

4/27/2026

Network Operating Systems and Services

(ACCA5023_LON)

Name: Luciano Santos

ID: 2335472

Lecturer: Dr. Nitheesh Kaliyamurthy

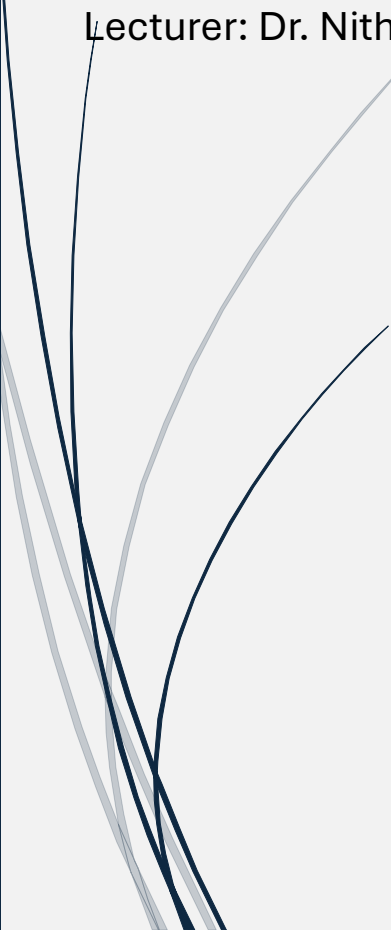


Table of Contents

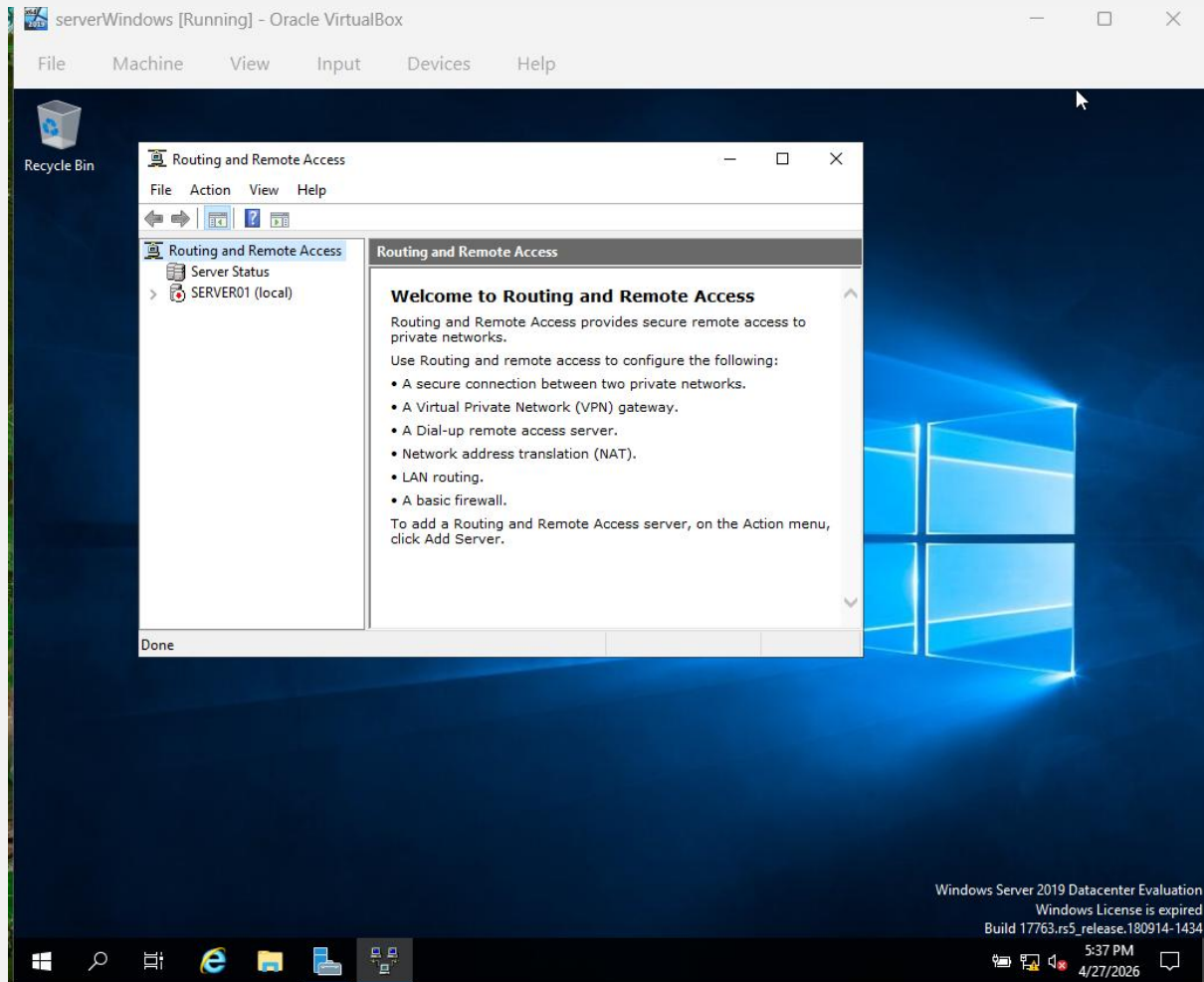
1.0 Introduction	
2.0 Network Configuration	
3.0 DHCP Configuration	
3.1 Scope Creation	
3.2 IP Allocation	
4.0 Test and Troubleshoot (Task 7)	
4.1 IP Configuration Check	
4.2 Ping Connectivity Test	
5.0 Disk Drive Configuration (Task 8)	
5.1 Disk Creation and Formatting	
5.2 Folder Sharing	
5.3 Permissions Setup	
5.4 Client Access Verification	
6.0 IIS Server Setup (Task 9)	
6.1 Website Creation	
6.2 File Location Setup	
6.3 IIS Configuration	
6.4 Website Testing	
7.0 Remote Desktop Services (Task 10)	
7.1 Enabling Remote Desktop	
7.2 Client Connection	
7.3 Authentication	
7.4 Remote Access Verification	
8.0 Conclusion	

Introduction

This assignment focuses on configuring and managing a virtualised enterprise network using Windows Server. The main objective is to set up essential network services such as routing, domain services, DHCP, file sharing, and a web server. Throughout the tasks, a Birmingham network environment was created and configured. Different components were tested to ensure proper communication between the server and client machines. The assignment demonstrates the practical implementation of network services and provides an understanding of how these services work together to support a functional enterprise network.

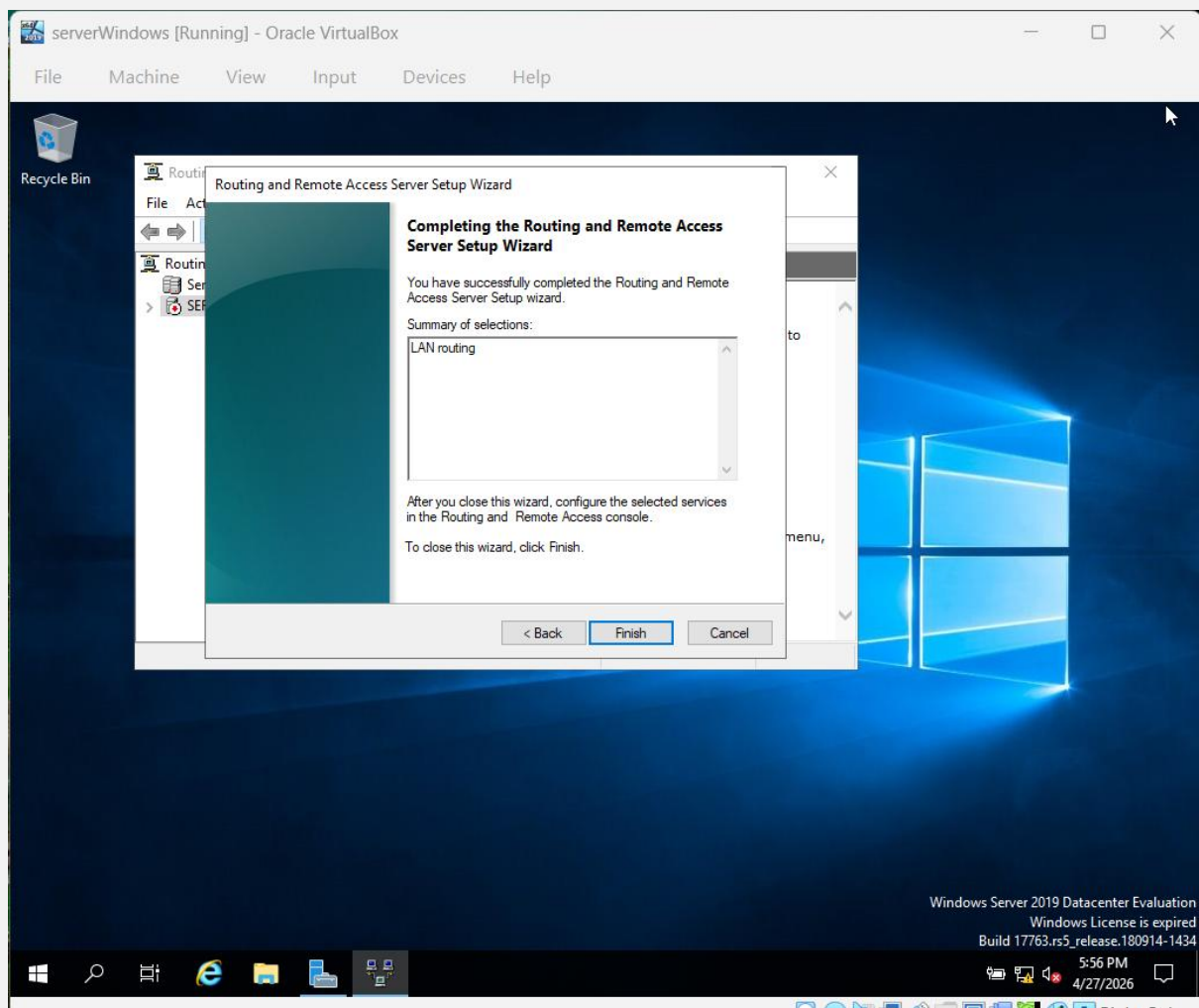
Task 1 – Routing Configuration

Routing and Remote Access Service Enabled



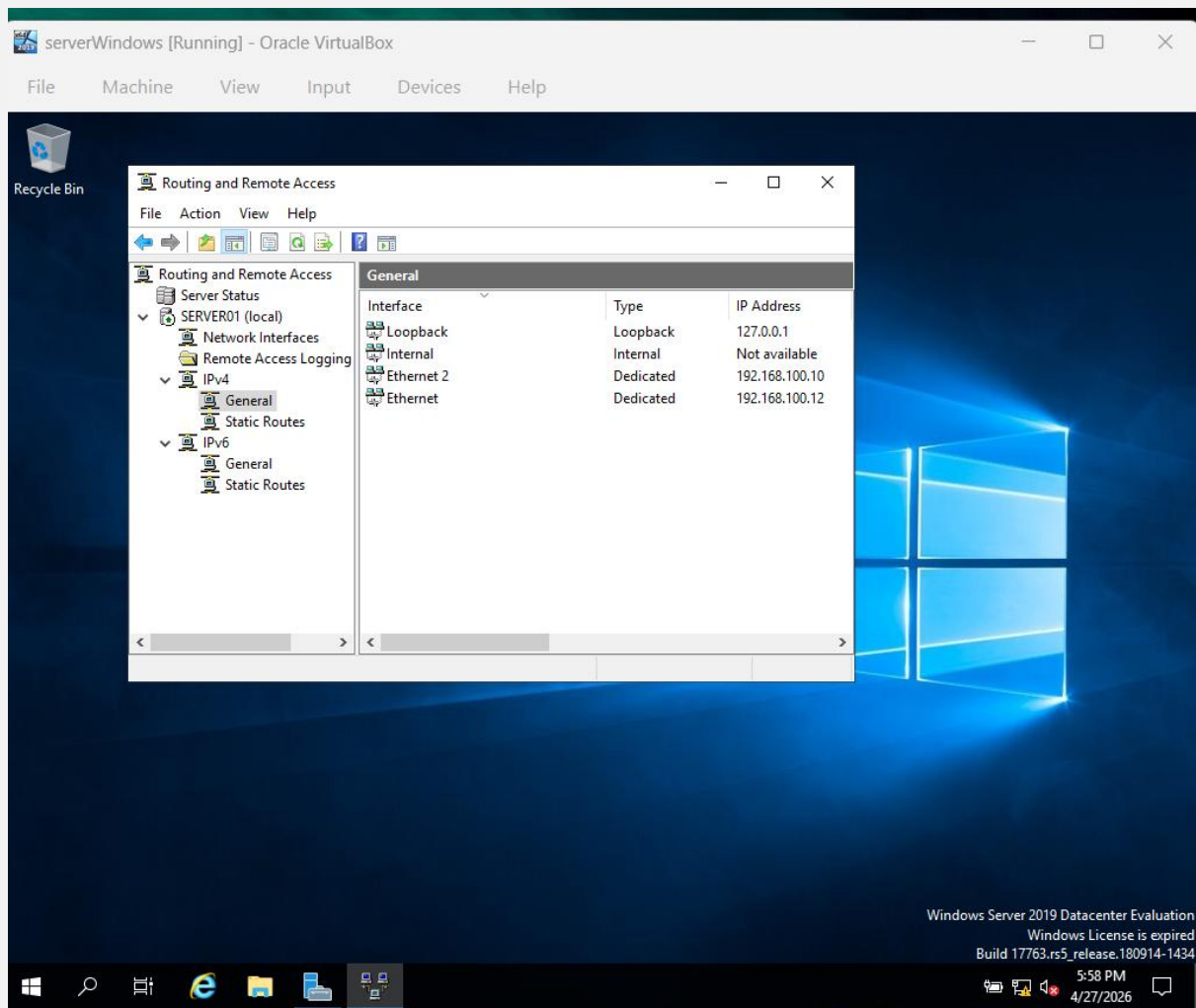
Routing and Remote Access (RRAS) was successfully enabled on SERVER01.
This confirms that the server is ready to perform routing between network interfaces.

LAN Routing Configuration Completed



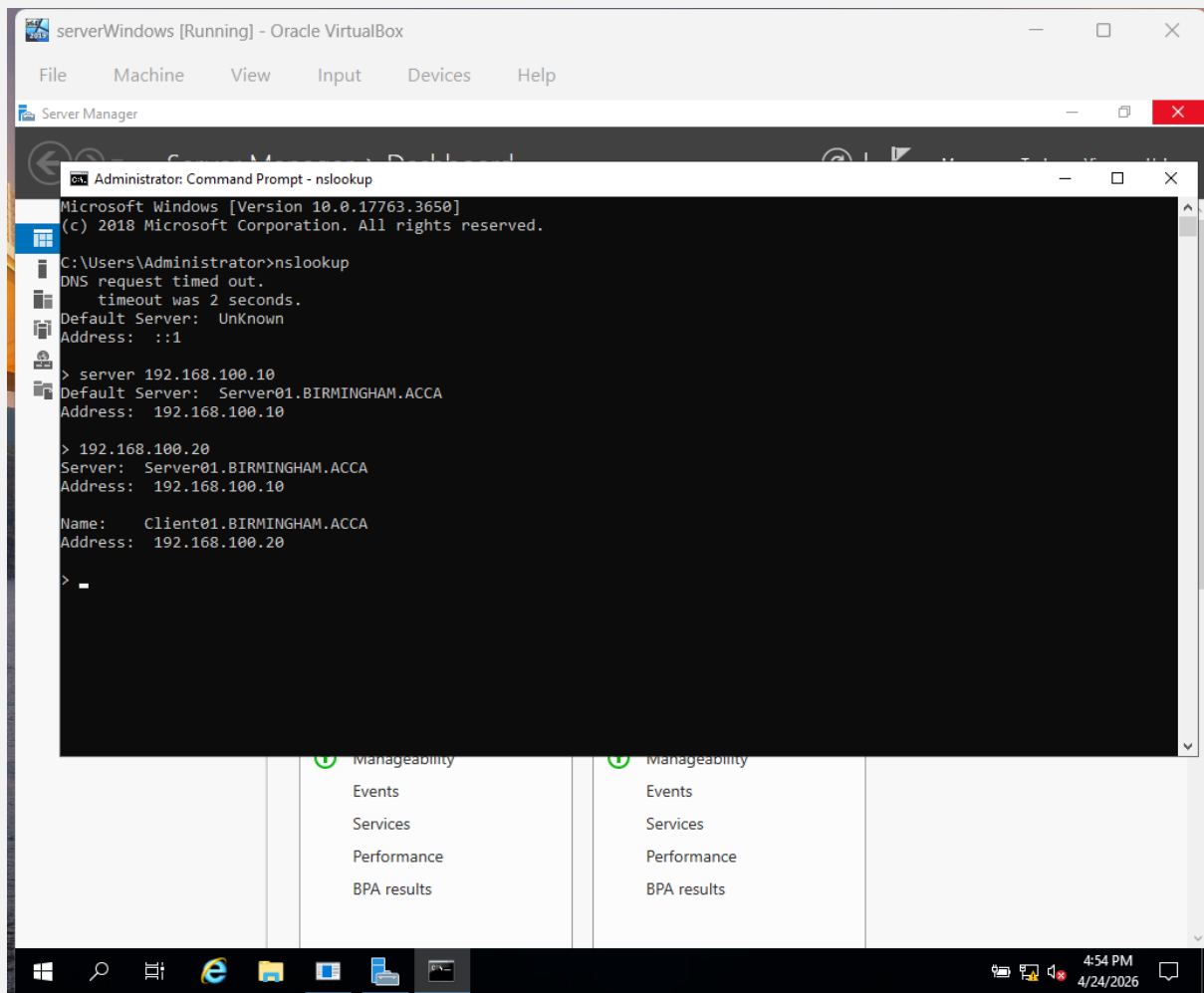
The Routing and Remote Access setup wizard was completed using custom configuration. LAN routing was selected to allow traffic to be routed between internal networks.

