

SETTING UP AN ACTIVE DIRECTORY LAB USING HYPER-V VIRTUALIZATION PLATFORM



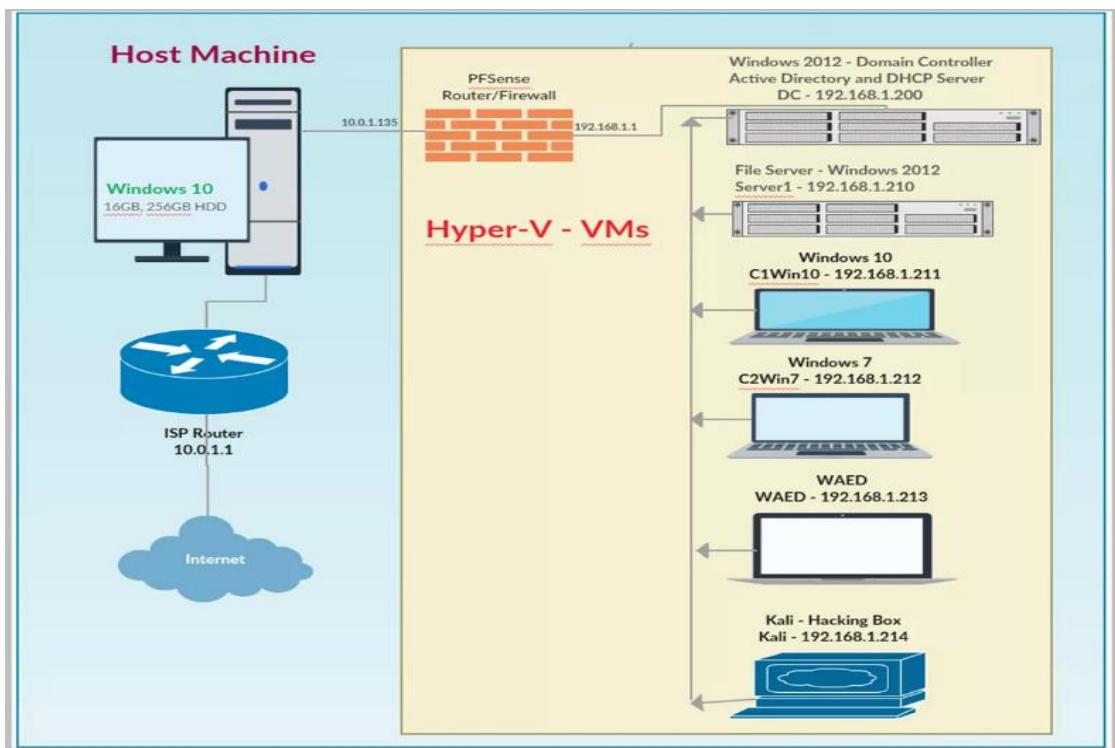
RAJGANESH PANDURANGAN

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!



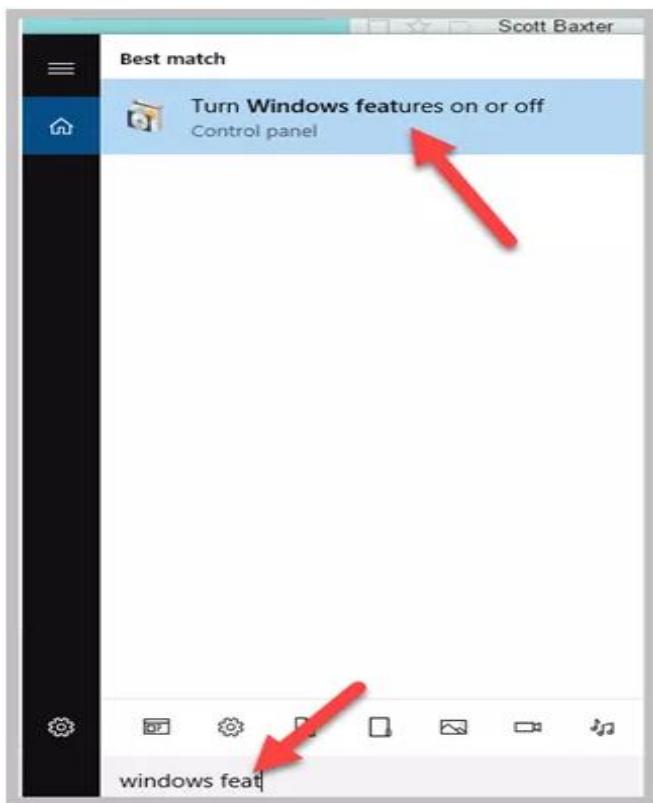
Requirements:

- Windows 10 host machine with at least 8GB Ram

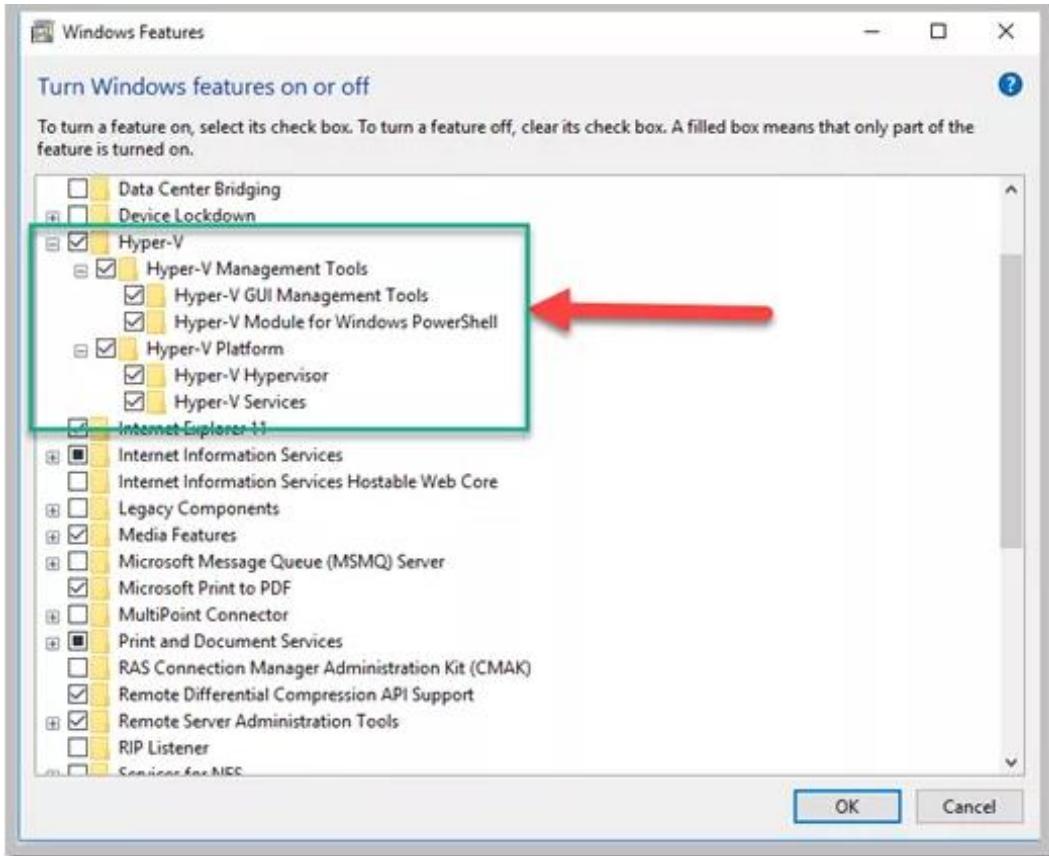
- Windows 2012 Server ISO trial version (<https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2012>)
- Windows 10 ISO trial version (<https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise>)
- Windows 7 ISO (I don't know of a trial version. Add two Windows 10 VMs instead)
- 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.



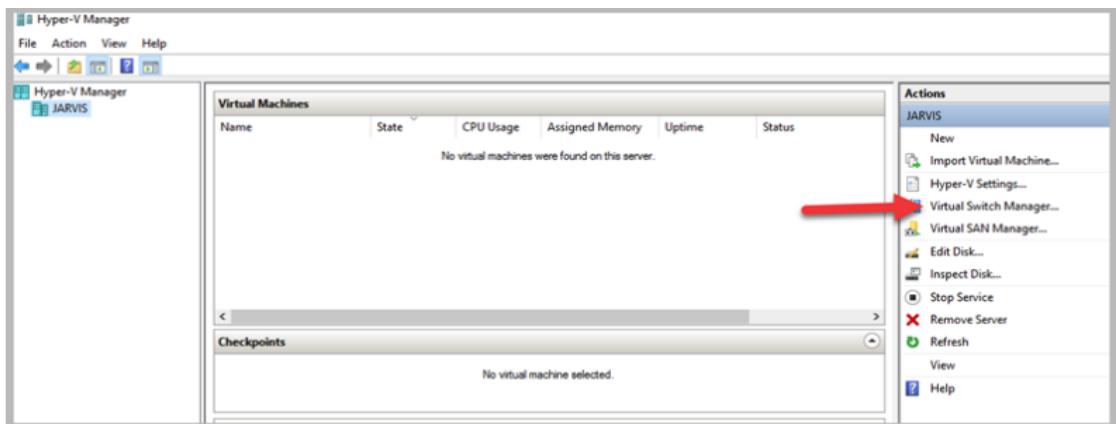
Check all the boxes as shown below, click OK, and restart the machine and Hyper-V should be installed



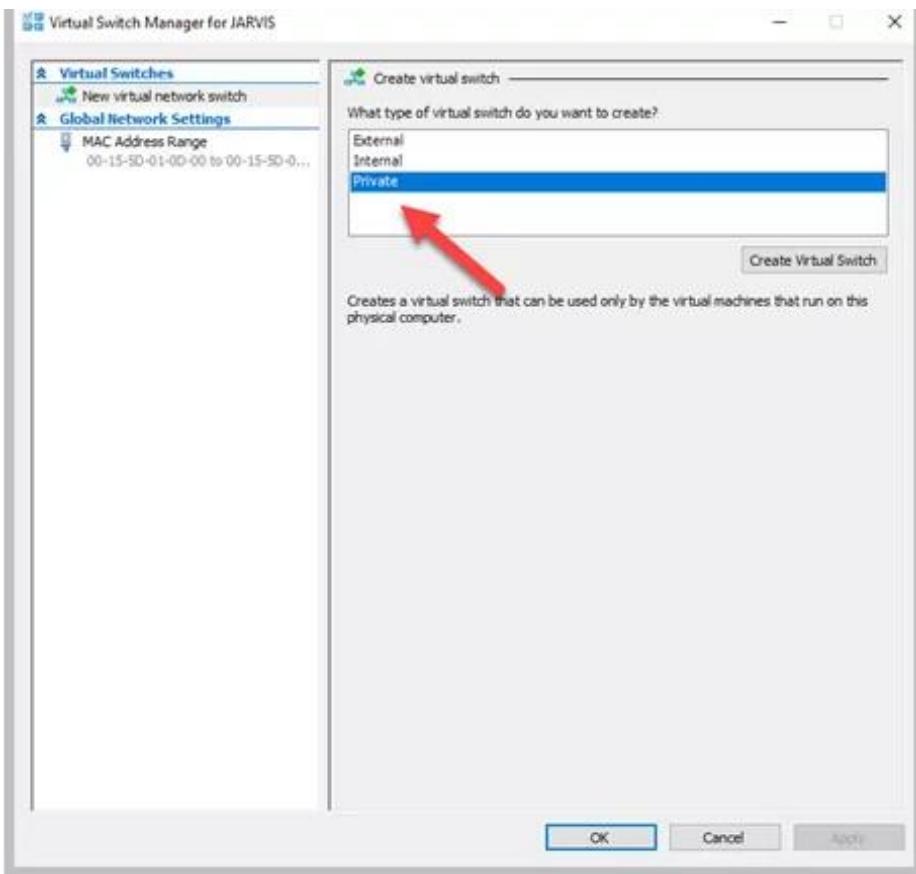
3. Setting up Virtual Switches in Hyper-V

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.

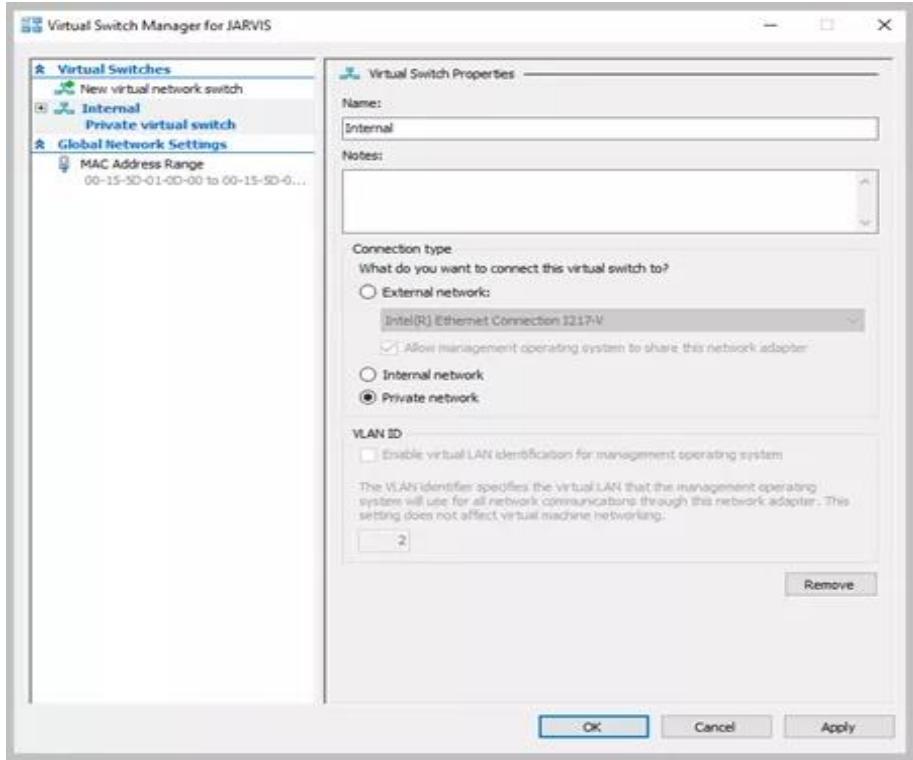
- In Hyper-V, click the ‘Virtual Switch Manager’ as shown below



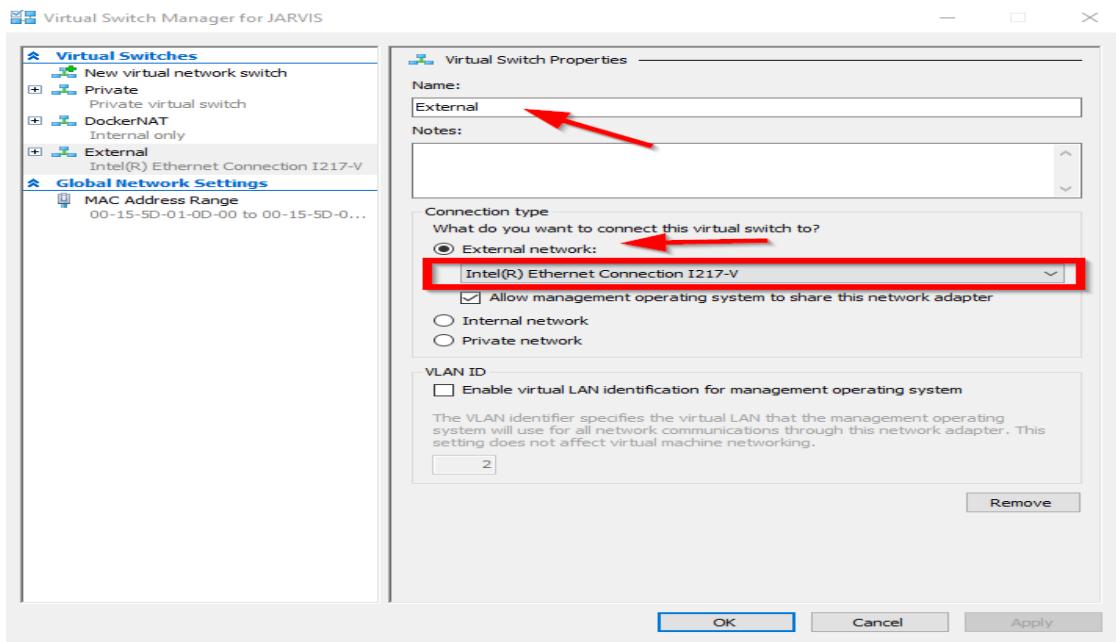
- Select the “Private” and click ‘Create Virtual Switch’ button



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

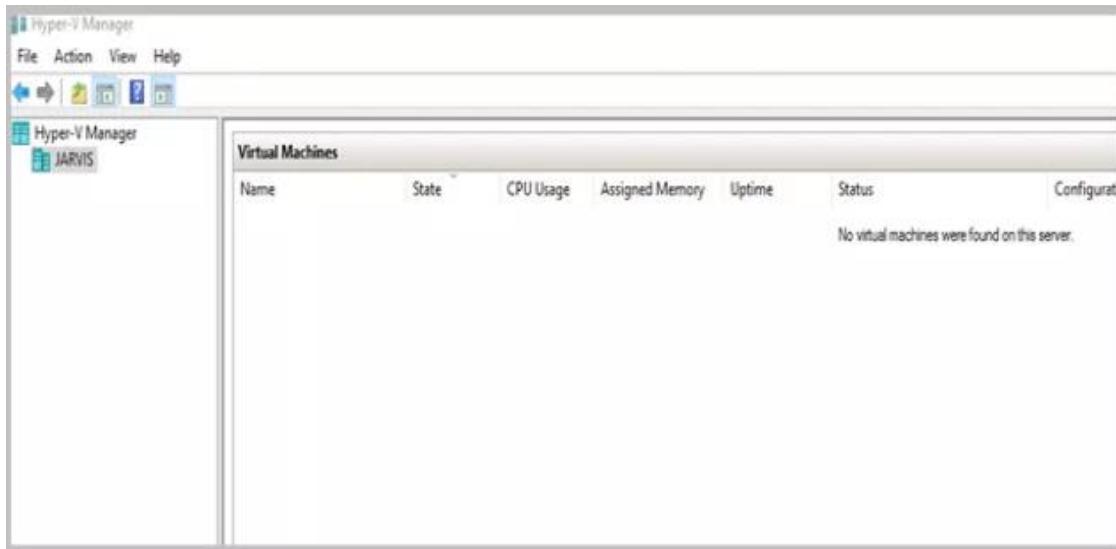


- Repeat the process for creating the “External” switch. Make sure to select the correct External network card for External virtual switch.

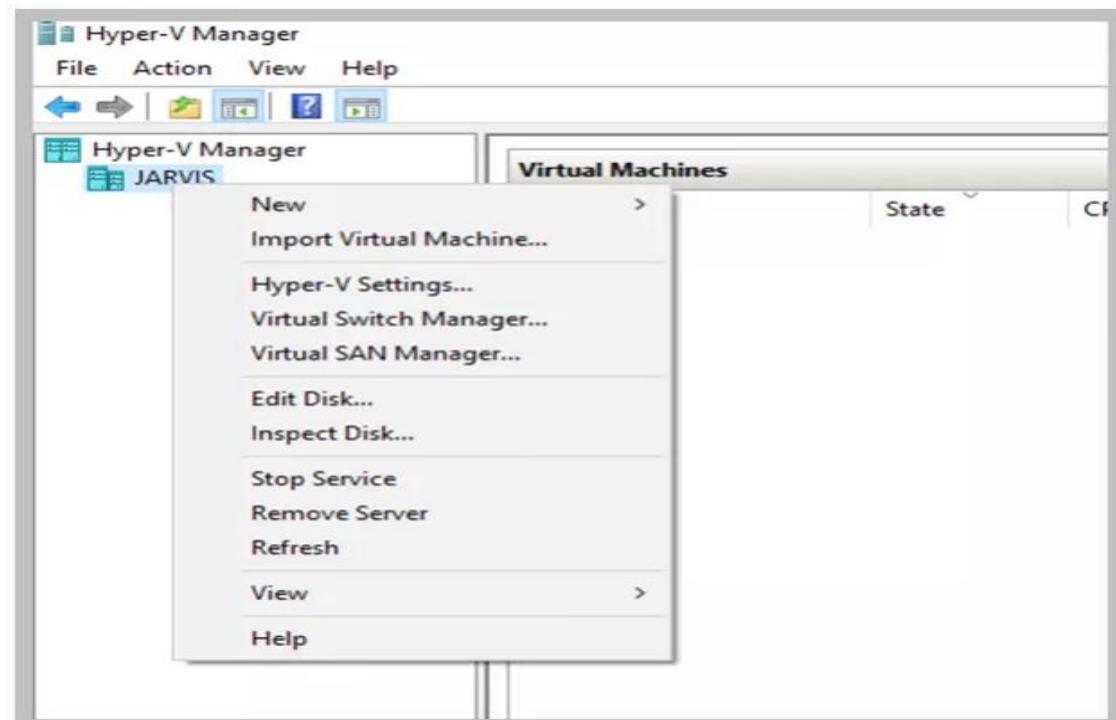


4. Installing Windows 2012 Server

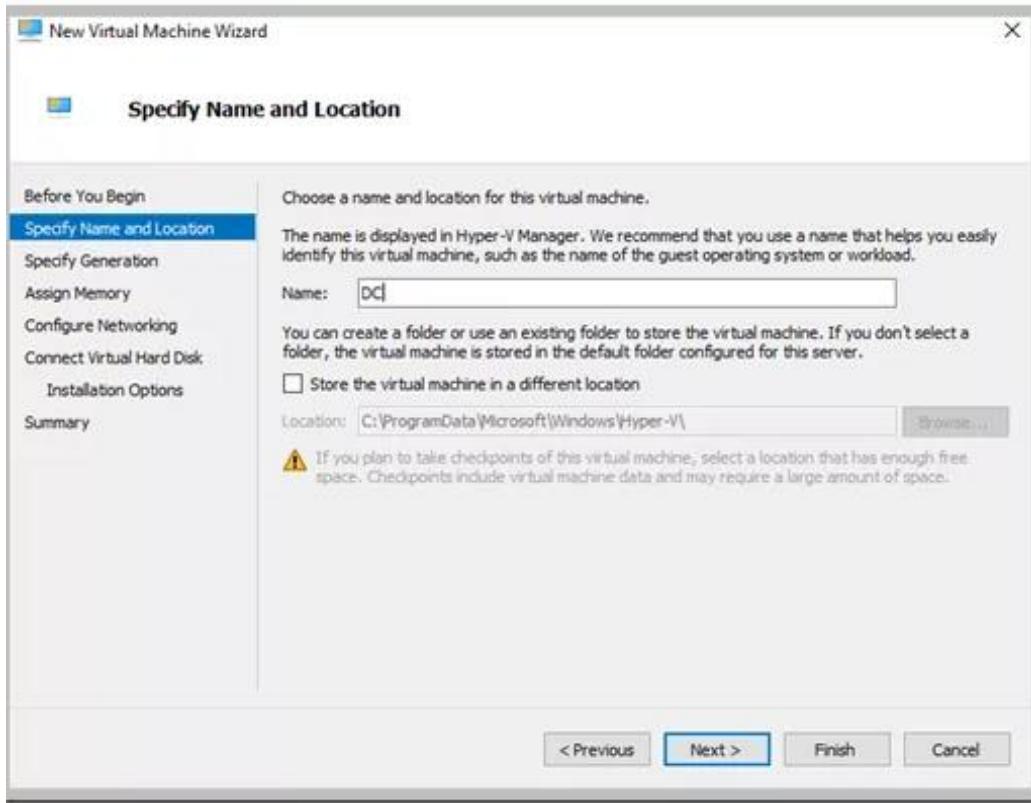
- Open the Hyper-V manager application, and it should have only one host named “Jarvis”, which is the name of my host machine



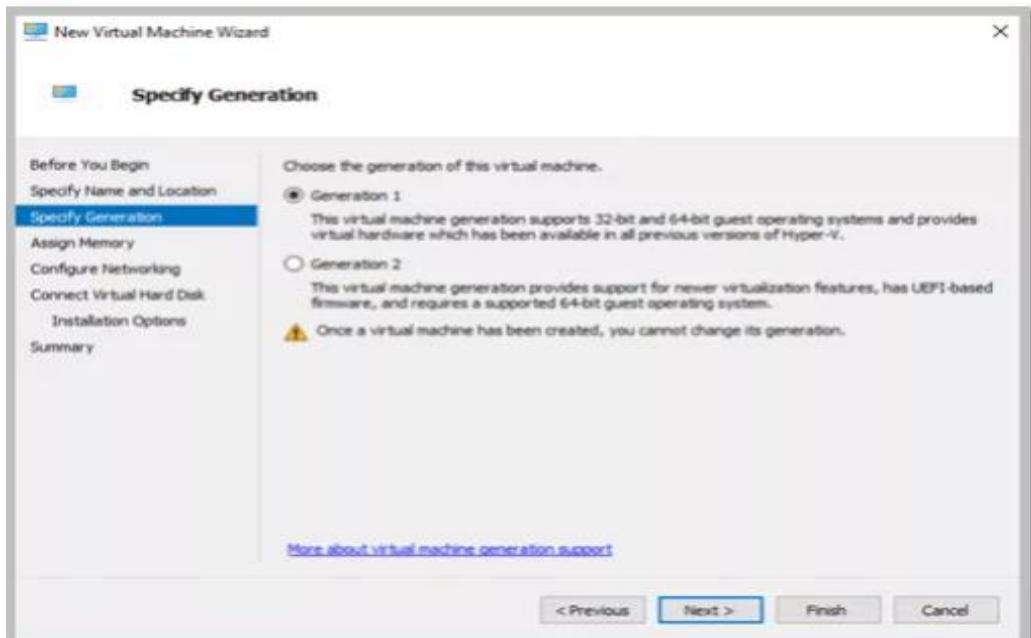
- Right click on “Jarvis” and click “New”



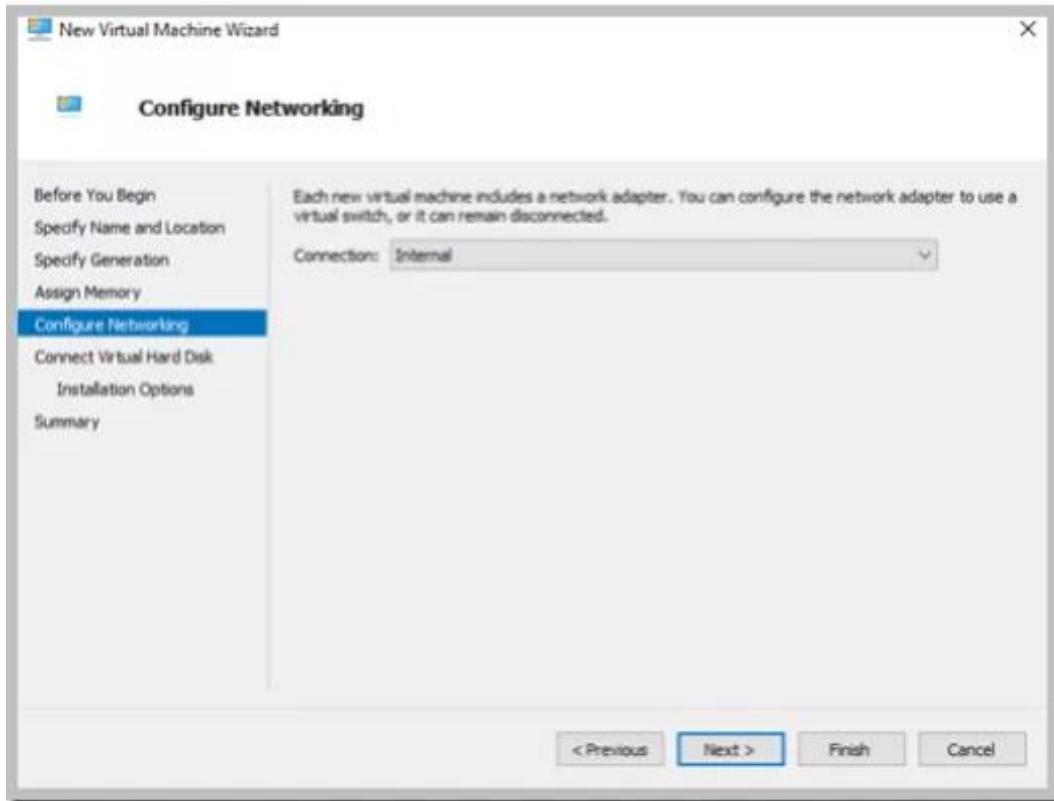
- Name the VM “DC”. This is how it will be identified in Hyper-V console



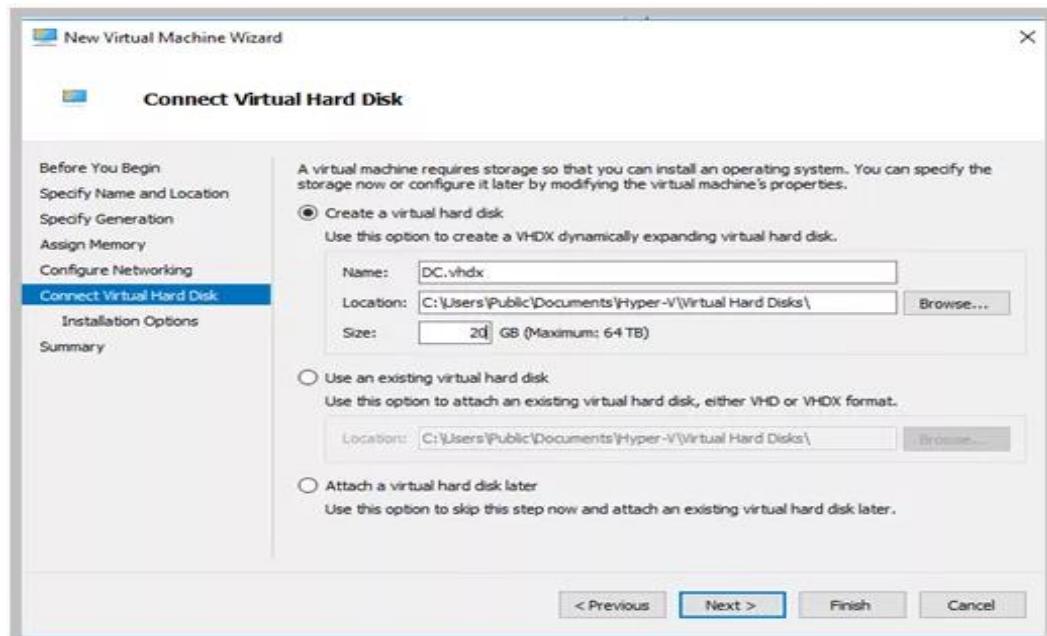
- Pick Generation 1 or Generation 2



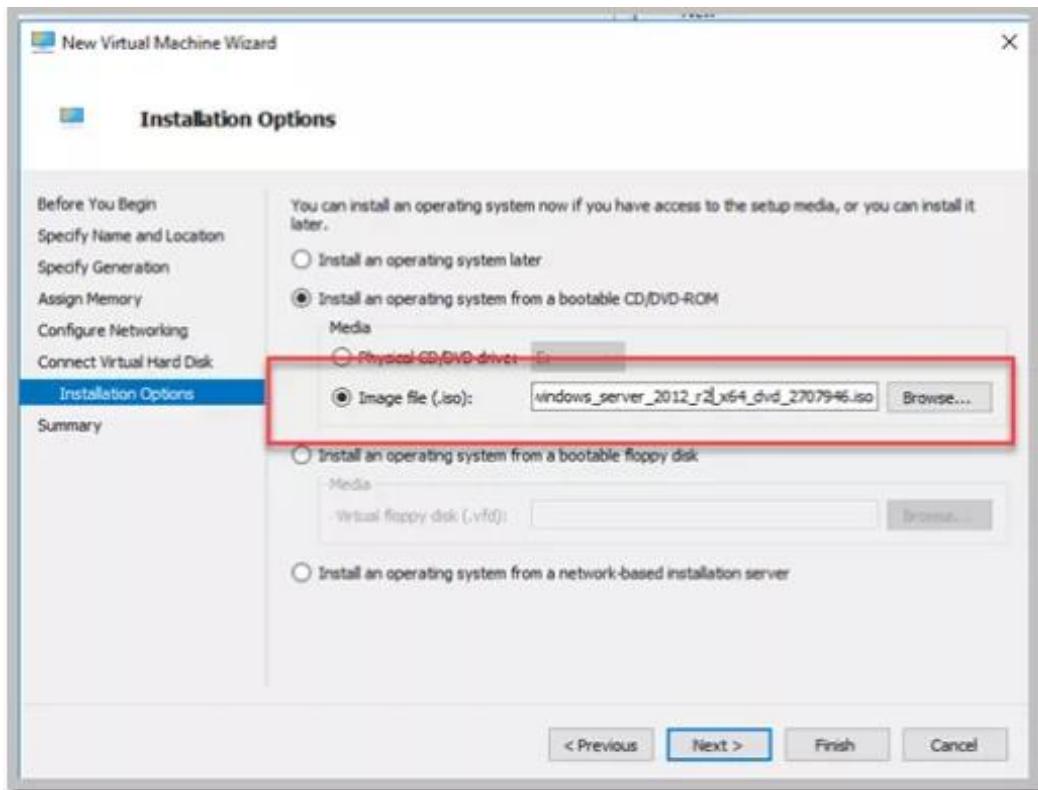
- Pick “Internal” for the network connection



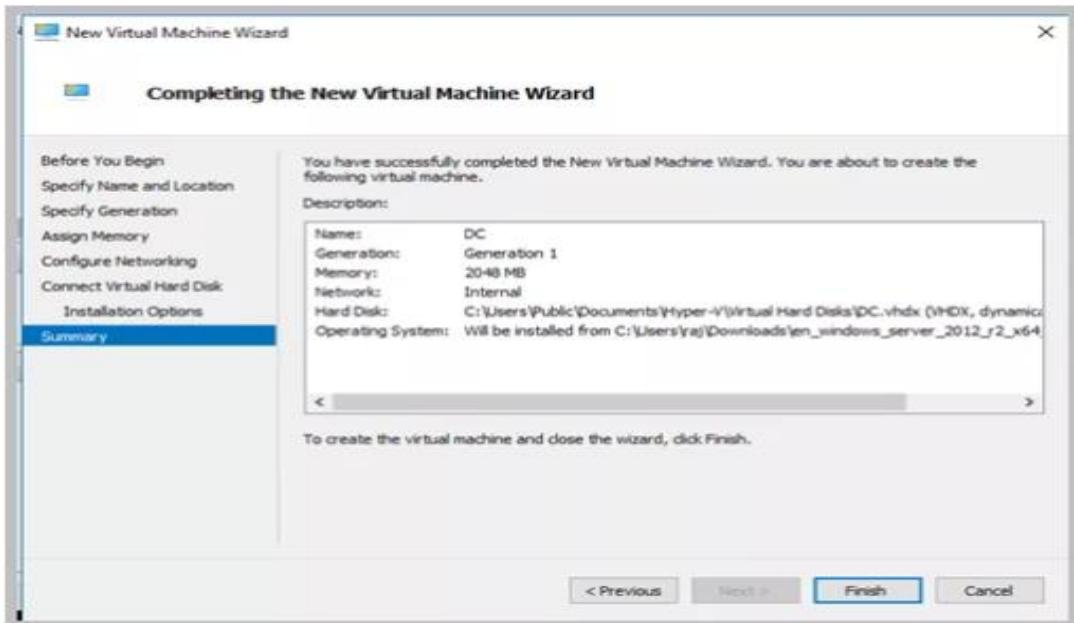
- Use 20GB for the hard drive size



- Choose the location of Windows 2012 iso



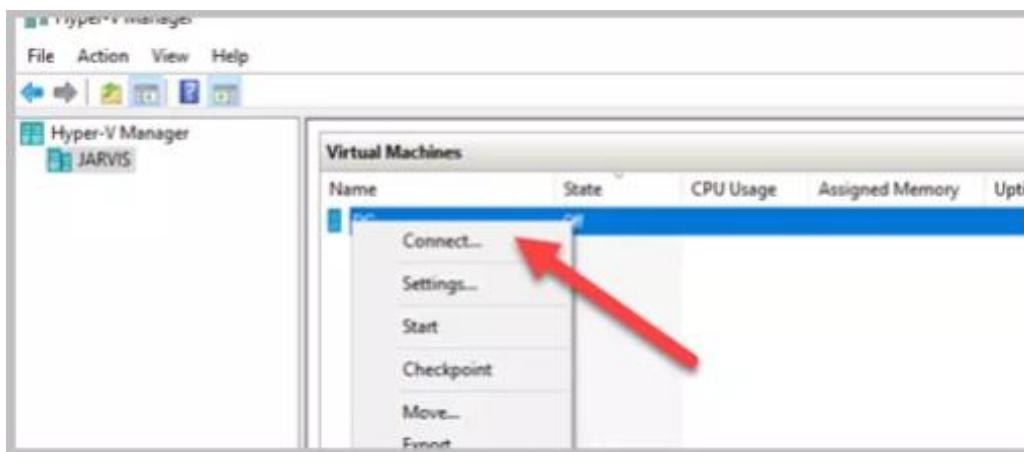
- Review and finish the initial setup process



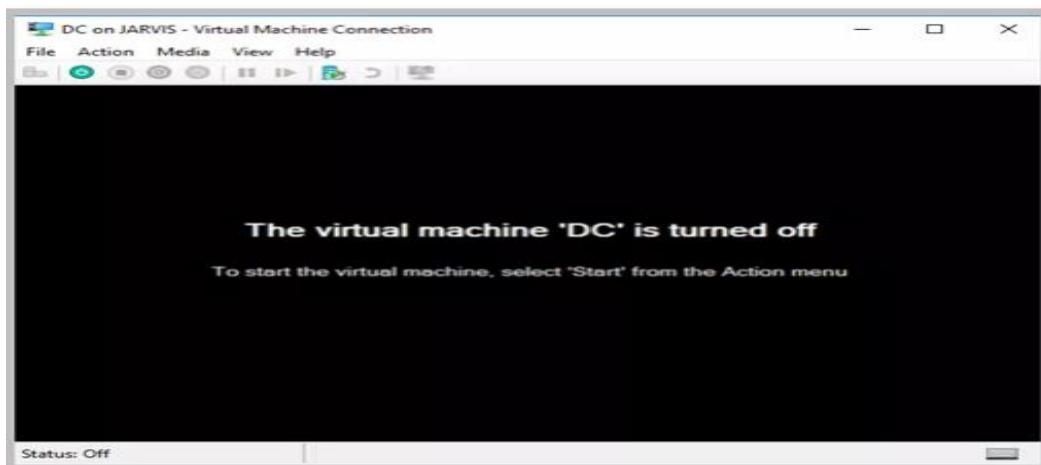
- Now there should be one VM called DC in the list of VM

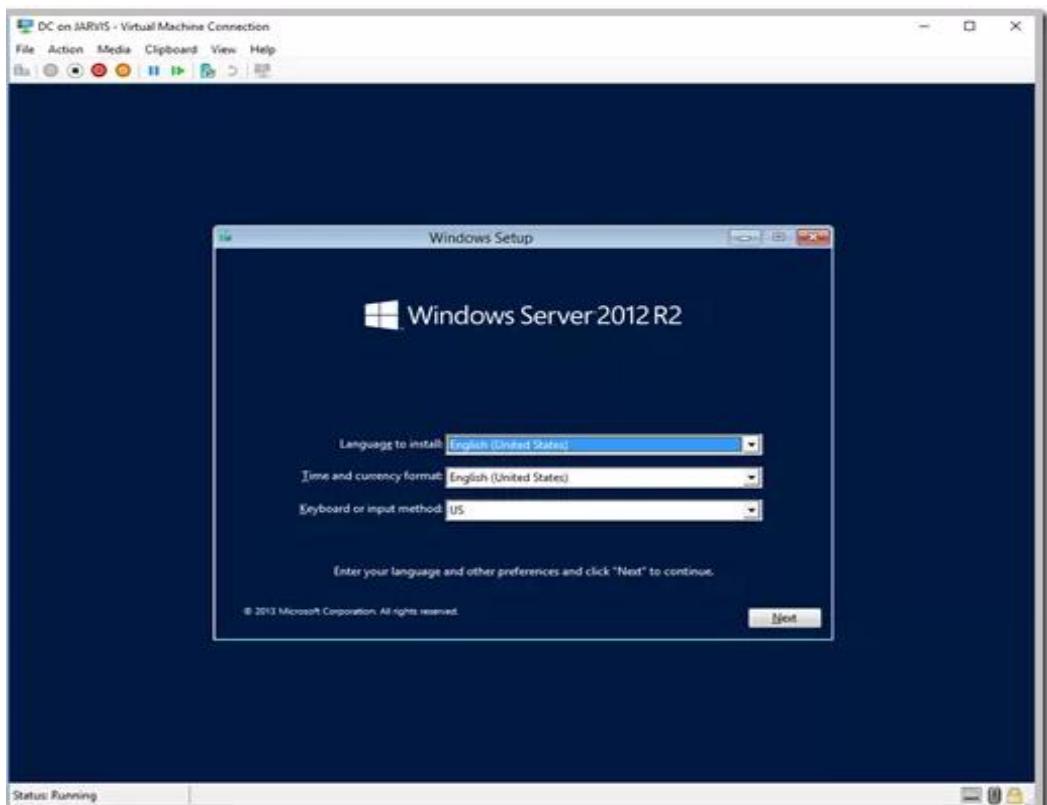


- Right click on "DC" and click "connect"

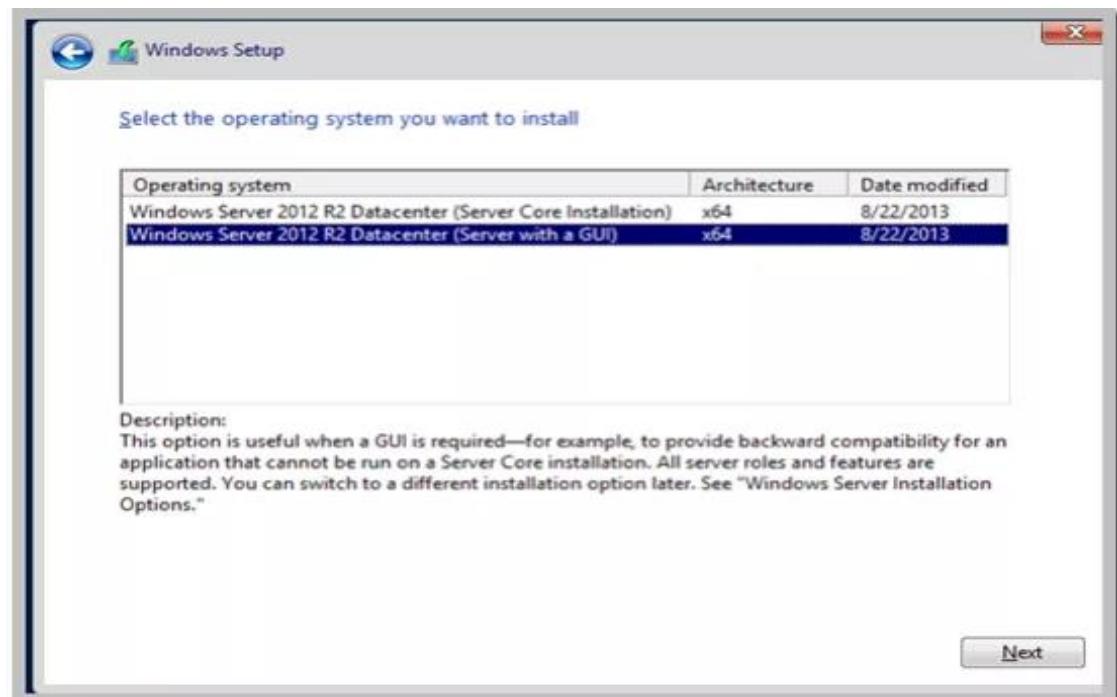


- Click on the Green power button on start the install process

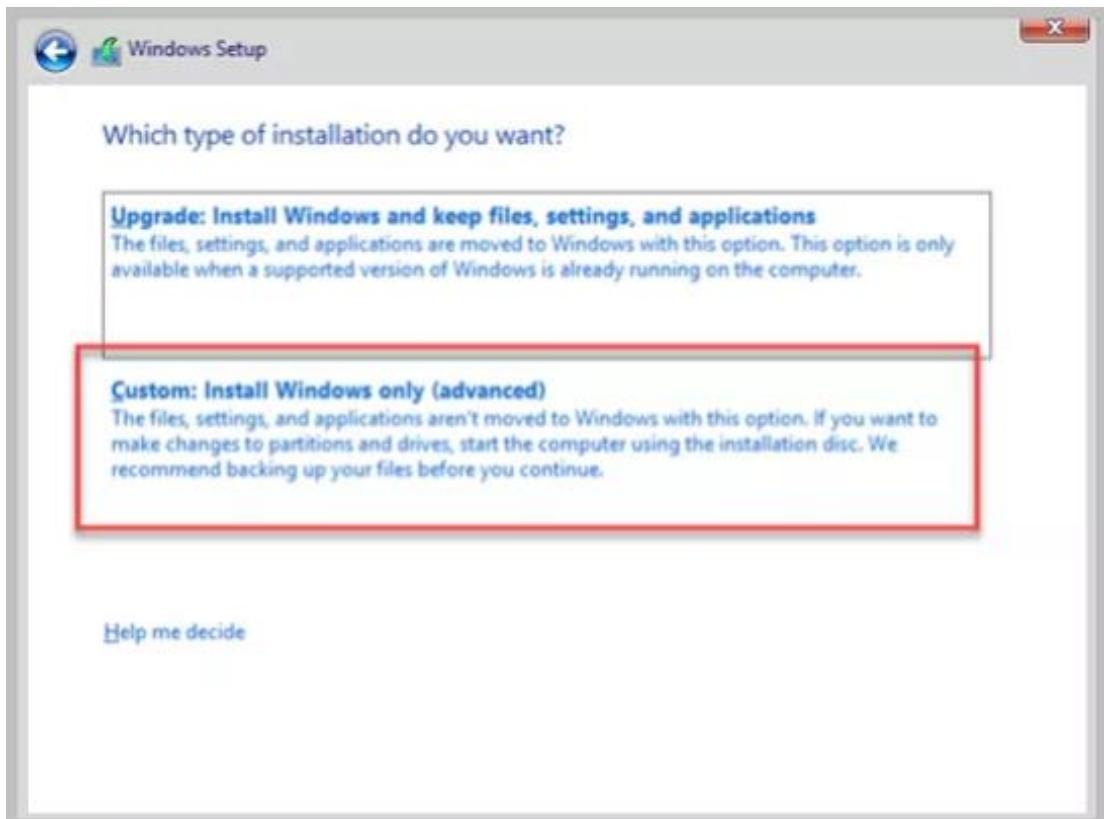




- Choose the option "Server with a GUI"



