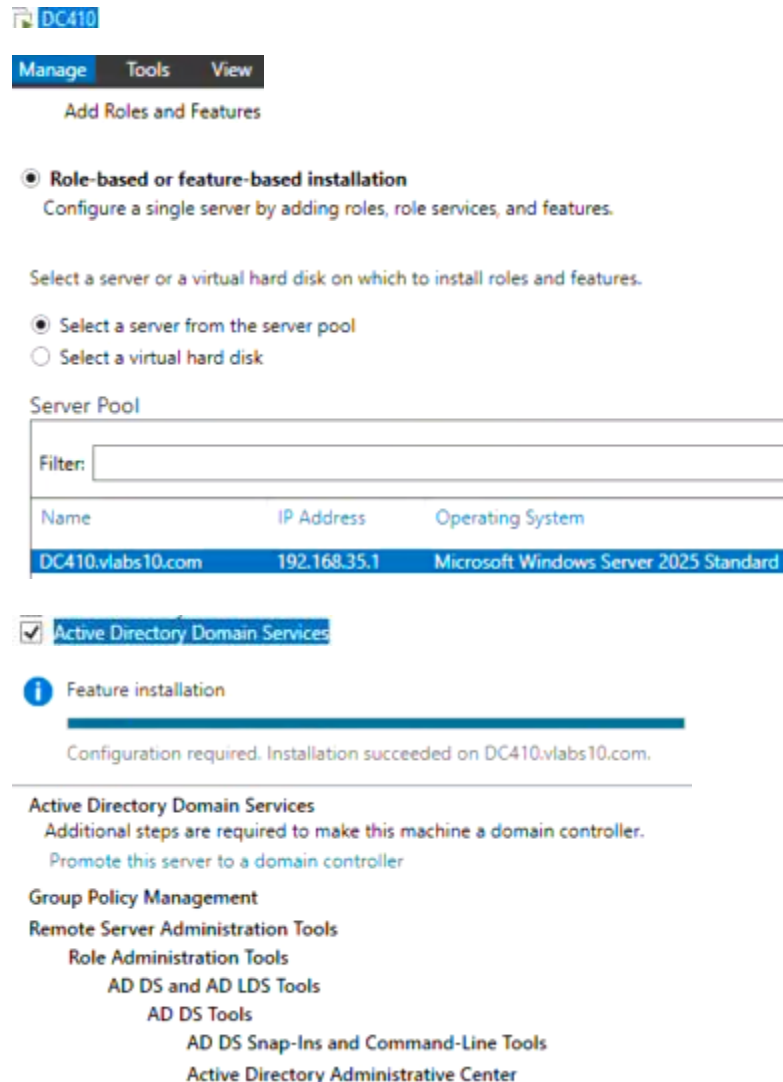


Lab Assignment (Part 1) – Managing AD Domains, Forests, and Trusts

Task 1: Promote DC4XX as a New Domain Controller in a New Forest

1. Promote DC4XX as a new DC in a New Forest named partnerXX.com using GUI
- Install AD DS role on DC4XX.



DC410

Manage Tools View

Add Roles and Features

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

Name	IP Address	Operating System
DC410.vlabs10.com	192.168.35.1	Microsoft Windows Server 2025 Standard

Filter:

☒ **Active Directory Domain Services**

i Feature installation

Configuration required. Installation succeeded on DC410.vlabs10.com.

Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller

Group Policy Management

Remote Server Administration Tools

Role Administration Tools

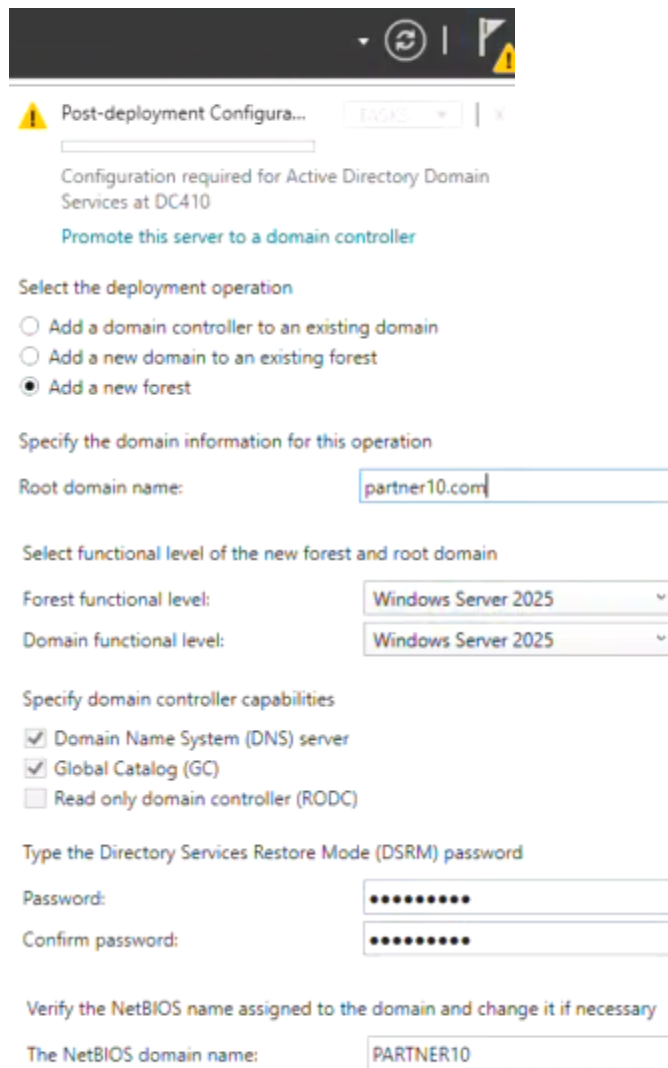
 AD DS and AD LDS Tools

 AD DS Tools

 AD DS Snap-Ins and Command-Line Tools

 Active Directory Administrative Center

- Create a new forest partnerXX.com.



The screenshot shows the 'Post-deployment Configuration Wizard' for Active Directory Domain Services. The title bar includes a 'TASKS' dropdown and a close button. The main window has a yellow warning icon and the text 'Configuration required for Active Directory Domain Services at DC410'. A link 'Promote this server to a domain controller' is visible. Under 'Select the deployment operation', the 'Add a new forest' radio button is selected. The 'Specify the domain information for this operation' section shows 'Root domain name' as 'partner10.com'. The 'Select functional level of the new forest and root domain' section shows both 'Forest functional level' and 'Domain functional level' set to 'Windows Server 2025'. The 'Specify domain controller capabilities' section has 'Domain Name System (DNS) server' and 'Global Catalog (GC)' checked, while 'Read only domain controller (RODC)' is unchecked. The 'Type the Directory Services Restore Mode (DSRM) password' section has two password fields, both masked with dots. The 'Verify the NetBIOS name assigned to the domain and change it if necessary' section shows 'The NetBIOS domain name' as 'PARTNER10'.

Post-deployment Configura... TASKS | X

Configuration required for Active Directory Domain Services at DC410

[Promote this server to a domain controller](#)

Select the deployment operation

☐ Add a domain controller to an existing domain

☐ Add a new domain to an existing forest

☒ Add a new forest

Specify the domain information for this operation

Root domain name: partner10.com

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2025

Domain functional level: Windows Server 2025

Specify domain controller capabilities

☒ Domain Name System (DNS) server

☒ Global Catalog (GC)

☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:

Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name: PARTNER10

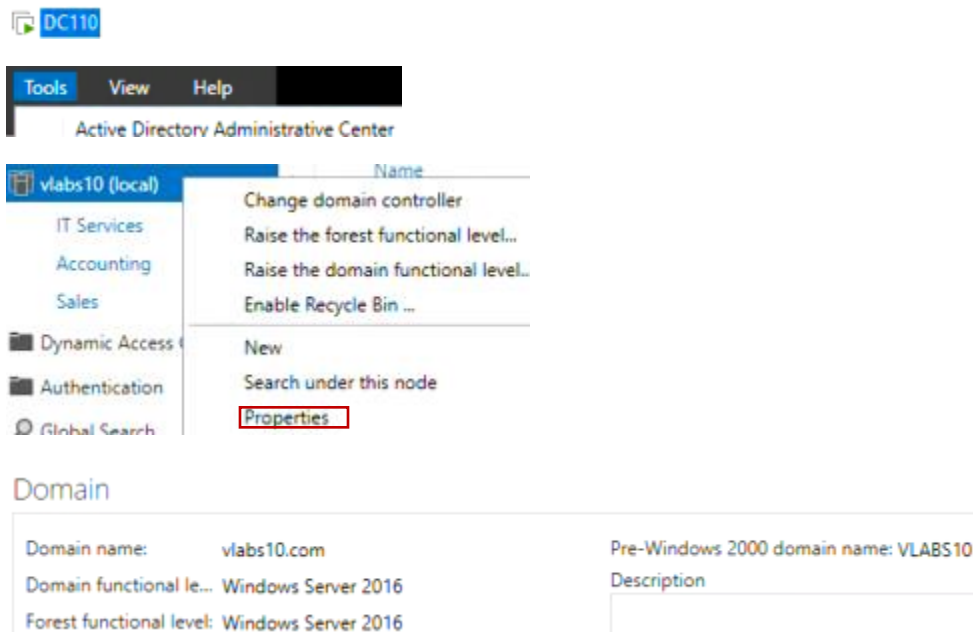




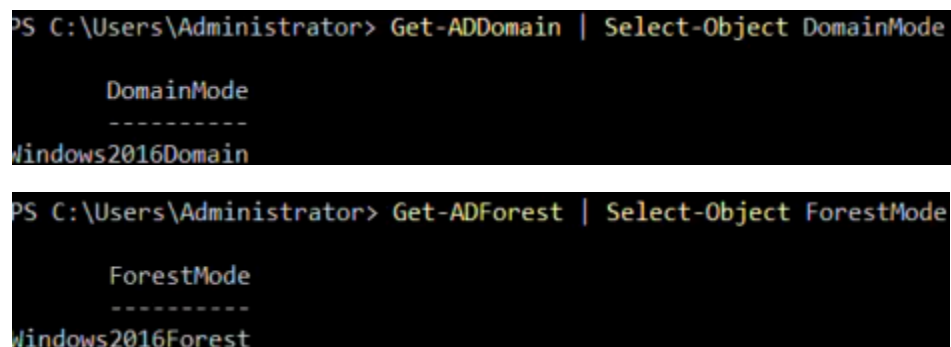
Task 2: Verify Domain and Forest Functional Levels

1. Check the Domain and Forest Functional Levels on vlabsXX.com

- Using Active Directory Administrative Center



- Using PowerShell

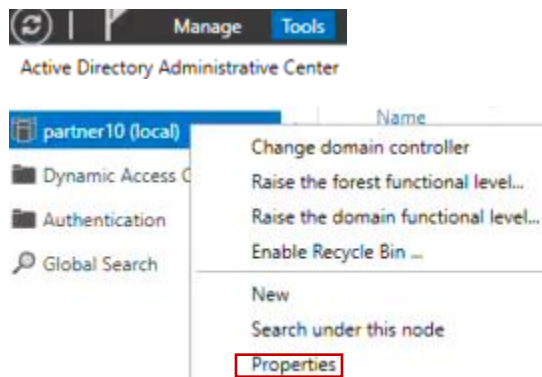


Task 2: Verify Domain and Forest Functional Levels

2. Check the Domain and Forest Functional Levels on partnerXX.com

- Using Active Directory Administrative Center





Domain

Domain name:	partner10.com	Pre-Windows 2000 domain name: PARTNER10
Domain functional level:	Subsequent to Windows Server 2025	Description
Forest functional level:	Subsequent to Windows Server 2025	

