Mini Project: Active Directory Domain Setup in Virtualized Environment

Author: Rishav Kumar Thapa
Platform: Oracle VirtualBox
Client OS: Windows 10 Pro
Server OS: Windows Server 2022
Domain Name: crop.local

Date : 6/14/2025

1. Executive Summary

This project demonstrates a practical deployment of Active Directory Domain Services (AD DS) in a controlled lab environment using virtualization. It simulates an enterprise setup where a Windows Server 2022 machine acts as a Domain Controller (DC) managing users, DHCP, and DNS. A Windows 10 Pro client successfully joins the domain and interacts with AD-based services. The project includes Group Policy (GPO) enforcement for centralized control, such as desktop wallpaper configuration.

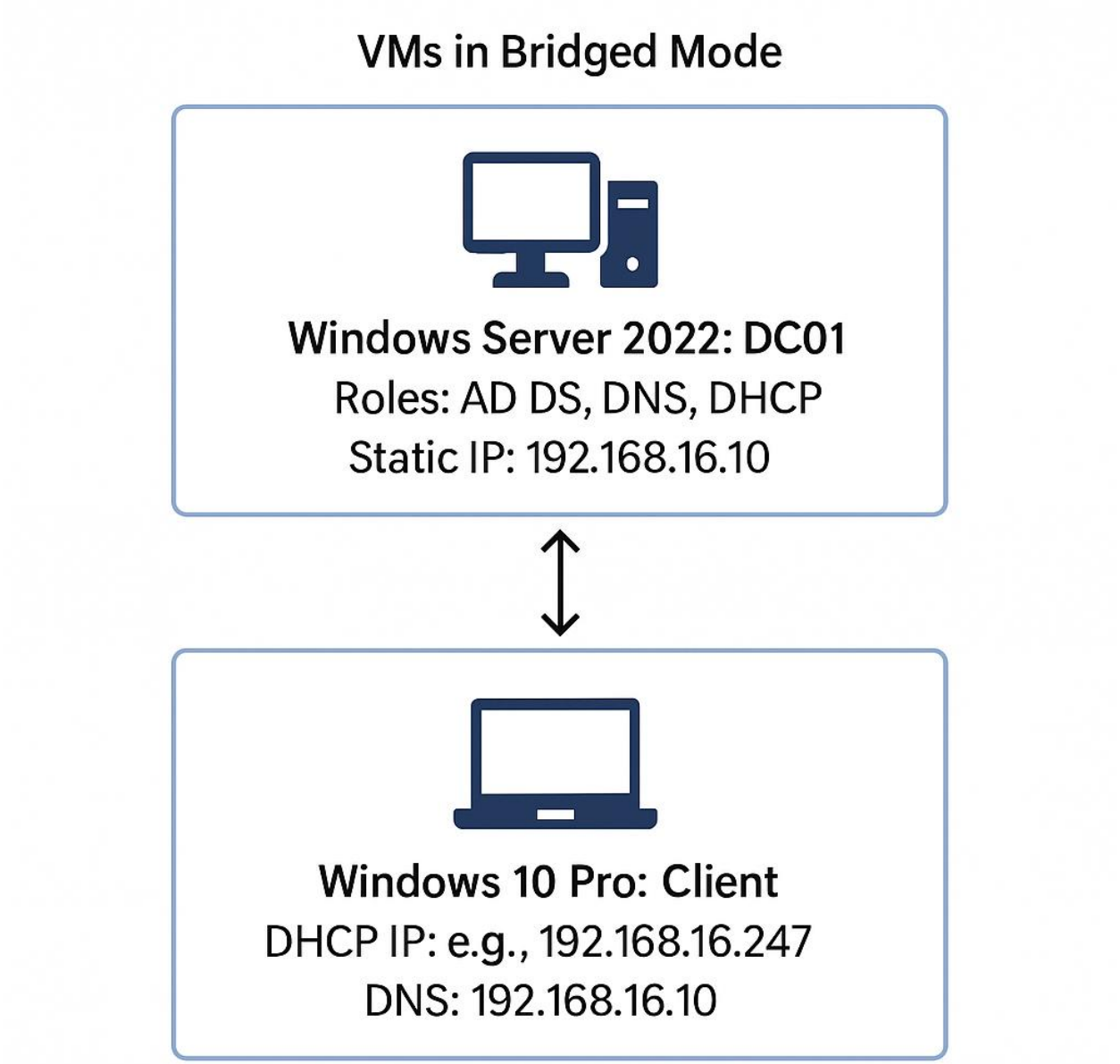
2. Project Objectives

- Create a virtual lab using Oracle VirtualBox
- Install and configure Windows Server 2022 as a Domain Controller
- Set up DHCP and DNS services
- Join a Windows 10 Pro client to the domain crop.local
- Create Organizational Units and domain user accounts
- Test login, network, and domain communication
- Apply Group Policy Objects for user environment control

3. Tools & Technologies Used

- Oracle VirtualBox – for virtualization
- Windows Server 2022 – Domain Controller (DC), DNS, DHCP
- Windows 10 Pro – domain-joined client
- Active Directory Users and Computers (ADUC)
- Group Policy Management Console (GPMC)
- IPConfig / Ping – for network testing
- Server Manager – role and feature installation

4. Network Architecture Overview



5. Implementation Steps for Setup

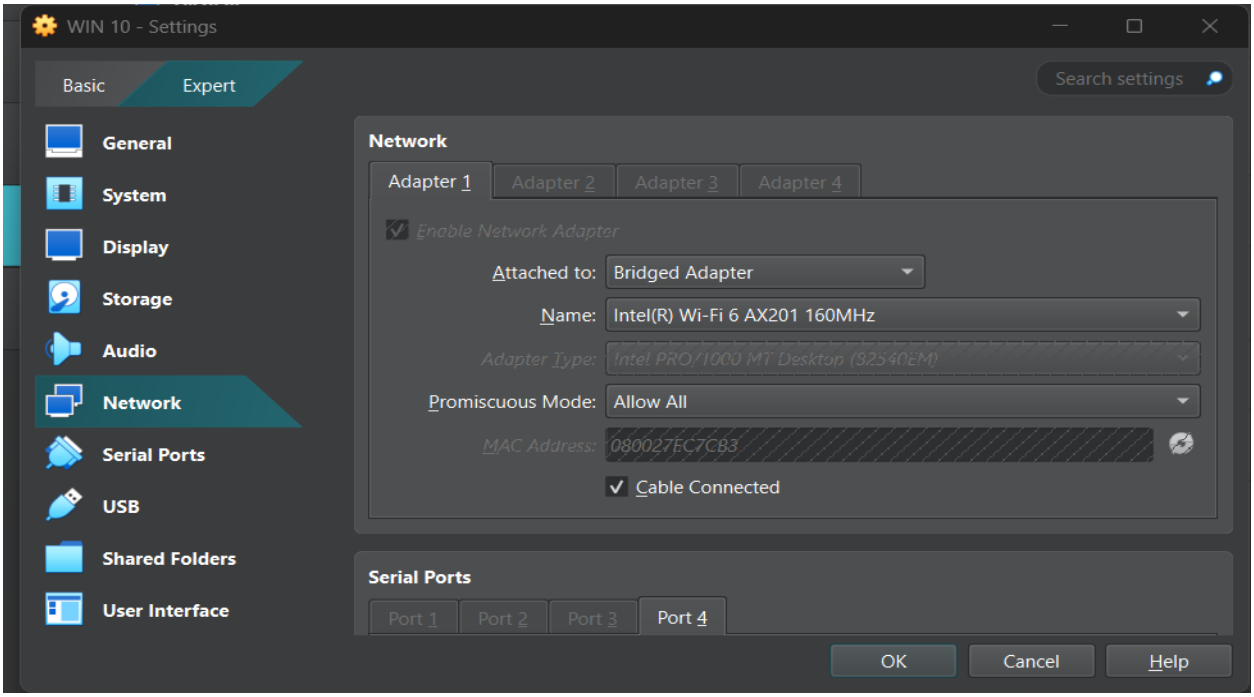
Step 1: Virtual Machine Setup & Networking Configuration

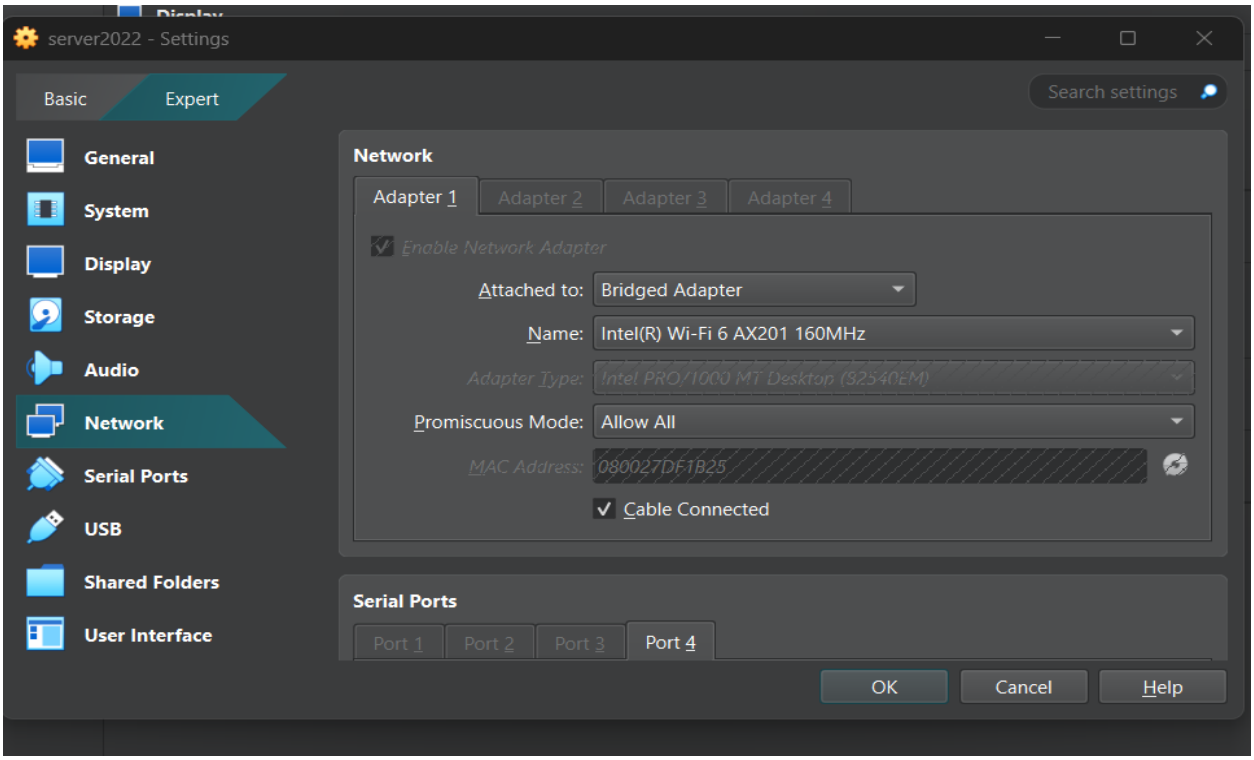
To simulate a real-world enterprise environment, two virtual machines were created using **Oracle VirtualBox**:

- **Windows Server 2022**: Acts as the Domain Controller (DC), DNS server, and DHCP server.
- **Windows 10 Pro**: Acts as the domain-joined client system.

VirtualBox Network Configuration:

Both virtual machines were configured to use the **Bridged Adapter** network mode. This setup allows each VM to receive an IP address from the same network as the host machine, simulating a real-world LAN setup and enabling direct communication between client and server.





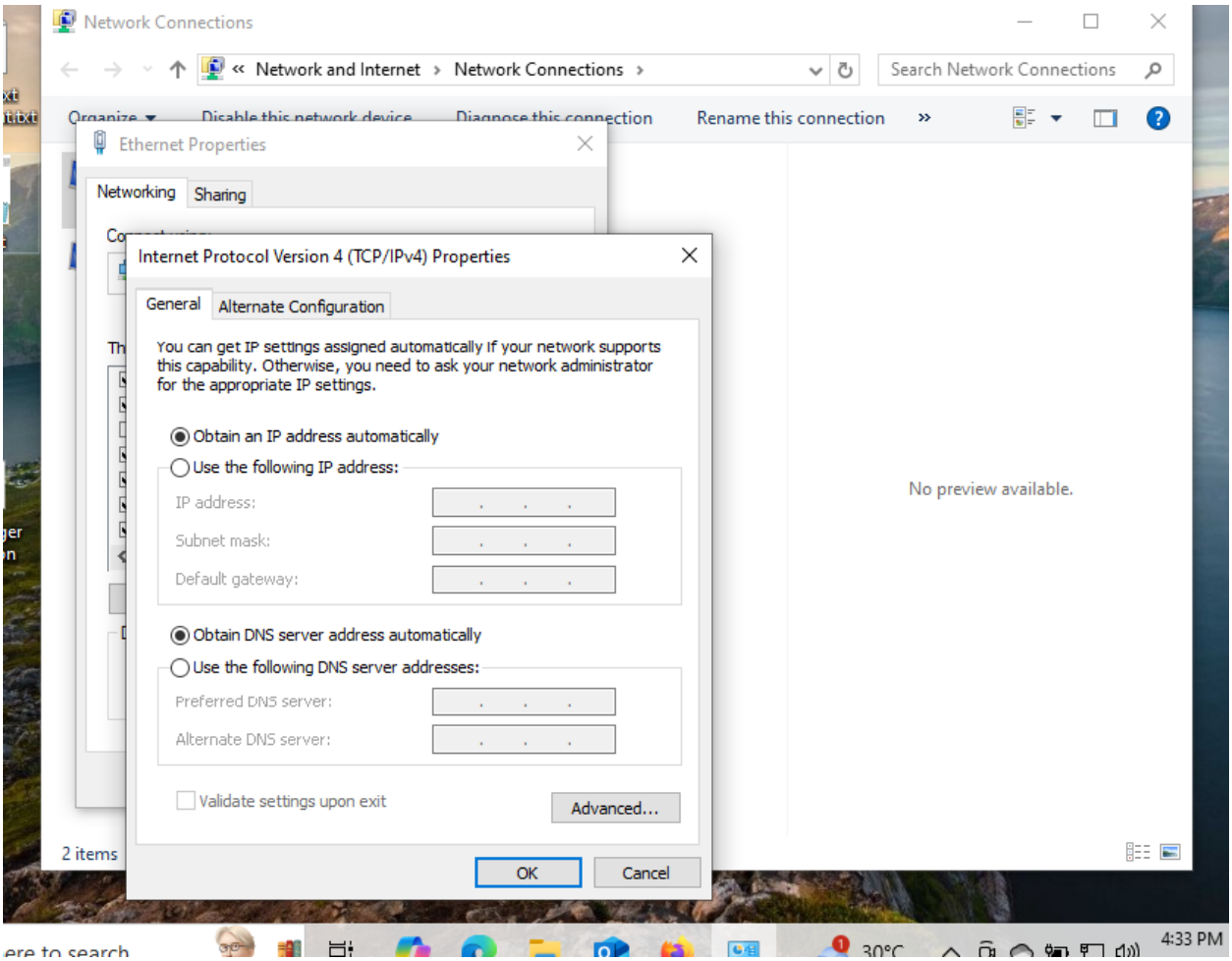
Step 2: Configuring Windows 10 to Receive IP from DHCP

After setting up the Windows Server 2022 machine to act as the DHCP server, the Windows 10 Pro client machine was configured to automatically obtain its IP address via **DHCP**.

