Active Directory Project

Introduction

Project Overview

This project demonstrates my understanding of **Active Directory (AD)** administration, including tasks such as configuring security settings, managing users and groups, and performing basic vulnerability assessments within an Active Directory environment. Through this project, I aim to showcase essential administrative skills in Active Directory, which is widely used in enterprise settings to manage and control multiple devices and users across an organization.

Active Directory (AD) is a tool developed by Microsoft that allows administrators to manage and secure resources, users, and devices within a networked environment. It is especially valuable in enterprise networks with multiple domains and devices because it centralizes control, improving the efficiency and security of large-scale IT environments.

Core Concepts in Active Directory

Domains

A domain is the fundamental organizational unit within an Active Directory structure, used to manage and control all network resources, including user accounts, computers, printers, and other devices. Domains allow administrators to enforce policies and permissions across all devices within the network.
Examples of domain controllers include Windows Server editions (such as Windows Server 2019 or 2022), which help manage domain authentication, security policies, and resource access within an Active Directory environment.

Windows Clients

Windows clients refer to individual workstations and laptops running Microsoft's Windows OS that are integrated into an Active Directory domain. Devices like Windows 10 and Windows 11 PCs can join a domain, allowing them to be centrally managed and controlled by administrators.
Administrators can control settings, enforce security policies, and push software updates across all connected Windows clients, providing a streamlined way to manage large numbers of computers from a central location.

Project Tools and Technologies

1. **Virtual Machines (VirtualBox):**
VirtualBox was used to create isolated virtual environments for the Windows Server (acting as the domain controller) and Windows client systems. This setup enabled the creation of a simulated enterprise network environment without impacting any production systems.

2. **Windows Server:**
A virtual machine running Windows Server was configured to serve as the domain controller. This machine managed the Active Directory environment, including the configuration of roles, domain setup, security settings, and implementation of group policies.

3. **Windows Clients:**
Windows 10 or Windows 11 virtual machines acted as client devices within the network. These clients joined the Active Directory domain and were used to demonstrate user and group management, policy enforcement, and device administration.

4. **CherryTree:**

CherryTree, a hierarchical note-taking application, was utilized for documenting configurations, processes, and observations throughout the project.

5. **Greenshot:**
Greenshot, a lightweight screenshot tool, was used to capture images and document visual aspects of the configurations and processes during the project for reporting and reference purposes.

This project will not only demonstrate my ability to perform fundamental AD administrative tasks but will also highlight my understanding of security configurations and vulnerability analysis using BloodHound and SharpHound. By the end, I aim to have a well-documented setup of an AD environment with controlled access, applied security settings within an enterprise-like environment.

Lab Environment Setup

Description

The **lab environment setup** for this project will involve several key steps designed to simulate a real-world enterprise network within a virtualized environment. This setup will include the installation of virtual machines, configuration of network settings, and the installation of Windows Server and Windows client operating systems to create an Active Directory (AD) domain environment. The lab environment will provide a controlled setting for practicing AD administrative tasks, security configurations, and vulnerability assessments without affecting any live systems.

Key Setup Steps

1. **Installation of Virtual Machines (VMs)**:

• **Virtualization Software**: To create the lab, I will use **VirtualBox** (or an alternative like VMware Workstation) as the virtualization platform. VirtualBox enables me to run multiple virtual machines on a single physical computer, simulating different roles within a networked environment.

• **Creating VMs for Server and Clients**: Separate VMs will be created to represent a Windows Server (which will act as the Domain Controller) and several Windows clients. Each virtual machine will be configured with resources like CPU, RAM, and storage according to the requirements of the operating system it will run.

2. **Configuration of Network Settings**:

◇ **Network Mode**: Virtual machines will be connected using a **"Host-Only"** or **"Internal Network"** mode, which ensures that the VMs can communicate with each other without needing external internet access, creating an isolated network.

◇ **IP Address Allocation**: IP addresses will be manually assigned to each VM or managed via a DHCP server on the Windows Server. This setup will replicate a small office network and allow for seamless communication within the domain.

◇ **Domain Controller Configuration**: The Windows Server will be configured to serve as a domain controller within the network, managing the Active Directory domain and ensuring all client machines can authenticate and communicate within this domain environment.

3. **Installation of Windows Server**:

◇ **Operating System Installation**: A VM will be installed with **Windows Server** (e.g., Windows Server 2019 or 2022) to act as the domain controller. This server will host the Active Directory Domain Services (AD DS) role, which is responsible for managing the domain.

◇ **Active Directory Setup**: After installation, the AD DS role will be configured on the server, establishing a new domain (e.g., *lab.local*) to which client machines will be added. This will involve setting up the forest, domain name, and additional configurations necessary for AD functionality.

◇ **DNS and DHCP Services**: The server will also be configured to manage DNS and, optionally, DHCP, allowing it to handle both name resolution and dynamic IP address allocation within the virtual network. DNS is essential for AD operations, as it allows client machines to locate the domain controller for authentication and resource access.

4. **Installation of Windows Client Operating Systems**:

◇ **Client VMs**: Separate virtual machines running Windows 10 or Windows 11 will be created to act as domain-joined clients. These VMs simulate the workstations and laptops typically found in an enterprise environment.

◇ **Domain Joining Process**: Each client machine will be configured to join the domain established on the Windows Server. This will allow administrators to apply security policies, manage user accounts, and enforce permissions from a central location.

◇ **User and Group Policies**: Once the clients are added to the domain, group policies and security

configurations can be applied to these machines from the domain controller, replicating a realistic enterprise control setup.

Expected Outcome

At the end of this setup phase, I will have a functioning Active Directory environment that replicates a small enterprise network. This environment will consist of:

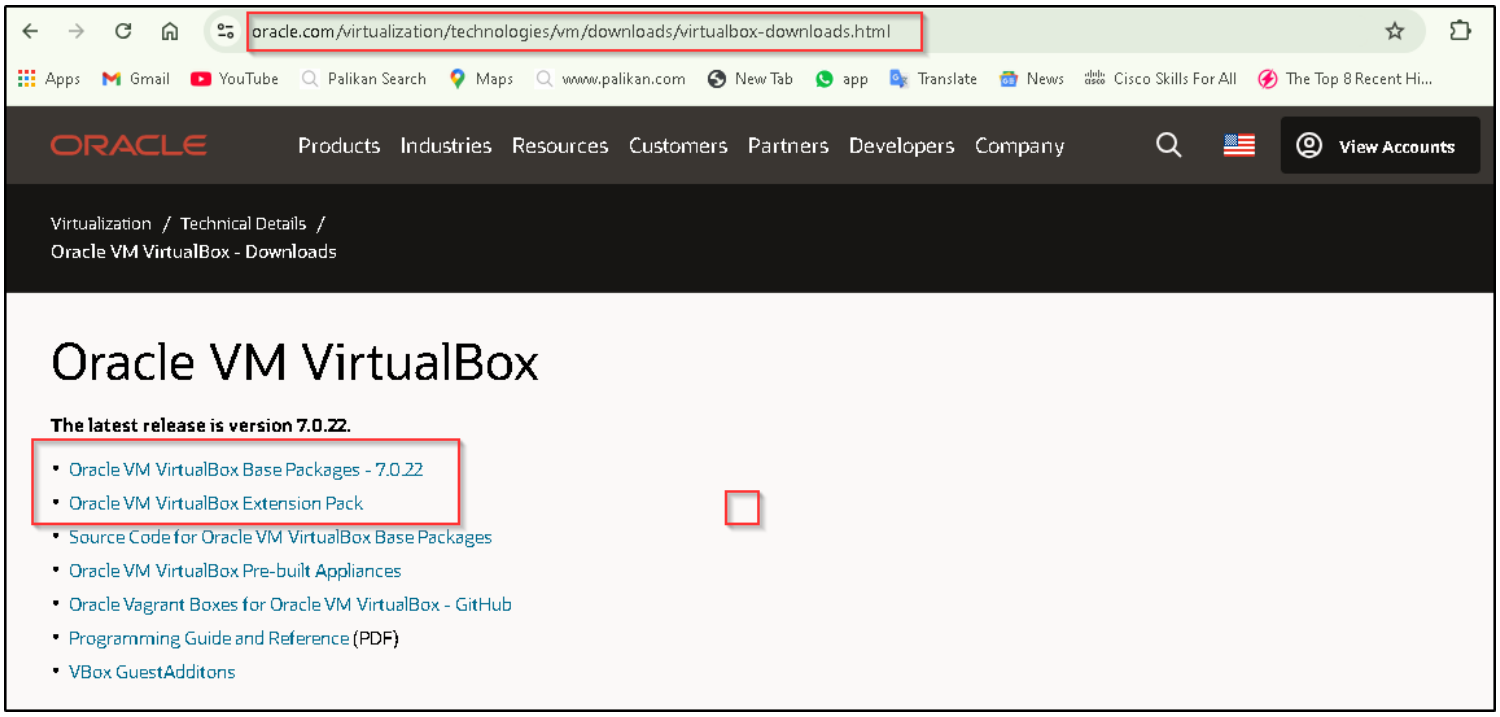
- A centralized **Windows Server** configured as the domain controller and managing AD services, DNS, and potentially DHCP.
- Multiple **Windows client machines** integrated into the domain, ready for AD management tasks, policy enforcement, and security configurations.
- A secure network configuration that isolates the lab environment and facilitates controlled testing and experimentation with AD management and security practices.

This lab environment will provide a comprehensive foundation for experimenting with AD administration, configuring user and group permissions, applying security policies, and identifying potential vulnerabilities within the domain, all while documenting each step for reference and learning.

Installation of Virtual Machines (VMs)

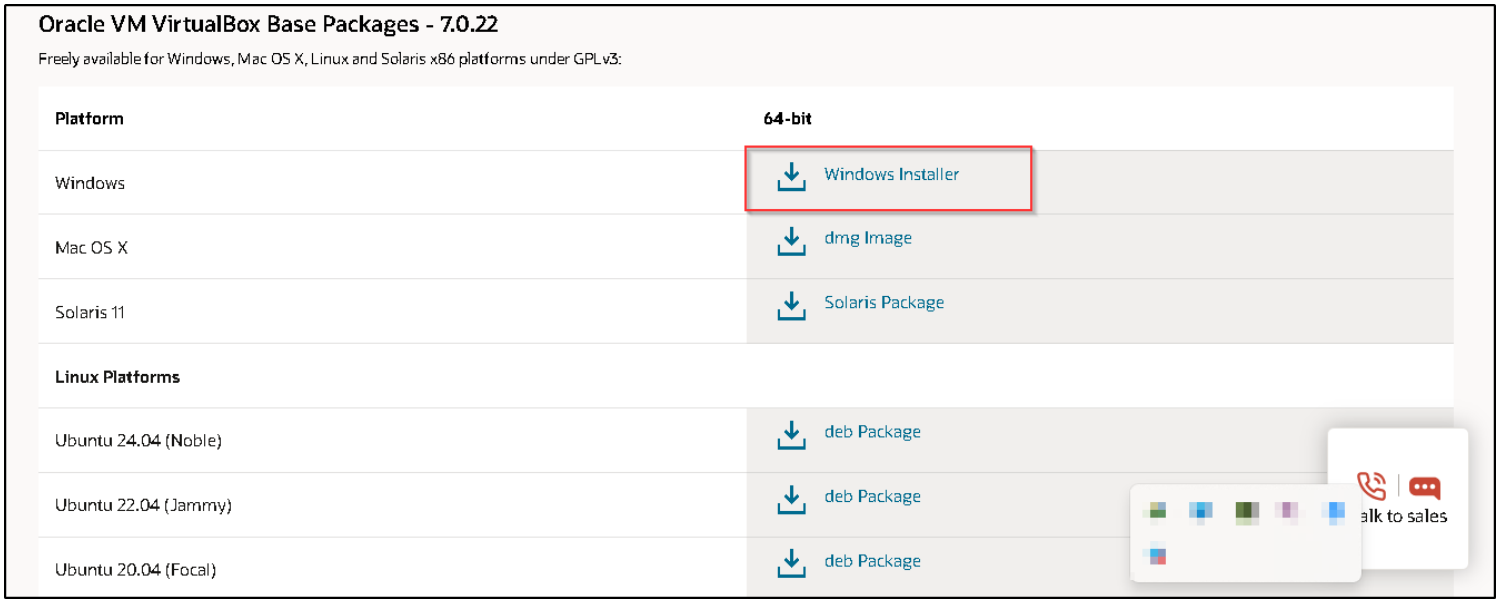
Downloan the Virtual box at Oracel website.

I downloaded VirtualBox from Oracle's website, including both the **Oracle VM VirtualBox Base Package (version 7.0.22)** and the **Extension Pack**. The Extension Pack adds support for additional features like USB 2.0/3.0 devices, VirtualBox RDP, disk encryption, and more, which are useful for enhancing the virtual environment.



I selected the Windows installation option since my host system is running Windows OS.

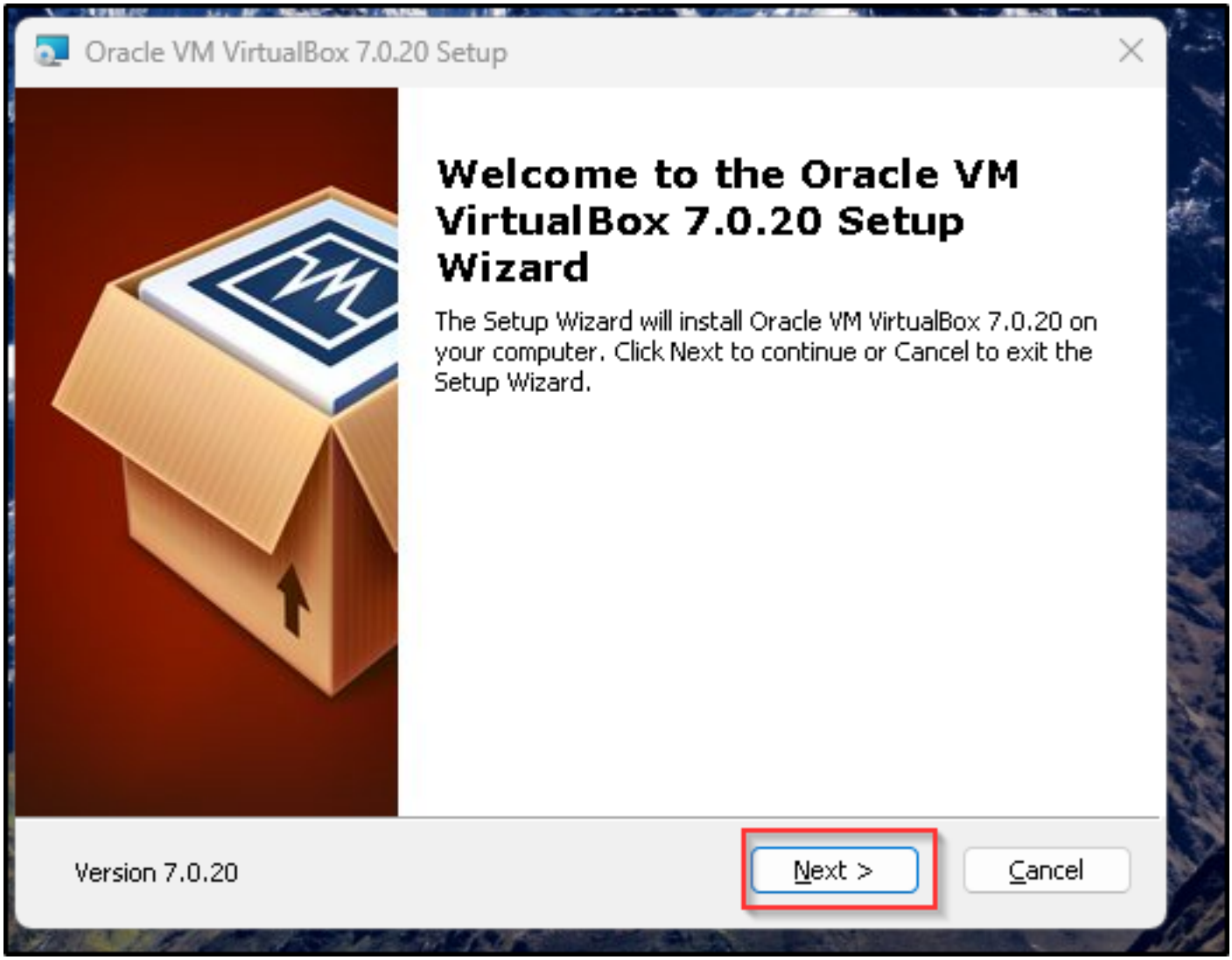
I'm using **VirtualBox version 7.0.20** as my virtualization software.



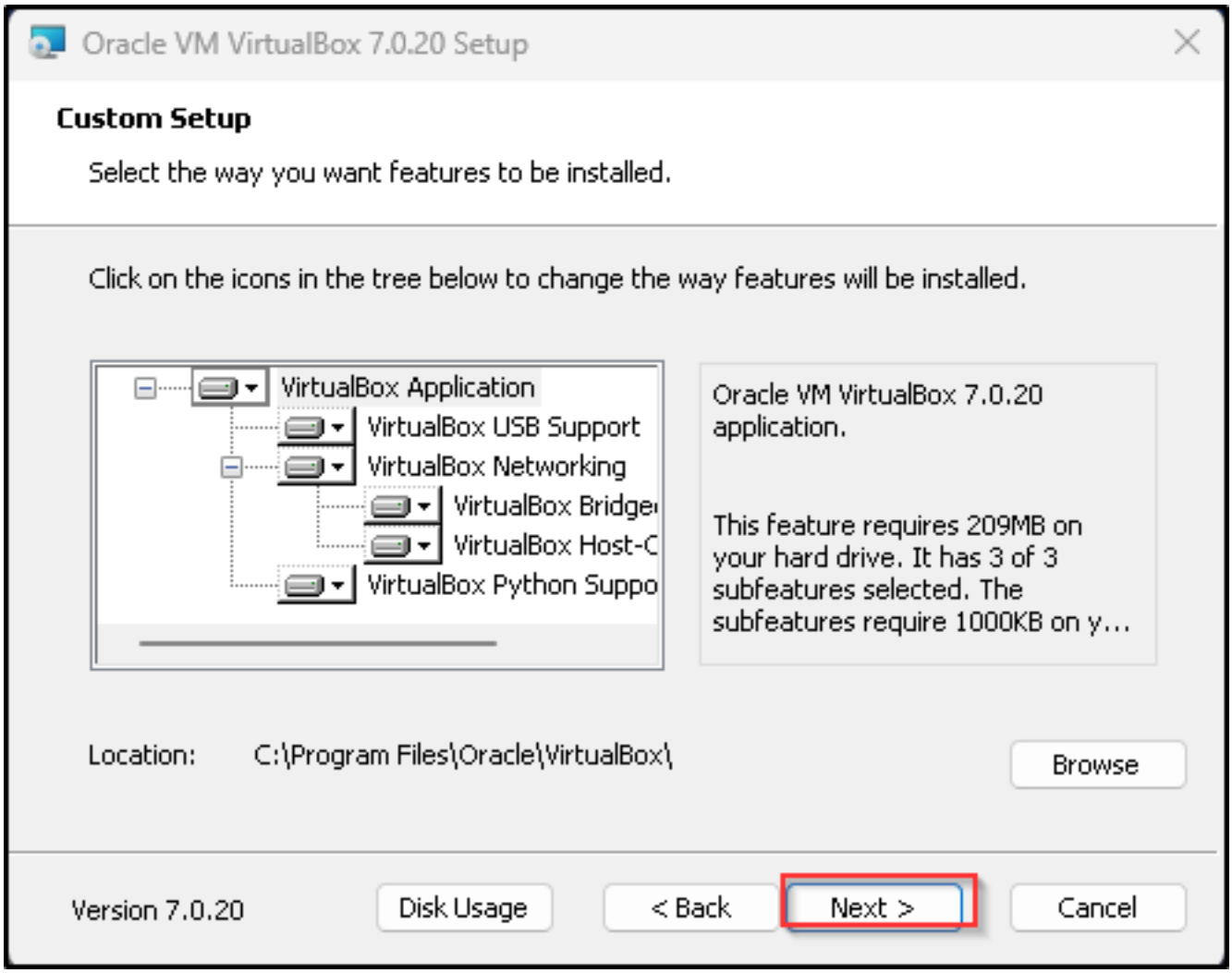
Installation Process:

Step 1:

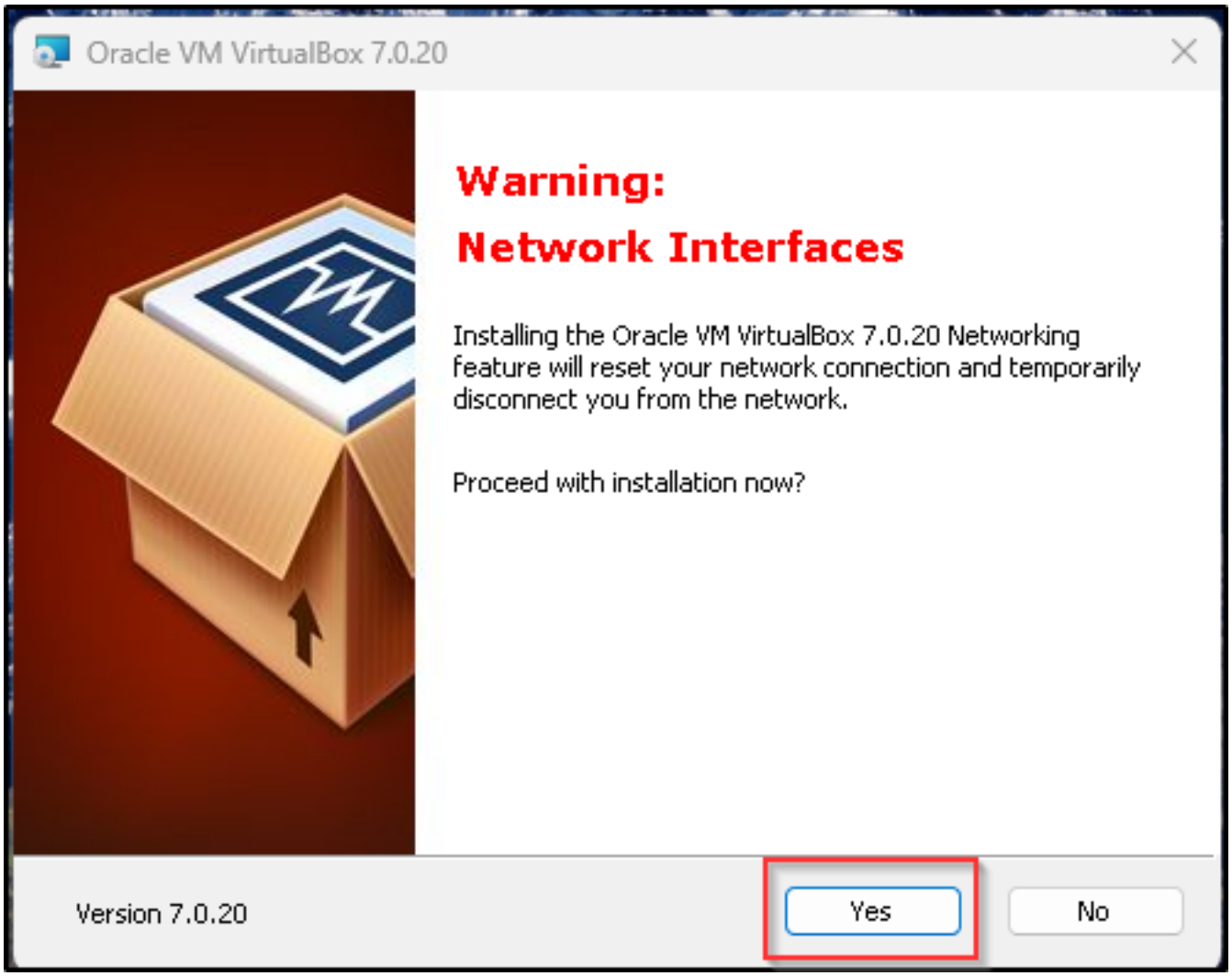
I navigated to my **Downloads** folder and double-clicked the VirtualBox installation file.
A setup window appeared, and I clicked **Next** to begin the installation process.



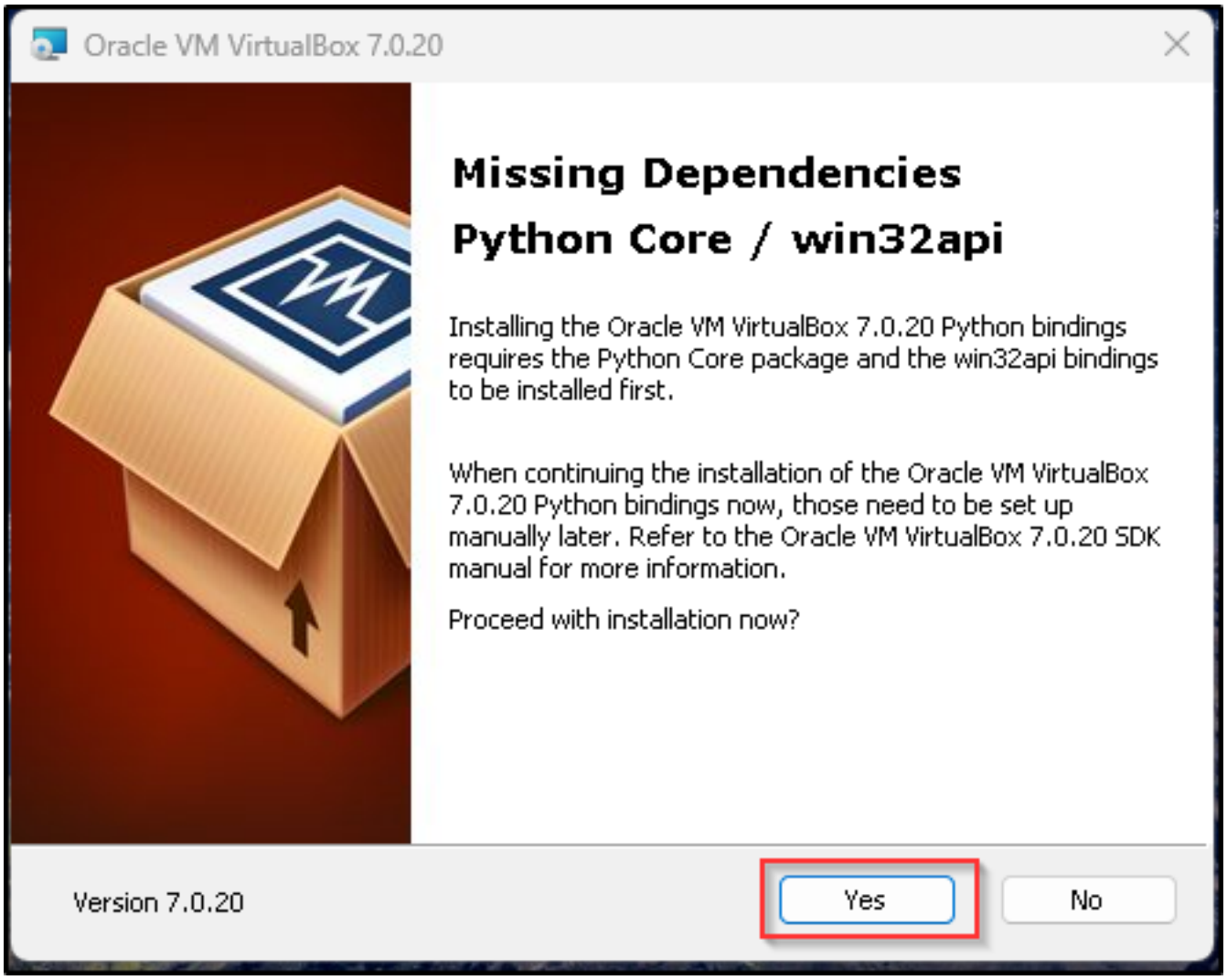
Step 2:
At this stage, I chose the default file location for installing VirtualBox files. Alternatively, I could select a preferred location if needed.
I then clicked **Next** to proceed.



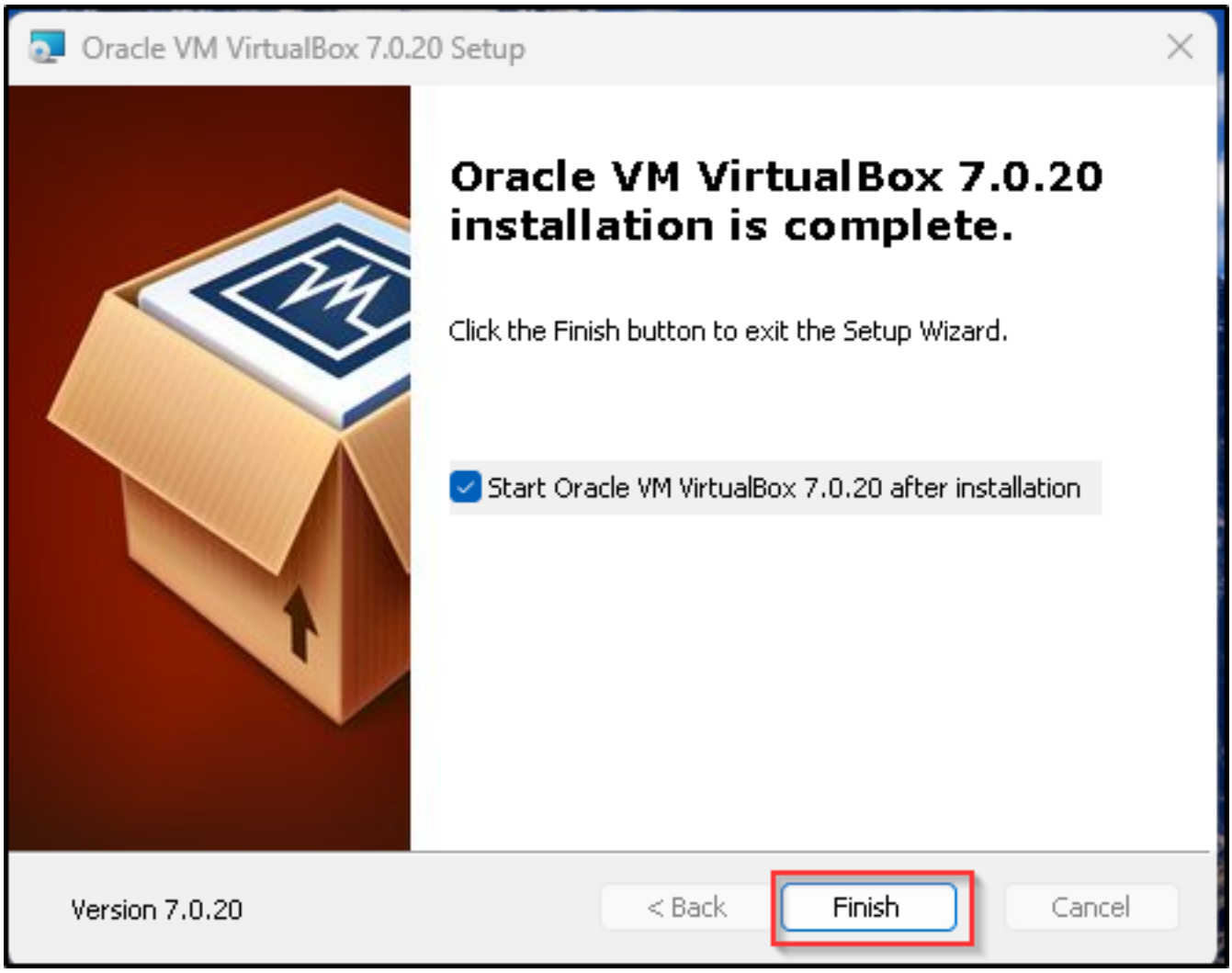
I ignored this warning and clicked **Yes** to continue.



For VirtualBox to install properly, it requires certain dependencies, such as **Python Core** and **win32api**. I clicked **Yes** to confirm the installation of these dependencies.



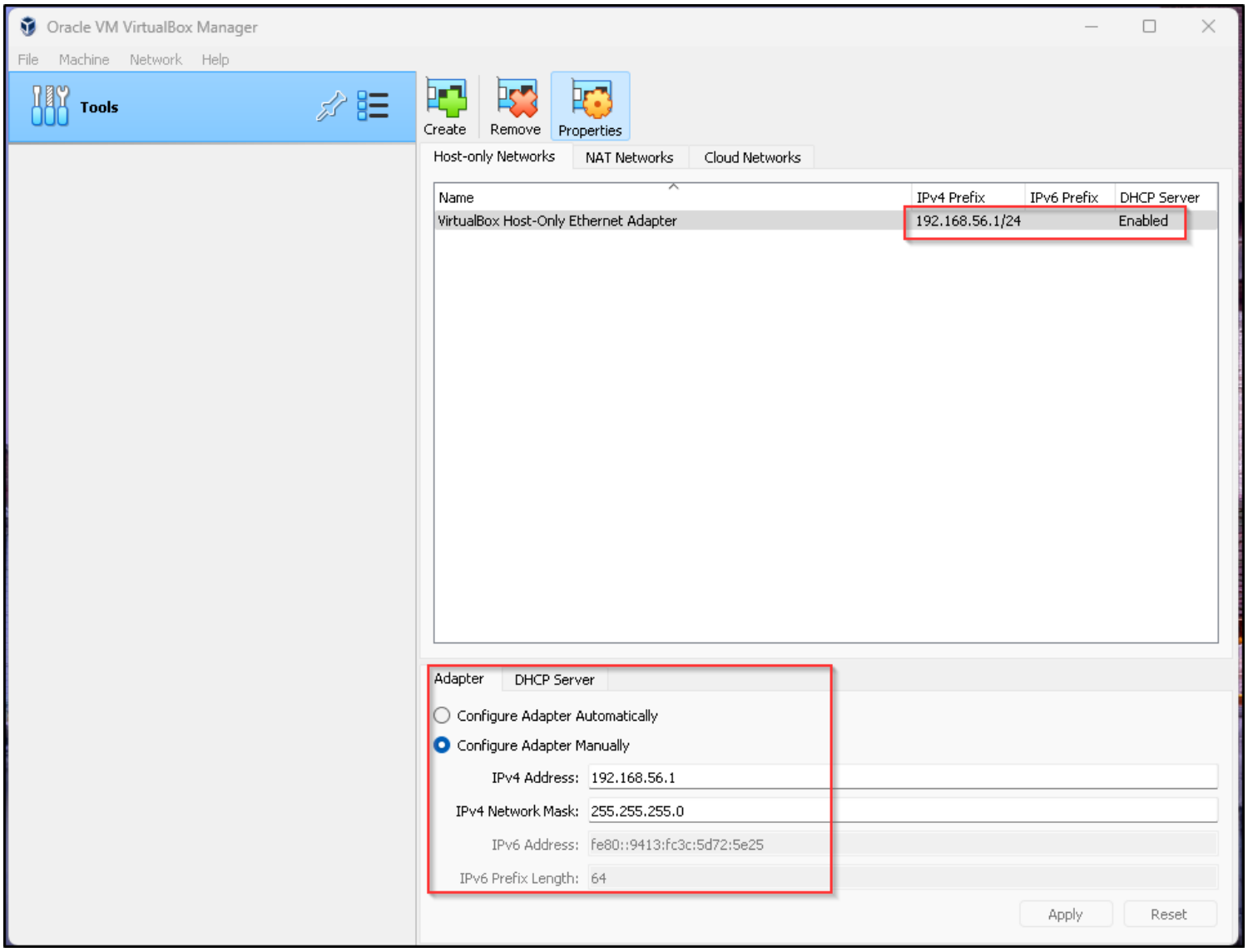
I continued clicking **Next** through each setup stage until I reached the final screen, where I clicked **Finish** to complete the installation.



I successfully installed VirtualBox.

Network and System Configuration in VirtualBox

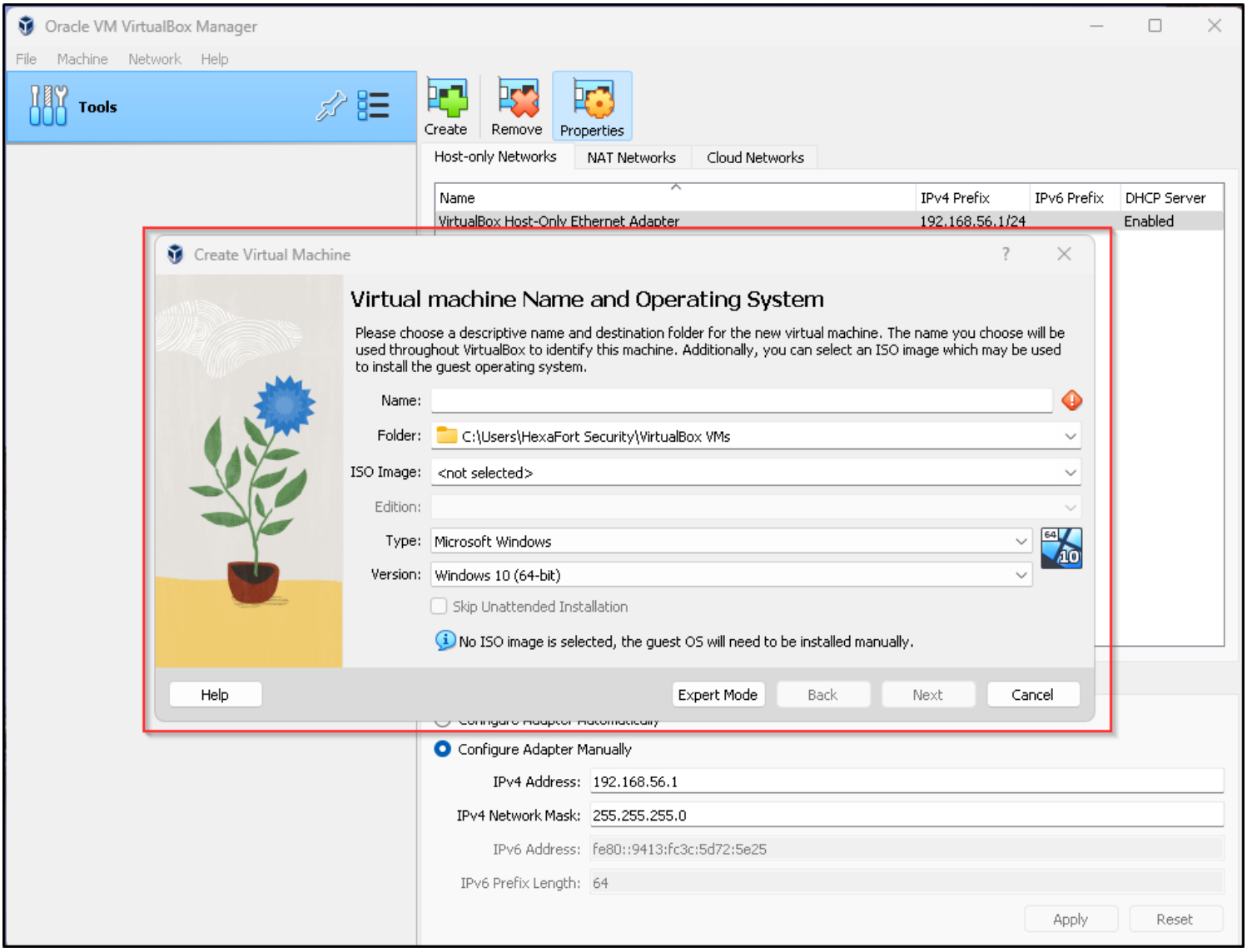
The VM opened with its default network settings. The **Network Adapter** is set to **Host-only Ethernet Adapter**, with a default IP address configuration of **192.168.56.1/24**.



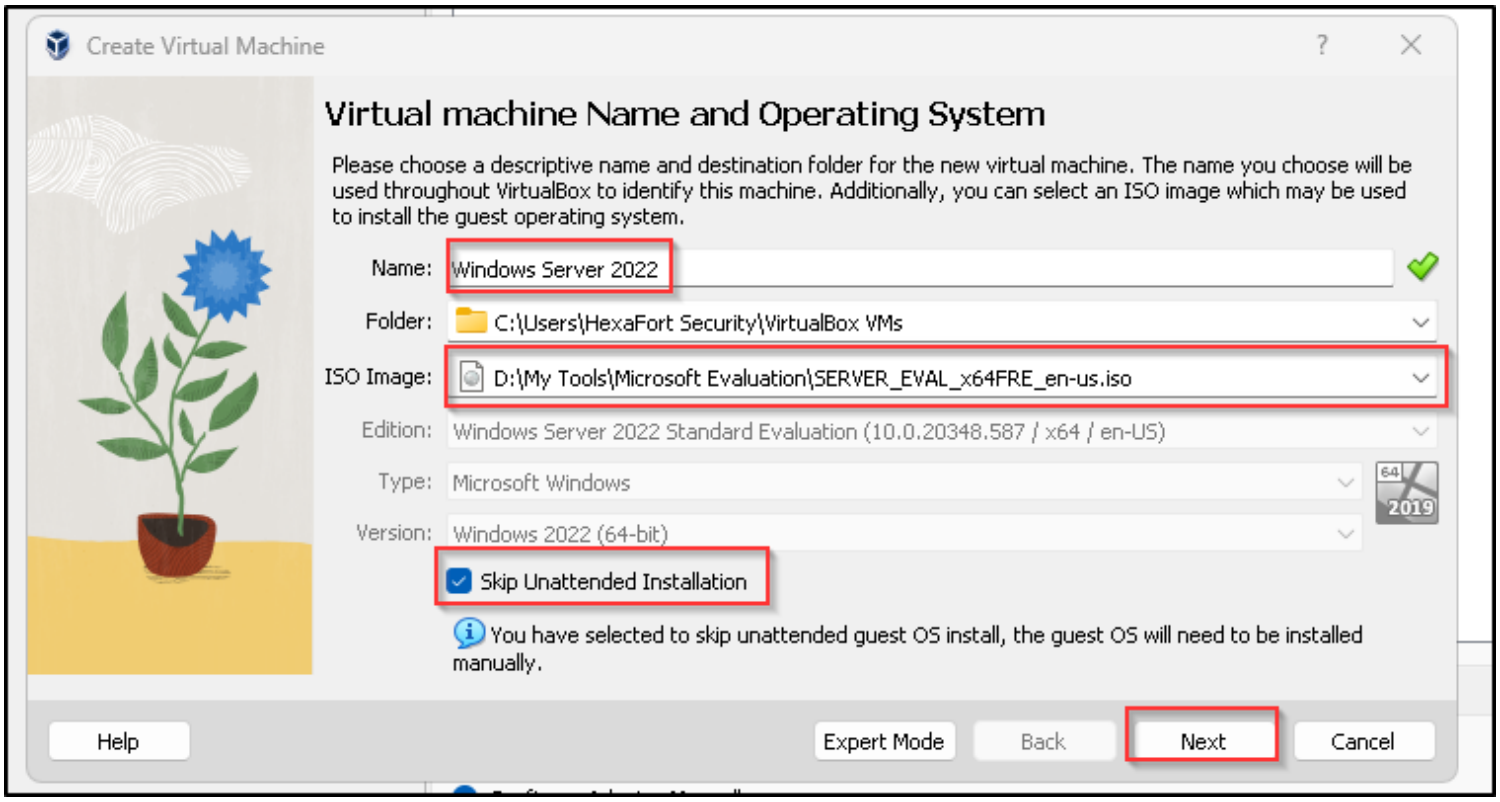
Creating the Windows Server VM and Its Configurations

I clicked on **"Machine"** in the top-left corner of VirtualBox and then selected **"New."**

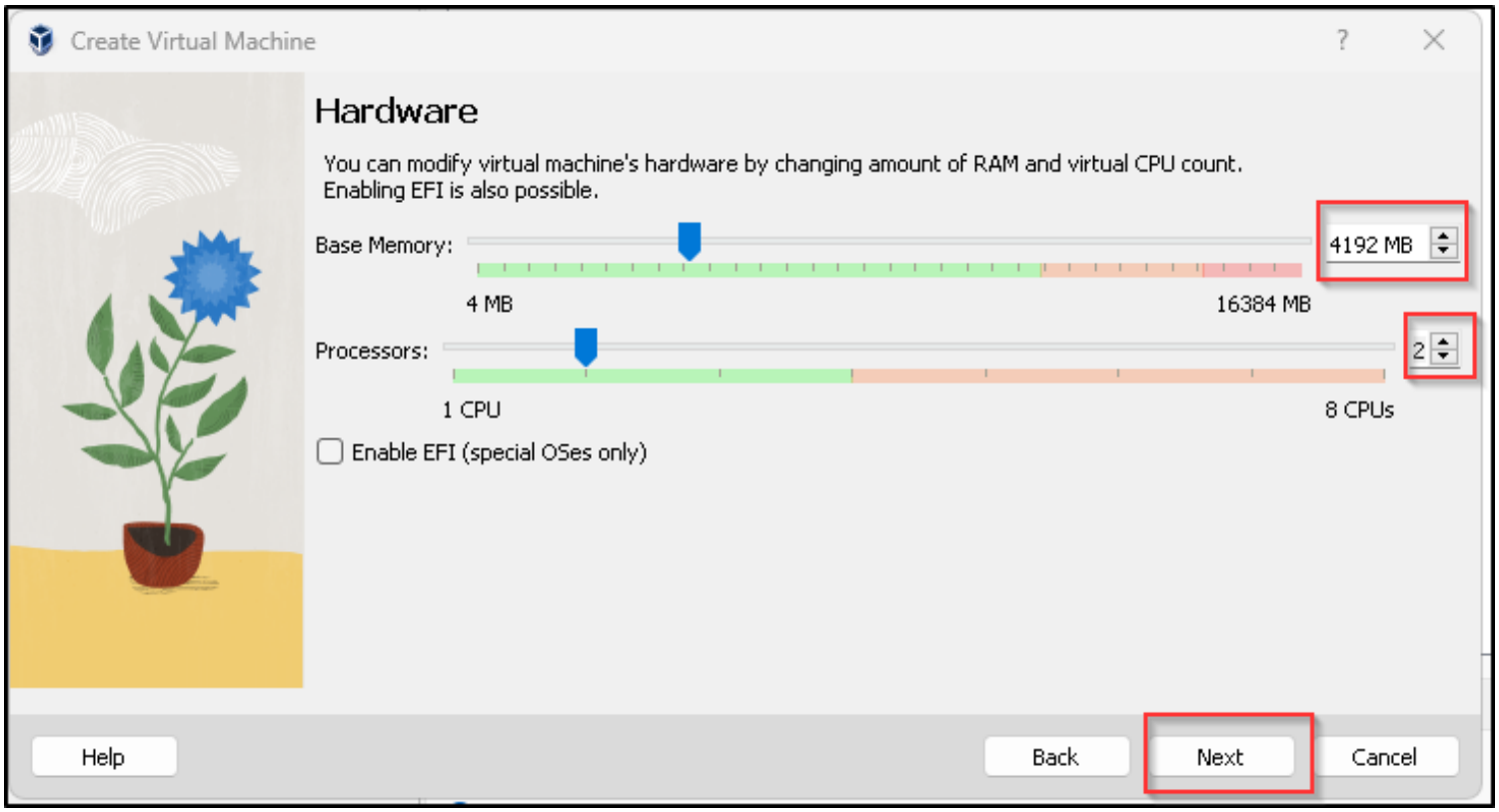
These are the default settings:



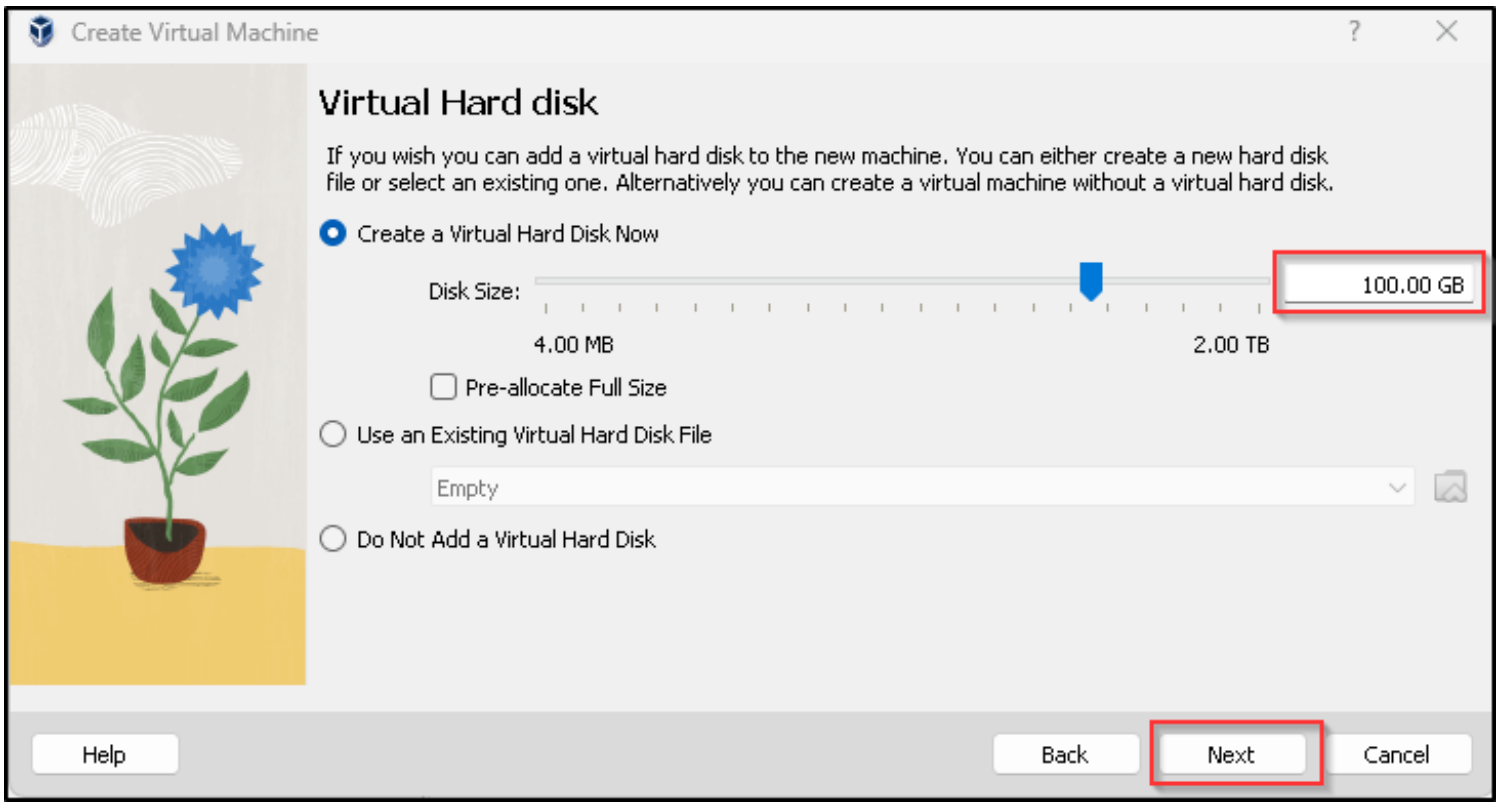
I named the VM **"Windows Server 2022"** for easy identification.
Next, I navigated to my **D:** drive, where I stored my Server ISO file.
I selected **"Skip Unattended Installation"** because I wanted to manually configure the VM and maintain full control over its settings.
I then clicked **Next** to continue.



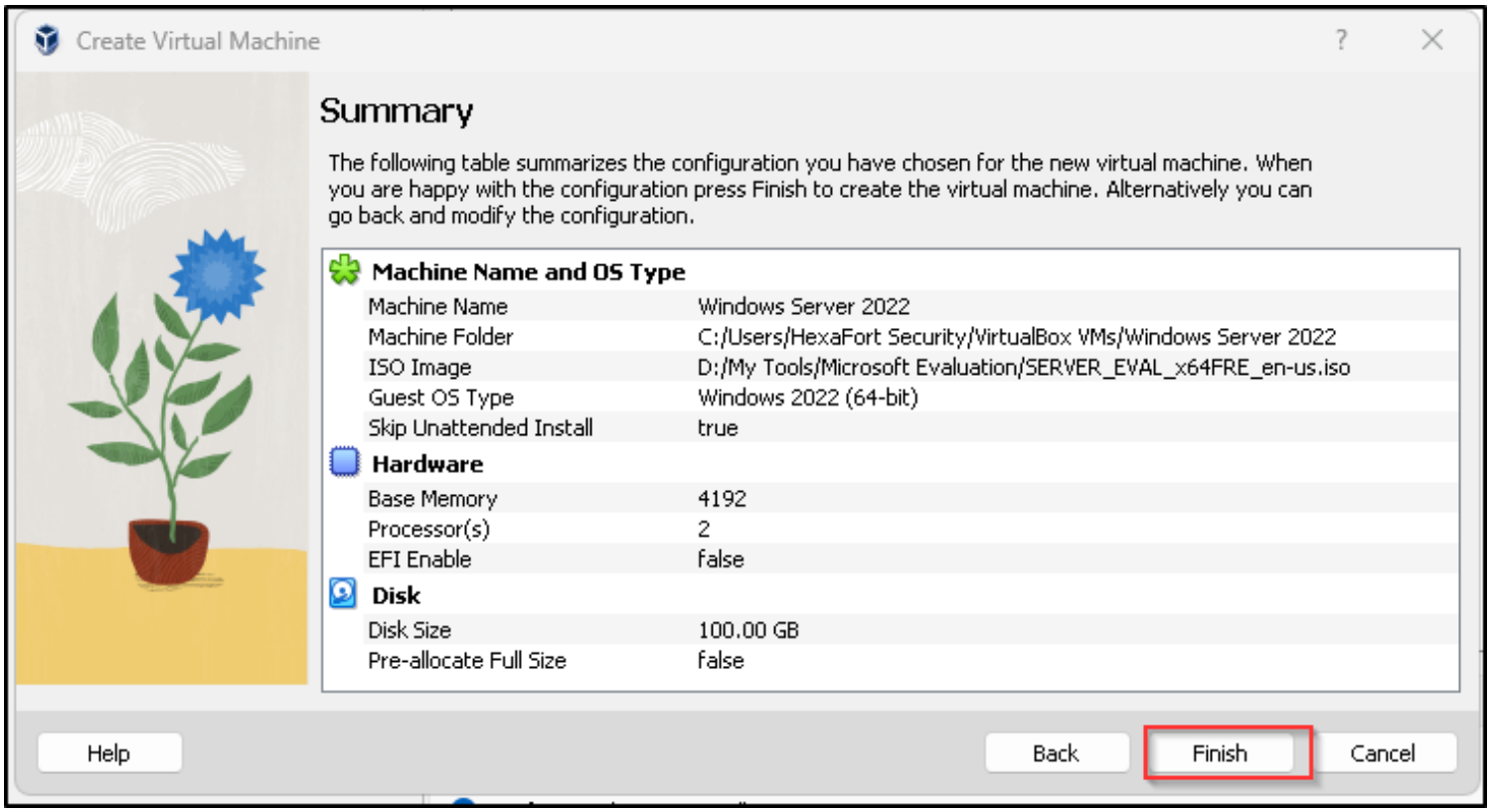
I increased the RAM to **4 GB** for this server, as my host system has **16 GB** of memory. I allocated **2 CPUs** to the VM since my host has a total of **8 CPUs**.
I then clicked **Next** to proceed.



