This lab provides students with hands-on experience in configuring and managing Active Directory Sites and Replication.

The tasks include setting up sites, subnets, site links, and replication monitoring using both GUI and PowerShell. By completing this lab, students will gain a deep understanding of AD DS replication and inter-site communication.

Lab Assignment 1 (Part II) - Managing AD Sites and replication

420-636-AB-Network Installation and Administration II

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

Table of Contents

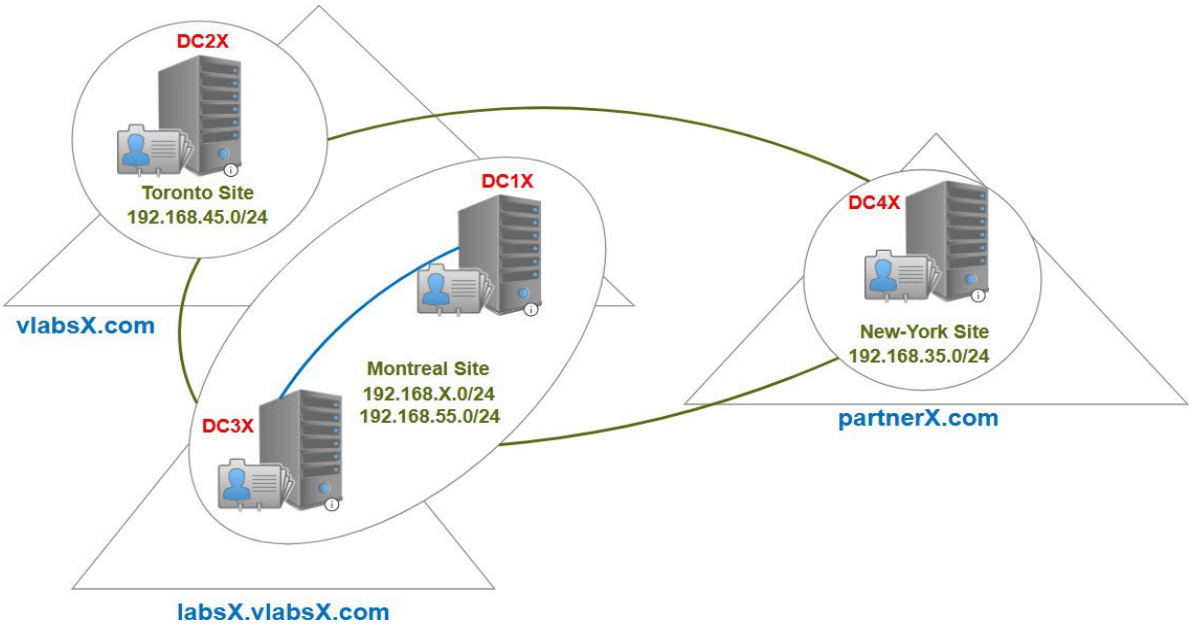
Lab Assignment 1 (Part II) - Managing AD Sites and replication

1 Lab Overview

This lab provides students with hands-on experience in configuring and managing **Active Directory Sites and Replication**.

The tasks include setting up sites, subnets, site links, and replication monitoring using both **GUI and PowerShell**. By completing this lab, students will gain a deep understanding of **AD DS replication and inter-site communication**.

2 Lab Topology Overview



3 Task 1 Preparation

The base of the assignment part 2 is Lab 6, some changes are to be made to have the topology described in the previous section.

Domain Hierarchy

- Forest Root: vlabs1.com
- Child Domain: lab1.vlabs1.com
- DCs Present:
  - DC101: Primary DC for vlabs1.com
  - DC201: RODC in vlabs1.com
  - DC301: DC for lab1.vlabs1.com
  - DC401: Currently a member server of vlabs1.com, IP: 192.168.35.1, planned to become the DC for a new child domain partner1.vlabs1.com

Domain	Hostname	IP Address	Role	Site/Subnet
vlabs1.com	DC101	192.168.1.1	Primary DC, GC	192.168.1.0/24
vlabs1.com	DC201	192.168.45.1	Read-Only DC (RODC)	192.168.45.0/24
lab1.vlabs1.com	DC301	192.168.1.3	Child Domain DC, GC	192.168.1.0/24
(to be) partner1.vlabs1.com	DC401	192.168.35.1	Planned Child DC	192.168.35.0/24

There is a Cisco router not included in the picture of topology, but it is part of the topology , This Cisco Router is the Layer 3 device that enables routing between the VLANs/subnets housing the domain controllers. All DCs use the router as their default gateway.

Router details

Interface	IP Address	Connected Subnet
GigabitEthernet1	192.168.1.50	VLAN/Subnet for DC101/DC301
GigabitEthernet2	192.168.35.50	VLAN/Subnet for DC401
GigabitEthernet3	192.168.45.50	VLAN/Subnet for DC201
GigabitEthernet0	10.164.0.253	Possibly internet/WAN

3.1 Router configuration

1. Download the Cisco-Router.ova file using the following link: Cisco Router VM
2. Import the Cisco-Router using the Cisco-Router.ova file.
3. Before starting the router, open the VM settings and make sure that:
   - Network Adapter Bridged
   - Network Adapter 2 LAN1
   - Network Adapter 3 LAN2
   - Network Adapter 4 LAN3

4. Start the Cisco-Router VM. Click inside the VM and press any key to continue. It will take a couple of minutes to boot. Just wait.

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

6. Verify the following:
   - **GigabitEthernet1** has an address **192.168.1.50** ➔ **To Modify**
   - **GigabitEthernet2** has an address **192.168.35.50** ➔ **Keep it as it is.**
   - **GigabitEthernet3** has an address **192.168.45.50** ➔ **Keep it as it is.**
   - **GigabitEthernet 0** has a **Bridged** address ➔ **Keep it as it is.**

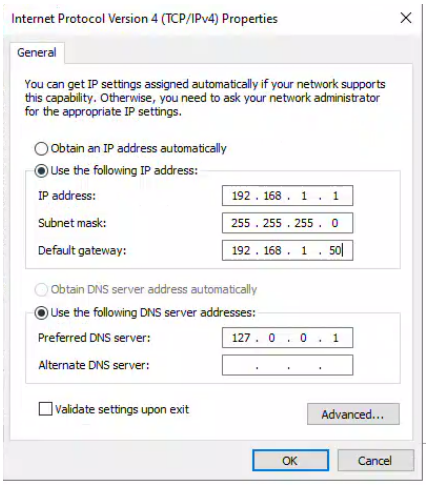
7. You need to modify this IP address of **GigabitEthernet1** and use **192.168.*1*.50/24 (where 1 is your remote PC number).**

```
Press RETURN to get started!


Cisco-Router>
Cisco-Router>enable
Cisco-Router#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       192.168.25.50   YES NVRAM  up                    up
GigabitEthernet2       192.168.35.50   YES NVRAM  up                    up
GigabitEthernet3       192.168.45.50   YES NVRAM  up                    up
GigabitEthernet0       10.164.0.253    YES DHCP   up                    up
Cisco-Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Cisco-Router(config)#int g
Cisco-Router(config)#int g
Cisco-Router(config)#int g1
Cisco-Router(config-if)#ipa
Cisco-Router(config-if)#ip a
Cisco-Router(config-if)#ip address 192.168.1.50 255.255.255.0
Cisco-Router(config-if)#end
Cisco-Router#
Cisco-Router#
Cisco-Router#_
```

```
Cisco-Router#sho ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       192.168.1.50    YES manual up                    up
GigabitEthernet2       192.168.35.50   YES NVRAM  up                    up
GigabitEthernet3       192.168.45.50   YES NVRAM  up                    up
GigabitEthernet0       10.164.0.253    YES DHCP   up                    up
Cisco-Router#
Cisco-Router#
Cisco-Router#wr
Building configuration...
[OK]
Cisco-Router#_
```

3.2 Configure DC101

3.2.1 Set default gateway to 192.168.1.50



3.2.1.1 Pings and connection test

3.2.1.1.1 Ping default gateway

```
PS C:\Users\Administrator> ping 192.168.1.50

Pinging 192.168.1.50 with 32 bytes of data:
Reply from 192.168.1.50: bytes=32 time<1ms TTL=255
Reply from 192.168.1.50: bytes=32 time<1ms TTL=255
Reply from 192.168.1.50: bytes=32 time<1ms TTL=255
Reply from 192.168.1.50: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator>
```

3.2.1.1.2 Ping DC201

nslookup dc201.vlabs1.com

ping 192.168.45.1

```
PS C:\Users\Administrator> # Ping DC201
PS C:\Users\Administrator> ping 192.168.45.1

Pinging 192.168.45.1 with 32 bytes of data:
Reply from 192.168.45.1: bytes=32 time<1ms TTL=127
Reply from 192.168.45.1: bytes=32 time=1ms TTL=127
Reply from 192.168.45.1: bytes=32 time<1ms TTL=127
Reply from 192.168.45.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.45.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\Administrator>
PS C:\Users\Administrator> nslookup dc201.vlabs1.com
Server:  localhost
Address:  127.0.0.1

Name:    dc201.vlabs1.com
Address:  192.168.45.1

PS C:\Users\Administrator>
```

3.2.1.1.3 Ping DC301

nslookup DC301.lab1.vlabs1.com

```
PS C:\Users\Administrator> nslookup DC301.lab1.vlabs1.com
Server:  localhost
Address:  127.0.0.1

Non-authoritative answer:
Name:    DC301.lab1.vlabs1.com
Address:  192.168.1.3

PS C:\Users\Administrator>
```

ping 192.168.1.3

```
PS C:\Users\Administrator> ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator>
```

3.2.1.1.4 Ping DC401

nslookup DC401.vlabs1.com

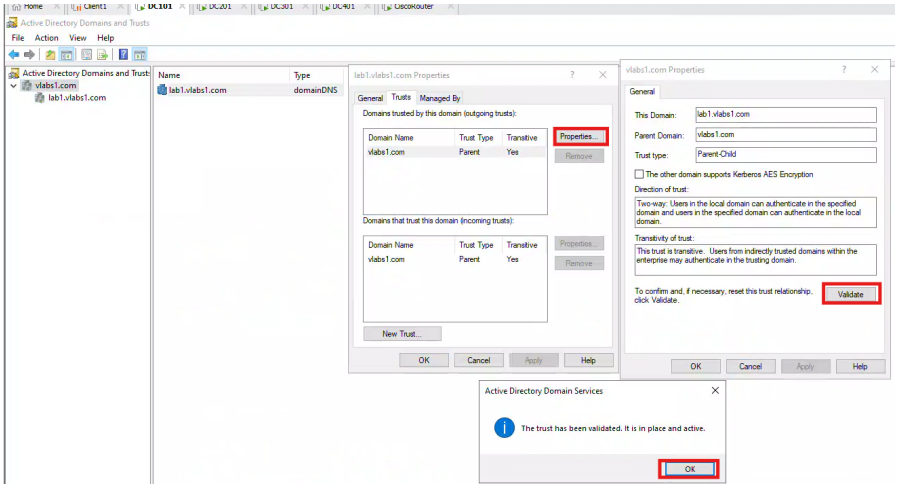
ping 192.168.35.1

```
PS C:\Users\Administrator> ping 192.168.35.1

Pinging 192.168.35.1 with 32 bytes of data:
Reply from 192.168.35.1: bytes=32 time<1ms TTL=127
Reply from 192.168.35.1: bytes=32 time<1ms TTL=127
Reply from 192.168.35.1: bytes=32 time=11ms TTL=127
Reply from 192.168.35.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.35.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 2ms
PS C:\Users\Administrator>
```

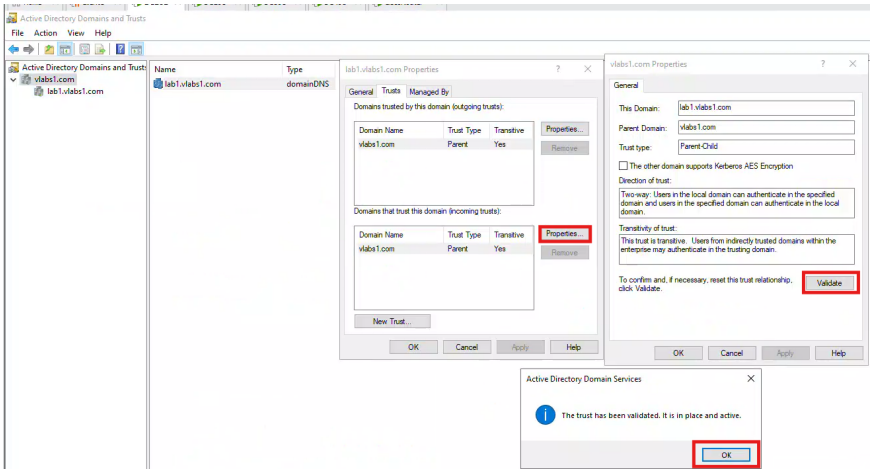
3.2.1.2 Verify domains and trusts

3.2.1.2.1 GUI Active Directory Domains and Trusts

Outgoing trust



Incoming trust



3.2.1.2.2 Powershell

Get-ADDomainController

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


ComputerObjectDN           : CN=DC101,OU=Domain Controllers,DC=vlabs1,DC=com
DefaultPartition           : DC=vlabs1,DC=com
Domain                     : vlabs1.com
Enabled                    : True
Forest                     : vlabs1.com
HostName                   : DC101.vlabs1.com
InvocationId               : 6d4f756b-185b-401f-84a0-d6d08a09a098
IPv4Address                : 192.168.1.1
IPv6Address                : ::1
IsGlobalCatalog            : True
IsReadOnly                 : False
LdapPort                   : 389
Name                       : DC101
NTDSSettingsObjectDN       : CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
OperatingSystem            : Windows Server 2022 Datacenter
OperatingSystemHotfix      :
OperatingSystemServicePack :
OperatingSystemVersion     : 10.0 (20348)
OperationMasterRoles       : {SchemaMaster, DomainNamingMaster, PDCEmulator, RIDMaster...}
Partitions                 : {DC=ForestDnsZones,DC=vlabs1,DC=com, DC=DomainDnsZones,DC=vlabs1,DC=com, CN=Schema,CN=Configuration,DC=vlabs1,DC=com,
                             CN=Configuration,DC=vlabs1,DC=com...}
ServerObjectDN             : CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
ServerObjectGuid           : 8a7311bb-fe58-4b16-8357-75bf0ecdcf51
Site                       : Default-First-Site-Name
SslPort                    : 636
```

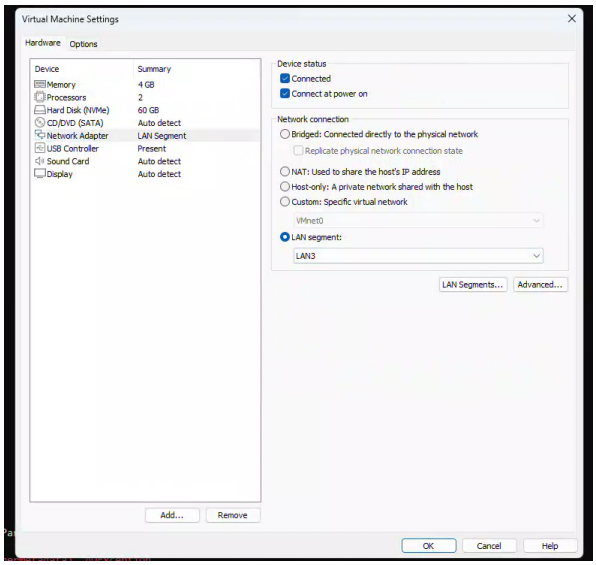
Get-ADTrust -filter *

```
PS C:\Users\Administrator> # List all trusted domains
PS C:\Users\Administrator> Get-ADTrust -filter *


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

3.3 Configure DC201

3.3.1 Modify VM

1. Start the **DC201** VM.
2. After starting and **login** into **DC201**, open its **VM Settings**, modify the **LAN segment** to
   - **LAN3**.

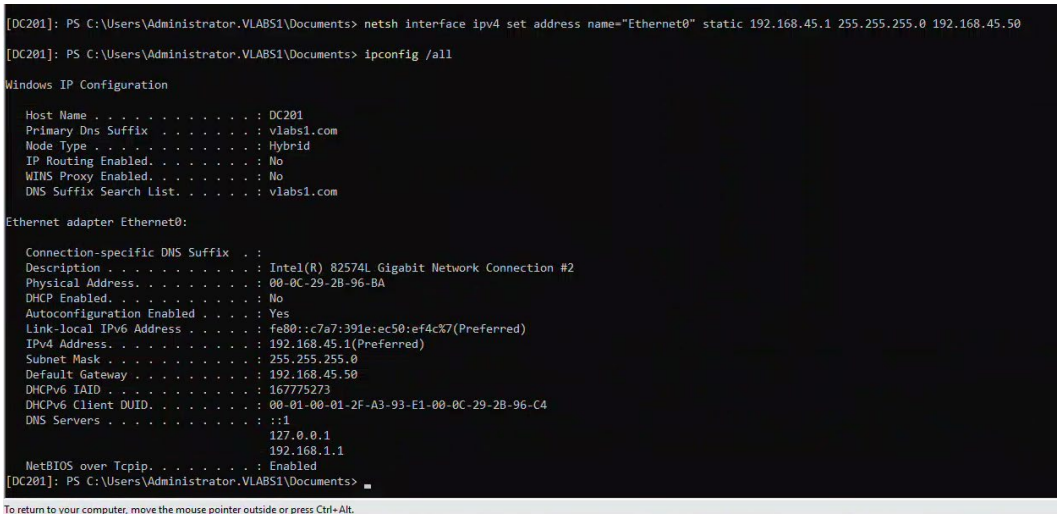


3.3.2 Set IP address and default gateway

- Change the NIC IP address to **192.168.45.1/24** with default gateway to **192.168.45.50**.

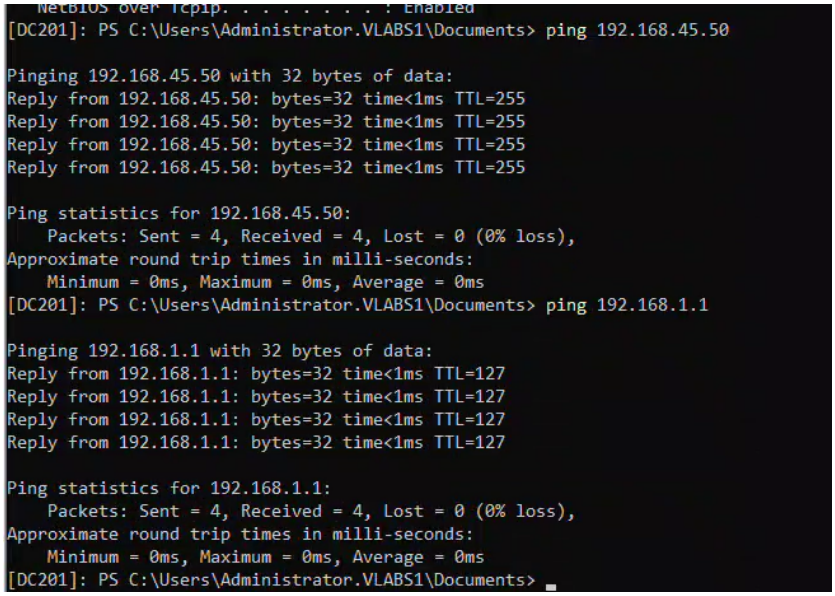
netsh interface ipv4 set address name="Ethernet0" static 192.168.45.1 255.255.255.0 192.168.45.50

- Keep the **DNS IP address as it is ➔ 192.168.1.1**

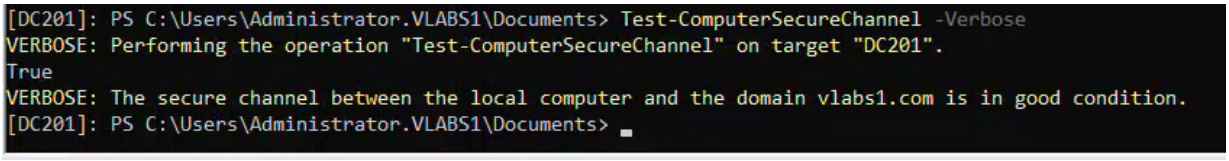


3.3.3 Ping DNS and default gateway

- **Ping** the default gateway **192.168.45.50** and DNS **192.168.1.1**



Tests the secure channel between the local computer and a domain controller



3.3.4 Domains and trust

Get-ADDomainController

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


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               : bcc25508-7de9-42e0-b28f-062e6682cf71
IPv4Address                : 192.168.45.1
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                 : {DC=ForestDnsZones,DC=vlabs1,DC=com, DC=DomainDnsZones,DC=vlabs1,DC=com, CN=Schema,CN=Configuration,DC=vlabs1,DC=com, CN=Configuration,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
```

3.3.5 Test connections

3.3.5.1 Ping DC101

nslookup DC101.vlabs1.com

ping 192.168.1.1

```
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> nslookup dc101.vlabs1.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Name:    dc101.vlabs1.com
Address:  192.168.1.1

[DC201]: PS C:\Users\Administrator.VLABS1\Documents> 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=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3.3.5.2 Ping DC301

nslookup DC301.lab1.vlabs1.com

ping 192.168.1.3

```
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> nslookup DC301.lab1.vlabs1.com
nslookup : Non-authoritative answer:
    + CategoryInfo          : NotSpecified: (Non-authoritative answer::String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError

DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Name:    DC301.lab1.vlabs1.com
Address:  192.168.1.3

[DC201]: PS C:\Users\Administrator.VLABS1\Documents> ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3.3.5.3 Ping DC401

nslookup DC401.vlabs1.com

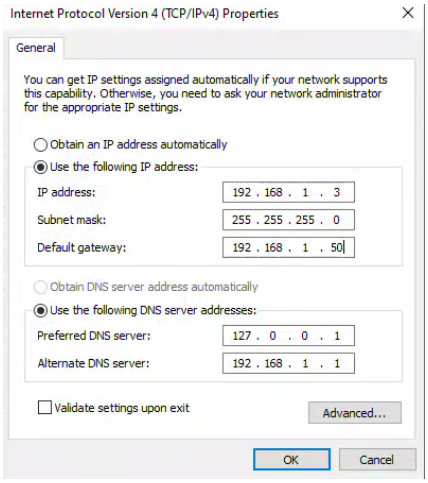
ping 192.168.35.1

```
[DC201]: PS C:\Users\Administrator.VLABS1\Documents> nslookup DC401.vlabs1.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Name:    DC401.vlabs1.com
Address:  192.168.35.1

[DC201]: PS C:\Users\Administrator.VLABS1\Documents> ping 192.168.35.1

Pinging 192.168.35.1 with 32 bytes of data:
Reply from 192.168.35.1: bytes=32 time<1ms TTL=127
Reply from 192.168.35.1: bytes=32 time<1ms TTL=127
Reply from 192.168.35.1: bytes=32 time<1ms TTL=127
Reply from 192.168.35.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.35.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
[DC201]: PS C:\Users\Administrator.VLABS1\Documents>
```

3.4 Configure DC301

3.4.1 Set default gateway

Set default gateway to 192.168.1.50



3.4.2 Ping DNS and default gateway

```
PS C:\Users\Administrator> ping 192.168.1.50

Pinging 192.168.1.50 with 32 bytes of data:
Reply from 192.168.1.50: bytes=32 time<1ms TTL=255
Reply from 192.168.1.50: bytes=32 time<1ms TTL=255
Reply from 192.168.1.50: bytes=32 time<1ms TTL=255
Reply from 192.168.1.50: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator> 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
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator>
```

3.4.3 Test Connections

3.4.3.1 Ping DC101

nslookup DC101.vlabs1.com
ping 192.168.1.1

```
PS C:\Users\Administrator> nslookup DC101.vlabs1.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Non-authoritative answer:
Name:    DC101.vlabs1.com
Address:  192.168.1.1

PS C:\Users\Administrator> 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
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3.4.3.2 Ping DC201

nslookup DC201.vlabs1.com

ping 192.168.45.1

```
PS C:\Users\Administrator> nslookup DC201.vlabs1.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Name:    DC201.vlabs1.com
Address:  192.168.45.1

PS C:\Users\Administrator> ping 192.168.45.1

Pinging 192.168.45.1 with 32 bytes of data:
Reply from 192.168.45.1: bytes=32 time<1ms TTL=127
Reply from 192.168.45.1: bytes=32 time<1ms TTL=127
Reply from 192.168.45.1: bytes=32 time<1ms TTL=127
Reply from 192.168.45.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.45.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

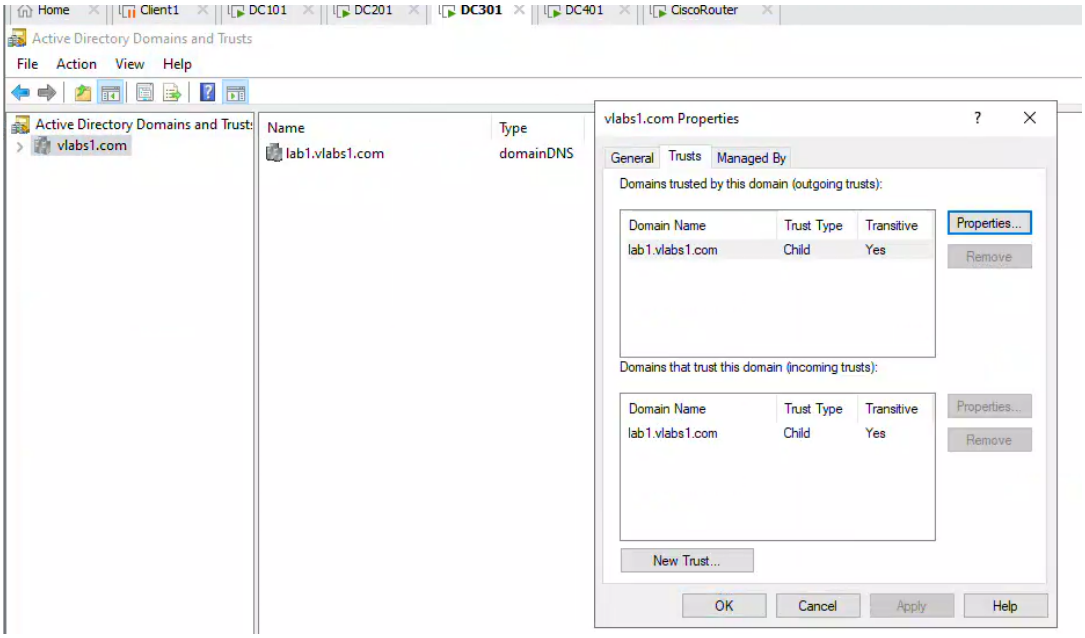
3.4.3.3 Ping DC401

nslookup DC401.vlabs1.com

ping 192.168.35.1

```
PS C:\Users\Administrator> nslookup DC401.vlabs1.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Name:    DC401.vlabs1.com
Address:  192.168.35.1

PS C:\Users\Administrator> ping 192.168.35.1

Pinging 192.168.35.1 with 32 bytes of data:
Reply from 192.168.35.1: bytes=32 time<1ms TTL=127
Reply from 192.168.35.1: bytes=32 time<1ms TTL=127
Reply from 192.168.35.1: bytes=32 time<1ms TTL=127
Reply from 192.168.35.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.35.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator>
```

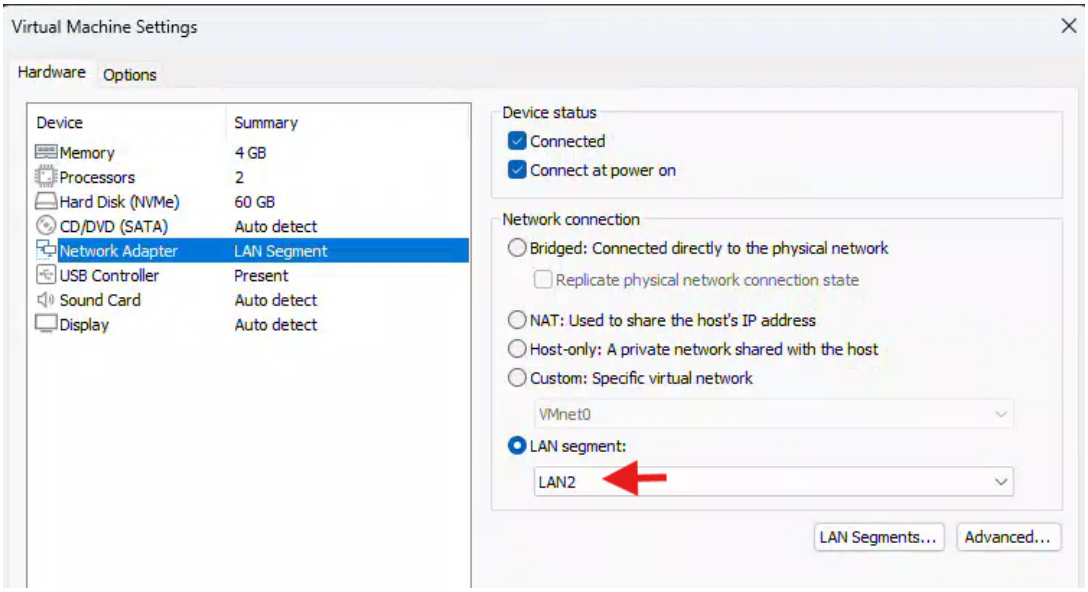
3.4.4 Trust and domains



3.5 Configure DC401

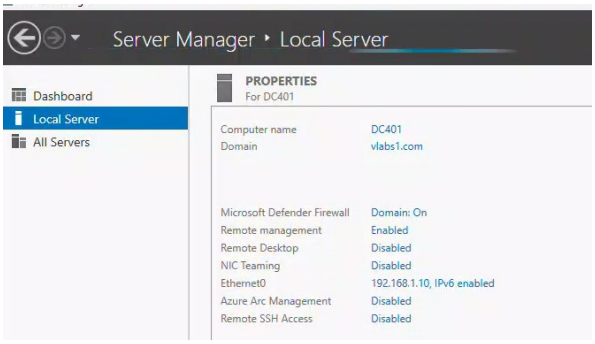
3.5.1 Verify VM settings

Make sure is LAN2 segment



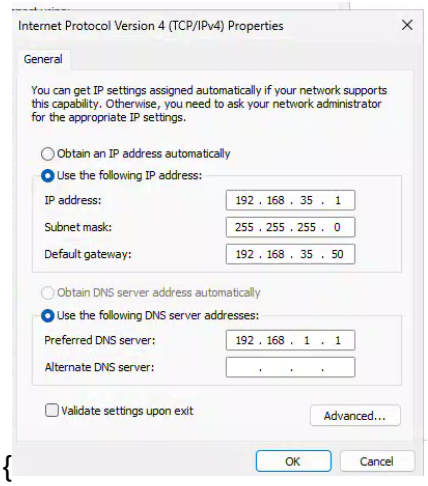
3.5.2 Change name

a) Name was changed from SRV01 to DC401 and DC401 was restarted



3.5.3 Change DNS and default gateway

Set IP Address to 192.168.35.1 and default gateway to 192.168.35.50 and DNS to 192.168.1.1



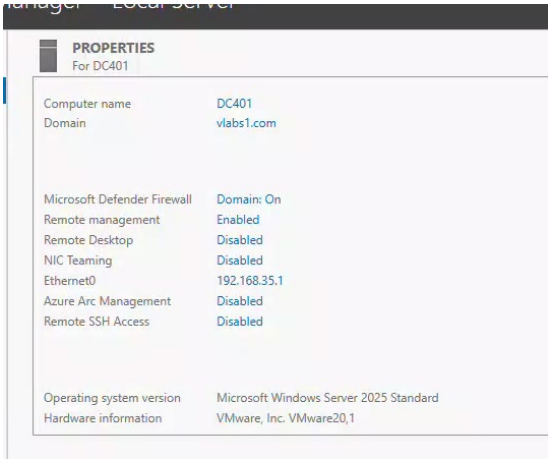
{

3.5.4 Disable IPV6

Disable-NetAdapterBinding -Name "Ethernet0" -ComponentID ms_tcpip6

```
PS C:\Users\administrator.VLABS1> Disable-NetAdapterBinding -Name "Ethernet0" -ComponentID ms_tcpip6
```

Verify in Local server



3.5.5 Ping the DNS Server and default gateway

ping 192.168.1.1
ping 191.168.35.59

```
PS C:\Users\administrator.VLABS1>
PS C:\Users\administrator.VLABS1> 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=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\administrator.VLABS1> ping 192.168.35.50

Pinging 192.168.35.50 with 32 bytes of data:
Reply from 192.168.35.50: bytes=32 time<1ms TTL=255
Reply from 192.168.35.50: bytes=32 time<1ms TTL=255
Reply from 192.168.35.50: bytes=32 time<1ms TTL=255
Reply from 192.168.35.50: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.35.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\administrator.VLABS1>
```

3.5.6 Test Connections

3.5.6.1 Ping DC101

nslookup DC101.vlabs1.com
ping 192.168.1.1

```
PS C:\Users\administrator.VLABS1> whoami
vlabs1\administrator
PS C:\Users\administrator.VLABS1> nslookup DC101.vlabs1.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  192.168.1.1

Name:    DC101.vlabs1.com
Address:  192.168.1.1

PS C:\Users\administrator.VLABS1> 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=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\administrator.VLABS1>
```

3.5.6.2 Ping DC201

nslookup DC201.vlabs1.com

ping 192.168.45.1

```
PS C:\Users\administrator.VLABS1> nslookup DC201.vlabs1.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  192.168.1.1

Name:    DC201.vlabs1.com
Address:  192.168.45.1

PS C:\Users\administrator.VLABS1> ping 192.168.45.1

Pinging 192.168.45.1 with 32 bytes of data:
Reply from 192.168.45.1: bytes=32 time<1ms TTL=127
Reply from 192.168.45.1: bytes=32 time<1ms TTL=127
Reply from 192.168.45.1: bytes=32 time<1ms TTL=127
Reply from 192.168.45.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.45.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\administrator.VLABS1>
PS C:\Users\administrator.VLABS1>
```

3.5.6.3 Ping DC301

nslookup DC301.lab1.vlabs1.com
ping 192.168.1.3

```
PS C:\Users\administrator.VLABS1>
PS C:\Users\administrator.VLABS1> nslookup DC301.lab1.vlabs1.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
Name:    DC301.lab1.vlabs1.com
Address:  192.168.1.3

PS C:\Users\administrator.VLABS1> ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\administrator.VLABS1>
PS C:\Users\administrator.VLABS1>
PS C:\Users\administrator.VLABS1>
```

4 Task 2: Configuring DC401 as a new child domain

New child domain called **partner1.vlabs1.com** must be created

4.1 Precheck DC401

4.1.1 Basic System Info

```
# Hostname
hostname

# Confirm current domain membership (should be WORKGROUP before join)
(Get-ComputerInfo).CsDomain
```

```
PS C:\Users\administrator.VLABS1> # Hostname
PS C:\Users\administrator.VLABS1> hostname
DC401
PS C:\Users\administrator.VLABS1>
PS C:\Users\administrator.VLABS1> # Confirm current domain membership (should be WORKGROUP before join)
PS C:\Users\administrator.VLABS1> (Get-ComputerInfo).CsDomain
vlabs1.com
PS C:\Users\administrator.VLABS1>
```

4.1.2 Network and DNS Checks

```
# Check DNS resolution of the forest root domain
nslookup vlabs1.com
```

```
PS C:\Users\administrator.VLABS1> # Check DNS resolution of the forest root domain
PS C:\Users\administrator.VLABS1> 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
```

```
# Confirm you can reach the primary domain controller
Test-Connection -ComputerName 192.168.1.1 -Count 4
```

```
PS C:\Users\administrator.VLABS1> # Confirm you can reach the primary domain controller
PS C:\Users\administrator.VLABS1> Test-Connection -ComputerName 192.168.1.1 -Count 4

Source        Destination     IPV4Address      IPV6Address                              Bytes    Time(ms)
------        -----------     -----------      -----------                              -----    --------
DC401         192.168.1.1                                                               32       0
DC401         192.168.1.1                                                               32       0
DC401         192.168.1.1                                                               32       0
DC401         192.168.1.1                                                               32       0
```

```
# Verify DNS is set to the right DC
Get-DnsClientServerAddress
```

```
PS C:\Users\administrator.VLABS1>
PS C:\Users\administrator.VLABS1> # Verify DNS is set to the right DC
PS C:\Users\administrator.VLABS1> Get-DnsClientServerAddress

InterfaceAlias               Interface Address ServerAddresses
                             Index     Family
-------------               --------- ------- ---------------
Ethernet0                           6 IPv4    {192.168.1.1}
Ethernet0                           6 IPv6    {}
Loopback Pseudo-Interface 1         1 IPv4    {}
Loopback Pseudo-Interface 1         1 IPv6    {}
```

```
# Display full IP config
ipconfig /all
```

```
PS C:\Users\administrator.VLABS1>
PS C:\Users\administrator.VLABS1> # Display full IP config
PS C:\Users\administrator.VLABS1> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DC401
   Primary Dns Suffix  . . . . . . . : vlabs1.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : vlabs1.com

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-CE-5B-60
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.35.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.35.50
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
PS C:\Users\administrator.VLABS1>
```

4.1.3 Test Required Ports to DC101

```
# Test core AD-related ports to the parent DC (DC101)
$dc = "192.168.1.1"
$ports = @(53, 88, 135, 389, 445, 636)

foreach ($port in $ports) {
    Test-NetConnection -ComputerName $dc -Port $port
}
```

```
PS C:\Users\administrator.VLABS1>
PS C:\Users\administrator.VLABS1> # Test core AD-related ports to the parent DC (DC101)
PS C:\Users\administrator.VLABS1> $dc = "192.168.1.1"
PS C:\Users\administrator.VLABS1> $ports = @(53, 88, 135, 389, 445, 636)
PS C:\Users\administrator.VLABS1>
PS C:\Users\administrator.VLABS1> foreach ($port in $ports) {
>>     Test-NetConnection -ComputerName $dc -Port $port
>> }
>>


ComputerName     : 192.168.1.1
RemoteAddress    : 192.168.1.1
RemotePort       : 53
InterfaceAlias   : Ethernet0
SourceAddress    : 192.168.35.1
TcpTestSucceeded : True

ComputerName     : 192.168.1.1
RemoteAddress    : 192.168.1.1
RemotePort       : 88
InterfaceAlias   : Ethernet0
SourceAddress    : 192.168.35.1
TcpTestSucceeded : True

ComputerName     : 192.168.1.1
RemoteAddress    : 192.168.1.1
RemotePort       : 135
InterfaceAlias   : Ethernet0
SourceAddress    : 192.168.35.1
TcpTestSucceeded : True

ComputerName     : 192.168.1.1
RemoteAddress    : 192.168.1.1
RemotePort       : 389
InterfaceAlias   : Ethernet0
SourceAddress    : 192.168.35.1
TcpTestSucceeded : True

ComputerName     : 192.168.1.1
RemoteAddress    : 192.168.1.1
RemotePort       : 445
InterfaceAlias   : Ethernet0
```

```
ComputerName     : 192.168.1.1
RemoteAddress    : 192.168.1.1
RemotePort       : 636
InterfaceAlias   : Ethernet0
SourceAddress    : 192.168.35.1
TcpTestSucceeded : True


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

4.1.4 Time Synchronization Check

```
# Check if time is synced with DC
w32tm /query /status
```

```
PS C:\Users\administrator.VLABS1> # Check if time is synced with DC
PS C:\Users\administrator.VLABS1> w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 2 (secondary reference - syncd by (S)NTP)
Precision: -23 (119.209ns per tick)
Root Delay: 0.0016337s
Root Dispersion: 10.5913176s
ReferenceId: 0xC0A82D01 (source IP:  192.168.45.1)
Last Successful Sync Time: 5/17/2025 7:23:16 PM
Source: DC201.vlabs1.com
Poll Interval: 10 (1024s)

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

4.1.5 DNS Zone Check on Parent (run on DC101 if you have access)

Manually verify the `vlabs1.com` DNS zone is working:

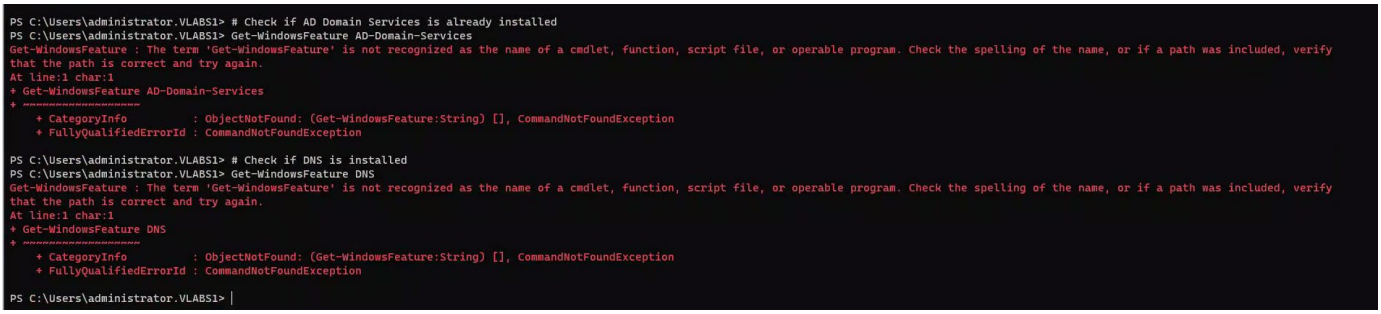
```
# On DC101, verify DNS zones (manually via DNS Manager preferred)
Get-DnsServerZone
```

```
PS C:\Users\Administrator>
PS C:\Users\Administrator>   # On DC101, verify DNS zones (manually via DNS Manager preferred)
PS C:\Users\Administrator> Get-DnsServerZone  # On DC101, verify DNS zones (manually via DNS Manager preferred)

ZoneName                          ZoneType        IsAutoCreated   IsDsIntegrated  IsReverseLookupZone  IsSigned
--------                          --------        -------------   --------------  -------------------  --------
_msdcs.vlabs1.com                 Primary         False           True            False                False
0.in-addr.arpa                    Primary         True            False           True                 False
127.in-addr.arpa                  Primary         True            False           True                 False
255.in-addr.arpa                  Primary         True            False           True                 False
TrustAnchors                      Primary         False           True            False                False
vlabs1.com                        Primary         False           True            False                False


PS C:\Users\Administrator>
```

4.1.6 Confirm AD DS and DNS Roles Are NOT Yet Installed

Giving the following command will results in Errors since DC has not been installed.

```
# Check if AD Domain Services is already installed
Get-WindowsFeature AD-Domain-Services

# Check if DNS is installed
Get-WindowsFeature DNS
```



4.2 Integrate DC401 into the forest as a new child domain

Integrate into the existing **vlabs1.com** forest, a new child domain called **partner1.vlabs1.com.**

4.2.1 Check Domain Membership

1. Verify if the server **DC401** is part of the domain **vlabs1.com**

Get-WmiObject -Class Win32_ComputerSystem | Select-Object Domain

```
PS C:\Users\administrator.VLABS1> Get-WmiObject -Class Win32_ComputerSystem | Select-Object Domain

Domain
------
vlabs1.com


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

a) If the output shows vlabs1.com, your computer is already joined to the domain.

b) If output shows WORKGROUP, your computer is not part of a domain.

Add-Computer -DomainName vlabs1.com -Credential vlabs1\administrator -Verbose -Restart -Force

After **restarting,** login with the **vlabs1\administrator** user account.

4.2.2 Create a new child domain **partner1.vlabs1.com** using **PowerShell**

A. install the AD DS role manually

Install-WindowsFeature AD-Domain-Services -IncludeManagementTools

Get-WindowsFeature AD-Domain-Services

```
PS C:\Users\administrator.VLABS1>
PS C:\Users\administrator.VLABS1> Install-WindowsFeature AD-Domain-Services -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services, Group P...


PS C:\Users\administrator.VLABS1> Get-WindowsFeature AD-Domain-Services

Display Name                                            Name                    Install State
------------                                            ----                    -------------
[X] Active Directory Domain Services                    AD-Domain-Services          Installed


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

```
Install-ADDSDomain `
    -NewDomainName "partner1" `
    -ParentDomainName "vlabs1.com" `
    -InstallDns `
    -CreateDnsDelegation `
    -DomainMode "WinThreshold" `
    -NoGlobalCatalog:$true `
    -SafeModeAdministratorPassword (ConvertTo-SecureString "Passw0rd$" -AsPlainText
-Force) `
 -Force
```

```
PS C:\Users\administrator.VLABS1> Install-ADDSDomain `
>>     -NewDomainName "partner1" `
>>     -ParentDomainName "vlabs1.com" `
>>     -InstallDns `
>>     -CreateDnsDelegation `
>>     -DomainMode "WinThreshold" `
>>     -NoGlobalCatalog:$true `
>>     -SafeModeAdministratorPassword (ConvertTo-SecureString "Passw0rd$" -AsPlainText -Force) `
>>     -Force
```

Command failed because of local password

The new domain cannot be created because the local Administrator account password does not meet requirements. Currently, the local Administrator password is blank, which might lead to security issues

```
PS C:\Users\administrator.VLABS1> Install-ADDSDomain `
>>     -NewDomainName "partner1" `
>>     -ParentDomainName "vlabs1.com" `
>>     -InstallDns `
>>     -CreateDnsDelegation `
>>     -DomainMode "WinThreshold" `
>>     -NoGlobalCatalog:$true `
>>     -SafeModeAdministratorPassword (ConvertTo-SecureString "Passw0rd$" -AsPlainText -Force) `
>>     -Force
Install-ADDSDomain : Verification of prerequisites for Domain Controller promotion failed. The local Administrator account becomes the domain Administrator account when you create a new domain. The new
domain cannot be created because the local Administrator account password does not meet requirements.
Currently, the local Administrator password is blank, which might lead to security issues. We recommend that you press Ctrl+Alt+Delete, use the net user command-line tool, or use Local Users and Groups to
set a strong password for the local Administrator account before you create the new domain.
At line:1 char:1
+ Install-ADDSDomain `
+ ~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Install-ADDSDomain], TestFailedException
    + FullyQualifiedErrorId : Test.VerifyDcPromoCore.DCPromo.General.94,Microsoft.DirectoryServices.Deployment.PowerShell.Commands.InstallADDSDomainCommand

Message
-------
Verification of prerequisites for Domain Controller promotion failed. The local Administrator account becomes the domain Administrator account when you create a new domain. The new domain cannot be created...
```

If command fails because of local password

Reset local password to Passw0rd

1. Check if the Local Administrator Password Is Blank

   runas /user:Administrator cmd

   If received RUNAS ERROR: Unable to run...: The user name or password is incorrect.

   Then the password is not blank (but could still be weak or expired).

2. Check Password Status Using PowerShell (No Password Disclosure)

   Get-LocalUser -Name "administrator"

3. Force Set a Secure Password (Safe and Recommended)

   # Reset the password

   net user Administrator "Passw0rd$"

4. Test password

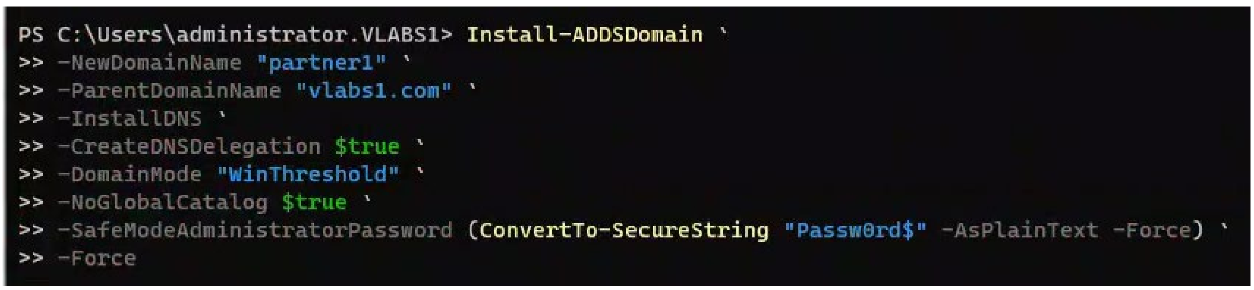
   # Test the password

   runas /user:administrator cmd

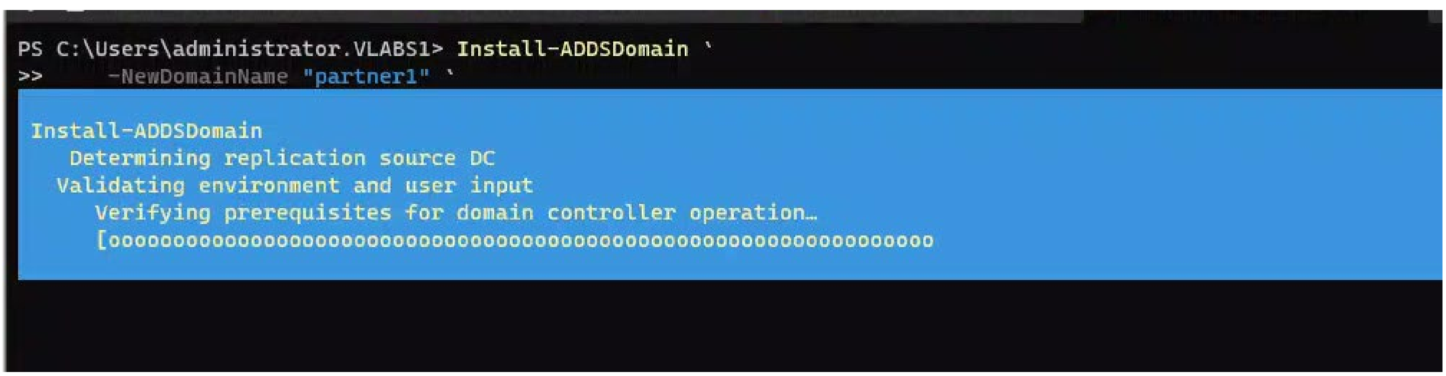
```
PS C:\Users\administrator.VLABS1> runas /user:administrator cmd
Enter the password for administrator:
Attempting to start cmd as user "DC401\administrator" ...
RUNAS ERROR: Unable to run - cmd
1326: The user name or password is incorrect.

PS C:\Users\administrator.VLABS1> Get-LocalUser -Name "administrator"

Name          Enabled Description
----          ------- -----------
Administrator True    Built-in account for administering the computer/domain


PS C:\Users\administrator.VLABS1> ## Reste the password
PS C:\Users\administrator.VLABS1> net user Administrator "Passw0rd$"
The command completed successfully.

