

Project: Active Directory & Network Infrastructure Deployment for Centralized Management

Executive Summary

This project demonstrates the end-to-end deployment and configuration of a robust Active Directory domain environment, complete with essential network services (DHCP, NAT/Routing) to support centralized user authentication, resource management, and internet connectivity for client machines. Utilizing a Windows Server Domain Controller, the project established a fully functional domain, facilitated automated IP addressing, enabled internet access for isolated clients, and streamlined user provisioning. This initiative showcases strong capabilities in server administration, network services, and Active Directory management.

1. Project Objectives

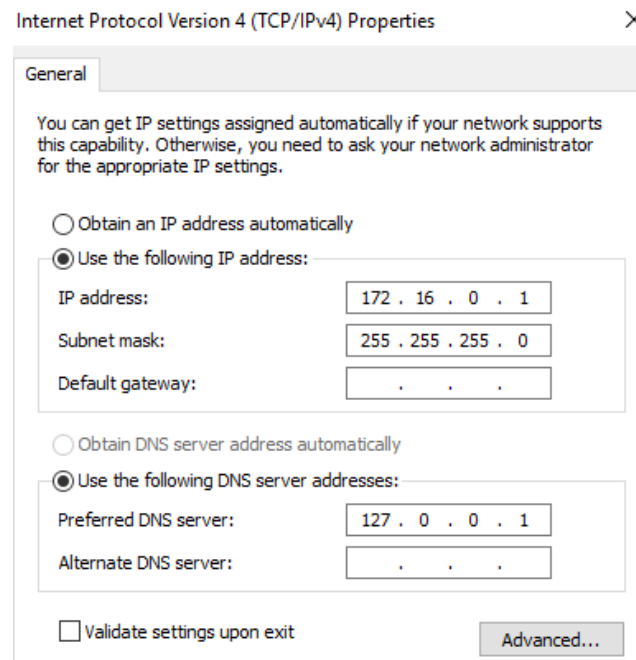
- **Establish a Centralized Authentication & Management System:** Deploy and configure Active Directory Domain Services (ADDS) to enable centralized user authentication, authorization, and resource management within a custom domain.
- **Provide Automated Network Services:** Configure DHCP to dynamically assign IP addresses to client machines, ensuring efficient network provisioning.
- **Enable Internet Connectivity for Internal Clients:** Implement NAT/Routing services to allow clients on an isolated internal network to access the internet securely through the Domain Controller.
- **Streamline User & Computer Management:** Demonstrate effective management of domain users and client computer objects within Active Directory.
- **Validate End-to-End Functionality:** Confirm seamless integration and operation of all deployed services, from IP assignment to domain login and internet access.

2. Architectural Design & Core Infrastructure Setup

The foundation of this project involved deploying virtual machines on a chosen virtualization platform (VirtualBox) to simulate a complete network environment.

- **2.1 Domain Controller (DC) Provisioning:**

- A Windows Server operating system (with Desktop Experience for streamlined management) was provisioned to serve as the foundational Domain Controller.
- An administrative account was secured with a strong password.
- **2.2 Network Adapter Configuration:**
 - The DC was equipped with two distinct network adapters for segmented connectivity:
 - **External (NAT) Adapter:** Configured to provide internet access to the DC itself and act as the egress point for client internet traffic.
 - **Internal Network Adapter:** Dedicated to establishing the isolated internal domain network, ensuring clients could only communicate via the DC.
 - Network adapters were descriptively renamed for ease of identification (_INTERNET_ and X_Internal_X).
 - The **Internal Network Adapter** was assigned a static IP address within a chosen private subnet (172.16.0.1/24). Its DNS server was configured to point to itself (127.0.0.1), establishing it as the authoritative DNS server for the domain.