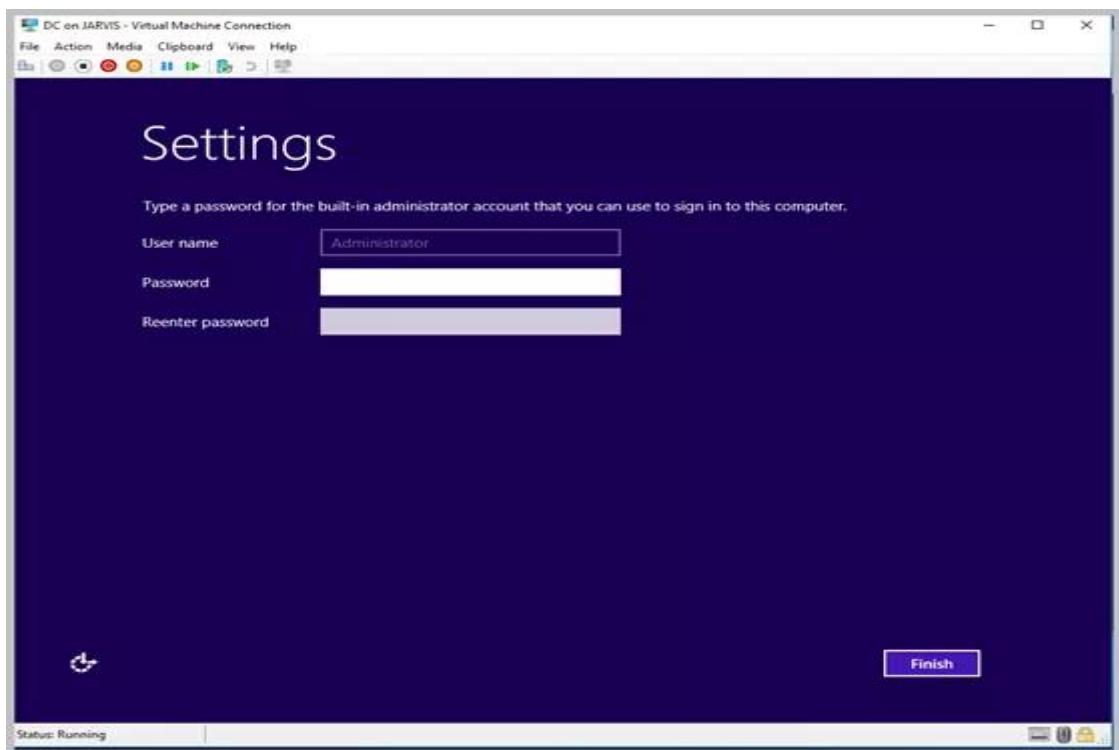
- choose Custom install



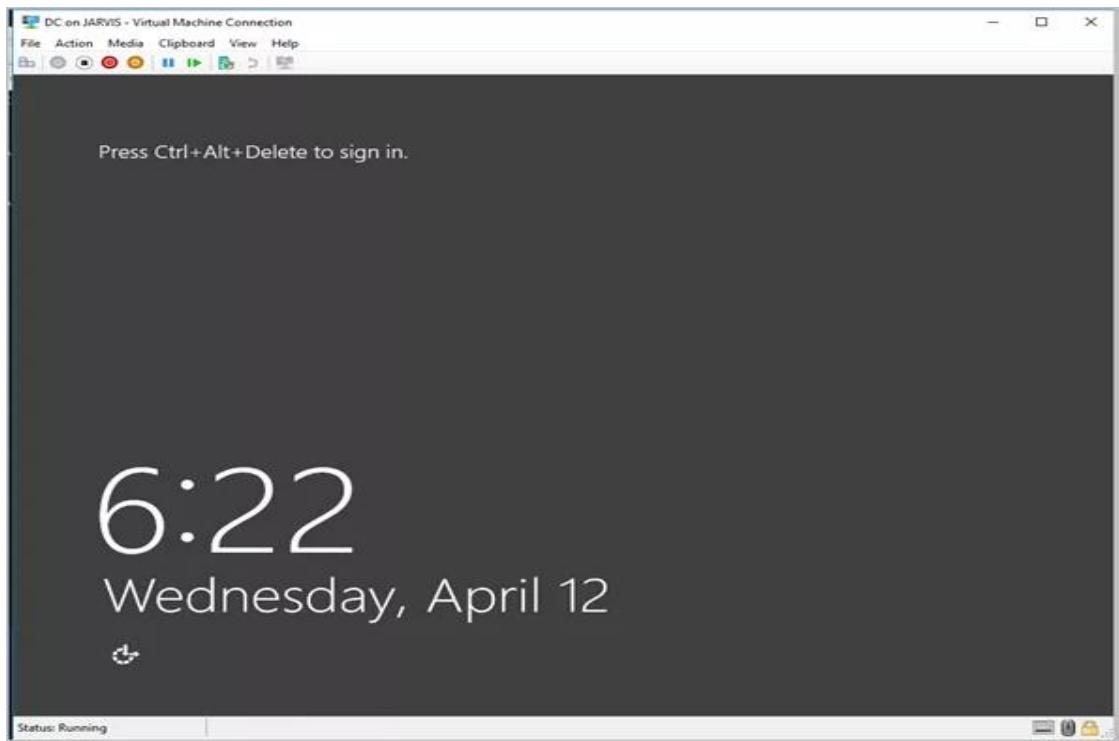
- Wait for the process to complete. It should take around 15 to 20 minutes to complete depending upon the ram of the virtual machine.



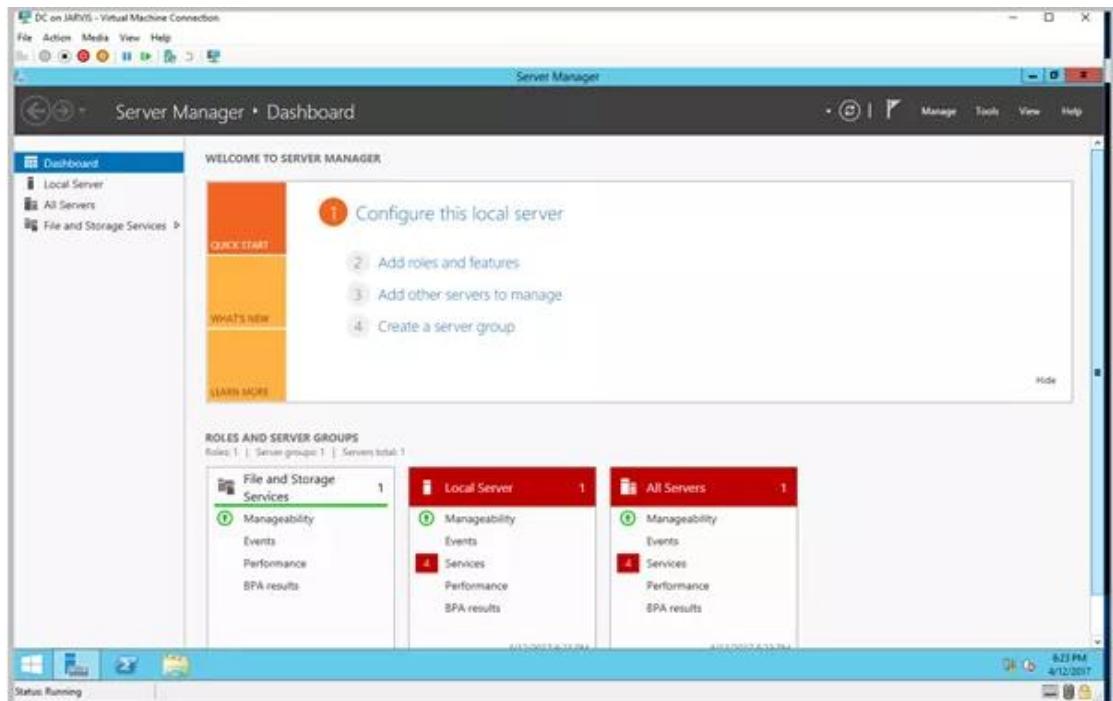
- Choose a strong password. This is the local password of the Windows 2012 system.



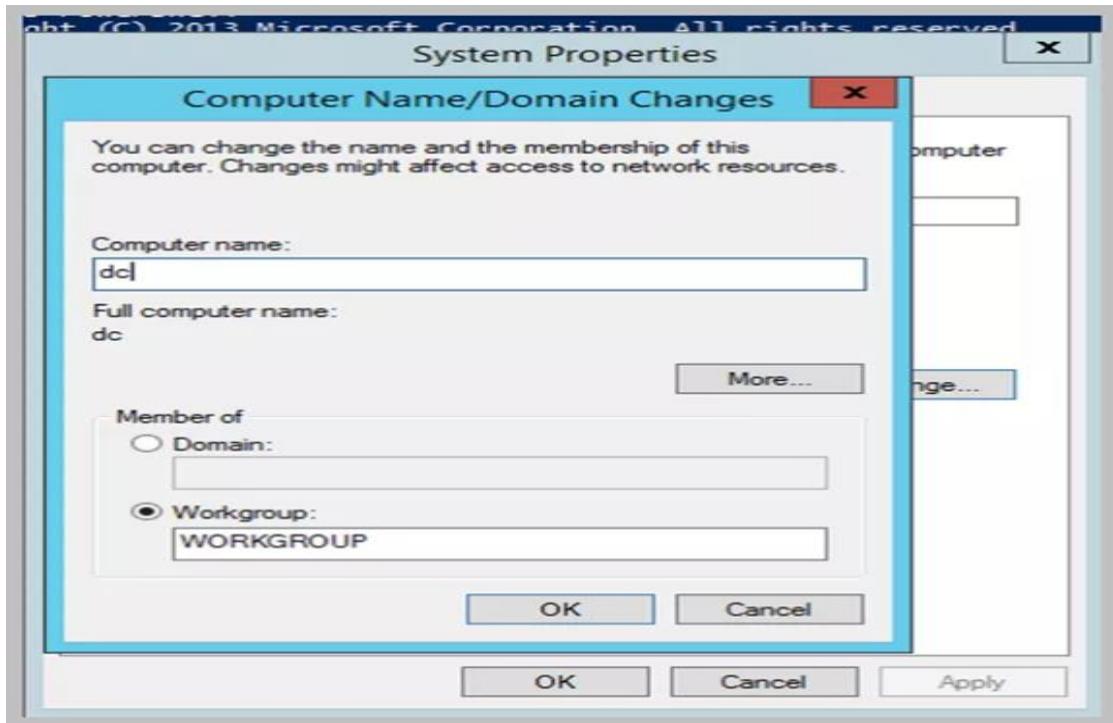
- Go to "Action/Ctrl+Alt+Del" to sign in. Enter Administrator's password to login



- 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.

```

DC on JARVIS - Virtual Machine Connection
File Action Media View Help
Recycle Bin

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ipconfig
windows IP Configuration

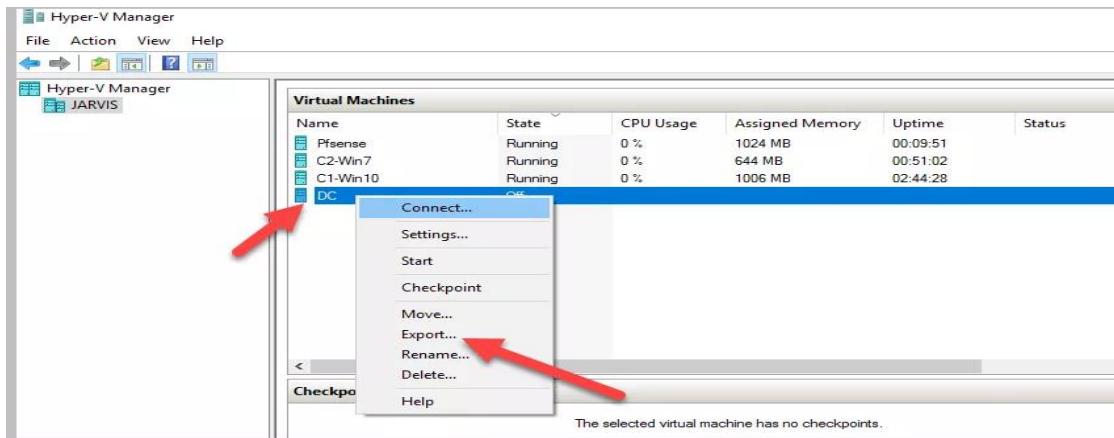
Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . :
  Link-Local IPv6 Address . . . . : fe80::300e:6a0d:ab8f:5a02%12
  Autoconfiguration IPv4 Address . . . . : 169.254.90.2
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . :

Tunnel adapter Local Area Connection* 11:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
  PS C:\Users\Administrator>

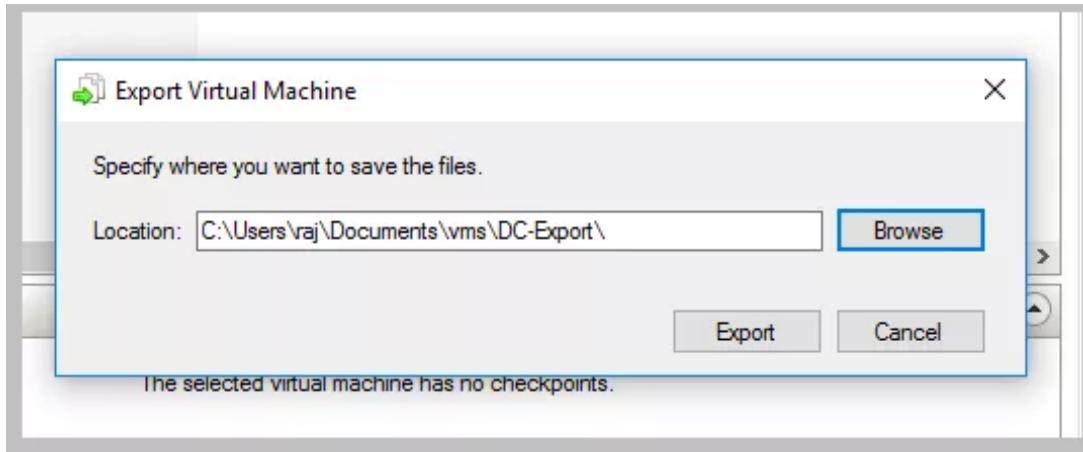
```

It is a private IP address assigned by OS, as it cannot connect to a network

- 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"



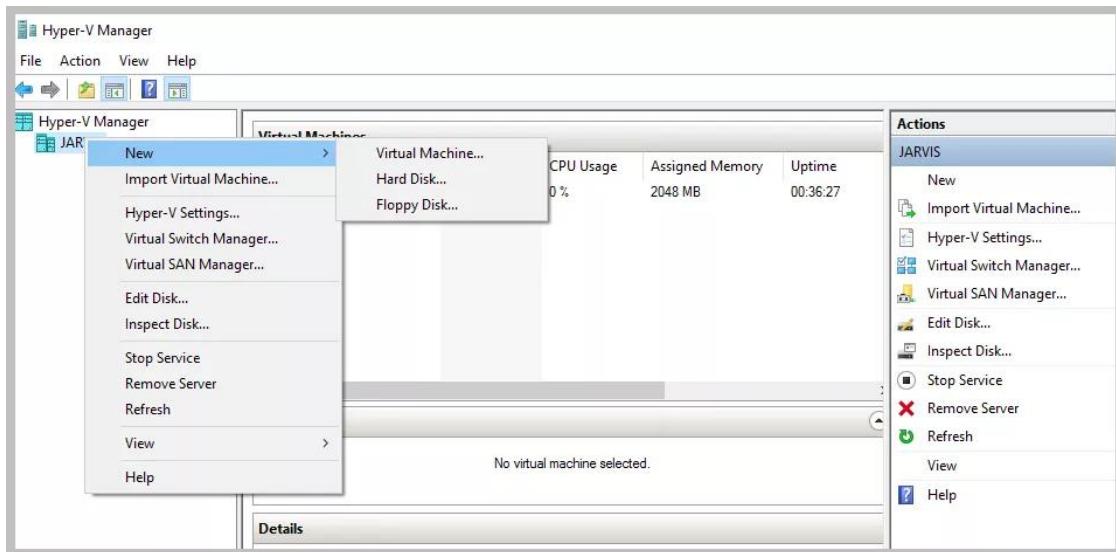
- Choose a location to save the files. We will use these files to create another server in later modules



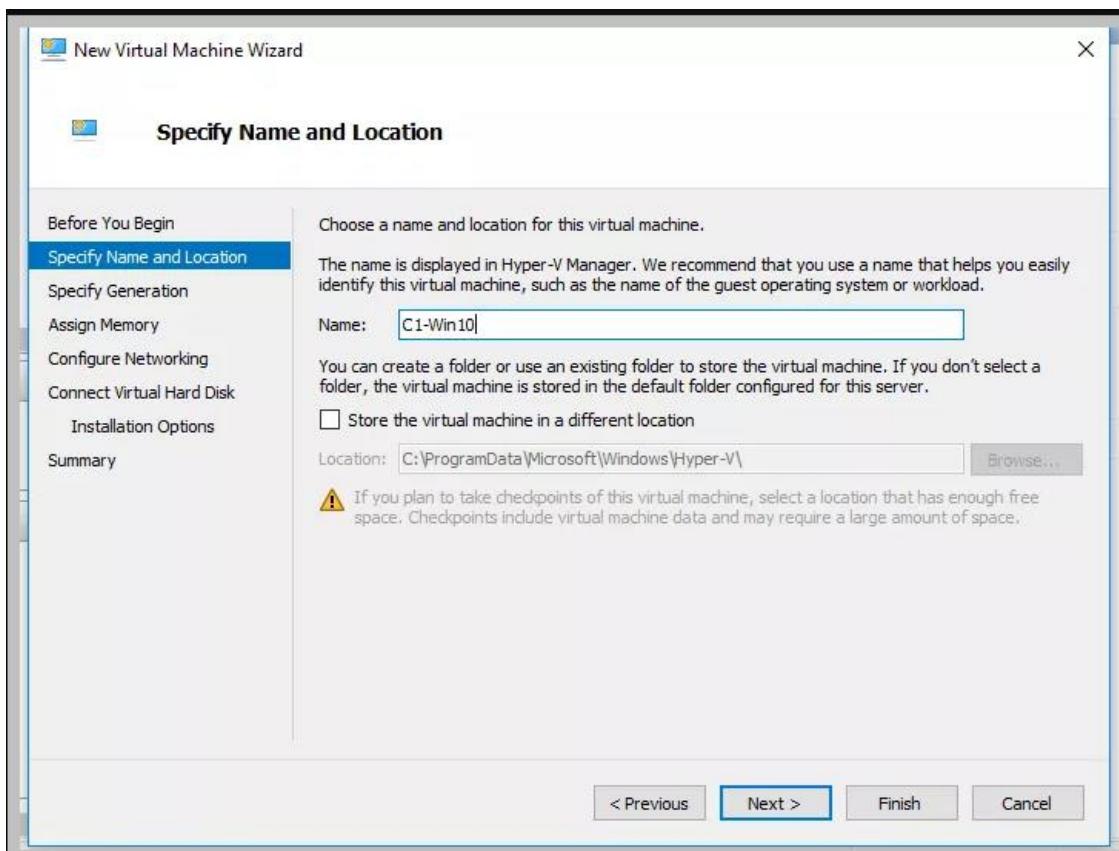
- Wait for the process to complete. All exported files will be stored in the selected folder.

5. Installing Windows 10–64 bit version

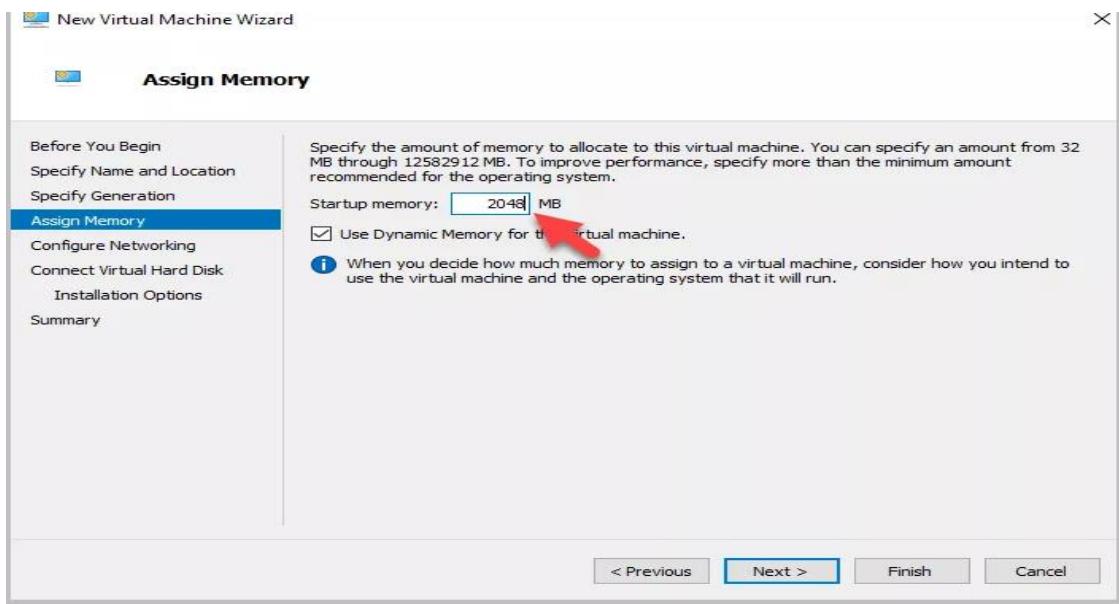
- Right click on “Jarvis” and create a new virtual machine



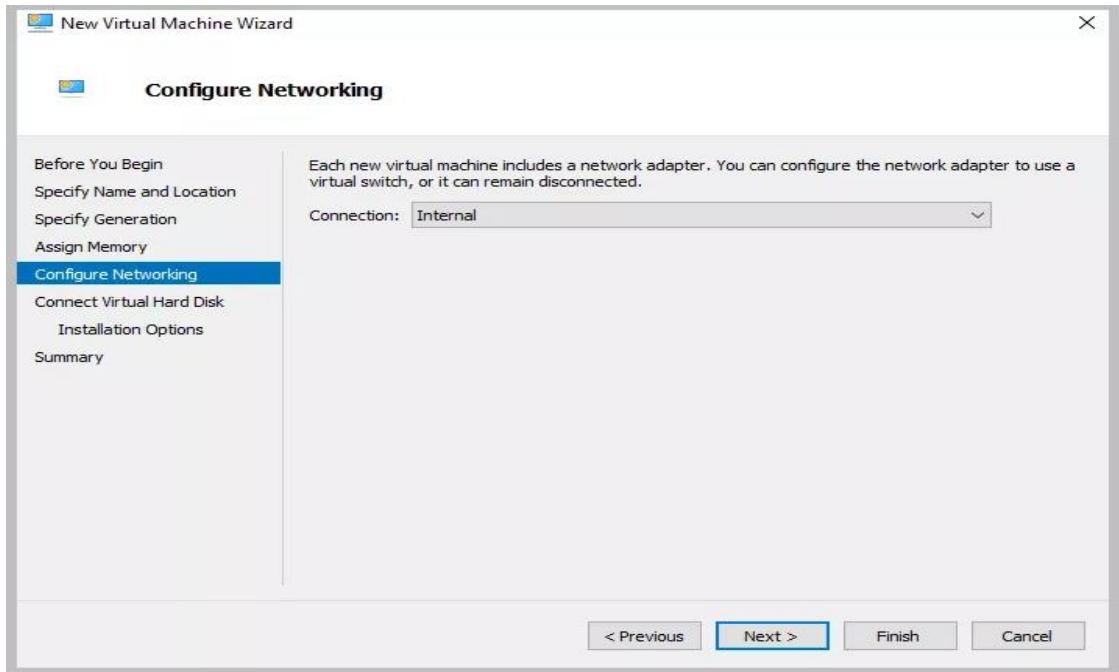
- Name the VM as C1-Win10, which stands for Client1 - Windows 10 machine.



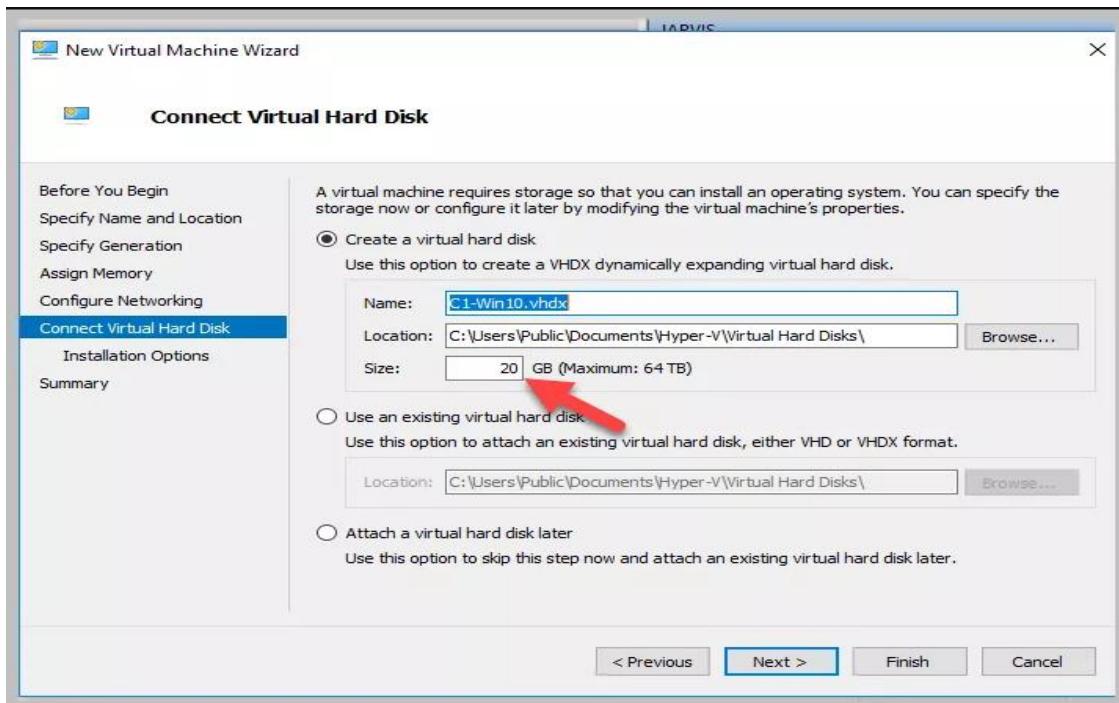
- Assign 2048 ram for the Windows 10 machine



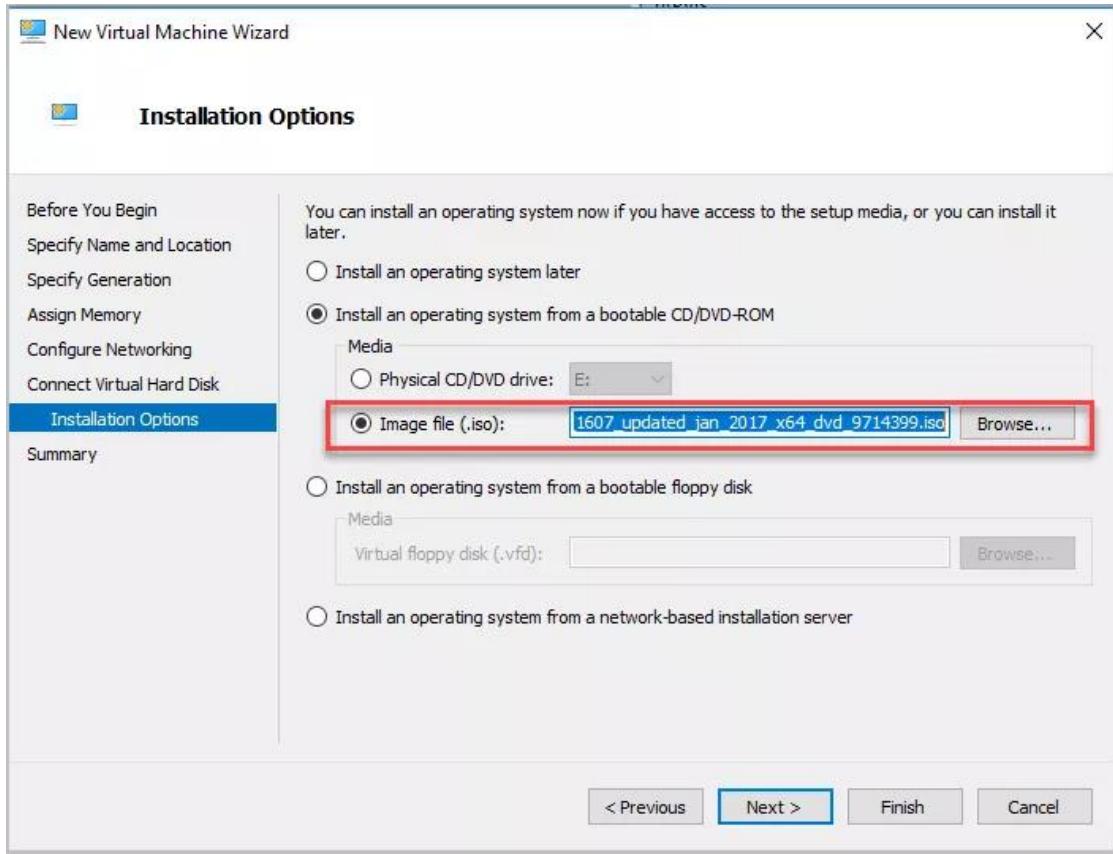
- Choose "Internal" for network connection



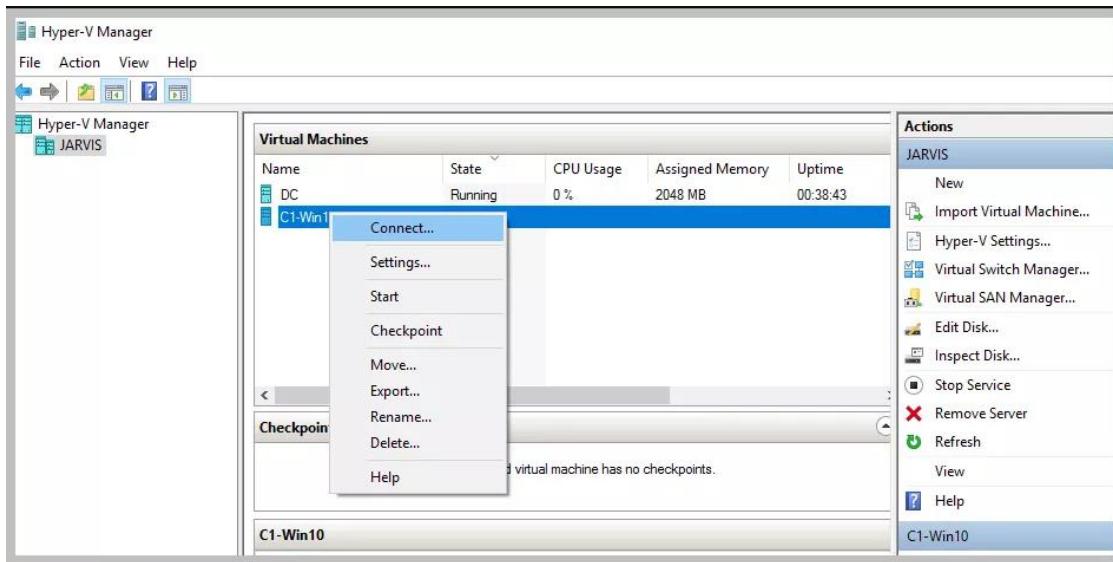
- Assign 20GB for the virtual machine



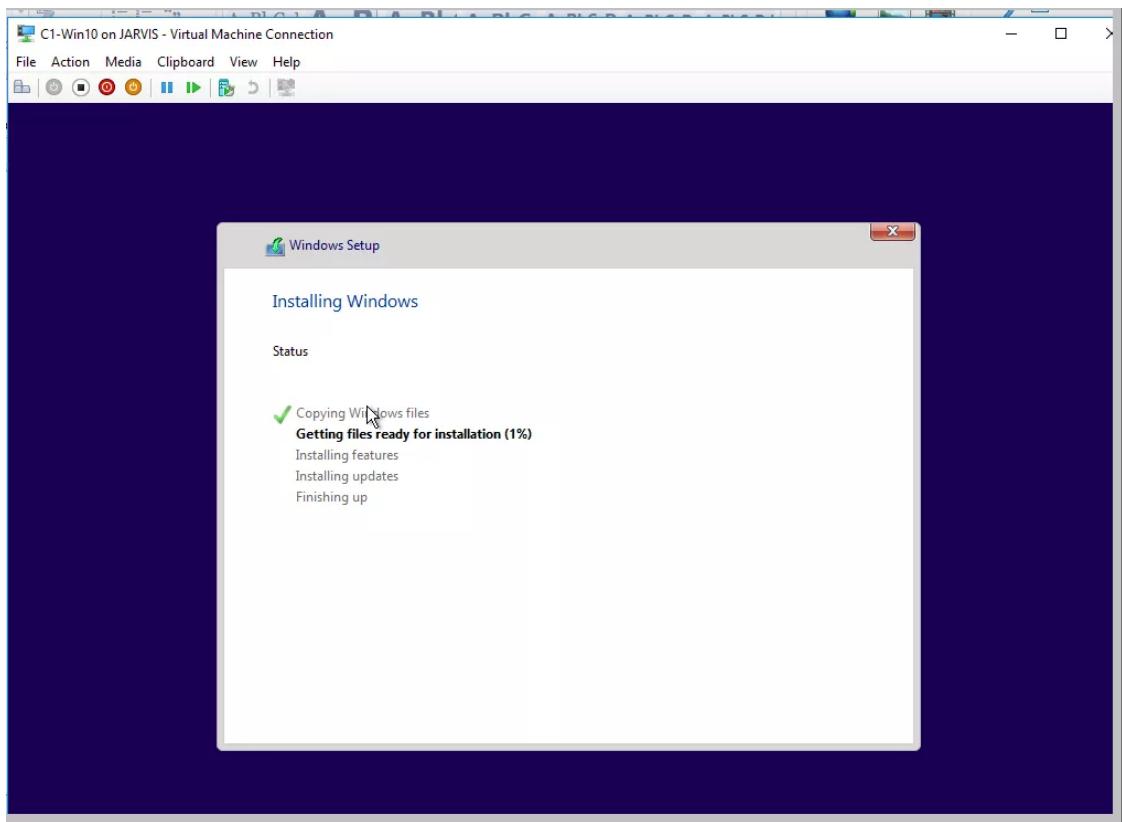
- Point to the downloaded Windows 10, ISO image and finish the configuration process



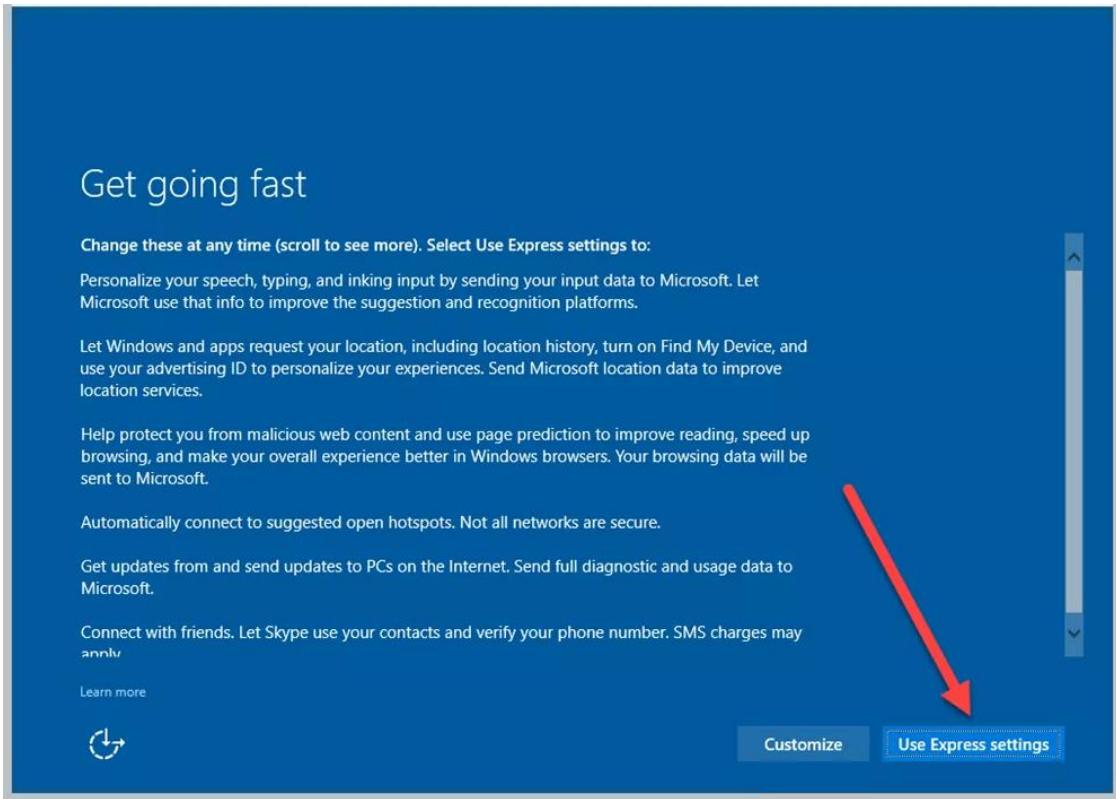
- Right click on C1-Win10 and click connect



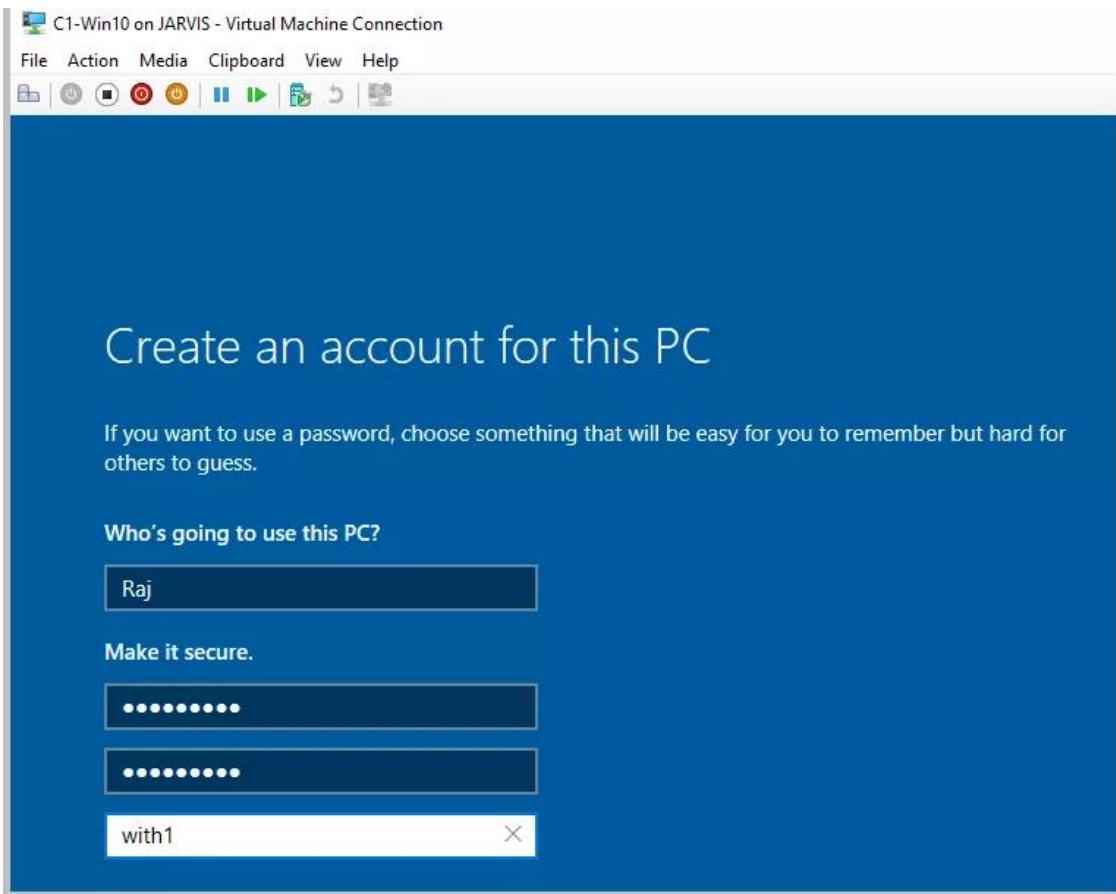
- Wait for the install to complete. it should take around 15 minutes to complete.



