlabsXX.com.
- **DC301 (Windows Server 2022):** Child DC for lab.vlabsXX.com.
- **DC401 (Windows Server 2025)**: New DC for partnerXX.com.
- **Client1 (Windows 11):** Domain-joined to vlabsXX.com.
- **Cisco-Router (CSR1000V)**: For routing between forests

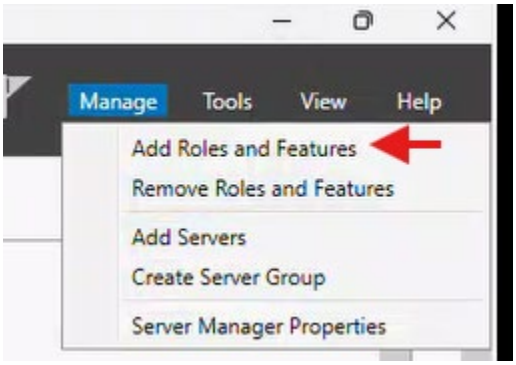
2.4 Lab Tasks

2.4.1 Task 1: Promote DC401 as a New Domain Controller in a New Forest

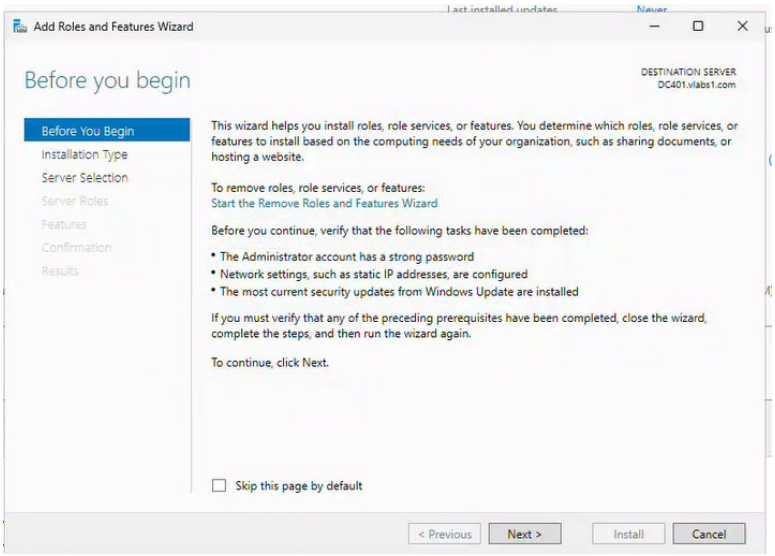
2.4.1.1 Promote DC401 as a new DC in a New Forest named partner1.com using GUI

2.4.1.1.1 Install AD DS role on **DC401**

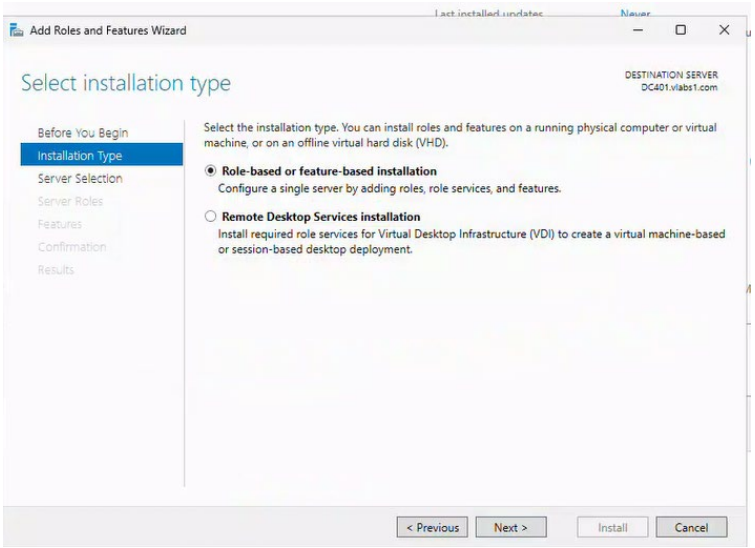
1. **Log in** to DC401 with administrative credentials
2. **Open Server Manager**
3. Click **"Add roles and features"** from the Dashboard or the Manage menu



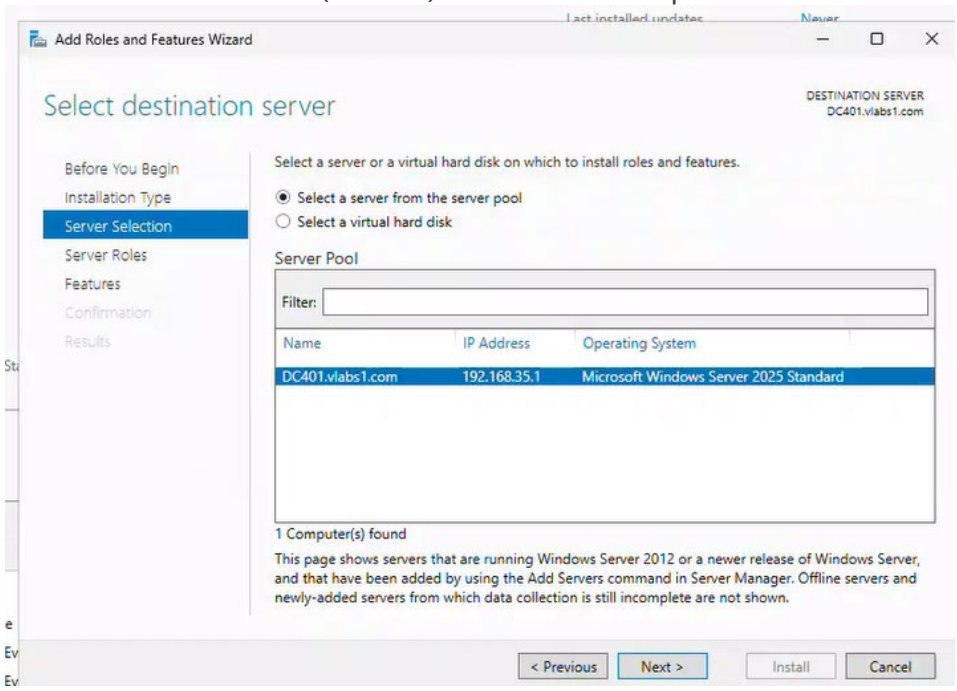
4. In the **Before You Begin** page, click **Next**



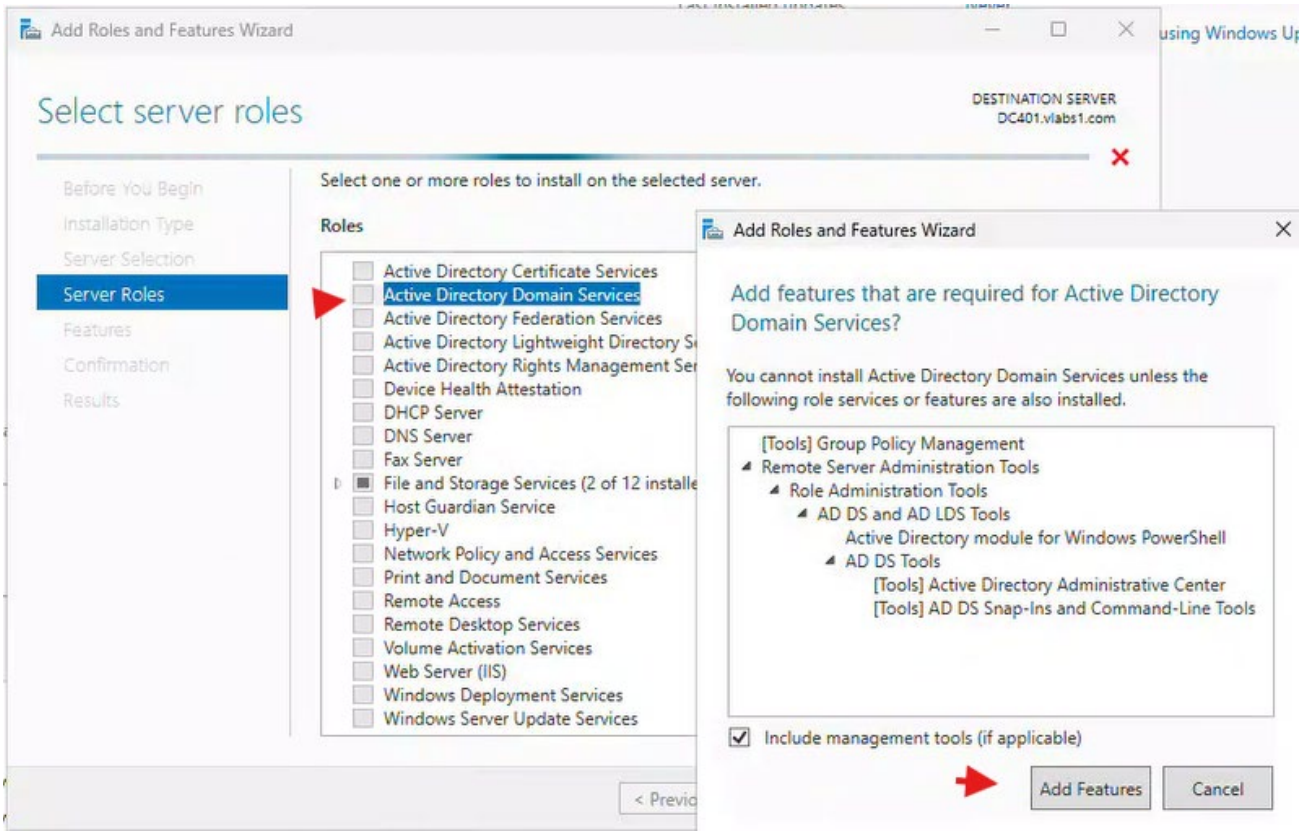
5. Select **"Role-based or feature-based installation"** and click **Next**



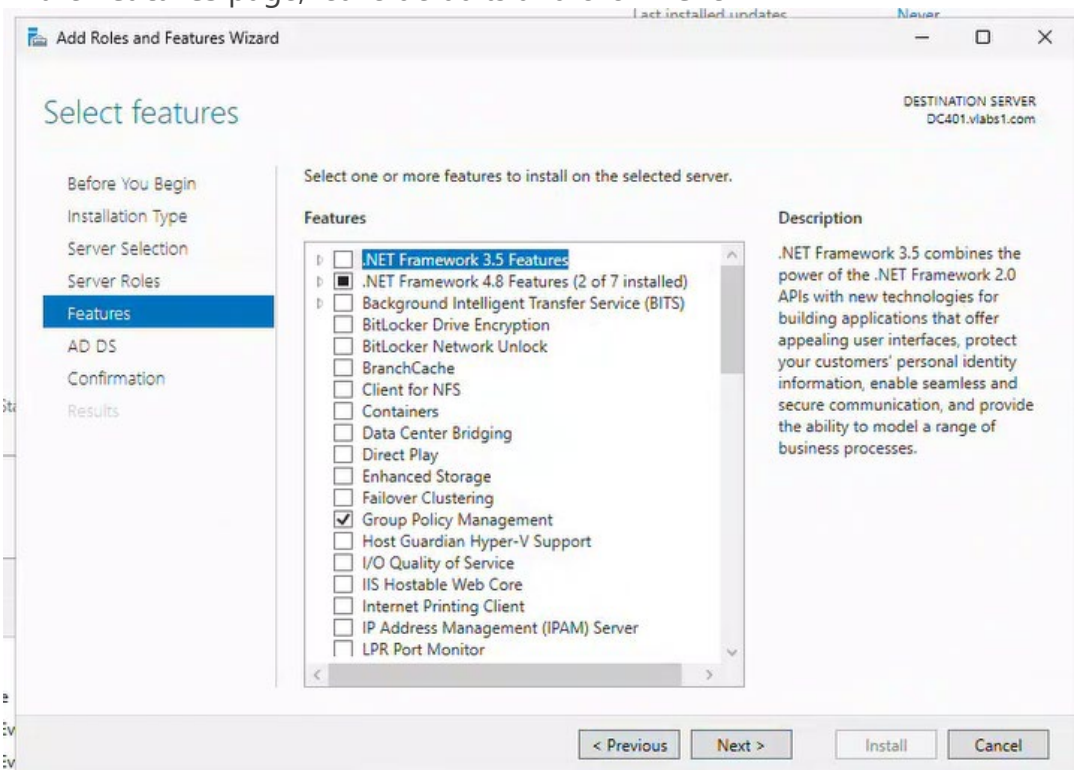
6. Select the local server (**DC401**) from the server pool and click **Next**



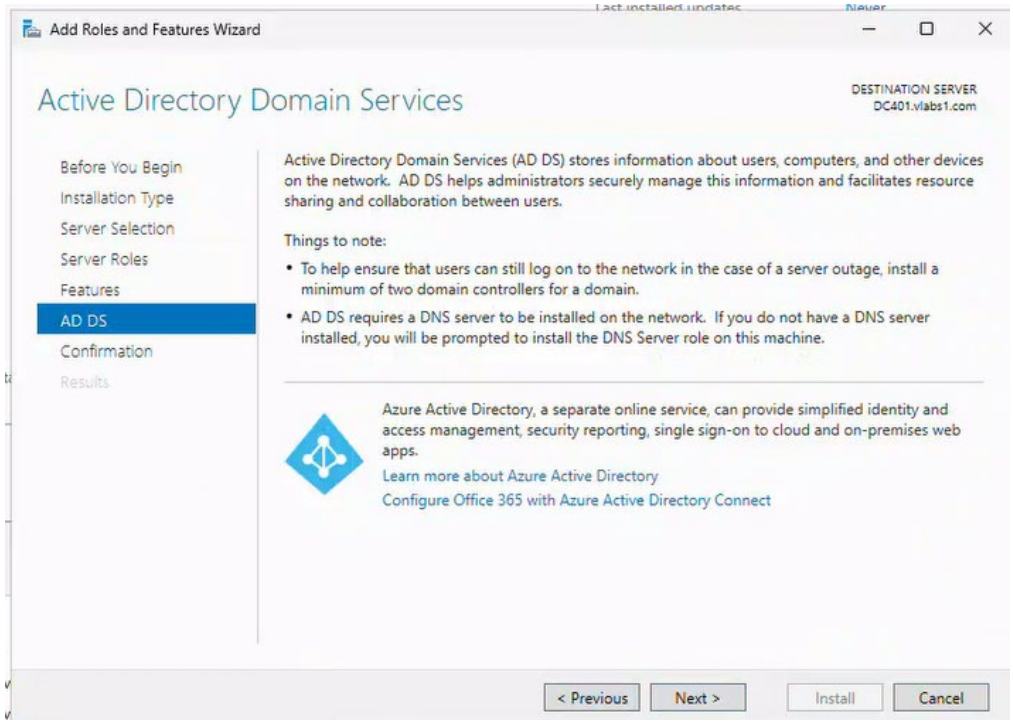
7. In the **Server Roles** page:
    - Check **"Active Directory Domain Services"**
    - A pop-up will appear asking to add required features - click **"Add Features"**
    - Click **Next**



