Setting up an Active Directory Lab using Hyper-V Virtualization Platform

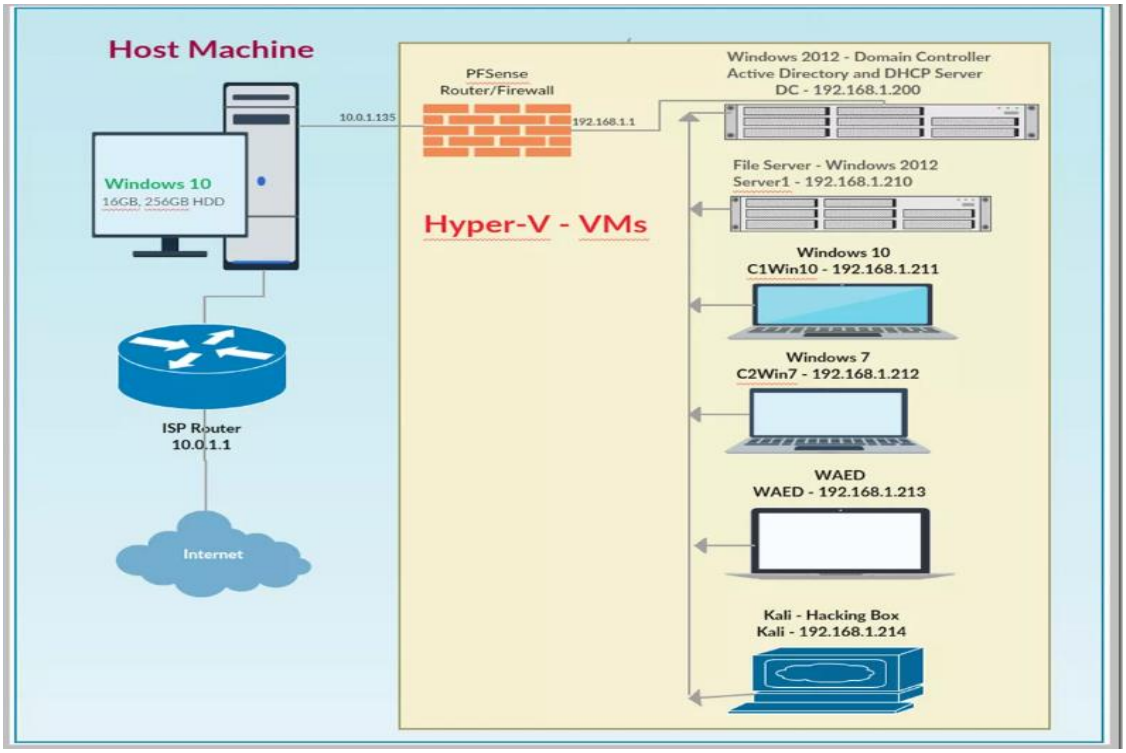
Rajganesh Pandurangan

Table of Contents

1. Introduction
2. Adding Hyper-V Role in Windows 10
3. Setting up Virtual Switches in Hyper-V
4. Installing Windows 2012 Server
5. Installing Windows 10–64 bit version
6. Installing Windows 7
7. File Server Installation – Windows 2012
8. Installing Routing/Firewall - PFSense
9. Setting up PFSense
10. Promoting Windows 2012 Server to Domain Controller
11. Creating Users in Active Directory
12. Setting Up Static IP in Domain Controller
13. Installing DHCP in Domain Controller
14. Configuring DHCP Server in Windows 2012 server
15. Joining Windows 10 to Domain
16. Joining Windows 7 to Domain
17. Adding FileServer to Domain
18. Viewing DHCP leases in Domain Controller
19. Exporting, Saving, and creating Checkpoints for all VMs
20. Protect you host computer

1. Introduction

Setting up a secure active directory lab is an uphill task for any newbie IT professionals, but it's an absolute requirement to have a playground for practicing the skills in a controlled manner. This manual is one of the most authoritative and detailed step-by-step instructions on how to set up an active directory based lab. In this comprehensive series, I'll show you how to install and configure an active directory lab from scratch using Microsoft's free Hyper-V virtualization platform. I decided to move away from VMWare (another virtualization platform), as it was expensive, and one of the challenges I faced was to migrate all the existing labs to Hyper-V. Since I was starting over, I documented the whole process, so anyone trying to accomplish the same goals will be benefited. The entire lab is setup in one machine with an i7 chipset, 16GB ram, and 256 GB SSD configuration. All the internal lab machines will have full internet connectivity. We will provision a firewall between lab network and the host system, which will protect the host from any malware infection by the lab systems. I recommend following the tutorials in the same order as laid out in this manual. At the end, you will have a lab similar to the network diagram below. I'll use the same lab for my other training courses such as how to setup pentest lab, windows event monitoring using Elastic Stack, ethical hacking, advanced windows penetration testing, kali Linux training, etc. I promise that you will learn a lot by following this series, so strap your belts and get ready for an exciting ride!



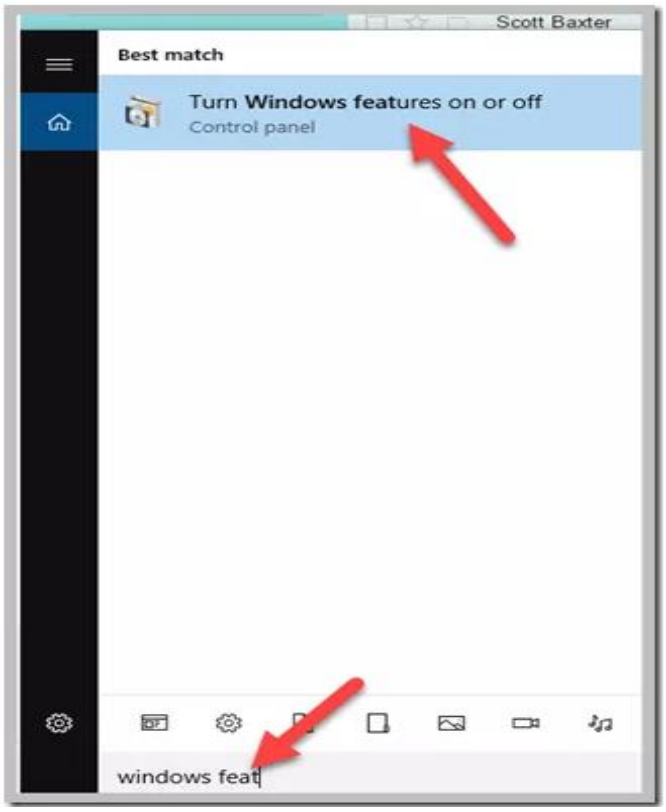
Requirements:

- Windows 10 host machine with at least 8GB Ram

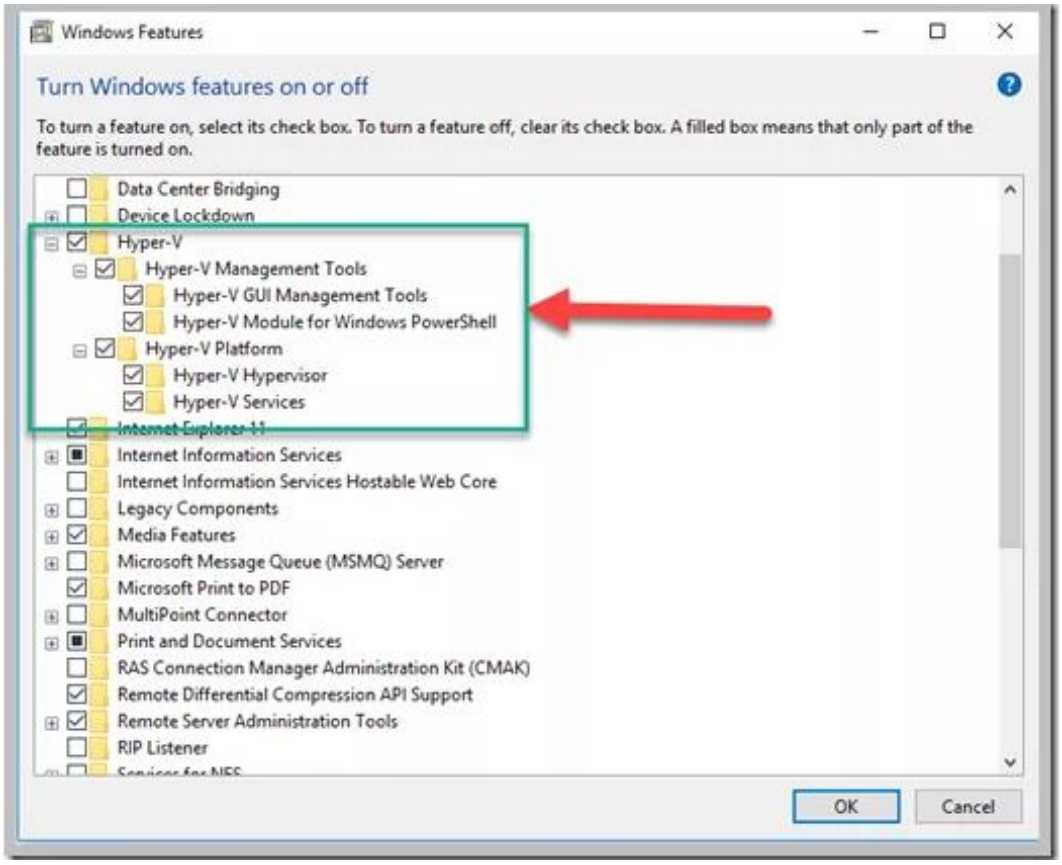
- Windows 2012 Server ISO trial version (https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2012)
- Windows 10 ISO trial version (https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise)
- Windows 7 ISO (I don't know of a trial version. Add two Windows 10 VMs instead)
- Pfsense – Download from http://www.pfsense.org
- WAED (Optional) – Download from https://drive.google.com/open?id=0B_GgpShRlRa2WElnQ2VTUmxlRjA
- Kali (Optional) - Download from https://www.kali.org/downloads/

2. Adding Hyper-V Role in Windows 10

Hyper-V is a pre-requisite for setting up the active directory lab. Before installing Hyper-V, remove VMware/VirtualBox, as it not compatible with Hyper-V. Hyper-V is enabled in the "Turn Windows features on or off" section as outlined below.



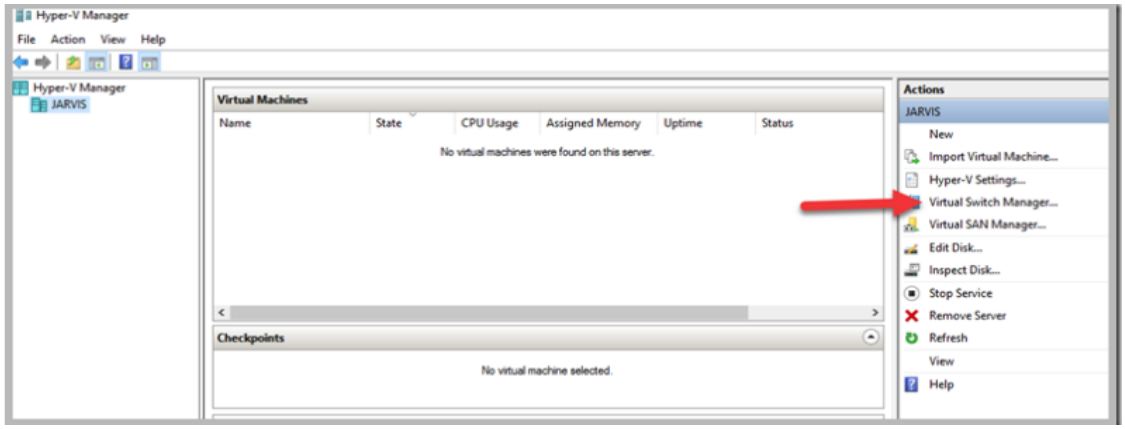
Check all the boxes as shown below, click OK, and restart the machine and Hyper-V should be installed



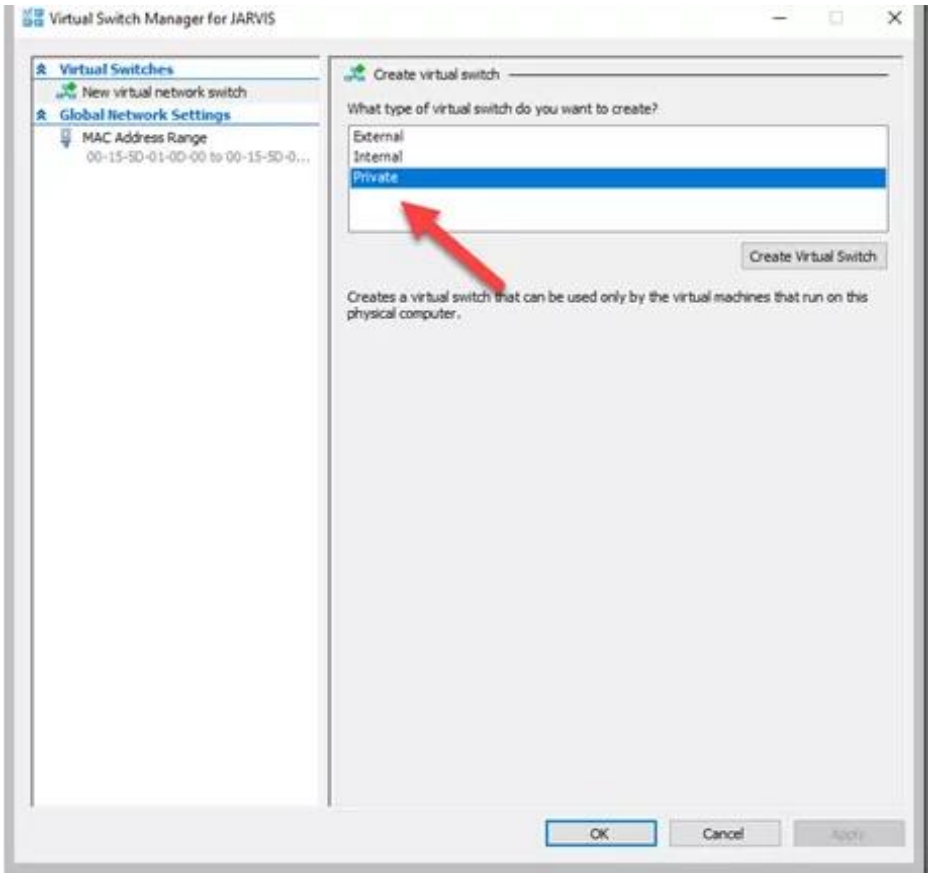
3. Setting up Virtual Switches in Hyper-V

In Hyper-V, we will create two virtual switches "**Private**" and "**External**." The External switch is used for internet connectivity, and the Internal is for internal network communications. PFSense will act as our firewall/router and is used to bridge between the internal network to the internet.

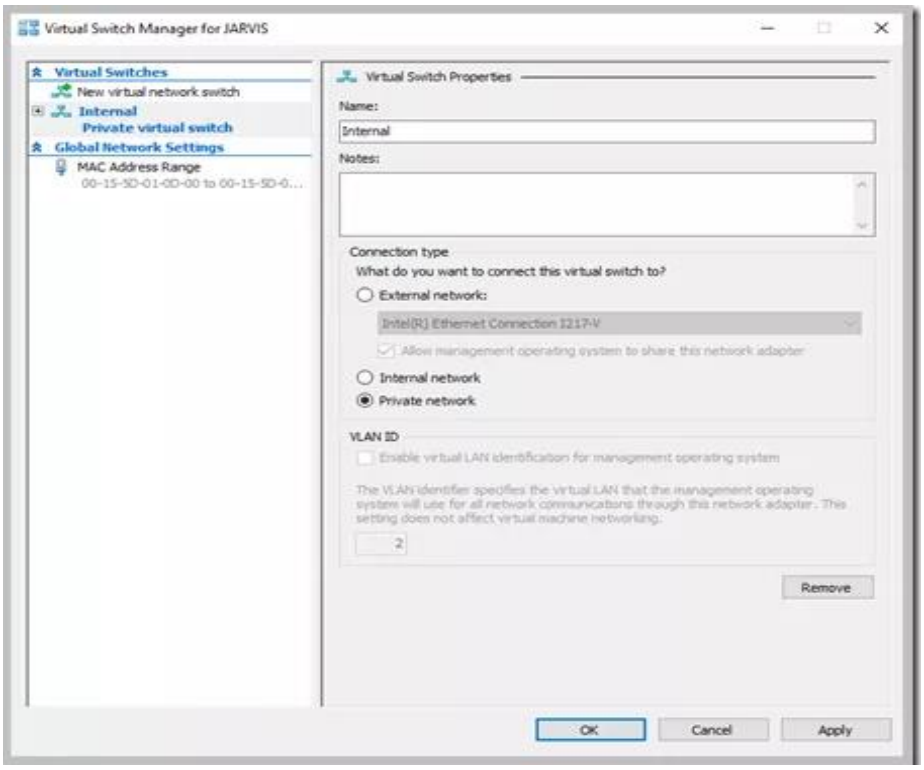
- In Hyper-V, click the 'Virtual Switch Manager' as shown below



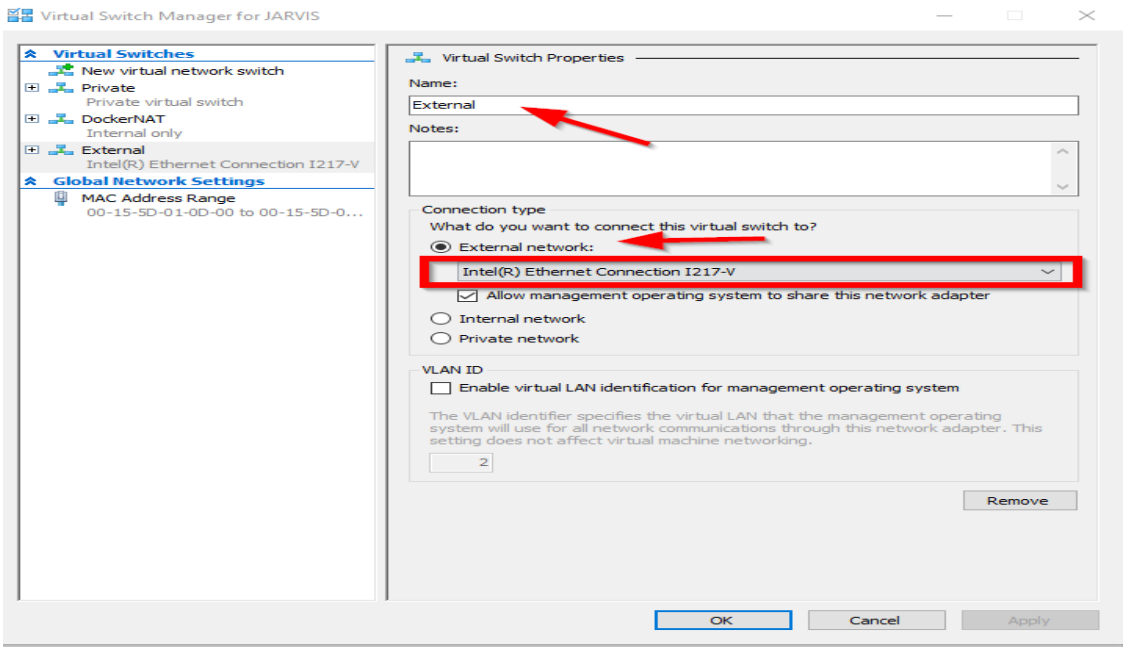
- Select the “Private” and click ‘Create Virtual Switch’ button



- Confirm the “Private Network” radio button is selected. Click ‘Apply’ to create the switch

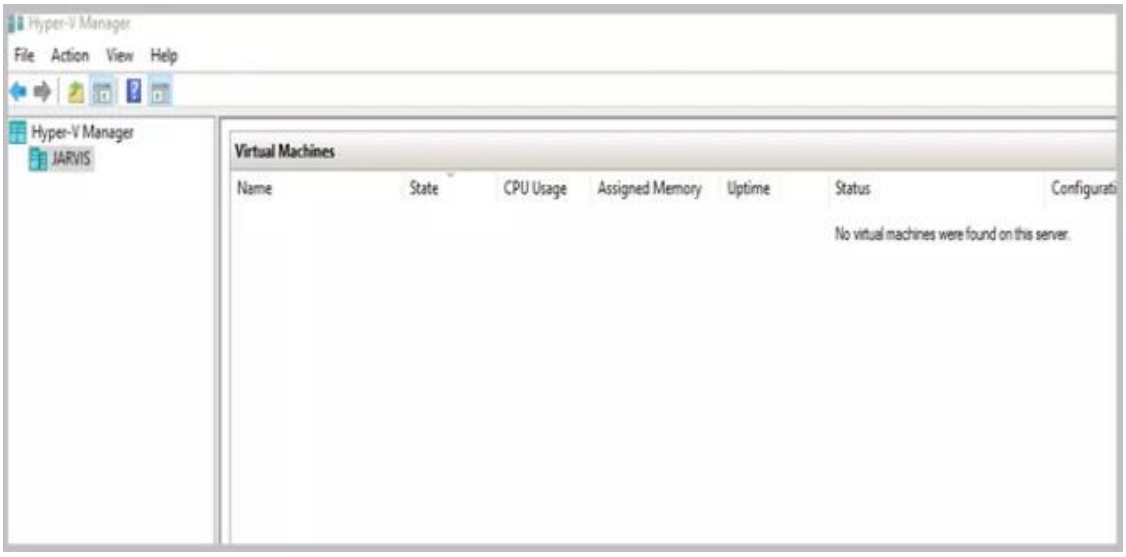


- Repeat the process for creating the "**External**" switch. Make sure to select the correct External network card for External virtual switch.

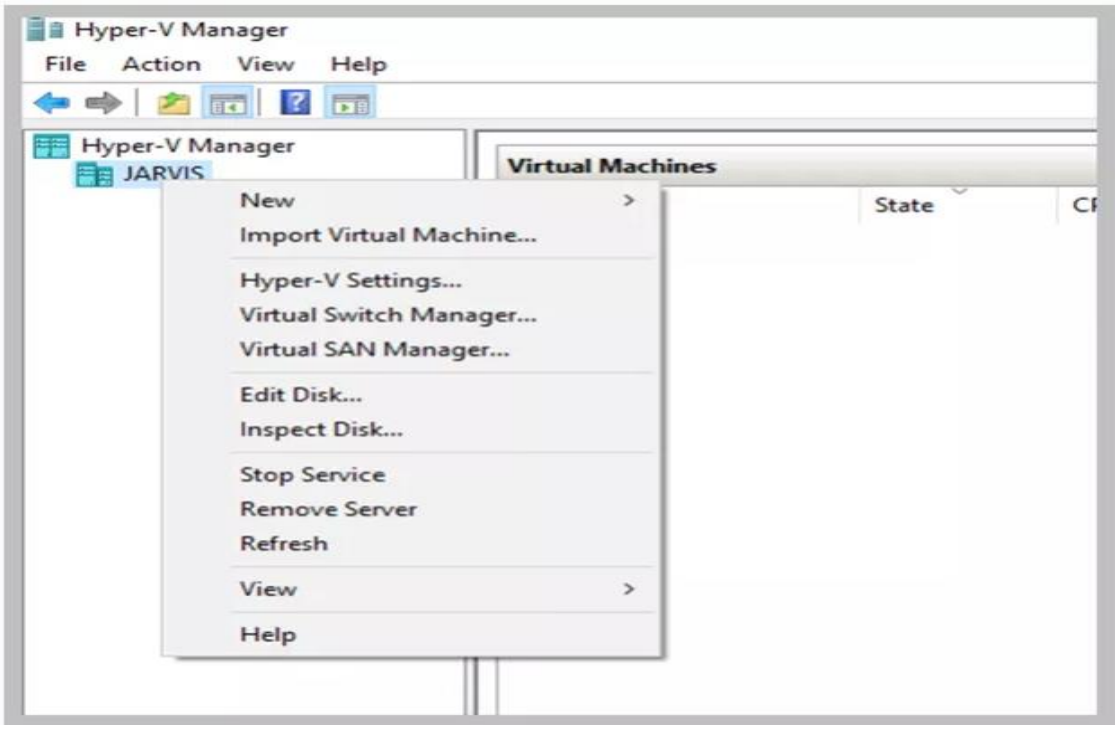


4. Installing Windows 2012 Server

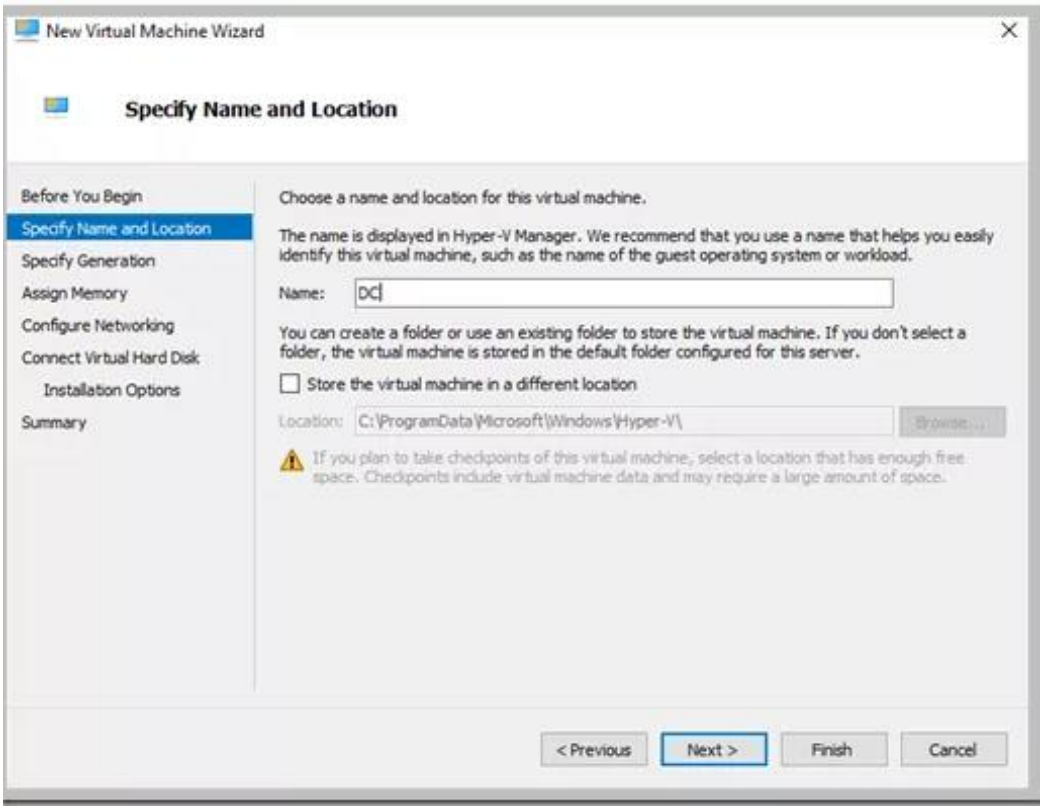
- Open the Hyper-V manager application, and it should have only one host named "**Jarvis**", which is the name of my host machine



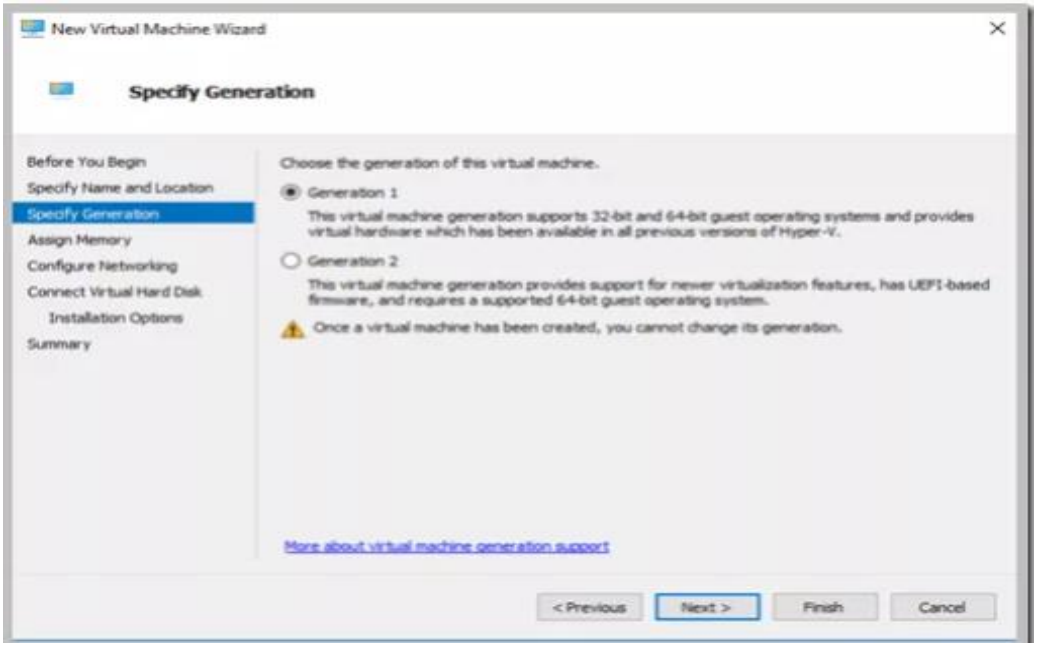
- Right click on "Jarvis" and click "New"



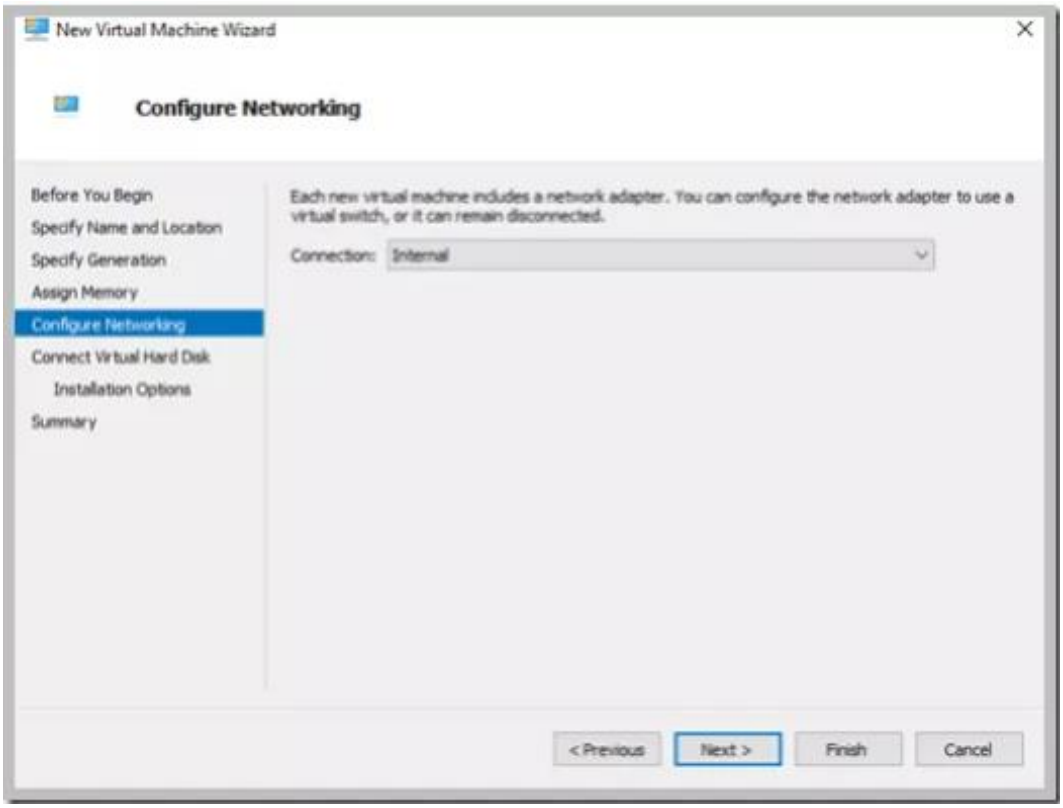
- Name the VM "**DC**". This is how it will be identified in Hyper-V console



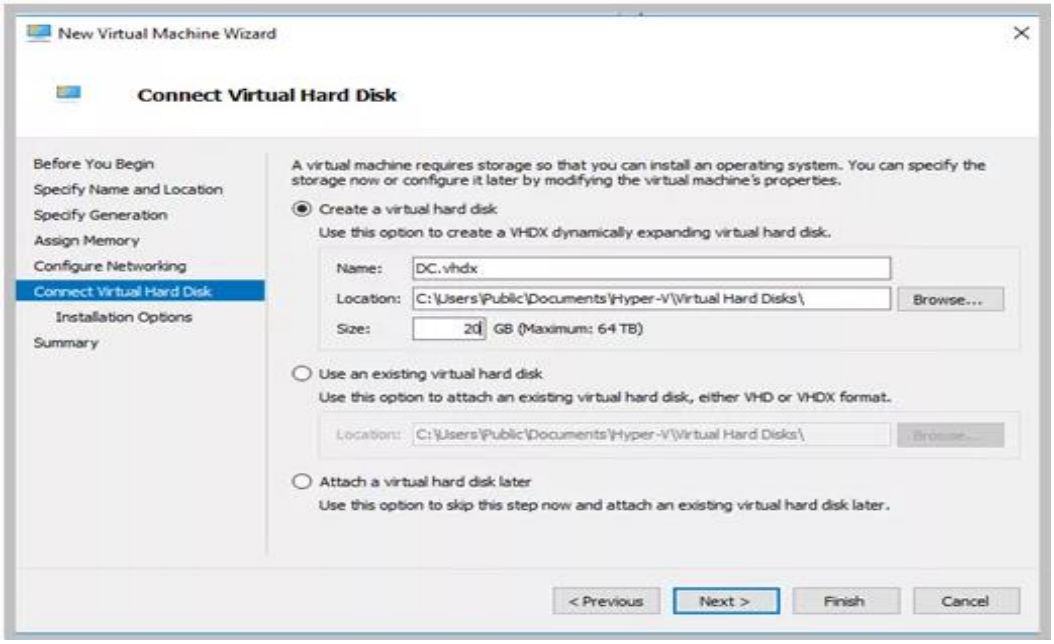
- Pick Generation 1 or Generation 2



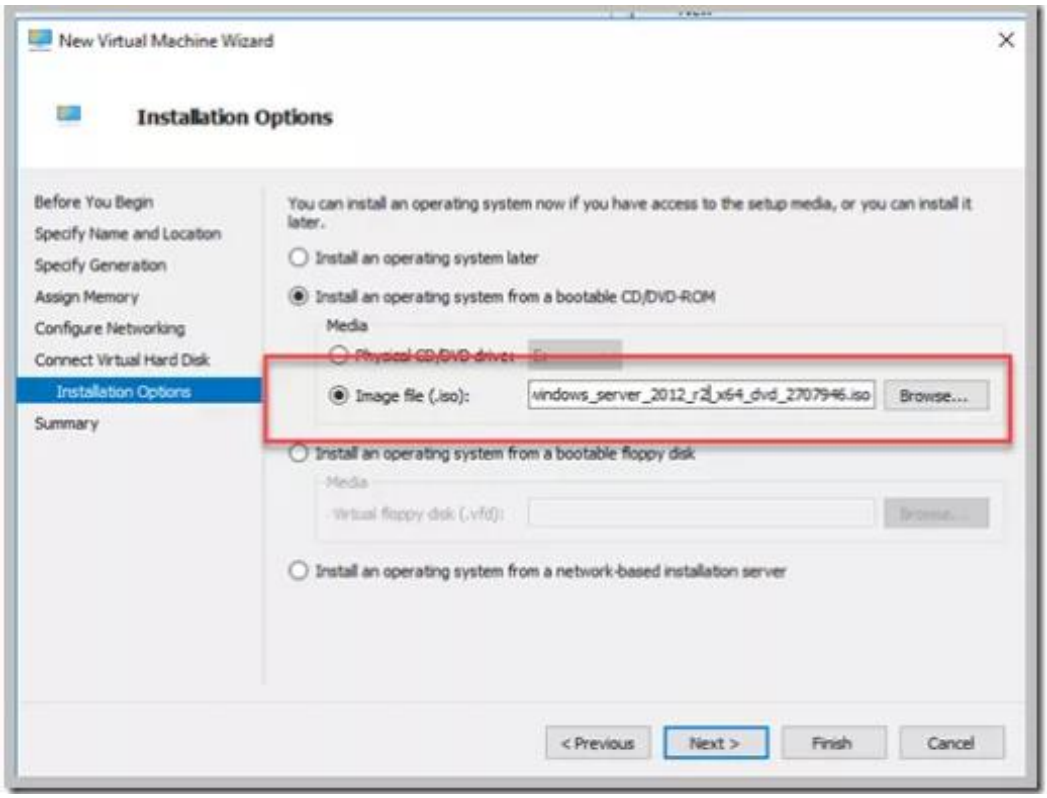
- Pick “Internal” for the network connection



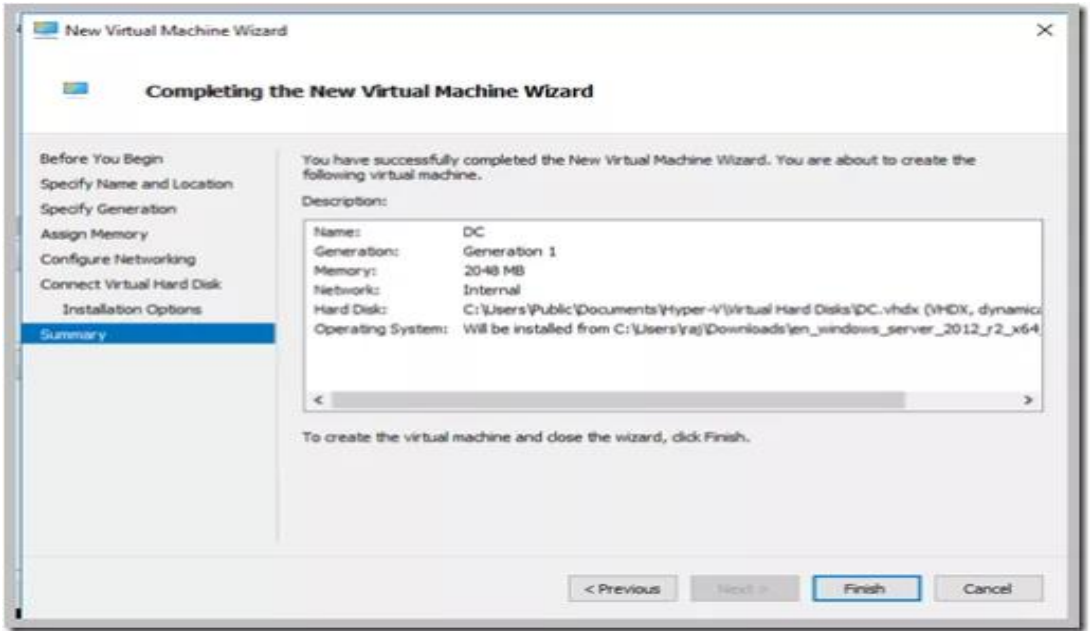
- Use 20GB for the hard drive size



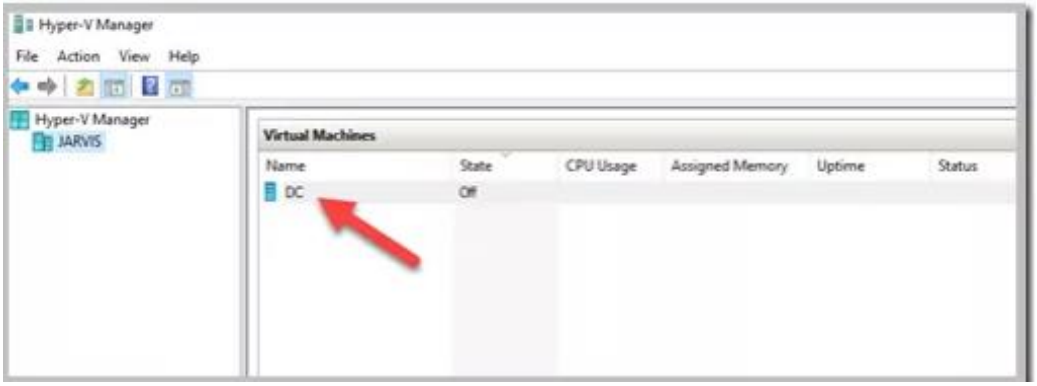
- Choose the location of Windows 2012 iso



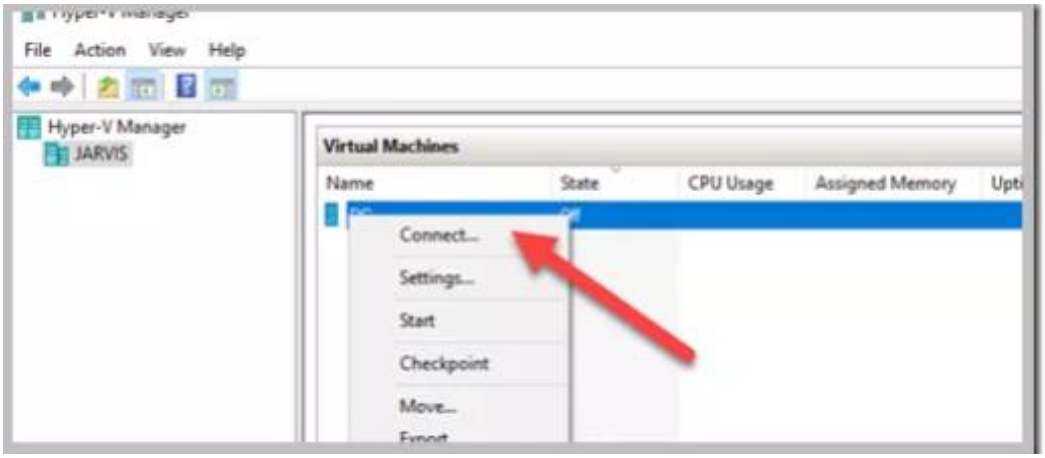
- Review and finish the initial setup process



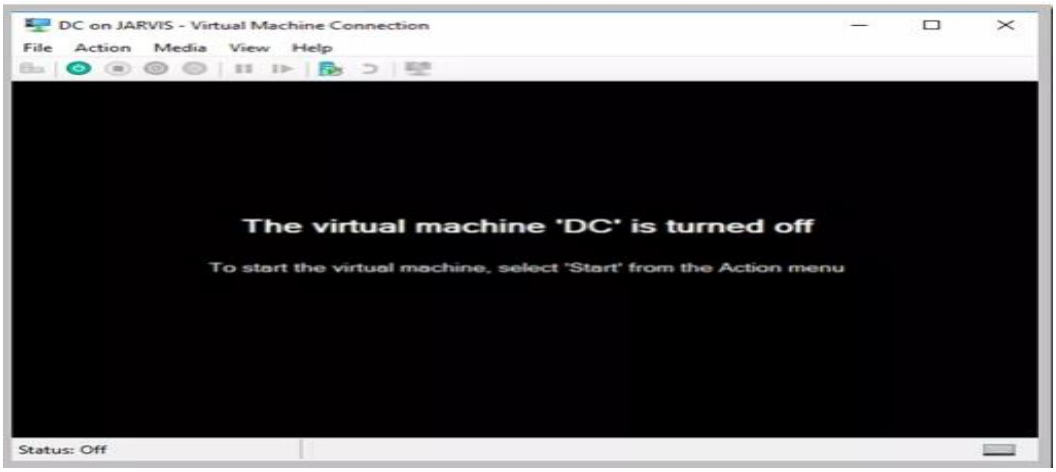
- Now there should be one VM called DC in the list of VM

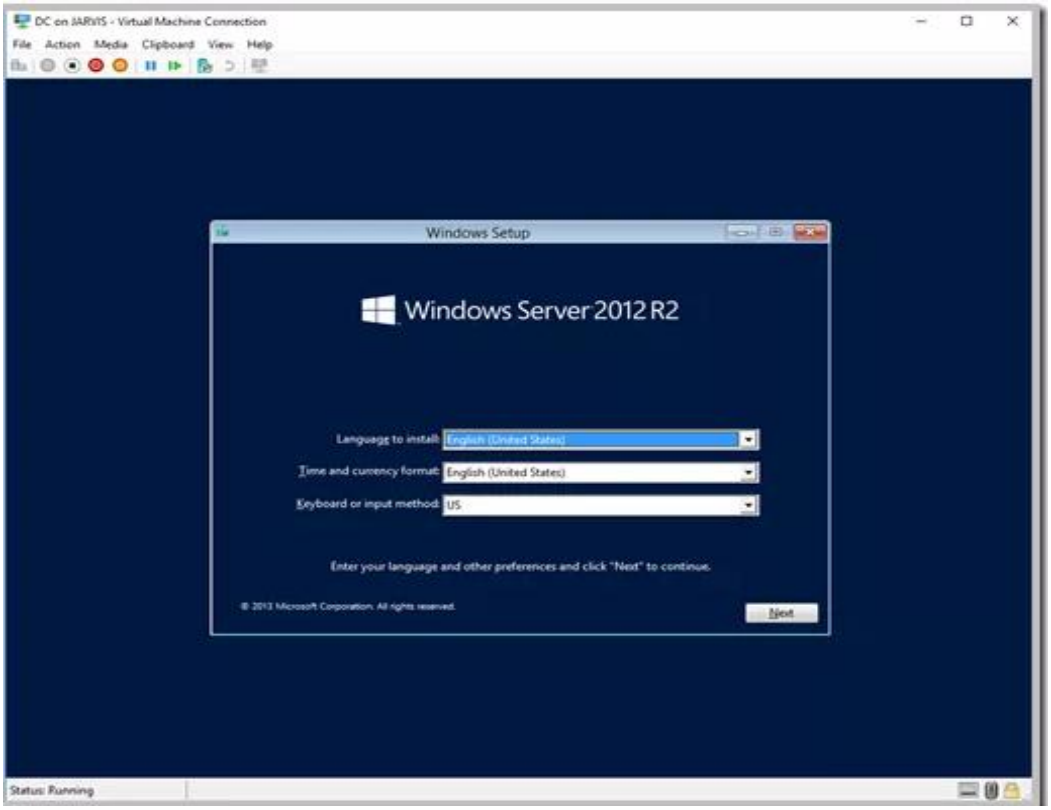


- Right click on “DC” and click “connect”

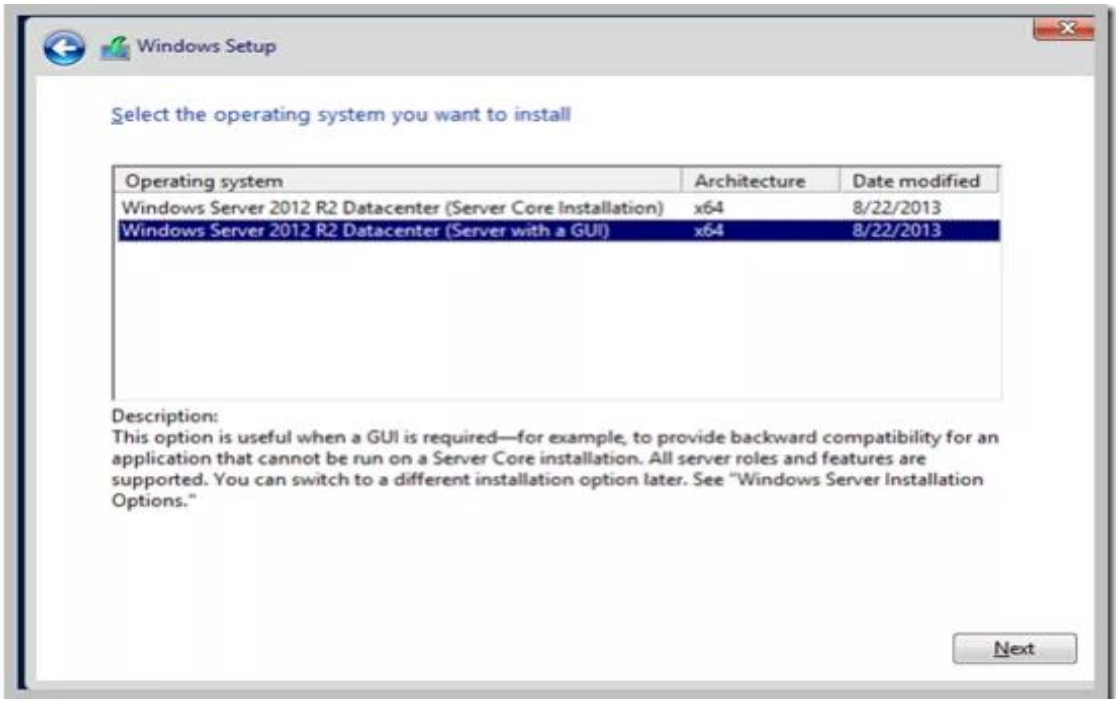


- Click on the Green power button on start the install process

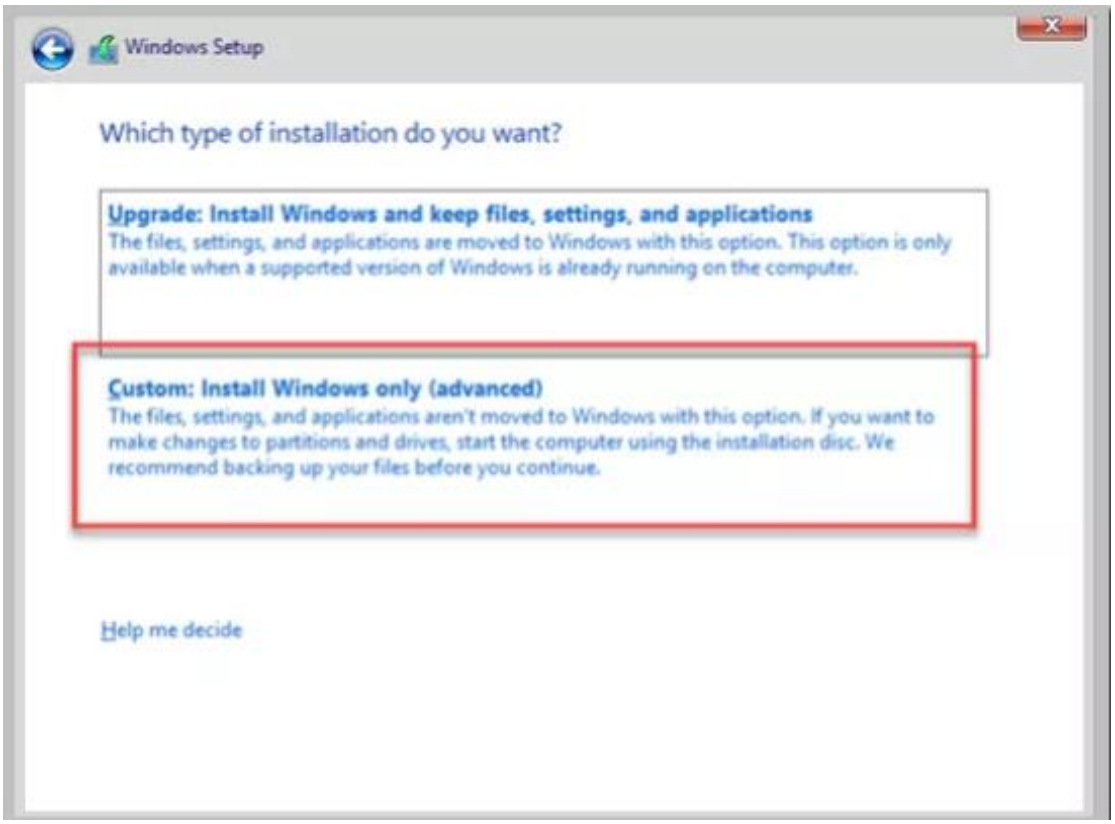




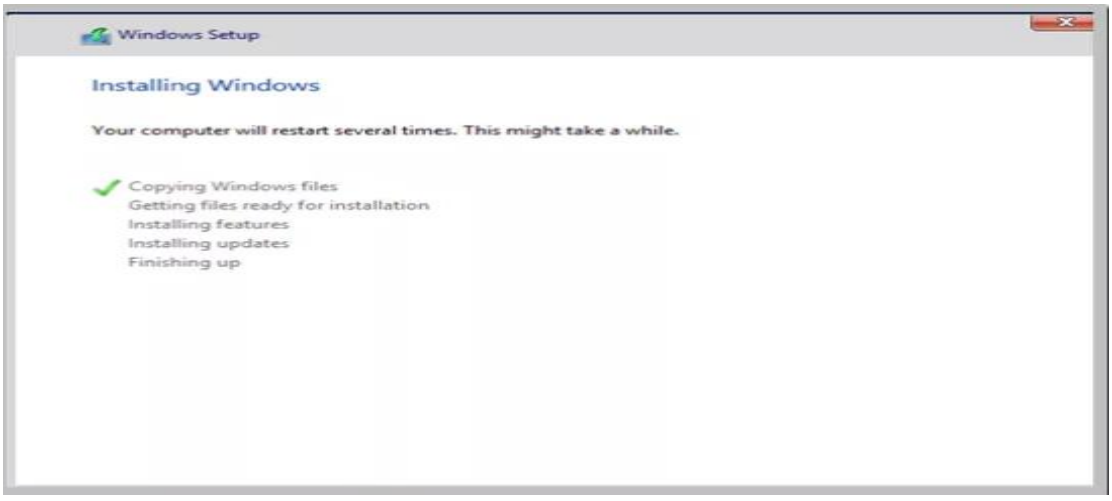
- Choose the option "Server with a GUI"



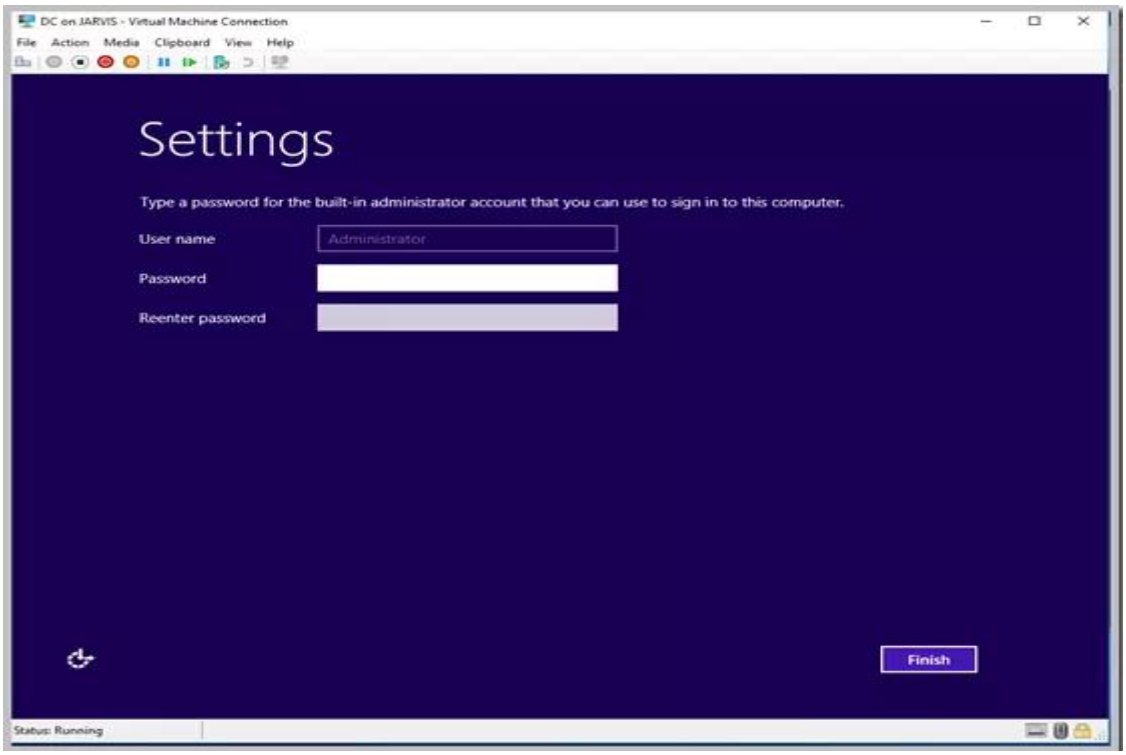
- choose Custom install



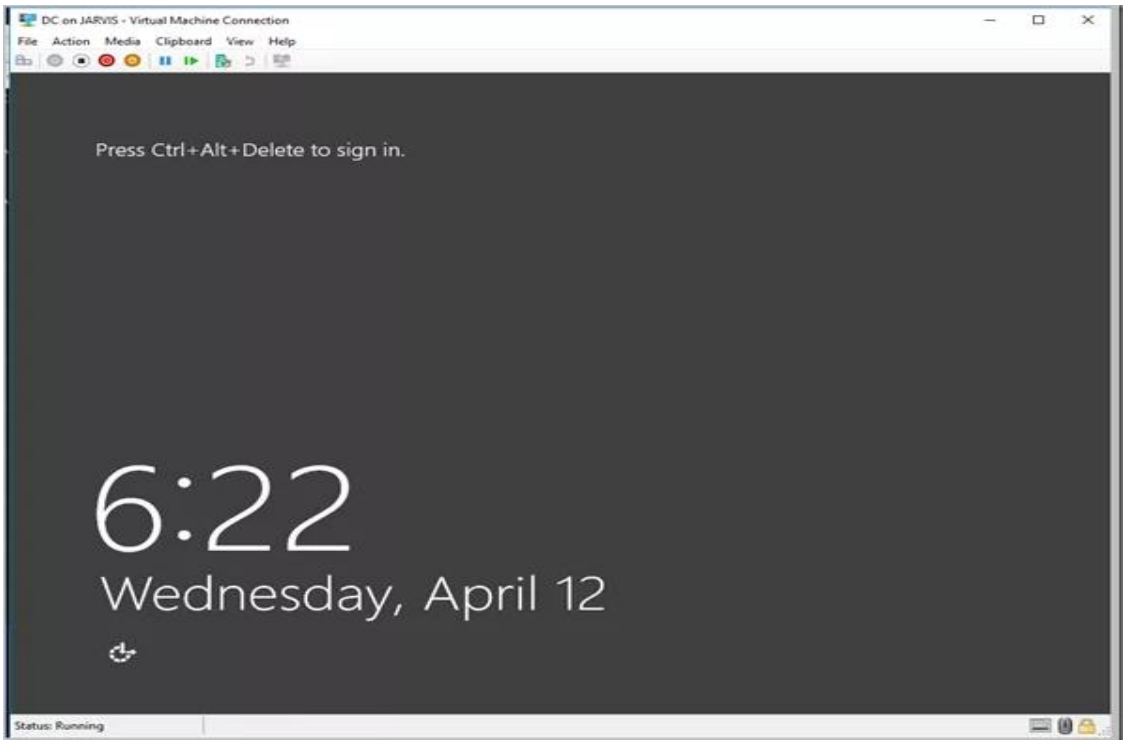
- Wait for the process to complete. it should take around 15 to 20 minutes to complete depending upon the ram of the virtual machine.



