



This lab focuses on deploying and configuring multiple domain controllers to establish and manage an Active Directory environment.

## Lab 3 - Deploying Domain Controllers

420-636-AB-Network  
Installation and Administration  
II

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

## Table of Contents

|       |  |    |
|-------|--|----|
| 1     | Lab 3 - Deploying Domain Controllers.....  | 4  |
| 1.1   | Objective.....   | 4  |
| 2     | Topology .....   | 4  |
| 3     | Step 1: Configure DC101 (Primary Domain Controller) .....  | 0  |
| 3.1   | Before starting <b>DC101</b> , remove the network card <b>NAT then start the server.</b> .....         | 0  |
| 3.2   | Using Server Manager, install Active Directory Domain Services (AD DS).....                            | 1  |
| 3.3   | Promote <b>DC101</b> to a Domain Controller in a new Forest: <b>vlabs1.com</b> .....                   | 9  |
| 4     | Step 2: Join Client1 to the Domain .....   | 21 |
| 4.1   | Join Client1 to the vlabs1.com Domain. ....  | 21 |
| 4.2   | Login with the domain <b>administrator</b> to test it. ....  | 25 |
| 5     | Step 3: Configure DC201 as a Domain Controller Replica for vlabs1.com.....                             | 26 |
| 5.1   | Promote DC201 as DC for vlabs1.com (Not Global Catalog). ....  | 27 |
| 5.1.1 | Add a RODC(Core) to an existing domain .....   | 27 |
| 5.1.2 | Verifying the RODC Installation.....   | 28 |
| 6     | Step 4: Deploy DC301 as a Child Domain (lab1.vlabs1.com) using PowerShell.....                         | 40 |
| 6.1   | Using PowerShell, promote DC301 as a Child Domain for lab1.vlabs1.com. ....                            | 40 |
| 6.2   | Verify the Child Domain Setup.....   | 42 |
| 6.2.1 | In DC301 .....   | 42 |
| 6.2.2 | AD ON DC101 .....  | 44 |
| 7     | Step 5: Validate All Domain Controllers.....   | 47 |
| 7.1   | Check All Domain Controllers in AD.....  | 47 |
| 7.2   | DC101 .....  | 47 |
| 7.2.1 | Check All Domain Controllers in Active Directo .....   | 47 |
| 7.2.2 | Check FSMO role holders .....  | 47 |
| 7.2.3 | Validate replication health .....  | 48 |
| 7.2.4 | Test AD Tools (Active Directory Users and Computers, AD Sites & Services, AD PowerShell Commands)..... | 49 |
| 7.3   | DC201 .....  | 53 |
| 7.3.1 | Check All Domain Controllers in Active Directo .....   | 53 |
| 7.3.2 | Check FSMO role holders .....  | 54 |
| 7.3.3 | Validate replication health .....  | 54 |

|  |    |
|--|----|
| 7.3.4 Test AD Tools (Active Directory Users and Computers, AD Sites & Services, AD PowerShell Commands)..... | 56 |
| 7.1 DC301.....   | 59 |
| 7.1.1 Check All Domain Controllers in Active Directo .....   | 59 |
| 7.1.2 Check FSMO role holders .....  | 59 |
| 7.1.3 Validate replication health .....  | 60 |
| 7.1.4 Test Commands .....  | 61 |
| 8 Test AD Tools (Active Directory Users and Computers, AD Sites & Services, AD PowerShell Commands).....     | 65 |
| 9 Lab Deliverables .....   | 69 |
| 9.1 DC101: Domain Controller setup verification.....   | 69 |
| 9.2 DC201 (RODC) .....   | 70 |
| 9.2.1 Successful RODC promotion.....   | 70 |
| 9.2.2 Verify if the server is a Domain Controller.....   | 71 |
| 9.2.3 Check if the server is an RODC .....   | 71 |
| 9.2.4 In Server DC101 .....  | 71 |
| 9.2.5 repadmin /showrepl results.....  | 72 |
| 9.2.6 List of AD objects from RODC.....  | 72 |
| 9.3 DC301 (Child Domain Controller): Confirmation of lab1.vlabs1.com. ....                                   | 77 |
| 9.3.1 Confirmation of lab1.vlabs1.com .....  | 77 |
| 9.3.2 Get-ADDomain -Identity "labX.vlabsX.com".....  | 78 |
| 9.3.3 List of AD objects of this domain.....   | 78 |

# 1 Lab 3 - Deploying Domain Controllers

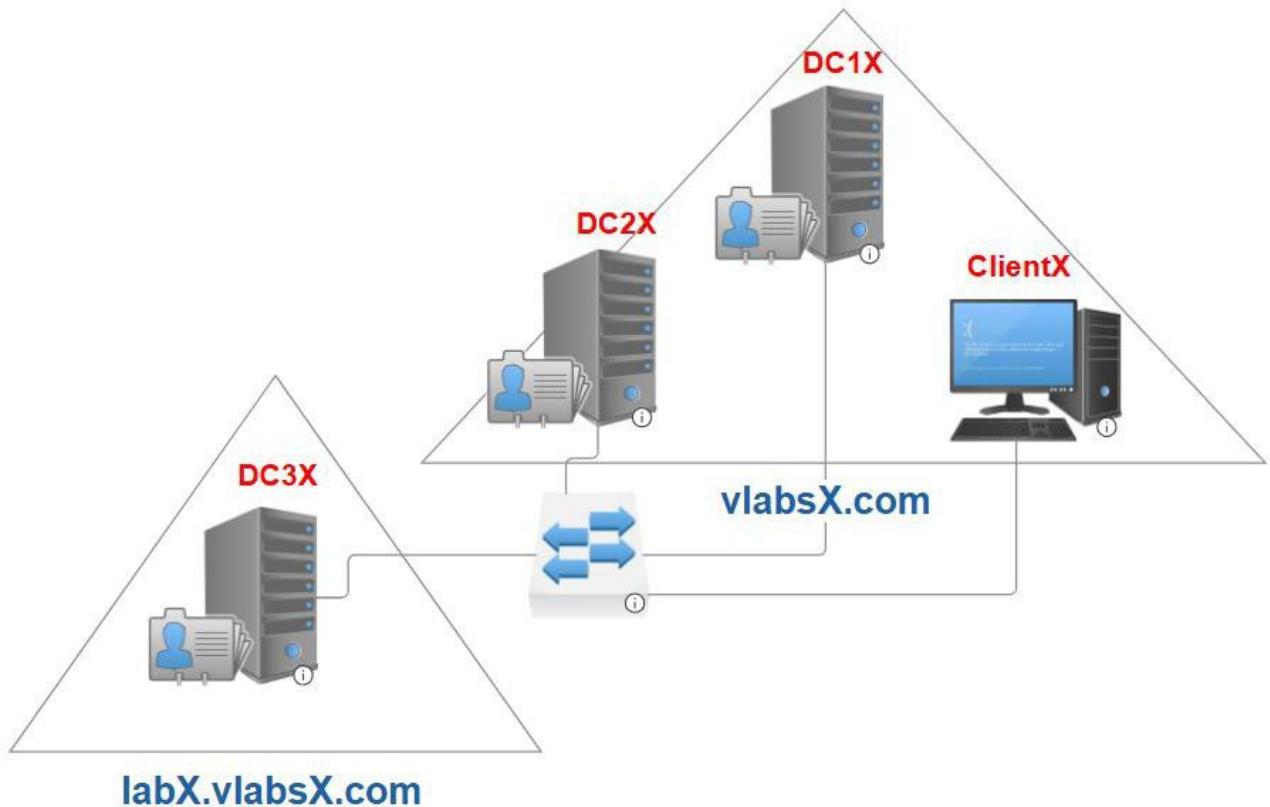
## 1.1 Objective

In this lab you will **deploy multiple domain controllers** and configure the Active Directory environment. The lab includes:

- Installing and configuring **DC1XX** as the first domain controller for **vlabsX.com**
- Joining **ClientXX** to the domain.
- Configuring **DC2XX** as a **Read-Only Domain Controller (RODC)**.
- Deploying **DC3XX** as a **Child Domain Controller (labXX.vlabsXX.com)** using PowerShell.
- Verifying the domain controller promotion and testing Active Directory tools.

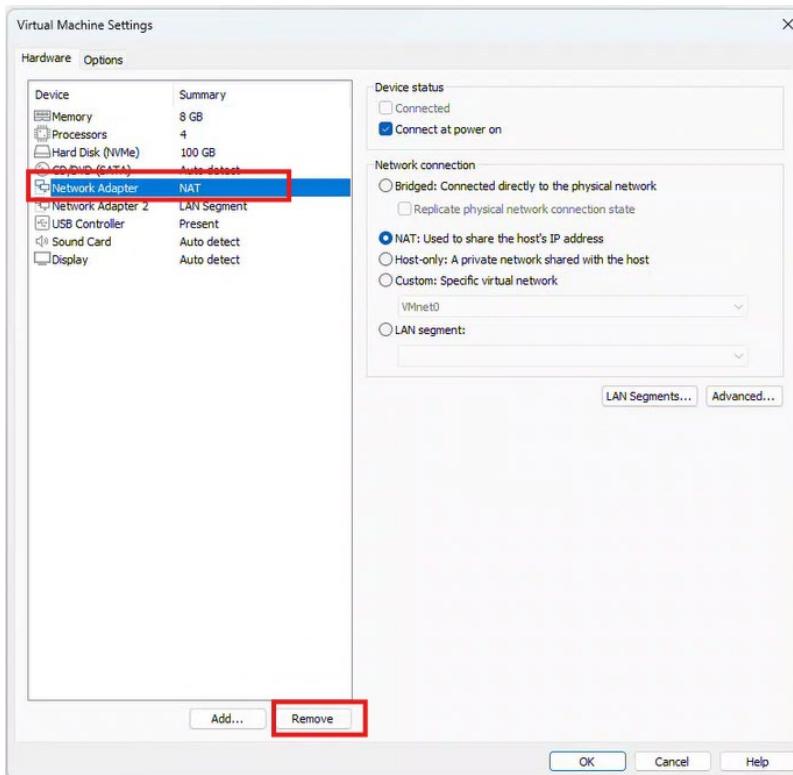
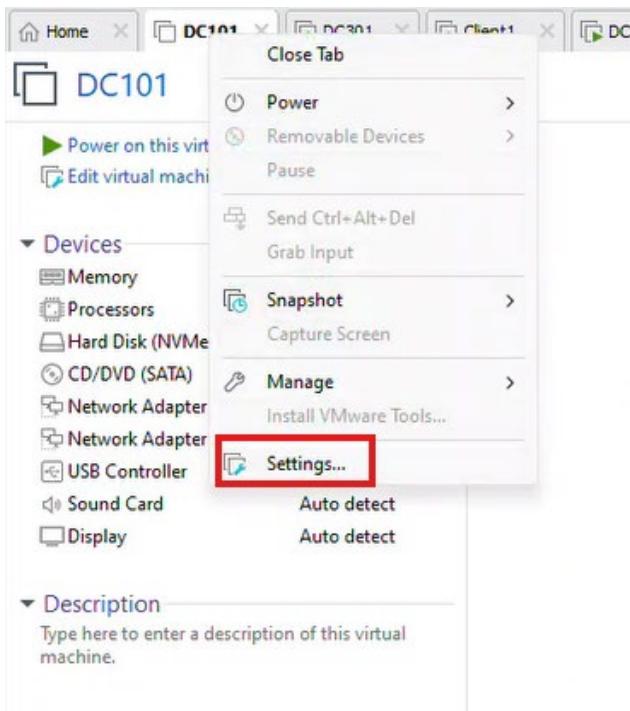
---

## 2 Topology



### 3 Step 1: Configure DC101 (Primary Domain Controller)

#### 3.1 Before starting DC101, remove the network card **NAT** then start the server.





## 3.2 Using Server Manager, install Active Directory Domain Services (AD DS).

### Disable IP V6

PROPERTIES  
For DC101

|                             |                           |
|-----------------------------|---------------------------|
| Computer name               | DC101                     |
| Workgroup                   | WORKGROUP                 |
| Microsoft Defender Firewall | Public: On                |
| Remote management           | Enabled                   |
| Remote Desktop              | Enabled                   |
| NIC Teaming                 | Disabled                  |
| Ethernet1                   | 192.168.1.1, IPv6 enabled |

Network Connections

Ethernet1 Status

Ethernet1 Properties

Networking

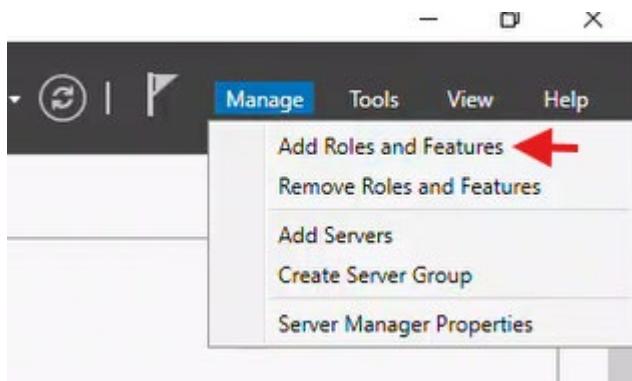
Internet Protocol Version 6 (TCP/IPv6)

The screenshot shows the Windows Server Manager interface. The left navigation pane includes 'Dashboard', 'Local Server' (which is selected and highlighted in blue), 'All Servers', and 'File and Storage Services'. The right pane is titled 'PROPERTIES' for 'DC101'. It displays the following information:

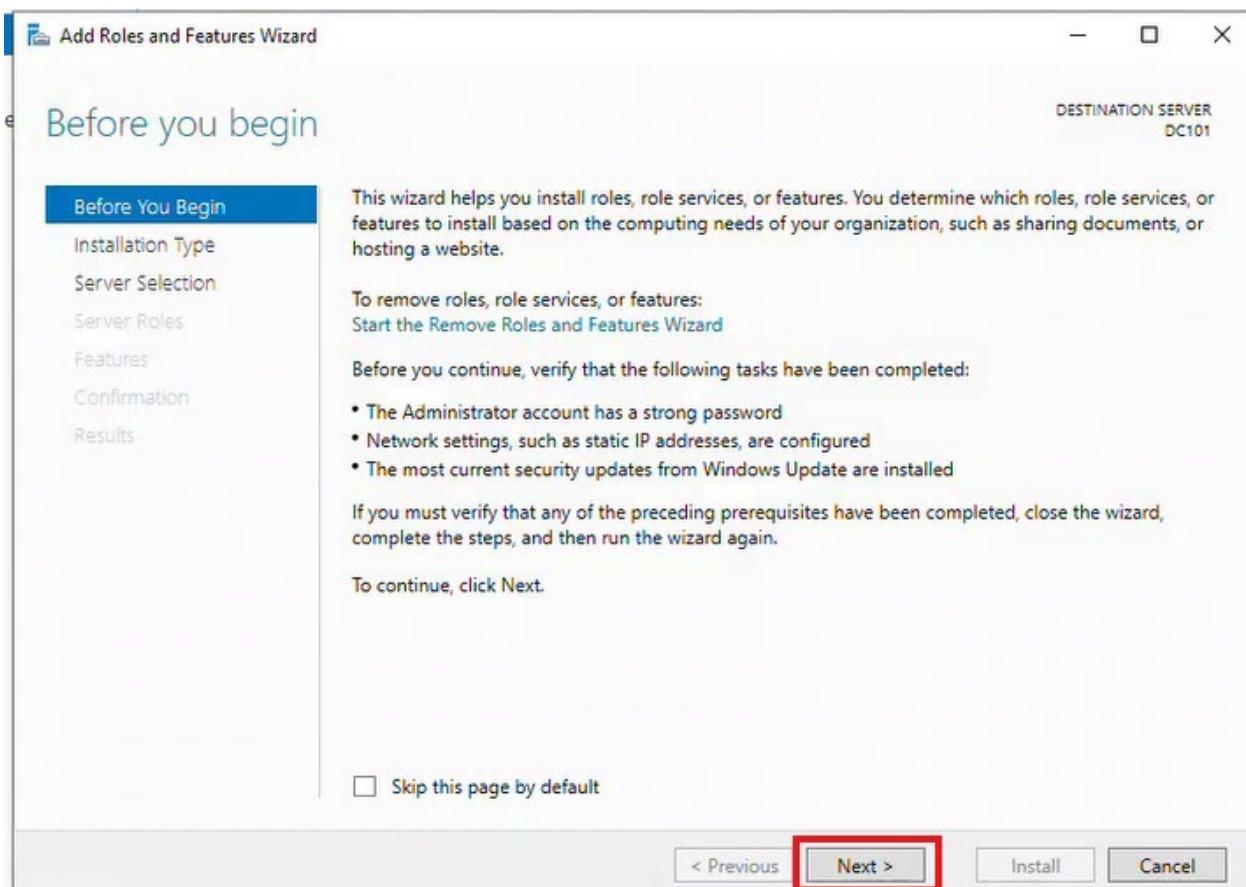
| Computer name               | DC101                                    |
|-----------------------------|--|
| Workgroup                   | WORKGROUP                                |
| Microsoft Defender Firewall | Public: On                               |
| Remote management           | Enabled                                  |
| Remote Desktop              | Enabled                                  |
| NIC Teaming                 | Disabled                                 |
| Ethernet1                   | 192.168.1.1                              |
| Operating system version    | Microsoft Windows Server 2022 Datacenter |

A red arrow points to the IP address '192.168.1.1' under the 'Ethernet1' row.

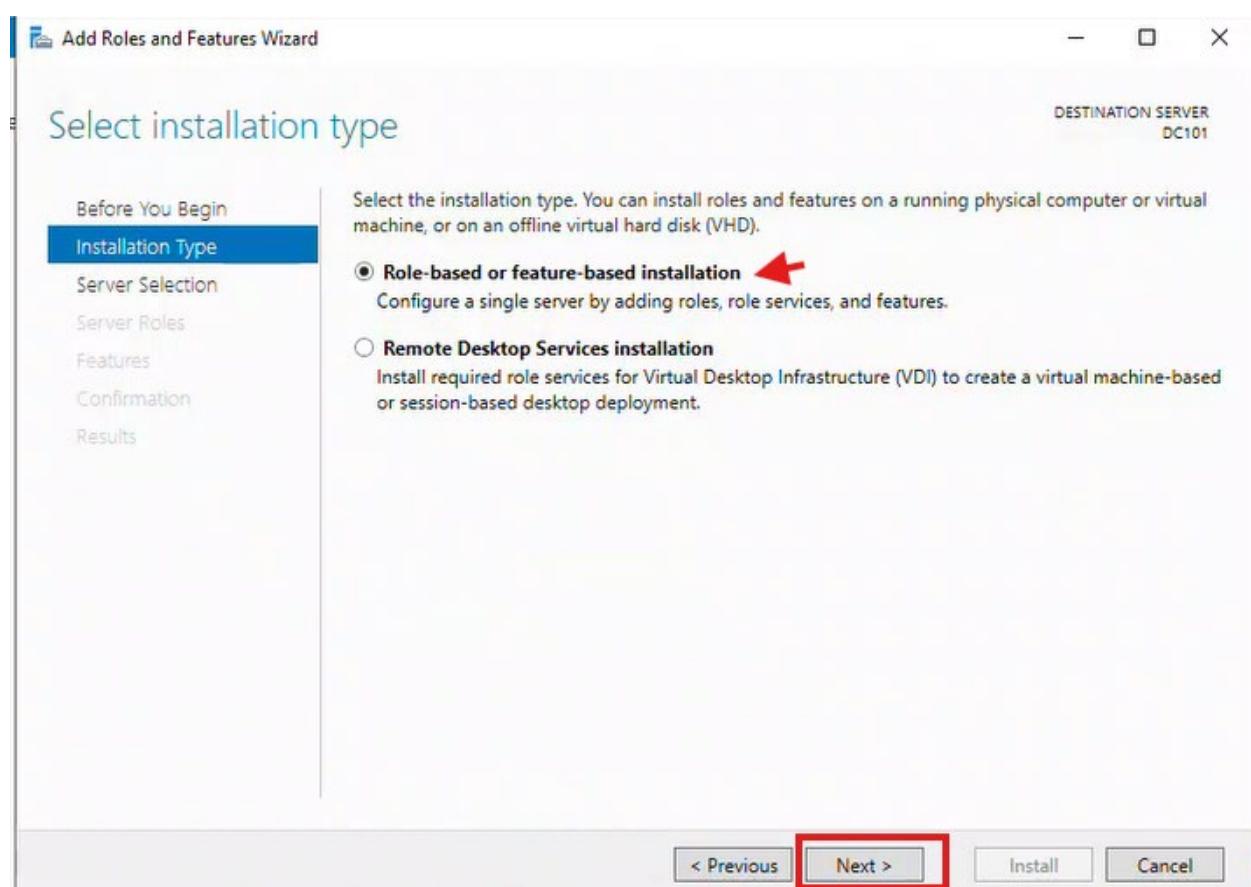
A) Add Roles and Features: Click Manage > Add Roles and Features



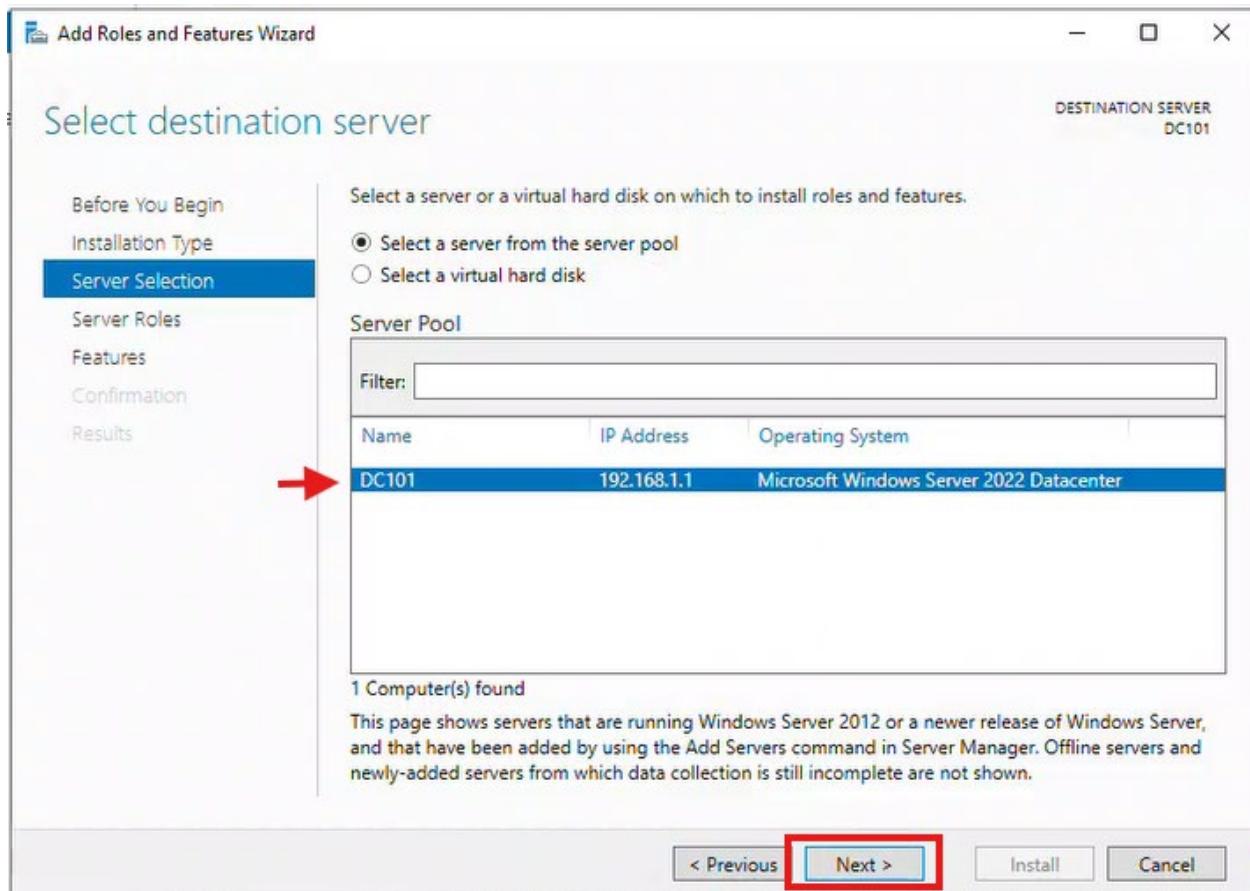
B) Add roles and features Wizard appears click Next



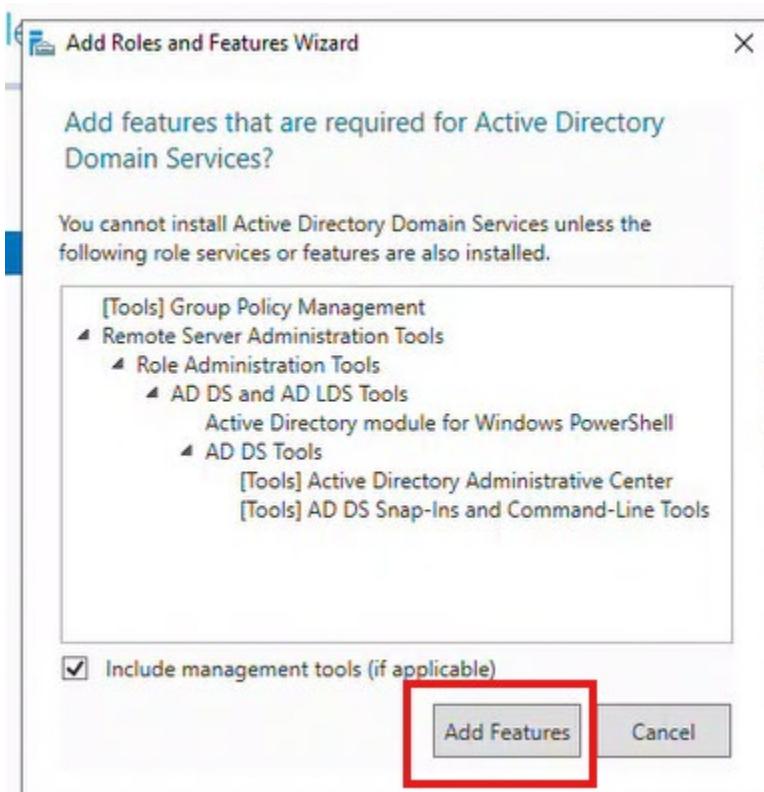
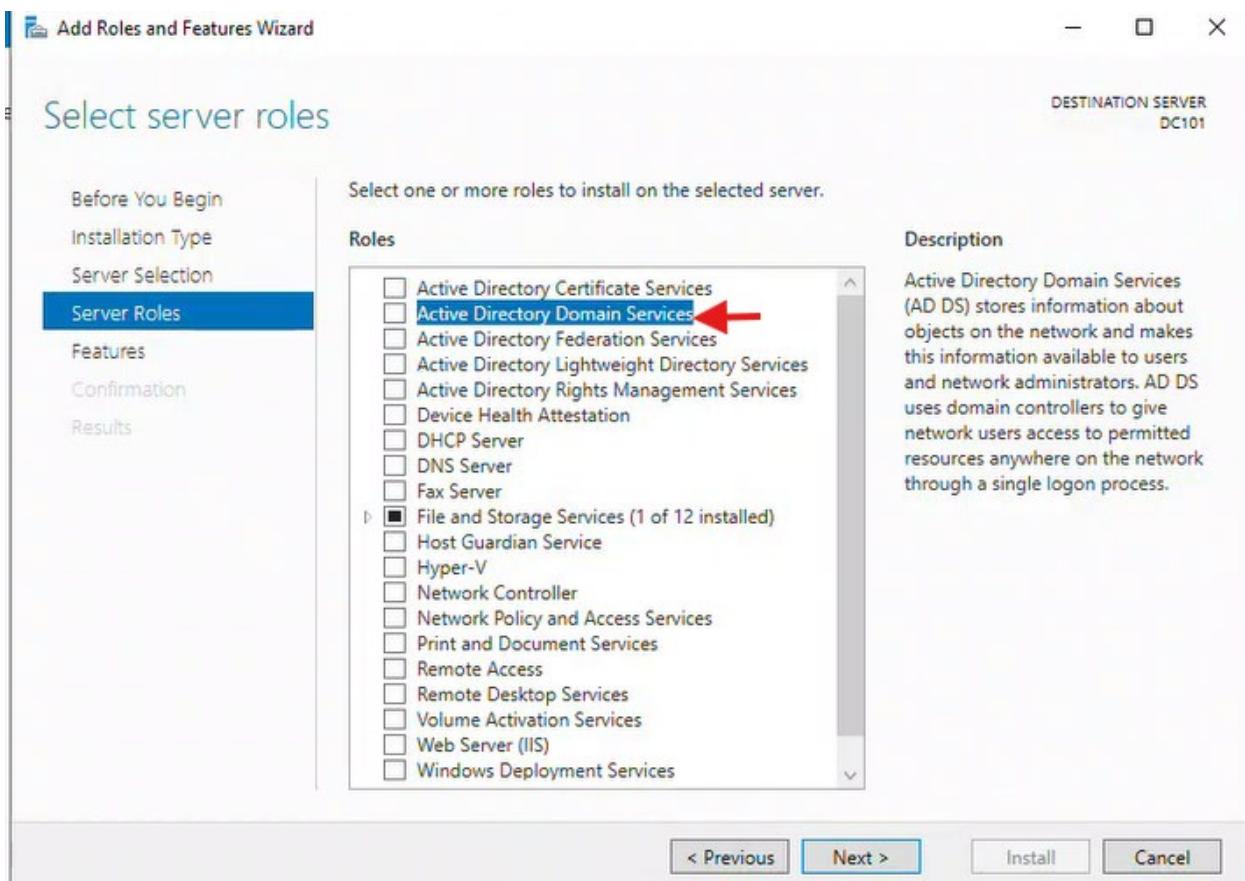
C) Installation Type: Choose Role-based or feature-based installation and click Next