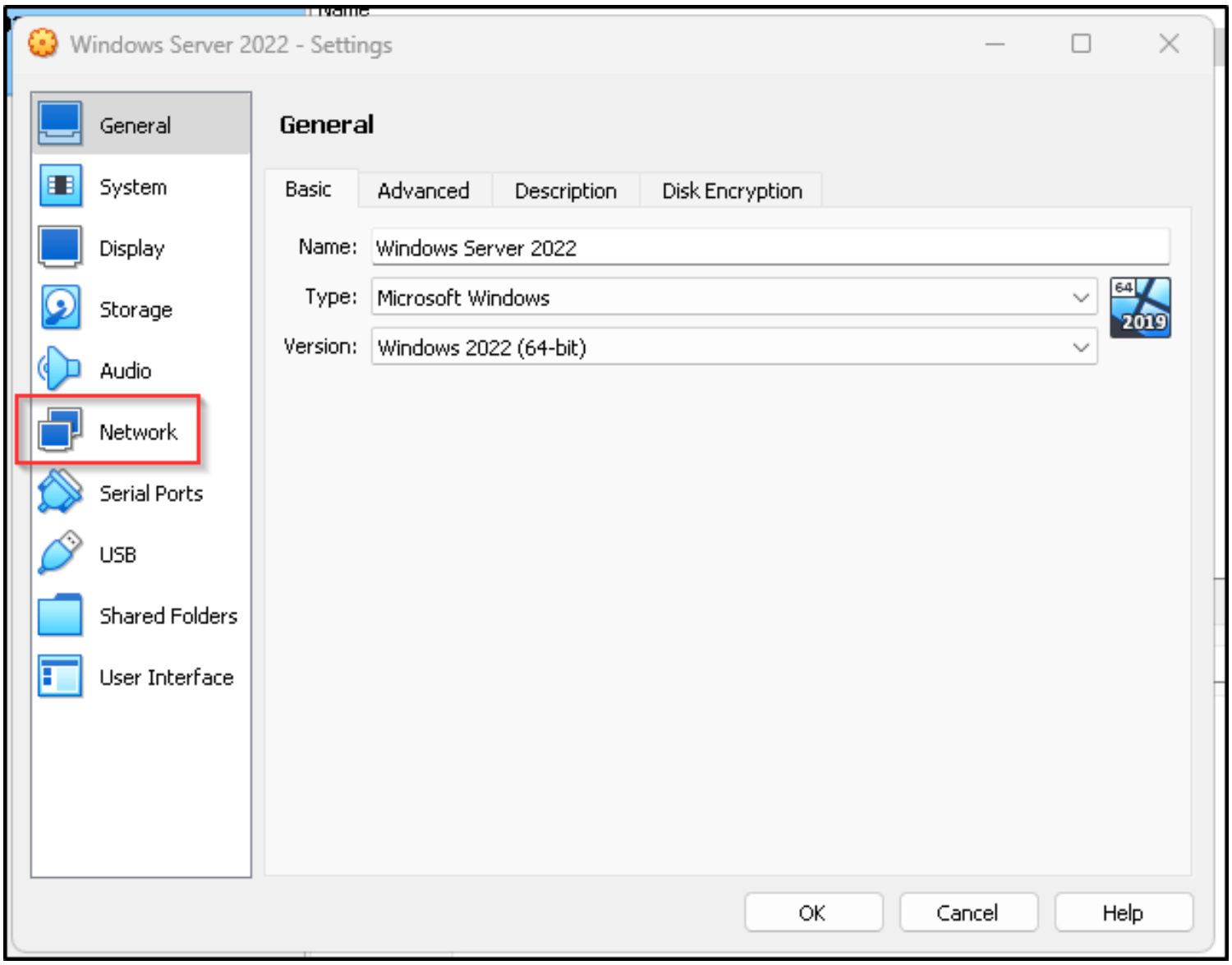
I increased the disk size to **100 GB** since I have **1 TB** of available storage space.
I then clicked **Next** to continue.



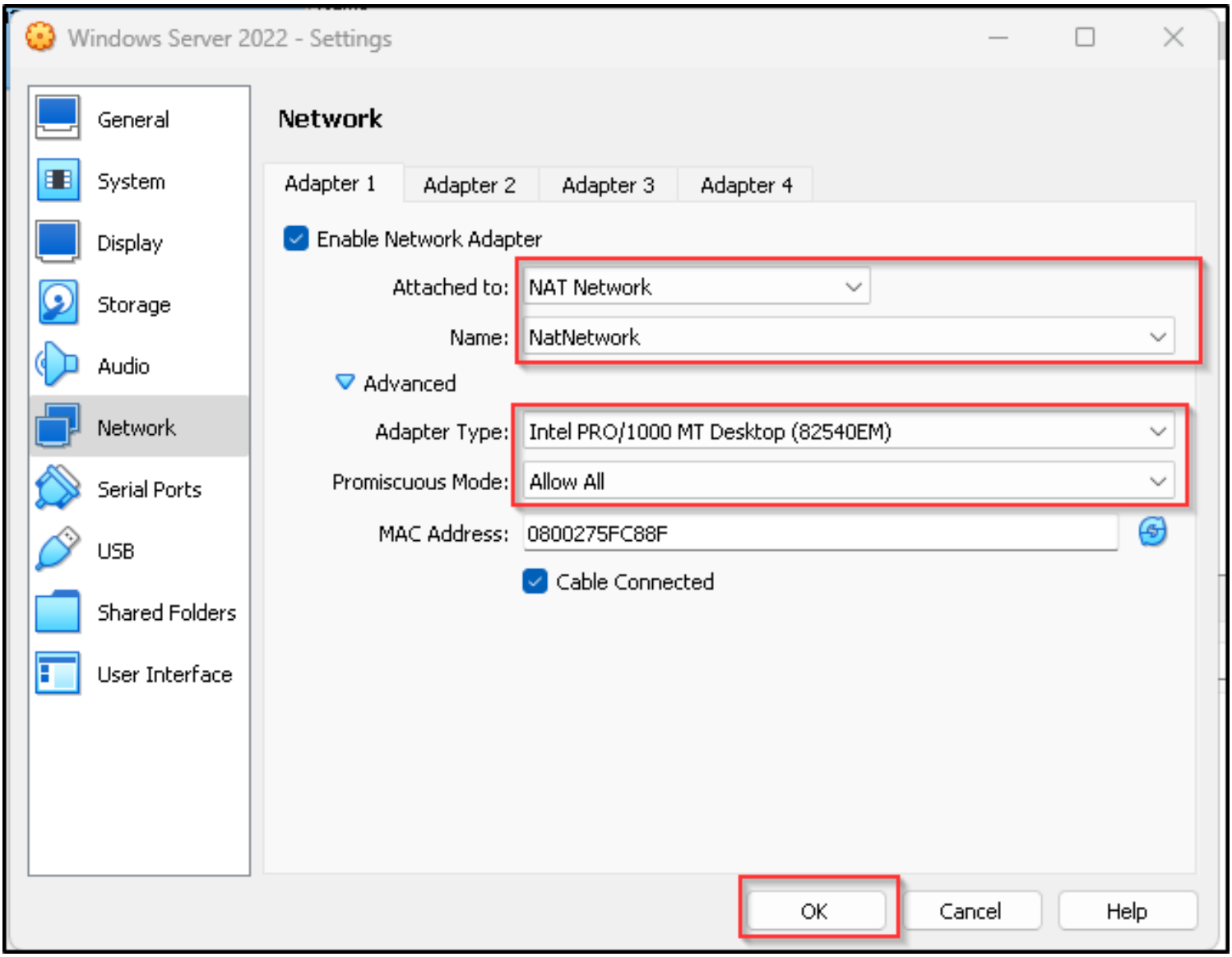
I Confirmed all settings and Click on “Finish”



After successfully setting up the server, I accessed the network settings by clicking on **Settings** at the top center of VirtualBox.
Then, I selected the **"Network"** tab to change the network settings.

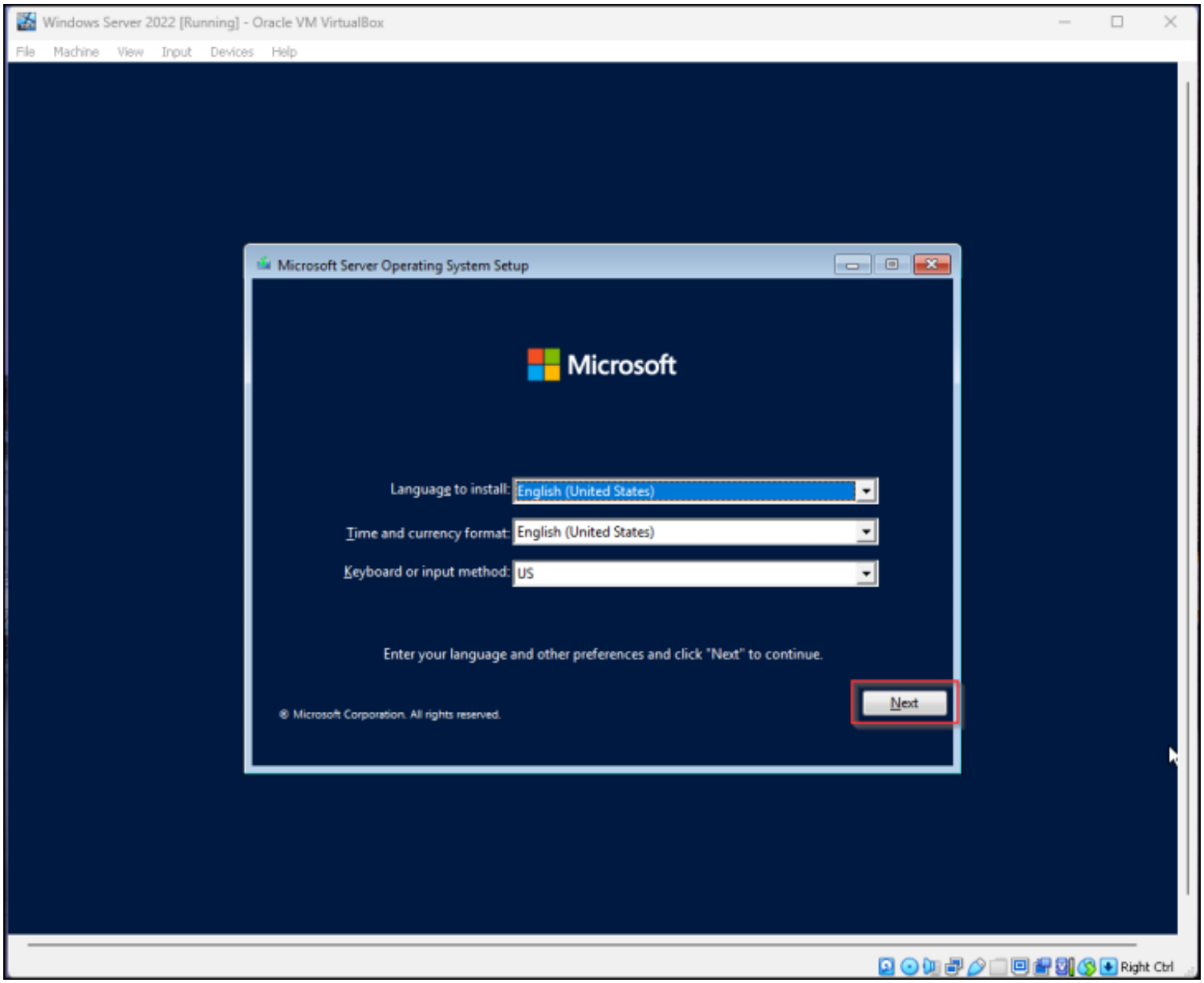


In the **Network** section, I changed the adapter to **NAT Networking**. I chose this option because I want my VM to communicate with other VMs and access the internet, while preventing communication with other VMs or PCs that are not on the same **NAT Network**.
In the **Advanced** section, I selected my local interface as the adapter type, set the **Promiscuous Mode** to **"Allow All,"** and clicked **OK** to save the changes.

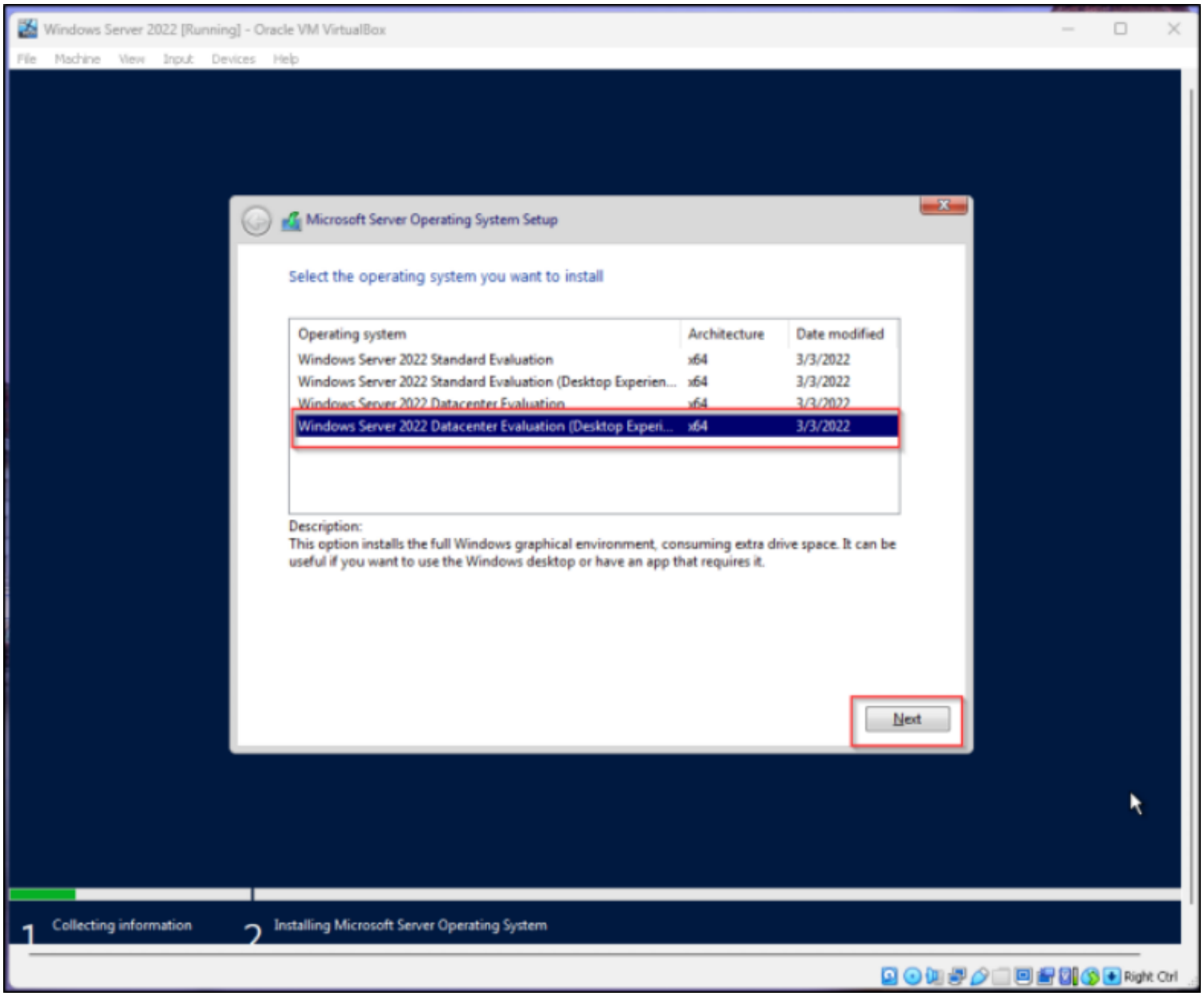


Windows Server Installation Process

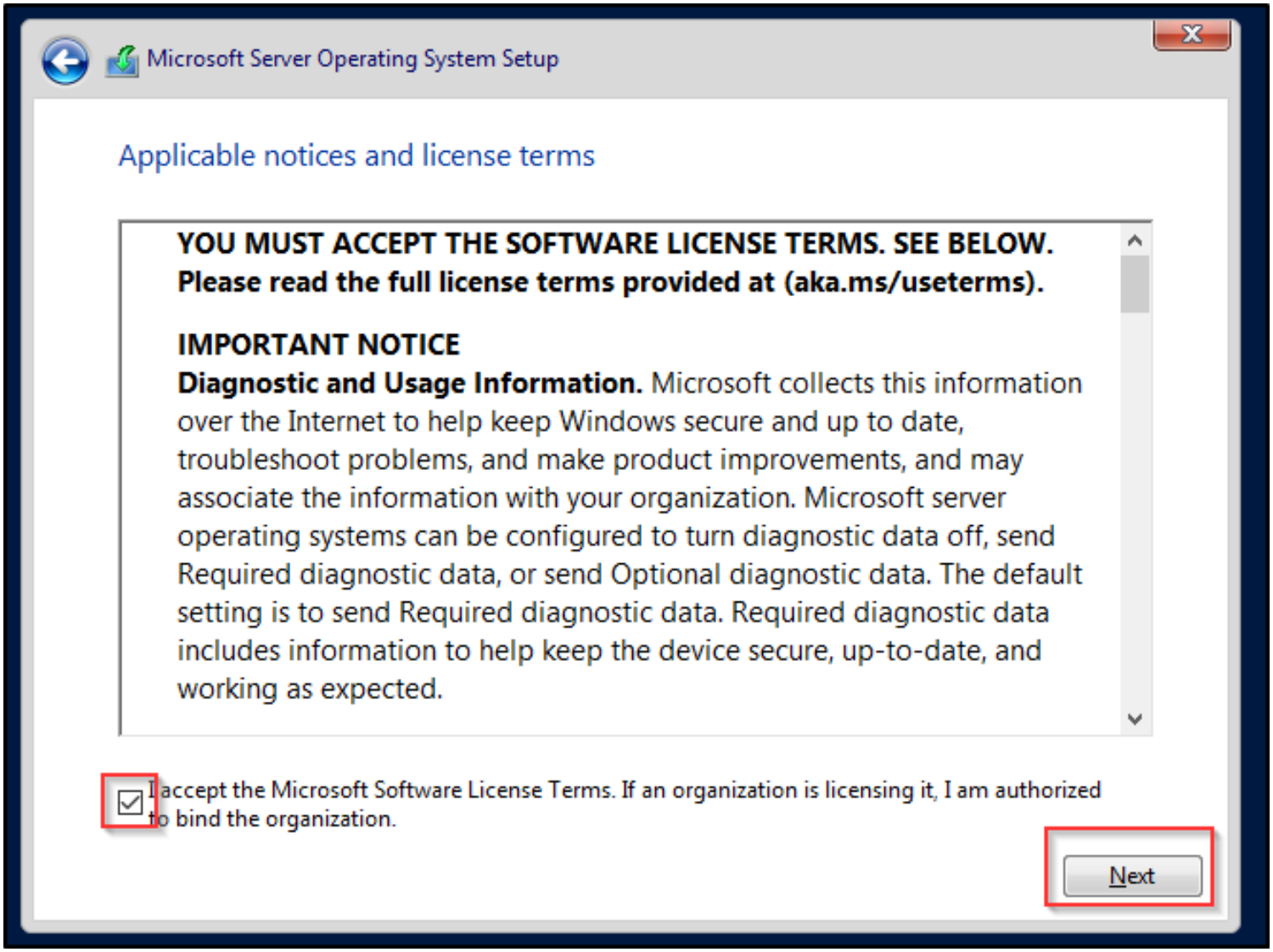
I clicked the **"Start"** arrow to begin the installation process.
I left all settings at their default values, clicked **Next**, and then clicked **Install** to proceed.



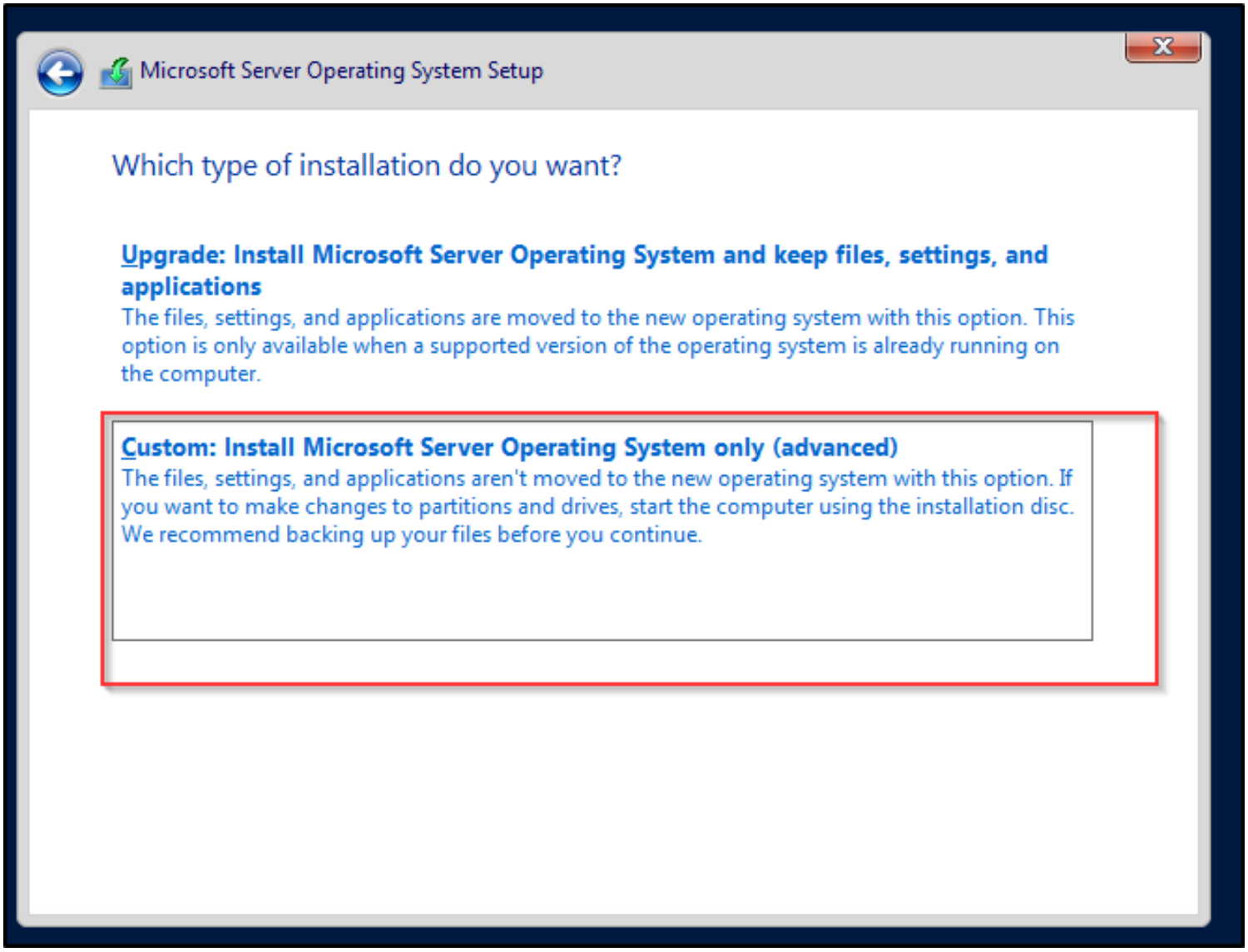
I selected **Windows Server 2022 Datacenter Evaluation (Desktop Experience)** since this is an enterprise lab setup and I prefer using the desktop environment for its user-friendly interface.
I then clicked **Next** to continue the installation process.



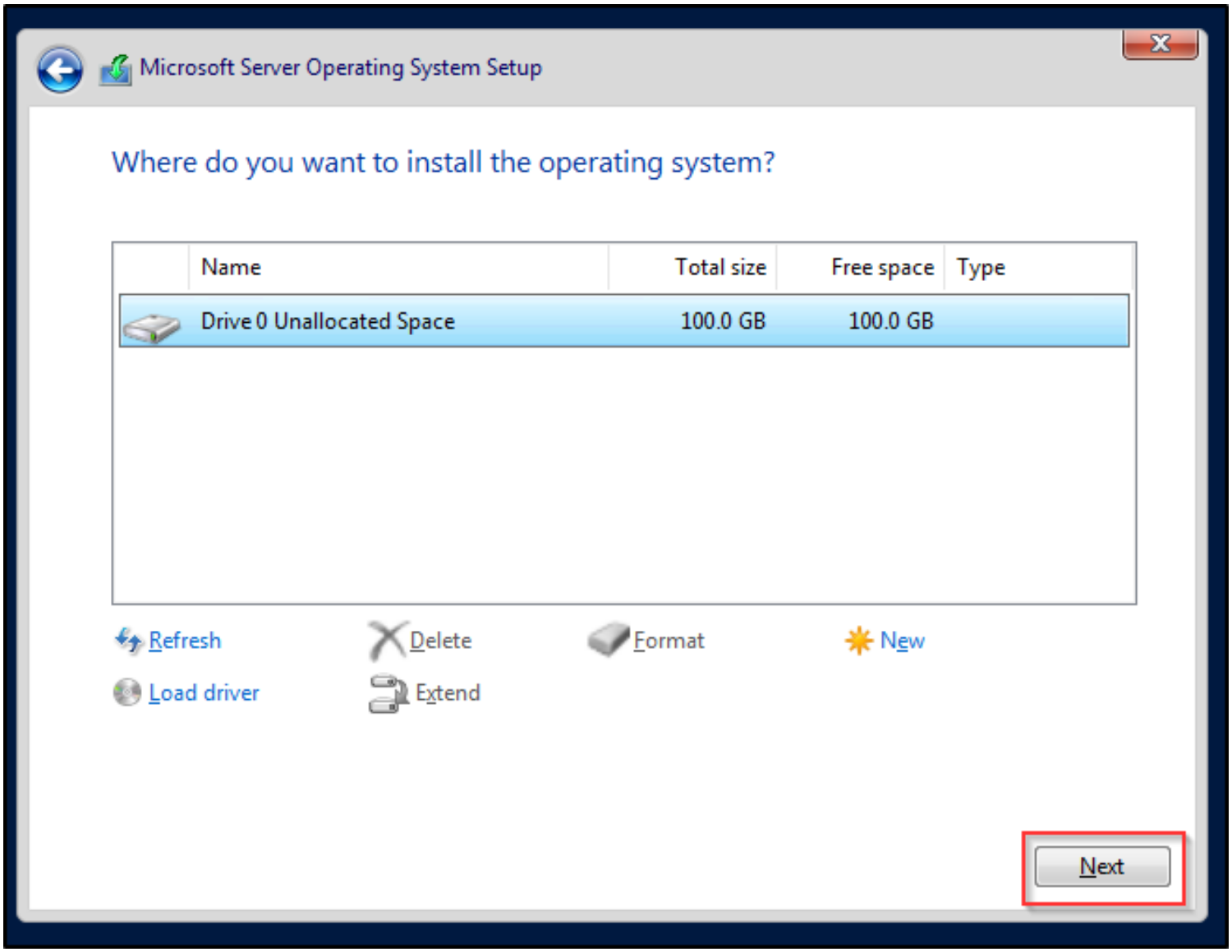
I accepted the license terms and click on “Next”



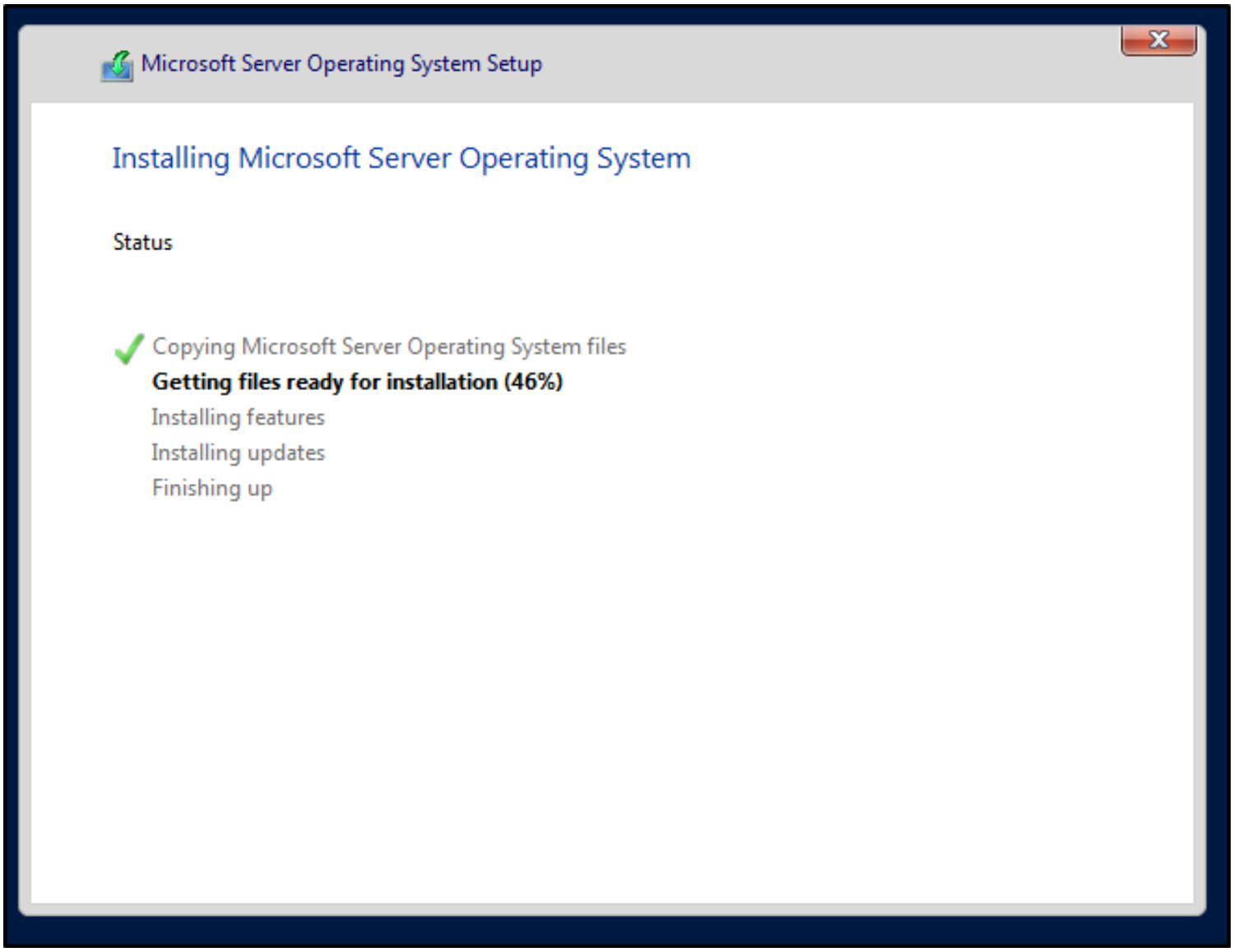
I selected **Custom installation** since this is a fresh installation and I am not upgrading from a previous operating system.



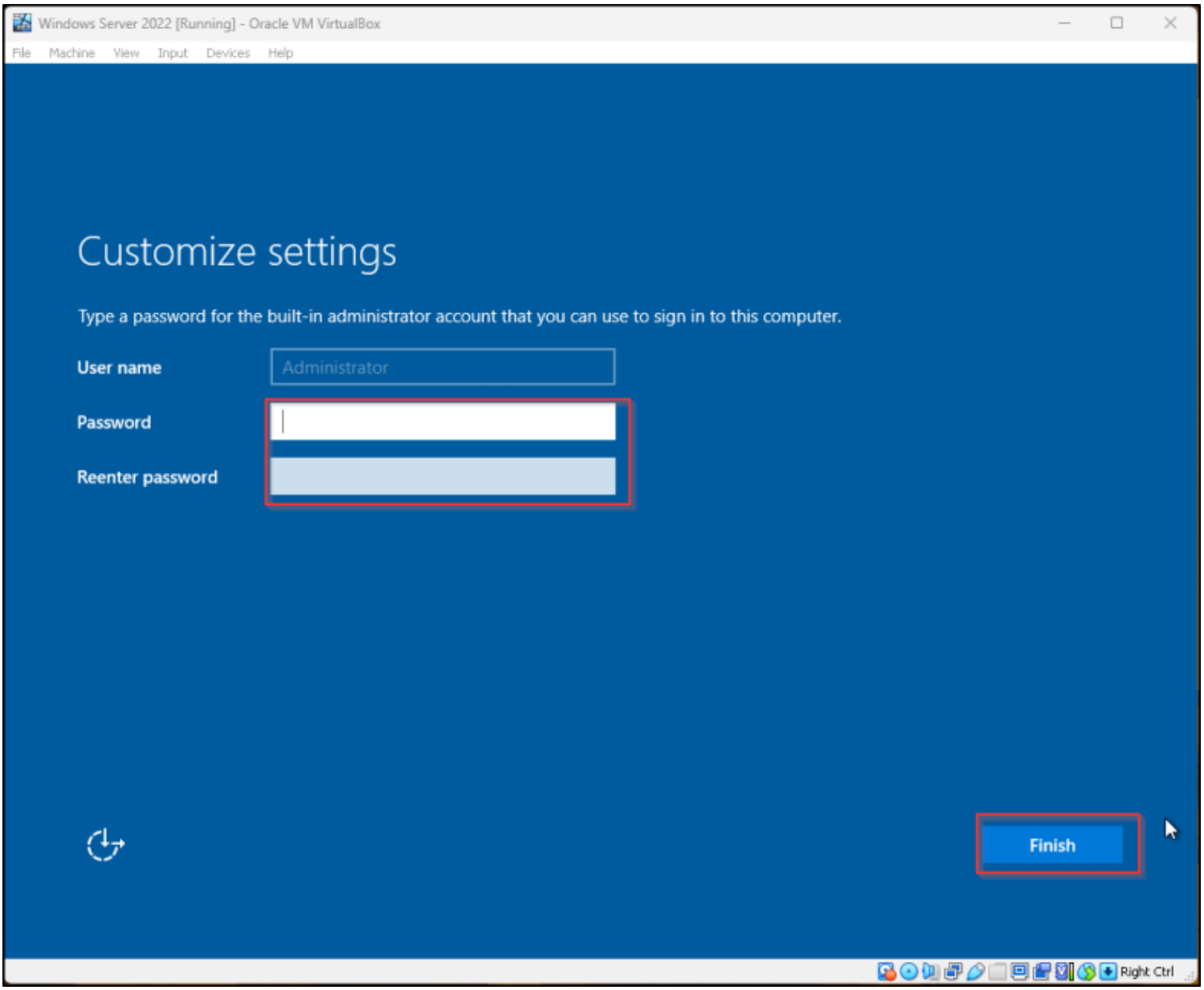
I used the entire disk that I previously allocated for this VM, as I do not need to partition it. I then clicked **Next** to proceed.



The installation continued, and after it finished, the server automatically restarted twice.

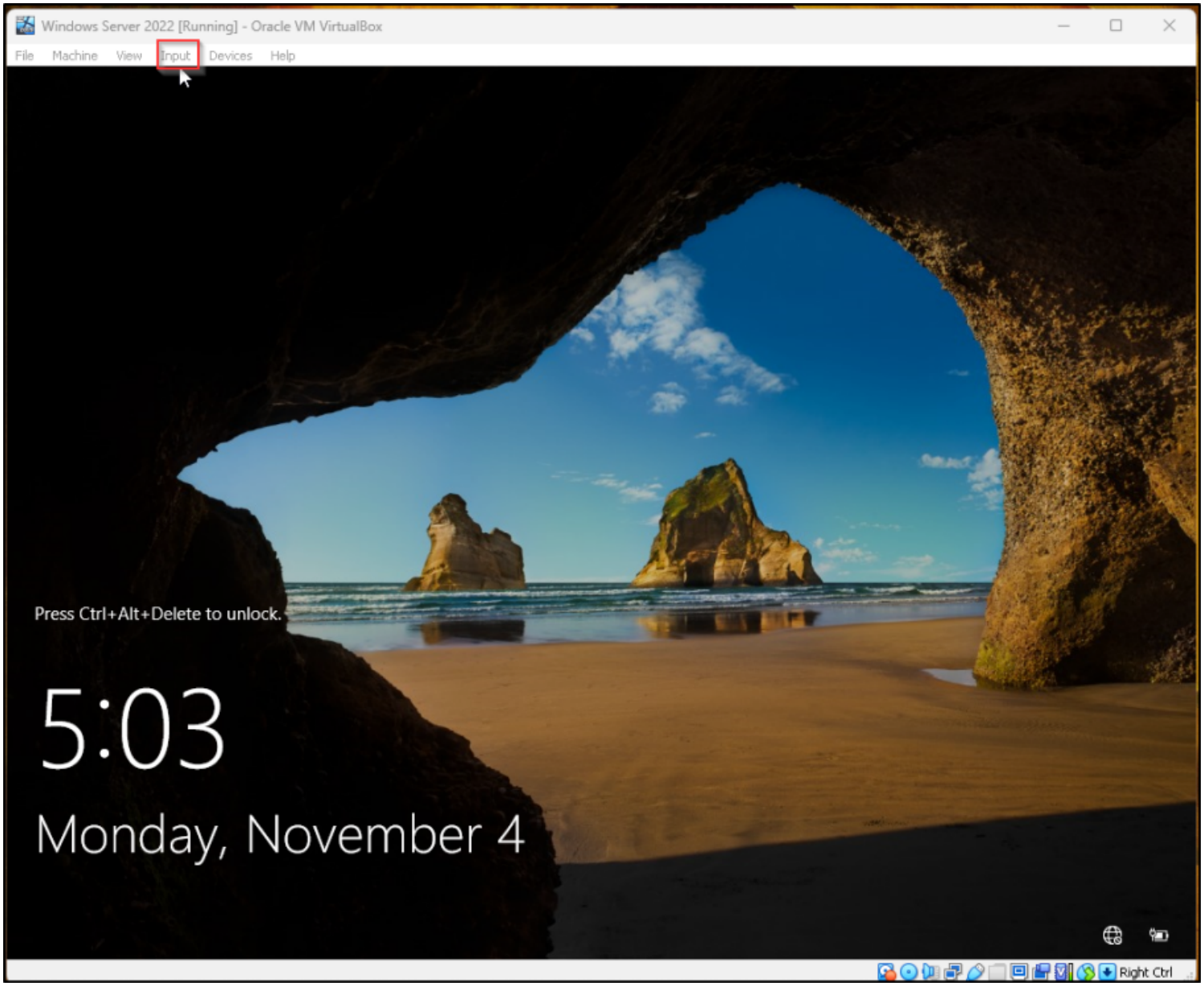


I continued customizing some settings.
Since this is a server, the default account name is **"Administrator."** I entered my password, re-entered it for confirmation, and then clicked **Finish** to complete the setup.

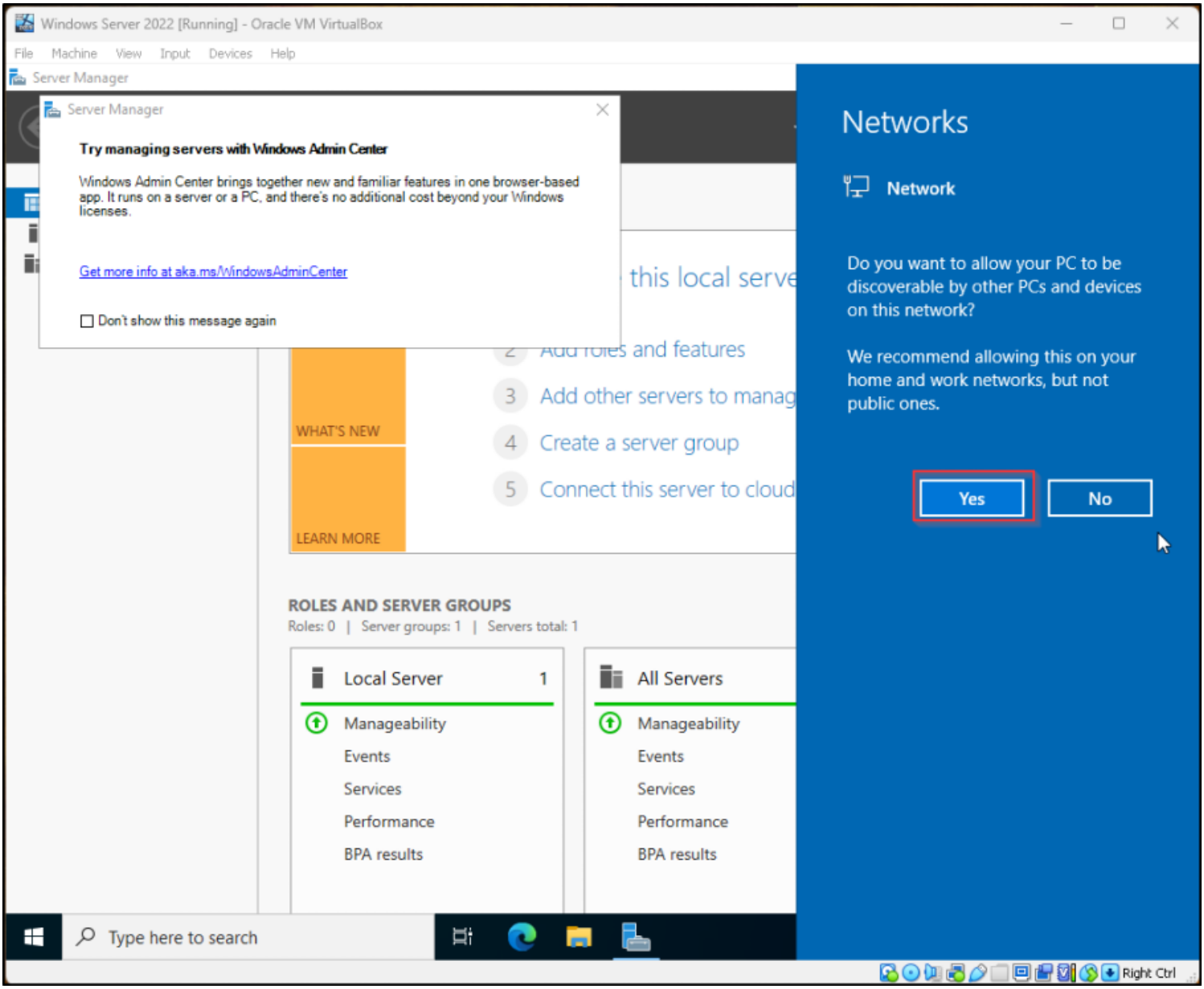


Installation Completed

In the top-left corner, I clicked on **Input**, then selected **Keyboard**, and chose **Insert Ctrl+Alt+Delete**.
Next, I entered my **Administrative Password** and pressed **Enter**.



The installation of Windows Server 2022 has been completed.
A window popped up asking whether to allow other devices on the same network to discover my server. I clicked **Yes** because I want my Windows clients to be able to find my server.

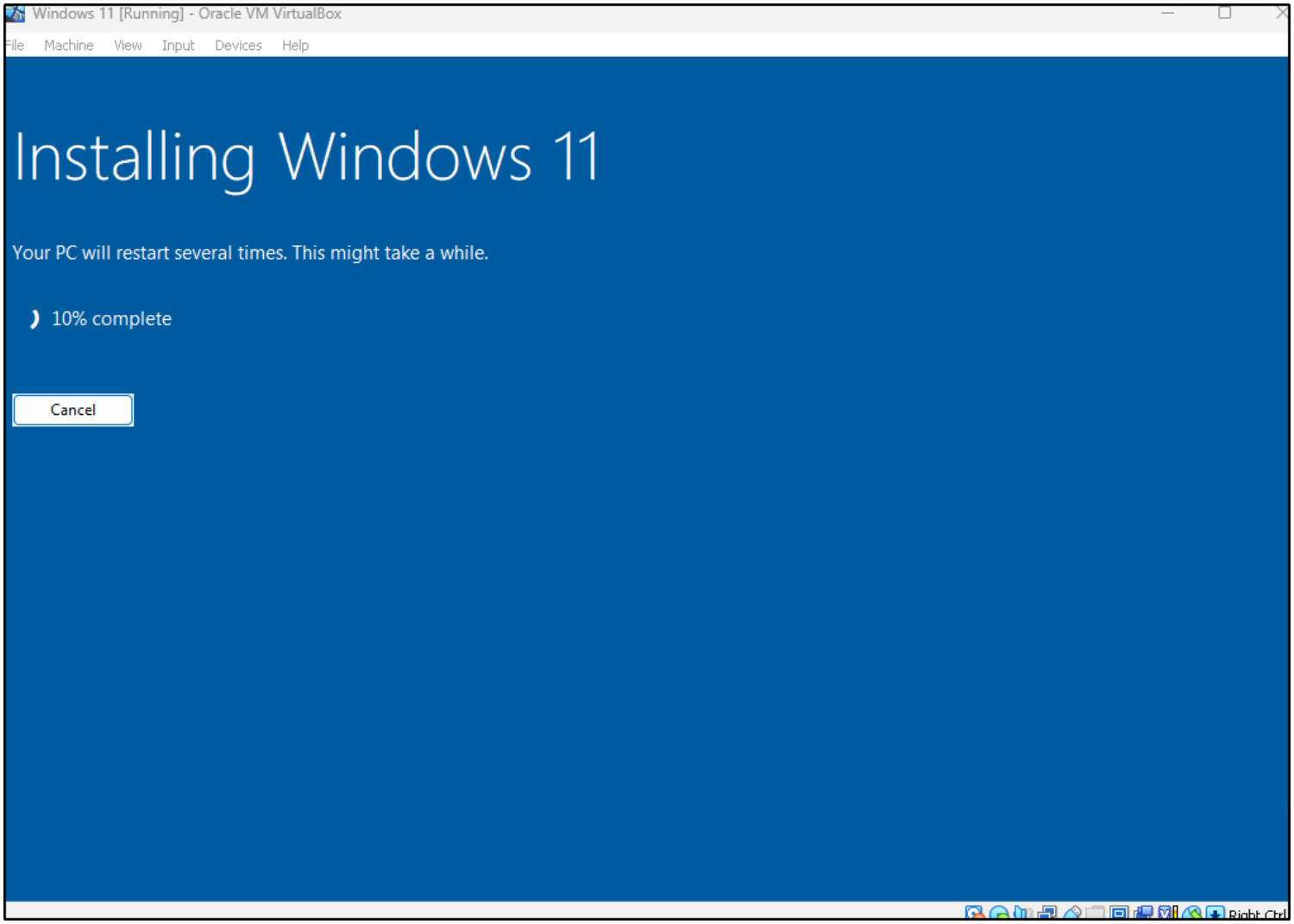


Installation and Configuration of Windows 10 Client

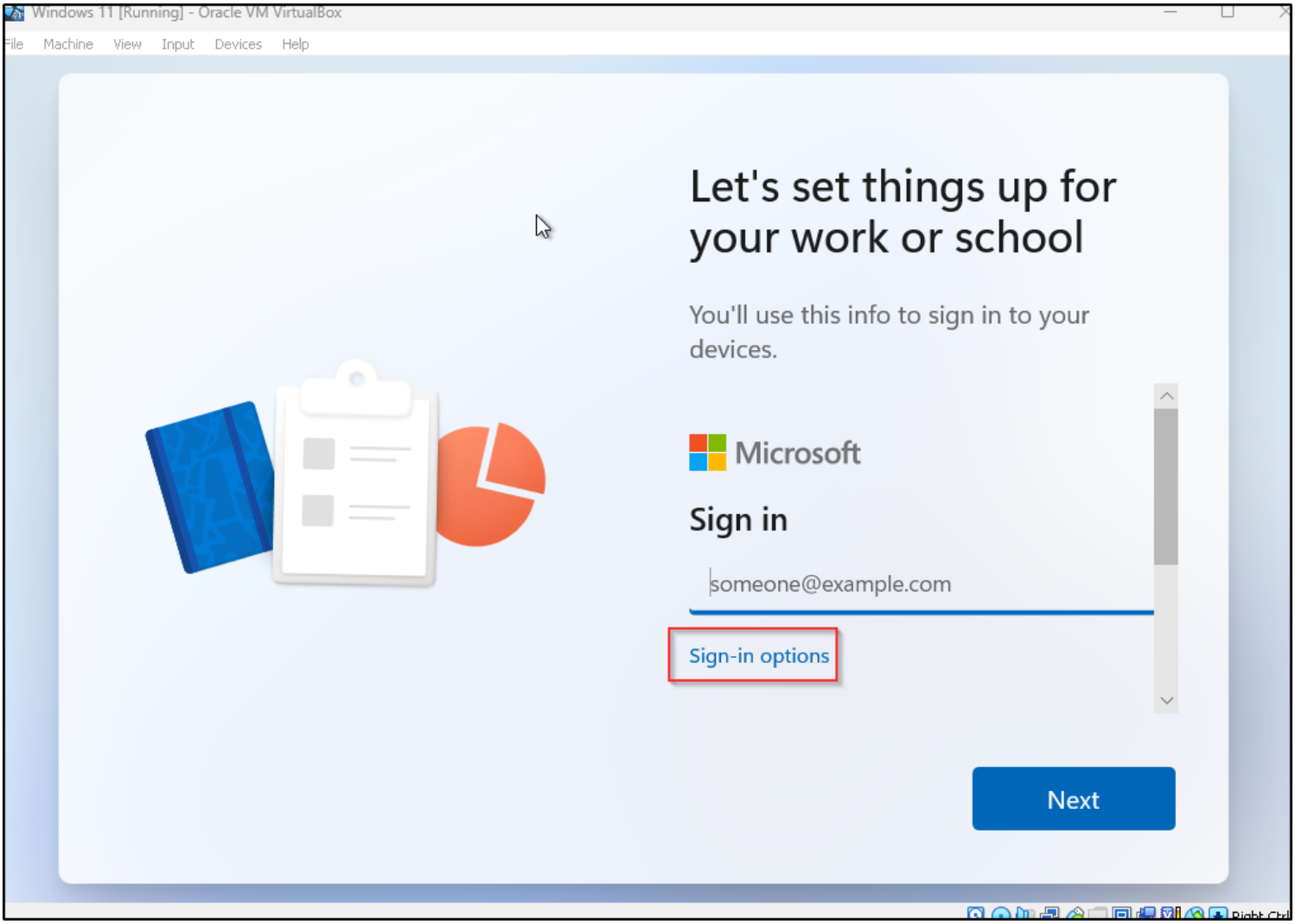
The configuration and network settings for the Windows 10 client are the same as those used for the Windows Server 2022 VM, and the installation process for the operating system is also similar. Therefore, I followed the same steps.

I named the VM **"Windows 11,"** allocated **4 GB** of RAM, set the disk size to **70 GB**, and configured the network adapter to **NAT Networking**.