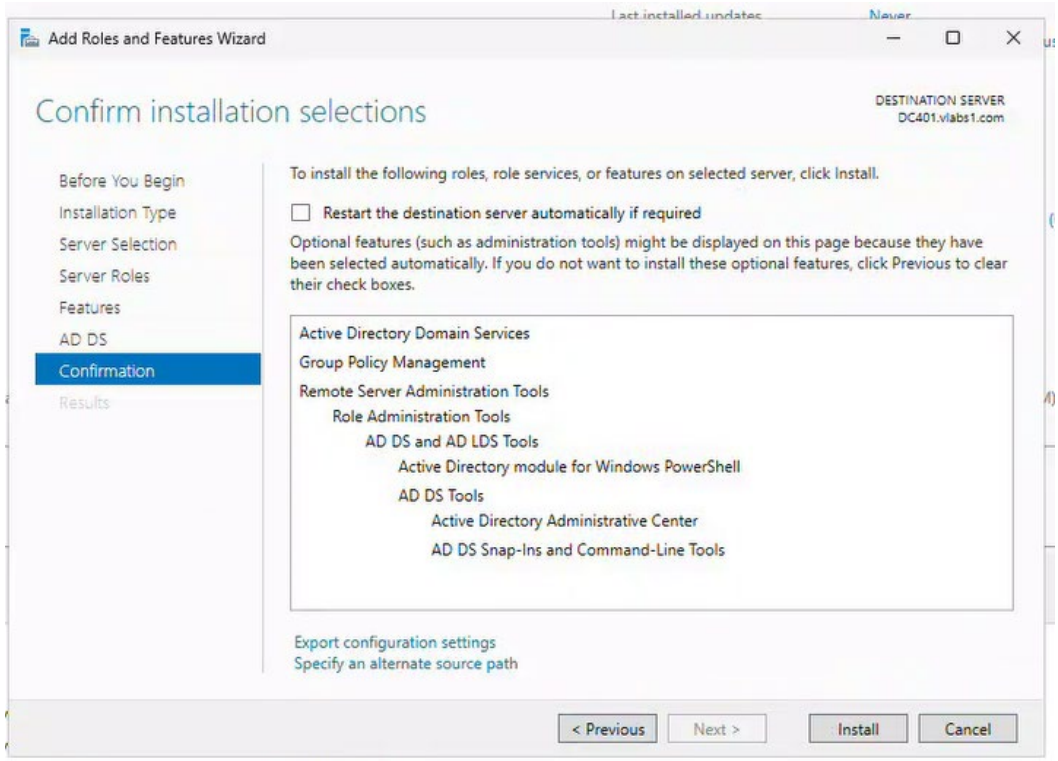
8. In the **Features** page, leave defaults and click **Next**



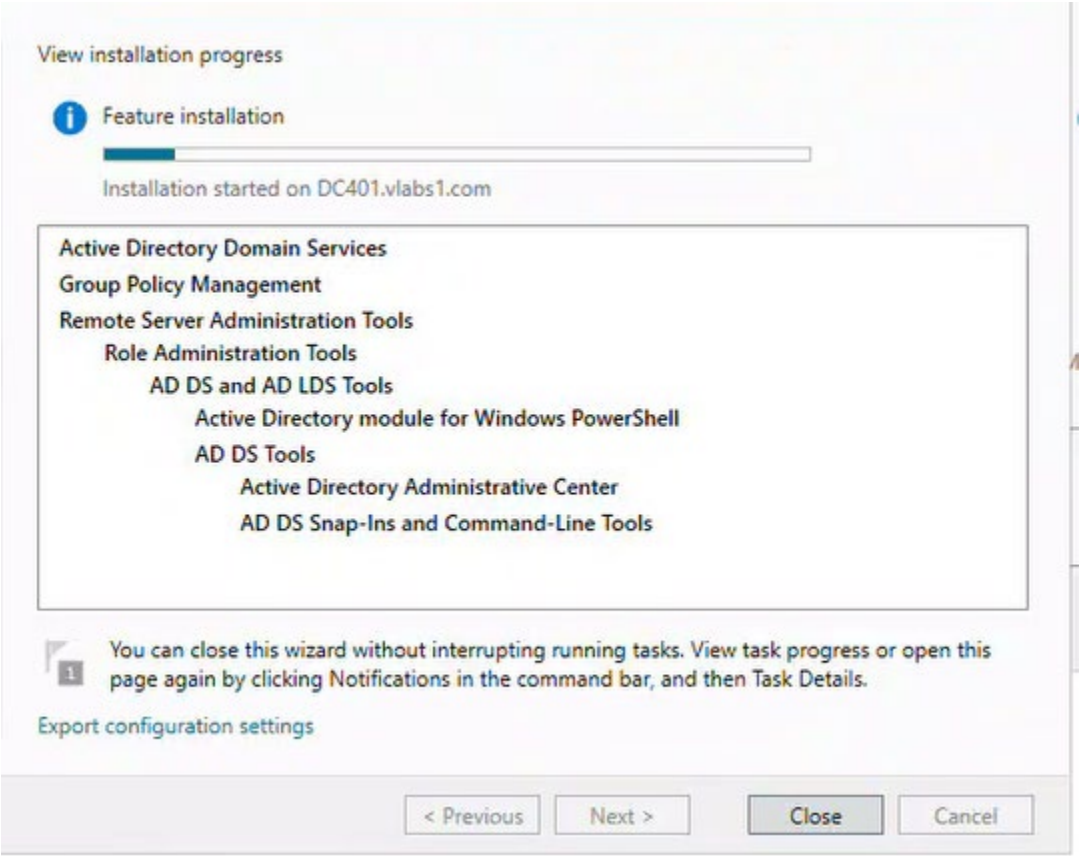
9. Review the information on the **AD DS** page and click **Next**



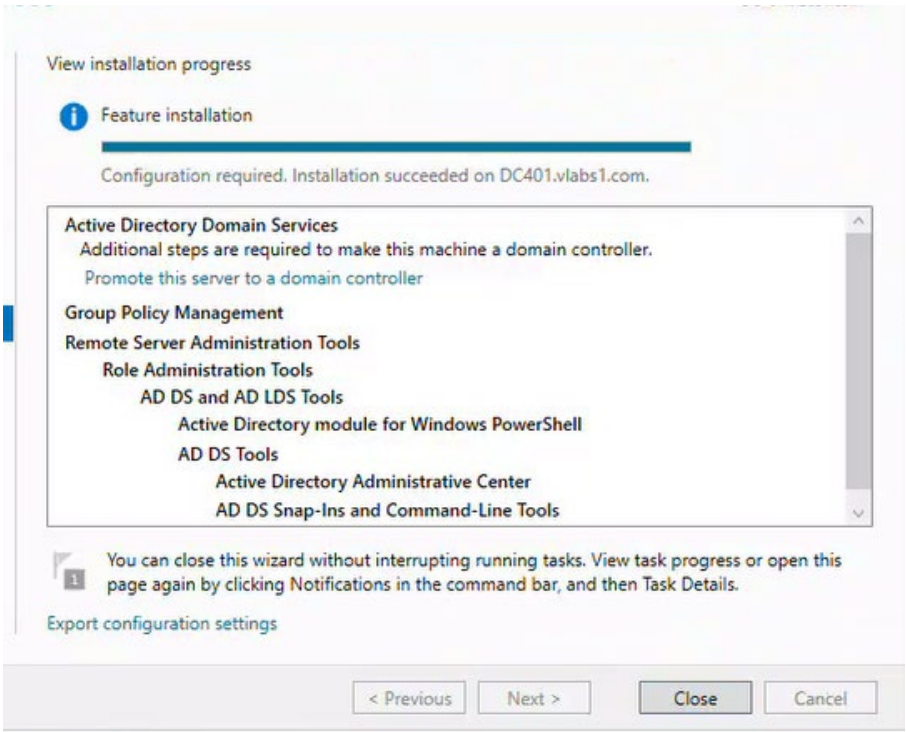
10. On the **Confirmation** page, check **"Restart the destination server automatically if required"**
11. Click **Install**



12. Wait for the installation to complete (this may take several minutes)



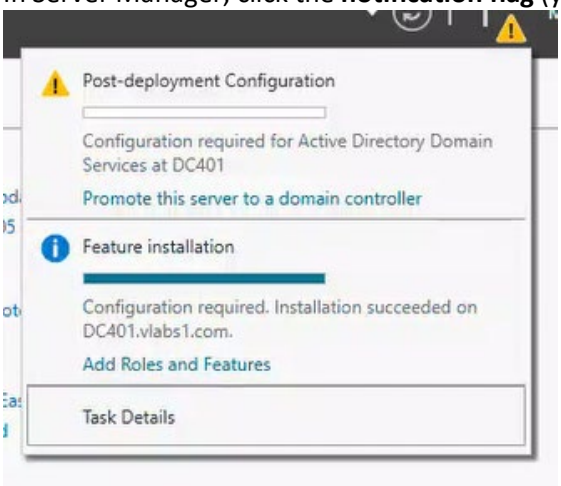
13. Click **Close** when installation is finished



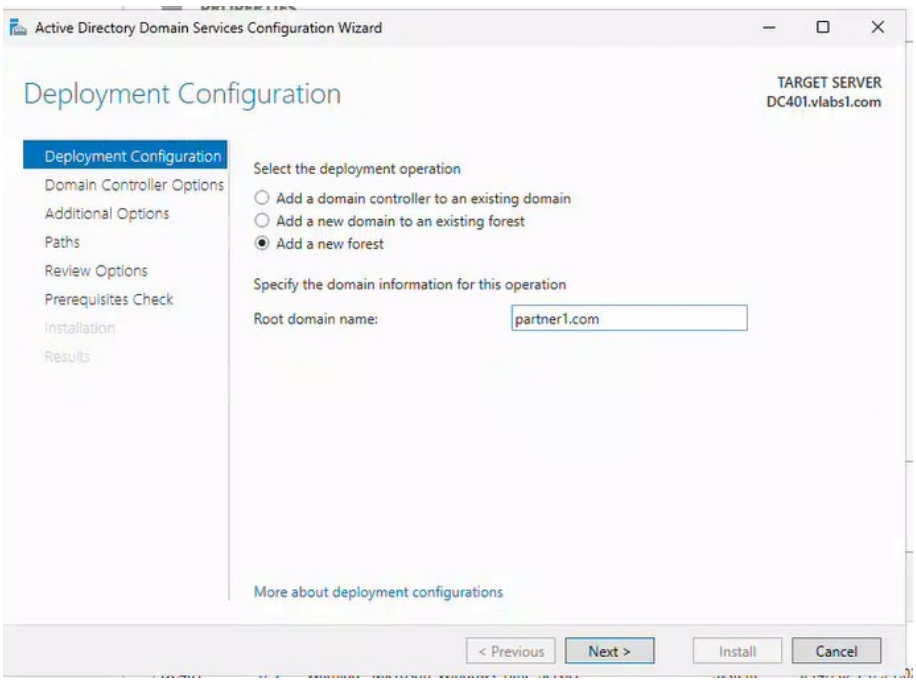
2.4.1.1.2 Create a new forest partner1.com.

Promote DC401 as a New Domain Controller in New Forest partner1.com

1. In Server Manager, click the **notification flag** (yellow triangle with exclamation mark)

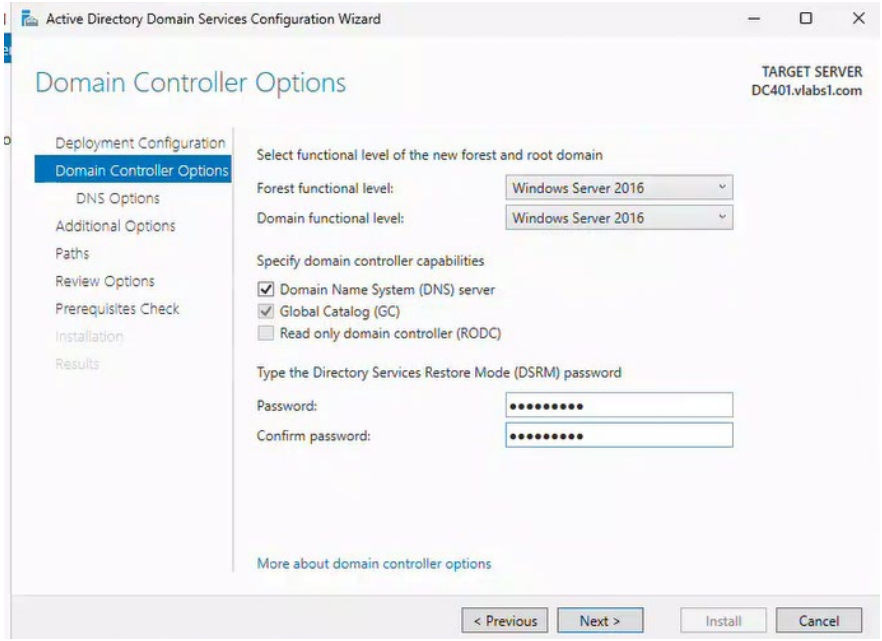


2. Click **"Promote this server to a domain controller"**
3. In the **Deployment Configuration** screen:
   - Select **"Add a new forest"**
   - Enter **"partner1.com"** as the Root domain name
   - Click **Next**

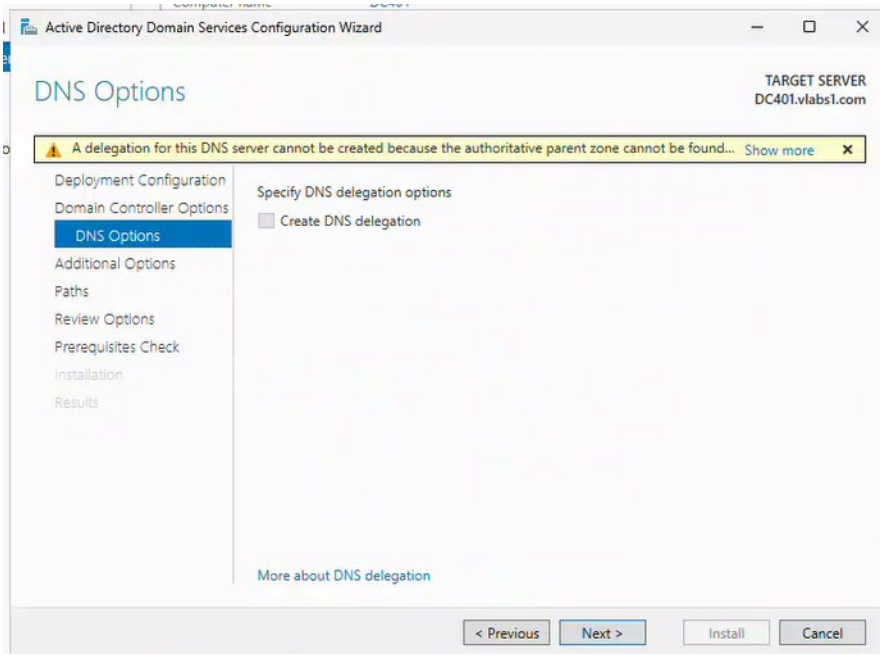


4. In the **Domain Controller Options** screen:
   - Set the **Forest functional level** (select Windows Server 2016 or later as appropriate)
   - Set the **Domain functional level** (select same as above)