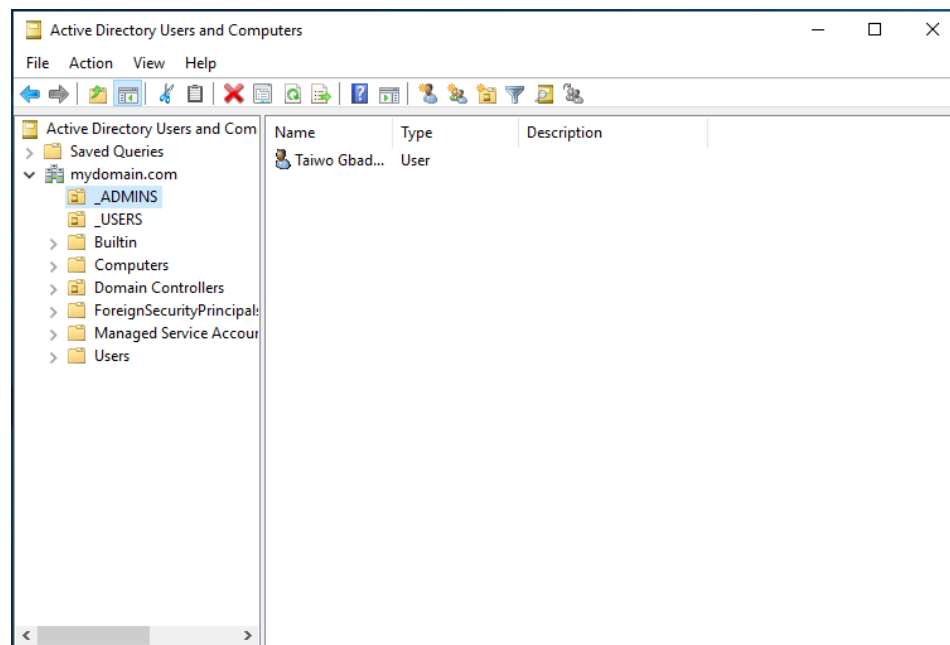


DC Internal Network IP

3. Core Services Deployment & Configuration

Key network and domain services were systematically deployed and configured on the Domain Controller to support the network infrastructure.