Client (Windows 10 Pro) – Network Configuration:

1. Opened **Control Panel > Network and Sharing Center > Change adapter settings**.
2. Right-clicked on the active network adapter and selected **Properties**.
3. Chose **Internet Protocol Version 4 (TCP/IPv4)** and clicked **Properties**.
4. Selected:
    - **Obtain an IP address automatically**
    - **Obtain DNS server address automatically**

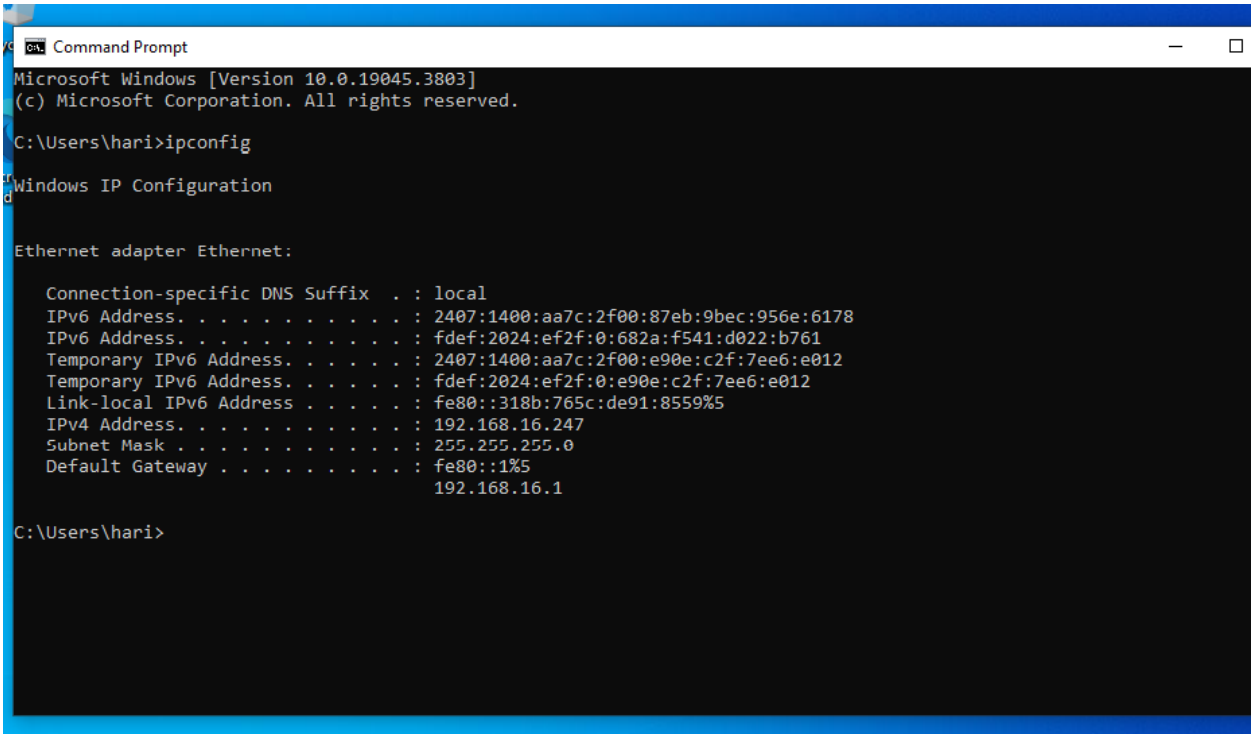
Rishav



Verification:

- Opened **Command Prompt** and ran ipconfig.
- Confirmed that the Windows 10 client successfully received an IP address from the **DHCP scope configured on the server** (e.g., 192.168.16.247)

Rishav



Step 3: Configuring Static IP on Windows Server 2022 and change hostname

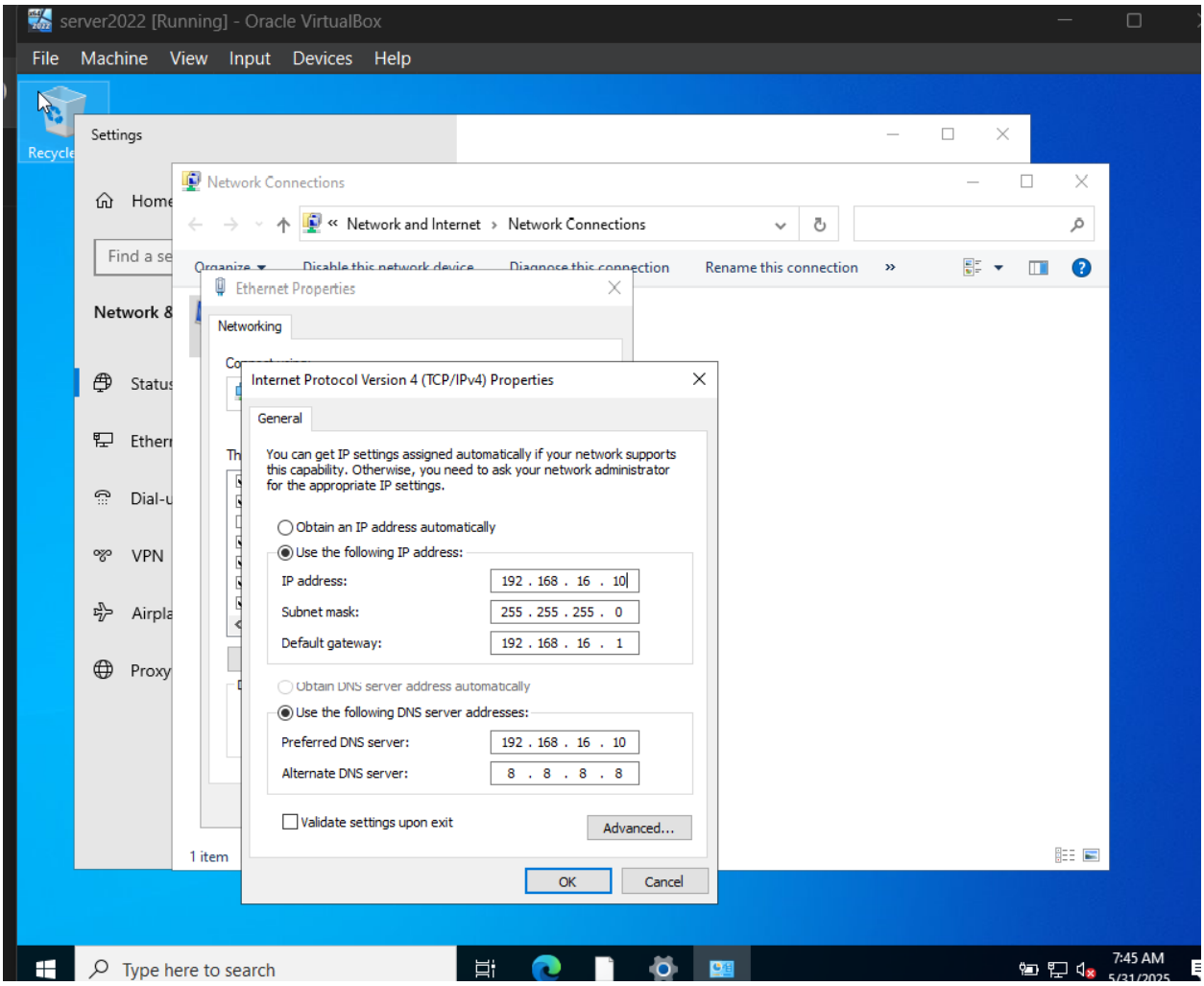
To ensure consistent network communication and reliable DNS resolution for domain services, a **static IP address** was assigned to the Windows Server 2022 machine. This server will later function as the **Domain Controller, DNS, and DHCP server**.

Server (Windows Server 2022) – Static IP Configuration:

1. Opened **Control Panel > Network and Sharing Center > Change adapter settings**.
2. Right-clicked on the active network adapter and selected **Properties**.
3. Selected **Internet Protocol Version 4 (TCP/IPv4)** and clicked **Properties**.
4. Entered the configuration needed.

By using its own IP as the preferred DNS server, the server is prepared to run Active Directory and DNS services without relying on external name resolution.

Rishav



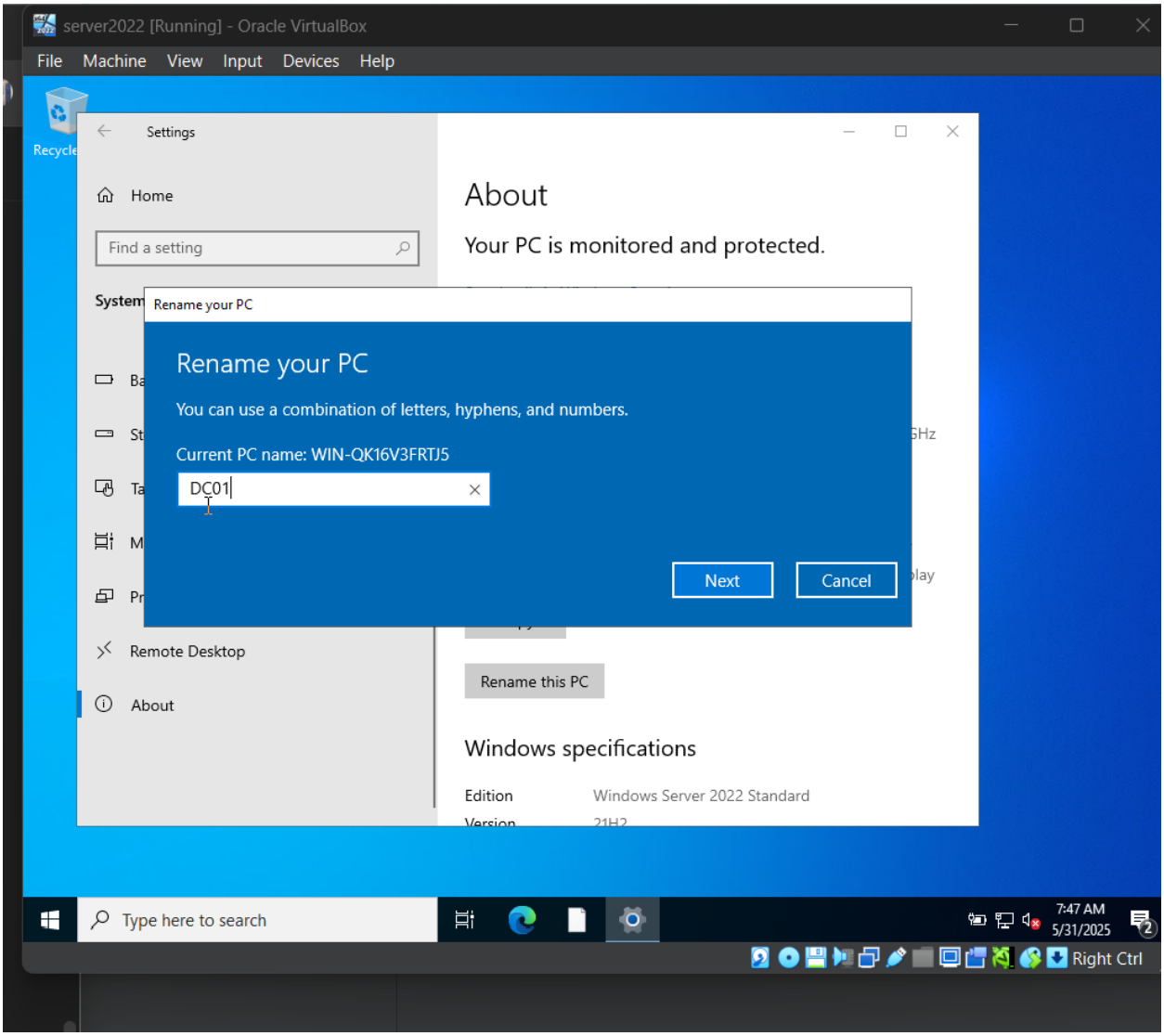
The server successfully retained the assigned **static IP configuration**. This was confirmed using the ipconfig command, which displayed the following network settings:

- **IPv4 Address**: 192.168.16.10
- **Subnet Mask**: 255.255.255.0
- **Default Gateway**: 192.168.16.1
- **Preferred DNS Server**: Set to the server's own IP (192.168.16.10)

The **DNS suffix** appeared as .local, aligning with the intended Active Directory domain (crop.local). These settings confirm the server is properly positioned to act as a domain controller and DNS server within the virtualized bridged network

Rishav

To maintain clarity and follow best practices in server naming conventions, the hostname of the Windows Server 2022 machine was changed from its default-generated name to DC01. Renaming the server to a meaningful and identifiable name before promoting it to a Domain Controller is a critical step in enterprise network design.



Step 4: Active Directory Domain Controller Setup

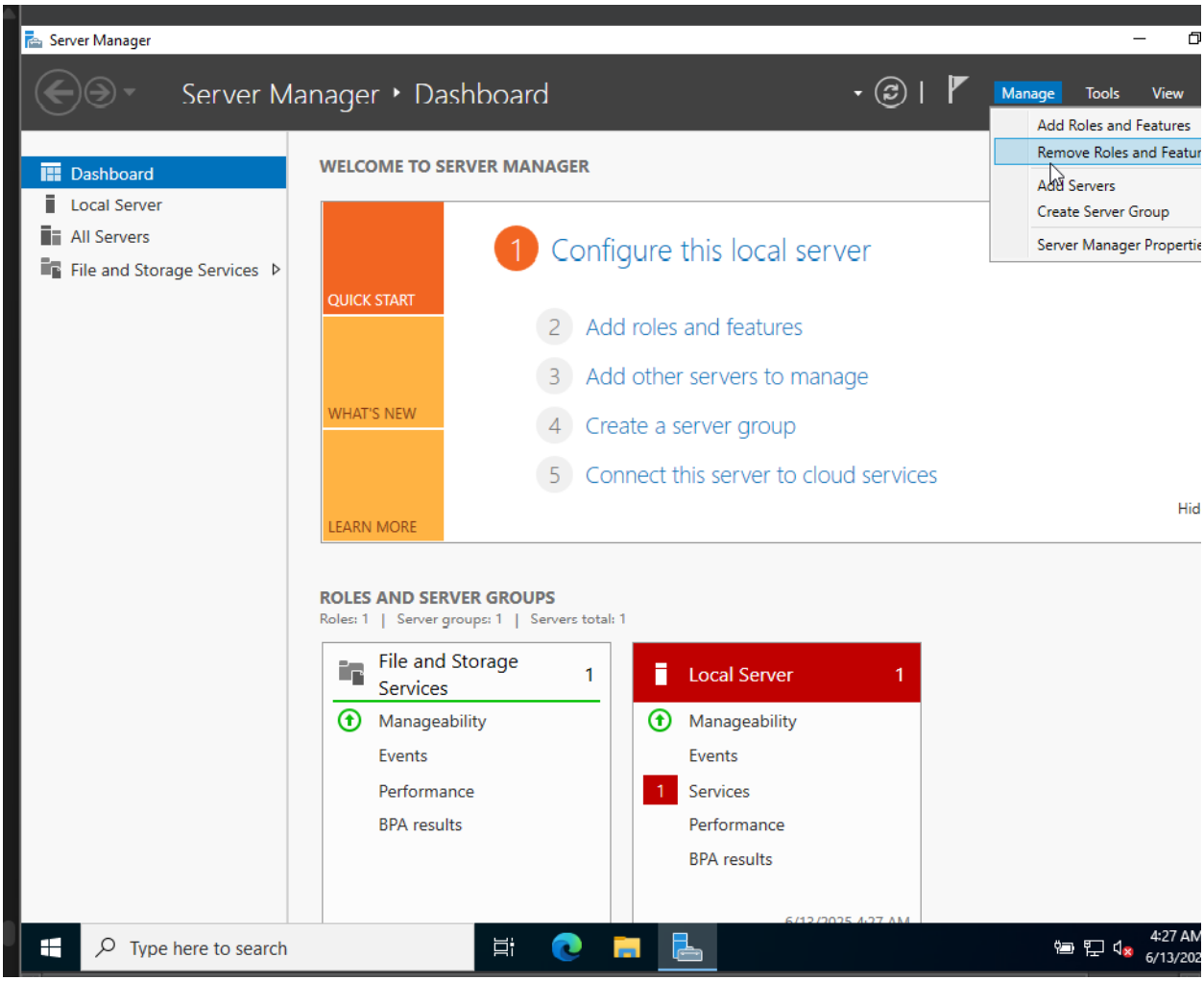
- **step 1: Add Roles and Features Wizard – Launching**

The configuration process began by launching the **Server Manager** and selecting:

Manage > Add Roles and Features

Rishav

This wizard guides the administrator through the installation of required server roles like **Active Directory Domain Services (AD DS)**, **DNS Server**, and **DHCP Server**, all of which are essential for domain environment setup.



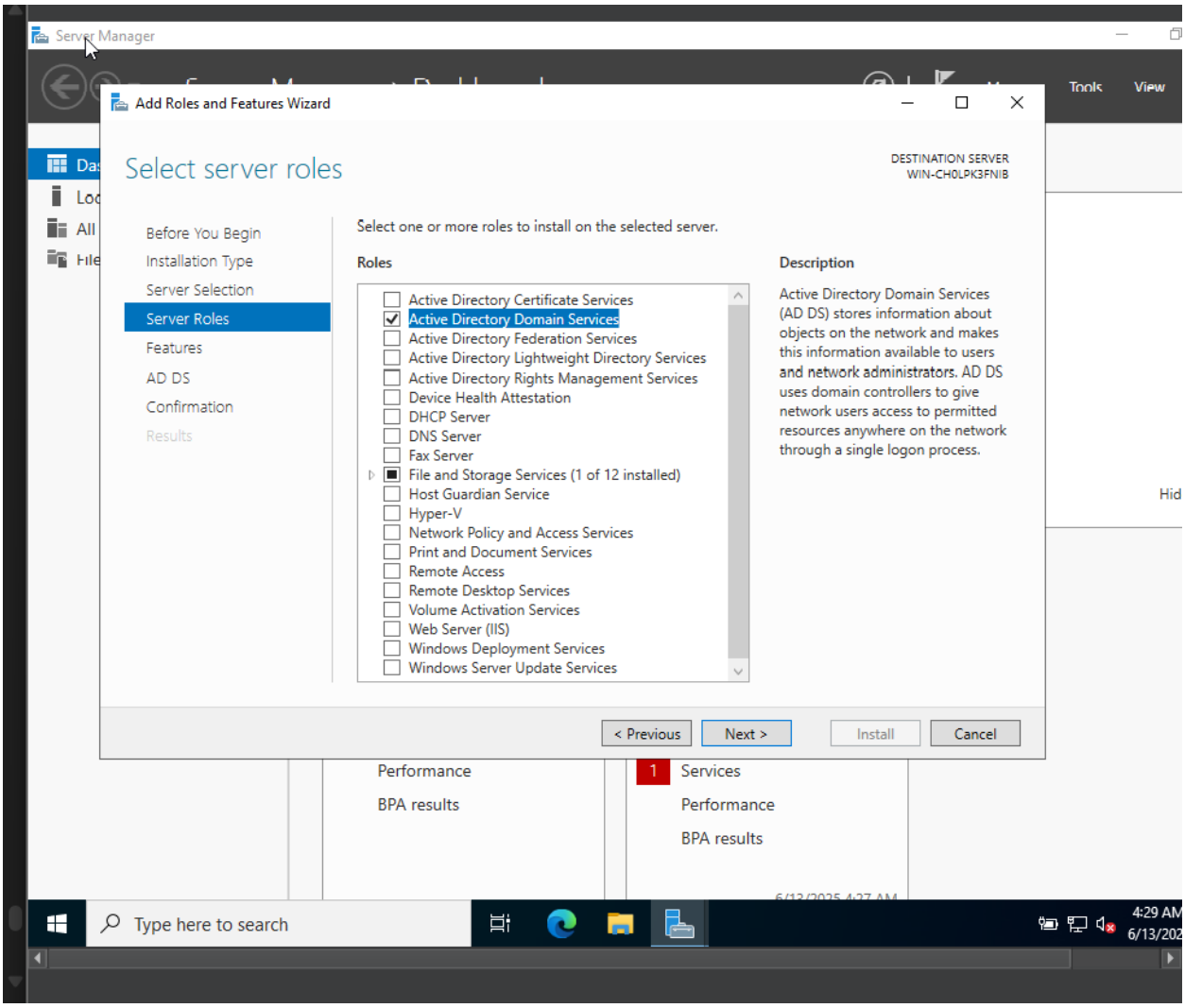
- **Step 2: Selecting Server Roles**

In the **"Select Server Roles"** section of the **Add Roles and Features Wizard**, the following roles were selected to configure a fully functional domain environment:

1. **Active Directory Domain Services (AD DS)**
   Enables the server to operate as a Domain Controller (DC), which stores and manages the directory of users, computers, and other resources within the domain.

