Active Directory Lab Pro: Mastering AD Administration

Author: Harshitkumar R. Panwala

Date: August 2, 2024

Documentation

Introduction

In this project, we're setting up an Active Directory (AD) environment using Windows Server 2019 and Windows 10 virtual machines in Oracle VirtualBox. Our goal is to create a domain controller, configure DNS and DHCP services, and integrate a client machine into the domain. This guide offers a detailed, step-by-step walkthrough of the setup process, covering configurations and validations.

Objectives

- **Active Directory Setup:** Install and configure Active Directory Domain Services (AD DS) on a Windows Server 2019 VM.
- **DNS and DHCP Configuration:** Set up DNS for internal network resolution and DHCP for IP address allocation.
- **Client Integration:** Connect a Windows 10 client VM to the domain, and verify connectivity and domain membership.

Description

Key Features

- **Active Directory Installation:** Deploy and configure AD DS on Windows Server 2019.
- **DNS and DHCP Configuration:** Set up DNS and DHCP services to manage internal network addressing.
- **Client Domain Integration:** Add a Windows 10 client to the domain and check network and domain connectivity.

Project Components

- **Windows Server 2019 VM:** This will act as the domain controller.
- **Windows 10 VM:** This will be the client machine connected to the domain.
- **Oracle VirtualBox:** The platform used for hosting the VMs.

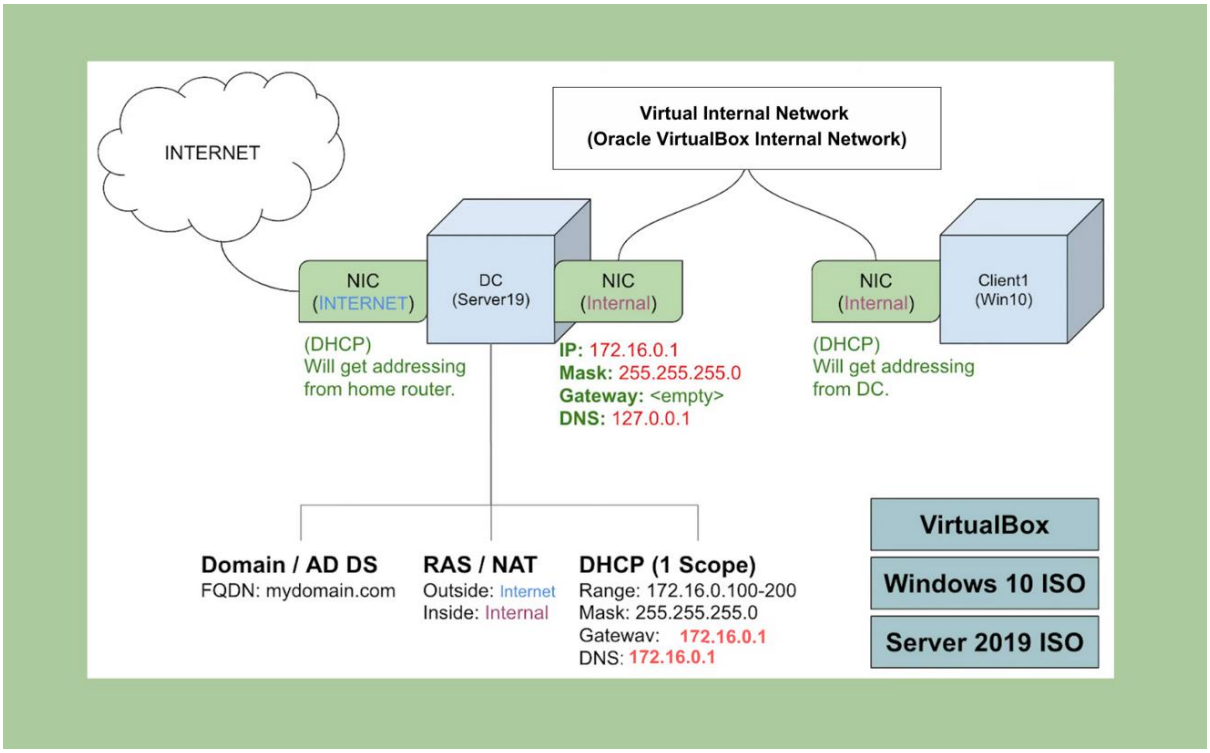
Setup and Usage

Prerequisites

- **Oracle VirtualBox** installed on your host machine.
- **Windows Server 2019 ISO** and **Windows 10 ISO**.
- Basic knowledge of IP addressing and networking.

Network Configuration

Network Diagram



Netwokr Adapter Setup

For Windows Server 2019 VM:

- **Adapter 1 (NAT):** Provides internet access through the host machine's network connection, useful for downloading updates and patches.
- **Adapter 2 (Internal Network):** Allows communication between the Windows Server and Windows 10 VMs without external exposure.

For Windows 10 Client VM:

- **Adapter 1 (Internal Network):** Connects to the internal network, allowing it to join the domain and communicate with the Windows Server VM.

Steps to Set Up Network Adapters

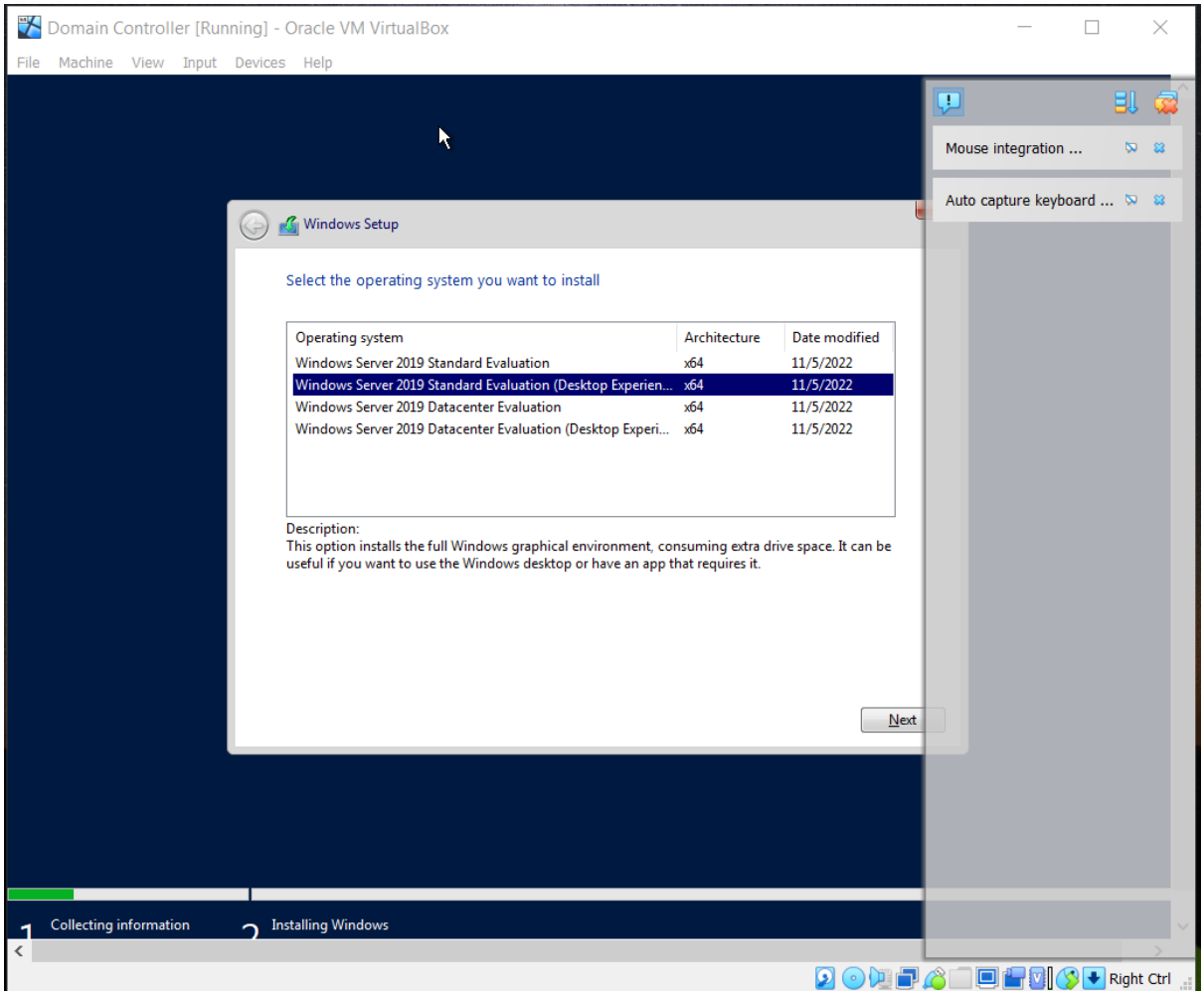
1. **Configure Network Adapters in VirtualBox:**
    - Windows Server VM:
        - **Adapter 1:** Set to **NAT**.
        - **Adapter 2:** Set to **Internal Network** and use a consistent network name (e.g., "IntNet").
    - **Windows 10 Client VM:**
        - **Adapter 1:** Set to **Internal Network** with the same network name ("IntNet").
2. **Finalize Network Settings on Windows Server VM:**
    - **Open Control Panel** -> **Network and Sharing Center** -> **Change adapter settings**.
    - **Right-click the internal network adapter** -> **Properties**.
    - **Set IP Configuration:**
        - **IP Address:** 172.16.0.1
        - **Subnet Mask:** 255.255.255.0
        - **Gateway:** None
        - **Preferred DNS Server:** 127.0.0.1
    - **Verify settings** with ipconfig and ping commands.

