

Active Directory

Configure Active Directory in Oracle VirtualBox, Add Users using PowerShell

Objective:

- Learn how to set up and configure a server running Active Directory using Oracle VirtualBox
- Learn how to use PowerShell script to add Users to the Domain Controller we created
- Set up a device to connect to the Domain Controller we set up that is running Active Directory

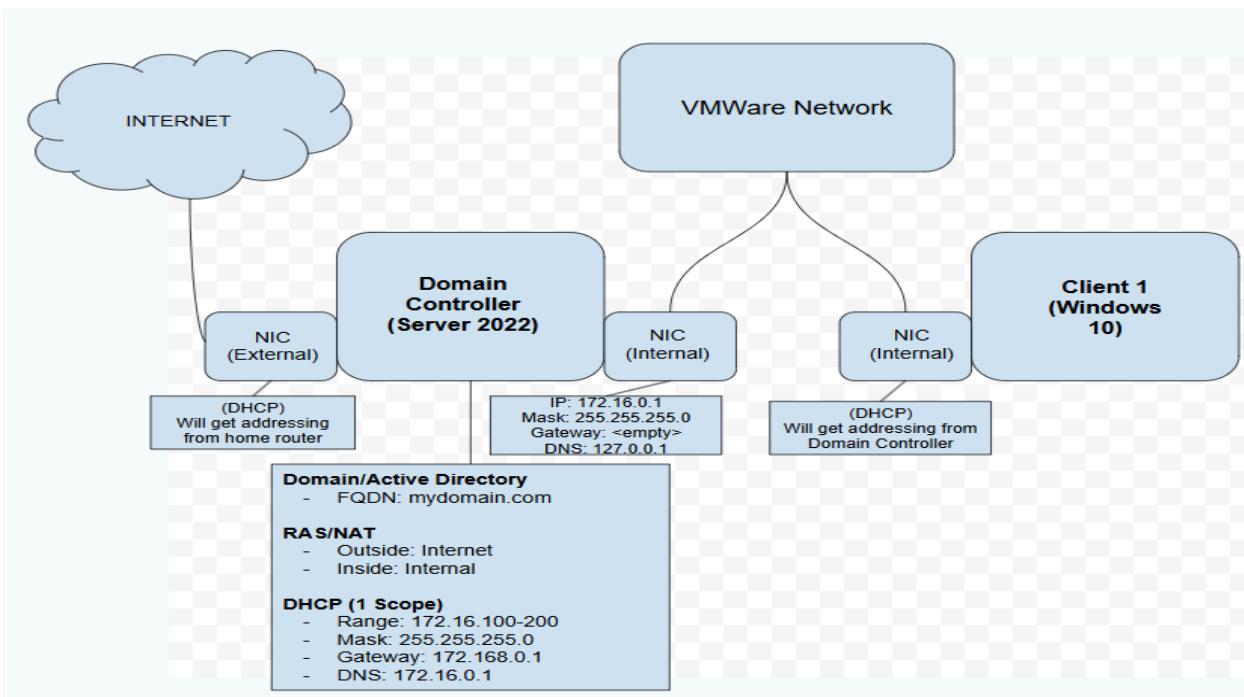
Skills:

- Become familiar with using Oracle VirtualBox
- Become familiar with configuring Active Directory
- Basic Networking
 - Network Infrastructure design
 - Configuring DHCP
 - Subnetting
- Become familiar with using PowerShell scripts and commands

System Requirements:

- Oracle VirtualBox
- Windows 10 ISO
- Server 2022 ISO

Network Architecture Diagram:



Step 1:

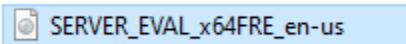
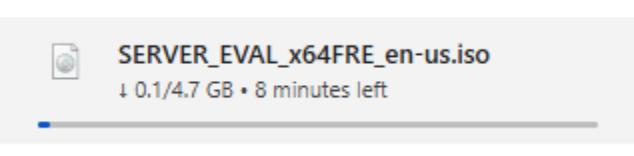
Download ISO Files

Download **Windows Server 2022 ISO** -

<https://info.microsoft.com/ww-landing-windows-server-2022.html>

English (United States)

ISO downloads
[64-bit edition >](#)



Download Windows 10 ISO -

<https://www.microsoft.com/en-us/software-download/windows10>

Create Windows 10 installation media

To get started, you will first need to have a license to install Windows 10. You can then download information on how to use the tool, see the instructions below.

[Download Now](#)

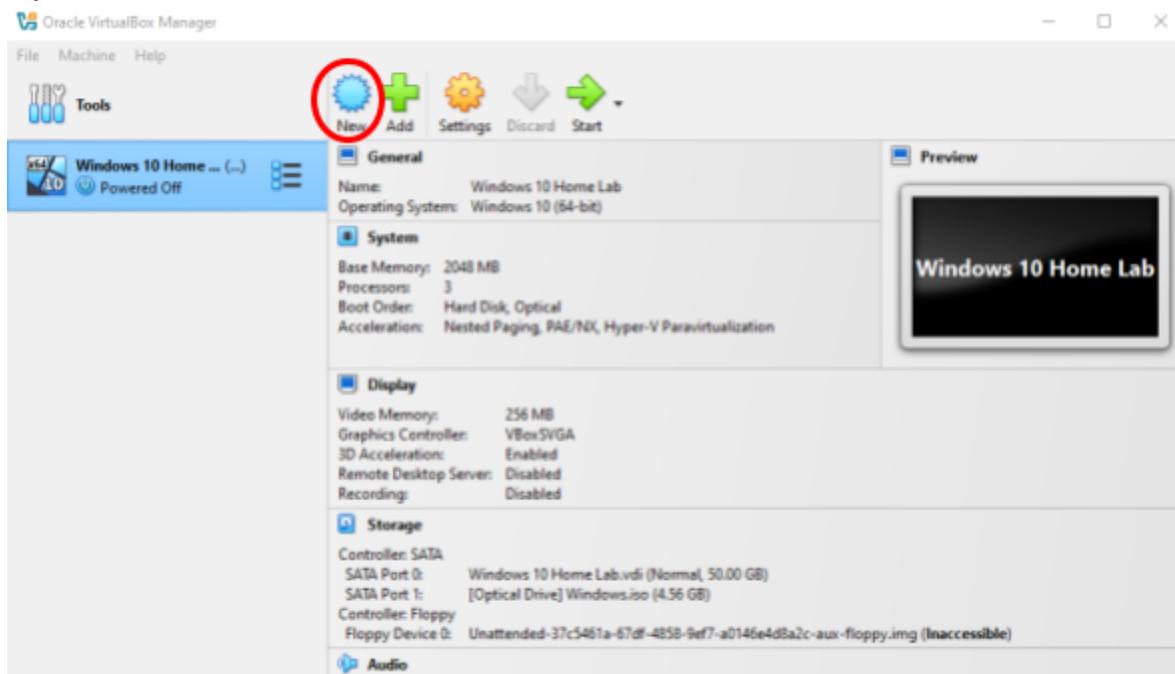
Download Oracle VirtualBox - <https://www.virtualbox.org/wiki/Downloads>



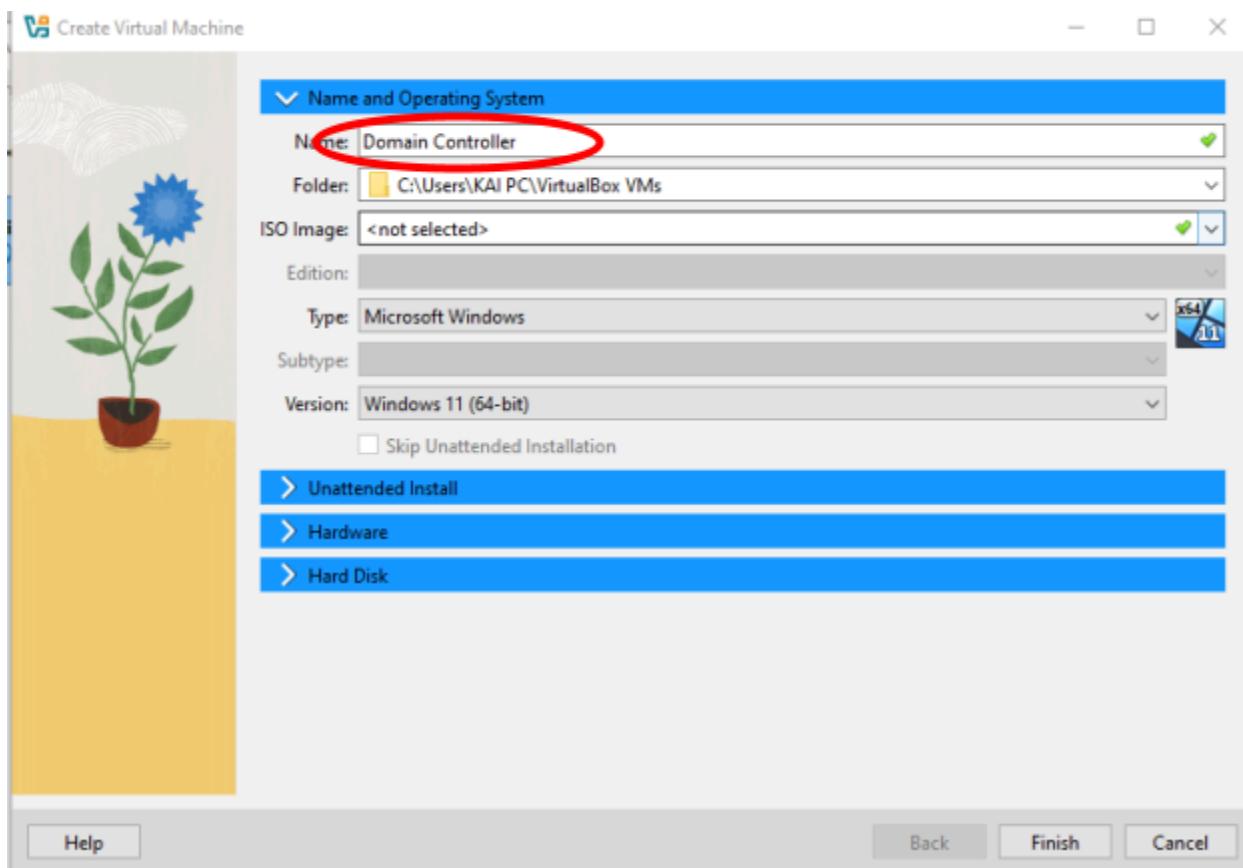
Step 2: Set Up Virtual Machines

Set up Domain Controller Virtual Machine with Windows Server 2022

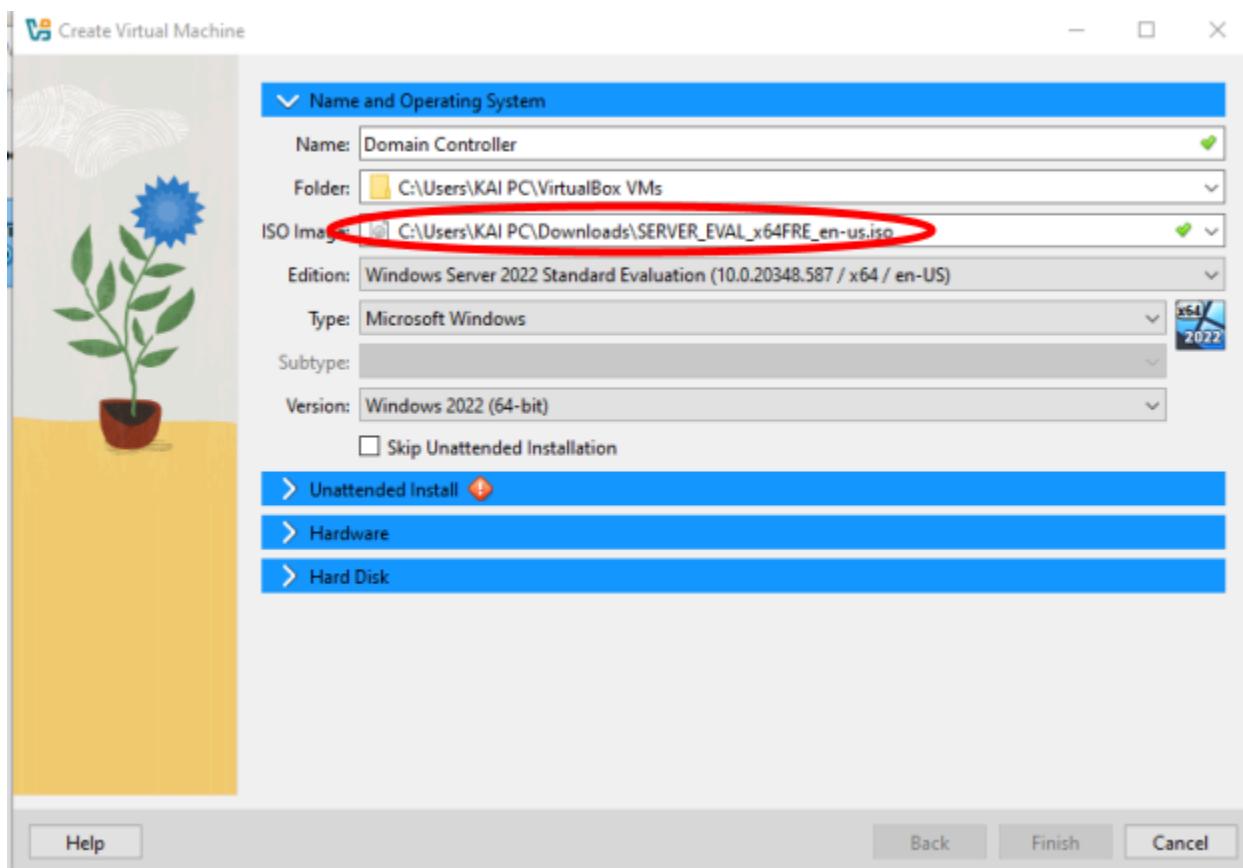
Open VirtualBox and click on New



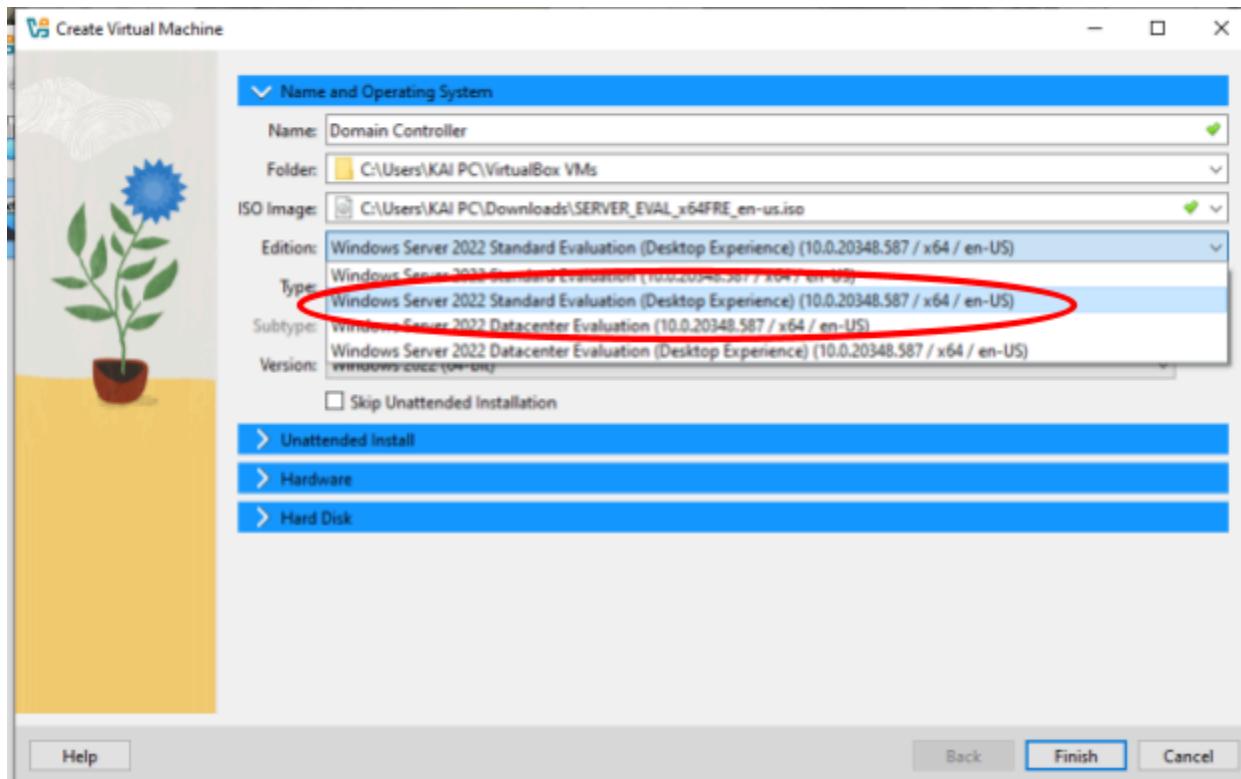
Name the Virtual Machine Domain Controller



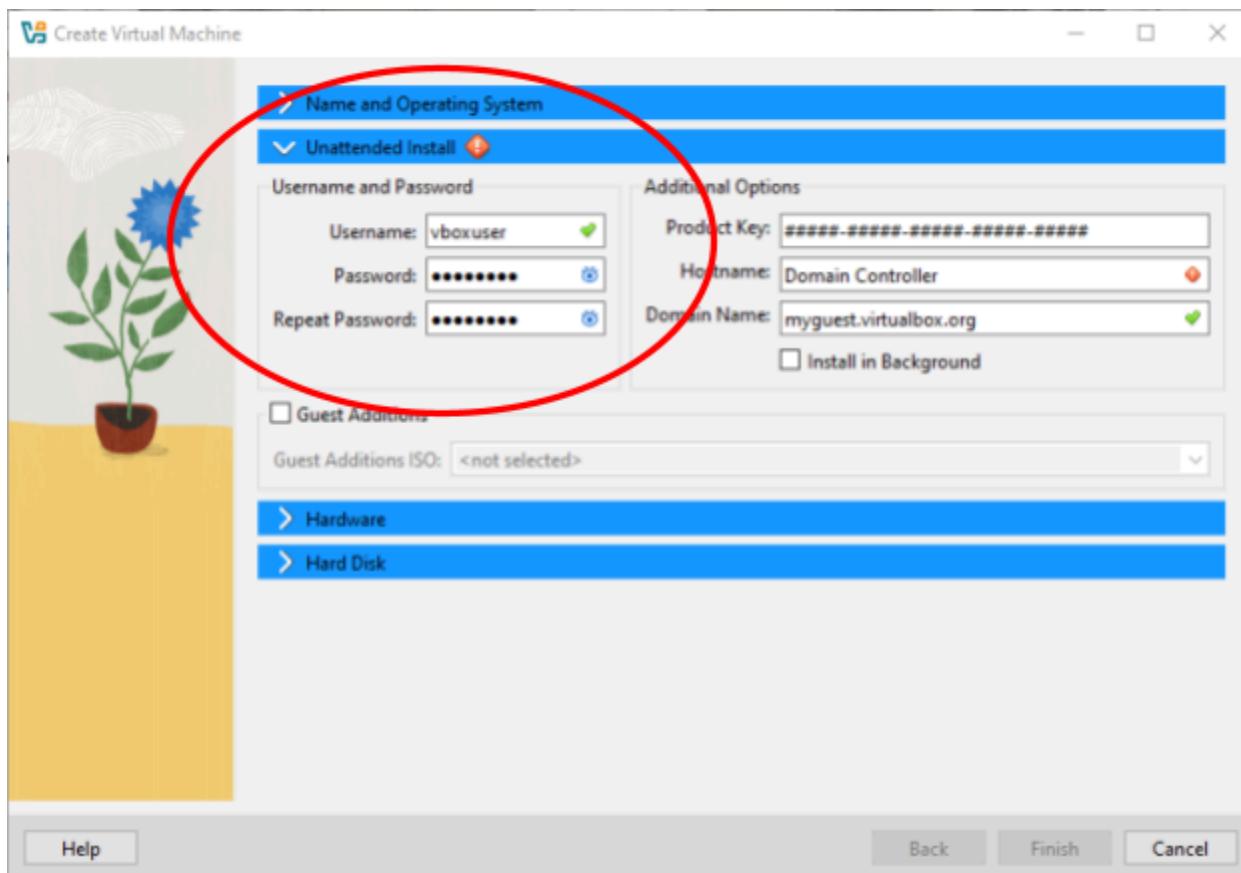
Select the Windows Server ISO File we downloaded earlier.



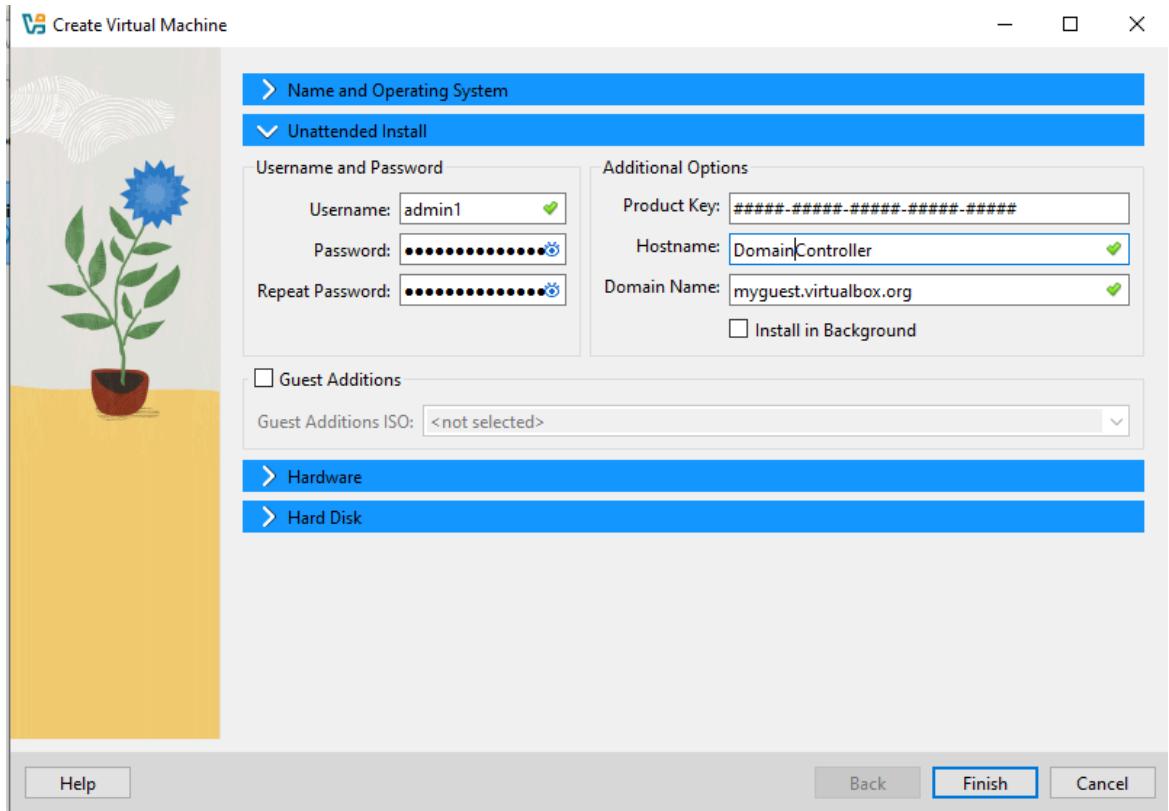
Select the Windows Edition Windows Server 2022 Standard Evaluation (Desktop Experience)



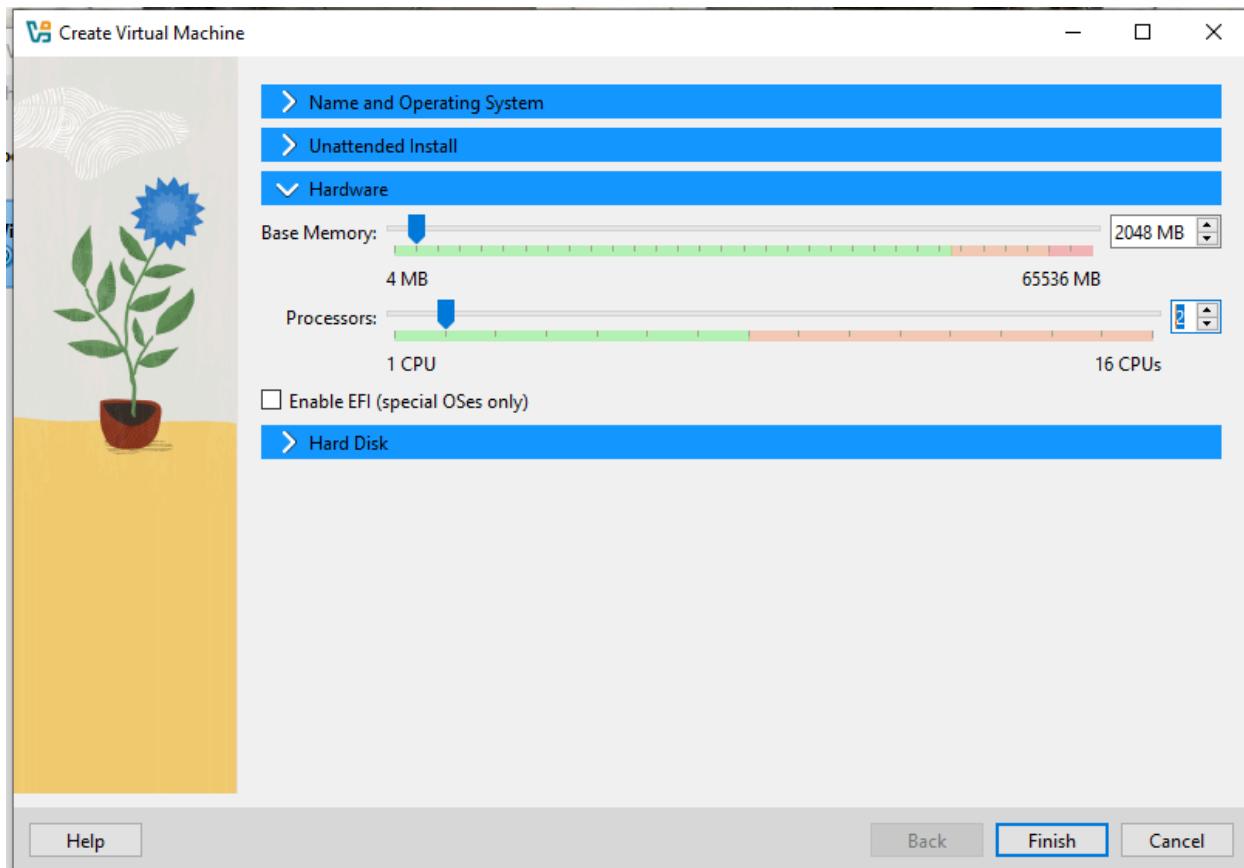
Add a username and password to your virtual box account. This is a temporary account as we will be creating an Admin account once we set up Active Directory



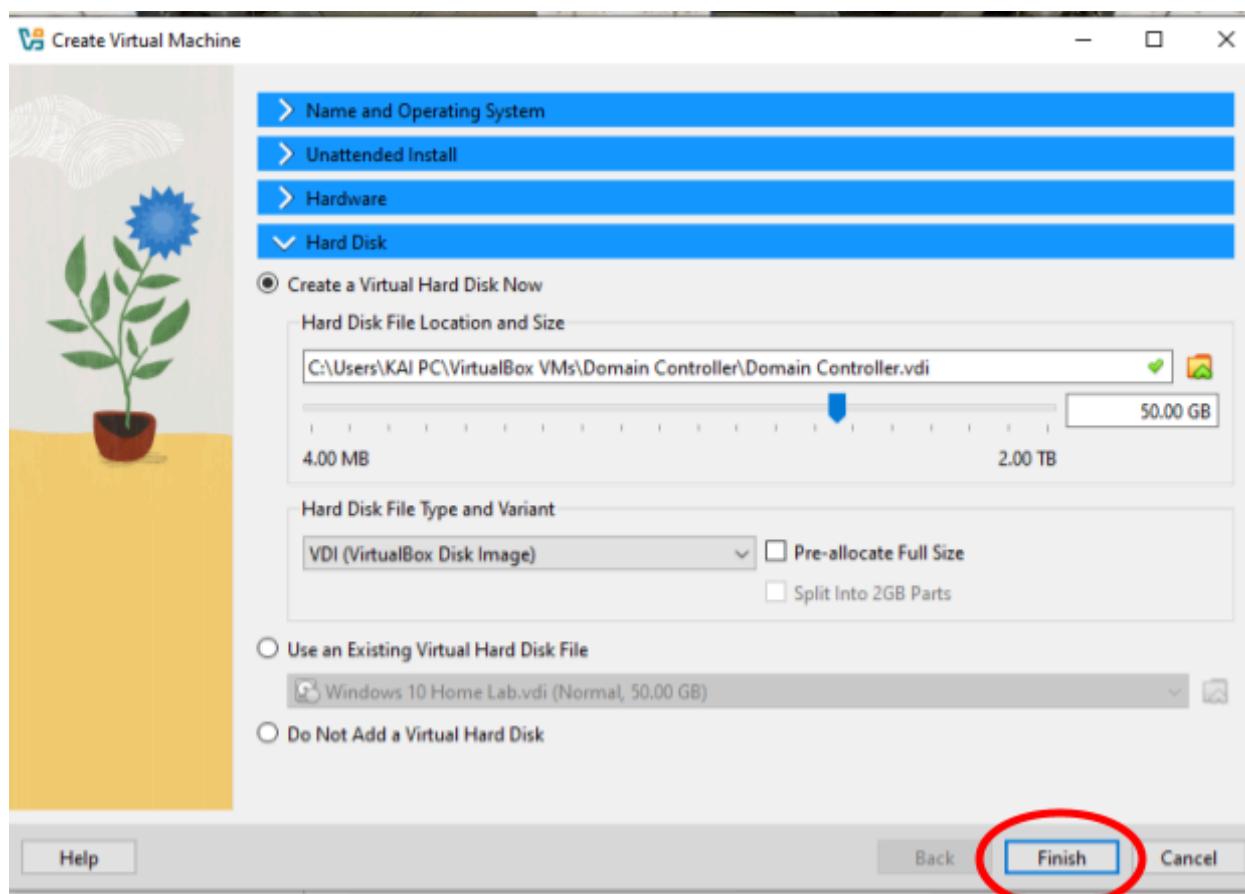
Create a hostname



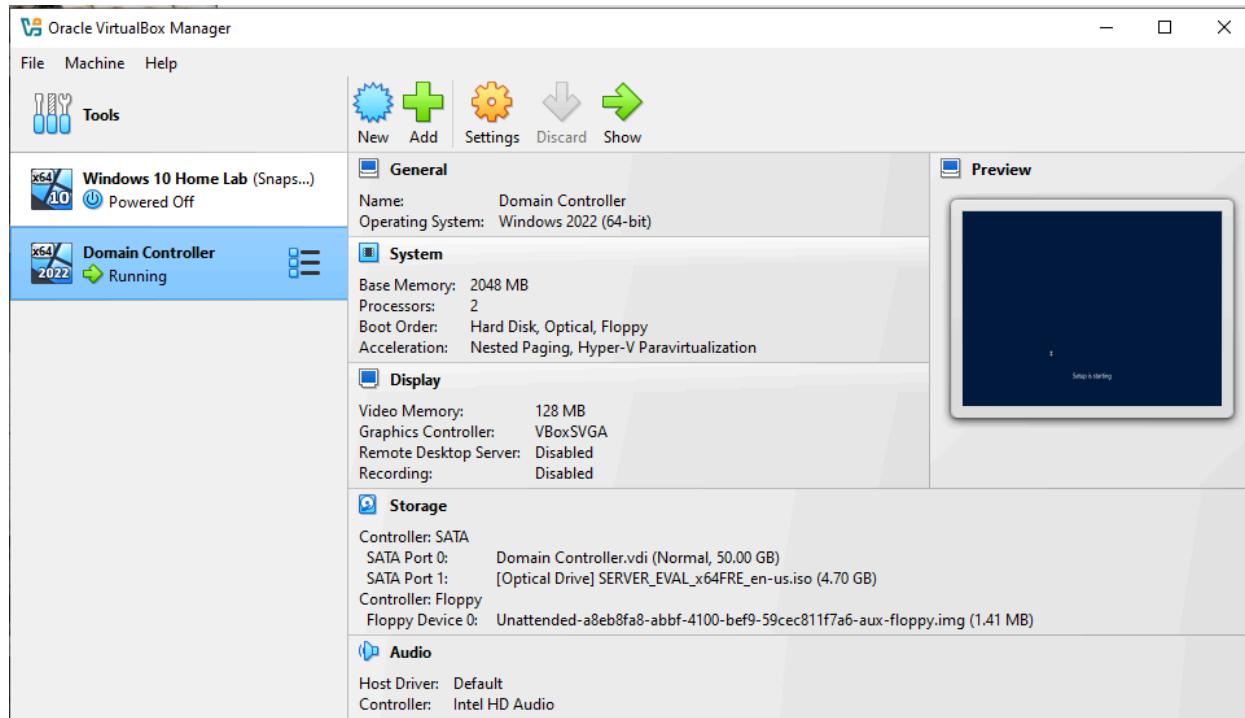
Allocate hardware to your Virtual Machine. In this case, I added 2048 MB (2 GB) of RAM, and 2 CPU core processors



Leave the Virtual Hard Disk as it is and click Finish

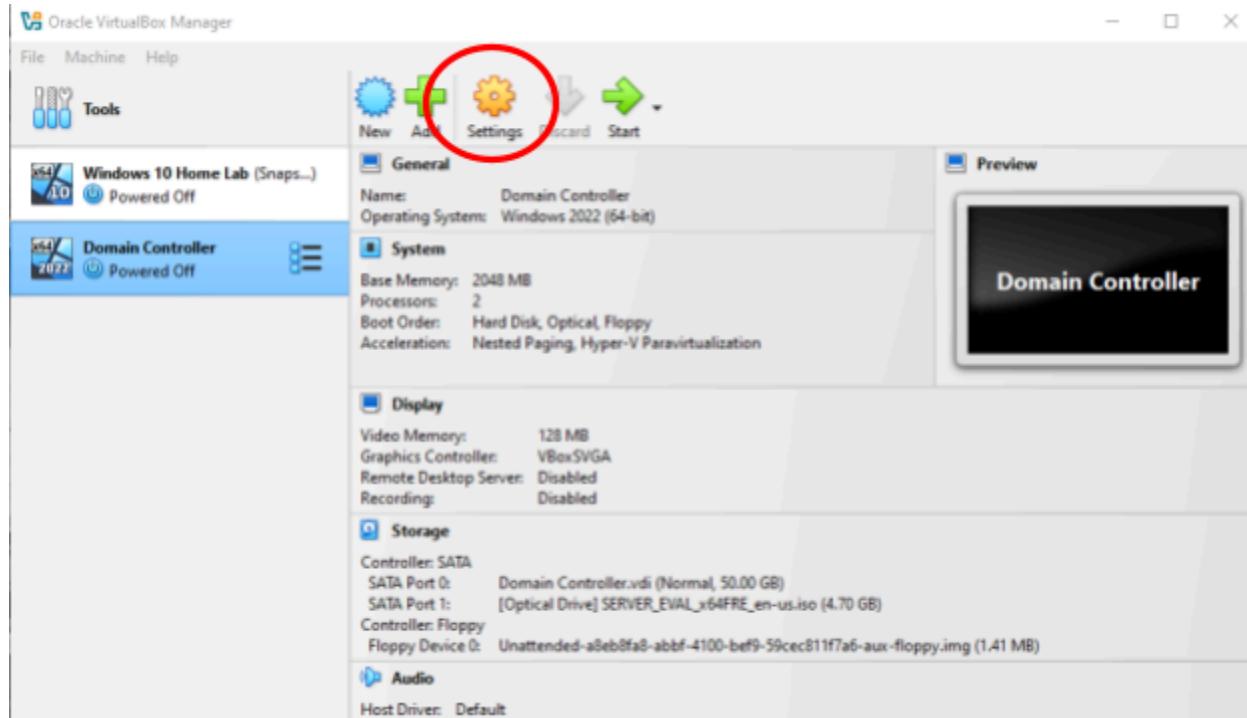


You've created a Virtual Machine.

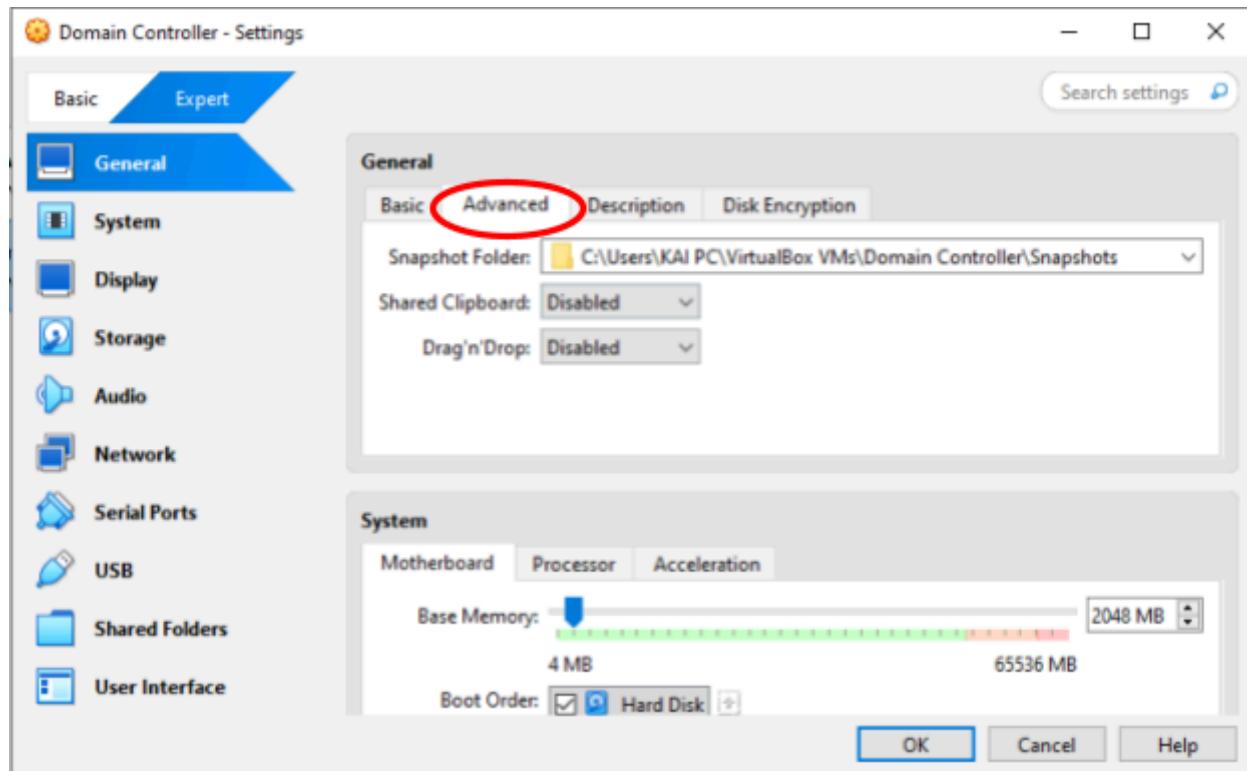


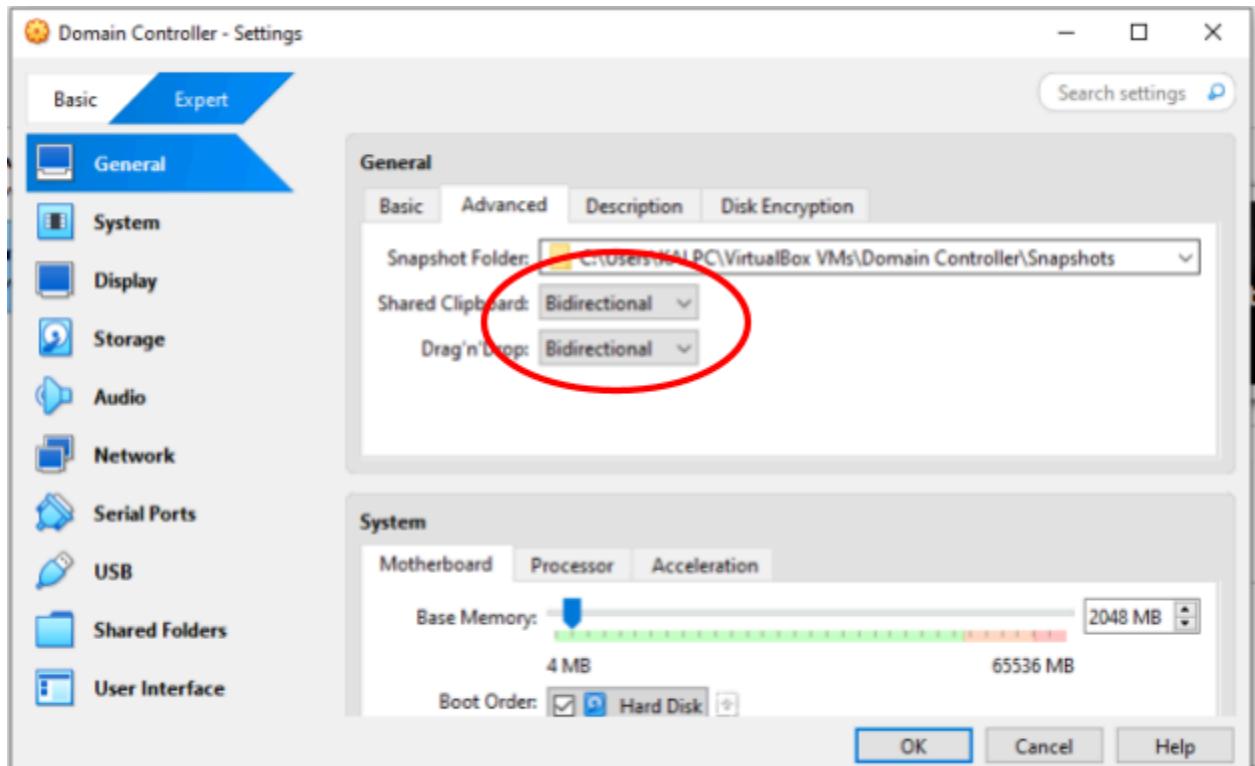
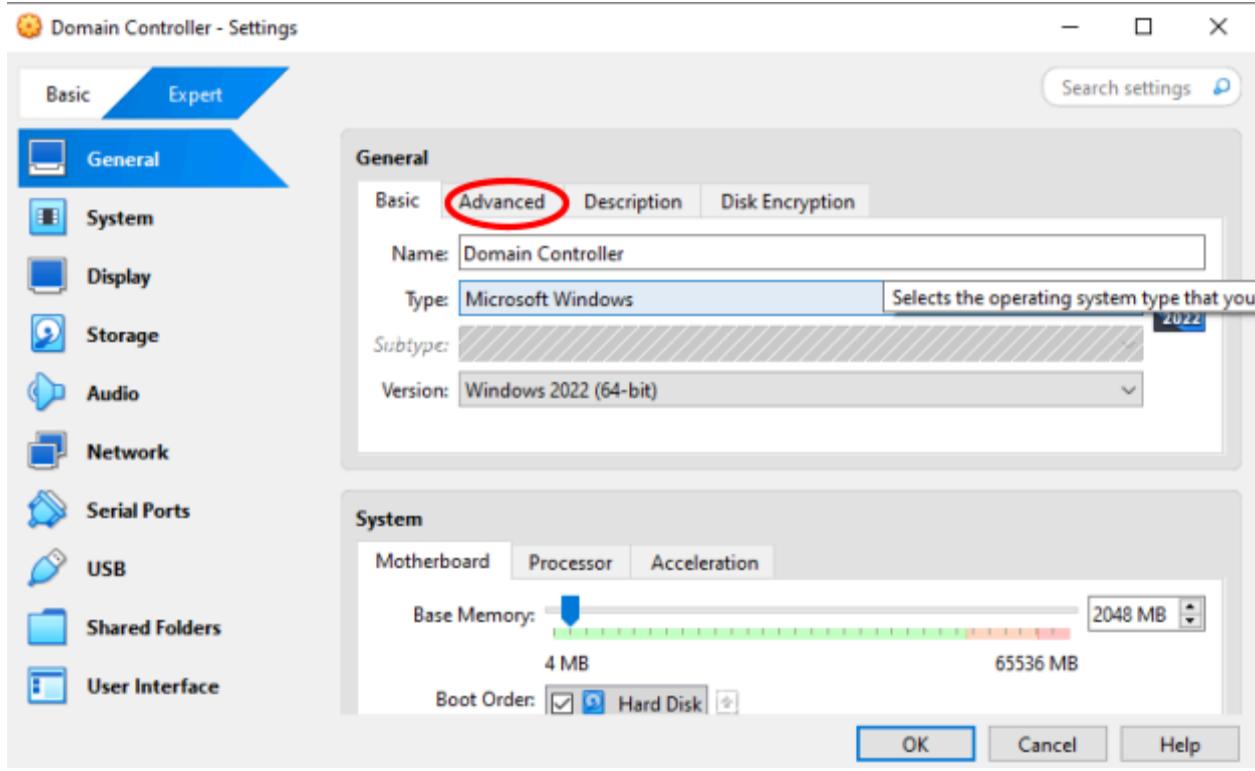
Before firing it up, we need to change its settings so that it is ideal for a LAB Environment.

Click on Settings

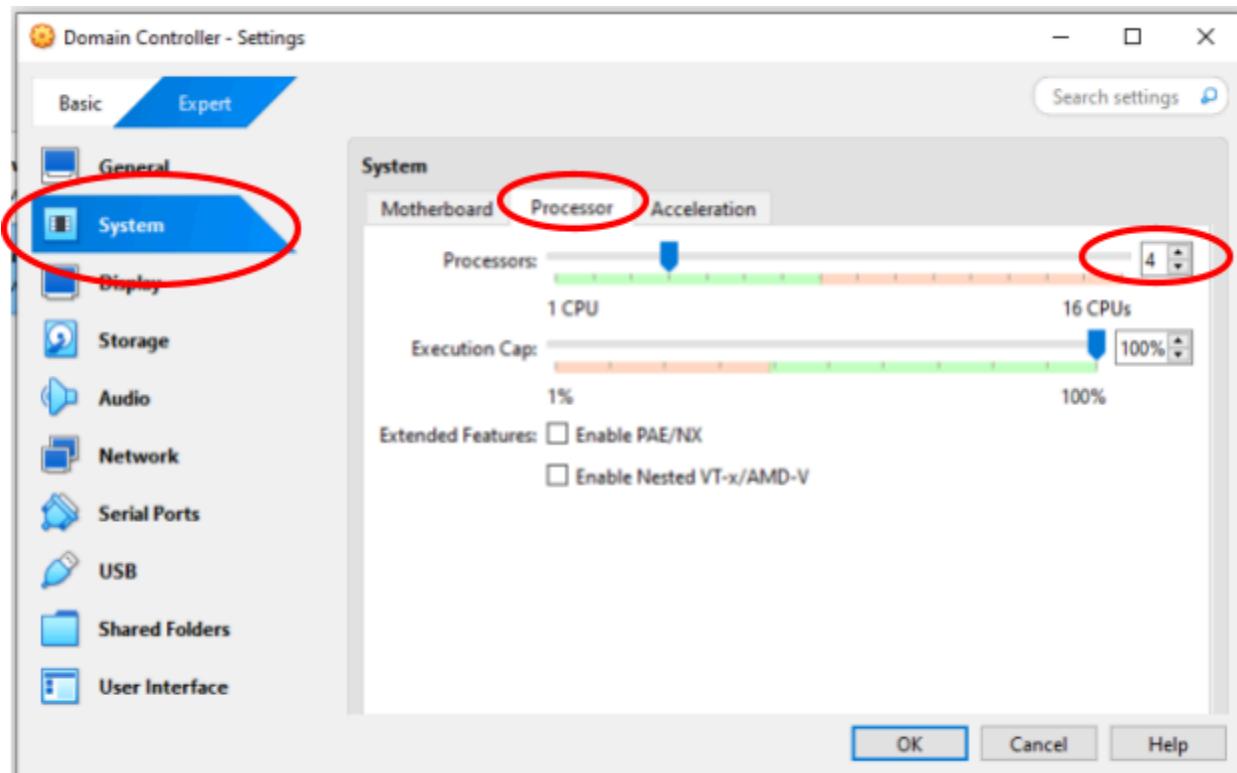


Go to Advanced in the General Tab and change the Shared Clipboard from Disabled to Bidirectional. This makes it easier to share files among your virtual machines.

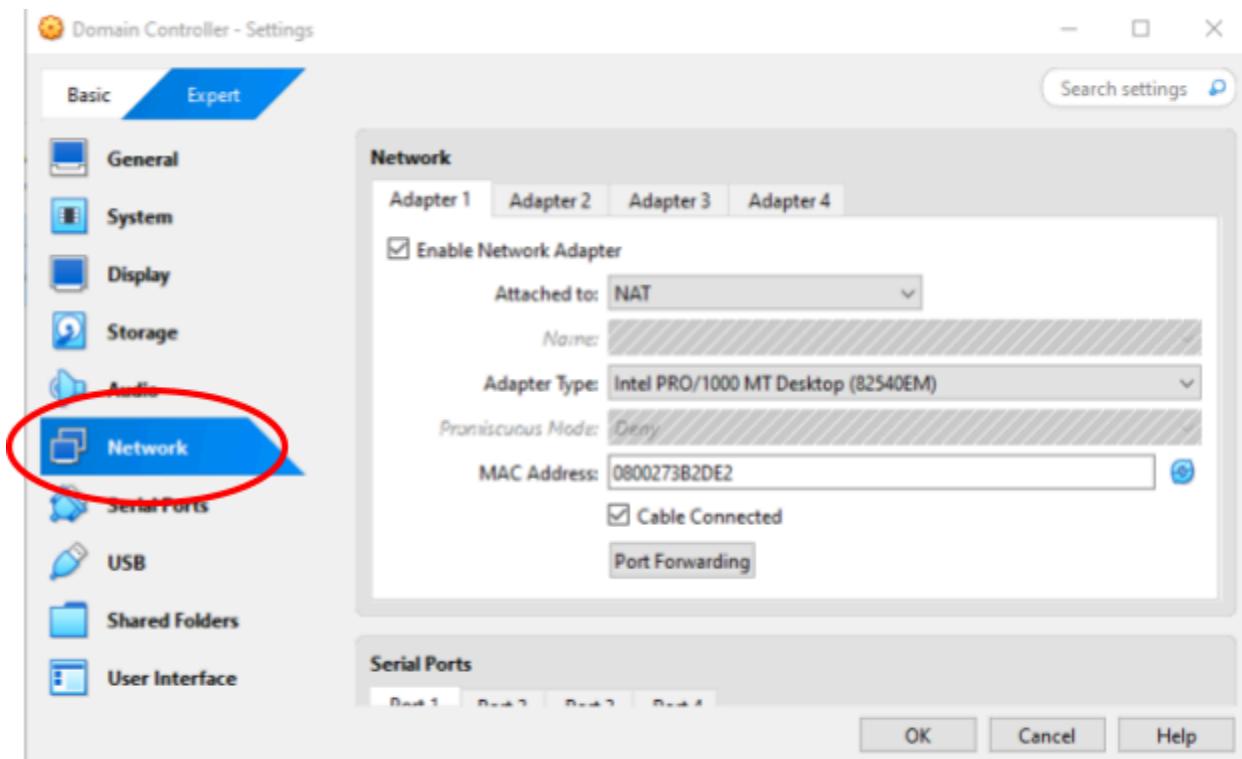


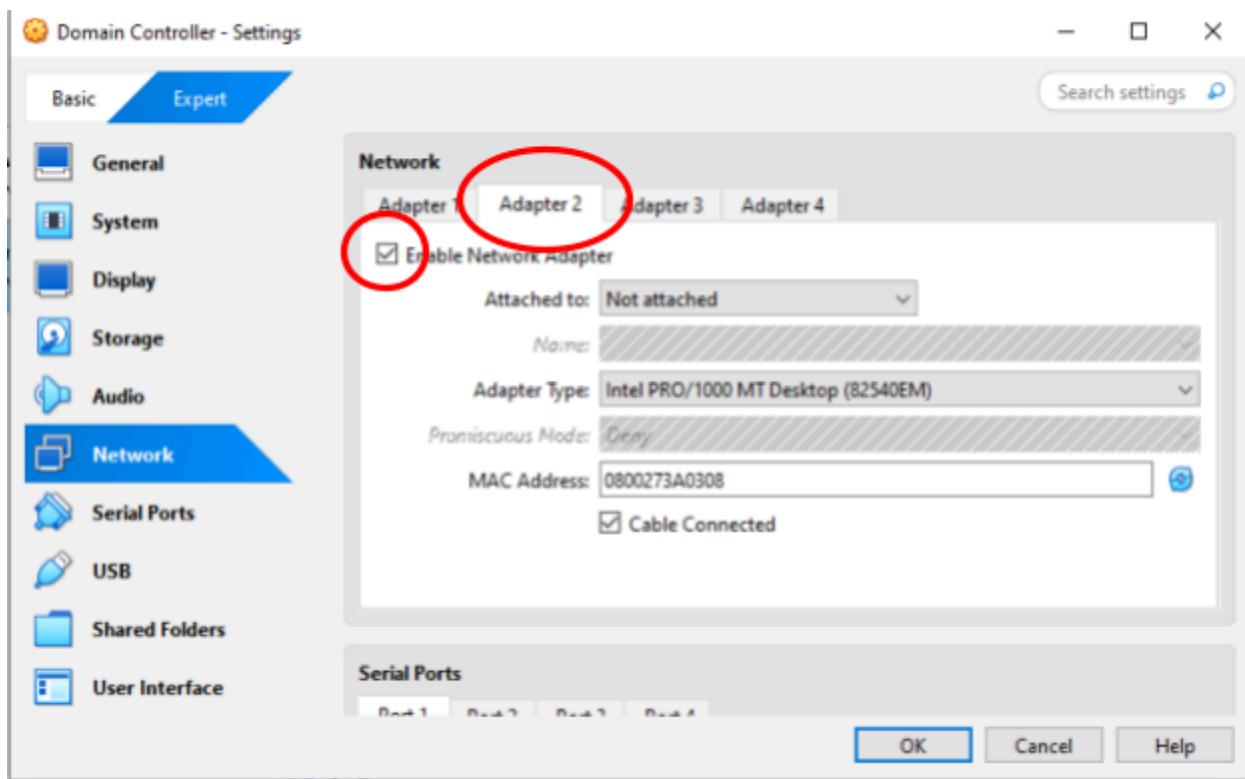
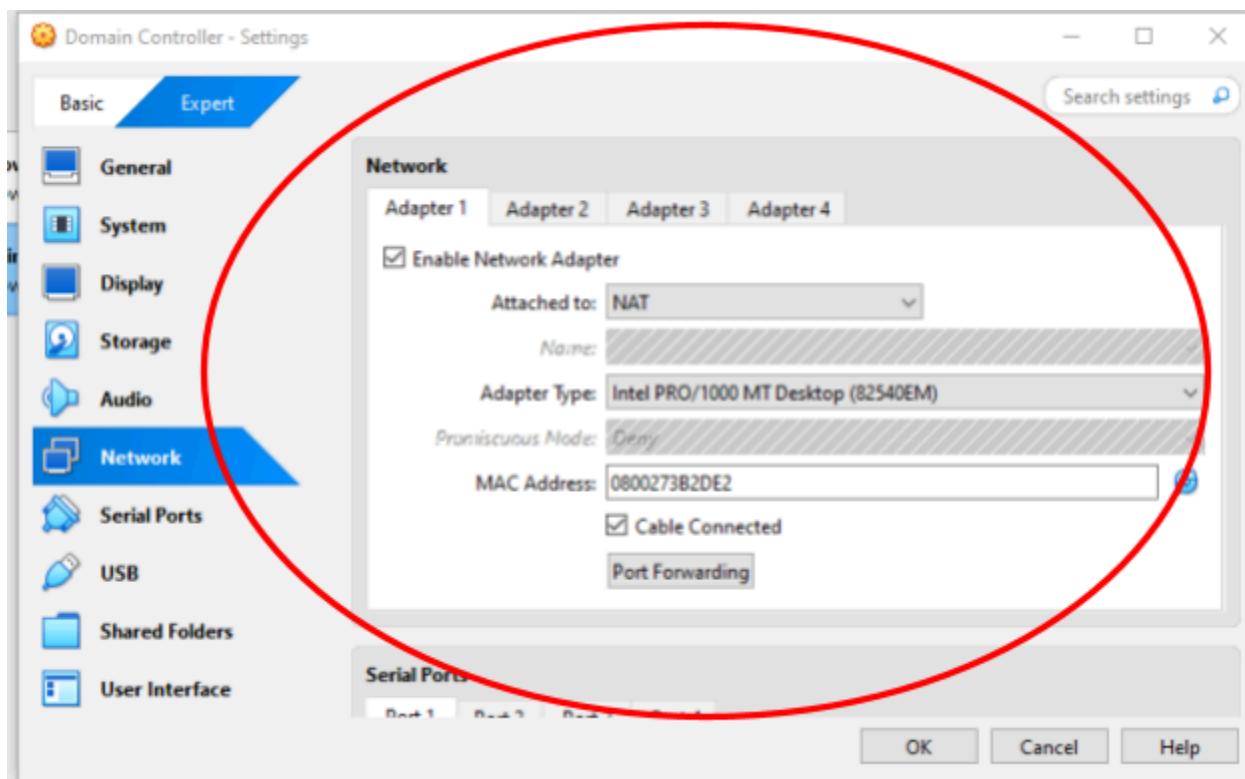


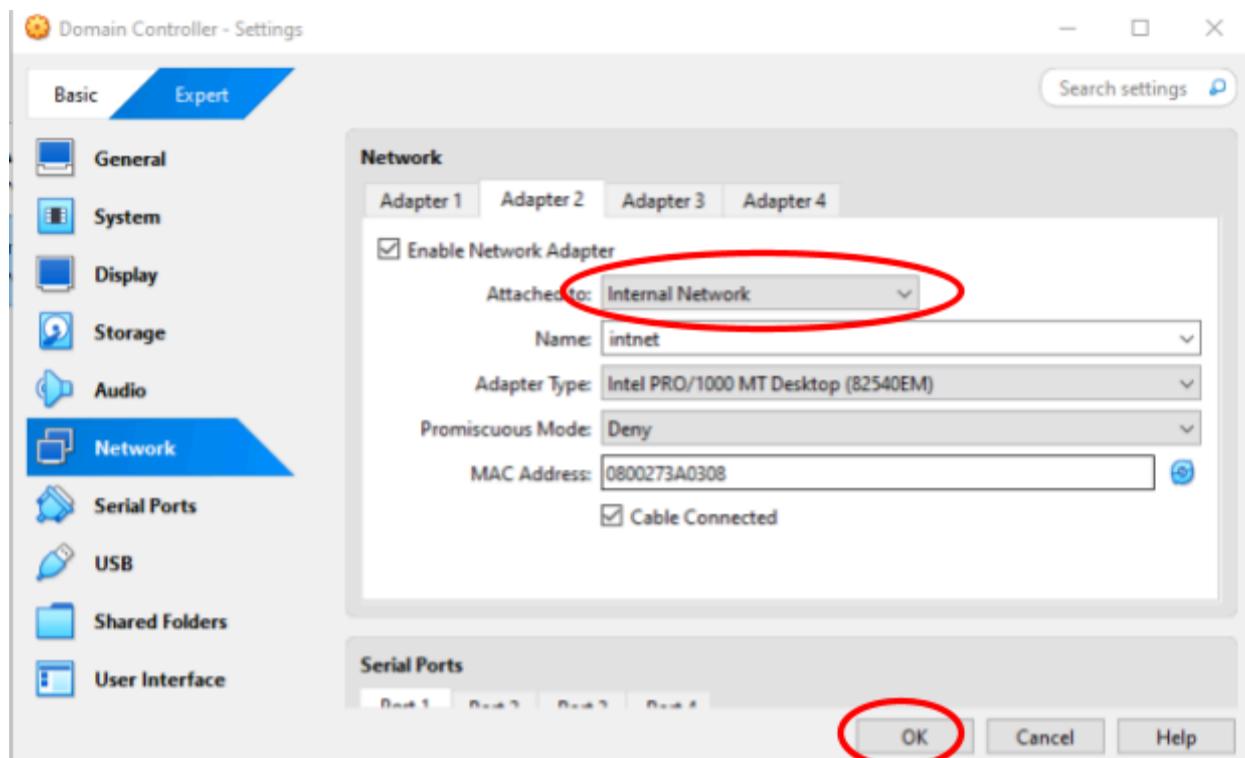
Add more CPUs to your processor under the System Tab



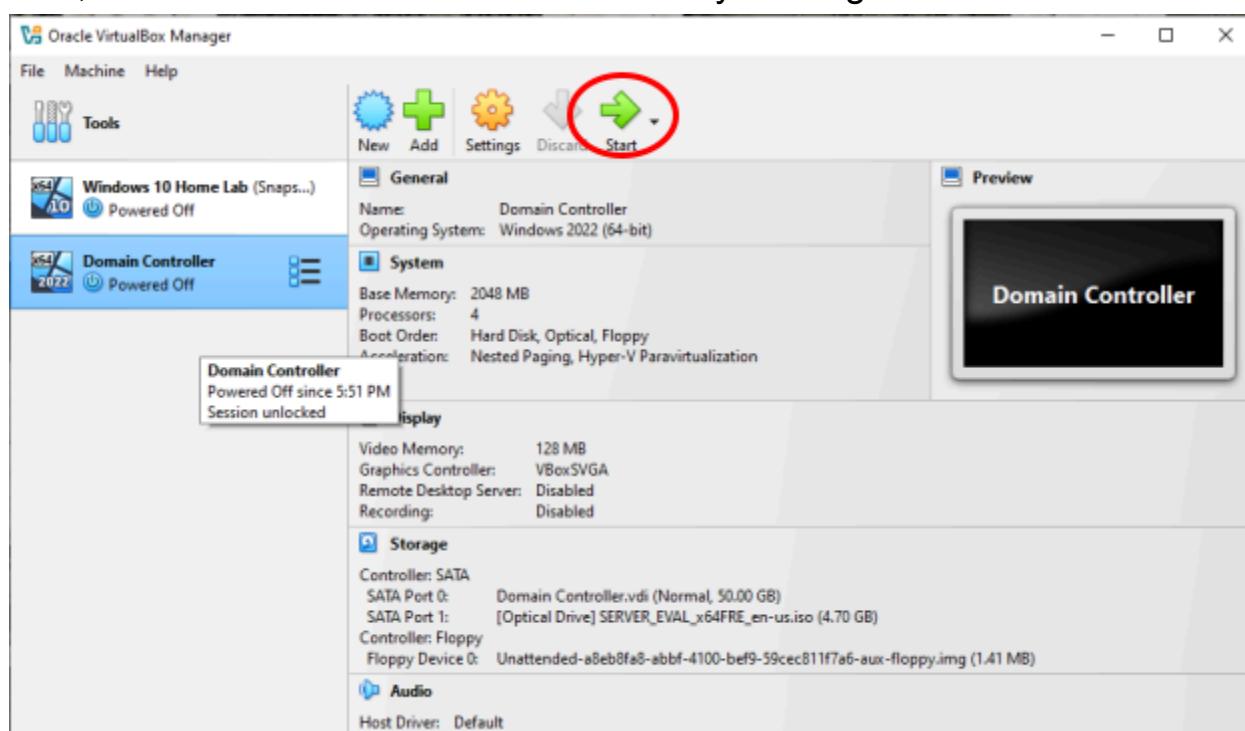
Under the Network Tab, make sure that Adapter 1 is attached to NAT and Adapter 2 is attached to your Internal Network. Once that is all configured, click Finish



