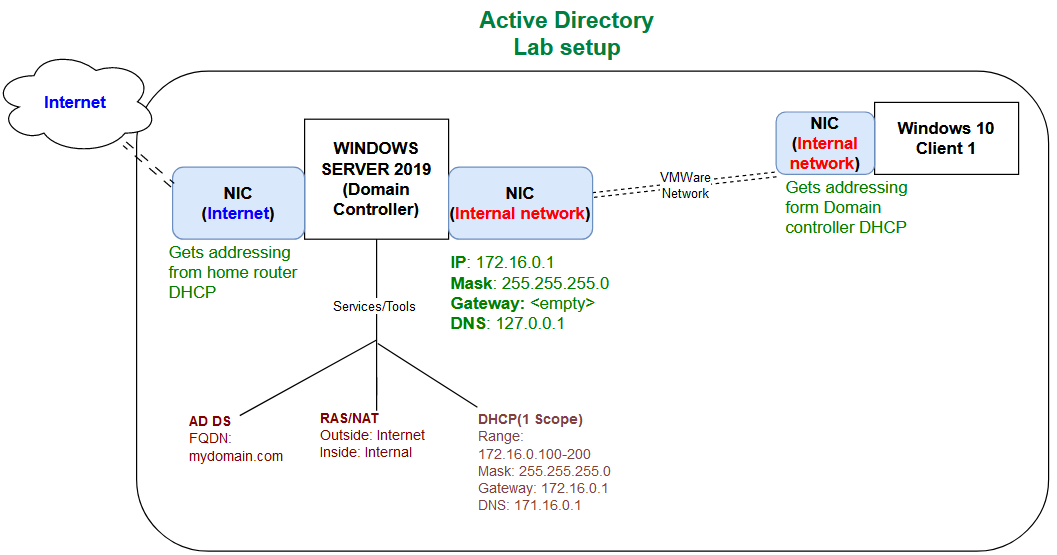
**Beginners guide to creating Active Directory and Adding users**

AD is a database and set of services that connect users with the network resources they need to get their work done.

Learning how to create an Active Directory(AD) is crucial as it serves as the foundation for managing and organizing network resources, ensuring efficient user management, centralizing security controls, and enabling seamless collaboration across an organization's IT infrastructure.

This article aims to demonstrate a step-by-step process of creating AD in a Windows Server 2019 Virtual machine.

**Table of Contents**



**Requirements**

Windows server 2019 iso https://www.microsoft.com/en-us/evalcenter/download-windows-server-2019

Windows 10 iso https://www.microsoft.com/en-us/software-download/windows10ISO

Oracle VirtualBox https://www.virtualbox.org/wiki/Downloads

Create Accounts Scripts https://codeload.github.com/joshmadakor1/AD\_PS/zip/refs/heads/master

**Outline**

We will be using VirtualBox to run Windows server 2019 iso and windows 10 iso as two separate virtual machines.

Windows server 2019 VM will be our Domain Controller hosting the Active Directory. It will have two Network Adapters, one connecting to the internet and second one connecting to internal network in our VirtualBox that our domain clients (using Windows 10 VM) will connect to. We will setup DHCP server on the domain controller’s network adapter that will be used to provide addressing to clients in the internal network

Windows 10 (Client 1) VM will be connected to Internal network in VirtualBox and will receive its addressing from the DHCP server we created in Windows server 2019, our domain controller.

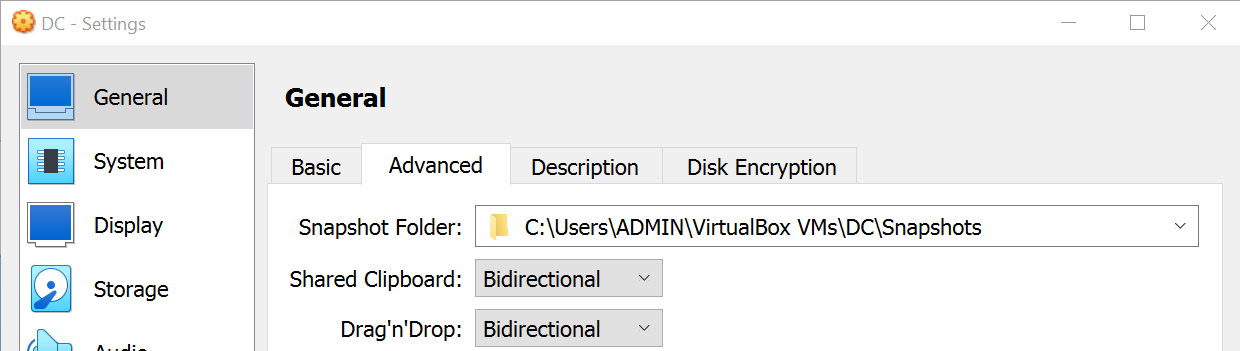
We will create client accounts both manually and using PowerShell scripts in the AD and use them to login into the domain using our Windows 10 VM