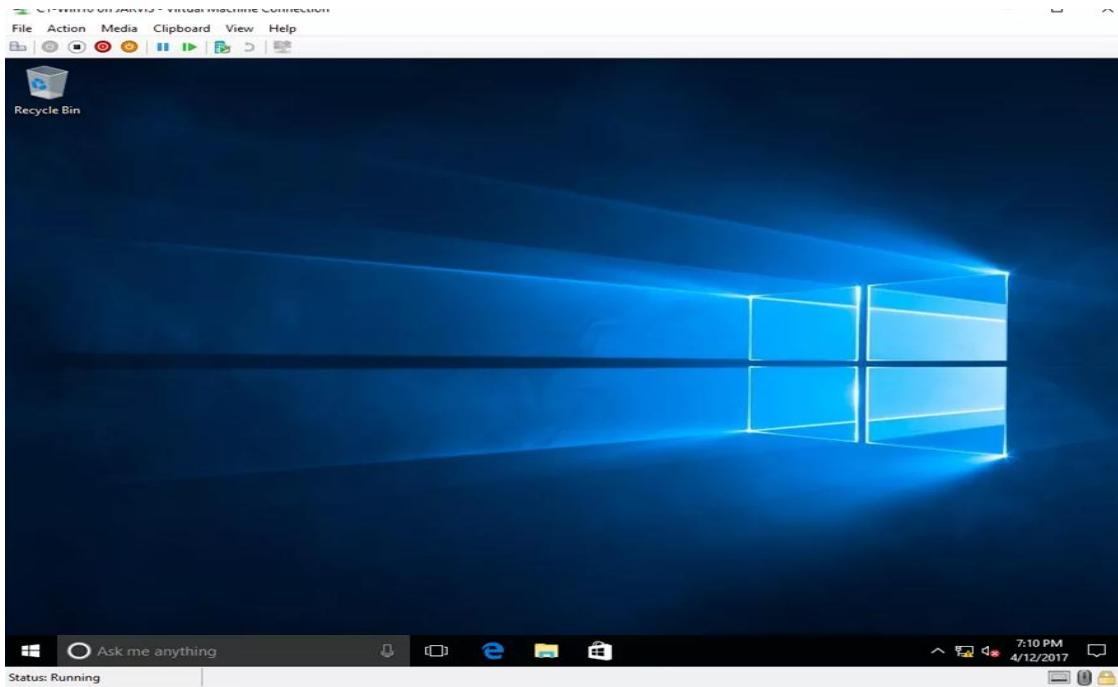
- Use Express settings



- Create an account and give it a strong password



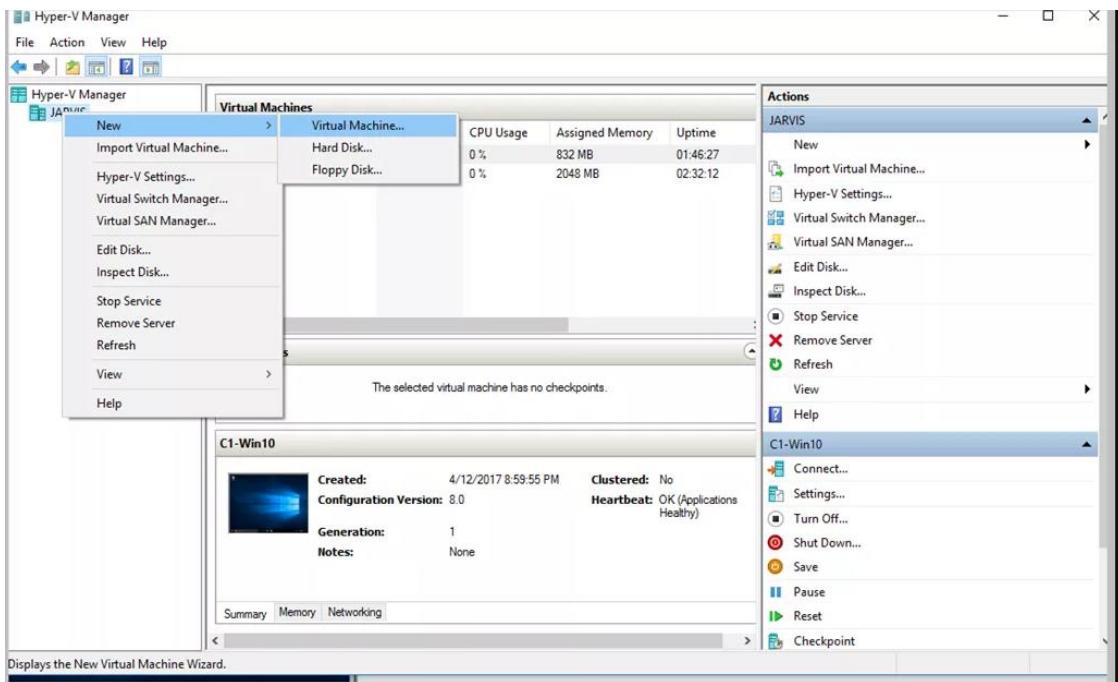
- Complete the process and reboot the machine



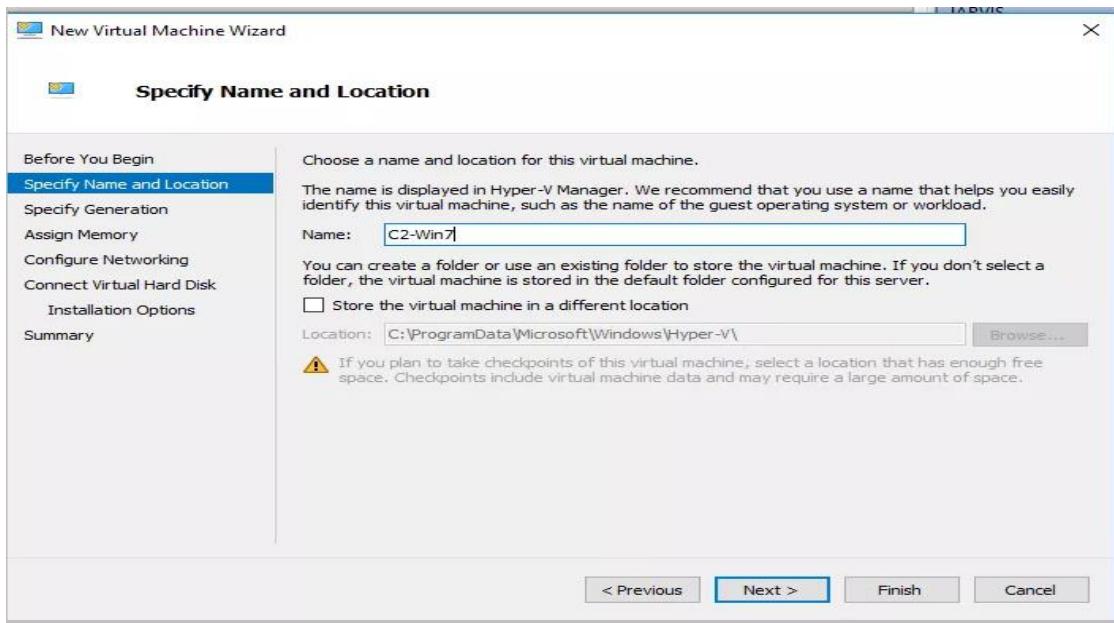
- Let's change the host name to **C1-Win10**. Restart the computer.

6. Installing Windows 7

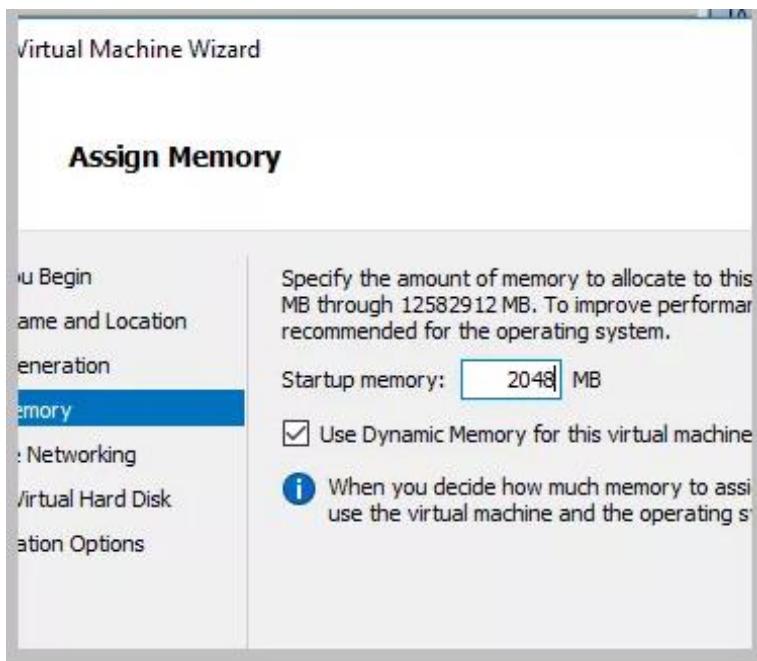
- Right click on "Jarvis" and create a virtual machine



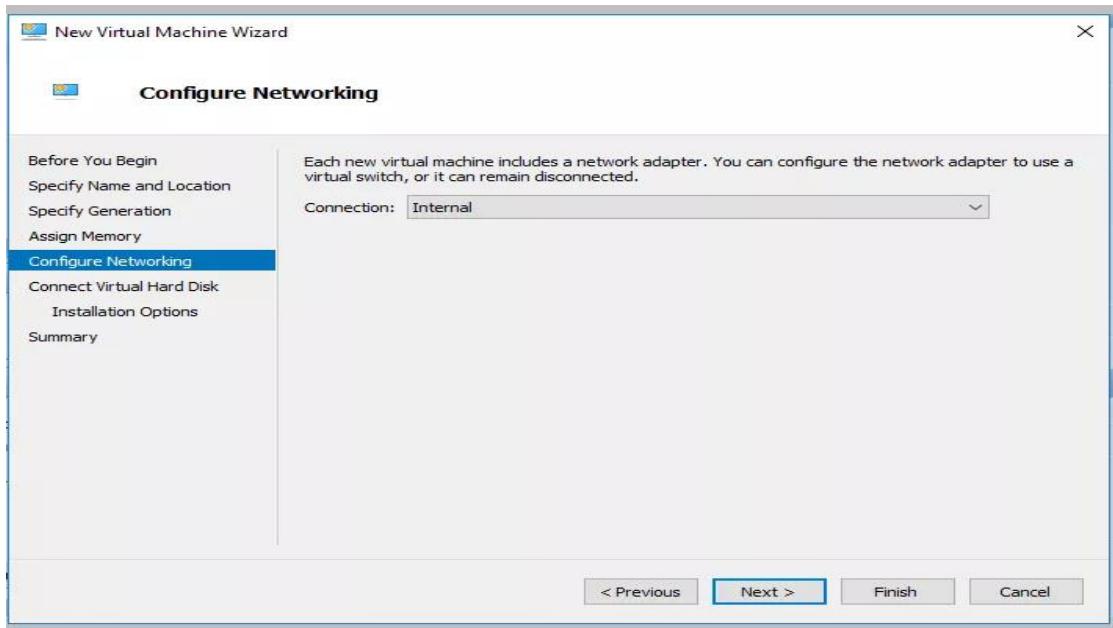
- Name the VM as C2-Win7, which denotes Client 2 - Windows 7 machine.



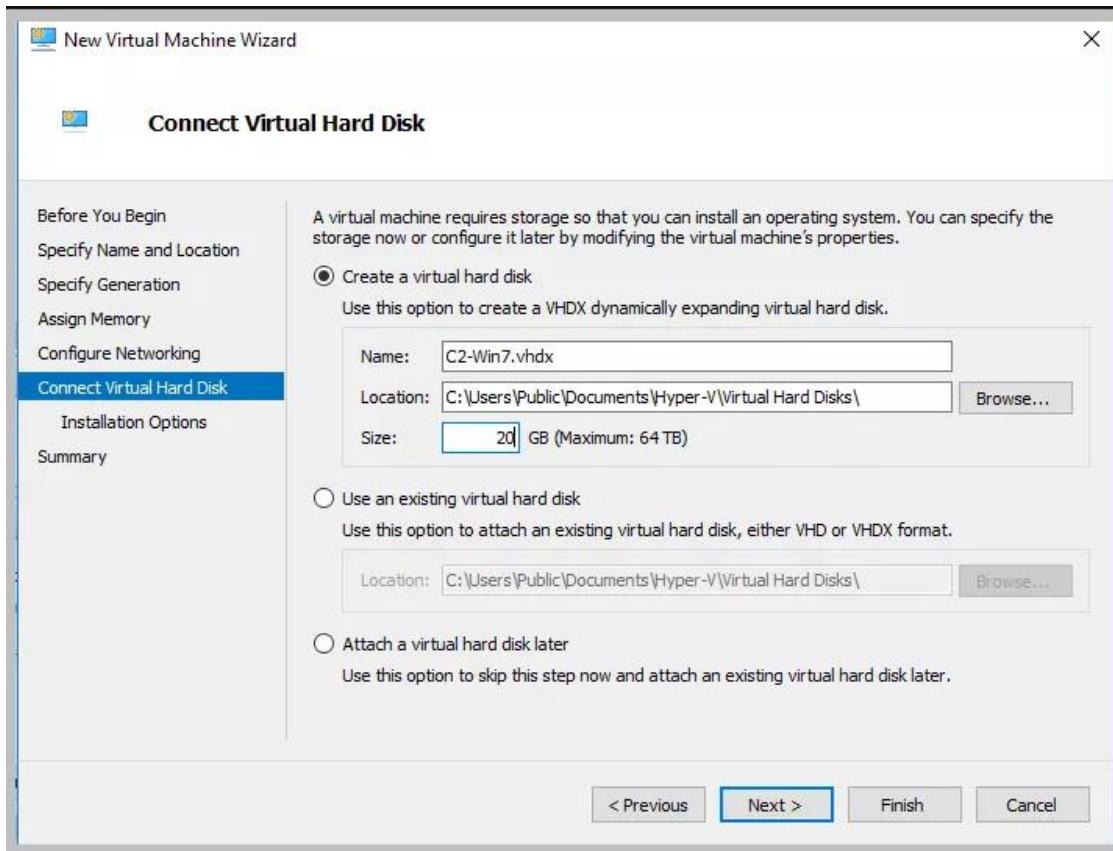
- Assign 2048 MB ram



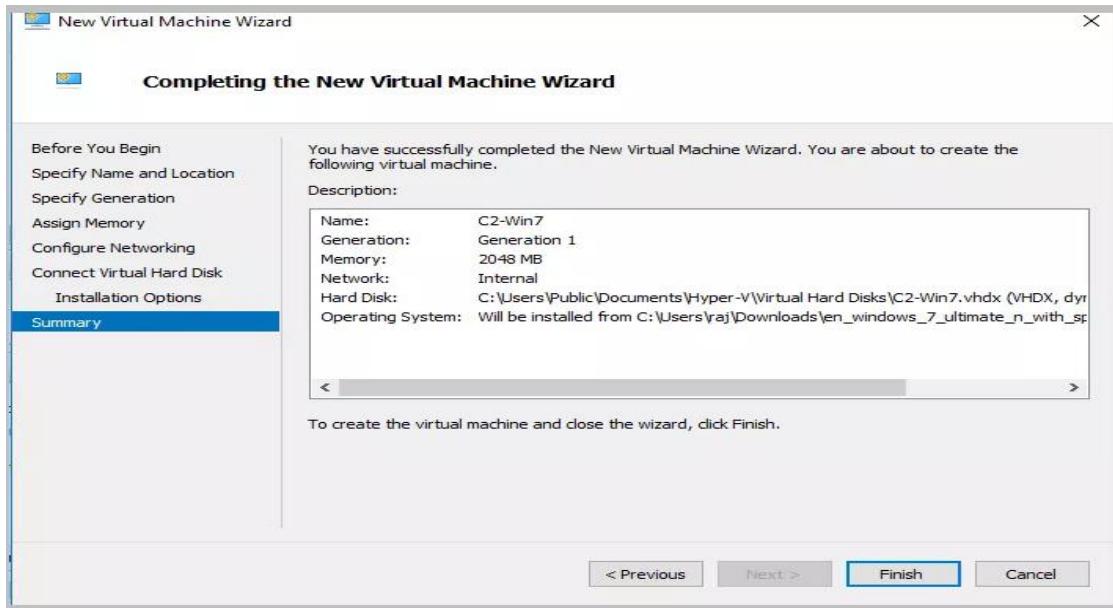
- Connect to “Internal” network



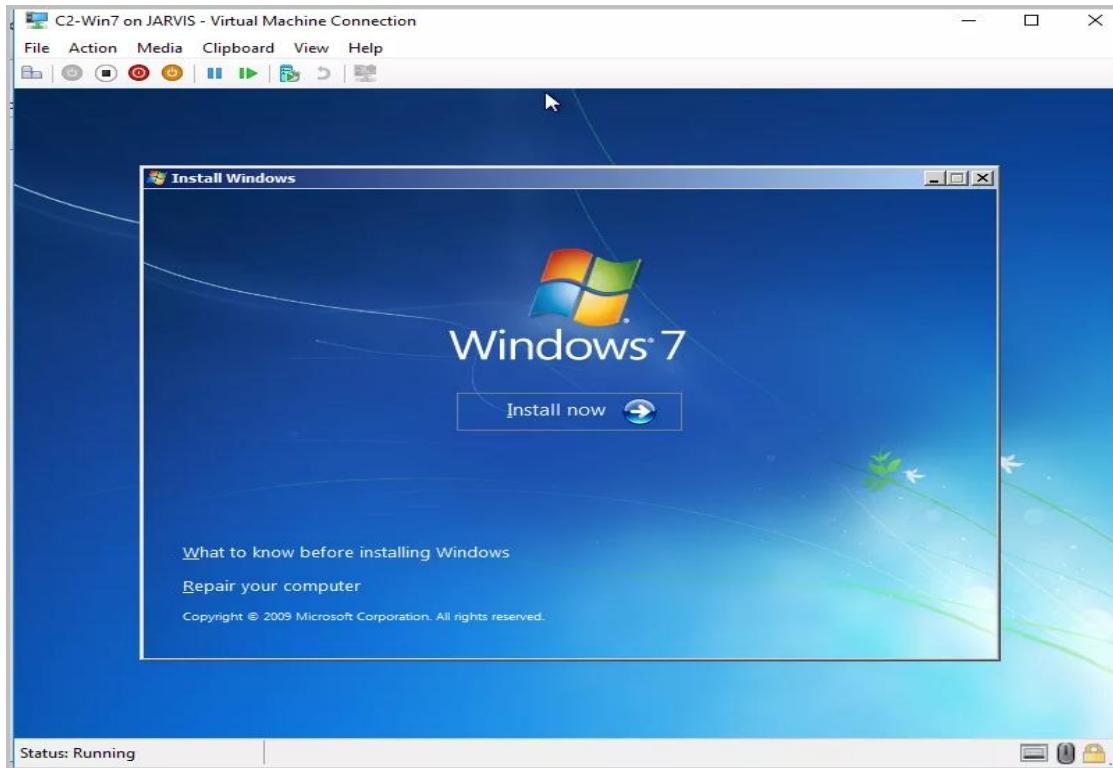
- Assign 20 GB for the virtual machine



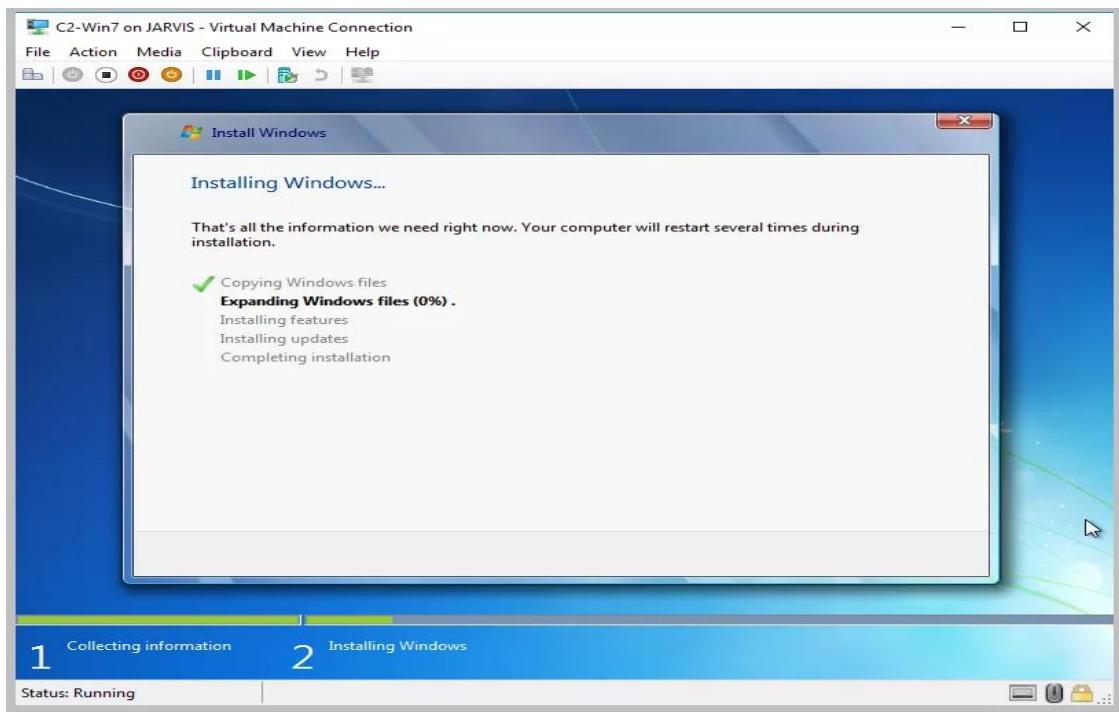
- Review and finish the setup process



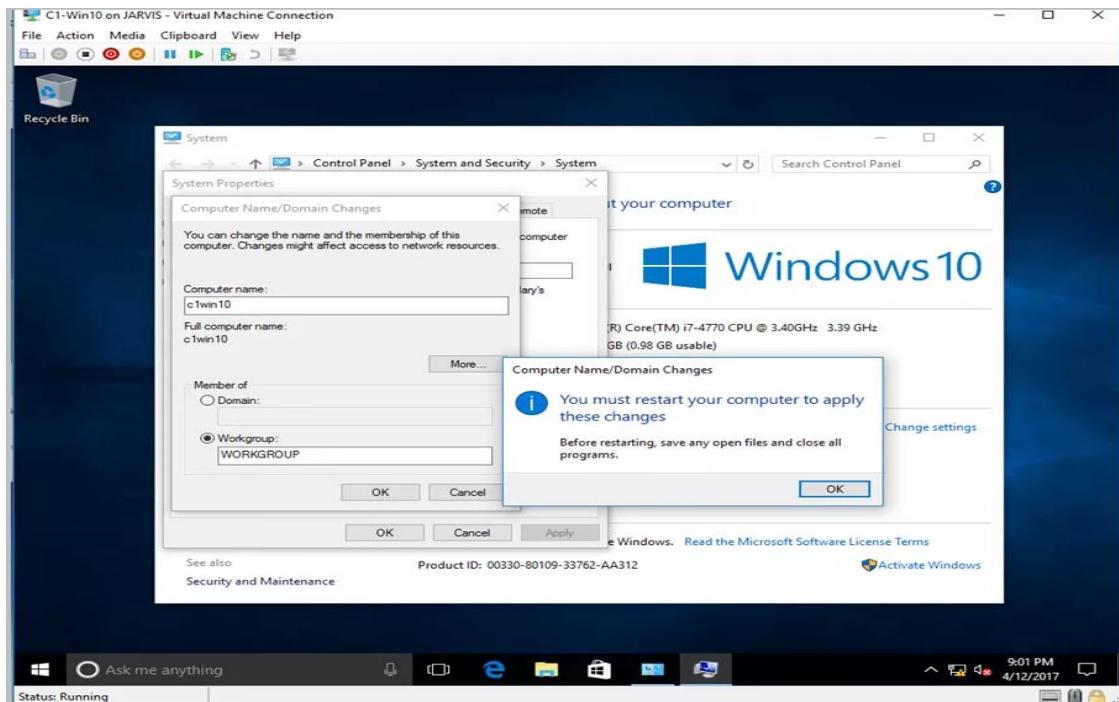
- Right click an C2-Win7, and connect to the VM, and click "Install Now"



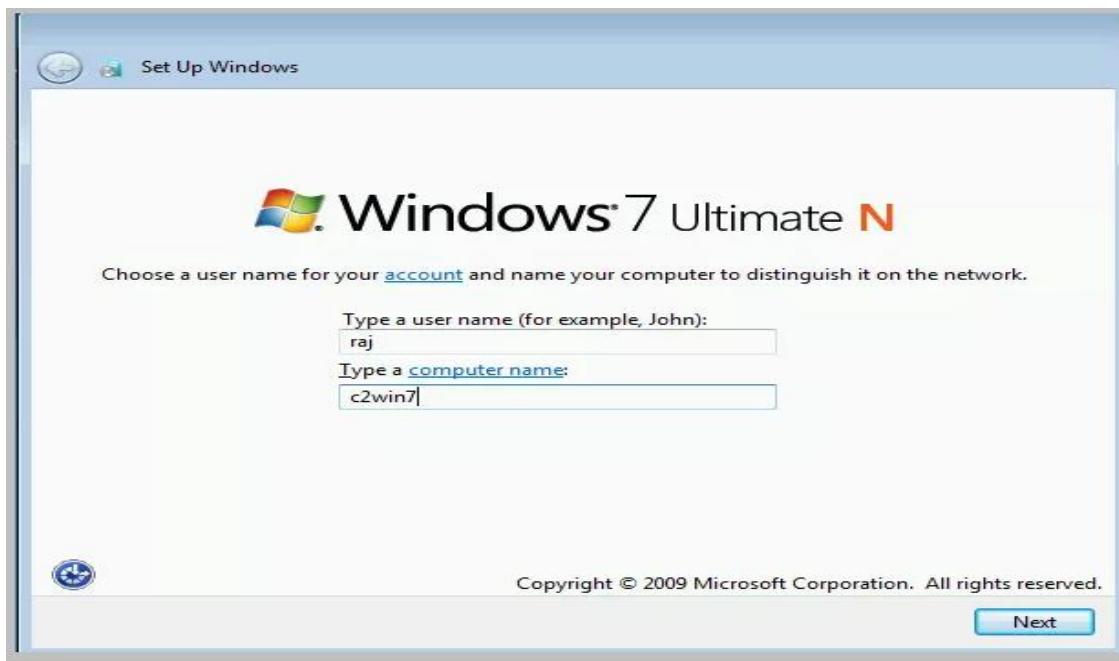
- Wait for the install process to complete



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



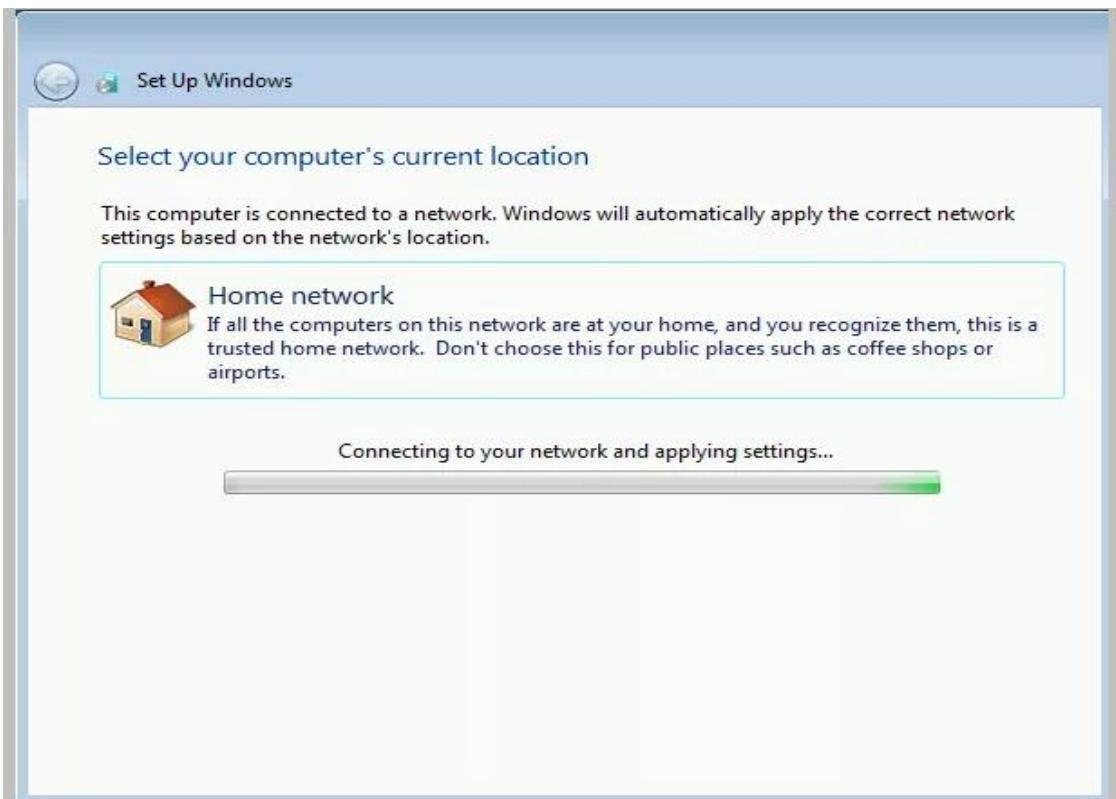
- Use a user name of your choice



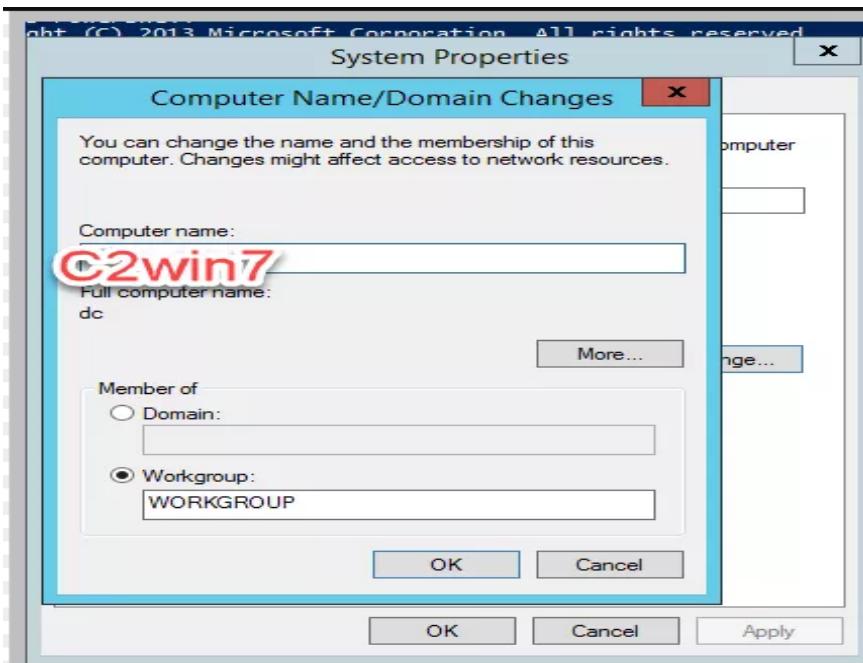
- Use recommended settings



- Choose "Home network"



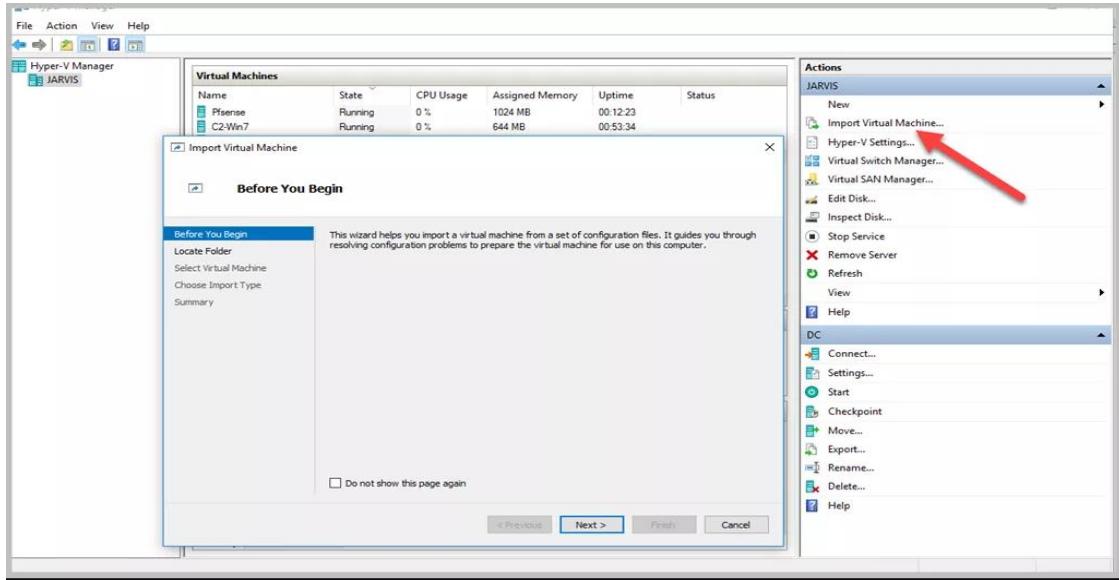
- After installation, change the computer name to C2win7



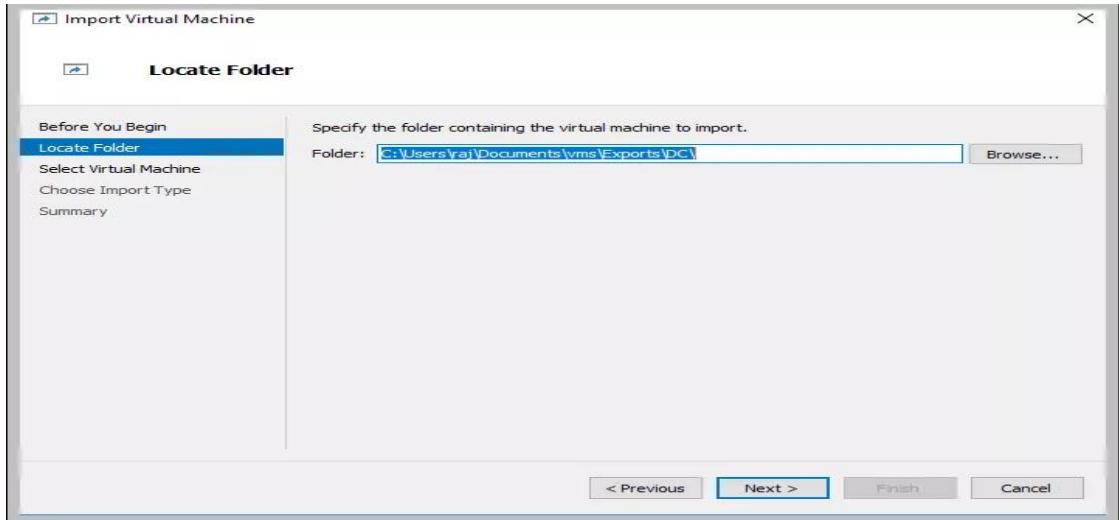
- Restart the machine to complete the process

7. File Server Installation – Windows 2012

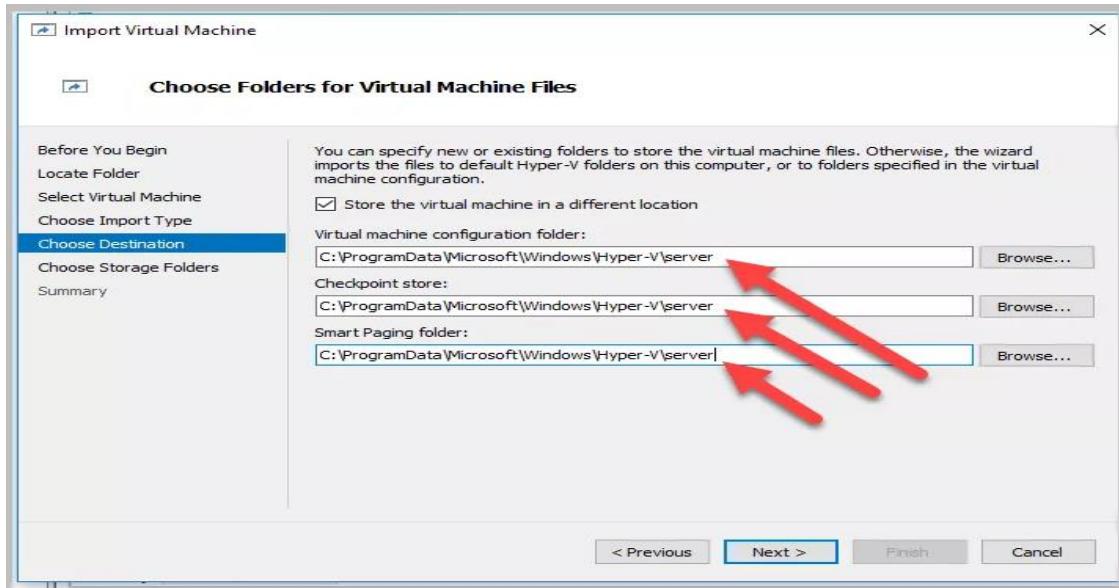
- Let's create another member server for our lab using the exported image in step 4 . Click "Import Virtual Machine".



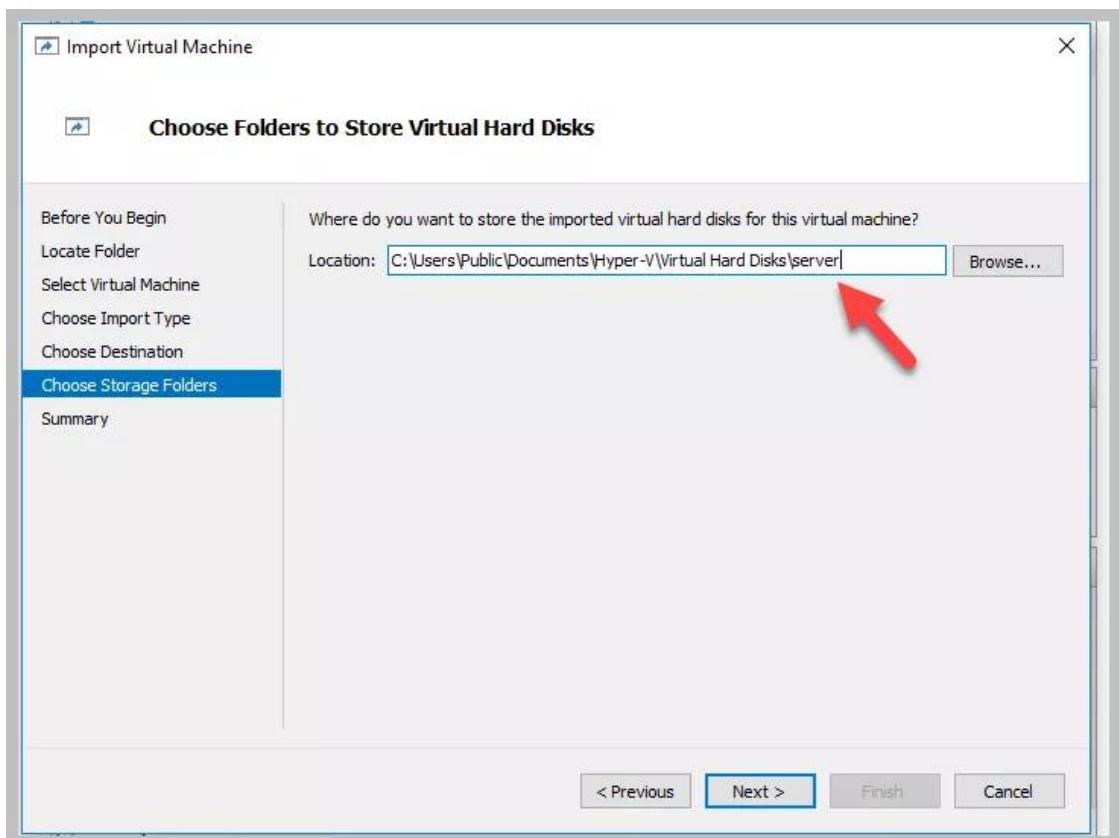
- Choose the file location of the source files and click "Next"



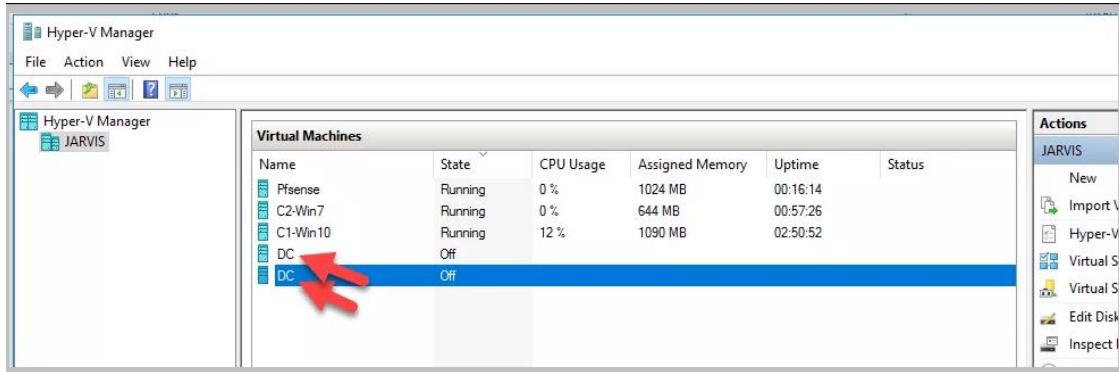
- Choose destination location. It is safe to add “server” or any other unique name to save the files in a separate folder



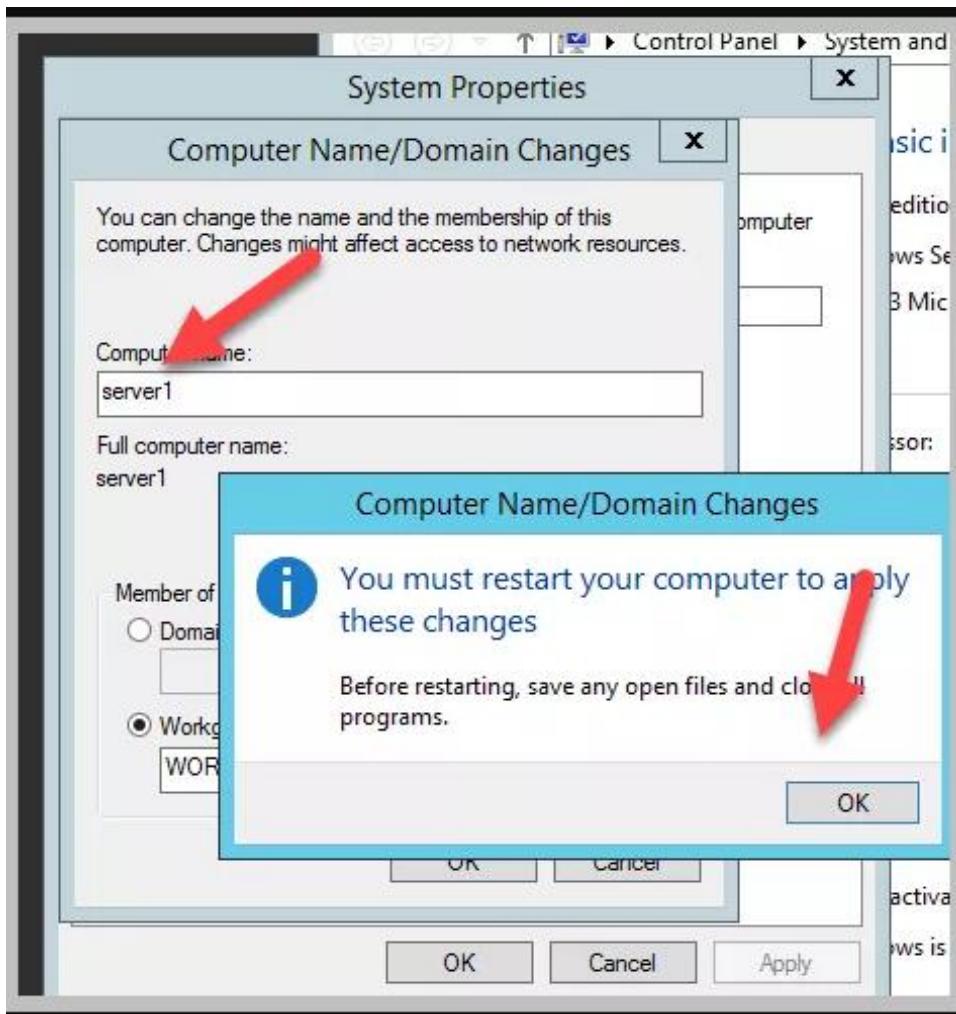
- Choose a folder for the hard disk



- Click “Next” and complete the process.