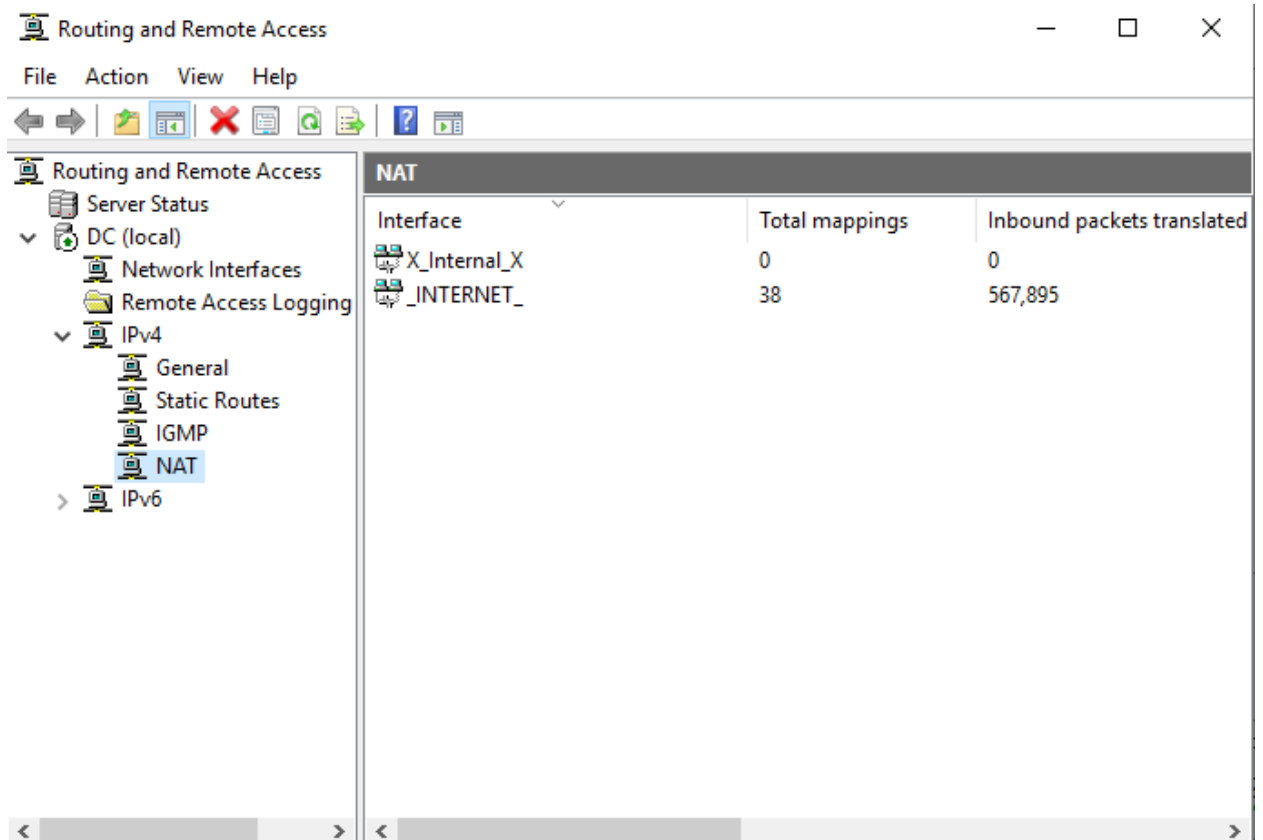
- **3.1 Active Directory Domain Services (ADDS) Deployment:**
 - The ADDS role was installed via Server Manager's "Add Roles and Features Wizard."
 - The server was then promoted to a Domain Controller within a new forest, establishing a new Active Directory domain (mydomain.com). This action automatically configured the DC as the primary DNS server for the domain.
- **3.2 Centralized User & Group Management:**
 - Within "Active Directory Users and Computers" (ADUC), a new **Organizational Unit (OU)** was created to logically structure domain resources.
 - Dedicated **administrative groups** were established within this OU, adhering to the principle of least privilege.
 - New user accounts were created within these groups, including a personal administrator account, demonstrating proper delegation and access control.