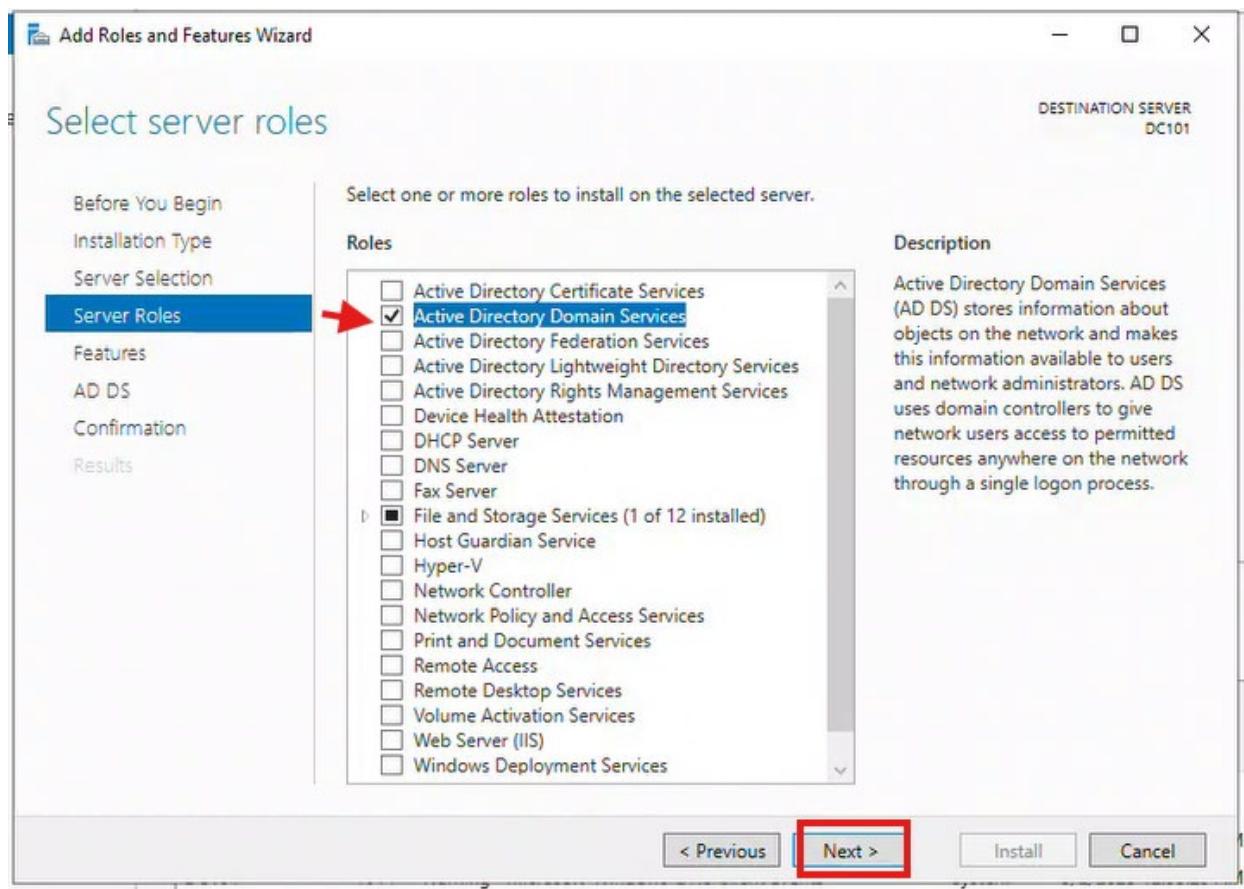


D) Server Selection: Select the server you want to install AD DS on and click Next

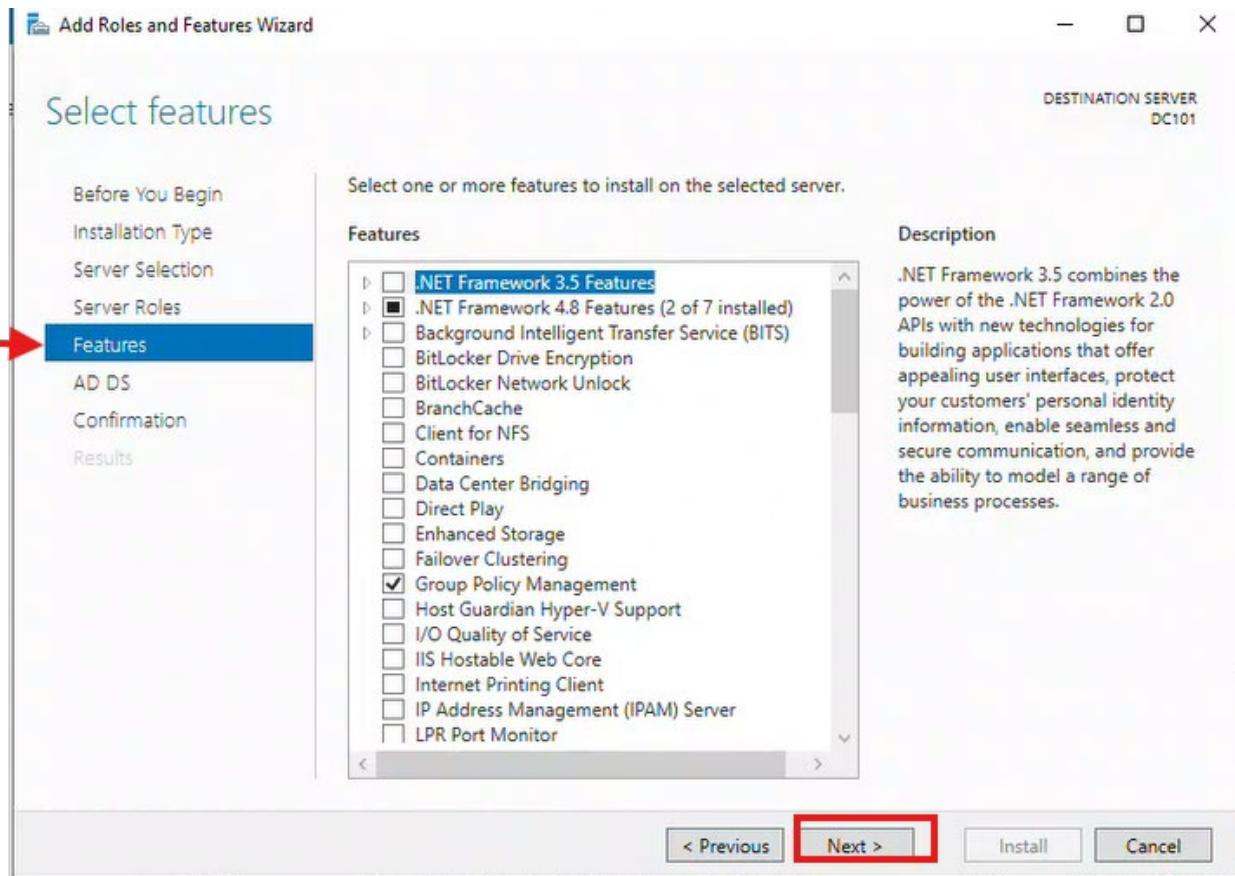


E) Server Roles: Check Active Directory Domain Services (very important to choose just the second option), new small window will appear and click Add Features

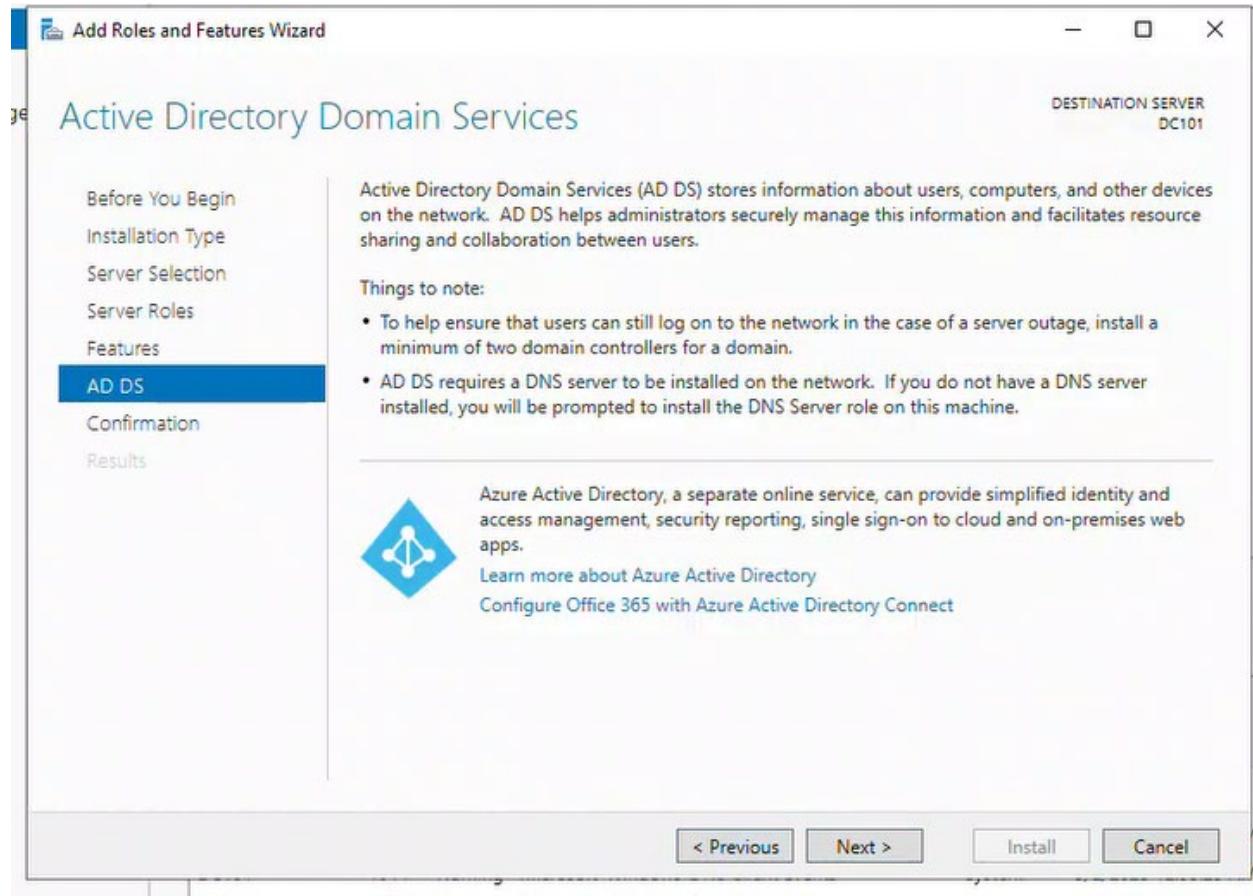




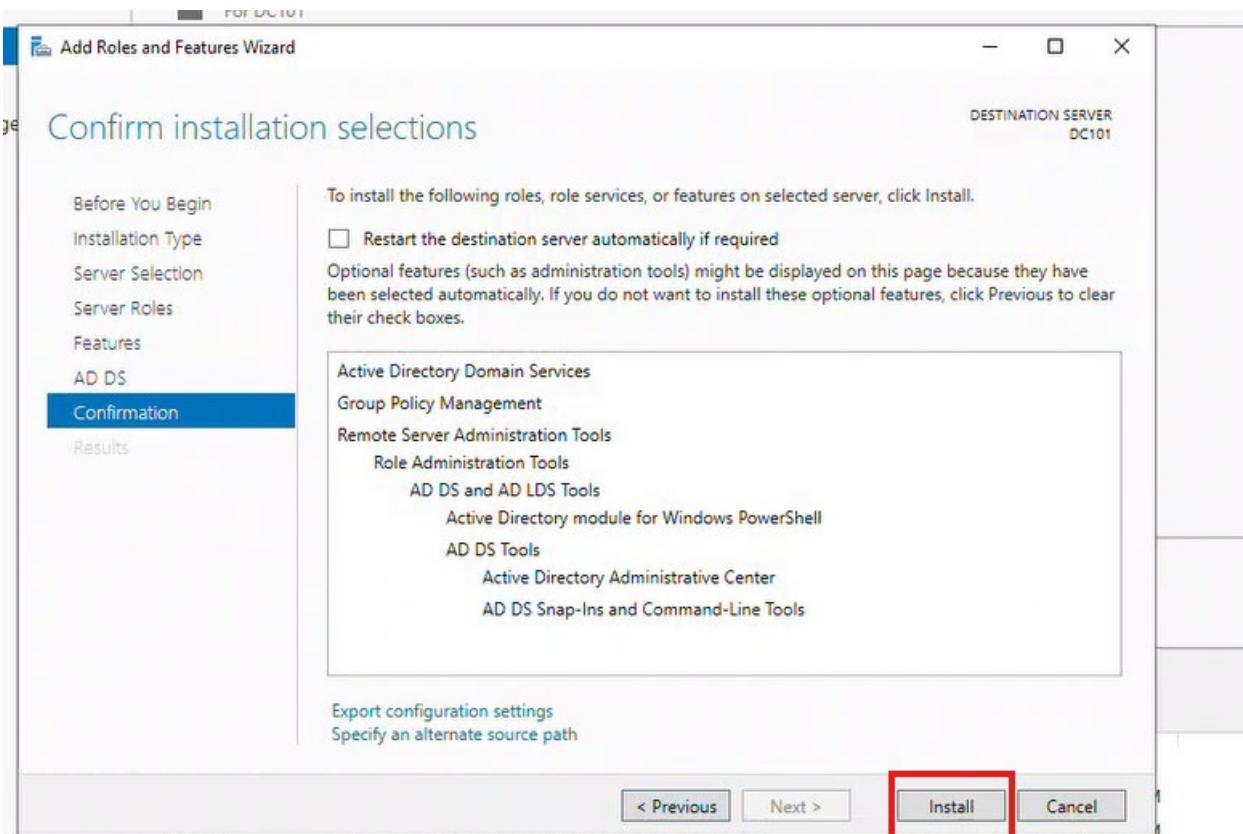
F) Select Features: Click Next (features are chosen by default)



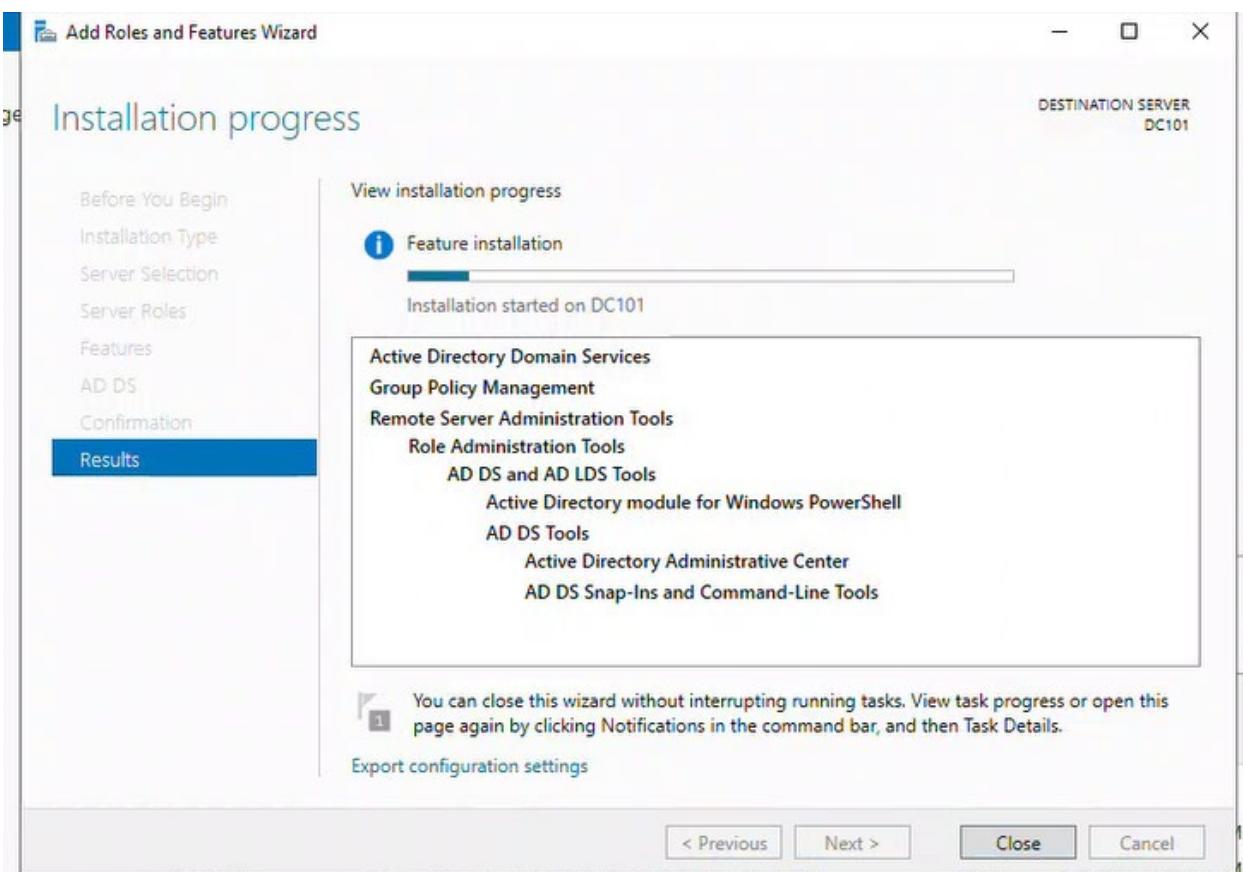
G) Active Directory domain Services windows appear Select Next



H) Confirm Installation: Review the summary and click Install

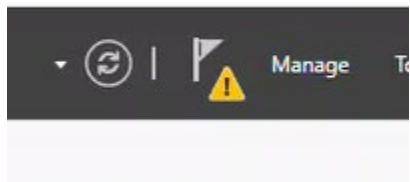


- I) There we go we're starting to install Active Directory it's installing a whole bunch of other tools

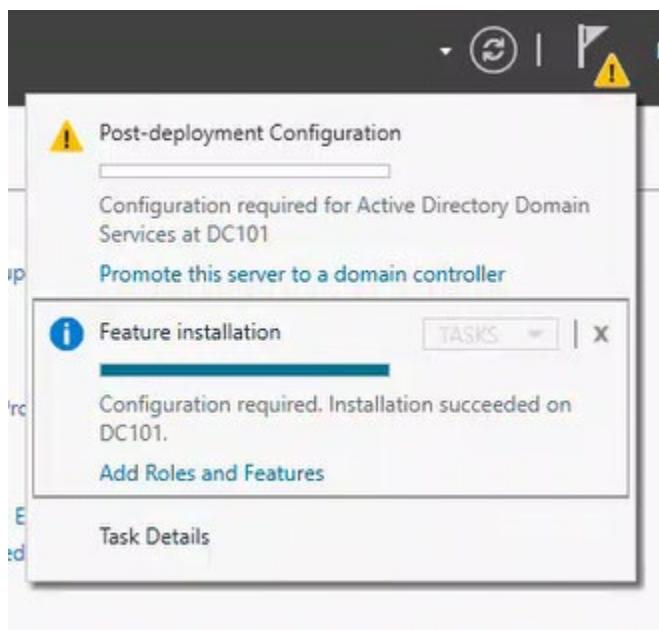


### 3.3 Promote DC101 to a Domain Controller in a new Forest: vlabs1.com

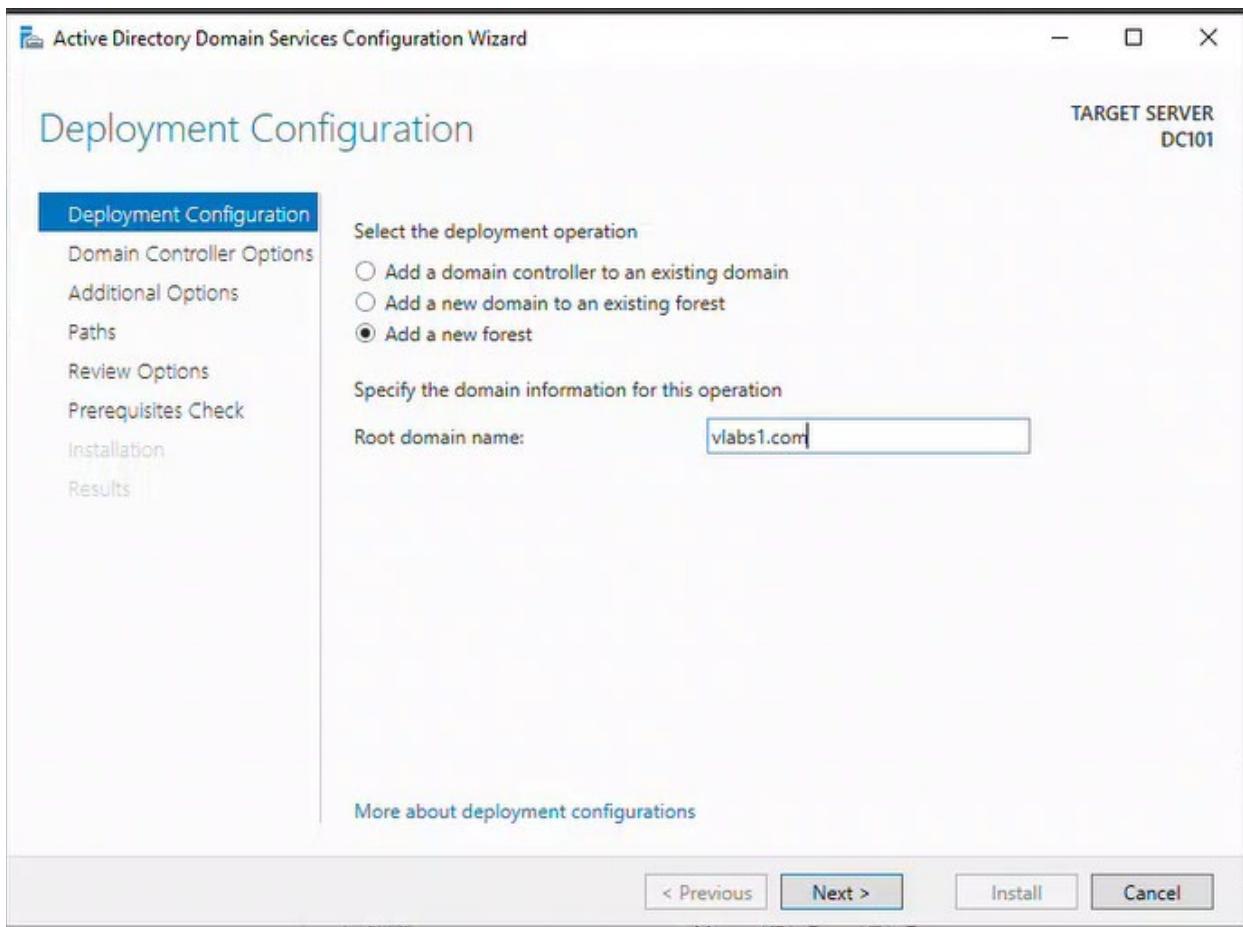
- A) Open Server Manager: After installation, you'll see a notification in Server Manager. Top right Promote to Domain Controller: Click the notification and select Promote this server to a domain controller



Warning says **Promote the Server to a Domain Controller**, click on it



- B) In Deployment Configuration: Choose Add a new forest  
C) Domain Name: Enter your organization's root domain name  
vlab<mynumber>.com and click Next

