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

Task 1: Promote DC407 as a New Domain Controller in a New Forest

* Explanation:

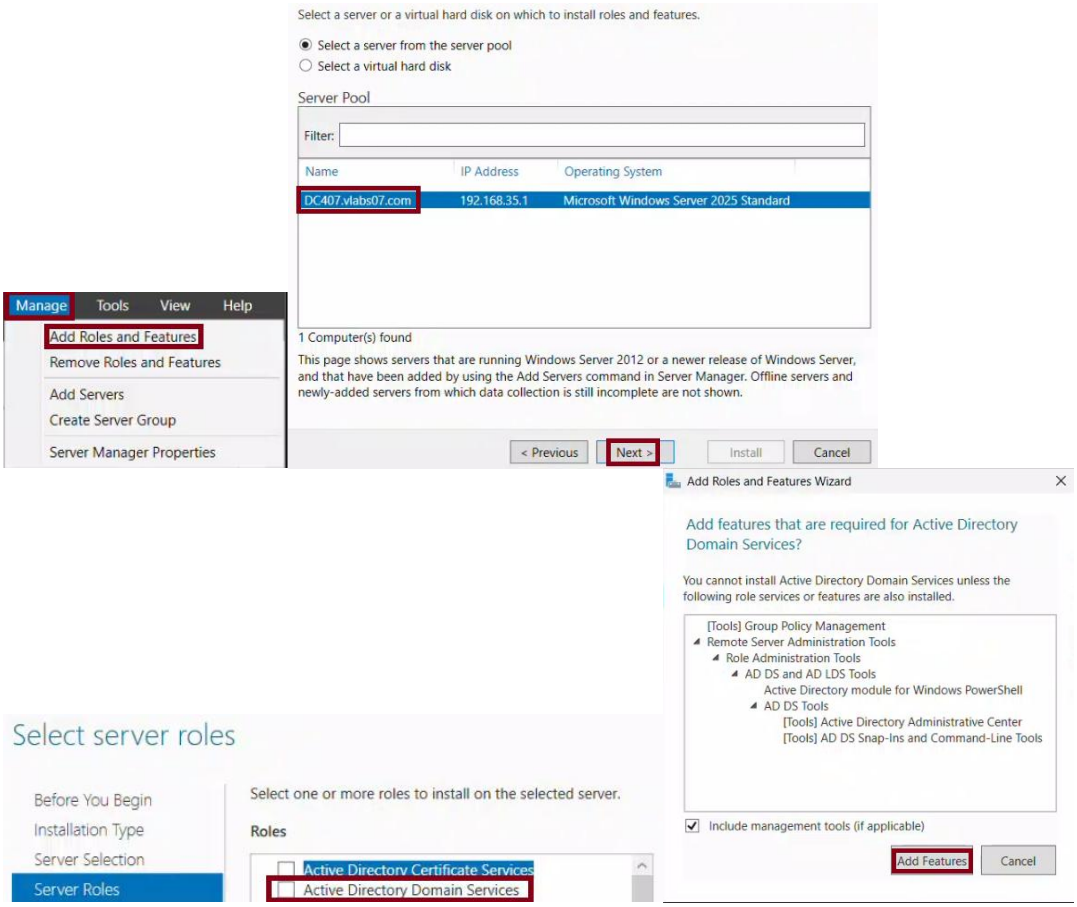
In this task, I installed the Active Directory Domain Services (AD DS) role on DC407 and promoted it as the first domain controller in a new forest called 'partner07.com'. I followed the GUI method as instructed in the lab.

* Steps Taken:

Step 1: Install AD DS Role using Server Manager

I opened Server Manager → Manage → Add Roles and Features
- Chose: Role-based or feature-based installation
- Selected: DC407
- Selected: Active Directory Domain Services (AD DS)
- Confirmed required features and proceeded with installation
- Waited for the installation to complete

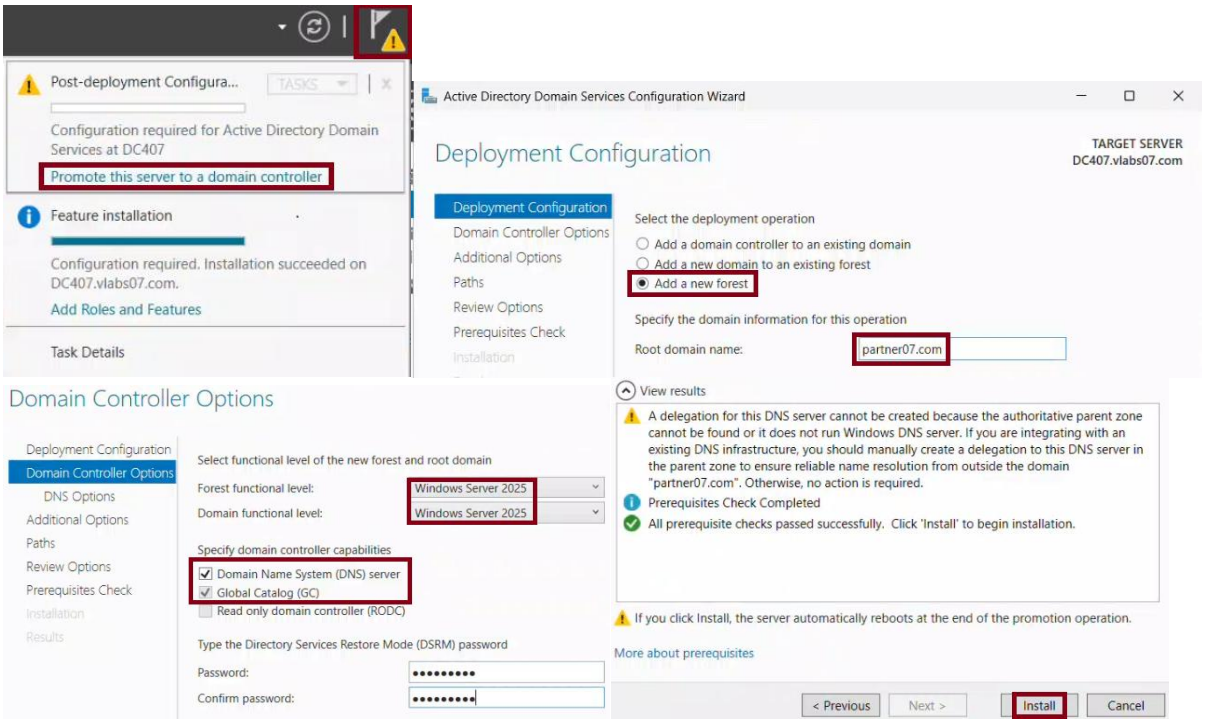
🖼 Screenshots:



Step 2: Promote DC407 to a New Forest

- Clicked on "Promote this server to a domain controller"
- Selected: Add a new forest
- Entered root domain name: partner07.com
- Chose Forest and Domain functional level: Windows Server 2025
- Ensured DNS Server was checked
- Set DSRM password
- Left NetBIOS name as default
- Accepted default folder locations for DB, logs, and SYSVOL
- Reviewed and installed
- Server restarted automatically

🖼 Screenshots:



* Verification:

After reboot, I logged in as:
Username: partner07\Administrator

I ran the following command to verify the domain:
Get-ADDomain

```
PS C:\Users\Administrator> Get-ADDomain
AllowedDNSSuffixes                : {}
ChildDomains                      : {}
ComputersContainer                : CN=Computers,DC=partner07,DC=com
DeletedObjectsContainer           : CN=Deleted Objects,DC=partner07,DC=com
DistinguishedName                 : DC=partner07,DC=com
DNSRoot                           : partner07.com
DomainControllersContainer        : OU=Domain Controllers,DC=partner07,DC=com
DomainMode                        : Windows2025Domain
DomainSID                         : S-1-5-21-2651038912-892051809-387436388
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=partner07,DC=com
Forest                            : partner07.com
InfrastructureMaster              : DC407.partner07.com
LastLogonReplicationInterval      :
LinkedGroupPolicyObjects          : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=pa
                                    rtner07,DC=com}
LostAndFoundContainer             : CN=LostAndFound,DC=partner07,DC=com
ManagedBy                         :
Name                              : partner07
NetBIOSName                       : PARTNER07
ObjectClass                       : domainDNS
ObjectGUID                        : 678ab754-b6e0-41ea-9cec-5f63ff61587e
```

Output confirmed that the domain 'partner07.com' exists and is active.

I ran the following command to verify the forest:
Get-ADForest

```
PS C:\Users\Administrator> Get-ADForest


ApplicationPartitions : {DC=DomainDnsZones,DC=partner07,DC=com, DC=ForestDnsZones,DC=partner07,DC=com}
CrossForestReferences : {}
DomainNamingMaster    : DC407.partner07.com
Domains               : {partner07.com}
ForestMode            : Windows2025Forest
GlobalCatalogs        : {DC407.partner07.com}
Name                  : partner07.com
PartitionsContainer   : CN=Partitions,CN=Configuration,DC=partner07,DC=com
RootDomain            : partner07.com
SchemaMaster          : DC407.partner07.com
Sites                 : {Default-First-Site-Name}
SPNSuffixes           : {}
UPNSuffixes           : {}
```

Output confirmed that the forest was successfully created with DC407 as the root.

** At this point, DC407 is the domain controller for a brand new forest named partner07.com. **

Task 2: Verify Domain and Forest Functional Levels

Explanation:

In this task, I verified the Domain and Forest Functional Levels for both:
- vlabs07.com (existing domain)
- partner07.com (newly created forest)

Functional levels control the AD features available across domain controllers. Higher levels support newer features but require newer OS versions.

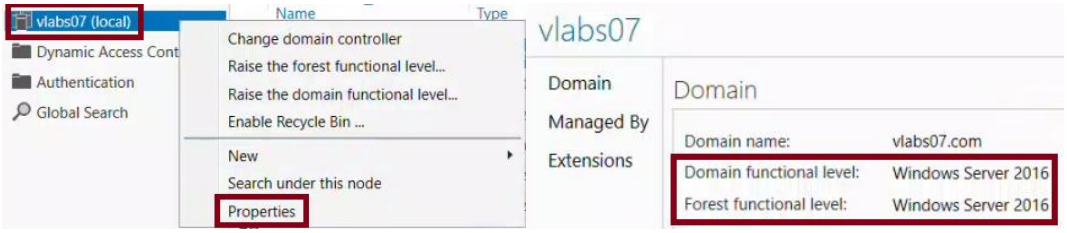
I used both GUI (ADAC) and PowerShell methods to confirm the configuration.

Steps Taken:

Step 1: On DC107 (vlabs07.com) – GUI Method

- Opened Server Manager → Tools → Active Directory Administrative Center
- In the left pane, I selected "vlabs07 (local)"
- Right-clicked on the domain "vlabs07" and selected "Properties"
- The properties window showed:
  - Domain functional level: Windows Server 2016
  - Forest functional level: Windows Server 2016

Screenshots:



Step 2: On DC1XX – PowerShell Method

```
Get-ADDomain | Select-Object Name, DomainMode
```

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

Name           DomainMode
----           ----------
vlabs07 Windows2016Domain
```

```
Get-ADForest | Select-Object Name, ForestMode
```

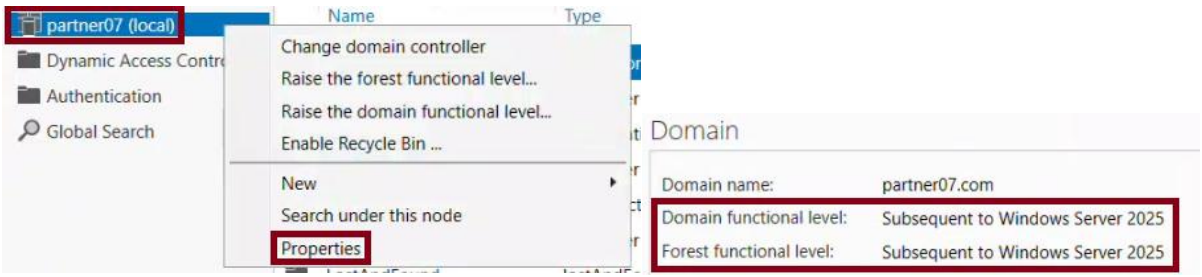
```
PS C:\Users\Administrator> Get-ADForest | Select-Object Name, ForestMode

Name               ForestMode
----               ----------
vlabs07.com Windows2016Forest
```

Step 3: On DC407 (partner07.com) – GUI Method

- Repeated the same steps in ADAC
- Right-clicked domain "partner07" → Properties
- Confirmed both functional levels were set to Windows Server 2016

Screenshots:



Step 4: On DC407 – PowerShell Method

```
Get-ADDomain | Select-Object Name, DomainMode
Get-ADForest | Select-Object Name, ForestMode
```

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

Name             DomainMode
----             ----------
partner07 Windows2025Domain


PS C:\Users\Administrator> Get-ADForest | Select-Object Name, ForestMode

Name                 ForestMode
----                 ----------
partner07.com Windows2025Forest
```

Verification:

The outputs confirmed:
- vlabs07.com is running at Windows Server 2016 domain and forest levels
- partner07.com is using Windows Server 2025 for both domain and forest

Task 3: Listing Trusts

Explanation:

In this task, I listed all the existing trust relationships on both forests:
- vlabs07.com and lab.vlabs07.com
- partner07.com