PS C:\Users\administrator.VLABS1> Get-LocalUser -Name "administrator"

Name          Enabled Description
----          ------- -----------
Administrator True    Built-in account for administering the computer/domain


PS C:\Users\administrator.VLABS1> runas /user:administrator cmd
Enter the password for administrator:
Attempting to start cmd as user "DC401\administrator" ...
PS C:\Users\administrator.VLABS1>
```

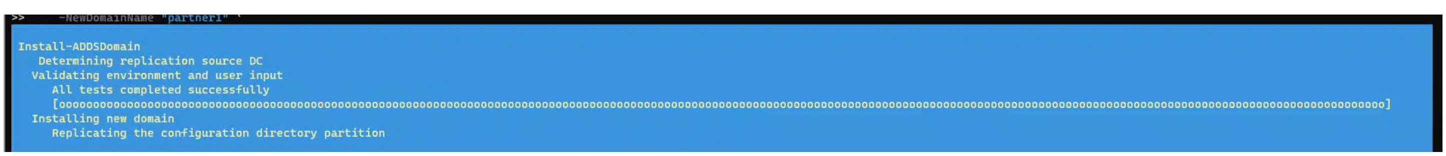
Re-run the Promotion

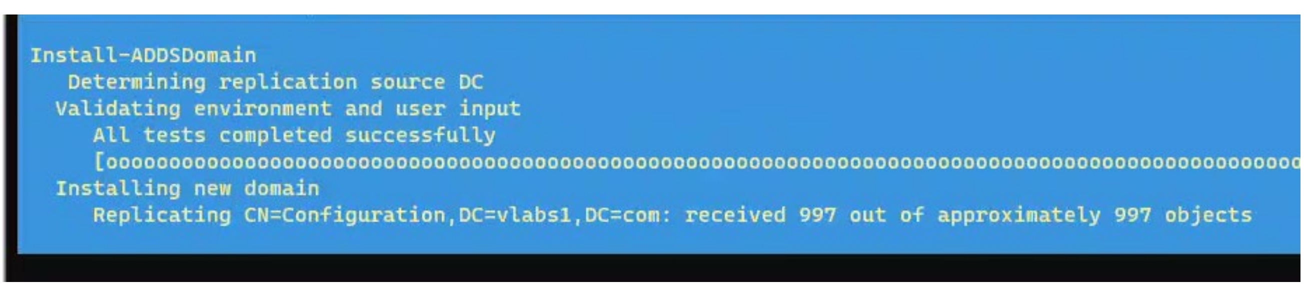
```
Install-ADDSDomain `
    -NewDomainName "partner1" `
    -ParentDomainName "vlabs1.com" `
    -InstallDns `
    -CreateDnsDelegation `
    -DomainMode "WinThreshold" `
    -NoGlobalCatalog:$true `
    -SafeModeAdministratorPassword (ConvertTo-SecureString "Passw0rd$" -AsPlainText
-Force) `
 -Force
```

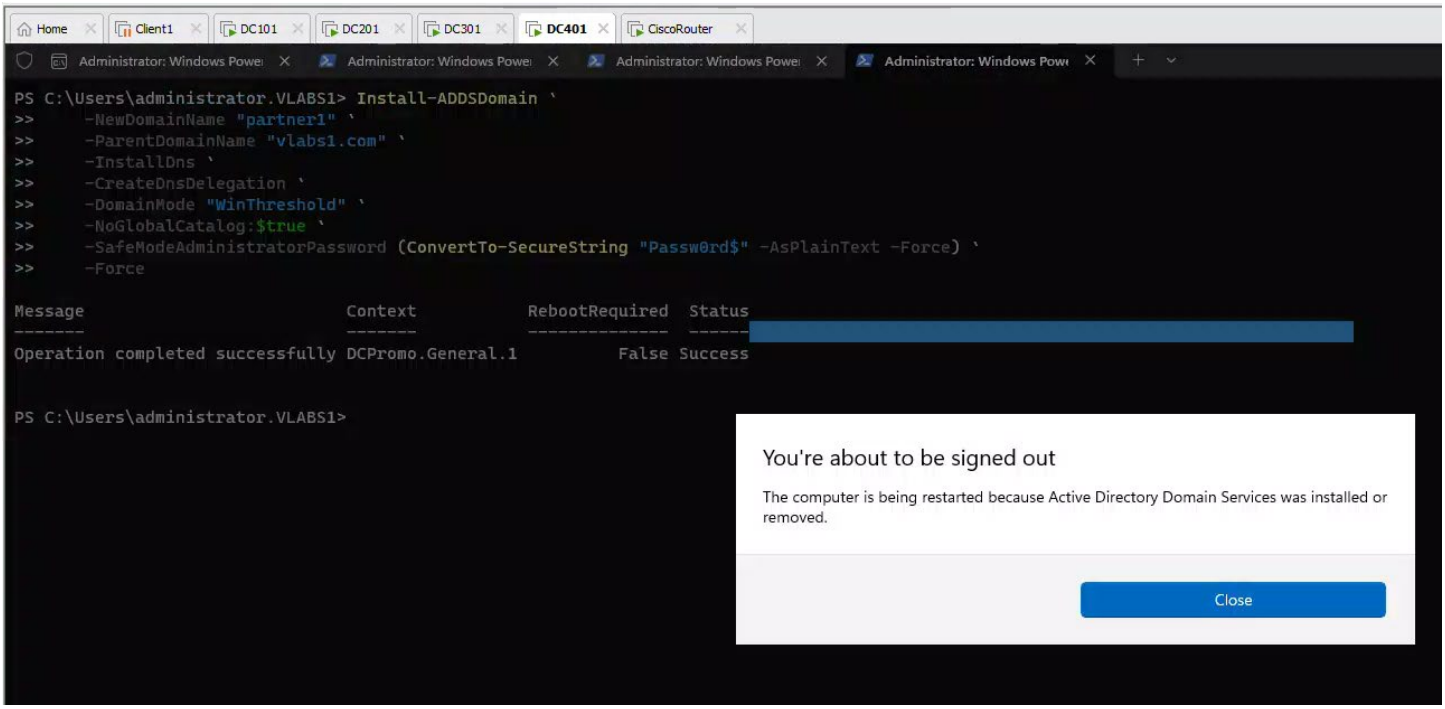


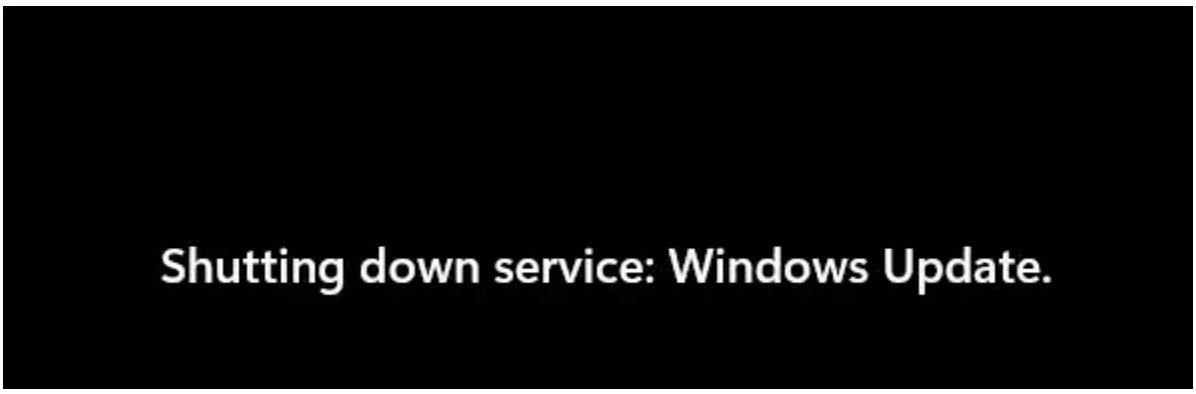
Wait

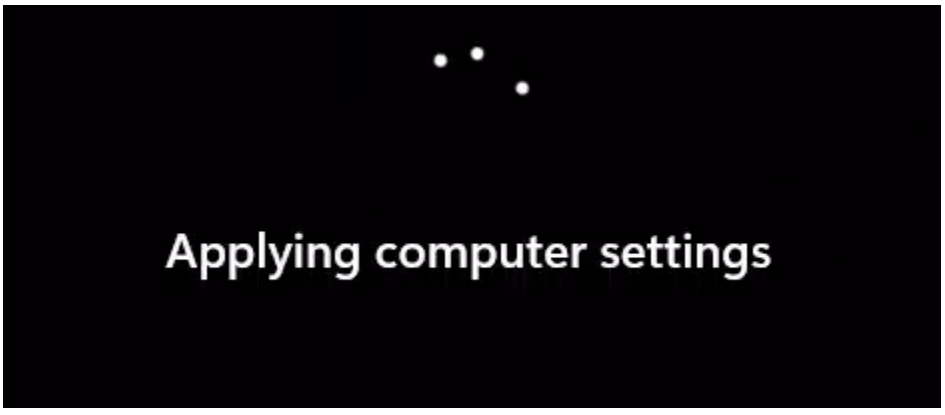




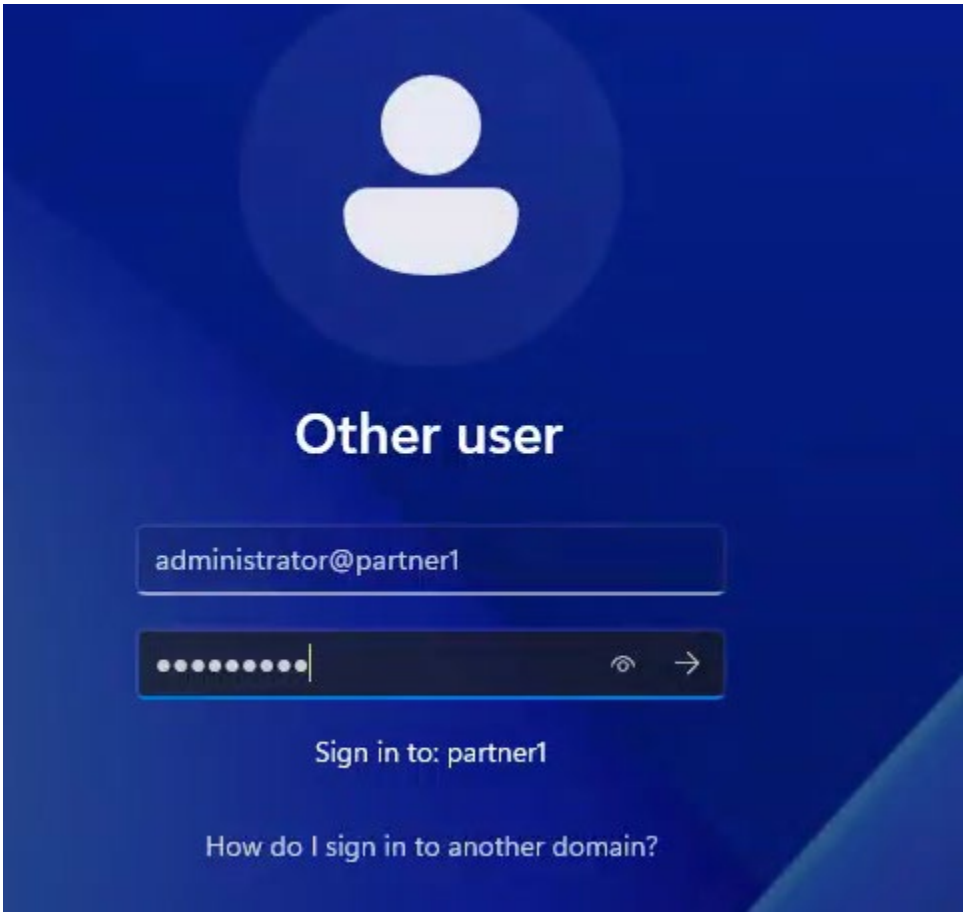



Home
Client1
DC101
DC201
DC301
DC401
CiscoRouter
Administrator: Windows Powe
Administrator: Windows Powe
Administrator: Windows Powe
Administrator: Windows Powe
PS C:\Users\administrator.VLABS1> Install-ADDSDomain `
>> -NewDomainName "partner1" `
>> -ParentDomainName "vlabs1.com" `
>> -InstallDns `
>> -CreateDnsDelegation `
>> -DomainMode "WinThreshold" `
>> -NoGlobalCatalog:$true `
>> -SafeModeAdministratorPassword (ConvertTo-SecureString "Passw0rd$" -AsPlainText -Force) `
>> -Force
Message Context RebootRequired Status
Operation completed successfully DCPromo.General.1 False Success
PS C:\Users\administrator.VLABS1>
You're about to be signed out
The computer is being restarted because Active Directory Domain Services was installed or removed.
Close


Shutting down service: Windows Update.


Applying computer settings

Login



4.3 Postchecks

4.3.1 Verify Domain and Forest Membership

 # Verify the current domain on DC401
(Get-ADDomain).DNSRoot
(Get-ADDomain).DistinguishedName
(Get-ADForest).RootDomain

```
PS C:\Users\Administrator> # Verify the current domain on DC401
PS C:\Users\Administrator> (Get-ADDomain).DNSRoot
partner1.vlabs1.com
PS C:\Users\Administrator> (Get-ADDomain).DistinguishedName
DC=partner1,DC=vlabs1,DC=com
PS C:\Users\Administrator> (Get-ADForest).RootDomain
vlabs1.com
PS C:\Users\Administrator>
```

4.3.2 Verify Domain Controller Status

Check that DC401 is functioning properly as a domain controller:

 # Check if this server is recognized as a DC
Get-ADDomainController -Discover -Service "PrimaryDC"

```
vlabs1.com
PS C:\Users\Administrator> # Check if this server is recognized as a DC
PS C:\Users\Administrator> Get-ADDomainController -Discover -Service "PrimaryDC"


Domain      : partner1.vlabs1.com
Forest      : vlabs1.com
HostName    : {DC401.partner1.vlabs1.com}
IPv4Address : 192.168.35.1
IPv6Address : ::1
Name        : DC401
Site        : Default-First-Site-Name



PS C:\Users\Administrator>
```

 # Verify Global Catalog setting
(Get-ADDomainController).IsGlobalCatalog

```
PS C:\Users\Administrator> # Verify Global Catalog setting
PS C:\Users\Administrator> (Get-ADDomainController).IsGlobalCatalog
False
PS C:\Users\Administrator>
```

 # Check AD DS service status
Get-Service NTDS, Netlogon, KDC

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> # Check AD DS service status
PS C:\Users\Administrator> Get-Service NTDS, Netlogon, KDC

Status   Name               DisplayName
------   ----               -----------
Running  KDC                Kerberos Key Distribution Center
Running  Netlogon           Netlogon
Running  NTDS               Active Directory Domain Services


PS C:\Users\Administrator>
```

4.3.3 DNS Verification

Confirm DNS for the new child domain is in place and delegated correctly.

 # Check for the presence of partner1.vlabs1.com DNS zone on DC401
Get-DnsServerZone

```
PS C:\Users\Administrator> # Check for the presence of partner1.vlabs1.com DNS zone on DC401
PS C:\Users\Administrator> Get-DnsServerZone

ZoneName                          ZoneType        IsAutoCreated   IsDsIntegrated  IsReverseLookupZone  IsSigned
--------                          --------        -------------   --------------  -------------------  --------
_msdcs.vlabs1.com                 Primary         False           True            False                False
0.in-addr.arpa                    Primary         True            False           True                 False
127.in-addr.arpa                  Primary         True            False           True                 False
255.in-addr.arpa                  Primary         True            False           True                 False
partner1.vlabs1.com               Primary         False           True            False                False
TrustAnchors                      Primary         False           True            False                False


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

 # Test forward lookup
nslookup dc401.partner1.vlabs1.com

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> # Test forward and reverse lookup
PS C:\Users\Administrator> nslookup dc401.partner1.vlabs1.com
Server:  localhost
Address:  127.0.0.1

Name:    dc401.partner1.vlabs1.com
Address:  192.168.35.1
```

 # Check DNS server settings
Get-DnsServerSetting

 # Verify DNS forwarders
Get-DnsServerForwarder

```
PS C:\Users\Administrator> # Check DNS server settings
PS C:\Users\Administrator> Get-DnsServerSetting


ComputerName       : DC401.partner1.vlabs1.com
MajorVersion       : 10
MinorVersion       : 0
BuildNumber        : 26100
IsReadOnlyDC       : False
EnableDnsSec       : True
EnableIPv6         : True
ListeningIPAddress : 192.168.35.1
AllIPAddress       : 192.168.35.1



PS C:\Users\Administrator>
PS C:\Users\Administrator> # Verify DNS forwarders
PS C:\Users\Administrator> Get-DnsServerForwarder


UseRootHint        : True
Timeout(s)         : 3
EnableReordering   : True
IPAddress          : 192.168.1.1
ReorderedIPAddress : 192.168.1.1
```

4.3.4 Active Directory Replication

Ensure replication is working between DC401 and the rest of the forest.

 # General replication summary
repadmin /replsummary

```
*** Request to localhost timed out
PS C:\Users\Administrator> # General replication summary
PS C:\Users\Administrator> repadmin /replsummary
Replication Summary Start Time: 2025-05-17 21:45:54

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


Source DSA          largest delta    fails/total %%   error
 DC101                      56m:28s    1 /  15    6  (1908) Could not find the domain controller for this domain.
 DC301                      56m:28s    0 /  13    0
 DC401                      15m:17s    0 /  12    0


Destination DSA     largest delta    fails/total %%   error
 DC101                      48m:24s    0 /   9    0
 DC201                      56m:29s    0 /  16    0
 DC301                      50m:19s    0 /   9    0
 DC401                      28m:35s    1 /   6   16  (1908) Could not find the domain controller for this domain.


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

Error 1908 appears

(1908) Could not find the domain controller for this domain.

The error 1908 usually occurs when:

- A DC cannot locate another DC in the forest (via DNS).
- Trust or replication paths are incomplete or misconfigured.
- There’re missing or incorrect DNS records (A or SRV).
- A site link or replication connection hasn't been auto-generated or manually added.

This is especially common right after promoting a new child domain (like partner1.vlabs1.com) before full replication topology stabilizes.

After some minutes a recheck is done and now it is successful

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> repadmin /replsummary
Replication Summary Start Time: 2025-05-17 21:50:48

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


Source DSA          largest delta    fails/total %%   error
 DC101                      55m:12s    0 /  15    0
 DC301                      53m:17s    0 /  13    0
 DC401                      20m:11s    0 /  12    0


Destination DSA     largest delta    fails/total %%   error
 DC101                      53m:17s    0 /   9    0
 DC201                      01m:22s    0 /  16    0
 DC301                      55m:12s    0 /   9    0
 DC401                      01m:16s    0 /   6    0


PS C:\Users\Administrator>
```

 # Show replication partners and status for DC401
repadmin /showrepl

```
PS C:\Users\Administrator> # Show replication partners and status for DC401
PS C:\Users\Administrator> repadmin /showrepl

Repadmin: running command /showrepl against full DC localhost
Default-First-Site-Name\DC401
DSA Options: (none)
Site Options: (none)
DSA object GUID: 01004c70-51e1-4b52-9a48-aac4cc610935
DSA invocationID: c2041984-2615-45fd-89e7-5413c2204d8b

==== 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 @ 2025-05-17 21:49:32 was successful.
    Default-First-Site-Name\DC301 via RPC
        DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
        Last attempt @ 2025-05-17 21:49:32 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 @ 2025-05-17 21:49:32 was successful.
    Default-First-Site-Name\DC301 via RPC
        DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
        Last attempt @ 2025-05-17 21:49:32 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 @ 2025-05-17 21:49:32 was successful.
    Default-First-Site-Name\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-17 21:49:32 was successful.

Source: Default-First-Site-Name\DC101
******* 1 CONSECUTIVE FAILURES since 2025-05-17 21:17:20
Last error: 1908 (0x774):
            Could not find the domain controller for this domain.

PS C:\Users\Administrator>
```

Replication Warning (DC101 as a source)

Source: Default-First-Site-Name\DC101
******* *1 CONSECUTIVE FAILURES since 2025-05-17 21:17:20*
Last error: 1908 (0x774):
Could not find the domain controller for this domain.

This is a replication failure recorded in the past, likely during or immediately after promotion.

Error 1908 again indicates domain controller discovery failed temporarily (likely before DNS delegation or replication links stabilized).

Since all recent replication attempts from DC101 to DC401 are now successful, this old failure is not critical — no further action is required unless it continues.

4.3.4.1 Repair

1. Clear Old Error by Forcing Replication Again
This resets the failure count and ensures stability:

repadmin /syncall /AdeP

```
PS C:\Users\Administrator> repadmin /syncall /AdeP
Syncing all NC's held on DC401.
Syncing partition: DC=DomainDnsZones,DC=partner1,DC=vlabs1,DC=com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

Syncing partition: DC=partner1,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

Syncing partition: DC=ForestDnsZones,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: Error issuing replication: 8453 (0x2105):
    Replication access was denied.
    From: CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: Error issuing replication: 8453 (0x2105):
    Replication access was denied.
    From: CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: SyncAll Finished.
```

... (printout edited because it was long)

```
Syncing partition: CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: Error issuing replication: 8453 (0x2105):
    Replication access was denied.
    From: CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: Error issuing replication: 8453 (0x2105):
    Replication access was denied.
    From: CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: SyncAll Finished.

SyncAll reported the following errors:
Error issuing replication: 8453 (0x2105):
    Replication access was denied.
    From: CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
Error issuing replication: 8453 (0x2105):
    Replication access was denied.
    From: CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com

PS C:\Users\Administrator>
```

Error issuing replication: 8453 (0x2105): Replication access was denied.
…indicates that DC401 is not authorized to push replication to DC101 and DC301.

4.3.4.1.1 Repair from DC101

Run repadmin Remotely from DC101

Log in to DC101 or DC301 and run:

repadmin /syncall /AdeP

This pushes replication down from parent to child — which is usually how replication is managed in multi-domain forests.

```
PS C:\Users\Administrator> repadmin /syncall /AdeP
Syncing all NC's held on DC101.
Syncing partition: DC=ForestDnsZones,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

Syncing partition: DC=DomainDnsZones,DC=vlabs1,DC=com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

Syncing partition: CN=Schema,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
```

... (printout edited because it was long)

```
Syncing partition: DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

Syncing partition: DC=partner1,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

Syncing partition: DC=lab1,DC=vlabs1,DC=com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

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

4.3.4.2 Re-test

Run again on DC401

General replication summary
repadmin /replsummary

```
PS C:\Users\Administrator> repadmin /replsummary
Replication Summary Start Time: 2025-05-17 22:35:14

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


Source DSA          largest delta    fails/total %%   error
 DC101                  45m:48s    0 /  15    0
 DC301                  45m:48s    0 /  13    0
 DC401                  45m:48s    0 /  12    0


Destination DSA     largest delta    fails/total %%   error
 DC101                  37m:42s    0 /   9    0
 DC201                  45m:48s    0 /  16    0
 DC301                  39m:38s    0 /   9    0
 DC401                  45m:42s    0 /   6    0
```

Show replication partners and status for DC401
repadmin /showrepl

```
PS C:\Users\Administrator> # Show replication partners and status for DC401
PS C:\Users\Administrator> repadmin /showrepl

Repadmin: running command /showrepl against full DC localhost
Default-First-Site-Name\DC401
DSA Options: (none)
Site Options: (none)
DSA object GUID: 01004c70-51e1-4b52-9a48-aac4cc610935
DSA invocationID: c2041984-2615-45fd-89e7-5413c2204d8b

==== 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 @ 2025-05-17 21:49:32 was successful.
    Default-First-Site-Name\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-17 22:33:37 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 @ 2025-05-17 21:49:32 was successful.
    Default-First-Site-Name\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-17 22:33:36 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 @ 2025-05-17 21:49:32 was successful.
    Default-First-Site-Name\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-17 22:33:36 was successful.

PS C:\Users\Administrator>
```

Verify if objects from the parent forest are visible
Get-ADForest | Select Domains

```
PS C:\Users\Administrator> # Verify if objects from the parent forest are visible
PS C:\Users\Administrator> Get-ADForest | Select Domains

Domains
-------
{lab1.vlabs1.com, partner1.vlabs1.com, vlabs1.com}
```

4.3.5 Trust Relationship Validation

Validate automatic trust between child and parent domains:

4.3.5.1 From DC401

From DC401
Get-ADTrust -Filter *

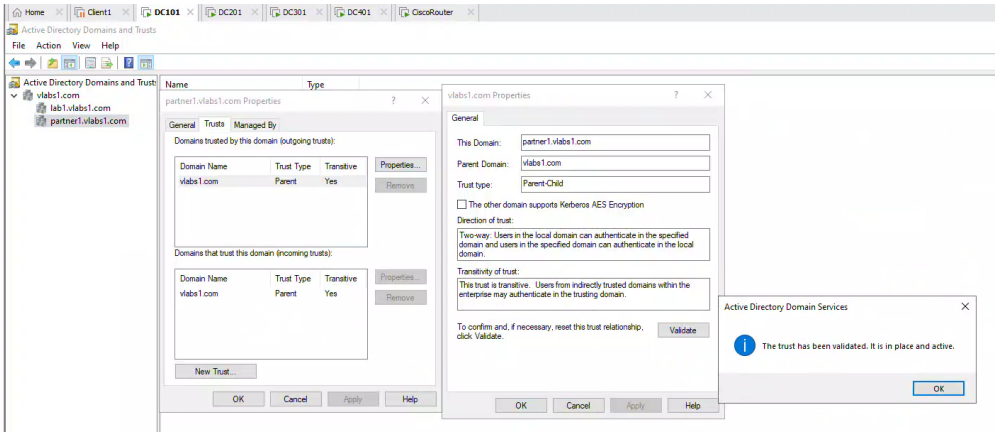
```
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADTrust -Filter *


Direction               : BiDirectional
DisallowTransivity      : False
DistinguishedName       : CN=vlabs1.com,CN=System,DC=partner1,DC=vlabs1,DC=com
ForestTransitive        : False
IntraForest             : True
IsTreeParent            : False
IsTreeRoot              : False
Name                    : vlabs1.com
ObjectClass             : trustedDomain
ObjectGUID              : 34c5e84f-598f-4c59-86e1-4f94a2d0a223
SelectiveAuthentication : False
SIDFilteringForestAware : False
SIDFilteringQuarantined : False
Source                  : DC=partner1,DC=vlabs1,DC=com
Target                  : vlabs1.com
TGTDelegation           : False
TrustAttributes         : 32
TrustedPolicy           :
TrustingPolicy          :
TrustType               : Uplevel
UplevelOnly             : False
UsesAESKeys             : False
UsesRC4Encryption       : False



PS C:\Users\Administrator>
```

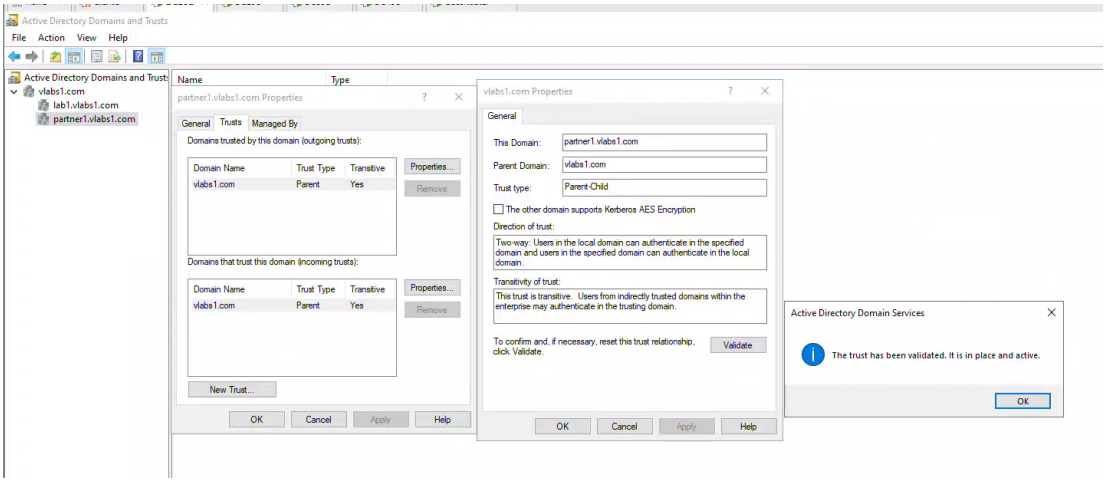
4.3.5.2 From DC101

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


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

Direction               : BiDirectional
DisallowTransivity      : False
DistinguishedName       : CN=partner1.vlabs1.com,CN=System,DC=vlabs1,DC=com
ForestTransitive        : False
IntraForest             : True
IsTreeParent            : False
IsTreeRoot              : False
Name                    : partner1.vlabs1.com
ObjectClass             : trustedDomain
ObjectGUID              : d79b69a1-ab85-4402-b9de-86e424056814
SelectiveAuthentication : False
SIDFilteringForestAware : False
SIDFilteringQuarantined : False
Source                  : DC=vlabs1,DC=com
Target                  : partner1.vlabs1.com
TGTDelegation           : False
TrustAttributes         : 32
TrustedPolicy           :
TrustingPolicy          :
TrustType               : Uplevel
UplevelOnly             : False
UsesAESKeys             : False
UsesRC4Encryption       : False


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

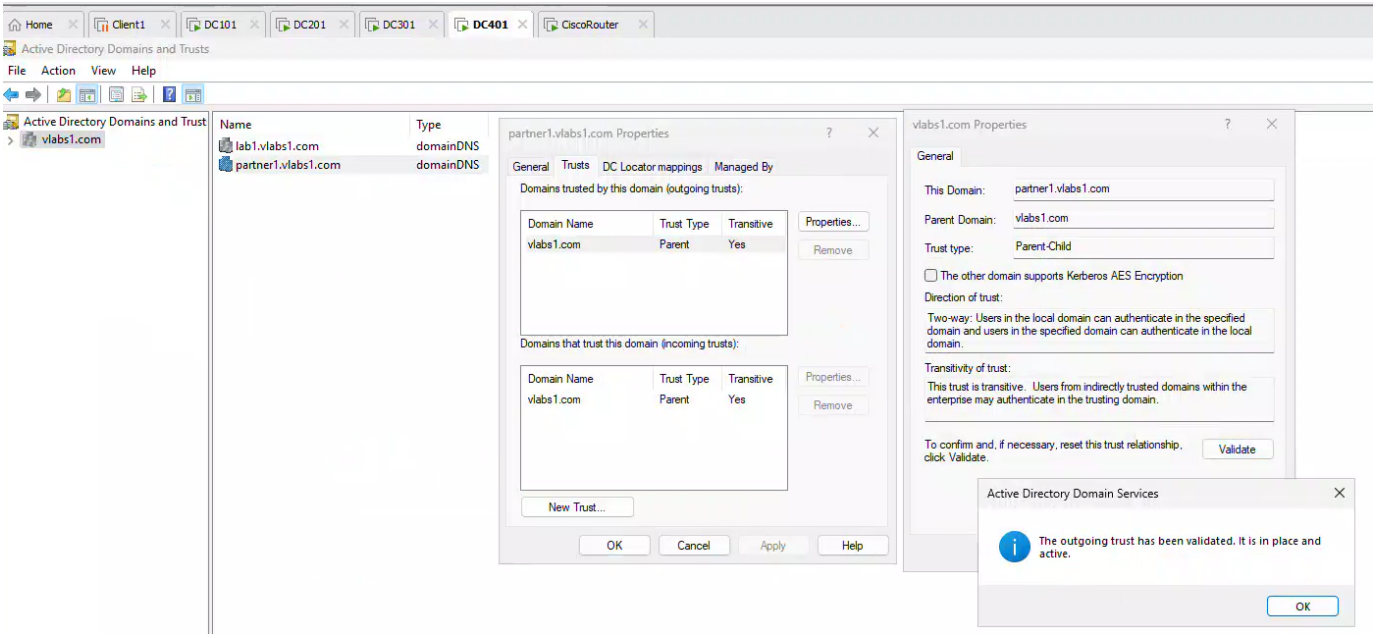
4.3.5.3 GUI check

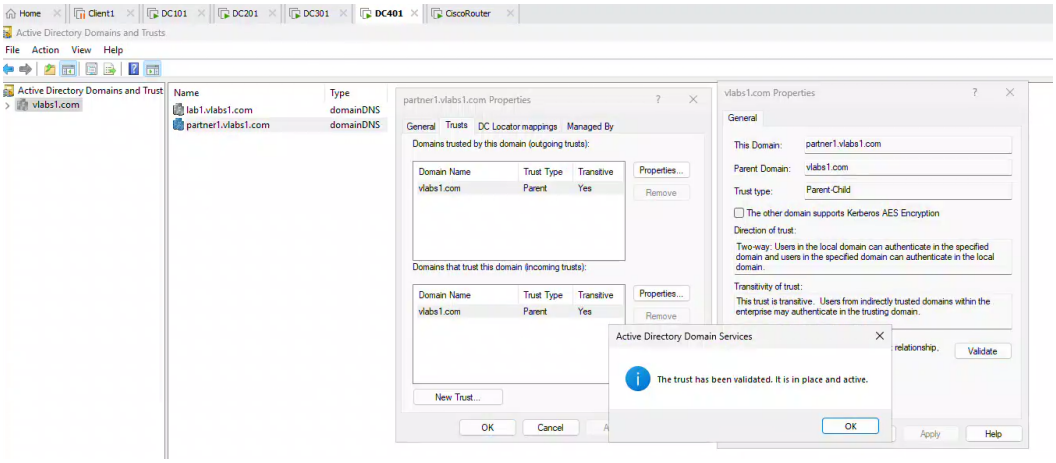
4.3.5.3.1 DC101





4.3.5.3.2 DC401





4.3.6 Event Log Review

Check for errors or warnings after promotion:

Get-EventLog -LogName "Directory Service" -Newest 20
Get-EventLog -LogName "DNS Server" -Newest 20

```
PS C:\Users\Administrator> Get-EventLog -LogName "Directory Service" -Newest 20

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
      76 May 17 21:49  Error       NTDS Database          3221226883 Active Directory Domain Services failed to construct a mutual authentication service principal name (SPN) for the following directory se...
      75 May 17 21:49  Information NTDS Database          1073743865 Duplicate event log entries were suppressed....
      74 May 17 21:34  Error       NTDS Database          3221226883 Active Directory Domain Services failed to construct a mutual authentication service principal name (SPN) for the following directory se...
      73 May 17 21:34  Information NTDS Database          1073744851 Internal event: Online Defragment Start succeeded....
      72 May 17 21:34  Information NTDS Database          1073744857 Internal event: Online Defragment Stop invoked but defrag was not running.
      71 May 17 21:34  Information NTDS Database          1073743865 Duplicate event log entries were suppressed....
      70 May 17 21:34  Information NTDS ISAM                   701 NTDS (792,D,0,0) NTDSA: Online defragmentation has completed a full pass on database 'C:\WINDOWS\NTDS\ntds.dit', freeing 3 pages. This p...
      69 May 17 21:34  Information NTDS ISAM                   700 NTDS (792,D,0,0) NTDSA: Online defragmentation is beginning a full pass on database 'C:\WINDOWS\NTDS\ntds.dit'.
      68 May 17 21:34  Information NTDS ISAM                   330 NTDS (792,D,2,0) NTDSA: The database [C:\WINDOWS\NTDS\temp.edb] format version is being held back to 9600 (0x2580) due to application pa...
      67 May 17 21:34  Information NTDS ISAM                   326 NTDS (792,D,50,0) NTDSA: The database engine attached a database (1, C:\WINDOWS\NTDS\ntds.dit). (Time=0 seconds)...
      66 May 17 21:34  Information NTDS ISAM                   330 NTDS (792,D,50,0) NTDSA: The database [C:\WINDOWS\NTDS\ntds.dit] format version is being held back to 9600 (0x2580) due to application p...
      65 May 17 21:34  Information NTDS ISAM                   105 NTDS (792,D,0,0) NTDSA: The database engine started a new instance (0). (Time=0.023 seconds)...
      64 May 17 21:34  Information NTDS ISAM                   102 NTDS (792,P,98,0) NTDSA: The database engine (10.00.26100.0000) is starting a new instance (0).
      63 May 17 21:31  Error       NTDS Database          3221226883 Active Directory Domain Services failed to construct a mutual authentication service principal name (SPN) for the following directory se...
      62 May 17 21:24  Information NTDS Database          1073743693 Active Directory Domain Services has located a global catalog in the following site....
      61 May 17 21:24  Information NTDS Database          1073744786 Created 8 optional system indices.
      60 May 17 21:24  Information NTDS Database          1073743838 Active Directory Domain Services successfully completed rebuilding the following number of indices....
      59 May 17 21:24  Information NTDS Database          1073743837 Active Directory Domain Services is rebuilding the following number of indices as part of the initialization process....
      58 May 17 21:24  Information NTDS Database          1073744785 Creating 8 optional system indices....
      57 May 17 21:22  Information NTDS Database          1073743889 Active Directory Domain Services has completed rebuilding the quota-tracking table.  Quota enforcement is now in effect.


PS C:\Users\Administrator> Get-EventLog -LogName "DNS Server" -Newest 20

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
      12 May 17 21:36  Information Microsoft-Windows...         4500 The description for Event ID '4500' in Source 'Microsoft-Windows-DNS-Server-Service' cannot be found.  The local computer may not have t...
      11 May 17 21:28  Warning     Microsoft-Windows...         4512 The description for Event ID '4512' in Source 'Microsoft-Windows-DNS-Server-Service' cannot be found.  The local computer may not have t...
      10 May 17 21:23  Information Microsoft-Windows...         7648 The description for Event ID '7648' in Source 'Microsoft-Windows-DNS-Server-Service' cannot be found.  The local computer may not have t...
       9 May 17 21:20  Information Microsoft-Windows...         4502 The description for Event ID '4502' in Source 'Microsoft-Windows-DNS-Server-Service' cannot be found.  The local computer may not have t...
       8 May 17 21:20  Information Microsoft-Windows...            2 The description for Event ID '2' in Source 'Microsoft-Windows-DNS-Server-Service' cannot be found.  The local computer may not have the ...
       7 May 17 21:20  Information Microsoft-Windows...            4 The description for Event ID '4' in Source 'Microsoft-Windows-DNS-Server-Service' cannot be found.  The local computer may not have the ...
       6 May 17 21:20  Information Microsoft-Windows...          769 The description for Event ID '769' in Source 'Microsoft-Windows-DNS-Server-Service' cannot be found.  The local computer may not have th...
       5 May 17 21:19  Warning     Microsoft-Windows...         4013 The description for Event ID '4013' in Source 'Microsoft-Windows-DNS-Server-Service' cannot be found.  The local computer may not have t...
       4 May 17 21:19  Information Microsoft-Windows...         7693 The description for Event ID '7693' in Source 'Microsoft-Windows-DNS-Server-Service' cannot be found.  The local computer may not have t...
       3 May 17 21:19  Information Microsoft-Windows...            3 The description for Event ID '3' in Source 'Microsoft-Windows-DNS-Server-Service' cannot be found.  The local computer may not have the ...
       2 May 17 21:18  Information Microsoft-Windows...         3150 The description for Event ID '3150' in Source 'Microsoft-Windows-DNS-Server-Service' cannot be found.  The local computer may not have t...
       1 May 17 21:18  Information Microsoft-Windows...         2631 The description for Event ID '2631' in Source 'Microsoft-Windows-DNS-Server-Service' cannot be found.  The local computer may not have t...
```

4.3.7 Verify ports

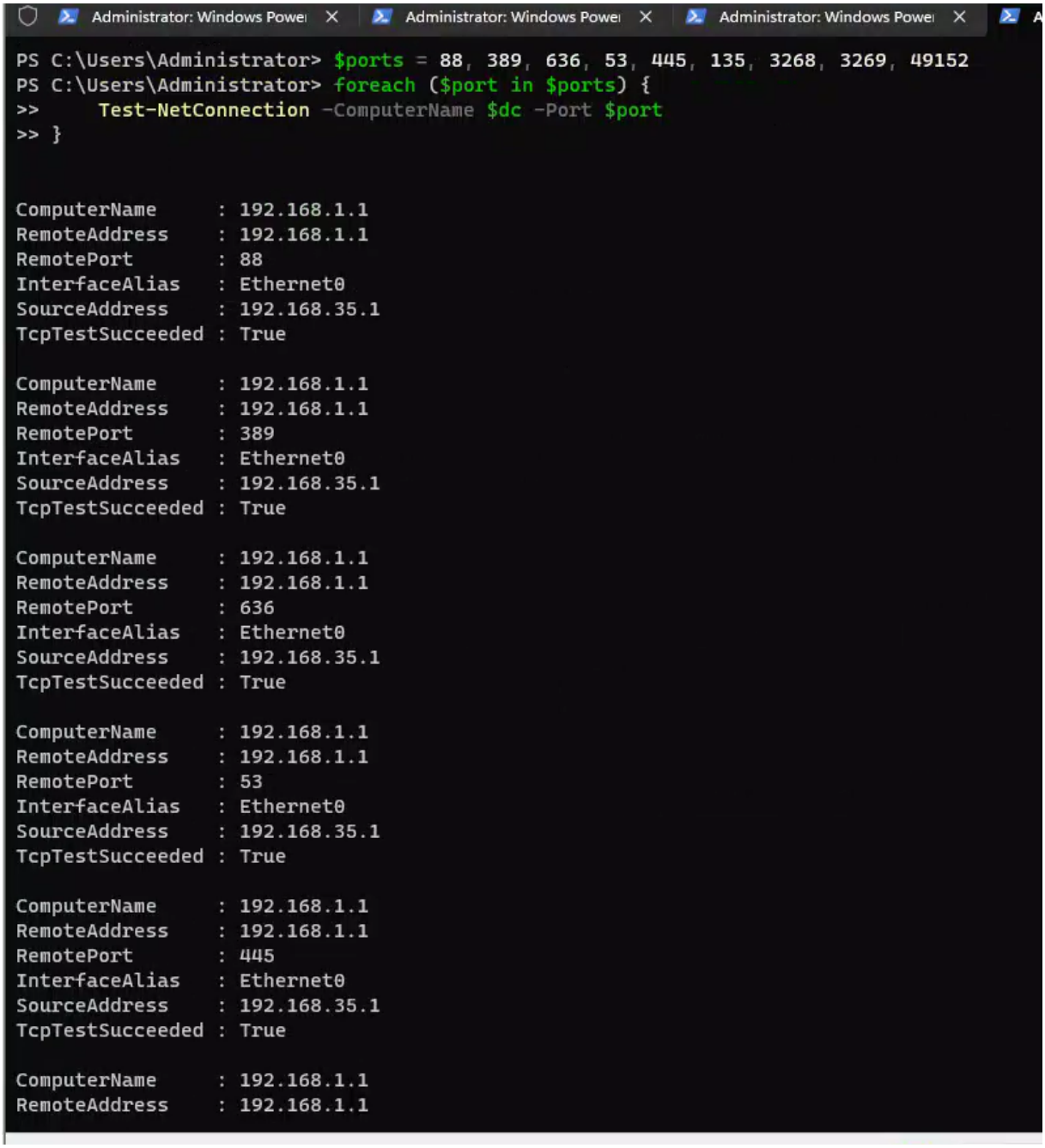
The following ports are verified

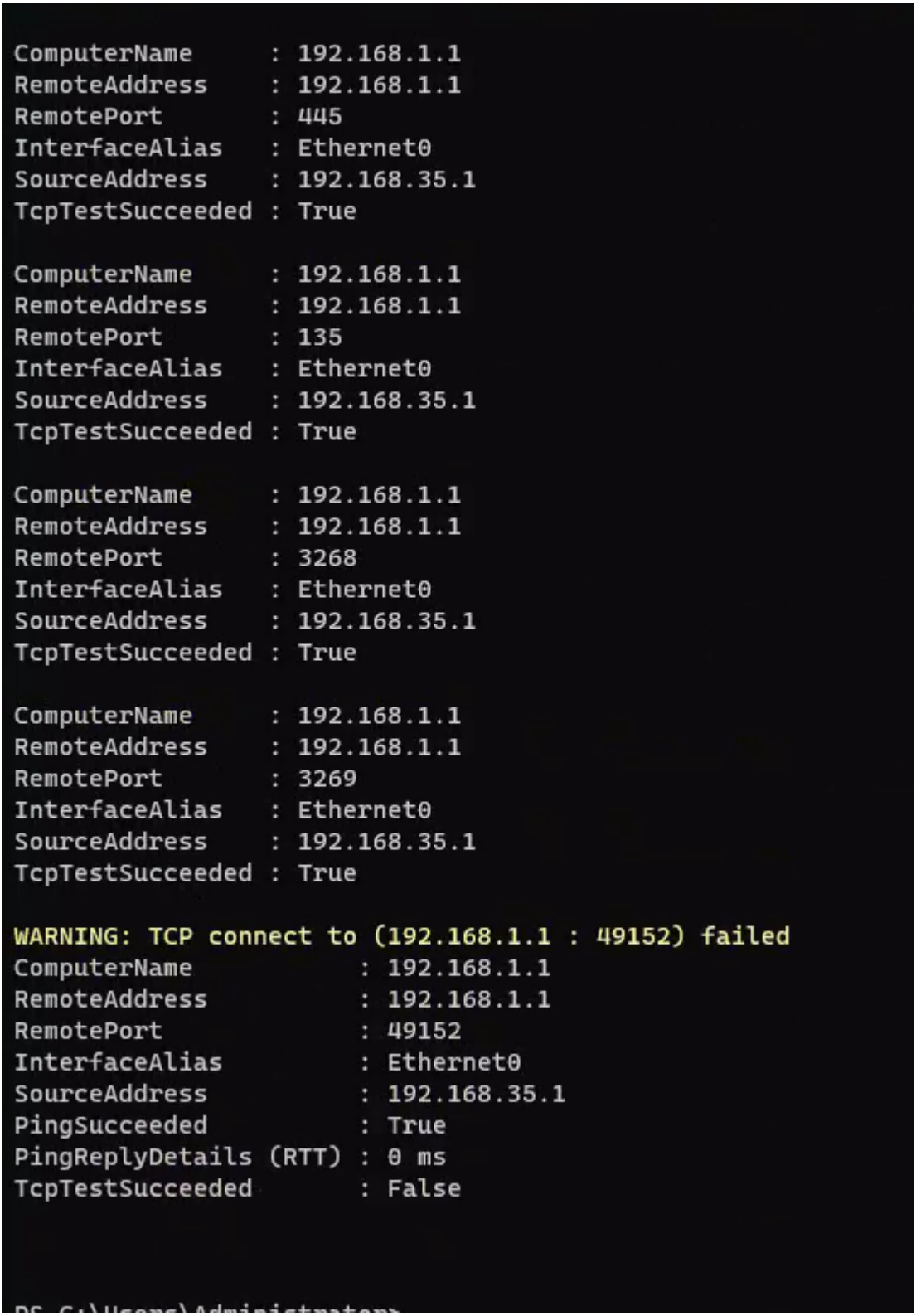
Protocol	Port	Direction	Purpose
TCP	88	Inbound/Outbound	**Kerberos authentication**
TCP/UDP	389	Inbound/Outbound	**LDAP** (Directory Services)
TCP	636	Inbound/Outbound	**LDAPS** (LDAP over SSL)
TCP/UDP	53	Inbound/Outbound	**DNS lookups & zone transfers**
TCP	445	Inbound/Outbound	**SMB (for SYSVOL, NETLOGON)**
TCP	135	Inbound/Outbound	**RPC endpoint mapper**
TCP	139	Inbound/Outbound	**NetBIOS Session** (legacy, optional)
UDP	137-138	Inbound/Outbound	**NetBIOS Name/DATAGRAM** (legacy, optional)
TCP	3268	Inbound/Outbound	**Global Catalog** (if GC is enabled)
TCP	3269	Inbound/Outbound	**Global Catalog over SSL**

TCP	49152–65535	Inbound/Outbound	**Dynamic RPC ports** (required for replication)

DC401

```
# Show all firewall rules affecting port 49152
Get-NetFirewallRule | Where-Object {
  ($_.Direction -eq "Inbound") -and
  ($_.Action -eq "Allow")
} | Get-NetFirewallPortFilter | Where-Object { $_.LocalPort -eq "49152" }
```





DC101
Create a firewall rule to allow in DC101

```
PS C:\Users\Administrator> New-NetFirewallRule -DisplayName "Allow RPC Dynamic Ports" `
>>   -Direction Inbound -Protocol TCP -LocalPort 49152-65535 `
>>   -Action Allow


Name                          : {62448d82-ed77-4a7b-936c-5fc0b43d4157}
DisplayName                   : Allow RPC Dynamic Ports
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Inbound
Action                        : Allow
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId                   :
```

No service is actively listening on port 49152 on DC101
This is expected because RPC dynamic ports are not always listening — they're assigned dynamically by the OS when a service (like AD replication or WMI) needs them.

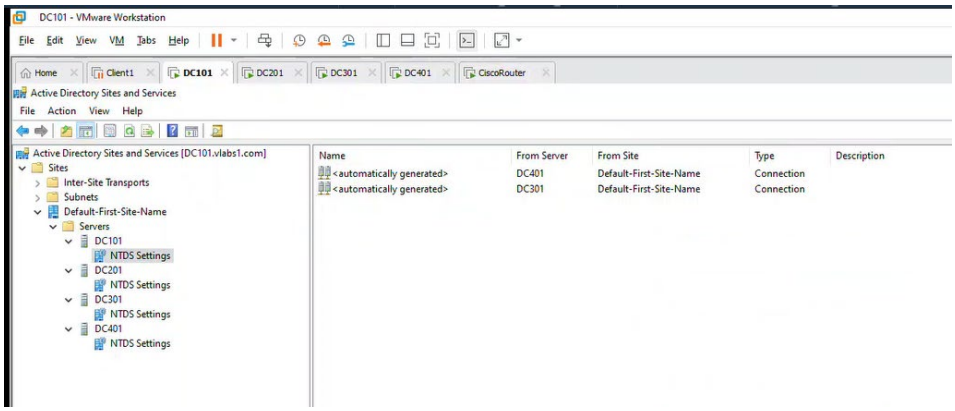
Port could not be tested.

5 Task 3: Managing the Connections Objects

5.1 Using GUI

- List the automatically created **Connection Objects** on **DC101.**

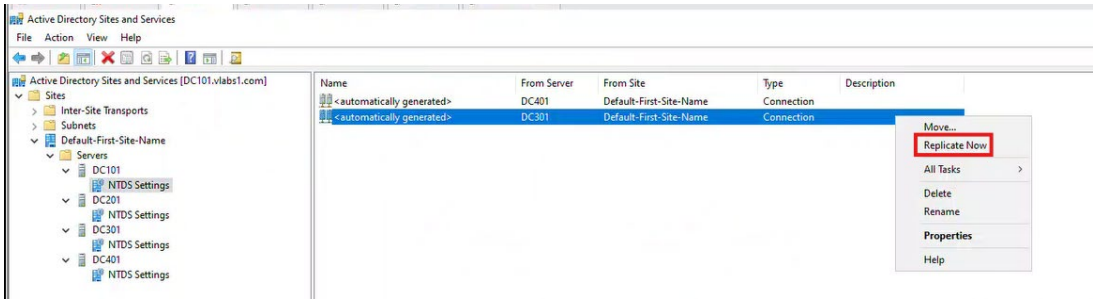
1. Open Active Directory Sites and Services (dssite.msc).
2. Navigate to: Sites → Default-First-Site-Name → Servers → DC101 → NTDS Settings
3. Right-click and check the Connection Objects listed



On the right pane, you'll see Connection Objects.
These are created by the Knowledge Consistency Checker (KCC) automatically.
See entries like: Automatically generated from DC301

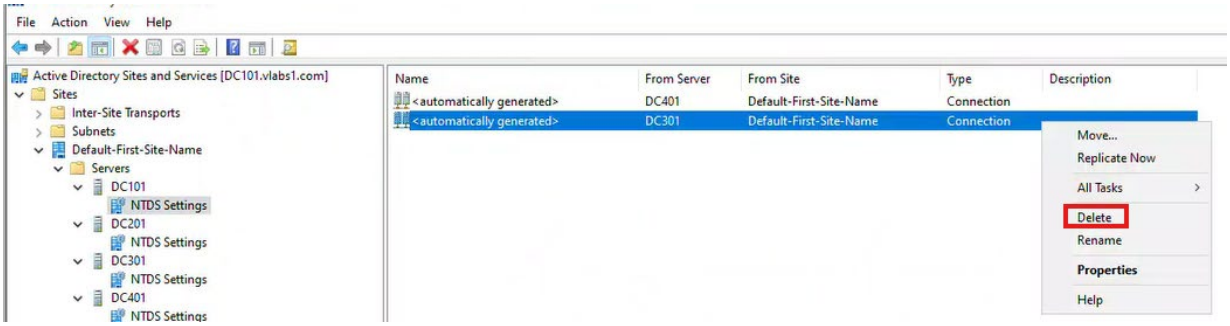
- Replicate manually to **DC301.**

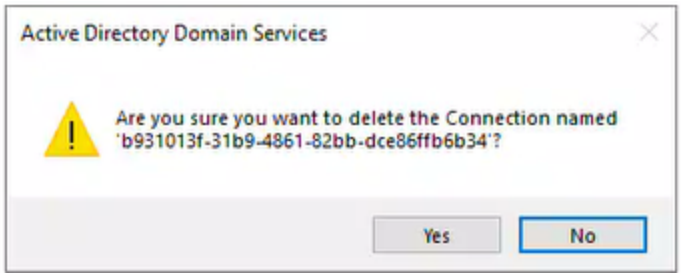
    1. Right-click on the Connection Object that points to DC301.
    2. Choose "Replicate Now".

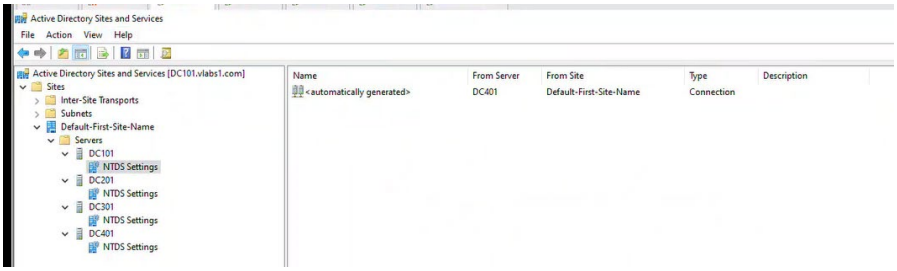


- Delete this Connection object to **DC301.**

    1. Right-click the Connection Object for DC301.
    2. Select Delete and confirm.

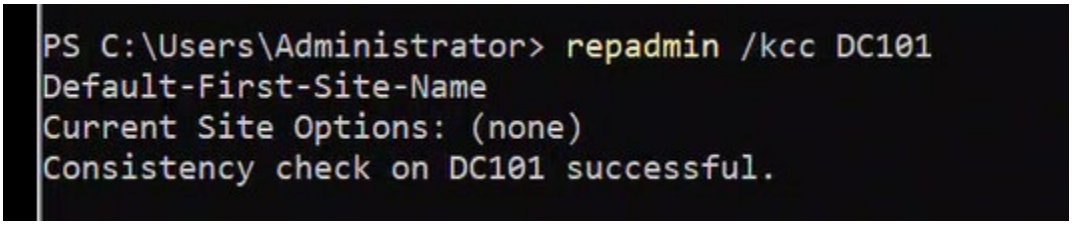


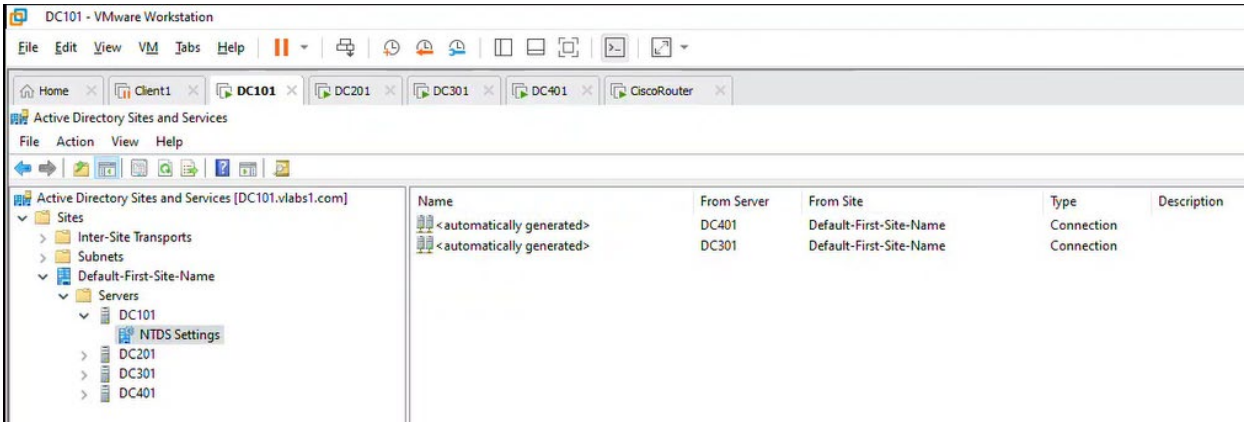




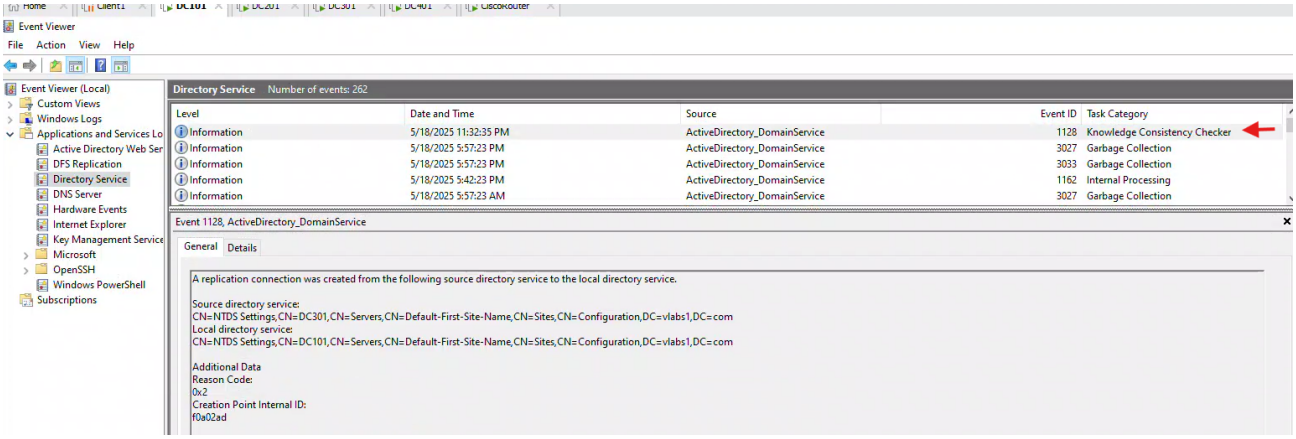
- Recreate it again using the KCC to regenerate it automatically.

  repadmin /kcc DC101





See in events



5.2 Using PowerShell

- Replicate manually to **DC401**.

  repadmin /syncall DC401.partner1.vlabs1.com /force