Walkthrough

Step 1: Create and Configure Windows Server 2019 VM

Set Up Windows Server 2019 VM:

- Create the VM in VirtualBox.
- Assign network settings: NAT for Adapter 1 and Internal Network for Adapter 2.
- Install Windows Server 2019 using the ISO file.
- Proceed to configure network settings and rename the PC as detailed below.



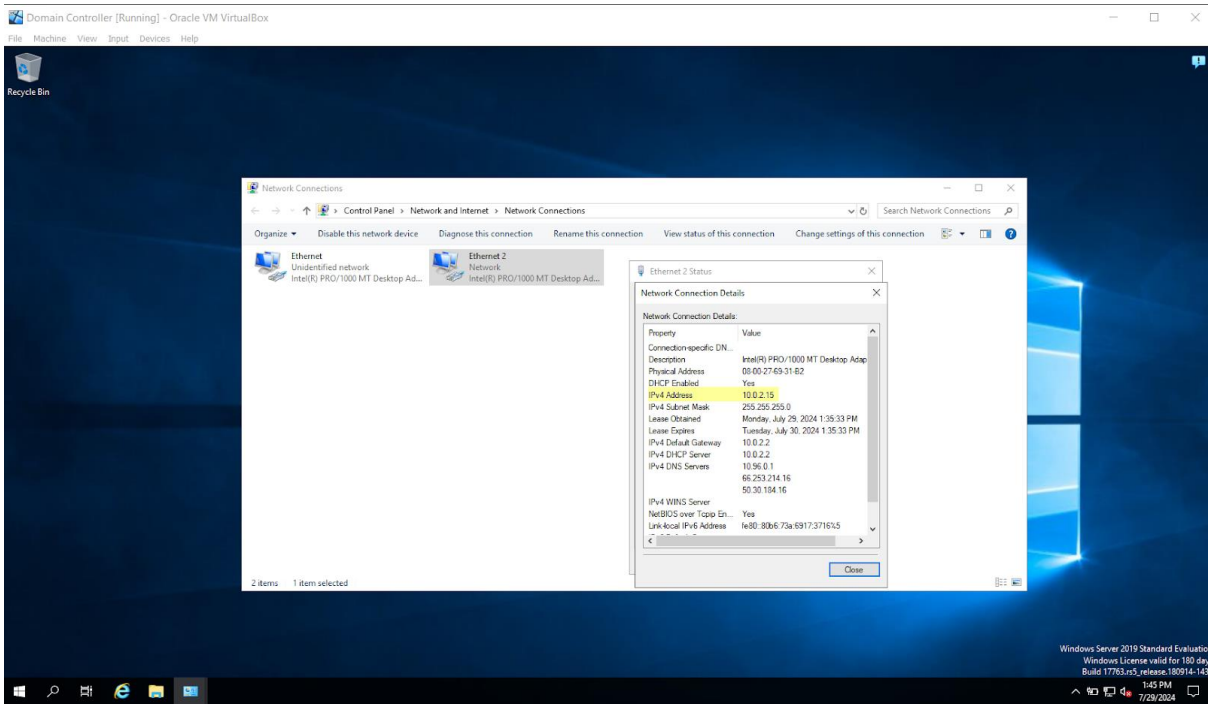
Step 2: Rename the PC and Configure Network Settings

Open System Properties and Rename the PC:

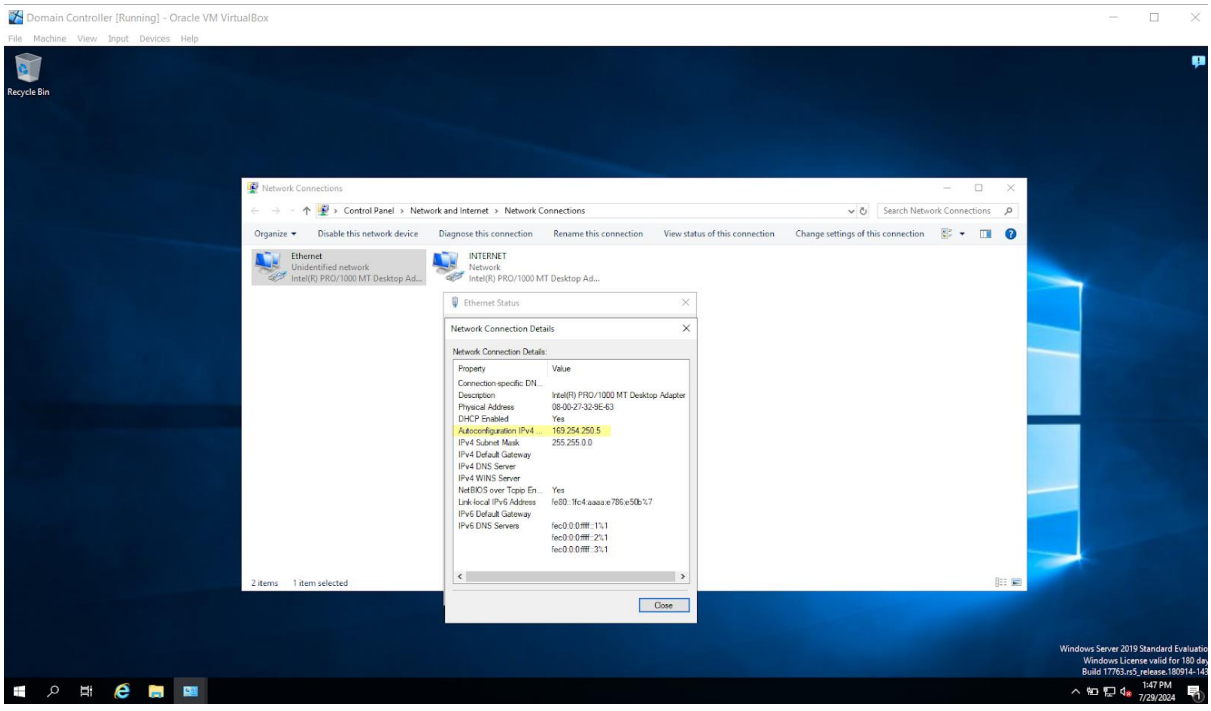
1. Go to **Start** and right-click **This PC**.
2. Select **Properties**.
3. Click on **Advanced system settings** on the left to open the **System Properties** window.
4. Go to the **Computer Name** tab and click on **Change...**.
5. In the **Computer Name/Domain Changes** dialog, enter a new name for the computer (e.g., `DomainController`) in the **Computer name** field.
6. **Change the Domain Name:**
    1. Click on **Domain** and enter `mydomain.com` to set the domain name.

Configure Network Adapters:

- **Rename Network Adapters:**
    - Open **Network Connections** by typing `ncpa.cpl` in the Start menu search bar and pressing Enter.
    - Right-click on each network adapter and select **Rename**.
    - Rename Adapter 1 to **INTERNET** (connected via NAT) and Adapter 2 to **INTERNAL** (connected to the internal network).



- **Configure Internal Network Adapter:**
  - Right-click on the **INTERNAL** adapter and select **Properties**.
  - In the **Ethernet Properties** window, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
  - Set the following IP address configuration:
    - **IP Address:** `172.16.0.1`
    - **Subnet Mask:** `255.255.255.0`
    - **Default Gateway:** Leave this blank. The Domain Controller itself will act as the gateway for internal network traffic.
  - In the **Preferred DNS server** field, enter `127.0.0.1` to ensure DNS queries are resolved locally by the Domain Controller.
  - Click **OK** to save the settings.
- **Internal Network Adapter's IP Issue:**
  - If you initially see an IP address starting with `169.x.x.x`, this indicates an automatic private IP address (APIPA) assigned because no DHCP server was available. This IP range is used by Windows when it cannot obtain an IP address from a DHCP server.
  - Ensure the **INTERNAL** adapter is configured correctly as mentioned above to resolve this issue.