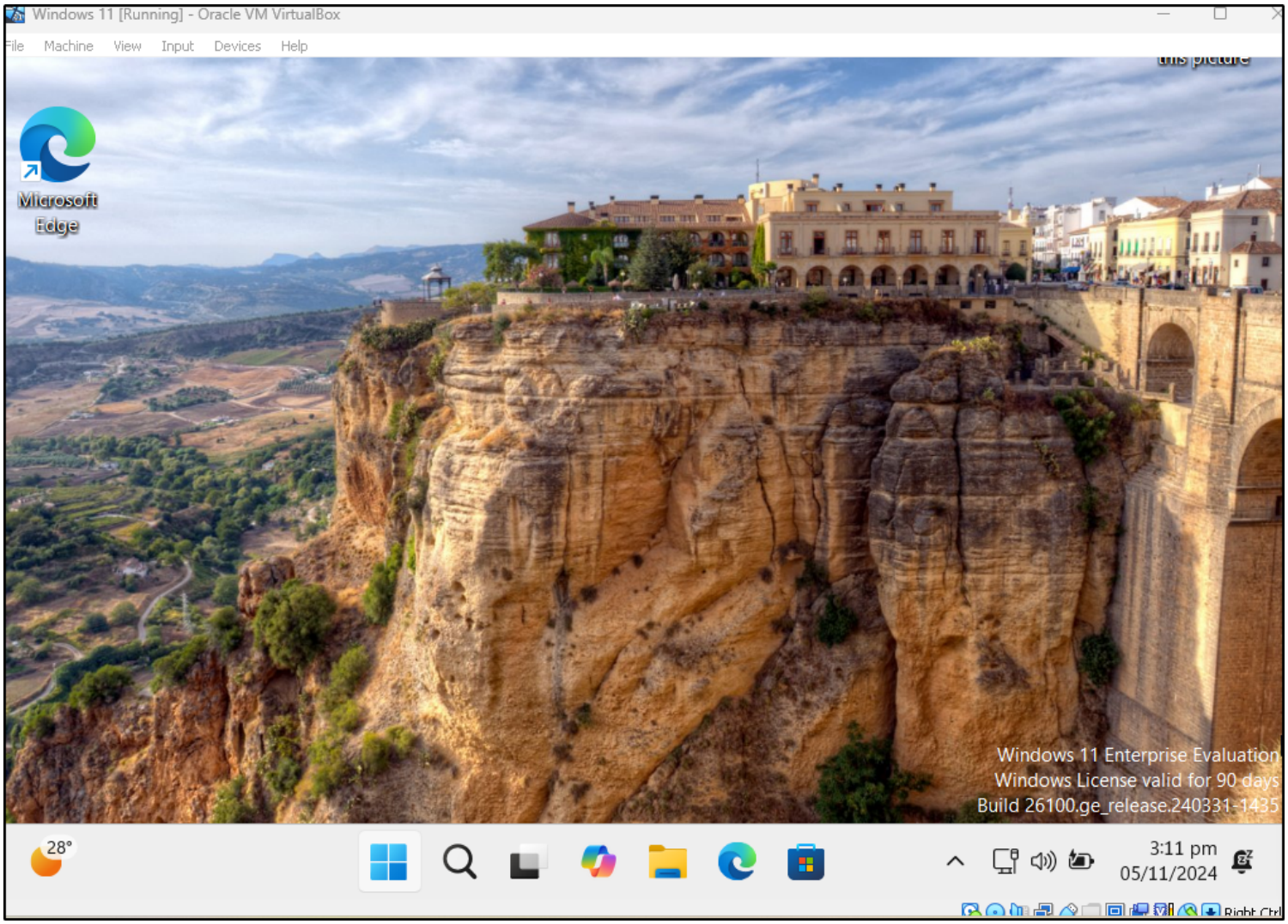
I continued following the same steps until the installation process began. During the installation, I left all settings at their default values.



After the installation was completed, the system restarted twice.
I set the region to my country, selected **US** as the keyboard layout, and continued.
I clicked on **Sign-in options** and chose **Domain Join Instead**.
I set the account name to **"User"** since I will be creating multiple accounts on the domain.

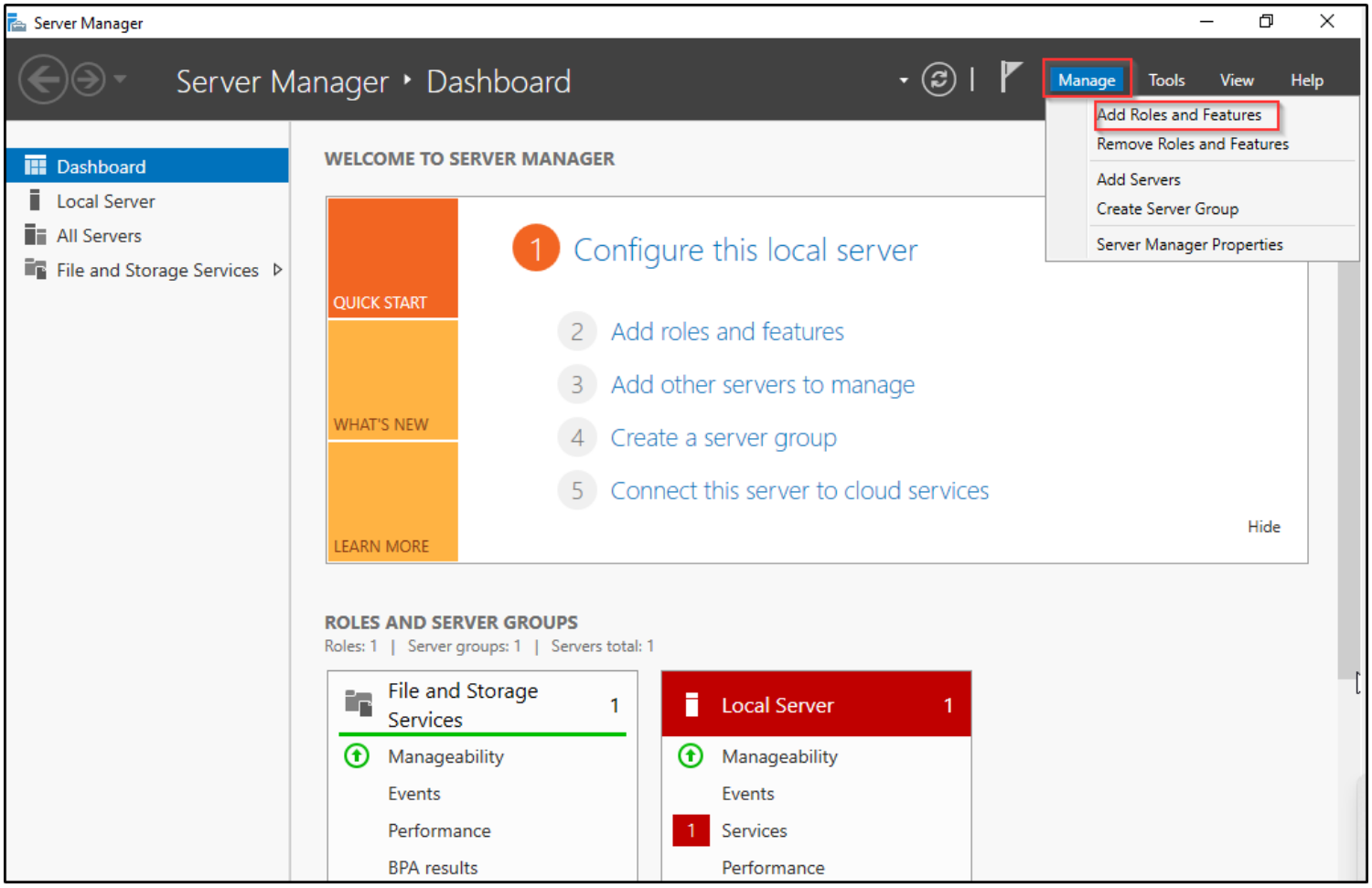


I clicked **Next** and accepted the license terms.
The installation was then completed.

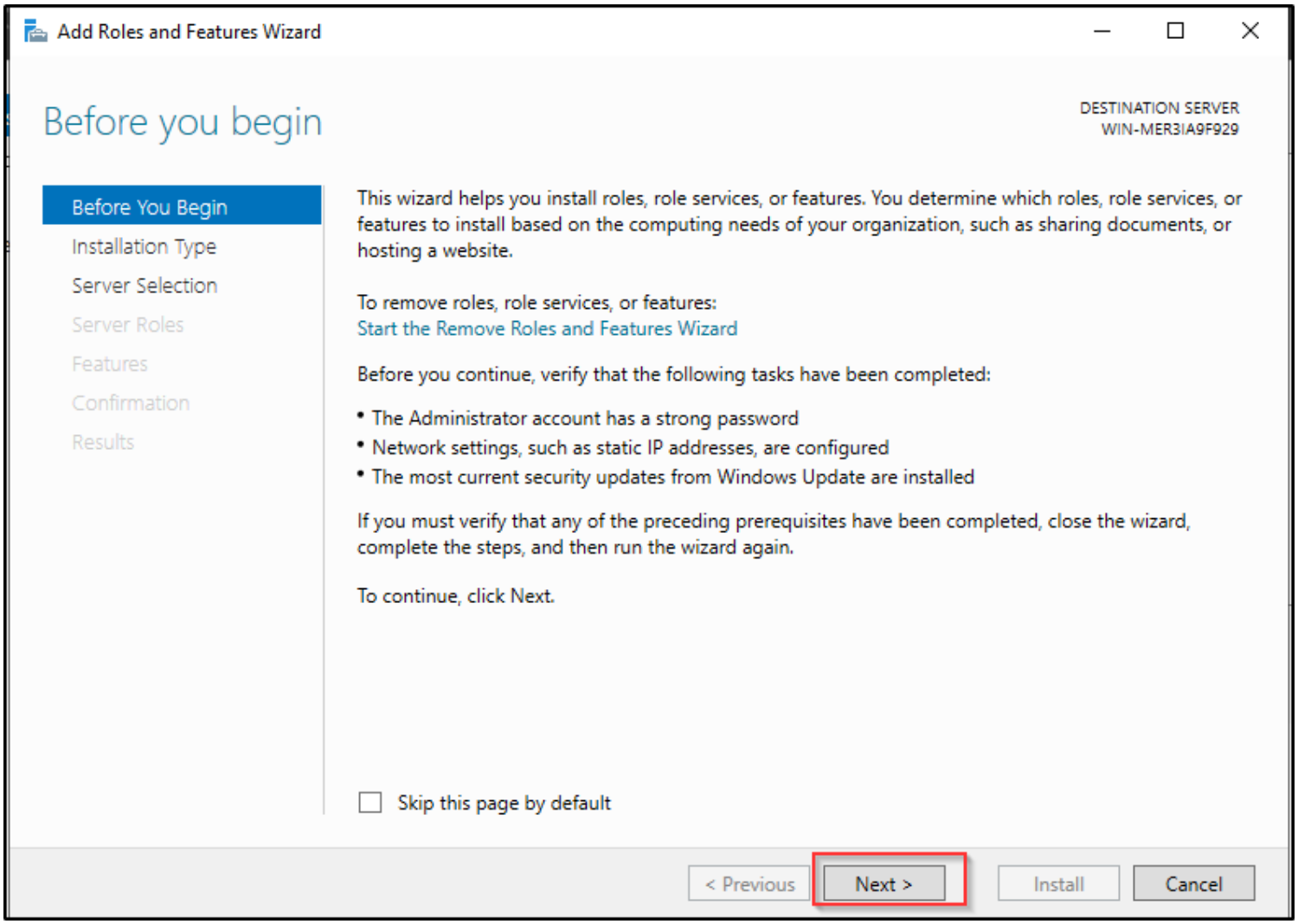

Windows 11 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Microsoft Edge
Windows 11 Enterprise Evaluation
Windows License valid for 90 days
Build 26100.ge_release.240331-1435
28°
3:11 pm
05/11/2024

Active Directory Setup

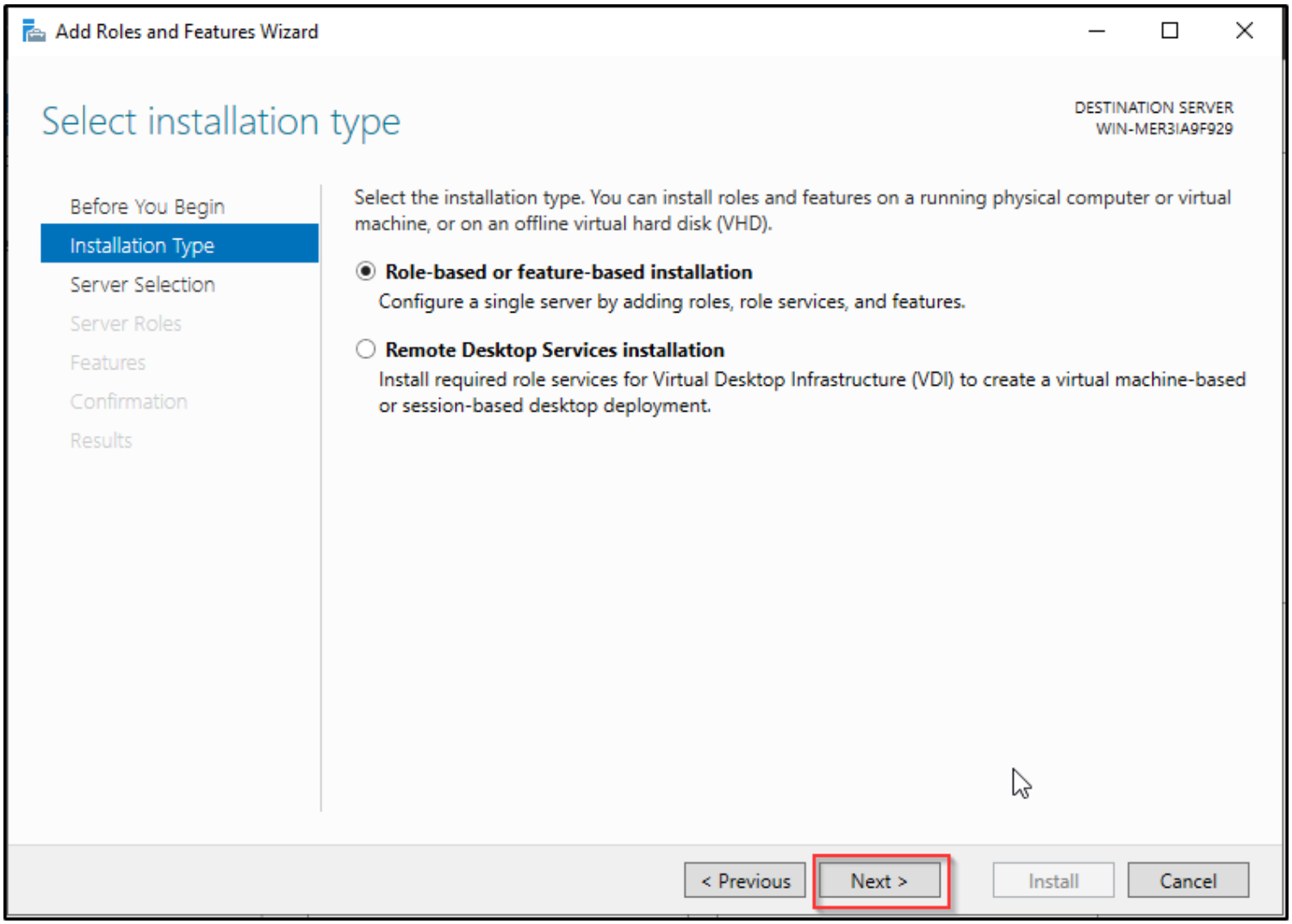
Active Directory Roles and Features Installation
To install the Active Directory Roles and Features, I used the **Server Manager Dashboard**.
1. In the top-left corner of the Dashboard, I clicked **Manage**.
2. Then, I selected **Add Roles and Features**



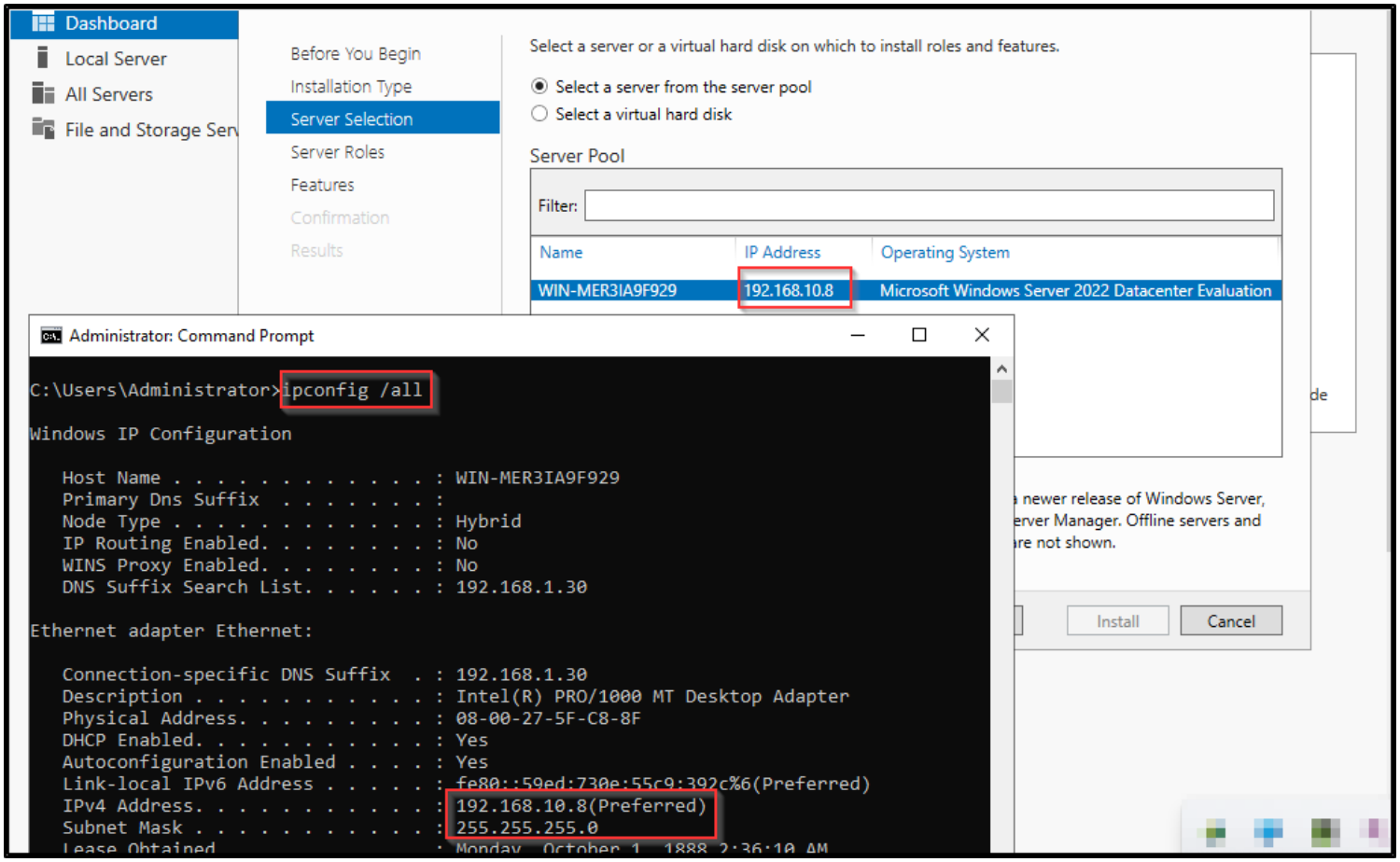
I left all settings as default and clicked **Next**.



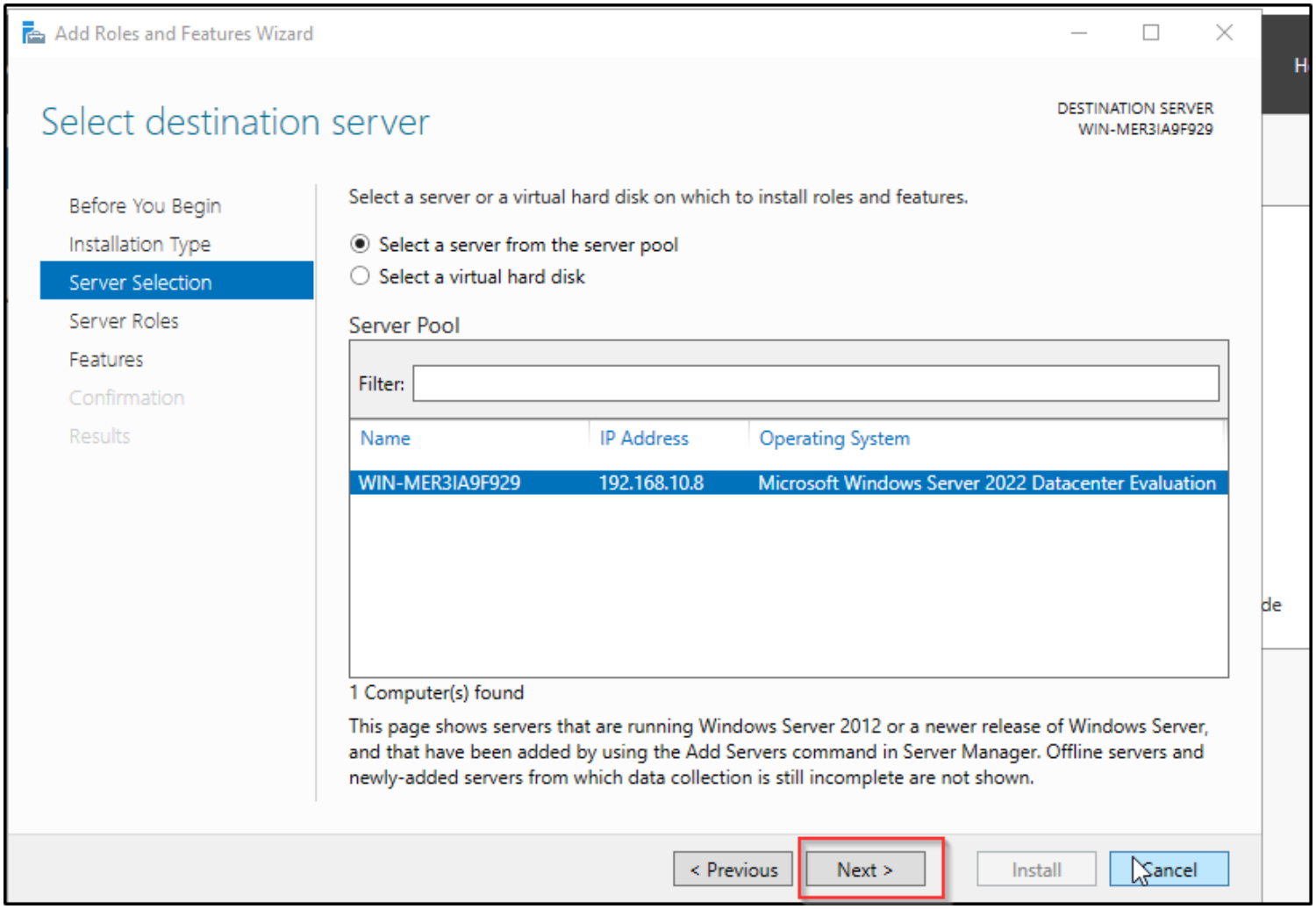
By default, **Role-based or feature-based installation** was selected, so I simply clicked **Next**.



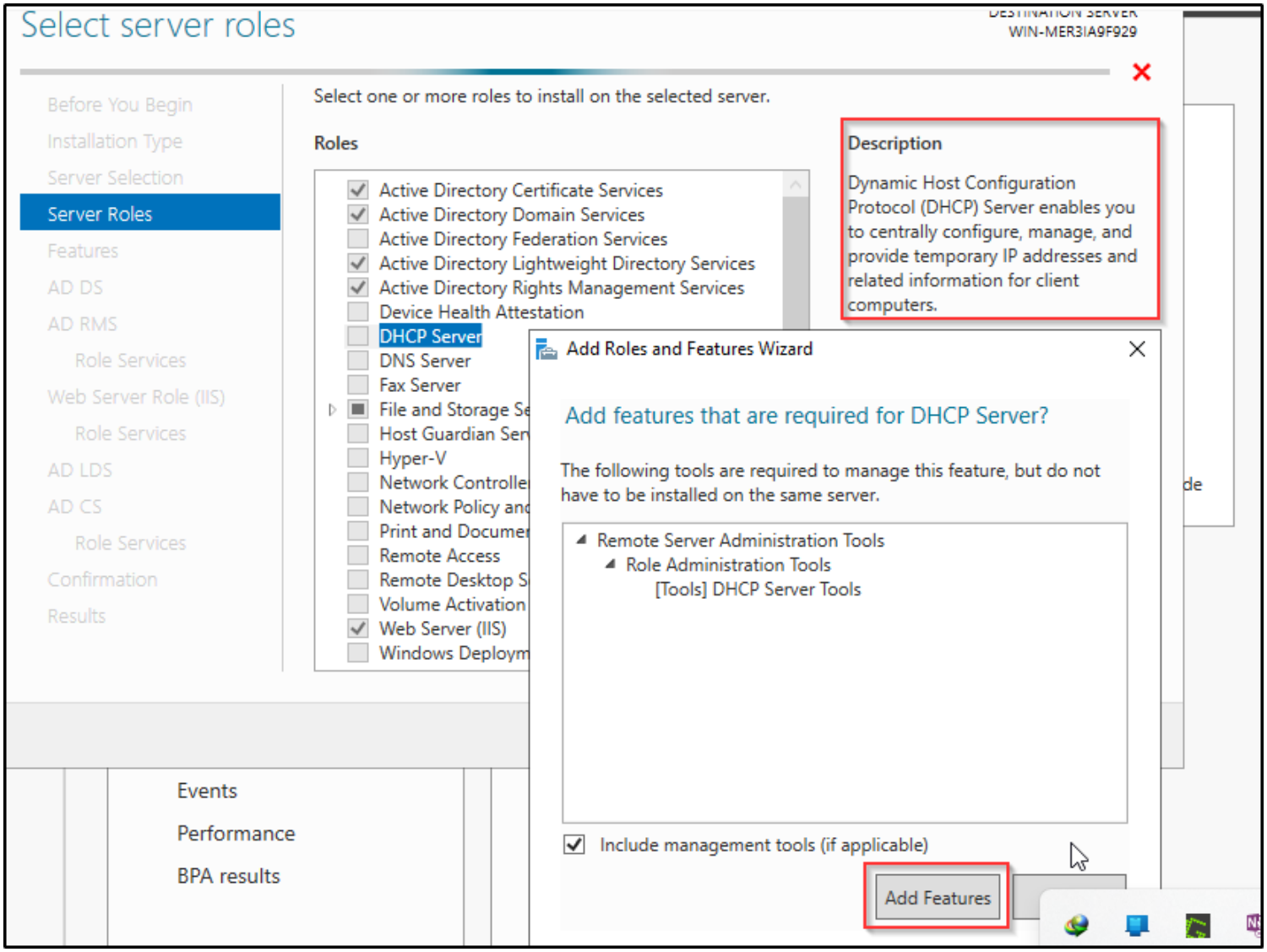
Here, my server's IP address is shown as **192.168.10.8/24**. I opened **Command Prompt (CMD)** and used the command `ipconfig /all` to verify the IP address and subnet.



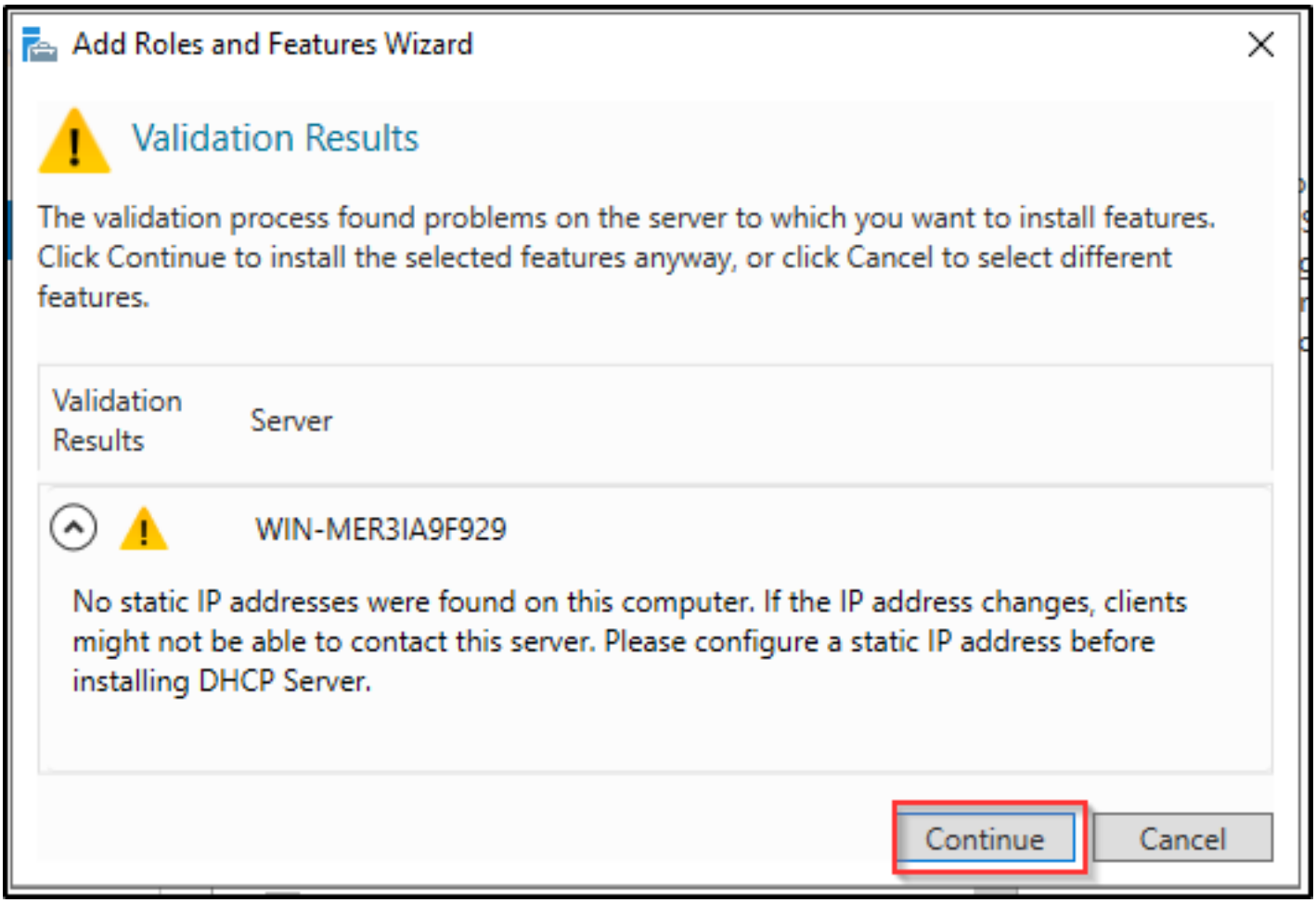
After confirming the IP address, I clicked **Next** with the default settings.



I selected the necessary roles for this project. For each role I considered, I reviewed the **Description** section to better understand its purpose. When I clicked on a role, a pop-up window appeared prompting me to add the required features for that role, so I selected **Add Features**.

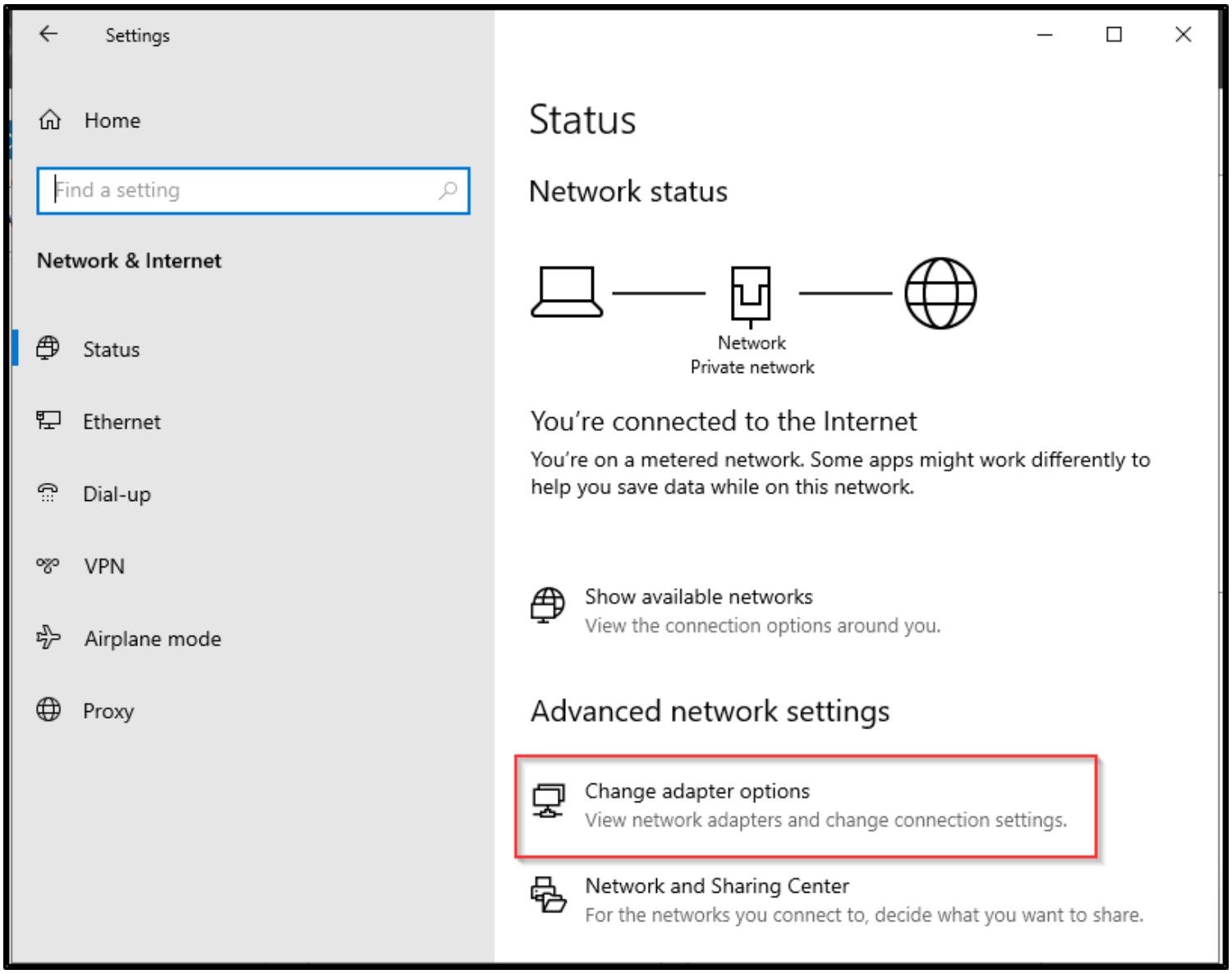


When I attempted to add the **DHCP Server Features**, a warning window popped up, indicating that no static IP address was set for the server. To resolve this, I canceled the process and updated my IP configuration to a static IP.

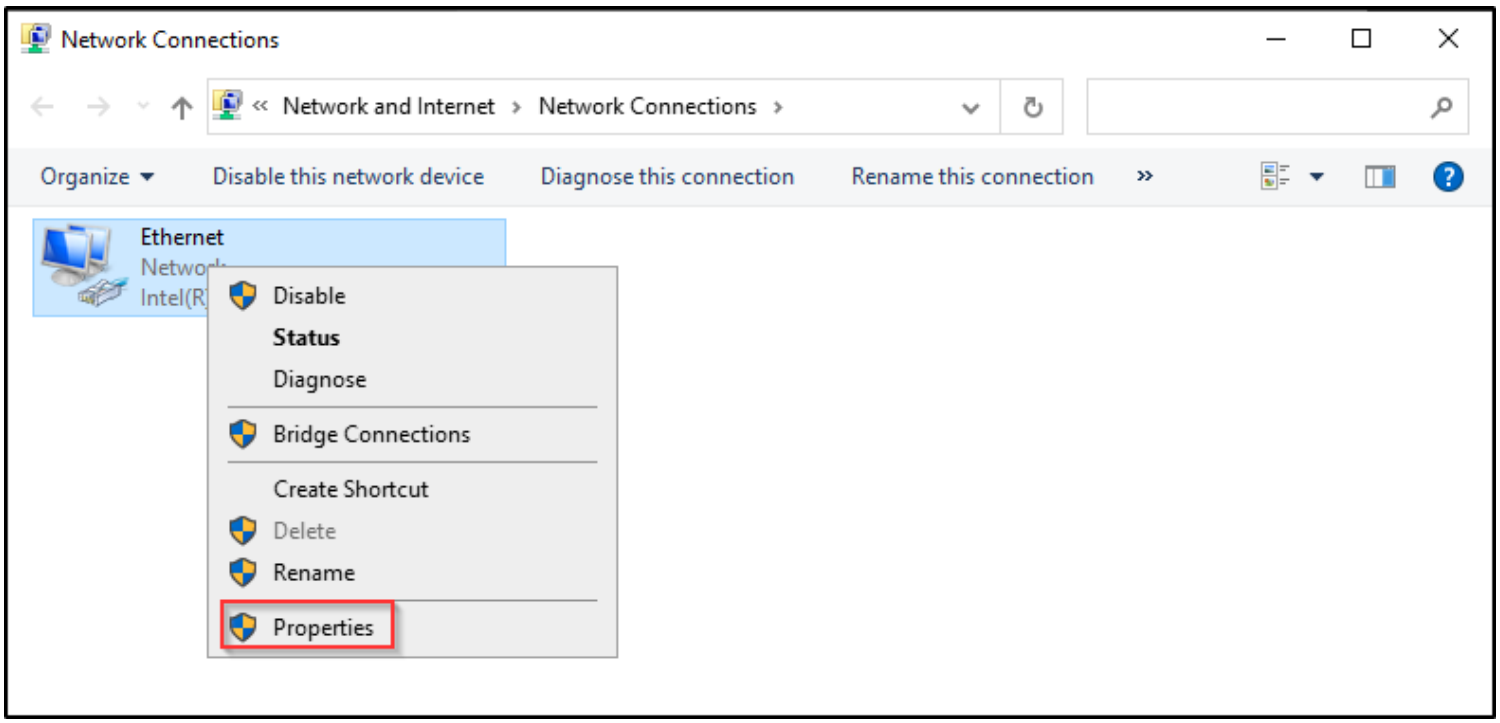


Changing IP Configuration to a Static IP

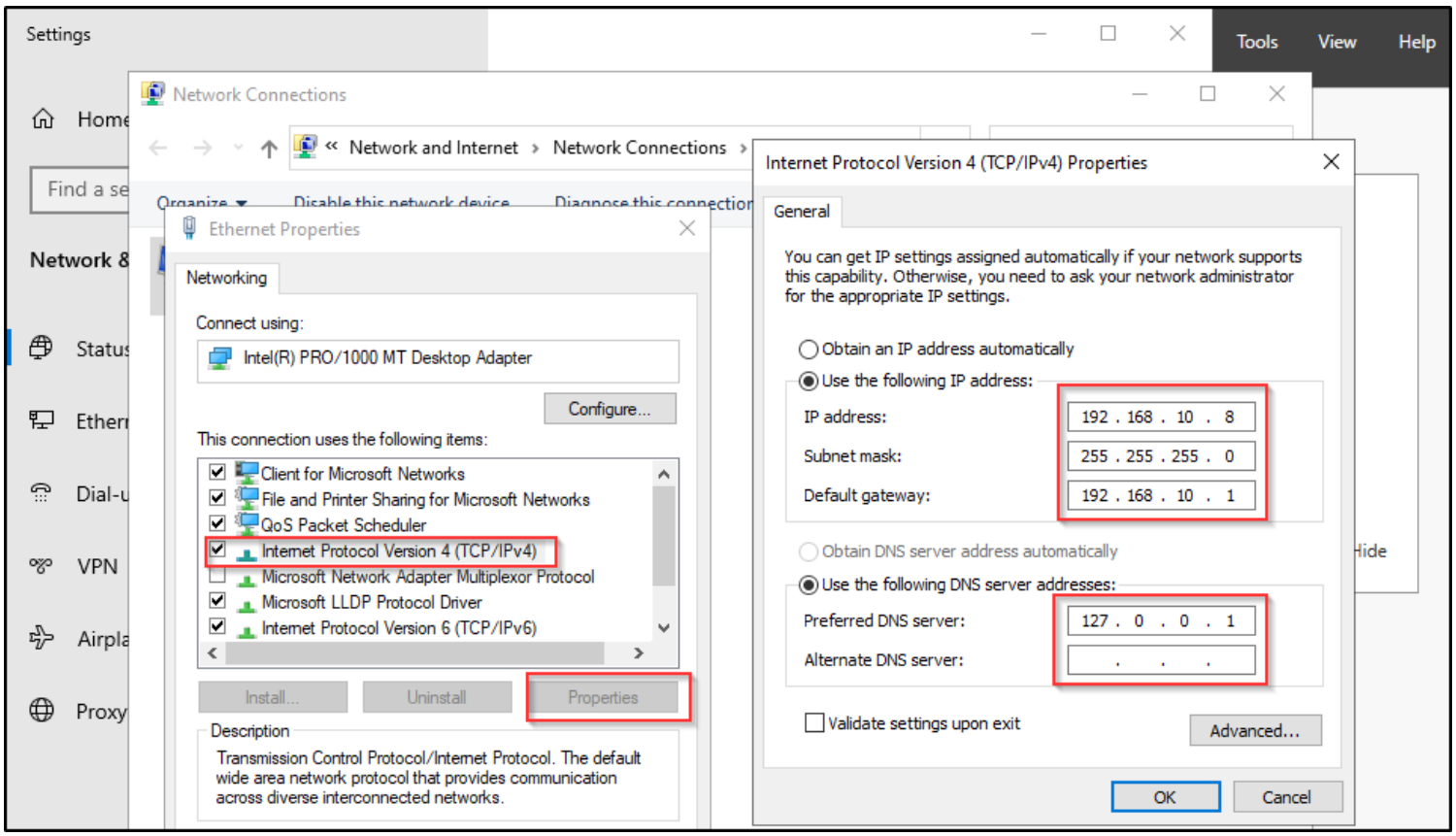
1. I opened **Settings** by searching for it in the Windows search bar.
2. Then, I clicked on **Change adapter options**.



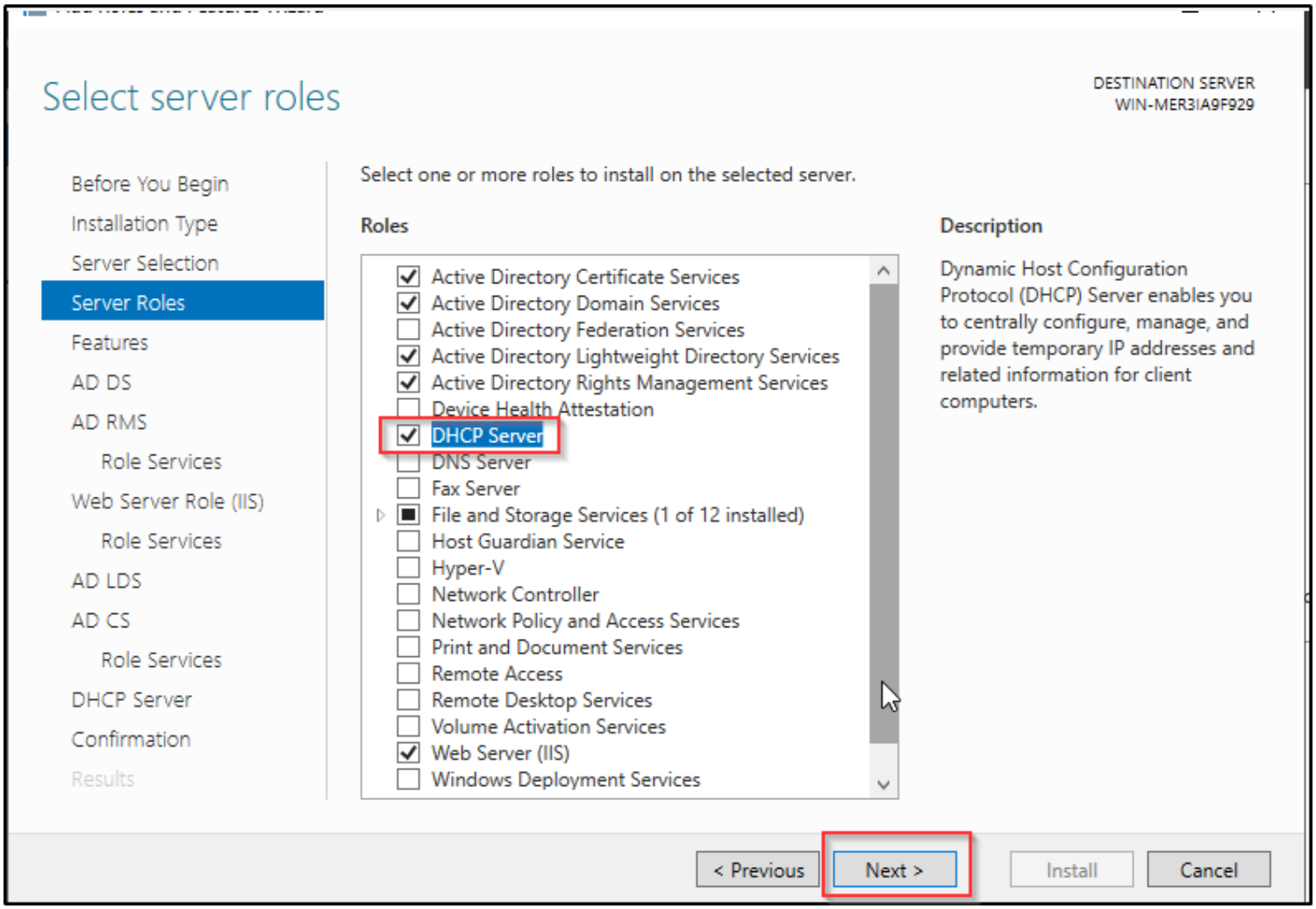
I right-clicked on **Ethernet** and selected **Properties**.



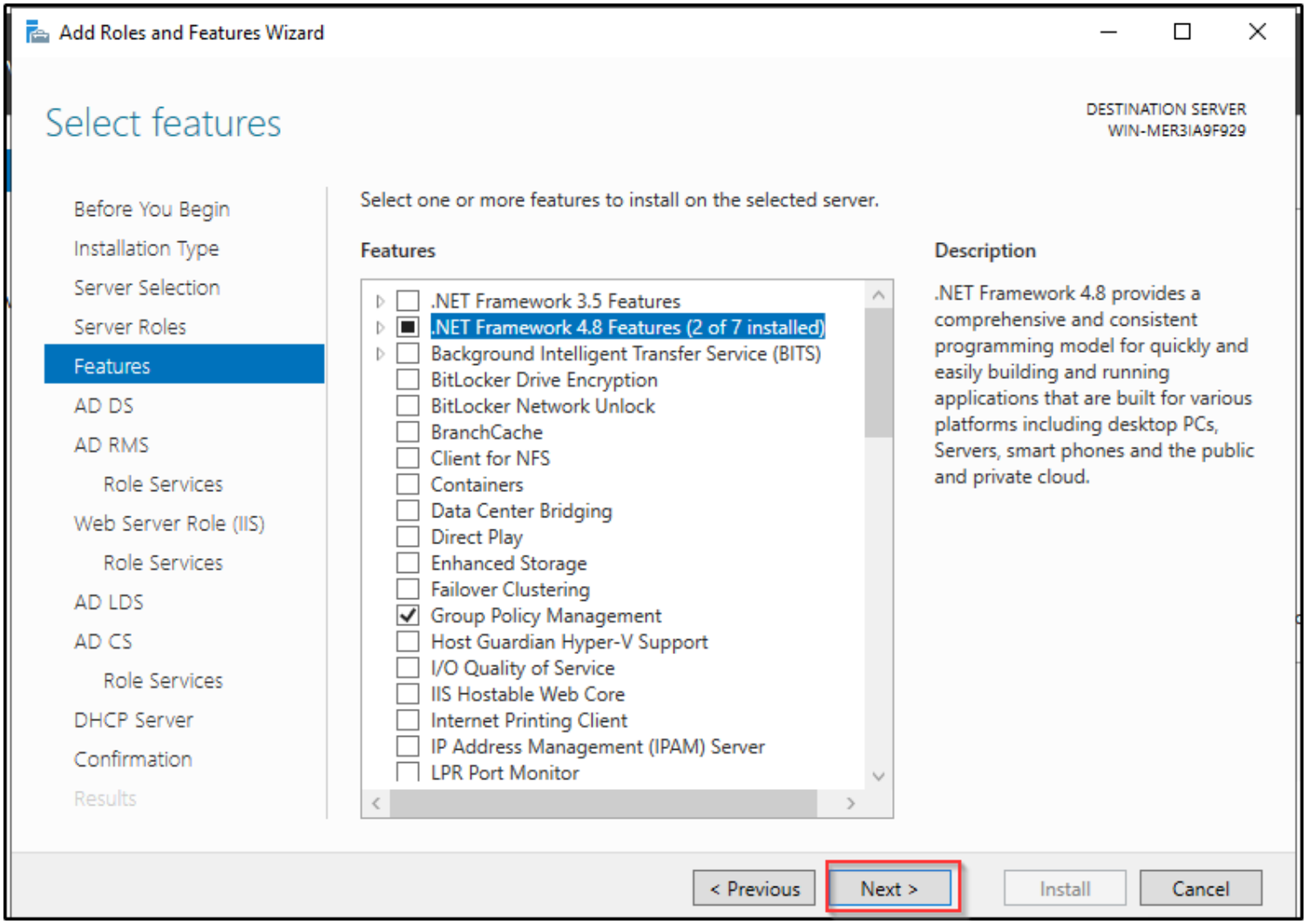
I clicked on **Internet Protocol Version 4 (TCP/IPv4)** and then selected **Properties**.
In the new window, I chose **Use the following IP address** and entered the static IP for my server.
Finally, I clicked **OK** and **Close** to apply the changes.



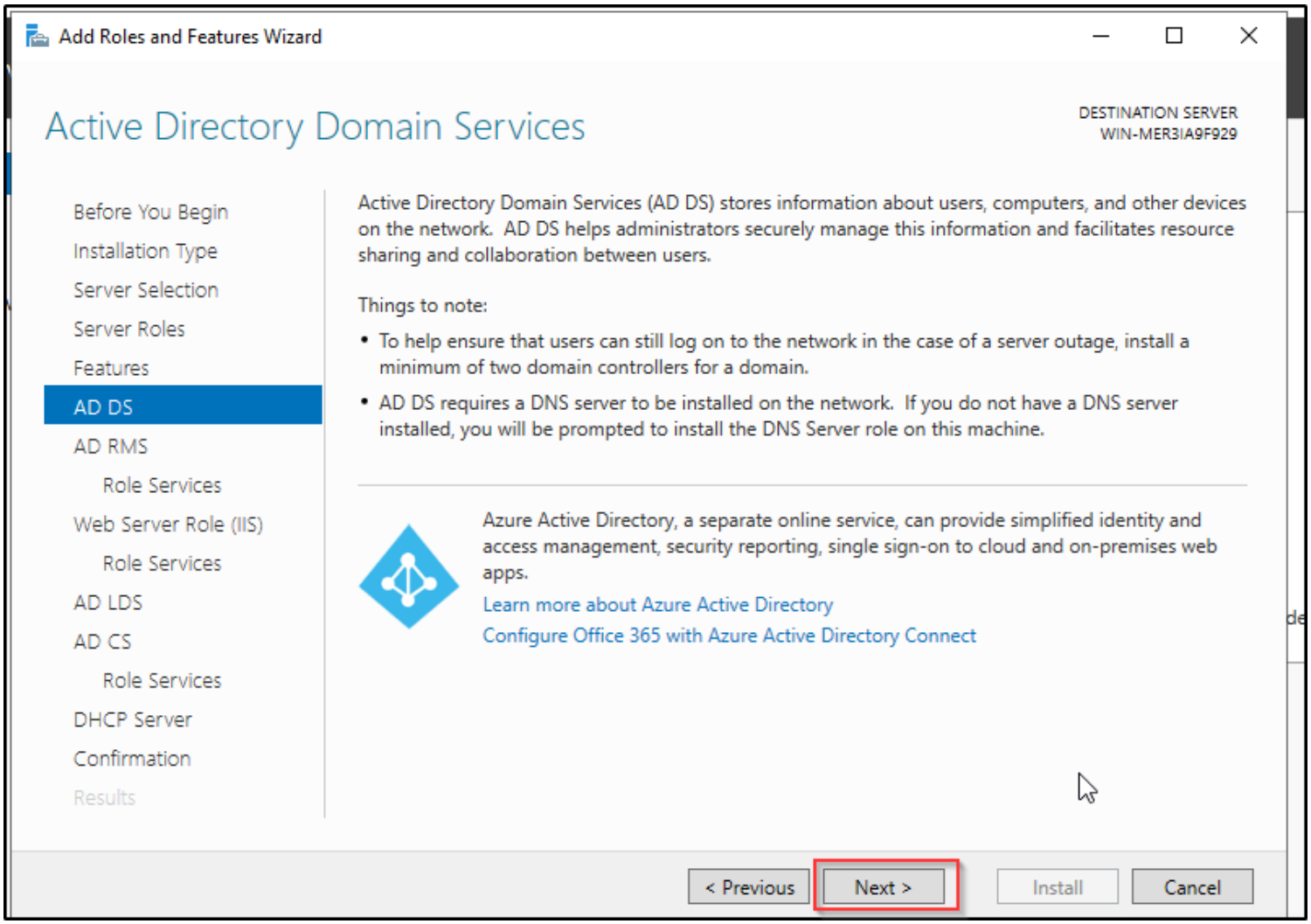
I returned to the **Select Server Roles** page, clicked on **DHCP Server**, and then selected **Add Features**.
After the features were successfully added, I clicked **Next** to continue.