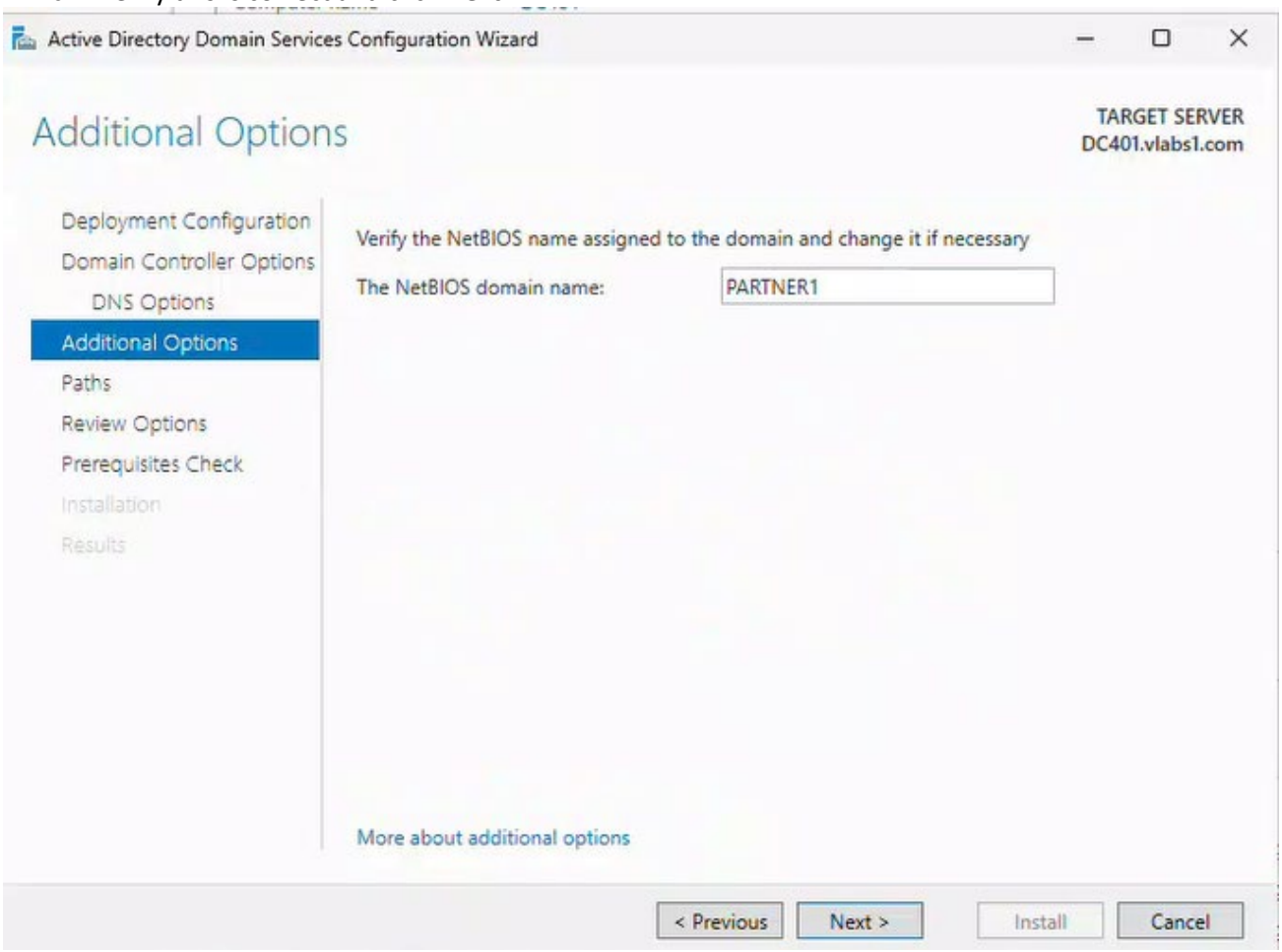
- Enter and confirm a **DSRM (Directory Services Restore Mode) password**
- Ensure **Domain Name System (DNS) server** is checked
- Ensure **Global Catalog (GC)** is checked
- Set password for as Passw0rd$
- Click **Next**



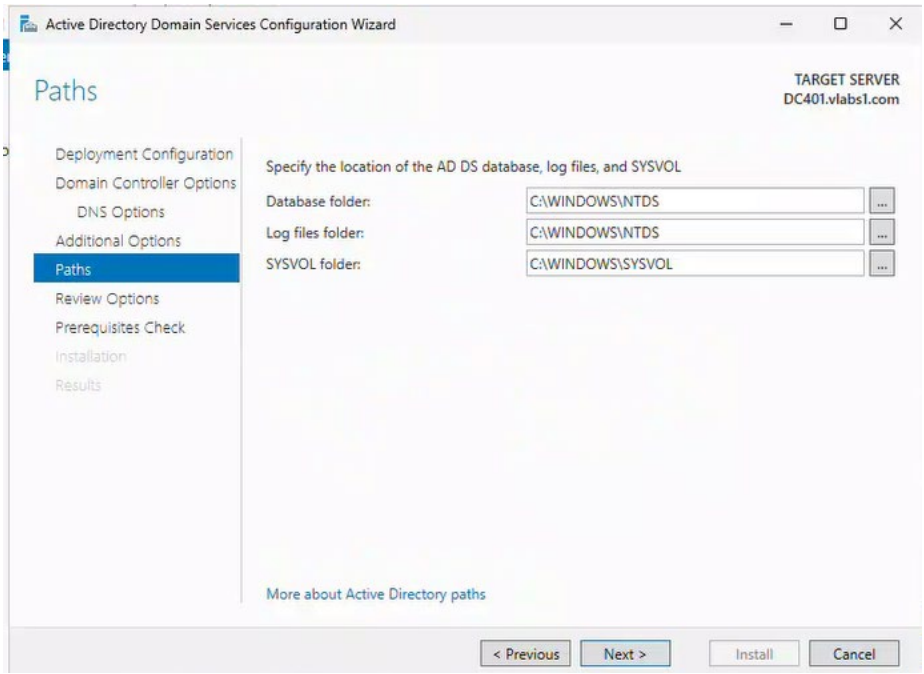
5. In the **DNS Options** screen (you may get a warning about DNS delegation - this is normal for a new forest):
   - Click **Next**



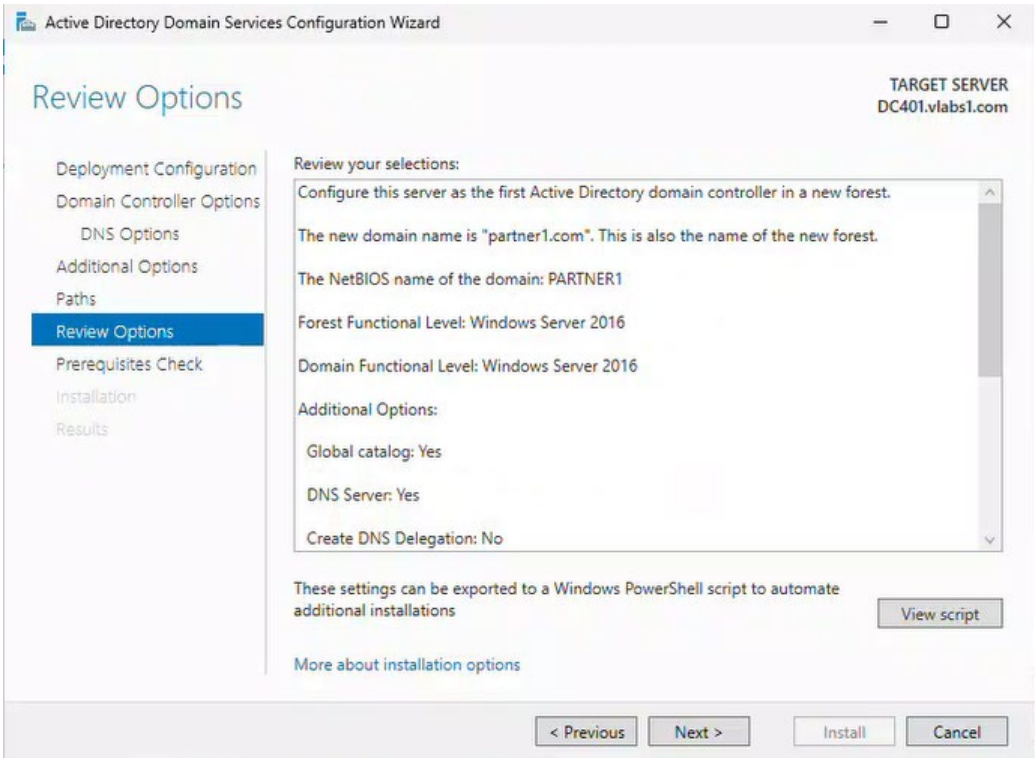
6. In the **Additional Options** screen:
    - The NetBIOS domain name will auto-populate as **PARTNER1**
    - Verify this is correct and click **Next**



7. In the **Paths** screen:
    - Specify locations for:
        - Database folder
        - Log files folder
        - SYSVOL folder
    - You can leave defaults or specify alternative paths if needed
    - Click **Next**



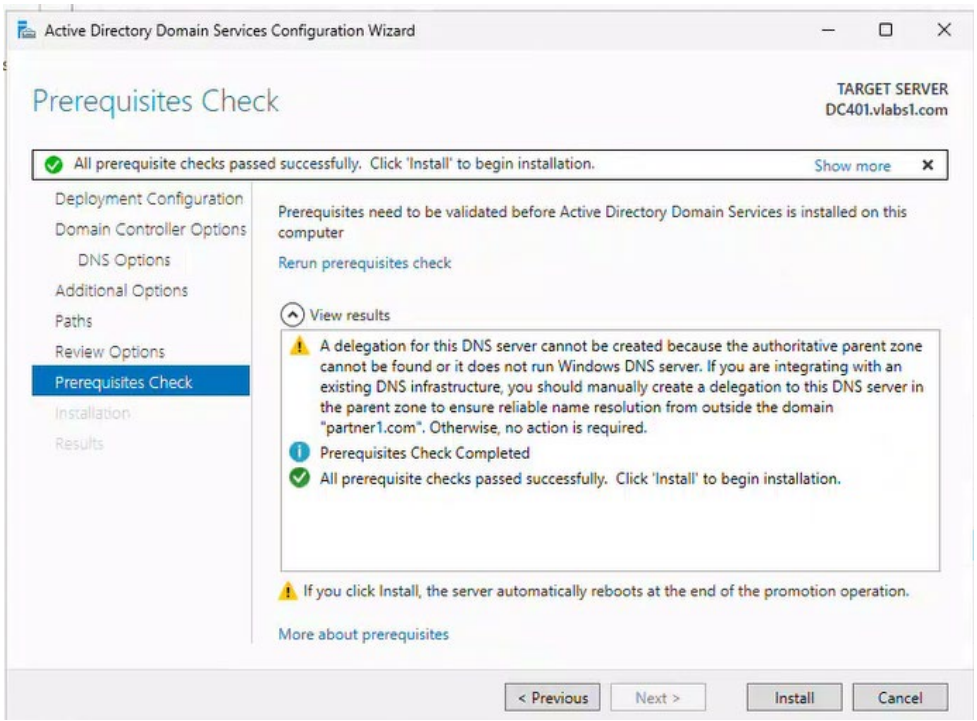
8. In the **Review Options** screen:
    - Review your selections
    - Click **View script** if you want to see the PowerShell equivalent
    - Click **Next**



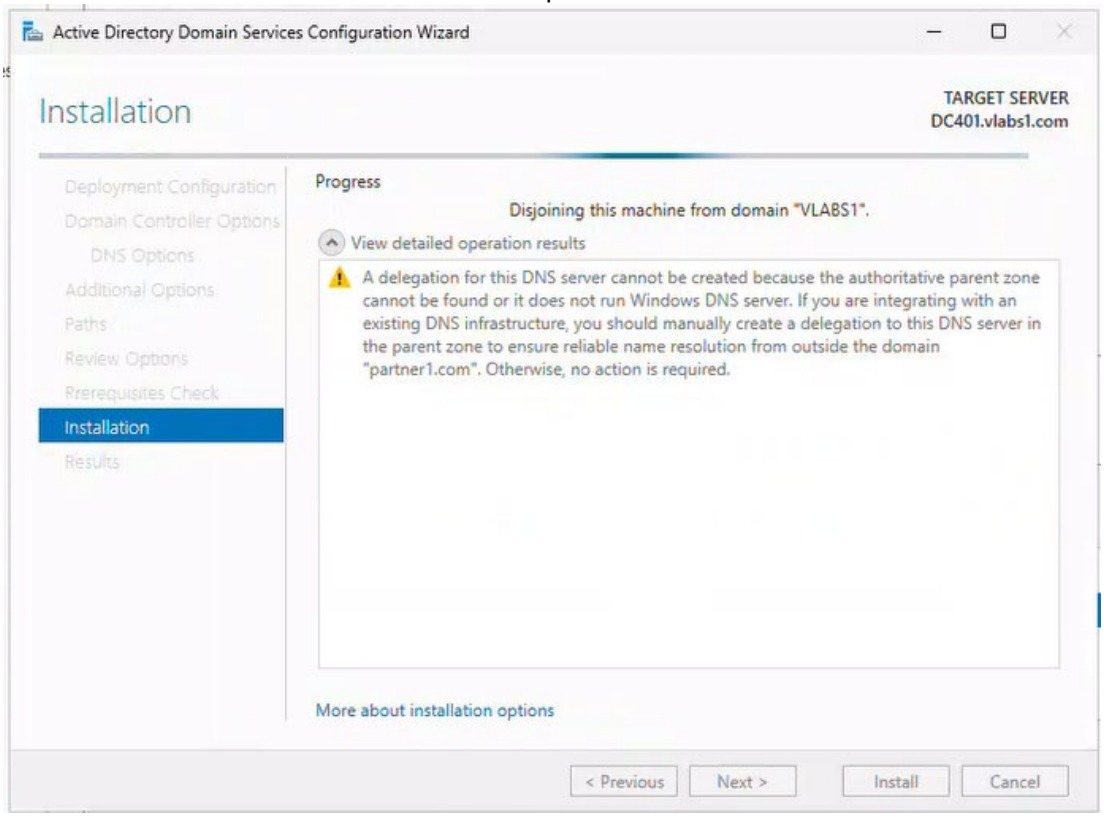
1

9. In the **Prerequisites Check** screen:
    - Wait for the system to verify all prerequisites are met
    - If any warnings appear, address them before proceeding

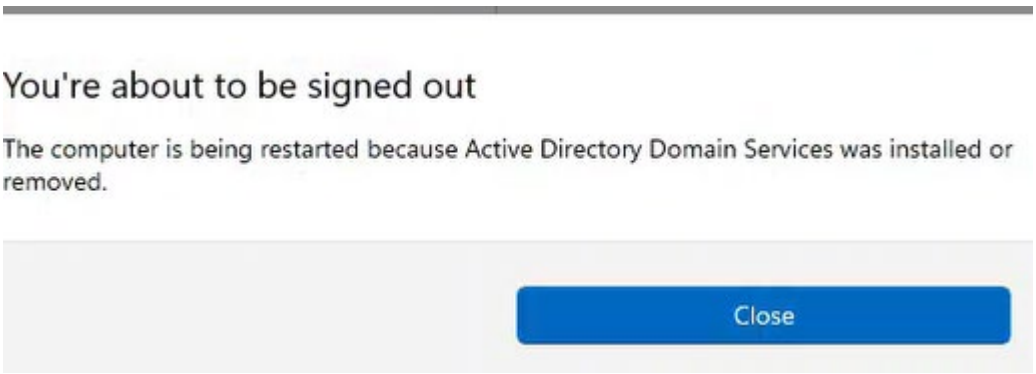
- Click **Install** when ready



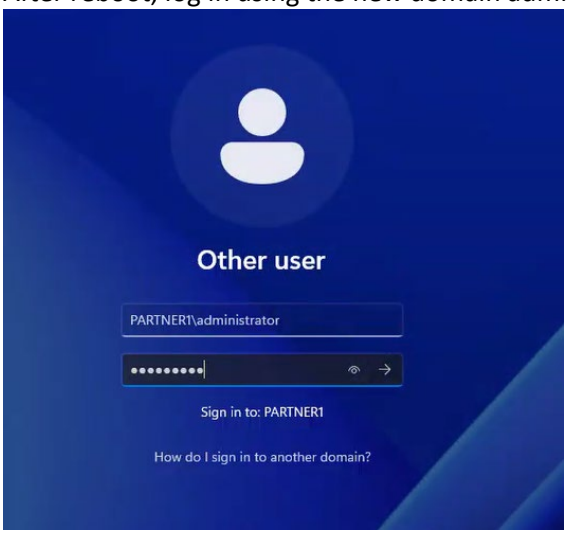
10. The server will now install AD DS and promote itself as the first DC in the new forest