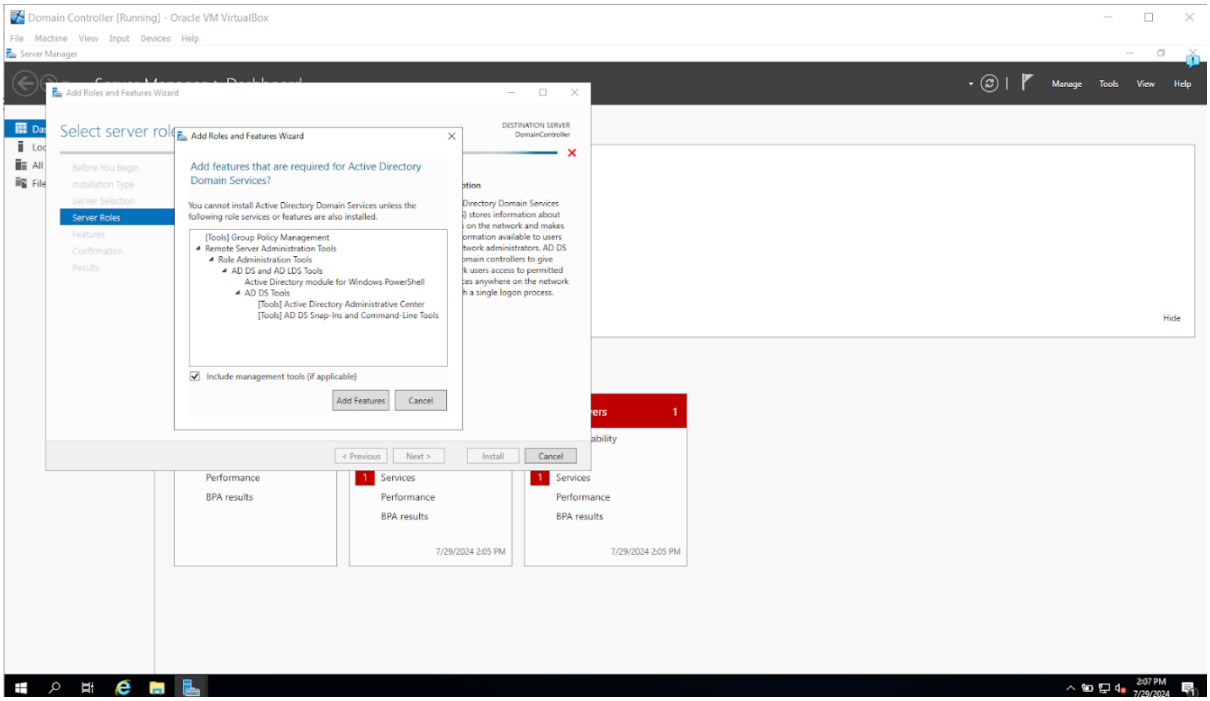
Restart the Machine:

- Restart the computer to ensure all changes are applied correctly.

Step 3: Install Active Directory Domain Services

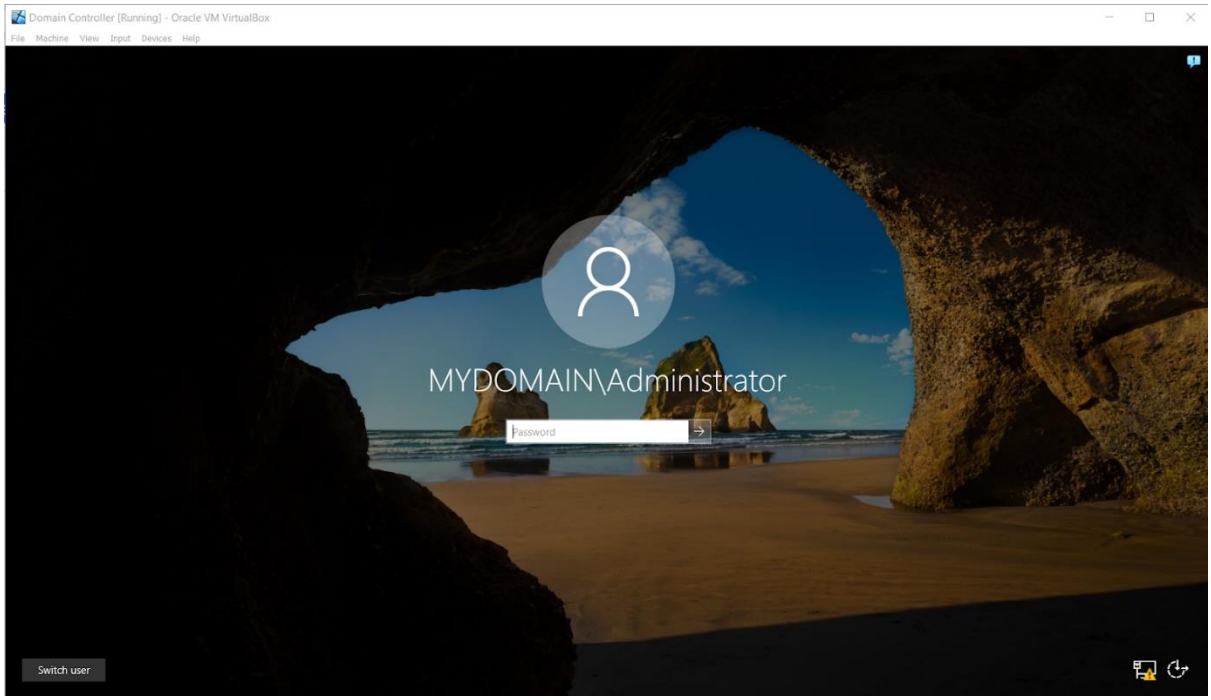
- **Add Roles and Features:**

    1. Open **Server Manager**.
    2. Go to **Manage** -> **Add Roles and Features**.
    3. Select **Active Directory Domain Services (AD DS)** and complete the installation.
    4. The server will restart to apply changes.



- **Verify Domain Change:**

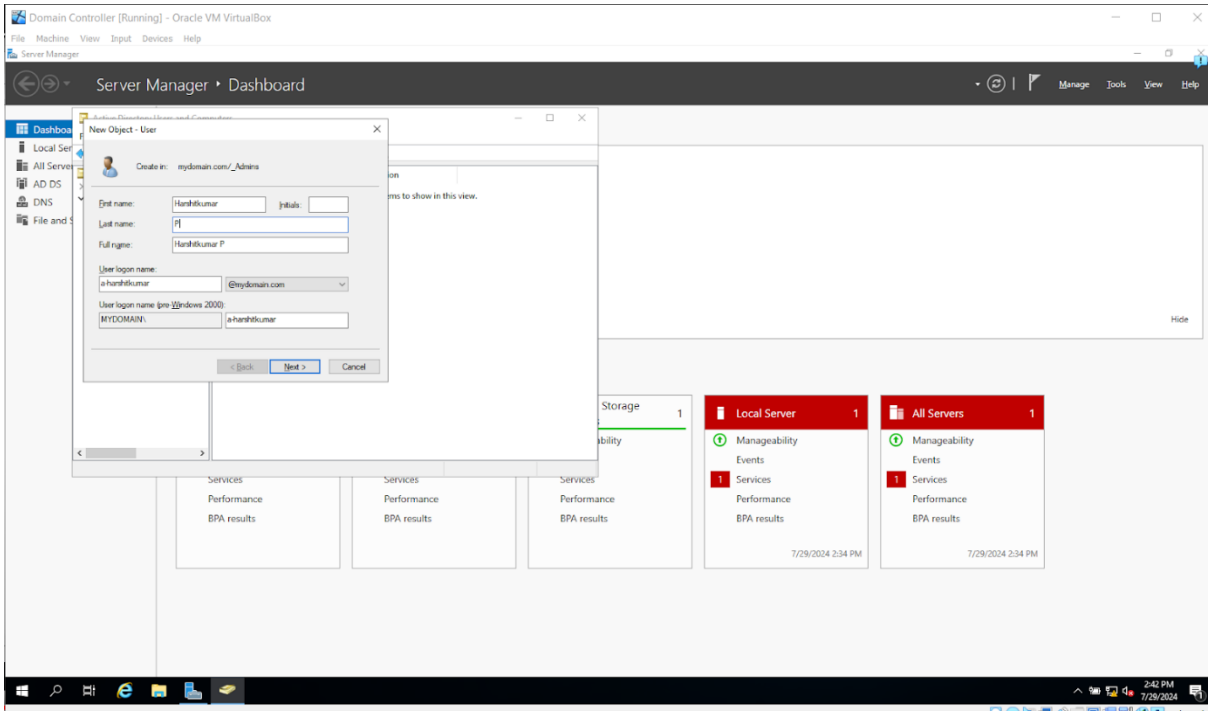
    Log in using `MYDOMAIN\Administrator` with the password `Password@123`.



Step 4: Create Active Directory Admin Account

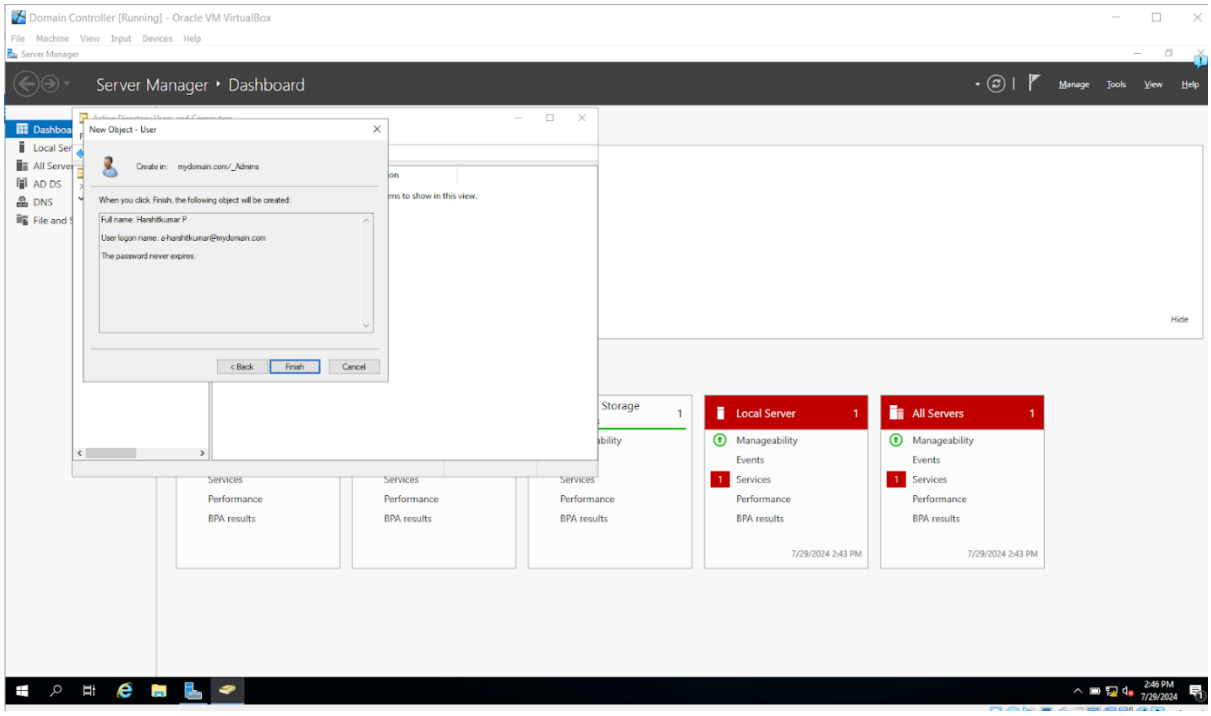
Create a New User Account:

- Open Windows Administrative Tools -> Active Directory Users and Computers.
- Create an Organizational Unit (OU) named _Admins.
- Within this OU, create a new user with the logon name a-harshitkumar.
- Set the password as Password@123 and uncheck all options except Password never expires (this is not the best practice but as we are doing it for the home lab so it’s ok).