Network Interfaces and IP Configuration



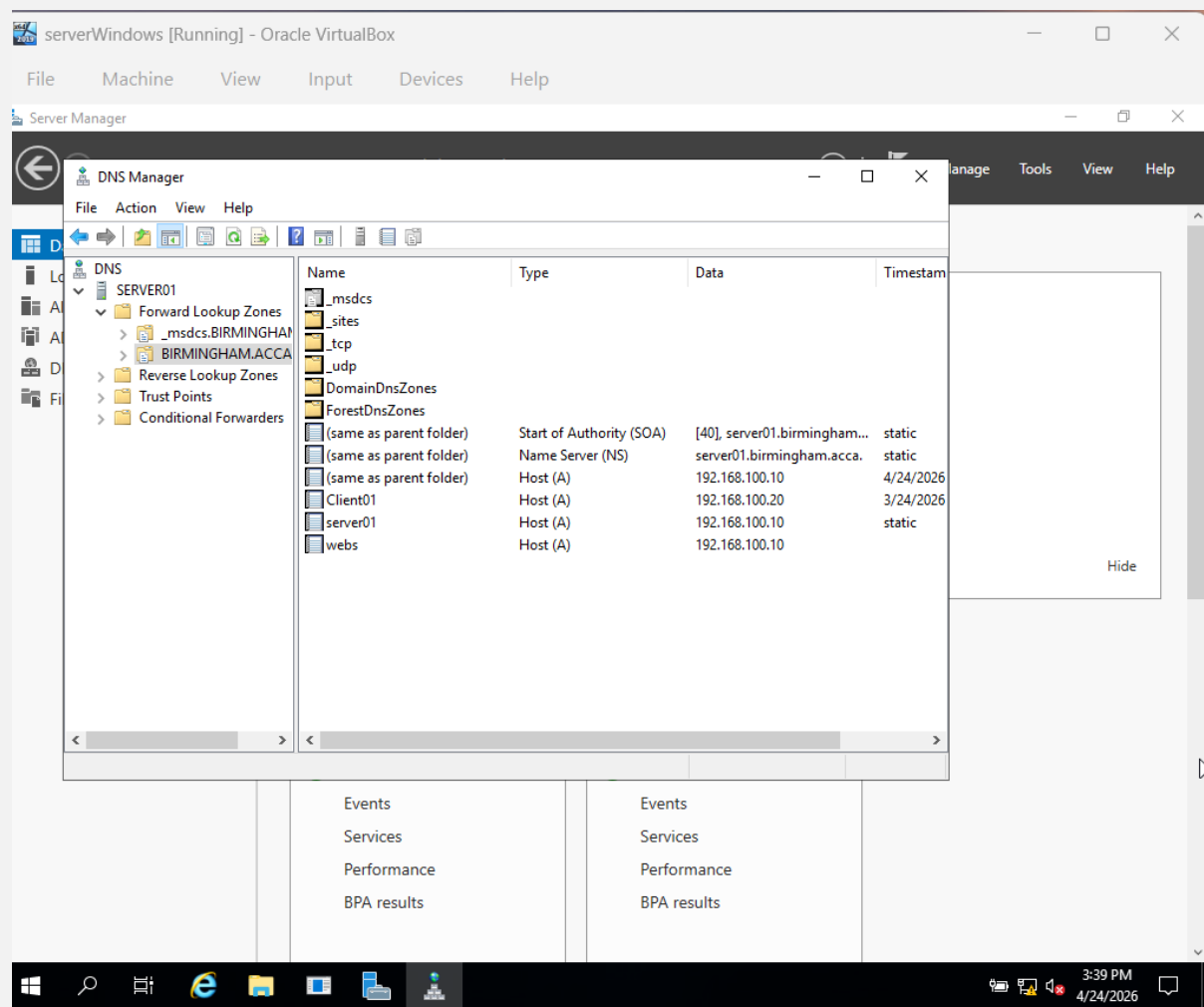
The IPv4 configuration shows active network interfaces, including Ethernet adapters with assigned IP addresses. This confirms that routing is correctly configured and operational.

Domain Forest Creation (Birmingham.acca)



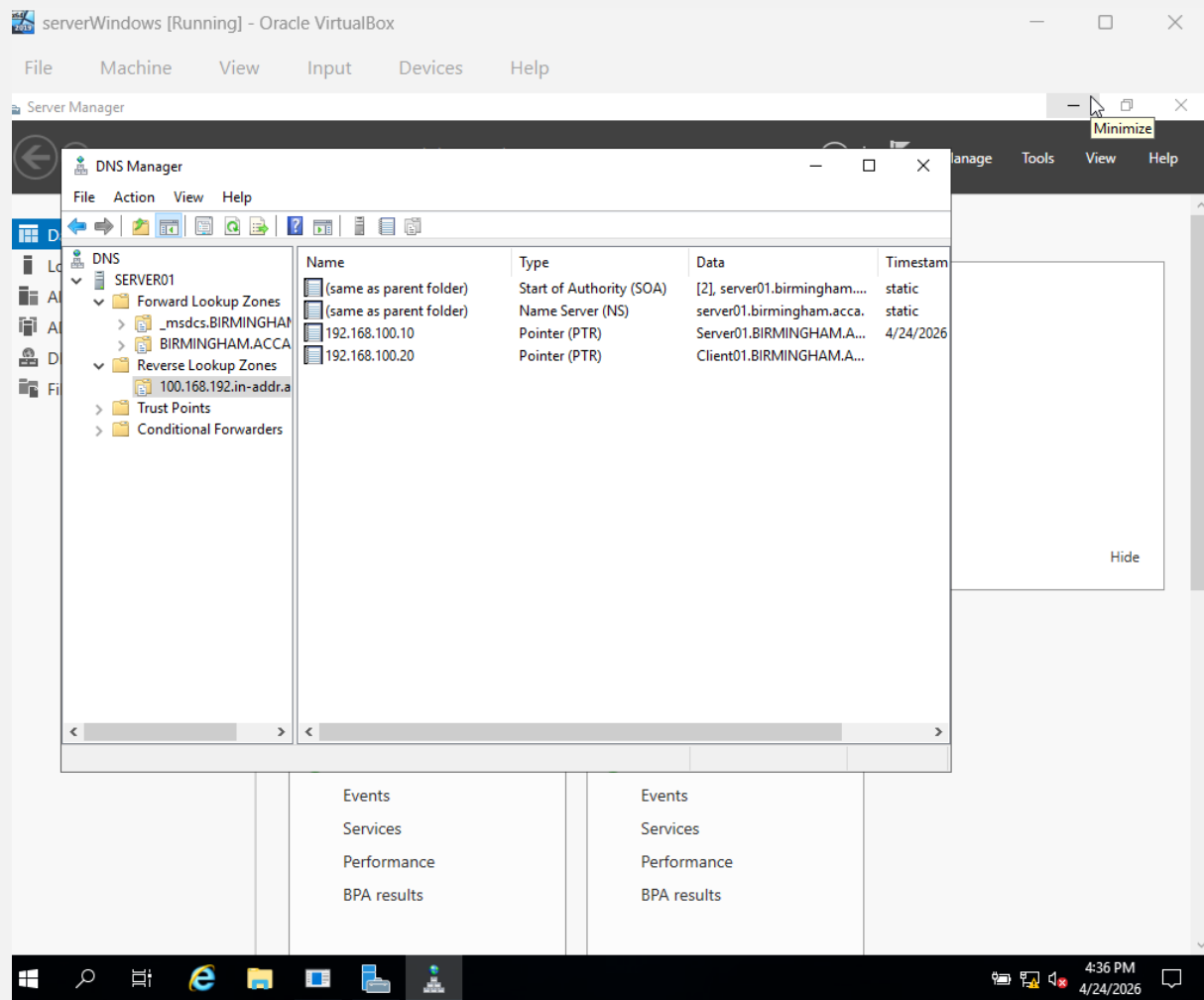
The domain **birmingham.acca** was successfully created using Active Directory. This acts as the central point for managing users, computers, and network resources.

Forward Lookup Zone with A Records



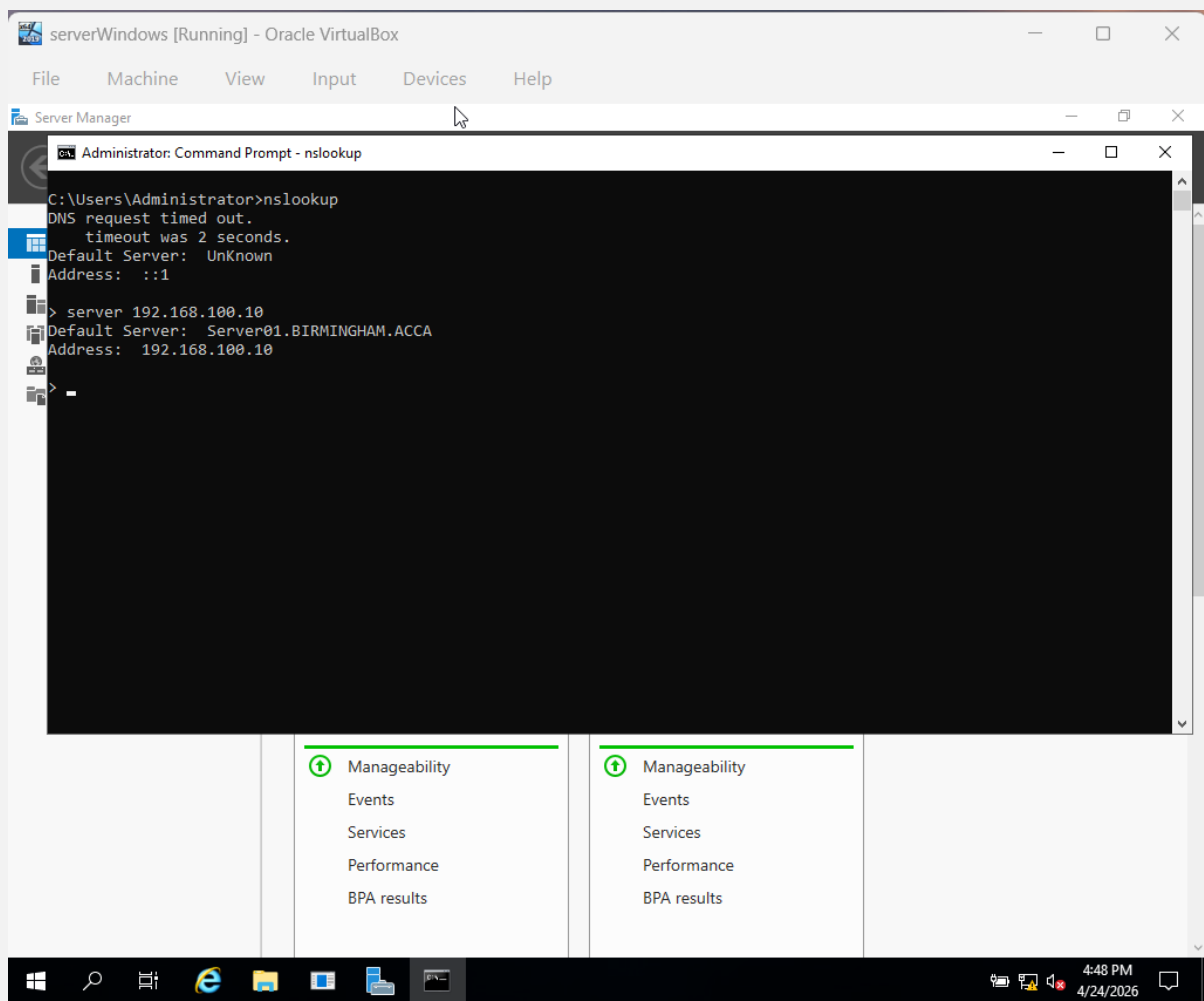
A forward lookup zone was configured to allow hostname to IP address resolution. A records were created for all devices including the server, client, and web server.

Reverse Lookup Zone with PTR Records



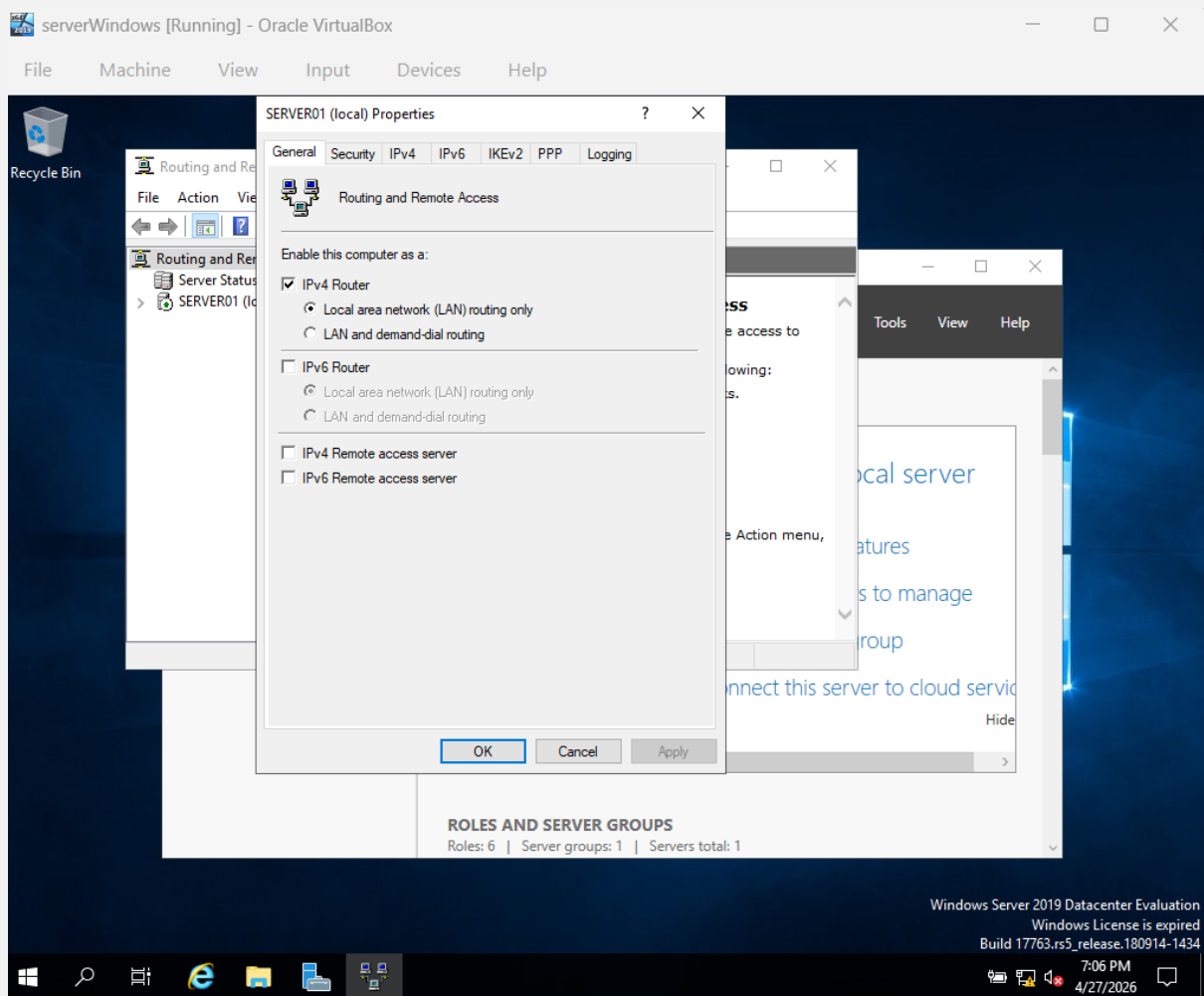
A reverse lookup zone was created to map IP addresses back to hostnames. PTR records were configured to ensure proper reverse DNS resolution.

DNS Resolution Test using nslookup



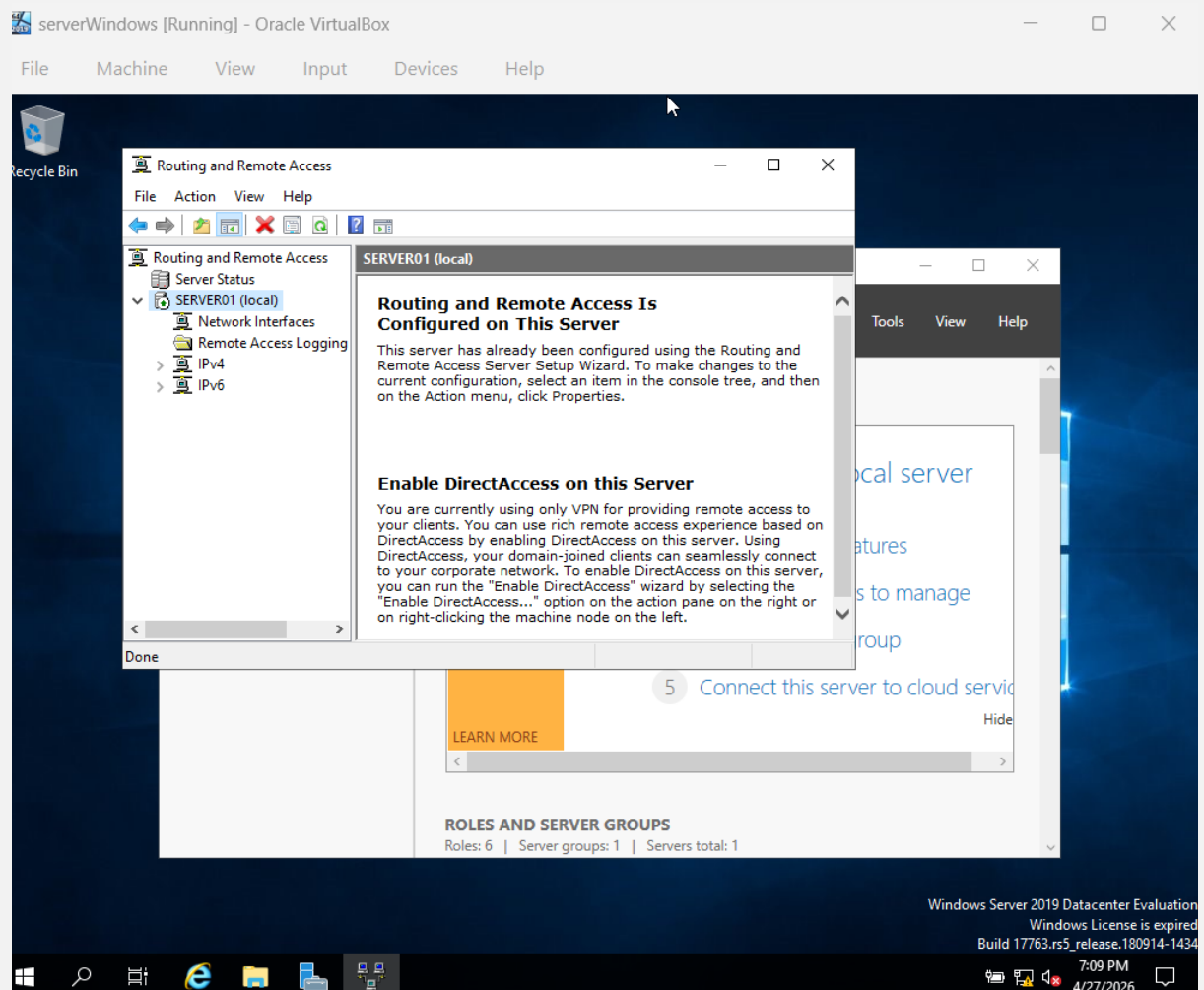
The nslookup command was used to test DNS functionality. The results confirm that hostnames are correctly resolved to IP addresses.