11. The server will **automatically restart** when complete

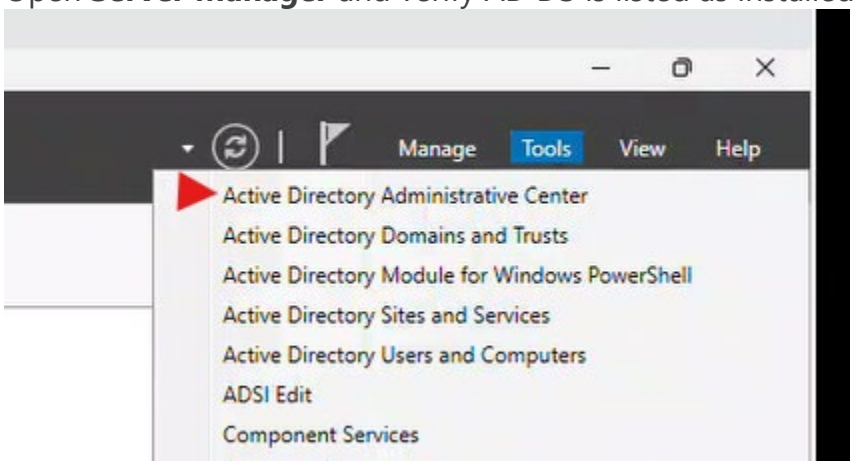


12. After reboot, log in using the new domain administrator credentials (PARTNER1\Administrator)

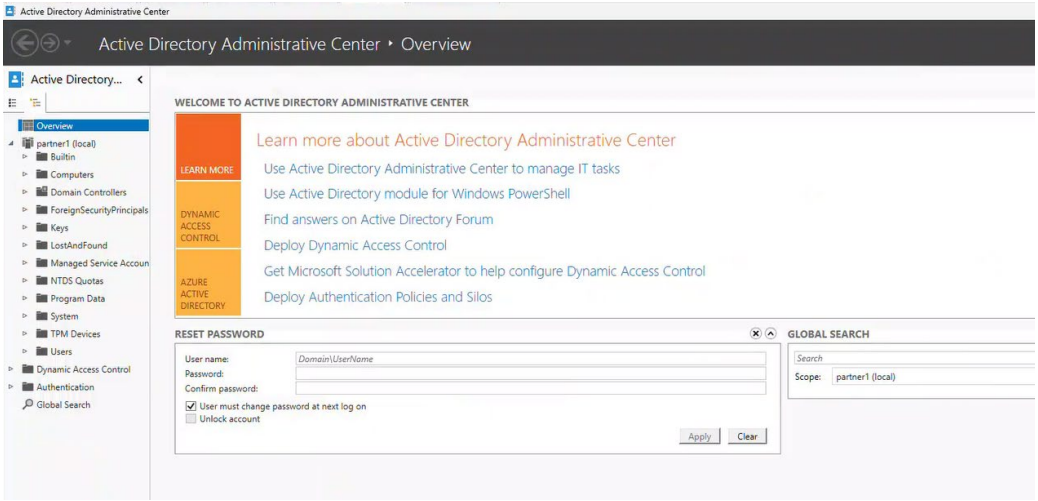


2.4.1.1.3 Verification Steps

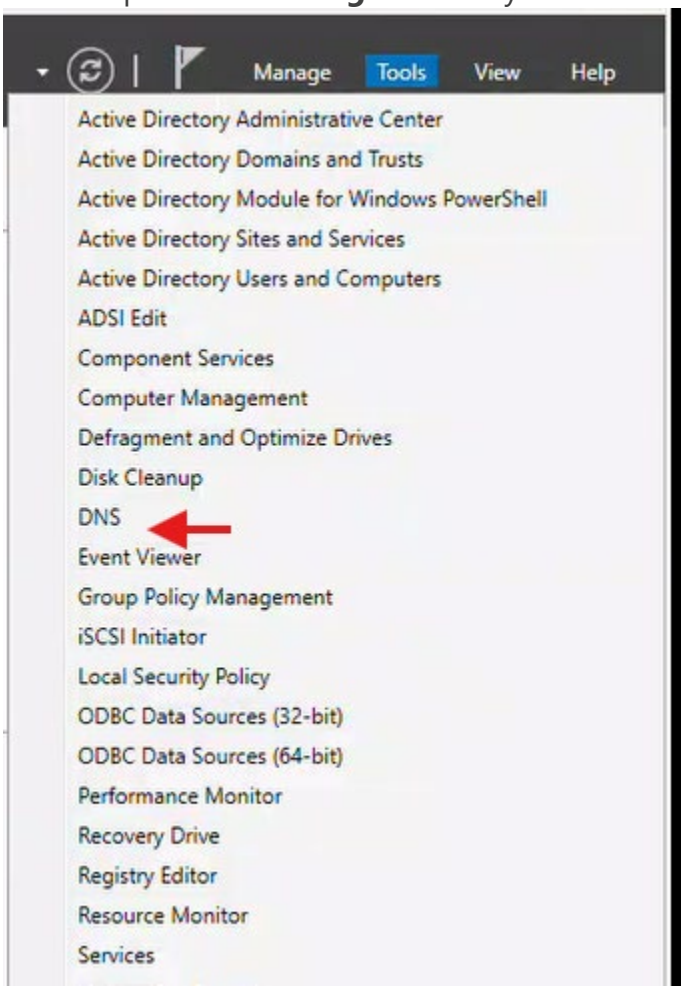
1. After promotion completes and server reboots:
    - Open **Server Manager** and verify AD DS is listed as installed

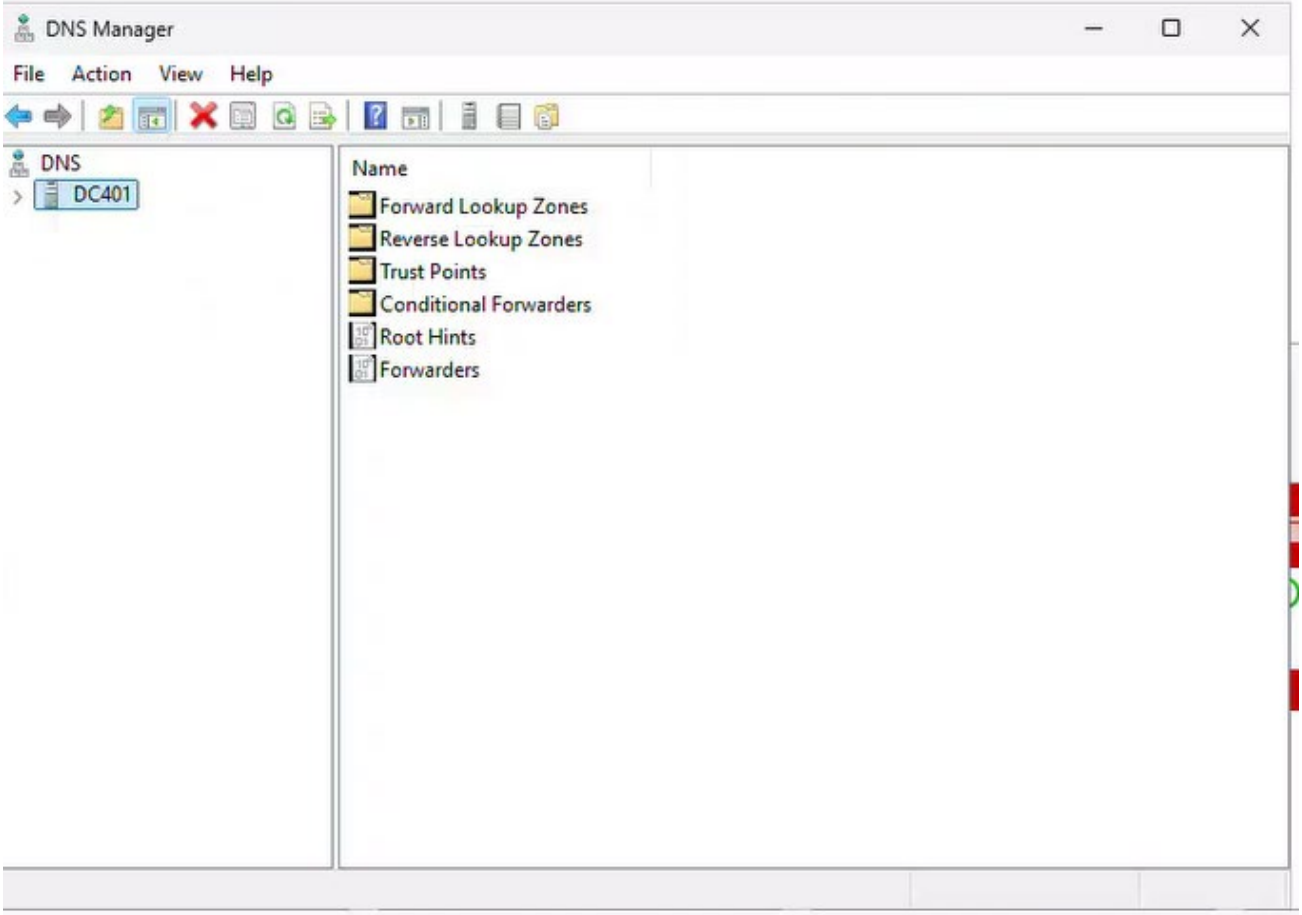


    - Open **Active Directory Users and Computers** to verify the domain structure exists

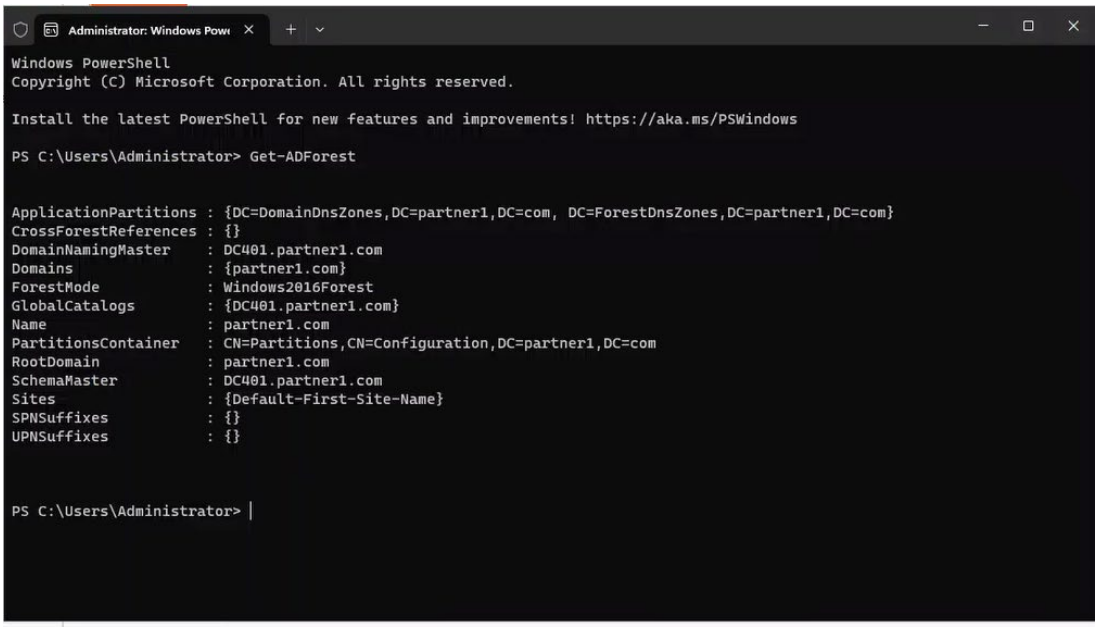


- Open **DNS Manager** to verify DNS zones were created properly





- Run `Get-ADForest` in PowerShell to verify forest information

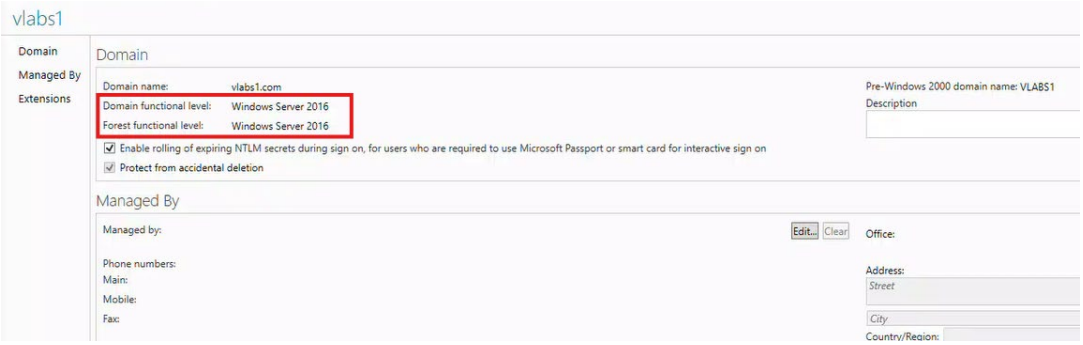


2.4.2 Task 2: Verify Domain and Forest Functional Levels

2.4.2.1 Check the Domain and Forest Functional Levels on vlabs1.com

2.4.2.1.1 Method 1: Using Active Directory Administrative Center (GUI)

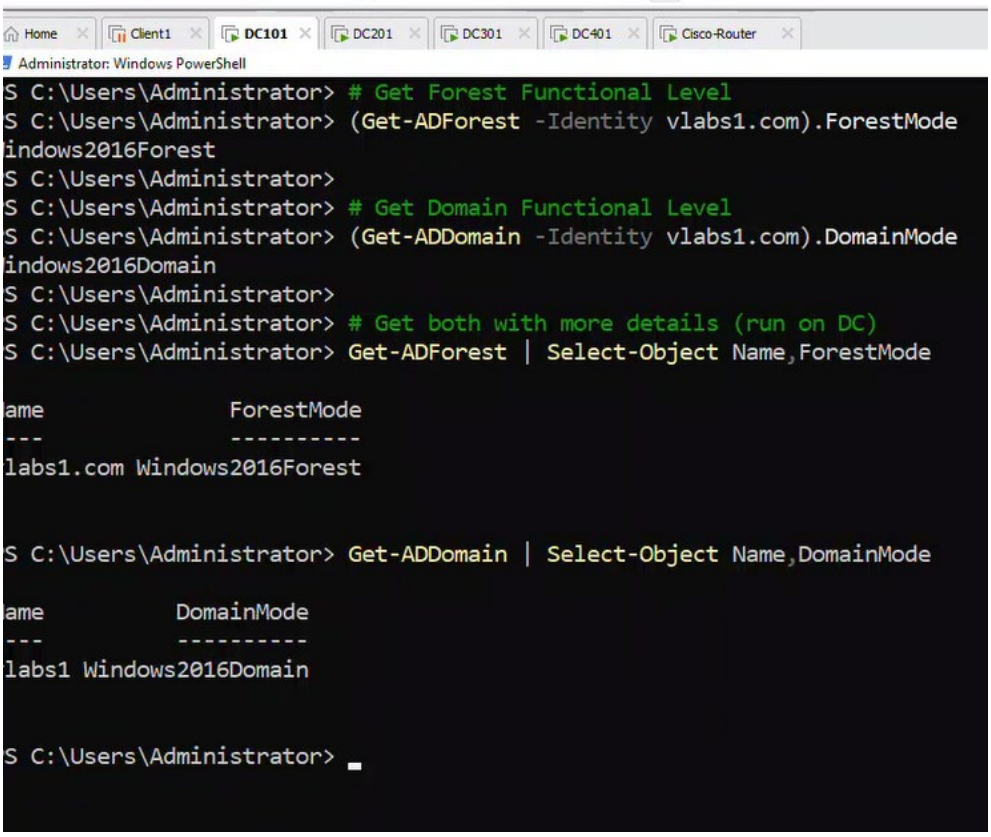
1. **Open Active Directory Administrative Center**:
   - Open Server Manager > Tools > Active Directory Administrative Center

2. **View Functional Levels**:
   - In the left pane, right-click your domain (`vlabs1.com`)
   - Select **Properties**
   - In the properties window, look for:
     - **Forest functional level**
     - **Domain functional level**
   - 

   -

2.4.2.1.2 Method 2: Using PowerShell

```
# Get Forest Functional Level
(Get-ADForest -Identity vlabs1.com).ForestMode

# Get Domain Functional Level
(Get-ADDomain -Identity vlabs1.com).DomainMode

# Get both with more details (run on DC)
Get-ADForest | Select-Object Name,ForestMode
Get-ADDomain | Select-Object Name,DomainMode
```