**Setting up Domain Controller Network Adapters (Windows server 2019)**

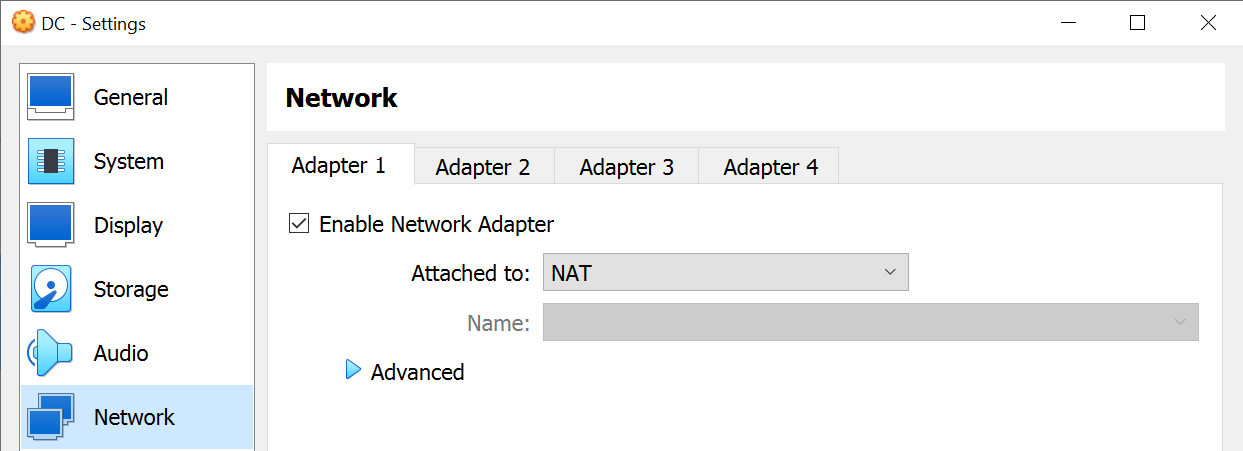
This article assumes you already know how to create VMs in VirtualBox. I will skip that part and concentrate on setting up the AD.

Right Click on Domain Controller VM (Windows server 2019) you created using the ISO and select **Settings**

Under **Advanced** tab in General Settings, change the settings of Shared Clipboard and Drag’n’Drop as shown below. This will enable us to easily copy and past the scripts between out local computer and VM



In the **Network** settings, **Adapter 1** should be attached to **NAT**. Network Address Translation(NAT) allows multiple devices on a local network to share a single public IP address when communicating with devices on the internet. It will enable our domain controller VM to use adapter 1 to connect to internet using the local machine address.

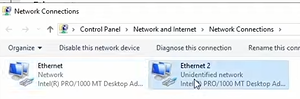


Setup **Adapter 2** of the domain controller to be attached to **internal network**. Our domain controller(Windows server 2019) will host the DHCP server that addresses the clients in the internal network

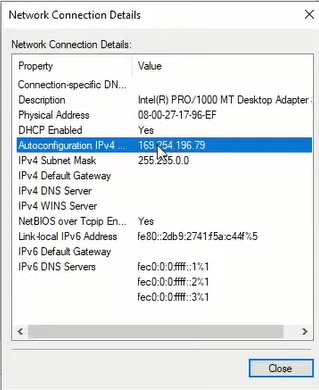
After all this is done, click OK and Power on the Domain controller VM

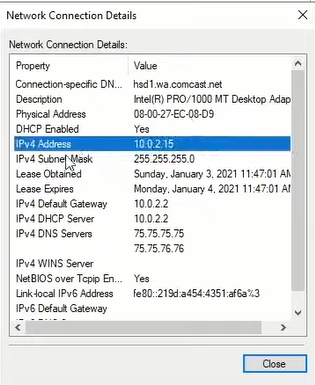
**Setup Domain Controller’s IP address on the Network Adapters**

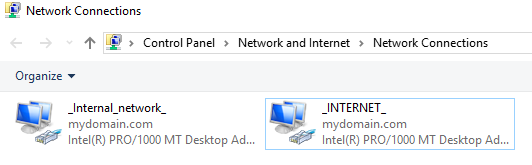
Remember we have two Network Adapters with adapter 1 connecting to the internet and adapter two connecting for connecting to the internal network created during setting up the Domain Controller VM. Open Windows Settings, Network & internet then select **Change adapter options**

Rename them accordingly so that we can easily identify them when setting up our AD.