2. **DNS Server**
   Required for domain name resolution. AD DS is tightly integrated with DNS, and configuring this role ensures the domain controller can resolve both internal domain names and assist client systems in locating domain services.

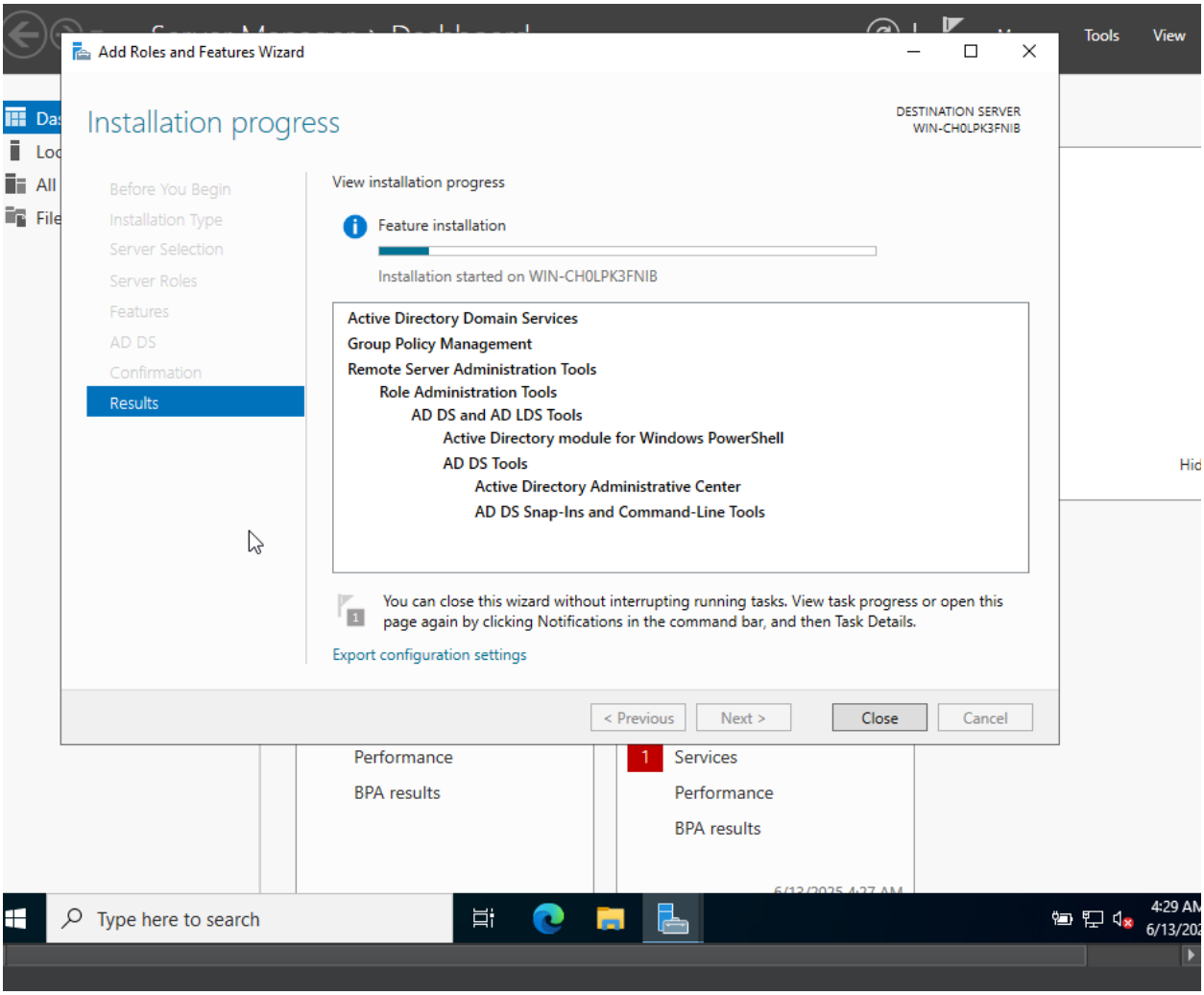
Rishav



- **Step 3: Installing Active Directory Domain Services and Management Tools**

Following the selection of necessary roles, the installation of **Active Directory Domain Services (AD DS)** and its associated management tools commenced.

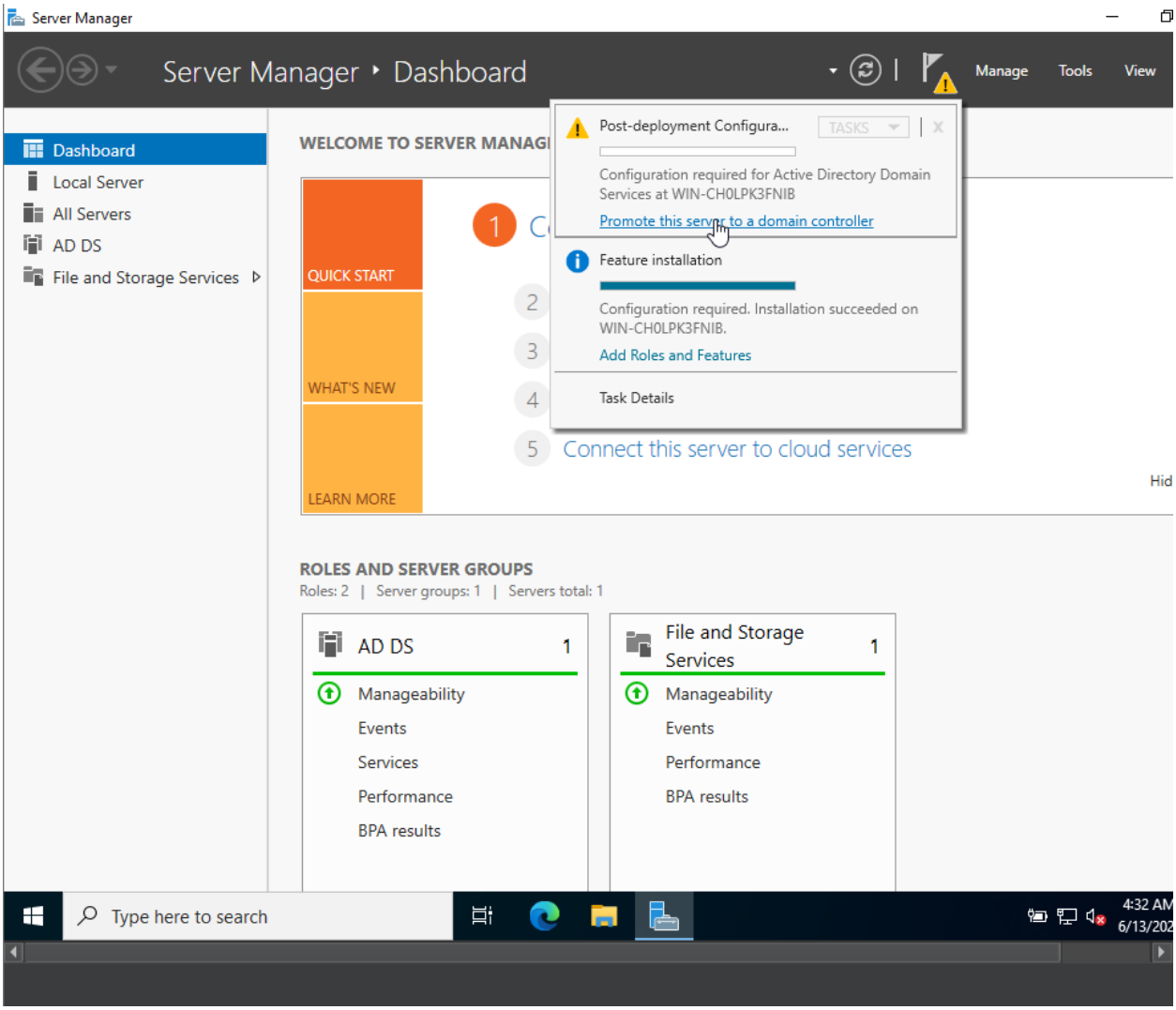
Rishav



- **Step 4: Promoting the Server to a Domain Controller**

After the successful installation of Active Directory Domain Services, the server was promoted to a domain controller by selecting **“Promote this server to a domain controller”** in the Server Manager post-installation notification.

Rishav



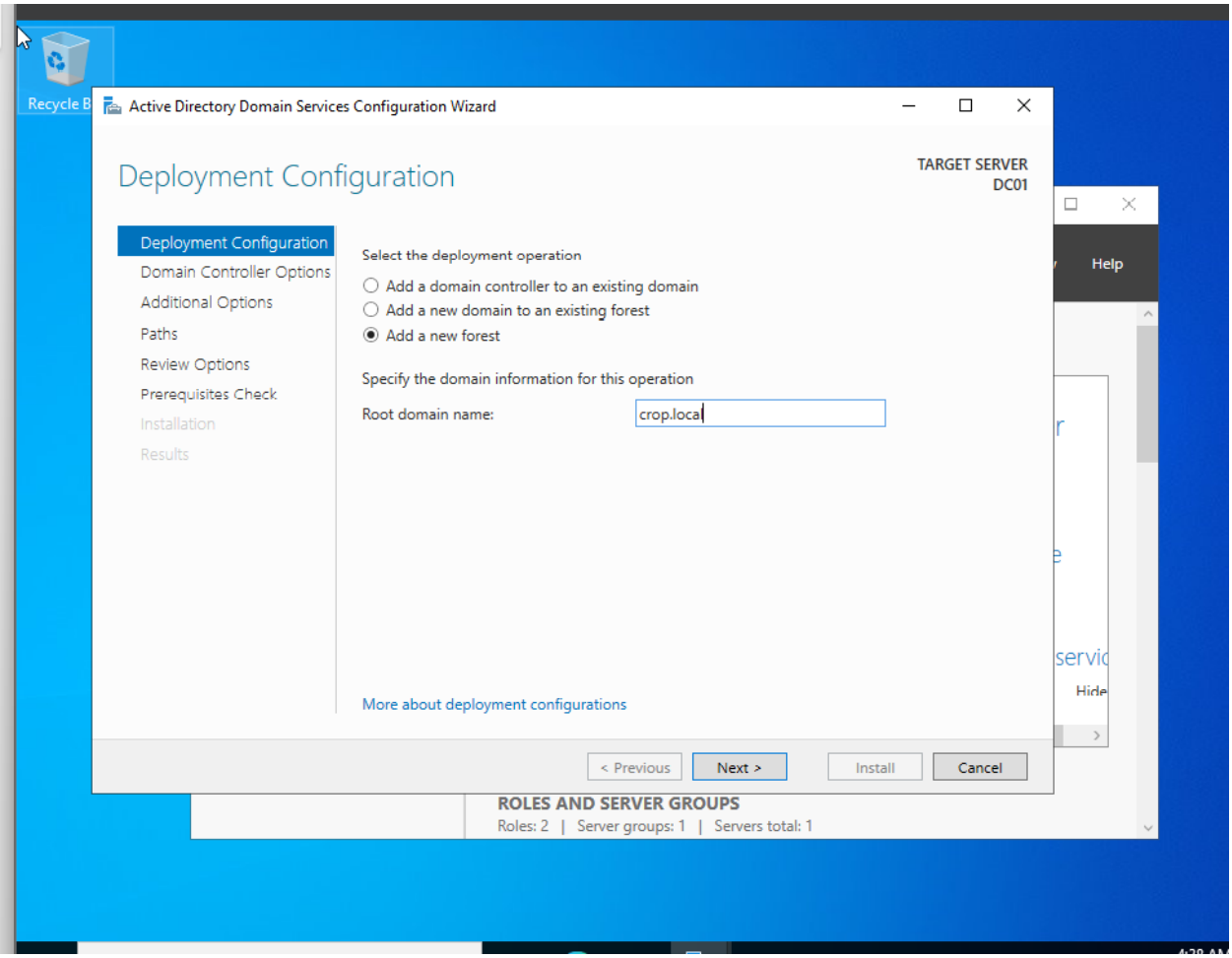
- **Step 5: Deployment Configuration /Creating a New Forest**

Within the **Active Directory Domain Services Configuration Wizard**, the option to **"Add a new forest"** was selected to establish a new Active Directory environment.

The root domain name was set as **crop.local**, defining the namespace for all domain objects and services. This step initiated the creation of a fresh Active Directory forest, which serves as the highest-level container for all domains, users, groups, and policies within the network.

Selecting this option allows full control over the domain environment and is ideal for new infrastructure deployments.

Rishav



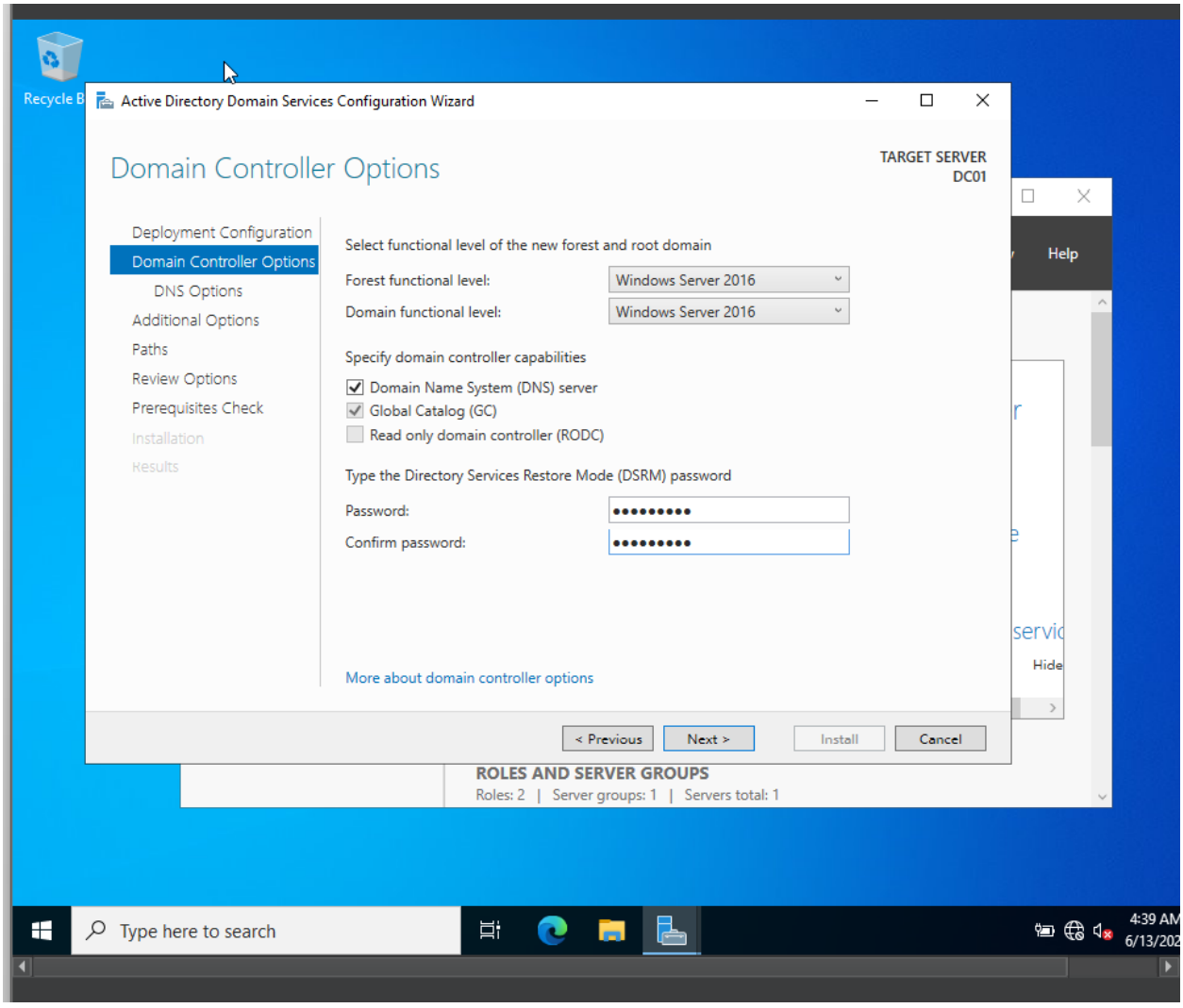
- **Step 6: Domain Controller Options Configuration**

In this step of the **Active Directory Domain Services Configuration Wizard**, key domain controller settings were configured:

- **Forest Functional Level** and **Domain Functional Level** were both set to **Windows Server 2016**. This defines the minimum supported Windows Server version for domain controllers and enables advanced Active Directory features compatible with this version.
- The server was configured to act as a **DNS Server**, which is required to support Active Directory domain name resolution and service location within the network.
- The **Global Catalog (GC)** option was enabled, allowing this domain controller to hold a partial replica of all objects in the forest to facilitate efficient user logon and directory searches.