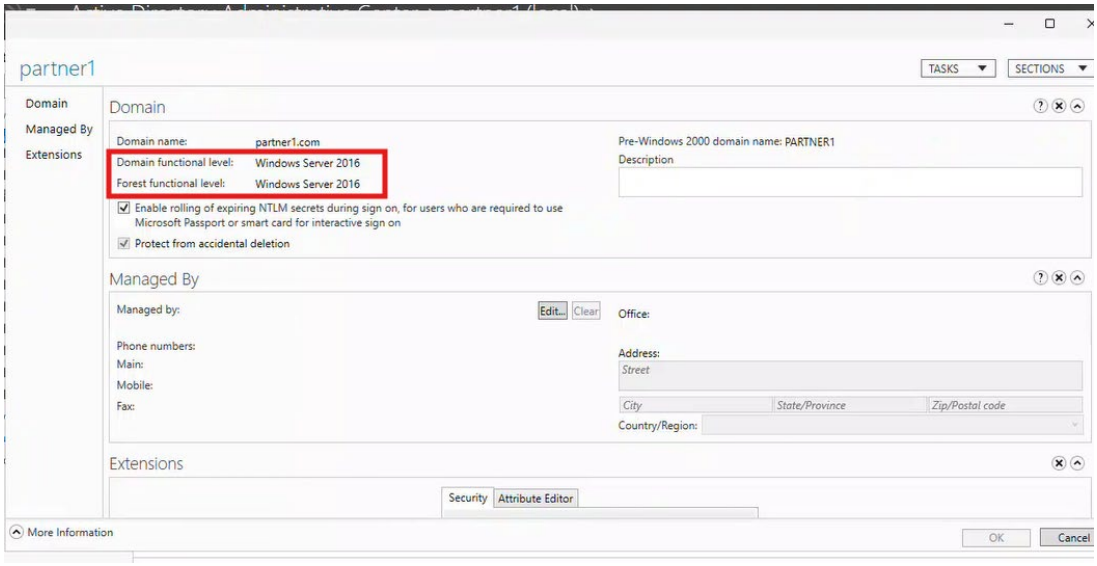
2.4.2.2 Check the Domain and Forest Functional Levels on partner1.com

- Using **Active Directory Administrative Center**
- Using **PowerShell**

2.4.2.2.1 Method 1: Using Active Directory Administrative Center (GUI)

1. **Open Active Directory Administrative Center**:
   - Open Server Manager > Tools > Active Directory Administrative Center

2. **View Functional Levels**:
   - In the left pane, right-click your domain (`partner1.com`)
   - Select **Properties**
   - In the properties window, look for:
     - **Forest functional level**
     - **Domain functional level**



2.4.2.2.2 Method 2: Using PowerShell

```
# Get Forest Functional Level
(Get-ADForest -Identity partner1.com).ForestMode

# Get Domain Functional Level
(Get-ADDomain -Identity partner1.com).DomainMode

# Get both with more details (run on DC)
Get-ADForest | Select-Object Name,ForestMode
Get-ADDomain | Select-Object Name,DomainMode
```

```
Administrator: Windows Powe
PS C:\Users\Administrator> # Get Forest Functional Level
PS C:\Users\Administrator> (Get-ADForest -Identity partner1.com).ForestMode
Windows2016Forest
PS C:\Users\Administrator>
PS C:\Users\Administrator> # Get Domain Functional Level
PS C:\Users\Administrator> (Get-ADDomain -Identity partner1.com).DomainMode
Windows2016Domain
PS C:\Users\Administrator> # Get both with more details (run on DC)
PS C:\Users\Administrator> Get-ADForest | Select-Object Name,ForestMode

Name                ForestMode
----                ----------
partner1.com Windows2016Forest


PS C:\Users\Administrator> Get-ADDomain | Select-Object Name,DomainMode

Name            DomainMode
----            ----------
partner1 Windows2016Domain


PS C:\Users\Administrator>
```

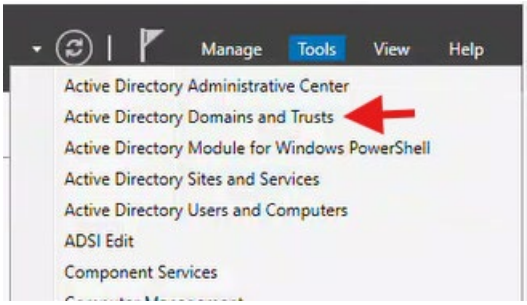
2.4.3 Task 3: Listing Trusts

2.4.3.1 List all Trusts on vlabs1.com and labs1.vlabs1.com

- Using **Active Directory Domains and Trusts.**
- Using **PowerShell.**

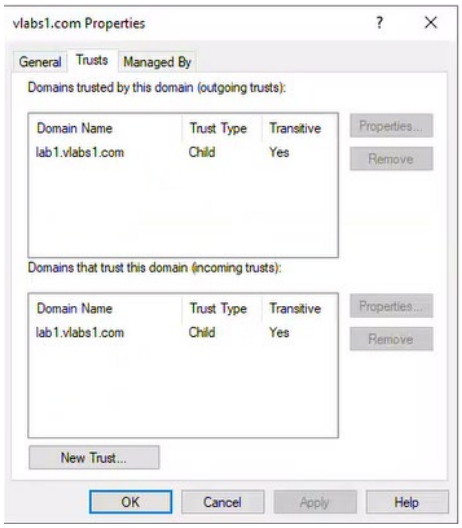
2.4.3.1.1 Using Active Directory Domains and Trusts

1. open from **Server Manager > Tools > Active Directory Domains and Trusts**.

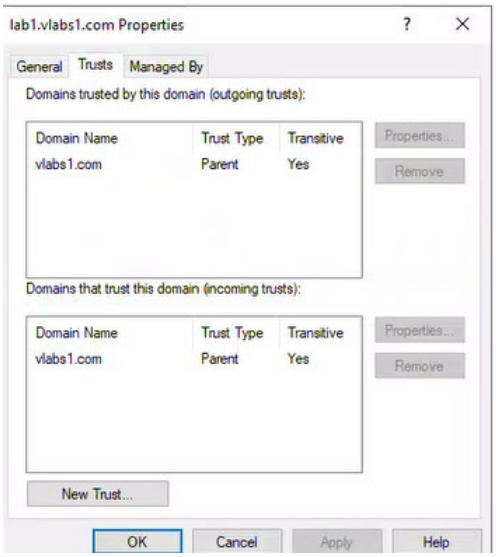


2. **View Trusts for** `vlabs1.com`:
   - Right-click `vlabs1.com` in the left pane.
   - Select **Properties**.
   - Go to the **Trusts** tab.
   - You will see:

- **Domains trusted by this domain (outgoing trusts)**
- **Domains that trust this domain (incoming trusts)**



3. **View Trusts for** `lab1.vlabs1.com`:
   - Right-click `lab1.vlabs1.com`.
   - Select **Properties**.
   - Go to the **Trusts** tab.



2.4.3.1.2 Using PowerShell

 # List Trusts for vlabs1.com
Get-ADTrust -Filter * -Server vlabs1.com |
Select-Object Name, Direction, TrustType, TrustAttributes |
Format-Table -AutoSize

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> # List Trusts for vlabs1.com
PS C:\Users\Administrator> Get-ADTrust -Filter * -Server vlabs1.com |
>>     Select-Object Name, Direction, TrustType, TrustAttributes |
>>     Format-Table -AutoSize

Name                Direction TrustType TrustAttributes
----                --------- --------- --------------
lab1.vlabs1.com BiDirectional   Uplevel             32


PS C:\Users\Administrator>
```

 # List Trusts for labs1.vlabs1.com
Get-ADTrust -Filter * -Server lab1.vlabs1.com |
Select-Object Name, Direction, TrustType, TrustAttributes |
Format-Table -AutoSize

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> # List Trusts for labs1.vlabs1.com
PS C:\Users\Administrator> Get-ADTrust -Filter * -Server lab1.vlabs1.com |
>>     Select-Object Name, Direction, TrustType, TrustAttributes |
>>     Format-Table -AutoSize

Name           Direction TrustType TrustAttributes
----           --------- --------- --------------
vlabs1.com BiDirectional   Uplevel             32


PS C:\Users\Administrator>
```

 # List All trusts in the current domain
Get-ADTrust -Filter * | Select-Object Name, Target, TrustType, Direction

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> # List All trusts in the current domain
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADTrust -Filter * | Select-Object Name, Target, TrustType, Direction

Name            Target          TrustType     Direction
----            ------          ---------     ---------
lab1.vlabs1.com lab1.vlabs1.com   Uplevel BiDirectional


PS C:\Users\Administrator>
PS C:\Users\Administrator>
```

 # Get all trusts with full details

Get-ADTrust -Filter * | Format-List *

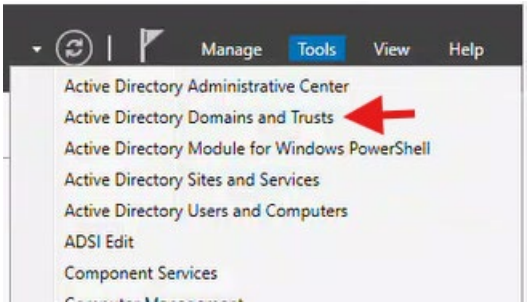
```
PS C:\Users\Administrator>
PS C:\Users\Administrator> # Get all trusts with full details
PS C:\Users\Administrator> Get-ADTrust -Filter * | Format-List *


Direction               : BiDirectional
DisallowTransivity      : False
DistinguishedName       : CN=lab1.vlabs1.com,CN=System,DC=vlabs1,DC=com
ForestTransitive        : False
IntraForest             : True
IsTreeParent            : False
IsTreeRoot              : False
Name                    : lab1.vlabs1.com
ObjectClass             : trustedDomain
ObjectGUID              : 538b8949-8cc3-4409-9bfc-ea7bb07f9abb
SelectiveAuthentication : False
SIDFilteringForestAware : False
SIDFilteringQuarantined : False
Source                  : DC=vlabs1,DC=com
Target                  : lab1.vlabs1.com
TGTDelegation           : False
TrustAttributes         : 32
TrustedPolicy           :
TrustingPolicy          :
TrustType               : Uplevel
UplevelOnly             : False
UsesAESKeys             : False
UsesRC4Encryption       : False
PropertyNames           : {Direction, DisallowTransivity, DistinguishedName, ForestTransitive...}
AddedProperties         : {}
RemovedProperties       : {}
ModifiedProperties      : {}
PropertyCount           : 23



PS C:\Users\Administrator>
```

*2.4.3.2 List all Trusts on **partner1.com***

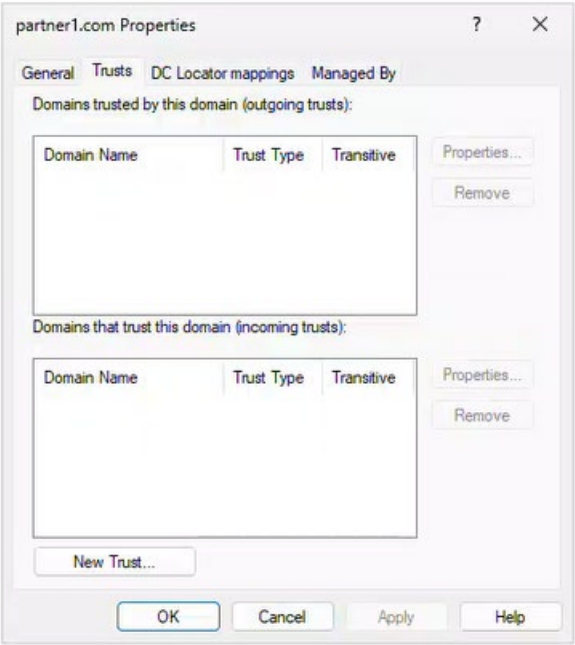
- Using **Active Directory Domains and Trusts.**
- Using **PowerShell.**

2.4.3.2.1 Using Active Directory Domains and Trusts

4. open from **Server Manager > Tools > Active Directory Domains and Trusts**.

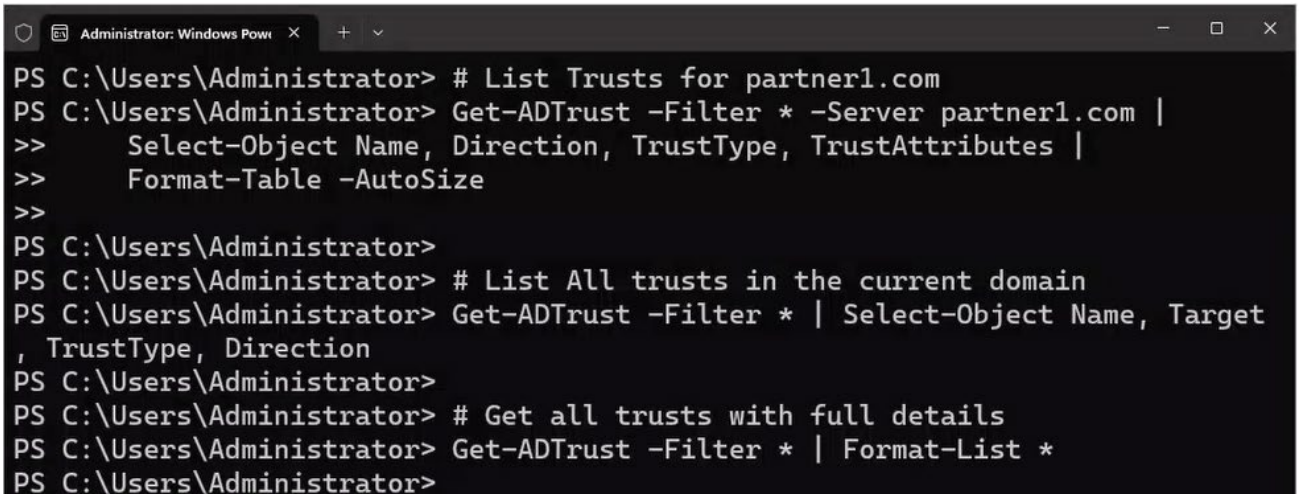


5. **View Trusts for** `partner1.com`:
   - Right-click `partner1.com` in the left pane.
   - Select **Properties**.
   - Go to the **Trusts** tab.
   - You will see:
     - **Domains trusted by this domain (outgoing trusts)**
     - **Domains that trust this domain (incoming trusts)**



2.4.3.2.2 Using PowerShell

```
# List Trusts for partner1.com
Get-ADTrust -Filter * -Server partner1.com |
   Select-Object Name, Direction, TrustType, TrustAttributes |
   Format-Table -AutoSize

# List All trusts in the current domain
Get-ADTrust -Filter * | Select-Object Name, Target, TrustType, Direction

# Get all trusts with full details
Get-ADTrust -Filter * | Format-List *
```



2.4.4 Task 4: Creating Trusts

2.4.4.1 Create DNS additional forwarders

1. **Create DNS Conditional Forwarders** to ensure both forests can resolve each other's domains.

   - On the **DNS** server of **DC101** create a **Conditional Forwarder** for **partner1.com** using **PowerShell**
     DC401_IP_Address -192.168.35.1

     ```
     # Create a conditional forwarder for partner1.com
     Add-DnsServerConditionalForwarderZone `
       -Name "partner1.com" `
       -MasterServers 192.168.35.1 `
       -ReplicationScope Forest `
       -PassThru
     ```

```
PS C:\Users\Administrator> # Create a conditional forwarder for partner1.com
PS C:\Users\Administrator> Add-DnsServerConditionalForwarderZone `
>>      -Name "partner1.com" `
>>      -MasterServers 192.168.35.1 `
>>      -ReplicationScope Forest `
>>      -PassThru