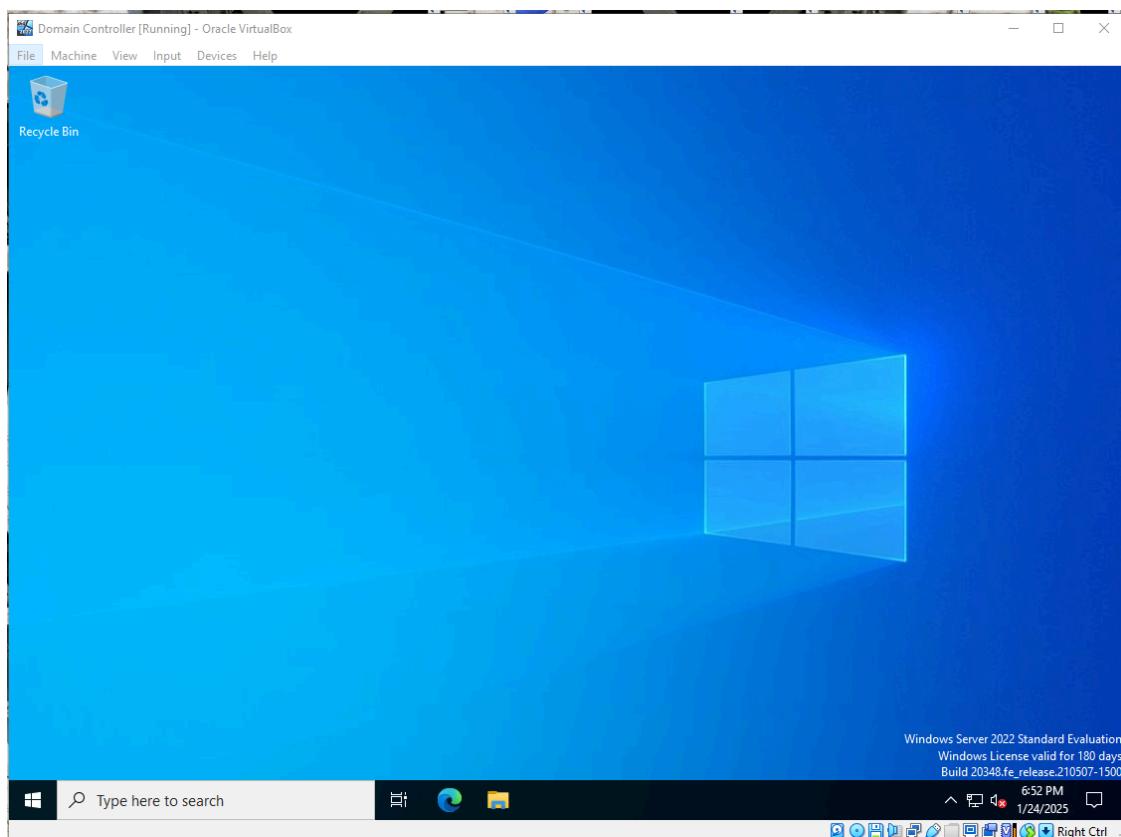
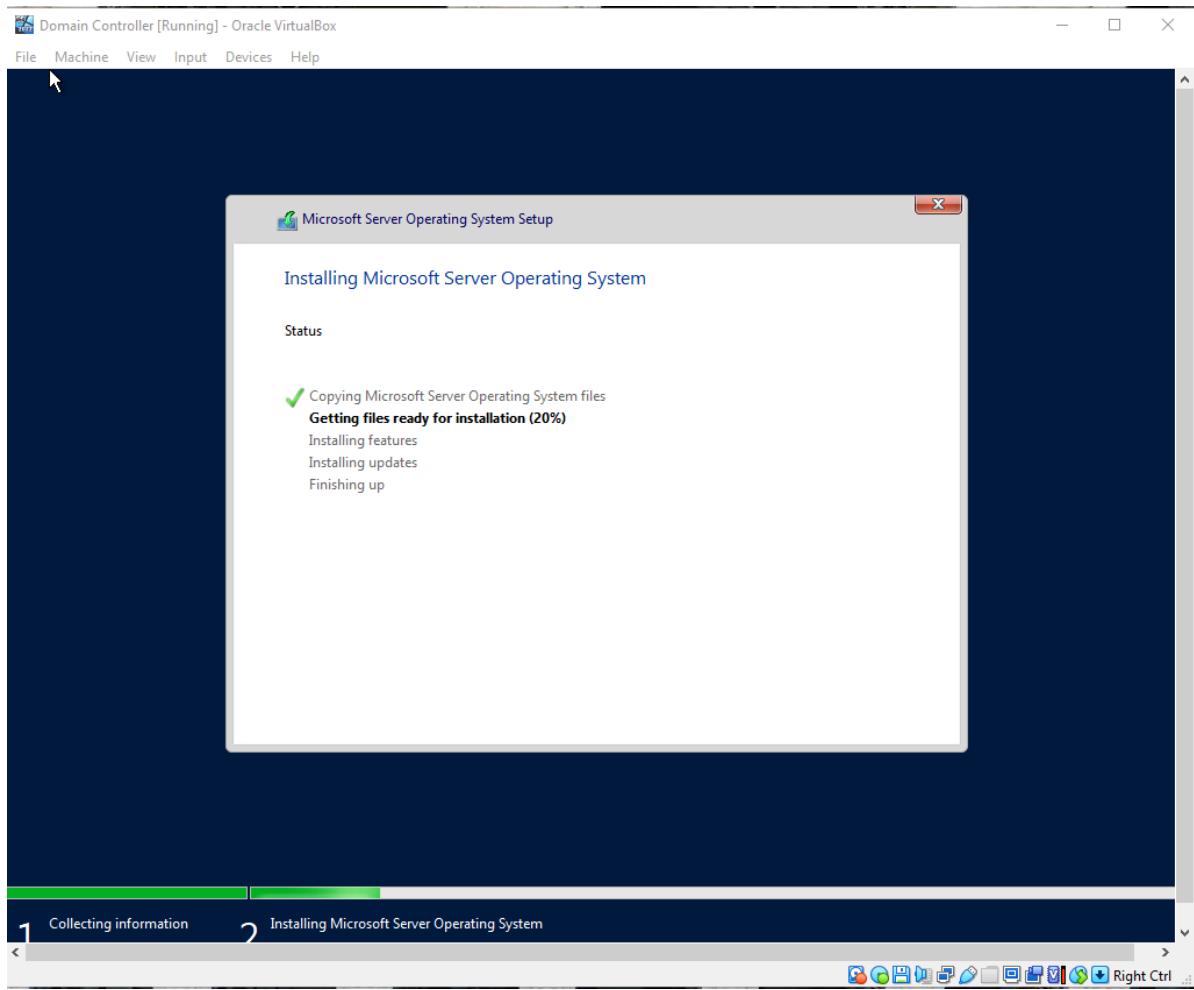




Now, it's time to Start the Virtual Machine by clicking Start

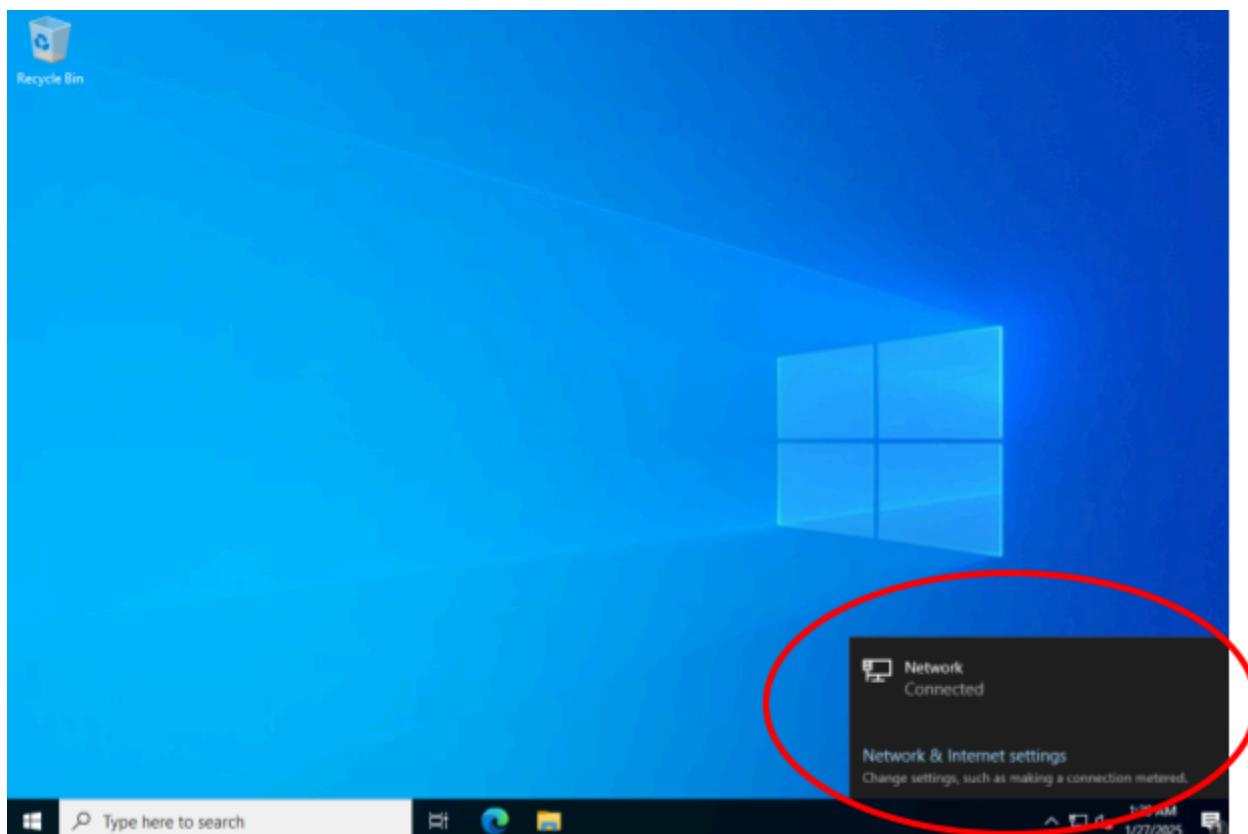
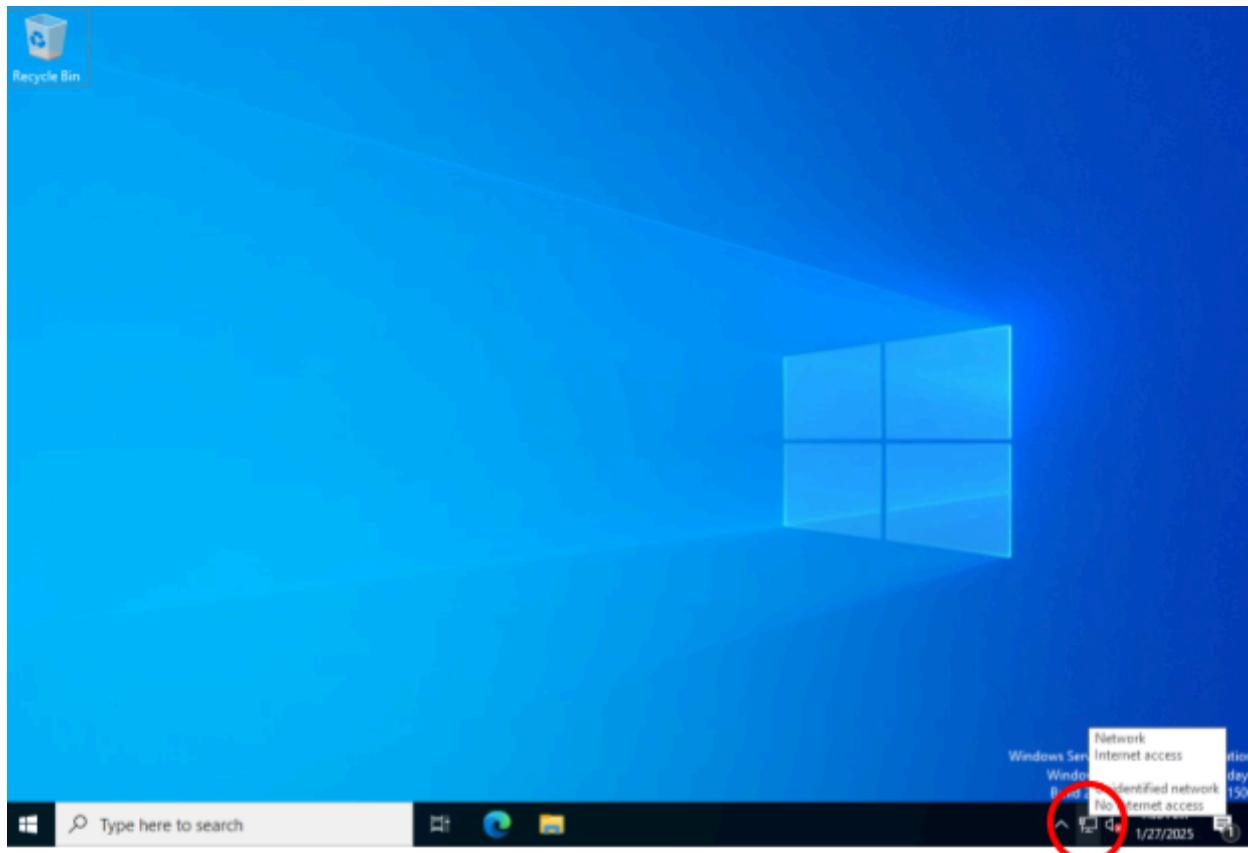


Go through the Installation Process and System Setup

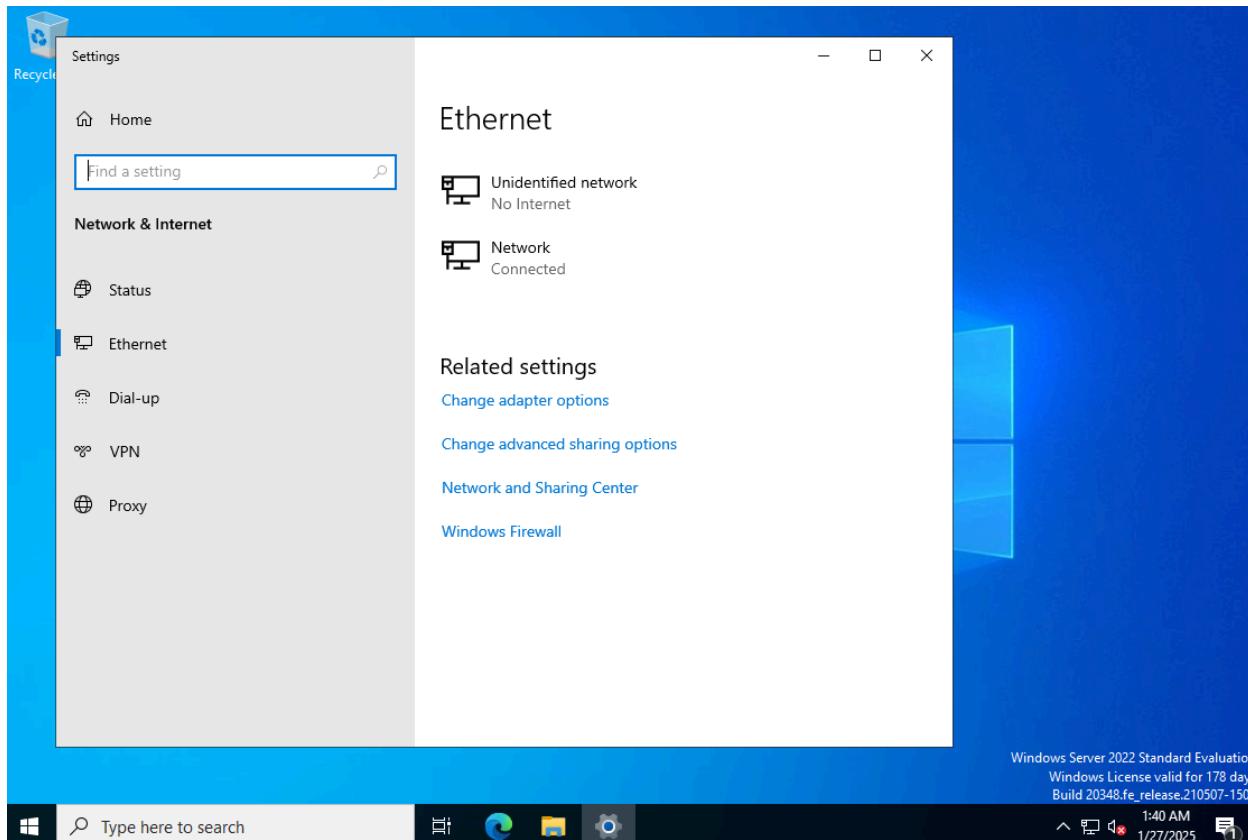


Step 3: Set Up the IP Addressing of the Windows Server 2022 Virtual Machine

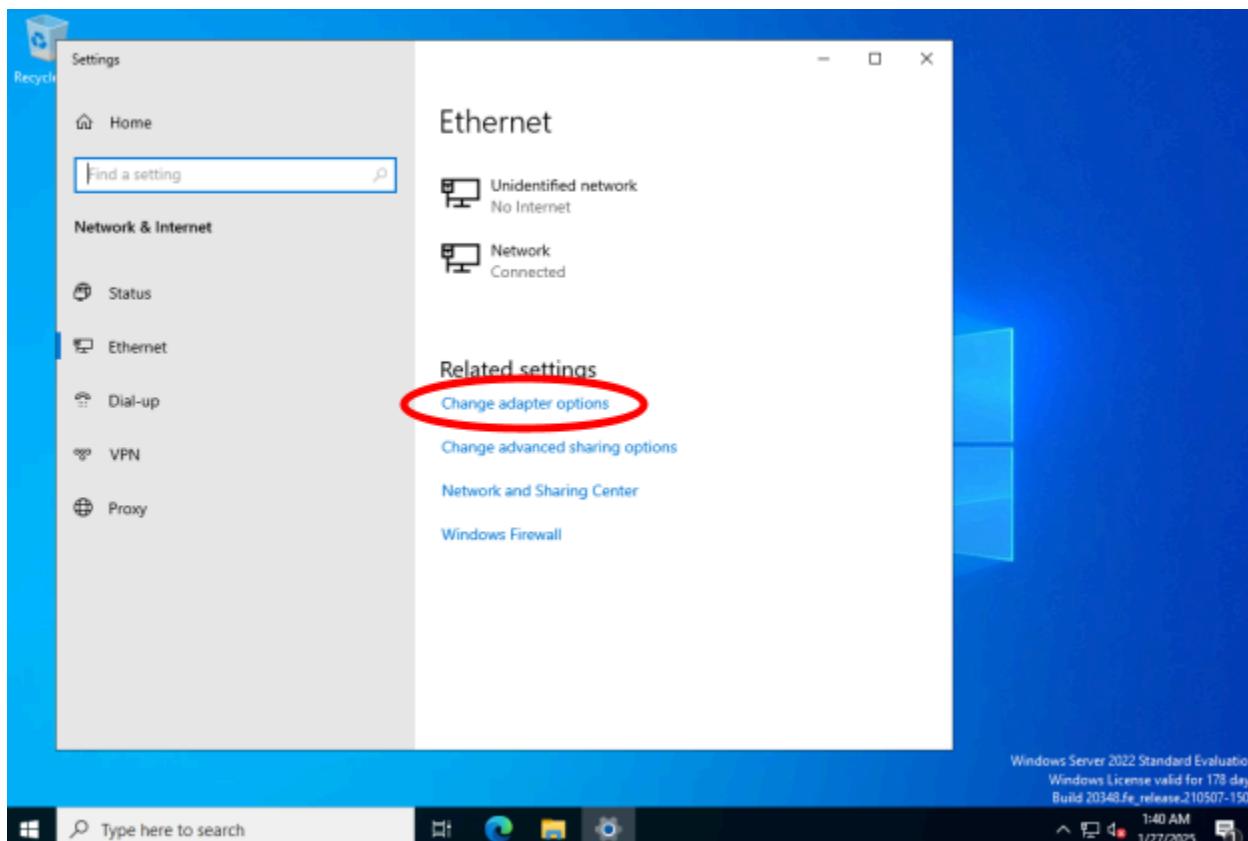
Start by navigating to the Notification Area on the bottom right of the OS and Left-Click on the Network Icon.



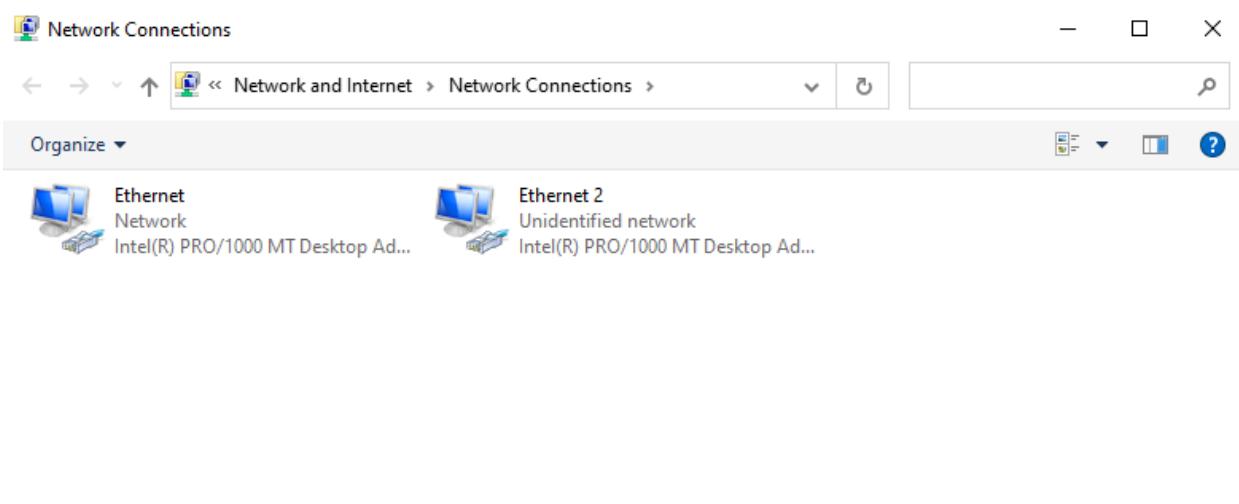
Click on Network & Internet Settings



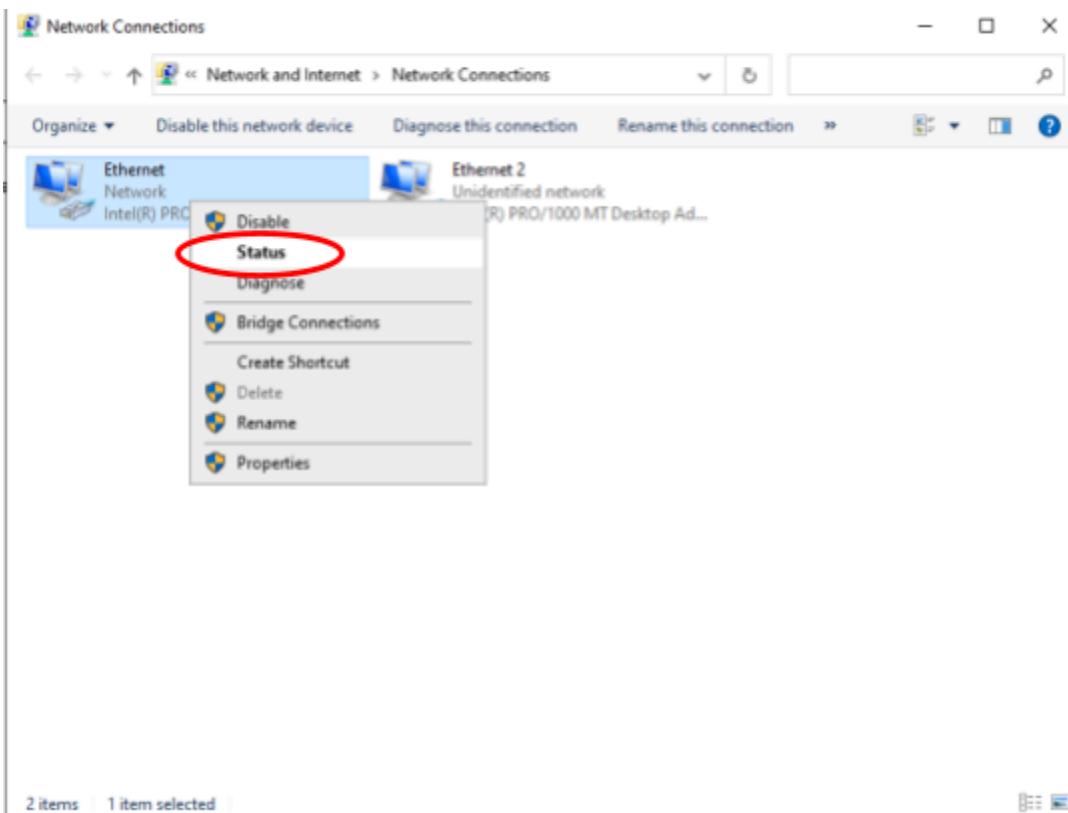
Select Change Adapter Options



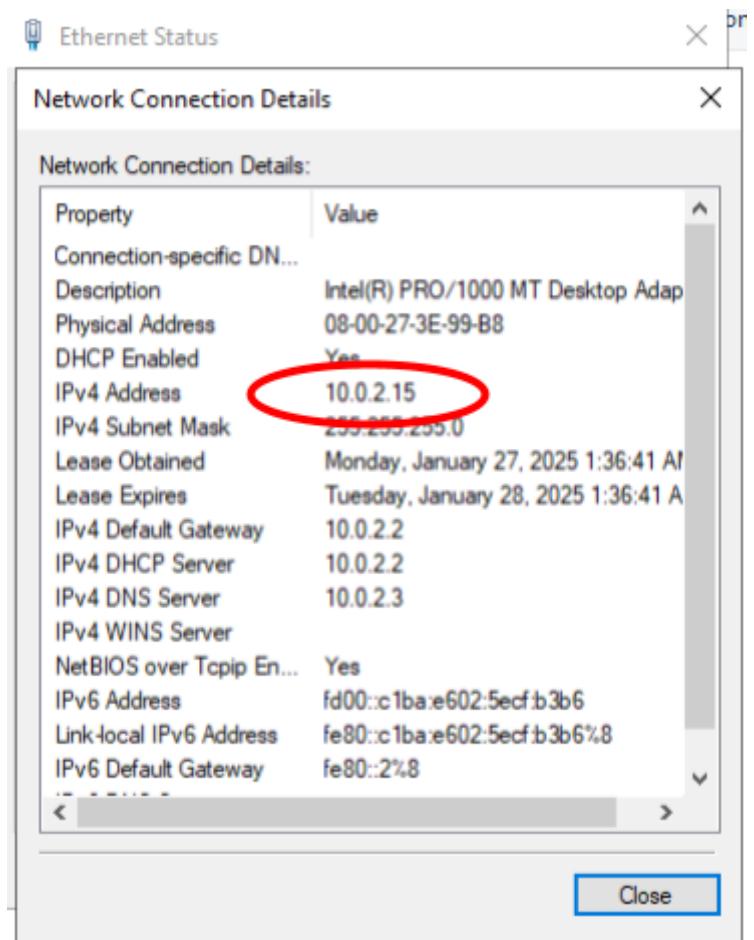
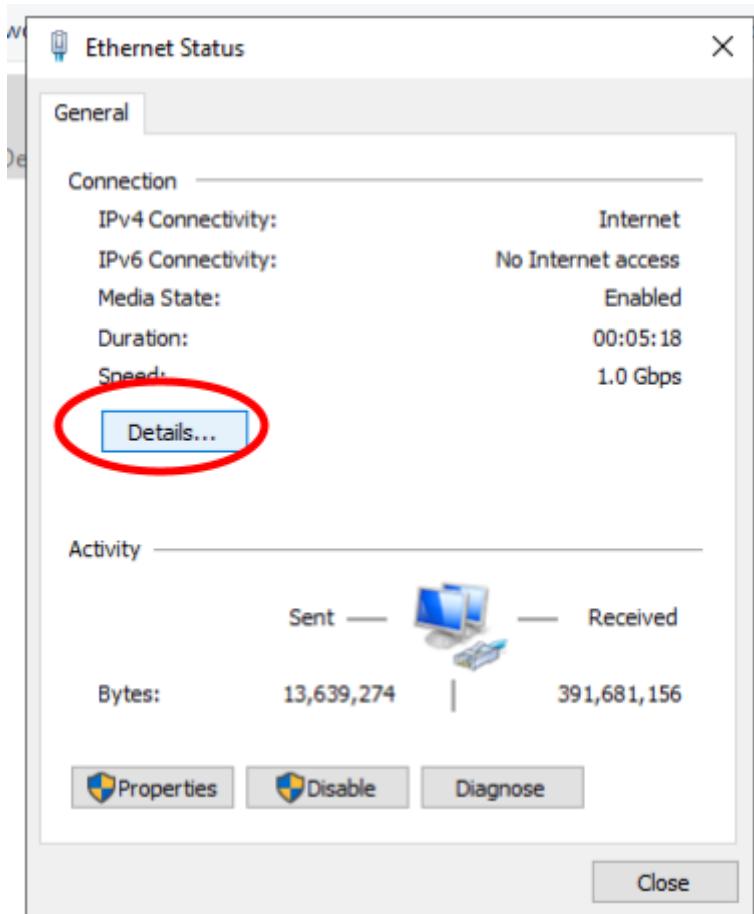
You will see your 2 Network Adapters we set up in the Virtual Box Settings



Right-Click on Ethernet 1 (Ethernet) and select Status to figure out which one is connected to the Internet and which one is connected to the Internal network. We will name them according to their connection.

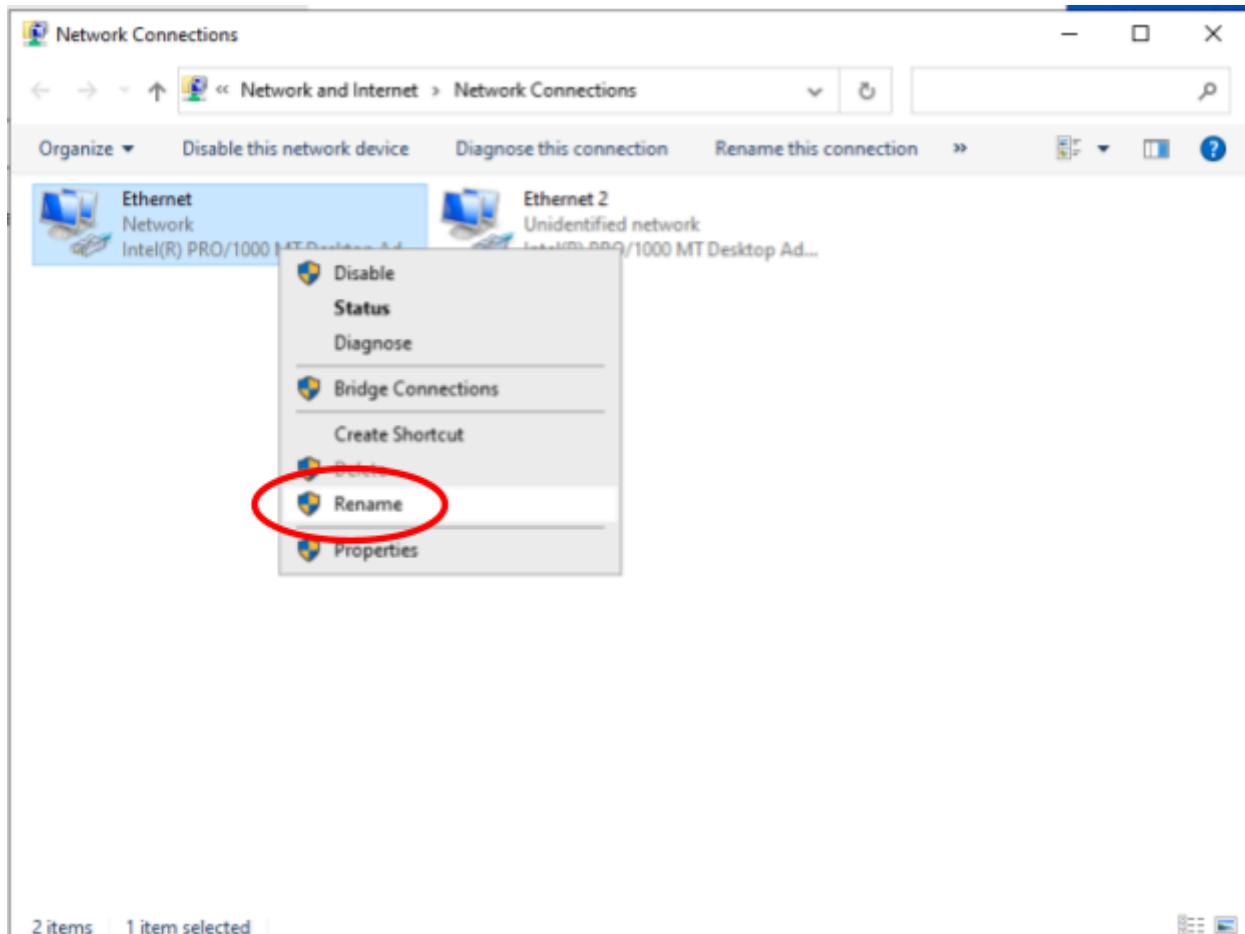


Click on Details

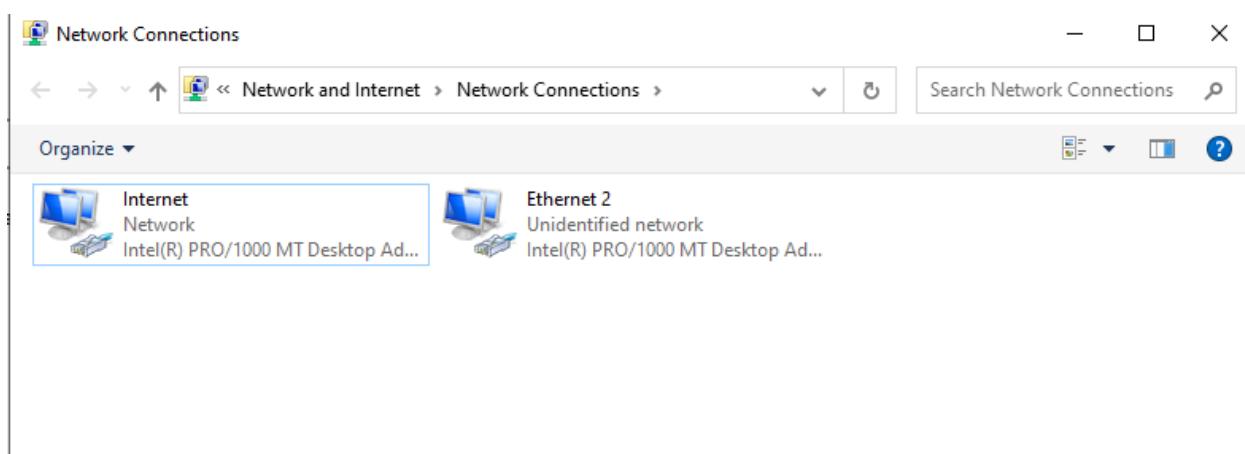


Above, we can see that the Ethernet Adapter has an IPv4 Address of 10.0.2.15, which is a proper home IP address so it's safe to assume that this adapter is connected to the Internet.

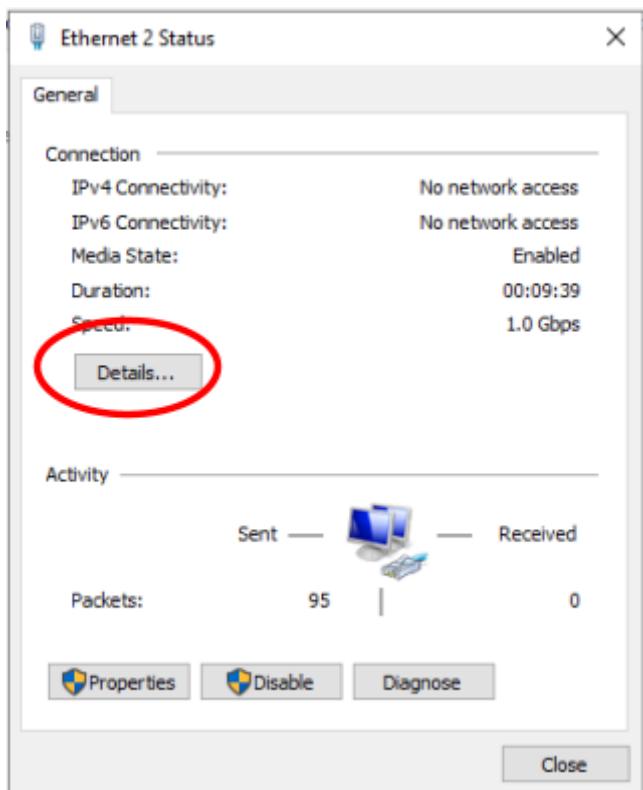
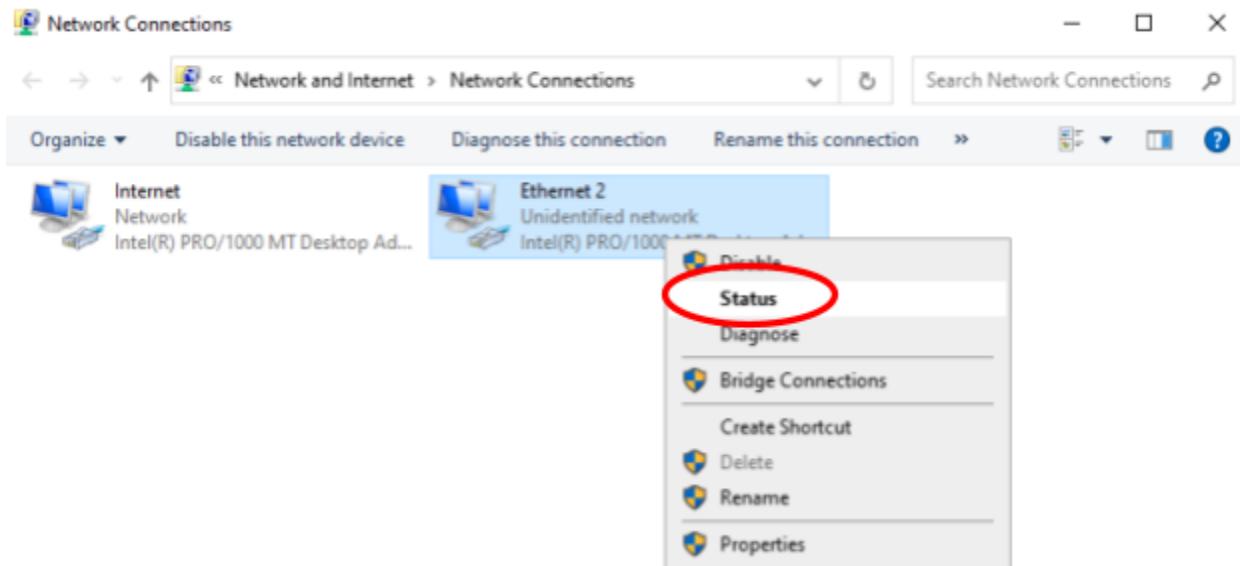
We can close that Dialog Box and right click on the adapter name Ethernet (Not Ethernet 2) and select Rename.

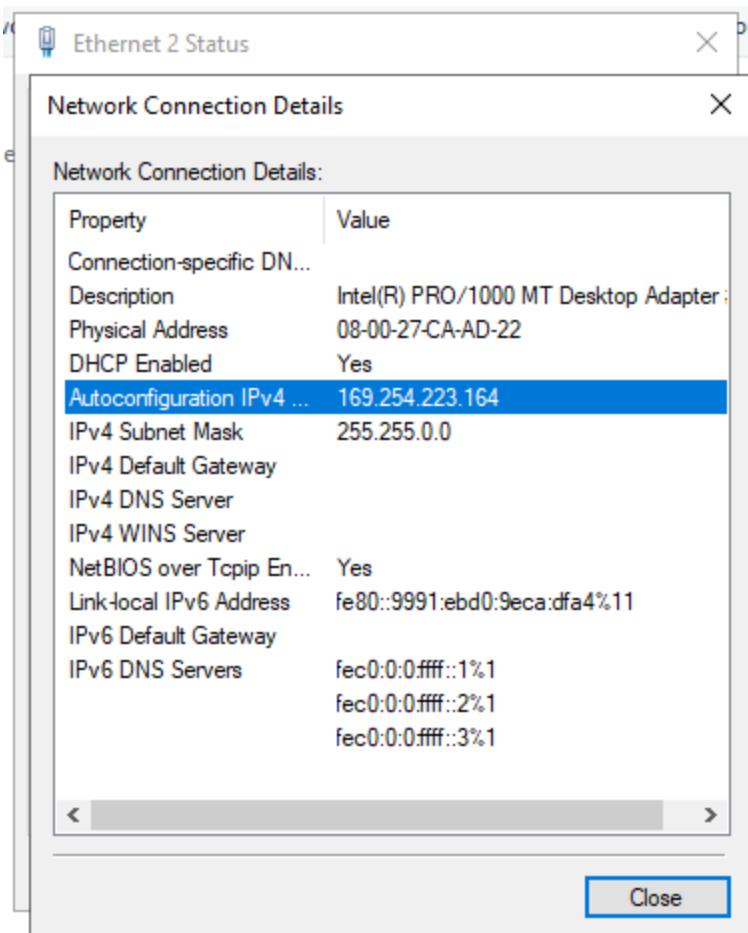


We will Rename it Internet



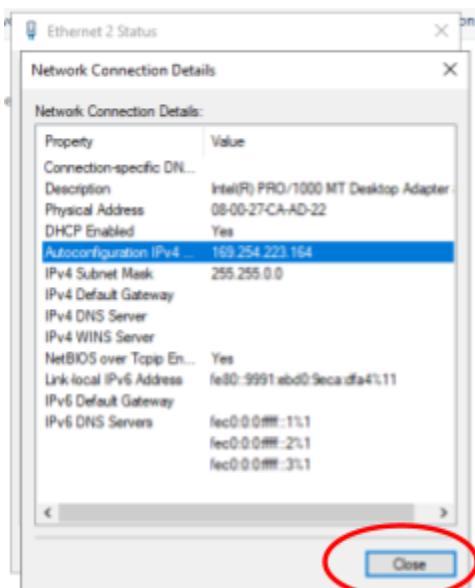
Next, we will check the IPv4 Address of Ethernet 2 by going through the same steps we did for Ethernet. We will Right-Click on Ethernet 2 and select Status

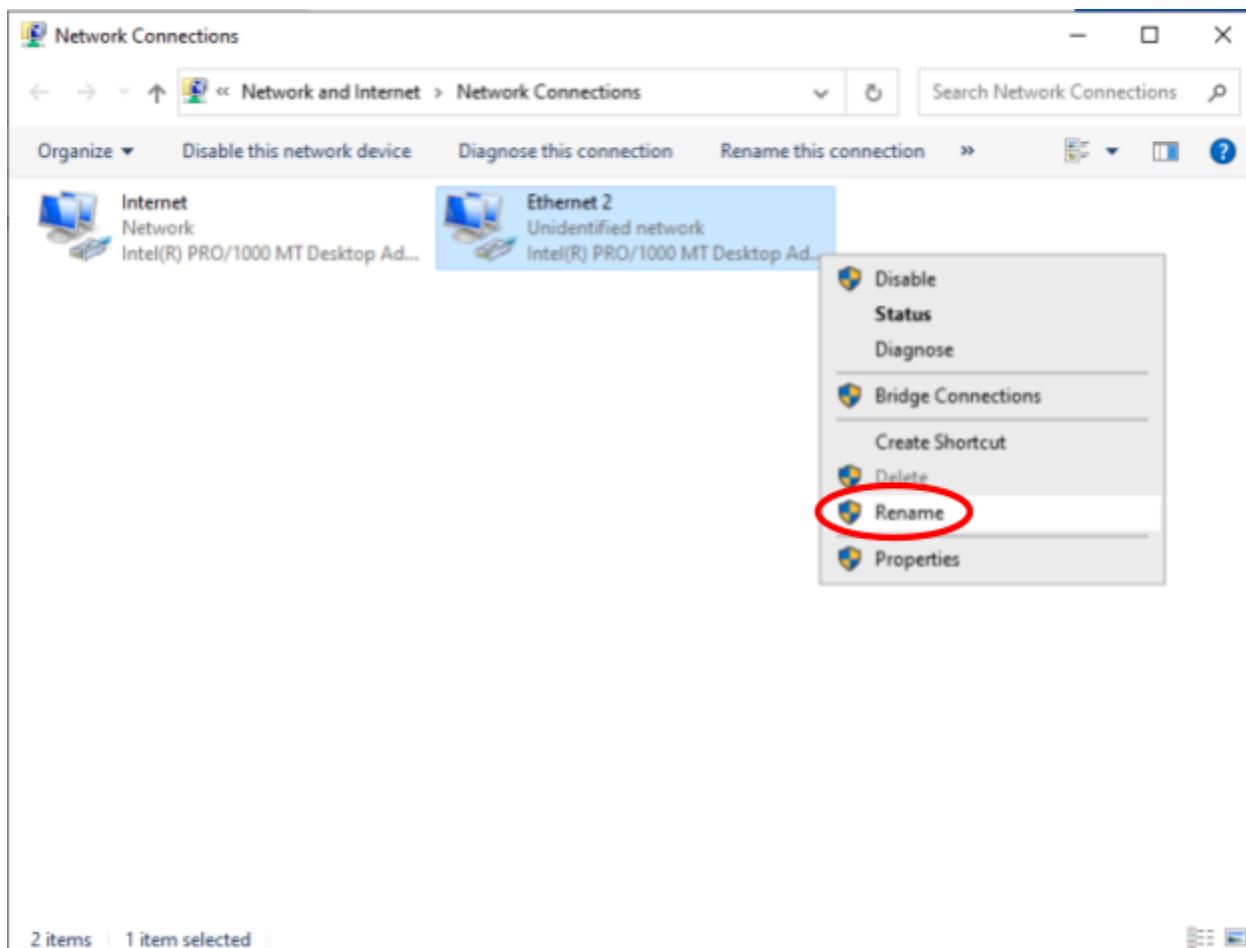




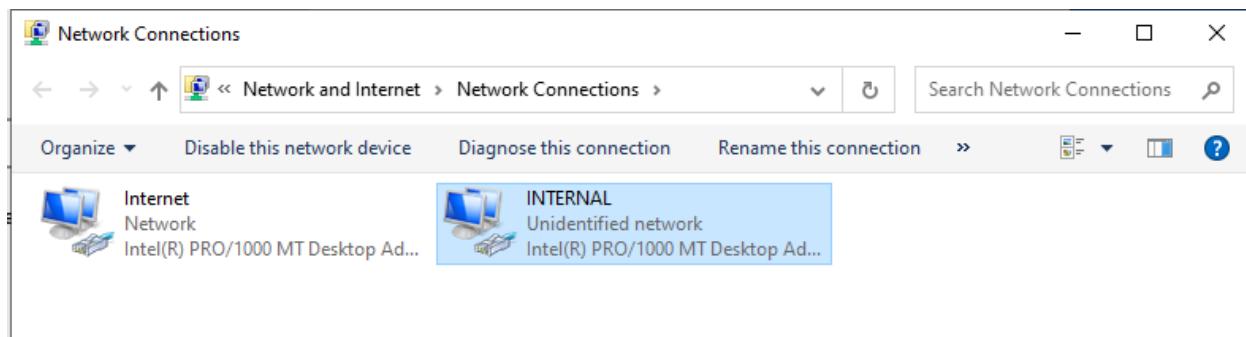
We can see that the Ethernet 2 adapter has an IPv4 address of 169.254.223.164. This means that this adapter was looking for a DHCP server to acquire an IP address and was unable to find one. Therefore, the IP address 169.254.223.164 was automatically assigned to it. This is how we can tell it is the Internal Adapter and we will name it as such.

We will close the Dialog Box and rename the adapter.

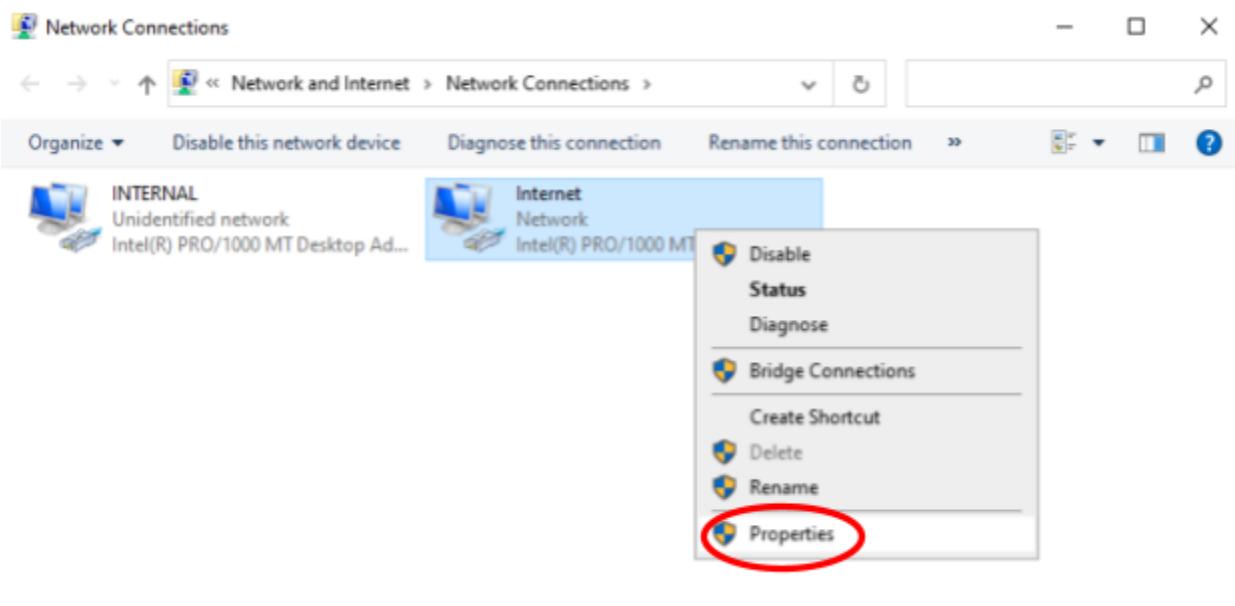




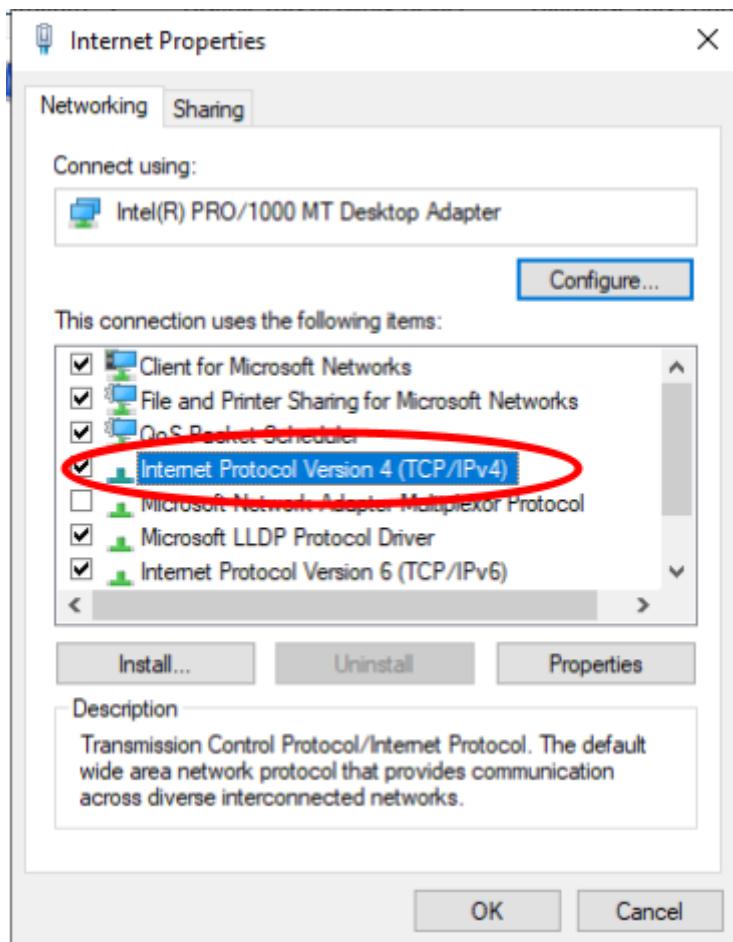
We will Rename it INTERNAL



Next, we will assign an IP address to the INTERNAL Adapter by Right-Clicking on it and selecting Properties



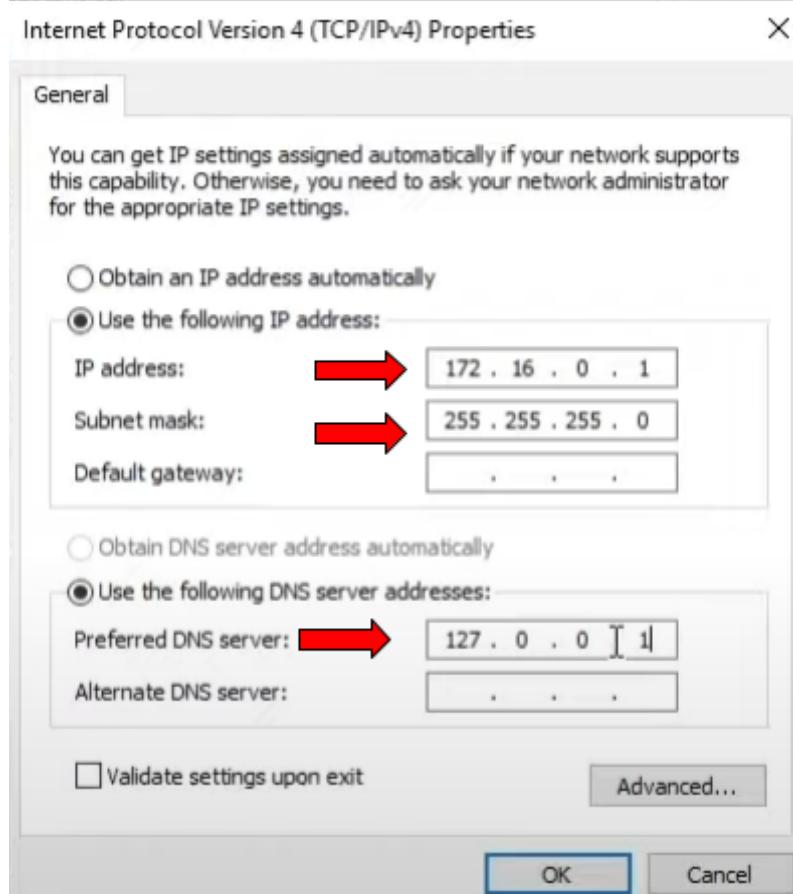
Double-click on the Internet Protocol Version 4 (TCP /IPv4)



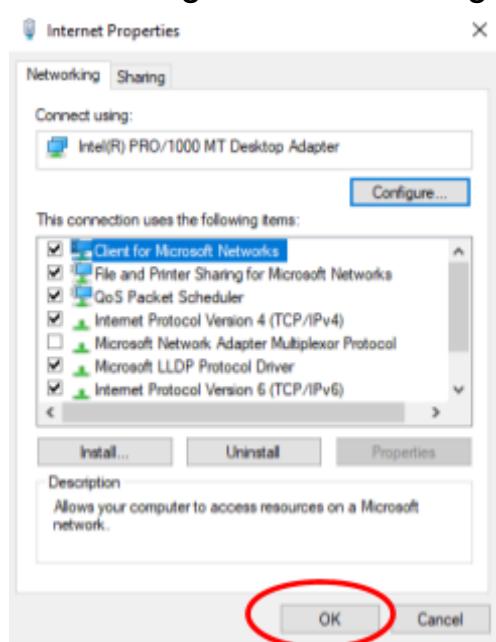
Select the Use the following IP address and assign it the IP address according to the Network Diagram on the first page of this Documentation

We will use the Loopback Address of 127.0.0.1 to use as the DNS server so that our Domain Controller can assign IP addresses to Clients based on a Scope of IP addresses.

Click OK when finished

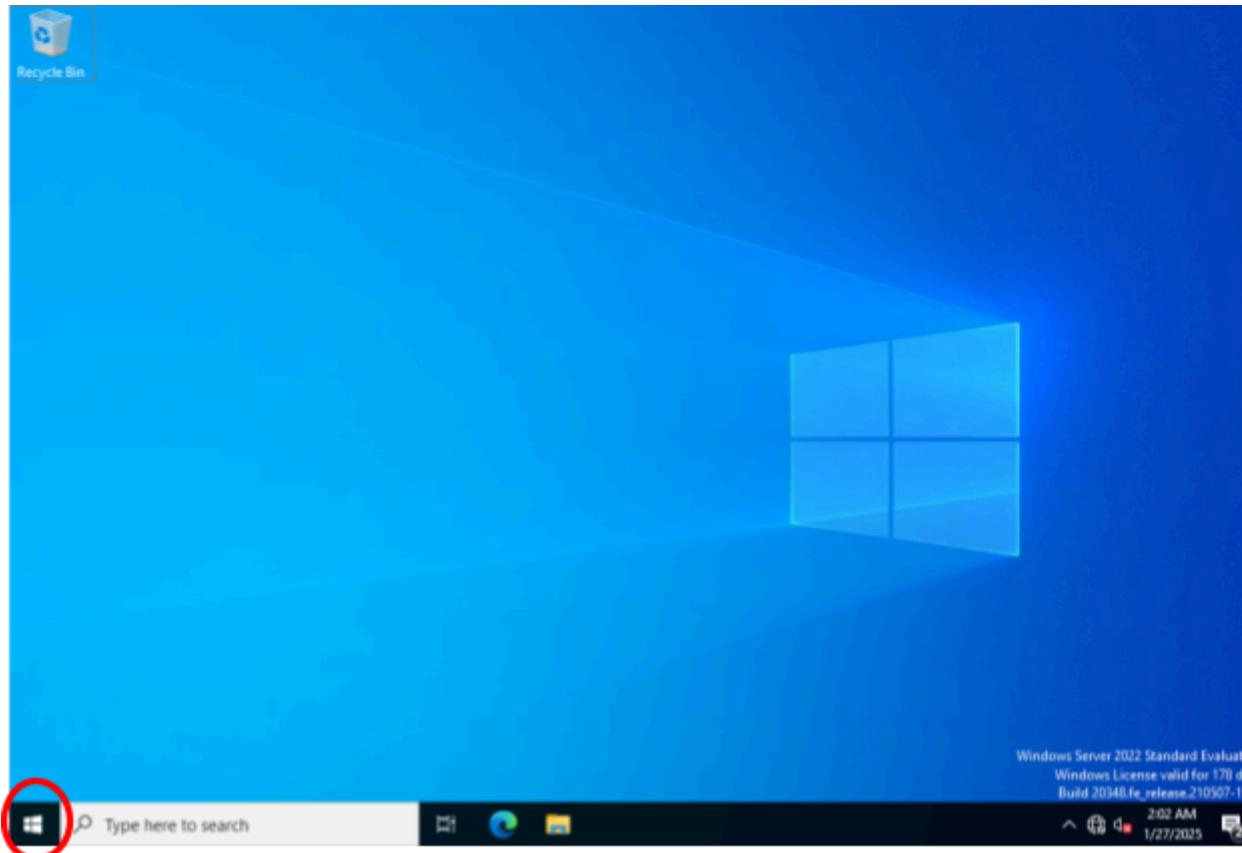


Click OK again to finish assigning an IP address to the Internal Adapter

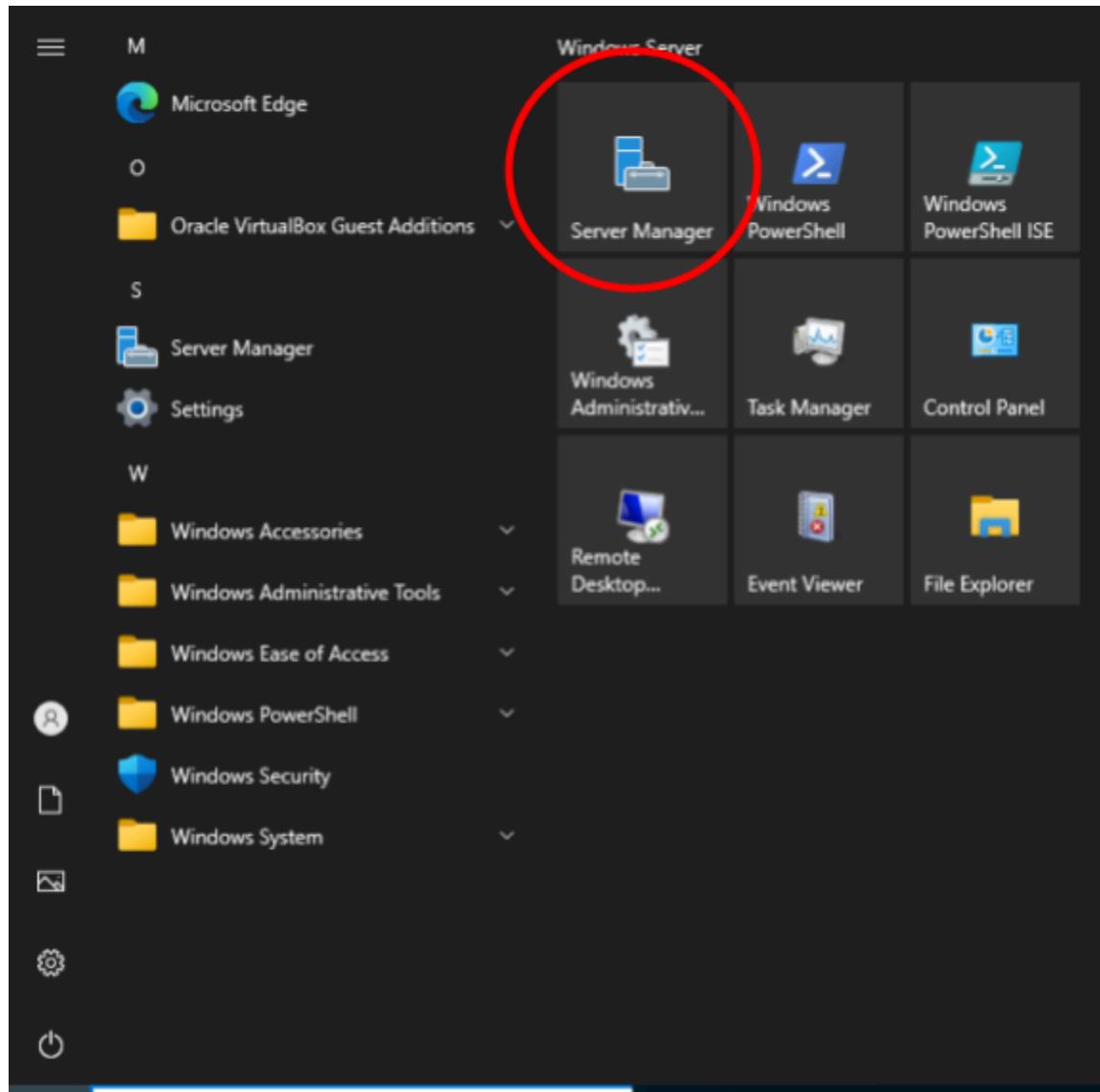


Step 4: Install Active Directory Domain Services and Create a Domain

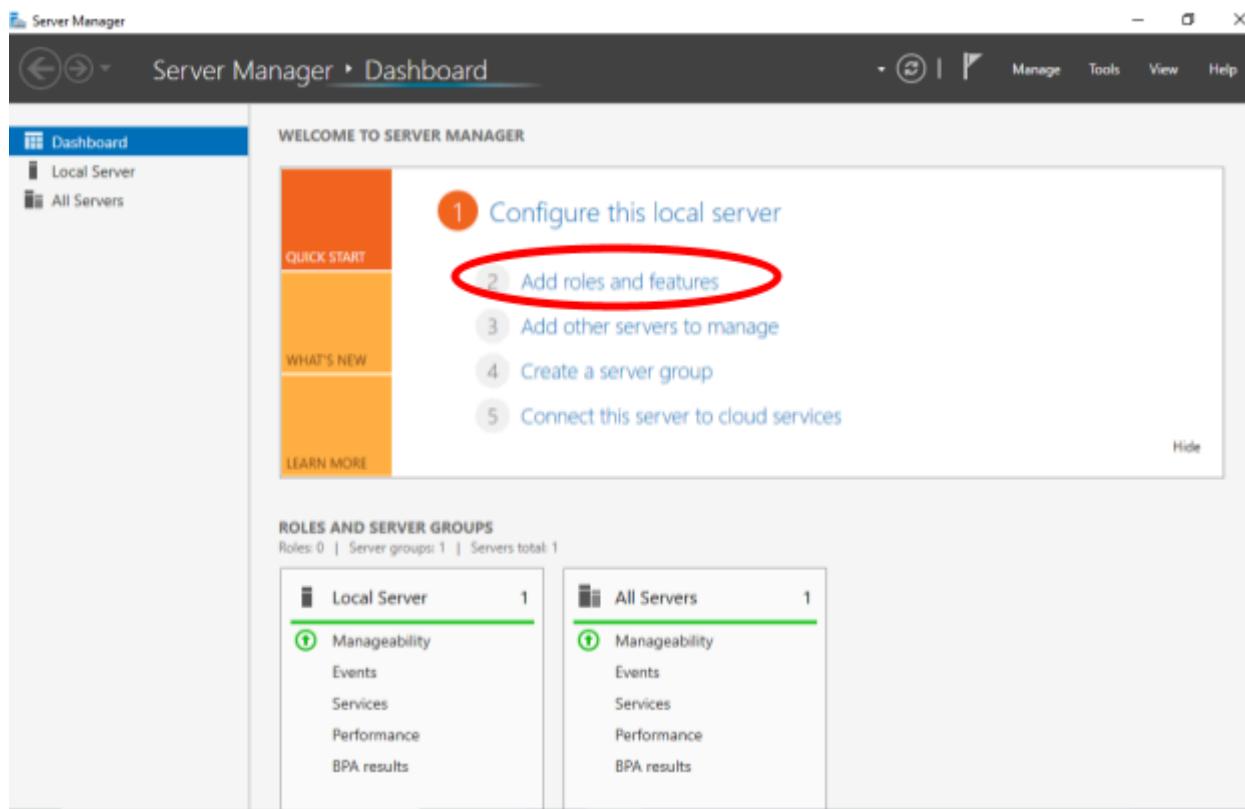
Start by Selecting the Start menu on the Bottom-Left Corner of the screen