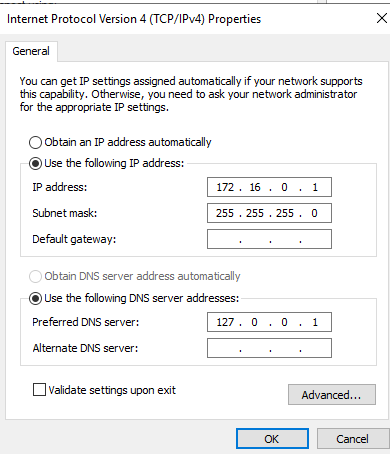
The adapter assigned IPv4 address by our local machine is the internet connection while the Autoconfigured IPv4 address is the internal network. Right click on the any adapter, then select **status** then click on **Details**





Renamed connections

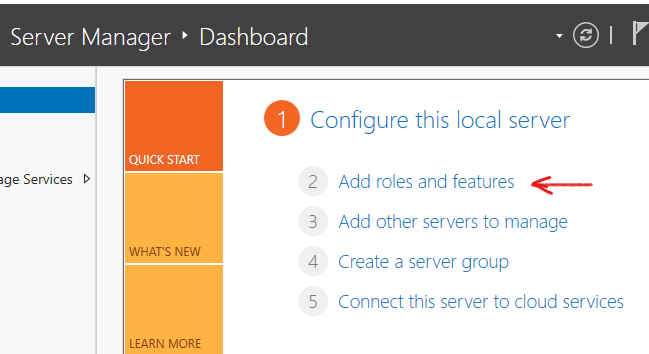
Assign our Internal Network address IP address. Right click on Internal Network adapter, select **Properties** then click on **Internet Protocol Version (TCP/IPv4).** Input the addresses as shown in the Lab setup diagram and apply the changes.



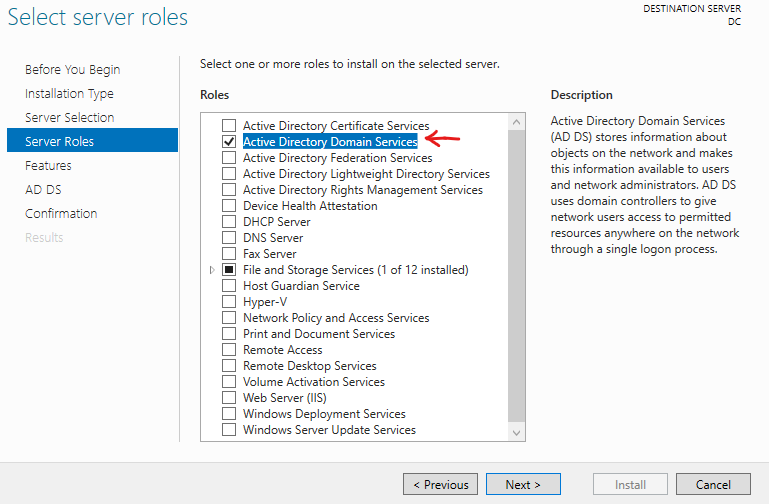
Rename the PC into a recognizable name for example DC for domain controller. Right click on **Start** and select **System** then rename your VM. Let the VM start to effect the changes.

**Installing Active Directory Domain Services (AD DS)**

Open **Service Manager** dashboard and click on **Add roles and features.**



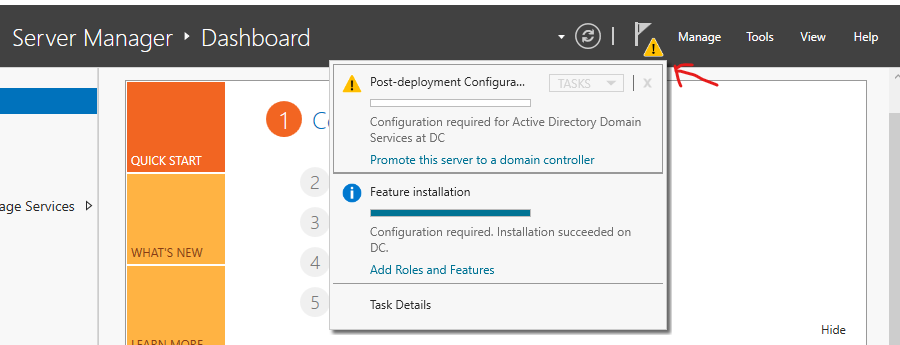
In the Add roles and features wizard, the first three steps are left at default. Make sure you select our server in **Server selection** step then click **Next**

****

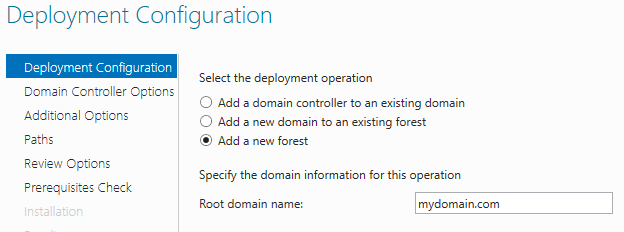
Select **Active Directory Domain Services** and add features then click **Next**

The proceeding steps are left at default then we click on **Install.** Let the installation process finish then close the wizard.