ZoneName                          ZoneType        IsAutoCreated   IsDsIntegrated  IsReverseLookupZone  IsSigned
--------                          --------        -------------   --------------  -------------------  --------
partner1.com                      Forwarder       False           True            False
```

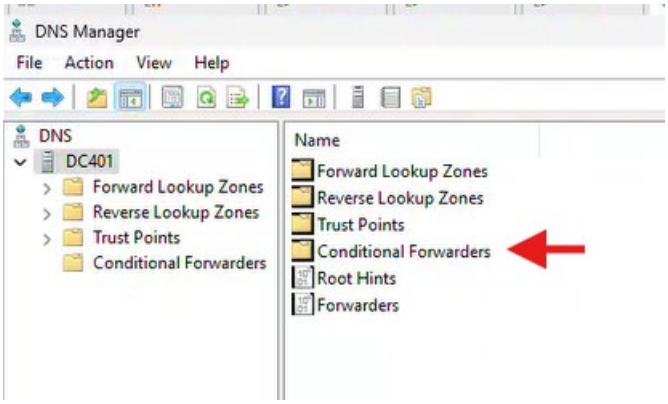
- Verify using **nslookup.**
  nslookup dc401.partner1.com

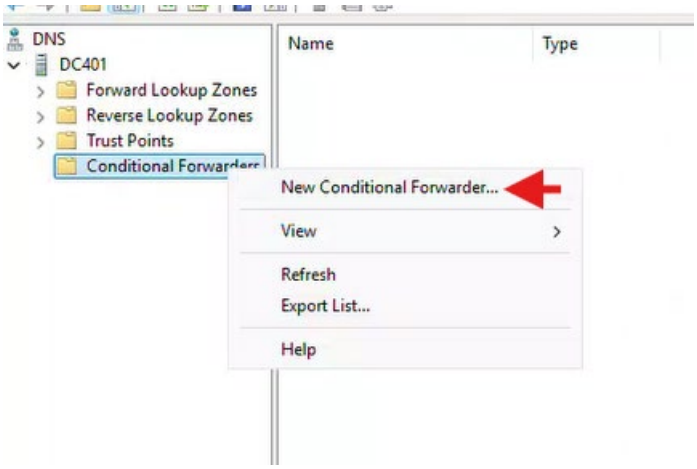
```
PS C:\Users\Administrator> nslookup dc401.partner1.com
Server:  localhost
Address:  127.0.0.1

Non-authoritative answer:
Name:    dc401.partner1.com
Address:  192.168.35.1

PS C:\Users\Administrator>
```

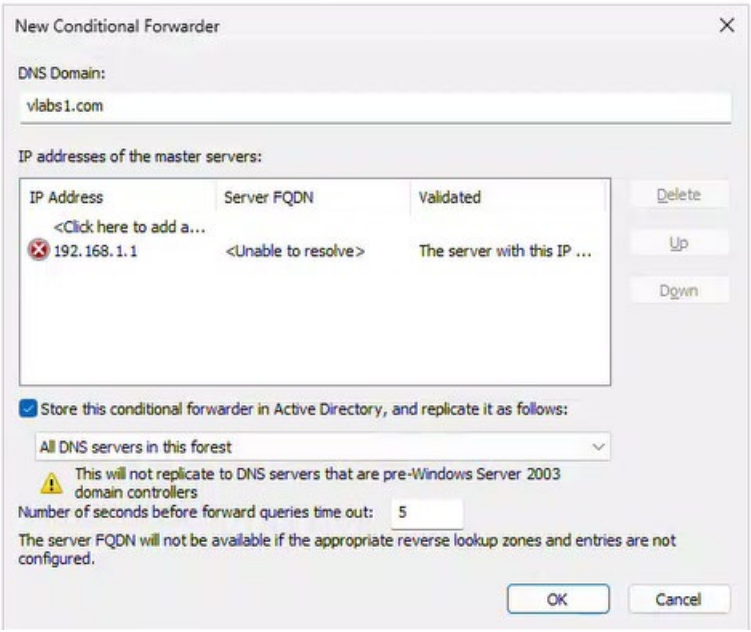
]

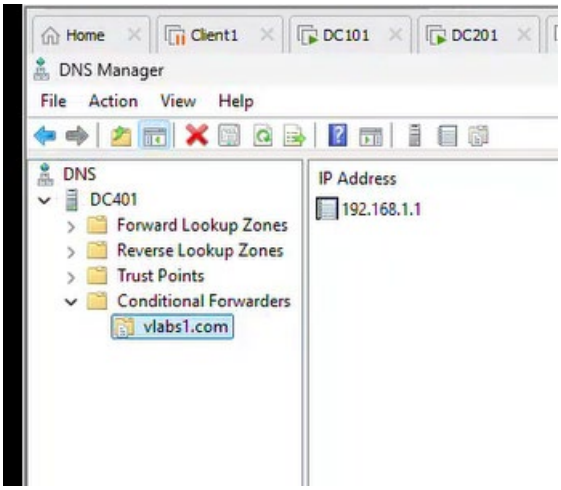
- On the **DNS** server of **DC401** create a **Conditional Forwarder** for **vlabs1.com** using **GUI**

  1. Open DNS Manager
  2. Expand DC401 > Conditional Forwarders.
  3. Right-click Conditional Forwarders → New Conditional Forwarder.
  4. Enter:
     - DNS Domain: vlabs1.com
     - IP Addresses of Master Servers: 192.168.1.1
  5. Check "Store this conditional forwarder in Active Directory".
  6. Click OK.


DNS Manager
File Action View Help
DNS
DC401
Forward Lookup Zones
Reverse Lookup Zones
Trust Points
Conditional Forwarders
Name
Forward Lookup Zones
Reverse Lookup Zones
Trust Points
Conditional Forwarders
Root Hints
Forwarders


DNS
DC401
Forward Lookup Zones
Reverse Lookup Zones
Trust Points
Conditional Forwarders
Name
Type
New Conditional Forwarder...
View
Refresh
Export List...
Help


New Conditional Forwarder
DNS Domain:
vlabs1.com
IP addresses of the master servers:
IP Address
Server FQDN
Validated
<Click here to add a...
192.168.1.1
<Unable to resolve>
The server with this IP ...
Delete
Up
Down
Store this conditional forwarder in Active Directory, and replicate it as follows:
All DNS servers in this forest
This will not replicate to DNS servers that are pre-Windows Server 2003 domain controllers
Number of seconds before forward queries time out: 5
The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.
OK
Cancel



- Verify using **nslookup.**

```
PS C:\Users\Administrator> nslookup dc101.vlabs1.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Non-authoritative answer:
Name:    dc101.vlabs1.com
Address:  192.168.1.1

PS C:\Users\Administrator>
```

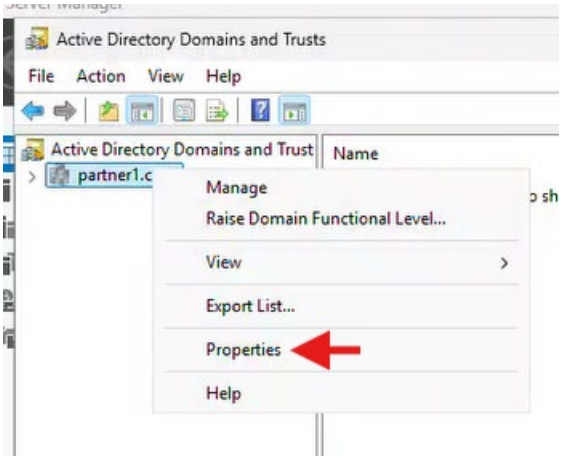
2.4.4.2 Create a Two-Way Transitive Forest Trust between vlabs1.com and Partner1.com

2.4.4.2.1 Using **GUI**:

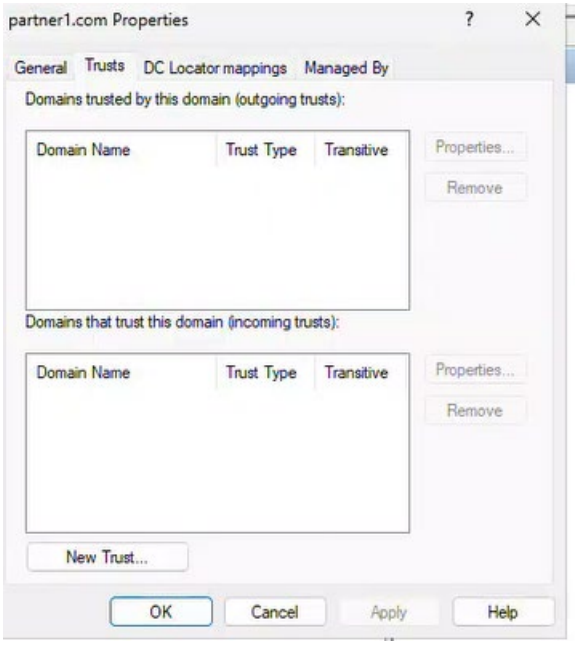
- Create a **Two-Way Transitive Forest Trust** between **vlabs1.com** and **Partner1.com**

On DC401 (partner1.com)

a) Open Active Directory Domains and Trusts
b) Right-click vlabs1.com → Properties → Trusts tab.

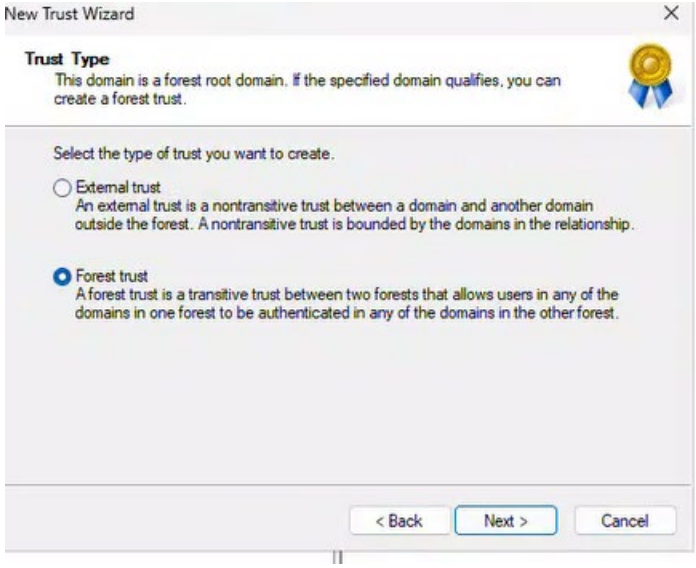


c) Click New Trust → Next.

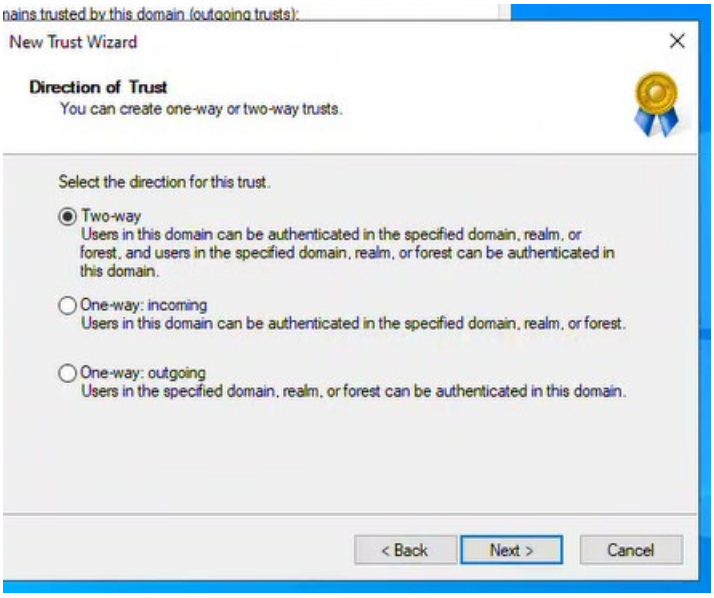


d) Enter vlabs1.com → Next.

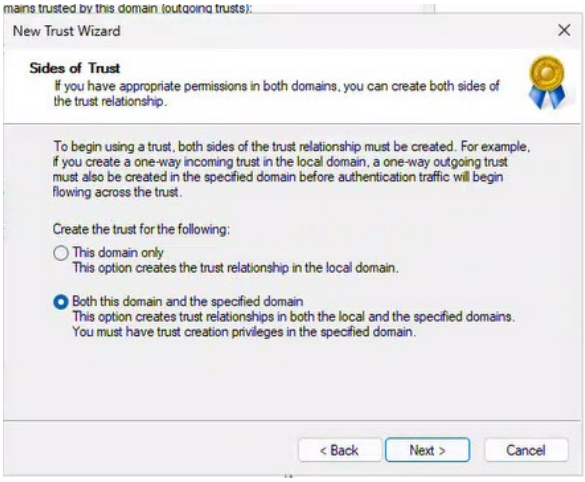
e) Select "Forest trust" → Next.



f) Select "Two-way" → Next.



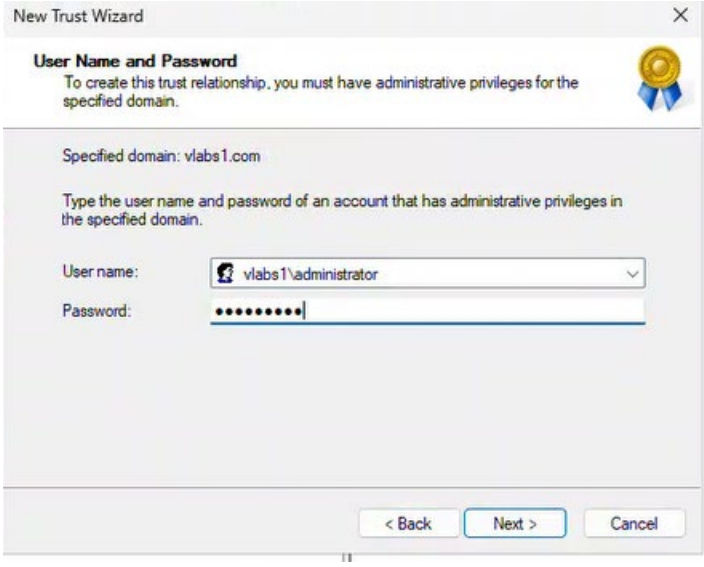
g) Choose "Both this domain and the specified domain" → Next.



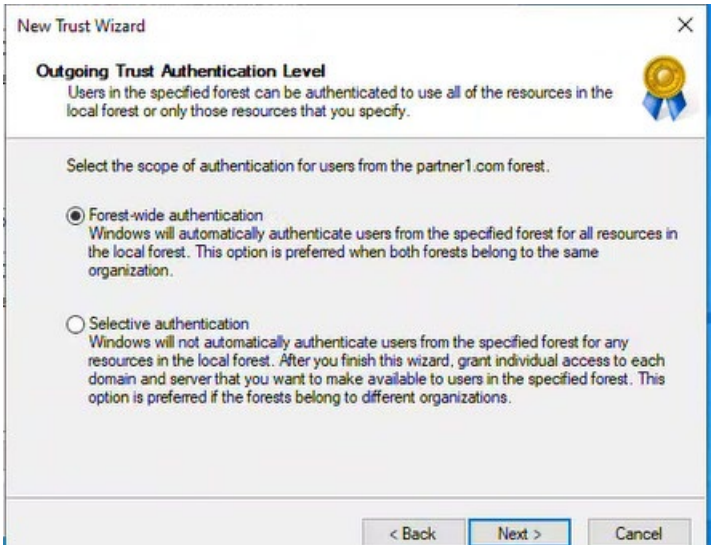
h) User name and password for vlabs1.

Vlabs1\administrator

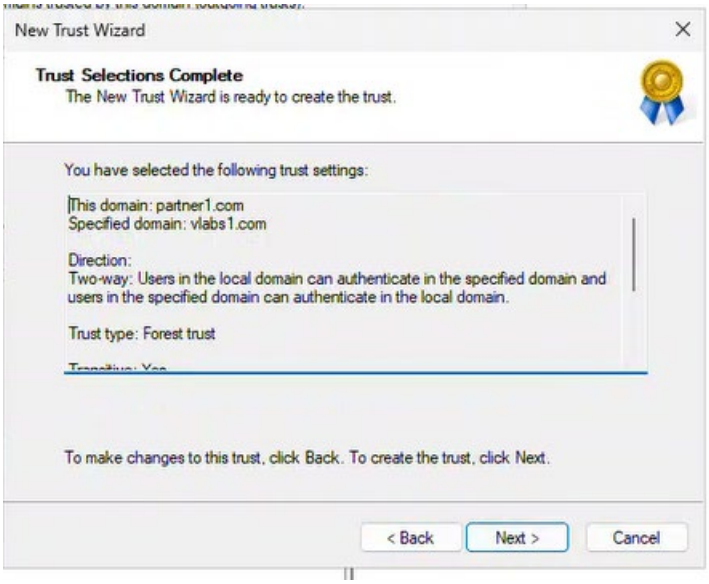
Pwd Passw0rd$



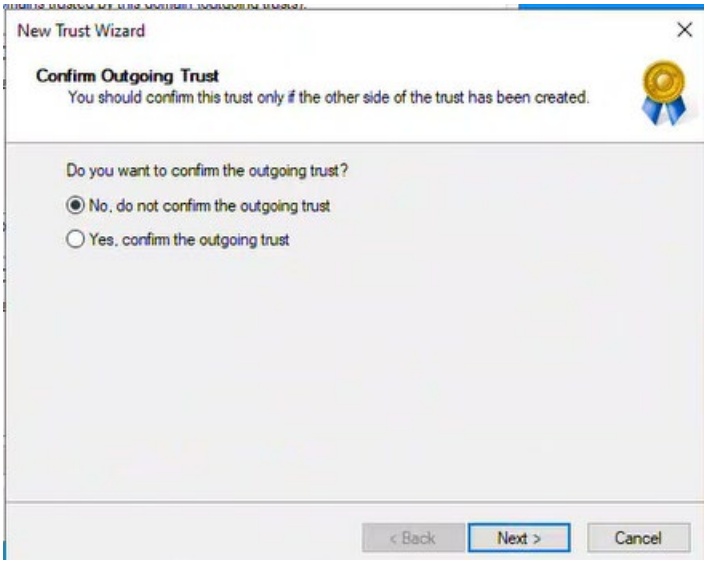
i) Select "Forest-wide authentication" → Next.

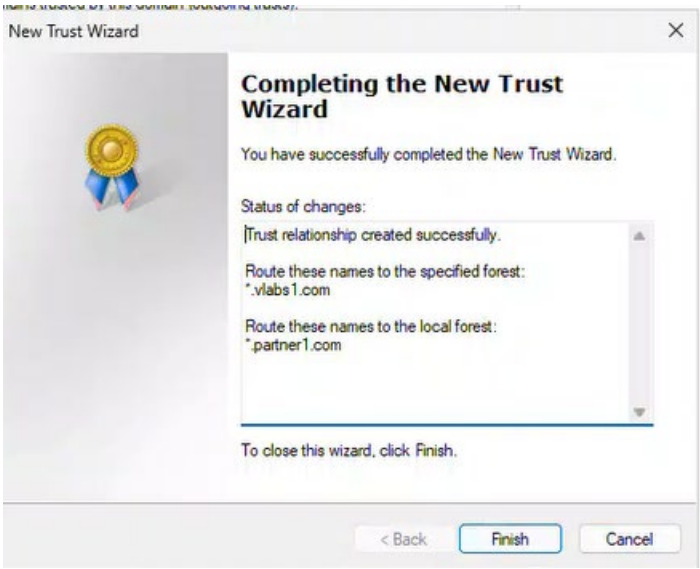


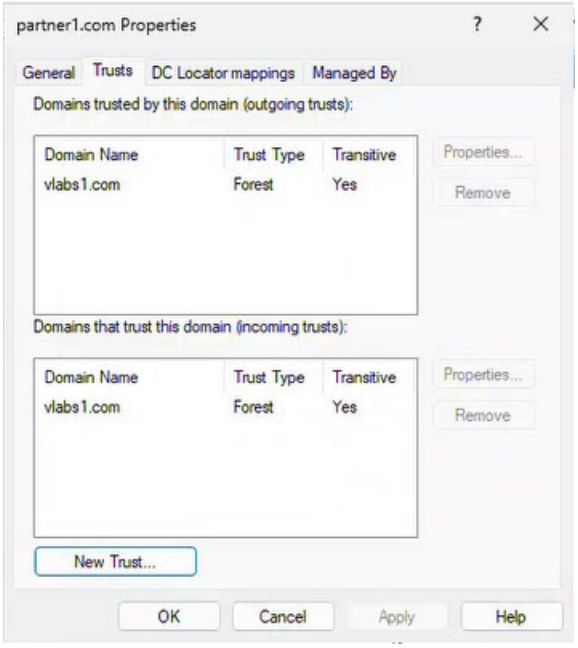
j) Confirm settings → Next → Finish.



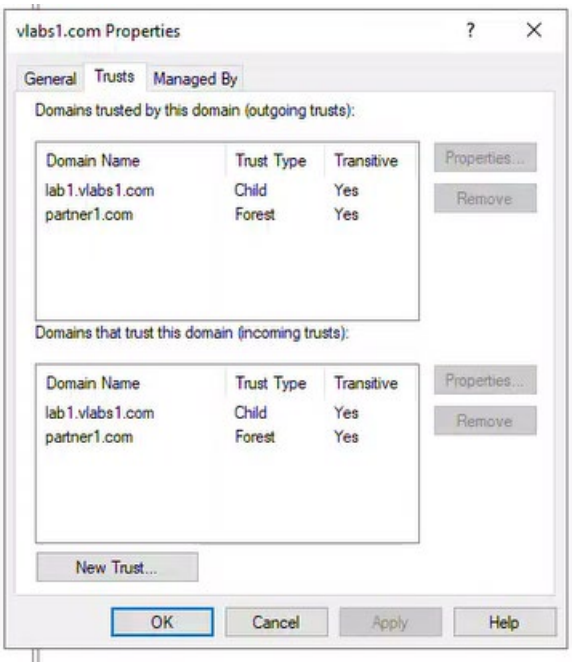
K) No, do not confirm the outgoing trust


New Trust Wizard
Confirm Outgoing Trust
You should confirm this trust only if the other side of the trust has been created.
Do you want to confirm the outgoing trust?
No, do not confirm the outgoing trust
Yes, confirm the outgoing trust
< Back
Next >
Cancel


New Trust Wizard
Completing the New Trust Wizard
You have successfully completed the New Trust Wizard.
Status of changes:
Trust relationship created successfully.
Route these names to the specified forest:
*.vlabs1.com
Route these names to the local forest:
*.partner1.com
To close this wizard, click Finish.
< Back
Finish
Cancel



DC101



2.4.4.2.1 Using PowerShell:

- **Verify the Trust Status on both Servers.**

Get-ADTrust -Filter * | Select-Object Name, Target , TrustType, Direction

DC101