Active Directory Users and Computers – Admin

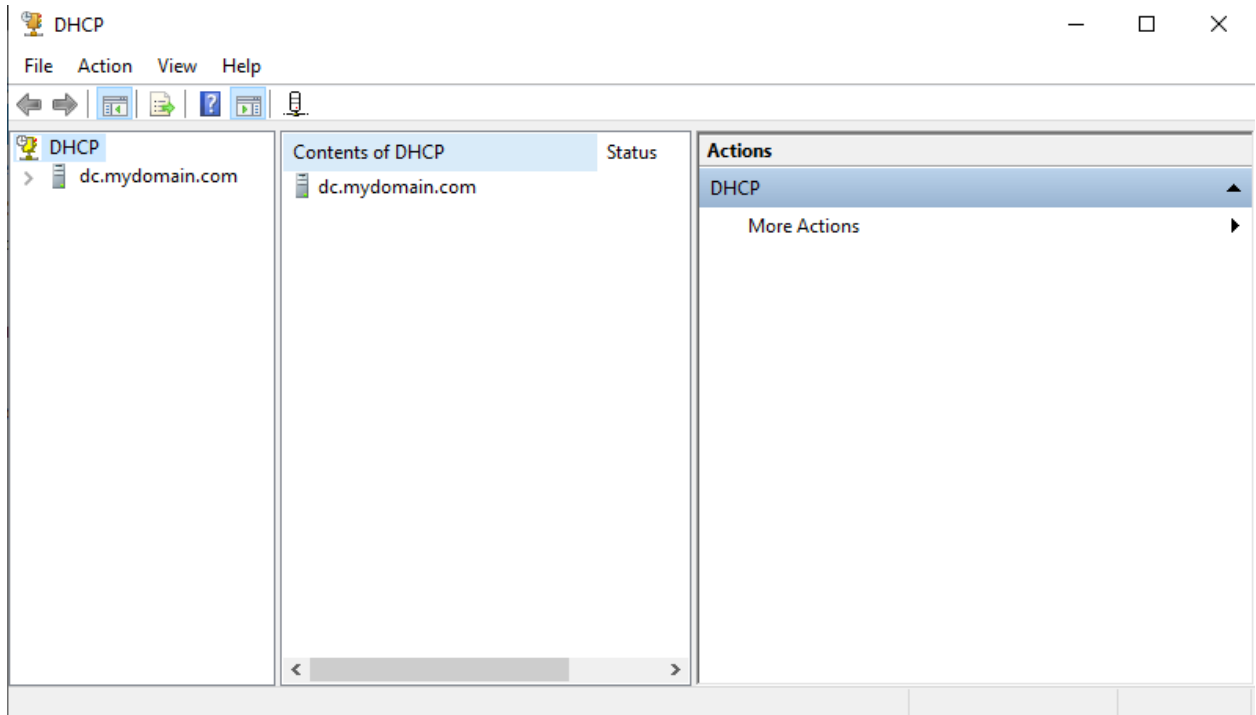
- **3.3 Routing and Remote Access Service (RRAS) / Network Address Translation (NAT) Implementation:**
 - The Remote Access role (specifically the Routing role service) was installed on the DC.

- RRAS was enabled and configured for **Network Address Translation (NAT)**. The external (NAT-connected) network adapter was selected as the internet-facing interface, allowing internal clients to share the DC's internet connection.