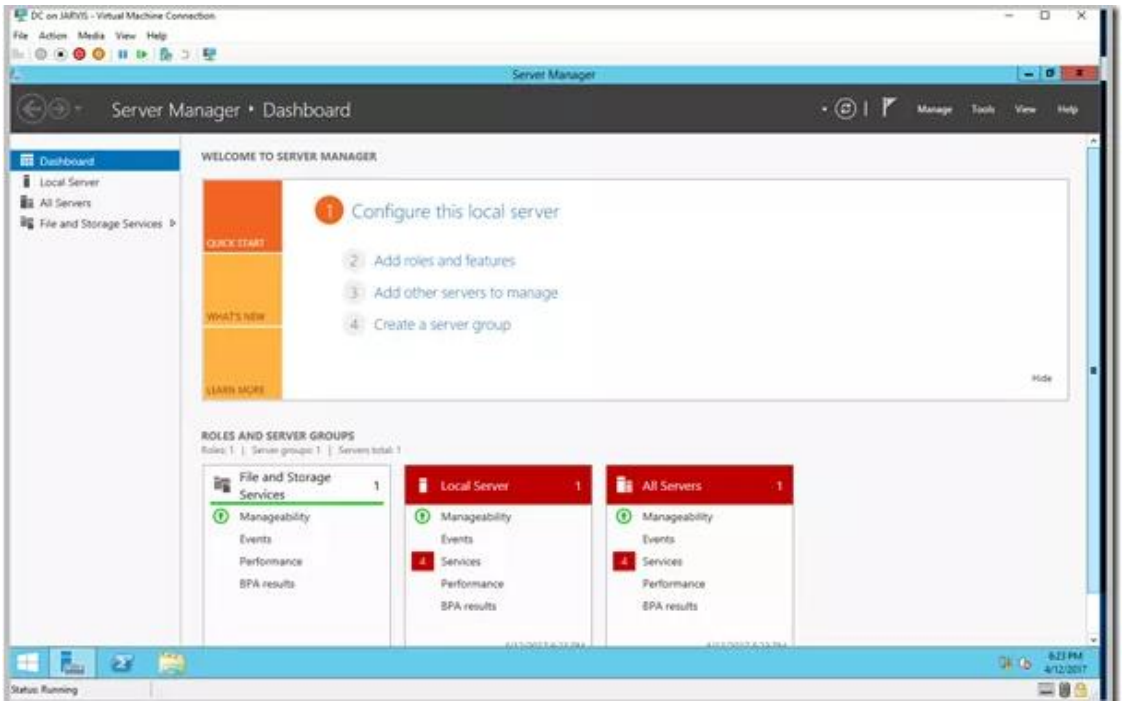
- Choose a strong password. This is the local password of the Windows 2012 system.



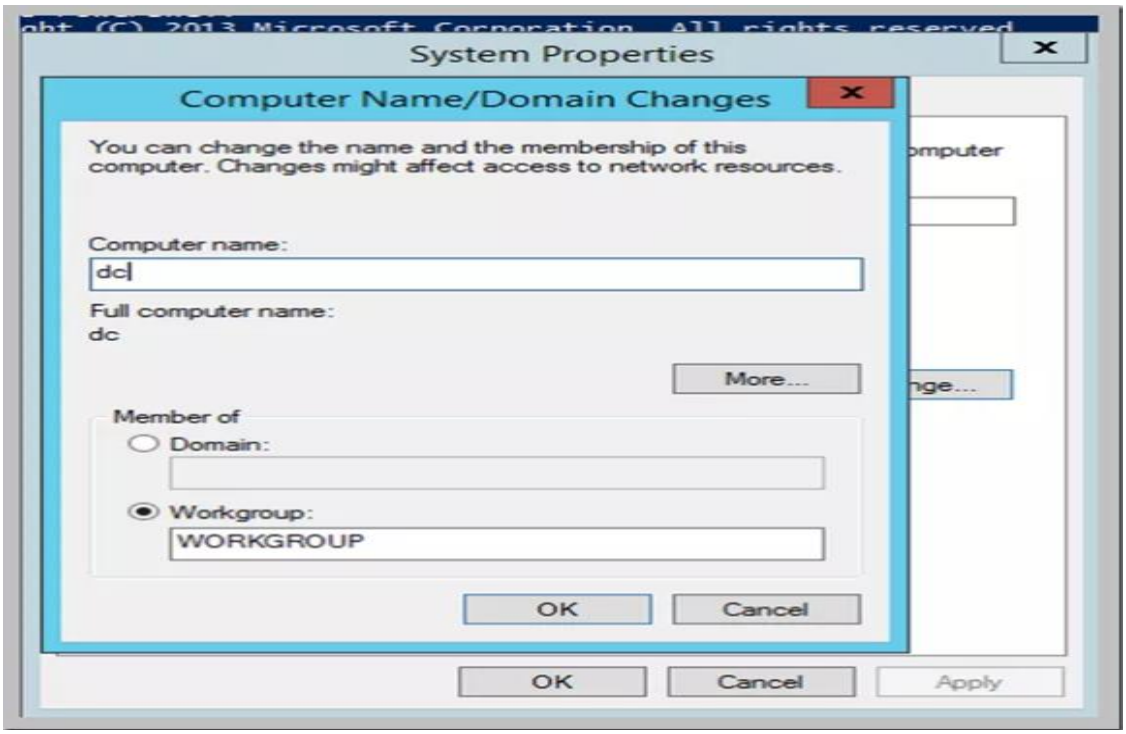
- Go to “Action/Ctrl+Alt+Del” to sign in. Enter Administrator’s password to login



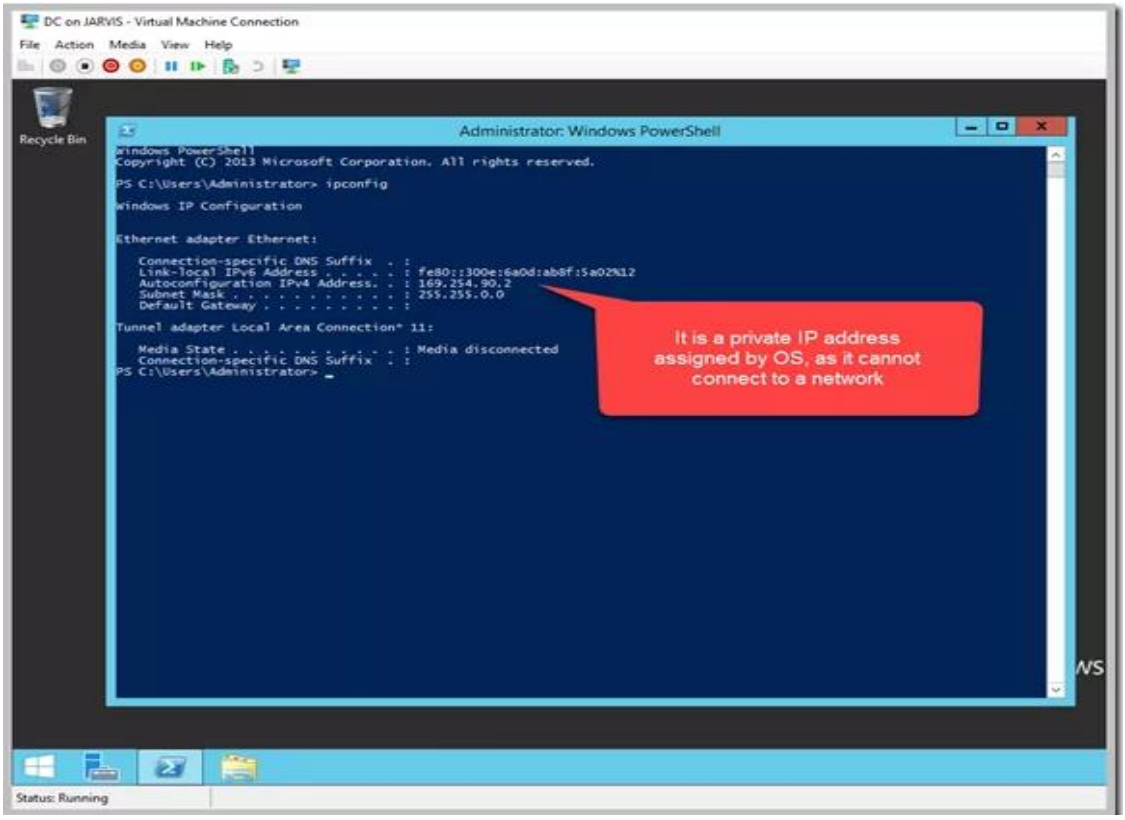
- Server Manager dashboard will launch by default.



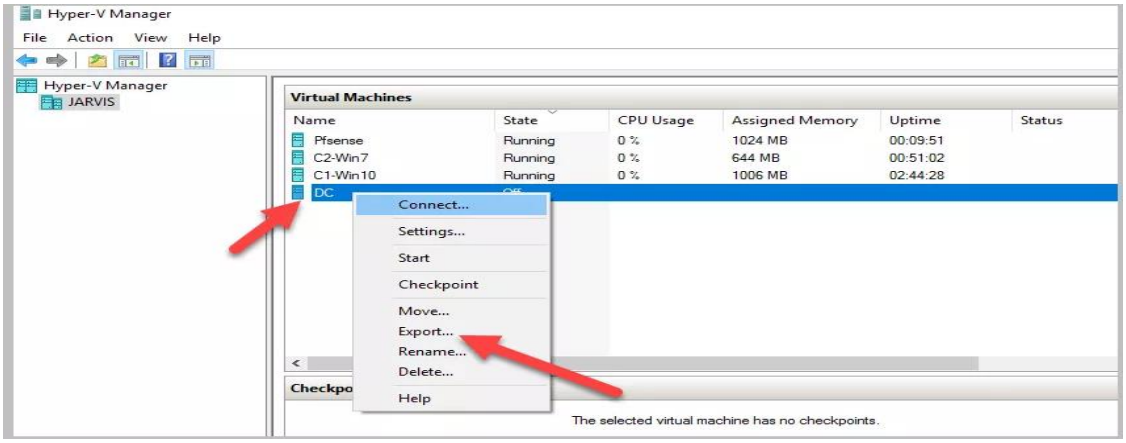
- Let's change the computer name to "DC". Restart the machine after changing hostname



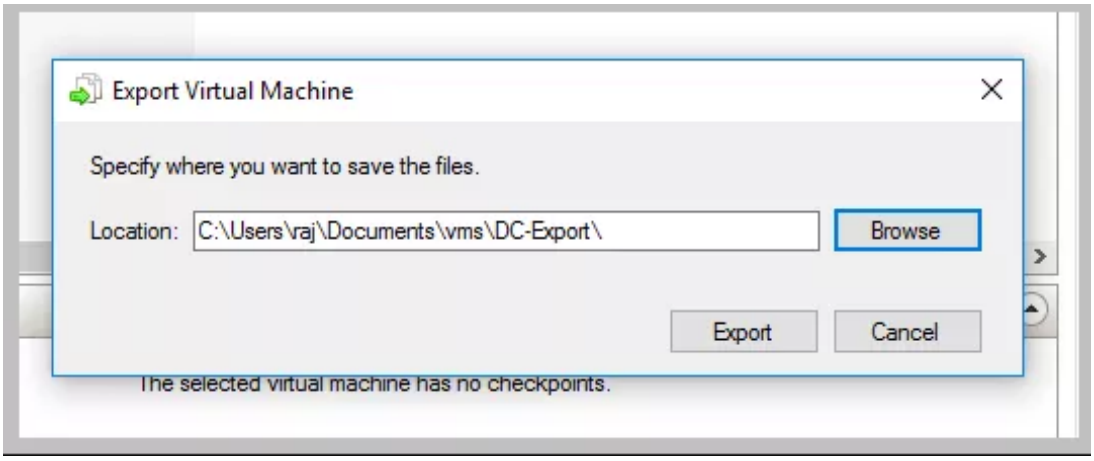
- After restarting, open a command prompt and type ipconfig. Currently, the DC will not have an IP address.



- Before promoting the server to "Domain Controller" role in Windows 2012 server, let's take a quick export, so it's easy to create new VMs using this image. We will use this exported image to create the FileServer virtual machine. Right click on **DC** and click "Export"



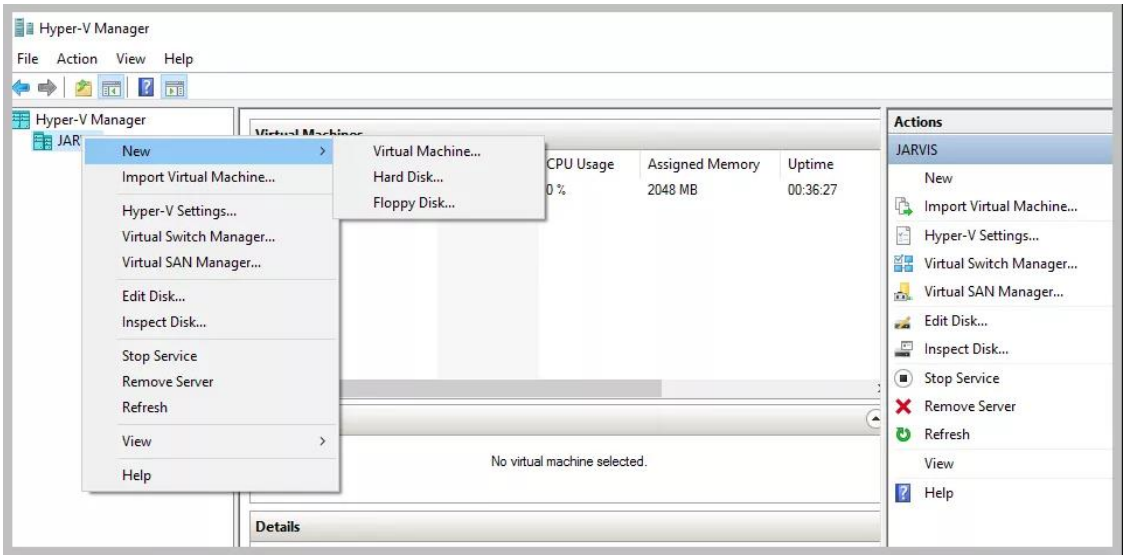
- Choose a location to save the files. We will use these files to create another server in later modules



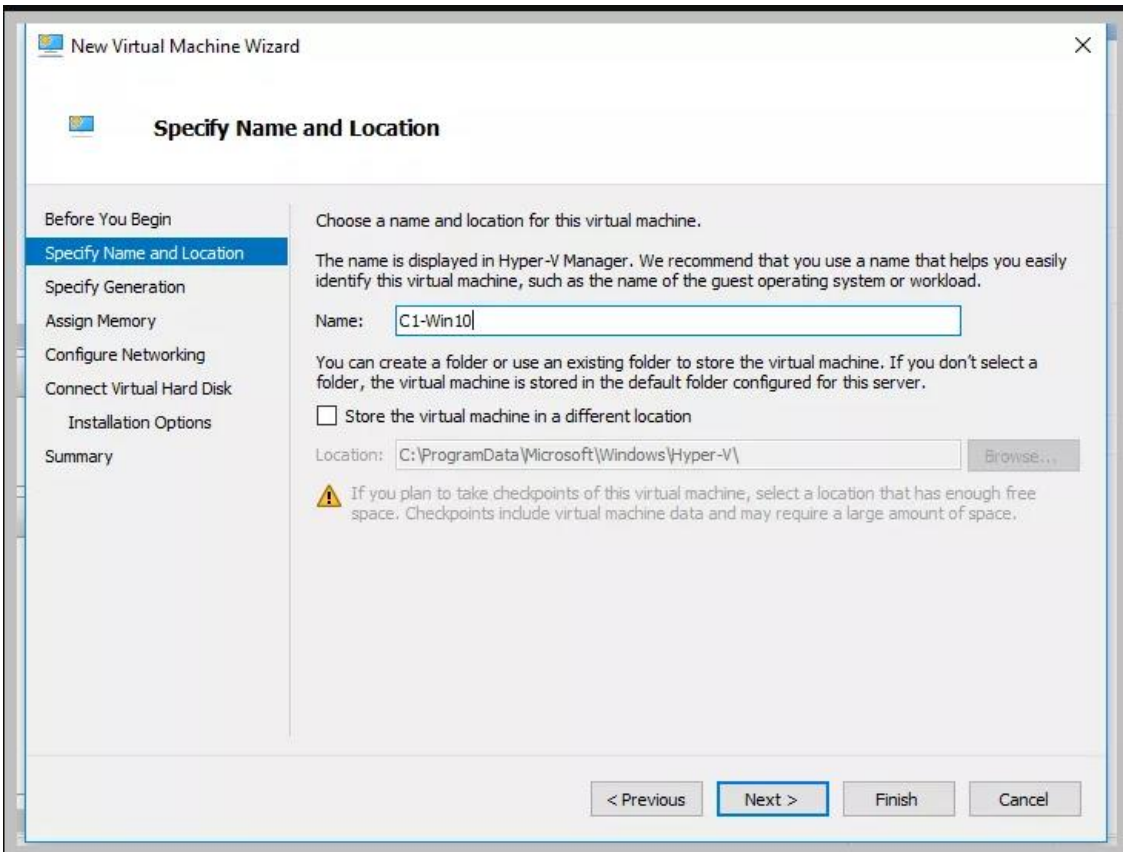
- Wait for the process to complete. All exported files will be stored in the selected folder.

5. Installing Windows 10–64 bit version

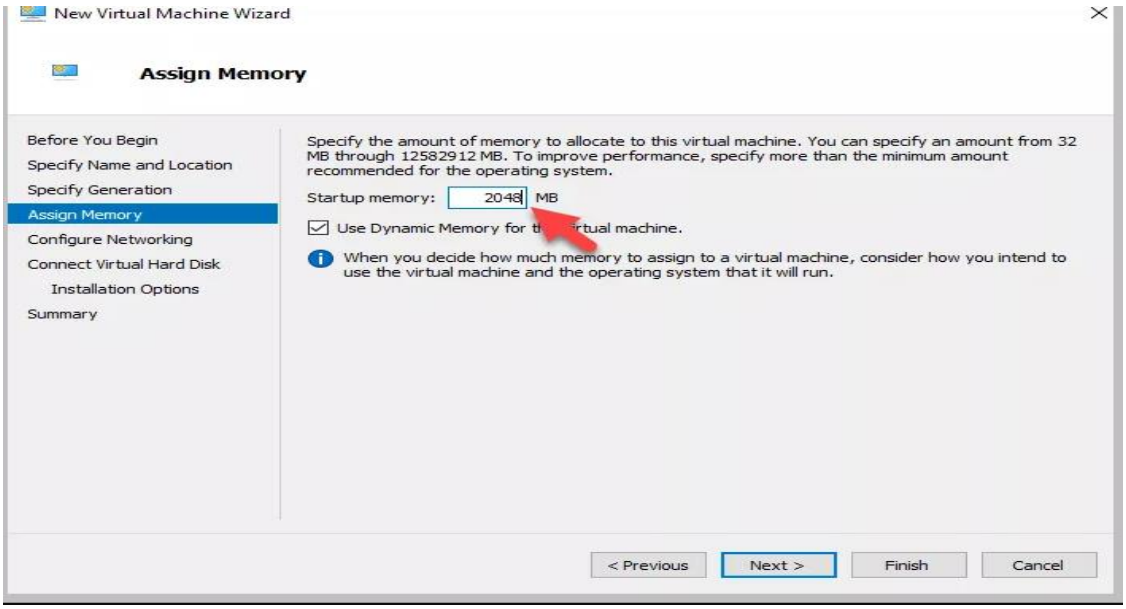
- Right click on “Jarvis” and create a new virtual machine



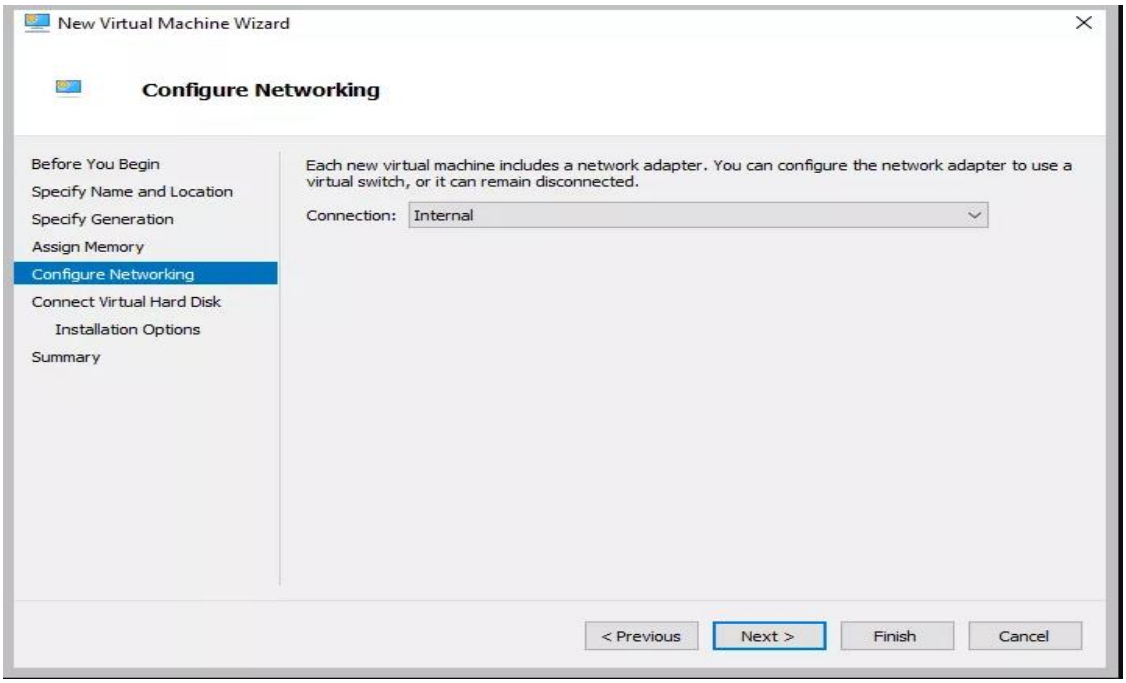
- Name the VM as C1-Win10, which stands for Client1 - Windows 10 machine.



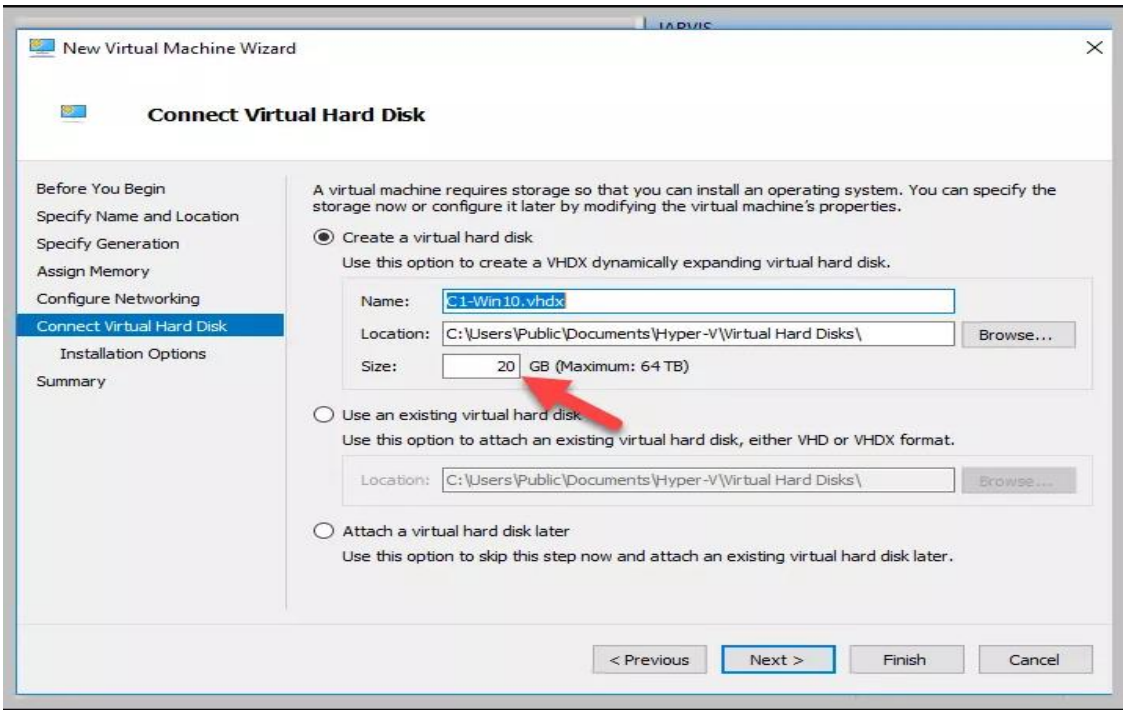
- Assign 2048 ram for the Windows 10 machine



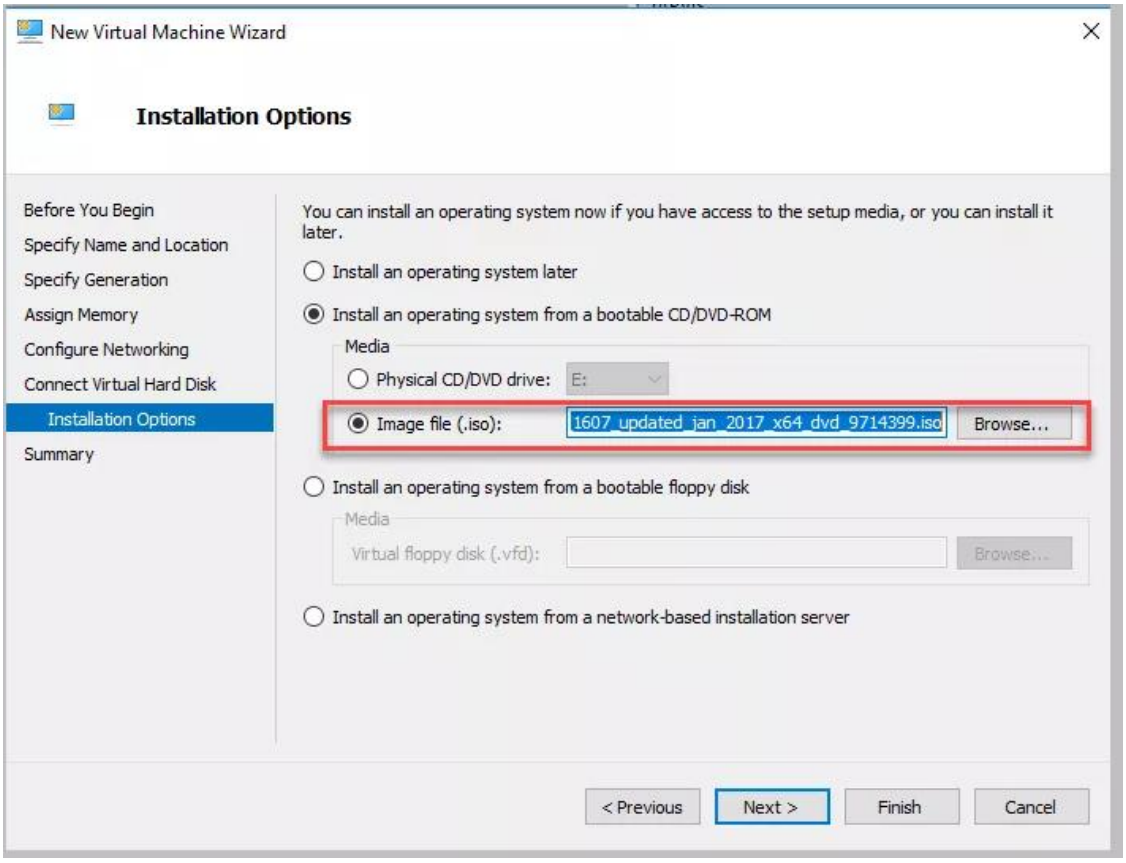
- Choose “Internal” for network connection



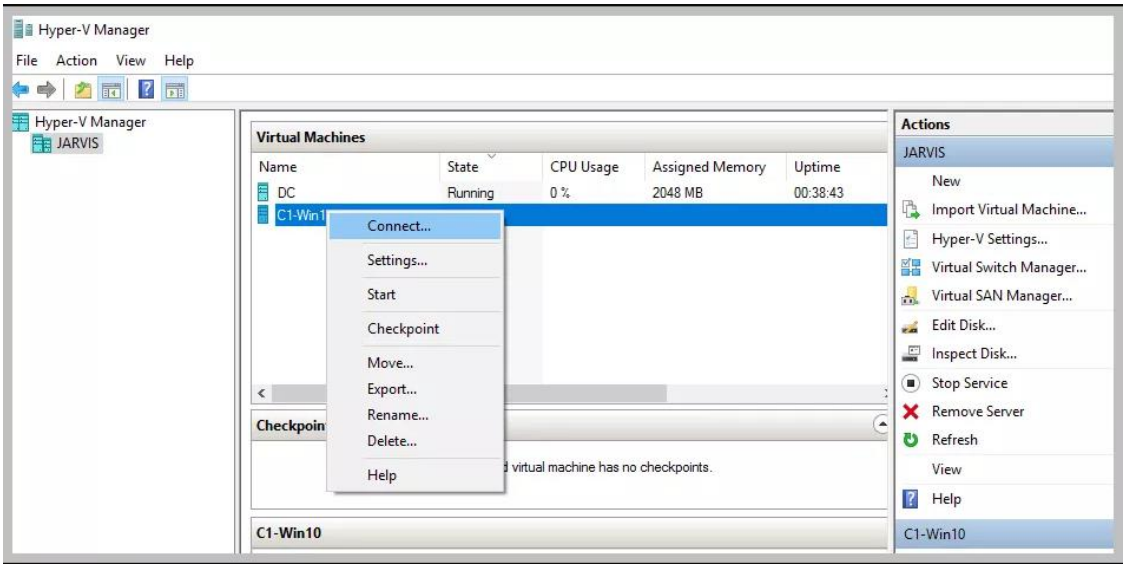
- Assign 20GB for the virtual machine



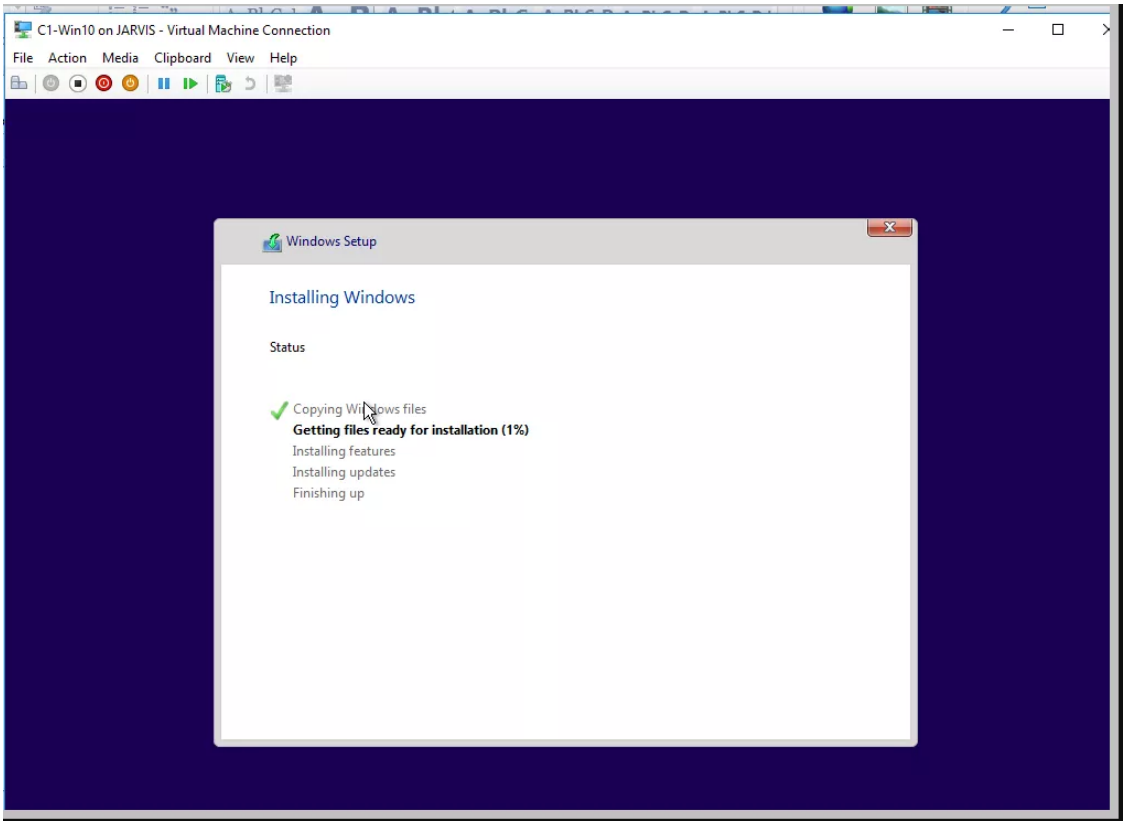
- Point to the downloaded Windows 10, ISO image and finish the configuration process



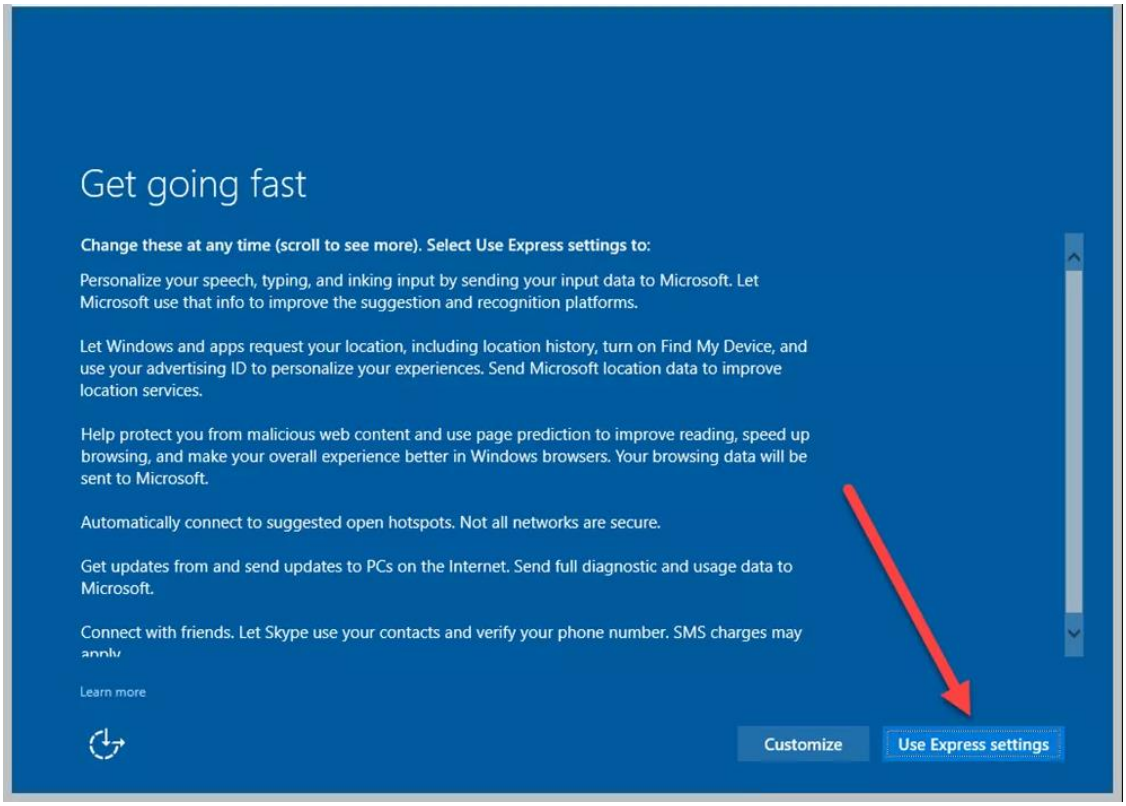
- Right click on C1-Win10 and click connect



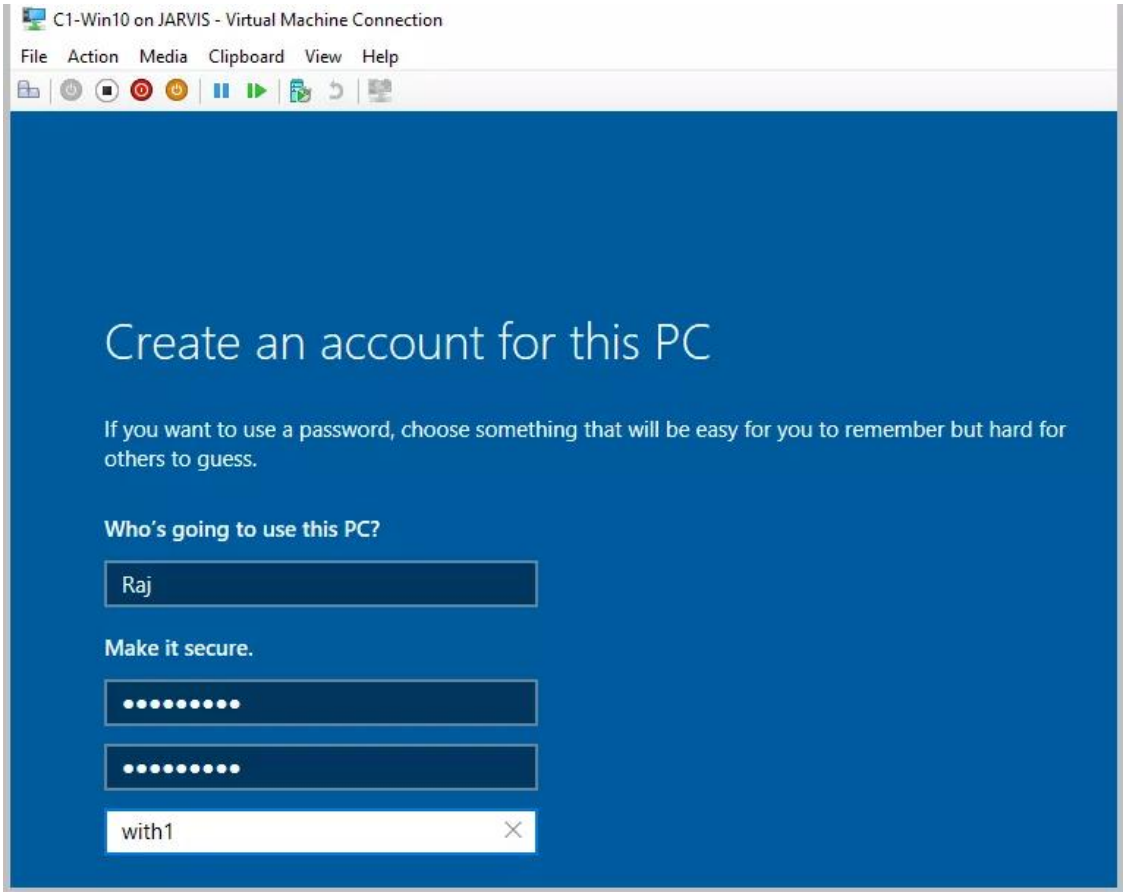
- Wait for the install to complete. it should take around 15 minutes to complete.



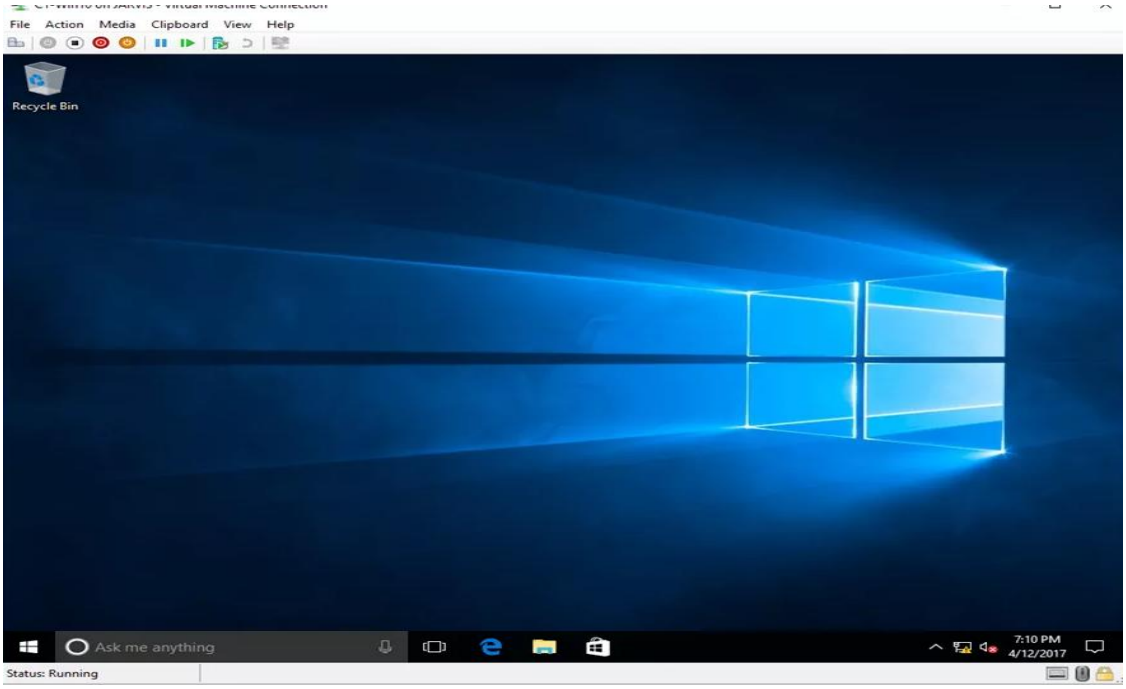
- Use Express settings



- Create an account and give it a strong password



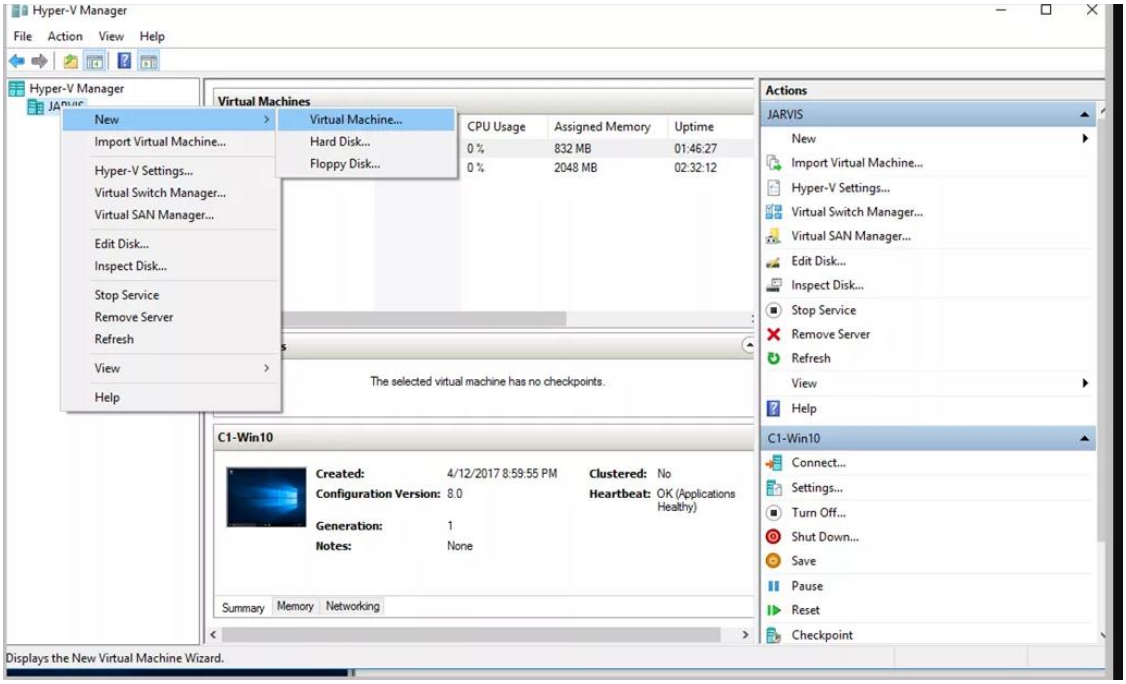
- Complete the process and reboot the machine



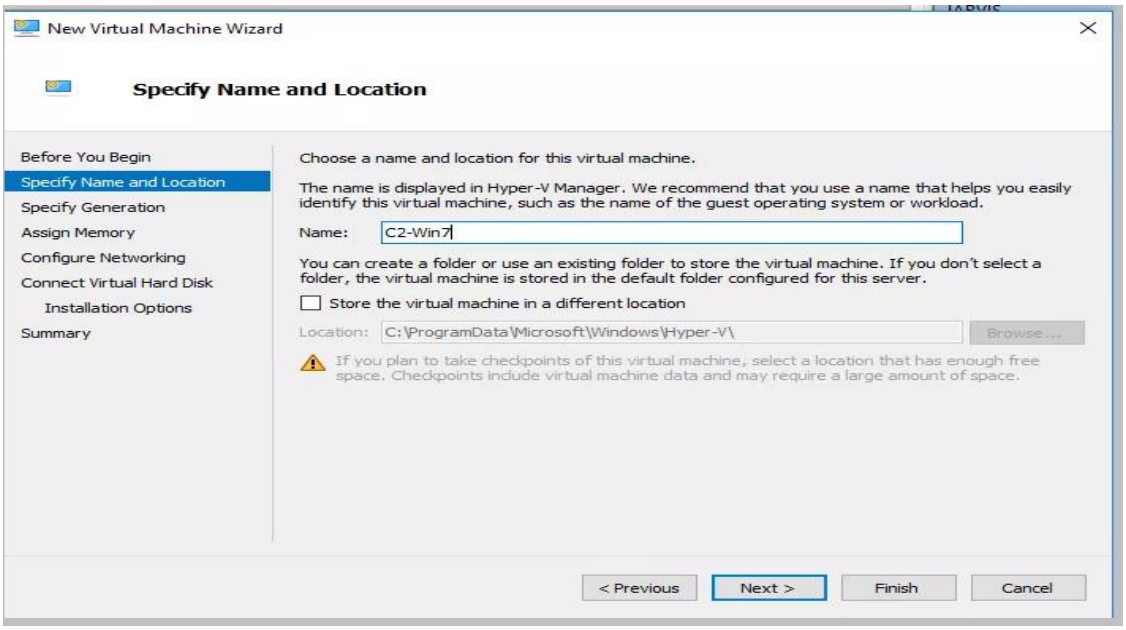
- Let's change the host name to **C1-Win10**. Restart the computer.

6. Installing Windows 7

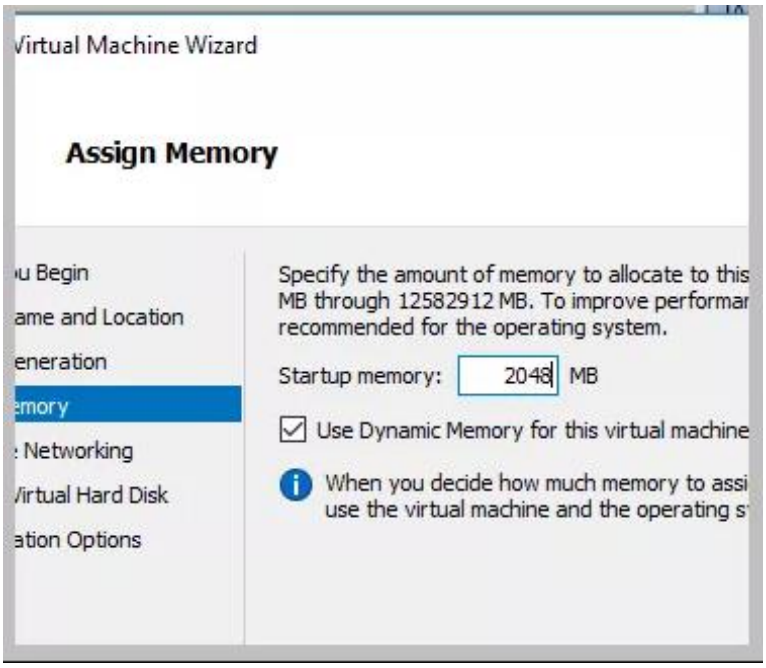
- Right click on "Jarvis" and create a virtual machine



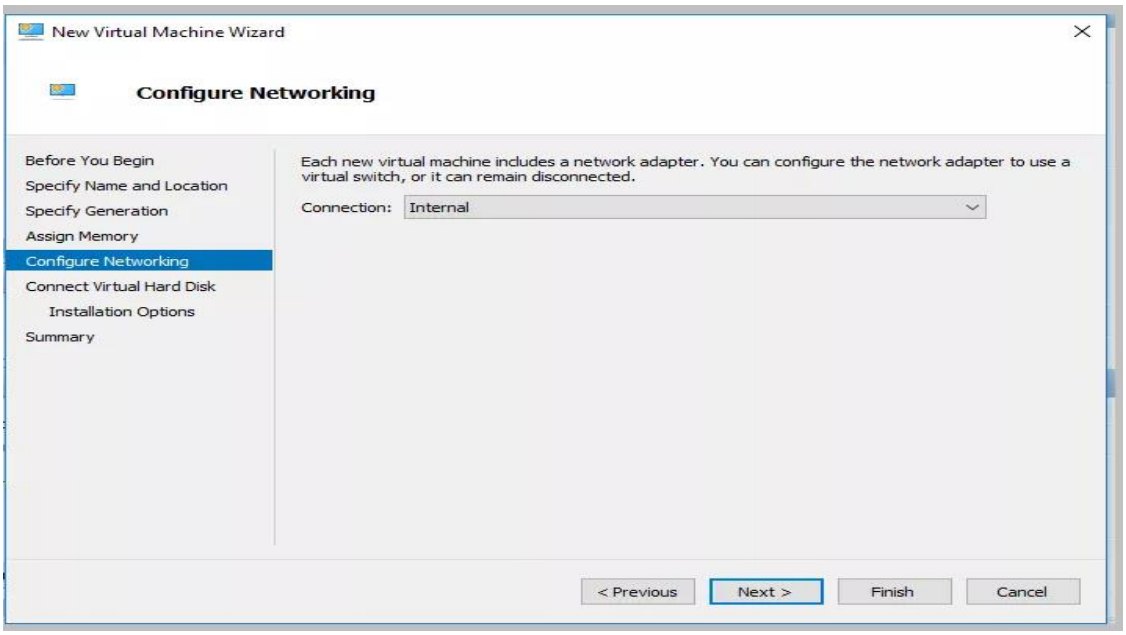
- Name the VM as C2-Win7, which denotes Client 2 - Windows 7 machine.