```
PS C:\Users\Administrator> Get-ADTrust -Filter * | Select-Object Name, Target , TrustType, Direction

Name            Target          TrustType     Direction
----            ------          ---------     ---------
lab1.vlabs1.com lab1.vlabs1.com   Uplevel BiDirectional
partner1.com    partner1.com      Uplevel BiDirectional


PS C:\Users\Administrator>
```

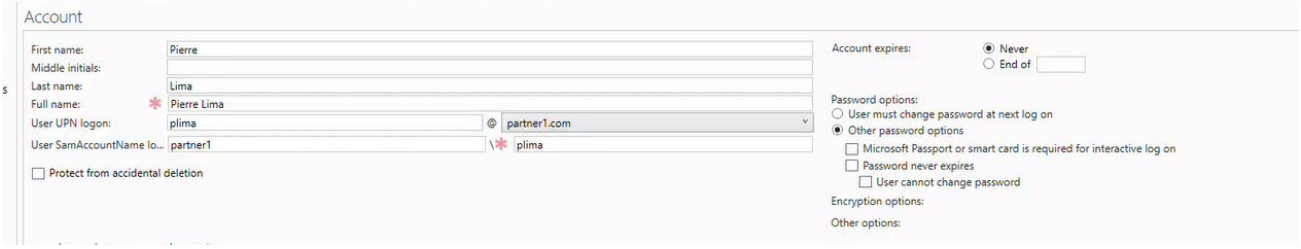
DC401

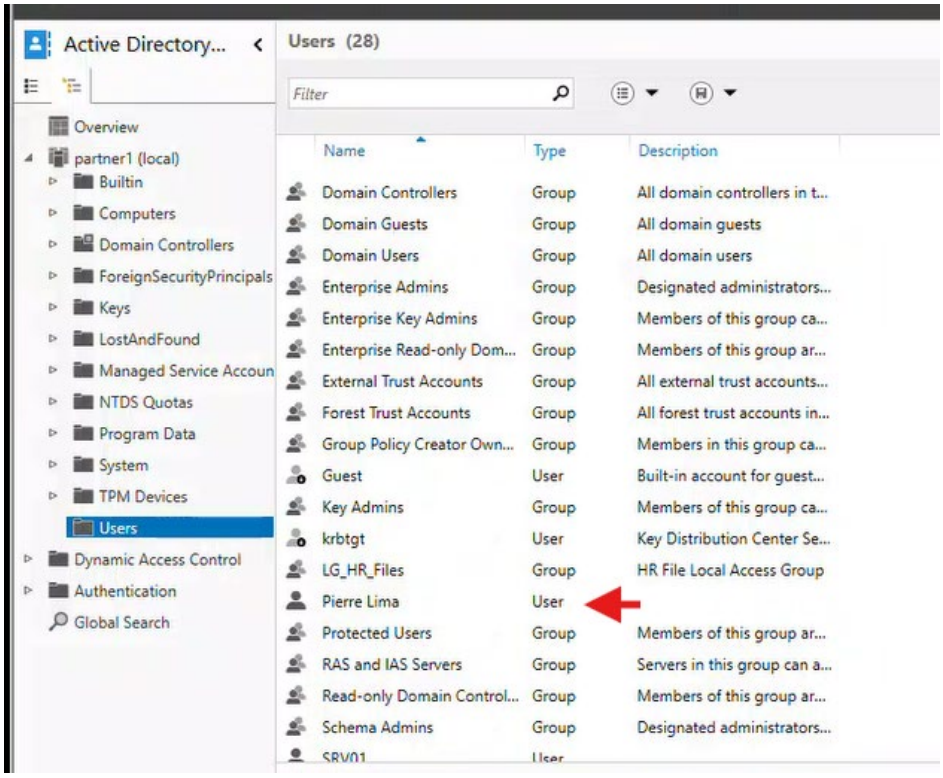
```
PS C:\Users\Administrator> Get-ADTrust -Filter * | Select-Object Name, Target , TrustType, Direction

Name       Target     TrustType     Direction
----       ------     ---------     ---------
vlabs1.com vlabs1.com   Uplevel BiDirectional
```

2.4.5 Task 5: Testing Trust Between Two Forests

1. **On DC401.partner1.com:**

   - Create **a new user** in **partner1.com** ➔ **Pierre Lima / Passw0rd$**

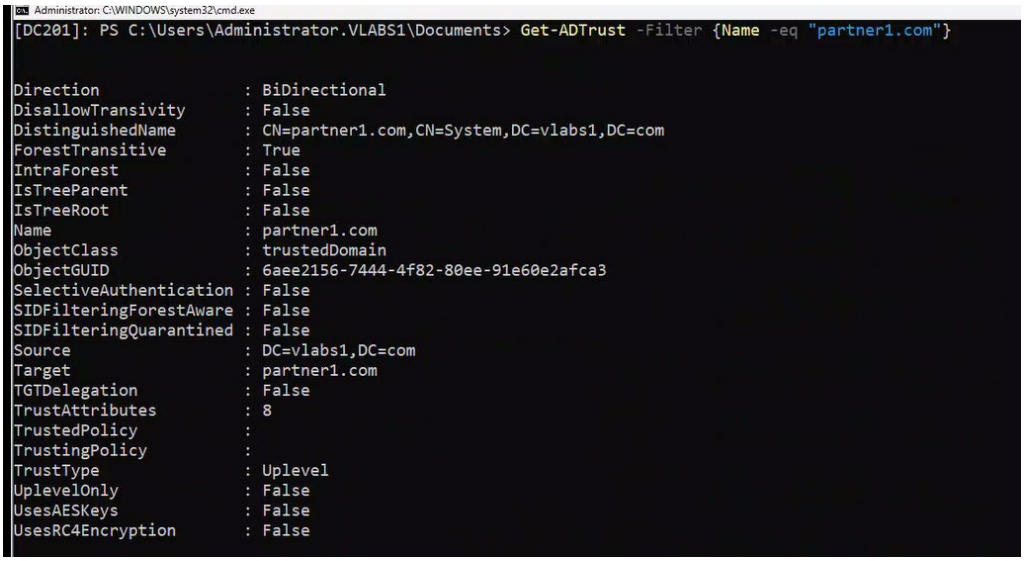




2. On DC201.vlabs1.com (Windows Server Core, RODC):

1. Verify the **trust** relationship with **partner1.com** using **PowerShell.**

Get-ADTrust -Filter {Name -eq "partner1.com"}



```
Administrator: C:\WINDOWS\system32\cmd.exe
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> Get-ADTrust -Filter {Name -eq "partner1.com"}


Direction               : BiDirectional
DisallowTransivity      : False
DistinguishedName       : CN=partner1.com,CN=System,DC=vlabs1,DC=com
ForestTransitive        : True
IntraForest             : False
IsTreeParent            : False
IsTreeRoot              : False
Name                    : partner1.com
ObjectClass             : trustedDomain
ObjectGUID              : 6aee2156-7444-4f82-80ee-91e60e2afca3
SelectiveAuthentication : False
SIDFilteringForestAware : False
SIDFilteringQuarantined : False
Source                  : DC=vlabs1,DC=com
Target                  : partner1.com
TGTDelegation           : False
TrustAttributes         : 8
TrustedPolicy           :
TrustingPolicy          :
TrustType               : Uplevel
UplevelOnly             : False
UsesAESKeys             : False
UsesRC4Encryption       : False
```

Get-ADTrust -Identity "partner1.com" | Format-List *

```
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> Get-ADTrust -Identity "partner1.com" | Format-List


Direction               : BiDirectional
DisallowTransivity      : False
DistinguishedName       : CN=partner1.com,CN=System,DC=vlabs1,DC=com
ForestTransitive        : True
IntraForest             : False
IsTreeParent            : False
IsTreeRoot              : False
Name                    : partner1.com
ObjectClass             : trustedDomain
ObjectGUID              : 6aee2156-7444-4f82-80ee-91e60e2afca3
SelectiveAuthentication : False
SIDFilteringForestAware : False
SIDFilteringQuarantined : False
Source                  : DC=vlabs1,DC=com
Target                  : partner1.com
TGTDelegation           : False
TrustAttributes         : 8
TrustedPolicy           :
TrustingPolicy          :
TrustType               : Uplevel
UplevelOnly             : False
UsesAESKeys             : False
UsesRC4Encryption       : False


[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
```

2. Create a folder **C:\Secret**

   New-Item -Path "C:\Secret" -ItemType Directory -Force

```
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> New-Item -Path "C:\Secret" -ItemType Directory -Force


    Directory: C:\


Mode                 LastWriteTime         Length Name

----                 -------------         ------ ----

d-----         5/15/2025   1:13 AM                Secret
```

3. Share **C:\Secret** and assign permissions **Read/Write** to 1 **plima@partner1.com.**

   New-SmbShare -Name "Secret" -Path "C:\Secret" -FullAccess plima@partner1.com

```
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> New-SmbShare -Name "Secret" -Path "C:\Secret" -FullAccess plima@partner1.com

Name   ScopeName Path      Description
----   --------- ----      -----------
Secret *         C:\Secret
```

   $acl = Get-Acl "C:\Secret"

$rule = New-Object System.Security.AccessControl.FileSystemAccessRule("plima@partner1.com", "Modify", "ContainerInherit,ObjectInherit", "None", "Allow")

$acl.AddAccessRule($rule)

Set-Acl "C:\Secret" $acl