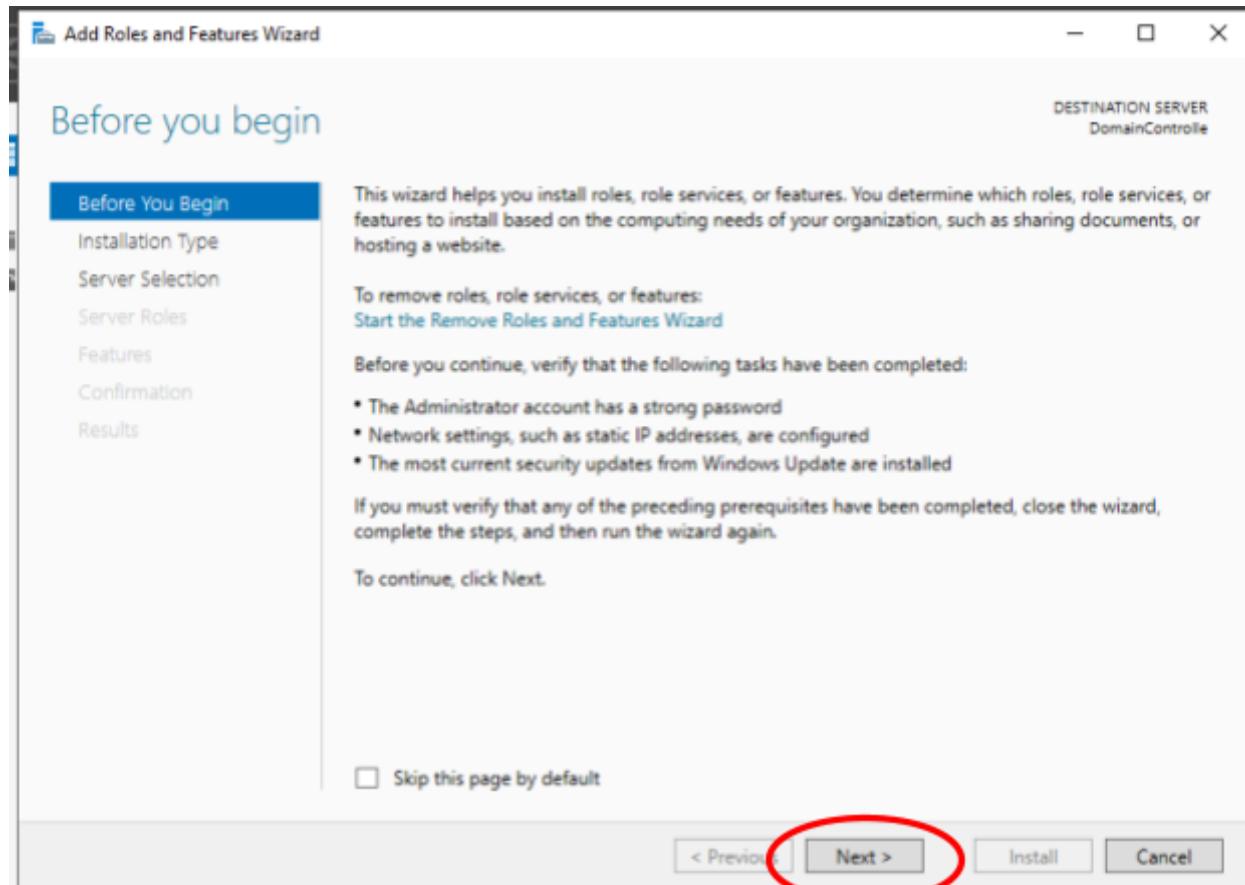
Select Server Manager

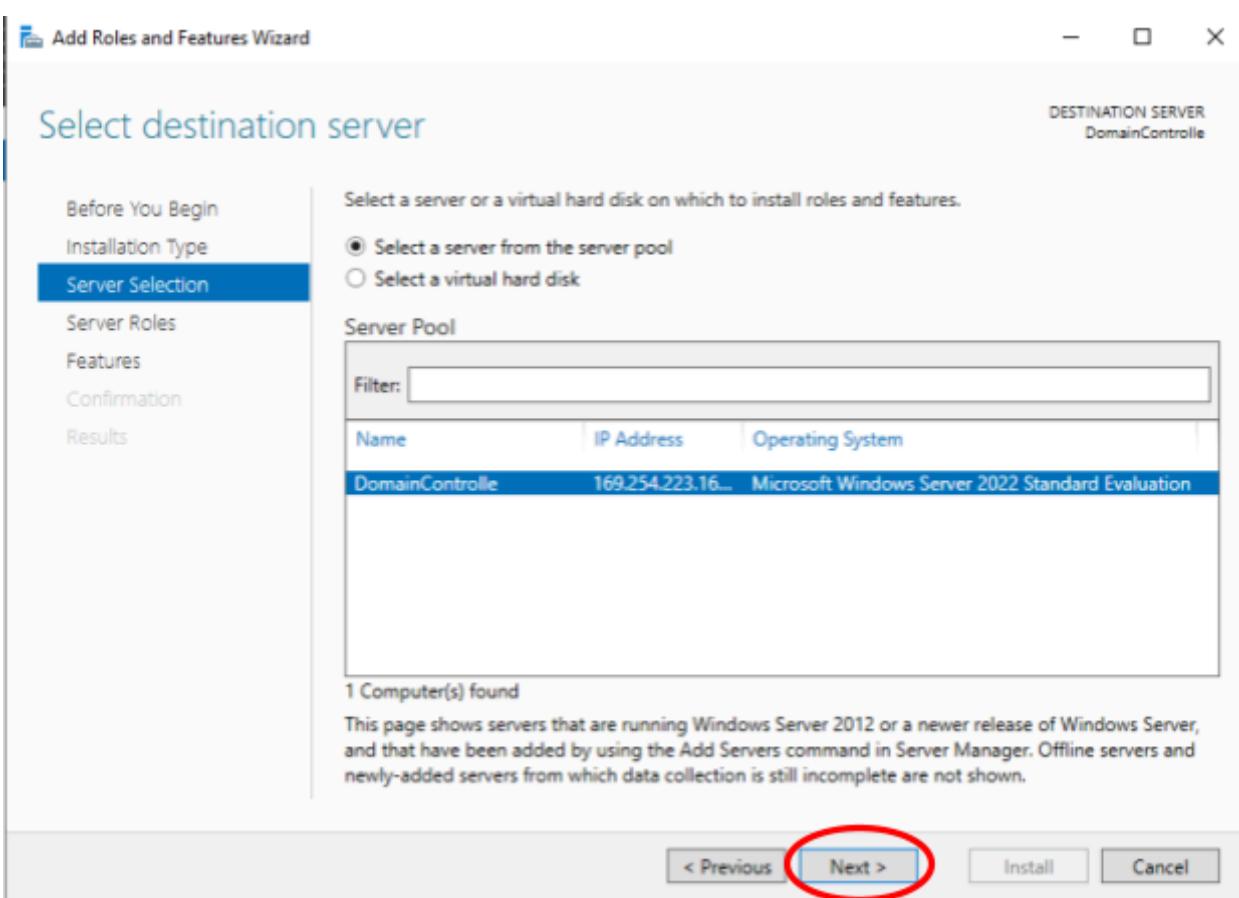
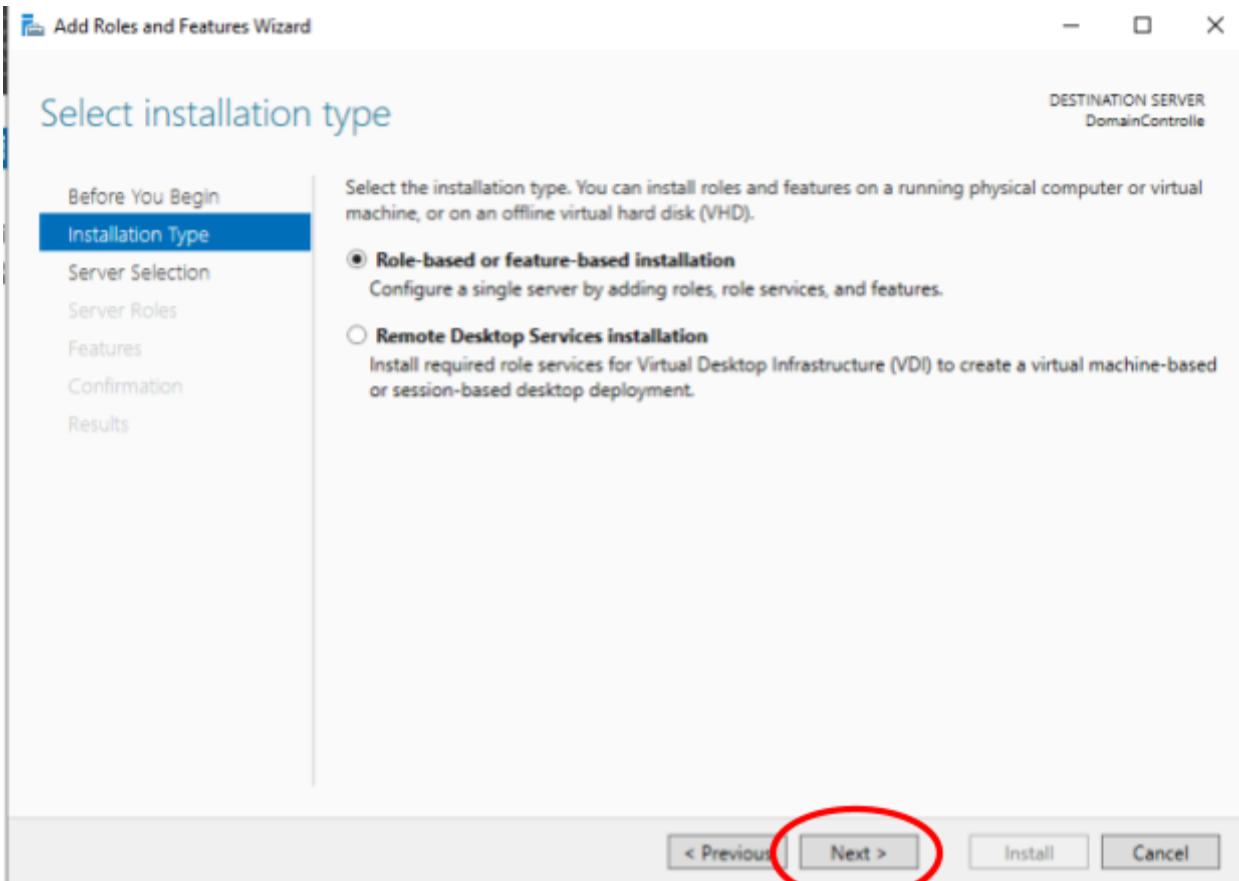


Select Add Roles and Features



Click Next until you get to Select Server Roles tab





Select server roles

DESTINATION SERVER
DomainController

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

- Active Directory Certificate Services
- Active Directory Domain Services
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Device Health Attestation
- DHCP Server
- DNS Server
- Fax Server
- File and Storage Services (1 of 12 installed)
- Host Guardian Service
- Hyper-V
- Network Policy and Access Services
- Print and Document Services
- Remote Access
- Remote Desktop Services
- Volume Activation Services
- Web Server (IIS)
- Windows Deployment Services
- Windows Server Update Services

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

< Previous

Next >

Install

Cancel

Select Active Directory Domain Services

DESTINATION SERVER
DomainController

Select server roles

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

- Active Directory Certificate Services
- Active Directory Domain Services
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Device Health Attestation
- DHCP Server
- DNS Server
- Fax Server
- File and Storage Services (1 of 12 installed)
- Host Guardian Service
- Hyper-V
- Network Policy and Access Services
- Print and Document Services
- Remote Access
- Remote Desktop Services
- Volume Activation Services
- Web Server (IIS)
- Windows Deployment Services
- Windows Server Update Services

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

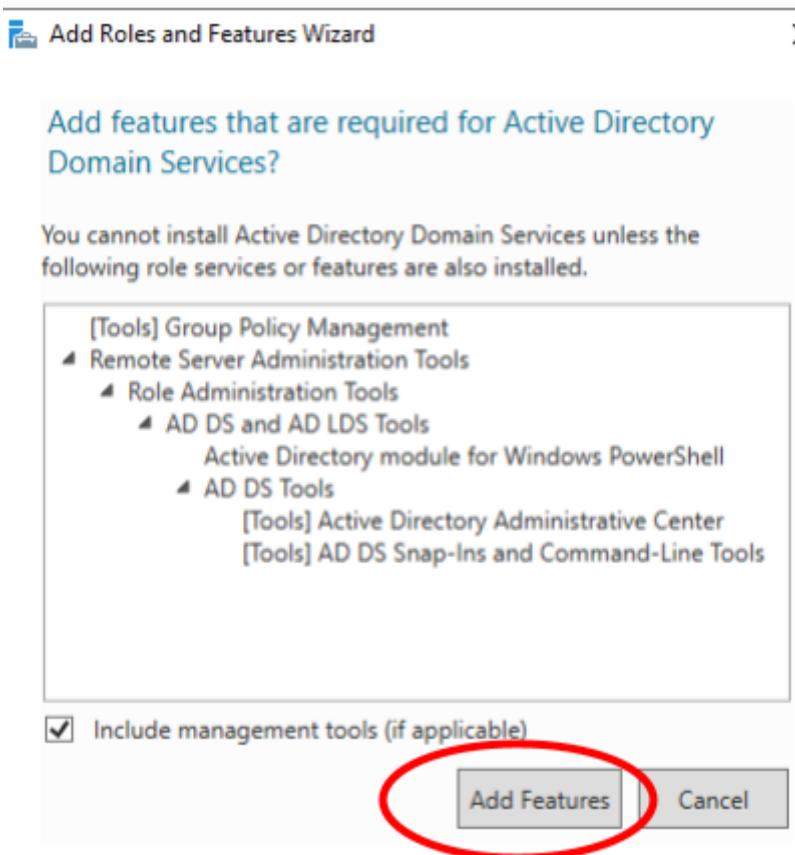
< Previous

Next >

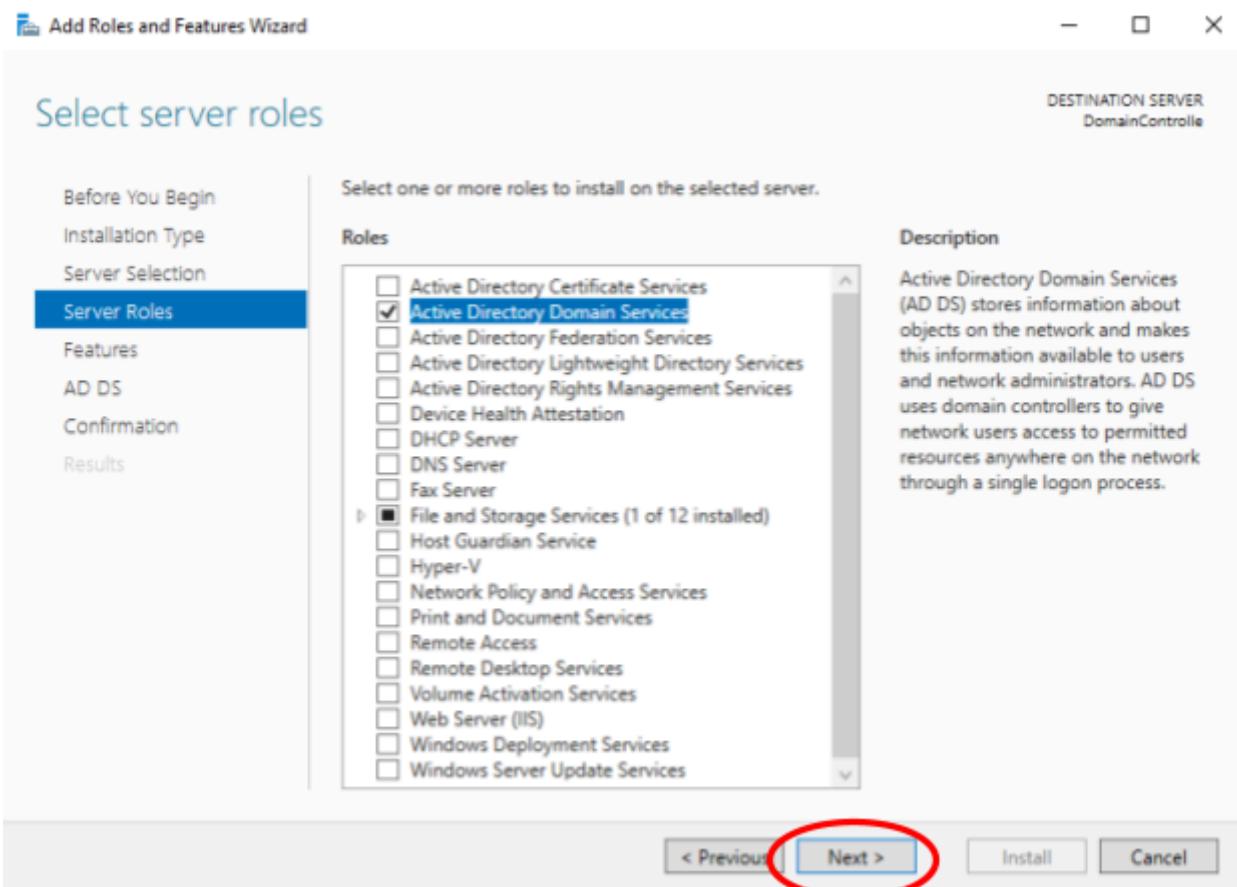
Install

Cancel

Click Add Features



Click Next until you reach the Install Option



Add Roles and Features Wizard

Select features

DESTINATION SERVER
DomainController

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results

Select one or more features to install on the selected server.

Features

Features	Description
<input type="checkbox"/> .NET Framework 3.5 Features	.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
<input checked="" type="checkbox"/> .NET Framework 4.8 Features (2 of 7 installed)	
<input type="checkbox"/> Background Intelligent Transfer Service (BITS)	
<input type="checkbox"/> BitLocker Drive Encryption	
<input type="checkbox"/> BitLocker Network Unlock	
<input type="checkbox"/> BranchCache	
<input type="checkbox"/> Client for NFS	
<input type="checkbox"/> Containers	
<input type="checkbox"/> Data Center Bridging	
<input type="checkbox"/> Direct Play	
<input type="checkbox"/> Enhanced Storage	
<input type="checkbox"/> Failover Clustering	
<input checked="" type="checkbox"/> Group Policy Management	
<input type="checkbox"/> Host Guardian Hyper-V Support	
<input type="checkbox"/> I/O Quality of Service	
<input type="checkbox"/> IIS Hostable Web Core	
<input type="checkbox"/> Internet Printing Client	
<input type="checkbox"/> IP Address Management (IPAM) Server	
<input type="checkbox"/> LPR Port Monitor	

< Previous | **Next >** | Install | Cancel

Add Roles and Features Wizard

Active Directory Domain Services

DESTINATION SERVER
DomainController

Before You Begin
Installation Type
Server Selection
Server Roles
AD DS
Confirmation
Results

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.

 Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.
[Learn more about Azure Active Directory](#)
[Configure Office 365 with Azure Active Directory Connect](#)

< Previous | **Next >** | Install | Cancel

DESTINATION SERVER
DomainController

Confirm installation selections

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

Confirmation

Results

To install the following roles, role services, or features on selected server, click Install.

 Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Domain Services

Group Policy Management

Remote Server Administration Tools

Role Administration Tools

AD DS and AD LDS Tools

Active Directory module for Windows PowerShell

AD DS Tools

Active Directory Administrative Center

AD DS Snap-Ins and Command-Line Tools

Export configuration settings

Specify an alternate source path

< Previous

Next >

Install

Cancel

Click Install

DESTINATION SERVER
DomainController

Installation progress

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

Confirmation

Results

View installation progress

i Feature installation

Installation started on DomainController

Active Directory Domain Services

Group Policy Management

Remote Server Administration Tools

Role Administration Tools

AD DS and AD LDS Tools

Active Directory module for Windows PowerShell

AD DS Tools

Active Directory Administrative Center

AD DS Snap-Ins and Command-Line Tools

 You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

< Previous

Next >

Close

Cancel

Installation progress

DESTINATION SERVER
DomainController

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results

View installation progress

i Feature installation

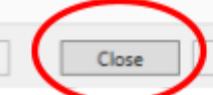
Configuration required. Installation succeeded on DomainController.

Active Directory Domain Services

Additional steps are required to make this machine a domain controller.

[Promote this server to a domain controller](#)**Group Policy Management****Remote Server Administration Tools****Role Administration Tools****AD DS and AD LDS Tools****Active Directory module for Windows PowerShell****AD DS Tools****Active Directory Administrative Center****AD DS Snap-Ins and Command-Line Tools**

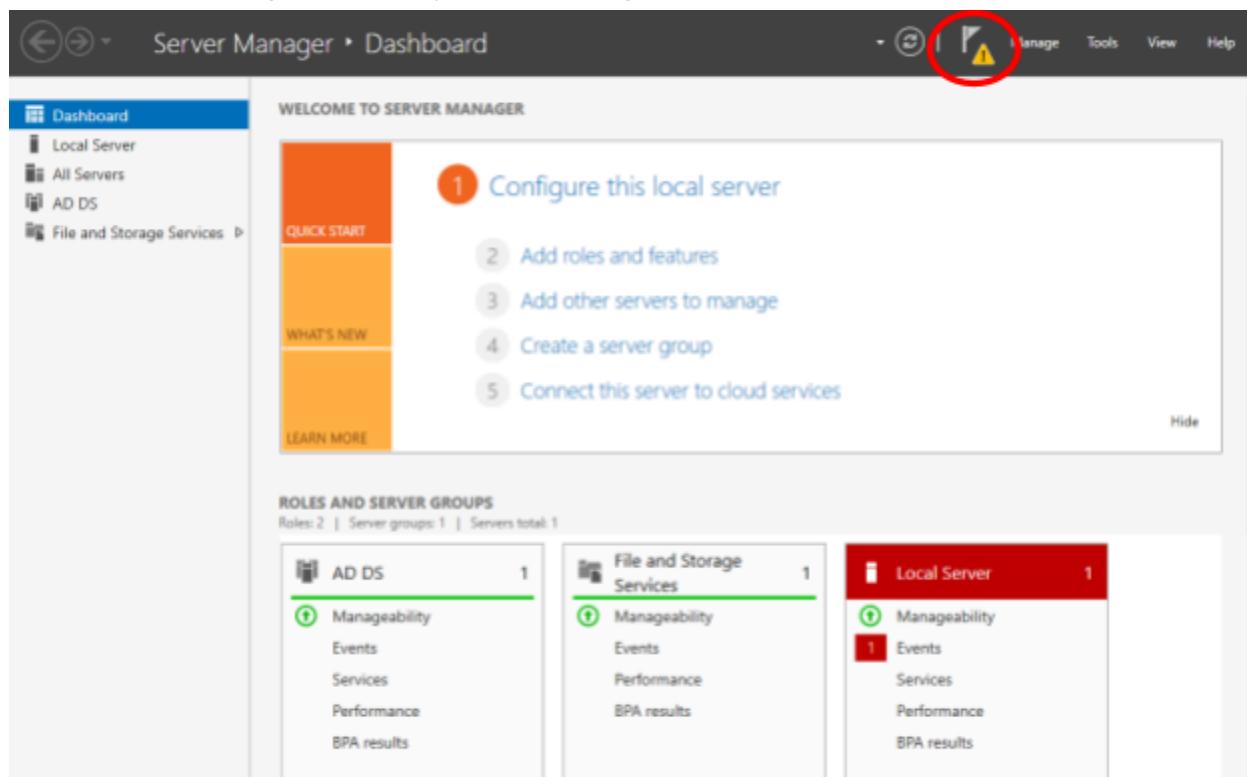
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

[Export configuration settings](#)[< Previous](#)[Next >](#)[Close](#)[Cancel](#)

Once it is finished Installing, click Close

This will bring you back to the Server Manager Dashboard

Click on the Flag with the yellow triangle with an exclamation mark



The screenshot shows the Server Manager Dashboard. At the top, there's a navigation bar with icons for Back, Forward, Home, and Help, followed by "Server Manager • Dashboard". To the right of the navigation bar is a "Manage" button with a yellow warning icon (exclamation mark) and a red circle around it. Below the navigation bar, the main area has a "WELCOME TO SERVER MANAGER" header. On the left, there's a sidebar with links: Dashboard, Local Server, All Servers, AD DS, and File and Storage Services. The "File and Storage Services" link is expanded, showing sub-links: QUICK START, WHAT'S NEW, and LEARN MORE. The main content area displays a list of tasks: 1. Configure this local server, 2. Add roles and features, 3. Add other servers to manage, 4. Create a server group, and 5. Connect this server to cloud services. At the bottom, there's a section titled "ROLES AND SERVER GROUPS" with a summary: Roles: 2 | Server groups: 1 | Servers total: 1. Three cards are shown: "AD DS" (green background), "File and Storage Services" (green background), and "Local Server" (red background). Each card lists "Manageability", "Events", "Services", "Performance", and "BPA results".

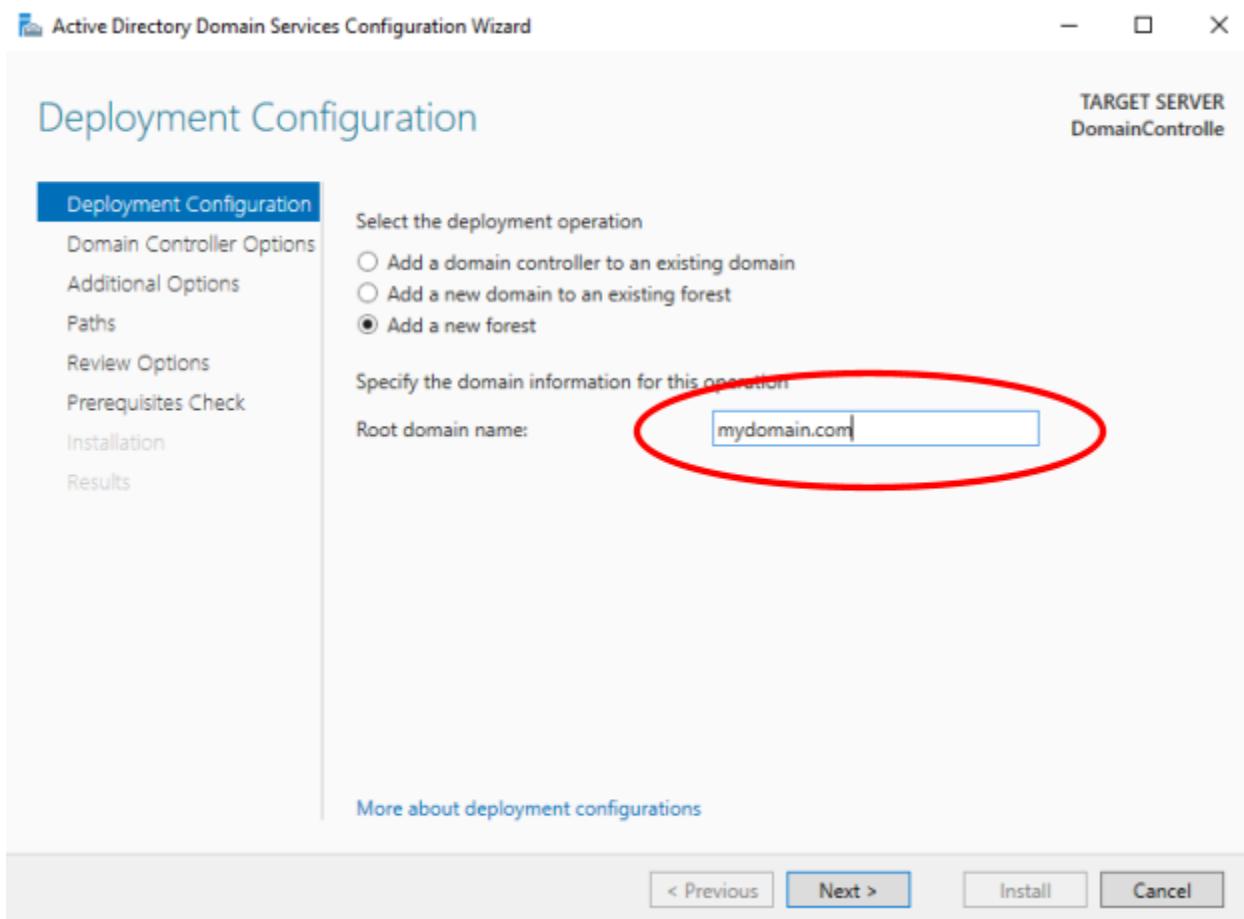
Select “Promote this server to a domain controller”

The screenshot shows the Windows Server Manager Dashboard. A red circle highlights the "Post-deployment Configuration" section, which contains a link labeled "Promote this server to a domain controller". Below this, there is a "Feature Installation" status message indicating successful installation on DomainController. The dashboard also displays sections for "QUICK START", "WHAT'S NEW", and "LEARN MORE". Under "ROLES AND SERVER GROUPS", three categories are listed: AD DS (1 instance), File and Storage Services (1 instance), and Local Server (1 instance). Each category has a "Manageability" section and other metrics like Events, Services, Performance, and BPA results.

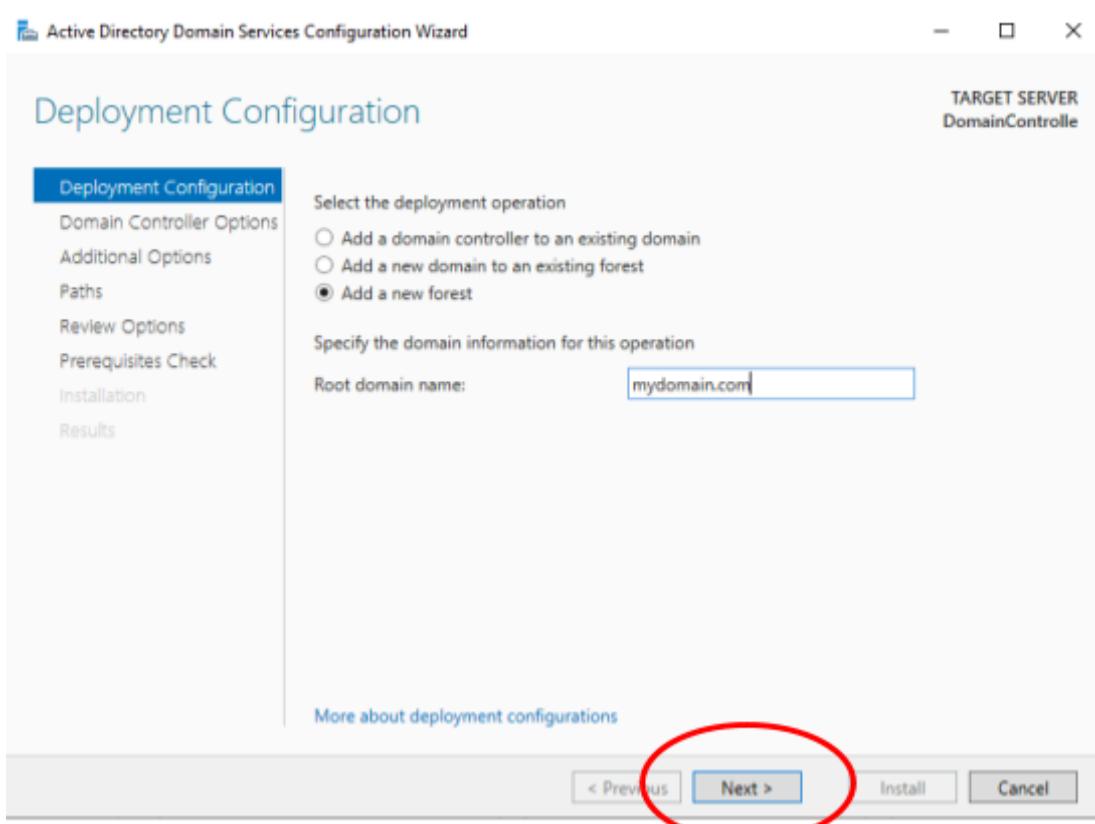
Select Add a new forest

The screenshot shows the "Active Directory Domain Services Configuration Wizard" window, specifically the "Deployment Configuration" step. On the left, a navigation pane lists steps: Deployment Configuration, Domain Controller Options, Additional Options, Paths, Review Options, Prerequisites Check, Installation, and Results. The main area is titled "Deployment Configuration" and shows the "Select the deployment operation" section. It includes three radio button options: "Add a domain controller to an existing domain" (selected), "Add a new domain to an existing forest", and "Add a new forest". A red circle highlights the "Add a new forest" option. Below this, it says "Specify the domain information for this operation" and "Domain:" followed by a text input field and a "Select..." button. At the bottom, it says "Supply the credentials to perform this operation" and shows "<No credentials provided>" with a "Change..." button. At the very bottom, there is a link "More about deployment configurations" and a row of buttons: < Previous, Next >, Install, and Cancel.

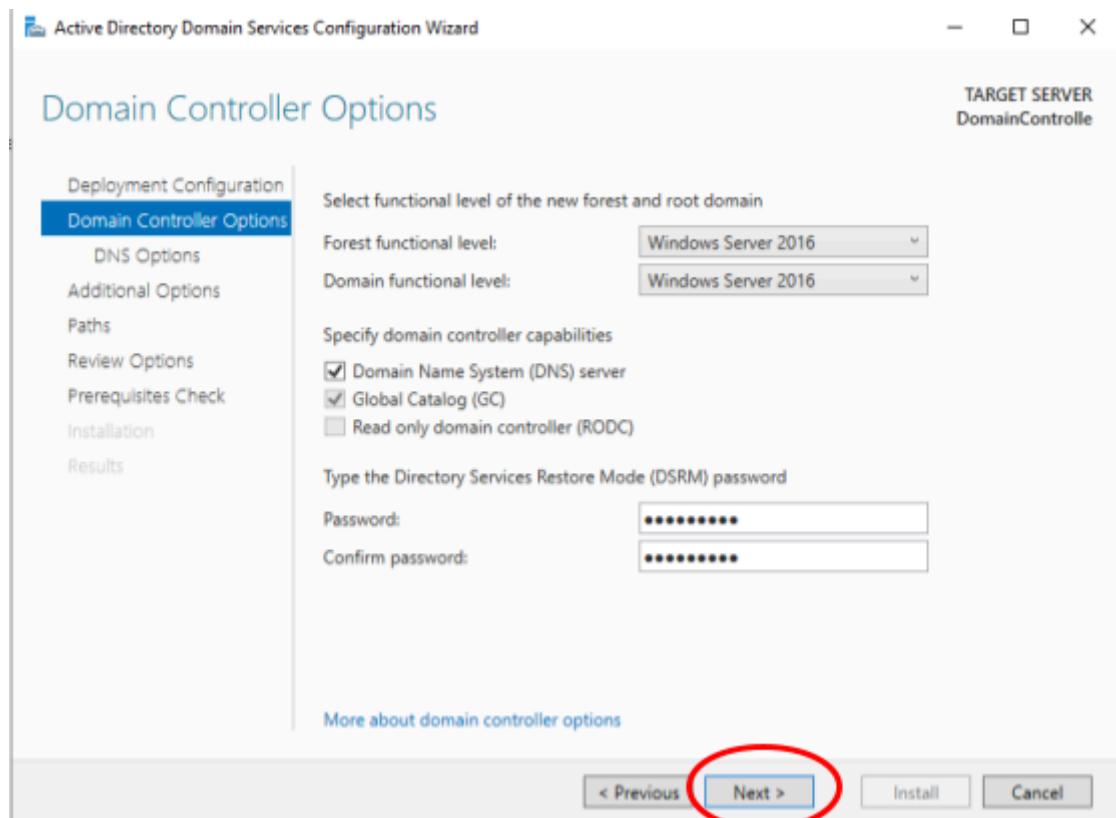
Select a Root Domain Name. Since this is a lab environment, we will name this domain "mydomain.com"



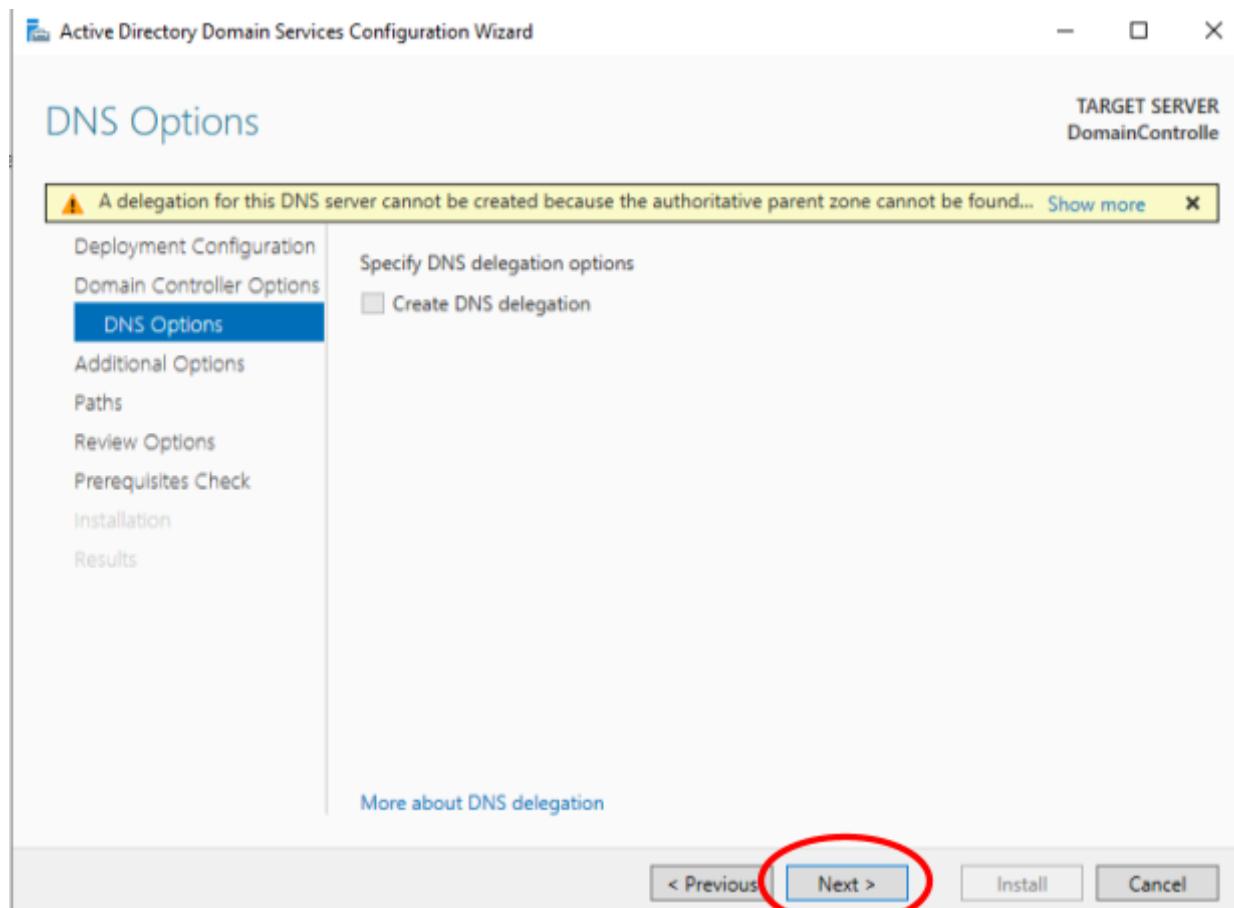
Click Next



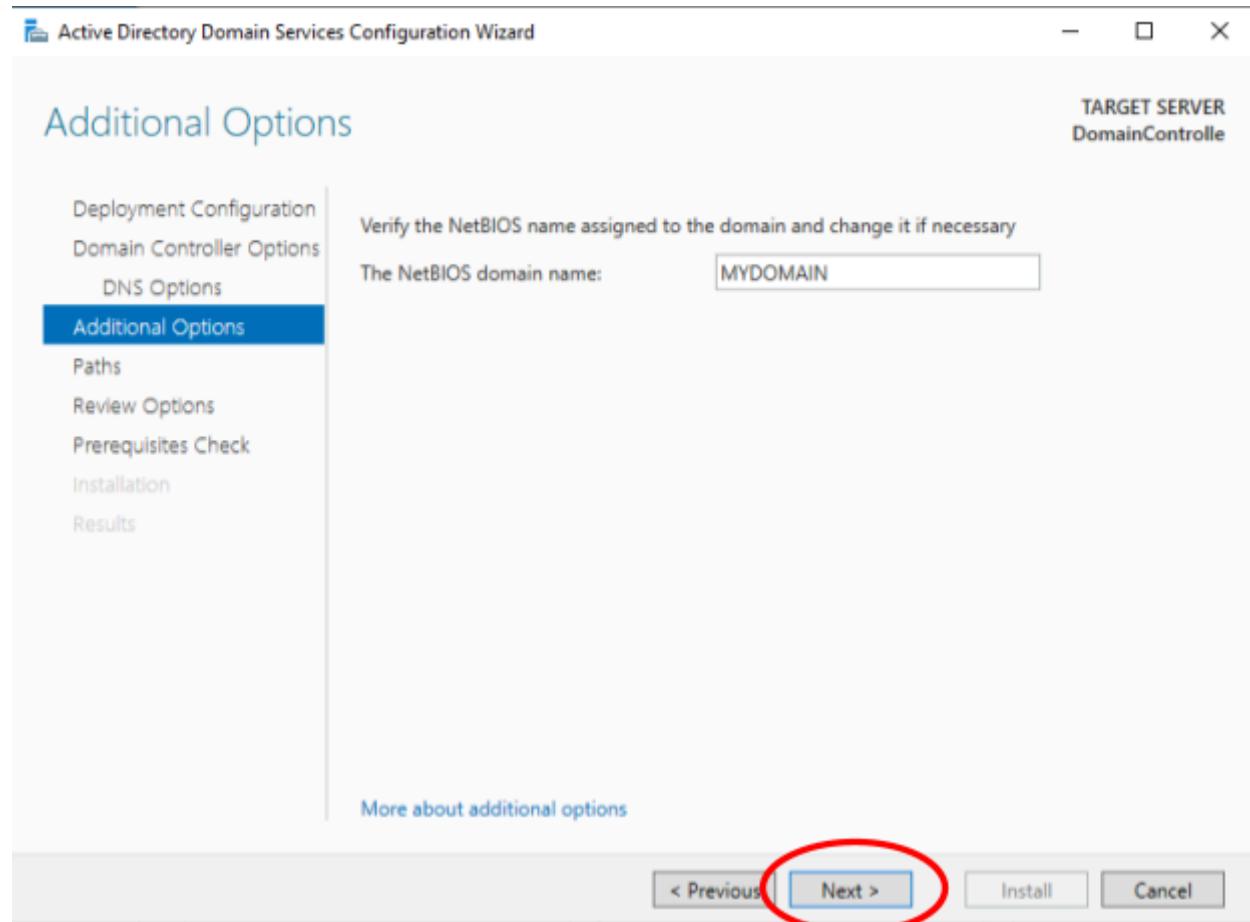
Add a Password and click Next



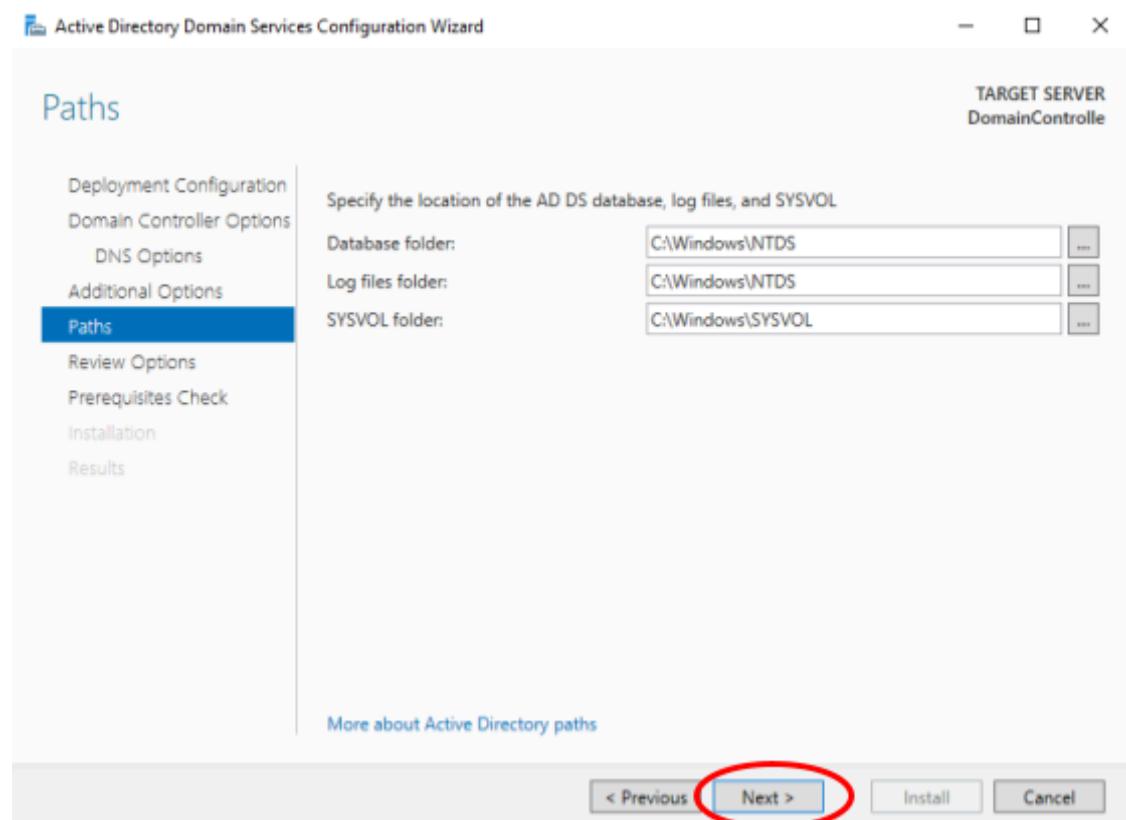
Click Next



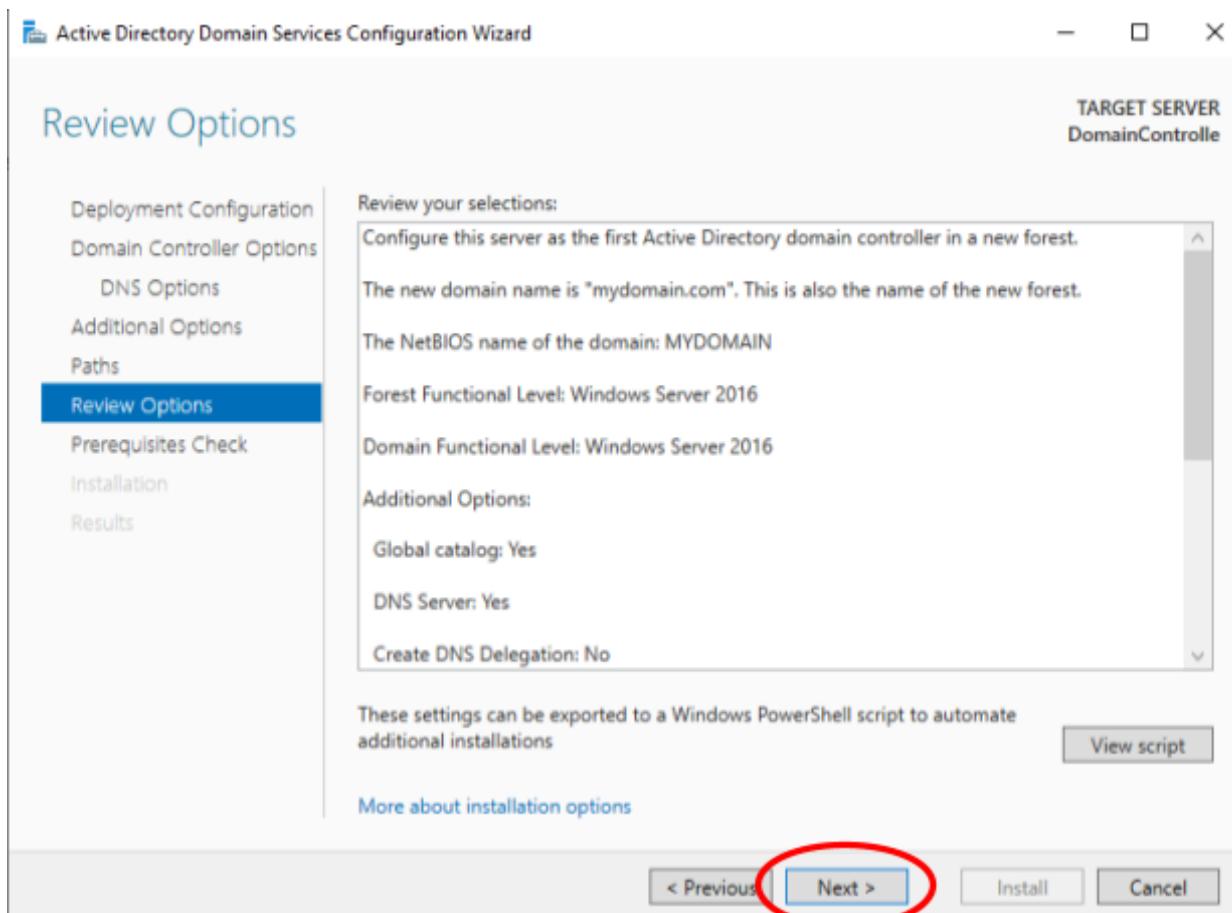
Click Next



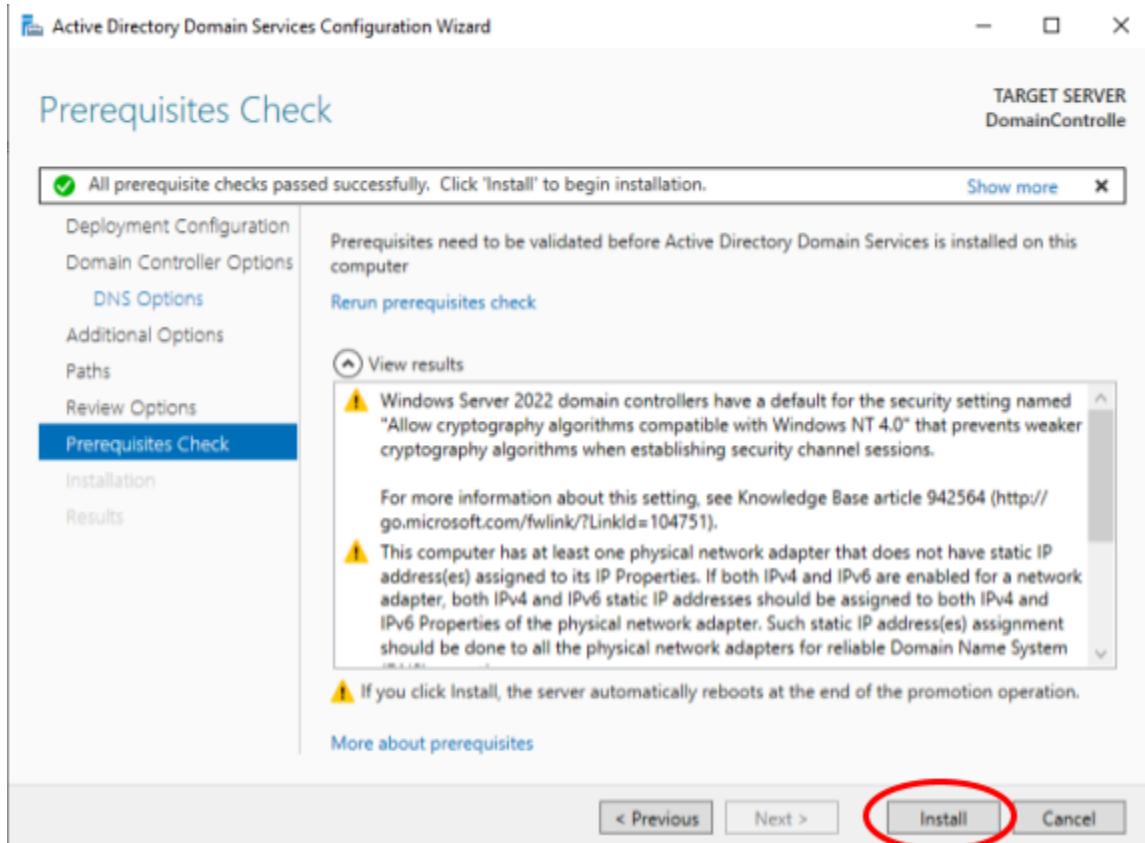
Click Next

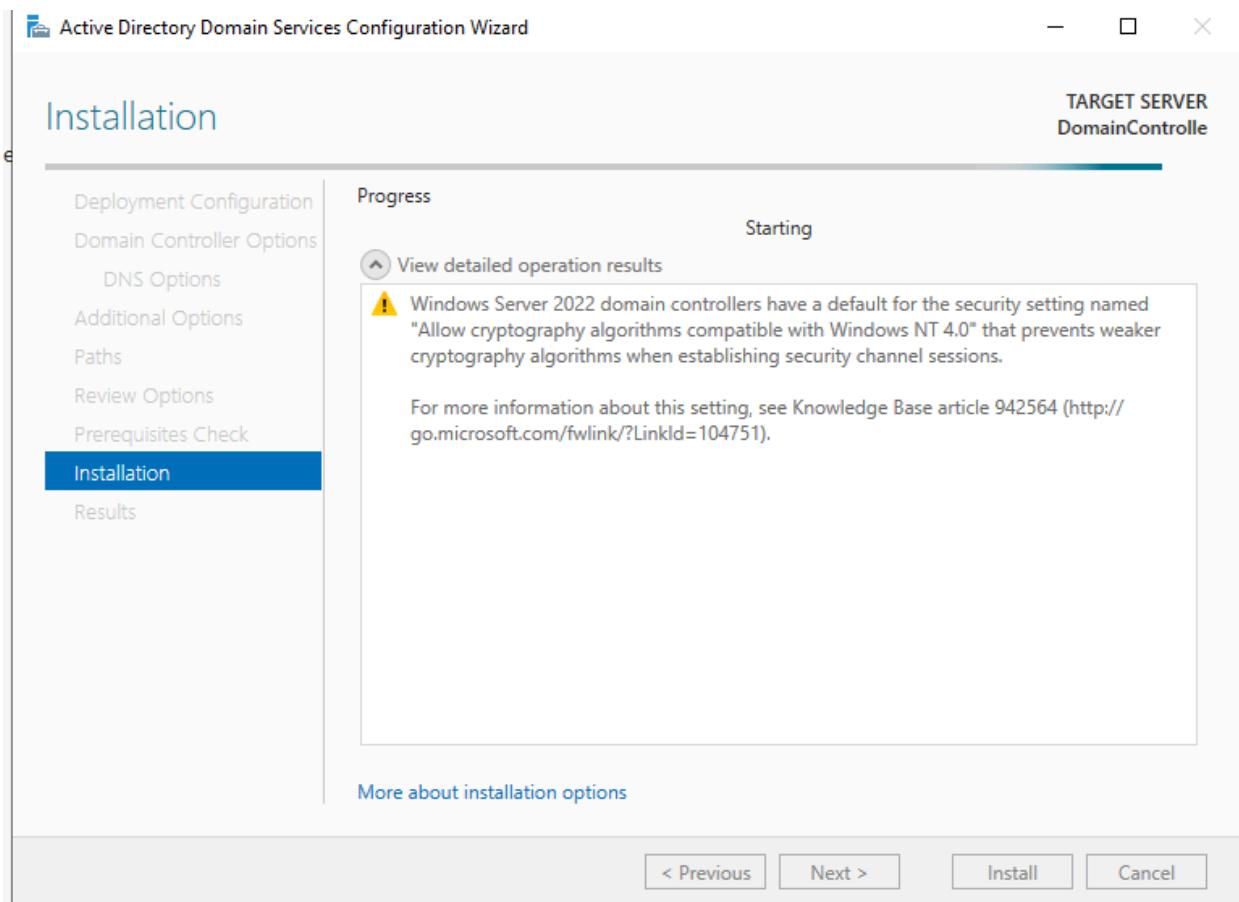


Click Next



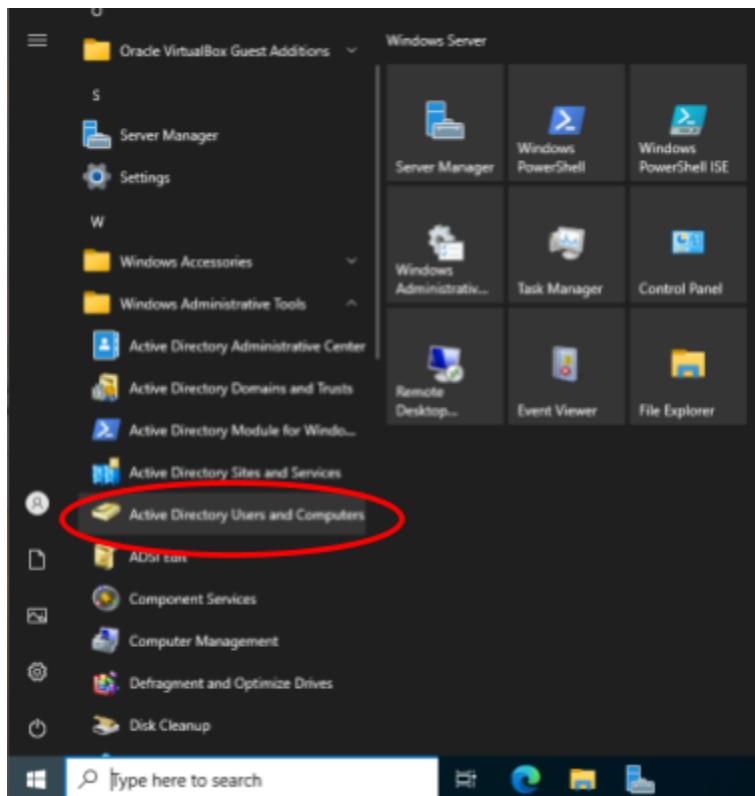
Click Install





Step 5: Create a Dedicated Admin Account

We will start by navigating to Active Directory Users and Computers in the Start menu



Select mydomain.com where we will see that the forest was created for our domain

Active Directory Users and Computers

File Action View Help

Active Directory Users and Com > Saved Queries > mydomain.com

Name	Type	Description
Saved Queries		Folder to store your favo...
mydomain.com	Domain	

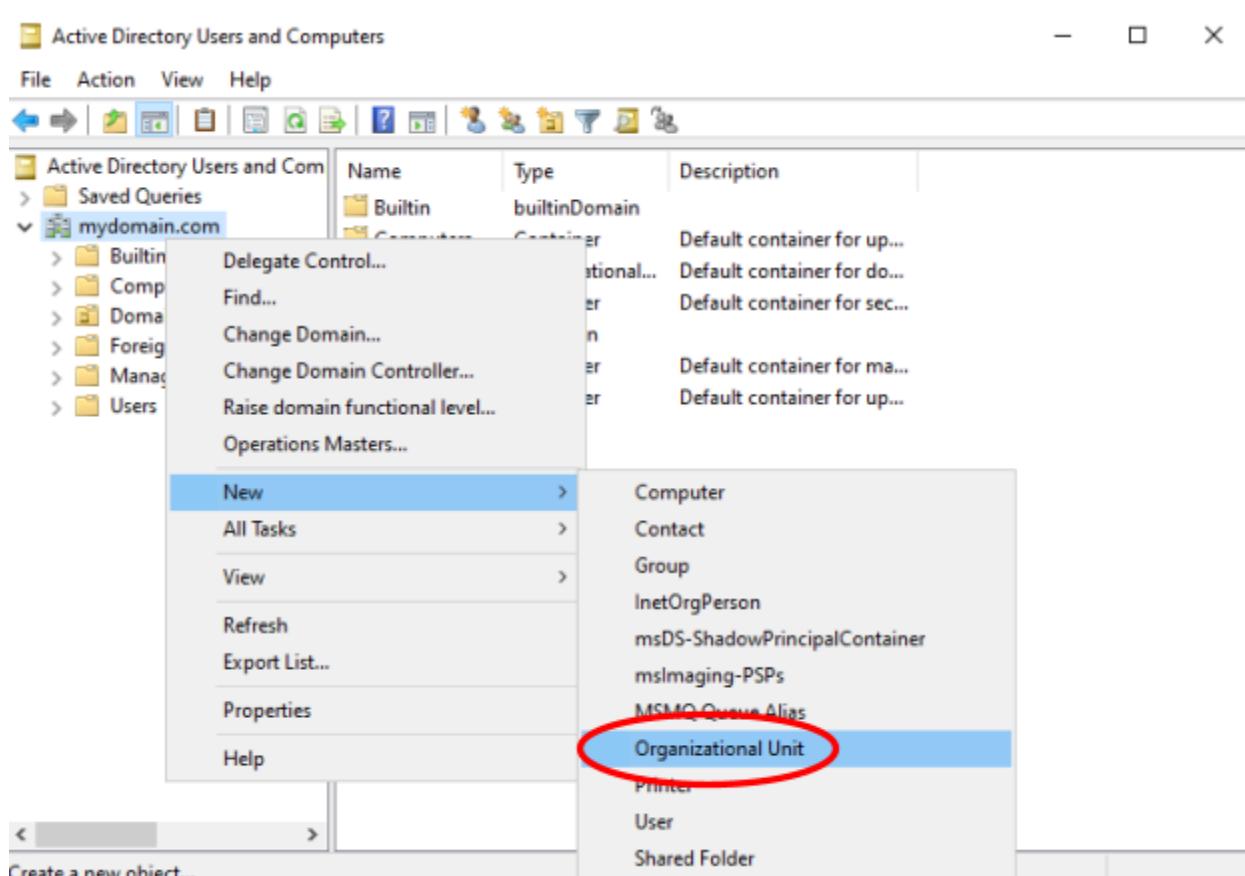
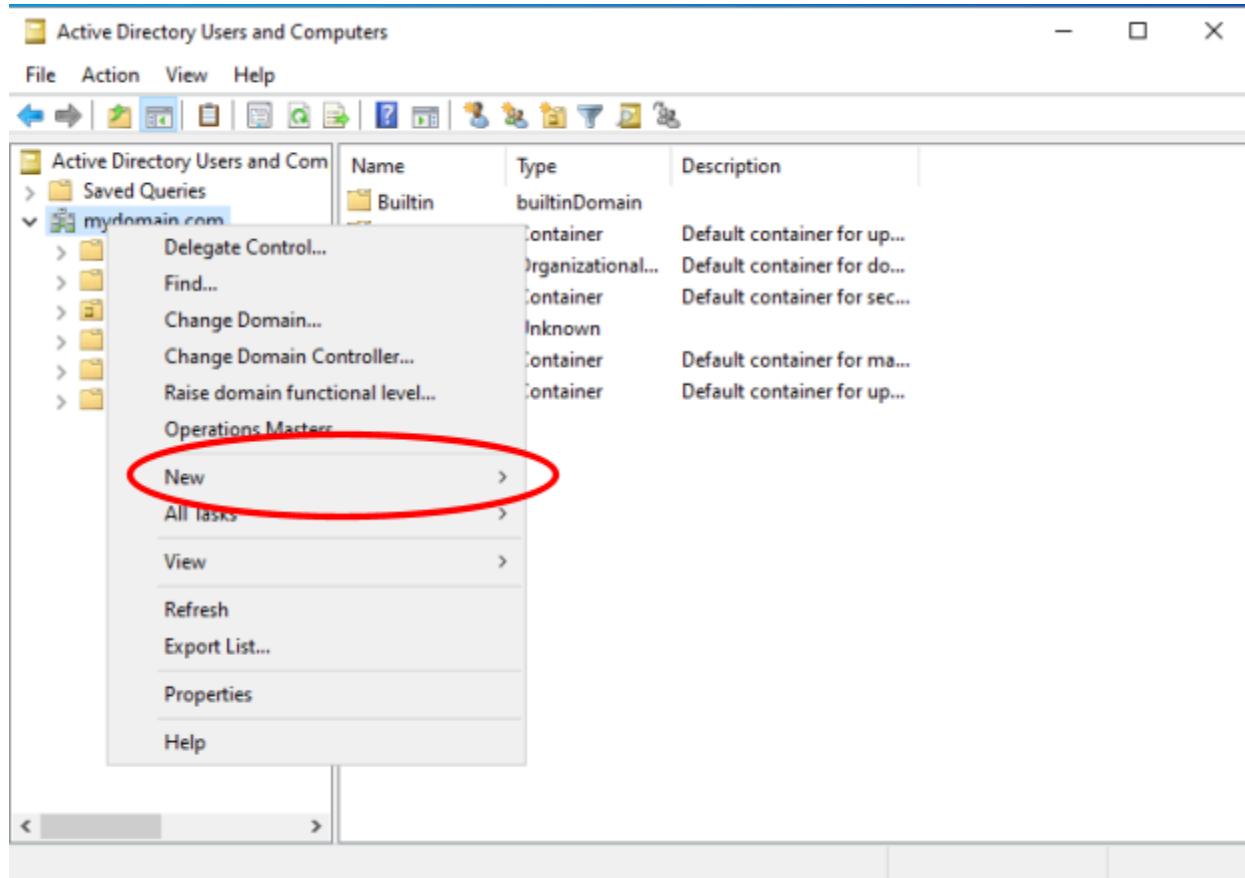
Active Directory Users and Computers

File Action View Help

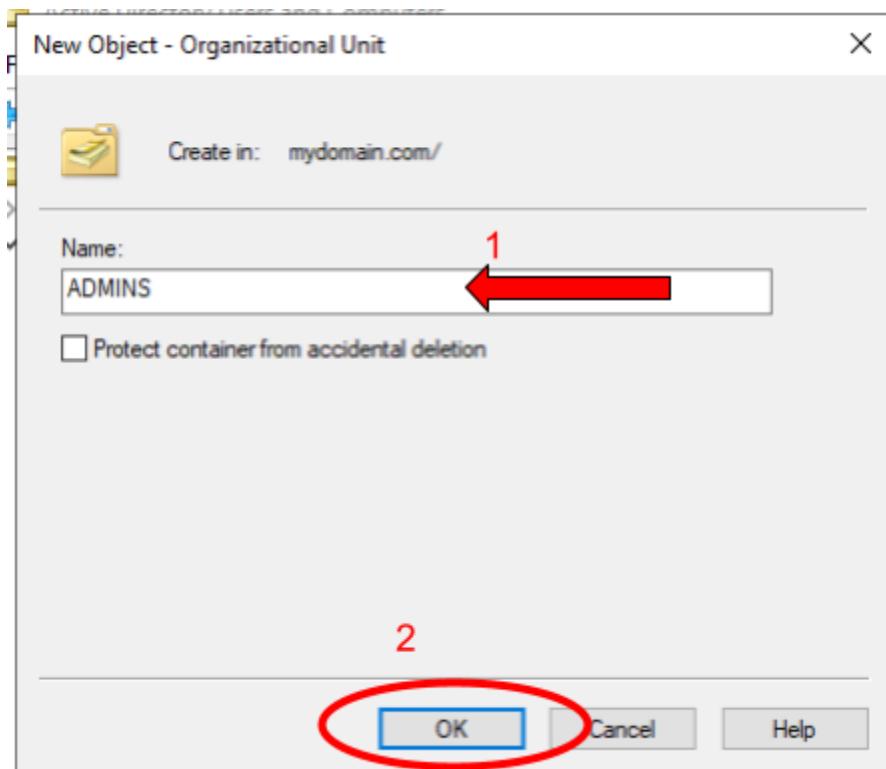
Active Directory Users and Com > mydomain.com

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Keys	Unknown	
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...