RRAS Server Configuration Settings



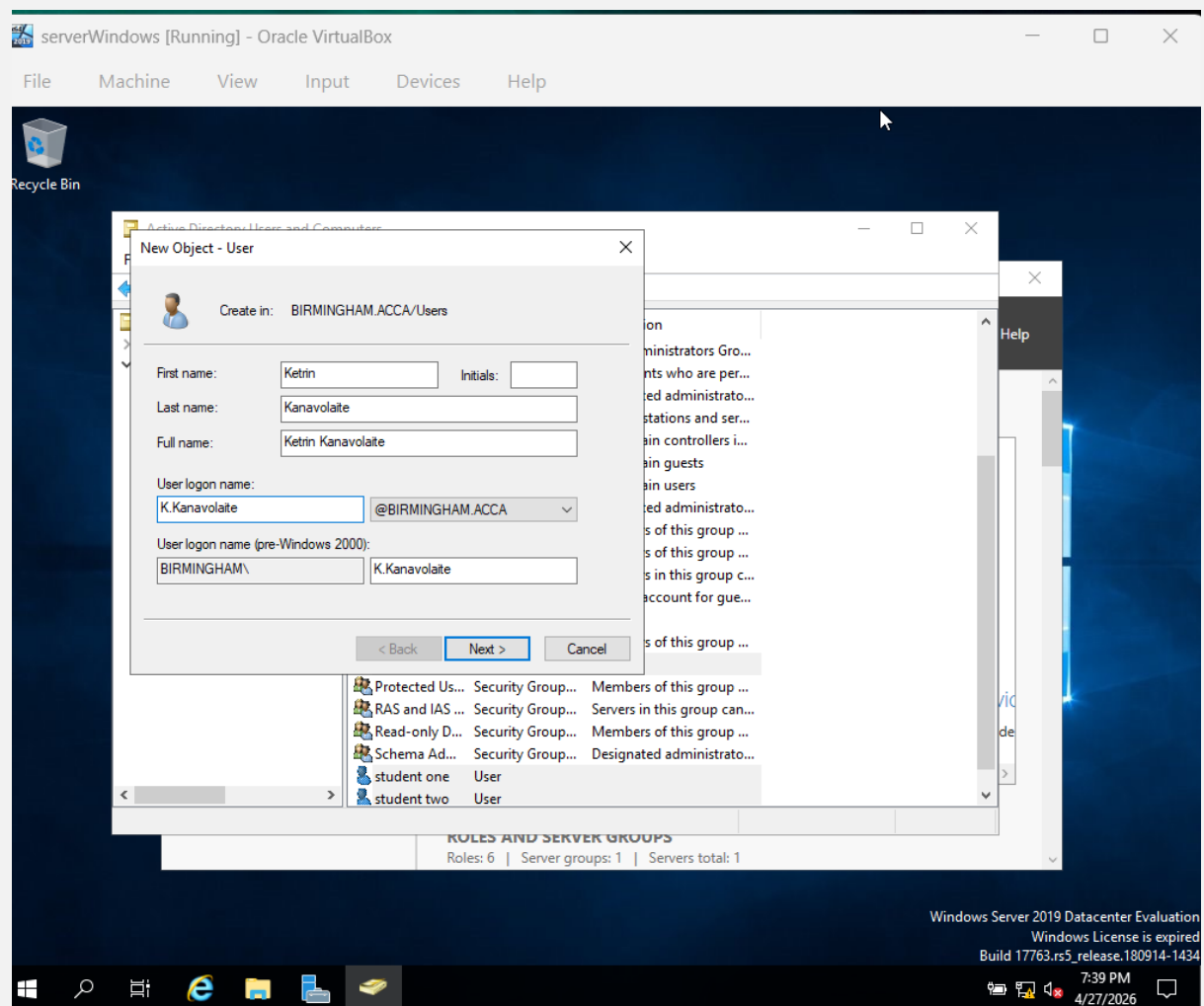
The Routing and Remote Access server properties were configured. IPv4 routing was enabled, allowing the server to route traffic between networks and support remote access services.

Routing and Remote Access Service Configured



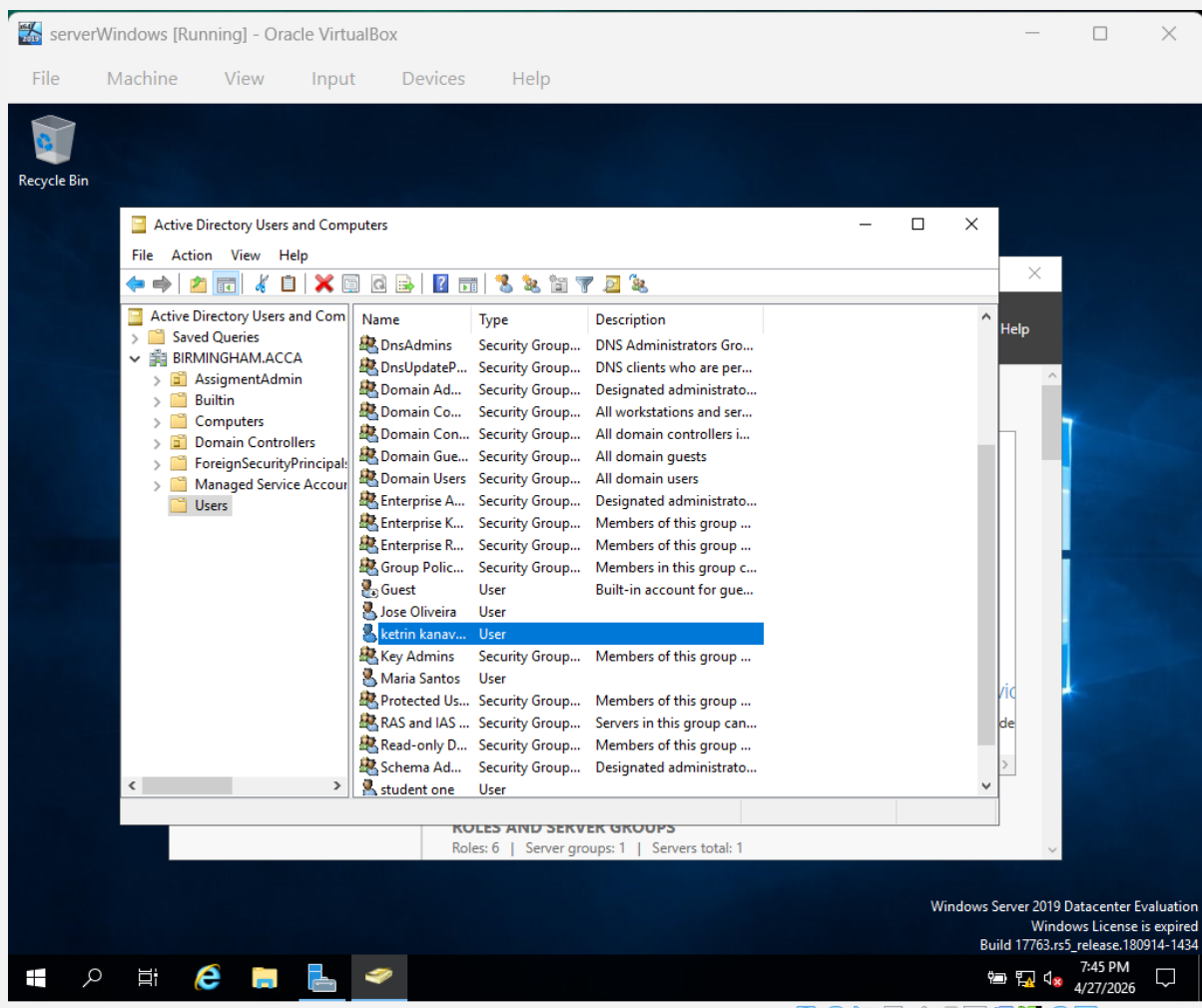
The Routing and Remote Access service was successfully configured on the server. The system shows that VPN functionality is available, enabling secure communication between networks.

Creating User Account in Active Directory



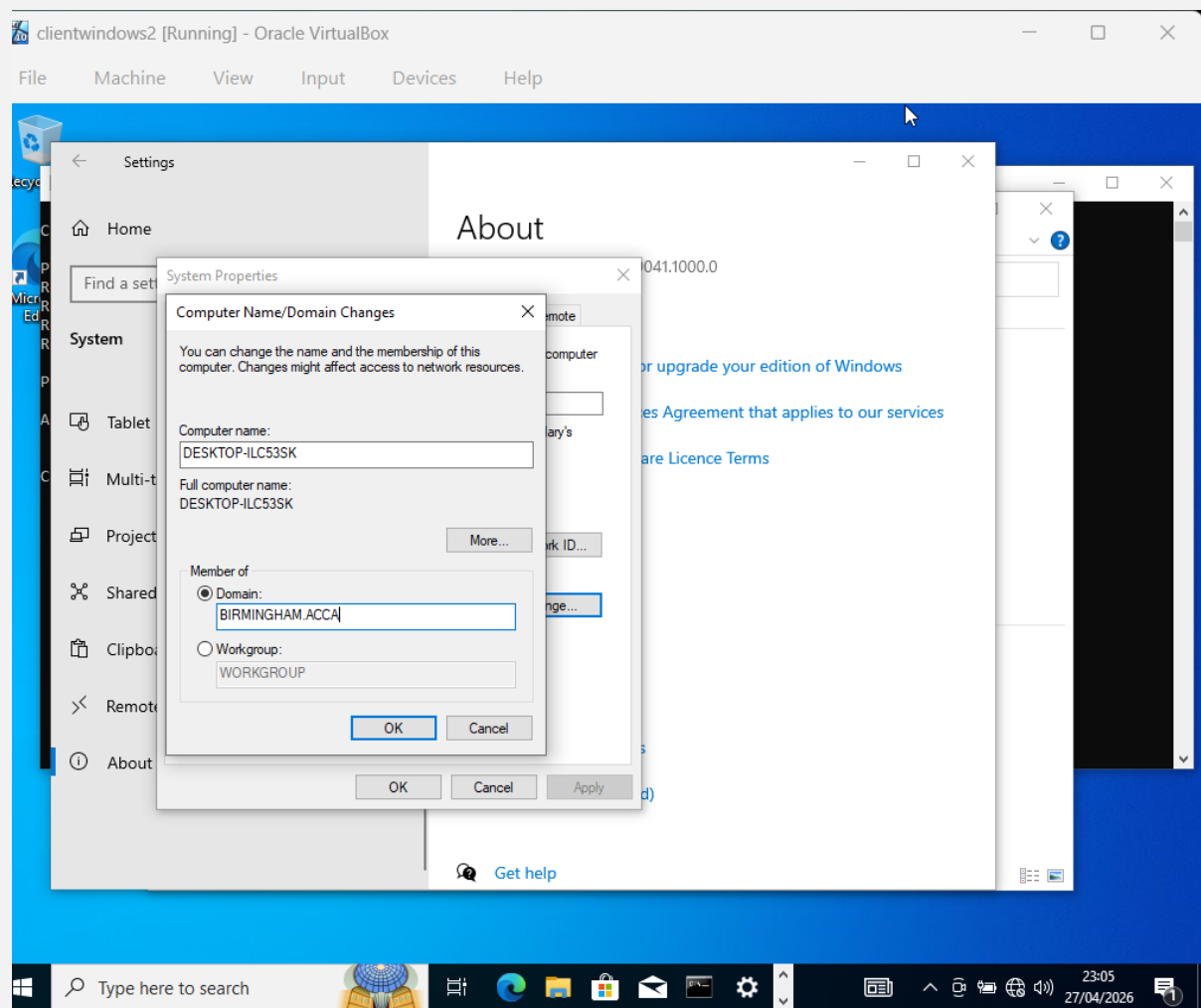
A new user account is being created in Active Directory within the Birmingham domain. The username follows the required naming convention using the first letter of the first name and the full last name.

User Account Successfully Created



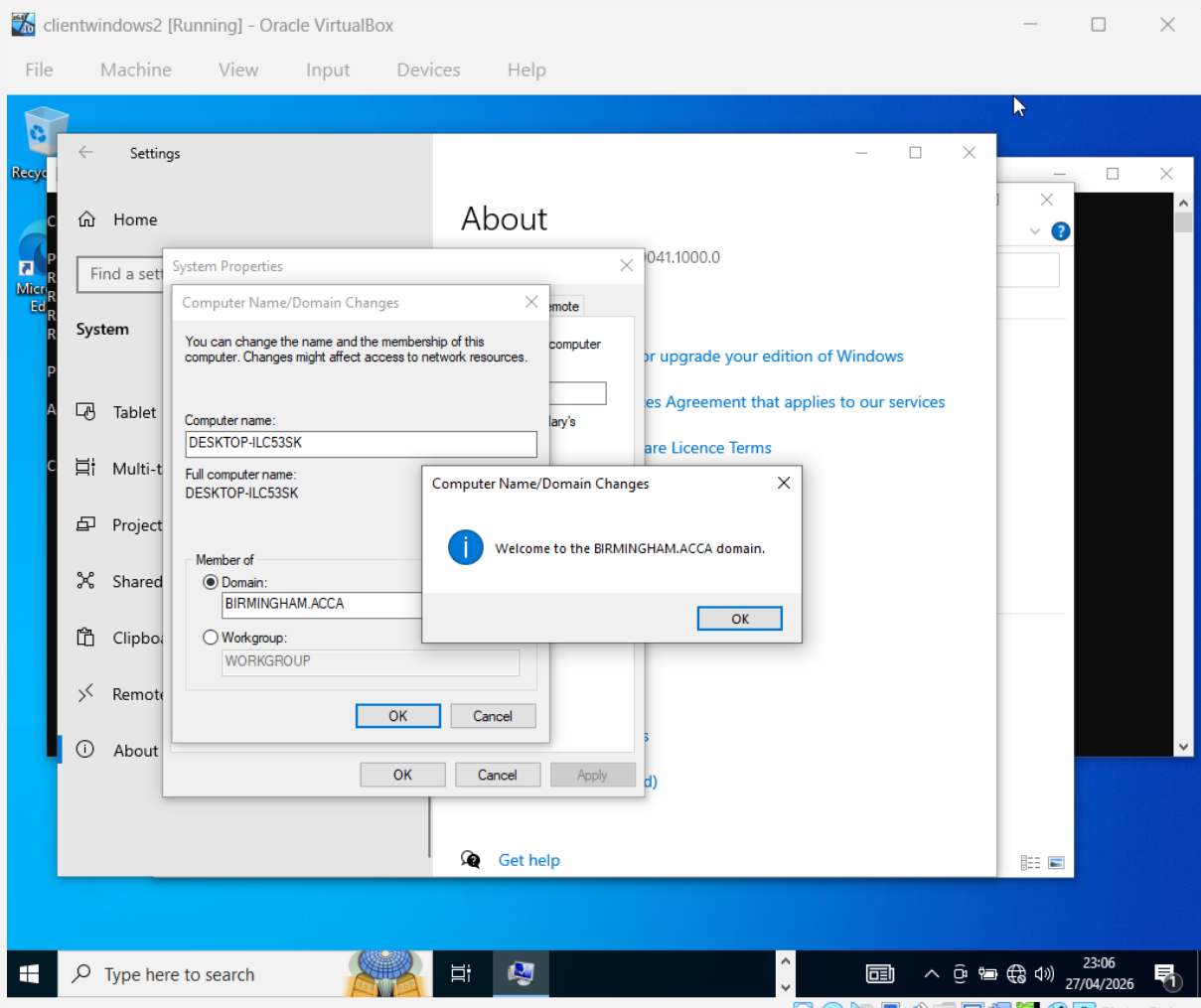
The user account has been successfully created and is visible in the Active Directory Users container. This confirms that user creation and management within the domain is working correctly.

Entering the Domain Name



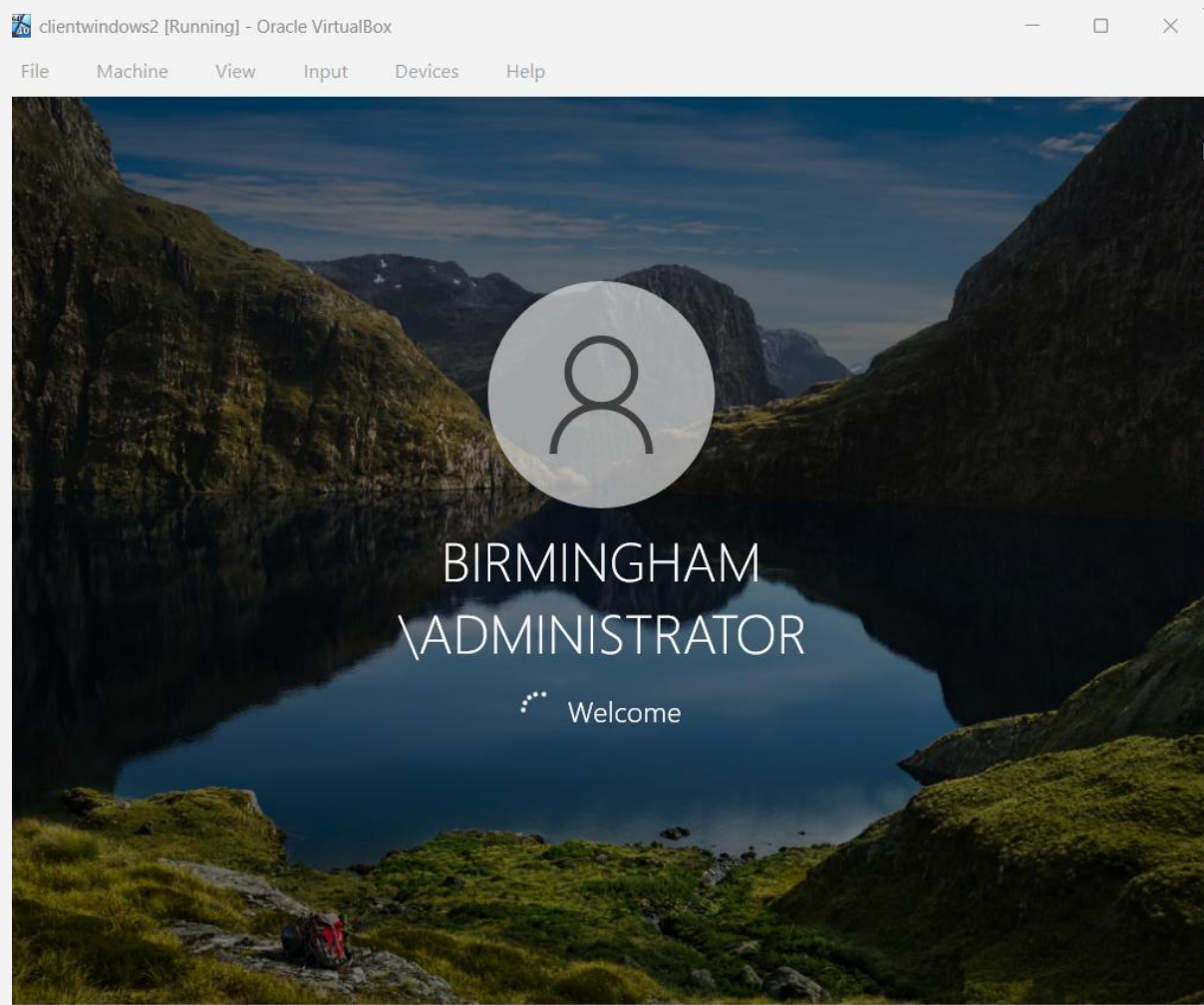
The domain name *BIRMINGHAM.ACCA* was entered in the System Properties to begin the process of joining the client machine to the Active Directory domain.