```
PS C:\Users\Administrator> repadmin /syncall DC401.partner1.vlabs1.com /force
CALLBACK MESSAGE: The following replication is in progress:
    From: be029329-3ebb-4c85-b57e-d1a1e5fe4e87._msdcs.vlabs1.com
    To  : 01004c70-51e1-4b52-9a48-aac4cc610935._msdcs.vlabs1.com
CALLBACK MESSAGE: The following replication completed successfully:
    From: be029329-3ebb-4c85-b57e-d1a1e5fe4e87._msdcs.vlabs1.com
    To  : 01004c70-51e1-4b52-9a48-aac4cc610935._msdcs.vlabs1.com
CALLBACK MESSAGE: The following replication is in progress:
    From: 250991af-de4f-4e49-b0df-f46c18bb4651._msdcs.vlabs1.com
    To  : 01004c70-51e1-4b52-9a48-aac4cc610935._msdcs.vlabs1.com
CALLBACK MESSAGE: The following replication completed successfully:
    From: 250991af-de4f-4e49-b0df-f46c18bb4651._msdcs.vlabs1.com
    To  : 01004c70-51e1-4b52-9a48-aac4cc610935._msdcs.vlabs1.com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.
```

- Delete this Connection object to **DC301.**

  1. List all connection objects:

     repadmin /showconn DC101

     This will output all current connection objects for DC101.
     Find the GUID of the one that points to DC301.
     CN={GUID},CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com

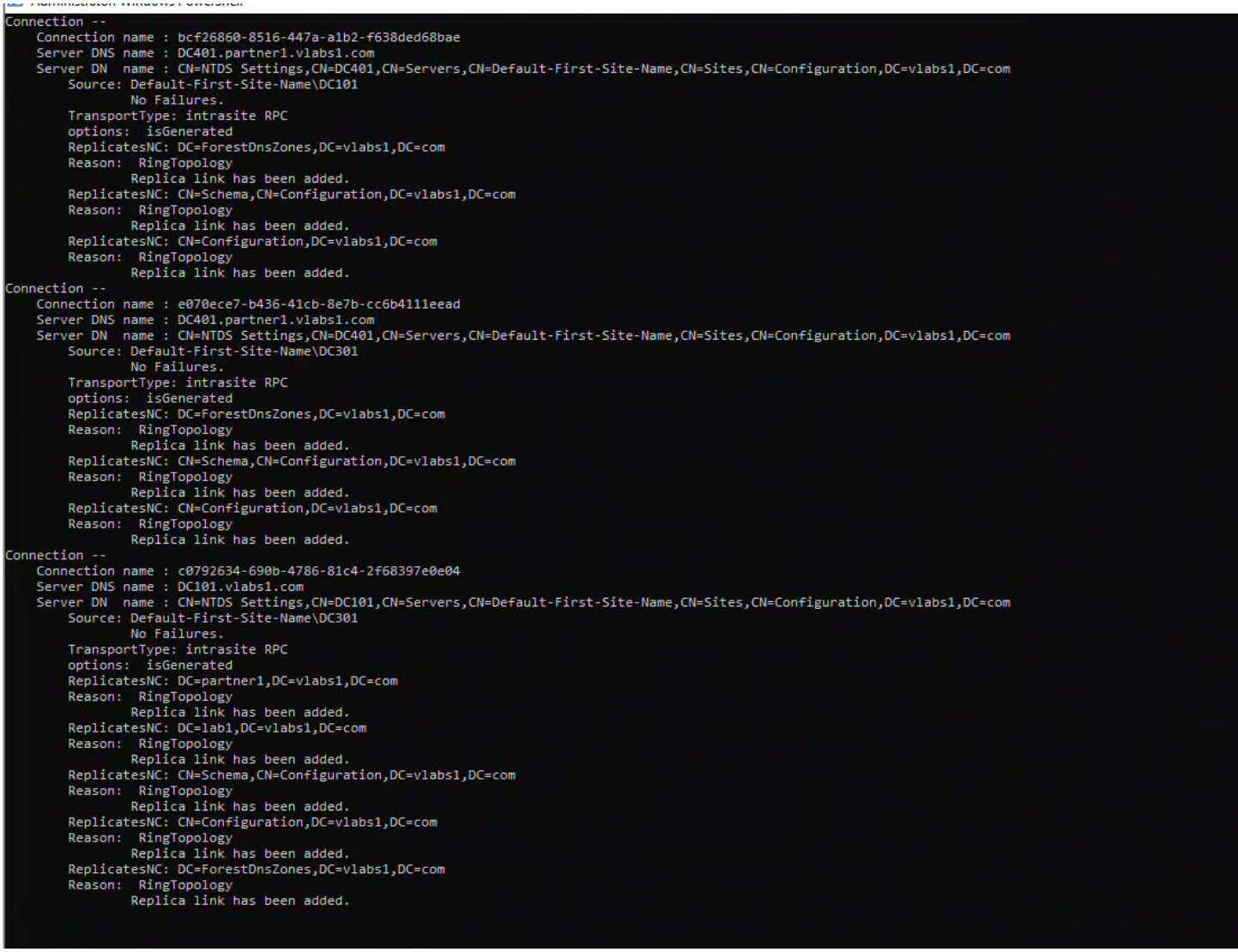
```
PS C:\Users\Administrator> repadmin /showconn DC101
Base DN: CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
==== KCC CONNECTION OBJECTS ============================================
Connection --
    Connection name : RODC Connection (SYSVOL)
    Server DNS name : DC201.vlabs1.com
    Server DN  name : CN=NTDS Settings,CN=DC201,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
        Source: Default-First-Site-Name\DC101
                No Failures.
        TransportType: intrasite RPC
        options:  isGenerated
Connection --
    Connection name : 37c6dac5-f7d1-4d78-acb6-1b34c686ec78
    Server DNS name : DC301.lab1.vlabs1.com
    Server DN  name : CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
        Source: Default-First-Site-Name\DC101
                No Failures.
        TransportType: intrasite RPC
        options:  isGenerated
        ReplicatesNC: DC=partner1,DC=vlabs1,DC=com
        Reason:  RingTopology
                Replica link has been added.
        ReplicatesNC: DC=ForestDnsZones,DC=vlabs1,DC=com
        Reason:  RingTopology
                Replica link has been added.
        ReplicatesNC: DC=vlabs1,DC=com
        Reason:  RingTopology
                Replica link has been added.
        ReplicatesNC: CN=Schema,CN=Configuration,DC=vlabs1,DC=com
        Reason:  RingTopology
                Replica link has been added.
        ReplicatesNC: CN=Configuration,DC=vlabs1,DC=com
        Reason:  RingTopology
                Replica link has been added.
Connection --
    Connection name : 79c536b2-e701-4917-878a-9398fbb60e03
    Server DNS name : DC101.vlabs1.com
    Server DN  name : CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
        Source: Default-First-Site-Name\DC401
                No Failures.
```

Remove-ADObject -Identity "CN=37c6dac5-f7d1-4d78-acb6-1b34c686ec78,CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com" -Confirm:$false

```
PS C:\Users\Administrator> Remove-ADObject -Identity "CN=37c6dac5-f7d1-4d78-acb6-1b34c686ec78,CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=
:$false
PS C:\Users\Administrator>
```

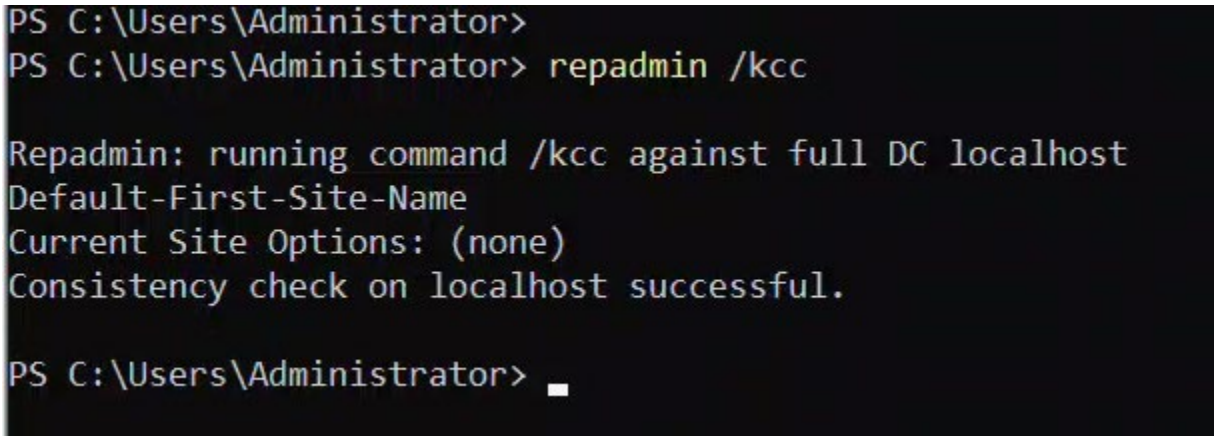
Verify it does not exists

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> repadmin /showconn DC101
Base DN: CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
==== KCC CONNECTION OBJECTS ============================================
Connection --
    Connection name : RODC Connection (SYSVOL)
    Server DNS name : DC201.vlabs1.com
    Server DN  name : CN=NTDS Settings,CN=DC201,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
        Source: Default-First-Site-Name\DC101
                No Failures.
        TransportType: intrasite RPC
        options:  isGenerated
Connection --
    Connection name : 79c536b2-e701-4917-878a-9398fbb60e03
    Server DNS name : DC101.vlabs1.com
    Server DN  name : CN=NTDS Settings,CN=DC101,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
        Source: Default-First-Site-Name\DC401
                No Failures.
        TransportType: intrasite RPC
        options:  isGenerated
        ReplicatesNC: DC=ForestDnsZones,DC=vlabs1,DC=com
        Reason:  RingTopology
                Replica link has been added.
        ReplicatesNC: DC=partner1,DC=vlabs1,DC=com
        Reason:  RingTopology
                Replica link has been added.
        ReplicatesNC: CN=Schema,CN=Configuration,DC=vlabs1,DC=com
        Reason:  RingTopology
                Replica link has been added.
        ReplicatesNC: CN=Configuration,DC=vlabs1,DC=com
        Reason:  RingTopology
                Replica link has been added.
Connection --
    Connection name : ac097acd-1c5e-4fbf-b0f5-46f6a40bcf9a
    Server DNS name : DC301.lab1.vlabs1.com
    Server DN  name : CN=NTDS Settings,CN=DC301,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
        Source: Default-First-Site-Name\DC401
                No Failures.
        TransportType: intrasite RPC
        options:  isGenerated
        ReplicatesNC: DC=ForestDnsZones,DC=vlabs1,DC=com
        Reason:  RingTopology
                Replica link has been added.
        ReplicatesNC: DC=partner1,DC=vlabs1,DC=com
        Reason:  RingTopology
                Replica link has been added.
        ReplicatesNC: CN=Schema,CN=Configuration,DC=vlabs1,DC=com
        Reason:  RingTopology
                Replica link has been added.
        ReplicatesNC: CN=Configuration,DC=vlabs1,DC=com
        Reason:  RingTopology
                Replica link has been added.
Connection --
    Connection name : bcf26860-8516-447a-a1b2-f638ded68bae
    Server DNS name : DC401.partner1.vlabs1.com
    Server DN  name : CN=NTDS Settings,CN=DC401,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
        Source: Default-First-Site-Name\DC101
                No Failures.
        TransportType: intrasite RPC
```



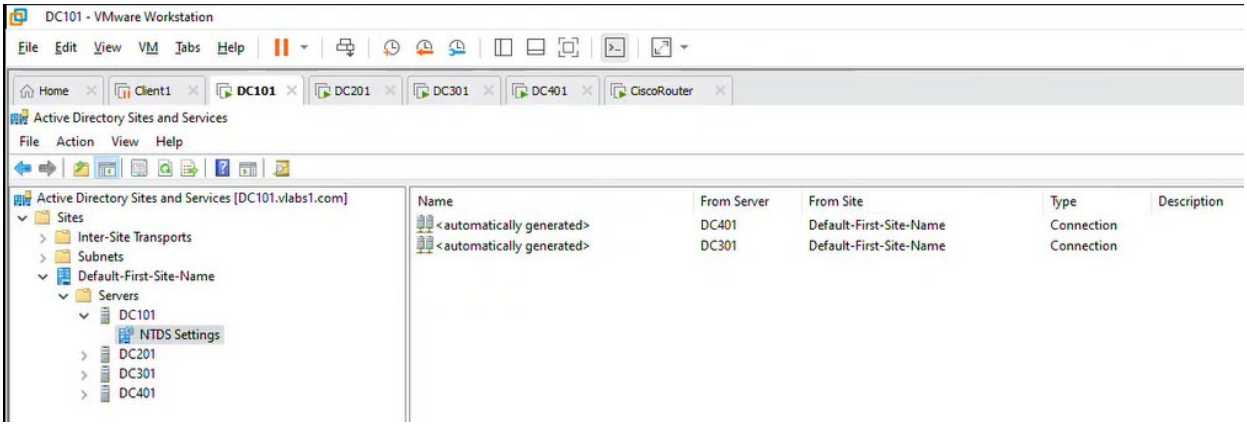
- Recreate it again using the **KCC to regenerate it automatically** and verify that it is created.

  repadmin /kcc

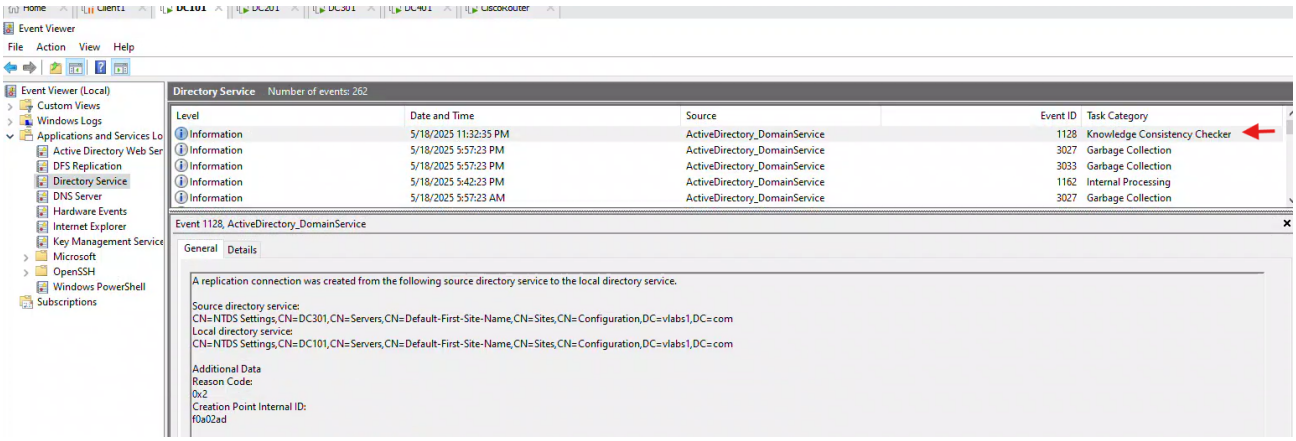


- Open **Event Viewer** to list the KCC events and verify if there are any errors.
  1. Open **Event Viewer**
  2. Navigate to:

     Applications and Services Logs → Directory Service



See in events



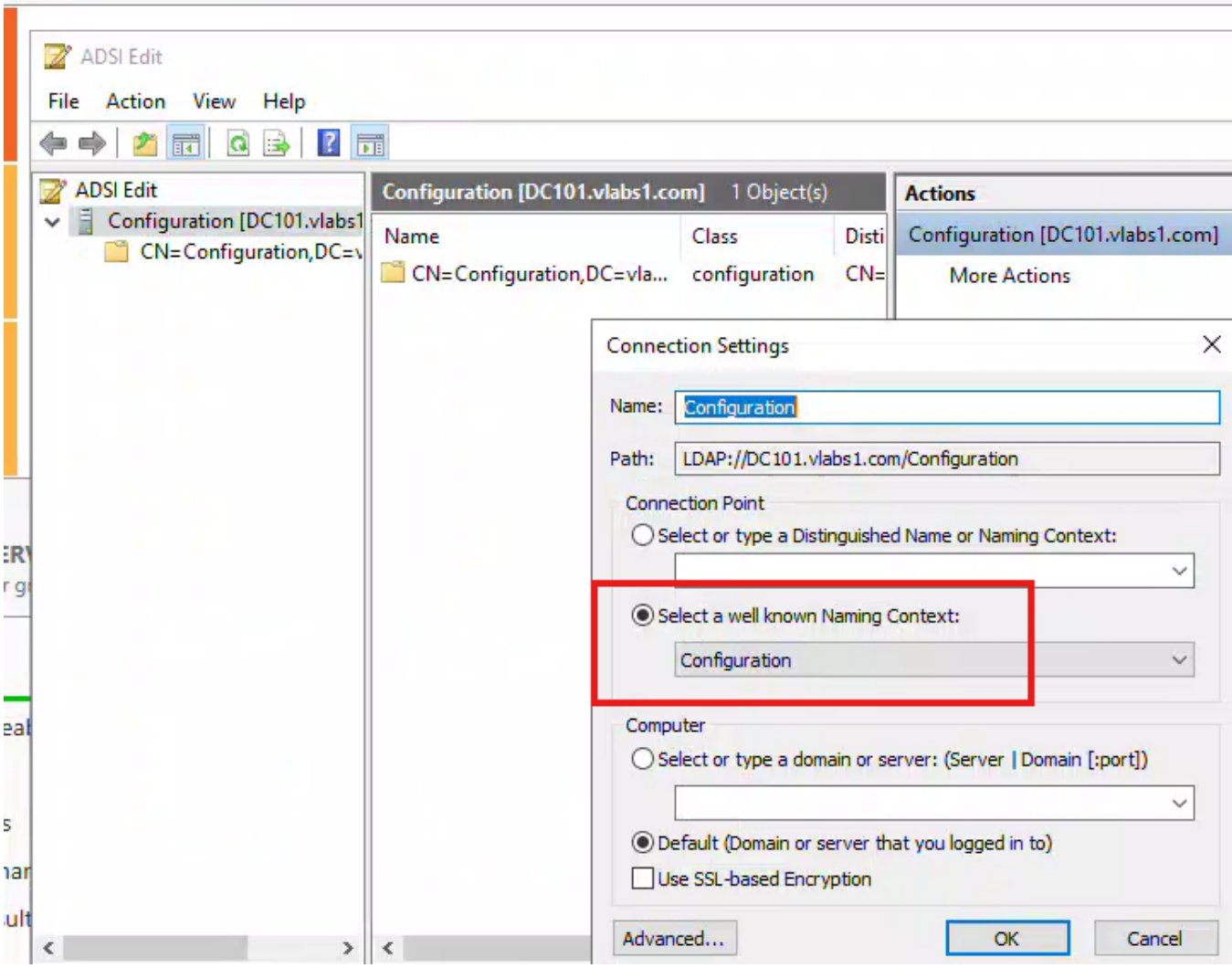
6 Task 4: Managing the Notification-Based Replication

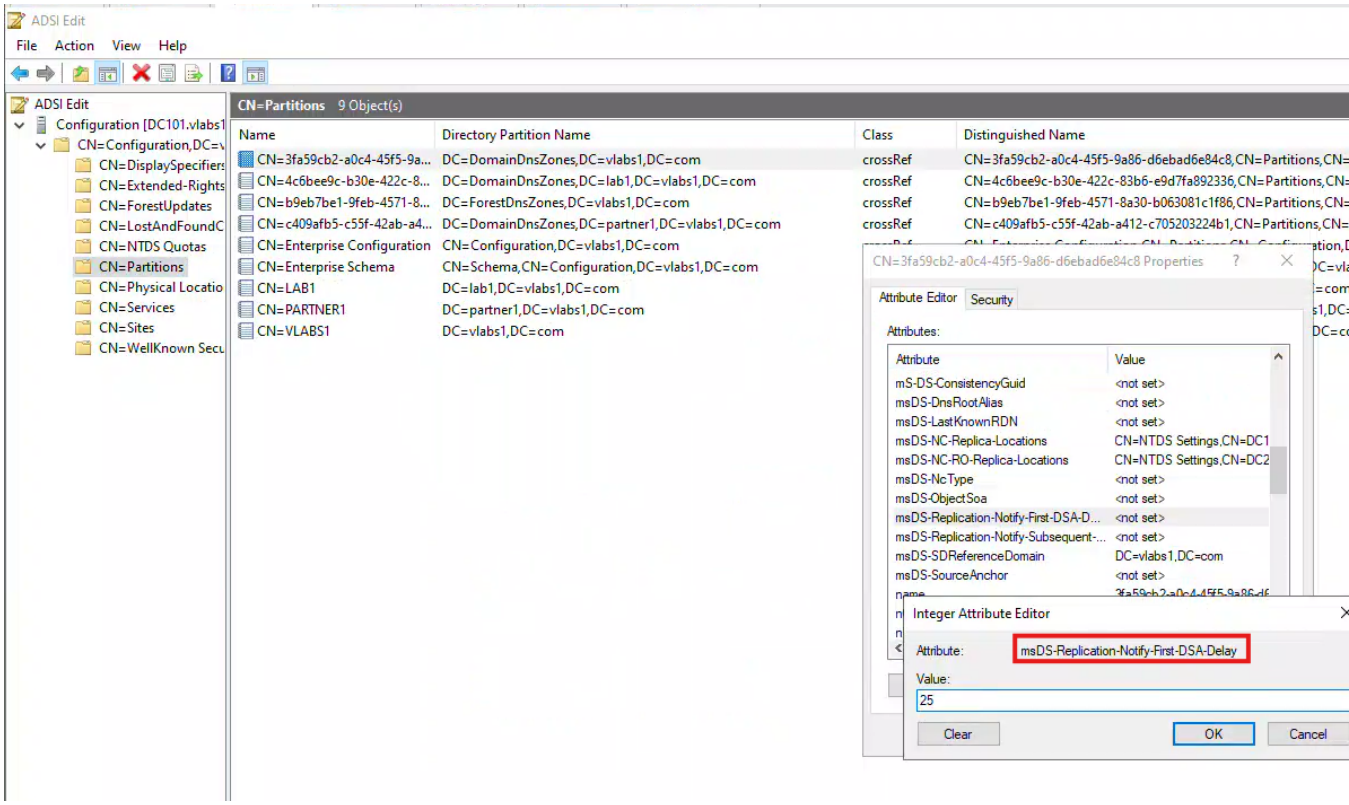
6.1 Using GUI from DC101

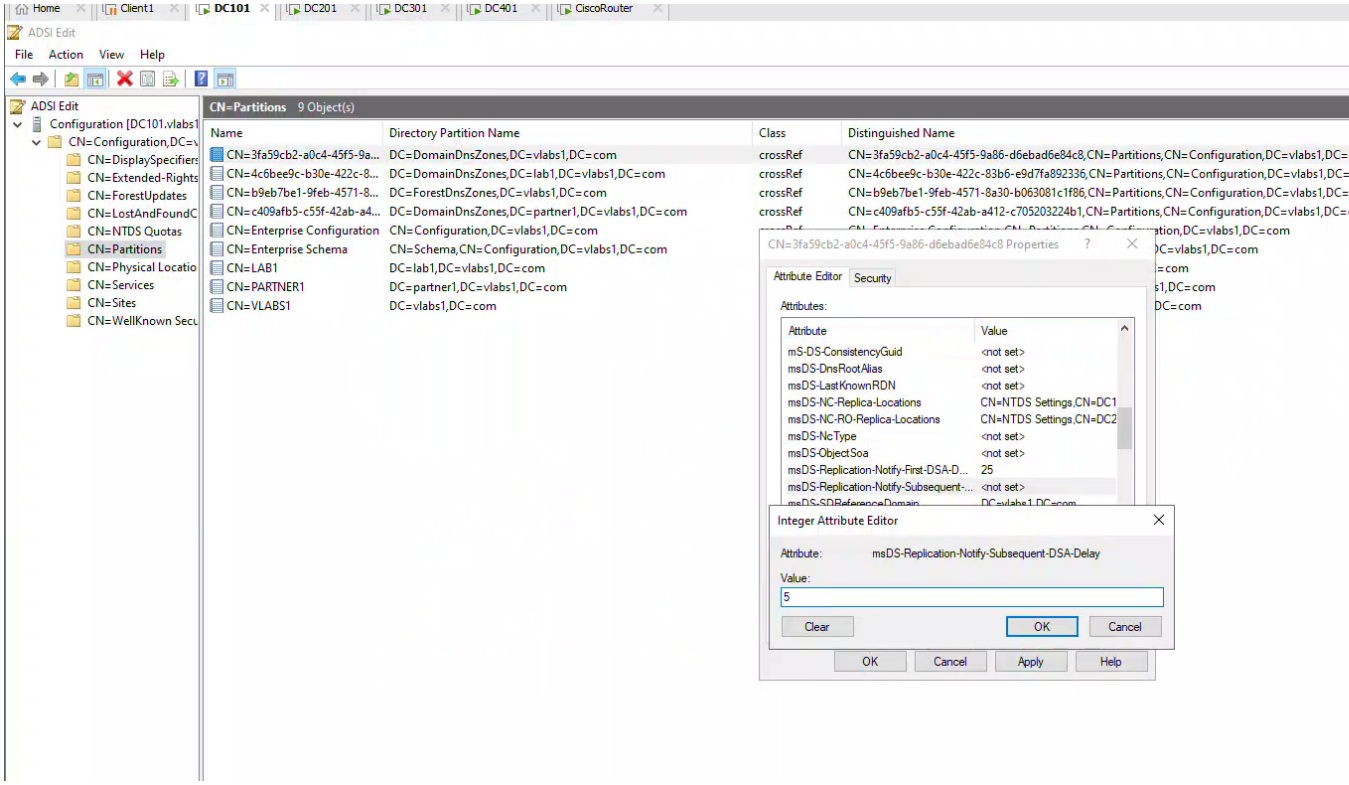
- Modify **First Replication Delay** to **25 sec** and **Subsequent Notifications** to **5 sec**.

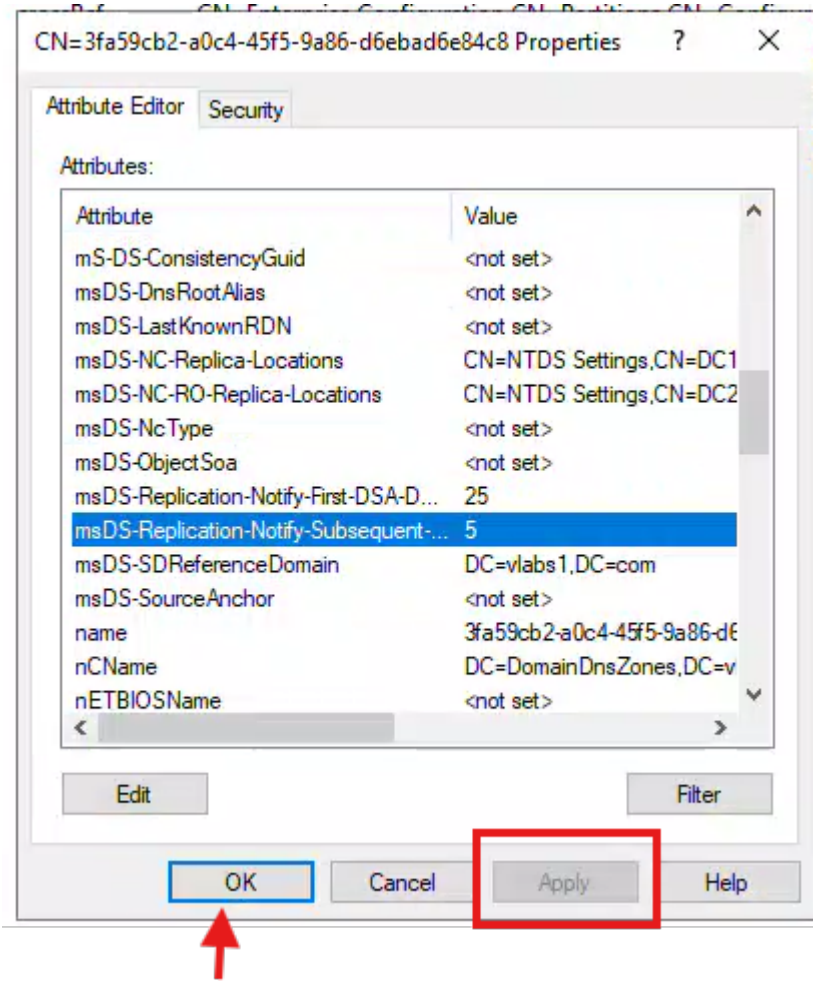
Use ADSI Edit to modify the Notification-Based replication → First replication delay and Subsequent replication delay :

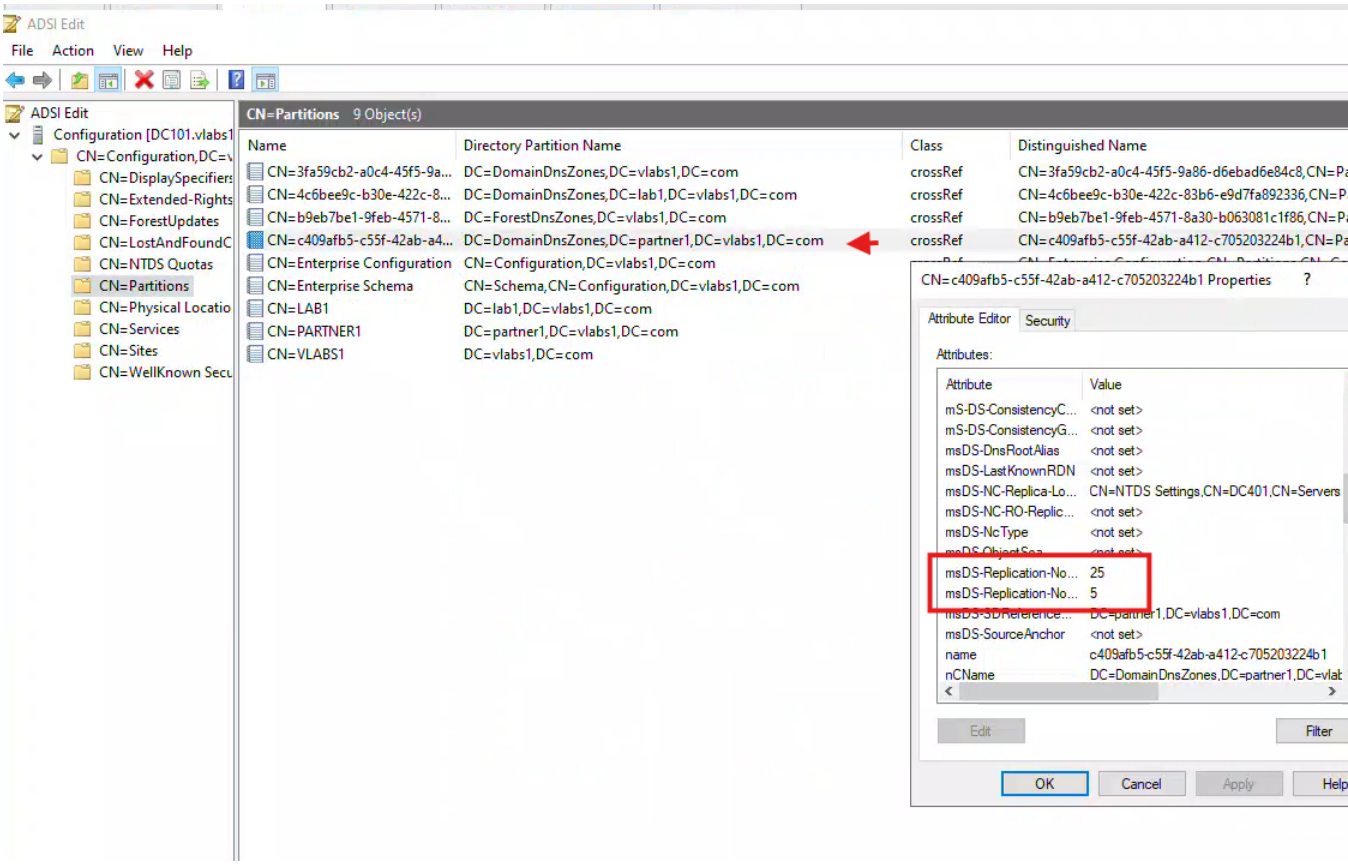
Set the msDS-Replication-Notify-First-DSA-Delay and msDS-Replication-Notify-Subsequent-DSA-Delay attributes to the number of seconds

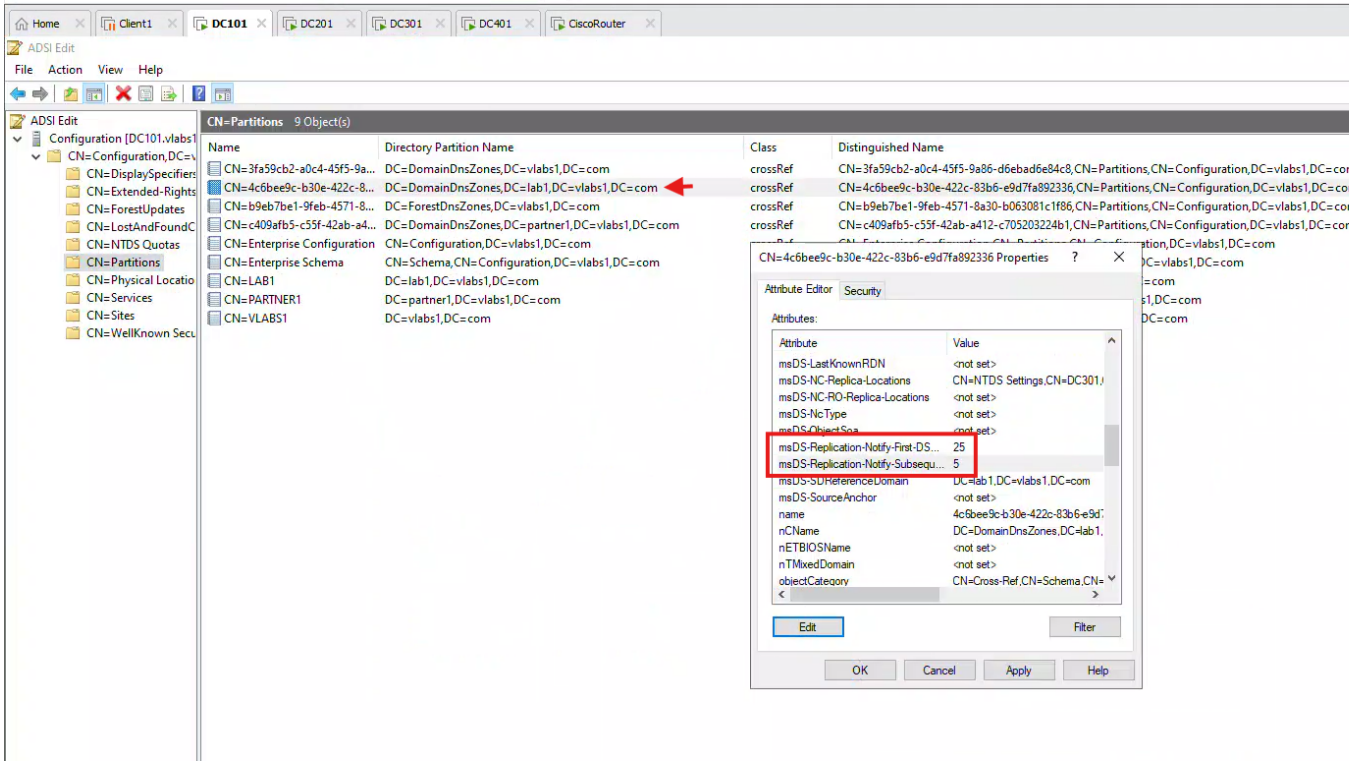


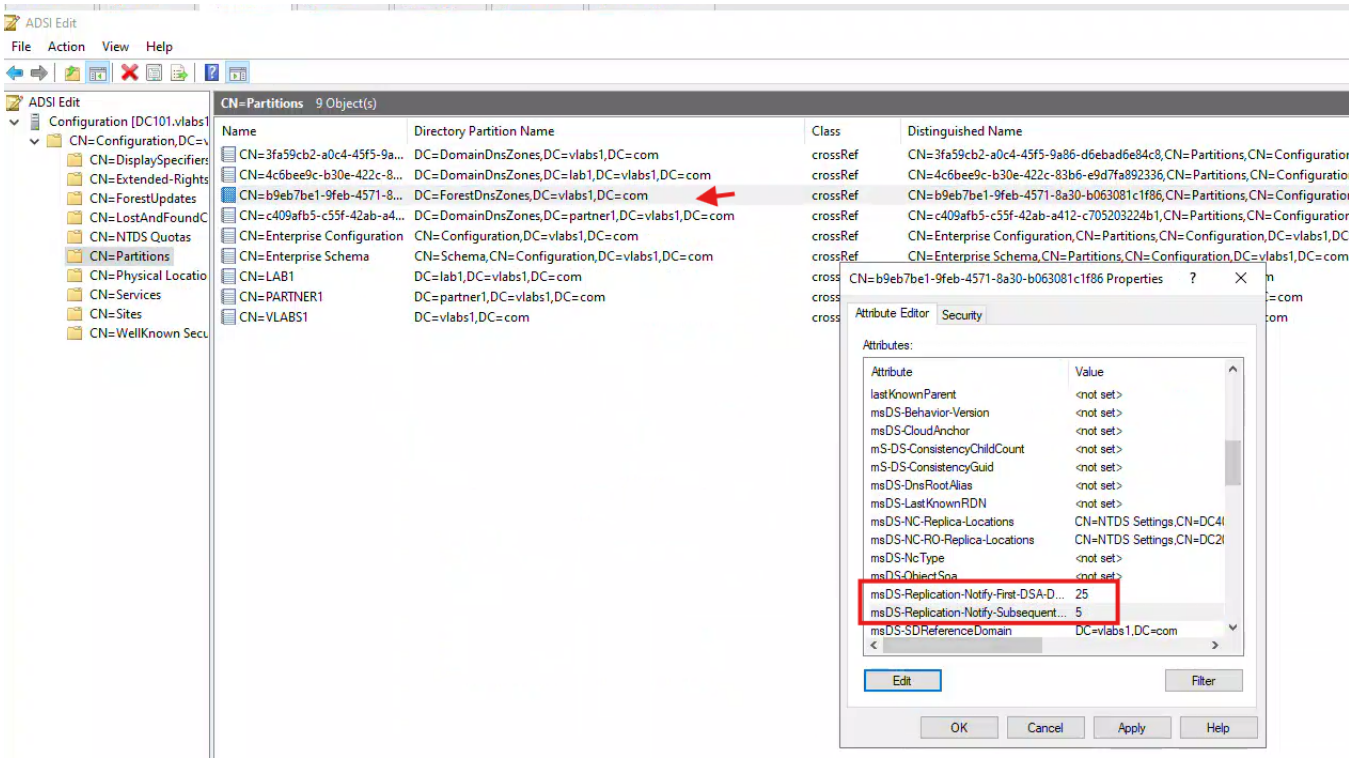

ADSI Edit
File Action View Help
ADSI Edit
Configuration [DC101.vlabs1
CN=Configuration,DC=v
CN=DisplaySpecifiers
CN=Extended-Rights
CN=ForestUpdates
CN=LostAndFoundC
CN=NTDS Quotas
CN=Partitions
CN=Physical Locatio
CN=Services
CN=Sites
CN=WellKnown Secu
CN=Partitions 9 Object(s)
Name
Directory Partition Name
Class
Distinguished Name
CN=3fa59cb2-a0c4-45f5-9a... DC=DomainDnsZones,DC=vlabs1,DC=com crossRef CN=3fa59cb2-a0c4-45f5-9a86-d6ebad6e84c8,CN=Partitions,CN=
CN=4c6bee9c-b30e-422c-8... DC=DomainDnsZones,DC=lab1,DC=vlabs1,DC=com crossRef CN=4c6bee9c-b30e-422c-83b6-e9d7fa892336,CN=Partitions,CN=
CN=b9eb7be1-9feb-4571-8... DC=ForestDnsZones,DC=vlabs1,DC=com crossRef CN=b9eb7be1-9feb-4571-8a30-b063081c1f86,CN=Partitions,CN=
CN=c409afb5-c55f-42ab-a4... DC=DomainDnsZones,DC=partner1,DC=vlabs1,DC=com crossRef CN=c409afb5-c55f-42ab-a412-c705203224b1,CN=Partitions,CN=
CN=Enterprise Configuration CN=Configuration,DC=vlabs1,DC=com
CN=Enterprise Schema CN=Schema,CN=Configuration,DC=vlabs1,DC=com
CN=LAB1 DC=lab1,DC=vlabs1,DC=com
CN=PARTNER1 DC=partner1,DC=vlabs1,DC=com
CN=VLABS1 DC=vlabs1,DC=com
CN=3fa59cb2-a0c4-45f5-9a86-d6ebad6e84c8 Properties
Attribute Editor
Security
Attributes:
Attribute
Value
mS-DS-ConsistencyGuid <not set>
msDS-DnsRootAlias <not set>
msDS-LastKnownRDN <not set>
msDS-NC-Replica-Locations CN=NTDS Settings,CN=DC1
msDS-NC-RO-Replica-Locations CN=NTDS Settings,CN=DC2
msDS-NcType <not set>
msDS-ObjectSoa <not set>
msDS-Replication-Notify-First-DSA-D... <not set>
msDS-Replication-Notify-Subsequent-... <not set>
msDS-SDReferenceDomain DC=vlabs1,DC=com
msDS-SourceAnchor <not set>
Integer Attribute Editor
Attribute:
msDS-Replication-Notify-First-DSA-Delay
Value:
25
Clear
OK
Cancel


Home
Client1
DC101
DC201
DC301
DC401
CiscoRouter
ADSI Edit
File Action View Help
ADSI Edit
Configuration [DC101.vlabs1
CN=Configuration,DC=v
CN=DisplaySpecifiers
CN=Extended-Rights
CN=ForestUpdates
CN=LostAndFoundC
CN=NTDS Quotas
CN=Partitions
CN=Physical Locatio
CN=Services
CN=Sites
CN=WellKnown Secu
CN=Partitions 9 Object(s)
Name
Directory Partition Name
Class
Distinguished Name
CN=3fa59cb2-a0c4-45f5-9a... DC=DomainDnsZones,DC=vlabs1,DC=com crossRef CN=3fa59cb2-a0c4-45f5-9a86-d6ebad6e84c8,CN=Partitions,CN=Configuration,DC=vlabs1,DC=
CN=4c6bee9c-b30e-422c-8... DC=DomainDnsZones,DC=lab1,DC=vlabs1,DC=com crossRef CN=4c6bee9c-b30e-422c-83b6-e9d7fa892336,CN=Partitions,CN=Configuration,DC=vlabs1,DC=
CN=b9eb7be1-9feb-4571-8... DC=ForestDnsZones,DC=vlabs1,DC=com crossRef CN=b9eb7be1-9feb-4571-8a30-b063081c1f86,CN=Partitions,CN=Configuration,DC=vlabs1,DC=
CN=c409afb5-c55f-42ab-a4... DC=DomainDnsZones,DC=partner1,DC=vlabs1,DC=com crossRef CN=c409afb5-c55f-42ab-a412-c705203224b1,CN=Partitions,CN=Configuration,DC=vlabs1,DC=
CN=Enterprise Configuration CN=Configuration,DC=vlabs1,DC=com
CN=Enterprise Schema CN=Schema,CN=Configuration,DC=vlabs1,DC=com
CN=LAB1 DC=lab1,DC=vlabs1,DC=com
CN=PARTNER1 DC=partner1,DC=vlabs1,DC=com
CN=VLABS1 DC=vlabs1,DC=com
CN=3fa59cb2-a0c4-45f5-9a86-d6ebad6e84c8 Properties
Attribute Editor
Security
Attributes:
Attribute
Value
mS-DS-ConsistencyGuid <not set>
msDS-DnsRootAlias <not set>
msDS-LastKnownRDN <not set>
msDS-NC-Replica-Locations CN=NTDS Settings,CN=DC1
msDS-NC-RO-Replica-Locations CN=NTDS Settings,CN=DC2
msDS-NcType <not set>
msDS-ObjectSoa <not set>
msDS-Replication-Notify-First-DSA-D... 25
msDS-Replication-Notify-Subsequent-... <not set>
Integer Attribute Editor
Attribute:
msDS-Replication-Notify-Subsequent-DSA-Delay
Value:
5
Clear
OK
Cancel
OK
Cancel
Apply
Help


CN=3fa59cb2-a0c4-45f5-9a86-d6ebad6e84c8 Properties
Attribute Editor
Security
Attributes:
Attribute
Value
mS-DS-ConsistencyGuid
<not set>
msDS-DnsRootAlias
<not set>
msDS-LastKnownRDN
<not set>
msDS-NC-Replica-Locations
CN=NTDS Settings,CN=DC1
msDS-NC-RO-Replica-Locations
CN=NTDS Settings,CN=DC2
msDS-NcType
<not set>
msDS-ObjectSoa
<not set>
msDS-Replication-Notify-First-DSA-D...
25
msDS-Replication-Notify-Subsequent-...
5
msDS-SDReferenceDomain
DC=vlabs1,DC=com
msDS-SourceAnchor
<not set>
name
3fa59cb2-a0c4-45f5-9a86-d6
nCName
DC=DomainDnsZones,DC=v
nETBIOSName
<not set>
Edit
Filter
OK
Cancel
Apply
Help


ADSI Edit
File
Action
View
Help
ADSI Edit
Configuration [DC101.vlabs1
CN=Configuration,DC=v
CN=DisplaySpecifiers
CN=Extended-Rights
CN=ForestUpdates
CN=LostAndFoundC
CN=NTDS Quotas
CN=Partitions
CN=Physical Locatio
CN=Services
CN=Sites
CN=WellKnown Secu
CN=Partitions 9 Object(s)
Name
Directory Partition Name
Class
Distinguished Name
CN=3fa59cb2-a0c4-45f5-9a...
DC=DomainDnsZones,DC=vlabs1,DC=com
crossRef
CN=3fa59cb2-a0c4-45f5-9a86-d6ebad6e84c8,CN=Pa
CN=4c6bee9c-b30e-422c-8...
DC=DomainDnsZones,DC=lab1,DC=vlabs1,DC=com
crossRef
CN=4c6bee9c-b30e-422c-83b6-e9d7fa892336,CN=P
CN=b9eb7be1-9feb-4571-8...
DC=ForestDnsZones,DC=vlabs1,DC=com
crossRef
CN=b9eb7be1-9feb-4571-8a30-b063081c1f86,CN=Pa
CN=c409afb5-c55f-42ab-a4...
DC=DomainDnsZones,DC=partner1,DC=vlabs1,DC=com
crossRef
CN=c409afb5-c55f-42ab-a412-c705203224b1,CN=Pa
CN=Enterprise Configuration
CN=Configuration,DC=vlabs1,DC=com
CN=Enterprise Schema
CN=Schema,CN=Configuration,DC=vlabs1,DC=com
CN=LAB1
DC=lab1,DC=vlabs1,DC=com
CN=PARTNER1
DC=partner1,DC=vlabs1,DC=com
CN=VLABS1
DC=vlabs1,DC=com
CN=c409afb5-c55f-42ab-a412-c705203224b1 Properties
Attribute Editor
Security
Attributes:
Attribute
Value
mS-DS-ConsistencyC...
<not set>
mS-DS-ConsistencyG...
<not set>
msDS-DnsRootAlias
<not set>
msDS-LastKnownRDN
<not set>
msDS-NC-Replica-Lo...
CN=NTDS Settings,CN=DC401,CN=Servers
msDS-NC-RO-Replic...
<not set>
msDS-NcType
<not set>
msDS-Replication-No...
25
msDS-Replication-No...
5
msDS-SourceAnchor
<not set>
name
c409afb5-c55f-42ab-a412-c705203224b1
nCName
DC=DomainDnsZones,DC=partner1,DC=vlab
Edit
Filter
OK
Cancel
Apply
Help

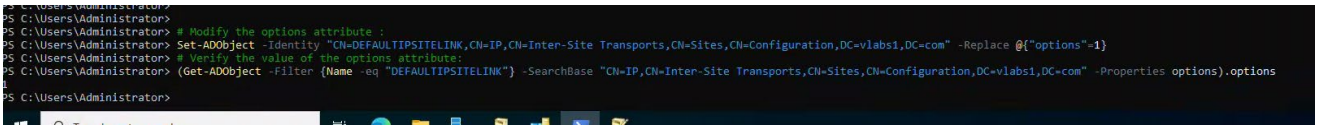

Home
Client1
DC101
DC201
DC301
DC401
CiscoRouter
ADSI Edit
File Action View Help
ADSI Edit
Configuration [DC101.vlabs1
CN=Configuration,DC=v
CN=DisplaySpecifiers
CN=Extended-Rights
CN=ForestUpdates
CN=LostAndFoundC
CN=NTDS Quotas
CN=Partitions
CN=Physical Locatio
CN=Services
CN=Sites
CN=WellKnown Secu
CN=Partitions 9 Object(s)
Name
Directory Partition Name
Class
Distinguished Name
CN=3fa59cb2-a0c4-45f5-9a...
DC=DomainDnsZones,DC=vlabs1,DC=com
crossRef
CN=3fa59cb2-a0c4-45f5-9a86-d6ebad6e84c8,CN=Partitions,CN=Configuration,DC=vlabs1,DC=com
CN=4c6bee9c-b30e-422c-8...
DC=DomainDnsZones,DC=lab1,DC=vlabs1,DC=com
crossRef
CN=4c6bee9c-b30e-422c-83b6-e9d7fa892336,CN=Partitions,CN=Configuration,DC=vlabs1,DC=com
CN=b9eb7be1-9feb-4571-8...
DC=ForestDnsZones,DC=vlabs1,DC=com
crossRef
CN=b9eb7be1-9feb-4571-8a30-b063081c1f86,CN=Partitions,CN=Configuration,DC=vlabs1,DC=com
CN=c409afb5-c55f-42ab-a4...
DC=DomainDnsZones,DC=partner1,DC=vlabs1,DC=com
crossRef
CN=c409afb5-c55f-42ab-a412-c705203224b1,CN=Partitions,CN=Configuration,DC=vlabs1,DC=com
CN=Enterprise Configuration
CN=Configuration,DC=vlabs1,DC=com
CN=Enterprise Schema
CN=Schema,CN=Configuration,DC=vlabs1,DC=com
CN=LAB1
DC=lab1,DC=vlabs1,DC=com
CN=PARTNER1
DC=partner1,DC=vlabs1,DC=com
CN=VLABS1
DC=vlabs1,DC=com
CN=4c6bee9c-b30e-422c-83b6-e9d7fa892336 Properties
Attribute Editor
Security
Attributes:
Attribute
Value
msDS-LastKnownRDN
<not set>
msDS-NC-Replica-Locations
CN=NTDS Settings,CN=DC301,
msDS-NC-RO-Replica-Locations
<not set>
msDS-NcType
<not set>
msDS-Replication-Notify-First-DS...
25
msDS-Replication-Notify-Subsequ...
5
msDS-SDReferenceDomain
DC=lab1,DC=vlabs1,DC=com
msDS-SourceAnchor
<not set>
name
4c6bee9c-b30e-422c-83b6-e9d7
nCName
DC=DomainDnsZones,DC=lab1,
nETBIOSName
<not set>
nTMixedDomain
<not set>
objectCategory
CN=Cross-Ref,CN=Schema,CN=
Edit
Filter
OK
Cancel
Apply
Help


ADSI Edit
File Action View Help
ADSI Edit
Configuration [DC101.vlabs1
CN=Configuration,DC=v
CN=DisplaySpecifiers
CN=Extended-Rights
CN=ForestUpdates
CN=LostAndFoundC
CN=NTDS Quotas
CN=Partitions
CN=Physical Locatio
CN=Services
CN=Sites
CN=WellKnown Secu
CN=Partitions 9 Object(s)
Name
Directory Partition Name
Class
Distinguished Name
CN=3fa59cb2-a0c4-45f5-9a...
DC=DomainDnsZones,DC=vlabs1,DC=com
crossRef
CN=3fa59cb2-a0c4-45f5-9a86-d6ebad6e84c8,CN=Partitions,CN=Configuration
CN=4c6bee9c-b30e-422c-8...
DC=DomainDnsZones,DC=lab1,DC=vlabs1,DC=com
crossRef
CN=4c6bee9c-b30e-422c-83b6-e9d7fa892336,CN=Partitions,CN=Configuration
CN=b9eb7be1-9feb-4571-8...
DC=ForestDnsZones,DC=vlabs1,DC=com
crossRef
CN=b9eb7be1-9feb-4571-8a30-b063081c1f86,CN=Partitions,CN=Configuration
CN=c409afb5-c55f-42ab-a4...
DC=DomainDnsZones,DC=partner1,DC=vlabs1,DC=com
crossRef
CN=c409afb5-c55f-42ab-a412-c705203224b1,CN=Partitions,CN=Configuration
CN=Enterprise Configuration
CN=Configuration,DC=vlabs1,DC=com
crossRef
CN=Enterprise Configuration,CN=Partitions,CN=Configuration,DC=vlabs1,DC
CN=Enterprise Schema
CN=Schema,CN=Configuration,DC=vlabs1,DC=com
crossRef
CN=Enterprise Schema,CN=Partitions,CN=Configuration,DC=vlabs1,DC=com
CN=LAB1
DC=lab1,DC=vlabs1,DC=com
CN=PARTNER1
DC=partner1,DC=vlabs1,DC=com
CN=VLABS1
DC=vlabs1,DC=com
CN=b9eb7be1-9feb-4571-8a30-b063081c1f86 Properties
Attribute Editor
Security
Attributes:
Attribute
Value
lastKnownParent
<not set>
msDS-Behavior-Version
<not set>
msDS-CloudAnchor
<not set>
mS-DS-ConsistencyChildCount
<not set>
mS-DS-ConsistencyGuid
<not set>
msDS-DnsRootAlias
<not set>
msDS-LastKnownRDN
<not set>
msDS-NC-Replica-Locations
CN=NTDS Settings,CN=DC4
msDS-NC-RO-Replica-Locations
CN=NTDS Settings,CN=DC2
msDS-NcType
<not set>
msDS-Replication-Notify-First-DSA-D...
25
msDS-Replication-Notify-Subsequent...
5
msDS-SDReferenceDomain
DC=vlabs1,DC=com
Edit
Filter
OK
Cancel
Apply
Help

6.2 Using PowerShell:

- Verify if **Notification-Based Replication** is enabled.

```
# Modify the options attribute :
Set-ADObject -Identity "CN=DEFAULTIPSITELINK,CN=IP,CN=Inter-Site
Transports,CN=Sites,CN=Configuration,DC=vlabs1,DC=com" -Replace @{"options"=1}

# Verify the value of the options attribute:
(Get-ADObject -Filter {Name -eq "DEFAULTIPSITELINK"} -SearchBase "CN=IP,CN=Inter-Site
Transports,CN=Sites,CN=Configuration,DC=vlabs1,DC=com" -Properties options).options
```



By default is 1

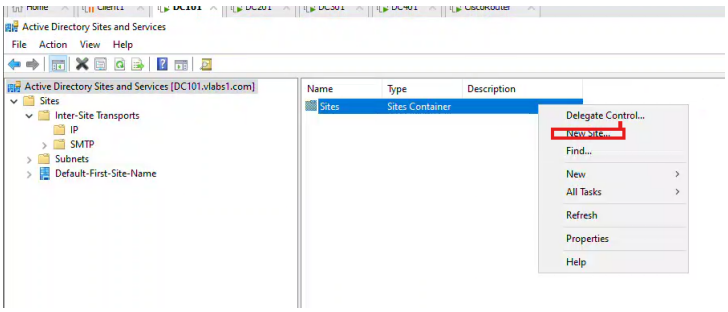
Decimal Value	Binary Value	Explanation
1	1	USE_NOTIFY
2	10	TWOWAY_SYNC
4	100	DISABLE_COMPRESSION

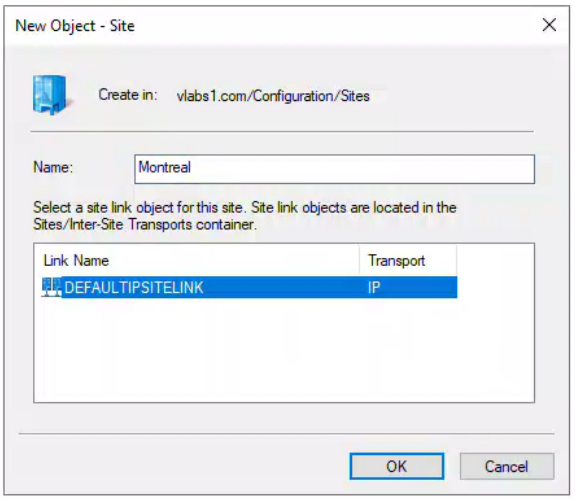
7 Task 5: Creating Sites

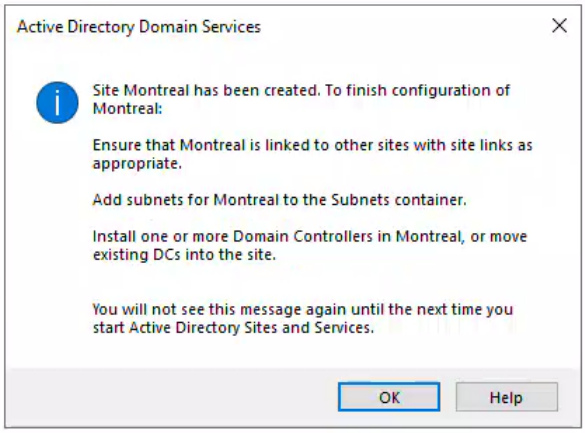
7.1 Create the sites **Montreal** and **New-York.**

Using GUI (on a Domain Controller with Active Directory Sites and Services)

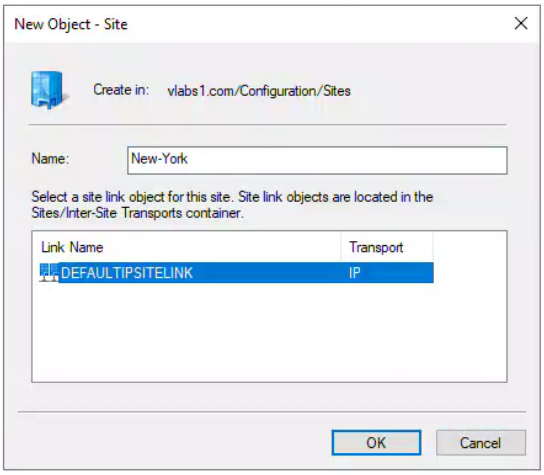
1. **Create the Montreal Site:**
   - Open **Active Directory Sites and Services** (dssite.msc).
   - In the console tree, expand **Sites**.
   - Right-click on the **Sites** container and select **New Site...**.
   - In the **New Object - Site** dialog box:
     - In the **Name** field, type **Montreal**.
     - Select the default **DEFAULTIPSITELINK** in the **Link name** list.
     - Click **OK**.