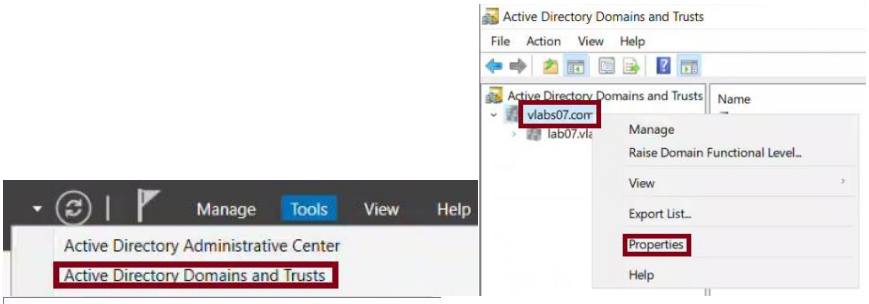
I used two methods:
1. GUI: Active Directory Domains and Trusts
2. PowerShell: Using Get-ADTrust cmdlet

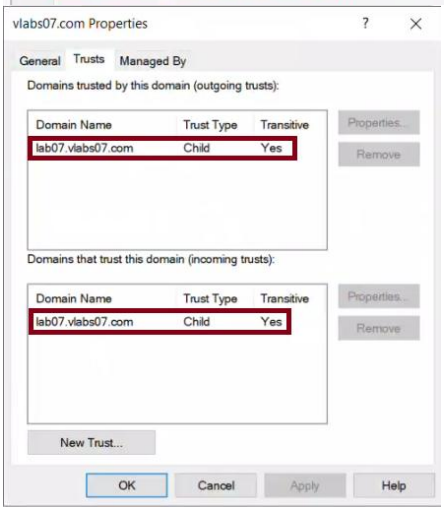
Steps Taken:

Step 1: On DC107 (vlabs07.com) – GUI Method

 - Opened Server Manager → Tools → Active Directory Domains and Trusts
 - In the left pane, I right-clicked on "vlabs07.com" and selected "Properties"
 - Switched to the "Trusts" tab
 - I saw that this domain has a default trust with its child domain: lab07.vlabs07.com

Screenshots:





Step 2: On DC107 – PowerShell Method

I ran the following command:

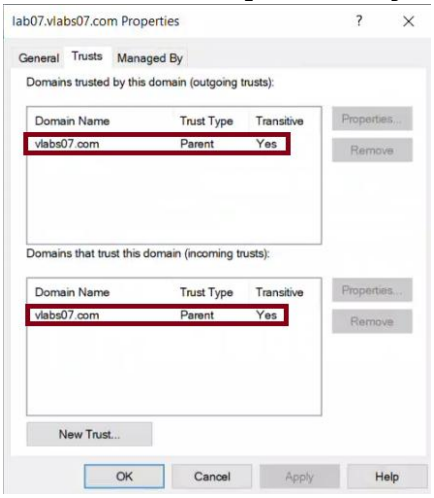
```
Get-ADTrust -Filter * | Select-Object Name, Target, TrustType, Direction
```

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

Name              Target            TrustType     Direction
----              ------            ---------     ---------
lab07.vlabs07.com lab07.vlabs07.com   Uplevel BiDirectional
```

Step 3: On DC307 (lab.vlabs07.com) – GUI and PowerShell

- Repeated the same steps **using** AD Domains and Trusts
- Confirmed any existing trust with the parent domain vlabs07.com



- Ran:

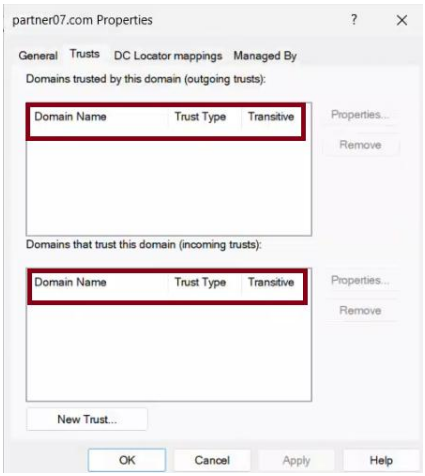
```
Get-ADTrust -Filter * | Select-Object Name, Target, TrustType, Direction
```

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

Name         Target       TrustType     Direction
----         ------       ---------     ---------
vlabs07.com vlabs07.com   Uplevel BiDirectional
```

Step 4: On DC407 (partner07.com) - GUI Method

- Opened AD Domains and Trusts
- Right-clicked on "partner07.com" → Properties → Trusts tab
- Confirmed that no trusts were yet established



Step 5: On DC407 - PowerShell Method

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

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

▨ Verification:

All commands confirmed that no trust relationships had been created yet.
This matches the lab instructions, since the trust will be configured in Task 4.

Task 4: Creating Trusts

Explanation:

In this task, I configured DNS Conditional Forwarders so that both domains can resolve each others names. Then, I created a two-way transitive forest trust between vlabs07.com and partner07.com. I used PowerShell where instructed, and GUI where specified.

Steps Taken:

Step 1: On DC107 – Add Conditional Forwarder for partner07.com (using PowerShell)

I used the IP address of the domain controller for partner07.com (DC407):
Add-DnsServerConditionalForwarderZone -Name "partner07.com" -MasterServers 192.168.35.1 -ReplicationScope Forest

```
PS C:\Users\Administrator> Add-DnsServerConditionalForwarderZone -Name "partner07.com" -MasterS
ervers 192.168.35.1 -ReplicationScope Forest
```