Domain Join Confirmation Message



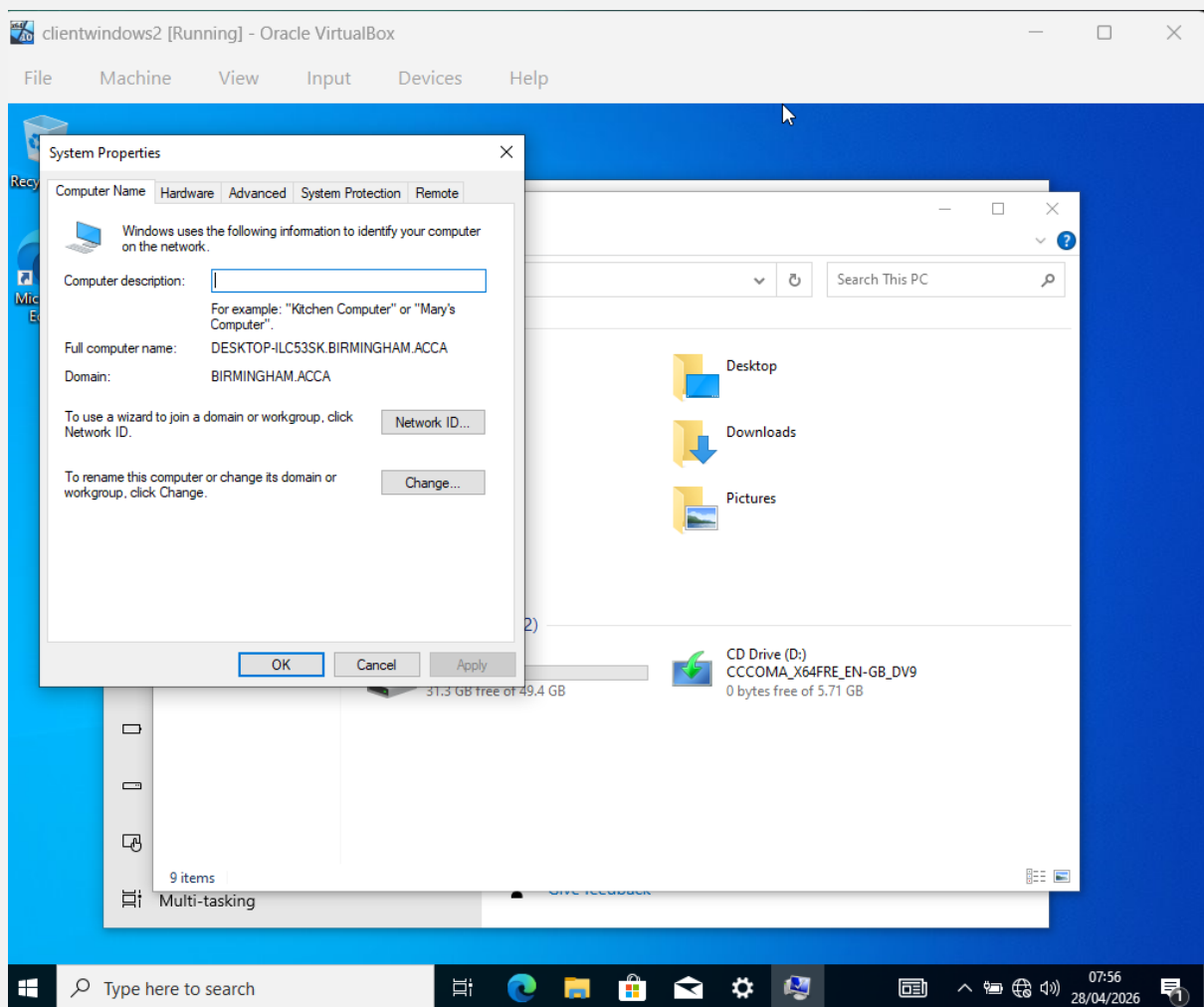
A confirmation message was displayed indicating that the client machine successfully joined the *BIRMINGHAM.ACCA* domain.

Domain Login Screen



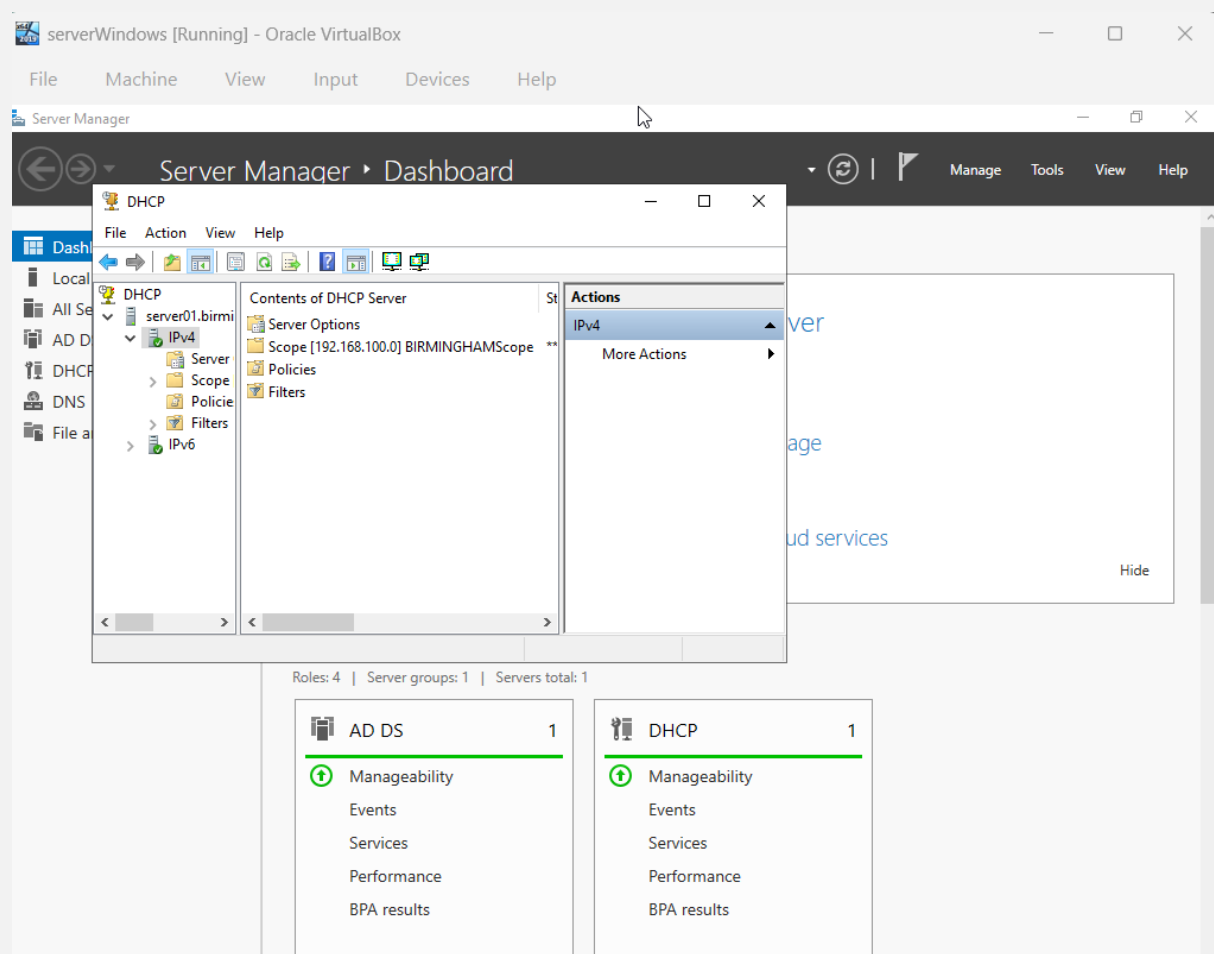
The system login screen shows authentication using the domain account *BIRMINGHAM\Administrator*, confirming successful integration with Active Directory.

Domain Membership Verified



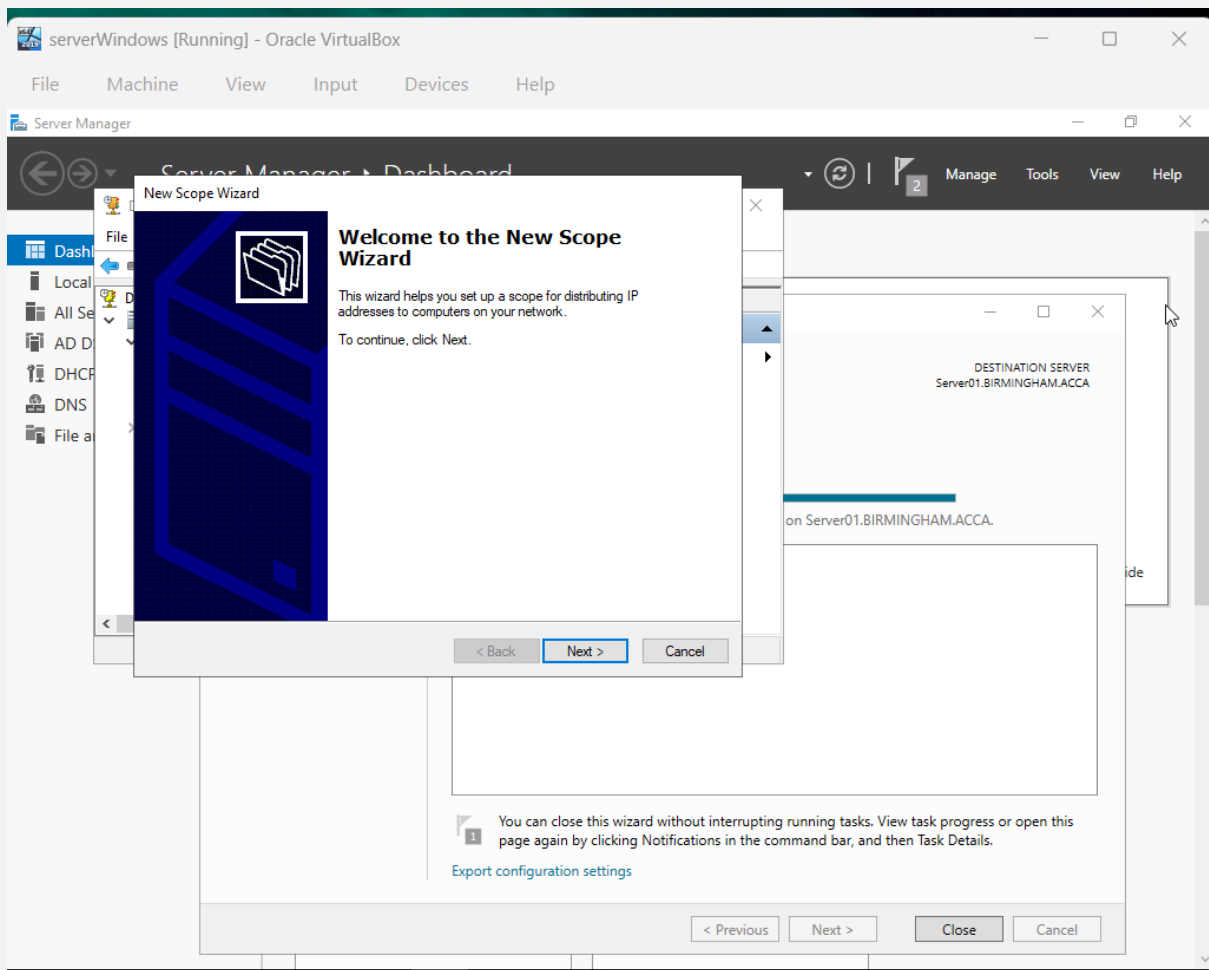
The System Properties confirm that the computer is now part of the *BIRMINGHAM.ACCA* domain.

DHCP Server Configuration in Server Manager



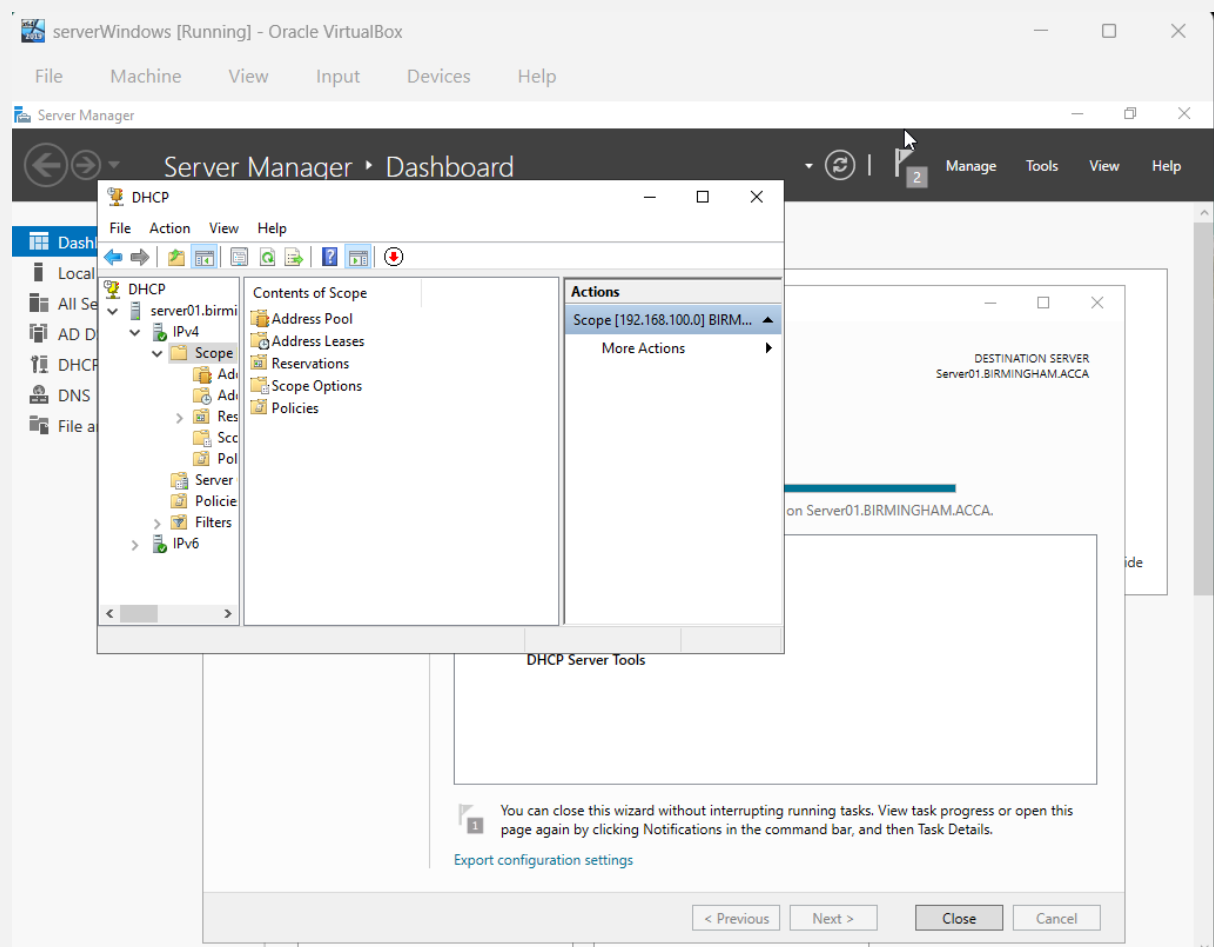
This image shows the DHCP Server successfully configured on the Windows Server. The IPv4 scope (192.168.100.0) is visible under the DHCP console, confirming that the DHCP service is active and ready to assign IP addresses to clients automatically.