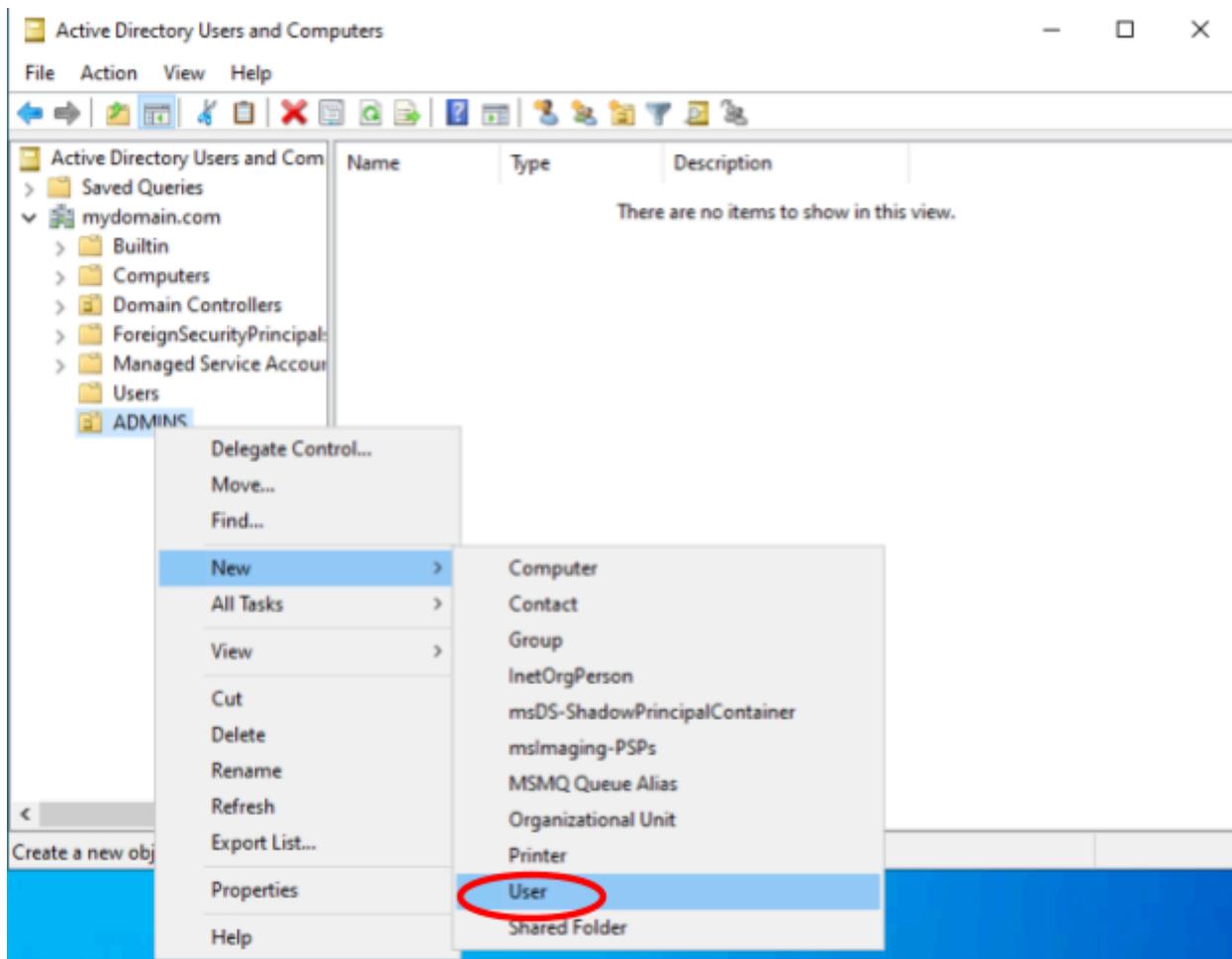
Right-Click on mydomain.com and select New → Organizational Unit



Name the new OU “ADMINS”



Then, we will create a new User as our Admin Account



Fill in the appropriate boxes

New Object - User

X



Create in: mydomain.com/ADMINS

First name: Angelito Initials:

Last name: Tuguinay

Full name: Angelito Tuguinay

User logon name:

a-atuguinay @mydomain.com

User logon name (pre-Windows 2000):

MYDOMAIN\ a-atuguinay

< Back

Next >

Cancel

New Object - User

X



Create in: mydomain.com/ADMINS

First name: Angelito Initials:

Last name: Tuguinay

Full name: Angelito Tuguinay

User logon name:

a-atuguinay @mydomain.com

User logon name (pre-Windows 2000):

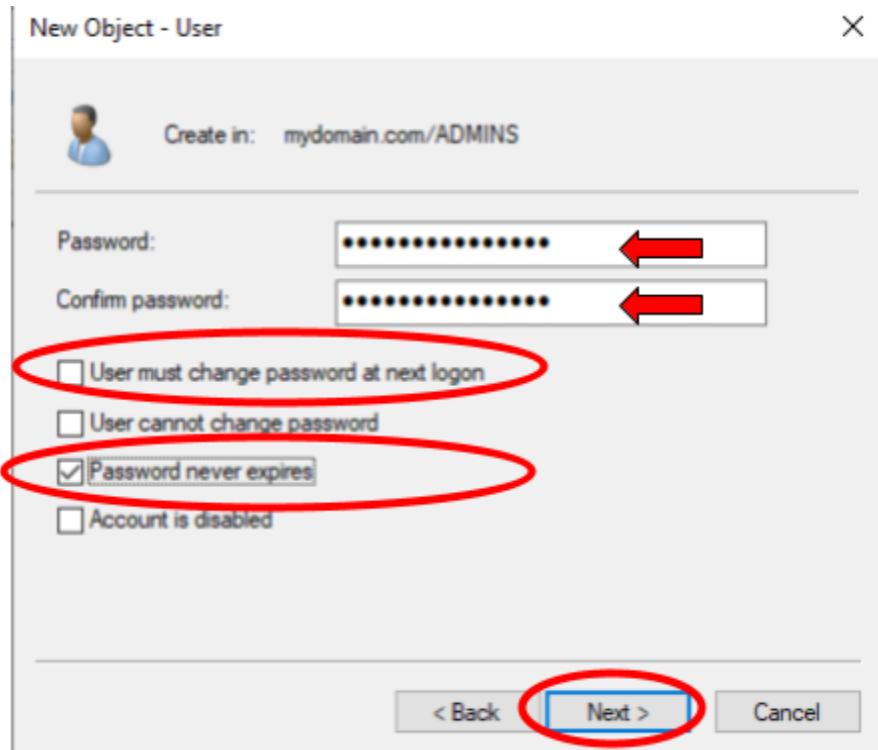
MYDOMAIN\ a-atuguinay

< Back

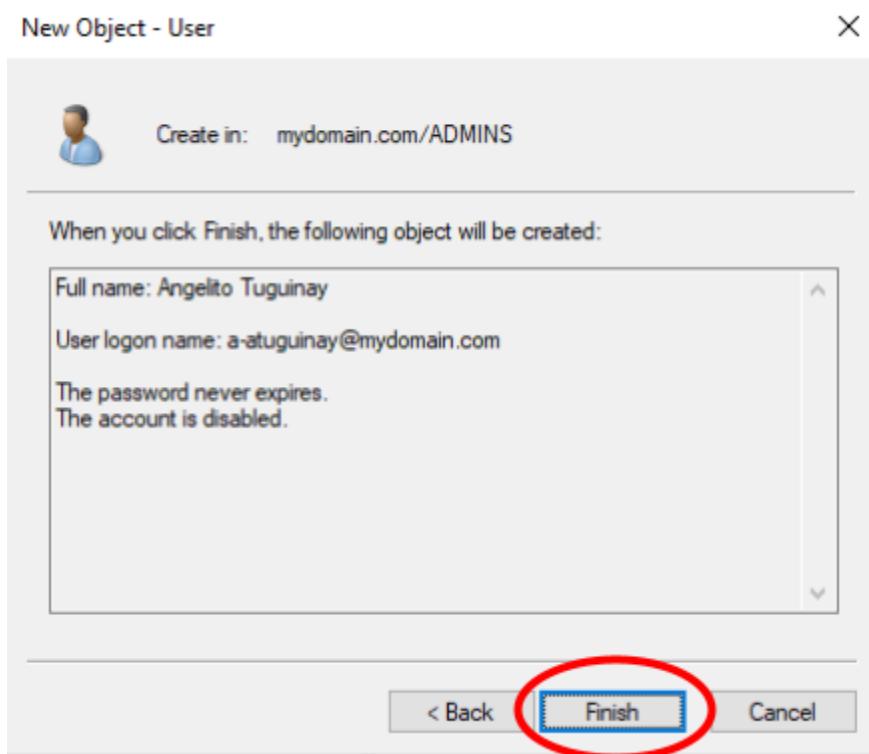
Next >

Cancel

Because this is a Lab Environment, we will uncheck the “User must change password at next logon” box and check the “Password never expires” box. In a production environment, these boxes will be checked to ensure the integrity of security.



Click Next and Finish



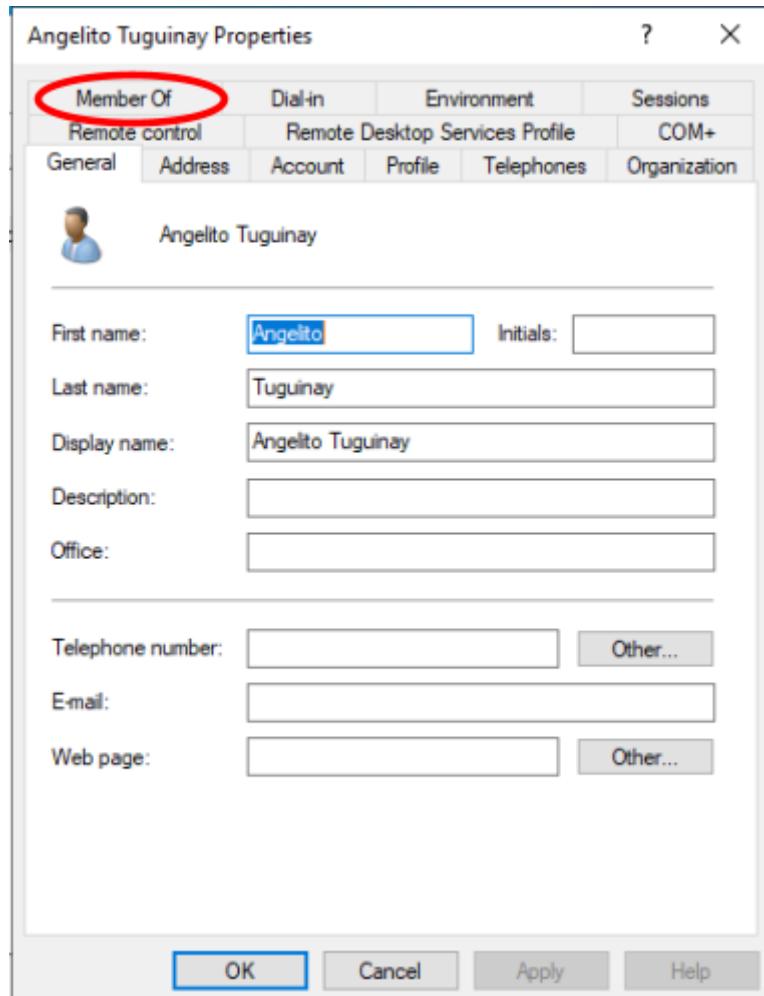
Back at the Active Directory Users and Computers, we should be able to see our created user under the ADMINS folder. We still need to add this account as a member of the domain Admin

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, the navigation pane displays the tree structure: Active Directory Users and Computers, Saved Queries, mydomain.com (with sub-nodes: Builtin, Computers, Domain Controllers, ForeignSecurityPrincipals, Managed Service Accounts, and Users), and ADMINS. The right pane lists users with columns: Name, Type, and Description. A single user, "Angelito Tuguinay", is listed under the "Type" column as "User". This row is highlighted with a red oval. Below the table, there are navigation arrows and a status bar message: "Opens the properties dialog box for the current selection."

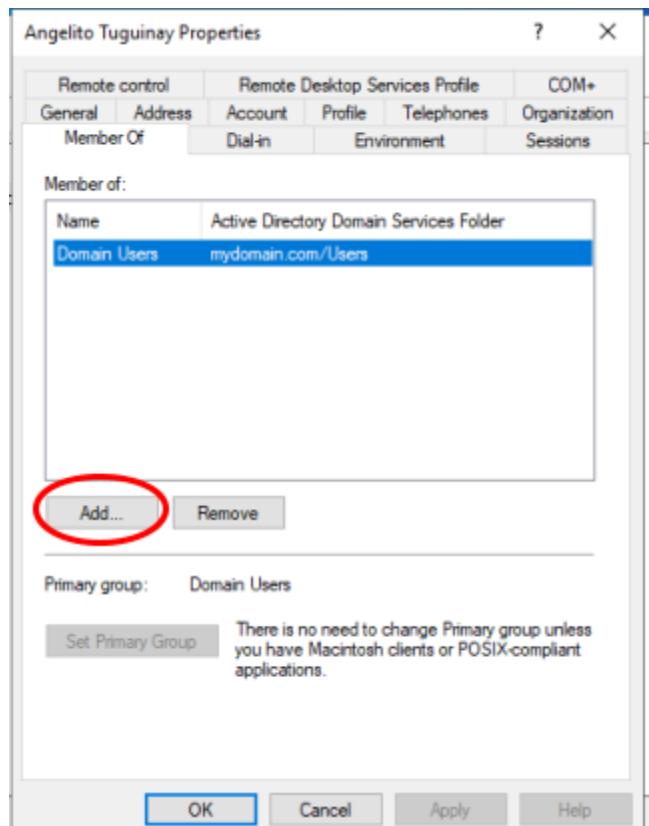
Next, we will add this user as a member of the domain Admin
Right-click on the user and select Properties

The screenshot shows the same Active Directory Users and Computers interface. The user "Angelito Tuguinay" is selected in the list, and a context menu is open. The menu items include: Copy..., Add to a group..., Enable Account, Reset Password..., Move..., Open Home Page, Send Mail, All Tasks (with a submenu), Cut, Delete, Rename, and Properties. The "Properties" option is highlighted with a blue oval. The status bar at the bottom of the window also indicates: "Opens the properties dialog box for the current selection."

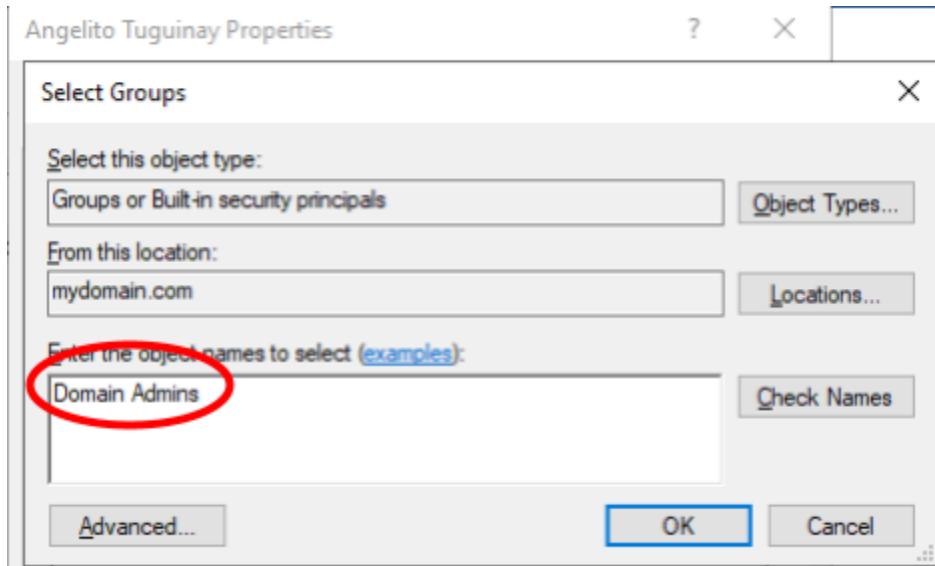
Click on the Member Of tab



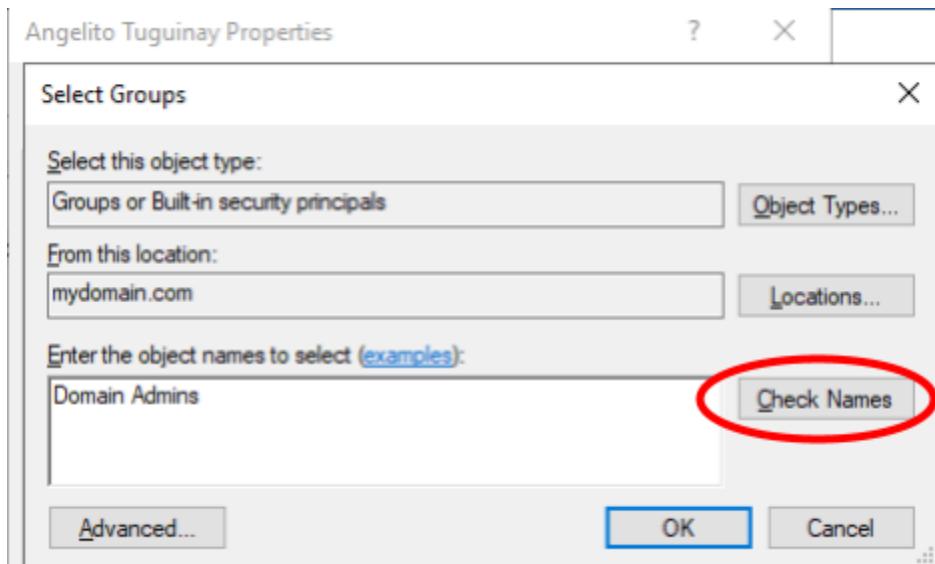
Click Add



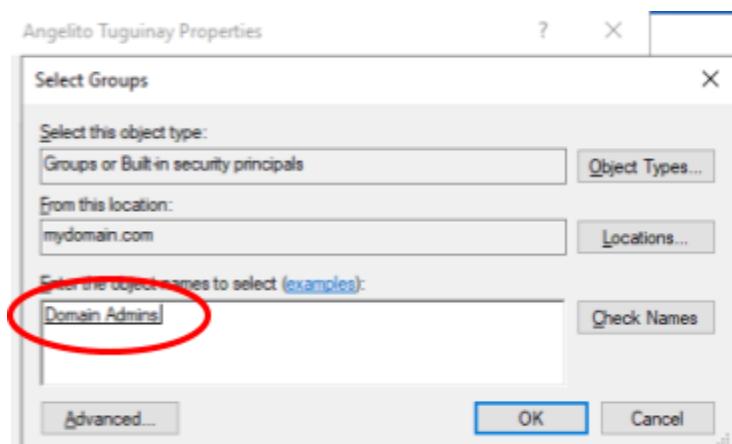
On the “Enter the object names to select (examples):”, type Domain Admins



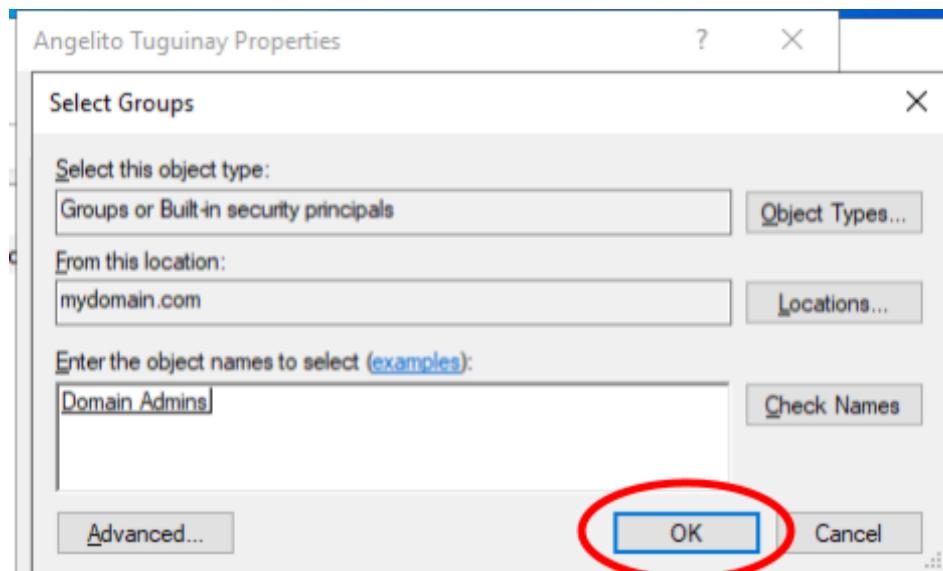
Click on Check Names



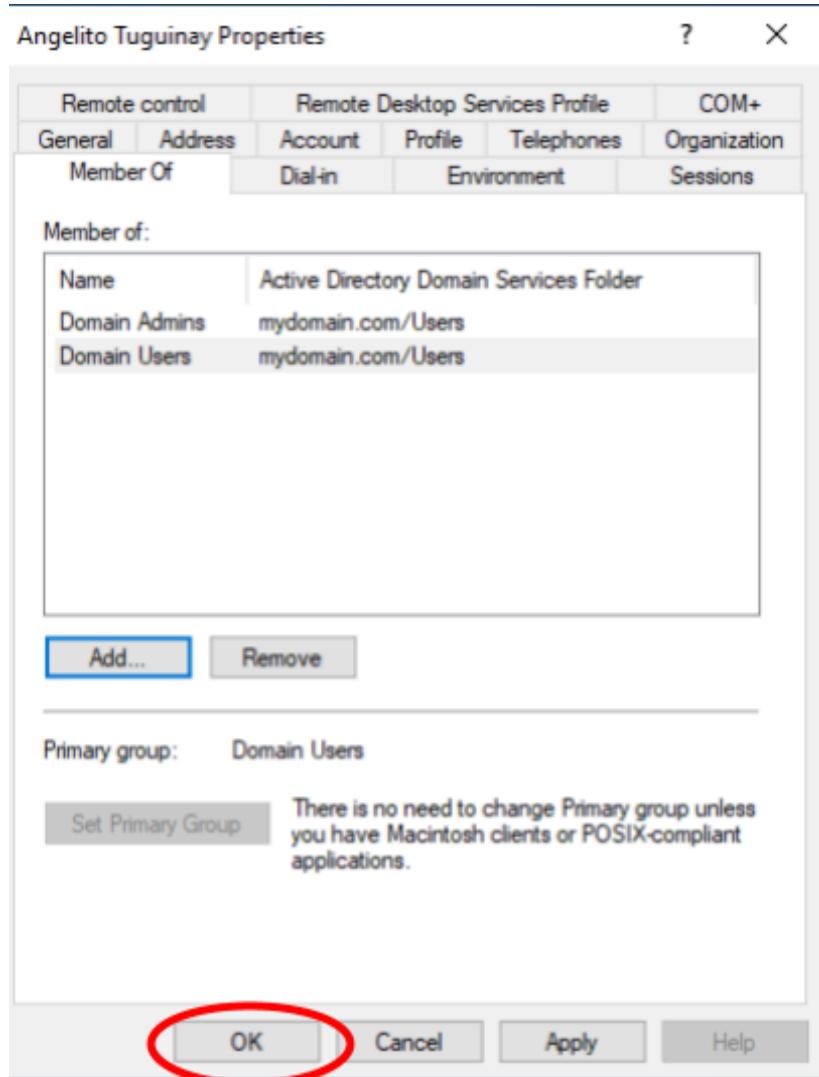
The Domain Admins should be underlined to signify that the Domain Admins group is selected



Click OK



Click OK again

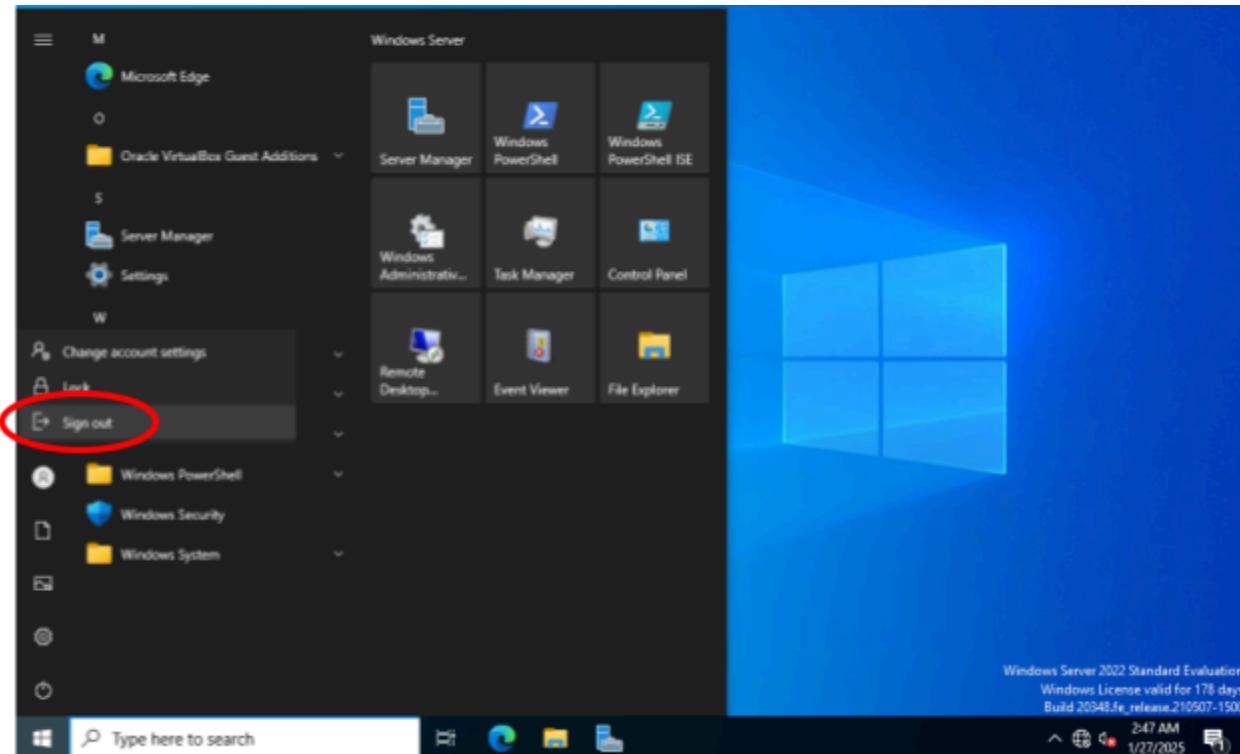


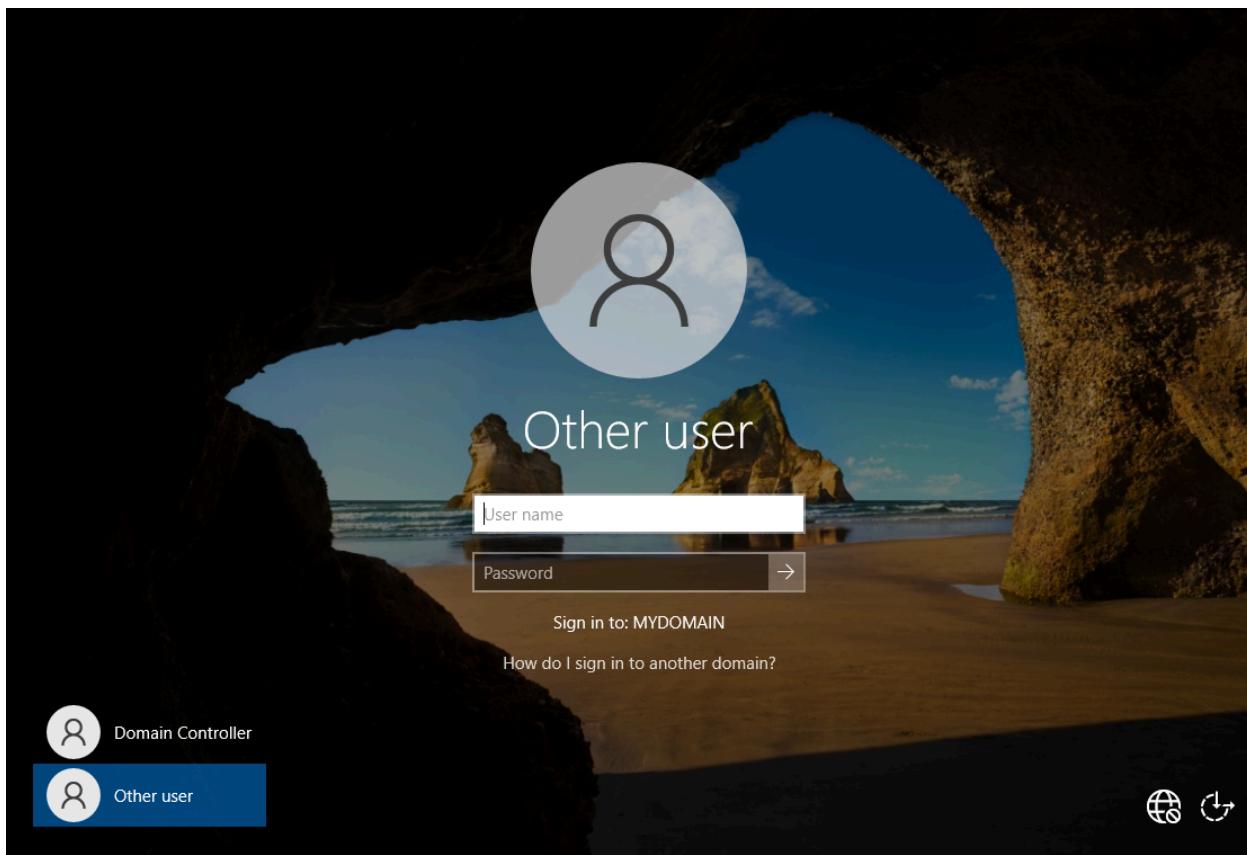
The screenshot shows the Windows Server interface for managing Active Directory. On the left, the navigation pane includes 'Active Directory Users and Computers', 'File', 'Action', 'View', and 'Help'. The main pane displays the 'Active Directory Users and Computers [DomainController.mydomain.com]' view. A tree view on the left lists 'Saved Queries', 'mydomain.com' (which is expanded to show 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipal', 'Managed Service Account', 'Users', and 'ADMINS'), and 'Description'. A table on the right shows one entry: 'Angelito Tuguinay' under the 'User' category. The status bar at the bottom indicates the window title and the path 'Active Directory Users and Computers [DomainController.mydomain.com]'. Navigation arrows are visible at the bottom left.

Now, we have successfully created and added an Admin User

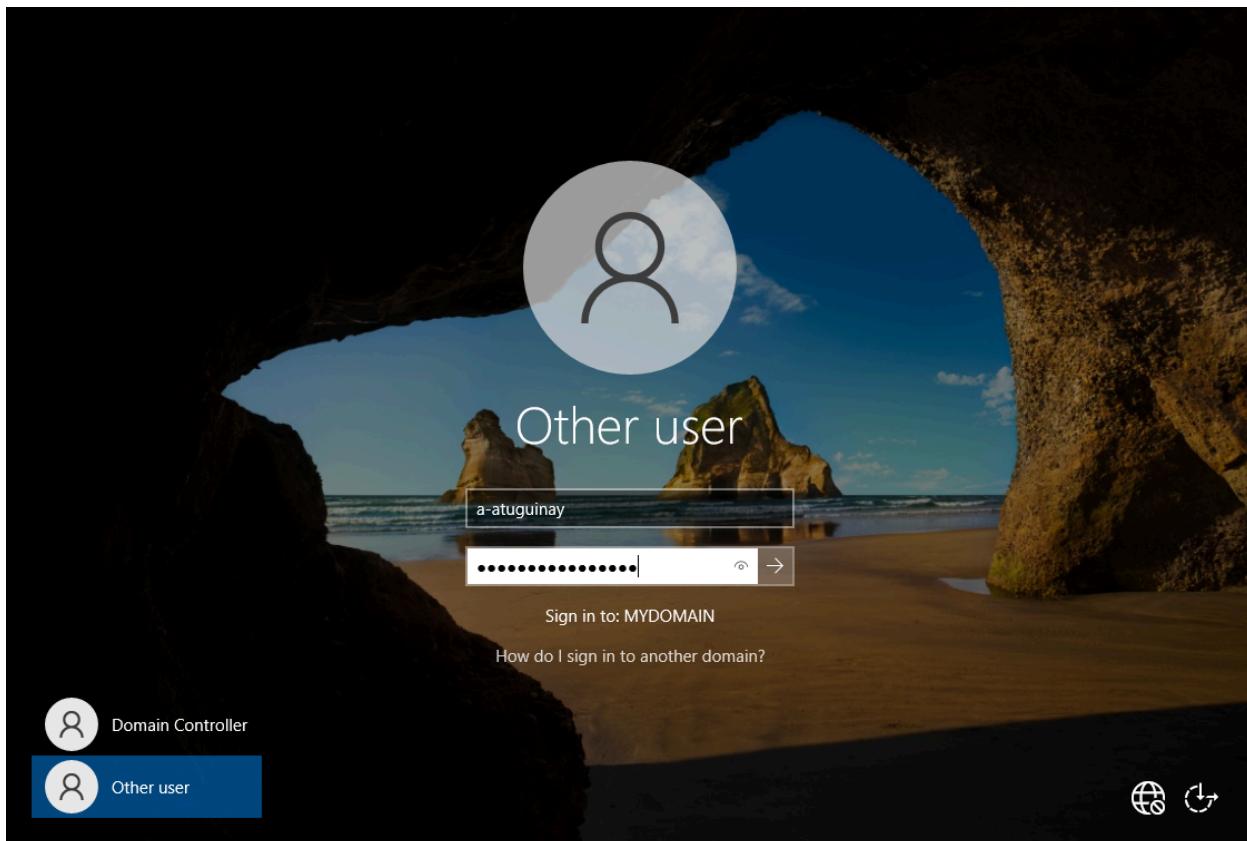
Step 6: Log in as the Admin User we just created

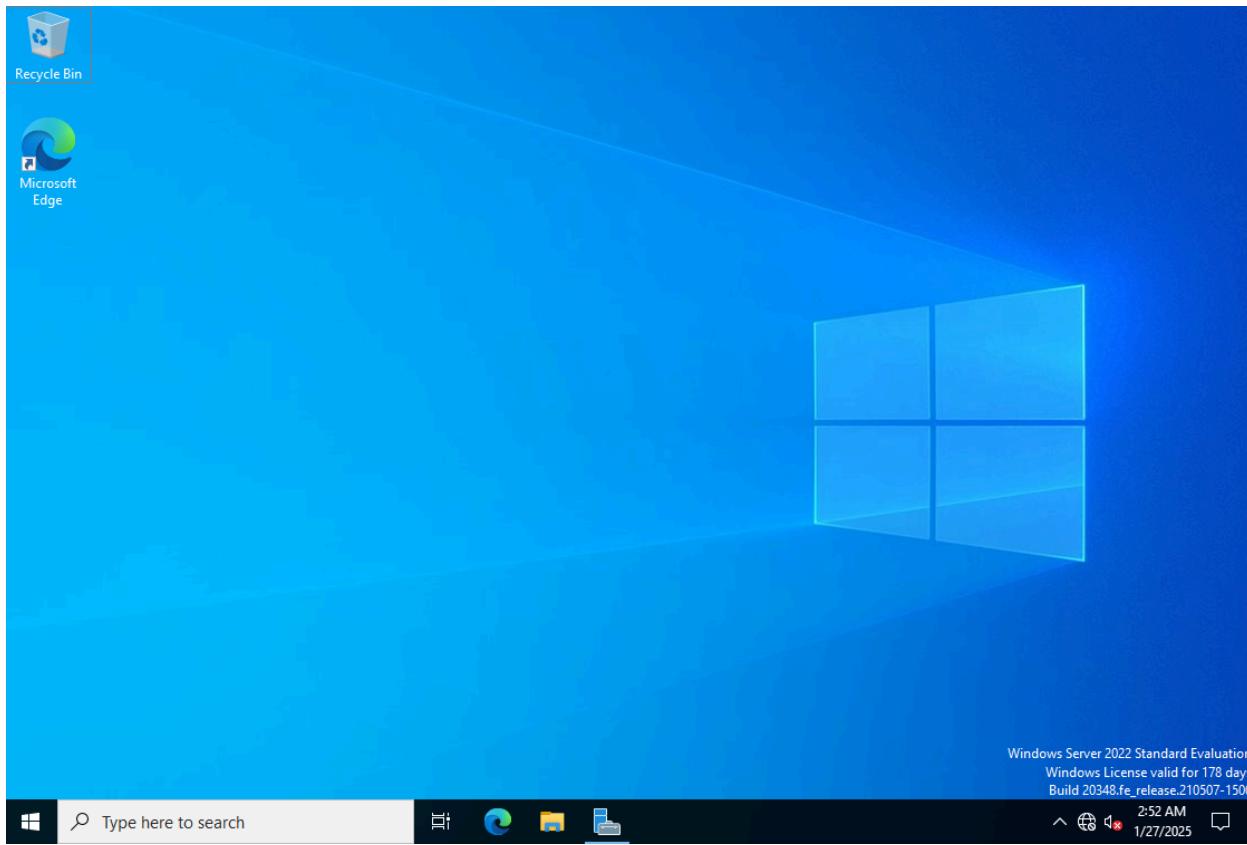
We will begin by signing out





Select Other User and input the credentials we created earlier





Wonderful. Next, we will install RAS/NAT on our Domain Controller so that we can use our Domain Controller as the Default Gateway for the Computers that are connected to it.

Step 7: Install RAS/NAT (Remote Access Server/Network Address Translation)

We will begin by opening up Server Manager Dashboard and Selecting Add roles and features

A screenshot of the Server Manager Dashboard. The dashboard has a dark header with the title 'Server Manager • Dashboard' and navigation links for 'Manage', 'Tools', 'View', and 'Help'. On the left, there's a sidebar with 'Dashboard' selected, followed by 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and Storage Services'. The main area is titled 'WELCOME TO SERVER MANAGER' and contains a 'QUICK START' section with five numbered steps: 1. Configure this local server, 2. Add roles and features (which is circled in red), 3. Add other servers to manage, 4. Create a server group, and 5. Connect this server to cloud services. Below this is a 'ROLES AND SERVER GROUPS' section showing three items: 'AD DS' (1 item), 'DNS' (1 item), and 'File and Storage Services' (1 item). Each item has a green status indicator and a list of sub-components: AD DS includes Manageability, Events, Services, Performance, and BPA results; DNS includes Manageability, Events, Services, Performance, and BPA results; and File and Storage Services includes Manageability, Events, Services, Performance, and BPA results.

Before you begin

DESTINATION SERVER
DomainController.mydomain.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
[Start the Remove Roles and Features Wizard](#)

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

Skip this page by default

< Previous

Next >

Install

Cancel

Click Next until we can select Remote access

Select installation type

DESTINATION SERVER
DomainController.mydomain.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

Role-based or feature-based installation

Configure a single server by adding roles, role services, and features.

Remote Desktop Services installation

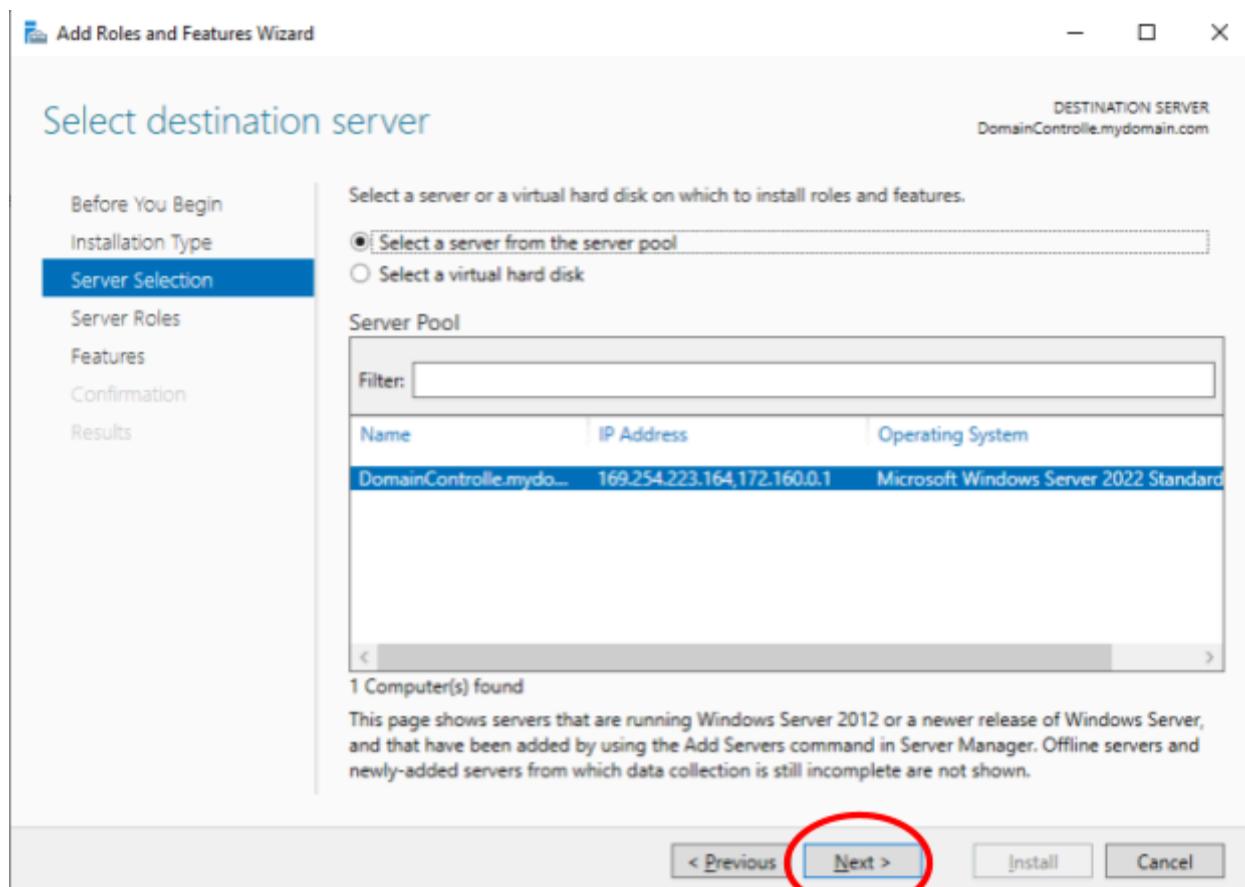
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous

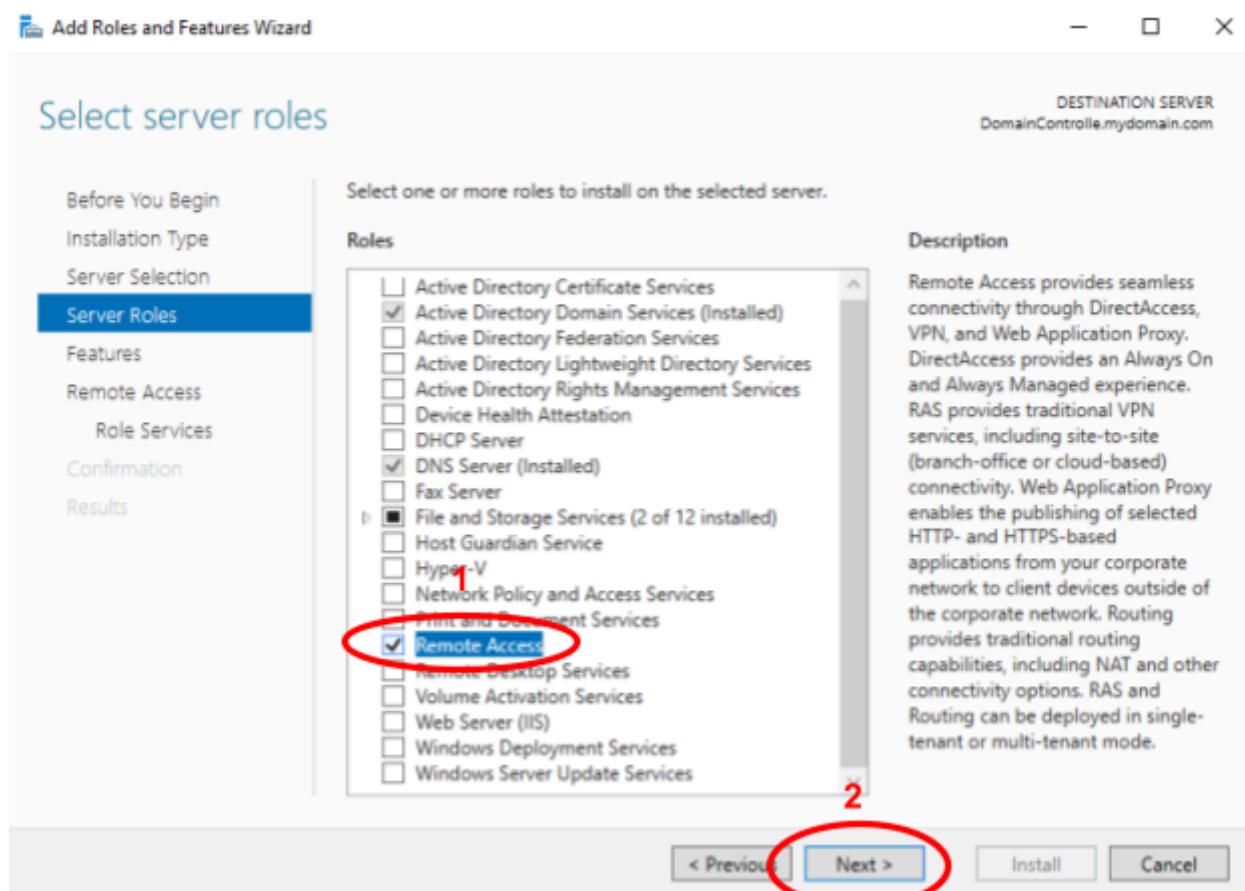
Next >

Install

Cancel



Select Remote Access and click Next



Click Next

Add Roles and Features Wizard

Select features

DESTINATION SERVER
DomainController.mydomain.com

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Confirmation
Results

Select one or more features to install on the selected server.

Features

	Description
<input type="checkbox"/> .NET Framework 3.5 Features	.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
<input checked="" type="checkbox"/> .NET Framework 4.8 Features (2 of 7 installed)	
<input type="checkbox"/> Background Intelligent Transfer Service (BITS)	
<input type="checkbox"/> BitLocker Drive Encryption	
<input type="checkbox"/> BitLocker Network Unlock	
<input type="checkbox"/> BranchCache	
<input type="checkbox"/> Client for NFS	
<input type="checkbox"/> Containers	
<input type="checkbox"/> Data Center Bridging	
<input type="checkbox"/> Direct Play	
<input type="checkbox"/> Enhanced Storage	
<input type="checkbox"/> Failover Clustering	
<input checked="" type="checkbox"/> Group Policy Management (Installed)	
<input type="checkbox"/> Host Guardian Hyper-V Support	
<input type="checkbox"/> I/O Quality of Service	
<input type="checkbox"/> IIS Hostable Web Core	
<input type="checkbox"/> Internet Printing Client	
<input type="checkbox"/> IP Address Management (IPAM) Server	
<input type="checkbox"/> LPR Port Monitor	

< Previous **Next >** Install Cancel

Click Next

Add Roles and Features Wizard

Remote Access

DESTINATION SERVER
DomainController.mydomain.com

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Confirmation
Results

Remote Access integrates DirectAccess, VPN, and Web Application Proxy in a single management console.

Deploy DirectAccess to allow managed domain-joined computers to connect to the internal corporate network as DirectAccess clients. Connectivity is seamless and transparent, and is available any time client computers are located on the Internet. DirectAccess administrators can remotely manage clients, ensuring that mobile computers are kept up-to-date with security updates and corporate compliance requirements.

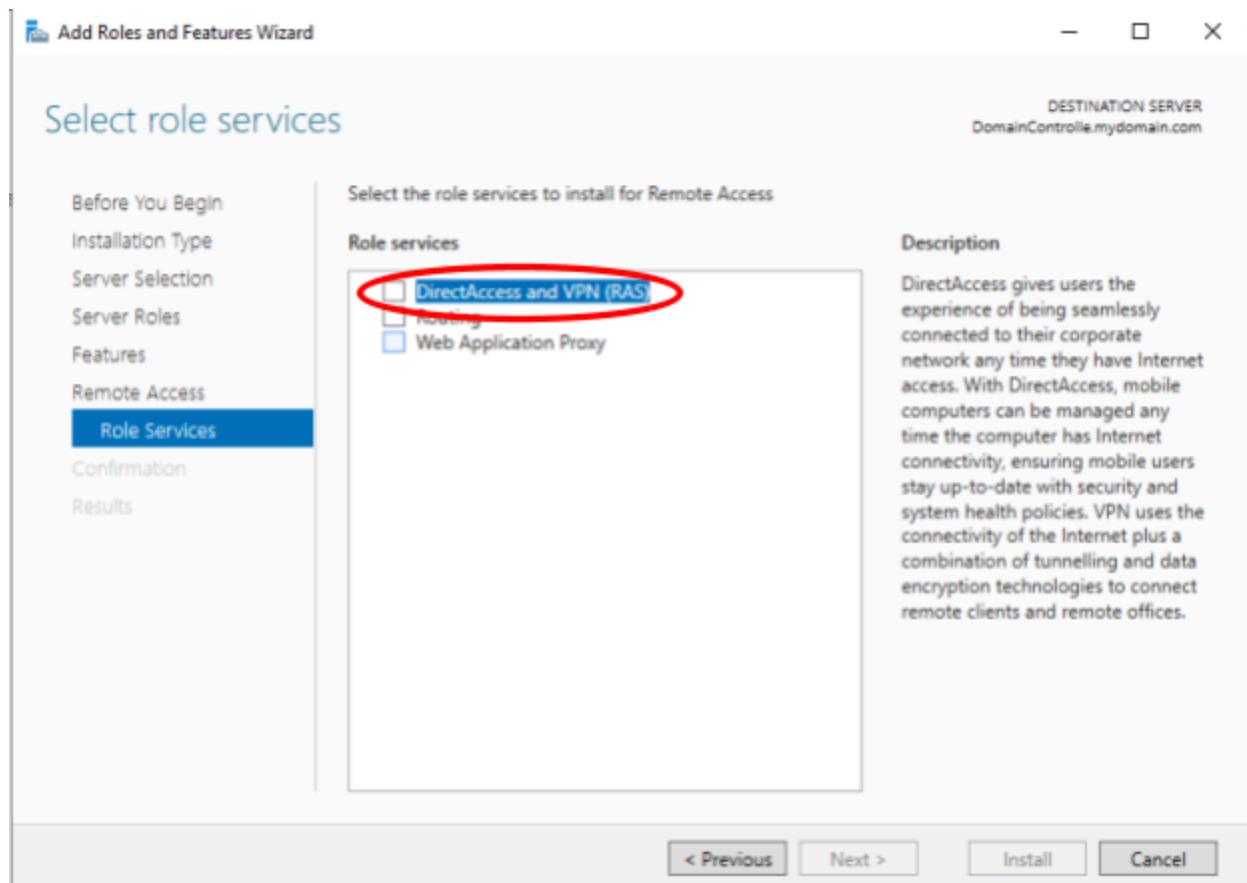
Deploy VPN to allow client computers running operating systems not supported by DirectAccess, or configured in a workgroup, to remotely access corporate networks over a VPN connection.

Deploy Web Application Proxy to publish selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. It can use AD FS to ensure that users are authenticated before they gain access to published applications. Web Application Proxy also provides proxy functionality for your AD FS servers.

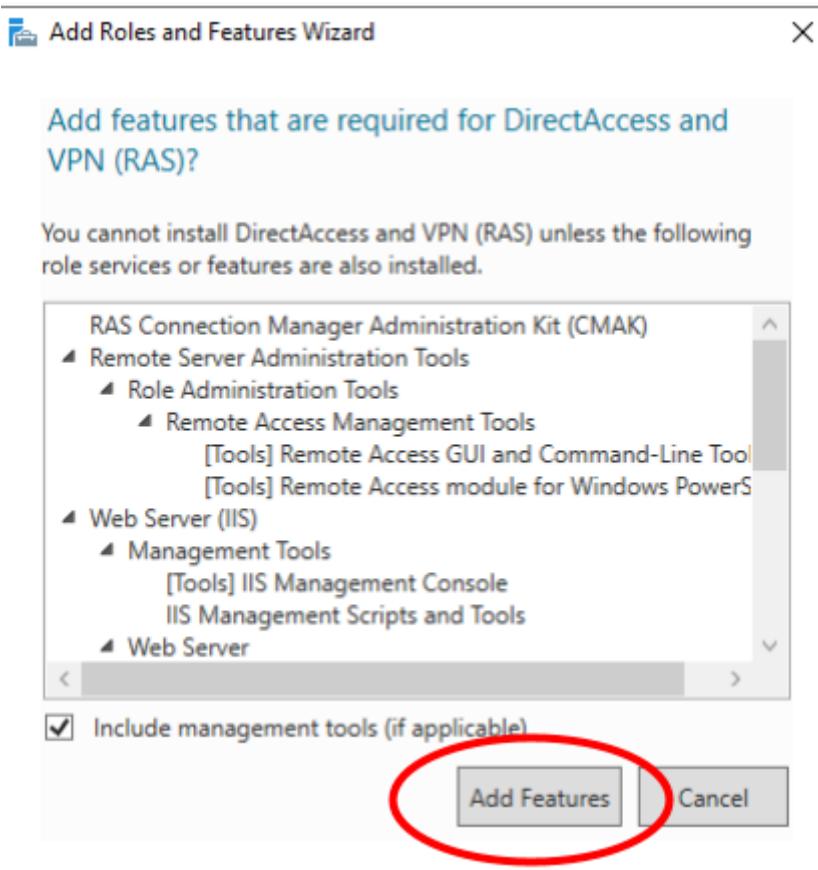
Configure RRAS routing features using the Routing and Remote Access console.

< Previous **Next >** Install Cancel

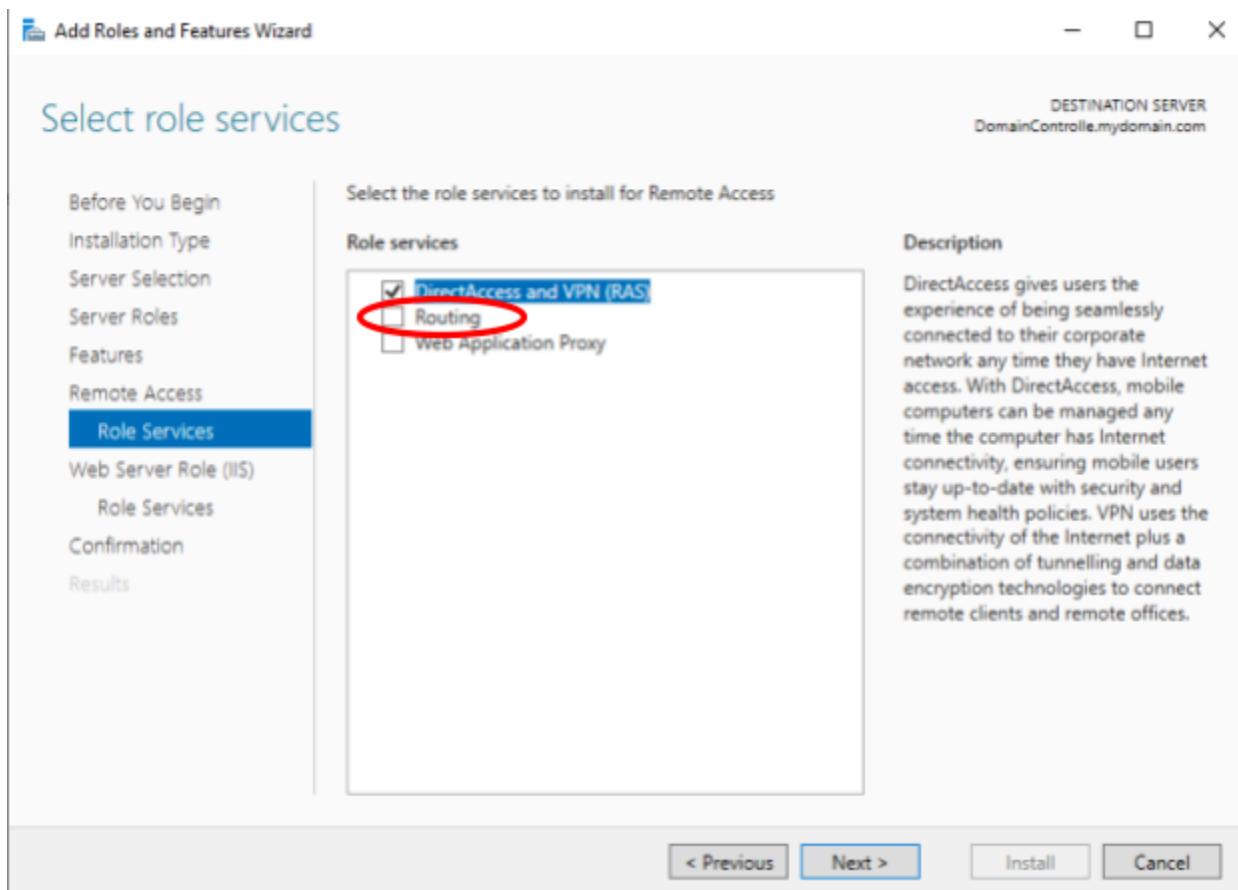
Select DirectAccess and VPN (RAS)