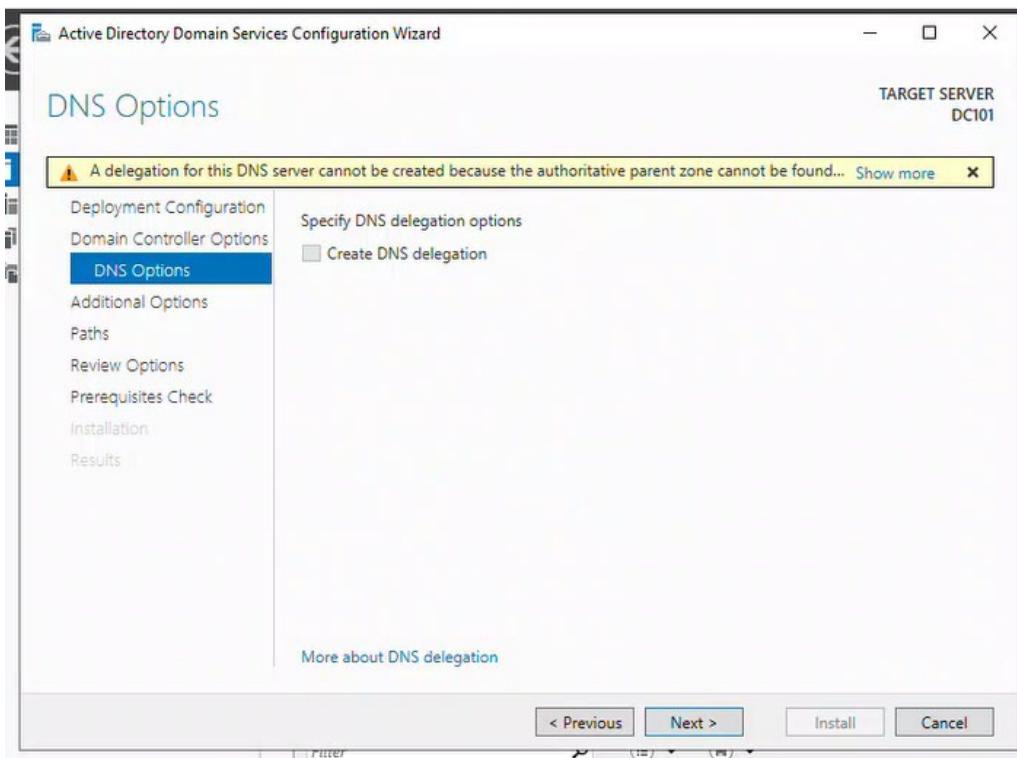
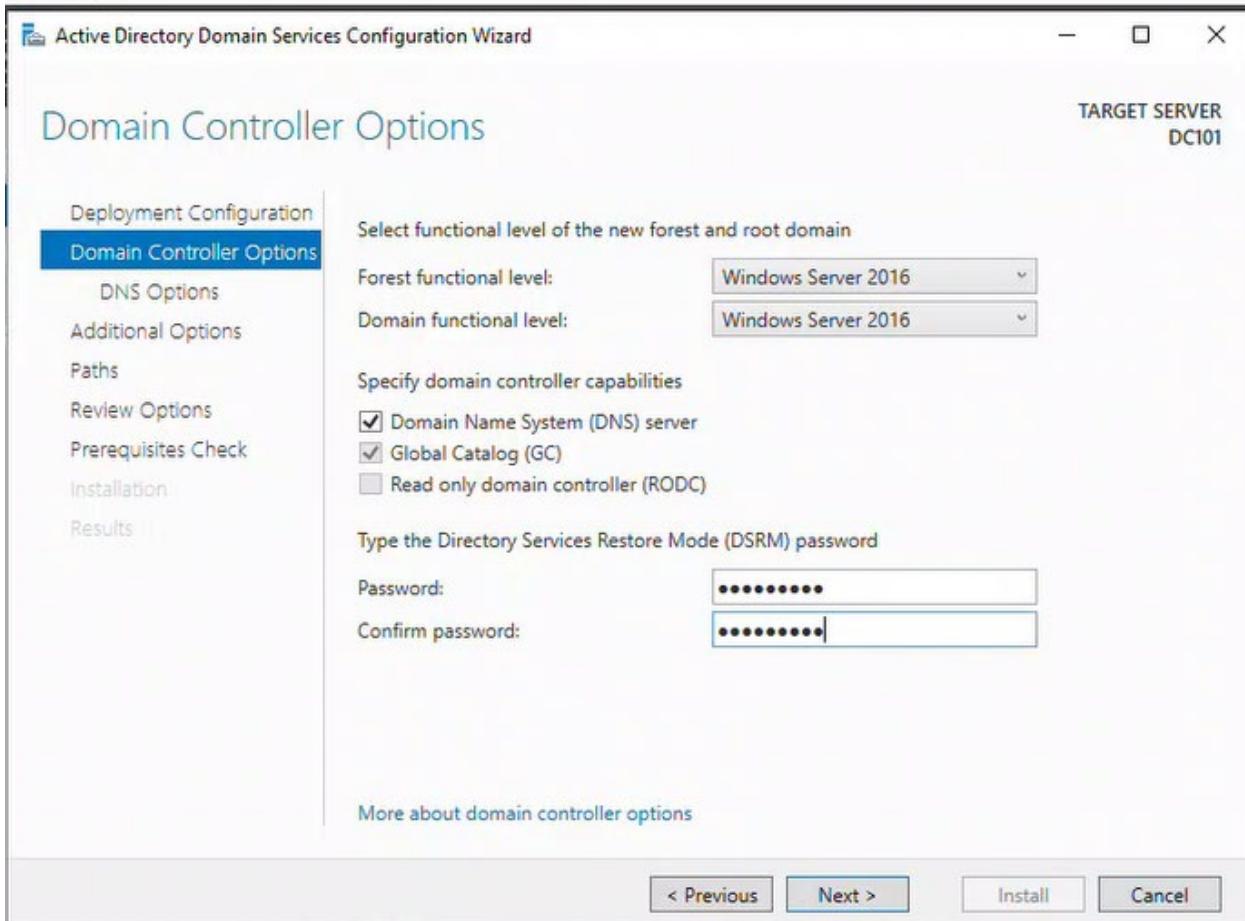


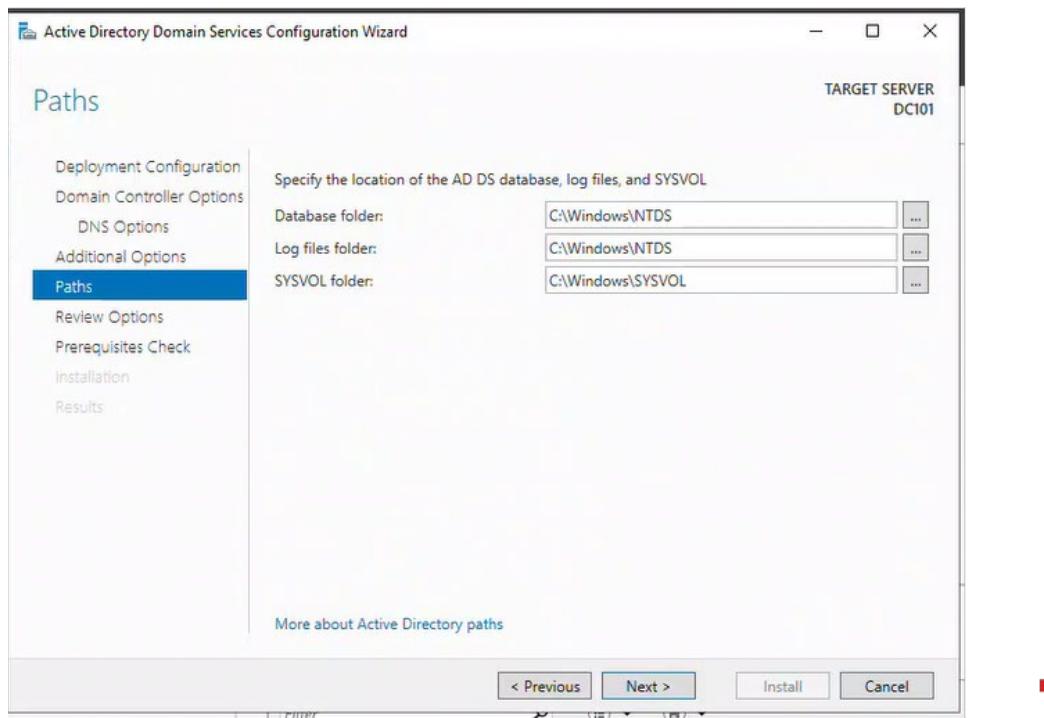
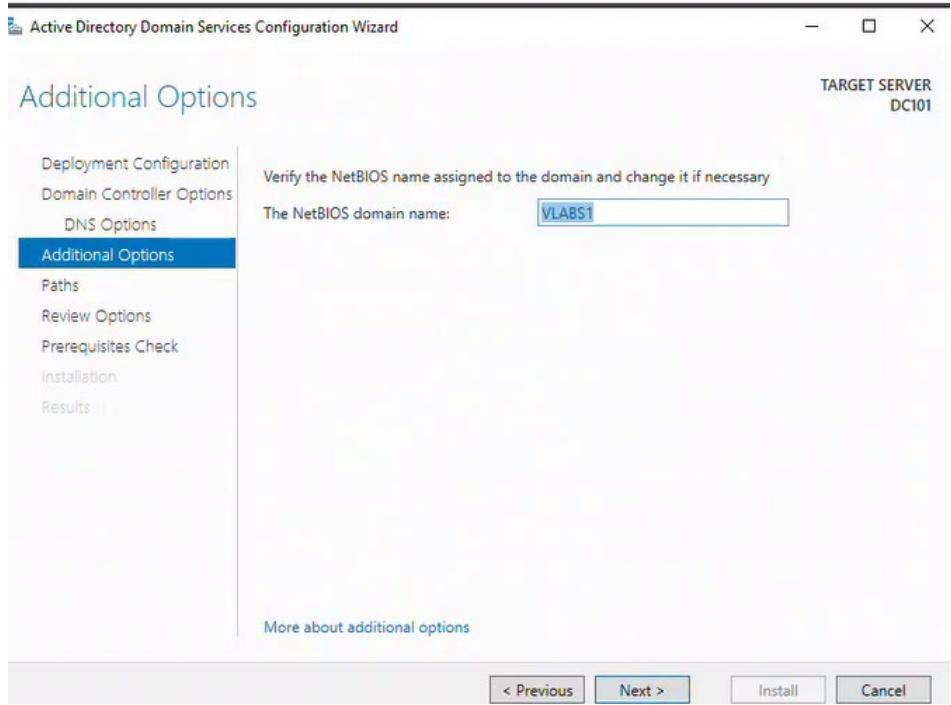
#### D) Domain Controller Options

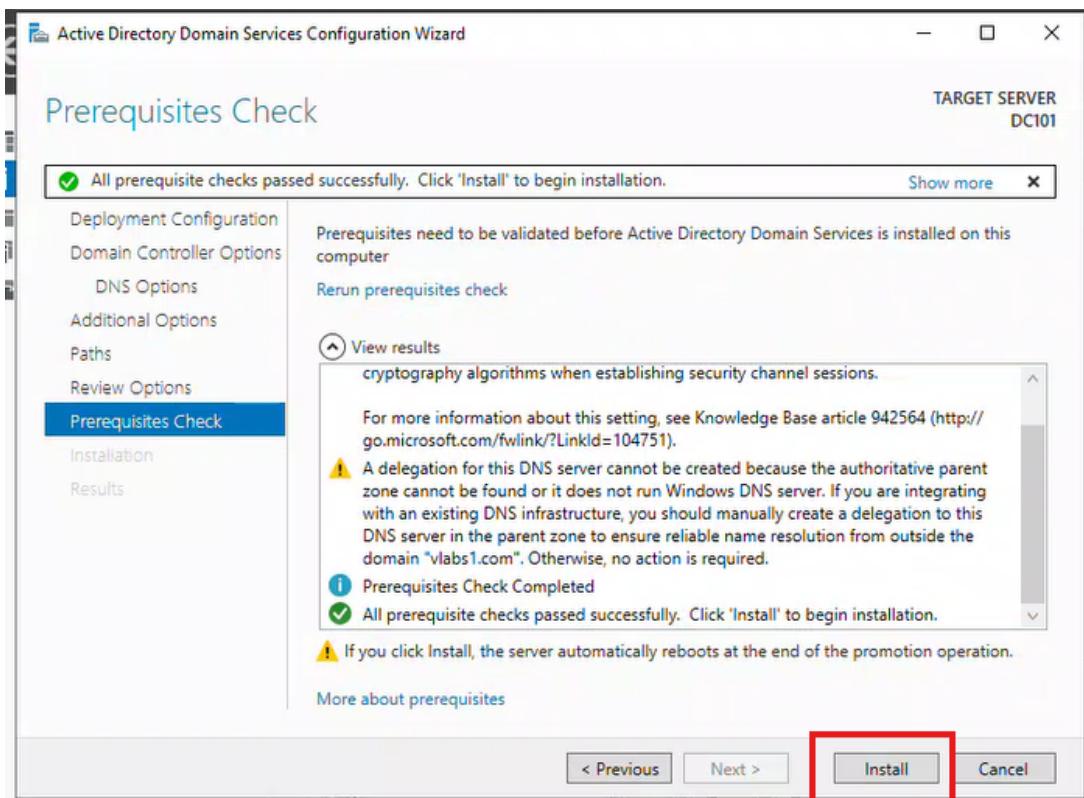
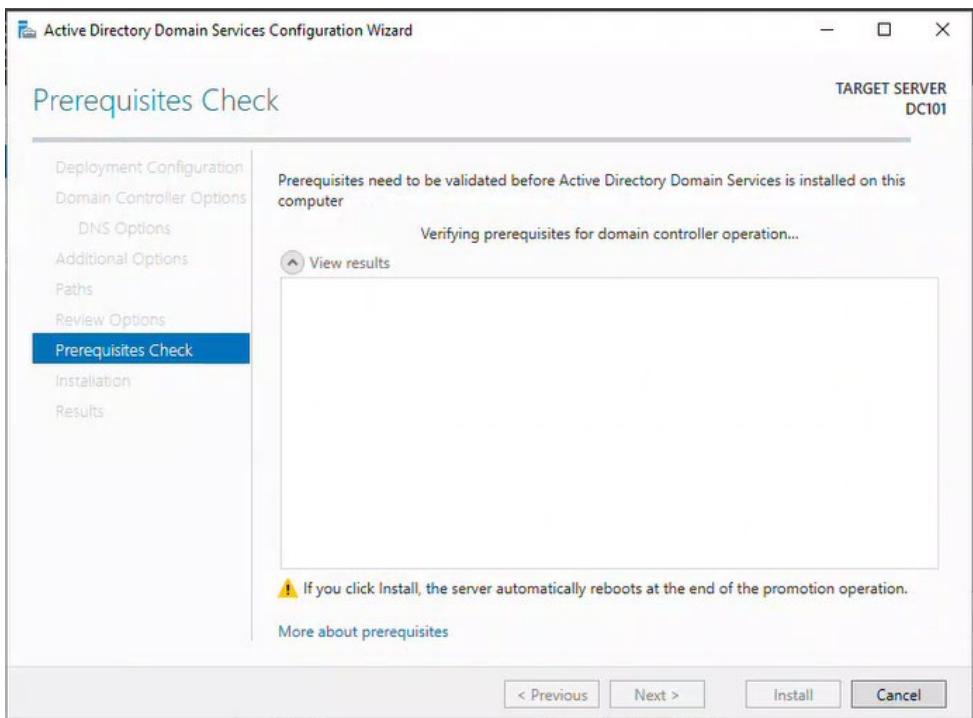
Leave as Windows Server 2016 in Forest Functional Level and Domain Functional Level

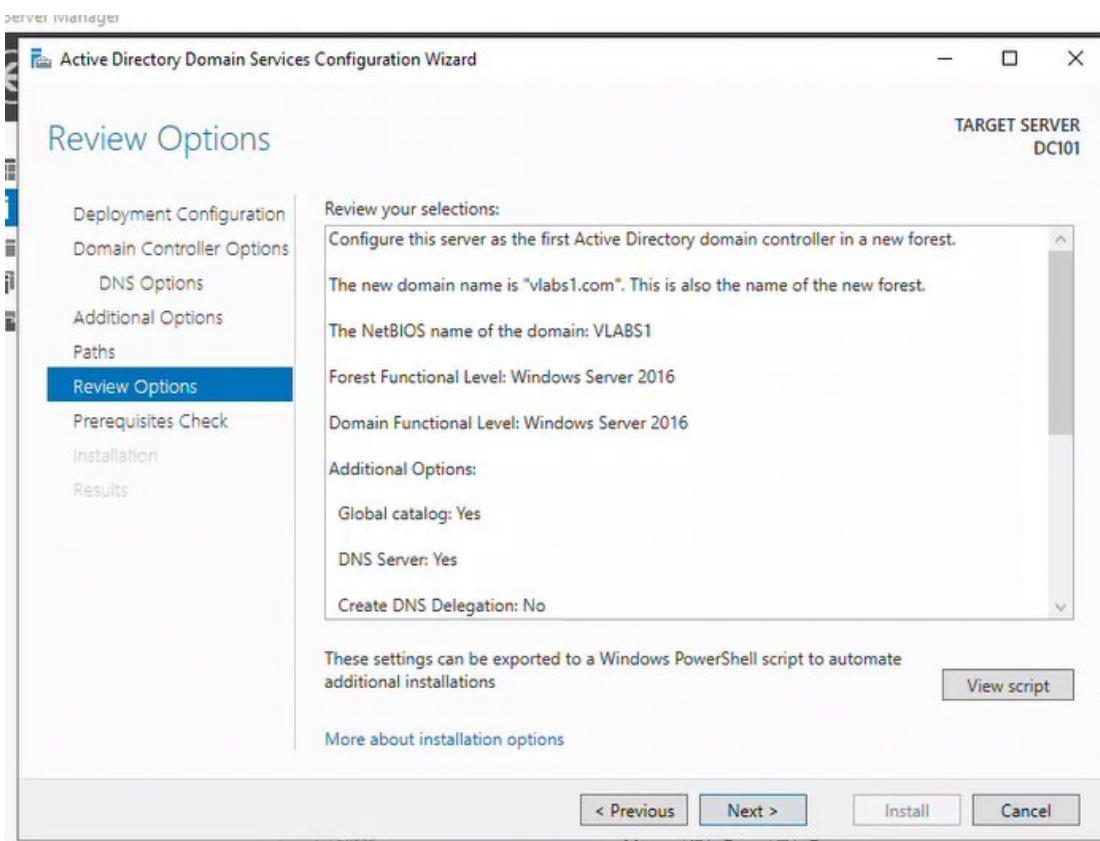
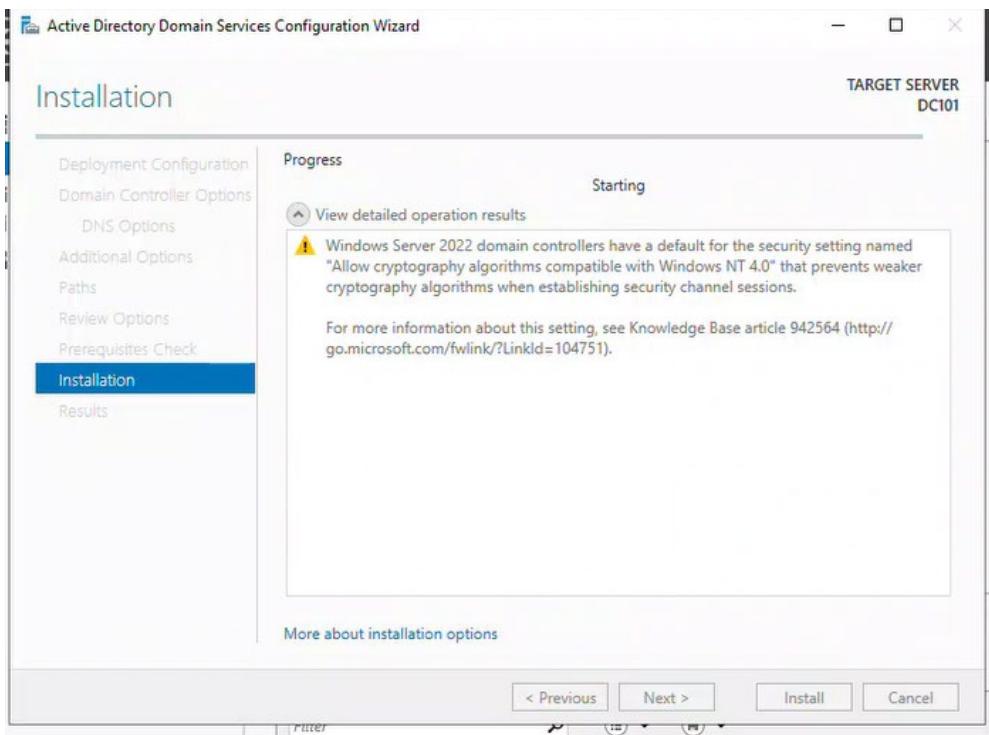
Set password for [administrator@vlans1.com](mailto:administrator@vlans1.com) as Passw0rd\$

Click Next









**Restart will be automatically done**

1. Verify the DC Installation.



---

Verify AD DS Installation:

Get-Serviceadws,kdc,netlogon,dns

- Check Domain Membership:

Get-ADDomain

```

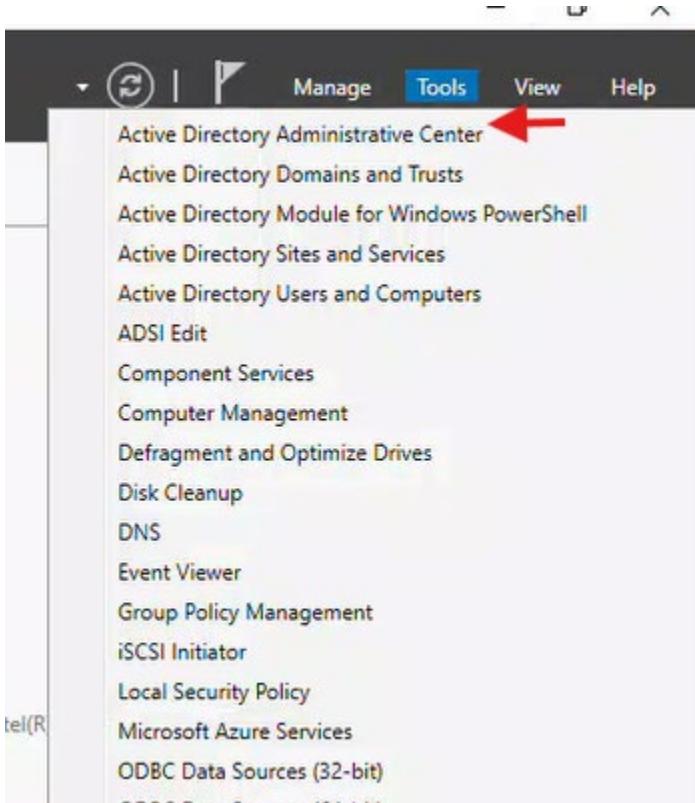
PS C:\Users\Administrator> Get-Service adws,kdc,netlogon,dns
Status     Name           DisplayName
-----   -----
Running    adws          Active Directory Web Services
Running    dns            DNS Server
Running    kdc            Kerberos Key Distribution Center
Running    Netlogon       netlogon

PS C:\Users\Administrator> Get-ADDomain

AllowedDNSSuffixes      : {}
ChildDomains             : {}
ComputersContainer       : CN=Computers,DC=vlabs1,DC=com
DeletedObjectsContainer  : CN=Deleted Objects,DC=vlabs1,DC=com
DistinguishedName        : DC=vlabs1,DC=com
DNSRoot                 : vlabs1.com
DomainControllersContainer: OU=Domain Controllers,DC=vlabs1,DC=com
DomainMode               : Windows2016Domain
DomainSID                : S-1-5-21-1268601764-4050707287-4025116504
ForeignSecurityPrincipalsContainer: CN=ForeignSecurityPrincipals,DC=vlabs1,DC=com
Forest                  : vlabs1.com
InfrastructureMaster      : DC101.vlabs1.com
LastLogonReplicationInterval: {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=vlabs1,DC=com}
LinkedGroupPolicyObjects  : CN=LostAndFound,DC=vlabs1,DC=com
LostAndFoundContainer    :
ManagedBy                :
Name                     : vlabs1
NetBIOSName              : VLABS1
ObjectClass               : domainDNS
ObjectGUID                : 402b24e7-c605-4172-bb2c-f1356eab96a2
ParentDomain              :
PDCEmulator              : DC101.vlabs1.com
PublicKeyRequiredPasswordRolling: True
QuotasContainer           : CN=NTDS Quotas,DC=vlabs1,DC=com
ReadOnlyReplicaDirectoryServers: {}
ReplicaDirectoryServers   : DC101.vlabs1.com
RIDMaster                 :
SubordinateReferences     : {DC=ForestDnsZones,DC=vlabs1,DC=com, DC=DomainDnsZones,DC=vlabs1,DC=com, CN=Configuration,DC=vlabs1,DC=com}
SystemsContainer           : CN=System,DC=vlabs1,DC=com
UsersContainer             : CN=Users,DC=vlabs1,DC=com

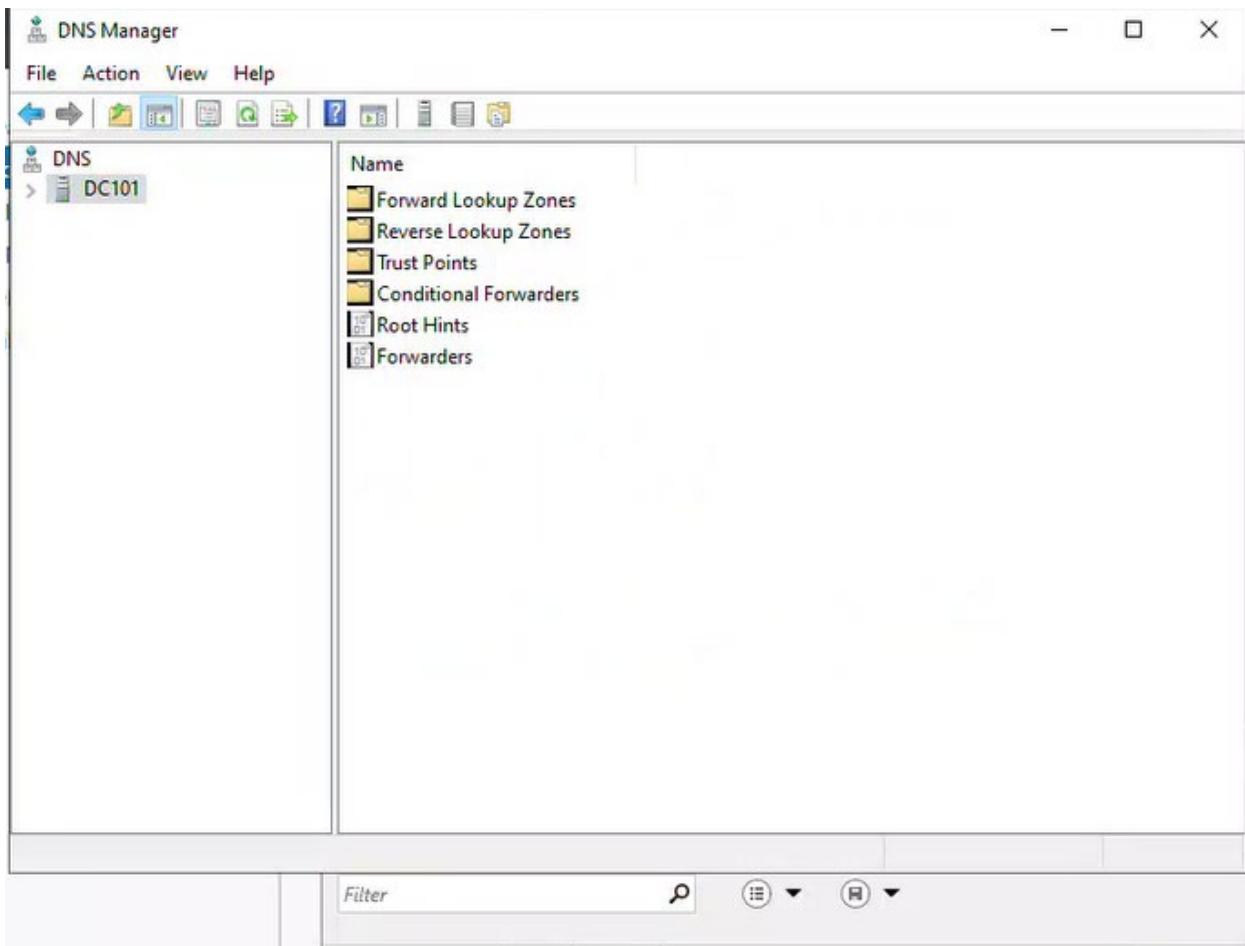
PS C:\Users\Administrator>

```



- Ensure DNS is configured correctly.