We now have Active Directory Domain Services installed but we now have to do post deployment configuration. Notice the flag icon that has been raised on the top right corner of the service manager window. Click on **Promote this server to a domain controller**



Under **Deployment Configuration** select **Add new forest** then give the domain a name of your choice



Under **Domain controller options** in the wizard, ensure to input a password that you will remember for Directory Services Restore Mode then click next. The proceeding steps are left at default as they are then finally click **install.** You will be signed out once the process I complete

Our default local VM Administrator account is now in our created domain, **MYDOMAIN\Administrator**



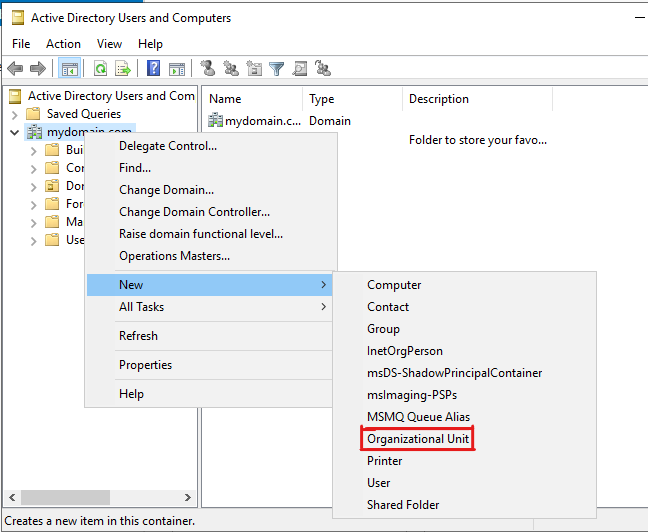
Input your password and log in

**Creating Admin user account**

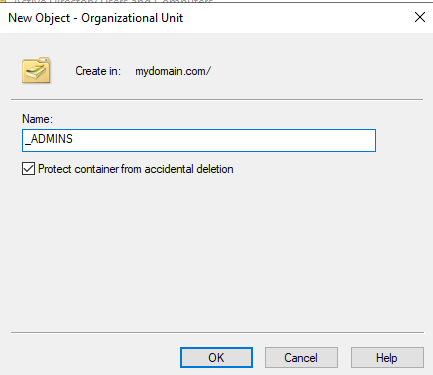
We are going to create our personal account instead of using the default domain administrator account.

Under the Windows Administrative Tools in Start menu, select **Active Directory users and computers**

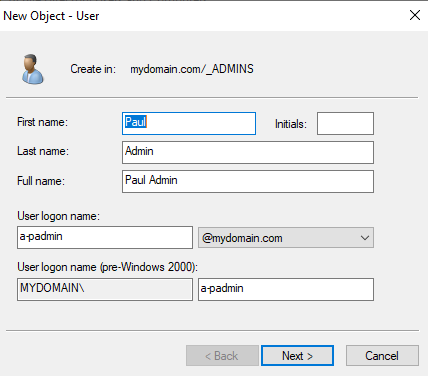
We are going to create a new **Organizational unit** to put out admin account in. The unit is a folder that will contain admins in our domain. Right click on our domain, then click on Organizational unit under new.



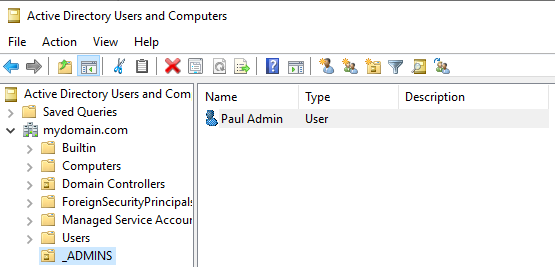
Give the Organizational unit a name i.e **\_ADMINS** and click **ok**



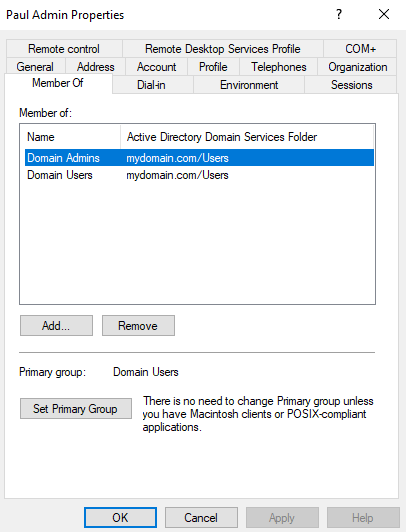
Now that we have the folder set, right click the it and create new **User.** Creating new user is quite straight forward. Input your first, last name and your user logon name. The next step you input your password. Since this is a lab setup for our experimental use, select **password never expired** , then finish the setup.