Rishav

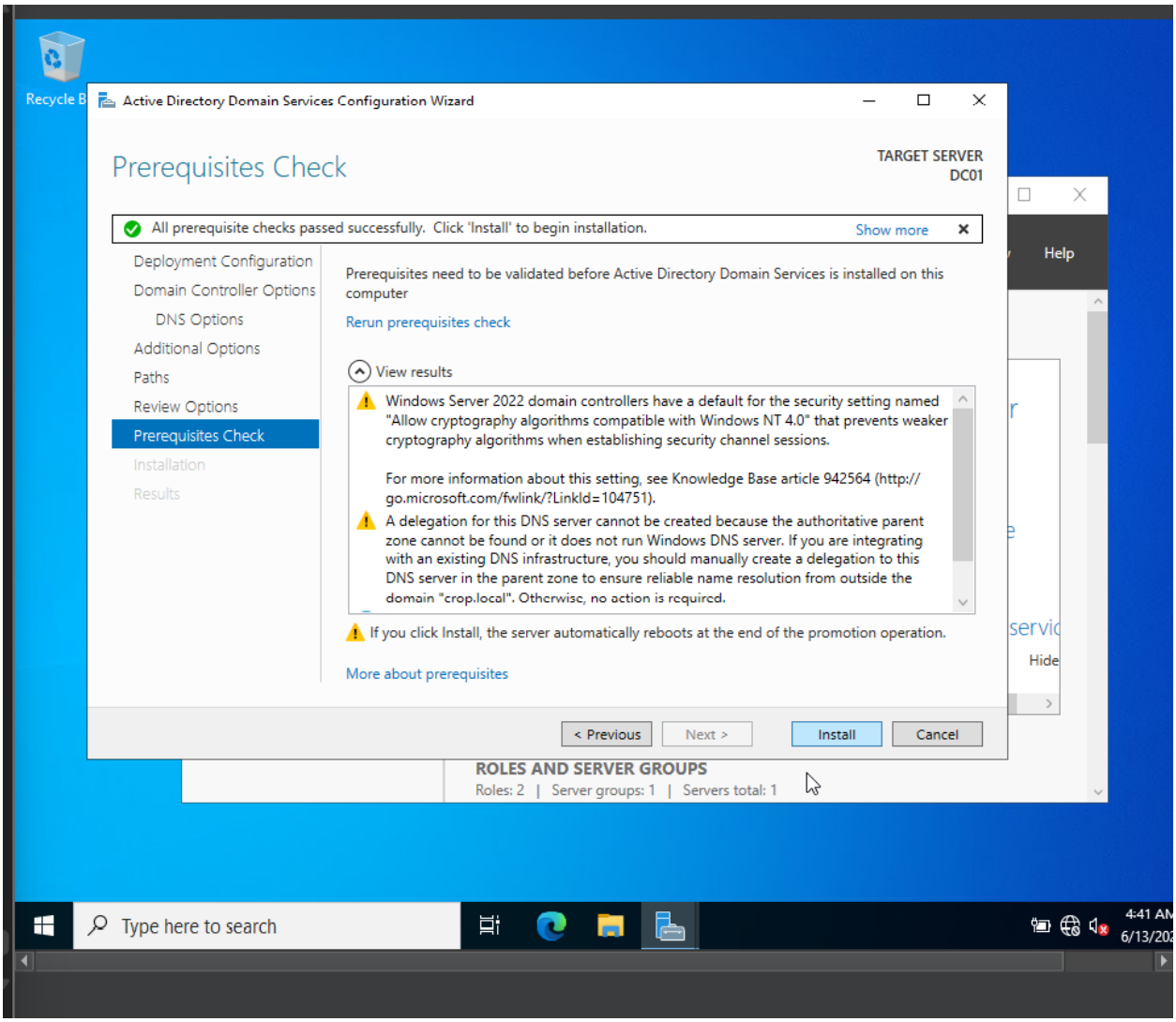
- The **Read-Only Domain Controller (RODC)** option was left disabled since this server is the primary writable domain controller.
- A **Directory Services Restore Mode (DSRM) password** was set and confirmed. This password is critical for performing recovery operations on Active Directory in case of system failure or maintenance.



- **Step 7: Prerequisites Validation and Final Installation**

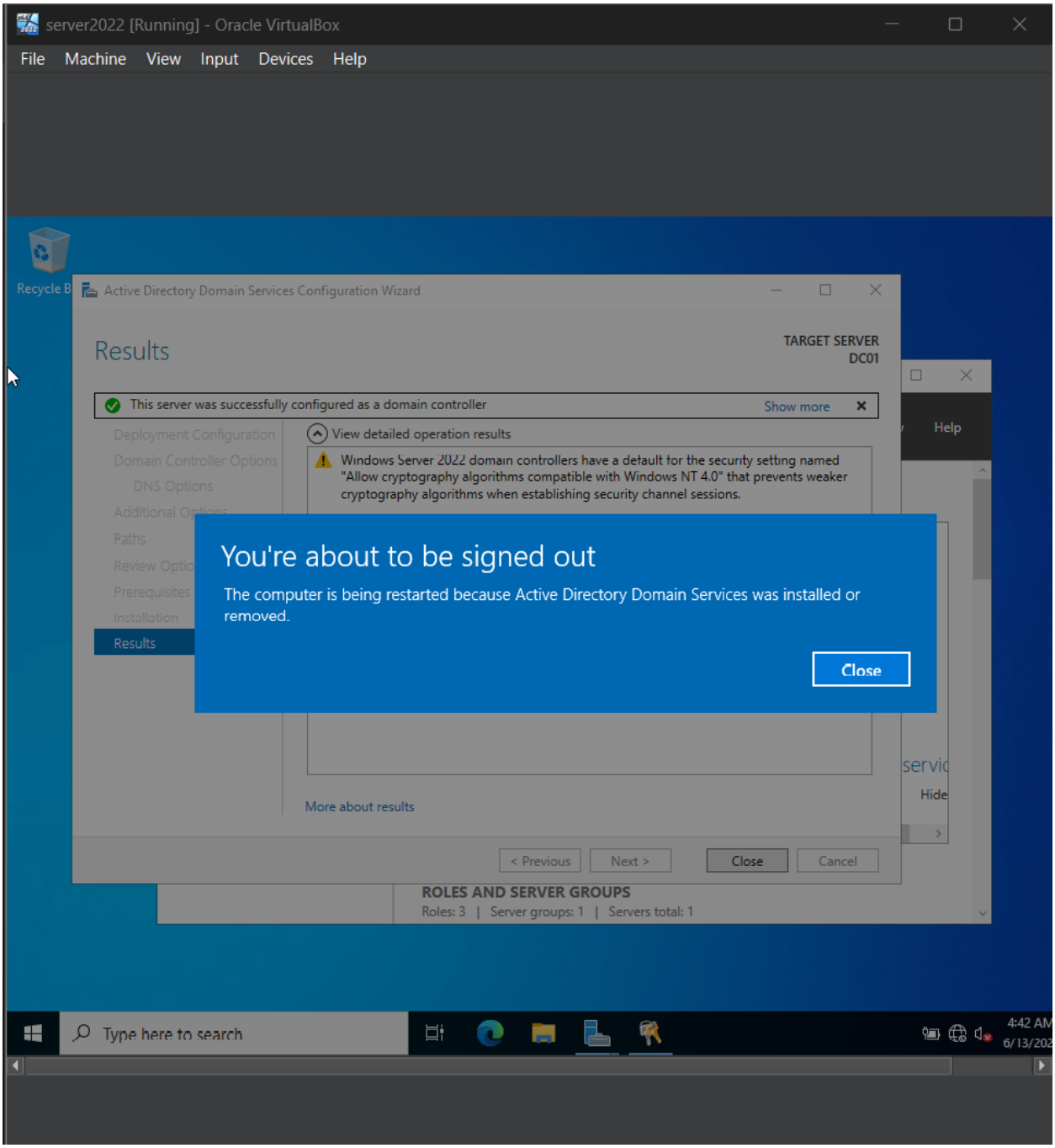
Before initiating the final installation and promotion, the wizard conducted a comprehensive **Prerequisites Check** to verify that all necessary conditions for a successful domain controller setup were met.

Rishav



Following the initiation of the Active Directory Domain Services installation, the server automatically restarted to complete the promotion process. This reboot finalizes the configuration changes, activates the domain controller role, and starts the associated services.

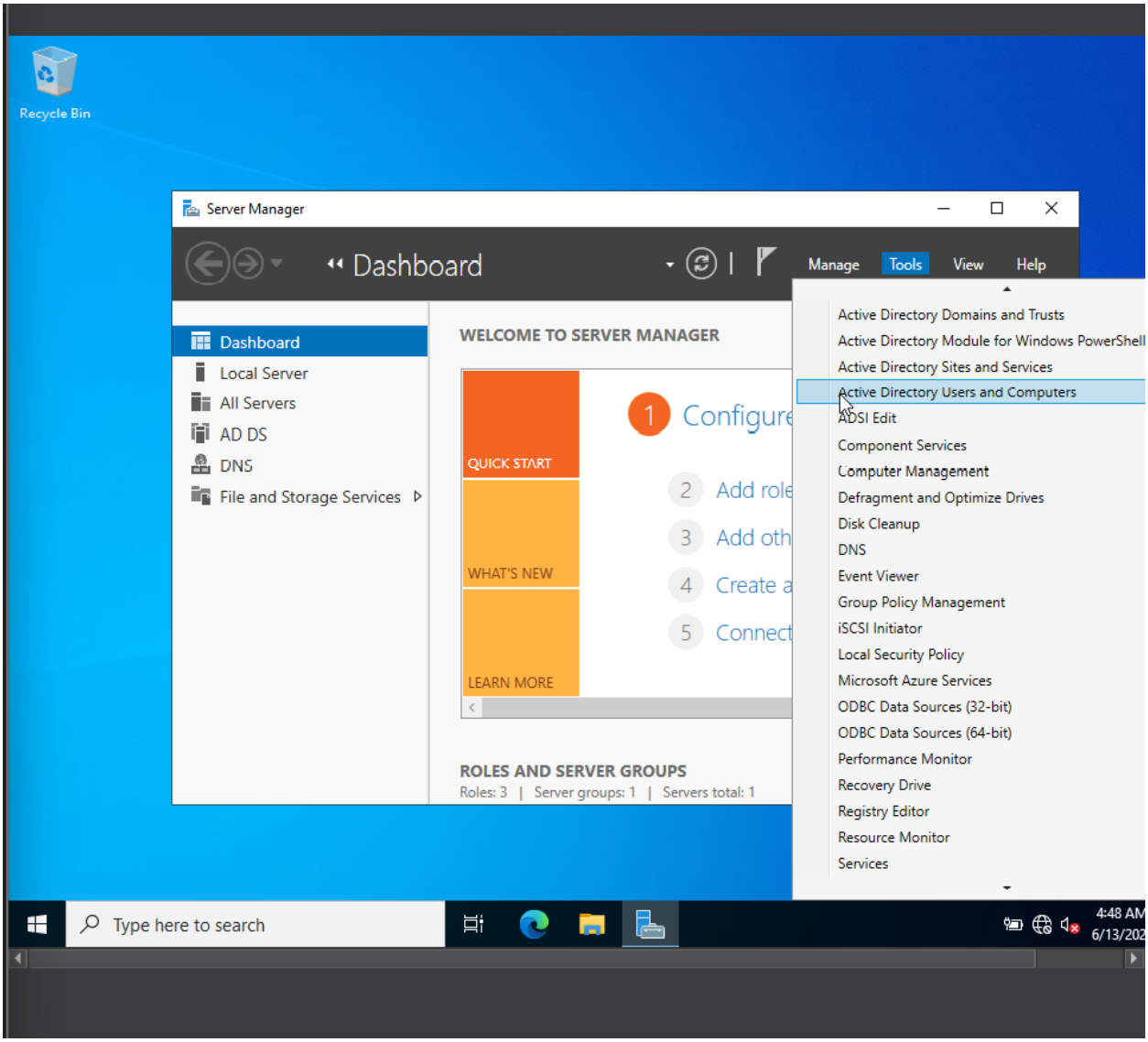
Rishav



- **Step 8: Accessing Active Directory Users and Computers**

To manage the domain environment, the **Active Directory Users and Computers** (ADUC) console was launched by the Server Manager. This tool provides a graphical interface to create, modify, and organize domain objects such as users, groups, and computers.

Rishav

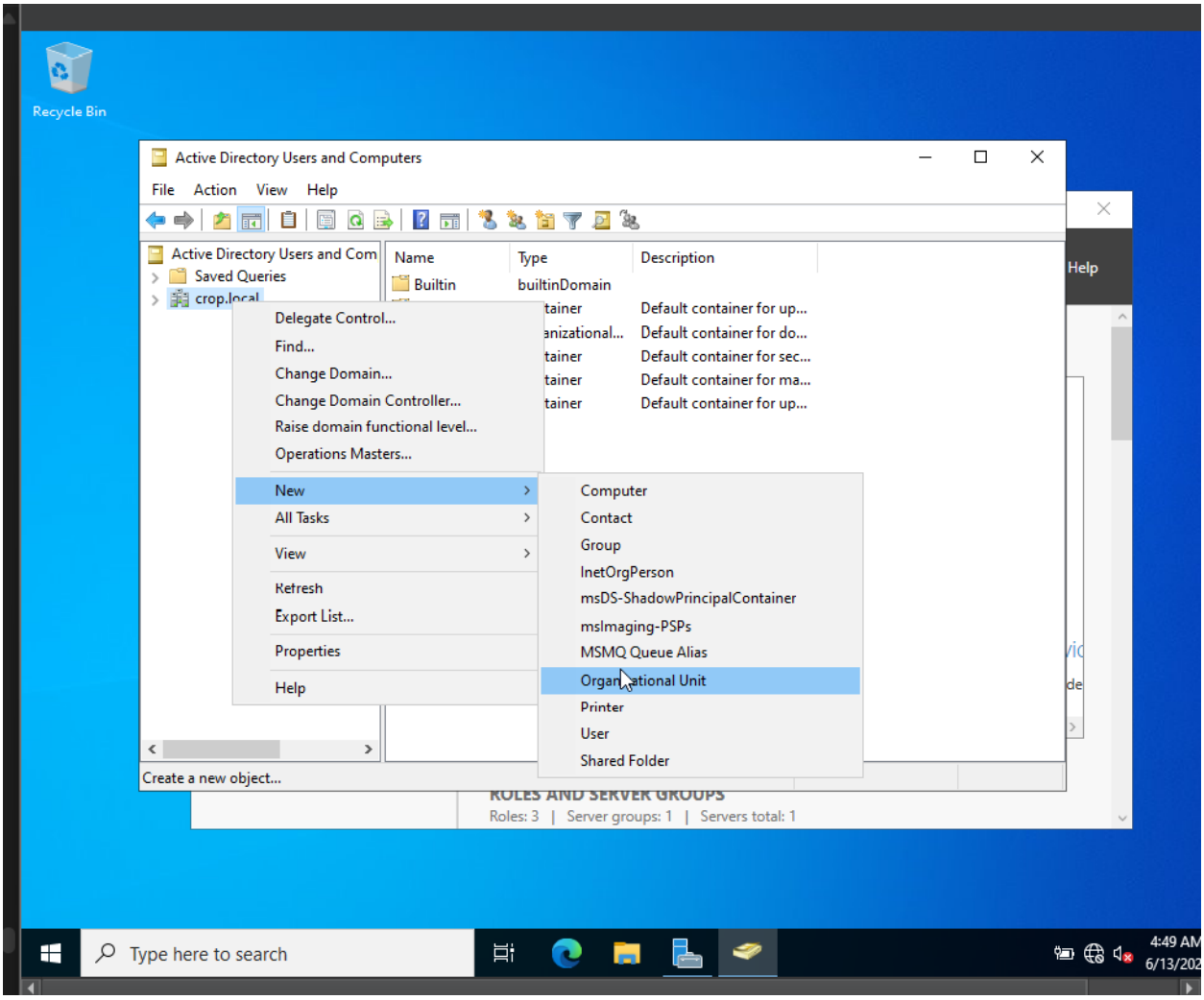


- **Step 9: Creating an Organizational Unit (OU)**

Within the **Active Directory Users and Computers** console, an **Organizational Unit (OU)** was created to logically organize and manage domain resources such as users, groups, and computers.

The OU provides a container to delegate administrative control and apply Group Policy settings selectively within the domain. This structure enhances management efficiency and security by grouping related objects based on department, role, or function.