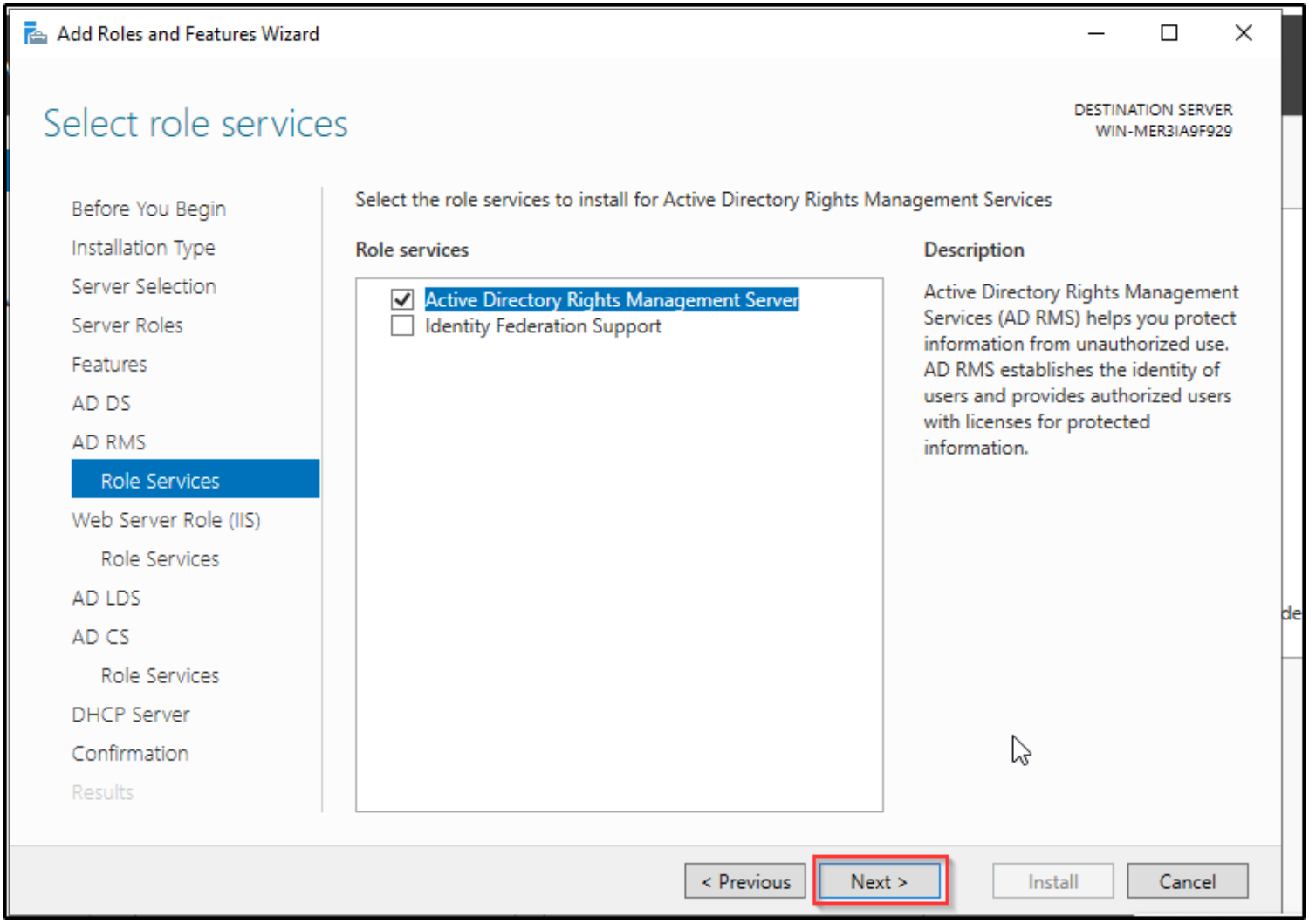
I left all other settings as default and clicked **Next** to proceed.



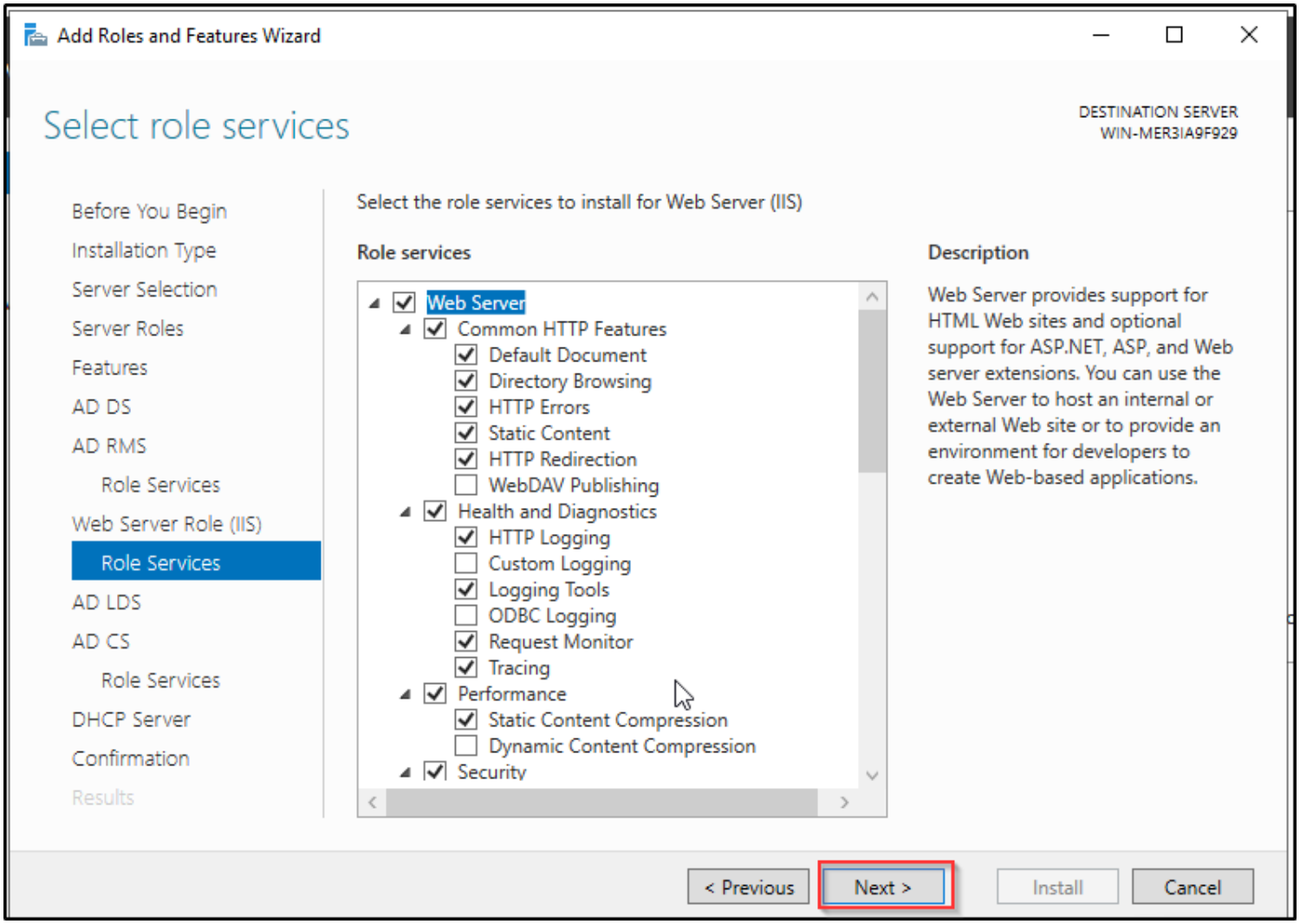
I clicked **Next** and then clicked **Next** again to continue.



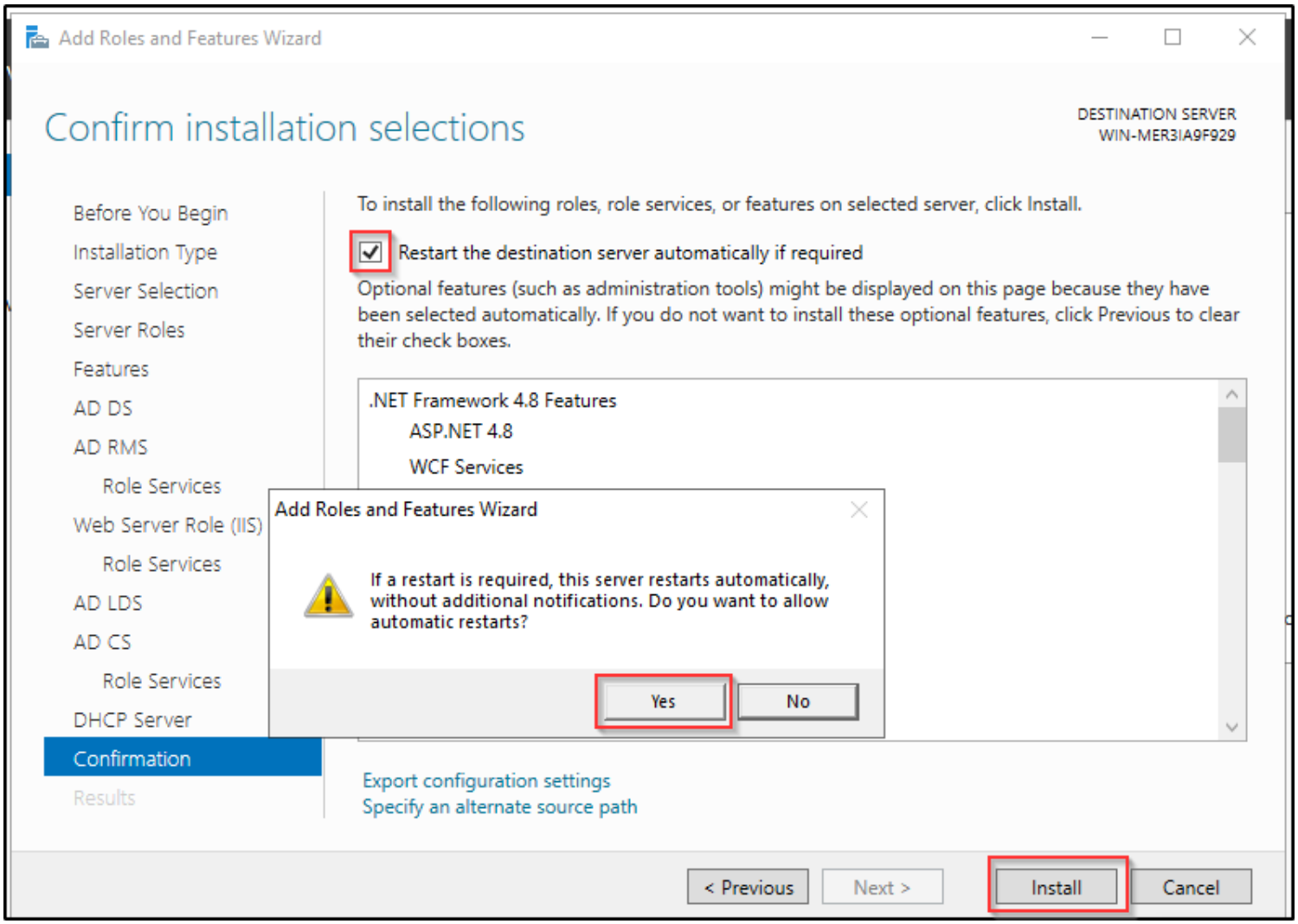
I clicked **Next** and then clicked **Next** again to continue.



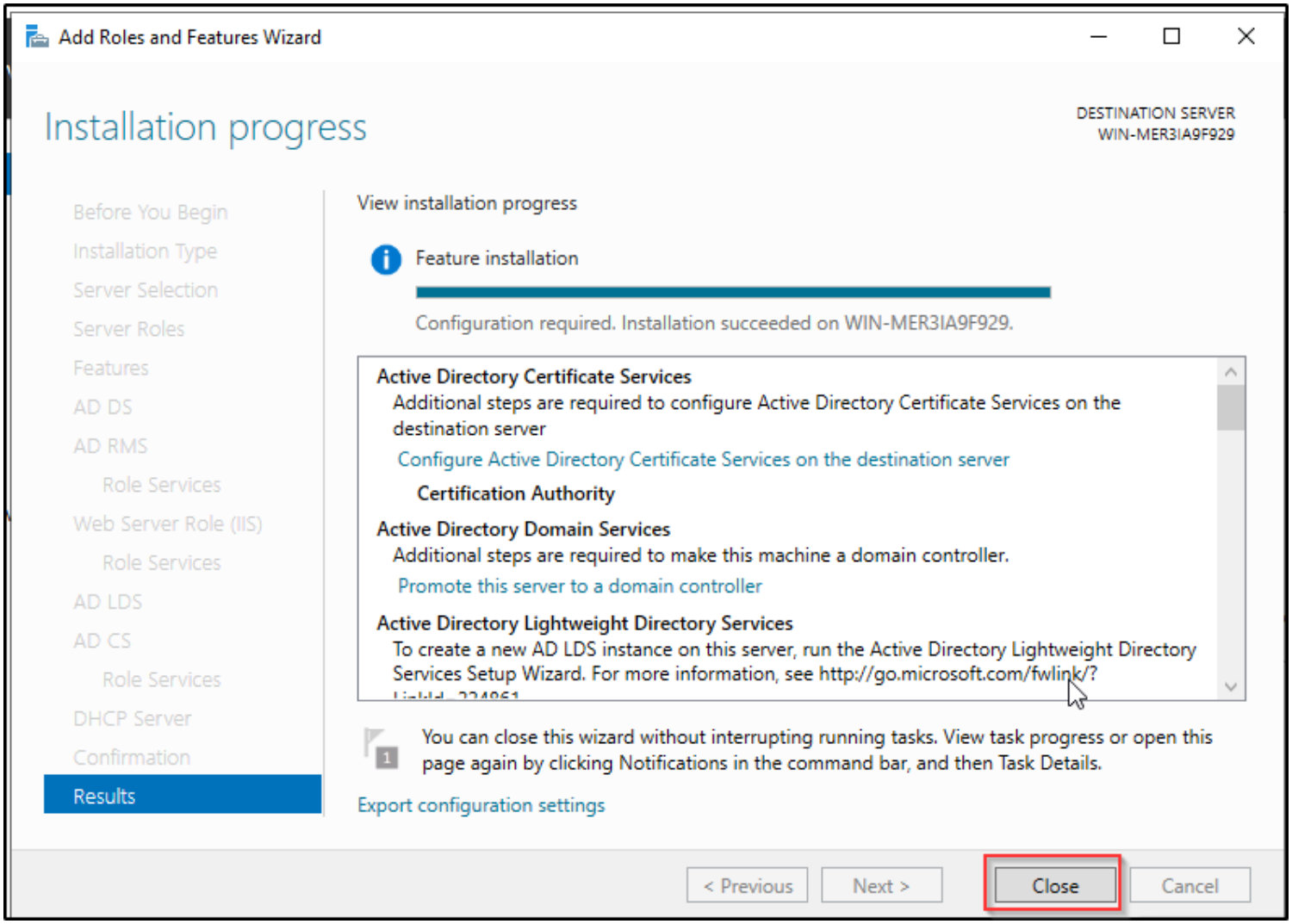
I confirmed all the selected roles and clicked **Next**, then clicked **Next** again, and finally clicked **Next** to proceed.



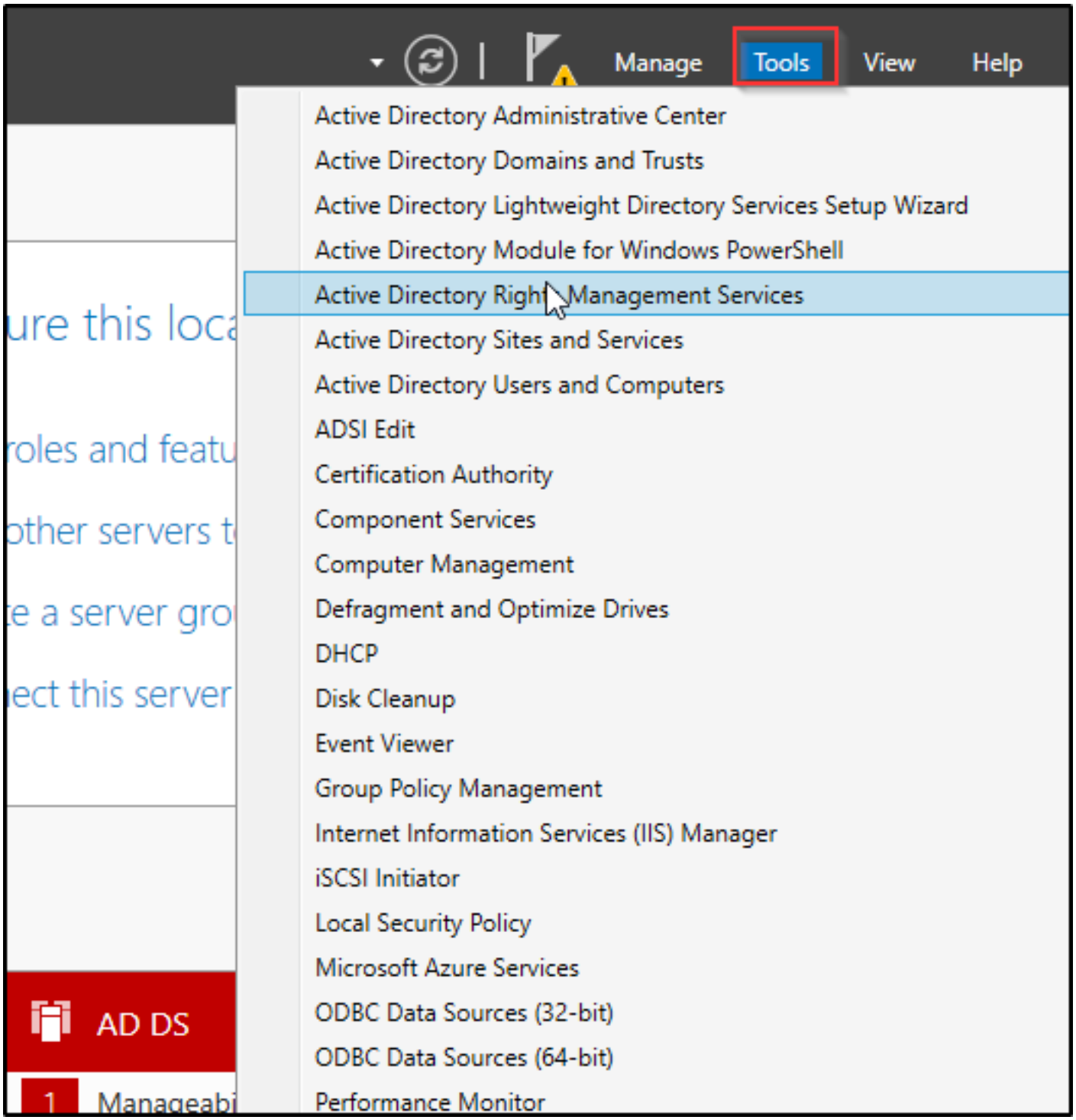
I selected **Automatic restart** and confirmed by clicking **Yes**, then clicked **Install** to begin the installation process.



1. I waited for the installation process to complete and then clicked **Close**.

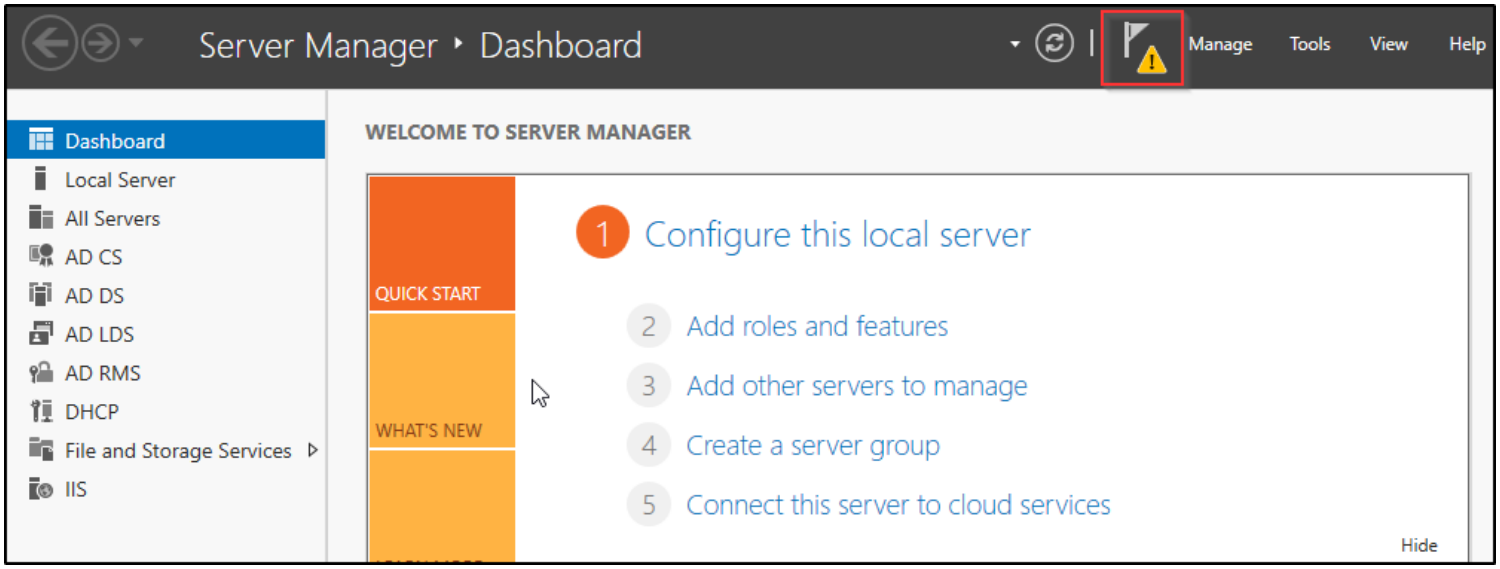


I clicked on **Tools** to verify that the tools were successfully installed, and then I restarted the server.

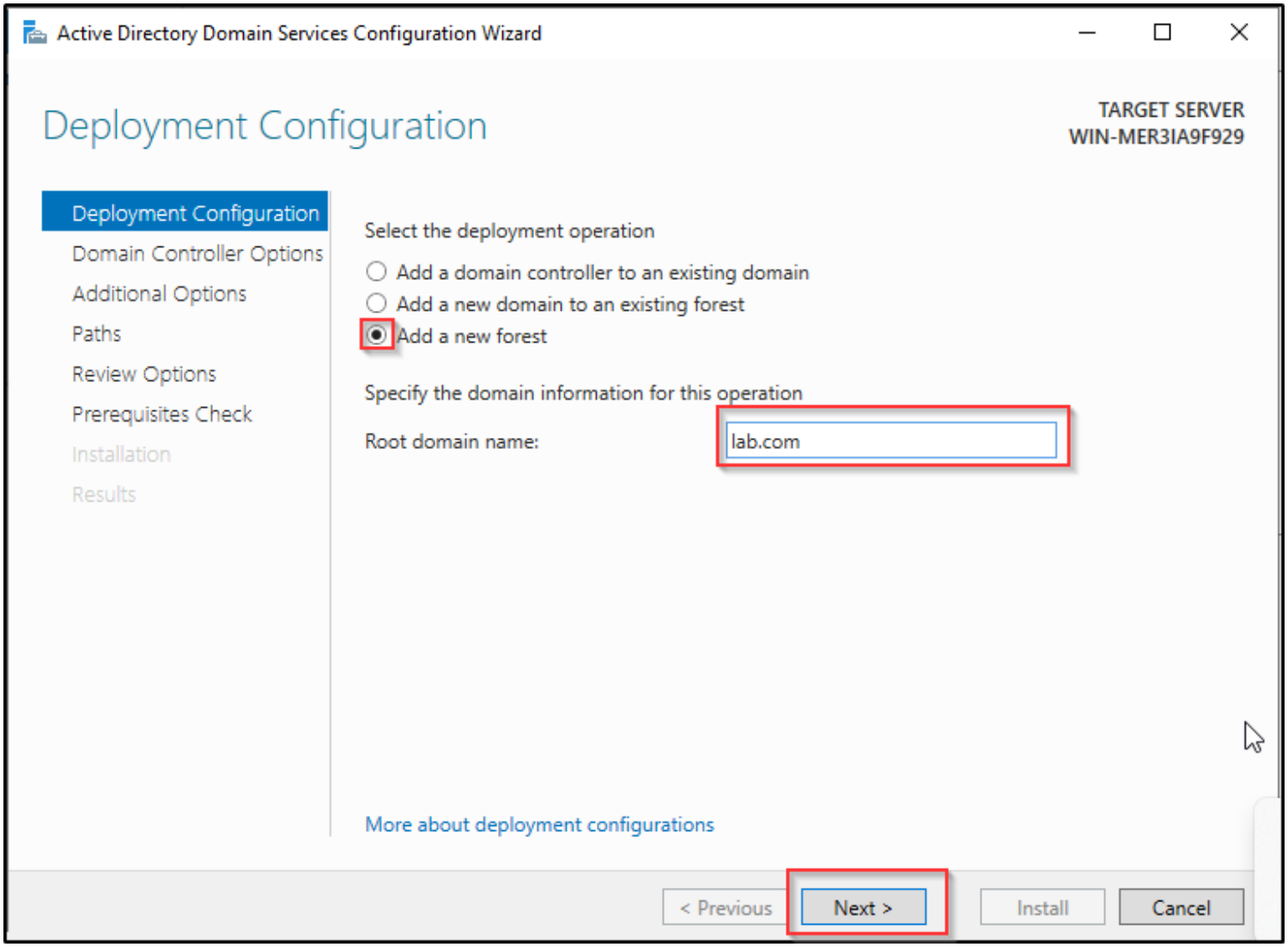

Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Lightweight Directory Services Setup Wizard
Active Directory Module for Windows PowerShell
Active Directory Rights Management Services
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Certification Authority
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
Disk Cleanup
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
AD DS

Domain Controller (DC) Configuration:

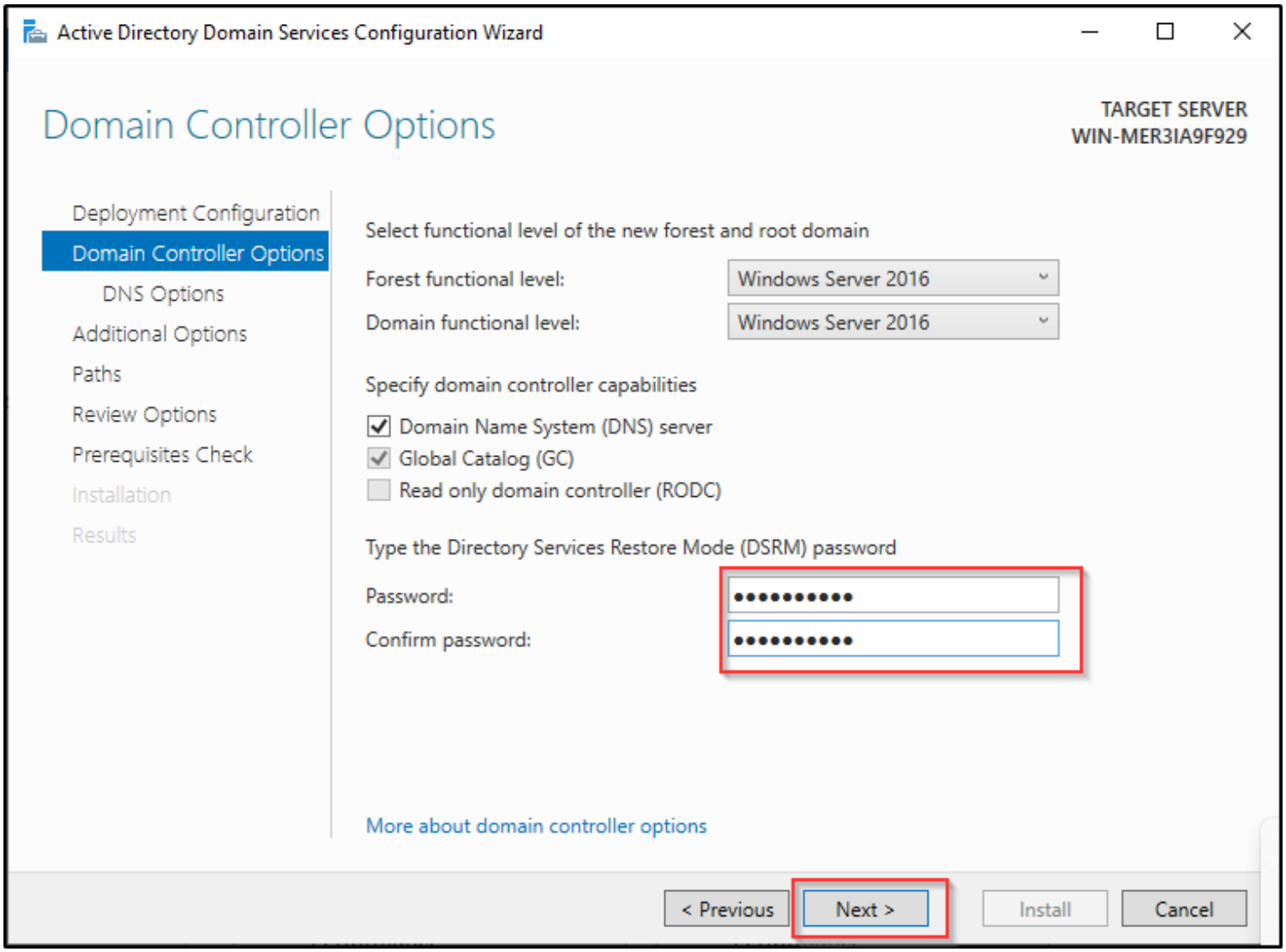
Domain Controller (DC) Configuration:
1. At the top of the **Server Manager** window, I clicked on the yellow error flag and selected **Promote this server to a Domain Controller**.



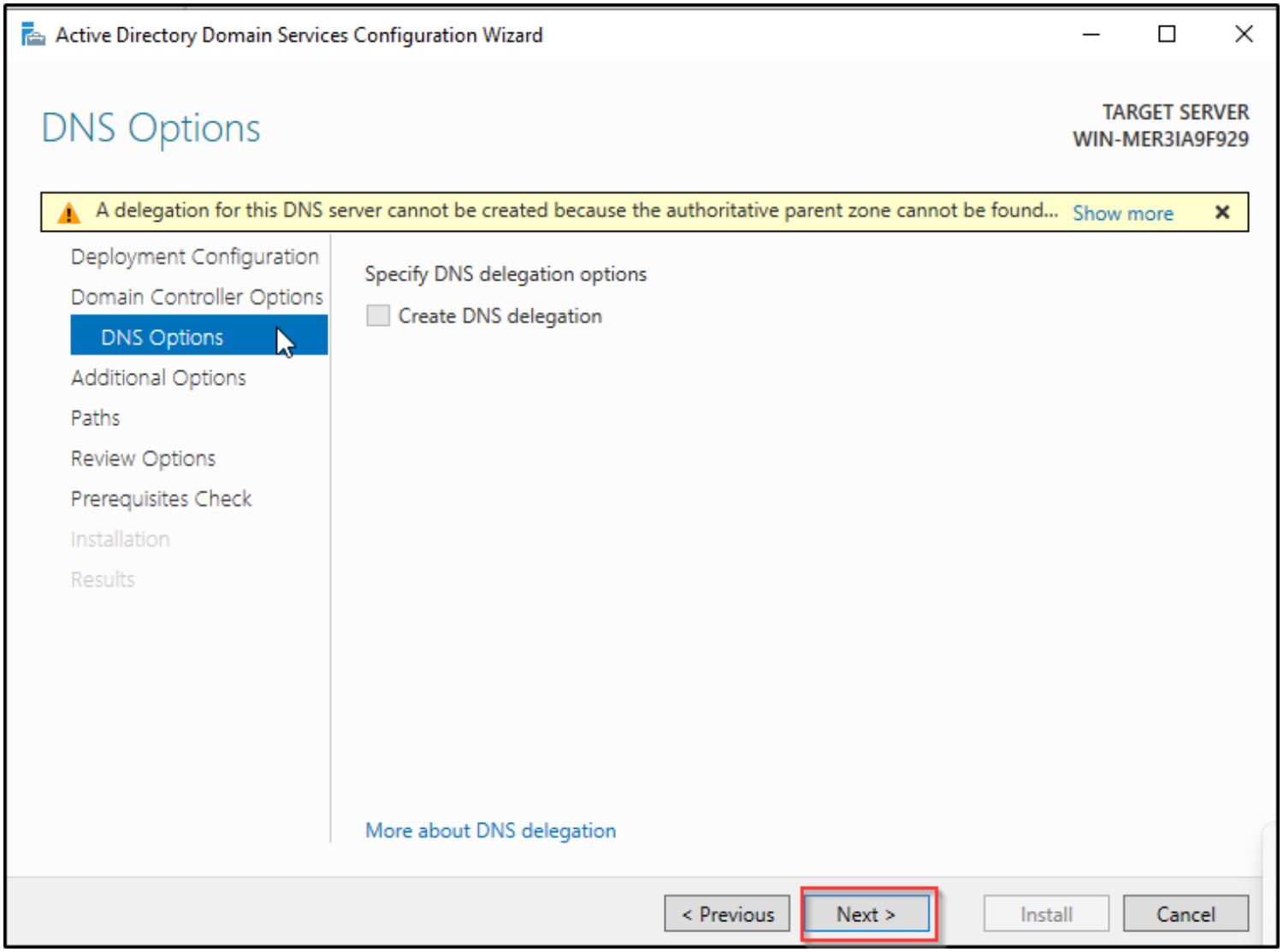
I selected **Add a new Forest** since this is a new Domain Controller setup.
I then entered the **Domain Name** as lab.com and clicked **Next**.



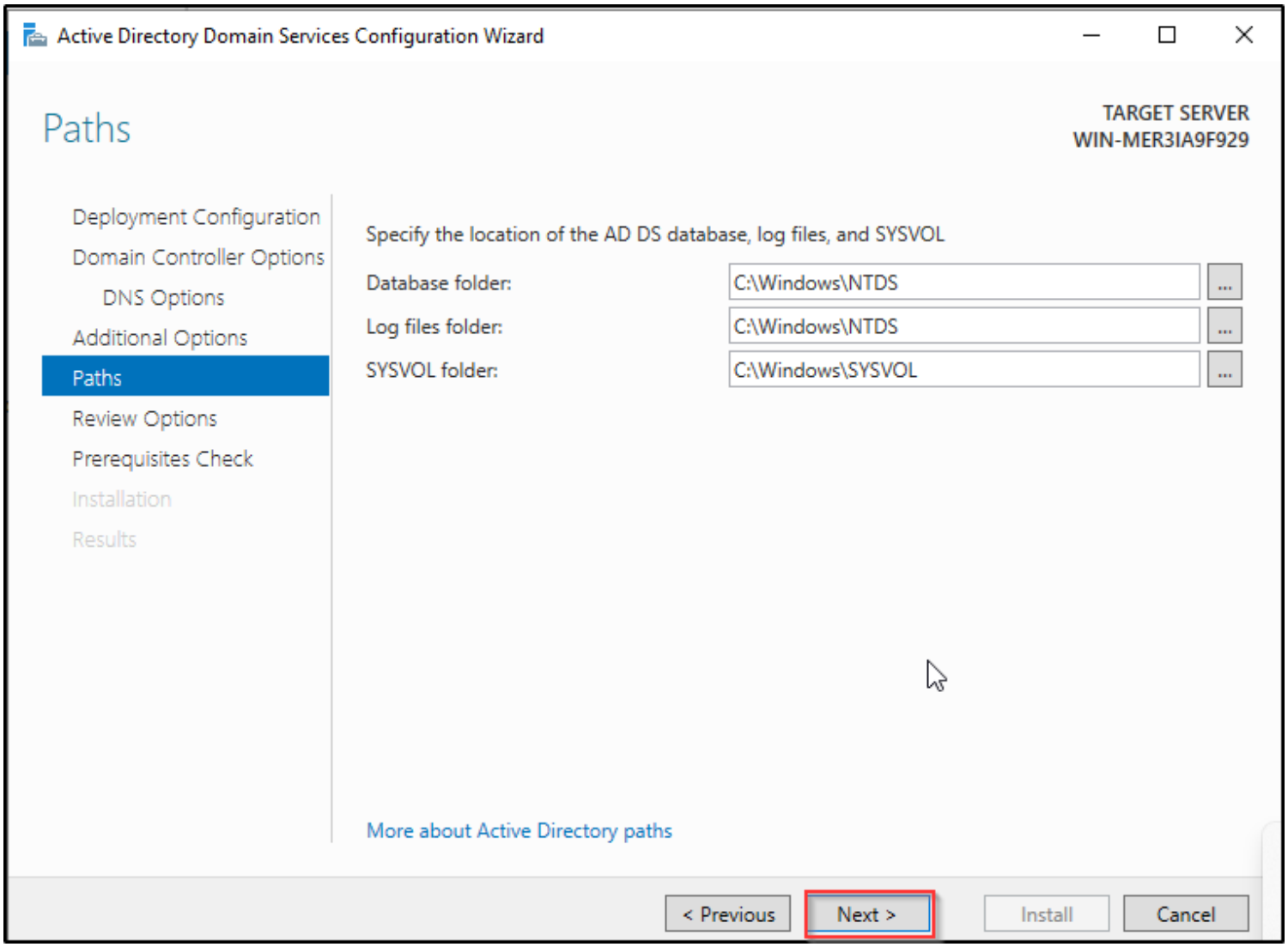
I entered the **Directory Services Restore Mode (DSRM) password** and left all other settings as default. I then clicked **Next**.



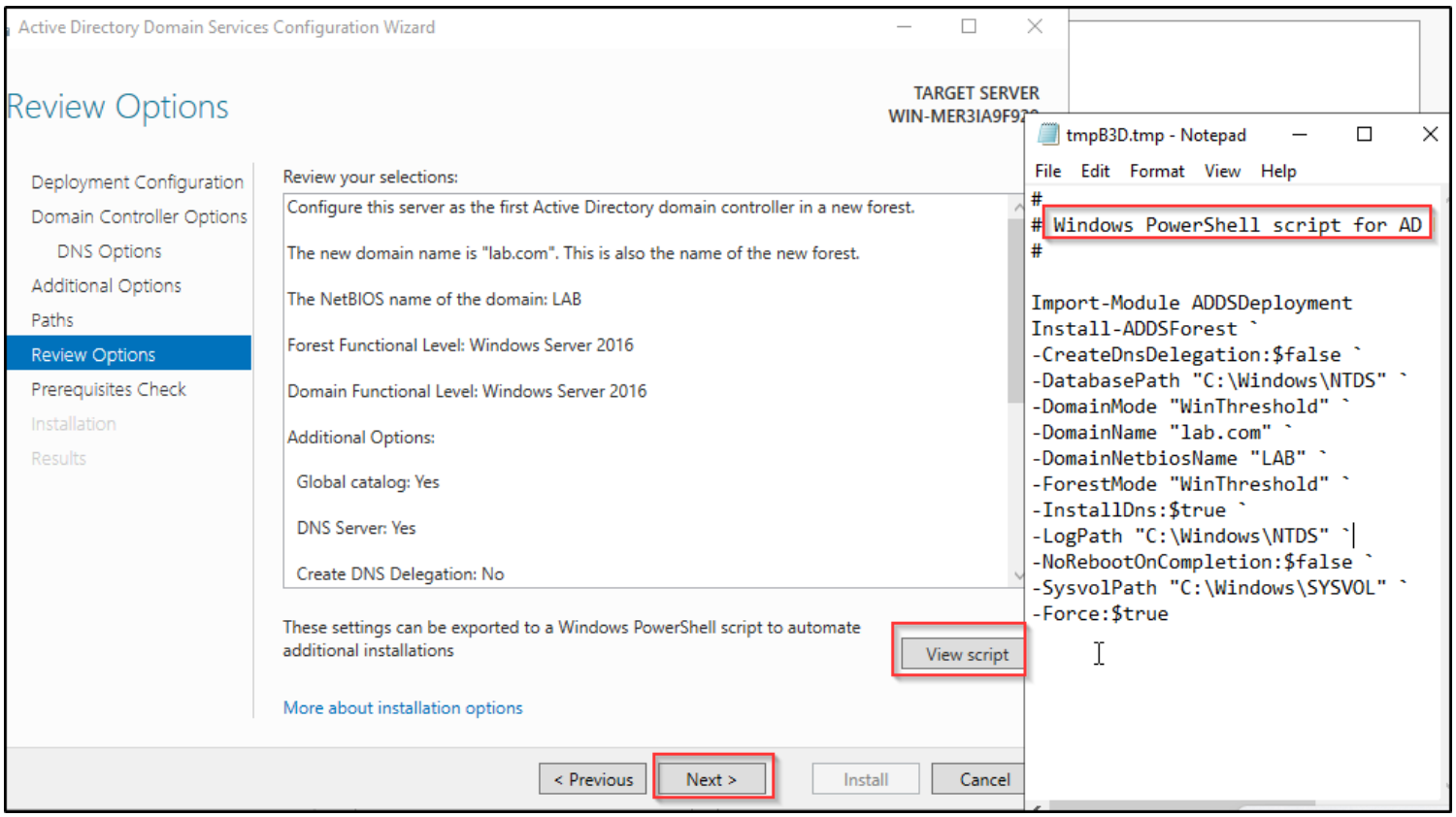
I ignored the warning and clicked **Next** and **Next**.



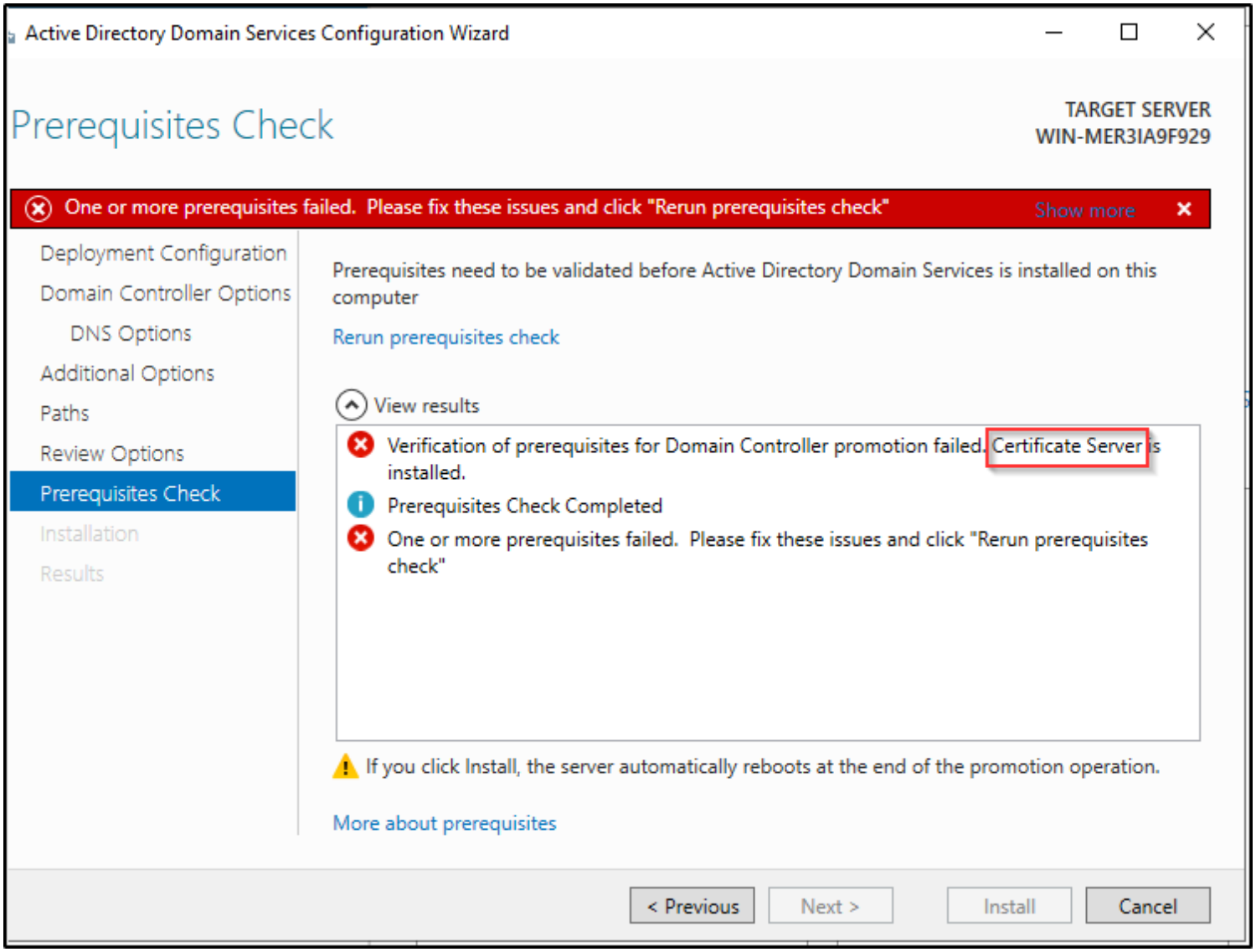
I left everything as default and clicked **Next**.



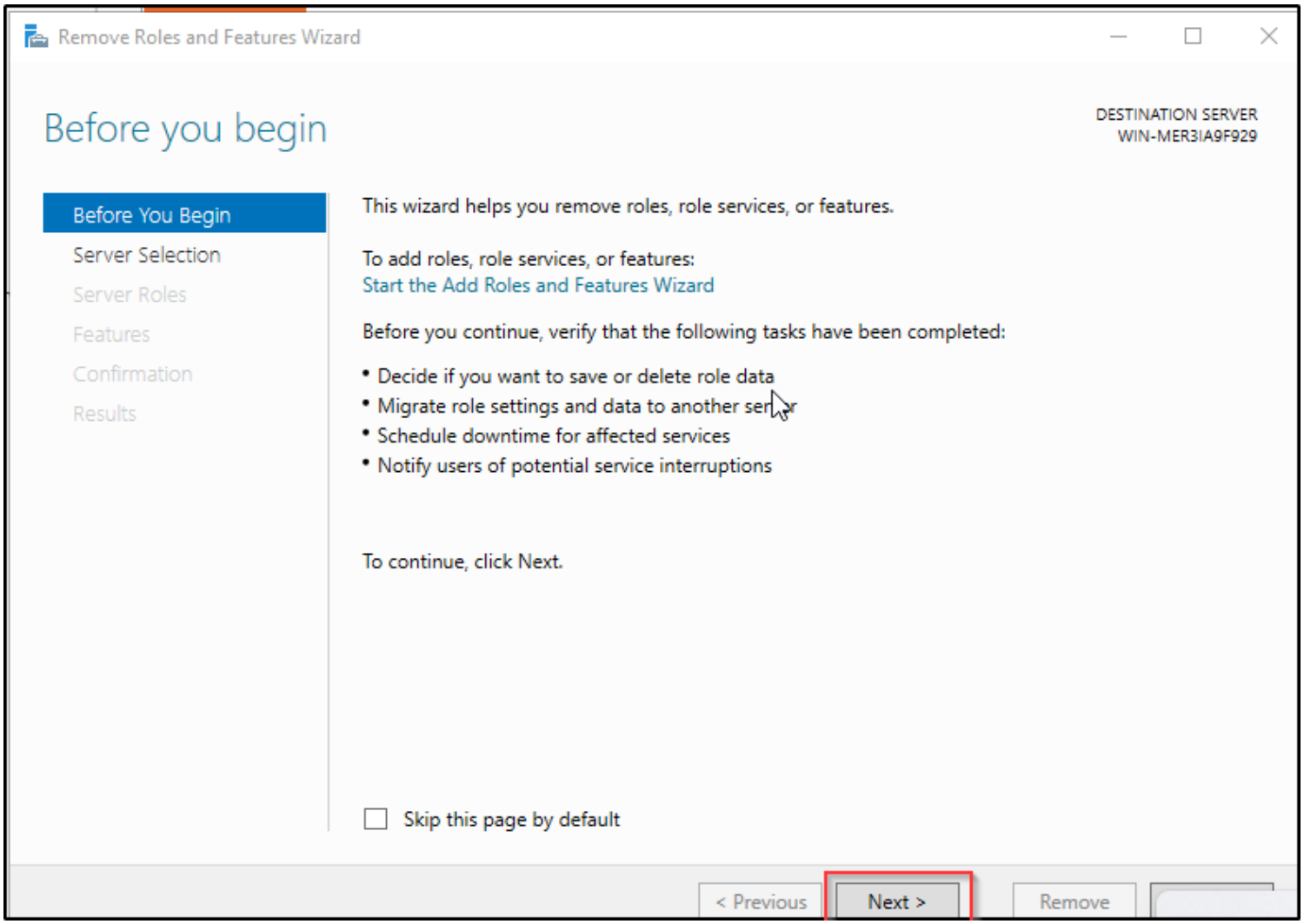
Here, I clicked on **View script**, which displayed a PowerShell automated script that can also be used to promote the server to a Domain Controller (DC). I clicked **Next** since I preferred to proceed with a manual setup.



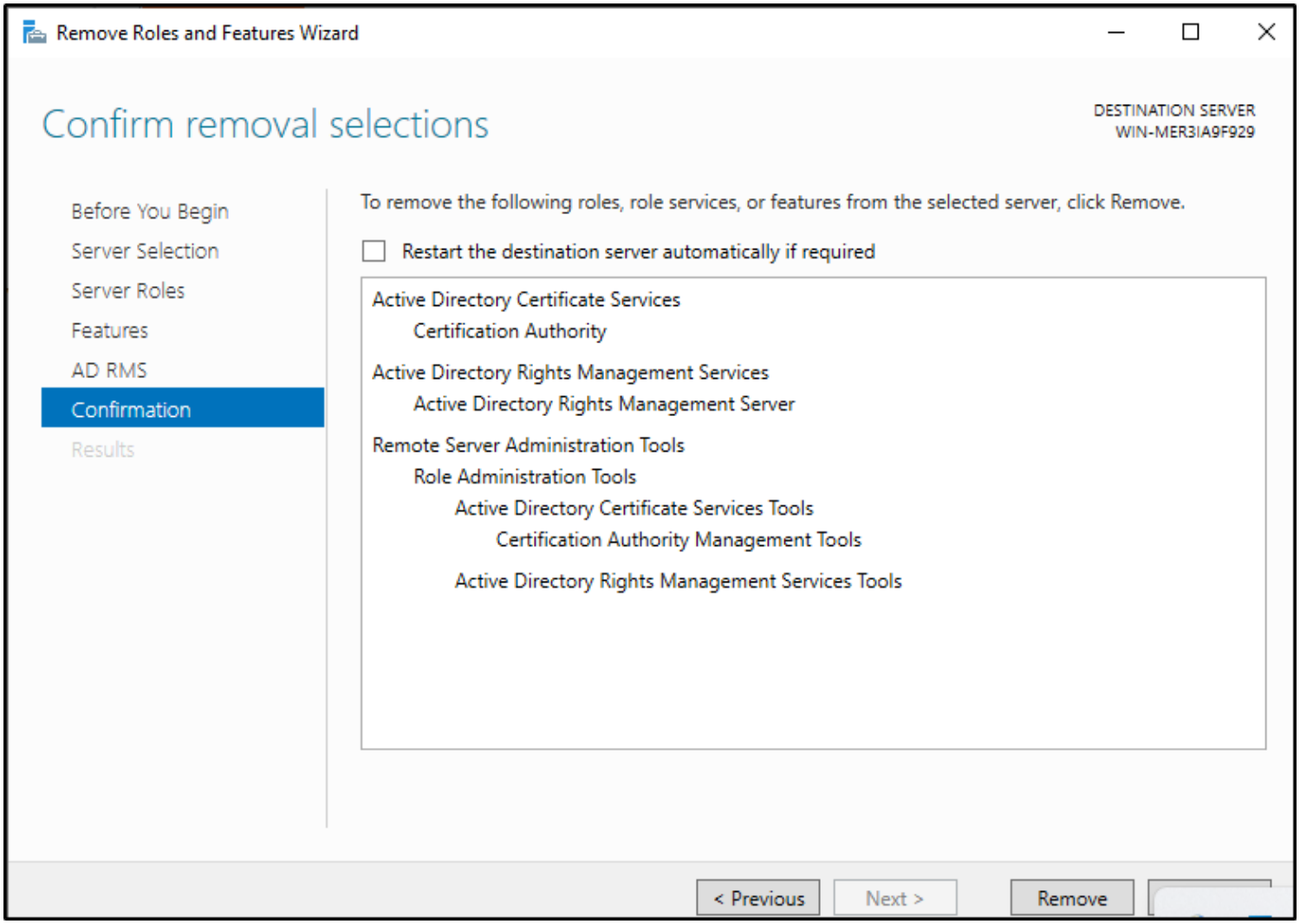
I encountered this issue due to the **Certificate Service** I had installed. Since I don't need it for this lab, I uninstalled it.