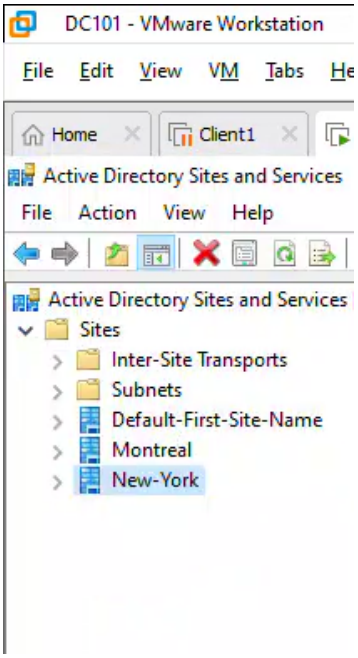






2. **Create the New-York Site:**
    - Repeat the steps above, but in the **Name** field, type **New-York**.

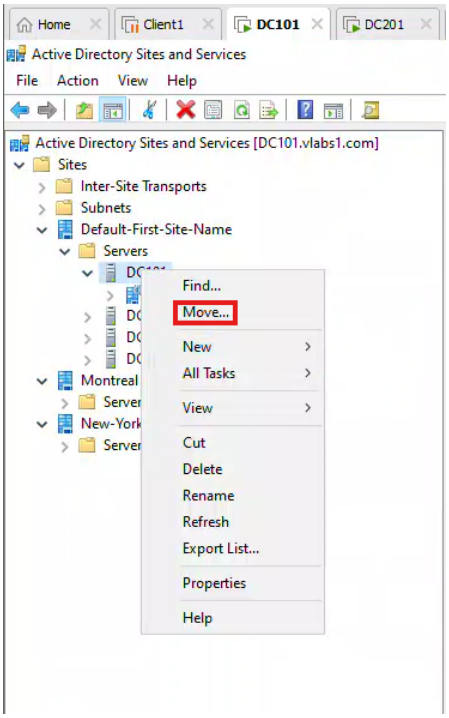


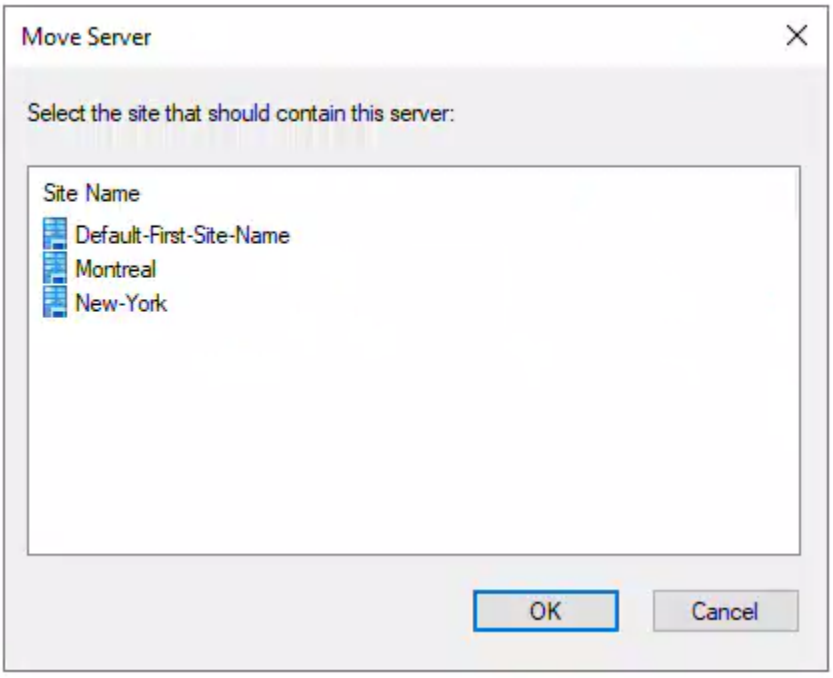


7.2 Move DC101 and DC301 under the Montreal site.

7.2.1 Move DC101 to the Montreal Site:

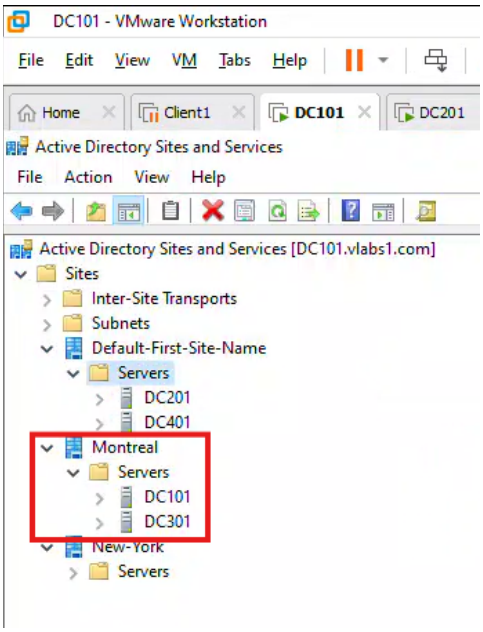
1. In the console tree, expand Sites and then expand Default-First-Site-Name (or the site where DC101 currently resides).
2. Expand Servers.
3. Locate and click on the DC101 server object.
4. Right-click on DC101, select Move....
5. In the Move Server dialog box, select Montreal and click OK.



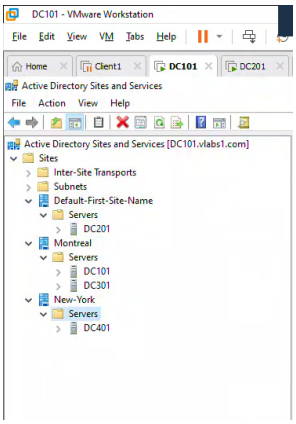


7.2.2 Move DC301 to the Montreal Site:

- Follow the same steps as moving DC101, but select the DC301 server object.



7.2.3 Move **DC401** under the **New-York** site.



7.3 Using PowerShell

- Create the site **Toronto** and verify that it has been created.

```
New-ADReplicationSite -Name "Toronto"

Get-ADReplicationSite -Filter "Name -eq 'Toronto'"
```

- Modify it by adding a description.

```
Set-ADReplicationSite -Identity "Toronto" -Description "Main site for the Toronto office"
```

```
PS C:\Users\Administrator> # Create the site Toronto and verify that it has been created.
PS C:\Users\Administrator> New-ADReplicationSite -Name "Toronto"
PS C:\Users\Administrator> Get-ADReplicationSite -Filter "Name -eq 'Toronto'"


Description                     :
DistinguishedName               : CN=Toronto,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
InterSiteTopologyGenerator      :
ManagedBy                       :
Name                            : Toronto
ObjectClass                     : site
ObjectGUID                      : 25ba797b-4d5d-4466-bc55-69f56c6492a7
ReplicationSchedule             :
UniversalGroupCachingRefreshSite :



PS C:\Users\Administrator> # Modify it by adding a description.
PS C:\Users\Administrator> Set-ADReplicationSite -Identity "Toronto" -Description "Main site for the Toronto office"
PS C:\Users\Administrator> Get-ADReplicationSite -Filter "Name -eq 'Toronto'"


Description                     : Main site for the Toronto office
DistinguishedName               : CN=Toronto,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
InterSiteTopologyGenerator      :
ManagedBy                       :
Name                            : Toronto
ObjectClass                     : site
ObjectGUID                      : 25ba797b-4d5d-4466-bc55-69f56c6492a7
ReplicationSchedule             :
UniversalGroupCachingRefreshSite :
```

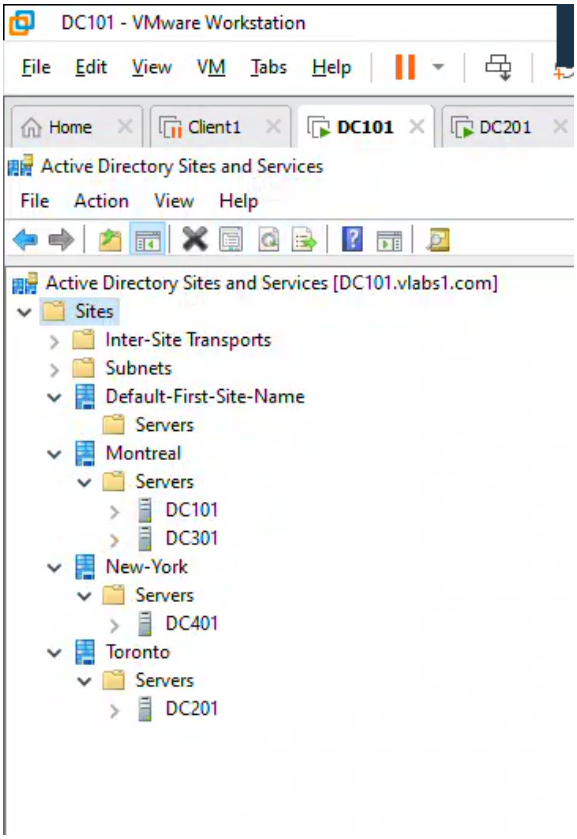
- Move **DC201** to **Toronto** site

  ```
  Move-ADDirectoryServer -Identity "DC201" -Site "Toronto"
  ```

- Verify that it was moved.

  Get-ADDomainController -Identity "DC201" | Select-Object Name, Site

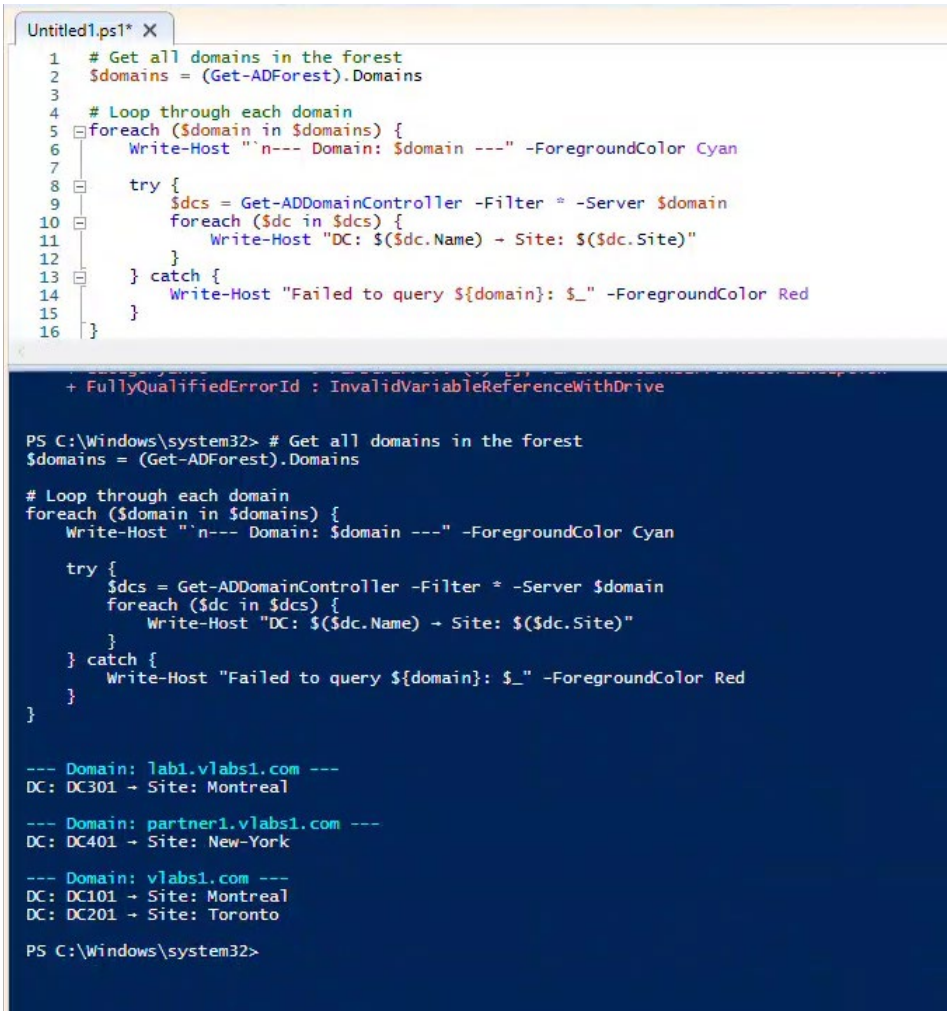
```
PS C:\Users\Administrator> # Move DC201 to Toronto site
PS C:\Users\Administrator> Move-ADDirectoryServer -Identity "DC201" -Site "Toronto"
PS C:\Users\Administrator> # Verify the move
PS C:\Users\Administrator> Get-ADDomainController -Identity "DC201" | Select-Object Name, Site

Name  Site
----  ----
DC201 Toronto


PS C:\Users\Administrator>
```



Verify Sites

Run powershell script to verify sites

```
# Get all domains in the forest
$domains = (Get-ADForest).Domains

# Loop through each domain
foreach ($domain in $domains) {
    Write-Host "`n--- Domain: $domain ---" -ForegroundColor Cyan

    try {
        $dcs = Get-ADDomainController -Filter * -Server $domain
        foreach ($dc in $dcs) {
            Write-Host "DC: $($dc.Name) → Site: $($dc.Site)"
        }
    } catch {
        Write-Host "Failed to query ${domain}: $_" -ForegroundColor Red
    }
}
```



Domain Controller	FQDN	Domain	Site	IP Address
DC101	dc101.vlabs1.com	vlabs1.com	Montreal	192.168.1.1
DC201	dc201.vlabs1.com	vlabs1.com	Toronto	192.168.45.1
DC301	dc301.lab1.vlabs1.com	lab1.vlabs1.com	Montreal	192.168.1.3
DC401	dc401.partner1.vlabs1.com	partner1.vlabs1.com	New-York	192.168.35.1

8 Task 6: Creating Subnets

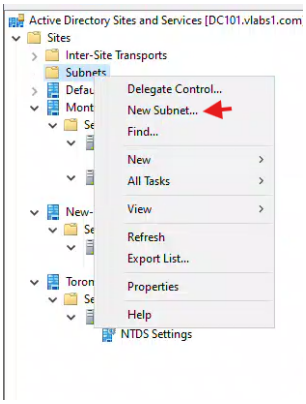
8.1 Using GUI

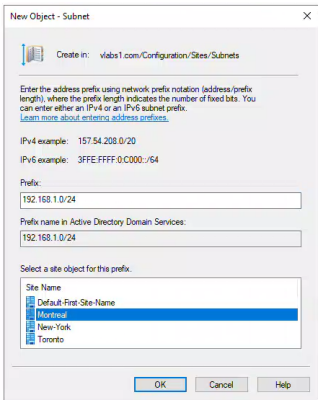
- Create subnet **192.168.1.0/24** and associate it with the **Montreal** site.

1. Open Active Directory Sites and Services
2. Expand Subnets > Right-click Subnets > Select New Subnet
   Enter:

Network Prefix: 192.168.1.0/24
Site: Montreal

3. Click OK

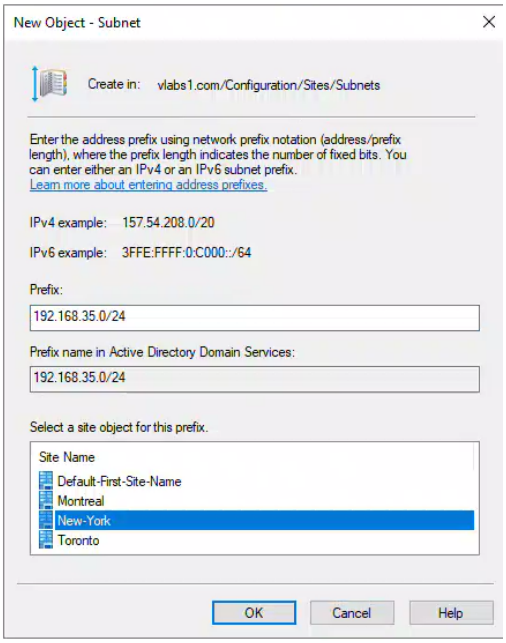




- Create subnet **192.168.35.0/24** and associate it with the **New-York** site.

Repeat steps above with:

- **Network Prefix**: `192.168.35.0/24`
- **Site**: `New-York`



8.2 Using PowerShell

- Create subnet **192.168.45.0/24** and associate it with the **Toronto** site.

  New-ADReplicationSubnet -Name "192.168.45.0/24" -Site "Toronto"

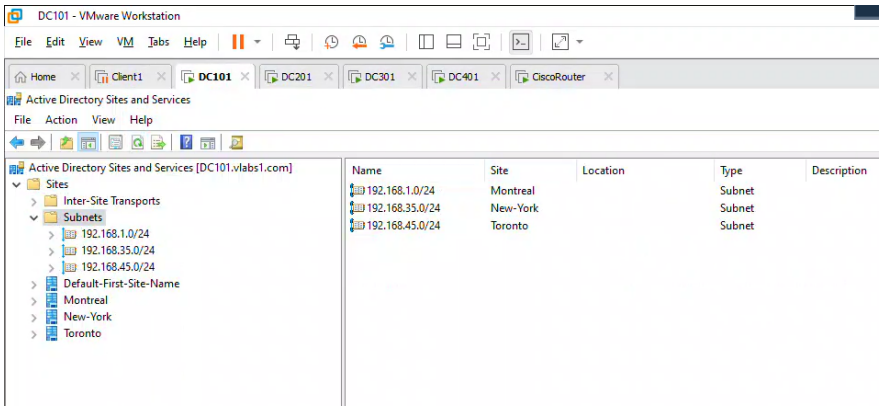
  This creates the subnet object and links it to the **Toronto** site (where DC201 resides).

```
PS C:\Users\Administrator> # Create subnet 192.168.45.0/24 and associate it with the Toronto site.
PS C:\Users\Administrator> New-ADReplicationSubnet -Name "192.168.45.0/24" -Site "Toronto"
PS C:\Users\Administrator> #This creates the subnet object and links it to the Toronto site (where DC201 resi
PS C:\Users\Administrator>
```

- Verify the creation.

Get-ADReplicationSubnet -filter * | Select-Object Name, Site

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

Name            Site
----            ----
192.168.1.0/24  CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
192.168.45.0/24 CN=Toronto,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
192.168.35.0/24 CN=New-York,CN=Sites,CN=Configuration,DC=vlabs1,DC=com


PS C:\Users\Administrator>
```



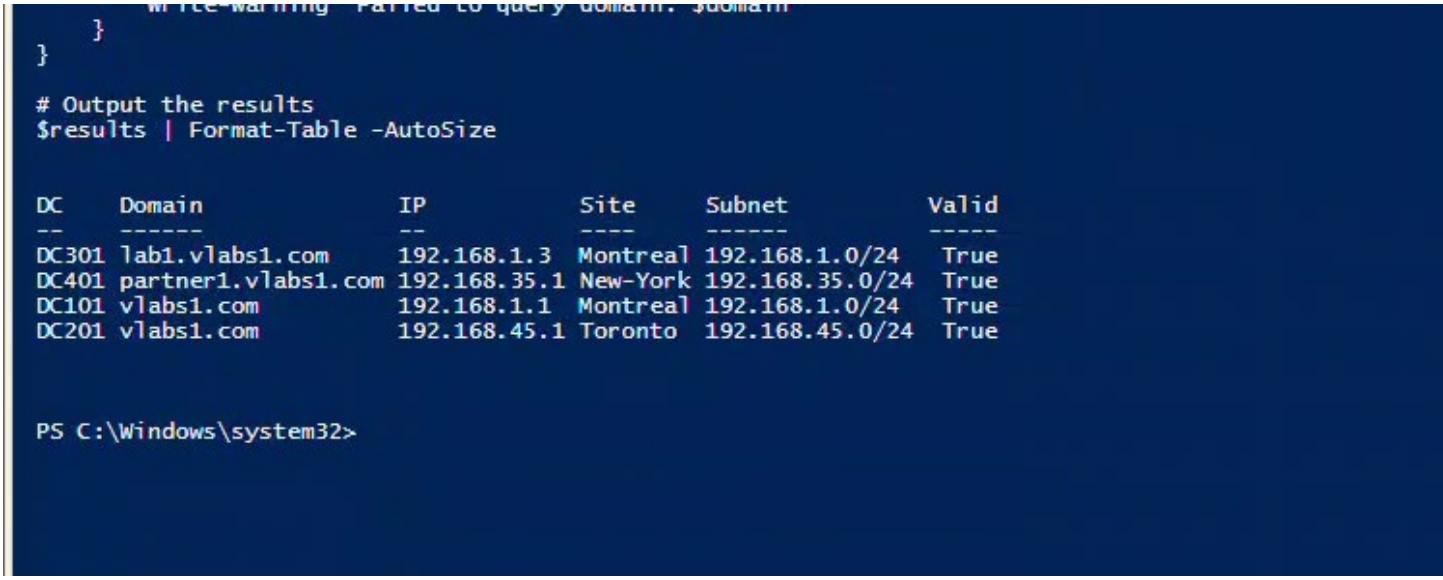
8.2.1 Verification

Validate with DC IP Addresses

Run script

```
# Define site-to-subnet mapping
$subnetMap = @{
  "Montreal" = "192.168.1.0/24"
  "New-York" = "192.168.35.0/24"
  "Toronto" = "192.168.45.0/24"
}

# Get all domains in the forest
$domains = (Get-ADForest).Domains

# Loop through each domain and collect DC info
$results = foreach ($domain in $domains) {
  try {
    Get-ADDomainController -Filter * -Server $domain | ForEach-Object {
      $dc = $_
      $subnet = $subnetMap[$dc.Site]
      [PSCustomObject]@{
        DC     = $dc.Name
        Domain = $domain
        IP     = $dc.IPv4Address
```

```
            Site   = $dc.Site
            Subnet = $subnet
            Valid  = $dc.IPv4Address -like "$($subnet.Split('/')[0].Substring(0,$subnet.Split('/')[0].LastIndexOf('.')))*"
          }
        }
      } catch {
        Write-Warning "Failed to query domain: $domain"
      }
    }

    # Output the results
$results | Format-Table -AutoSize
```



- At this point, DC101, DC301 (in Montreal) and DC401 (in New-York) will match subnets.
- Clients and DCs will now be correctly mapped to their AD Sites based on their IP addresses.
- Intrasite replication will work as expected.
- Logon and DC locator processes will be more efficient

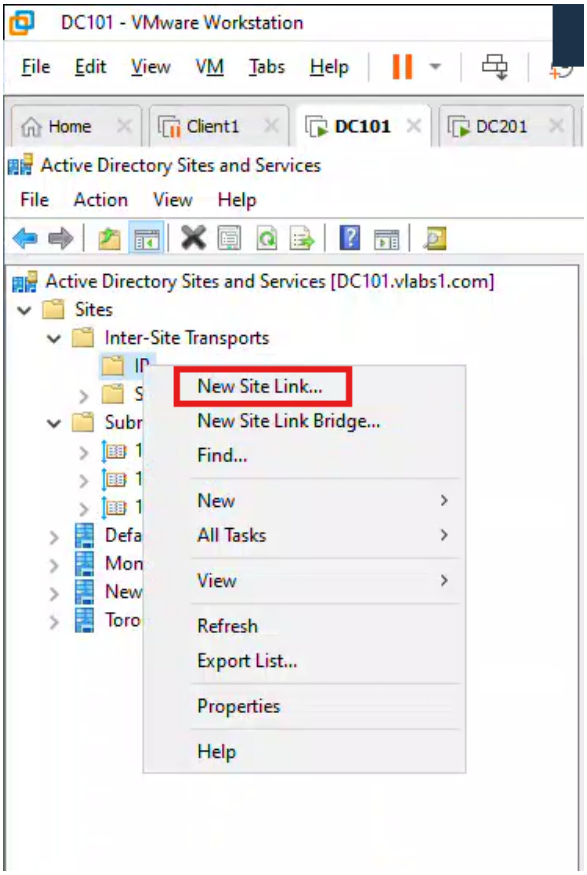
9 Task 7: Creating Site Links

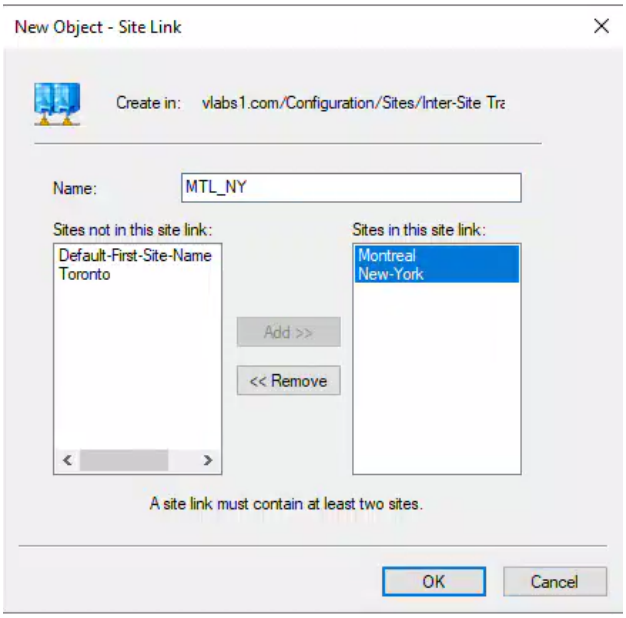
Using GUI:

- Create Site Link **MTL_NY** to link **Montreal** and **New-York** sites.

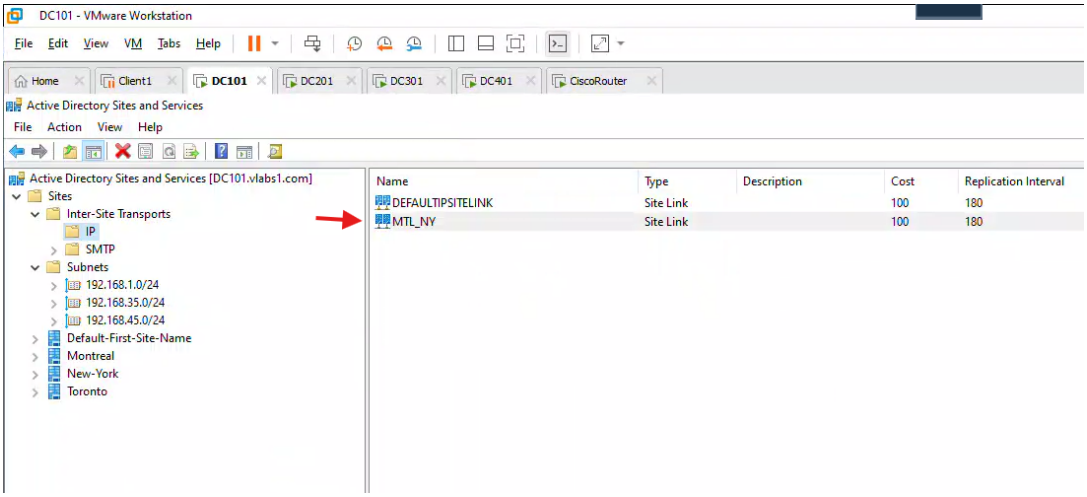
1. Open **Active Directory Sites and Services**
2. Expand the **Inter-Site Transports → IP**
3. Right-click **IP → New Site Link**
4. Name it: `MTL_NY`
5. Select **Montreal** and **New-York** from the list of sites → Click **Add**
6. Click **OK** to create the site link

Adjust replication cost and frequency





You've now created the MTL_NY site link connecting Montreal and New-York.



Using PowerShell:

- Create Site Link **TOR_MTL** to link **Toronto** and **Montreal** sites.

```
New-ADReplicationSiteLink -Name "TOR_MTL" -SitesIncluded "Toronto", "Montreal"
```

- Verify the creation

```
Get-ADReplicationSiteLink -Filter *
```

```
PS C:\Users\Administrator> # Create Site Link TOR_MTL to link Toronto and Montreal sites.
PS C:\Users\Administrator>
PS C:\Users\Administrator> New-ADReplicationSiteLink -Name "TOR_MTL" -SitesIncluded "Toronto", "Montreal"
PS C:\Users\Administrator> # Verify the creation
PS C:\Users\Administrator> Get-ADReplicationSiteLink -Filter *


Cost                          : 100
DistinguishedName             : CN=DEFAULTIPSITELINK,CN=IP,CN=Inter-Site Transports,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
Name                          : DEFAULTIPSITELINK
ObjectClass                   : siteLink
ObjectGUID                    : 106d1d49-97bc-4c71-87cd-14b9bb3c4d40
ReplicationFrequencyInMinutes : 180
SitesIncluded                 : {CN=New-York,CN=Sites,CN=Configuration,DC=vlabs1,DC=com, CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com, CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=

Cost                          : 100
DistinguishedName             : CN=MTL_NY,CN=IP,CN=Inter-Site Transports,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
Name                          : MTL_NY
ObjectClass                   : siteLink
ObjectGUID                    : 815cab75-7ff7-40a5-a763-4b5e6d965869
ReplicationFrequencyInMinutes : 180
SitesIncluded                 : {CN=New-York,CN=Sites,CN=Configuration,DC=vlabs1,DC=com, CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com}

Cost                          :
DistinguishedName             : CN=TOR_MTL,CN=IP,CN=Inter-Site Transports,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
Name                          : TOR_MTL
ObjectClass                   : siteLink
ObjectGUID                    : ef8688bb-39cf-4f51-9e7e-079f0017dc4d
ReplicationFrequencyInMinutes :
SitesIncluded                 : {CN=Toronto,CN=Sites,CN=Configuration,DC=vlabs1,DC=com, CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com}
```

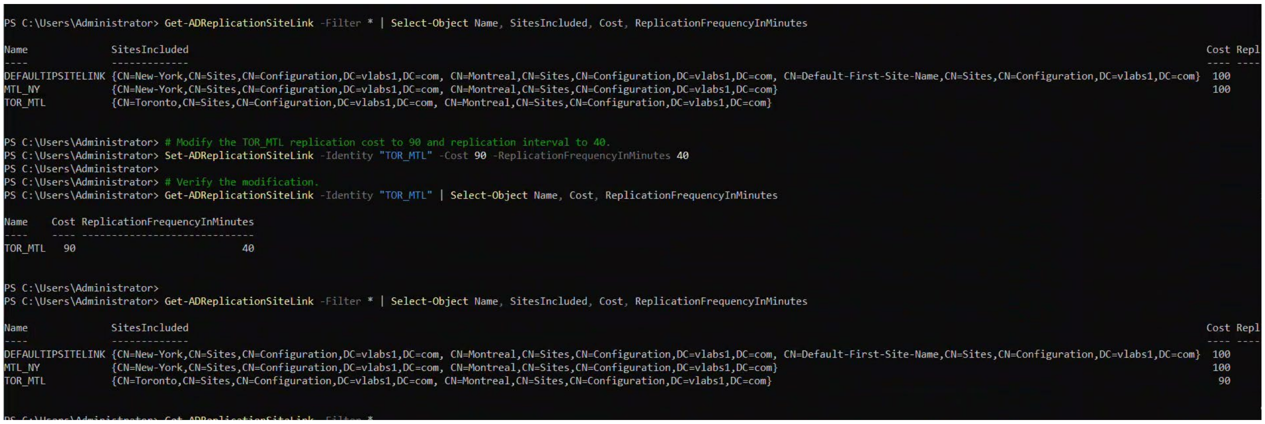
```
Get-ADReplicationSiteLink -Filter * | Select-Object Name, SitesIncluded, Cost, ReplicationFrequencyInMinutes
```

- Modify the **TOR_MTL** replication cost to **90** and replication interval to **40**.

```
Set-ADReplicationSiteLink -Identity "TOR_MTL" -Cost 90 -ReplicationFrequencyInMinutes 40
```

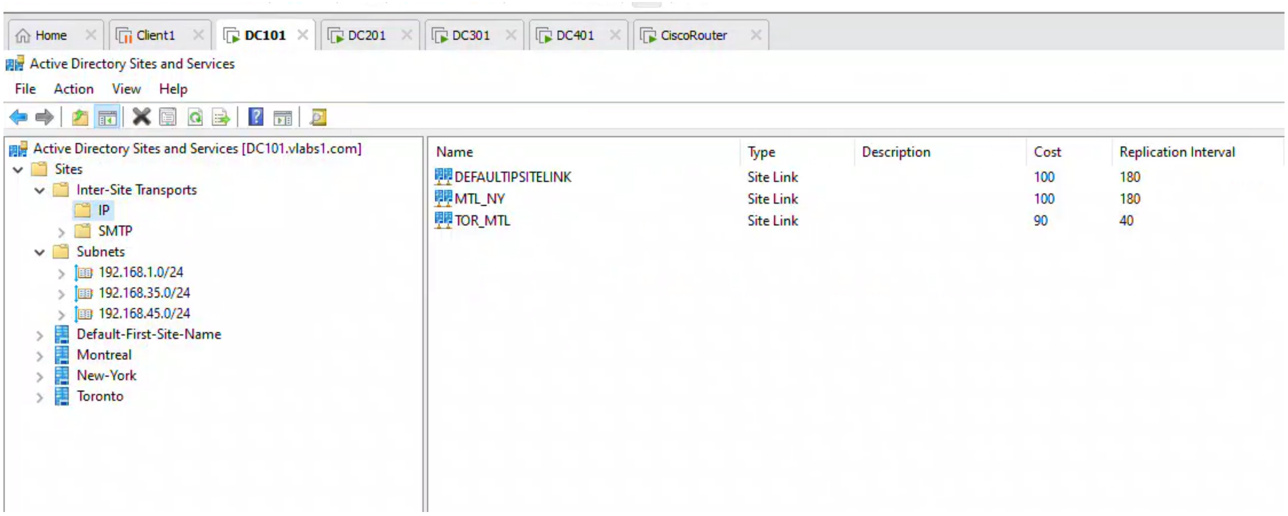
- Verify the modification.

```
Get-ADReplicationSiteLink -Identity "TOR_MTL" | Select-Object Name, Cost, ReplicationFrequencyInMinutes
```



```
PS C:\Users\Administrator> Get-ADReplicationSiteLink -Filter * | Select-Object Name, SitesIncluded, Cost, ReplicationFrequencyInMinutes

Name              SitesIncluded                                                                                                                                                      Cost Repl
----              -------------                                                                                                                                                      ---- ----
DEFAULTIPSITELINK {CN=New-York,CN=Sites,CN=Configuration,DC=vlabs1,DC=com, CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com, CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com}  100
MTL_NY            {CN=New-York,CN=Sites,CN=Configuration,DC=vlabs1,DC=com, CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com}                                                    100
TOR_MTL           {CN=Toronto,CN=Sites,CN=Configuration,DC=vlabs1,DC=com, CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com}


PS C:\Users\Administrator> # Modify the TOR_MTL replication cost to 90 and replication interval to 40.
PS C:\Users\Administrator> Set-ADReplicationSiteLink -Identity "TOR_MTL" -Cost 90 -ReplicationFrequencyInMinutes 40
PS C:\Users\Administrator>
PS C:\Users\Administrator> # Verify the modification.
PS C:\Users\Administrator> Get-ADReplicationSiteLink -Identity "TOR_MTL" | Select-Object Name, Cost, ReplicationFrequencyInMinutes

Name    Cost ReplicationFrequencyInMinutes
----    ---- -----------------------------
TOR_MTL   90                            40


PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-ADReplicationSiteLink -Filter * | Select-Object Name, SitesIncluded, Cost, ReplicationFrequencyInMinutes

Name              SitesIncluded                                                                                                                                                      Cost Repl
----              -------------                                                                                                                                                      ---- ----
DEFAULTIPSITELINK {CN=New-York,CN=Sites,CN=Configuration,DC=vlabs1,DC=com, CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com, CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com}  100
MTL_NY            {CN=New-York,CN=Sites,CN=Configuration,DC=vlabs1,DC=com, CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com}                                                    100
TOR_MTL           {CN=Toronto,CN=Sites,CN=Configuration,DC=vlabs1,DC=com, CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com}                                                      90
```

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


Cost                          : 100
DistinguishedName             : CN=DEFAULTIPSITELINK,CN=IP,CN=Inter-Site Transports,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
Name                          : DEFAULTIPSITELINK
ObjectClass                   : siteLink
ObjectGUID                    : 106d1d49-97bc-4c71-87cd-14b9bb3c4d40
ReplicationFrequencyInMinutes : 180
SitesIncluded                 : {CN=New-York,CN=Sites,CN=Configuration,DC=vlabs1,DC=com, CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com, CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=

Cost                          : 100
DistinguishedName             : CN=MTL_NY,CN=IP,CN=Inter-Site Transports,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
Name                          : MTL_NY
ObjectClass                   : siteLink
ObjectGUID                    : 815cab75-7ff7-40a5-a763-4b5e6d965869
ReplicationFrequencyInMinutes : 180
SitesIncluded                 : {CN=New-York,CN=Sites,CN=Configuration,DC=vlabs1,DC=com, CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com}

Cost                          : 90
DistinguishedName             : CN=TOR_MTL,CN=IP,CN=Inter-Site Transports,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
Name                          : TOR_MTL
ObjectClass                   : siteLink
ObjectGUID                    : ef8688bb-39cf-4f51-9e7e-079f0017dc4d
ReplicationFrequencyInMinutes : 40
SitesIncluded                 : {CN=Toronto,CN=Sites,CN=Configuration,DC=vlabs1,DC=com, CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com}


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

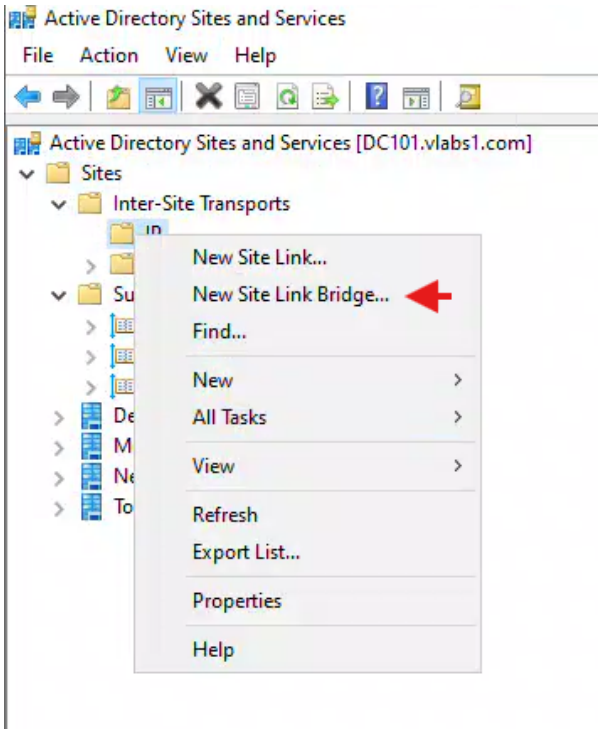


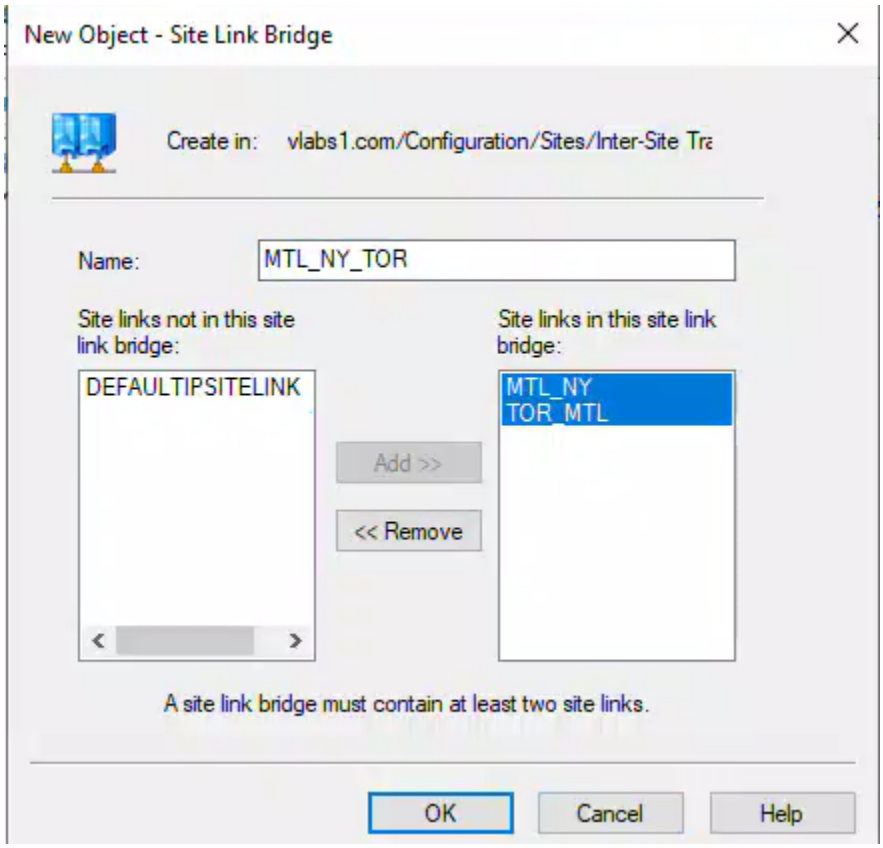
10 Task 8: Creating Site Link Bridge

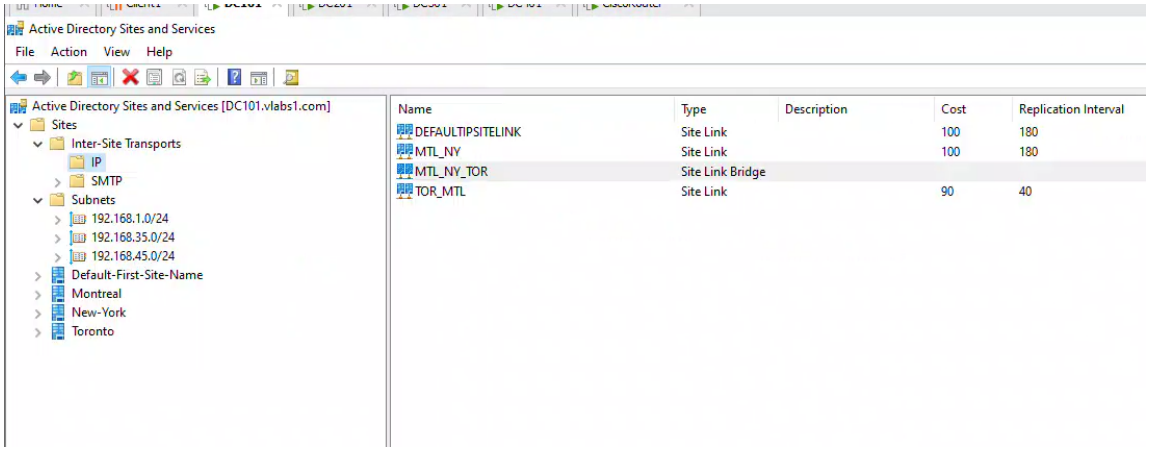
10.1 Using GUI:

- Create a Site Link Bridge MTL_NY_TOR and add the two links: MTL_NY and TOR_MTL.
  1. Open Active Directory Sites and Services
  2. Expand Inter-Site Transports → IP
  3. Right-click IP → New Site Link Bridge
  4. Name: MTL_NY_TOR
  5. In Site links, select:
  6. MTL_NY
  7. TOR_MTL

8. Click Add, then OK







10.2 Using PowerShell:

- **Verify the new Site Link Bridge.**

Get-ADReplicationSiteLinkBridge -Filter * | Select-Object Name, SiteLinksIncluded

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

Name       SiteLinksIncluded
----       -----------------
MTL_NY_TOR {CN=TOR_MTL,CN=IP,CN=Inter-Site Transports,CN=Sites,CN=Configuration,DC=vlabs1,DC=com, CN=MTL_NY,CN=IP,CN=Inter-Site Transports,CN=Sites,CN=Configuration,DC=vlabs1,DC=com}


PS C:\Users\Administrator>
```

Get-ADReplicationSiteLinkBridge -Filter *

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


DistinguishedName : CN=MTL_NY_TOR,CN=IP,CN=Inter-Site Transports,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
Name              : MTL_NY_TOR
ObjectClass       : siteLinkBridge
ObjectGUID        : 4c3b3e37-d889-4d10-ba67-73ebce460cbc
SiteLinksIncluded : {CN=TOR_MTL,CN=IP,CN=Inter-Site Transports,CN=Sites,CN=Configuration,DC=vlabs1,DC=com, CN=MTL_NY,CN=IP,CN=Inter-Site Transports,CN=Sites,CN=Configuration,DC=vlabs1,DC=com}


PS C:\Users\Administrator>
```

11 Task 9: Selecting a Bridgehead

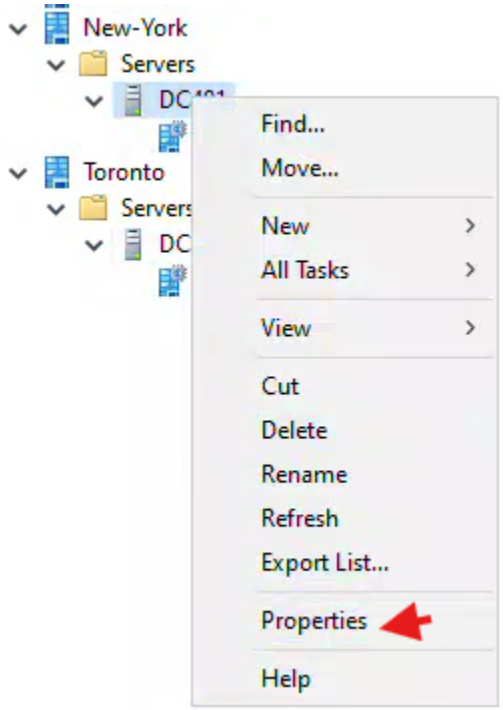
Using GUI:

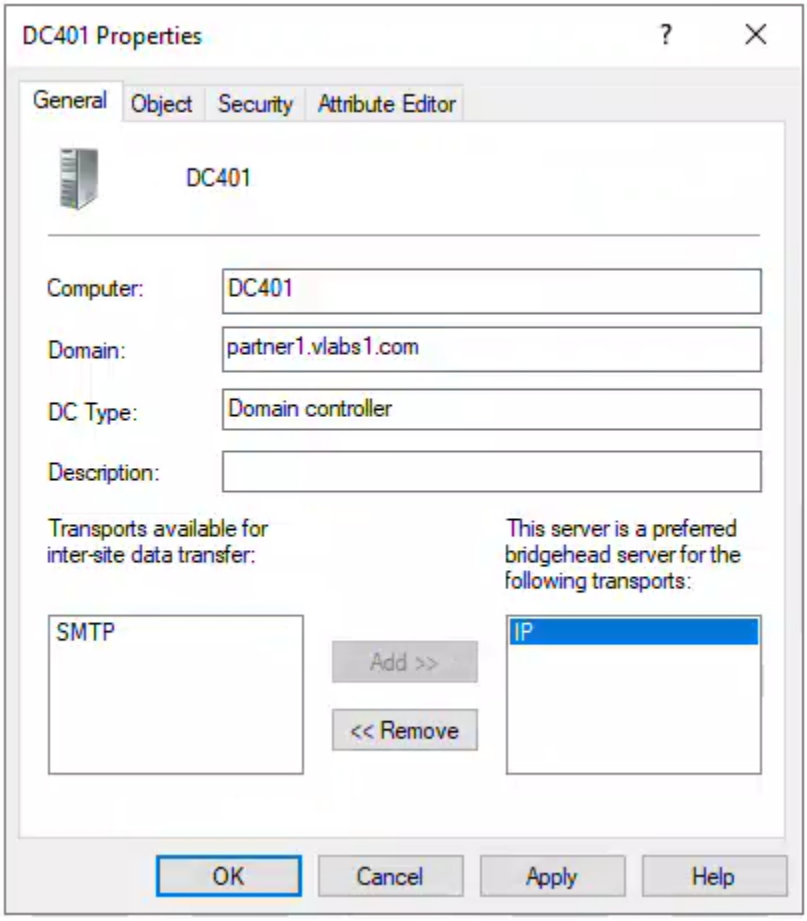
- Select **DC201** as a bridgehead for the **New-York** Site.
  NOTE - DC401 is in New-York

1. Open Active Directory Sites and Services
2. Expand:
   Sites → New-york → Servers → DC401
3. Right-click → Properties
4. Under Transports available for inter-site data transfer:
   - Select IP

- Check: "This server is a preferred bridgehead server for the selected transport."

5. Click Add, then OK





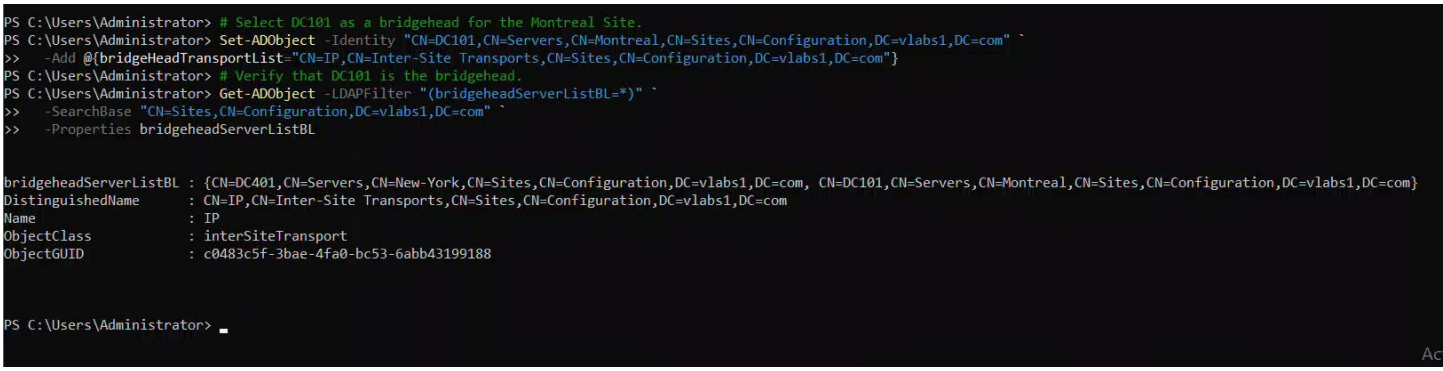
Using PowerShell:

- Select **DC101** as a **bridgehead** for the **Montreal** Site.