Starting the New Scope Wizard



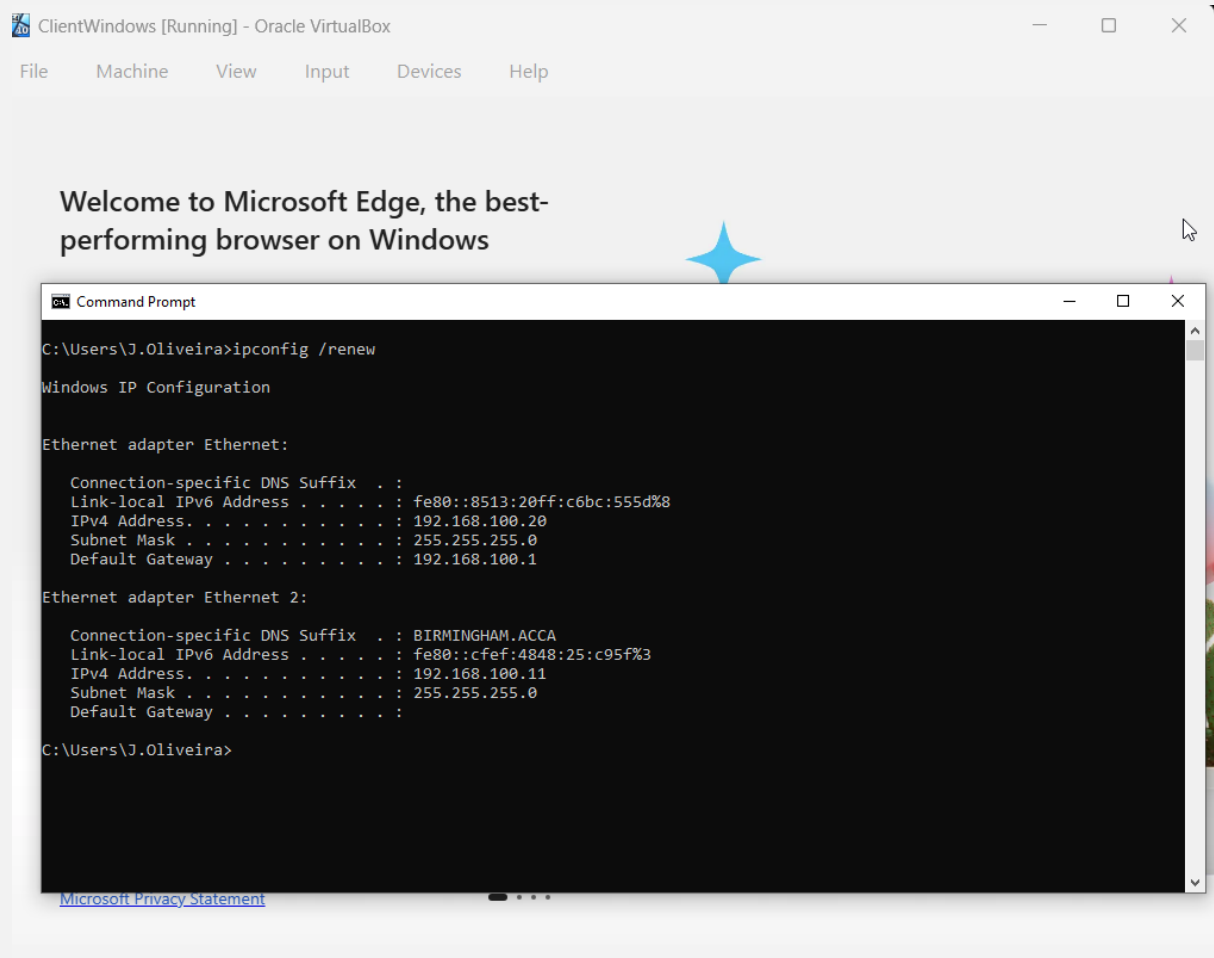
This image shows the beginning of the New Scope Wizard used to configure DHCP. This wizard allows the administrator to define the IP address range and settings that will be assigned automatically to clients on the network.

Overview of DHCP Scope Configuration



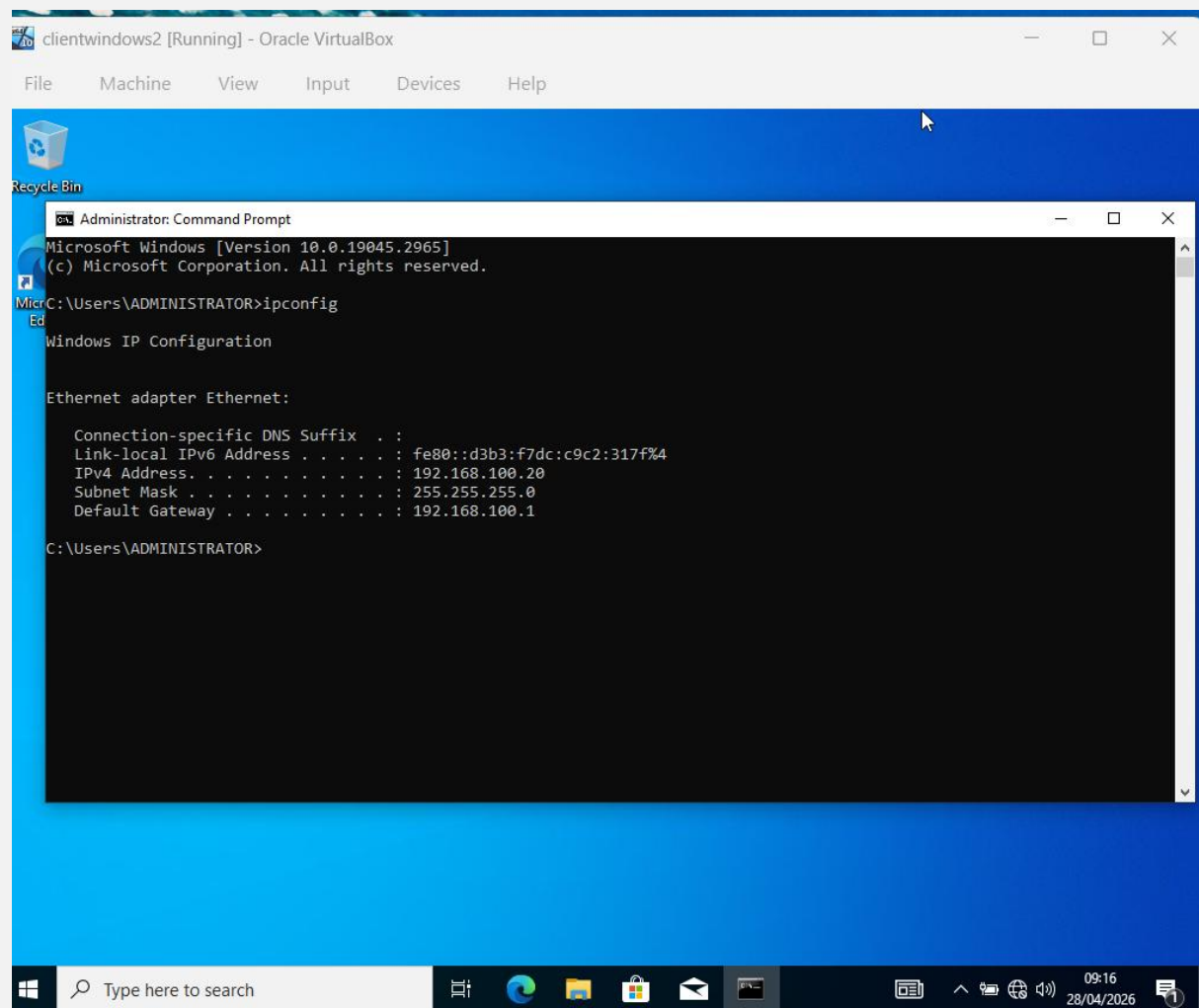
This image shows the detailed configuration of the DHCP scope, including the Address Pool, Address Leases, Reservations, and Scope Options. This confirms that the DHCP scope has been successfully configured and is ready to assign IP addresses to clients

Client Receiving IP Address via DHCP



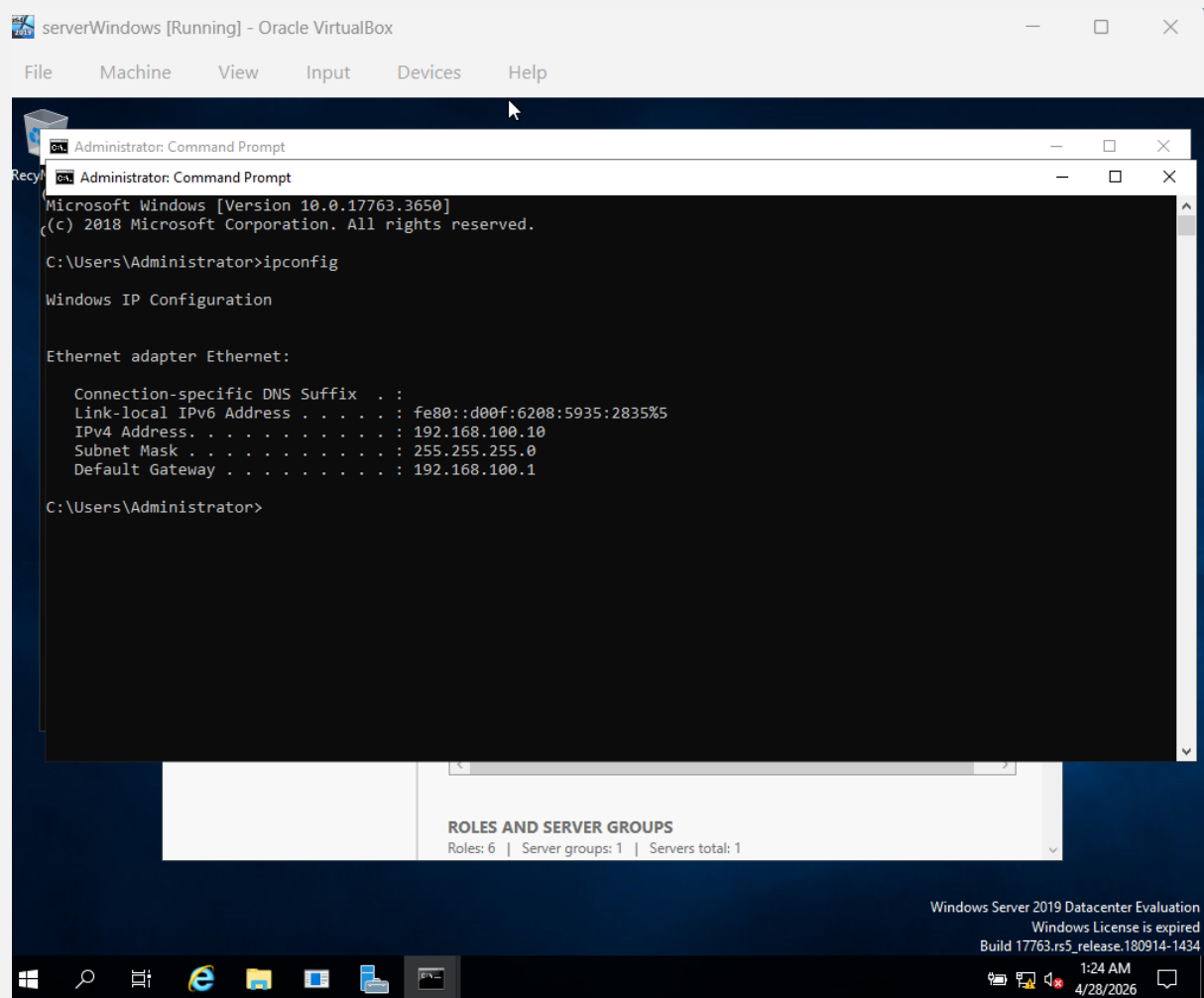
This image shows the client computer successfully obtaining an IP address automatically from the DHCP server using the `ipconfig /renew` command. The assigned IP address (192.168.100.20) is within the configured DHCP scope range, confirming that the DHCP server is working correctly and distributing network settings to clients.

Client IP Configuration Using DHCP



This image shows the client machine displaying its IP configuration using the `ipconfig` command. The assigned IP address (192.168.100.20) is within the DHCP scope range, confirming that the client successfully received network settings automatically from the DHCP server.

Server IP Configuration (ipconfig)

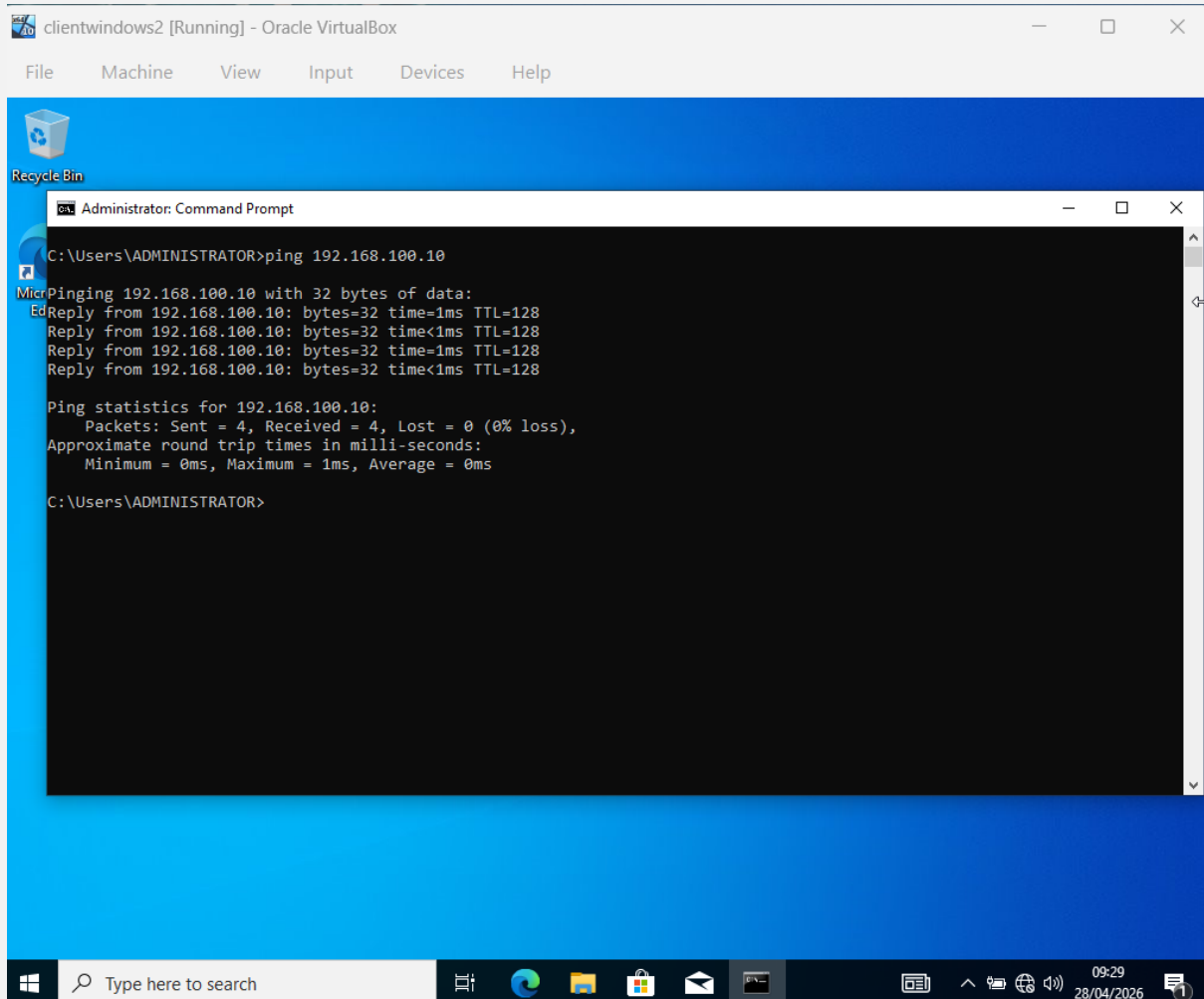


This screenshot shows the IP configuration of the Windows Server.

The server has been assigned the IP address **192.168.100.10**, with a subnet mask of **255.255.255.0** and a default gateway of **192.168.100.1**.

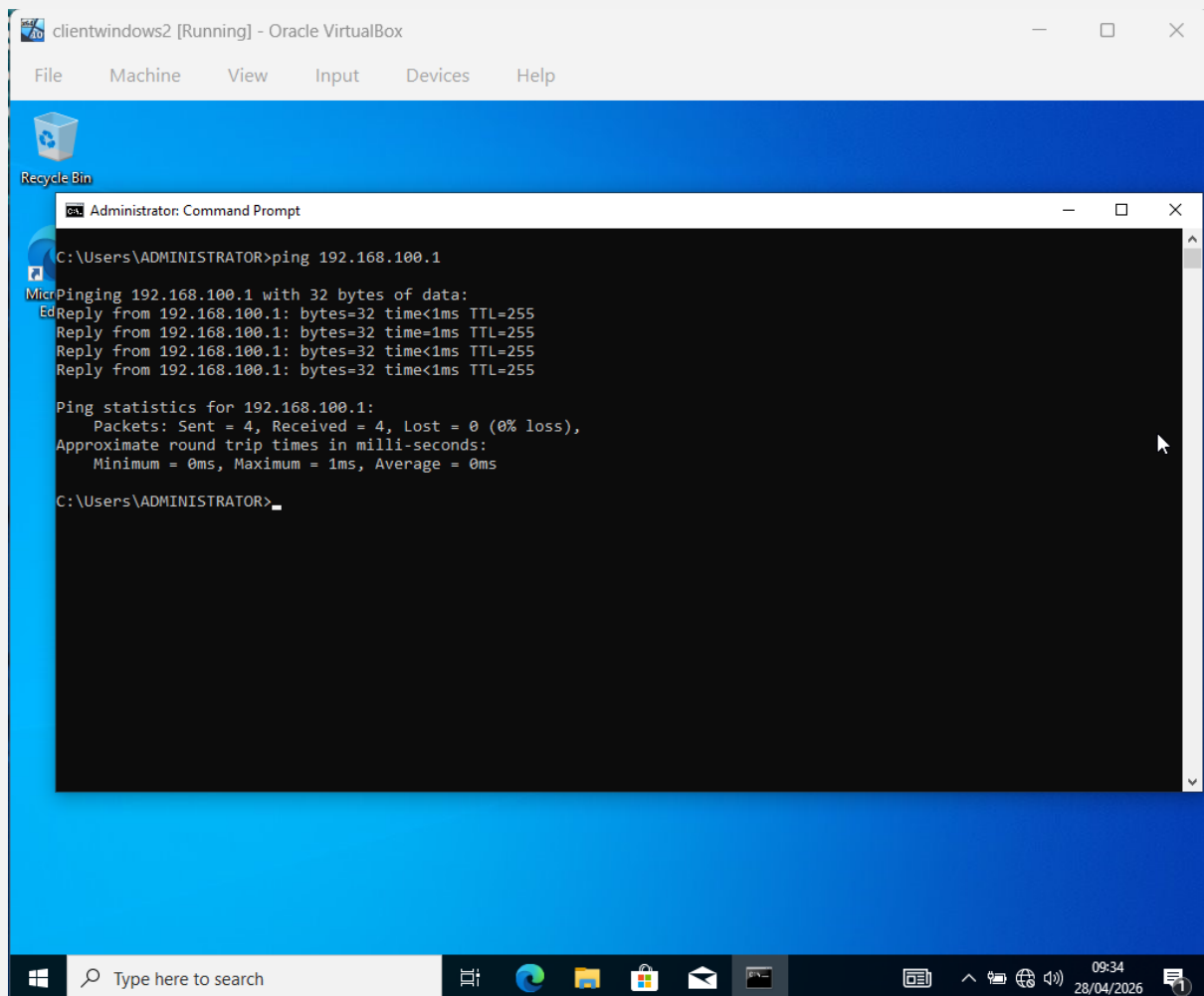
This confirms that the server is correctly configured within the network and ready to communicate with client machines.