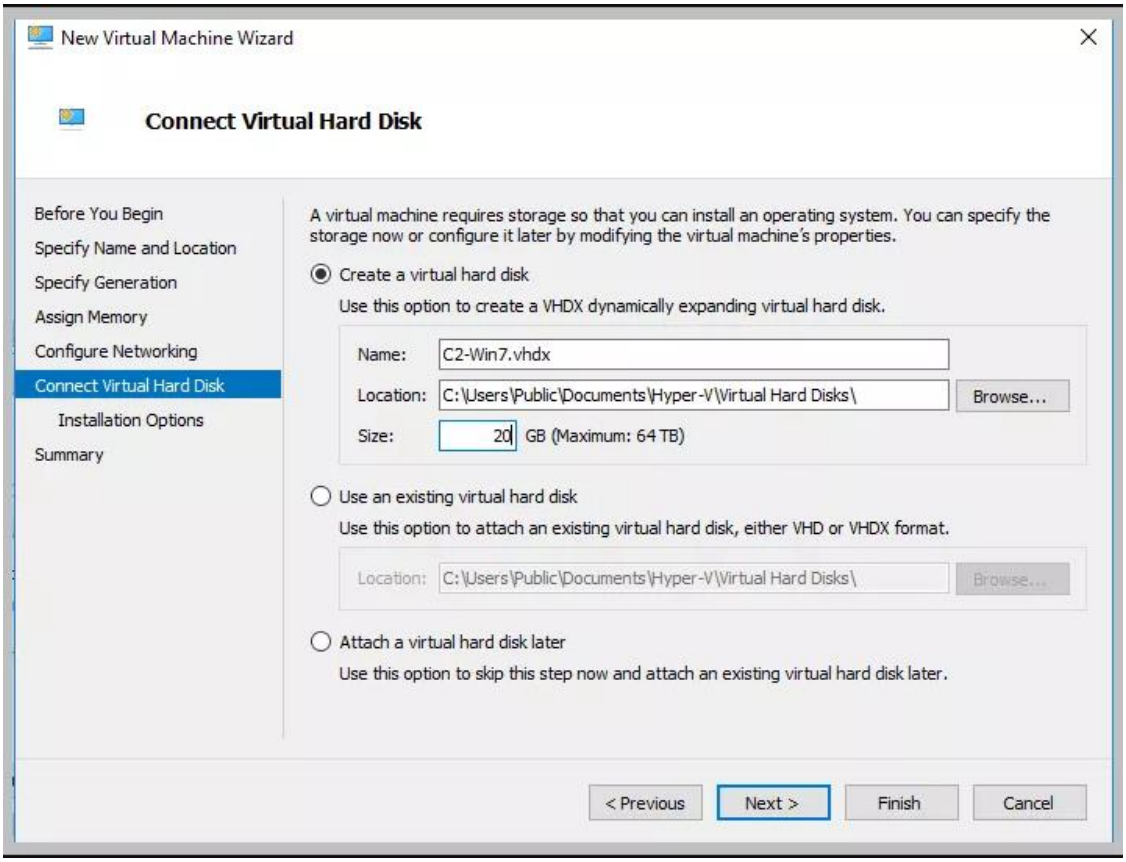
- Assign 2048 MB ram



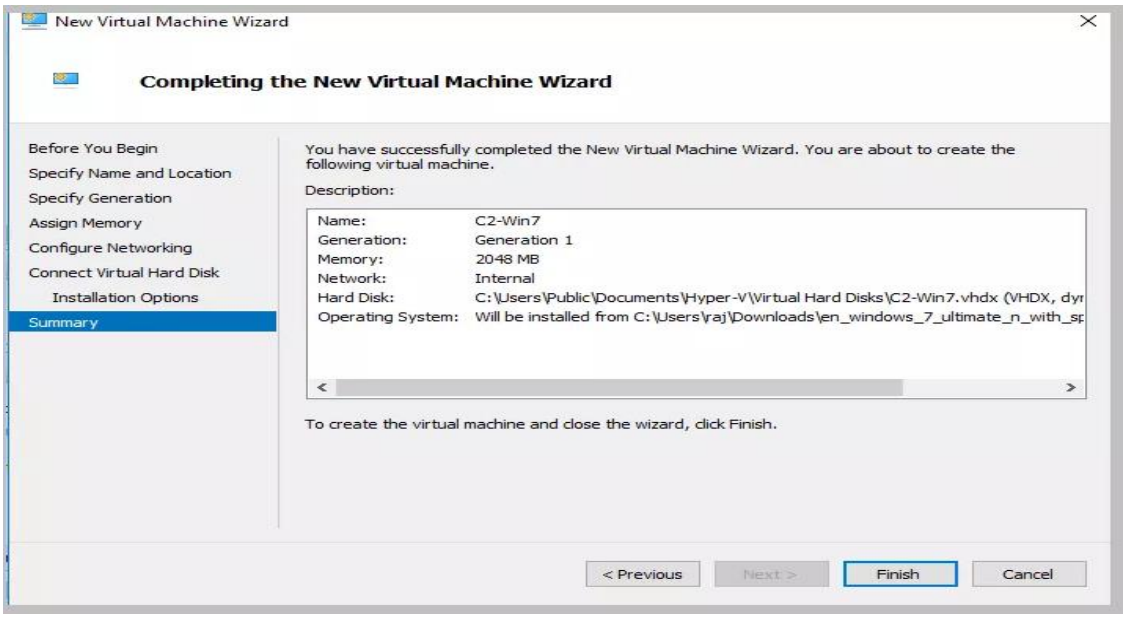
- Connect to “Internal” network



- Assign 20 GB for the virtual machine

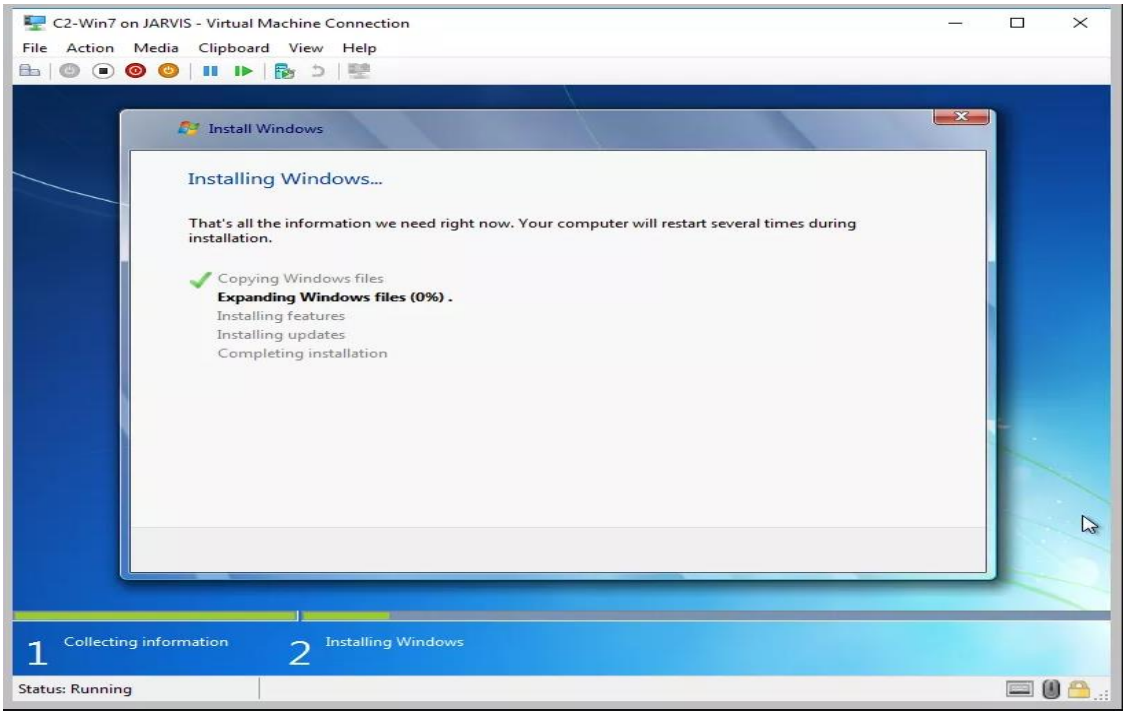


- Review and finish the setup process

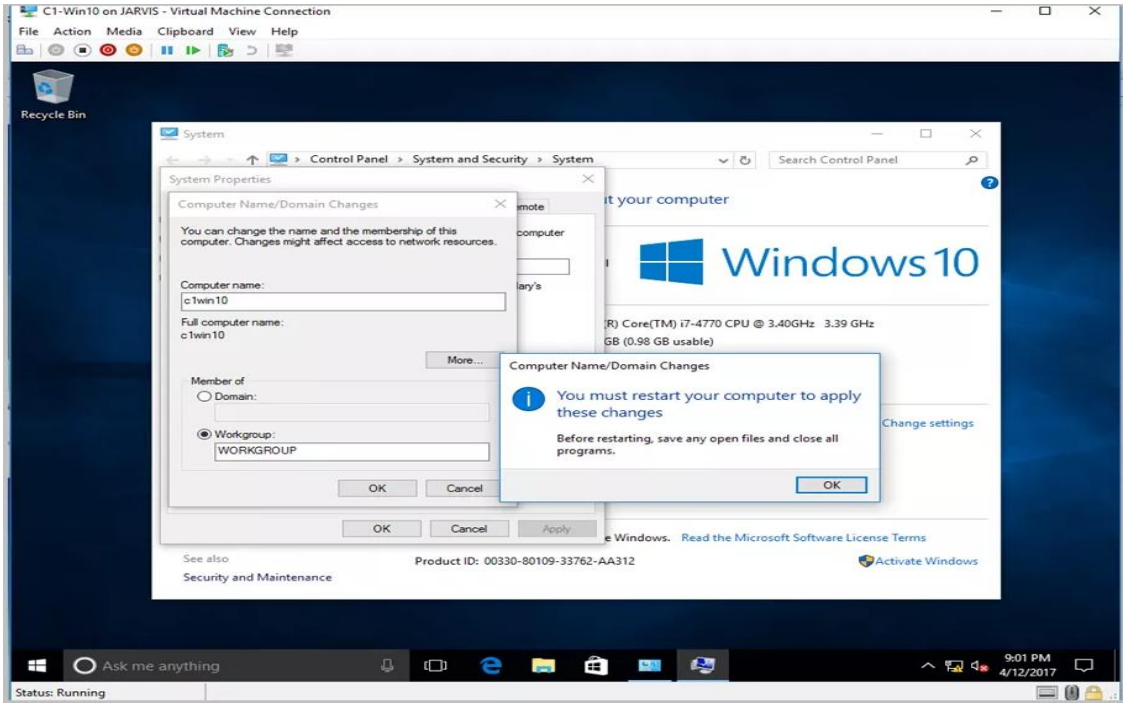


- Right click an C2-Win7, and connect to the VM, and click “Install Now”

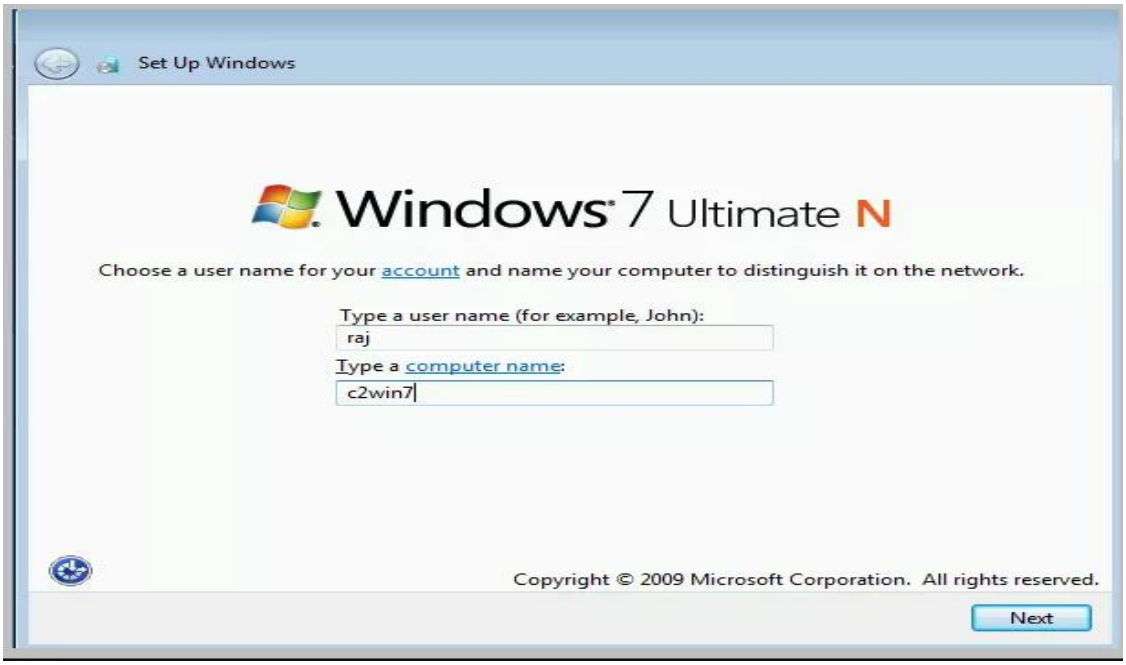
- Wait for the install process to complete



- After installation, change the computer name to “C2Win7” and restart the VM

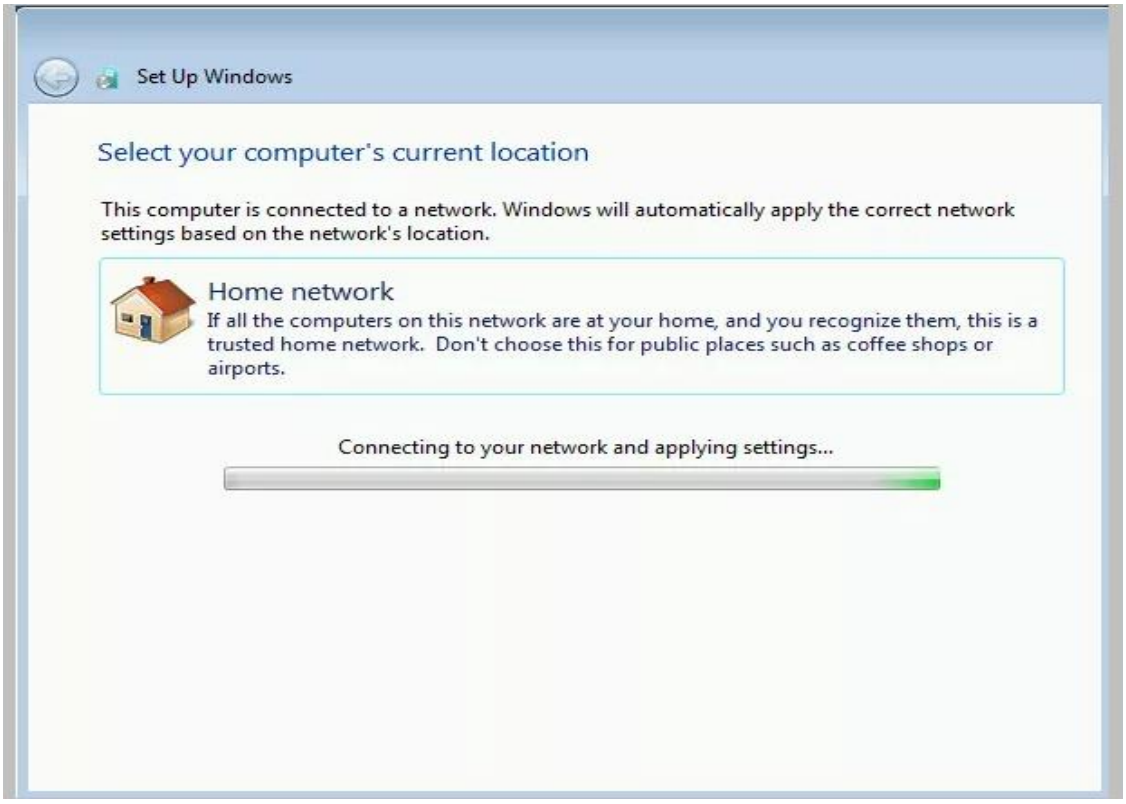


- Use a user name of your choice

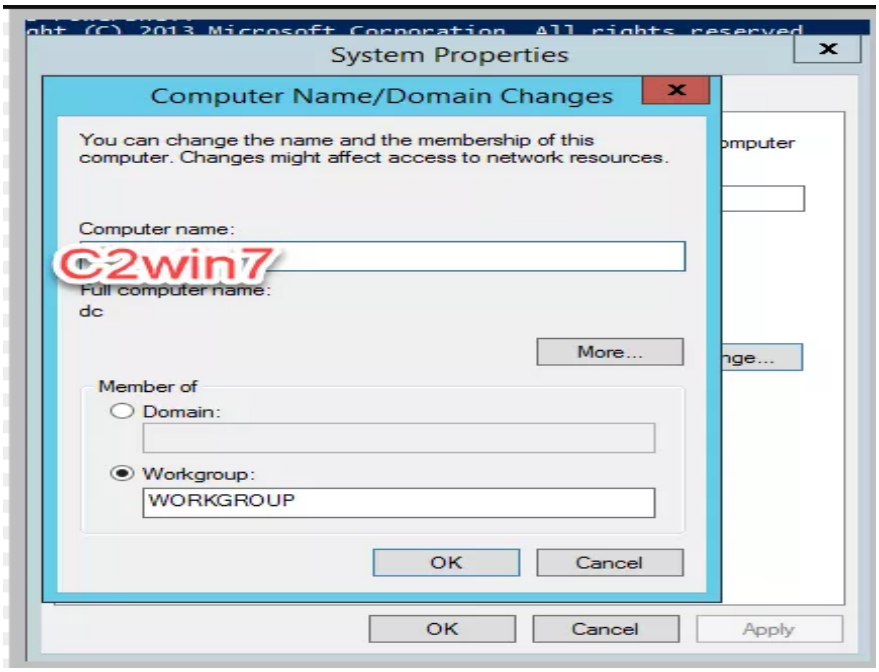


- Use recommended settings

- Choose “Home network”



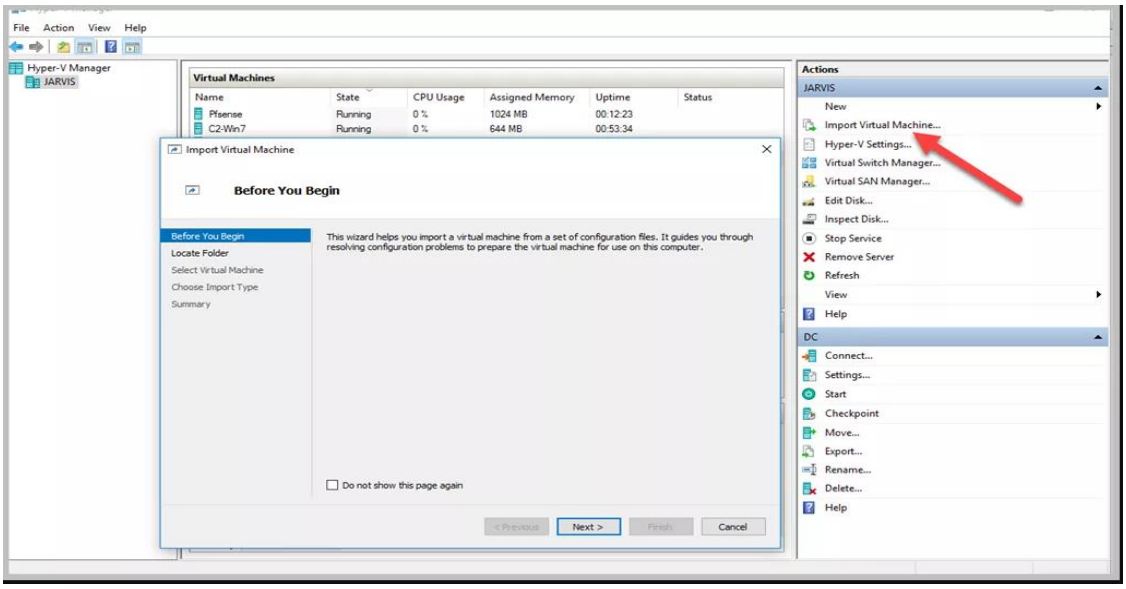
- After installation, change the computer name to C2win7



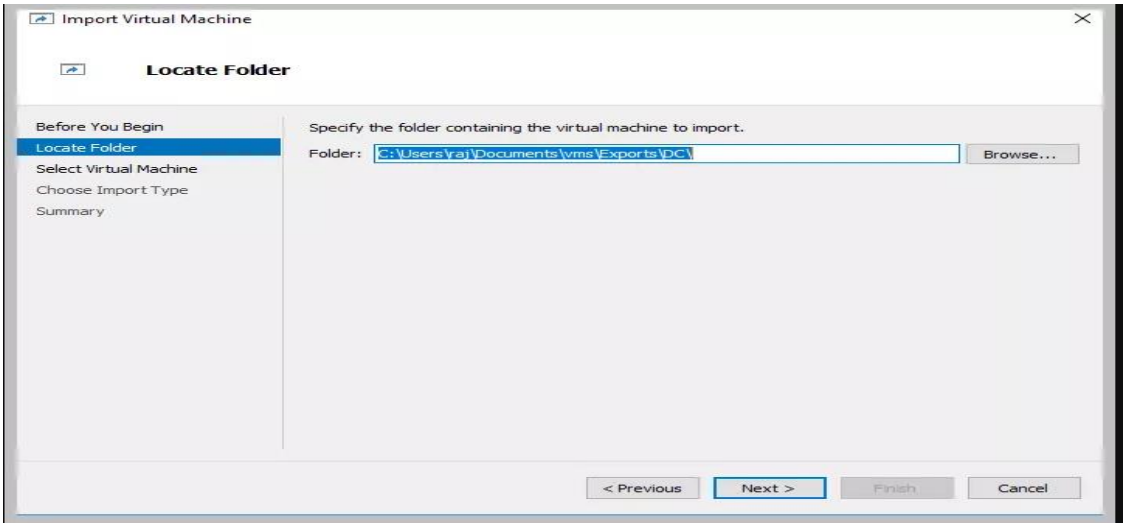
- Restart the machine to complete the process

7. File Server Installation – Windows 2012

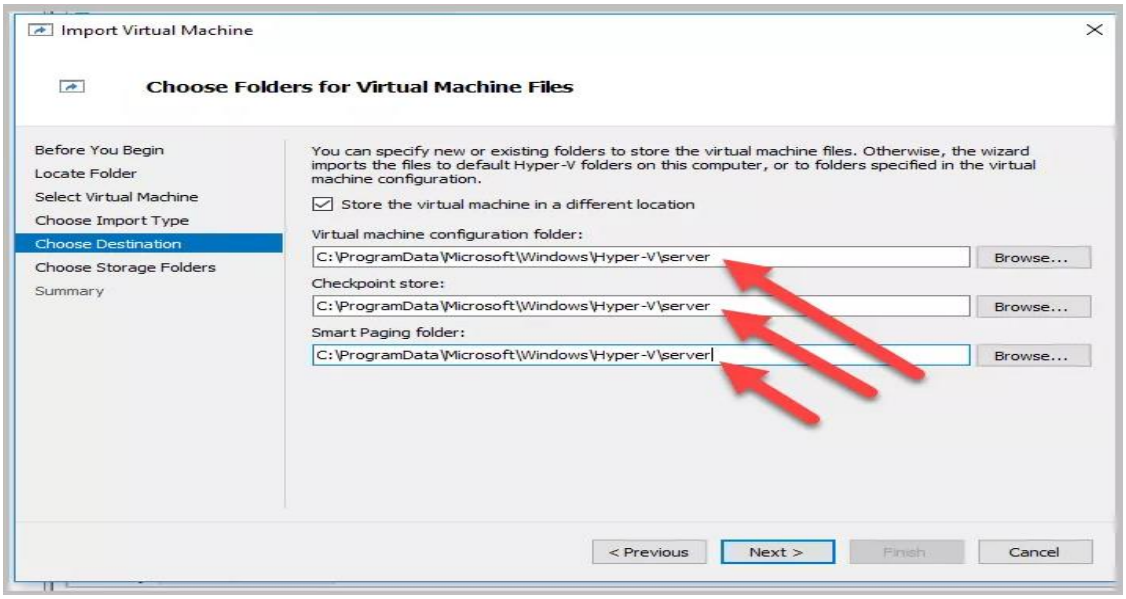
- Let's create another member server for our lab using the exported image in step 4 . Click "Import Virtual Machine".



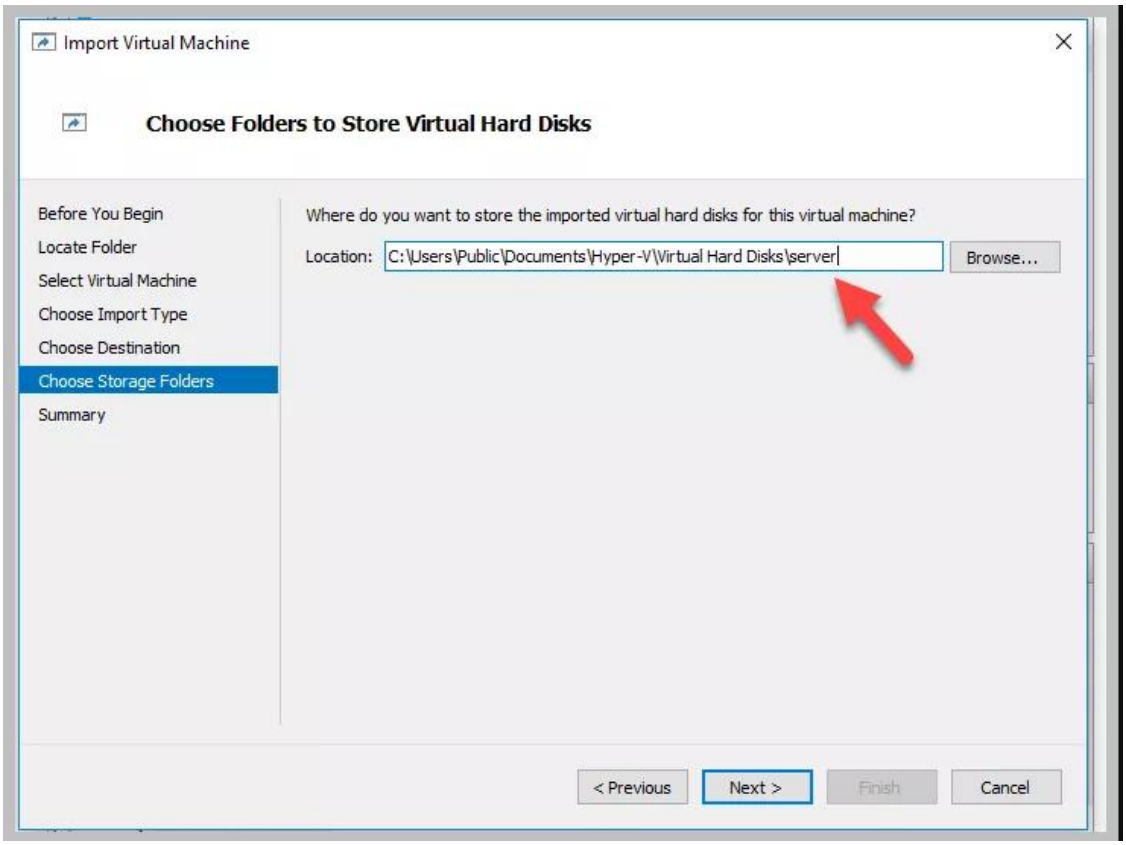
- Choose the file location of the source files and click "Next"



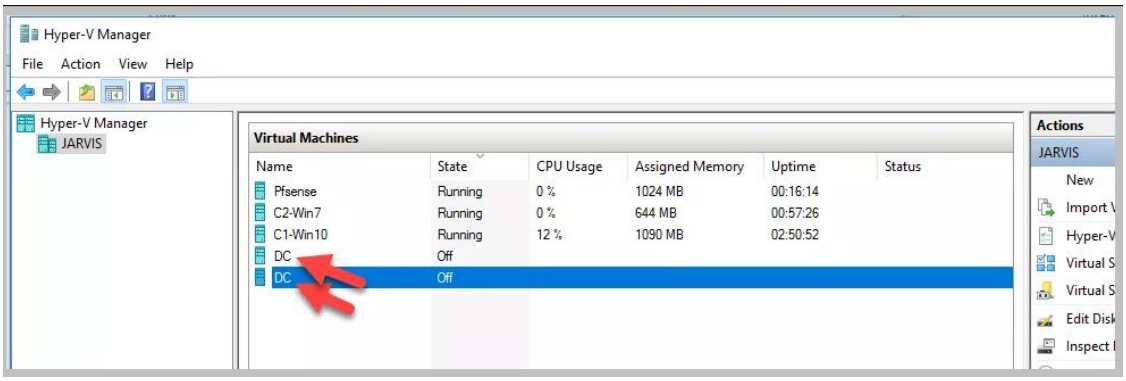
3) Choose destination location. It is safe to add "server" or any other unique name to save the files in a separate folder



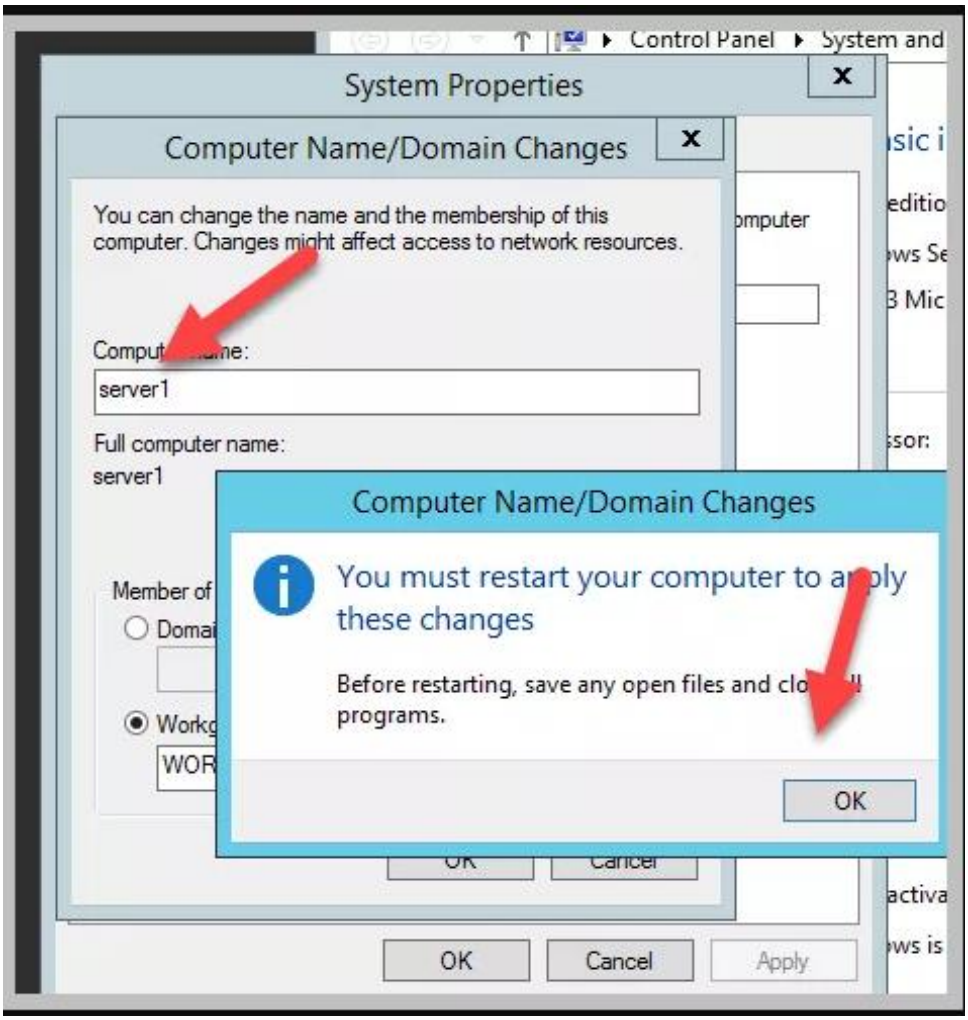
- Choose a folder for the hard disk



- Click “Next” and complete the process.



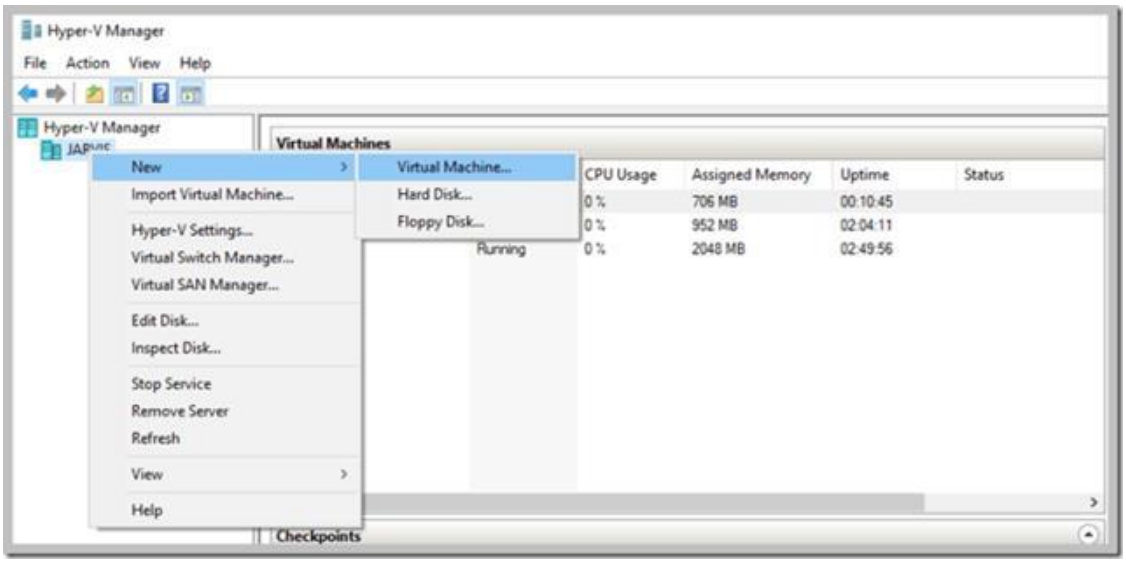
- Restart the server and rename the Computer name to “**server1**”



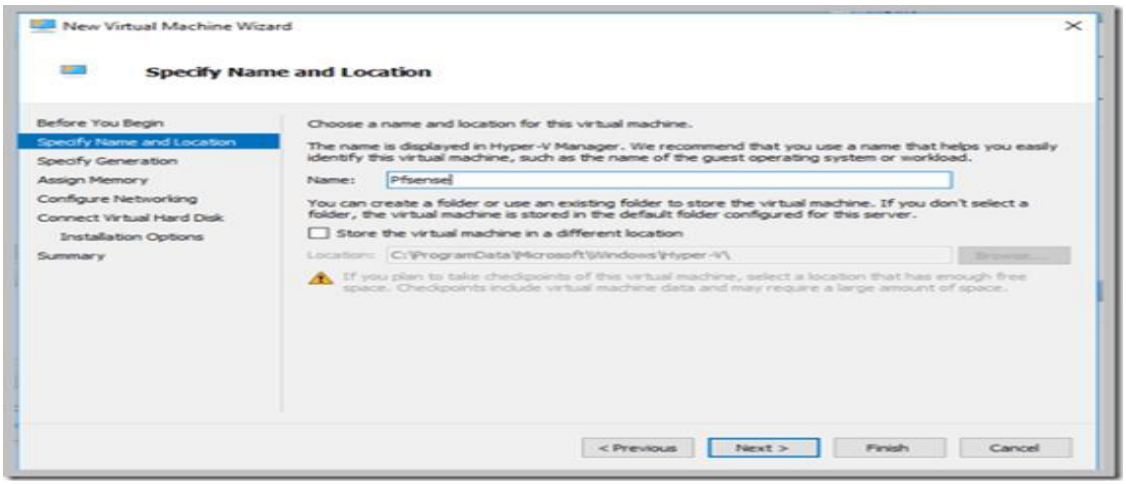
8. Installing Routing/Firewall - PFSense

1) **pfSense** is an open source firewall/router computer software distribution based on FreeBSD. It is installed on a computer to make a dedicated firewall/router for a network and is noted for its reliability and offering features often only found in expensive commercial firewalls. It can be configured and upgraded through a web-based interface, and requires no knowledge of the underlying FreeBSD system to manage. pfSense is commonly deployed as a perimeter firewall, router, wireless access point, DHCP server, DNS server, and as a VPN endpoint. Take a look at their website to learn more about the product. [**http://www.pfsense.org**. Download the 64 bit ISO from this link [**https://www.pfsense.org/download/**

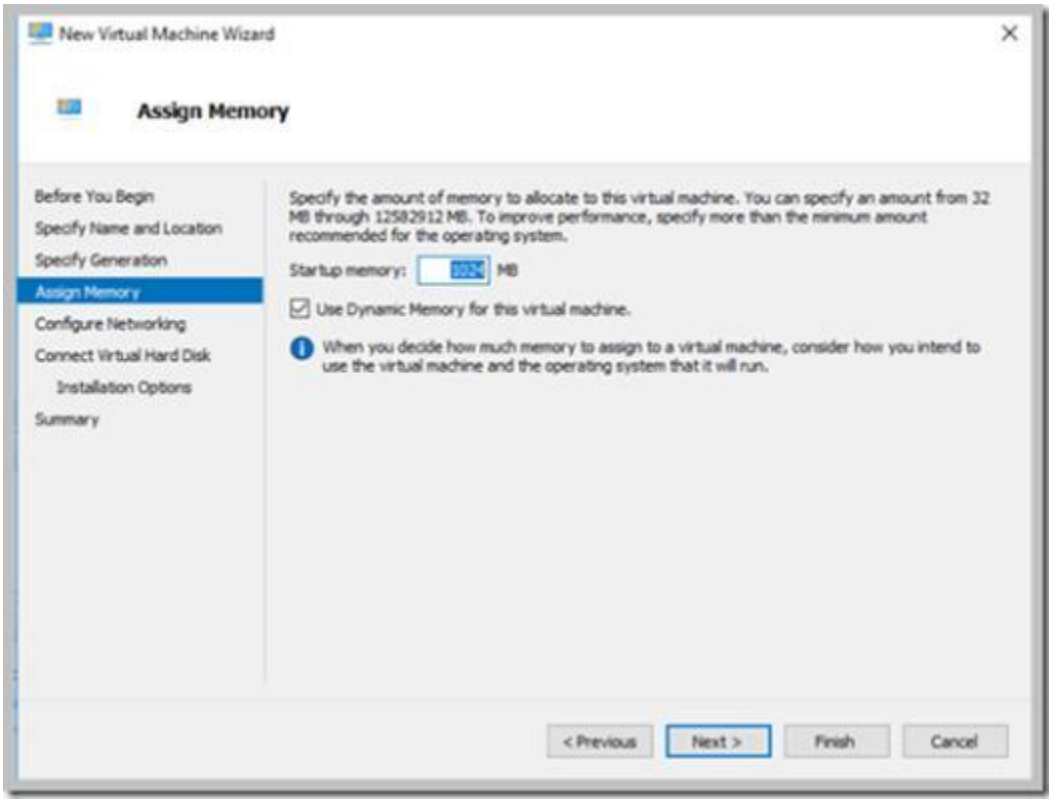
- Right click on “Jarvis” and create a new “Virtual Machine”



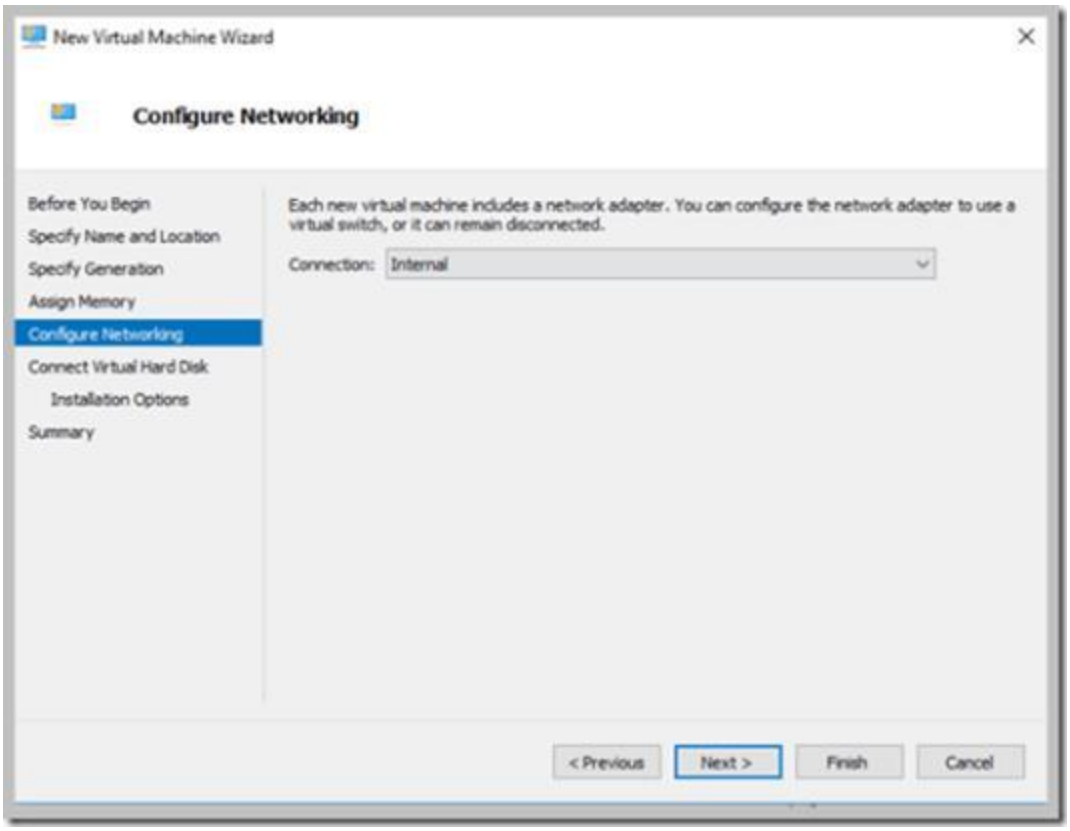
- Specify the name as “Pfsense”



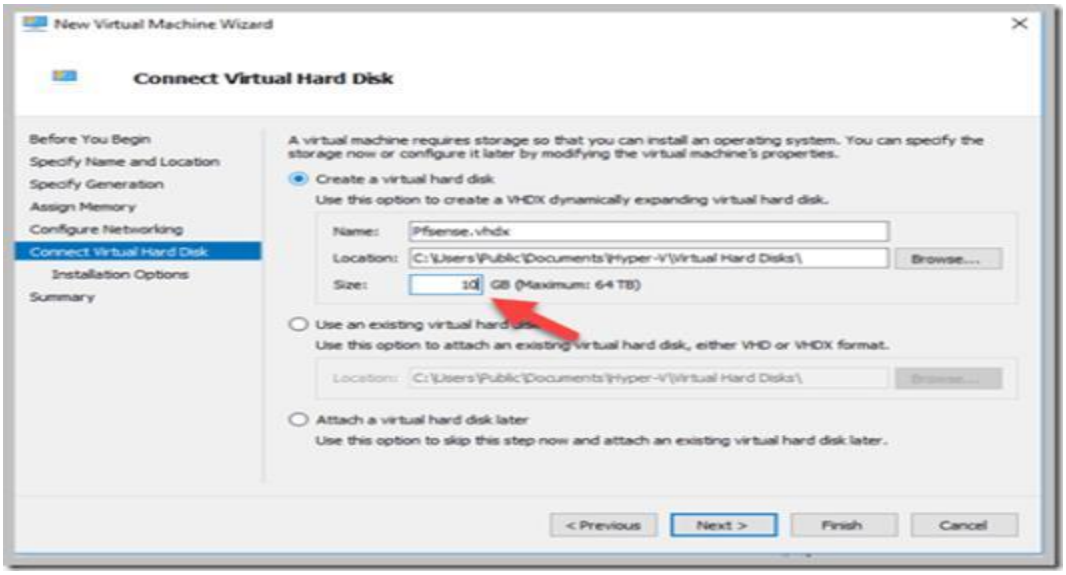
- Assign 1024 MB ram



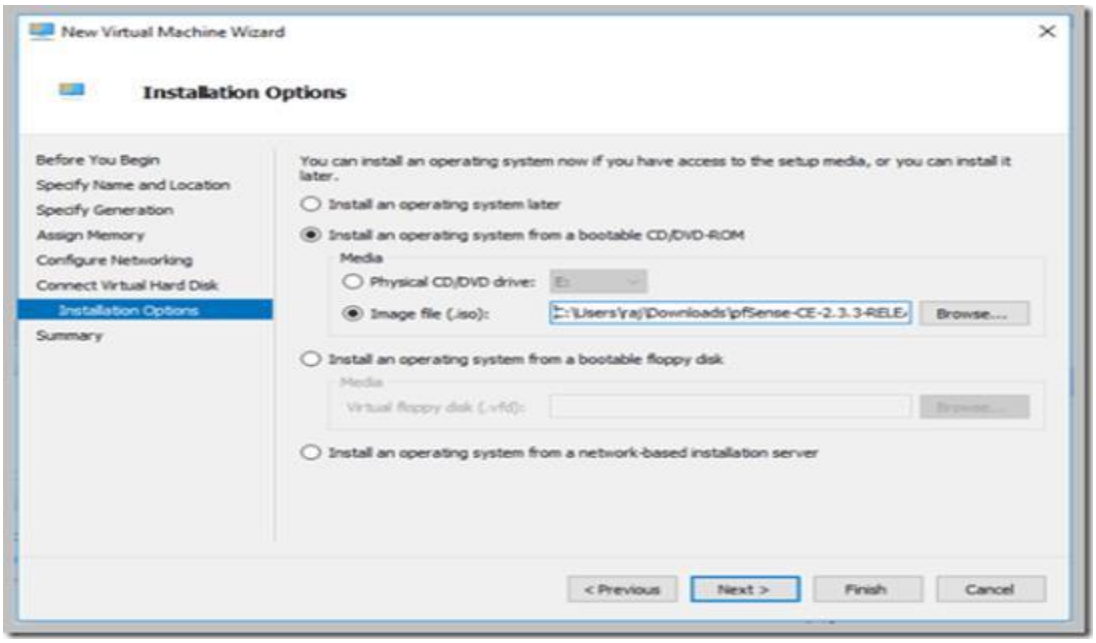
- Use the “Internal” for the network type



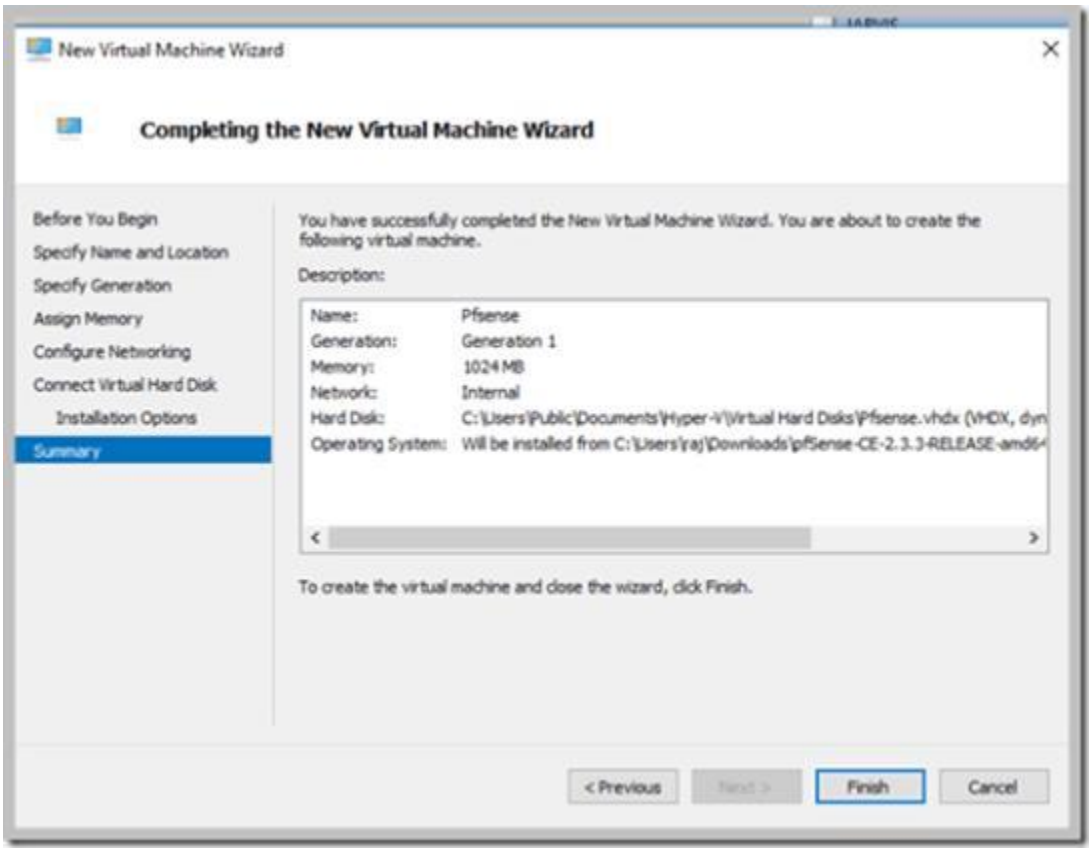
- 10 GB should be more than sufficient for PFsense for our lab environment