Step 2: Verify Forwarder on DC107

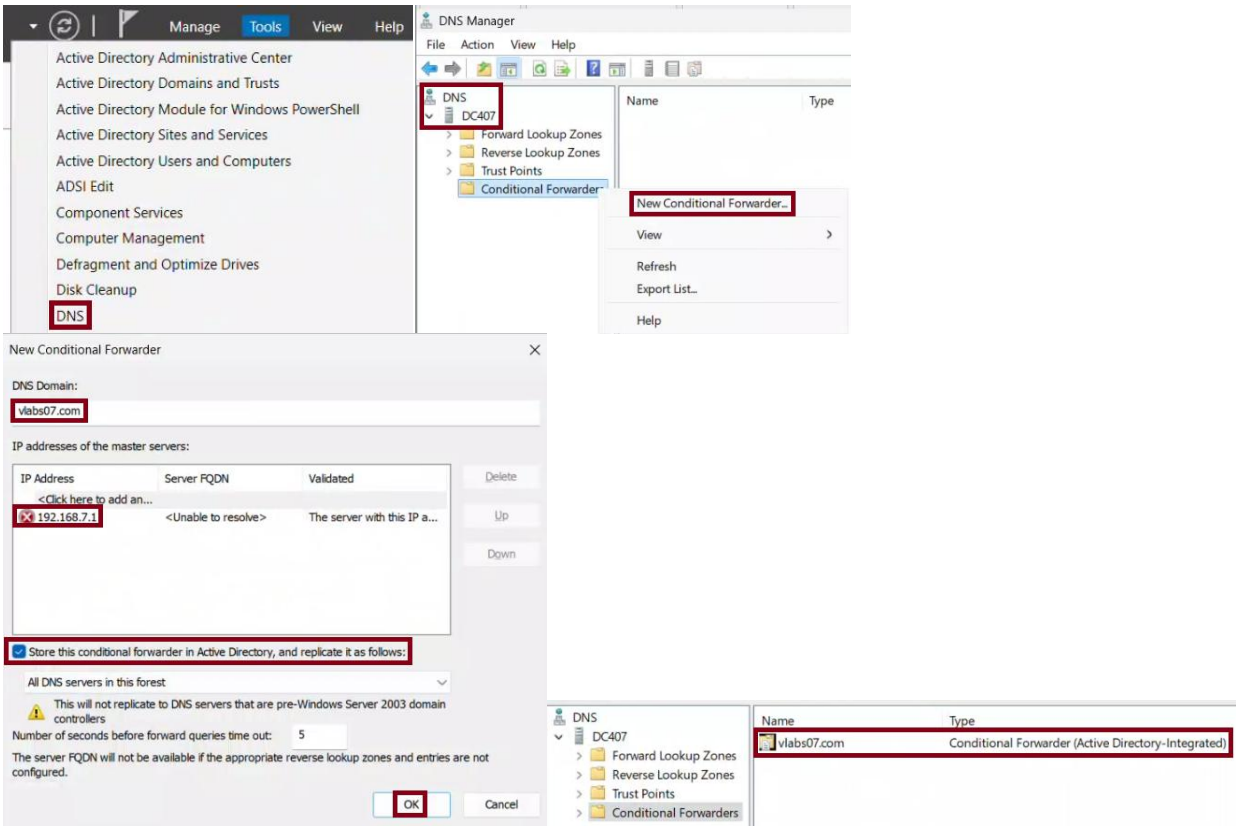
I ran nslookup from DC107 to ensure partner07.com names could be resolved:
nslookup partner07.com

```
PS C:\Users\Administrator> nslookup partner07.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Non-authoritative answer:
Name:    partner07.com
Address:  192.168.35.1
```

Step 3: On DC407 – Add Conditional Forwarder for vlabs07.com (using GUI)

- Opened Server Manager → Tools → DNS
- Expanded DC407 → Right-clicked on "Conditional Forwarders" → New Conditional Forwarder
- Entered domain: vlabs07.com
- Added IP: 192.168.7.1 (IP of DC107)
- Checked: "Store this conditional forwarder in Active Directory" (forest-wide)
- Clicked OK



Step 4: Verify Forwarder on DC407

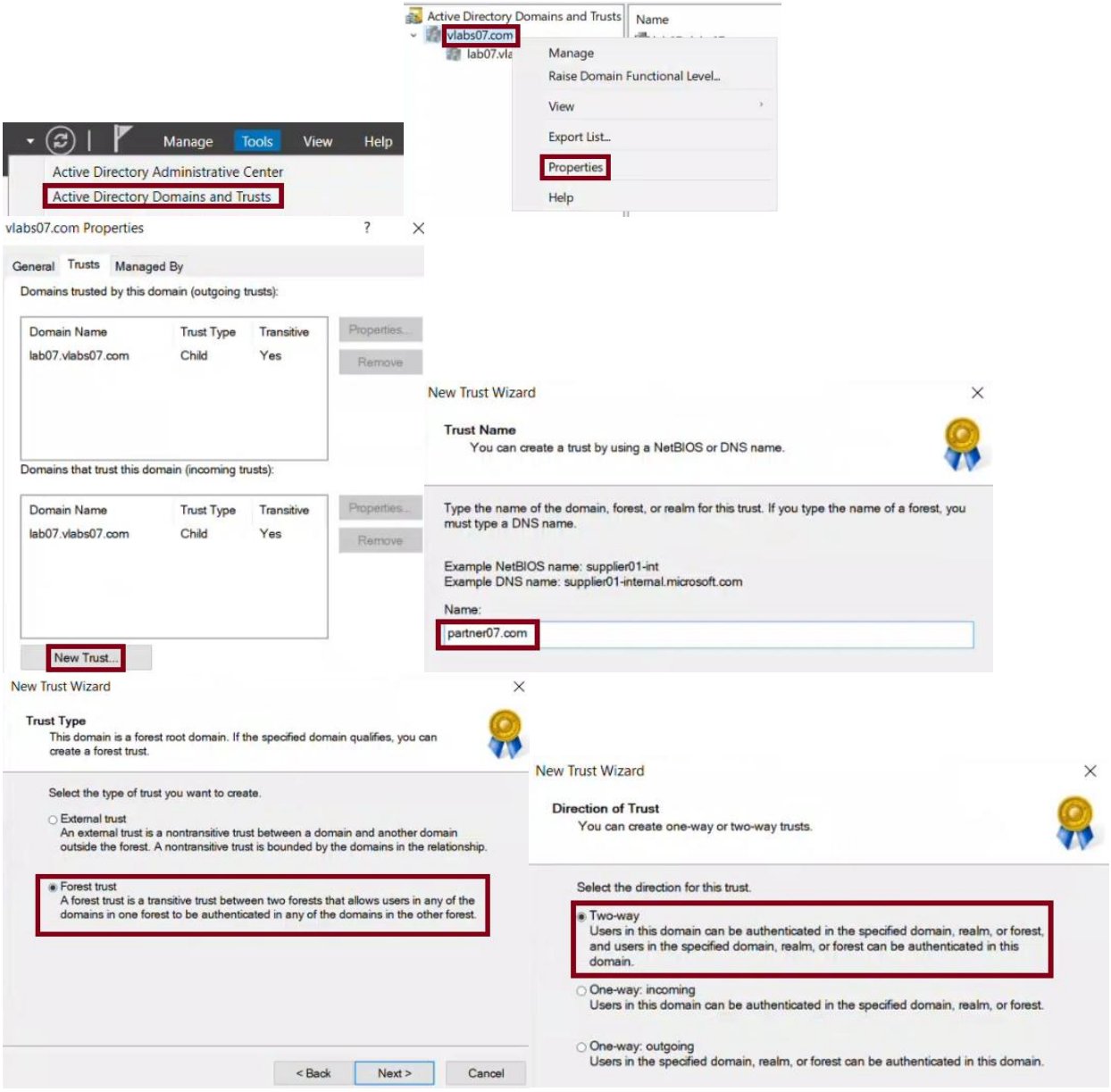
From DC407, I ran:
nslookup vlabs07.com

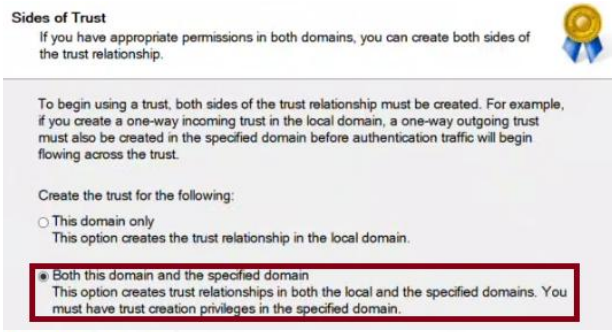
```
PS C:\Users\Administrator> nslookup vlabs07.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Non-authoritative answer:
Name:    vlabs07.com
Address:  192.168.7.1
```