Add User to Domain Admins Group:

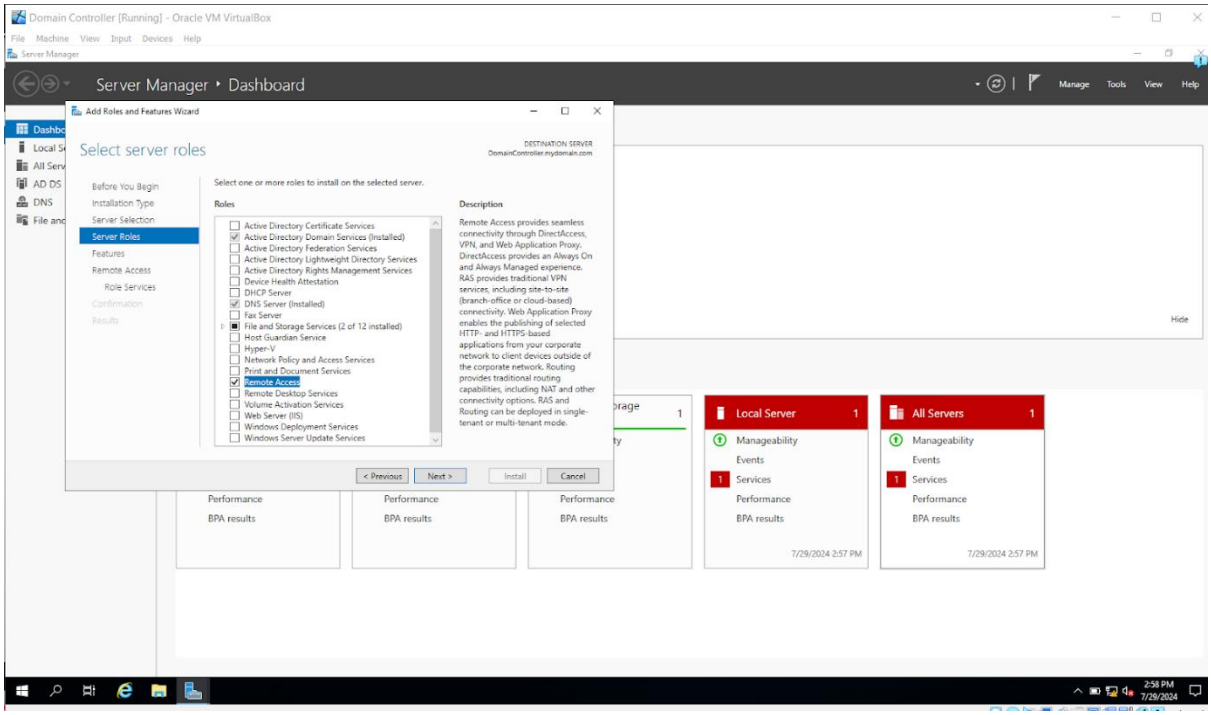
- Add the new user to the Domain Admins group.
- Log out of the default Administrator account and log in with the new account a-harshitkumar.



Step 5: Configure Remote Access and Routing

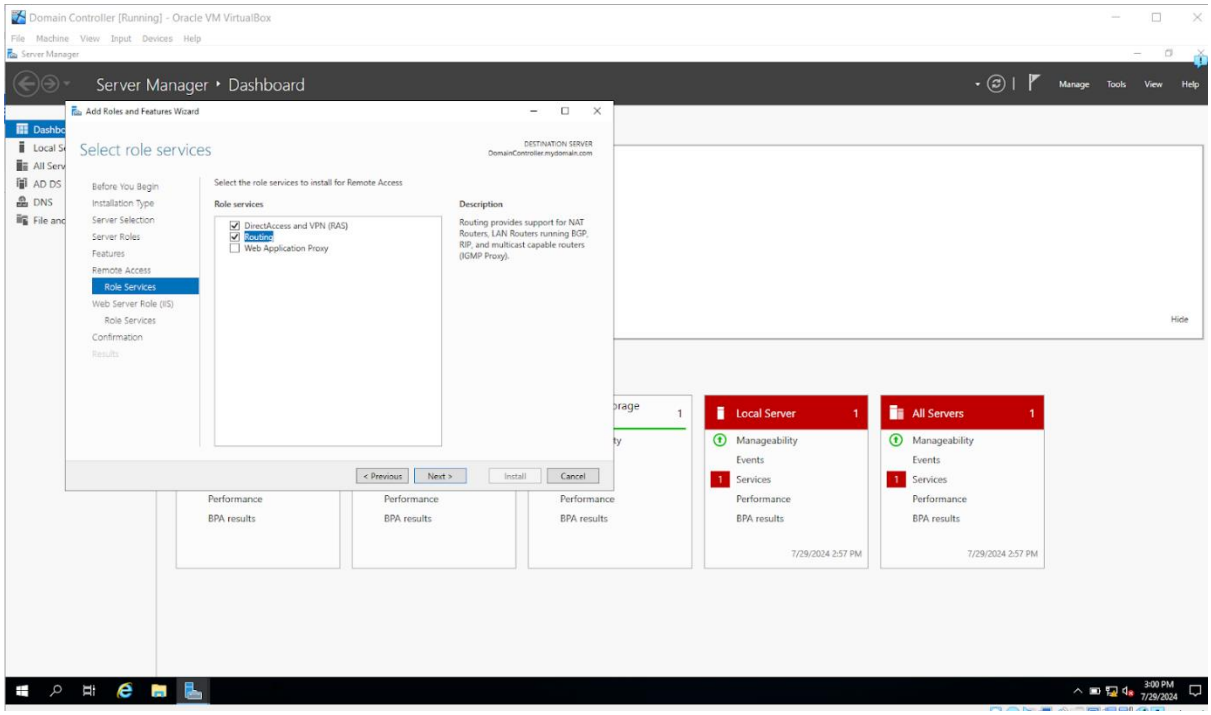
Add Remote Access Role:

1. Open **Server Manager**.
2. Go to **Manage** -> **Add Roles and Features**.
3. Select **Remote Access** and add **RAS and VPN** and **Routing**.
4. Click **Next** and **Install**.



Set Up Routing and Remote Access:

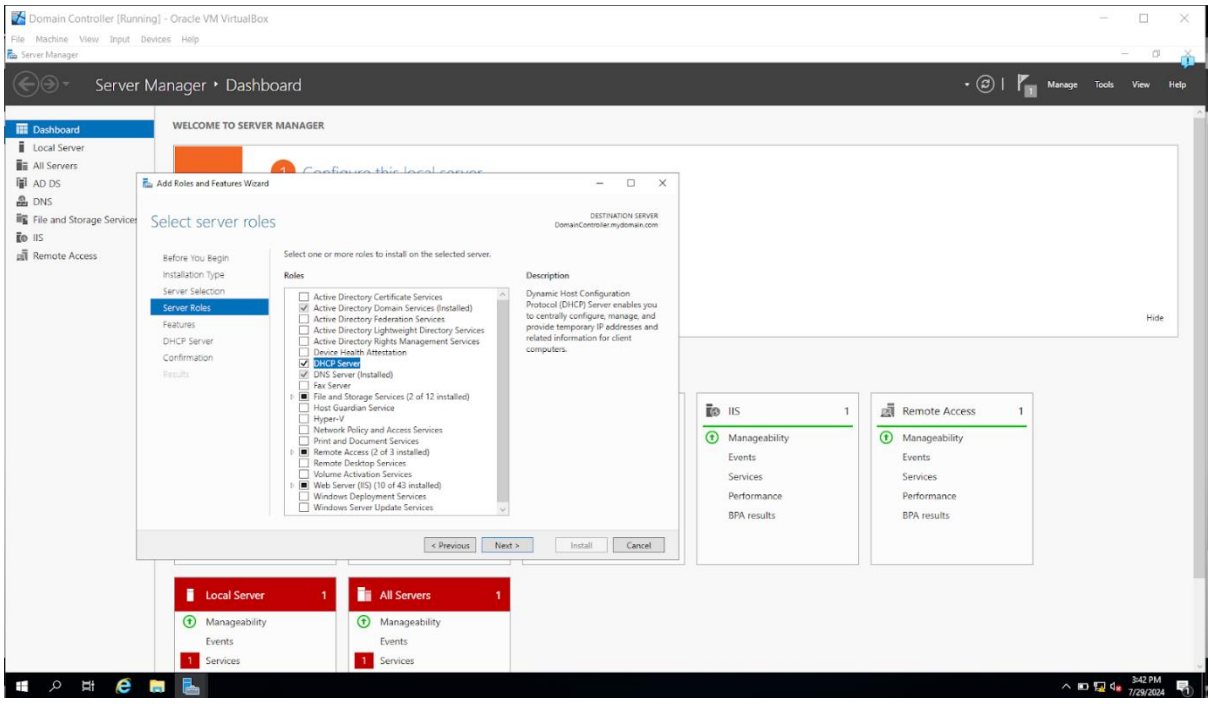
1. Go to **Tools** -> **Routing and Remote Access**.
2. Right-click on **DomainController** and select **Configure and Enable Routing and Remote Access**.
3. Choose **NAT** to allow the server to connect to the internet with one IP address. Ensure the correct interface (**INTERNET**) is selected.