```
Select Administrator: C:\WINDOWS\system32\cmd.exe
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> $acl = Get-Acl "C:\Secret"
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> $rule = New-Object System.Security.AccessControl.FileSystemAccessRule("plima@partner1.com", "Modify", "Container
,ObjectInherit", "None", "Allow")
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> $acl.AddAccessRule($rule)
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> Set-Acl "C:\Secret" $acl
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
```

4. Verify the **shared folder** and **NTFS permissions.**

Get-SmbShare -Name "Secret" | Format-List *

```
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> Get-SmbShare -Name "Secret" | Format-List *


PresetPathAcl          : System.Security.AccessControl.DirectorySecurity
ShareState             : Online
AvailabilityType       : NonClustered
ShareType              : FileSystemDirectory
FolderEnumerationMode  : Unrestricted
CachingMode            : Manual
LeasingMode            : Full
QoSFlowScope           : File
SmbInstance            : Default
CATimeout              : 0
CompressData           : False
ConcurrentUserLimit    : 0
ContinuouslyAvailable  : False
CurrentUsers           : 0
Description            :
DirectoryHandleLeasing : True
EncryptData            : False
IdentityRemoting       : False
Infrastructure         : False
IsolatedTransport      : False
Name                   : Secret
Path                   : C:\Secret
QoSPolicyId            : {00000000-0000-0000-0000-000000000000}
Scoped                 : False
ScopeName              : *
SecurityDescriptor     : O:SYG:SYD:(A;;FA;;;S-1-5-21-1245985154-6628414-958437321-1107)
ShadowCopy             : False
Special                : False
Temporary              : False
Volume                 : \\?\Volume{492ba56e-e44a-47db-9dec-edcb9e32c85a}\
PSComputerName         :
CimClass               : ROOT/Microsoft/Windows/SMB:MSFT_SmbShare
CimInstanceProperties  : {AvailabilityType, CachingMode, CATimeout, CompressData...}
CimSystemProperties    : Microsoft.Management.Infrastructure.CimSystemProperties


[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
```

(Get-Acl "C:\Secret").Access

```
Administrator: C:\WINDOWS\system32\cmd.exe
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> (Get-Acl "C:\Secret").Access


FileSystemRights  : Modify, Synchronize
AccessControlType : Allow
IdentityReference : PARTNER1\plima
IsInherited       : False
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags  : None

FileSystemRights  : FullControl
AccessControlType : Allow
IdentityReference : NT AUTHORITY\SYSTEM
IsInherited       : True
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags  : None

FileSystemRights  : FullControl
AccessControlType : Allow
IdentityReference : BUILTIN\Administrators
IsInherited       : True
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags  : None

FileSystemRights  : ReadAndExecute, Synchronize
AccessControlType : Allow
IdentityReference : BUILTIN\Users
IsInherited       : True
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags  : None

FileSystemRights  : AppendData
AccessControlType : Allow
IdentityReference : BUILTIN\Users
IsInherited       : True
InheritanceFlags  : ContainerInherit
PropagationFlags  : None

FileSystemRights  : CreateFiles
AccessControlType : Allow
IdentityReference : BUILTIN\Users
IsInherited       : True
InheritanceFlags  : ContainerInherit
PropagationFlags  : None

FileSystemRights  : 268435456
AccessControlType : Allow
IdentityReference : CREATOR OWNER
IsInherited       : True
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags  : InheritOnly
```

 # Grant Change permissions at share level

Grant-SmbShareAccess -Name "Secret" -AccountName "partner1\plima" -AccessRight Change -Force

 # Verify

Get-SmbShareAccess -Name "Secret" | Where-Object {$_.AccountName -like "*plima*"}

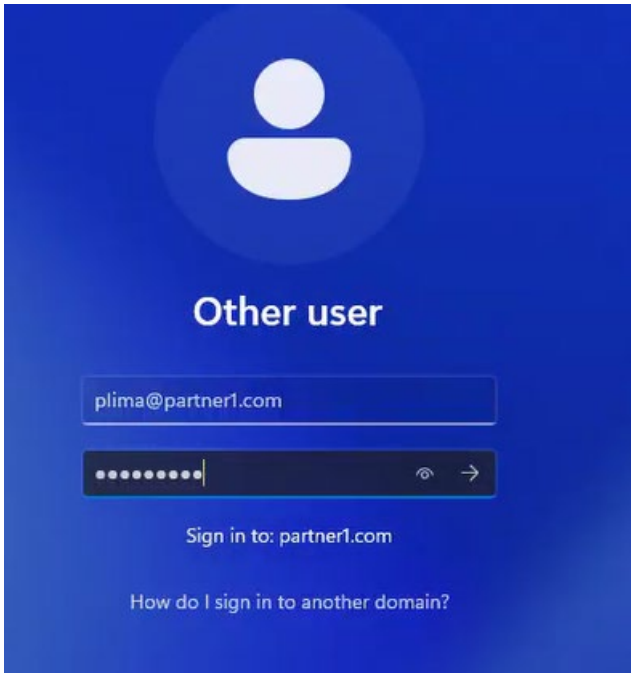
```
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> # Grant Change permissions at share level
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> Grant-SmbShareAccess -Name "Secret" -AccountName "partner1\plima" -AccessRight Change -Force

Name   ScopeName AccountName                                  AccessControlType AccessRight
----   --------- -----------                                  ----------------- -----------
Secret *         *S-1-5-21-1245985154-6628414-958437321-1107 Allow             Full
Secret *         PARTNER1\plima                               Allow             Change


[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> # Verify
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> Get-SmbShareAccess -Name "Secret" | Where-Object {$_.AccountName -like "*plima*"}

Name   ScopeName AccountName    AccessControlType AccessRight
----   --------- -----------    ----------------- -----------
Secret *         PARTNER1\plima Allow             Change


[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
```

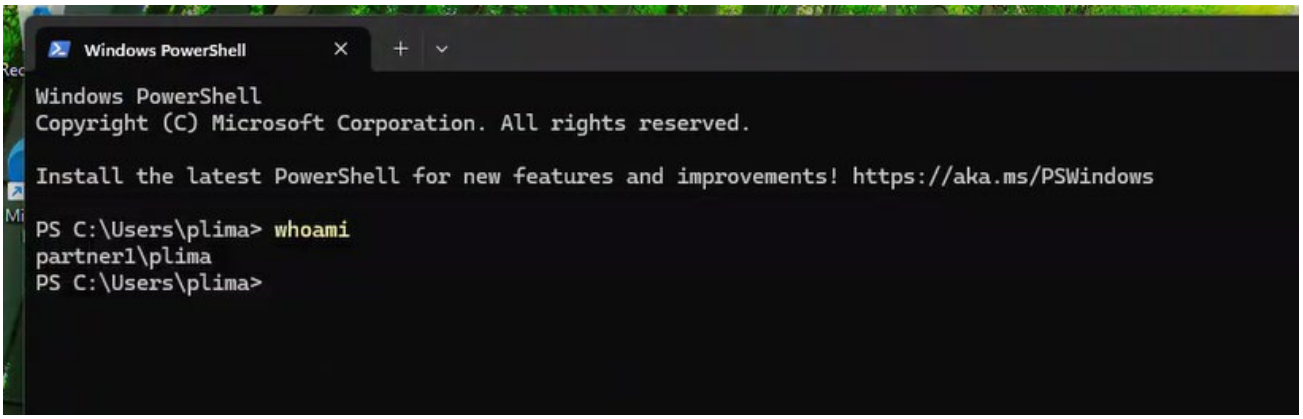
Get-SmbShareAccess -Name "Secret" | Format-List *

```
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> Get-SmbShareAccess -Name "Secret" | Format-List *


AccessControlType     : Allow
AccessRight           : Full
AccountName           : *S-1-5-21-1245985154-6628414-958437321-1107
Name                  : Secret
ScopeName             : *
PSComputerName        :
CimClass              : ROOT/Microsoft/Windows/Smb:MSFT_SmbShareAccessControlEntry
CimInstanceProperties : {AccessControlType, AccessRight, AccountName, Name...}
CimSystemProperties   : Microsoft.Management.Infrastructure.CimSystemProperties

AccessControlType     : Allow
AccessRight           : Change
AccountName           : PARTNER1\plima
Name                  : Secret
ScopeName             : *
PSComputerName        :
CimClass              : ROOT/Microsoft/Windows/Smb:MSFT_SmbShareAccessControlEntry
CimInstanceProperties : {AccessControlType, AccessRight, AccountName, Name...}
CimSystemProperties   : Microsoft.Management.Infrastructure.CimSystemProperties
```

5. **From Client1:**

   a. Log in with **Pierre Lima** from **partner1.com**





b. Map the shared folder **\\DC201\Secret** as drive **S:**

c. Test file creation and access.

 # Check mapped drives

Get-PSDrive -PSProvider FileSystem

 # Create test file

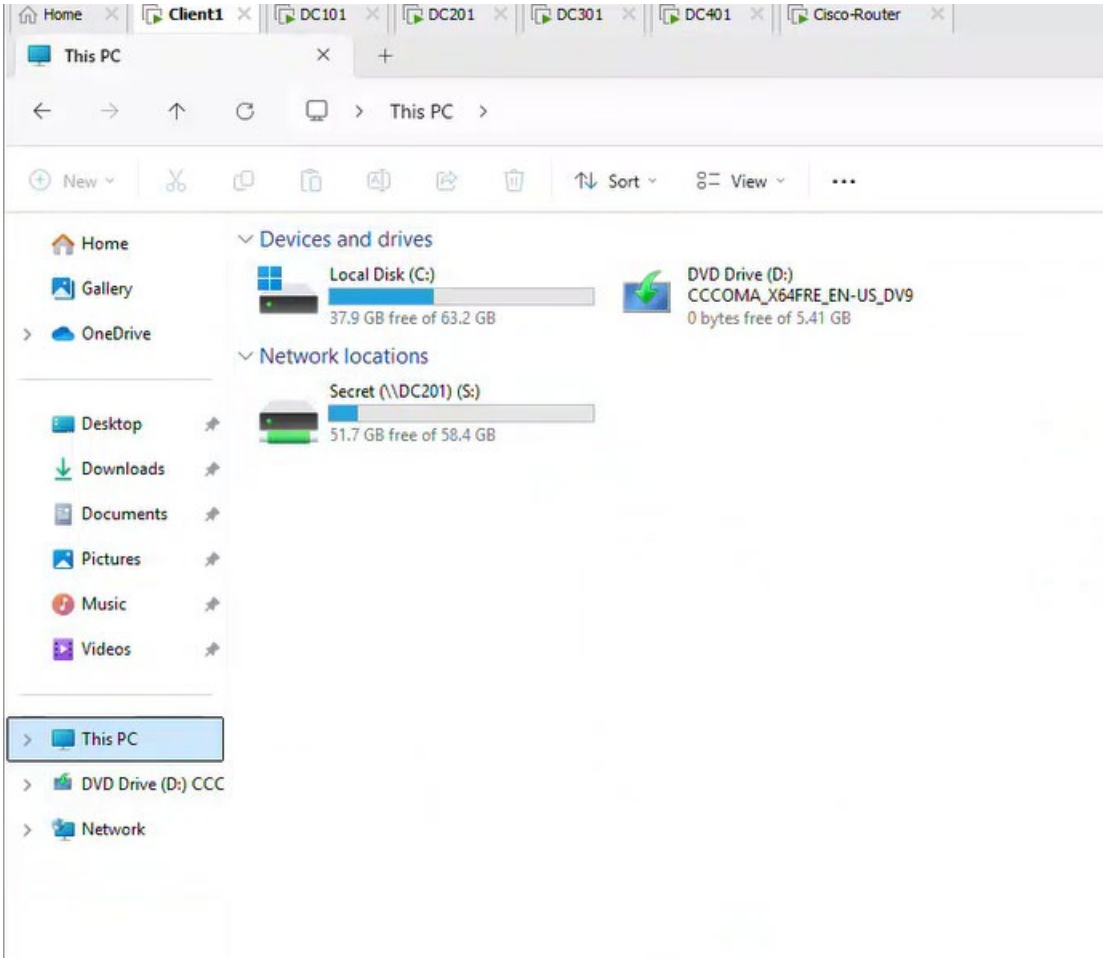
"Cross-forest test $(Get-Date)" | Out-File -FilePath S:\testfile.txt

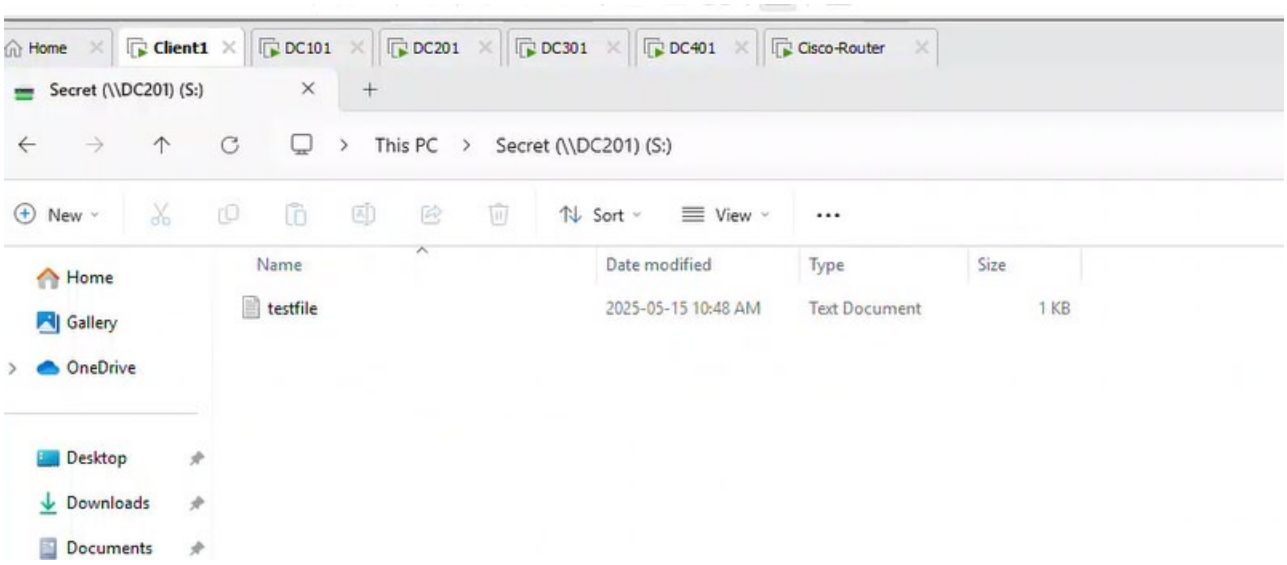
 # Verify creation

dir S:

```
PS C:\Users\plima>
PS C:\Users\plima> Get-PSDrive -PSProvider FileSystem

Name           Used (GB)     Free (GB) Provider      Root
----           ---------     --------- --------      ----
C                  25.29         37.96 FileSystem    C:\
D                   5.42          0.00 FileSystem    D:\
S                   6.65         51.80 FileSystem    \\DC201\Secret


PS C:\Users\plima> "Cross-forest test $(Get-Date)" | Out-File -FilePath S:\testfile.txt
PS C:\Users\plima> dir s:


    Directory: S:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        2025-05-15  10:48 AM             80 testfile.txt


PS C:\Users\plima> |
```

From file explorer


Home
Client1
DC101
DC201
DC301
DC401
Cisco-Router
This PC
This PC
New
Sort
View
Home
Gallery
OneDrive
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
DVD Drive (D:) CCC
Network
Devices and drives
Local Disk (C:)
37.9 GB free of 63.2 GB
DVD Drive (D:)
CCCOMA_X64FRE_EN-US_DV9
0 bytes free of 5.41 GB
Network locations
Secret (\\DC201) (S:)
51.7 GB free of 58.4 GB


Home
Client1
DC101
DC201
DC301
DC401
Cisco-Router
Secret (\\DC201) (S:)
This PC
Secret (\\DC201) (S:)
New
Sort
View
Home
Gallery
OneDrive
Desktop
Downloads
Documents
Name
Date modified
Type
Size
testfile
2025-05-15 10:48 AM
Text Document
1 KB