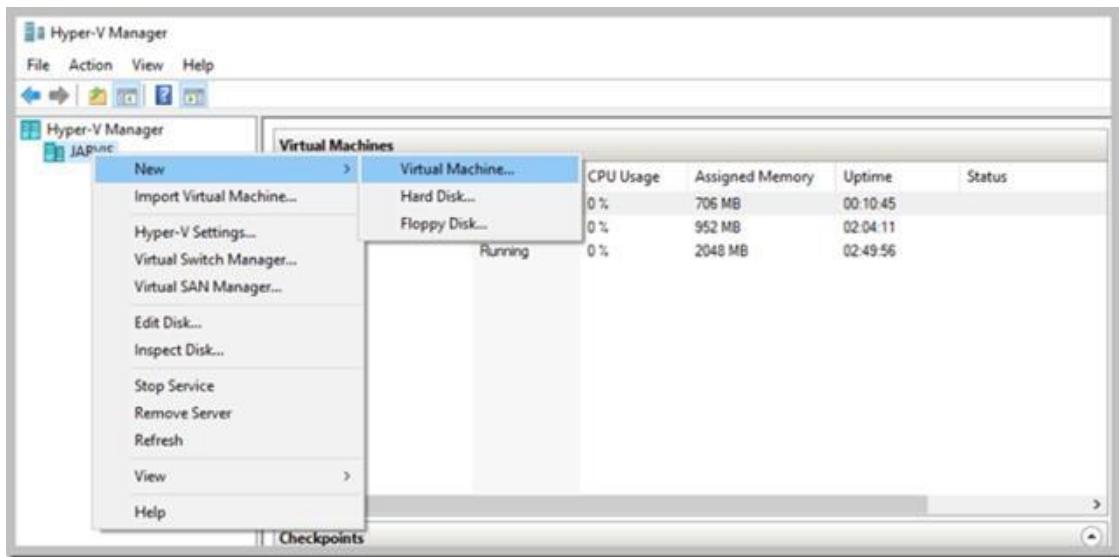
- Restart the server and rename the Computer name to “server1”



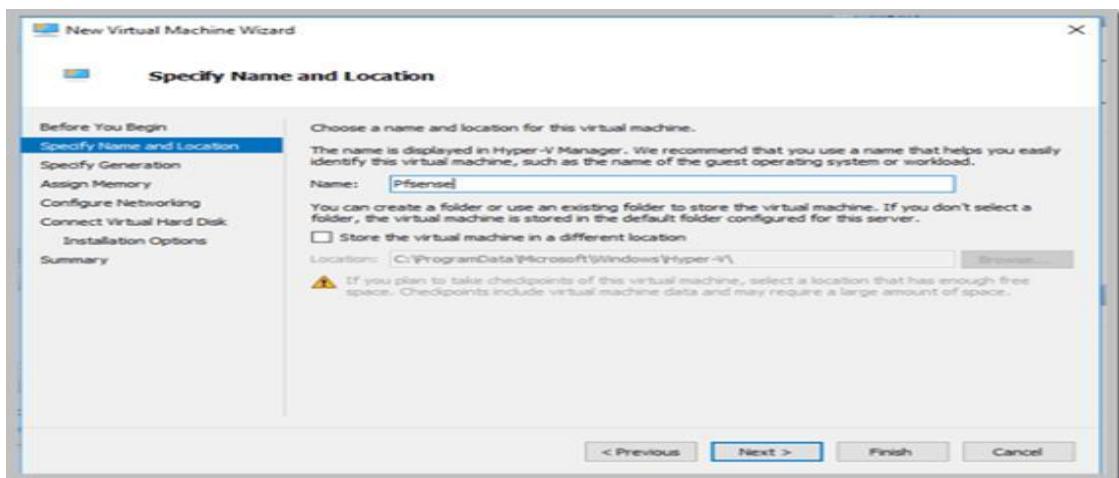
8. Installing Routing/Firewall - PFsense

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/>]

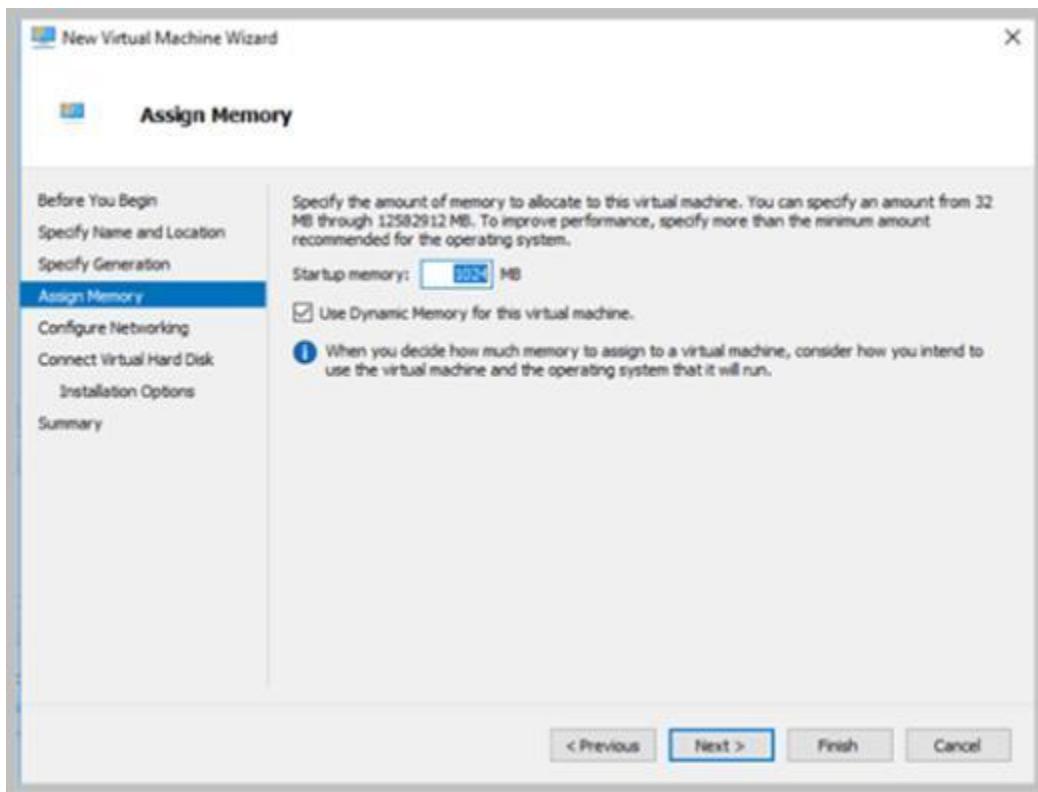
- Right click on “Jarvis” and create a new “Virtual Machine”



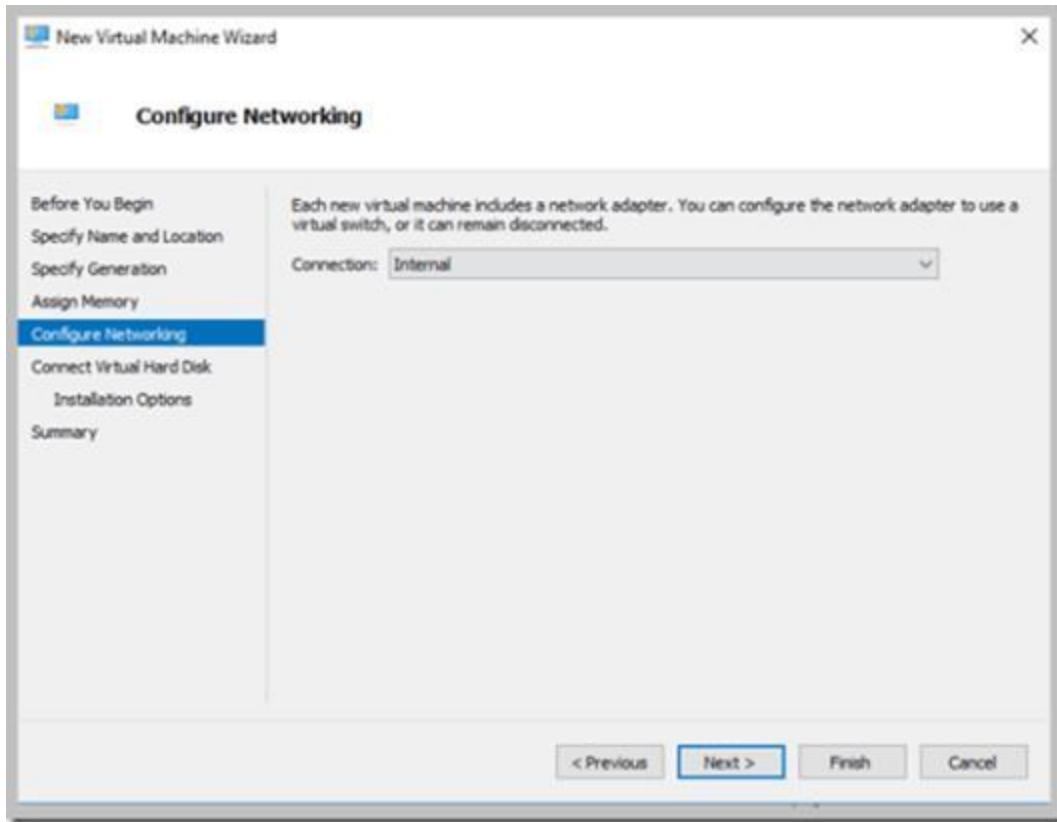
- Specify the name as “Pfsense”



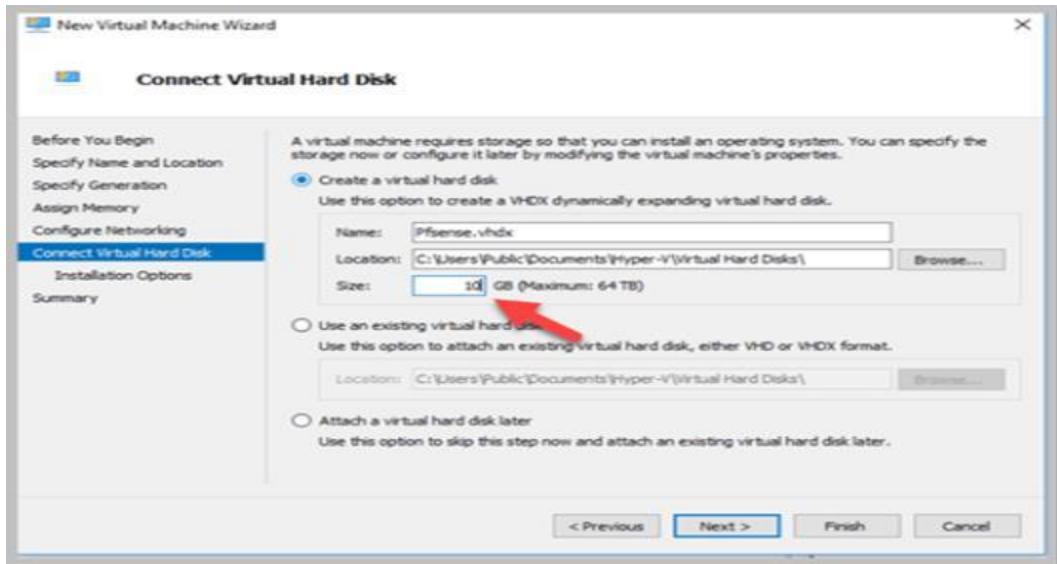
- Assign 1024 MB ram



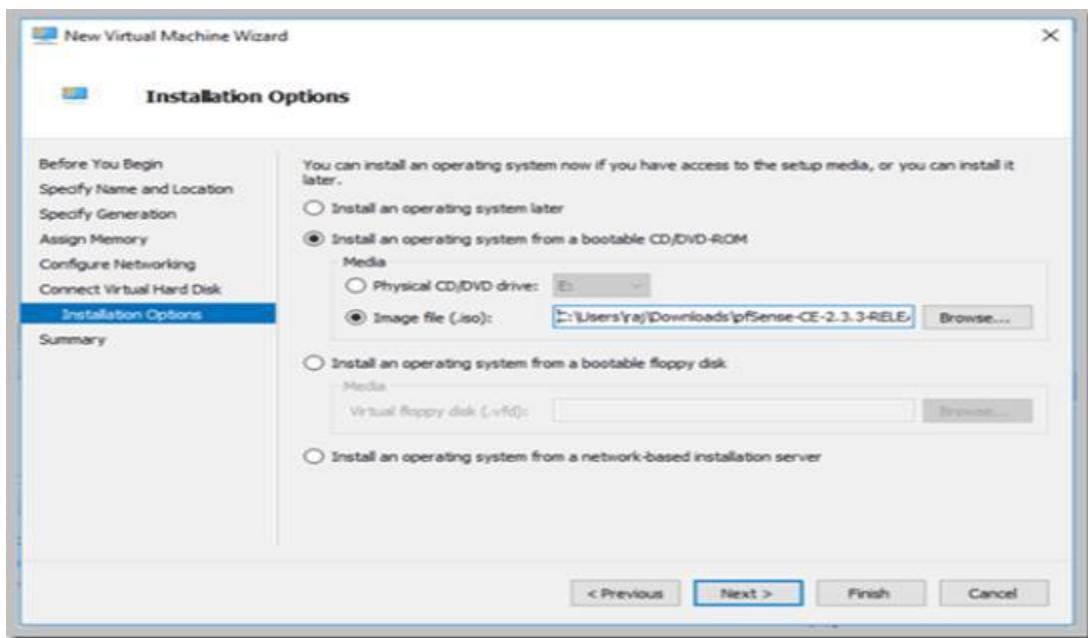
- Use the "Internal" for the network type



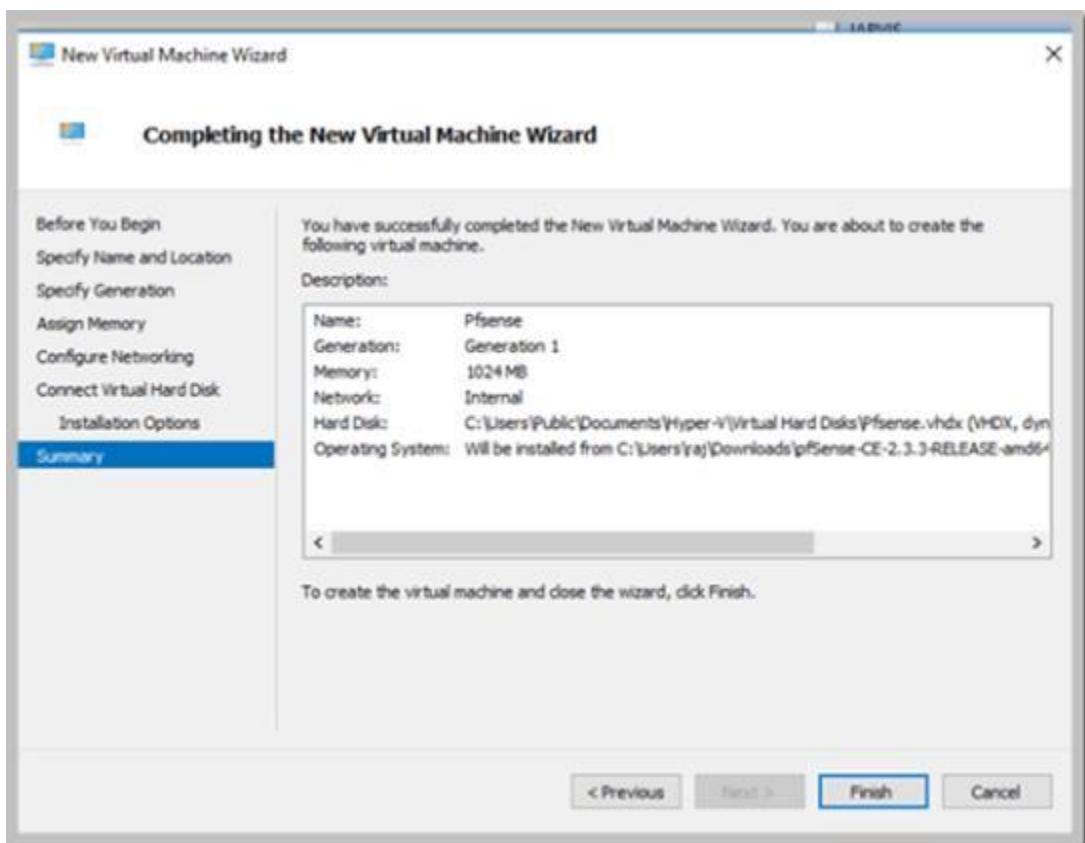
- 10 GB should be more than sufficient for PFsense for our lab environment



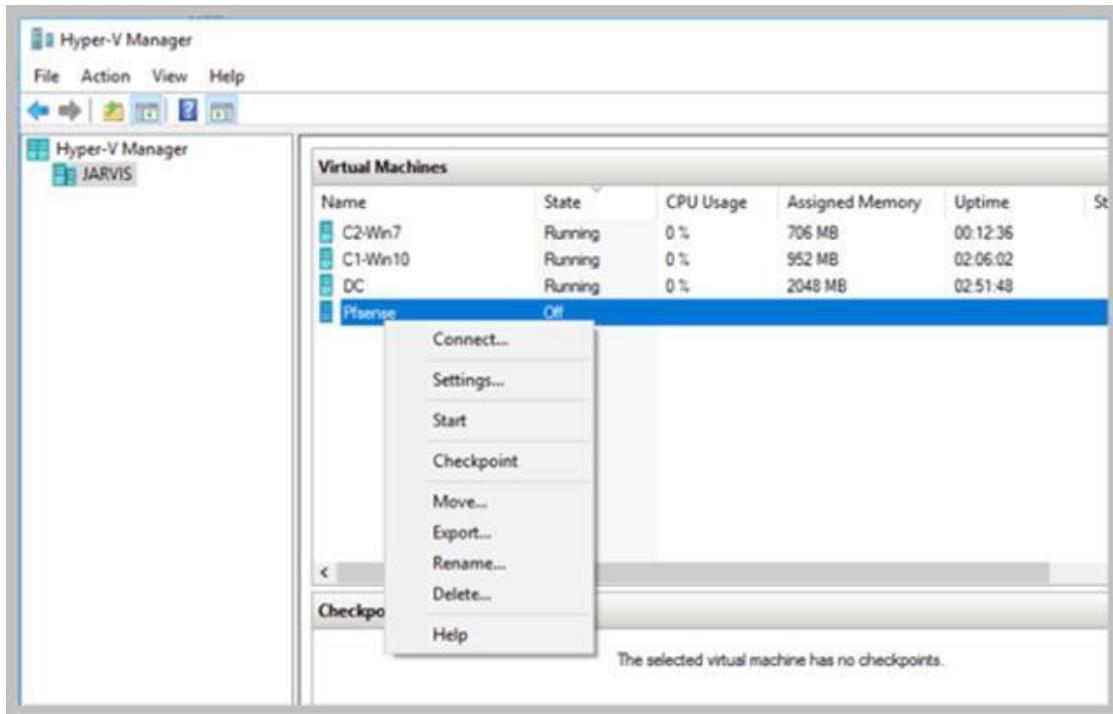
- Choose the ISO downloaded earlier



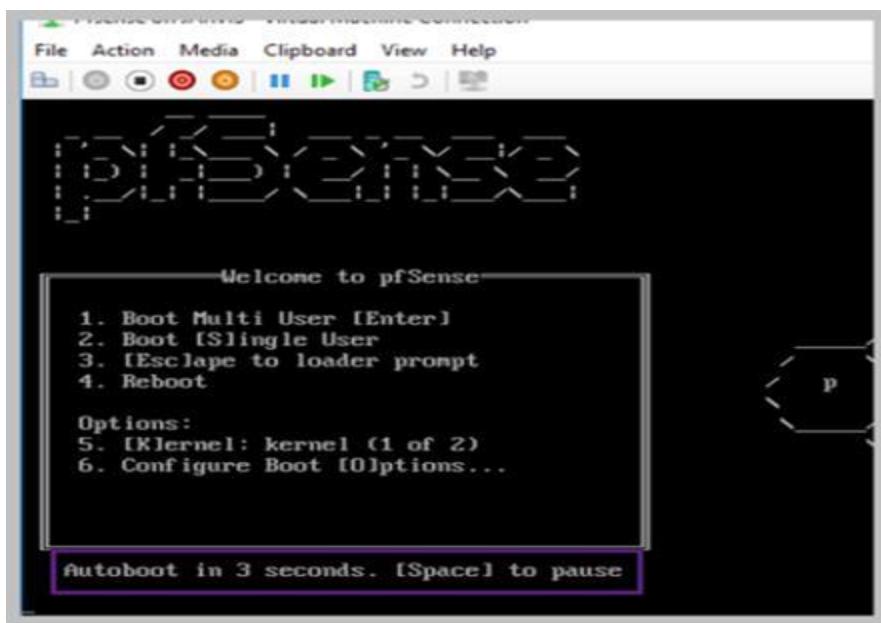
- Finish the setup dialog box



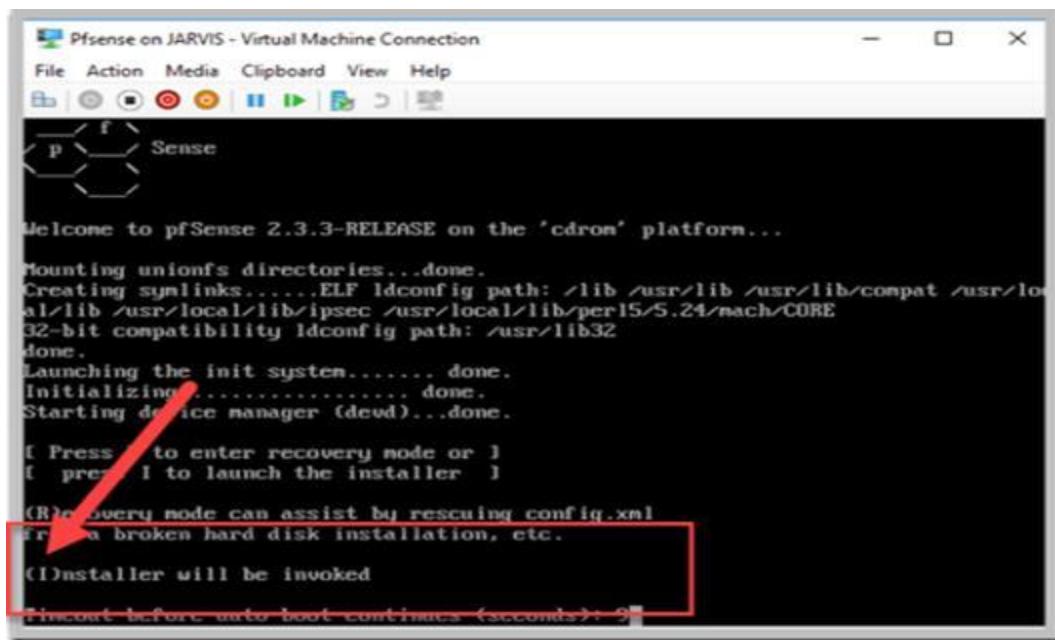
- Right click and connect to PFsense VM



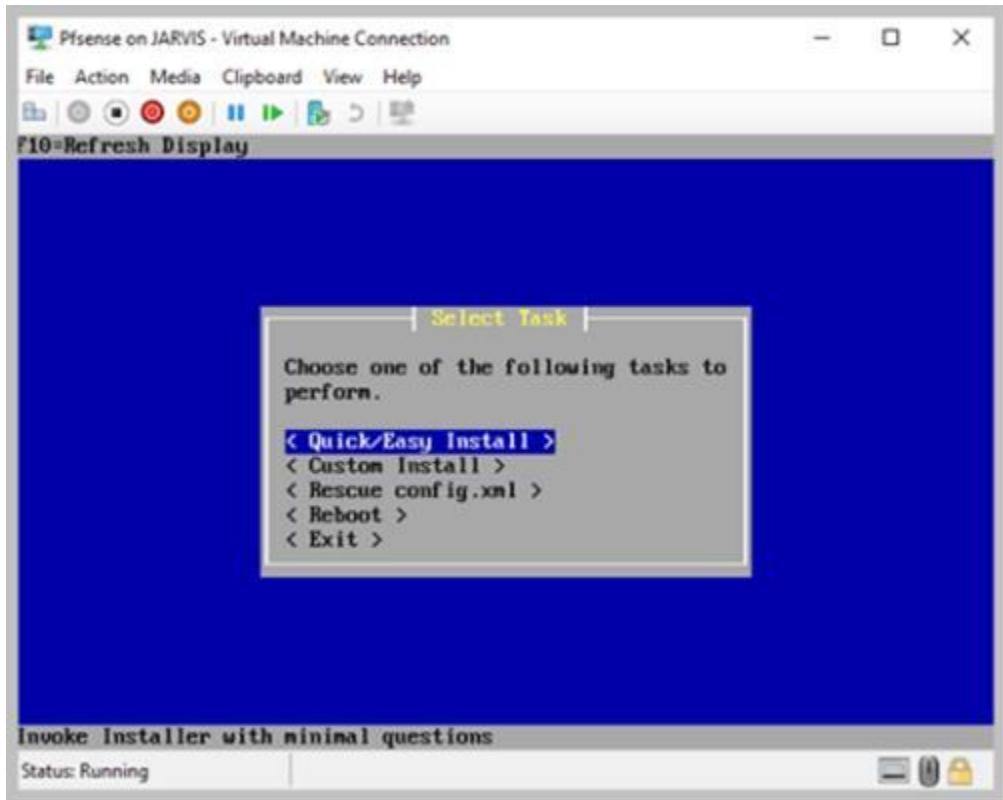
- Allow it to Autoboot



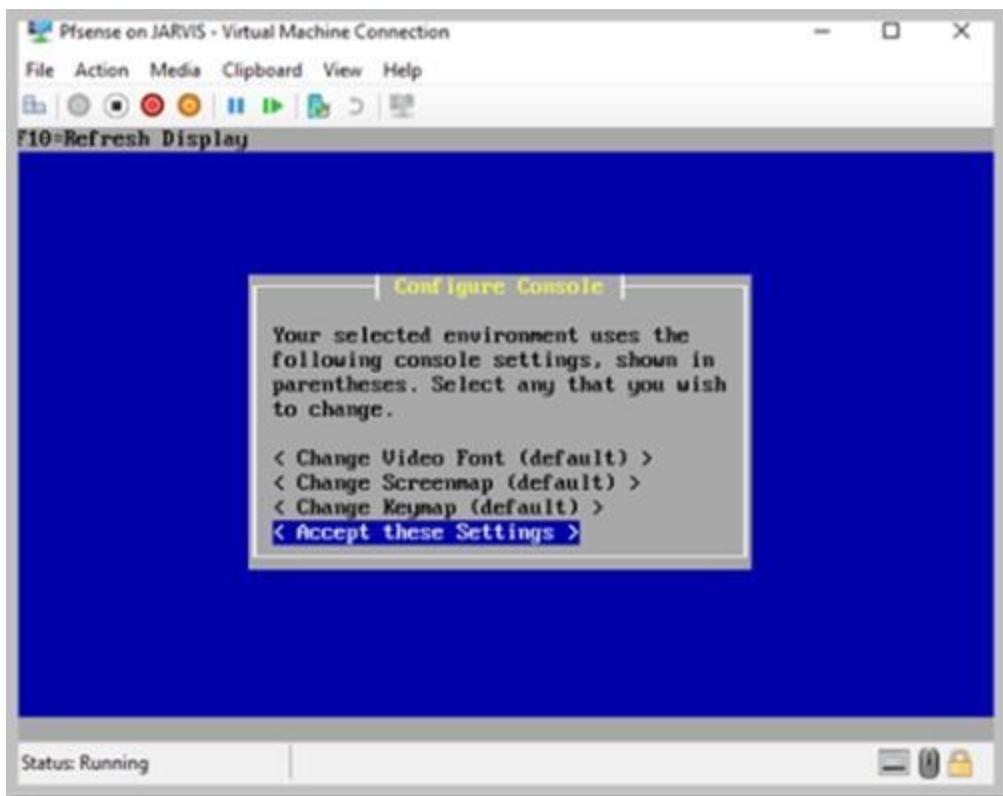
- Watch the messages carefully and **type "I" using the keyboard** to start installing



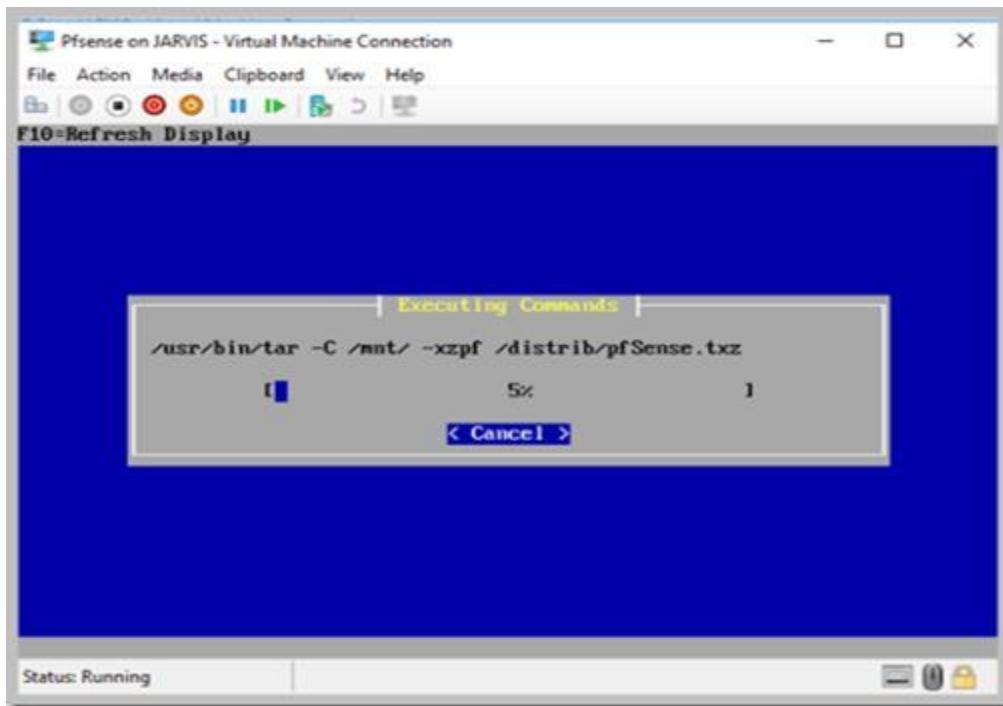
- Choose “Quick/Easy” install



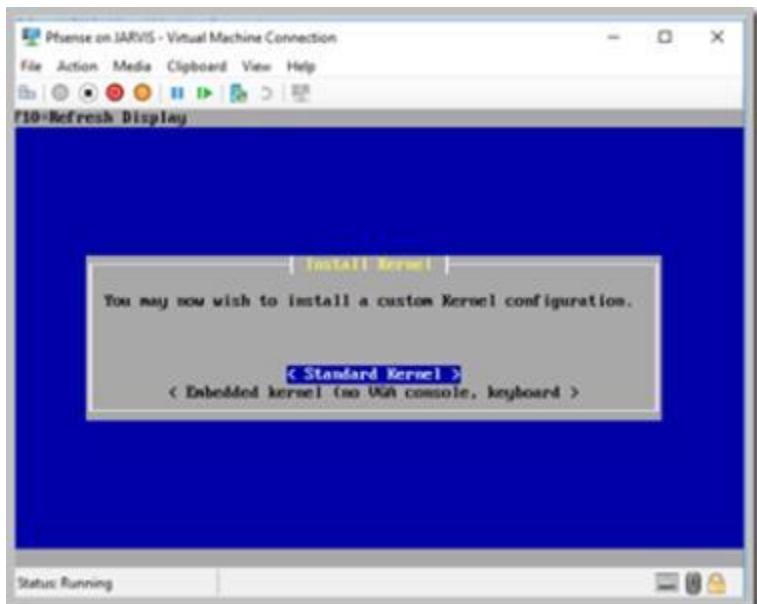
- Select “Accept these Settings”



- Wait for the install process to continue



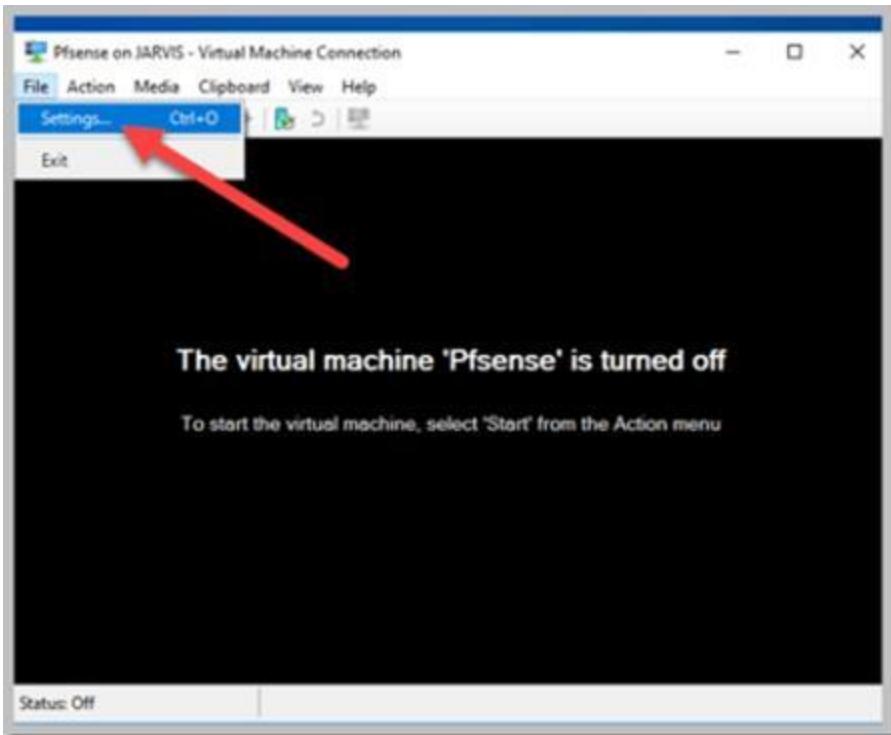
- Select “Standard Kernel”



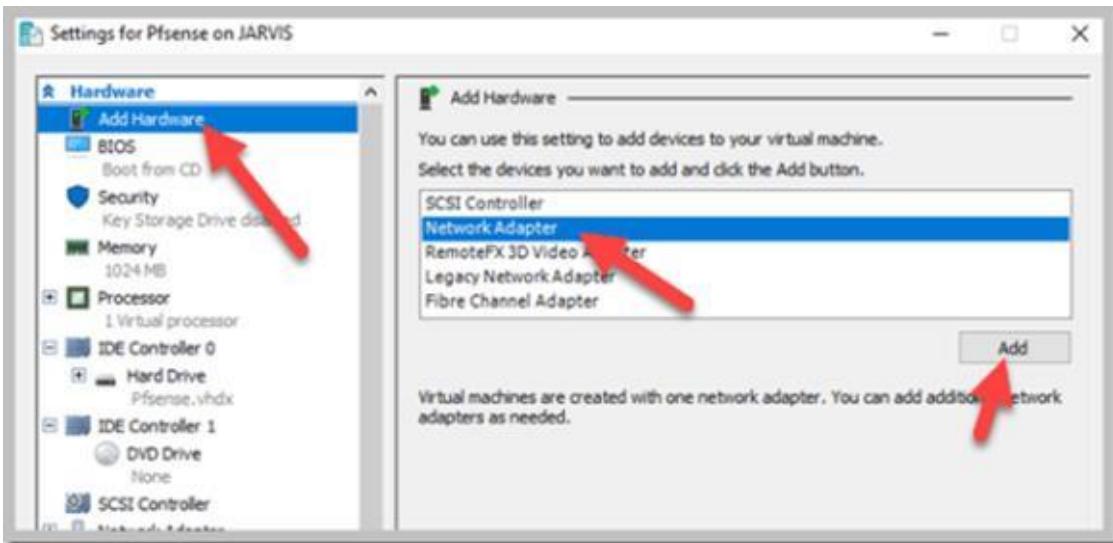
- Reboot the VM



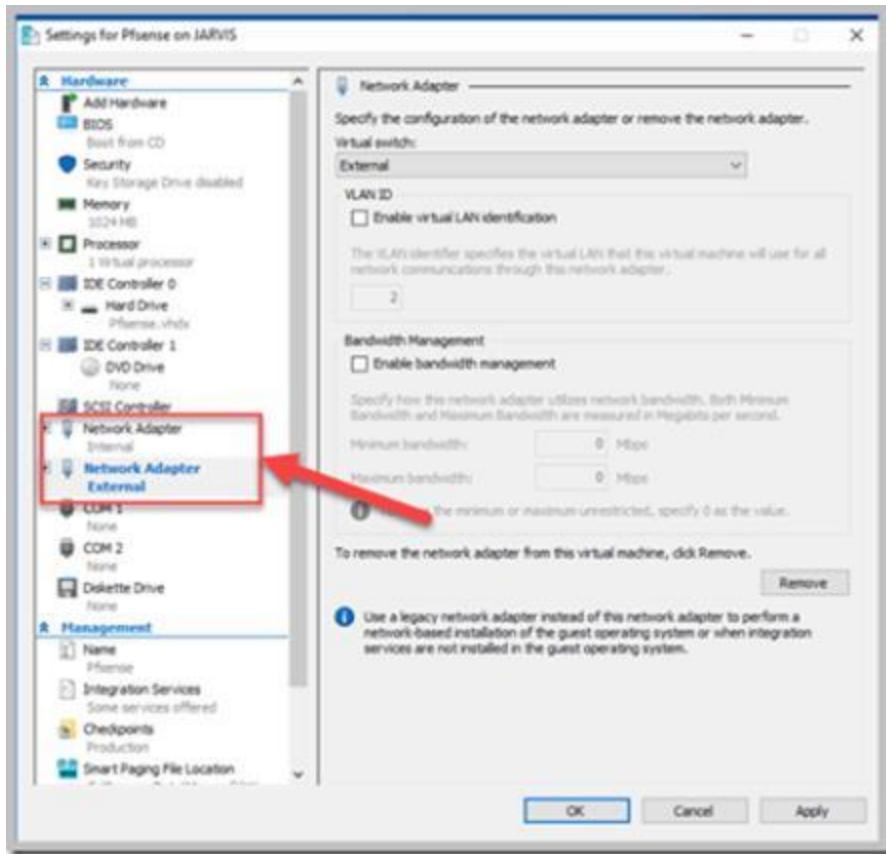
- Turn Off the VM to add additional switch. Choose settings.



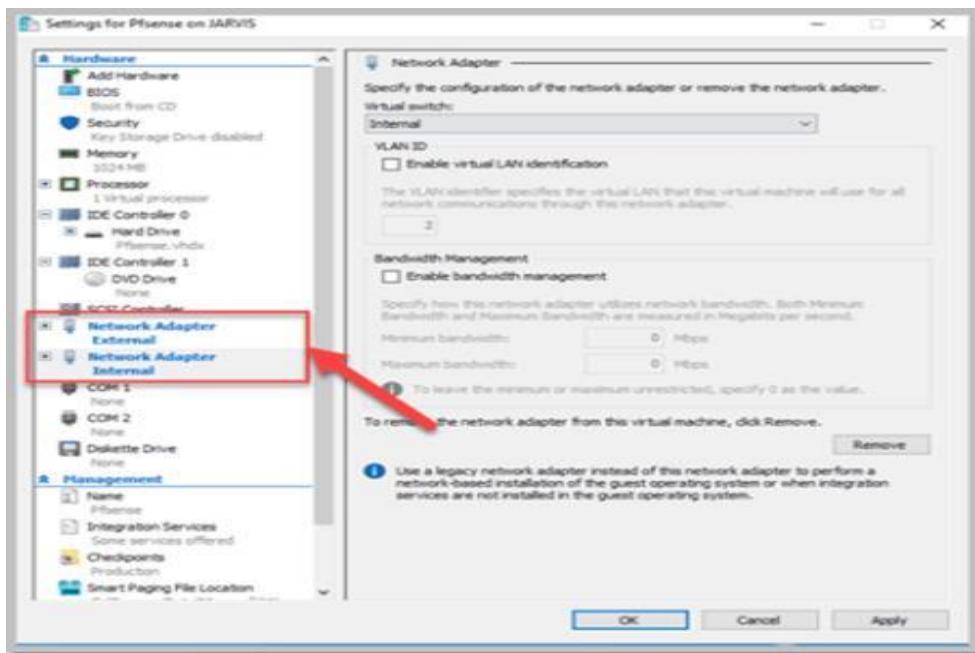
- Click "Add Hardware" and select "Network Adapter". Click Add



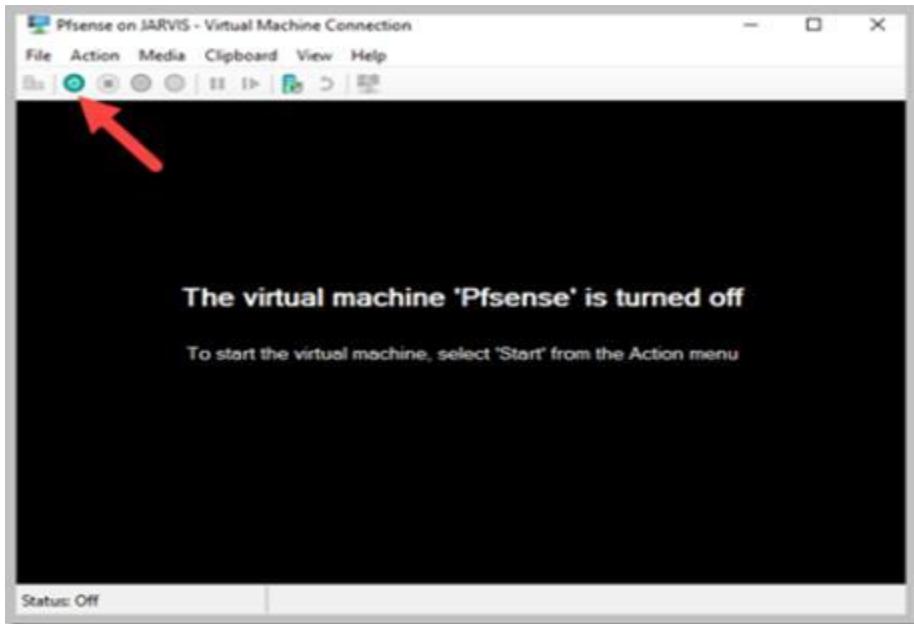
- Select the "Internal" adapter from left menu and choose "External" from the drop down. This is done to flip the order. ***"External" adapter should be the first network adapter followed by "Internal" adapter as shown in the subsequent diagram***



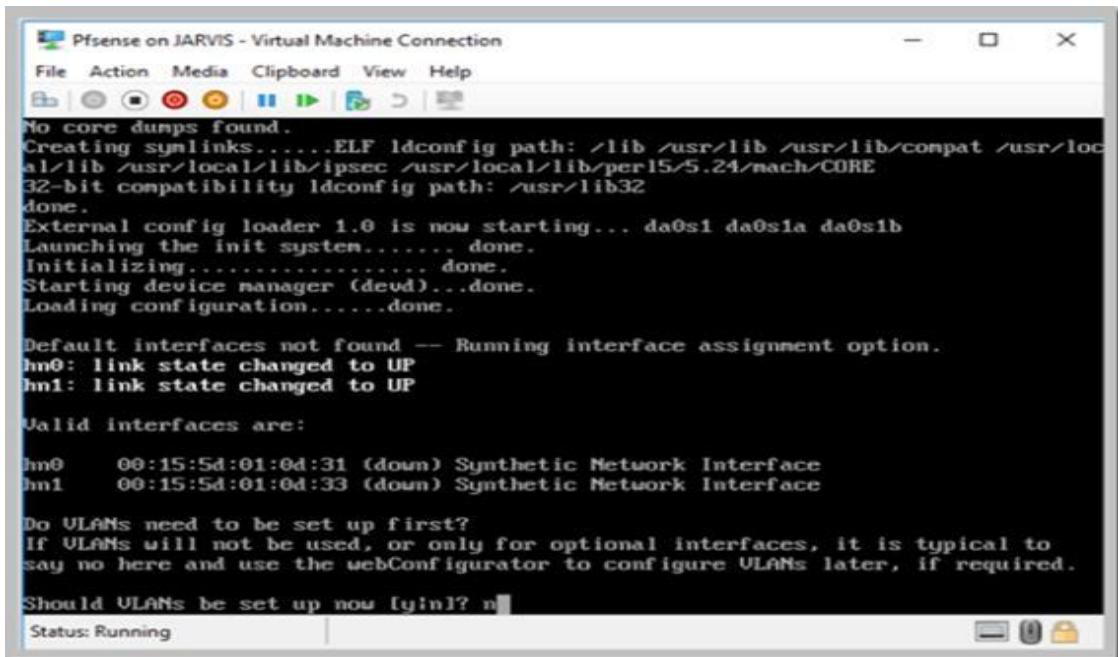
- Figure below shows the correct order of network adapters.