```
Set-ADObject -Identity "CN=DC101,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com" `
 -Add @{bridgeHeadTransportList="CN=IP,CN=Inter-Site Transports,CN=Sites,CN=Configuration,DC=vlabs1,DC=com"}
```

- Verify that **DC101** is the bridgehead.

```
Get-ADObject -LDAPFilter "(bridgeheadServerListBL=*)" `
 -SearchBase "CN=Sites,CN=Configuration,DC=vlabs1,DC=com" `
-Properties bridgeheadServerListBL
```



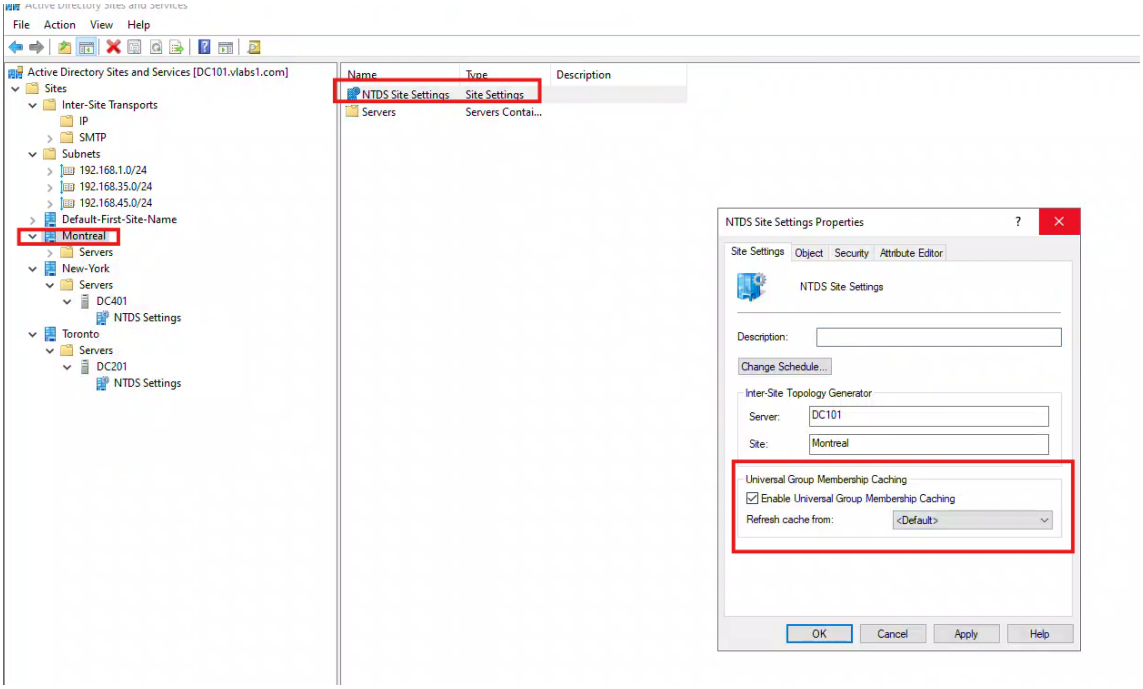
12 Task 10: Managing Universal Group Membership

Using GUI:

- Enable **Universal Group Membership** on the **Montreal** site.

1. Open Active Directory Sites and Services
2. Expand Sites → Montreal
3. Right-click Montreal, then select NTDS Site Settings -> Properties
4. Check the box:

   Enable Universal Group Membership Caching
5. Select a site from which UGMC will be refreshed (usually a site with a Global Catalog like Montreal itself or the forest root).
6. Click OK



Using PowerShell:

- Enable **Universal Group Membership** on the **New-York** site.

Set-ADReplicationSite -Identity "New-York"

```
PS C:\Users\Administrator> Set-ADReplicationSite -Identity "New-York"
PS C:\Users\Administrator>
```

13 Task 11: Monitoring and Troubleshooting Replication

From DC101, using PowerShell:

- Check the **replication partner** and the **replication status.**

repadmin/showrepl

```
PS C:\Users\Administrator> # Check the replication partner and the replication sta
PS C:\Users\Administrator> repadmin /showrepl

Repadmin: running command /showrepl against full DC localhost
Montreal\DC101
DSA Options: IS_GC
Site Options: IS_GROUP_CACHING_ENABLED
DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
DSA invocationID: 6d4f756b-185b-401f-84a0-d6d08a09a098

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

CN=Configuration,DC=vlabs1,DC=com
    Montreal\DC301 via RPC
        DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
        Last attempt @ 2025-05-19 21:27:07 was successful.
    New-York\DC401 via RPC
        DSA object GUID: 01004c70-51e1-4b52-9a48-aac4cc610935
        Last attempt @ 2025-05-19 21:37:39 was successful.

CN=Schema,CN=Configuration,DC=vlabs1,DC=com
    Montreal\DC301 via RPC
        DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
        Last attempt @ 2025-05-19 20:46:49 was successful.
    New-York\DC401 via RPC
        DSA object GUID: 01004c70-51e1-4b52-9a48-aac4cc610935
        Last attempt @ 2025-05-19 21:21:49 was successful.

DC=ForestDnsZones,DC=vlabs1,DC=com
    Montreal\DC301 via RPC
        DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
        Last attempt @ 2025-05-19 20:46:49 was successful.
    New-York\DC401 via RPC
        DSA object GUID: 01004c70-51e1-4b52-9a48-aac4cc610935
        Last attempt @ 2025-05-19 21:21:49 was successful.

DC=lab1,DC=vlabs1,DC=com
    Montreal\DC301 via RPC
        DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
        Last attempt @ 2025-05-19 21:17:37 was successful.

DC=partner1,DC=vlabs1,DC=com
    Montreal\DC301 via RPC
        DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
        Last attempt @ 2025-05-19 20:46:49 was successful.
    New-York\DC401 via RPC
        DSA object GUID: 01004c70-51e1-4b52-9a48-aac4cc610935
        Last attempt @ 2025-05-19 21:21:49 was successful.

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

- Identify any **replication errors** and **resolve** them.

Get-ADReplicationFailure -Target DC101 -Scope Server

repadmin/showrepl/errorsonly

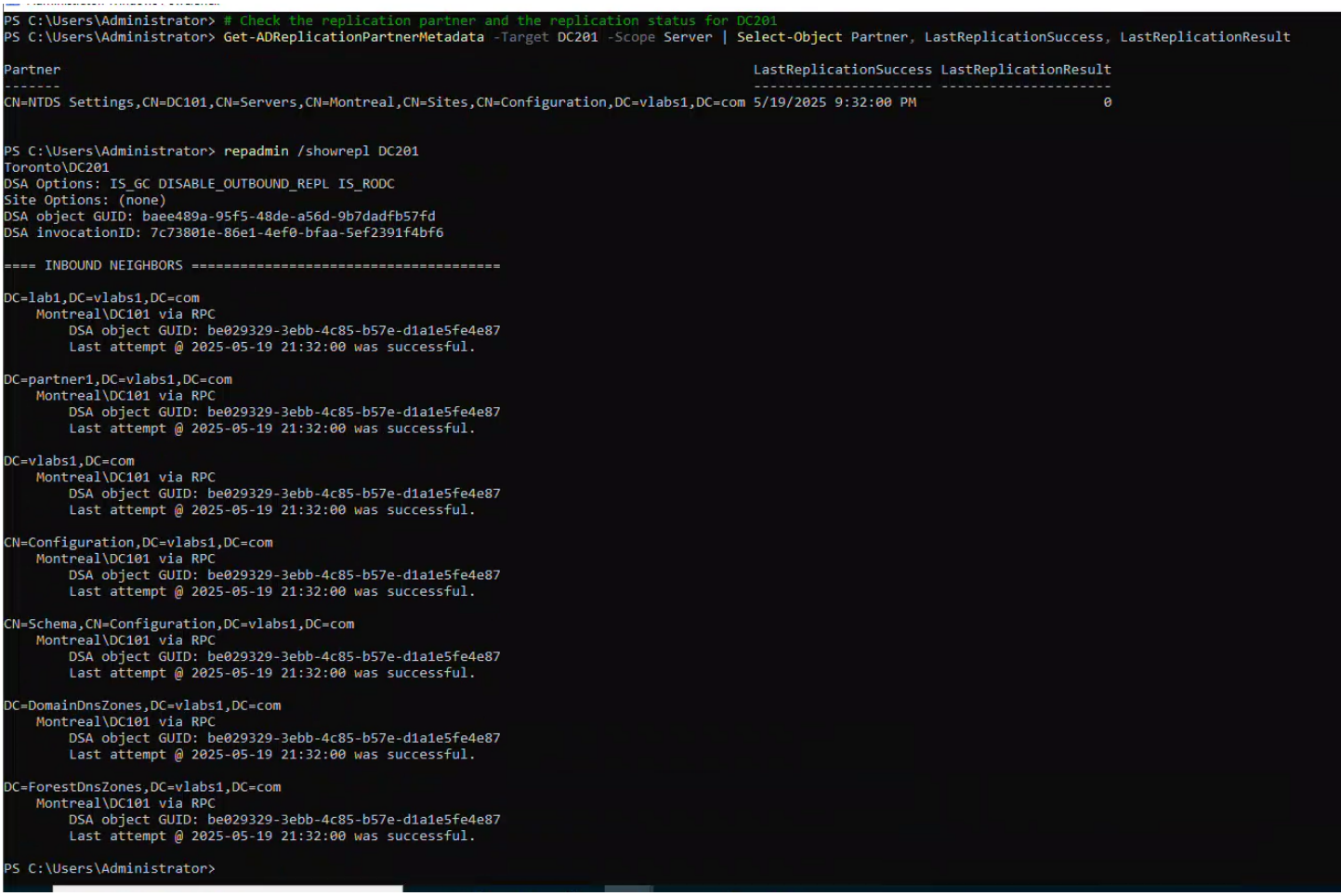
```
PS C:\Users\Administrator>
PS C:\Users\Administrator> #Identify any replication errors and resolve them.
PS C:\Users\Administrator> Get-ADReplicationFailure -Target DC101 -Scope Server


FailureCount     : 0
FailureType      : Link
FirstFailureTime : 5/19/2025 3:57:45 AM
LastError        : 8524
Partner          : CN=NTDS Settings,CN=DC301,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
PartnerGuid      : 250991af-de4f-4e49-b0df-f46c18bb4651
Server           : DC101.vlabs1.com



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

Repadmin: running command /showrepl against full DC localhost
Montreal\DC101
DSA Options: IS_GC
Site Options: IS_GROUP_CACHING_ENABLED
DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
DSA invocationID: 6d4f756b-185b-401f-84a0-d6d08a09a098

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

PS C:\Users\Administrator>
```

cl

- Check the **replication partner** and the **replication status for DC201**

Get-ADReplicationPartnerMetadata -Target DC201 -Scope Server | Select-Object Partner, LastReplicationSuccess, LastReplicationResult

repadmin/showrepl DC201



```
PS C:\Users\Administrator> # Check the replication partner and the replication status for DC201
PS C:\Users\Administrator> Get-ADReplicationPartnerMetadata -Target DC201 -Scope Server | Select-Object Partner, LastReplicationSuccess, LastReplicationResult

Partner                                                                                 LastReplicationSuccess LastReplicationResult
-------                                                                                 ---------------------- --------------------
CN=NTDS Settings,CN=DC101,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com 5/19/2025 9:32:00 PM                      0


PS C:\Users\Administrator> repadmin /showrepl DC201
Toronto\DC201
DSA Options: IS_GC DISABLE_OUTBOUND_REPL IS_RODC
Site Options: (none)
DSA object GUID: baee489a-95f5-48de-a56d-9b7dadfb57fd
DSA invocationID: 7c73801e-86e1-4ef0-bfaa-5ef2391f4bf6

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

DC=lab1,DC=vlabs1,DC=com
    Montreal\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-19 21:32:00 was successful.

DC=partner1,DC=vlabs1,DC=com
    Montreal\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-19 21:32:00 was successful.

DC=vlabs1,DC=com
    Montreal\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-19 21:32:00 was successful.

CN=Configuration,DC=vlabs1,DC=com
    Montreal\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-19 21:32:00 was successful.

CN=Schema,CN=Configuration,DC=vlabs1,DC=com
    Montreal\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-19 21:32:00 was successful.

DC=DomainDnsZones,DC=vlabs1,DC=com
    Montreal\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-19 21:32:00 was successful.

DC=ForestDnsZones,DC=vlabs1,DC=com
    Montreal\DC101 via RPC
        DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
        Last attempt @ 2025-05-19 21:32:00 was successful.

PS C:\Users\Administrator>
```

- Summarize the **replication status** and the **overall replication health.**

repadmin /replsummary

```
PS C:\Users\Administrator> repadmin /replsummary
Replication Summary Start Time: 2025-05-19 21:45:28

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

Source DSA          largest delta    fails/total %%   error
 DC101                  01h:43m:04s    0 /  15    0
 DC301                      58m:39s    0 /   5    0
 DC401                      23m:39s    0 /   4    0

Destination DSA     largest delta    fails/total %%   error
 DC101                      58m:39s    0 /   9    0
 DC201                      13m:27s    0 /   7    0
 DC301                      58m:05s    0 /   5    0
 DC401                  01h:43m:04s    0 /   3    0

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

- Check the **replication queue**.

repadmin /queue

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

Repadmin: running command /queue against full DC localhost
Queue contains 0 items.

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

- Force replication between **DC101** and **DC301** by **pulling** from **DC301**

repadmin /syncall DC301 /aPed

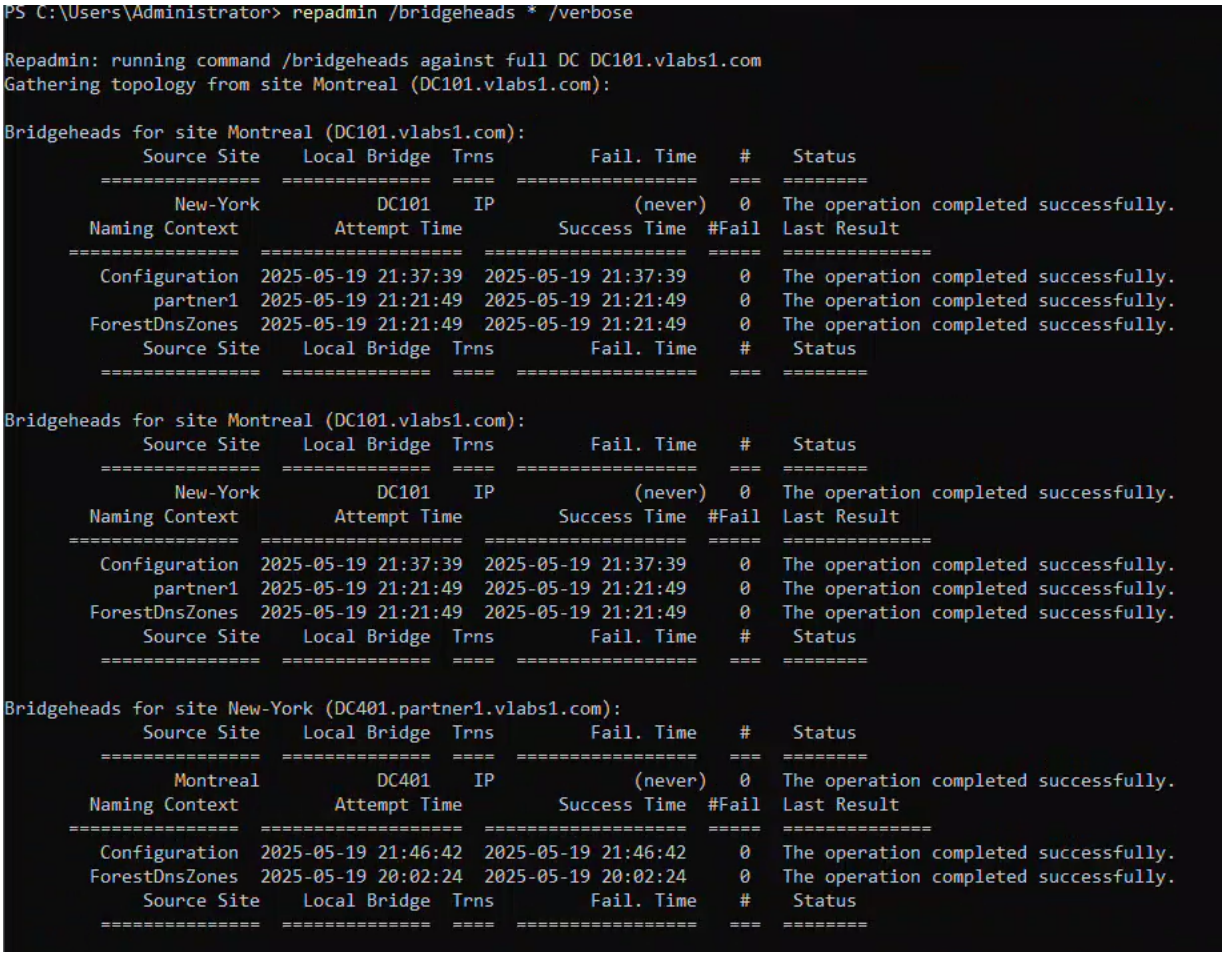
```
PS C:\Users\Administrator> repadmin /syncall DC301 /aPed
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC301,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC101,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC301,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC101,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication is in progress:
    From: CN=NTDS Settings,CN=DC101,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC401,CN=Servers,CN=New-York,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: The following replication completed successfully:
    From: CN=NTDS Settings,CN=DC101,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
    To  : CN=NTDS Settings,CN=DC401,CN=Servers,CN=New-York,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.

PS C:\Users\Administrator>
```

- List the **Topology information**.

repadmin /showrepl

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

Repadmin: running command /showrepl against full DC localhost
Montreal\DC101
DSA Options: IS_GC
Site Options: IS_GROUP_CACHING_ENABLED
DSA object GUID: be029329-3ebb-4c85-b57e-d1a1e5fe4e87
DSA invocationID: 6d4f756b-185b-401f-84a0-d6d08a09a098

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

CN=Configuration,DC=vlabs1,DC=com
    New-York\DC401 via RPC
        DSA object GUID: 01004c70-51e1-4b52-9a48-aac4cc610935
        Last attempt @ 2025-05-19 21:37:39 was successful.
    Montreal\DC301 via RPC
        DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
        Last attempt @ 2025-05-19 21:46:49 was successful.

CN=Schema,CN=Configuration,DC=vlabs1,DC=com
    New-York\DC401 via RPC
        DSA object GUID: 01004c70-51e1-4b52-9a48-aac4cc610935
        Last attempt @ 2025-05-19 21:21:49 was successful.
    Montreal\DC301 via RPC
        DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
        Last attempt @ 2025-05-19 21:46:49 was successful.

DC=ForestDnsZones,DC=vlabs1,DC=com
    New-York\DC401 via RPC
        DSA object GUID: 01004c70-51e1-4b52-9a48-aac4cc610935
        Last attempt @ 2025-05-19 21:21:49 was successful.
    Montreal\DC301 via RPC
        DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
        Last attempt @ 2025-05-19 21:46:49 was successful.

DC=lab1,DC=vlabs1,DC=com
    Montreal\DC301 via RPC
        DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
        Last attempt @ 2025-05-19 21:46:49 was successful.

DC=partner1,DC=vlabs1,DC=com
    New-York\DC401 via RPC
        DSA object GUID: 01004c70-51e1-4b52-9a48-aac4cc610935
        Last attempt @ 2025-05-19 21:21:49 was successful.
    Montreal\DC301 via RPC
        DSA object GUID: 250991af-de4f-4e49-b0df-f46c18bb4651
        Last attempt @ 2025-05-19 21:46:49 was successful.
```

repadmin /bridgeheads * /verbose



```
PS C:\Users\Administrator> repadmin /bridgeheads * /verbose

Repadmin: running command /bridgeheads against full DC DC101.vlabs1.com
Gathering topology from site Montreal (DC101.vlabs1.com):

Bridgeheads for site Montreal (DC101.vlabs1.com):
            Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ==============  ==============  ====  ================   ===  ========
                New-York           DC101    IP             (never)   0   The operation completed successfully.
       Naming Context         Attempt Time         Success Time  #Fail  Last Result
     ===============  ==================  ==================  =====  ==============
        Configuration  2025-05-19 21:37:39  2025-05-19 21:37:39     0   The operation completed successfully.
              partner1  2025-05-19 21:21:49  2025-05-19 21:21:49     0   The operation completed successfully.
       ForestDnsZones  2025-05-19 21:21:49  2025-05-19 21:21:49     0   The operation completed successfully.
            Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ==============  ==============  ====  ================   ===  ========

Bridgeheads for site Montreal (DC101.vlabs1.com):
            Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ==============  ==============  ====  ================   ===  ========
                New-York           DC101    IP             (never)   0   The operation completed successfully.
       Naming Context         Attempt Time         Success Time  #Fail  Last Result
     ===============  ==================  ==================  =====  ==============
        Configuration  2025-05-19 21:37:39  2025-05-19 21:37:39     0   The operation completed successfully.
              partner1  2025-05-19 21:21:49  2025-05-19 21:21:49     0   The operation completed successfully.
       ForestDnsZones  2025-05-19 21:21:49  2025-05-19 21:21:49     0   The operation completed successfully.
            Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ==============  ==============  ====  ================   ===  ========

Bridgeheads for site New-York (DC401.partner1.vlabs1.com):
            Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ==============  ==============  ====  ================   ===  ========
                Montreal           DC401    IP             (never)   0   The operation completed successfully.
       Naming Context         Attempt Time         Success Time  #Fail  Last Result
     ===============  ==================  ==================  =====  ==============
        Configuration  2025-05-19 21:46:42  2025-05-19 21:46:42     0   The operation completed successfully.
       ForestDnsZones  2025-05-19 20:02:24  2025-05-19 20:02:24     0   The operation completed successfully.
            Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ==============  ==============  ====  ================   ===  ========
```

```
Repadmin: not running against read-only DC DC201.vlabs1.com since it is incompatible with this command.

Repadmin: running command /bridgeheads against full DC DC301.lab1.vlabs1.com
Gathering topology from site Montreal (DC301.lab1.vlabs1.com):

Bridgeheads for site Montreal (DC101.vlabs1.com):
            Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ==============  ==============  ====  ================   ===  ========
                New-York           DC101    IP             (never)   0   The operation completed successfully.
       Naming Context         Attempt Time         Success Time  #Fail  Last Result
     ===============  ==================  ==================  =====  ==============
        Configuration  2025-05-19 21:37:39  2025-05-19 21:37:39     0   The operation completed successfully.
             partner1  2025-05-19 21:21:49  2025-05-19 21:21:49     0   The operation completed successfully.
       ForestDnsZones  2025-05-19 21:21:49  2025-05-19 21:21:49     0   The operation completed successfully.
            Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ==============  ==============  ====  ================   ===  ========

Bridgeheads for site Montreal (DC101.vlabs1.com):
            Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ==============  ==============  ====  ================   ===  ========
                New-York           DC101    IP             (never)   0   The operation completed successfully.
       Naming Context         Attempt Time         Success Time  #Fail  Last Result
     ===============  ==================  ==================  =====  ==============
        Configuration  2025-05-19 21:37:39  2025-05-19 21:37:39     0   The operation completed successfully.
             partner1  2025-05-19 21:21:49  2025-05-19 21:21:49     0   The operation completed successfully.
       ForestDnsZones  2025-05-19 21:21:49  2025-05-19 21:21:49     0   The operation completed successfully.
            Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ==============  ==============  ====  ================   ===  ========

Bridgeheads for site New-York (DC401.partner1.vlabs1.com):
            Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ==============  ==============  ====  ================   ===  ========
                Montreal           DC401    IP             (never)   0   The operation completed successfully.
       Naming Context         Attempt Time         Success Time  #Fail  Last Result
     ===============  ==================  ==================  =====  ==============
        Configuration  2025-05-19 21:46:42  2025-05-19 21:46:42     0   The operation completed successfully.
       ForestDnsZones  2025-05-19 20:02:24  2025-05-19 20:02:24     0   The operation completed successfully.
            Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ==============  ==============  ====  ================   ===  ========

Repadmin: running command /bridgeheads against full DC DC401.partner1.vlabs1.com
```

```
Repadmin: running command /bridgeheads against full DC DC401.partner1.vlabs1.com
Gathering topology from site New-York (DC401.partner1.vlabs1.com):

Bridgeheads for site Montreal (DC101.vlabs1.com):
            Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ==============  ==============  ====  ================   ===  ========
                New-York           DC101    IP            (never)   0   The operation completed successfully.
       Naming Context         Attempt Time         Success Time  #Fail  Last Result
     ================  ==================  ==================  =====  ==============
        Configuration  2025-05-19 21:37:39  2025-05-19 21:37:39     0   The operation completed successfully.
              partner1  2025-05-19 21:21:49  2025-05-19 21:21:49     0   The operation completed successfully.
       ForestDnsZones  2025-05-19 21:21:49  2025-05-19 21:21:49     0   The operation completed successfully.
            Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ==============  ==============  ====  ================   ===  ========

Bridgeheads for site Montreal (DC101.vlabs1.com):
            Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ==============  ==============  ====  ================   ===  ========
                New-York           DC101    IP            (never)   0   The operation completed successfully.
       Naming Context         Attempt Time         Success Time  #Fail  Last Result
     ================  ==================  ==================  =====  ==============
        Configuration  2025-05-19 21:37:39  2025-05-19 21:37:39     0   The operation completed successfully.
              partner1  2025-05-19 21:21:49  2025-05-19 21:21:49     0   The operation completed successfully.
       ForestDnsZones  2025-05-19 21:21:49  2025-05-19 21:21:49     0   The operation completed successfully.
            Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ==============  ==============  ====  ================   ===  ========

Bridgeheads for site New-York (DC401.partner1.vlabs1.com):
            Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ==============  ==============  ====  ================   ===  ========
                Montreal           DC401    IP            (never)   0   The operation completed successfully.
       Naming Context         Attempt Time         Success Time  #Fail  Last Result
     ================  ==================  ==================  =====  ==============
        Configuration  2025-05-19 21:46:42  2025-05-19 21:46:42     0   The operation completed successfully.
       ForestDnsZones  2025-05-19 20:02:24  2025-05-19 20:02:24     0   The operation completed successfully.
            Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ==============  ==============  ====  ================   ===  ========

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

- Detailed partner and connection metadata:

```
# Get summary replication status across the forest
$summary = repadmin /replsummary

# Get detailed per-DC status
$details = repadmin /showrepl *

# Get any replication errors
$errorsOnly = repadmin /showrepl /errorsonly

# Save to a report file
$reportPath = "$env:USERPROFILE\Desktop\AD_Replication_Report.txt"
```

```
@"
```

```
======== Active Directory Replication Health Report ========

Date: $(Get-Date -Format "yyyy-MM-dd HH:mm:ss")

--- Replication Summary (repadmin /replsummary) ---
$summary

--- Replication Details (repadmin /showrepl *) ---
$details

--- Replication Errors Only (repadmin /showrepl /errorsonly) ---
$errorsOnly

============================================================
"@ | Out-File -Encoding UTF8 -FilePath $reportPath

Start-Process notepad.exe $reportPath
```

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> # Get summary replication status across the forest
PS C:\Users\Administrator> $summary = repadmin /replsummary
PS C:\Users\Administrator>
PS C:\Users\Administrator> # Get detailed per-DC status
PS C:\Users\Administrator> $details = repadmin /showrepl *
PS C:\Users\Administrator>
PS C:\Users\Administrator> # Get any replication errors
PS C:\Users\Administrator> $errorsOnly = repadmin /showrepl /errorsonly
PS C:\Users\Administrator>
PS C:\Users\Administrator> # Save to a report file
PS C:\Users\Administrator> $reportPath = "$env:USERPROFILE\Desktop\AD_Replication_Report.txt"
PS C:\Users\Administrator>
PS C:\Users\Administrator> @"
>> ======== Active Directory Replication Health Report ========
>>
>> Date: $(Get-Date -Format "yyyy-MM-dd HH:mm:ss")
>>
>> --- Replication Summary (repadmin /replsummary) ---
>> $summary
>>
>> --- Replication Details (repadmin /showrepl *) ---
>> $details
>>
>> --- Replication Errors Only (repadmin /showrepl /errorsonly) ---
>> $errorsOnly
>>
>> ============================================================
>> "@ | Out-File -Encoding UTF8 -FilePath $reportPath
PS C:\Users\Administrator>
PS C:\Users\Administrator> Start-Process notepad.exe $reportPath
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
```

======== Active Directory Replication Health Report ========

Date: 2025-05-19 22:07:07

--- Replication Summary (repadmin /replsummary) ---

Replication Summary Start Time: 2025-05-19 22:07:03

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

.....

Source DSA	Largest Delta	Fails/Total	% Error
DC101	02h:04m:39s	0 / 15	0
DC301	00h:02m:41s	0 / 5	0
DC401	00h:45m:14s	0 / 4	0

Destination DSA	Largest Delta	Fails/Total	% Error
DC101	00h:45m:14s	0 / 9	0
DC201	00h:35m:02s	0 / 7	0
DC301	00h:19m:40s	0 / 5	0
DC401	02h:04m:40s	0 / 3	0

--- Replication Details (repadmin /showrepl *) ---

DC101.vlabs1.com (Site: Montreal)

CN=Configuration,DC=vlabs1,DC=com

New-York\DC401 via RPC (Last success: 21:52:39)

Montreal\DC301 via RPC (Last success: 22:04:23)

CN=Schema,CN=Configuration,DC=vlabs1,DC=com

DC401 (Last success: 21:21:49)

DC301 (Last success: 22:04:22)

DC=ForestDnsZones,DC=vlabs1,DC=com

DC401 (Last success: 21:21:49)

DC301 (Last success: 22:04:22)

DC=lab1,DC=vlabs1,DC=com
   DC301 (Last success: 22:04:23)

DC=partner1,DC=vlabs1,DC=com
   DC401 (Last success: 22:02:44)
   DC301 (Last success: 22:04:23)

DC201.vlabs1.com (Site: Toronto - RODC)

All replication from Montreal\DC101

DC=lab1,DC=vlabs1,DC=com (Last success: 21:32:00)
DC=partner1,DC=vlabs1,DC=com (Last success: 21:32:00)
DC=vlabs1,DC=com (Last success: 21:32:00)
CN=Configuration,DC=vlabs1,DC=com (Last success: 21:32:00)
CN=Schema,CN=Configuration (Last success: 21:32:00)
DC=DomainDnsZones,DC=vlabs1,DC=com (Last success: 21:32:00)
DC=ForestDnsZones,DC=vlabs1,DC=com (Last success: 21:32:00)

DC301.lab1.vlabs1.com (Site: Montreal)

All replication from Montreal\DC101

CN=Configuration (Last success: 22:07:04)
CN=Schema (Last success: 21:47:23)
DC=ForestDnsZones (Last success: 21:47:23)
DC=vlabs1.com (Last success: 22:02:05)
DC=partner1.vlabs1.com (Last success: 21:47:23)

DC401.partner1.vlabs1.com (Site: New-York)

All

- View intersite topology generation

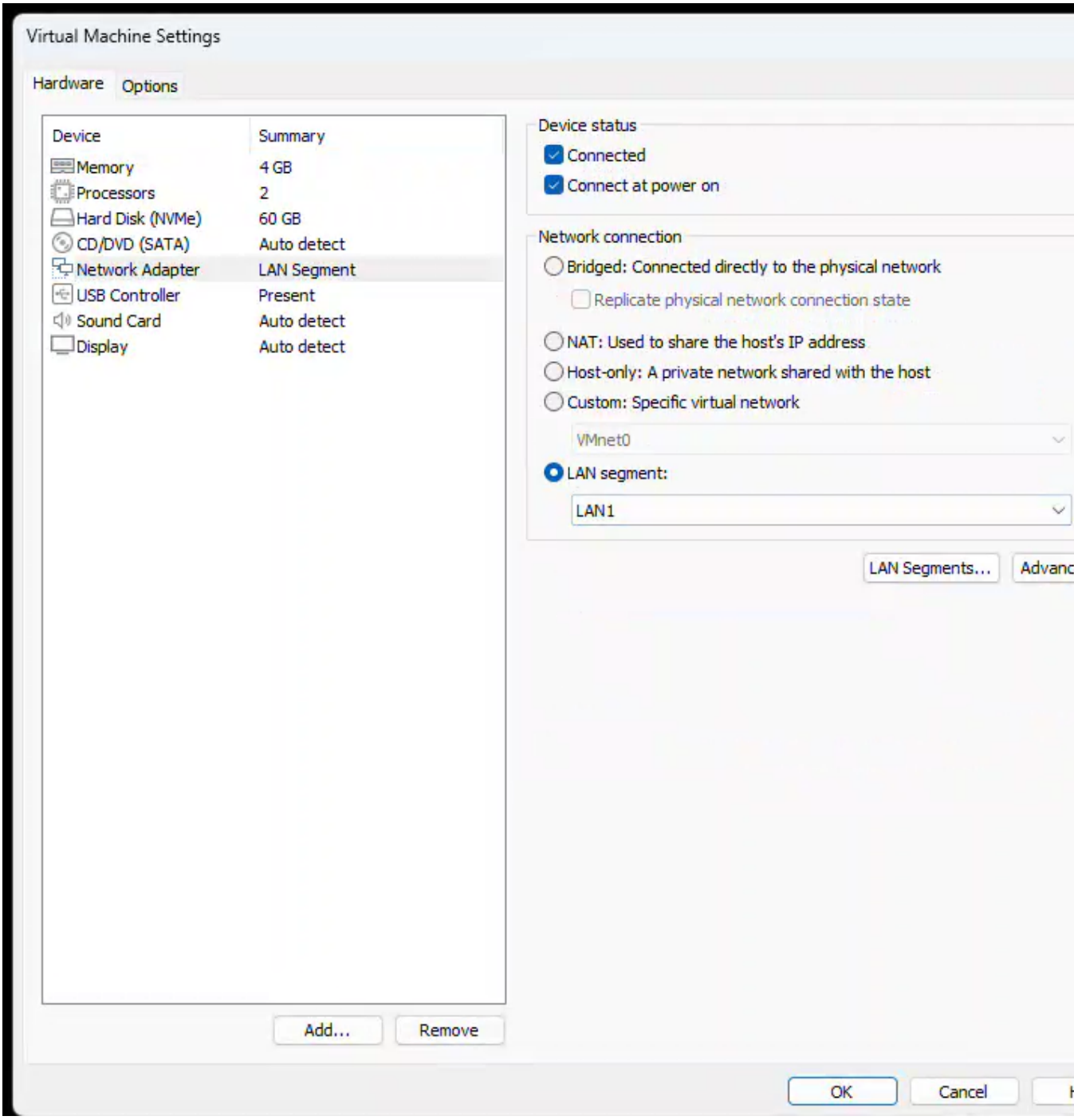
repadmin /istg* /verbose

```
PS C:\Users\Administrator> repadmin /istg * /verbose

Repadmin: running command /istg against full DC DC101.vlabs1.com
Gathering topology from site Montreal (DC101.vlabs1.com):
                  Site                  ISTG
      ================   ================
 Default-First-Site-Name              DC101
               Montreal               DC101
               New-York               DC401

Repadmin: running command /istg against read-only DC DC201.vlabs1.com
Gathering topology from site Toronto (DC201.vlabs1.com):
                  Site                  ISTG
      ================   ================
 Default-First-Site-Name              DC101
               Montreal               DC101
               New-York               DC401

Repadmin: running command /istg against full DC DC301.lab1.vlabs1.com
Gathering topology from site Montreal (DC301.lab1.vlabs1.com):
                  Site                  ISTG
      ================   ================
 Default-First-Site-Name              DC101
               Montreal               DC101
               New-York               DC401

Repadmin: running command /istg against full DC DC401.partner1.vlabs1.com
Gathering topology from site New-York (DC401.partner1.vlabs1.com):
                  Site                  ISTG
      ================   ================
 Default-First-Site-Name              DC101
               Montreal               DC101
               New-York               DC401

PS C:\Users\Administrator>
```

14 Task 12: Managing FSMO role and Global Catalog

1. Reconfigure DC201

- **Login to DC201**
  - Use the **vlabs1\administrator** account.
  - Keep the session open.
- **Modify VM Network Settings**
  - Open the **VM settings** for **DC201.**
  - Change the **LAN segment** to **LAN1.**



- **Update IP Configuration on DC201**

- Go back to the open session on **DC201.**

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

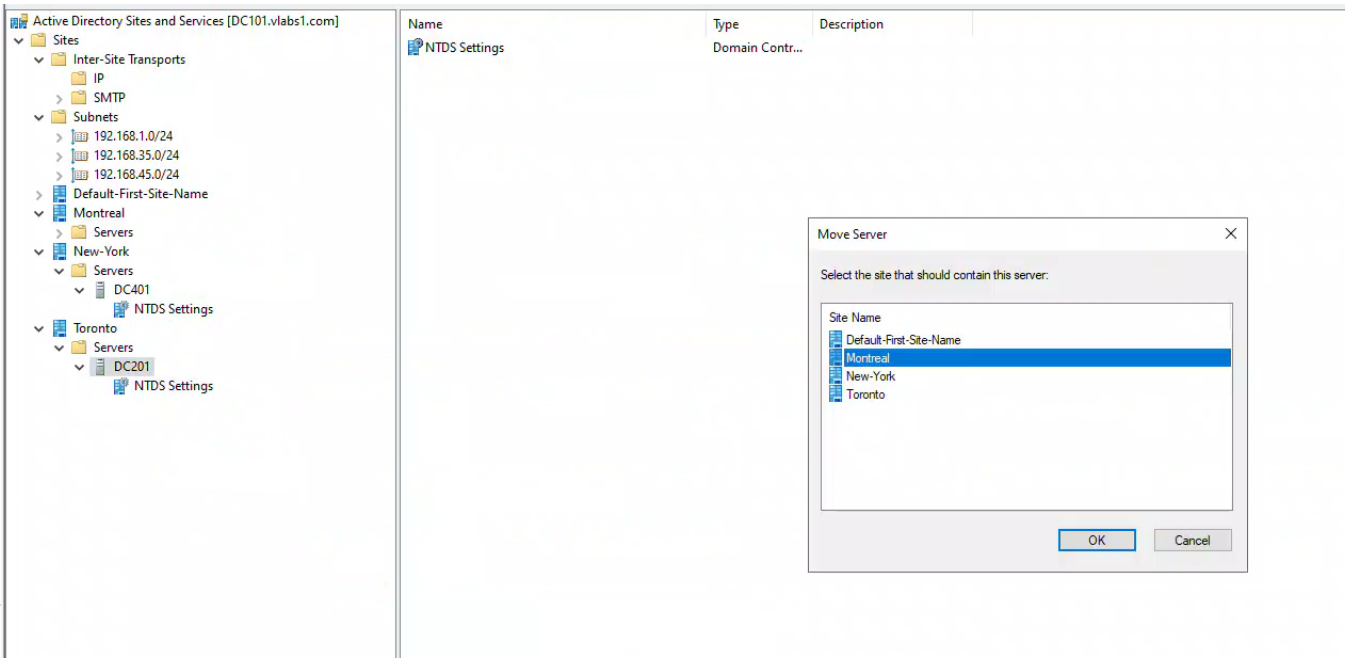
```
PS C:\Users\Administrator.VLABS1>
PS C:\Users\Administrator.VLABS1> netsh interface ip set address name="Ethernet0" static 192.168.1.2 255.255.255.0 192.168.1.50

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

```
PS C:\Users\Administrator.WIN-ICKPP93UL3C>
PS C:\Users\Administrator.WIN-ICKPP93UL3C>
PS C:\Users\Administrator.WIN-ICKPP93UL3C> Get-NetIPAddress | Where-Object {$_.InterfaceAlias -eq "Ethernet0" -and $_.AddressFamily -eq "


IPAddress         : 192.168.1.2
InterfaceIndex    : 5
InterfaceAlias    : Ethernet0
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Preferred
ValidLifetime     :
PreferredLifetime :
SkipAsSource      : False
PolicyStore       : ActiveStore


PS C:\Users\Administrator.WIN-ICKPP93UL3C>
```

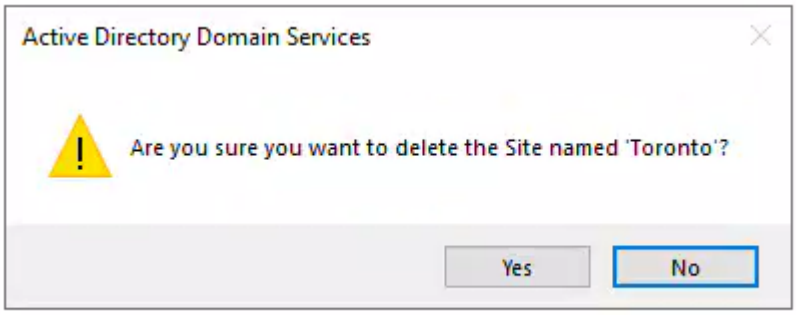
- **Test Network and DNS**
  - **ping 192.168.1.1**
  - **nslookup vlabs1.com**

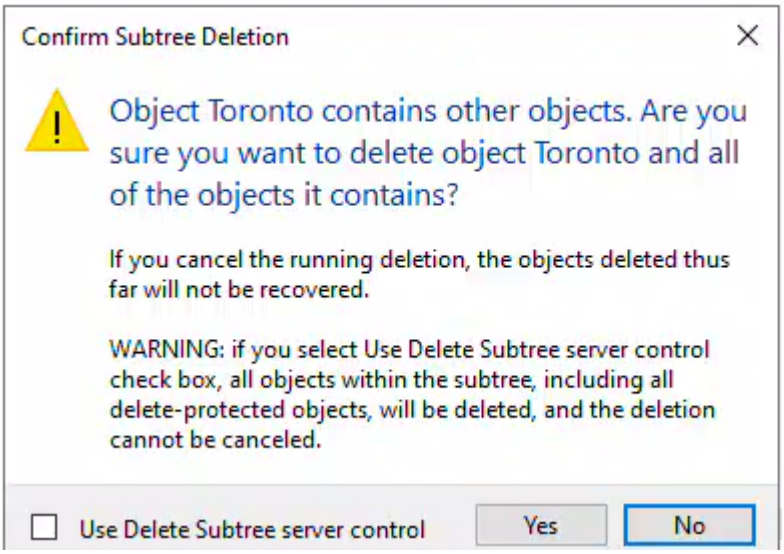
```
PS C:\Users\Administrator.VLABS1>
PS C:\Users\Administrator.VLABS1> ping 192.168.1.1

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
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator.VLABS1> nslookup vlabs1.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  ::1

Name:    vlabs1.com
Address:  192.168.1.1

PS C:\Users\Administrator.VLABS1> nslookup vlabs1.com
Server:  UnKnown
Address:  ::1

Name:    vlabs1.com
Address:  192.168.1.1

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

- **Reconfigure Active Directory Sites on DC101**
  - Log in to **DC101.**
  - Open **Active Directory Sites and Services.**
  - Move **DC201** from the **Toronto** site to the **Montreal** site.

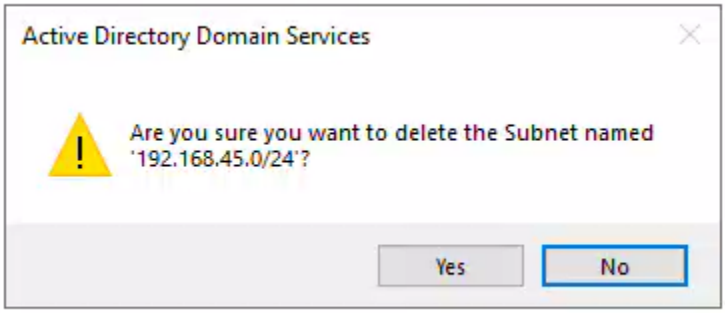


- Delete the **Toronto site.**





- Delete the **subnet 192.168.45.0/24.**



5. Promote a Writable Domain Controller (Replica) – First try fails

- **Promote a member server to become a writable domain controller for an existing domain (vlabs1.com) in the Montreal site.**

  Install-ADDSDomainController `

  -DomainName "vlabs1.com" `

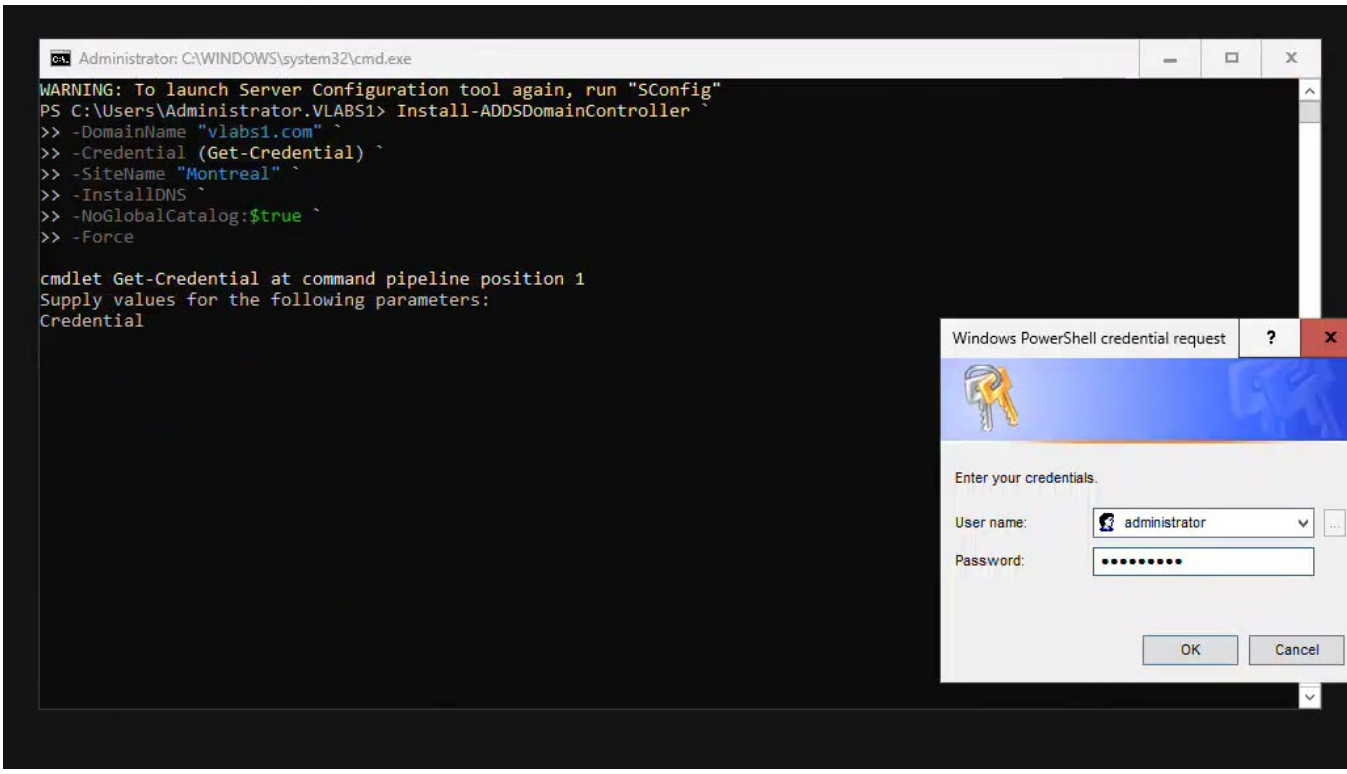
  -Credential (Get-Credential) `

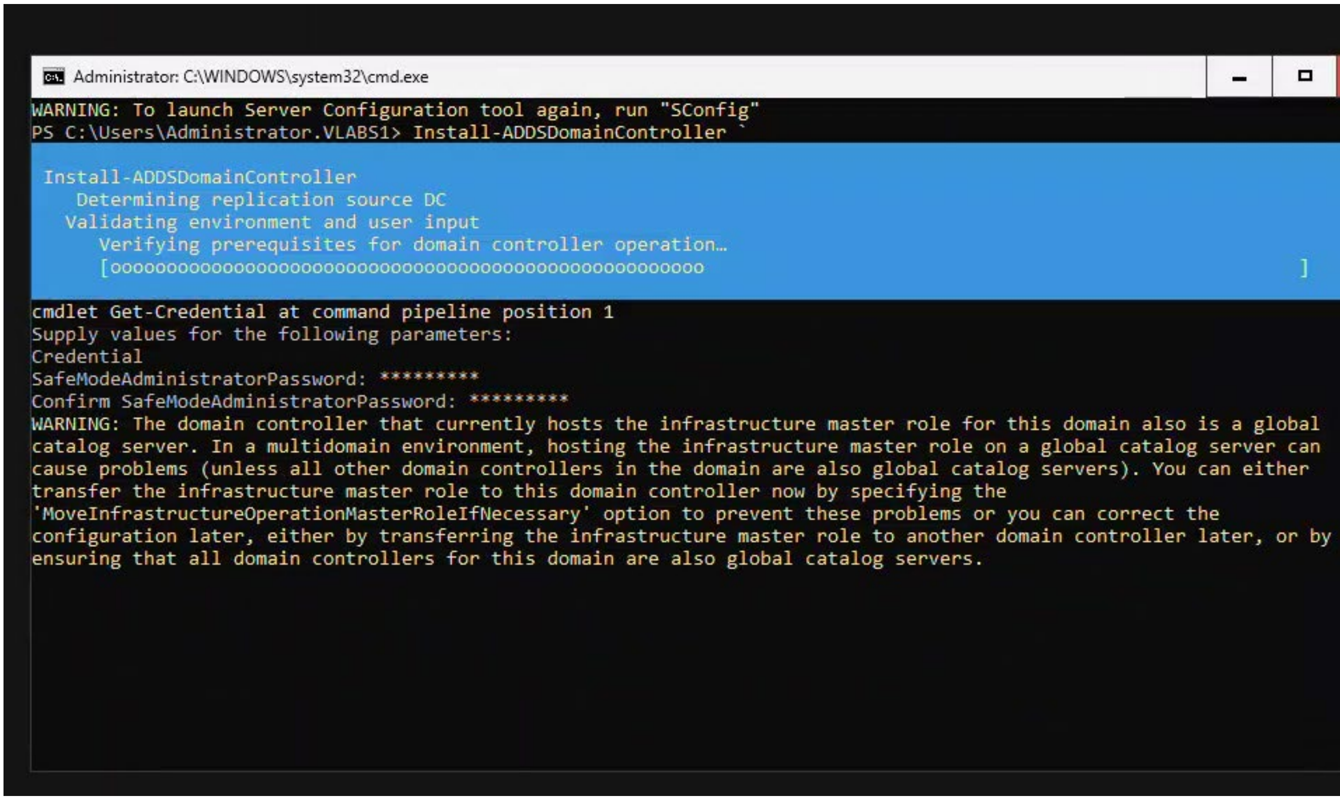
  -SiteName "Montreal" `

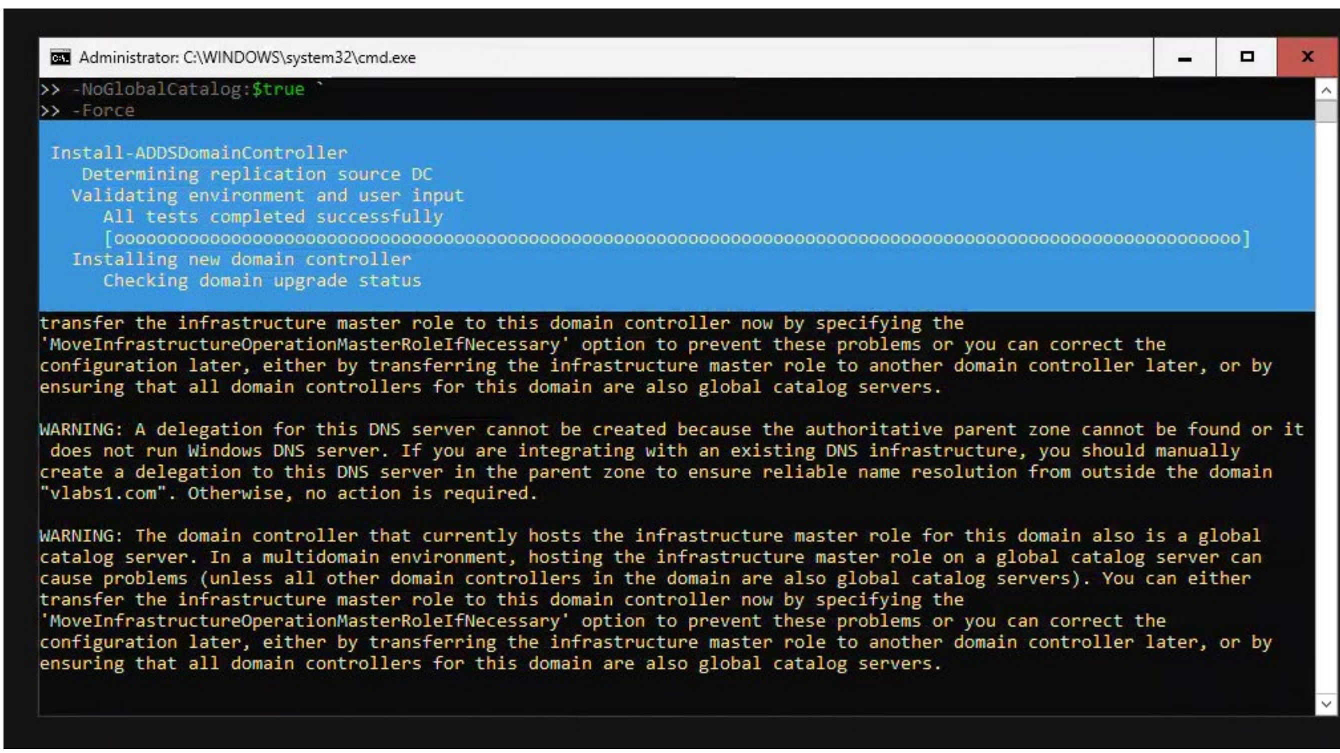
  -InstallDNS `

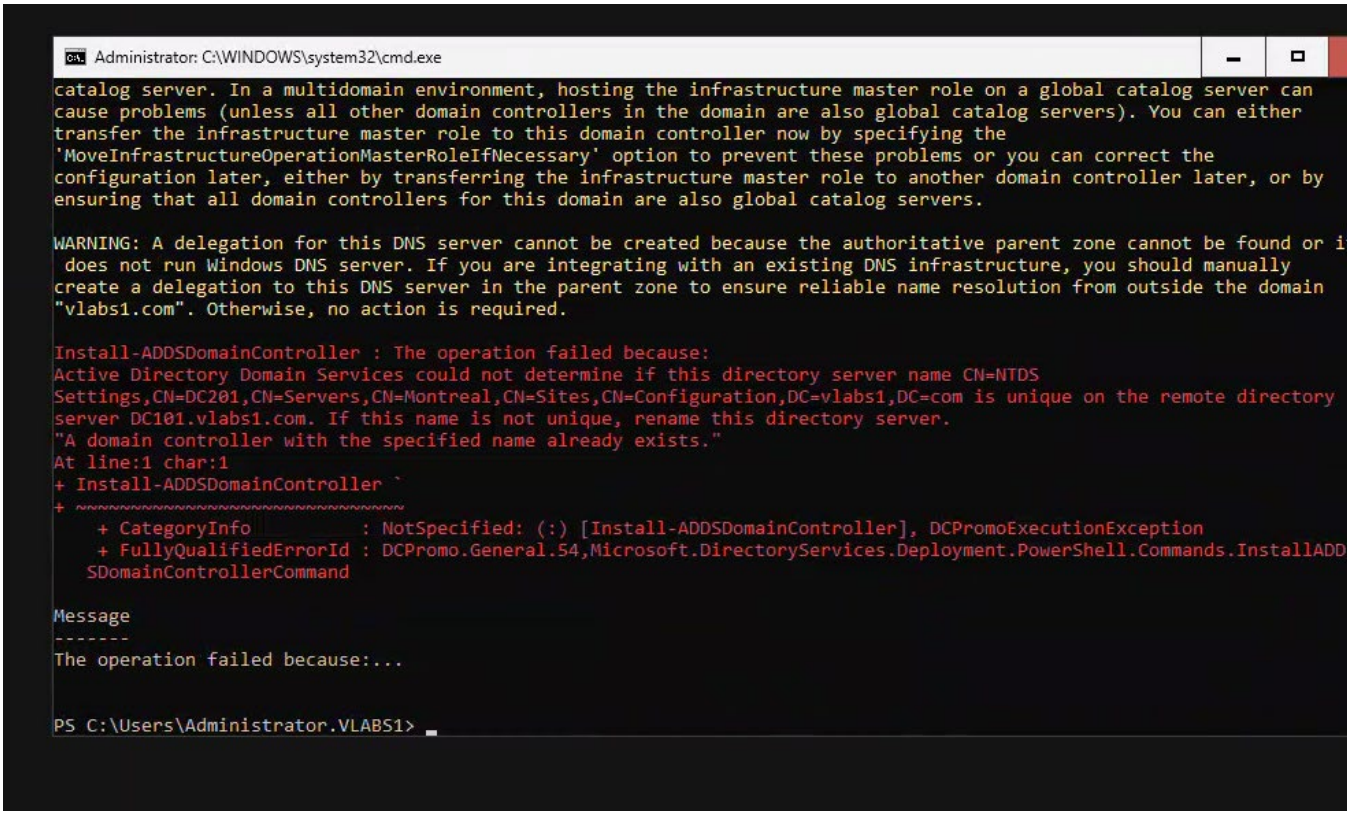
  -NoGlobalCatalog:$true `

  -Force



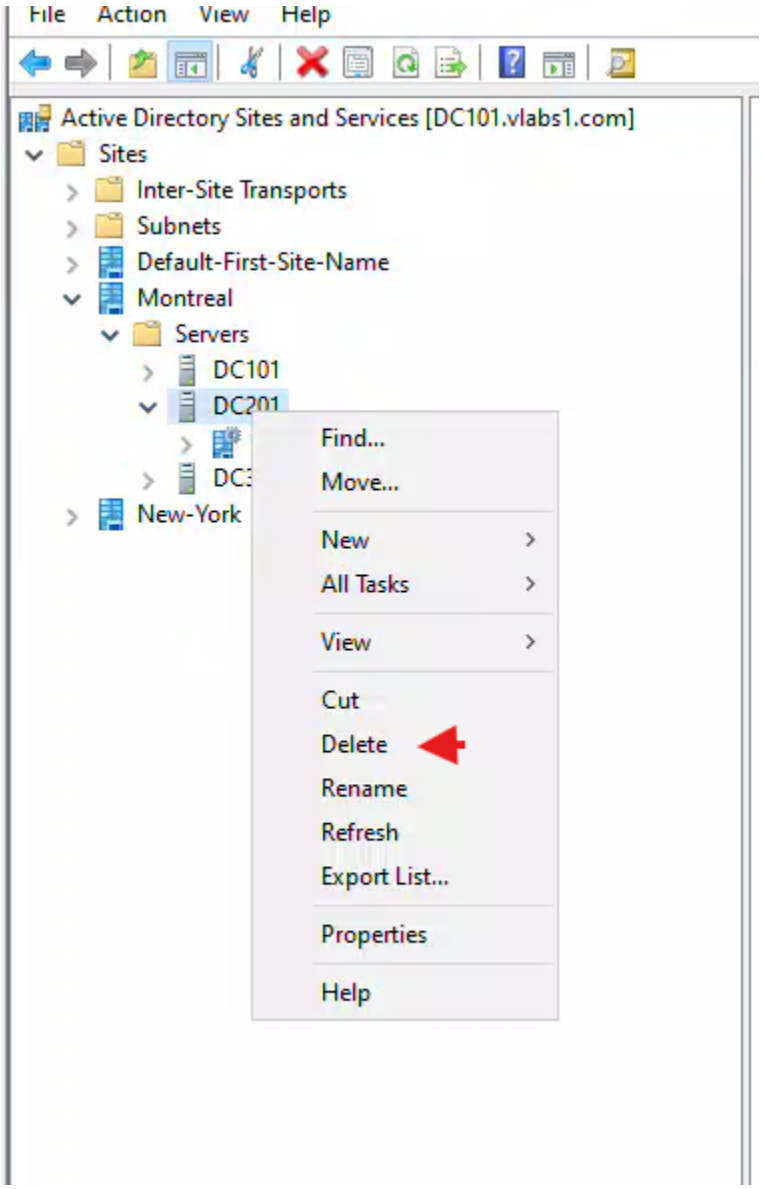

Administrator: C:\WINDOWS\system32\cmd.exe
WARNING: To launch Server Configuration tool again, run "SConfig"
PS C:\Users\Administrator.VLABS1> Install-ADDSDomainController `
Install-ADDSDomainController
Determining replication source DC
Validating environment and user input
Verifying prerequisites for domain controller operation…
[oooooooooooooooooooooooooooooooooooooooooooooooooooooo]
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
SafeModeAdministratorPassword: *********
Confirm SafeModeAdministratorPassword: *********
WARNING: The domain controller that currently hosts the infrastructure master role for this domain also is a global catalog server. In a multidomain environment, hosting the infrastructure master role on a global catalog server can cause problems (unless all other domain controllers in the domain are also global catalog servers). You can either transfer the infrastructure master role to this domain controller now by specifying the 'MoveInfrastructureOperationMasterRoleIfNecessary' option to prevent these problems or you can correct the configuration later, either by transferring the infrastructure master role to another domain controller later, or by ensuring that all domain controllers for this domain are also global catalog servers.