Lets give administrator rights to the user we have created



Right click on the user and click on **Properties**. Under **Member of** tab, click on **Add..**. We need to assign **Domain Admin** rights to the user we created. Write domain admin on the text field then click on **Check Names** then click OK. You will notice Domain admin has been added to **Member of.** Now the user we created is admin with domain admin rights.

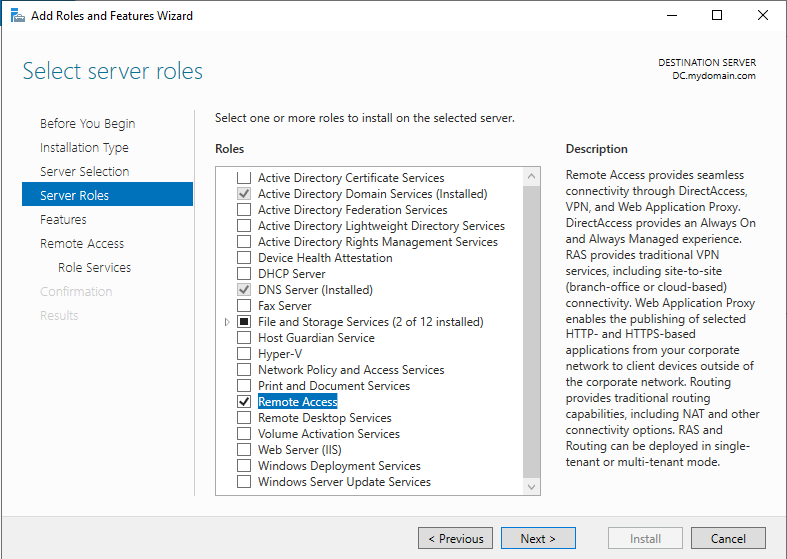


Logout and sign in with the user logon name and password we created.

**Setting up NAT (Network address translation)**

We are going to setup NAT in order to allow our clients in the internal network to access the internet via the domain controller. NAT allows multiple devices on a local network to share a single public IP address when communicating with devices on the internet.

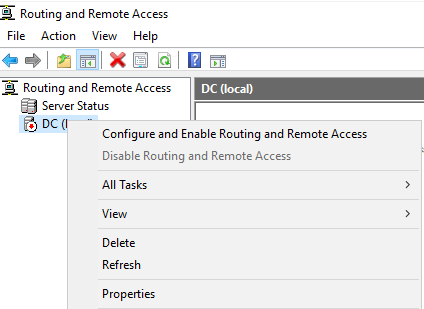
Open **Service Manager Dashboard.** We are going to add **Remote Access** feature. Click on **Add roles and features.** Under server roles in the wizard, select **Remote Access** and click Next



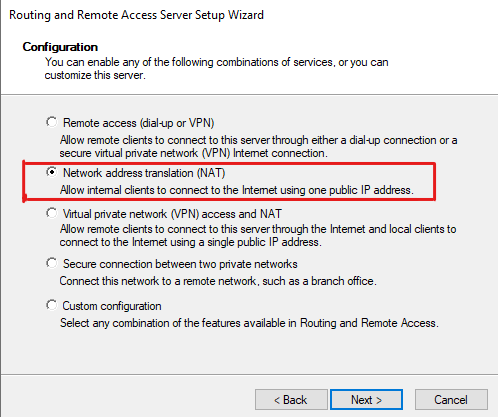
The proceeding steps are left at default as they are. Under **Select roles and services** in the wizard, select **Routing** then add features. **DirectAccess and VPN (RAS)** will be automatically selected in the process. Then click next and Install the new features.

Once the installation is completed we have to configure it. Select **Tools** on the top right corner of the dashboard then click on **Routing and remote access**

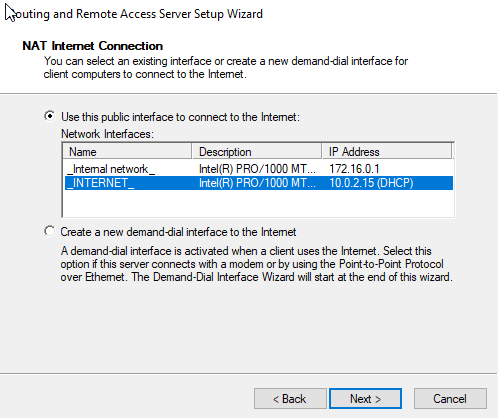
Right click on the domain controller’s name, in my case I renamed my PC to DC. Then click **Configure and Enable Routing and Remote Access** to initiate the setup wizard.