Step 6: Install and Configure DHCP

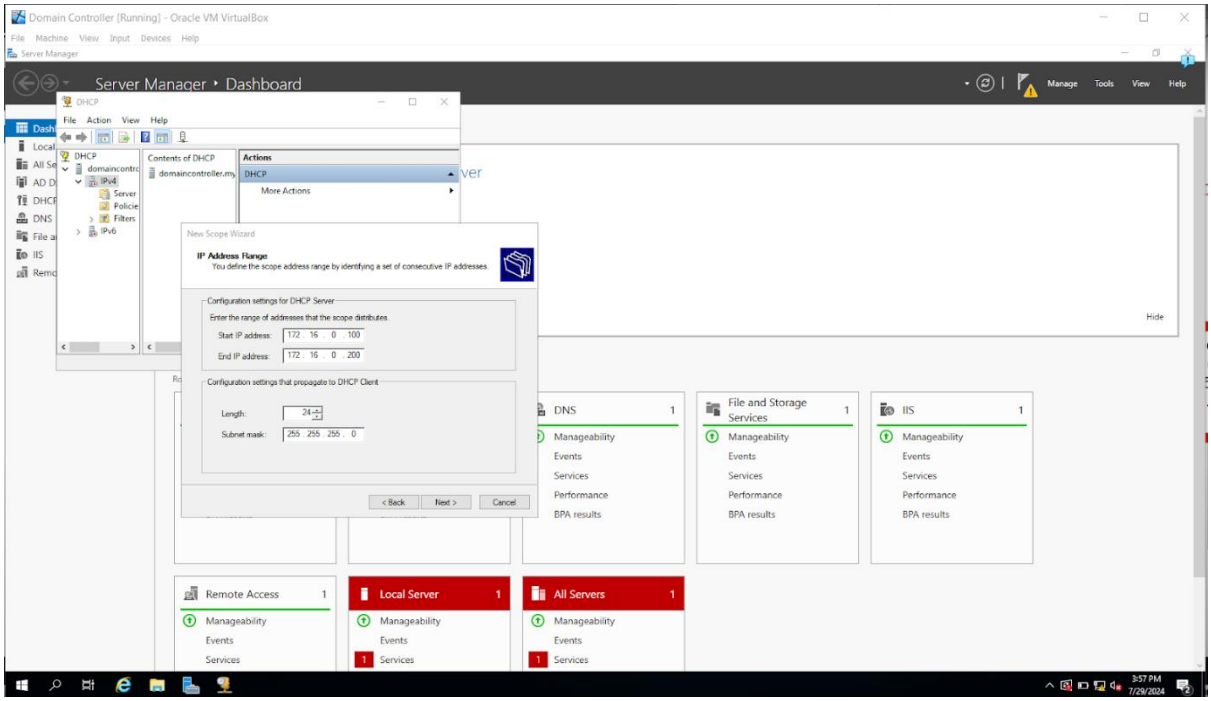
Add DHCP Role:

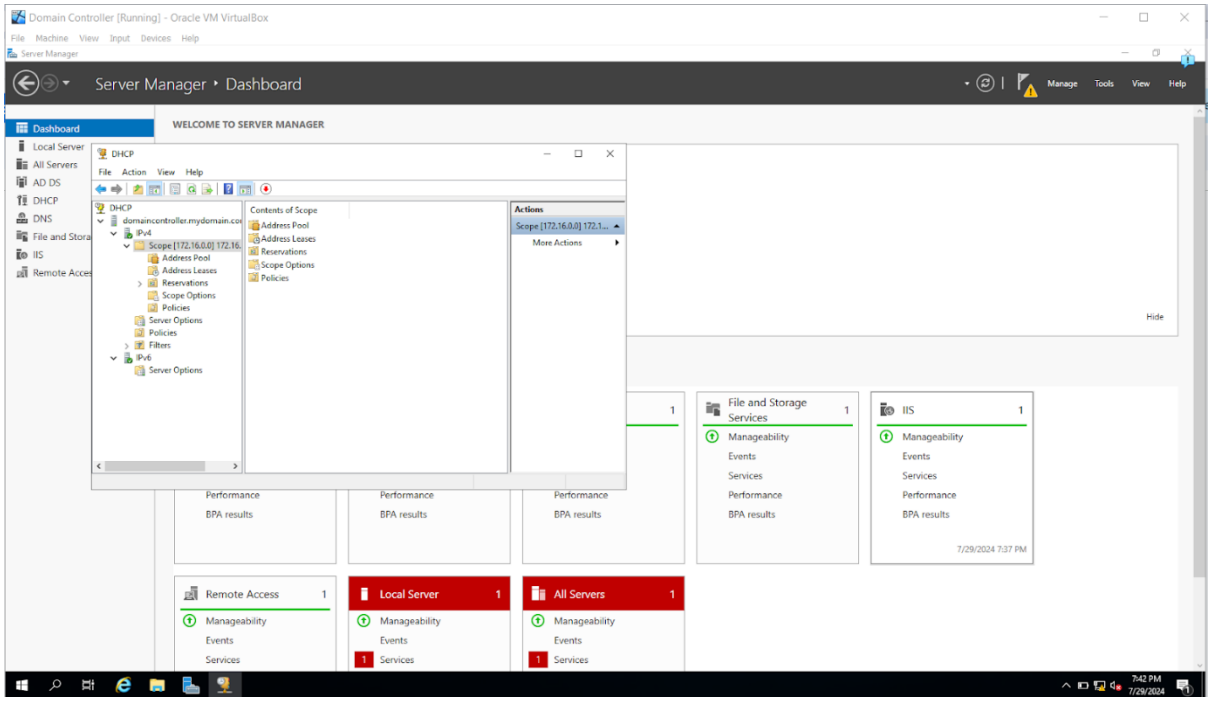
1. Go to **Server Manager** -> **Manage** -> **Add Roles and Features**.
2. Select **DHCP Server** and complete the installation.



Configure DHCP:

1. Open **Tools** -> **DHCP**.
2. Set the lease duration to 1 day (or adjust as needed) and configure the DHCP scope to allocate IP addresses to up to 100 users.