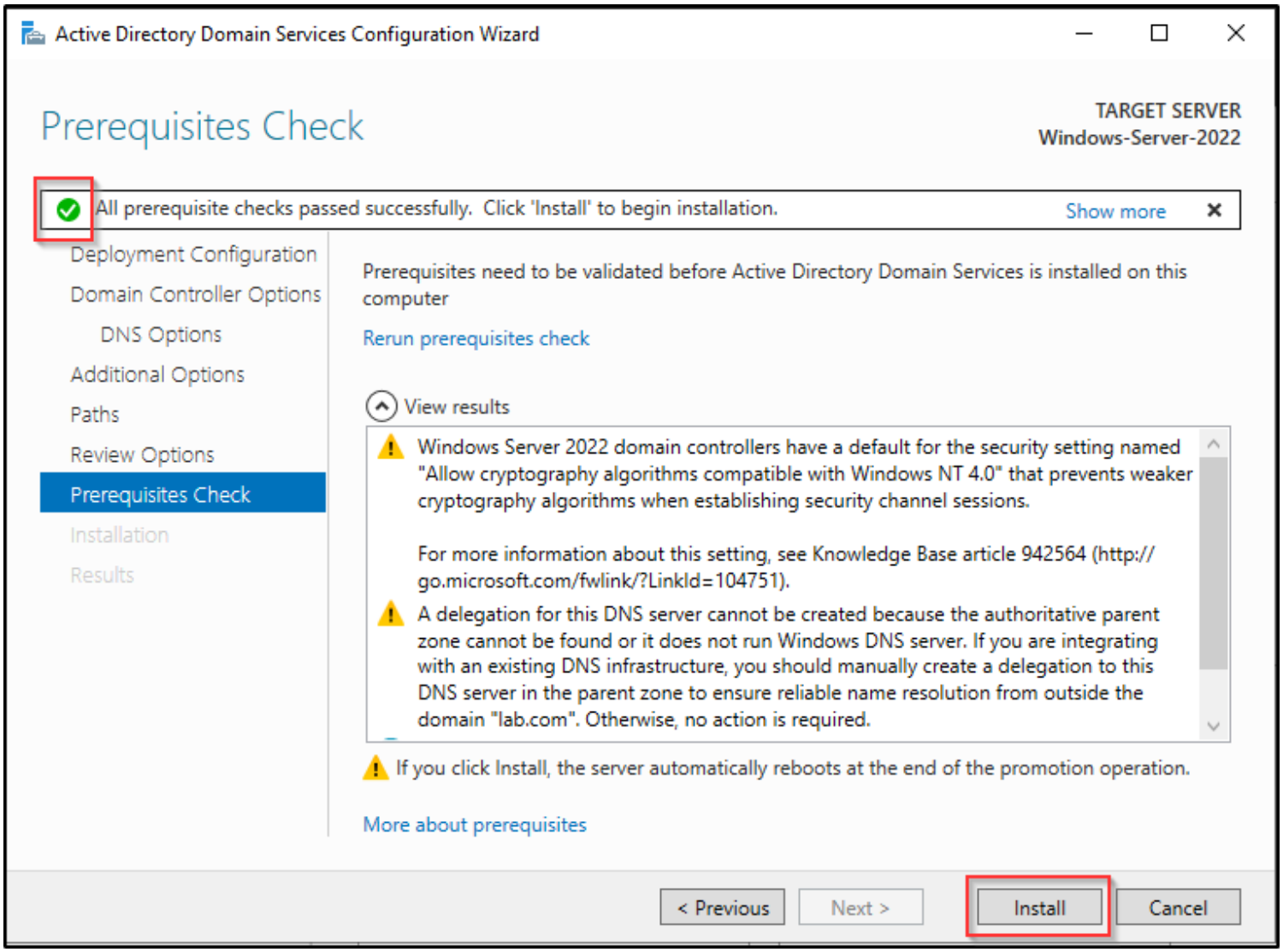
At the **Server Manager Dashboard**, I clicked on **Remove Roles and Features** to remove the **Certificate Services** and **Rights Management Services** roles and features, then clicked on **Next**.



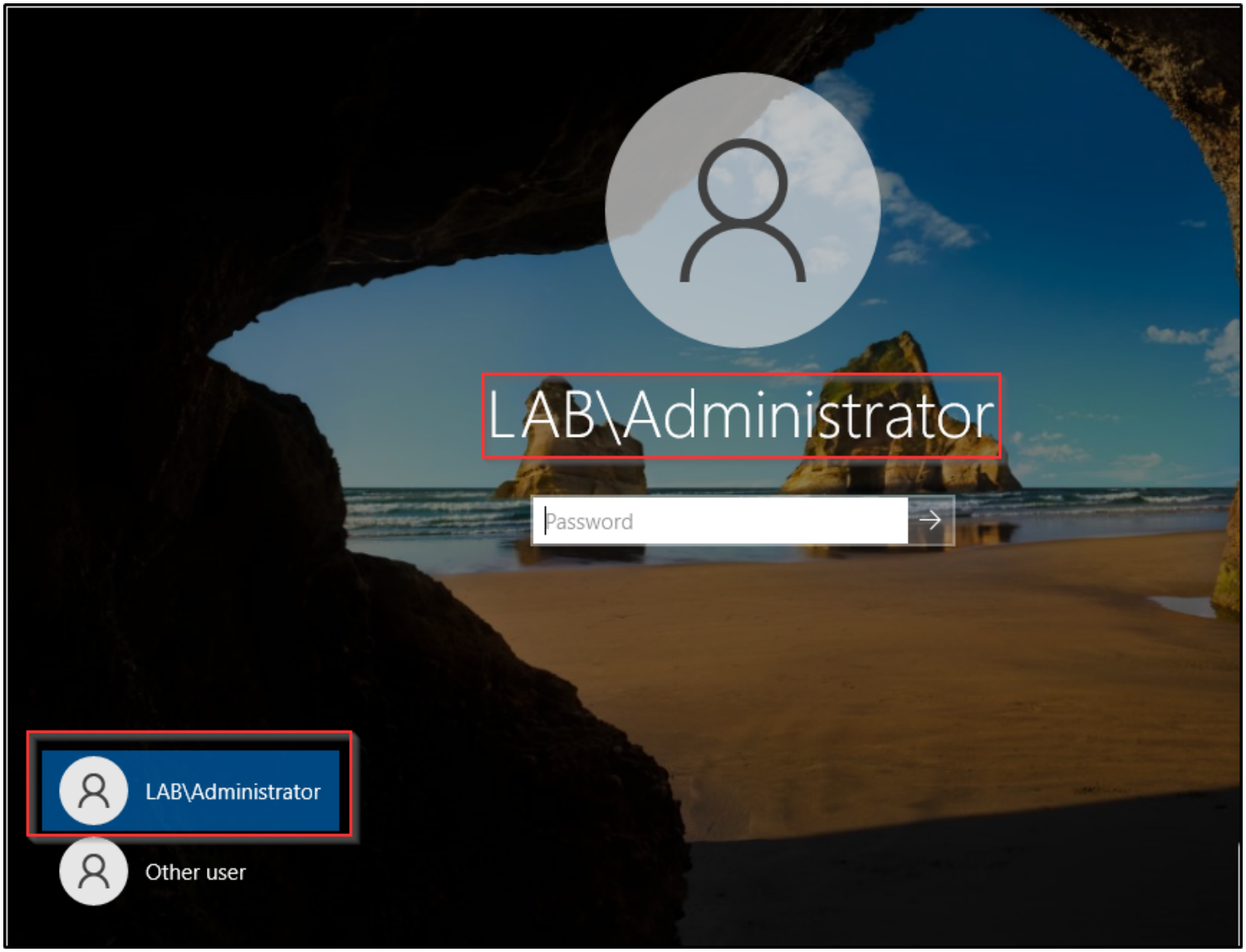
I continued clicking **Next** until I reached this screen, then clicked **Remove**.



After the removal was completed, I started the process of **promoting the server to a Domain Controller (DC)**.
The **Prerequisites Check** was successful.
Then, I clicked on **Install**.



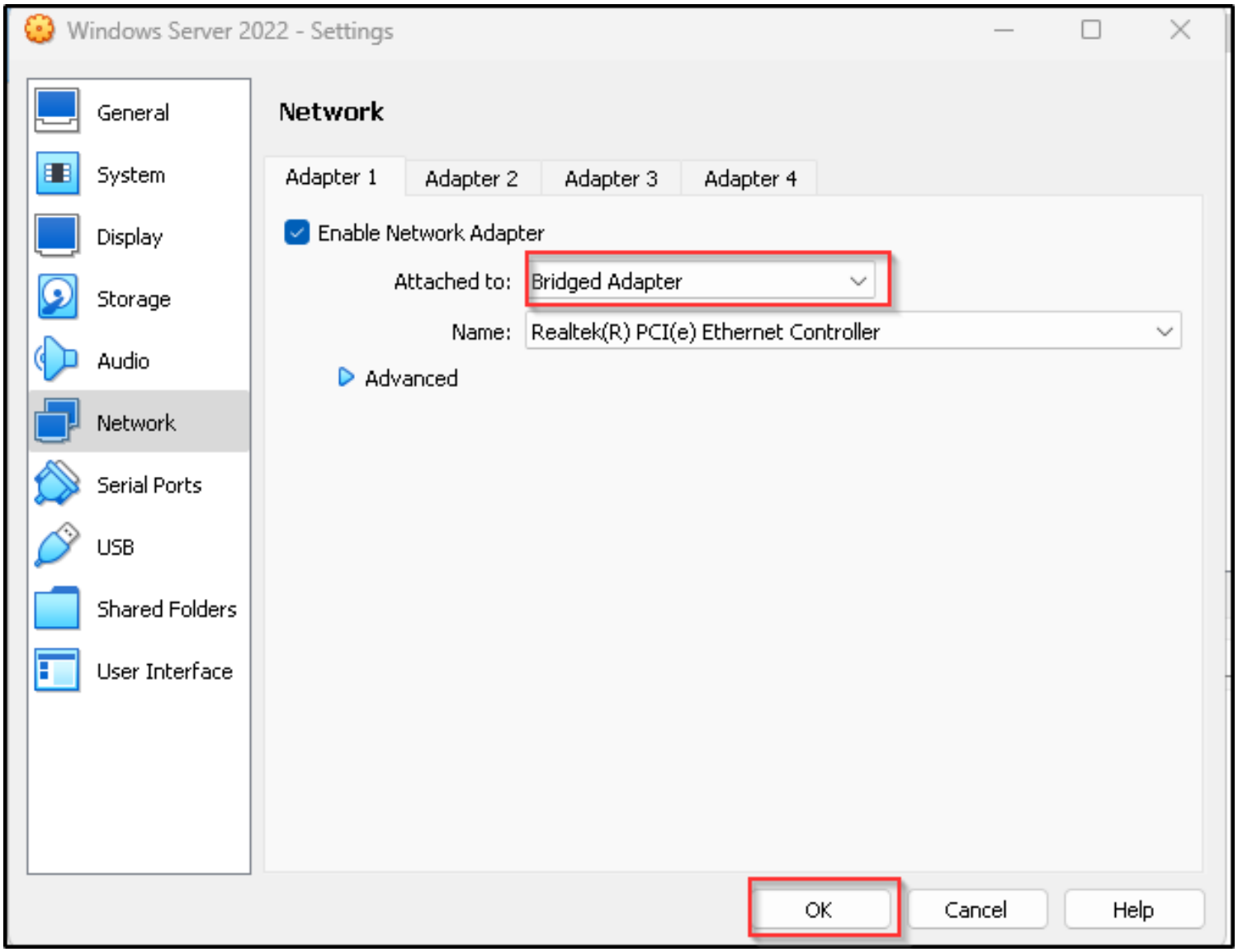
The **Domain Controller** was successfully set up.


LAB\Administrator
Password
LAB\Administrator
Other user

Joining a Windows 11 Client to a Domain

Joining a Windows 11 Client to the Domain (lab.com):

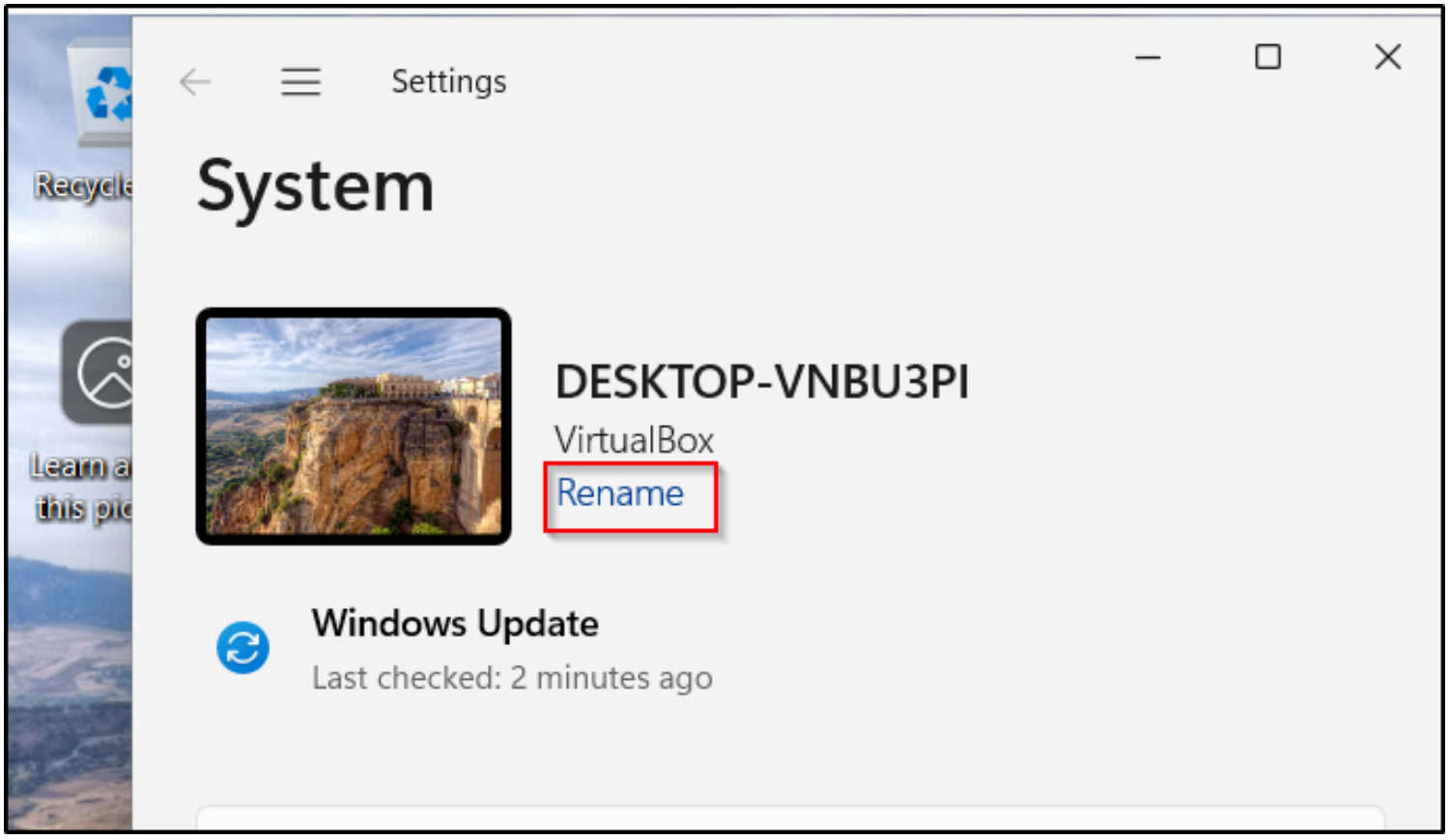
Due to limited hardware resources like memory and CPU, I decided to install the Windows 11 client on a separate host.
Additionally, I changed the network settings to a "Bridged" adapter, allowing VMs from other hosts to communicate with it.



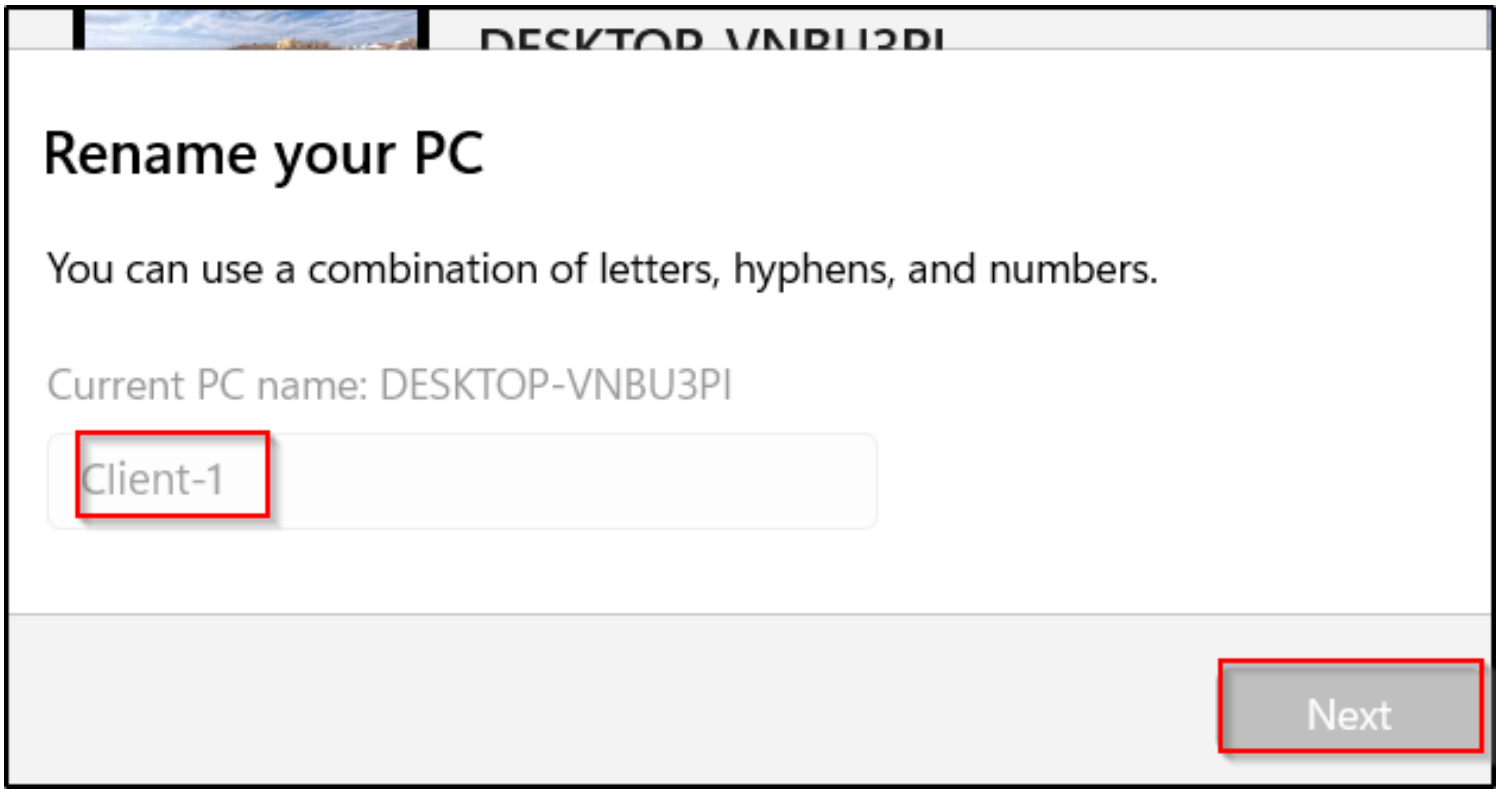
I used the `ipconfig /all` command to verify the IP address of my Windows client to ensure it is on the same network as the domain. I also used the `ping` command to check network reachability.

```
C:\Users\LAB>ping 192.168.1.128

Pinging 192.168.1.128 with 32 bytes of data:
Reply from 192.168.1.128: bytes=32 time=3ms TTL=128
Reply from 192.168.1.128: bytes=32 time=1ms TTL=128
Reply from 192.168.1.128: bytes=32 time=2ms TTL=128
Reply from 192.168.1.128: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms

C:\Users\LAB>
```

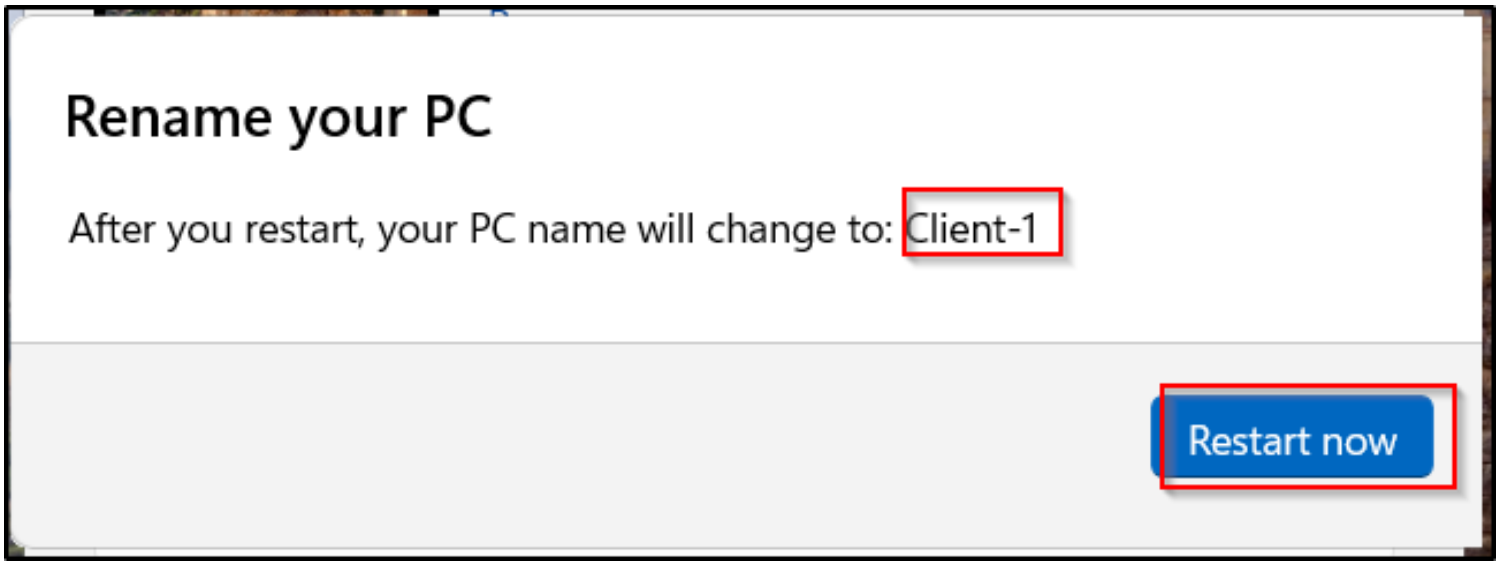
I used the Windows search bar to find **Settings**. In **Settings**, I selected **Rename this PC** to give the computer a more recognizable name.



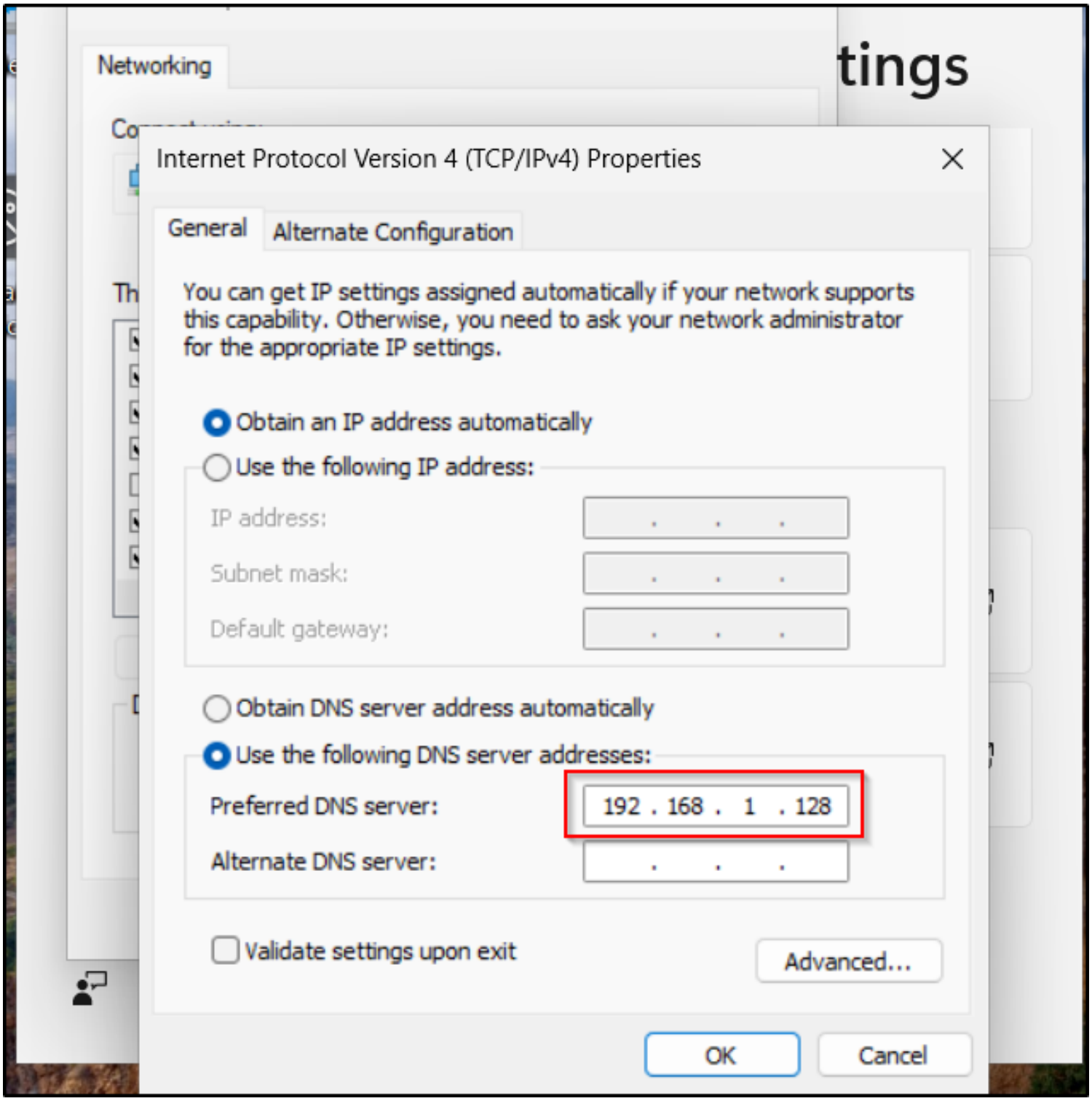
I entered the new name as **Client-1** and clicked **Next** to proceed.



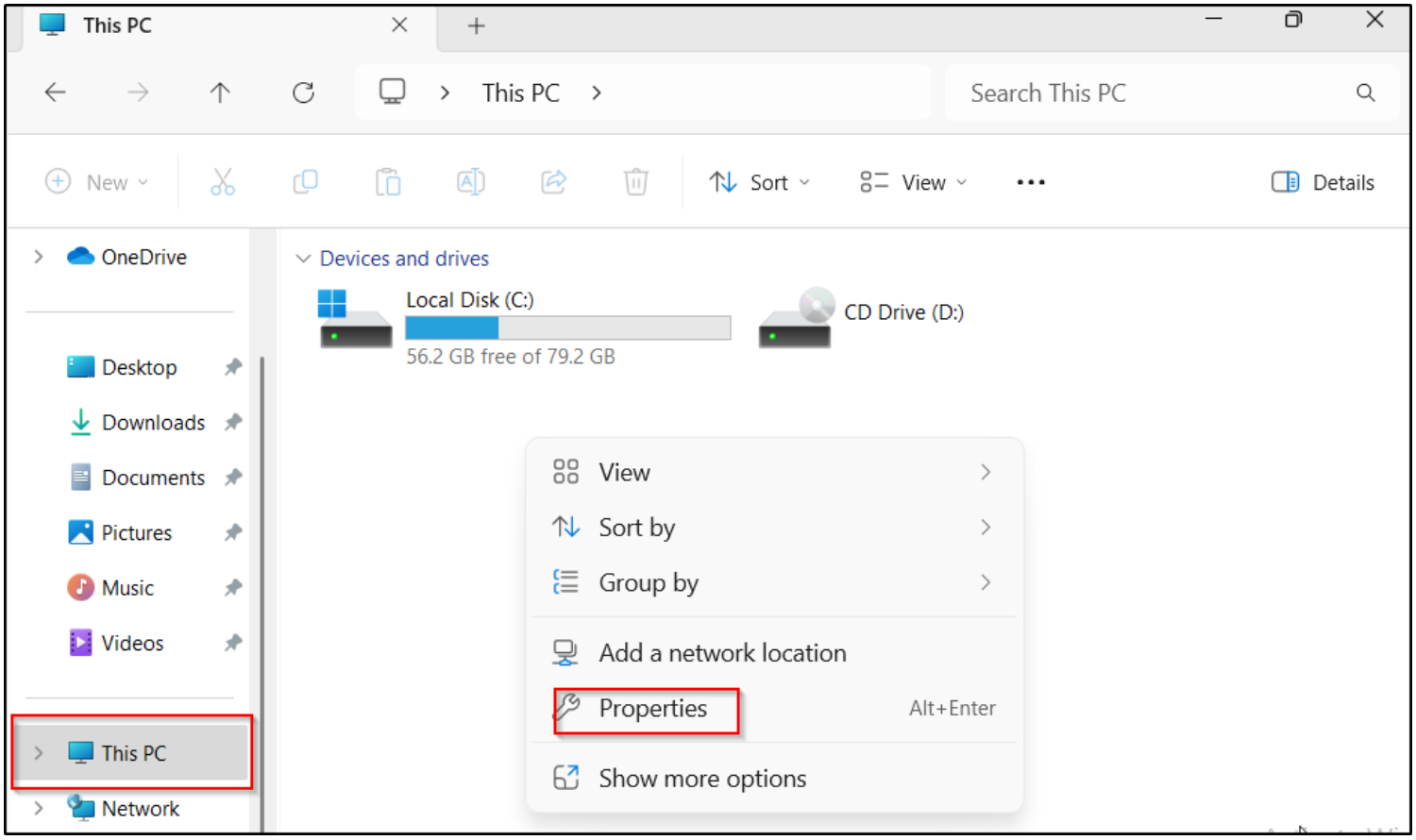
After renaming the PC, I restarted it to apply the changes.



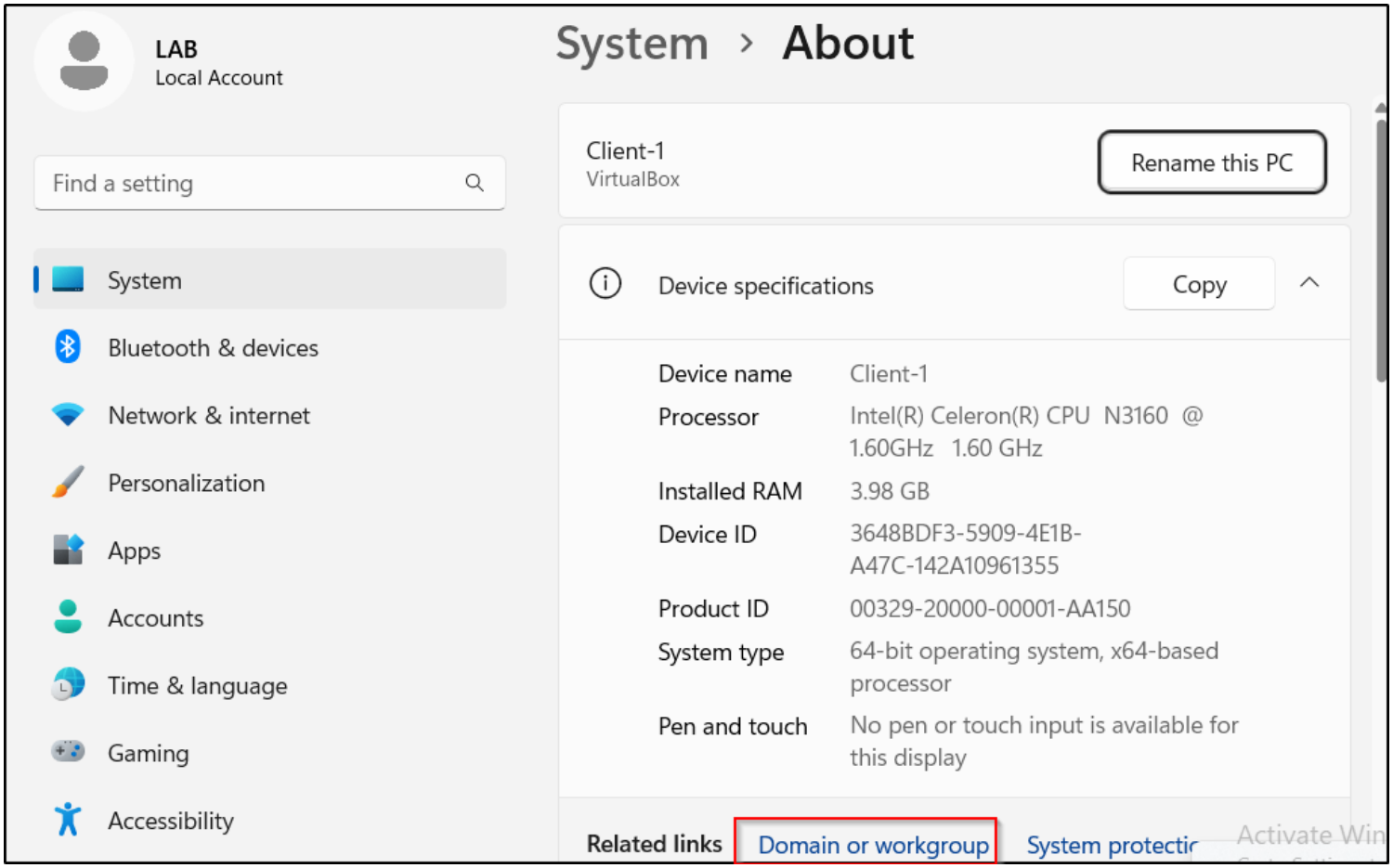
I updated the DNS configuration on my Client-1 PC to point to the Domain Controller's IP address.



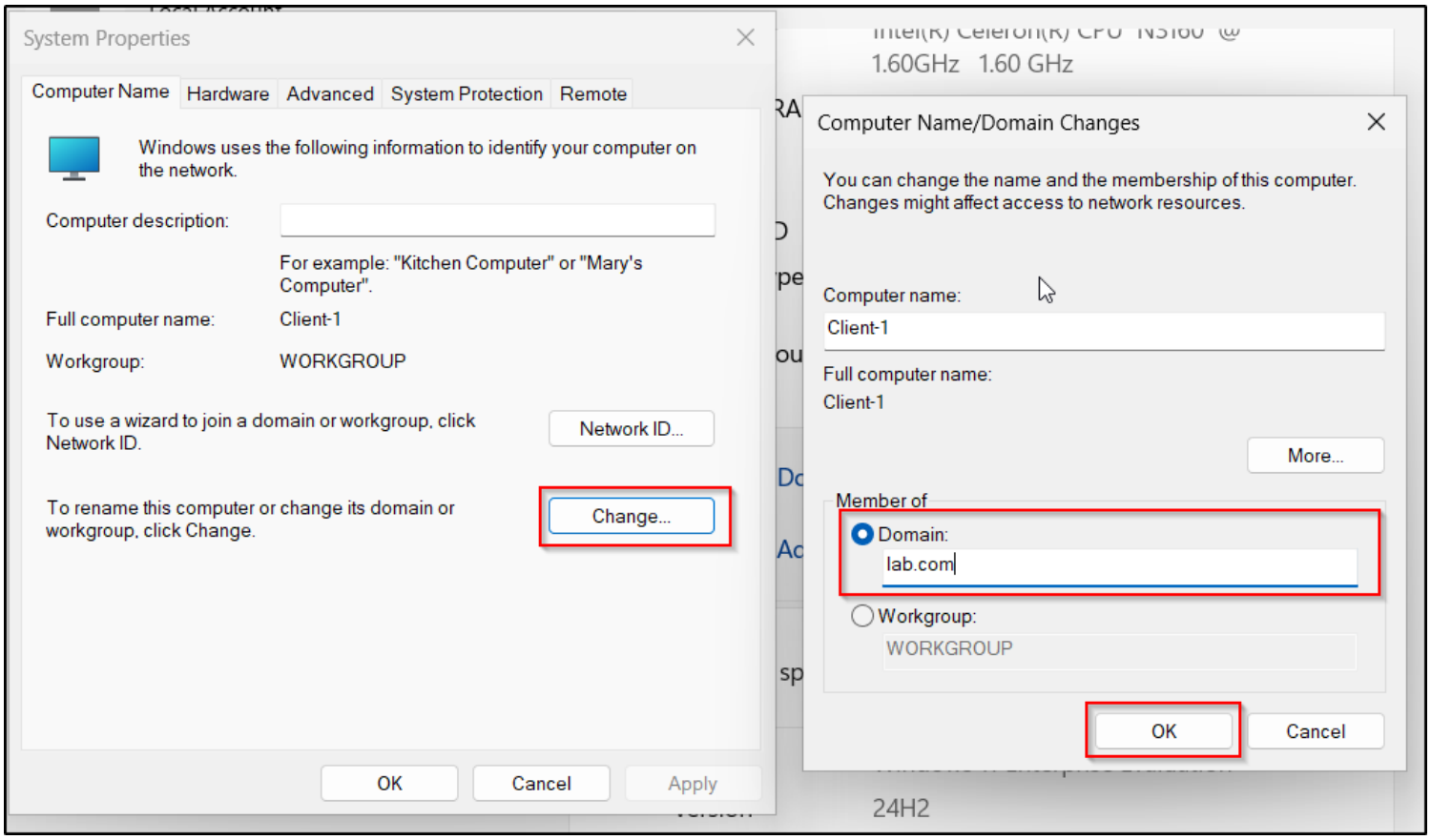
To join Client-1 to the domain, I opened "File Explorer."



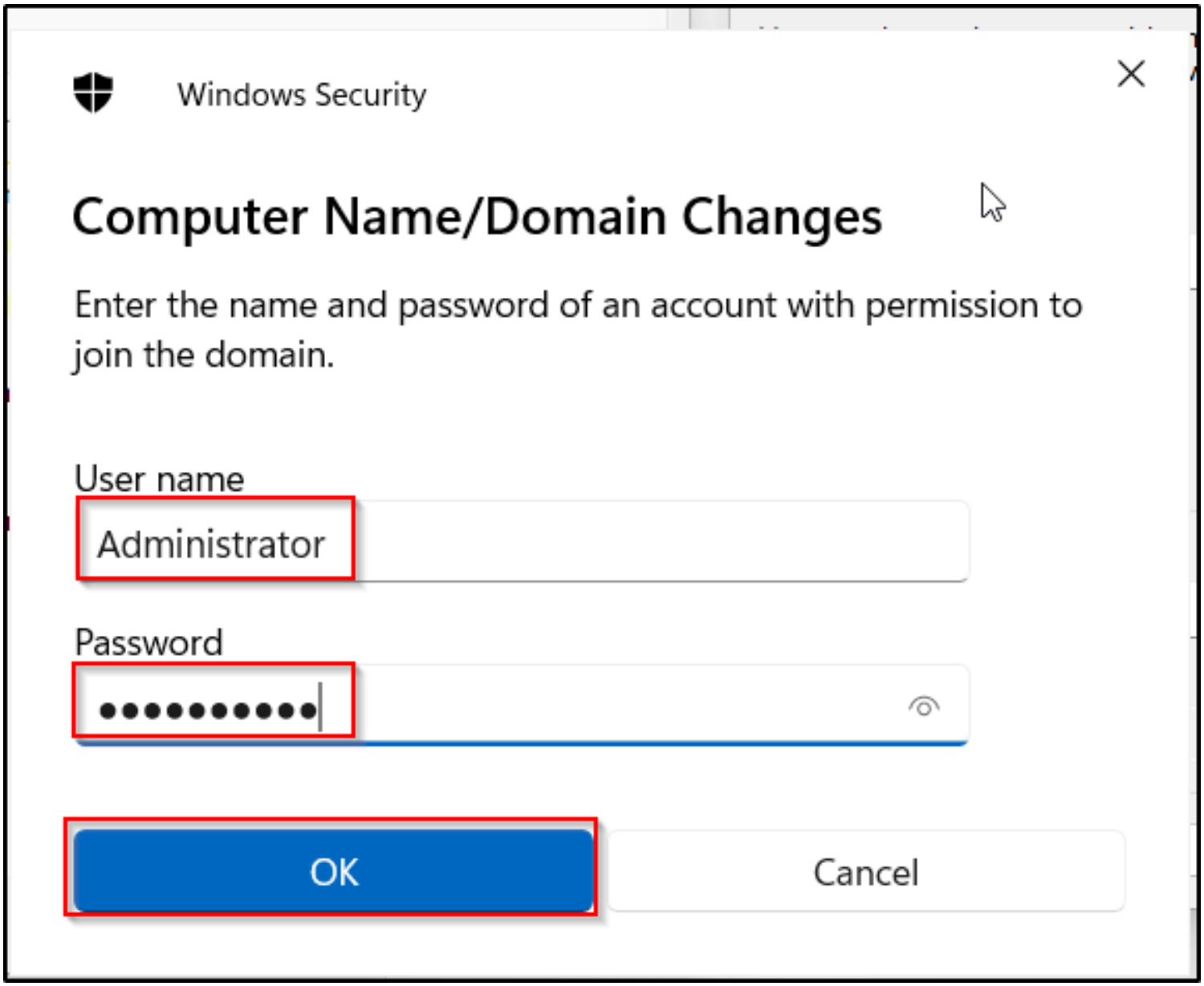
I clicked on **System Properties** and selected **Domain or Workgroup** settings.



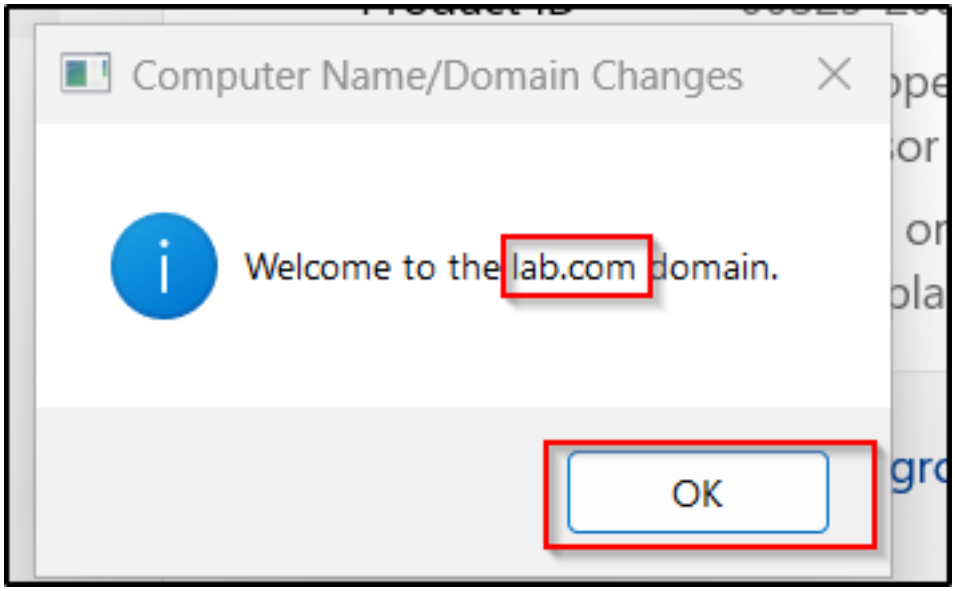
I clicked on **Change** in the **System Properties** window. Under **Member of**, I selected **Domain** and entered the domain name "lab.com." Then, I clicked **OK** to proceed.



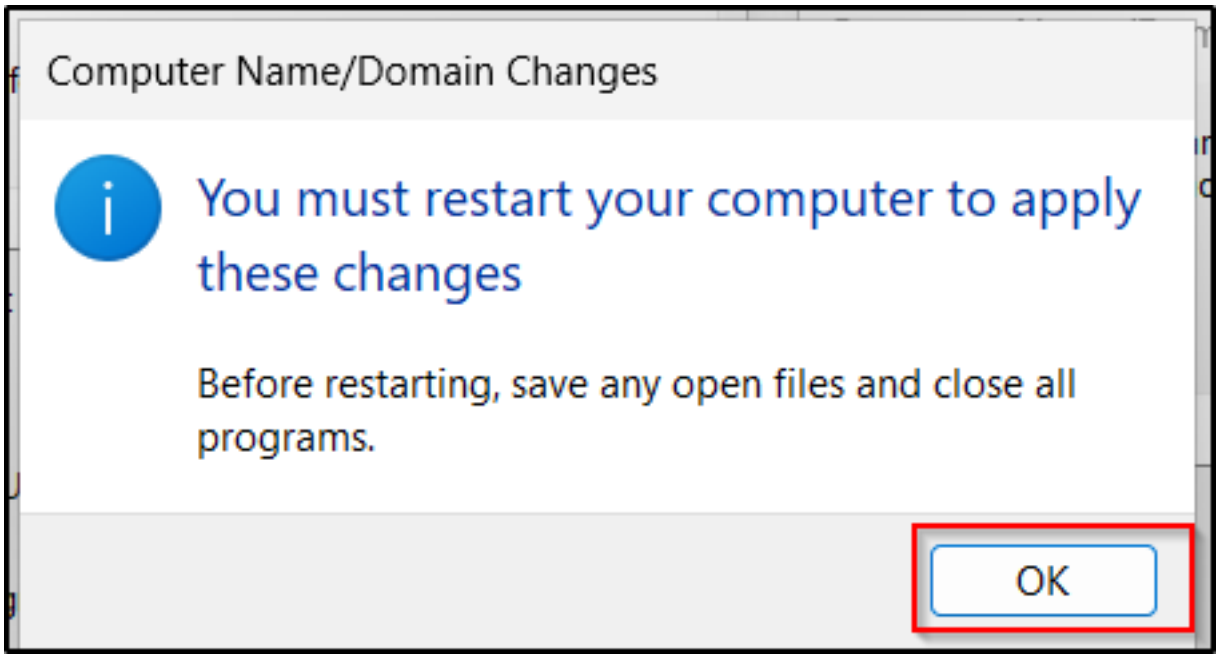
In the **Windows Security** window, I entered the domain username "Administrator" and the associated password. After filling in these credentials, I clicked **OK** to continue.



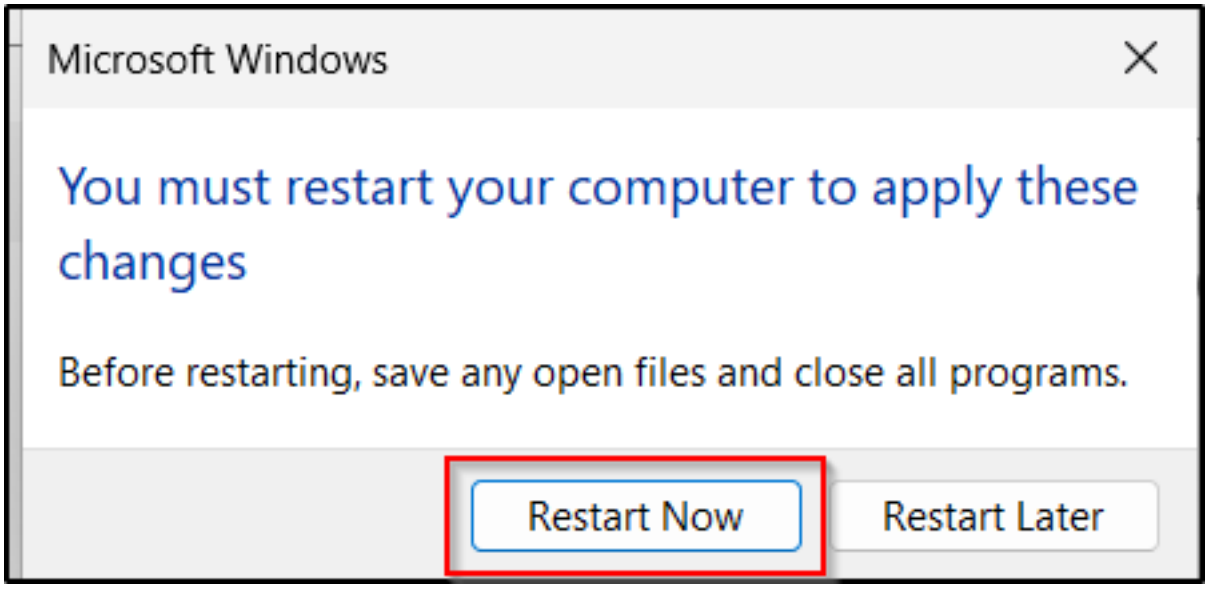
Client-1 was successfully joined to the domain.



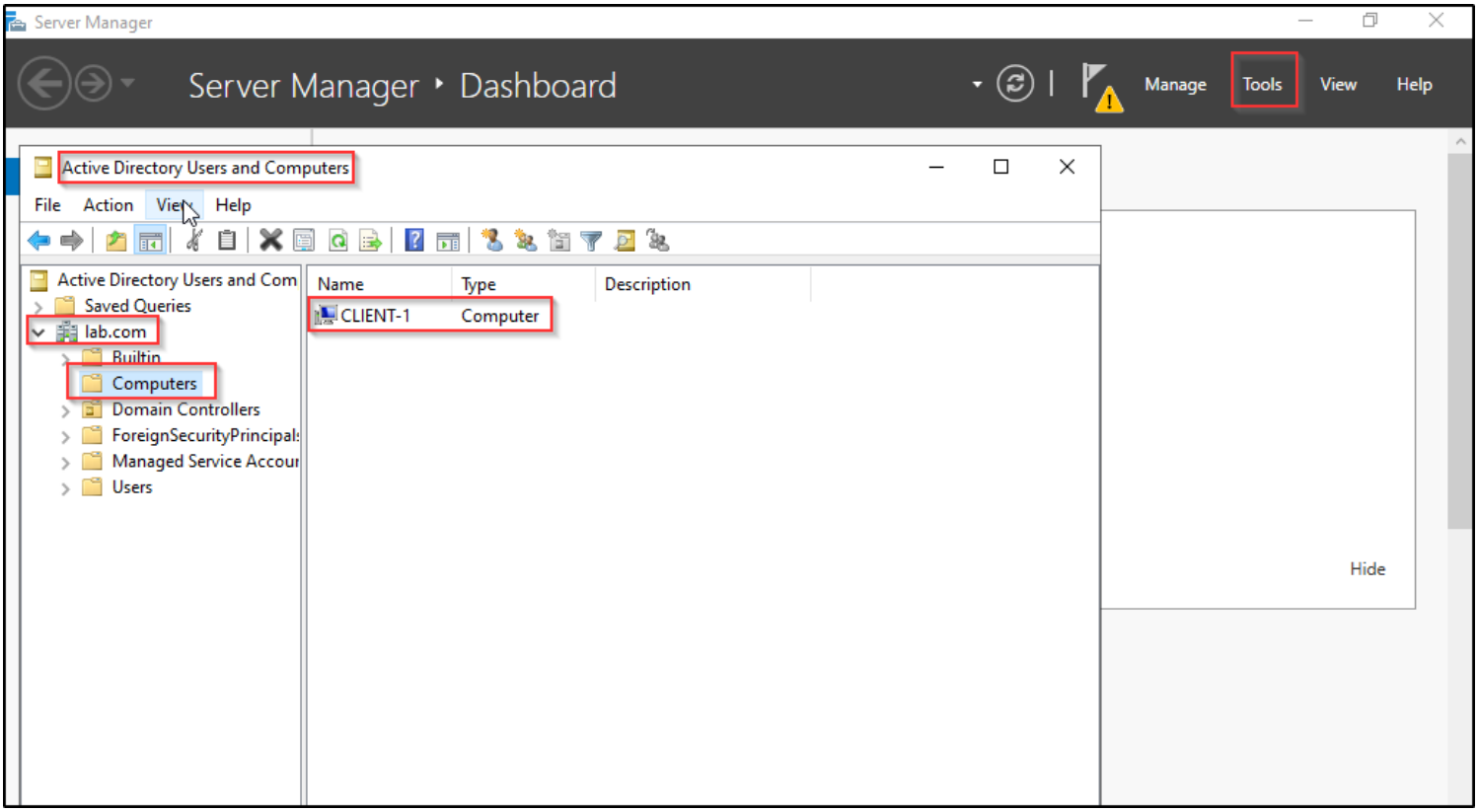
I clicked on "OK" to restart my PC.



And finally, I clicked on "Restart Now."

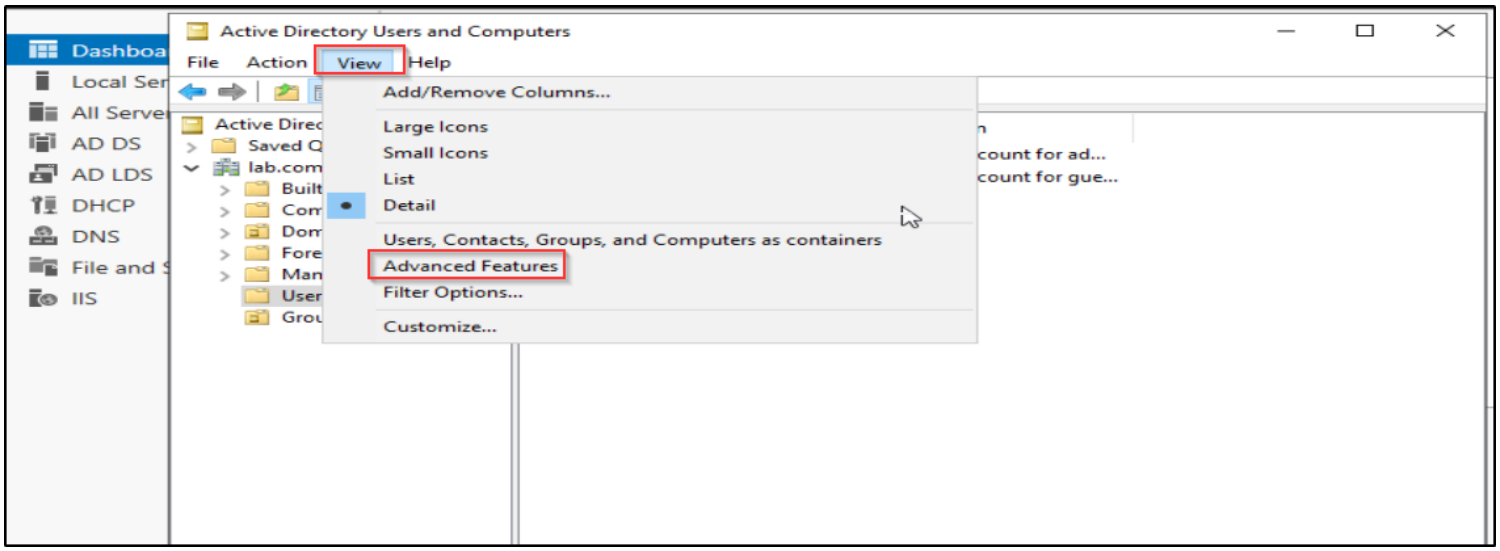


I confirmed on the Domain.
On the Domain, I opened the Server Manager Dashboard, clicked on “Tools,” then selected “Active Directory Users and Computers.” I clicked on the Domain name “lab.com,” and then selected “Computers.” There, I confirmed that the Client-1 PC was successfully joined to the domain.