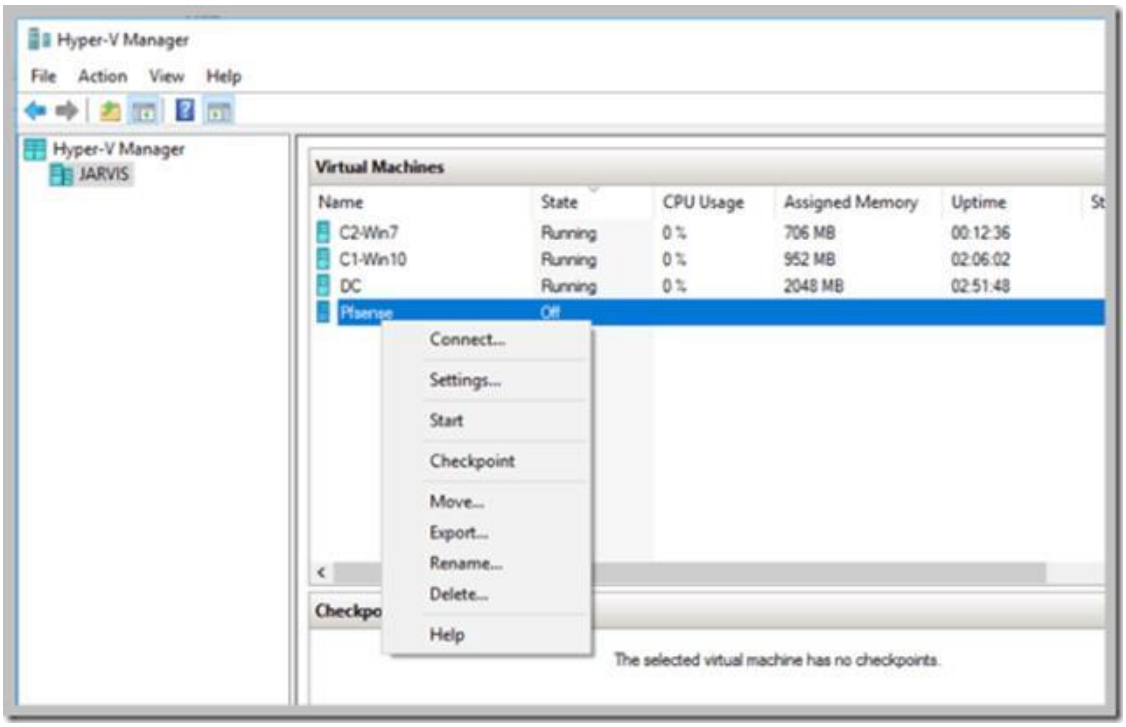
- Choose the ISO downloaded earlier



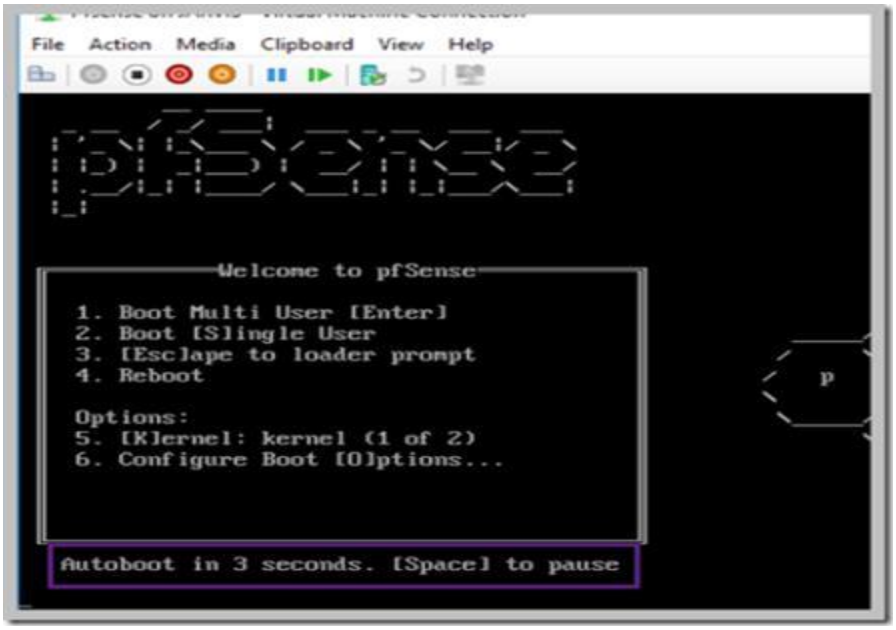
- Finish the setup dialog box



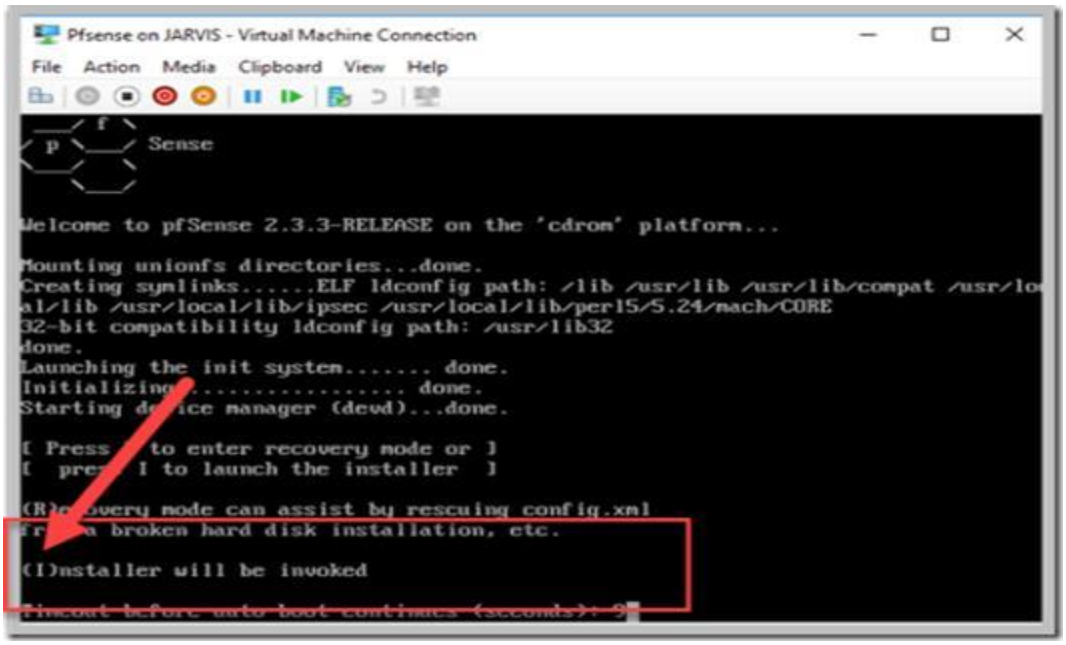
- Right click and connect to PFSense VM



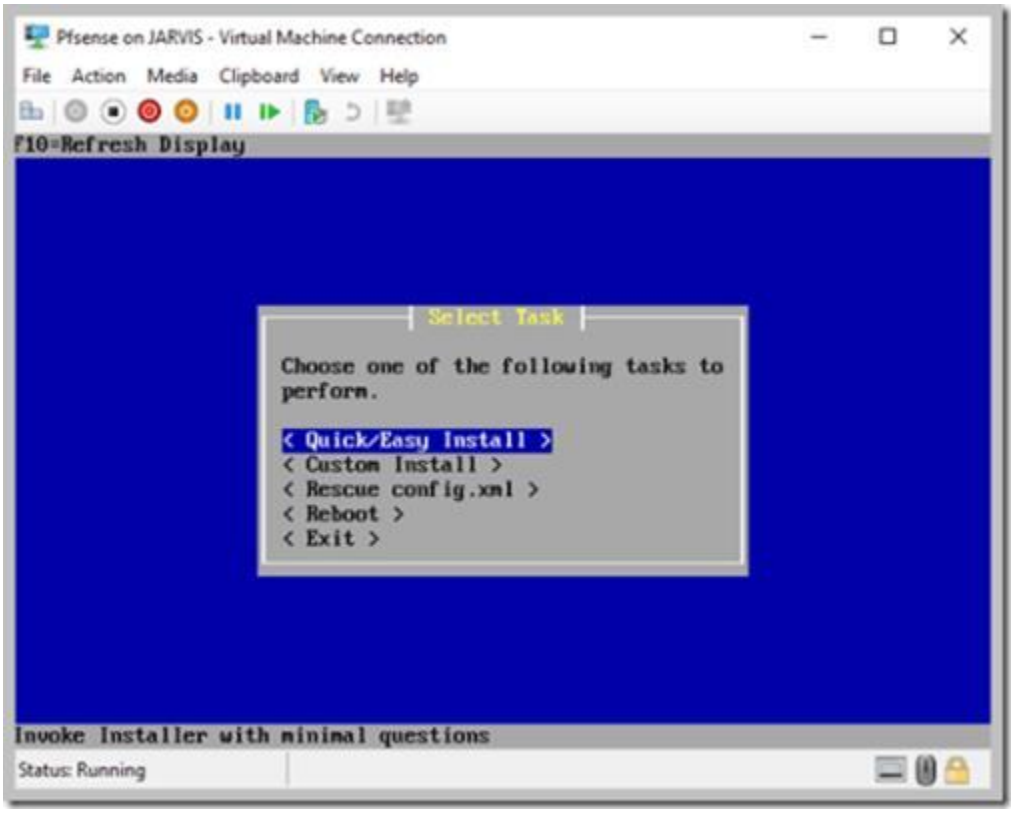
- Allow it to Autoboot



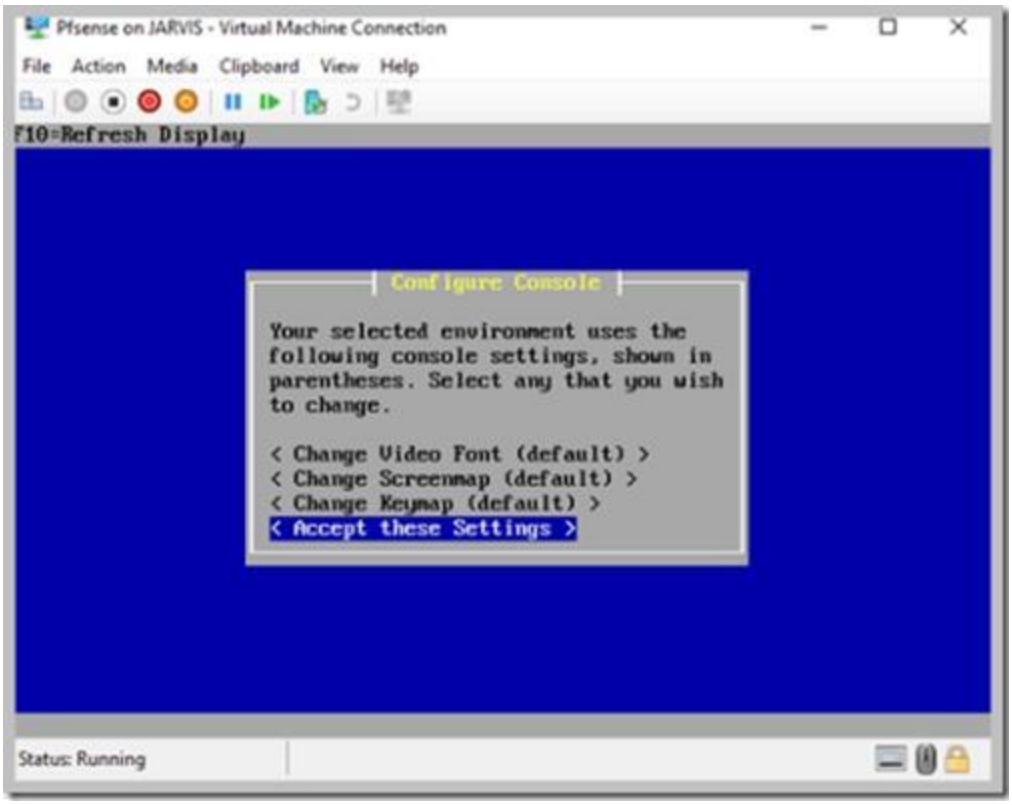
- Watch the messages carefully and ***type "I" using the keyboard*** to start installing



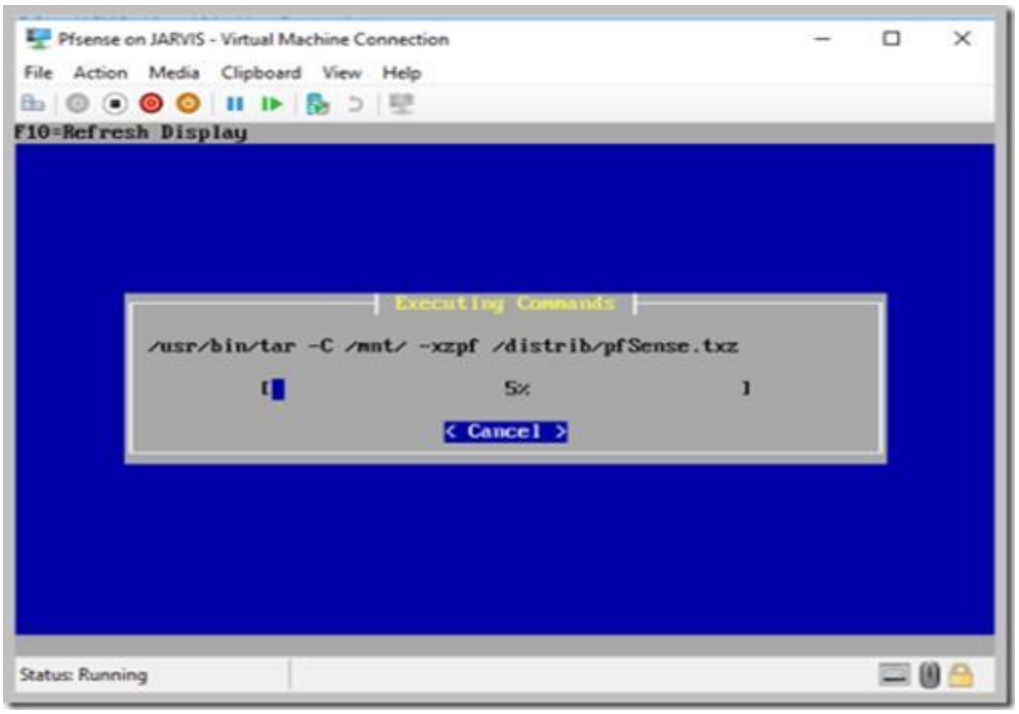
- Choose “Quick/Easy” install



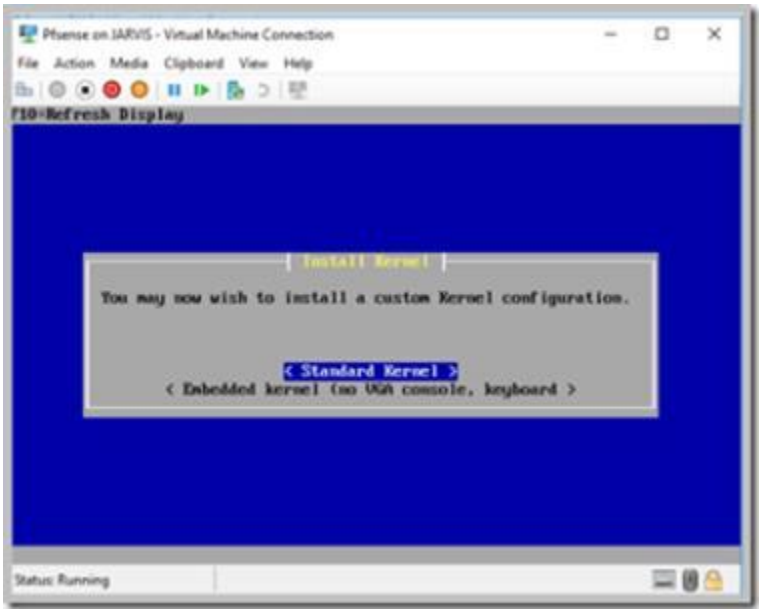
- Select “Accept these Settings”



- Wait for the install process to continue

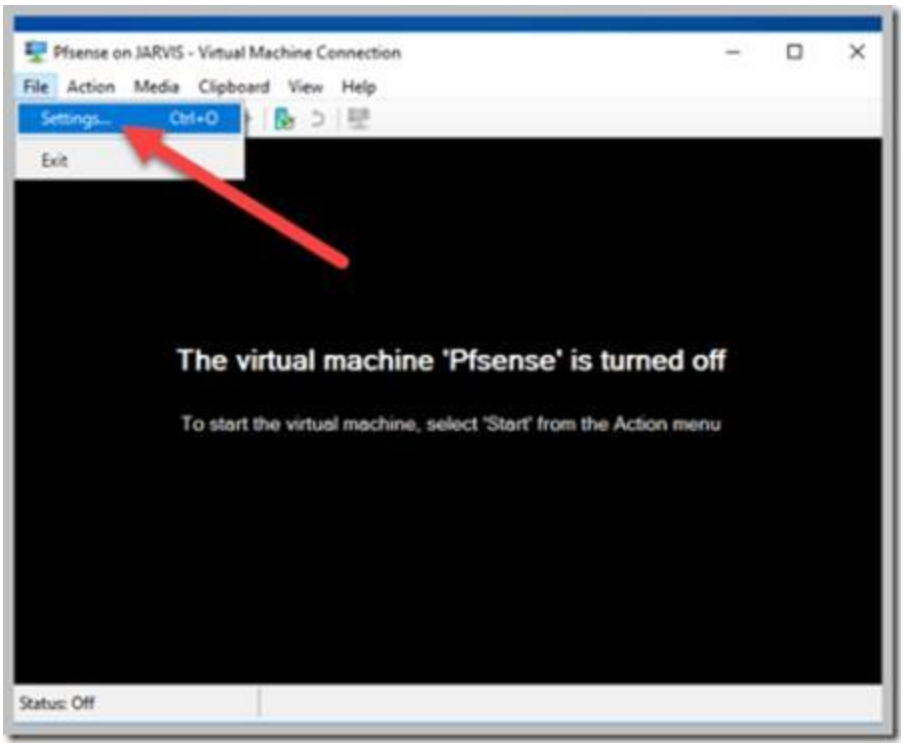


- Select “Standard Kernel”

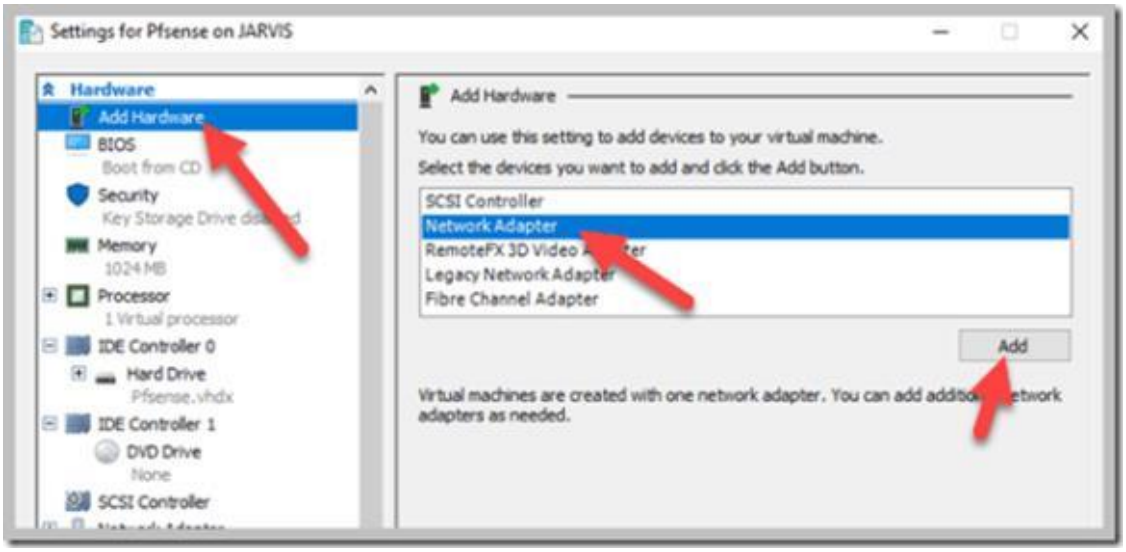


- Reboot the VM

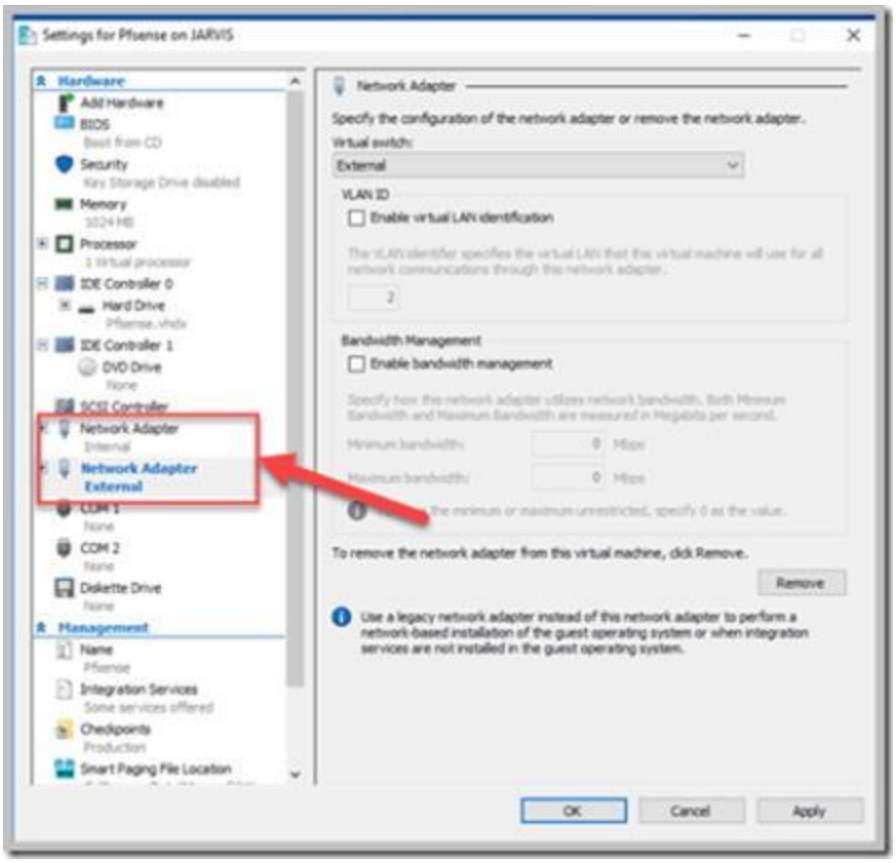
- Turn Off the VM to add additional switch. Choose settings.



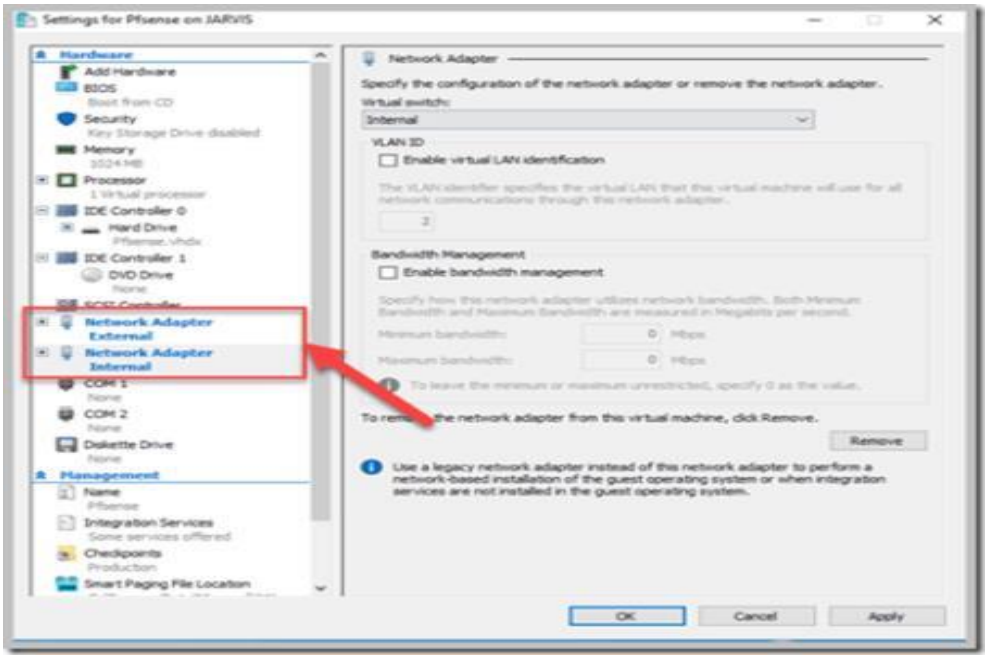
- Click “Add Hardware” and select “Network Adapter”. Click Add



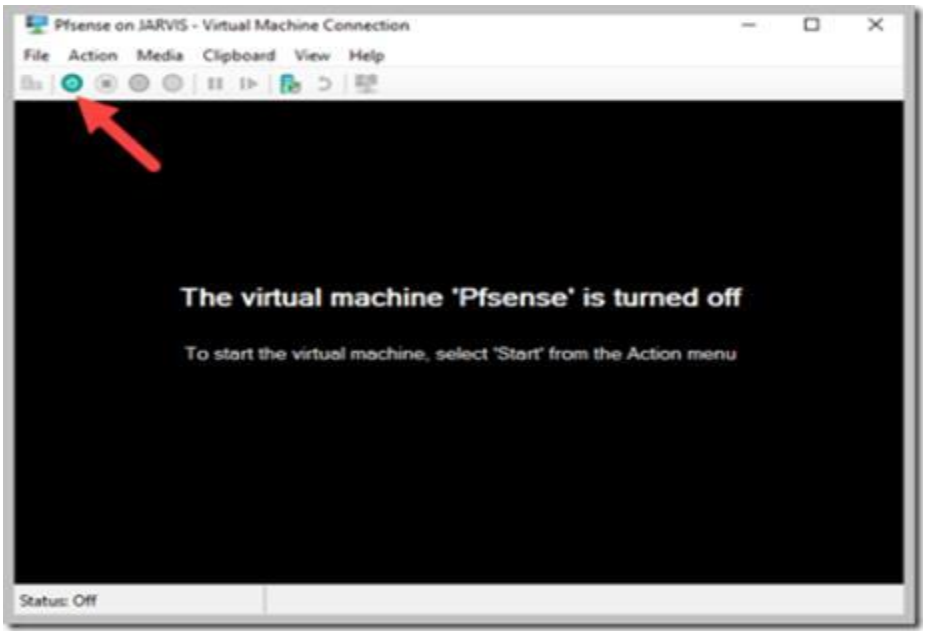
- Select the “Internal” adapter from left menu and choose “External” from the drop down. This is done to flip the order. ***“External” adapter should be the first network adapter followed by “Internal” adapter as shown in the subsequent diagram***



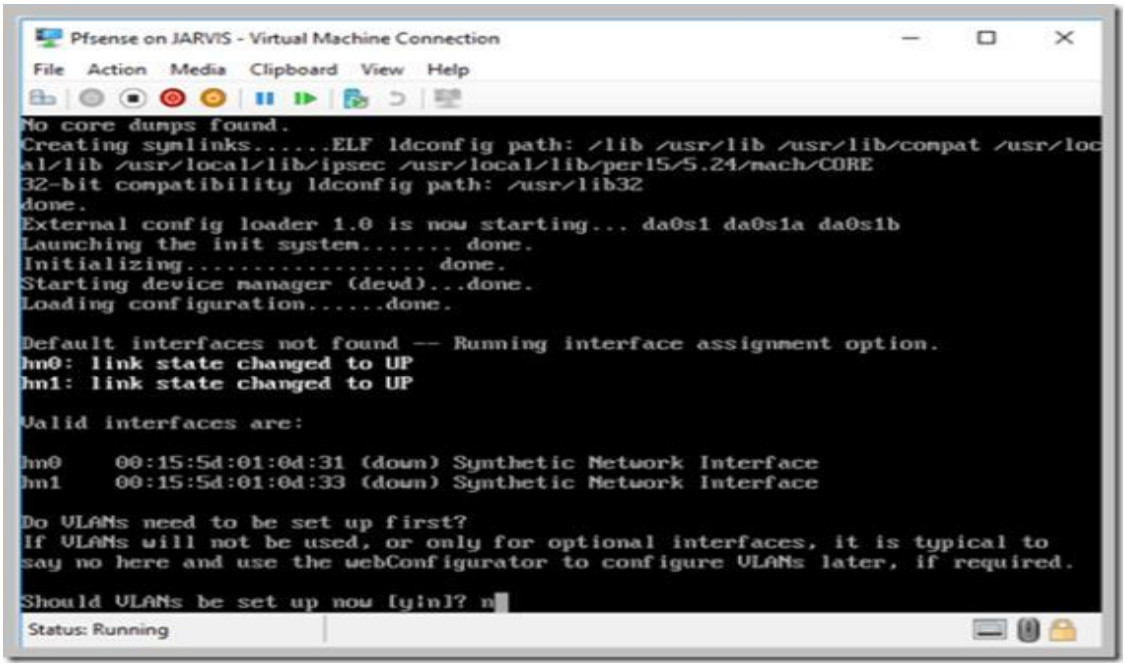
- Figure below shows the correct order of network adapters.



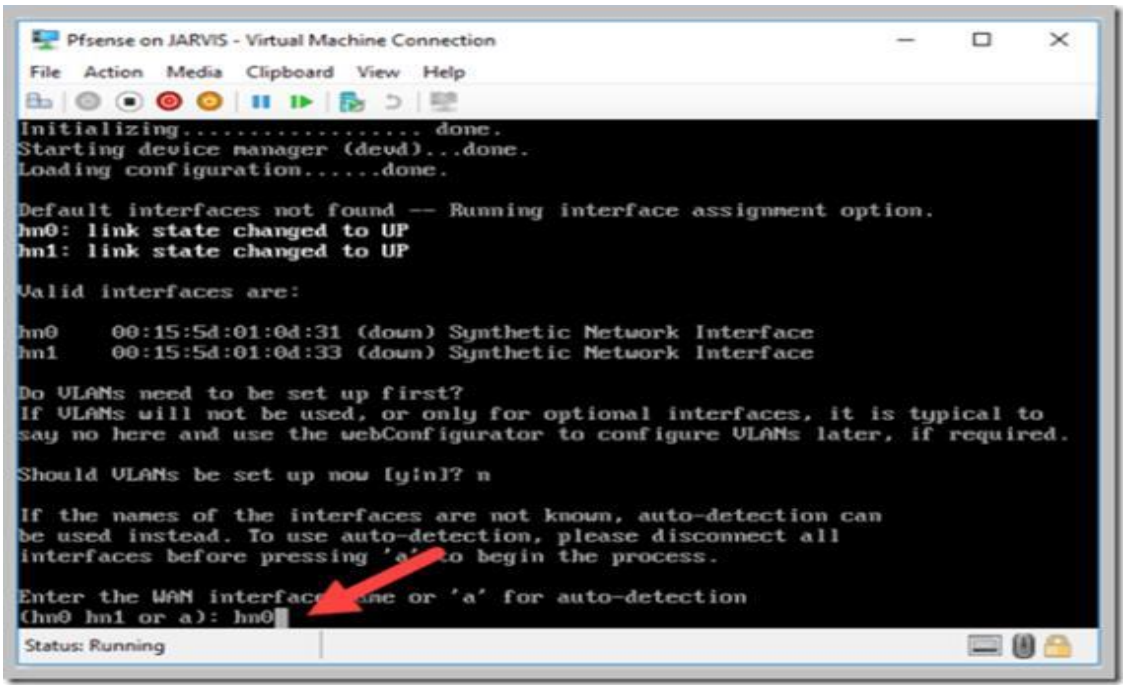
- Start the VM



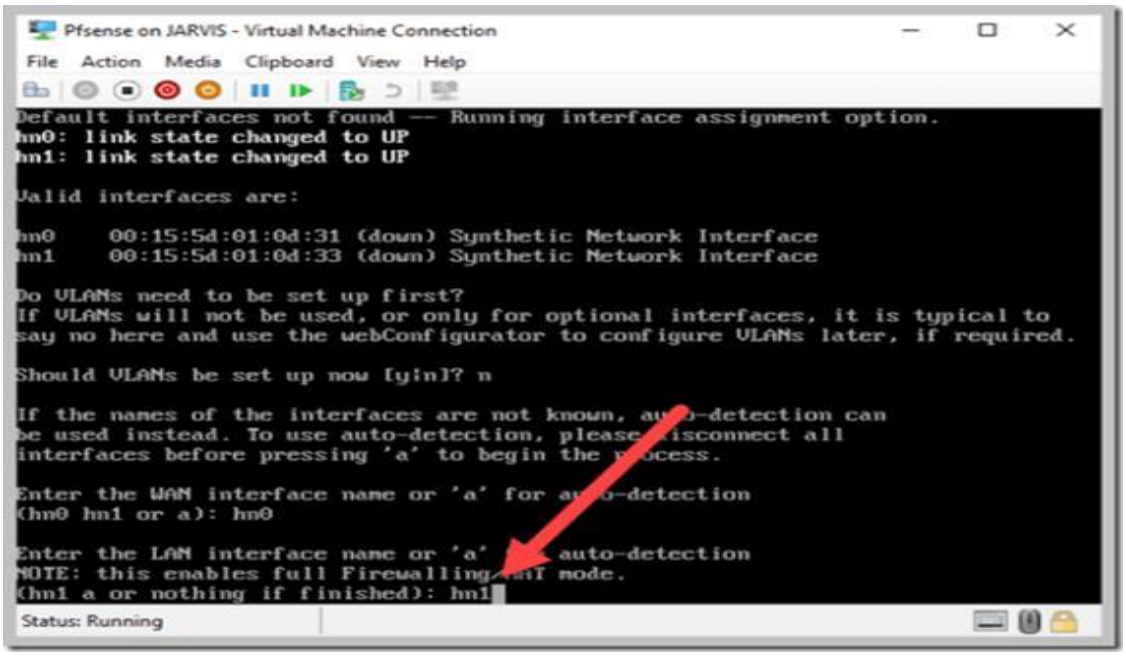
- Choose “n” for VLAN setup



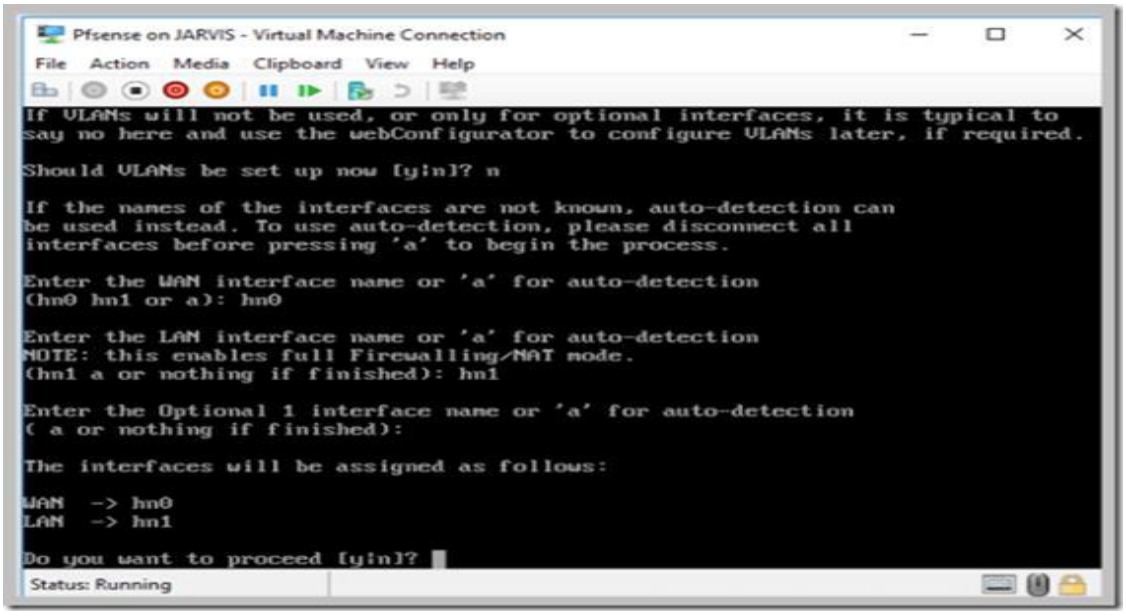
- Choose **hn0** for WAN interface



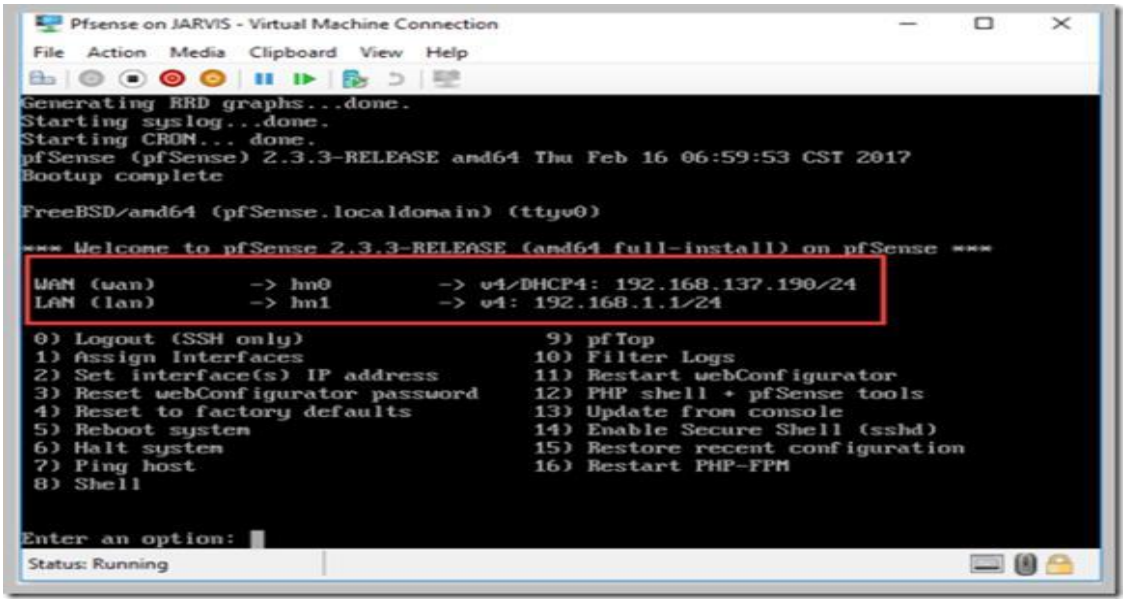
- Choose **hn1** for LAN interface



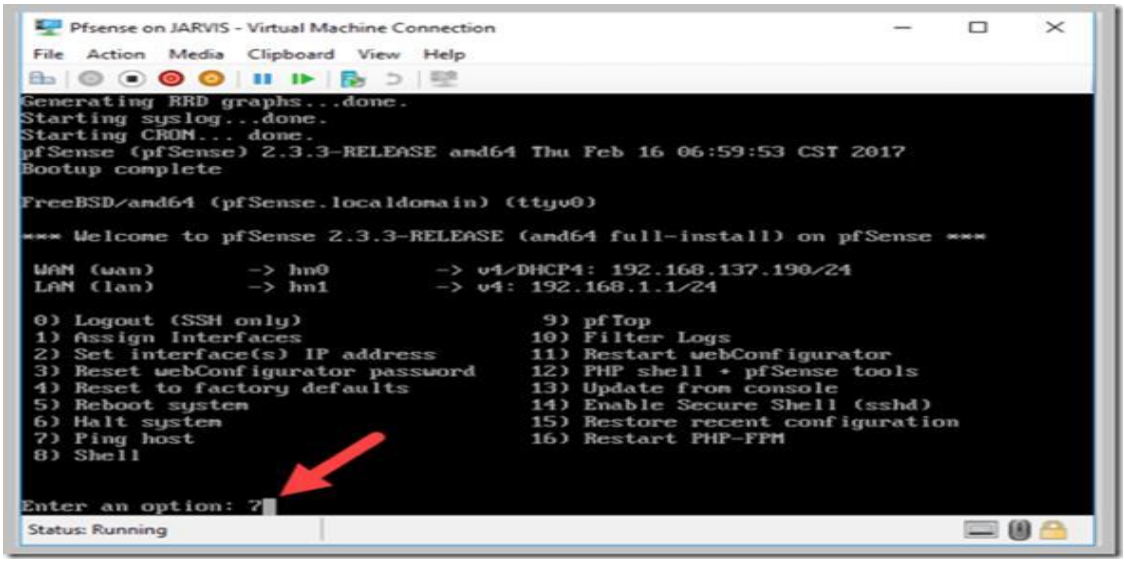
- Choose “y” to complete the setup process



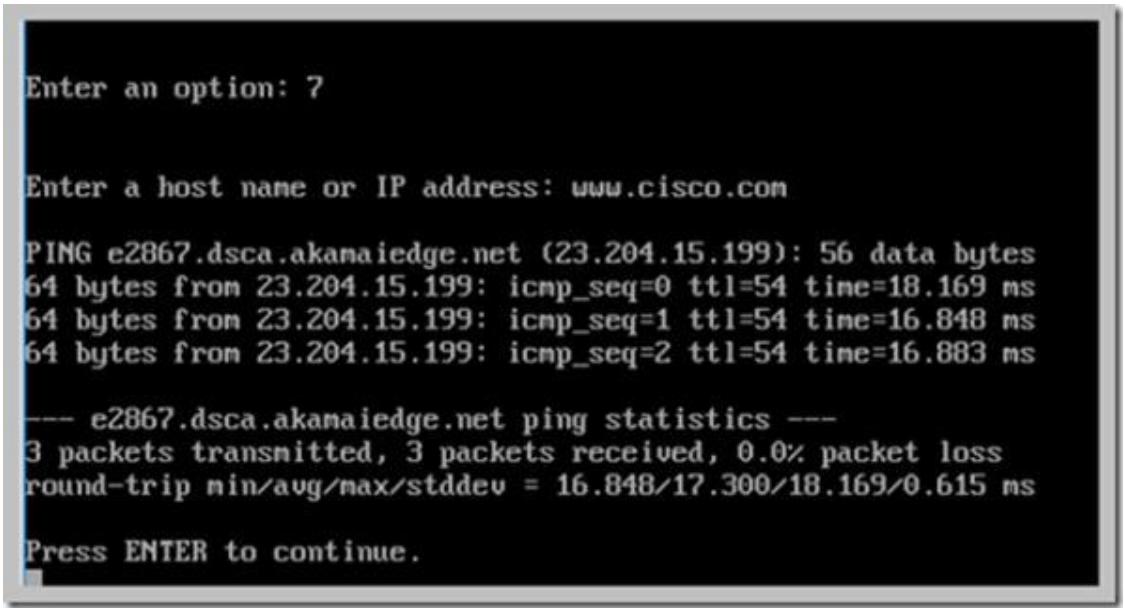
- WAN will pick up an IP using DHCP and LAN segment will also use a default 192.168.1.1/24 address range



- Choose option 7 to check internet connectivity

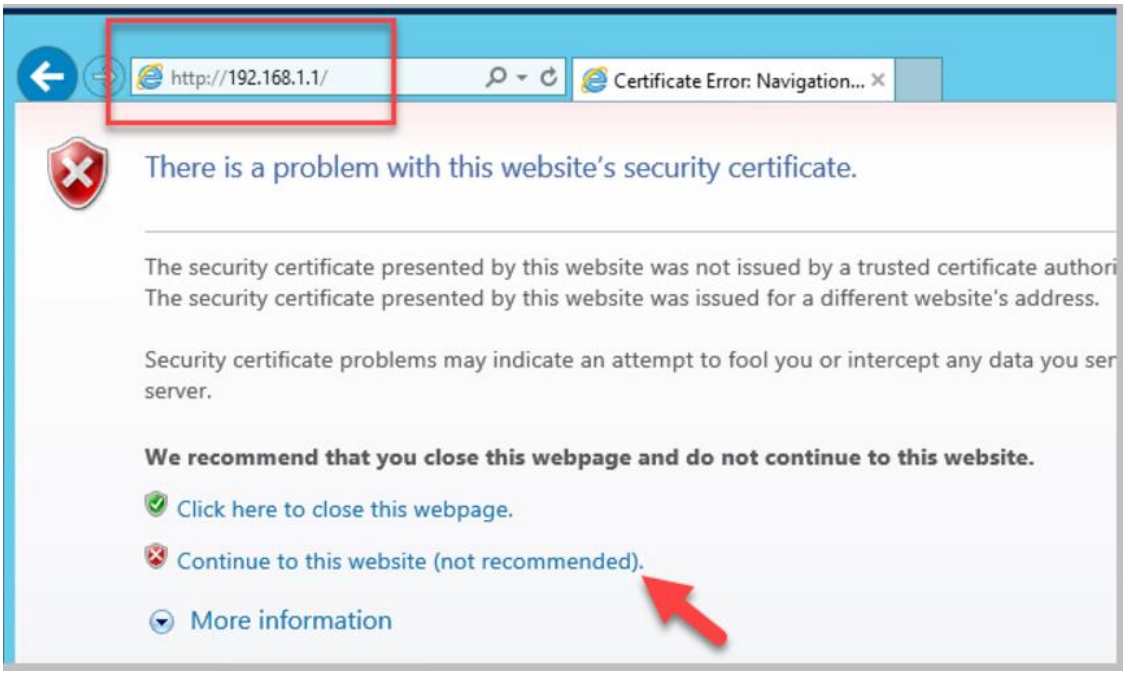


- ping **www.cisco.com** and make sure you get valid responses.

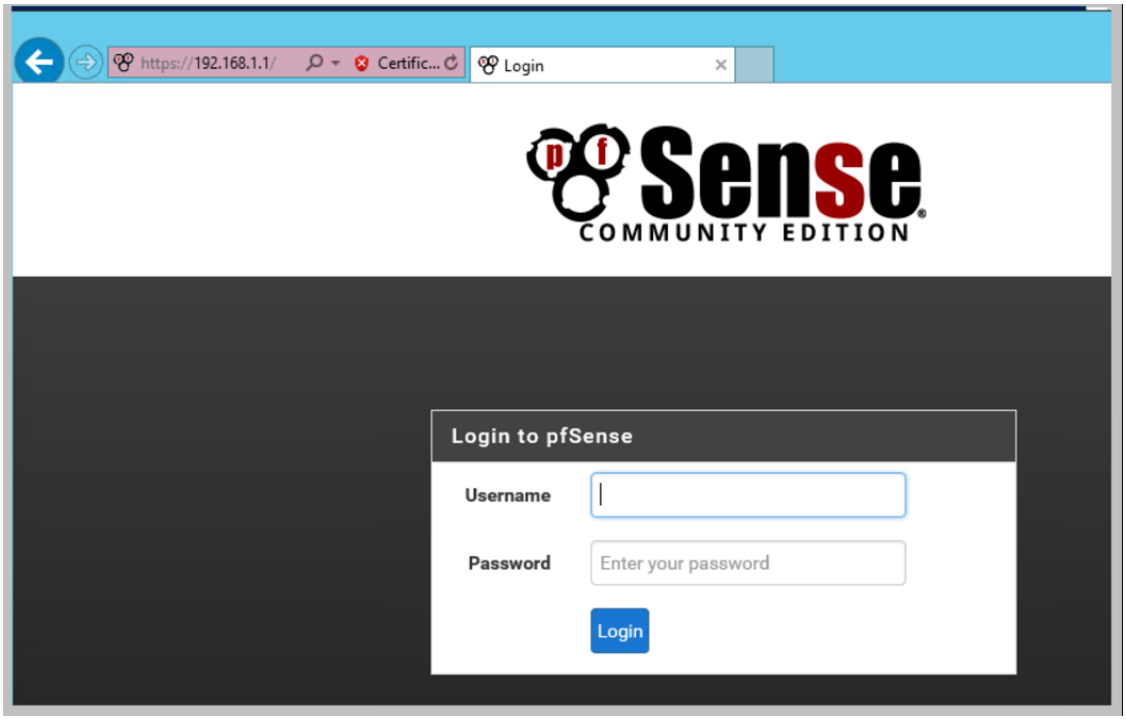


9. Setting up PFSense

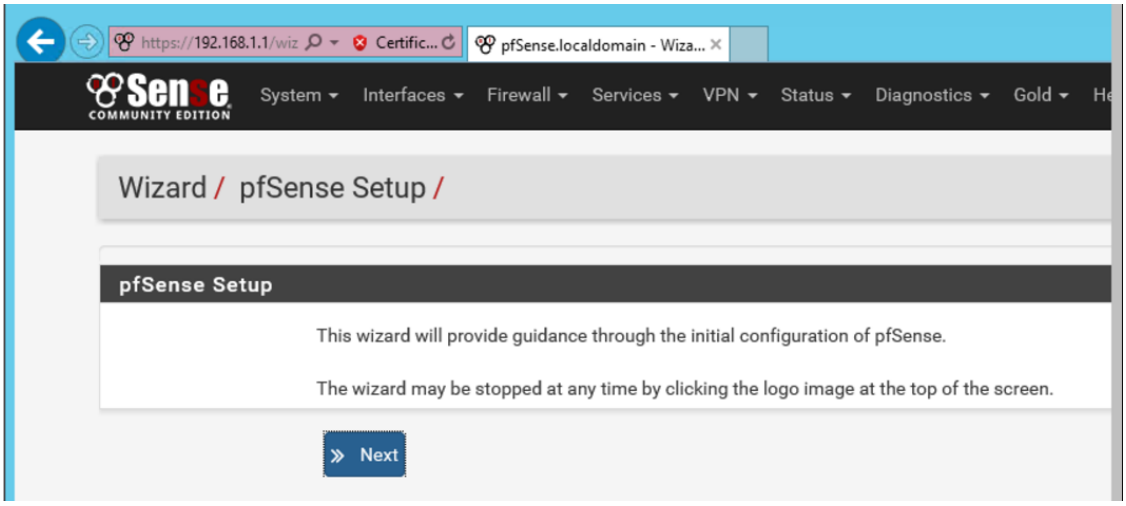
- PFSense must be configured prior to configuring our lab. From Windows 2012 system or any other lab system, open explorer and go to https://192.168.1.1. Click "Continue to this website"



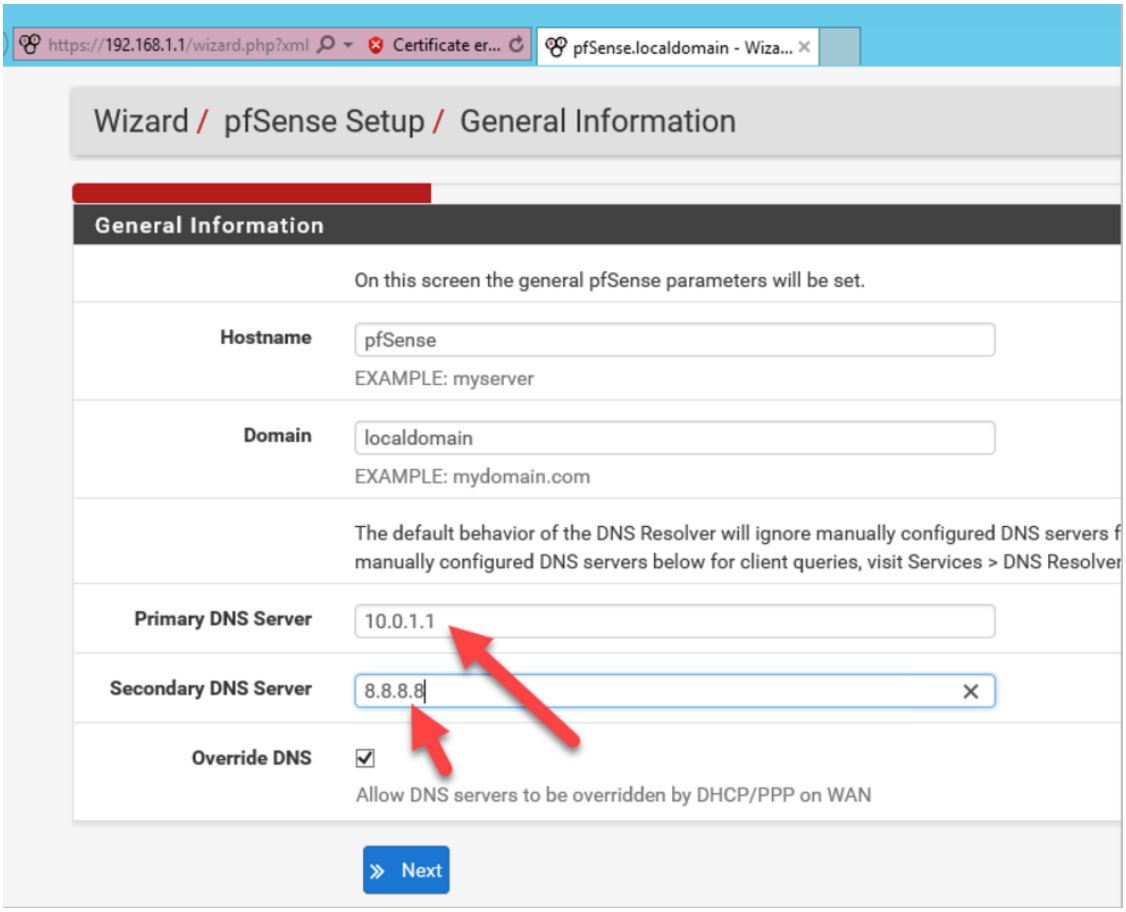
- Login with admin/pfsense



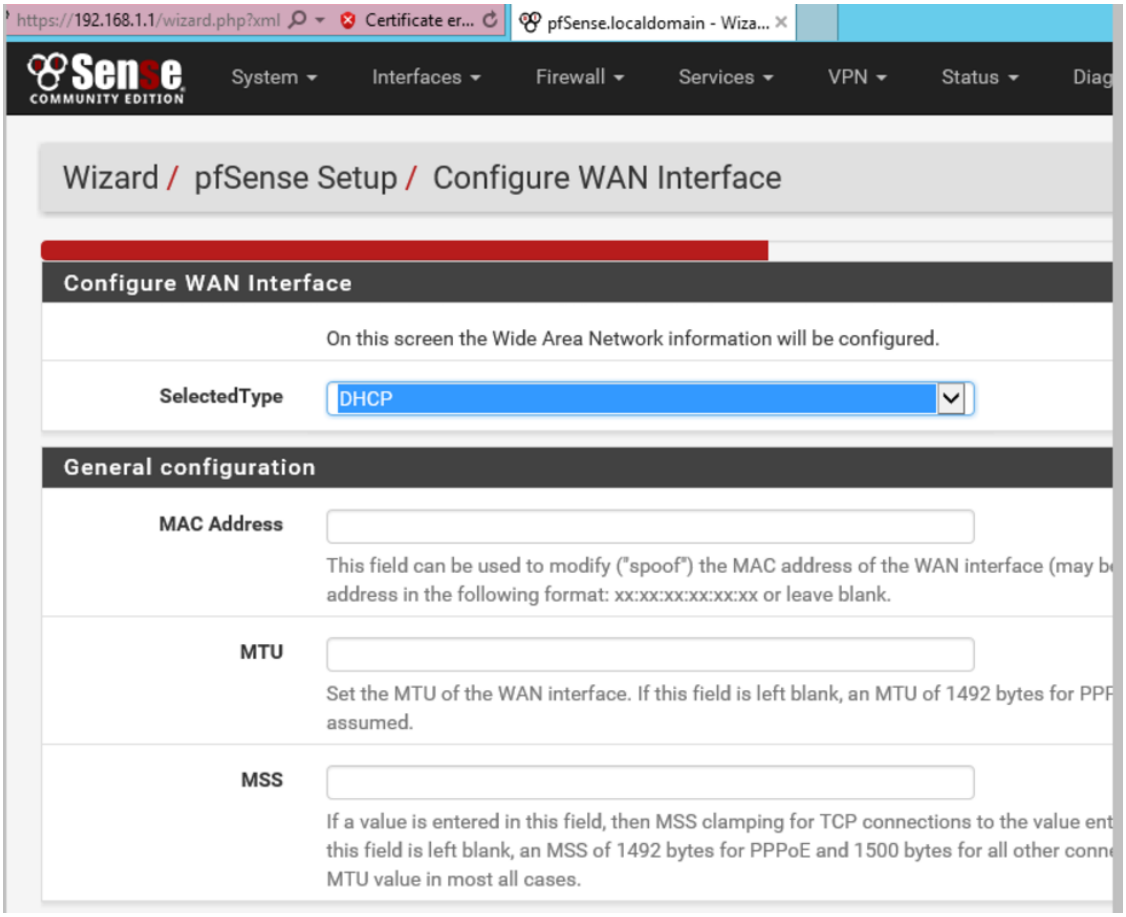
- Click “Next” to continue



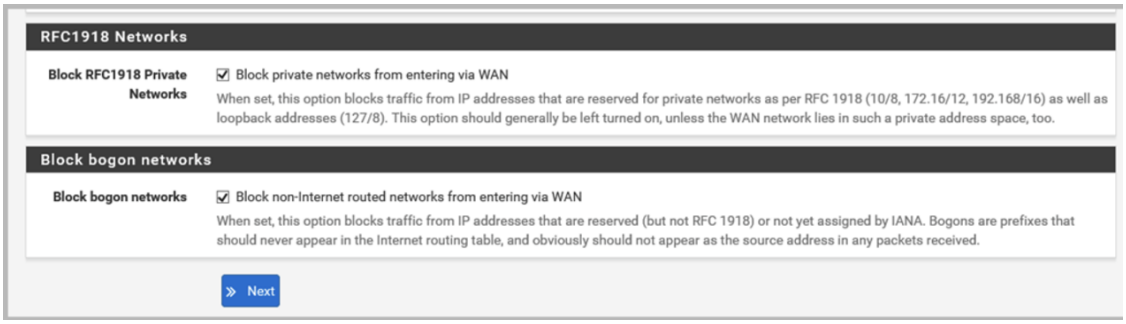
- Use your host system gateway address for primary DNS. Type ipconfig /all in you host computer and use the DNS server address.