- Using PowerShell

```
PS C:\Users\Administrator.SRV110> Get-ADDomain | Select-Object DomainMode

DomainMode
-----
Windows2025Domain
```

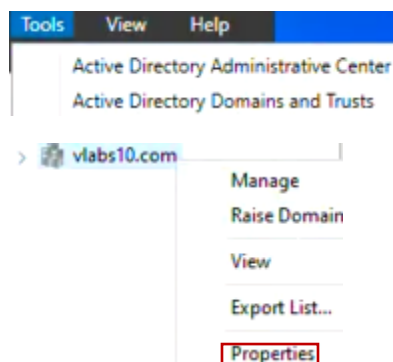
```
PS C:\Users\Administrator.SRV110> Get-ADForest | Select-Object ForestMode

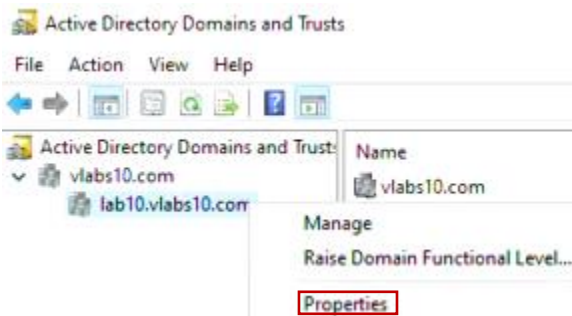
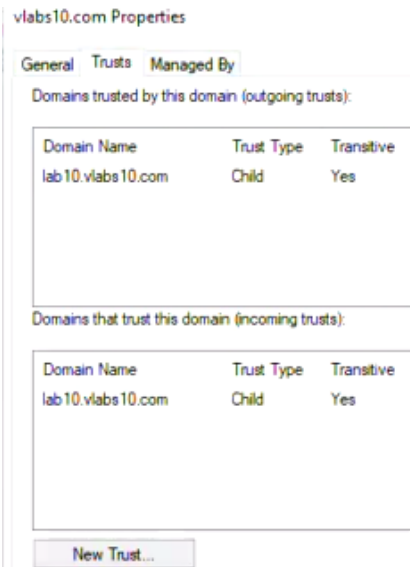
ForestMode
-----
Windows2025Forest
```

Task 3: Listing Trusts

1. List all Trusts on vlabsXX.com and labsXX.vlabsXX.com

- Using Active Directory Domains and Trusts.





- Using PowerShell.

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

Name	Target	TrustType	Direction
lab10.vlabs10.com	lab10.vlabs10.com	Uplevel BiDirectional	

2. List all Trusts on partnerXX.com

- Using Active Directory Domains and Trusts.



- Using PowerShell.

```
PS C:\Users\Administrator.SRV110> Get-ADTrust -Filter * | Select-Object Name, Target, TrustType, Direction
```

Task 4: Creating Trusts

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

- On the DNS server of DC1XX create a Conditional Forwarder for partnerXX.com using PowerShell

```
PS C:\Users\Administrator> Add-DnsServerConditionalForwarderZone -Name "partner10.com" -MasterServers 192.168.35.1 -ReplicationScope Forest
```