Active Directory Administrative Center  
 Active Directory Domains and Trusts  
 Active Directory Module for Windows PowerShell  
 Active Directory Sites and Services  
 Active Directory Users and Computers  
 ADSI Edit  
 Component Services  
 Computer Management  
 Defragment and Optimize Drives  
 Disk Cleanup  
**DNS** ←  
 Event Viewer  
 Group Policy Management  
 iSCSI Initiator  
 Local Security Policy  
 Microsoft Azure Services  
 ODBC Data Sources (32-bit)  
 ODBC Data Sources (64-bit)  
 Performance Monitor  
 Recovery Drive  
 Registry Editor  
 Resource Monitor  
 Services  
 System Configuration  
 System Information  
 Task Scheduler  
 Windows Defender Firewall with Advanced Security  
 Windows Memory Diagnostic  
 Windows PowerShell  
 Windows PowerShell (x86)  
 Windows Server Backup



On client ping Server to verify DNS is working

ping 192.168.1.1

ping dc101.vlabs1.com

```
Home DC101 DC301 Client1 DC201
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.26100.3775]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Windows\System32>ping dc101.vlabs1.com
^C
C:\Windows\System32>ping dc101.vlabs1.com

Pinging dc101.vlabs1.com [192.168.1.1] with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=13ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 4ms
Control-C
^C
C:\Windows\System32>
```

Active directory administrative center

| Name                      | Type            | Description                    |
|---------------------------|-----------------|--------------------------------|
| Builtin                   | builtinDom...   |                                |
| Computers                 | Container       | Default container for upgr...  |
| Domain Controllers        | Organizati...   | Default container for dom...   |
| ForeignSecurityPrincipals | Container       | Default container for secur... |
| Infrastructure            | infrastructu... |                                |
| Keys                      | Container       | Default container for key o... |
| LostAndFound              | lostAndFou...   | Default container for orph...  |
| Managed Service Accounts  | Container       | Default container for man...   |
| NTDS Quotas               | msDS-Quo...     | Quota specifications conta...  |
| Program Data              | Container       | Default location for storag... |
| System                    | Container       | Builtin system settings        |
| TPM Devices               | msTPM-Inf...    |                                |
| Users                     | Container       | Default container for upgr...  |

## Check on Power shell active directory

```
Administrator: Active Directory Module for Windows PowerShell
PS C:\Users\Administrator> Get-WindowsFeature AD-Domain-Services
Display Name                               Name           Install State
-----[X] Active Directory Domain Services   AD-Domain-Services   Installed

PS C:\Users\Administrator> Get-Service adws,kdc,netlogon,dns
Status    Name          DisplayName
----     --          -----
Running   adws         Active Directory Web Services
Running   dns          DNS Server
Running   kdc          Kerberos Key Distribution Center
Running   Netlogon      netlogon

PS C:\Users\Administrator>
```

## Get Active Directory domain

Check Domain Membership:

Get-ADDomain

```

PS C:\Users\Administrator> Get-ADDomain

AllowedDNSSuffixes          : {}
ChildDomains                 : {}
ComputersContainer           : CN=Computers,DC=vlabs1,DC=com
DeletedObjectsContainer      : CN=Deleted Objects,DC=vlabs1,DC=com
DistinguishedName            : DC=vlabs1,DC=com
DNSRoot                      : vlabs1.com
DomainControllersContainer   : OU=Domain Controllers,DC=vlabs1,DC=com
DomainMode                   : Windows2016Domain
DomainSID                    : S-1-5-21-1268601764-4050707287-4025116504
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=vlabs1,DC=com
Forest                        : vlabs1.com
InfrastructureMaster          : DC101.vlabs1.com
LastLogonReplicationInterval : 
LinkedGroupPolicyobjects     : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=vlabs1,DC=com}
LostAndFoundContainer         : CN=LostAndFound,DC=vlabs1,DC=com
ManagedBy                     : 
Name                          : vlabs1
NetBIOSName                  : VLABS1
ObjectClass                  : domainDNS
ObjectGUID                   : 402b24e7-c605-4172-bb2c-f1356eab96a2
ParentDomain                 : 
PDCEmulator                  : DC101.vlabs1.com
PublicKeyRequiredPasswordRolling : True
QuotasContainer               : CN=NTDS Quotas,DC=vlabs1,DC=com
ReadOnlyReplicaDirectoryServers : {} 
ReplicaDirectoryServers       : {DC101.vlabs1.com}
RIDMaster                     : DC101.vlabs1.com
SubordinateReferences         : {DC=ForestDnsZones,DC=vlabs1,DC=com, DC=DomainDnsZones,DC=vlabs1,DC=com, CN=Configuration,DC=vlabs1,DC=com}
SystemsContainer               : CN=System,DC=vlabs1,DC=com
UsersContainer                : CN=Users,DC=vlabs1,DC=com

```

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

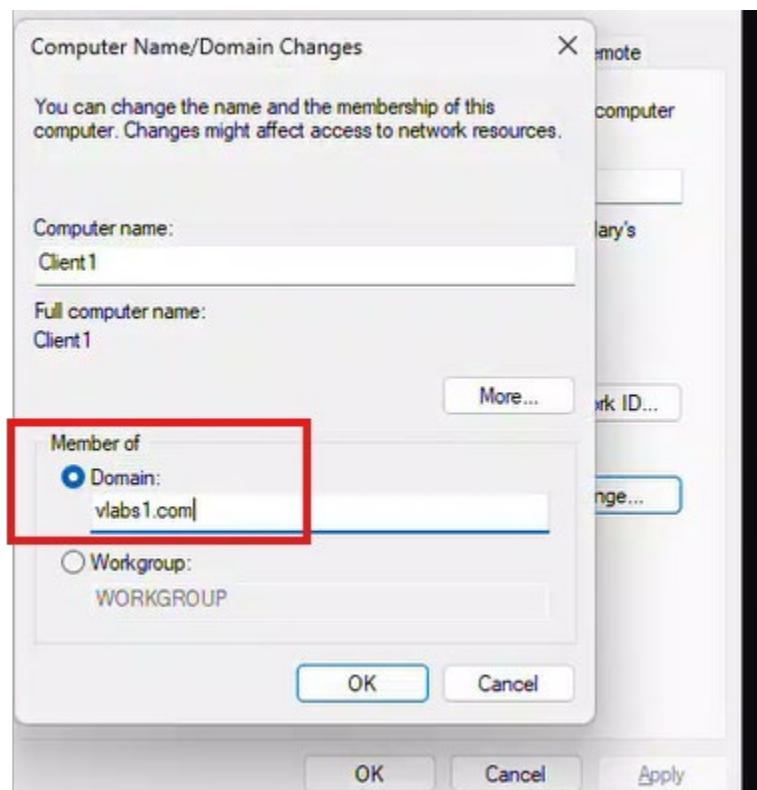
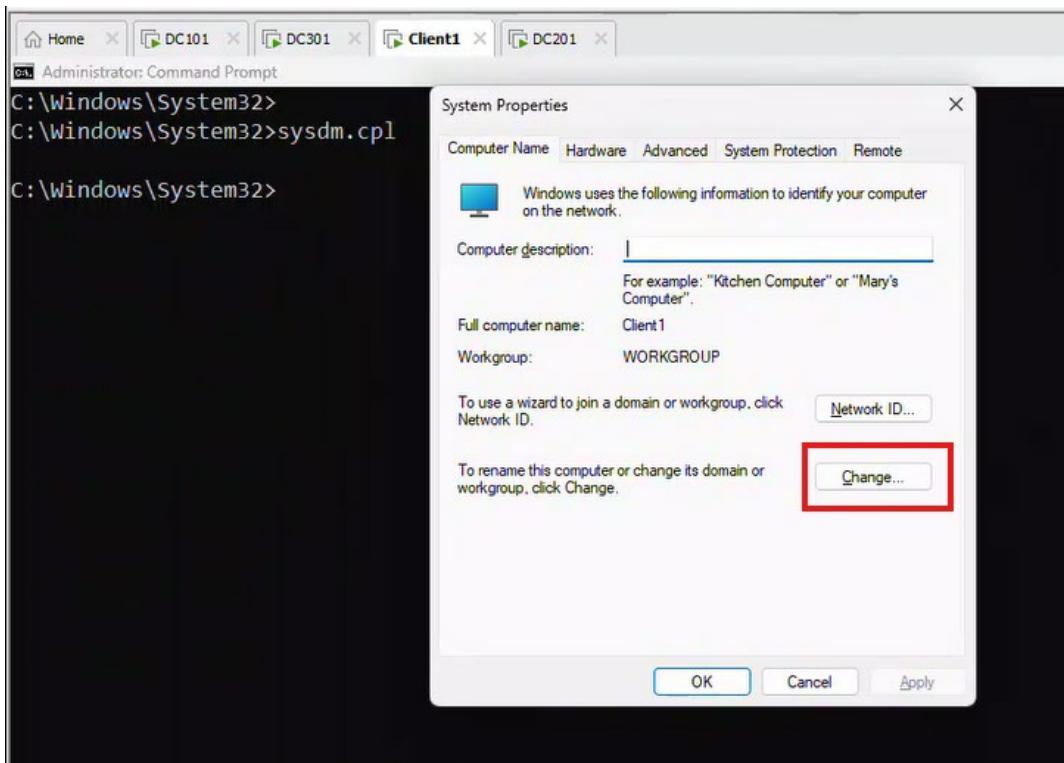
## 4 Step 2: Join Client1 to the Domain

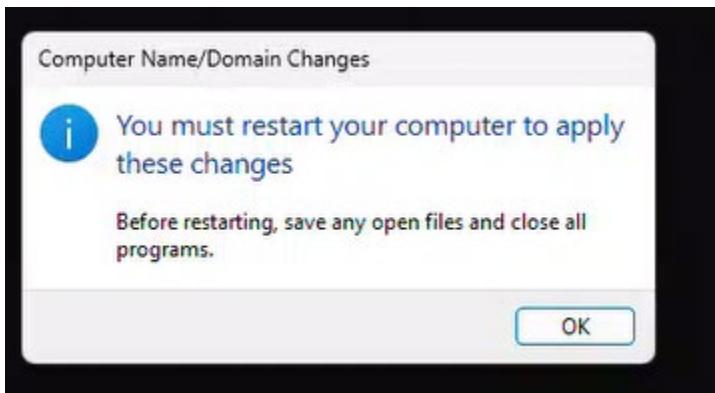
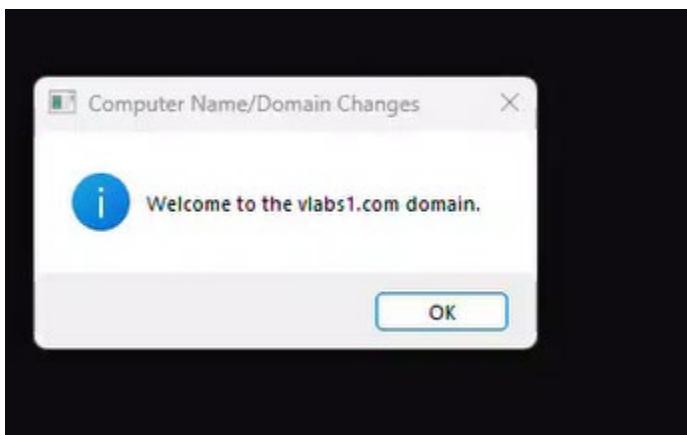
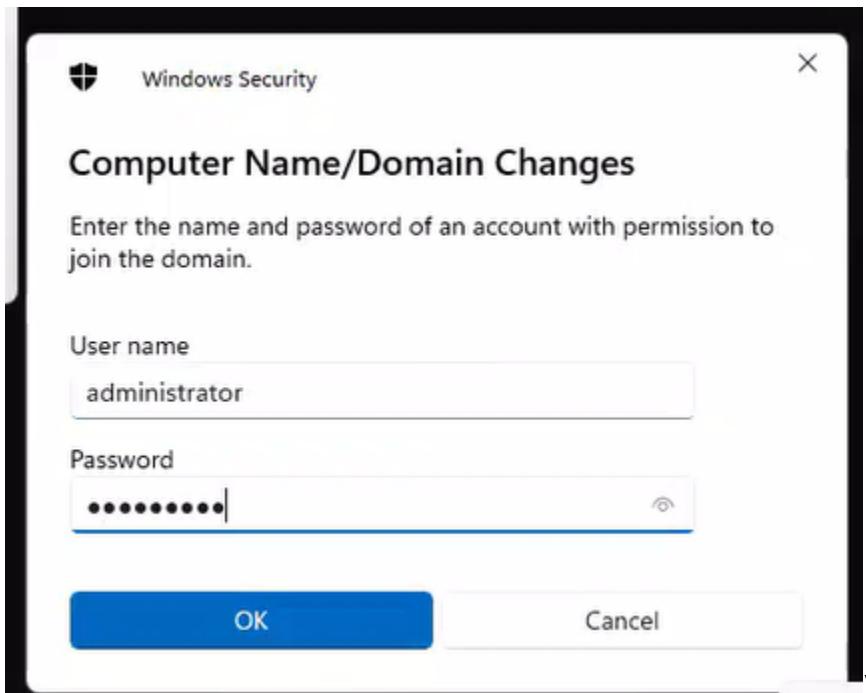
### 4.1 Join Client1 to the vlabs1.com Domain.

#### On client

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

Select change





Computer will restart

23

Server DC 101

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

The screenshot shows the 'Active Directory Administrative Center' interface. In the left navigation pane, under 'vLabs1 (local)', the 'Computers' node is selected. The main pane displays a table titled 'Computers (1)' with one entry: 'CLIENT1' of type 'Computer'. A red arrow points to the 'CLIENT1' row in the table.

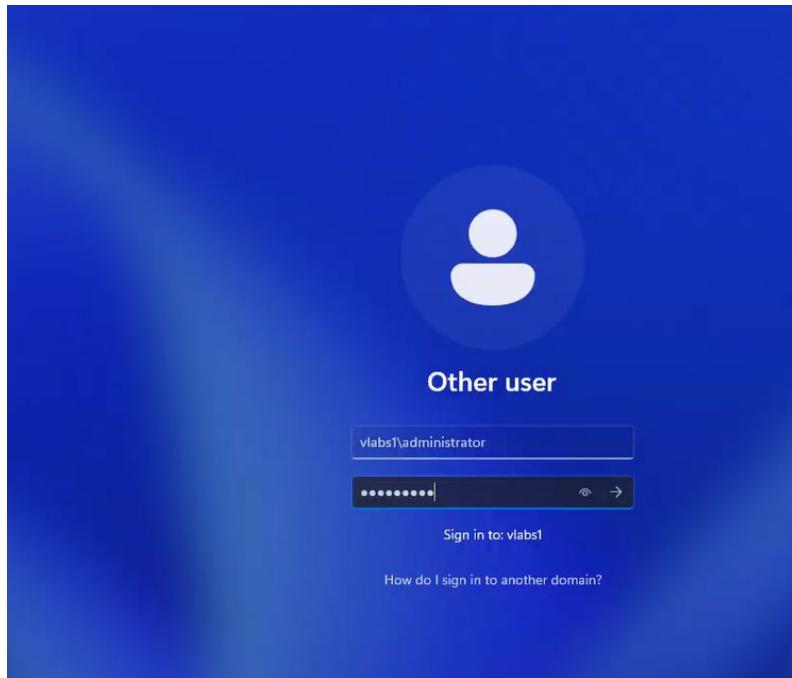
The screenshot shows the 'CLIENT1' properties dialog box. The 'Computer' tab is selected. Key details shown include:

| Computer  | Computer              |
|---|-----------------------|
| Computer name:  | CLIENT1               |
| DNS name:   | Client1.vLabs1.com    |
| Domain controller type:                                   | Workstation or server |
| Site:   |                       |
| Description:  |                       |
| <input type="checkbox"/> Protect from accidental deletion |                       |

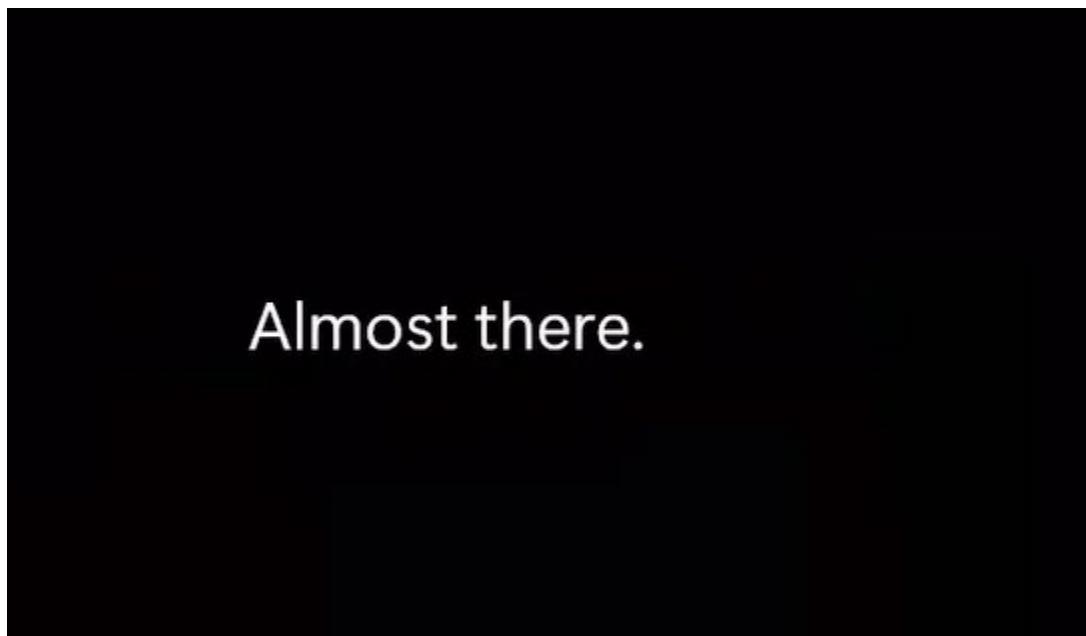
Below the main table, there are sections for 'Managed By' and 'Member Of'.

## 4.2 Login with the domain **administrator** to test it.

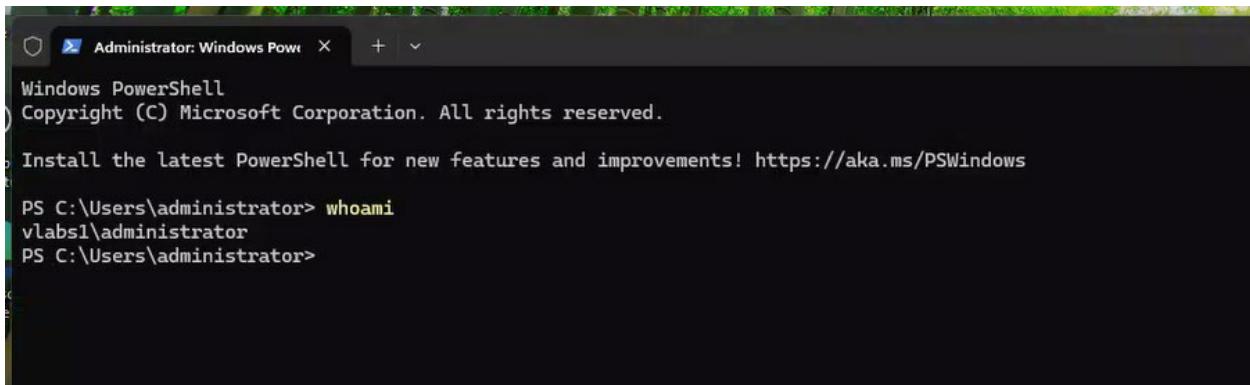
From client login as administrator



Wait



Verify connection



```
Administrator: Windows PowerShell + 
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

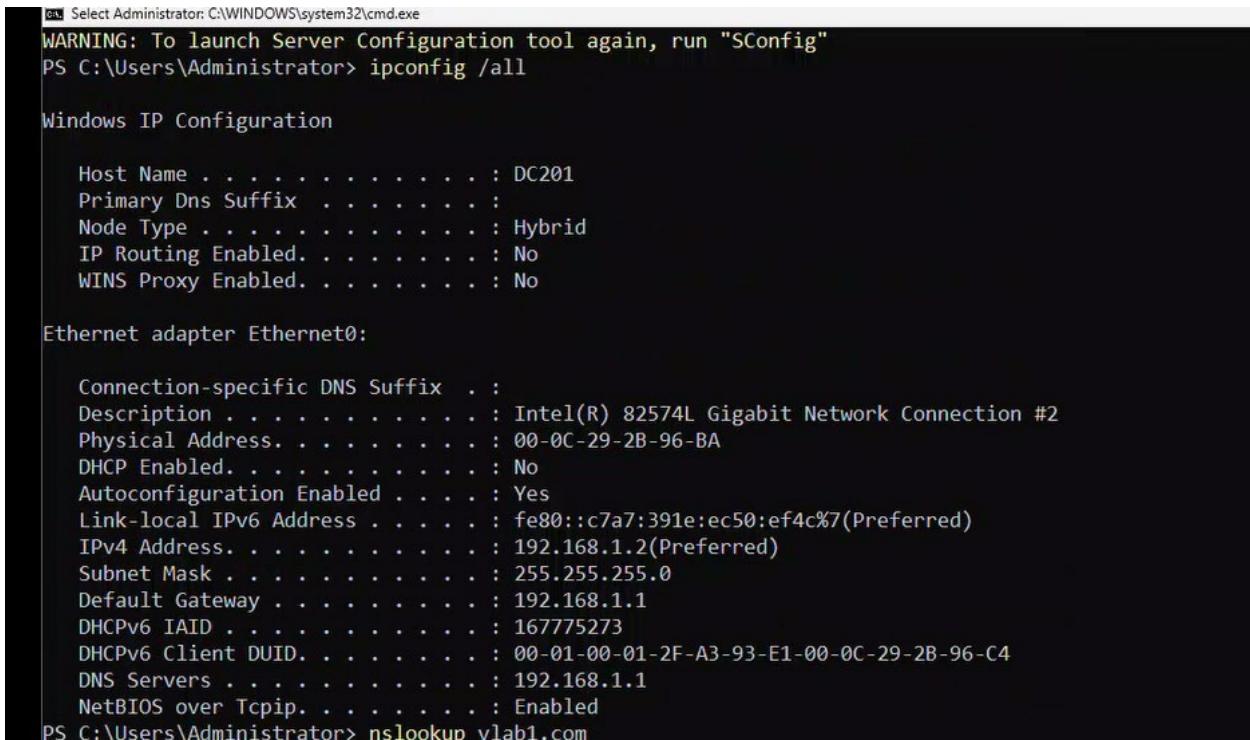
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\administrator> whoami
vlabs1\administrator
PS C:\Users\administrator>
```

## 5 Step 3: Configure DC201 as a Domain Controller Replica for vlabs1.com

1. Verify DC Configuration.
2. Test AD Replication.
3. List AD Objects (Users, Groups, OUs).

Verify config in DC201



```
Select Administrator: C:\WINDOWS\system32\cmd.exe
WARNING: To launch Server Configuration tool again, run "SConfig"
PS C:\Users\Administrator> ipconfig /all

Windows IP Configuration

Host Name . . . . . : DC201
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) 82574L Gigabit Network Connection #2
Physical Address. . . . . : 00-0C-29-2B-96-BA
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c7a7:391e:ec50:ef4c%7(PREFERRED)
IPv4 Address. . . . . : 192.168.1.2(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 167775273
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-A3-93-E1-00-0C-29-2B-96-C4
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
PS C:\Users\Administrator> nslookup vlabs1.com
```

Make sure you can control DNS

```
PS C:\Users\Administrator> ^C
PS C:\Users\Administrator> nslookup vlabs1.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  192.168.1.1

Name:      vlabs1.com
Address:   192.168.1.1

PS C:\Users\Administrator>
```

## 5.1 Promote DC201 as DC for vlabs1.com (Not Global Catalog).

### 5.1.1 Add a RODC(Core) to an existing domain

1. Using PowerShell, join **DC201** to the Domain

#### **Install-WindowsFeature AD-Domain-Services -IncludeManagementTools**

```
Administrator: C:\WINDOWS\system32\cmd.exe
PS C:\Users\Administrator> Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
Success Restart Needed Exit Code      Feature Result
----- -----           ----- {Active Directory Domain Services, Group P...
True   No            Success          {Active Directory Domain Services, Group P...
```

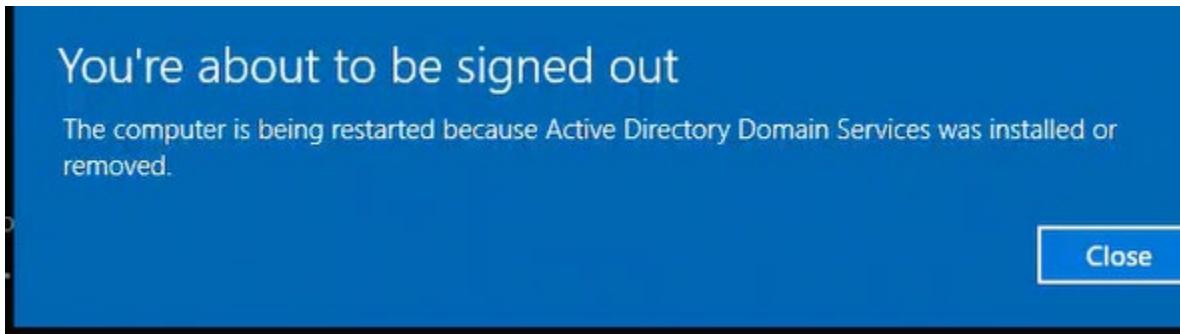
```
PS C:\Users\Administrator>
```

2. Promote a server as a Domain Controller for the Active Directory domain vlabs1.com

```
Install-ADDSDomainController-DomainName"vlabs1.com" -Credential (Get-Credential) -
ReadOnlyReplica-InstallDns-SiteName "Default-First-Site-Name" -NoGlobalCatalog:$false -
LogPath "C:\Windows\NTDS" –SysvolPath "C:\Windows\SYSVOL" -Force
```



Passwords will be asked again, and restart will be initiated automatically



## 5.1.2 Verifying the RODC Installation

### 5.1.2.1 Verify if the server is a Domain Controller

**Get-ADDomainController -Identity "DC201"**

```

PS C:\Users\Administrator> Get-ADDomainController -Identity "DC201"

ComputerObjectDN      : CN=DC201,OU=Domain Controllers,DC=vlabs1,DC=com
DefaultPartition       : DC=vlabs1,DC=com
Domain                : vlabs1.com
Enabled               : True
Forest                : vlabs1.com
HostName              : DC201.vlabs1.com
InvocationId          : 00000000-0000-0000-0000-000000000000
IPv4Address           : 192.168.1.2
IPv6Address           :
IsGlobalCatalog       : True
IsReadOnly             : True
LdapPort              : 389
Name                  : DC201
NTDSSettingsObjectDN : CN=NTDS Settings,CN=DC201,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
OperatingSystem        : Windows Server 2025 Standard
OperatingSystemHotfix  :
OperatingSystemServicePack:
OperatingSystemVersion : 10.0 (26100)
OperationMasterRoles   : {}
Partitions             : {CN=Schema,CN=Configuration,DC=vlabs1,DC=com, CN=Configuration,DC=vlabs1,DC=com, DC=vlabs1,DC=com}
ServerObjectDN         : CN=DC201,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
ServerObjectGuid       : 31d1cc60-d7d6-4f15-9dab-8bf15bcc428e
Site                  : Default-First-Site-Name
SslPort               : 636

PS C:\Users\Administrator>

```

### 5.1.2.2 Check if the server is an RODC

**Get-ADDomainController -Filter \* | Select Name, IsReadOnly**

```

PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADDomainController -Filter * | Select Name, IsReadOnly

Name  IsReadOnly
---- -
DC101 False
DC201 True

PS C:\Users\Administrator>

```

### 5.1.2.3 In Server DC101

Tool Active Directory Sites and Services

| Name  | Domain     | Bridgehead | DC Type | Description   |
|-------|------------|------------|---------|---------------|
| DC101 | vlabs1.com |            | GC      |               |
| DC201 | vlabs1.com |            | GC      | Read-only, GC |

#### 5.1.2.4 From a writable DC (DC101)

1. Verify Replication:

**Readmin /showrepl**

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> repadmin /showrepl

Readmin: running command /showrepl against full DC localhost
Default-First-Site-Name\DC101
DSA Options: IS_GC
Site Options: (none)
DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
DSA invocationID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87

PS C:\Users\Administrator>
```

2. To replicate from the writable DC to RODC:

**Readmin /syncall**

```
PS C:\Users\Administrator> repadmin /syncall
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

PS C:\Users\Administrator>
```

3. Force the replication manually:

**repadmin/ syncall /Adept**

#### 5.1.2.5 From RODC (DC201):

##### 5.1.2.5.1 Verify Replication

**repadmin/showrepl**

```
PS C:\Users\Administrator.VLABS1> repadmin /showrepl

Repadmin: running command /showrepl against full DC localhost
Default-First-Site-Name\DC201
DSA Options: IS_GC DISABLE_OUTBOUND_REPL IS_RODC
Site Options: (none)
DSA object GUID: bae489a-95f5-48de-a56d-9b7dadfb57fd
DSA invocationID: bcc25508-7de9-42e0-b28f-062e6682cf71

===== INBOUND NEIGHBORS =====

DC=vlabs1,DC=com
  Default-First-Site-Name\DC101 via RPC
    DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
    Last attempt @ 2025-05-05 12:32:29 was successful.