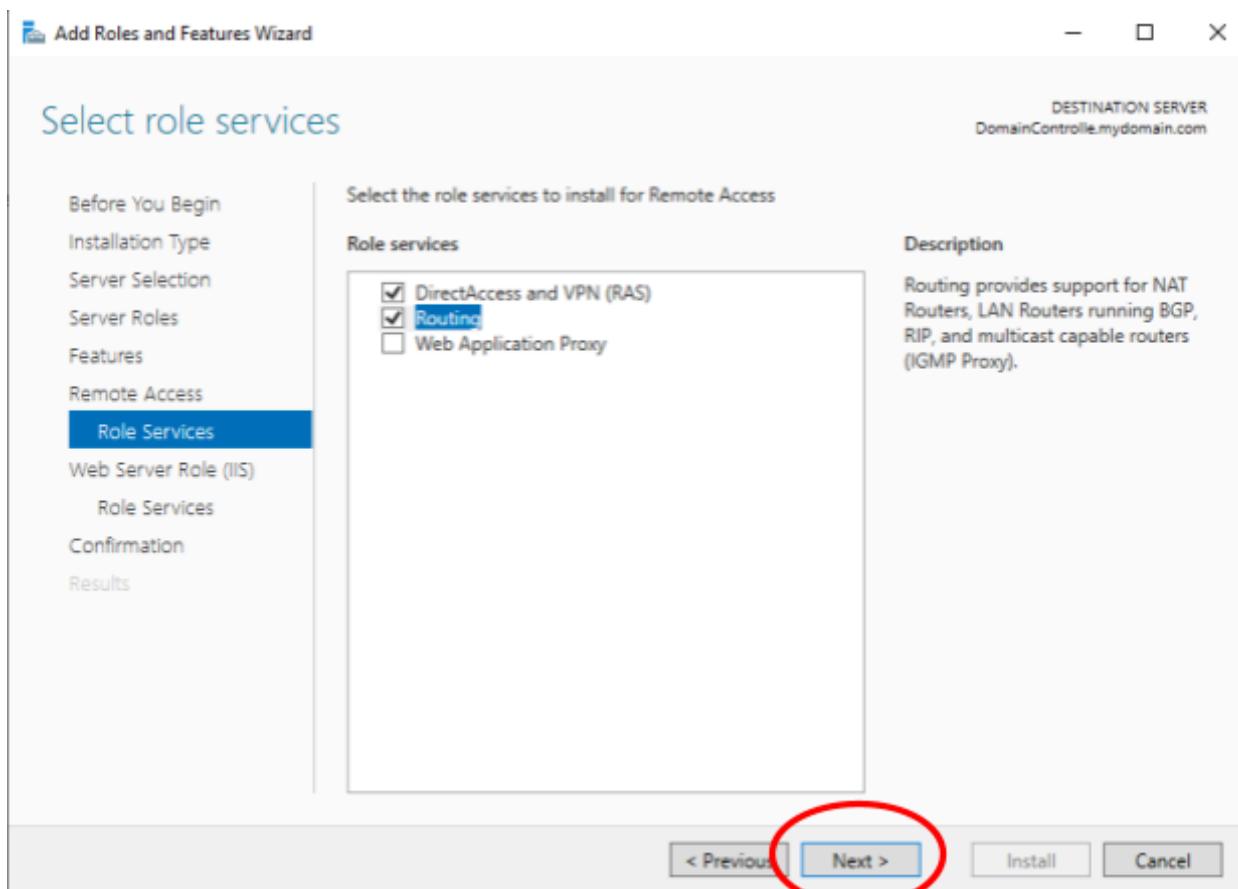
Click Add Features



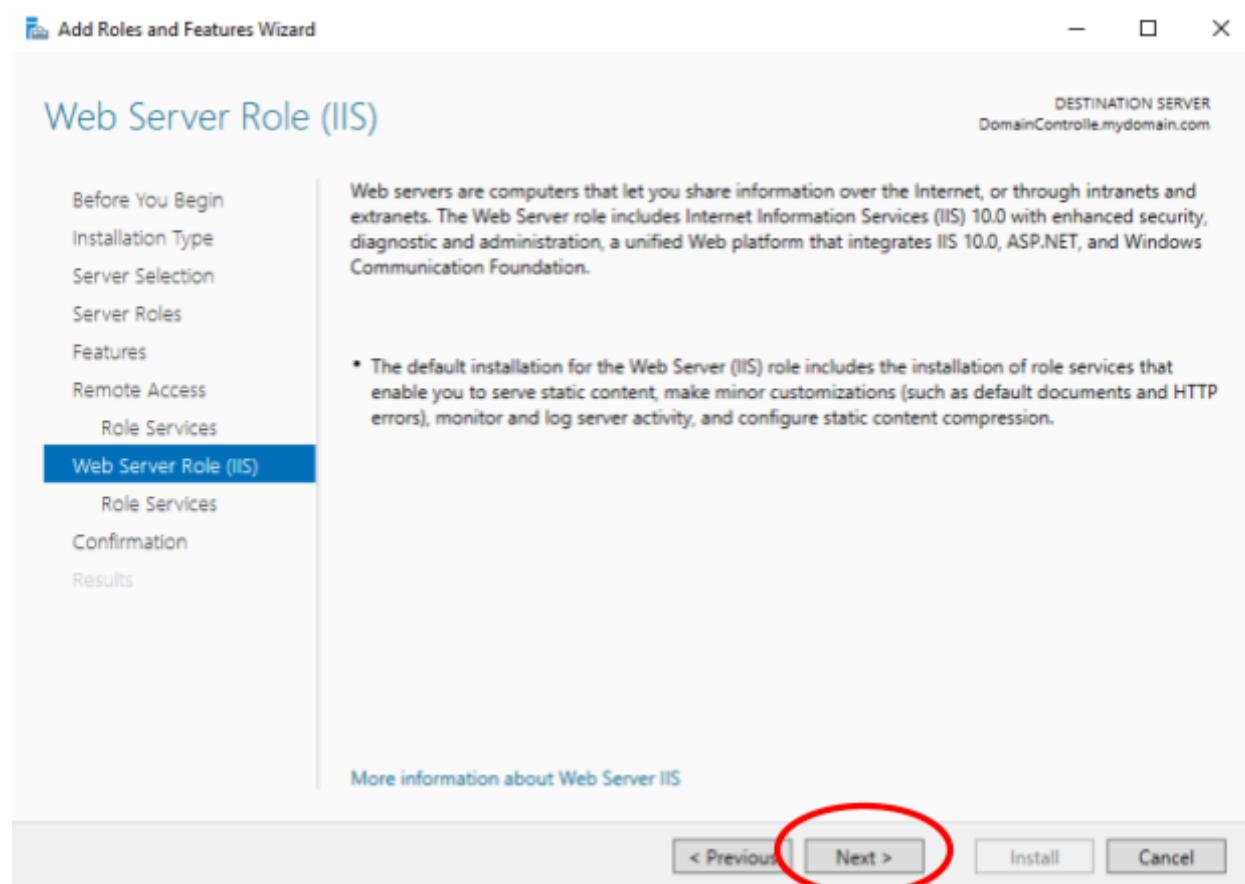
Then, select Routing and click Next



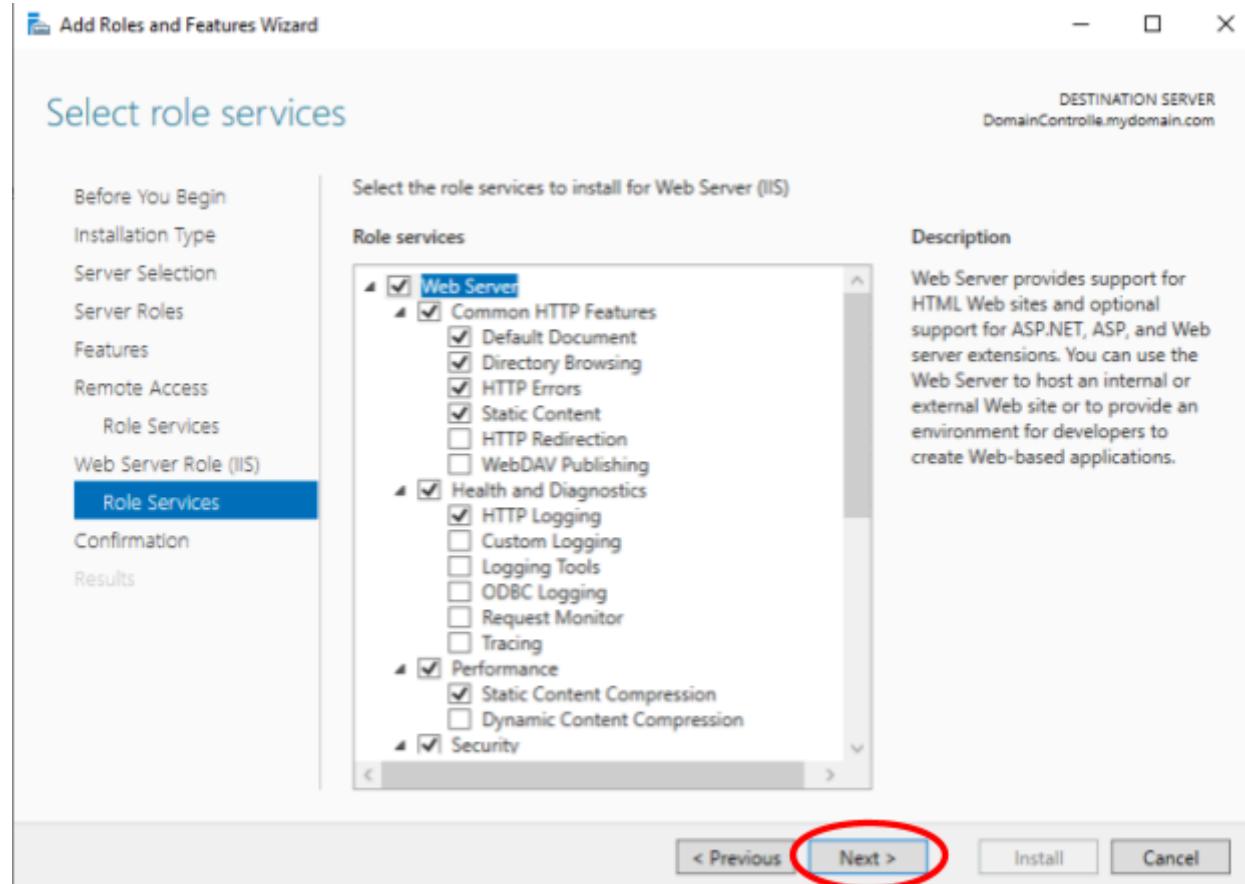
Click Next



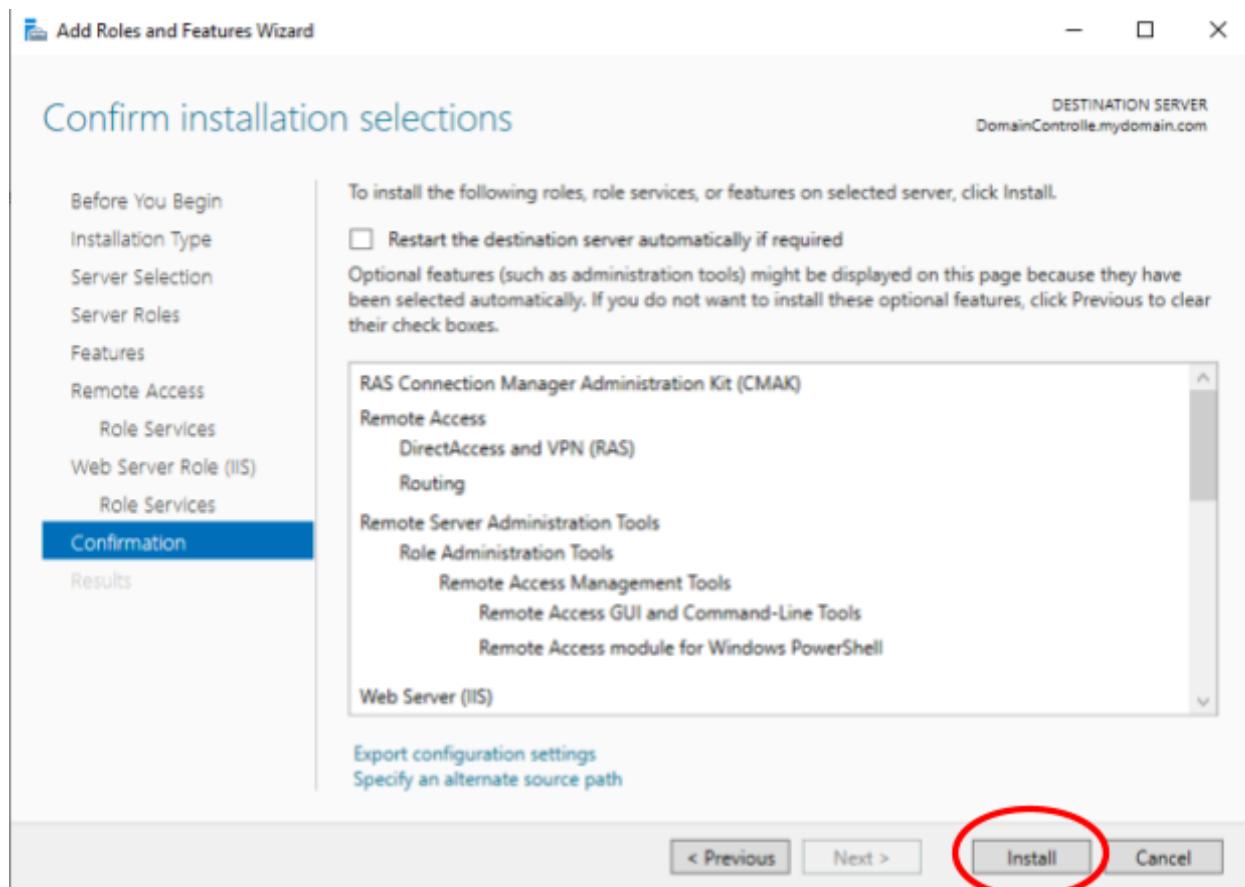
Click Next



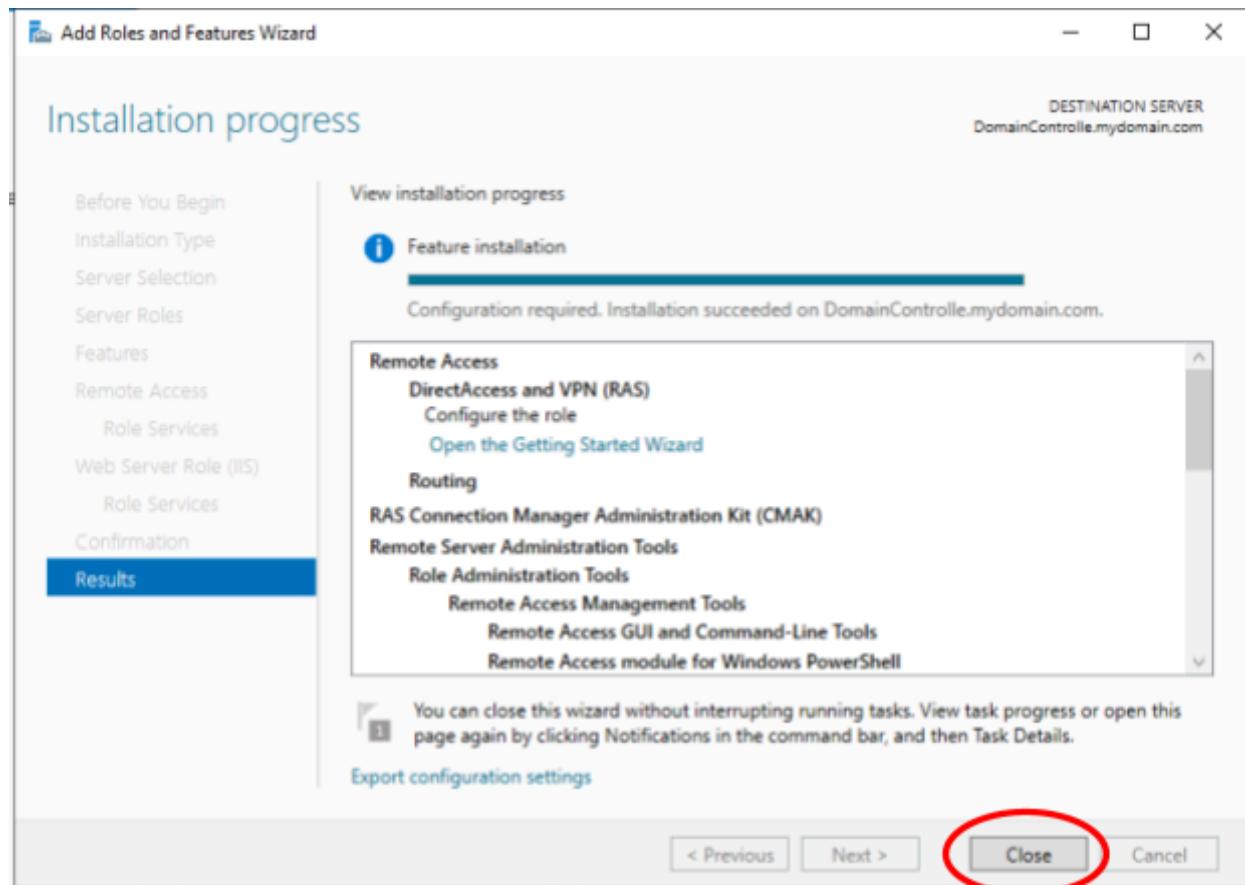
Click Next



Click Install



Click Close when finished installing

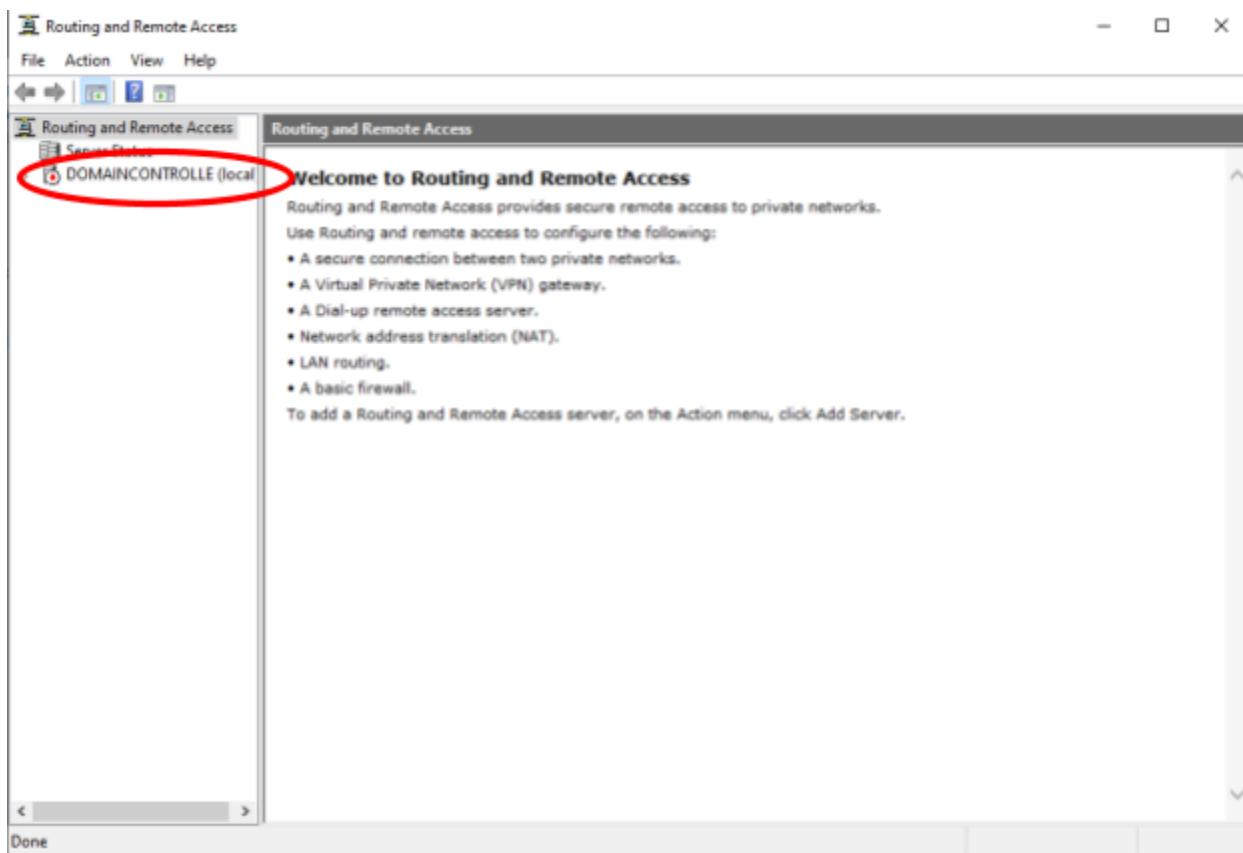


Once it is finished installing, navigate to Tools on the Top-Right corner of the Server Manager Dashboard

The screenshot shows the 'Server Manager > Dashboard' interface. On the left is a navigation bar with links like 'Dashboard', 'Local Server', 'All Servers', 'AD DS', 'DNS', 'File and Storage Services', 'IIS', and 'Remote Access'. The main area is titled 'WELCOME TO SERVER MANAGER' and features a 'QUICK START' section with numbered steps: 1. Configure this local server, 2. Add roles and features, 3. Add other servers to manage, 4. Create a server group, and 5. Connect this server to cloud services. Below this is a 'ROLES AND SERVER GROUPS' section showing three groups: AD DS (1), DNS (1), and File and Storage Services (1), each with sub-options like Manageability, Events, Services, Performance, and BPA results. At the top right, there are 'Manage', 'Tools' (circled in red), 'View', and 'Help' buttons.

Select Routing and Remote Access

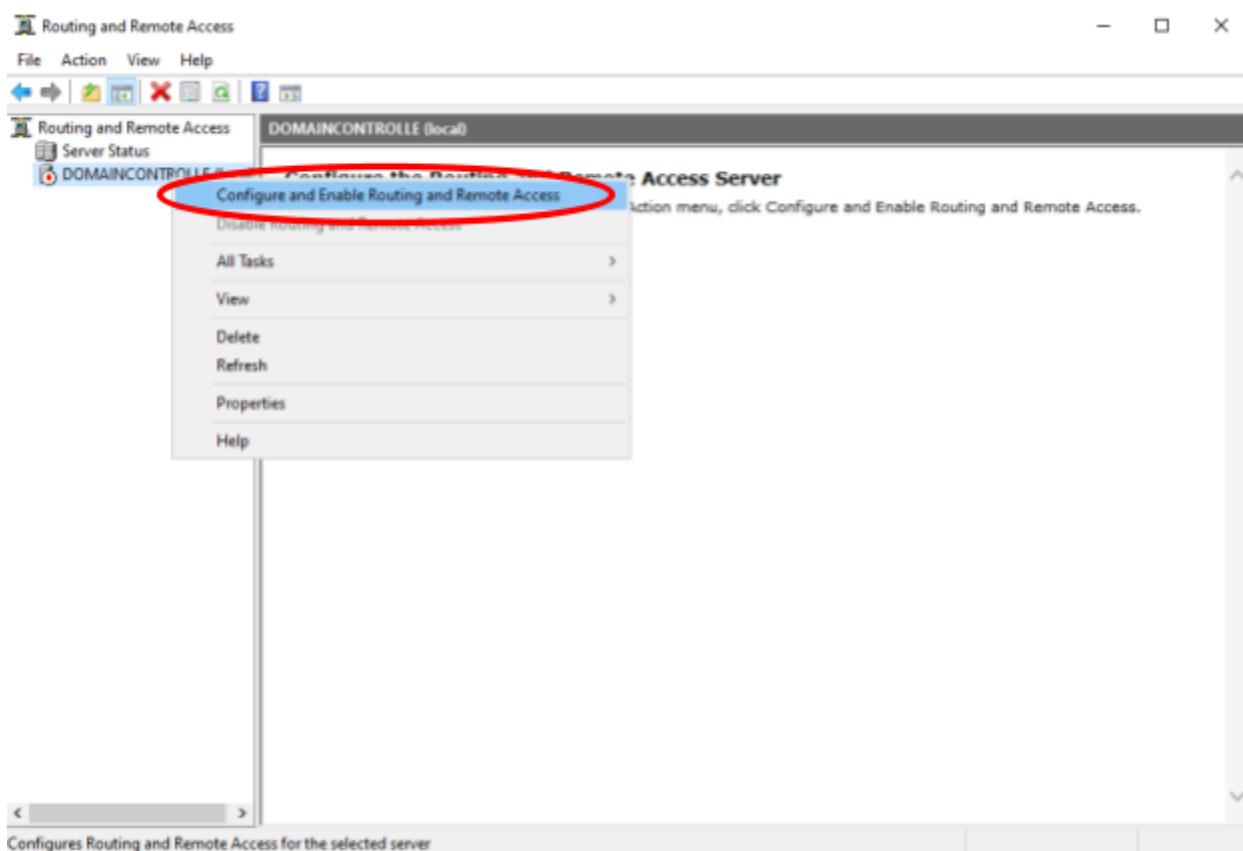
This screenshot is similar to the first one but shows the 'Tools' menu expanded. The 'Tools' menu includes options such as Computer Management, Connection Manager Administration Kit, Defragment and Optimize Drives, Disk Cleanup, DNS, Event Viewer, Group Policy Management, Internet Information Services (IIS) Manager, iSCSI Initiator, Local Security Policy, Microsoft Azure Services, Network Policy Server, ODBC Data Sources (32-bit), ODBC Data Sources (64-bit), Performance Monitor, Recovery Drive, Registry Editor, Remote Access Management, Resource Monitor, and Routing and Remote Access. The 'Routing and Remote Access' option is highlighted with a blue selection bar.



Notice that our domain has a red arrow-down icon.

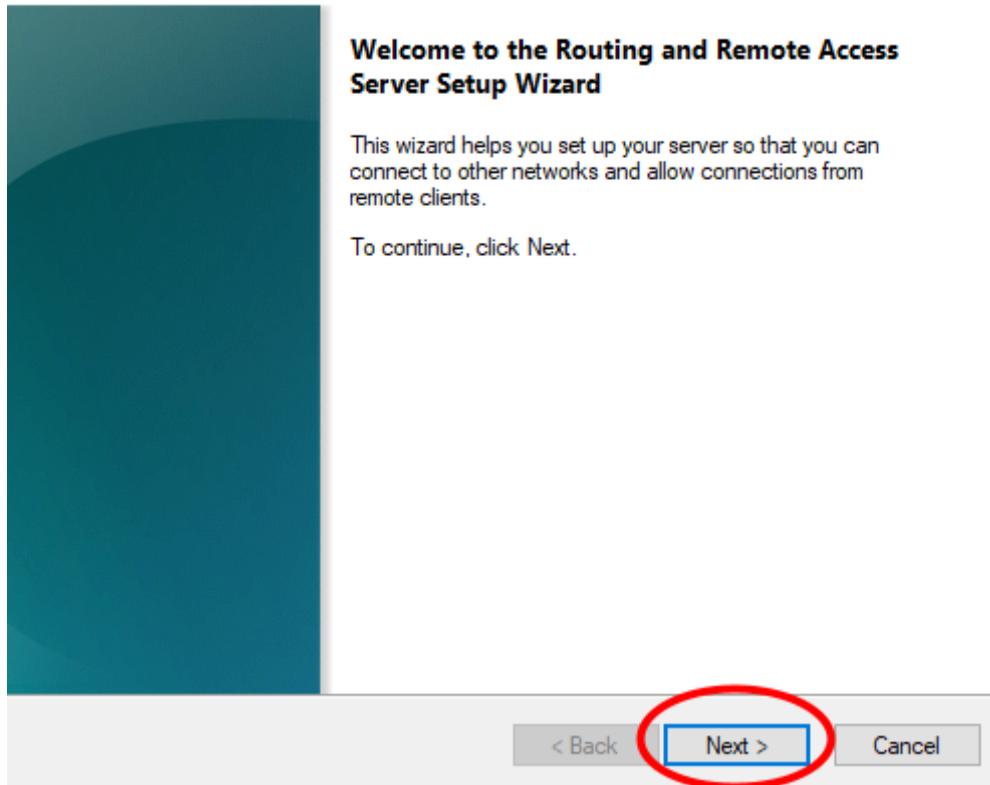
We will need to configure and enable Routing and Remote Access.

Right-click on the domain and select Configure and Enable Routing and Remote Access.



Click Next

Routing and Remote Access Server Setup Wizard



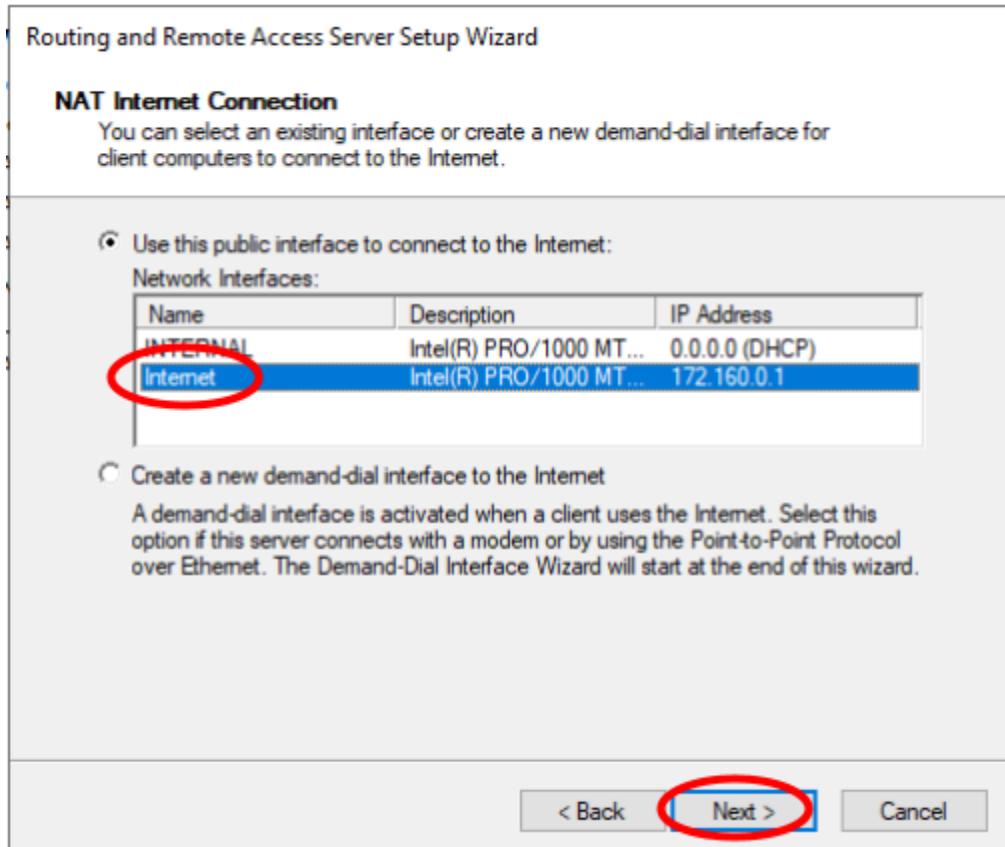
Select Network Address Translation (NAT) and click Next

The screenshot shows the 'Configuration' screen of the setup wizard. It lists several service options:

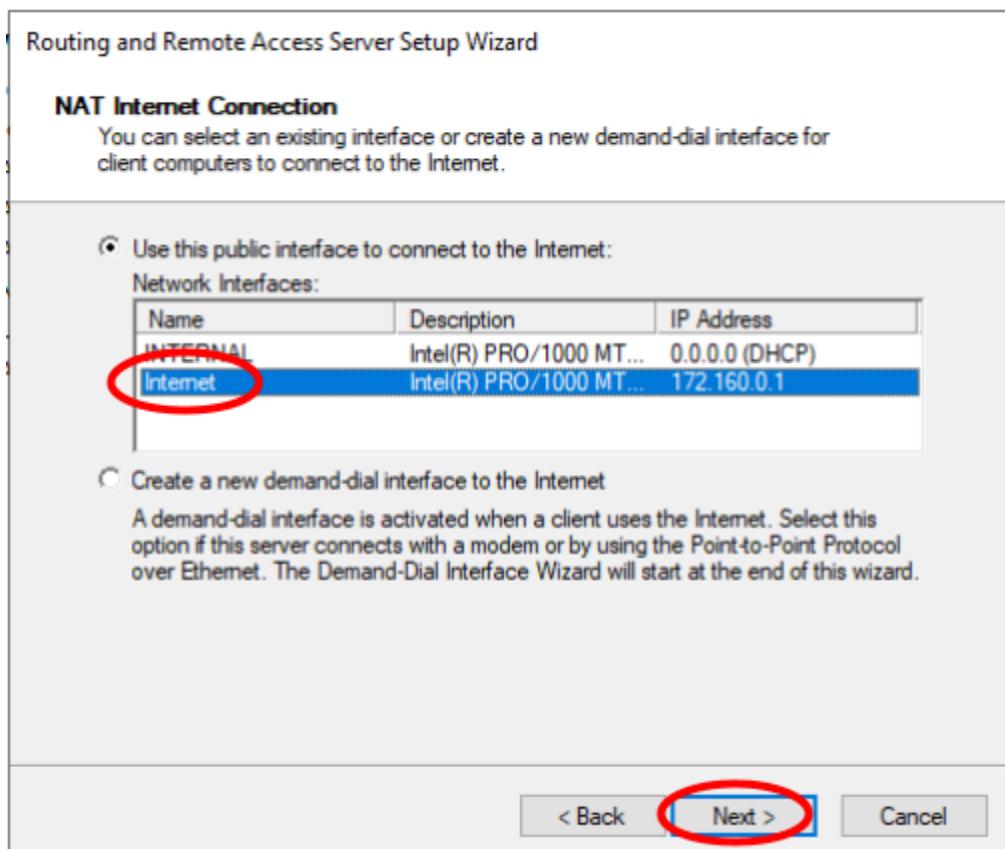
- Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.
- Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address. **1**
- Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.
- Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
- Custom configuration
Select any combination of the features available in Routing and Remote Access.

At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red oval. A large red number '2' is overlaid on the bottom right of the configuration area.

Select Internet since we are using this domain as our default gateway for computers connected to it



Click Next



Click Finish

Routing and Remote Access Server Setup Wizard

Completing the Routing and Remote Access Server Setup Wizard

You have successfully completed the Routing and Remote Access Server Setup wizard.

Summary:

Configured NAT for the following Internet interface: Internet

NAT relies on external DNS and DHCP servers. Confirm that these services are configured properly.

To enable servers to respond to Internet requests, configure port mappings and update your firewall.

To close this wizard, click Finish.

< Back

Finish

Cancel

Completing Initialization



Please wait while the Routing and Remote Access service finishes initialization.

To enable servers to respond to Internet requests, configure port mappings and update your firewall.

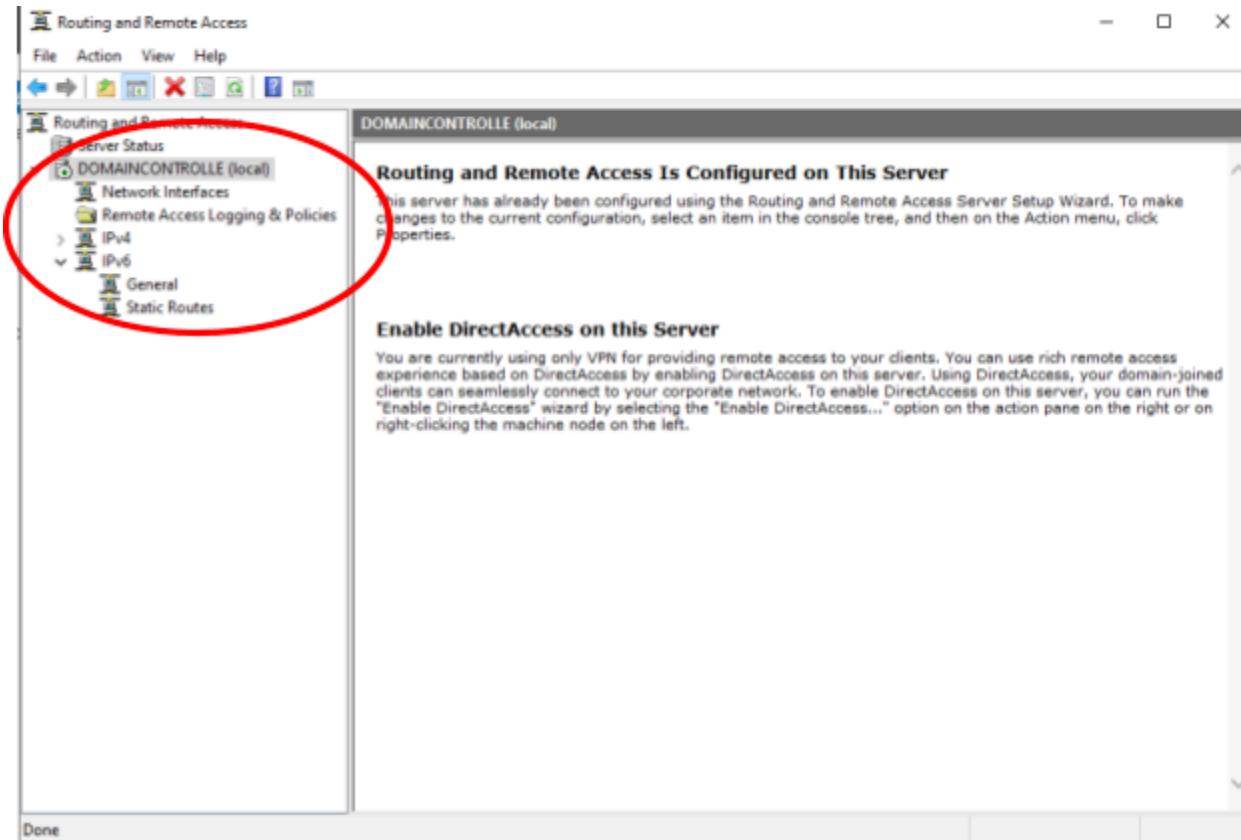
To close this wizard, click Finish.

< Back

Finish

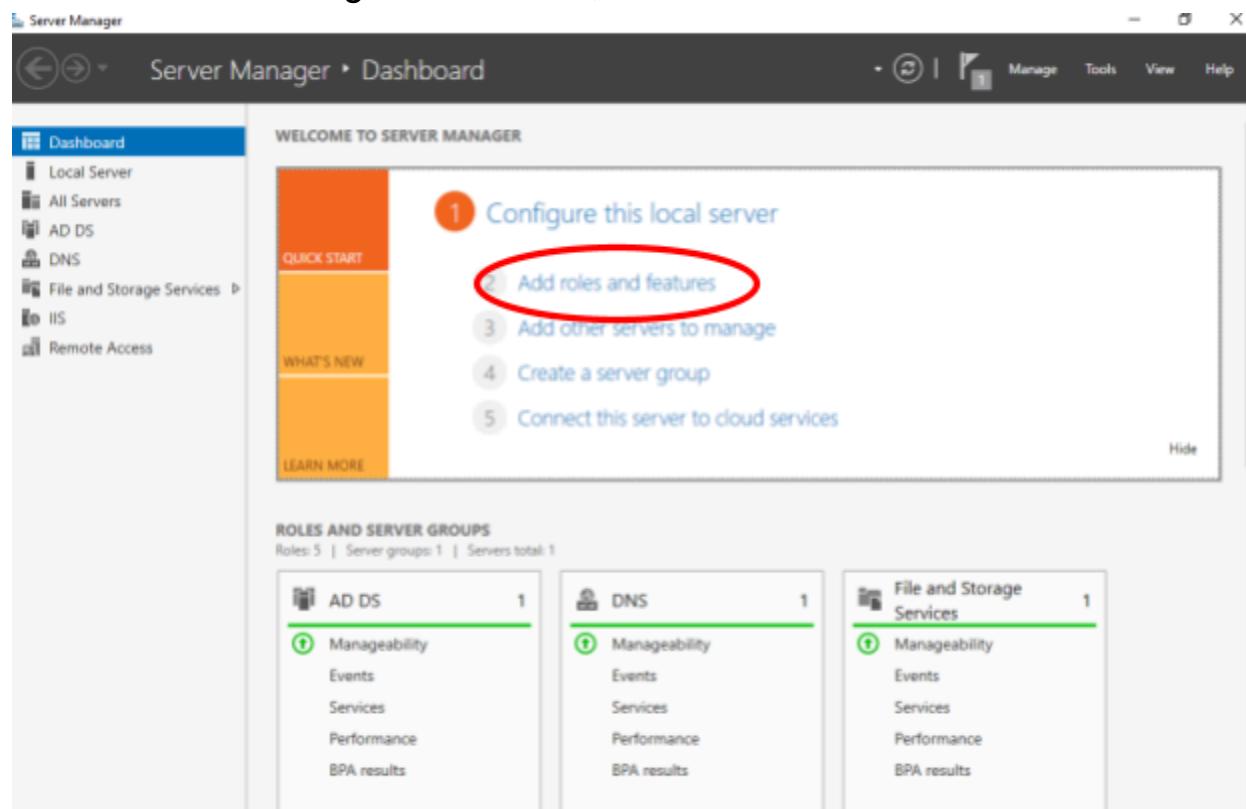
Cancel

Now, RAS and NAT are configured and enabled for this domain



Step 8: Set up a DHCP server on our Domain Controller

On the Server Manager Dashboard, click on Add Roles and Features



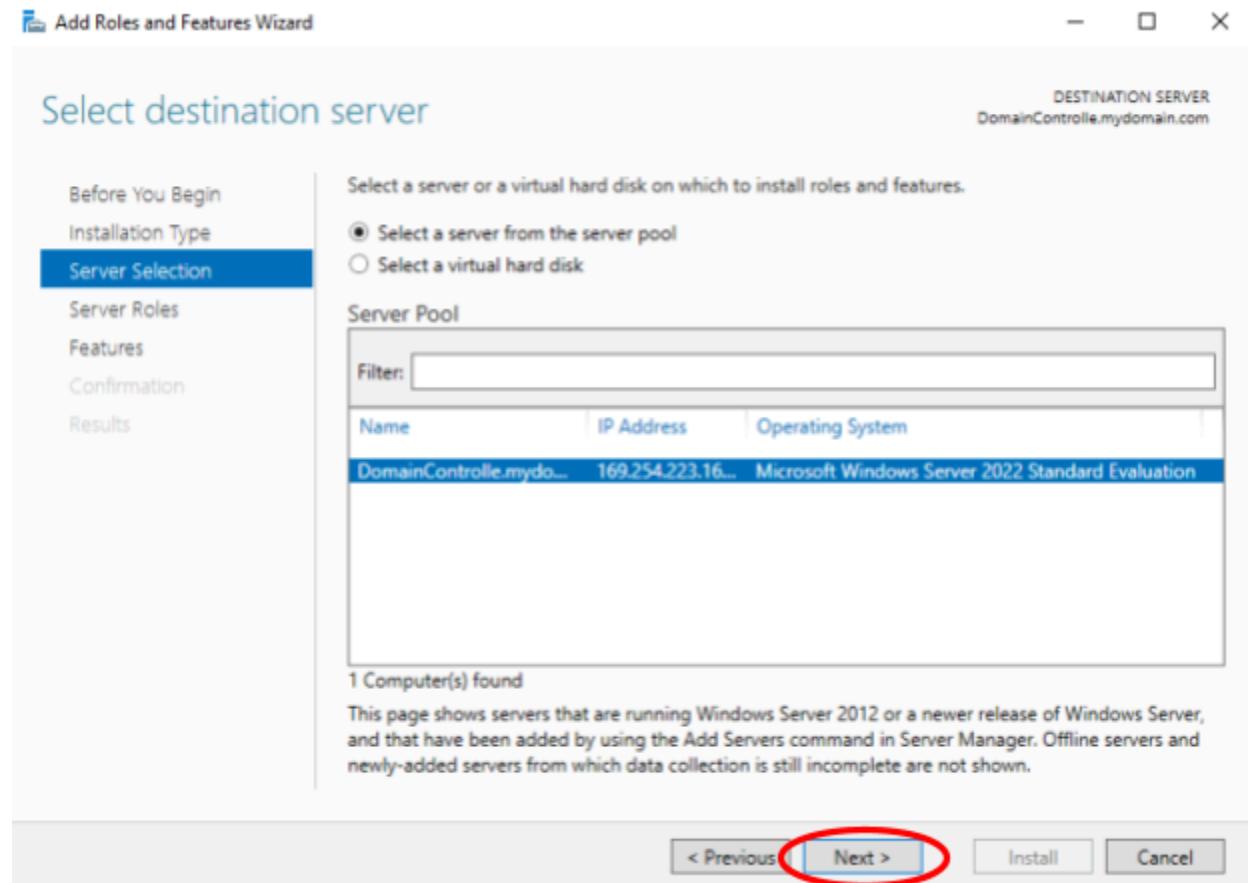
Click Next

The screenshot shows the 'Before you begin' step of the 'Add Roles and Features Wizard'. The title bar says 'Add Roles and Features Wizard'. The top right corner shows 'DESTINATION SERVER' and 'DomainController.mydomain.com'. On the left, a sidebar lists steps: 'Before You Begin' (selected), 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main content area contains text about the wizard's purpose, instructions for removing roles, and a list of prerequisites. It also includes a note about verifying prerequisites and a link to continue. A checkbox for skipping the page by default is present. At the bottom, there are buttons for '< Previous', 'Next >', 'Install', and 'Cancel'. The 'Next >' button is circled in red.

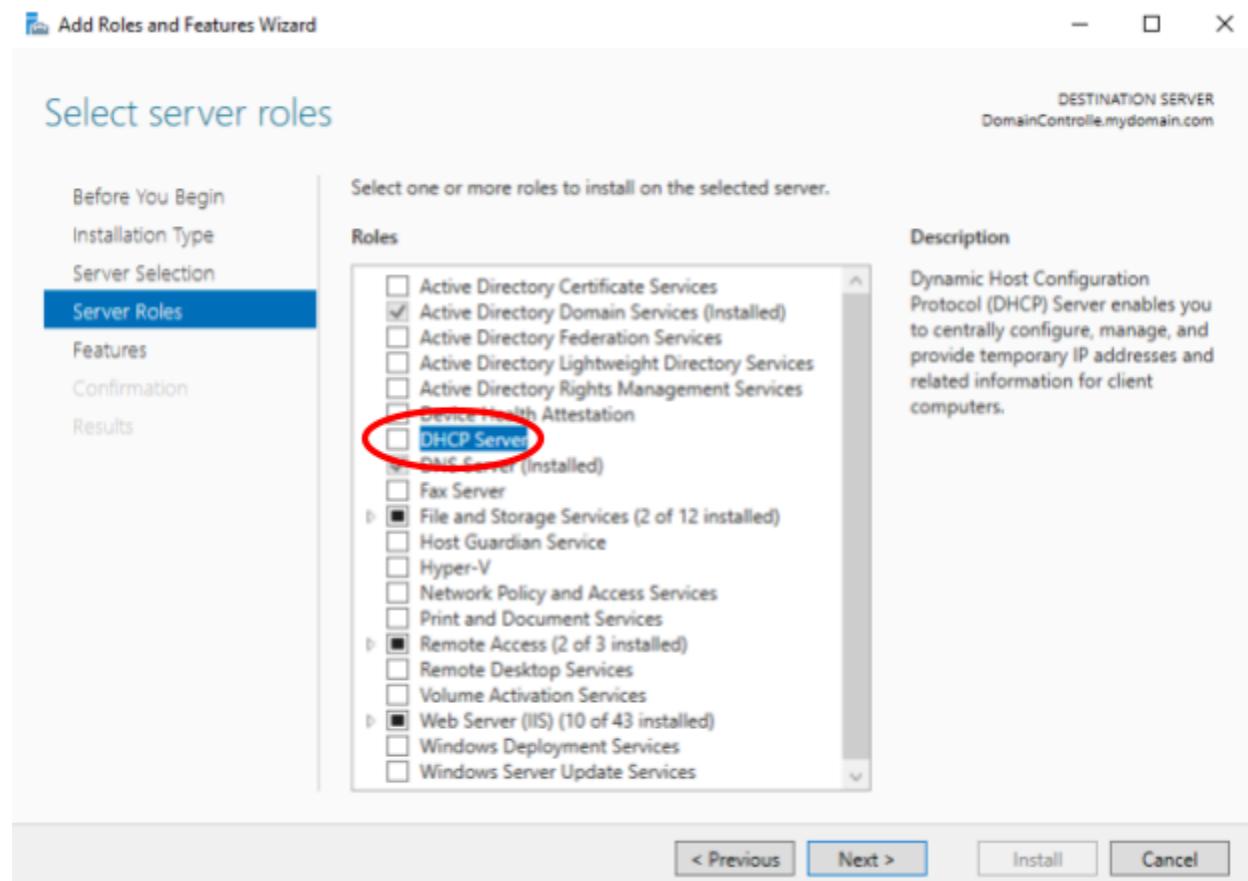
Click Next

The screenshot shows the 'Select installation type' step of the 'Add Roles and Features Wizard'. The title bar says 'Add Roles and Features Wizard'. The top right corner shows 'DESTINATION SERVER' and 'DomainController.mydomain.com'. On the left, a sidebar lists steps: 'Before You Begin' (selected), 'Installation Type' (selected), 'Server Selection', 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main content area contains text about selecting the installation type (physical computer or virtual machine) and two options: 'Role-based or feature-based installation' (selected) and 'Remote Desktop Services installation'. The 'Role-based or feature-based installation' section includes a sub-instruction about configuring a single server. At the bottom, there are buttons for '< Previous', 'Next >', 'Install', and 'Cancel'. The 'Next >' button is circled in red.

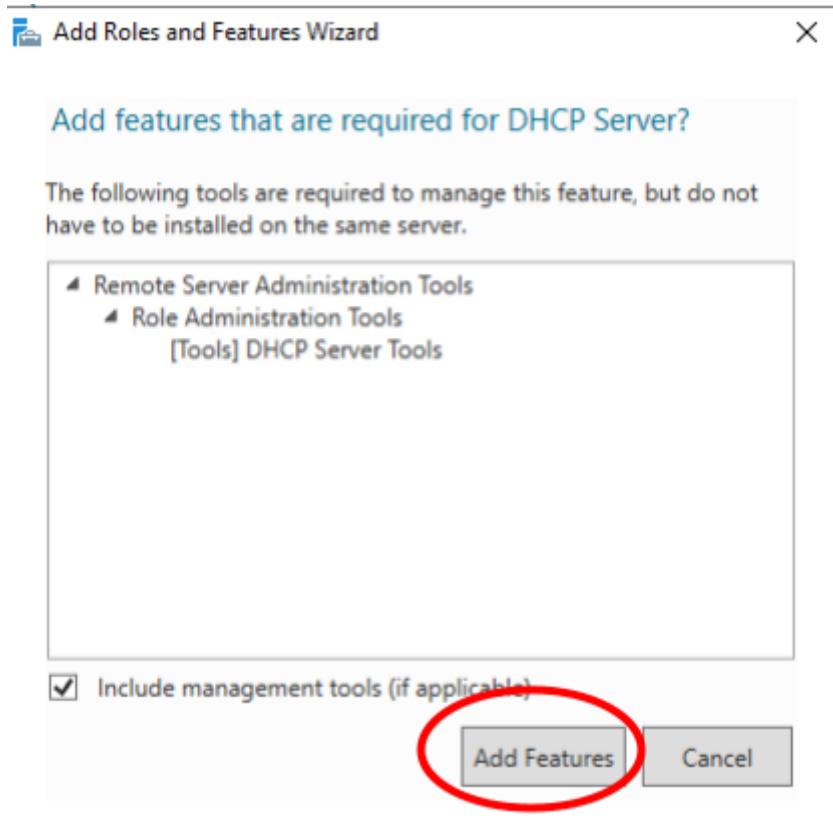
Click Next



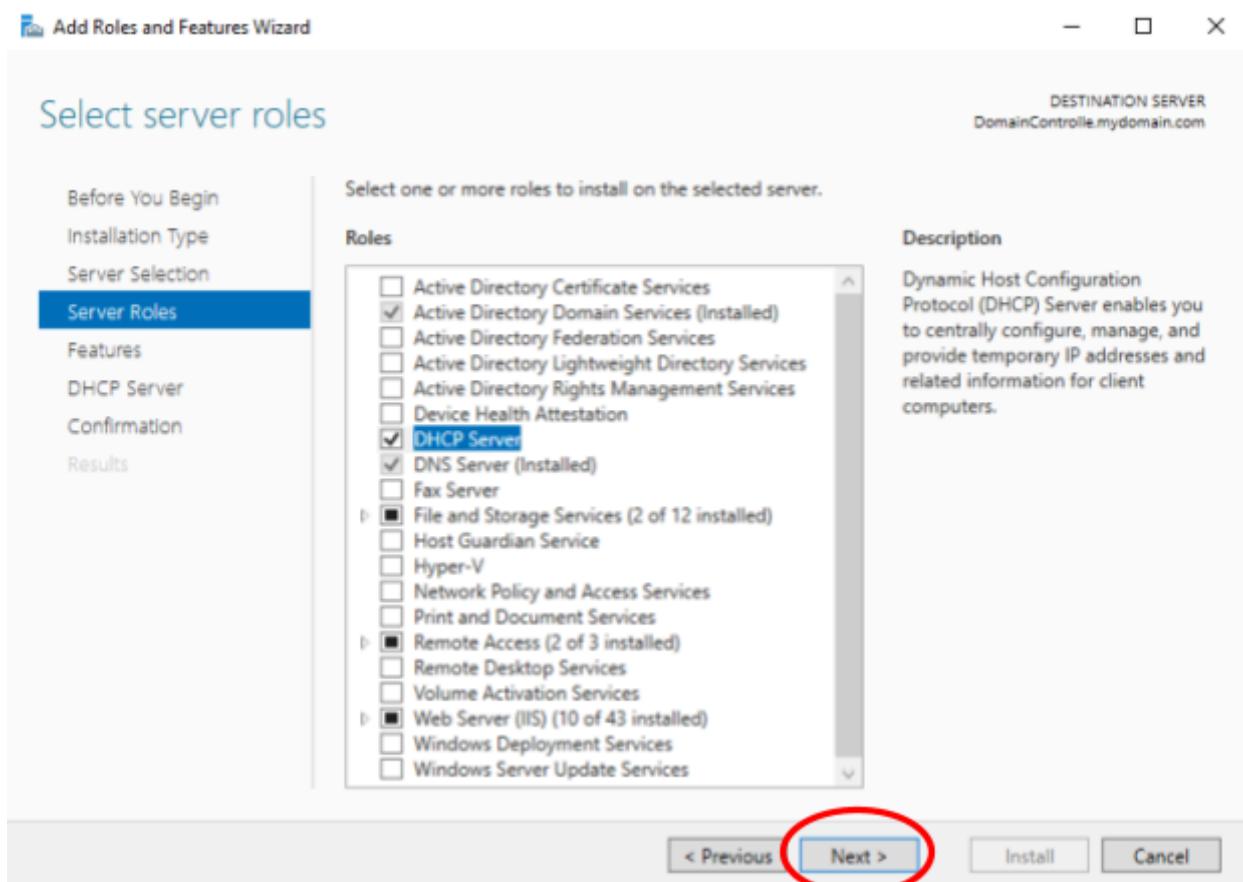
Select DHCP Server



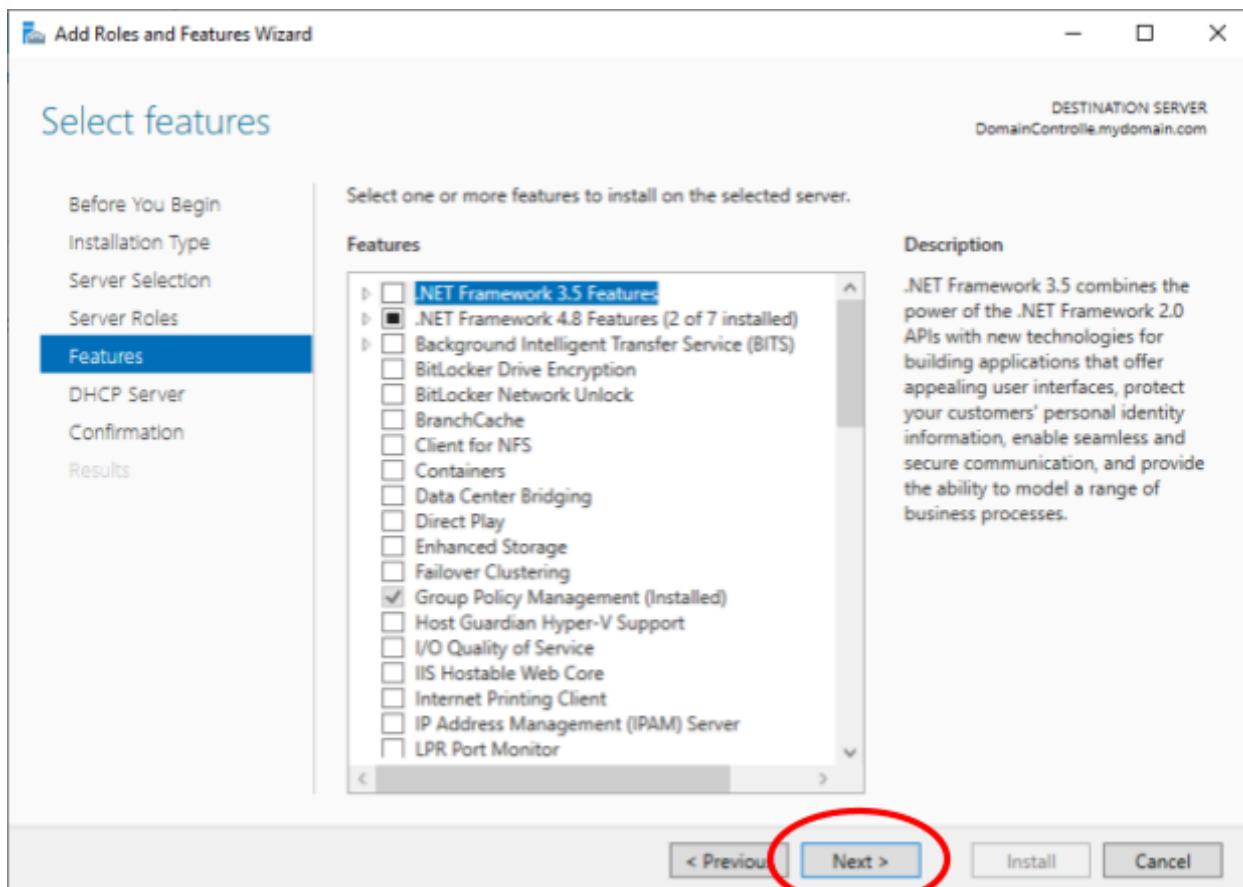
Click Add Feature



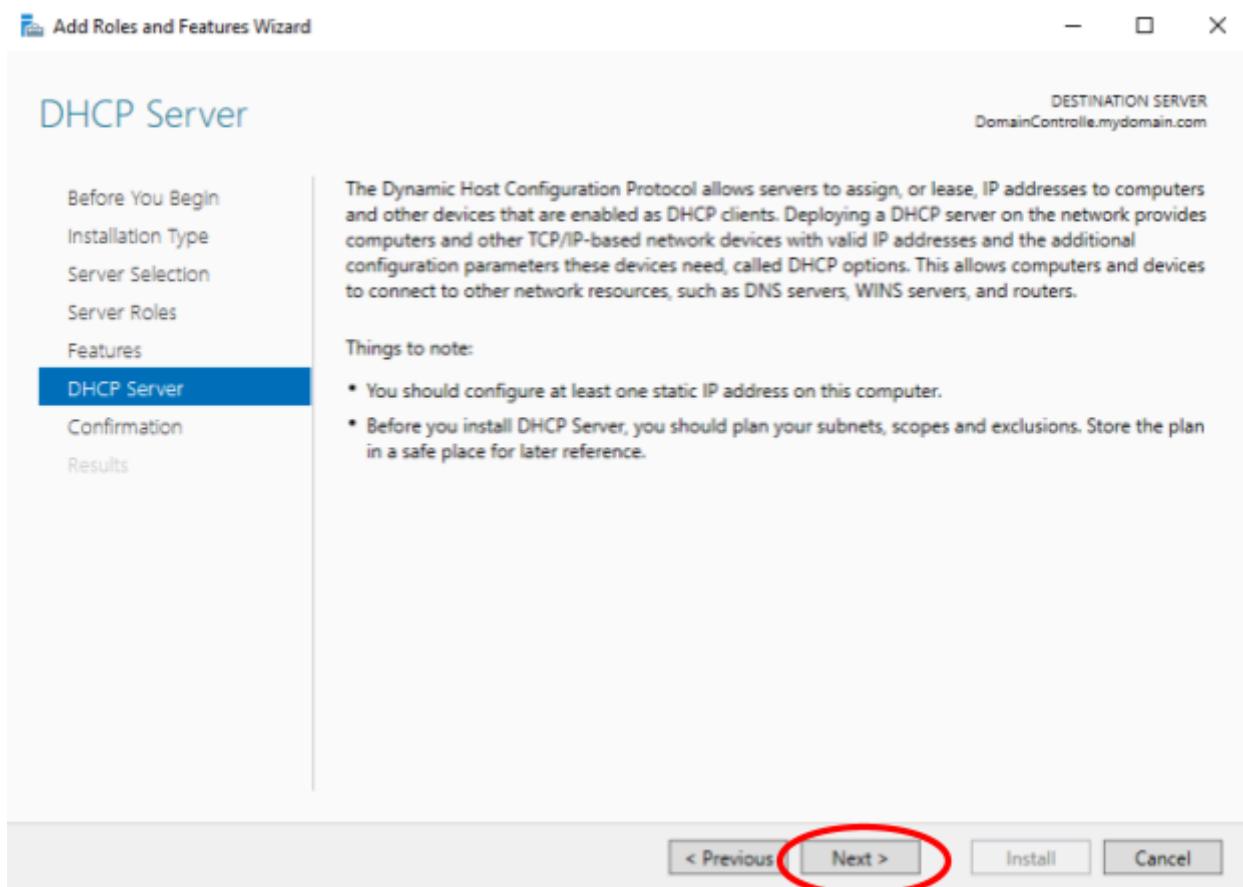
Click Next



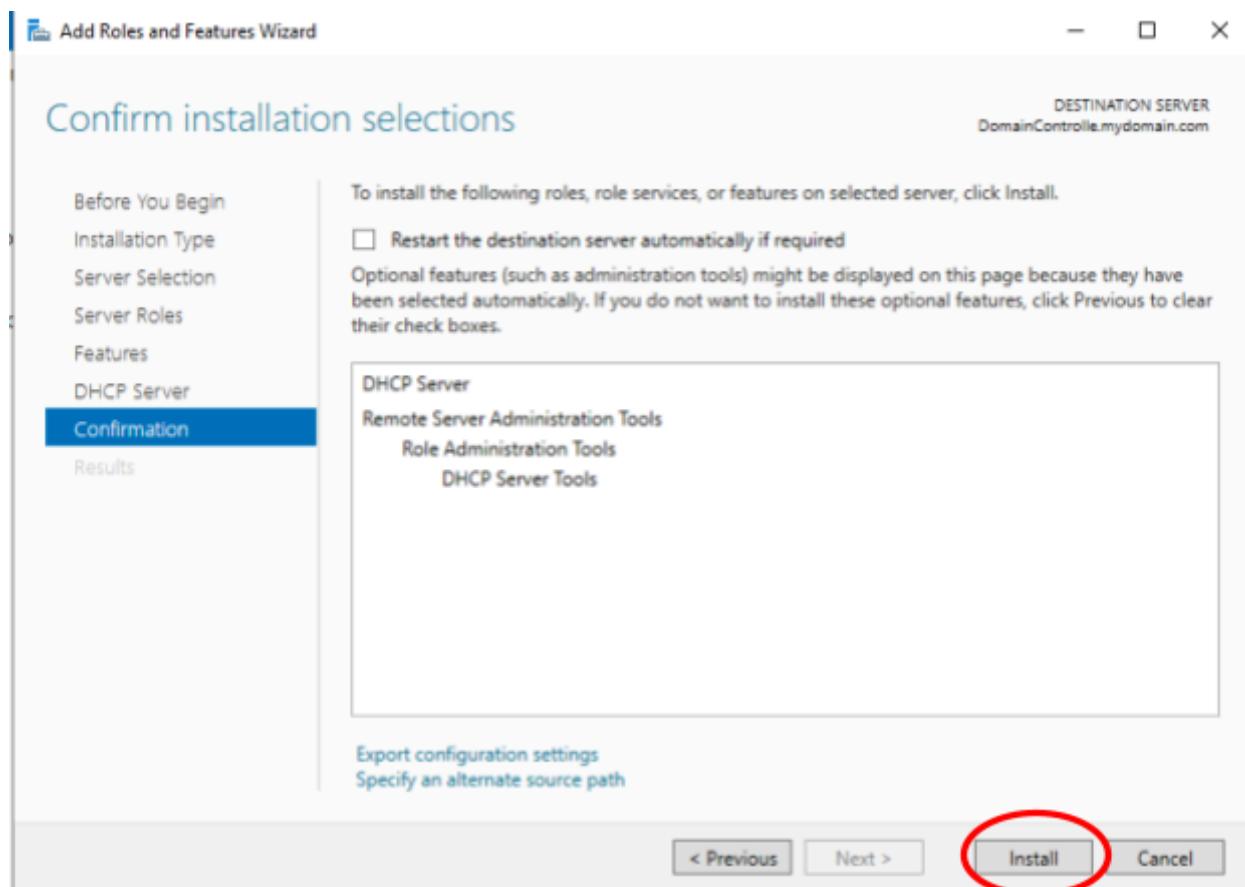
Click Next



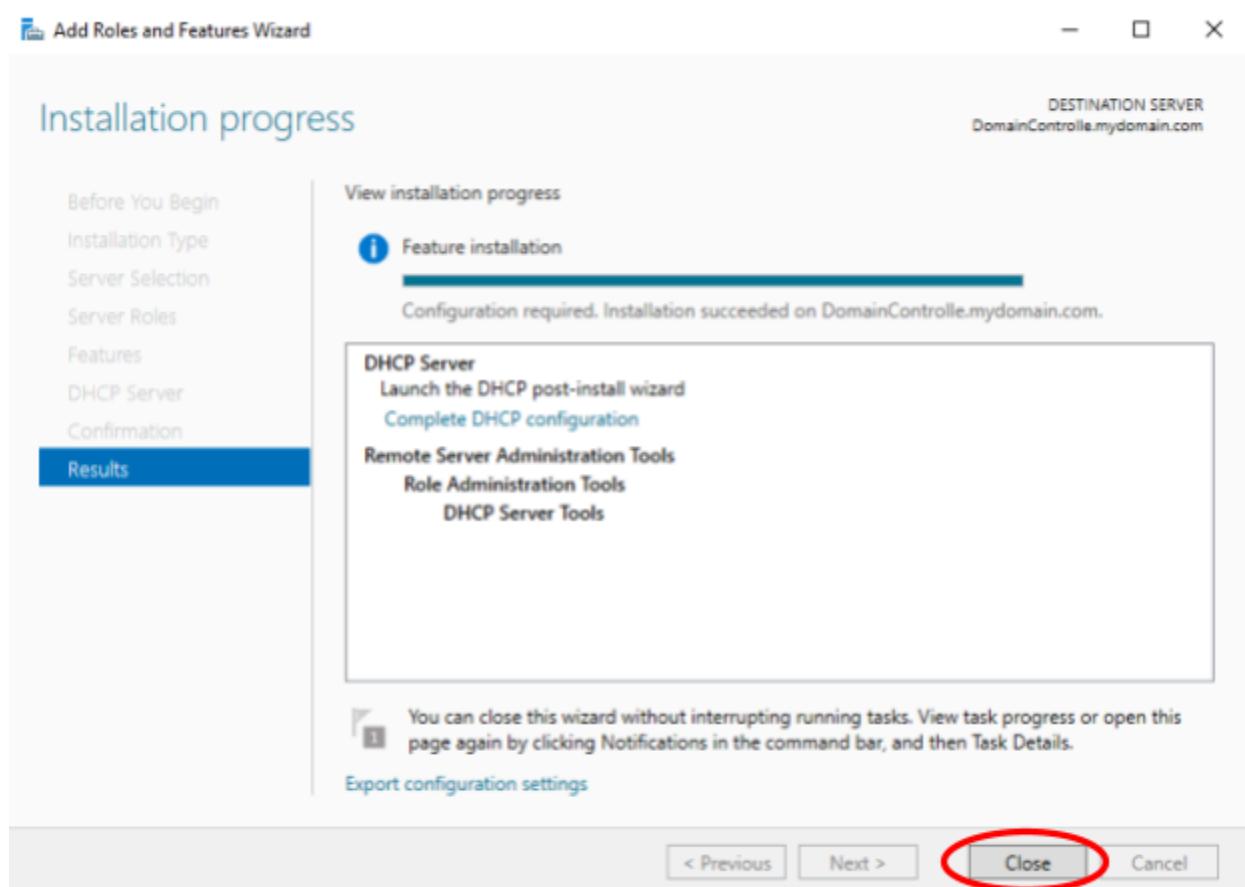
Click Next



Click Install



Click Close when Installation is finished



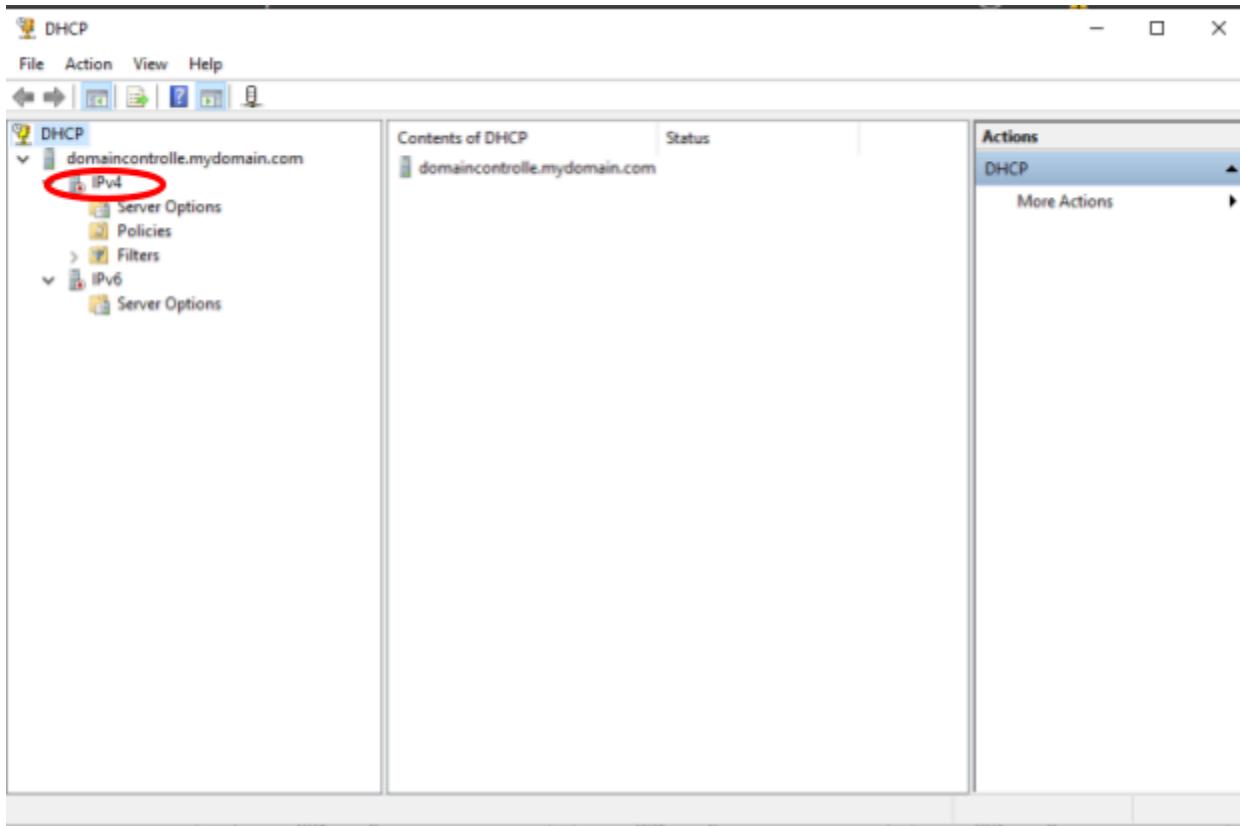
Again, select Tools on the Top-Right Corner

The screenshot shows the Windows Server Manager Dashboard. On the top right, there is a navigation bar with icons for Manage, Tools (which is circled in red), View, and Help. Below this, the main area displays a 'WELCOME TO SERVER MANAGER' message and a 'QUICK START' panel with five numbered steps: 1. Configure this local server, 2. Add roles and features, 3. Add other servers to manage, 4. Create a server group, and 5. Connect this server to cloud services. To the left is a sidebar with links for Dashboard, Local Server, All Servers, AD DS, DHCP, DNS, File and Storage Services, IIS, and Remote Access. At the bottom, there's a 'ROLES AND SERVER GROUPS' section showing AD DS, DHCP, and DNS roles.

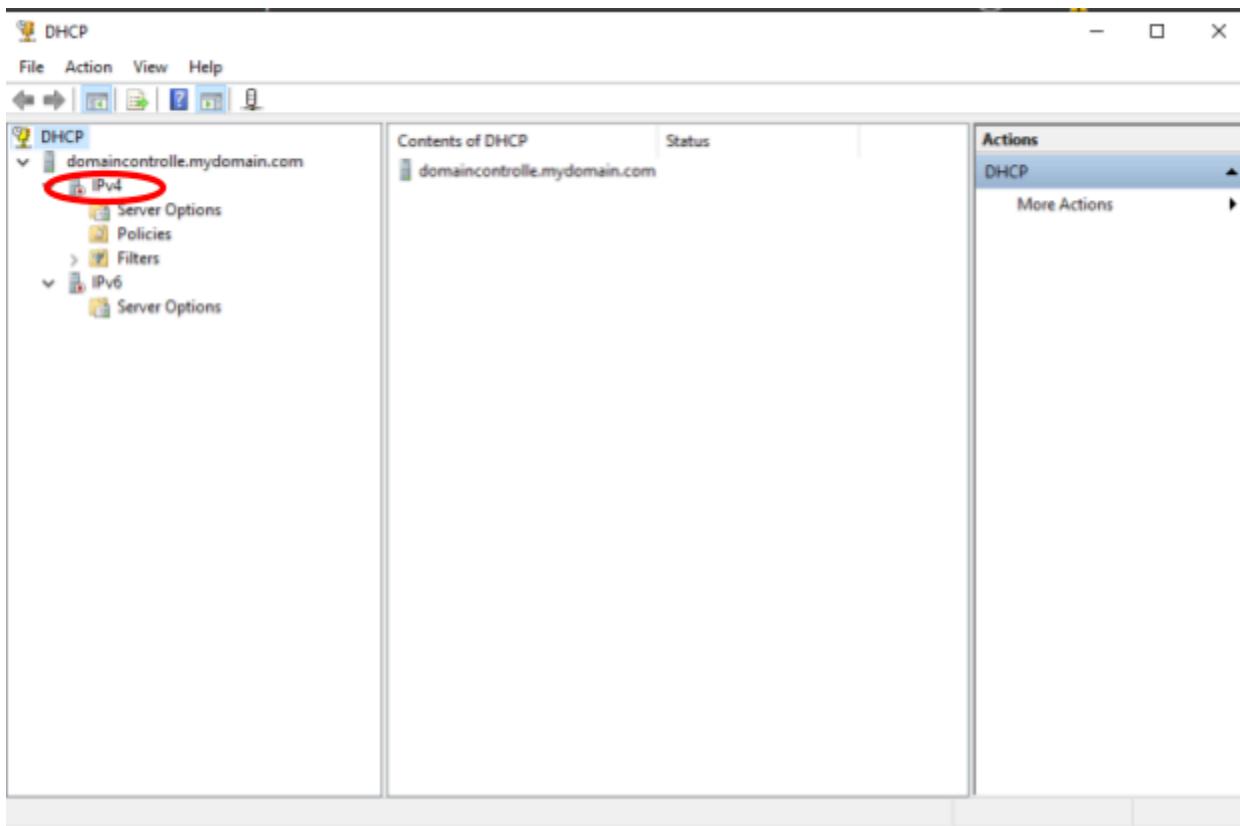
Select DHCP

This screenshot is similar to the previous one, showing the Server Manager Dashboard. However, the 'Tools' menu has been expanded, and the 'DHCP' option is highlighted with a red circle. The expanded menu includes: Component Services, Computer Management, Connection Manager Administration Kit, Defragment and Optimize Drives, DHCP (which is highlighted), Disk Cleanup, DNS, Event Viewer, Group Policy Management, Internet Information Services (IIS) Manager, iSCSI Initiator, Local Security Policy, Microsoft Azure Services, Network Policy Server, ODBC Data Sources (32-bit), ODBC Data Sources (64-bit), Performance Monitor, Recovery Drive, Registry Editor, Remote Access Management, Resource Monitor, Routing and Remote Access, Services, System Configuration, System Information, Task Scheduler, Windows Defender Firewall with Advanced Security, and Windows Memory Diagnostic.