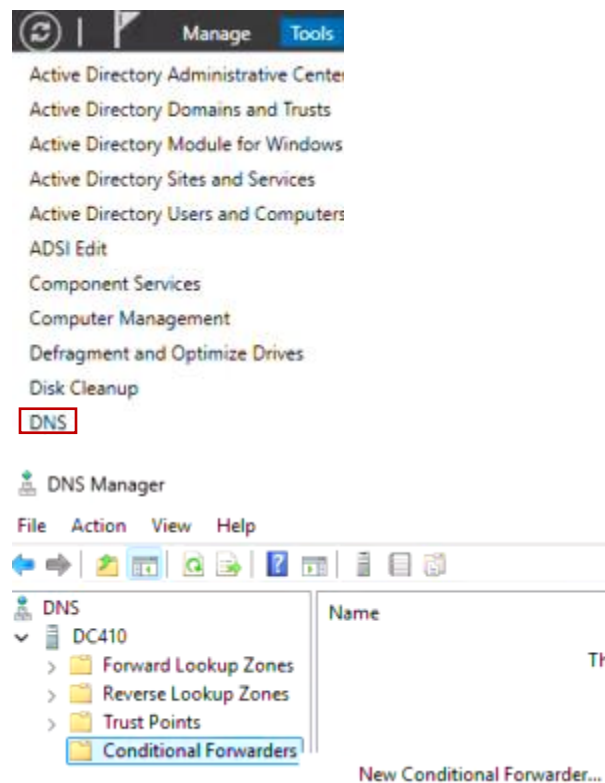
- Verify using nslookup.

```
PS C:\Users\Administrator> nslookup partner10.com
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: ::1

Non-authoritative answer:
Name:   partner10.com
Address: 192.168.35.1
```

- On the DNS server of DC4XX create a Conditional Forwarder for vlabsXX.com using GUI

DC410



New Conditional Forwarder

DNS Domain:

vlabs10.com

IP addresses of the master servers:

IP Address	Server FQDN
192.168.10.1	

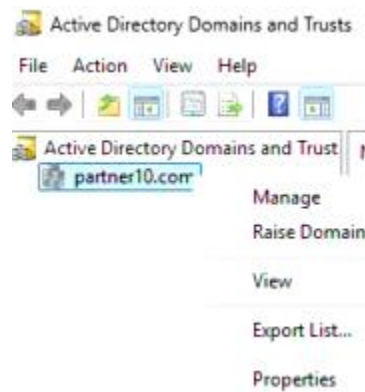
- Verify using nslookup.

```
PS C:\Users\Administrator.SRV110> nslookup vlabs10.com
DNS request timed out.
    timeout was 2 seconds.
Server:      UnKnown
Address:     ::1

Name:   vlabs10.com
Address: 192.168.10.1
```

2. Using GUI:

- Create a Two-Way Transitive Forest Trust between vlabsXX.com and partnerX.com



partner10.com Properties

General Trusts DC Locator mappings Managed By

Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive

New Trust...

New Trust Wizard



Trust Name

You can create a trust by using a NetBIOS or DNS name.



Type the name of the domain, forest, or realm for this trust. If you type the name of a forest, you must type a DNS name.

Example NetBIOS name: supplier01-int

Example DNS name: supplier01-internal.microsoft.com

Name:

vlabs10.com]

New Trust Wizard



Trust Type

This domain is a forest root domain. If the specified domain qualifies, you can create a forest trust.



Select the type of trust you want to create.

☐ External trust

An external trust is a nontransitive trust between a domain and another domain outside the forest. A nontransitive trust is bounded by the domains in the relationship.

☒ Forest trust

A forest trust is a transitive trust between two forests that allows users in any of the domains in one forest to be authenticated in any of the domains in the other forest.

Direction of Trust

You can create one-way or two-way trusts.



Select the direction for this trust.

- ☒ **Two-way**
Users in this domain can be authenticated in the specified domain, realm, or forest, and users in the specified domain, realm, or forest can be authenticated in this domain.
- ☐ **One-way: incoming**
Users in this domain can be authenticated in the specified domain, realm, or forest.
- ☐ **One-way: outgoing**
Users in the specified domain, realm, or forest can be authenticated in this domain.

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.