Rishav



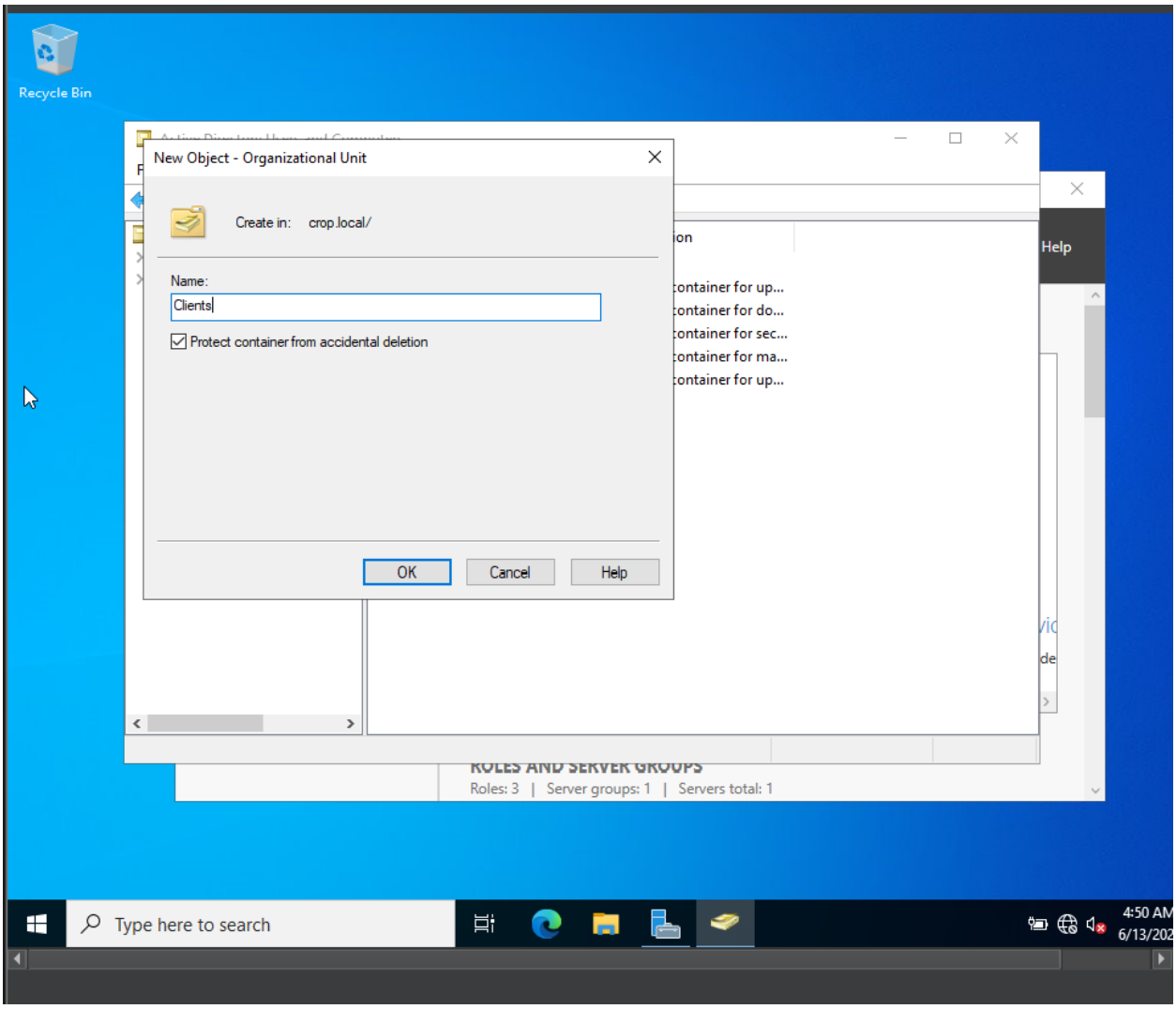
- **Step 10: Creating a New Organizational Unit Named "Client"**

Within the **Active Directory Users and Computers** console, a new Organizational Unit (OU) was created to organize and manage domain objects efficiently.

The **New Object – Organizational Unit** dialog was used to create an OU named **Client**. This OU serves as a dedicated container for client-related resources such as user accounts and computer objects, allowing centralized management and application of Group Policies specific to client devices.

The creation of the **Client** OU enhances administrative control and enables logical segregation within the **crop.local** domain structure.

Rishav

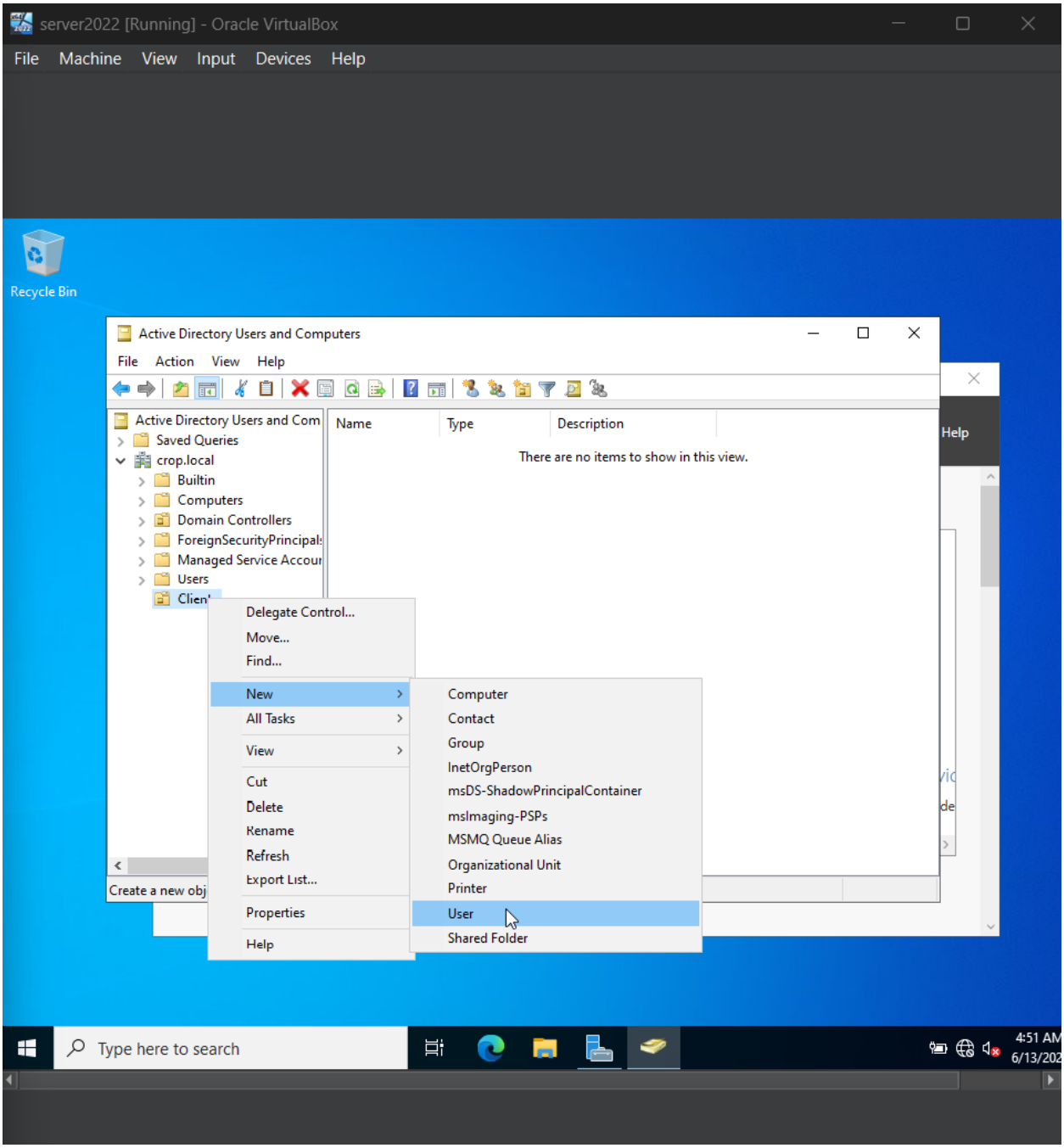


- **Step 11: Creating a New User in the Client Organizational Unit**

Within the **Client** Organizational Unit (OU) in **Active Directory Users and Computers**, a new user account was created by right-clicking the OU, selecting **New**, then **User**. This process involves specifying the user's details such as username, full name, and password.

Creating user accounts in the appropriate OU facilitates centralized management of users, enabling administrators to assign permissions, apply group policies, and control access within the **crop.local** domain.

Rishav



- **Step 12: Entering User Details for New Account Creation**

In the **New Object - User** dialog box within the **Client** Organizational Unit (OU) of **crop.local**, the following user details were entered to create a new user account:

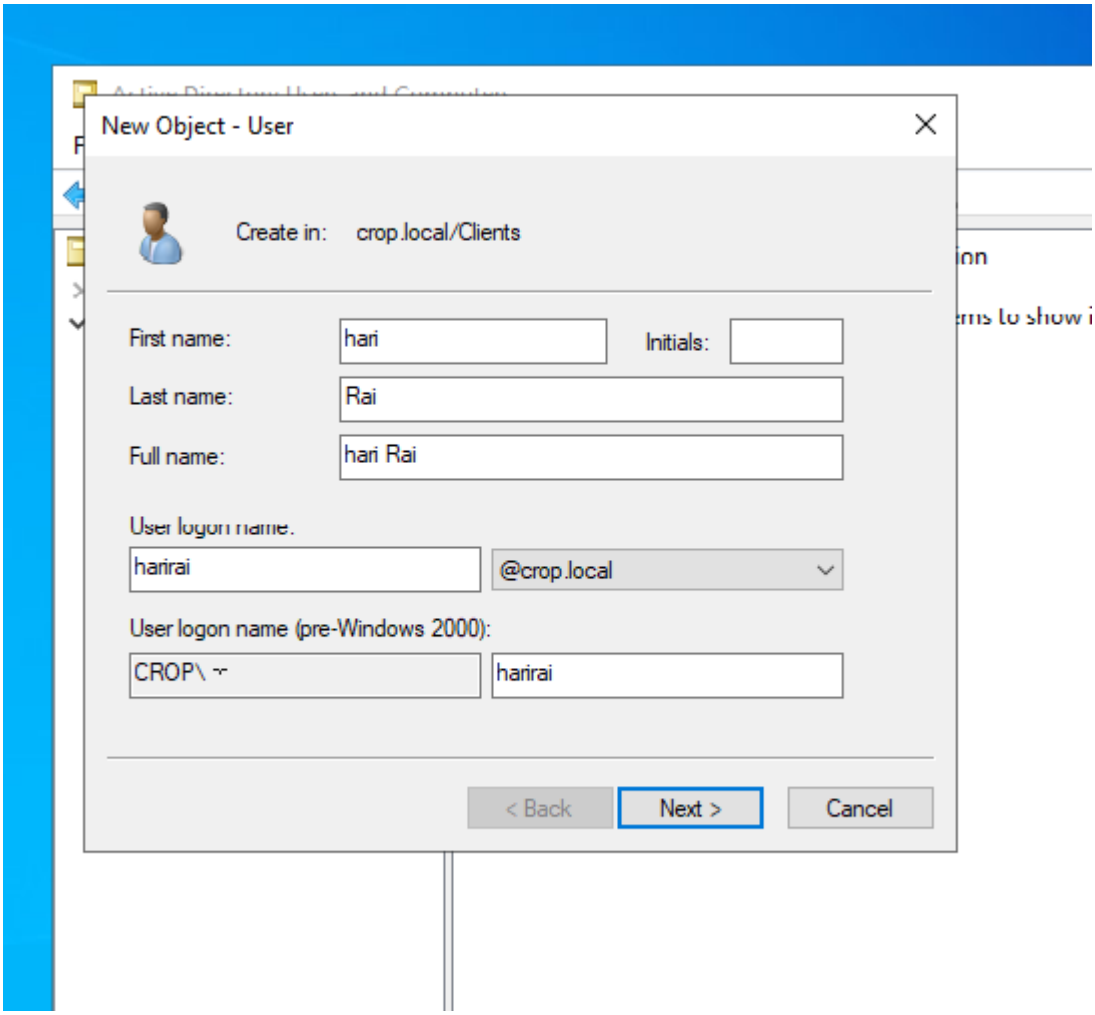
Example

- **First Name:** Hari

Rishav

- **Last Name:** Rai
- **Full Name:** Automatically populated as *Harirai Hari Rai*
- **User Logon Name (pre-Windows 2000):** [CROP\]

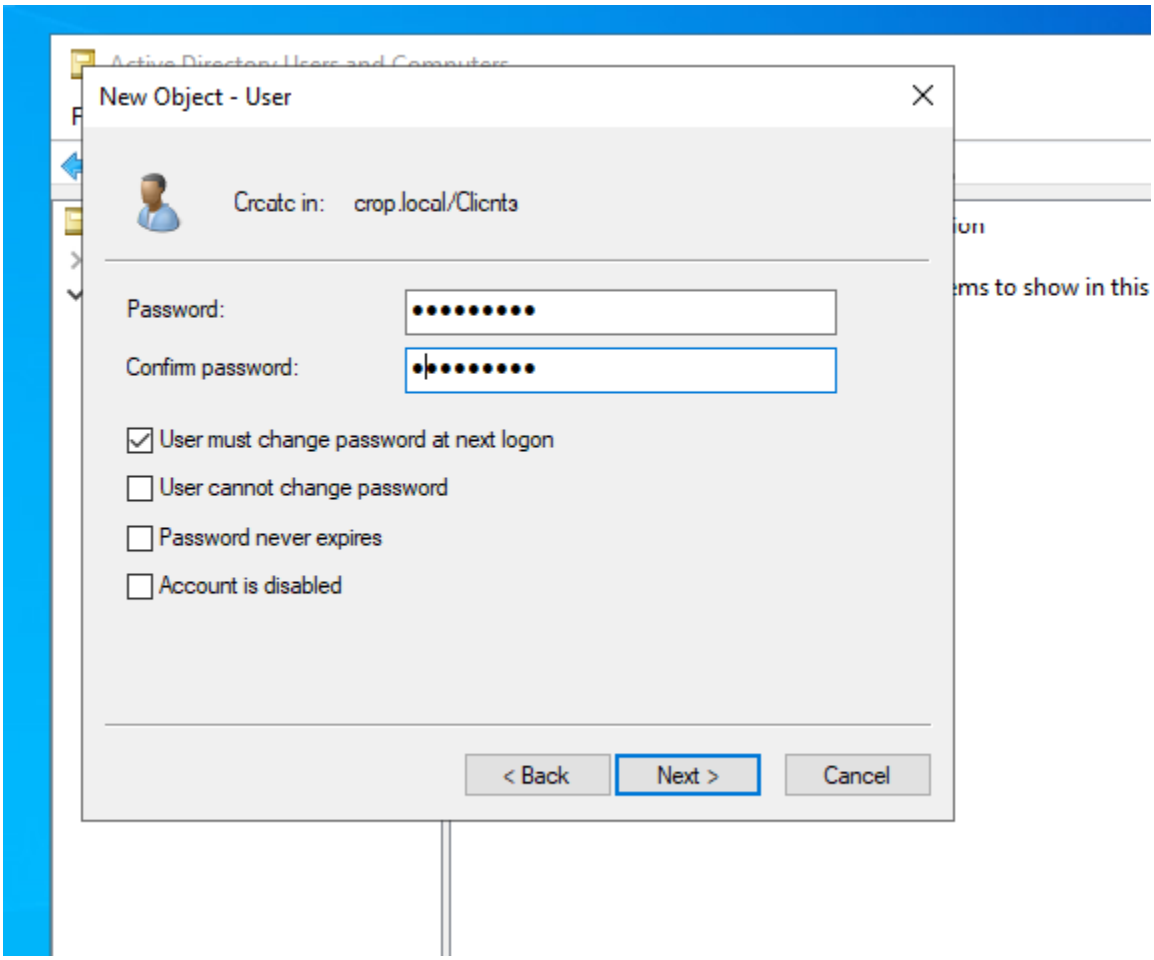
These details uniquely identify the user in the Active Directory and will be used for domain logon and authentication.



- **Step 13: Configuring Password and Account Options**

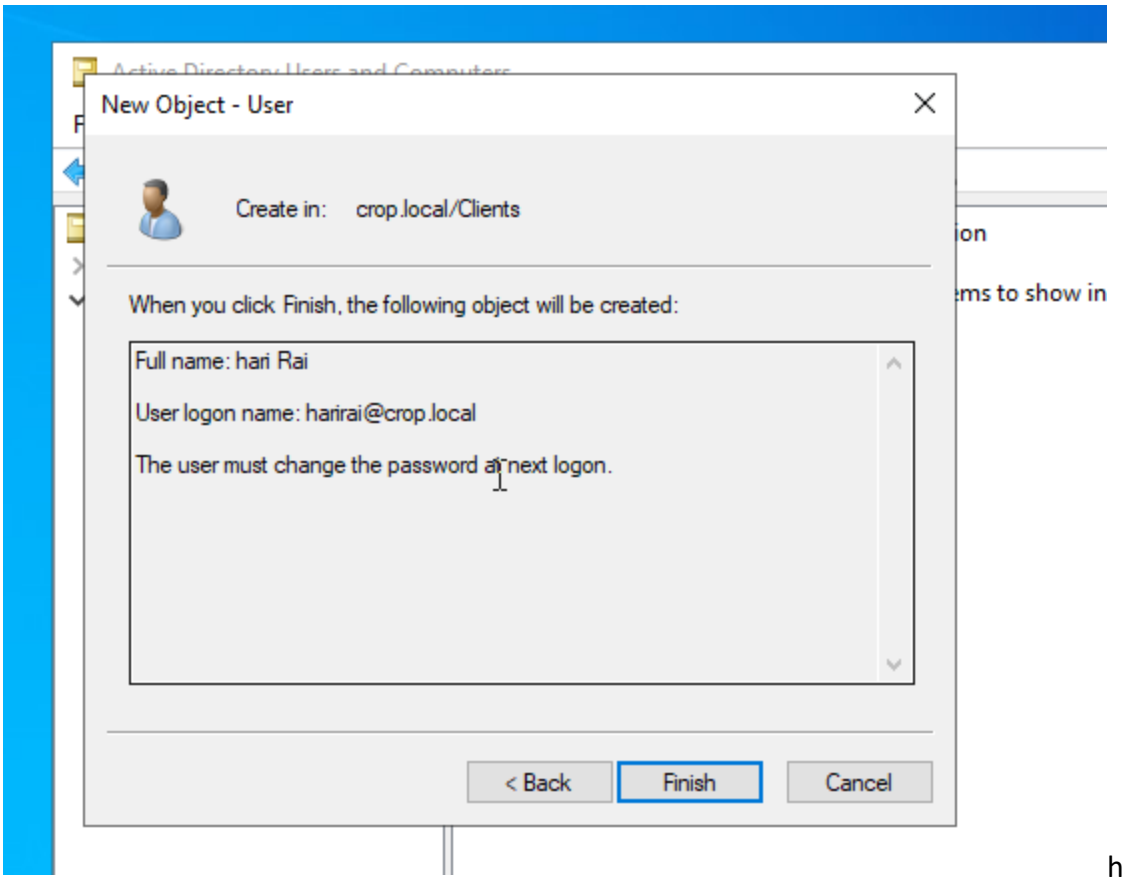
In the **New Object - User** dialog, the password for the new user account was set by entering and confirming a secure password.