CN=Configuration,CN=Configuration,DC=vlabs1,DC=com
  Default-First-Site-Name\DC101 via RPC
    DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
    Last attempt @ 2025-05-05 11:56:20 was successful.

CN=Schema,CN=Configuration,DC=vlabs1,DC=com
  Default-First-Site-Name\DC101 via RPC
    DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
    Last attempt @ 2025-05-05 11:56:20 was successful.

DC=DomainDnsZones,DC=vlabs1,DC=com
  Default-First-Site-Name\DC101 via RPC
    DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
    Last attempt @ 2025-05-05 11:56:20 was successful.

DC=ForestDnsZones,DC=vlabs1,DC=com
  Default-First-Site-Name\DC101 via RPC
    DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
    Last attempt @ 2025-05-05 11:56:20 was successful.

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

### 5.1.2.5.2 List AD Objects (Users, Groups, OUs):

**Get-ADUser -Filter \***

```
PS C:\Users\Administrator.VLABS1> Get-ADUser -Filter *

DistinguishedName : CN=Guest,CN=Users,DC=vlabs1,DC=com
Enabled          : False
GivenName        :
Name              : Guest
ObjectClass      : user
ObjectGUID       : 20d66d19-6340-477f-bc89-66c90ad43855
SamAccountName   : Guest
SID               : S-1-5-21-1268601764-4050707287-4025116504-501
Surname          :
UserPrincipalName :

DistinguishedName : CN=Administrator,CN=Users,DC=vlabs1,DC=com
Enabled          : True
GivenName        :
Name              : Administrator
ObjectClass      : user
ObjectGUID       : faf775cd-17fc-4117-a3ec-0e97672130fd
SamAccountName   : Administrator
SID               : S-1-5-21-1268601764-4050707287-4025116504-500
Surname          :
UserPrincipalName :

DistinguishedName : CN=krbtgt,CN=Users,DC=vlabs1,DC=com
Enabled          : False
GivenName        :
Name              : krbtgt
ObjectClass      : user
ObjectGUID       : 8730b3db-2a32-4e4f-a33e-f604b27047df
SamAccountName   : krbtgt
SID               : S-1-5-21-1268601764-4050707287-4025116504-502
Surname          :
UserPrincipalName :

DistinguishedName : CN=krbtgt_24591,CN=Users,DC=vlabs1,DC=com
Enabled          : False
GivenName        :
Name              : krbtgt_24591
ObjectClass      : user
ObjectGUID       : bb66ef22-79aa-49c4-8dd8-eedb28ee4cbf
SamAccountName   : krbtgt_24591
SID               : S-1-5-21-1268601764-4050707287-4025116504-1105
Surname          :
UserPrincipalName :
```

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

**Get-ADGroup -Filter \***

```
PS C:\Users\Administrator.VLABS1> Get-ADGroup -Filter *
```

```
DistinguishedName : CN=Administrators,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Administrators
ObjectClass       : group
ObjectGUID        : 8f48efe0-dc95-440d-a591-74e62b578dab
SamAccountName   : Administrators
SID               : S-1-5-32-544

DistinguishedName : CN=Users,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Users
ObjectClass       : group
ObjectGUID        : fc705250-ebe6-4173-8cba-821f6249ee99
SamAccountName   : Users
SID               : S-1-5-32-545

DistinguishedName : CN=Guests,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Guests
ObjectClass       : group
ObjectGUID        : 1b161632-6baa-43fb-b182-67f0cfcc2e316
SamAccountName   : Guests
SID               : S-1-5-32-546

DistinguishedName : CN=Remote Desktop Users,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Remote Desktop Users
ObjectClass       : group
ObjectGUID        : ee804a45-d4d3-4604-91ef-d44e8d45ec12
SamAccountName   : Remote Desktop Users
SID               : S-1-5-32-555

DistinguishedName : CN=Network Configuration Operators,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Network Configuration Operators
ObjectClass       : group
ObjectGUID        : 58422ac1-0153-4494-879b-bb42ae626ef8
SamAccountName   : Network Configuration Operators
SID               : S-1-5-32-556
```

```
DistinguishedName : CN=Performance Monitor Users,CN=Builtin,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Performance Monitor Users
ObjectClass       : group
ObjectGUID        : 9e2c02e2-078a-45ff-9233-de0cd5756e5b
SamAccountName   : Performance Monitor Users
SID               : S-1-5-32-558

DistinguishedName : CN=Performance Log Users,CN=Builtin,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Performance Log Users
ObjectClass       : group
ObjectGUID        : 8e40dbd9-a8fc-46fd-b1ff-0850c2b9901e
SamAccountName   : Performance Log Users
SID               : S-1-5-32-559

DistinguishedName : CN=Distributed COM Users,CN=Builtin,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Distributed COM Users
ObjectClass       : group
ObjectGUID        : 2eb5f259-42e6-4f00-8e55-0c2fb0be9033
SamAccountName   : Distributed COM Users
SID               : S-1-5-32-562

DistinguishedName : CN=IIS_IUSRS,CN=Builtin,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : IIS_IUSRS
ObjectClass       : group
ObjectGUID        : 66b7fd6c-08bf-45a9-8b7d-a3a884e528f8
SamAccountName   : IIS_IUSRS
SID               : S-1-5-32-568

DistinguishedName : CN=Cryptographic Operators,CN=Builtin,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Cryptographic Operators
ObjectClass       : group
ObjectGUID        : 5f127b27-4019-4685-b95f-62870c001ae5
SamAccountName   : Cryptographic Operators
SID               : S-1-5-32-569
```

```
PS Select Administrator: C:\WINDOWS\system32\cmd.exe
DistinguishedName : CN=Event Log Readers,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Event Log Readers
ObjectClass       : group
ObjectGUID        : 9a53da7c-c45c-47ef-8ae3-14d6cc97ebd2
SamAccountName   : Event Log Readers
SID               : S-1-5-32-573

DistinguishedName : CN=Certificate Service DCOM Access,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Certificate Service DCOM Access
ObjectClass       : group
ObjectGUID        : 4c699344-f57c-45e6-9eab-573b99d7b7ed
SamAccountName   : Certificate Service DCOM Access
SID               : S-1-5-32-574

DistinguishedName : CN=RDS Remote Access Servers,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : RDS Remote Access Servers
ObjectClass       : group
ObjectGUID        : f972b9f6-b894-472b-ab59-3350f491b607
SamAccountName   : RDS Remote Access Servers
SID               : S-1-5-32-575

DistinguishedName : CN=RDS Endpoint Servers,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : RDS Endpoint Servers
ObjectClass       : group
ObjectGUID        : f334f48c-3e42-4044-a57b-0ad423c5f3d1
SamAccountName   : RDS Endpoint Servers
SID               : S-1-5-32-576

DistinguishedName : CN=RDS Management Servers,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : RDS Management Servers
ObjectClass       : group
ObjectGUID        : 5086b440-b35b-490d-9490-df69602bd83d
SamAccountName   : RDS Management Servers
SID               : S-1-5-32-577
```

```
PS Select Administrator: C:\WINDOWS\system32\cmd.exe
Name          : Hyper-V Administrators
ObjectClass   : group
ObjectGUID    : 1ab42a01-797e-45be-8fd8-c93875801e00
SamAccountName : Hyper-V Administrators
SID           : S-1-5-32-578

DistinguishedName : CN=Access Control Assistance Operators,CN=Builtin,DC=vlabs1,DC=com
GroupCategory   : Security
GroupScope      : DomainLocal
Name           : Access Control Assistance Operators
ObjectClass    : group
ObjectGUID     : b302274c-79f4-4a30-9ebd-b7c3a5e7c076
SamAccountName : Access Control Assistance Operators
SID           : S-1-5-32-579

DistinguishedName : CN=Remote Management Users,CN=Builtin,DC=vlabs1,DC=com
GroupCategory   : Security
GroupScope      : DomainLocal
Name           : Remote Management Users
ObjectClass    : group
ObjectGUID     : b4f7bcc4-d14a-4bb5-a5cd-3b5a99fe0445
SamAccountName : Remote Management Users
SID           : S-1-5-32-580

DistinguishedName : CN=Storage Replica Administrators,CN=Builtin,DC=vlabs1,DC=com
GroupCategory   : Security
GroupScope      : DomainLocal
Name           : Storage Replica Administrators
ObjectClass    : group
ObjectGUID     : d404966c-917d-4be1-bfe6-85d7d5a08b4e
SamAccountName : Storage Replica Administrators
SID           : S-1-5-32-582

DistinguishedName : CN=Domain Computers,CN=Users,DC=vlabs1,DC=com
GroupCategory   : Security
GroupScope      : Global
Name           : Domain Computers
ObjectClass    : group
ObjectGUID     : a356a5e9-c6a6-4404-ae0a-52d02c23316d
SamAccountName : Domain Computers
SID           : S-1-5-21-1268601764-4050707287-4025116504-515
```

```
PS Select Administrator: C:\WINDOWS\system32\cmd.exe
DistinguishedName : CN=Cert Publishers,CN=Users,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Cert Publishers
ObjectClass       : group
ObjectGUID        : 14ceb6df-ae40-41ef-92ef-134321732b3f
SamAccountName   : Cert Publishers
SID               : S-1-5-21-1268601764-4050707287-4025116504-517

DistinguishedName : CN=Domain Users,CN=Users,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : Global
Name              : Domain Users
ObjectClass       : group
ObjectGUID        : ba9d6b13-049f-49e7-a383-a71b17fc7b07
SamAccountName   : Domain Users
SID               : S-1-5-21-1268601764-4050707287-4025116504-513

DistinguishedName : CN=Domain Guests,CN=Users,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : Global
Name              : Domain Guests
ObjectClass       : group
ObjectGUID        : a5bb8886-35f9-4bfd-9358-d3de531f7d5b
SamAccountName   : Domain Guests
SID               : S-1-5-21-1268601764-4050707287-4025116504-514

DistinguishedName : CN=RAS and IAS Servers,CN=Users,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : RAS and IAS Servers
ObjectClass       : group
ObjectGUID        : 60daaab7-8c95-4ce4-af9e-62559d291cac
SamAccountName   : RAS and IAS Servers
SID               : S-1-5-21-1268601764-4050707287-4025116504-553

DistinguishedName : CN=Incoming Forest Trust Builders,CN=Builtin,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Incoming Forest Trust Builders
ObjectClass       : group
ObjectGUID        : af95f5a4-1c62-4f93-9f2c-62ecd7b48fb8
SamAccountName   : Incoming Forest Trust Builders
SID               : S-1-5-32-557

DistinguishedName : CN=Terminal Server License Servers,CN=Builtin,DC=vlabs1,DC=com
```

```
DistinguishedName : CN=Terminal Server License Servers,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory      : Security
GroupScope         : DomainLocal
Name               : Terminal Server License Servers
ObjectClass        : group
ObjectGUID         : aeca360b-c793-48e1-a374-0ec5f8e35027
SamAccountName    : Terminal Server License Servers
SID                : S-1-5-32-561

DistinguishedName : CN=Domain Admins,CN=Users,DC=vlabs1,DC=com
GroupCategory      : Security
GroupScope         : Global
Name               : Domain Admins
ObjectClass        : group
ObjectGUID         : fe7ad86c-9953-4e3c-a719-6ac6927f4b8b
SamAccountName    : Domain Admins
SID                : S-1-5-21-1268601764-4050707287-4025116504-512

DistinguishedName : CN=Schema Admins,CN=Users,DC=vlabs1,DC=com
GroupCategory      : Security
GroupScope         : Universal
Name               : Schema Admins
ObjectClass        : group
ObjectGUID         : 9f8f83fb-3357-48b5-98e9-65ad3e092c1a
SamAccountName    : Schema Admins
SID                : S-1-5-21-1268601764-4050707287-4025116504-518

DistinguishedName : CN=Enterprise Admins,CN=Users,DC=vlabs1,DC=com
GroupCategory      : Security
GroupScope         : Universal
Name               : Enterprise Admins
ObjectClass        : group
ObjectGUID         : b3823127-1974-42d3-86e1-880058b0f4aa
SamAccountName    : Enterprise Admins
SID                : S-1-5-21-1268601764-4050707287-4025116504-519

DistinguishedName : CN=Group Policy Creator Owners,CN=Users,DC=vlabs1,DC=com
GroupCategory      : Security
GroupScope         : Global
Name               : Group Policy Creator Owners
ObjectClass        : group
ObjectGUID         : 4b92c347-145d-4465-ae5e-75fb472774ad
SamAccountName    : Group Policy Creator Owners
SID                : S-1-5-21-1268601764-4050707287-4025116504-520

DistinguishedName : CN=Pre-Windows 2000 Compatible Access,CN=BuiltIn,DC=vlabs1,DC=com
```

```

DistinguishedName : CN=Pre-Windows 2000 Compatible Access,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory    : Security
GroupScope       : DomainLocal
Name             : Pre-Windows 2000 Compatible Access
ObjectClass      : group
ObjectGUID       : 68f73fc9-5621-4e78-96e4-fa02c7037814
SamAccountName   : Pre-Windows 2000 Compatible Access
SID              : S-1-5-32-554

DistinguishedName : CN=Windows Authorization Access Group,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory    : Security
GroupScope       : DomainLocal
Name             : Windows Authorization Access Group
ObjectClass      : group
ObjectGUID       : 2f7de5d1-baeb-4d21-ad9c-ce0f35cfa940
SamAccountName   : Windows Authorization Access Group
SID              : S-1-5-32-560

DistinguishedName : CN=Allowed RODC Password Replication Group,CN=Users,DC=vlabs1,DC=com
GroupCategory    : Security
GroupScope       : DomainLocal
Name             : Allowed RODC Password Replication Group
ObjectClass      : group
ObjectGUID       : 27efe94d-5b77-4fce-94cc-83aa4b47195e
SamAccountName   : Allowed RODC Password Replication Group
SID              : S-1-5-21-1268601764-4050707287-4025116504-571

DistinguishedName : CN=Denied RODC Password Replication Group,CN=Users,DC=vlabs1,DC=com
GroupCategory    : Security
GroupScope       : DomainLocal
Name             : Denied RODC Password Replication Group
ObjectClass      : group
ObjectGUID       : 5a1e43b5-8024-4f6c-a263-3b9d2c85128b
SamAccountName   : Denied RODC Password Replication Group
SID              : S-1-5-21-1268601764-4050707287-4025116504-572

DistinguishedName : CN=Enterprise Read-only Domain Controllers,CN=Users,DC=vlabs1,DC=com
GroupCategory    : Security
GroupScope       : Universal
Name             : Enterprise Read-only Domain Controllers
ObjectClass      : group
ObjectGUID       : d45a9869-2216-4720-843d-e70c9a5fb1cb
SamAccountName   : Enterprise Read-only Domain Controllers
SID              : S-1-5-21-1268601764-4050707287-4025116504-498

DistinguishedName : CN=Cloneable Domain Controllers,CN=Users,DC=vlabs1,DC=com

```

## Get-ADOrganizationalUnit -Filter \*

```

PS C:\Administrator: C:\WINDOWS\system32\cmd.exe
PS C:\Users\Administrator.VLABS1> Get-ADOrganizationalUnit -Filter *

City          :
Country       :
DistinguishedName : OU=Domain Controllers,DC=vlabs1,DC=com
LinkedGroupPolicyObjects : {CN={6AC1786C-016F-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=vlabs1,DC=com}
ManagedBy     :
Name          : Domain Controllers
ObjectClass   : organizationalUnit
ObjectGUID    : 51bc9792-b0b2-4870-8367-e872172012ad
PostalCode    :
State         :
StreetAddress :

```

PS C:\Users\Administrator.VLABS1> ■

## 6 Step 4: Deploy DC301 as a Child Domain (lab1.vlabs1.com) using PowerShell

### 6.1 Using PowerShell, promote DC301 as a Child Domain for lab1.vlabs1.com.

In DC301

**Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools**

```
PS C:\Users\Administrator> Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
Success Restart Needed Exit Code      Feature Result
----- ----- ----- -----
True    No        Success          {Active Directory Domain Services, Group P...
PS C:\Users\Administrator> ■
```

```
PS C:\Users\Administrator> Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
Success Restart Needed Exit Code      Feature Result
----- ----- ----- -----
True    No        Success          {Active Directory Domain Services, Group P...
PS C:\Users\Administrator> Install-ADDSDomain `>> -NoGlobalCatalog:$false `>> -CreateDnsDelegation:$true `>> -Credential (Get-Credential) `>> -DatabasePath "C:\Windows\NTDS" `>> -DomainMode "winThreshold" `>> -DomainType "ChildDomain" `>> -InstallDns:$true `>> -LogPath "C:\Windows\NTDS" `>> -NewDomainName "lab1" `>> -NewDomainNetbiosName "LAB1" `>> -ParentDomainName "vlabs1.com" `>> -NoRebootOnCompletion:$false `>> -SiteName "Default-First-Site-Name" `>> -SysvolPath "C:\Windows\SYSVOL" `>> -Force:$true

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
```

A screenshot of a Windows PowerShell credential request dialog box. It has a blue header bar with the text 'Windows PowerShell credential request'. Below the header is a logo of a key and a lock. The main area contains the text 'Enter your credentials.' followed by two input fields: 'User name:' with a placeholder '@' and 'Password:' with a placeholder 'password'. At the bottom right are 'OK' and 'Cancel' buttons.

|      |    |         |   |
|------|----|---------|---|
| True | No | Success | {Active Directory Domain Services, Group 1} |
|------|----|---------|---|

```

PS C:\Users\Administrator> Install-ADDSDomain
>> -NoGlobalCatalog:$false
>> -CreateDnsDelegation:$true
>> -Credential (Get-Credential)
>> -DatabasePath "C:\Windows\NTDS"
>> -DomainMode "winThreshold"
>> -DomainType "ChildDomain"
>> -InstallDns:$true
>> -LogPath "C:\Windows\NTDS"
>> -NewDomainName "lab1"
>> -NewDomainNetbiosName "LAB1"
>> -ParentDomainName "vlabs1.com"
>> -NoRebootOnCompletion:$false
>> -SiteName "Default-First-Site-Name"
>> -SysvolPath "C:\Windows\SYSVOL"
>> -Force:$true

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
SafeModeAdministratorPassword: *****

```

```

PS C:\Users\Administrator> Install-ADDSDomain
>> -NoGlobalCatalog:$false
>> -CreateDnsDelegation:$true
>> -Credential (Get-Credential)
>> -DatabasePath "C:\Windows\NTDS"
>> -DomainMode "winThreshold"
>> -DomainType "ChildDomain"
>> -InstallDns:$true
>> -LogPath "C:\Windows\NTDS"
>> -NewDomainName "lab1"
>> -NewDomainNetbiosName "LAB1"
>> -ParentDomainName "vlabs1.com"
>> -NoRebootOnCompletion:$false
>> -SiteName "Default-First-Site-Name"
>> -SysvolPath "C:\Windows\SYSVOL"
>> -Force:$true

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
SafeModeAdministratorPassword: *****
Confirm SafeModeAdministratorPassword: *****
WARNING: Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing sessions.

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
```

Activate Windows  
Go to Settings to activate Windows.

WARNING: Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing sessions.

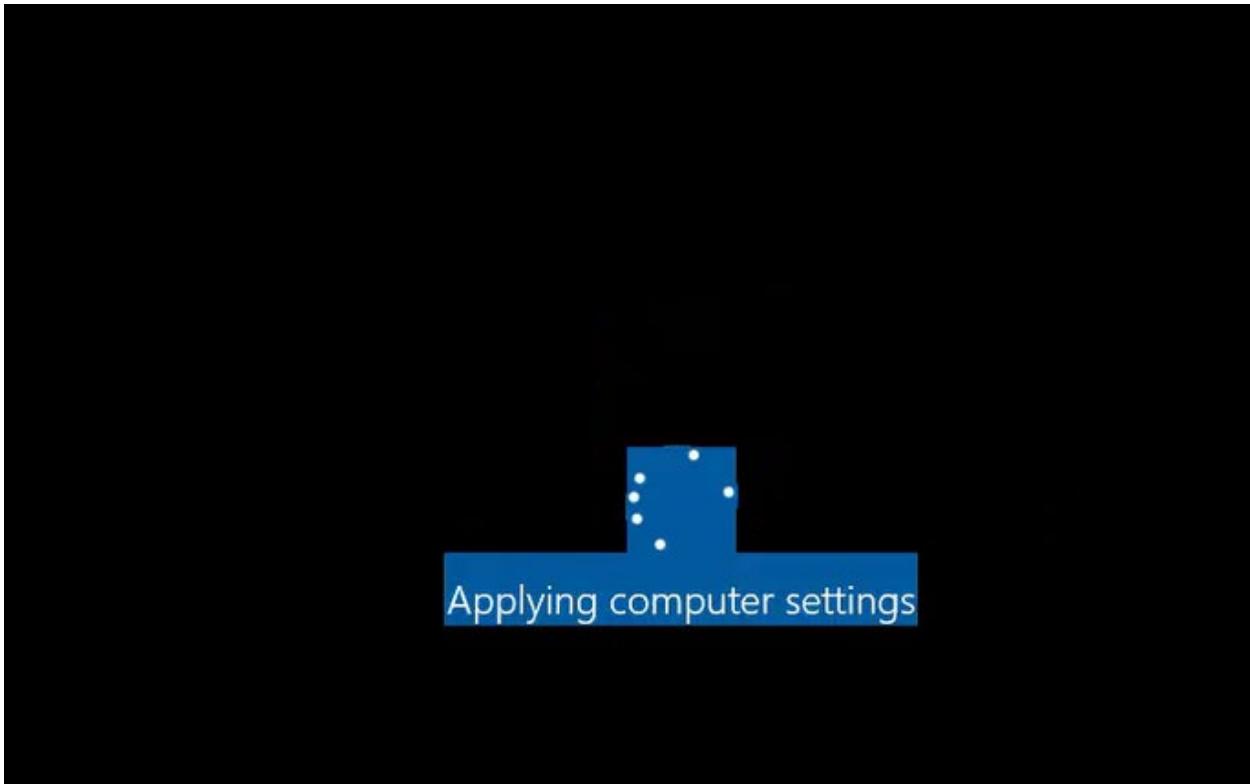
```

PS C:\Users\Administrator Install-ADDSDomain
>> -NoGlobalCatalog:$false
>> -CreateDsDelegation:$true
>> -Credential (Get-Credential)
>> -DatabasePath "C:\Windows\ITDS"
>> -DomainMode "winThreshold"
>> -DomainType "ChildDomain"
>> -InstallLogs:$true
>> -LogonAddress "[WINS]NTDS"
>> -NewDomainName "lab1"
>> -NewDomainNetbiosName "lab1"
>> -ParentDomainName "vlabs1.com"
>> -NoRebootOnCompletion:$false
>> -SiteName "Default-First-Site-Name"
>> -SysvolPath "C:\Windows\SYSVOL"
>> -Force:$true

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
[Credential]
SafeModeAdministratorPassword: *****
Confirm SafeModeAdministratorPassword: *****
WARNING: Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
WARNING: Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

```

You're about to be signed out  
The computer is being restarted because Active Directory Domain Services was installed or removed.  
Close



## 6.2 Verify the Child Domain Setup.

### 6.2.1 In DC301

1. Retrieve detailed Active Directory domain information

`Get-ADDomain | Format-List *`

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADDomain | Format-List *
```

|                                    |  |
|------------------------------------|--|
| AllowedDNSSuffixes                 | : {}   |
| ChildDomains                       | : {}   |
| ComputersContainer                 | : CN=Computers,DC=lab1,DC=vlabs1,DC=com  |
| DeletedObjectsContainer            | : CN=Deleted Objects,DC=lab1,DC=vlabs1,DC=com  |
| DistinguishedName                  | : DC=lab1,DC=vlabs1,DC=com   |
| DNSRoot                            | : lab1.vlabs1.com  |
| DomainControllersContainer         | : OU=Domain Controllers,DC=lab1,DC=vlabs1,DC=com   |
| DomainNode                         | : Windows20160main   |
| DomainID                           | : S-1-5-21-327770921-3136444610-3217977211   |
| ForeignSecurityPrincipalsContainer | : CN=ForeignSecurityPrincipals,DC=lab1,DC=vlabs1,DC=com                                    |
| Forest                             | : vlabs1.com   |
| InfrastructureMaster               | : DC301.lab1.vlabs1.com  |
| LastLogonReplicationInterval       | :  |
| LinkedGroupPolicyObjects           | : {CN={31B2F340-0160-11D2-945F-00C04FB984F9},CN=Policy,CN=System,DC=lab1,DC=vlabs1,DC=com} |
| LostAndFoundContainer              | : CN=LostAndFound,DC=lab1,DC=vlabs1,DC=com   |
| ManagedBy                          | :  |
| Name                               | : lab1   |
| NetBIOSName                        | : LAB1   |
| ObjectClass                        | : domainDNS  |
| ObjectGUID                         | : 1322c581-a93a-40b0-998e-ab1256a52e7d   |
| ParentDomain                       | : vlabs1.com   |
| PDCEmulator                        | : DC301.lab1.vlabs1.com  |
| PublicKeyRequiredPasswordRolling   | : True   |
| QuotasContainer                    | : CN=NTDS Quotas,DC=lab1,DC=vlabs1,DC=com  |
| ReadOnlyReplicaDirectoryServers    | : {}   |
| ReplicaDirectoryServers            | : {DC301.lab1.vlabs1.com}  |
| RIDMaster                          | : DC301.lab1.vlabs1.com  |
| SubContainerReferences             | : {DC=Configuration,DC=vlabs1,DC=com,DC=System,DC=lab1,DC=vlabs1,DC=com}                   |
| SystemContainer                    | : CN=System,DC=lab1,DC=vlabs1,DC=com   |
| UsersContainer                     | : CN=Users,DC=lab1,DC=vlabs1,DC=com  |
| PropertyNames                      | : {AllowedDNSSuffixes, ChildDomains, ComputersContainer, DeletedObjectsContainer...}       |
| AddedProperties                    | : {}   |
| RemovedProperties                  | : {}   |
| ModifiedProperties                 | : {PublicKeyRequiredPasswordRolling}   |
| PropertyCount                      | : 30   |

## 2. Display the replication status of Active Directory domain controllers.

### Readmin /showrepl

```
PS C:\Users\Administrator> Repadmin /showrepl

Readmin: running command /showrepl against full DC localhost
Default-First-Site-Name\DC301
DSA Options: IS_GC
Site Options: (none)
DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
DSA invocationID: 5de39122-8c54-4e68-9a4a-2cde0aaa094b

===== INBOUND NEIGHBORS =====

CN=Configuration,DC=vlabs1,DC=com
    Default-First-Site-Name\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-05 15:48:44 was successful.

CN=Schema,CN=Configuration,DC=vlabs1,DC=com
    Default-First-Site-Name\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-05 15:48:44 was successful.

DC=ForestDnsZones,DC=vlabs1,DC=com
    Default-First-Site-Name\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-05 15:48:44 was successful.

DC=vlabs1,DC=com
    Default-First-Site-Name\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-05 16:31:28 was successful.

PS C:\Users\Administrator>
```

## 3. Overview of Active Directory replication status

### Readmin /replicsummary

```

PS C:\Users\Administrator>
PS C:\Users\Administrator> Repadmin /replsummary
Replication Summary Start Time: 2025-05-05 14:33:21

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



Source DSA      largest delta    fails/total %%   error
DC101           44m:37s     0 / 10    0
DC301           43m:46s     0 /  8    0



Destination DSA      largest delta    fails/total %%   error
DC101            43m:46s     0 /  4    0
DC201            37m:02s     0 / 10    0
DC301            44m:37s     0 /  4    0



PS C:\Users\Administrator> Repadmin /showopen

```

#### 4. Verify AD DNS entries

Query the DNS server to resolve the domain name lab1.vlabs1.com and return its associated IP address.

#### **Resolve-DnsName lab1.vlabs1.com**

```

Last attempt @ 2025-05-05 14:33:20 was successful.