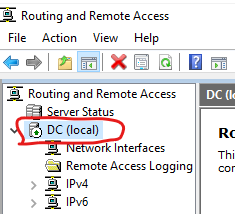
Under configuration select **Network Address Translation (NAT)**



In the next step under “**Use this public interface to connect to the internet”** select the network adapter that connects to the internet. Recall we renamed it earlier during setting up the networks



After clicking finish, our NAT will be configured and running. This can be seen by the small green play icon on local VM name



**Setting up DHCP server**

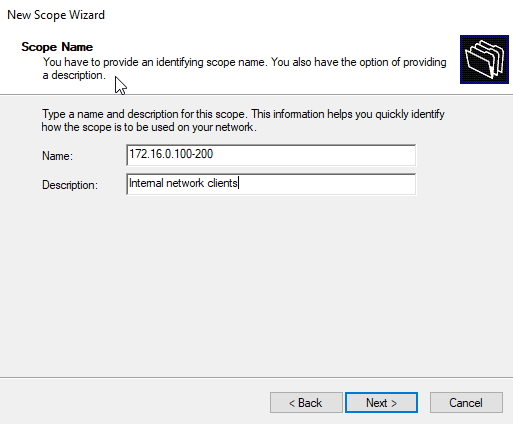
To enable other clients get addresses to join the internal network, we will setup the DHCP server.

Open **Server manager** Dashboard and click on **Add roles and features**.

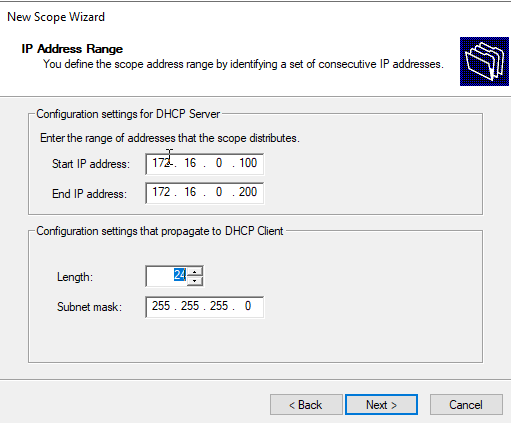
Under Select server roles step, select **DHCP** and add features then click Next then finally click **Install**

After the installations, Click on **Tools** on top right of Dashboard and select **DHCP**

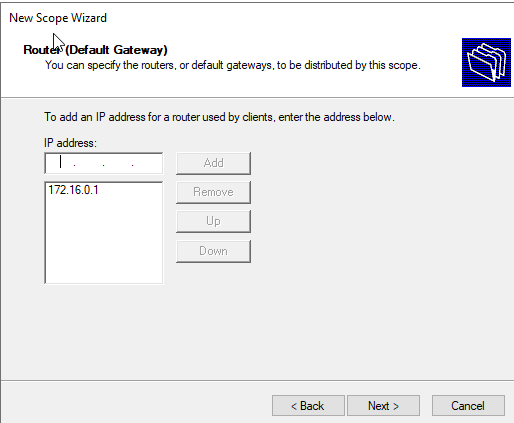
We are going to create a **Scope** of IP addresses that will be assigned automatically to new clients in our internal network. Select on our domain then right click on **IPv4** then click on **New Scope**. Give the scope the name of your choice for example



Configure that IP address range as shown below

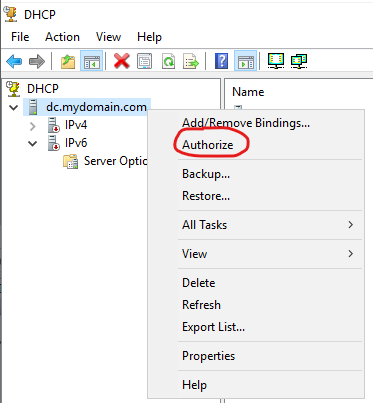


Click Next steps are left on default as they are. On **Router (Default Gateway),** we will add the address of the Domain Controllers internal network we set earlier **172.16.0.1.**

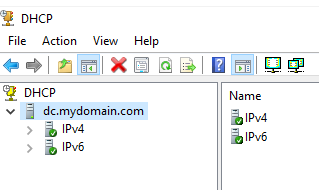
****

The remain steps are left as they are. Click **Finish**

Right click on DHCP server we created as shown below and click on **Authorize**. Then right click and click on refresh. This will enable the server to run in our domain. The icon will turn green when the operation is successful