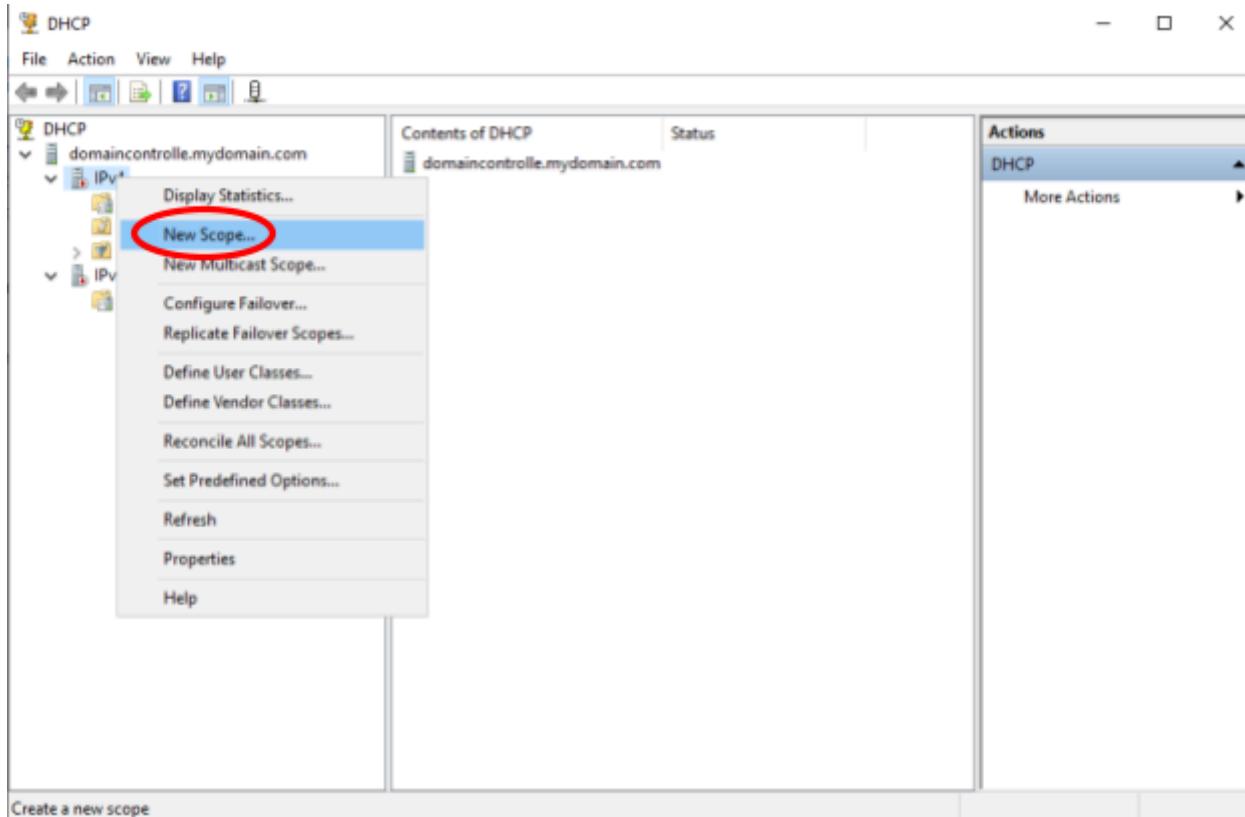
We're going to add a scope of IP Addresses that this domain will give to computers that are connected to it



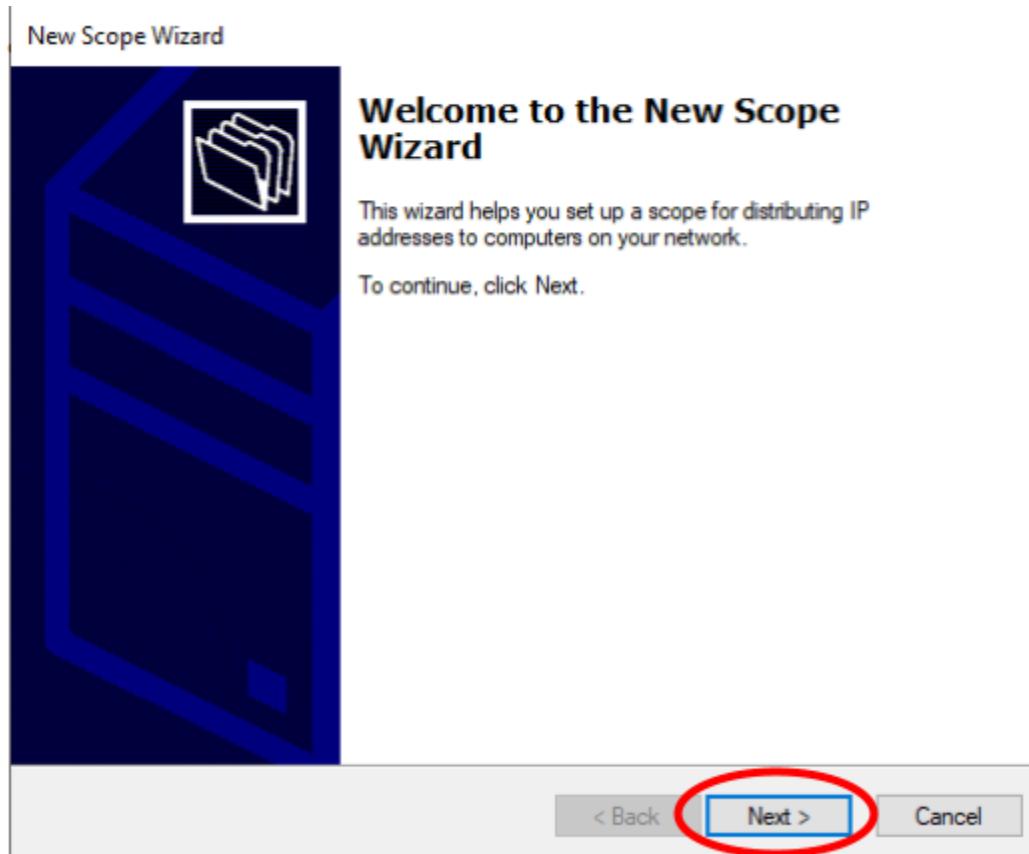
We notice that the IPv4 has a red arrow down icon, meaning that the DHCP is not configured



Right-click on the IPv4 and select New Scope



Click Next on the New Scope Wizard



Name the Scope. In this case, we will name it the scope of IPv4 addresses we are going to add to it.

New Scope Wizard

Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name: 

Description:

[< Back](#) [Next >](#) [Cancel](#)

Add the Start IP Address and End IP Address, and the length of the subnet mask and the subnet mask. Click Next when finished.

New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 

End IP address: 

Configuration settings that propagate to DHCP Client

Length: 

Subnet mask: 

[< Back](#) [Next >](#) [Cancel](#)

We are not going to add any Exclusions and Delays. Click Next

New Scope Wizard

Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCPOFFER message.



Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: End IP address:

Excluded address range:

Subnet delay in milli second:

We are going to add 8 days for the Lease Duration since it is a Lab Environment.

New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days: Hours: Minutes:

Select “Yes, I want to configure these options now”, and click Next

New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

Yes, I want to configure these options now

No, I will configure these options later

[< Back](#) [Next >](#) [Cancel](#)

We will add the Default Gateway IP address according to our network diagram in the beginning of the Document. In this case, we will add 172.16.0.1 as the IP address. Click Add

New Scope Wizard

Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address: [Add](#)

[< Back](#) [Next >](#) [Cancel](#)

Once the IP Address is added, click Next

New Scope Wizard

Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.



To add an IP address for a router used by clients, enter the address below.

IP address:

<input type="text" value="172.16.0.1"/>	<input type="button" value="Add"/>
<input type="button" value="172.16.0.1"/>	<input type="button" value="Remove"/>
<input type="button" value="Up"/>	
<input type="button" value="Down"/>	

< Back Cancel



Click Next

New Scope Wizard

Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.



You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

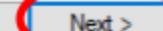
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

IP address:

<input type="text"/>	<input type="text" value="169.254.223.164"/>	<input type="button" value="Add"/>
<input type="button" value="Resolve"/>	<input type="button" value="Remove"/>	<input type="button" value="Up"/>
		<input type="button" value="Down"/>

< Back Cancel



Click Next

New Scope Wizard

WINS Servers

Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.



Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.

Server name:

Resolve

IP address:

 . . .

Add
Remove
Up
Down

To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.

< Back

Next >

Cancel

Ensure that “Yes, I want to activate this scope now” is selected. Click Next

New Scope Wizard

Activate Scope

Clients can obtain address leases only if a scope is activated.



Do you want to activate this scope now?

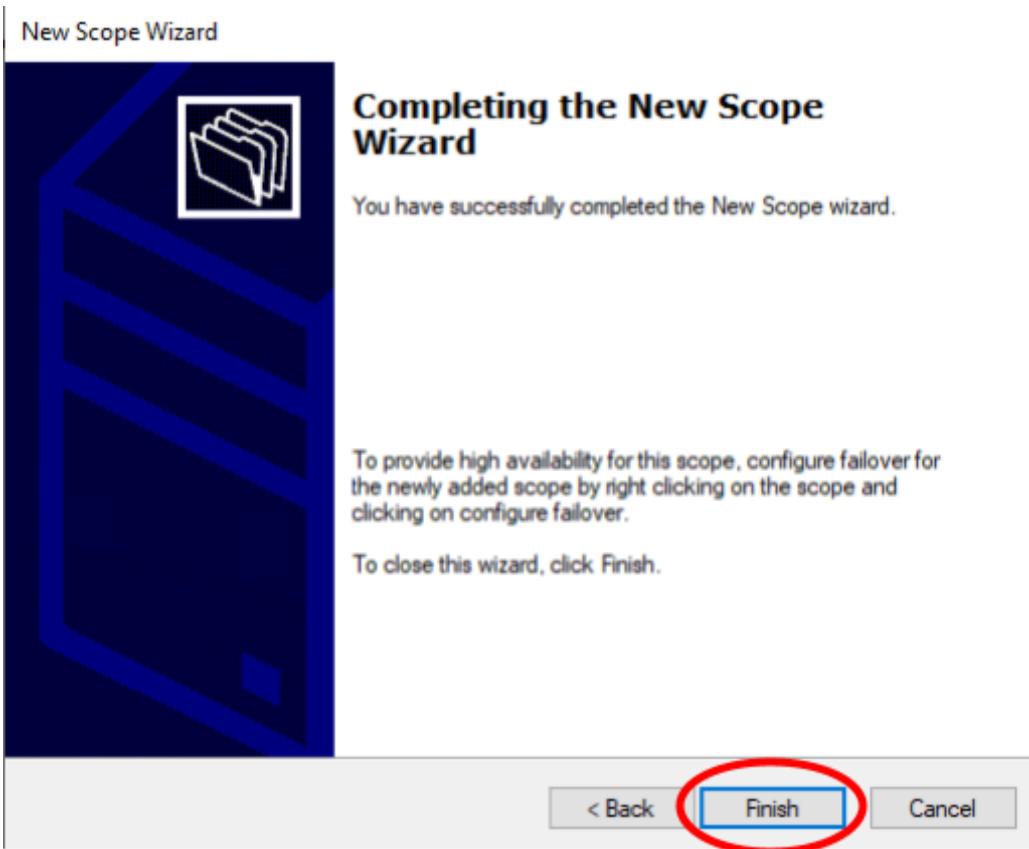
- Yes, I want to activate this scope now
 No, I will activate this scope later

< Back

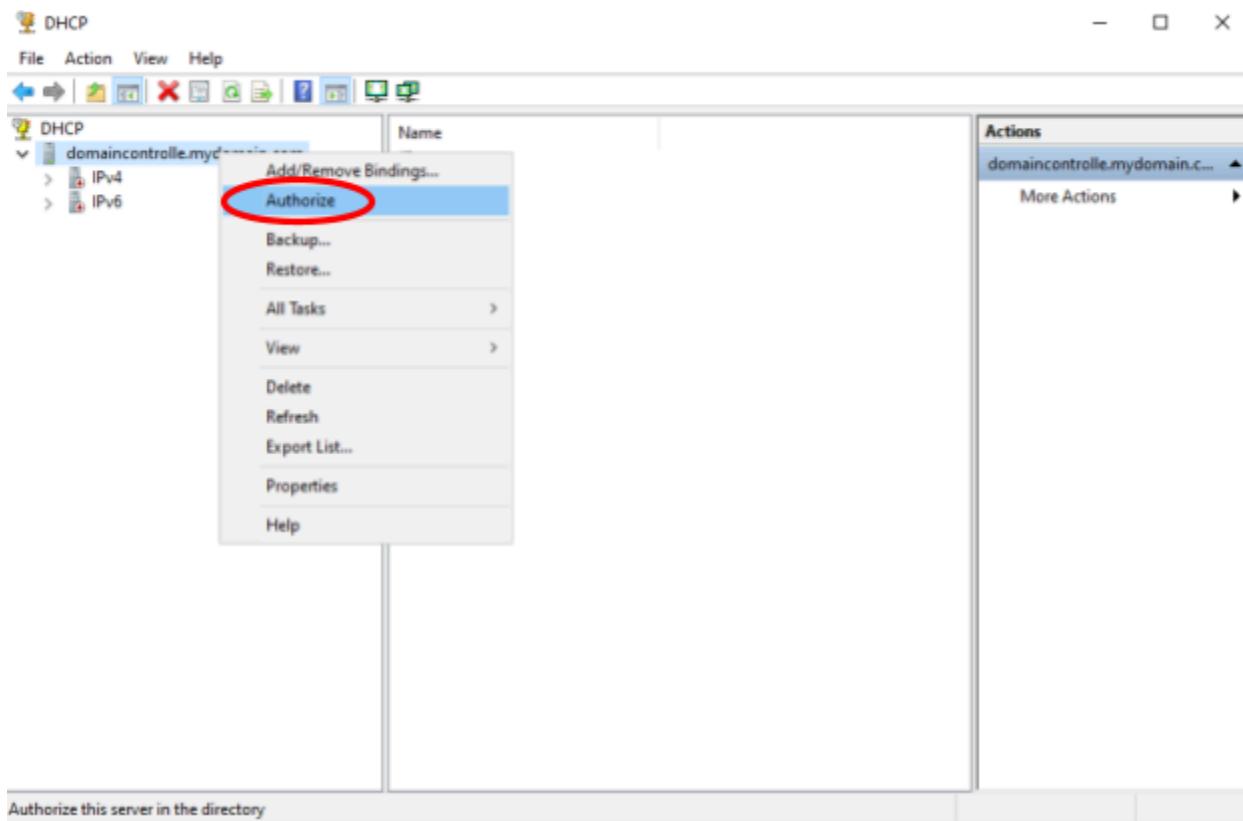
Next >

Cancel

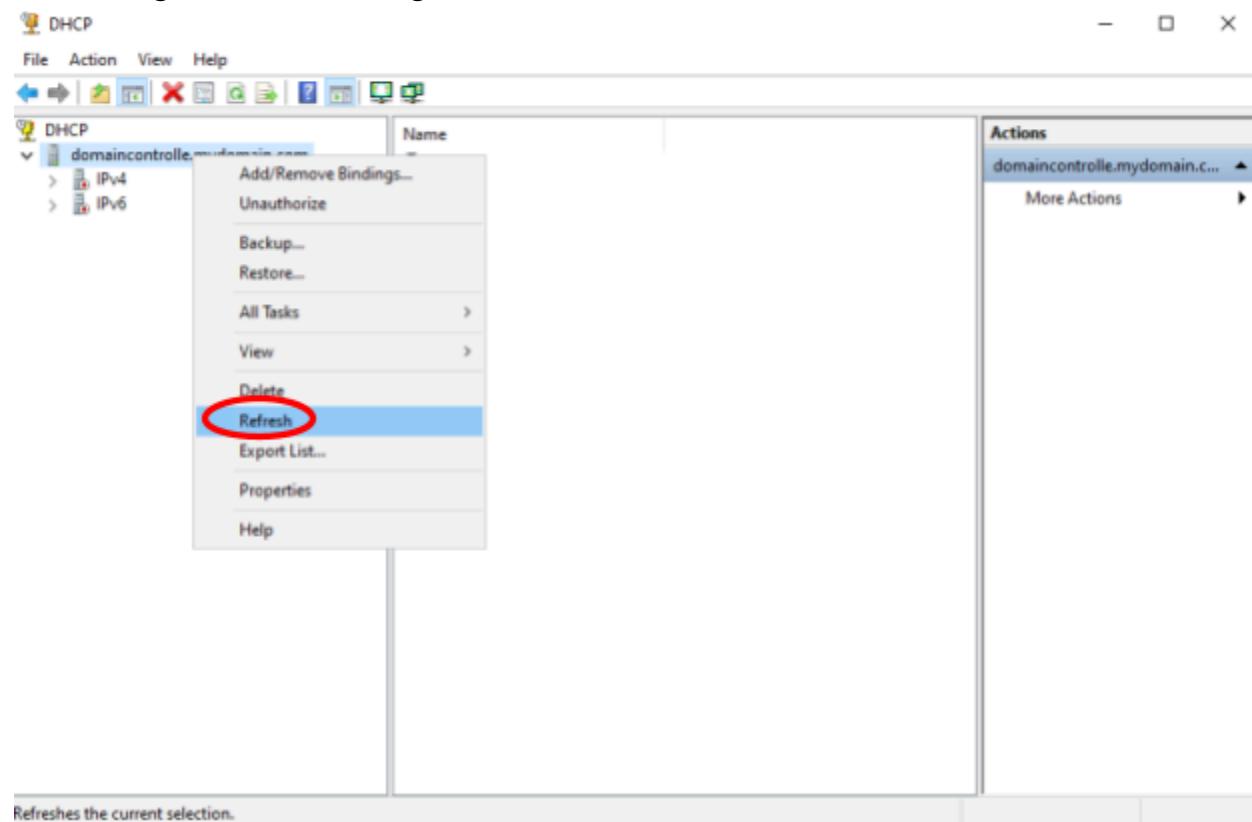
Click Finish



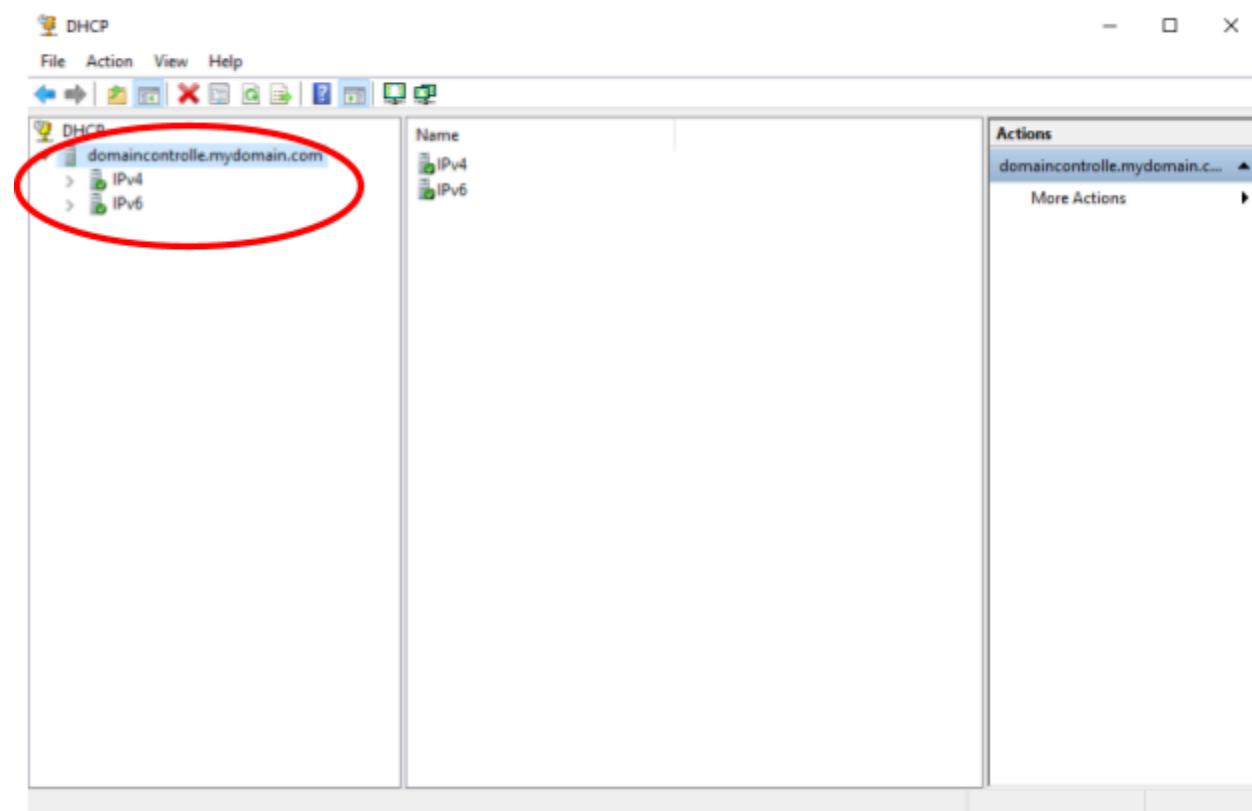
Back in the DHCP window, Right-Click on the domain controller name and select Authorize

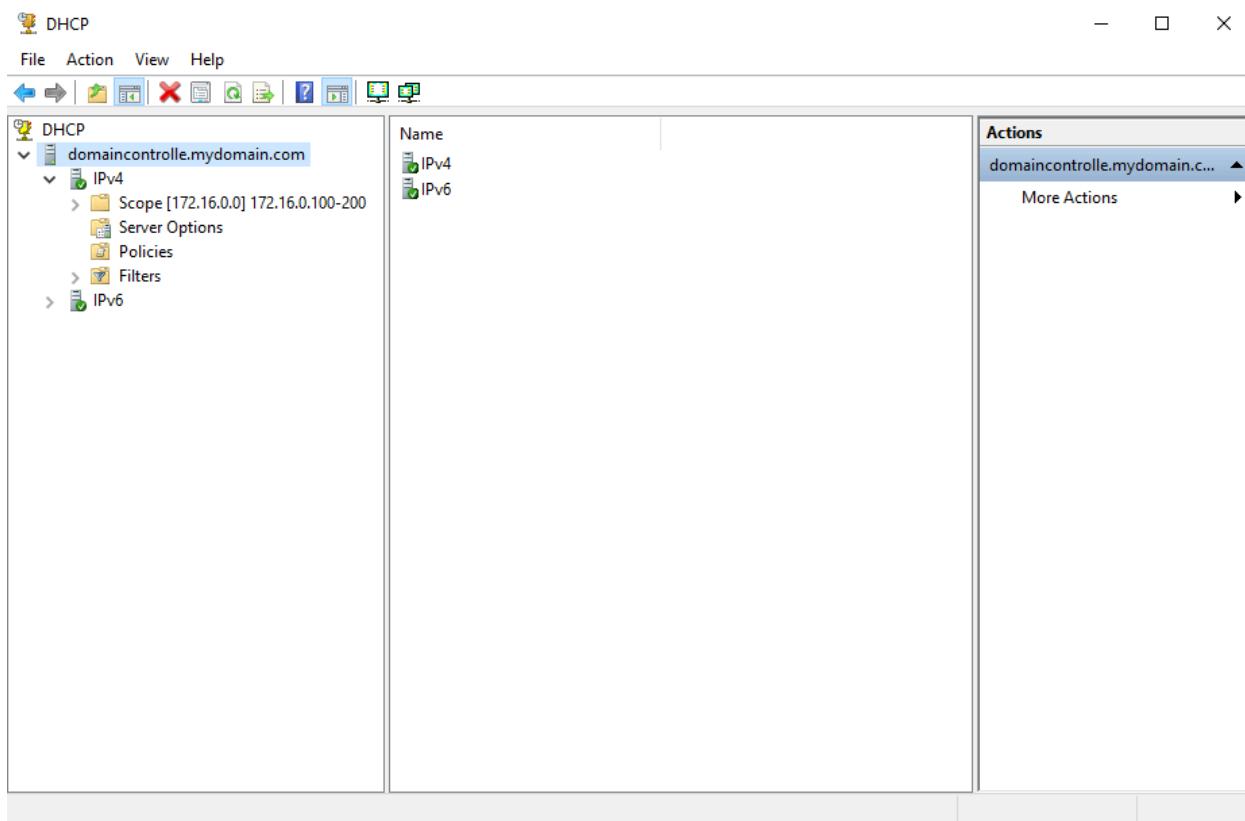


Then, Right-Click on it again and select Refresh



The IPv4 and IPv6 should now have a green arrow up icon

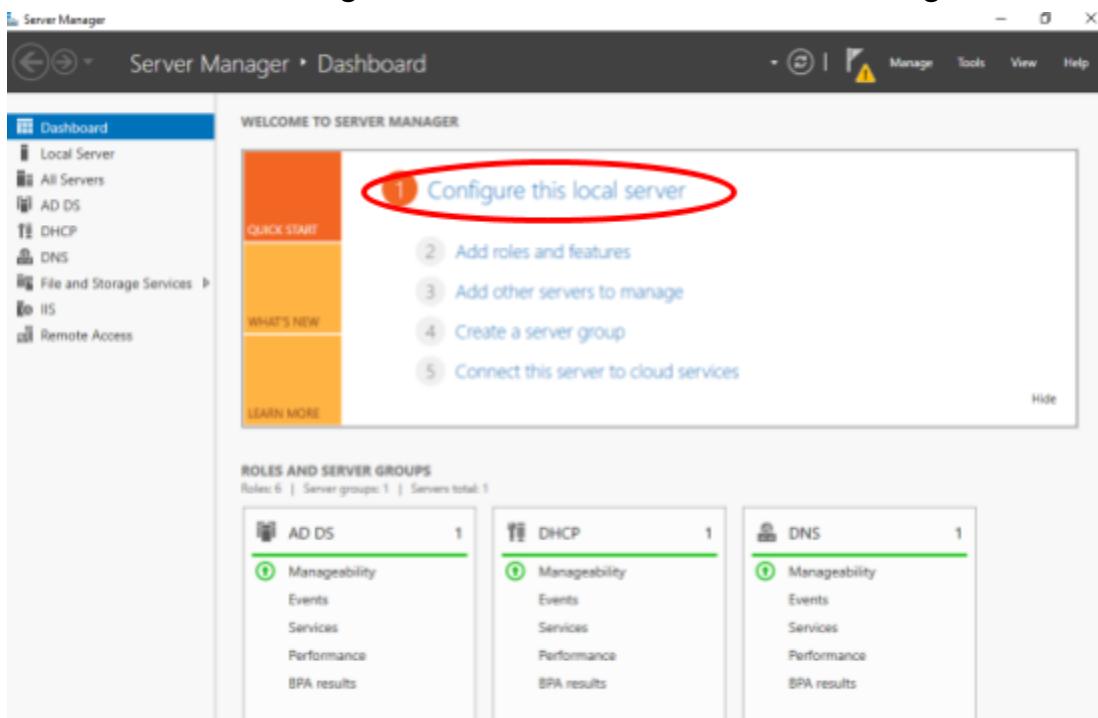




Step 9: Download the PowerShell Script that will add 1000 users to the Domain.

To begin, we must configure the server to let us browse the Internet so that we can download the PowerShell Script from the internet. This is usually not done in a Production Environment, but since this is a Lab Environment, we will make an exception.

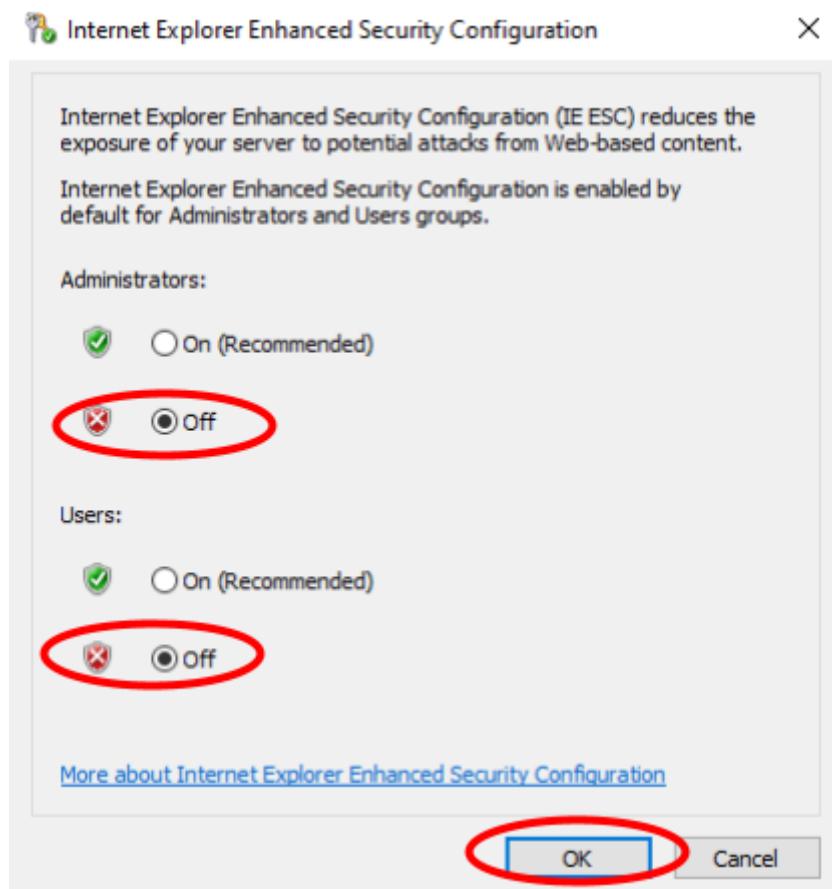
On the Server Manager Dashboard, we will select Configure this local server

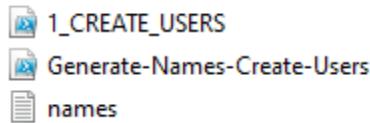


Navigate to the IE Enhanced Security Configuration and click on the On

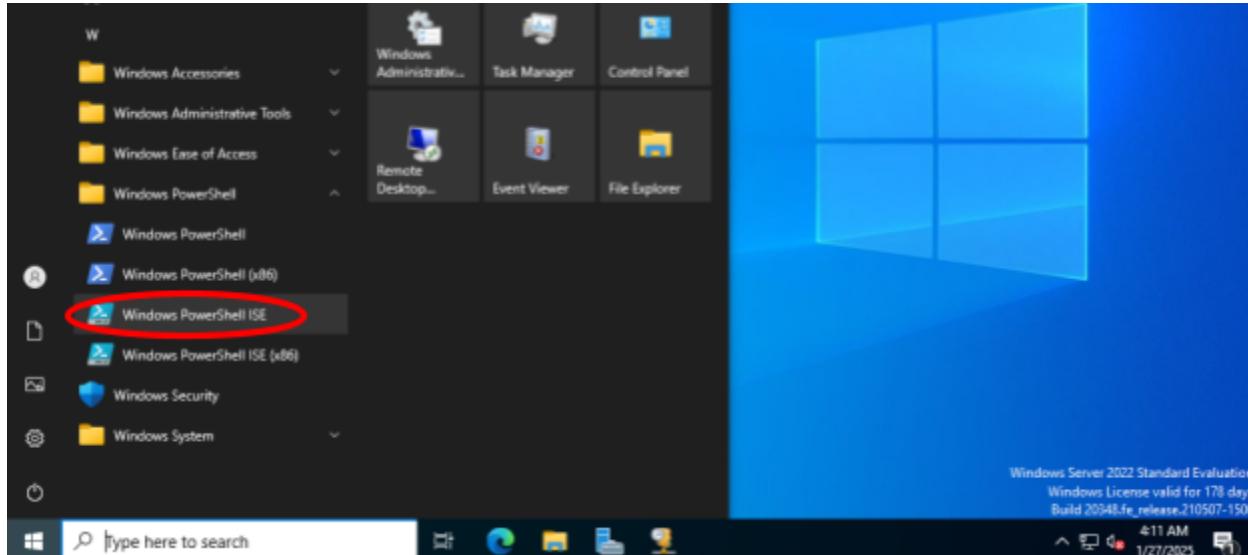
The screenshot shows the Windows Server Manager interface. The left navigation pane is open, showing options like Dashboard, Local Server (which is selected), All Servers, AD DS, DHCP, DNS, File and Storage Services, IIS, and Remote Access. The main content area displays the 'PROPERTIES' tab for the 'Local Server' (DomainController). It shows various system details such as Computer name (DomainController), Domain (mydomain.com), Microsoft Defender Firewall (Domain: On), and Microsoft Defender Antivirus (Real-Time Protection: On). The 'IE Enhanced Security Configuration' setting is highlighted with a red circle. Below this, the 'EVENTS' section shows a list of recent events, including errors related to Microsoft-Windows-DHCP-Server, Microsoft-Windows-DNS Client Events, and Microsoft-Windows-WMI.

Select Off for both the Administrators and Users. Click OK when finished.

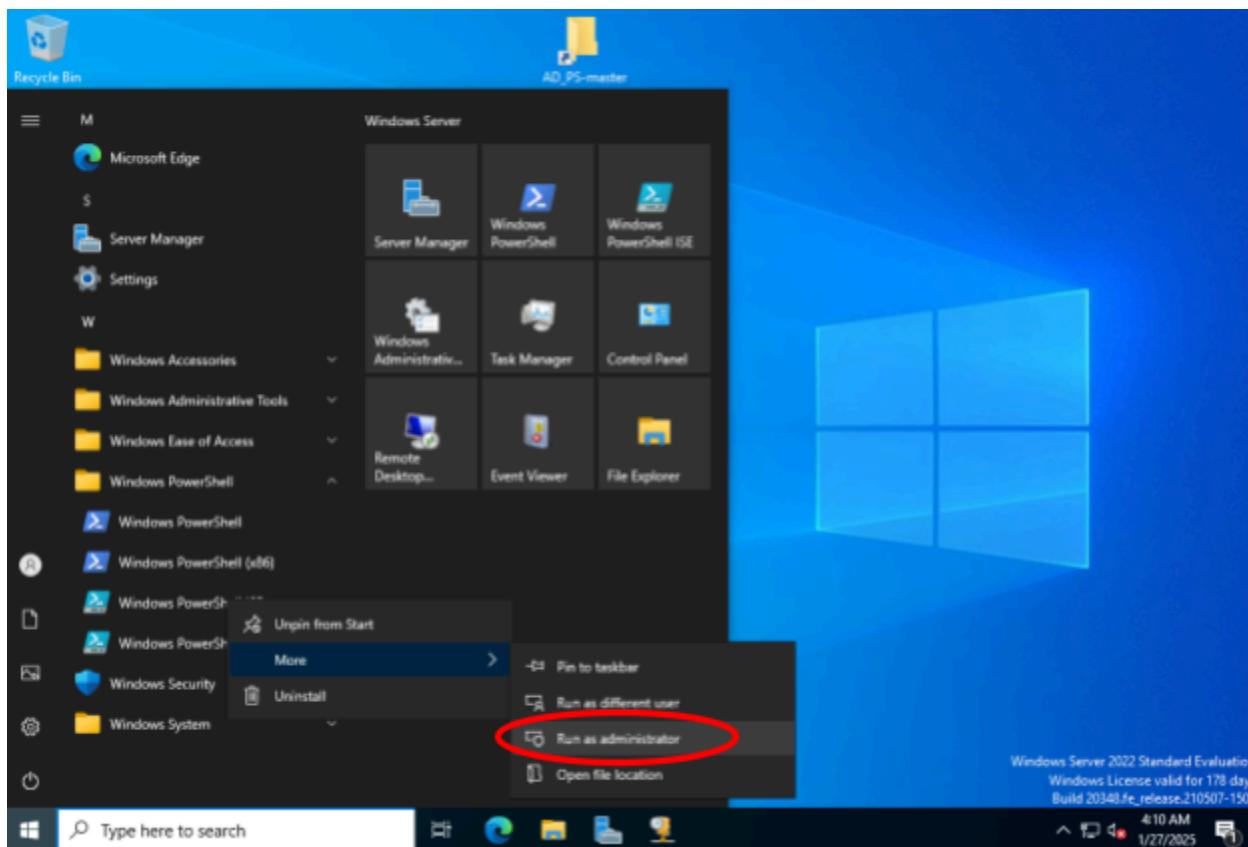




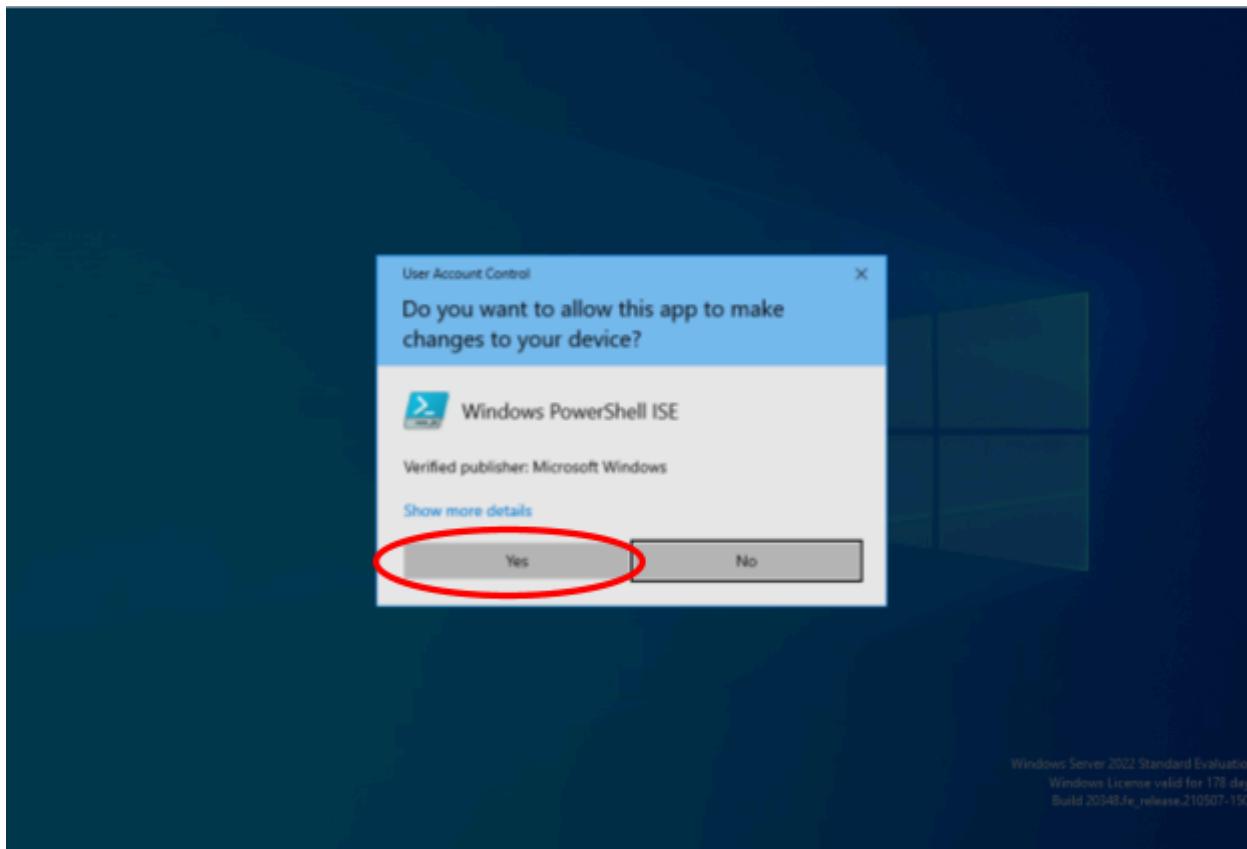
Once we've downloaded the Script Files, we will open up PowerShell
In the Start Menu, Right-Click on the Windows PowerShell ISE



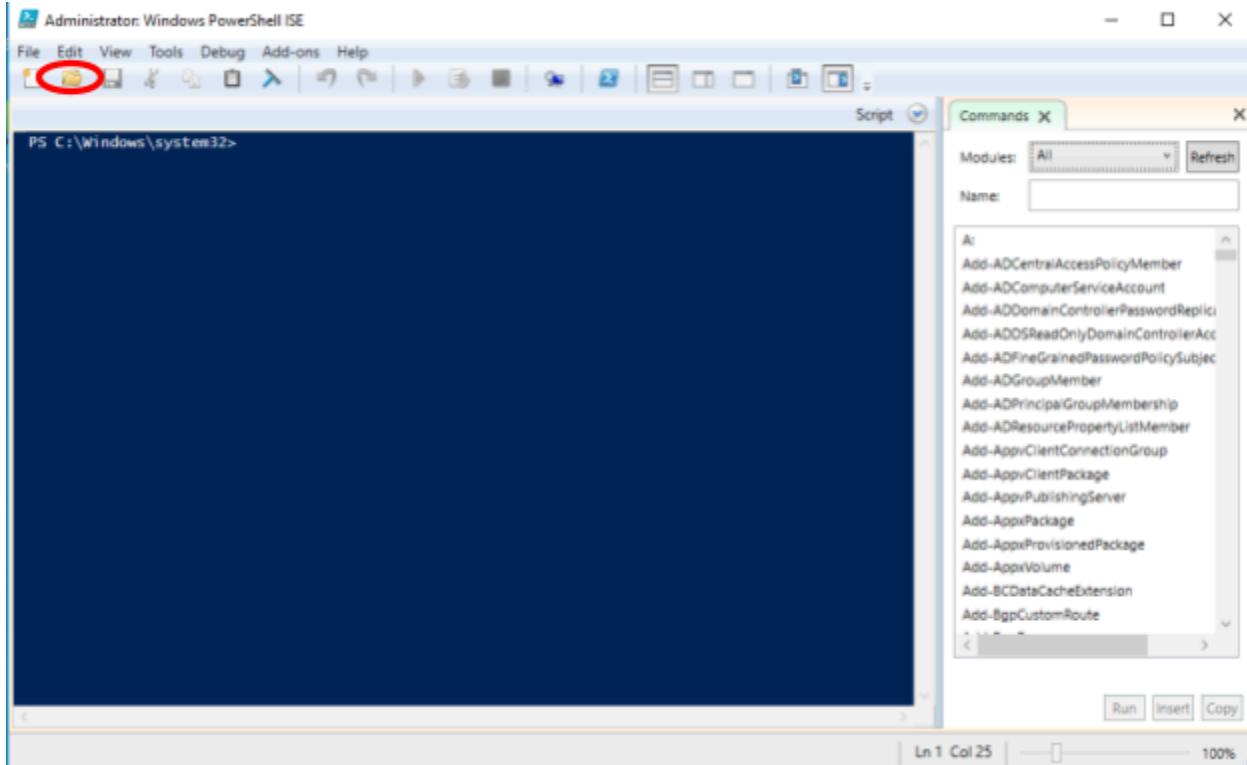
Select More and then select Run as Administrator



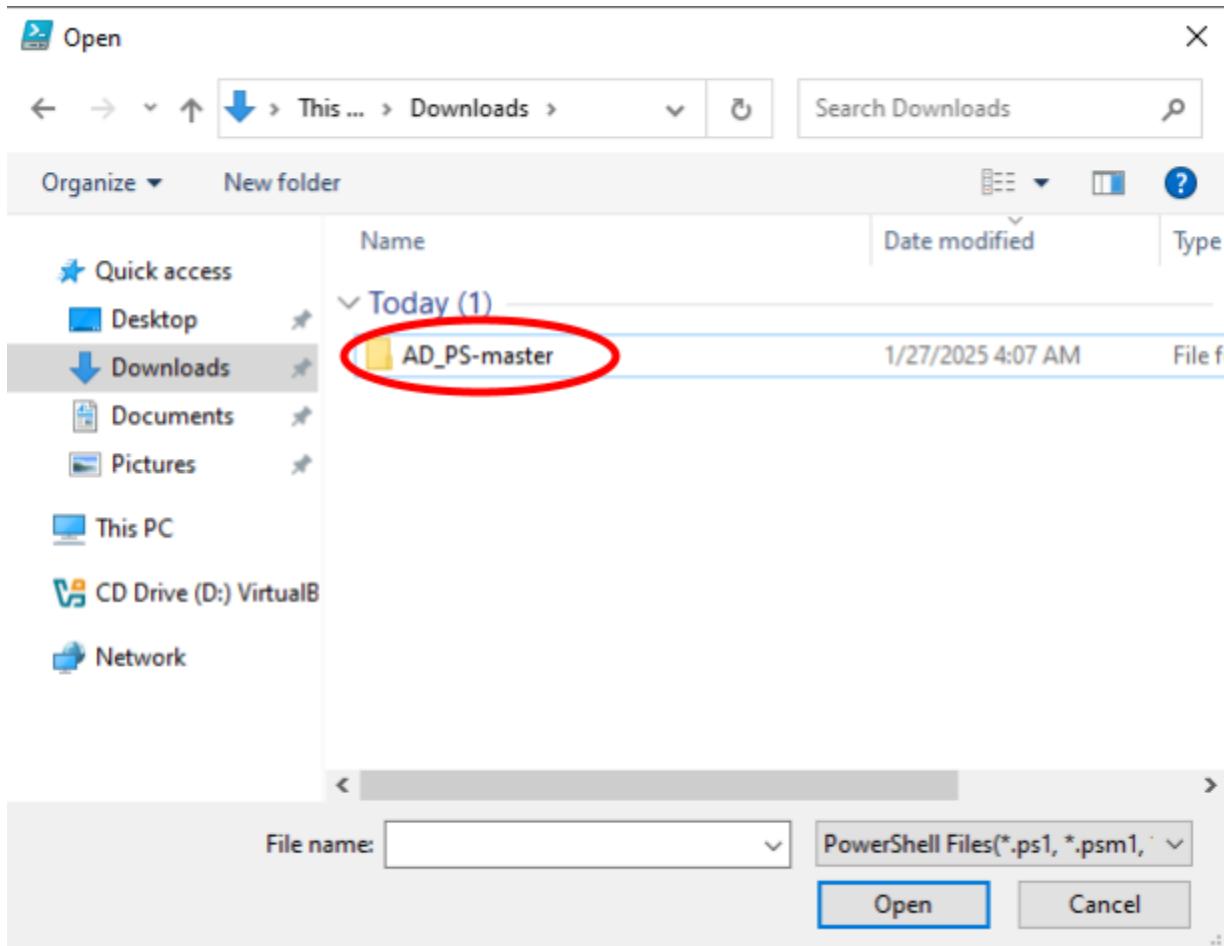
Select Yes



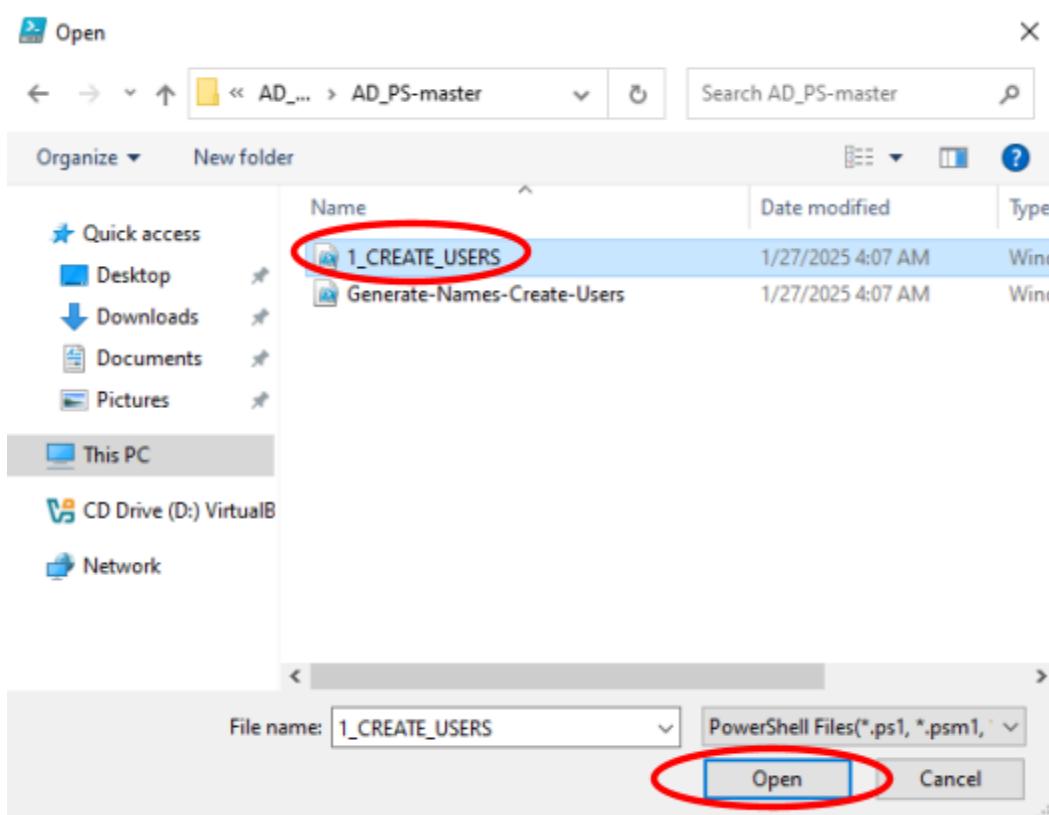
On the Top-Right Corner, select the Folder Icon for Open



Double Click to access the folder



Select 1_CREATE_USERS file and click Open



This should display the PowerShell Script.

It will create a Default Password for the users, create an Organizational Unit called _USERS, and run a foreach loop that will go through each name on the list of Users and split the First and Last Name according to the space that separates them, then add them to the OU called _USERS.

The screenshot shows the Windows PowerShell ISE interface. On the left, the script file '1_CREATE_USERS.ps1' is open, displaying PowerShell code. On the right, a 'Commands' pane is open, showing a list of available cmdlets. A red circle highlights the command 'Set-ExecutionPolicy Unrestricted' in the command history at the bottom of the ISE window.

```
1 # ----- Edit these Variables for your own Use Case ----- #
2 $PASSWORD_FOR_USERS = "Password1"
3 $USER_FIRST_LAST_LIST = Get-Content .\names.txt
4 # -----
5
6 $password = ConvertTo-SecureString $PASSWORD_FOR_USERS -AsPlainText -Force
7 New-ADOrganizationalUnit -Name _USERS -ProtectedFromAccidentalDeletion $false
8
9 foreach ($n in $USER_FIRST_LAST_LIST) {
10     $first = $n.Split(" ")[0].ToLower()
11     $last = $n.Split(" ")[1].ToLower()
12     $username = $($first.Substring(0,1))$($last).ToLower()
13     Write-Host "Creating user: $($username)" -BackgroundColor Black -ForegroundColor Cyan
14
15     New-AdUser -AccountPassword $password `
16                 -GivenName $first `
17                 -Surname $last `
18                 -DisplayName $username `
19                 -Name $username `
20                 -EmployeeID $username `
21                 -PasswordNeverExpires $true `
22                 -Path "ou=_USERS,$([ADSI]::Get("").distinguishedName)" `
23                 -Enabled $true
24 }
```

To run this script, since it is in a lab environment, we will run a command:
Set-ExecutionPolicy Unrestricted

The screenshot shows the Windows PowerShell ISE interface. The script '1_CREATE_USERS.ps1' is open on the left. A red circle highlights the command 'Set-ExecutionPolicy Unrestricted' in the command history at the bottom of the ISE window.

```
1 # ----- Edit these Variables for your own Use Case ----- #
2 $PASSWORD_FOR_USERS = "Password1"
3 $USER_FIRST_LAST_LIST = Get-Content .\names.txt
4 # -----
5
6 $password = ConvertTo-SecureString $PASSWORD_FOR_USERS -AsPlainText -Force
7 New-ADOrganizationalUnit -Name _USERS -ProtectedFromAccidentalDeletion $false
8
9 foreach ($n in $USER_FIRST_LAST_LIST) {
10     $first = $n.Split(" ")[0].ToLower()
11     $last = $n.Split(" ")[1].ToLower()
12     $username = $($first.Substring(0,1))$($last).ToLower()
13     Write-Host "Creating user: $($username)" -BackgroundColor Black -ForegroundColor Cyan
14
15     New-AdUser -AccountPassword $password `
16                 -GivenName $first `
17                 -Surname $last `
18                 -DisplayName $username `
19                 -Name $username `
20                 -EmployeeID $username `
21                 -PasswordNeverExpires $true `
22                 -Path "ou=_USERS,$([ADSI]::Get("").distinguishedName)" `
23                 -Enabled $true
24 }
```

Click “Yes to All”

The screenshot shows a Windows PowerShell ISE window with a script named `1_CREATE_USERS.ps1`. Below the script, a command `Set-ExecutionPolicy Unrestricted` is run in the PowerShell window. A modal dialog box titled "Execution Policy Change" is displayed, asking if the user wants to change the execution policy. The "Yes to All" button is highlighted with a red circle.

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
1_CREATE_USERS.ps1 X
1 # ----- Edit these Variables for your own Use Case ----- #
2 $PASSWORD_FOR_USERS = "Password1"
3 $USER_FIRST_LAST_LIST = Get-Content .\names.txt
4 # -----
5
6 $password = ConvertTo-SecureString $PASSWORD_FOR_USERS -AsPlainText -Force
7 New-ADOrganizationalUnit -Name _USERS -ProtectedFromAccidentalDeletion $false
8
9 foreach ($n in $USER_FIRST_LAST_LIST) {
10     $first = $n.Split(" ")[0].ToLower()
11     $last = $n.Split(" ")[1].ToLower()
12     $username = $($first.Substring(0,1))$($last).ToLower()
13     Write-Host "Creating user: $username" -BackgroundColor Black -ForegroundColor Cyan
14
15     New-AdUser -AccountPassword $password `
16                 -GivenName $first `
17                 -Surname $last `
18                 -DisplayName $username `
19                 -Name $username `
20                 -EmployeeID $username `
21                 -PasswordNeverExpires $true `
22                 -Path "ou=_USERS,$([ADSI]::").distinguishedName)" `
23                 -Enabled $true
24 }

PS C:\Windows\system32> Set-ExecutionPolicy Unrestricted

The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose you to the security risks described in the about_Execution_Policies help topic at https://go.microsoft.com/fwlink/?LinkId=135170. Do you want to change the execution policy?

[Yes] [Yes to All] [No] [No to All] [Suspend]
```

PS C:\Windows\system32> |

The screenshot shows the same Windows PowerShell ISE window after the execution policy change. The script has been run, and the output shows the creation of users. The status bar at the bottom indicates "Completed".

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
1_CREATE_USERS.ps1 X
1 # ----- Edit these Variables for your own Use Case ----- #
2 $PASSWORD_FOR_USERS = "Password1"
3 $USER_FIRST_LAST_LIST = Get-Content .\names.txt
4 # -----
5
6 $password = ConvertTo-SecureString $PASSWORD_FOR_USERS -AsPlainText -Force
7 New-ADOrganizationalUnit -Name _USERS -ProtectedFromAccidentalDeletion $false
8
9 foreach ($n in $USER_FIRST_LAST_LIST) {
10     $first = $n.Split(" ")[0].ToLower()
11     $last = $n.Split(" ")[1].ToLower()
12     $username = $($first.Substring(0,1))$($last).ToLower()
13     Write-Host "Creating user: $username" -BackgroundColor Black -ForegroundColor Cyan
14
15     New-AdUser -AccountPassword $password `
16                 -GivenName $first `
17                 -Surname $last `
18                 -DisplayName $username `
19                 -Name $username `
20                 -EmployeeID $username `
21                 -PasswordNeverExpires $true `
22                 -Path "ou=_USERS,$([ADSI]::").distinguishedName)" `
23                 -Enabled $true
24 }

PS C:\Windows\system32> Set-ExecutionPolicy Unrestricted

PS C:\Windows\system32> |

Completed
```

To run the script, we must navigate to the directory the script file is in

Administrator: Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

1_CREATE_USERS.ps1 X

```
1 # ----- Edit these Variables for your own Use Case ----- #
2 $PASSWORD_FOR_USERS = "Password1"
3 $USER_FIRST_LAST_LIST = Get-Content .\names.txt
4 # ----- #
5
6 $password = ConvertTo-SecureString $PASSWORD_FOR_USERS -AsPlainText -Force
7 New-ADOrganizationalUnit -Name _USERS -ProtectedFromAccidentalDeletion $false
8
9 foreach ($n in $USER_FIRST_LAST_LIST) {
10     $first = $n.Split(" ")[0].ToLower()
11     $last = $n.Split(" ")[1].ToLower()
12     $username = $($first.Substring(0,1))$($last).ToLower()
13     Write-Host "Creating user: $($username)" -BackgroundColor Black -ForegroundColor Cyan
14
15     New-AdUser -AccountPassword $password
16         -GivenName $first
17         -Surname $last
18         -DisplayName $username
19         -Name $username
20         -EmployeeID $username
21         -PasswordNeverExpires $true
22         -Path "ou=_USERS,$([ADSI]'').distinguishedName"
23         -Enabled $true
24 }
```

-a--- 5/8/2021 2:14 AM 102400 zipcontainer.dll
-a--- 5/8/2021 2:14 AM 315392 zipfldr.dll
-a--- 5/8/2021 2:14 AM 53248 ztrace_maps.dll

PS C:\Windows\system32> cd C:\Users\a-atuguinay\Downloads\AD_PS-master

Use the ls command to display the files in this directory.
Here, we find the names.txt file that the script will pull from.

Administrator: Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

1_CREATE_USERS.ps1 X

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

PS C:\Users\a-atuguinay\Downloads\AD_PS-master> ls

Directory: C:\Users\a-atuguinay\Downloads\AD_PS-master\AD_PS-master

Mode	LastWriteTime	Length	Name
----	-----	---	---
-a---	1/27/2025 4:07 AM	1811	.gitignore
-a---	1/27/2025 4:07 AM	1025	1_CREATE_USERS.ps1
-a---	1/27/2025 4:07 AM	1532	Generate-Names-Create-Users.ps1
-a---	1/27/2025 4:08 AM	15587	names.txt

Completed | Ln 4269 Col 62 | 100%

Now, we can click the Green Play Icon on the top of the window to run the script

Click the Run once button

The screenshot shows the Windows PowerShell ISE interface. The title bar reads "Administrator: Windows PowerShell ISE". The menu bar includes File, Edit, View, Tools, Debug, Add-ons, Help. The toolbar has icons for New, Open, Save, Run Script (F5), and others. The main code editor window contains a PowerShell script named "1_CREATE_USERS.ps1" with the following content:

```
1 # ----- Edit these Variables for your own Use Case ----- #
2 $PASSWORD_FOR_USERS = "Password1"
3 $USER_FIRST_LAST_LIST = Get-Content .\names.txt
4 # -----
5
6 $password = ConvertTo-SecureString $PASSWORD_FOR_USERS -AsPlainText -Force
7 New-ADOrganizationalUnit -Name „USERS“ -ProtectedFromAccidentalDeletion $false
8
9 foreach ($n in $USER_FIRST_LAST_LIST) {
10     $First = $n.Split(" ")[0].ToLower()
11     $Last = $n.Split(" ")[1].ToLower()}
```

A "Security warning" dialog box is displayed over the script, stating: "Run only scripts that from the internet can be useful, this script can potentially harm your computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning message. Do you want to run C:\Users\atuguinay\Downloads\AD_PS-master\AD_PS-master\1_CREATE_USERS.ps1?". The "Run once" button is highlighted with a red circle.

The PowerShell session output window shows the execution of the script:

```
-a--- 1/27/2025 4:07 AM 1025 1_CREATE_USERS.ps1
-a--- 1/27/2025 4:07 AM 1532 Generate-Names-Create-Users.ps1
-a--- 1/27/2025 4:08 AM 15587 names.txt
```

The command entered in the PowerShell prompt is: PS C:\Users\atuguinay\Downloads\AD_PS-master\AD_PS-master> C:\Users\atuguinay\Downloads\AD_PS-master\AD_PS-master\1_CREATE_USERS.ps1

At the bottom, status information includes: Running script / selection. Press Ctrl+Break to stop. Press Ctrl+B to break into debugger. Line 4270 Col 1. 100%. Windows Server 2022 Standard Evaluation. Windows License valid for 178 days. Build 20348.64_release.210507-1500.

Give PowerShell time to run the script. It is adding one thousand users after all.

The screenshot shows the Windows PowerShell ISE interface with the title bar "Administrator: Windows PowerShell ISE". The menu bar includes File, Edit, View, Tools, Debug, Add-ons, and Help. The toolbar contains various icons for file operations. A tab labeled "1_CREATE_USERS.ps1" is open. The code in the editor is as follows:

```
1 # ----- Edit these Variables for your own Use Case ----- #
2 $PASSWORD_FOR_USERS = "Password1"
3 $USER_FIRST_LAST_LIST = Get-Content .\names.txt
4 # -----
5
6 $password = ConvertTo-SecureString $PASSWORD_FOR_USERS -AsPlainText -Force
7 New-ADOrganizationalUnit -Name _USERS -ProtectedFromAccidentalDeletion $false
8
9 foreach ($n in $USER_FIRST_LAST_LIST) {
10     $first = $n.Split(" ")[0].ToLower()
11     $last = $n.Split(" ")[1].ToLower()
12     $username = $($first.Substring(0,1))$($last).ToLower()
13     Write-Host "Creating user: $($username)" -BackgroundColor Black -ForegroundColor Cyan
14
15     New-AdUser -AccountPassword $password `
16                 -GivenName $first `
17                 -Surname $last `
18                 -Enabled $true `
19
20
21 Creating user: lvanepps
22 Creating user: vkay
23 Creating user: dwain
24 Creating user: clux
25 Creating user: dbaham
26 Creating user: sdrews
27 Creating user: jcastaneda
28 Creating user: rrolls
29 Creating user: sschooley
30 Creating user: jhohlt
31 Creating user: wbumgarner
32 Creating user: mfulow
33 Creating user: bmcloughlin
34 Creating user: sbirden
35 Creating user: wpothier
```

The output window shows the progress of user creation, with each user being printed in cyan text on a black background. The status bar at the bottom indicates "Running script / selection. Press Ctrl+Break to stop. Press Ctrl+B to break into debugger." and "Ln 4348 Col 1 100%".

The screenshot shows the Windows PowerShell ISE interface with the title bar "Administrator: Windows PowerShell ISE". The menu bar includes File, Edit, View, Tools, Debug, Add-ons, and Help. The toolbar contains various icons for file operations. A tab labeled "1_CREATE_USERS.ps1" is open. The code in the editor is identical to the first screenshot.

```
1 # ----- Edit these Variables for your own Use Case ----- #
2 $PASSWORD_FOR_USERS = "Password1"
3 $USER_FIRST_LAST_LIST = Get-Content .\names.txt
4 # -----
5
6 $password = ConvertTo-SecureString $PASSWORD_FOR_USERS -AsPlainText -Force
7 New-ADOrganizationalUnit -Name _USERS -ProtectedFromAccidentalDeletion $false
8
9 foreach ($n in $USER_FIRST_LAST_LIST) {
10     $first = $n.Split(" ")[0].ToLower()
11     $last = $n.Split(" ")[1].ToLower()
12     $username = $($first.Substring(0,1))$($last).ToLower()
13     Write-Host "Creating user: $($username)" -BackgroundColor Black -ForegroundColor Cyan
14
15     New-AdUser -AccountPassword $password `
16                 -GivenName $first `
17                 -Surname $last `
18                 -Enabled $true `
19
20
21 Creating user: mchestnut
22 Creating user: nlefrevre
23 Creating user: cwestover
24 Creating user: vezzell
25 Creating user: dannunziata
26 Creating user: smitschke
27 Creating user: kmarden
28 Creating user: mraper
29 Creating user: dwillmore
30 Creating user: tbasilio
31 Creating user: bgilmer
32 Creating user: cconboy
33 Creating user: mhakes
34 Creating user: arettig
```

The output window shows the progress of user creation, with each user being printed in cyan text on a black background. The status bar at the bottom indicates "PS C:\Users\atuguinay\Downloads\AD_PS-master\AD_PS-master>" and "Completed".

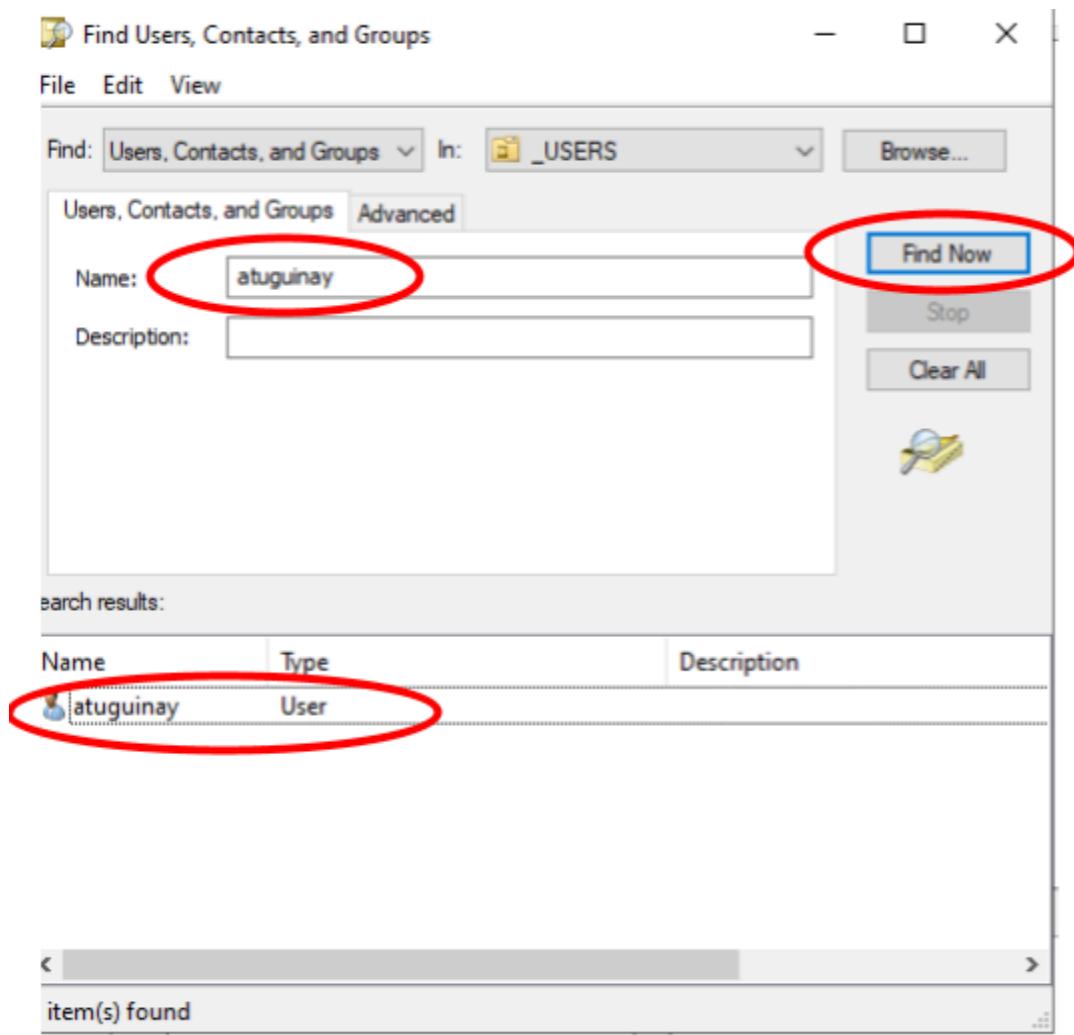
Once completed, we can navigate back to the Active Directory Users and Computers to check if the _USERS OU was added and populated with the users from the names.txt. We added our name in there too so that we know for sure all the names were added.