Successful Ping from Client to Server



This screenshot shows a successful ping from the client machine to the server (192.168.100.10). All packets were received with 0% loss, confirming that network communication between the client and server is working correctly.

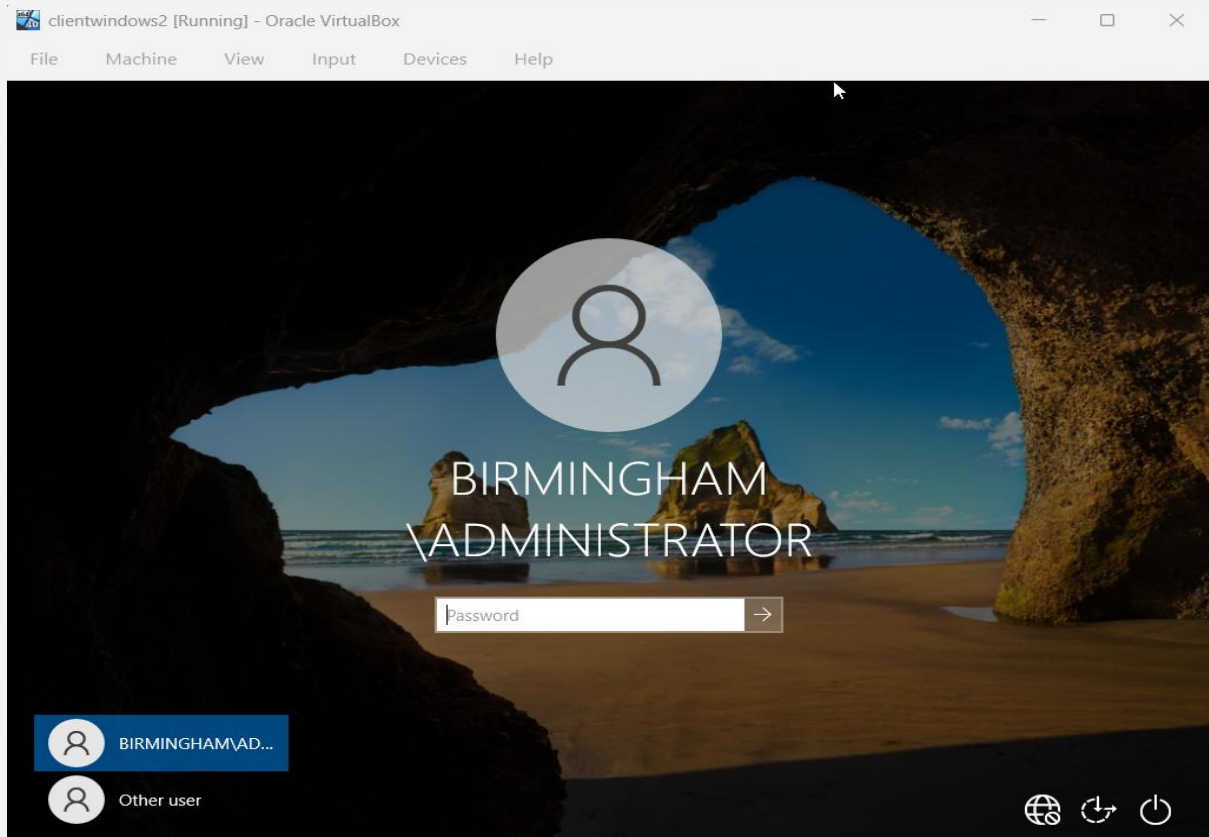
Successful Ping to Network Gateway



This screenshot shows a successful ping from the client machine to the network gateway (192.168.100.1).

All packets were received with 0% loss, confirming that the client can communicate with the network and that the overall network configuration is working correctly.

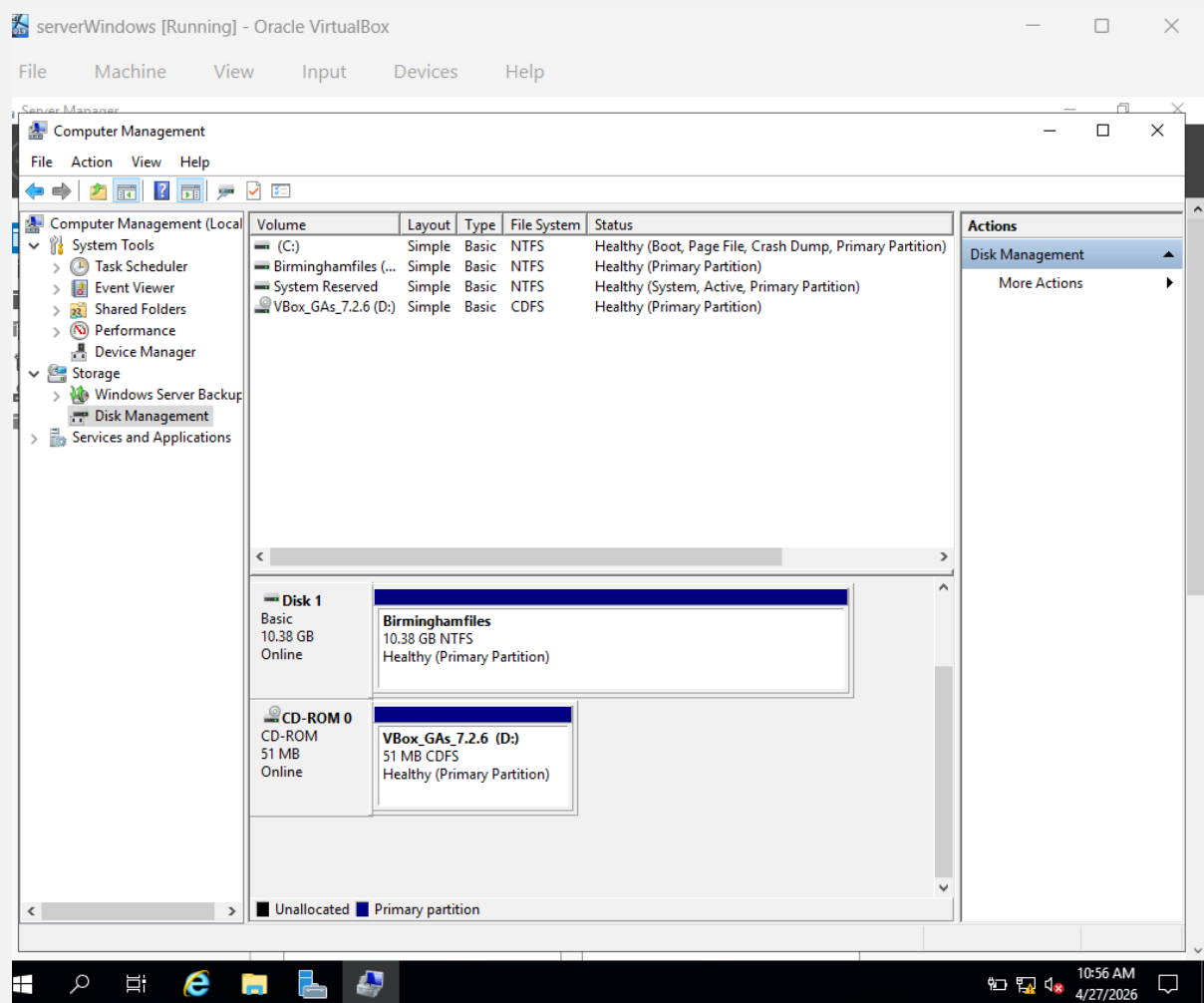
Client Login to Domain (BIRMINGHAM)



This screenshot shows the client machine login screen connected to the domain BIRMINGHAM.

The presence of the domain user (BIRMINGHAM\Administrator) confirms that the client is successfully joined to the domain.

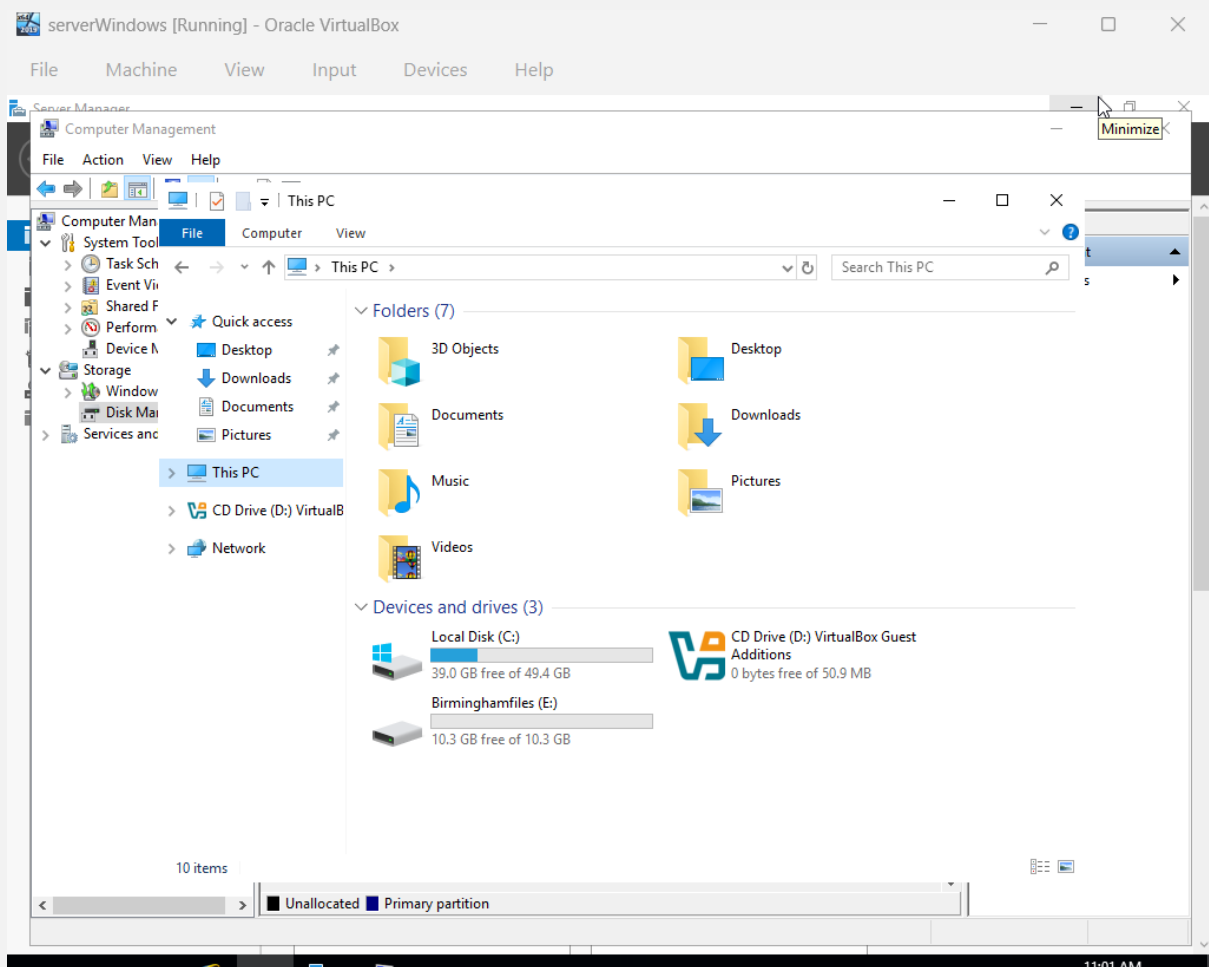
Creating and Formatting the Secondary Disk (E:)



This screenshot shows the Disk Management tool where the secondary disk was created and formatted.

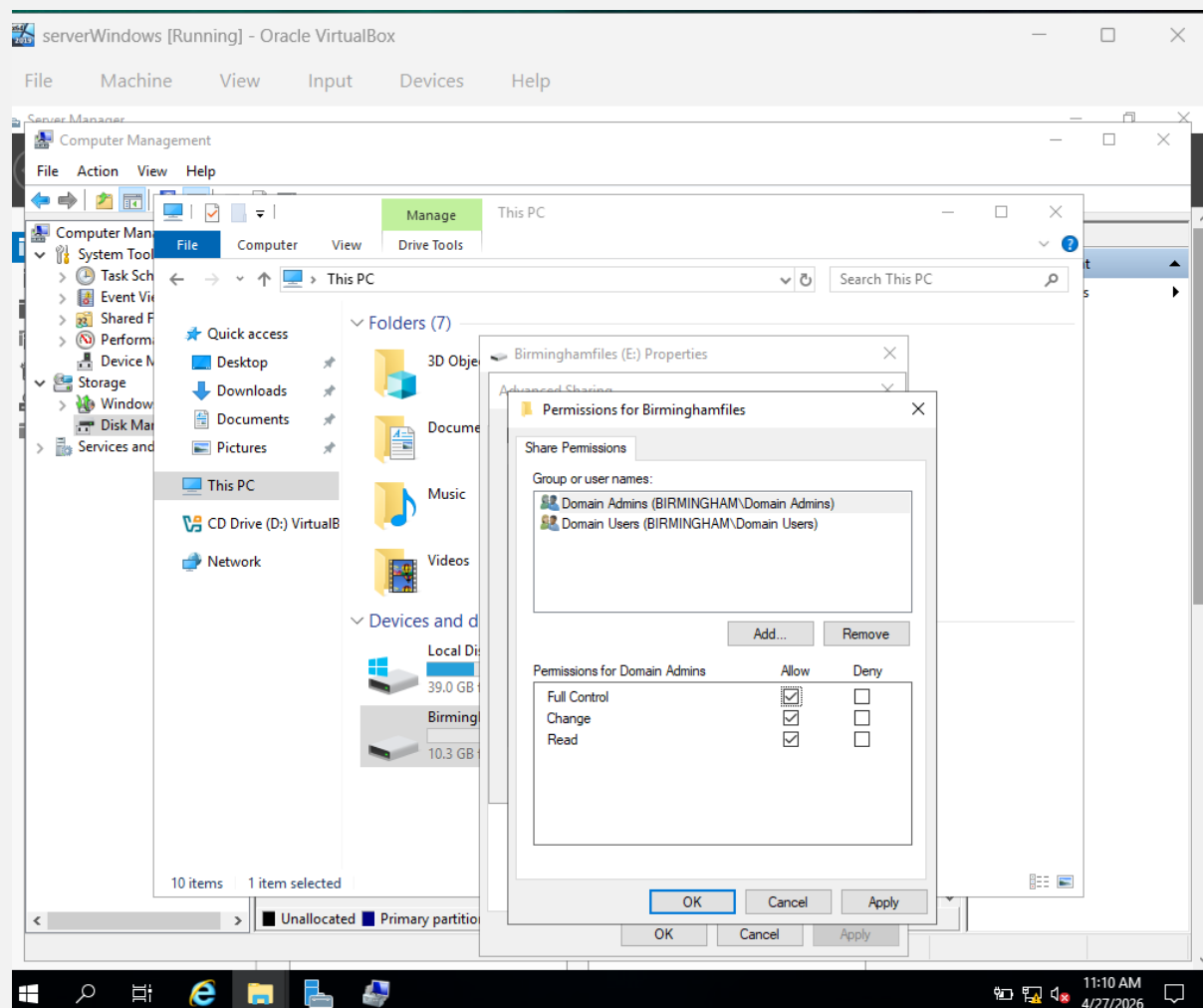
The disk was configured using the NTFS file system and assigned as drive E: named Birminghamfiles

Verification of the New Drive in This PC



This screenshot shows the newly created drive “Birminghamfiles (E:)” visible in This PC. This confirms that the disk has been successfully created, formatted, and mounted in the system.

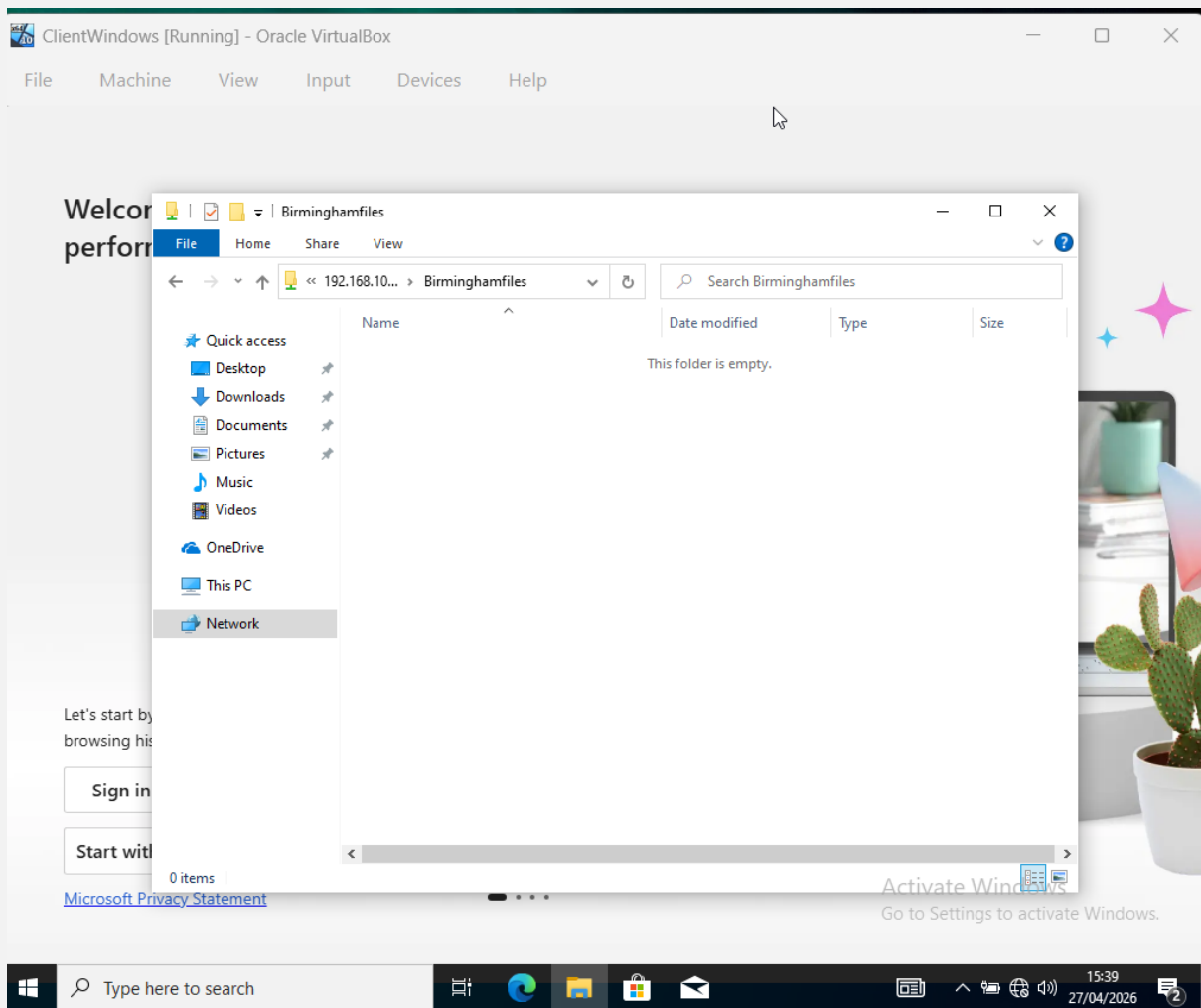
Configuring Shared Folder Permissions



This screenshot shows the configuration of shared folder permissions for Birminghamfiles.