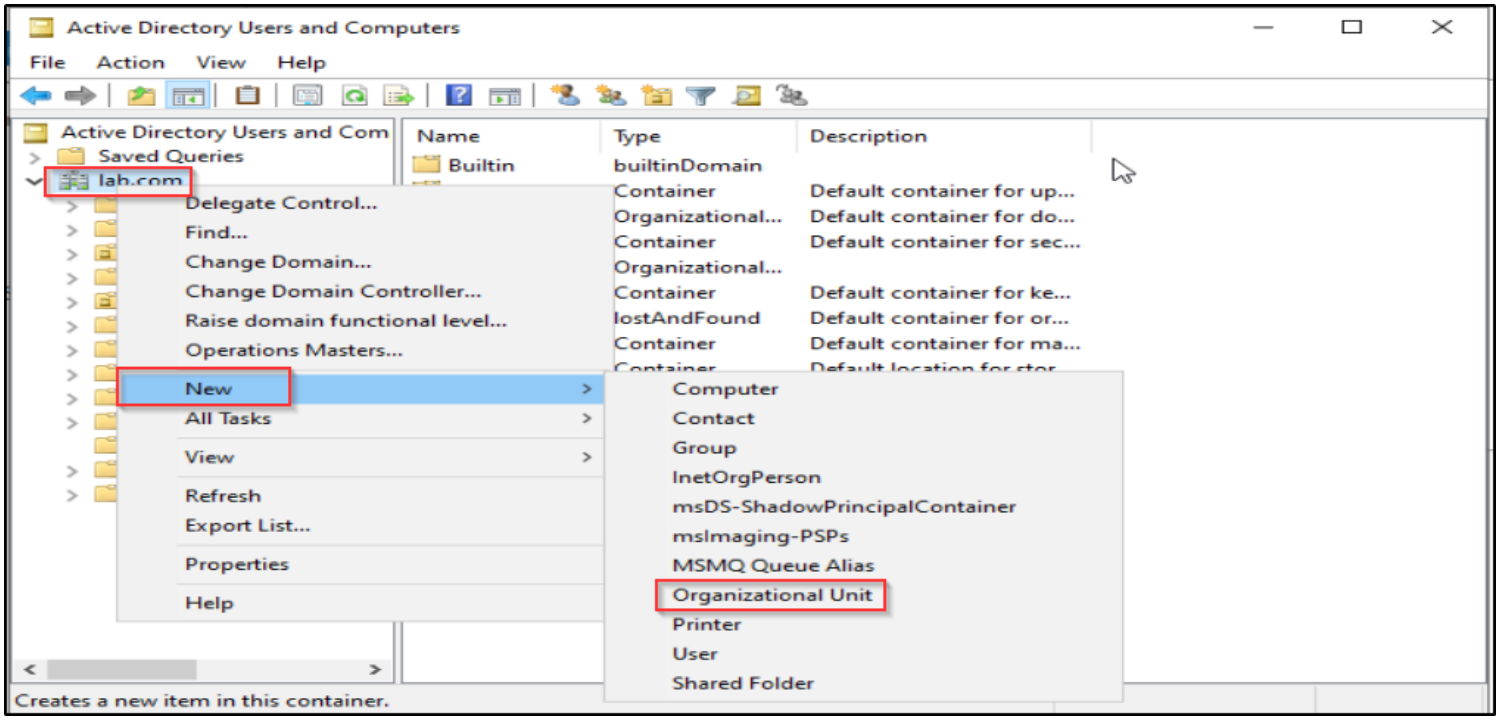

Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
lab.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accou
Users
Name
Type
Description
CLIENT-1
Computer
Hide

Users, Groups and Organisational Units Creation

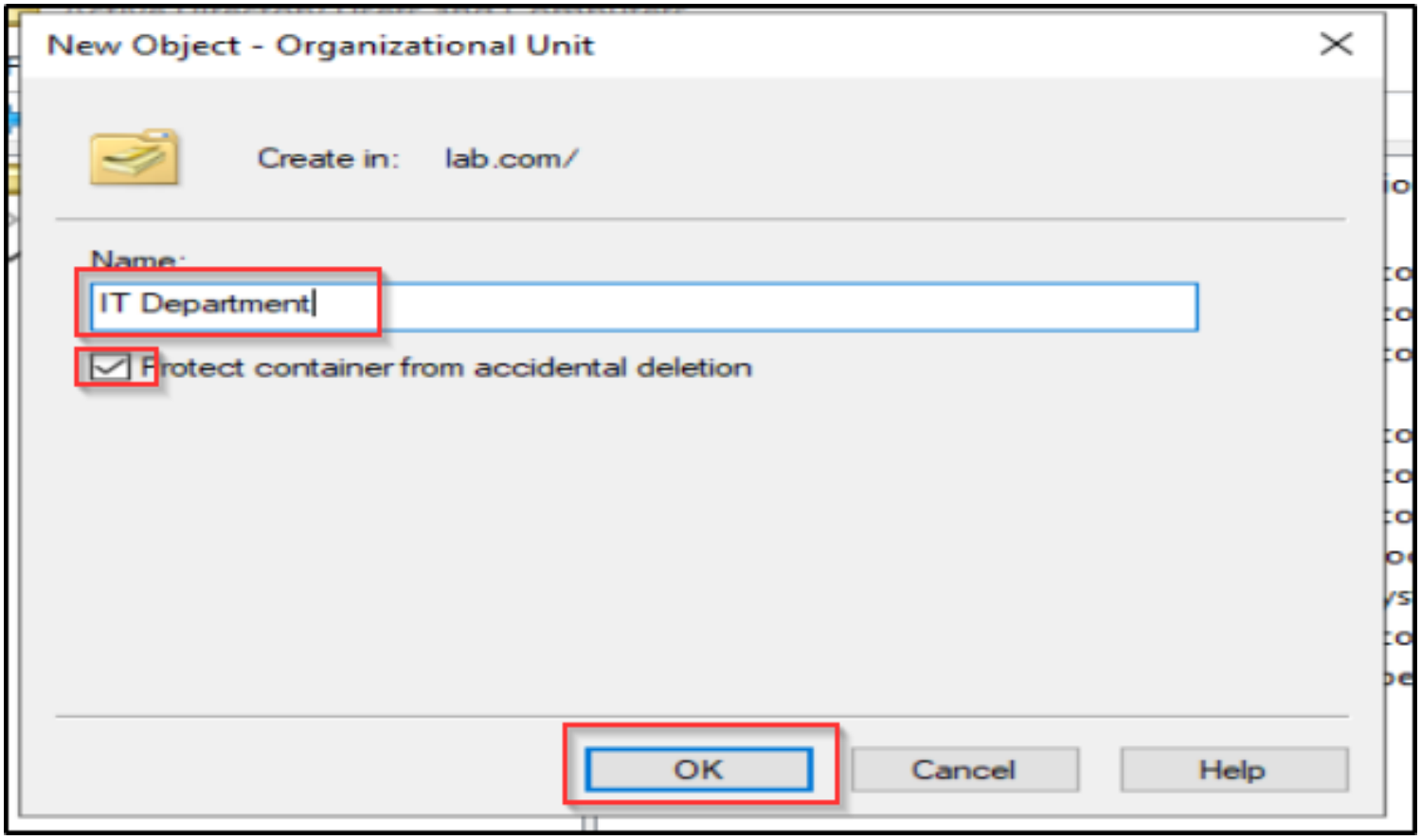
Creating Organizational Units
I navigated to the Server Manager Dashboard and clicked on **Tools**, then selected **Active Directory Users and Computers**.
In the new window, I clicked on **View** and enabled **Advanced Features**. This option provides additional settings and controls, allowing access to more advanced configuration options.



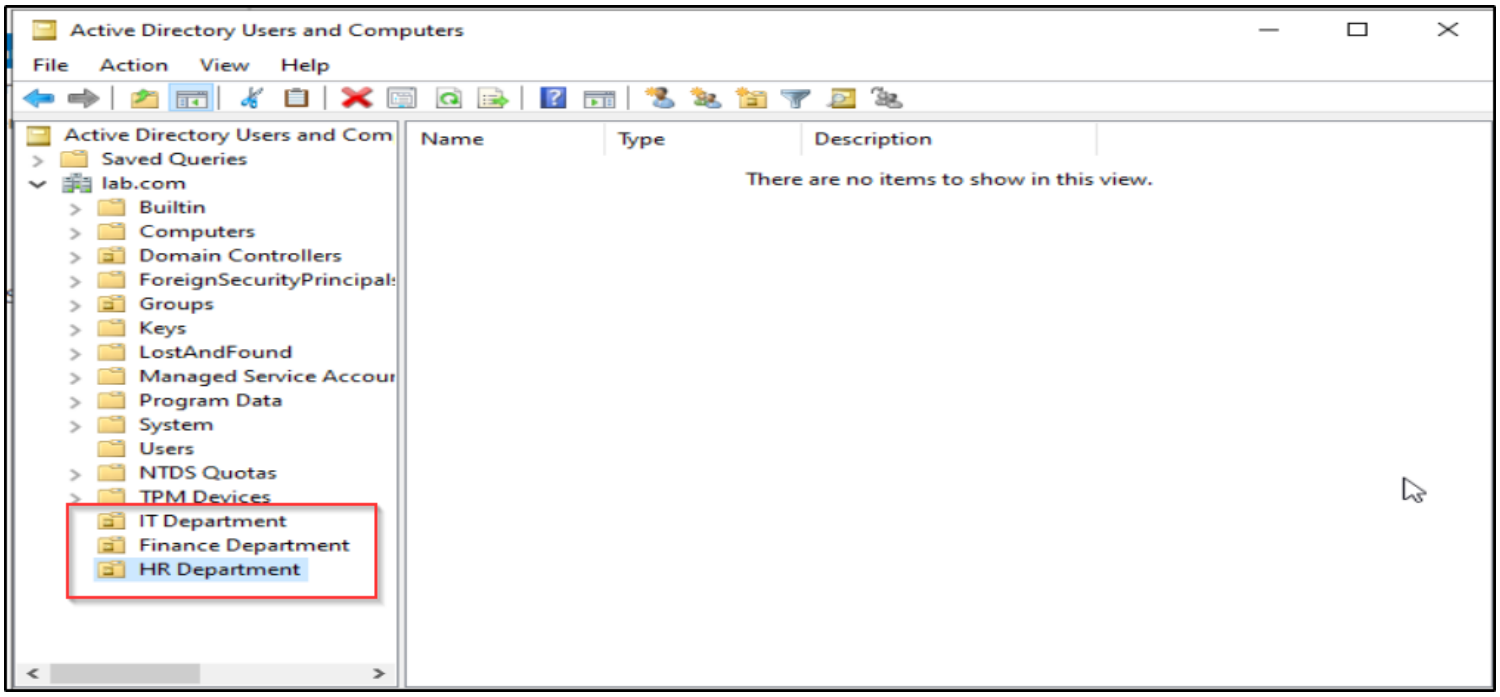
I started by creating Organizational Units (OUs) such as **IT Department**, **Finance Department**, and **HR Department**.
To accomplish this, I right-clicked on the domain name "lab.com," selected **New**, and then clicked on **Organizational Unit**.



I entered the name of the unit I wanted to create, "IT Department," and ensured that **Protect container from accidental deletion** was checked to prevent any unintended deletion. I then clicked **OK** to create the unit.



I repeated the same process to create additional organizational units, such as the **Finance Department** and **HR Department**.



Creating Users in Active Directory

In Active Directory (AD), there are two primary methods for creating users:

1. **Copy Method**: This approach is useful for creating new users who will have the same attributes as an existing user within the same group or organizational unit. It helps save time and reduces repetitive tasks.

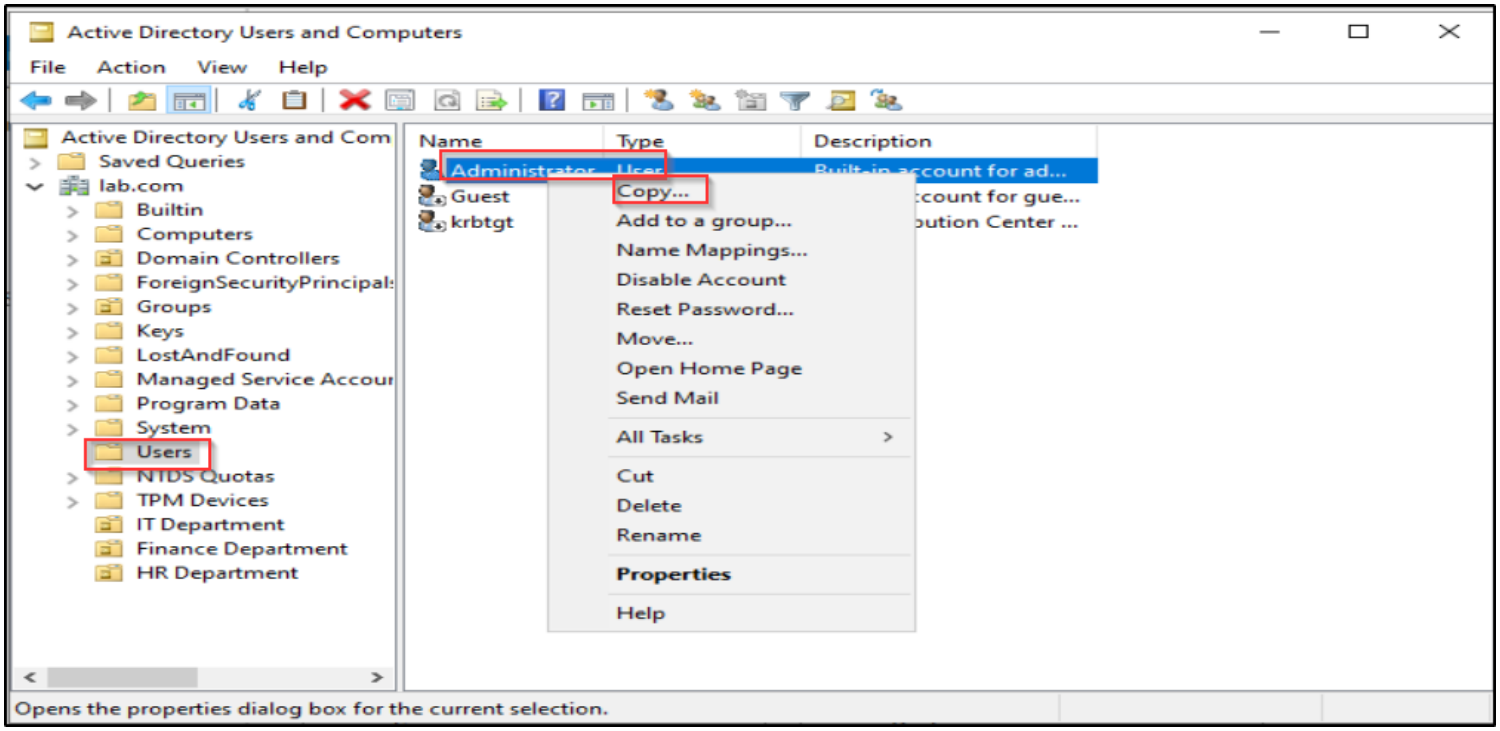
2. **Manual Creation**: This method involves manually inputting all attributes for a new user, which is ideal when the new user requires unique attributes.

I used both methods to create users:

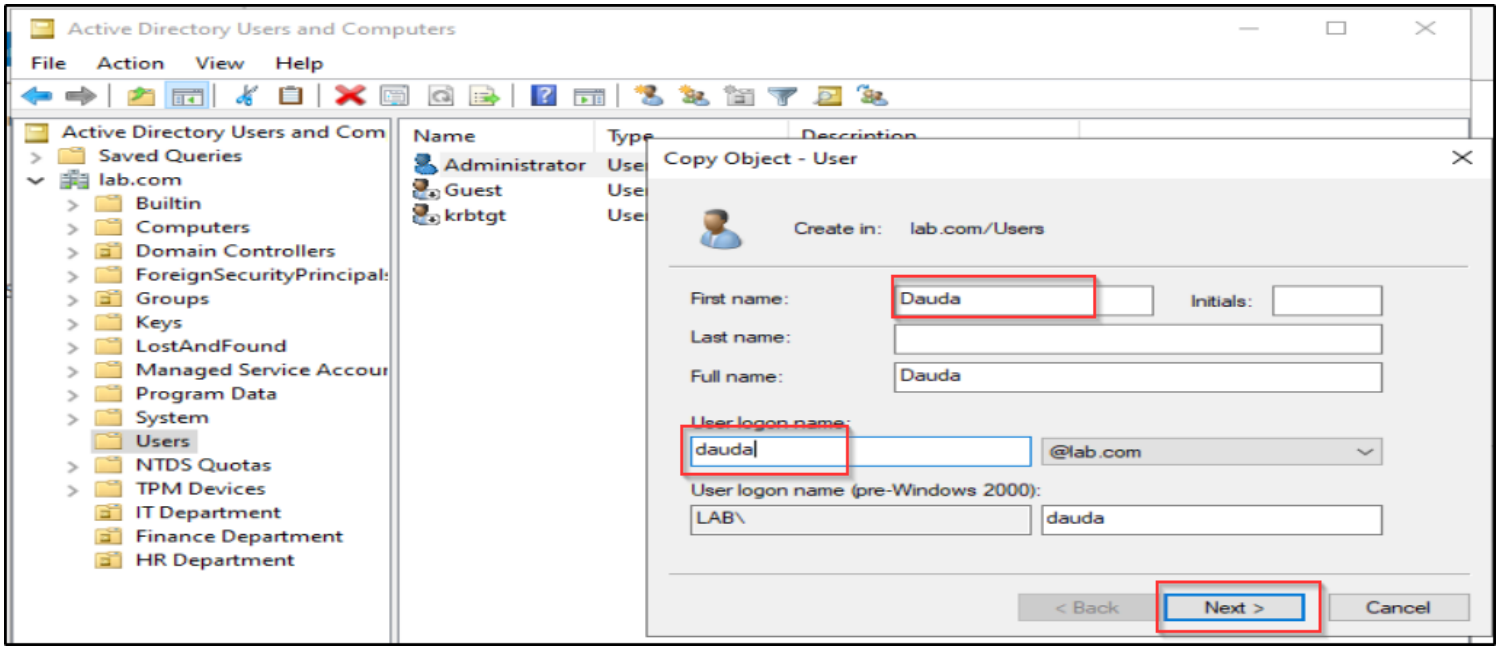
Using the Copy Method

I started by creating the **IT Department Admin** using the Copy method since I wanted the IT manager to inherit all attributes of the Domain Administrator. Here's how I did it:

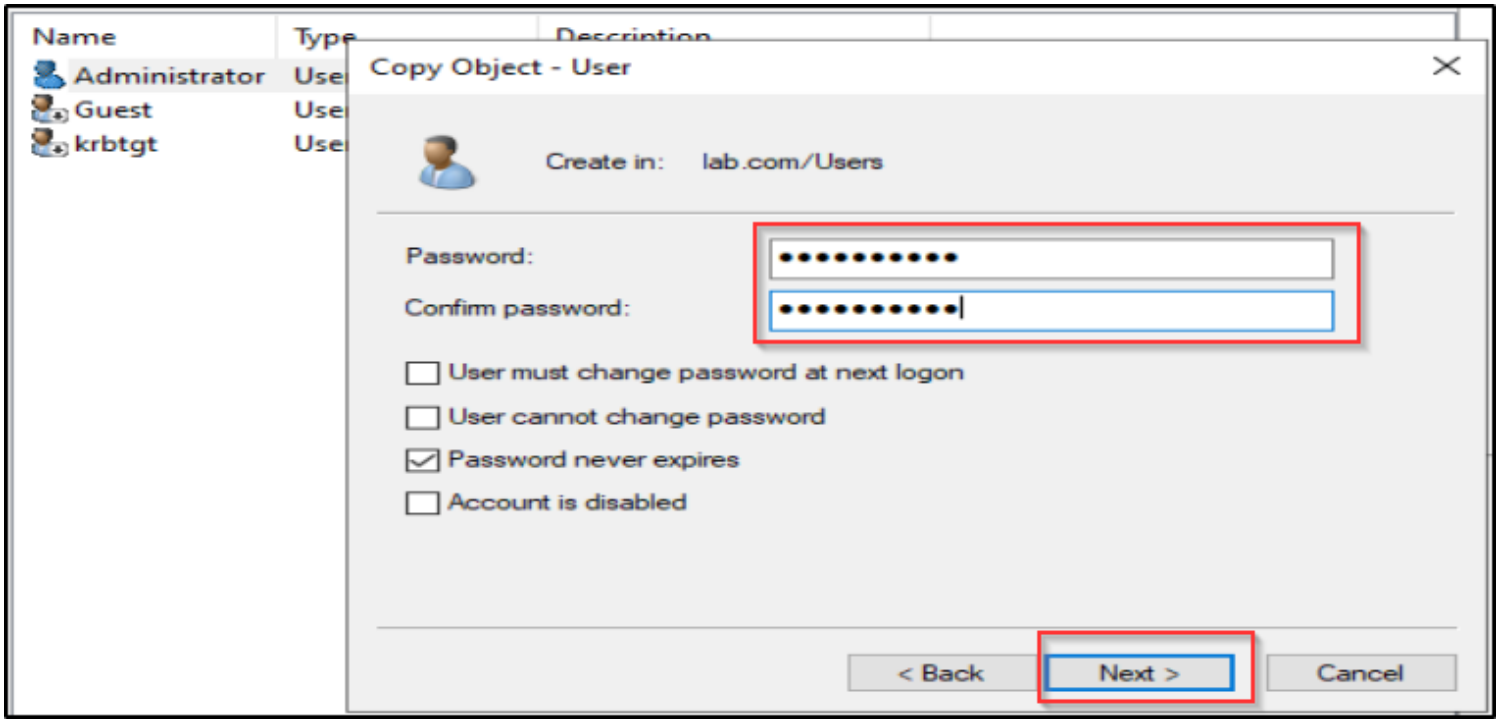
1. I navigated to the **Users** folder.
2. Right-clicked on the existing **Administrator** account.
3. Selected **Copy** to duplicate the account with the desired attributes.



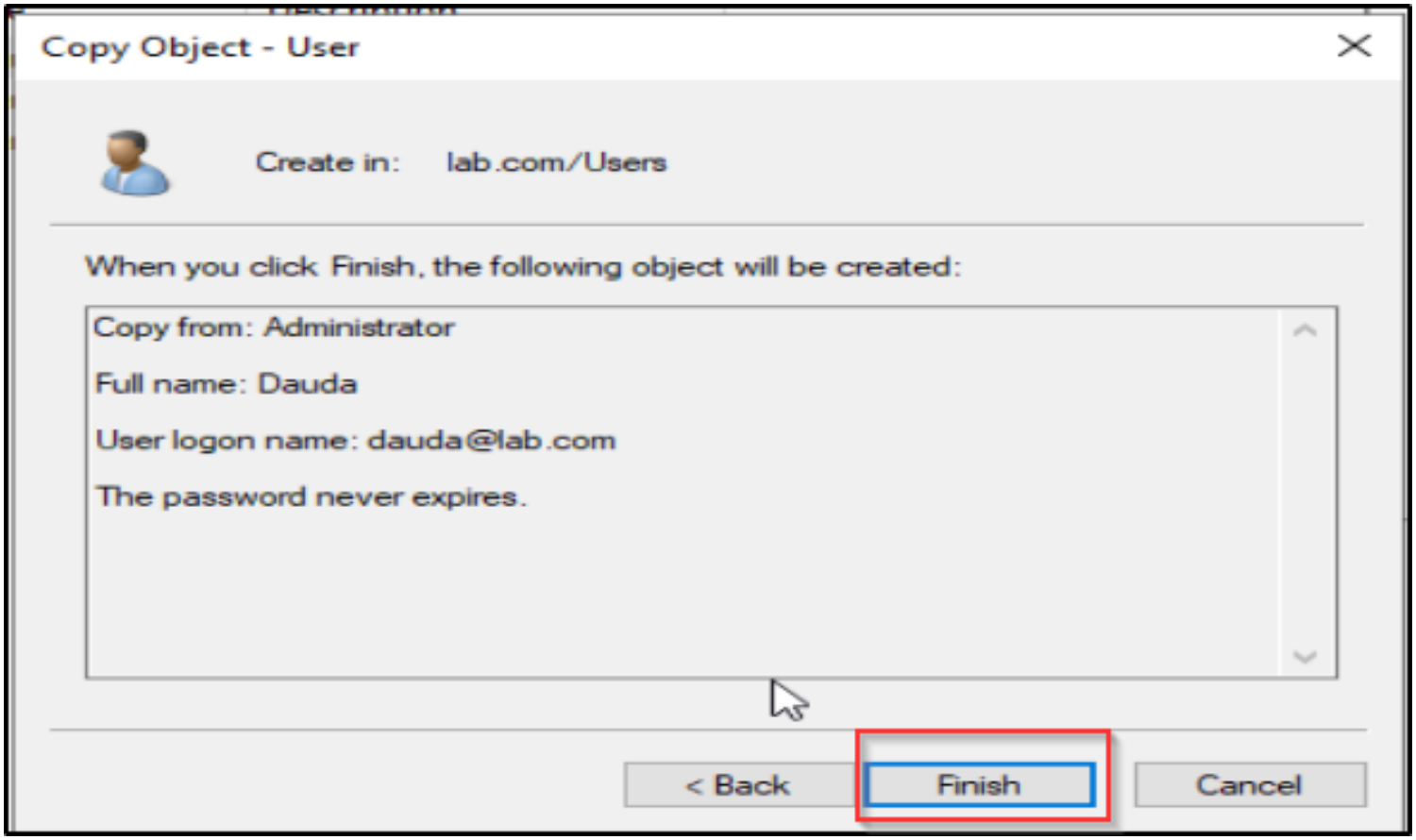
I filled in all the account information, including the **username**, **password**, and other required details for the new IT Department Admin. After ensuring all fields were completed accurately, I clicked on **Next** to proceed.



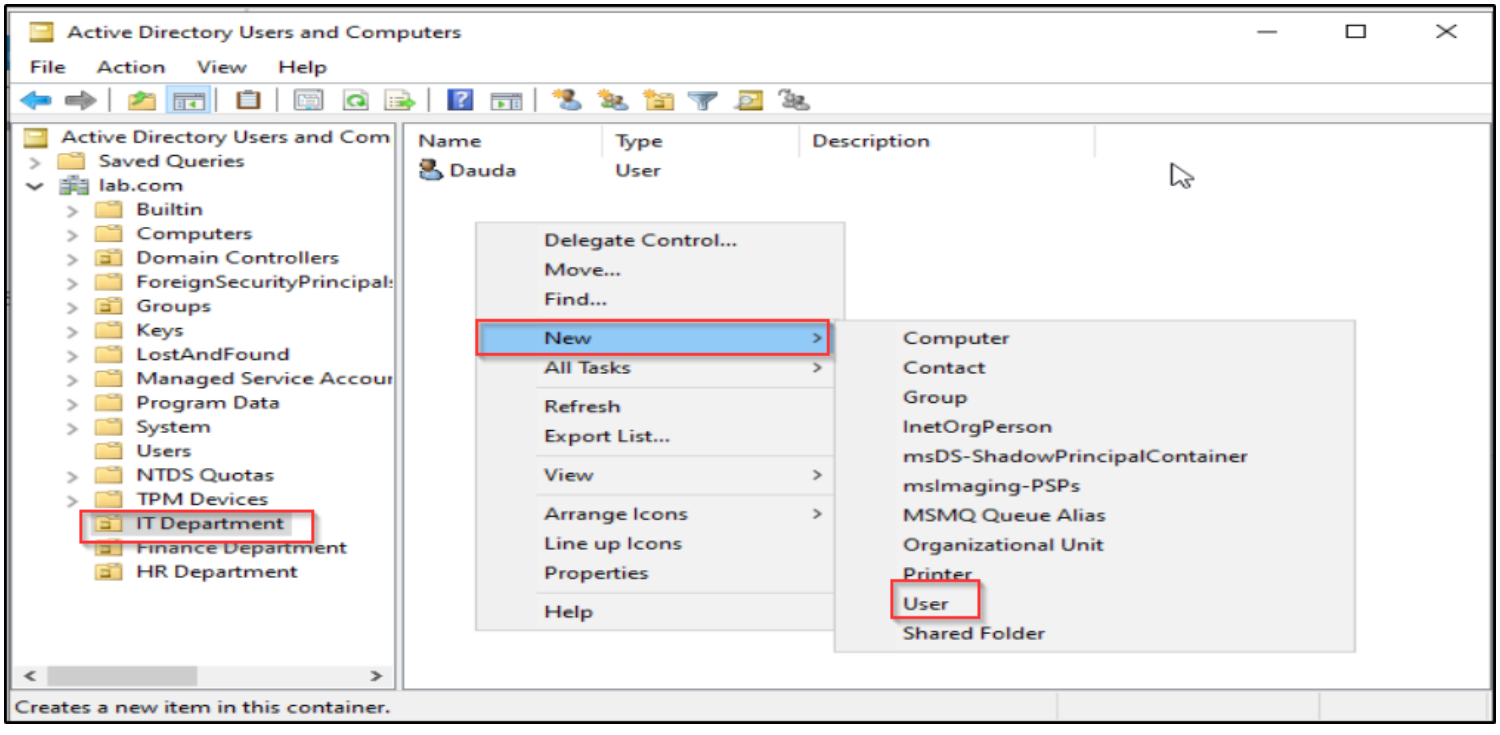
I set the account password, ensuring it met the required complexity standards, and left all other settings at their default configurations. Once the password was set, I clicked on **Next** to continue.



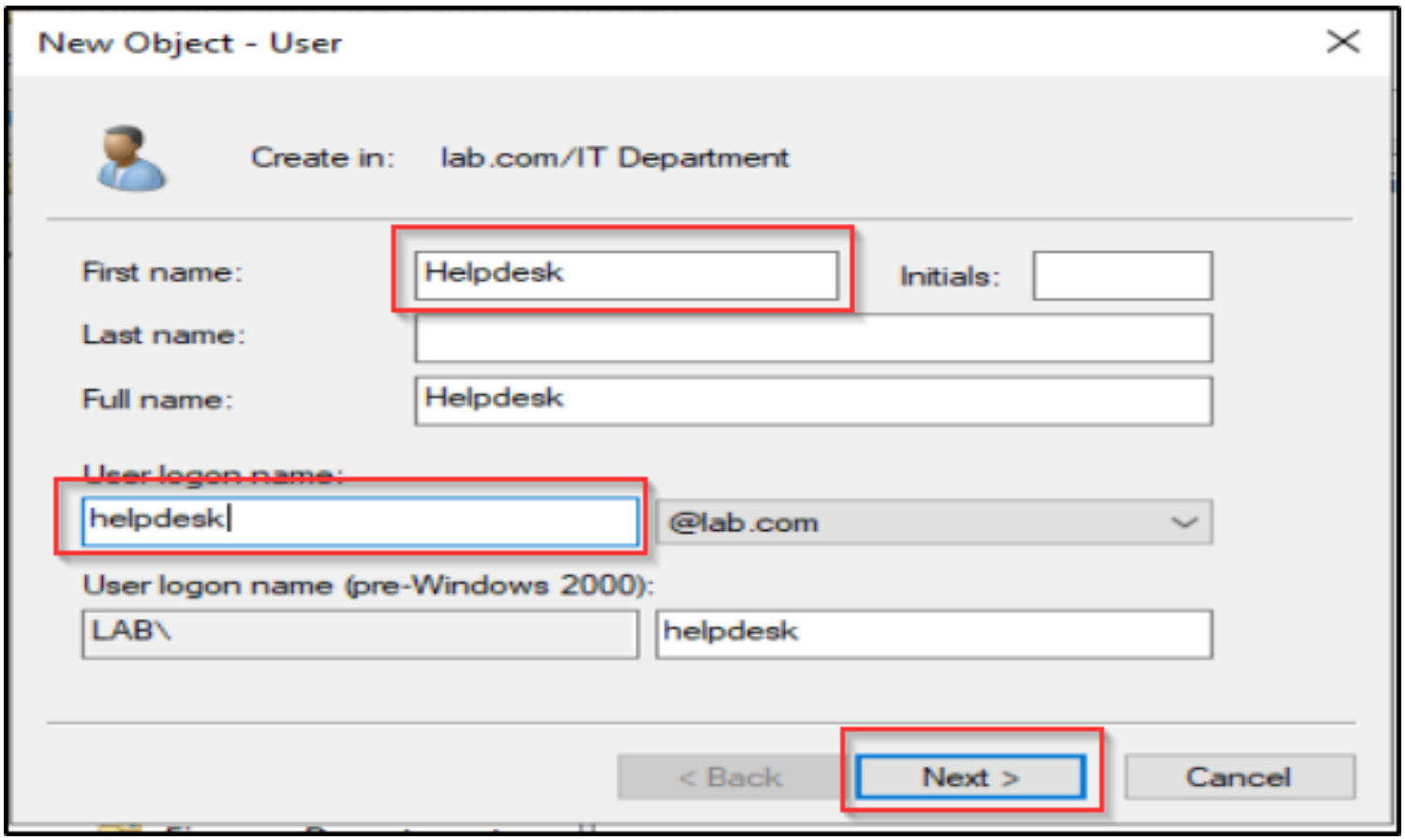
I reviewed the account information carefully to ensure accuracy, then clicked on **Finish** to complete the account creation process.



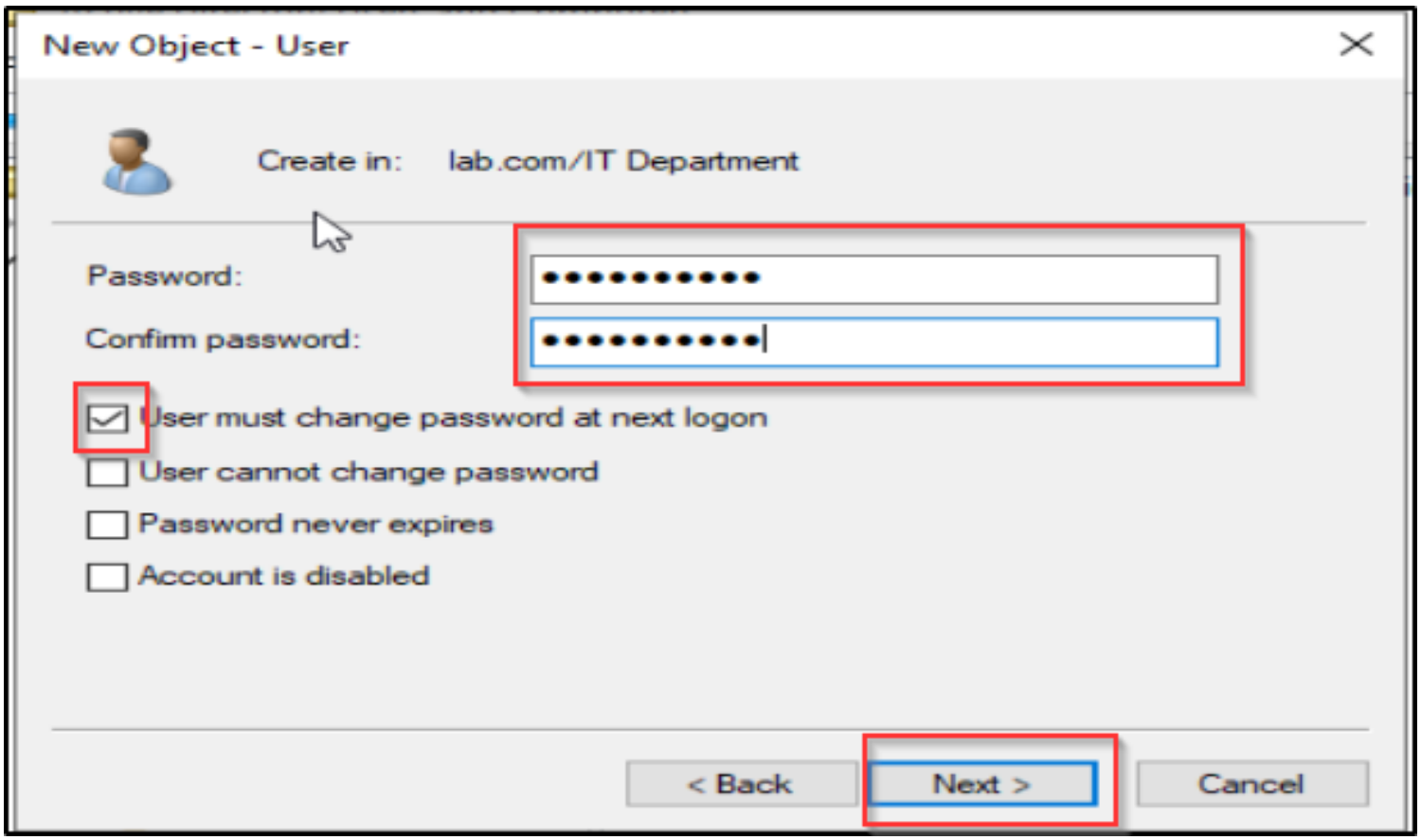
After successfully creating the first user, I clicked on the user, held down **Ctrl**, and dragged the cursor to the **IT Department**. This action moved the user from the **Users** folder to the **IT Department**.
Next, I used the second method, which is manually creating a user. I right-clicked on **IT Department**, navigated to **New**, and then clicked on **User**.



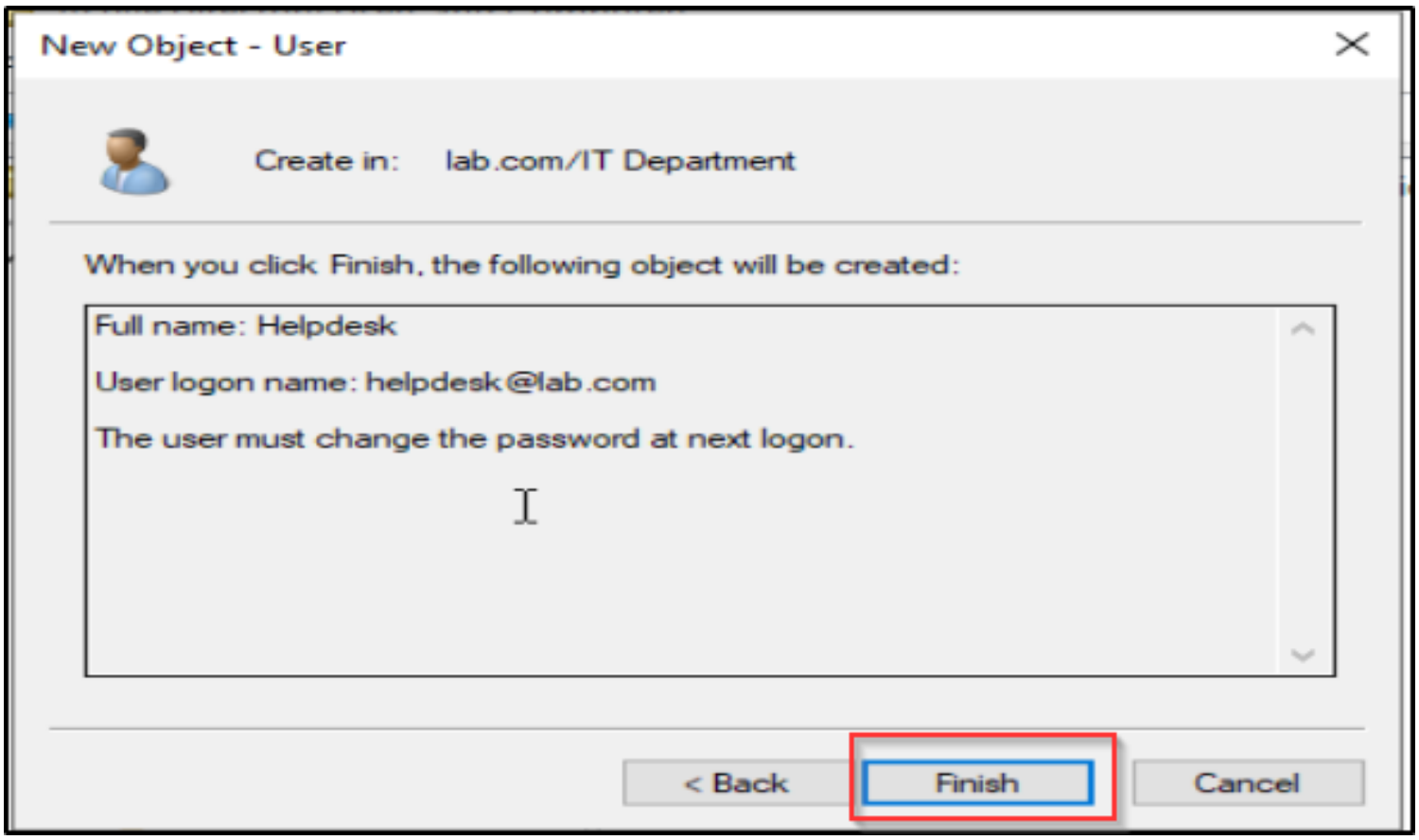
I created a new user called "Helpdesk" and clicked on **Next** after entering the username.



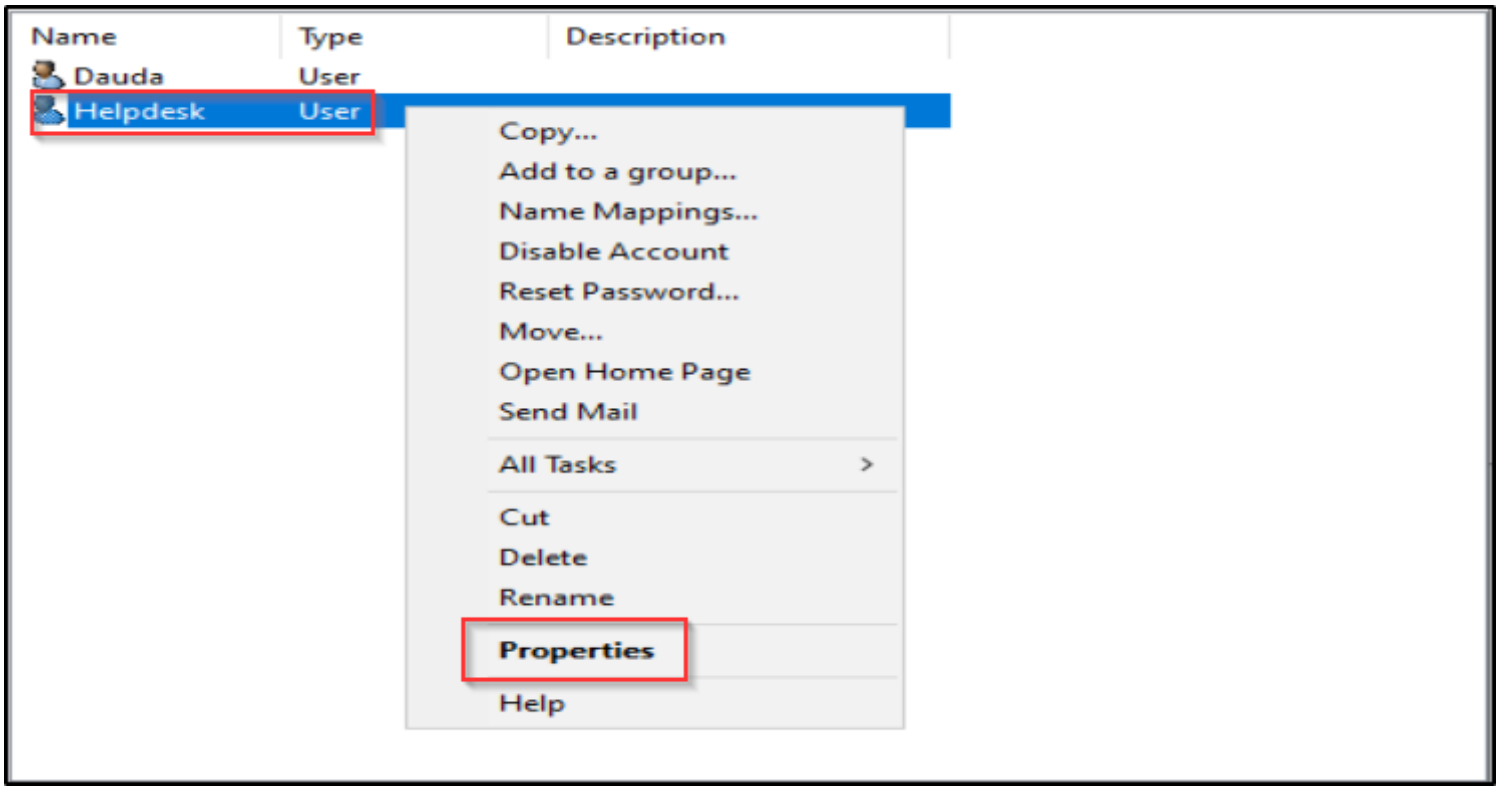
I set the user's password, ensured that the user must change the password at the next logon, and then clicked on **Next**.



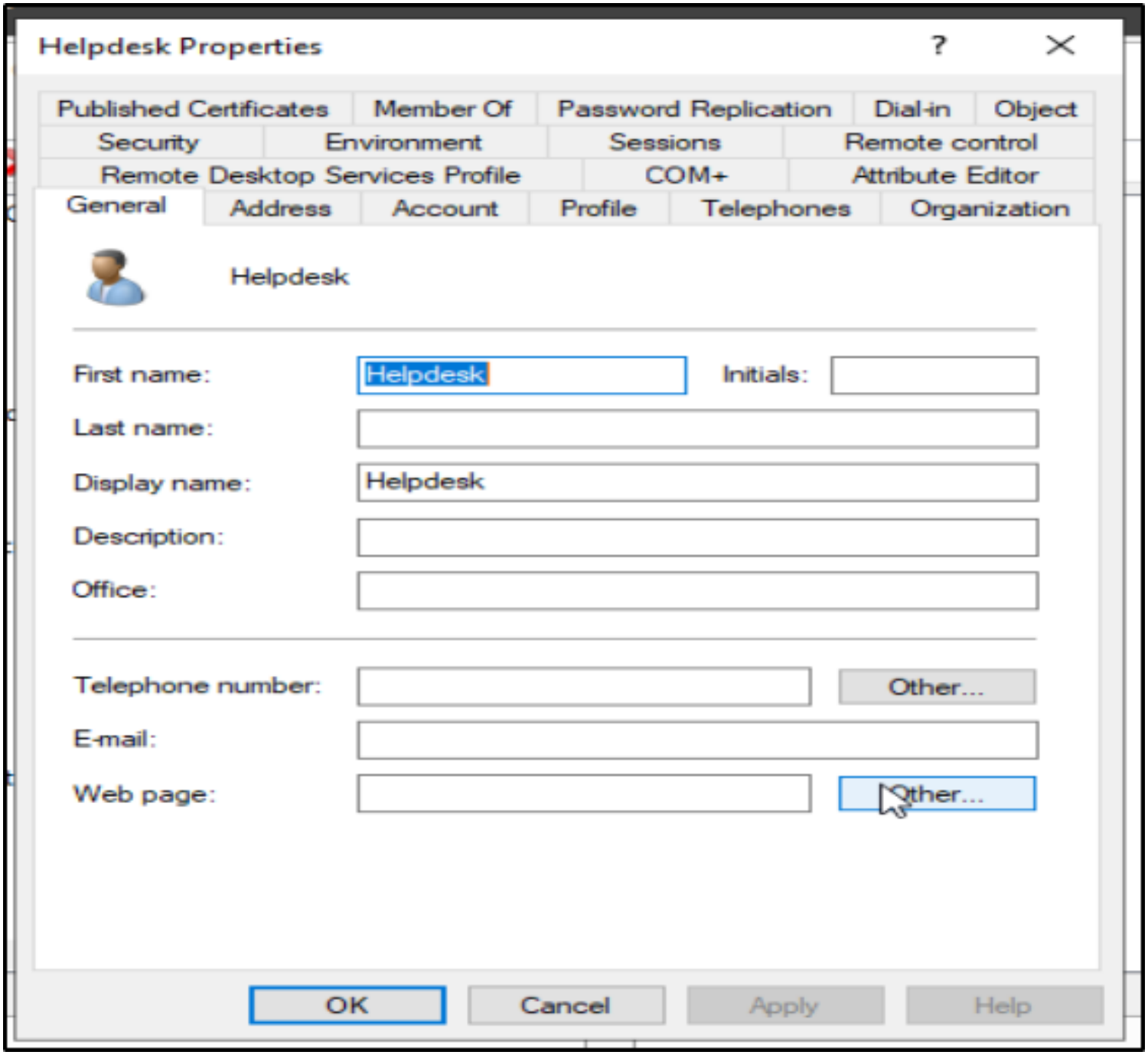
I verified the user information and clicked on **Finish**.



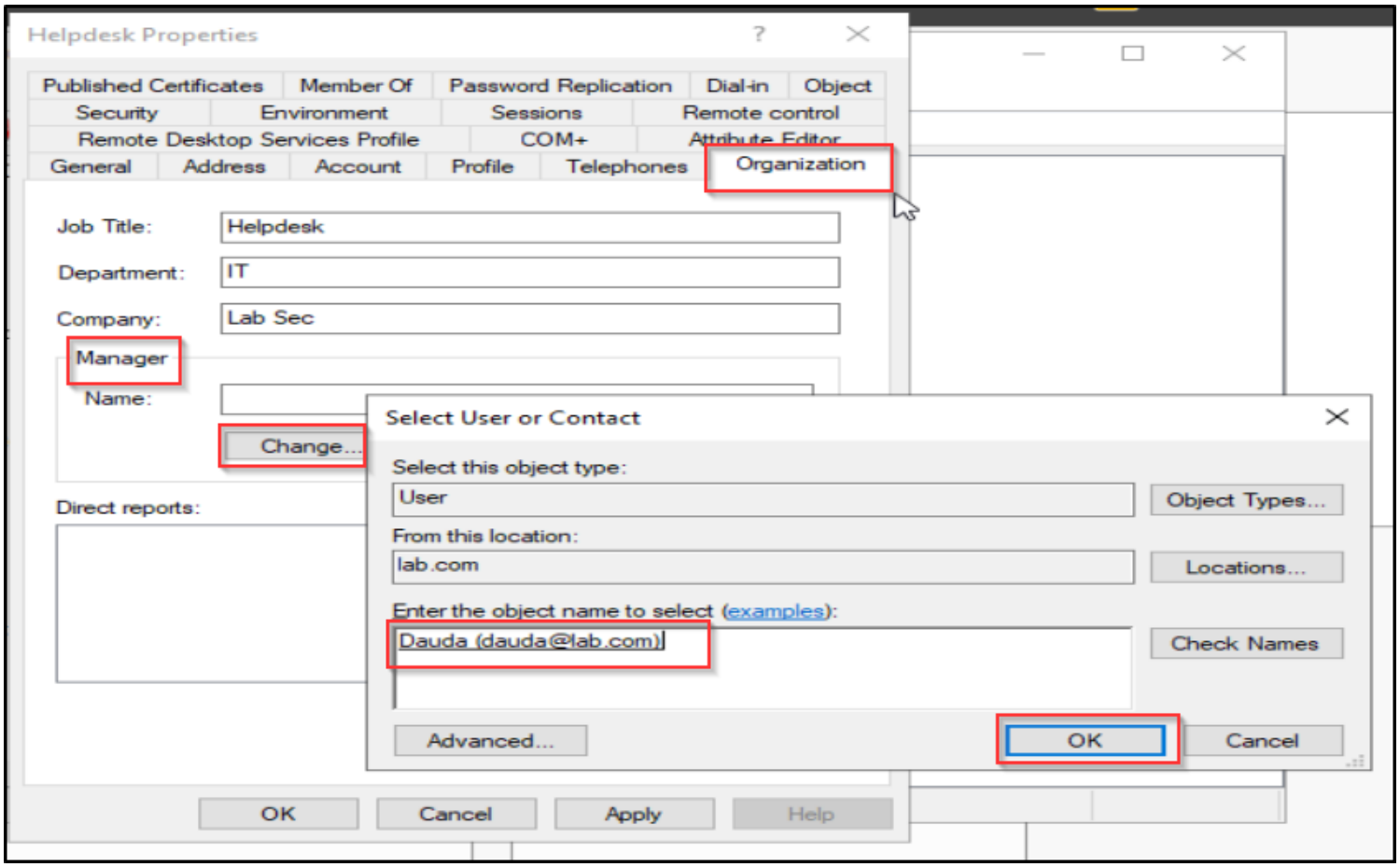
To edit user settings, I right-clicked on the user and then selected **Properties**.