Now the DHCP serve is in our domain



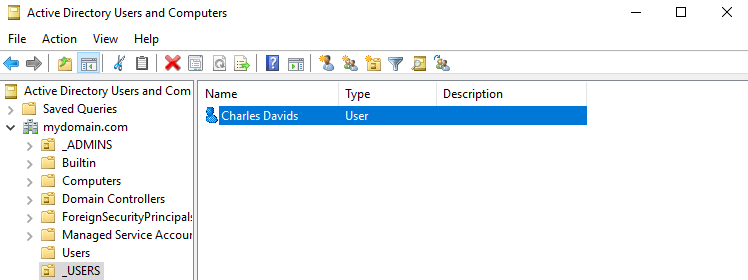
**Creating users**

Creating users follows the same steps we used when creating our domain admin in step **X X X X .** Follow the steps to create several users. We will use the created users to log in into the domain using a separate window 10 VM created.

For this lab experiment, we will not assign a group to users created but they will have ability to login into the domain using a VM in the internal network. You will learn more about creating groups ,roles and assign to users as you advance your knowledge in AD

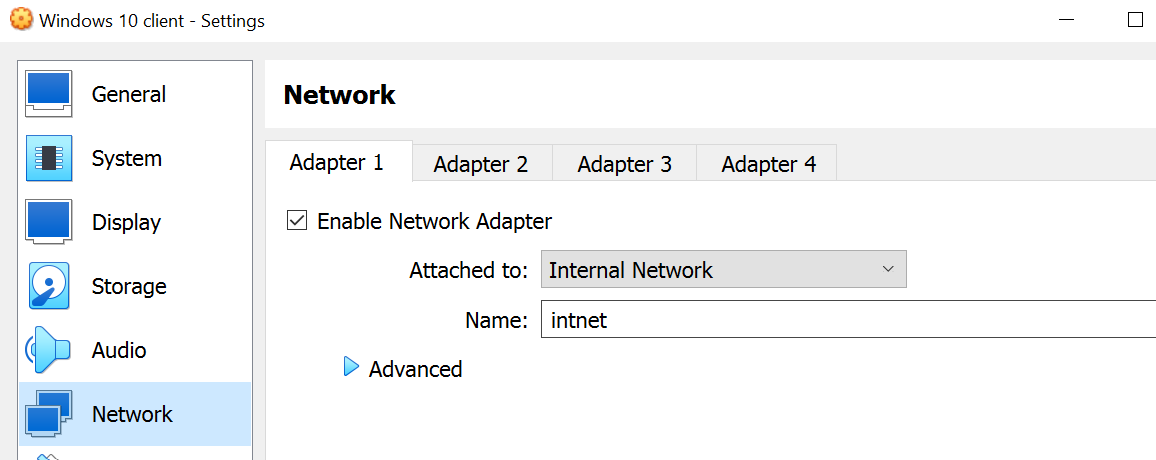
I created a user Charles Davids under **\_USERS** organizational unit with logon name **u-cdavids**.

In this article **XXXXXX**, I will demonstrate how to add many users automatically using PowerShell script.



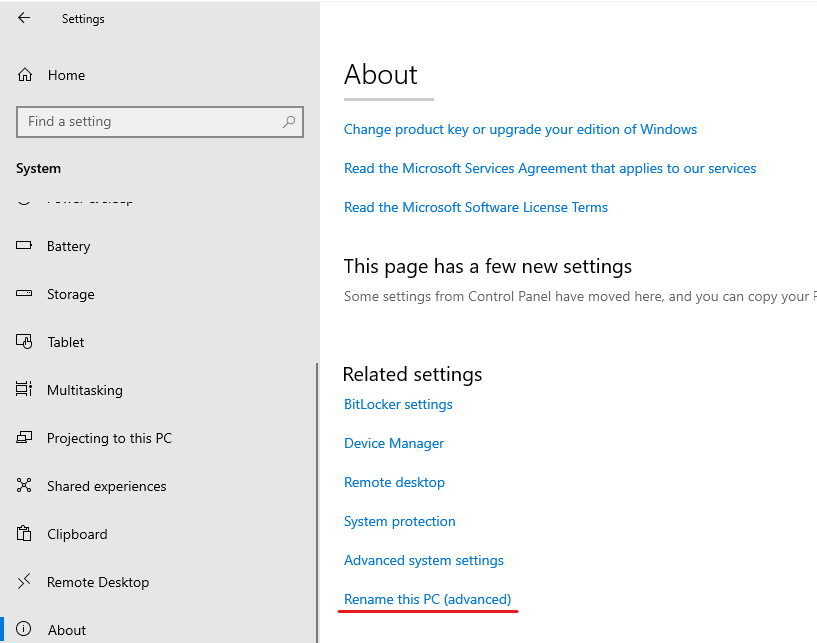
**Configuring the Client VM and Logging into the Domain**

Now that we have our client account setup in the domain, we will use a VM in the internal network to log in. Right click on the Windows 10 VM you created and apply the below setting under Network. Click OK then start the VM.