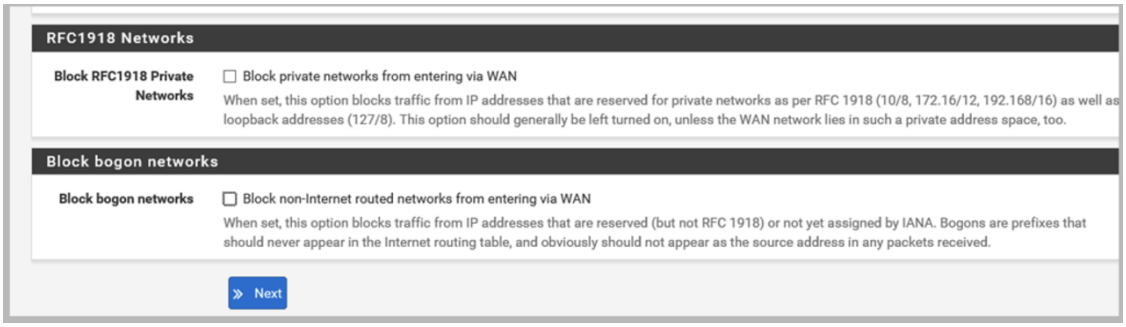
- Let's use DHCP for WAN interface, so our host system will assign IPs automatically



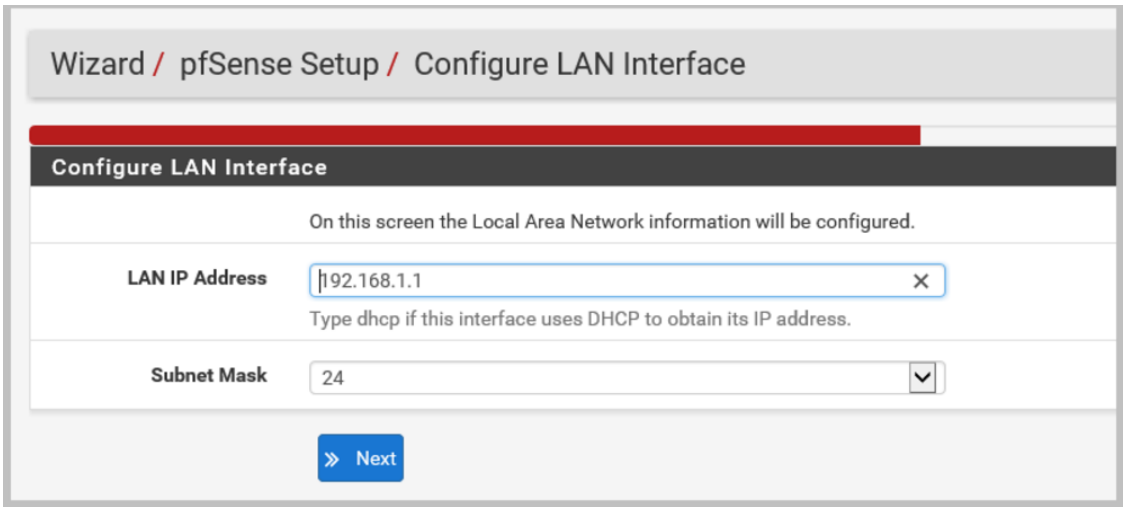
- Scroll down to the RFC settings in the bottom



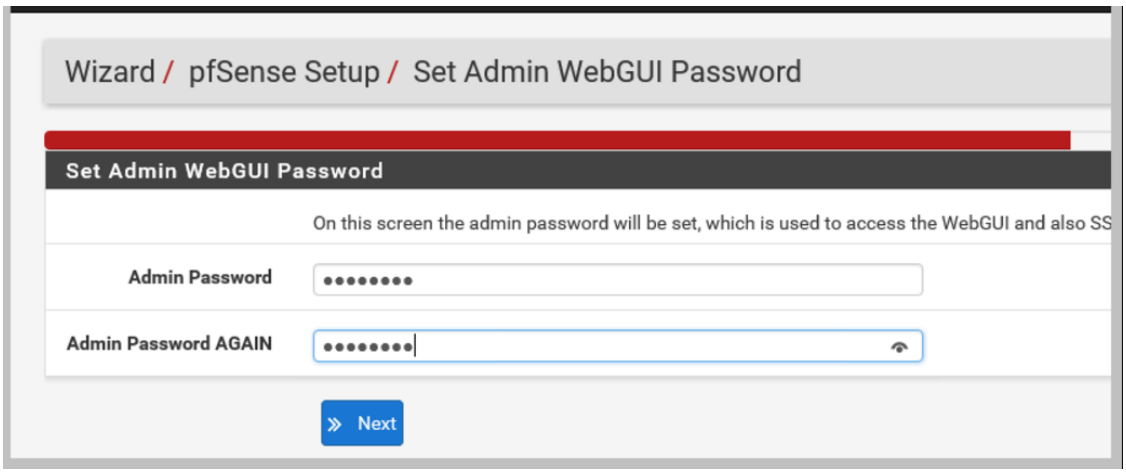
- Uncheck the boxes



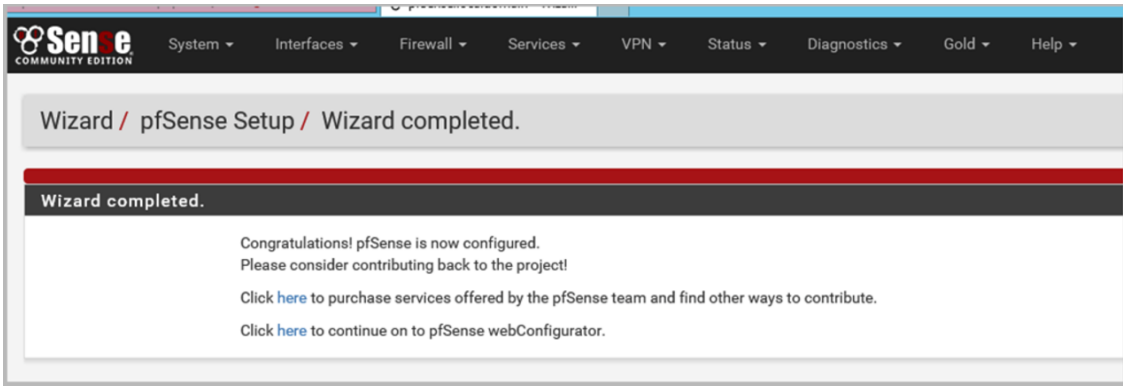
- Click “next” to continue



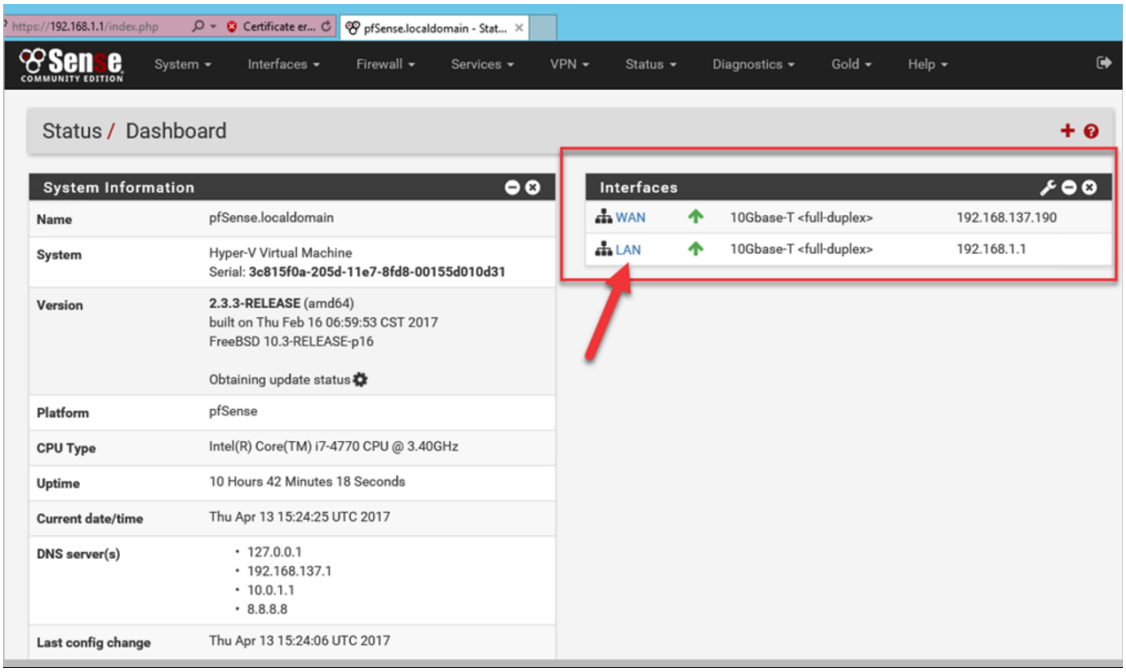
- Click “next” to continue and change the admin password



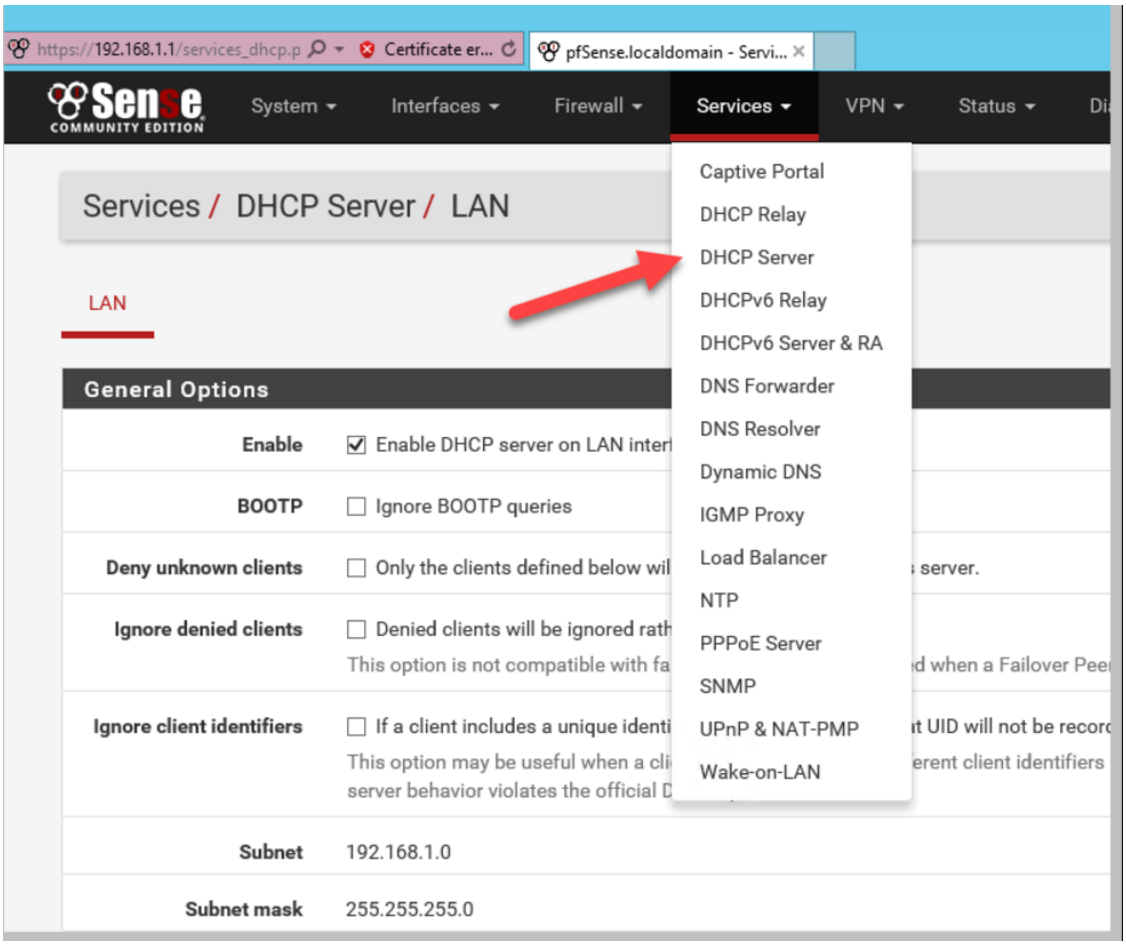
- PFSense setup is now complete



- Go to Menu “Status” and click dashboard. Click on “LAN” interface



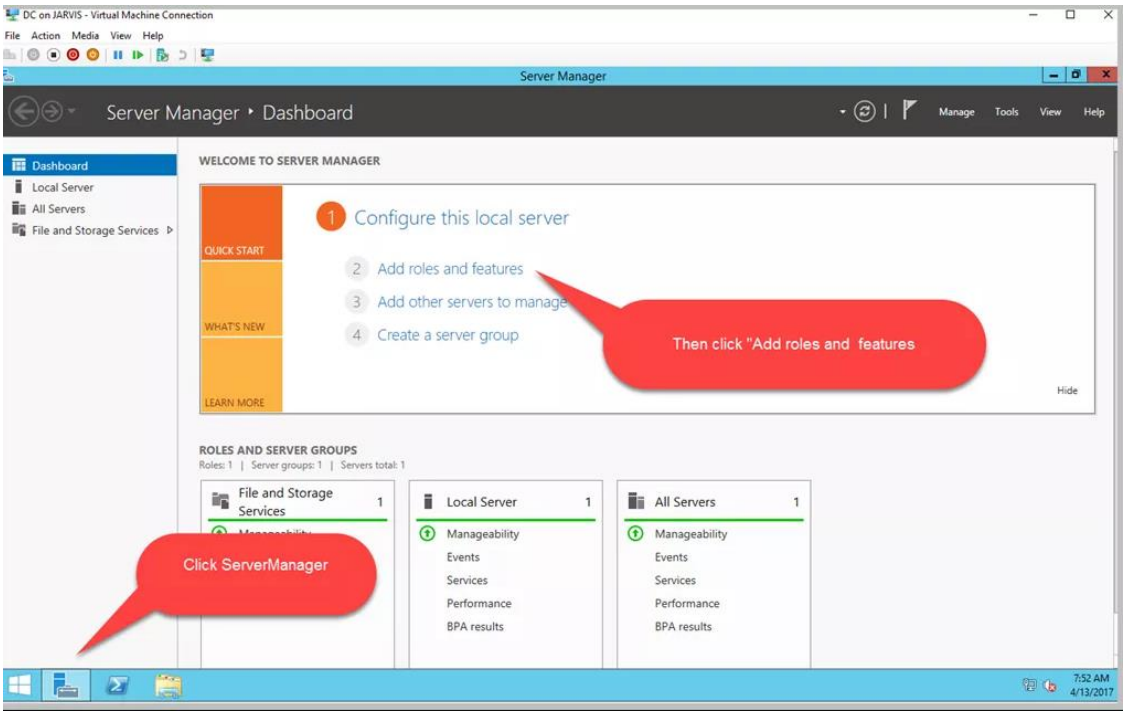
- Go to “Services” menu and click “DHCP Server”



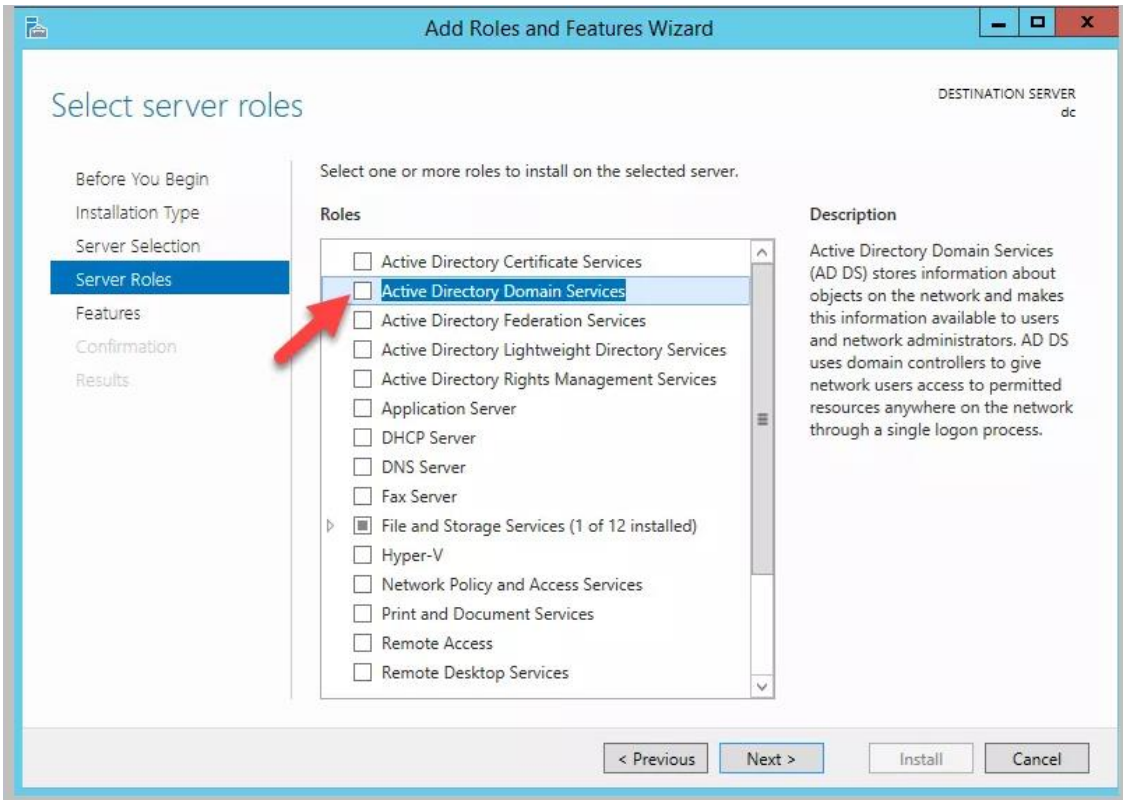
- Uncheck the “Enable DHCP server on LAN interface”. We will setup DHCP role in Windows 2012 server, which will be used to hand out IPs to client systems. Save the settings and we’re done with PFSense for now.

10. Promoting Windows 2012 Server to Domain Controller

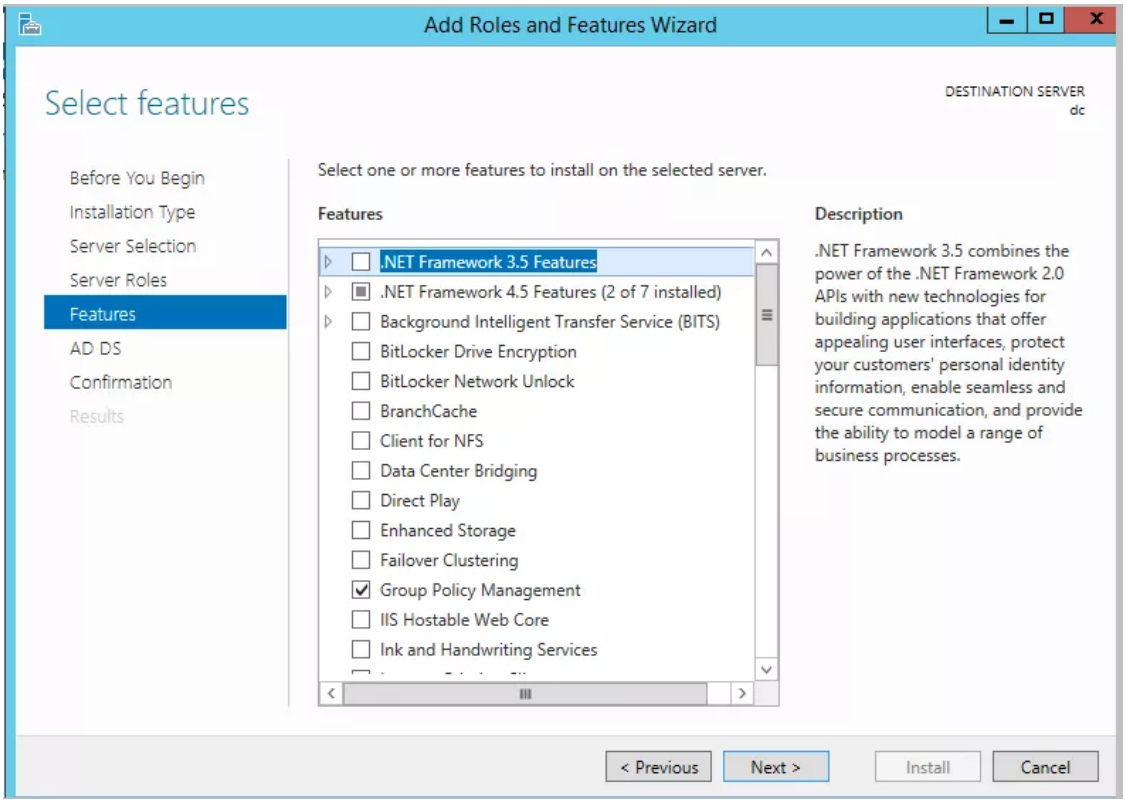
- Let’s promote Windows 2012 to Domain Controller. Connect to Windows 2012 system and launch “ServerManager an Click “Add roles and features”



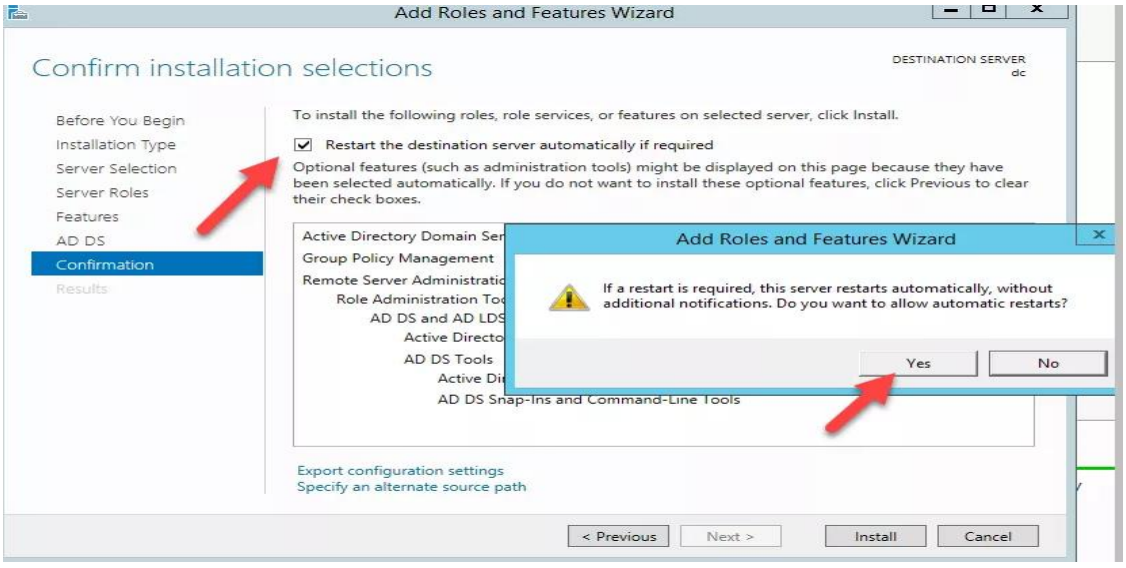
- Check “Active Directory Domain Services”



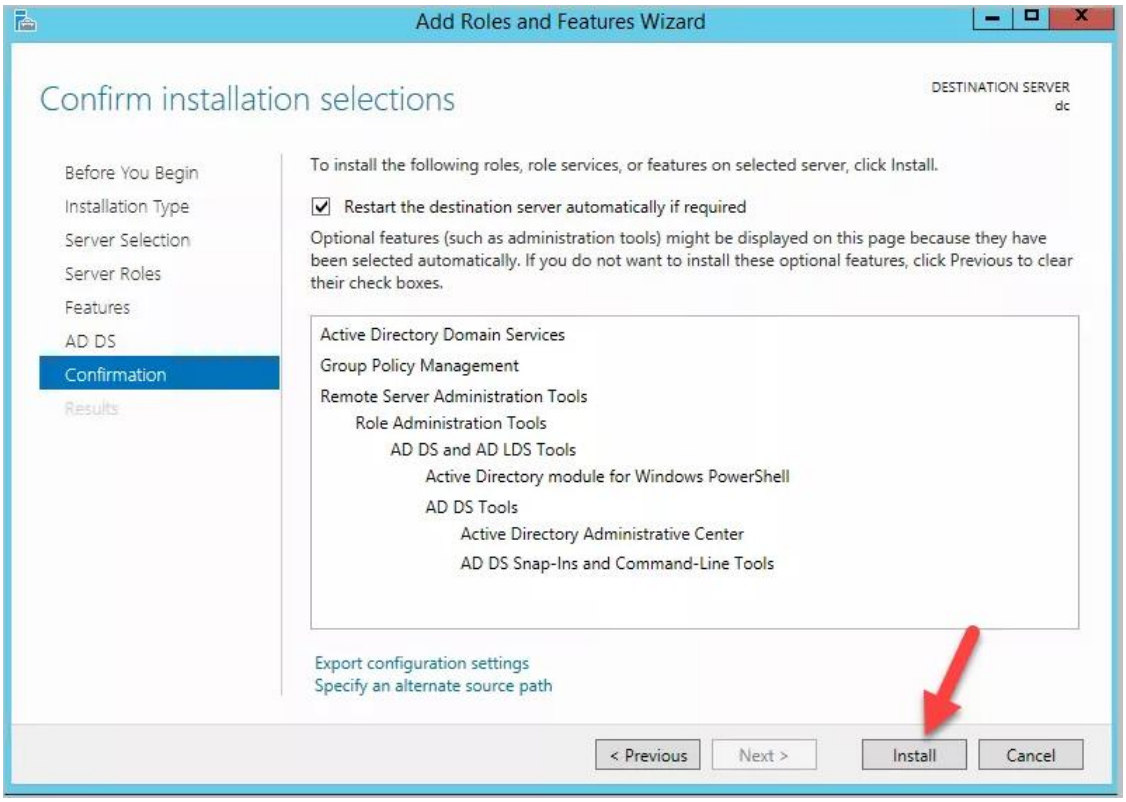
- Use the defaults



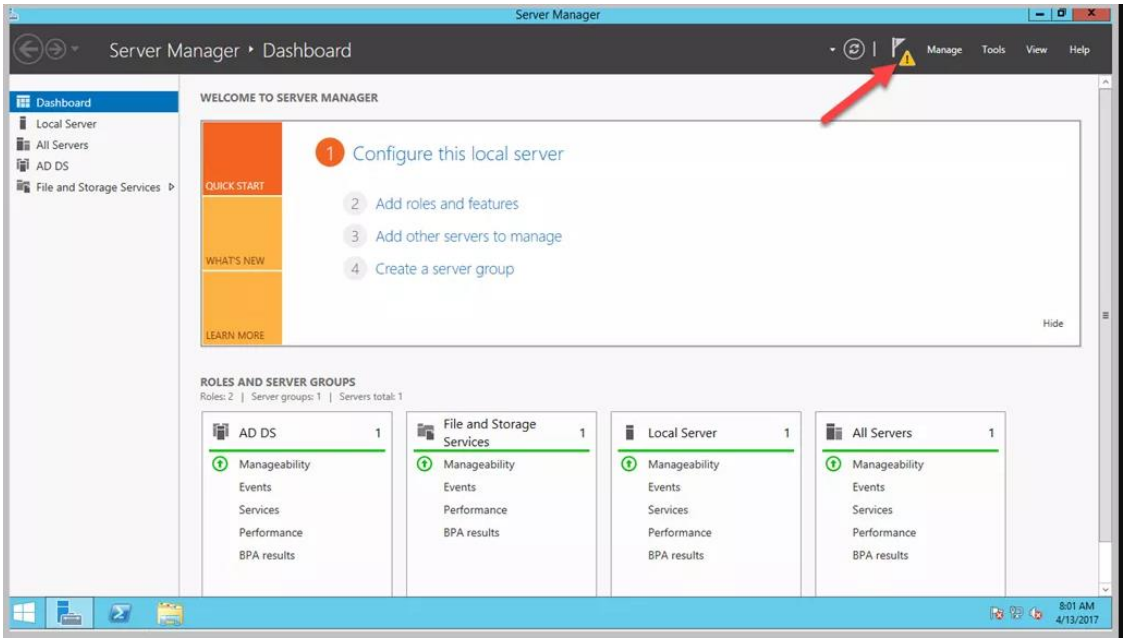
- Check the box and click “yes”



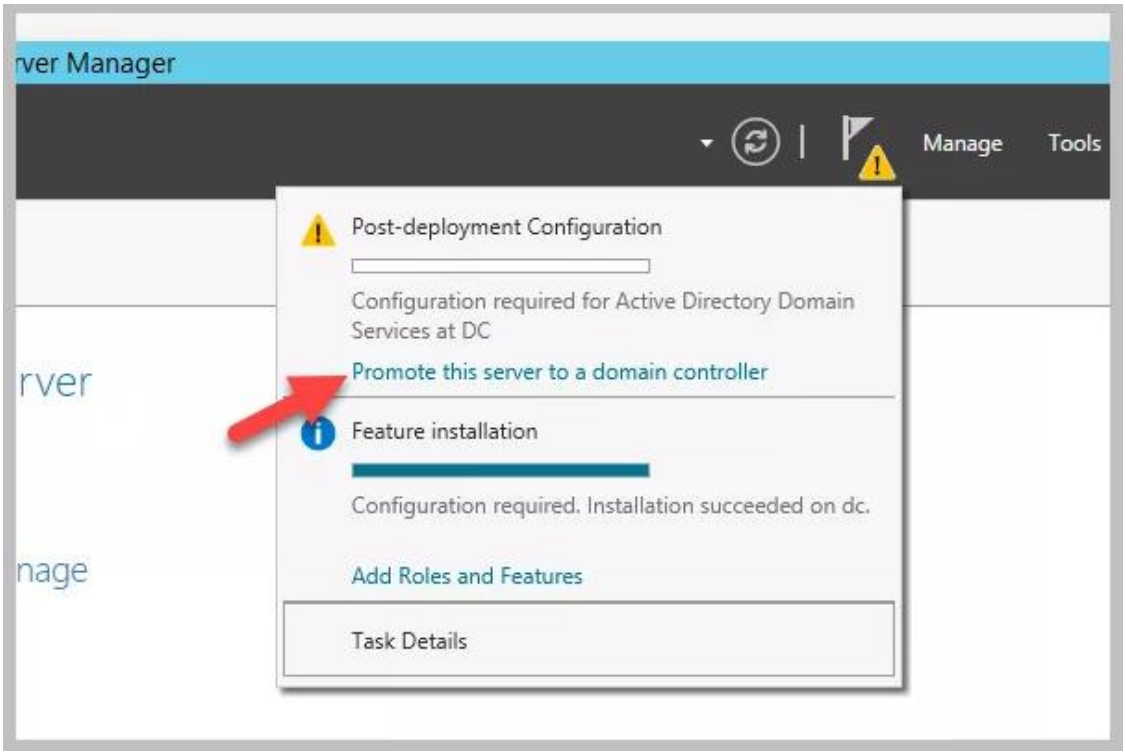
- Click Install and wait for the process to complete



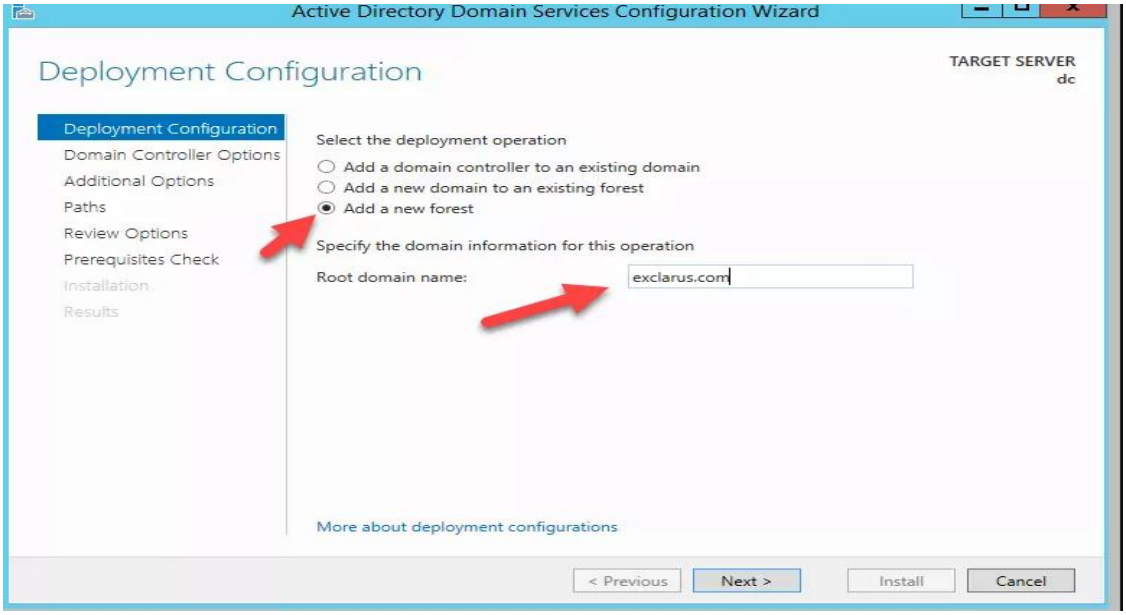
- Click the "**Exclamation**" mark and shown



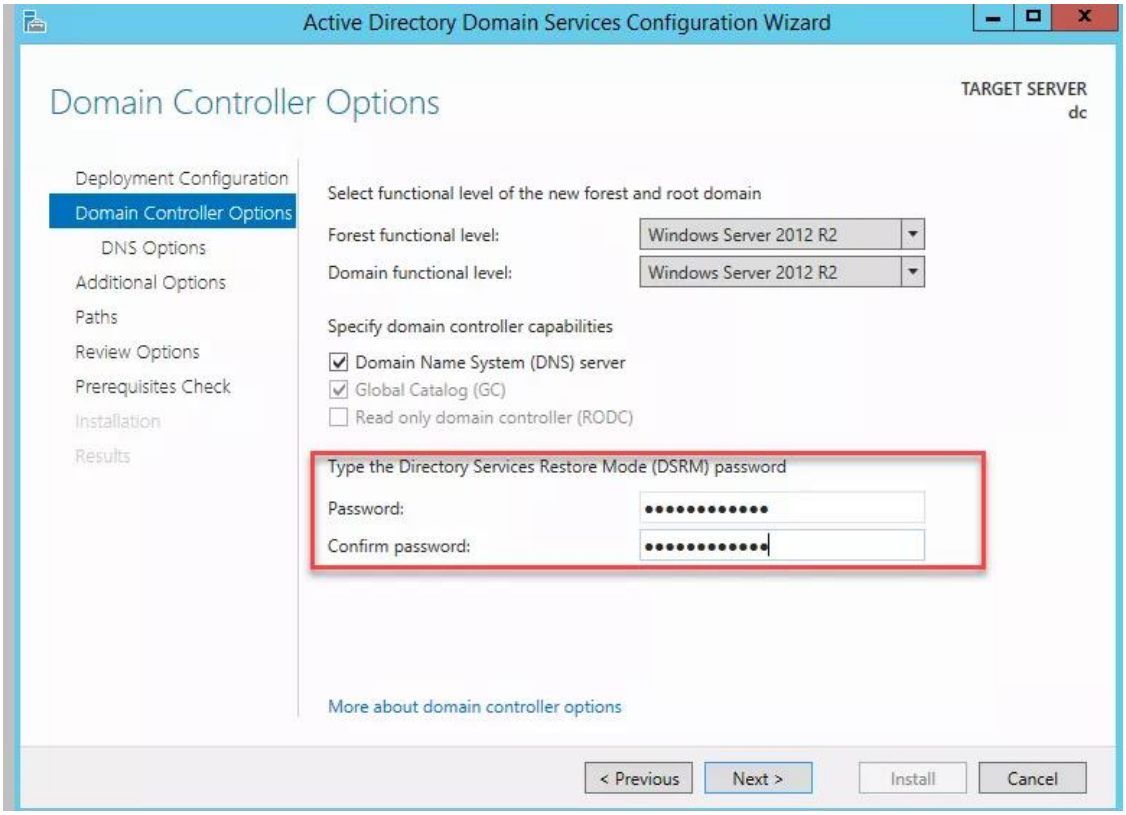
- Click on "Promote this server to a domain controller"



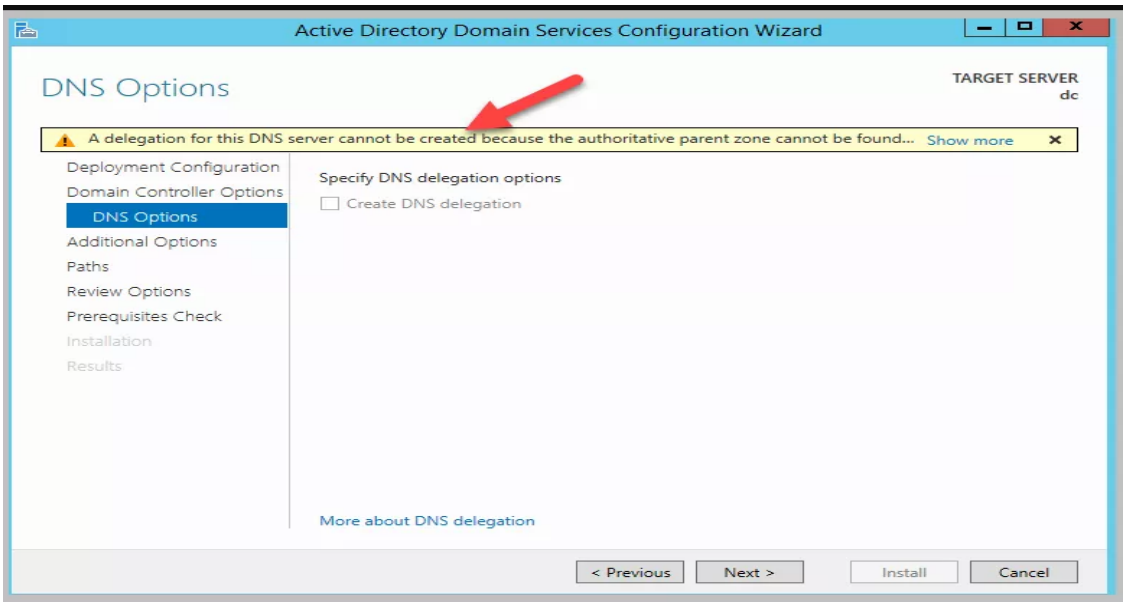
- Check the radio box “Add a new forest” and use a domain name. Feel free to use any domain name



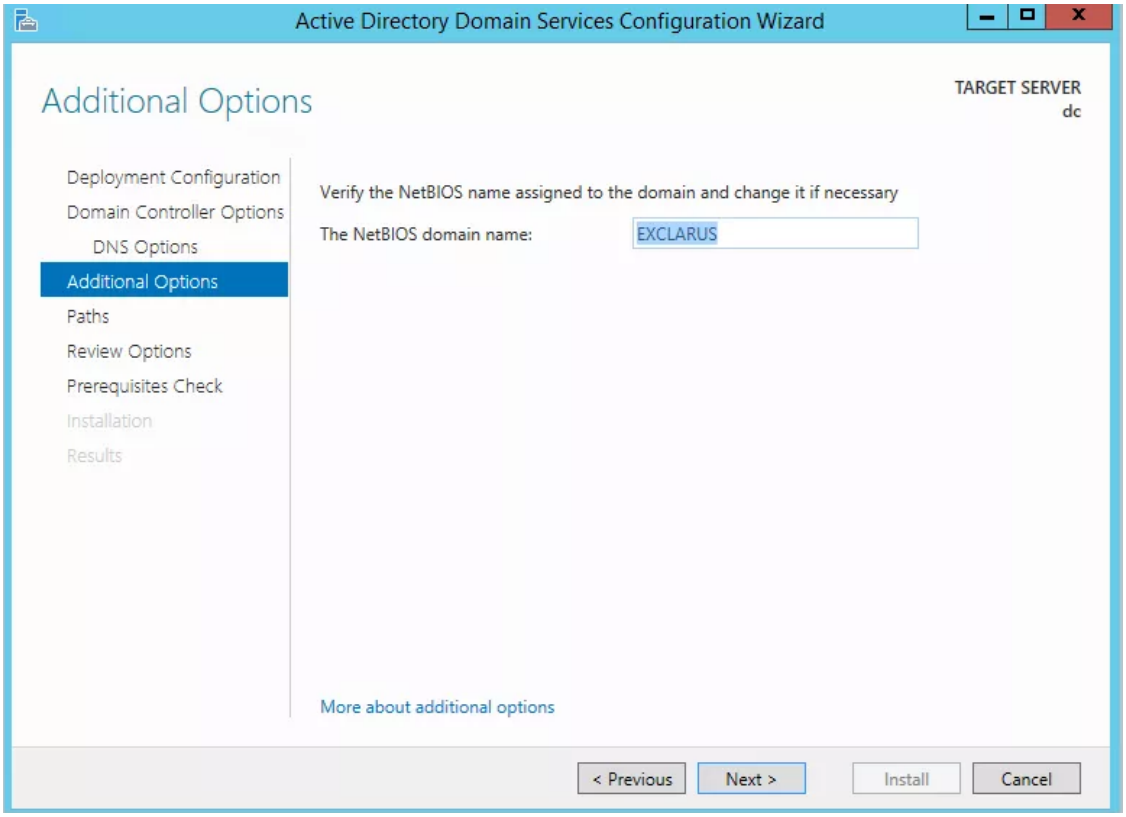
- Use a strong password for restore mode



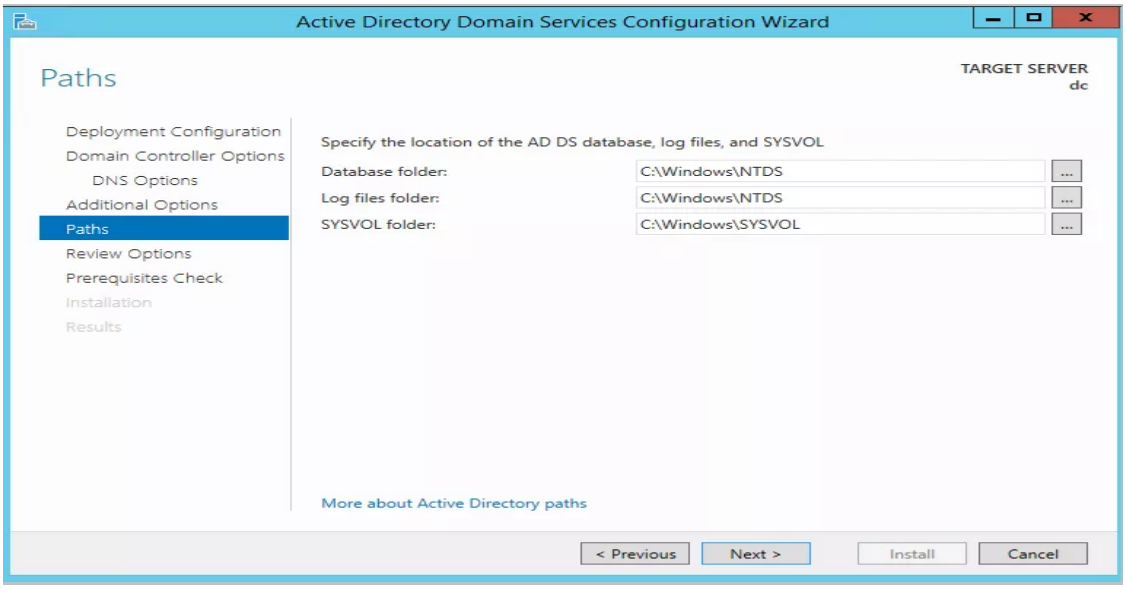
- DNS services will be installed automatically so ignore this warning



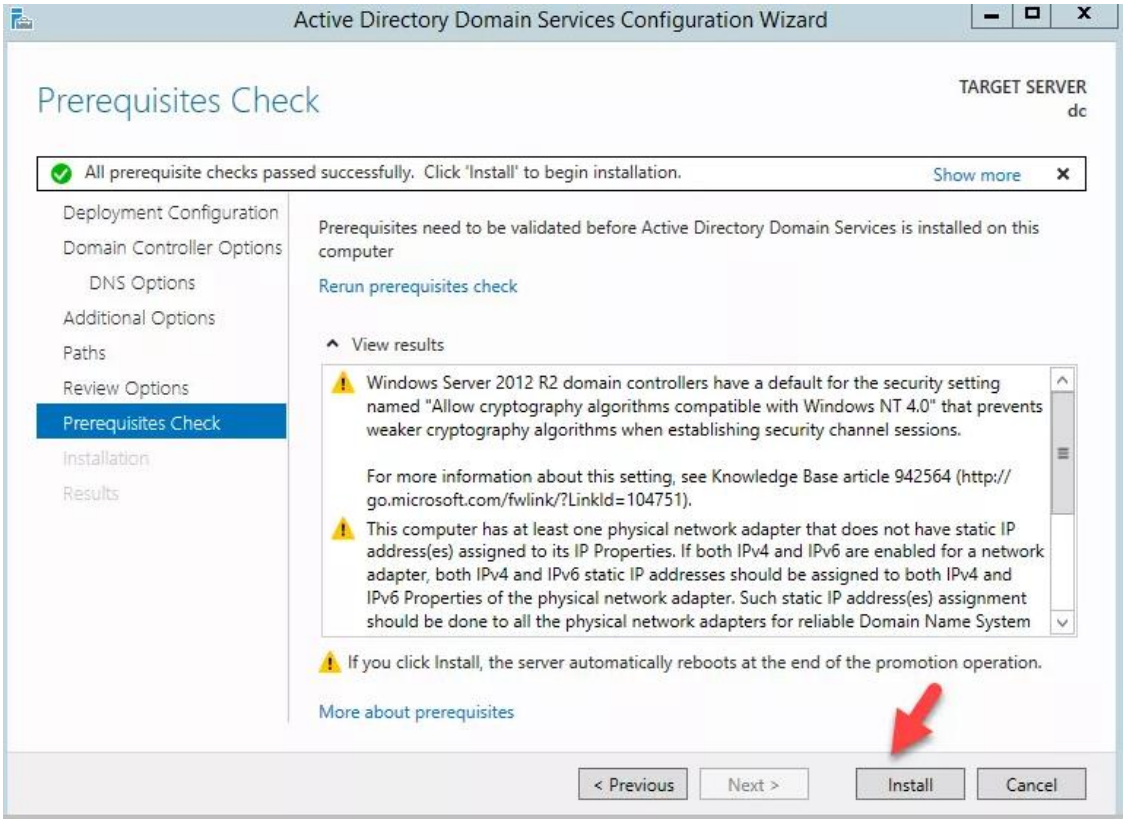
- Use the default netbios name



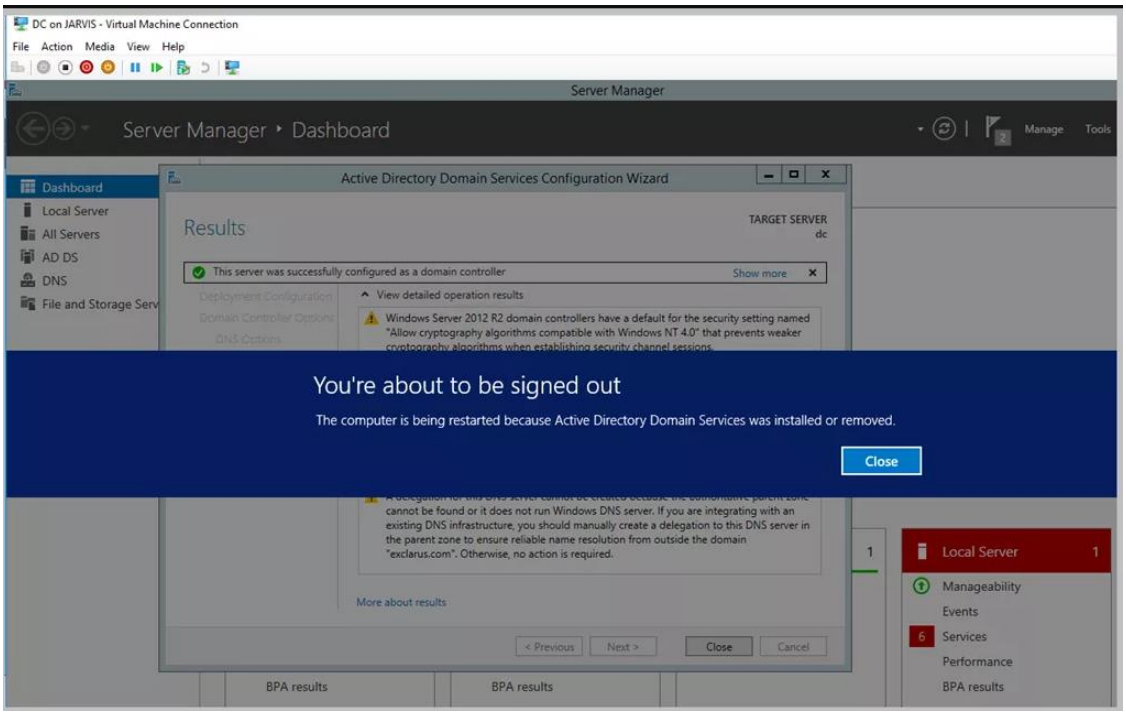
- Production active directory servers will change the location of the following files, but we will stick with the defaults for our lab environment. NTDS is a critical file which has all user hashes.



- Click Install

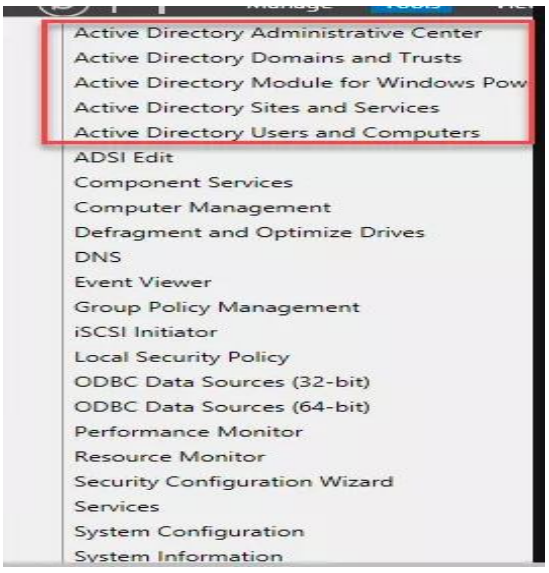


- The server will reboot



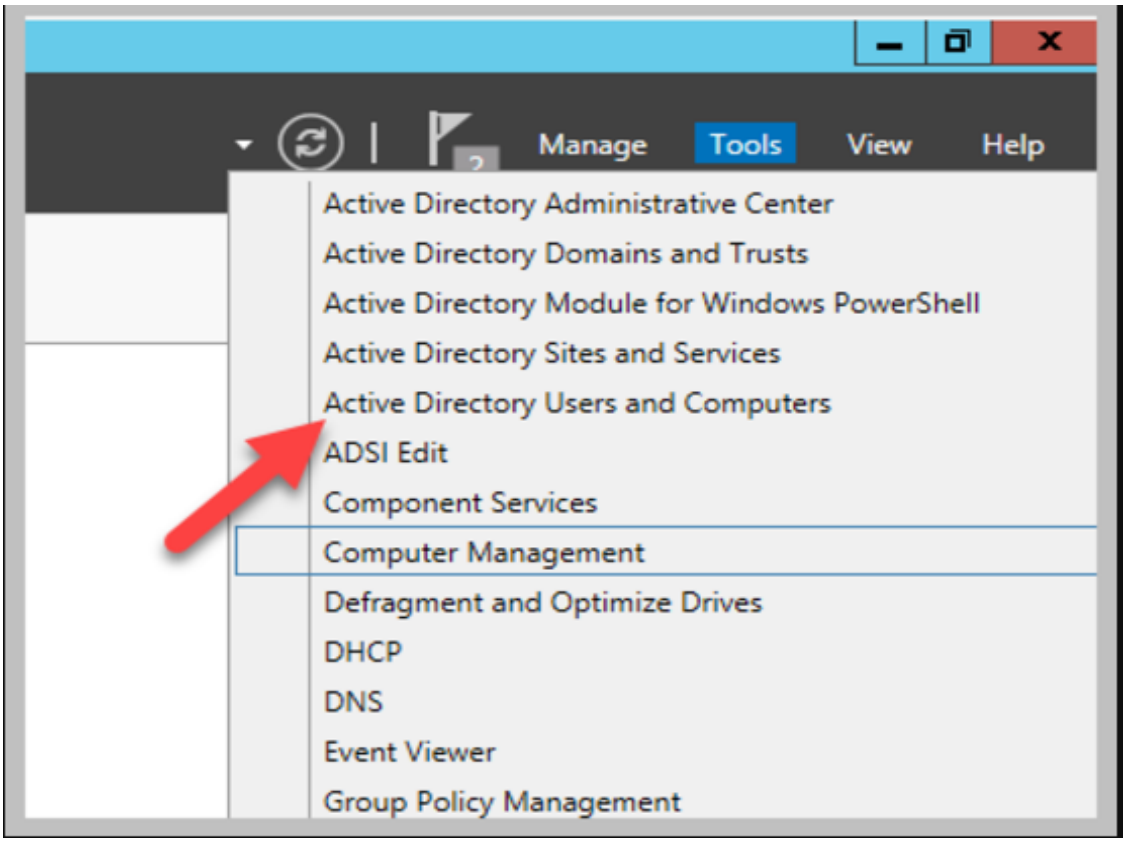
- Now login to the domain controller. The same password is also used for the domain administrator account.