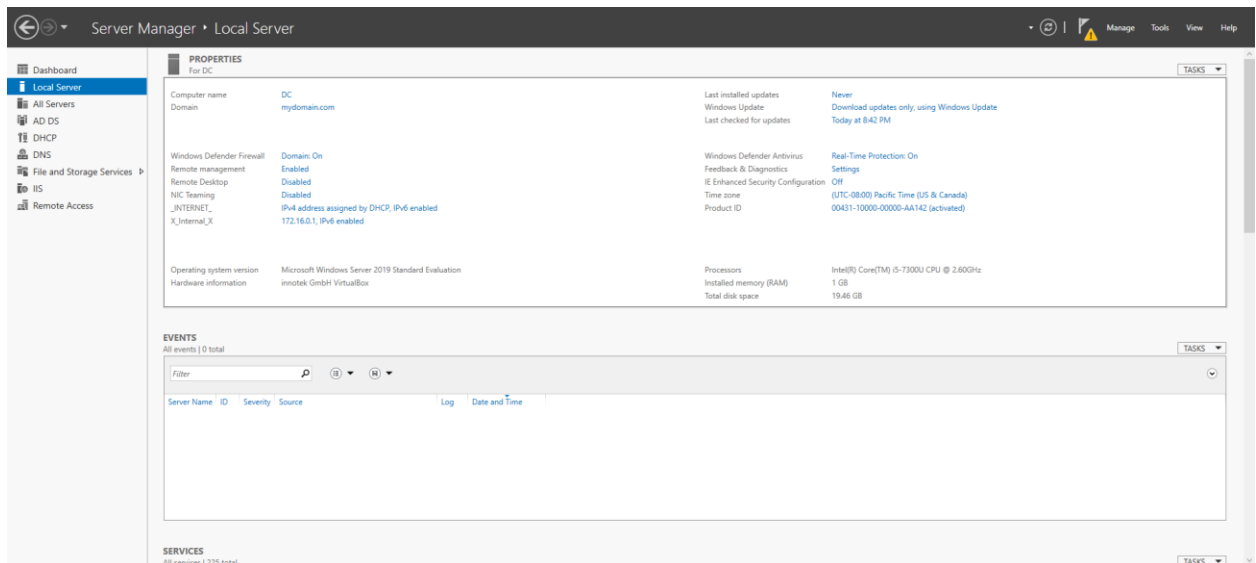


Routing and Remote Access Console (RRAS) showing NAT configuration

- **3.4 Dynamic Host Configuration Protocol (DHCP) Server Setup:**
 - The DHCP Server role was installed and configured on the DC.
 - A **new DHCP scope** was created, named intuitively after its IP range (172.16.0.100-200).
 - The DC's internal IP address (172.16.0.1) was specified as the **router/default gateway** for clients within this scope, directing their internet bound traffic through the DC's NAT service.



DHCP Management Console of configured scope and router option



Server manager Dashboard

- **3.5 Scalable User Provisioning:**
 - A text file containing a list of first and last names was prepared.
 - A **PowerShell script** was developed and executed to efficiently create multiple new domain user accounts in bulk, demonstrating automation skills for large-scale user management.

```

1 $PASSWORD_FOR_USERS = "Password1"
2 $USER_FIRST_LAST_LIST = Get-Content .\names.txt
3
4 $password = ConvertTo-SecureString $PASSWORD_FOR_USERS -AsPlainText -Force
5 New-ADOrganizationalUnit -Name _USERS -ProtectedFromAccidentalDeletion $false
6
7 foreach ($n in $USER_FIRST_LAST_LIST) {
8     $first = $n.Split(" ")[0].ToLower()
9     $last = $n.Split(" ")[1].ToLower()
10    $username = "$($first.Substring(0,1))$($last)".ToLower()
11    Write-Host "Creating user: $($username)" -BackgroundColor Black -ForegroundColor Cyan
12
13    New-AdUser -AccountPassword $password `
14        -GivenName $first `
15        -Surname $last `
16        -DisplayName $username `
17        -Name $username `
18        -EmployeeID $username `

```

Creating user: rsmithrick
Creating user: fbokaw
Creating user: eburgener
Creating user: lsever
Creating user: isoliman
Creating user: jfordham
Creating user: usargent
Creating user: vgrube
Creating user: snicastro
Creating user: rrector
Creating user: dmowrey
Creating user: tdelprione
Creating user: ehovey
Creating user: dfrausto
Creating user: msingh
Creating user: gdarville
Creating user: lmciver
Creating user: kbutcher
Creating user: mchestnut
Creating user: nlefevre
Creating user: cwestover
Creating user: vezzelli
Creating user: dannunziata
Creating user: smitschke
Creating user: kwarden
Creating user: mrapar
Creating user: dwillmore
Creating user: tbasilio
Creating user: bgilmer
Creating user: cconboy
Creating user: mhakes
Creating user: arettig

PS C:\users\atgbadamosi\desktop\AD_PS-master>

Powershell script to automate user creation

Name	Type	Description
tellington	User	
tellsworth	User	
tfenderson	User	
tfu	User	
tgbadamosi	User	
tgoggans	User	
tgrigg	User	
thaug	User	
thultman	User	
tjanuary	User	
tjoines	User	
tkarter	User	
tkopczynski	User	
tkruchten	User	
tkulesza	User	
tlamers	User	
tlavalle	User	
tlirette	User	
tlitchford	User	
tlongacre	User	
tmaniscalco	User	