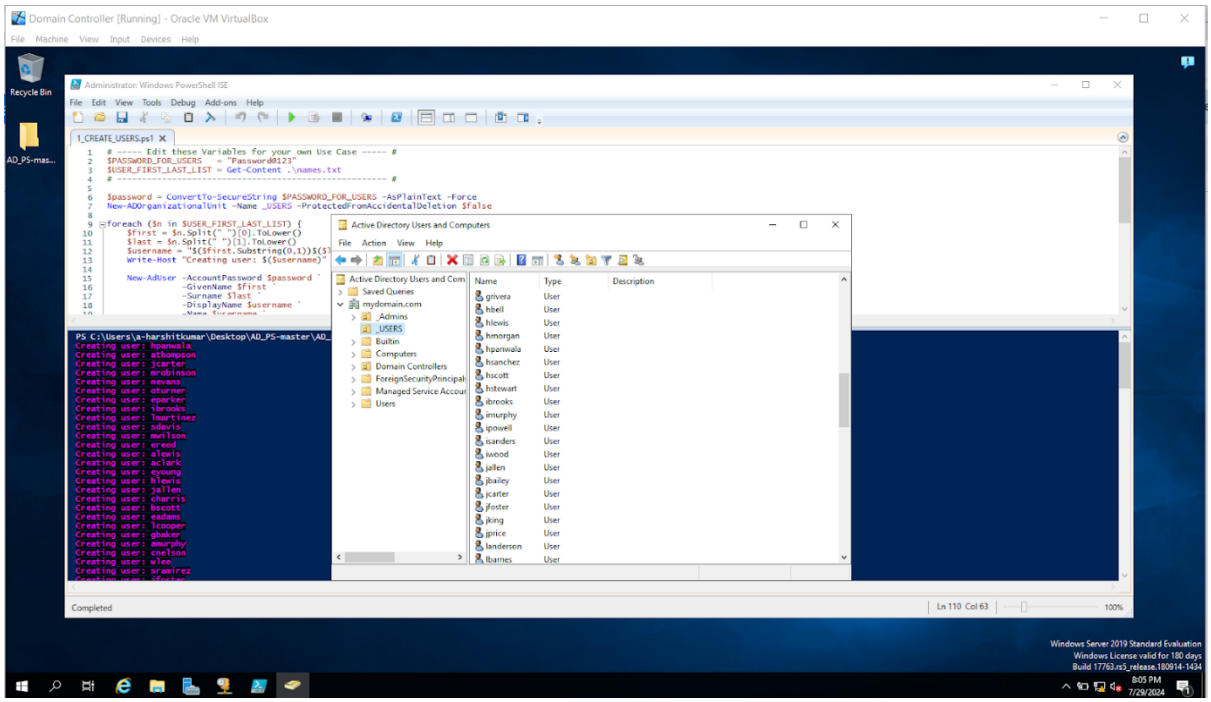




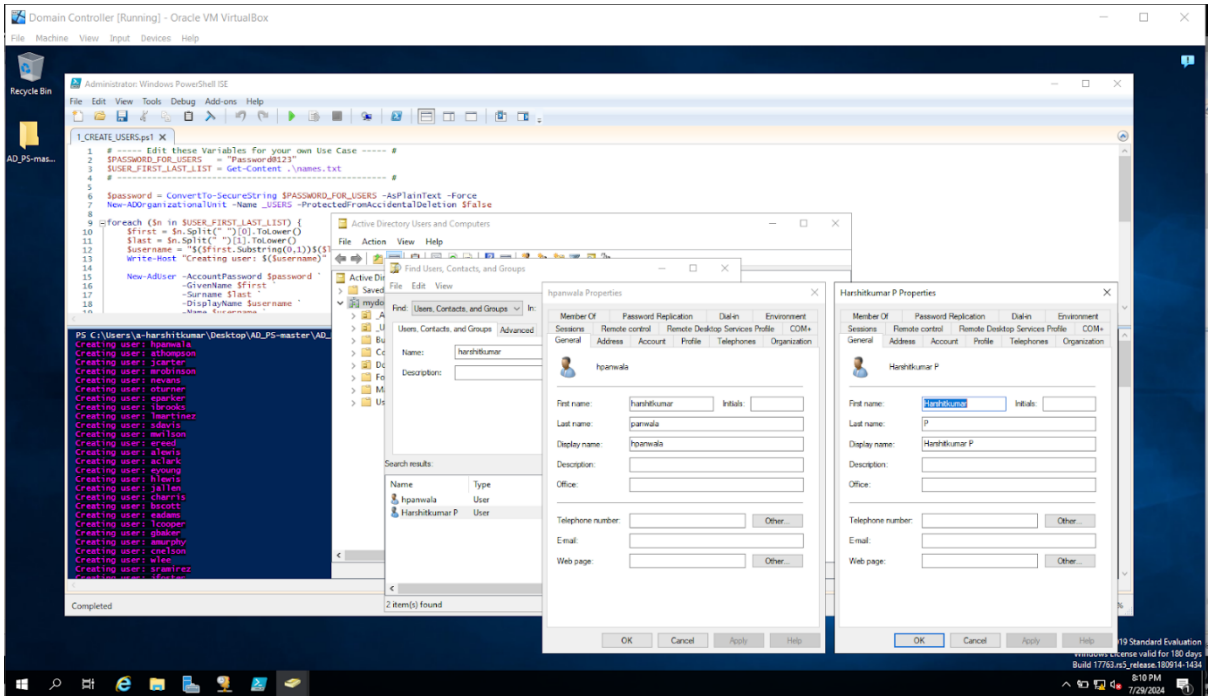
Step 7: Create Bulk User Accounts Using PowerShell

Generate User Accounts:

1. Prepare a names.txt file containing 100 names. Include your name at the top and generate 99 additional random names.
2. Use a PowerShell script to create user accounts based on the names in names.txt. The usernames will use the first letter of the first name and the full last name, with the password Password@123.
3. Ensure all users have the same password, which can be changed during the first login but is disabled in this lab environment for simplicity. Password expiration is also disabled for the same reason.



4. If you search for your first name and don't find the user created through the PowerShell script, simply refresh the **mydomain** in Active Directory and try again.



Step 8: Set Up and Connect Windows 10 Client

Create and Configure Windows 10 VM:

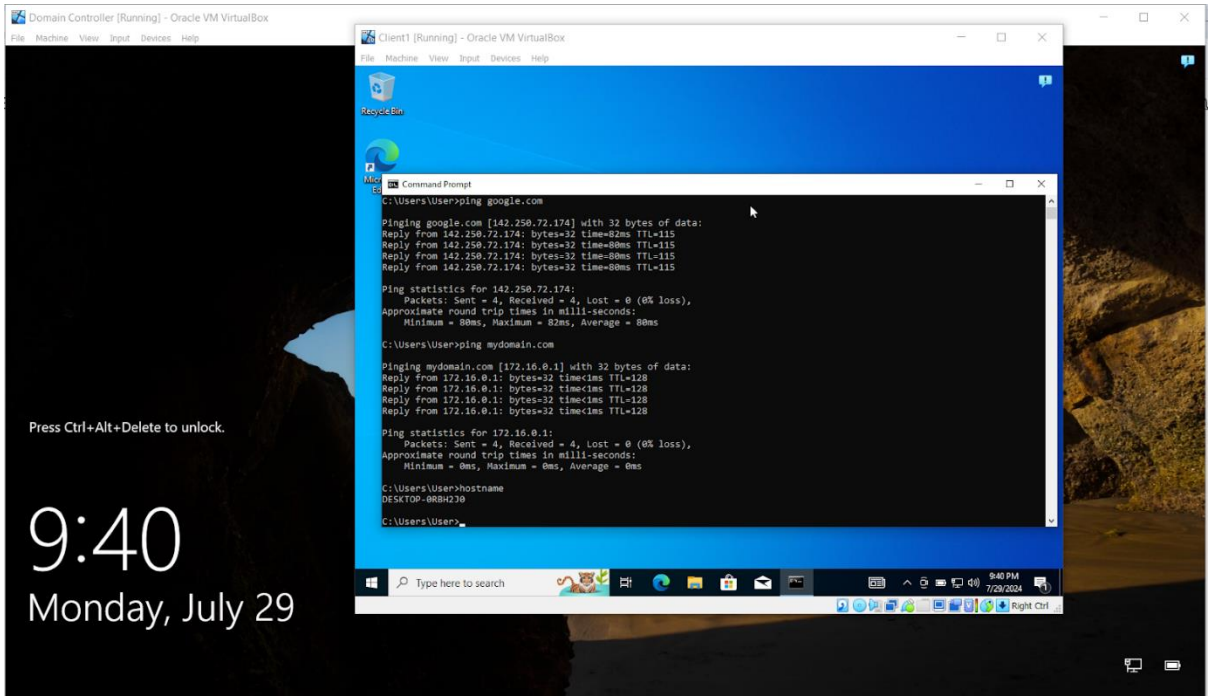
1. Create the VM in VirtualBox.
2. Assign network settings: Internal Network for Adapter 1.
3. Install Windows 10 using the ISO file.

Configure Network Settings on Windows 10:

1. Ensure the Windows 10 VM is on the same internal network.
2. Set it to obtain an IP address from the DHCP server.

Verify Network Connectivity:

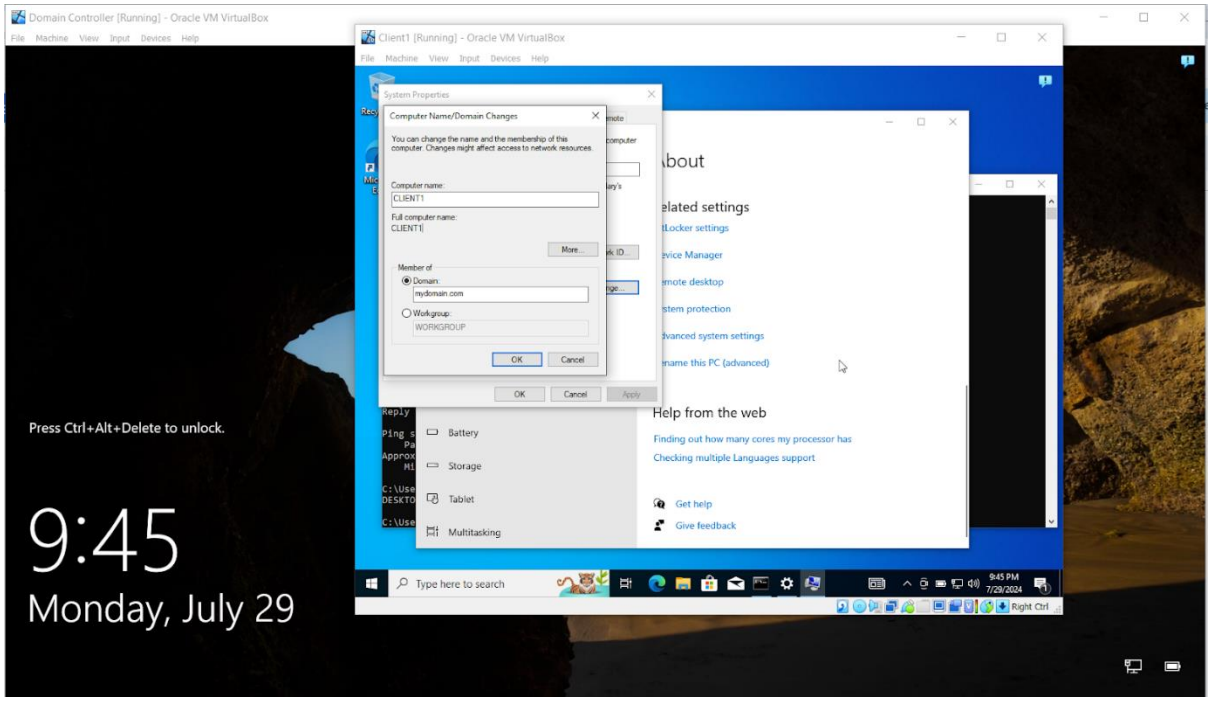
1. Ping google.com and mydomain.com.