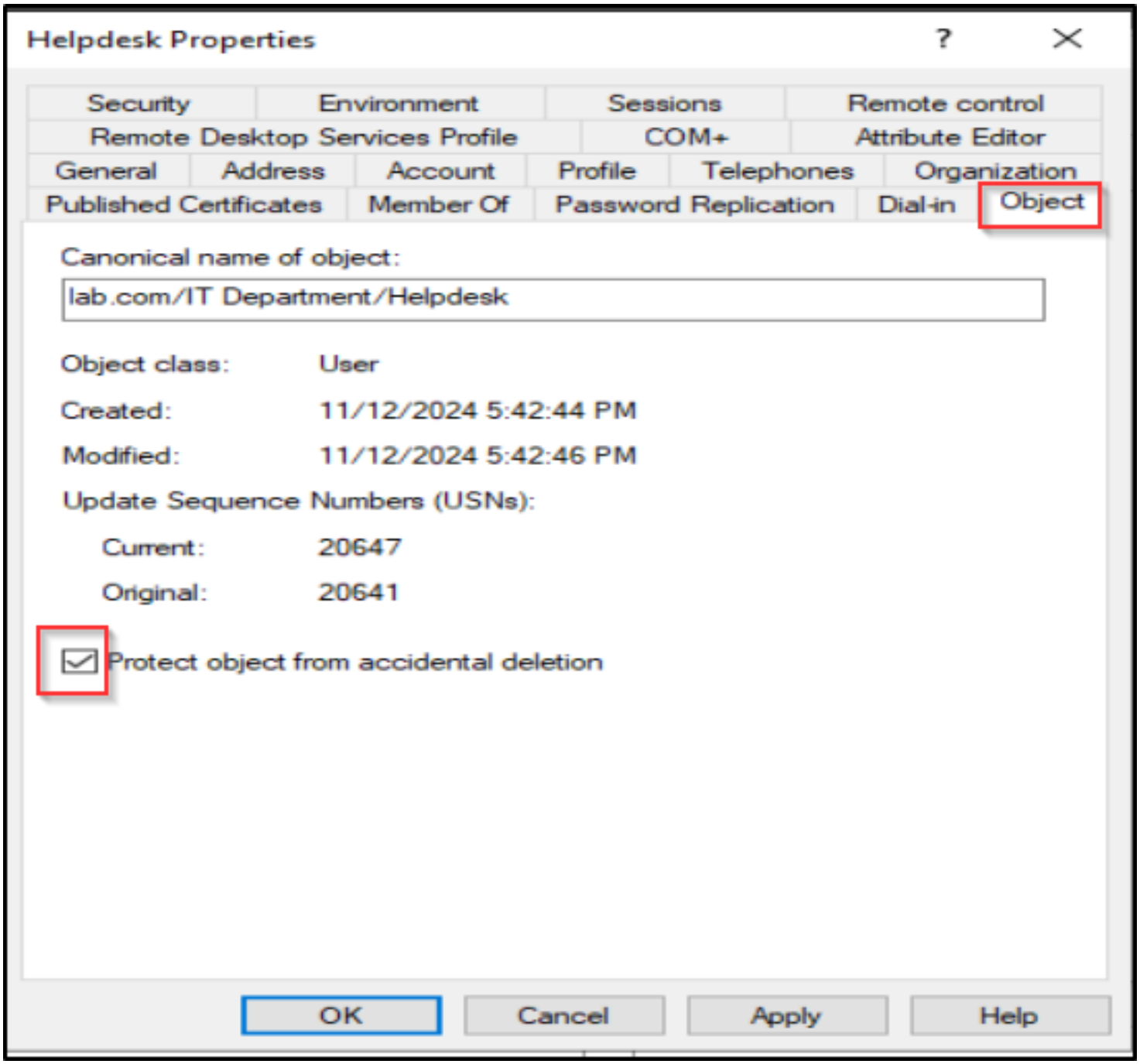
This is the **General** settings of the account



I changed to the **Organization** tab, filled in all the necessary information, and in the **Manager** field, I clicked on "Change." I then searched for the user I wanted to be the manager of this account, which was the IT Manager's account I created, and clicked on "OK."



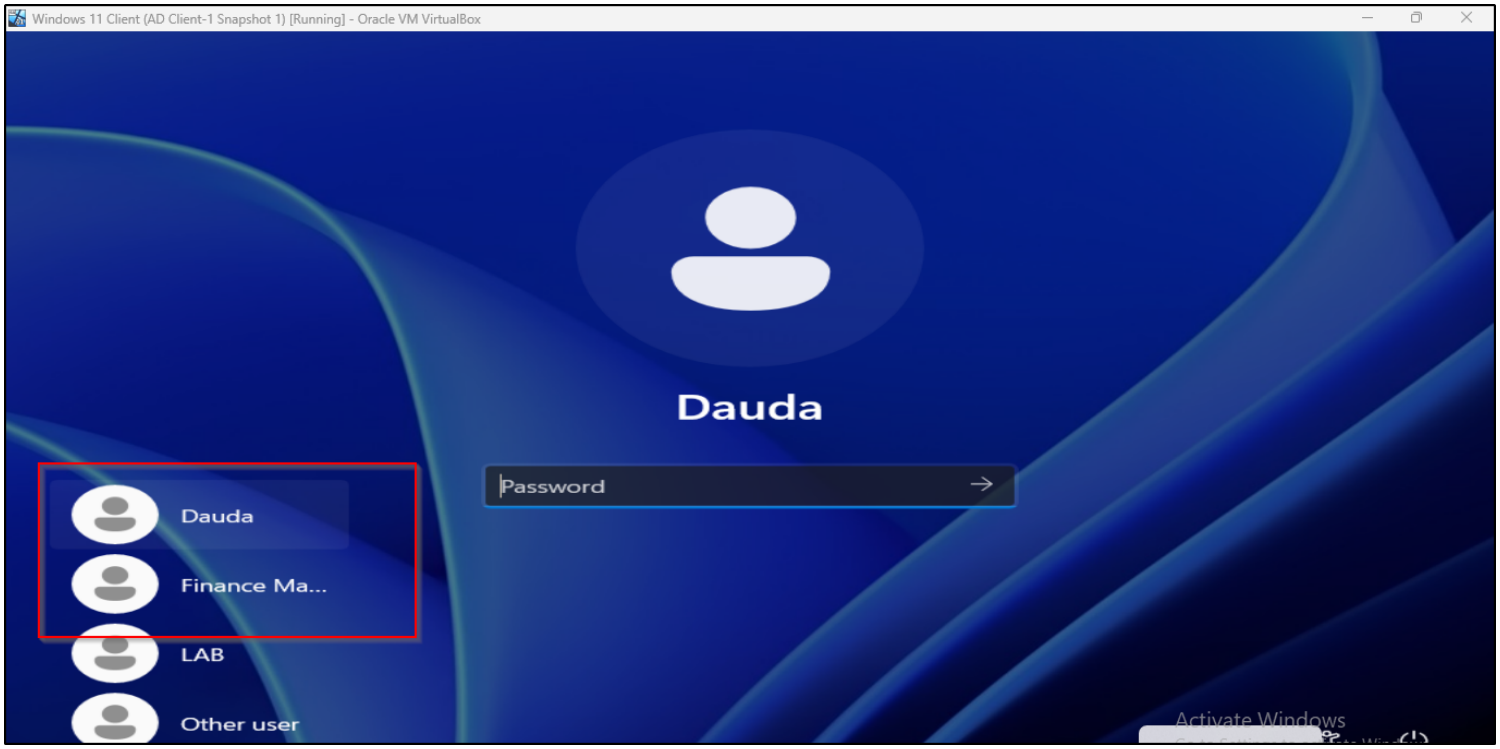
I clicked on the **Object** tab to verify the account information, then clicked on **Apply** and **OK** to save the changes.



This process continued with other users from different units. I repeated the steps for each user, carefully configuring their details and assigning the appropriate manager to each account.

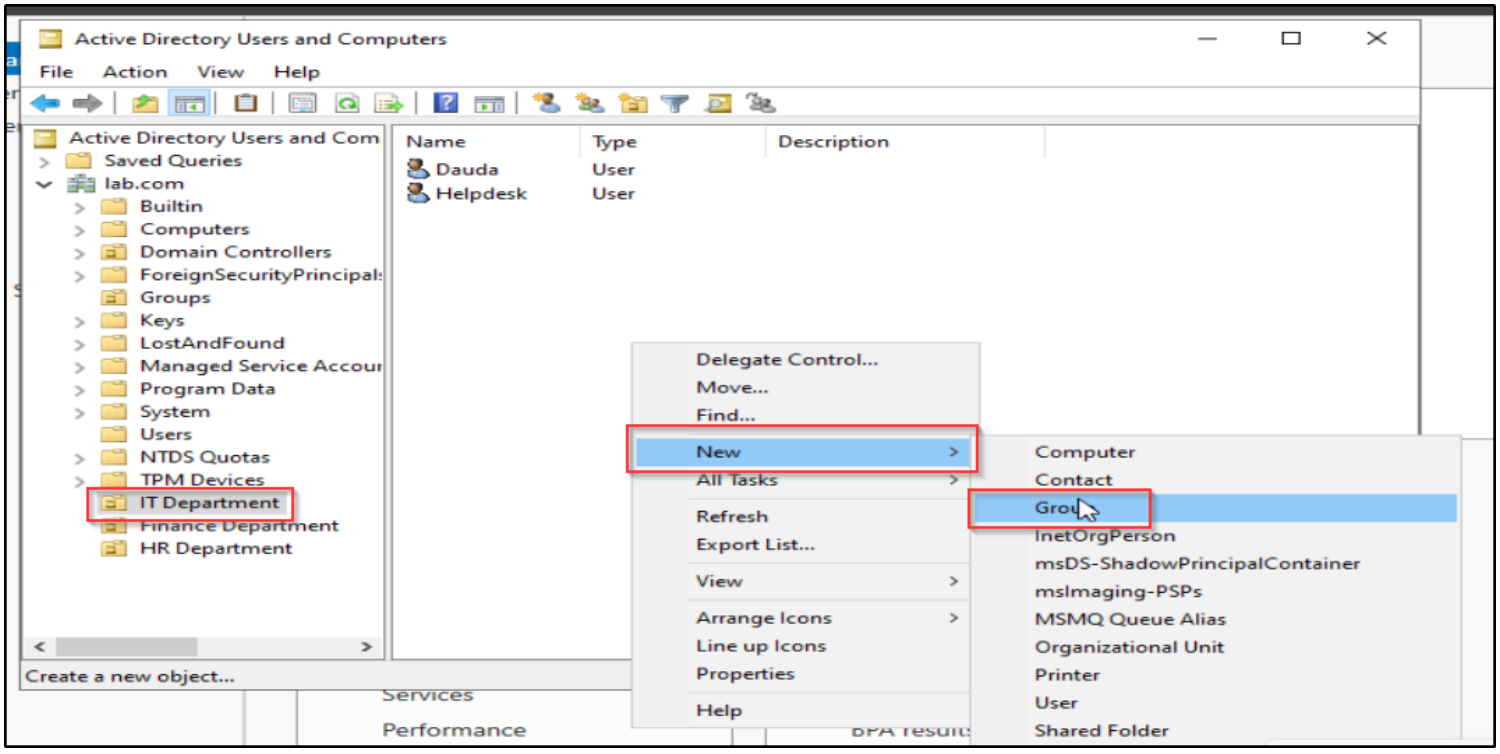
Confirmation of Accounts on Client-1

On Client-1, each user successfully confirmed access to their accounts, verifying that permissions and settings were correctly applied.

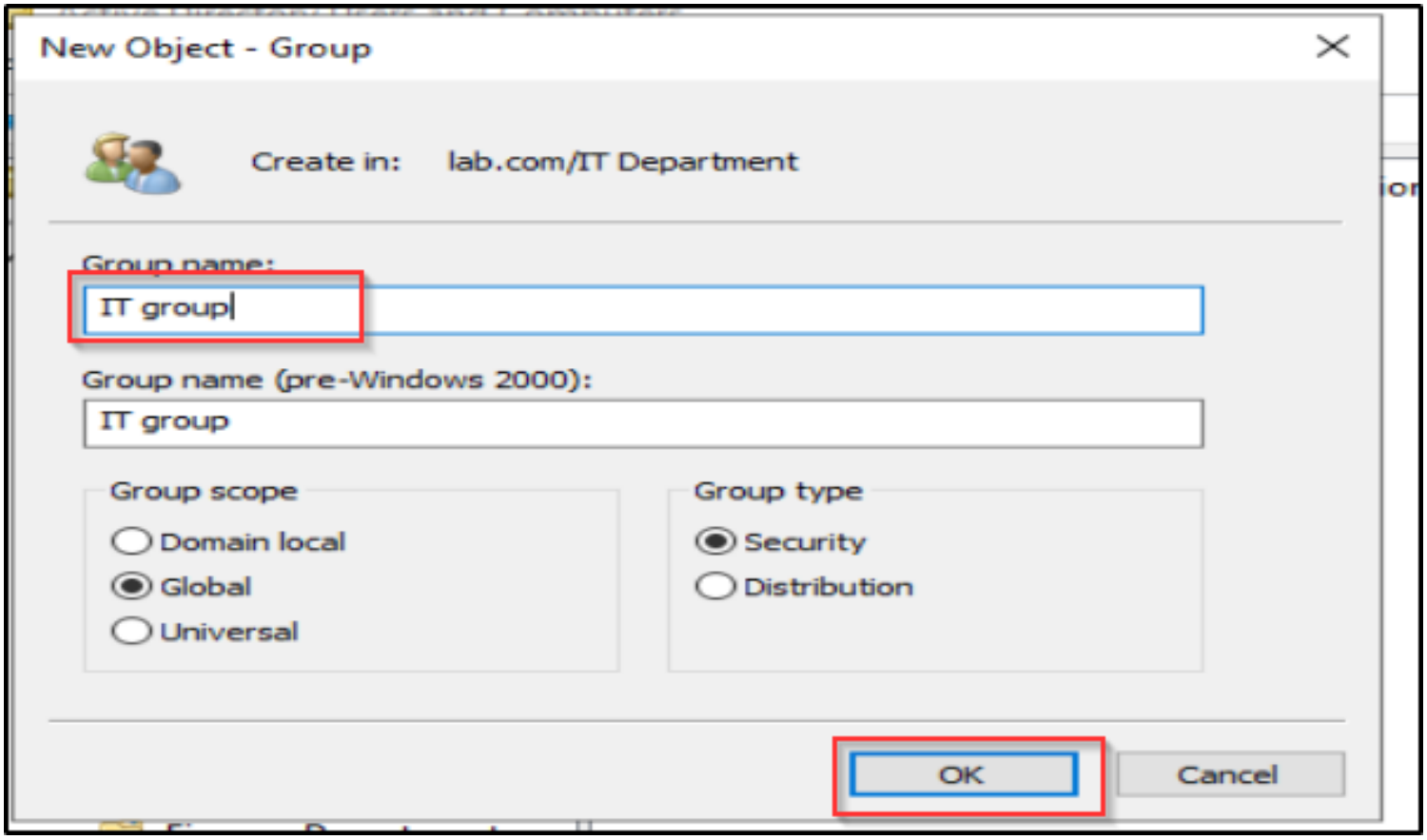


Creating Groups

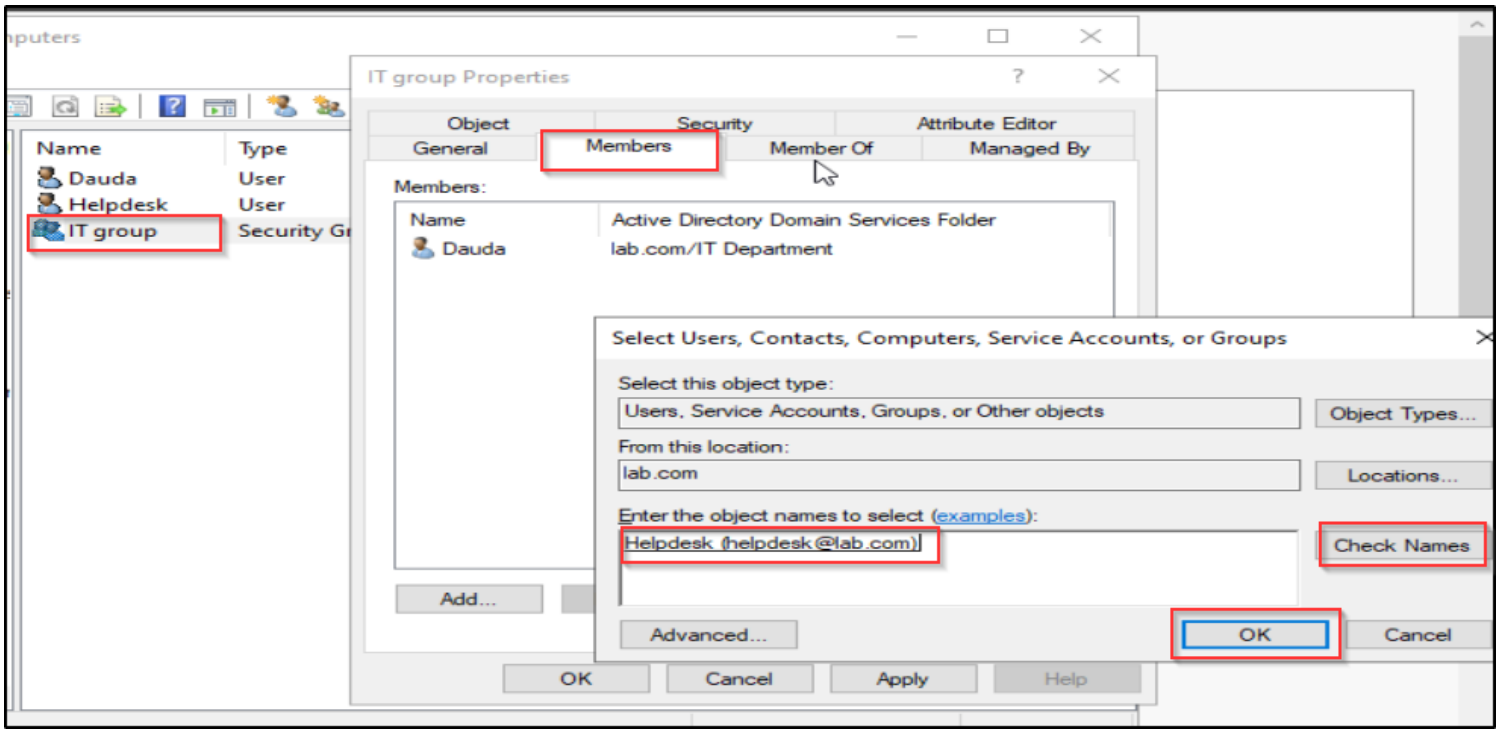
To organize users within departments, I began by creating a group for the IT department. I selected the "IT Department," right-clicked to access additional options, navigated to “New,” and selected "Group."



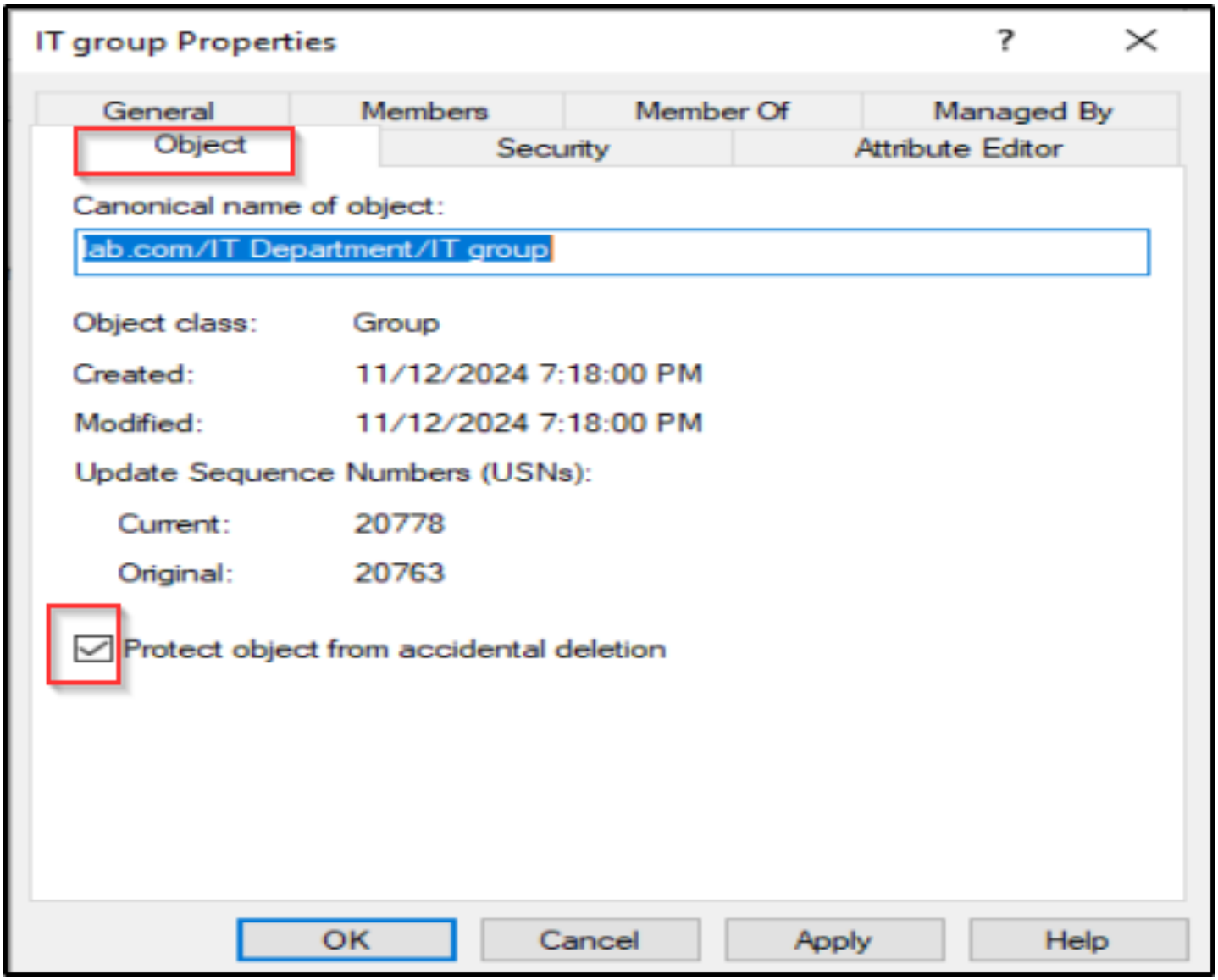
I entered “IT Group” in the Group Name field, left all other settings as default, and clicked “OK” to create the group.



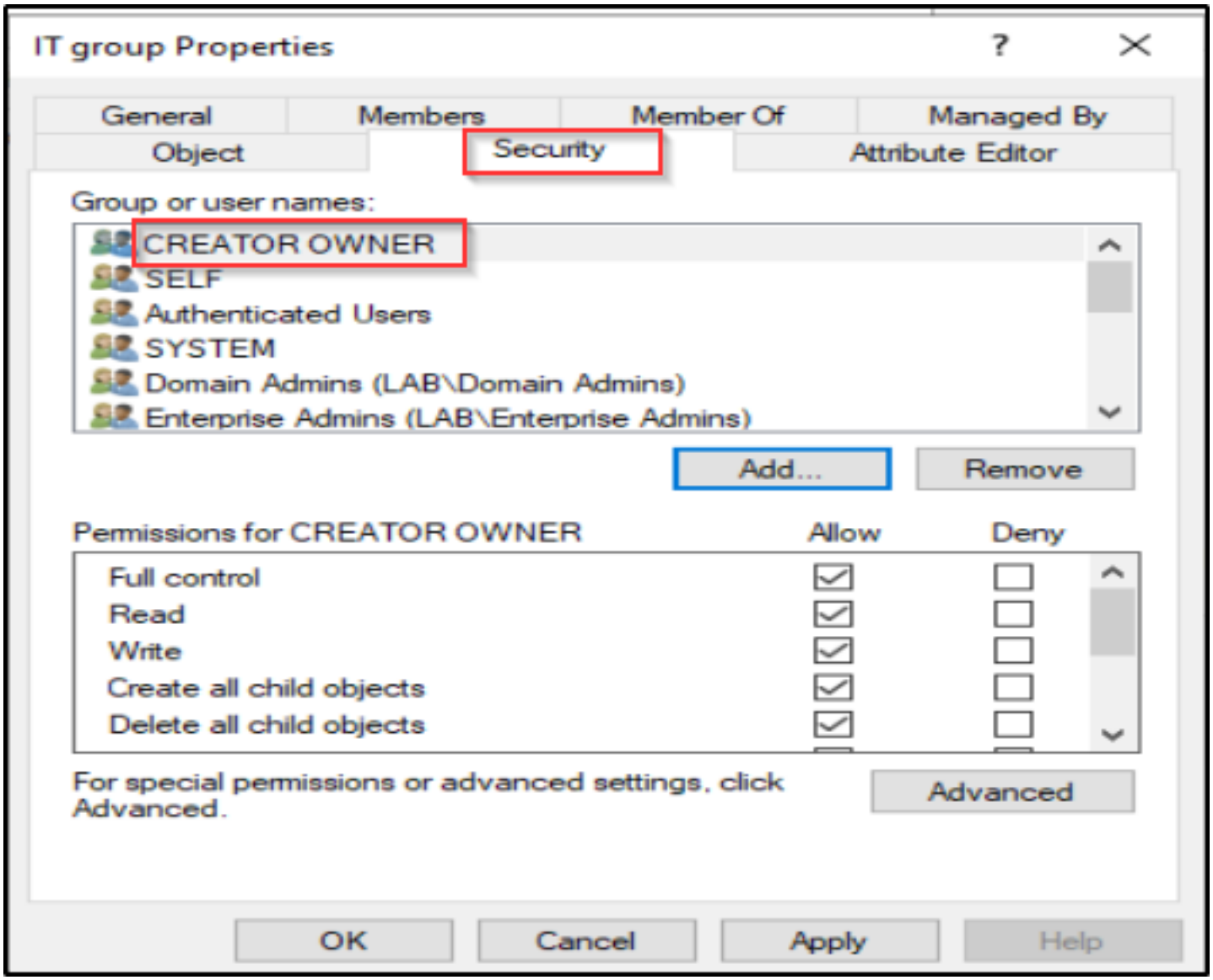
I added members to the group, such as "Dauda" and the "Helpdesk" accounts. To do this, I clicked on the **Members** tab and selected **Add**. In the new window, I searched for the account name I wanted to include, clicked on **Check Names** to confirm the account, and then clicked **OK** to add it to the group.



I selected the **Object** tab and checked the **Protect object from accidental deletion** box. This setting helps to prevent accidental removal of the group.



I then navigated to the **Security** tab to set the appropriate security permissions for the group. Once all settings were configured, I clicked **Apply** and then **OK** to save the changes.
I repeated this process to create additional groups for the **HR** and **Finance** departments, ensuring each group had the necessary permissions and members assigned accordingly.

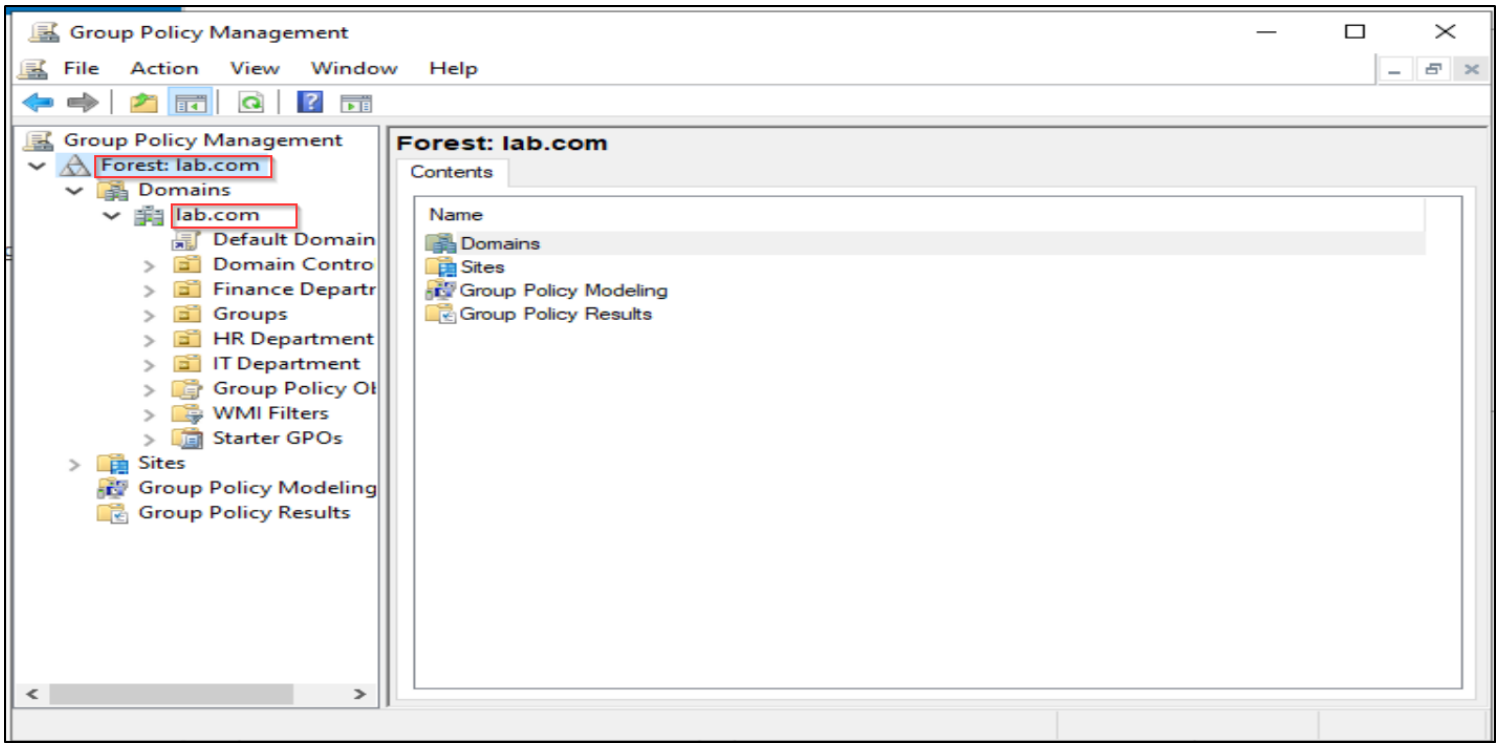

IT group Properties
General
Members
Member Of
Managed By
Object
Security
Attribute Editor
Group or user names:
CREATOR OWNER
SELF
Authenticated Users
SYSTEM
Domain Admins (LAB\Domain Admins)
Enterprise Admins (LAB\Enterprise Admins)
Add...
Remove
Permissions for CREATOR OWNER
Allow
Deny
Full control
Read
Write
Create all child objects
Delete all child objects
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help

Security

Applying Group Policies.

To apply group policies, I opened the "Server Manager" navigate to the "Tools" area and select the "Group Policy Management"

I start by creating "Account Lockout Ploicy" for all users and computers.
For the sake of limited hardware resources, I Created only one Clients. Therefore the single client will be used for all objects.



Creating an "Account Lockout Policy"

Why?

Applying an **Account Lockout Policy** is an important security measure designed to prevent unauthorized access to accounts within a domain. Here's why it's beneficial:
1. **Protection Against Brute-Force Attacks**:
• An account lockout policy helps protect against brute-force attacks, where an attacker attempts multiple password guesses to gain access to user accounts. By limiting the number of failed login attempts, it reduces the risk of attackers guessing passwords through repeated attempts.

• **Mitigates Insider Threats**:
◇ In addition to external threats, an account lockout policy helps guard against potential misuse by insiders who may try to access unauthorized accounts within the network.

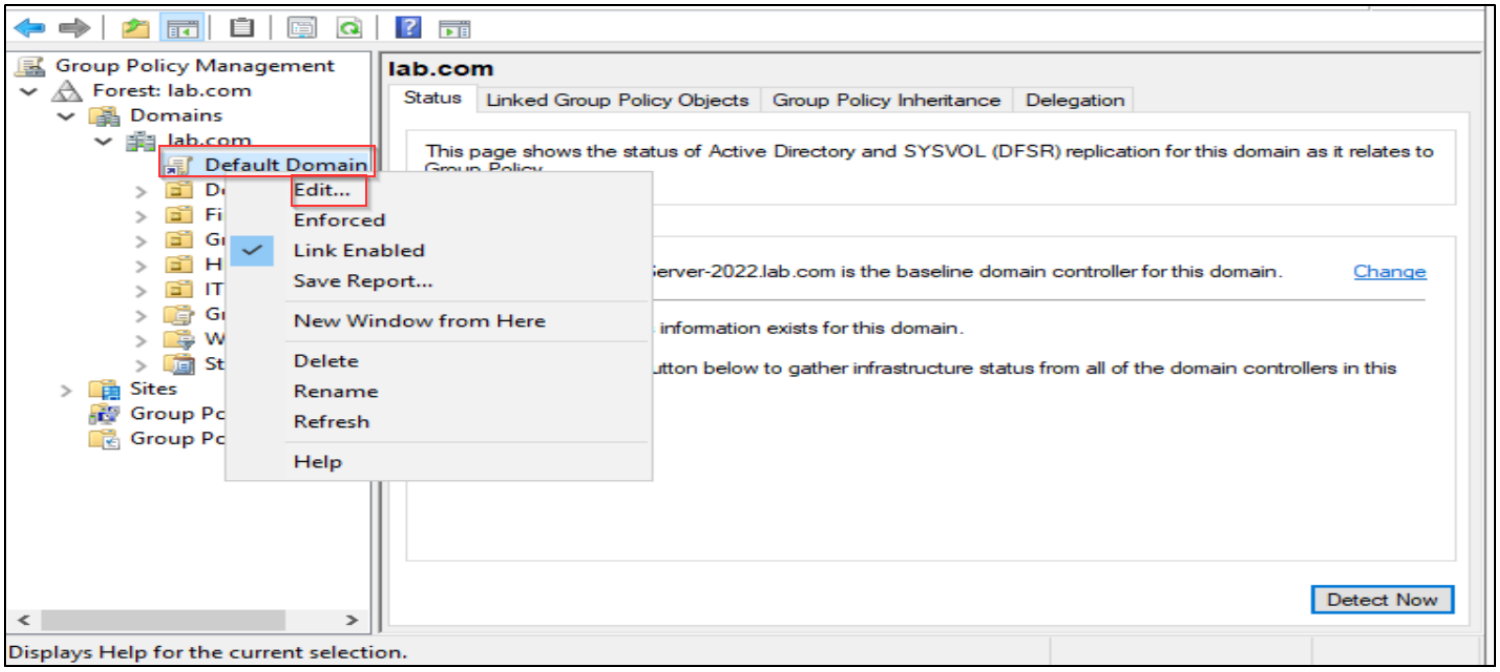
• **Alerts to Potential Security Incidents**:
◇ Frequent account lockouts can signal attempted unauthorized access. Administrators can investigate repeated lockouts as potential indicators of attempted attacks or misconfigurations in the system.

• **Maintains Compliance**:
◇ Many organizations must adhere to security standards and compliance requirements (e.g., HIPAA, PCI-DSS, and ISO standards) that mandate controls for user authentication, including account lockout settings.

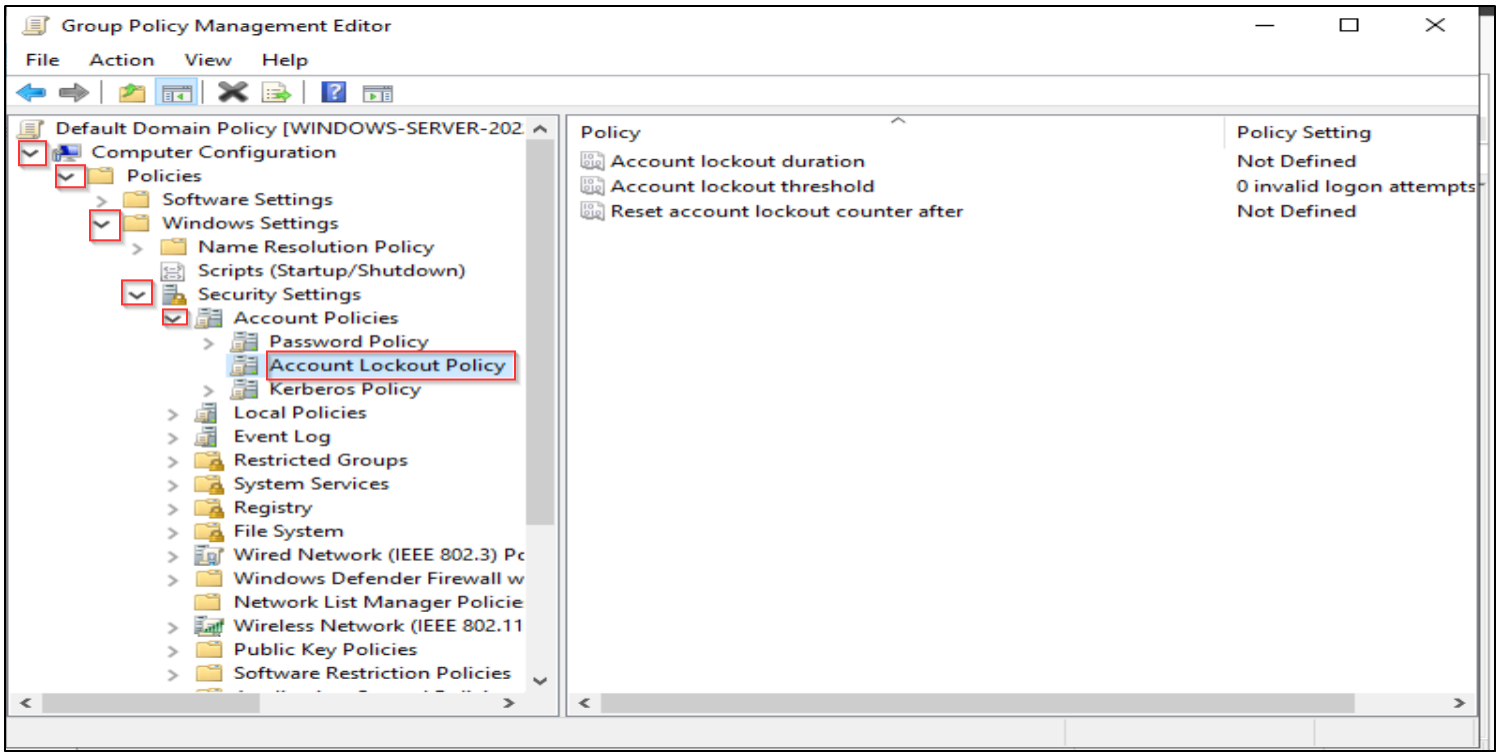
• **Enhances Security for Remote Access**:
◇ With many users accessing corporate networks remotely, account lockout policies add an extra layer of security against external login attempts that could compromise sensitive resources.

However, while an account lockout policy enhances security, it must be configured with balance. Setting the **lock-out threshold** too low can lead to users being locked out by accidental login mistakes, while setting it too high may not provide adequate protection against guessing attacks.

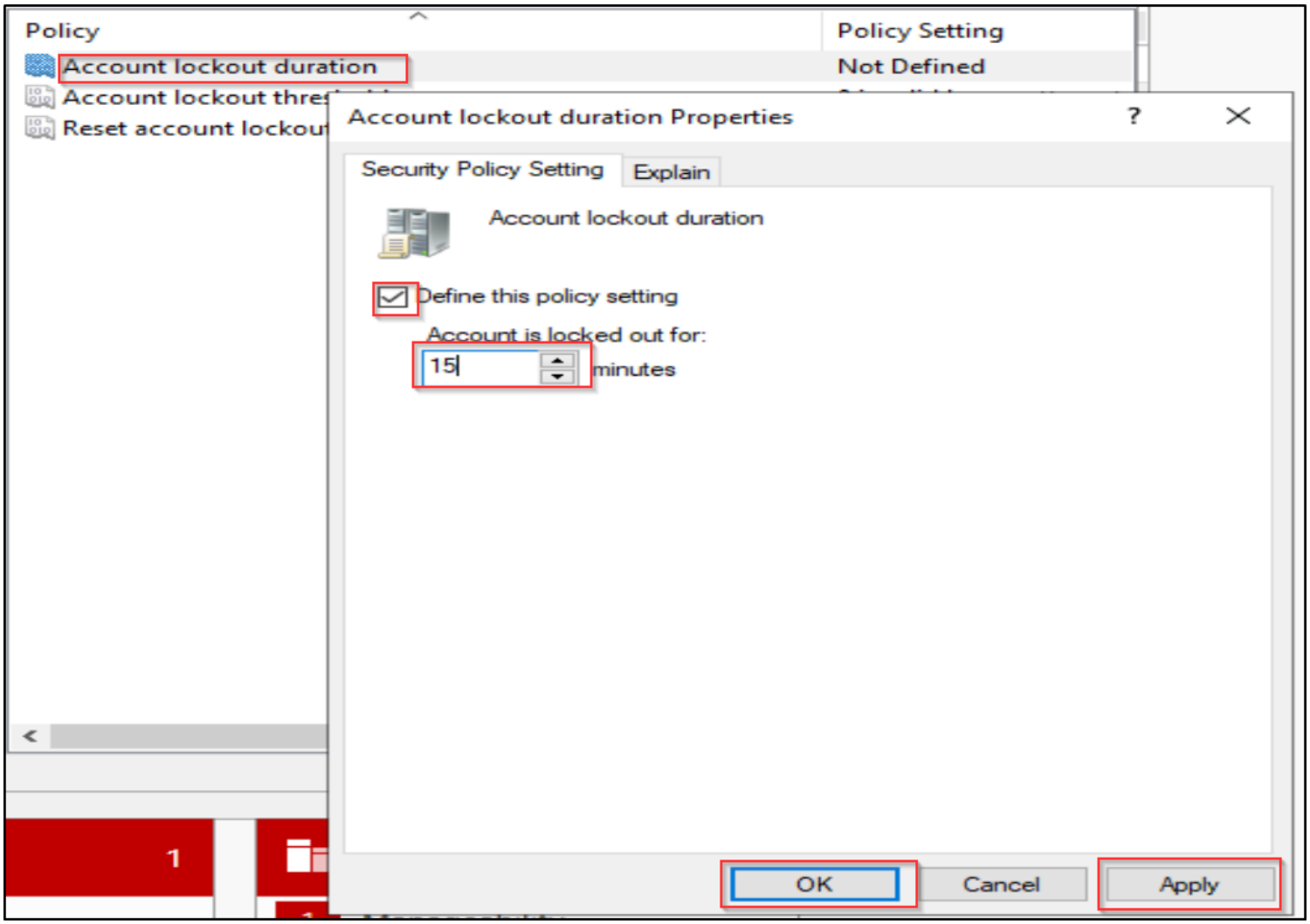
To set this policy, I right-clicked on the "Default Domain Policy" and then clicked on "Edit."



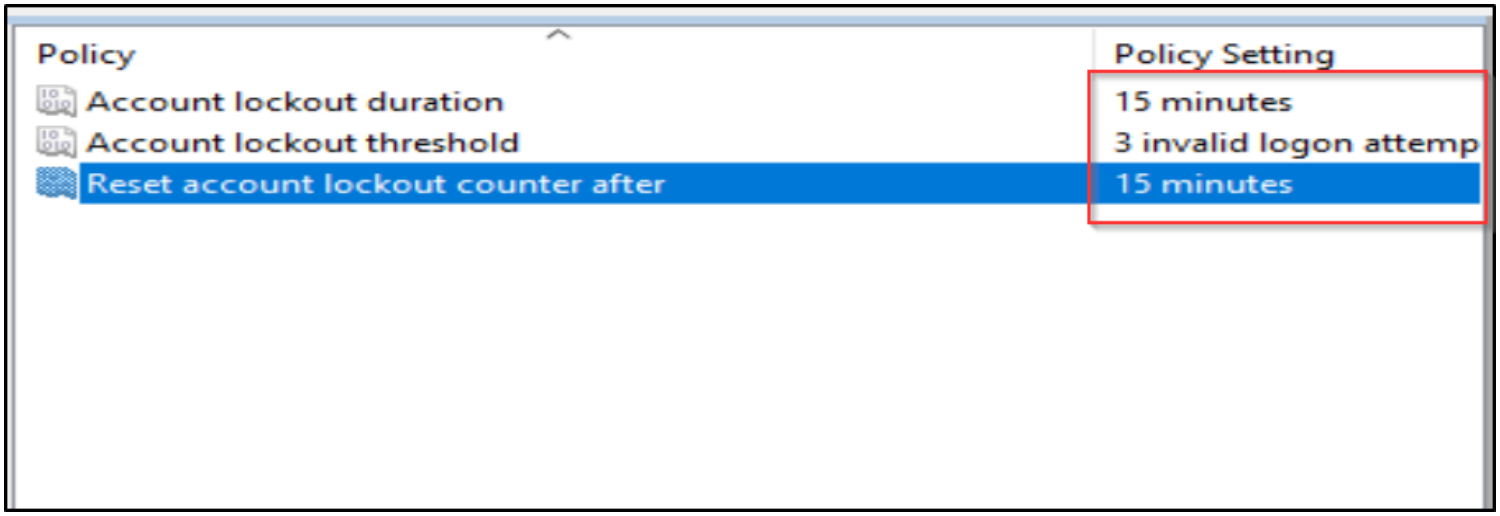
Here, I navigated from "Computer Configuration" to "Account Policy" and then selected "Account Lockout Policy."



I then edited the policy settings.



And these are the final policy settings:



Creating Password Policy

Why?

Creating a **Password Policy** is essential to secure accounts and protect sensitive information within an organization's network. Here are the key reasons for implementing a password policy:

1. **Prevents Easy-to-Guess Passwords**:

• A strong password policy requires users to create complex passwords that are difficult for attackers to guess or brute-force. By enforcing length, character variety, and other requirements, the policy reduces the chances of weak passwords like "password123" or "admin."

• **Protects Against Unauthorized Access**:

◇ Password policies prevent unauthorized access by ensuring that each user account has a secure password. This makes it harder for attackers to break into accounts and gain access to sensitive resources or systems.

• **Reduces Impact of Phishing Attacks**:

◇ By enforcing regular password changes, the policy limits the effectiveness of phishing attacks. Even if a password is stolen, requiring users to update passwords regularly reduces the timeframe an attacker can use it.

• **Limits Risks of Reused Passwords**:

◇ Password policies can prevent users from reusing passwords. Since reused passwords are often used across multiple sites, preventing reuse reduces the risk if another site suffers a data breach that exposes passwords.

• **Supports Regulatory Compliance**:

◇ Many regulations and standards (like GDPR, HIPAA, and PCI-DSS) require organizations to implement password policies as part of their security protocols to protect customer data and sensitive information.

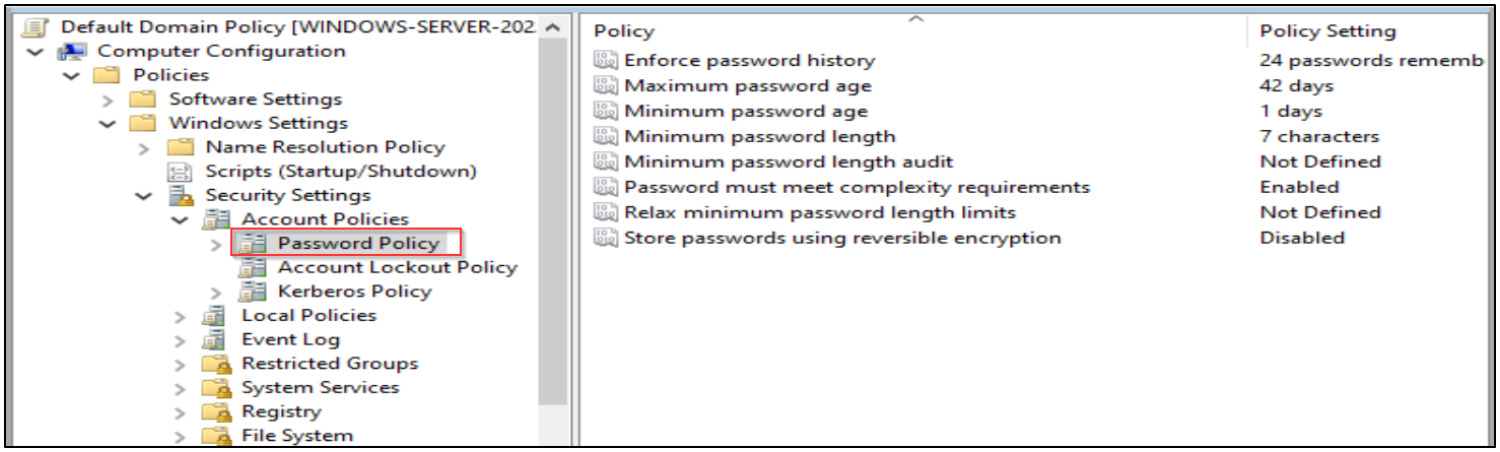
• **Mitigates Insider Threats**:

◇ A strong password policy also protects against potential threats from insiders by ensuring all users follow the same security standards, reducing the likelihood of weak or shared passwords that could lead to unauthorized access.

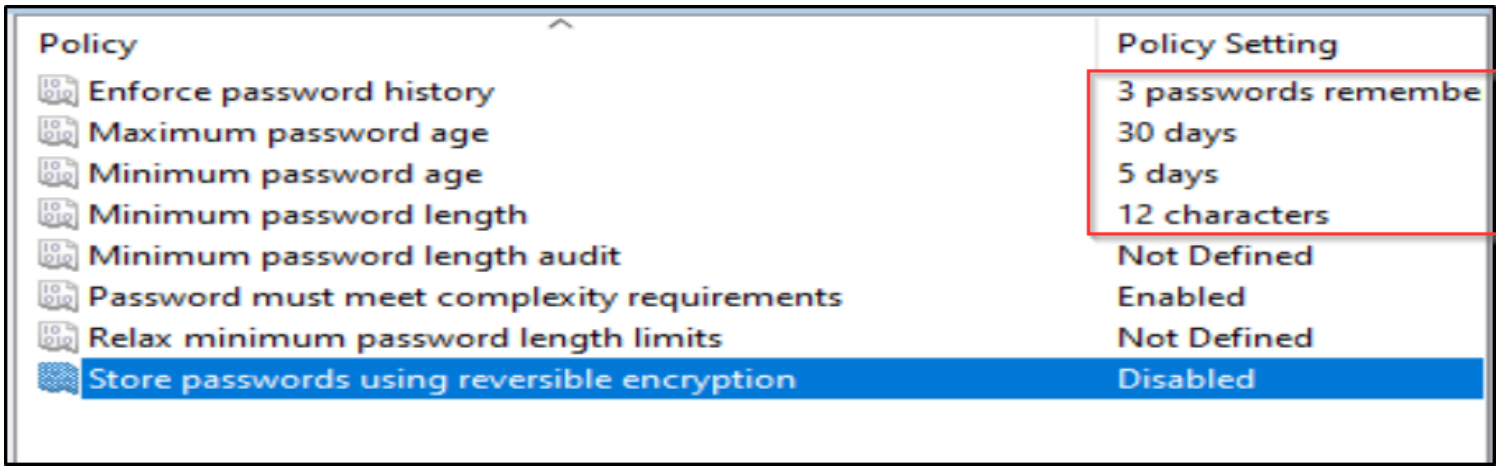
• **Encourages Good Security Habits**:
◇ A password policy can serve as an educational tool, helping users understand the importance of strong passwords and encouraging better password management practices, such as avoiding common passwords and using secure password storage methods.

By implementing a password policy, organizations can enforce security standards that protect their systems, maintain compliance, and encourage users to follow good password practices, ultimately strengthening overall network security.

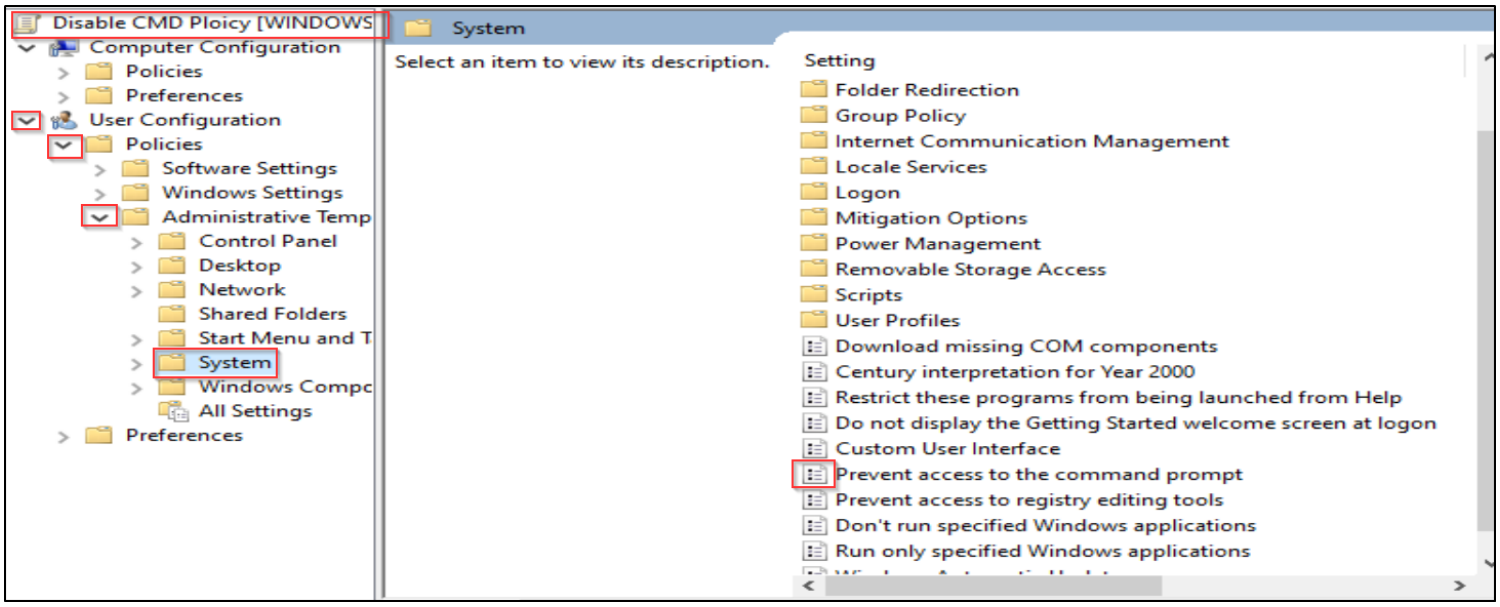
I clicked on "Password Policy" and edited the "Policy Settings."