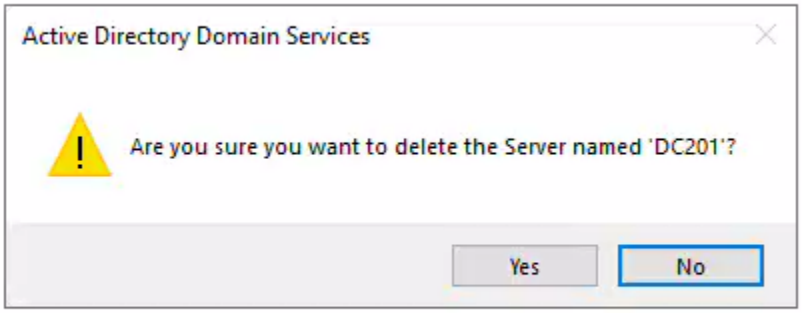

Administrator: C:\WINDOWS\system32\cmd.exe
>> -NoGlobalCatalog:$true `
>> -Force
Install-ADDSDomainController
Determining replication source DC
Validating environment and user input
All tests completed successfully
[oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo]
Installing new domain controller
Checking domain upgrade status
transfer the infrastructure master role to this domain controller now by specifying the 'MoveInfrastructureOperationMasterRoleIfNecessary' option to prevent these problems or you can correct the configuration later, either by transferring the infrastructure master role to another domain controller later, or by ensuring that all domain controllers for this domain are also global catalog servers.
WARNING: A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "vlabs1.com". Otherwise, no action is required.
WARNING: The domain controller that currently hosts the infrastructure master role for this domain also is a global catalog server. In a multidomain environment, hosting the infrastructure master role on a global catalog server can cause problems (unless all other domain controllers in the domain are also global catalog servers). You can either transfer the infrastructure master role to this domain controller now by specifying the 'MoveInfrastructureOperationMasterRoleIfNecessary' option to prevent these problems or you can correct the configuration later, either by transferring the infrastructure master role to another domain controller later, or by ensuring that all domain controllers for this domain are also global catalog servers.

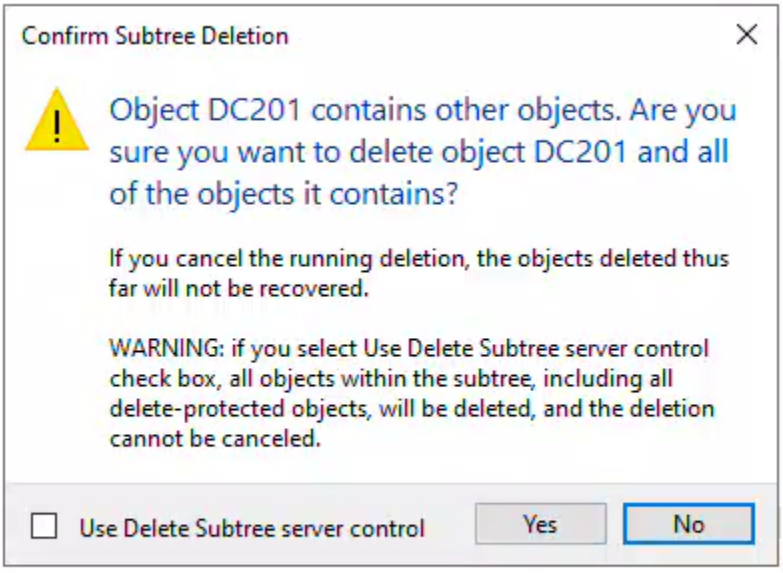

Administrator: C:\WINDOWS\system32\cmd.exe
catalog server. In a multidomain environment, hosting the infrastructure master role on a global catalog server can cause problems (unless all other domain controllers in the domain are also global catalog servers). You can either transfer the infrastructure master role to this domain controller now by specifying the 'MoveInfrastructureOperationMasterRoleIfNecessary' option to prevent these problems or you can correct the configuration later, either by transferring the infrastructure master role to another domain controller later, or by ensuring that all domain controllers for this domain are also global catalog servers.
WARNING: A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or i does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "vlabs1.com". Otherwise, no action is required.
Install-ADDSDomainController : The operation failed because:
Active Directory Domain Services could not determine if this directory server name CN=NTDS Settings,CN=DC201,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com is unique on the remote directory server DC101.vlabs1.com. If this name is not unique, rename this directory server.
"A domain controller with the specified name already exists."
At line:1 char:1
+ Install-ADDSDomainController `
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : NotSpecified: (:) [Install-ADDSDomainController], DCPromoExecutionException
+ FullyQualifiedErrorId : DCPromo.General.54,Microsoft.DirectoryServices.Deployment.PowerShell.Commands.InstallADDSDomainControllerCommand
Message

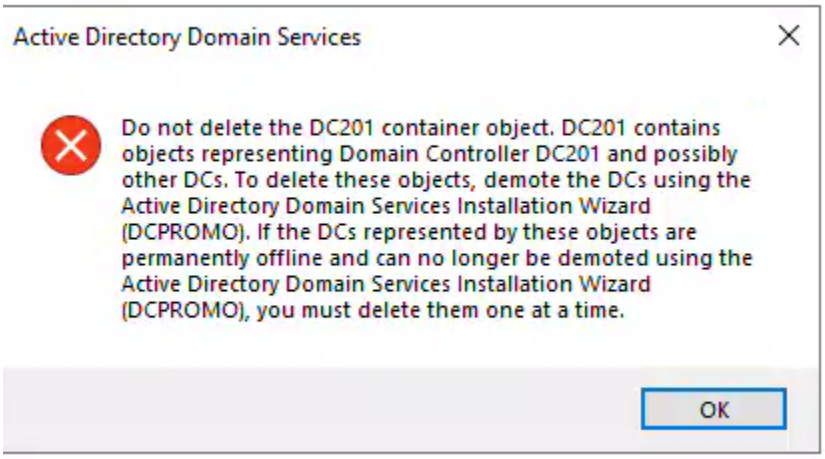
The operation failed because:...
PS C:\Users\Administrator.VLABS1>

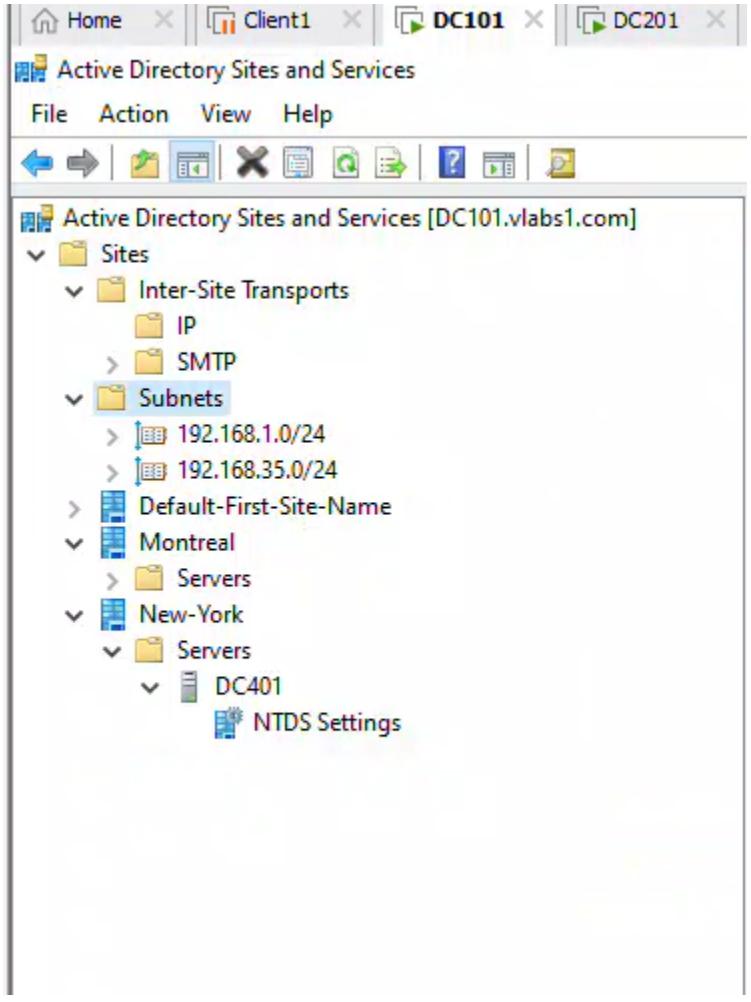
Delete


File
Action
View
Help
Active Directory Sites and Services [DC101.vlabs1.com]
Sites
Inter-Site Transports
Subnets
Default-First-Site-Name
Montreal
Servers
DC101
DC201
New-York
Find...
Move...
New
All Tasks
View
Cut
Delete
Rename
Refresh
Export List...
Properties
Help


Active Directory Domain Services
Are you sure you want to delete the Server named 'DC201'?
Yes
No


Confirm Subtree Deletion
Object DC201 contains other objects. Are you sure you want to delete object DC201 and all of the objects it contains?
If you cancel the running deletion, the objects deleted thus far will not be recovered.
WARNING: if you select Use Delete Subtree server control check box, all objects within the subtree, including all delete-protected objects, will be deleted, and the deletion cannot be canceled.
Use Delete Subtree server control
Yes
No



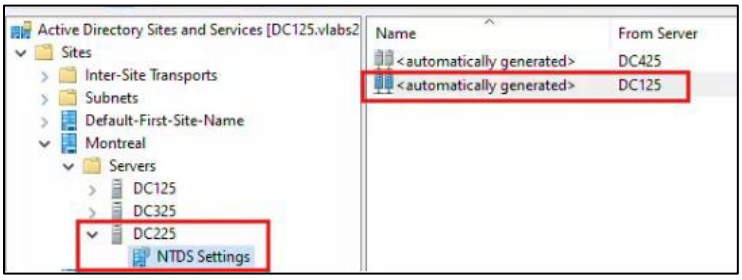


Force Replication from DC101

- **Locate the NTDS connection between DC101 and DC201.**
- **Right-click the connection object and select Replicate now.**

6. Demote the Domain Controller (RODC)

- Return to **DC201**.
- Safely remove a domain controller (typically an RODC) from the domain and return it to a standalone server.



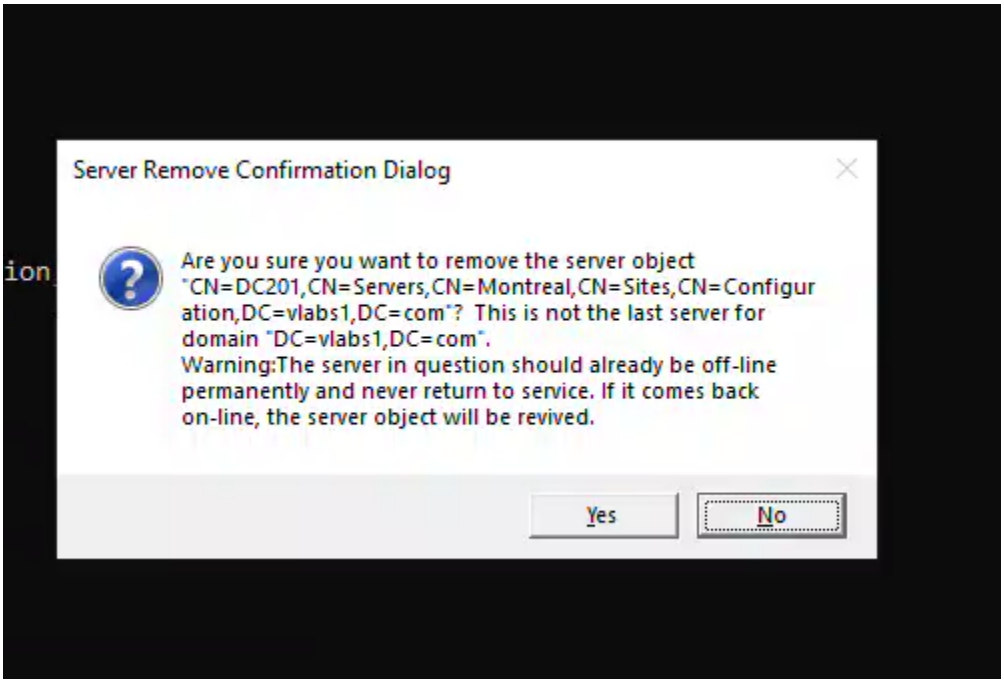

```
Uninstall-ADDSDomainController `
 -LocalAdministratorPassword (Read-Host -Prompt "Enter local admin password" -
AsSecureString) `
 -Force
```

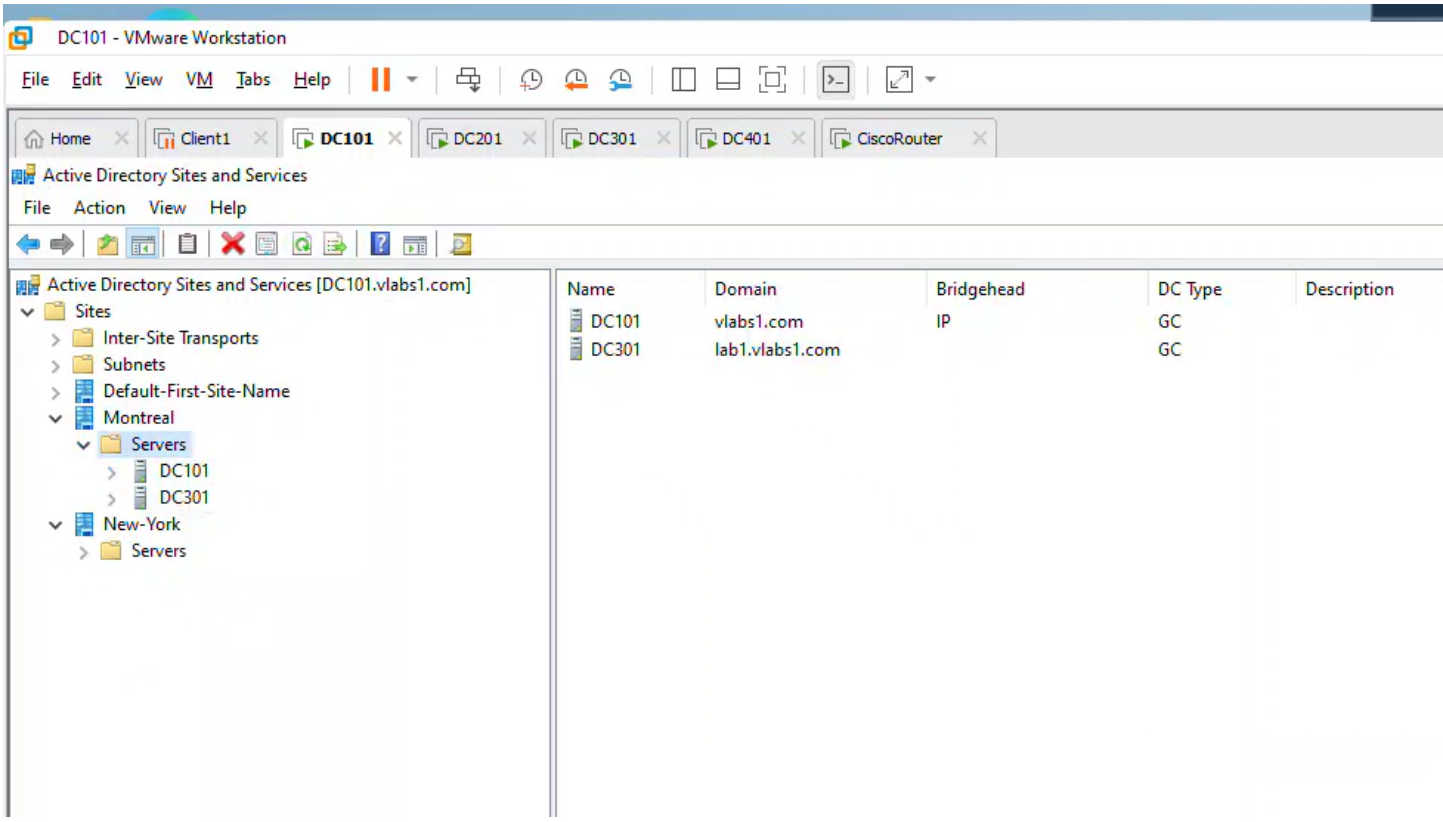
Need to unistall using ntdsutil

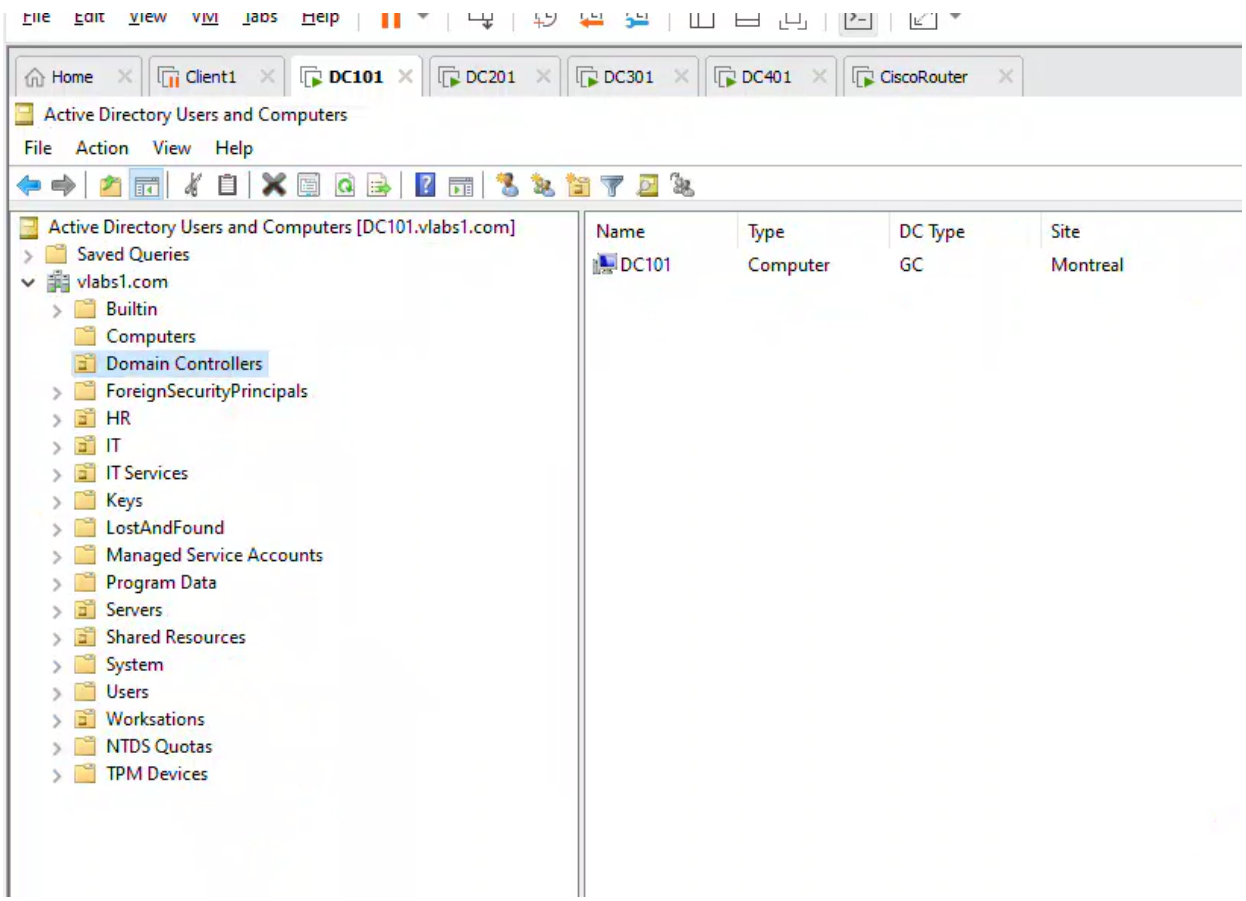
```
PS C:\Users\Administrator> ntdsutil
C:\Windows\system32\ntdsutil.exe: metadata cleanup
metadata cleanup: connections
server connections: connect to server DC101
Binding to DC101 ...
Connected to DC101 using credentials of locally logged on user.
server connections: quit
metadata cleanup: select operation target
select operation target: list domains
Found 3 domain(s)
0 - DC=vlabs1,DC=com
1 - DC=lab1,DC=vlabs1,DC=com
2 - DC=partner1,DC=vlabs1,DC=com
select operation target: select domain <vlabs1.com domain number>
Error parsing Input - Invalid Syntax.
select operation target: select domain vlabs.com DC201
Error parsing Input - Invalid Syntax.
select operation target: select domain vlabs.com 201
Error parsing Input - Invalid Syntax.
select operation target: select domain 0
No current site
```

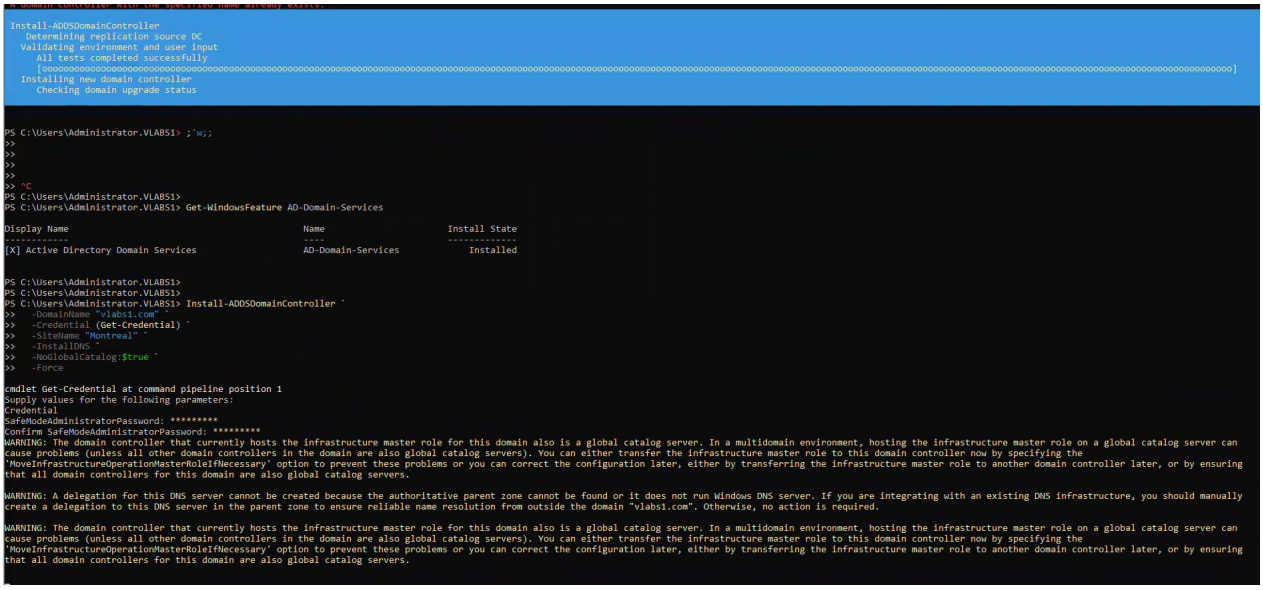
```
Domain - DC=vlabs1,DC=com
No current server
No current Naming Context
select operation target: list sites
Found 3 site(s)
0 - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
1 - CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
2 - CN=New-York,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
select operation target: 1
Error parsing Input - Invalid Syntax.
select operation target: CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
Error parsing Input - Invalid Syntax.
select operation target: list sites
Found 3 site(s)
0 - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
1 - CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
2 - CN=New-York,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
select operation target: select site 1
Site - CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
Domain - DC=vlabs1,DC=com
No current server
No current Naming Context
select operation target: list servers in site
Found 3 server(s)
0 - CN=DC101,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
1 - CN=DC301,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
2 - CN=DC201,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
select operation target: select server 2
Site - CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
Domain - DC=vlabs1,DC=com
Server - CN=DC201,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
        DSA object - CN=NTDS
Settings,CN=DC201,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
        DNS host name - DC201.vlabs1.com
        Computer object - CN=DC201,OU=Worksations,DC=vlabs1,DC=com
No current Naming Context
select operation target: remove selected server
Error parsing Input - Invalid Syntax.
select operation target: quit
metadata cleanup: remove selected server
Transferring / Seizing FSMO roles off the selected server.
Removing FRS metadata for the selected server.
```

```
Searching for FRS members under "CN=DC201,OU=Worksations,DC=vlabs1,DC=com".

Deleting subtree under "CN=DC201,OU=Worksations,DC=vlabs1,DC=com".

The attempt to remove the FRS settings on
CN=DC201,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com failed because "Element
not found.";

metadata cleanup is continuing.

"CN=DC201,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com" removed from server
"DC101"

metadata cleanup:
```

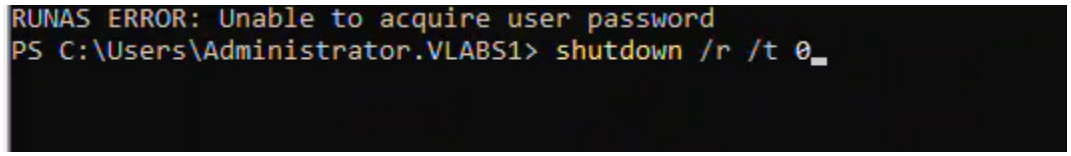


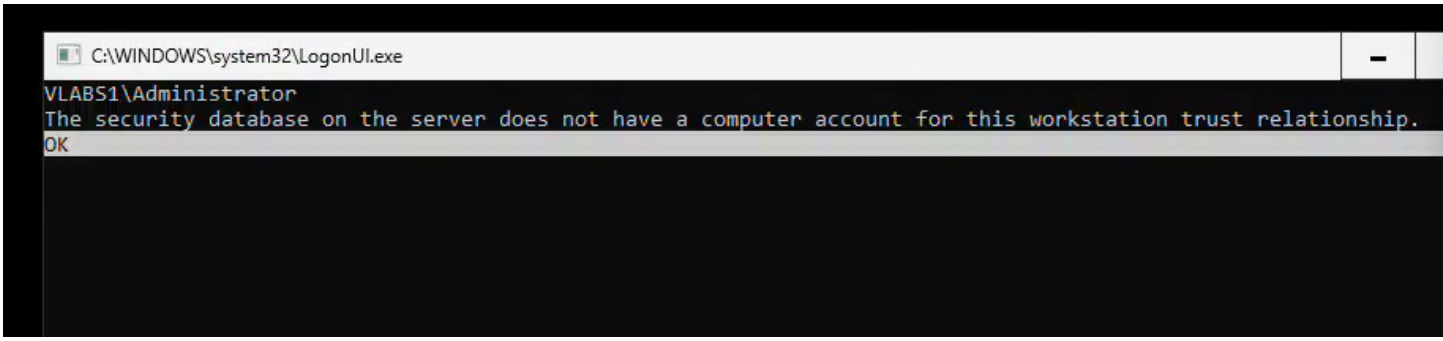

DC101 - VMware Workstation
File Edit View VM Tabs Help
Home
Client1
DC101
DC201
DC301
DC401
CiscoRouter
Active Directory Sites and Services
File Action View Help
Active Directory Sites and Services [DC101.vlabs1.com]
Sites
Inter-Site Transports
Subnets
Default-First-Site-Name
Montreal
Servers
DC101
DC301
New-York
Servers
Name
Domain
Bridgehead
DC Type
Description
DC101
vlabs1.com
IP
GC
DC301
lab1.vlabs1.com
GC


Home
Client1
DC101
DC201
DC301
DC401
CiscoRouter
Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [DC101.vlabs1.com]
Saved Queries
vlabs1.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
HR
IT
IT Services
Keys
LostAndFound
Managed Service Accounts
Program Data
Servers
Shared Resources
System
Users
Worksations
NTDS Quotas
TPM Devices
Name
Type
DC Type
Site
DC101
Computer
GC
Montreal

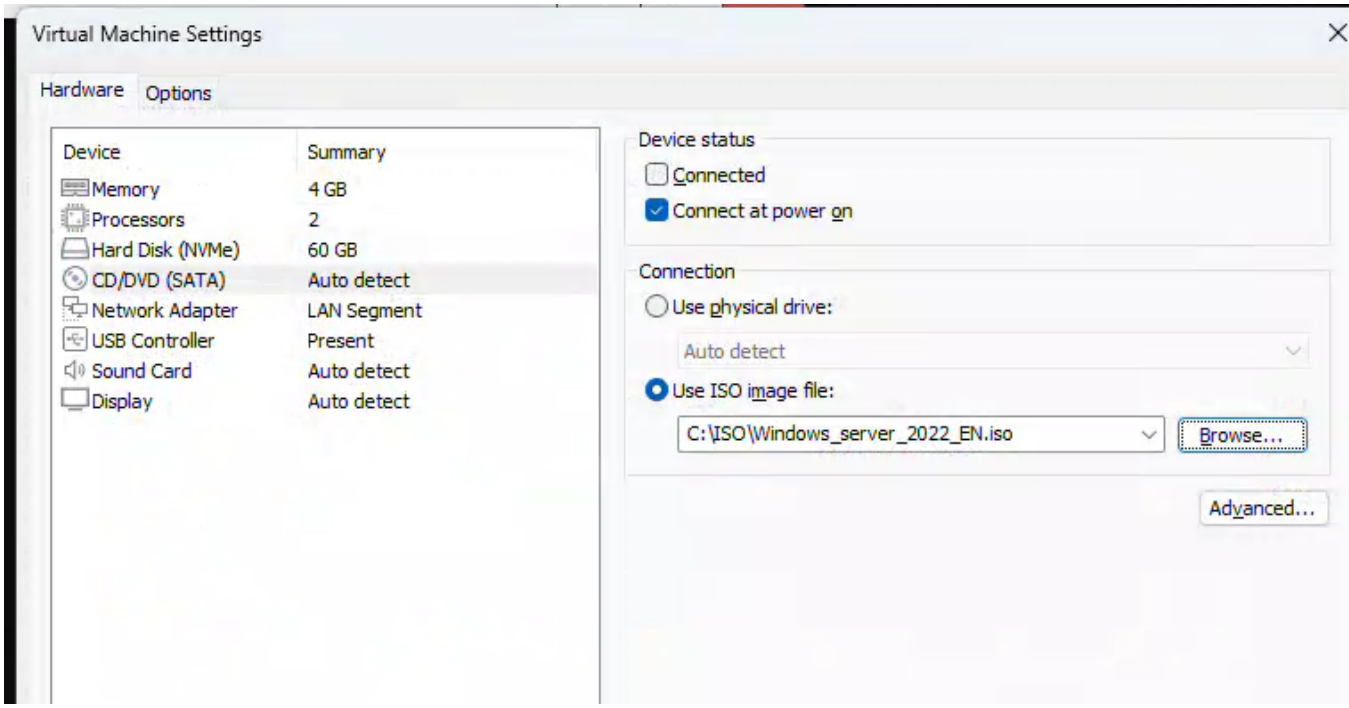


shutdown /r /t 0

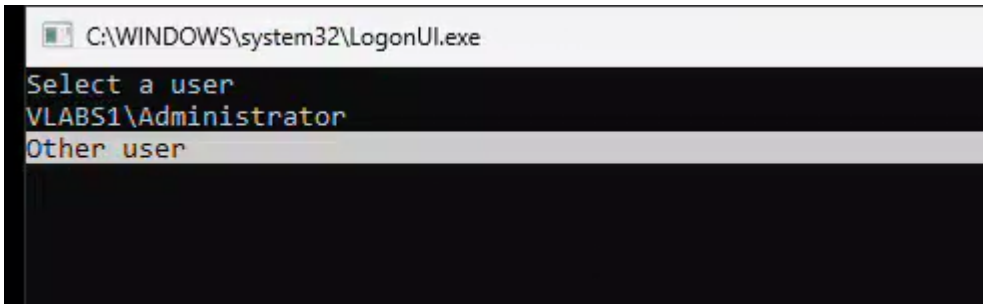




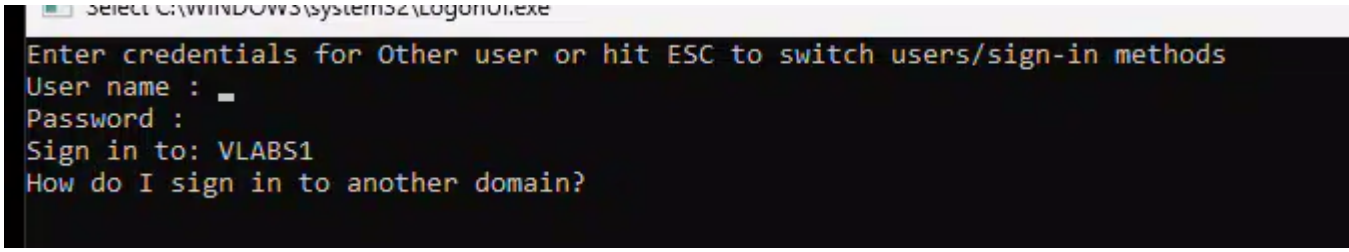
Need to restart in bootable mode

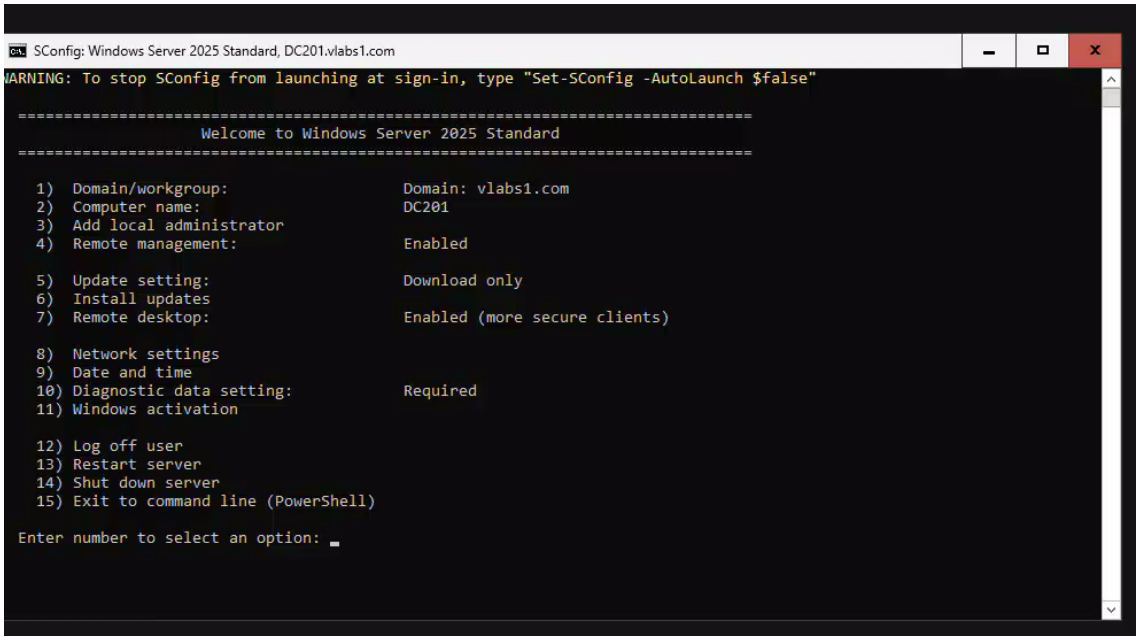


Other user

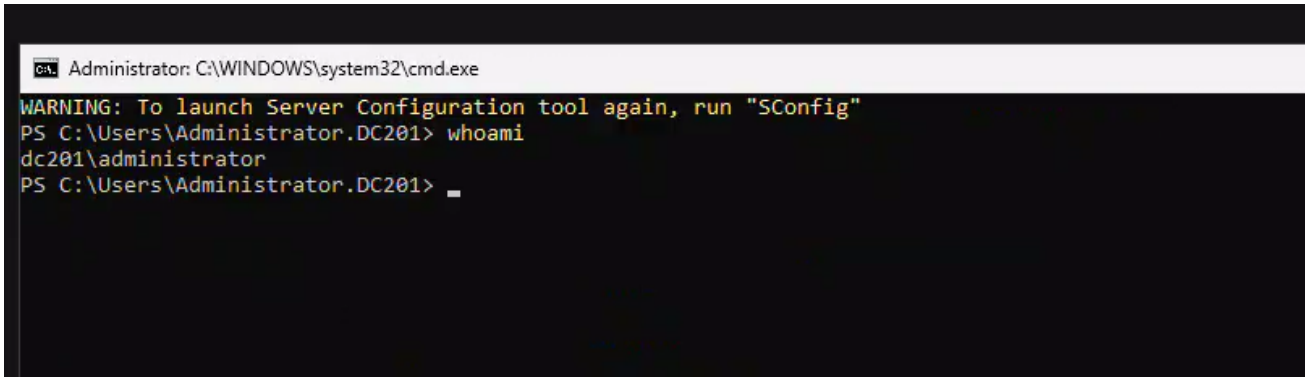


Select DC201\Administrator



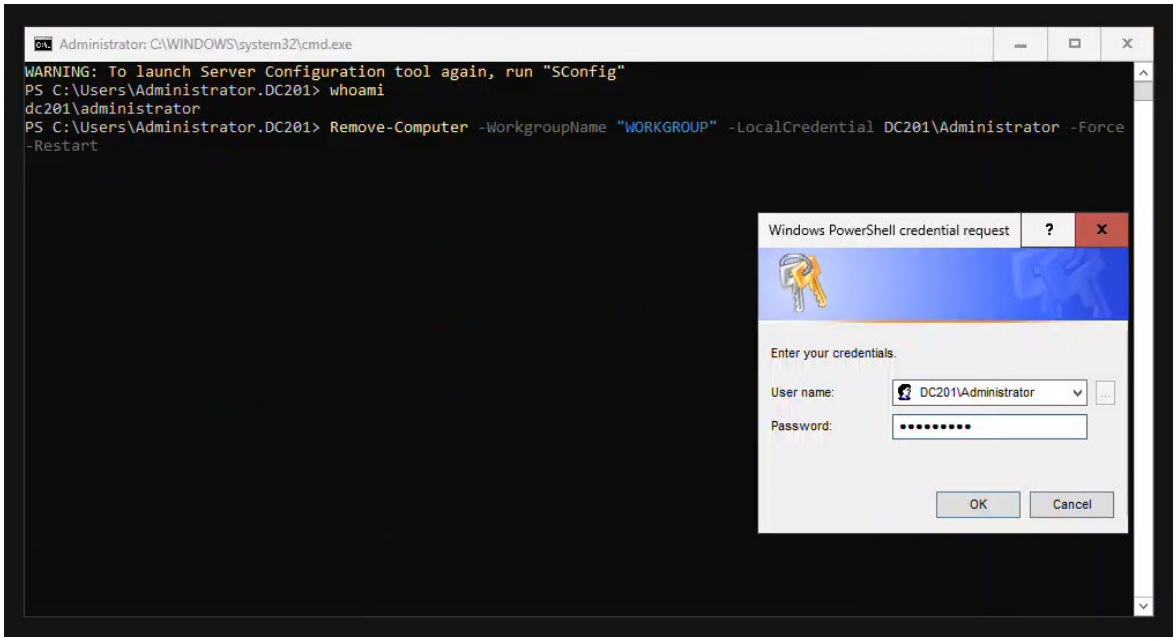


Now as local user



Remove from domain join to WORKGROUP

Remove-Computer -WorkgroupName "WORKGROUP" -LocalCredential DC201\Administrator -Force -Restart



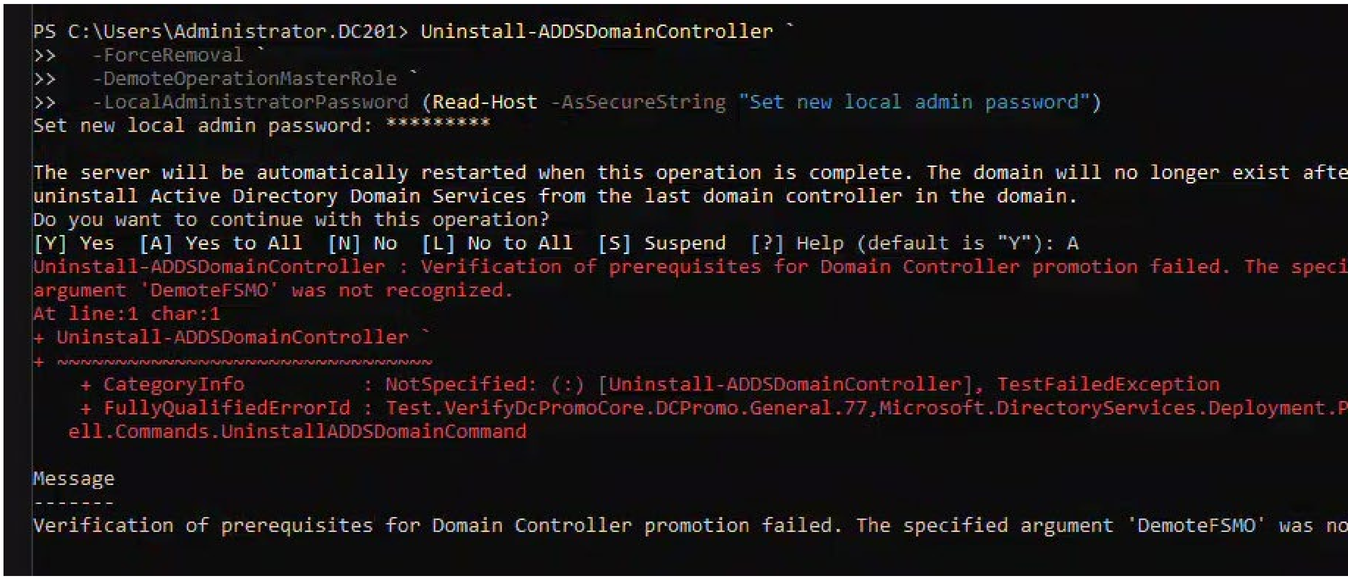
It does not work since the password is not known

Confirm DC201 is NOT a Domain Controller

```
PS C:\Users\Administrator.DC201> # Confirm DC201 is NOT a Domain Controller
PS C:\Users\Administrator.DC201> Get-WindowsFeature AD-Domain-Services

Display Name                                            Name                    Install State
------------                                            ----                    -------------
[X] Active Directory Domain Services                    AD-Domain-Services          Installed


PS C:\Users\Administrator.DC201>
```

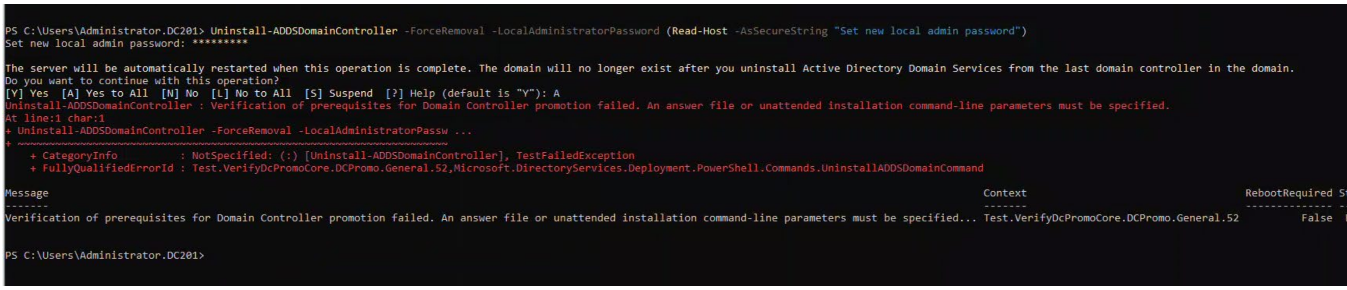
Force Demote the Domain Controller (DC201)

It does not work



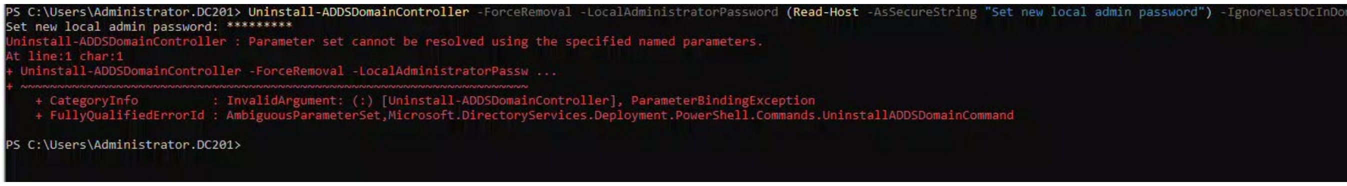
Change command

Uninstall-ADDSDomainController -ForceRemoval -LocalAdministratorPassword (Read-Host -AsSecureString "Set new local admin password")



Change command again

Uninstall-ADDSDomainController -ForceRemoval -LocalAdministratorPassword (Read-Host -AsSecureString "Set new local admin password") -IgnoreLastDcInDomainMismatch



Create an unsatended file

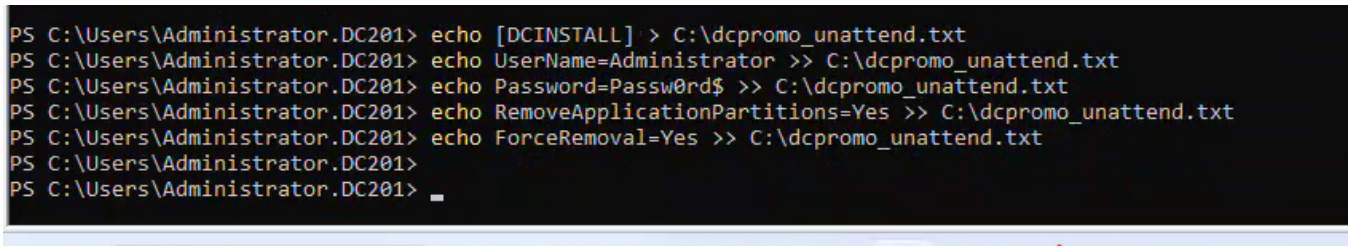
echo [DCINSTALL] > C:\dcpromo_unattend.txt

echo UserName=Administrator >> C:\dcpromo_unattend.txt

echo Password=Passw0rd$ >> C:\dcpromo_unattend.txt

echo RemoveApplicationPartitions=Yes >> C:\dcpromo_unattend.txt

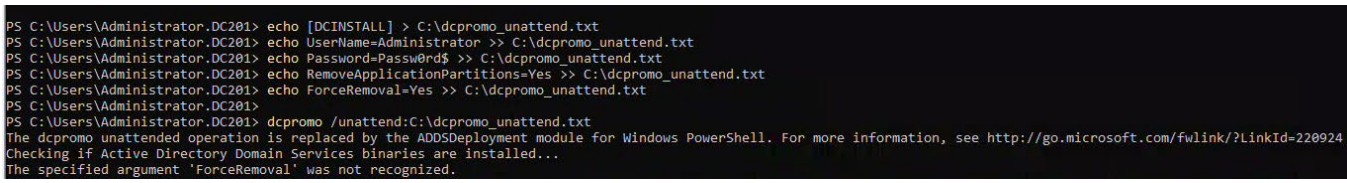
echo ForceRemoval=Yes >> C:\dcpromo_unattend.txt



Run the file

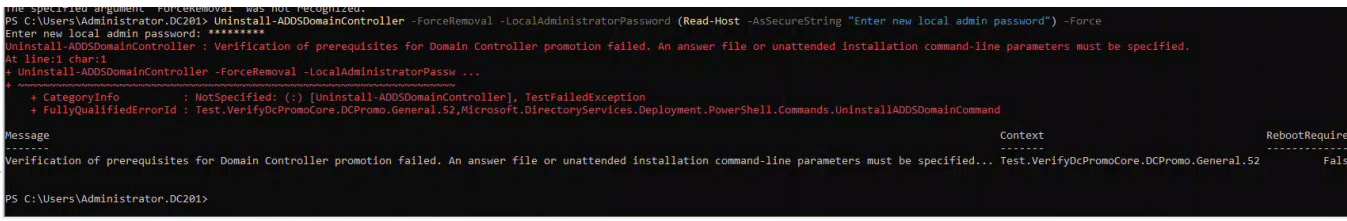
dcpromo /unattend:C:\dcpromo_unattend.txt

it did not worked



Change command again

Uninstall-ADDSDomainController -ForceRemoval -LocalAdministratorPassword (Read-Host -AsSecureString "Enter new local admin password") -Force



Cannot uninstall will now demote with unattended file

echo "[DCInstall]

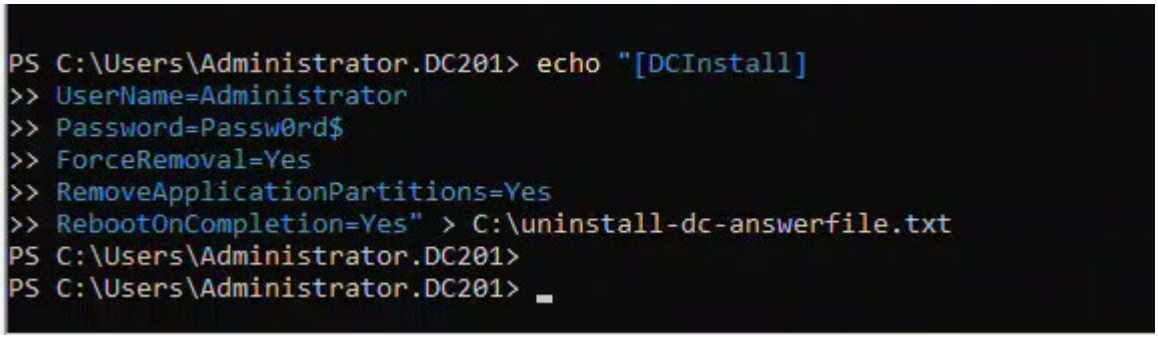
UserName=Administrator

Password=Passw0rd$

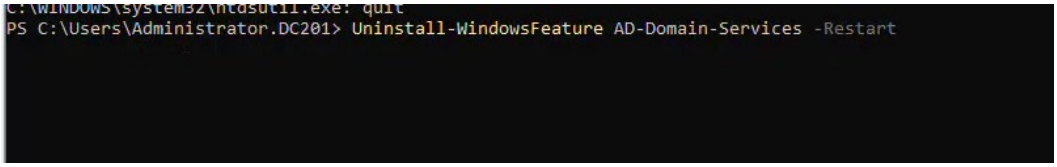
ForceRemoval=Yes

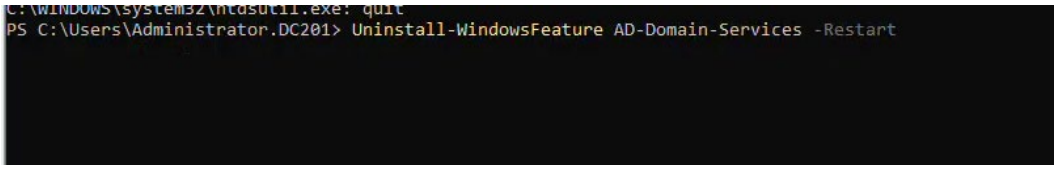
RemoveApplicationPartitions=Yes

RebootOnCompletion=Yes" > C:\uninstall-dc-answerfile.txt

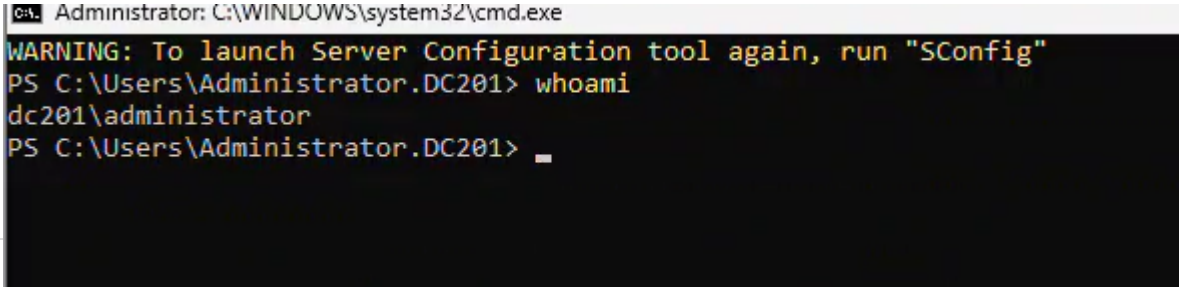


Finally unistall



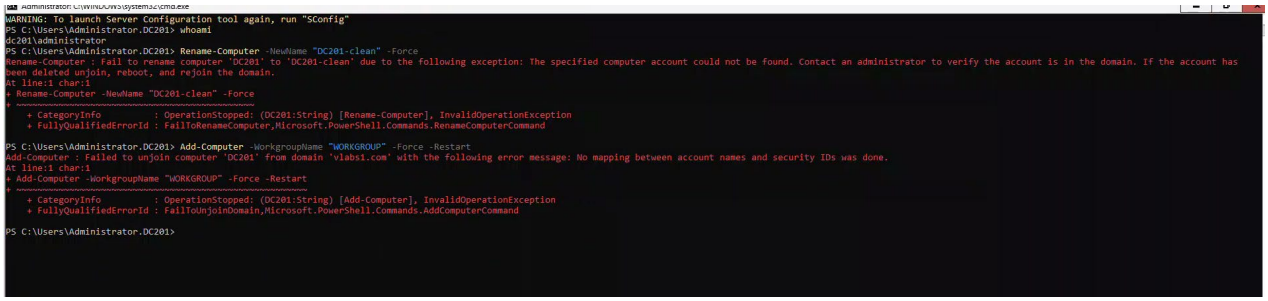


Rename Computer / Join Workgroup (After Reboot)
Once the server reboots:



Rename-Computer -NewName "DC201-clean" -Force
Add-Computer -WorkgroupName "WORKGROUP" -Force -Restart

Command gives errors



Still half-demoted state: the server is not a functioning Domain Controller, but it's still joined to the domain and can't cleanly unjoin due to broken trust and missing security identifiers (SIDs). This is common when AD DS is force-removed or corrupted

Leave the Domain by Forcing Registry Change
⚠️ This is not officially supported by Microsoft but works in lab/testing environments when standard tools fail.