PS C:\Users\Administrator> Resolve-DnsName lab1.vlabs1.com

Name                           Type    TTL   Section   IPAddress
----                           ----   --   -----   -----
lab1.vlabs1.com                A       600  Answer   192.168.1.3

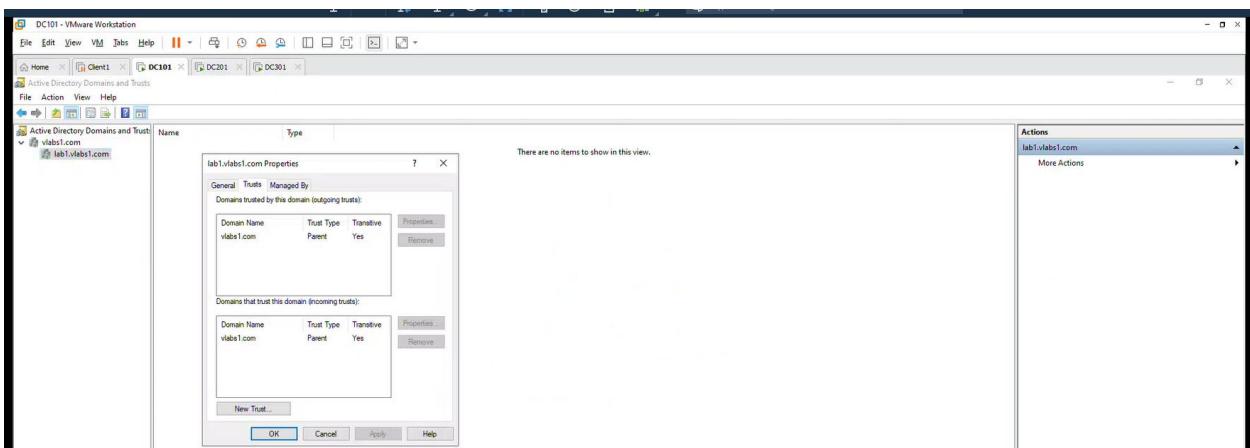
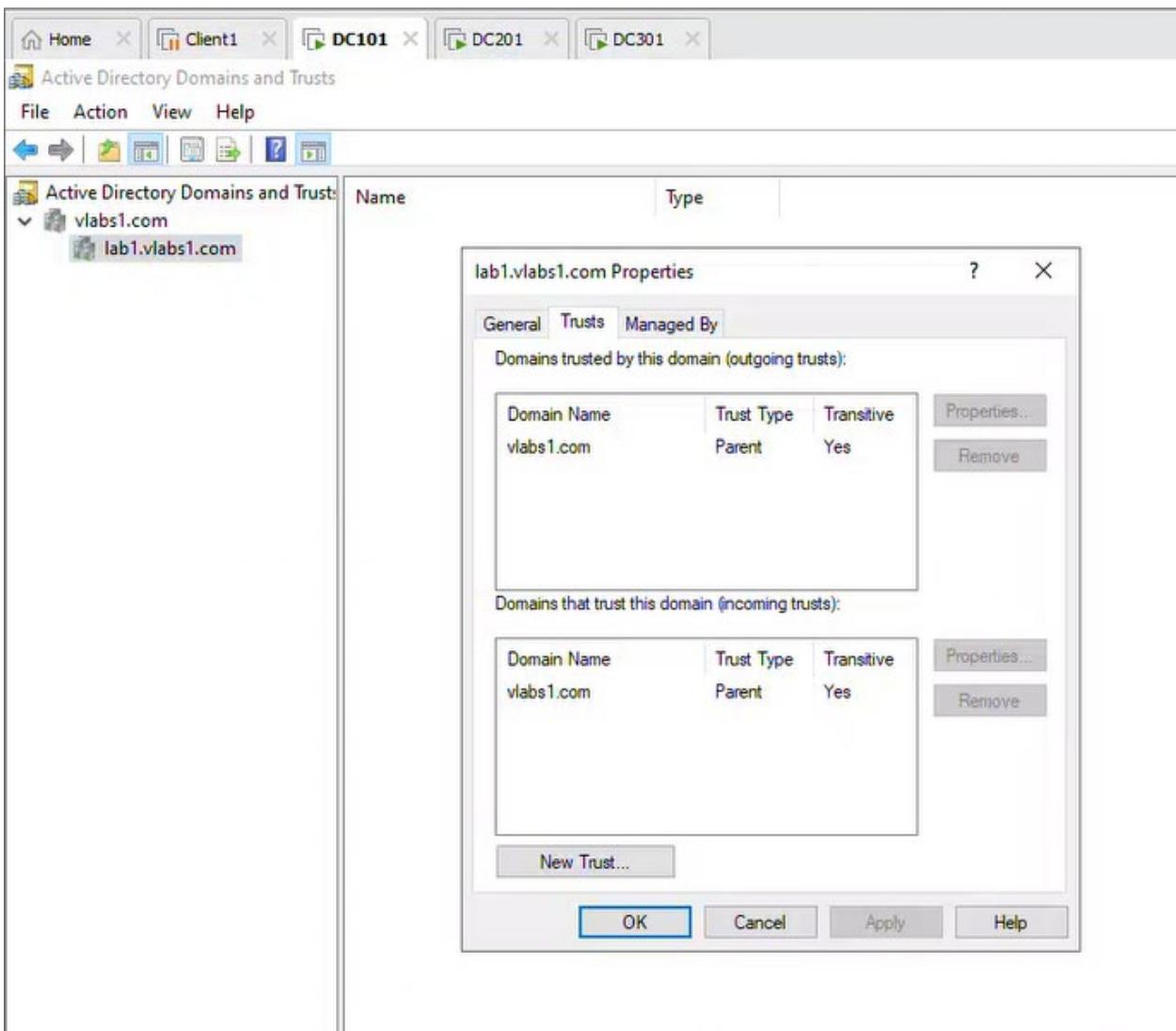
PS C:\Users\Administrator>

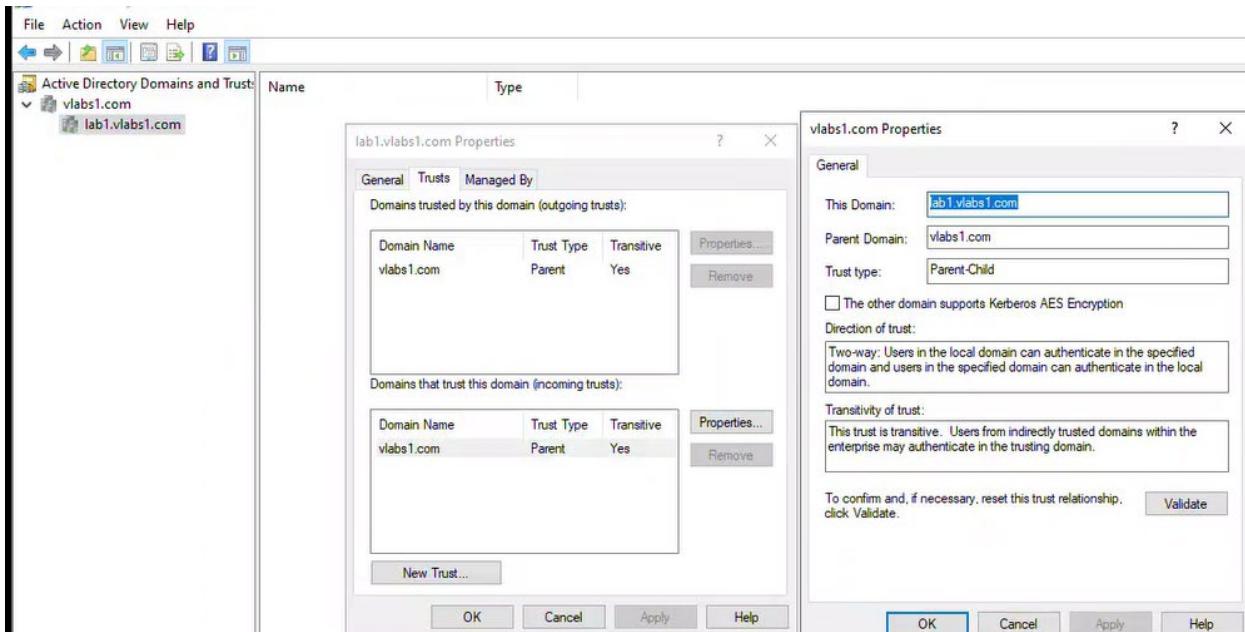
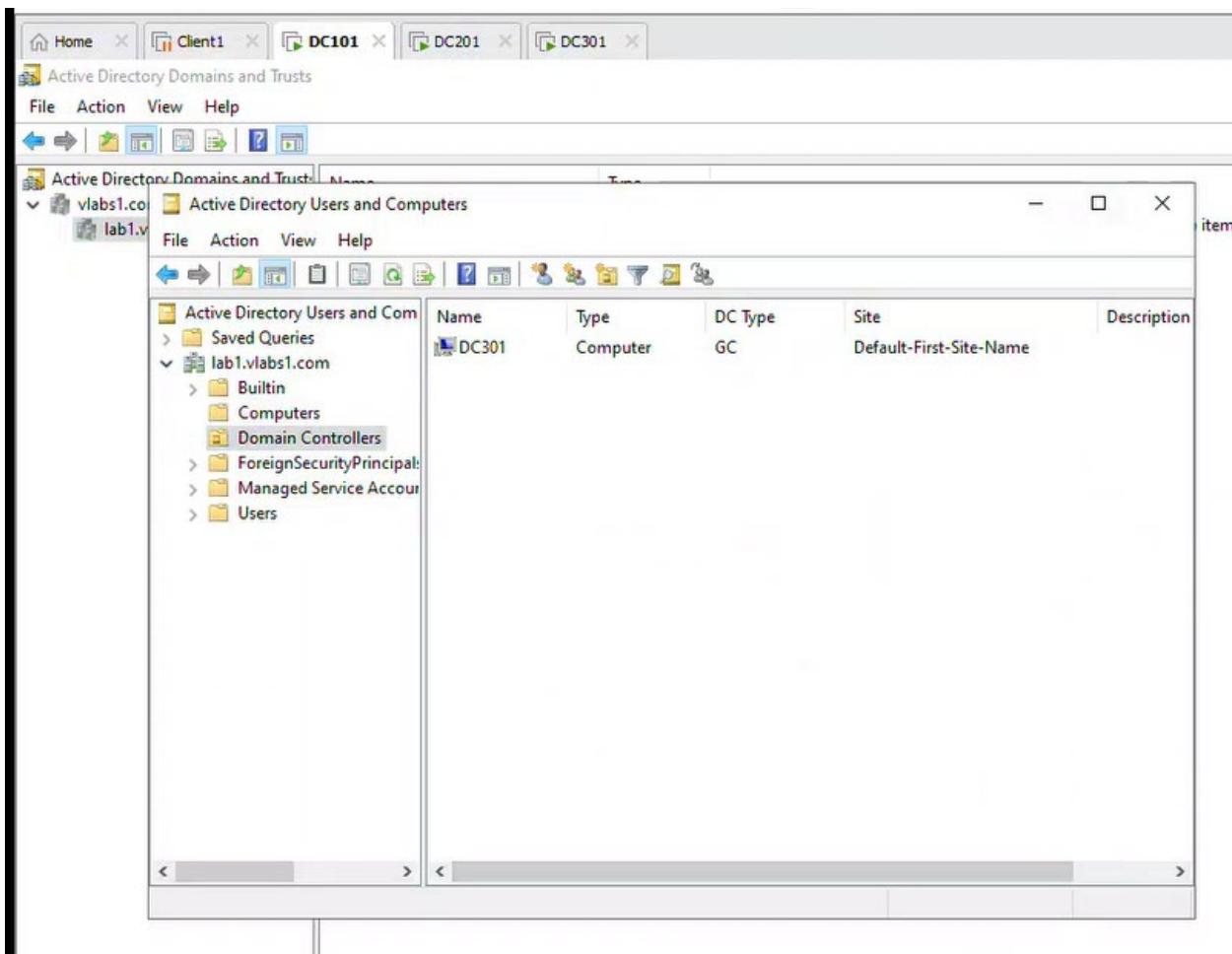
```

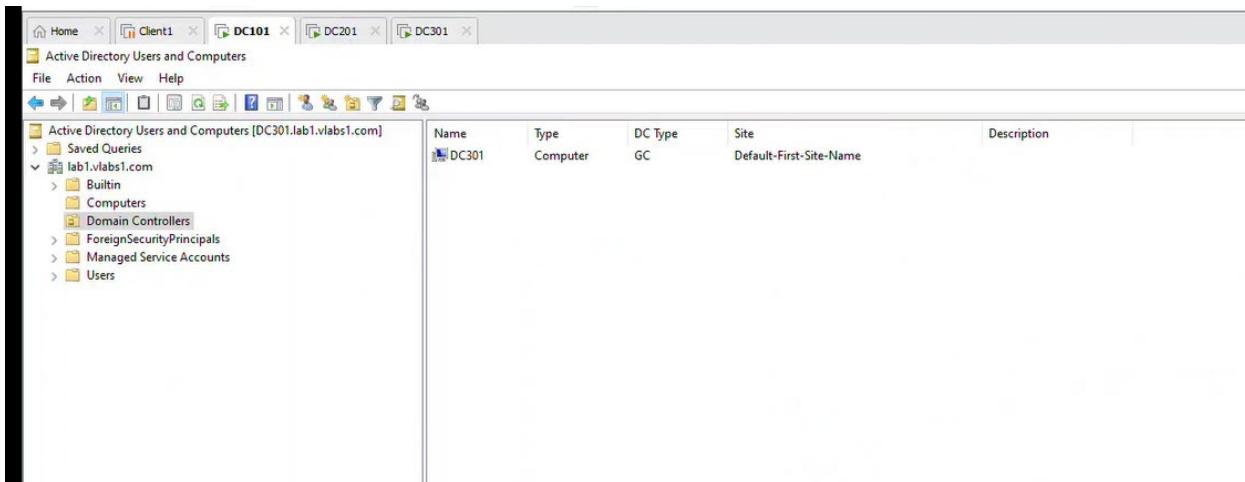
## 6.2.2 AD ON DC101

### 1. Check in tools Active Directory domains and Trusts

Verify the Child Domain Setup.







## 7 Step 5: Validate All Domain Controllers

### 7.1 Check All Domain Controllers in AD.

### 7.2 DC101

#### 7.2.1 Check All Domain Controllers in Active Directo

```
Get-ADDomainController -Filter * | Select-Object Name, Domain, Site, IPv4Address, IsGlobalCatalog
```

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Get-ADDomainController -Filter * | Select-Object Name, Domain, Site, IPv4Address, IsGlobalCatalog

Name      : DC101
Domain   : vlab1.com
Site     : Default-First-Site-Name
IPv4Address : 192.168.1.1
IsGlobalCatalog : True

Name      : DC201
Domain   : vlab1.com
Site     : Default-First-Site-Name
IPv4Address : 192.168.1.2
IsGlobalCatalog : True
```

#### 7.2.2 Check FSMO role holders

Identify the Flexible Single Master Operations (FSMO) role holders in an Active Directory domain

```
netdom query fsmo
```

```
PS C:\Users\Administrator> netdom query fsmo
Schema master           DC101.vlabs1.com
Domain naming master    DC101.vlabs1.com
PDC                   DC101.vlabs1.com
RID pool manager       DC101.vlabs1.com
Infrastructure master   DC101.vlabs1.com
The command completed successfully.
```

## 7.2.3 Validate replication health

7.2.3.1 *Summary of Active Directory replication across all domain controllers.*

**Repadmin /replsummary**

```
PS C:\Users\Administrator> Repadmin /replsummary
Replication Summary Start Time: 2025-05-05 17:55:10

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



Source DSA      largest delta    fails/total %%  error
DC101           58m:50s     0 / 10    0
DC301           58m:50s     0 /  8    0



Destination DSA      largest delta    fails/total %%  error
DC101            05m:35s     0 /  4    0
DC201            58m:50s     0 / 10    0
DC301            06m:26s     0 /  4    0
```

7.2.3.2 *Detailed information about inbound replication from other domain controllers*

**Repadmin /showrepl**

```
PS C:\Users\Administrator> Repadmin /showrepl

Repadmin: running command /showrepl against full DC localhost
Default-First-Site-Name\DC101
DSA Options: IS_GC
Site Options: (none)
DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
DSA invocationID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87

===== INBOUND NEIGHBORS =====

CN=Configuration,DC=vlabs1,DC=com
  Default-First-Site-Name\DC301 via RPC
    DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
    Last attempt @ 2025-05-05 17:49:35 was successful.

CN=Schema,CN=Configuration,DC=vlabs1,DC=com
  Default-First-Site-Name\DC301 via RPC
    DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
    Last attempt @ 2025-05-05 17:49:35 was successful.

DC=ForestDnsZones,DC=vlabs1,DC=com
  Default-First-Site-Name\DC301 via RPC
    DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
    Last attempt @ 2025-05-05 17:49:35 was successful.

DC=lab1,DC=vlabs1,DC=com
  Default-First-Site-Name\DC301 via RPC
    DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
    Last attempt @ 2025-05-05 17:49:35 was successful.

PS C:\Users\Administrator>
```

## 7.2.4 Test AD Tools (Active Directory Users and Computers, AD Sites & Services, AD PowerShell Commands).

### 7.2.4.1 Get All Users in Active Directory

```
Get-ADUser -Filter * | Select-Object Name, SamAccountName
```

```
PS C:\Users\Administrator> Get-ADUser -Filter * | Select-Object Name, SamAccountName  
Name      SamAccountName  
----  
Administrator Administrator  
Guest     Guest  
krbtgt    krbtgt  
krbtgt_24591 krbtgt_24591  
LAB1$     LAB1$  
  
PS C:\Users\Administrator> ■
```

**Get-ADUser-Filter \***

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADUser -Filter *
```

```
DistinguishedName : CN=Administrator,CN=Users,DC=vlabs1,DC=com
Enabled          : True
GivenName        :
Name             : Administrator
ObjectClass      : user
ObjectGUID       : faf775cd-17fc-4117-a3ec-0e97672130fd
SamAccountName   : Administrator
SID              : S-1-5-21-1268601764-4050707287-4025116504-500
Surname          :
UserPrincipalName :  
  
DistinguishedName : CN=Guest,CN=Users,DC=vlabs1,DC=com
Enabled          : False
GivenName        :
Name             : Guest
ObjectClass      : user
ObjectGUID       : 20d66d19-6340-477f-bc89-66c90ad43855
SamAccountName   : Guest
SID              : S-1-5-21-1268601764-4050707287-4025116504-501
Surname          :
UserPrincipalName :  
  
DistinguishedName : CN=krbtgt,CN=Users,DC=vlabs1,DC=com
Enabled          : False
GivenName        :
Name             : krbtgt
ObjectClass      : user
ObjectGUID       : 8730b3db-2a32-4e4f-a33e-f604b27047df
SamAccountName   : krbtgt
SID              : S-1-5-21-1268601764-4050707287-4025116504-502
Surname          :
UserPrincipalName :  
  
DistinguishedName : CN=krbtgt_24591,CN=Users,DC=vlabs1,DC=com
Enabled          : False
GivenName        :
Name             : krbtgt_24591
ObjectClass      : user
ObjectGUID       : bb66ef22-79aa-49c4-8dd8-eedb28ee4cbf
SamAccountName   : krbtgt_24591
SID              : S-1-5-21-1268601764-4050707287-4025116504-1105
Surname          :
UserPrincipalName :  
  
DistinguishedName : CN=LAB1$,CN=Users,DC=vlabs1,DC=com
Enabled          : True
GivenName        :
Name             : LAB1$
ObjectClass      : user
```

#### 7.2.4.2 Get All Groups in Active Directory

**Get-ADGroup-Filter \***

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADGroup -Filter *

DistinguishedName : CN=Administrators,CN=Builtin,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Administrators
ObjectClass       : group
ObjectGUID        : 8f48efe0-dc95-440d-a591-74e62b578dab
SamAccountName   : Administrators
SID               : S-1-5-32-544

DistinguishedName : CN=Users,CN=Builtin,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Users
ObjectClass       : group
ObjectGUID        : fc705250-ebe6-4173-8cba-821f6249ee99
SamAccountName   : Users
SID               : S-1-5-32-545

DistinguishedName : CN=Guests,CN=Builtin,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Guests
ObjectClass       : group
ObjectGUID        : 1b161632-6baa-43fb-b182-67f0fcfc2e316
SamAccountName   : Guests
SID               : S-1-5-32-546

DistinguishedName : CN=Print Operators,CN=Builtin,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Print Operators
ObjectClass       : group
ObjectGUID        : 191faf76-bf0c-4293-9a92-e4cf71e63a17
SamAccountName   : Print Operators
SID               : S-1-5-32-550

DistinguishedName : CN=Backup Operators,CN=Builtin,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Backup Operators
ObjectClass       : group
ObjectGUID        : 1c93dc7d-a92c-48cb-ba9c-0361a3247d66
SamAccountName   : Backup Operators
SID               : S-1-5-32-551

DistinguishedName : CN=Replicator,CN=Builtin,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Replicator
ObjectClass       : group
```

#### 7.2.4.3 Get Organizational Units

**Get-ADOrganizationalUnit-Filter \***

```
PS C:\Users\Administrator> Get-ADOrganizationalUnit -Filter *

City          :
Country       :
DistinguishedName : OU=Domain Controllers,DC=vlabs1,DC=com
LinkedGroupPolicyObjects : {CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=vlabs1,DC=com}
ManagedBy     :
Name          : Domain Controllers
ObjectClass   : organizationalUnit
ObjectGUID    : 51bc9792-b0b2-4870-8367-e872172012ad
PostalCode    :
State         :
StreetAddress  :
```

## 7.3 DC201

### 7.3.1 Check All Domain Controllers in Active Directo

```
Get-ADDomainController -Filter * | Select-Object Name, Domain, Site, IPv4Address, IsGlobalCatalog
```

```
File Edit View VM Tabs Help || □ ▾ | ↴ ↵ | ⌂ ⌃ ⌁ | □

Home Client1 DC101 DC201 DC301
Administrator: C:\WINDOWS\system32\cmd.exe
PS C:\Users\Administrator.VLABS1> Get-ADDomainController

Name          : DC101
Domain        : vlabs1.com
Site          : Default-First-Site-Name
IPv4Address   : 192.168.1.1
IsGlobalCatalog : True

Name          : DC201
Domain        : vlabs1.com
Site          : Default-First-Site-Name
IPv4Address   : 192.168.1.2
IsGlobalCatalog : True

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

### 7.3.2 Check FSMO role holders

Identify the Flexible Single Master Operations (FSMO) role holders in an Active Directory domain

**netdom query fsmo**

```
PS C:\Users\Administrator.VLABS1> netdom query fsmo
Schema master           DC101.vlabs1.com
Domain naming master    DC101.vlabs1.com
PDC                   DC101.vlabs1.com
RID pool manager       DC101.vlabs1.com
Infrastructure master   DC101.vlabs1.com
The command completed successfully.
```

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

### 7.3.3 Validate replication health

7.3.3.1 *Summary of Active Directory replication across all domain controllers.*

**Readmin /replsummary**

```
PS C:\Users\Administrator.VLABS1> Repadmin /replsummary
Replication Summary Start Time: 2025-05-05 18:19:52

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

| Source DSA | largest delta | fails/total | %% | error |
|------------|---------------|-------------|----|-------|
| DC101      | 31m:08s       | 0 / 10      | 0  |       |
| DC301      | 30m:17s       | 0 / 8       | 0  |       |

| Destination DSA | largest delta | fails/total | %% | error |
|-----------------|---------------|-------------|----|-------|
| DC101           | 30m:17s       | 0 / 4       | 0  |       |
| DC201           | 23m:31s       | 0 / 10      | 0  |       |
| DC301           | 31m:08s       | 0 / 4       | 0  |       |

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

7.3.3.2 *Detailed information about inbound replication from other domain controllers*

**Readmin /showrepl**

```
PS C:\Users\Administrator.VLABS1> Repadmin /showrepl

Readmin: running command /showrepl against full DC localhost
Default-First-Site-Name\DC201
DSA Options: IS_GC DISABLE_OUTBOUND_REPL IS_RODC
Site Options: (none)
DSA object GUID: baee489a-95f5-48de-a56d-9b7dadfb57fd
DSA invocationID: bcc25508-7de9-42e0-b28f-062e6682cf71

===== INBOUND NEIGHBORS =====

DC=lab1,DC=vlabs1,DC=com
    Default-First-Site-Name\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-05 17:56:21 was successful.
    Default-First-Site-Name\DC301 via RPC
        DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
        Last attempt @ 2025-05-05 17:56:21 was successful.

DC=vlabs1,DC=com
    Default-First-Site-Name\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-05 18:19:50 was successful.

CN=Configuration,DC=vlabs1,DC=com
    Default-First-Site-Name\DC301 via RPC
        DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
        Last attempt @ 2025-05-05 17:56:21 was successful.
    Default-First-Site-Name\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-05 17:56:21 was successful.

CN=Schema,CN=Configuration,DC=vlabs1,DC=com
    Default-First-Site-Name\DC301 via RPC
        DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
        Last attempt @ 2025-05-05 17:56:21 was successful.
    Default-First-Site-Name\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-05 17:56:21 was successful.

DC=DomainDnsZones,DC=vlabs1,DC=com
    Default-First-Site-Name\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-05 17:56:21 was successful.

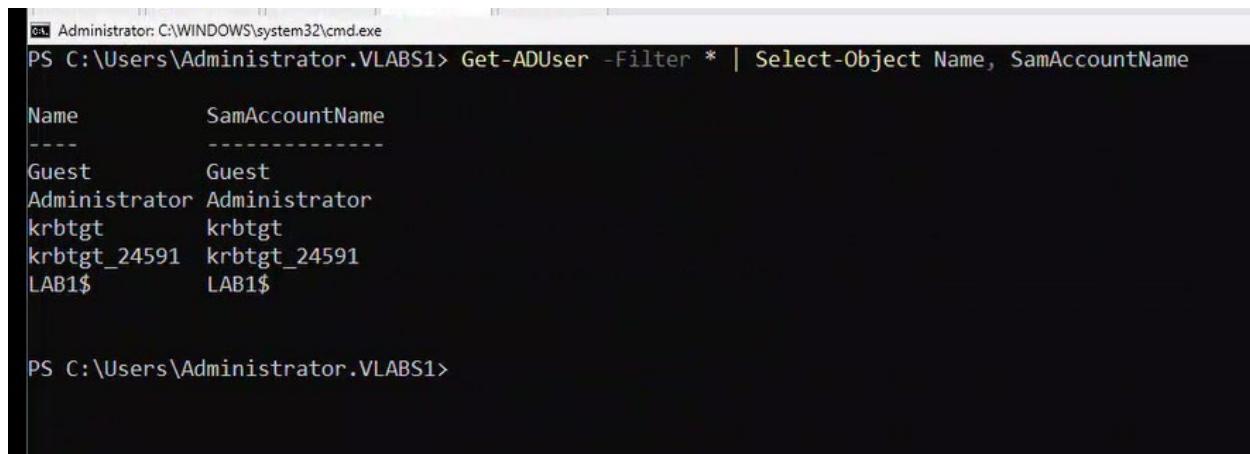
DC=ForestDnsZones,DC=vlabs1,DC=com
    Default-First-Site-Name\DC301 via RPC
        DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
        Last attempt @ 2025-05-05 17:56:21 was successful.
    Default-First-Site-Name\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-05 17:56:21 was successful.

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

## 7.3.4 Test AD Tools (Active Directory Users and Computers, AD Sites & Services, AD PowerShell Commands).

### 7.3.4.1 Get All Users in Active Directory

**Get-ADUser -Filter \* | Select-Object Name, SamAccountName**