2. Ensure the default gateway on Windows 10 is set to 172.16.0.1.

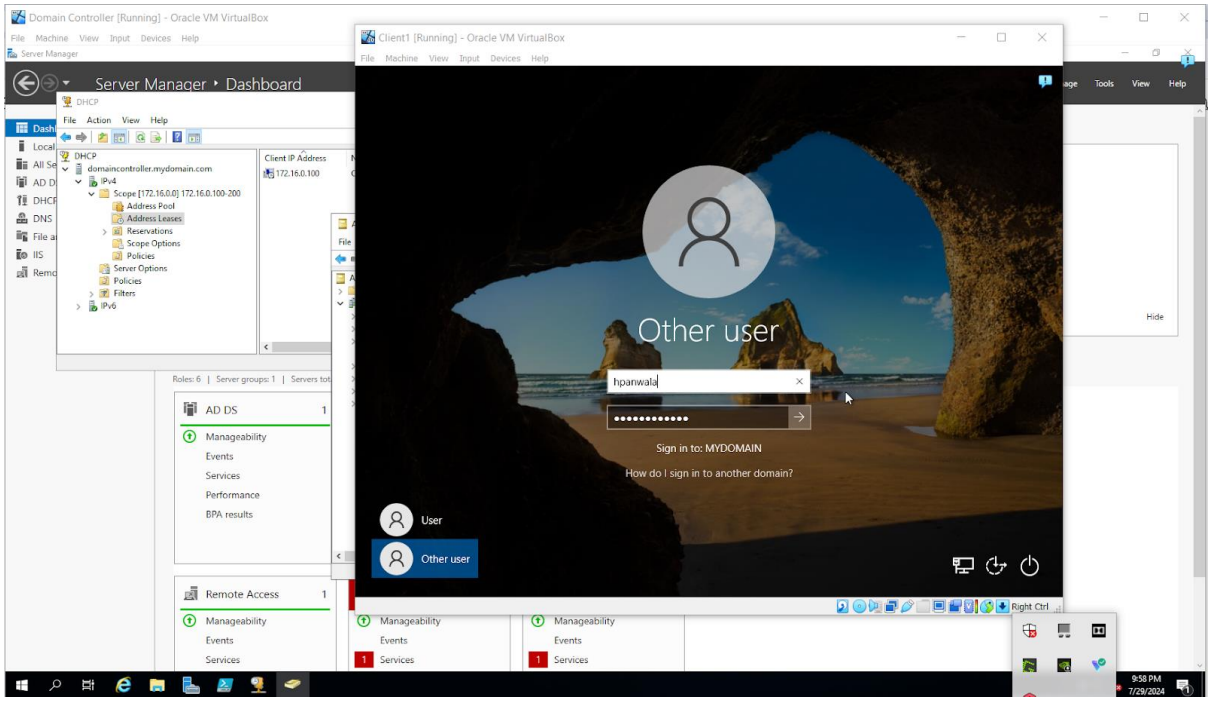
Join Windows 10 to the Domain:

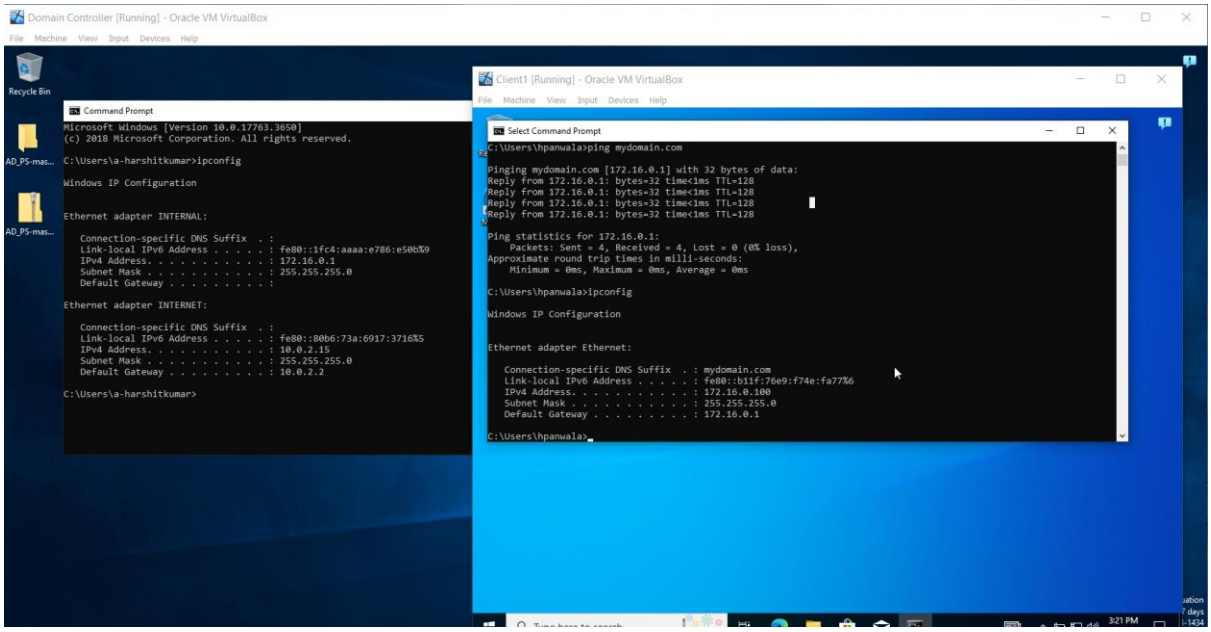
1. Go to **System Properties** -> **Change settings** -> **Change** and join the domain MYDOMAIN.
2. Enter domain credentials and restart the machine.



Log In with Domain User:

1. Log in using the domain user account hpanwala with the password Password@123.

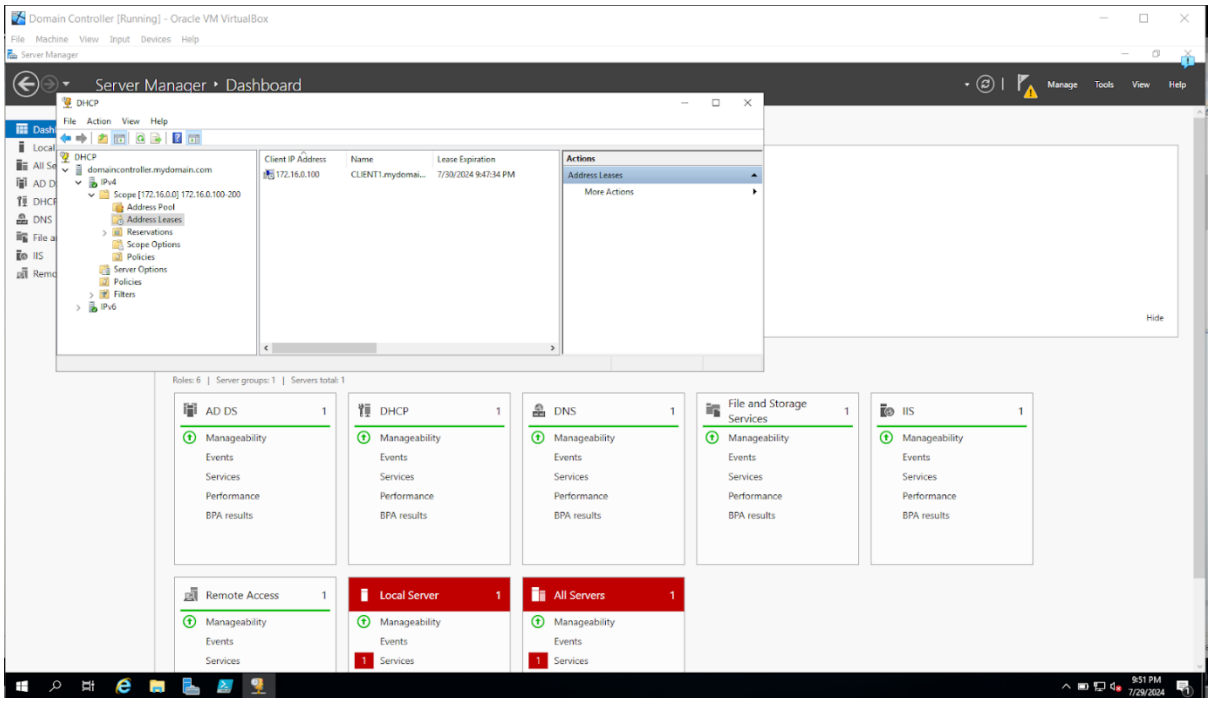




Step 9: Validate Configuration

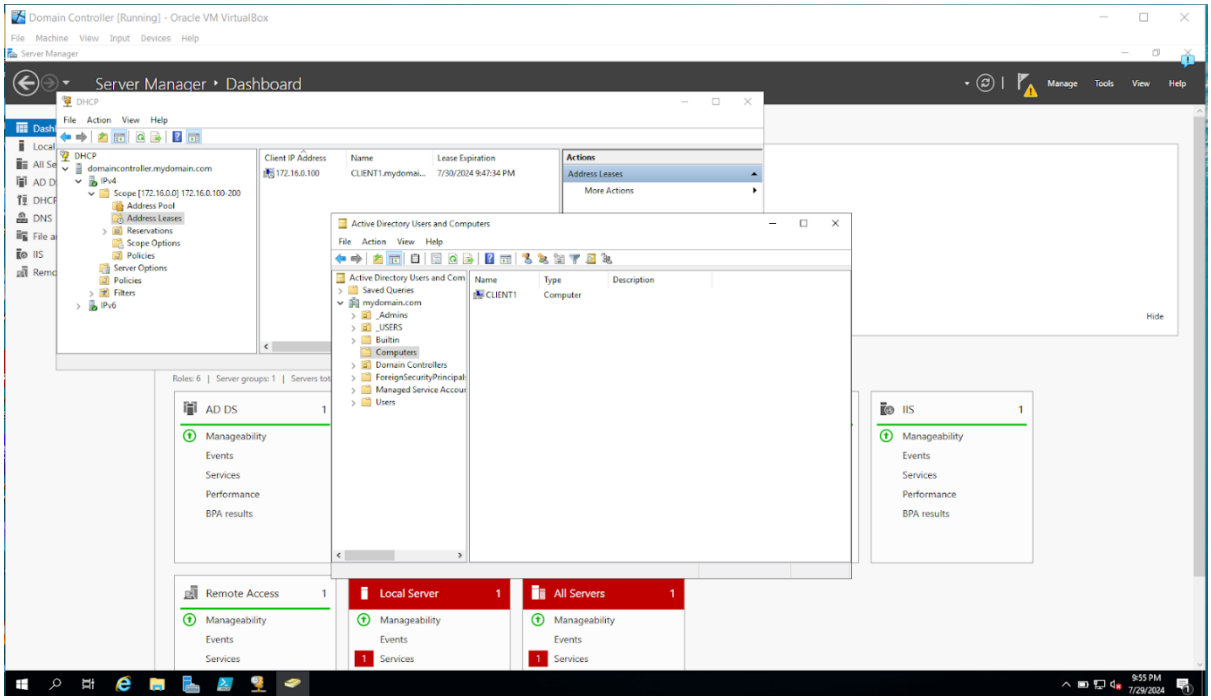
Check DHCP Leases:

1. On the Windows Server, go to **Server Manager** -> **Tools** -> **DHCP**.
2. Verify that CLIENT1 appears under **Address Leases**.



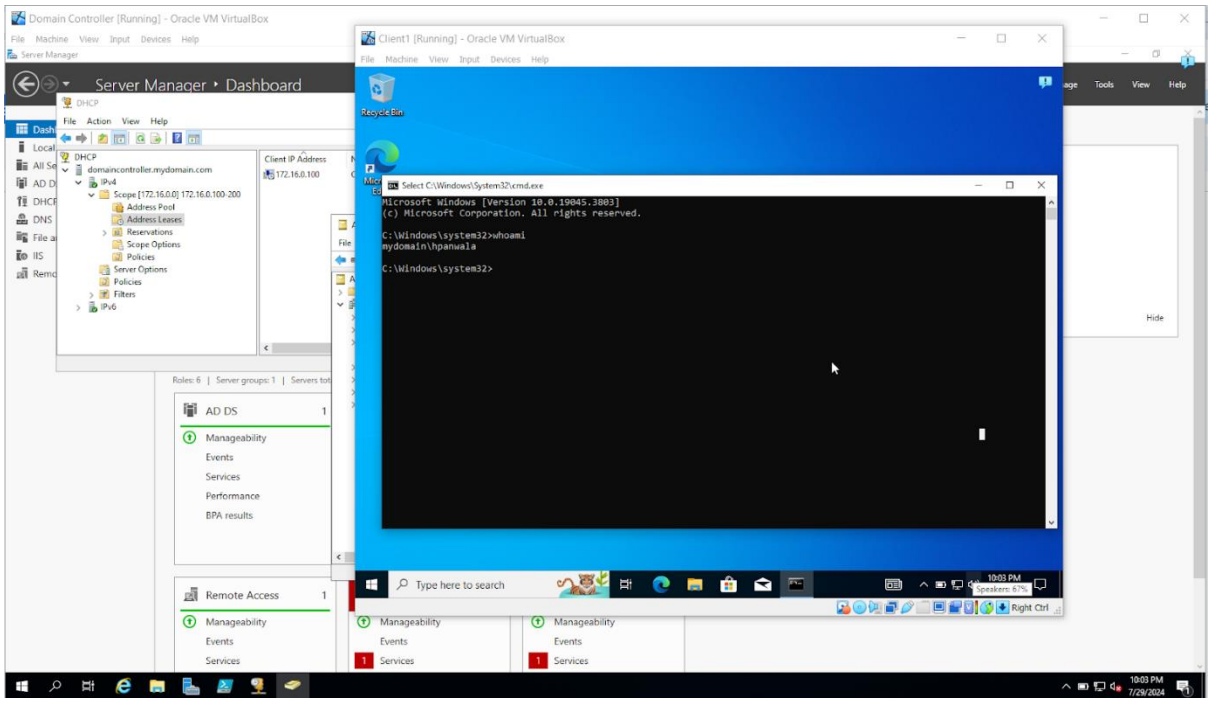
Check Active Directory Computers:

1. Open **Windows Administrative Tools** -> **Active Directory Users and Computers**.
2. Ensure CLIENT1 is listed under **Computers**.



Verify Domain User:

On the Windows 10 VM, open **Command Prompt** and type whoami to check the logged-in user.

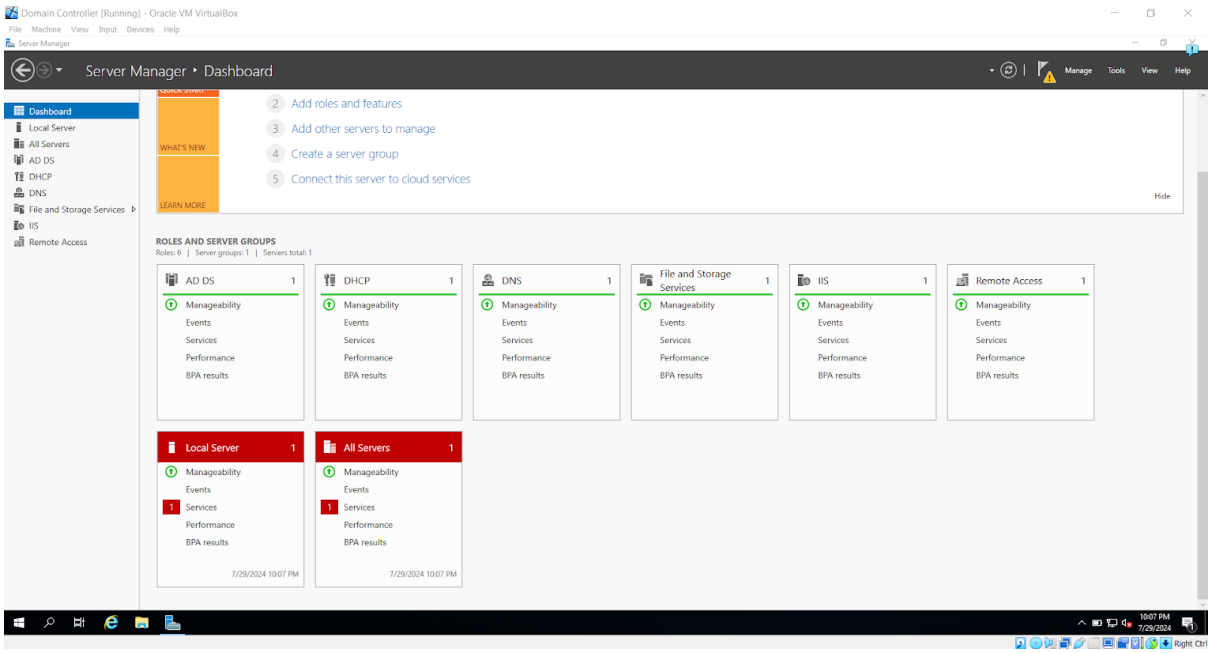


Best Practices Note

For real-world scenarios, ensure that user passwords meet strong security policies. Avoid using a single password for all accounts, and consider enabling password expiration and complexity requirements to enhance security.

Final Output

Active Directory Setup: A fully functional Active Directory environment with DNS, DHCP, and domain management.
Client Integration: Successful connection of a Windows 10 client to the domain with validated settings.



Conclusion and Future Work

This guide provided a comprehensive walkthrough for setting up and configuring an Active Directory environment with Windows Server 2019 and Windows 10 VMs in Oracle VirtualBox. By following these steps, you've built a domain controller, configured necessary network services, and integrated a client machine into the domain.

Future Enhancements

- **Enhance Security Configurations:**
  - Implement stricter password policies and account lockout policies to improve security.
  - Enable multi-factor authentication for critical accounts.
- **Improve Network Management:**
  - Configure VLANs to segment different network traffic types.
  - Use dedicated hardware firewalls to enhance network security.
- **Expand Active Directory:**
  - Implement Group Policies to enforce security and configuration settings across the domain.
  - Set up additional domain controllers for redundancy and load balancing.
- **Automate User Management:**
  - Develop scripts or use third-party tools for automated user provisioning and de-provisioning.
  - Integrate with a centralized identity management system.