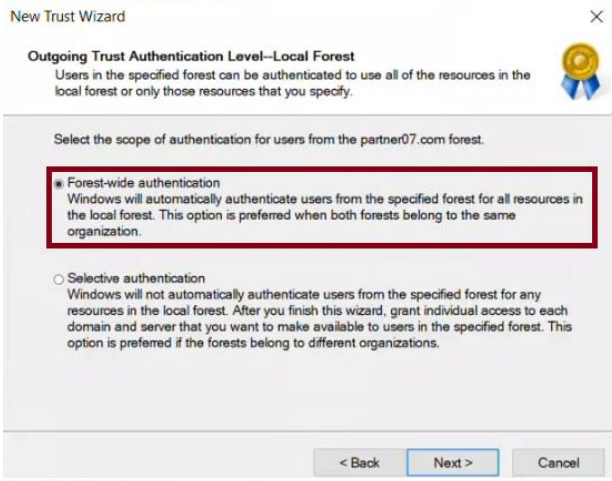
Step 5: On DC107 – Create Two-Way Forest Trust (GUI)

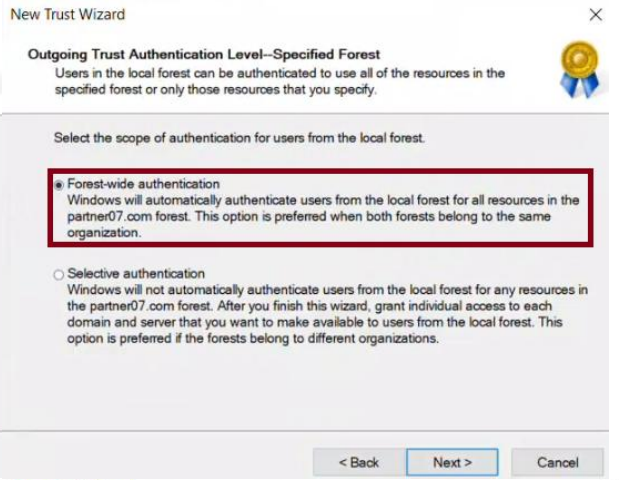
- Opened Active Directory Domains and Trusts
- Right-clicked vlabs07.com → Properties → Trusts tab → New Trust
- Trust name: partner07.com
- Selected: Forest Trust → Two-way → Both this domain and the specified domain
- Entered credentials for partner07\Administrator when prompted
- Verified trust was successfully created

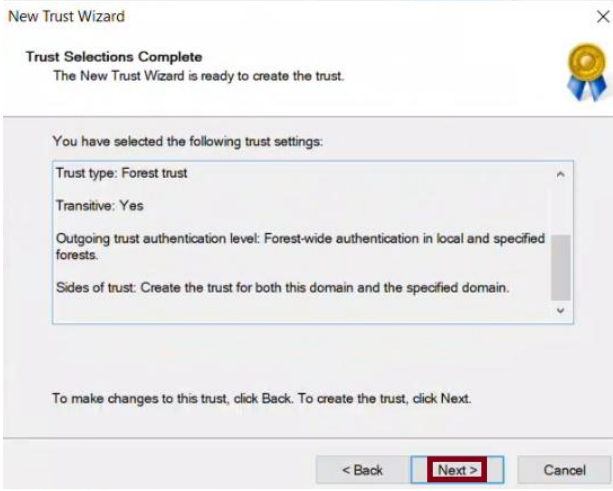


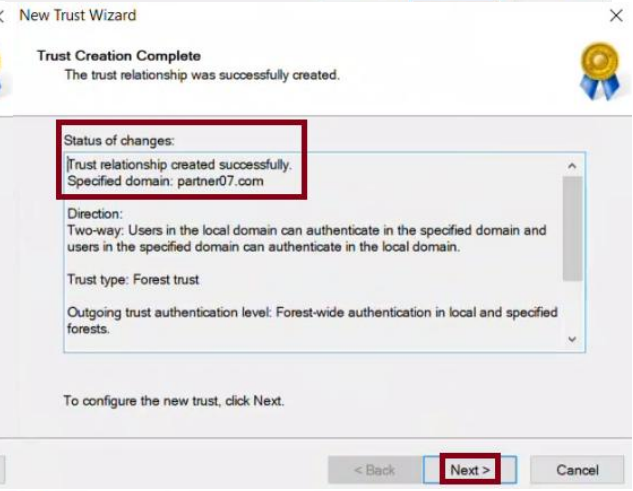

Sides of Trust
If you have appropriate permissions in both domains, you can create both sides of the trust relationship.
To begin using a trust, both sides of the trust relationship must be created. For example, if you create a one-way incoming trust in the local domain, a one-way outgoing trust must also be created in the specified domain before authentication traffic will begin flowing across the trust.
Create the trust for the following:
This domain only
This option creates the trust relationship in the local domain.
Both this domain and the specified domain
This option creates trust relationships in both the local and the specified domains. You must have trust creation privileges in the specified domain.

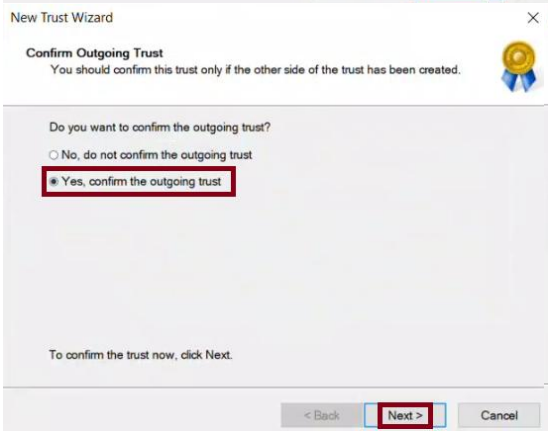

New Trust Wizard
User Name and Password
To create this trust relationship, you must have administrative privileges for the specified domain.
Specified domain: partner07.com
Type the user name and password of an account that has administrative privileges in the specified domain.
User name:
administrator@partner07.com
Password:

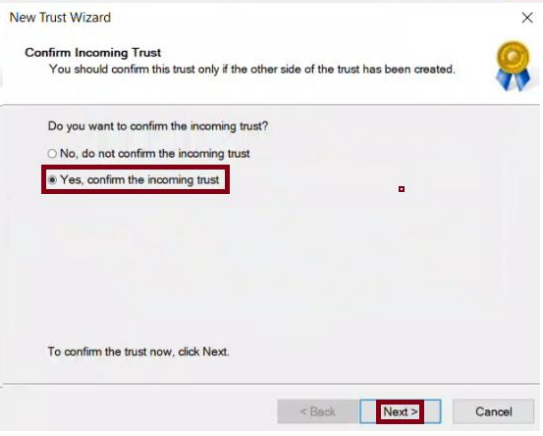

New Trust Wizard
Outgoing Trust Authentication Level--Local Forest
Users in the specified forest can be authenticated to use all of the resources in the local forest or only those resources that you specify.
Select the scope of authentication for users from the partner07.com forest.
Forest-wide authentication
Windows will automatically authenticate users from the specified forest for all resources in the local forest. This option is preferred when both forests belong to the same organization.
Selective authentication
Windows will not automatically authenticate users from the specified forest for any resources in the local forest. After you finish this wizard, grant individual access to each domain and server that you want to make available to users in the specified forest. This option is preferred if the forests belong to different organizations.
< Back
Next >
Cancel


New Trust Wizard
Outgoing Trust Authentication Level--Specified Forest
Users in the local forest can be authenticated to use all of the resources in the specified forest or only those resources that you specify.
Select the scope of authentication for users from the local forest.
Forest-wide authentication
Windows will automatically authenticate users from the local forest for all resources in the partner07.com forest. This option is preferred when both forests belong to the same organization.
Selective authentication
Windows will not automatically authenticate users from the local forest for any resources in the partner07.com forest. After you finish this wizard, grant individual access to each domain and server that you want to make available to users from the local forest. This option is preferred if the forests belong to different organizations.
< Back
Next >
Cancel


New Trust Wizard
Trust Selections Complete
The New Trust Wizard is ready to create the trust.
You have selected the following trust settings:
Trust type: Forest trust
Transitive: Yes
Outgoing trust authentication level: Forest-wide authentication in local and specified forests.
Sides of trust: Create the trust for both this domain and the specified domain.
To make changes to this trust, click Back. To create the trust, click Next.
< Back
Next >
Cancel


New Trust Wizard
Trust Creation Complete
The trust relationship was successfully created.
Status of changes:
Trust relationship created successfully.
Specified domain: partner07.com
Direction:
Two-way: Users in the local domain can authenticate in the specified domain and users in the specified domain can authenticate in the local domain.
Trust type: Forest trust
Outgoing trust authentication level: Forest-wide authentication in local and specified forests.
To configure the new trust, click Next.
< Back
Next >
Cancel


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
To confirm the trust now, click Next.
< Back
Next >
Cancel


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

Step 6: On DC407 – Verify and Complete Trust Setup (GUI)

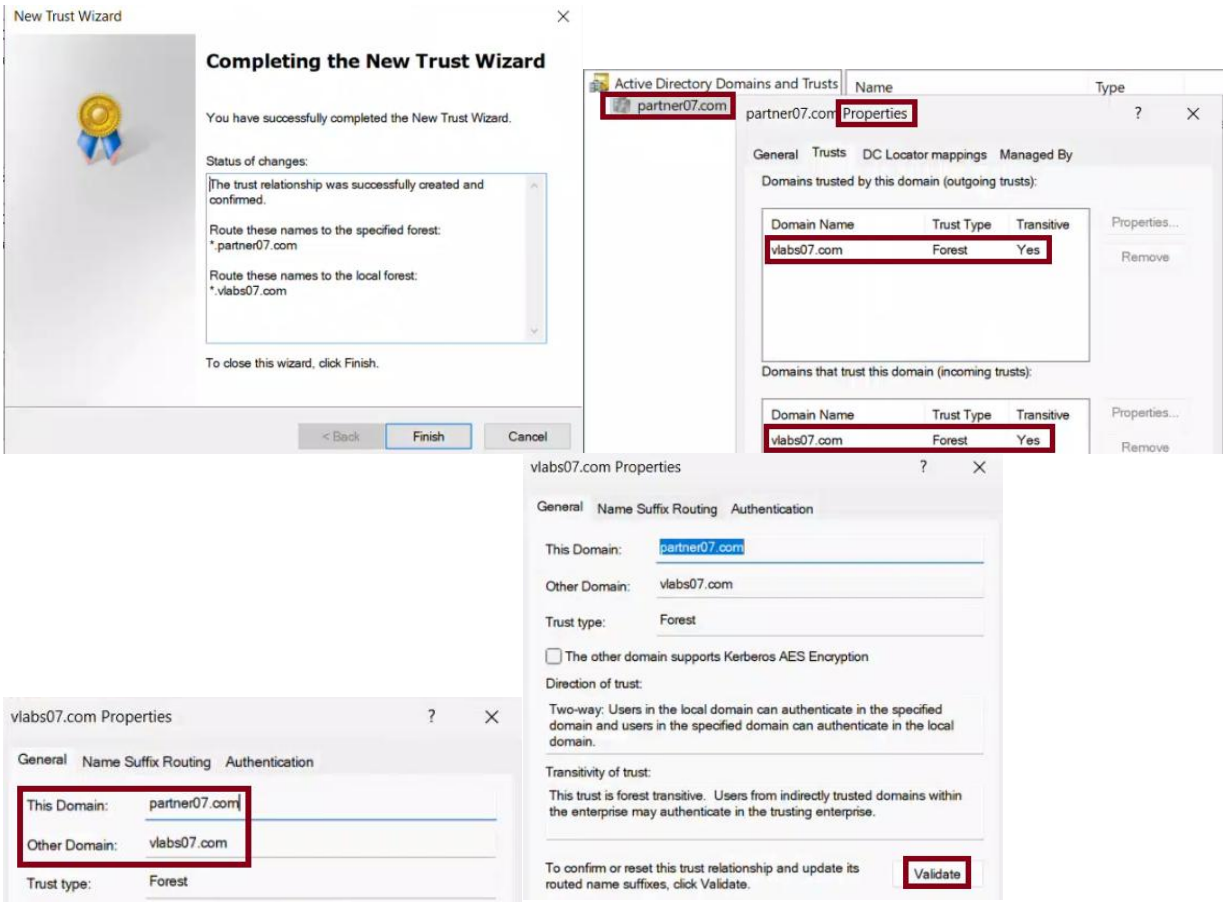
- Opened **Active Directory Domains and Trusts** on DC407.
- Right-clicked **partner07.com** → Selected **Properties** → Navigated to the **Trusts** tab.
- Verified that **vlabs07.com** trust appeared in the list.
- Checked that the status was **"Trusted"** and properties matched the intended configuration.