User Name and Password

To create this trust relationship, you must have administrative privileges for the specified domain.



Specified domain: vlabs10.com

Type the user name and password of an account that has administrative privileges in the specified domain.

User name:

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 vlabs10.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.

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 vlabs10.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 vlabs10.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.

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

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

partner10.com Properties

General Trusts DC Locator mappings Managed By

Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
vlabs10.com	Forest	Yes

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
vlabs10.com	Forest	Yes

New Trust...

3. Using PowerShell:

- Verify the Trust Status on both Servers.

DC110

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

Name	Target	TrustType	Direction
lab10.vlabs10.com	lab10.vlabs10.com	Uplevel	BiDirectional
partner10.com	partner10.com	Uplevel	BiDirectional

DC410

```
PS C:\Users\Administrator.SRV110> Get-ADTrust -Filter * | Select-Object Name, Target, TrustType, Direction
```

Name	Target	TrustType	Direction
vlabs10.com	vlabs10.com	Uplevel	BiDirectional

Task 5: Testing Trust Between Two Forests

1. On DC4XX.partnerXX.com:

- Create a new user in partnerXX.com → Pierre Lima / Passw0rd\$

Active Directory Administrative Center

« partner10 (local) »

Active Directory... < partner10 (local) (13)

Filter

Overview

partner10 (local) >

Dynamic Access Control >

Authentication >

Global Search

Name

Keys

LostAndFound

Managed Service Accou

NTDS Quotas

Program Data

System

TPM Devices

Users

New >

Delete

Search under this node

InetOrgPerson

Group

User

Create User: Pierre Lima

TASKS >

SECTIONS >

Account

Organization

Member Of

Password Settings

Profile

Policy

Silo

Account

First name: Pierre

Middle initials:

Last name: Lima

Full name: * Pierre Lima

User UPN logon: plima @ partner10.com

User SamAccountNam... partner10 * plima

Password: *****

Confirm password: *****

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...

☒ Password never expires

☐ User cannot change password

Expiration options:

2. On DC2XX.vlabsXX.com (Windows Server Core, RODC):
- Verify the trust relationship with partnerXX.com using PowerShell.



```
PS C:\Users\Administrator.VLABS10> Get-ADTrust -Filter {Name -eq "partner10.com"}

Direction           : BiDirectional
DisallowTransitivity : False
DistinguishedName    : CN=partner10.com,CN=System,DC=vlabs10,DC=com
ForestTransitive     : True
IntraForest          : False
IsTreeParent         : False
IsTreeRoot           : False
Name                 : partner10.com
ObjectClass           : trustedDomain
ObjectGUID           : 83bb2a3f-81c6-4a51-b38d-16d391fb2d99
SelectiveAuthentication : False
SIDFilteringForestAware : False
SIDFilteringQuarantined : False
Source               : DC=vlabs10,DC=com
Target               : partner10.com
TGTDlegation         : False
TrustAttributes      : 8
TrustedPolicy        :
TrustingPolicy       :
TrustType            : Uplevel
UplevelOnly          : False
UsesAESKeys          : False
UsesRC4Encryption    : False
```

```
PS C:\Users\Administrator.VLABS10> Get-ADTrust -Identity "partner10.com" | Format-List *

Direction           : BiDirectional
DisallowTransitivity : False
DistinguishedName    : CN=partner10.com,CN=System,DC=vlabs10,DC=com
ForestTransitive     : True
IntraForest          : False
IsTreeParent         : False
IsTreeRoot           : False
Name                 : partner10.com
ObjectClass           : trustedDomain
ObjectGUID           : 83bb2a3f-81c6-4a51-b38d-16d391fb2d99
SelectiveAuthentication : False
SIDFilteringForestAware : False
SIDFilteringQuarantined : False
Source               : DC=vlabs10,DC=com
Target               : partner10.com
TGTDlegation         : False
TrustAttributes      : 8
TrustedPolicy        :
TrustingPolicy       :
TrustType            : Uplevel
UplevelOnly          : False
UsesAESKeys          : False
UsesRC4Encryption    : False
PropertyNames        : (Direction, DisallowTransitivity, DistinguishedName, ForestTransitive...)
AddedProperties       : {}
RemovedProperties     : {}
ModifiedProperties    : {}
PropertyCount        : 23
```