Rishav



- **Step 14: Completing User Account Creation**

After entering all required information and configuring password policies, clicking **Finish** in the **New Object – User** wizard successfully created the user account



hari

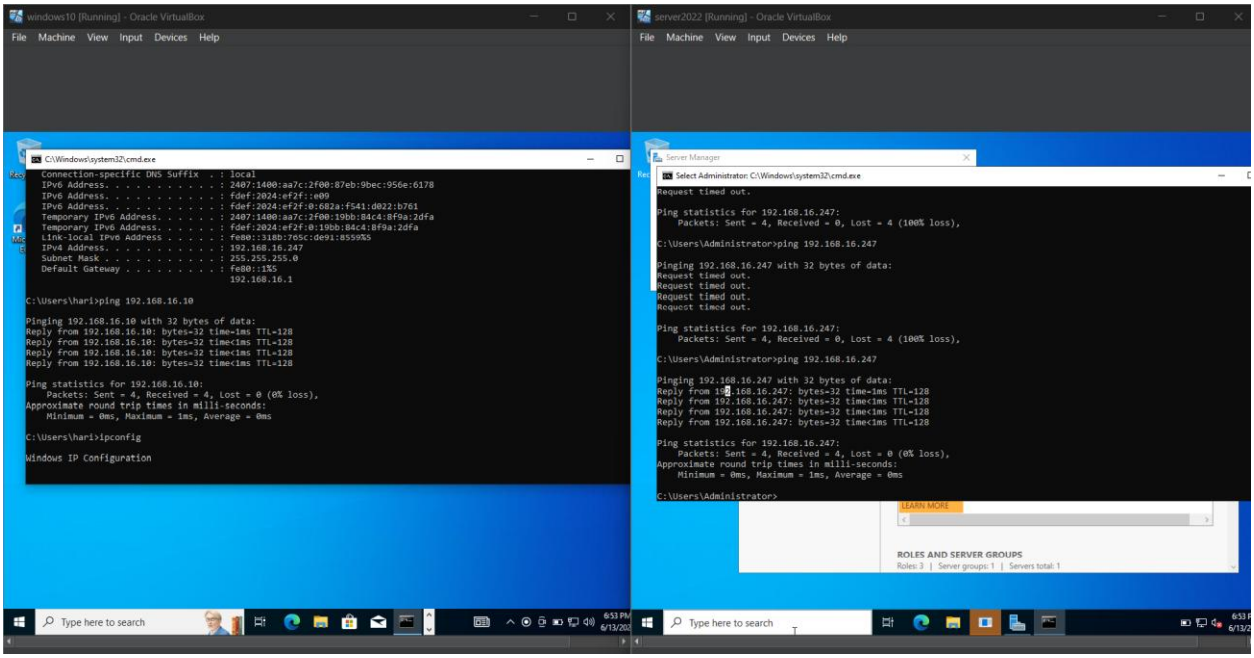
- **Step 15: Verifying Network Connectivity Between Windows 10 Client and Server 2022 Domain Controller**

To ensure proper communication within the domain environment, a network connectivity test was performed by pinging the Windows 10 client machine from the Server 2022 domain controller (DC01).

This step confirms that both machines are reachable over the network, which is essential for domain join operations, authentication, and Active Directory services.

Successful ping responses indicate that the client and server are correctly configured on the same network segment, with proper IP addressing and routing.

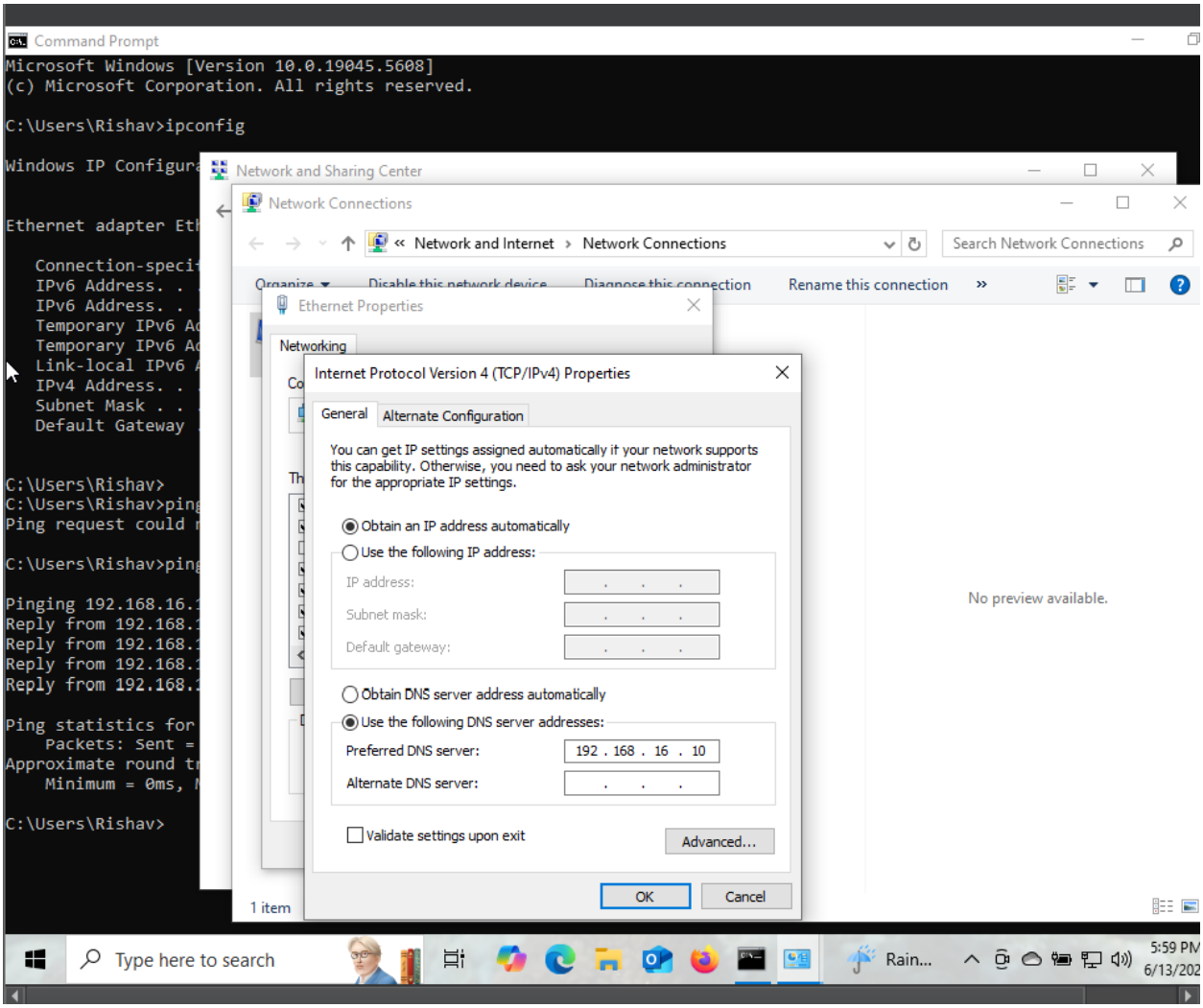
Rishav



- **Step 16: Configuring Windows 10 Client to Use Server 2022 as Preferred DNS Server**

To ensure proper name resolution within the Active Directory domain, the Windows 10 client was configured to use the Server 2022 domain controller's IP address as its **Preferred DNS Server**.

Rishav



- **Step 17: Changing Windows 10 Client Computer Name and Joining the Domain**

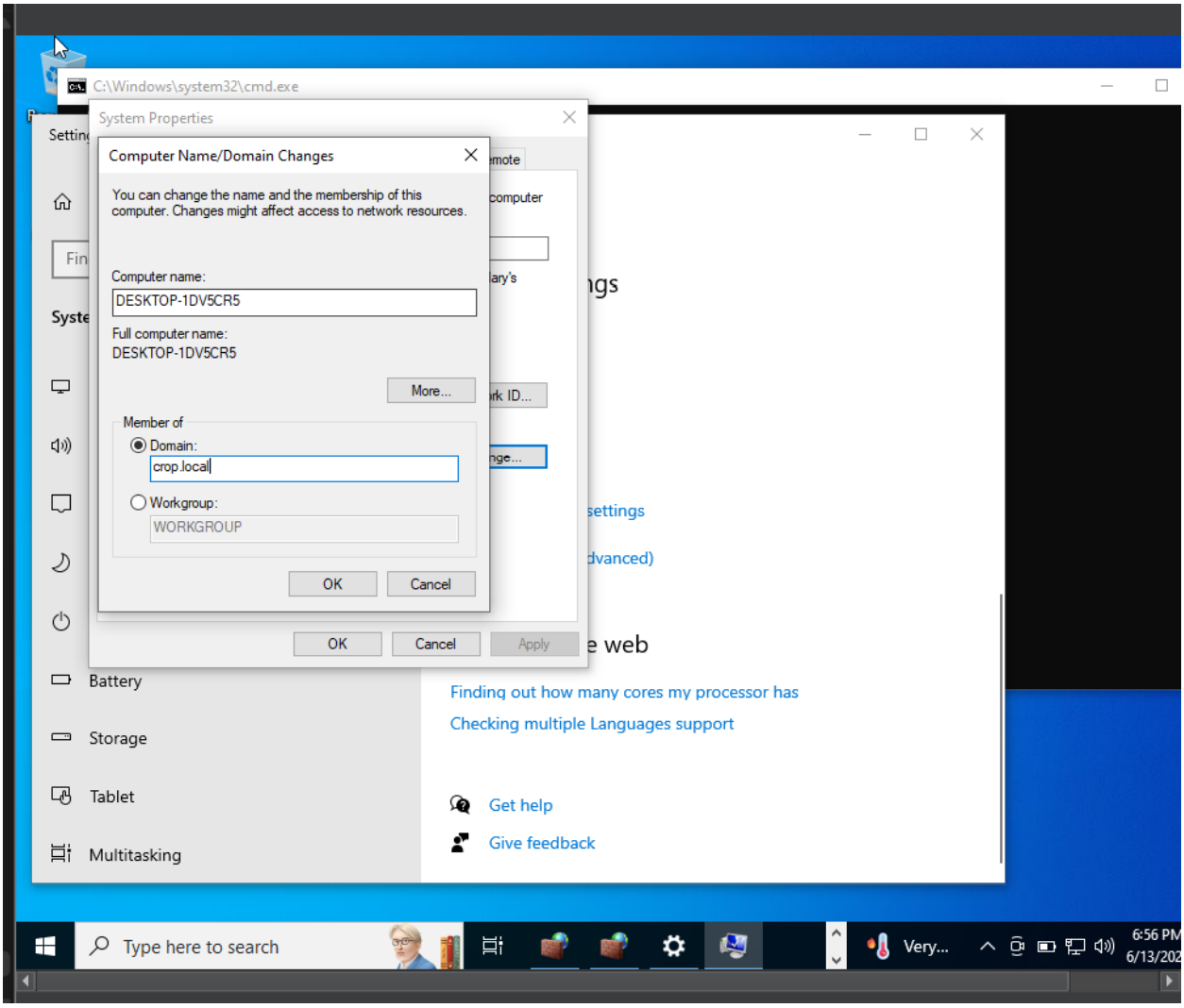
From the Windows 10 client, the system properties were accessed through **This PC → Properties → Advanced system settings → Computer Name**.

In the **Computer Name/Domain Changes** window, the following actions were performed:

- The client computer name was modified to a meaningful hostname (e.g., DESKTOP-IDVSCRS).
- The computer was switched from the default **WORKGROUP** to join the **crop.local** domain.

This change enables the Windows 10 machine to be recognized as a member of the Active Directory domain, allowing centralized management, domain-based authentication, and access to domain resources.

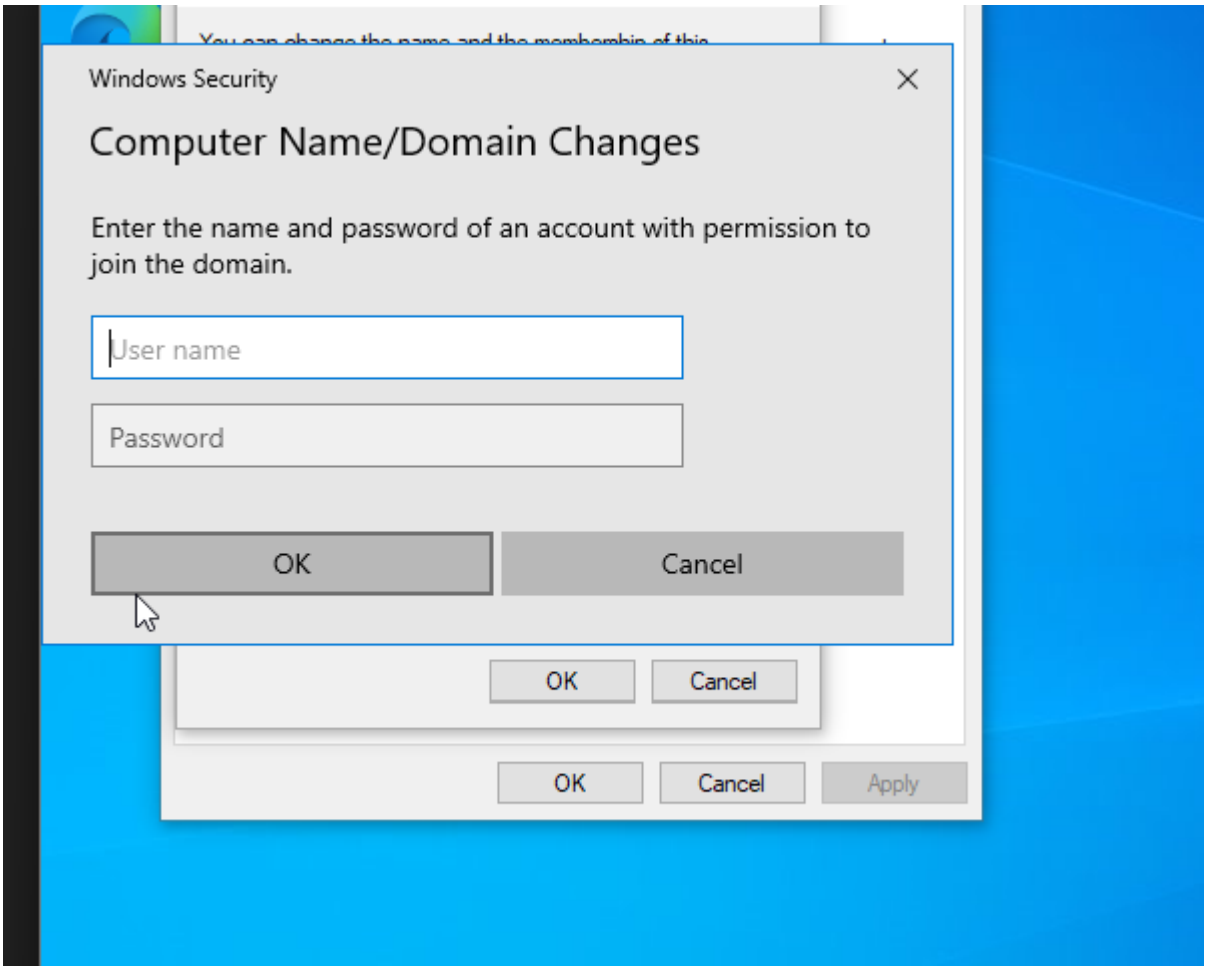
Rishav



- **Step 18: Providing Domain Credentials to Join Windows 10 Client to Domain**

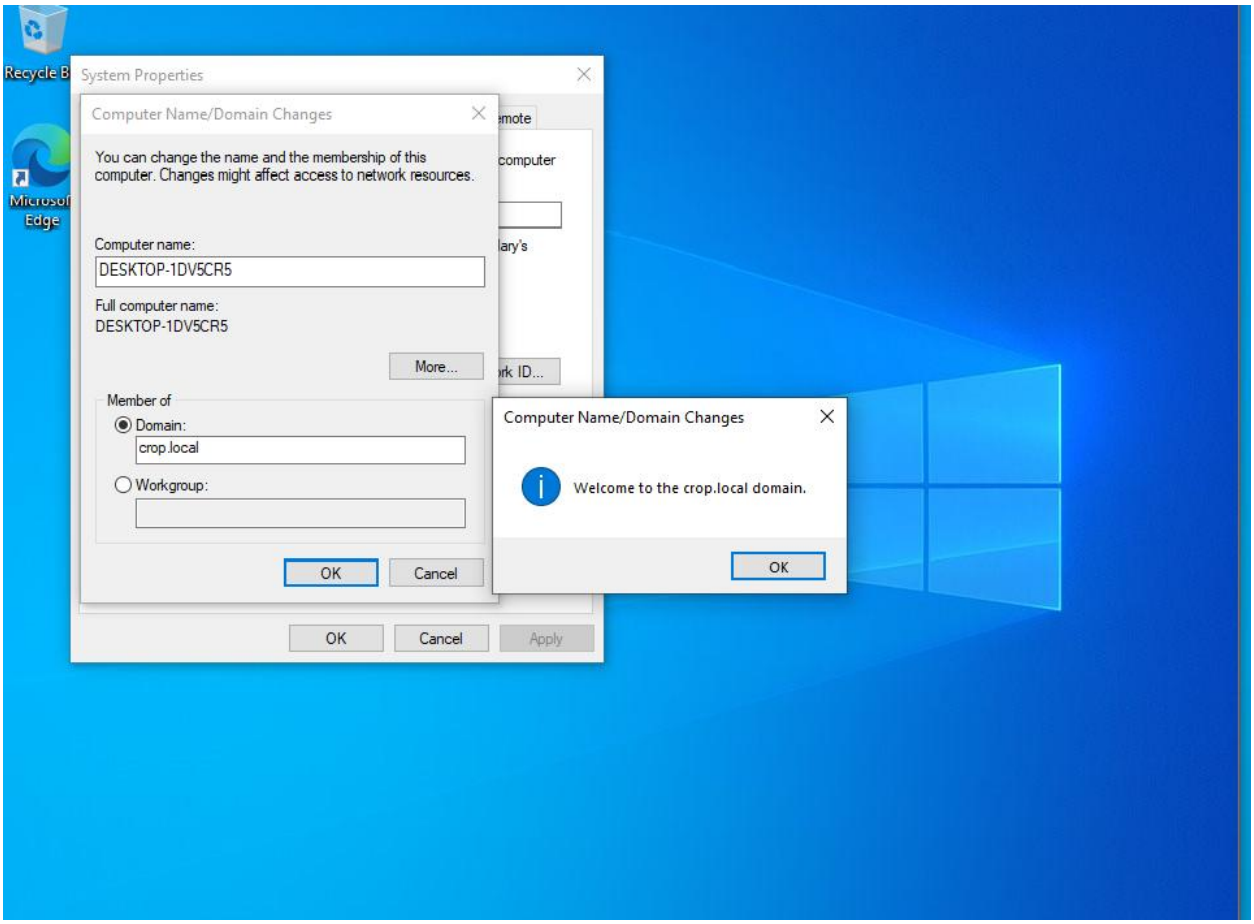
When attempting to join the Windows 10 client to the **crop.local** domain, the system prompts for credentials with sufficient privileges to add a computer to the domain.