- Tools menu will have additional menu items

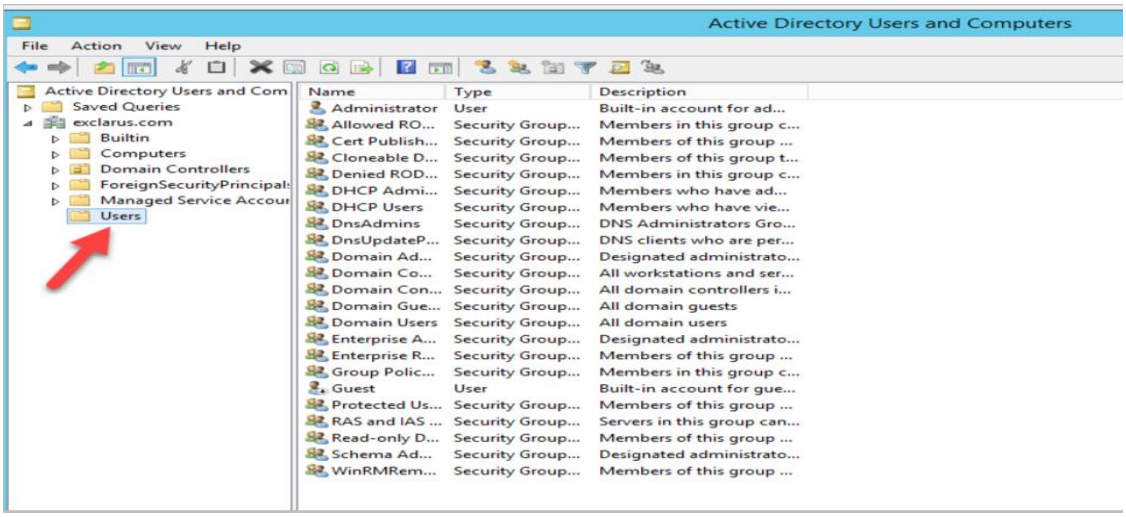


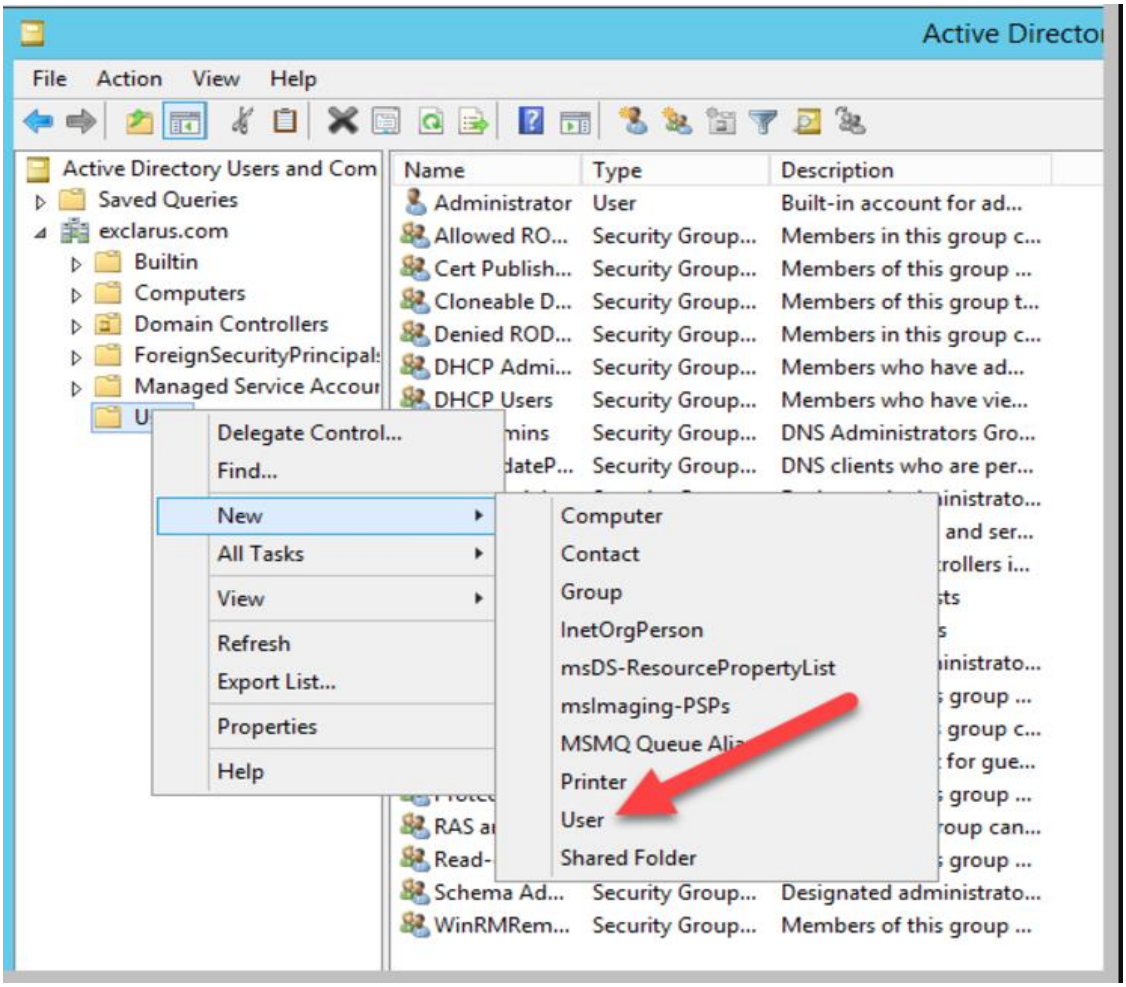
11. Creating Users in Active Directory

- Let's create some users for our client machines to login. Open "Active Directory Users and Computers" from Tools menu

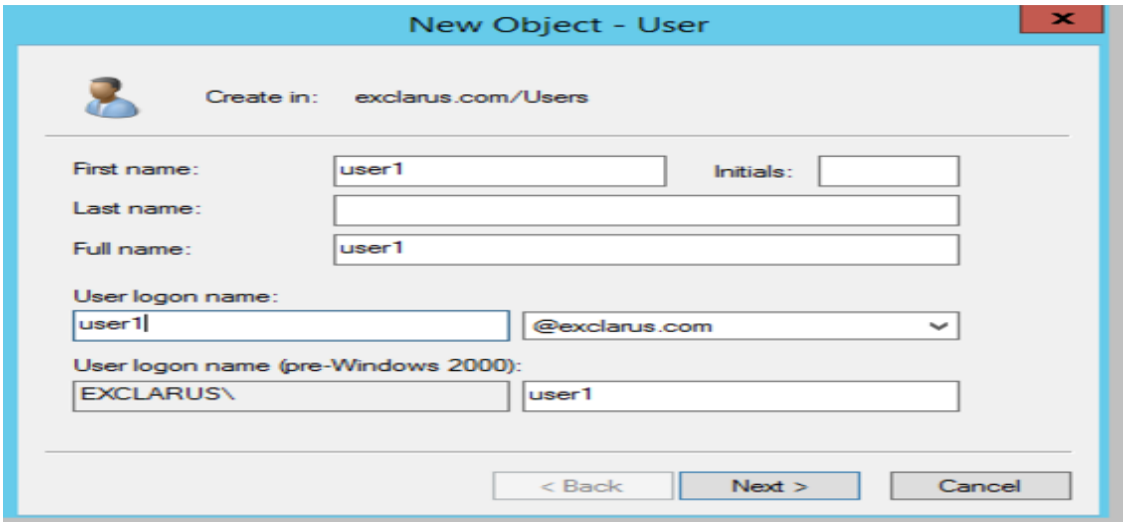


- Right click on users and "New User" as shown below





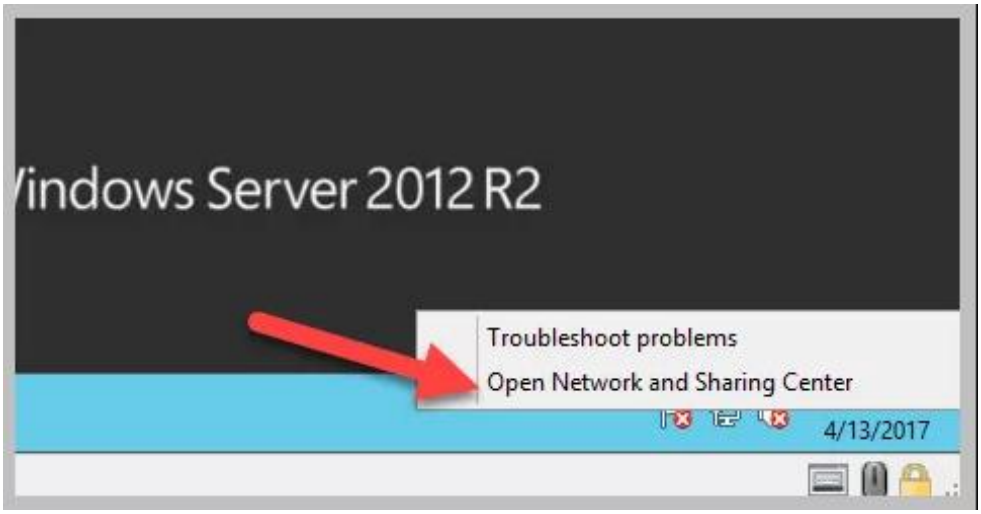
- Type the relevant details. I'm creating a user called **"user1"**



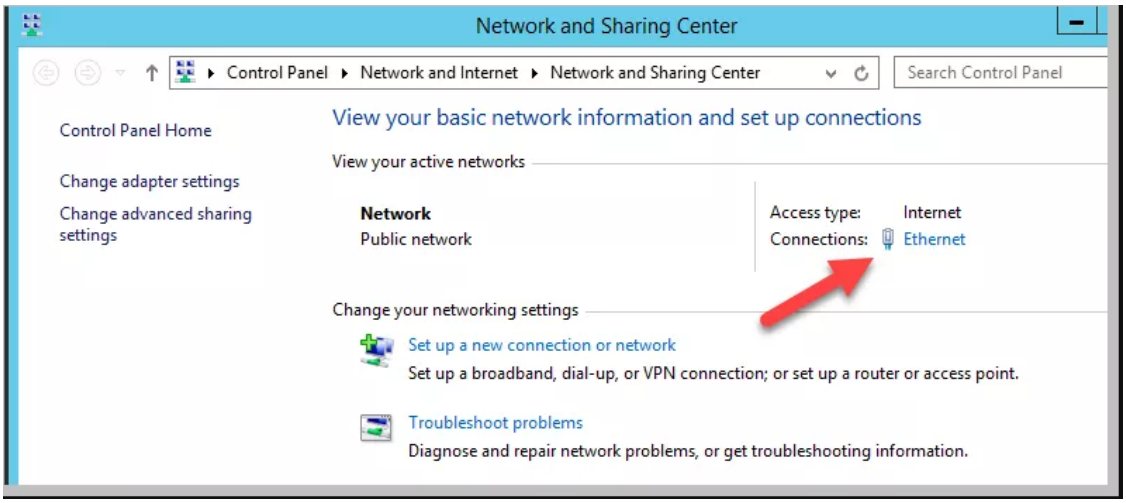
- Now **user1** is a one of the users in the active directory
- Use the same process to create few user accounts.

12. Setting Up Static IP in Domain Controller

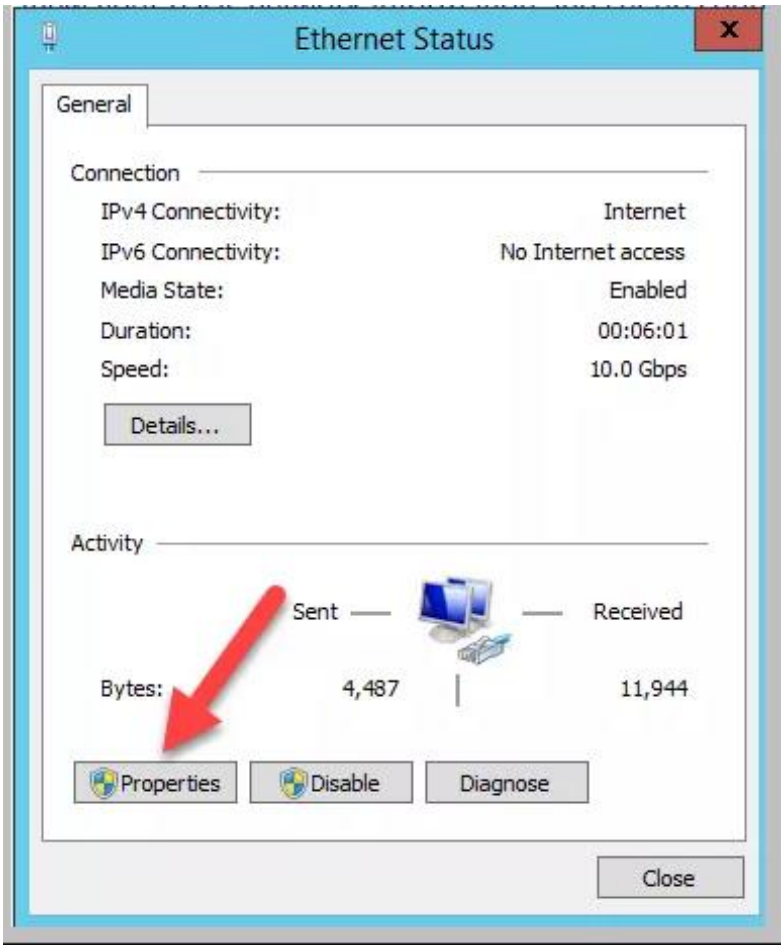
- Right click on the computer and "Open Network Sharing Center"



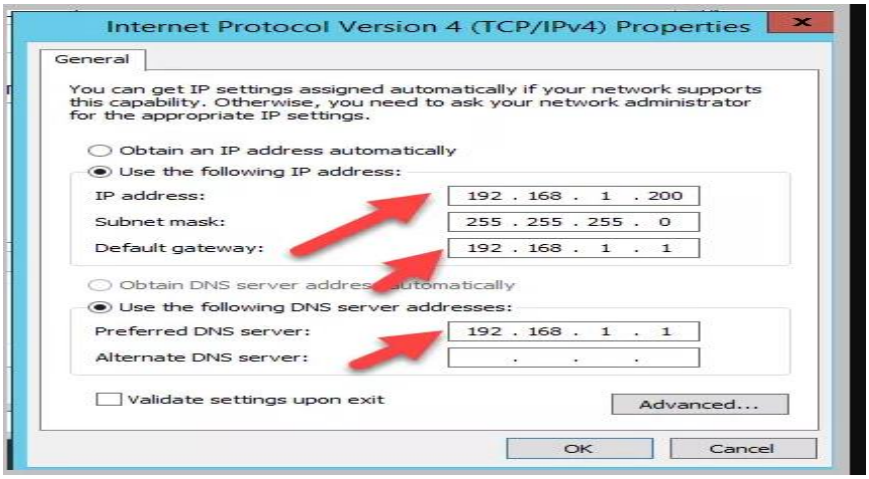
- Click the Ethernet connection hyperlink.



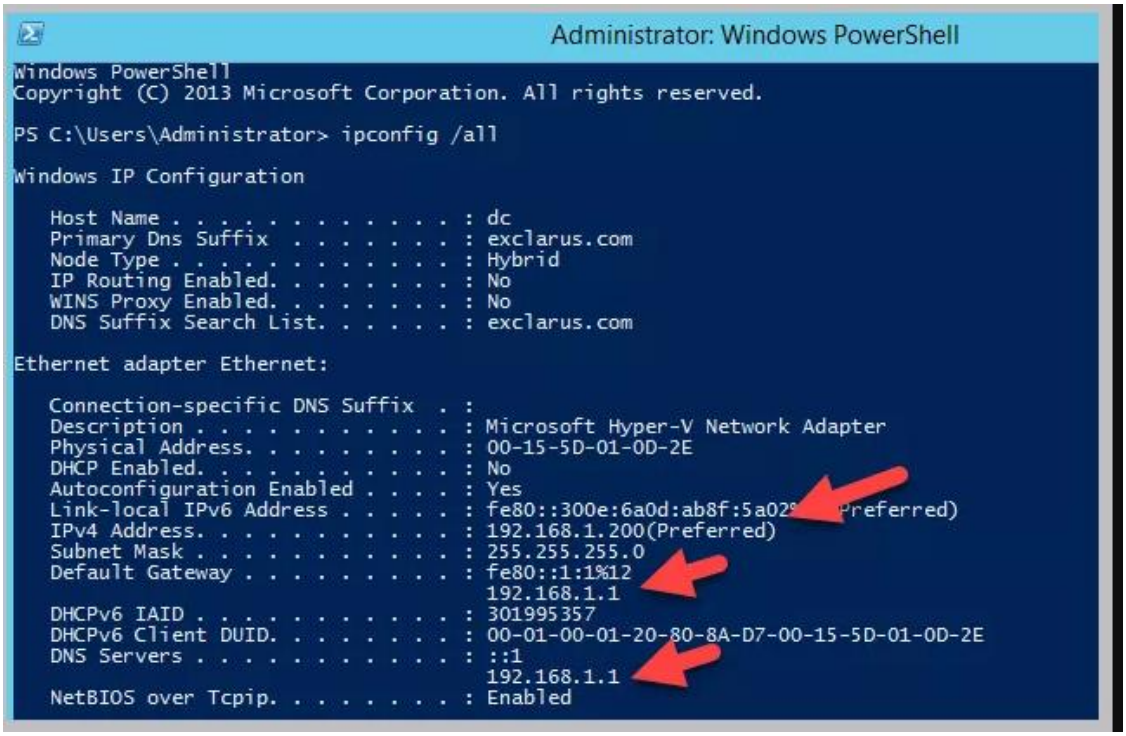
- Click on properties button.



- Use the following configuration or feel free to use any other static IP. Click OK to accept the settings

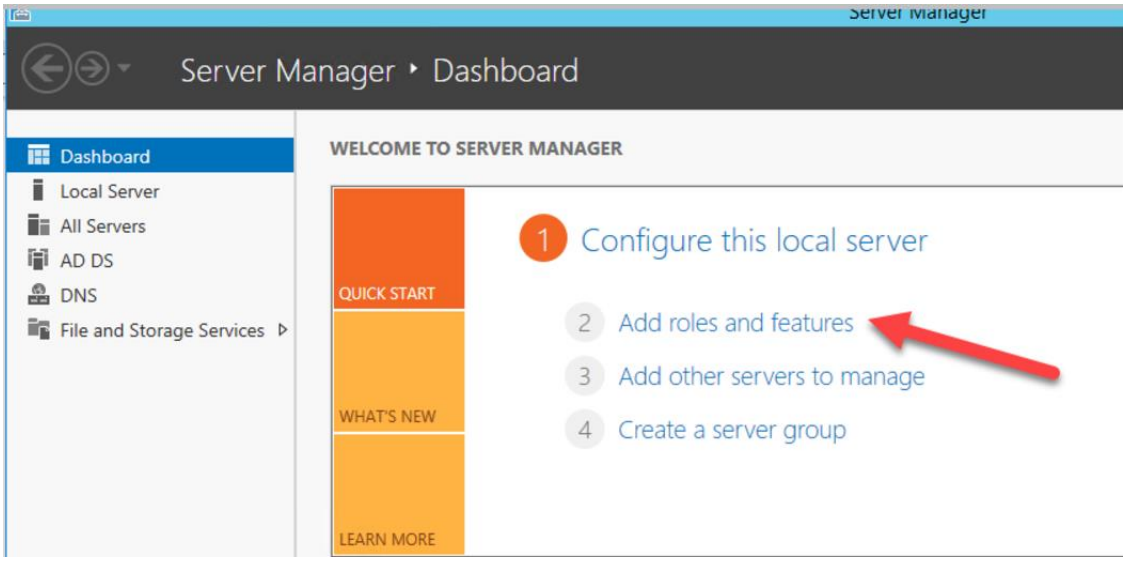


- Open command prompt and type ipconfig /all.

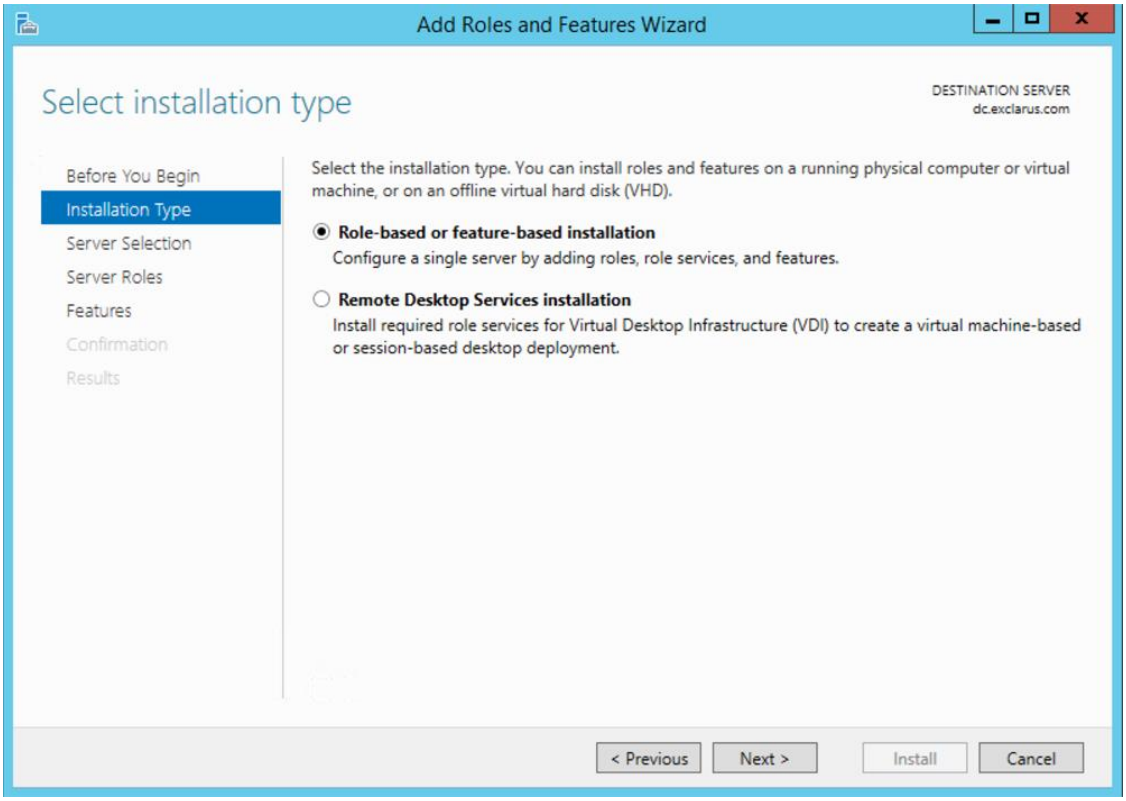


13. Installing DHCP in Domain Controller

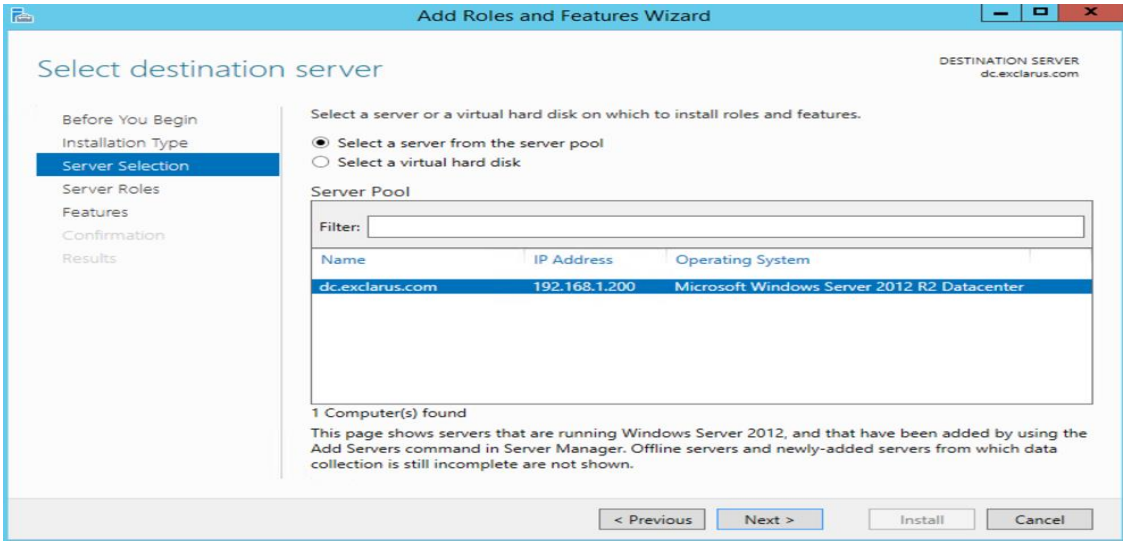
- DHCP service is used to hand out IPs to client systems. First, let's install DHCP and configure it. Let's launch "ServerManager" and click "Add roles and features"



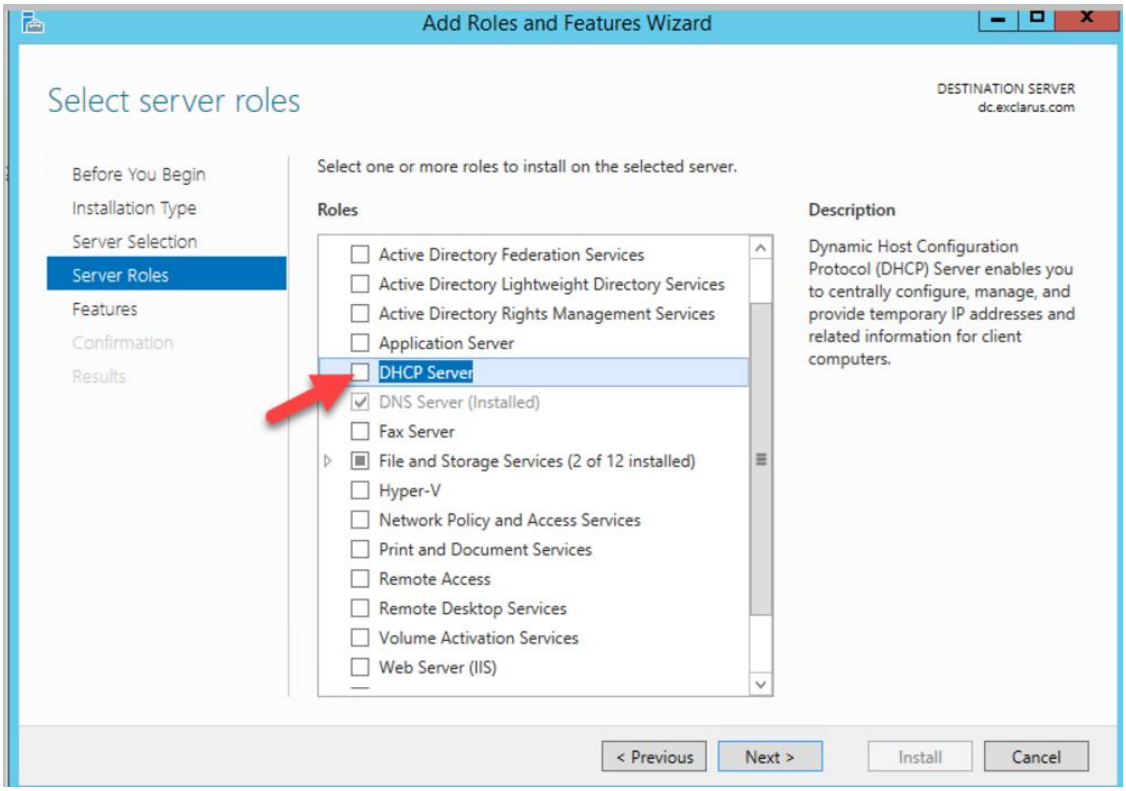
- Check "Role-based or feature-based installation" and click next



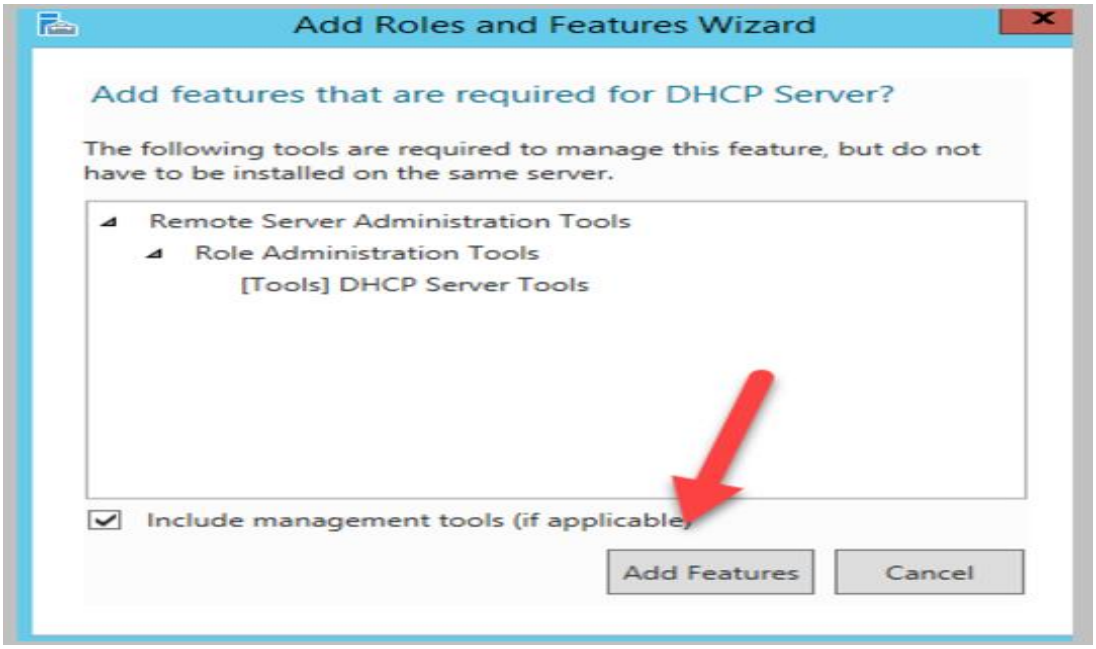
- Click “Next” to continue



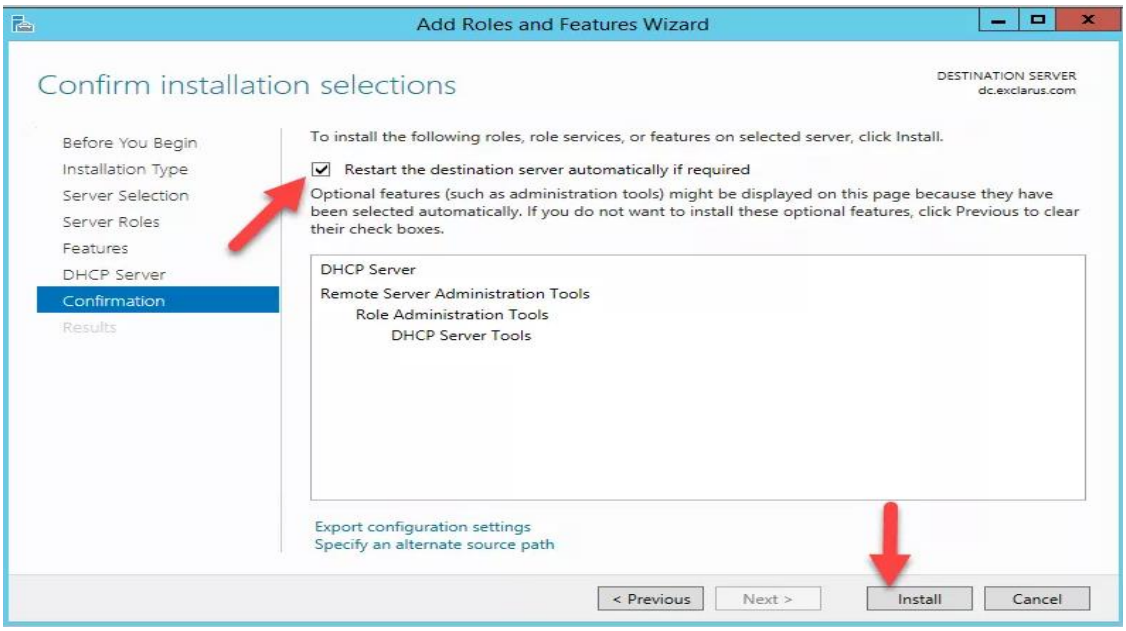
- Check “DHCP Server”



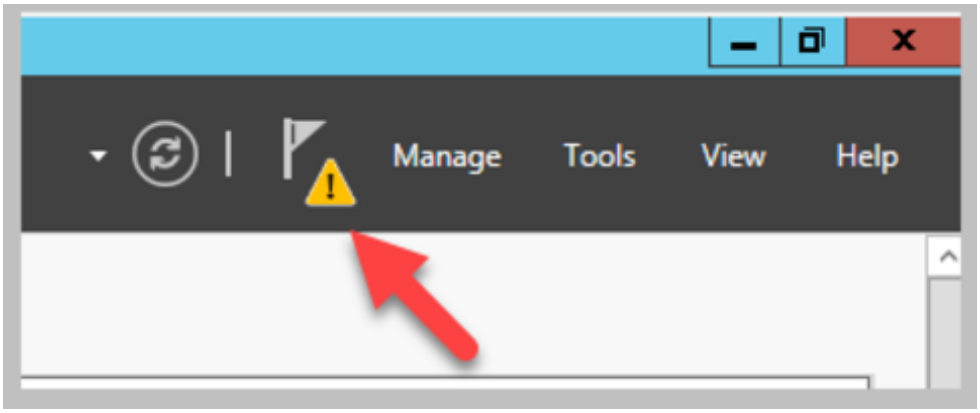
- Click “Add Features”



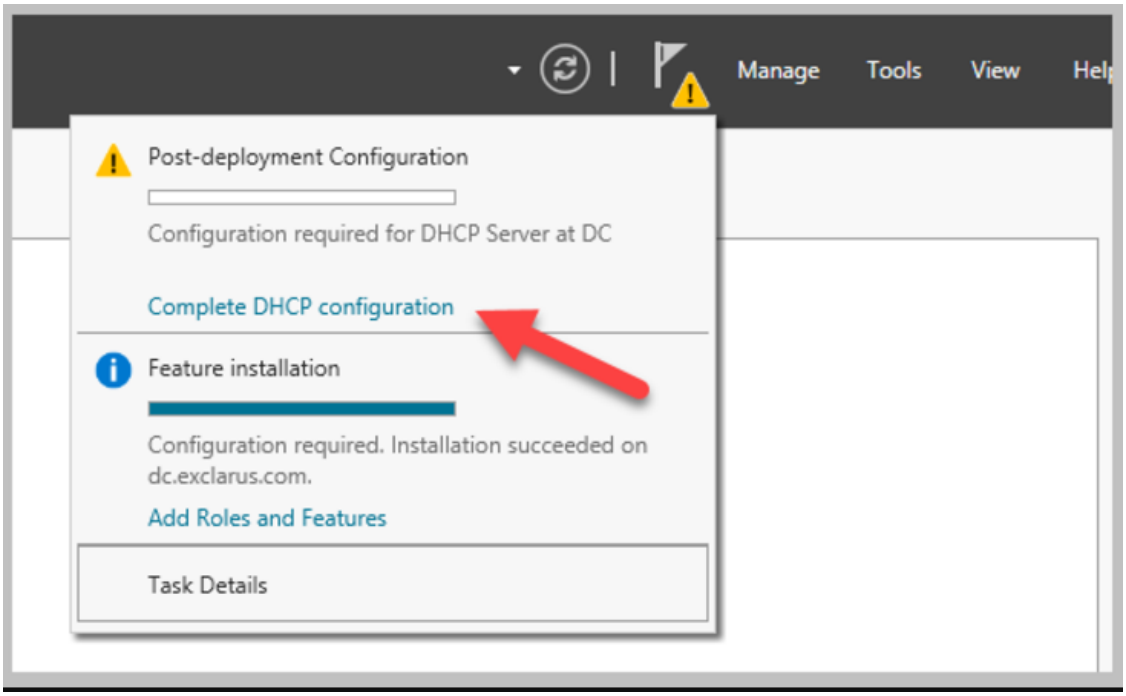
- Click Install to complete the process



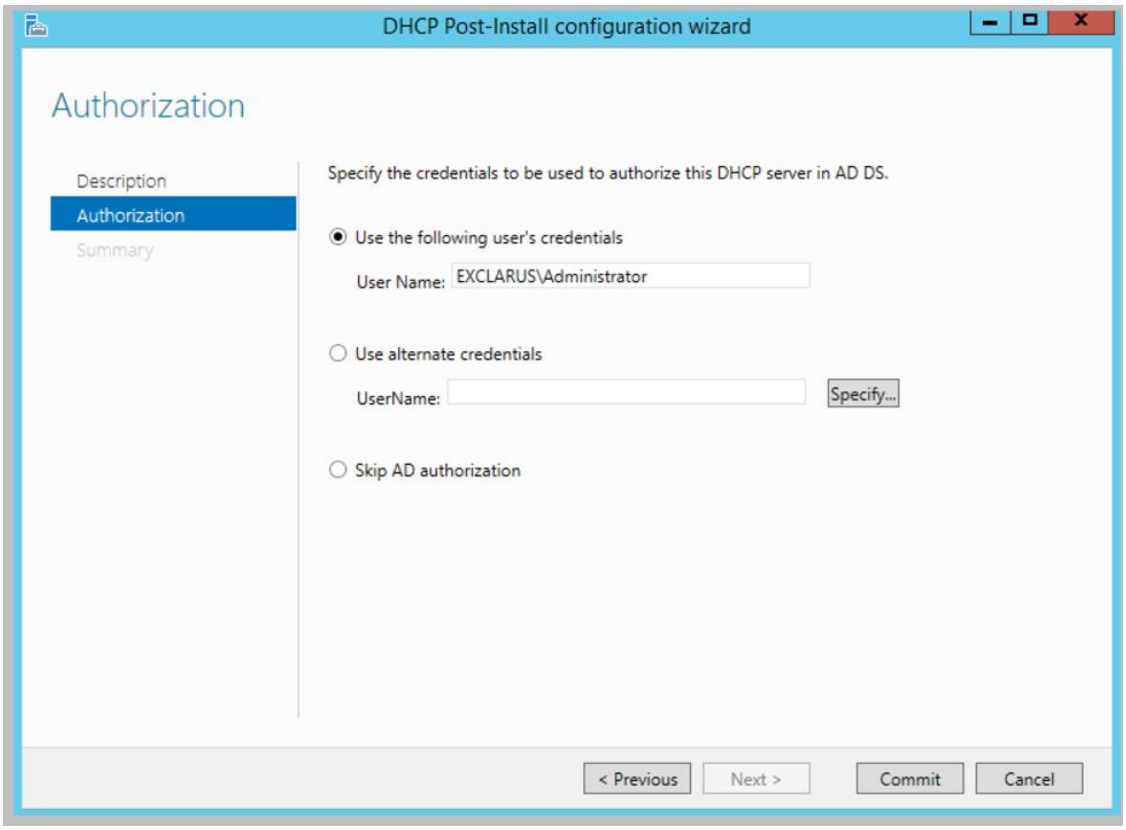
- Click the yellow Exclamation mark to complete the installation process



- Click “Complete DHCP configuration”

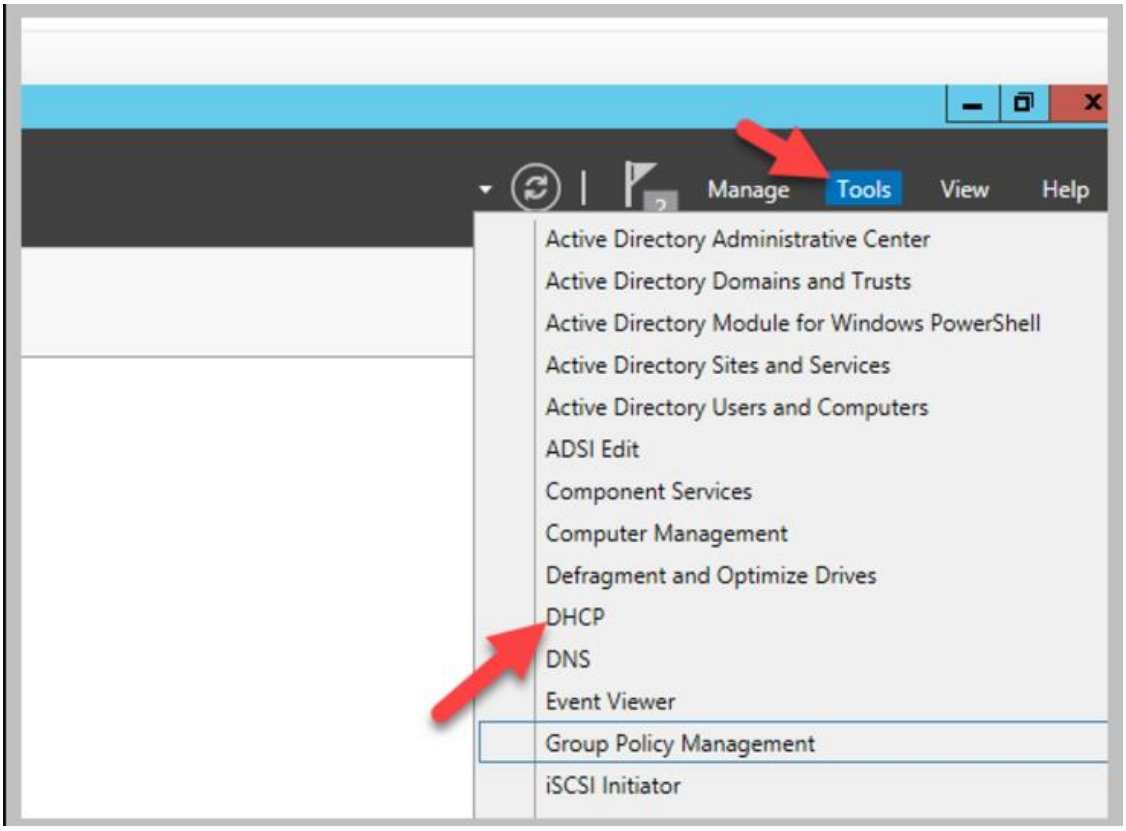


- Finally, click commit to complete the DHCP installation process

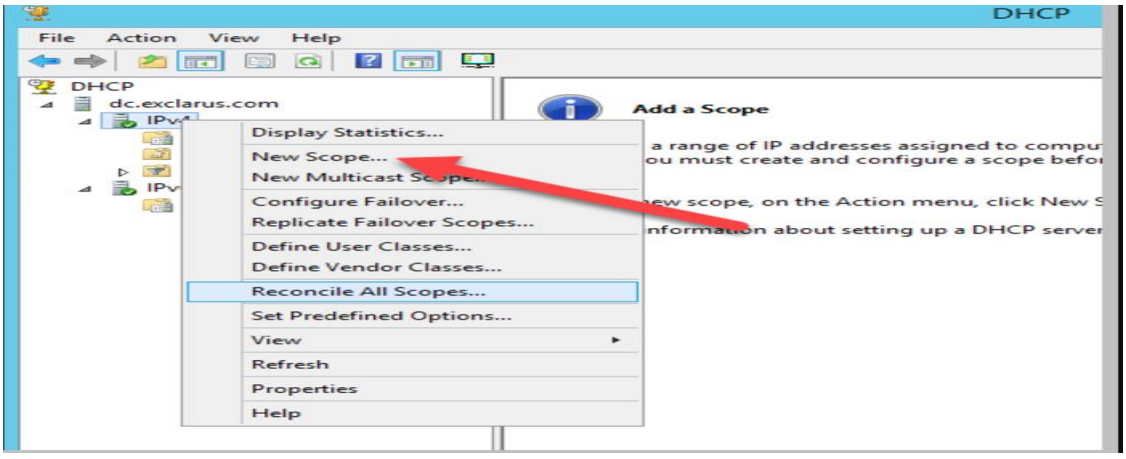


14. Configuring DHCP Server in Windows 2012 server

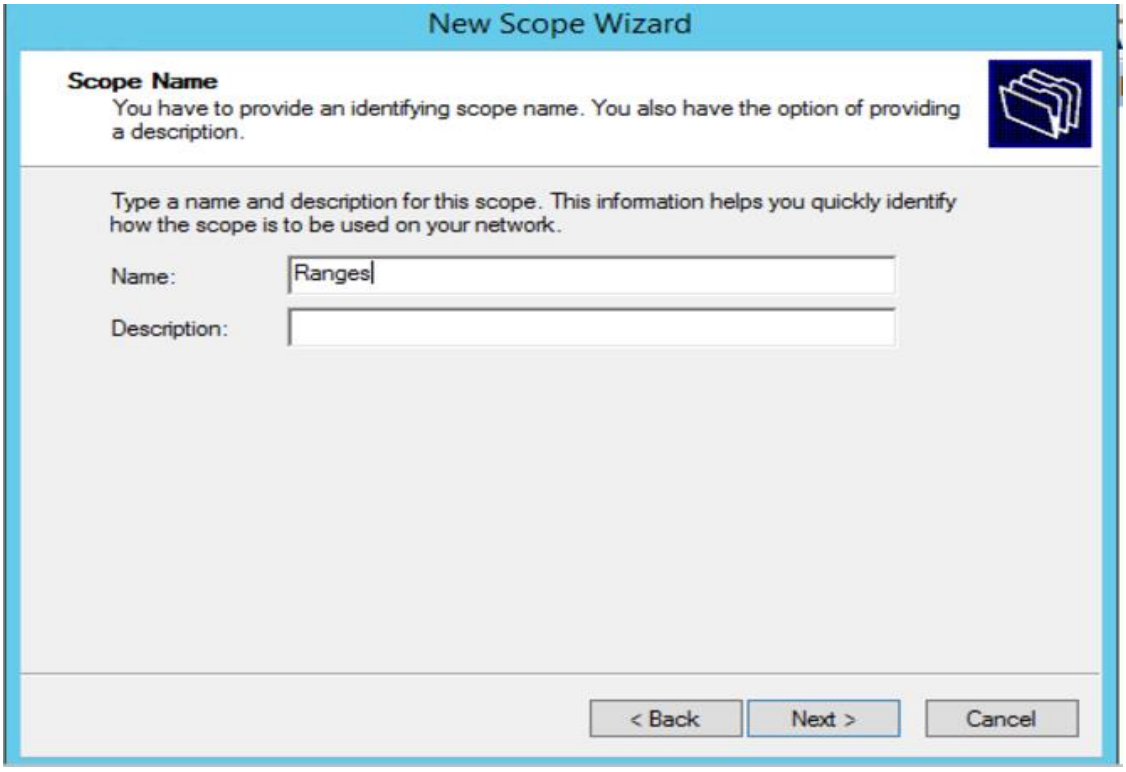
- Click "Tools" and select **DHCP** to configure the scope



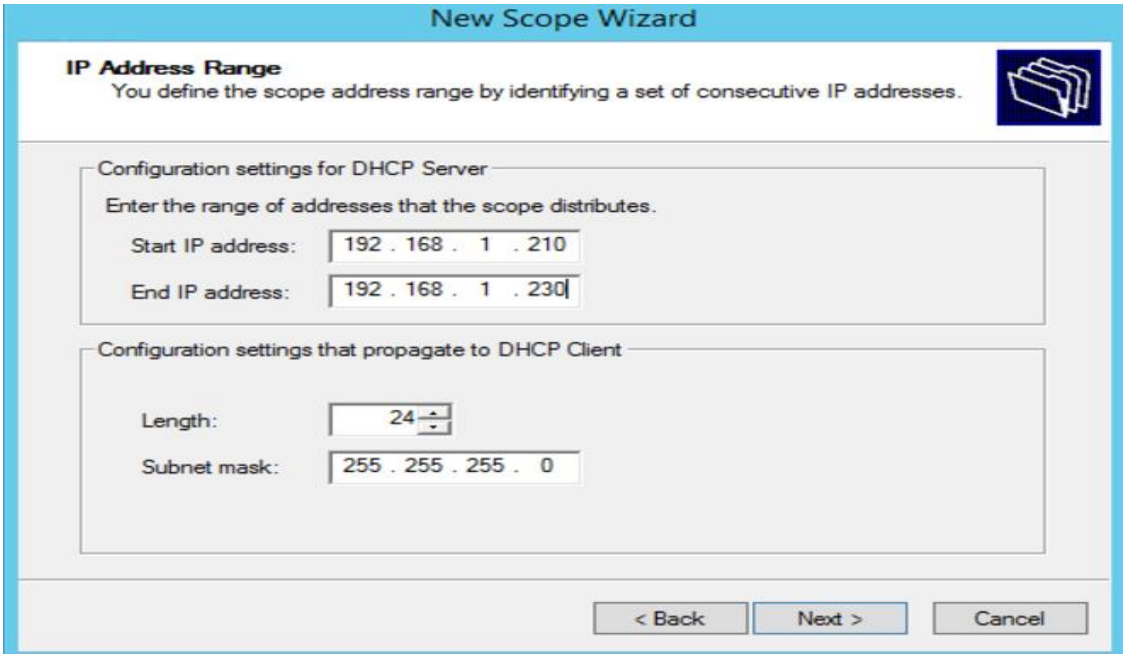
- Right click on IPv4 and click “New Scope”



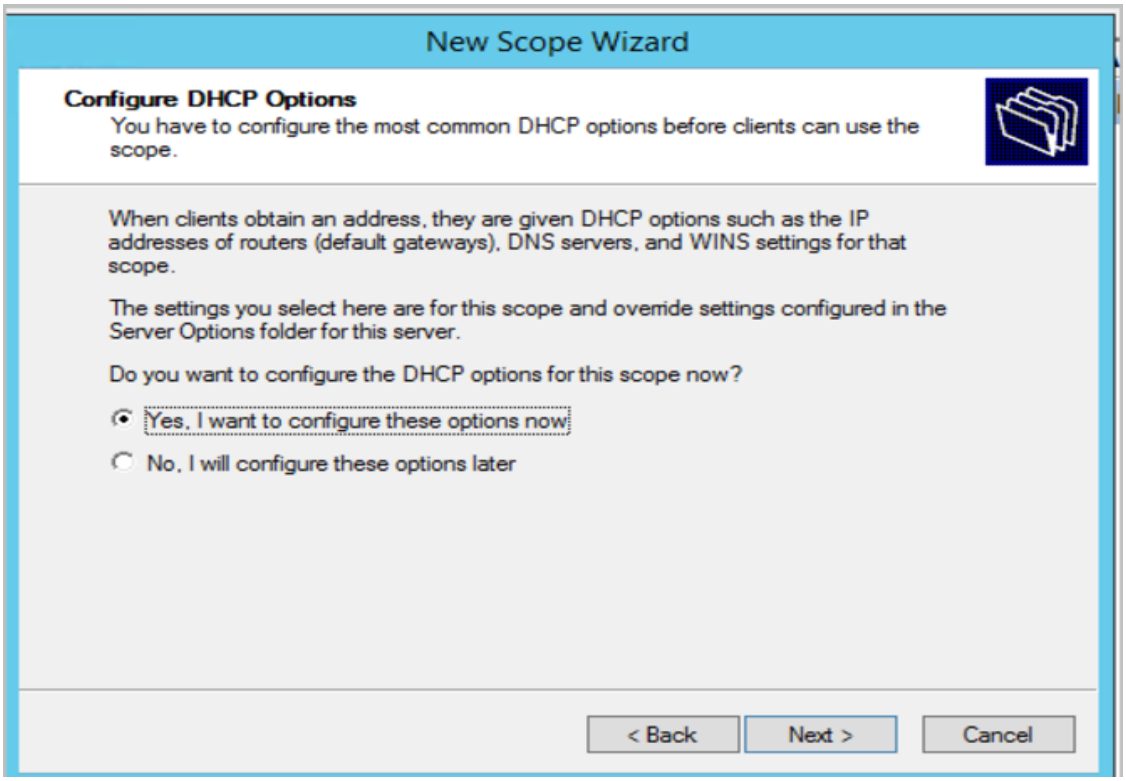
- Choose any name for the scope



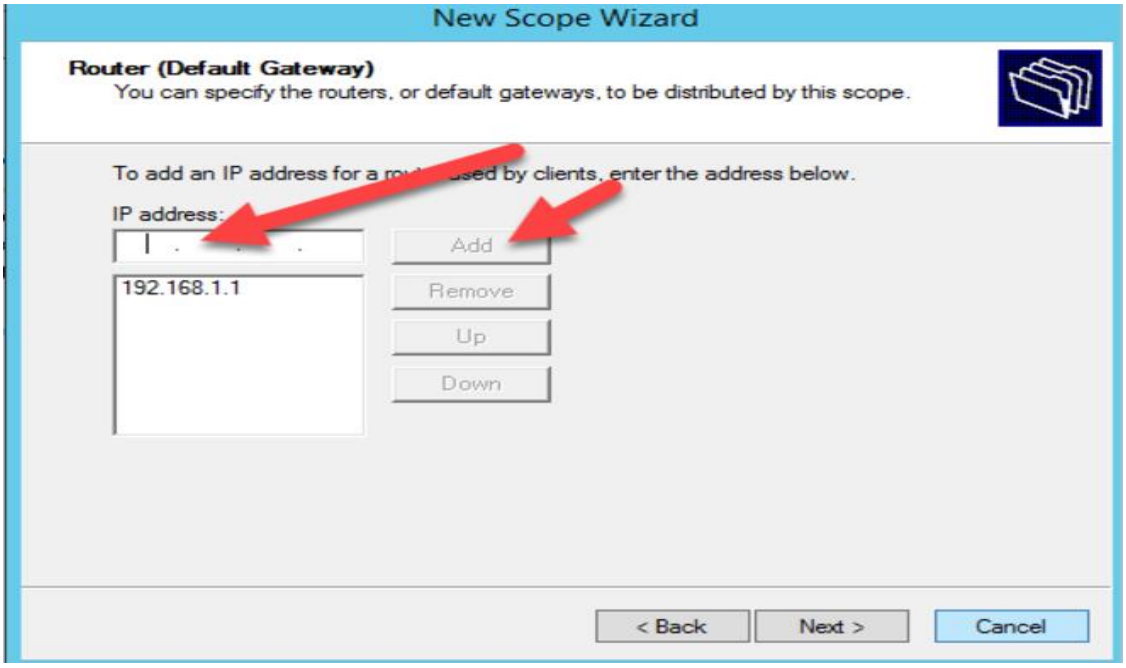
- Enter the Start IP address and End IP address as shown. Client systems will get an IP from this range. Click “next”