- Start the VM



- Choose "n" for VLAN setup



- Choose **hn0** for WAN interface

```
Initializing..... done.  
Starting device manager (devd)...done.  
Loading configuration.....done.  
  
Default interfaces not found -- Running interface assignment option.  
hn0: link state changed to UP  
hn1: link state changed to UP  
  
Valid interfaces are:  
  
hn0  00:15:5d:01:0d:31 (down) Synthetic Network Interface  
hn1  00:15:5d:01:0d:33 (down) Synthetic Network Interface  
  
Do VLANs need to be set up first?  
If VLANs will not be used, or only for optional interfaces, it is typical to  
say no here and use the webConfigurator to configure VLANs later, if required.  
  
Should VLANs be set up now [y/n]? n  
  
If the names of the interfaces are not known, auto-detection can  
be used instead. To use auto-detection, please disconnect all  
interfaces before pressing 'a' to begin the process.  
  
Enter the WAN interface name or 'a' for auto-detection  
(hn0 hn1 or a): hn0  
  
Status: Running
```

- Choose **hn1** for LAN interface

```
Default interfaces not found -- Running interface assignment option.  
hn0: link state changed to UP  
hn1: link state changed to UP  
  
Valid interfaces are:  
  
hn0  00:15:5d:01:0d:31 (down) Synthetic Network Interface  
hn1  00:15:5d:01:0d:33 (down) Synthetic Network Interface  
  
Do VLANs need to be set up first?  
If VLANs will not be used, or only for optional interfaces, it is typical to  
say no here and use the webConfigurator to configure VLANs later, if required.  
  
Should VLANs be set up now [y/n]? n  
  
If the names of the interfaces are not known, auto-detection can  
be used instead. To use auto-detection, please disconnect all  
interfaces before pressing 'a' to begin the process.  
  
Enter the WAN interface name or 'a' for auto-detection  
(hn0 hn1 or a): hn0  
  
Enter the LAN interface name or 'a' for auto-detection  
NOTE: this enables full Firewalling/MT mode.  
(hn1 a or nothing if finished): hn1  
  
Status: Running
```

- Choose "y" to complete the setup process

```
Pfsense on JARVIS - Virtual Machine Connection
File Action Media Clipboard View Help
File | Open | Save | Print | Copy | Paste | Find | Replace | Exit
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y/n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(hm0 hm1 or a): hm0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/MAT mode.
(hm1 a or nothing if finished): hm1

Enter the Optional 1 interface name or 'a' for auto-detection
(a or nothing if finished):

The interfaces will be assigned as follows:

WAN -> hm0
LAN -> hm1

Do you want to proceed [y/n]? y
Status: Running
```

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

```
Pfsense on JARVIS - Virtual Machine Connection
File Action Media Clipboard View Help
File | Open | Save | Print | Copy | Paste | Find | Replace | Exit
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense (pfSense) 2.3.3-RELEASE amd64 Thu Feb 16 06:59:53 CST 2017
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

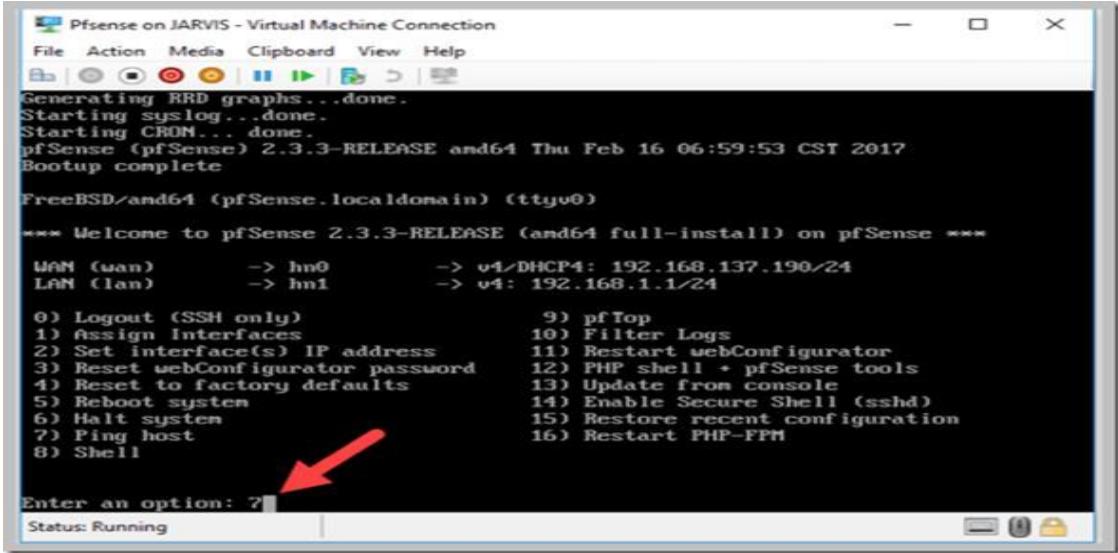
*** Welcome to pfSense 2.3.3-RELEASE (amd64 full-install) on pfSense ***

WAN (wan)      -> hm0          -> v4/DHCP4: 192.168.137.190/24
LAN (lan)      -> hm1          -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 7
Status: Running
```

- Choose option 7 to check internet connectivity



```
Pfsense on JARVIS - Virtual Machine Connection
File Action Media Clipboard View Help
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense (pfSense) 2.3.3-RELEASE amd64 Thu Feb 16 06:59:53 CST 2017
Bootstrap complete

FreeBSD/amd64 (pfSense.localdomain) (ttyu0)

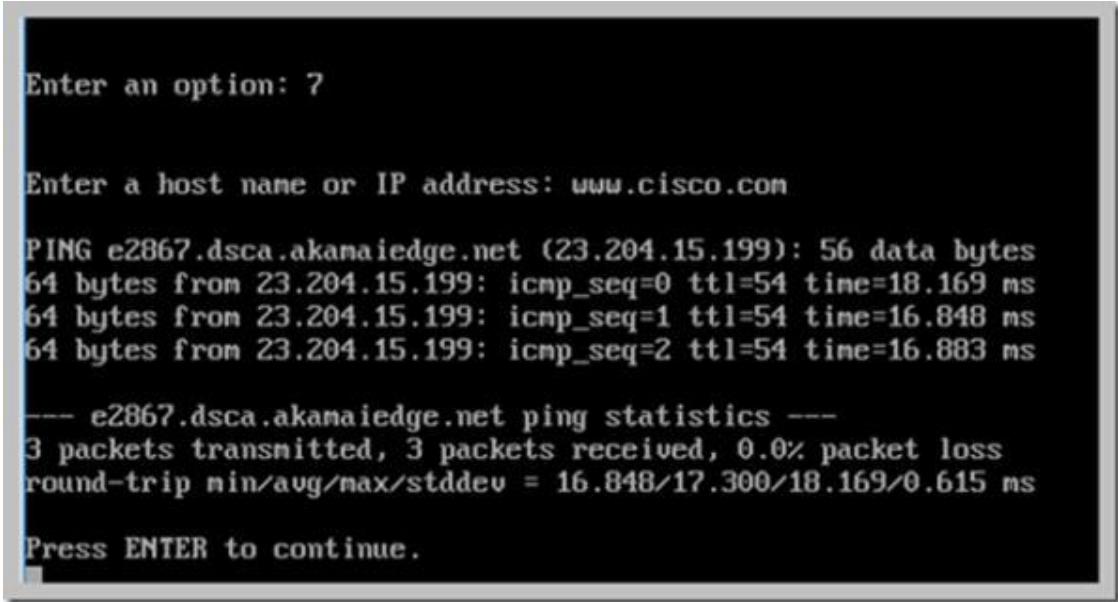
*** Welcome to pfSense 2.3.3-RELEASE (amd64 full-install) on pfSense ***

WAN (wan)      -> hm0          -> v4/DHCP4: 192.168.137.190/24
LAN (lan)      -> hm1          -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces           10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: ?
```

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



```
Enter an option: 7

Enter a host name or IP address: www.cisco.com

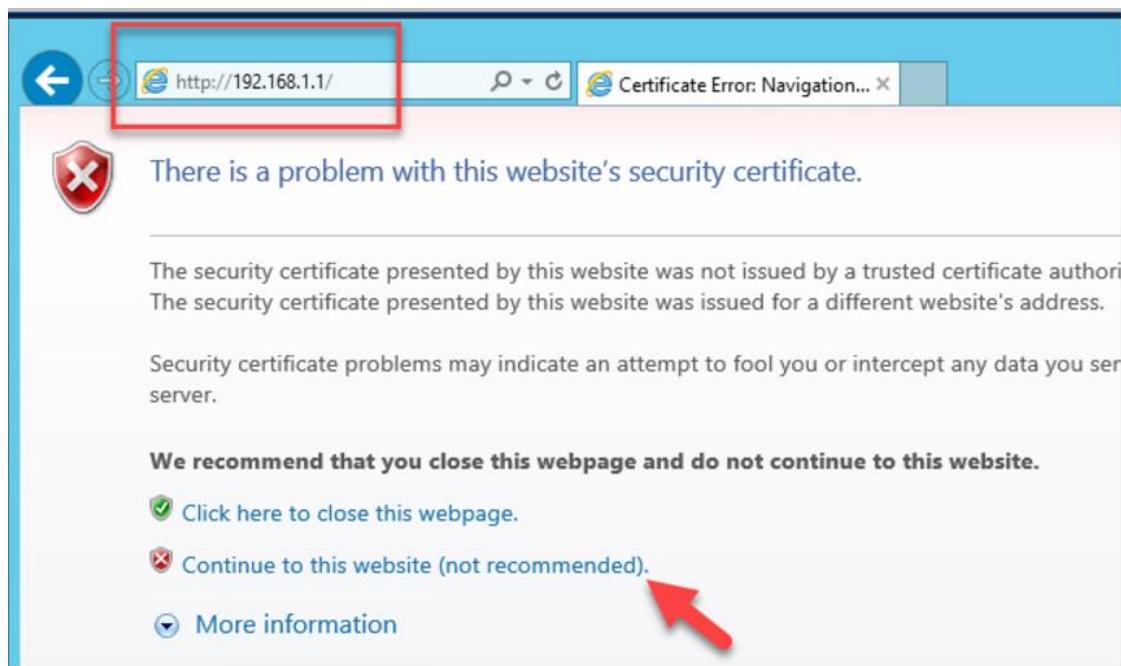
PING e2867.dsca.akamaiedge.net (23.204.15.199): 56 data bytes
64 bytes from 23.204.15.199: icmp_seq=0 ttl=54 time=18.169 ms
64 bytes from 23.204.15.199: icmp_seq=1 ttl=54 time=16.848 ms
64 bytes from 23.204.15.199: icmp_seq=2 ttl=54 time=16.883 ms

--- e2867.dsca.akamaiedge.net ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 16.848/17.300/18.169/0.615 ms

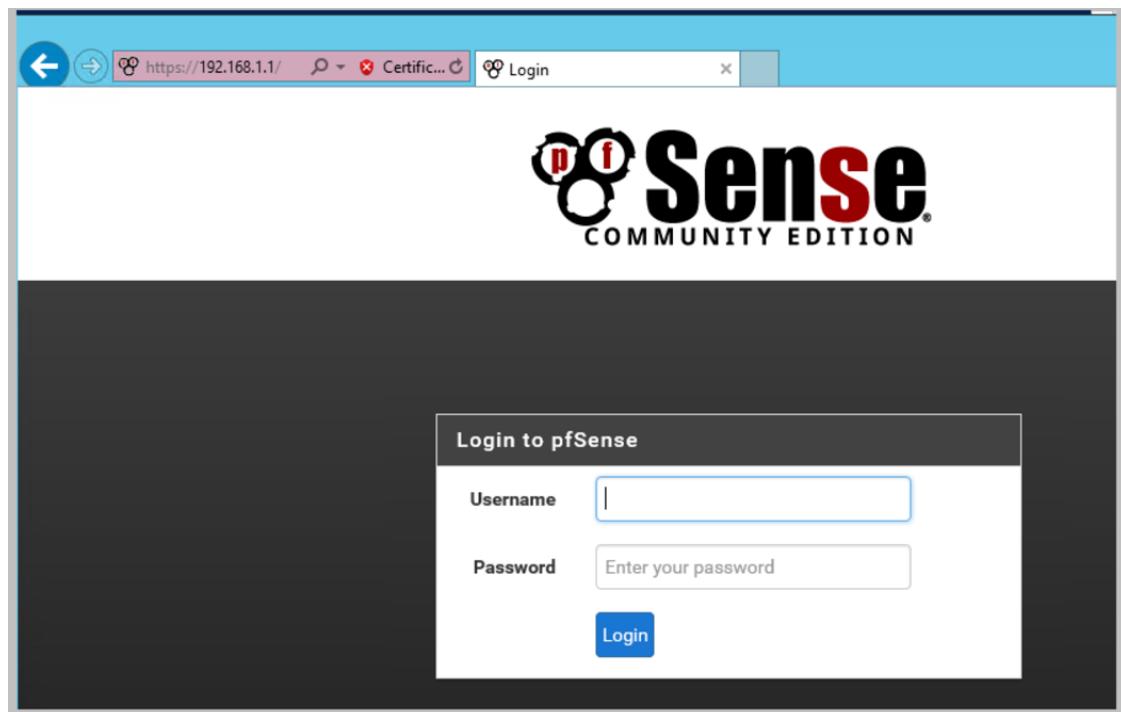
Press ENTER to continue.
```

9. Setting up PFsense

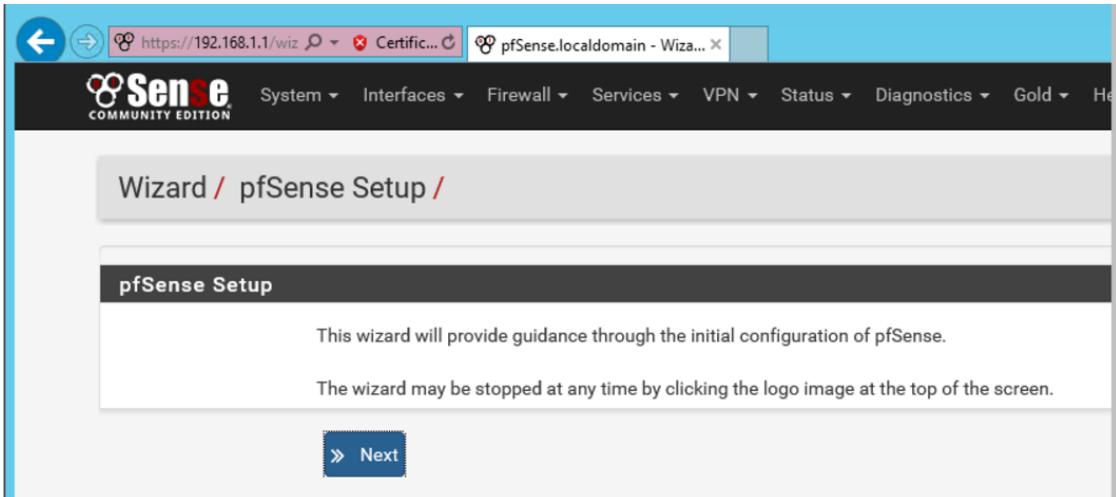
- PFsense must be configured prior to configuring our lab. From Windows 2012 system or any other lab system, open explorer and go to <https://192.168.1.1>. Click “Continue to this website”



- Login with admin/pfsense



- Click "Next" to continue



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

The screenshot shows the "General Information" setup screen. It displays fields for Hostname (pfSense) and Domain (localdomain). Below these, there is a note about the DNS resolver's behavior. The "Primary DNS Server" field contains "10.0.1.1" and the "Secondary DNS Server" field contains "8.8.8.8". A red arrow points to the "Primary DNS Server" field, and another red arrow points to the "Secondary DNS Server" field. At the bottom, there is a checkbox for "Override DNS" which is checked, with the sub-instruction "Allow DNS servers to be overridden by DHCP/PPP on WAN". A blue "» Next" button is at the bottom.

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

The screenshot shows the pfSense Setup Wizard interface. The title bar reads "Wizard / pfSense Setup / Configure WAN Interface". Below it, a red progress bar is partially filled. The main content area has a header "Configure WAN Interface" and a sub-header "On this screen the Wide Area Network information will be configured.". A dropdown menu labeled "SelectedType" shows "DHCP" selected. The configuration section is titled "General configuration" and contains three fields: "MAC Address" (with a note about spoofing), "MTU" (with a note about PPPoE), and "MSS" (with a note about TCP connections). The "DHCP" option is highlighted in blue.

- Scroll down to the RFC settings in the bottom

The screenshot shows the "RFC1918 Networks" configuration page. It includes two sections: "Block RFC1918 Private Networks" (with a note about RFC 1918 reserved IP ranges) and "Block bogon networks" (with a note about IANA reserved IP ranges). Both sections have a checked checkbox for "Block private networks from entering via WAN" and "Block non-Internet routed networks from entering via WAN". A "Next" button is at the bottom.

- Uncheck the boxes

The screenshot shows the 'RFC1918 Networks' configuration page. It contains two sections: 'Block RFC1918 Private Networks' and 'Block bogon networks'. Both sections have an unchecked checkbox labeled 'Block private networks from entering via WAN'. A detailed explanatory text follows each checkbox. At the bottom right is a blue '» Next' button.

Block RFC1918 Private Networks

Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks

Block non-Internet routed networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

» Next

- Click "next" to continue

The screenshot shows the 'Configure LAN Interface' screen. It displays a message: 'On this screen the Local Area Network information will be configured.' Below this are fields for 'LAN IP Address' (set to 192.168.1.1) and 'Subnet Mask' (set to 24). A dropdown menu is shown next to the subnet mask field. At the bottom right is a blue '» Next' button.

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address X
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask ▼

» Next

- Click "next" to continue and change the admin password

The screenshot shows the 'Set Admin WebGUI Password' screen. It displays a message: 'On this screen the admin password will be set, which is used to access the WebGUI and also S...'. Below this are two password input fields: 'Admin Password' and 'Admin Password AGAIN', both containing masked text. At the bottom right is a blue '» Next' button.

Set Admin WebGUI Password

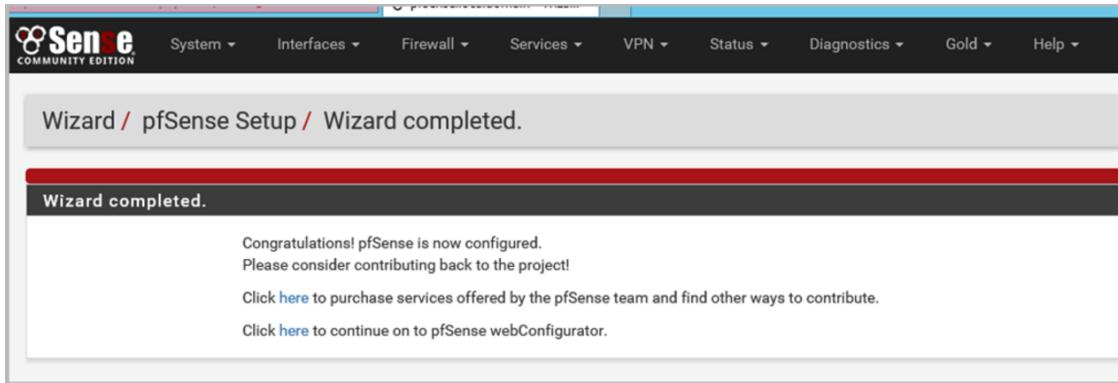
On this screen the admin password will be set, which is used to access the WebGUI and also S...

Admin Password

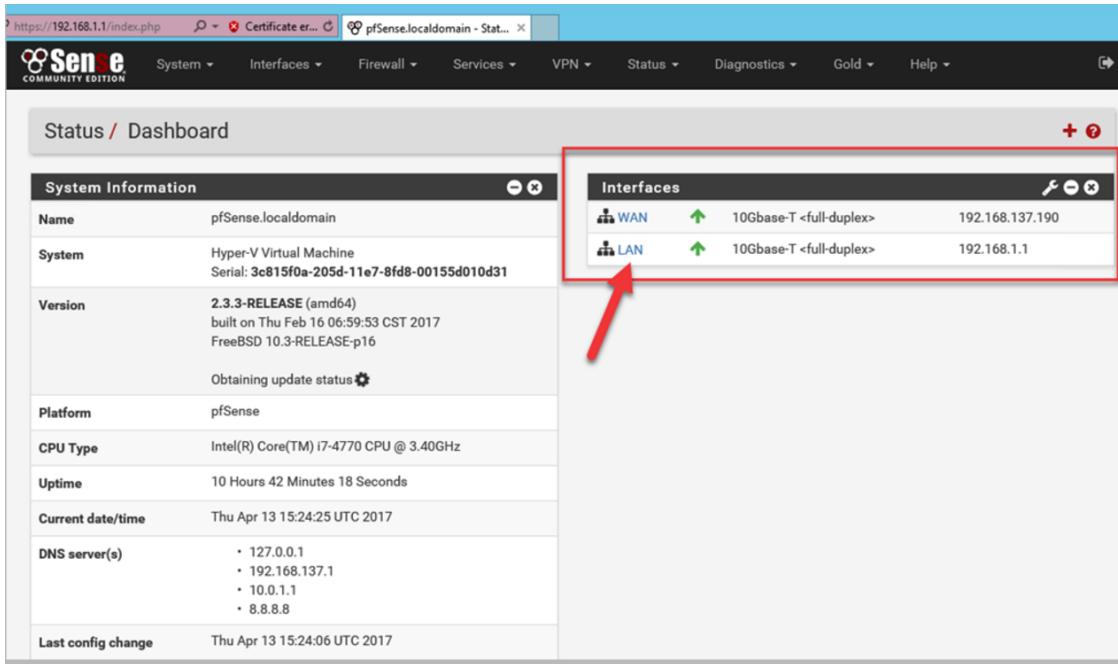
Admin Password AGAIN ▼

» Next

- PFsense setup is now complete



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



A screenshot of the pfSense status dashboard. On the left, there's a "System Information" sidebar with various system details like Name (pfSense.localdomain), System (Hyper-V Virtual Machine), Version (2.3.3-RELEASE), Platform (pfSense), CPU Type (Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz), Uptime (10 Hours 42 Minutes 18 Seconds), Current date/time (Thu Apr 13 15:24:25 UTC 2017), DNS server(s) (127.0.0.1, 192.168.137.1, 10.0.1.1, 8.8.8.8), and Last config change (Thu Apr 13 15:24:06 UTC 2017). On the right, there's a "Interfaces" section with two entries: "WAN" (10Gbase-T <full-duplex>, IP 192.168.137.190) and "LAN" (10Gbase-T <full-duplex>, IP 192.168.1.1). A red box highlights the "Interfaces" section, and a red arrow points to the "LAN" entry.

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

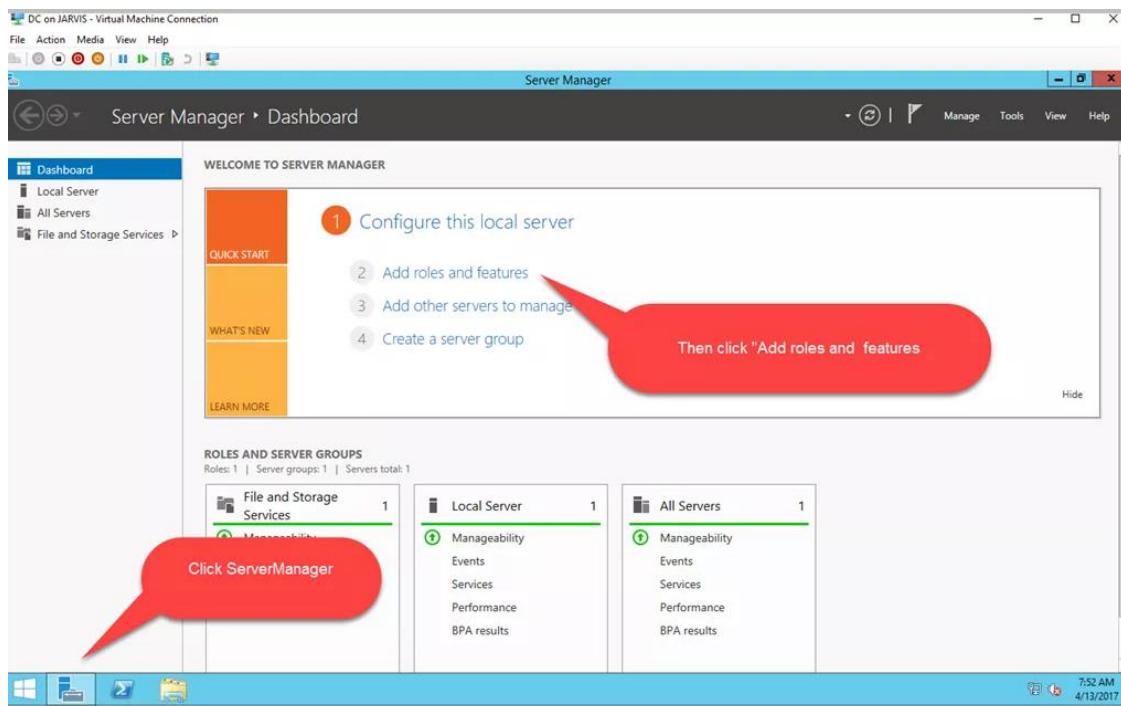
The screenshot shows the pfSense web interface with the URL https://192.168.1.1/services_dhcp.php. The top navigation bar includes links for System, Interfaces, Firewall, Services (which is currently selected), VPN, Status, and Diagnostics. A red arrow points from the Services dropdown menu to the "DHCP Server" option in the list. The main content area is titled "Services / DHCP Server / LAN". Under the "General Options" tab, there are several configuration options:

- Enable:** Enable DHCP server on LAN interface.
- BOOTP:** Ignore BOOTP queries.
- Deny unknown clients:** Only the clients defined below will be allowed to obtain an IP address.
- Ignore denied clients:** Denied clients will be ignored rather than sending them an error message. This option is not compatible with failover.
- Ignore client identifiers:** If a client includes a unique identifier in its DHCP request, it will be recorded. This option may be useful when a client's server behavior violates the official DHCP standard.
- Subnet:** 192.168.1.0
- Subnet mask:** 255.255.255.0

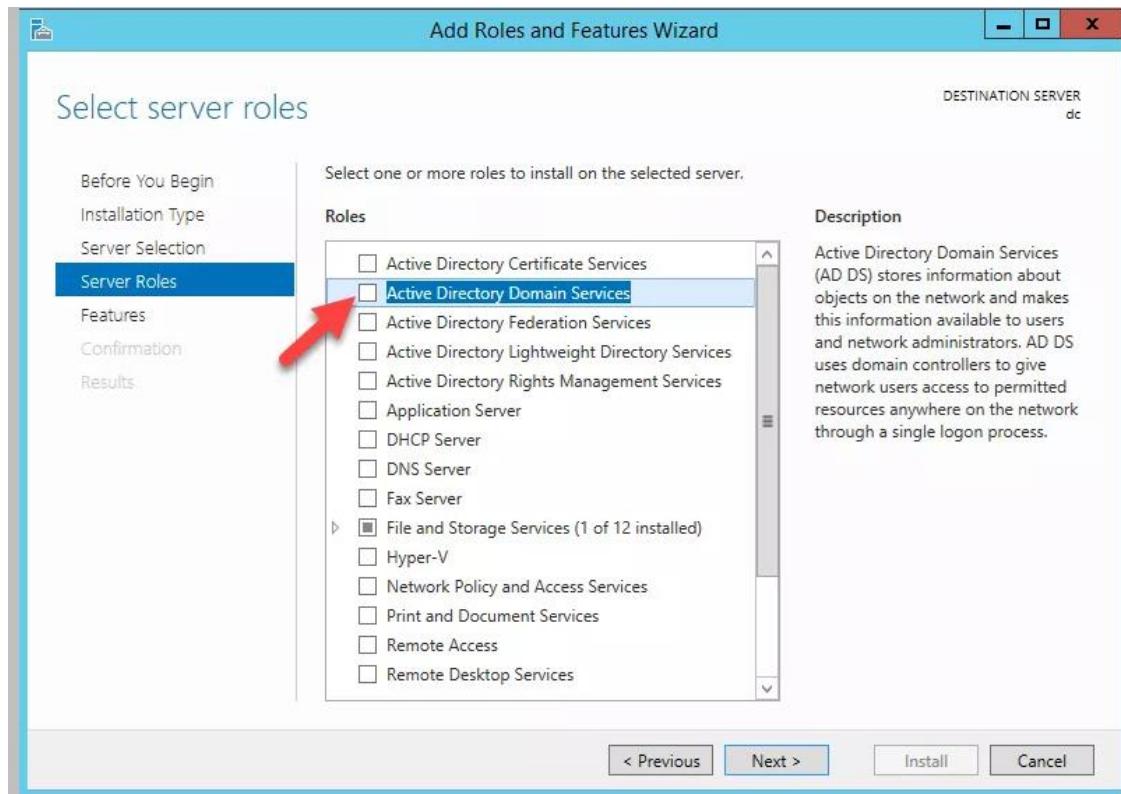
- Uncheck the “Enable DHCP server on LAN interface”. We will setup DHCP role in Windows 2012 server, which will be used to hand out IPs to client systems. Save the settings and we’re done with PFsense for now.

10. Promoting Windows 2012 Server to Domain Controller

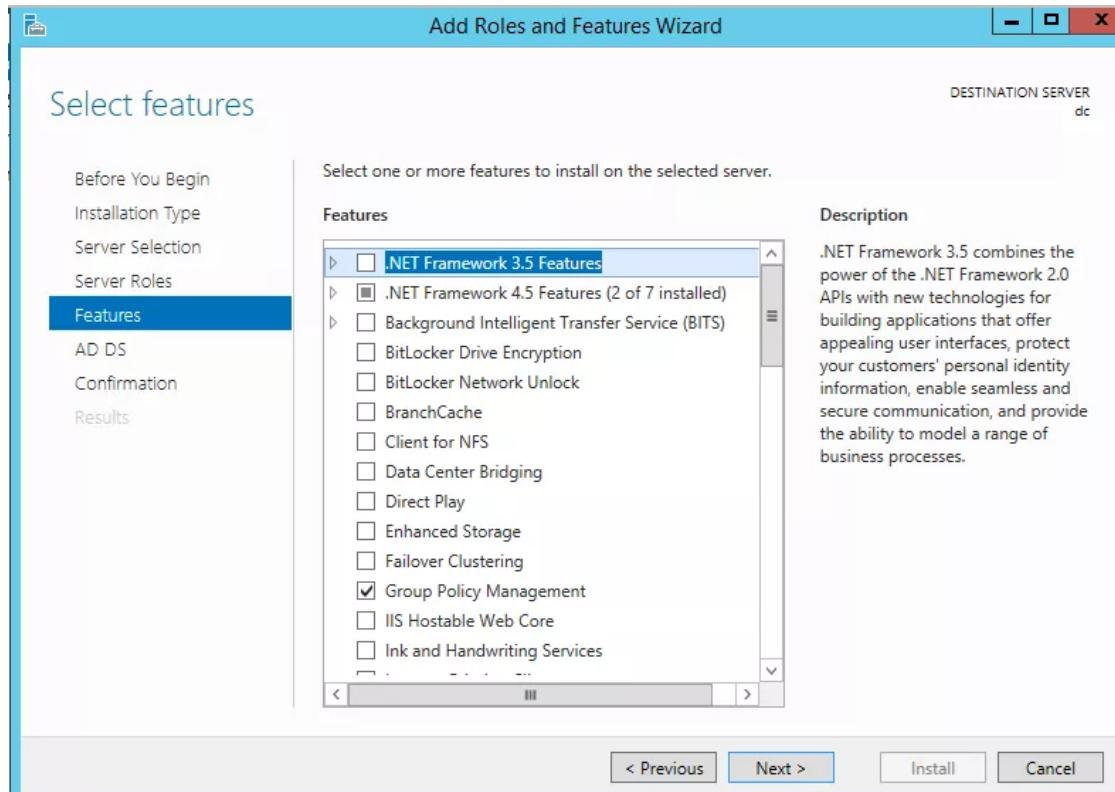
- Let’s promote Windows 2012 to Domain Controller. Connect to Windows 2012 system and launch “ServerManager” and Click “Add roles and features”



- Check “Active Directory Domain Services”



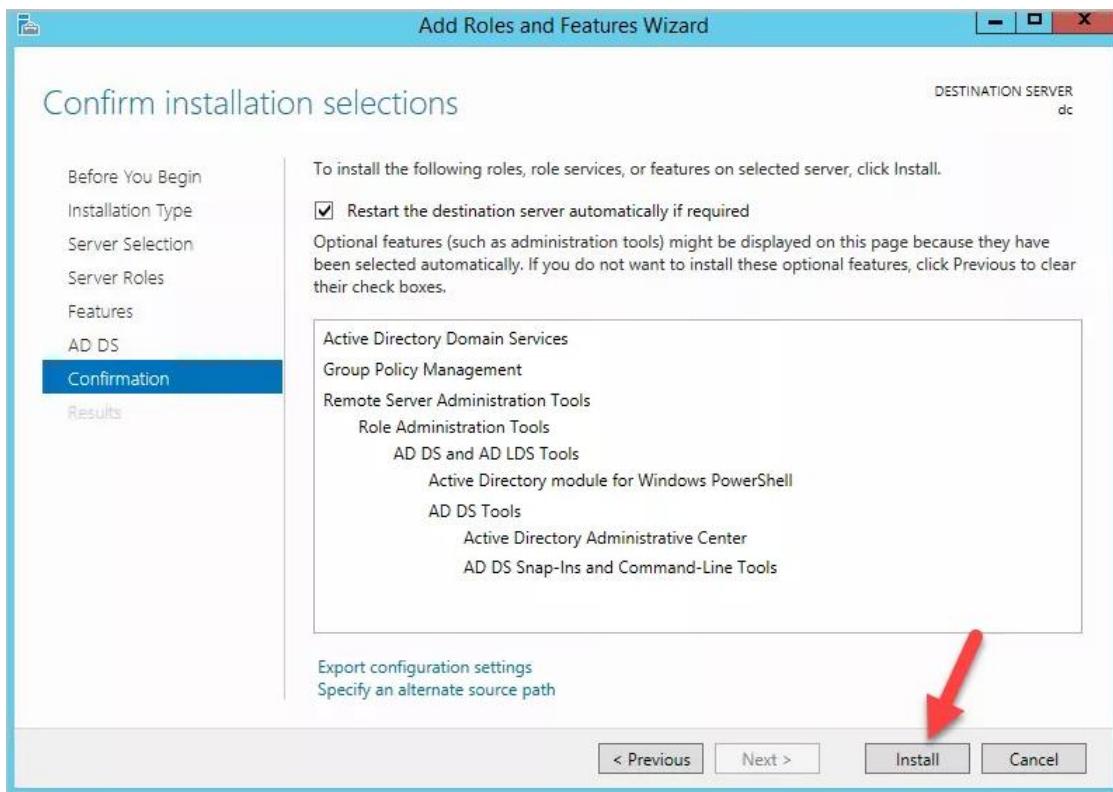
- Use the defaults



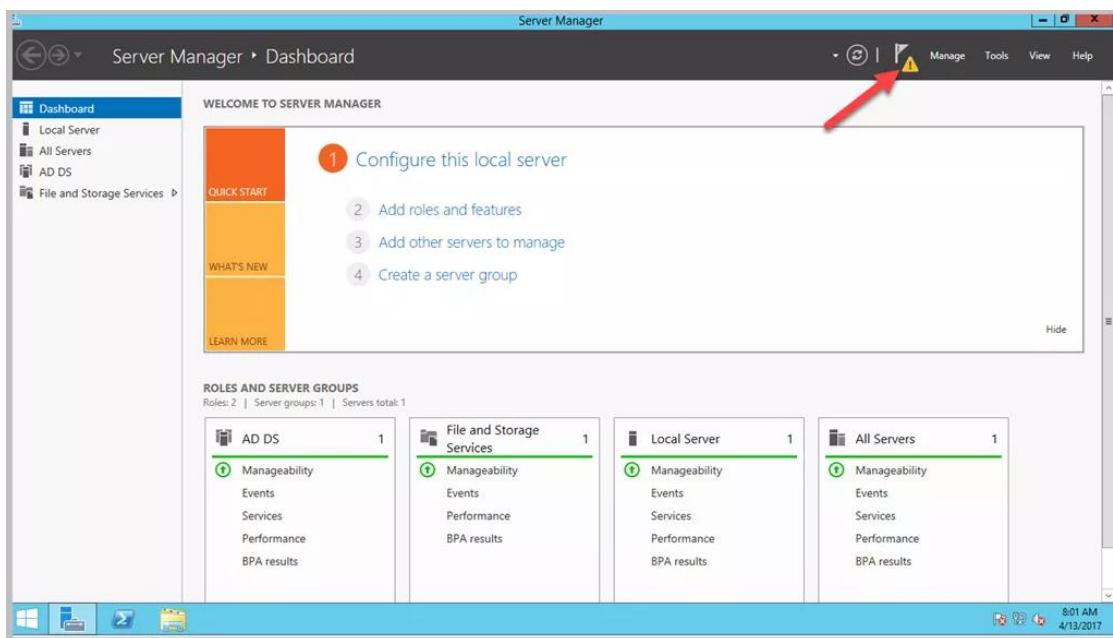
- Check the box and click "yes"



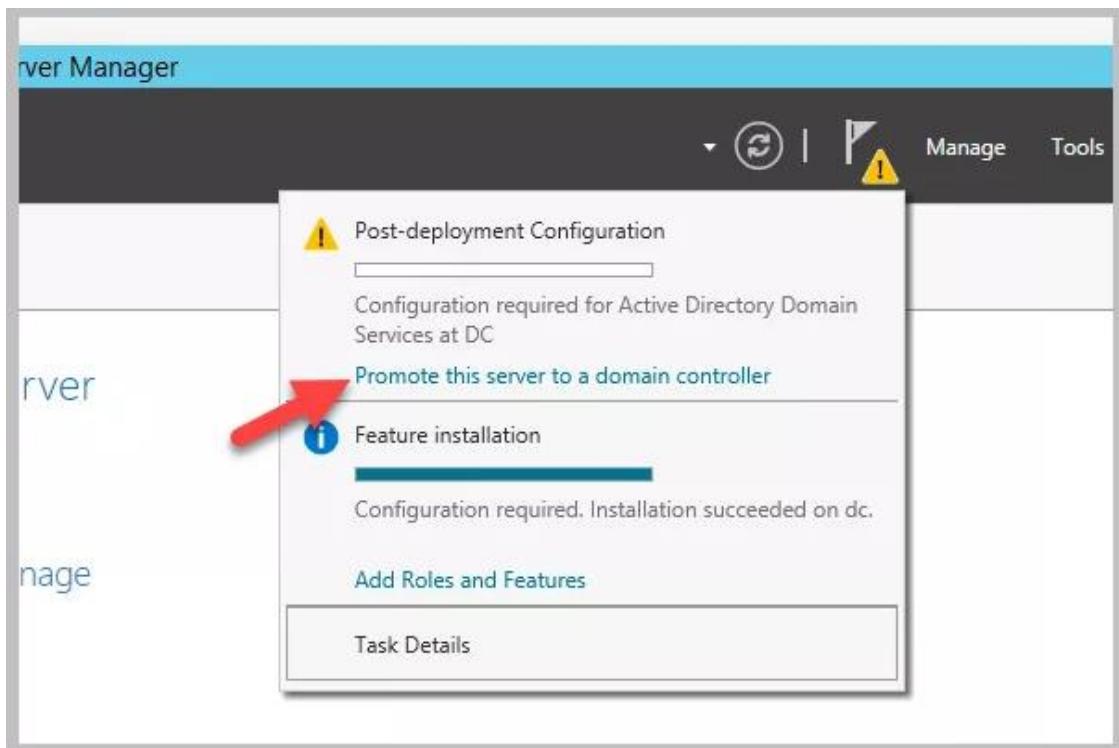
- Click Install and wait for the process to complete



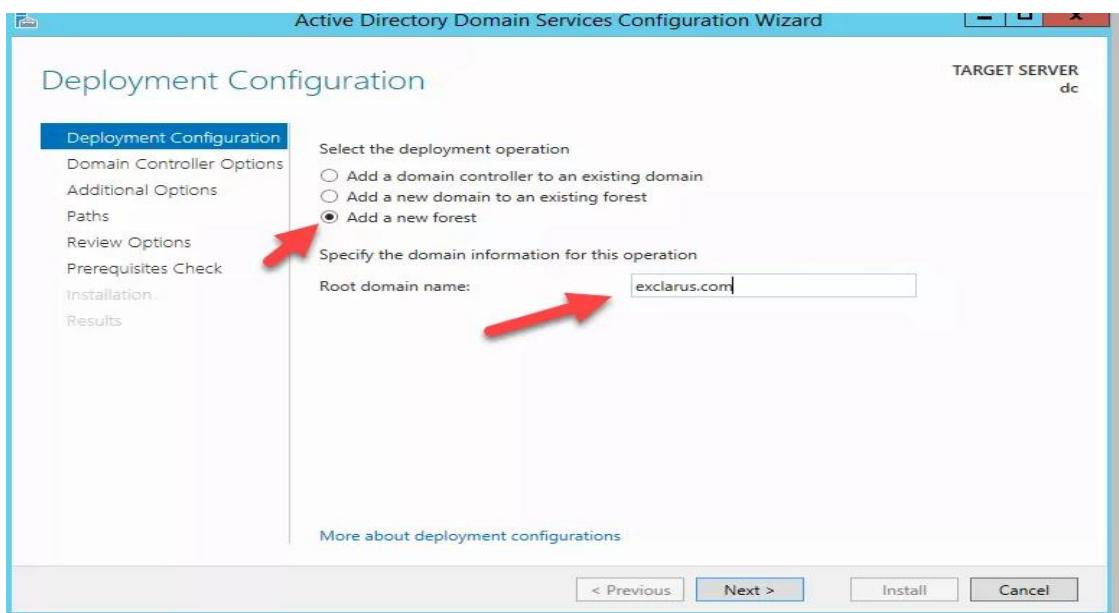
- Click the “**Exclamation**” mark and shown



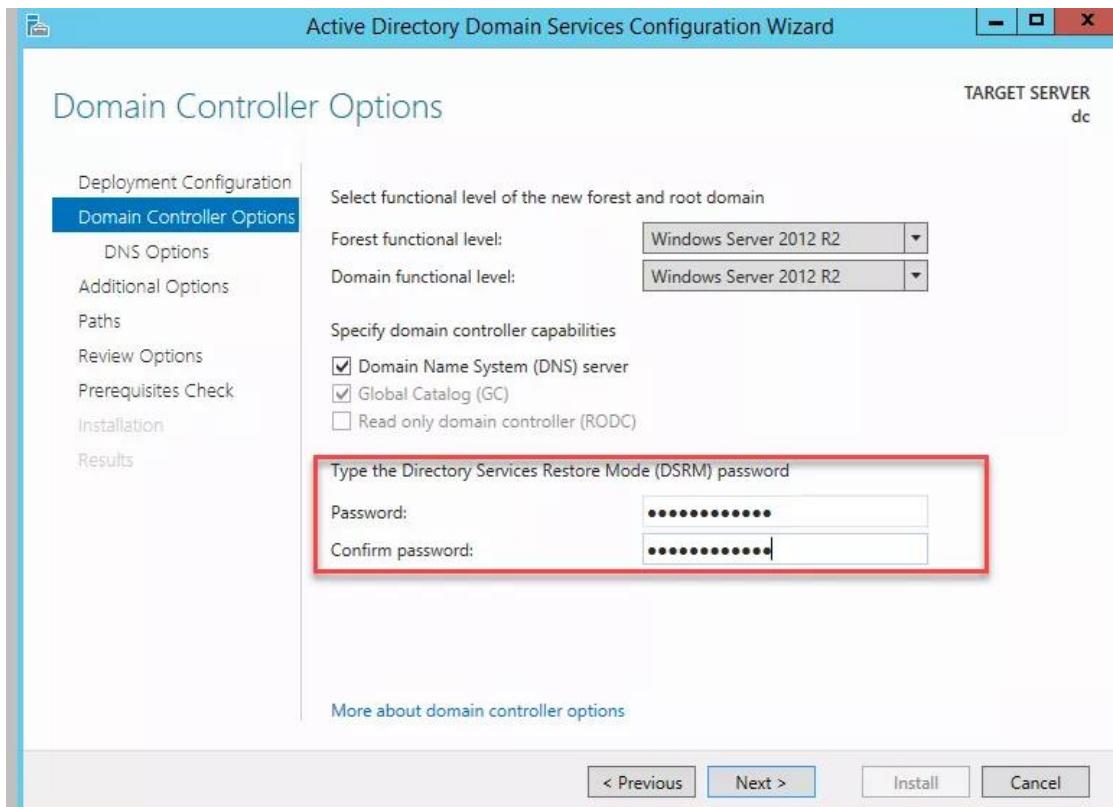
- Click on “Promote this server to a domain controller”



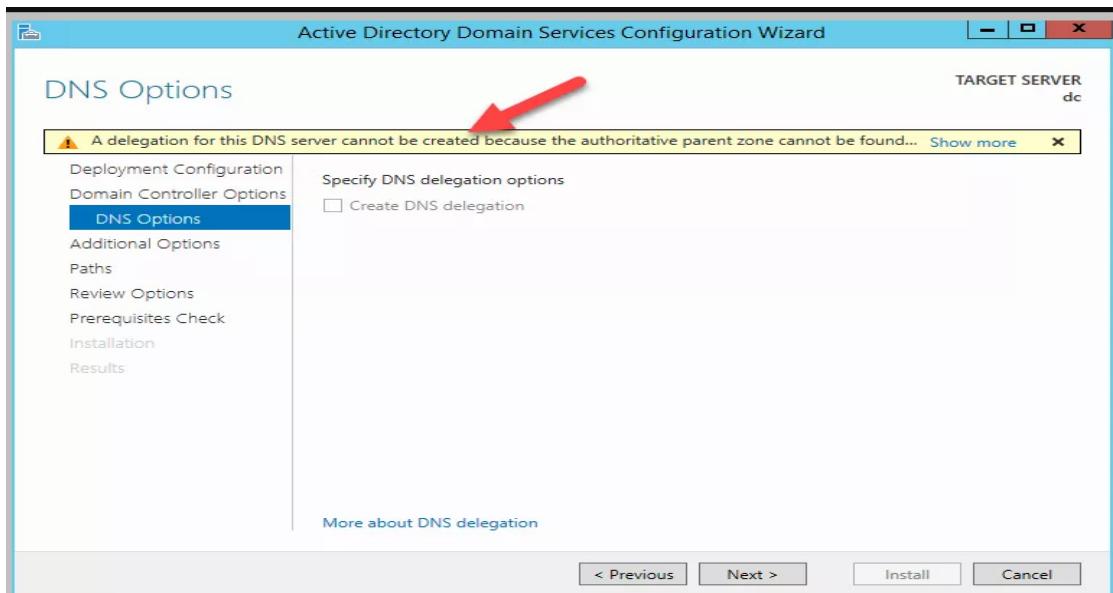
- Check the radio box “Add a new forest” and use a domain name. Feel free to use any domain name