Rishav



- **Step 19: Successful Domain Join Confirmation**

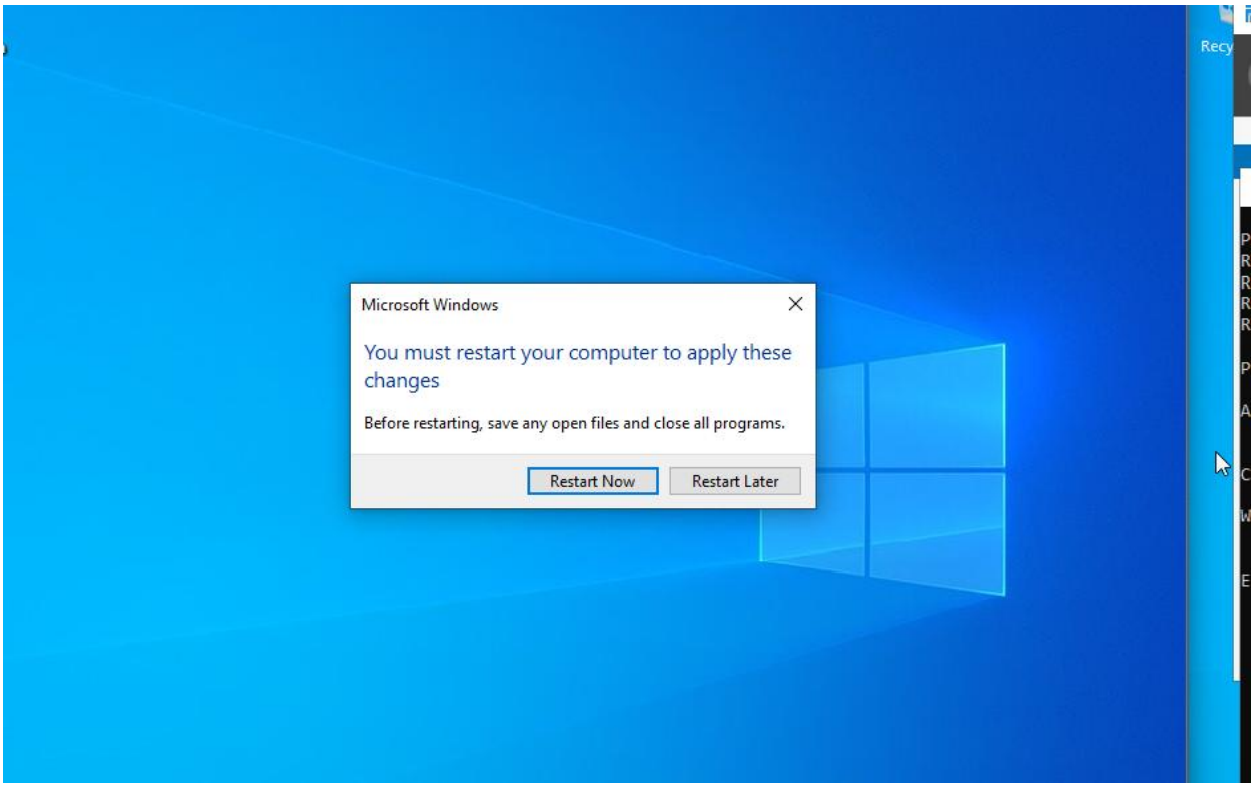
After providing valid credentials, the Windows 10 client successfully joined the **crop.local** domain.



- **Step 20: Restarting Windows 10 Client to Apply Domain Join Changes**

After successfully joining the **crop.local** domain, a prompt appears requesting a system restart to apply the changes.

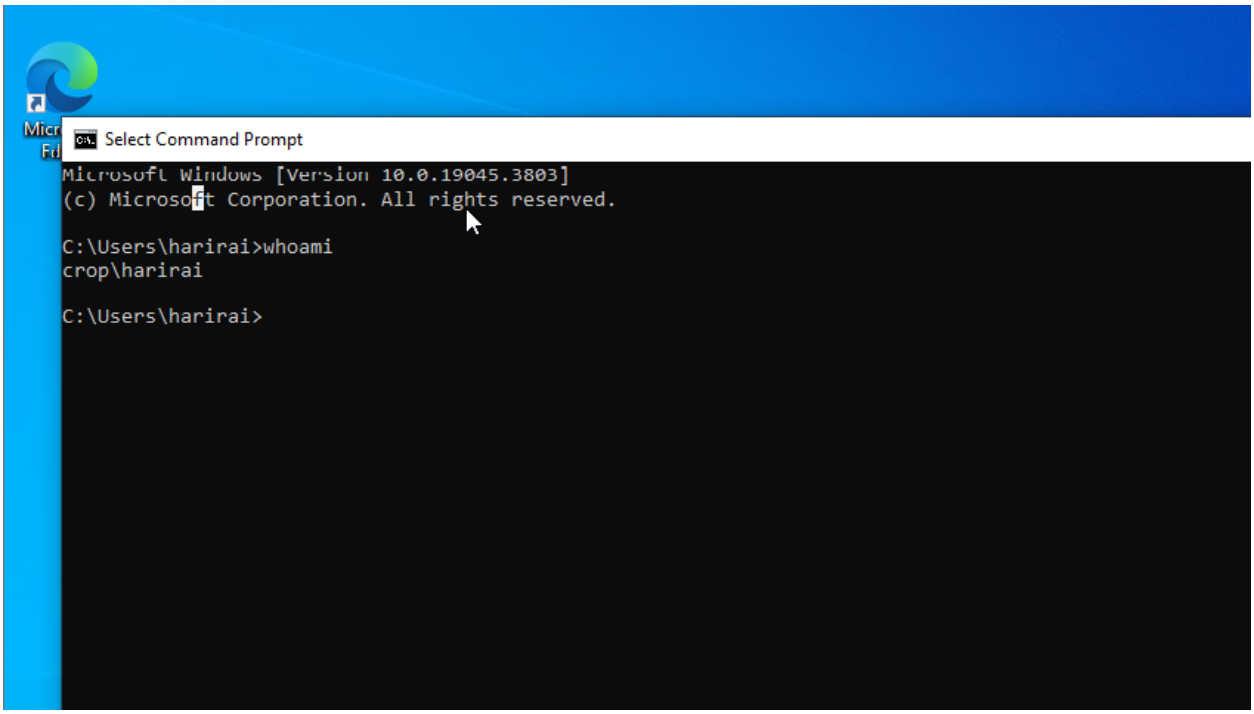
Rishav



- **Step 21: Verifying Domain User Login on Windows 10 Client**

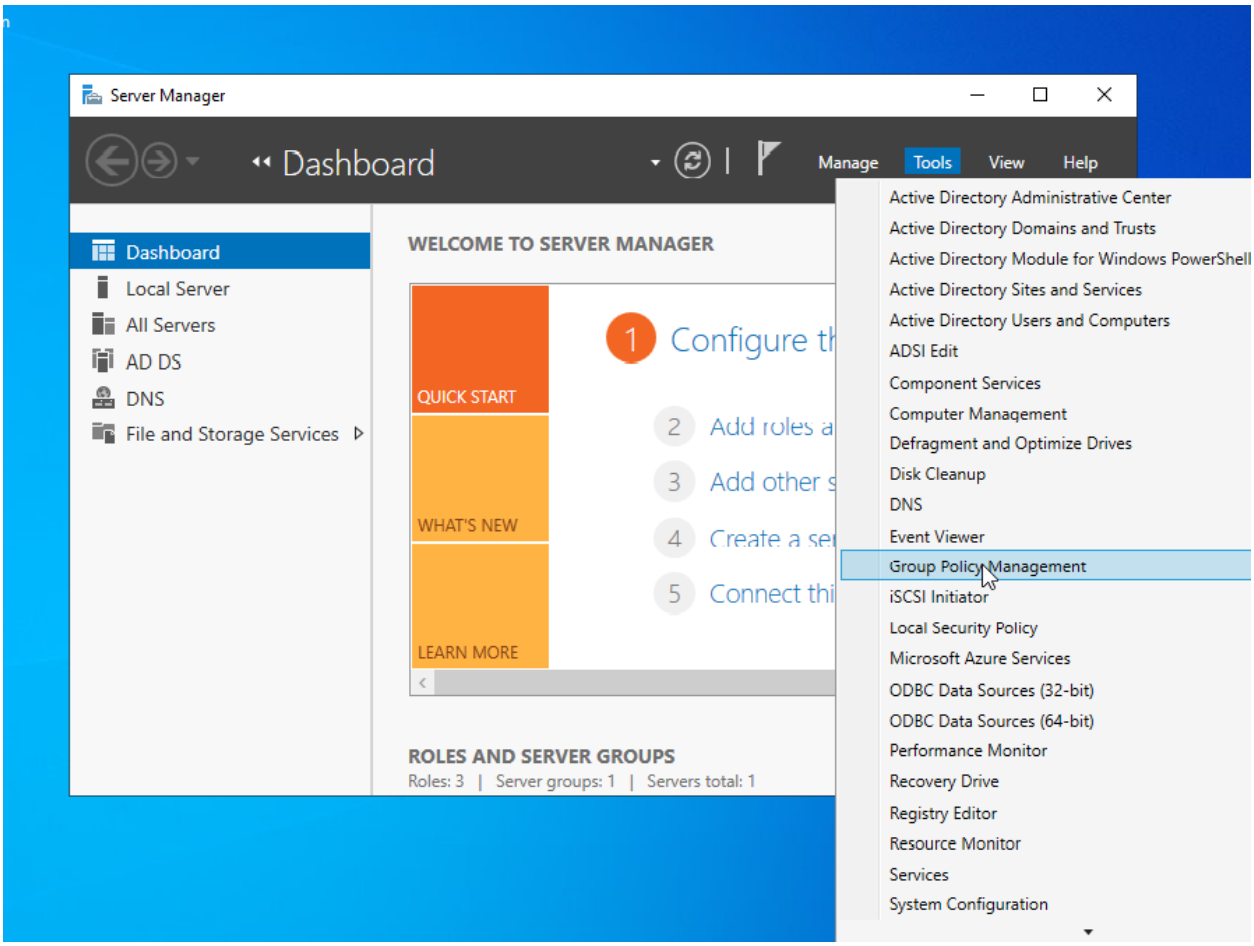
After restarting, the Windows 10 client was logged in using the domain user account **harirai**.

To confirm the login context, the command prompt was opened, and the command whoami was executed.



- **Step 22: Setting Up Group Policy Management on Server 2022**

To centrally manage and enforce security and configuration settings across all domain-joined computers and users, the **Group Policy Management Console (GPMC)** was accessed on the Server 2022 domain controller.

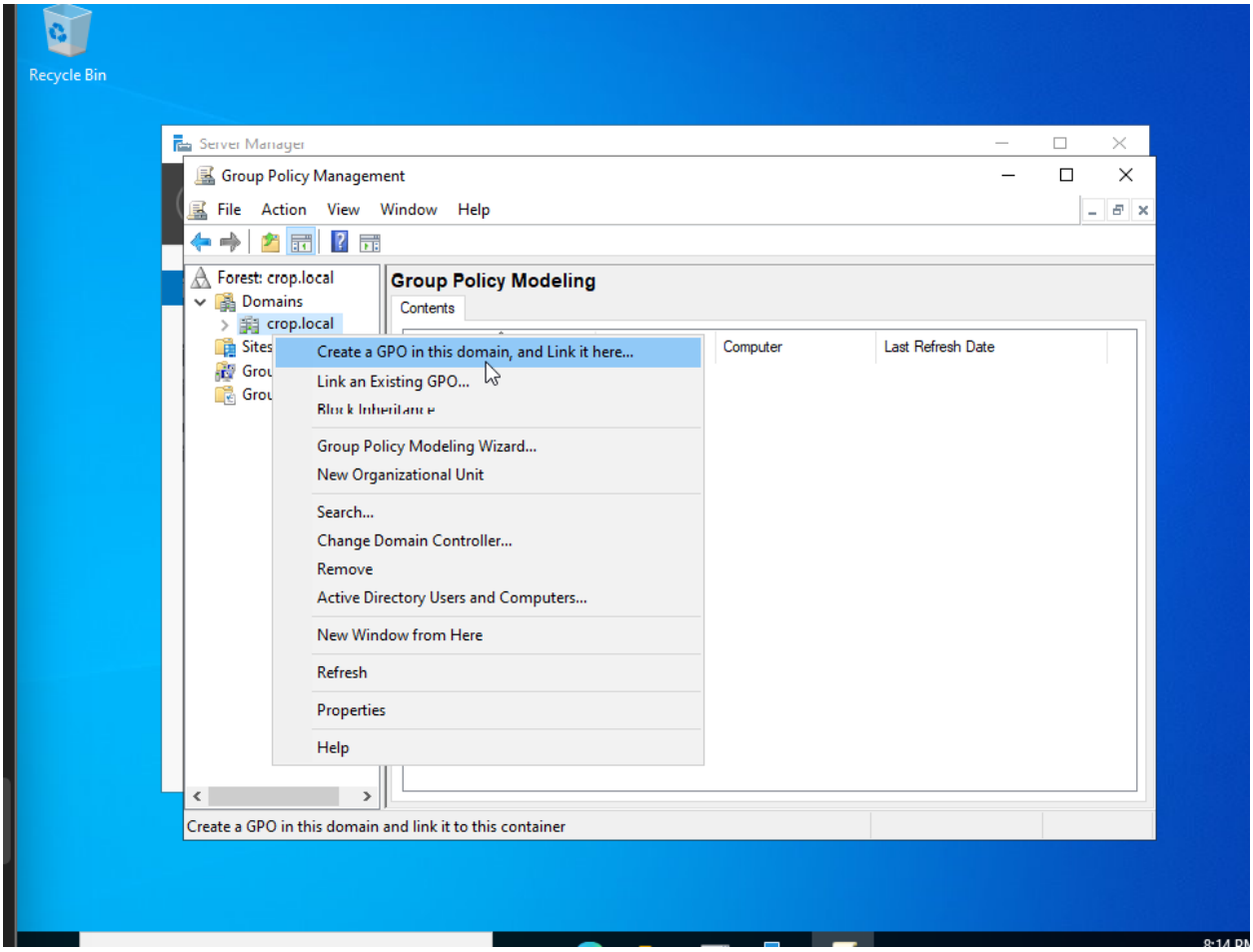


- **Step 23: Creating and Linking a New Group Policy Object (GPO)**

Within the Group Policy Management Console (GPMC) on the Server 2022 domain controller, the **crop.local** domain was selected.

To implement specific configurations or policies, a new Group Policy Object (GPO) was created and linked directly to the domain or a specific Organizational Unit (OU).