- Create a folder C:\Secret

```
PS C:\Users\Administrator.VLABS10> New-Item -Path "C:\Secret" -ItemType Directory -Force

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----          5/14/2025   8:29 PM             Secret
```

- Share C:\Secret and assign permissions Read/Write to plima@partnerX.com.

```
PS C:\Users\Administrator.VLABS10> New-SmbShare -Name "Secret" -Path "C:\Secret" -FullAccess "plima@partner10.com"
```

Name	ScopeName	Path	Description
Secret	*	C:\Secret	

- Verify the shared folder and NTFS permissions.

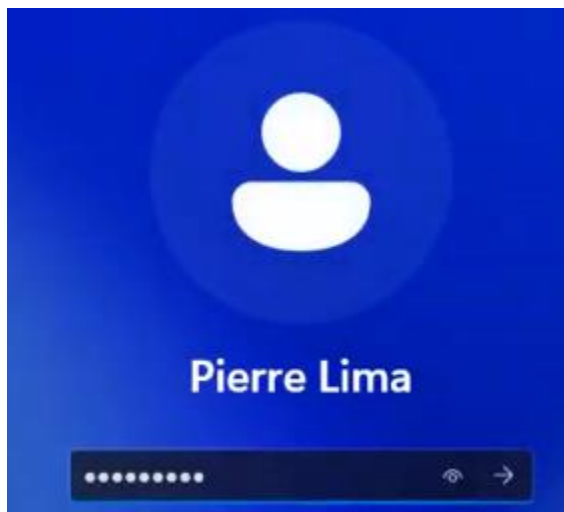
```
PS C:\Users\Administrator.VLABS10> Get-SmbShareAccess -Name "Secret"
```

Name	ScopeName	AccountName	AccessControlType	AccessRight
Secret	*	PARTNER10\plima	Allow	Full

3. From ClientXX:

- Log in with Pierre Lima from partnerXX.com

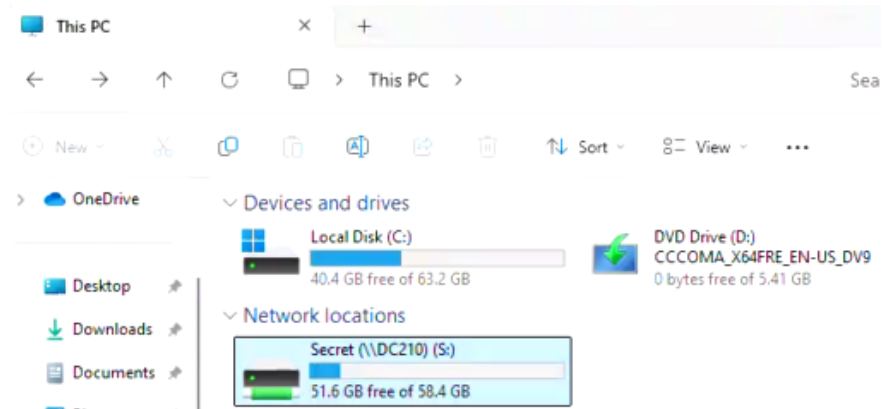
Client10



- Map the shared folder \\DC2XX\Secret as drive S:


```
PS C:\Users\plima> New-PSDrive -Name S -PSProvider FileSystem -Root "\\DC210\Secret" -Persist
```

Name	Used (GB)	Free (GB)	Provider	Root
S	6.81	51.64	FileSystem	\\DC210\Secret



- Test file creation and access.