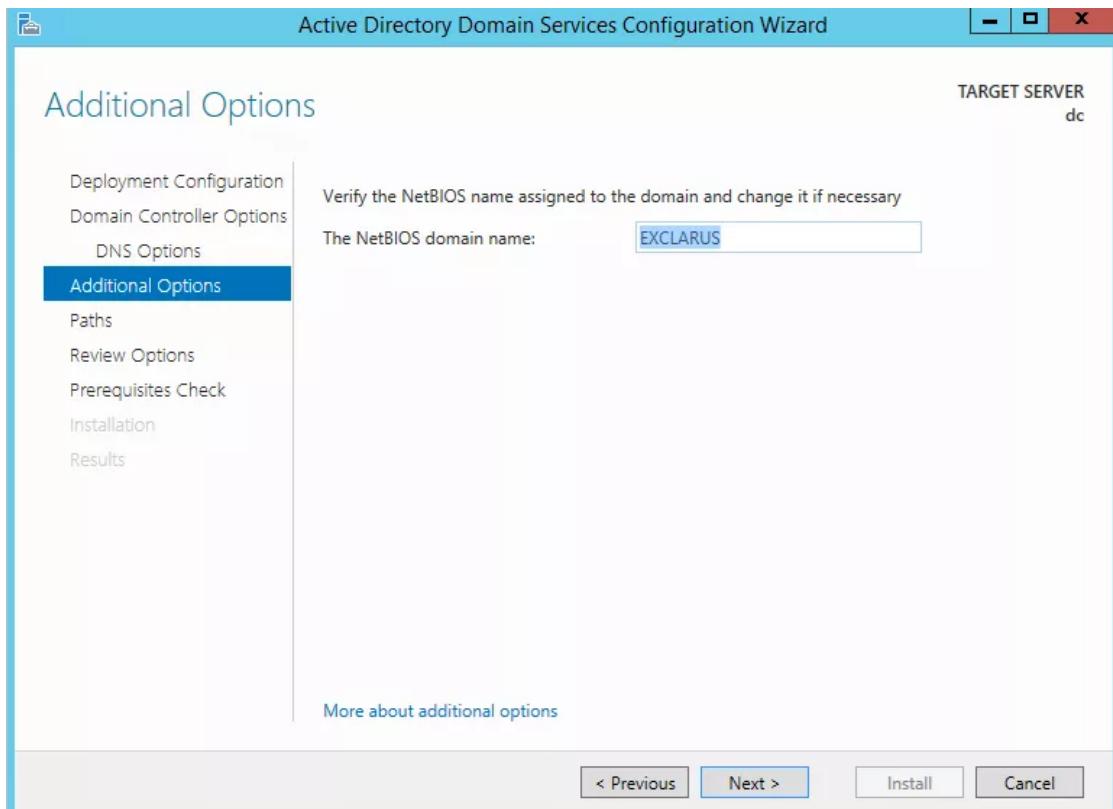
- Use a strong password for restore mode



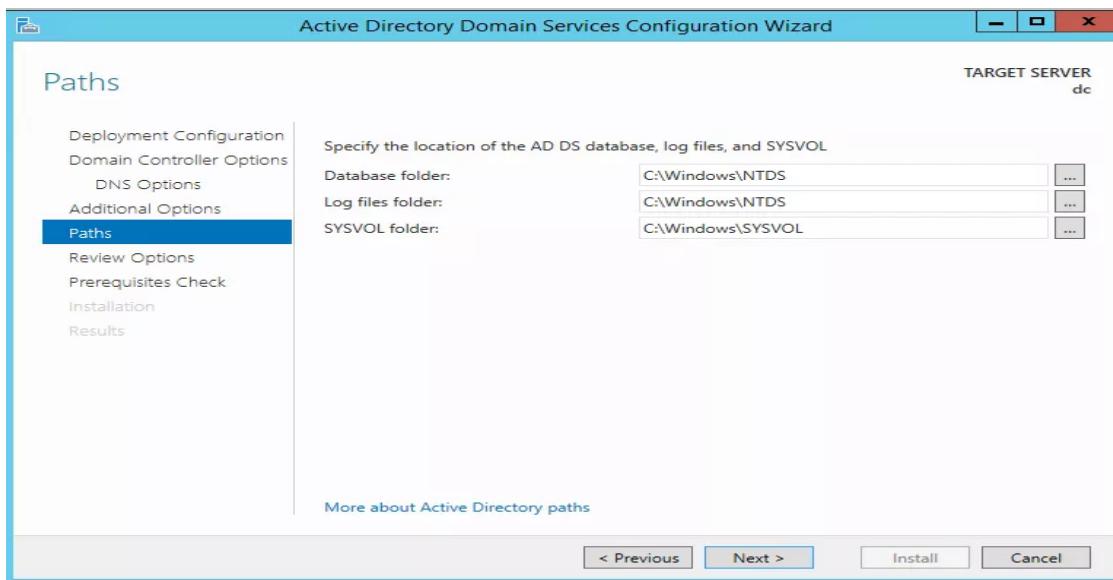
- DNS services will be installed automatically so ignore this warning



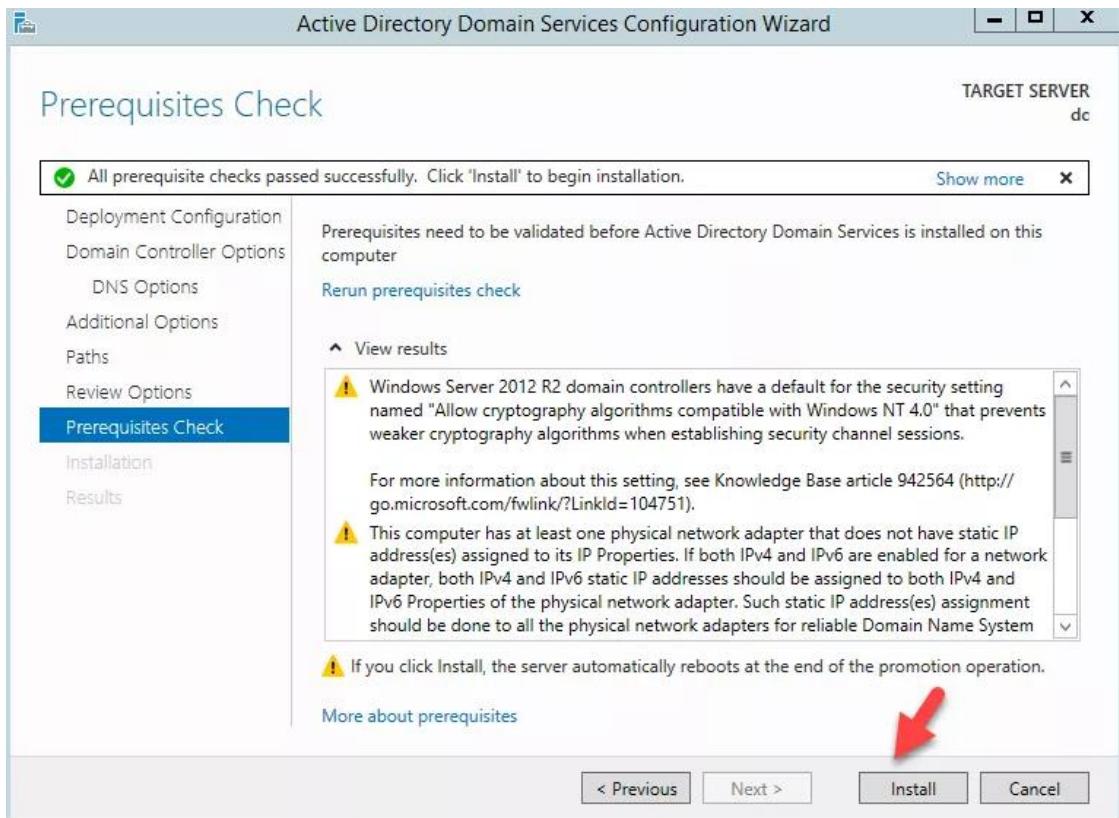
- Use the default netbios name



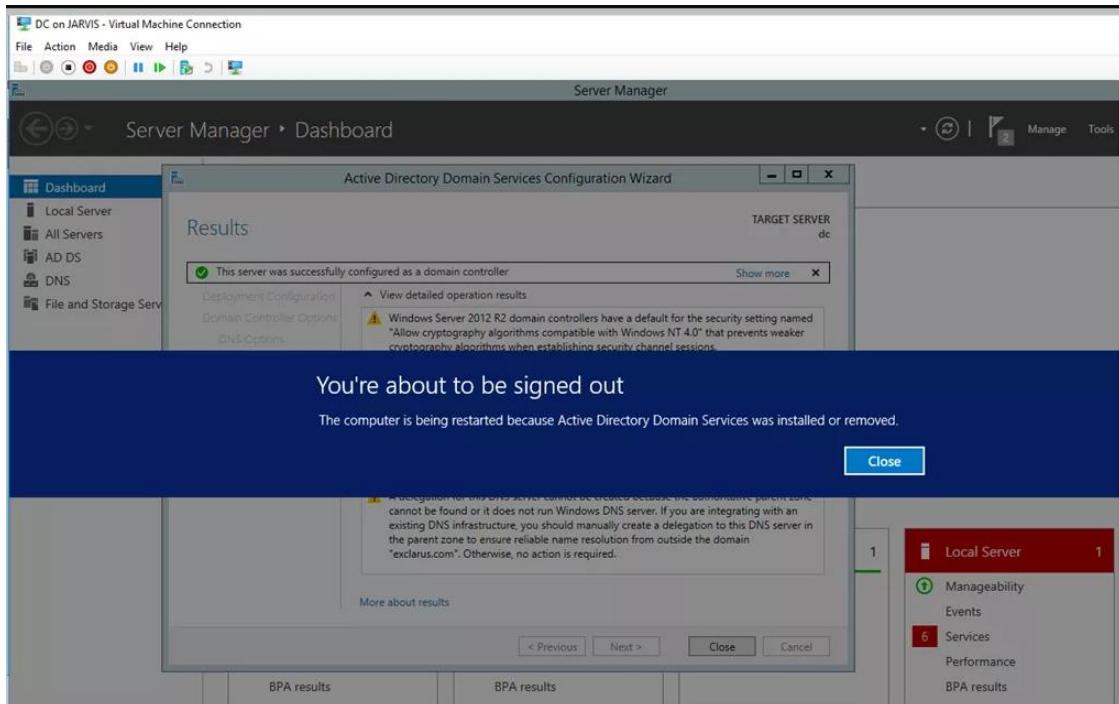
- Production active directory servers will change the location of the following files, but we will stick with the defaults for our lab environment. NTDS is a critical file which has all user hashes.



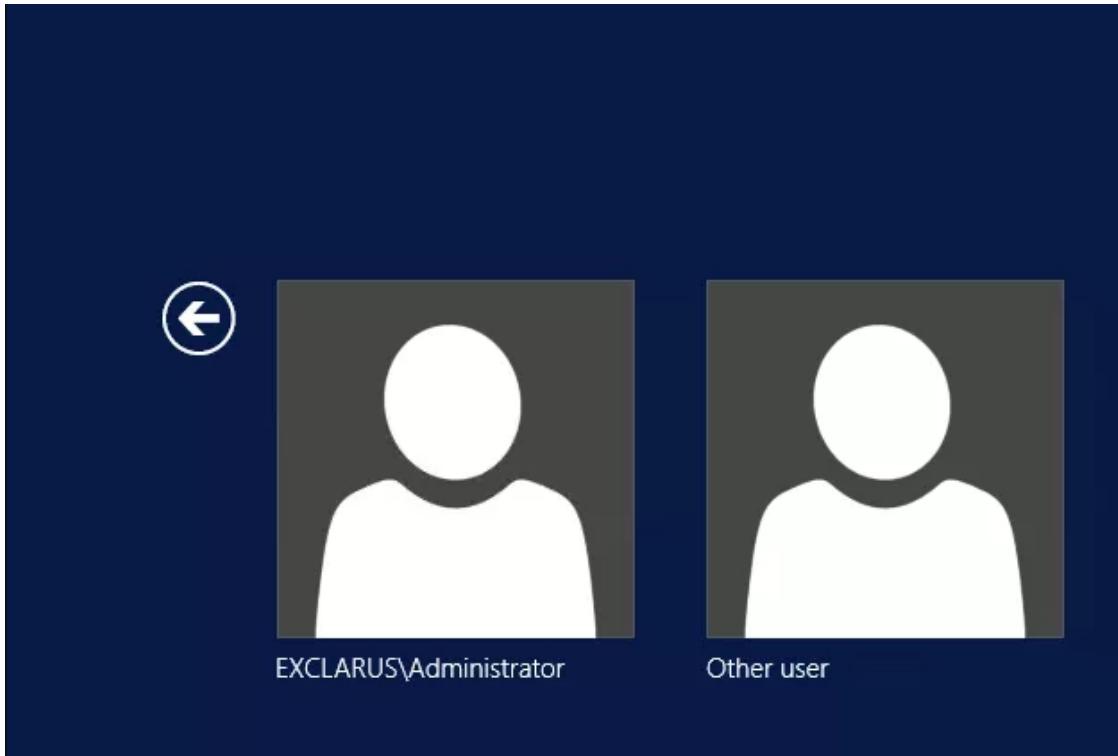
- Click Install



- The server will reboot



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

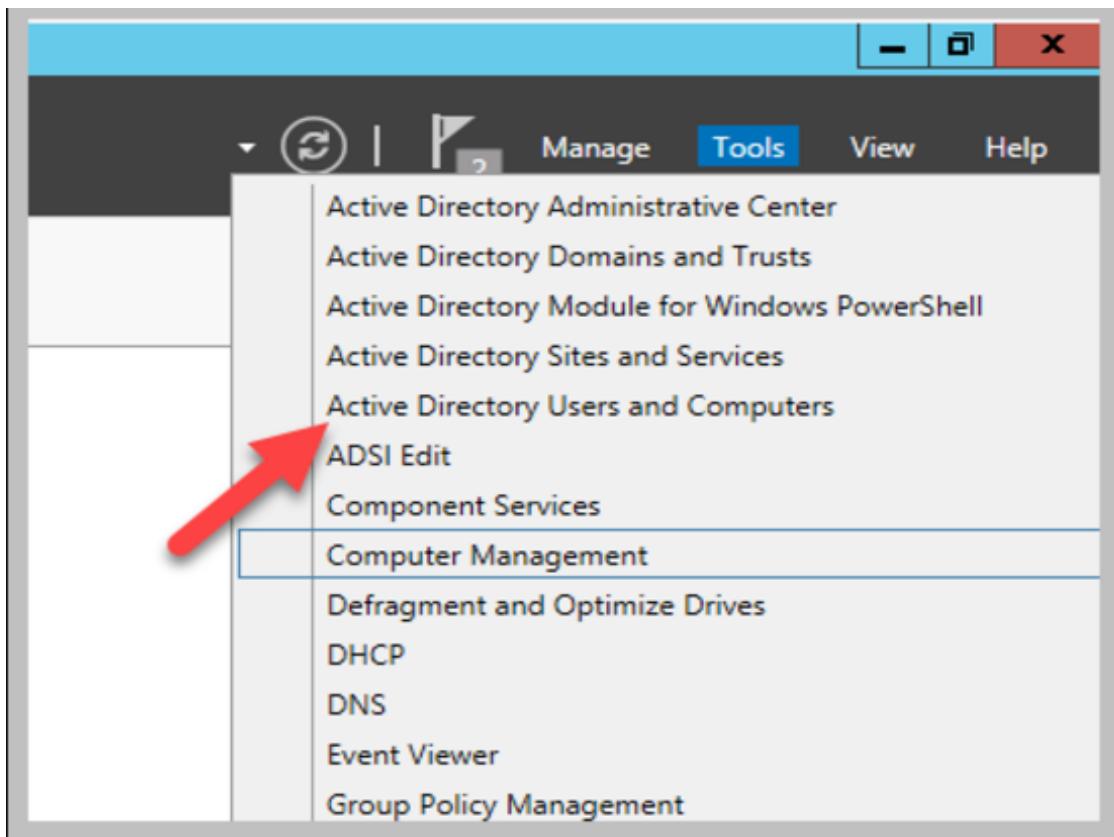


- Tools menu will have additional menu items

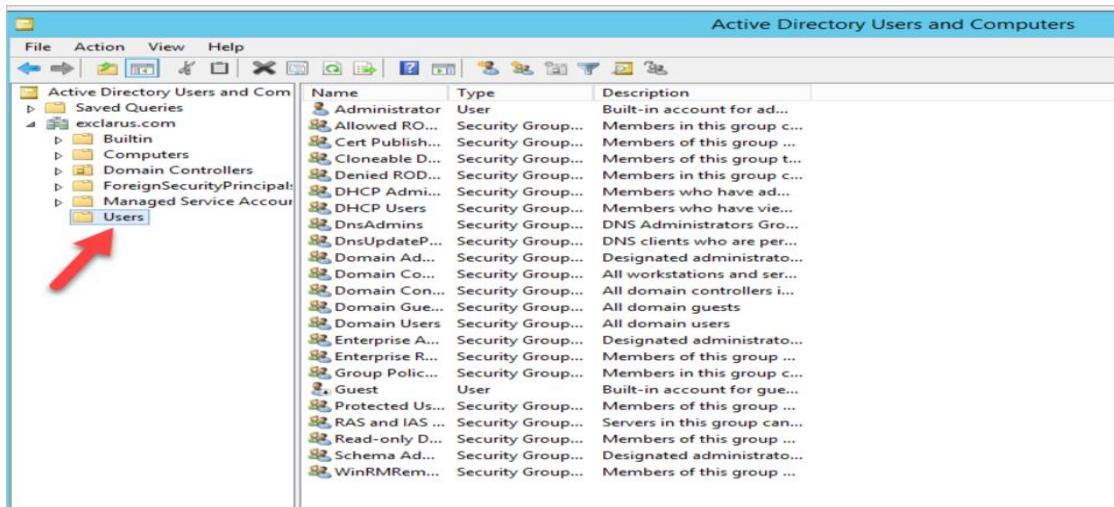


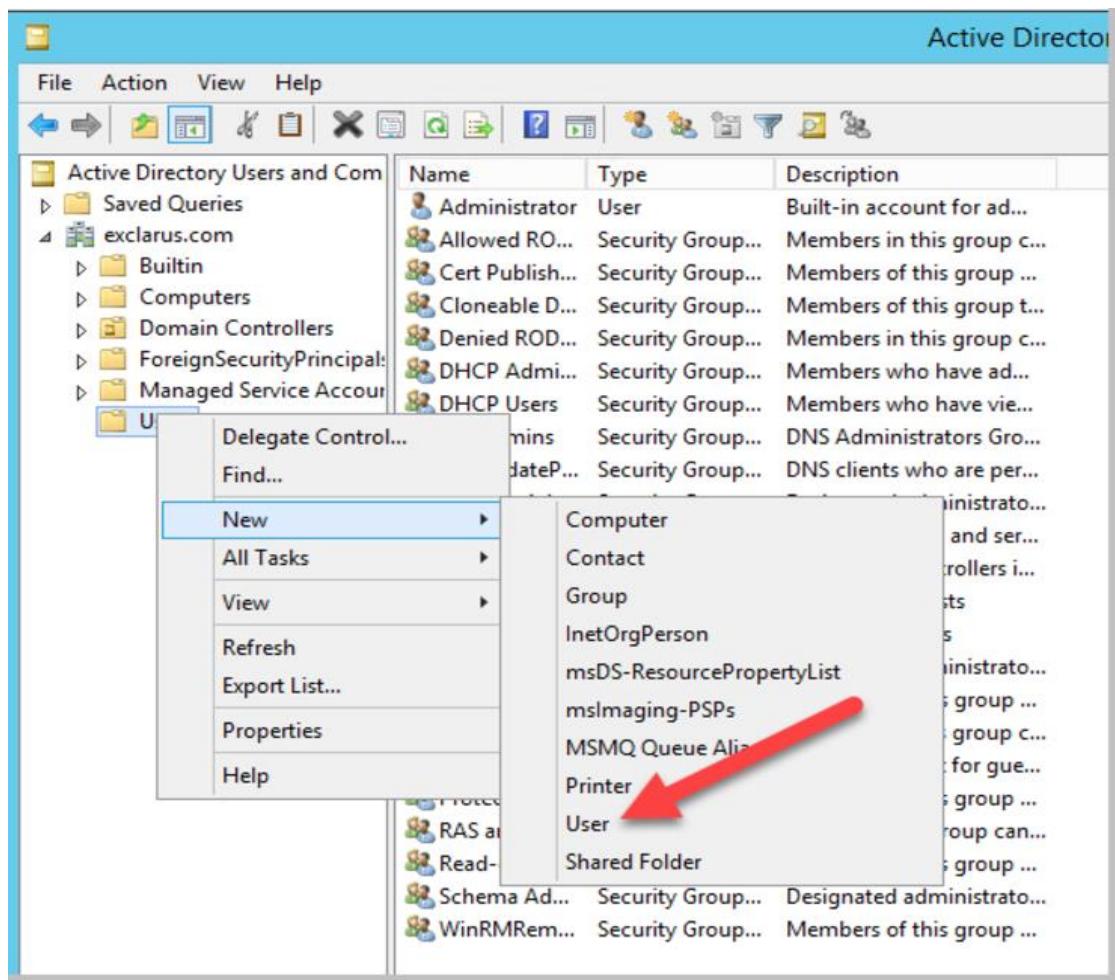
11. Creating Users in Active Directory

- 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





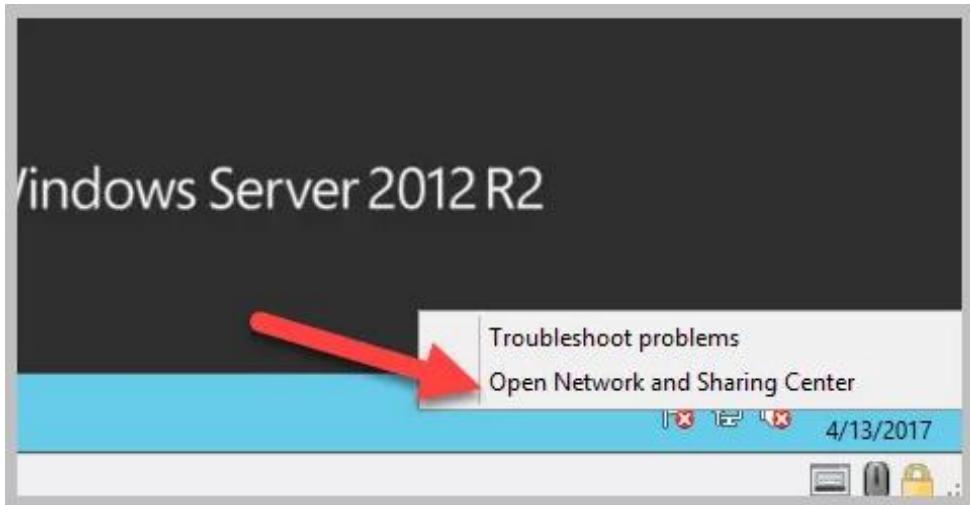
- Type the relevant details. I'm creating a user called “**user1**”

The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: exclarus.com/Users'. The form fields are as follows:
First name: Initials:
Last name:
Full name:
User logon name: (dropdown menu)
User logon name (pre-Windows 2000):
At the bottom are buttons: < Back, Next >, and Cancel.

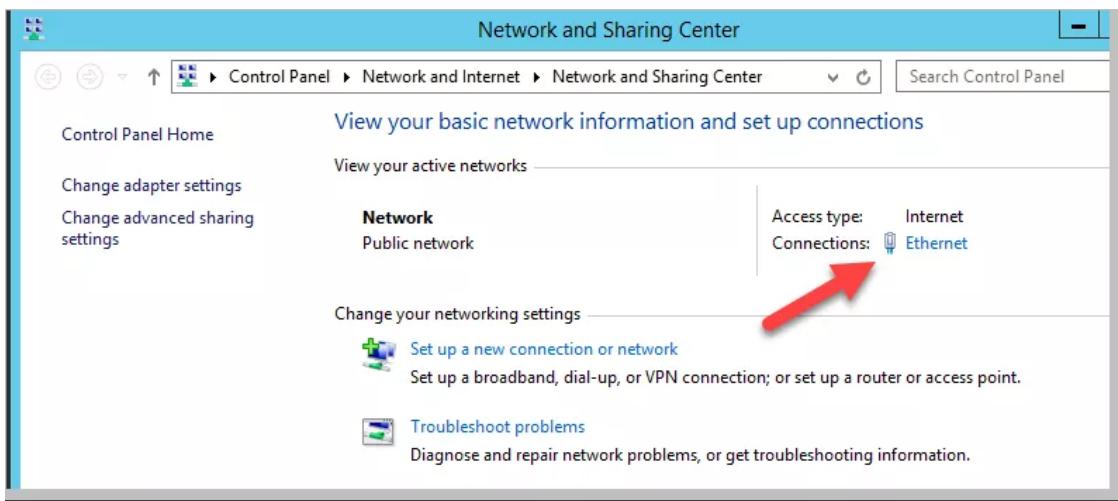
- Now **user1** is a one of the users in the active directory
- Use the same process to create few user accounts.

12. Setting Up Static IP in Domain Controller

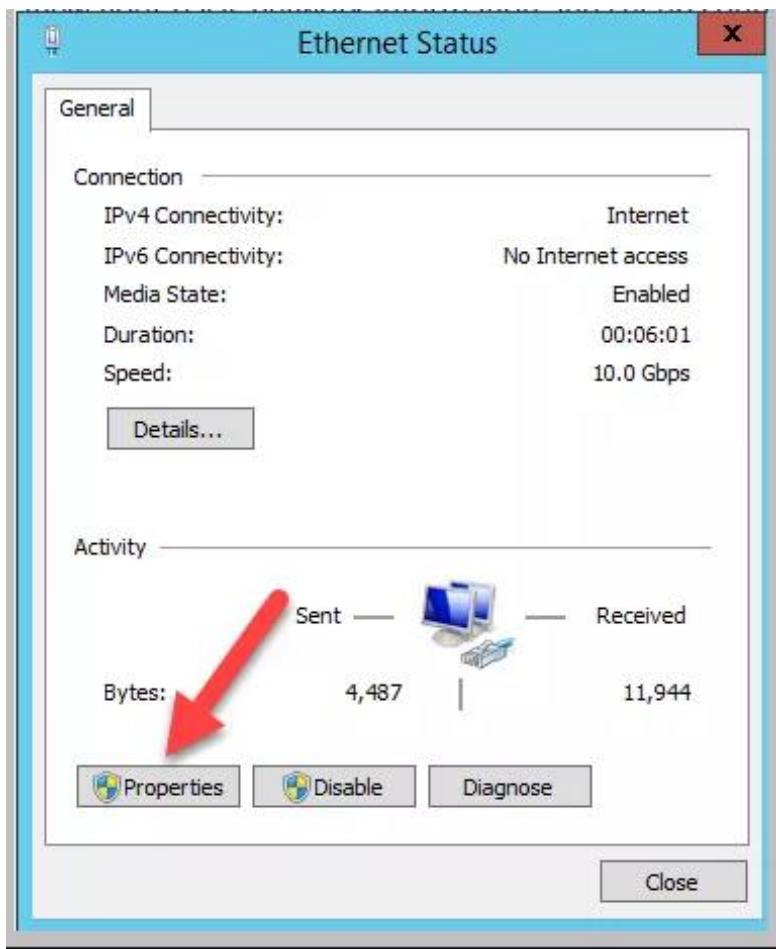
- Right click on the computer and “Open Network Sharing Center”



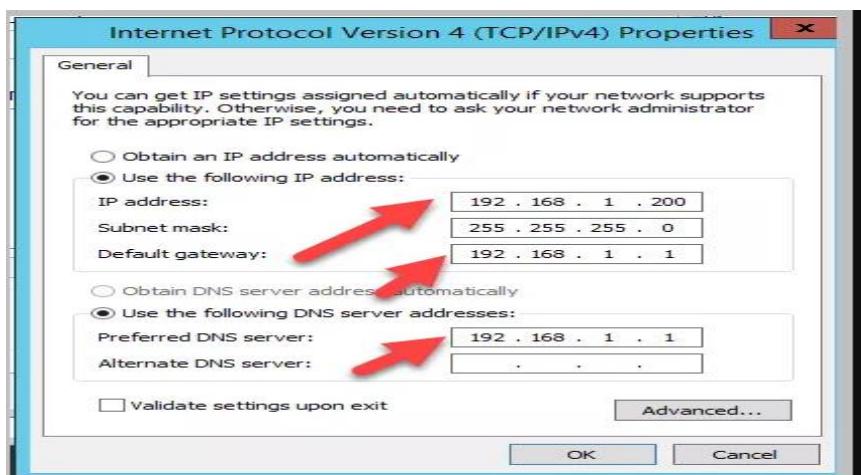
- Click the Ethernet connection hyperlink.



- Click on properties button.



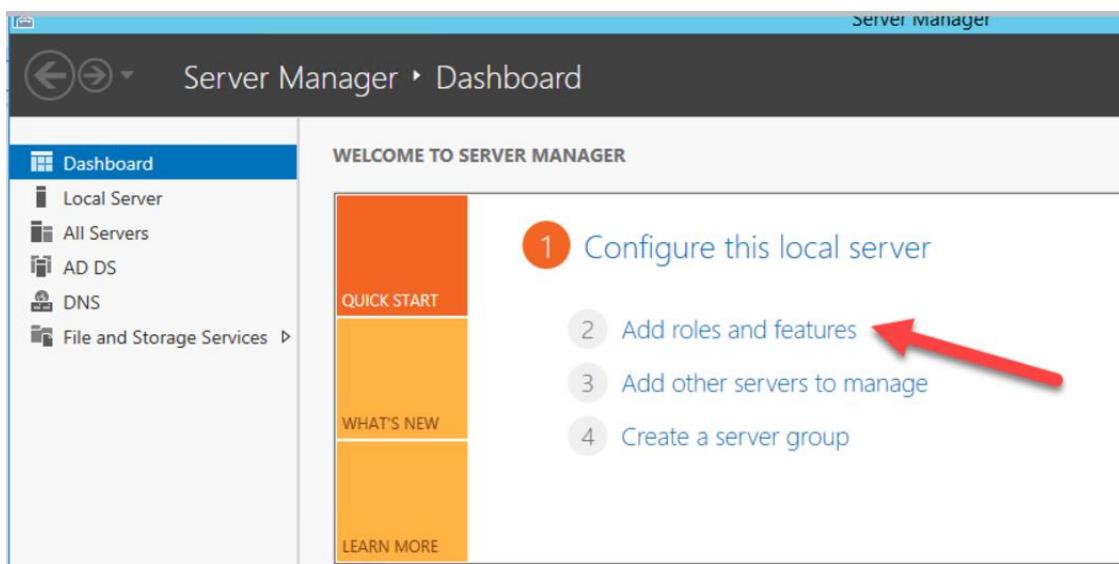
- Use the following configuration or feel free to use any other static IP. Click OK to accept the settings



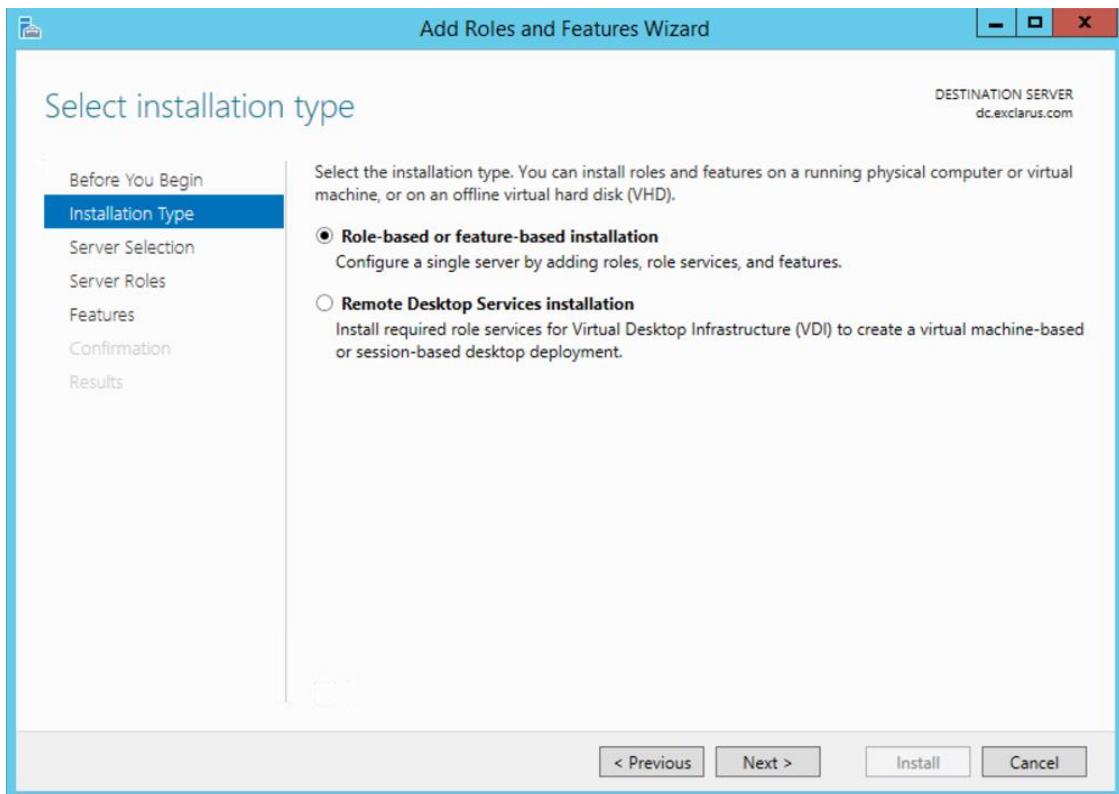
- Open command prompt and type ipconfig /all.

13. Installing DHCP in Domain Controller

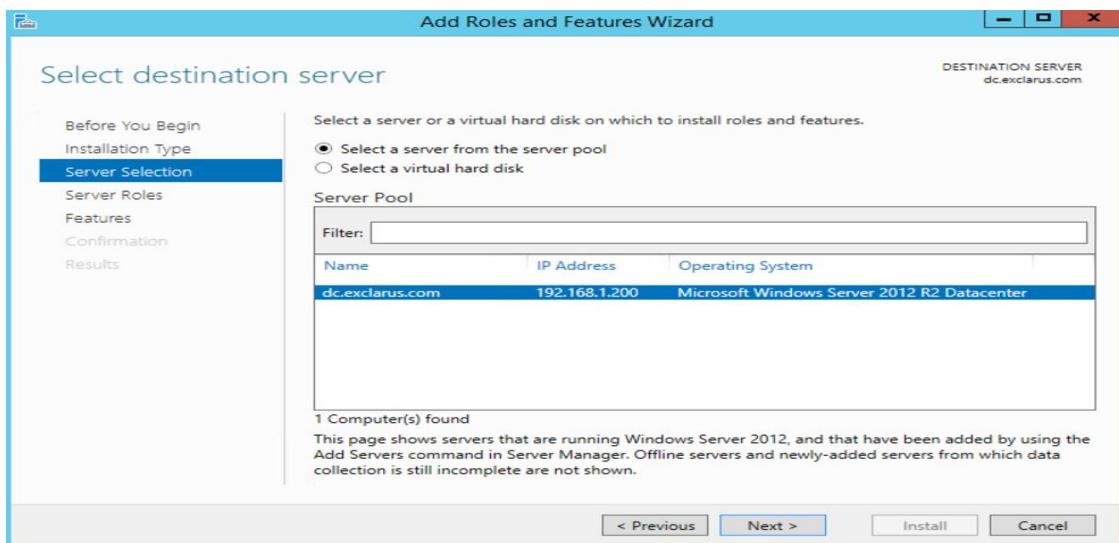
- DHCP service is used to hand out IPs to client systems. First, let's install DHCP and configure it. Let's launch "ServerManager" and click "Add roles and features"



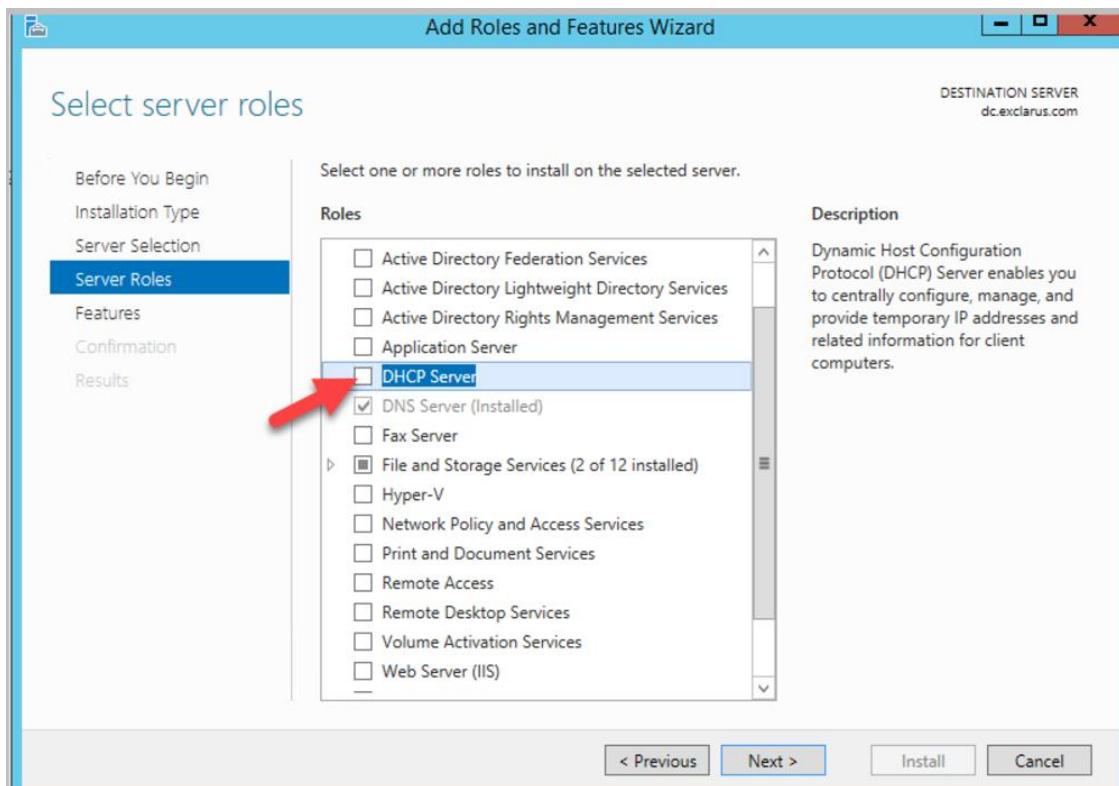
- Check “Role-based or feature-based installation” and click next



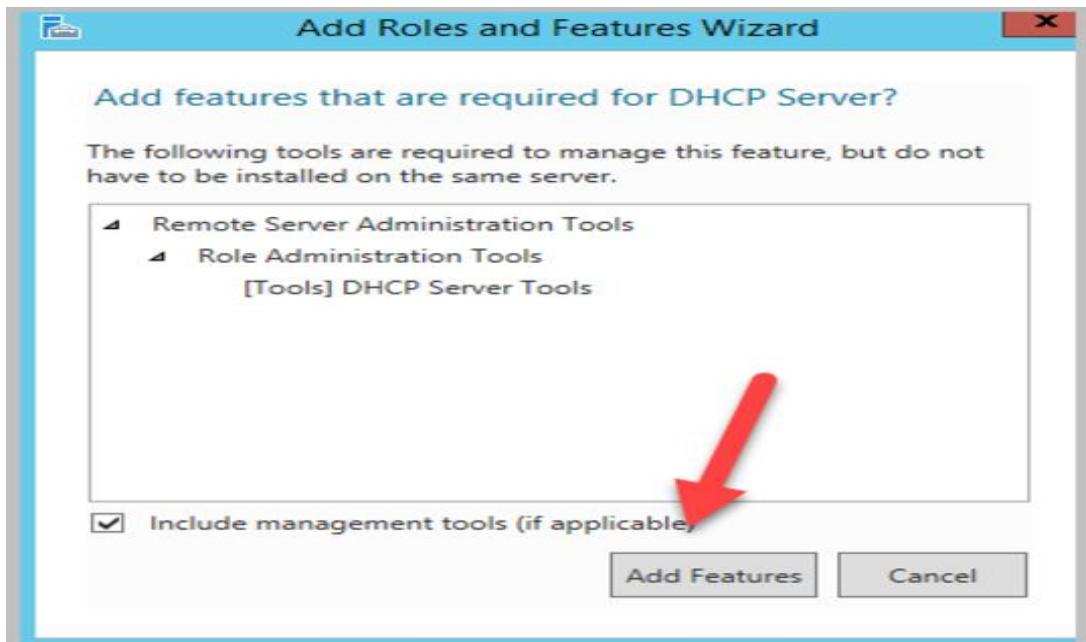
- Click "Next" to continue



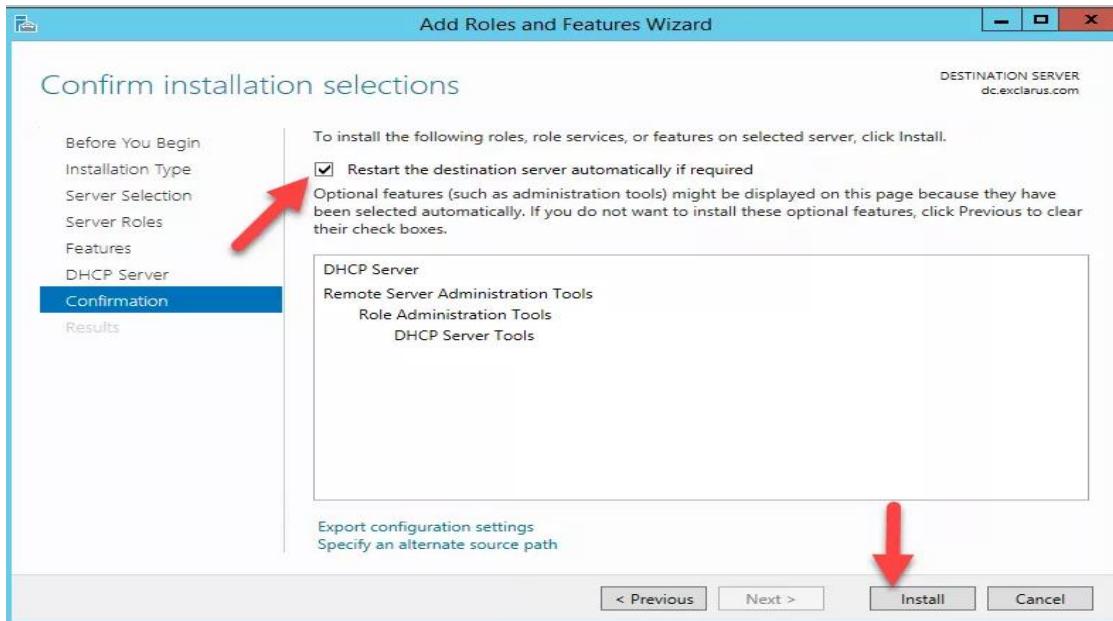
- Check "DHCP Server"



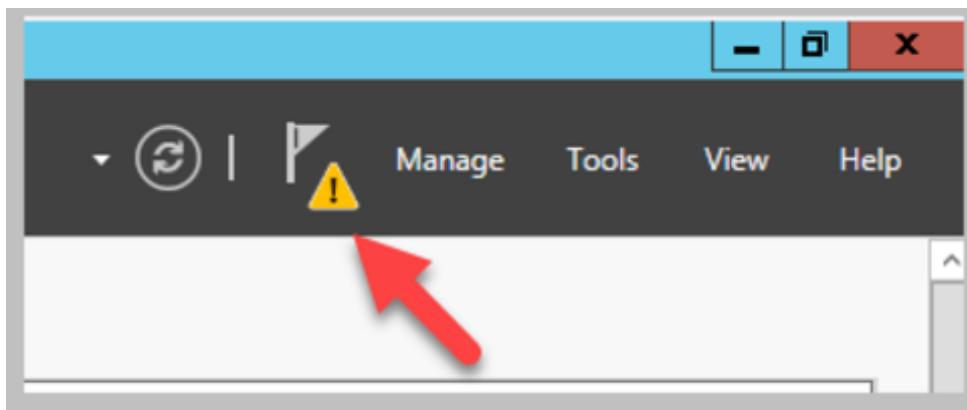
- Click "Add Features"