```
Administrator: C:\WINDOWS\system32\cmd.exe
PS C:\Users\Administrator.VLABS1> Get-ADUser -Filter * | Select-Object Name, SamAccountName
Name          SamAccountName
----          -----
Guest         Guest
Administrator Administrator
krbtgt        krbtgt
krbtgt_24591  krbtgt_24591
LAB1$         LAB1$
```

PS C:\Users\Administrator.VLABS1>

**Get-ADUser -Filter \***

```
PS C:\Users\Administrator.VLABS1> Get-ADUser -Filter *
```

```
DistinguishedName : CN=Guest,CN=Users,DC=vlabs1,DC=com
Enabled          : False
GivenName        :
Name             : Guest
ObjectClass      : user
ObjectGUID       : 20d66d19-6340-477f-bc89-66c90ad43855
SamAccountName   : Guest
SID              : S-1-5-21-1268601764-4050707287-4025116504-501
Surname          :
UserPrincipalName :

DistinguishedName : CN=Administrator,CN=Users,DC=vlabs1,DC=com
Enabled          : True
GivenName        :
Name             : Administrator
ObjectClass      : user
ObjectGUID       : faf775cd-17fc-4117-a3ec-0e97672130fd
SamAccountName   : Administrator
SID              : S-1-5-21-1268601764-4050707287-4025116504-500
Surname          :
UserPrincipalName :

DistinguishedName : CN=krbtgt,CN=Users,DC=vlabs1,DC=com
Enabled          : False
GivenName        :
Name             : krbtgt
ObjectClass      : user
ObjectGUID       : 8730b3db-2a32-4e4f-a33e-f604b27047df
SamAccountName   : krbtgt
SID              : S-1-5-21-1268601764-4050707287-4025116504-502
Surname          :
UserPrincipalName :

DistinguishedName : CN=krbtgt_24591,CN=Users,DC=vlabs1,DC=com
Enabled          : False
GivenName        :
Name             : krbtgt_24591
ObjectClass      : user
ObjectGUID       : bb66ef22-79aa-49c4-8dd8-eedb28ee4cbf
SamAccountName   : krbtgt_24591
SID              : S-1-5-21-1268601764-4050707287-4025116504-1105
Surname          :
UserPrincipalName :

DistinguishedName : CN=LAB1$,CN=Users,DC=vlabs1,DC=com
Enabled          : True
GivenName        :
Name             : LAB1$
ObjectClass      : user
ObjectGUID       : 706d6aca-3f25-4173-a34e-3dc78ede7046
SamAccountName   : LAB1$
SID              : S-1-5-21-1268601764-4050707287-4025116504-1106
Surname          :
UserPrincipalName :
```

#### 7.3.4.2 Get All Groups in Active Directory

**Get-ADGroup -Filter \***

```
Administrator: C:\WINDOWS\system32\cmd.exe
PS C:\Users\Administrator.VLABS1> Get-ADGroup -Filter *

DistinguishedName : CN=Administrators,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Administrators
ObjectClass       : group
ObjectGUID        : 8f48efe0-dc95-440d-a591-74e62b578dab
SamAccountName   : Administrators
SID               : S-1-5-32-544

DistinguishedName : CN=Users,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Users
ObjectClass       : group
ObjectGUID        : fc705250-ebe6-4173-8cba-821f6249ee99
SamAccountName   : Users
SID               : S-1-5-32-545

DistinguishedName : CN=Guests,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Guests
ObjectClass       : group
ObjectGUID        : 1b161632-6baa-43fb-b182-67f0cfcc2e316
SamAccountName   : Guests
SID               : S-1-5-32-546

DistinguishedName : CN=Remote Desktop Users,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Remote Desktop Users
ObjectClass       : group
ObjectGUID        : ee804a45-d4d3-4604-91ef-d44e8d45ec12
SamAccountName   : Remote Desktop Users
SID               : S-1-5-32-555

DistinguishedName : CN=Network Configuration Operators,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Network Configuration Operators
ObjectClass       : group
ObjectGUID        : 58422ac1-0153-4494-879b-bb42ae626ef8
SamAccountName   : Network Configuration Operators
SID               : S-1-5-32-556

DistinguishedName : CN=Performance Monitor Users,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Performance Monitor Users
ObjectClass       : group
ObjectGUID        : 9e2c02e2-078a-45ff-9233-de0cd5756e5b
SamAccountName   : Performance Monitor Users
SID               : S-1-5-32-558
```

### 7.3.4.3 Get Organizational Units

Get-ADOrganizationalUnit -Filter \*

```
PS C:\Users\Administrator.VLABS1> Get-ADOrganizationalUnit -Filter *

City          :
Country       :
DistinguishedName : OU=Domain Controllers,DC=vlabs1,DC=com
LinkedGroupPolicyObjects : {CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=vlabs1,DC=com}
ManagedBy     :
Name          : Domain Controllers
ObjectClass   : organizationalUnit
ObjectGUID    : 51bc9792-b0b2-4870-8367-e872172012ad
PostalCode    :
State         :
StreetAddress  :

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

## 7.1 DC301

### 7.1.1 Check All Domain Controllers in Active Directo

**Get-ADDomainController -Filter \* | Select-Object Name, Domain, Site, IPv4Address, IsGlobalCatalog**

```
[Administrator: Windows PowerShell]
PS C:\Users\Administrator> Get-ADDomainController -Filter * | Select-Object Name, Domain, Site, IPv4Address, IsGlobalCatalog

Name      : DC301
Domain    : lab1.vlabs1.com
Site      : Default-First-Site-Name
IPv4Address : 192.168.1.3
IsGlobalCatalog : True

PS C:\Users\Administrator>
```

### 7.1.2 Check FSMO role holders

Identify the Flexible Single Master Operations (FSMO) role holders in an Active Directory domain

**netdom query fsmo**

```
PS C:\Users\Administrator> netdom query fsmo
Schema master          DC101.vlabs1.com
Domain naming master   DC101.vlabs1.com
PDC                   DC301.lab1.vlabs1.com
RID pool manager       DC301.lab1.vlabs1.com
Infrastructure master  DC301.lab1.vlabs1.com
The command completed successfully.

PS C:\Users\Administrator>
```

### 7.1.3 Validate replication health

#### 7.1.3.1 Summary of Active Directory replication across all domain controllers.

**Readmin /replsummary**

```
PS C:\Users\Administrator.VLABS1> Repadmin /replsummary
Replication Summary Start Time: 2025-05-05 18:19:52

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



Source DSA      largest delta    fails/total %%  error
DC101           31m:08s     0 /  10    0
DC301           30m:17s     0 /   8    0



Destination DSA      largest delta    fails/total %%  error
DC101            30m:17s     0 /   4    0
DC201            23m:31s     0 /  10    0
DC301            31m:08s     0 /   4    0



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

#### 7.1.3.2 Detailed information about inbound replication from other domain controllers

**Readmin /showrepl**

```

PS C:\Users\Administrator.VLABS1> Repadmin /showrepl

Repadmin: running command /showrepl against full DC localhost
Default-First-Site-Name\DC201
DSA Options: IS_GC DISABLE_OUTBOUND_REPL IS_RODC
Site Options: (none)
DSA object GUID: baee489a-95f5-48de-a56d-9b7dadfb57fd
DSA invocationID: bcc25508-7de9-42e0-b28f-062e6682cf71

===== INBOUND NEIGHBORS =====

DC=lab1,DC=vlabs1,DC=com
  Default-First-Site-Name\DC101 via RPC
    DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
    Last attempt @ 2025-05-05 17:56:21 was successful.
  Default-First-Site-Name\DC301 via RPC
    DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
    Last attempt @ 2025-05-05 17:56:21 was successful.

DC=vlabs1,DC=com
  Default-First-Site-Name\DC101 via RPC
    DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
    Last attempt @ 2025-05-05 18:19:50 was successful.

CN=Configuration,DC=vlabs1,DC=com
  Default-First-Site-Name\DC301 via RPC
    DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
    Last attempt @ 2025-05-05 17:56:21 was successful.
  Default-First-Site-Name\DC101 via RPC
    DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
    Last attempt @ 2025-05-05 17:56:21 was successful.

CN=Schema,CN=Configuration,DC=vlabs1,DC=com
  Default-First-Site-Name\DC301 via RPC
    DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
    Last attempt @ 2025-05-05 17:56:21 was successful.
  Default-First-Site-Name\DC101 via RPC
    DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
    Last attempt @ 2025-05-05 17:56:21 was successful.

DC=DomainDnsZones,DC=vlabs1,DC=com
  Default-First-Site-Name\DC101 via RPC
    DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
    Last attempt @ 2025-05-05 17:56:21 was successful.

DC=ForestDnsZones,DC=vlabs1,DC=com
  Default-First-Site-Name\DC301 via RPC
    DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
    Last attempt @ 2025-05-05 17:56:21 was successful.
  Default-First-Site-Name\DC101 via RPC
    DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
    Last attempt @ 2025-05-05 17:56:21 was successful.

PS C:\Users\Administrator.VLABS1>

```

## 7.1.4 Test Commands

### 7.1.4.1 Get All Users in Active Directory

## **Get-ADUser -Filter \* | Select-Object Name, SamAccountName**

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

Name          SamAccountName
----          -----
Administrator Administrator
Guest         Guest
krbtgt        krbtgt
VLABS1$       VLABS1$
```

```
PS C:\Users\Administrator> ■
```

## **Get-ADUser -Filter \***

```
PS C:\Users\Administrator> Get-ADUser -Filter *
```

```
DistinguishedName : CN=Administrator,CN=Users,DC=lab1,DC=vlabs1,DC=com
Enabled          : True
GivenName        :
Name             : Administrator
ObjectClass      : user
ObjectGUID       : 4aaef231-19b5-4e40-acdd-f50d9ff48437
SamAccountName   : Administrator
SID              : S-1-5-21-32770921-3136444610-3217977211-500
Surname          :
UserPrincipalName :

DistinguishedName : CN=Guest,CN=Users,DC=lab1,DC=vlabs1,DC=com
Enabled          : False
GivenName        :
Name             : Guest
ObjectClass      : user
ObjectGUID       : 1655280c-e37f-429b-9ca6-d3b7f3670594
SamAccountName   : Guest
SID              : S-1-5-21-32770921-3136444610-3217977211-501
Surname          :
UserPrincipalName :

DistinguishedName : CN=krbtgt,CN=Users,DC=lab1,DC=vlabs1,DC=com
Enabled          : False
GivenName        :
Name             : krbtgt
ObjectClass      : user
ObjectGUID       : 1fe69e08-1bce-4271-b2ba-549d54fc8faa
SamAccountName   : krbtgt
SID              : S-1-5-21-32770921-3136444610-3217977211-502
Surname          :
UserPrincipalName :

DistinguishedName : CN=VLABS1$,CN=Users,DC=lab1,DC=vlabs1,DC=com
Enabled          : True
GivenName        :
Name             : VLABS1$
ObjectClass      : user
ObjectGUID       : 06f074f4-5cb0-42c7-8be7-c267dfc11b59
SamAccountName   : VLABS1$
SID              : S-1-5-21-32770921-3136444610-3217977211-1103
```

#### 7.1.4.2 Get All Groups in Active Directory

**Get-ADGroup -Filter \***

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADGroup -Filter *

DistinguishedName : CN=Administrators,CN=BuiltIn,DC=lab1,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Administrators
ObjectClass       : group
ObjectGUID        : 947538db-d891-4972-a1cf-9c09c1e356e1
SamAccountName   : Administrators
SID               : S-1-5-32-544

DistinguishedName : CN=Users,CN=BuiltIn,DC=lab1,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Users
ObjectClass       : group
ObjectGUID        : 3720153d-2bfb-4d09-96e0-a4a0ffebcc7a
SamAccountName   : Users
SID               : S-1-5-32-545

DistinguishedName : CN=Guests,CN=BuiltIn,DC=lab1,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Guests
ObjectClass       : group
ObjectGUID        : b2d144e4-3cd6-4955-98dd-8a0550defe24
SamAccountName   : Guests
SID               : S-1-5-32-546

DistinguishedName : CN=Print Operators,CN=BuiltIn,DC=lab1,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Print Operators
ObjectClass       : group
ObjectGUID        : e6de6431-5a14-43cd-8114-518833ad28e1
SamAccountName   : Print Operators
SID               : S-1-5-32-550

DistinguishedName : CN=Backup Operators,CN=BuiltIn,DC=lab1,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Backup Operators
ObjectClass       : group
ObjectGUID        : 2b33d8d6-87c1-4a87-a8d0-5909580e169c
```

#### 7.1.4.3 Get Organizational Units

**Get-ADOrganizationalUnit -Filter \***

```

PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADOrganizationalUnit -Filter *

City
Country
DistinguishedName : OU=Domain Controllers,DC=vlabs1,DC=com
LinkedGroupPolicyObjects : {CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=vlabs1,DC=com}
ManagedBy
Name : Domain Controllers
ObjectClass : organizationalUnit
ObjectGUID : 51bc9792-b0b2-4870-8367-e872172012ad
PostalCode :
State :
StreetAddress :

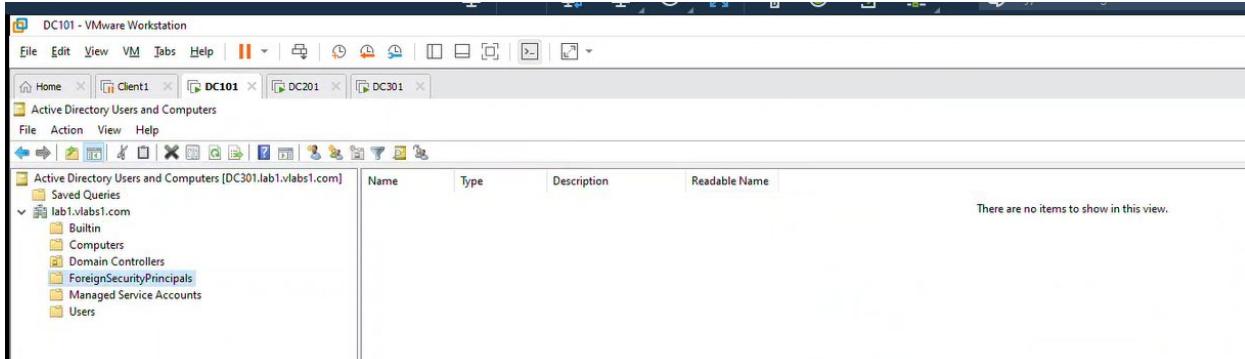
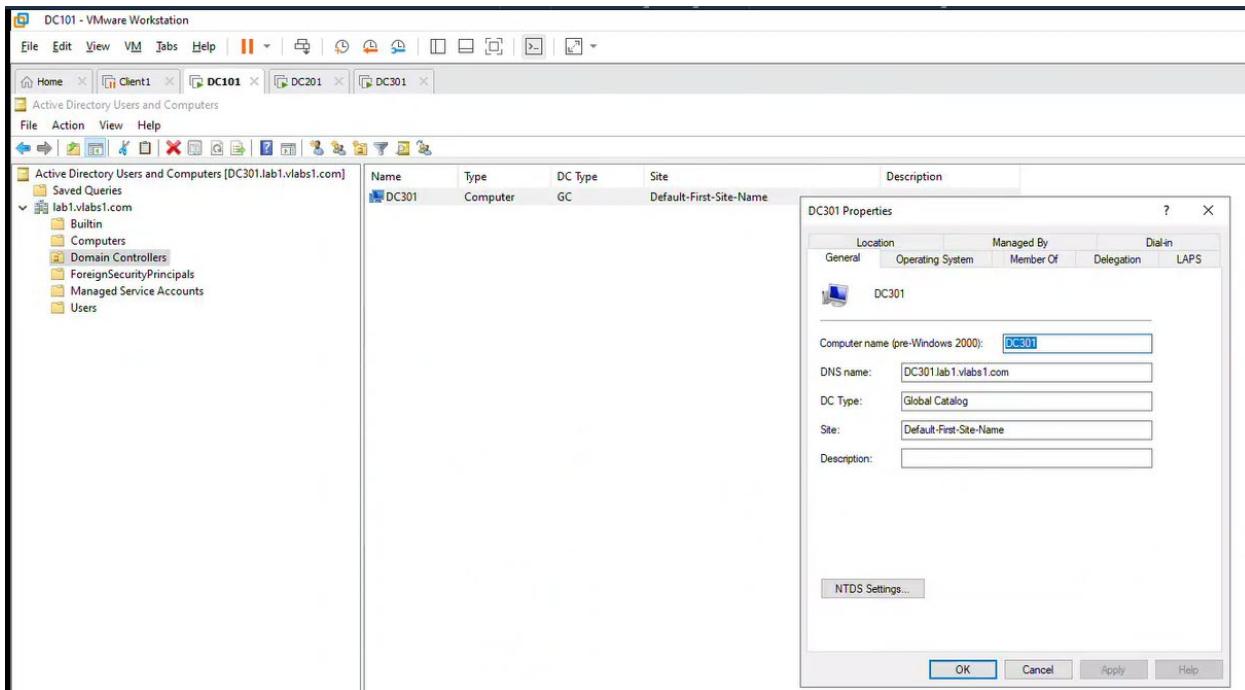
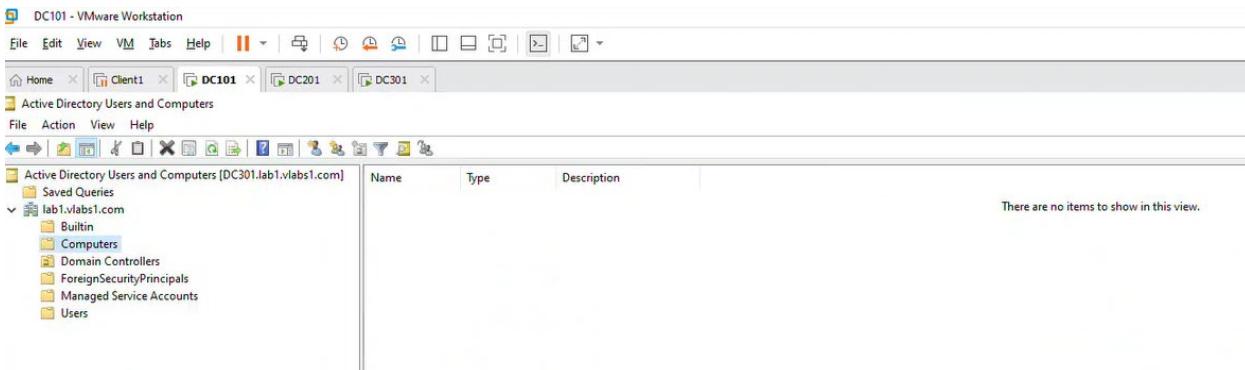

PS C:\Users\Administrator>

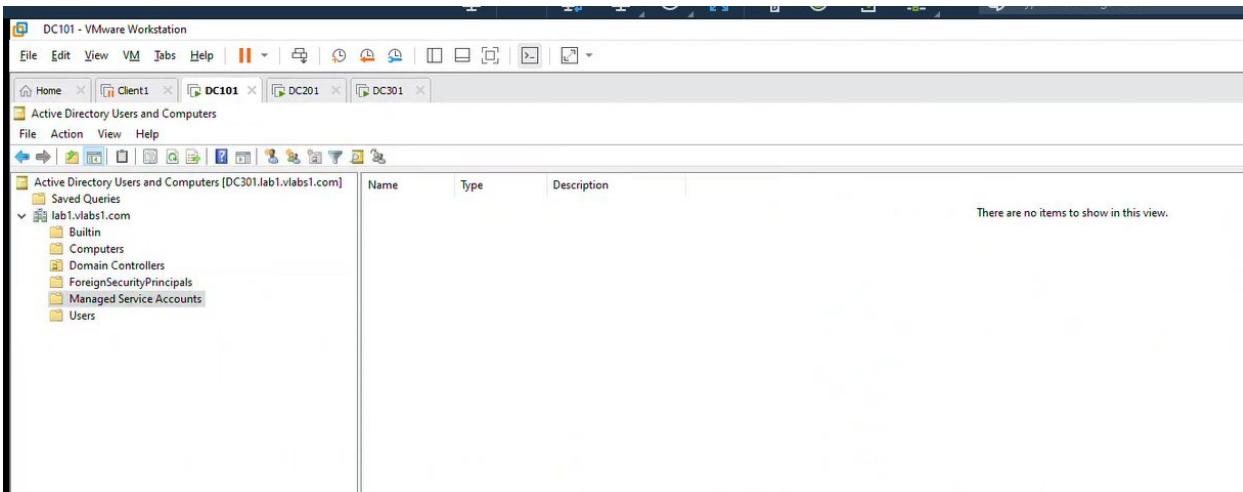
```

## 8 Test AD Tools (Active Directory Users and Computers, AD Sites & Services, AD PowerShell Commands)

### 8.1 Active Directory Users and Computers

| Name                                | Type                          | Description  |
|-------------------------------------|-------------------------------|--|
| Access Control Assistance Operators | Security Group - Domain Local | Members of this group can remotely query authorization attributes and permissions for resources on this computer.  |
| Account Operators                   | Security Group - Domain Local | Members can administer domain user and group accounts.   |
| Administrators                      | Security Group - Domain Local | Members of this group have complete and unrestricted access to all features of the computer/domain.  |
| Backup Operators                    | Security Group - Domain Local | Backup Operators can execute security-restricted tasks for the sole purpose of backing up or restoring files.  |
| Certificate Service DCOM Access     | Security Group - Domain Local | Members of this group are allowed to connect to Certification Authorities in the enterprise.   |
| Cryptographic Operators             | Security Group - Domain Local | Members are authorized to perform cryptographic operations.  |
| Distributed COM Users               | Security Group - Domain Local | Members are allowed to launch, activate and use Distributed COM objects on this machine.   |
| Event Log Readers                   | Security Group - Domain Local | Members of this group can read event logs from local machine.  |
| Guests                              | Security Group - Domain Local | Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted.  |
| Hyper-V Administrators              | Security Group - Domain Local | Members of this group have complete and unrestricted access to all features of Hyper-V.  |
| IIS_IUSRS                           | Security Group - Domain Local | Built-in group used by Internet Information Services.  |
| Network Configuration Operators     | Security Group - Domain Local | Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remote access to this computer.                                    |
| Performance Log Users               | Security Group - Domain Local | Members of this group can access performance counter data locally and remotely.  |
| Pre-Windows 2000 Compatible Access  | Security Group - Domain Local | A backward compatibility group which allows read access on all users and groups in the domain.   |
| Print Operators                     | Security Group - Domain Local | Members can administer printers installed on domain controllers.   |
| RDS Endpoint Servers                | Security Group - Domain Local | Servers in this group run virtual machines and host sessions where users RemoteApp programs and personal virtual desktops run. This group needs to be populated on servers running RD Connection Bro...      |
| RDS Management Servers              | Security Group - Domain Local | Servers in this group can perform routine administrative actions on servers running Remote Desktop Services. This group needs to be populated on all servers in a Remote Desktop Services deployment. T...   |
| RDS Remote Access Servers           | Security Group - Domain Local | Servers in this group enable users of RemoteApp programs and personal virtual desktops access to these resources. In Internet-facing deployments, these servers are typically deployed in an edge network... |
| Remote Desktop Users                | Security Group - Domain Local | Members of this group have granted the right to logon remotely.  |
| Remote Management Users             | Security Group - Domain Local | Members of this group have complete and unrestricted access to all features of WS-Management.  |
| Replicator                          | Security Group - Domain Local | Supports file replication in a domain.   |
| Server Operators                    | Security Group - Domain Local | Members can administer domain servers.   |
| Storage Replica Administrators      | Security Group - Domain Local | Members of this group have complete and unrestricted access to all features of Storage Replica.  |
| Terminal Server License Servers     | Security Group - Domain Local | Members of this group can update user accounts in Active Directory with information about license issuance, for the purpose of tracking and reporting TS Per User CAL usage.                                 |
| Users                               | Security Group - Domain Local | Users are prevented from making accidental or intentional system-wide changes and can run most applications.   |
| Windows Authorization Access Group  | Security Group - Domain Local | Members of this group have access to the computed tokenGroupsGlobalAndUniversal attribute on User objects.   |

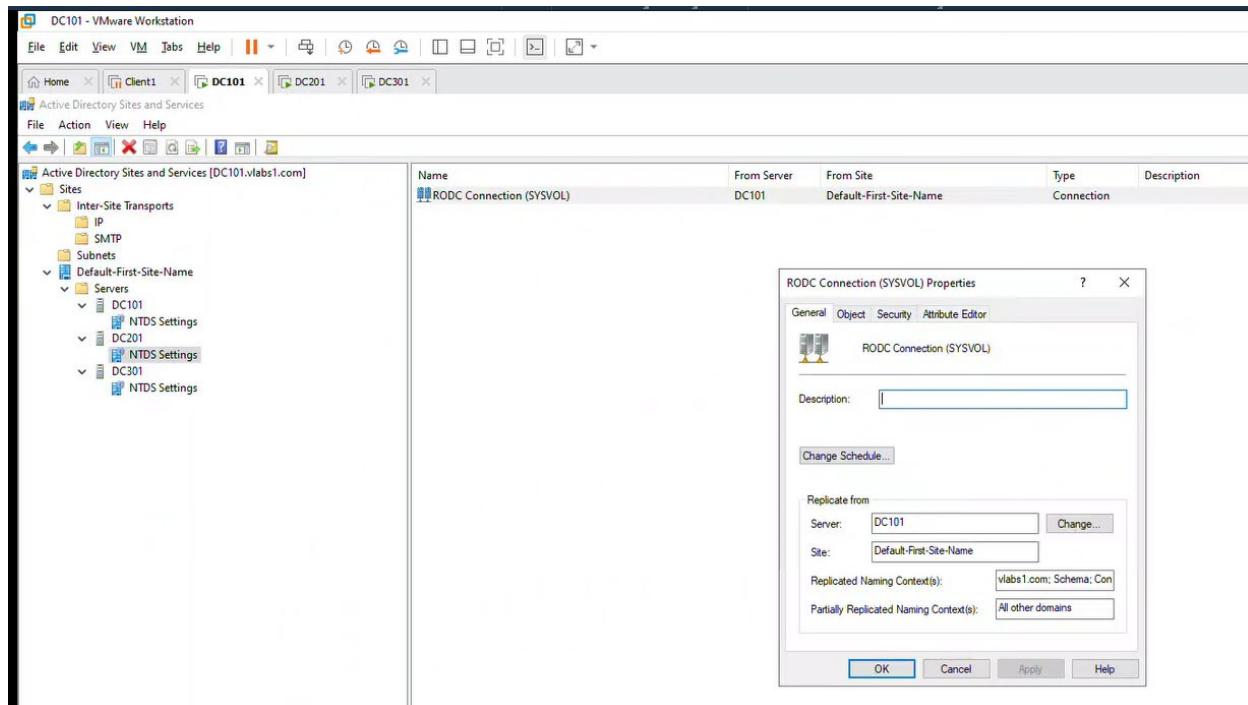
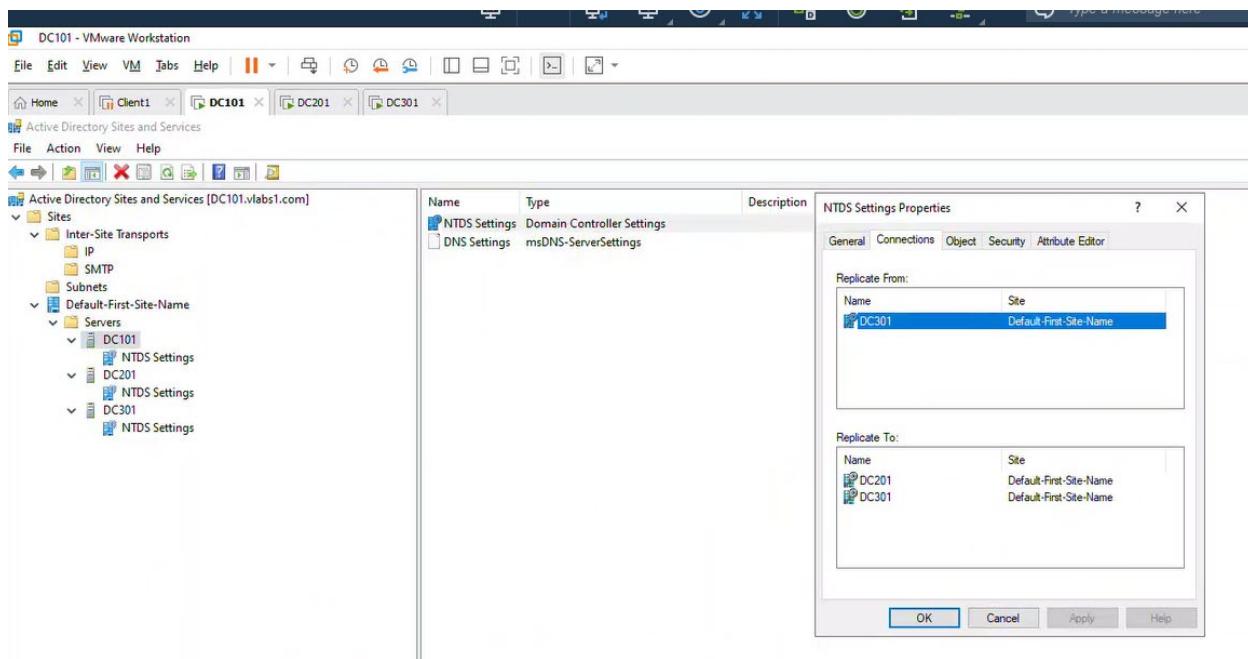


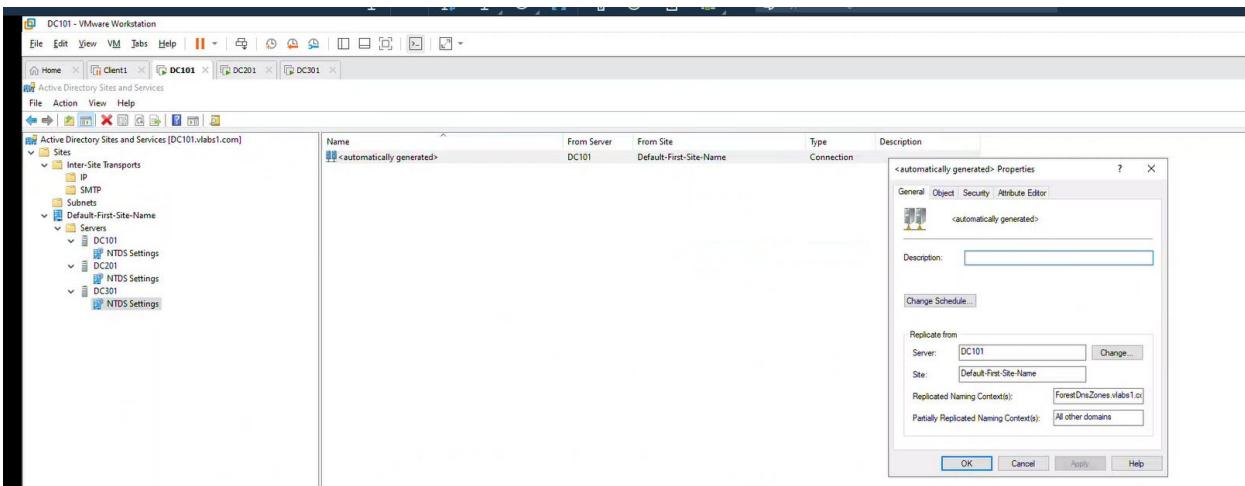


| Name                                   | Type                          | Description  |
|--|-------------------------------|--|
| Administrator                          | User                          | Built-in account for administering the computer/domain   |
| Allowed RPC Password Replication Group | Security Group - Domain Local | Members in this group can have their passwords replicated to all read-only domain controllers in the domain  |
| Cert Publishers                        | Security Group - Domain Local | Members of this group are permitted to publish certificates to the directory   |
| Cloneable Domain Controllers           | Security Group - Global       | Members of this group are domain controllers may be cloned   |
| Denied RPC Password Replication Group  | Security Group - Domain Local | Members in this group cannot have their passwords replicated to any read-only domain controllers in the domain   |
| DnsAdmins                              | Security Group - Domain Local | DNS Administrators Group   |
| DnsUpdateProxy                         | Security Group - Global       | DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHCP servers).   |
| Domain Admins                          | Security Group - Global       | Designated administrators of the domain  |
| Domain Controllers                     | Security Group - Global       | All domain controllers and servers joined to the domain  |
| Domain Guests                          | Security Group - Global       | All domain guests  |
| Domain Users                           | Security Group - Global       | All domain users   |
| Group Policy Creator Owners            | Security Group - Global       | Members in this group can modify group policy for the domain   |
| Guest                                  | User                          | Built-in account for guest access to the computer/domain   |
| Key Admins                             | Security Group - Global       | Members of this group can perform administrative actions on key objects within the domain.   |
| Protected Users                        | Security Group - Global       | Members of this group are afforded additional protections against authentication security threats. See <a href="http://go.microsoft.com/fwlink/?LinkId=298939">http://go.microsoft.com/fwlink/?LinkId=298939</a> for more information. |
| IAS and IAS Servers                    | Security Group - Domain Local | Servers in this group can access remote access properties of users   |
| Read-only Domain Controllers           | Security Group - Global       | Members of this group are Read-Only Domain Controllers in the domain   |

## 8.2 AD Sites & Services

| Name              | Type      | Description | Cost | Replication Interval |
|-------------------|-----------|-------------|------|----------------------|
| DEFAUTLIPSITELINK | Site Link |             | 100  | 180                  |





## 8.3 AD PowerShell Commands

WINDOWS POWERSHELL HISTORY