The permissions were set so that Domain Users have Full Control access, ensuring they can read and modify files within the shared folder.

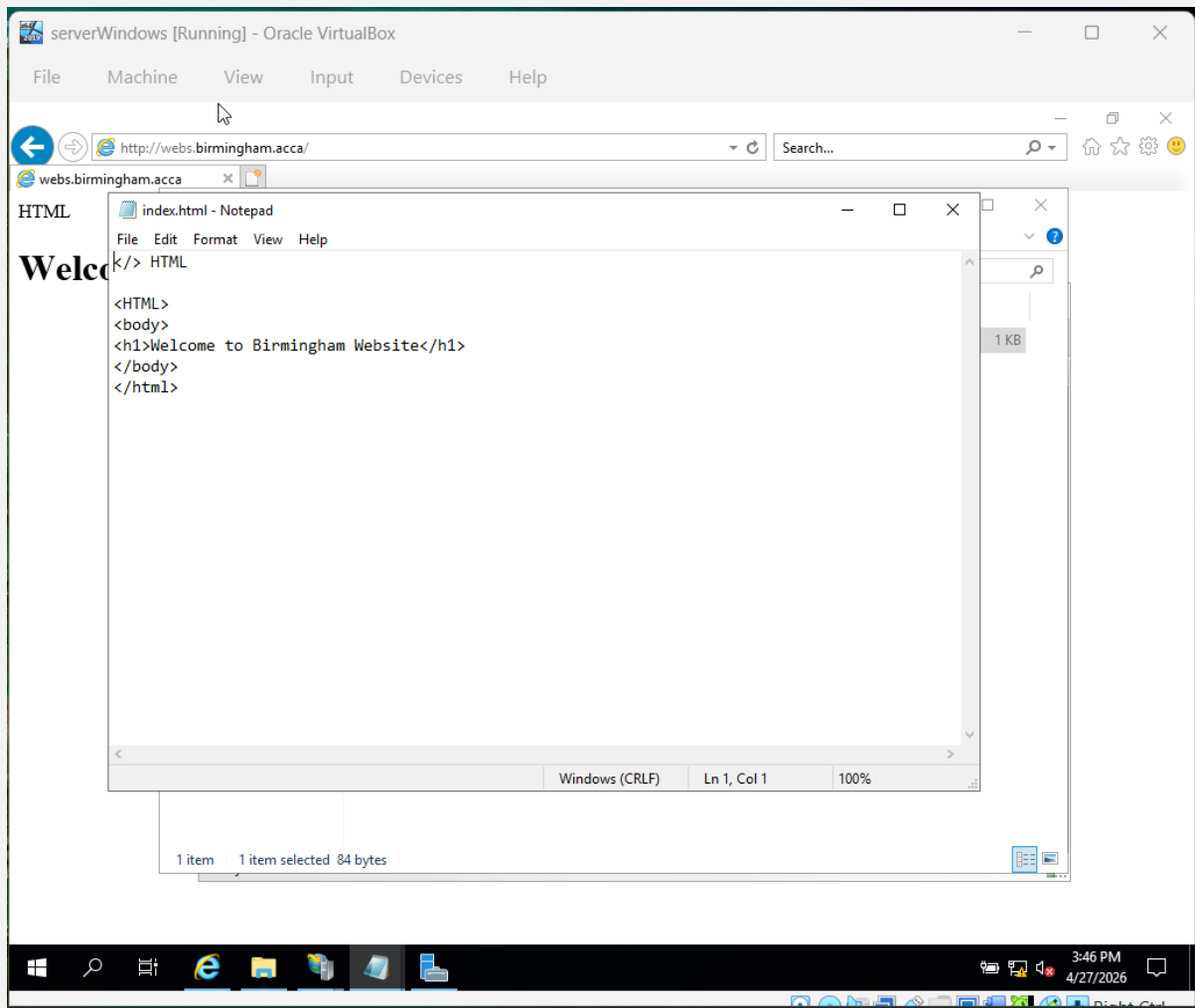
Accessing Shared Folder from Client Machine



This screenshot shows the client computer successfully accessing the shared folder Birminghamfiles through the network path.

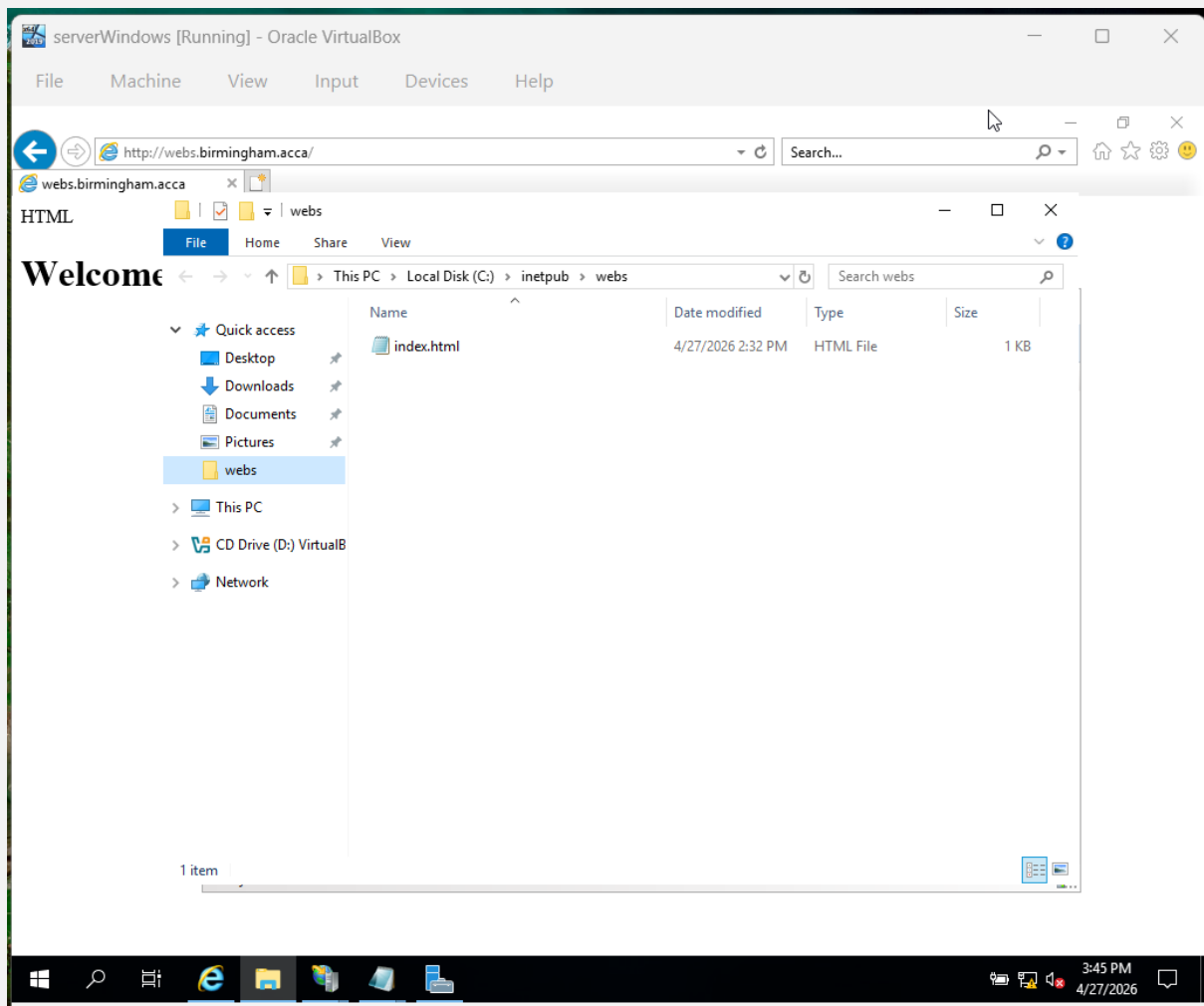
This confirms that the shared drive is accessible from another machine, meeting the requirement for network-wide access.

Creating Website HTML File



This screenshot shows the creation of the index.html file using Notepad. The file contains the message “Welcome to Birmingham Website” which will be displayed on the website.

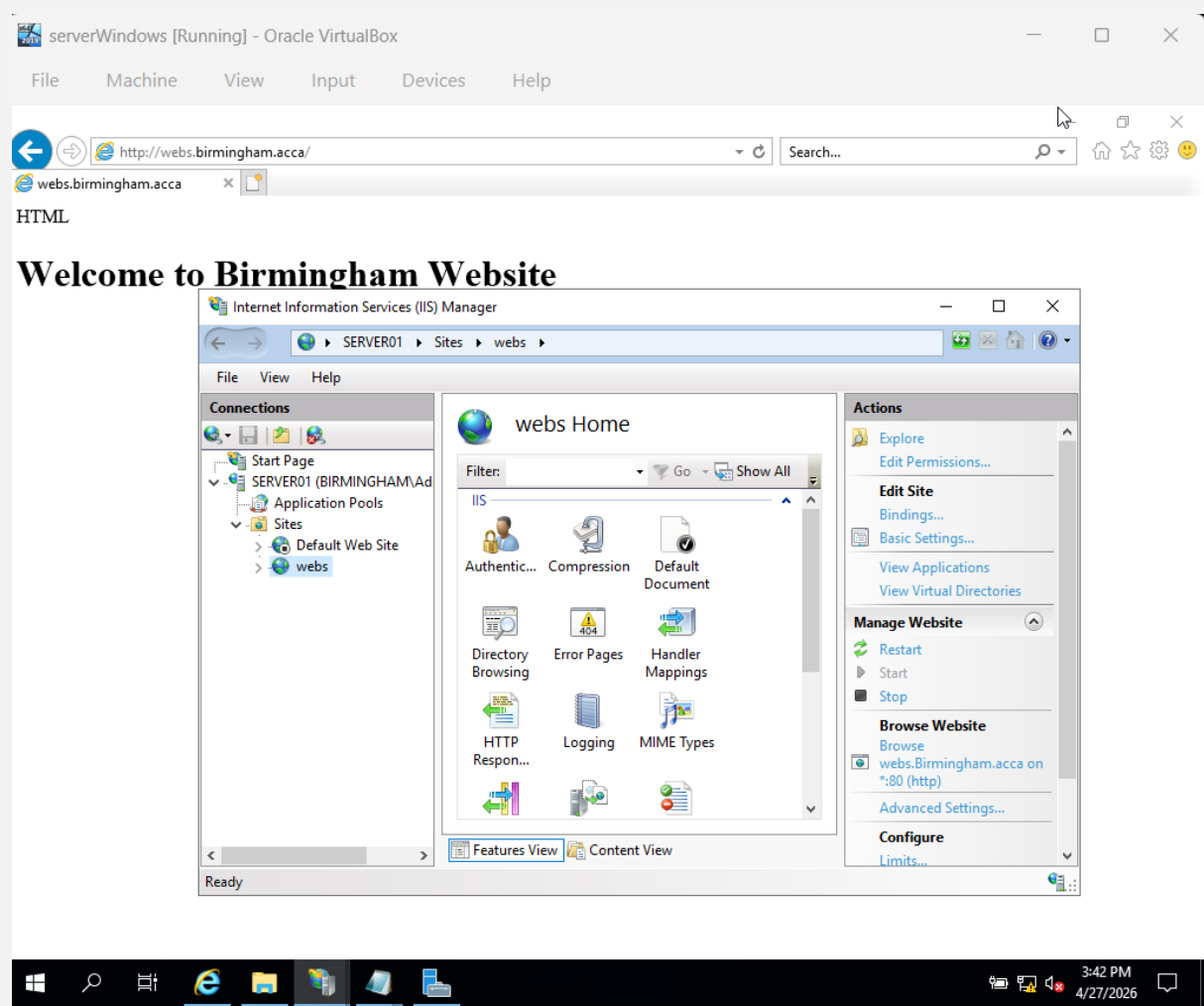
Website File Location in Server Directory



This screenshot shows the location of the website files on the server.

The index.html file is stored in the "inetpub\webs" directory, which is used by IIS to host the website content. This ensures that the web server can access and display the website correctly.

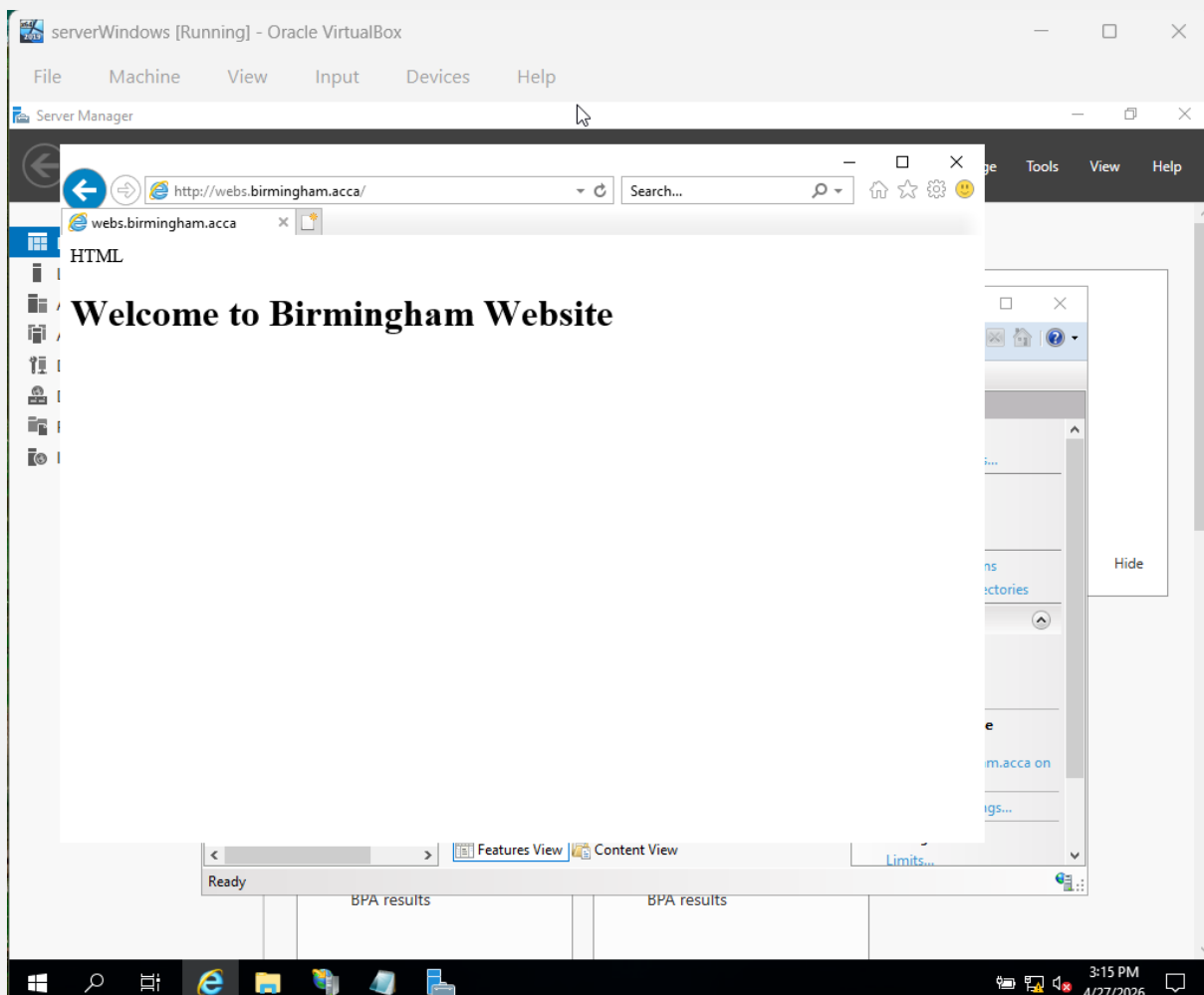
IIS Website Configuration (webs site)



This screenshot shows the configuration of the website in Internet Information Services (IIS) Manager.

The site named “webs” is created under the server and is properly configured. It includes features such as authentication, default documents, and bindings, which allow the website to be accessed using the domain name.