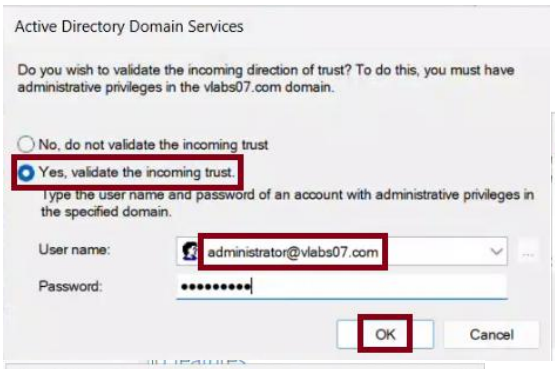
- Selected the **vlabs07.com** trust entry → Clicked **Properties** → Clicked **Validate**.
- In the trust validation prompt:
    - Chose **"Yes, validate the incoming trust"**.
    - Entered credentials for **vlabs07\administrator**.

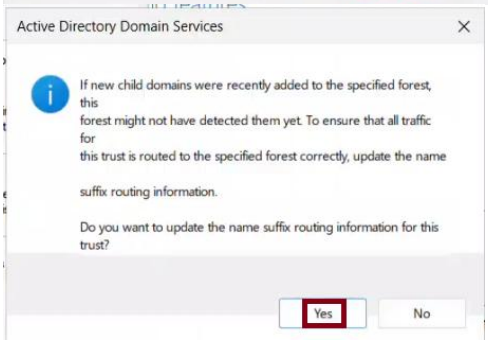
- A pop-up appeared prompting to update name suffix routing:
    - Clicked **Yes** to ensure routing of authentication requests for any child domains.

- Validation completed successfully with the message:
    "The trust between vlabs07.com and partner07.com has been successfully verified."

📸 Screenshot:







Step 7: Verify Trust Using PowerShell on Both Servers

Explanation:
To confirm that the two-way transitive forest trust between vlabs07.com and partner07.com is fully functional, I used PowerShell and Netdom to verify the trust status from both ends.

Actions Performed:

---

1. On **DC107 (vlabs07.com)**:
   - Ran the following command to verify the trust:
     netdom trust /d:partner07.com vlabs07.com /uo:vlabs07\administrator /ud:partner07\administrator /pd:* /po:* /verify /verbose

```
PS C:\Users\Administrator> netdom trust /d:partner07.com vlabs07.com /uo:vlabs07\administrator
/ud:partner07\administrator /pd:* /po:* /verify /verbose
The trust between vlabs07.com and partner07.com has been successfully verified

Deleting the session with \\DC407.partner07.com

Deleting the session with \\DC107.vlabs07.com

The command completed successfully.
PS C:\Users\Administrator> Get-ADTrust -Filter * | Select-Object Name, Target, TrustType, Direc
tion

Name             Target           TrustType     Direction
----             ------           ---------     ---------
lab07.vlabs07.com lab07.vlabs07.com   Uplevel BiDirectional
partner07.com     partner07.com       Uplevel BiDirectional
```

2. On **DC407 (partner07.com)**:
   - Ran the matching verification command:
     netdom trust /d:vlabs07.com partner07.com /uo:partner07\administrator /ud:vlabs07\administrator /pd:* /po:* /verify /verbose

```
PS C:\Users\Administrator> netdom trust /d:vlabs07.com partner07.com /uo:partner07\administrato
r /ud:vlabs07\administrator /pd:* /po:* /verify /verbose
The trust between partner07.com and vlabs07.com has been successfully verified

Deleting the session with \\DC107.vlabs07.com

Deleting the session with \\DC407.partner07.com

The command completed successfully.
PS C:\Users\Administrator> Get-ADTrust -Filter * | Select-Object Name, Target, TrustType, Direc
tion

Name        Target      TrustType     Direction
----        ------      ---------     ---------
vlabs07.com vlabs07.com   Uplevel BiDirectional
```

Results:

- On both systems, the command returned:
  "The trust between vlabs07.com and partner07.com has been successfully verified."
- No errors were reported.
- Trust is fully operational and secured with bidirectional authentication.

Task 5: Testing Trust Between Two Forests

System: DC407 (partner07.com), DC207 (vlabs07.com – RODC), Client07

🛠️ Objective:
To confirm that the trust is working, a user from the partner07.com forest will access shared resources in the vlabs07.com domain using their credentials.

Step 1: Create a User in partner07.com (on DC407)

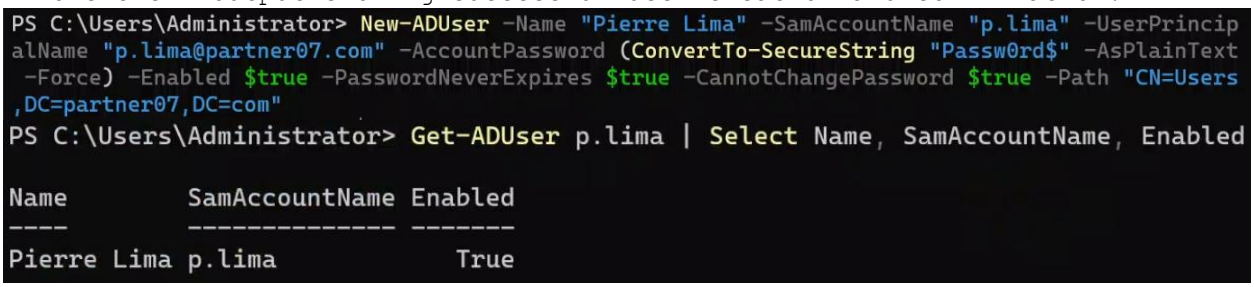
Create a new user account "Pierre Lima" with the username "p.lima"

```
New-ADUser
    -Name "Pierre Lima"
    -SamAccountName "p.lima"
    -UserPrincipalName "p.lima@partner07.com"
    -AccountPassword (ConvertTo-SecureString "Passw0rd$" -AsPlainText -Force)
`
    -Enabled $true
    -PasswordNeverExpires $true
    -CannotChangePassword $true
    -Path "CN=Users,DC=partner07,DC=com"
```

Confirm the user was created:

```
Get-ADUser plima | Select Name, SamAccountName, Enabled
```

📸 Screenshot:
- PowerShell output showing successful user creation and confirmation.