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, the navigation pane displays the domain structure under 'mydomain.com': Active Directory Users and Computers, Saved Queries, mydomain.com (expanded), _USERS (selected), ADMINS, Builtin, Computers, Domain Controllers, ForeignSecurityPrincipal:, Managed Service Account, and Users. The main pane lists users under the _USERS container. The columns are Name, Type, and Description. The list includes: aabrev, aacre, abargo, abilderback, abirk, ablackwater, ablaker, abonavita, abreelove, aburtt, acarron, acastleberry, acoke, acosey, adandrea, adeguzman, ademello, adove, aebinger, afasching, and afegan. All entries are of type 'User'.

We can Right-Click on the Domain name and select Find

The screenshot shows the same Active Directory Users and Computers interface. A context menu is open over the 'mydomain.com' entry in the navigation pane. The menu options include: Delegate Control..., Find..., Change Domain..., Change Domain Controller..., Raise domain functional level..., Operations Masters..., New, All Tasks, Refresh, Properties, and Help. The 'Find...' option is highlighted with a red circle.

We will type our account name and click Find Now

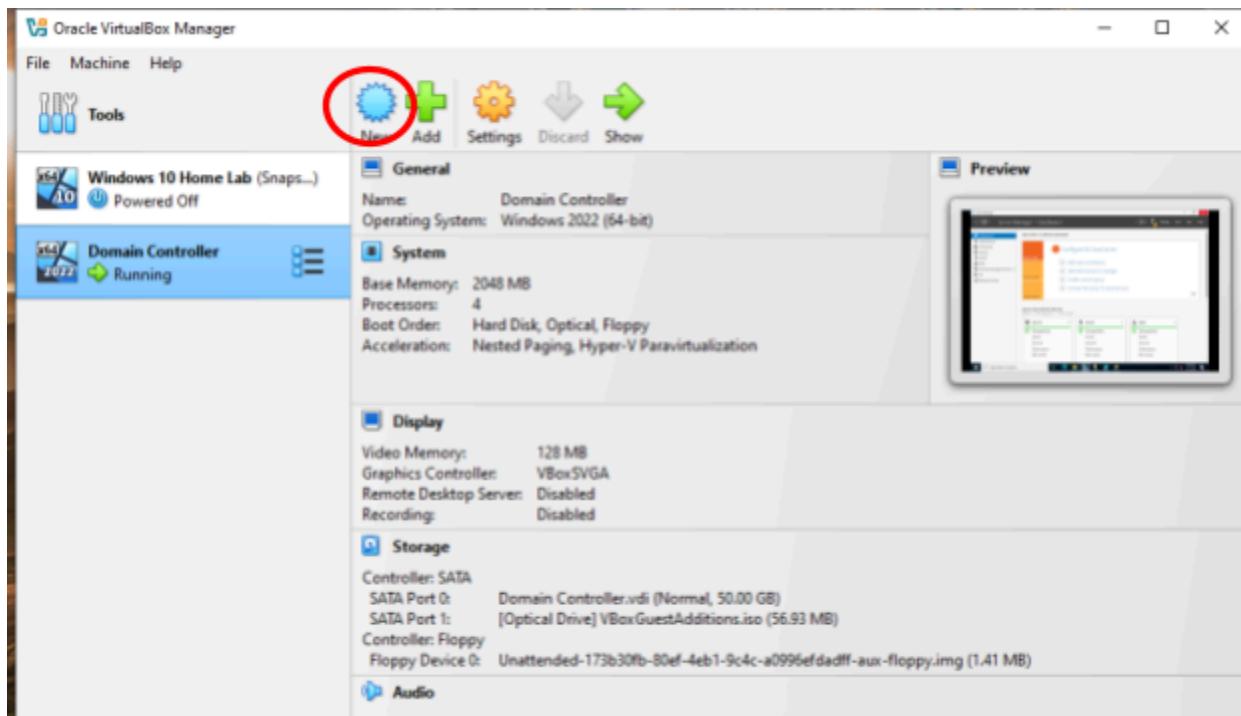


Our name was displayed, which means the adding of users from the text file using the PowerShell script was a success.

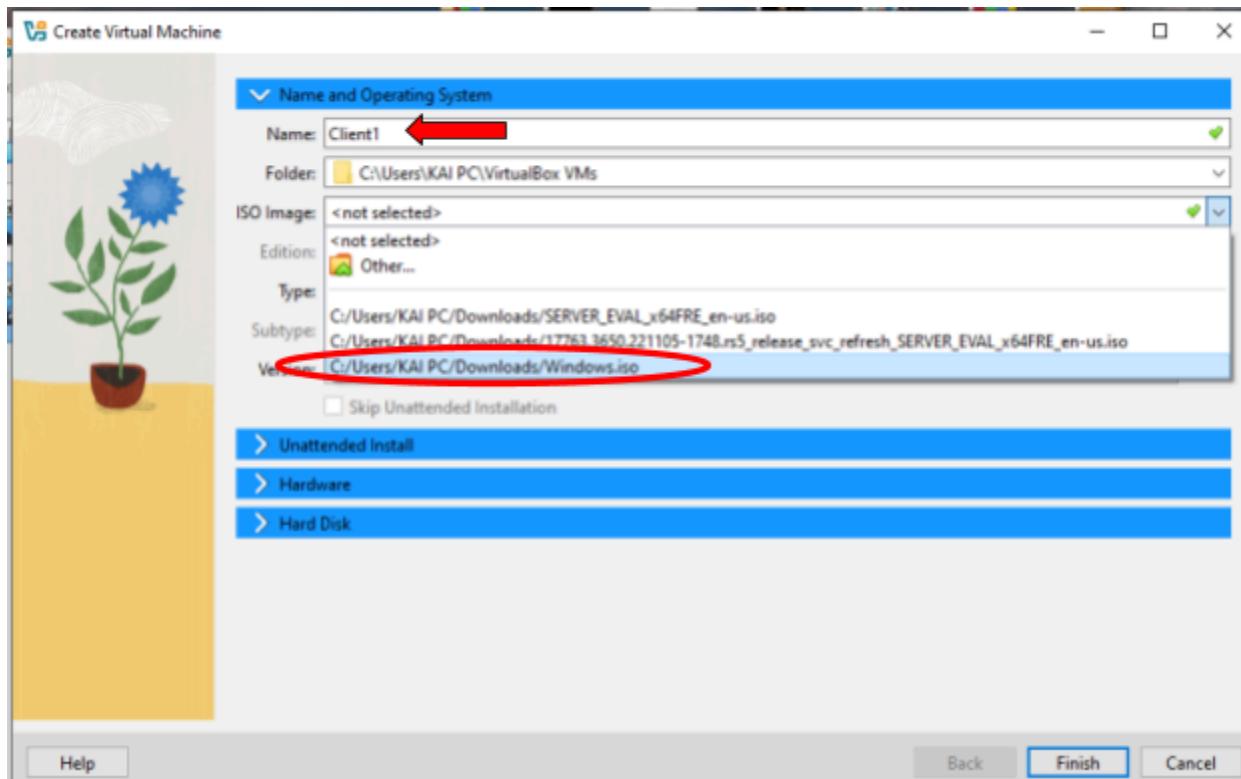
Step 10: Set up a Client virtual machine that will connect to the Domain Controller

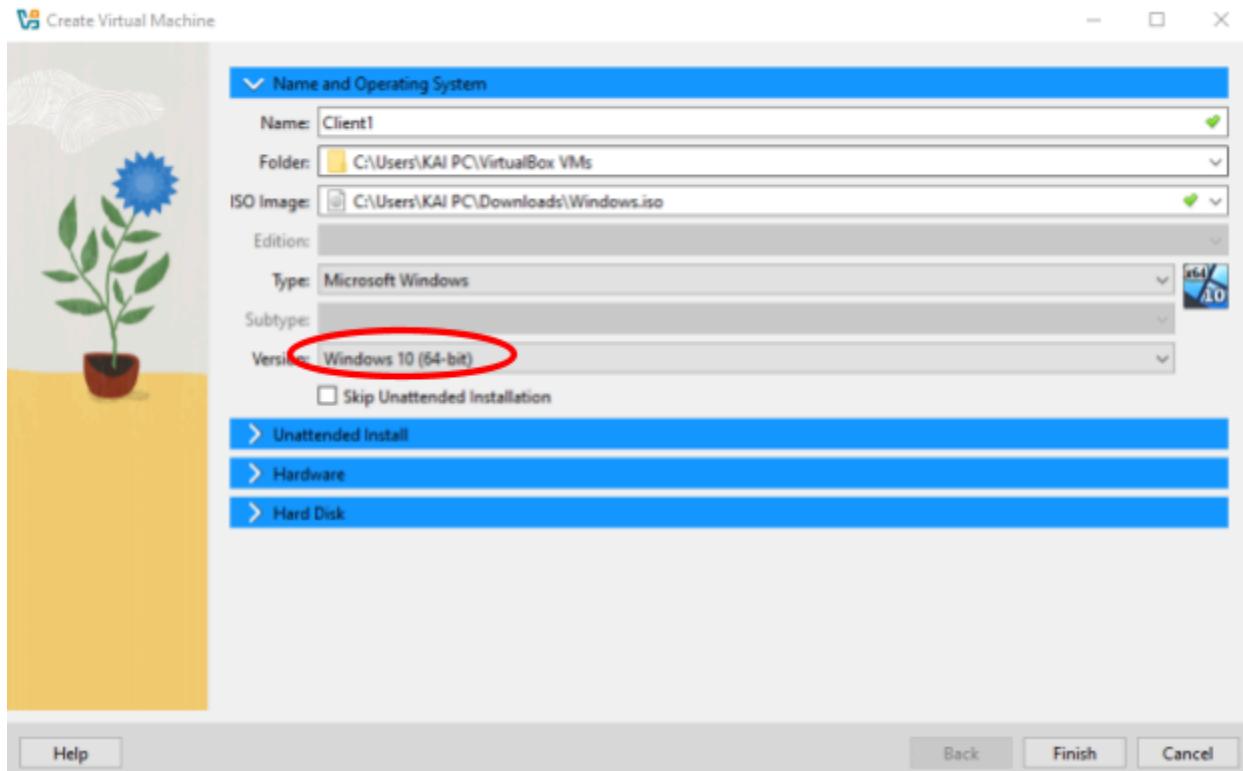
We will begin by going back to the VirtualBox Manager

Click New

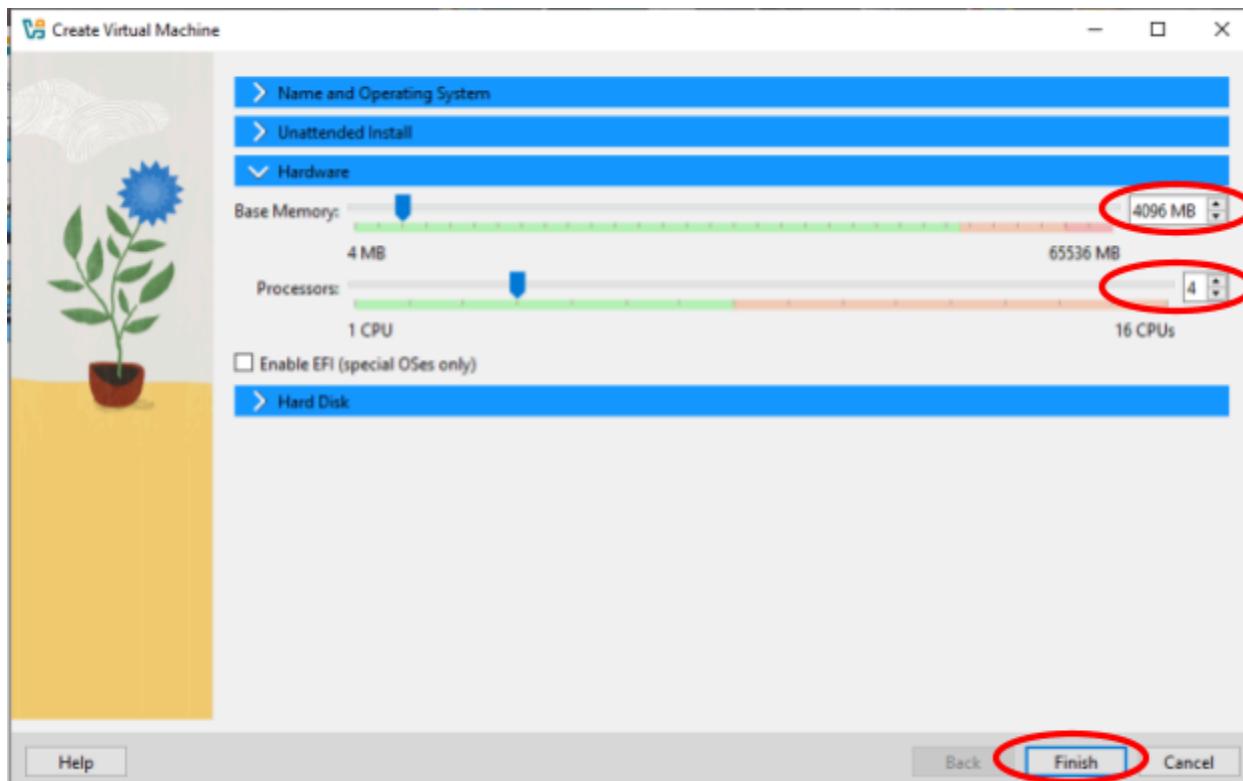


Name the Machine Client1 and select the Windows 10 ISO we downloaded in the beginning of the Document

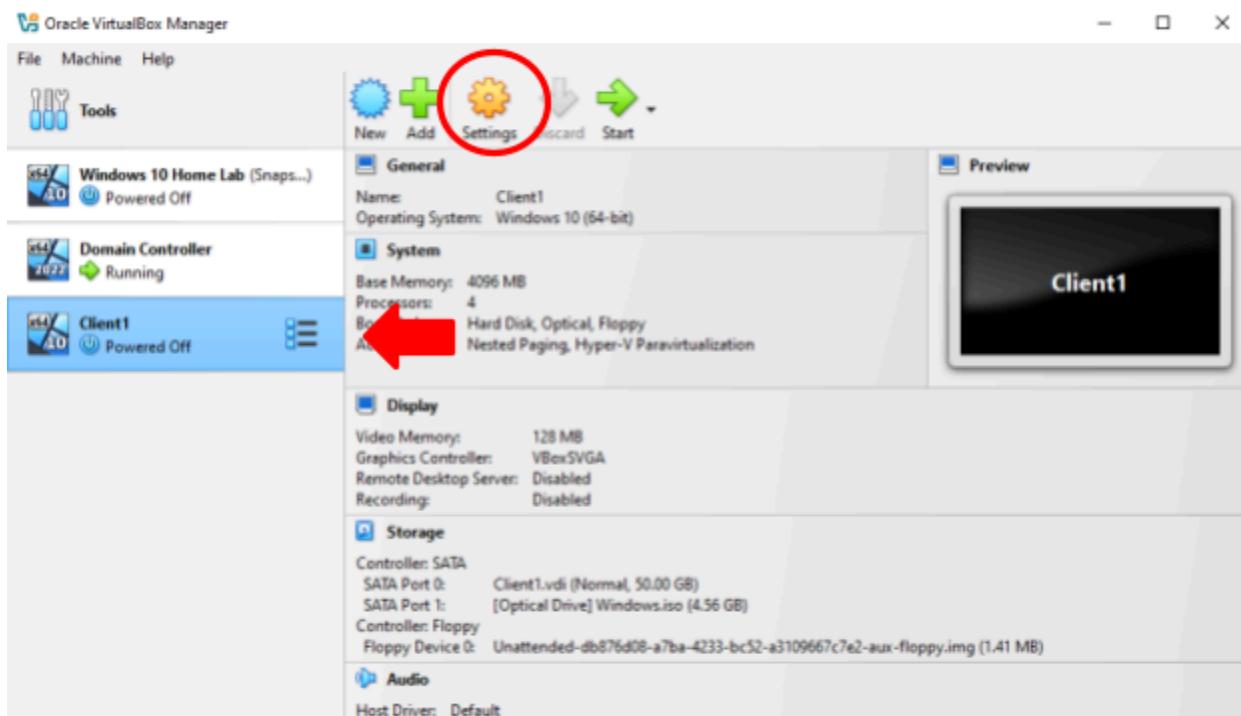




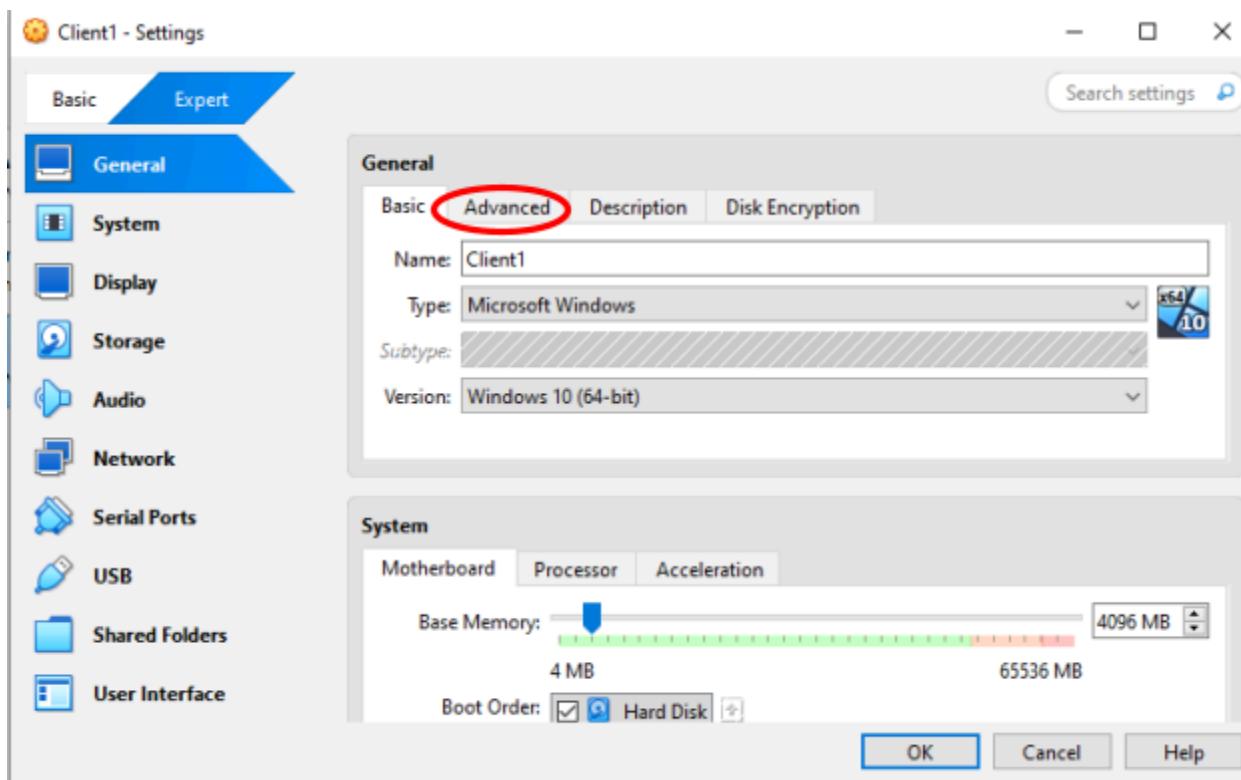
Navigate to the Hardware tab and add 4 GB of RAM and 4 processors. Click finish



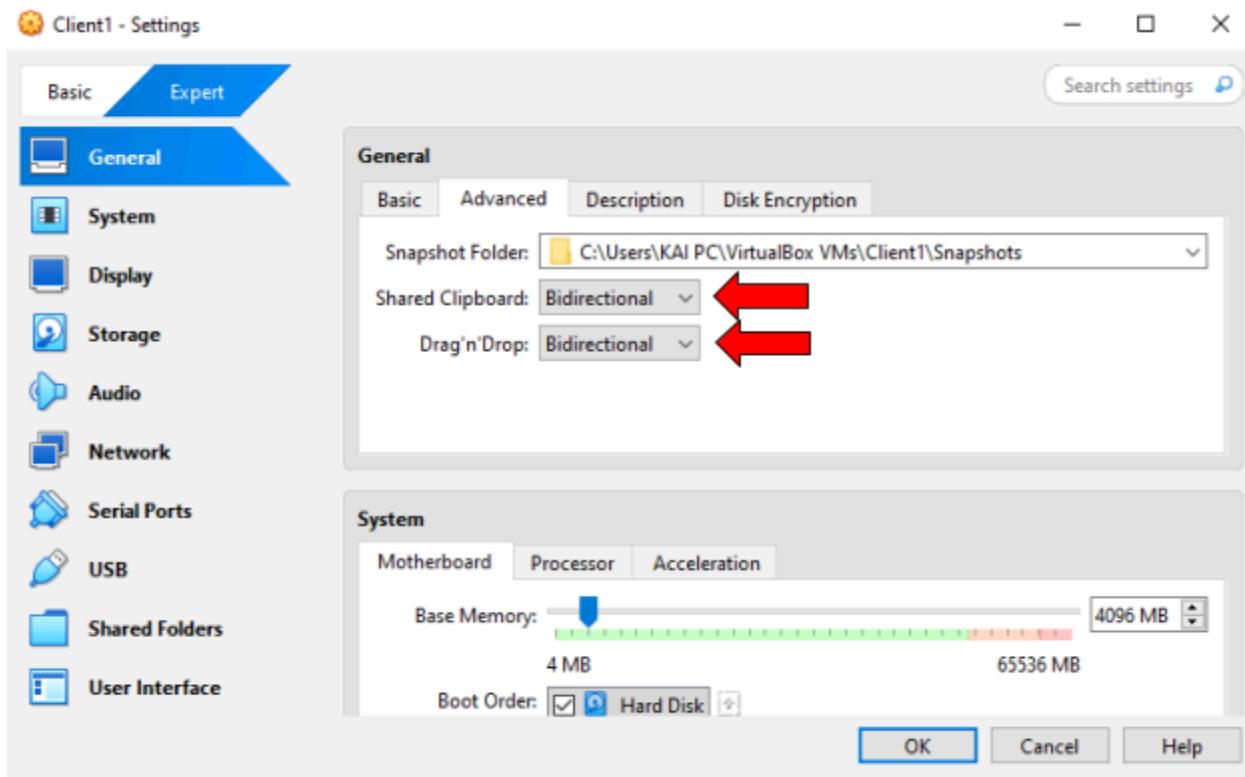
Just like last time, before we power up Client1, we must configure the settings. Select Client1 and click on Settings



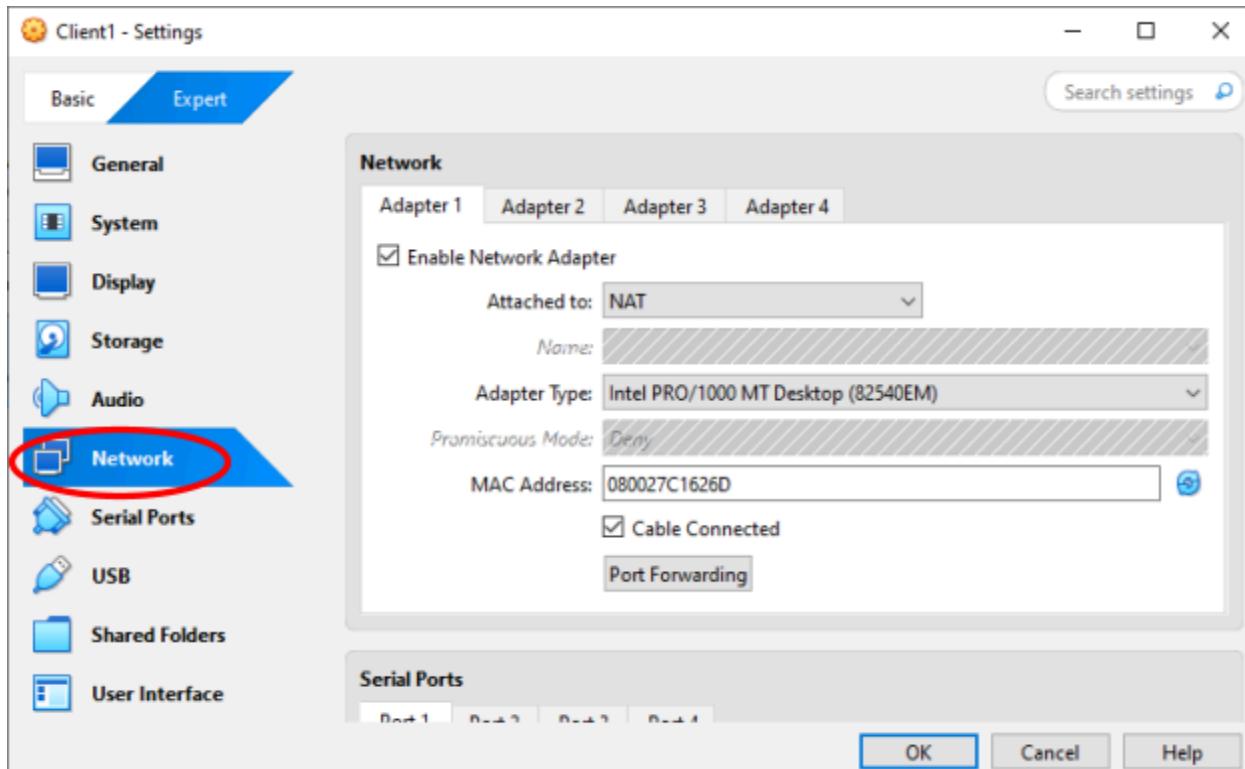
Click on Advanced in General tab



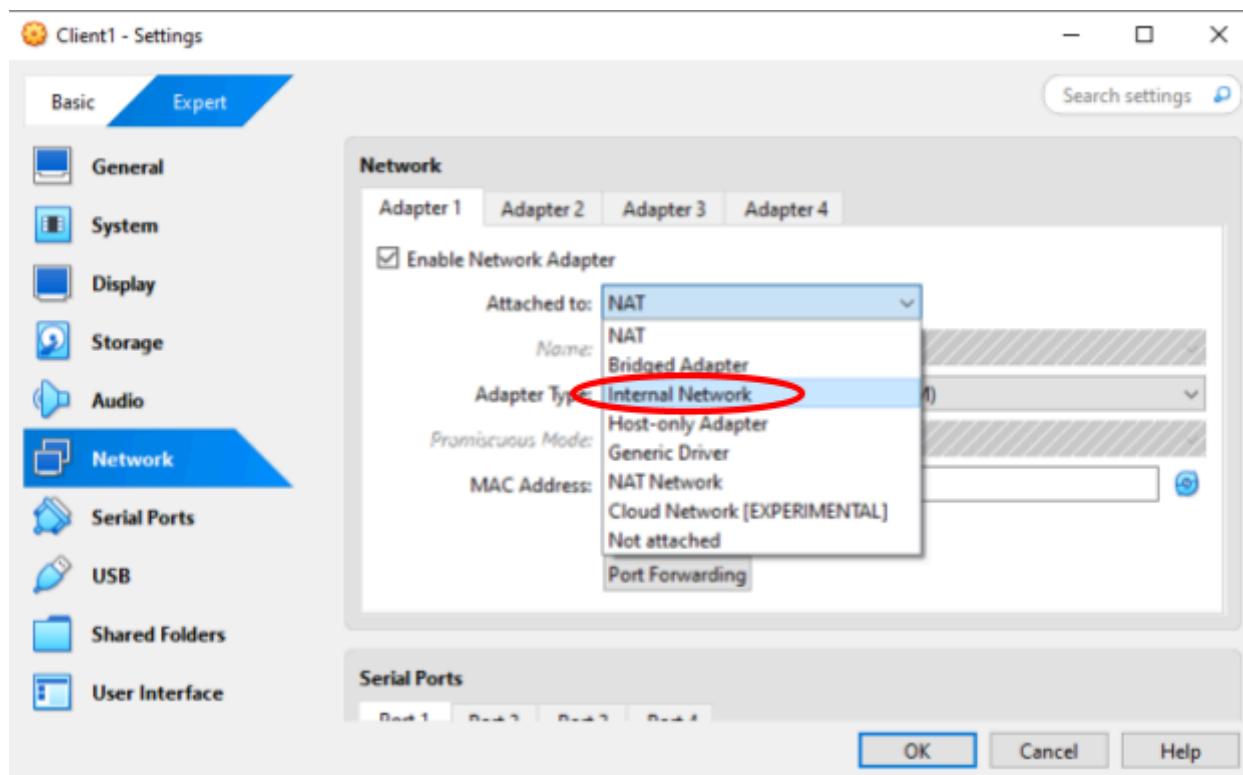
Change the Shared Clipboard and Drag'n'Drop to Bidirectional



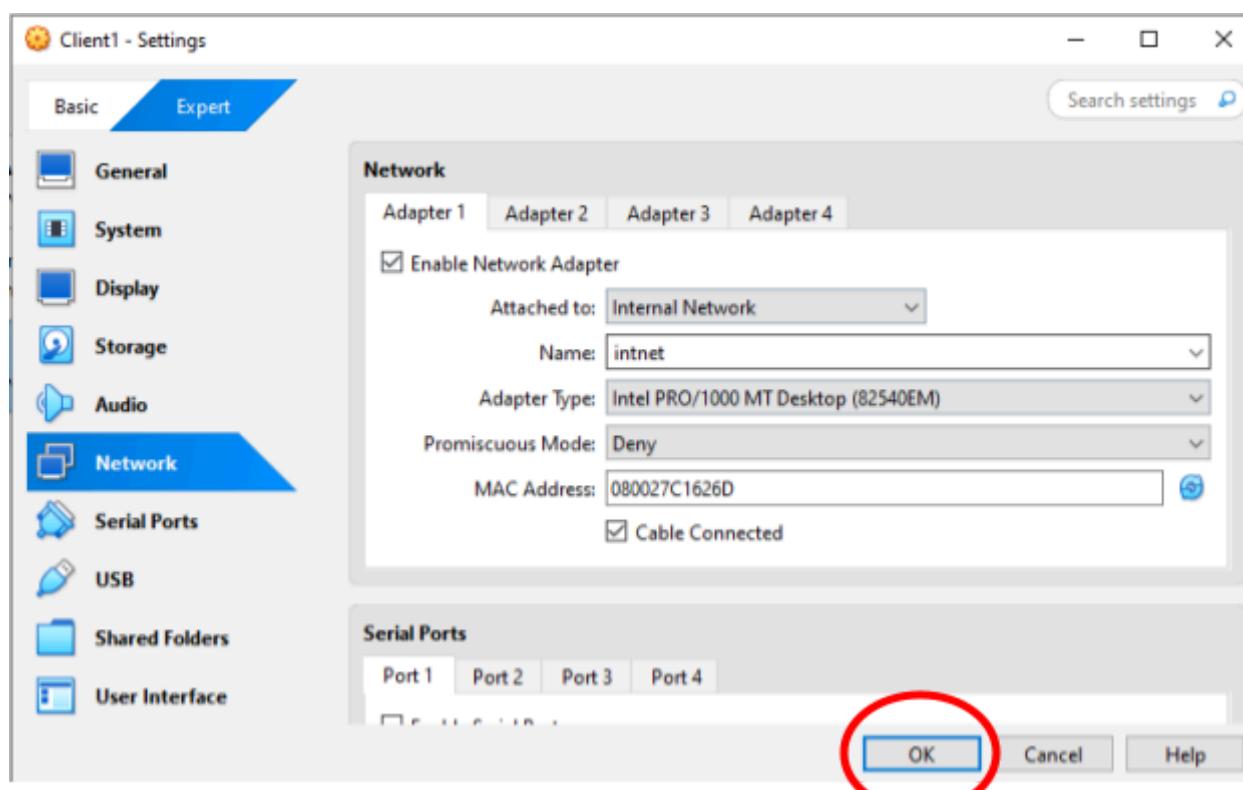
Navigate to the Network Tab



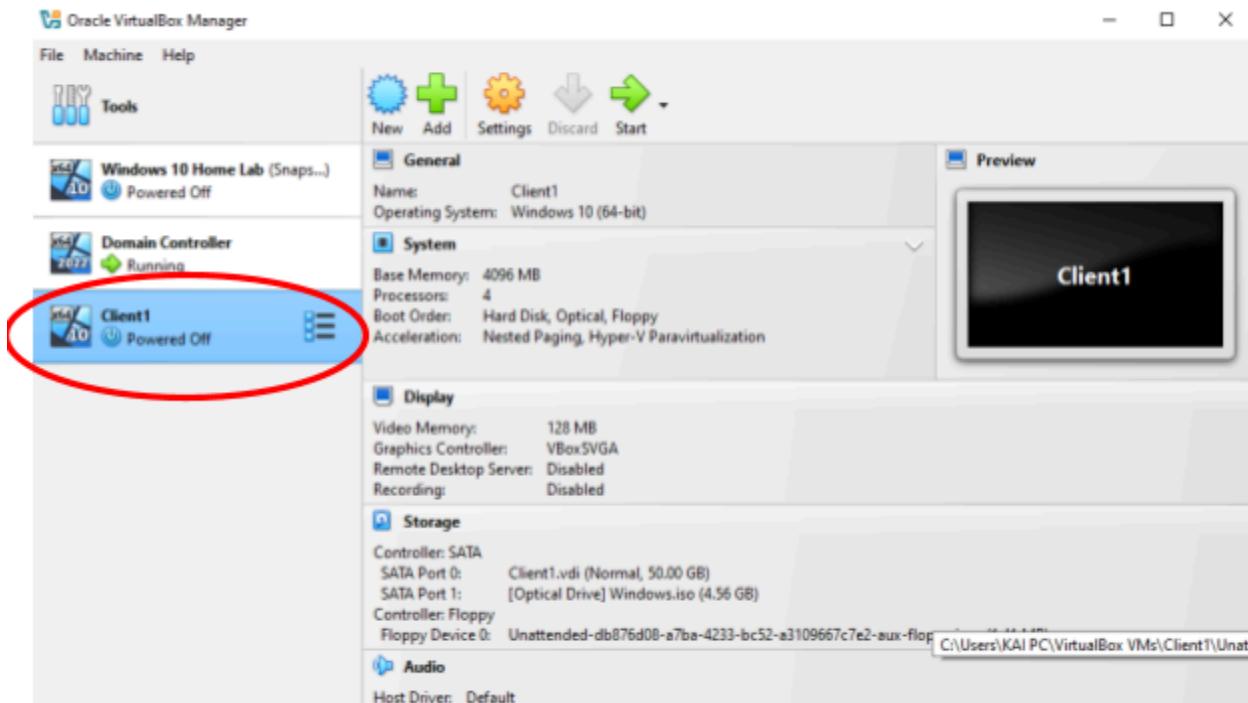
Change the Adapter 1 from NAT to Internal Network. This is to ensure that the Client1 Machine will connect to the Domain Controller and use it as the Default Gateway to connect to the Internet.



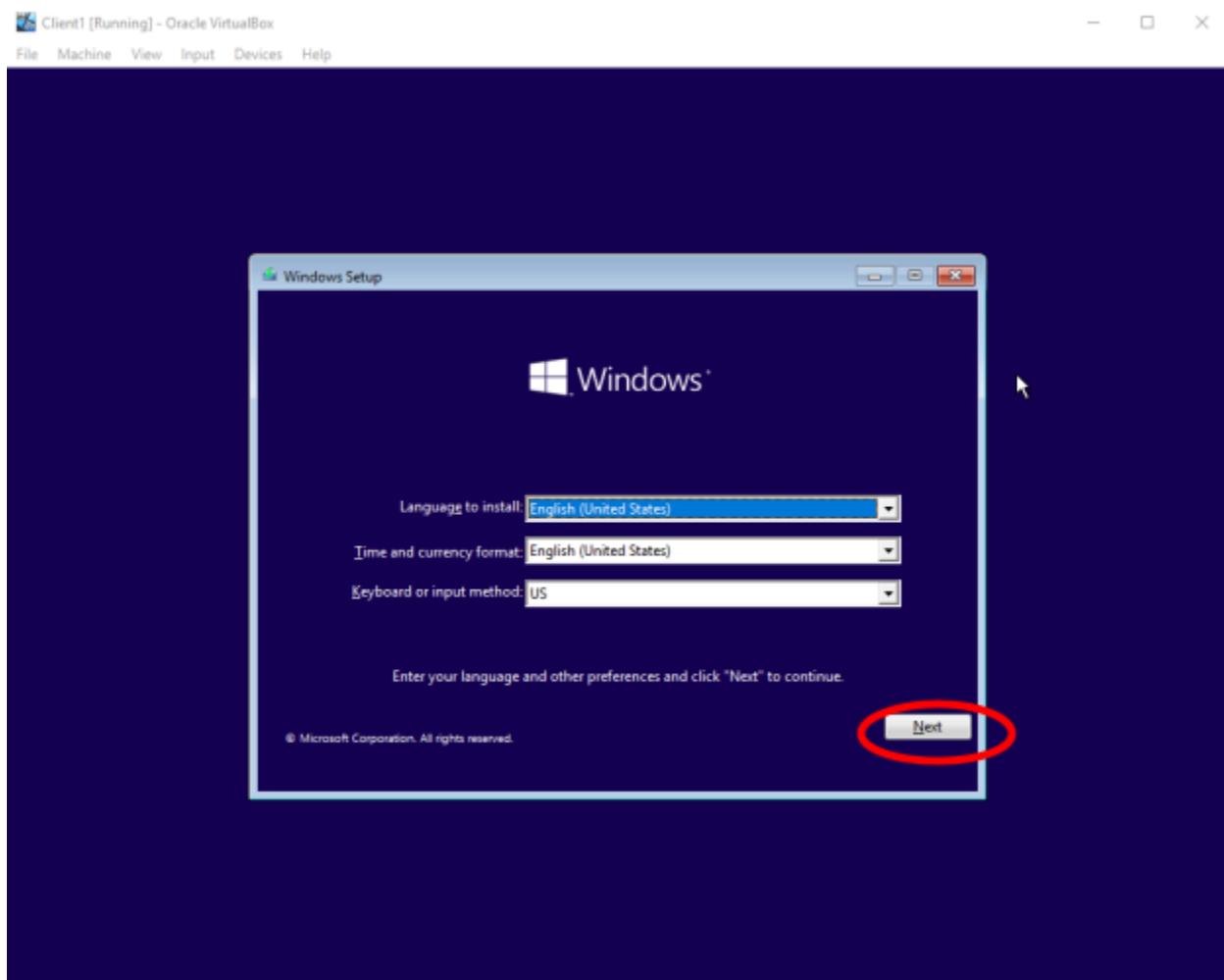
Click OK



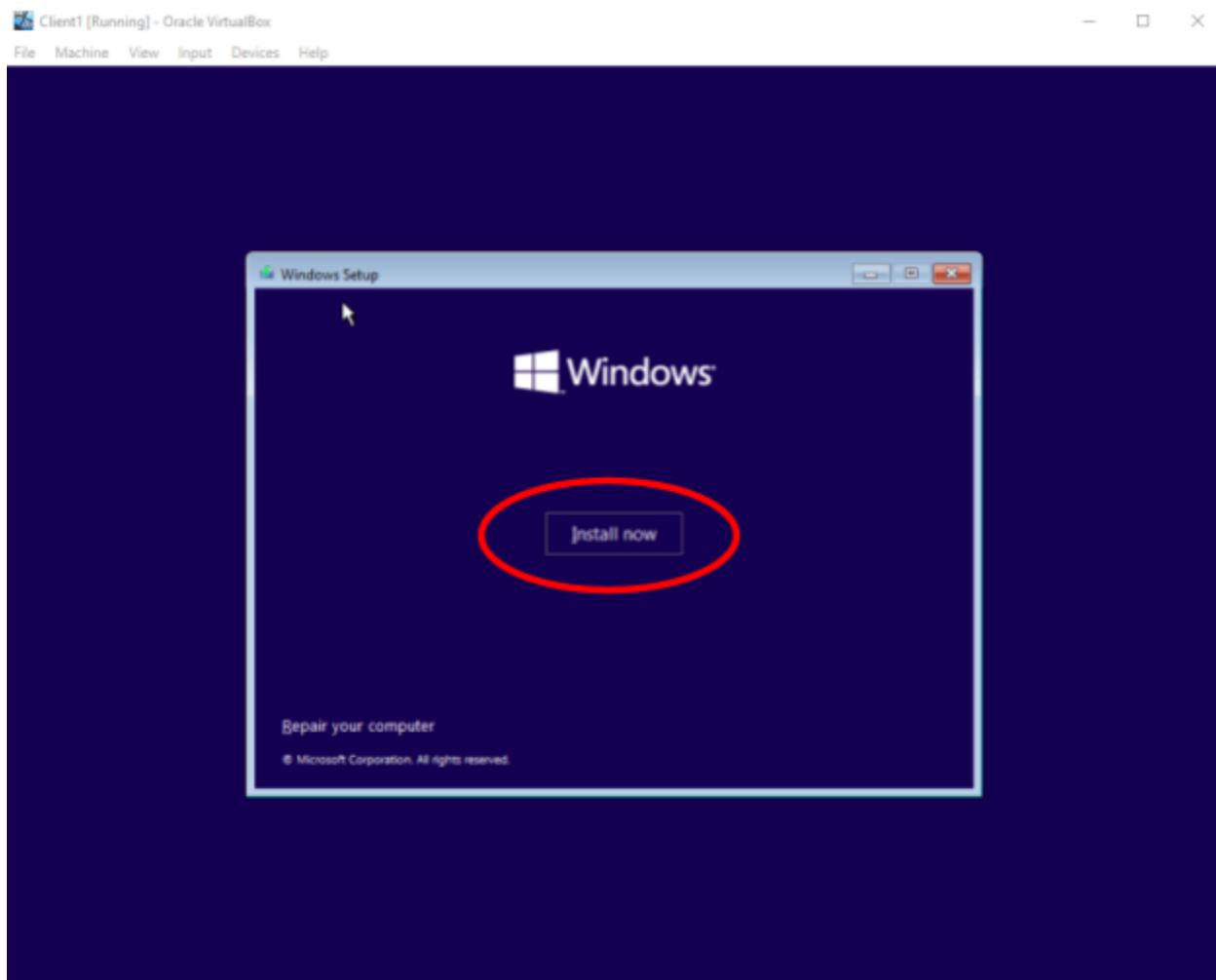
Double-Click on the Client1 Machine to run it



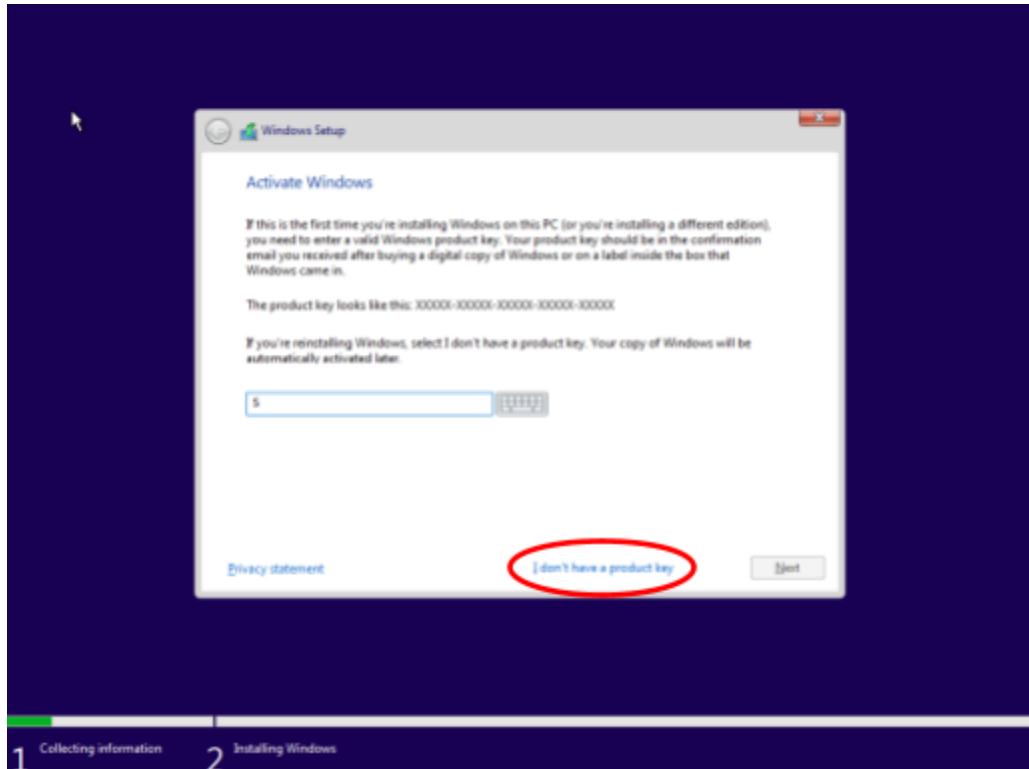
Go through the installation process



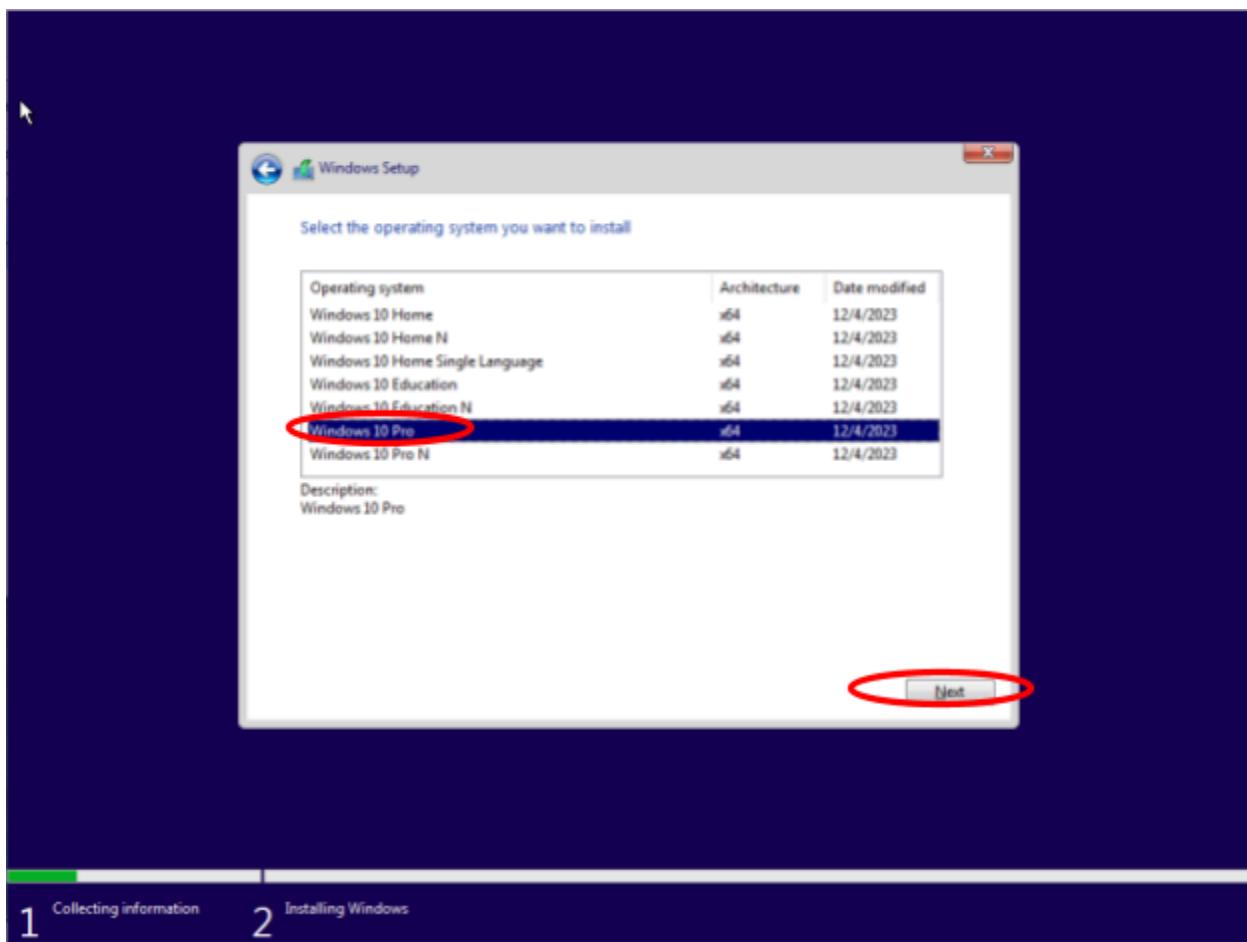
Click Install now



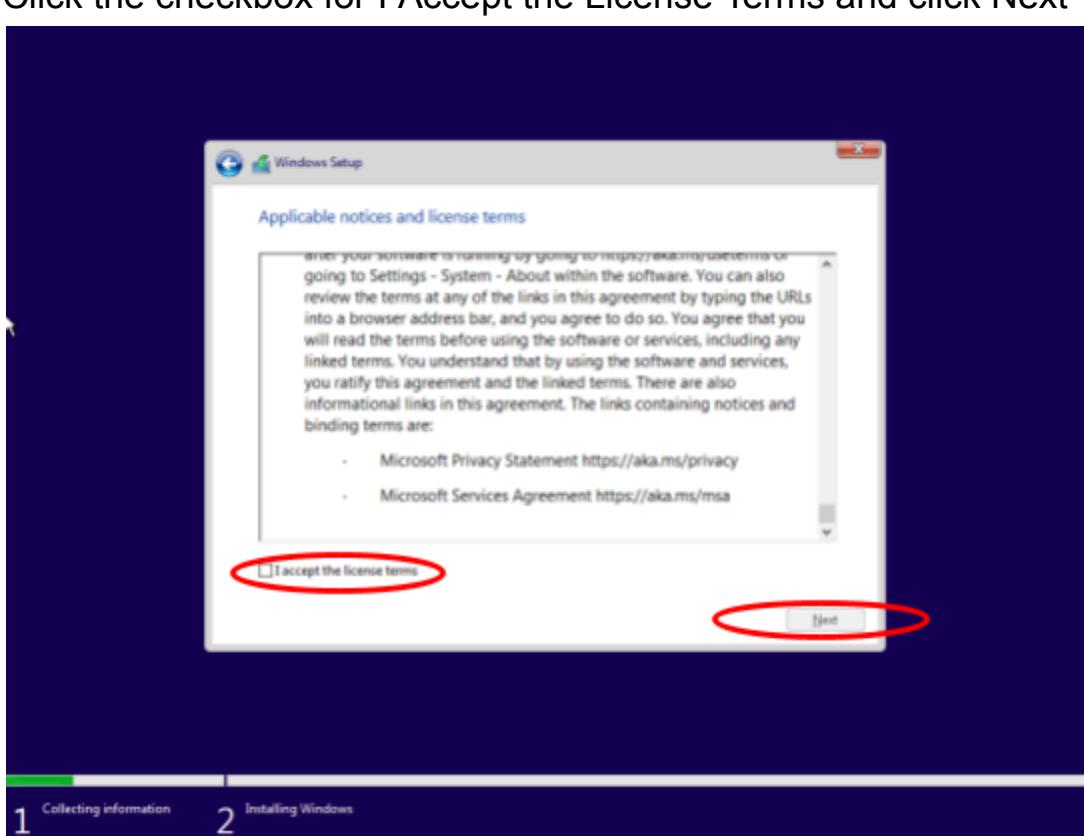
Select “I don’t have a product key”



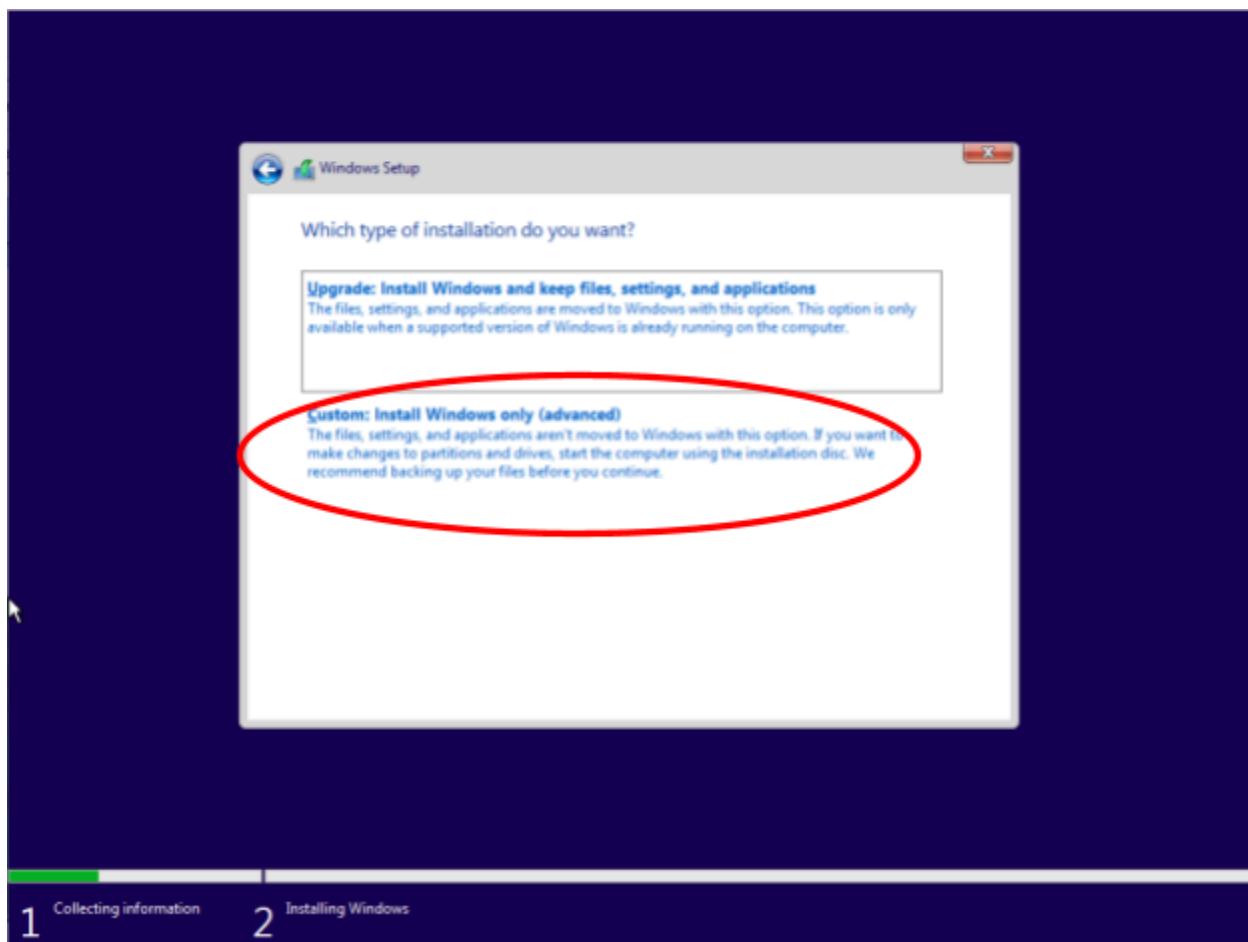
Select Windows 10 Pro to be able to connect to a domain. Click Next



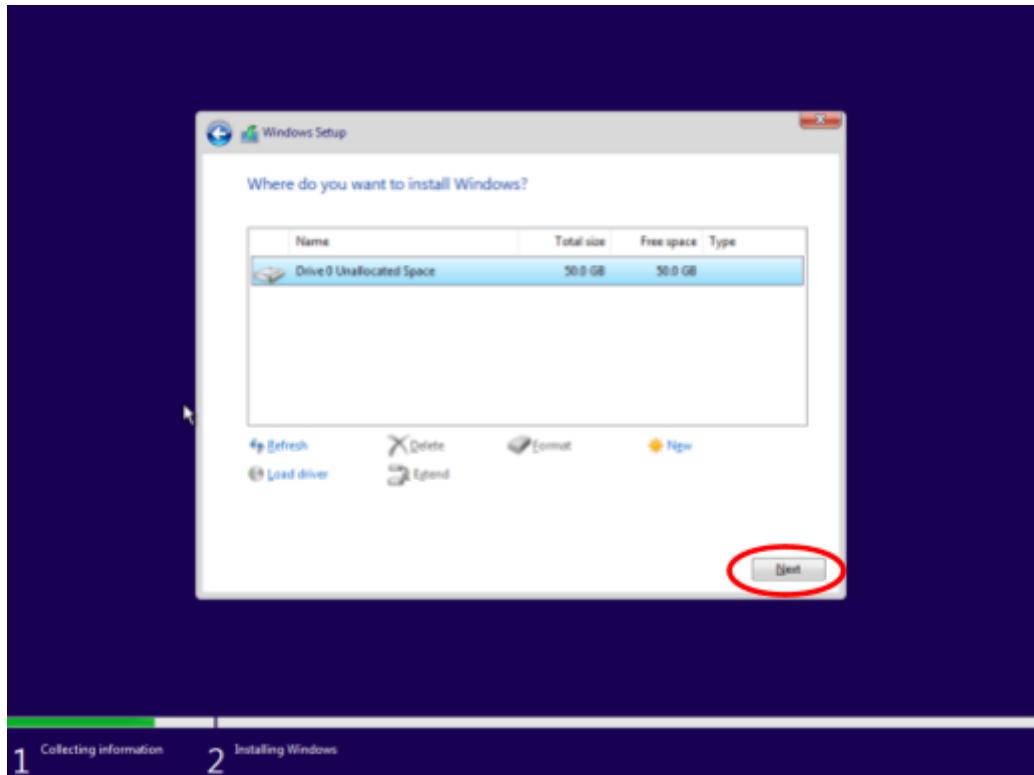
Click the checkbox for I Accept the License Terms and click Next

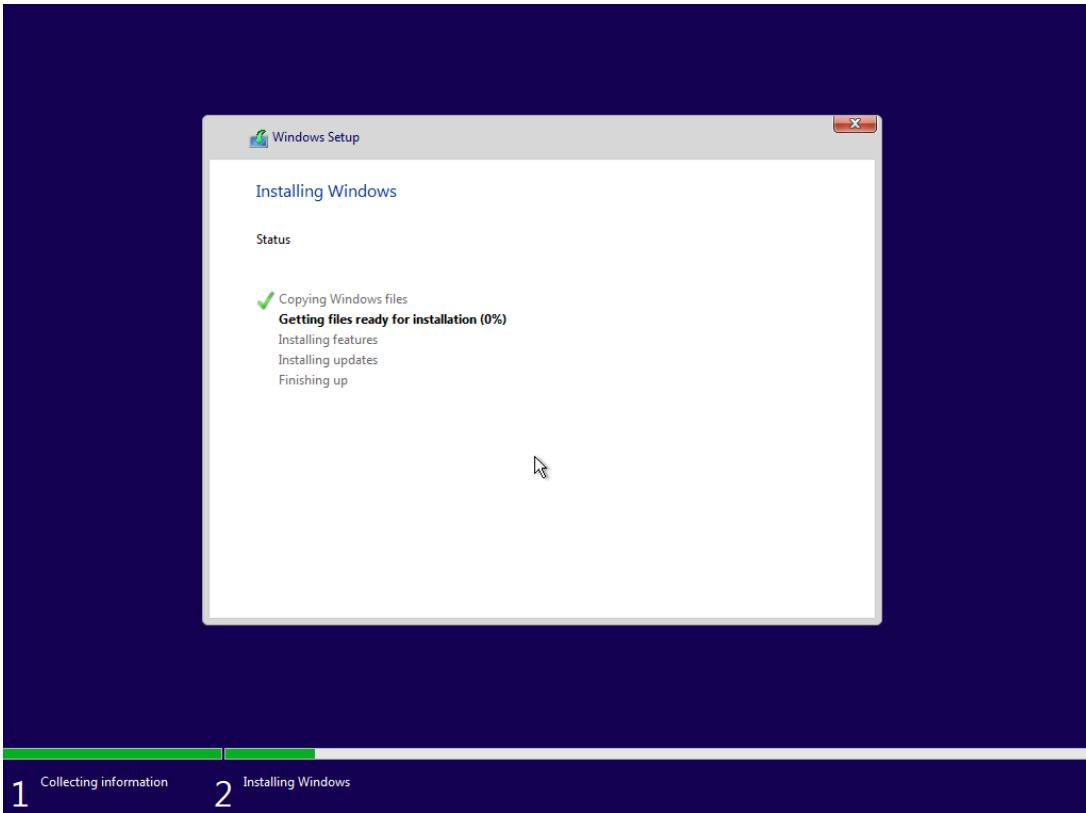


Select Custom

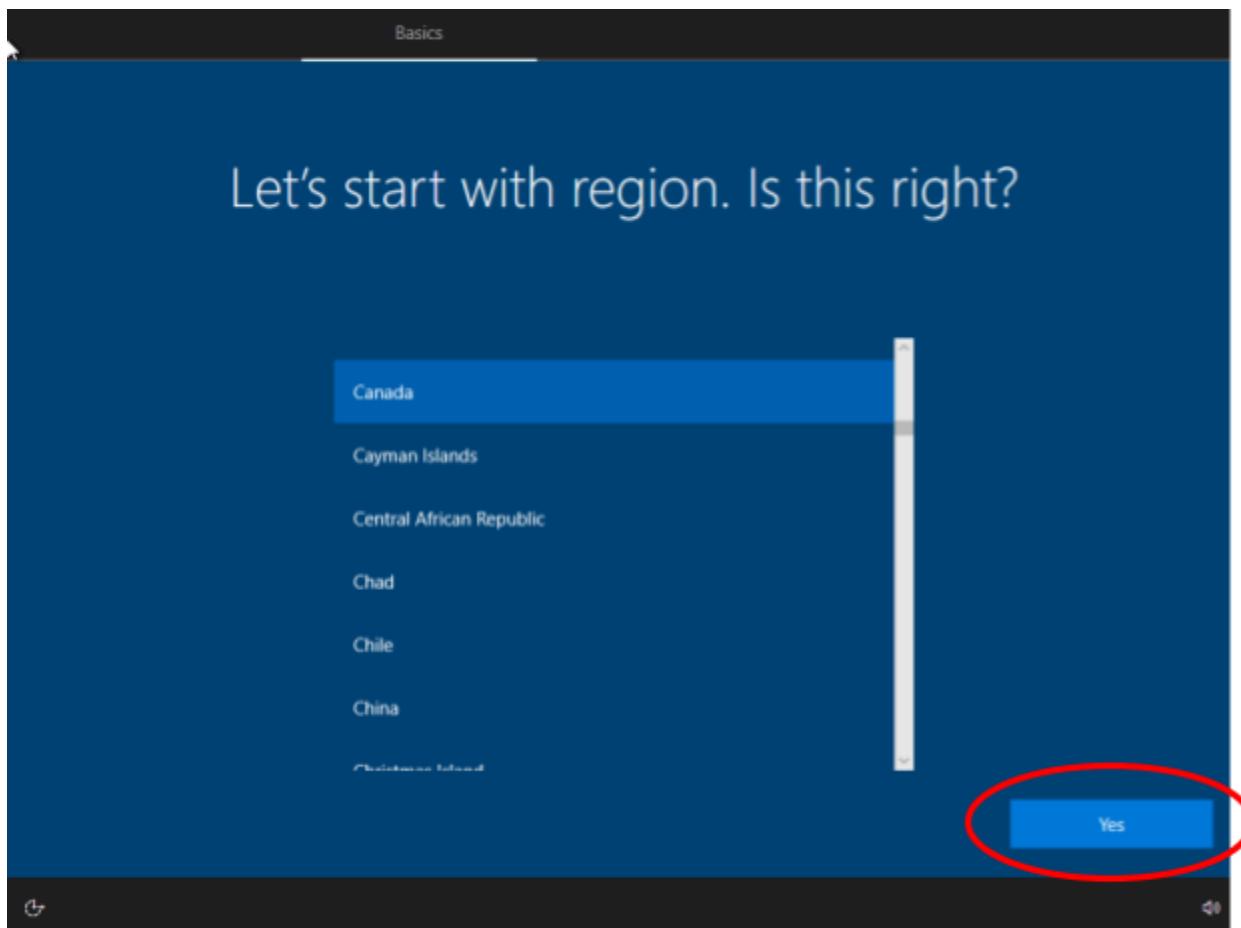


Click Next

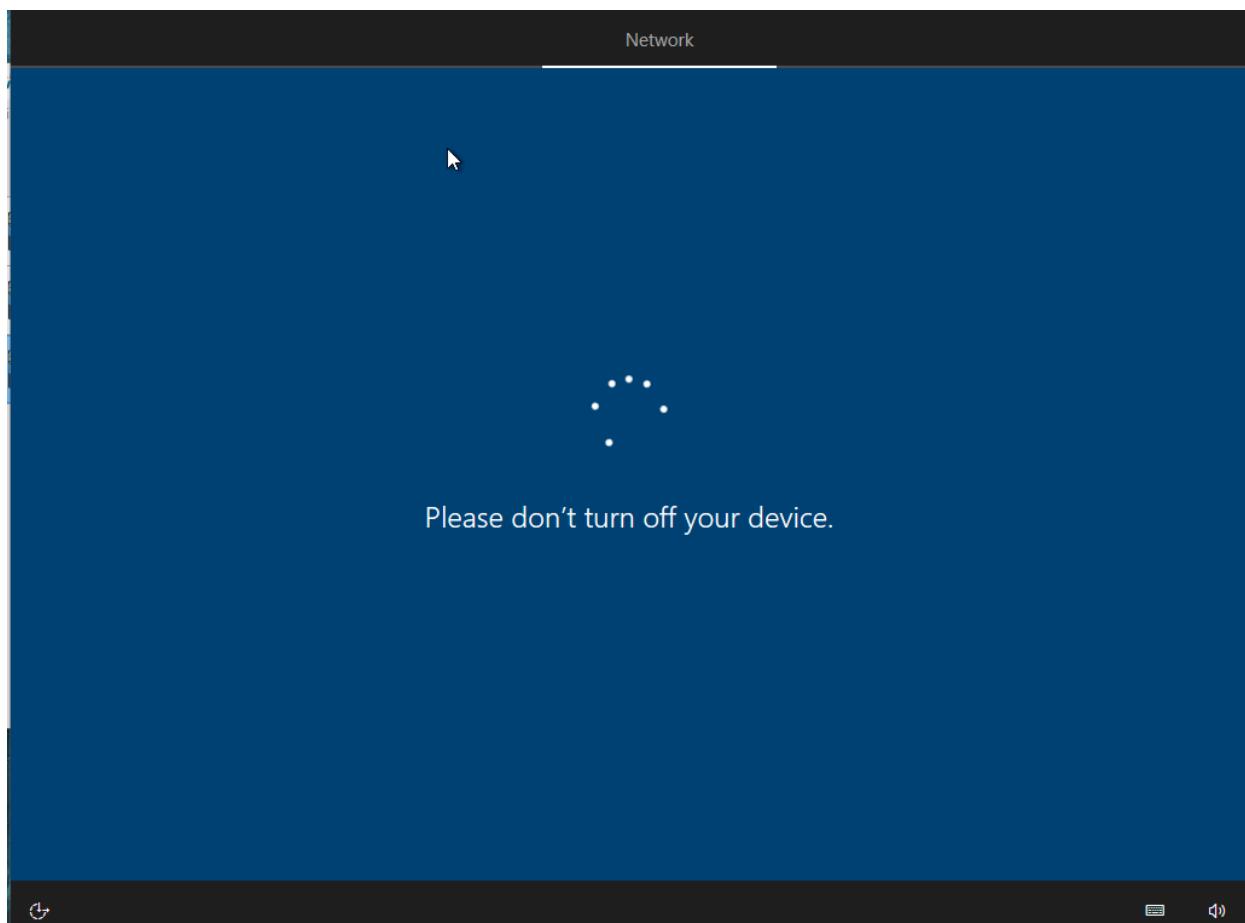
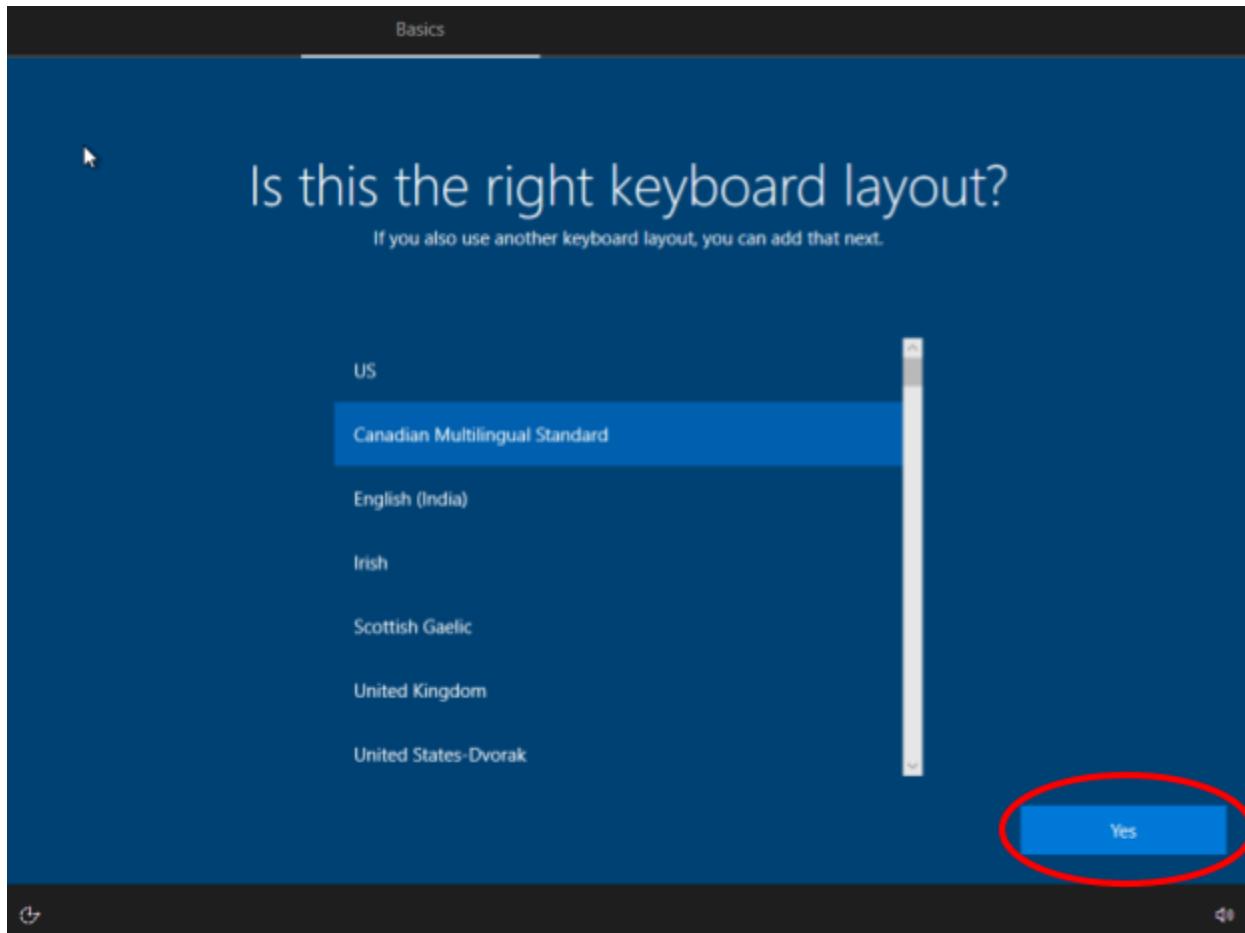