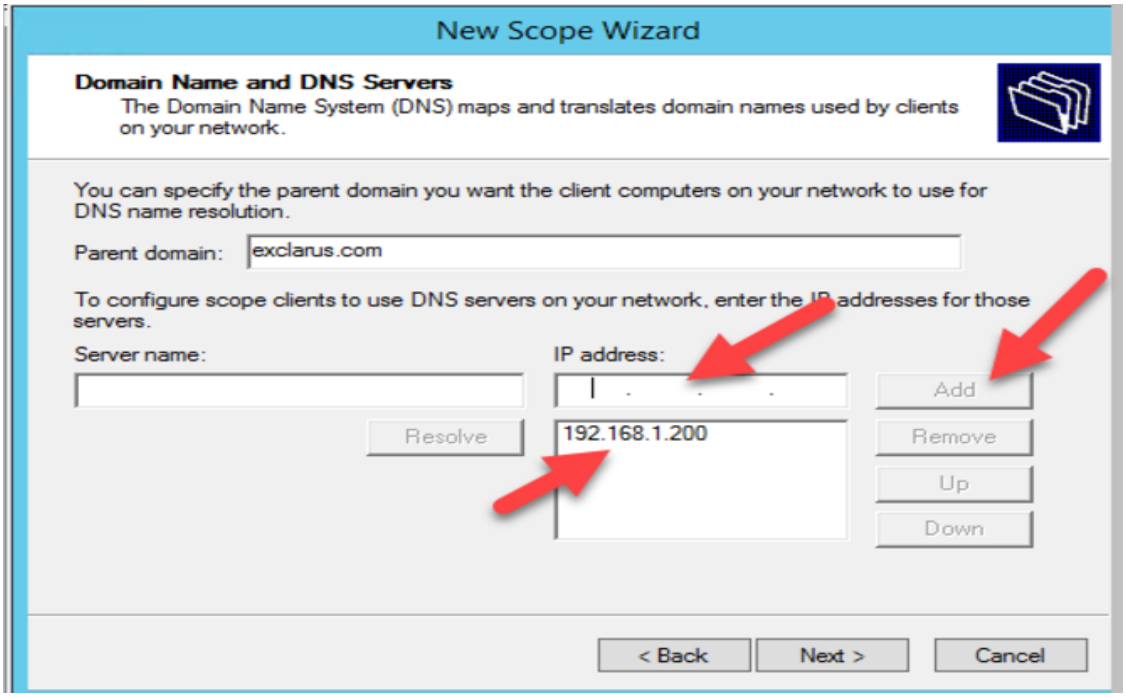
- Check “Yes” and click “Next”



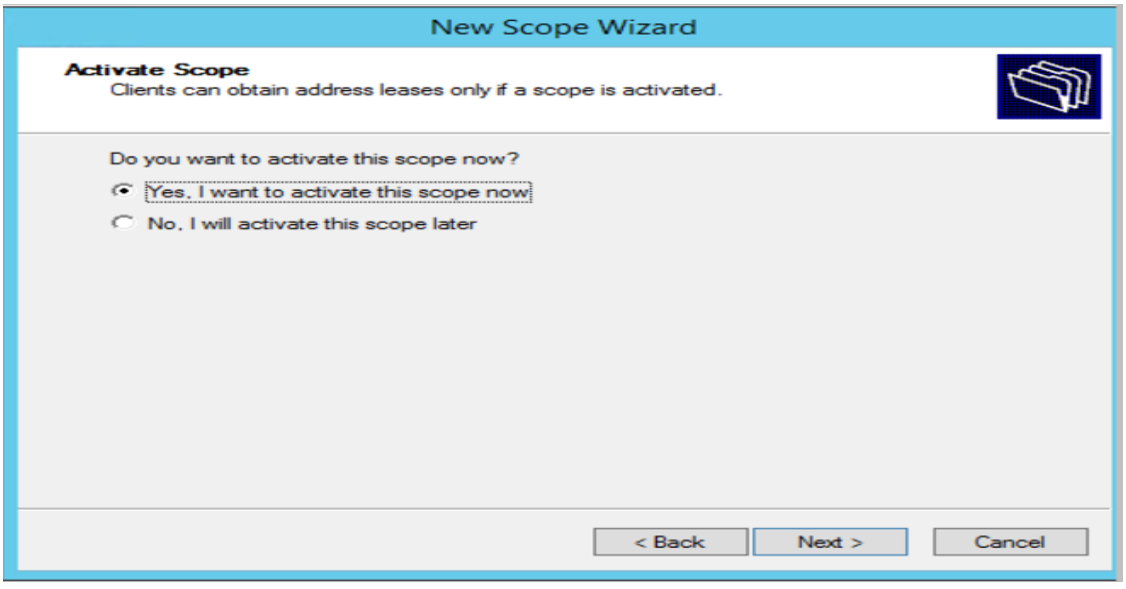
- Type IP address and click “Add”. Click “Next”



- For the DNS servers, type the IP address of 192.168.1.200 and click Add. All the client systems will use DC as the DNS server



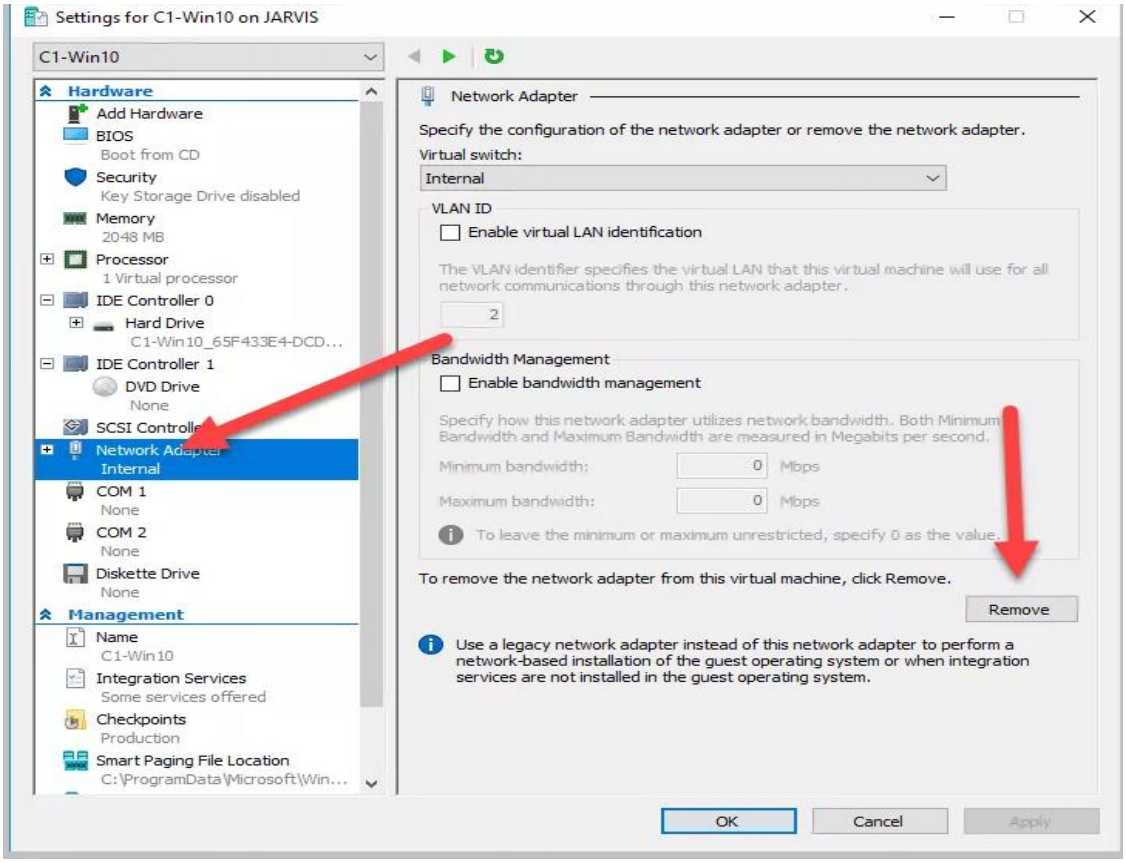
- Check “Yes” and click “Next”

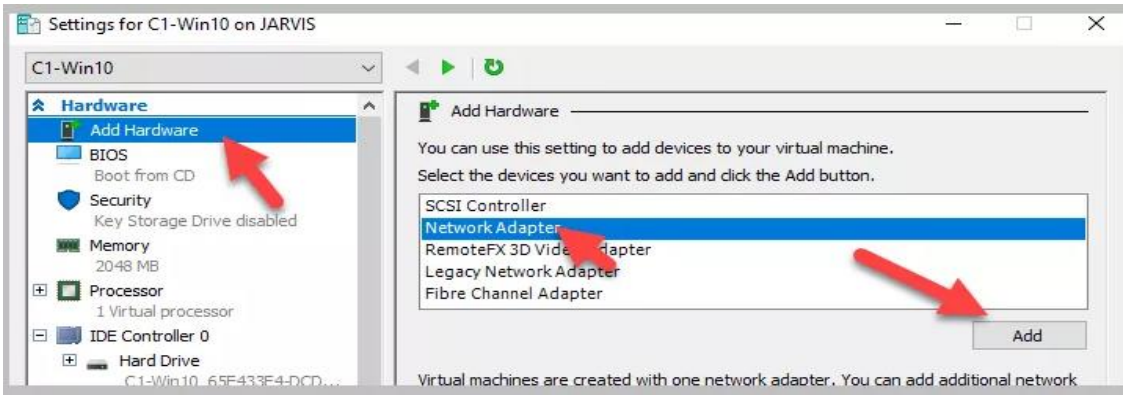


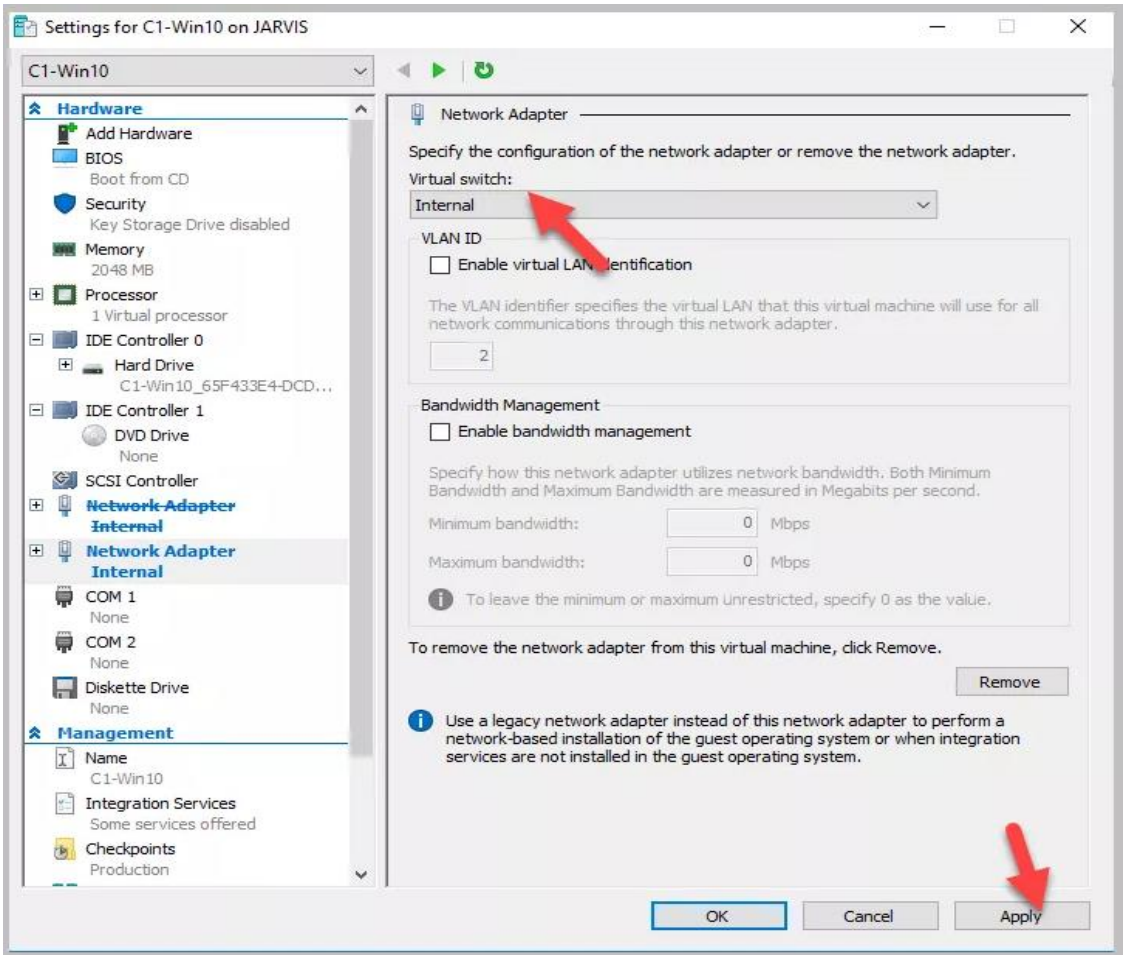
- The DHCP scope is now ready and the client systems will automatically be assigned a gateway as 192.168.1.1 and DNS server as 192.168.1.200

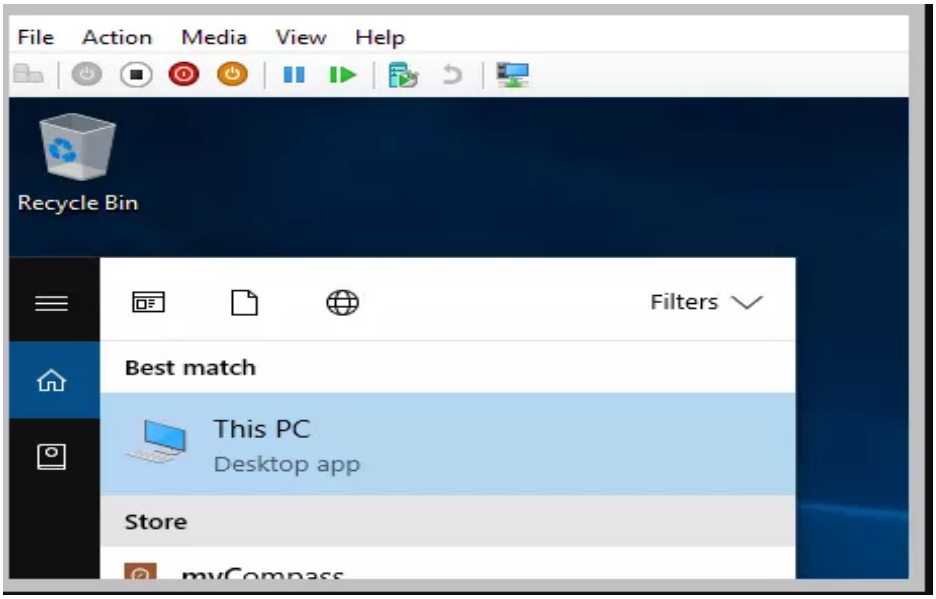
15. Joining Windows 10 to Domain

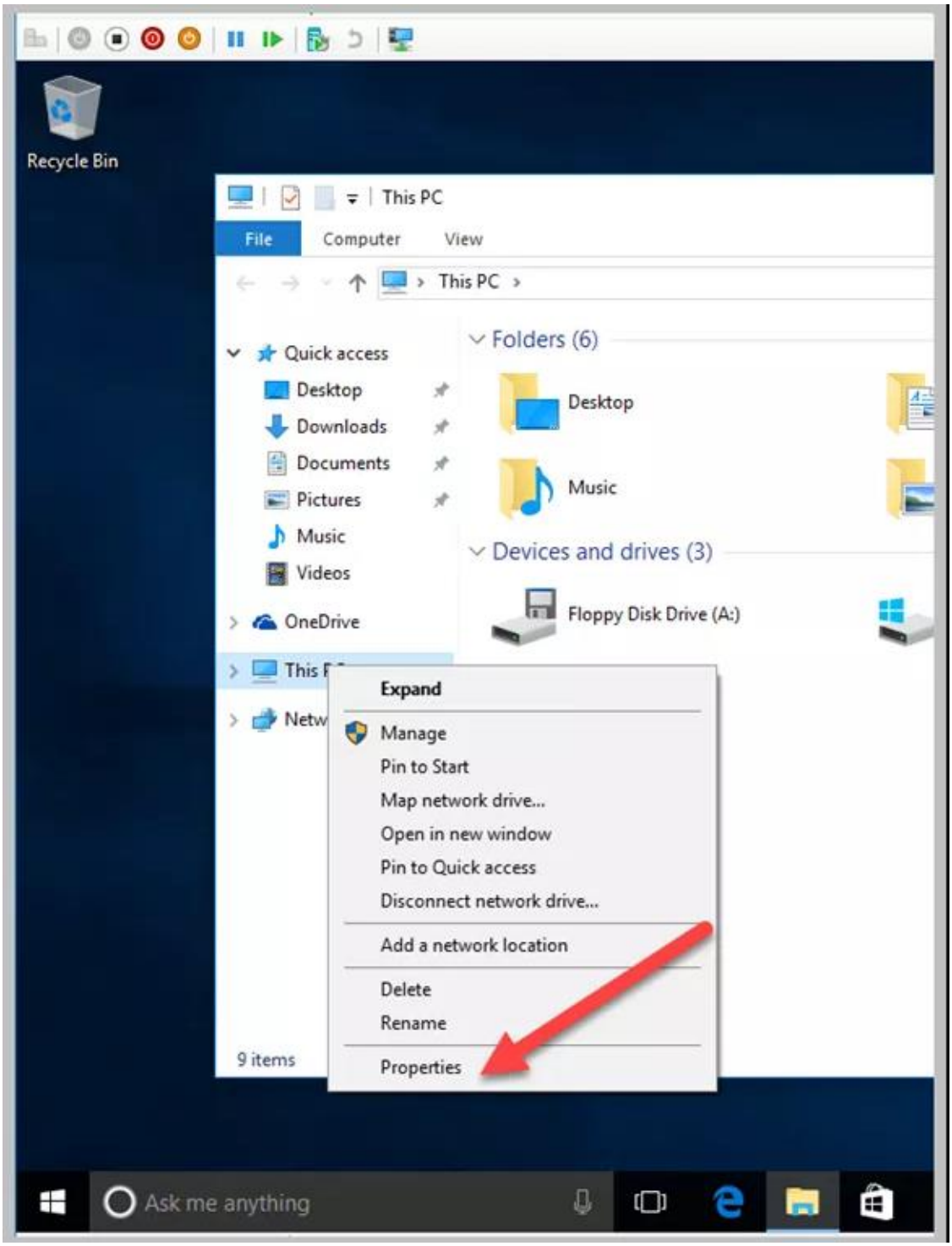
- Let's join the Windows 10 machine to the newly created domain exclarus.com. Before adding the computer to domain, it is better to remove the adapter and add a new adapter again as shown below. This will resolve any connectivity issues.



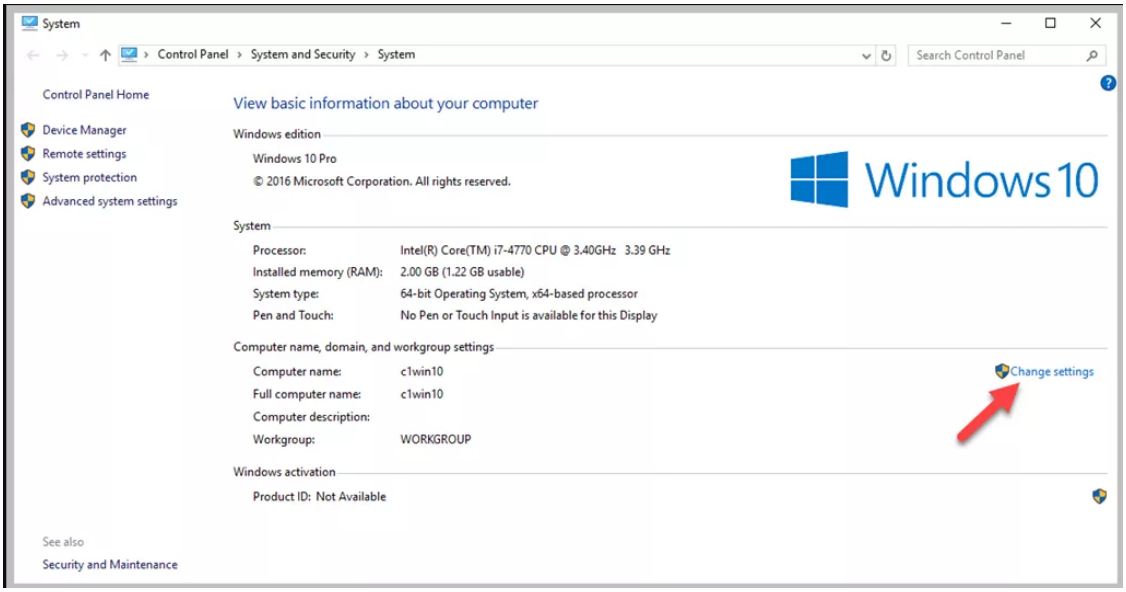



Settings for C1-Win10 on JARVIS
C1-Win10
Hardware
Add Hardware
BIOS
Boot from CD
Security
Key Storage Drive disabled
Memory
2048 MB
Processor
1 Virtual processor
IDE Controller 0
Hard Drive
C1-Win10_65F433E4-DCD...
IDE Controller 1
DVD Drive
None
SCSI Controller
Network Adapter
Internal
Network Adapter
Internal
COM 1
None
COM 2
None
Diskette Drive
None
Management
Name
C1-Win10
Integration Services
Some services offered
Checkpoints
Production
Network Adapter
Specify the configuration of the network adapter or remove the network adapter.
Virtual switch:
Internal
VLAN ID
Enable virtual LAN identification
The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.
2
Bandwidth Management
Enable bandwidth management
Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.
Minimum bandwidth:
0
Mbps
Maximum bandwidth:
0
Mbps
To leave the minimum or maximum unrestricted, specify 0 as the value.
To remove the network adapter from this virtual machine, click Remove.
Remove
Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.
OK
Cancel
Apply

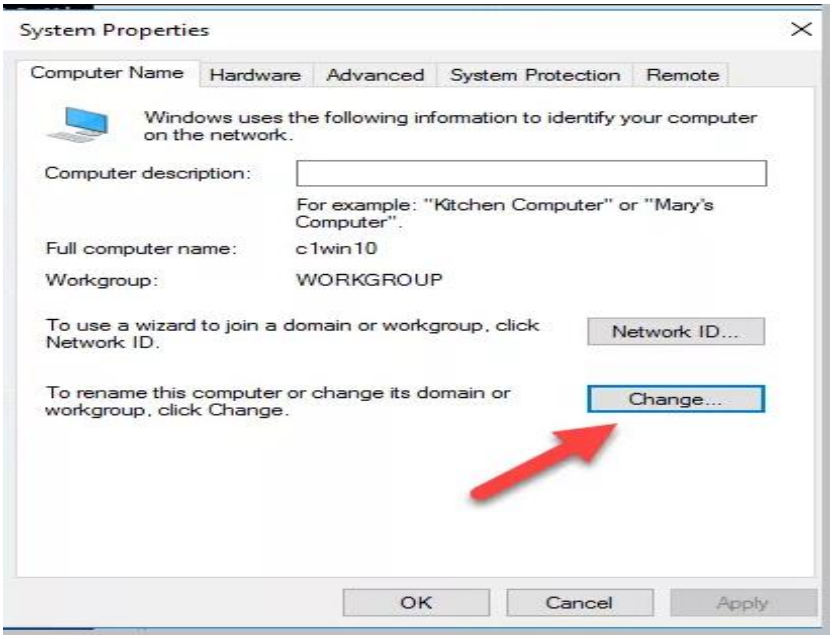

File
Action
Media
View
Help
Recycle Bin
Filters
Best match
This PC
Desktop app
Store



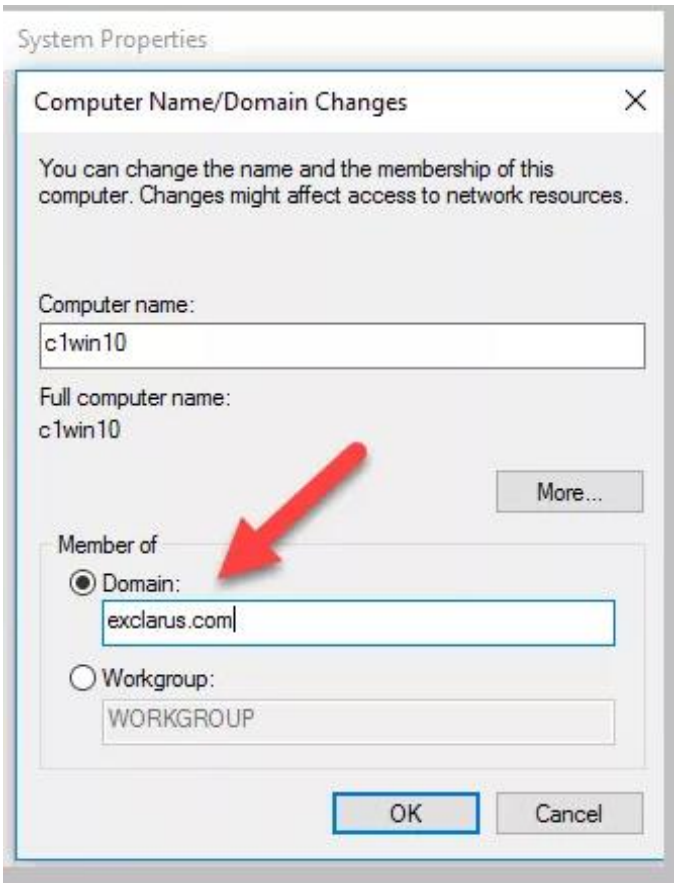
- Click “Change Settings”



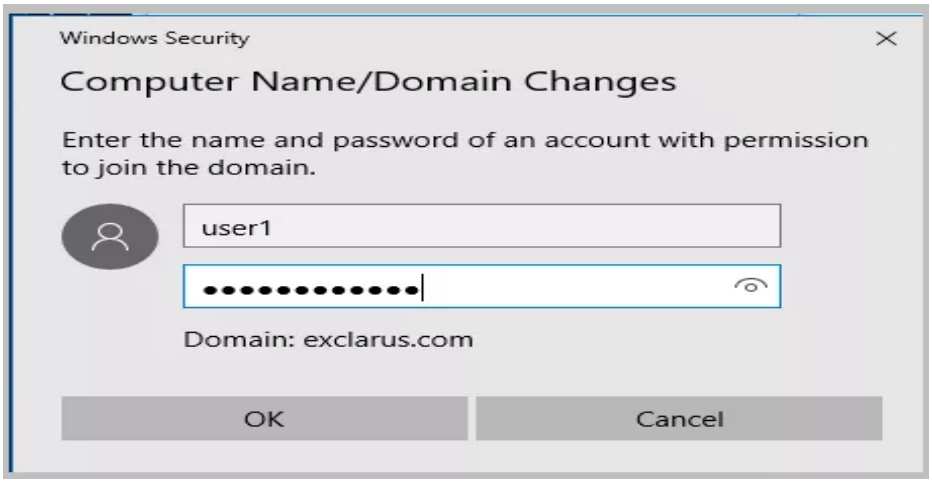
- Click “Change”



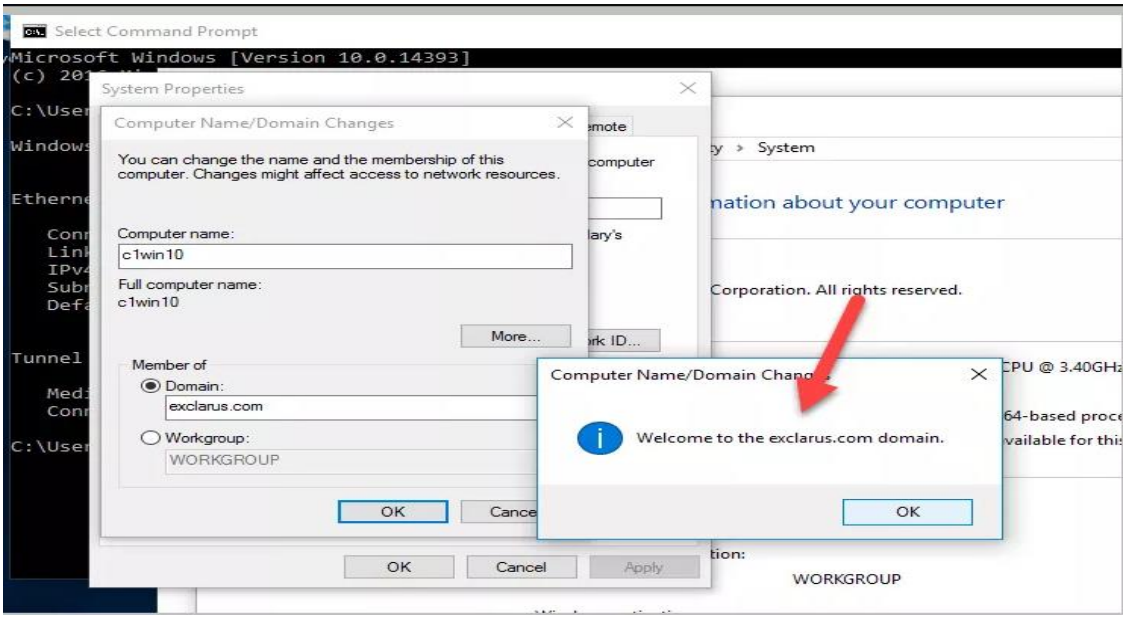
- Change the Domain to exclarus.com as shown below



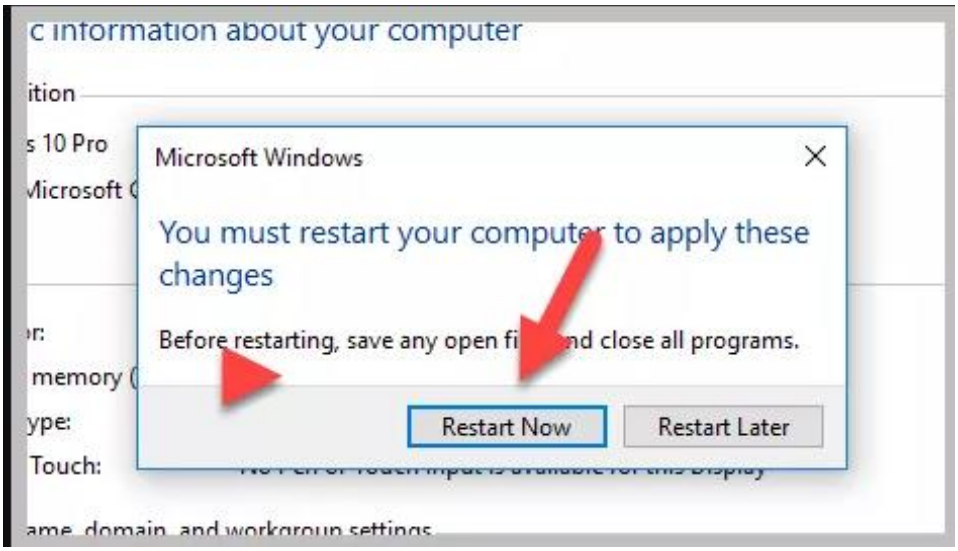
- When you click okay in the previous message box, it will prompt for a user name. Type the **user1** credentials we created in the previous steps



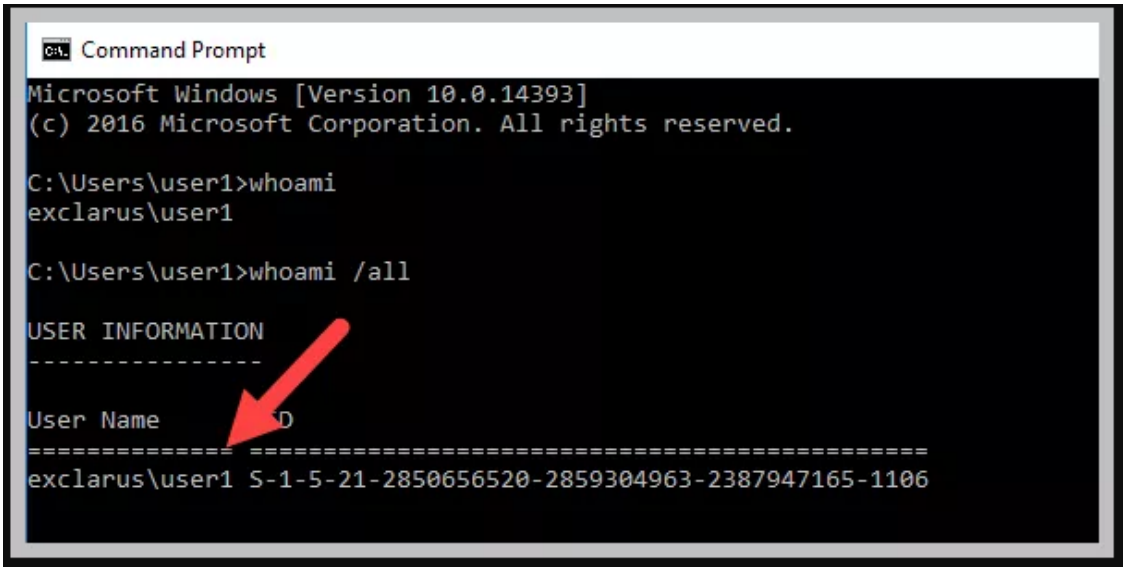
- Finally, we added the first machine to the active directory domain



- Restart the computer and login with new credentials. When entering the user name use exclarus\user1



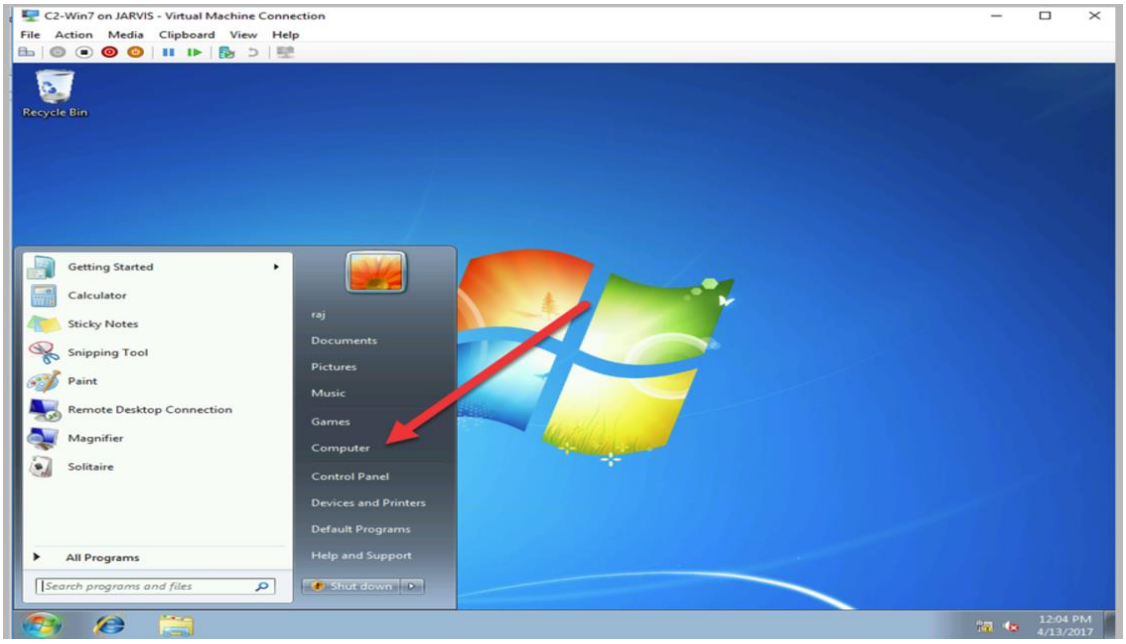
- After restart, open a command prompt and type whoam /all

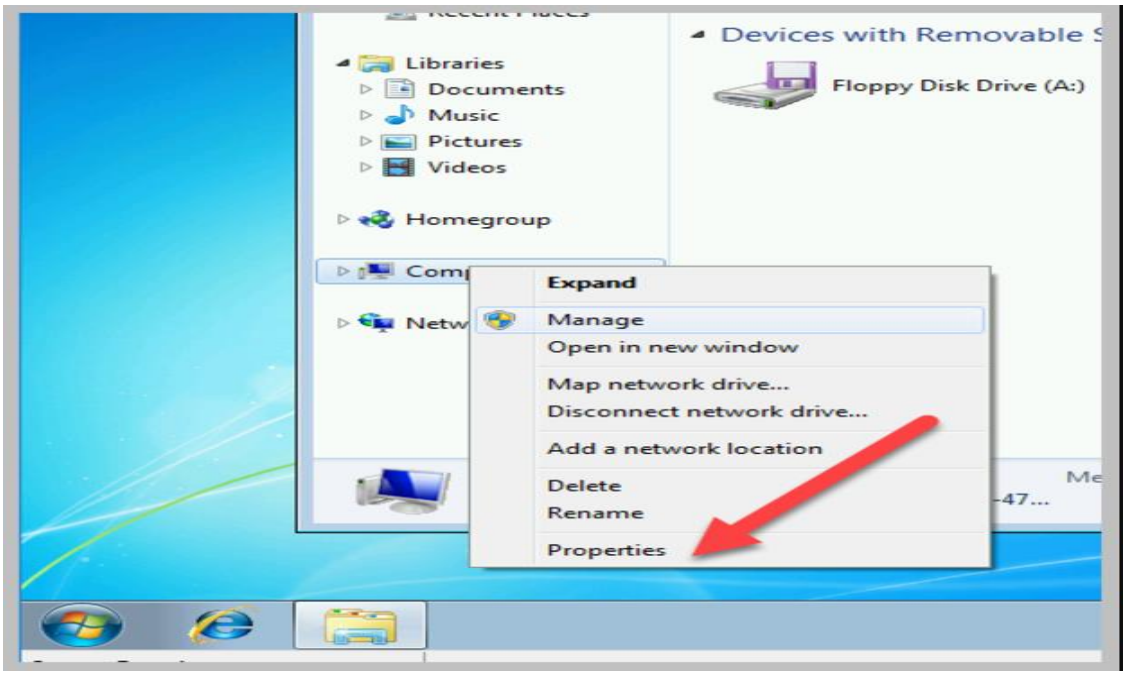


- Type Ipconfig /all and view all the details as shown below. It is getting this settings from Active Directory

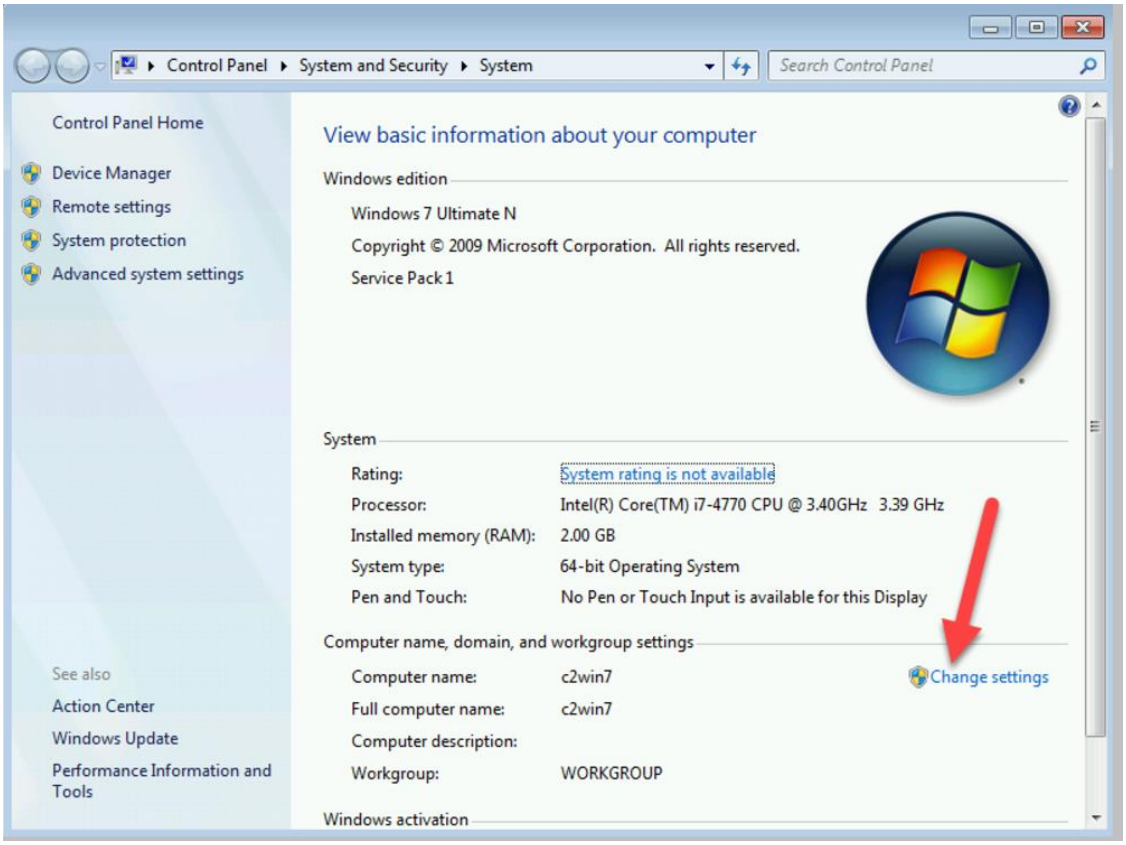
16. Joining Windows 7 to Domain

- Add and remove adapters as shown in Windows 10 tutorial. Click Computer/properties as shown below

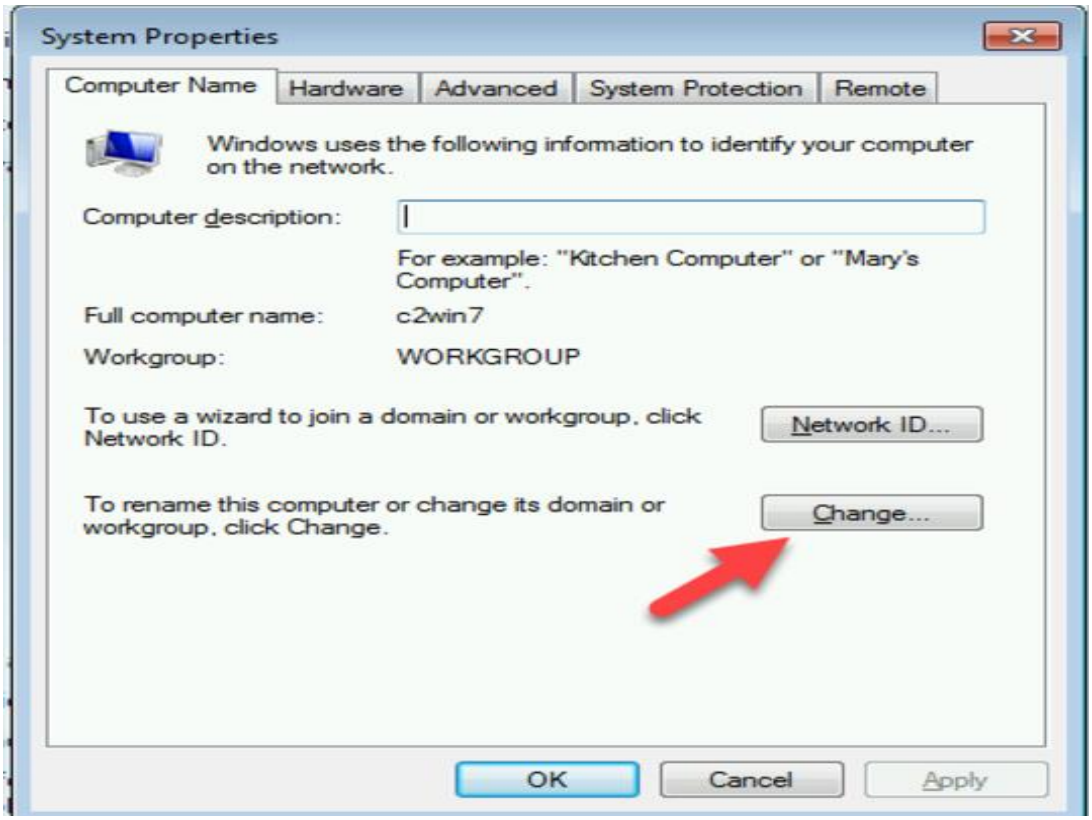




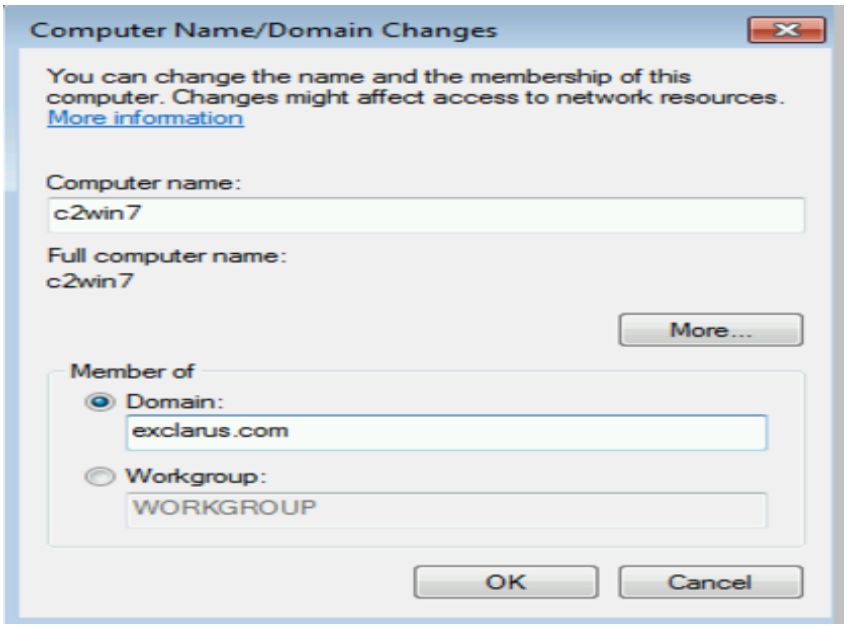
- Click “Change settings”



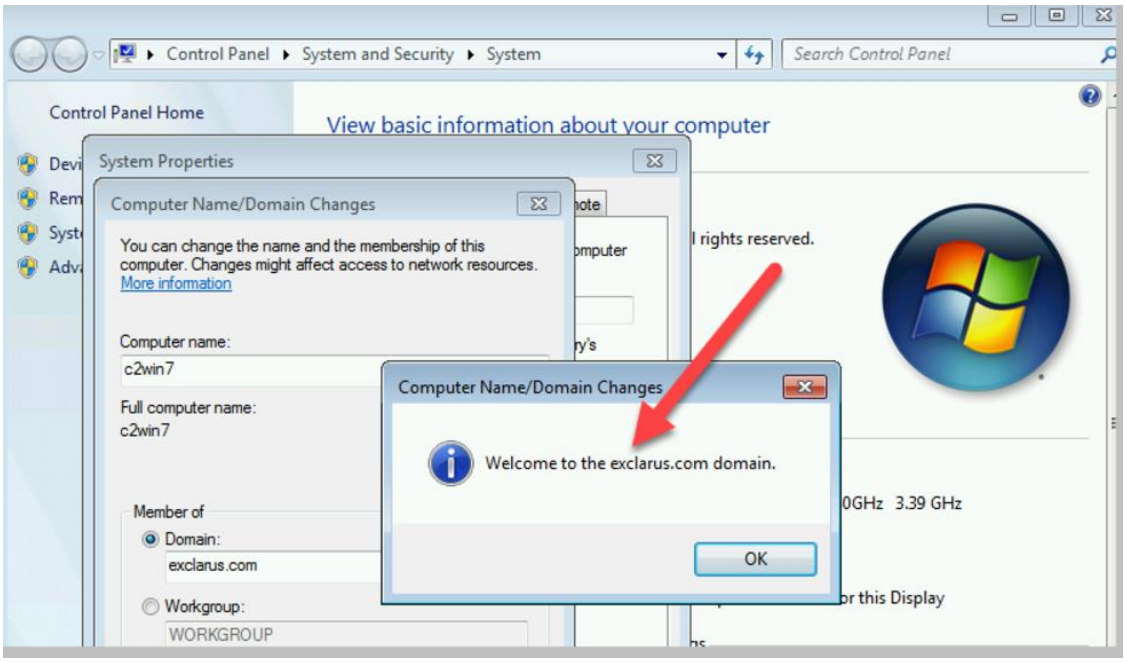
- Click “Change”



- Use Domain as exclarus.com and click ok. It should prompt for credentials

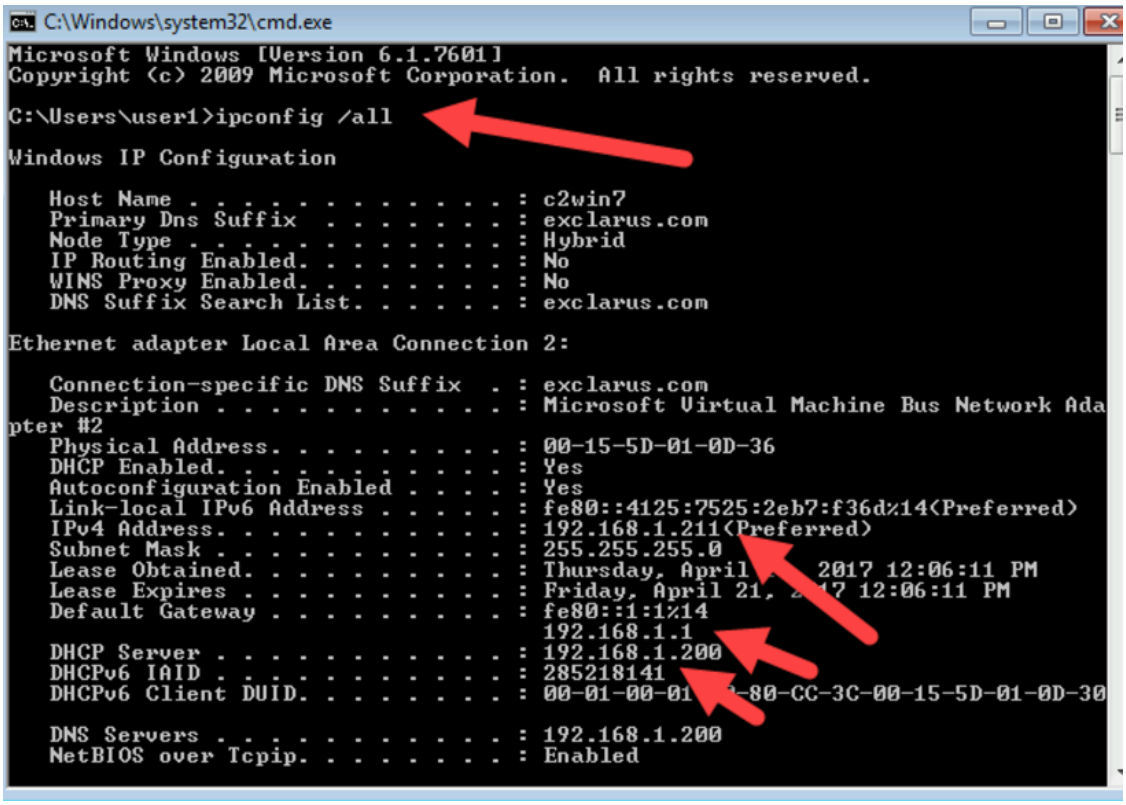


- Windows 7 is now a member of domain



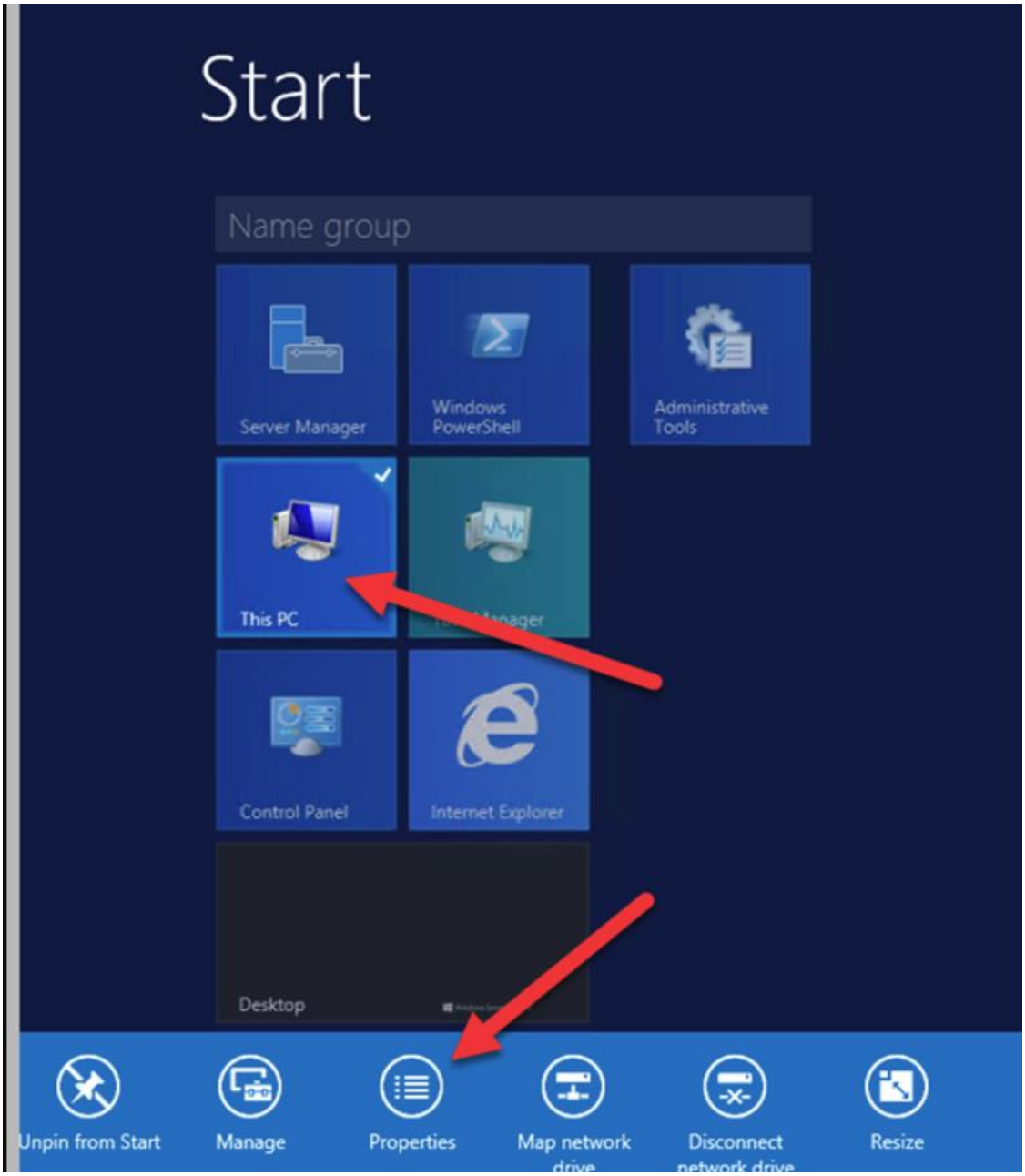
- Login with the same user user1 or any other active users