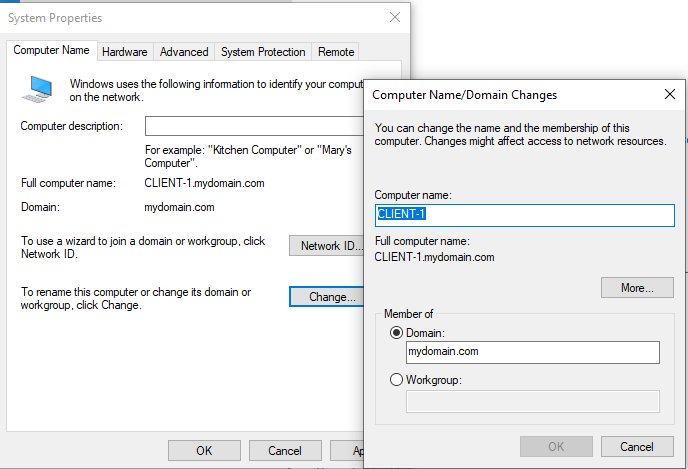
****

Since it is a **fresh install**, you will be required to create an initial account to login the VM.

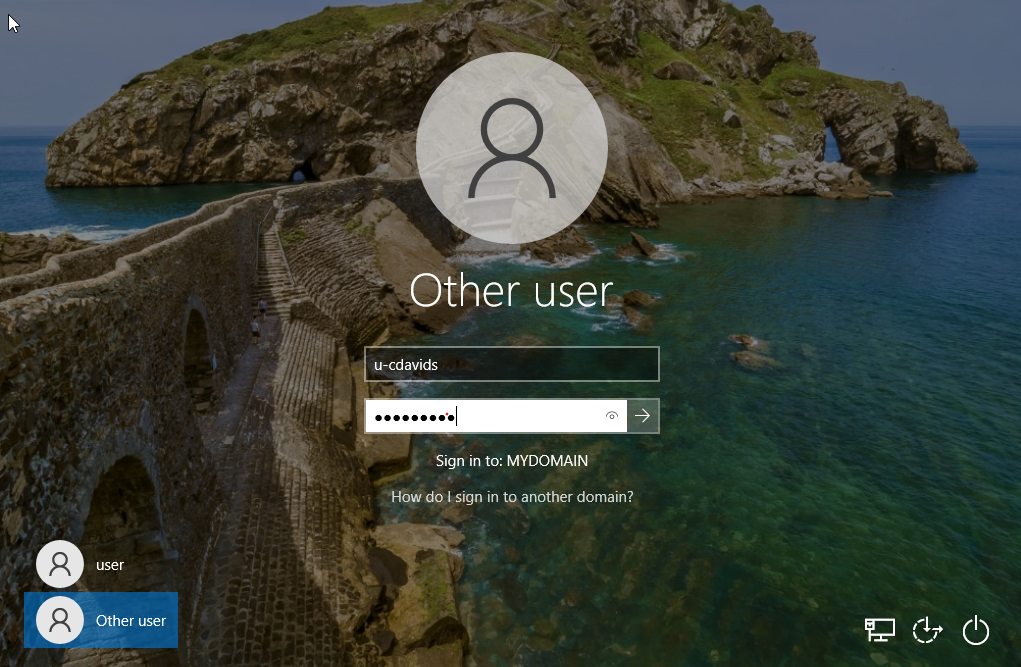
**Rename the Client VM** and add it into the domain. In **settings,** click on **System** then select **About.** Scroll down and click on **Rename this PC (Advanced)**



Under System Properties, click on **Change** button then rename the computer to client-1 and enter our created domain name. You will be required to input username and password to effect the changes and add the computer into the domain. Input the Admin credentials we created on step **X X x x.**

****

Restart the client VM then login into our domain as a **other user** with the credentials (**u-cdavids**) we created in Domain Controller



**CONCLUSION**

This is a beginner’s level article that has demonstrated the process of creating an Active Directory and adding users. You have learnt the basic networking in AD and how to create DHCP server and routing client’s internet traffic via NAT.

I hope this has been an interesting journey into learning Active Directory. **Share the article and follow me for more interesting step by step tutorials in technology !**