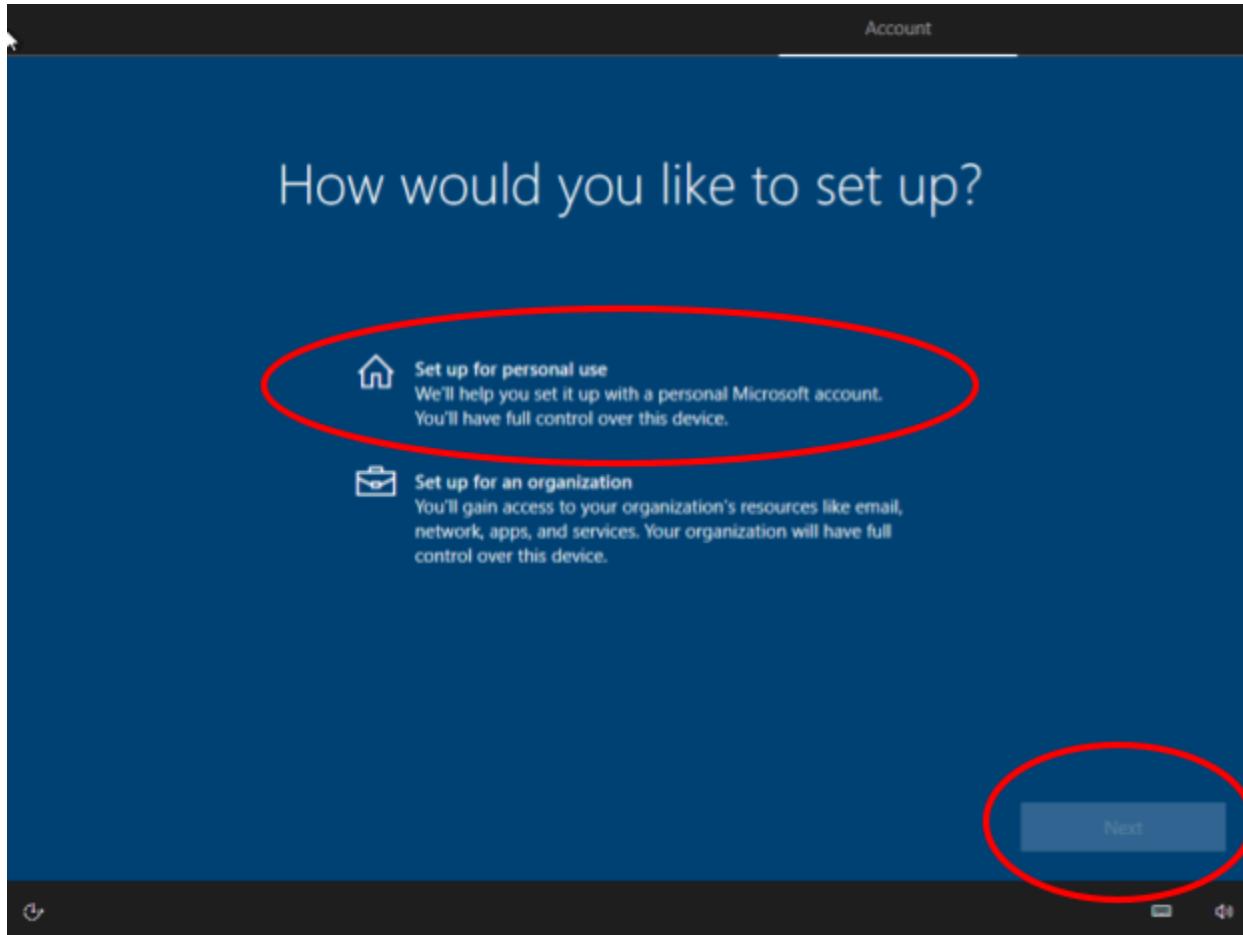
Select Yes



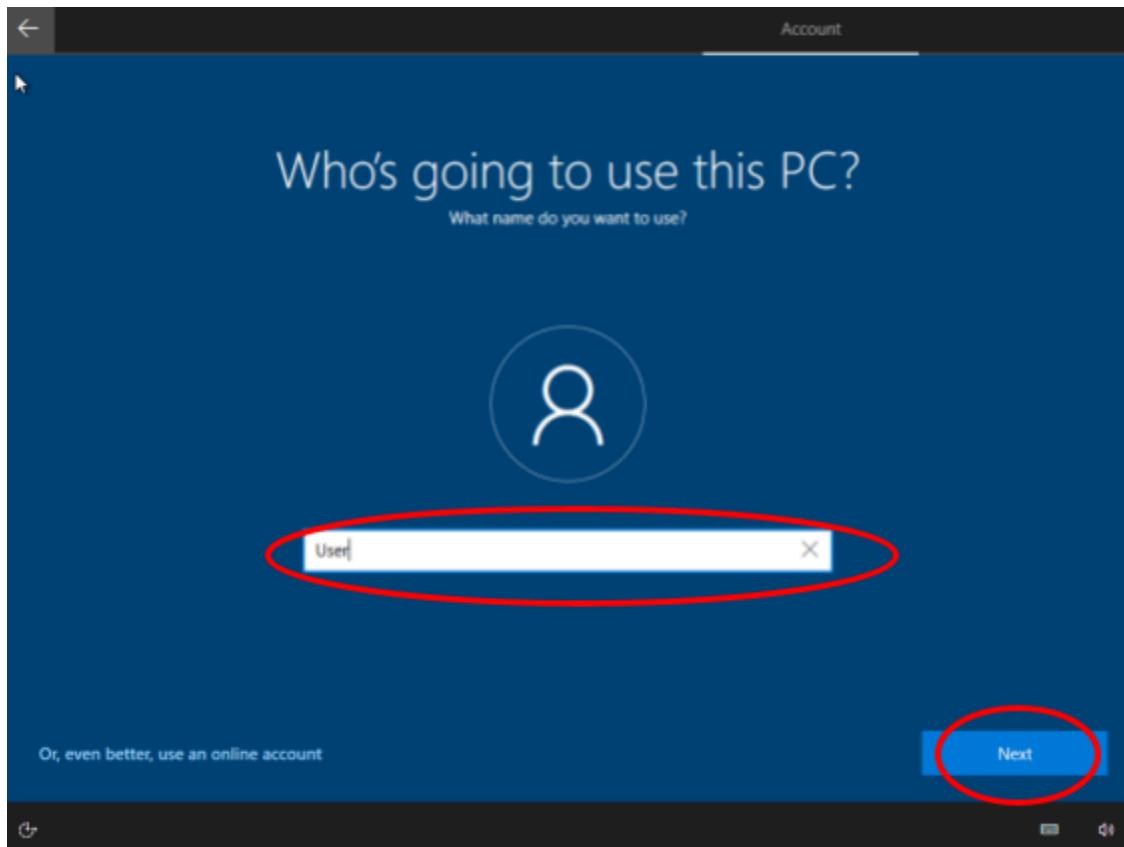
Select Yes



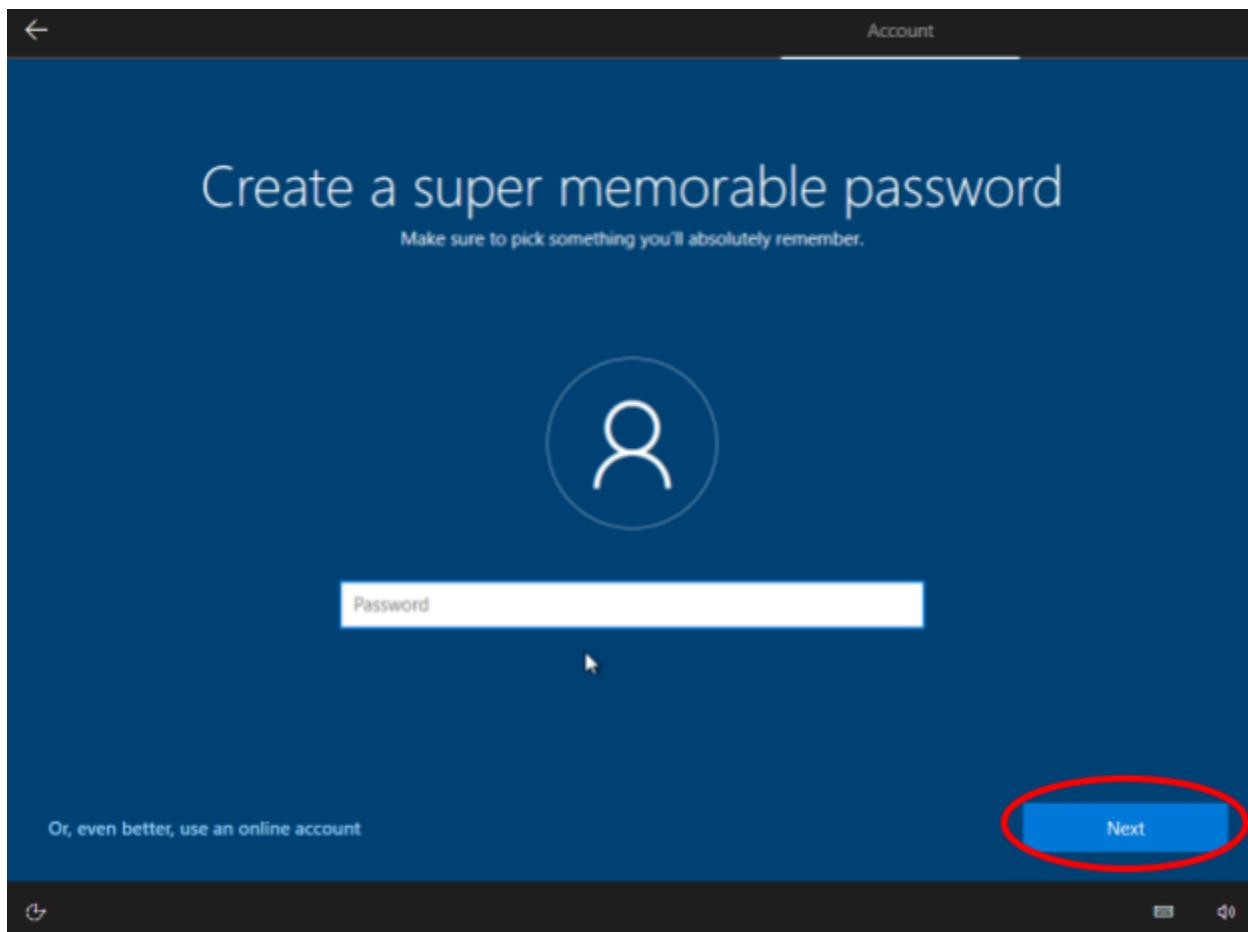
Choose Set up for personal use and click Next



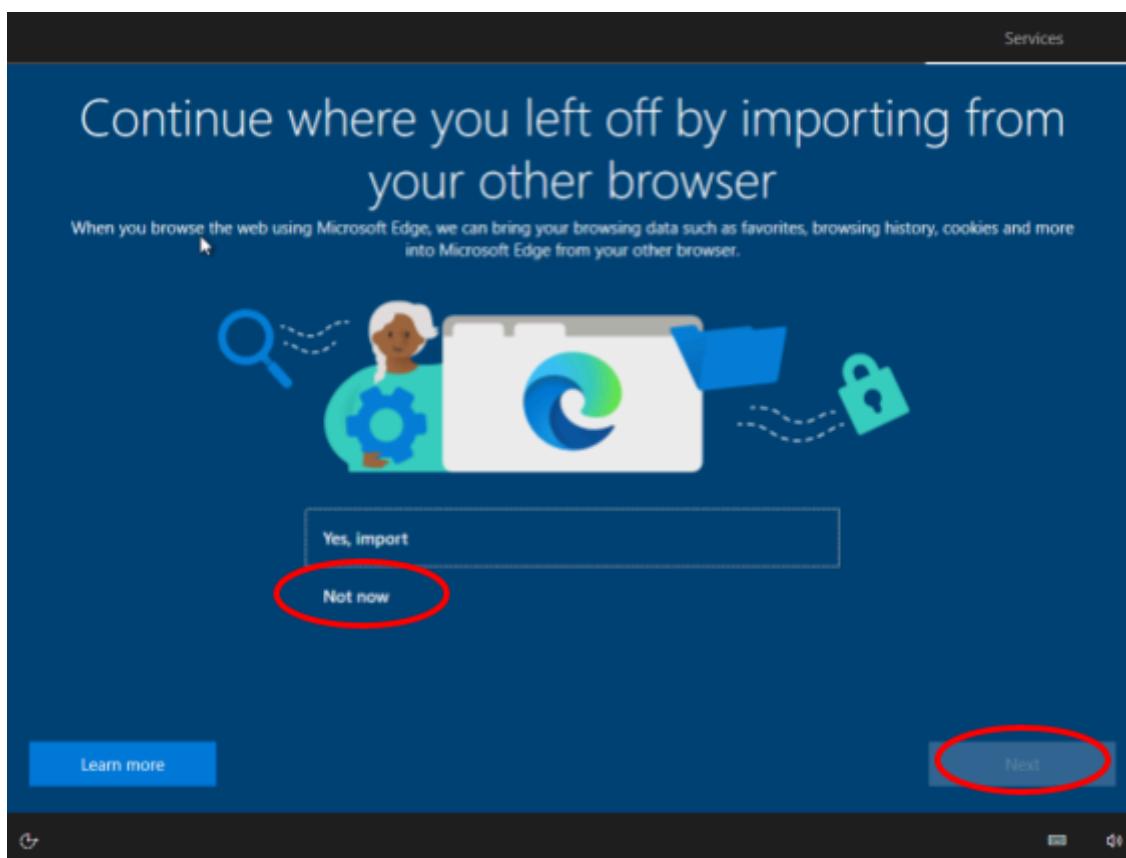
Name it User for now. We will change the name later. Click Next



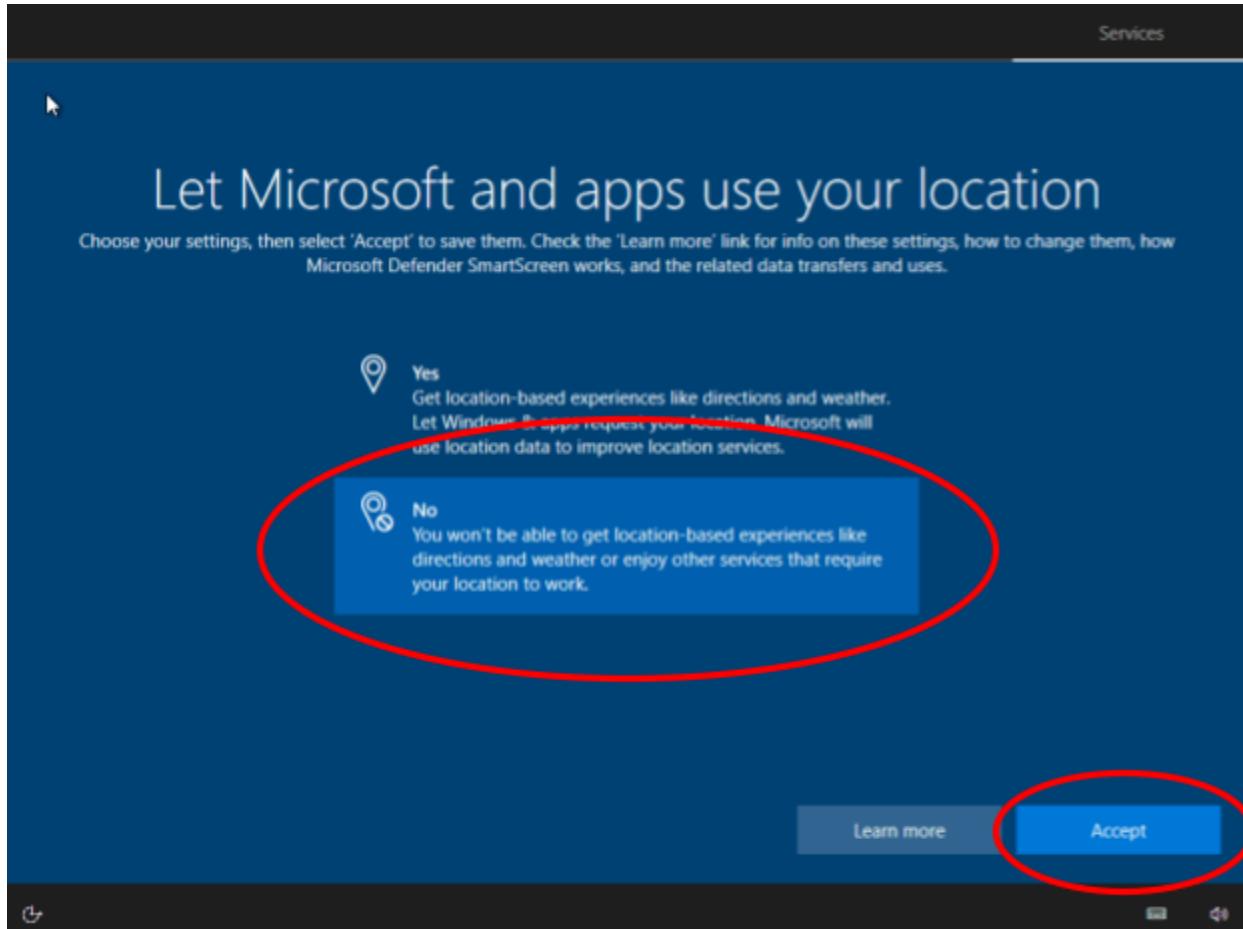
Create a Password and click Next



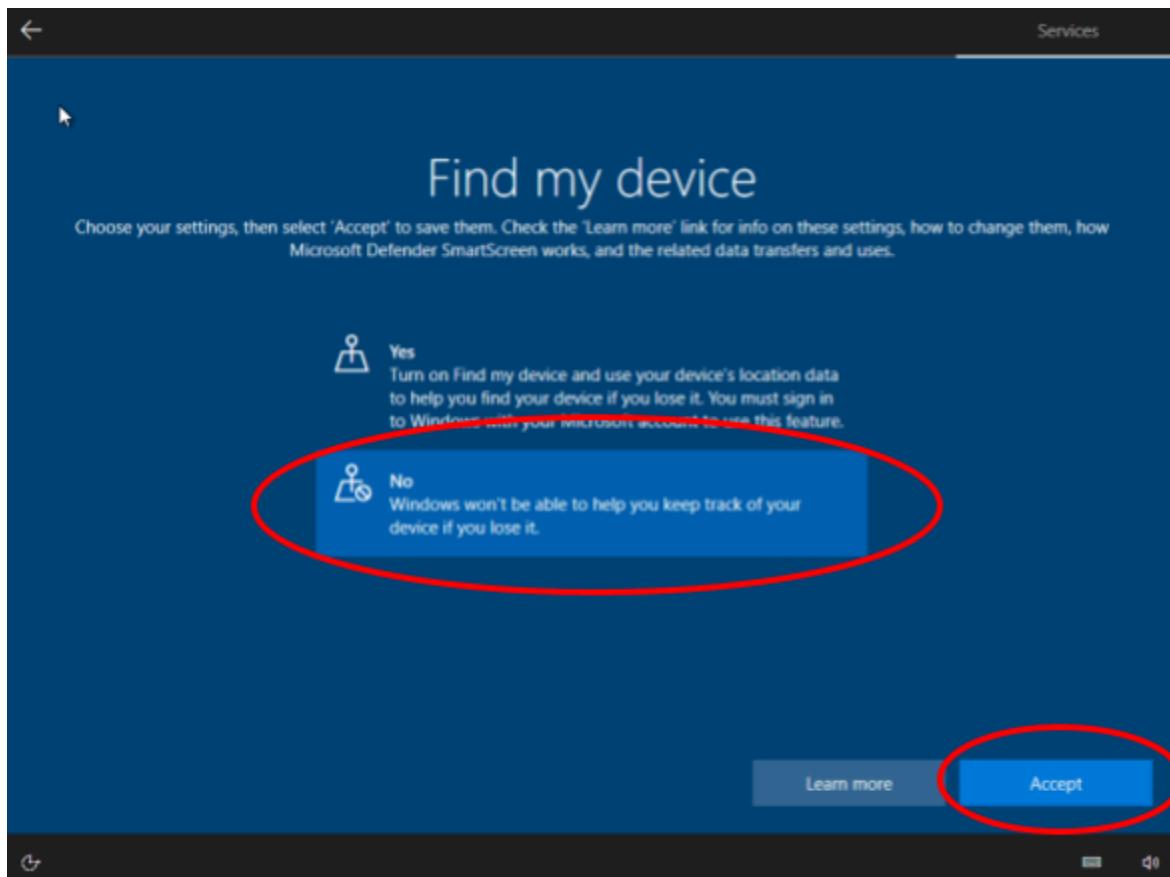
Click Next



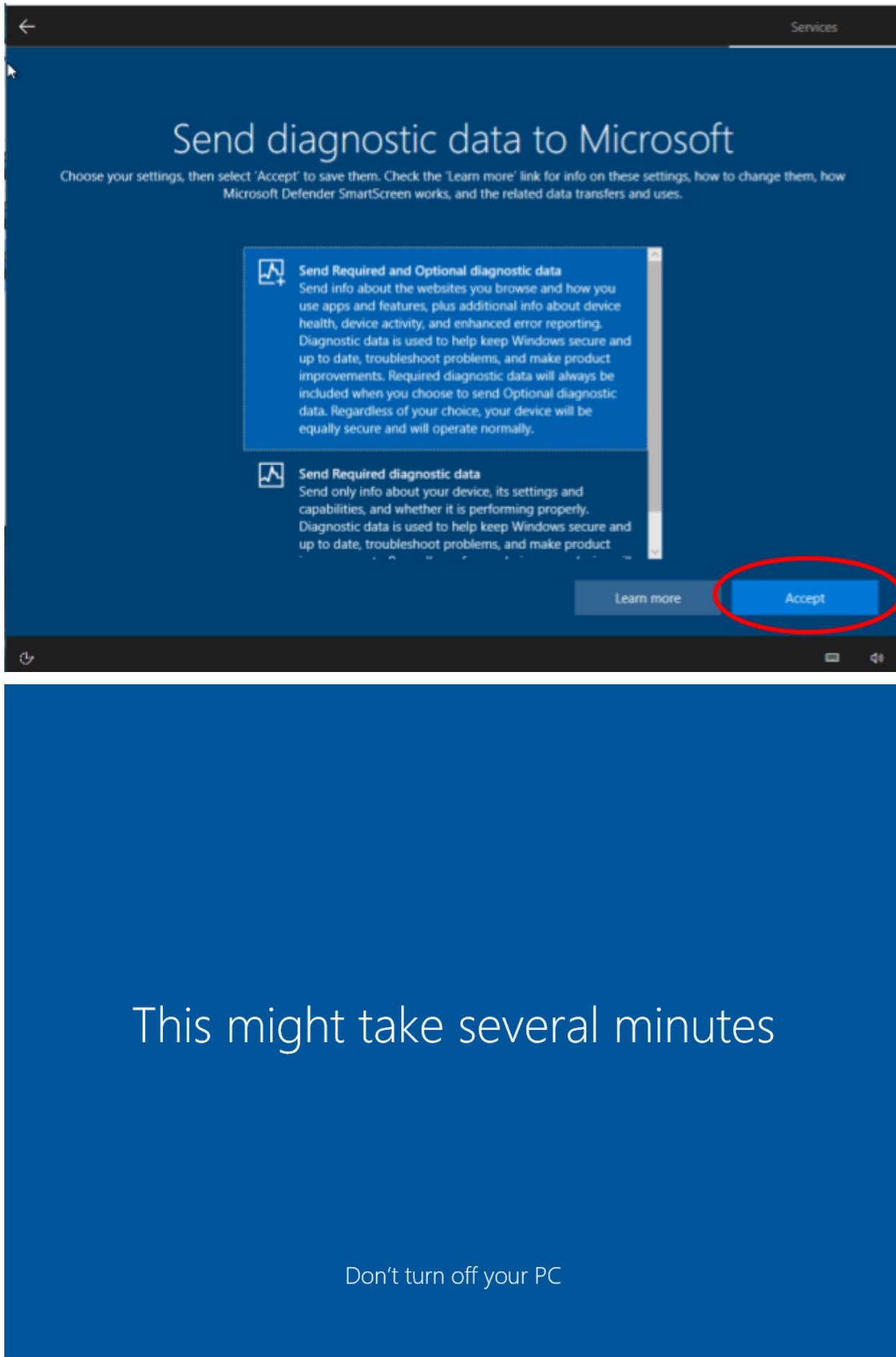
Select No and Accept



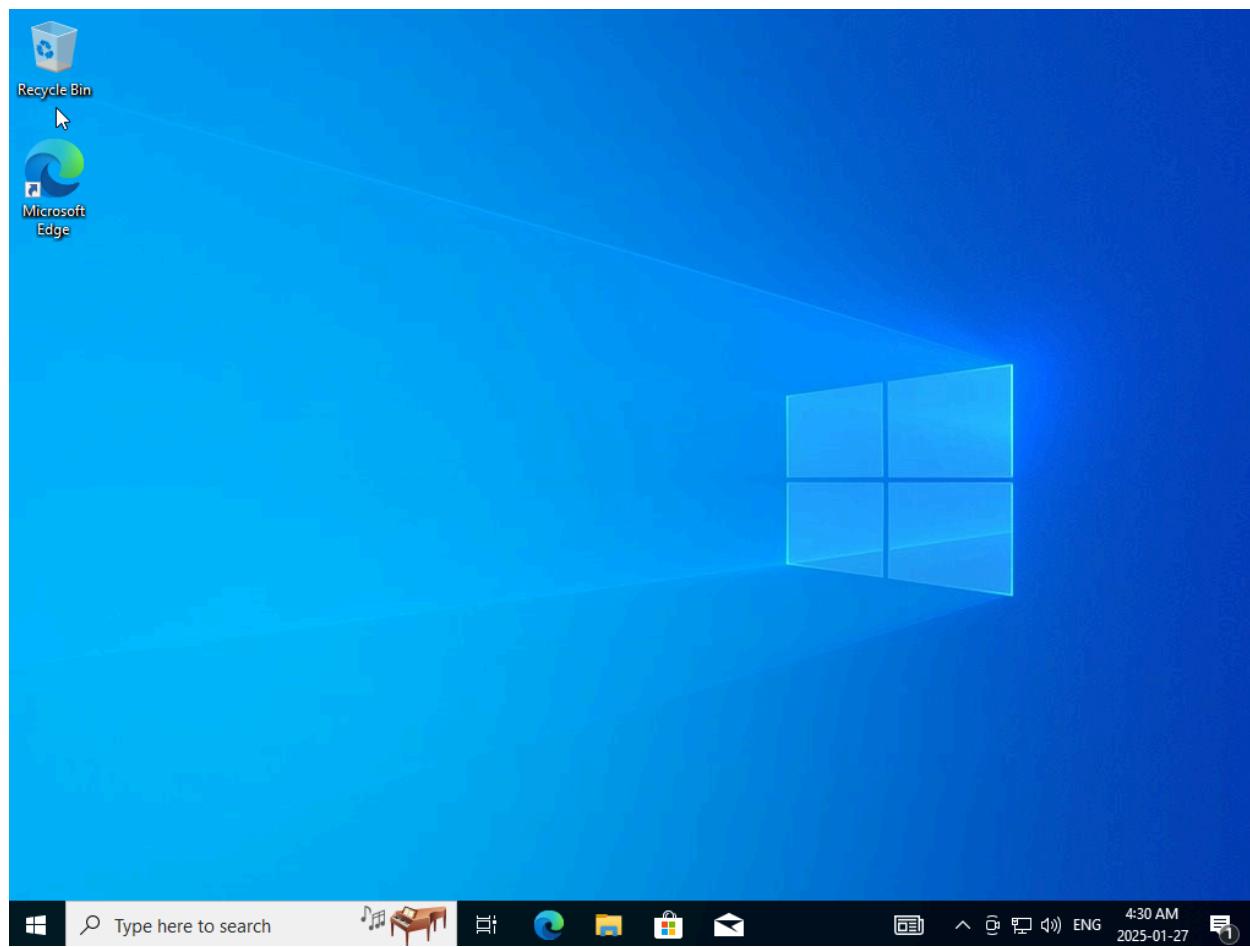
Select No and Accept



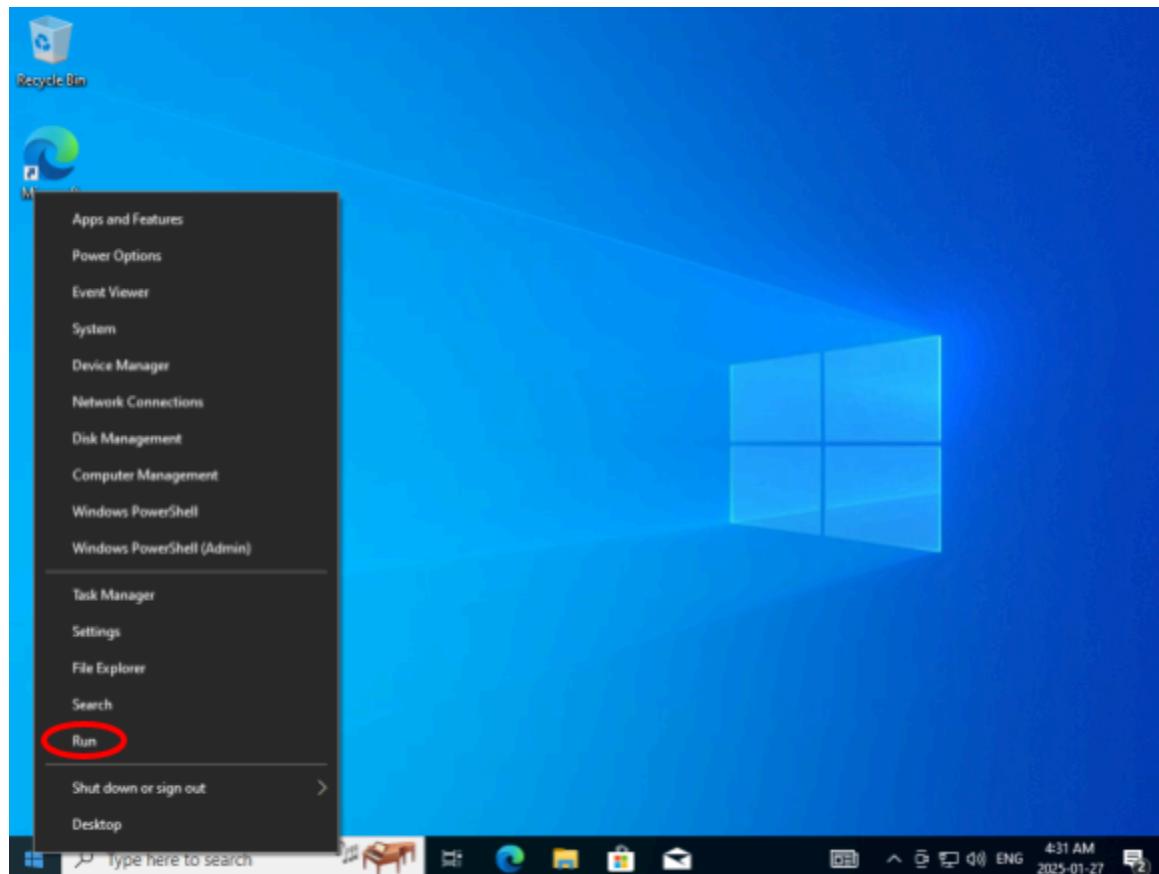
Select Send Required and Optional diagnostic data and click Accept



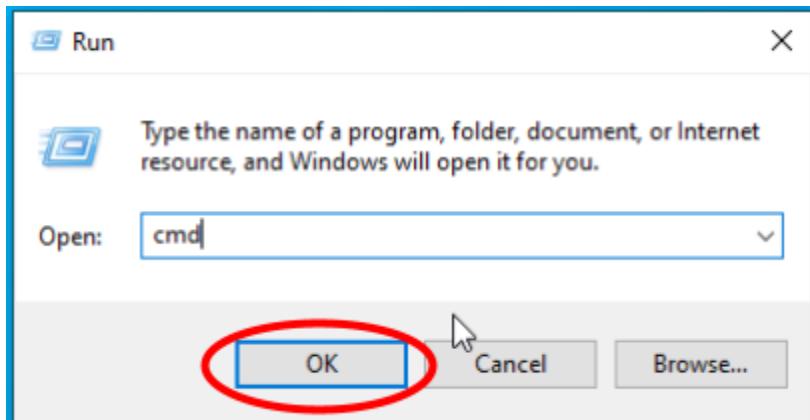
Success. Now, let's check if the Client1 VM is connected to the Internet



Right-Click on the Windows Menu Icon and Click on Run



Type cmd - short for command line interface and click OK



Type the command ipconfig to display network information

We can see that the Client1 machine has an IPv4 Address, a Subnet Mask, and a Default Gateway.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix  . :
  IPv6 Address. . . . . : fd00::652e:8fc:7379:a3d6
  Temporary IPv6 Address. . . . . : fd00::4140:4161:4526:6c35
  Link-local IPv6 Address . . . . . : fe80::87c3:985a:93b5:dc8fx6
  IPv4 Address. . . . . : 10.0.2.15
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : fe80::2%6
                               10.0.2.2

C:\Users\User>
```

The screenshot shows a Windows Command Prompt window. The user has typed "ipconfig" and pressed Enter. The output displays network configuration for an "Ethernet adapter Ethernet". The "IPv4 Address" is highlighted with a red circle, showing "10.0.2.15". The "Subnet Mask" and "Default Gateway" are also highlighted with a red circle, both showing "10.0.2.2".

To ensure that it is connected to the Internet, we will use the **ping** command to ping www.google.com

```
C:\Windows\system32\cmd.exe
C:\Users\User>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
IPv6 Address . . . . . : fd00::652e:8fc:7379:a3d6
Temporary IPv6 Address. . . . . : fd00::4140:4161:4526:6c35
Link-local IPv6 Address . . . . . : fe80::87c3:9859:93b5:dc8f%6
IPv4 Address. . . . . : 10.0.2.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::2%6
                           10.0.2.2

C:\Users\User>ping www.google.com

Pinging www.google.com [142.251.215.228] with 32 bytes of data:
Reply from 142.251.215.228: bytes=32 time=24ms TTL=255
Reply from 142.251.215.228: bytes=32 time=24ms TTL=255
Reply from 142.251.215.228: bytes=32 time=25ms TTL=255
Reply from 142.251.215.228: bytes=32 time=25ms TTL=255

Ping statistics for 142.251.215.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 25ms, Average = 24ms

C:\Users\User>
```

Let's also ping our Domain Controller

```
C:\Windows\system32\cmd.exe
Default Gateway . . . . . : fe80::2%6
                           10.0.2.2

C:\Users\User>ping www.google.com

Pinging www.google.com [142.251.215.228] with 32 bytes of data:
Reply from 142.251.215.228: bytes=32 time=24ms TTL=255
Reply from 142.251.215.228: bytes=32 time=24ms TTL=255
Reply from 142.251.215.228: bytes=32 time=25ms TTL=255
Reply from 142.251.215.228: bytes=32 time=25ms TTL=255

Ping statistics for 142.251.215.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 25ms, Average = 24ms

C:\Users\User>ping mydomain.com

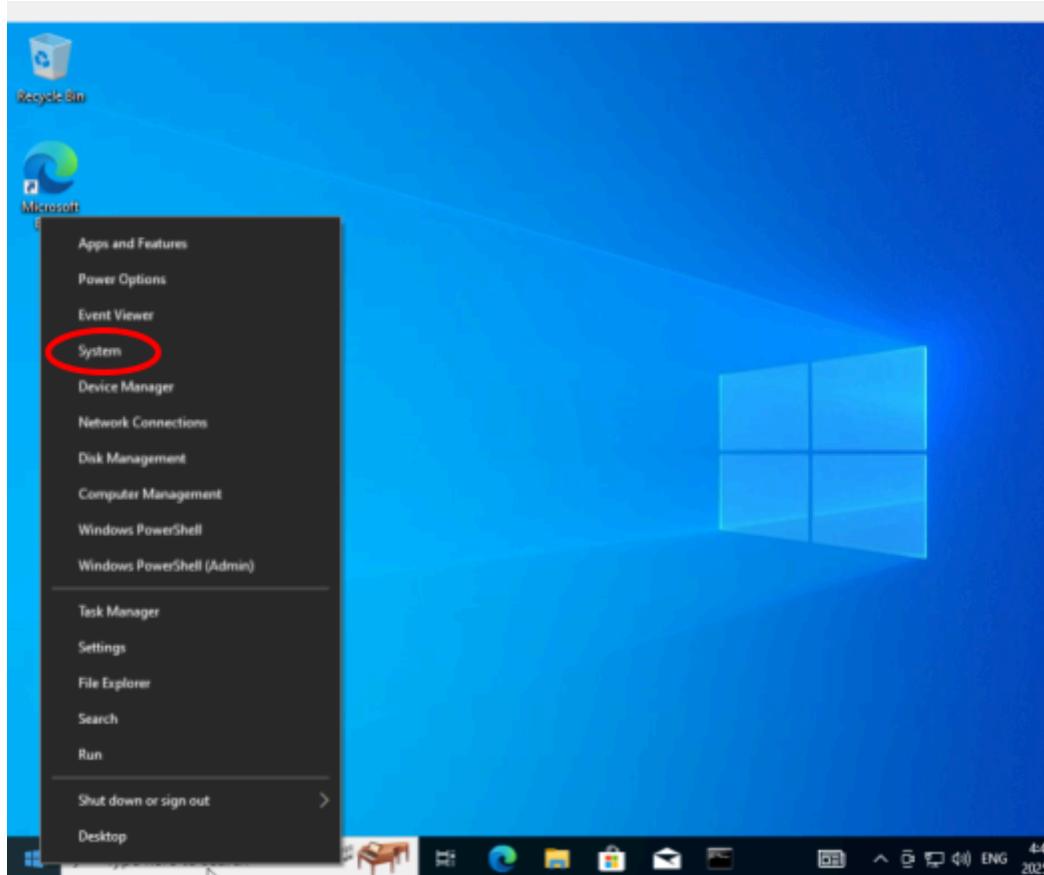
Pinging mydomain.com [65.254.242.180] with 32 bytes of data:
Reply from 65.254.242.180: bytes=32 time=69ms TTL=255
Reply from 65.254.242.180: bytes=32 time=69ms TTL=255
Reply from 65.254.242.180: bytes=32 time=69ms TTL=255
Reply from 65.254.242.180: bytes=32 time=68ms TTL=255

Ping statistics for 65.254.242.180:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 68ms, Maximum = 69ms, Average = 68ms

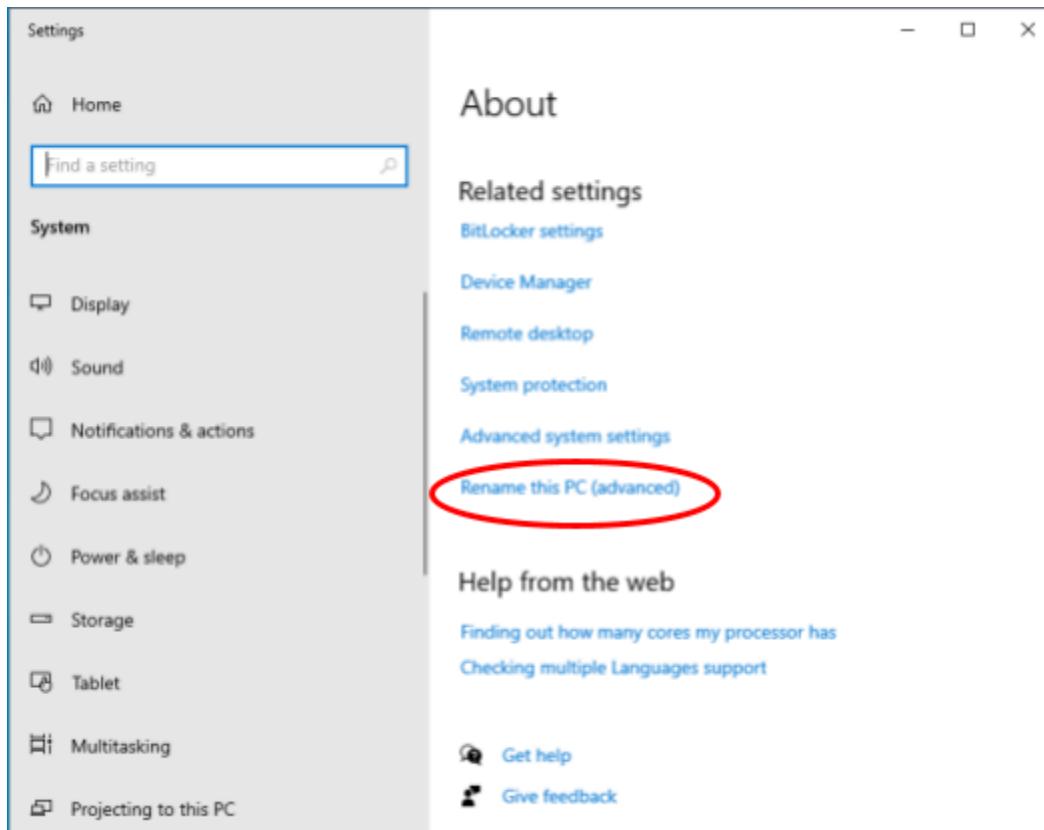
C:\Users\User>
```

Step 11: Rename the Client1 PC and Join it to the Domain

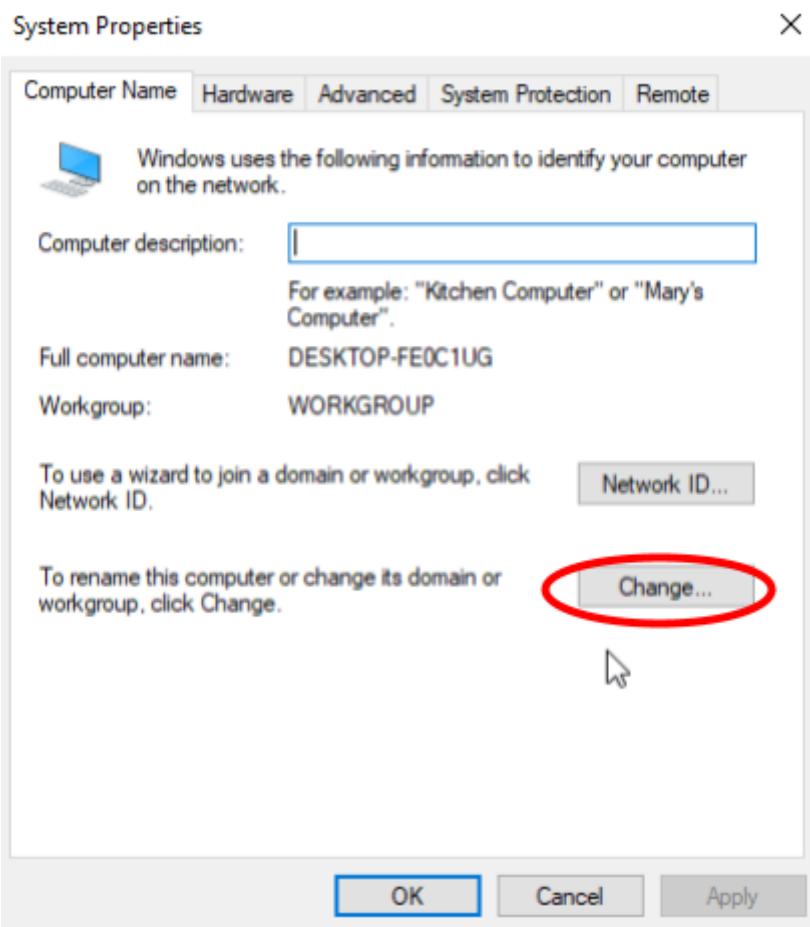
To begin, we will Right-Click on the Windows Menu Icon and select System



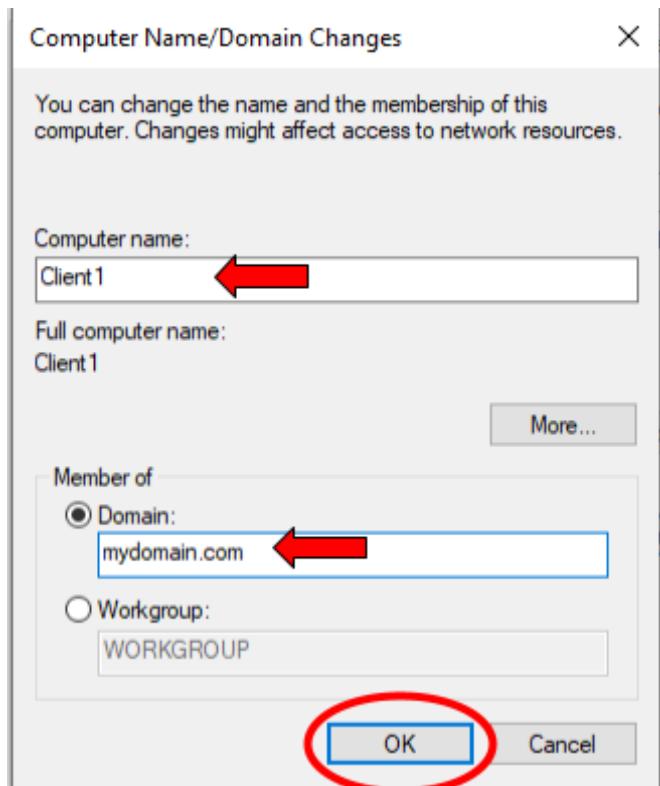
Select “Rename this PC (advanced)”. This will allow us to rename the PC and connect it to the Domain Controller



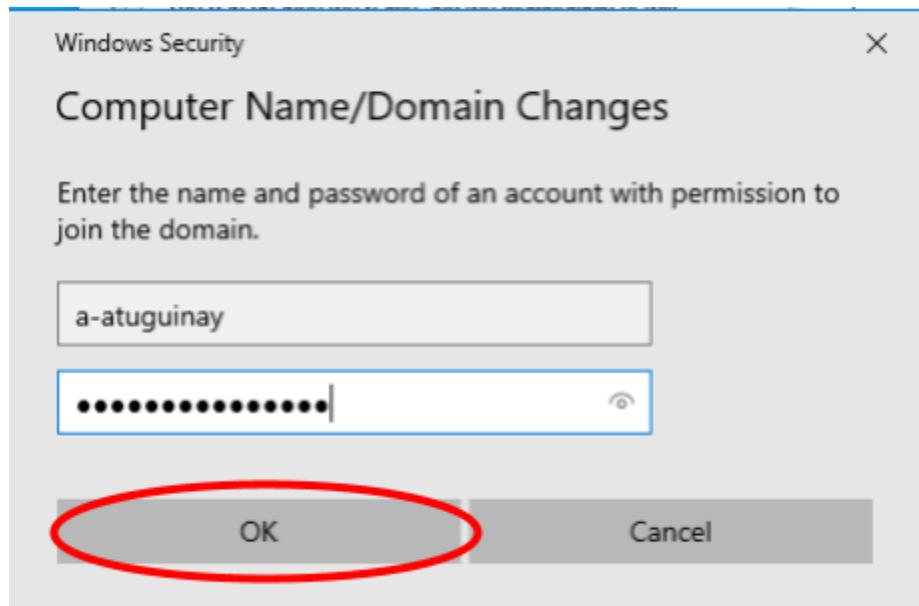
Click on Change...



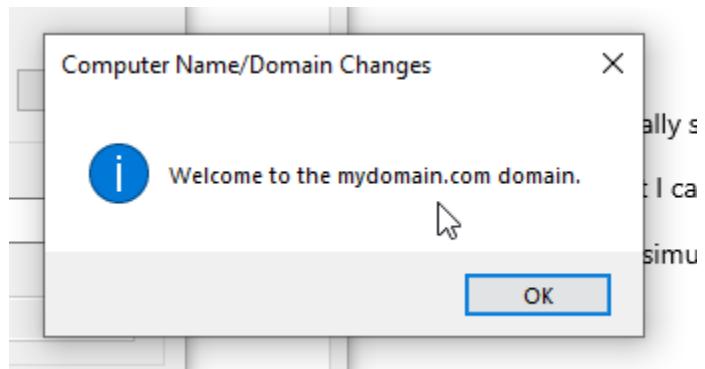
Change the name to Client1 and select Domain. Type in the domain name of our Domain Controller: mydomain.com and click OK



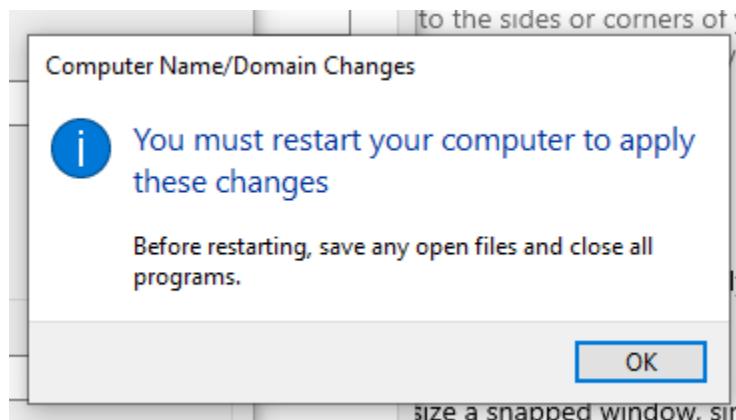
Authorize by using our Admin credentials that we created earlier
Click OK



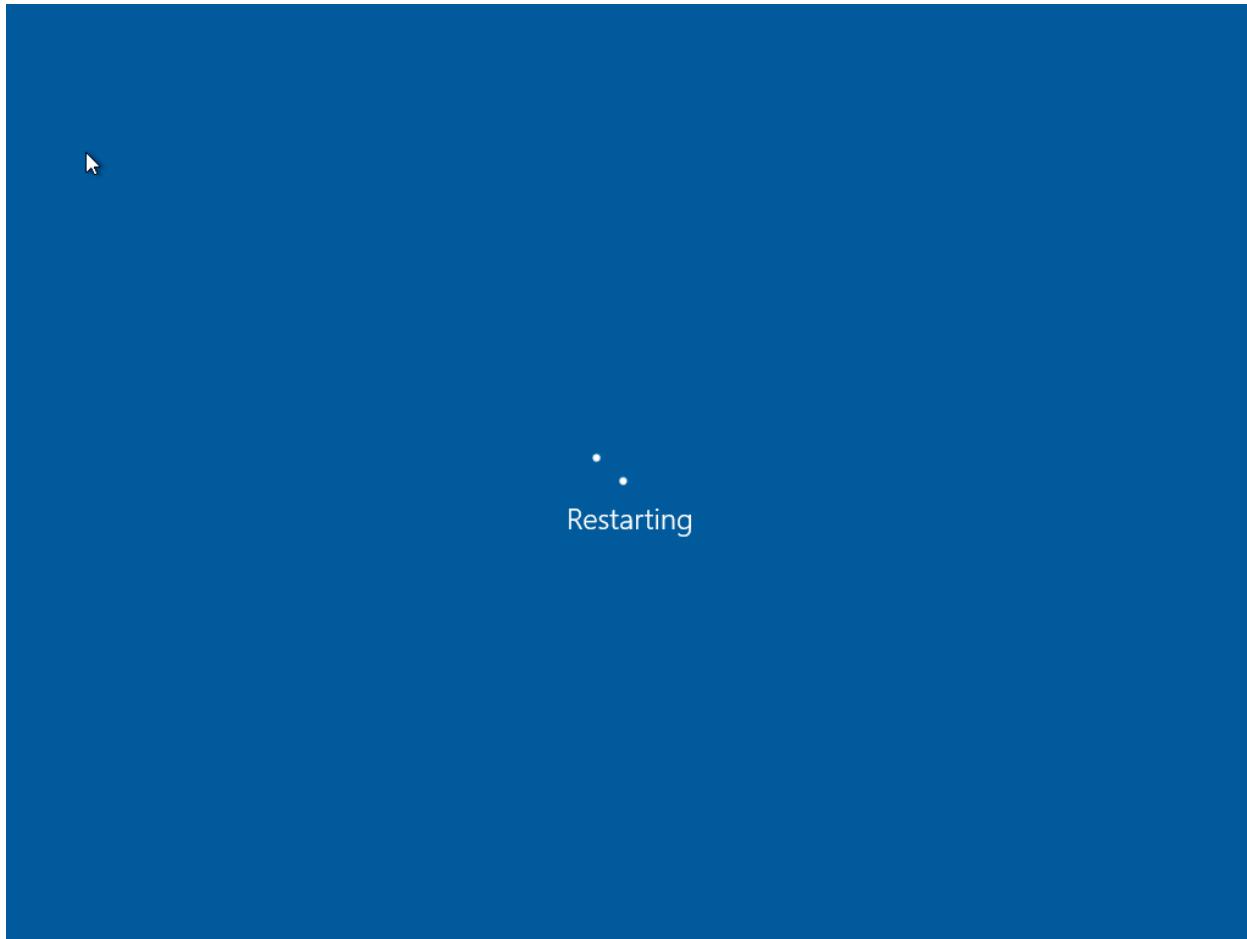
Click OK



Click OK



Restart the Virtual Machine



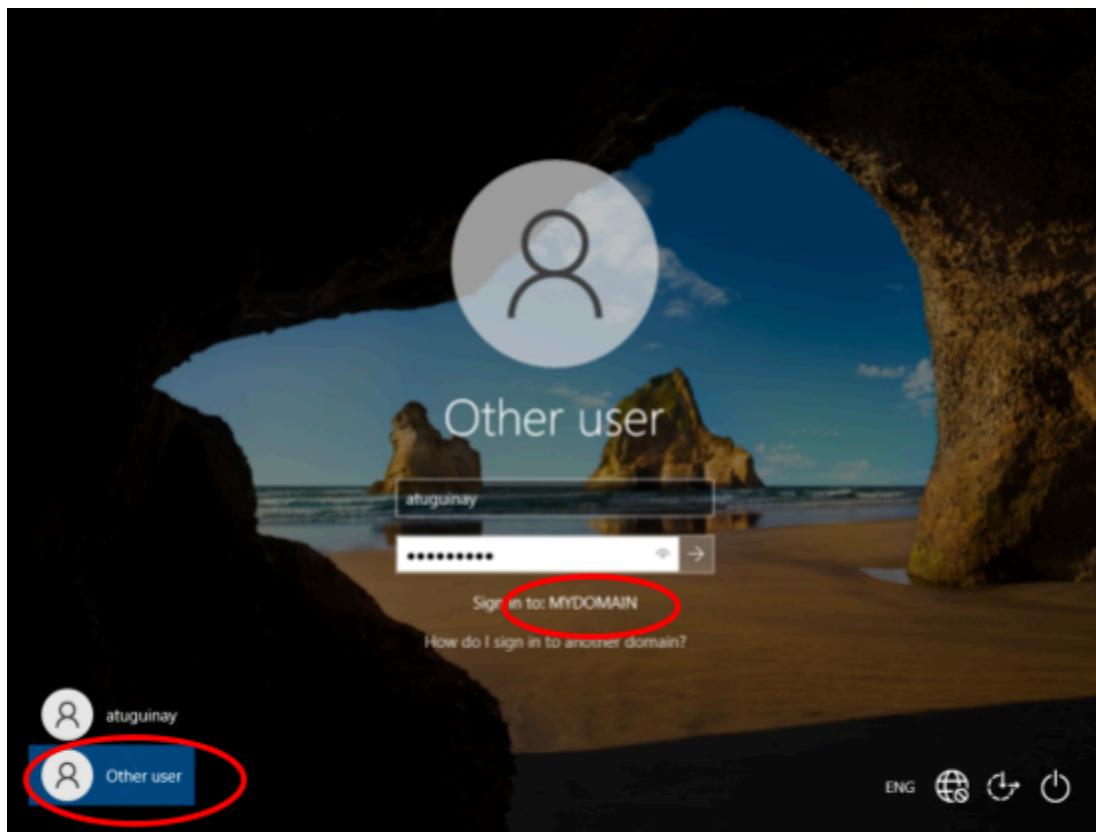
Back in the Domain Controller Virtual Machine, when we open up the DHCP window, we can see that Client1 was added to the DHCP Address Leases folder, showing that Client1 has indeed joined the mydomain.com domain

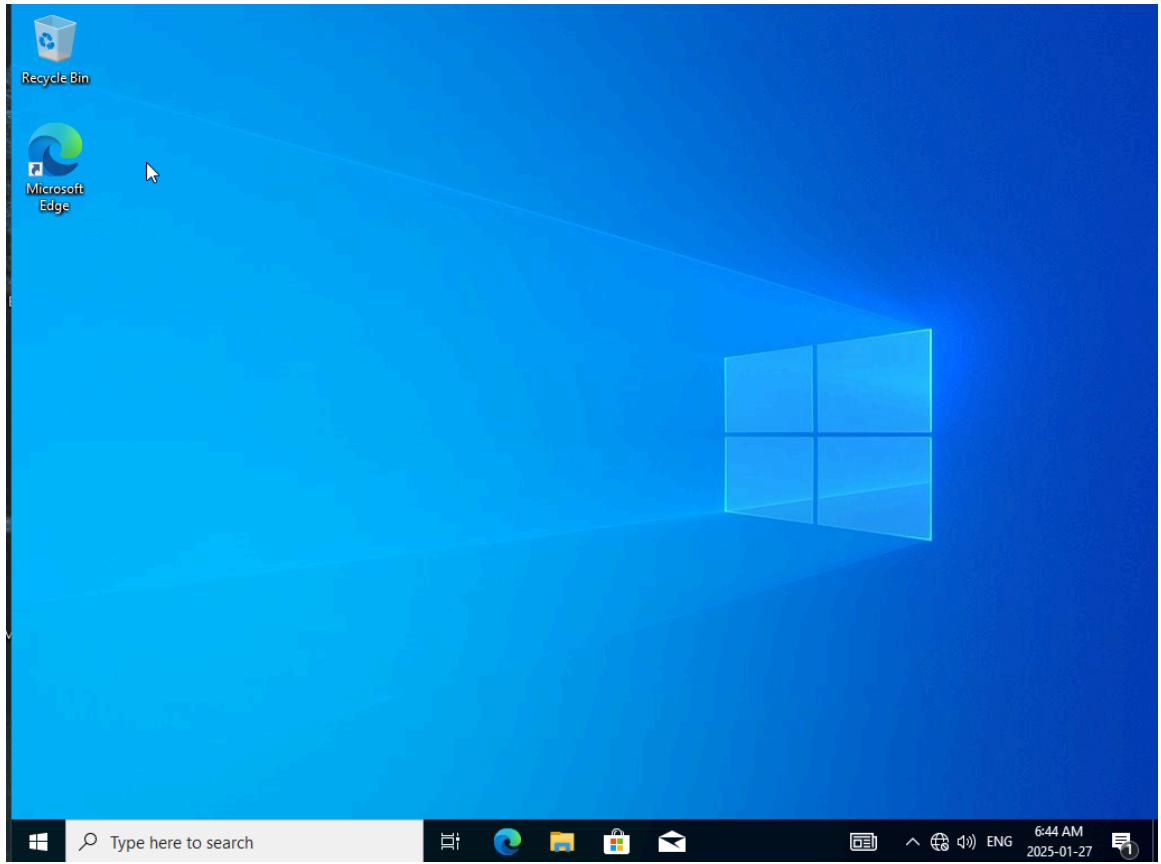
A screenshot of the Microsoft DHCP Management console window. The title bar says "DHCP". The left pane shows a tree view of the DHCP configuration, including "domaincontroller.mydomain.com" and its sub-sections like "IPv4" and "Scope [172.16.0.0] 172.16.0.100-200". The right pane displays a table titled "Address Leases". One row in the table is circled in red. The circled row contains the following information: Client IP Address: 172.16.0.100, Client Name: Client1.mydomain..., and Lease Start Time: 2/4/2025 7:31:27 AM. The "Actions" pane on the right is set to "Address Leases".

In the Computers Folder under mydomain.com in Active Directory Users and Computers, Client1 has been added to show that it has joined mydomain.com

The screenshot shows the Windows Active Directory Users and Computers interface. On the left, the navigation pane displays the tree structure: Active Directory Users and Computers, Saved Queries, mydomain.com (expanded to show _USERS, ADMINS, Builtin, Computers, Domain Controllers, ForeignSecurityPrincipals, Managed Service Accounts, and Users). On the right, a table lists objects with columns: Name, Type, and Description. A single row is visible: CLIENT1, Computer. This row is circled in red.

Next, we will log into our Client1 Computer with a user that was added to the domain using the PowerShell script that we ran in the Domain Controller account. In this case, we added our own name to the list of users and we will use it to log into Client1 computer.





Success.

A screenshot of a Command Prompt window titled 'C:\Windows\system32\cmd.exe'. The window shows the following text:

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\atuguina>whoami
mydomain\atuguinay
C:\Users\atuguinay>
```

A red arrow points to the command 'whoami' in the first line of the output, and another red arrow points to the user handle 'atuguinay' in the second line.

When we open up the Command Line and run the command **whoami**, we can see that the user “atuguinay” is a part of the “mydomain” domain.

This is the end of the lab.