Run the following in PowerShell to force the system into Workgroup mode:

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" -Name Domain -Value ""
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName" -Name ComputerName -Value "DC201-clean"
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName" -Name ComputerName -Value "DC201-clean"
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName" -Name ActiveComputerName -Value "DC201-clean"

# Force into workgroup
```

Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters" -Name Domain -Value "WORKGROUP"

```
PS C:\Users\Administrator.DC201> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" -Name Domain -Value ""
PS C:\Users\Administrator.DC201> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName" -Name ComputerName -Value "DC201-clean"
PS C:\Users\Administrator.DC201> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName" -Name ComputerName -Value "DC201-clean"
PS C:\Users\Administrator.DC201> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName" -Name ActiveComputerName -Value "DC201-clean"
PS C:\Users\Administrator.DC201>
PS C:\Users\Administrator.DC201> # Force into workgroup
PS C:\Users\Administrator.DC201> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters" -Name Domain -Value "WORKGROUP"
PS C:\Users\Administrator.DC201>
```

Restart computer

```
PS C:\Users\Administrator.DC201>
PS C:\Users\Administrator.DC201>
PS C:\Users\Administrator.DC201> Restart-Computer -Force
```

After Reboot, Confirm Workgroup Status

```
================================================================================
                Welcome to Windows Server 2025 Standard
================================================================================

  1)  Domain/workgroup:                 Domain: vlabs1.com
  2)  Computer name:                    DC201-clean
  3)  Add local administrator
  4)  Remote management:                Enabled

  5)  Update setting:                   Download only
  6)  Install updates
  7)  Remote desktop:                   Enabled (more secure clients)

  8)  Network settings
  9)  Date and time
  10) Diagnostic data setting:          Required
  11) Windows activation

  12) Log off user
  13) Restart server
  14) Shut down server
  15) Exit to command line (PowerShell)

Enter number to select an option:
```

Still as local user

```
PS C:\Users\Administrator.DC201> whoami
dc201-clean\administrator
PS C:\Users\Administrator.DC201>
```

Run:

(Get-WmiObject Win32_ComputerSystem).PartOfDomain
(Get-WmiObject Win32_ComputerSystem).Workgroup

It should return: WORKGROUP

Failed

```
PS C:\Users\Administrator.DC201> whoami
dc201-clean\administrator
PS C:\Users\Administrator.DC201> (Get-WmiObject Win32_ComputerSystem).PartOfDomain
True
PS C:\Users\Administrator.DC201> (Get-WmiObject Win32_ComputerSystem).Workgroup
PS C:\Users\Administrator.DC201>
PS C:\Users\Administrator.DC201>
```

This confirms **DC201 is still joined to the domain**, even though it's in a broken state

Set Workgroup and Rename via Registry
Run in PowerShell:

```
# Force rename
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName" -
Name ComputerName -Value "DC201-CLEAN"
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName" -Name
ComputerName -Value "DC201-CLEAN"

# Force workgroup
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters" -Name
Domain -Value "WORKGROUP"
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" -
Name Domain -Value ""
```

```
PS C:\Users\Administrator.DC201>
PS C:\Users\Administrator.DC201> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName" -Name ComputerName -Value "DC201-CLEAN"
PS C:\Users\Administrator.DC201> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName" -Name ComputerName -Value "DC201-CLEAN"
PS C:\Users\Administrator.DC201>
PS C:\Users\Administrator.DC201> # Force workgroup
PS C:\Users\Administrator.DC201> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters" -Name Domain -Value "WORKGROUP"
PS C:\Users\Administrator.DC201> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" -Name Domain -Value ""
PS C:\Users\Administrator.DC201> hostname
DC201
PS C:\Users\Administrator.DC201>
```

You successfully renamed the system to DC201-CLEAN in the registry, but:

⚠️ hostname still reports DC201, because the system hasn't been rebooted yet.

⚠️ You're still seeing (Get-WmiObject Win32_ComputerSystem).PartOfDomain = True, which means the system still thinks it's in the domain, likely due to cached or stuck values in memory or the registry.

Clean Stale Domain Info (again)

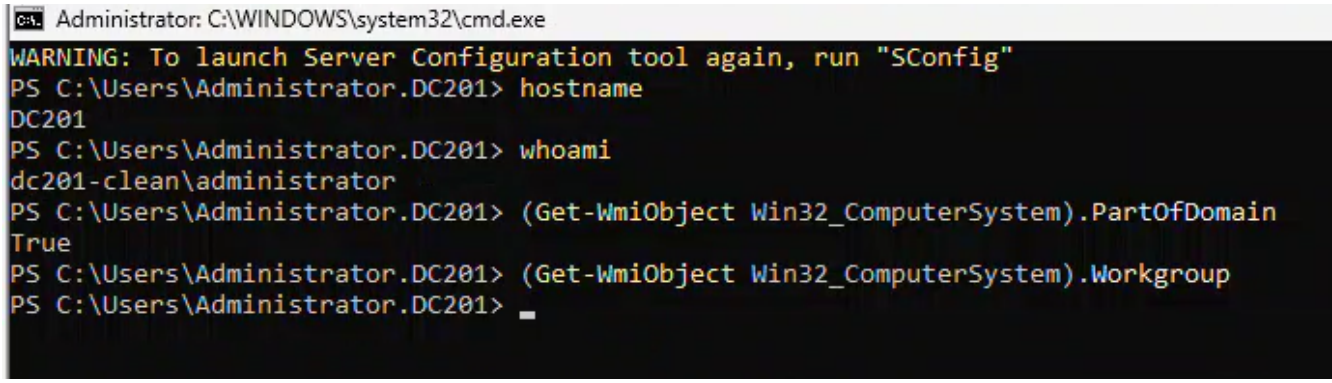
```
Remove-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName" -Name "Domain" -ErrorAction SilentlyContinue
Remove-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName" -Name "Domain" -ErrorAction SilentlyContinue
Remove-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" -Name "NV Domain" -ErrorAction SilentlyContinue
```

```
DC201
PS C:\Users\Administrator.DC201> Remove-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName" -Name "Domain" -ErrorAction SilentlyConti
PS C:\Users\Administrator.DC201> Remove-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName" -Name "Domain" -ErrorAction SilentlyContinue
PS C:\Users\Administrator.DC201> Remove-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" -Name "NV Domain" -ErrorAction SilentlyContinue
PS C:\Users\Administrator.DC201>
```

Reboot machine

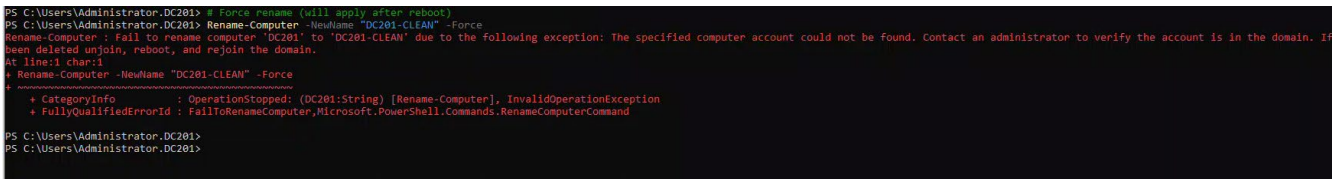
When reboot comes back , Run These to Confirm Clean State:

Still not working
hostname
whoami
(Get-WmiObject Win32_ComputerSystem).PartOfDomain
(Get-WmiObject Win32_ComputerSystem).Workgroup



Force Local SAM Login + Clean Rename
Run the following commands in PowerShell as Administrator:

 # Force rename (will apply after reboot)
Rename-Computer -NewName "DC201-CLEAN" -Force



Force Registry Cleanup of Domain Bindings
Run the following in PowerShell as Administrator:

 # Clear domain info in network settings
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" -Name Domain -Value ""
Remove-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" -Name "NV Domain" -ErrorAction SilentlyContinue

 # Ensure workgroup is set
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName" -Name ComputerName -Value "DC201-CLEAN"
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName" -Name ComputerName -Value "DC201-CLEAN"
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName" -Name "Workgroup" -Value "WORKGROUP"
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName" -Name "Workgroup" -Value "WORKGROUP"

```
PS C:\Users\Administrator.DC201>
PS C:\Users\Administrator.DC201> # Clear domain info in network settings
PS C:\Users\Administrator.DC201> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" -Name Domain -Value ""
PS C:\Users\Administrator.DC201> Remove-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" -Name "NV Domain" -ErrorAction SilentlyContinue
PS C:\Users\Administrator.DC201> # Ensure workgroup is set
PS C:\Users\Administrator.DC201> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName" -Name ComputerName -Value "DC201-CLEAN"
PS C:\Users\Administrator.DC201> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName" -Name ComputerName -Value "DC201-CLEAN"
PS C:\Users\Administrator.DC201> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName" -Name "Workgroup" -Value "WORKGROUP"
PS C:\Users\Administrator.DC201> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName" -Name "Workgroup" -Value "WORKGROUP"
PS C:\Users\Administrator.DC201> Restart-Computer
```

Restart computer

Check if changes took effect

```
Administrator: C:\WINDOWS\system32\cmd.exe
WARNING: To launch Server Configuration tool again, run "SConfig"
PS C:\Users\Administrator.DC201> whoami
dc201-clean\administrator
PS C:\Users\Administrator.DC201> hostname
DC201
PS C:\Users\Administrator.DC201> (Get-WmiObject Win32_ComputerSystem).PartOfDomain
True
PS C:\Users\Administrator.DC201> (Get-WmiObject Win32_ComputerSystem).Workgroup
PS C:\Users\Administrator.DC201>
```

This "zombie domain membership" state happens when a DC is force-demoted or when the domain no longer exists, but registry/service entries are left behind.

Reset Domain Membership (Force Workgroup Join)
Use this PowerShell command to force rejoin to a workgroup even if domain unjoin fails:

Add-Computer -WorkgroupName "WORKGROUP" -Force

If it fails with an error like "No mapping between account names and security IDs", it's because domain metadata is corrupt or incomplete **— go to next step.**

```
True
PS C:\Users\Administrator.DC201> (Get-WmiObject Win32_ComputerSystem).Workgroup
PS C:\Users\Administrator.DC201> Add-Computer -WorkgroupName "WORKGROUP" -Force
Add-Computer : Failed to unjoin computer 'DC201' from domain 'vlabs1.com' with the following error message: No mapping between account names and security IDs was
At line:1 char:1
+ Add-Computer -WorkgroupName "WORKGROUP" -Force
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OperationStopped: (DC201:String) [Add-Computer], InvalidOperationException
    + FullyQualifiedErrorId : FailToUnjoinDomain,Microsoft.PowerShell.Commands.AddComputerCommand

PS C:\Users\Administrator.DC201>
```

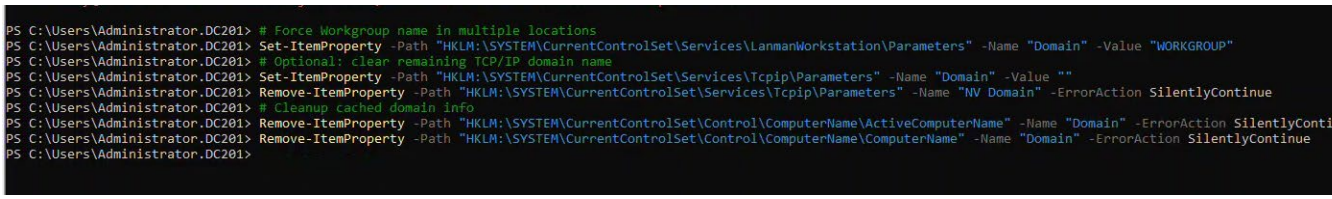
Hard Reset Domain Bindings via Registry (Advanced)
We'll fully sever domain links manually. Run all of these in PowerShell as Administrator:

```
# Force Workgroup name in multiple locations
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters" -Name
```

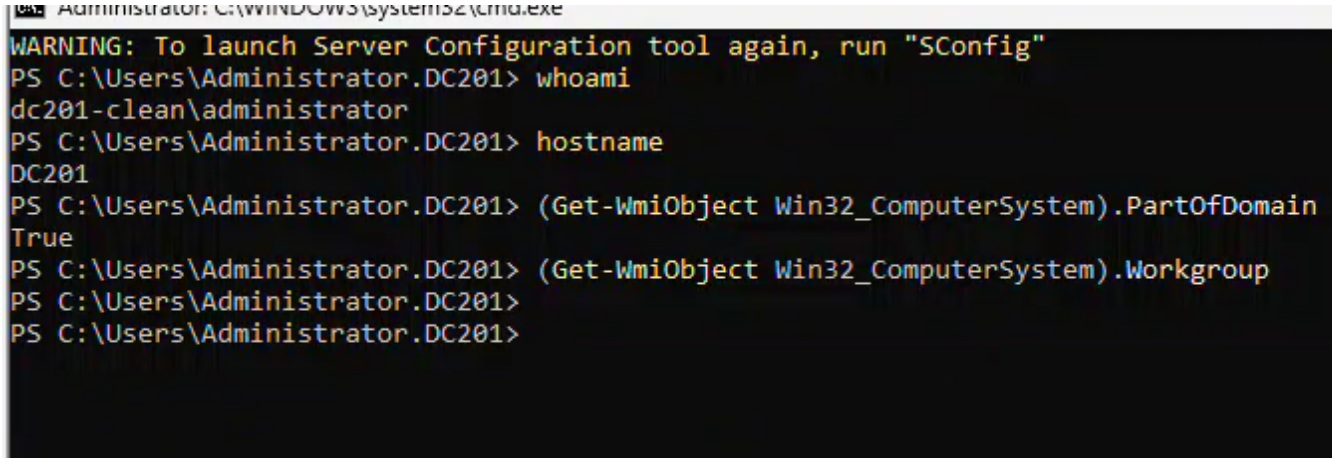
"Domain" -Value "WORKGROUP"

Optional: clear remaining TCP/IP domain name
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" -Name "Domain" -Value ""
Remove-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" -Name "NV Domain" -ErrorAction SilentlyContinue

Cleanup cached domain info
Remove-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName" -Name "Domain" -ErrorAction SilentlyContinue
Remove-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName" -Name "Domain" -ErrorAction SilentlyContinue



Restart-Computer



Steps to Reset Domain Join Using sysprep

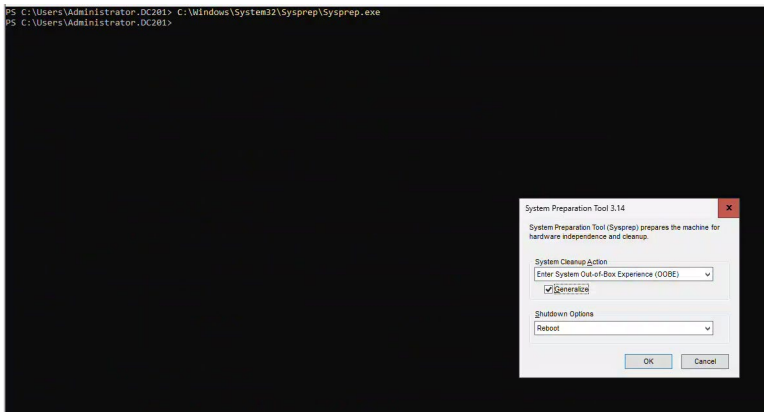
Open PowerShell or Command Prompt as Administrator

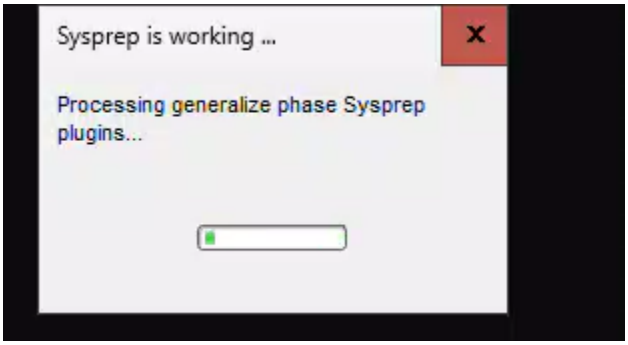
Run Sysprep:

C:\Windows\System32\Sysprep\Sysprep.exe

In the Sysprep window:

Select "Enter System Out-of-Box Experience (OOBE)"
Check "Generalize"
Select "Reboot" in Shutdown Options
Click OK

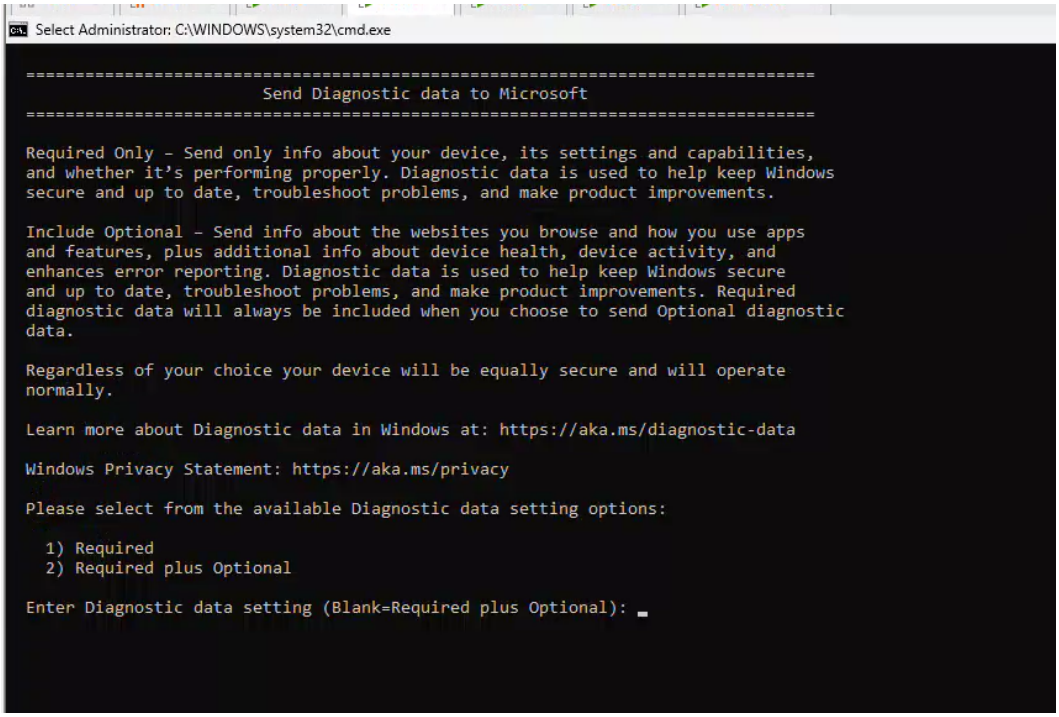




This

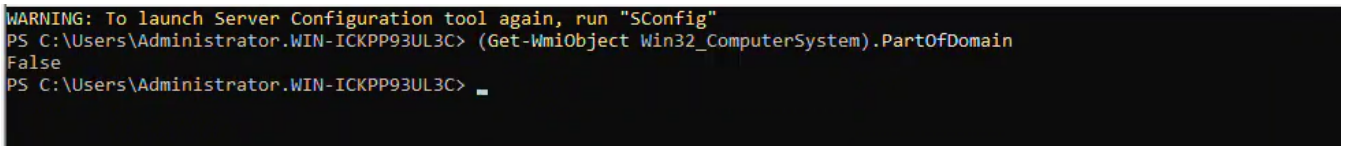
- Removes all domain bindings
- Clears SID and machine identifiers
- Allows machine to boot as if it's a fresh install, but keeps installed apps and settings
- Prompts for new computer name and network setup

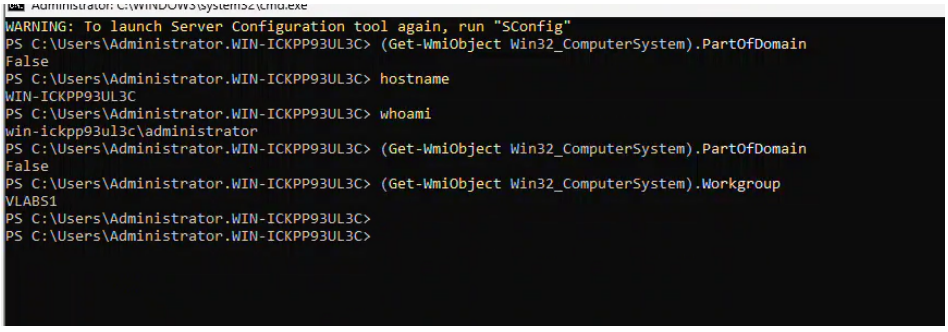
After reboot comes back



It now returns false

(Get-WmiObject Win32_ComputerSystem).PartOfDomain



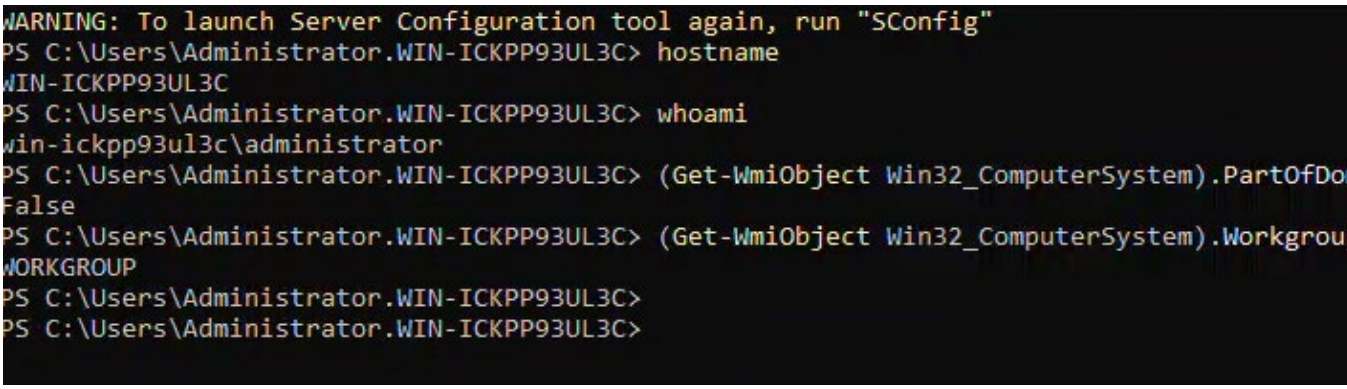


Success — machine is now no longer joined to a domain:

(Get-WmiObject Win32_ComputerSystem).PartOfDomain → False
whoami confirms you're logged into the local SAM account
hostname reflects a generic name (likely after Sysprep or reinstallation)
Workgroup is now set to VLABS1 (you can optionally change it to WORKGROUP)

Add-Computer -WorkgroupName "WORKGROUP" -Force -Restart

After machine comes back



Cleans up of DC201 in DC101

```
<#
.SYNOPSIS
   Cleans up old DC201 metadata from AD and DNS
.DESCRIPTION
   This script performs all necessary checks and cleanup for reusing the name "DC201"
   as a domain controller in vlabs1.com.
   Run on a writable DC with RSAT tools (like DC101).
#>

Import-Module ActiveDirectory
Import-Module DNSServer

$dcName = "DC201"
$siteName = "Montreal"
$domain = "vlabs1.com"
$rootDN = (Get-ADDomain).DistinguishedName
$configDN = (Get-ADRootDSE).configurationNamingContext

Write-Host "=== Starting cleanup for $dcName ===" -ForegroundColor Cyan

# 1. Check if computer account exists
$computer = Get-ADComputer -Filter "Name -eq '$dcName'" -ErrorAction SilentlyContinue
if ($computer) {
   Write-Host "[+] AD Computer object found. Deleting..." -ForegroundColor Yellow
   Remove-ADComputer -Identity $computer.DistinguishedName -Confirm:$false
} else {
   Write-Host "[-] AD Computer object not found." -ForegroundColor Green
}

# 2. Check NTDS Settings object
$ntdsObject = Get-ADObject -Filter "ObjectClass -eq 'nTDSDSA' -and Name -like '*$dcName*'" -SearchBase $configDN -
ErrorAction SilentlyContinue
```

```
if ($ntdsObject) {
   Write-Host "[+] NTDS Settings found. Deleting..." -ForegroundColor Yellow
   Remove-ADObject -Identity $ntdsObject.DistinguishedName -Recursive -Confirm:$false
} else {
   Write-Host "[-] NTDS Settings not found." -ForegroundColor Green
}

# 3. Check Server object in Sites
$serverObject = Get-ADObject -Filter "ObjectClass -eq 'server' -and Name -eq '$dcName'" -SearchBase
"CN=Servers,CN=$siteName,CN=Sites,$configDN" -ErrorAction SilentlyContinue
if ($serverObject) {
   Write-Host "[+] Server object in Site found. Deleting..." -ForegroundColor Yellow
   Remove-ADObject -Identity $serverObject.DistinguishedName -Confirm:$false
} else {
   Write-Host "[-] Server object in Site not found." -ForegroundColor Green
}

# 4. Clean DNS entries in domain zone
Write-Host "[*] Checking DNS records in zone $domain for $dcName..." -ForegroundColor Cyan
try {
   $dnsRecords = Get-DnsServerResourceRecord -ZoneName $domain -Name $dcName -ErrorAction Stop
   foreach ($record in $dnsRecords) {
      Write-Host "[+] Deleting DNS record: $($record.RecordType) $($record.HostName)" -ForegroundColor Yellow
      Remove-DnsServerResourceRecord -ZoneName $domain -RRType $record.RecordType -Name $record.HostName -
RecordData $record.RecordData -Force
   }
} catch {
   Write-Host "[-] No DNS records found for $dcName in $domain zone." -ForegroundColor Green
}

# 5. Clean DNS entries in _msdcs zone
$msdcsZone = "_msdcs.$domain"
Write-Host "[*] Checking DNS records in zone $msdcsZone for $dcName..." -ForegroundColor Cyan
try {
   $msdcsRecords = Get-DnsServerResourceRecord -ZoneName $msdcsZone -Name $dcName -ErrorAction Stop
   foreach ($record in $msdcsRecords) {
      Write-Host "[+] Deleting DNS record: $($record.RecordType) $($record.HostName)" -ForegroundColor Yellow
      Remove-DnsServerResourceRecord -ZoneName $msdcsZone -RRType $record.RecordType -Name
$record.HostName -RecordData $record.RecordData -Force
   }
} catch {
   Write-Host "[-] No DNS records found for $dcName in $msdcsZone zone." -ForegroundColor Green
}

Write-Host "=== Cleanup complete for $dcName ===" -ForegroundColor Cyan
```

```
=== Starting cleanup for DC201 ===
[-] AD Computer object not found.
[-] NTDS Settings not found.
[-] Server object in Site not found.
[*] Checking DNS records in zone vlabs1.com for DC201...
[-] No DNS records found for DC201 in vlabs1.com zone.
[*] Checking DNS records in zone _msdcs.vlabs1.com for DC201...
[-] No DNS records found for DC201 in _msdcs.vlabs1.com zone.
=== Cleanup complete for DC201 ===

PS C:\Windows\system32>
```

- **DC201** metadata cleanup is effectively complete.
- The name **DC201can be safely reused** for a new domain controller in the environment.
- No residual objects are blocking reuse.

7. **Retry Promote a Writable Domain Controller (Replica) – after cleaning everything**

Install-WindowsFeature AD-Domain-Services -IncludeManagementTools

```
PS C:\Users\Administrator.WIN-ICKPP93UL3C> Install-WindowsFeature AD-Domain-Services -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services}

PS C:\Users\Administrator.WIN-ICKPP93UL3C>
```

Change host name

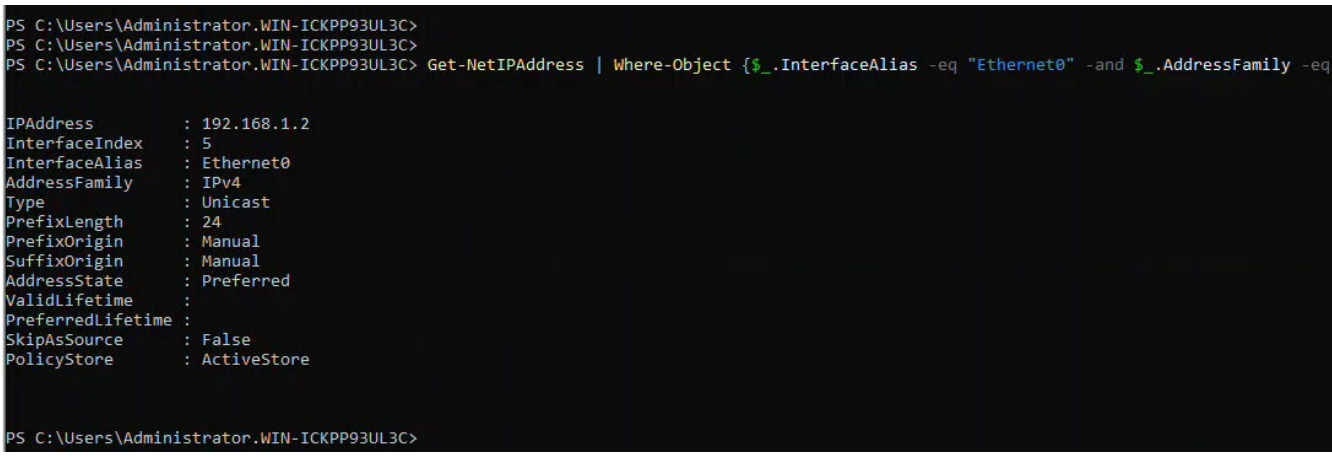
Rename-Computer -NewName "DC201" -Restart

```
WARNING: To launch Server Configuration tool again, run "SConfig"
PS C:\Users\Administrator.WIN-ICKPP93UL3C> hostname
DC201
PS C:\Users\Administrator.WIN-ICKPP93UL3C> whoami
dc201\administrator
PS C:\Users\Administrator.WIN-ICKPP93UL3C>
```

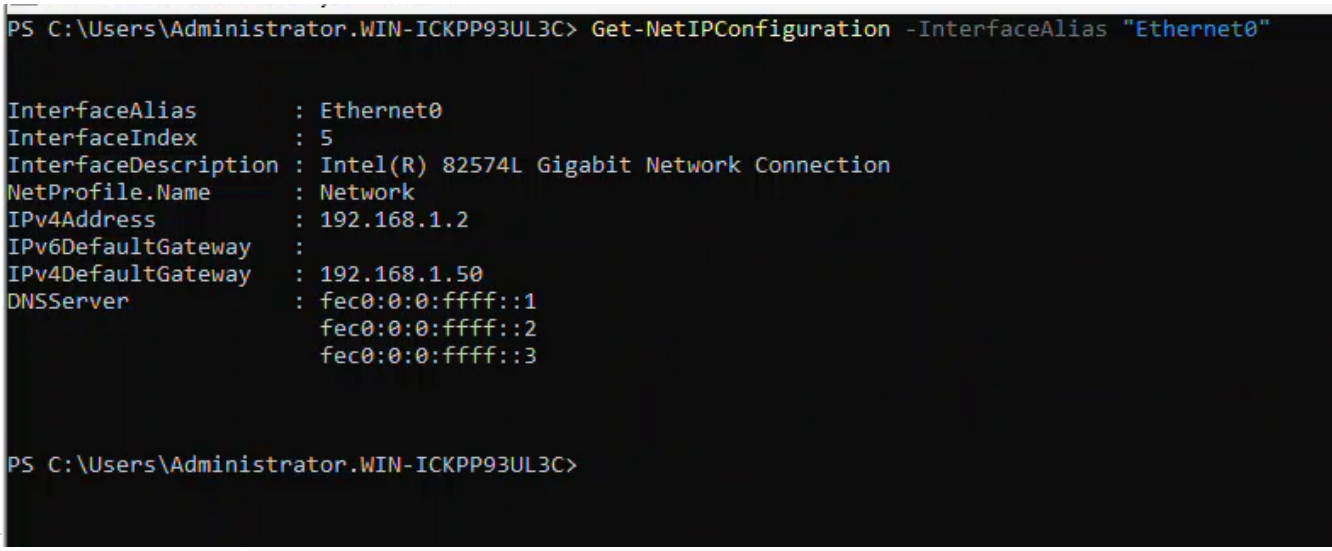
- Promote a member server to become a writable domain controller for an existing domain (vlabs1.com) in the Montreal site.

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

Get-NetIPAddress | Where-Object {$_.InterfaceAlias -eq "Ethernet0" -and $_.AddressFamily -eq "IPv4"}



Get-NetIPConfiguration -InterfaceAlias "Ethernet0"



New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters" -Name "DisabledComponents" -PropertyType DWord -Value 0xFF -Force

```
PS C:\Users\Administrator.WIN-ICKPP93UL3C> New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters" -Name "DisabledComponents" -PropertyType DWord -Value 0xFF -F


DisabledComponents : 255
PSPath             : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters
PSParentPath       : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6
PSChildName        : Parameters
PSDrive            : HKLM
PSProvider         : Microsoft.PowerShell.Core\Registry
```

Restart to disable ipv6

After restart complete the pre-check

 # Check computer name (should be DC201)
hostname

 # Check current IP configuration on Ethernet0
Get-NetIPConfiguration -InterfaceAlias "Ethernet0"

 # Verify IP address, subnet mask, and default gateway
Get-NetIPAddress -InterfaceAlias "Ethernet0" | Where-Object {$_.AddressFamily -eq "IPv4"}

 # Verify DNS server settings
Get-DnsClientServerAddress -InterfaceAlias "Ethernet0"

```
Administrator: C:\WINDOWS\system32\cmd.exe
WARNING: To launch Server Configuration tool again, run "SConfig"
PS C:\Users\Administrator.WIN-ICKPP93UL3C> # Check computer name (should be DC201)
PS C:\Users\Administrator.WIN-ICKPP93UL3C> hostname
DC201
PS C:\Users\Administrator.WIN-ICKPP93UL3C> # Check current IP configuration on Ethernet0
PS C:\Users\Administrator.WIN-ICKPP93UL3C> Get-NetIPConfiguration -InterfaceAlias "Ethernet0"


InterfaceAlias       : Ethernet0
InterfaceIndex       : 5
InterfaceDescription : Intel(R) 82574L Gigabit Network Connection
NetProfile.Name      : Network
IPv4Address          : 192.168.1.2
IPv4DefaultGateway   : 192.168.1.50
DNSServer            :



PS C:\Users\Administrator.WIN-ICKPP93UL3C> # Verify IP address, subnet mask, and default gateway
PS C:\Users\Administrator.WIN-ICKPP93UL3C> Get-NetIPAddress -InterfaceAlias "Ethernet0" | Where-Object {$_.AddressFamily -eq "IPv4"}


IPAddress         : 192.168.1.2
InterfaceIndex    : 5
InterfaceAlias    : Ethernet0
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Preferred
ValidLifetime     :
PreferredLifetime :
SkipAsSource      : False
PolicyStore       : ActiveStore



PS C:\Users\Administrator.WIN-ICKPP93UL3C>
PS C:\Users\Administrator.WIN-ICKPP93UL3C> # Verify DNS server settings
PS C:\Users\Administrator.WIN-ICKPP93UL3C> Get-DnsClientServerAddress -InterfaceAlias "Ethernet0"

InterfaceAlias               Interface Address ServerAddresses
                             Index     Family
-------------                --------- ------- --------------
Ethernet0                            5 IPv4    {}
Ethernet0                            5 IPv6    {}


PS C:\Users\Administrator.WIN-ICKPP93UL3C>
```

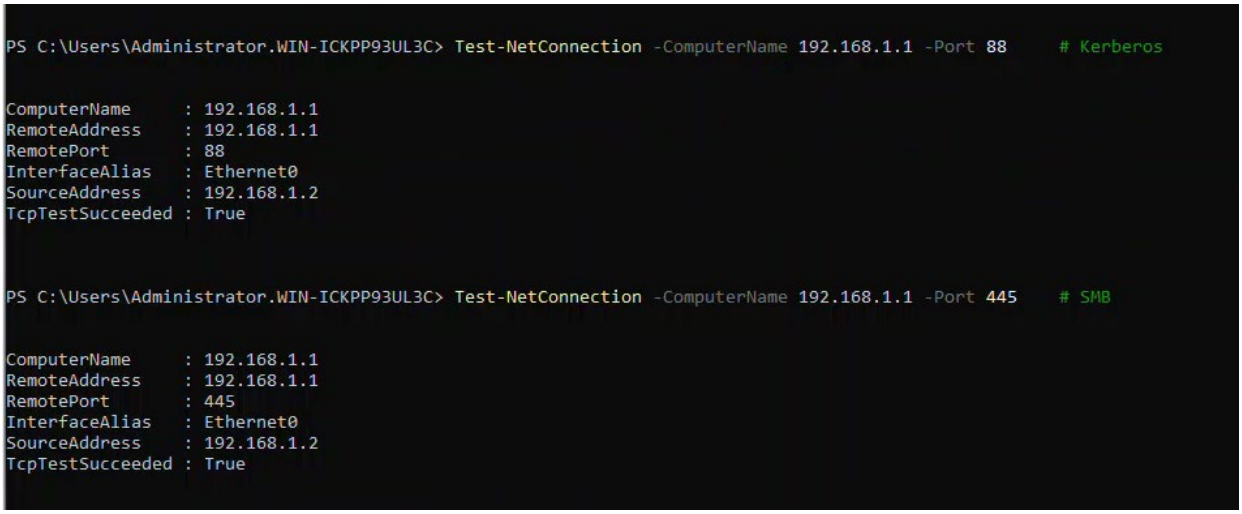
 # Check if Active Directory Domain Services role is installed
Get-WindowsFeature AD-Domain-Services, RSAT-ADDS

 # Check if DNS Server role is installed (if DNS on this DC)
Get-WindowsFeature DNS

```
PS C:\Users\Administrator.WIN-ICKPP93UL3C> # Check if Active Directory Domain Services role is installed
PS C:\Users\Administrator.WIN-ICKPP93UL3C> Get-WindowsFeature AD-Domain-Services, RSAT-ADDS

Display Name                                            Name                    Install State
------------                                            ----                    -------------
[X] Active Directory Domain Services                    AD-Domain-Services          Installed
            [ ] AD DS Tools                             RSAT-ADDS                   Available


PS C:\Users\Administrator.WIN-ICKPP93UL3C>
PS C:\Users\Administrator.WIN-ICKPP93UL3C> # Check if DNS Server role is installed (if DNS on this DC)
PS C:\Users\Administrator.WIN-ICKPP93UL3C> Get-WindowsFeature DNS

Display Name                                            Name                    Install State
------------                                            ----                    -------------
[X] DNS Server                                          DNS                         Installed
```

 # Check network connectivity to DC101 (Primary DC, IP 192.168.1.1)
Test-NetConnection -ComputerName 192.168.1.1 -Port 389 # LDAP
Test-NetConnection -ComputerName 192.168.1.1 -Port 135 # RPC
Test-NetConnection -ComputerName 192.168.1.1 -Port 88 # Kerberos
Test-NetConnection -ComputerName 192.168.1.1 -Port 445 # SMB

```
PS C:\Users\Administrator.WIN-ICKPP93UL3C> # Check network connectivity to DC101 (Primary DC, IP 192.168.1.1)
PS C:\Users\Administrator.WIN-ICKPP93UL3C> Test-NetConnection -ComputerName 192.168.1.1 -Port 389    # LDAP


ComputerName     : 192.168.1.1
RemoteAddress    : 192.168.1.1
RemotePort       : 389
InterfaceAlias   : Ethernet0
SourceAddress    : 192.168.1.2
TcpTestSucceeded : True



PS C:\Users\Administrator.WIN-ICKPP93UL3C> Test-NetConnection -ComputerName 192.168.1.1 -Port 135    # RPC


ComputerName     : 192.168.1.1
RemoteAddress    : 192.168.1.1
RemotePort       : 135
InterfaceAlias   : Ethernet0
SourceAddress    : 192.168.1.2
TcpTestSucceeded : True
```



 # Ping primary domain controller
ping 192.168.1.1

 # Check if DC201 can resolve the domain DNS name
nslookup vlabs1.com

 # Check if DC201 can resolve the DC locator DNS record
nslookup _ldap._tcp.dc._msdcs.vlabs1.com

 # Check time synchronization status
w32tm /query /status

```
PS C:\Users\Administrator.WIN-ICKPP93UL3C> # Ping primary domain controller
PS C:\Users\Administrator.WIN-ICKPP93UL3C> 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
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator.WIN-ICKPP93UL3C>
PS C:\Users\Administrator.WIN-ICKPP93UL3C> # Check if DC201 can resolve the domain DNS name
PS C:\Users\Administrator.WIN-ICKPP93UL3C> nslookup vlabs1.com
Server:  localhost
Address:  127.0.0.1

Name:    vlabs1.com
Address:  192.168.1.1

PS C:\Users\Administrator.WIN-ICKPP93UL3C>
PS C:\Users\Administrator.WIN-ICKPP93UL3C> # Check if DC201 can resolve the DC locator DNS record
PS C:\Users\Administrator.WIN-ICKPP93UL3C> nslookup _ldap._tcp.dc._msdcs.vlabs1.com
Server:  localhost
Address:  127.0.0.1

Name:    _ldap._tcp.dc._msdcs.vlabs1.com

PS C:\Users\Administrator.WIN-ICKPP93UL3C>
PS C:\Users\Administrator.WIN-ICKPP93UL3C> # Check time synchronization status
PS C:\Users\Administrator.WIN-ICKPP93UL3C> w32tm /query /status
Leap Indicator: 3(not synchronized)
Stratum: 0 (unspecified)
Precision: -23 (119.209ns per tick)
Root Delay: 0.0000000s
Root Dispersion: 0.0000000s
ReferenceId: 0x00000000 (unspecified)
Last Successful Sync Time: unspecified
Source: Local CMOS Clock
Poll Interval: 6 (64s)

PS C:\Users\Administrator.WIN-ICKPP93UL3C>
```

 # Check current FSMO role holder info (run on DC201 to see current roles)
netdom query fsmo /Domain:vlabs1.com

```
PS C:\Users\Administrator.WIN-ICKPP93UL3C>
PS C:\Users\Administrator.WIN-ICKPP93UL3C>
PS C:\Users\Administrator.WIN-ICKPP93UL3C> netdom query fsmo /Domain:vlabs1.com
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.WIN-ICKPP93UL3C>
```

 # Configure DC201 to sync time with DC101 (assuming DC101 is authoritative time source)
w32tm /config /syncfromflags:manual /manualpeerlist:"192.168.1.1" /reliable:no /update
w32tm /resync /force

PRE-REQuistes before promoting DC201

 # Confirm time sync status after forcing resync
w32tm /query /status

 # Verify DNS server setting (make sure DNS points to DC101 or itself if DNS installed)
Get-DnsClientServerAddress -InterfaceAlias "Ethernet0"

 # Check domain membership and replication status
nltest /dsgetdc:vlabs1.com
repadmin /replsummary

```
The command completed successfully.
PS C:\Users\Administrator.WIN-ICKPP93UL3C> # 1. Confirm time sync status after forcing resync
PS C:\Users\Administrator.WIN-ICKPP93UL3C> w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 2 (secondary reference - syncd by (S)NTP)
Precision: -23 (119.209ns per tick)
Root Delay: 0.0003045s
Root Dispersion: 14.3391458s
ReferenceId: 0xC0A80101 (source IP:  192.168.1.1)
Last Successful Sync Time: 5/20/2025 3:20:33 AM
Source: 192.168.1.1
Poll Interval: 6 (64s)

PS C:\Users\Administrator.WIN-ICKPP93UL3C>
PS C:\Users\Administrator.WIN-ICKPP93UL3C> # 2. Verify DNS server setting (make sure DNS points to DC101 or itself if DNS installed)
PS C:\Users\Administrator.WIN-ICKPP93UL3C> Get-DnsClientServerAddress -InterfaceAlias "Ethernet0"

InterfaceAlias               Interface Address ServerAddresses
                             Index     Family
-------------                --------- ------- ---------------
Ethernet0                            5 IPv4    {}
Ethernet0                            5 IPv6    {}


PS C:\Users\Administrator.WIN-ICKPP93UL3C>
PS C:\Users\Administrator.WIN-ICKPP93UL3C>
PS C:\Users\Administrator.WIN-ICKPP93UL3C> # 3. Check domain membership and replication status
PS C:\Users\Administrator.WIN-ICKPP93UL3C> nltest /dsgetdc:vlabs1.com
           DC: \\DC101.vlabs1.com
      Address: \\192.168.1.1
     Dom Guid: 402b24e7-c605-4172-bb2c-f1356eab96a2
     Dom Name: vlabs1.com
  Forest Name: vlabs1.com
 Dc Site Name: Montreal
Our Site Name: Montreal
        Flags: PDC GC DS LDAP KDC TIMESERV GTIMESERV WRITABLE DNS_DC DNS_DOMAIN DNS_FOREST CLOSE_SITE FULL_SECRET WS DS_8 DS_9 DS_10 KEYLIST
The command completed successfully
PS C:\Users\Administrator.WIN-ICKPP93UL3C> repadmin /replsummary
Replication Summary Start Time: 2025-05-20 03:21:50

Repadmin can't locate a "home server" or determine our domain because of the following error.  Try specifying specific "home server" with /homeserver:[dns name]
Error: An error occurred:
    Win32 Error 8419(0x20e3): The DSA object could not be found.