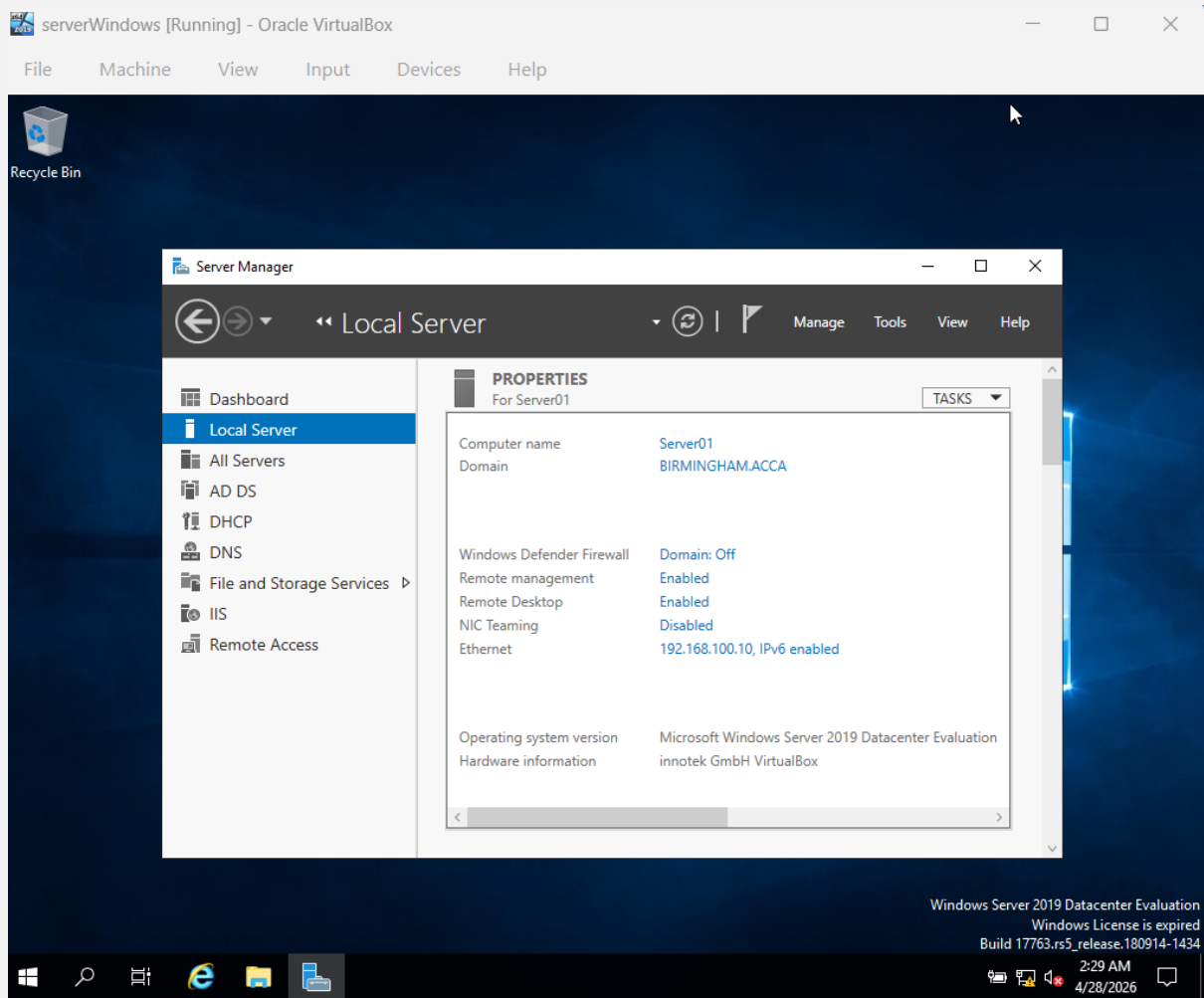
Website Access via Browser



This screenshot shows the successful access to the website through a web browser using the domain name `http://webs.birmingham.acca`.

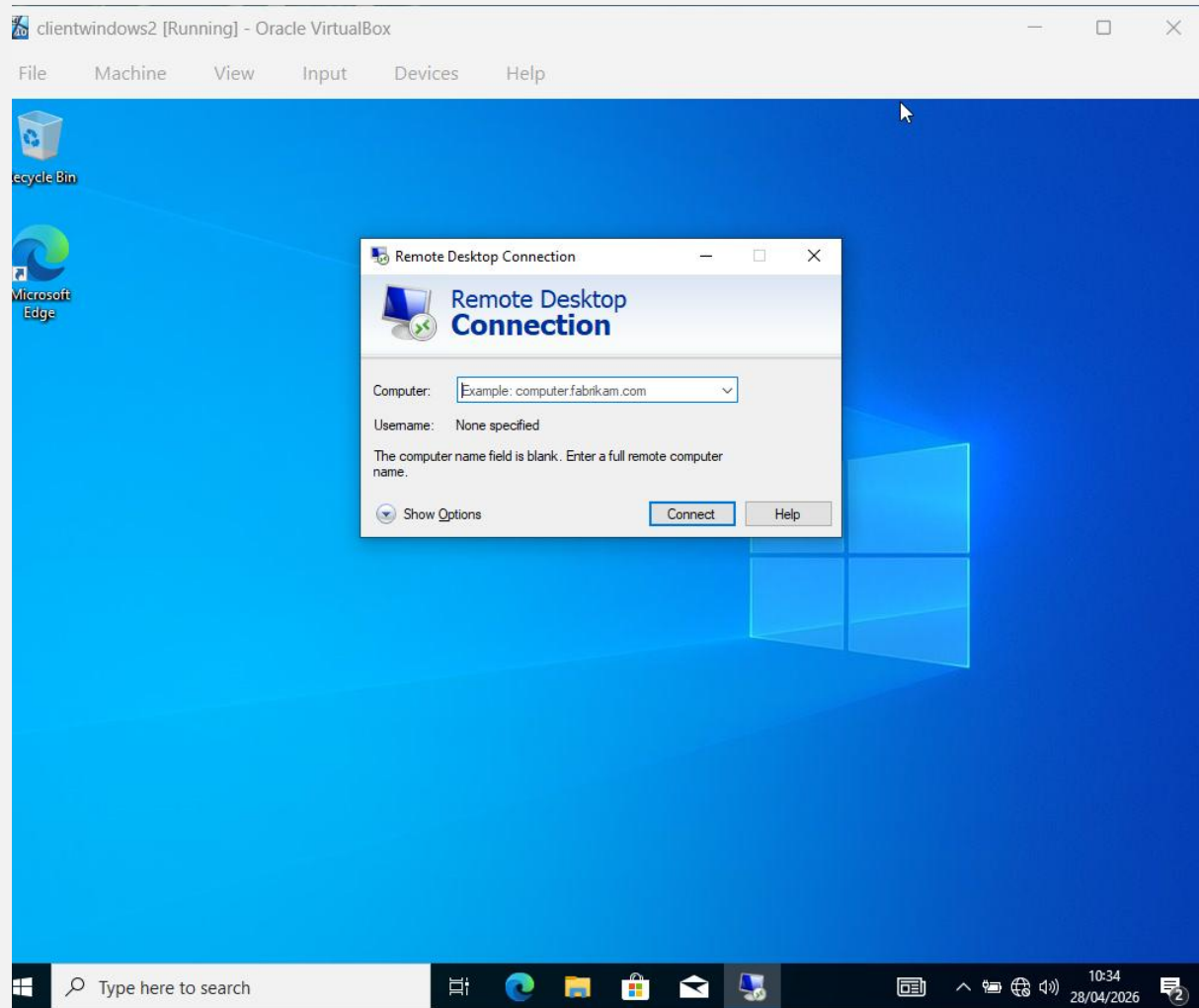
The page displays the message “Welcome to Birmingham Website,” confirming that the IIS server is correctly configured and the website is accessible to users on the network.

Remote Desktop Enabled on Server



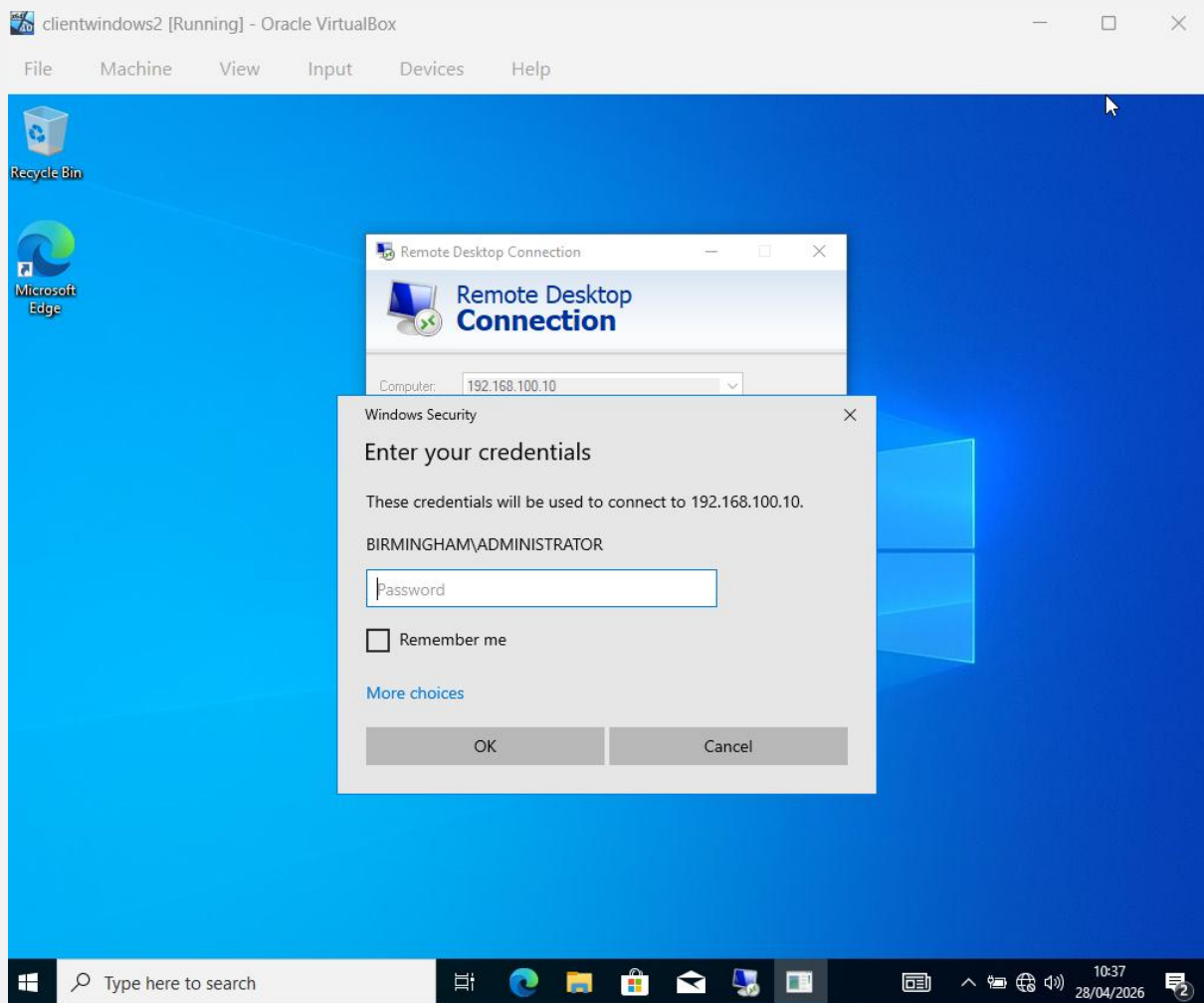
This screenshot shows that Remote Desktop is enabled on the server through Server Manager. This allows remote connections from other machines on the network to access the server.

Remote Desktop Connection (Client Side)



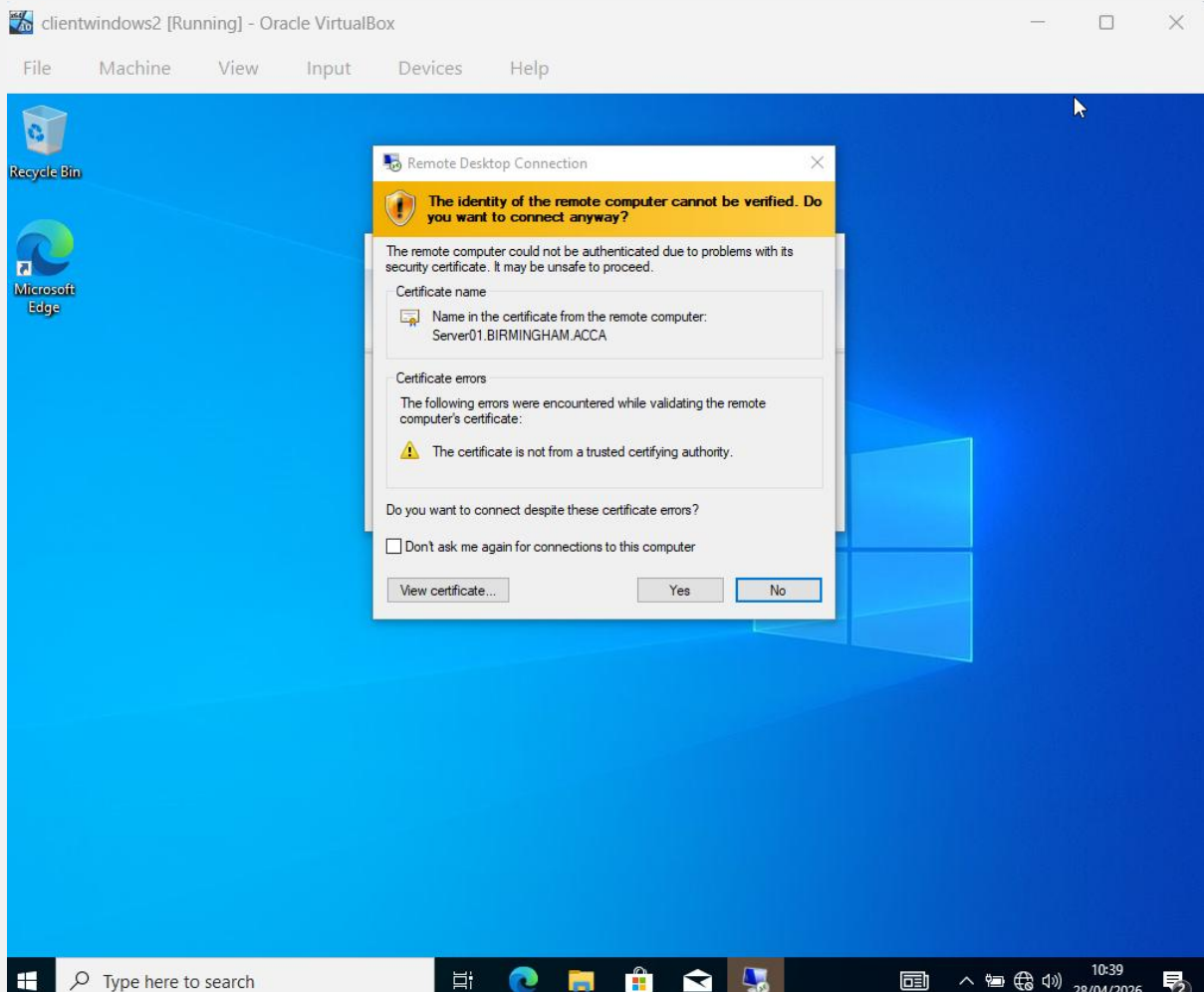
This screenshot shows the Remote Desktop Connection tool opened on the client machine. It is used to establish a remote connection to the server by entering the server's IP address or hostname.

Remote Desktop Login (Domain Credentials)



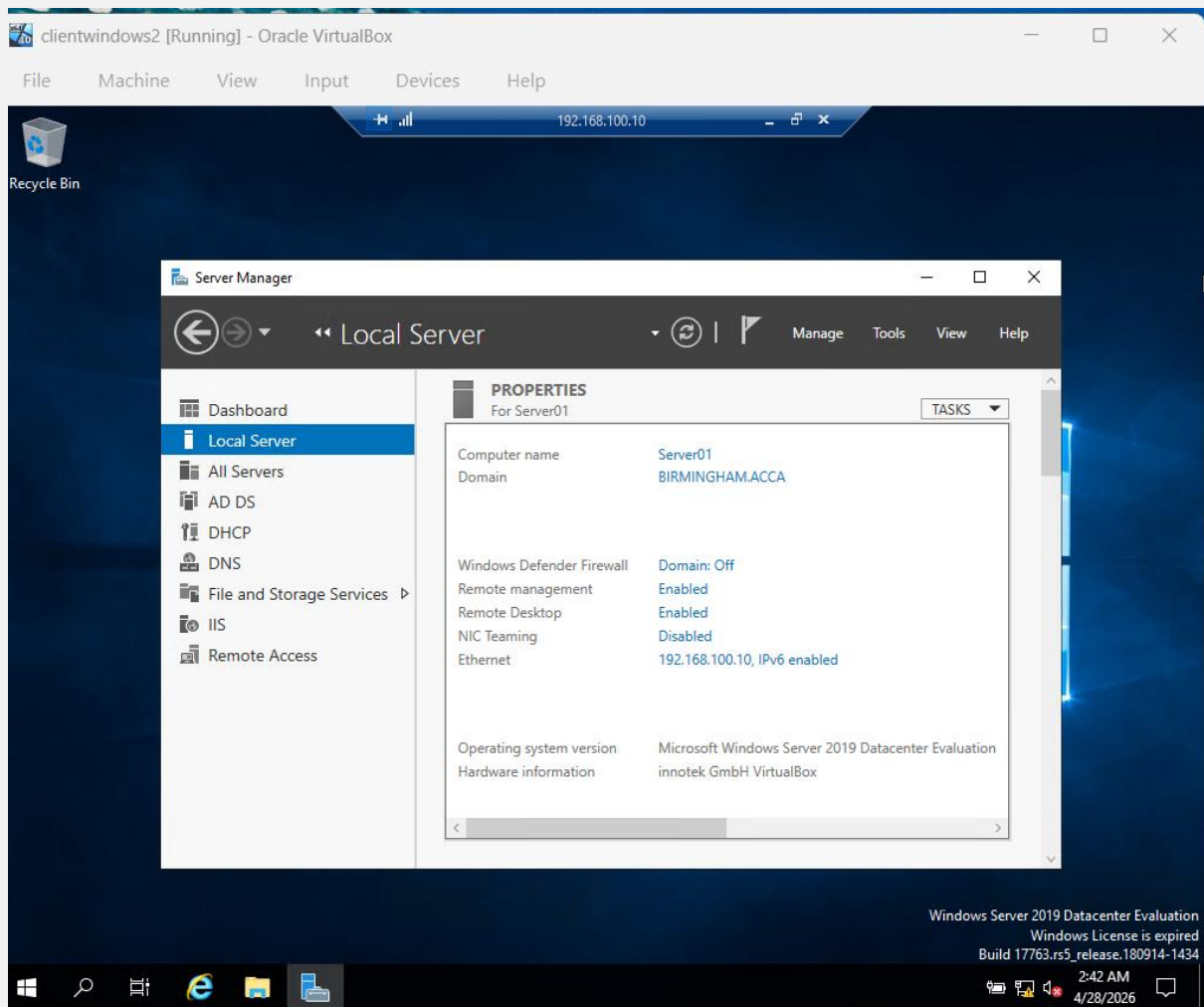
This screenshot shows the Remote Desktop login screen where domain credentials are required. The user is connecting to the server using the domain account BIRMINGHAM\Administrator, which confirms that authentication is configured correctly.

Certificate Warning during Remote Connection



This screenshot shows a security warning during the Remote Desktop connection. The certificate cannot be verified because it is not from a trusted authority. This is expected in a lab environment. The connection can still proceed safely by accepting the warning.

Successful Remote Desktop Session



This screenshot shows a successful Remote Desktop session where the client machine has connected to the server. The Server Manager is visible, confirming that full remote access to the server has been established.

Conclusion

This project successfully set up a Windows Server environment with working network connectivity between client and server. Services such as DHCP, file sharing, IIS, and Remote Desktop were correctly configured and tested. The system is fully functional and meets the assignment requirements.