- Open a command prompt and type **ipconfig /all** to verify the settings

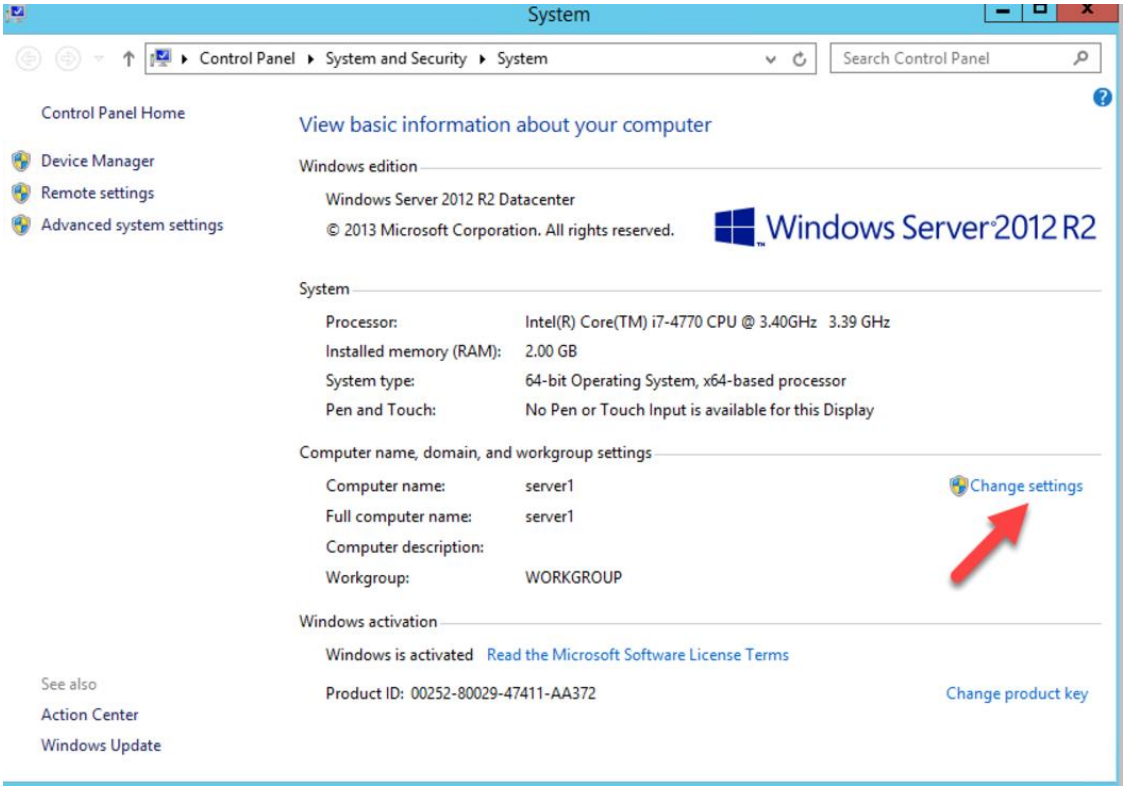


17. Adding FileServer to Domain

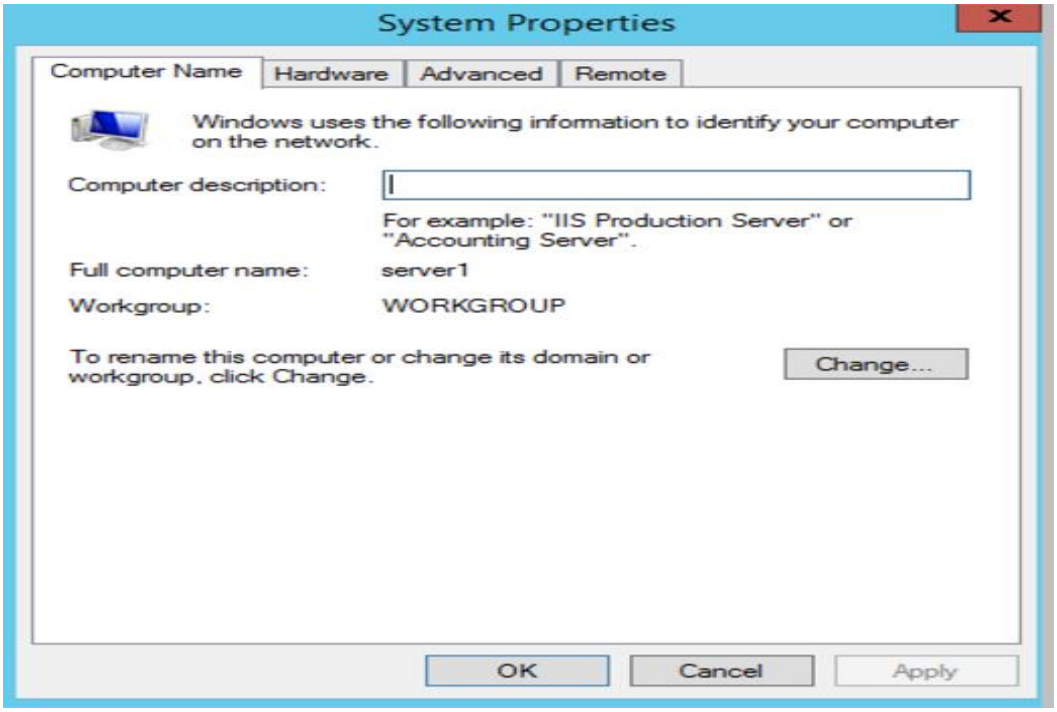
- Let's add the server1 to exclarus.com domain. Search for "This PC" and click properties



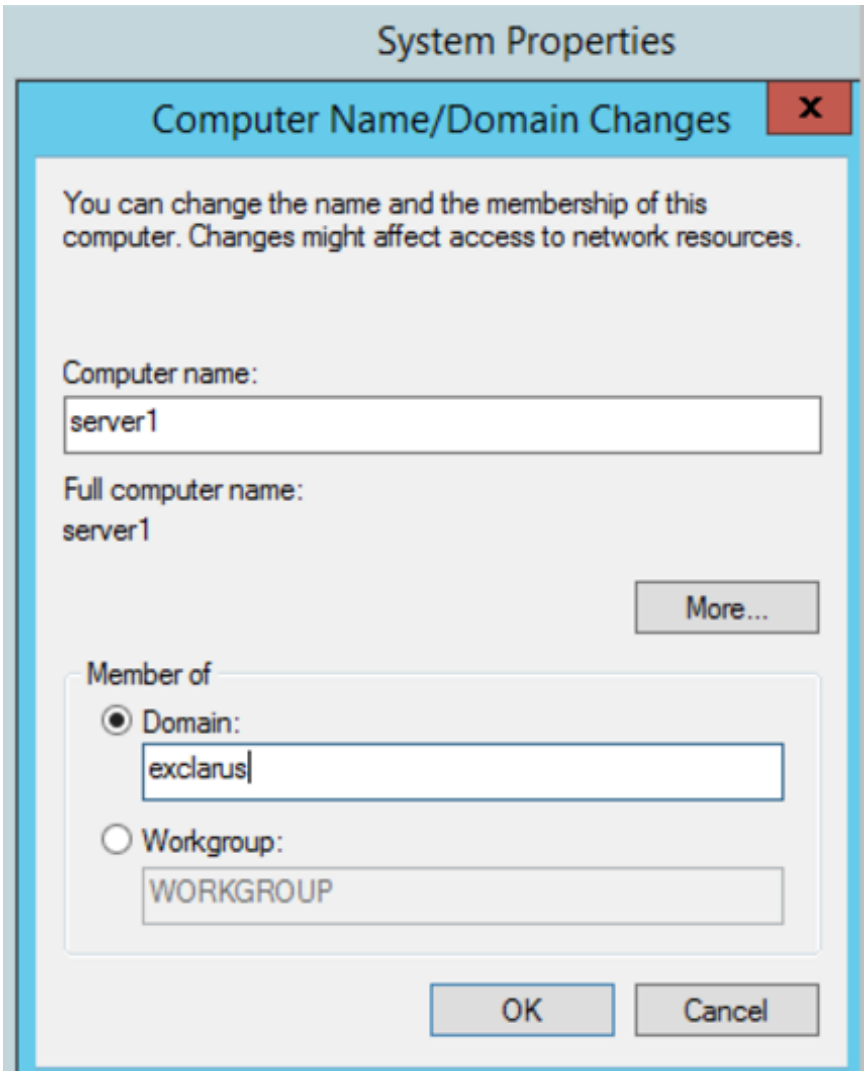
- Click "Change settings



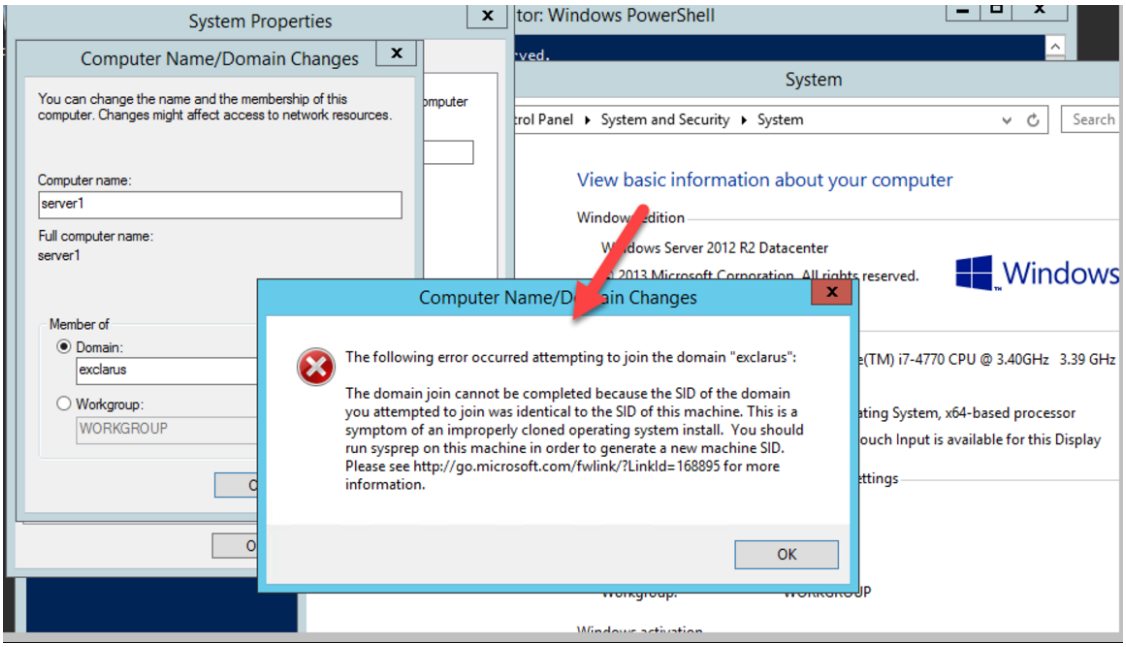
- Click “Change”



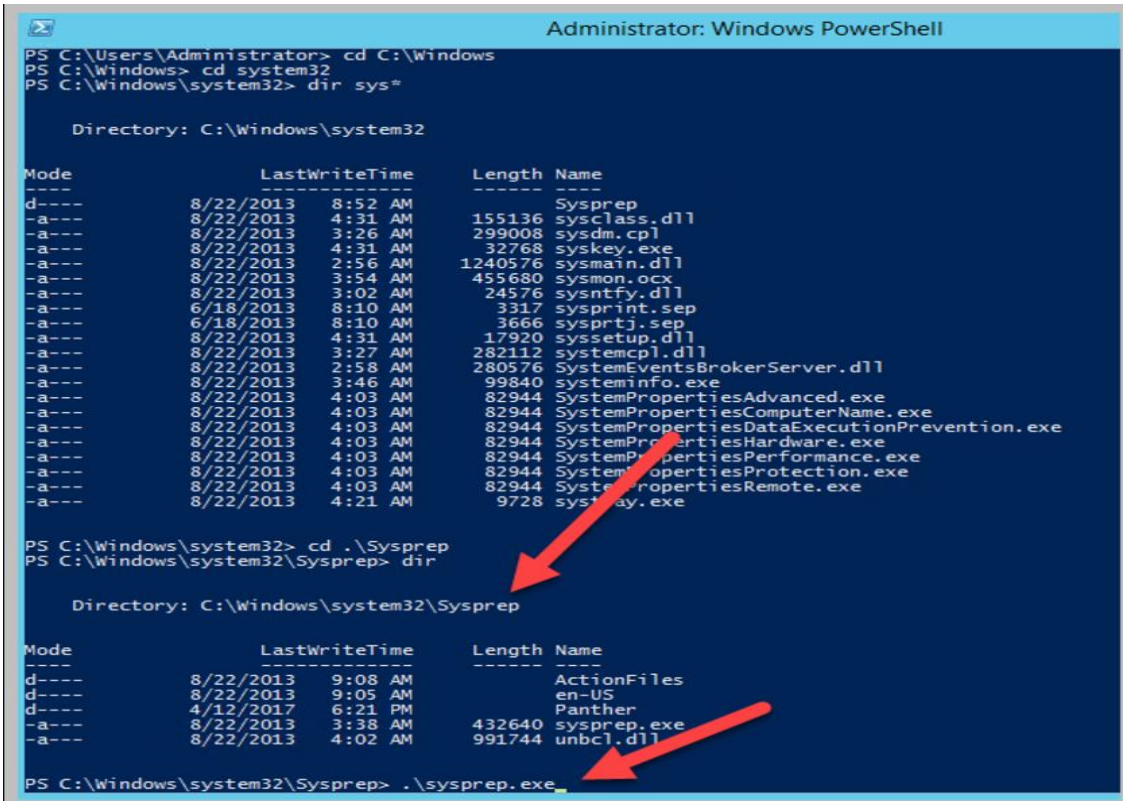
- Change domain to exclarus.com and click OK



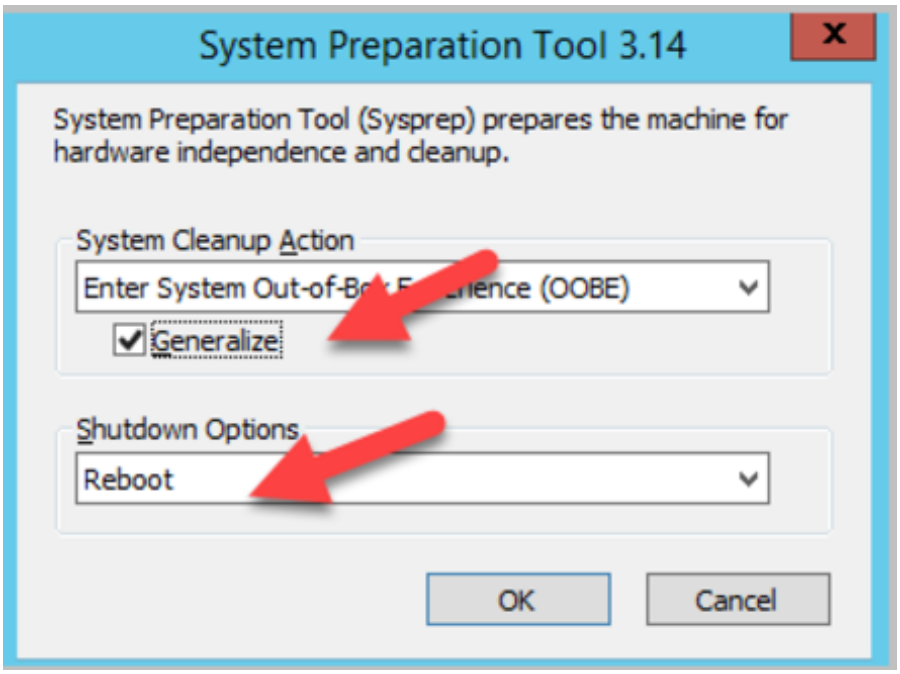
- If you followed in order, you will get the same error. This error is due to the fact we imported the machine from existing DC image. Whenever you clone or import a machine from other virtual image, you should perform **sysprep** as shown below



- Open a command prompt and go to c:\windows\system32\sysprep directory. Launch the command as shown below



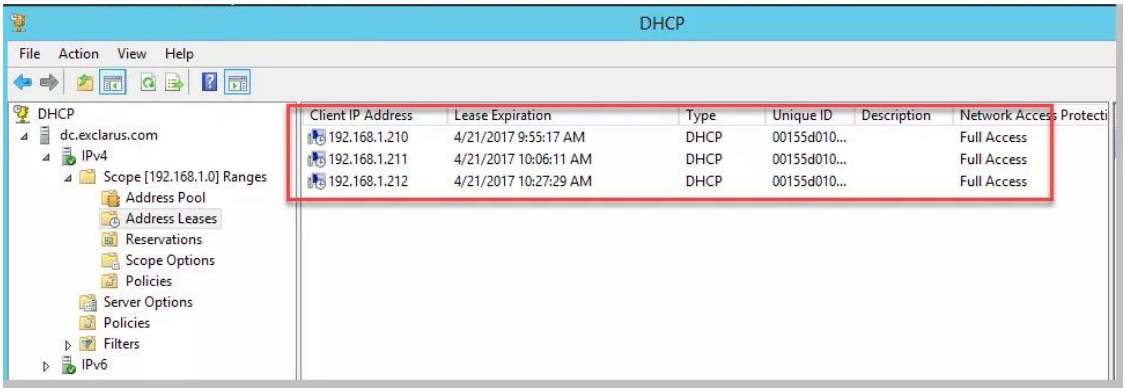
- Make sure to check the “Generalize” and reboot the system



- Now repeat the same steps as before to join the **server1** to domain

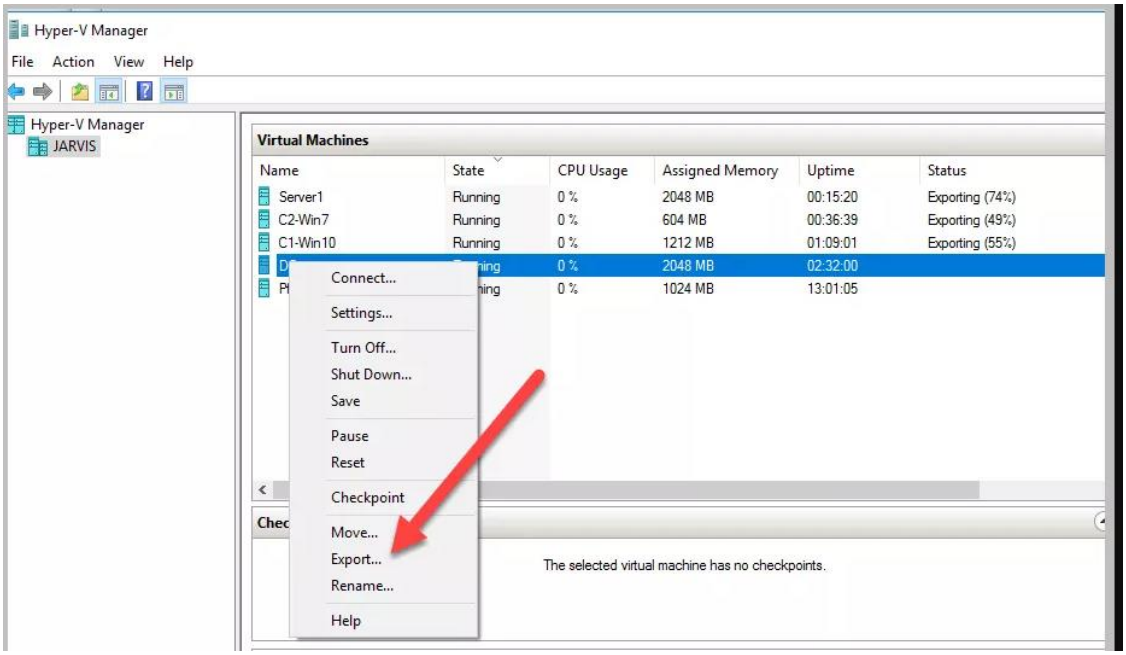
18. Viewing DHCP leases in Domain Controller

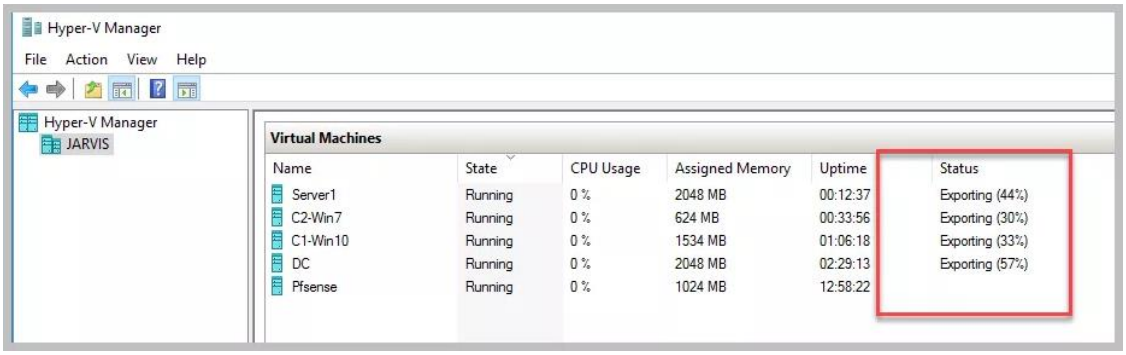
- Go to our domain controller DC and view DHCP leases, and you should see three machines in the list. Windows 10, Windows 7, and 2012 server



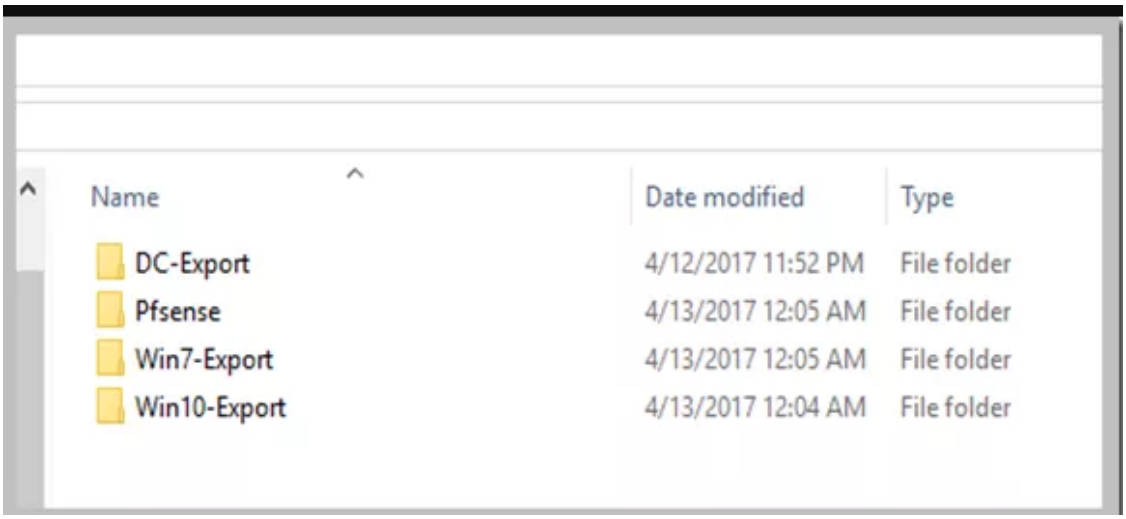
19. Exporting, Saving, and creating Checkpoints for all VMs

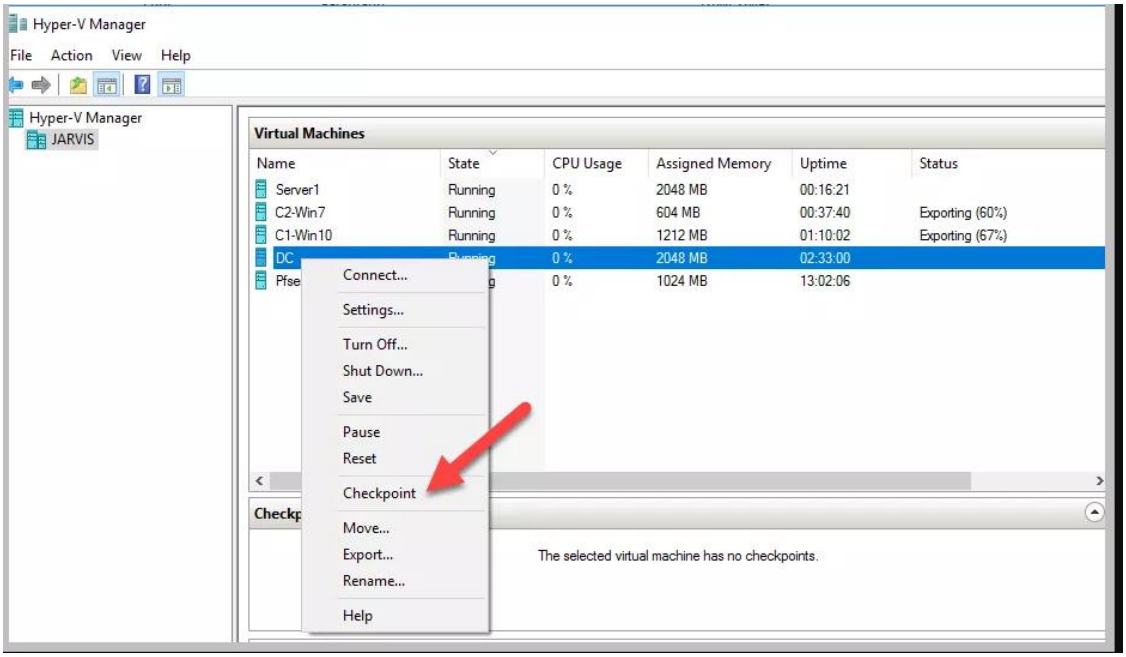
- Since we spent a lot of time creating these VMs, it is better to export all the VMs and create checkpoints, so we can restore without having to install and configure again. Right click on each VM and click export





- Click on each VM and create a check point as well





- We can create multiple checkpoints and restore to any state. Use this feature to try new things and restore back to clean image.

20. Protect you host computer

- Login to host computer

```
C:\Users\raj>hostname
Jarvis
```

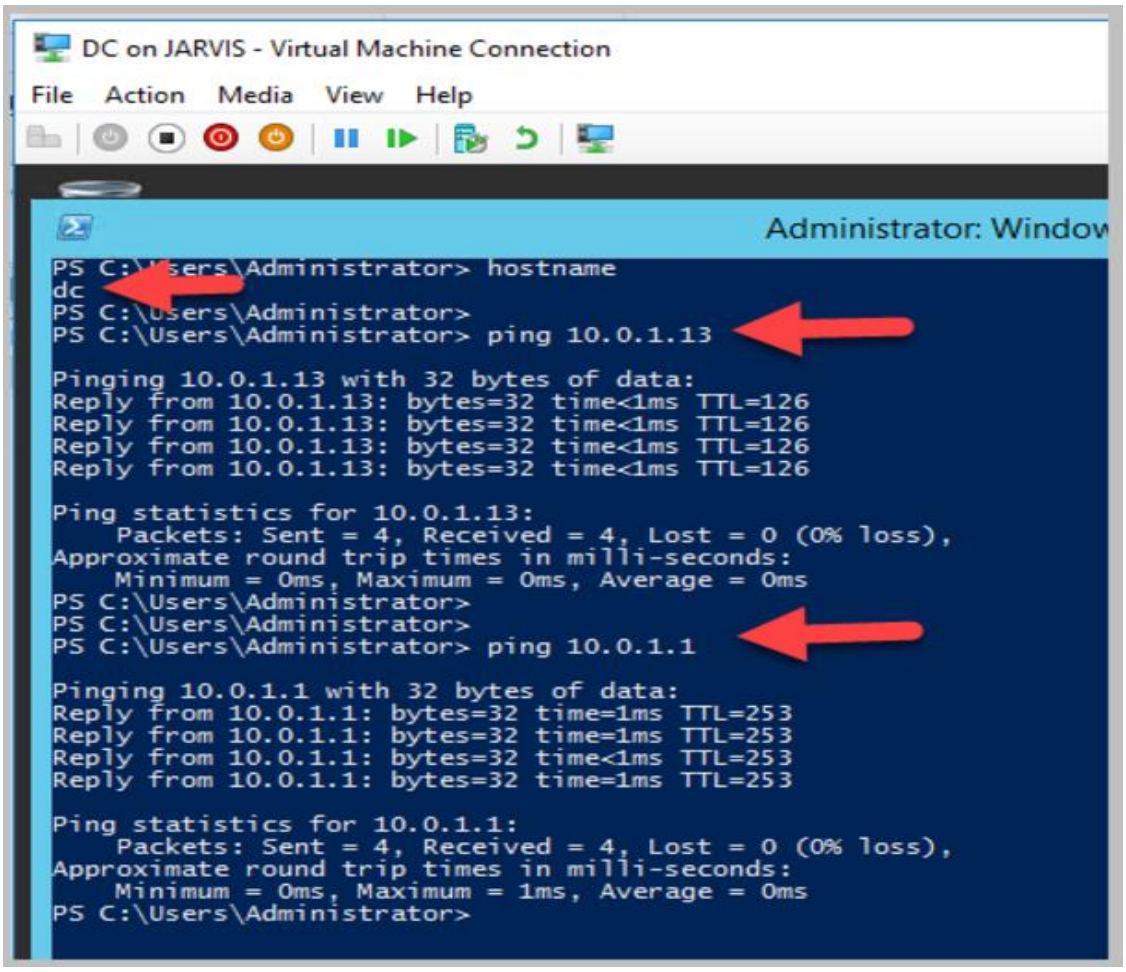
- Check the IP address of your host machine

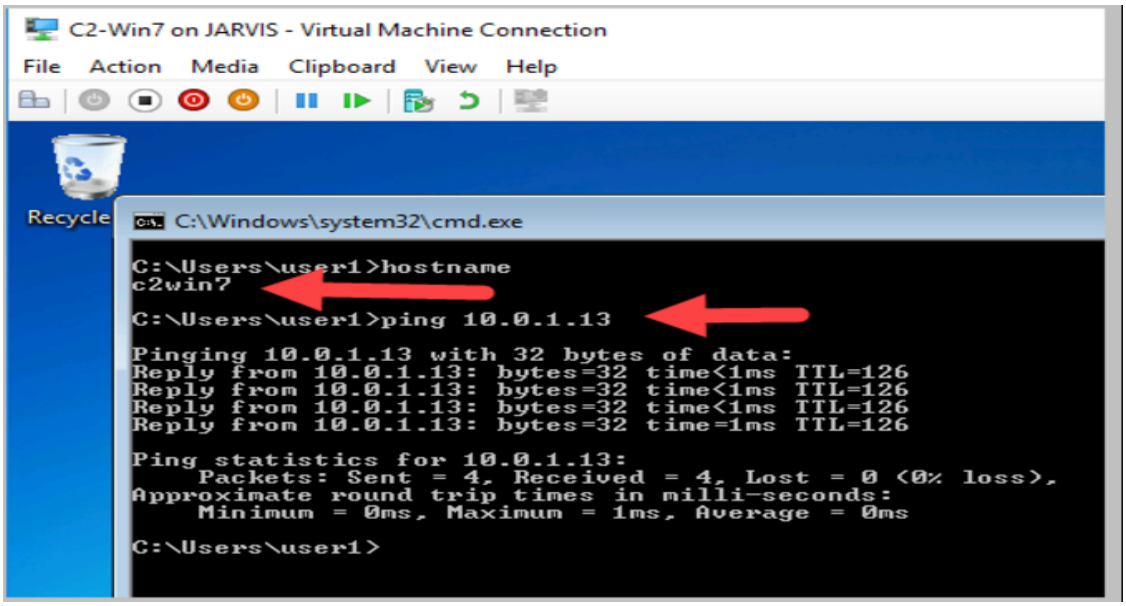
```
Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : tx.rr.com
   IPv6 Address. . . . . . . . . . . : 2605:6000:151e:80be:f83f:af66:bbcc:fafa
   Temporary IPv6 Address. . . . . . : 2605:6000:151e:80be:68bf:[illegible]bcc:2099:dc09
   Link-local IPv6 Address . . . . . : fe80::f83f:af[illegible]:fafa%10
   IPv4 Address. . . . . . . . . . . : 10.0.1.13
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::6e70:9fff:fed4:2900%10
                                       10.0.1.1
```

- Try to ping the lab systems. Remember the DC is 192.168.1.200. Since we chose "**Private**" when we created the switch, the host machine cannot see the lab VMs

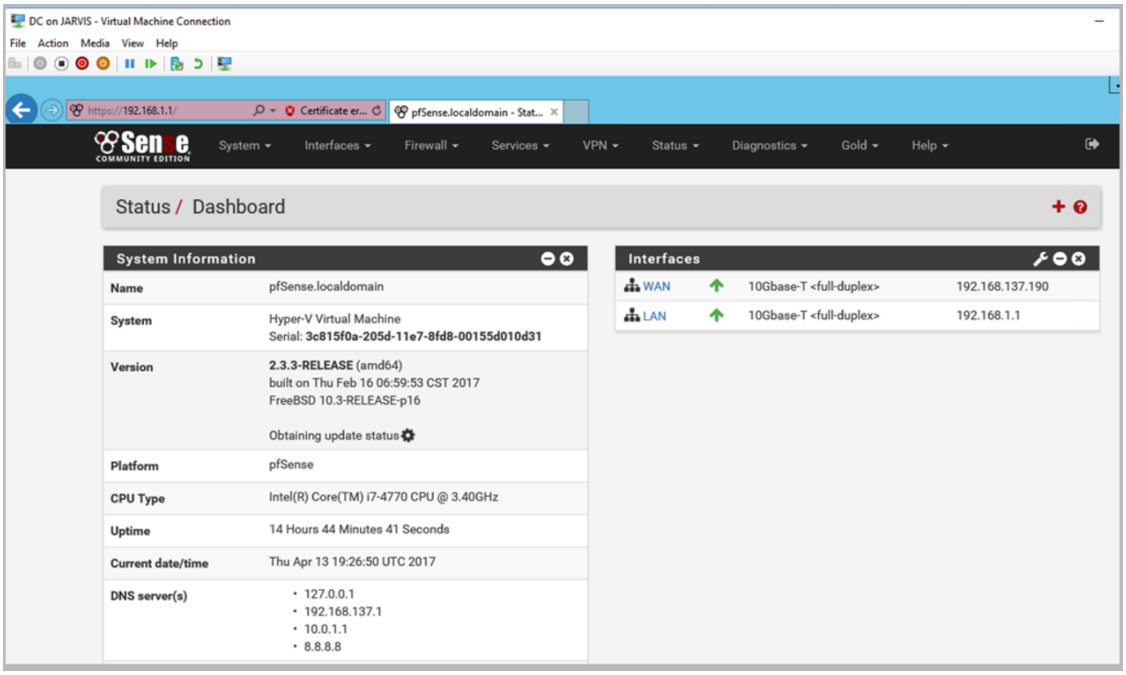
```
C:\Users\raj>ping 192.168.1.200

Pinging 192.168.1.200 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 192.168.1.200:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
C:\Users\raj>
C:\Users\raj>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\raj>
```

- Switch to one of the lab computers, and try to ping the host system. As you can see, all lab systems (Windows 10 and Windows 7) can ping the host IP.

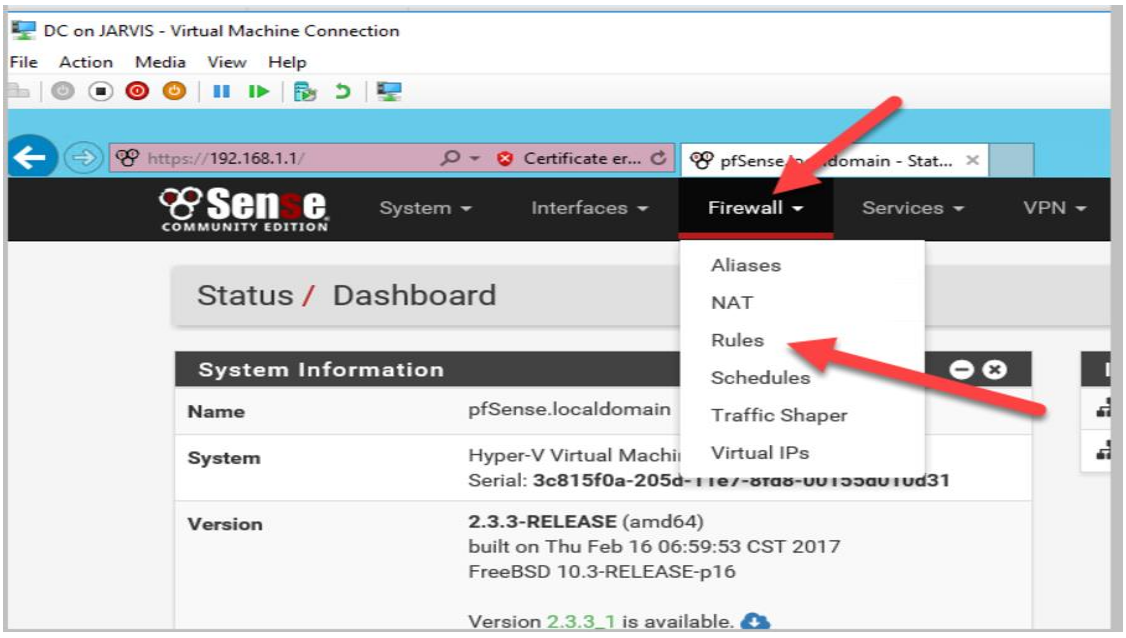

DC on JARVIS - Virtual Machine Connection
File Action Media View Help
Administrator: Windo
PS C:\Users\Administrator> hostname
dc
PS C:\Users\Administrator>
PS C:\Users\Administrator> ping 10.0.1.13
Pinging 10.0.1.13 with 32 bytes of data:
Reply from 10.0.1.13: bytes=32 time<1ms TTL=126
Reply from 10.0.1.13: bytes=32 time<1ms TTL=126
Reply from 10.0.1.13: bytes=32 time<1ms TTL=126
Reply from 10.0.1.13: bytes=32 time<1ms TTL=126
Ping statistics for 10.0.1.13:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> ping 10.0.1.1
Pinging 10.0.1.1 with 32 bytes of data:
Reply from 10.0.1.1: bytes=32 time=1ms TTL=253
Reply from 10.0.1.1: bytes=32 time=1ms TTL=253
Reply from 10.0.1.1: bytes=32 time<1ms TTL=253
Reply from 10.0.1.1: bytes=32 time=1ms TTL=253
Ping statistics for 10.0.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\Administrator>


C2-Win7 on JARVIS - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle
C:\Windows\system32\cmd.exe
C:\Users\user1>hostname
c2win7
C:\Users\user1>ping 10.0.1.13
Pinging 10.0.1.13 with 32 bytes of data:
Reply from 10.0.1.13: bytes=32 time<1ms TTL=126
Reply from 10.0.1.13: bytes=32 time<1ms TTL=126
Reply from 10.0.1.13: bytes=32 time<1ms TTL=126
Reply from 10.0.1.13: bytes=32 time=1ms TTL=126
Ping statistics for 10.0.1.13:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\user1>

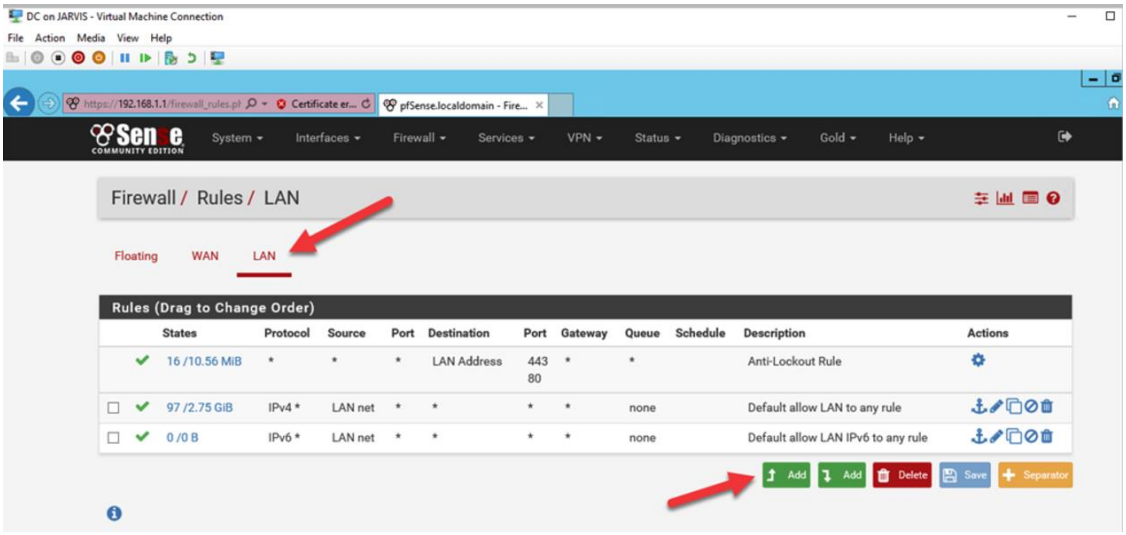
- Let's fix this issue using our PFSense firewall. We can do a whole lot with PFSense, but this will get your feet wet to learn the basics.



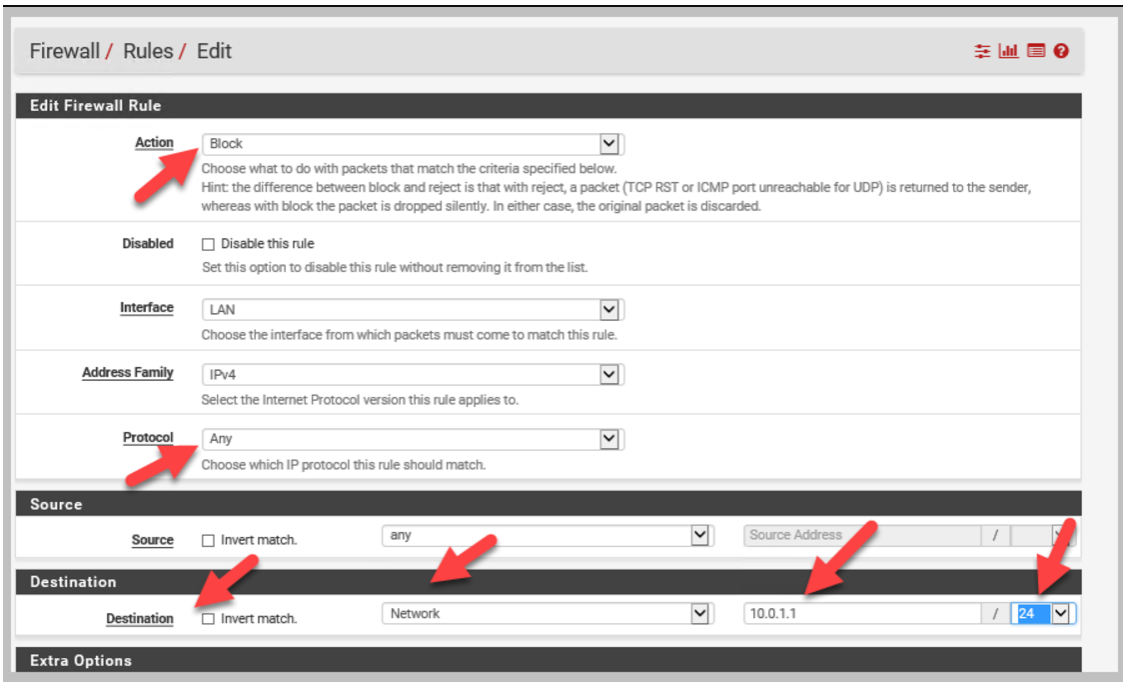
- Login to DC and go to http://192.168.1.1 and login with admin. Password is something you changed when we configured PFSense



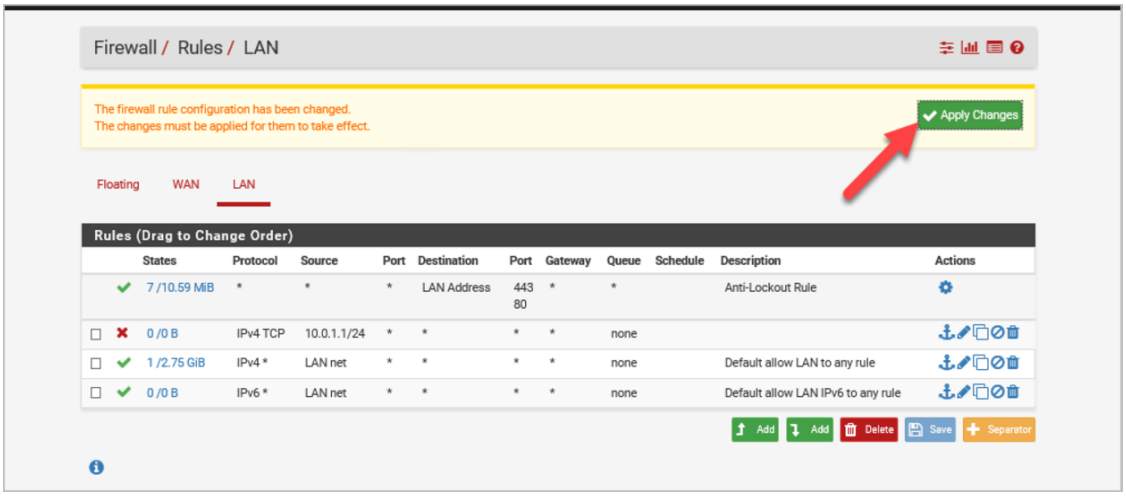
- Got to Firewall/rules/LAN



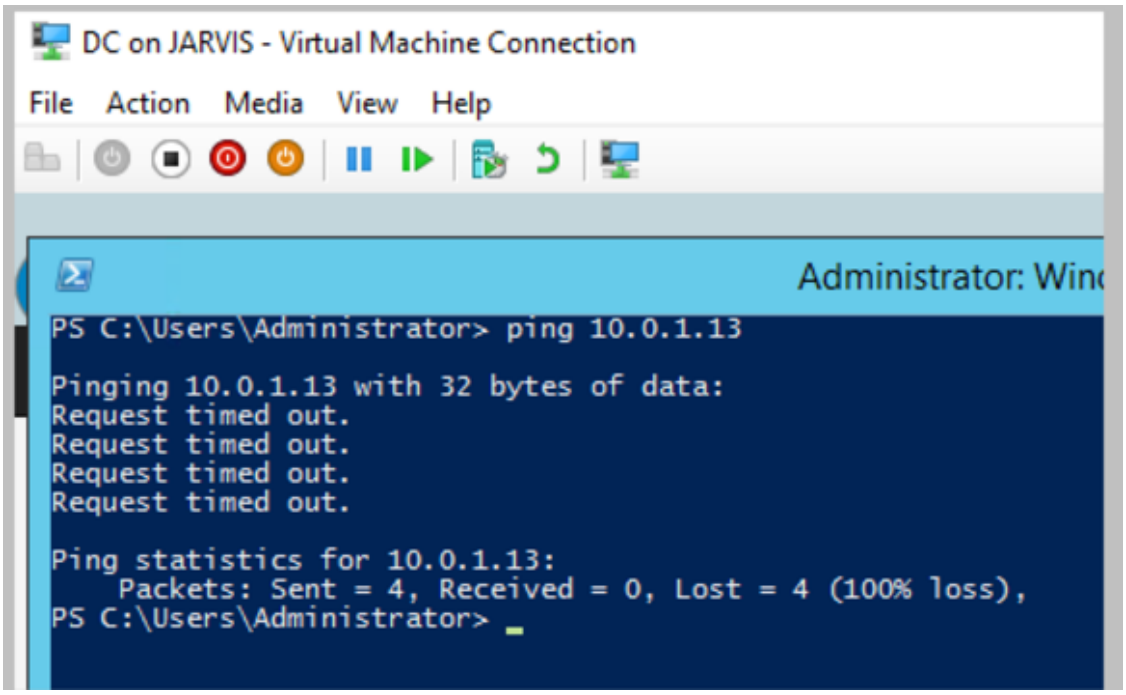
- Select "**Block**" in Action. Select protocol to "**Any**". For destination, choose **network** and give the range in your network. In my example, it is 10.0.1.1/24

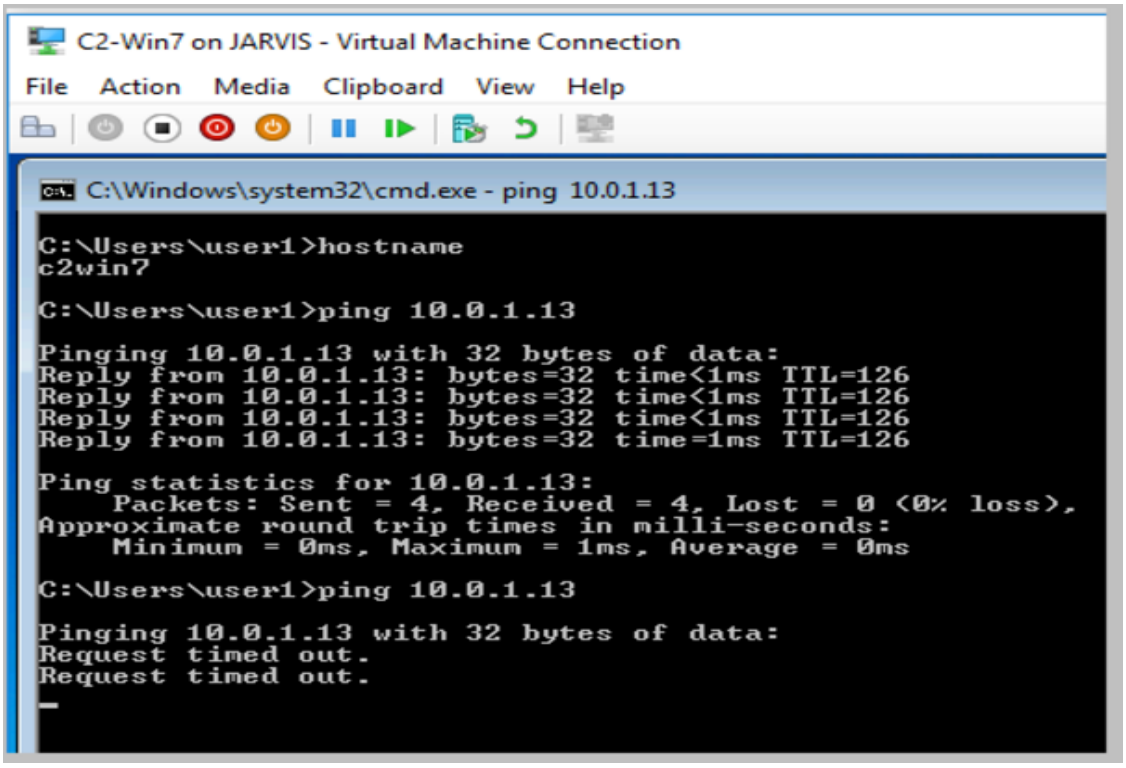


- Finally, Apply changes



- Now try ping our host computer from any of the lab machines. It will fail. Even if you have a Malware in you lab network, your host machine will be protected.





if you have come this far, you should have a fully functional active directory lab, and kudos to you for your perseverance and motivation. Don't stop here. Be creative and add more virtual machines to the lab by exporting the existing VMs and importing with different host names. Also by creating snapshots, you should be able to restore to any point in time. I'll update the manual the with more complex scenarios as I see fit. Have fun hacking away in the labs.