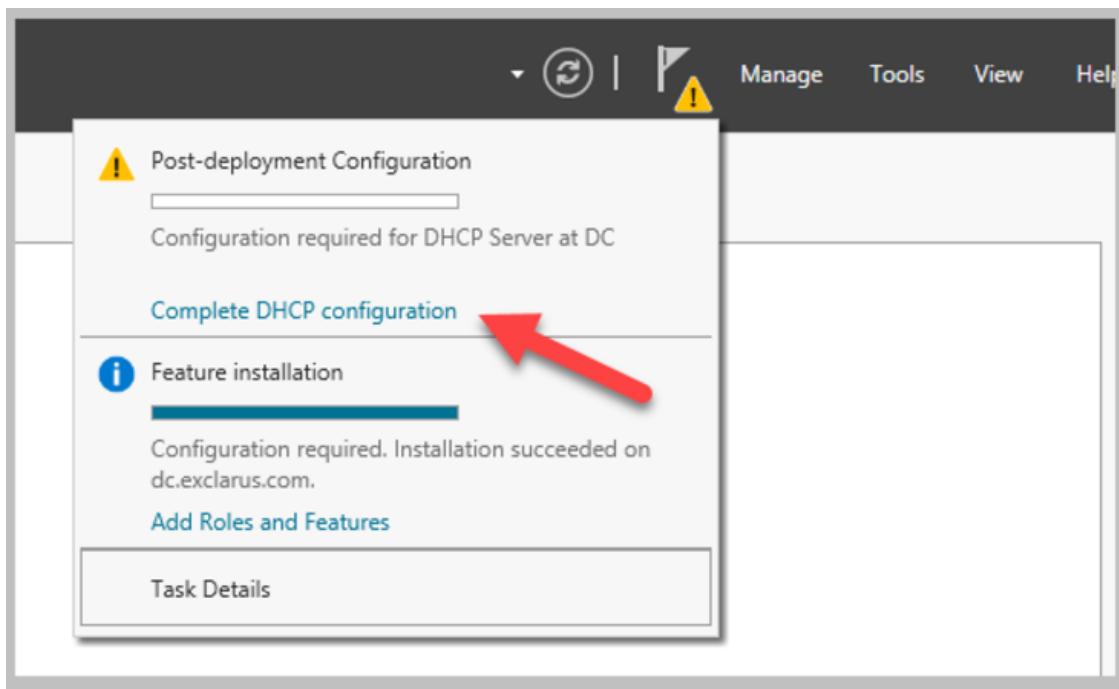
- Click Install to complete the process



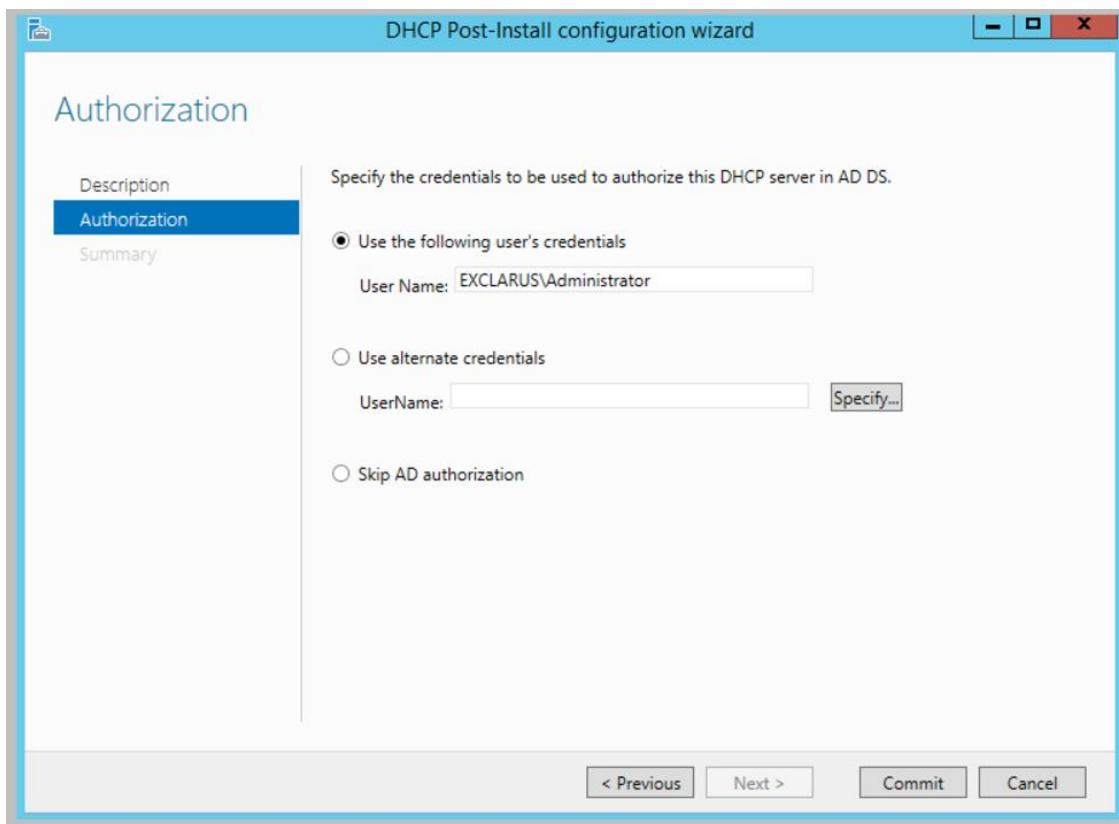
- Click the yellow Exclamation mark to complete the installation process



- Click "Complete DHCP configuration"

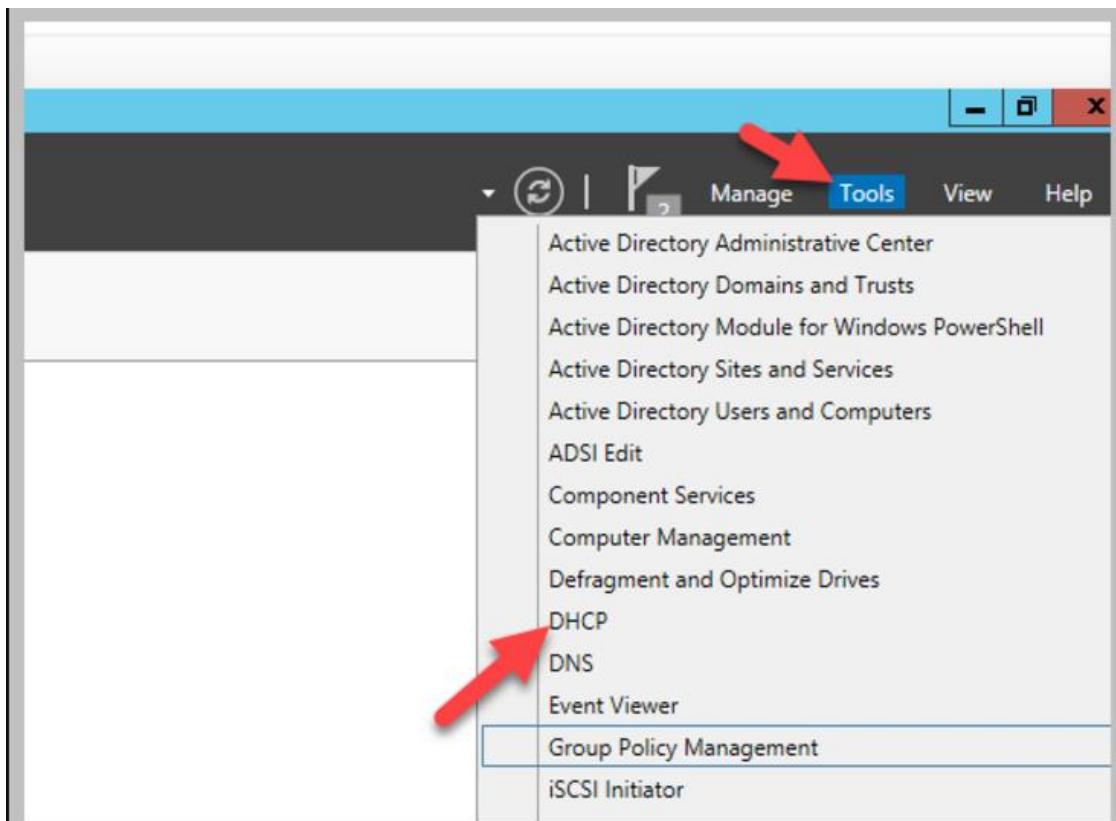


- Finally, click commit to complete the DHCP installation process

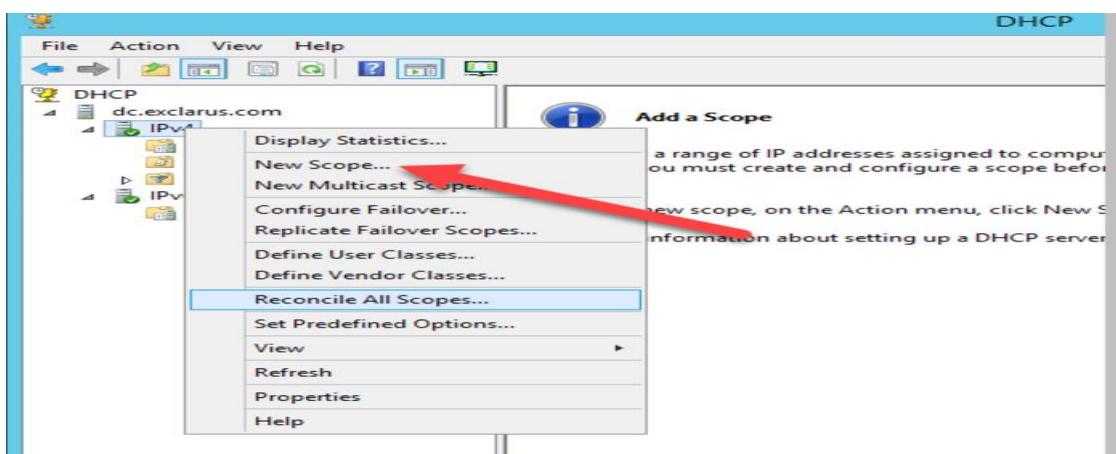


14. Configuring DHCP Server in Windows 2012 server

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



- Right click on IPv4 and click "New Scope"



- Choose any name for the scope

New Scope Wizard

Scope Name

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

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

Name:

Description:

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

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

New Scope Wizard

IP Address Range

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

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

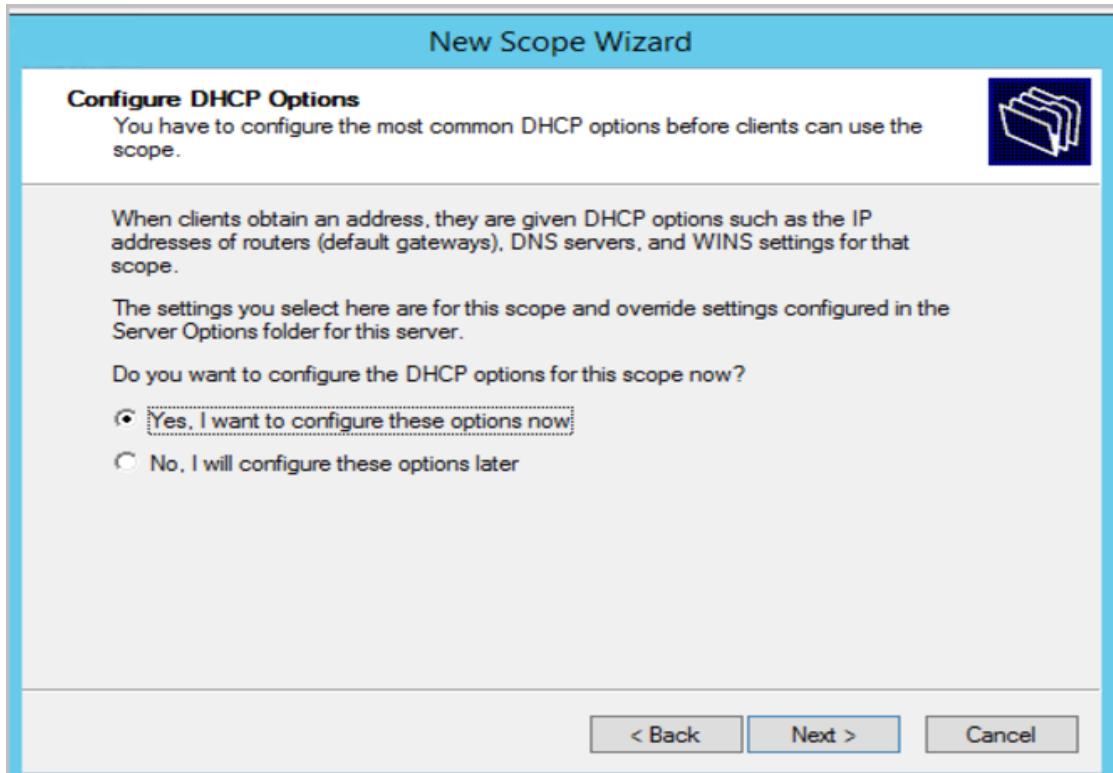
Configuration settings that propagate to DHCP Client

Length:

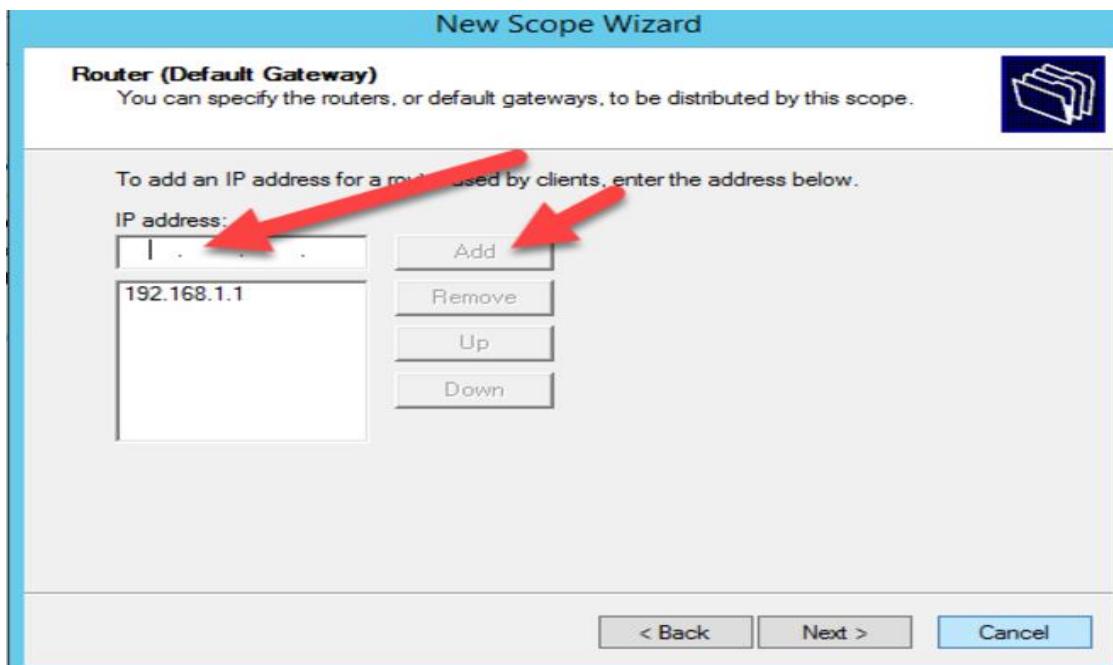
Subnet mask:

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

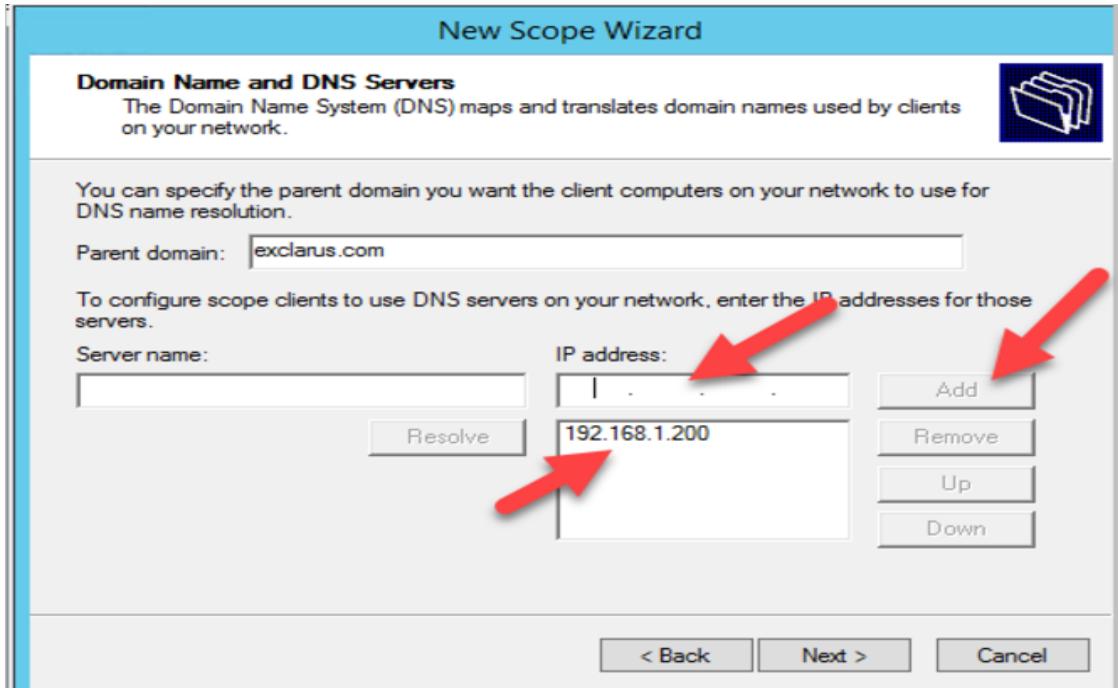
- Check “Yes” and click “Next”



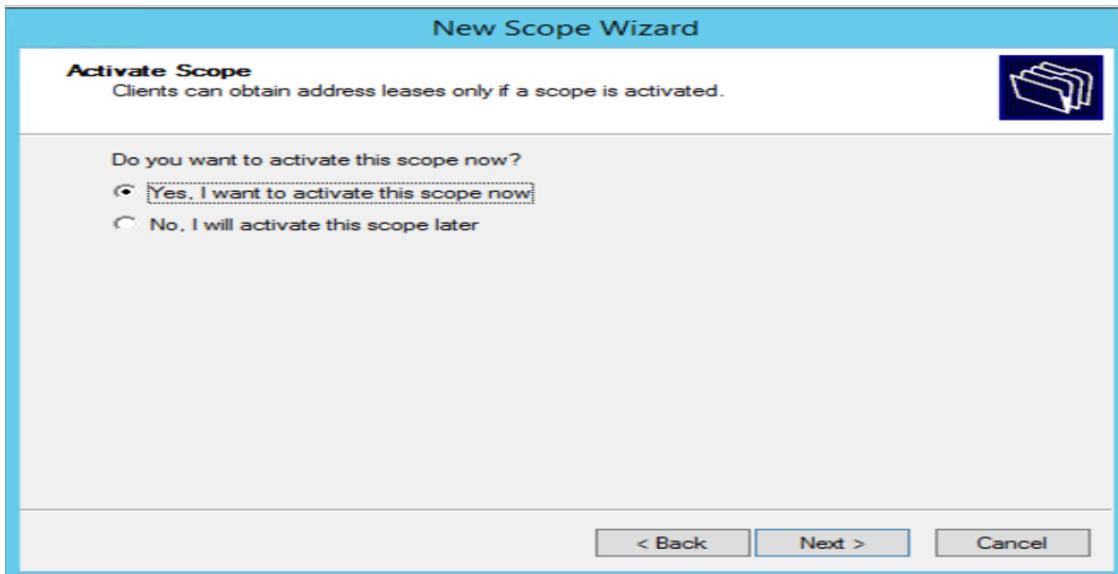
- Type IP address and click "Add". Click "Next"



- 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



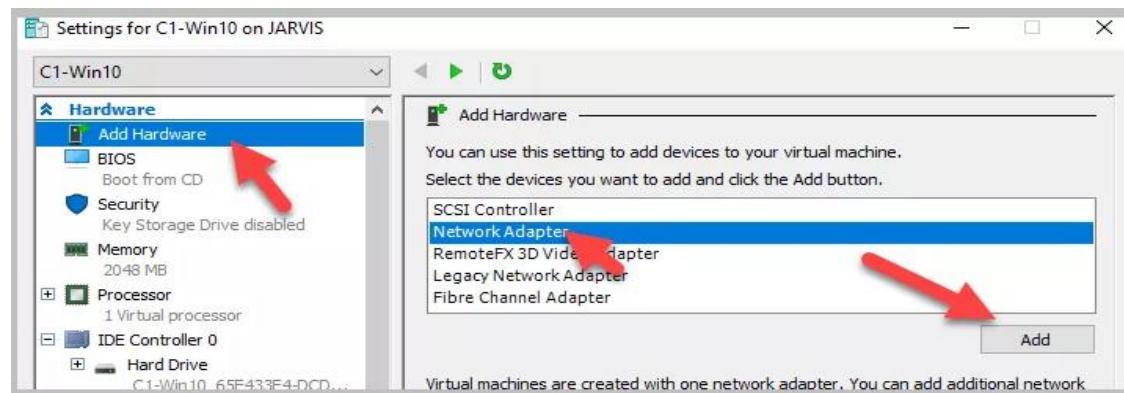
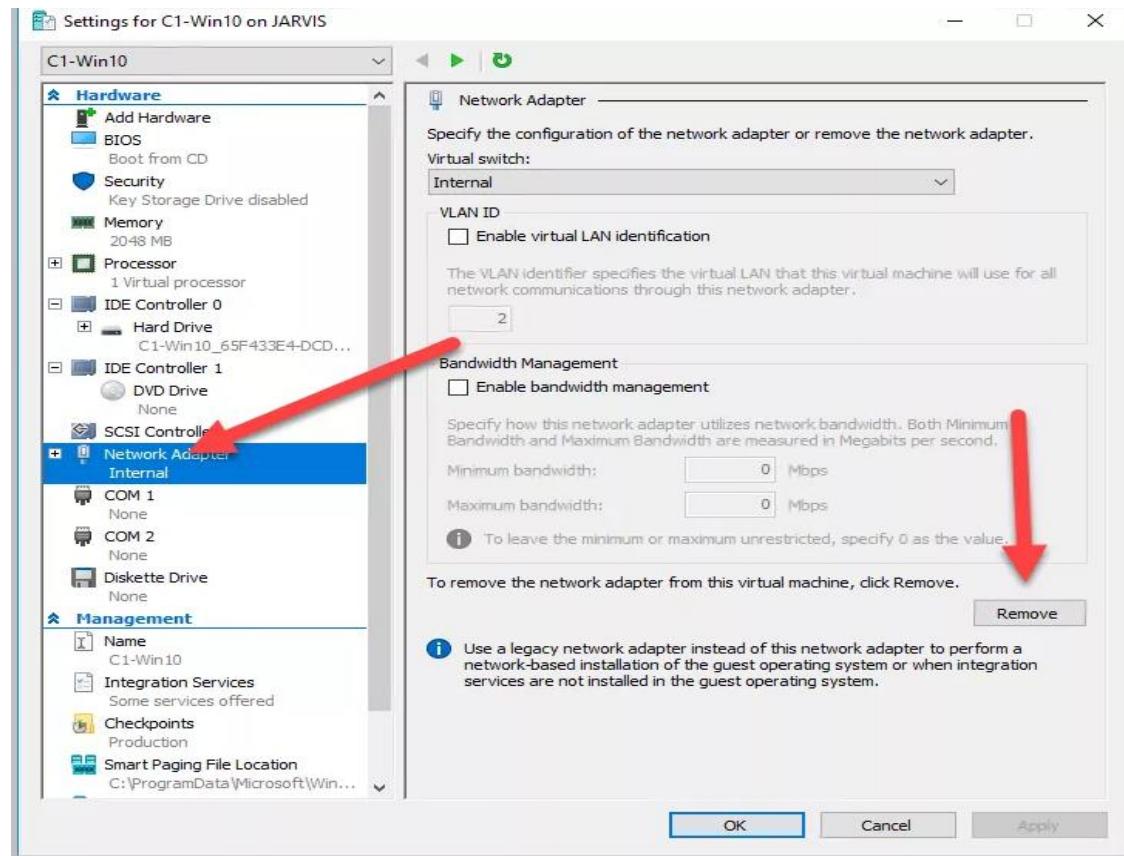
- Check "Yes" and click "Next"

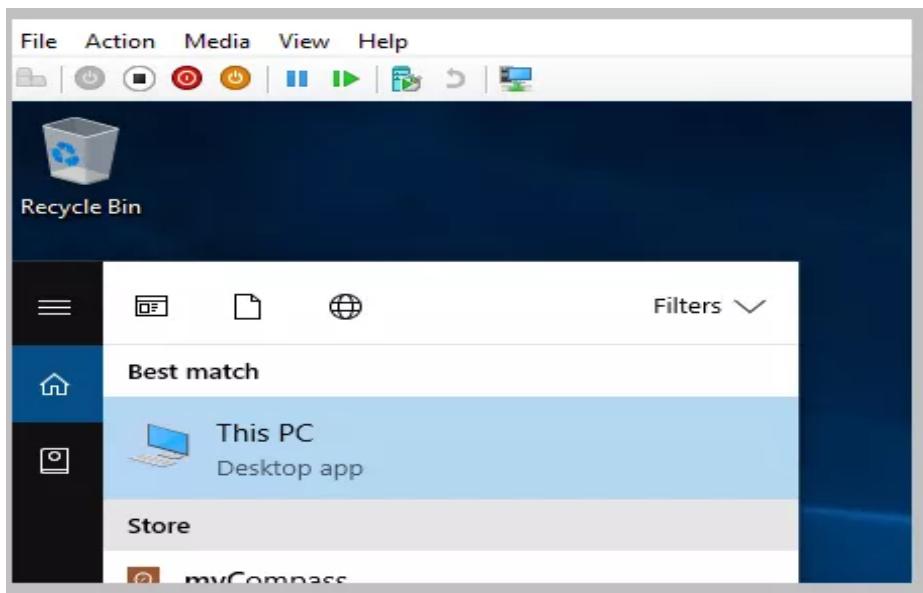
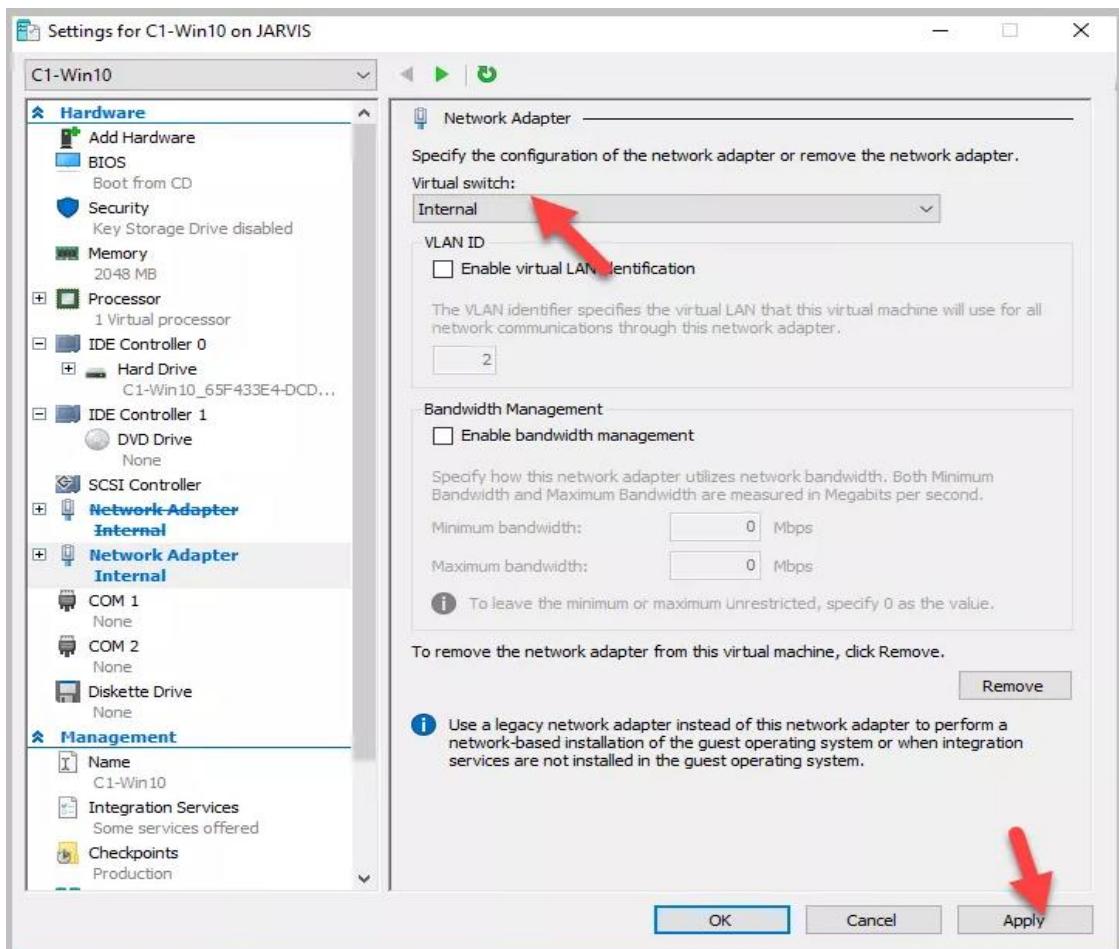


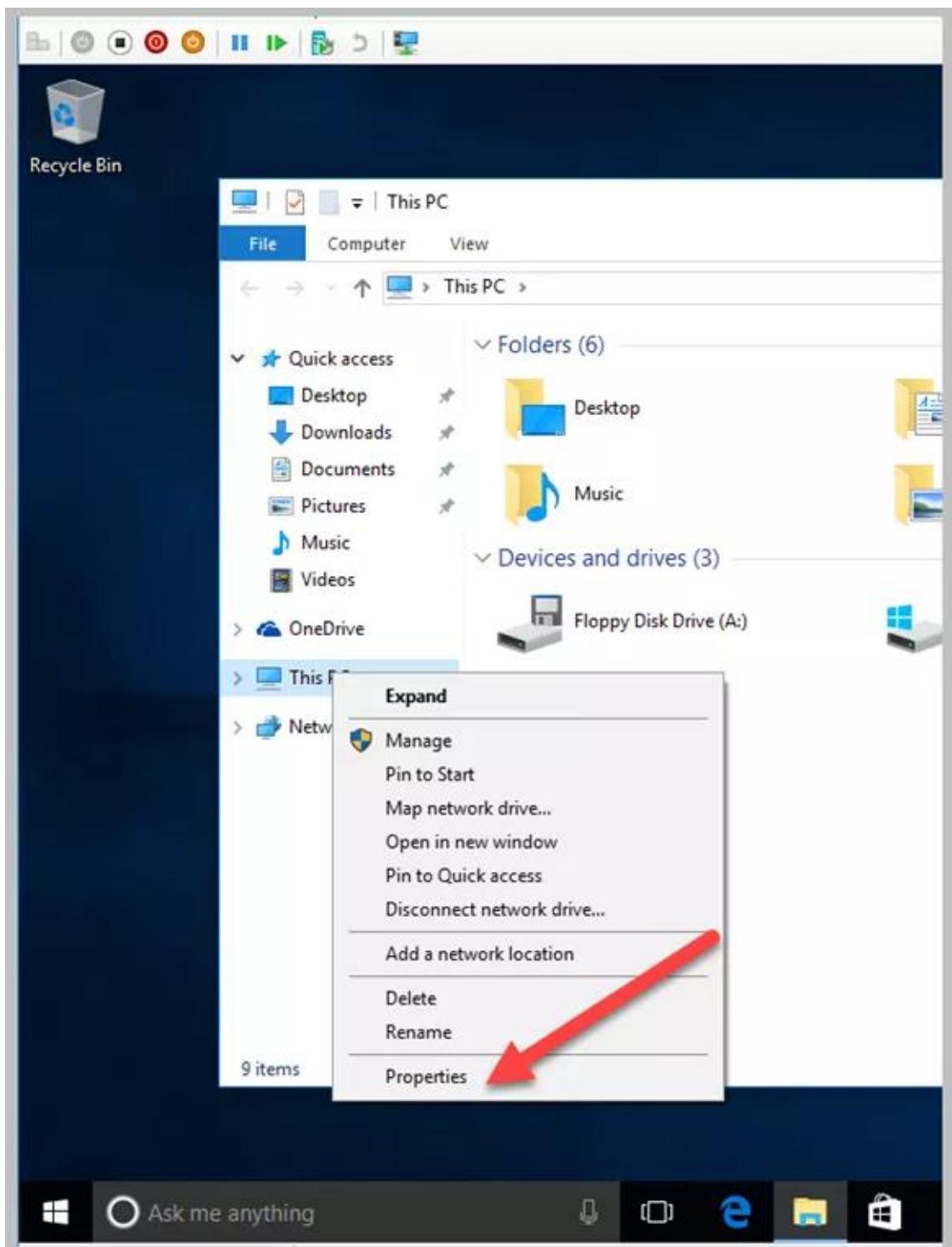
- The DHCP scope is now ready and the client systems will automatically be assigned a gateway as 192.168.1.1 and DNS server as 192.168.1.200

15. Joining Windows 10 to Domain

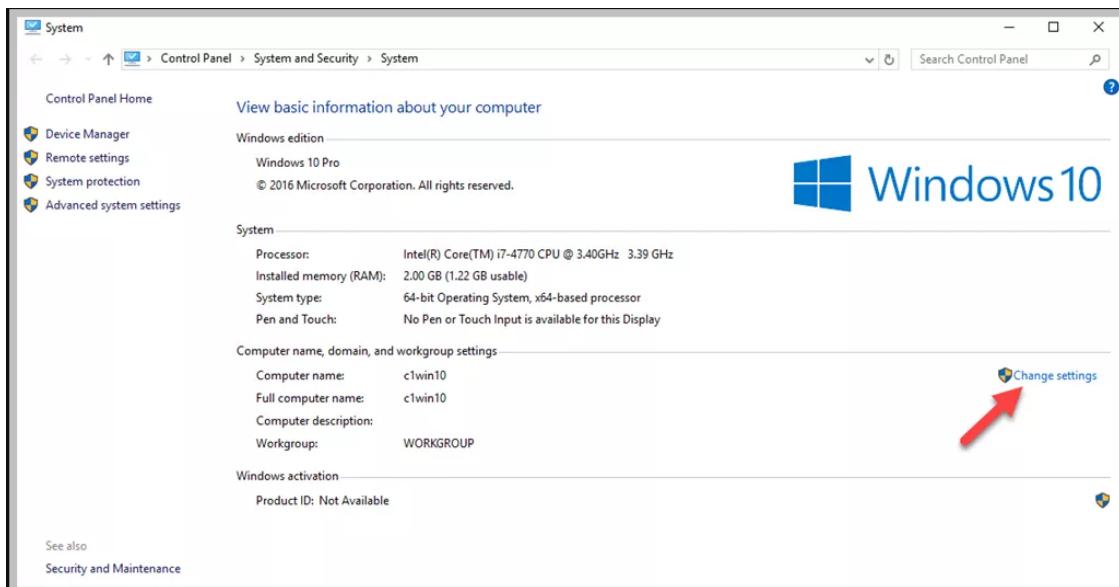
- Let's join the Windows 10 machine to the newly created domain exclarus.com. Before adding the computer to domain, it is better to remove the adapter and add a new adapter again as shown below. This will resolve any connectivity issues.



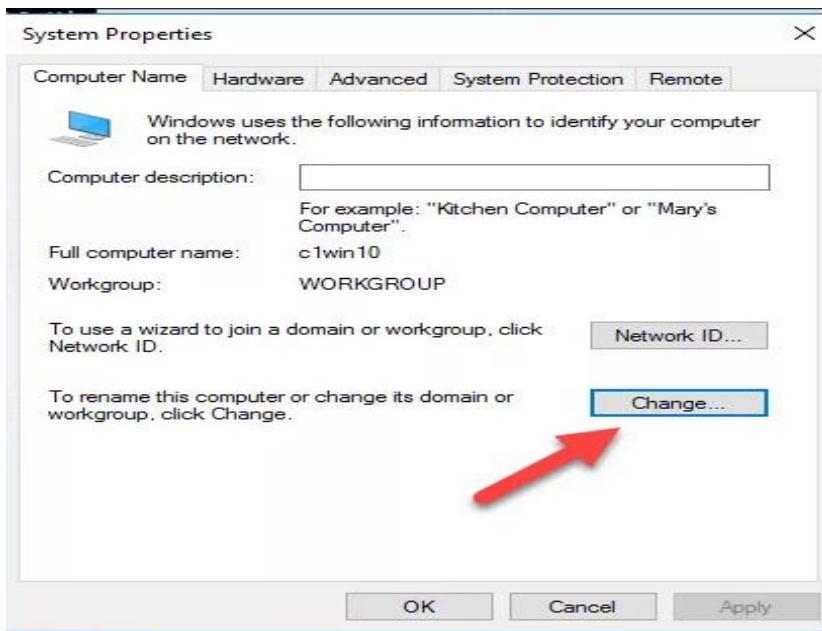




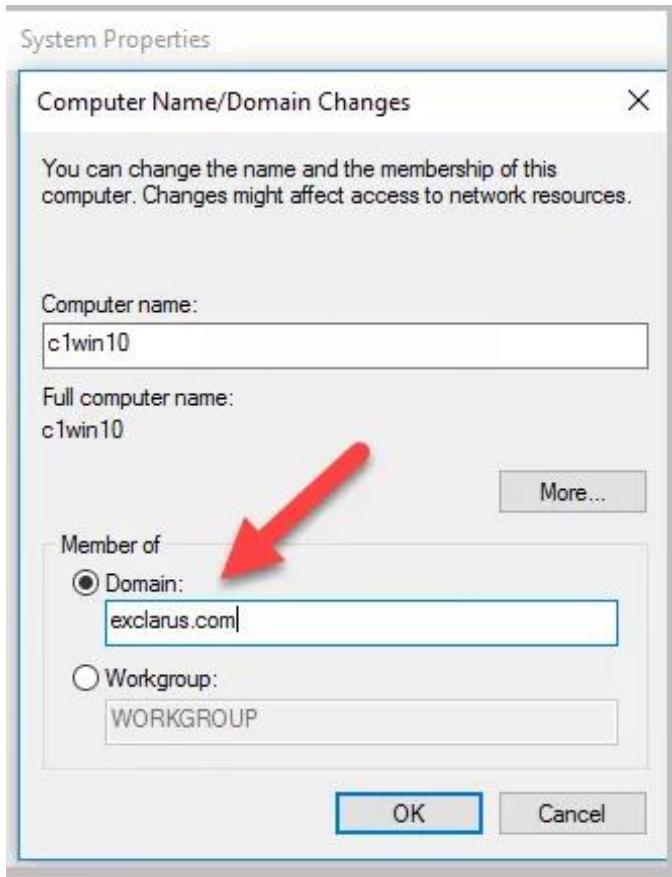
- Click “Change Settings”



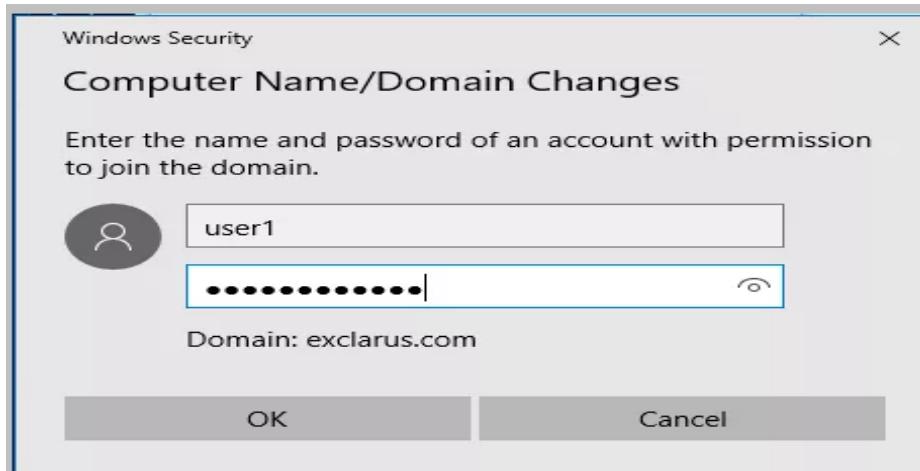
- Click “Change”



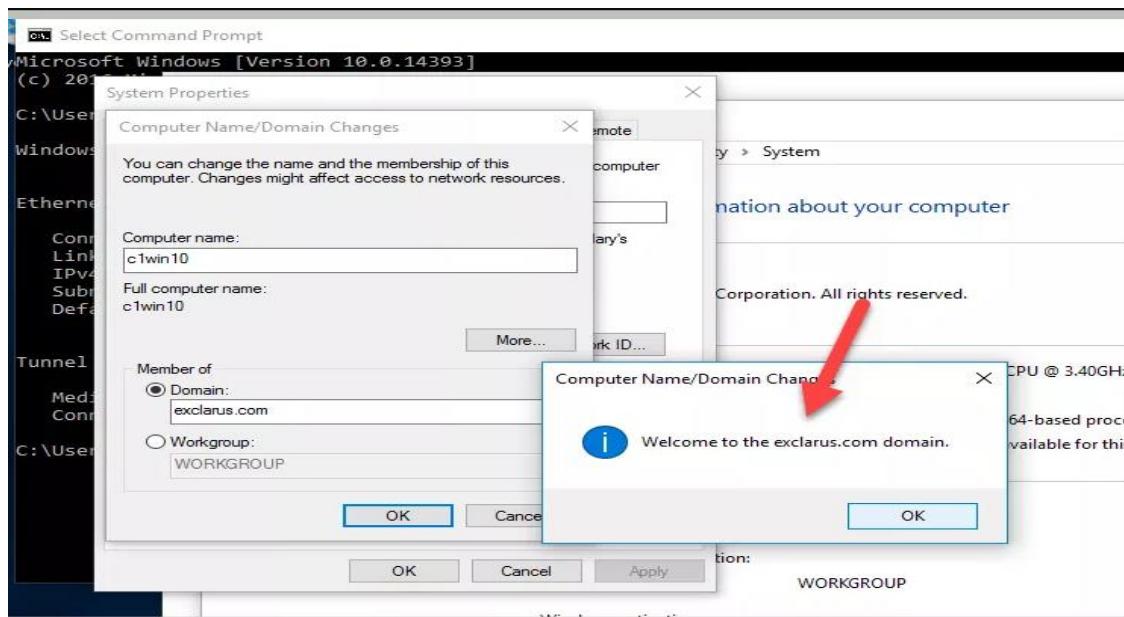
- Change the Domain to exclarus.com as shown below



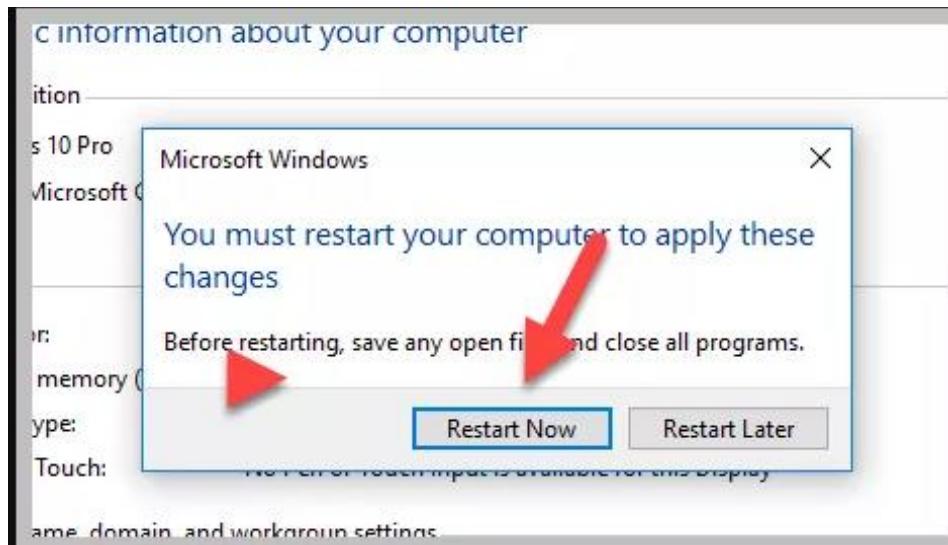
- When you click okay in the previous message box, it will prompt for a user name. Type the **user1** credentials we created in the previous steps



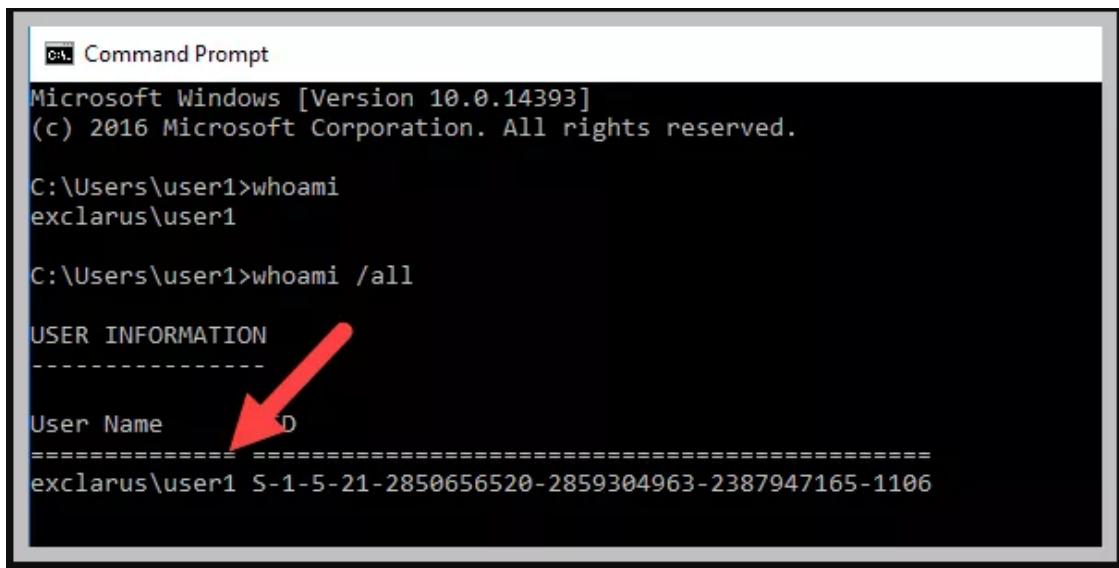
- Finally, we added the first machine to the active directory domain