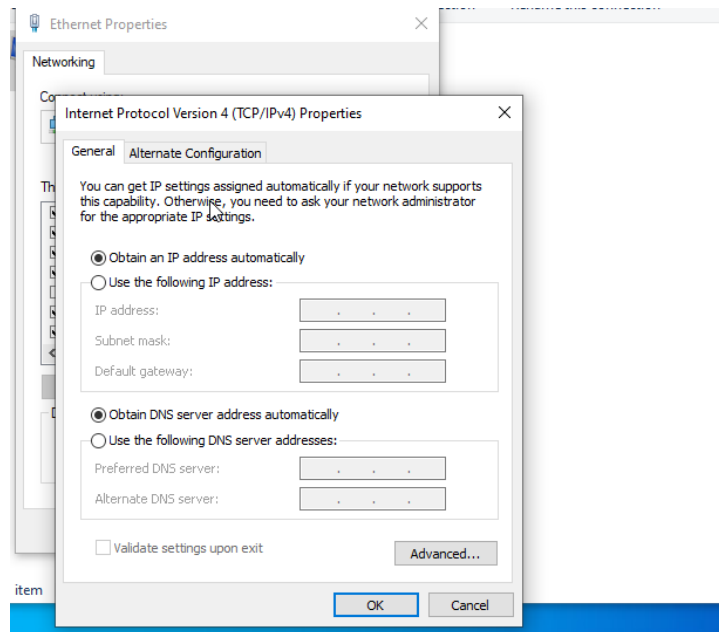
Active Directory Users and Computers – Admin

4. Client Integration & Verification

A Windows 10 client machine was provisioned and integrated into the newly established domain to validate end-to-end functionality.

- **4.1 Client Network Configuration:**

- The Windows 10 client VM was configured with a single **Internal Network adapter**, aligning it with the DC's internal LAN segment.
- The client was set to automatically obtain its IP address via DHCP, successfully receiving an address from the DHCP server configured on DC.



```
Command Prompt
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\tgbadamosi>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

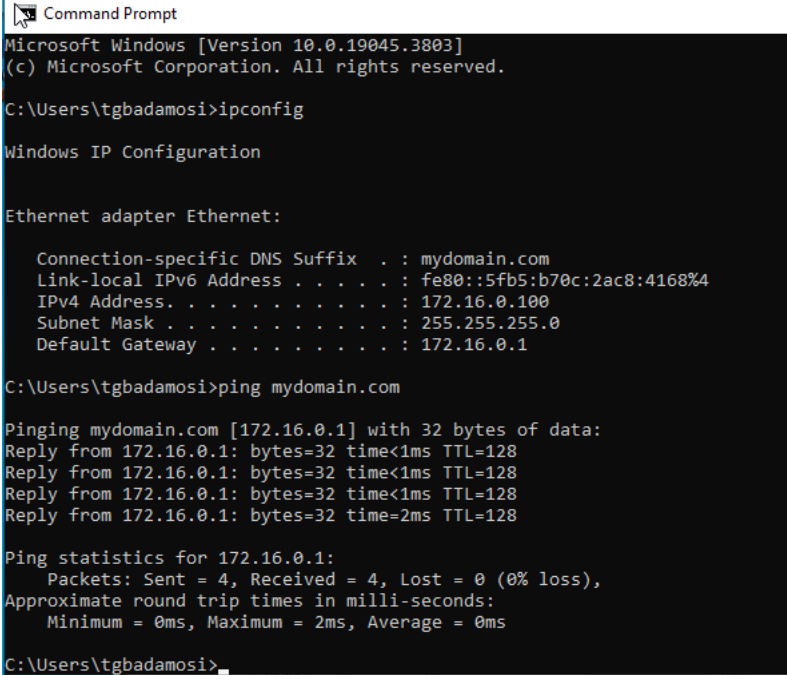
    Connection-specific DNS Suffix  . : mydomain.com
    Link-local IPv6 Address . . . . . : fe80::5fb5:b70c:2ac8:4168%4
    IPv4 Address. . . . . : 172.16.0.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.0.1

C:\Users\tgbadamosi>
```