Step 2: Share Folder on DC207 (vlabs07.com – RODC)

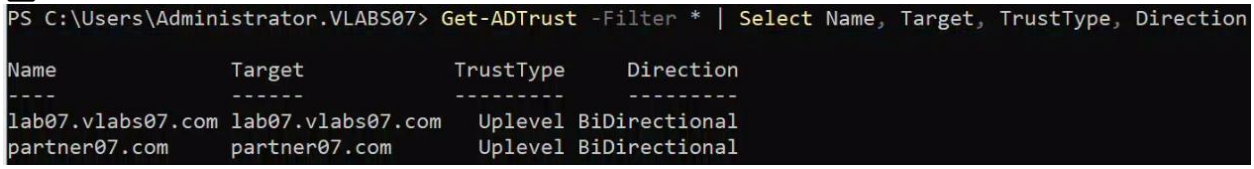
System: DC207 (vlabs07.com – RODC)

Verify the trust relationship with partner07.com

Check that a trust with partner07.com exists and is bidirectional:

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

📸 Screenshot:



◇ Create a new folder at C:\Secret

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

📸 Screenshot:

```
PS C:\Users\Administrator.VLABS07> New-Item -Path "C:\Secret" -ItemType Directory


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/15/2025  10:51 AM                Secret
```

◇ Create SMB Share and Grant Share Permissions

Create the SMB share (initial share creation without assigning access yet)

```
New-SmbShare -Name "Secret" -Path "C:\Secret"
```

📸 Screenshot:

```
PS C:\Users\Administrator.VLABS07> New-SmbShare -Name "Secret" -Path "C:\Secret"
```

Grant share-level permissions with Change (Read/Write) access to the remote user from partner07.com

```
Grant-SmbShareAccess -Name "Secret" -AccountName "partner07\p.lima" -
AccessRight Change -Force
```

📸 Screenshot:

```
PS C:\Users\Administrator.VLABS07> Grant-SmbShareAccess -Name "Secret" -AccountName "partner07\p.lima"
-AccessRight Change -Force

Name   ScopeName AccountName      AccessControlType AccessRight
----   --------- -----------      ----------------- -----------
Secret *         PARTNER07\p.lima Allow             Change
```

```
# Note: The lab instructions mention assigning permissions to p.laurin,
# but since only p.lima was created in Step 1, all permissions were applied
to that user instead.
```

◇ Set NTFS permissions

*Get current NTFS permissions (ACL) on the folder
This stores the current access control settings for C:\Secret in the $acl variable

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

📸 Screenshot:

```
PS C:\Users\Administrator.VLABS07> $acl = Get-Acl "C:\Secret"
```

*Create a new permission rule for partner07\p.lima
This rule grants Modify (Read/Write) permission, inheritable by subfolders and files

```
$rule = New-Object System.Security.AccessControl.FileSystemAccessRule(
    "partner07\p.lima", "Modify", "ContainerInherit,ObjectInherit", "None",
"Allow"
)
```

📸 Screenshot:

```
PS C:\Users\Administrator.VLABS07> $rule = New-Object System.Security.AccessControl.FileSystemAccessRul
e("partner07\p.lima", "Modify", "ContainerInherit,ObjectInherit", "None", "Allow")
```

*Add the new rule to the ACL object
This updates the ACL in memory by adding the rule for partner07\p.lima

```
$acl.AddAccessRule($rule)
```

📸 Screenshot:

```
PS C:\Users\Administrator.VLABS07> $acl.AddAccessRule($rule)
```

*Apply the updated ACL back to the folder
This writes the new permission settings to the actual folder on disk

```
Set-Acl -Path "C:\Secret" -AclObject $acl
```

📸 Screenshot:

```
PS C:\Users\Administrator.VLABS07> Set-Acl -Path "C:\Secret" -AclObject $acl
```

*Verify Share and NTFS Permissions Before Proceeding

Confirm the SMB share exists

```
Get-SmbShare -Name "Secret"
```

📸 Screenshot:

```
PS C:\Users\Administrator.VLABS07> Get-SmbShare -Name "Secret"

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

*Confirm the share access permissions

```
Get-SmbShareAccess -Name "Secret"
```

📸 Screenshot:

```
PS C:\Users\Administrator.VLABS07> Get-SmbShareAccess -Name "Secret"

Name   ScopeName AccountName      AccessControlType AccessRight
----   --------- -----------      ----------------- -----------
Secret *         PARTNER07\p.lima Allow             Change
```

*Confirm NTFS (file system) permissions for the user
This command retrieves all access control entries (ACEs) for C:\Secret
and filters the results to show only those related to "p.lima"

```
(Get-Acl "C:\Secret").Access | Where-Object { $_.IdentityReference -like
"*p.lima*" }
```

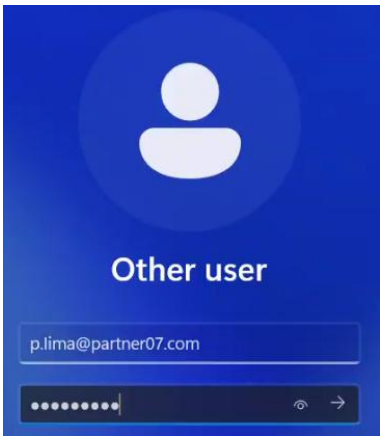
📸 Screenshot:

```
PS C:\Users\Administrator.VLABS07> (Get-Acl "C:\Secret").Access | Where-Object { $_.IdentityReference
like "*p.lima*" }


FileSystemRights  : Modify, Synchronize
AccessControlType : Allow
IdentityReference : PARTNER07\p.lima
IsInherited       : False
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags  : None
```

Step 3: Test Access from Client07

Log in to Client07 as:
Username: p.lima@partner07.com
Password: Passw0rd$
📸 Screenshot:



◇ Map the shared folder as a network drive (Drive S:)

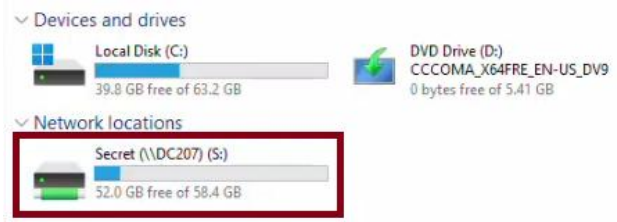
Command:
```
New-PSDrive -Name "S" -PSProvider "FileSystem" -Root "\\DC207\Secret" -Persist
```

Explanation:
- New-PSDrive: Creates a new logical drive (like a mapped network drive).
- -Name "S": This assigns drive letter S: to the mapped location.
- -PSProvider "FileSystem": Tells PowerShell youre mapping a file system drive.
- -Root "\\DC207\Secret": The network path to the shared folder created earlier.
- -Persist: Makes the drive visible in File Explorer and survive reboots (like GUI mapping).

📸 Screenshot:

```
PS C:\Users\p.lima> New-PSDrive -Name "S" -PSProvider "FileSystem" -Root "\\DC207\Secret" -Persist

Name           Used (GB)     Free (GB) Provider      Root                                               CurrentLocation
----           ---------     --------- --------      ----                                               ---------------
S                   6.35         52.10 FileSystem    \\DC207\Secret
```



◇ Create a test file in the shared folder to verify write access

Command:
```
New-Item -Path "S:\testfile.txt" -ItemType "File"
```

Explanation:
- New-Item: Creates a new file or folder.
- -Path "S:\testfile.txt": The full path to the new file inside the mapped drive.
- -ItemType "File": Specifies that a file should be created (not a folder or shortcut).

📸 Screenshot:

```
PS C:\Users\p.lima> New-Item -Path "S:\testfile.txt" -ItemType "File"


    Directory: S:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/15/2025   9:53 AM              0 testfile.txt
```