- 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



```
Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\user1>whoami
exclarus\user1

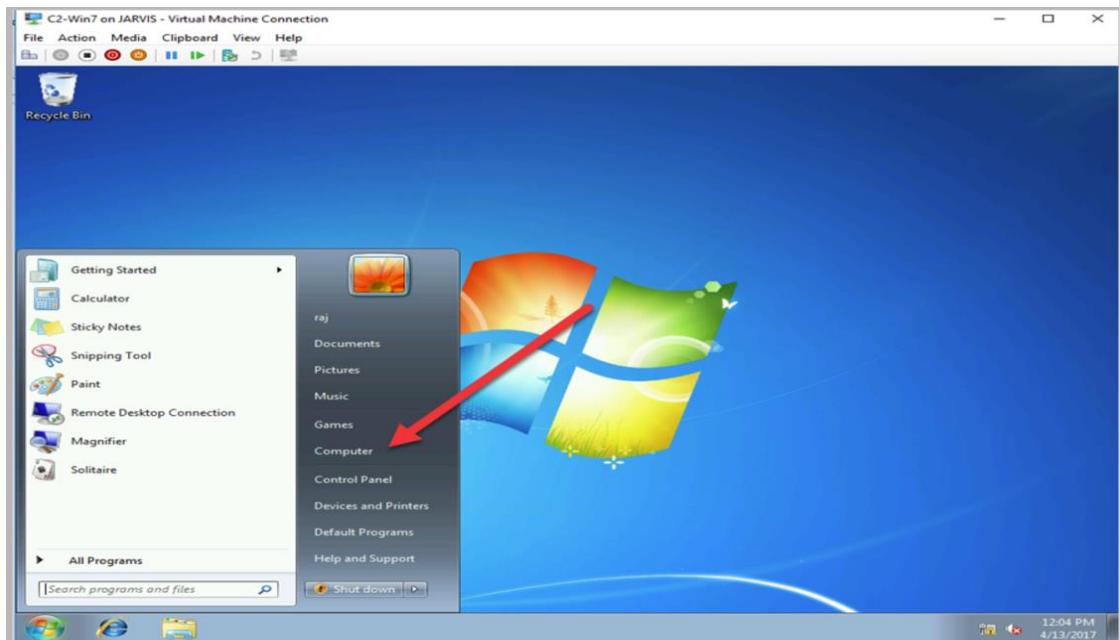
C:\Users\user1>whoami /all

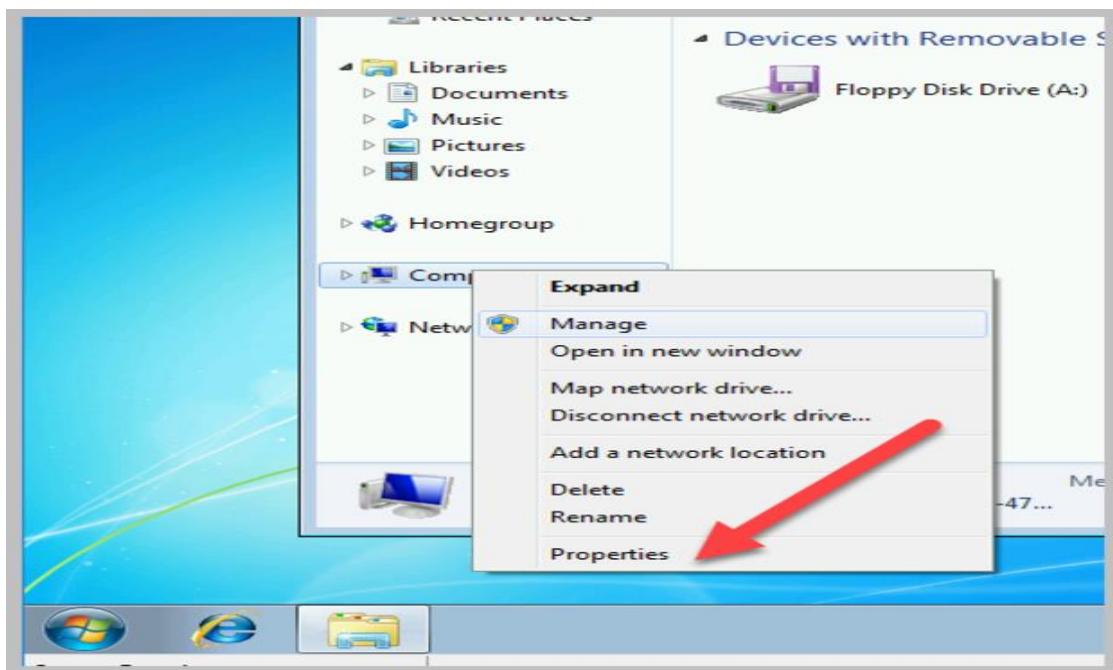
USER INFORMATION
-----
User Name          S
=====
exclarus\user1  S-1-5-21-2850656520-2859304963-2387947165-1106
```

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

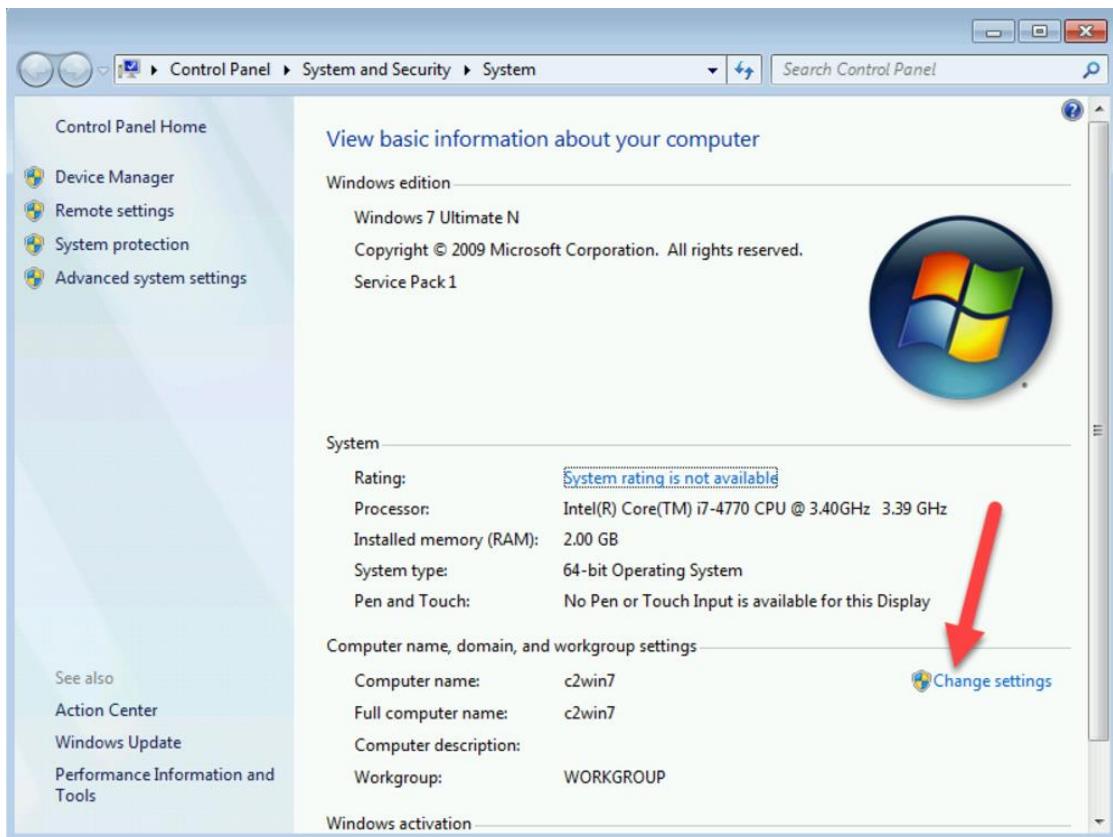
16. Joining Windows 7 to Domain

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

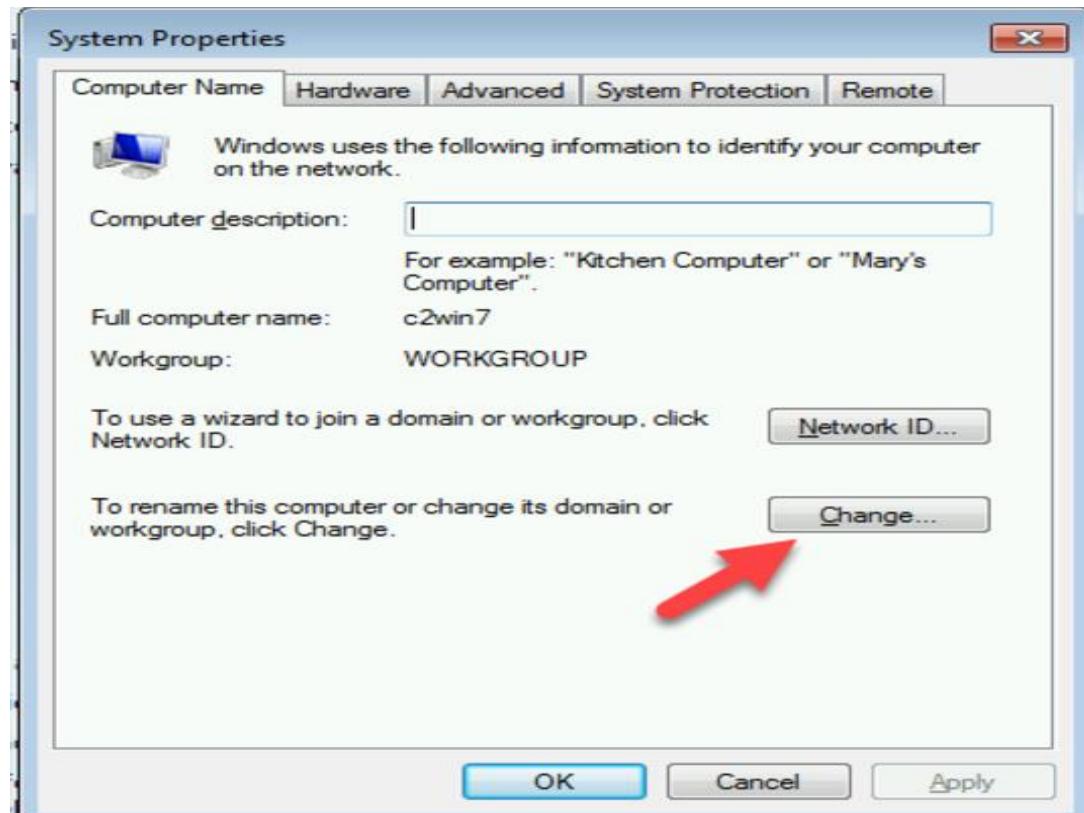




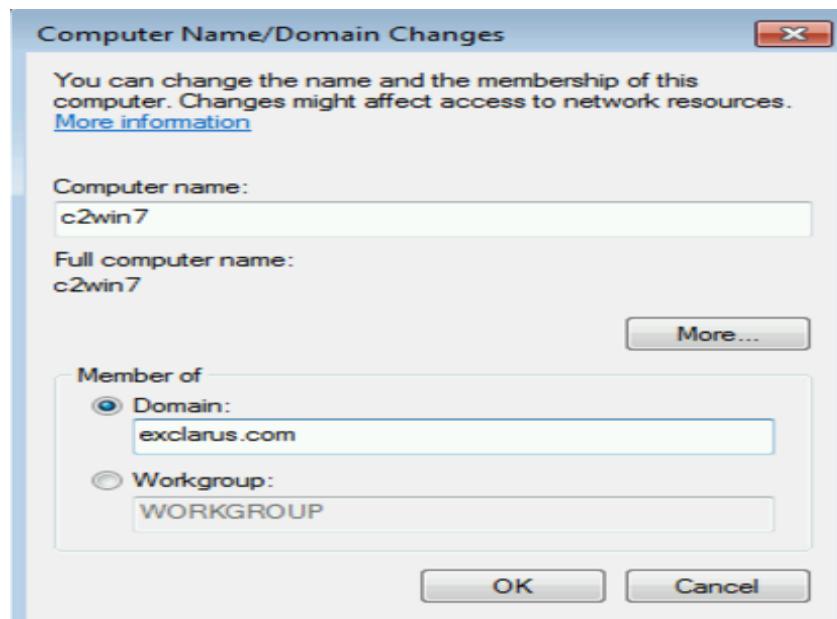
- Click "Change settings"



- Click "Change"

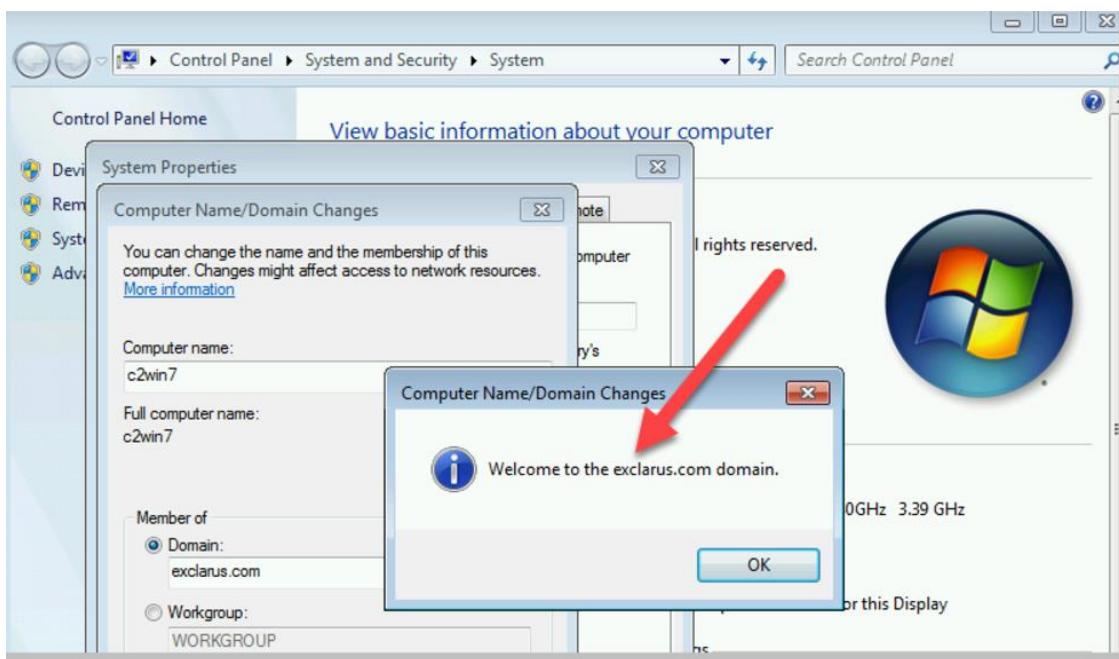


- Use Domain as exclarus.com and click ok. It should prompt for credentials





- 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

```
C:\> C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>Users\user1>ipconfig /all
Windows IP Configuration

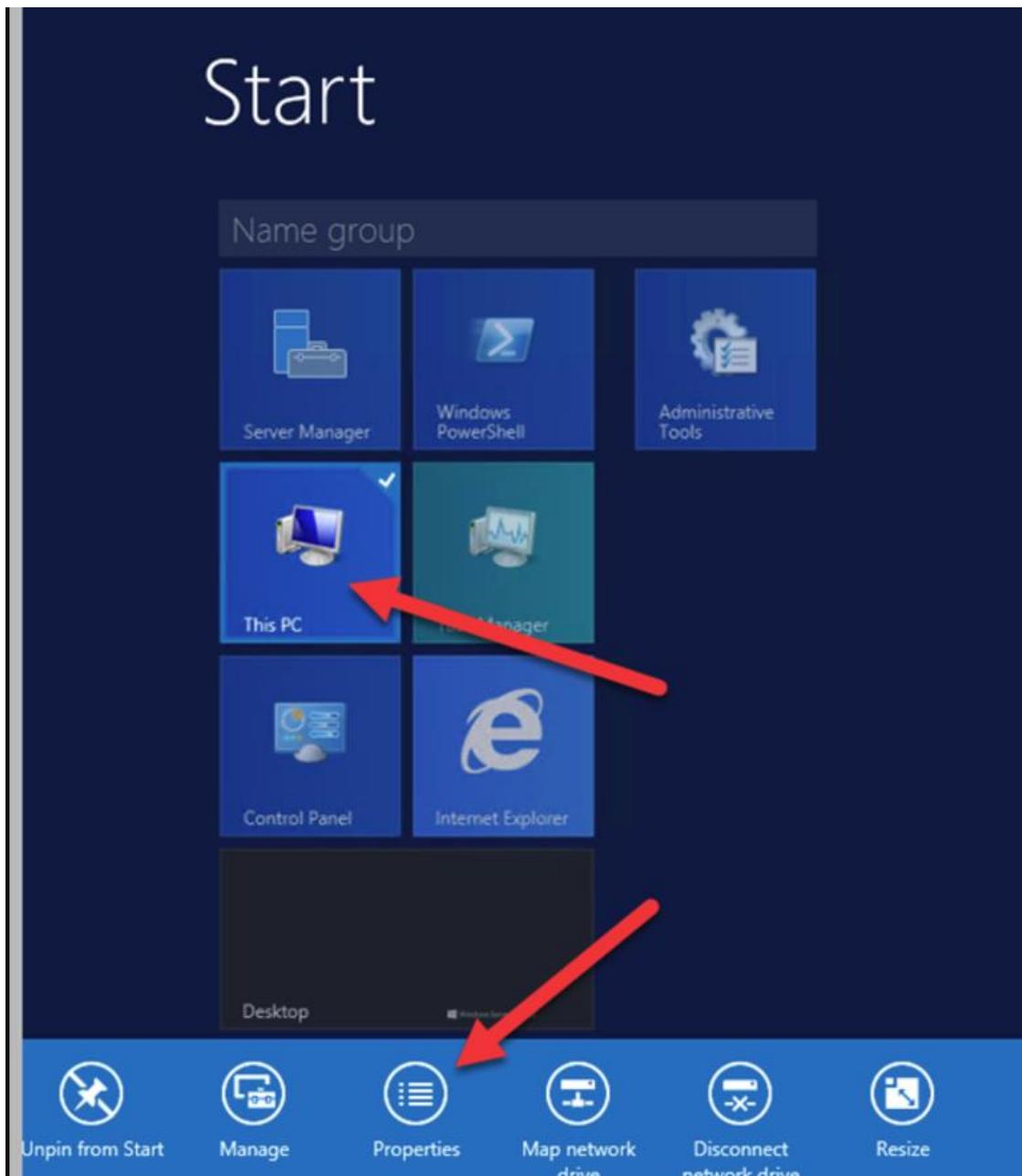
Host Name . . . . . : c2win7
Primary Dns Suffix . . . . . : exclarus.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : exclarus.com

Ethernet adapter Local Area Connection 2:

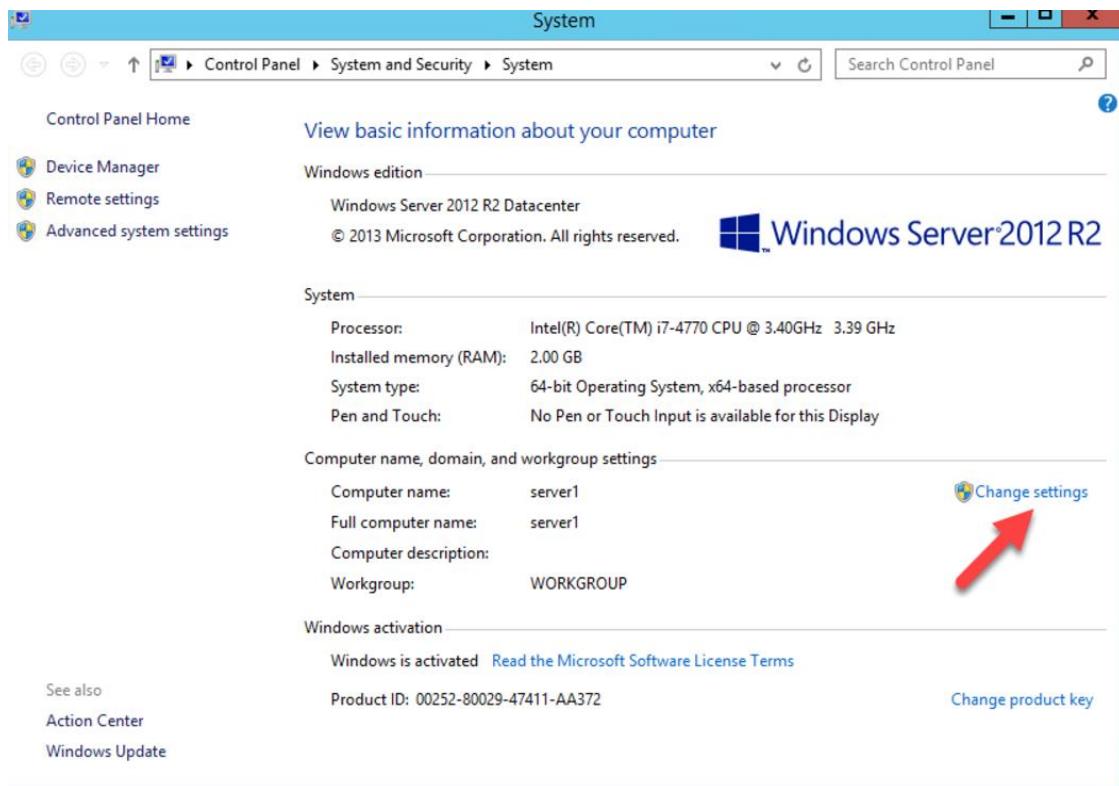
  Connection-specific DNS Suffix . . . . . : exclarus.com
  Description . . . . . : Microsoft Virtual Machine Bus Network Adapter #2
  Physical Address. . . . . : 00-15-5D-01-0D-36
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::4125:7525:2eb7:f36d%14<(Preferred)
  IPv4 Address. . . . . : 192.168.1.211<(Preferred)
  Subnet Mask . . . . . : 255.255.255.0
  Lease Obtained. . . . . : Thursday, April 20, 2017 12:06:11 PM
  Lease Expires . . . . . : Friday, April 21, 2017 12:06:11 PM
  Default Gateway . . . . . : fe80::1:1%14
                               192.168.1.1
  DHCP Server . . . . . : 192.168.1.200
  DHCPv6 IAID . . . . . : 285218141
  DHCPv6 Client DUID. . . . . : 00-01-00-01-80-CC-3C-00-15-5D-01-0D-30
  DNS Servers . . . . . : 192.168.1.200
  NetBIOS over Tcpip. . . . . : Enabled
```

17. Adding FileServer to Domain

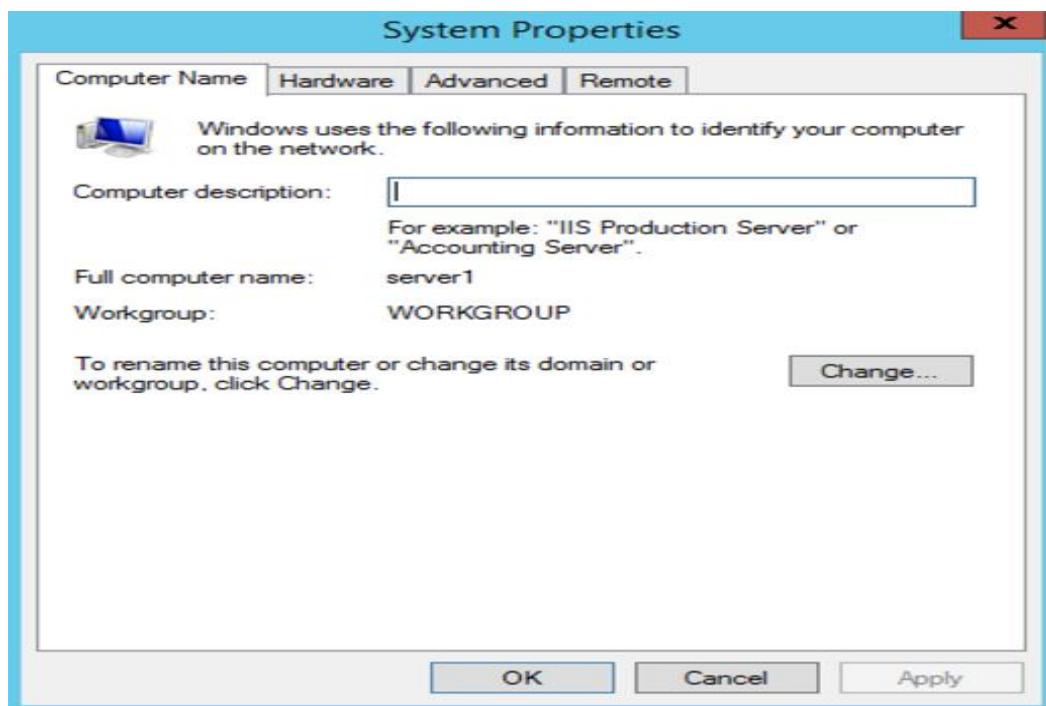
- Let's add the server1 to exclarus.com domain. Search for "This PC" and click properties



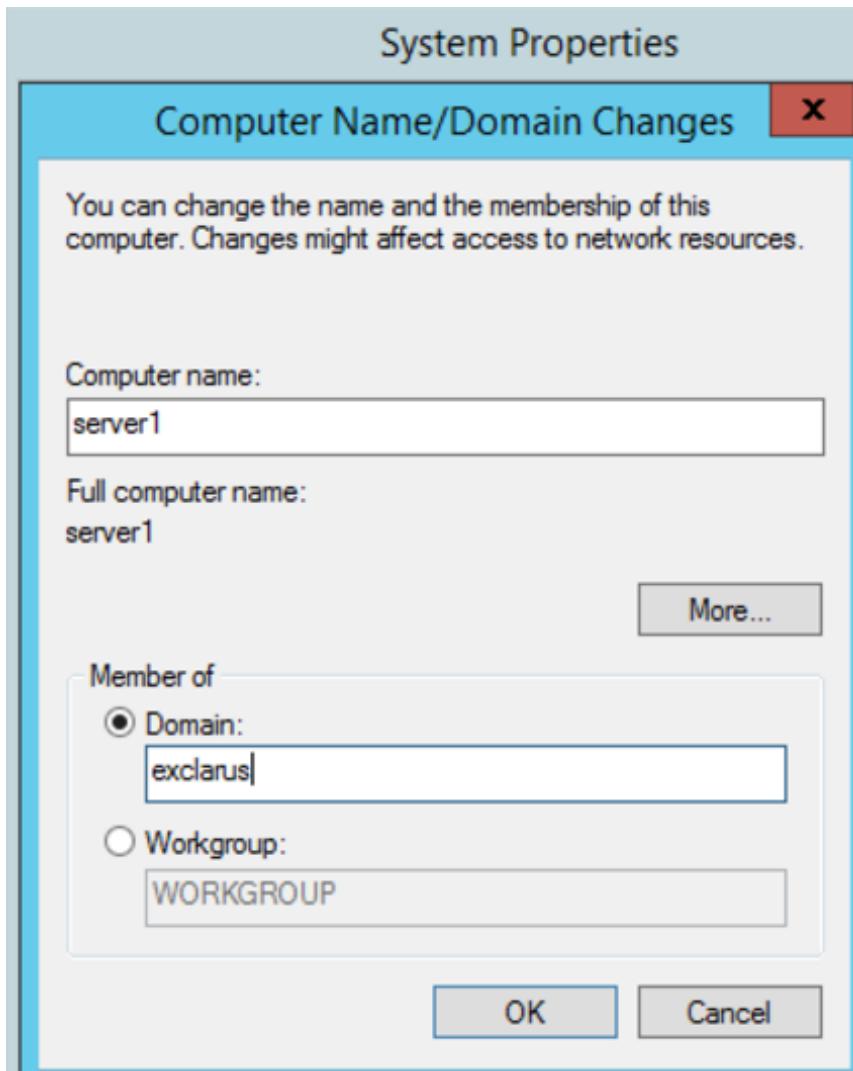
- Click "Change settings"



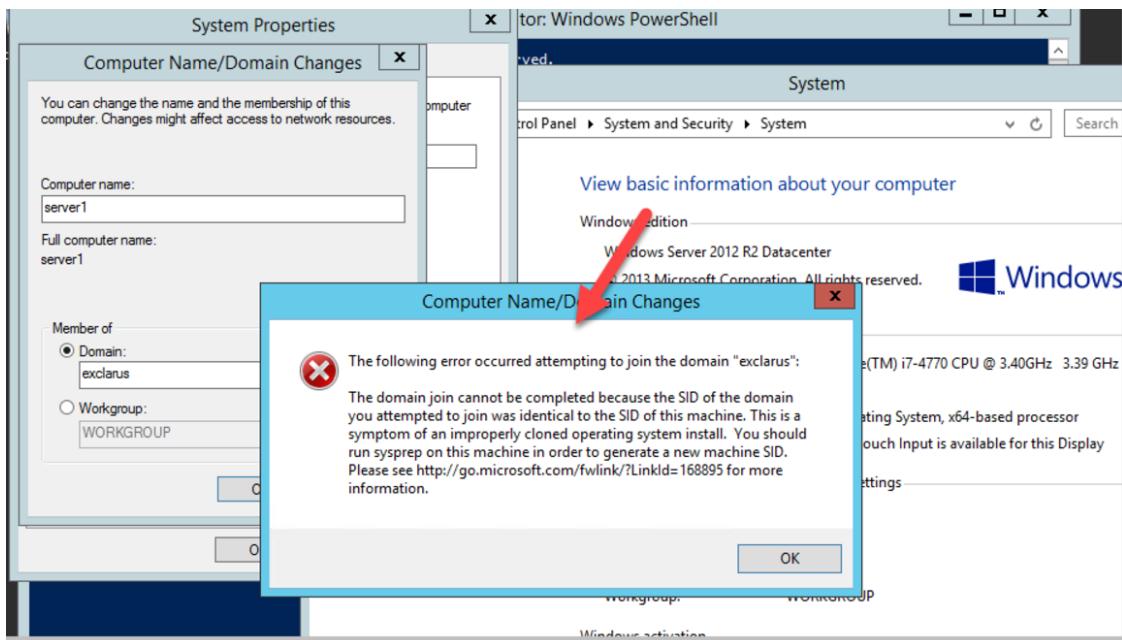
- Click "Change"



- 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



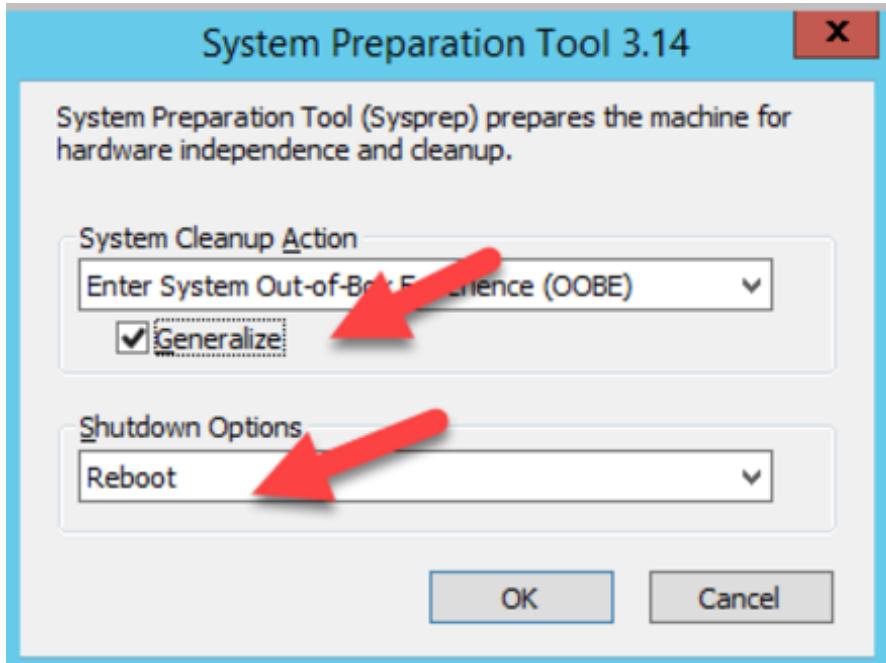
- Open a command prompt and go to c:\windows\system32\sysprep directory. Launch the command as shown below

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> cd C:\Windows
PS C:\Windows> cd system32
PS C:\Windows\system32> dir sys*
    Directory: C:\Windows\system32

Mode                LastWriteTime         Length Name
----                -              -          -
d----

```

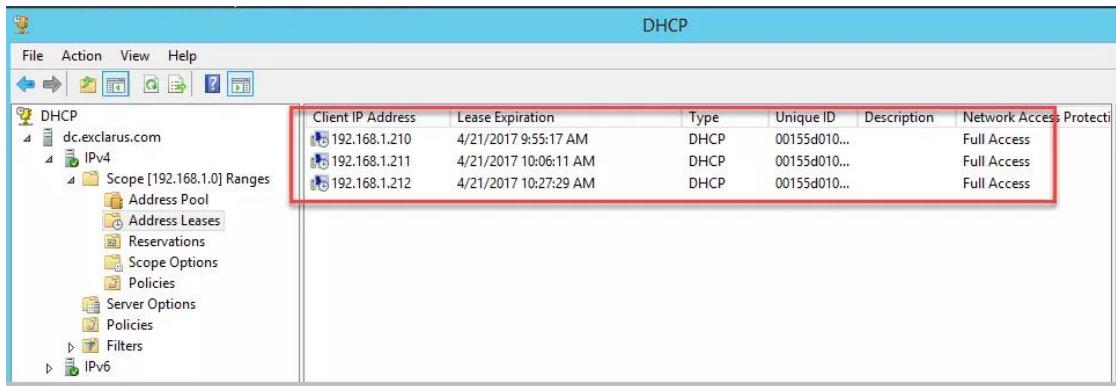
- Make sure to check the “Generalize” and reboot the system



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

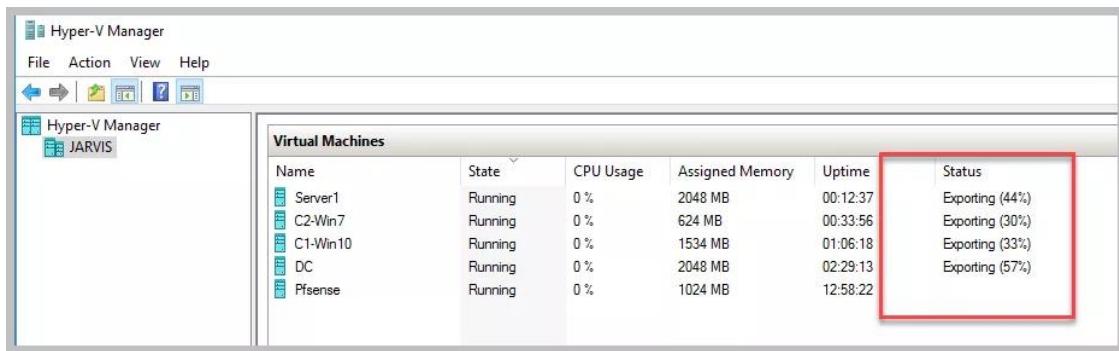
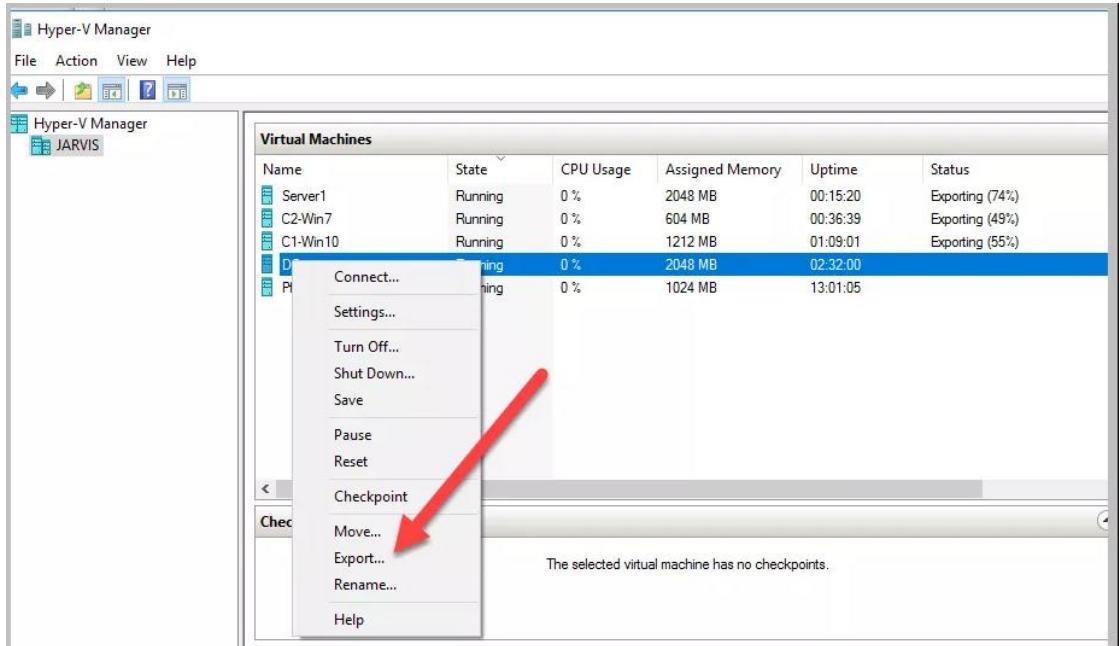
18. Viewing DHCP leases in Domain Controller

- 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

Name	Date modified	Type
DC-Export	4/12/2017 11:52 PM	File folder
Pfsense	4/13/2017 12:05 AM	File folder
Win7-Export	4/13/2017 12:05 AM	File folder
Win10-Export	4/13/2017 12:04 AM	File folder

The screenshot shows the Hyper-V Manager interface. In the center, there is a table titled "Virtual Machines" listing several virtual machines. One machine, named "DC", is selected and highlighted with a blue background. A context menu is open over the "DC" entry, displaying various options: Connect..., Settings..., Turn Off..., Shut Down..., Save, Pause, Reset, Checkpoint, Move..., Export..., Rename..., and Help. A red arrow points specifically to the "Checkpoint" option in the menu.

Name	State	CPU Usage	Assigned Memory	Uptime	Status
Server1	Running	0 %	2048 MB	00:16:21	
C2-Win7	Running	0 %	604 MB	00:37:40	Exporting (60%)
C1-Win10	Running	0 %	1212 MB	01:10:02	Exporting (67%)
DC	Running	0 %	2048 MB	02:33:00	
Pse	Running	0 %	1024 MB	13:02:06	

The status bar at the bottom right of the interface displays the message: "The selected virtual machine has no checkpoints."

- 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:3bcc:2099:dc09  
Link-local IPv6 Address . . . . . : fe80::f83f:af66:bbcc: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: Windows

```
PS C:\Users\Administrator> hostname
dc ←
PS C:\Users\Administrator>
PS C:\Users\Administrator> ping 10.0.1.13 ←
Ping 10.0.1.13 with 32 bytes of data:
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 ←
Ping 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

Administrator: Windows

```
cmd C:\Windows\system32\cmd.exe
C:\Users\user1>hostname
c2win7 ←
C:\Users\user1>ping 10.0.1.13 ←
Ping 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.

The screenshot shows the pfSense Status / Dashboard page. On the left, there is a System Information table with the following details:

Name	pfSense.loca...domain
System	Hyper-V Virtual Machine Serial: 3c815f0a-205d-11e7-8fd8-00155d010d31
Version	2.3.3-RELEASE (amd64) built on Thu Feb 16 06:59:53 CST 2017 FreeBSD 10.3-RELEASE-p16
Obtaining update status	
Platform	pfSense
CPU Type	Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz
Uptime	14 Hours 44 Minutes 41 Seconds
Current date/time	Thu Apr 13 19:26:50 UTC 2017
DNS server(s)	• 127.0.0.1 • 192.168.137.1 • 10.0.1.1 • 8.8.8.8

On the right, there is an Interfaces table showing two ports:

WAN	10Gbase-T <full-duplex>	192.168.137.190
LAN	10Gbase-T <full-duplex>	192.168.1.1

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

The screenshot shows the pfSense Status / Dashboard page. A red arrow points to the Firewall dropdown menu in the top navigation bar. When expanded, the menu shows the following options:

- Aliases
- NAT
- Rules
- Schedules
- Traffic Shaper
- Virtual IPs

- Got to Firewall/rules/LAN

The screenshot shows the pfSense Firewall / Rules / LAN interface. The 'LAN' tab is selected. In the bottom right corner of the main table area, there is a green 'Add' button with a white plus sign. Red arrows point to both the 'LAN' tab and the 'Add' button.

- 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

The screenshot shows the 'Edit Firewall Rule' configuration page. Several fields are highlighted with red arrows:

- Action:** Set to 'Block'.
- Protocol:** Set to 'Any'.
- Source:** 'Source' dropdown is 'any'. 'Source Address' dropdown shows '10.0.1.1/24'.
- Destination:** 'Destination' dropdown is 'Network'. 'Destination Address' dropdown shows '10.0.1.1/24'.

- Finally, Apply changes

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Floating WAN LAN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 7 /10.59 MB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	⚙️
✗ 0 /0 B	IPv4 TCP	10.0.1.1/24	*	*	*	*	none			🔗 🛡️ 🗑️ 🗑️
✗ 1 /2.75 GiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	🔗 🛡️ 🗑️ 🗑️
✗ 0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	🔗 🛡️ 🗑️ 🗑️

Add Add Delete Save Separator

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

DC on JARVIS - Virtual Machine Connection

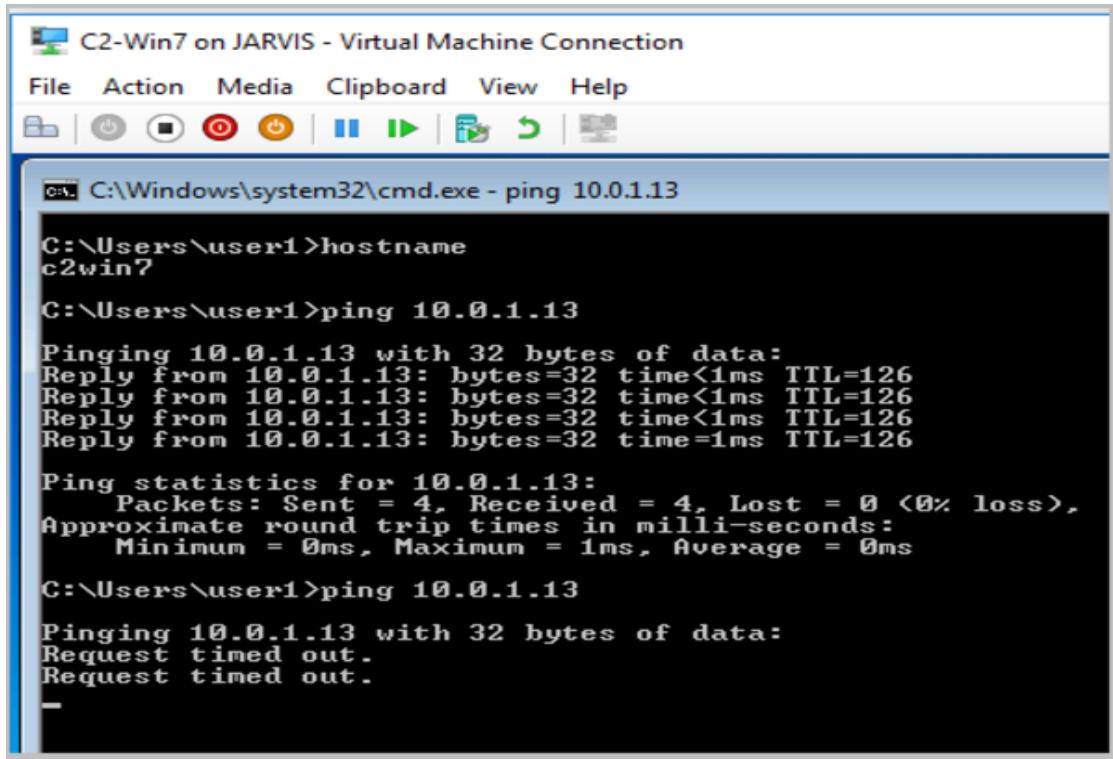
File Action Media View Help

Administrator: Windows PowerShell

```
PS C:\Users\Administrator> ping 10.0.1.13

Pinging 10.0.1.13 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.1.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\Administrator>
```



```
C:\Windows\system32\cmd.exe - ping 10.0.1.13

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>ping 10.0.1.13

Pinging 10.0.1.13 with 32 bytes of data:
Request timed out.
Request timed out.
```

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.