```

New-PSDrive
-Name:"ADDriveD"
-PSProvider:"ActiveDirectory"
-Root:"DC101.vlabs1.com"
$Server="DC101.vlabs1.com"

Get-ADRootDSE

```

Administrator: Windows PowerShell

```

PS C:\Users\Administrator> Get-ADDomainController -Discover:$true -DomainName:"VLABS1" -ForceDiscover:$true -Service:ADWS -Writable:$true

Domain      : vlabs1.com
Forest     : vlabs1.com
HostName   : {DC101.vlabs1.com}
IPv4Address : 192.168.1.1
IPv6Address : ::1
Name       : DC101
Site       : Default-First-Site-Name

```

## 9 Lab Deliverables

### 9.1 DC101: Domain Controller setup verification.

1. Verify the DC Installation.



Verify AD DS Installation:

Get-Serviceadws,kdc,netlogon,dns

- Check Domain Membership:

Get-ADDomain

```
PS C:\Users\Administrator> Get-Service adws,kdc,netlogon,dns

Status    Name          DisplayName
----      --           -----
Running   adws         Active Directory Web Services
Running   dns          DNS Server
Running   kdc          Kerberos Key Distribution Center
Running   Netlogon     netlogon

PS C:\Users\Administrator> Get-ADDomain

AllowedDNSSuffixes          : {}
ChildDomains                 : {}
ComputersContainer           : CN=Computers,DC=vlabs1,DC=com
DeletedObjectsContainer      : CN=Deleted Objects,DC=vlabs1,DC=com
DistinguishedName            : DC=vlabs1,DC=com
DNSRoot                      : vlabs1.com
DomainControllersContainer   : OU=Domain Controllers,DC=vlabs1,DC=com
DomainMode                    : Windows2016Domain
DomainSID                     : S-1-5-21-1268601764-4050707287-4025116504
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=vlabs1,DC=com
Forest                        : vlabs1.com
InfrastructureMaster          : DC101.vlabs1.com
LastLogonReplicationInterval : 
LinkedGroupPolicyObjects     : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=vlabs1,DC=com}
LostAndFoundContainer         : CN=LostAndFound,DC=vlabs1,DC=com
ManagedBy                     : 
Name                          : vlabs1
NetBIOSName                  : VLABS1
ObjectClass                  : domainDNS
ObjectGUID                   : 402b24e7-c605-4172-bb2c-f1356eab96a2
ParentDomain                 : 
PDCEmulator                  : DC101.vlabs1.com
PublicKeyRequiredPasswordRolling : True
QuotasContainer               : CN=NTDS Quotas,DC=vlabs1,DC=com
ReadOnlyReplicaDirectoryServers : {} {DC101.vlabs1.com}
ReplicaDirectoryServers       : DC101.vlabs1.com
RIDMaster                     : 
SubordinateReferences         : {DC=ForestDnsZones,DC=vlabs1,DC=com, DC=DomainDnsZones,DC=vlabs1,DC=com, CN=Configuration,DC=vlabs1,DC=com}
SystemsContainer               : CN=System,DC=vlabs1,DC=com
UsersContainer                : CN=Users,DC=vlabs1,DC=com

PS C:\Users\Administrator>
```

## 9.2 DC201 (RODC)

### 9.2.1 Successful RODC promotion

**Get-ADDomainController -Filter {IsReadOnly -eq \$true} | Select Name, Domain, Site, IPv4Address**

```
PS C:\Users\Administrator.VLABS1> Get-ADDomainController -Filter {IsReadOnly -eq $true} | Select Name, Domain, Site, IPv4Address

Name  Domain      Site          IPv4Address
----  --          --           -----
DC201  vlabs1.com  Default-First-Site-Name 192.168.1.2

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

## 9.2.2 Verify if the server is a Domain Controller

**Get-ADDomainController -Identity "DC201"**

```
PS C:\Users\Administrator> Get-ADDomainController -Identity "DC201"

ComputerObjectDN      : CN=DC201,OU=Domain Controllers,DC=vlabs1,DC=com
DefaultPartition       : DC=vlabs1,DC=com
Domain                : vlabs1.com
Enabled               : True
Forest                : vlabs1.com
HostName              : DC201.vlabs1.com
InvocationId          : 00000000-0000-0000-0000-000000000000
IPv4Address           : 192.168.1.2
IPv6Address           :
IsGlobalCatalog       : True
IsReadOnly             : True
LdapPort               : 389
Name                  : DC201
NTDSSettingsObjectDN : CN=NTDS Settings,CN=DC201,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
OperatingSystem        : Windows Server 2025 Standard
OperatingSystemHotfix  :
OperatingSystemServicePack :
OperatingSystemVersion : 10.0 (26100)
OperationMasterRoles   : {}
Partitions             : {CN=Schema,CN=Configuration,DC=vlabs1,DC=com, CN=Configuration,DC=vlabs1,DC=com, DC=vlabs1,DC=com}
ServerObjectDN         : CN=DC201,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
ServerObjectGuid       : 31d1cc60-d7d6-4f15-9dab-8bf15bcc428e
Site                  : Default-First-Site-Name
SslPort                : 636

PS C:\Users\Administrator>
```

## 9.2.3 Check if the server is an RODC

**Get-ADDomainController -Filter \* | Select Name, IsReadOnly**

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADDomainController -Filter * | Select Name, IsReadOnly

Name  IsReadOnly
----  -----
DC101 False
DC201 True

PS C:\Users\Administrator>
```

## 9.2.4 In Server DC101

Tool Active Directory Sites and Services

The screenshot shows the Active Directory Sites and Services console. The left pane displays the site structure under 'DC101'. The right pane is a table with columns: Name, Domain, Bridgehead, DC Type, and Description. It lists two servers: DC101 (Domain vlabs1.com) and DC201 (Domain vlabs1.com). DC201 is highlighted with a red arrow and has a description of 'Read-only, GC'.

| Name  | Domain     | Bridgehead | DC Type       | Description |
|-------|------------|------------|---------------|-------------|
| DC101 | vlabs1.com |            | GC            |             |
| DC201 | vlabs1.com |            | Read-only, GC |             |

## 9.2.5 repadmin /showrepl results

Verify Replication:

**repadmin /showrepl**

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> repadmin /showrepl

Readmin: running command /showrepl against full DC localhost
Default-First-Site-Name\DC101
DSA Options: IS_GC
Site Options: (none)
DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
DSA invocationID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87

PS C:\Users\Administrator>
```

## 9.2.6 List of AD objects from RODC

From RODC (DC201):

**9.2.6.1 Verify Replication**

**Readmin /showrepl**

DC201 - VMware Workstation

File Edit View VM Tabs Help || | | | | | | | | | | | | | | | | |

Home Client1 DC101 DC201 DC301

Administrator: C:\WINDOWS\system32\cmd.exe

```
PS C:\Users\Administrator.VLABS1> repadmin /showrepl

Repadmin: running command /showrepl against full DC localhost
Default-First-Site-Name\DC201
DSA Options: IS_GC DISABLE_OUTBOUND_REPL IS_RODC
Site Options: (none)
DSA object GUID: baee489a-95f5-48de-a56d-9b7dadfb57fd
DSA invocationID: bcc25508-7de9-42e0-b28f-062e6682cf71

===== INBOUND NEIGHBORS =====

DC=lab1,DC=vlabs1,DC=com
  Default-First-Site-Name\DC101 via RPC
    DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
      Last attempt @ 2025-05-05 21:56:21 was successful.
  Default-First-Site-Name\DC301 via RPC
    DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
      Last attempt @ 2025-05-05 22:34:02 was successful.

DC=vlabs1,DC=com
  Default-First-Site-Name\DC101 via RPC
    DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
      Last attempt @ 2025-05-05 22:41:19 was successful.

CN=Configuration,DC=vlabs1,DC=com
  Default-First-Site-Name\DC301 via RPC
    DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
      Last attempt @ 2025-05-05 21:56:21 was successful.
  Default-First-Site-Name\DC101 via RPC
    DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
      Last attempt @ 2025-05-05 21:56:21 was successful.

CN=Schema,CN=Configuration,DC=vlabs1,DC=com
  Default-First-Site-Name\DC301 via RPC
    DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
      Last attempt @ 2025-05-05 21:56:21 was successful.
  Default-First-Site-Name\DC101 via RPC
    DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
      Last attempt @ 2025-05-05 21:56:21 was successful.

DC=DomainDnsZones,DC=vlabs1,DC=com
  Default-First-Site-Name\DC101 via RPC
    DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
      Last attempt @ 2025-05-05 21:56:21 was successful.

DC=ForestDnsZones,DC=vlabs1,DC=com
  Default-First-Site-Name\DC301 via RPC
    DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
      Last attempt @ 2025-05-05 21:56:21 was successful.
  Default-First-Site-Name\DC101 via RPC
    DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
      Last attempt @ 2025-05-05 21:56:21 was successful.

PS C:\Users\Administrator.VLABS1> _
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

## 9.2.6.2 List AD Objects (Users, Groups, OUs)

### 9.2.6.2.1 Users

#### Get-ADUser -Filter \*

The screenshot shows a Windows Server 2012 R2 desktop environment with multiple virtual machines running. The taskbar includes icons for Home, Client1, DC101, DC201, and DC301. The PowerShell window is open with the command PS C:\Users\Administrator.VLabs1> Get-ADUser -Filter \*. The output lists several Active Directory users:

```
DistinguishedName : CN=Guest,CN=Users,DC=vlabs1,DC=com
Enabled          : False
GivenName        :
Name             : Guest
ObjectClass      : user
ObjectGUID       : 20d66d19-6340-477f-bc89-66c90ad43855
SamAccountName   : Guest
SID              : S-1-5-21-1268601764-4050707287-4025116504-501
Surname          :
UserPrincipalName :

DistinguishedName : CN=Administrator,CN=Users,DC=vlabs1,DC=com
Enabled          : True
GivenName        :
Name             : Administrator
ObjectClass      : user
ObjectGUID       : faf775cd-17fc-4117-a3ec-0e97672130fd
SamAccountName   : Administrator
SID              : S-1-5-21-1268601764-4050707287-4025116504-500
Surname          :
UserPrincipalName :

DistinguishedName : CN=krbtgt,CN=Users,DC=vlabs1,DC=com
Enabled          : False
GivenName        :
Name             : krbtgt
ObjectClass      : user
ObjectGUID       : 8730b3db-2a32-4e4f-a33e-f604b27047df
SamAccountName   : krbtgt
SID              : S-1-5-21-1268601764-4050707287-4025116504-502
Surname          :
UserPrincipalName :

DistinguishedName : CN=krbtgt_24591,CN=Users,DC=vlabs1,DC=com
Enabled          : False
GivenName        :
Name             : krbtgt_24591
ObjectClass      : user
ObjectGUID       : bb66ef22-79aa-49c4-8dd8-eedb28ee4cbf
SamAccountName   : krbtgt_24591
SID              : S-1-5-21-1268601764-4050707287-4025116504-1105
Surname          :
UserPrincipalName :

DistinguishedName : CN=LAB1$,CN=Users,DC=vlabs1,DC=com
Enabled          : True
GivenName        :
Name             : LAB1$
ObjectClass      : user
ObjectGUID       : 706d6aca-3f25-4173-a34e-3dc78ede7046
SamAccountName   : LAB1$
SID              : S-1-5-21-1268601764-4050707287-4025116504-1106
Surname          :
UserPrincipalName :
```

## 9.2.6.2.2 Groups

### Get-ADGroup -Filter \* -Server DC201 | Select-Object Name, GroupCategory

```
PS C:\Users\Administrator.VLABS1> Get-ADGroup -Filter * -Server DC201 | Select-Object Name, GroupCategory
Name                           GroupCategory
----                           -----
Administrators                 Security
Users                          Security
Guests                         Security
Remote Desktop Users          Security
Network Configuration Operators Security
Performance Monitor Users     Security
Performance Log Users         Security
Distributed COM Users         Security
IIS_IUSRS                      Security
Cryptographic Operators        Security
Event Log Readers              Security
Certificate Service DCOM Access Security
RDS Remote Access Servers     Security
RDS Endpoint Servers          Security
RDS Management Servers        Security
Hyper-V Administrators        Security
Access Control Assistance Operators Security
Remote Management Users      Security
Storage Replica Administrators Security
Domain Computers               Security
Cert Publishers                Security
Domain Users                  Security
Domain Guests                 Security
RAS and IAS Servers           Security
Incoming Forest Trust Builders Security
Terminal Server License Servers Security
Domain Admins                  Security
Schema Admins                  Security
Enterprise Admins              Security
Group Policy Creator Owners    Security
Pre-Windows 2000 Compatible Access Security
Windows Authorization Access Group Security
Allowed RODC Password Replication Group Security
Denied RODC Password Replication Group Security
Enterprise Read-only Domain Controllers Security
Cloneable Domain Controllers   Security
Protected Users                Security
Key Admins                     Security
Enterprise Key Admins          Security
Replicator                     Security
Print Operators                Security
Backup Operators                Security
Account Operators               Security
Server Operators                Security
Read-only Domain Controllers   Security
Domain Controllers              Security
DnsAdmins                      Security
DnsUpdateProxy                 Security

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

### Get-ADGroup -Filter \*

..Shortened printout

```
PS C:\Users\Administrator.VLABS1> Get-ADGroup -Filter *
```

```
DistinguishedName : CN=Administrators,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Administrators
ObjectClass       : group
ObjectGUID        : 8f48efe0-dc95-440d-a591-74e62b578dab
SamAccountName   : Administrators
SID               : S-1-5-32-544

DistinguishedName : CN=Users,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Users
ObjectClass       : group
ObjectGUID        : fc705250-ebe6-4173-8cba-821f6249ee99
SamAccountName   : Users
SID               : S-1-5-32-545

DistinguishedName : CN=Guests,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Guests
ObjectClass       : group
ObjectGUID        : 1b161632-6baa-43fb-b182-67f0fcfc2e316
SamAccountName   : Guests
SID               : S-1-5-32-546

DistinguishedName : CN=Remote Desktop Users,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Remote Desktop Users
ObjectClass       : group
ObjectGUID        : ee804a45-d4d3-4604-91ef-d44e8d45ec12
SamAccountName   : Remote Desktop Users
SID               : S-1-5-32-555

DistinguishedName : CN=Network Configuration Operators,CN=BuiltIn,DC=vlabs1,DC=com
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Network Configuration Operators
ObjectClass       : group
ObjectGUID        : 58422ac1-0153-4494-879b-bb42ae626ef8
SamAccountName   : Network Configuration Operators
SID               : S-1-5-32-556
```

#### 9.2.6.2.3 Organizational Units

**Get-ADOrganizationalUnit -Filter \***

```
Administrator: C:\WINDOWS\system32\cmd.exe
PS C:\Users\Administrator.VLABS1> Get-ADOrganizationalUnit -Filter *

City          :
Country       :
DistinguishedName : OU=Domain Controllers,DC=vlabs1,DC=com
LinkedGroupPolicyObjects : {CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=vlabs1,DC=com}
ManagedBy     :
Name          : Domain Controllers
ObjectClass   : organizationalUnit
ObjectGUID    : 51bc9792-b0b2-4870-8367-e872172012ad
PostalCode    :
State         :
StreetAddress  :

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

## 9.3 DC301 (Child Domain Controller): Confirmation of lab1.vlabs1.com.

### 9.3.1 Confirmation of lab1.vlabs1.com

**Get-ADDomain | Format-List \***

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-ADDomain | Format-List *

AllowedDNSSuffixes          : {}
ChildDomains                 : {}
ComputersContainer           : CN=Computers,DC=lab1,DC=vlabs1,DC=com
DeletedObjectsContainer      : CN=Deleted Objects,DC=lab1,DC=vlabs1,DC=com
DistinguishedName            : DC=lab1,DC=vlabs1,DC=com
DNSRoot                      : lab1.vlabs1.com
DomainControllersContainer   : OU=Domain Controllers,DC=lab1,DC=vlabs1,DC=com
DomainMode                    : Windows2016Domain
DomainSID                     : S-1-5-21-32770921-3136444610-3217977211
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=lab1,DC=vlabs1,DC=com
Forest                        : vlabs1.com
InfrastructureMaster           : DC301.lab1.vlabs1.com
LastLogonReplicationInterval : 
LinkedGroupPolicyObjects      : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=lab1,DC=vlabs1,DC=com}
LostAndFoundContainer         : CN=LostAndFound,DC=lab1,DC=vlabs1,DC=com
ManagedBy                     : 
Name                          : lab1
NetBIOSName                  : LAB1
ObjectClass                   : domainDNS
ObjectGUID                    : 2321c581-a93a-40b0-998e-ab1256a52e7d
ParentDomain                  : vlabs1.com
PDCEmulator                   : DC301.lab1.vlabs1.com
PublicKeyRequiredPasswordRolling : True
QuotasContainer                : CN=NTDS Quotas,DC=lab1,DC=vlabs1,DC=com
ReadOnlyReplicaDirectoryServers : {} {DC301.lab1.vlabs1.com}
ReplicaDirectoryServers        : DC301.lab1.vlabs1.com
RIDMaster                      : DC301.lab1.vlabs1.com
SubordinateReferences          : {DC=DomainDnsZones,DC=lab1,DC=vlabs1,DC=com}
SystemsContainer                : CN=System,DC=lab1,DC=vlabs1,DC=com
UsersContainer                 : CN=Users,DC=lab1,DC=vlabs1,DC=com
PropertyNames                  : {AllowedDNSSuffixes, ChildDomains, ComputersContainer, DeletedObjectsContainer...}
AddedProperties                : {}
RemovedProperties              : {}
ModifiedProperties             : {PublicKeyRequiredPasswordRolling}
PropertyCount                  : 30

```

### 9.3.2 Get-ADDomain -Identity "labX.vlabsX.com".

```

PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADDomain -Identity "lab1.vlabs1.com"

AllowedDNSSuffixes          : {}
ChildDomains                 : {}
ComputersContainer           : CN=Computers,DC=lab1,DC=vlabs1,DC=com
DeletedObjectsContainer      : CN=Deleted Objects,DC=lab1,DC=vlabs1,DC=com
DistinguishedName            : DC=lab1,DC=vlabs1,DC=com
DNSRoot                      : lab1.vlabs1.com
DomainControllersContainer   : OU=Domain Controllers,DC=lab1,DC=vlabs1,DC=com
DomainMode                    : Windows2016Domain
DomainSID                     : S-1-5-21-32770921-3136444610-3217977211
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=lab1,DC=vlabs1,DC=com
Forest                        : vlabs1.com
InfrastructureMaster           : DC301.lab1.vlabs1.com
LastLogonReplicationInterval : 
LinkedGroupPolicyObjects      : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=lab1,DC=vlabs1,DC=com}
LostAndFoundContainer         : CN=LostAndFound,DC=lab1,DC=vlabs1,DC=com
ManagedBy                     : 
Name                          : lab1
NetBIOSName                  : LAB1
ObjectClass                   : domainDNS
ObjectGUID                    : 2321c581-a93a-40b0-998e-ab1256a52e7d
ParentDomain                  : vlabs1.com
PDCEmulator                   : DC301.lab1.vlabs1.com
PublicKeyRequiredPasswordRolling : True
QuotasContainer                : CN=NTDS Quotas,DC=lab1,DC=vlabs1,DC=com
ReadOnlyReplicaDirectoryServers : {} {DC301.lab1.vlabs1.com}
ReplicaDirectoryServers        : DC301.lab1.vlabs1.com
RIDMaster                      : DC301.lab1.vlabs1.com
SubordinateReferences          : {DC=DomainDnsZones,DC=lab1,DC=vlabs1,DC=com}
SystemsContainer                : CN=System,DC=lab1,DC=vlabs1,DC=com
UsersContainer                 : CN=Users,DC=lab1,DC=vlabs1,DC=com

```

### 9.3.3 List of AD objects of this domain

#### 9.3.3.1 List All AD Users

**Get-ADUser -Filter \* | Select-Object Name, SamAccountName**

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

Name      SamAccountName
----      -----
Administrator Administrator
Guest     Guest
krbtgt   krbtgt
VLABS1$  VLABS1$
```

### 9.3.3.2 List All AD Groups

**Get-ADGroup -Filter \* | Select-Object Name, GroupCategory**

```
PS C:\Users\Administrator> Get-ADGroup -Filter * | Select-Object Name, GroupCategory

Name          GroupCategory
----          -----
Administrators Security
Users         Security
Guests        Security
Print Operators Security
Backup Operators Security
Replicator    Security
Remote Desktop Users Security
Network Configuration Operators Security
Performance Monitor Users Security
Performance Log Users Security
Distributed COM Users Security
IIS_IUSRS    Security
Cryptographic Operators Security
Event Log Readers Security
Certificate Service DCOM Access Security
RDS Remote Access Servers Security
RDS Endpoint Servers Security
RDS Management Servers Security
Hyper-V Administrators Security
Access Control Assistance Operators Security
Remote Management Users Security
Storage Replica Administrators Security
Domain Computers Security
Domain Controllers Security
Cert Publishers Security
Domain Admins  Security
Domain Users   Security
Domain Guests  Security
Group Policy Creator Owners Security
RAS and IAS Servers Security
Server Operators Security
Account Operators Security
Pre-Windows 2000 Compatible Access Security
Windows Authorization Access Group Security
Terminal Server License Servers Security
Allowed RODC Password Replication Group Security
Denied RODC Password Replication Group Security
Read-only Domain Controllers Security
Cloneable Domain Controllers Security
Protected Users  Security
Key Admins     Security
DnsAdmins     Security
DnsUpdateProxy Security
```

### 9.3.3.3 List Organizational Units (OUs)

**Get-ADOrganizationalUnit -Filter \* | Select-Object Name, DistinguishedName**

```
PS C:\Users\Administrator> Get-ADOrganizationalUnit -Filter * | Select-Object Name, DistinguishedName
Name          DistinguishedName
-----
Domain Controllers OU=Domain Controllers,DC=lab1,DC=vlabs1,DC=com

PS C:\Users\Administrator>
```