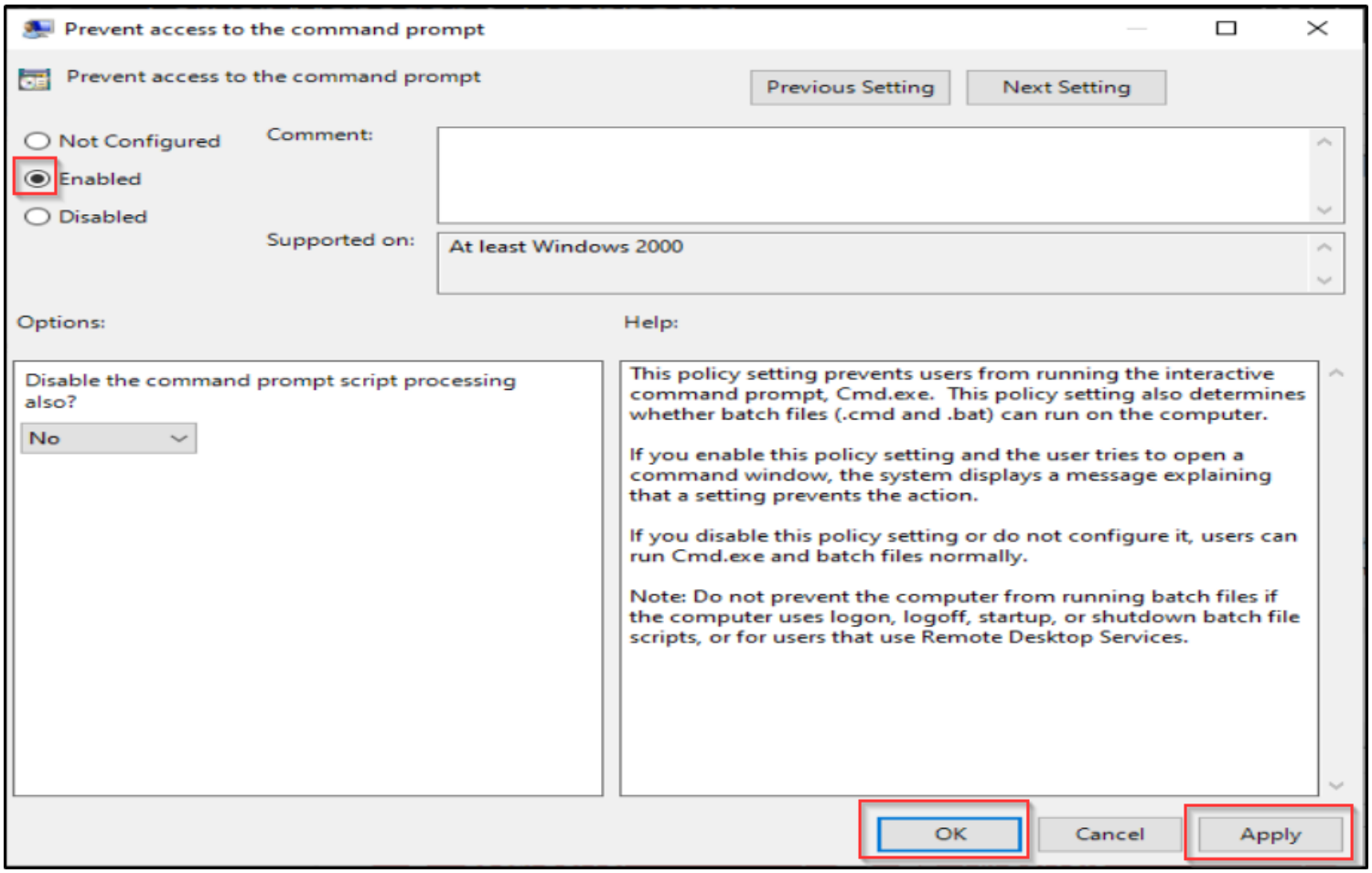
Here are the edited "Policy Settings":



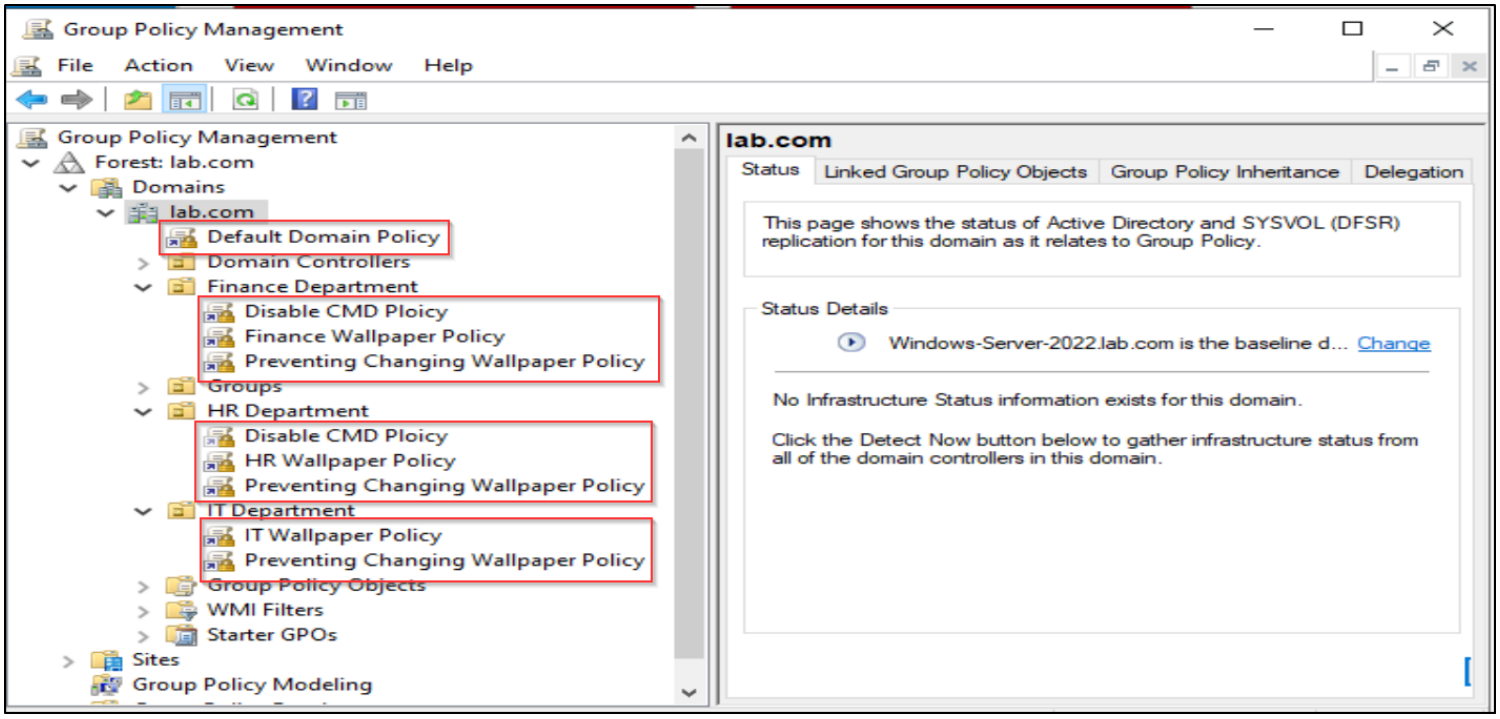
I also set up a CMD Disable Policy to prevent users from running the command line.
I navigated to the "System Policy" under User Configuration, and then clicked on "Prevent access to the Command Prompt."

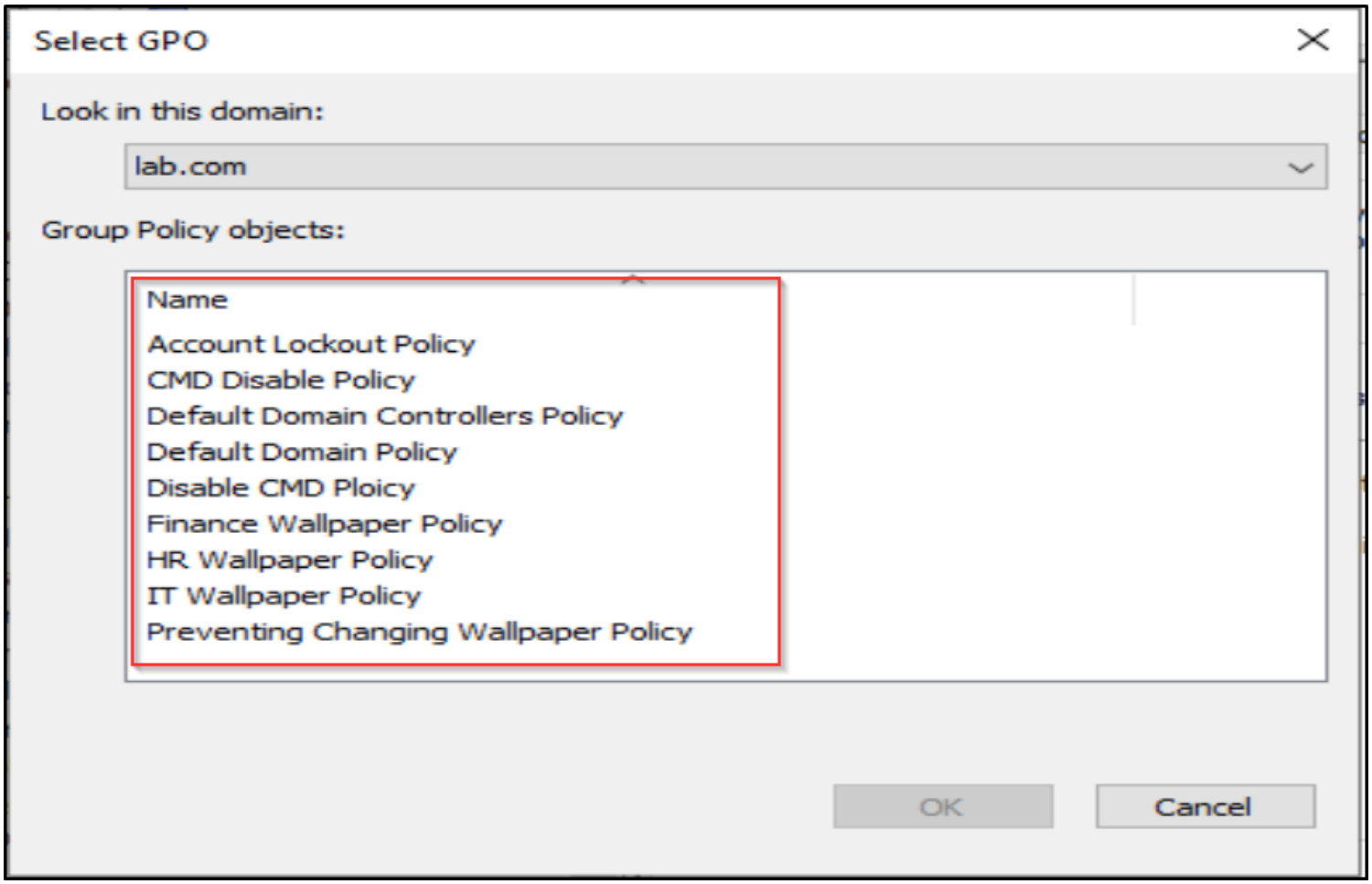


I selected "Enabled," clicked on "Apply," and then clicked on "OK."



These are a few of the policies I created.

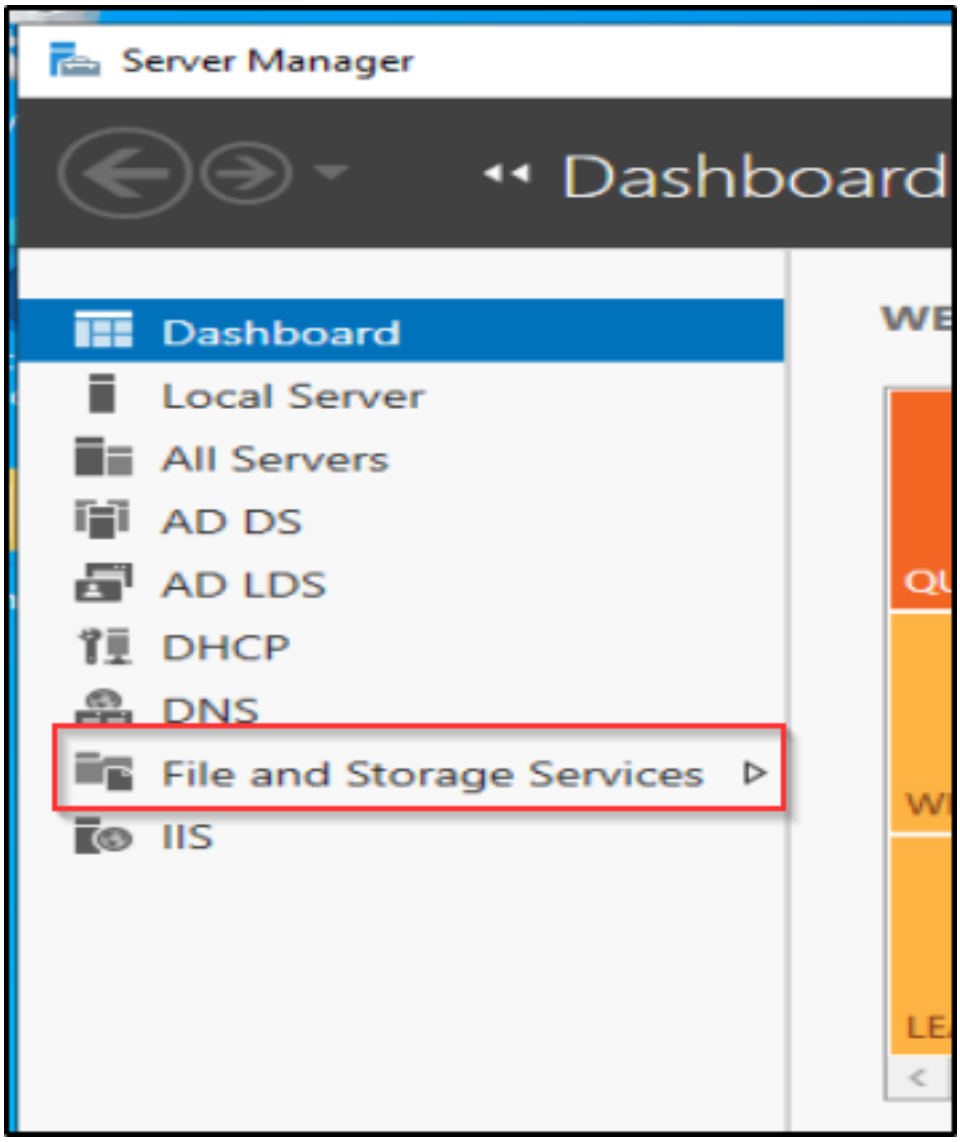

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: lab.com
Domains
lab.com
Default Domain Policy
Domain Controllers
Finance Department
Disable CMD Ploicy
Finance Wallpaper Policy
Preventing Changing Wallpaper Policy
Groups
HR Department
Disable CMD Ploicy
HR Wallpaper Policy
Preventing Changing Wallpaper Policy
IT Department
IT Wallpaper Policy
Preventing Changing Wallpaper Policy
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
lab.com
Status
Linked Group Policy Objects
Group Policy Inheritance
Delegation
This page shows the status of Active Directory and SYSVOL (DFSR) replication for this domain as it relates to Group Policy.
Status Details
Windows-Server-2022.lab.com is the baseline d... Change
No Infrastructure Status information exists for this domain.
Click the Detect Now button below to gather infrastructure status from all of the domain controllers in this domain.


Select GPO
Look in this domain:
lab.com
Group Policy objects:
Name
Account Lockout Policy
CMD Disable Policy
Default Domain Controllers Policy
Default Domain Policy
Disable CMD Ploicy
Finance Wallpaper Policy
HR Wallpaper Policy
IT Wallpaper Policy
Preventing Changing Wallpaper Policy
OK
Cancel

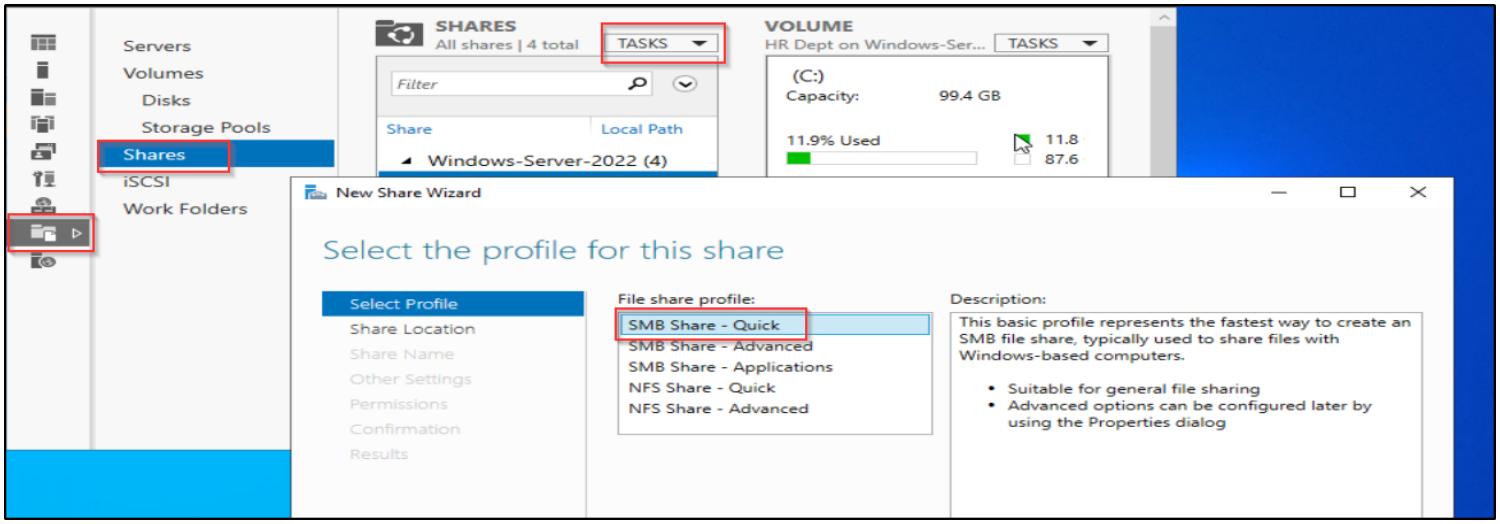
Create a Share Folders and Files

Creating a Shared Drive
Creating a shared drive allows multiple users or departments to access and collaborate on files centrally stored on the server. This improves data organization, ensures consistent backups, and facilitates controlled access through permissions, enhancing both security and efficiency within an organization.

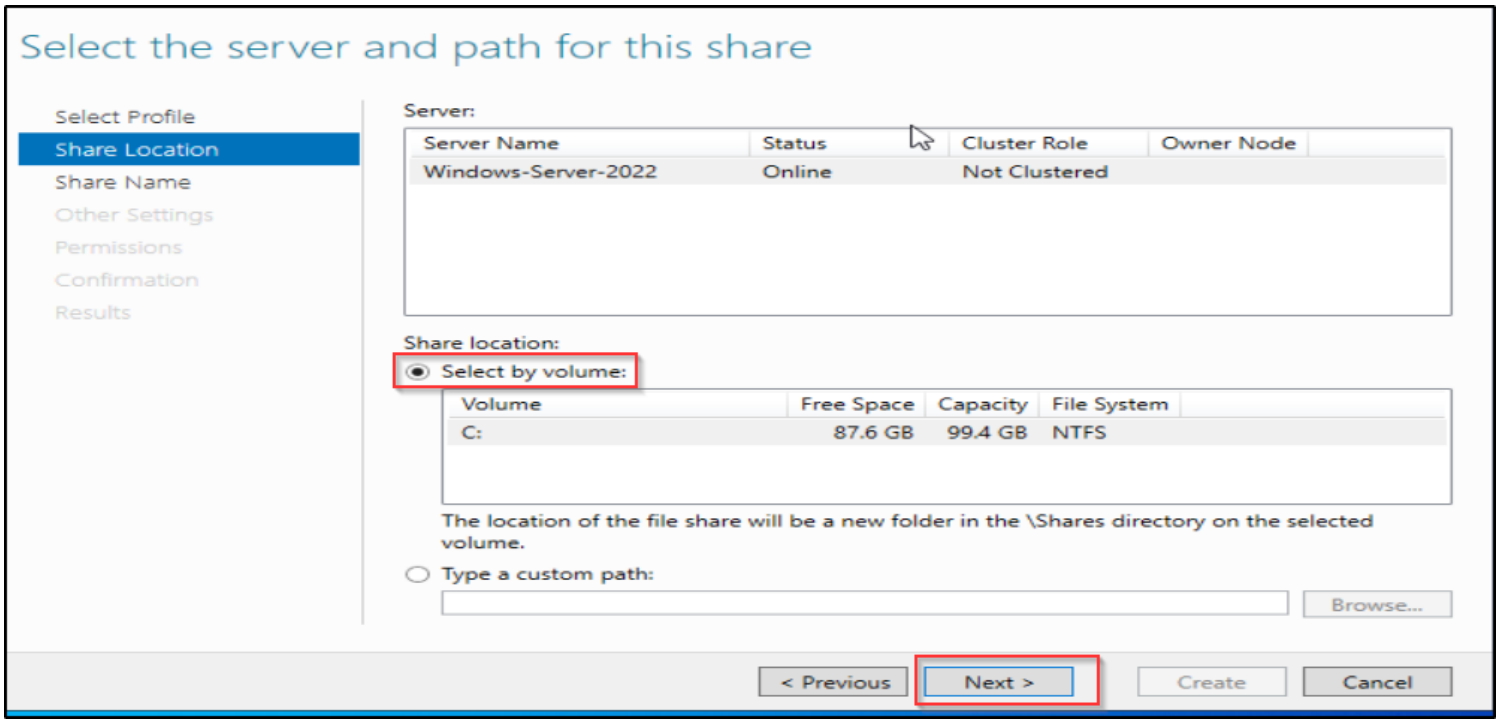
In the Server Manager Dashboard, I clicked on **"File and Storage Services"**.



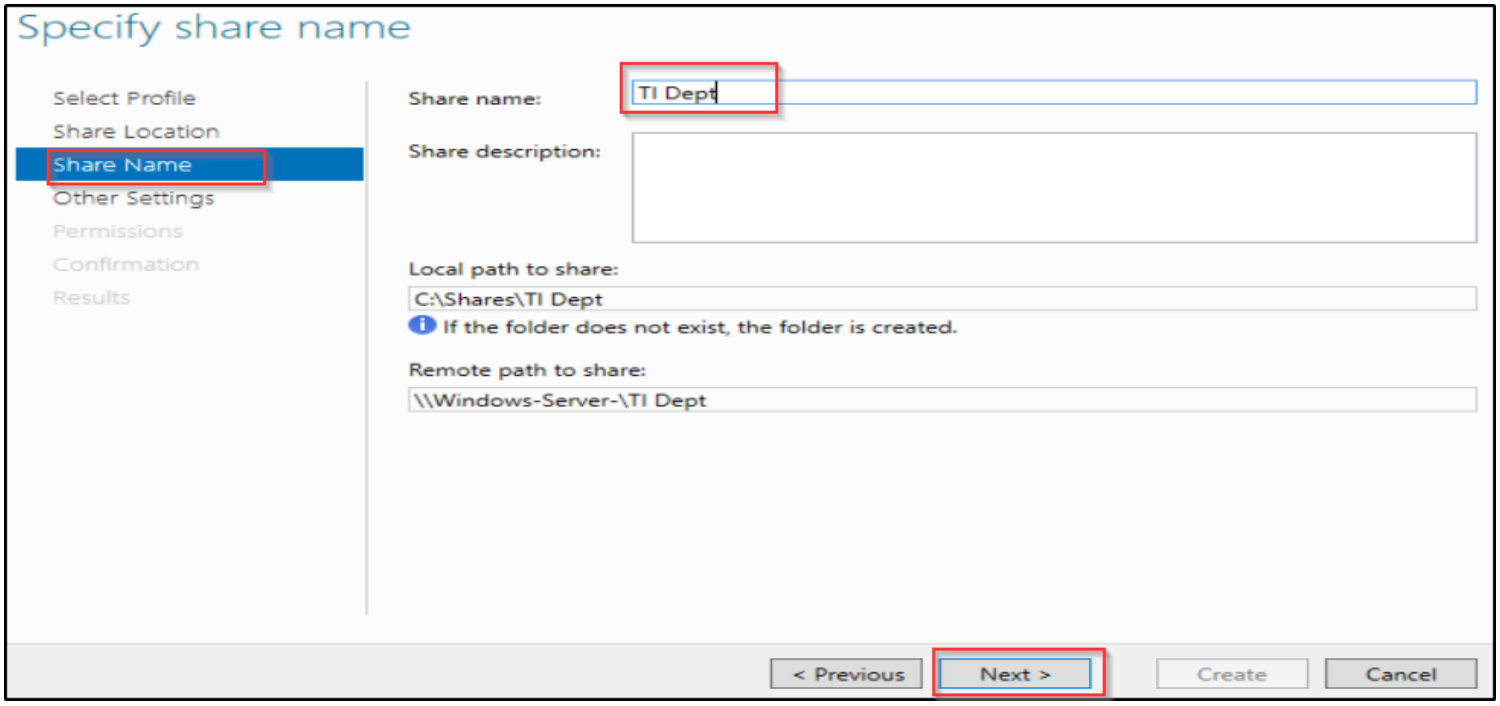
When the new window opened, I clicked on **"Shares"**, then on **"Tasks"**, and selected **"New Share"**. I chose **"SMB Share - Quick"** for a simple and efficient setup.



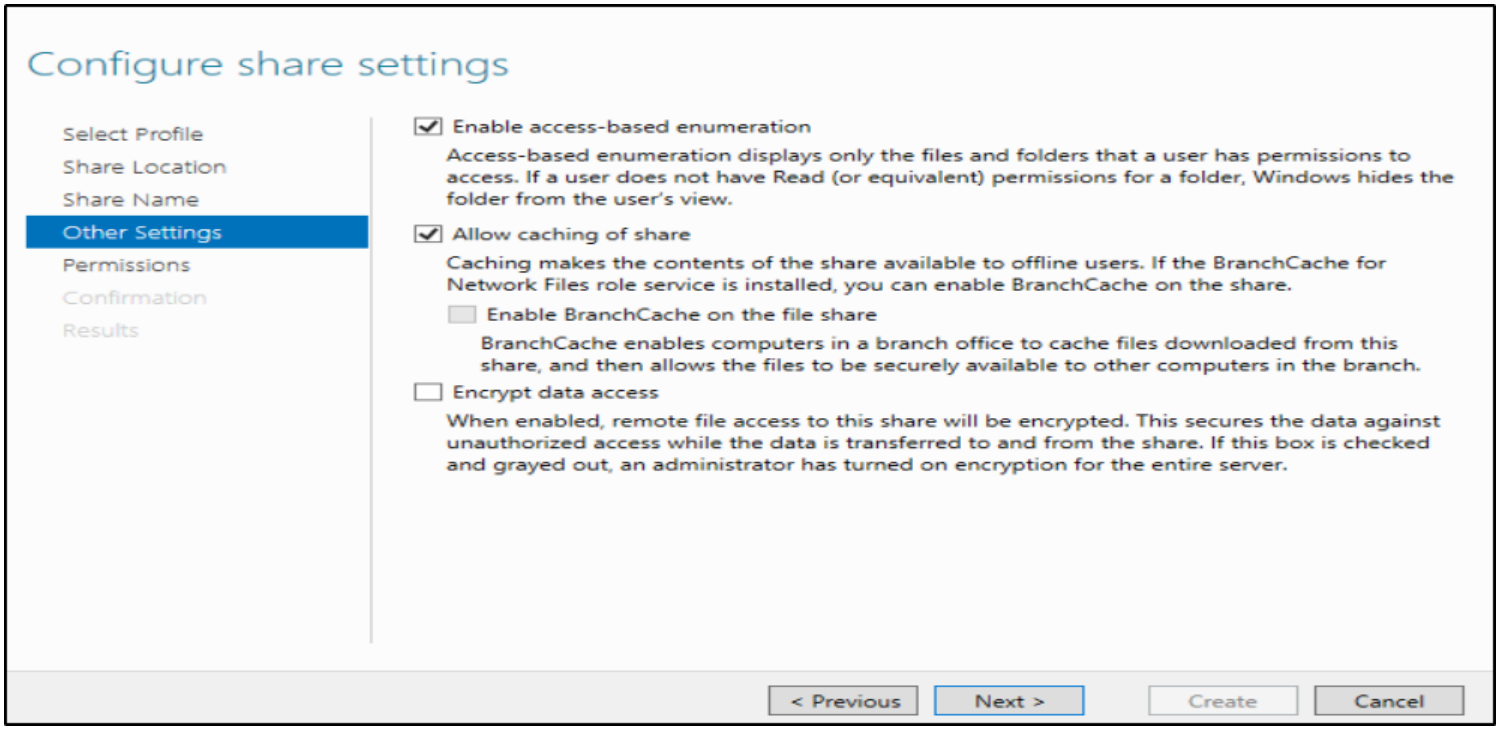
Here, I selected the **share location** and clicked on **"Next"**.



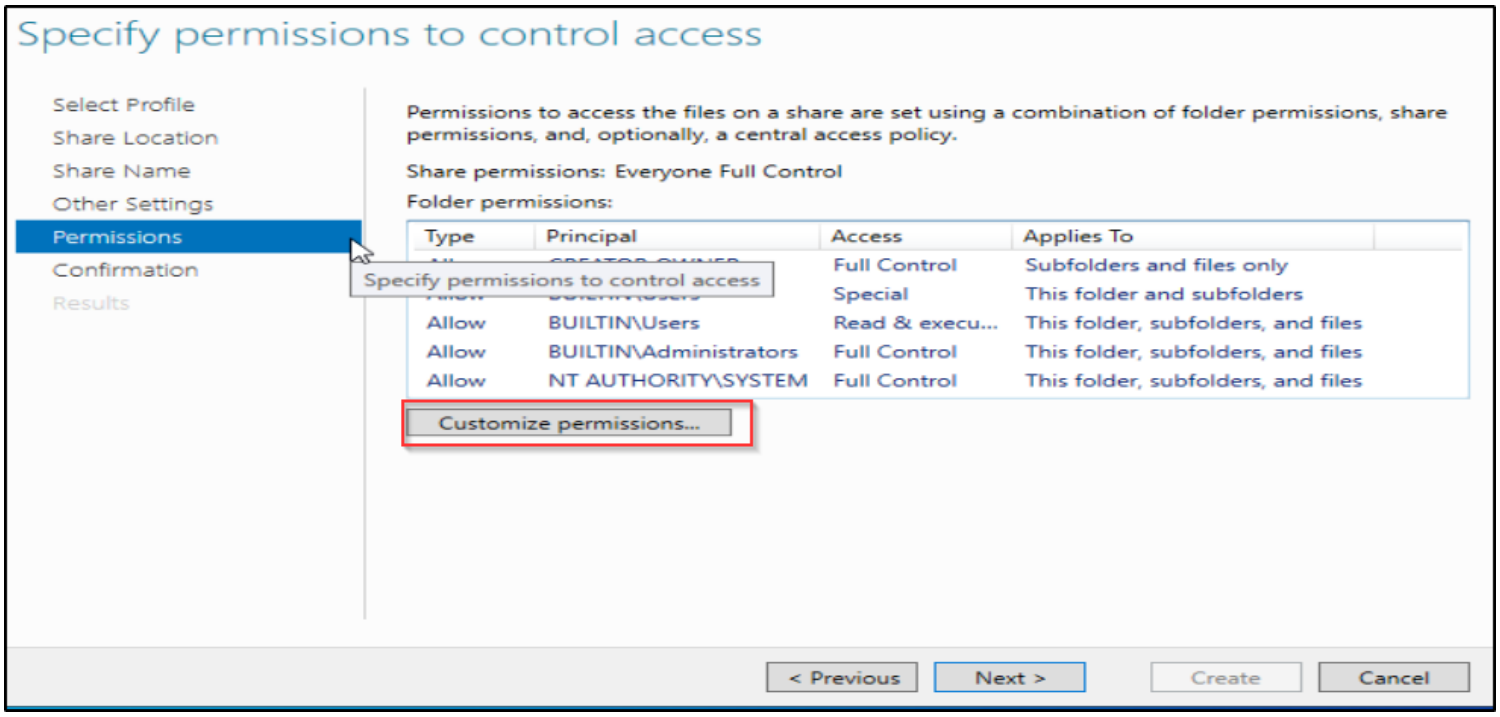
On the **Share Name** page, I entered the name of the folder I wanted to share and clicked on **"Next"**.



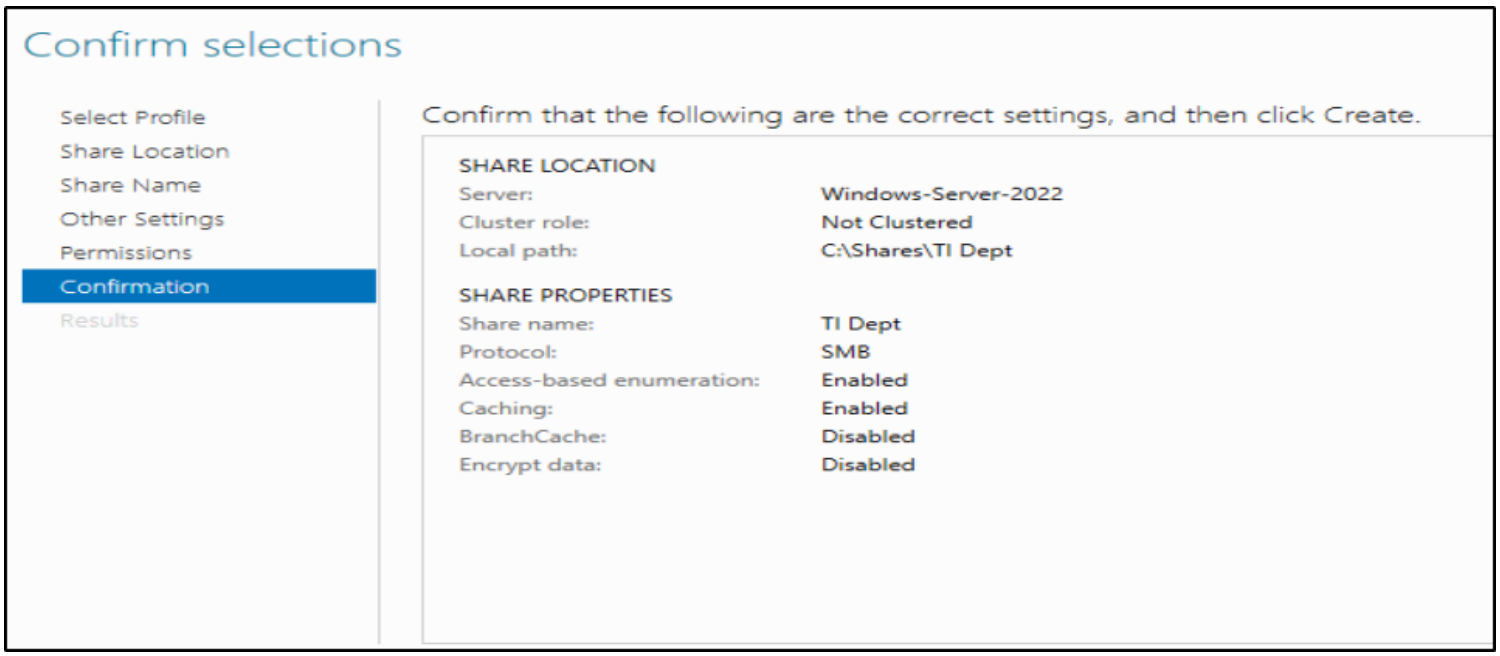
On the **Other Settings** page, I enabled **Access-Based Enumeration** and **Allow Caching of Share**, then clicked on **"Next"**.



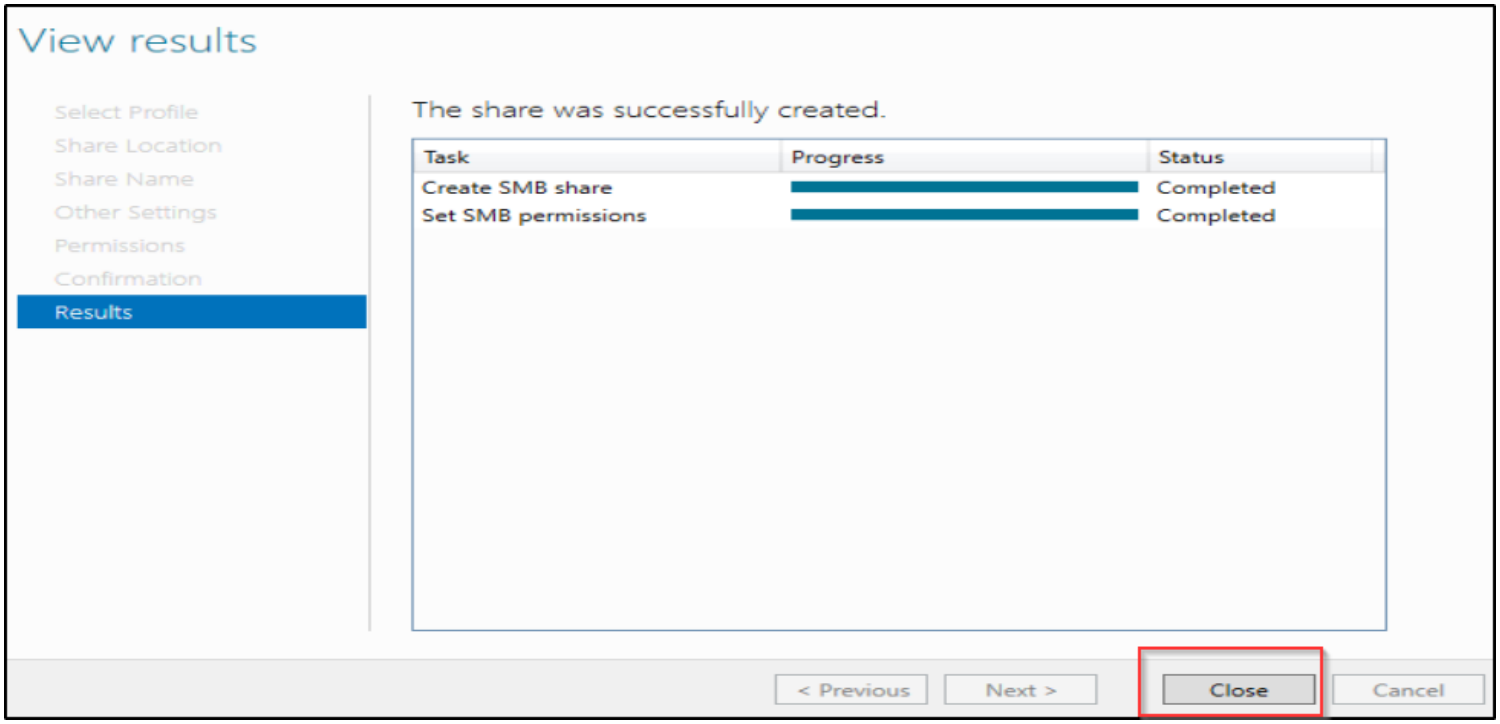
On the **Permissions** page, I clicked on **Customize Permissions** to adjust the permission settings according to my requirements. After configuring the permissions, I clicked **"OK"**.



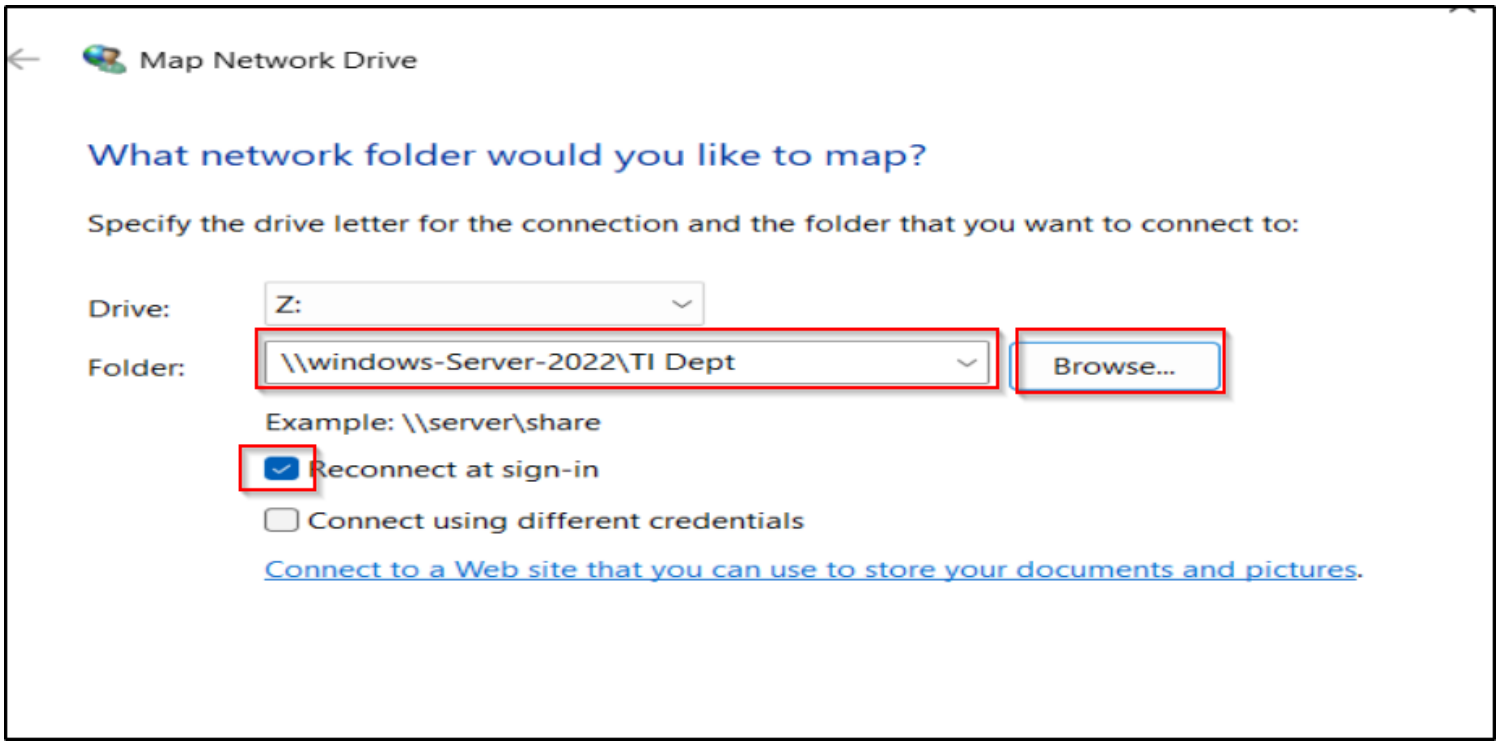
I reviewed and confirmed all the settings to ensure they were correct. Once satisfied, I clicked **"Finish"** to complete the setup process.



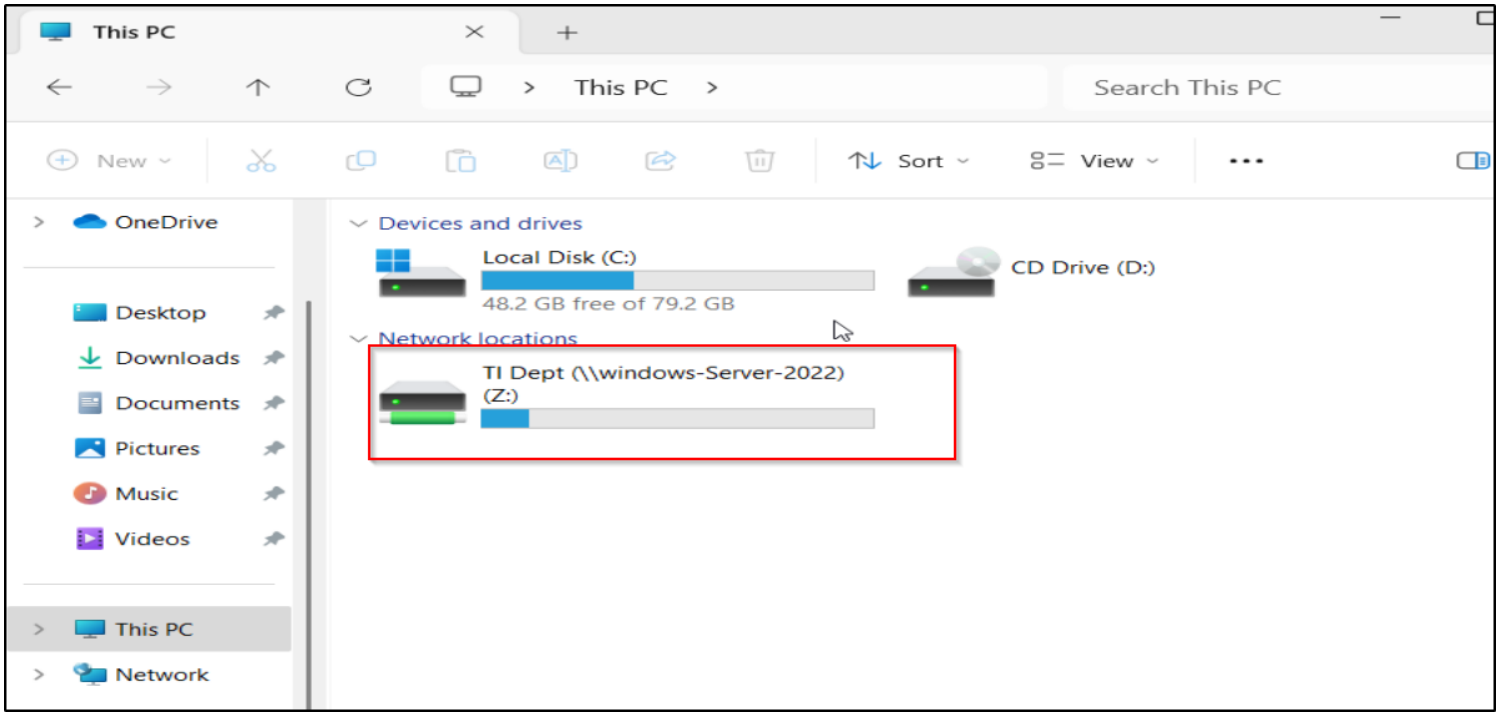
The process completed successfully, and I received a confirmation message. I then clicked **"Close"** to exit the setup window.



On the client side, I right-clicked on **"This PC"** and selected the **"Map network drive"** option.
In the dialog box, I entered the full path of the shared folder I wanted to map by typing it in or clicking **"Browse"** to locate it. I then checked the **"Reconnect at sign-in"** option to ensure the drive would automatically reconnect each time the user signed in. Finally, I clicked **"Finish"** to complete the mapping process.



The shared drive mapping was successfully completed on the client side, confirming access to the shared folder. The mapped network drive is now visible under **"This PC"** and can be accessed seamlessly.



This is the end of this project.This marks the successful completion of the project, showcasing the creation and implementation of key Active Directory configurations, user and group management, policy setups, and shared drive access. All objectives were achieved, ensuring a well-structured and secure environment.

Active Directory (AD) Project Summary

Active Directory (AD) Project Summary

This project involved setting up and managing a Windows Server Active Directory (AD) environment, integrating a Windows 11 client, and implementing various administrative configurations. The goal was to demonstrate expertise in configuring and managing domain services, user and group administration, security policies, and shared resources tailored to organizational requirements.

Key Steps and Achievements:

1. **Domain Configuration and Client Integration:**

• Installed and configured a Windows Server AD domain named `lab.com`.

• Successfully joined a Windows 11 client (`Client-1`) to the domain after verifying network connectivity using tools like `ipconfig` and `ping`.

• Organizational Unit (OU) Setup:

◇ Created OUs for core departments: IT, Finance, and HR.

◇ Enabled protection against accidental deletion for all OUs to prevent misconfigurations.

• User Account Management:

◇ Used two methods for creating user accounts:▪ **Copy Method:** Efficiently created accounts with similar attributes, such as creating an IT admin account based on the domain administrator.

▪ **Manual Method:** Created unique accounts, including Helpdesk staff, with tailored settings.

◇ Configured organizational and account properties for each user, including assigning managers for proper hierarchy.

• Group Management:

◇ Created security groups for each department (e.g., IT Group, HR Group, Finance Group) to streamline resource and policy management.

◇ Assigned appropriate members to each group and set security permissions.

◇ Protected group objects from accidental deletion and customized group permissions to ensure secure access to shared resources.

• Policy Implementation:

◇ Configured department-specific desktop wallpaper policies to maintain uniformity and professionalism.

◇ Implemented a **Wallpaper Policy** to prevent users from changing their desktop backgrounds.

◇ Enforced critical security policies, including:▪ **Account Lockout Policy:** Locked accounts after multiple failed login attempts to mitigate unauthorized access risks.

▪ **Password Policy:** Ensured password complexity and expiration settings for enhanced security.

▪ **Disable CMD Policy:** Prevented unauthorized use of the Command Prompt for standard users to reduce potential system misuse.

• **Shared Drive Setup:**
◇ Configured shared folders for each department (IT, HR, Finance) using the `SMB Share - Quick` method.
◇ Enabled advanced features like access-based enumeration and caching for optimized performance and security.
◇ Customized permissions for each department's shared folder to ensure only authorized users had access.
◇ Mapped shared drives on client machines, enabling seamless and automatic reconnection during user sign-ins.

Results and Verification:

◇ Verified the successful creation and configuration of user accounts, OUs, groups, and shared resources.
◇ Ensured each department had access to its respective shared drive, with proper permissions and automatic reconnection.
◇ Confirmed policy enforcement, including uniform wallpapers and restricted desktop background changes, across all client devices.

Conclusion:

This project demonstrated a robust and structured approach to setting up and managing an Active Directory environment. By integrating domain services with tailored policies and resource management, it showcased essential IT administration practices. The implementation of security measures, shared resources, and departmental policies reflects a comprehensive understanding of enterprise-level IT infrastructure management. These skills are vital for effectively managing and securing organizational IT environments.

Recommendations for Future Improvement

Recommendations for Future Improvement
To further enhance the functionality, security, and efficiency of this Active Directory (AD) environment, the following recommendations are suggested:

1. Advanced Security Configurations:

• **Enable Multi-Factor Authentication (MFA):** Implement MFA for domain admin accounts and privileged users to add an extra layer of security.
• **Audit Policies:** Set up detailed auditing policies to track user activities, failed login attempts, and modifications to critical AD objects.
• **Group Policy Restrictions:** Expand Group Policy Object (GPO) configurations to include restrictions on USB usage, unauthorized software installation, and execution of scripts.

2. Centralized Monitoring and Backup:

◇ **Event Log Monitoring:** Deploy tools like Microsoft Advanced Threat Analytics (ATA) or third-party solutions to monitor security events and detect anomalies in real-time.
◇ **Regular Backups:** Configure scheduled backups of AD, including system state and critical data, to ensure quick recovery in case of failures or attacks.

3. Enhanced Group Management:

◇ **Dynamic Distribution Groups:** Use dynamic groups based on user attributes (e.g., department, role) to automate group membership.
◇ **Role-Based Access Control (RBAC):** Define roles and assign permissions based on job responsibilities to reduce administrative overhead and minimize risks.

4. Expand Policy Management:

◇ **Software Deployment Policies:** Use Group Policy to deploy and manage department-specific software centrally.
◇ **Browser Settings:** Configure group policies to enforce secure browser settings, such as disabling untrusted plugins and enforcing safe browsing practices.
◇ **Patch Management:** Implement WSUS (Windows Server Update Services) or a similar solution to ensure that all clients and servers receive timely updates.

5. Improve User Experience:

◇ **Self-Service Password Reset:** Enable self-service options for password resets to reduce helpdesk dependency and improve user satisfaction.
◇ **Department-Specific Drive Mapping:** Use logon scripts or GPO preferences to automatically map department-specific shared drives for users based on their roles.

6. Training and Documentation:

◇ **Staff Training:** Conduct regular training sessions for users to ensure awareness of IT security policies and best practices.
◇ **Detailed Documentation:** Maintain up-to-date documentation of the AD structure, policies, and configurations to facilitate troubleshooting and onboarding of new IT staff.

7. Scalability and Advanced Features:

◇ **Deploy Additional Domain Controllers:** Add secondary domain controllers in different locations for load balancing, redundancy, and disaster recovery.
◇ **Integrate Azure Active Directory (AAD):** Explore hybrid solutions with Azure AD for cloud-based authentication and enhanced mobility features.
◇ **Single Sign-On (SSO):** Enable SSO for organizational applications to streamline user authentication and improve productivity.

8. Regular Performance Review:

◇ **Policy Review:** Periodically review and update GPOs to align with changing organizational needs and security standards.
◇ **System Health Checks:** Perform regular health checks of the AD environment using tools like DCdiag and repadmin to detect and resolve issues proactively.

By implementing these improvements, the Active Directory environment will become more secure, efficient, and aligned with modern IT standards, ensuring the organization's IT infrastructure can scale and adapt to future demands.