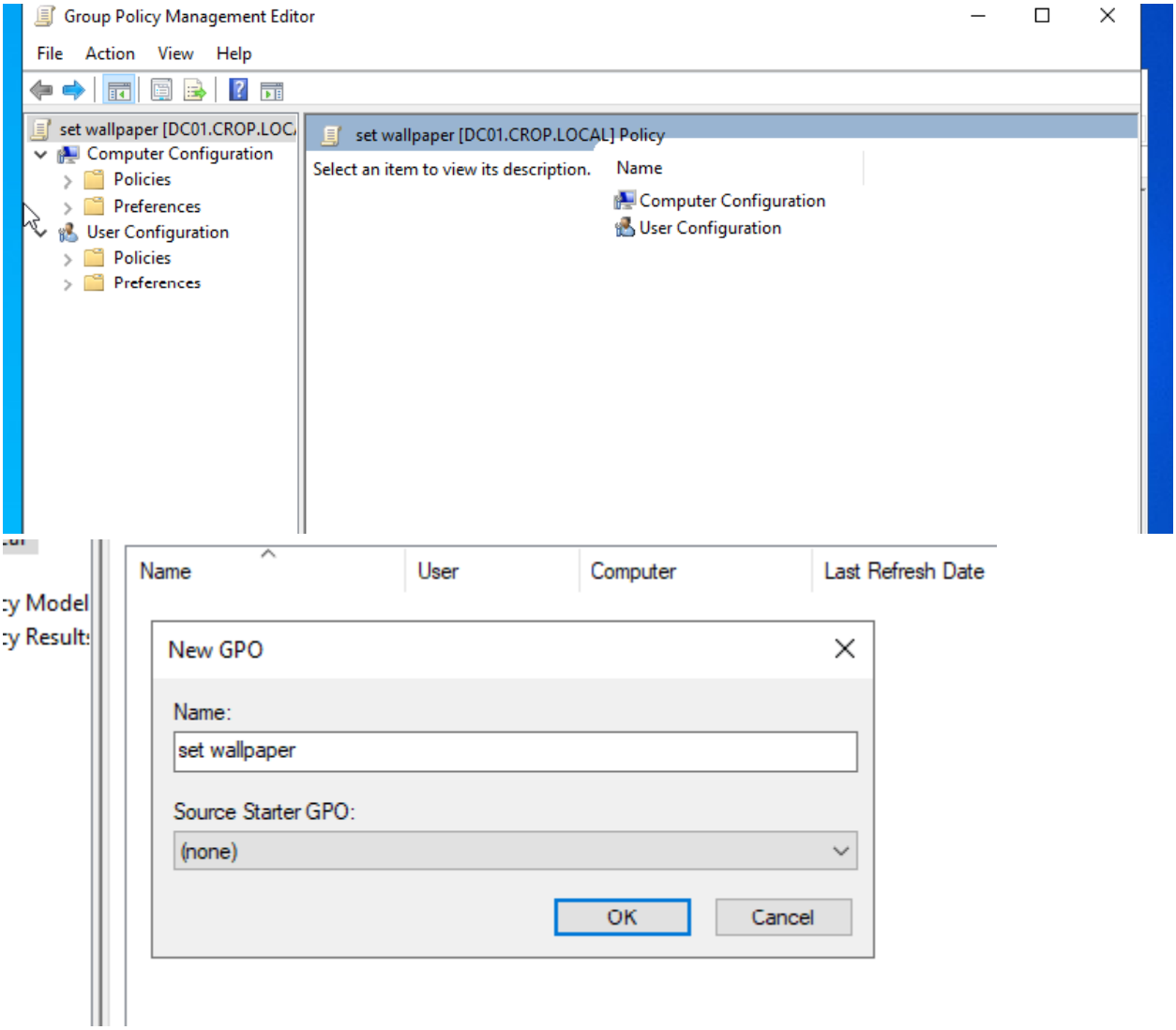
Rishav



- **Step 24: Configuring Group Policy to Enforce Windows 10 Wallpaper**

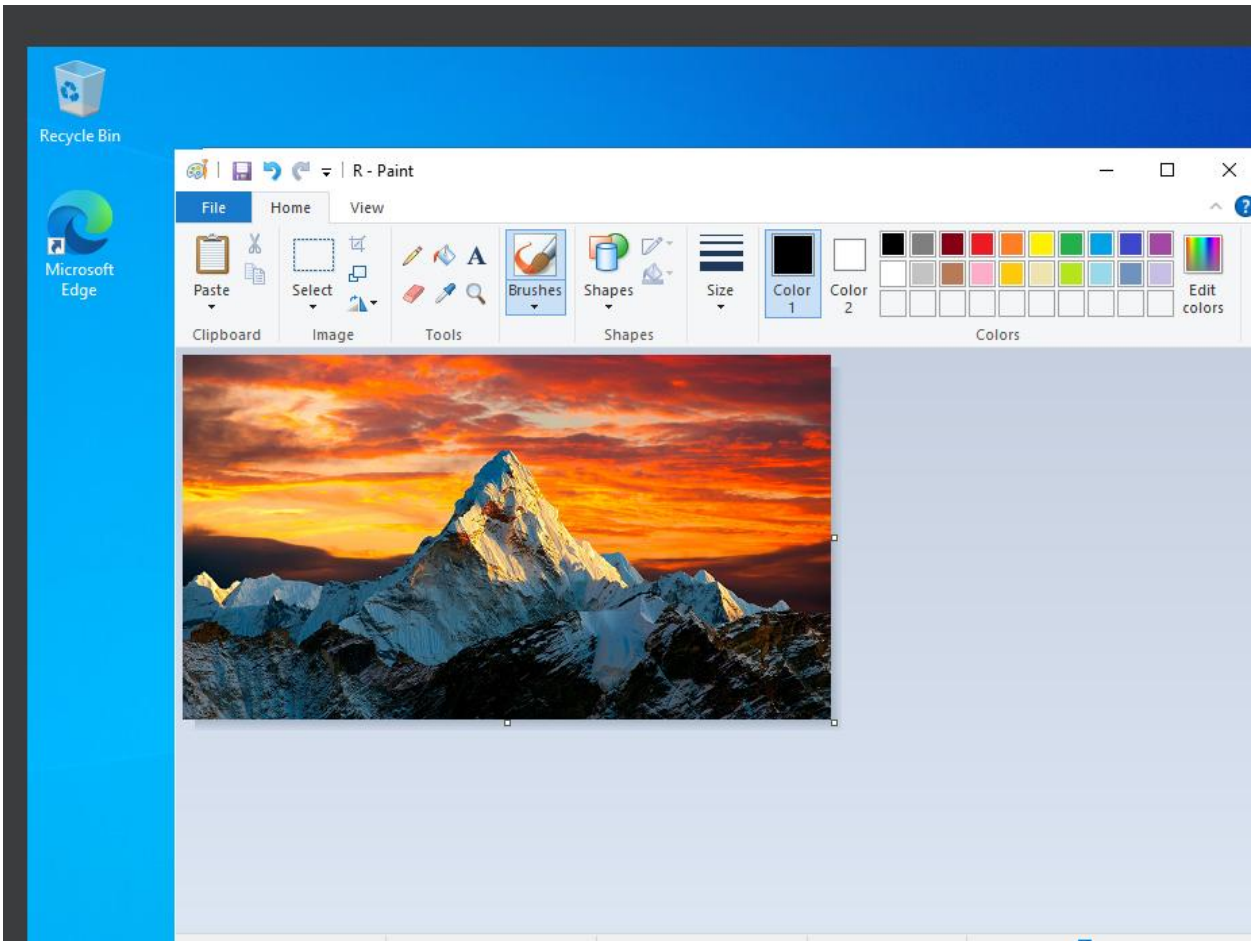
A Group Policy was created to centrally enforce the desktop wallpaper settings on all Windows 10 client machines within the domain.

This policy ensures that the wallpaper image is deployed from a centralized server location, providing a consistent corporate branding or security message across all user desktops.



The wallpaper used for the Windows 10 clients is a designated image file (e.g., **wallpaper.jpg**) stored on a centralized file share on the server.

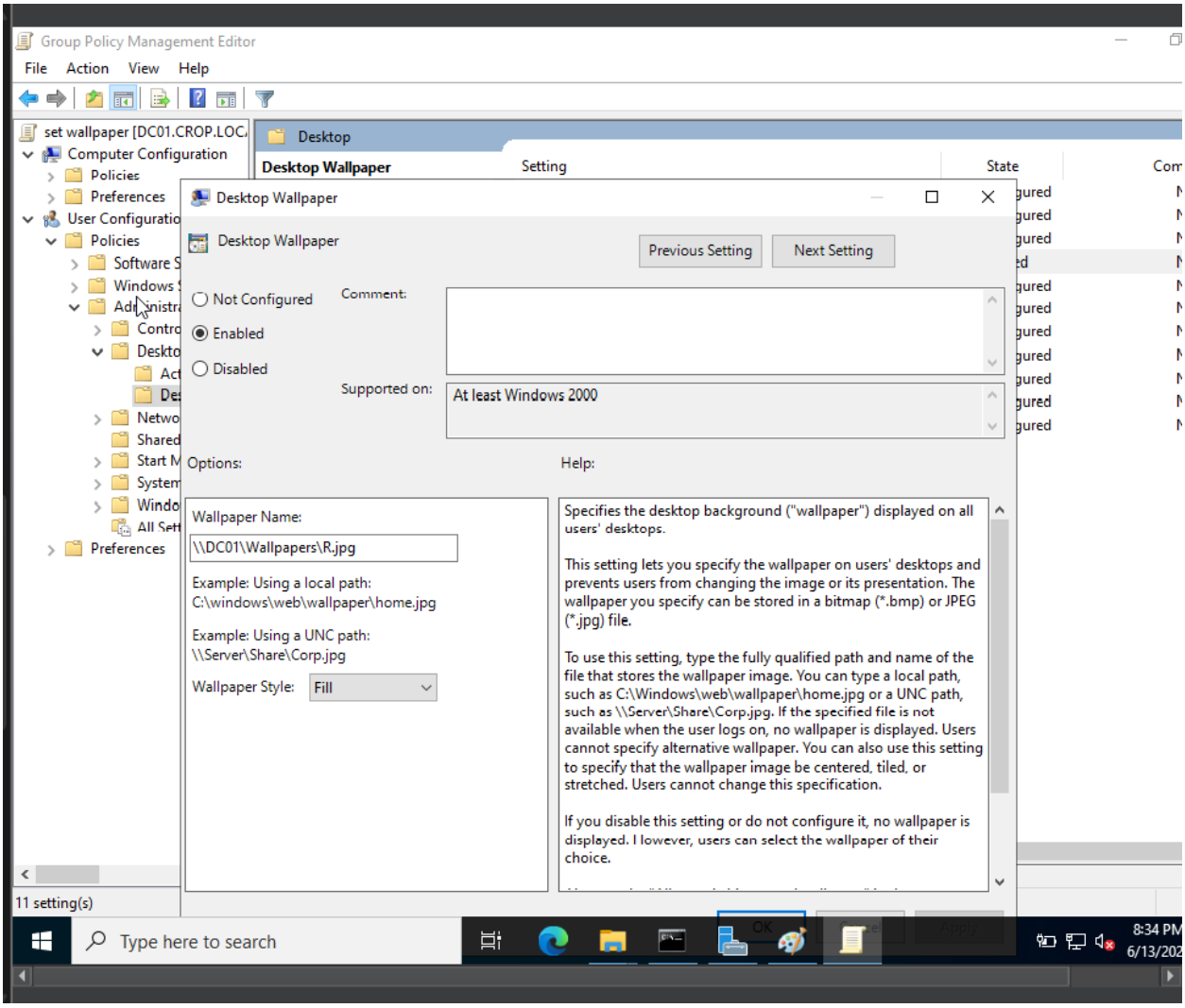
Rishav



- **Step 25: Configuring Desktop Wallpaper Policy**

The **Desktop Wallpaper** Group Policy setting is configured to enforce a specific wallpaper image on all domain-joined Windows 10 clients.

This policy requires specifying the full path to the wallpaper image file, which can be stored locally on the machine or accessed via a network UNC path (e.g., \\server\share\wallpaper.jpg).

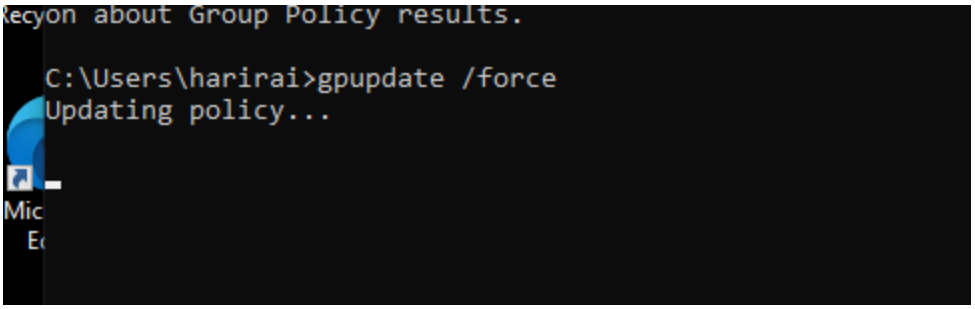


Step 26: Configuring Group Policy to Enforce Windows 10 Wallpaper

A Group Policy was created to centrally enforce the desktop wallpaper settings on all Windows 10 client machines within the domain.

This policy ensures that the wallpaper image is deployed from a centralized server location, providing consistent corporate branding or security message across all user desktops.

Rishav



Step 26: Applying Group Policy on Windows 10 Client

To ensure the newly configured Group Policy (GPO) for enforcing the desktop wallpaper is applied on the Windows 10 machine, the following command was executed:

- gpupdate /force

As a result of the Group Policy update, the wallpaper on the Windows 10 desktop is now automatically set according to the configuration defined in the server-based policy. This confirms that the domain-linked GPO is successfully pushing settings to client systems across the network. Moreover, users are restricted from changing the wallpaper manually, ensuring a consistent and centrally managed desktop environment in alignment with organizational standards.

This successful deployment of policy-based wallpaper not only demonstrates domain controller functionality but also reflects real-world enterprise-level centralized IT management practices.

6. Testing & Validation

Task	Result
IP assigned via DHCP	✅
Domain join successful	✅
DNS resolves DC	✅
Domain login with harirai	✅
Group Policy wallpaper applied	⚠️ *(Activation required)*
ping between client & server	✅

7. Challenges Faced

- **Group Policy for Wallpaper Not Applied:**
  The GPO to enforce a desktop wallpaper did not apply on the Windows 10 client. Upon investigation, it was found that the system was not activated.
  Reason: Non-activated versions of Windows 10 restrict personalization features, including the ability to apply wallpaper through Group Policy.
- DNS misconfiguration initially (resolved)
- Needed admin privileges for domain join

8. Future Scope

- Add more OUs for departments
- Configure logon scripts
- Add backup domain controller
- Set account lockout & password policies
- Implement printer/file server roles

9. Conclusion

This project successfully implemented a complete Active Directory environment within a virtual lab. It mimics real-world enterprise network operations like user management, policy enforcement, and domain services. The experience builds a strong foundation in Windows Server administration and network infrastructure.

10. Appendix

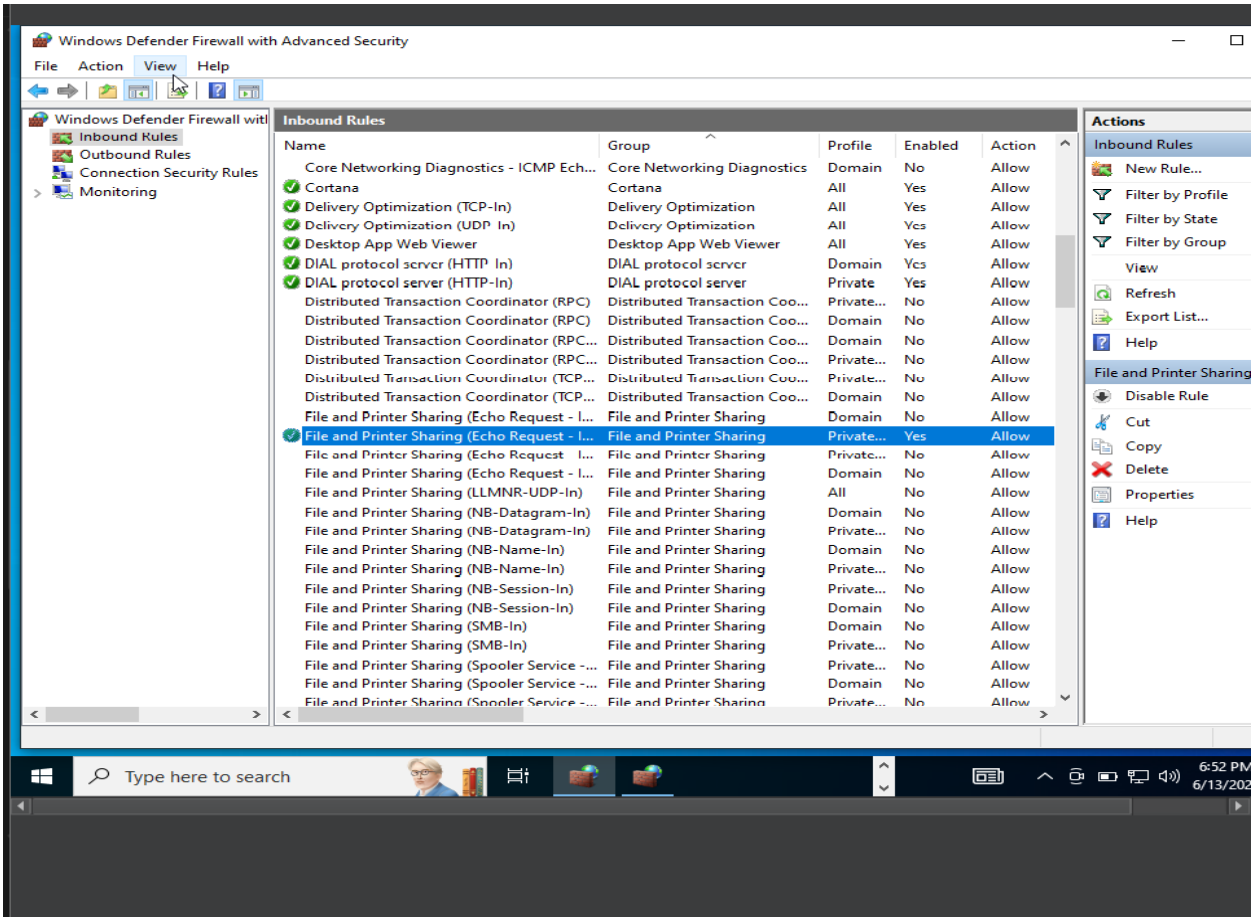
Problem Faced:

During the post-configuration testing phase of the domain environment, an issue was encountered when attempting to **ping the Windows 10 client from the Server 2022 machine** (DC01). While **pinging from the Windows 10 client to the server was successful**, the reverse from **Server 2022 to Windows 10 failed**. This raised concerns about network communication and firewall configurations.

Root Cause:

After investigation, it was determined that **Windows Defender Firewall on the Windows 10 client** was **blocking inbound ICMP (ping) requests**. By default, modern versions of Windows have ICMP (Echo Request) rules disabled in the firewall for security reasons.

Solution:



To resolve the issue, the following firewall rule was manually enabled on the Windows 10 client:

- **Rule Name:** File and Printer Sharing (Echo Request - ICMPv4-In)
- **Group:** File and Printer Sharing
- **Profile:** Private
- **Action:** Allow
- **Status:** Enabled

Steps Taken:

1. Windows **Defender Firewall with Advanced Security** on the Windows 10 machine.
2. Navigated to **Inbound Rules**.
3. Located and **enabled** the rule:
   File and Printer Sharing (Echo Request - ICMPv4-In) [Profile: Private]
4. Confirmed that the firewall rule now **allows incoming ping requests (ICMPv4)**.
5. Re-tested connectivity by pinging from **Server 2022 to Windows 10**, which now succeeded.

Result:

The issue was resolved. This step ensured **bi-directional network communication** was functional for testing and administrative purposes across the domain environment.