Client IP configuration

- **4.2 Internet Connectivity Verification:**

- Internet connectivity on the client was verified by successfully pinging the DC's domain name (ping mydomain.com), confirming DNS resolution and internal network routing.
- Further internet access was confirmed by Browse external websites.



```
Command Prompt
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\tgbadamosi>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : mydomain.com
    Link-local IPv6 Address . . . . . : fe80::5fb5:b70c:2ac8:4168%4
    IPv4 Address. . . . . : 172.16.0.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.0.1

C:\Users\tgbadamosi>ping mydomain.com

Pinging mydomain.com [172.16.0.1] with 32 bytes of data:
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time=2ms TTL=128

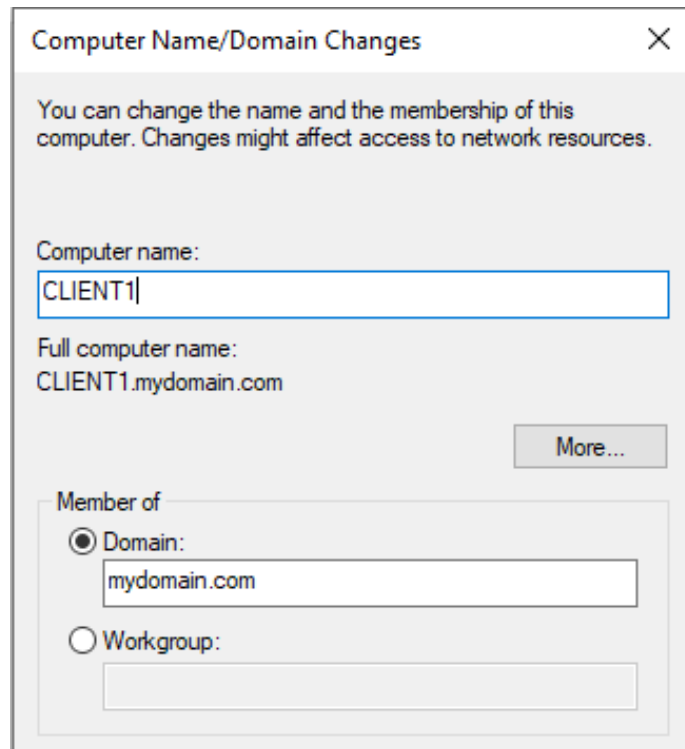
Ping statistics for 172.16.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\tgbadamosi>
```

Client able to ping domain server, and able to connect to internet

- **4.3 Domain Join & User Authentication:**

- The client PC's name was updated using advanced system settings to adhere to domain naming conventions.
- The client was then successfully joined as a member of the newly created domain (mydomain.com).
- Following the domain join, successful login to the client machine was performed using a newly created domain user account, confirming centralized authentication and Active Directory integration.



5. Key Learnings & Demonstrated Capabilities

This project provided extensive hands-on experience and demonstrated proficiency in:

- **Active Directory Domain Services (ADDS):** Installation, promotion of Domain Controllers, forest and domain creation, OU structuring, and user/group management.
- **Network Infrastructure:** Configuration of internal and external network adapters, static IP addressing, DNS, and subnetting.
- **Dynamic Host Configuration Protocol (DHCP):** Setting up scopes, assigning IP ranges, and configuring gateway/DNS options for clients.
- **Network Address Translation (NAT) & Routing:** Implementing internet sharing for isolated internal networks using RRAS.
- **PowerShell Scripting:** Automating administrative tasks, specifically bulk user creation, to enhance efficiency.
- **Windows Server Administration:** Core server management, roles and features installation, and system configuration.
- **Client-Server Integration:** Seamlessly integrating client machines into a domain environment and verifying functionality.
- **Troubleshooting:** Identifying and resolving connectivity, DNS, and authentication issues within a complex network setup.

6. Conclusion

This Active Directory and Network Infrastructure Deployment project successfully established a robust, centrally managed network environment. The integration of ADDS, DHCP, and NAT/Routing services provided a comprehensive solution for user management, automated IP assignment, and controlled internet access for internal clients. This initiative stands as a strong testament to practical skills in foundational IT infrastructure deployment, crucial for any enterprise or secured network environment.