Source DSA          largest delta    fails/total %%   error


Destination DSA     largest delta    fails/total %%   error
```

 # Optional: Run dcdiag to check health of DC201
dcdiag /v

 # Set the DNS server to point to DC101 (192.168.1.1) on the Ethernet0 interface:
Set-DnsClientServerAddress -InterfaceAlias "Ethernet0" -ServerAddresses "192.168.1.1"

```
PS C:\Users\Administrator.WIN-ICKPP93UL3C>
PS C:\Users\Administrator.WIN-ICKPP93UL3C> # 4. Optional: Run dcdiag to check health of DC201
PS C:\Users\Administrator.WIN-ICKPP93UL3C> dcdiag /v

Directory Server Diagnosis

Performing initial setup:
   Trying to find home server...
   * Verifying that the local machine DC201, is a Directory Server.
   ***Error: DC201 is not a Directory Server.  Must specify /s:<Directory Server> or  /n:<Naming Context> or nothing to use the local machine.
   ERROR: Could not find home server.
PS C:\Users\Administrator.WIN-ICKPP93UL3C>
PS C:\Users\Administrator.WIN-ICKPP93UL3C>
PS C:\Users\Administrator.WIN-ICKPP93UL3C> Set-DnsClientServerAddress -InterfaceAlias "Ethernet0" -ServerAddresses "192.168.1.1"
PS C:\Users\Administrator.WIN-ICKPP93UL3C>
```

Get-DnsClientServerAddress -InterfaceAlias "Ethernet0"

```
PS C:\Users\Administrator.WIN-ICKPP93UL3C> Get-DnsClientServerAddress -InterfaceAlias "Ethernet0"

InterfaceAlias               Interface Address ServerAddresses
                             Index     Family
-------------                --------- ------- ---------------
Ethernet0                            5 IPv4    {192.168.1.1}
Ethernet0                            5 IPv6    {}


PS C:\Users\Administrator.WIN-ICKPP93UL3C>
```

Check connectivity again (ping DC101, nslookup, etc.)

Ping primary domain controller
ping 192.168.1.1

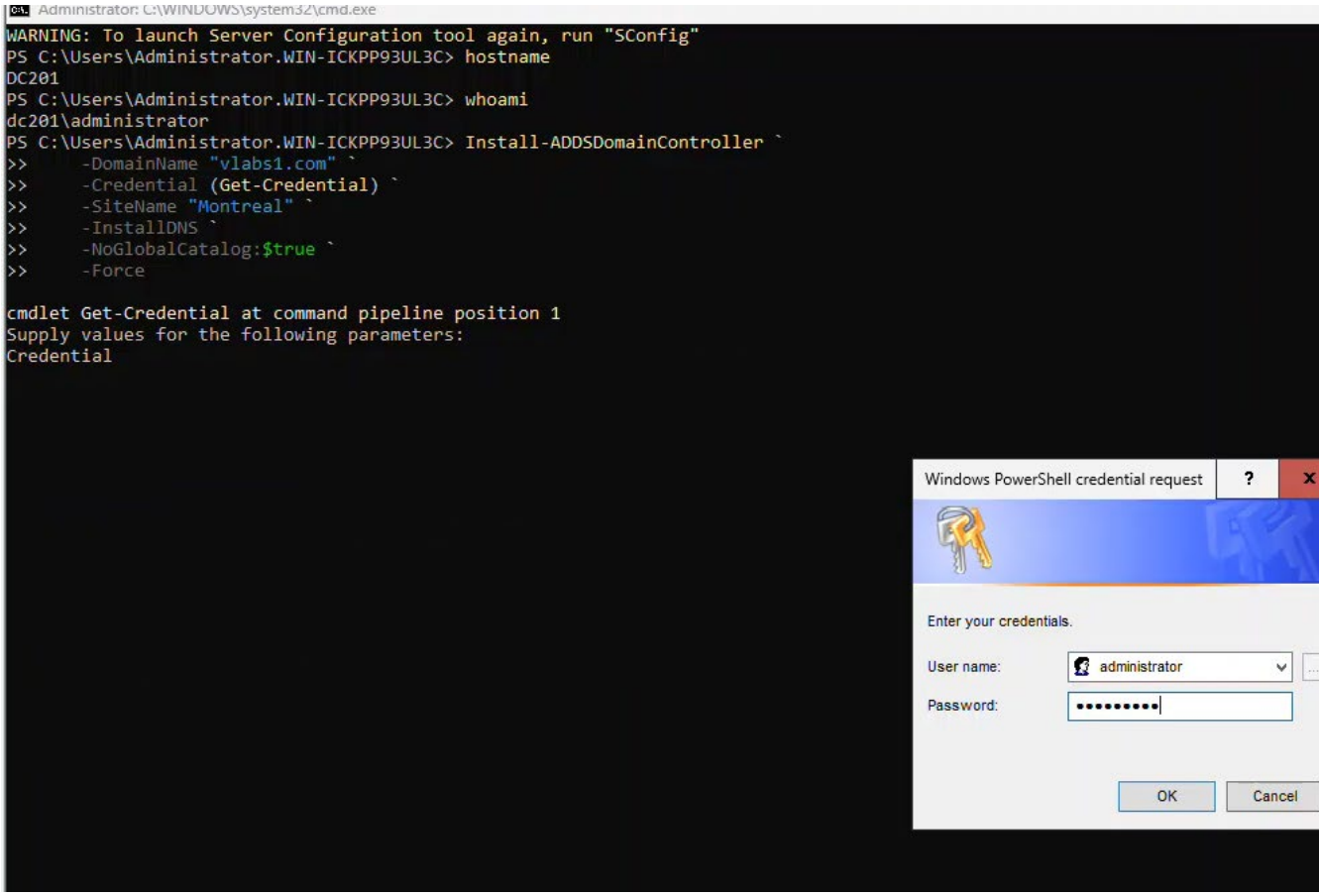
Check if DC201 can resolve the domain DNS name
nslookup vlabs1.com

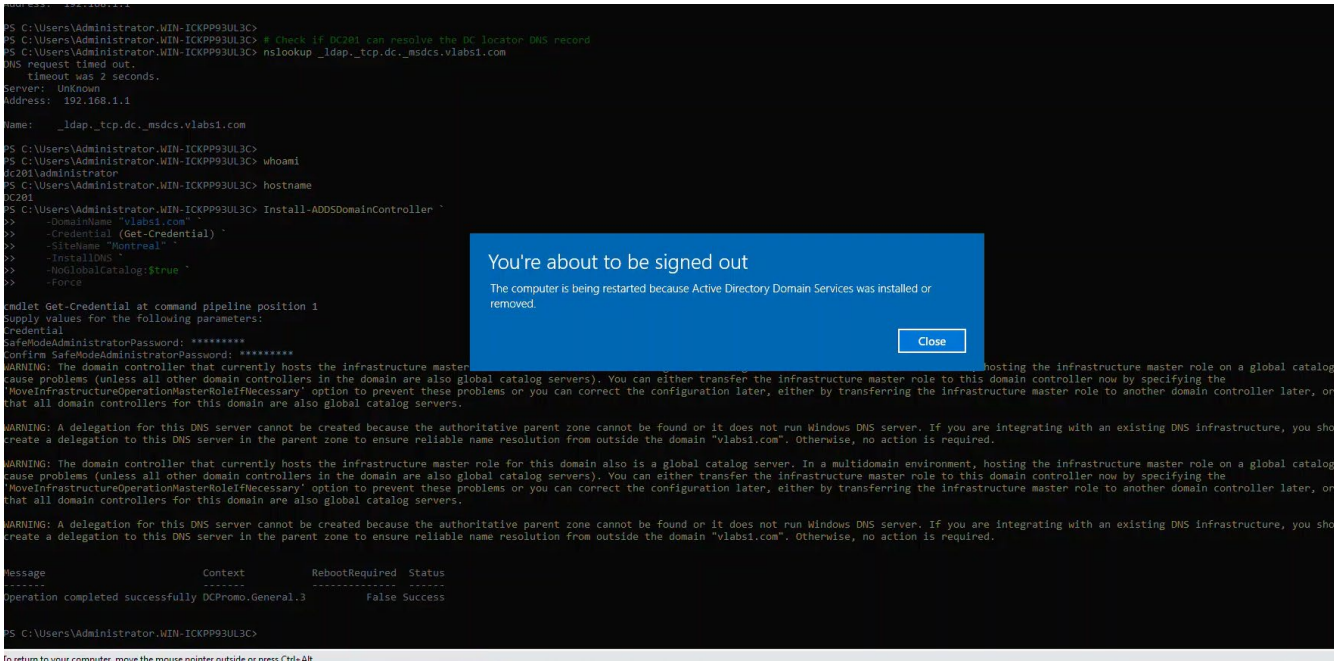
Check if DC201 can resolve the DC locator DNS record
nslookup _ldap._tcp.dc._msdcs.vlabs1.com

```
PS C:\Users\Administrator.WIN-ICKPP93UL3C> # Ping primary domain controller
PS C:\Users\Administrator.WIN-ICKPP93UL3C> 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
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator.WIN-ICKPP93UL3C>
PS C:\Users\Administrator.WIN-ICKPP93UL3C> # Check if DC201 can resolve the domain DNS name
PS C:\Users\Administrator.WIN-ICKPP93UL3C> 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.WIN-ICKPP93UL3C>
PS C:\Users\Administrator.WIN-ICKPP93UL3C> # Check if DC201 can resolve the DC locator DNS record
PS C:\Users\Administrator.WIN-ICKPP93UL3C> nslookup _ldap._tcp.dc._msdcs.vlabs1.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  192.168.1.1

Name:    _ldap._tcp.dc._msdcs.vlabs1.com

PS C:\Users\Administrator.WIN-ICKPP93UL3C>
```

Promote DC201 as Writable DC replica
Run on DC201 (the member server you want to promote):

```
Install-ADDSDomainController `
  -DomainName "vlabs1.com" `
  -Credential (Get-Credential) `
  -SiteName "Montreal" `
  -InstallDNS `
  -NoGlobalCatalog:$true `
  -Force
```





- This will prompt for credentials of an account with Domain Admin rights.
- It installs the DC as a writable replica in the Montreal site.
- DNS server role will be installed.
- Global Catalog is disabled initially

Verify AD health and replication status

After reboot, verify domain controller health
dcdiag /v /c /d /e /s:DC201

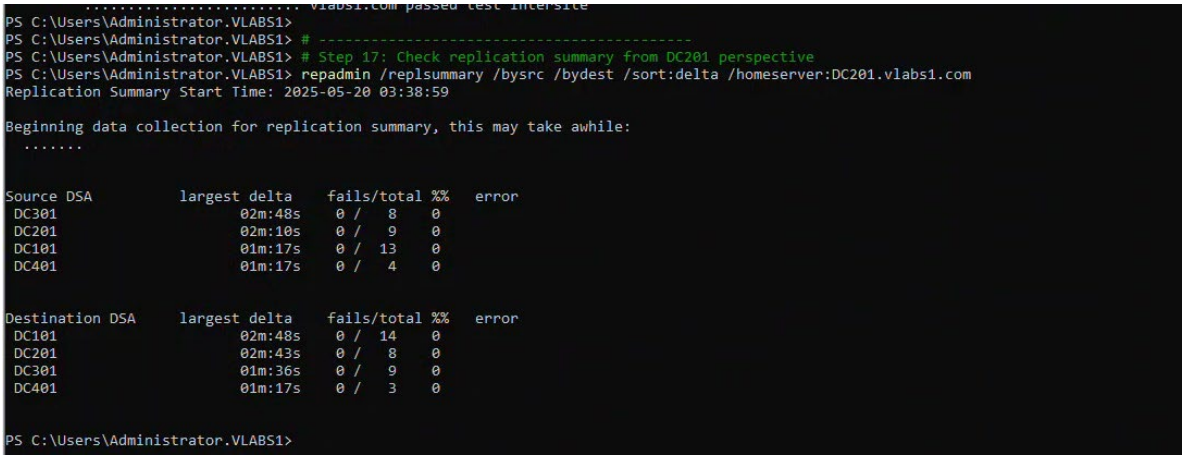
```
PS C:\Users\Administrator.VLABS1> hostname
DC201
PS C:\Users\Administrator.VLABS1> # Step 16: After reboot, verify domain controller health
PS C:\Users\Administrator.VLABS1> dcdiag /v /c /d /e /s:DC201
Command Line: "dcdiag.exe
/v /c /d /e /s:DC201"

Directory Server Diagnosis

Performing initial setup:
   * Connecting to directory service on server DC201.
   DC201.currentTime = 20250520073404.0Z
   DC201.highestCommittedUSN = 12323
   DC201.isSynchronized = 1
   DC201.isGlobalCatalogReady = 0
   * Identified AD Forest.
   Collecting AD specific global data
   * Collecting site info.
   Calling ldap_search_init_page(hld,CN=Sites,CN=Configuration,DC=vlabs1,DC=com,LDAP_SCOPE_SUBTREE,(objectCategory=ntDSSiteSettings),.......
   The previous call succeeded
   Iterating through the sites
   Looking at base site object: CN=NTDS Site Settings,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
   Getting ISTG and options for the site
   Looking at base site object: CN=NTDS Site Settings,CN=New-York,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
   Getting ISTG and options for the site
   Looking at base site object: CN=NTDS Site Settings,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
   Getting ISTG and options for the site
   * Identifying all servers.
   Calling ldap_search_init_page(hld,CN=Sites,CN=Configuration,DC=vlabs1,DC=com,LDAP_SCOPE_SUBTREE,(objectClass=ntDSDsa),.......
   The previous call succeeded....
   The previous call succeeded
   Iterating through the list of servers
   Getting information for the server CN=NTDS Settings,CN=DC101,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
   objectGuid obtained
   InvocationID obtained
   dnsHostname obtained
   site info obtained
   All the info for the server collected
   Getting information for the server CN=NTDS Settings,CN=DC301,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
   objectGuid obtained
   InvocationID obtained
   dnsHostname obtained
   site info obtained
   All the info for the server collected
   Getting information for the server CN=NTDS Settings,CN=DC401,CN=Servers,CN=New-York,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
   objectGuid obtained
   InvocationID obtained
   dnsHostname obtained
   site info obtained
   All the info for the server collected
   Getting information for the server CN=NTDS Settings,CN=DC201,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
   objectGuid obtained
   InvocationID obtained
   dnsHostname obtained
   site info obtained
```

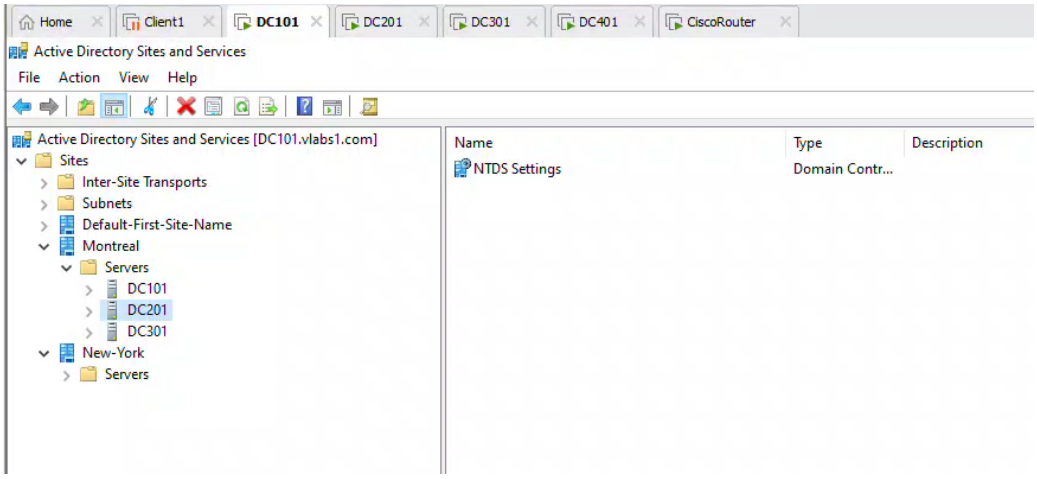
.... Not all screens included

```
         KDC Name: \\DC201.vlabs1.com
         Locator Flags: 0xe007f1f8
         ..... vlabs1.com passed test FsmoCheck
      Starting test: Intersite
         Skipping site Default-First-Site-Name, this site is outside the scope provided by the command line arguments provided.
         Doing intersite inbound replication test on site New-York:
            Locating & Contacting Intersite Topology Generator (ISTG) ...
               The ISTG for site New-York is: DC401.
               ISTG (DC401) Failure Parameters:
                   Failover Tries: 1
                   Failover Time: 120
            Checking for down bridgeheads ...
               Bridghead Montreal\DC101 is up and replicating fine.
               Bridghead New-York\DC401 is up and replicating fine.
            Doing in depth site analysis ...
               All expected sites and bridgeheads are replicating into site New-York.
         Doing intersite inbound replication test on site Montreal:
            Locating & Contacting Intersite Topology Generator (ISTG) ...
               The ISTG for site Montreal is: DC101.
               ISTG (DC101) Failure Parameters:
                   Failover Tries: 1
                   Failover Time: 120
            Checking for down bridgeheads ...
               Bridghead New-York\DC401 is up and replicating fine.
               Bridghead Montreal\DC101 is up and replicating fine.
            Doing in depth site analysis ...
               All expected sites and bridgeheads are replicating into site Montreal.
         ..... vlabs1.com passed test Intersite
PS C:\Users\Administrator.VLABS1>
```

Check replication summary from DC201 perspective

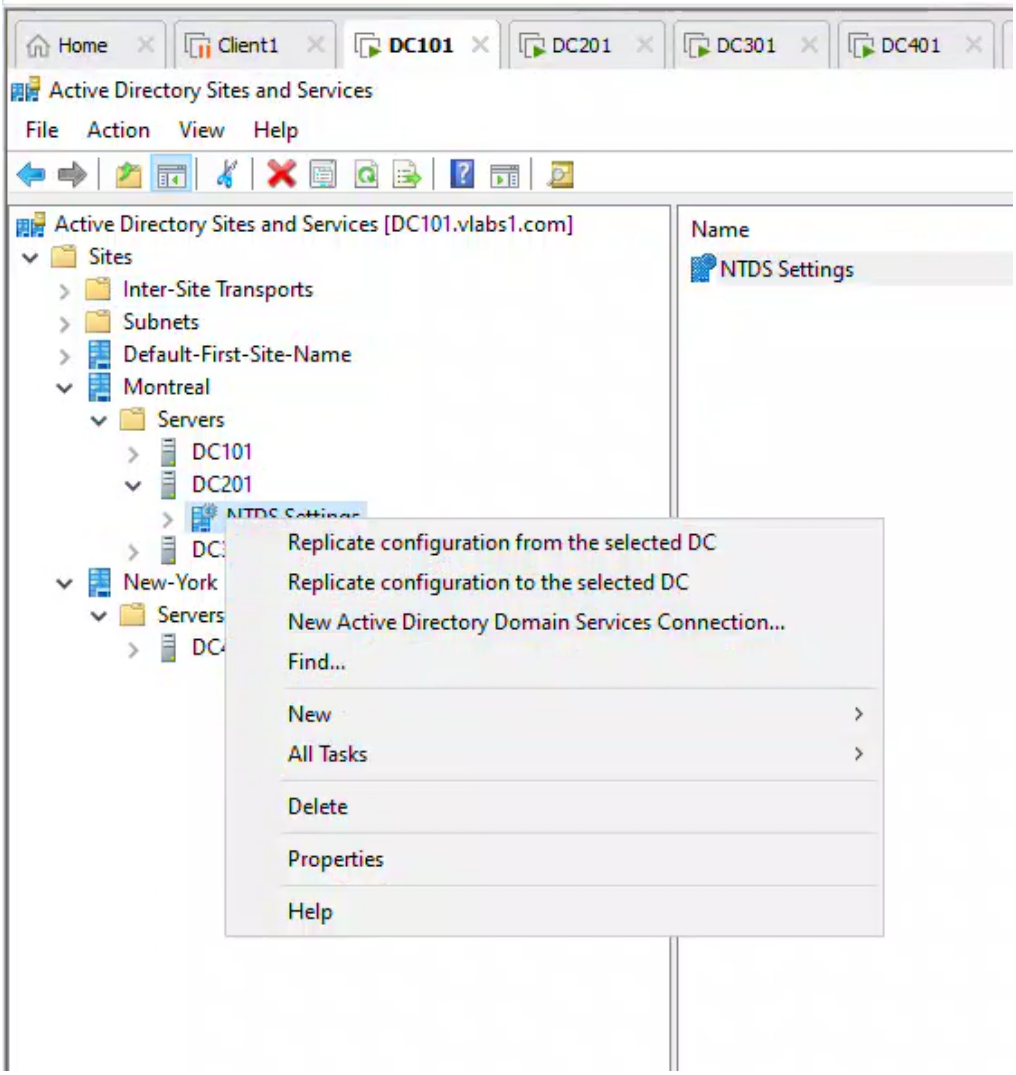
repadmin /replsummary /bysrc /bydest /sort:delta /homeserver:DC201.vlabs1.com

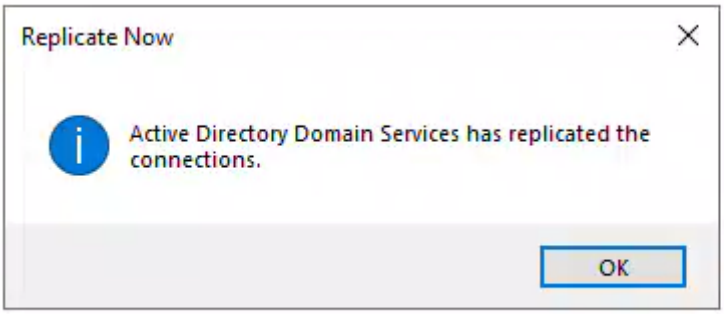




15 Managing FSMO role and Global Catalog

- Before starting these tasks, from **DC101**, open **Active Directory Sites and Services.**
- Locate the **NTDS connection** between **DC101** and **DC201.**
- Right-click the **connection object** and select **Replicate now.**





- On **DC201**, use the **netdom tool** to locate the **FSMO** roles of all the domains.

netdom query fsmo

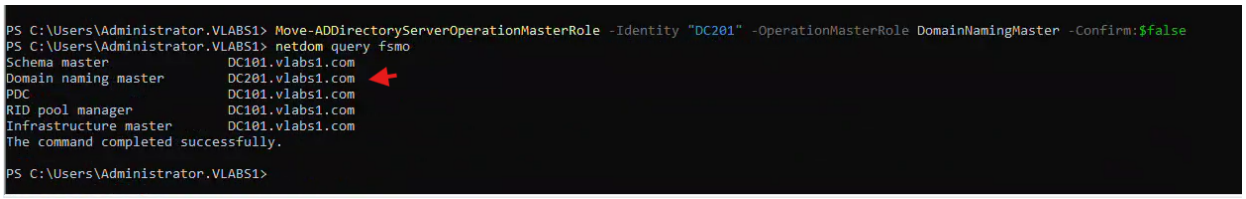
Get-ADForest | Select-Object DomainNamingMaster, SchemaMaster

Get-ADDomain | Select-Object PDCEmulator, RIDMaster, InfrastructureMaster

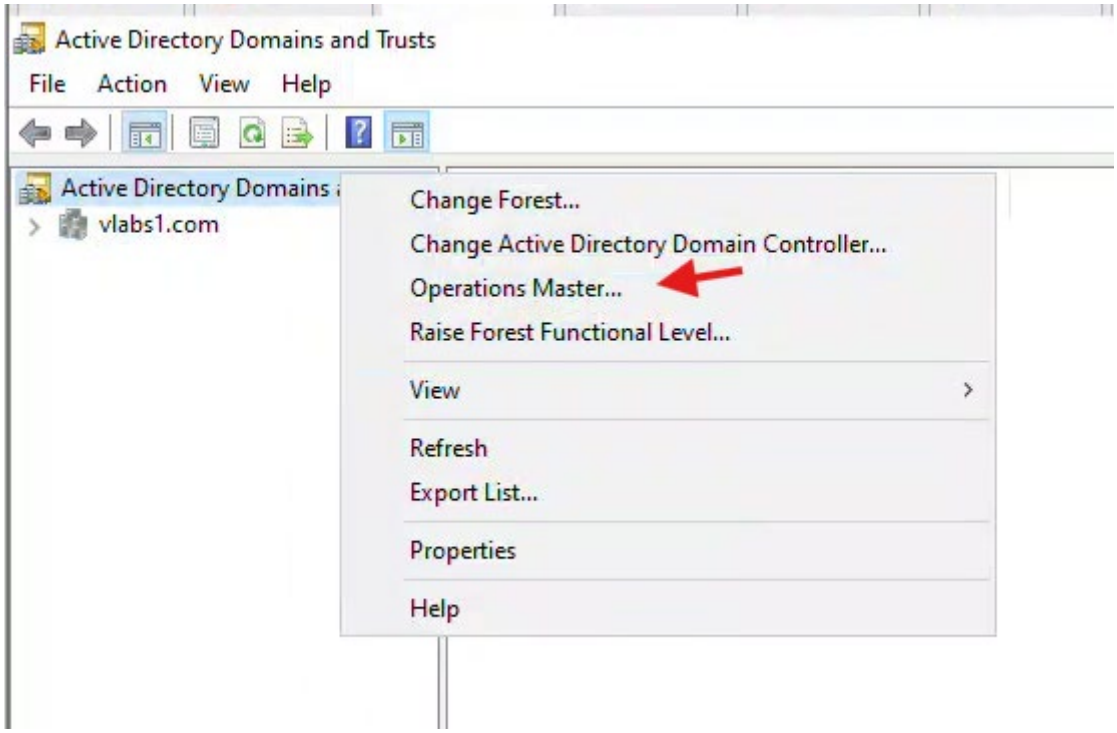
```
PS C:\Users\Administrator.VLABS1>
PS C:\Users\Administrator.VLABS1>
PS C:\Users\Administrator.VLABS1> netdom query fsmo
Schema master               DC101.vlabs1.com
Domain naming master        DC101.vlabs1.com
PDC                         DC101.vlabs1.com
RID pool manager            DC101.vlabs1.com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

PS C:\Users\Administrator.VLABS1> Get-ADForest | Select-Object DomainNamingMaster, SchemaMaster

DomainNamingMaster SchemaMaster
------------------ ------------
DC101.vlabs1.com   DC101.vlabs1.com


PS C:\Users\Administrator.VLABS1> Get-ADDomain | Select-Object PDCEmulator, RIDMaster, InfrastructureMaster

PDCEmulator      RIDMaster        InfrastructureMaster
-----------      ---------        --------------------
DC101.vlabs1.com DC101.vlabs1.com DC101.vlabs1.com


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

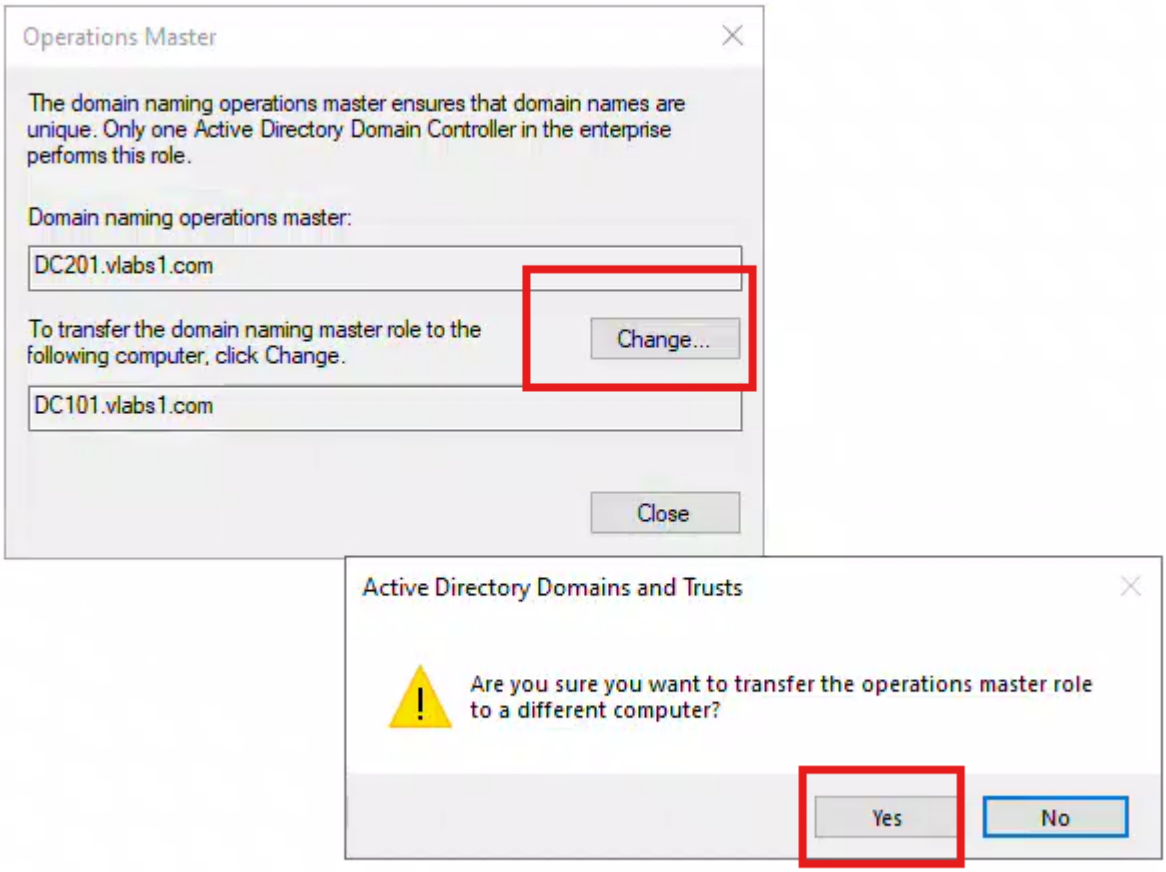
- On **DC201**, use **PowerShell** to transfer the **Domain Naming Master FSMO role** from **DC101** to **DC201**, then verify that the role has been successfully moved.

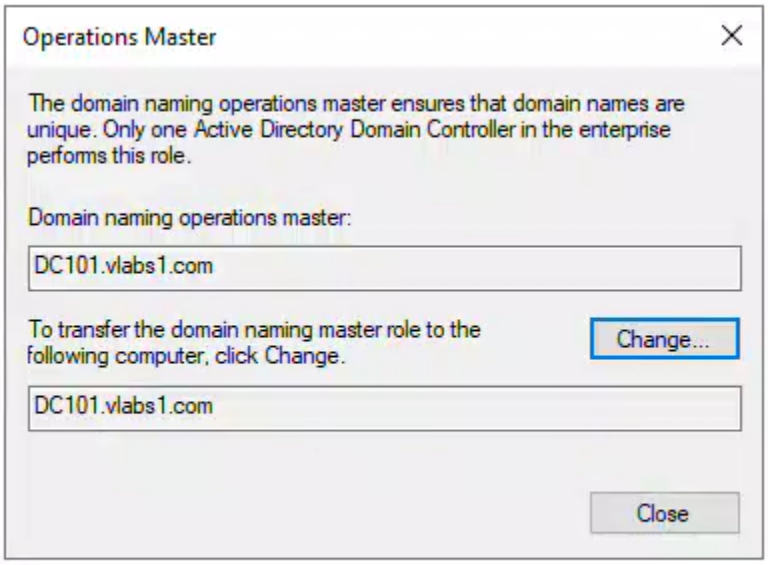
  Move-ADDirectoryServerOperationMasterRole -Identity "DC201" -OperationMasterRole DomainNamingMaster -Confirm:$false



- Go back to **DC101,** use the **GUI** to transfer the **Domain Naming Master FSMO role** back to **DC101**.


Active Directory Domains and Trusts
File
Action
View
Help
Active Directory Domains
vlabs1.com
Change Forest...
Change Active Directory Domain Controller...
Operations Master...
Raise Forest Functional Level...
View
Refresh
Export List...
Properties
Help


Operations Master
The domain naming operations master ensures that domain names are unique. Only one Active Directory Domain Controller in the enterprise performs this role.
Domain naming operations master:
DC201.vlabs1.com
To transfer the domain naming master role to the following computer, click Change.
Change...
DC101.vlabs1.com
Close
Active Directory Domains and Trusts
Are you sure you want to transfer the operations master role to a different computer?
Yes
No




```
PS C:\Users\Administrator.VLABS1> hostname
DC201
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>
```

- Simulate a failure scenario:
  - Stop the **DC101** server.

Stop-Computer -ComputerName DC101 -Force

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Stop-Computer -ComputerName DC101 -Force
```

- On **DC201**, use the **ntdsutil** tool to **seize** the **PDC Emulator FSMO** role.

  ntdsutil

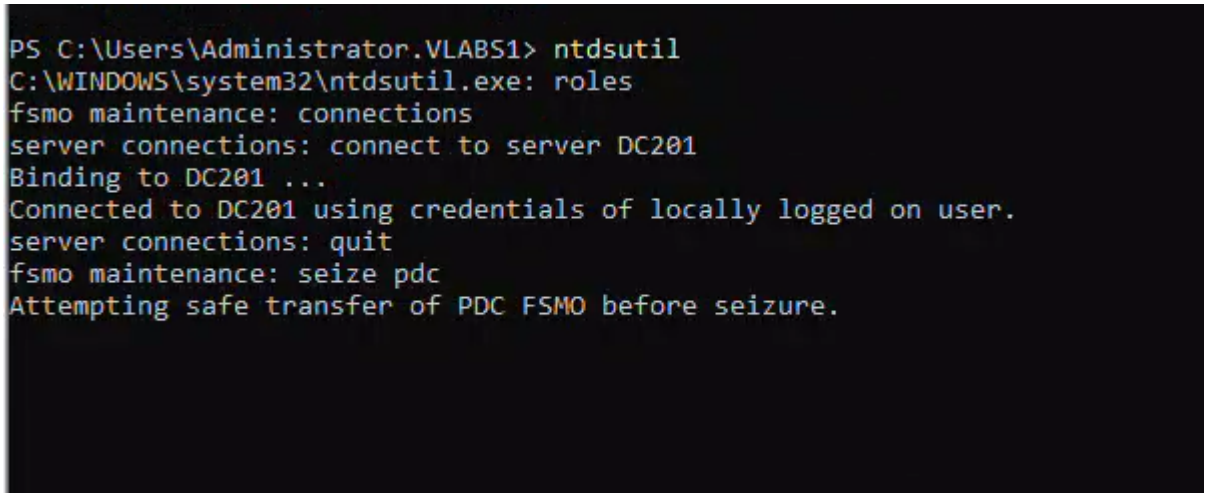
  roles

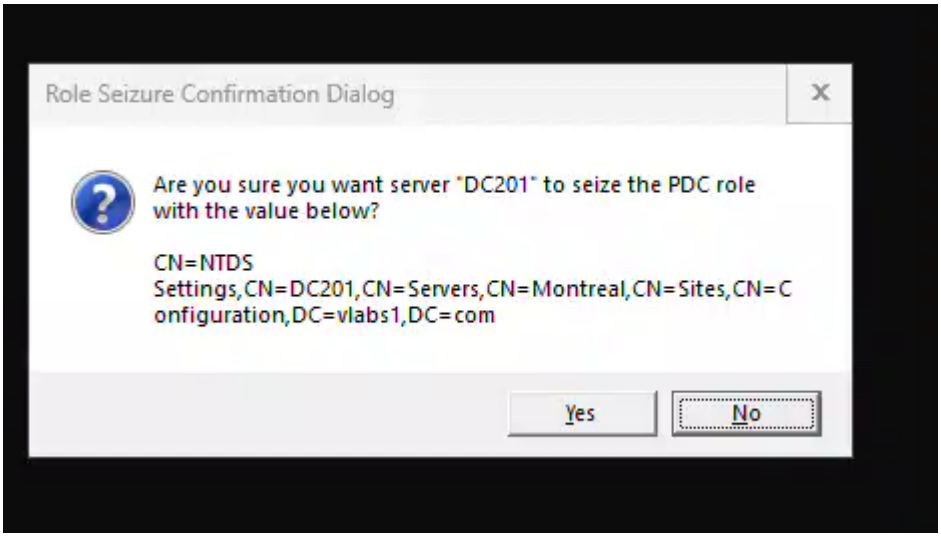
  connections

  connect to server DC201

  quit

  seize pdc





The following line confirms the PDC role is now held by DC201:

PDC - CN=NTDS Settings,CN=DC201,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com

```
PS C:\Users\Administrator.VLABS1> ntdsutil
C:\WINDOWS\system32\ntdsutil.exe: roles
fsmo maintenance: connections
server connections: connect to server DC201
Binding to DC201 ...
Connected to DC201 using credentials of locally logged on user.
server connections: quit
fsmo maintenance: seize pdc
Attempting safe transfer of PDC FSMO before seizure.
ldap_modify_sW error 0x34(52 (Unavailable).
Ldap extended error message is 000020AF: SvcErr: DSID-03210901, problem 5002 (UNAVAILABLE), data 1722

Win32 error returned is 0x20af(The requested FSMO operation failed. The current FSMO holder could not be contacted.)
)
Depending on the error code this may indicate a connection,
ldap, or role transfer error.
Transfer of PDC FSMO failed, proceeding with seizure ...
Server "DC201" knows about 5 roles
Schema - CN=NTDS Settings,CN=DC101,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
Naming Master - CN=NTDS Settings,CN=DC101,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
PDC - CN=NTDS Settings,CN=DC201,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
RID - CN=NTDS Settings,CN=DC101,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
Infrastructure - CN=NTDS Settings,CN=DC101,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com
fsmo maintenance:
fsmo maintenance: quit
C:\WINDOWS\system32\ntdsutil.exe: quit
PS C:\Users\Administrator.VLABS1> netdom query fsmo
Schema master               DC101.vlabs1.com
Domain naming master        DC101.vlabs1.com
PDC                         DC201.vlabs1.com
RID pool manager            DC101.vlabs1.com
Infrastructure master       DC101.vlabs1.com
The command completed successfully.

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

- Start the **DC101** server again.

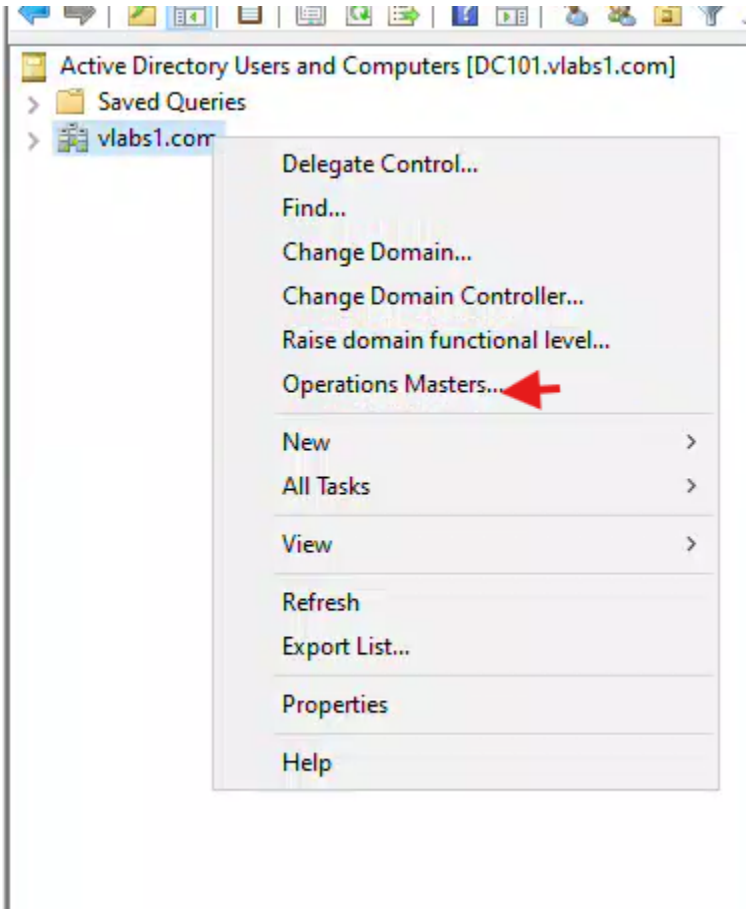
Power on the virtual machine

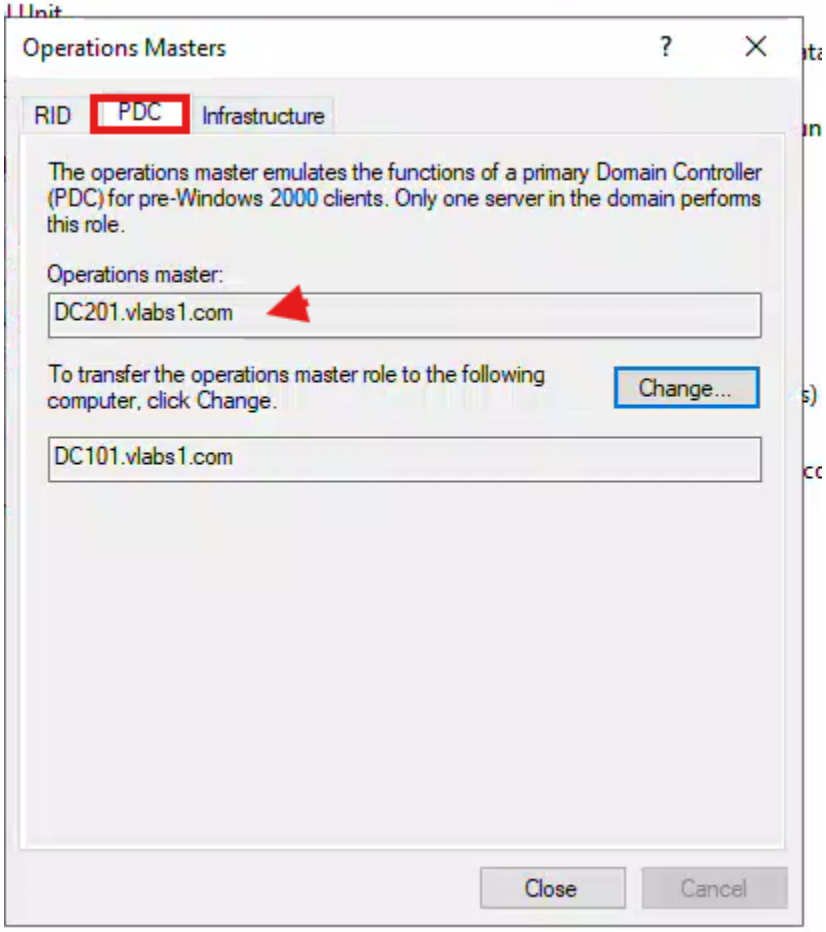
- From **DC101**, use the **GUI** to verify that the **PDC Emulator FSMO role** is now held by **DC201**.

Open **Active Directory Users and Computers**

Right-click the domain name > Click **Operations Masters**

Go to **PDC tab** → Confirm **DC201** is listed as the holder





- Go back to **DC201**:
  - Configure the **PDC Emulator DC** to synchronize time with a reliable time source.

    w32tm /config /manualpeerlist:"time.windows.com,0x1" /syncfromflags:manual /reliable:yes /update

    w32tm /resync /force

    w32tm /query /status

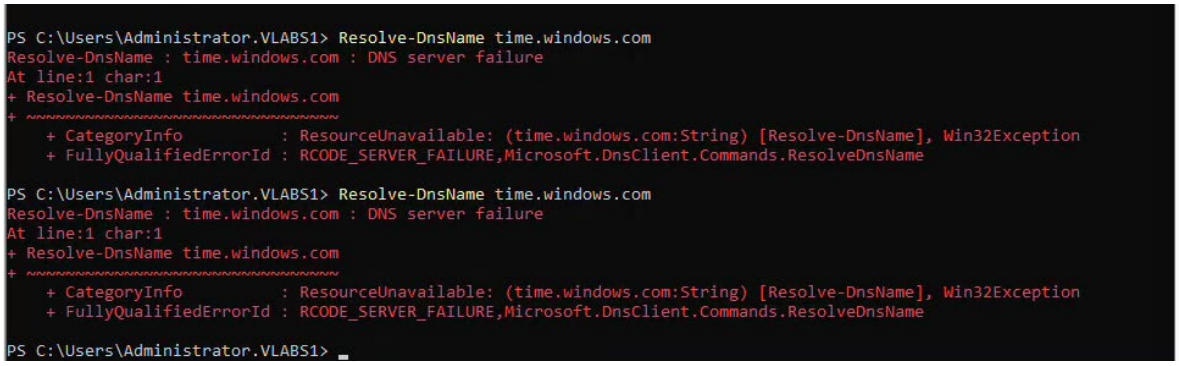
```
Administrator: C:\WINDOWS\system32\cmd.exe
PS C:\Users\Administrator.VLABS1> w32tm /config /manualpeerlist:"time.windows.com,0x1" /syncfromflags:manual /reliable:yes /update
The command completed successfully.
PS C:\Users\Administrator.VLABS1> w32tm /resync /force
Sending resync command to local computer
The computer did not resync because no time data was available.
PS C:\Users\Administrator.VLABS1> w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 2 (secondary reference - syncd by (S)NTP)
Precision: -23 (119.209ns per tick)
Root Delay: 0.0000000s
Root Dispersion: 10.0000000s
ReferenceId: 0xC0A80101 (source IP:  192.168.1.1)
Last Successful Sync Time: 5/20/2025 4:29:37 AM
Source: DC101.vlabs1.com
Poll Interval: 6 (64s)

PS C:\Users\Administrator.VLABS1> net stop w32time
The Windows Time service is stopping.
The Windows Time service was stopped successfully.

PS C:\Users\Administrator.VLABS1> w32tm /unregister
W32Time successfully unregistered.
PS C:\Users\Administrator.VLABS1> w32tm /register
W32Time successfully registered.
PS C:\Users\Administrator.VLABS1> net start w32time
The Windows Time service is starting.
The Windows Time service was started successfully.

PS C:\Users\Administrator.VLABS1>
PS C:\Users\Administrator.VLABS1> w32tm /config /manualpeerlist:"time.windows.com,0x1" /syncfromflags:manual /reliable:yes /update
The command completed successfully.
PS C:\Users\Administrator.VLABS1> w32tm /resync /force
Sending resync command to local computer
The computer did not resync because no time data was available.
PS C:\Users\Administrator.VLABS1> w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 1 (primary reference - syncd by radio clock)
Precision: -23 (119.209ns per tick)
Root Delay: 0.0000000s
Root Dispersion: 10.0000000s
ReferenceId: 0x4C4F434C (source name:  "LOCL")
Last Successful Sync Time: 5/20/2025 4:32:08 AM
Source: Local CMOS Clock
Poll Interval: 6 (64s)

PS C:\Users\Administrator.VLABS1> w32tm /query /source
Local CMOS Clock
```

```
PS C:\Users\Administrator.VLABS1>
PS C:\Users\Administrator.VLABS1>
PS C:\Users\Administrator.VLABS1> Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\W32Time\Parameters" -Name "Type" -Value "NTP"
PS C:\Users\Administrator.VLABS1> w32tm /config /manualpeerlist:"time.windows.com,0x1" /syncfromflags:manual /reliable:yes /update
The command completed successfully.
PS C:\Users\Administrator.VLABS1> New-NetFirewallRule -DisplayName "Allow NTP" -Direction Outbound -Protocol UDP -LocalPort 123 -Action Allow


Name                          : {b440362f-d647-4563-a8cb-917adb7ee8c2}
DisplayName                   : Allow NTP
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Outbound
Action                        : Allow
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId                   :
PackageFamilyName             :
```

```
PS C:\Users\Administrator.VLABS1> net stop w32time
The Windows Time service is stopping.
The Windows Time service was stopped successfully.

PS C:\Users\Administrator.VLABS1> net start w32time
The Windows Time service is starting......
The Windows Time service was started successfully.

PS C:\Users\Administrator.VLABS1> w32tm /resync /force
Sending resync command to local computer
The computer did not resync because no time data was available.
PS C:\Users\Administrator.VLABS1> w32tm /resync /force
Sending resync command to local computer
The computer did not resync because no time data was available.
PS C:\Users\Administrator.VLABS1>
PS C:\Users\Administrator.VLABS1>
PS C:\Users\Administrator.VLABS1> w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 1 (primary reference - syncd by radio clock)
Precision: -23 (119.209ns per tick)
Root Delay: 0.0000000s
Root Dispersion: 10.0000000s
ReferenceId: 0x4C4F434C (source name:  "LOCL")
Last Successful Sync Time: 5/20/2025 4:36:07 AM
Source: Local CMOS Clock
Poll Interval: 6 (64s)

PS C:\Users\Administrator.VLABS1> w32tm /query /source
Local CMOS Clock
PS C:\Users\Administrator.VLABS1> _
```

```
PS C:\Users\Administrator.VLABS1> w32tm /stripchart /computer:time.windows.com /dataonly /samples:5
The following error occurred: This is usually a temporary error during hostname resolution and means that the local server did not receive a response from an authoritative server. (0x80072AFA)
PS C:\Users\Administrator.VLABS1>
PS C:\Users\Administrator.VLABS1> PS C:\Users\Administrator.VLABS1> w32tm /stripchart /computer:time.windows.com /dataonly /samples:5
Get-Process : A positional parameter cannot be found that accepts argument 'w32tm'.
At line:1 char:1
+ PS C:\Users\Administrator.VLABS1> w32tm /stripchart /computer:time.wi ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Get-Process], ParameterBindingException
    + FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.GetProcessCommand
```

```
PS C:\Users\Administrator.VLABS1>
PS C:\Users\Administrator.VLABS1>
PS C:\Users\Administrator.VLABS1> Get-DnsClientServerAddress

InterfaceAlias               Interface Address ServerAddresses
                             Index     Family
--------------               --------- ------- ---------------
Ethernet0                            5 IPv4    {192.168.1.1, 127.0.0.1}
Ethernet0                            5 IPv6    {}
Loopback Pseudo-Interface 1          1 IPv4    {}
Loopback Pseudo-Interface 1          1 IPv6    {fec0:0:0:ffff::1, fec0:0:0:ffff::2, fec0:0:0:ffff::3}


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



Command user to setup and troubleshoot NTP

 # 1. Set the time source to time.windows.com

w32tm /config /manualpeerlist:"time.windows.com,0x1" /syncfromflags:manual /reliable:yes /update

 # → Configures this server to use time.windows.com as its manual NTP peer and marks it as a reliable time source.

 # 2. Force a resynchronization

w32tm /resync /force

 # → Attempts to force the time service to synchronize immediately.

 # 3. Check current time sync status

w32tm /query /status

 # → Displays details like source, last sync time, stratum level, and accuracy.

 # 4. Query the current time source

w32tm /query /source

 # → Shows the currently used time source (e.g., Local CMOS Clock or time.windows.com).

 # 5. Stop the Windows Time service

net stop w32time

 # → Stops the W32Time (Windows Time) service.

 # 6. Unregister the time service

w32tm /unregister

 # → Unregisters the W32Time service (clears config).

 # 7. Register the time service again

w32tm /register

 # → Registers W32Time and resets to default settings.

 # 8. Start the Windows Time service again

net start w32time

 # → Starts the W32Time service.

 # 9. Reset time type in registry to use NTP explicitly

Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\W32Time\Parameters" -Name "Type" -Value "NTP"

 # → Ensures the time service is set to use NTP rather than NT5DS or other methods.

 # 10. Allow outbound NTP traffic through Windows Firewall

New-NetFirewallRule -DisplayName "Allow NTP" -Direction Outbound -Protocol UDP -LocalPort 123 -Action Allow

 # → Ensures outbound NTP requests on UDP port 123 are not blocked by Windows Firewall.

 # 11. Test connectivity to external NTP server

w32tm /stripchart /computer:time.windows.com /dataonly /samples:5

 # → Attempts to graph time offset from a remote time server; failed in your case due to DNS issues.

 # 12. View configured DNS servers

Get-DnsClientServerAddress

 # → Lists the DNS servers used by the local network interface.

 # 13. Test DNS resolution for time.windows.com

Resolve-DnsName time.windows.com

 # → Tests whether the local system can resolve the NTP server's hostname to an IP address.

 # → Failed due to DNS server failure (DC101 being unreachable or non-recursive).

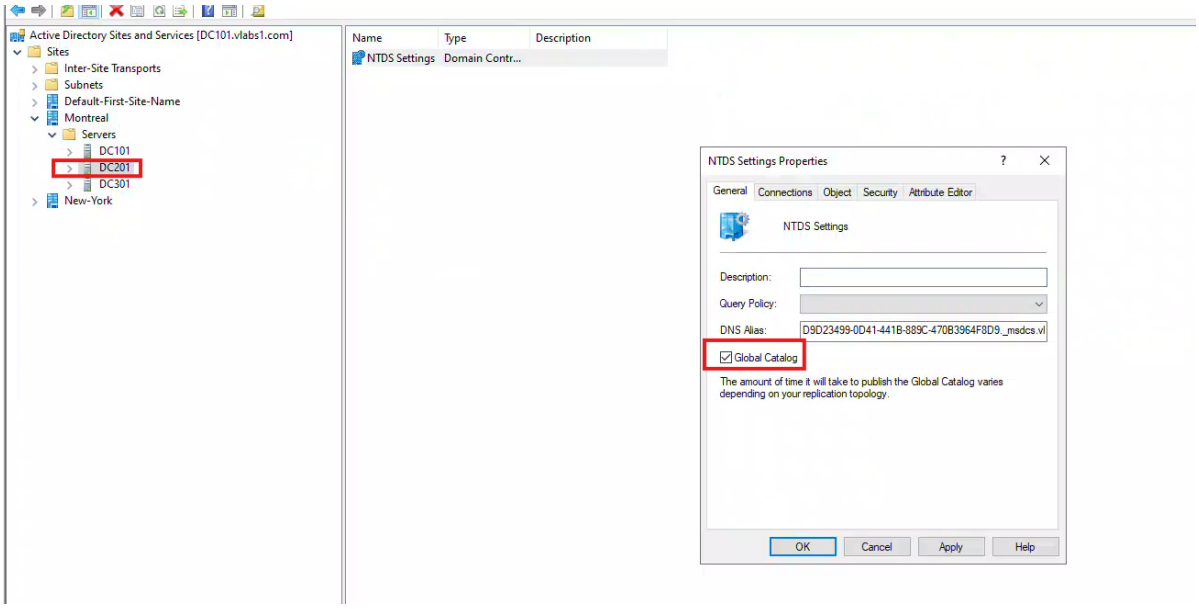
Since DC101 is not connected to the internet the NTP fails

- Enable the **Global Catalog** role.

Open **Active Directory Sites and Services**

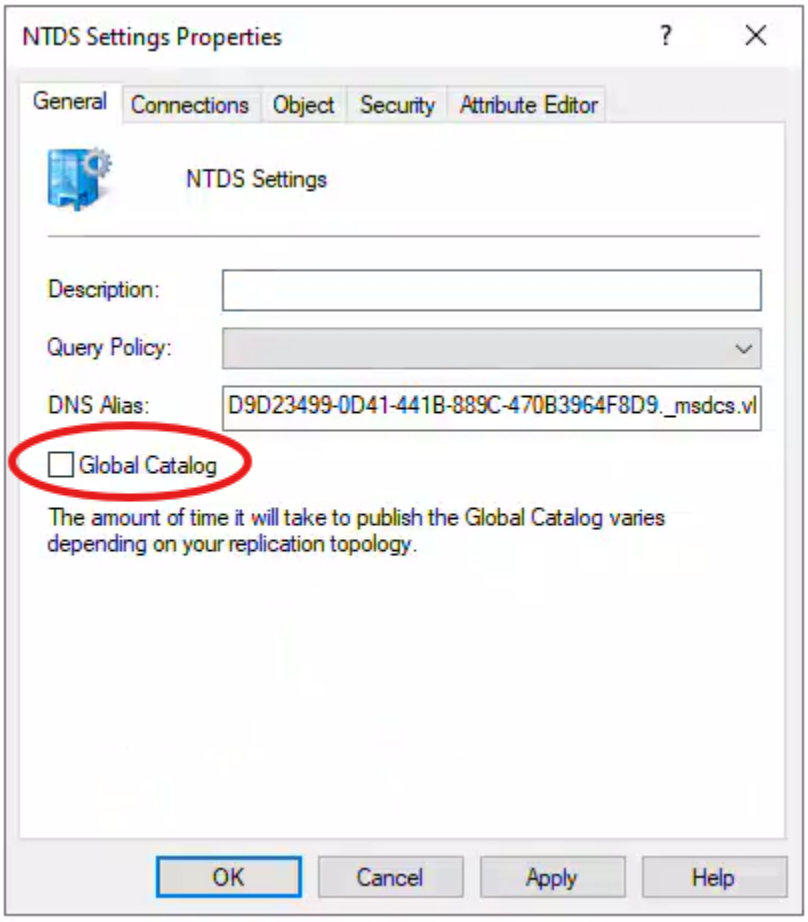
Navigate to: Sites > Montreal > Servers > DC201 > NTDS Settings

1. Right-click **NTDS Settings** > Properties
2. Check the box: **Global Catalog**



- Return to **DC101**, use the **GUI** to **disable** the **Global Catalog** on **DC201.**

1. Open **Active Directory Sites and Services**
2. Navigate to: Sites > Montreal > Servers > DC201 > NTDS Settings
3. Right-click **NTDS Settings** > Properties
4. **Uncheck** the box for **Global Catalog**


NTDS Settings Properties
General
Connections
Object
Security
Attribute Editor
NTDS Settings
Description:
Query Policy:
DNS Alias:
D9D23499-0D41-441B-889C-470B3964F8D9._msdcs.vl
Global Catalog
The amount of time it will take to publish the Global Catalog varies depending on your replication topology.
OK
Cancel
Apply
Help